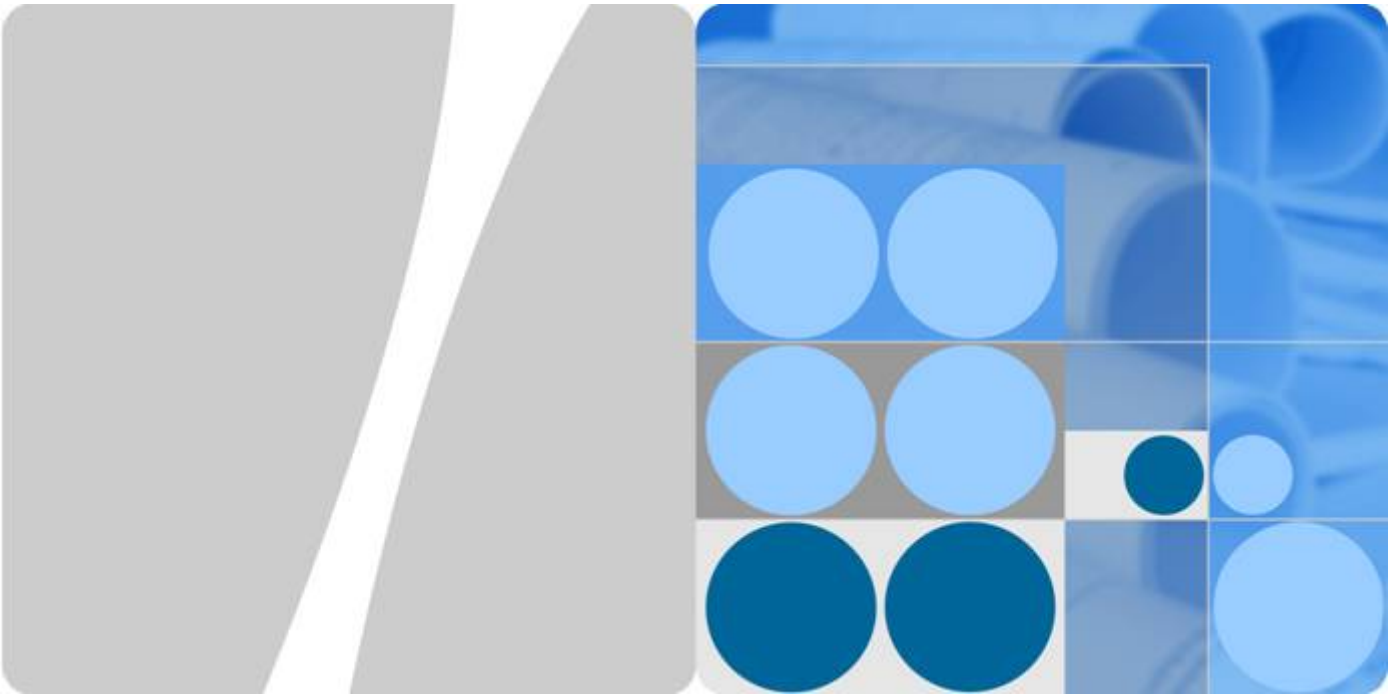


NetEngine AR

V300R022

典型配置案例（命令行）

文档版本　09

发布日期　2023-04-03

华为技术有限公司

版权所有 © 华为技术有限公司 2023。 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、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明

和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： https://e.huawei.com

目 录

1 前言.....1
2 入门和基础操作.....4
2.1 开局部署.....4
2.1.1 配置通过 U 盘完成软件升级、业务部署的示例.....4
2.2 登录设备（命令行方式）.....8
2.2.1 配置用户通过 Console 口首次登录设备的示例.....8
2.2.2 配置用户以 Console 口登录设备时要通过密码验证的示例.....11
2.2.3 通过 Console 口对设备进行基本配置示例.....12
2.2.4 配置用户通过 Telnet 登录设备.....13
2.2.5 配置用户通过异步串口重定向登录其他设备的示例.....14
2.2.6 配置用户通过 STelnet 登录设备（Password 认证方式）.....16
2.2.7 配置用户通过 STelnet 登录设备示例（RSA 认证方式）.....17
2.2.8 配置设备作为客户端，采用 RADIUS 认证登录其他设备的示例.....23
2.2.9 查看设备基本状态.....25
2.3 升级设备（命令行方式）.....28
2.3.1 通过 BootLoader SFTP 方式升级系统文件的示例.....29
2.3.2 通过 BootLoader FTP 方式升级系统文件的示例.....32
2.3.3 通过 BootLoader TFTP 方式升级系统文件的示例.....35
2.3.4 配置路由器作为 TFTP Client 升级系统文件的示例.....38
2.3.5 配置路由器作为 FTP Client 升级系统文件的示例.....40
2.3.6 配置路由器作为 FTP Server 升级系统文件的示例.....41
2.4 操作 BootLoader 菜单.....43
2.4.1 配置通过 BootLoader 清除 Console 口和 Telnet 密码的示例.....43
2.4.2 配置通过 BootLoader 修改文件名的示例.....47
2.4.3 配置通过 BootLoader 修改 BootLoader 密码的示例.....50
2.5 设备管理.....51
2.5.1 配置向日志主机输出日志信息的示例.....51
2.5.2 配置向日志文件输出日志信息的示例.....52
3 访问 Internet 外网.....54
3.1 NAT.....54
3.1.1 配置内网用户通过 Easy IP 方式访问 Internet 外网的示例.....54
3.1.2 配置内网用户通过 NAT 地址池方式访问 Internet 外网的示例.....55

 版权所有 © 华为技术有限公司

3.1.3 配置通过 NAT 访问 Internet 外网，并对外提供 www 服务的示例 57
3.1.4 配置 VPN 用户通过 NAT 方式访问 Internet 外网的示例 59
3.1.5 配置通过 NAT Static 和 NAT Outbound 实现公网用户与公网服务器间互访的示例 60
3.1.6 配置通过 NAT 和重定向实现双出口，且对外提供 web 服务的示例 62
3.1.7 配置内网用户通过 NAT 访问地址重叠的外网服务器 65
3.1.8 配置 NAT 实现对源和目的 IP 地址同时进行转换 66
3.1.9 配置公网和私网用户通过非公网口的 IP 地址访问内部服务器和 Internet 示例 67
3.1.10 配置公网和私网用户通过公网口的 IP 地址访问内部服务器和 Internet 示例 71
3.1.11 配置私网用户通过公网口的 IP 地址访问内部服务器和 Internet 示例 76
3.1.12 配置公网和私网用户通过非公网口的 IP 地址访问内部服务器示例 80
3.1.13 配置公网用户通过非公网口的 IP 地址访问内部服务器示例 82
3.1.14 配置公网用户通过公网口的 IP 地址访问内部服务器示例 85
3.2 双出口 89
3.2.1 配置 PPPoE 拨号双链路负载分担示例 89
3.2.2 配置 PPPoE 拨号双链路上行备份示例 92
3.2.3 配置静态 IP 双链路负载分担示例 94
3.2.4 配置静态 IP 双链路上行备份示例 97
3.2.5 配置 PPPoE 拨号和静态 IP 双链路负载分担示例 100
3.2.6 配置 PPPoE 拨号和静态 IP 双链路上行备份示例 104
4 组建局域网 108
4.1 配置三层链路聚合增加链路带宽并提高可靠性的示例 108
4.2 配置划分 VLAN 的示例 110
4.3 配置子接口实现 VLAN 间通信的示例 111
4.4 配置 VLANIF 接口实现 VLAN 间通信的示例 113
4.5 配置 GVRP 实现 VLAN 自动注册的示例 114
4.6 配置透明网桥实现远程同一网段互通的示例 116
4.7 配置透明网桥实现远程不同网段互通的示例 117
4.8 配置透明网桥实现 QinQ 传输的示例 119
4.9 配置 UDP Helper 实现跨网用户使用主机名互访的示例 120
4.10 配置路由式 Proxy ARP 实现远程同一网段互通的示例 121
5 通过专线实现广域网互联 123
5.1 配置端口隔离示例 124
5.2 配置 POS 接口示例 125
5.3 配置 CPOS 接口示例 126
5.4 配置 ATM 接口示例 128
5.5 配置银行网点通过 E1 链路接入二级分行示例（E1 模式） 129
5.6 配置银行网点通过 E1 链路接入二级分行示例（CE1 模式） 130
5.7 配置企业采用 3G 链路访问互联网示例（通过 WCDMA 网络） 131
5.8 配置企业通过 LTE 链路接入 Internet 示例 133
5.9 配置 IPoA 实现局域网接入 Internet 的示例 134
5.10 配置 IPoEoA 实现局域网接入 Internet 的示例 135
5.11 配置 PPPoEoA 实现用户利用 PPP 协议接入 Internet 的示例 137

 版权所有 © 华为技术有限公司

5.12 配置 PPPoA 实现用户利用 PPP 协议接入 Internet 的示例 139
5.13 配置帧中继专线利用 PPP 协议实现局域网互联的示例 140
5.14 配置帧中继专线利用 IP 协议实现局域网互联的示例 142
5.15 配置采用 MP-Group 进行 MP 绑定示例 143
5.16 配置将 PPP 链路直接绑定到 VT 上实现 MP 的示例 144
5.17 配置按照用户名查找虚拟接口模板实现 MP 的示例 146
5.18 配置设备作为 PPPoE Client，实现设备接入 Internet 的示例 147
5.19 配置设备作为 PPPoE Client（IPv6），实现设备接入 Internet 的示例 149
5.20 配置设备作为 PPPoE Server，实现用户安全接入 Internet 的示例 151
5.21 配置设备利用 PPPoE 技术通过外置的 ADSL Modem 接入 Internet 的示例 153
5.22 配置设备通过 Modem 拨号接入 PSTN 的示例(轮询 DCC 方式) 154
5.23 配置设备通过 ISDN PRI 接口拨号接入 ISDN 的示例（共享 DCC 方式） 156
5.24 配置设备利用 HDLC 技术实现互通的示例 157
6 通过 VPN 实现广域网互联 159
6.1 L2TP 159
6.1.1 配置来自分支机构不同域的用户通过 L2TP 实现与总部互通的示例 159
6.1.2 配置分支与总部之间通过 L2TP 方式实现互通，且与总部服务器之间的数据通过 IPSec 加密传输的示例 162
6.1.3 配置分支机构与总部之间通过 L2TP over IPSec 方式实现安全互通的示例 165
6.1.4 配置远程拨号用户通过 L2TP 隧道接入总部的示例 167
6.1.5 配置远程拨号用户通过认证域建立 L2TP 隧道接入总部的示例（Windows 7） 169
6.1.6 配置移动办公用户通过认证域建立 L2TP 隧道接入总部的示例（Windows 10） 172
6.1.7 配置远程拨号用户通过认证域建立 L2TP 隧道接入总部的示例（VPN Client） 174
6.1.8 配置远程拨号用户通过 L2TP over IPSec 方式接入总部的示例 180
6.1.9 配置 LAC 接入 PPPoE 用户发起 L2TP 隧道连接来实现分支与总部互通的示例 186
6.1.10 配置 LAC 接入 PPPoE 用户发起 L2TP 隧道连接来实现分支与总部互通的示例（RADIUS 服务器） 188
6.1.11 配置 LAC 自拨号发起 L2TP 隧道连接来实现分支与总部互通的示例 190
6.1.12 配置 LAC 自拨号发起 L2TP 隧道连接来实现分支与总部互通的示例（RADIUS 服务器） 192
6.1.13 配置 LNS 多实例实现分支与总部互通的示例 194
6.1.14 配置 LNS 多实例实现分支与总部互通的示例（RADIUS 服务器） 197
6.1.15 配置 LAC 自拨号发起 L2TP 隧道连接来实现分支与总部互通示例（使用 3G 接口） 200
6.1.16 配置 LAC 自拨号发起 L2TP 隧道连接来实现分支与总部互通示例（使用 4G 接口） 202
6.1.17 配置移动办公用户使用 Android 手机发起 L2TP 隧道连接示例 204
6.1.18 配置分支机构与总部之间通过 L2TP over Bridge 方式建立二层网络互通的示例 206
6.2 GRE 209
6.2.1 配置 GRE 隧道，并在隧道上运行静态路由实现互通的示例 209
6.2.2 配置 GRE 隧道，并在隧道上运行 OSPF 实现互通的示例 211
6.2.3 配置 GRE over GRE 实现数据加密示例 213
6.2.4 配置分支机构与总部之间通过 IPSec Over GRE 方式实现安全互通的示例 215
6.2.5 配置分支与总部通过 GRE 隧道实现互通的示例 217
6.2.6 配置 IPv6 over IPv4 GRE 隧道示例 220
6.2.7 配置 Ethernet over GRE 隧道示例 222

 版权所有 © 华为技术有限公司

6.3 DSVPN 226
6.3.1 配置分支机构之间相互路由学习，并通过 DSVPN 方式实现互通的示例（适用少量分支机构） 226
6.3.2 配置分支机构只保存到总部的汇聚路由，并通过 DSVPN 方式实现分支机构之间互通的示例（适用多个分支机构） 228
6.3.3 配置利用总部 Hub 备份，分支机构之间通过 DSVPN 方式实现稳定互通的示例 230
6.4 IPSec 240
6.4.1 配置采用手工方式建立 IPSec 隧道示例 240
6.4.2 配置设备之间通过 IKE 动态协商方式建立 IPSec 隧道的示例（不对对等体存活进行检测） 242
6.4.3 配置设备之间通过 IKE 动态协商方式建立 IPSec 隧道的示例（对对等体存活进行检测） 244
6.4.4 配置穿越 NAT 设备建立 IPSec 隧道的示例 246
6.4.5 配置分支机构与总部利用 IPSec 隧道实现总部多个访问资源独立保护的示例 249
6.4.6 配置远程拨号用户通过 IPSec 隧道接入总部的示例 252
6.4.7 配置设备之间建立 IPSec 隧道时需要通过 PKI 方式的身份认证的示例 255
6.4.8 配置总部部署 VRRP 的场景下，分支机构利用 VRRP 虚地址与总部建立 IPSec 隧道的示例 260
6.4.9 配置总部采用 IPSec 策略模板与分支建立多条 IPSec 隧道的示例 263
6.4.10 配置分支机构通过 3G 接口访问 Internet，总部利用 IPSec 策略模板与分支建立 IPSec 隧道的示例 266
6.4.11 配置设备之间通过 GRE Over IPSec 方式实现互通的示例 268
6.4.12 配置分支机构与总部之间运行 OSPF，并通过 GRE Over IPSec 方式实现互通的示例 271
6.4.13 配置分支机构与总部之间通过 GRE Over IPSec 方式实现互通，并穿越 NAT 设备实现分支之间互通的示例（运行 OSPF） 275
6.4.14 配置分支与总部之间建立 IPSec over GRE 隧道示例（基于 ACL 方式） 280
6.4.15 配置分支与总部之间建立 IPSec over DSVPN 隧道示例（基于 ACL 方式） 283
6.4.16 配置分支机构与总部之间采用域名进行 IKE 自动协商，建立 IPSec 隧道的示例 287
6.4.17 配置出差用户利用 L2TP over IPSec 隧道接入总部的示例 290
6.4.18 配置手工和 IKE 协商混合建立 IPSec 隧道示例 292
6.4.19 配置分支采用多链路共享功能与总部建立 IPSec 隧道示例 296
6.4.20 配置 IPSec 反向路由注入功能示例 299
6.4.21 配置对 IPSec 隧道内流量进行 QoS 保证示例 303
6.4.22 配置分支机构通过 4G 接口访问 Internet，总部利用 IPSec 策略模板与分支建立 IPSec 隧道的示例 307
6.4.23 配置分支通过主备链路与总部建立 IPSec 隧道的示例 309
6.4.24 配置分支使用有线线路和总部之间建立 IPSec 隧道的示例 312
6.5 BGP/MPLS IP VPN 314
6.5.1 配置设备之间部署 BGP/MPLS IP VPN 实现互通的示例 314
6.5.2 配置分支机构与总部之间部署 BGP/MPLS IP VPN 实现互通，并通过总部实现分支之间互通的示例 319
6.5.3 配置在层次化网络中设备之间部署 BGP/MPLS IP VPN 实现互通的示例 323
6.5.4 配置采用 OptionA 方式实现跨域的 BGP/MPLS IP VPN 示例 327
6.5.5 配置采用 OptionB 方式实现跨域的 BGP/MPLS IP VPN 示例 331
6.5.6 配置采用 OptionC 方式实现跨域的 BGP/MPLS IP VPN 示例 336
6.5.7 配置设备之间部署 BGP/MPLS IP VPN 实现互通的示例（PE 和 CE 之间使用 ISIS） 340
6.5.8 配置设备之间部署 BGP/MPLS IP VPN 实现互通的示例（PE 和 CE 之间使用 BGP） 344
6.5.9 配置设备之间部署 BGP/MPLS IP VPN 实现互通的示例（PE 和 CE 之间使用 OSPF） 348
6.5.10 配置 OSPF 伪连接，避免在同一个 OSPF 区域内属于同一个 VPN 的用户之间的通信总是通过 OSPF 区域内路由转发示例 351

 版权所有 © 华为技术有限公司

6.5.11 配置设备之间部署 BGP/MPLS IP VPN 实现互通的示例（PE 和 CE 之间使用静态路由） 356
6.5.12 配置设备之间部署 BGP/MPLS IP VPN 实现互通的示例（PE 和 CE 之间使用 RIP） 359
6.5.13 配置路由反射器优化 VPN 骨干层的示例 363
6.6 VLL 367
6.6.1 配置设备之间部署 Martini 方式 VLL 实现互通的示例 368
6.6.2 配置设备之间部署 VLL 采用 GRE 隧道实现互通的示例 370
6.7 PWE3 373
6.7.1 配置空中交通管制场景中使用 E&M 接口传输甚高频业务（骨干网使用双链路保护） 373
7 部署 5G 378
7.1 5G 拨号上网场景 378
7.1.1 配置企业通过 5G 链路接入 Internet 示例 378
7.1.2 配置企业通过 5G IPv6 链路接入 Internet 示例 382
7.1.3 配置企业通过 5G 双 DNN 同时接入 Internet 和 IMS 示例 387
7.2 5G2B 专线场景 391
7.2.1 配置分支使用 5G 链路和总部建立 GRE 隧道互联示例 391
7.2.2 配置分支使用 5G 链路和总部建立 IPSec 加密隧道示例 397
7.2.3 配置分支使用 5G 链路和总部建立 L2TP 隧道互联示例 405
7.2.4 配置分支使用 5G 链路和总部建立 DSVPN over IPSec 互连示例 409
7.2.5 配置分支使用 5G 链路和总部建立 VPDN 互联示例 419
7.2.6 配置分支使用 5G 链路和总部建立 Ethernet over GRE 隧道互联示例 425
7.2.7 配置双网关多发选收示例（5G CPE 场景） 433
7.2.8 配置 5G 场景二层多发选收示例 446
7.2.9 配置 5G 场景二层重定向多发选收示例 455
7.2.10 配置二层多发选收示例（5G CPE 场景） 463
7.2.11 配置二层重定向多发选收示例（5G CPE 场景） 477
7.3 5G 冗余保护场景 493
7.3.1 配置企业使用 5G 主备双 SIM 卡上网示例 493
7.3.2 配置企业使用有线和 5G 主备双链路上网示例 498
7.3.3 配置分支使用 5G 双链路和总部建立 GRE 主备隧道互联示例 502
7.3.4 配置分支使用 5G 双链路和总部建立 Ethernet over GRE 主备隧道互联示例 510
8 获取 IP 地址 521
8.1 配置设备作为 DHCP Server，为用户分配 IP 地址的示例 521
8.2 配置设备作为 DHCP Client，动态获取 IP 地址的示例 523
8.3 配置用户通过 DHCP Relay 功能从 DHCP Server 获取 IP 地址的示例 524
8.4 配置用户自动获取 IPv6 地址的示例 525
8.5 配置用户通过 IPv6 方式上网 527
9 部署路由 529
9.1 静态路由协议 529
9.1.1 配置 IPv4 静态路由基本功能示例 529
9.1.2 配置 NQA for IPv4 静态路由示例 531
9.1.3 配置 IPv6 静态路由基本功能示例 534

 版权所有 © 华为技术有限公司

9.1.4 配置 IPv4 静态路由与 BFD 联动配置 536
9.1.5 配置路由器通过 IPv4 静态路由与三层交换机对接示例 538
9.1.6 配置 IPv4 静态路由双出口固定地址的案例 540
9.2 RIP 路由协议 541
9.2.1 配置 RIP 路由协议基本功能示例 542
9.2.2 配置 RIP 路由协议与 BFD 联动示例 543
9.3 RIPng 路由协议 545
9.3.1 配置 RIPng 路由协议基本功能示例 546
9.4 OSPF 路由协议 547
9.4.1 配置 OSPF 路由协议基本功能示例 547
9.4.2 配置 OSPF 虚连接且验证的示例 549
9.4.3 配置 OSPF 的 STUB 区域示例 551
9.4.4 配置 OSPF 的 NSSA 区域示例 553
9.4.5 配置 OSPF 区域路由聚合功能示例 555
9.4.6 配置 OSPF 引入路由聚合功能示例 556
9.4.7 配置 OSPF 路由信息过滤功能示例 558
9.4.8 配置 OSPF 路由协议与 BFD 联动示例 562
9.5 OSPFv3 路由协议 565
9.5.1 配置 OSPFv3 路由协议基本功能示例 565
9.5.2 配置 OSPFv3 双进程路由互通功能示例 567
9.5.3 配置 OSPFv3 路由信息过滤功能示例 569
9.6 IS-IS（IPv4）路由协议 573
9.6.1 配置 IS-IS 的路由渗透功能示例 573
9.6.2 配置 IS-IS 的路由聚合功能示例 576
9.6.3 配置 IS-IS 路由协议与 BFD 联动示例 578
9.7 IS-IS（IPv6）路由协议 580
9.7.1 配置 IS-IS IPv6 的基本功能示例 580
9.8 BGP 路由协议 583
9.8.1 配置 BGP 路由协议基本功能示例 583
9.8.2 配置 BGP 路由反射器功能示例 585
9.8.3 配置 BGP 路由策略应用本地优先级和团体属性功能示例 587
9.8.4 配置 BGP 路由策略应用 AS_Path 属性功能示例 588
9.8.5 配置 BGP4+路由反射器功能示例 591
9.8.6 配置 BGP4+负载分担功能示例 593
9.8.7 配置 BGP4+路由协议联盟功能示例 595
9.8.8 配置 BGP 路由协议与 BFD 联动示例 598
9.9 策略路由 602
9.9.1 配置接口策略路由的基本功能示例 602
9.9.2 配置策略路由示例 603
9.10 路由策略 605
9.10.1 配置路由策略基本功能示例 605
10 部署 IP 组播 610

 版权所有 © 华为技术有限公司

10.1 配置通过 IGMP 实现用户主机接收组播视频信息的示例 610
10.2 配置通过 PIM-SM 实现组播数据在网络中传输的示例 611
10.3 配置组播数据通过 GRE 隧道实现跨单播网段交换的示例 613
10.4 配置基于 VLAN 的 IGMP Snooping 策略以实现用户接收特定的组播组数据示例 616
10.5 配置使用静态端口实现二层组播示例 617
11 部署 MPLS 620
11.1 配置骨干网设备 MPLS 本地会话功能实现数据在 MPLS 网络中转发示例 620
11.2 配置骨干网设备 MPLS 远端会话功能实现 VPN 数据在 MPLS 网络中承载示例 622
11.3 配置静态 LSP 实现分支和总部的互通示例 624
11.4 配置 LDP LSP 实现分支和总部的互通示例 627
11.5 配置 MPLS TE 实现分支和总部的互通示例 631
12 部署 WLAN AP 637
12.1 配置无线用户接入 WLAN 示例 637
12.2 配置安全策略为 WEP 认证（open-system+WEP 加密）的业务示例 639
12.3 配置安全策略为 WPA 认证（PSK 认证+TKIP 加密）的业务示例 640
12.4 配置安全策略为 WPA2 认证（PSK 认证+CCMP 加密）的业务示例 641
12.5 配置安全策略为 WAPI 认证的业务示例 643
12.6 配置 WLAN QoS 策略的业务示例 644
13 部署 WLAN AC 647
13.1 配置小型网络 WLAN 基本业务示例（AC 通过二层口管理 AP） 647
13.2 配置中型网络 WLAN 基本业务示例（AC 通过二层口管理 AP） 650
13.3 配置大型网络 WLAN 基本业务示例（AC 通过二层口管理 AP） 652
13.4 配置小型网络 WLAN 基本业务示例（AC 通过三层口管理 AP） 655
13.5 配置中型网络 WLAN 基本业务示例（AC 通过三层口管理 AP） 661
13.6 配置家庭消费用户无线上网示例（AC 通过三层口管理 AP） 667
13.7 配置安全策略为 Portal 认证的业务示例 675
13.8 配置安全策略为 802.1X 认证的业务示例 682
13.9 配置安全策略为 MAC 认证的业务示例 690
14 部署语音 699
14.1 配置 AR 作为分支网关接入 UC 示例 699
14.2 配置不同企业间共享 PBX 示例 707
14.3 配置现网 PBX 扩容示例 713
14.4 配置分布式组网示例 723
14.5 配置中小企业语音业务示例 731
15 部署可靠性 737
15.1 配置接口备份的示例（3G+3G） 737
15.2 配置接口备份的示例（ADSL+3G） 738
15.3 配置接口备份的示例（以太网+以太网） 740
15.4 配置通过动态路由备份，实现 ISDN 网络对 IP 网络备份的示例 741
15.5 配置 BFD 单跳检测链路的示例 743

 版权所有 © 华为技术有限公司

15.6 配置 BFD 多跳检测链路的示例 745
15.7 配置通过部署 VRRP，实现设备网关冗余备份的示例 746
15.8 配置通过部署 VRRP，实现主备设备共同分担用户业务的示例 748
16 用户接入与认证 752
16.1 配置 802.1x 本地认证，以识别用户身份的示例 752
16.2 配置 802.1x 远端认证，由 Radius 服务器识别用户身份的示例 753
16.3 配置 802.1x 远端认证，由 Radius 主备服务器识别用户身份的示例 755
16.4 配置采用 HWTACACS 协议对 Telnet 用户进行命令行授权示例 756
16.5 配置用户通过 STelnet 登录设备的身份认证示例（RADIUS 认证） 759
16.6 配置用户通过 Telnet 登录设备的身份认证示例（HWTACACS 认证） 762
17 部署设备或网络安全 764
17.1 配置本机防攻击的综合示例 764
17.2 配置通过部署 ASPF，使内网仅提供 FTP 服务的示例 766
17.3 配置通过基于 ACL 规则的包过滤，使内网用户无法访问所有外网的示例 767
17.4 如何限制外网用户访问 WEB 网管 768
17.5 配置通过部署 DHCP Snooping，使用户与合法的 DHCP 服务器进行通信的示例 769
18 部署 QoS 771
18.1 配置流量整形综合示例 771
18.2 配置流量整形，对内网 IP 限速的示例 773
18.3 配置流量监管，对网段总流量限速的示例 775
18.4 配置流量监管，对网段的每个 IP 单独限速的示例 777
18.5 配置拥塞管理和拥塞避免的示例 778
18.6 配置禁止 BT 下载的示例 783
18.7 配置基于源 MAC 地址控制访问的示例 784
18.8 配置双出口实现内部互访和重定向的示例 786
18.9 配置队列模板实现拥塞管理和拥塞避免的示例 789
18.10 配置 CBQ 综合示例 791
18.11 带宽管理 796
18.11.1 配置禁止 P2P 软件下载的示例 796
18.11.2 配置流量整形，对内网 IP 限速的示例 798
19 网络管理与监控 800
19.1 配置通过部署 SNMP，使设备与网管进行通信的示例 800
19.2 配置通过部署 Netstream，对用户流量进行统计方便计费的示例 801
19.3 配置 UDP Jitter 测试示例 802
19.4 配置 TCP 测试示例 803
19.5 配置通过 RMON 功能实现对设备的远程监控和管理 805
19.6 配置通过带验证的单播 NTP 服务器/客户端模式实现时钟同步示例 806
19.7 配置通过带验证的 NTP 广播模式实现时钟同步示例 809
19.8 配置通过 NTP 组播模式实现时钟同步示例 811
19.9 配置本地端口镜像，对用户的行为进行监控的示例 813
20 综合案例 815

 版权所有 © 华为技术有限公司

20.1 配置 DHCP 和 NAT，实现用户动态获取 IP 地址并访问 Internet 公网的示例 815
20.2 IPSec 与 NQA 联动实现主备对等体和主备链路快速切换 817
20.3 配置 SPR 实现语音业务智能选路示例 824

 版权所有 © 华为技术有限公司

1 前言

本手册不区分产品版本。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，本手册仅作为使用参考。

读者对象

本文档介绍了AR路由器各特性在典型应用场景中的配置举例。

本文档主要适用于以下工程师：

- 数据配置工程师
- 调测工程师
- 网络监控工程师
- 系统维护工程师

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号	说明
	表示如不避免则将会导致死亡或严重伤害的具有高等级风险的危害。
	表示如不避免则可能导致死亡或严重伤害的具有中等级风险的危害。
	表示如不避免则可能导致轻微或中度伤害的具有低等级风险的危害。
	用于传递设备或环境安全警示信息。如不避免则可能会导致设备损坏、数据丢失、设备性能降低或其它不可预知的结果。 “须知”不涉及人身伤害。

 版权所有 © 华为技术有限公司

符号	说明
说明	对正文中重点信息的补充说明。 “说明”不是安全警示信息，不涉及人身、设备及环境伤害信息。

命令行格式约定

在本文中可能出现下列命令行格式，它们所代表的含义如下。

格式	意义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从两个或多个选项中选取一个。
[x | y | ...]	表示从两个或多个选项中选取一个或者不选。
{ x | y | ... }*	表示从两个或多个选项中选取多个，最少选取一个，最多选取所有选项。
[x | y | ...]*	表示从两个或多个选项中选取多个或者不选。
&<1-n>	表示符号&的参数可以重复1～n次。
#	由“#”开始的行表示为注释行。

接口编号约定

本手册中出现的接口编号仅作示例，并不代表设备上实际具有此编号的接口，实际使用中请以设备上存在的接口编号为准。

安全约定

- 密码配置约定
  - 配置密码时请尽量选择密文模式(cipher)。为充分保证设备安全，请用户不要关闭密码复杂度检查功能，并定期修改密码。
  - 配置明文模式的密码时，请不要以“%@%@.....%@%@”或“@%@%.....@%@%”或“%#%#.....%#%#”或“%^%#.....%^%#”作为起始和结束符。因为用这些字符为起始和结束符的是合法密文（本设备可以解密的密文），配置文件会显示与用户配置相同的明文密码。
  - 配置密文密码时，不同特性的密文密码不能互相使用。例如AAA特性生成的密文密码不能用于配置其他特性的密文密码。
- 加密算法约定

 版权所有 © 华为技术有限公司

目前设备采用的加密算法包括3DES、AES、RSA、SHA1、SHA2和MD5。3DES、RSA和AES加密算法是可逆的，SHA1、SHA2和MD5加密算法是不可逆的。DES/3DES/RSA(1024位以下)/MD5(数字签名场景和口令加密)/SHA1(数字签名场景)加密算法安全性低，存在安全风险。在协议支持的加密算法选择范围内，建议使用更安全的加密算法，比如AES/RSA(2048位以上)/SHA2/HMAC-SHA2。具体采用哪种加密算法请根据场景而定：对于管理员类型的密码，必须采用不可逆加密算法，推荐使用安全性更高的SHA2。

- 个人数据约定

  您购买的产品、服务或特性在业务运营或故障定位的过程中将可能获取或使用用户的某些个人数据（如终端用户的MAC地址或IP地址），因此您有义务根据所适用国家的法律制定必要的用户隐私政策并采取足够的措施以确保用户的个人数据受到充分的保护。

- 本文档中出现的“镜像端口、端口镜像、流镜像、镜像”等相关词汇仅限于为了描述该产品进行检测通信传输中的故障和错误的目的而使用，不涉及采集、处理任何个人数据或任何用户通信内容。

特别声明

- 本手册仅作为使用指导，其内容（如Web界面、CLI命令格式、命令输出）依据实验室设备信息编写。手册提供的内容具有一般性的指导意义，并不确保涵盖所有型号产品的所有使用场景。因版本升级、设备型号不同、配置文件不同等原因，可能造成手册中提供的内容与用户使用的设备界面不一致。请以用户设备界面的信息为准，本手册不再针对前述情况造成的差异一一说明。
- 本手册中提供的最大值是设备在实验室特定场景（例如，被测试设备上只有某种类型的单板，或者只配置了某一种协议）达到的最大值。在现实网络中，由于设备硬件配置不同、承载的业务不同等原因会使设备测试出的最大值与手册中提供的数据不一致。
- 出于特性介绍及配置示例的需要，本文档可能会使用公网IP地址，如无特殊说明出现的公网IP地址均为示意，不指代任何实际意义。
- 本手册中“NetEngine AR路由器”包括AR300&AR600&AR700&AR6100&AR6200&AR6300系列。

 版权所有 © 华为技术有限公司

2 入门和基础操作

2.1 开局部署
2.2 登录设备（命令行方式）
2.3 升级设备（命令行方式）
2.4 操作BootLoader菜单
2.5 设备管理

2.1 开局部署

2.1.1 配置通过 U 盘完成软件升级、业务部署的示例

规格

适用于所有版本、所有形态的AR路由器。

说明

RU-5G-101不支持此功能。

组网需求

企业项目需要对大量的设备进行批量开局，此时采用U盘开局配置，可以实现软件人员不到现场即可批量进行设备的开局及软件升级。设备安装完毕后，将U盘插入USB接口并上电启动，通过U盘开局功能，设备自动完成软件升级。当前要求对两台设备进行U盘开局，需求如下:

- 两台设备的开局时间均为2011年06月28日08时09分10秒
- 网管不在线
- 第一台设备的ESN为0000080123456789，MAC地址为00e0-fc03-1234
- 第二台设备的ESN为6666680123456789，MAC地址为00e0-fc03-5678

 版权所有 © 华为技术有限公司

- 系统软件位于U盘根目录下，名称为software.cc，版本号为v1，第一台设备不需要加载配置文件，第二台设备需要加载配置文件，需要加载的配置文件名称为config.zip

操作步骤

步骤1 编辑U盘开局索引文件USB_AR.ini。

用户可以在PC上编辑U盘开局索引文件，具体步骤如下：

1. 新建一个空的文本文档
2. 编辑索引文件内容，索引文件的格式如下：

说明

加粗字体根据设备实际情况填写。

```
BEGIN AR
[USB CONFIG]
SN=20110628.080910
EMS_ONLINE_STATE=NO
[UPGRADE INFO]
OPTION=AUTO
DEVICENUM=2
[DEVICE1 DESCRIPTION]
OPTION=OK
ESN=0000080123456789
MAC=00e0-fc03-1234
VERSION=v1
DIRECTORY=DEFAULT
FILENUM=1
TYPE1=SYSTEM-SOFTWARE
FILENAME1=software.cc
[DEVICE2 DESCRIPTION]
OPTION=OK
ESN=6666680123456789
MAC=00e0-fc03-5678
VERSION=v1
DIRECTORY=DEFAULT
FILENUM=2
TYPE1=SYSTEM-SOFTWARE
FILENAME1=software.cc
TYPE2=SYSTEM-CONFIG
FILENAME2=config.zip
END AR
```

表 2-1 索引文件字段含义

字段	描述
BEGIN AR	起始标志。
USB CONFIG	U盘配置信息。
SN	每次数据变更的时间（年月日.时分秒）。 例如，2011年06月28日08时09分10秒，则设置为SN=20110628.080910。
EMS_ONLINE_STATE	网管是否在线： – YES表示网管在线 – NO表示网管不在线

 版权所有 © 华为技术有限公司

字段	描述
UPGRADE INFO	升级信息。
OPTION	用于标识升级模式，为固定值，即OPTION=AUTO。
DEVICENUM	设备描述信息的个数： – 如果仅需要给一台设备升级软件版本，设置DEVICENUM=1，ESN的取值为设备序列号，MAC的取值为设备的MAC地址。 – 如果需要给多台同系列的设备升级至同一版本，设置DEVICENUM=1，ESN=DEFAULT，MAC=DEFAULT。 – 如果需要给多台设备升级至不同版本，DEVICENUM的取值为需要升级设备的数目，ESN和MAC的取值根据设备的实际情况填写。
DEVICE*n* DESCRIPTION	设备*n*的描述信息头，*n*的取值从1开始。
OPTION	用于标识设备是否需要升级： – OK表示需要升级 **说明** 如果此字段不是“OK”，表示不需要升级。
ESN	设备序列号。如果ESN=DEFAULT，则表示U盘索引文件匹配所有设备。
MAC	设备MAC地址。如果MAC=DEFAULT，则表示U盘索引文件匹配所有设备。
VERSION	升级版本号。
DIRECTORY	用于标识升级的文件路径： – 若DIRECTORY=DEFAULT，则文件位于U盘根目录下 – 若DIRECTORY=/abc，则文件位于U盘的abc文件夹下
FILENUM	需要加载的文件个数。 例如设备仅需要加载系统软件，那么FILENUM的取值为1；如果设备需要加载系统软件和补丁文件，那么FILENUM的取值为2。

版权所有 © 华为技术有限公司

字段	描述
TYPE*n*	用于标识升级的文件类型: – SYSTEM-SOFTWARE为系统软件 – SYSTEM-CONFIG为配置文件 **说明** ■ 如果设备支持语音功能且工作在PBX模式时，配置文件表示为SYSTEM-CONFIG_PBX。 ■ 如果设备支持语音功能且工作在SIPAG模式时，配置文件表示为SYSTEM-CONFIG_SIPAG。 – SYSTEM-PAT为补丁文件 – SYSTEM-LICENSE为License文件 – SYSTEM-VOICE为语音文件 – USER-DEFINE为用户自定义文件 新增**SYSTEM-EXECUTE**可执行文件类型，只支持shell类型可执行文件。 *n*的取值从1开始。
FILENAME*n*	用于标识升级的文件名。例如TYPE1=SYSTEM-SOFTWARE，系统软件的名称为software.cc，则FILENAME1=software.cc。 *n*的取值从1开始。
END AR	文件结束标志。

3. 将此文本文档的文件名另存为“USB_AR.ini”

步骤2 将U盘索引文件USB_AR.ini、系统软件（software.cc）和配置文件（config.zip）拷贝到U盘根目录下。（略）

步骤3 U盘插入设备中，设备上电启动。

步骤4 系统检测到U盘在位，检测U盘中是否存在U盘开局索引文件USB_AR.ini并检测其合法性。

- 如果文件不存在，开局指示灯熄灭；如果文件存在但不合法，开局失败，红灯常亮。
- 如果文件存在且合法，则进入U盘开局流程，绿灯闪烁。

说明

进入开局流程后，系统首先按照USB_AR.ini文件中的描述信息从U盘中获取开局文件复制到设备缺省的存储介质中。然后，主机程序将系统软件、配置文件设置为系统下次启动文件。

步骤5 验证配置结果。

设备重启后，系统检测开局状态。开局指示灯常绿，表示U盘开局成功。

----结束

 版权所有 © 华为技术有限公司

配置注意事项

- U盘开局文件包括：U盘开局索引文件，系统软件、配置文件、补丁文件、语音文件、License文件、可执行文件和用户自定义文件。其中，U盘开局索引文件是必选的，其他几个开局文件至少选择一个。
- U盘规格：文件系统格式是FAT32，硬件接口是标准的USB3.0。
- 使用U盘进行写操作时，请务必保证关闭U盘写保护功能。
- U盘开局前，保证开局设备可以正常启动，并且保证设备Flash中有足够的内存空间保存开局文件。
- U盘开局支持经华为认证的指定型号的U盘，以保证U盘和设备的良好兼容性。
- U盘开局不支持同时插入2个U盘进行开局。
- SN不是指设备的SN号，而是U盘开局的一个标识。设备有一个默认的U盘开局标识，当U盘上存在.ini文件时，就会对比设备原有的U盘开局SN号和.ini文件中SN号是否一致。如果不一致，则触发U盘开局，使用U盘指定的开局文件启动。开局成功后，设备的开局SN号会更新为.ini文件中设置的SN号。

2.2 登录设备（命令行方式）

2.2.1 配置用户通过 Console 口首次登录设备的示例

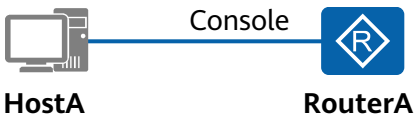
规格

适用于所有版本、所有形态的AR路由器。

组网需求

当路由器第一次上电，需要对此路由器进行配置和管理时，可以通过Console口登录。如图2-1，RouterA的Console口与用户侧主机HostA相连，要求用户通过Console口登录RouterA。

图 2-1 配置 Console 口首次登录设备组网图



操作步骤

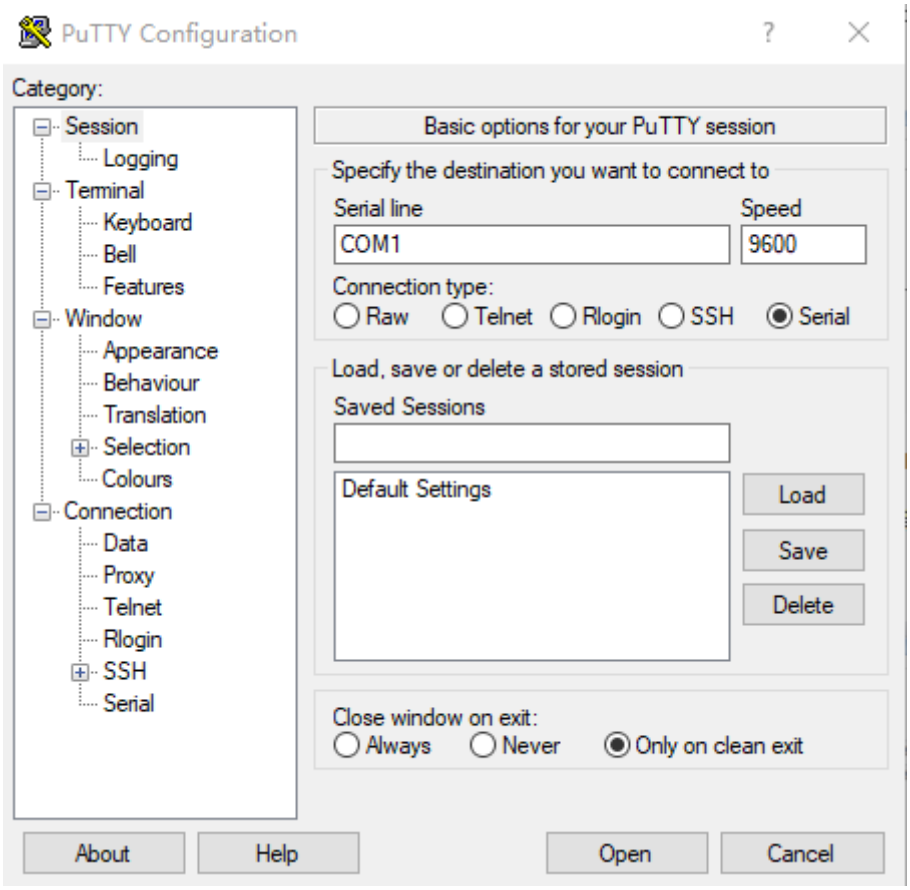
步骤1 使用Console通信电缆将RouterA的Console口与HostA的COM口进行物理连接。

步骤2 在PC上打开终端仿真软件，新建连接，设置连接的接口以及通信参数。（此处使用第三方软件PuTTY为例进行介绍）

1. 如图2-2所示，单击“Session”，新建连接。

 版权所有 © 华为技术有限公司

图 2-2 新建连接



2. 如图2-3所示，设置连接的接口以及通信参数。

   一般情况下，连接的接口是COM1。如果选择COM1无法登录设备，可依次尝试其它COM接口。

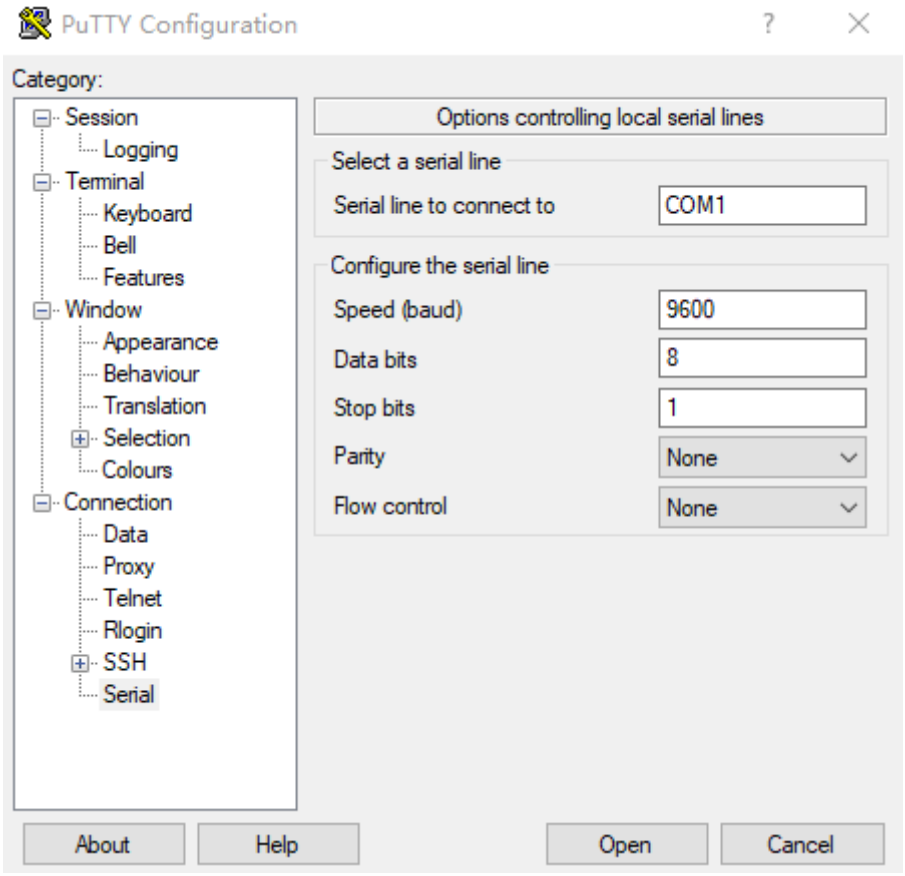
   设置终端软件的通信参数需与设备的缺省值保持一致，分别为：传输速率为9600bit/s、8位数据位、1位停止位、无校验和无流控。

   说明

   缺省情况下，设备没有流控方式。RTS/CTS缺省情况下处于使能状态，因此需要将该选项勾选掉，否则终端界面中无法输入命令行。

版权所有 © 华为技术有限公司

图 2-3 设置连接的接口以及通信参数



步骤3 按Enter键，直到出现用户视图的命令行提示符，如<Huawei>，至此用户进入了用户视图配置环境。

V300R021C00之前版本。

```
Login authentication      // 提示用户输入用户名和验证密码，您可以在《AR路由器 缺省帐号与密码》（企业网、运营商）文档中获取各种缺省帐号与密码信息。获取该文档需要权限，如需升级权限，请查看网站帮助。

Username:admin
Password:
<Huawei>
Info: The entered password is the same as the default. You are advised to change
 it to ensure security.
```

V300R021C00及之后版本。

```
Login authentication      // 提示用户设置密码。

Warning: An initial username and password are required for the first login via the console.
Set a username and password and keep them safe.Otherwise you will not be able to login via the
console.
New Username:
Password:
Confirm password:
The account create success.
  Info:Configuration console exit, please retry to log on
```

此时用户可以键入命令，对路由器进行配置，需要帮助可以随时键入“?”。

版权所有 © 华为技术有限公司

说明

用户通过Console口登录新出厂（或没有启动配置文件）的路由器时，系统会提示：“Auto-Config is working. Before configuring the device, stop Auto-Config. If you perform configurations when Auto-Config is running, the DHCP, routing, DNS, and VTY configurations will be lost. Do you want to stop Auto-Config? [y/n]:”，

- 如果需要进行Auto-Config，选择n，并回车；
- 如果不需要进行Auto-Config，选择y，并回车；
- 如果不需要进行Auto-Config，但选择的是n，会导致后续配置的dhcp、路由、dns和vty用户配置丢失。

----结束

配置注意事项

- 终端通信参数（包括每秒位数、数据位、奇偶校验、停止位和流量控制）需要与RouterA的缺省值保持一致，否则将无法登录RouterA。

2.2.2 配置用户以 Console 口登录设备时要通过密码验证的示例

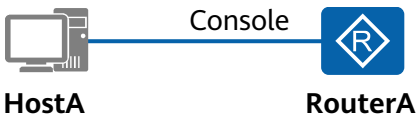
规格

适用于所有版本、所有形态的AR路由器。

组网需求

RouterA的Console口与用户侧主机HostA相连。要求用户从Console口登录时输入正确的密码才能登录成功。

图 2-4 配置 Console 口登录认证功能组网图



操作步骤

步骤1 RouterA的配置

```
#
user-interface con 0
 authentication-mode password  //配置Console口登录的用户验证方式为密码验证
 set authentication password cipher   //配置Console口登录密码为YsHsjx_202206
#
```

步骤2 验证配置结果

配置完成后，使用**quit**命令断开HostA与RouterA的连接。当HostA再次通过Console口登录RouterA时，输入密码YsHsjx_202206后，进入用户视图则表示配置成功。

----结束

 版权所有 © 华为技术有限公司

2.2.3 通过 Console 口对设备进行基本配置示例

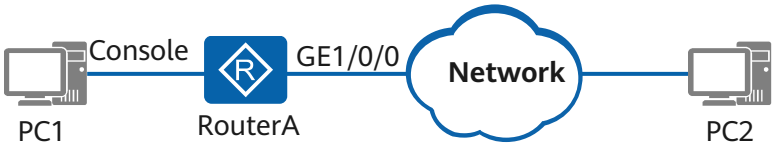
规格

适用于所有版本、所有形态的AR路由器。

组网需求

通过Console口首次登录设备后，对设备进行基本配置，配置设备的时区、设备名称和管理IP地址，并配置0～4号Telnet用户的级别为15级，认证方式为AAA认证以实现远程登录。

图 2-5 通过 Console 口进行基本配置组网图



操作步骤

步骤1 PC1通过设备Console口登录设备，具体操作请参见**配置用户通过Console口首次登录设备的示例**

步骤2 对RouterA进行基本配置

```
#
 sysname Server  //配置设备名称
#
 clock timezone BJ add 08:00:00  //配置系统的时区
#
aaa
 local-user admin1234 password irreversible-cipher  //创建本地用户，用户名为admin1234，密文密码为YsHsjx_202206
 local-user admin1234 privilege level 15  //配置本地用户admin1234的优先级为15，数值越高，权限越大
 local-user admin1234 service-type telnet  //配置本地用户admin1234的接入方式为Telnet
#
interface GigabitEthernet1/0/0
 ip address 10.137.217.159 255.255.255.0  //配置连接PC2的接口的IP地址
#
 telnet server permit interface GigabitEthernet1/0/0  //配置Telnet服务器允许客户端连接的接口，否则无法使能Telnet服务。
 telnet server enable  //使能Telnet服务器功能
 telnet server port 10181  //配置Telnet服务器端口号
#
user-interface vty 0 4  //进入VTY0～VTY4用户界面视图
 authentication-mode aaa  //配置VTY类型用户界面的验证方式为AAA
#
return
```

步骤3 验证配置结果

在PC2上通过Telnet访问RouterA，可以选择使用Windows命令行提示符或第三方软件。此处以Windows命令行提示符为例。

```
C:\Documents and Settings\Administrator> telnet 10.137.217.159 10181

Login authentication
```


版权所有 © 华为技术有限公司

```
Username:admin1234
Password:
<Server>
```

----结束

配置注意事项

- PC2登录设备使用的用户名和密码要和设备的配置保持一致。
- 在PC2上执行Telnet操作时，需要输入正确的IP地址及端口号。

2.2.4 配置用户通过 Telnet 登录设备

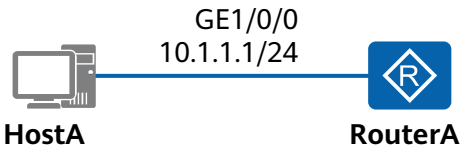
规格

适用于所有版本、所有形态的AR路由器。

组网需求

RouterA的GE1/0/0与用户侧主机HostA相连。要求用户通过Telnet登录设备时输入正确的用户名和密码才能登录成功。

图 2-6 配置用户通过 Telnet 登录设备组网图



说明

使用Telnet协议存在安全风险，建议使用STelnet V2登录设备。

操作步骤

步骤1 RouterA的配置

```
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.1 255.255.255.0  //配置连接HostA接口的源IP地址
#
aaa
 local-user huawei password irreversible-cipher   //创建本地用户，用户名为huawei、密文密码为YsHsjx_202206
 local-user huawei service-type telnet  //配置本地用户huawei的接入类型为telnet
 local-user huawei privilege level 3  //配置本地用户huawei的优先级为3
#
 telnet server permit interface all //配置Telnet服务器允许客户端连接的接口，否则无法使能Telnet服务。
 telnet server enable  //使能Telnet服务器功能
#
user-interface vty 0 4  //进入VTY0～VTY4用户界面视图
 authentication-mode aaa  //配置VTY类型用户界面的验证方式为AAA
#
```

步骤2 验证配置结果

 版权所有 © 华为技术有限公司

在HostA上通过Telnet访问RouterA，可以选择使用Windows命令行提示符或第三方软件。此处以Windows命令行提示符为例。

```
C:\Documents and Settings\Administrator> telnet 10.1.1.1

Login authentication


Username:huawei
Password:
<RouterA>
```

----结束

配置注意事项

- HostA登录设备使用的用户名和密码要和RouterA的配置保持一致。

相关信息

视频

远程登录设备--Telnet方式

2.2.5 配置用户通过异步串口重定向登录其他设备的示例

规格

适用于AR700&AR6100&AR6200&AR6300系列款型设备。

组网需求

在电信、金融等领域，某些终端设备只提供了串口访问功能，或者无法通过telnet进行访问。这时，通过路由器提供的串口重定向功能，通过telnet对挂接终端设备进行配置管理。

如图2-7，RouterA使用异步串口线将异步串口与RouterB的串口（Console）互联。支持属于私网vpna的远程PC通过RouterA登录终端设备RouterB进行配置管理，即RouterA充当串口服务器的功能，vpna私网用户的PC与RouterA之间有可达路由。远程PC可以按照IP+特定端口号的方式登录RouterA下挂的终端设备。

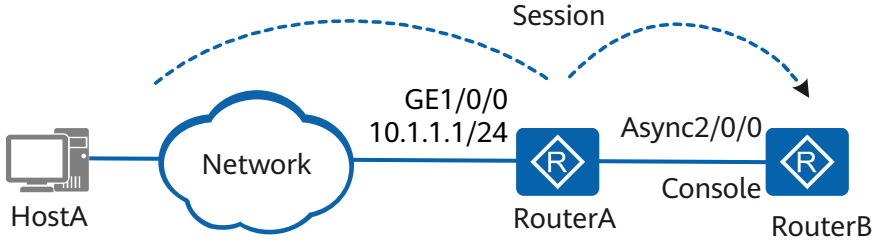
说明

异步串口可以使用Async接口或者工作在异步方式下的Serial接口。本示例中以Async接口为例。

连接Async接口的异步串口线相关内容请参见《NetEngine AR路由器 了解产品 – 硬件描述 – 线缆》中的“8AS电缆”。

连接Serial接口的异步串口线相关内容请参见《NetEngine AR路由器 了解产品 – 硬件描述 – 线缆》中的“SA电缆”。

图 2-7 配置通过重定向登录其他设备组网图



版权所有 © 华为技术有限公司

操作步骤

步骤1 获取异步口的TTY用户界面编号

```
<RouterA> display user-interface
  Idx  Type     Tx/Rx      Modem Privi ActualPrivi Auth  Int
  0    CON 0    9600        -     15    -          N     -
F 9    TTY 9    9600        -     0     -          N     2/0/0
  10   TTY 10   9600        -     0     -          N     2/0/1
  11   TTY 11   9600        -     0     -          N     2/0/2
  12   TTY 12   9600        -     0     -          N     2/0/3
  13   TTY 13   9600        -     0     -          N     2/0/4
  14   TTY 14   9600        -     0     -          N     2/0/5
  15   TTY 15   9600        -     0     -          N     2/0/6
  16   TTY 16   9600        -     0     -          N     2/0/7
+ 129  VTY 0               -     15    4          N     -
  130  VTY 1               -     15    -          N     -
  131  VTY 2               -     15    -          N     -
  132  VTY 3               -     15    -          N     -
  133  VTY 4               -     15    -          N     -
  145  VTY 16              -     0     -          P     -
  146  VTY 17              -     0     -          P     -
  147  VTY 18              -     0     -          P     -
  148  VTY 19              -     0     -          P     -
  149  VTY 20              -     0     -          P     -
```

步骤2 RouterA的配置

```
#
ip vpn-instance vpna
 ipv4-family
  route-distinguisher 1:1
  vpn-target 111:1 export-extcommunity
  vpn-target 111:1 import-extcommunity
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.1 255.255.255.0  //连接HostA的接口的IP地址
 ip binding vpn-instance vpna       //以太网口绑定VPN实例
#
interface Async2/0/0
 async mode flow  //配置异步串口工作在流模式
#
 telnet server permit interface all //配置Telnet服务器允许客户端连接的接口，否则无法使能Telnet服务。
 telnet server enable  //使能Telnet服务器功能
#
user-interface tty 9
 authentication-mode password
 set authentication password cipher
 redirect enable  //使能异步串口重定向功能
 redirect listen-port 2129     //更改异步串口重定向端口号
 redirect binding vpn-instance vpna   //异步串口关联vpn实例

#
```

步骤3 验证配置结果

在HostA上通过Telnet先登录至RouterA，然后按回车键登录RouterB。可以选择使用Windows命令行提示符或第三方软件。此处以Windows命令行提示符为例。

```
C:\Documents and Settings\Administrator> telnet 10.1.1.1 2129
Press CTRL_] to quit telnet mode
  Trying 10.1.1.1...
  Connected to 10.1.1.1...
Login authentication


Password:
```

 版权所有 © 华为技术有限公司

```
<RouterA>
[RouterB]
```

说明

绑定的VPN实例必须与私网用户属于同一VPN。如果不与VPN实例绑定，公网用户和任意私网用户均可以通过重定向功能登录RouterB。

----结束

配置注意事项

- 在HostA上执行telnet操作时，需要输入正确的IP地址和端口号。

2.2.6 配置用户通过 STelnet 登录设备（Password 认证方式）

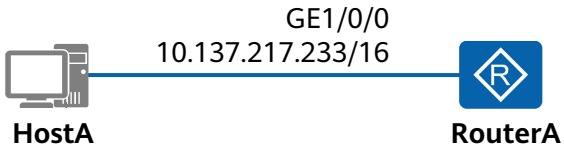
规格

适用于所有版本、所有形态的AR路由器。

组网需求

使能STelnet服务功能的RouterA的GE1/0/0与用户侧主机HostA相连。要求用户通过STelnet登录设备时输入正确的用户名和密码才能登录成功。

图 2-8 配置用户通过 STelnet 登录设备组网图



说明

使用STelnet V1协议存在安全风险，建议使用STelnet V2登录设备。

操作步骤

步骤1 RouterA生成本地密钥对

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] rsa local-key-pair create
```

步骤2 RouterA的配置

```
#
interface GigabitEthernet1/0/0
 ip address 10.137.217.223  255.255.0.0  //连接HostA的接口的IP地址
#
aaa
 local-user client001 password irreversible-cipher %@%@6W-mT:ZGe)0B*rMm,@#$LEyI;m_bQibe=46k.,#x$vk0EyLL%@%@  //创建本地用户，用户名为client001、密码为YsHsjx_202206。对于“password irreversible-cipher”后面的字段，可以是明文也可以是密文
 local-user client001 service-type ssh       //配置本地用户client001的接入类型为ssh
 local-user client001 privilege level 3      //配置本地用户client001的优先级为3
#
ssh server permit interface all             //配置SSH服务器允许客户端连接的接口，否则无法使能STelnet服务。
```

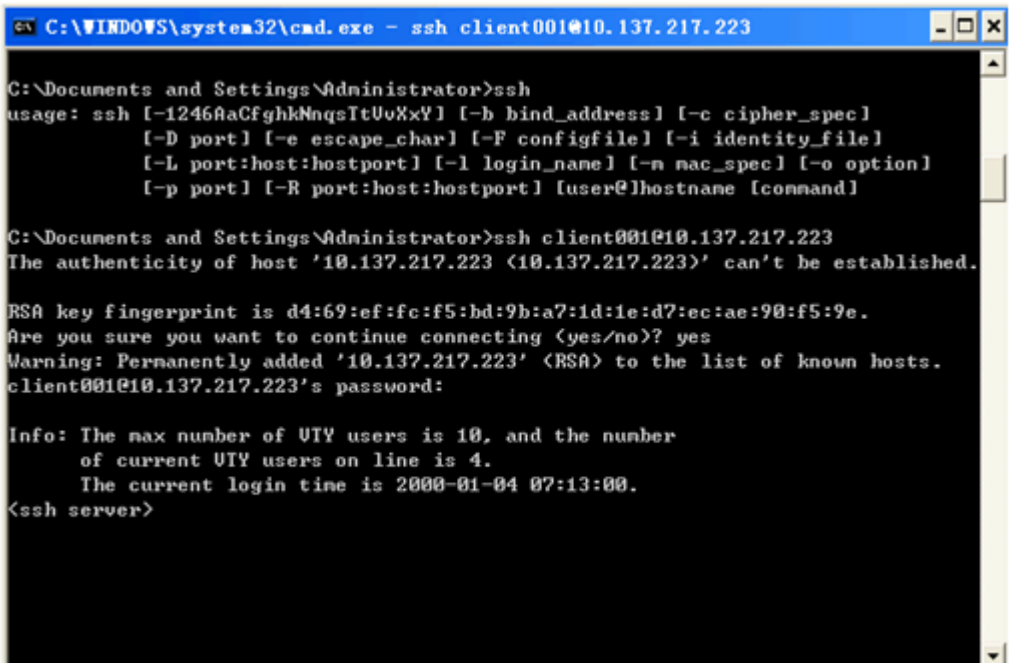
 版权所有 © 华为技术有限公司

```
stelnet server enable                    //使能stelnet服务
#
user-interface vty 0 4
 authentication-mode aaa  //配置VTY类型用户界面的验证方式为AAA
 protocol inbound ssh     //配置VTY类型用户界面只支持SSH协议
#
```

步骤3 验证配置结果

在HostA上通过SSH软件访问RouterA，此处以OpenSSH软件为例。

图 2-9 HostA 通过 SSH 软件访问 RouterA 示意图



----结束

配置注意事项

- HostA登录设备使用的用户名和密码要和RouterA的配置保持一致。
- 若配置VTY类型用户界面只支持SSH协议，设备将自动禁止Telnet功能。

2.2.7 配置用户通过 STelnet 登录设备示例（RSA 认证方式）

规格

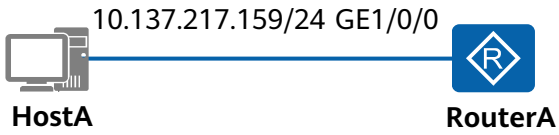
适用于所有版本、所有形态的AR路由器。

组网需求

用户通过STelnet方式进行安全的远程登录。终端主机HostA和SSH服务器RouterA之间路由可达，10.137.217.159是SSH服务器的管理口IP地址。在SSH服务器端配置登录用户client001，HostA使用client001用户通过RSA认证方式登录SSH服务器。

 版权所有 © 华为技术有限公司

图 2-10 配置用户通过 STelnet 登录设备（RSA 方式）组网图



说明

使用STelnet V1协议存在安全风险，建议使用STelnet V2登录设备。

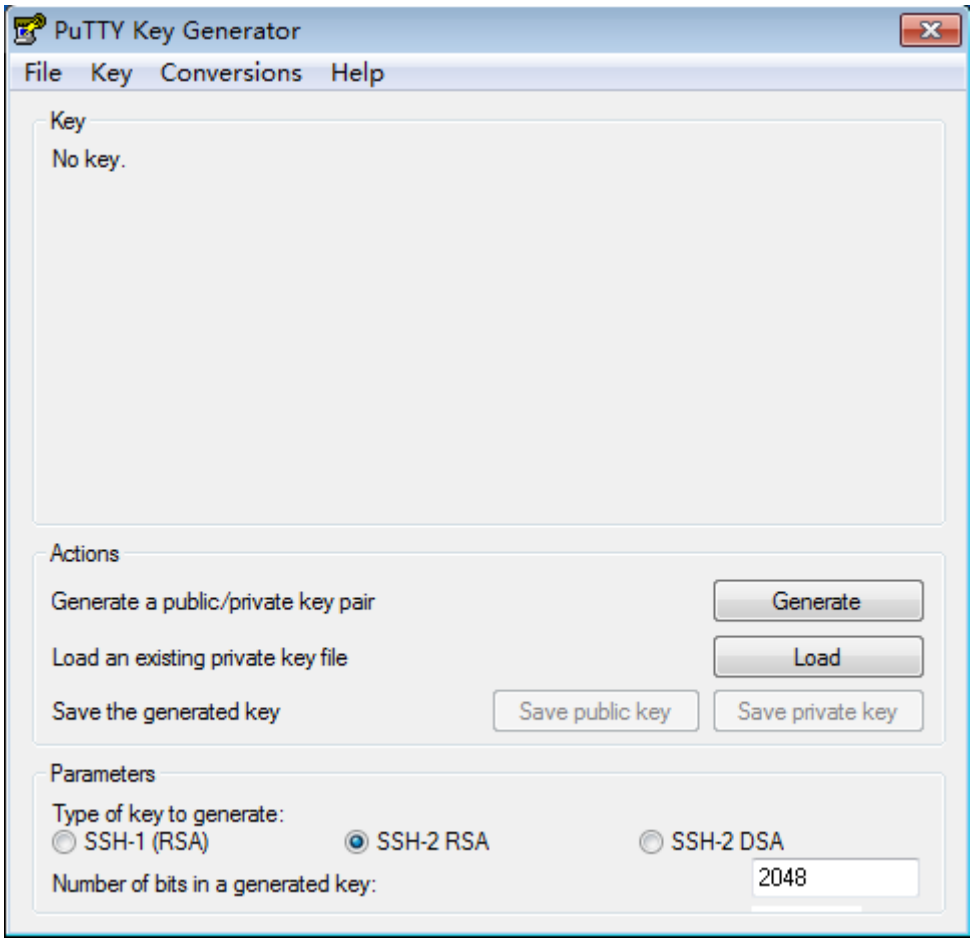
操作步骤

步骤1 在HostA上生成本地密钥对

1. 在HostA上运行puttygen.exe，生成公用密钥、私用密钥两个文件，供后续使用。

   # 如图2-11所示，选择“SSH-2 RSA”，单击“Generate”，进入密钥生成状态。在生成密钥对的过程中需在空白处不停地移动鼠标，否则进程条会停止显示，密钥对将停止产生。

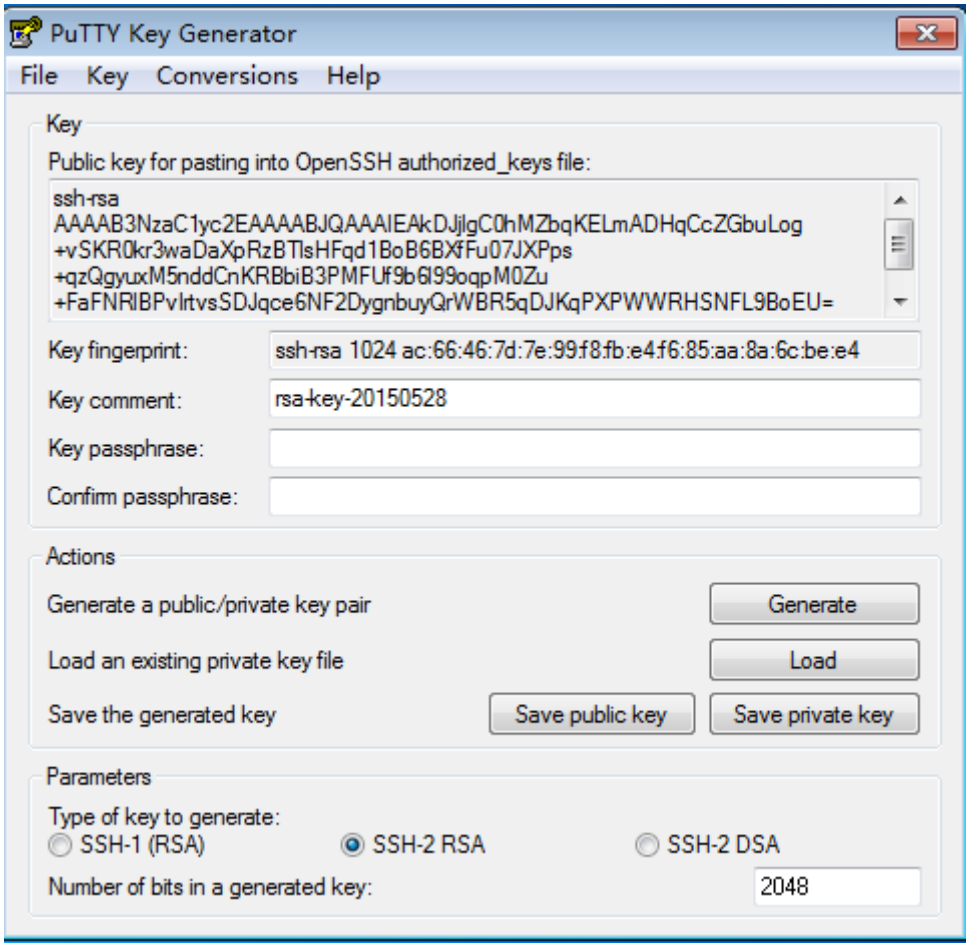
图 2-11 生成客户端密钥对（1）



 版权所有 © 华为技术有限公司

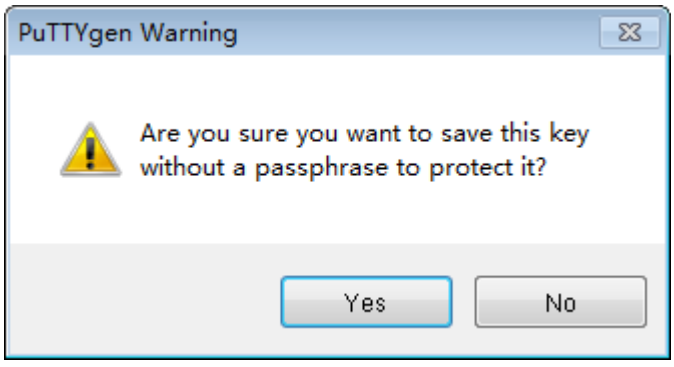
如图2-12所示，待到密钥生成完毕，单击“Save public key”保存文件名为key.pub。

图 2-12 生成客户端密钥对（2）



如图2-12所示，单击“Save private key”，弹出对话框，提醒是否保存没做任何保护措施的私钥，选择“是”，保存文件名为private.ppk。

图 2-13 生成客户端密钥对（3）



版权所有 © 华为技术有限公司

2. 配置RSA公共密钥编码格式为pem格式后，再在服务器上配置puttygen.exe工具生成的公有密钥文件key.pub中的密钥（pem格式）。

步骤2 RouterA的配置

```
#
 sysname SSH Server  //配置设备名称
#
 rsa peer-public-key rsakey001 encoding-type pem  //配置RSA公共密钥编码格式是PEM
  public-key-code begin
  ---- BEGIN SSH2 PUBLIC KEY ----
  AAAAB3NzaC1yc2EAAAABJQAAAQEAm03bm5EFuIgYKWSq6HlltY/hjYhWI/bb5efN
  5u9EGOYNzXLFsECW74X5SSvKHE5YvbDVhD1N/Vinh3ox8U7lY6UNKuOmQZF9OrCO
  dbekrvMOuDVo8zuiZOgrLTVpTFHdgi0BbbSnGvpDzdn6ovm9ZBS+j2omm/D3pWYB
  9YJTARhLILmrrBaiFiYy76F3tCwDhkZwMYOp6ueDKqdJIYYc/jZPnAICr5ByscmB
  0ezlVO3jo5lHn3k5H+rUQmyOEOw8fZDI8zzRN63QOx2NWXZxDZUs9EiReVw7sJIG
  g9zVoCpMsM7PhniFF0DUJoUEF6ryl54noHEmT3lcn4ulWJw1cQ==
  ---- END SSH2 PUBLIC KEY ----
 public-key-code end
peer-public-key end  //生成本地密钥对
#
aaa
 local-user client001 password irreversible-cipher   //创建本地用户，用户名为client001，密文密码为YsHsjx_202206。对于“password irreversible-cipher”后面的字段，可以是明文也可以是密文
 local-user client001 privilege level 15  //配置本地用户client001的优先级为15
 local-user client001 service-type ssh //配置本地用户client001的接入方式为Stelnet
#
interface GigabitEthernet1/0/0
 ip address 10.137.217.159 255.255.255.0  //配置连接HostA的接口的IP地址
#
 ssh user client001 authentication-type rsa  //配置本地用户client001的认证方式为RSA
 ssh user client001 assign rsa-key rsakey001  //指定本地用户client001要连接的SSH服务器端的主机公钥名称
 ssh server permit interface all            //配置SSH服务器允许客户端连接的接口，否则无法使能STelnet服务。
 stelnet server enable  //使能SSH服务器功能
#
user-interface vty 0 4
user privilege level 15  //配置用户的优先级为15
 authentication-mode aaa  //配置VTY类型用户界面的验证方式为AAA
 protocol inbound ssh  //配置VTY类型用户界面只支持SSH协议
#
return
```

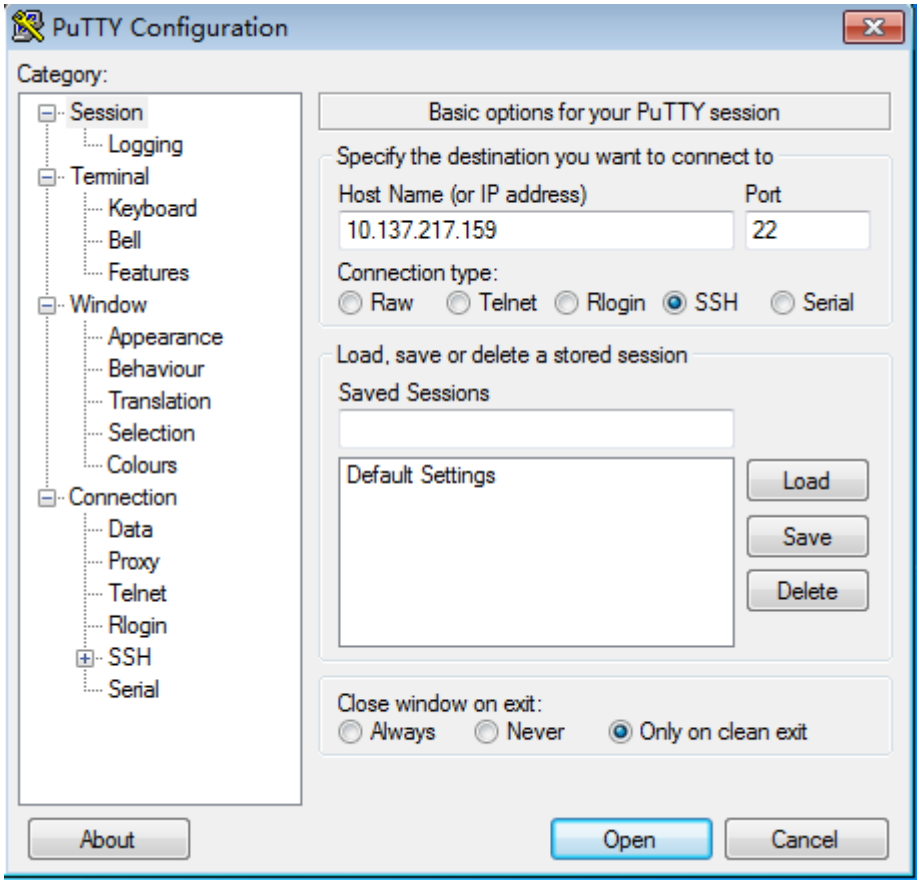
步骤3 验证配置结果

在HostA上通过SSH软件访问RouterA，此处以PuTTY软件为例。

如图2-14所示，通过PuTTY软件登录设备，输入设备的IP地址，选择协议类型为SSH。

 版权所有 © 华为技术有限公司

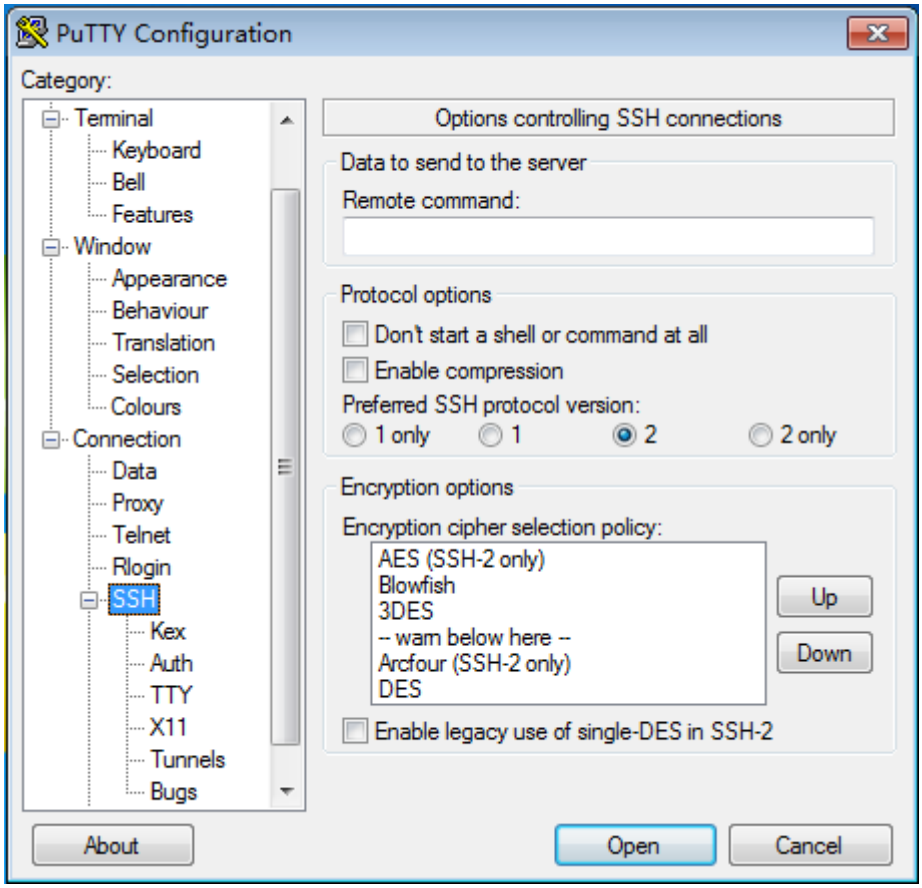
图 2-14 通过 PuTTY 软件用 RSA 认证方式连接 SSH 服务器示意图（1）



单击左侧导航栏“Connection > SSH”，进入图2-15的界面，选择SSH协议版本为“2”。

版权所有 © 华为技术有限公司

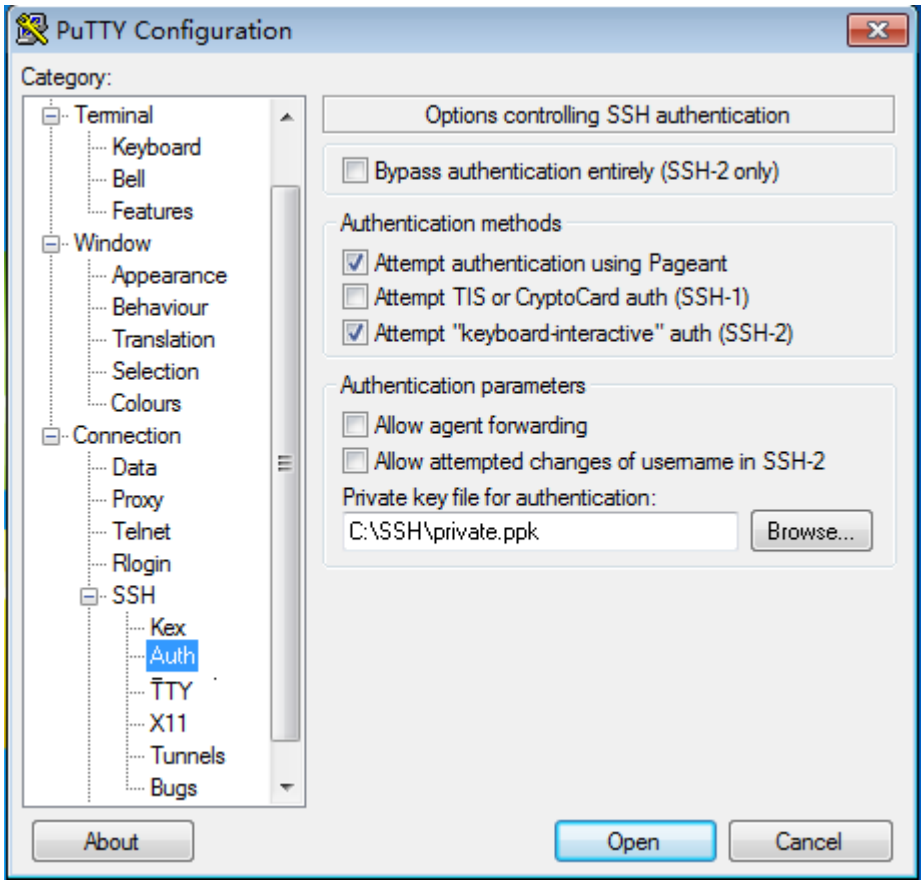
图 2-15 通过 PuTTY 软件用 RSA 认证方式连接 SSH 服务器示意图（2）



单击左侧导航栏“Connection > SSH > Auth”，进入图2-16的界面。选择与配置到服务器端的公钥对应的私钥文件private.ppk。

版权所有 © 华为技术有限公司

图 2-16 通过 PuTTY 软件用 RSA 认证方式连接 SSH 服务器示意图（3）



单击“Open”，进入如下界面，输入用户名，并按Enter键，至此已登录到SSH服务器。以下显示信息仅为示意。

```
login as: client001

Authenticating with public key "rsa-key-20150528"

<SSH Server>
```

----结束

配置注意事项

- 当用户使用RSA认证方式时，需要在SSH服务器上输入SSH客户端生成的密钥中的公钥部分。这样当客户端登录服务器时，自己的私钥如果与输入的公钥匹配成功，则认证通过。
- 若配置VTY类型用户界面只支持SSH协议，设备将自动禁止Telnet功能。

2.2.8 配置设备作为客户端，采用 RADIUS 认证登录其他设备的示例

规格

适用于所有版本、所有形态的AR路由器。

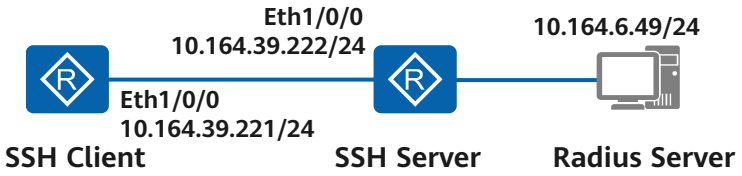
版权所有 © 华为技术有限公司

组网需求

用户使用STelnet方式连接SSH服务器（即AR设备），要求在SSH认证过程中，配置SSH服务器支持SSH客户端通过RADIUS服务器进行远端认证。

RADIUS服务器认证该用户，将认证结果返回给SSH服务器。SSH服务器根据认证结果决定是否允许SSH客户端建立连接。

图 2-17 配置 SSH 支持 RADIUS 认证组网图



操作步骤

步骤1 在SSH服务器端生成本地密钥对

```
<Huawei> system-view
[Huawei] sysname ssh server
[ssh server] rsa local-key-pair create
```

步骤2 SSH Server的不同版本的配置存在差异，请关注对应版本的配置

```
#
 user-interface vty 0 4
 authentication-mode aaa //指定配置VTY0～4用户的验证方式为AAA
 protocol inbound ssh    //配置VTY支持SSH协议
#
aaa
 local-user ssh1@ssh.com password cipher %@%@0qu\:lj<uNH#kN5W/e*A_:G#%@%@  //创建本地用户，用户名为ssh1@ssh.com，密文密码为YsHsjx_202207
 local-user ssh1@ssh.com privilege level 15                    //配置本地用户ssh1@ssh.com级别为15
 authentication-scheme newscheme                               //配置SSH服务器端认证方案newscheme
  authentication-mode radius                                   //指定newscheme的认证方法为RADIUS
 domain ssh.com                                                //配置SSH服务端的RADIUS域名为ssh.com
  authentication-scheme newscheme                              //在域下应用认证方案为newscheme
  radius-server ssh                                            //指定域下RADIUS模板为ssh
#
radius-server template ssh                                     //指定服务器端的RADIUS模板为ssh
 radius-server shared-key cipher N`C55QK<`=/Q=^Q`MAF4<1!! //配置RADIUS服务器密钥为密文密码YsHsjx_202206
 radius-server authentication 10.164.6.49 1812                 //配置RADIUS认证服务器的IP地址和端口号
#
  ssh server permit interface all          //配置SSH服务器允许客户端连接的接口，否则无法使能STelnet服务。
  stelnet server enable //在SSH服务器端使能Stelnet服务器功能。
#
```

步骤3 SSH客户端的配置

```
#
 ssh client first-time enable  //第一次登录，则需要在SSH客户端使能首次认证功能
#
```

步骤4 验证配置结果

SSH客户端采用RADIUS认证连接SSH服务器。

```
<ssh client> system-view
[ssh client] stelnet 10.164.39.222
```


版权所有 © 华为技术有限公司

```
Please input the username: ssh1@ssh.com
Trying 10.164.39.222 ...
Press CTRL+K to abort
Connected to 10.164.39.222 ...
The server is not authenticated. Do you continue to access it?(Y/N):y
Save the server's public key? [Y/N] :y
The server's public key will be saved with the name: 10.164.39.222. Please wait...
Enter password:
```

输入密码huawei，显示登录成功信息如下：

```
Info: The max number of VTY users is 10, and the current number
      of VTY users on line is 2.
```

在SSH服务器端执行**display radius-server configuration**命令和**display ssh server session**命令，可以查看到SSH服务器端关于RADIUS服务器的配置，并且看到STelnet客户端采用RADIUS认证已经成功连接到SSH服务器。

```
[ssh server] display ssh server session
------------------------------------------------------------------------
 Conn    Ver    Encry     State  Auth-type        Username
 ------------------------------------------------------------------------
 VTY 0  2.0    AES       run    password         ssh1@ssh.com
 ------------------------------------------------------------------------
```

----结束

配置注意事项

- 在RADIUS服务器端添加对应客户端的用户名。
- 在RADIUS服务器端指定SSH服务器的地址和密钥。
- 如果配置SSH客户端用户使用password验证，只需在SSH服务器端生成本地RSA密钥。如果配置SSH客户端用户使用RSA验证，则在SSH服务器端和客户端都需生成本地RSA密钥，并将客户端上产生的RSA公钥输入到服务器端。

2.2.9 查看设备基本状态

操作步骤

- 查看系统软件版本信息

  确认当前的系统软件版本是进行软件升级、定位问题的前提。

  执行命令**display version**，可以查看设备当前的版本信息。

```
<Huawei> display version
Huawei Versatile Routing Platform Software  //华为公司虚拟路由平台（VRP）软
件
VRP (R) software, Version 5.120 (AR6300 V300R022C00)  //产品的版本为V300R022C00，与之匹配的
VRP版本为5.120
Copyright (C) 2011-2021 HUAWEI TECH CO., LTD   //华为公司版权声明
Huawei AR6300 Router uptime is 0 week, 6 days, 16 hours, 39 minutes    //设备启动后已经运行的时间
BKP 0 version information:   //背板的版本信息
1. PCB      Version  : SUA2BKPA VER.A       //背板的PCB版本号
2. If Supporting PoE : No          //是否支持POE功能
3. Board    Type     : AR6300      //背板的单板类型
4. MPU Slot Quantity : 1
5. LPU Slot Quantity : 1

MPU 0(Master) : uptime is 0 week, 6 days, 16 hours, 37 minutes   //主控板启动后已经运行的时间
SDRAM Memory Size    : 31744   M bytes  //系统内存的空间大小
Flash 0 Memory Size  : 3082    M bytes  //闪存的空间大小
VHDD0 Memory Size    : 56674   M bytes   //VHDD的空间大小
MPU version information :      //主控板的版本信息
```

 版权所有 © 华为技术有限公司

```
1. PCB      Version  : SRU-400H VER.B
2. MAB      Version  : 0
3. Board    Type     : SRU-400H
4. CPLD0    Version  : 64

LPU 1 : uptime is 0 week, 6 days, 16 hours, 36 minutes
SDRAM Memory Size    : 256     M bytes
Flash 0 Memory Size  : 16      M bytes
VHDD0 Memory Size    : 56674   M bytes
LPU version information :
1. PCB      Version  : AR01SDCE2A VER.B
2. MAB      Version  : 0
3. Board    Type     : 1E1/T1-F
4. CPLD0    Version  : 64
5. BootROM  Version  : 510
```

- 查看设备的部件信息

  当设备或单板发生异常时，可以查看设备或某接口板是否在位以及状态是否正常。

  执行命令**display device**，可以查看设备的部件信息。例如：

```
<Huawei> display device
AR6300's Device status:
Slot  Sub Type           Online   Power     Register      Alarm       Primary
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
1     -   2FE            Present  PowerOn   Registered    Normal      NA
2     -   -              Present  PowerOff  Unregistered  Nonsupport  NA
3     -   2SA            Present  PowerOn   Registered    Normal      NA
5     -   8E1/T1-F       Present  PowerOn   Registered    Normal      NA
6     -   -              Present  PowerOff  Unregistered  TimeOutReg  NA
8     -   24GE           Present  PowerOn   Registered    Normal      NA
14    -   SRU-400H       Present  PowerOn   Registered    Normal      Master
```

- 查看设备的健康状态

  执行命令**display health**，可以查看设备的温度信息、电源信息、风扇信息、功率信息、CPU占用率信息、内存占用率信息以及存储介质使用信息。例如：

```
<Huawei> display health
-------------------------------------------------------------------------------
 Slot  Card  Sensor No.  SensorName      Status  Upper  Lower  Temperature.(C)
-------------------------------------------------------------------------------
 1     -     1          8FE1GE TEMP     NORMAL  75     0      29  //1号槽位所在8FE1GE单板的当前温度为29℃，产生温度告警的上限阈值为75℃，下限阈值为0℃
 2     -     1          8FE1GE TEMP     NORMAL  75     0      31
 5     -     1          8AS TEMP        NORMAL  75     0      30
 6     -     1          8FE1GE TEMP     NORMAL  85     0      32
 13    -     1          SRU-600H TEMP   NORMAL  70     0      38
-------------------------------------------------------------------------------
 PowerNo  Present  Mode   State     Current(A)   Voltage(V)   Power(W)
-------------------------------------------------------------------------------
  9       YES     AC     Supply    N/A          12           350  //9号槽位所在的电源模块为交流电源，供电正常，电源额定电压为12伏特，额定功率为350瓦
  10      NO      N/A    N/A       N/A          N/A          N/A
-------------------------------------------------------------------------
        FanId  FanNum  Present  Register  Speed  Mode
-------------------------------------------------------------------------
        12     [1-5]   YES      YES       35%    AUTO  //12号槽位所在的风扇在线且已注册，工作模式为自动方式，风扇转速为35%
                1                  2130
                2                  2070
                3                  2070
                4                  2160
                5                  2130
 The  total power is : 350(W)  //设备总功率
 The   used power is : 141(W)  //设备已用功率
 The remain power is : 209(W)  //设备剩余功率
 The system used power detail information :  //设备所用功率的详细信息
```

 版权所有 © 华为技术有限公司

```
--------------------------------------------------------------------------------
 SlotID  BoardType    Power-Used(W)  Power-Requested(W)
--------------------------------------------------------------------------------
 1       8FE1GE       7.366          14  //1号槽位所在的8FE1GE单板的额定功率为14瓦，已消耗功率为7.366
瓦。
 2       8FE1GE       7.366          14
 5       8AS          3.968          5
 6       8FE1GE       7.366          14
 13      SRU-600H     55.790         84
System CPU Usage Information:
 System cpu usage at 2012-04-27  10:27:34 290 ms
--------------------------------------------------------------------------------
 SlotID  CPU Usage  Upper Limit
--------------------------------------------------------------------------------
 5       2 %        80%  //5号槽位所在单板的CPU占用率为2%，超过80%时设备会触发过载告
警。
 6       4 %        80%
 13      8 %        80%
System Memory Usage Information:
 System memory usage at 2012-04-27  10:27:34 370 ms
--------------------------------------------------------------------------------
 SlotID  Total Memory(MB)  Used Memory(MB)  Used Percentage  Upper Limit
--------------------------------------------------------------------------------
 5       176              3                1 %              95%  //5号槽位所在的单板总内存为176MB，已用3MB，
内存占用率为1%，当占用率超过95%时，设备会触发告警
 6       176              20               11%              95%
 13      1257             186              14%              95%
System Disk Usage Information:  //设备存储介质使用情况
 System disk usage at 2012-04-27  10:27:34 450 ms
--------------------------------------------------------------------------------
 SlotID  Device  Total Memory(MB)  Used Memory(MB)  Used Percentage
--------------------------------------------------------------------------------
 13      usb1:   1882             874              46%
         flash:  2                0                6%
```

- 查看CPU占用率的统计信息

  CPU占用率是衡量设备性能的重要指标之一。在网络运行中，CPU占用率过高常常会导致其他业务异常，例如BGP震荡、VRRP频繁切换甚至设备无法登录。

  执行命令**display cpu-usage**，可以查看设备CPU占用率的统计信息。例如：

```
<Huawei> display cpu-usage
CPU Usage Stat. Cycle: 10 (Second)  //CPU占用率统计周期为10秒
CPU Usage Stat. Time : 2012-04-27  11:34:05  //最近一次统计CPU占用率的时刻
Control Plane  //最近一次统计到的控制平面的CPU的占用率
   CPU Usage:   7%  Max: 100%
   User: 10.7%   System:  6.9%   SoftIrq:  0.0%   HardIrq:  5.5%   Idle:
76.7%
   CPU utilization for ten seconds:  7%  one minute:   5%  five minutes:   5%.
Data    Plane  //最近一次统计到的转发平面的CPU的占用率
   CPU Usage:   1%  Max:   5%
   CPU utilization for ten seconds:  1%  one minute:   1%  five minutes:   1%.

PID   ProcessName        CPU%     CoreIndex      Runtime     State
194   cap32              1.7%     CPU1           26132042
193   vrp               20.0%     CPU0           11216335    S
191   monitor            0.0%     CPU0           2324        S
74    loop0              0.0%     CPU0           1913        S
13    bdi-default        0.0%     CPU0           977         S
7     events/0           0.0%     CPU0           708         S
138   k3gdevd            0.0%     CPU0           423         S
192   cap32              0.0%     CPU0           211         S
12    sync_supers        0.0%     CPU0           204         S
56    VFDS               0.0%     CPU0           166         S
1     init               0.0%     CPU0           90          S
19    kswapd0            0.0%     CPU0           63          S
30    mtdblockd          0.0%     CPU0           35          S
16    khubd              0.0%     CPU0           10          S
2     kthreadd           0.0%     CPU0           0           S
```

 版权所有 © 华为技术有限公司

```
3     migration/0        0.0%      CPU0          0          S
4     ksoftirqd/0        0.0%      CPU0          0          S
5     migration/1        0.0%      CPU0          0          S
6     ksoftirqd/1        0.0%      CPU0          0          S
8     events/1           0.0%      CPU0          0          R
9     cpuset             0.0%      CPU0          0          S
10    khelper            0.0%      CPU0          0          S
11    async/mgr          0.0%      CPU0          0          S
14    kblockd/0          0.0%      CPU0          0          S
15    kblockd/1          0.0%      CPU0          0          S
20    aio/0              0.0%      CPU0          0          S
21    aio/1              0.0%      CPU0          0          S
22    crypto/0           0.0%      CPU0          0          S
23    crypto/1           0.0%      CPU0          0          S
29    sdcardqueue        0.0%      CPU0          0          S
139   k3gtxd             0.0%      CPU0          0          S
153   udpsvd             0.0%      CPU0          0          S
271   loop1              0.0%      CPU0          0          S
486   flush-mtd-unmap    0.0%      CPU0          0          S
```

- 查看当前的配置信息

  执行命令**display current-configuration**，可以查看设备当前的配置信息。例如：

```
<Huawei> display current-configuration
[V300R019C00SPC200]  //设备版本信息
#  //FTP服务器配置信息
 ftp server permit interface all
 ftp server enable
#  //槽位最近一次在位的单板信息
 board add 0/1 4G.SHDSL
 board add 0/2 8FE1GE
 board add 0/3 1SA
 board add 0/4 2E1-MFT
 board add 0/5 8FE1GE
#  //SNMP代理配置信息
 snmp-agent local-engineid 800007DB0380FB063545B3
 snmp-agent
#  //接口配置信息
interface Ethernet2/0/0
 ip address 2.2.2.2 255.255.255.0
#  //OSPF路由协议配置信息
ospf 1
 area 0.0.0.0
  network 19.19.19.0 0.0.0.255
#  //静态路由配置信息
ip route-static 0.0.0.0 0.0.0.0 192.168.200.100
#  //语音配置信息
voice
 #
 r2 signalling-type argentina
 #
 r2 signalling-type brazil
 #
 r2 signalling-type mexico
 #
 r2 signalling-type standard
 #
 diagnose
#
return
```

----结束

2.3 升级设备（命令行方式）

 版权所有 © 华为技术有限公司

2.3.1 通过 BootLoader SFTP 方式升级系统文件的示例

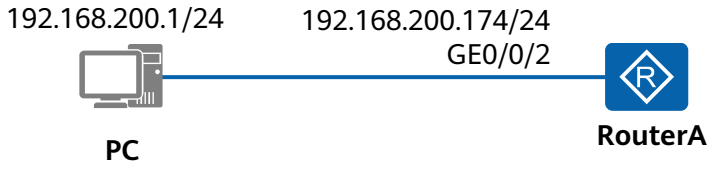
规格

适用于所有版本、所有形态的AR路由器。

组网需求

RouterA的管理网口与用户侧主机PC相连。要求通过BootLoader菜单下载系统文件至RouterA完成系统升级。

图 2-18 通过 BootLoader SFTP 方式升级系统文件的组网图



操作步骤

步骤1 在PC端启动SFTP Server服务。

步骤2 用串口线连接并通过Console口登录设备。

步骤3 重启设备，在设备出现“Press Ctrl+B to break auto startup ...”打印信息时，按下“Ctrl+B”并键入密码后进入BootLoader主菜单。

```
Press Ctrl+B to break auto startup ... 3
BootLoader management port is GE 0/0/8.

Enter Password:
```

步骤4 进入BootLoader菜单后，选择第3项，进入网络子菜单。

```
    Main Menu

  1. Default startup
  2. Serial submenu
  3. Ethernet submenu
  4. Startup parameters submenu
  5. File system submenu
  6. Password manager submenu
  0. Reboot

Enter your choice(0-6):3
```

步骤5 进入网络子菜单后，选择第3项，修改属性。

```
   Ethernet submenu

  1. Update software
  2. Display parameters
  3. Modify parameters
  4. Save parameters
  0. Return

Enter your choice(0-4):3
```


版权所有 © 华为技术有限公司

步骤6 选择FTP type为SFTP类型，设置SFTP Server的IP地址、用户名和密码，设置设备管理网口的IP地址、子网掩码。

```
NOTE:
Net type define  0(ftp), 1(tftp), 2(sftp),
ENTER = no change;

FTP type(0:FTP 1:TFTP 2:SFTP): 0  2
Server IP address     : 192.168.1.20
Local IP address      : 192.168.1.8
Local IP mask         : 255.255.255.0
FTP username           : huawei
FTP password          : *******
```

步骤7 完成属性配置后，返回至BootLoader主菜单，选择第5项，进入文件管理菜单。

```
      Main Menu

  1. Default startup
  2. Serial submenu
  3. Ethernet submenu
  4. Startup parameters submenu
  5. File system submenu
  6. Password manager submenu
  0. Reboot

Enter your choice(0-6):5
      File system submenu

  1. Flash file system
  0. Return

Enter your choice(0-1):
```

步骤8 进入文件系统菜单，选择第1项，进入**Flash file system**菜单。

```
      File system submenu

  1. Flash file system
  0. Return

Enter your choice(0-1):1
      Flash file system

  1. List file
  2. Rename file
  3. Delete file
  4. Format flash
  5. Upload file to server
  6. Download file from server
  0. Return

Enter your choice(0-6):
```

步骤9 选择第6项，进入**Download file from server**菜单，可以从此菜单从服务器下载文件到设备。

```
Enter your choice(0-6): 6
Please input the file name: software.cc
Downloading ....
file downloading is completed,writing file:[ flash:/software.cc ]to file system OK!
```

步骤10 下载文件成功后返回主菜单，修改启动配置信息。

```
      Flash file system

  1. List file
  2. Rename file
  3. Delete file
  4. Format flash
  5. Upload file to server
  6. Download file from server
```

 版权所有 © 华为技术有限公司

```
  0. Return

Enter your choice(0-6):0
      File system submenu

  1. Flash file system
  0. Return

Enter your choice(0-1):0
      Main Menu

  1. Default startup
  2. Serial submenu
  3. Ethernet submenu
  4. Startup parameters submenu
  5. File system submenu
  6. Password manager submenu
  0. Reboot

Enter your choice(0-6):4
```

步骤11 设置下次启动的系统软件。

```
      Startup parameters submenu

  1. Display current startup configuration
  2. Modify the startup file
  3. Modify the configuration file
  4. Modify the patch file

  0. Return

Enter your choice(0-5):2
      Modify the startup file

  1. flash
  0. Return

Enter your choice(0-1):1
NOTE: Boot file must be .cc or .CC

Current boot file: flash:/softwarenew.cc
Press ENTER directly for no change.
Or, please input the new file name: flash:/software.cc
Save the boot file name: flash::/software.cc ? Yes or No(Y/N)y
Save load state word...OK!
```

步骤12 返回主菜单，重启设备。

```
      Startup parameters submenu

  1. Display current startup configuration
  2. Modify the startup file
  3. Modify the configuration file
  4. Modify the patch file

  0. Return

Enter your choice(0-5):0
      Main Menu

  1. Default startup
  2. Serial submenu
  3. Ethernet submenu
  4. Startup parameters submenu
  5. File system submenu
  6. Password manager submenu
  0. Reboot
```

 版权所有 © 华为技术有限公司

```
Enter your choice(0-6):0
```

----结束

配置注意事项

不建议在BootLoader菜单操作，若特别必要，可联系技术支持人员指导操作。

2.3.2 通过 BootLoader FTP 方式升级系统文件的示例

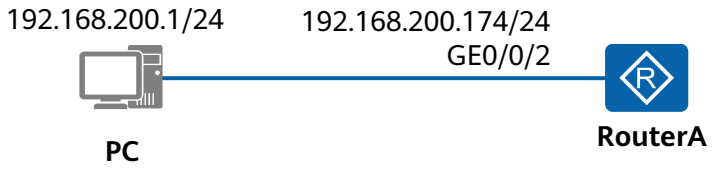
规格

适用于所有版本、所有形态的AR路由器。

组网需求

RouterA的管理网口与用户侧主机PC相连。要求通过BootLoader菜单下载系统文件至RouterA完成系统升级。

图 2-19 通过 BootLoader FTP 方式升级系统文件的组网图



说明

FTP为不安全协议，用户如果对网络安全要求较高，建议使用SFTP。

操作步骤

步骤1 在PC端启动FTP Server服务。

步骤2 用串口线连接并通过Console口登录设备。

步骤3 重启设备，在设备出现“Press Ctrl+B to break auto startup ...”打印信息时，按下“Ctrl+B”并键入密码后进入BootLoader主菜单。

```
Press Ctrl+B to break auto startup ... 3
BootLoader management port is GE 0/0/8.

Enter Password:
```

步骤4 进入BootLoader菜单后，选择第3项，进入网络子菜单。

```
    Main Menu

  1. Default startup
  2. Serial submenu
  3. Ethernet submenu
  4. Startup parameters submenu
  5. File system submenu
  6. Password manager submenu
  0. Reboot
```


版权所有 © 华为技术有限公司

```
Enter your choice(0-6):3
```

步骤5 进入网络子菜单后，选择第3项，修改属性。

```
      Ethernet submenu

  1. Update software
  2. Display parameters
  3. Modify parameters
  4. Save parameters
  0. Return

Enter your choice(0-4):3
```

步骤6 选择FTP type为FTP类型，设置FTP Server的IP地址、用户名和密码，设置设备管理网口的IP地址、子网掩码。

```
NOTE:
Net type define:  0(ftp), 1(tftp), 2(sftp),
ENTER = no change;

FTP type(0:FTP 1:TFTP 2:SFTP): 0 0
Warning: FTP is not secure. SFTP is recommended!
Server IP address     : 192.168.1.20
Local IP address      : 192.168.1.8
Local IP mask         : 255.255.255.0
FTP username          : huawei
FTP password          : *******
```

步骤7 完成属性配置后，返回至BootLoader主菜单，选择第5项，进入文件管理菜单。

```
      Main Menu

  1. Default startup
  2. Serial submenu
  3. Ethernet submenu
  4. Startup parameters submenu
  5. File system submenu
  6. Password manager submenu
  0. Reboot

Enter your choice(0-6):5
      File system submenu

  1. Flash file system
  0. Return

Enter your choice(0-1):
```

步骤8 进入文件系统菜单，选择第1项，进入**Flash file system**菜单。

```
      File system submenu

  1. Flash file system
  0. Return

Enter your choice(0-1):1
      Flash file system

  1. List file
  2. Rename file
  3. Delete file
  4. Format flash
  5. Upload file to server
  6. Download file from server
  0. Return

Enter your choice(0-6):
```

步骤9 选择第6项，进入**Download file from server**菜单，可以从此菜单从服务器下载文件到设备。

 版权所有 © 华为技术有限公司

```
Enter your choice(0-6): 6
Please input the file name: software.cc
Downloading ....
file downloading is completed,writing file:[ flash:/software.cc ]to file system OK!
```

步骤10 下载文件成功后返回主菜单，修改启动配置信息。

```
      Flash file system

  1. List file
  2. Rename file
  3. Delete file
  4. Format flash
  5. Upload file to server
  6. Download file from server
  0. Return

Enter your choice(0-6):0
      File system submenu

  1. Flash file system
  0. Return

Enter your choice(0-1):0
      Main Menu

  1. Default startup
  2. Serial submenu
  3. Ethernet submenu
  4. Startup parameters submenu
  5. File system submenu
  6. Password manager submenu
  0. Reboot

Enter your choice(0-6):4
```

步骤11 设置下次启动的系统软件。

```
      Startup parameters submenu

  1. Display current startup configuration
  2. Modify the startup file
  3. Modify the configuration file
  4. Modify the patch file

  0. Return

Enter your choice(0-5):2
      Modify the startup file

  1. flash
  0. Return

Enter your choice(0-1):1
NOTE: Boot file must be .cc or .CC

Current boot file: flash:/softwarenew.cc
Press ENTER directly for no change.
Or, please input the new file name: flash:/software.cc
Save the boot file name: flash::/software.cc ? Yes or No(Y/N)y
Save load state word...OK!
```

步骤12 返回主菜单，重启设备。

```
      Startup parameters submenu

  1. Display current startup configuration
  2. Modify the startup file
  3. Modify the configuration file
  4. Modify the patch file

  0. Return
```

 版权所有 © 华为技术有限公司

```
Enter your choice(0-5):0
      Main Menu

  1. Default startup
  2. Serial submenu
  3. Ethernet submenu
  4. Startup parameters submenu
  5. File system submenu
  6. Password manager submenu
  0. Reboot

Enter your choice(0-6):0
```

----结束

配置注意事项

不建议在BootLoader菜单操作，若特别必要，可联系技术支持人员指导操作。

2.3.3 通过 BootLoader TFTP 方式升级系统文件的示例

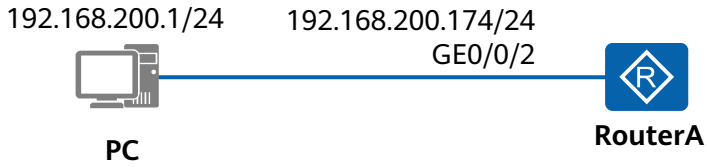
规格

适用于所有版本、所有形态的路由器。

组网需求

RouterA的管理网口与用户侧主机PC相连。要求通过BootLoader菜单下载系统文件至RouterA完成系统升级。

图 2-20 通过 BootLoader TFTP 方式升级系统文件的组网图



说明

TFTP为不安全协议，用户如果对网络安全要求较高，建议使用SFTP。

操作步骤

步骤1 在PC端启动TFTP Server服务。

步骤2 用串口线连接并通过Console口登录设备。

步骤3 重启设备，在设备出现“Press Ctrl+B to break auto startup ...”打印信息时，按下“Ctrl+B”并键入密码后进入BootLoader主菜单。

```
Press Ctrl+B to break auto startup ... 3
BootLoader management port is GE 0/0/8.

Enter Password:
```

 版权所有 © 华为技术有限公司

步骤4 进入BootLoader菜单后，选择第3项，进入网络子菜单。

```
    Main Menu

  1. Default startup
  2. Serial submenu
  3. Ethernet submenu
  4. Startup parameters submenu
  5. File system submenu
  6. Password manager submenu
  0. Reboot

Enter your choice(0-6):3
```

步骤5 进入网络子菜单后，选择第3项，修改属性。

```
   Ethernet submenu

  1. Update software
  2. Display parameters
  3. Modify parameters
  4. Save parameters
  0. Return

Enter your choice(0-4):3
```

步骤6 进入BootLoader菜单后，选择第3项，进入网络子菜单。

```
    Main Menu

  1. Default Startup
  2. Serial Menu
  3. Network Menu
  4. Startup Select
  5. File Manager
  6. Password Manager
  7. Reboot

Enter your choice(1-7):3
```

步骤7 选择FTP type为TFTP类型，设置TFTP Server的IP地址，设置设备管理网口的IP地址和子网掩码。

```
NOTE:
Net type define:  0(ftp), 1(tftp), 2(sftp),
ENTER = no change;

FTP type(0:FTP 1:TFTP 2:SFTP): 0 1
Warning: TFTP is not secure. SFTP is recommended!
Server IP address     : 192.168.1.20
Local IP address      : 192.168.1.8
Local IP mask         : 255.255.255.0
FTP username          :
FTP password          :
```

步骤8 完成属性配置后，返回至BootLoader主菜单，选择第5项，进入文件管理菜单。

```
    Main Menu

  1. Default startup
  2. Serial submenu
  3. Ethernet submenu
  4. Startup parameters submenu
  5. File system submenu
  6. Password manager submenu
  0. Reboot

Enter your choice(0-6):5
    File system submenu

  1. Flash file system
  0. Return
```

 版权所有 © 华为技术有限公司

```
Enter your choice(0-1):
```

步骤9 进入文件系统菜单，选择第1项，进入**Flash file system**菜单。

```
      File system submenu

  1. Flash file system
  0. Return

Enter your choice(0-1):1
      Flash file system

  1. List file
  2. Rename file
  3. Delete file
  4. Format flash
  5. Upload file to server
  6. Download file from server
  0. Return

Enter your choice(0-6):
```

步骤10 选择第6项，进入**Download file from server**菜单，可以从此菜单从服务器下载文件到设备。

```
Enter your choice(0-6): 6
Please input the file name: software.cc
Downloading ....
file downloading is completed,writing file:[ flash:/software.cc ]to file system OK!
```

步骤11 下载文件成功后返回主菜单，修改启动配置信息。

```
      Flash file system

  1. List file
  2. Rename file
  3. Delete file
  4. Format flash
  5. Upload file to server
  6. Download file from server
  0. Return

Enter your choice(0-6):0
      File system submenu

  1. Flash file system
  0. Return

Enter your choice(0-1):0
      Main Menu

  1. Default startup
  2. Serial submenu
  3. Ethernet submenu
  4. Startup parameters submenu
  5. File system submenu
  6. Password manager submenu
  0. Reboot

Enter your choice(0-6):4
```

步骤12 设置下次启动的系统软件。

```
      Startup parameters submenu

  1. Display current startup configuration
  2. Modify the startup file
  3. Modify the configuration file
  4. Modify the patch file

  0. Return
```

 版权所有 © 华为技术有限公司

```
Enter your choice(0-5):2
      Modify the startup file

   1. flash
   0. Return

Enter your choice(0-1):1
NOTE: Boot file must be .cc or .CC

Current boot file: flash:/softwarenew.cc
Press ENTER directly for no change.
Or, please input the new file name: flash:/software.cc
Save the boot file name: flash::/software.cc ? Yes or No(Y/N)y
Save load state word...OK!
```

步骤13 返回主菜单，重启设备。

```
      Startup parameters submenu

   1. Display current startup configuration
   2. Modify the startup file
   3. Modify the configuration file
   4. Modify the patch file

   0. Return

Enter your choice(0-5):0
      Main Menu

   1. Default startup
   2. Serial submenu
   3. Ethernet submenu
   4. Startup parameters submenu
   5. File system submenu
   6. Password manager submenu
   0. Reboot

Enter your choice(0-6):0
```

----结束

配置注意事项

不建议在BootLoader菜单操作，若特别必要，可联系技术支持人员指导操作。

2.3.4 配置路由器作为 TFTP Client 升级系统文件的示例

规格

适用于所有版本、所有形态的AR路由器。

组网需求

AR路由器作为TFTP客户端与TFTP服务器端相连。要求通过TFTP方式下载系统文件至路由器完成系统升级。

图 2-21 配置路由器作为 TFTP Client 升级系统文件组网图

 版权所有 © 华为技术有限公司

操作步骤

步骤1 路由器的基本配置。

```
#
 interface GigabitEthernet0/0/0
  ip address 10.1.1.2 255.255.255.0 //用于连接Server的IP地址
```

步骤2 查看设备启动时使用的系统文件与配置文件信息。

```
<Huawei> display startup
MainBoard:
  Startup system software:                  flash:/software.cc
  Next startup system software:               flash:/software.cc
  Backup system software for next startup:   null
  Startup saved-configuration file:          flash:/initcfg.cfg
  Next startup saved-configuration file:     flash:/initcfg.cfg
```

步骤3 下载设备启动文件，并查看文件是否下载成功。

```
<Huawei> tftp 10.1.1.1 get software_new.cc
Info: Transfer file in binary mode.
Downloading the file from the remote TFTP server. Please wait...
77,582,080 bytes received in 241 seconds.
TFTP: Downloading the file successfully.
<Huawei> dir
Directory of flash:/

  Idx  Attr     Size(Byte)  Date        Time(LMT)   FileName
    0  -rw-     69,363,072  Nov 21 2011 19:58:50    software.cc
    5  -rw-     77,582,080  Dec 13 2011 10:41:12    software_new.cc
```

步骤4 指定设备下次启动时使用的系统文件。

```
<Huawei> startup system-software software_new.cc
This operation will take several minutes, please wait.........
Info: Succeeded in setting the file for booting system
```

步骤5 重新启动设备。

```
<Huawei> reboot
Info: The system is comparing the configuration, please wait.
Warning: All the configuration will be saved to the next startup configuration.
Continue ? [y/n]:n
System will reboot! Continue ? [y/n]:y
Info: system is rebooting ,please wait...
```

步骤6 验证配置结果。

```
<Huawei> display startup
MainBoard:
  Startup system software:                  flash:/software_new.cc
  Next startup system software:               flash:/software_new.cc
  Backup system software for next startup:   null
  Startup saved-configuration file:          flash:/initcfg.cfg
  Next startup saved-configuration file:     flash:/initcfg.cfg
```

----结束

配置注意事项

- PC端需使能TFTP服务器功能，并存放系统文件。
- 保证设备操作期间，不能出现断电现象，断电后，可能会导致信息丢失，设备无法正常启动。

 版权所有 © 华为技术有限公司

2.3.5 配置路由器作为 FTP Client 升级系统文件的示例

规格

适用于所有版本、所有形态的AR路由器。

组网需求

AR设备作为FTP客户端与FTP服务器端相连。要求通过FTP方式下载系统文件至设备完成系统升级。

图 2-22 配置路由器作为 FTP Client 升级系统文件组网图

操作步骤

步骤1 设备的基本配置

```
#
 interface GigabitEthernet0/0/0
  ip address 10.1.1.2 255.255.255.0 //用于连接Server的IP地址
```

步骤2 查看设备启动时使用的系统文件与配置文件信息

```
<Huawei> display startup
MainBoard:
  Startup system software:                flash:/software.cc
  Next startup system software:           flash:/software.cc
  Backup system software for next startup:   null
  Startup saved-configuration file:       flash:/initcfg.cfg
  Next startup saved-configuration file:     flash:/initcfg.cfg
```

步骤3 从FTP Server端下载系统文件并查看是否下载成功

```
<Huawei> ftp 10.1.1.1
Trying 10.1.1.1 ...
Press CTRL+K to abort
Connected to 10.1.1.1.
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
User(192.168.200.1:(none)):huawei
331 Give me your password, please
Enter password:
230 Logged in successfully
[Huawei-ftp]binary
200 Type set to I.

[Huawei-ftp]get software_new.cc
200 PORT command okay
150 "D:\ftp\software_new.cc" file ready to send (77582080 bytes) in i
mage / Binary mode
.....
.....
.....
.....
.....
.....
```


版权所有 © 华为技术有限公司

```
.....................................................................
.....................
226 Transfer finished successfully.
FTP: 77582080 byte(s) received in 152.403 second(s) 509.05Kbyte(s)/sec.
[Huawei-ftp]quit
221 Windows FTP Server (WFTPD, by Texas Imperial Software) says goodbye
<Huawei> dir
Directory of flash:/

  Idx  Attr     Size(Byte)  Date        Time(LMT)  FileName
    5  -rw-     69,363,072  Nov 21 2011 19:58:50   software.cc
    7  -rw-     77,582,080  Dec 14 2011 10:28:31   software_new.cc
```

步骤4 指定设备启动时使用的系统文件

```
<Huawei> startup system-software software_new.cc
This operation will take several minutes, please wait.........
Info: Succeeded in setting the file for booting system
```

步骤5 重新启动设备

```
<Huawei> reboot
Info: The system is comparing the configuration, please wait.
Warning: All the configuration will be saved to the next startup configuration.
Continue ? [y/n]:n
System will reboot! Continue ? [y/n]:y
Info: system is rebooting ,please wait...
```

步骤6 重启后完毕Telnet到设备，验证配置结果

```
<Huawei> display startup
MainBoard:
  Startup system software:                flash:/software_new.cc
  Next startup system software:           flash:/software_new.cc
  Backup system software for next startup:   null
  Startup saved-configuration file:       flash:/initcfg.cfg
  Next startup saved-configuration file:     flash:/initcfg.cfg
```

----结束

配置注意事项

- PC端需使能FTP服务器功能，并存放系统文件。
- 保证设备操作期间，不能出现断电重起现象，断电后，会导致信息丢失，设备无法正常启动。

相关资料

视频

配置路由器作为FTP Client升级系统文件

2.3.6 配置路由器作为 FTP Server 升级系统文件的示例

规格

适用于所有版本、所有形态的AR路由器。

组网需求

设备需要进行升级操作，要求将设备作为FTP服务器，从终端PC将系统软件上传至设备。

 版权所有 © 华为技术有限公司

图 2-23 配置路由器作为 FTP Server 升级系统文件组网图

操作步骤

步骤1 FTP Server的配置。

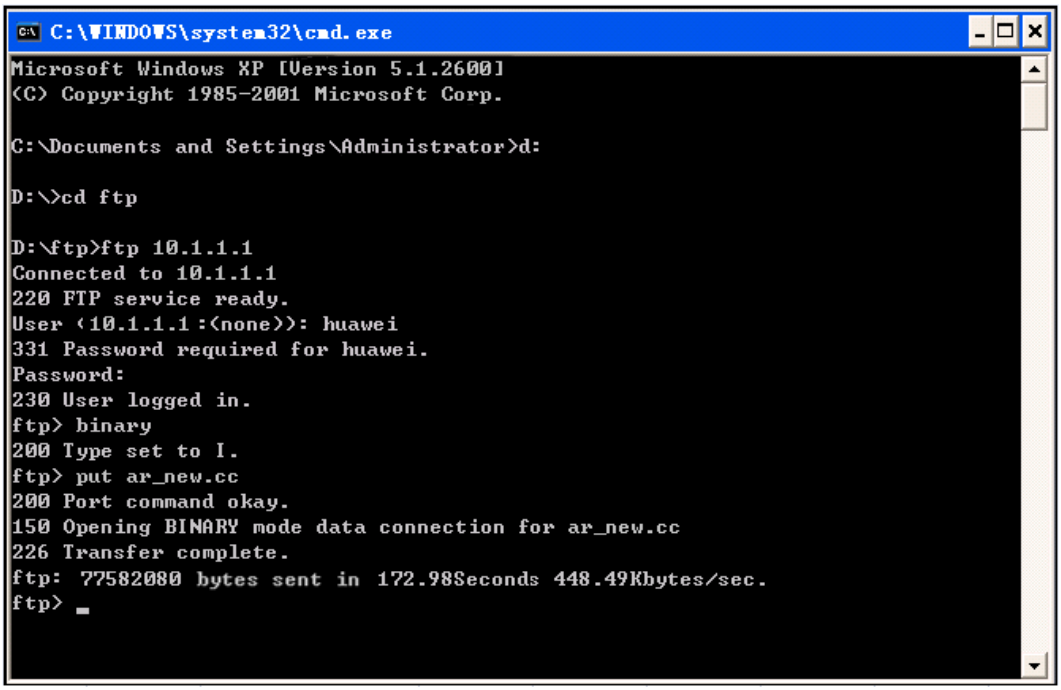
```
#
 ftp server permit interface all //配置FTP服务器允许客户端连接的接口，否则无法开启FTP服务器功能。
 ftp server enable //全局启用FTP Server
#
aaa
 local-user huawei password irreversible-cipher   //创建本地账号和密码
 local-user huawei privilege level 15  //配置本地用户的级别
 local-user huawei ftp-directory flash: //配置本地用户的授权目录
 local-user huawei service-type ftp //配置本地用户的服务类型为FTP
#
 interface GigabitEthernet0/0/0
 ip address 10.1.1.1 255.255.255.0 //用于连接Client的IP地址
```

步骤2 查看设备启动时使用的系统文件与配置文件信息。

```
<Huawei> display startup
MainBoard:
  Startup system software:                flash:/software.cc
  Next startup system software:           flash:/software.cc
  Backup system software for next startup:   null
  Startup saved-configuration file:       flash:/initcfg.cfg
  Next startup saved-configuration file:     flash:/initcfg.cfg
```

步骤3 在FTP Client端上传系统文件，如图2-24。

图 2-24 在 FTP Client 端上传系统文件



 版权所有 © 华为技术有限公司

步骤4 在FTP Server端查看系统文件是否上传成功。

```
<Huawei> dir
Directory of flash:/

  Idx  Attr     Size(Byte)   Date        Time(LMT)   FileName
    1  -rw-     69,363,072   Nov 21 2011 19:58:50    software.cc
    2  -rw-     77,582,080   Dec 13 2011 16:31:17    software_new.cc
```

步骤5 指定设备启动时使用的系统文件。

```
<Huawei> startup system-software software_new.cc
This operation will take several minutes, please wait.........
Info: Succeeded in setting the file for booting system
```

步骤6 重新启动设备。

```
<Huawei> reboot
Info: The system is comparing the configuration, please wait.
Warning: All the configuration will be saved to the next startup configuration.
Continue ? [y/n]:n
System will reboot! Continue ? [y/n]:y
Info: system is rebooting ,please wait...
```

步骤7 重启后完毕Telnet到设备，验证配置结果。

```
<Huawei> display startup
MainBoard:
  Startup system software:                flash:/software_new.cc
  Next startup system software:           flash:/software_new.cc
  Backup system software for next startup:   null
  Startup saved-configuration file:       flash:/initcfg.cfg
  Next startup saved-configuration file:     flash:/initcfg.cfg
```

----结束

配置注意事项

- 设备操作期间，尽量避免出现断电现象，如出现，可能会导致信息丢失，设备无法正常启动。
- FTP的工作目录必须配置，除了使用**local-user huawei ftp-directory**设置本地用户的授权目录，还可以通过**set default ftp-directory**来设置FTP用户的缺省工作目录。

2.4 操作 BootLoader 菜单

2.4.1 配置通过 BootLoader 清除 Console 口和 Telnet 密码的示例

规格

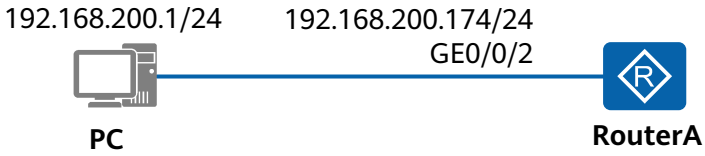
适用于所有版本、所有形态的AR路由器。

组网需求

RouterA的管理网口与用户侧主机PC相连。要求通过BootLoader菜单清除console口密码以及telnet密码。

 版权所有 © 华为技术有限公司

图 2-25 通过 BootLoader 清除 Console 口和 Telnet 密码的组网图



操作步骤

步骤1 用串口线连接并通过Console口登录设备。

步骤2 重启设备，在设备出现“Press Ctrl+B to break auto startup ...”打印信息时，按下“Ctrl+B”并键入密码后进入BootLoader主菜单。

```
Press Ctrl+B to break auto startup ... 3
BootLoader management port is GE 0/0/8.

Enter Password:
```

步骤3 进入BootLoader菜单后，可通过**a**或者**b**两种方法进行BootLoader清除Console口和Telnet密码。

1. 选择第4项，进入Startup parameters submenu菜单。

```
    Main Menu

  1. Default startup
  2. Serial submenu
  3. Ethernet submenu
  4. Startup parameters submenu
  5. File system submenu
  6. Password manager submenu
  0. Reboot

Enter your choice(0-6):4
```

   a. 查看系统使用的配置信息，进入Startup parameters submenu菜单后，选择第1项。

```
    Startup parameters submenu

  1. Display current startup configuration
  2. Modify the startup file
  3. Modify the configuration file
  4. Modify the patch file
  0. return

Enter your choice(0-5):1

************** Current Startup info ****************
Valid Flag State       : Vaild
Boot File Name         : flash:/software.cc
Config File Name       : flash:/vrpcfg.cfg
Licence File Name      :
Patch File Name        :
Voice File Name        :
```

   b. 重命名系统使用的配置文件。

```
    Startup parameters submenu

  1. Display current startup configuration
  2. Modify the startup file
  3. Modify the configuration file
  4. Modify the patch file
```


版权所有 © 华为技术有限公司

```
  0. return

Enter your choice(0-5):0
      Main Menu

  1. Default startup
  2. Serial submenu
  3. Ethernet submenu
  4. Startup parameters submenu
  5. File system submenu
  6. Password manager submenu
  0. Reboot

Enter your choice(0-6):5
      File system submenu

  1. Flash file system
  0. Return

Enter your choice(0-1):1
      Flash file system

  1. List file
  2. Rename file
  3. Delete file
  4. Format flash
  5. Upload file to server
  6. Download file from server
  0. Return

Enter your choice(0-6):2
Please input the file name: vrpcfg.cfg
Please input the new name: vrpcfg_cpy.cfg
Rename file[flash:/vrpcfg.cfg] to [flash:/vrpcfg_cpy.cfg], Yes or No(Y/N): y
 file rename OK!
```

c. 启动设备。

```
      Flash file system

  1. List file
  2. Rename file
  3. Delete file
  4. Format flash
  5. Upload file to server
  6. Download file from server
  0. Return

Enter your choice(0-6):0
      File system submenu

  1. Flash file system
  0. Return

Enter your choice(0-1):0
      Main Menu

  1. Default startup
  2. Serial submenu
  3. Ethernet submenu
  4. Startup parameters submenu
  5. File system submenu
  6. Password manager submenu
  0. Reboot

Enter your choice(0-6):1
```

d. 停止Auto-Config。

```
Please configure the login password (<8-128>)    //  设置首次Console登录密码
Enter Password:
Confirm Password:
```

 版权所有 © 华为技术有限公司

```
<Huawei> Auto-Config is working. Before configuring the device, stop Auto-Config.
 If you perform configurations when Auto-Config is running, the DHCP, routing, DNS,
 and VTY configurations will be lost. Do you want to stop Auto-Config? [y/n]:y
<Huawei>
```

e. 将重命名的配置文件改为可执行文件。根据文件格式，选择其中一种。

```
<Huawei>rename vrpcfg_cpy.cfg vrpcfg_cpy.bat   // 当文件是cfg结尾的时候，需要重命名为以bat结尾的可执行文件
Rename flash:/vrpcfg_cpy.cfg to flash:/vrpcfg_cpy.bat? (y/n)[n]:y
Info: Rename file flash:/vrpcfg_cpy.cfg to flash:/vrpcfg_cpy.bat .....Done
<Huawei>unzip vrpcfg_cpy.zip vrpcfg_cpy.bat   // 当文件是zip结尾的时候，需要解压为以bat结尾的可执行文件
Extract flash:/vrpcfg_cpy.zip to flash:/vrpcfg_cpy.bat? (y/n)[n]:y

100%  complete
%Decompressed file flash:/vrpcfg_cpy.zip flash:/vrpcfg_cpy.bat.
```

f. 恢复配置。

```
[Huawei]execute vrpcfg_cpy.bat
Information：The script file has been executed completely.
```

g. 重新设置Console口密码和Telnet密码，并记录好设置的密码。执行“save”命令保存配置。

2. 选择第6项，进入Password Manager菜单。

```
    Main Menu

  1. Default startup
  2. Serial submenu
  3. Ethernet submenu
  4. Startup parameters submenu
  5. File system submenu
  6. Password manager submenu
  0. Reboot

Enter your choice(0-6):6
```

a. 选择第2项，清除Console登录密码。

```
      Password manager submenu

  1. Modify bootloader password
  2. Clear the console login password
  3. Reset bootloader password
  0. Return

Enter your choice(0-3):2
Caution: A new console password must be set after the restart.Continue now? Yes(
y) or No(n):y
Clear password for console user successfully.

      Password manager submenu

  1. Modify bootloader password
  2. Clear the console login password
  3. Reset bootloader password
  0. Return

Enter your choice(0-3):
```

b. 选择第1项，继续启动，即可登录设备重新配置Telnet密码，并记录好设置的密码。执行“save”命令保存配置。

说明

根据需要配置Console用户界面的认证方式及新密码是必要步骤，否则设备重启后通过Console口登录时依然需要通过老密码认证。

```
    Main Menu

  1. Default startup
  2. Serial submenu
```

```
  3. Ethernet submenu
  4. Startup parameters submenu
  5. File system submenu
  6. Password manager submenu
  0. Reboot

Enter your choice(0-6):1
```

----结束

配置注意事项

执行步骤时，请保持串口用户在线，防止串口用户中途退出。

2.4.2 配置通过 BootLoader 修改文件名的示例

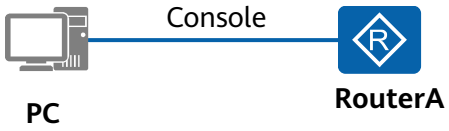
规格

适用于所有版本、所有形态的AR路由器。

组网需求

RouterA的Console口与用户侧主机PC相连。要求进入BootLoader菜单修改文件名。

图 2-26 通过 BootLoader 菜单修改文件名组网图



操作步骤

步骤1 用串口线连接并通过Console口登录设备。

步骤2 重启设备，在设备出现“Press Ctrl+B to break auto startup ...”打印信息时，按下“Ctrl+B”并键入密码后进入BootLoader主菜单。

```
Press Ctrl+B to break auto startup ... 3
BootLoader management port is GE 0/0/8.

Enter Password:
```

步骤3 进入BootLoader菜单后，选择第5项，进入File system submenu菜单。

```
    Main Menu

  1. Default startup
  2. Serial submenu
  3. Ethernet submenu
  4. Startup parameters submenu
  5. File system submenu
  6. Password manager submenu
  0. Reboot

Enter your choice(0-6):5
```

步骤4 进入File system submenu菜单后，根据文件所在的存储卡选择。

版权所有 © 华为技术有限公司

```
      File system submenu

  1. Flash file system
  0. Return

Enter your choice(0-1):1
```

步骤5 查看存储卡上的所有文件。

```
      Flash file system

  1. List file
  2. Rename file
  3. Delete file
  4. Format flash
  5. Upload file to server
  6. Download file from server
  0. Return

Enter your choice(0-6):1
 Files in Directory of flash :
total
drwxrwxrwx          224    Aug 29   2018 $_user
drwxr-xr-x          488    Aug 29   2018 .overlay
drwxr-xr-x          224    Sep  2  08:45 .work
-rwxr-xr-x         3283    Aug 28  06:19 124-AR651UA4.cfg
-rw-r--r--    190592512    Aug  2  08:03 software.cc
drwxr-xr-x          328    Sep  2  08:45 appm
-rwxr-xr-x    148282624    Jul 30  02:27 asoftware1.cc

 Total:   909 MB, Used:   482 MB, Free:   427 MB ( 47%)
```

步骤6 修改文件名为新的文件名。

```
      Flash file system

  1. List file
  2. Rename file
  3. Delete file
  4. Format flash
  5. Upload file to server
  6. Download file from server
  0. Return

Enter your choice(0-6):2
Please input the file name: software.cc
Please input the new name: softwarenew.cc
Rename file[flash:/software.cc] to [flash:/softwarenew.cc], Yes or No(Y/N): y
 file rename OK!
```

步骤7 重新查看存储卡上的文件。

```
      Flash file system

  1. List file
  2. Rename file
  3. Delete file
  4. Format flash
  5. Upload file to server
  6. Download file from server
  0. Return

Enter your choice(0-6):1
 Files in Directory of flash :
total
drwxrwxrwx          224    Aug 29   2018 $_user
drwxr-xr-x          488    Aug 29   2018 .overlay
drwxr-xr-x          224    Sep  2  08:45 .work
-rwxr-xr-x         3283    Aug 28  06:19 124-AR651UA4.cfg
-rw-r--r--    190592512    Aug  2  08:03 softwarenew.cc
drwxr-xr-x          328    Sep  2  08:45 appm
-rwxr-xr-x    148282624    Jul 30  02:27 asoftware1.cc
```

 版权所有 © 华为技术有限公司

```
Total:   909 MB, Used:   482 MB, Free:   427 MB ( 47%)
```

可以看到文件已经被重新命名成功。

步骤8 设置修改后的大包为启动大包。

```
      Flash file system

  1. List file
  2. Rename file
  3. Delete file
  4. Format flash
  5. Upload file to server
  6. Download file from server
  0. Return

Enter your choice(0-6):0
      File system submenu

  1. Flash file system
  0. Return

Enter your choice(0-1):0
      Main Menu

  1. Default startup
  2. Serial submenu
  3. Ethernet submenu
  4. Startup parameters submenu
  5. File system submenu
  6. Password manager submenu
  0. Reboot

Enter your choice(0-6):4
      Startup parameters submenu

  1. Display current startup configuration
  2. Modify the startup file
  3. Modify the configuration file
  4. Modify the patch file

  0. Return

Enter your choice(0-5):2
      Modify the startup file

  1. flash
  0. Return

Enter your choice(0-1):1
NOTE: Boot file must be .cc or .CC

Current boot file: flash:/software.cc
Press ENTER directly for no change.
Or, please input the new file name: flash:/softwarenew.cc ? Yes or No(Y/N)y
Save load state word...OK!
```

----结束

配置注意事项

- 不建议在BootLoader菜单操作，若特别必要，可联系技术支持人员指导操作。
- 执行步骤时，请保持串口用户在线，防止串口用户中途退出。
- 尽量不要修改启动大包的文件名，否则会导致系统启动不起来，如想修改，则修改完毕后，把修改后的大包设置成下次启动大包。

 版权所有 © 华为技术有限公司

- 尽量不要修改启动配置文件的文件名，否则会导致系统的配置丢失，如想修改，则修改完毕后，把修改后的配置文件设置成下次启动配置文件。

2.4.3 配置通过 BootLoader 修改 BootLoader 密码的示例

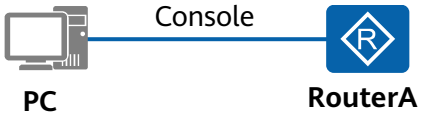
规格

适用于所有版本、所有形态的AR路由器。

组网需求

RouterA的管理网口与用户侧主机PC相连。要求进入BootLoader菜单修改BootLoader的密码。

图 2-27 通过 BootLoader 菜单修改 BootLoader 的密码组网图



操作步骤

步骤1 用串口线连接并通过Console口登录设备。

步骤2 重启设备，在设备出现“Press Ctrl+B to break auto startup ...”打印信息时，按下“Ctrl+B”并键入密码后进入BootLoader主菜单。

```
Press Ctrl+B to break auto startup ... 3
BootLoader management port is GE 0/0/8.

Enter Password:
```

步骤3 进入BootLoader菜单后，选择第6项，进入Password manager submenu菜单。

```
    Main Menu

  1. Default startup
  2. Serial submenu
  3. Ethernet submenu
  4. Startup parameters submenu
  5. File system submenu
  6. Password manager submenu
  0. Reboot

Enter your choice(0-6):6
```

步骤4 选择第1项，修改密码。

```
    Password manager submenu

  1. Modify bootloader password
  2. Clear the console login password
  3. Reset bootloader password
  0. Return

Enter your choice(0-3):1
Modify password. the password length must >= 6.Press Ctrl+c to break.
Old password:************
```

 版权所有 © 华为技术有限公司

```
New password:************
New password again:************
Are you sure to change password? [y/n]:y
Save new password Success.
```

----结束

配置注意事项

- 不建议在BootLoader菜单操作，若特别必要，可联系技术支持人员指导操作。
- 执行步骤时，请保持串口用户在线，防止串口用户中途退出。
- 修改密码后请做好记录妥善保管。

2.5 设备管理

2.5.1 配置向日志主机输出日志信息的示例

规格

适用于所有版本、所有形态的AR路由器。

组网需求

当设备出现异常或故障时，用户需要及时准确地收集设备运行过程中的运行信息。用户希望通过Router将日志信息发送到日志主机，实现对日志的收集功能，通过查询日志信息，了解设备的运行情况，方便监控设备的运行状态和进行故障定位。具体需求为Router通过接口Eth1/0/0接入IP网络，Router和日志主机之间路由可达，Router将日志信息发送到日志主机。

图 2-28 向日志主机输出日志信息组网图

操作步骤

步骤1 Router的配置

```
#
 sysname Router
#
interface Ethernet1/0/0
 ip address 11.1.1.1 255.255.255.0  //配置Router的接口IP地址
#
 info-center channel 6 name loghost1  //配置通道6的名称为loghost1
 info-center source IP channel 6 log level warning  //配置信息通道6允许输出IP模块的日志信息，允许输出的日志级别最低为warning
 info-center loghost source Ethernet1/0/0  //配置发送日志信息的源接口
 info-center loghost 10.1.1.1 channel 6  //配置日志信息输出到日志主机
#
ip route-static 10.1.1.1 255.255.255.255 Ethernet1/0/0 11.1.1.2  //配置静态路由，保证Router与日志主机之间路由可达
```


版权所有 © 华为技术有限公司

```
#
return
```

步骤2 配置日志主机（略）

日志主机可以是安装UNIX或LINUX操作系统的主机，也可以是安装第三方日志软件的主机。

步骤3 验证配置结果

在Router上执行**display info-center**查看配置的日志主机。其中，“Log host:”字段中的“channel name:”为**loghost1**。

----结束

配置注意事项

- 配置了信息通道级别（warning），只有高于或等于此信息级别的日志信息才会被输出，低于此级别的日志信息将会被过滤。

2.5.2 配置向日志文件输出日志信息的示例

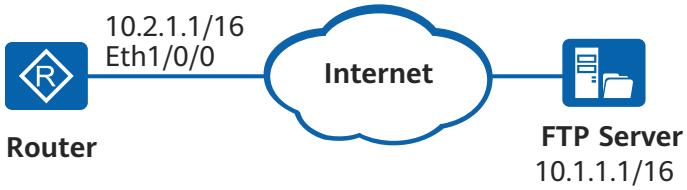
规格

适用于所有版本、所有形态的AR路由器。

组网需求

信息中心将指定级别的Log信息输出到日志文件中，网络维护人员将日志文件上传到FTP服务器上，通过查询日志信息，了解设备的运行情况。当设备出现故障时，进行故障定位。具体需求为Router通过接口Eth1/0/0接入Internet，Router和FTP Server之间路由可达。网络维护人员可以在FTP Server上查看Router上产生的日志文件。

图 2-29 向日志文件输出日志信息组网图



操作步骤

步骤1 Router的配置

```
#
 sysname Router
#
 info-center source IP channel 9 log level warning  //配置信息通道9允许输出IP模块的日志信息，允许输出的日志级别最低为warning
#
interface Ethernet1/0/0
 ip address 10.2.1.1 255.255.0.0  //配置Router的接口IP地址
#
ip route-static 10.1.0.0 255.255.0.0 Ethernet1/0/0 10.2.1.2  //配置静态路由，保证Router与FTP Server之间路由可达
```

 版权所有 © 华为技术有限公司

```
#
return
```

步骤2 配置日志文件传输到FTP Server

配置登录到FTP Server。

```
<Router> ftp 10.1.1.1
Trying 10.1.1.1 ...
Press CTRL+K to abort
Connected to 10.1.1.1.
220 FTP Server ready.
User(192.168.1.100:(none)):huawei
331 Password required for 1.
Enter password:
230 User 1 logged in.
```

将设备生成的日志文件传输到FTP Server（存储器以U盘为例）。

```
[Router-ftp] put usb1:/logfile/log.log
200 Port command successful.
150 Opening data connection for log.log
226 File received ok
FTP: 2761463 byte(s) sent in 26.062 second(s) 105.95Kbyte(s)/sec.
[Router-ftp] quit
```

步骤3 验证配置结果

配置完成后，用户可以在FTP Server上查看log.log文件里面的日志信息。

----结束

配置注意事项

- 缺省情况下，设备向日志文件输出信息使用9号通道。执行命令**info-center logfile channel** { *channel-number* | *channel-name* }，可以更改日志信息输出到日志文件所使用的通道。
- 缺省情况下，日志文件保存的路径为存储介质:/logfile（执行命令**info-center logfile path** *path*，可以更改日志文件的保存路径）。存储介质根据设备显示选择。缺省情况下，日志文件的存储介质按照rom、hdd0、hdd1、hdd2、hdd3、usb0、usb1和flash的优先级顺序进行选择。
- 缺省情况下，日志文件的大小为8M。执行命令**info-center logfile size** *size*，可以配置日志文件的大小。如果设备生成的日志文件超过所配置的大小，系统会自动将日志文件按照标准zip格式压缩成压缩文件。也可以通过执行命令**save logfile**手动保存信息到日志文件。
- 缺省情况下，日志文件的最大保存个数为200。执行命令**info-center max-logfile-number** *filenumbers*，可以配置日志文件的最大保存个数。如果产生的日志文件超过最大个数，系统将删除日期较老的日志文件，保持日志文件个数小于等于所配置的值。

 版权所有 © 华为技术有限公司

3 访问 Internet 外网

3.1 NAT
3.2 双出口

3.1 NAT

3.1.1 配置内网用户通过 Easy IP 方式访问 Internet 外网的示例

规格

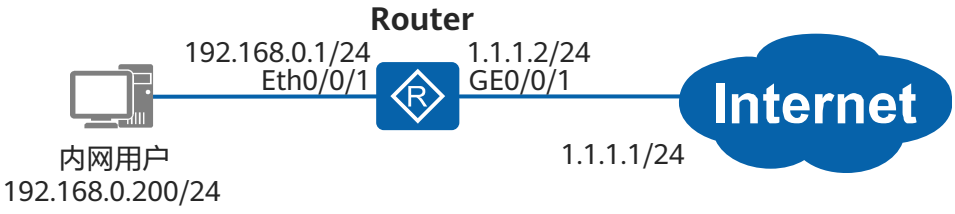
适用于所有版本、所有形态的AR路由器。

组网需求

企业内网用户需要访问外网时，可以通过配置NAT，将IP数据报文头中的内网IP地址转换为外网IP地址，实现内部网络访问外部网络的功能。当用户拥有的外网IP地址个数较少时，配置了NAT设备出接口的IP地址和其他应用之后，没有可用的空闲外网IP地址，此时可以选择Easy IP方式的动态NAT，实现内网主机访问外网的功能。Easy IP方式直接使用出接口的IP地址作为内网主机转换后的外网IP地址，无需额外的外网IP地址。

如图3-1所示，Router的出接口GE0/0/1的IP地址为1.1.1.2/24，接口Eth0/0/1的IP地址为192.168.0.1/24。连接Router出接口GE0/0/1的对端IP地址为1.1.1.1/24。通过在Router上配置Easy IP方式的动态NAT，可以实现内网主机访问外网服务器功能，并且限制IP地址为192.168.0.3的用户访问外网。

图 3-1 配置出接口做 EASY IP 组网图



版权所有 © 华为技术有限公司

操作步骤

步骤1 Router的配置

```
#
 sysname Router  //修改设备名称
#
acl number 2000
 rule 5 deny source 192.168.0.3 0  //配置拒绝访问外网的地址192.168.0.3
 rule 6 permit source 192.168.0.0 0.0.0.255  //配置允许进行NAT转换的内网地址段192.168.0.0/24
#
interface Ethernet0/0/1
 undo portswhich
 ip address 192.168.0.1 255.255.255.0  //配置内网网关地址
#
interface GigabitEthernet0/0/1
 ip address 1.1.1.2 255.255.255.0
 nat outbound 2000  //在出接口GE0/0/1上做Easy IP 方式的NAT
#
ip route-static 0.0.0.0 0.0.0.0 1.1.1.1  //配置默认路由，保证出接口到对端路由可达
#
```

步骤2 检查配置结果

在Router上执行**display nat outbound**命令查看出接口的Easy IP配置信息。

----结束

配置注意事项

- 配置ACL，确定对哪些网段进行NAT转换。
- 在出接口视图下配置NAT转换，注意转换方向。

相关资料

视频：**上网基本配置**

3.1.2 配置内网用户通过 NAT 地址池方式访问 Internet 外网的示例

规格

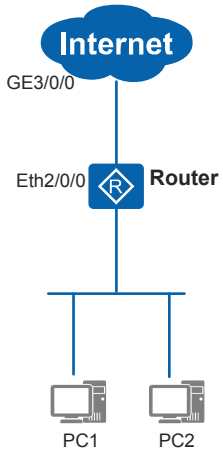
适用于所有版本、所有形态的AR路由器。

组网需求

如**图3-2**所示，某企业的内网用户通过路由器和Internet相连，且均有访问外网Internet的需求。内网用户希望使用外网地址池中（2.2.2.100～2.2.2.200）的地址和公司内部主机的地址（网段为192.168.20.0/24）进行一对一转换后，访问Internet。

 版权所有 © 华为技术有限公司

图 3-2 配置通过 NAT 地址池方式访问 Internet



版权所有 © 华为技术有限公司

操作步骤

步骤1 配置Router

```
#
 sysname Router
#
 vlan batch 100
#
acl number 2000    //配置允许进行NAT转换的内网地址段
 rule 5 permit source 192.168.20.0 0.0.0.255
#
 nat address-group 1 2.2.2.100 2.2.2.200  //配置NAT地址池
#
interface Vlanif100    //配置内网网关的IP地址
 ip address 192.168.20.1 255.255.255.0
#
interface Ethernet2/0/0
 port link-type access
 port default vlan 100
#
interface GigabitEthernet3/0/0
 ip address 2.2.2.1 255.255.255.0
 nat outbound 2000 address-group 1    //在出接口上配置NAT Outbound
#
 ip route-static 0.0.0.0 0.0.0.0 2.2.2.2    //配置默认路由
#
return
```

步骤2 验证配置结果

执行命令**display nat session**，查看设备上的NAT映射表项。

内网用户可以通过路由器的NAT地址池方式来访问Internet。

----结束

相关资料

视频：配置NAT Outbound

3.1.3 配置通过 NAT 访问 Internet 外网，并对外提供 www 服务的示例

规格

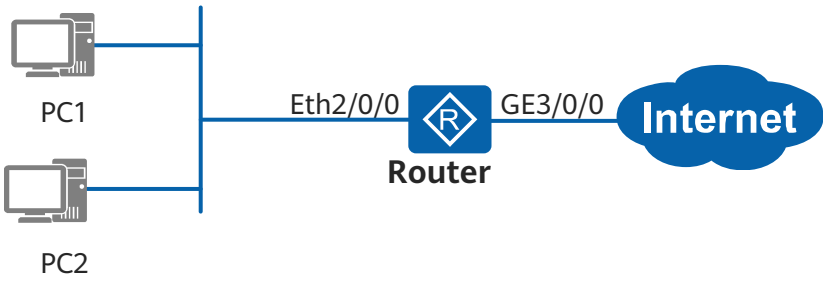
适用于所有版本、所有形态的AR路由器。

组网需求

如图3-3所示，内网用户通过路由器的NAT地址转换功能来访问Internet，并且向外网用户提供www服务。

 版权所有 © 华为技术有限公司

图 3-3 配置通过 NAT 对外提供 www 服务



操作步骤

步骤1 配置Router

```
#
 vlan batch 100
#
acl number 2000    //配置允许进行NAT转换的内网地址段
 rule 5 permit source 192.168.20.0 0.0.0.255
#
interface vlanif100    //配置内网网关的IP地址
 ip address 192.168.20.1 255.255.255.0
#
interface Ethernet2/0/0
 port link-type access
 port default vlan 100
#
interface GigabitEthernet3/0/0
 ip address 2.2.2.1 255.255.255.0
 nat outbound 2000 address-group 1    //在出接口上配置NAT Outbound
 nat static protocol tcp global 2.2.2.103 www inside 192.168.20.2 8080  //在出接口上配置内网服务器
192.168.20.2的www服务
#
 nat address-group 1 2.2.2.100 2.2.2.200    //配置NAT地址池
#
 ip route-static 0.0.0.0 0.0.0.0 2.2.2.2    //配置默认路由
```

步骤2 验证配置结果

执行命令**display nat outbound**，查看NAT Outbound的配置信息。

执行命令**display nat static**，查看NAT Static配置信息。

外网用户能正常使用内网的WWW服务。

----结束

相关资料

视频：配置NAT Outbound

版权所有 © 华为技术有限公司

3.1.4 配置 VPN 用户通过 NAT 方式访问 Internet 外网的示例

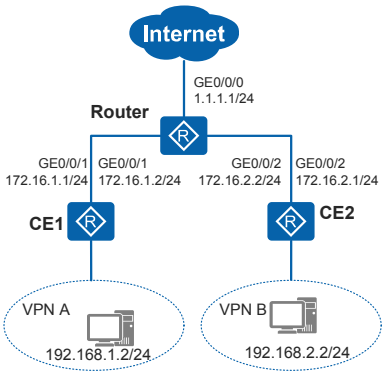
规格

适用于所有版本、所有形态的AR路由器。

组网需求

如图3-4所示，某企业为了降低通信成本，在内部建立了多个VPN用户，且均有访问外网Internet的需求。现在通过将内网VPN用户的访问控制列表ACL和NAT地址池关联，进行地址转换，从而实现内网VPN用户访问外网的需求。其中，企业网的出接口GE0/0/0的对端IP地址为1.1.1.2/24。

图 3-4 NAT 多实例组网图



操作步骤

步骤1 Router的配置

```
#
ip vpn-instance vpna  //配置VPN实例vpna
 ipv4-family
  route-distinguisher 100:1
  vpn-target 111:1 export-extcommunity
  vpn-target 111:1 import-extcommunity
#
ip vpn-instance vpnb  //配置VPN实例vpnb
 ipv4-family
  route-distinguisher 100:2
```


版权所有 © 华为技术有限公司

```
 vpn-target 222:2 export-extcommunity
 vpn-target 222:2 import-extcommunity
#
acl number 2000  //配置nat outbound的acl 2000
 rule 5 permit vpn-instance vpna source 192.168.1.0 0.0.0.255
 rule 10 permit vpn-instance vpnb source 192.168.2.0 0.0.0.255
#
interface GigabitEthernet0/0/0  //配置Router的出接口
 ip address 1.1.1.1 255.255.255.0
 nat outbound 2000
#
interface GigabitEthernet0/0/1  //连接vpna的接口
 ip binding vpn-instance vpna
 ip address 172.16.1.1 255.255.255.0
#
interface GigabitEthernet0/0/2  //连接vpnb的接口
 ip binding vpn-instance vpnb
 ip address 172.16.2.1 255.255.255.0
#
ip route-static 192.168.1.0 255.255.255.0 vpn-instance vpna 172.16.1.2  //配置Internet到vpna的主机的路由，下一跳为CE1
ip route-static 192.168.2.0 255.255.255.0 vpn-instance vpnb 172.16.2.2  //配置Internet到vpnb的主机的路由，下一跳为CE2
ip route-static vpn-instance vpna 0.0.0.0 0.0.0.0 1.1.1.2 public  //配置vpna到Internet的默认路由
ip route-static vpn-instance vpnb 0.0.0.0 0.0.0.0 1.1.1.2 public  //配置vpnb到Internet的默认路由
#
```

步骤2 验证配置结果

分别在vpna和vpnb的主机上**ping 1.1.1.2**，如果ping通则NAT多实例配置成功。

----结束

配置注意事项

- 配置NAT的ACL时必须要指定VPN实例。
- 配置VPN实例到公网的路由，也需要配置从公网到VPN实例的路由。
- 配置示例没有给出CE设备的配置，请用户根据实际情况自行配置。

3.1.5 配置通过 NAT Static 和 NAT Outbound 实现公网用户与公网服务器间互访的示例

规格

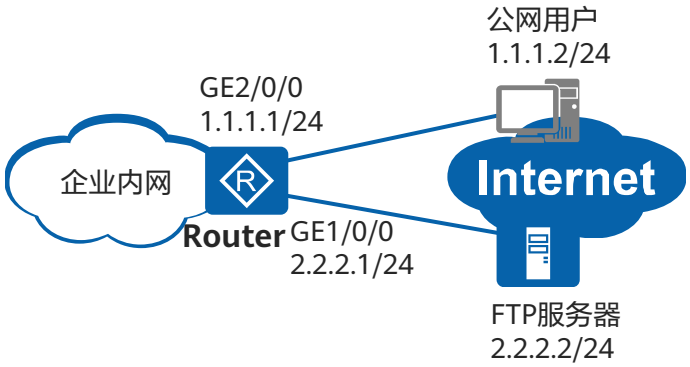
适用于所有版本、所有形态的AR路由器。

组网需求

如图3-5所示，企业在Internet部署了一台FTP服务器，Router作为企业出口网关。出于安全考虑，企业希望公网用户和FTP服务器之间的业务流量经过Router转发，且公网用户和公网服务器的IP地址彼此不感知。

 版权所有 © 华为技术有限公司

图 3-5 配置通过 NAT Static 和 NAT Outbound 实现公网 PC 与公网服务器间的互访组网图



操作步骤

步骤1 Router的配置

```
#
 sysname Router
#
acl number 2000
 rule 5 permit source any
#
interface GigabitEthernet1/0/0
 ip address 2.2.2.1 255.255.255.0
 nat outbound 2000  //配置NAT Outbound，对FTP服务器隐藏外网用户的真实IP地址，以接口GE1/0/0的IP地址体现
#
interface GigabitEthernet2/0/0
 ip address 1.1.1.1 255.255.255.0
 nat static global current-interface inside 2.2.2.2 //配置NAT Static，对外网用户隐藏FTP服务器的真实IP地址，以接口GE2/0/0的IP地址体现
#
return
```

步骤2 检查配置结果

在Router上执行**display nat outbound**操作，结果如下。

```
<Router> display nat outbound
 NAT Outbound Information:
 ----------------------------------------------------------------------
 Interface                 Acl     Address-group/IP/Interface      Type
 GigabitEthernet1/0/0      2000                  2.2.2.1     easyip
 ----------------------------------------------------------------------
  Total : 1
```

在Router上执行**display nat static**操作，结果如下。

```
<Router> display nat static
  Static Nat Information:
  Interface  : GigabitEthernet2/0/0
    Global IP/Port     : current-interface/---- (Real IP : 1.1.1.1)
    Inside IP/Port     : 2.2.2.2/----
    Protocol : ----
    VPN instance-name  : ----
    Acl number         : ----
    Vrrp id            : ----
    Netmask  : 255.255.255.255
    Description : ----
```


版权所有 © 华为技术有限公司

```
Total :   1
```

----结束

3.1.6 配置通过 NAT 和重定向实现双出口，且对外提供 web 服务的示例

规格

适用于所有版本、所有形态的AR路由器。

组网需求

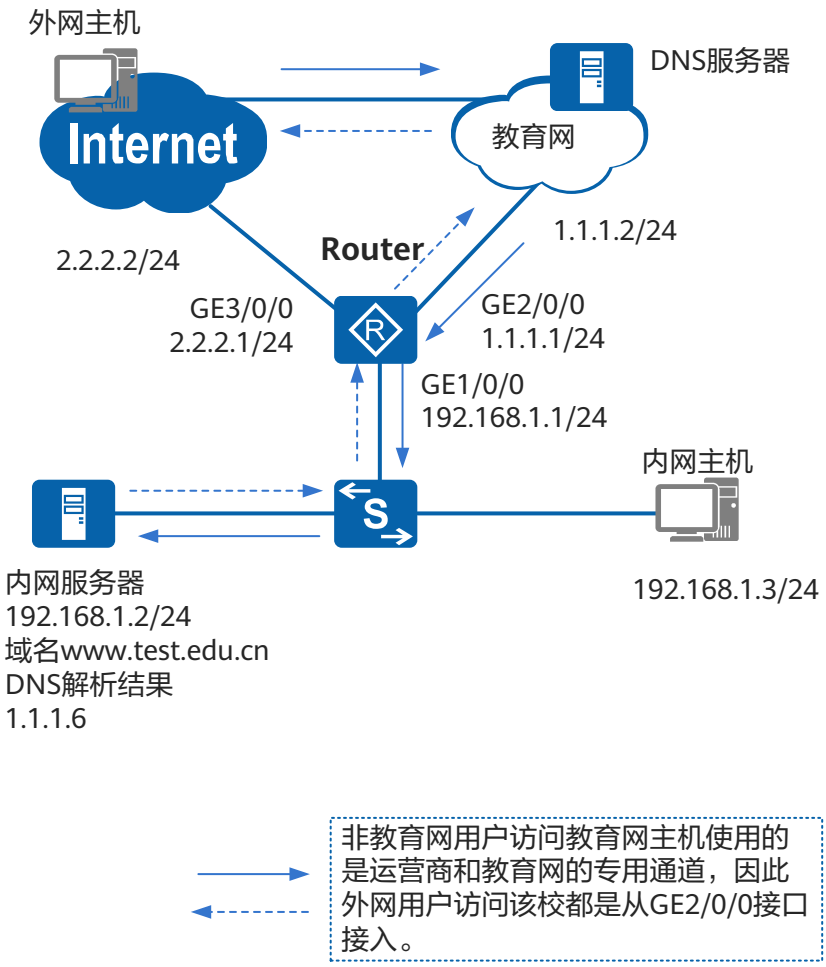
如**图3-6**所示，Router的GE1/0/0连接校园网，GE2/0/0连接教育网，GE3/0/0连接Internet。内网主机访问教育网通过GE2/0/0出去，其他访问通过缺省路由从GE3/0/0出去。

该校园网服务器提供内外网web服务，内网地址是192.168.1.2/24，其域名是www.test.edu.cn，外网地址是1.1.1.6。现要求外网主机和校园网内部主机都可以通过域名或1.1.1.6正常访问服务器，且要求校园网内部主机可以通过NAT任意访问Internet和教育网。其中，GE2/0/0的对端IP地址是1.1.1.2/24，GE3/0/0的对端IP地址是2.2.2.2/24。

根据网络规划，非教育网主机访问教育网主机，必须通过教育网专用通道访问，因此外网用户（包括教育网用户和非教育网用户）访问该校都是从GE2/0/0接入。并且，源地址为教育网地址（如1.1.1.6/24）的报文如果从GE3/0/0出去，会被运营商屏蔽。

版权所有 © 华为技术有限公司

图 3-6 配置双出口 NAT 示例组网图



操作步骤

步骤1 Router的配置

```
#
acl number 2000  //配置ACL规则，允许校园网中192.168.1.0/24网段的主机访问外网。
 rule 5 permit source 192.168.1.0 0.0.0.255
#
acl number 3000  //用于内部主机直接使用1.1.1.6访问服务器，只有内网发起的服务才会在GE1/0/0上进行NAT
 rule 5 permit ip source 192.168.1.0 0.0.0.255 destination 1.1.1.6 0
#
acl number 3001  //内部服务器返回内部主机的数据流不需被重定向到教育网出口
 rule 5 permit ip source 192.168.1.2 0 destination 192.168.1.0 0.0.0.255
#
acl number 3003  //用于将内部服务器发往外部的数据流重定向到教育网出口
 rule 10 permit ip source 192.168.1.2 0
#
traffic classifier permitover operator or  //定义不用重定向的数据流分类
 if-match acl 3001
traffic classifier redirectover operator or  //定义需要重定向的数据流分类
 if-match acl 3003
#
traffic behavior permitover  //定义permitover的流行为为permit
traffic behavior redirectover  //定义redirectover的流行为为redirect
 redirect ip-nexthop 1.1.1.2  //服务器响应外网访问的数据流都被重定向到教育网出口
```


版权所有 © 华为技术有限公司

```
#
traffic policy redirect  //绑定流策略
 classifier permitover behavior permitover precedence 5 //先匹配是否是内部服务器返回内部主机的数据流
 classifier redirectover behavior redirectover precedence 10 //后匹配重定向到教育网出口的数据流
#
 nat alg dns enable  //使能NAT alg的DNS功能
 #
 nat dns-map www.test.edu.cn 1.1.1.6 80 tcp  //配置dns-map，将DNS的解析结果转换成内网服务器地址
 #
 nat address-group 0 2.2.2.50 2.2.2.100  //访问非教育网地址时NAT用
 nat address-group 1 1.1.1.50 1.1.1.100  //访问教育网地址时NAT用
#
interface GigabitEthernet1/0/0
 ip address 192.168.1.1 255.255.255.0
 traffic-policy redirect inbound  //GE1/0/0对入方向的数据流执行流策略redirect
 nat static global 1.1.1.6 inside 192.168.1.2 netmask 255.255.255.255  //内网用户直接使用1.1.1.6访问服务器时进行NAT
 nat outbound 3000  //内网用户直接访问1.1.1.6时做Easy IP，将源地址改为GE1/0/0的地址,保证内网服务器和主机间的交互都经过Router转发
#
interface GigabitEthernet2/0/0
 ip address 1.1.1.1 255.255.255.0
 nat static global 1.1.1.6 inside 192.168.1.2 netmask 255.255.255.255  //教育网出口的NAT
 nat outbound 2000 address-group 1  //内网访问教育网时的NAT
#
interface GigabitEthernet3/0/0
 ip address 2.2.2.1 255.255.255.0
 nat outbound 2000 address-group 0  //内网访问非教育网时的NAT
#
ip route-static 0.0.0.0 0.0.0.0 2.2.2.2  //缺省路由
#
return
```

步骤2 验证配置结果

1. 教育网用户和非教育网用户可以通过域名www.test.endu.cn或1.1.1.6正常访问校园服务器。
2. 内网用户可以通过域名www.test.endu.cn或1.1.1.6正常访问校园服务器。
3. 内网用户可以正常访问外网。

----结束

配置注意事项

- 配置策略路由，保证内网服务器返回外网的流量都从教育网出口出去。如果从非教育网出口出去，会被运营商屏蔽。
- 注意策略路由流行为的先后顺序，先匹配是否是服务器响应内网的数据流，如果是则不进行重定向，否则将服务器响应的数据流重定向到教育网出口。
- 根据校内服务器提供的服务，选择正确的NAT alg。本例因为提供的是普通的web服务，所以只使能了alg的dns功能，以便内网主机可以正常的进行域名访问。
- 本例在下行接口GE1/0/0上应用NAT Static和NAT Outbound的作用是为了让内网用户可以直接使用1.1.1.6访问内网服务器。

  在内网直接使用服务器的外网地址访问，需要Router将地址转换成服务器的内网地址，即<192.168.1.3,1.1.1.6>变成<192.168.1.3,192.168.1.2>，然后发送给内网服务器。在服务器响应HTTP请求时，如果不做任何处理会直接将报文发送给192.168.1.3，内网主机收不到来自1.1.1.6的HTTP响应，因此打开网页失败。所以，内网服务器的响应报文必须经过Router转换成1.1.1.6后返回内网主机，才能实现正常访问。在GE1/0/0上应用Easy IP方式的NAT是为了将内网主机的访问报文的源地址变成GE1/0/0的接口地址，即<192.168.1.3,192.168.1.2>变成<192.168.1.1,192.168.1.2>，再将报文转发给内网服务器。内网服务器的响应报文

 版权所有 © 华为技术有限公司

会将GE1/0/0的地址作为目的地址发送给Router，即<192.168.1.2,192.168.1.1>，然后Router会查找NAT映射表，将源地址和目的地址变成对应的服务器外网地址和内网主机地址，即<1.1.1.6,192.168.1.3>。这样内网主机就会收到1.1.1.6发送的HTTP响应报文，实现使用1.1.1.6直接访问内网服务器。

- 绑定流策略redirect时，应该绑定permitover再绑定redirectover。对校园网服务器发往内部主机的数据流不能进行重定向，而发往校园网外部的数据流需重定向到GE2/0/0接口。

3.1.7 配置内网用户通过 NAT 访问地址重叠的外网服务器

规格

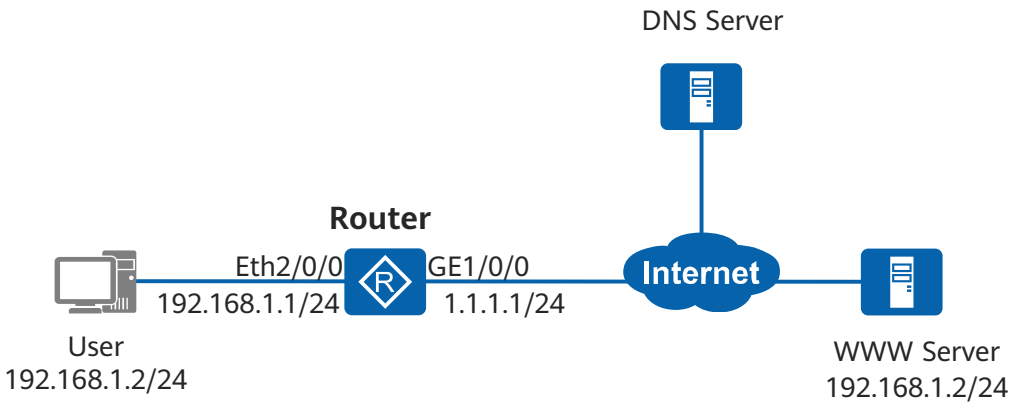
适用于所有版本、所有形态的AR路由器。

组网需求

如图3-7所示，Router作为某公司的网关，内网网段和外网WWW Server所在网段地址重叠。该公司拥有1.1.1.13和1.1.1.14两个公网地址。

现要求内网用户能够通过域名访问WWW Server。

图 3-7 配置内网用户通过 NAT 访问地址重叠的外网服务器示例组网图



操作步骤

步骤1 Router的配置

```
#
acl number 2001
 rule 5 permit ip source 192.168.1.0 0.0.0.255              //仅允许指定网段内的用户能够访问外网
#
 nat alg dns enable                    //使能DNS协议的NAT ALG功能
 #
 nat address-group 1 1.1.1.13 1.1.1.14              //配置NAT地址池
 #
 nat overlap-address 0 192.168.1.2 2.2.2.100 pool-length 10          //配置重叠地址池到临时地址池的映射关系
#
interface Ethernet2/0/0
 ip address 192.168.1.1 255.255.255.0
#
```


版权所有 © 华为技术有限公司

```
interface GigabitEthernet1/0/0
 ip address 1.1.1.1 255.255.255.0
 nat outbound 2001 address-group 1                //在出接口上配置NAT Outbound
#
ip route-static 0.0.0.0 0.0.0.0 1.1.1.2        //配置静态路由，保证内网到外网报文的下一跳地址是1.1.1.2
#
return
```

步骤2 验证配置结果

执行命令**display nat overlap-address all**查看重叠地址池映射关系。

执行命令**display nat outbound**查看NAT Outbound信息。

----结束

3.1.8 配置 NAT 实现对源和目的 IP 地址同时进行转换

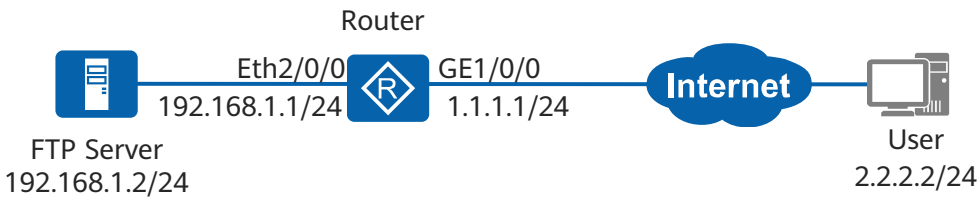
规格

适用于所有版本、所有形态的AR路由器。

组网需求

如图3-8所示，Router作为某公司的网关，FTP Server为内网服务器。现要求外网用户能够访问内网FTP Server服务器，同时对外网IP地址进行转换实现内网无需引入外网的路由。

图 3-8 配置 NAT 实现对源和目的 IP 地址同时进行转换示例组网图



操作步骤

步骤1 Router的配置

```
#
acl number 3000
 rule 5 permit ip source 2.2.2.0 0.0.0.255      //仅允许指定网段内的用户能够访问内网服务器
#
 nat alg ftp enable                    //使能FTP协议的NAT ALG功能
#
interface Ethernet2/0/0
 ip address 192.168.1.1 255.255.255.0
 nat outbound 3000                  //配置NAT Outbound功能，对外网用户访问内网的源IP地址进行转换，保证内网无需引入外网的路由
#
interface GigabitEthernet1/0/0
 ip address 1.1.1.1 255.255.255.0
 nat server protocol tcp global 1.1.1.3 ftp inside 192.168.1.2 ftp      //在出接口上配置NAT Server，使外网用户能够访问内网服务器
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.2        //配置静态路由，保证内网到外网报文的下一跳地址是1.1.1.2
```

 版权所有 © 华为技术有限公司

```
#
return
```

步骤2 验证配置结果

执行命令**display nat server**查看NAT Server信息。

执行命令**display nat outbound**查看NAT Outbound信息。

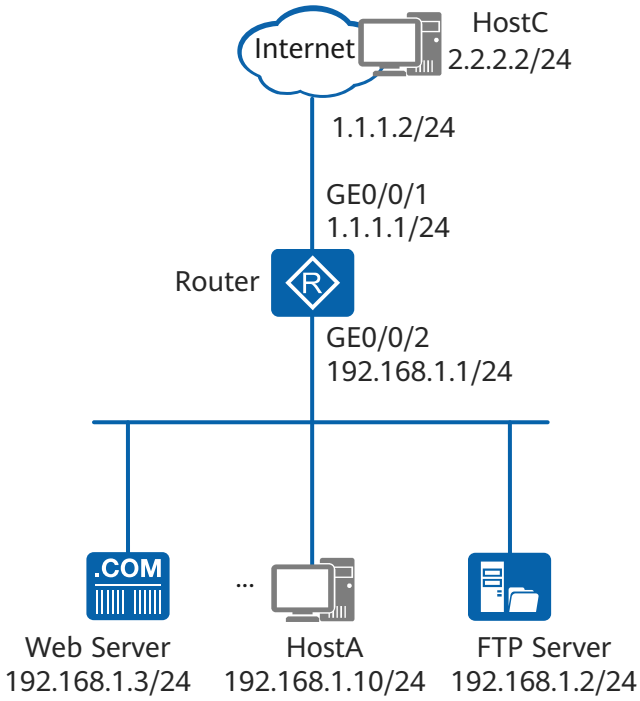
----结束

3.1.9 配置公网和私网用户通过非公网口的 IP 地址访问内部服务器和 Internet 示例

组网需求

如**3.1.9 配置公网和私网用户通过非公网口的IP地址访问内部服务器和Internet示例**所示，某小型企业内网部署了一台路由器、一台FTP服务器和一台Web服务器。路由器作为接入网关，为下挂的内网用户提供上网服务，主要包括浏览网页、使用即时通信工具、观看视频、访问邮箱等。企业内网的FTP/Web服务器对内网和外网用户分别提供FTP服务和WWW服务。该企业有两个公网IP地址，一个1.1.1.1/24部署在网关上行接口，另一个1.1.1.3/24预留给内部FTP/Web服务器使用。企业希望在路由器上配置NAT功能，使内网用户可以访问Internet，同时外网和内网用户都可以通过预留的公网IP地址访问内部FTP/Web服务器。

图 3-9 配置公网和私网用户通过非公网口的 IP 地址访问内部 FTP/Web 服务器和 Internet



版权所有 © 华为技术有限公司

数据准备

表 3-1 数据准备表

项目	数据	说明
路由器上行接口IP地址	GE0/0/1：1.1.1.1/24（公网口）	使用三层接口GE0/0/1连接Internet。
路由器下行接口IP地址	GE0/0/2：192.168.1.1/24	使用三层接口GE0/0/2连接企业内网用户。如果有多个内网用户需要上网，可以在路由器上下挂一个二层交换机来扩展用户个数。
对端运营商接口的IP地址	1.1.1.2/24	对端运营商接口的IP地址用于配置路由信息，否则内网用户上网的报文无法转发到Internet。
FTP服务器的内网IP地址和端口号 Web服务器的内网IP地址和端口号	192.168.1.2/24：21 192.168.1.3/24：80	企业内网分配给FTP/Web服务器的内网IP地址和端口号。本例中，虽然内网用户和FTP/Web服务器都在内网，但是为了防止内部服务器受内网用户的攻击，要求内网用户也通过预留的公网IP地址来访问FTP/Web服务器。
FTP服务器映射后的公网IP地址和端口号 Web服务器映射后的公网IP地址和端口号	1.1.1.3/24：21 1.1.1.3/24：9080	该企业预留了一个公网IP地址1.1.1.3/24给内部FTP/Web服务器使用。因此，可以使用该公网IP地址作为FTP/Web服务器映射后的公网IP地址。同时，需要规划不同的公网端口号21和9080来区分FTP/Web服务器。
内网用户HostA的IP地址	192.168.1.10/24	企业内部分配给用户的内网IP地址，用于验证内网用户访问Internet、FTP和Web服务器是否正常。
外网用户HostC的IP地址	2.2.2.2/24	外部用户的公网IP地址，用于验证外网用户访问内网的FTP/Web服务器是否正常。

配置思路

1. 配置路由器的接口IP地址、缺省路由，实现内部网络和外部Internet之间三层互通。
2. 在路由器的上行接口配置Easy IP方式的NAT Outbound，实现内网用户访问Internet功能。
3. 在路由器的上行接口配置服务器映射NAT Static，实现外网用户访问内部FTP/Web服务器功能。
4. 在路由器上，开启FTP的NAT ALG功能。FTP协议是一个多通道协议，需要配置NAT ALG功能，否则报文无法穿越NAT，HTTP协议不需要配置NAT ALG功能。

版权所有 © 华为技术有限公司

5. 在路由器的下行接口配置服务器映射NAT Static和Easy IP方式的NAT Outbound，将内部服务器与内网PC之间的流量都引到路由器上进行转发，实现内网用户通过预留的公网IP地址访问FTP/Web服务器功能。

操作步骤

步骤1 配置Router的接口IP地址、缺省路由，实现内部网络和外部Internet之间三层互通。

1. 配置上行接口和下行接口的IP地址。

```
<Huawei> system-view
[Huawei] sysname Router
[Router] interface gigabitethernet 0/0/1
[Router-GigabitEthernet0/0/1] undo portswitch      //有些二层接口需要切换成三层接口后，才可以配置IP地址
[Router-GigabitEthernet0/0/1] ip address 1.1.1.1 24
[Router-GigabitEthernet0/0/1] quit
[Router] interface gigabitethernet 0/0/2      //下行接口如果不是三层接口，这里可以使用VLANIF接口代替
[Router-GigabitEthernet0/0/2] undo portswitch
[Router-GigabitEthernet0/0/2] ip address 192.168.1.1 24
[Router-GigabitEthernet0/0/2] quit
```

2. 配置缺省路由，下一跳为对端运营商接口的IP地址，保证内网用户上网的报文可以到达Internet。

```
[Router] ip route-static 0.0.0.0 0.0.0.0 1.1.1.2
```

步骤2 在Router的上行接口配置Easy IP方式的NAT Outbound，使内网用户可以访问Internet。

```
[Router] acl 3000
[Router-acl-adv-3000] rule 5 permit ip source 192.168.1.0 0.0.0.255 //只允许192.168.1.0网段的用户访问Internet
[Router-acl-adv-3000] quit
[Router] interface gigabitethernet 0/0/1
[Router-GigabitEthernet0/0/1] nat outbound 3000
[Router-GigabitEthernet0/0/1] quit
```

步骤3 在Router的上行接口配置服务器映射NAT Static，实现外网用户通过预留的公网IP地址访问内部FTP/Web服务器功能。

```
[Router] interface gigabitethernet 0/0/1
[Router-GigabitEthernet0/0/1] nat static protocol tcp global 1.1.1.3 21 inside 192.168.1.2 21  //使用预留的IP地址进行NAT转换，供外网用户访问
[Router-GigabitEthernet0/0/1] nat static protocol tcp global 1.1.1.3 9080 inside 192.168.1.3 80  //对于知名端口号，可以配置成80，也可以配置成它代表的应用www
[Router-GigabitEthernet0/0/1] quit
```

步骤4 在Router上开启FTP的NAT ALG功能。

```
[Router] nat alg ftp enable
```

步骤5 在Router的下行接口配置Easy IP方式的NAT Outbound，将内部服务器与内网PC之间的流量都引到路由器上进行转发。

```
[Router] acl 3001
[Router-acl-adv-3001] rule 5 permit ip source 192.168.1.0 0.0.0.255 destination 1.1.1.3 0  //只有内部主机使用公网IP地址访问服务器的流量，才会引到Router上进行NAT转换
[Router-acl-adv-3001] quit
[Router] interface gigabitethernet 0/0/2
[Router-GigabitEthernet0/0/2] nat outbound 3001
[Router-GigabitEthernet0/0/2] quit
```

步骤6 在Router的下行接口配置服务器映射NAT Static，实现内网用户通过预留的公网IP地址访问内部FTP/Web服务器功能。

```
[Router] interface gigabitethernet 0/0/2
[Router-GigabitEthernet0/0/2] nat static protocol tcp global 1.1.1.3 21 inside 192.168.1.2 21  //使用预留的IP地址进行NAT转换，供内网用户访问
[Router-GigabitEthernet0/0/2] nat static protocol tcp global 1.1.1.3 9080 inside 192.168.1.3 80
```

 版权所有 © 华为技术有限公司

```
[Router-GigabitEthernet0/0/2] quit
[Router] quit
```

步骤7 验证配置结果。

1. 在Router上执行命令**display nat outbound**，查看动态NAT地址池配置。

```
<Router> display nat outbound
 NAT Outbound Information:
 --------------------------------------------------------------------------------
 Interface                 Acl     Address-group/IP/Interface      Type
 --------------------------------------------------------------------------------
 GigabitEthernet0/0/1      3000                  1.1.1.1     easyip
 GigabitEthernet0/0/2      3001                192.168.1.1     easyip
 --------------------------------------------------------------------------------
  Total : 2
```

2. 在Router上执行命令**display nat static**，查看静态NAT地址映射关系。

```
<Router> display nat static
  Static Nat Information:
  Interface  : GigabitEthernet0/0/1
    Global IP/Port     : 1.1.1.3/21(ftp)
    Inside IP/Port     : 192.168.1.2/21(ftp)
    Protocol : 6(tcp)
    VPN instance-name  : ----
    Acl number         : ----
    Vrrp id            : ----
    Netmask  : 255.255.255.255
    Description : ----

    Global IP/Port     : 1.1.1.3/9080
    Inside IP/Port     : 192.168.1.3/80(www)
    Protocol : 6(tcp)
    VPN instance-name  : ----
    Acl number         : ----
    Vrrp id            : ----
    Netmask  : 255.255.255.255
    Description : ----

  Interface  : GigabitEthernet0/0/2
    Global IP/Port     : 1.1.1.3/21(ftp)
    Inside IP/Port     : 192.168.1.2/21(ftp)
    Protocol : 6(tcp)
    VPN instance-name  : ----
    Acl number         : ----
    Vrrp id            : ----
    Netmask  : 255.255.255.255
    Description : ----

    Global IP/Port     : 1.1.1.3/9080
    Inside IP/Port     : 192.168.1.3/80(www)
    Protocol : 6(tcp)
    VPN instance-name  : ----
    Acl number         : ----
    Vrrp id            : ----
    Netmask  : 255.255.255.255
    Description : ----

  Total :    4
```

3. 在内网主机HostA上执行命令**ping 1.1.1.2**，模拟内网主机访问Internet，流量能Ping通，同时在Router上执行命令**display nat session all**可以查看到地址转换结果。
4. 在内网主机HostA上执行命令**ftp 1.1.1.3 21**，模拟内网主机访问内部FTP服务器，FTP能正常访问，同时在Router上执行命令**display nat session all**可以查看到地址转换结果。

 版权所有 © 华为技术有限公司

5. 在外网主机HostC上执行命令**ftp 1.1.1.3 21**，模拟外网主机访问内部FTP服务器，FTP能正常访问，同时在Router上执行命令**display nat session all**可以查看到地址转换结果。

----结束

配置文件

Router配置文件

```
#
 sysname Router
#
acl number 3000
 rule 5 permit ip source 192.168.1.0 0.0.0.255
acl number 3001
 rule 5 permit ip source 192.168.1.0 0.0.0.255 destination 1.1.1.3 0
#
nat alg ftp enable
#
interface GigabitEthernet0/0/1
 undo portswitch
 ip address 1.1.1.1 255.255.255.0
 nat static protocol tcp global 1.1.1.3 ftp inside 192.168.1.2 ftp netmask
255.255.255.255
 nat static protocol tcp global 1.1.1.3 9080 inside 192.168.1.3 www netmask
255.255.255.255
 nat outbound 3000
#
interface GigabitEthernet0/0/2
 undo portswitch
 ip address 192.168.1.1 255.255.255.0
 nat static protocol tcp global 1.1.1.3 ftp inside 192.168.1.2 ftp netmask
255.255.255.255
 nat static protocol tcp global 1.1.1.3 9080 inside 192.168.1.3 www netmask
255.255.255.255
 nat outbound 3001
#
ip route-static 0.0.0.0 0.0.0.0 1.1.1.2
#
return
```

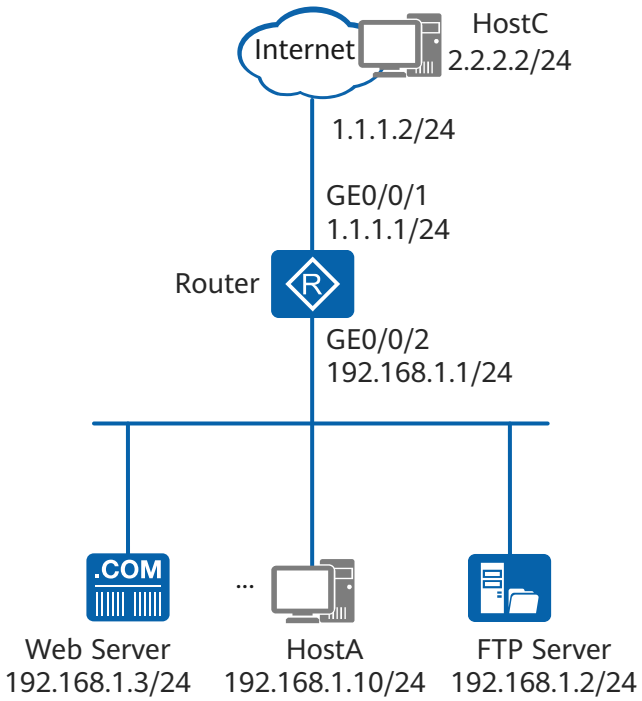
3.1.10 配置公网和私网用户通过公网口的 IP 地址访问内部服务器和 Internet 示例

组网需求

如图3-10所示，某小型企业内网部署了一台路由器、一台FTP服务器和一台Web服务器。路由器作为接入网关，为下挂的内网用户提供上网服务，主要包括浏览网页、使用即时通信工具、观看视频、访问邮箱等。企业内网的FTP/Web服务器对内网和外网用户分别提供FTP服务和WWW服务。由于IP地址资源有限，该企业只有一个可用的公网IP地址1.1.1.1/24，部署在网关的上行接口。企业希望在路由器上配置NAT功能，使内网用户可以访问Internet，同时外网和内网用户都可以通过公网口的IP地址访问内部FTP/Web服务器。

 版权所有 © 华为技术有限公司

图 3-10 配置公网和私网用户通过公网口的 IP 地址访问内部 FTP/Web 服务器和 Internet



数据准备

表 3-2 数据准备表

项目	数据	说明
路由器上行接口IP地址	GE0/0/1：1.1.1.1/24（公网口）	使用三层接口GE0/0/1连接Internet。
路由器下行接口IP地址	GE0/0/2：192.168.1.1/24	使用三层接口GE0/0/2连接企业内网用户。如果有多个内网用户需要上网，可以在路由器上下挂一个二层交换机来扩展用户个数。
对端运营商接口的IP地址	1.1.1.2/24	对端运营商接口的IP地址用于配置路由信息，否则内网用户上网的报文无法转发到Internet。
FTP服务器的内网IP地址和端口号 Web服务器的内网IP地址和端口号	192.168.1.2/24：21 192.168.1.3/24：80	企业内网分配给FTP/Web服务器的内网IP地址和端口号。本例中，虽然内网用户和FTP/Web服务器都在内网，但是为了防止内部服务器受内网用户的攻击，要求内网用户也通过公网口的IP地址来访问FTP/Web服务器。

版权所有 © 华为技术有限公司

项目	数据	说明
FTP服务器映射后的公网IP地址和端口号 Web服务器映射后的公网IP地址和端口号	1.1.1.1/24：21 1.1.1.1/24：9080	由于该企业只有一个可用的公网IP地址，部署在路由器上行接口。因此，只能使用该接口的IP地址作为FTP/Web服务器映射后的公网IP地址。同时，需要规划不同的公网端口号21和9080来区分FTP/Web服务器。
内网用户HostA的IP地址	192.168.1.10/24	企业内部分配给用户的内网IP地址，用于验证内网用户访问Internet、FTP和Web服务器是否正常。
外网用户HostC的IP地址	2.2.2.2/24	外部用户的公网IP地址，用于验证外网用户访问内网的FTP/Web服务器是否正常。

配置思路

1. 配置路由器的接口IP地址、缺省路由，实现内部网络和外部Internet之间三层互通。
2. 由于只有一个可用的公网IP地址，在路由器的上行接口配置Easy IP方式的NAT Outbound，实现内网用户访问Internet功能。
3. 在路由器的上行接口配置服务器映射NAT Static，实现外网用户访问内部FTP/Web服务器功能。
4. 在路由器上，开启FTP的NAT ALG功能。FTP协议是一个多通道协议，需要配置NAT ALG功能，否则报文无法穿越NAT，HTTP协议不需要配置NAT ALG功能。
5. 在路由器的下行接口配置服务器映射NAT Static和Easy IP方式的NAT Outbound，将内部服务器与内网PC之间的流量都引到路由器上进行转发，实现内网用户通过公网口的IP地址访问FTP/Web服务器功能。

操作步骤

步骤1 配置Router的接口IP地址、缺省路由，实现内部网络和外部Internet之间三层互通。

1. 配置上行接口和下行接口的IP地址。

```
<Huawei> system-view
[Huawei] sysname Router
[Router] interface gigabitethernet 0/0/1
[Router-GigabitEthernet0/0/1] undo portswitch      //有些二层接口需要切换成三层接口后，才可以配置IP地址
[Router-GigabitEthernet0/0/1] ip address 1.1.1.1 24
[Router-GigabitEthernet0/0/1] quit
[Router] interface gigabitethernet 0/0/2      //下行接口如果不是三层接口，这里可以使用VLANIF接口代替
[Router-GigabitEthernet0/0/2] undo portswitch
[Router-GigabitEthernet0/0/2] ip address 192.168.1.1 24
[Router-GigabitEthernet0/0/2] quit
```

2. 配置缺省路由，下一跳为对端运营商接口的IP地址，保证内网用户上网的报文可以到达Internet。

```
[Router] ip route-static 0.0.0.0 0.0.0.0 1.1.1.2
```


版权所有 © 华为技术有限公司

步骤2 在Router的上行接口配置Easy IP方式的NAT Outbound，使内网用户可以访问Internet。

```
[Router] acl 3000
[Router-acl-adv-3000] rule 5 permit ip source 192.168.1.0 0.0.0.255 //只允许192.168.1.0网段的用户访问Internet
[Router-acl-adv-3000] quit
[Router] interface gigabitethernet 0/0/1
[Router-GigabitEthernet0/0/1] nat outbound 3000
[Router-GigabitEthernet0/0/1] quit
```

步骤3 在Router的上行接口配置服务器映射NAT Static。由于只有一个可用的公网IP地址部署在上行接口，配置成**current-interface**，使用公网口的IP地址作为内部服务器映射后的IP地址，实现外网用户通过公网口的IP地址访问内部FTP/Web服务器功能。

```
[Router] interface gigabitethernet 0/0/1
[Router-GigabitEthernet0/0/1] nat static protocol tcp global current-interface 21 inside 192.168.1.2 21  //current-interface表示使用当前接口的IP地址进行NAT转换
Warning: The port is well-known(1~1023) port. If you continue it may cause function
failure.
Are you sure to continue?[Y/N]: y
[Router-GigabitEthernet0/0/1] nat static protocol tcp global current-interface 9080 inside 192.168.1.3 80  //对于知名端口号，可以配置成80，也可以配置成它代表的应用www
[Router-GigabitEthernet0/0/1] quit
```

步骤4 在Router上开启FTP的NAT ALG功能。

```
[Router] nat alg ftp enable
```

步骤5 在Router的下行接口配置Easy IP方式的NAT Outbound，将内部服务器与内网PC之间的流量都引到路由器上进行转发。

```
[Router] acl 3001
[Router-acl-adv-3001] rule 5 permit ip source 192.168.1.0 0.0.0.255 destination 1.1.1.1 0  //只有内部主机使用公网IP地址访问服务器的流量，才会引到Router上进行NAT转换
[Router-acl-adv-3001] quit
[Router] interface gigabitethernet 0/0/2
[Router-GigabitEthernet0/0/2] nat outbound 3001
[Router-GigabitEthernet0/0/2] quit
```

步骤6 在Router的下行接口配置服务器映射NAT Static。由于只有一个可用的公网IP地址部署在上行口GE0/0/1，只能指定该接口的IP地址作为内部服务器映射后的IP地址，实现内网用户通过公网口的IP地址访问内部FTP/Web服务器功能。

```
[Router] interface gigabitethernet 0/0/2
[Router-GigabitEthernet0/0/2] nat static protocol tcp global interface gigabitethernet 0/0/1 21 inside 192.168.1.2 21  //指明使用GE0/0/1接口的IP地址进行NAT转换
Warning: The port is well-known(1~1023) port. If you continue it may cause function
failure.
Are you sure to continue?[Y/N]: y
[Router-GigabitEthernet0/0/2] nat static protocol tcp global interface gigabitethernet 0/0/1 9080 inside 192.168.1.3 80
[Router-GigabitEthernet0/0/2] quit
[Router] quit
```

步骤7 验证配置结果。

1. 在Router上执行命令**display nat outbound**，查看动态NAT地址池配置。

```
<Router> display nat outbound
 NAT Outbound Information:
 ----------------------------------------------------------------------------
 Interface                 Acl     Address-group/IP/Interface      Type
 ----------------------------------------------------------------------------
 GigabitEthernet0/0/1      3000                  1.1.1.1     easyip
 GigabitEthernet0/0/2      3001                192.168.1.1     easyip
 ----------------------------------------------------------------------------
  Total : 2
```

2. 在Router上执行命令**display nat static**，查看静态NAT地址映射关系。

```
<Router> display nat static
 Static Nat Information:
```

 版权所有 © 华为技术有限公司

```
Interface  : GigabitEthernet0/0/1
  Global IP/Port     : current-interface/21(ftp)  (Real IP : 1.1.1.1)
  Inside IP/Port     : 192.168.1.2/21(ftp)
  Protocol : 6(tcp)
  VPN instance-name  : ----
  Acl number         : ----
  Vrrp id            : ----
  Netmask  : 255.255.255.255
  Description : ----

  Global IP/Port     : current-interface/9080 (Real IP : 1.1.1.1)
  Inside IP/Port     : 192.168.1.3/80(www)
  Protocol : 6(tcp)
  VPN instance-name  : ----
  Acl number         : ----
  Vrrp id            : ----
  Netmask  : 255.255.255.255
  Description : ----

Interface  : GigabitEthernet0/0/2
  Global IP/Port     : gigabitethernet0/0/1/21(ftp)  (Real IP : 1.1.1.1)
  Inside IP/Port     : 192.168.1.2/21(ftp)
  Protocol : 6(tcp)
  VPN instance-name  : ----
  Acl number         : ----
  Vrrp id            : ----
  Netmask  : 255.255.255.255
  Description : ----

  Global IP/Port     : gigabitethernet0/0/1/9080 (Real IP : 1.1.1.1)
  Inside IP/Port     : 192.168.1.3/80(www)
  Protocol : 6(tcp)
  VPN instance-name  : ----
  Acl number         : ----
  Vrrp id            : ----
  Netmask  : 255.255.255.255
  Description : ----

 Total :    4
```

3. 在内网主机HostA上执行命令**ping 1.1.1.2**，模拟内网主机访问Internet，流量能Ping通，同时在Router上执行命令**display nat session all**可以查看到地址转换结果。
4. 在内网主机HostA上执行命令**ftp 1.1.1.1 21**，模拟内网主机访问内部FTP服务器，FTP能正常访问，同时在Router上执行命令**display nat session all**可以查看到地址转换结果。
5. 在外网主机HostC上执行命令**ftp 1.1.1.1 21**，模拟外网主机访问内部FTP服务器，FTP能正常访问，同时在Router上执行命令**display nat session all**可以查看到地址转换结果。

----结束

配置文件

Router配置文件

```
#
 sysname Router
#
acl number 3000
 rule 5 permit ip source 192.168.1.0 0.0.0.255
acl number 3001
 rule 5 permit ip source 192.168.1.0 0.0.0.255 destination 1.1.1.1 0
#
nat alg ftp enable
```

 版权所有 © 华为技术有限公司

```
#
interface GigabitEthernet0/0/1
 undo portswitch
 ip address 1.1.1.1 255.255.255.0
 nat static protocol tcp global current-interface ftp inside 192.168.1.2 ftp netmask
255.255.255.255
 nat static protocol tcp global current-interface 9080 inside 192.168.1.3 www netmask
255.255.255.255
 nat outbound 3000
#
interface GigabitEthernet0/0/2
 undo portswitch
 ip address 192.168.1.1 255.255.255.0
 nat static protocol tcp global interface GigabitEthernet 0/0/1 ftp inside 192.168.1.2 ftp netmask
255.255.255.255
 nat static protocol tcp global interface GigabitEthernet 0/0/1 9080 inside 192.168.1.3 www netmask
255.255.255.255
 nat outbound 3001
#
ip route-static 0.0.0.0 0.0.0.0 1.1.1.2
#
return
```

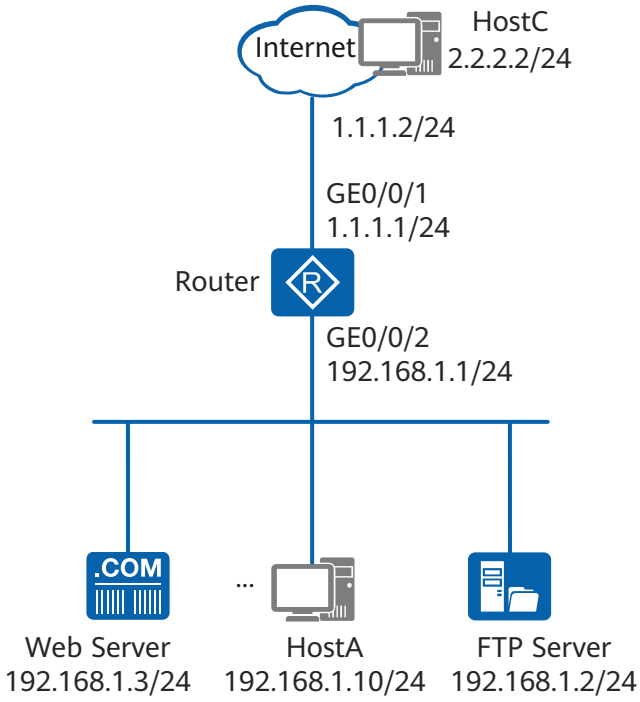
3.1.11 配置私网用户通过公网口的 IP 地址访问内部服务器和 Internet 示例

组网需求

如图3-11所示，某小型企业内网部署了一台路由器、一台FTP服务器和一台Web服务器。路由器作为接入网关，为下挂的内网用户提供上网服务，主要包括浏览网页、使用即时通信工具、观看视频、访问邮箱等。企业内网的FTP/Web服务器对内网用户提供FTP服务和WWW服务。由于IP地址资源有限，该企业只有一个可用的公网IP地址1.1.1.1/24，部署在网关的上行接口。为了防止内部服务器受内网用户的攻击，企业希望在路由器上配置NAT功能，使内网用户必须使用公网口的IP地址才能访问内部FTP/Web服务器和Internet。

 版权所有 © 华为技术有限公司

图 3-11 配置私网用户通过公网口的 IP 地址访问内部 FTP/Web 服务器和 Internet



数据准备

表 3-3 数据准备表

项目	数据	说明
路由器上行接口IP地址	GE0/0/1：1.1.1.1/24（公网口）	使用三层接口GE0/0/1连接Internet。
路由器下行接口IP地址	GE0/0/2：192.168.1.1/24	使用三层接口GE0/0/2连接企业内网用户。如果有多个内网用户需要上网，可以在路由器上下挂一个二层交换机来扩展用户个数。
对端运营商接口的IP地址	1.1.1.2/24	对端运营商接口的IP地址用于配置路由信息，否则内网用户上网的报文无法转发到Internet。
FTP服务器的内网IP地址和端口号 Web服务器的内网IP地址和端口号	192.168.1.2/24：21 192.168.1.3/24：80	企业内网分配给FTP/Web服务器的内网IP地址和端口号。本例中，为了防止内部服务器受内网用户的攻击，要求内网用户也通过公网口的IP地址来访问FTP/Web服务器。

版权所有 © 华为技术有限公司

项目	数据	说明
FTP服务器映射后的公网IP地址和端口号 Web服务器映射后的公网IP地址和端口号	1.1.1.1/24：21 1.1.1.1/24：9080	由于该企业只有一个可用的公网IP地址，部署在路由器上行接口。因此，只能使用该接口的IP地址作为FTP/Web服务器映射后的公网IP地址。同时，需要规划不同的公网端口号21和9080来区分FTP/Web服务器。
内网用户HostA的IP地址	192.168.1.10/24	企业内部分配给用户的内网IP地址，用于验证内网用户访问Internet、FTP和Web服务器是否正常。

配置思路

1. 配置路由器的接口IP地址、缺省路由，实现内部网络和外部Internet之间三层互通。
2. 由于只有一个可用的公网IP地址，在路由器的上行接口配置Easy IP方式的NAT Outbound，实现内网用户访问Internet功能。
3. 在路由器的下行接口配置服务器映射NAT Static和Easy IP方式的NAT Outbound，将内部服务器与内网PC之间的流量都引到路由器上进行转发，实现内网用户通过公网口的IP地址访问FTP/Web服务器功能。
4. 在路由器上，开启FTP的NAT ALG功能。FTP协议是一个多通道协议，需要配置NAT ALG功能，否则报文无法穿越NAT，HTTP协议不需要配置NAT ALG功能。

操作步骤

步骤1 配置Router的接口IP地址、缺省路由，实现内部网络和外部Internet之间三层互通。

1. 配置上行接口和下行接口的IP地址。

```
<Huawei> system-view
[Huawei] sysname Router
[Router] interface gigabitethernet 0/0/1
[Router-GigabitEthernet0/0/1] undo portswitch      //有些二层接口需要切换成三层接口后，才可以配置IP地址
[Router-GigabitEthernet0/0/1] ip address 1.1.1.1 24
[Router-GigabitEthernet0/0/1] quit
[Router] interface gigabitethernet 0/0/2      //下行接口如果不是三层接口，这里可以使用VLANIF接口代替
[Router-GigabitEthernet0/0/2] undo portswitch
[Router-GigabitEthernet0/0/2] ip address 192.168.1.1 24
[Router-GigabitEthernet0/0/2] quit
```

2. 配置缺省路由，下一跳为对端运营商接口的IP地址，保证内网用户上网的报文可以到达Internet。

```
[Router] ip route-static 0.0.0.0 0.0.0.0 1.1.1.2
```

步骤2 在Router的上行接口配置Easy IP方式的NAT Outbound，使内网用户可以访问Internet。

```
[Router] acl 3000
[Router-acl-adv-3000] rule 5 permit ip source 192.168.1.0 0.0.0.255 //只允许192.168.1.0网段的用户访问Internet
[Router-acl-adv-3000] quit
[Router] interface gigabitethernet 0/0/1
[Router-GigabitEthernet0/0/1] nat outbound 3000
[Router-GigabitEthernet0/0/1] quit
```

 版权所有 © 华为技术有限公司

步骤3 在Router的下行接口配置Easy IP方式的NAT Outbound，将内部服务器与内网PC之间的流量都引到路由器上进行转发。

```
[Router] acl 3001
[Router-acl-adv-3001] rule 5 permit ip source 192.168.1.0 0.0.0.255 destination 1.1.1.1 0  //只有内部主机使用公网IP地址访问内部服务器的流量，才会引到Router上进行NAT转换
[Router-acl-adv-3001] quit
[Router] interface gigabitethernet 0/0/2
[Router-GigabitEthernet0/0/2] nat outbound 3001
[Router-GigabitEthernet0/0/2] quit
```

步骤4 在Router的下行接口配置服务器映射NAT Static。由于只有一个可用的公网IP地址部署在上行口GE0/0/1，只能指定该接口的IP地址作为内部服务器映射后的IP地址，实现内网用户通过公网口的IP地址访问内部FTP/Web服务器功能。

```
[Router] interface gigabitethernet 0/0/2
[Router-GigabitEthernet0/0/2] nat static protocol tcp global interface gigabitethernet 0/0/1 21 inside 192.168.1.2 21  //指明使用GE0/0/1接口的IP地址进行NAT转换
Warning: The port is well-known(1~1023) port. If you continue it may cause function
failure.
Are you sure to continue?[Y/N]: y
[Router-GigabitEthernet0/0/2] nat static protocol tcp global interface gigabitethernet 0/0/1 9080 inside 192.168.1.3 80  //对于知名端口号，可以配置成80，也可以配置成它代表的应用www
[Router-GigabitEthernet0/0/2] quit
```

步骤5 在Router上开启FTP的NAT ALG功能。

```
[Router] nat alg ftp enable
[Router] quit
```

步骤6 验证配置结果。

1. 在Router上执行命令**display nat outbound**，查看动态NAT地址池配置。

```
<Router> display nat outbound
 NAT Outbound Information:
 ----------------------------------------------------------------------------
 Interface                Acl     Address-group/IP/Interface      Type
 ----------------------------------------------------------------------------
 GigabitEthernet0/0/1     3000                  1.1.1.1    easyip
 GigabitEthernet0/0/2     3001                192.168.1.1    easyip
 ----------------------------------------------------------------------------
 Total : 2
```

2. 在Router上执行命令**display nat static**，查看静态NAT地址映射关系。

```
<Router> display nat static
 Static Nat Information:
 Interface  : GigabitEthernet0/0/2
   Global IP/Port     : gigabitethernet0/0/1/21(ftp)  (Real IP : 1.1.1.1)
   Inside IP/Port     : 192.168.1.2/21(ftp)
   Protocol : 6(tcp)
   VPN instance-name  : ----
   Acl number         : ----
   Vrrp id            : ----
   Netmask  : 255.255.255.255
   Description : ----

   Global IP/Port     : gigabitethernet0/0/1/9080 (Real IP : 1.1.1.1)
   Inside IP/Port     : 192.168.1.3/80(www)
   Protocol : 6(tcp)
   VPN instance-name  : ----
   Acl number         : ----
   Vrrp id            : ----
   Netmask  : 255.255.255.255
   Description : ----

 Total :    2
```

3. 在内网主机HostA上执行命令**ping 1.1.1.2**，模拟内网主机访问Internet，流量能Ping通，同时在Router上执行命令**display nat session all**可以查看到地址转换结果。

 版权所有 © 华为技术有限公司

4. 在内网主机HostA上执行命令**ftp 1.1.1.1 21**，模拟内网主机访问内部FTP服务器，FTP能正常访问，同时在Router上执行命令**display nat session all**可以查看到地址转换结果。

----结束

配置文件

Router配置文件

```
#
 sysname Router
#
acl number 3000
 rule 5 permit ip source 192.168.1.0 0.0.0.255
acl number 3001
 rule 5 permit ip source 192.168.1.0 0.0.0.255 destination 1.1.1.1 0
#
nat alg ftp enable
#
interface GigabitEthernet0/0/1
 undo portswitch
 ip address 1.1.1.1 255.255.255.0
 nat outbound 3000
#
interface GigabitEthernet0/0/2
 undo portswitch
 ip address 192.168.1.1 255.255.255.0
 nat static protocol tcp global interface GigabitEthernet 0/0/1 ftp inside 192.168.1.2 ftp netmask
255.255.255.255
 nat static protocol tcp global interface GigabitEthernet 0/0/1 9080 inside 192.168.1.3 www netmask
255.255.255.255
 nat outbound 3001
#
ip route-static 0.0.0.0 0.0.0.0 1.1.1.2
#
return
```

3.1.12 配置公网和私网用户通过非公网口的 IP 地址访问内部服务器示例

规格

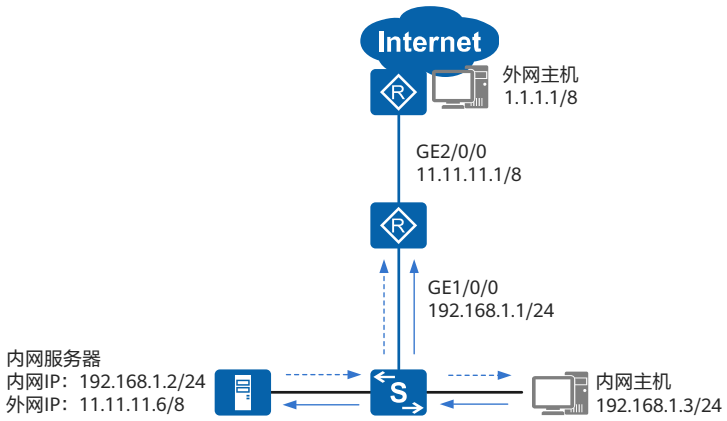
适用于V200R003C01以后版本所有形态的AR路由器。

组网需求

如图1所示，公司的内网部署了一台服务器，希望内网用户和外网用户都可以通过一个外网IP地址访问该服务器。公司为该服务器规划的内网IP地址为192.168.1.2/24，外网IP地址为11.11.11.6/8。路由器的公网口GE2/0/0的IP地址为11.11.11.1/8，LAN侧网关IP地址为192.168.1.1/24，外网主机IP地址为1.1.1.1/8，需要访问内网服务器的内网主机IP为192.168.1.3/24。

 版权所有 © 华为技术有限公司

图 3-12 配置私网用户通过非公网口的 IP 地址访问内部服务器



操作步骤

步骤1 Router的配置

```
#
acl number 3000  //用于内部主机直接使用11.11.11.6访问服务器，只有内网发起的服务才会在GE1/0/0上进行NAT
 rule 5 permit ip source 192.168.1.0 0.0.0.255 destination 11.11.11.6 0
#
interface GigabitEthernet1/0/0
 ip address 192.168.1.1 255.255.255.0
 nat static global 11.11.11.6 inside 192.168.1.2 netmask 255.255.255.255  //配置内网服务器地址的一对一NAT
 nat outbound 3000  //内网用户直接访问11.11.11.6时做Easy IP，将源地址改为GE1/0/0的地址，保证内网服务器和主机间的交互都经过Router转发
#
interface GigabitEthernet2/0/0
 ip address 11.11.11.1 255.0.0.0
 nat static global 11.11.11.6 inside 192.168.1.2 netmask 255.255.255.255  //保证外网用户使用11.11.11.6可以访问内网服务器
#
ip route-static 0.0.0.0 0.0.0.0 11.11.11.2  //配置缺省路由，保证内网用户与外网互通
#
return
```

步骤2 验证配置结果

内网用户和外网用户可以通过公网地址11.11.11.6正常访问内网服务器。

----结束

配置注意事项

- 配置ACL，确定对哪些网段进行NAT转换。

如果用户只被分配到一个公网IP（11.11.11.6），并且只需要通过NAT转换某些协议报文，可做如下处理：

- 在Router上配置Loopback口作为网关出口，配置Loopback口IP地址为11.11.11.6/8。
- 在系统视图下执行命令**nat static protocol** { **tcp** | **udp** } **global interface loopback** *interface-number global-port* **inside** *host-address* [**netmask** *mask*]配置全局NAT进行转换。

版权所有 © 华为技术有限公司

说明

对于V200R008C00及之后的版本，如果配置了NAT ALG功能，则需要将ACL规则（acl number 3000）中的目的地址改为服务器的内网地址：**rule 5 permit ip source 192.168.1.0 0.0.0.255 destination 192.168.1.2 0**。

相关资料

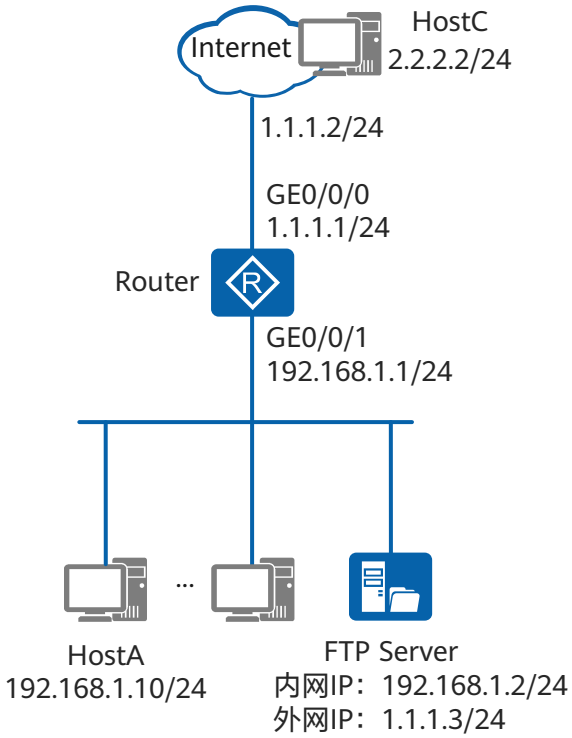
视频：**配置内网用户通过公网地址访问内网服务器**

3.1.13 配置公网用户通过非公网口的 IP 地址访问内部服务器示例

组网需求

如图3-13所示，某小型企业内网部署了一台AR路由器和一台FTP服务器。AR路由器作为接入网关，为下挂的内网用户提供上网服务，主要包括浏览网页、使用即时通信工具、观看视频、访问邮箱等。由于下挂用户的数量不确定，用户对带宽和下行用户的接入数量没有要求。此外，企业内网的FTP服务器对外提供FTP服务。企业希望在路由器上配置NAT功能，使外部用户可以正常访问内网FTP服务器。

图 3-13 配置公网用户通过非公网口的 IP 地址访问内部 FTP 服务器



版权所有 © 华为技术有限公司

数据准备

表 3-4 数据准备表

项目	数据	说明
AR路由器上行接口IP地址	GE0/0/0：1.1.1.1/24（公网口）	使用三层接口GE0/0/0连接Internet。
AR路由器下行接口IP地址	GE0/0/1：192.168.1.1/24	使用三层接口GE0/0/1连接企业内网用户。如果有多个内网用户需要上网，可以在路由器上下挂一个二层交换机来扩展用户个数。
对端运营商接口的IP地址	1.1.1.2/24	对端运营商接口的IP地址用于配置路由信息，否则内网用户上网的报文无法转发到Internet。
FTP服务器的内网IP地址	192.168.1.2/24	企业内网用户访问FTP服务器时使用的IP地址。内网用户和FTP服务器在同一个内网，可以直接使用内网IP地址来访问FTP服务器。 如果内网用户希望通过外网IP地址来访问内部服务器，详细配置请参见**3.1.12 配置公网和私网用户通过非公网口的IP地址访问内部服务器示例**。
FTP服务器对外发布的外网IP地址	1.1.1.3/24	企业外网用户访问FTP服务器时使用的IP地址。内网IP地址只能在内网中传播，无法在外网里使用，因此外网用户只能使用外网IP地址来访问FTP服务器。

配置思路

1. 配置AR路由器的接口IP地址、缺省路由，实现内部网络和外部Internet之间三层互通。
2. 在AR路由器的上行接口配置NAT Outbound，实现内网用户访问Internet功能。
3. 开启AR路由器的NAT ALG功能，并在上行接口配置NAT Static，实现外网用户访问内网FTP服务器功能。

版权所有 © 华为技术有限公司

操作步骤

步骤1 配置Router的接口IP地址、缺省路由，实现内部网络和外部Internet之间三层互通。

1. 配置上行接口和下行接口的IP地址。

```
<Huawei> system-view
[Huawei] sysname Router
[Router] interface gigabitethernet 0/0/0
[Router-GigabitEthernet0/0/0] undo portswitch      //有些二层接口需要切换成三层接口后，才可以配置IP地址
[Router-GigabitEthernet0/0/0] ip address 1.1.1.1 24
[Router-GigabitEthernet0/0/0] quit
[Router] interface gigabitethernet 0/0/1
[Router-GigabitEthernet0/0/1] undo portswitch
[Router-GigabitEthernet0/0/1] ip address 192.168.1.1 24
[Router-GigabitEthernet0/0/1] quit
```

2. 配置缺省路由，下一跳为对端运营商接口的IP地址，保证内网用户上网的报文可以到达Internet。

```
[Router] ip route-static 0.0.0.0 0.0.0.0 1.1.1.2
```

步骤2 在Router的上行接口配置NAT Outbound，使内网用户可以访问Internet。

```
[Router] acl 3000
[Router-acl-adv-3000] rule 5 permit ip source 192.168.1.0 0.0.0.255 //只允许192.168.1.0网段的用户访问Internet
[Router-acl-adv-3000] quit
[Router] interface gigabitethernet 0/0/0
[Router-GigabitEthernet0/0/0] nat outbound 3000
[Router-GigabitEthernet0/0/0] quit
```

步骤3 开启Router的NAT ALG功能，并在上行接口配置NAT Static，使外网用户可以访问内网FTP服务器。

```
[Router] nat alg ftp enable
[Router] interface gigabitethernet 0/0/0
[Router-GigabitEthernet0/0/0] nat static protocol tcp global 1.1.1.3 ftp inside 192.168.1.2 ftp  //配置内网FTP服务器对外发布的外网IP地址和内网IP地址之间的映射关系
[Router-GigabitEthernet0/0/0] quit
[Router] quit
```

步骤4 验证配置结果。

1. 在Router上执行命令**display nat outbound**，查看动态NAT地址池配置。

```
<Router> display nat outbound
 NAT Outbound Information:
 --------------------------------------------------------------------------
 Interface                 Acl     Address-group/IP/Interface      Type
 --------------------------------------------------------------------------
 GigabitEthernet0/0/0      3000                    1.1.1.1     easyip
 --------------------------------------------------------------------------
  Total : 1
```

2. 在Router上执行命令**display nat static**，查看静态NAT地址映射关系。

```
<Router> display nat static
  Static Nat Information:
  Interface  : GigabitEthernet0/0/0
    Global IP/Port     : 1.1.1.3/21(ftp)
    Inside IP/Port     : 192.168.1.2/21(ftp)
    Protocol : 6(tcp)
    VPN instance-name  : ----
    Acl number         : ----
    Vrrp id            : ----
    Netmask  : 255.255.255.255
    Description : ----

  Total :    1
```

3. 在内网主机HostA上执行命令**ping 1.1.1.2**，触发内网主机访问Internet，同时在Router上执行命令**display nat session all**查看地址转换结果。

 版权所有 © 华为技术有限公司

4. 在外网主机HostC上执行命令**ftp 1.1.1.3**，触发外网主机访问内网FTP服务器，同时在Router上执行命令**display nat session all**查看地址转换结果。

----结束

配置文件

Router配置文件

```
#
 sysname Router
#
acl number 3000
 rule 5 permit ip source 192.168.1.0 0.0.0.255
#
nat alg ftp enable
#
interface GigabitEthernet0/0/0
 undo portswitch
 ip address 1.1.1.1 255.255.255.0
 nat static protocol tcp global 1.1.1.3 ftp inside 192.168.1.2 ftp netmask 255.255.255.255
 nat outbound 3000
#
interface GigabitEthernet0/0/1
 undo portswitch
 ip address 192.168.1.1 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 1.1.1.2
#
return
```

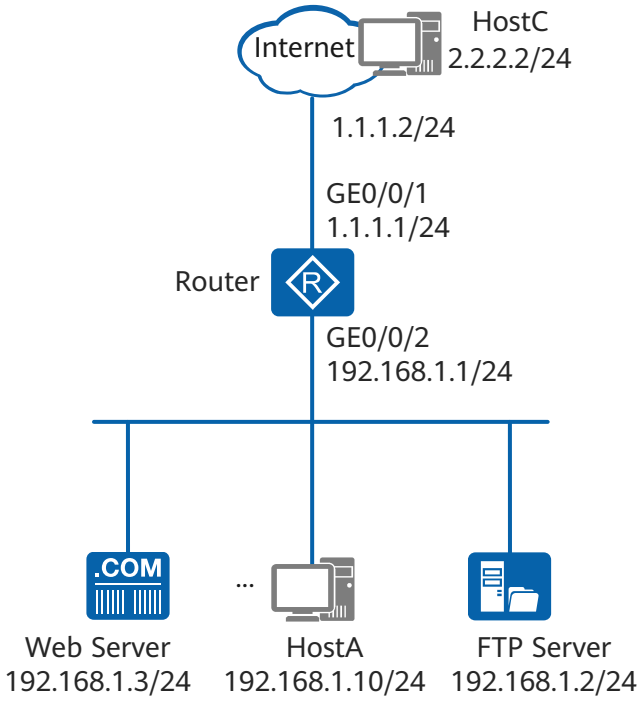
3.1.14 配置公网用户通过公网口的 IP 地址访问内部服务器示例

组网需求

如图3-14所示，某小型企业内网部署了一台路由器、一台FTP服务器和一台Web服务器。路由器作为接入网关，为下挂的内网用户提供上网服务，主要包括浏览网页、使用即时通信工具、观看视频、访问邮箱等。此外，企业内网的FTP/Web服务器对外网用户提供FTP服务和WWW服务。由于IP地址资源有限，该企业只有一个可用的公网IP地址1.1.1.1/24，部署在网关的上行接口。企业希望在路由器上配置NAT功能，使内网用户可以通过公网口的IP地址访问Internet，外网用户也可以通过公网口的IP地址访问内部FTP/Web服务器。

 版权所有 © 华为技术有限公司

图 3-14 配置公网用户通过公网口的 IP 地址访问内部 FTP/Web 服务器



数据准备

表 3-5 数据准备表

项目	数据	说明
路由器上行接口IP地址	GE0/0/1：1.1.1.1/24（公网口）	使用三层接口GE0/0/1连接Internet。
路由器下行接口IP地址	GE0/0/2：192.168.1.1/24	使用三层接口GE0/0/2连接企业内网用户。如果有多个内网用户需要上网，可以在路由器上下挂一个二层交换机来扩展用户个数。
对端运营商接口的IP地址	1.1.1.2/24	对端运营商接口的IP地址用于配置路由信息，否则内网用户上网的报文无法转发到Internet。

版权所有 © 华为技术有限公司

项目	数据	说明
FTP服务器的内网IP地址和端口号 Web服务器的内网IP地址和端口号	192.168.1.2/24：21 192.168.1.3/24：80	企业内网分配给FTP/Web服务器的内网IP地址和端口号。本例中，对内网用户访问内部FTP/Web服务器的方式没有要求。如果要求内网用户通过公网IP地址访问内部服务器，可参见**3.1.10 配置公网和私网用户通过公网口的IP地址访问内部服务器和Internet示例**。
FTP服务器映射后的公网IP地址和端口号 Web服务器映射后的公网IP地址和端口号	1.1.1.1/24：21 1.1.1.1/24：9080	由于该企业只有一个可用的公网IP地址，部署在路由器上行接口。因此，只能使用该接口的IP地址作为FTP/Web服务器映射后的公网IP地址。同时，需要规划不同的公网端口号21和9080来区分FTP/Web服务器。
内网用户HostA的IP地址	192.168.1.10/24	企业内网分配给用户的内网IP地址，用于验证内网用户访问Internet是否正常。
外网用户HostC的IP地址	2.2.2.2/24	外网用户的公网IP地址，用于验证外部用户访问内网的FTP/Web服务器是否正常。

配置思路

1. 配置路由器的接口IP地址、缺省路由，实现内部网络和外部Internet之间三层互通。
2. 由于只有一个可用的公网IP地址，在路由器的上行接口配置Easy IP方式的NAT Outbound，实现内网用户访问Internet功能。
3. 在路由器的上行接口配置服务器映射NAT Static，实现外网用户通过公网口的IP地址访问内部FTP/Web服务器功能。
4. 在路由器上，开启FTP的NAT ALG功能。FTP协议是一个多通道协议，需要配置NAT ALG功能，否则报文无法穿越NAT，HTTP协议不需要配置NAT ALG功能。

操作步骤

步骤1 配置Router的接口IP地址、缺省路由，实现内部网络和外部Internet之间三层互通。

1. 配置上行接口和下行接口的IP地址。

```
<Huawei> system-view
[Huawei] sysname Router
```

 版权所有 © 华为技术有限公司

```
[Router] interface gigabitethernet 0/0/1
[Router-GigabitEthernet0/0/1] undo portswitch      //有些二层接口需要切换成三层接口后，才可以配置IP地址
[Router-GigabitEthernet0/0/1] ip address 1.1.1.1 24
[Router-GigabitEthernet0/0/1] quit
[Router] interface gigabitethernet 0/0/2      //下行接口如果不是三层接口，这里可以使用VLANIF接口代替
[Router-GigabitEthernet0/0/2] undo portswitch
[Router-GigabitEthernet0/0/2] ip address 192.168.1.1 24
[Router-GigabitEthernet0/0/2] quit
```

2. 配置缺省路由，下一跳为对端运营商接口的IP地址，保证内网用户上网的报文可以到达Internet。

```
[Router] ip route-static 0.0.0.0 0.0.0.0 1.1.1.2
```

步骤2 在Router的上行接口配置Easy IP方式的NAT Outbound，使内网用户可以访问Internet。

```
[Router] acl 3000
[Router-acl-adv-3000] rule 5 permit ip source 192.168.1.0 0.0.0.255 //只允许192.168.1.0网段的用户访问Internet
[Router-acl-adv-3000] quit
[Router] interface gigabitethernet 0/0/1
[Router-GigabitEthernet0/0/1] nat outbound 3000
[Router-GigabitEthernet0/0/1] quit
```

步骤3 在Router的上行接口配置服务器映射NAT Static。由于只有一个可用的公网IP地址部署在上行接口，配置成**current-interface**，使用公网口的IP地址作为内部服务器映射后的IP地址，实现外网用户通过公网口的IP地址访问内部FTP/Web服务器功能。

```
[Router] interface gigabitethernet 0/0/1
[Router-GigabitEthernet0/0/1] nat static protocol tcp global current-interface 21 inside 192.168.1.2 21  //current-interface表示使用当前接口的IP地址进行NAT转换
Warning: The port is well-known(1~1023) port. If you continue it may cause function
failure.
Are you sure to continue?[Y/N]: y
[Router-GigabitEthernet0/0/1] nat static protocol tcp global current-interface 9080 inside 192.168.1.3 80  //对于知名端口号，可以配置成80，也可以配置成它代表的应用www
[Router-GigabitEthernet0/0/1] quit
```

步骤4 在Router上开启FTP的NAT ALG功能。

```
[Router] nat alg ftp enable
[Router] quit
```

步骤5 验证配置结果。

1. 在Router上执行命令**display nat outbound**，查看动态NAT地址池配置。

```
<Router> display nat outbound
 NAT Outbound Information:
 ----------------------------------------------------------------------------
 Interface                 Acl     Address-group/IP/Interface      Type
 ----------------------------------------------------------------------------
 GigabitEthernet0/0/1      3000                    1.1.1.1     easyip
 ----------------------------------------------------------------------------
 Total : 1
```

2. 在Router上执行命令**display nat static**，查看静态NAT地址映射关系。

```
<Router> display nat static
 Static Nat Information:
 Interface  : GigabitEthernet0/0/1
   Global IP/Port     : current-interface/21(ftp)  (Real IP : 1.1.1.1)
   Inside IP/Port     : 192.168.1.2/21(ftp)
   Protocol : 6(tcp)
   VPN instance-name  : ----
   Acl number         : ----
   Vrrp id            : ----
   Netmask  : 255.255.255.255
   Description : ----
```

 版权所有 © 华为技术有限公司

```
  Global IP/Port     : current-interface/9080 (Real IP : 1.1.1.1)
  Inside IP/Port     : 192.168.1.3/80(www)
  Protocol : 6(tcp)
  VPN instance-name  : ----
  Acl number         : ----
  Vrrp id            : ----
  Netmask  : 255.255.255.255
  Description : ----

 Total :    2
```

3. 在内网主机HostA上执行命令**ping 1.1.1.2**，模拟内网主机访问Internet，流量能Ping通，同时在Router上执行命令**display nat session all**可以查看到地址转换结果。
4. 在外网主机HostC上执行命令**ftp 1.1.1.3**，模拟外网主机访问内部FTP服务器，FTP能正常访问，同时在Router上执行命令**display nat session all**可以查看到地址转换结果。

----结束

配置文件

Router配置文件

```
#
 sysname Router
#
acl number 3000
 rule 5 permit ip source 192.168.1.0 0.0.0.255
#
nat alg ftp enable
#
interface GigabitEthernet0/0/1
 undo portswitch
 ip address 1.1.1.1 255.255.255.0
 nat static protocol tcp global current-interface ftp inside 192.168.1.2 ftp netmask
255.255.255.255
 nat static protocol tcp global current-interface 9080 inside 192.168.1.3 www netmask
255.255.255.255
 nat outbound 3000
#
interface GigabitEthernet0/0/2
 undo portswitch
 ip address 192.168.1.1 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 1.1.1.2
#
return
```

3.2 双出口

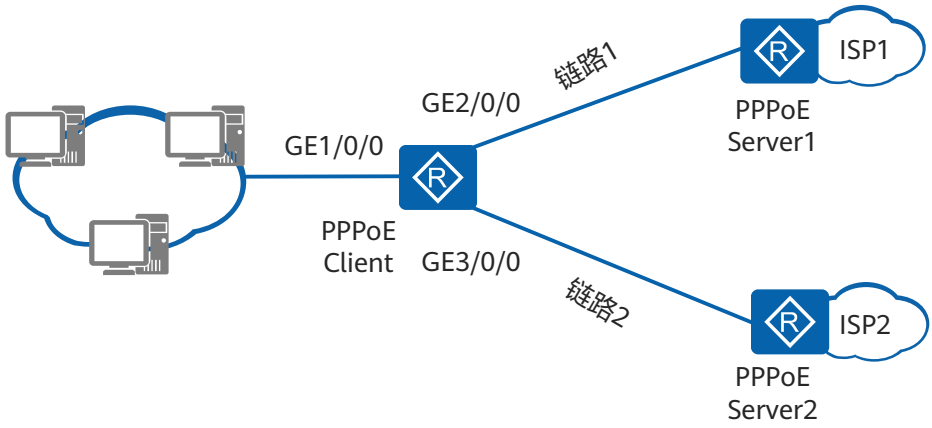
3.2.1 配置 PPPoE 拨号双链路负载分担示例

组网需求

如图3-15所示，设备作为企业出口网关，通过PPPoE拨号双上行接入Internet，链路1和链路2的出口路由采用等价路由进行负载分担。设备上配置NAT实现企业私网用户访问Internet。

 版权所有 © 华为技术有限公司

图 3-15 设备作为 PPPoE Client 双链路负载分担组网图



配置思路

采用如下的配置思路：

1. 在Dialer1接口和Dialer2接口下配置CHAP认证，实现设备通过PPP认证分别与PPPoE Server1和PPPoE Server2建立连接。
2. 配置拨号方式为自动拨号方式，这样，连接断开后，每隔一段时间设备会自动再次尝试建立拨号连接。
3. 配置NAT功能，实现局域网内的用户可以访问外网。
4. 配置等价路由，基于源IP地址进行负载分担。

操作步骤

步骤1 配置Dialer1接口，用户名和密码为用户向运营商获取接入网络的用户名和密码

```
<Huawei> system-view
[Huawei] sysname Router
[Router] interface dialer 1
[Router-Dialer1] dialer user user2
[Router-Dialer1] dialer bundle 1
[Router-Dialer1] ppp chap user user1@system
[Router-Dialer1] ppp chap password cipher YsHsjx_202206
[Router-Dialer1] ip address ppp-negotiate
[Router-Dialer1] quit
```

步骤2 配置Dialer2接口，用户名和密码为用户向运营商获取接入网络的用户名和密码

```
[Router] interface dialer 2
[Router-Dialer2] dialer user user2
[Router-Dialer2] dialer bundle 2
[Router-Dialer2] ppp chap user user1@system
[Router-Dialer2] ppp chap password cipher YsHsjx_202206
[Router-Dialer2] ip address ppp-negotiate
[Router-Dialer2] quit
```

步骤3 建立PPPoE会话

```
[Router] interface gigabitethernet 2/0/0
[Router-GigabitEthernet2/0/0] pppoe-client dial-bundle-number 1
[Router-GigabitEthernet2/0/0] quit
[Router] interface gigabitethernet 3/0/0
```


版权所有 © 华为技术有限公司

```
[Router-GigabitEthernet3/0/0] pppoe-client dial-bundle-number 2
[Router-GigabitEthernet3/0/0] quit
```

步骤4 配置局域网用户通过NAT转换将私网地址转换为公网地址，进行拨号上网

```
[Router] acl number 3002
[Router-acl-adv-3002] rule 5 permit ip source 192.168.10.0 0.0.0.255
[Router-acl-adv-3002] quit
[Router] interface dialer 1
[Router-Dialer1] nat outbound 3002
[Router-Dialer1] quit
[Router] interface dialer 2
[Router-Dialer2] nat outbound 3002
[Router-Dialer2] quit
```

步骤5 配置到PPPoE Server的等价路由，基于源IP地址进行负载分担

```
[Router] ip route-static 0.0.0.0 0 dialer 1
[Router] ip route-static 0.0.0.0 0 dialer 2
[Router] ip load-balance hash src-ip
```

步骤6 配置Dialer1接口拨号失败时转换为Down状态，自动切换为Dialer2接口进行拨号

```
[Router] interface dialer 1
[Router-Dialer1] dialer number 1 autodial
[Router-Dialer1] quit
[Router] quit
```

步骤7 验证配置结果

在PPPoE Client上执行命令**display pppoe-client session summary**，查看PPPoE会话状态和配置信息。根据显示信息判断会话状态是否正常（状态为UP表示正常）、配置是否正确（是否和之前的数据规划和组网一致）。

```
<Router> display pppoe-client session summary
PPPoE Client Session:
ID   Bundle  Dialer  Intf          Client-MAC    Server-MAC    State
1    1       1       GE2/0/0       00e0fc577510  0819a6cd0680  UP
1    2       2       GE3/0/0       00e0fc577511  001109141bd3  UP
```

----结束

配置文件

设备作为PPPoE Client的配置文件

```
#
 sysname Router
#
ip load-balance hash src-ip
#
acl number 3002
 rule 5 permit ip source 192.168.10.0 0.0.0.255
#
interface Dialer1
 link-protocol ppp
 ppp chap user user1@system
 ppp chap password cipher %^%#R=>NT8A-8KmWU38WOZq(s%MsRSg>3,}l9b%K.%!S%^%#
 ip address ppp-negotiate
 dialer user user2
 dialer bundle 1
 dialer number 1 autodial
 nat outbound 3002
#
interface Dialer2
 link-protocol ppp
 ppp chap user user1@system
 ppp chap password cipher %^%#$`GP<&RG`A@+F/'fP)xY84g7V/%g-Oahd"*"r/'Z%^%#
 ip address ppp-negotiate
```

 版权所有 © 华为技术有限公司

```
 dialer user user2
 dialer bundle 2
 nat outbound 3002
#
interface GigabitEthernet2/0/0
 pppoe-client dial-bundle-number 1
#
interface GigabitEthernet3/0/0
 pppoe-client dial-bundle-number 2
#
ip route-static 0.0.0.0 0.0.0.0 Dialer1
ip route-static 0.0.0.0 0.0.0.0 Dialer2
#
return
```

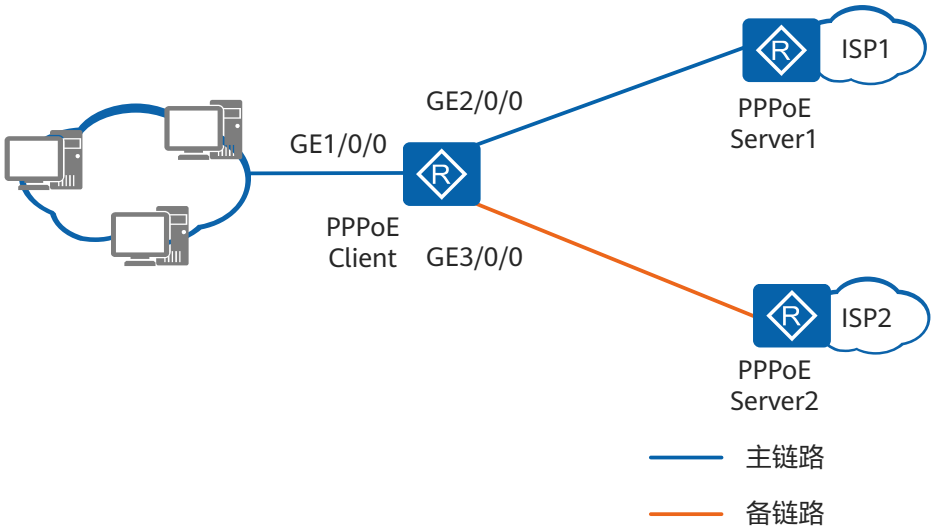
3.2.2 配置 PPPoE 拨号双链路上行备份示例

组网需求

如图3-16所示，设备下行通过GE1/0/0连接局域网用户，上行通过GE2/0/0接入PPPoE Server1作为主链路，通过GE3/0/0接入PPPoE Server2作为备份链路。Dialer1和Dialer2分别绑定到GE2/0/0接口和GE3/0/0接口，对应两个PPPoE会话。

为了增强PPPoE拨号的可靠性，用户希望在PPPoE拨号不成功的时候，能够通过备份链路完成PPPoE拨号。主备链路可以通过配置静态路由的优先级区分出来。

图 3-16 设备作为 PPPoE Client 双链路上行备份组网图



配置思路

采用如下的配置思路：

1. 在Dialer1接口和Dialer2接口下配置CHAP认证，实现设备通过PPP认证分别与PPPoE Server1和PPPoE Server2建立连接。
2. 配置拨号方式为自动拨号方式，这样，连接断开后，每隔一段时间设备会自动再次尝试建立拨号连接。

版权所有 © 华为技术有限公司

3. 配置NAT功能，实现局域网内的用户可以访问外网。
4. 配置静态路由的优先级，区分出主备链路。

操作步骤

步骤1 配置Dialer1接口，用户名和密码为用户向运营商获取接入网络的用户名和密码

```
<Huawei> system-view
[Huawei] sysname Router
[Router] interface dialer 1
[Router-Dialer1] dialer user user2
[Router-Dialer1] dialer bundle 1
[Router-Dialer1] ppp chap user user1@system
[Router-Dialer1] ppp chap password cipher YsHsjx_202206
[Router-Dialer1] ip address ppp-negotiate
[Router-Dialer1] quit
```

步骤2 配置Dialer2接口，用户名和密码为用户向运营商获取接入网络的用户名和密码

```
[Router] interface dialer 2
[Router-Dialer2] dialer user user2
[Router-Dialer2] dialer bundle 2
[Router-Dialer2] ppp chap user user1@system
[Router-Dialer2] ppp chap password cipher YsHsjx_202206
[Router-Dialer2] ip address ppp-negotiate
[Router-Dialer2] quit
```

步骤3 建立PPPoE会话

```
[Router] interface gigabitethernet 2/0/0
[Router-GigabitEthernet2/0/0] pppoe-client dial-bundle-number 1
[Router-GigabitEthernet2/0/0] quit
[Router] interface gigabitethernet 3/0/0
[Router-GigabitEthernet3/0/0] pppoe-client dial-bundle-number 2
[Router-GigabitEthernet3/0/0] quit
```

步骤4 配置局域网用户通过NAT转换将私网地址转换为公网地址，进行拨号上网

```
[Router] acl number 3002
[Router-acl-adv-3002] rule 5 permit ip source 192.168.10.0 0.0.0.255
[Router-acl-adv-3002] quit
[Router] interface dialer 1
[Router-Dialer1] nat outbound 3002
[Router-Dialer1] quit
[Router] interface dialer 2
[Router-Dialer2] nat outbound 3002
[Router-Dialer2] quit
```

步骤5 配置到PPPoE Server的静态路由，通过指定静态路由的优先级完成主备链路，优先选择Dialer1接口进行拨号

```
[Router] ip route-static 0.0.0.0 0 dialer 1
[Router] ip route-static 0.0.0.0 0 dialer 2 preference 100
```

步骤6 配置Dialer1接口拨号失败时转换为Down状态，自动切换为Dialer2接口进行拨号

```
[Router] interface dialer 1
[Router-Dialer1] dialer number 1 autodial
[Router-Dialer1] quit
[Router] quit
```

步骤7 验证配置结果

在PPPoE Client上执行命令**display pppoe-client session summary**，查看PPPoE会话状态和配置信息。根据显示信息判断会话状态是否正常（状态为UP表示正常）、配置是否正确（是否和之前的数据规划和组网一致）。

```
<Router> display pppoe-client session summary
PPPoE Client Session:
ID   Bundle  Dialer  Intf          Client-MAC    Server-MAC    State
```

 版权所有 © 华为技术有限公司

```
1   1     1     GE2/0/0        00e0fc577510  0819a6cd0680  UP
1   2     2     GE3/0/0        00e0fc577511  001109141bd3  UP
```

----结束

配置文件

设备作为PPPoE Client的配置文件

```
#
 sysname Router
#
acl number 3002
 rule 5 permit ip source 192.168.10.0 0.0.0.255
#
interface Dialer1
 link-protocol ppp
 ppp chap user user1@system
 ppp chap password cipher %^%#R=>NT8A-8KmWU38WOZq(s%MsRSg>3,}l9b%K.%!S%^%#
 ip address ppp-negotiate
 dialer user user2
 dialer bundle 1
 dialer number 1 autodial
 nat outbound 3002
#
interface Dialer2
 link-protocol ppp
 ppp chap user user1@system
 ppp chap password cipher %^%#$`GP<&RG`A@+F/'fP)xY84g7V/%g-Oahd"*"r/'Z%^%#
 ip address ppp-negotiate
 dialer user user2
 dialer bundle 2
 nat outbound 3002
#
interface GigabitEthernet2/0/0
 pppoe-client dial-bundle-number 1
#
interface GigabitEthernet3/0/0
 pppoe-client dial-bundle-number 2
#
ip route-static 0.0.0.0 0.0.0.0 Dialer1
ip route-static 0.0.0.0 0.0.0.0 Dialer2 preference 100
#
return
```

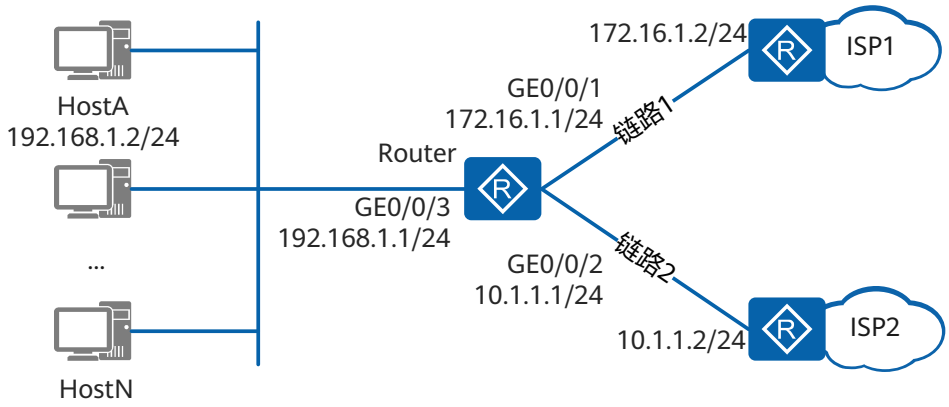
3.2.3 配置静态 IP 双链路负载分担示例

组网需求

如图3-17所示，某小型企业内网部署了一台路由器作为接入网关，为下挂的内网用户提供访问Internet服务。为了防止网络流量较大时，出现网络拥塞，影响上网体验，企业在路由器上部署了两条链路同时接入Internet。两条链路都通过静态IP方式接入运营商。企业希望用户的上网流量可以均匀在两条链路上转发，提高网络带宽，同时通过配置NAT功能使内网用户可以访问Internet。

 版权所有 © 华为技术有限公司

图 3-17 配置静态 IP 双链路负载分担示例



数据准备

表 3-6 数据准备表

项目	数据	说明
运营商1分配给链路1的静态IP地址	链路1接口：GE0/0/1 IP地址：172.16.1.1/24	使用三层接口GE0/0/1作为链路1接口上行连接到Internet，且GE0/0/1通过手工配置方式获取静态IP地址。 **说明** 此处的IP地址为用户向运营商获取接入网络的IP地址。
运营商2分配给链路2的静态IP地址	链路2接口：GE0/0/2 IP地址：10.1.1.1/24	使用三层接口GE0/0/2作为链路2接口上行连接到Internet，且GE0/0/2通过手工配置方式获取静态IP地址。 **说明** 此处的IP地址为用户向运营商获取接入网络的IP地址。
链路1对端运营商1网关的IP地址	172.16.1.2/24	对端运营商1网关的IP地址用于配置路由信息，否则内网用户上网的报文无法转发到Internet。
链路2对端运营商2网关的IP地址	10.1.1.2/24	对端运营商2网关的IP地址用于配置路由信息，否则内网用户上网的报文无法转发到Internet。
路由器下行接口的IP地址	GE0/0/3：192.168.1.1/24	使用三层接口GE0/0/3连接企业内网用户。如果有多个内网用户需要上网，可以在路由器上下挂一个二层交换机来扩展用户个数。
内网用户HostA的IP地址	192.168.1.2/24	企业内部分配给用户的内网IP地址，用于验证内网用户访问Internet是否正常。

版权所有 © 华为技术有限公司

配置思路

1. 在链路1接口GE0/0/1上配置静态IP地址，使主链路可以通过静态IP方式接入运营商1。
2. 在链路2接口GE0/0/2上配置静态IP地址，使备链路可以通过静态IP方式接入运营商2。
3. 在两个上行接口配置Easy IP方式的NAT Outbound，使企业内网用户可以访问Internet。
4. 配置两条等价默认路由，通过多条等价路由方式来实现负载分担，将流量分摊到两条链路上进行转发。

操作步骤

步骤1 在链路1接口GE0/0/1上配置静态IP地址，使主链路可以通过静态IP方式接入运营商1。

```
[Router] interface gigabitethernet 0/0/1
[Router-GigabitEthernet0/0/1] undo portswitch    //有些二层接口需要切换成三层接口后，才可以配置静态IP地址
[Router-GigabitEthernet0/0/1] ip address 172.16.1.1 24   //运营商1分配给链路1接口的IP地址
[Router-GigabitEthernet0/0/1] quit
```

步骤2 在链路2接口GE0/0/2上配置静态IP地址，使备链路可以通过静态IP方式接入运营商2。

```
[Router] interface gigabitethernet 0/0/2
[Router-GigabitEthernet0/0/2] undo portswitch
[Router-GigabitEthernet0/0/2] ip address 10.1.1.1 24  //运营商2分配给链路2接口的IP地址
[Router-GigabitEthernet0/0/2] quit
[Router] interface gigabitethernet 0/0/3
[Router-GigabitEthernet0/0/3] undo portswitch
[Router-GigabitEthernet0/0/3] ip address 192.168.1.1 24   //配置路由器下行连接内网接口的IP地址
[Router-GigabitEthernet0/0/3] quit
```

步骤3 在两个上行接口配置Easy IP方式的NAT Outbound，使企业内网用户可以访问Internet。

```
[Router] acl number 3002
[Router-acl-adv-3002] rule 5 permit ip source 192.168.1.0 0.0.0.255 //只允许192.168.1.0网段的用户访问Internet
[Router-acl-adv-3002] quit
[Router] interface gigabitethernet 0/0/1
[Router-GigabitEthernet0/0/1] nat outbound 3002
[Router-GigabitEthernet0/0/1] quit
[Router] interface gigabitethernet 0/0/2
[Router-GigabitEthernet0/0/2] nat outbound 3002
[Router-GigabitEthernet0/0/2] quit
```

步骤4 配置两条等价默认路由，通过多条等价路由来实现负载分担，并配置基于源IP地址方式进行负载分担。

```
[Router] ip route-static 0.0.0.0 0 172.16.1.2  //链路1的路由优先级为默认值60
[Router] ip route-static 0.0.0.0 0 10.1.1.2    //链路2的路由优先级也为默认值60，链路1和链路2为两条等价默认路由
[Router] ip load-balance hash src-ip     //基于源IP地址方式进行负载分担
[Router] quit
```

步骤5 验证配置结果。

1. 在Router上执行命令**display ip routing-table protocol static**，查看配置的静态路由表信息，路由表内有两条等价默认路由分别到运营商1和运营商2。

```
<Router> display ip routing-table protocol static
Route Flags: R - relay, D - download to fib, T - to vpn-instance
------------------------------------------------------------------------------
Public routing table : Static
         Destinations : 1        Routes : 2        Configured Routes : 2

Static routing table status : <Active>
```

 版权所有 © 华为技术有限公司

```
        Destinations : 0        Routes : 0

Static routing table status : <Inactive>
        Destinations : 1        Routes : 2

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        0.0.0.0/0   Static  60   0           172.16.1.2      Unknown
        0.0.0.0/0   Static  60   0           10.1.1.2        Unknown
```

2. 在内网主机HostA上执行**ping**命令，Ping对端运营商网关的IP地址，模拟内网主机访问Internet。HostA能同时Ping通运营商1网关的IP地址和运营商2网关的IP地址，两条链路可以同时转发流量，实现负载分担。

----结束

配置文件

Router配置文件

```
#
 sysname Router
#
ip load-balance hash src-ip
#
acl number 3002
 rule 5 permit ip source 192.168.1.0 0.0.0.255
#
interface GigabitEthernet0/0/1
 undo portswitch
 ip address 172.16.1.1 255.255.255.0
 nat outbound 3002
#
interface GigabitEthernet0/0/2
 undo portswitch
 ip address 10.1.1.1 255.255.255.0
 nat outbound 3002
#
interface GigabitEthernet0/0/3
 undo portswitch
 ip address 192.168.1.1 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 172.16.1.2
ip route-static 0.0.0.0 0.0.0.0 10.1.1.2
#
return
```

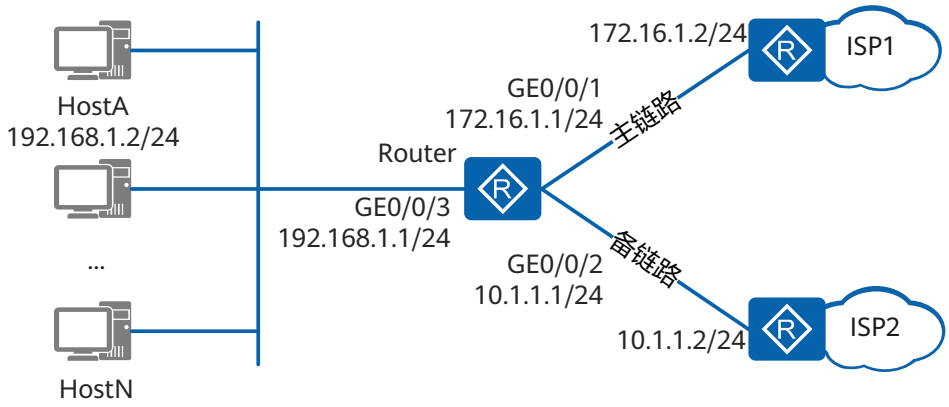
3.2.4 配置静态 IP 双链路上行备份示例

组网需求

如图3-18所示，某小型企业内网部署了一台路由器作为接入网关，为下挂的内网用户提供访问Internet服务。为了提高网络的可靠性，企业在路由器上部署了两条链路同时接入Internet。两条链路都通过静态IP方式接入运营商。企业希望两条链路一条为主链路，一条为备链路，当主链路发生故障时，流量可以切换到备链路上进行转发，同时通过配置NAT功能使内网用户可以访问Internet。

 版权所有 © 华为技术有限公司

图 3-18 配置静态 IP 双链路上行备份示例



数据准备

表 3-7 数据准备表

项目	数据	说明
运营商1分配给主链路的静态IP地址	主链路接口：GE0/0/1 IP地址：172.16.1.1/24	使用三层接口GE0/0/1作为主链路接口上行连接到Internet，且GE0/0/1通过手工配置方式获取静态IP地址。 **说明** 此处的IP地址为用户向运营商获取接入网络的IP地址。
运营商2分配给备链路的静态IP地址	备链路接口：GE0/0/2 IP地址：10.1.1.1/24	使用三层接口GE0/0/2作为备链路接口上行连接到Internet，且GE0/0/2通过手工配置方式获取静态IP地址。 **说明** 此处的IP地址为用户向运营商获取接入网络的IP地址。
主链路对端运营商1网关的IP地址	172.16.1.2/24	对端运营商1网关的IP地址用于配置路由信息，否则内网用户上网的报文无法转发到Internet。
备链路对端运营商2网关的IP地址	10.1.1.2/24	对端运营商2网关的IP地址用于配置路由信息，否则内网用户上网的报文无法转发到Internet。
路由器下行接口的IP地址	GE0/0/3：192.168.1.1/24	使用三层接口GE0/0/3连接企业内网用户。如果有多个内网用户需要上网，可以在路由器上下挂一个二层交换机来扩展用户个数。
内网用户HostA的IP地址	192.168.1.2/24	企业内部分配给用户的内网IP地址，用于验证内网用户访问Internet是否正常。

版权所有 © 华为技术有限公司

配置思路

1. 在主链路接口GE0/0/1上配置静态IP地址，使主链路可以通过静态IP方式接入运营商1。
2. 在备链路接口GE0/0/2上配置静态IP地址，使备链路可以通过静态IP方式接入运营商2。
3. 在两个上行接口配置Easy IP方式的NAT Outbound，使企业内网用户可以访问Internet。
4. 配置两条不同优先级的默认路由，通过优先级的高低来区分主备链路，主链路的优先级高，备链路的优先级低。

操作步骤

步骤1 在主链路接口GE0/0/1上配置静态IP地址，使主链路可以通过静态IP方式接入运营商1。

```
[Router] interface gigabitethernet 0/0/1
[Router-GigabitEthernet0/0/1] undo portswitch    //有些二层接口需要切换成三层接口后，才可以配置静态IP地址
[Router-GigabitEthernet0/0/1] ip address 172.16.1.1 24   //运营商1分配给主链路接口的IP地址
[Router-GigabitEthernet0/0/1] quit
```

步骤2 在备链路接口GE0/0/2上配置静态IP地址，使备链路可以通过静态IP方式接入运营商2。

```
[Router] interface gigabitethernet 0/0/2
[Router-GigabitEthernet0/0/2] undo portswitch
[Router-GigabitEthernet0/0/2] ip address 10.1.1.1 24  //运营商2分配给备链路接口的IP地址
[Router-GigabitEthernet0/0/2] quit
[Router] interface gigabitethernet 0/0/3
[Router-GigabitEthernet0/0/3] undo portswitch
[Router-GigabitEthernet0/0/3] ip address 192.168.1.1 24   //配置路由器下行连接内网接口的IP地址
[Router-GigabitEthernet0/0/3] quit
```

步骤3 在两个上行接口配置Easy IP方式的NAT Outbound，使企业内网用户可以访问Internet。

```
[Router] acl number 3002
[Router-acl-adv-3002] rule 5 permit ip source 192.168.1.0 0.0.0.255 //只允许192.168.1.0网段的用户访问Internet
[Router-acl-adv-3002] quit
[Router] interface gigabitethernet 0/0/1
[Router-GigabitEthernet0/0/1] nat outbound 3002
[Router-GigabitEthernet0/0/1] quit
[Router] interface gigabitethernet 0/0/2
[Router-GigabitEthernet0/0/2] nat outbound 3002
[Router-GigabitEthernet0/0/2] quit
```

步骤4 配置两条不同优先级的默认路由，通过优先级的高低来区分主备链路，主链路的优先级高，备链路的优先级低。

```
[Router] ip route-static 0.0.0.0 0 172.16.1.2  //主链路的路由优先级为默认值60
[Router] ip route-static 0.0.0.0 0 10.1.1.2 preference 100    //备链路的路由优先级为100，数值越小，优先级越高
[Router] quit
```

步骤5 验证配置结果。

1. 在Router上执行命令**display ip routing-table protocol static**，查看配置的静态路由表信息，路由表内到运营商1的路由优先级高于到运营商2的路由优先级。

```
<Router> display ip routing-table protocol static
Route Flags: R - relay, D - download to fib, T - to vpn-instance
------------------------------------------------------------------------------
Public routing table : Static
         Destinations : 1        Routes : 2        Configured Routes : 2
```

 版权所有 © 华为技术有限公司

```
Static routing table status : <Active>
        Destinations : 0        Routes : 0

Static routing table status : <Inactive>
        Destinations : 1        Routes : 2

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        0.0.0.0/0   Static  60   0           172.16.1.2      Unknown
        0.0.0.0/0   Static  100  0           10.1.1.2         Unknown
```

2. 在内网主机HostA上执行**ping**命令，Ping对端运营商网关的IP地址，模拟内网主机访问Internet。当主链路正常时，HostA只能Ping通运营商1网关的IP地址，当主链路故障时，HostA只能Ping通运营商2网关的IP地址，两条链路一条为主，一条为备，流量优先从主链路转发到运营商1。

----结束

配置文件

Router配置文件

```
#
 sysname Router
#
acl number 3002
 rule 5 permit ip source 192.168.1.0 0.0.0.255
#
interface GigabitEthernet0/0/1
 undo portswitch
 ip address 172.16.1.1 255.255.255.0
 nat outbound 3002
#
interface GigabitEthernet0/0/2
 undo portswitch
 ip address 10.1.1.1 255.255.255.0
 nat outbound 3002
#
interface GigabitEthernet0/0/3
 undo portswitch
 ip address 192.168.1.1 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 172.16.1.2
ip route-static 0.0.0.0 0.0.0.0 10.1.1.2 preference 100
#
return
```

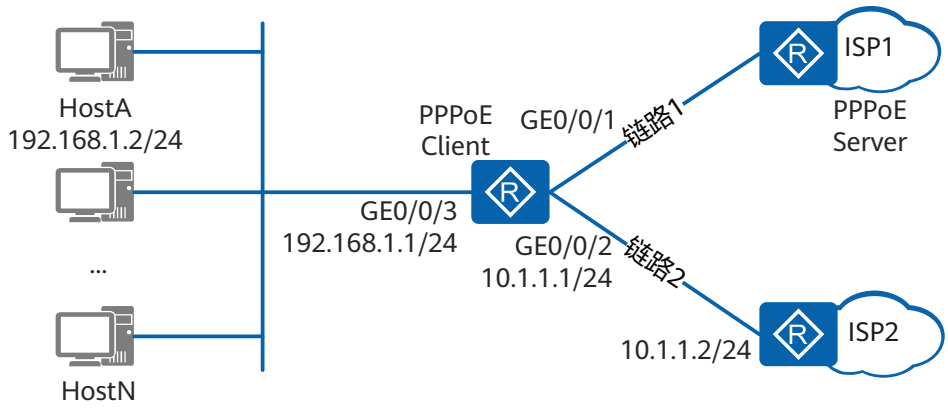
3.2.5 配置 PPPoE 拨号和静态 IP 双链路负载分担示例

组网需求

如图1所示，某小型企业内网部署了一台路由器作为接入网关，为下挂的内网用户提供访问Internet服务。为了防止网络流量较大时，出现网络拥塞，影响上网体验，企业在路由器上部署了两条链路同时接入Internet。链路1通过PPPoE拨号方式接入运营商1，链路2通过静态IP方式接入运营商2。企业希望用户的上网流量可以均匀在两条链路上转发，提高网络带宽，同时通过配置NAT功能使内网用户可以访问Internet。

 版权所有 © 华为技术有限公司

图 3-19 配置 PPPoE 拨号和静态 IP 双链路负载分担示例



数据准备

表 3-8 数据准备表

项目	数据	说明
运营商1分配给链路1的PPPoE用户名和密码	链路1接口：GE0/0/1 用户名：user1@system 密码：YsHsjx_202206	使用三层接口GE0/0/1作为链路1接口上行连接到Internet，且GE0/0/1通过PPPoE拨号方式自动获取IP地址。 **说明** 此处的用户名和密码为用户向运营商获取接入网络的用户名和密码。
运营商2分配给链路2的静态IP地址	链路2接口：GE0/0/2 IP地址：10.1.1.1/24	使用三层接口GE0/0/2作为链路2接口上行连接到Internet，且GE0/0/2通过手工配置方式获取静态IP地址。 **说明** 此处的IP地址为用户向运营商获取接入网络的IP地址。
链路2对端运营商2网关的IP地址	10.1.1.2/24	对端运营商2网关的IP地址用于配置路由信息，否则内网用户上网的报文无法转发到Internet。
路由器下行接口的IP地址	GE0/0/3：192.168.1.1/24	使用三层接口GE0/0/3连接企业内网用户。如果有多个内网用户需要上网，可以在路由器上下挂一个二层交换机来扩展用户个数。
内网用户HostA的IP地址	192.168.1.2/24	企业内部分配给用户的内网IP地址，用于验证内网用户访问Internet是否正常。

版权所有 © 华为技术有限公司

配置思路

1. 在路由器的Dialer1接口上配置共享DCC功能，使PPPoE Client用户可以按需拨号，节省费用。
2. 配置PPP链路的认证方式，使设备与PPPoE Server之间建立连接获取IP地址。
3. 配置PPPoE拨号方式为自动拨号，在连接断开后，设备可以自动建立拨号连接。
4. 在链路1接口GE0/0/1上建立PPPoE会话，使链路1可以通过PPPoE拨号方式接入运营商1；在链路2接口GE0/0/2上配置静态IP地址，使链路2可以通过静态IP方式接入运营商2。
5. 在两个上行接口配置Easy IP方式的NAT Outbound，使企业内网用户可以访问Internet。
6. 配置两条等价默认路由，通过多条等价路由方式来实现负载分担，将流量分摊到两条链路上进行转发。

操作步骤

步骤1 在Router的Dialer1接口上配置共享DCC功能，使PPPoE Client用户可以按需拨号。

```
<Huawei> system-view
[Huawei] sysname Router
[Router] interface dialer 1
[Router-Dialer1] dialer user user1    //启动共享DCC功能并设置对端用户名
[Router-Dialer1] dialer bundle 1
[Router-Dialer1] dialer number 1 autodial  //配置Dialer1接口拨号失败时转换为Down状态，流量切换到链路2转发
[Router-Dialer1] quit
```

步骤2 配置PPP链路的认证方式，使设备与PPPoE Server之间建立连接获取IP地址。PPP链路的认证方式有CHAP和PAP两种，请根据实际情况选择其中一种进行配置，和对端PPPoE Server的认证方式保持一致即可，本例中选择使用CHAP方式。

- 如果对端PPPoE Server使用CHAP认证，则配置PPP链路的认证方式为CHAP。

  ```
  [Router] interface dialer 1
  [Router-Dialer1] ppp chap user user1@system
  [Router-Dialer1] ppp chap password cipher YsHsjx_202206
  [Router-Dialer1] quit
  ```

- 如果对端PPPoE Server使用PAP认证，则配置PPP链路的认证方式为PAP认证。

  ```
  [Router] interface dialer 1
  [Router-Dialer1] ppp pap local-user user1@system password cipher YsHsjx_202206
  [Router-Dialer1] quit
  ```

步骤3 配置PPPoE拨号方式为自动拨号，在连接断开后，设备可以自动建立拨号连接。

```
[Router] interface dialer 1
[Router-Dialer1] ip address ppp-negotiate
[Router-Dialer1] ppp ipcp dns admit-any  //当设备通过PPP协议与其他设备相连时，若设备需要通过域名直接访问Internet，则需要配置对端设备为其分配DNS服务器地址
[Router-Dialer1] tcp adjust-mss 1200   //配置接口的TCP最大报文段长度为推荐值1200字节
[Router-Dialer1] quit
```

步骤4 在链路1接口GE0/0/1上建立PPPoE会话，使链路1可以通过PPPoE拨号方式接入运营商1；在链路2接口GE0/0/2上配置静态IP地址，使链路2可以通过静态IP方式接入运营商2。

```
[Router] interface gigabitethernet 0/0/1
[Router-GigabitEthernet0/0/1] undo portswitch    //有些二层接口需要切换成三层接口后，才可以配置PPPoE会话
[Router-GigabitEthernet0/0/1] pppoe-client dial-bundle-number 1
[Router-GigabitEthernet0/0/1] quit
[Router] interface gigabitethernet 0/0/2
[Router-GigabitEthernet0/0/2] undo portswitch    //有些二层接口需要切换成三层接口后，才可以配置IP地址
[Router-GigabitEthernet0/0/2] ip address 10.1.1.1 24  //运营商2分配给链路2的IP地址
[Router-GigabitEthernet0/0/2] quit
```

 版权所有 © 华为技术有限公司

```
[Router] interface gigabitethernet 0/0/3
[Router-GigabitEthernet0/0/3] undo portswitch    //配置路由器下行连接内网接口的IP地址
[Router-GigabitEthernet0/0/3] ip address 192.168.1.1 24
[Router-GigabitEthernet0/0/3] quit
```

步骤5 在两个上行接口配置Easy IP方式的NAT Outbound，使企业内网用户可以访问Internet。

```
[Router] acl number 3002
[Router-acl-adv-3002] rule 5 permit ip source 192.168.1.0 0.0.0.255 //只允许192.168.1.0网段的用户访问Internet
[Router-acl-adv-3002] quit
[Router] interface dialer 1              //链路1的NAT Outbound配置在Dialer1接口，不是物理口GE0/0/1
[Router-Dialer1] nat outbound 3002
[Router-Dialer1] quit
[Router] interface gigabitethernet 0/0/2    //链路2的NAT Outbound配置在实际使用的物理口GE0/0/2
[Router-GigabitEthernet0/0/2] nat outbound 3002
[Router-GigabitEthernet0/0/2] quit
```

步骤6 配置两条等价默认路由，通过多条等价路由来实现负载分担，并配置基于源IP地址方式进行负载分担。

```
[Router] ip route-static 0.0.0.0 0 dialer 1  //链路1的路由优先级为默认值60
[Router] ip route-static 0.0.0.0 0 10.1.1.2   //链路2的路由优先级也为默认值60，链路1和链路2为两条等价默认路由
[Router] ip load-balance hash src-ip    //基于源IP地址方式进行负载分担
[Router] quit
```

步骤7 验证配置结果。

1. 在Router上执行命令**display pppoe-client session summary**，查看PPPoE会话状态和配置信息。当“State”项显示为“UP”时，表示PPPoE会话建立成功。

   ```
   <Router> display pppoe-client session summary
   PPPoE Client Session:
   ID   Bundle  Dialer  Intf          Client-MAC    Server-MAC    State
   0    1       1       GE0/0/1       4cf95dca90ae  00e0fc030201  UP
   ```

2. 在Router上执行命令**display ip routing-table protocol static**，查看配置的静态路由表信息，路由表内有两条等价默认路由分别到运营商1和运营商2。
3. 在内网主机HostA上执行**ping**命令，Ping对端运营商网关的IP地址，模拟内网主机访问Internet。HostA能同时Ping通运营商1网关的IP地址和运营商2网关的IP地址，两条链路可以同时转发流量，实现负载分担。

----结束

配置文件

Router配置文件

```
#
 sysname Router
#
ip load-balance hash src-ip
#
acl number 3002
 rule 5 permit ip source 192.168.1.0 0.0.0.255
#
interface Dialer1
 link-protocol ppp
 ppp chap user user1@system
 ppp chap password cipher %^%#'hX'>!<#g*S(OP"3zuL<le&,6h2)g"g}#W.b,G<Z%^%#
 ppp ipcp dns admit-any
 tcp adjust-mss 1200
 ip address ppp-negotiate
 dialer user user1
 dialer bundle 1
 dialer number 1 autodial
```

 版权所有 © 华为技术有限公司

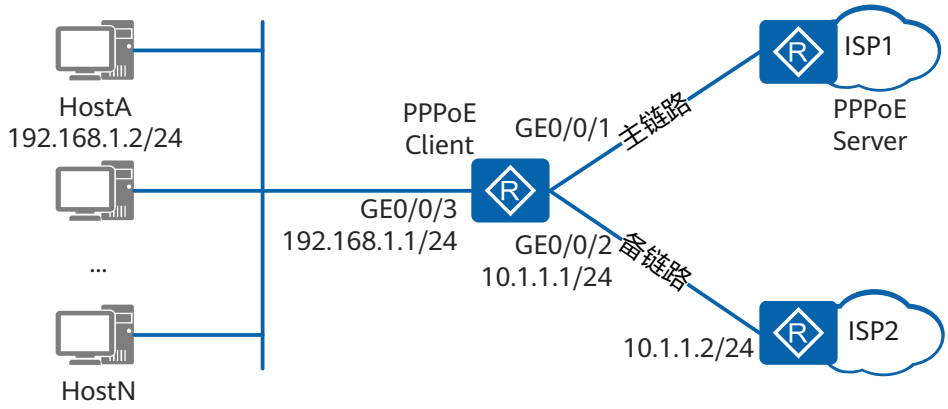
```
 nat outbound 3002
#
interface GigabitEthernet0/0/1
 undo portswitch
 pppoe-client dial-bundle-number 1
#
interface GigabitEthernet0/0/2
 undo portswitch
 ip address 10.1.1.1 255.255.255.0
 nat outbound 3002
#
interface GigabitEthernet0/0/3
 undo portswitch
 ip address 192.168.1.1 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 Dialer1
ip route-static 0.0.0.0 0.0.0.0 10.1.1.2
#
return
```

3.2.6 配置 PPPoE 拨号和静态 IP 双链路上行备份示例

组网需求

如图1所示，某小型企业内网部署了一台路由器作为接入网关，为下挂的内网用户提供访问Internet服务。为了提高网络的可靠性，企业在路由器上部署了两条链路同时接入Internet。企业希望两条链路一条为主链路，一条为备链路，主链路通过PPPoE拨号方式接入运营商1，备链路通过静态IP方式接入运营商2。当主链路发生故障时，流量可以切换到备链路上进行转发，同时通过配置NAT功能使内网用户可以访问Internet。

图 3-20 配置 PPPoE 拨号和静态 IP 双链路上行备份示例



版权所有 © 华为技术有限公司

数据准备

表 3-9 数据准备表

项目	数据	说明
运营商1分配给主链路的PPPoE用户名和密码	主链路接口：GE0/0/1 用户名：user1@system 密码：YsHsjx_202206	使用三层接口GE0/0/1作为主链路接口上行连接到Internet，且GE0/0/1通过PPPoE拨号方式自动获取IP地址。 **说明** 此处的用户名和密码为用户向运营商获取接入网络的用户名和密码。
运营商2分配给备链路的静态IP地址	备链路接口：GE0/0/2 IP地址：10.1.1.1/24	使用三层接口GE0/0/2作为备链路接口上行连接到Internet，且GE0/0/2通过手工配置方式获取静态IP地址。 **说明** 此处的IP地址为用户向运营商获取接入网络的IP地址。
备链路对端运营商2网关的IP地址	10.1.1.2/24	对端运营商2网关的IP地址用于配置路由信息，否则内网用户上网的报文无法转发到Internet。
路由器下行接口的IP地址	GE0/0/3：192.168.1.1/24	使用三层接口GE0/0/3连接企业内网用户。如果有多个内网用户需要上网，可以在路由器上下挂一个二层交换机来扩展用户个数。
内网用户HostA的IP地址	192.168.1.2/24	企业内部分配给用户的内网IP地址，用于验证内网用户访问Internet是否正常。

配置思路

1. 在路由器的Dialer1接口上配置共享DCC功能，使PPPoE Client用户可以按需拨号，节省费用。
2. 配置PPP链路的认证方式，使设备与PPPoE Server之间建立连接获取IP地址。
3. 配置PPPoE拨号方式为自动拨号，在连接断开后，设备可以自动建立拨号连接。
4. 在主链路接口GE0/0/1上建立PPPoE会话，使主链路可以通过PPPoE拨号方式接入运营商1；在备链路接口GE0/0/2上配置静态IP地址，使备链路可以通过静态IP方式接入运营商2。
5. 在两个上行接口配置Easy IP方式的NAT Outbound，使企业内网用户可以访问Internet。
6. 配置两条不同优先级的默认路由，通过优先级的高低来区分主备链路，主链路的优先级高，备链路的优先级低。

操作步骤

步骤1 在Router的Dialer1接口上配置共享DCC功能，使PPPoE Client用户可以按需拨号。

 版权所有 © 华为技术有限公司

```
<Huawei> system-view
[Huawei] sysname Router
[Router] interface dialer 1
[Router-Dialer1] dialer user user1    //启动共享DCC功能并设置对端用户名
[Router-Dialer1] dialer bundle 1
[Router-Dialer1] dialer number 1 autodial  //配置Dialer1接口拨号失败时转换为Down状态，流量切换到链路2转发
[Router-Dialer1] quit
```

步骤2 配置PPP链路的认证方式，使设备与PPPoE Server之间建立连接获取IP地址。PPP链路的认证方式有CHAP和PAP两种，请根据实际情况选择其中一种进行配置，和对端PPPoE Server的认证方式保持一致即可，本例中选择使用CHAP方式。

- 如果对端PPPoE Server使用CHAP认证，则配置PPP链路的认证方式为CHAP。

  ```
  [Router] interface dialer 1
  [Router-Dialer1] ppp chap user user1@system
  [Router-Dialer1] ppp chap password cipher YsHsjx_202206
  [Router-Dialer1] quit
  ```

- 如果对端PPPoE Server使用PAP认证，则配置PPP链路的认证方式为PAP认证。

  ```
  [Router] interface dialer 1
  [Router-Dialer1] ppp pap local-user user1@system password cipher YsHsjx_202206
  [Router-Dialer1] quit
  ```

步骤3 配置PPPoE拨号方式为自动拨号，在连接断开后，设备可以自动建立拨号连接。

```
[Router] interface dialer 1
[Router-Dialer1] ip address ppp-negotiate
[Router-Dialer1] ppp ipcp dns admit-any  //当设备通过PPP协议与其他设备相连时，若设备需要通过域名直接访问Internet，则需要配置对端设备为其分配DNS服务器地址
[Router-Dialer1] tcp adjust-mss 1200   //配置接口的TCP最大报文段长度为推荐值1200字节
[Router-Dialer1] quit
```

步骤4 在链路1接口GE0/0/1上建立PPPoE会话，使链路1可以通过PPPoE拨号方式接入运营商1；在链路2接口GE0/0/2上配置静态IP地址，使链路2可以通过静态IP方式接入运营商2。

```
[Router] interface gigabitethernet 0/0/1
[Router-GigabitEthernet0/0/1] undo portswitch    //有些二层接口需要切换成三层接口后，才可以配置PPPoE会话
[Router-GigabitEthernet0/0/1] pppoe-client dial-bundle-number 1
[Router-GigabitEthernet0/0/1] quit
[Router] interface gigabitethernet 0/0/2
[Router-GigabitEthernet0/0/2] undo portswitch    //有些二层接口需要切换成三层接口后，才可以配置IP地址
[Router-GigabitEthernet0/0/2] ip address 10.1.1.1 24  //运营商2分配给链路2的IP地址
[Router-GigabitEthernet0/0/2] quit
[Router] interface gigabitethernet 0/0/3
[Router-GigabitEthernet0/0/3] undo portswitch    //配置路由器下行连接内网接口的IP地址
[Router-GigabitEthernet0/0/3] ip address 192.168.1.1 24
[Router-GigabitEthernet0/0/3] quit
```

步骤5 在两个上行接口配置Easy IP方式的NAT Outbound，使企业内网用户可以访问Internet。

```
[Router] acl number 3002
[Router-acl-adv-3002] rule 5 permit ip source 192.168.1.0 0.0.0.255 //只允许192.168.1.0网段的用户访问Internet
[Router-acl-adv-3002] quit
[Router] interface dialer 1            //链路1的NAT Outbound配置在Dialer1接口，不是物理口GE0/0/1
[Router-Dialer1] nat outbound 3002
[Router-Dialer1] quit
[Router] interface gigabitethernet 0/0/2    //链路2的NAT Outbound配置在实际使用的物理口GE0/0/2
[Router-GigabitEthernet0/0/2] nat outbound 3002
[Router-GigabitEthernet0/0/2] quit
```

步骤6 配置两条不同优先级的默认路由，通过优先级的高低来区分主备链路，主链路的优先级高，备链路的优先级低。

```
[Router] ip route-static 0.0.0.0 0 dialer 1  //主链路的路由优先级为默认值60
[Router] ip route-static 0.0.0.0 0 10.1.1.2 preference 100   //备链路的路由优先级为100，数值越大，优先级
```

 版权所有 © 华为技术有限公司

```
越低
[Router] quit
```

步骤7 验证配置结果。

1. 在Router上执行命令**display pppoe-client session summary**，查看PPPoE会话状态和配置信息。当“State”项显示为“UP”时，表示PPPoE会话建立成功。

```
<Router> display pppoe-client session summary
PPPoE Client Session:
ID   Bundle  Dialer  Intf          Client-MAC    Server-MAC    State
0    1       1       GE0/0/1       4cf95dca90ae  00e0fc030201  UP
```

2. 在Router上执行命令**display ip routing-table protocol static**，查看配置的静态路由表信息，路由表内到运营商1的路由优先级高于到运营商2的路由优先级。
3. 在内网主机HostA上执行**ping**命令，Ping对端运营商网关的IP地址，模拟内网主机访问Internet。当主链路正常时，HostA只能Ping通运营商1网关的IP地址，当主链路故障时，HostA只能Ping通运营商2网关的IP地址，两条链路一条为主，一条为备，流量优先从主链路转发到运营商1。

----结束

配置文件

Router配置文件

```
#
 sysname Router
#
acl number 3002
 rule 5 permit ip source 192.168.1.0 0.0.0.255
#
interface Dialer1
 link-protocol ppp
 ppp chap user user1@system
 ppp chap password cipher %^%#'hX'>!<#g*S(OP"3zuL<le&,6h2)g"g}#W.b,G<Z%^%#
 ppp ipcp dns admit-any
 tcp adjust-mss 1200
 ip address ppp-negotiate
 dialer user user1
 dialer bundle 1
 dialer number 1 autodial
 nat outbound 3002
#
interface GigabitEthernet0/0/1
 undo portswitch
 pppoe-client dial-bundle-number 1
#
interface GigabitEthernet0/0/2
 undo portswitch
 ip address 10.1.1.1 255.255.255.0
 nat outbound 3002
#
interface GigabitEthernet0/0/3
 undo portswitch
 ip address 192.168.1.1 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 Dialer1
ip route-static 0.0.0.0 0.0.0.0 10.1.1.2 preference 100
#
return
```

 版权所有 © 华为技术有限公司

4 组建局域网

4.1 配置三层链路聚合增加链路带宽并提高可靠性的示例
4.2 配置划分VLAN的示例
4.3 配置子接口实现VLAN间通信的示例
4.4 配置VLANIF接口实现VLAN间通信的示例
4.5 配置GVRP实现VLAN自动注册的示例
4.6 配置透明网桥实现远程同一网段互通的示例
4.7 配置透明网桥实现远程不同网段互通的示例
4.8 配置透明网桥实现QinQ传输的示例
4.9 配置UDP Helper实现跨网用户使用主机名互访的示例
4.10 配置路由式Proxy ARP实现远程同一网段互通的示例

4.1 配置三层链路聚合增加链路带宽并提高可靠性的示例

规格

适用于所有版本的AR路由器。

组网需求

在某小型企业网环境中部署了两台AR路由器Router_1和Router_2，Router_1作为用户接入设备，Router_2作为网络接入设备。为了保证用户的带宽，当用户量较大时，可以部署多条链路或者链路聚合，达到增加链路带宽的目的，在实现增大带宽目的的同时，链路聚合采用备份链路的机制，可以有效的提高设备之间链路的可靠性。同时在链路之间实现负载分担保证业务流量的转发。具体实现如下功能：

- Router_1上接入的用户能够与Router_2信息互通。
- Router_1和Router_2之间链路带宽增加，在信息传输过程中能够实现负载分担，达到分流的目的。

 版权所有 © 华为技术有限公司

- Router_1和Router_2之间其中某条链路Down不影响信息互通，提高链路的可靠性。

图 4-1 三层链路聚合组网图

操作步骤

步骤1 Router_1的配置

```
#
 sysname Router_1
#
interface Eth-Trunk1    //创建Eth-Trunk接口，切换为三层模式，并配置IP地址
 undo portswitch
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/0    //将三层接口GE1/0/0～GE3/0/0加入到Eth-Trunk 1中
 eth-trunk 1
#
interface GigabitEthernet2/0/0
 eth-trunk 1
#
interface GigabitEthernet3/0/0
 eth-trunk 1
#
return
```

步骤2 Router_2的配置

```
#
 sysname Router_2
#
interface Eth-Trunk1
 undo portswitch
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/0
 eth-trunk 1
#
interface GigabitEthernet2/0/0
 eth-trunk 1
#
interface GigabitEthernet3/0/0
 eth-trunk 1
#
return
```

步骤3 验证配置结果

在Router_1和Router_2上执行**display eth-trunk**命令，显示GE1/0/0～GE3/0/0加入到Eth-Trunk 1中。

Router_1和Router_2能互相Ping通。

----结束

版权所有 © 华为技术有限公司

配置注意事项

- 一个Eth-Trunk接口中的成员接口必须是以太网类型和速率相同的接口。以太网类型和速率不同的接口不能加入同一个Eth-Trunk接口，如GE接口和FE接口不能加入同一个Eth-Trunk接口。
- 在手工负载分担模式下，设备支持将GE接口和XGE接口加入同一个Eth-Trunk接口中。加入后，Eth-Trunk各成员接口支持的带宽以其能够承载的带宽上限为准，如GE接口为1G，XGE接口为10G。
- 如果本端设备接口加入了Eth-Trunk，与该接口直连的对端接口也必须加入Eth-Trunk，两端才能正常通信。
- 成员接口不能配置某些业务，例如成员接口不能配置IP地址。

4.2 配置划分 VLAN 的示例

规格

适用于所有版本、所有形态的AR路由器。

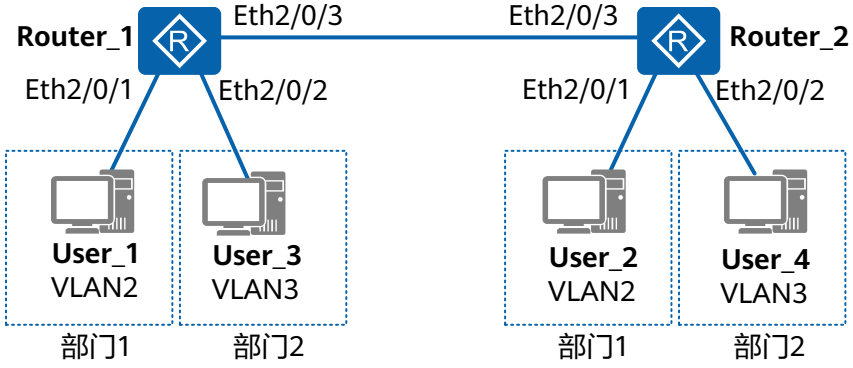
组网需求

如图4-2所示，某公司的设备连接两个部门，User_1和User_2属于部门1，但是通过不同的设备接入公司网络，User_3和User_4属于部门2，也通过不同的设备接入公司网络。

为了通信的安全性，以及避免广播报文泛滥，现要求部门内部主机能够互相通信，不同部门的主机不能互相通信。

此时，可以在设备上配置基于接口划分VLAN，连接同一部门的用户的接口划分到同一VLAN。同一VLAN内的用户可以直接互相通信，不同VLAN的用户不能直接进行二层通信。

图 4-2 划分 VLAN 组网图



操作步骤

步骤1 Router_1的配置

```
#
 sysname Router_1
#
vlan batch 2 to 3          //创建VLAN2和VLAN3
#
```


版权所有 © 华为技术有限公司

```
interface Ethernet2/0/1    //将连接User_1的接口配置为Access类型，缺省VLAN为VLAN2
 port link-type access
 port default vlan 2
#
interface Ethernet2/0/2    //将连接User_3的接口配置为Access类型，缺省VLAN为VLAN3
 port link-type access
 port default vlan 3
#
interface Ethernet2/0/3    //配置Router_1和Router_2互连的接口配置为Trunk类型，允许VLAN2和VLAN3通过
 port link-type trunk
 port trunk allow-pass vlan 2 to 3
#
return
```

步骤2 Router_2的配置

```
#
 sysname Router_2
#
vlan batch 2 to 3          //创建VLAN2和VLAN3
#
interface Ethernet2/0/1    //将连接User_2的接口配置为Access类型，缺省VLAN为VLAN2
 port link-type access
 port default vlan 2
#
interface Ethernet2/0/2    //将连接User_4的接口配置为Access类型，缺省VLAN为VLAN3
 port link-type access
 port default vlan 3
#
interface Ethernet2/0/3    //将Router_2和Router_1互连的接口配置为Trunk类型，允许VLAN2和VLAN3通过
 port link-type trunk
 port trunk allow-pass vlan 2 to 3
#
return
```

步骤3 验证配置结果

将User_1和User_2配置在一个网段，比如10.1.100.0/24；将User_3和User_4配置在一个网段，比如10.1.200.0/24。

User_1和User_2能够互相Ping通，但是均不能Ping通User_3和User_4。User_3和User_4能够互相Ping通，但是均不能Ping通User_1和User_2。

----结束

配置注意事项

- 要使链路能够传输VLAN2和VLAN3的报文，需要在设备上创建VLAN2和VLAN3，同时接口允许VLAN2和VLAN3通过。
- 设备连接用户的接口不需要区分不同VLAN，只收发Untagged帧，并为Untagged帧添加缺省VLAN的Tag，因此这些接口的类型应配置为Access。
- 设备互连的接口需要同时允许VLAN2和VLAN3的报文通过，因此这些接口的类型应配置为Trunk。

4.3 配置子接口实现 VLAN 间通信的示例

规格

适用于所有版本、所有形态的AR路由器。

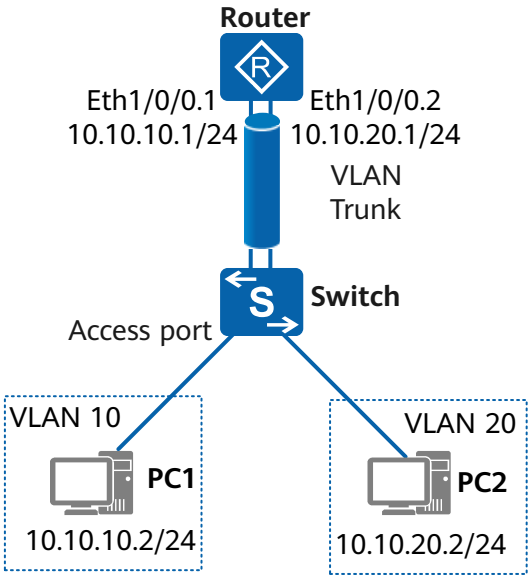
 版权所有 © 华为技术有限公司

组网需求

在某运营商用户接入场景中，当接入用户数量较多时会导致数据通信冲突严重、广播泛滥、性能显著下降甚至造成网络不可用等问题，为了有效减少以上问题，在组网中对接入的用户根据企业需要划分到不同的VLAN中，使得同VLAN之间的用户可以二层通信，不同VLAN之间的用户通过Router上的子接口进行三层通信，且广播报文限制在同VLAN之内。具体要求如下：

- 交换机通过Trunk类型接口与Router的Eth1/0/0相连，通过Access类型接口与用户PC相连。
- 用户PC1与PC2属于不同的VLAN。
- Router的Eth1/0/0创建两个子接口，子接口的IP地址为用户所在VLAN的网关地址，报文采用802.1Q方式封装。

图 4-3 子接口实现 VLAN 间通信



操作步骤

步骤1 Router的配置

```
#
 sysname Router
#
interface Ethernet1/0/0.1
 control-vid 1 dot1q-termination  //标识终结子接口，终结类型为dot1q，V200R002C01及之后版本不支持该命令
 dot1q termination vid 10  //处理VLAN ID为10的报文
 ip address 10.10.10.1 255.255.255.0  //VLAN 10的网关地址
 arp broadcast enable  //  接口可以处理ARP广播报文，V200R003C01及之后版本缺省情况下已使能ARP广播功能
#
interface Ethernet1/0/0.2
 control-vid 2 dot1q-termination
 dot1q termination vid 20  //处理VLAN ID为20的报文
 ip address 10.10.20.1 255.255.255.0  //VLAN 20的网关地址
 arp broadcast enable
```


版权所有 © 华为技术有限公司

```
#
return
```

步骤2 验证配置结果

PC1和PC2可以互相Ping通。

----结束

配置注意事项

- 交换机的下行接口连接终端，为Access类型；交换机的上行接口连接设备，为Trunk类型。
- PC上配置网关地址，网关地址为相应子接口的IP地址。
- 子接口使能ARP广播功能。
- 子接口封装的VLAN ID，和PC终端所在VLAN保持一致。

4.4 配置 VLANIF 接口实现 VLAN 间通信的示例

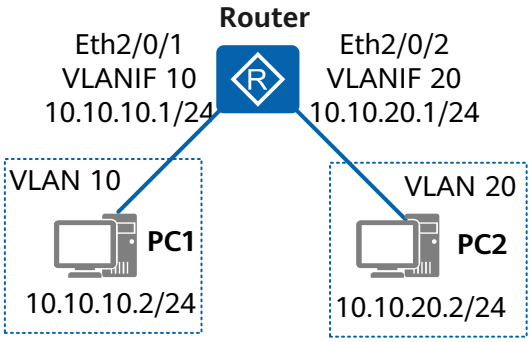
规格

适用于所有版本、所有形态的AR路由器。

组网需求

在某小型企业网内部署一台AR路由器作为用户接入设备，为用户提供上网服务。由于企业内用户数量较多时会导致数据通信冲突严重、广播泛滥、性能显著下降甚至造成网络不可用等问题，因此将企业网内用户划分为多个不同的VLAN，企业希望同属于一个VLAN的用户可以互相通信，不同VLAN之间的用户也可以通信，但是二层的广播报文要在同一个VLAN之内。

图 4-4 配置 VLANIF 接口实现 VLAN 间通信



操作步骤

步骤1 Router的配置

```
#
 sysname Router
#
vlan batch 10 20  //创建VLAN
```

 版权所有 © 华为技术有限公司

```
#
interface Vlanif10  //创建VLANIF接口
 ip address 10.10.10.1 255.255.255.0  //相同VLAN内PC终端的网关地址
#
interface Vlanif20
 ip address 10.10.20.1 255.255.255.0
#
interface Ethernet2/0/1
 port link-type access  //和PC终端相连，接口类型为Access
 port default vlan 10  //接口加入VLAN
#
interface Ethernet2/0/2
 port link-type access
 port default vlan 20
#
return
```

步骤2 验证配置结果

PC1和PC2可以互相Ping通。

----结束

配置注意事项

- 位于不同VLAN的PC终端网段不同。
- 路由器和PC终端相连的接口为二层接口，该接口类型可以是Access类型，也可使用缺省类型Hybrid。
- PC终端上配置网关地址，网关地址为相应VLANIF接口的IP地址。
- VLANIF接口的编号和VLAN ID保持一致。

相关资料

视频：配置VLAN间通信

4.5 配置 GVRP 实现 VLAN 自动注册的示例

规格

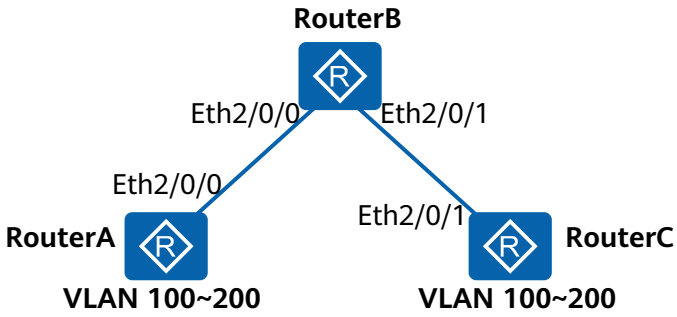
适用于所有版本、所有形态的AR路由器。

组网需求

RouterA、RouterC通过二层接口和RouterB相连，RouterA和RonterC上存在静态VLAN 100～200，要求RouterB自动学习到这些VLAN，而无需手工配置。在各台路由器全局和接口上启用GVRP，即可实现设备之间VLAN信息的动态注册和更新。

 版权所有 © 华为技术有限公司

图 4-5 通过 GVRP 实现 VLAN 自动注册



操作步骤

步骤1 RouterA的配置

```
#
 sysname RouterA
#
vlan batch 100 to 200  //创建VLAN
#
 gvrp  //全局使能GVRP功能
#
interface Ethernet2/0/0
 port link-type trunk  //接口类型修改为Trunk
 port trunk allow-pass vlan 2 to 4094  //加入所有VLAN
 gvrp  //接口使能GVRP功能
#
return
```

步骤2 RouterC的配置

```
#
 sysname RouterC
#
vlan batch 100 to 200
#
 gvrp
#
interface Ethernet2/0/1
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
 gvrp
#
return
```

步骤3 RouterB的配置

```
#
 sysname RouterB
#
 gvrp
#
interface Ethernet2/0/0
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094 //全局不需要创建VLAN，但配置了GVRP功能的端口都要加入所有VLAN
 gvrp
#
interface Ethernet2/0/1
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
```


版权所有 © 华为技术有限公司

```
 gvrp
#
return
```

步骤4 验证配置结果

在RouterB上执行命令**display vlan summary**，显示设备上学习到了VLAN 100～200，类型为**dynamic**；执行命令**display vlan brief**，显示**Eth2/0/0**和**Eth2/0/1**加入了VLAN 100～200。

----结束

配置注意事项

- 二层接口类型必须为Trunk类型。
- 使能GVRP的接口加入所有VLAN。

4.6 配置透明网桥实现远程同一网段互通的示例

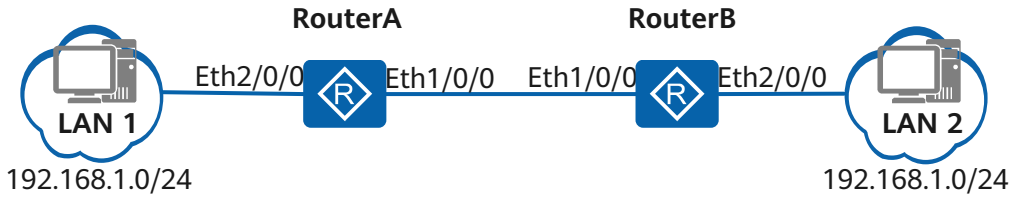
规格

适用于所有版本、所有形态的AR路由器。

组网需求

LAN 1和LAN 2中的PC终端可以通过桥接通信，不需要进行IP路由，从而达到透过广域网，进行网上邻居的直接访问和其他应用。

图 4-6 远程同一网段的桥接组网图



操作步骤

步骤1 RouterA的配置

```
#
 sysname RouterA
#
bridge 1  //创建网桥组，生成虚拟网桥
#
interface Ethernet1/0/0
 bridge 1  //接口加入网桥组，作为虚拟网桥的接口
#
interface Ethernet2/0/0
 bridge 1  //接口加入网桥组，作为虚拟网桥的接口
#
return
```

 版权所有 © 华为技术有限公司

步骤2 RouterB的配置

```
#
 sysname RouterB
#
bridge 1
#
interface Ethernet1/0/0
 bridge 1
#
interface Ethernet2/0/0
 bridge 1
#
return
```

步骤3 验证配置结果

LAN 1中的PC终端和LAN 2中的PC终端可以互相ping通。

----结束

配置注意事项

- 加入网桥组的接口为三层接口，三层接口除了以太类型，还有ATM、Serial等其他类型。
- LAN 1和LAN 2中的PC终端在同一网段。

4.7 配置透明网桥实现远程不同网段互通的示例

规格

适用于所有版本、所有形态的AR路由器。

组网需求

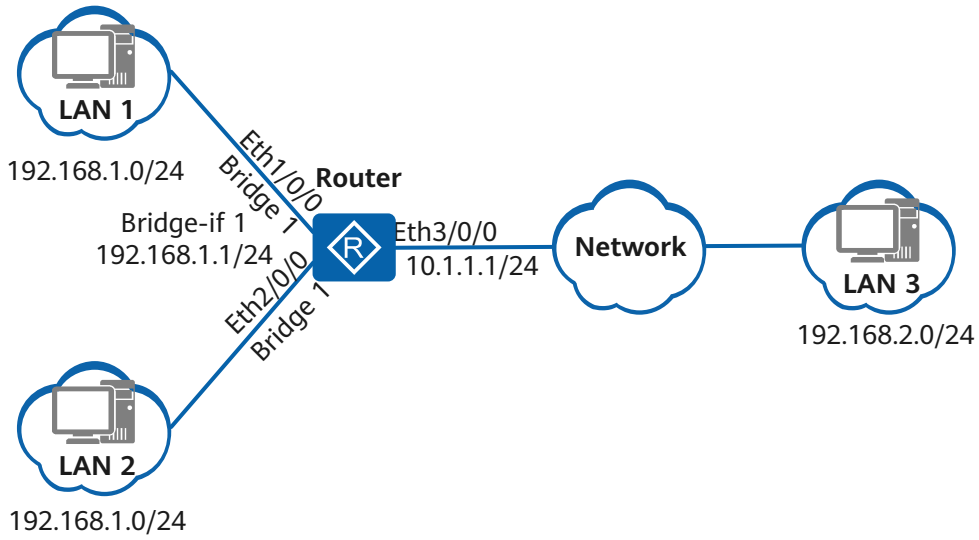
LAN 1和LAN 2网段相同，Router已配置到达LAN 3的路由。

将路由器的Eth1/0/0和Eth2/0/0加入相同的网桥组，LAN 1和LAN 2可以互通。

在路由器上创建网桥组虚接口Bridge-if 1，LAN 1和LAN 2通过网桥组虚接口路由转发报文，实现和LAN 3的通信。

 版权所有 © 华为技术有限公司

图 4-7 网桥组虚接口路由转发组网图



操作步骤

步骤1 Router的配置

```
#
 sysname Router
#
bridge 1  //创建网桥组，生成虚拟网桥
 routing ip  //使能网桥组对IP协议报文的路由功能
#
interface Ethernet1/0/0
 bridge 1  //接口加入网桥组，作为虚拟网桥的接口
#
interface Ethernet2/0/0
 bridge 1
#
interface Ethernet3/0/0
 ip address 10.1.1.1 255.255.255.0
#
interface Bridge-if1  //创建网桥组虚接口，绑定虚拟网桥的接口
 ip address 192.168.1.1 255.255.255.0  //用于IP路由转发，实际转发接口为虚拟网桥的接口
#
ip route-static 192.168.2.0 255.255.255.0 10.1.1.2
#
return
```

步骤2 验证配置结果

LAN 1和LAN 2中的PC终端可以互相ping通。

LAN 1和LAN 2中的PC终端可以ping通LAN 3中的PC终端。

----结束

配置注意事项

- 加入网桥组的接口必须是三层接口，三层接口除了以太类型，还有ATM、Serial等其他类型。
- LAN 1和LAN 2中的PC终端在同一网段。

版权所有 © 华为技术有限公司

- 创建的网桥组虚接口编号和网桥组编号保持一致。

4.8 配置透明网桥实现 QinQ 传输的示例

规格

适用于所有版本、所有形态的AR路由器。

组网需求

某企业有多个部门分布在不同的地区，由于业务发展的需要，不同区域的部门与部门之间有进行带有VLAN Tag的报文的传输需求。采用透明网桥的远程桥接和QinQ功能，可以实现企业在不同区域部门之间进行传输带有VLAN Tag的报文。

如图4-8所示，两个网桥Router_A和Router_B分布在不同地点，并通过中间链路连接。主机PC1和PC2属于不同局域网，通过透明网桥的远程桥接和QinQ功能实现不同地理位置主机之间透明传输添加VLAN Tag的报文。

图 4-8 透明网桥实现 QinQ 传输的组网图

操作步骤

步骤1 Router_A的配置

以Router_A为例。Router_B的配置与之类似，不再重复介绍。

```
#
vlan batch 2 to 4094
#
bridge 1                        //创建网桥组，生成虚拟网桥
#
interface GigabitEthernet0/0/1
 bridge 1                       //将LAN侧接口加入到bridge 1
 bridge vlan-transmit enable        //使能网桥组接口透明传输VLAN ID功能
#
interface GigabitEthernet0/0/2
 undo portswitch
 ip address 2.2.2.2 255.255.255.0
#
interface GigabitEthernet0/0/2.1
 bridge 1                       //将WAN侧子接口加入到bridge 1
 bridge vlan-transmit enable        //使能网桥组接口透明传输VLAN ID功能
 vlan allow-pass vid 3105           //配置子接口允许通过的VLAN
 vlan dot1q-tunnel 3105             //配置子接口的dot1q-tunnel功能
#
return
```

步骤2 验证配置结果

PC1和PC2可以互相Ping通。

----结束

版权所有 © 华为技术有限公司

配置注意事项

当WAN侧接口类型为VDSL或者G.SHDSL时，需先执行**set workmode slot** *slot-id* **vdsl ptm**或者**set workmode slot** *slot-id* **shdsl ptm**命令配置接口的工作模式为PTM。

4.9 配置 UDP Helper 实现跨网用户使用主机名互访的示例

规格

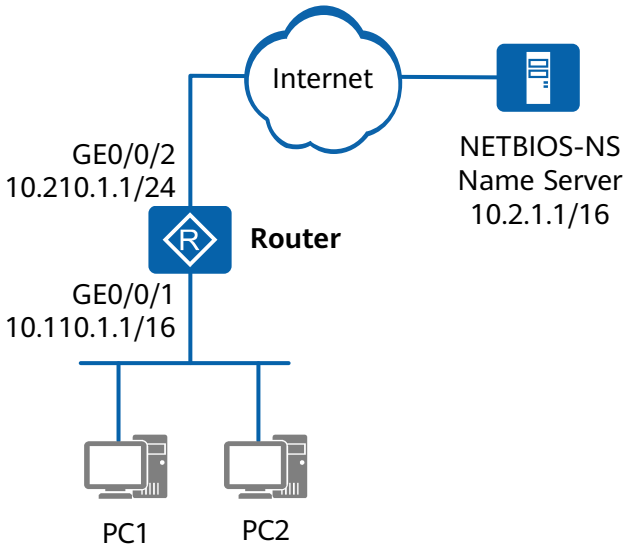
适用于所有版本、所有形态的AR路由器。

组网需求

如图4-9所示，Router的接口GE0/0/1的IP地址为10.110.1.1/16，接口GE0/0/2的IP地址为10.210.1.1/24。NetBIOS-NS name服务器的IP地址为10.2.1.1/16，Router与NetBIOS-NS name服务器不在同一网段。Router到10.2.0.0/16的下一跳地址为10.210.1.2/24。

配置将目的UDP端口号为137、目的IP地址为255.255.255.255和10.110.255.255的广播UDP报文中继转发到指定的目的NetBIOS-NS name服务器上。这样如果Router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。

图 4-9 配置 UDP Helper 组网图



操作步骤

步骤1 Router的配置

```
#
 udp-helper enable  //使能Router的UDP Helper功能
#
interface GigabitEthernet0/0/1
 ip address 10.110.1.1 255.255.0.0
```


版权所有 © 华为技术有限公司

```
 udp-helper server 10.2.1.1  //配置中继转发的目的服务器
#
interface GigabitEthernet0/0/2
 ip address 10.210.1.1 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 10.210.1.2  //配置默认路由，保证UDP Helper和目的服务器路由可达
#
```

步骤2 验证配置结果

在Router上执行**display udp-helper server**命令查看UDP Helper配置的目的服务器。

在Router上执行**display udp-helper port**命令查看已经配置的需要中继转发的UDP报文的目的端口号信息。

----结束

配置注意事项

- 全局使能UDP Helper功能。
- UDP Helper和目的服务器路由可达。

4.10 配置路由式 Proxy ARP 实现远程同一网段互通的示例

规格

适用于所有版本、所有形态的AR路由器。

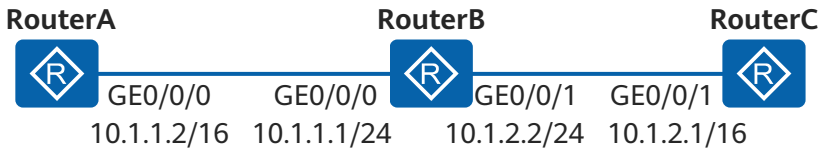
组网需求

企业内部进行子网划分时，可能会出现两个子网网络属于同一网段，但是却不属于同一物理网络的情况，两个子网网络间被路由器分隔。这时可以通过修改网络内主机的路由信息，使发往其它子网的数据先发送到连接不同子网的网关设备上，再由网关设备转发此数据报文。但是这种解决方案需要配置子网中所有主机的路由，并不便于管理和维护。

在网关上部署路由式Proxy ARP功能，可以有效解决子网划分带来的管理和维护方面的问题。路由式Proxy ARP的功能可以使IP地址属于同一网段却不属于同一物理网络的主机间能够相互通信，并且主机上不需要配置缺省网关，便于管理和维护。

如图4-10所示。RouterB通过接口10.1.1.1/24和10.1.2.2/24连接RouterA和RouterC，接口10.1.1.1/24和接口10.1.2.2/24的IP地址不在同一个网段。RouterA内的主机10.1.1.2/16与接口10.1.1.1/24的IP地址在同一网段，RouterC内的主机10.1.2.1/16与接口10.1.2.2/24的IP地址在同一网段，RouterA内的主机10.1.1.2/16与RouterC内的主机10.1.2.1/16的IP地址也在同一网段。RouterA和RouterC上未配置缺省网关。在RouterB上配置路由式Proxy ARP可以使RouterA和RouterC内主机间相互通信。

图 4-10 配置 Proxy ARP 功能组网图



 版权所有 © 华为技术有限公司

操作步骤

步骤1 RouterA上的配置

```
#
interface GigabitEthernet0/0/0
 ip address 10.1.1.2 255.255.0.0
#
```

步骤2 RouterB上的配置

```
#
interface GigabitEthernet0/0/0
 ip address 10.1.1.1 255.255.255.0
 arp-proxy enable
#
interface GigabitEthernet0/0/1
 ip address 10.1.2.2 255.255.255.0
 arp-proxy enable
#
```

步骤3 RouterC上的配置

```
#
interface GigabitEthernet0/0/1
 ip address 10.1.2.1 255.255.0.0
#
```

步骤4 验证配置结果

在RouterB上使能代理ARP功能后，在RouterA上ping 10.1.2.1，发现可以ping通。在RouterB上执行**display arp**，查看其ARP表项如下：

```
<RouterB> display arp
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE       INTERFACE   VPN-INSTANCE
                                VLAN/CEVLAN PVC
--------------------------------------------------------------------------------
10.1.1.2        00e0-fc74-b8b2  7         D-0        GE0/0/0
10.1.1.1        00e0-fc74-b86f            I -        GE0/0/0
10.1.2.1        00e0-fc74-b8b0  20        D-0        GE0/0/1
10.1.2.2        00e0-fc74-b87f            I -        GE0/0/1
--------------------------------------------------------------------------------
Total:4         Dynamic:2       Static:0    Interface:2
```

----结束

 版权所有 © 华为技术有限公司

5 通过专线实现广域网互联

5.1 配置端口隔离示例
5.2 配置POS接口示例
5.3 配置CPOS接口示例
5.4 配置ATM接口示例
5.5 配置银行网点通过E1链路接入二级分行示例（E1模式）
5.6 配置银行网点通过E1链路接入二级分行示例（CE1模式）
5.7 配置企业采用3G链路访问互联网示例（通过WCDMA网络）
5.8 配置企业通过LTE链路接入Internet示例
5.9 配置IPoA实现局域网接入Internet的示例
5.10 配置IPoEoA实现局域网接入Internet的示例
5.11 配置PPPoEoA实现用户利用PPP协议接入Internet的示例
5.12 配置PPPoA实现用户利用PPP协议接入Internet的示例
5.13 配置帧中继专线利用PPP协议实现局域网互联的示例
5.14 配置帧中继专线利用IP协议实现局域网互联的示例
5.15 配置采用MP-Group进行MP绑定示例
5.16 配置将PPP链路直接绑定到VT上实现MP的示例
5.17 配置按照用户名查找虚拟接口模板实现MP的示例
5.18 配置设备作为PPPoE Client，实现设备接入Internet的示例
5.19 配置设备作为PPPoE Client（IPv6），实现设备接入Internet的示例
5.20 配置设备作为PPPoE Server，实现用户安全接入Internet的示例
5.21 配置设备利用PPPoE技术通过外置的ADSL Modem接入Internet的示例
5.22 配置设备通过Modem拨号接入PSTN的示例(轮询DCC方式)
5.23 配置设备通过ISDN PRI接口拨号接入ISDN的示例（共享DCC方式）

版权所有 © 华为技术有限公司

5.24 配置设备利用HDLC技术实现互通的示例

5.1 配置端口隔离示例

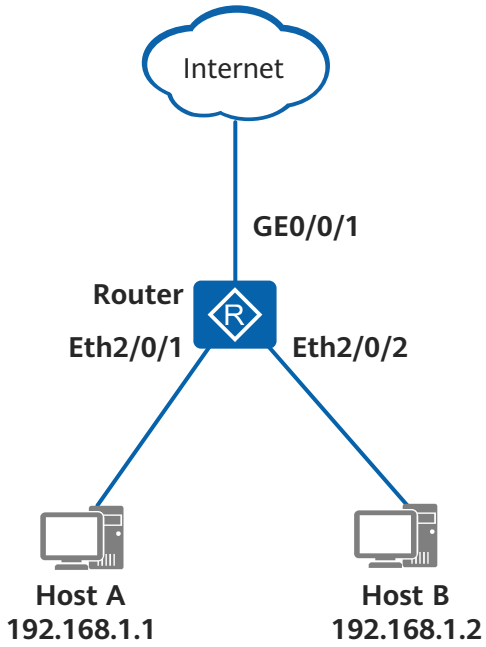
规格

适用于所有版本的AR路由器。

组网需求

如图5-1所示，小区用户Host A、Host B分别与Router的端口Eth2/0/1、Eth2/0/2相连，Router通过GE0/0/1端口与外部网络相连。现需要实现小区用户Host A和Host B之间二层报文不能互通，但可以和外部网络通信。

图 5-1 配置端口隔离组网图



操作步骤

步骤1 配置Router

```
#
 sysname Router
#
interface Ethernet2/0/1
 port-isolate enable group 1        //使能端口隔离功能，默认加入的端口隔离组为1
#
interface Ethernet2/0/2
 port-isolate enable group 1        //使能端口隔离功能，默认加入的端口隔离组为1
#
return
```

步骤2 验证配置结果

版权所有 © 华为技术有限公司

在Router上执行命令**display port-isolate group all**查看端口隔离组的配置信息，可以看到端口Eth2/0/1、Eth2/0/2已经加入端口隔离组1。

Host A和Host B不能互相Ping通。

----结束

配置注意事项

- 同一端口隔离组的接口之间互相隔离，不同端口隔离组的接口之间不隔离。
- 使能端口隔离功能时，如果不指定**group** *group-id*参数，默认加入的端口隔离组为1。
- 缺省情况下，端口隔离模式为二层隔离三层互通。执行命令**port-isolate mode all**，可以配置二层三层都隔离的模式。

5.2 配置 POS 接口示例

规格

适用于V200R003C00及更高版本、支持POS接口的AR路由器。

组网需求

如图5-2所示，两台设备通过SONET网络相连，RouterB已经完成配置，为了保证对接成功，需要完成RouterA的POS接口配置。

已知RouterB的POS接口物理参数：

- 帧格式为SONET
- 链路层协议为HDLC
- 时钟模式为从时钟模式
- MTU值为1200字节
- 对载荷数据不加扰
- CRC校验字长度为16位
- 开销字节c2为3，j0和j1都按16字节模式取值，其中，j0为abc，j1为xyz

图 5-2 配置 POS 接口物理参数的组网图

操作步骤

步骤1 配置RouterA

```
#
 sysname RouterA
```

```
#
interface Pos2/0/0
 link-protocol hdlc    //配置POS接口的链路层协议为HDLC
 mtu 1200    //配置POS接口的MTU值为1200字节
 ip address 10.1.1.1 255.255.255.252
 flag c2 3    //配置POS接口的开销字节c2为3
 flag j0 16byte-mode abc    //配置POS接口的开销字节j0按16字节模式取值，为abc
 flag j1 16byte-mode xyz    //配置POS接口的开销字节j1按16字节模式取值，为xyz
 frame-format sonet    //配置POS接口的帧格式为SONET
 undo scramble    //配置POS接口对载荷数据不加扰
 crc 16    //配置POS接口的CRC校验字长度为16位
#
return
```

步骤2 验证配置结果

在RouterA上执行命令**display interface pos**查看RouterA的POS接口连通状态。

RouterA和RouterB能够互相Ping通。

----结束

配置注意事项

保证两端设备POS接口的配置一致，否则会导致对接不成功。

5.3 配置 CPOS 接口示例

规格

适用于V200R001C01及更高版本、支持CPOS接口的AR路由器。

组网需求

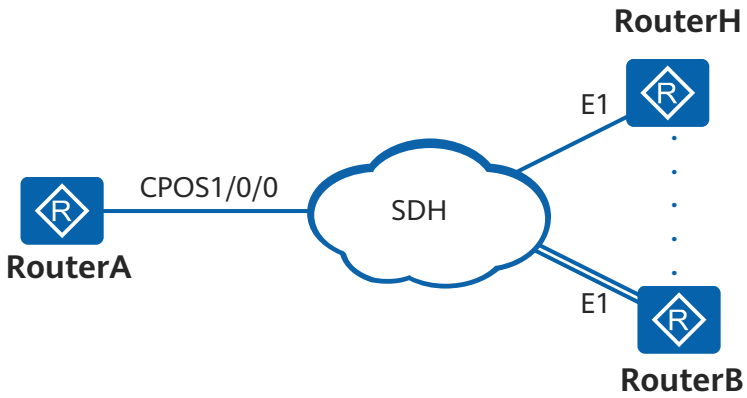
如图5-3所示，RouterA节点下属有RouterB～RouterH七个分支节点，每个分支节点设备通过E1线路上行连接到RouterA，RouterA通过CPOS接口汇聚上行的E1线路。

RouterB分支节点进行了扩容后，一条E1线路满足不了需求，因此添加了一条E1线路。要求用MP-Group接口的方式，对这两条E1线路进行捆绑。

已知：

- RouterA使用来自SDH网络的时钟。
- RouterA的CPOS接口的帧格式是SDH，AUG复用路径为au-4。

图 5-3 配置 CPOS 接口汇聚接入 E1 线路组网图



版权所有 © 华为技术有限公司

操作步骤

步骤1 配置RouterA

```
#
 sysname RouterA
#
interface Mp-group0/0/1    //创建并配置MP-Group
 ip address 10.10.10.1 255.255.255.0    //配置MP-Group的IP地址
#
controller cpos 1/0/0
 e1 1 unframed    //配置E1通道1工作在非通道化模式
 e1 2 unframed    //配置E1通道2工作在非通道化模式
 e1 1 set clock master    //配置E1通道1使用主时钟模式，与对端E1-F接口的时钟模式不同
 e1 2 set clock master    //配置E1通道2使用主时钟模式，与对端E1-F接口的时钟模式不同
#
interface Serial1/0/0/1:0    //进入E1通道1生成的逻辑通道
 link-protocol ppp
 ppp mp mp-group 0/0/1    //配置通道接口Serial1/0/0/1:0加入MP-Group
#
interface Serial1/0/0/2:0    //进入E1通道2生成的逻辑通道
 link-protocol ppp
 ppp mp mp-group 0/0/1    //配置通道接口Serial1/0/0/2:0加入MP-Group
#
return
```

步骤2 配置RouterB

```
#
 sysname RouterB
#
interface Mp-group0/0/1    //创建并配置MP-Group
 ip address 10.10.10.2 255.255.255.0    //配置MP-Group的IP地址
#
interface Serial1/0/0
 fe1 unframed    //配置E1-F接口工作在非成帧方式
 link-protocol ppp
 ppp mp mp-group 0/0/1    //配置物理接口Serial1/0/0加入MP-Group
#
interface Serial2/0/0
 fe1 unframed    //配置E1-F接口工作在非成帧方式
 link-protocol ppp
 ppp mp mp-group 0/0/1    //配置物理接口Serial2/0/0加入MP-Group
#
return
```

步骤3 验证配置结果

在RouterA上执行命令**display controller cpos 1/0/0 e1 1**查看CPOS1/0/0的1号E1通道的状态信息。

在RouterA上执行命令**display interface mp-group**查看RouterA MP-Group接口的状态信息。

RouterA和RouterB能够互相Ping通。

----结束

配置注意事项

CPOS接口形成E1通道的线路属性必须与对端设备E1线路的属性保持一致。

 版权所有 © 华为技术有限公司

相关信息

视频

如何配置CPOS接口

5.4 配置 ATM 接口示例

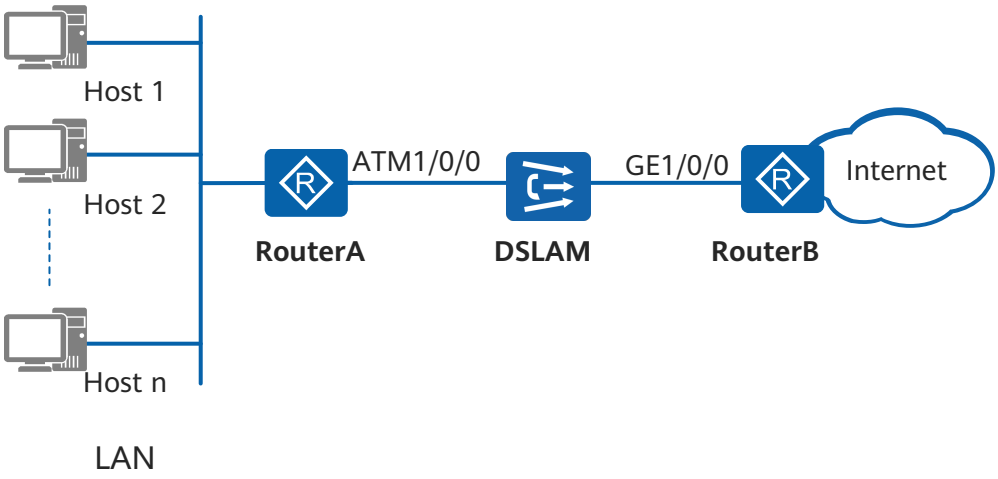
规格

适用于V200R001C00及更高版本、支持ATM接口的AR路由器。

组网需求

RouterA的ATM1/0/0连接DSLAM设备。RouterB的GE1/0/0连接DSLAM设备。要求RouterA采用IPoA应用方式与RouterB通信。

图 5-4 配置 IPoA 组网图



操作步骤

步骤1 RouterA的配置

```
#
interface Atm1/0/0
 ip address 1.1.0.1 255.255.255.0    //配置RouterA ATM1/0/0的IP地址
 pvc 0/35    //创建PVC，进入PVC视图
  map ip 1.1.0.2    //配置PVC上的IPoA映射
#
return
```

步骤2 RouterB的配置

```
#
interface GigabitEthernet1/0/0
 ip address 1.1.0.2 255.255.255.0    //配置RouterB GE1/0/0的IP地址
#
return
```

步骤3 配置DSLAM设备

版权所有 © 华为技术有限公司

具体步骤请参考具体DSLAM设备的产品手册。

步骤4 验证配置结果

RouterA能Ping通RouterB。

----结束

5.5 配置银行网点通过 E1 链路接入二级分行示例（E1 模式）

规格

适用于所有版本的AR路由器。

组网需求

如图5-5所示，某银行网点租用运营商E1链路与二级分行的汇聚设备相连，实现该网点与二级分行之间的互联互通。已知该E1链路使用全部32个时隙，封装PPP协议，使用CHAP认证。

图 5-5 配置银行网点通过 E1 链路接入二级分行组网图

操作步骤

步骤1 配置Router

```
#
controller e1 1/0/0   //进入E1的controller接口
 using e1     //配置接口模式为E1模式
#
interface serial 1/0/0:0       //进入虚拟生成的Serial接口
 link-protocol ppp      //配置PPP封装
 ip address 2.2.2.2 255.255.255.0
 ppp chap user user1       //配置CHAP认证使用的用户名
 ppp chap password cipher %@%@#0p7U*q6k~qRN7$#9'oY&\z&%@%@       //配置CHAP认证使用的密码
#
return
```

步骤2 验证配置结果

使用**display interface serial**命令查看Serial接口的状态，发现接口的物理层和链路层的状态都为Up。

向对端发起Ping测试，发现可以Ping通对端，说明双方链路是互通的。

----结束

版权所有 © 华为技术有限公司

配置注意事项

- 运营商广域网链路类型丰富，与路由器E1口对接的线缆接口可能有多种情况，还可能需要通过协议转换器做协议转换。这样用户就需要根据实际情况，选择合适的线缆接头和转接头。

  说明

  设备支持的E1/T1线缆详细信息请参考《NetEngine AR路由器 硬件描述 线缆》的E1/T1线缆。
- PPP认证有PAP认证和CHAP认证两种，配置PPP认证可以提高链路安全性。由于E1链路一般为运营商专线，有安全性保障，所以通常E1链路不配置PPP认证。是否配置PPP认证需要客户根据需求进行选择。
- 配置PPP认证时，路由器作为被认证方。

相关资料

视频：**AR系列路由器如何配置E1接口**

5.6 配置银行网点通过 E1 链路接入二级分行示例（CE1 模式）

规格

适用于所有版本的AR路由器。

组网需求

如图5-6所示，某银行网点租用运营商E1链路与二级分行的汇聚设备相连，实现该网点与二级分行之间的互联互通。已知该E1链路使用时隙1、10-16和18，封装PPP协议，使用CHAP认证。

图 5-6 配置银行网点通过 E1 链路接入二级分行组网图

操作步骤

步骤1 配置Router

```
#
controller e1 1/0/0   //进入E1的controller接口
 using ce1    //配置E1接口工作在CE1模式
 channel-set 1 timeslot-list 1,10-16,18   //将时隙1、10-16和18捆绑为1号通道口
#
interface serial 1/0/0:1     //进入虚拟生成的Serial接口，接口编号1/0/0:1的：1代表1号通道口
 link-protocol ppp
 ip address 2.2.2.2 255.255.255.0
 ppp chap user user1          //配置CHAP认证使用的用户名
 ppp chap password cipher %@%@#0p7U*q6k~qRN7$#9'oY&\z&%@%@   //配置CHAP认证使用的密码
```

 版权所有 © 华为技术有限公司

```
#
return
```

步骤2 验证配置结果

使用**display interface serial**命令查看Serial接口的状态，发现接口的物理层和链路层的状态都为Up。

向对端发起Ping测试，发现可以Ping通对端，说明双方链路是互通的。

----结束

配置注意事项

- 运营商广域网链路类型丰富，与路由器E1口对接的线缆接口可能有多种情况，还可能需要通过协议转换器做协议转换。这样用户就需要根据实际情况，选择合适的线缆接头和转接头。

  说明

  设备支持的E1/T1线缆详细信息请参考《NetEngine AR路由器 硬件描述 线缆》的E1/T1线缆。
- PPP认证有PAP认证和CHAP认证两种，配置PPP认证可以提高链路安全性。由于E1链路一般为运营商专线，有安全性保障，所以通常E1链路不配置PPP认证。是否配置PPP认证需要客户根据需求进行选择。
- 配置PPP认证时，路由器作为被认证方。

相关资料

视频：**AR系列路由器如何配置CE1接口**

5.7 配置企业采用 3G 链路访问互联网示例（通过 WCDMA 网络）

规格

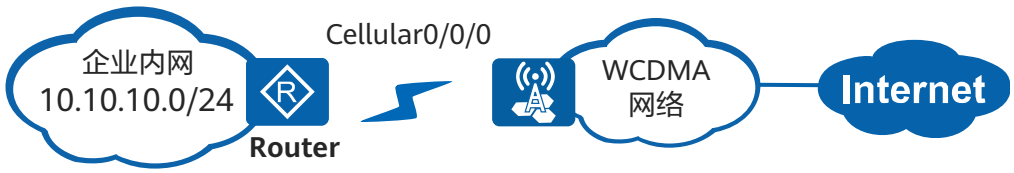
适用于V200R001C01及其以后版本的AR路由器。

组网需求

企业租用有线链路成本高、难度大，因此选择使用3G链路来访问互联网。

如图5-7所示，Router下行连接企业内网用户，上行使用3G链路拨号接入Internet，满足内网用户访问互联网的需求。

图 5-7 配置企业采用 3G 链路访问互联网组网图



版权所有 © 华为技术有限公司

操作步骤

步骤1 配置Router

```
#
dialer-rule  //配置触发拨号的规则
 dialer-rule 1 ip permit  //配置允许所有IP报文触发拨号
#
acl number 3002  //配置ACL
 rule 5 permit ip source 10.10.10.0 0.0.0.255  //表示允许来自内网网段的报文通过该ACL的过滤
#
apn profile 3gnet  //创建APN模板
 user name 3guser password cipher %@%@Gy-Z:-sDMYJ`qiLe/gJG)}hP%@%@ authentication-mode
chap  //配置接入外部PDN网络用户的用户名、密码和认证方式
 apn 3GNET  //配置APN。APN的获取需要咨询网络运营商
#
interface Cellular0/0/0
 link-protocol ppp
 mode wcdma wcdma-precedence  //配置接入WCDMA网络的方式是wcdma-precedence，此外还有gsm-
only、gsm-precedence和wcdma-only方式
 ppp ipcp dns request  //配置PPP协商DNS服务器地址
 ip address ppp-negotiate  //配置PPP协商IP地址。V200R005C00及其以后版本，推荐使用ip address
negotiate命令来自动获取IP地址
 dialer-group 1  //配置触发拨号的规则关联3G接口
 dialer enable-circular  //使能轮询DCC
 dialer number *99# autodial  //配置采用自动拨号方式向运营商网络拨号。不同运营商有不同的拨号串，只有
获取正确的拨号串，才能拨号成功
 dialer timer autodial 10  //配置自动拨号的时间间隔为10秒，即每隔10秒，3G链路自动拨号一次
 apn-profile 3gnet  //在3G接口上绑定APN模板，CHAP认证和APN才会生效
 nat outbound 3002  //配置NAT Outbound功能
#
ip route-static 0.0.0.0 0.0.0.0 Cellular0/0/0  //配置静态路由，出接口为3G接口，以便流量能够通过3G接口传输
到外网
#
return
```

步骤2 验证配置结果

执行**display interface cellular**命令查看接口的详细信息，当接口上有流量传送时，可以看到接口的物理层和链路层的状态都是Up状态，PPP的LCP和IPCP都是opened状态，以及3G接口成功获取IP地址。

----结束

配置注意事项

- 配置APN，在不同版本有不同的方法：
  - V200R005C00之前版本，假如APN为3GNET，在3G接口下执行**profile create**命令创建参数描述模板并手动配置APN，显示如下：
    ```
    #
    interface Cellular0/0/0
     profile create 1 static 3GNET
    ```
  - V200R005C00及其之后版本，假如APN为3GNET，需要先创建APN模板，然后在APN模板中配置APN为3GNET，最后在3G接口下绑定APN模板，显示如下：
    ```
    #
    apn profile 3gnet
     apn 3GNET
    #
    interface Cellular0/0/0
     apn-profile 3gnet
    ```
- 配置CHAP认证时，路由器作为被认证方。在3G接口下配置CHAP认证，在不同版本有不同方法：

 版权所有 © 华为技术有限公司

- V200R005C00之前版本，在3G接口下执行**ppp chap user**命令和**ppp chap password**命令分别配置CHAP认证的用户名和密码，显示如下：

```
#
interface Cellular0/0/0
 ppp chap user 3guser
 ppp chap password cipher %@%@9eCPJjmQR!gQxf6@q%.;,u5q%@%@
```

- V200R005C00及其之后版本，需要先创建APN模板，然后在APN模板中配置接入外部PDN网络用户的用户名、密码认证方式，最后在3G接口下绑定APN模板，显示如下：

```
#
apn profile 3gnet
 user name 3guser password cipher %@%@Gy-Z:-sDMYJ`qiLe/gJG)}hP%@%@ authentication-mode chap
#
interface Cellular0/0/0
 apn-profile 3gnet
```

- 如果配置了自动拨号，则路由器正常启动后，3G链路会一直保持连接状态，这样，会消耗更多的3G网络流量。因此，用户应根据具体情况来选择是否需要配置自动拨号。

5.8 配置企业通过 LTE 链路接入 Internet 示例

规格

适用于所有版本、支持LTE Cellular接口的AR路由器。

组网需求

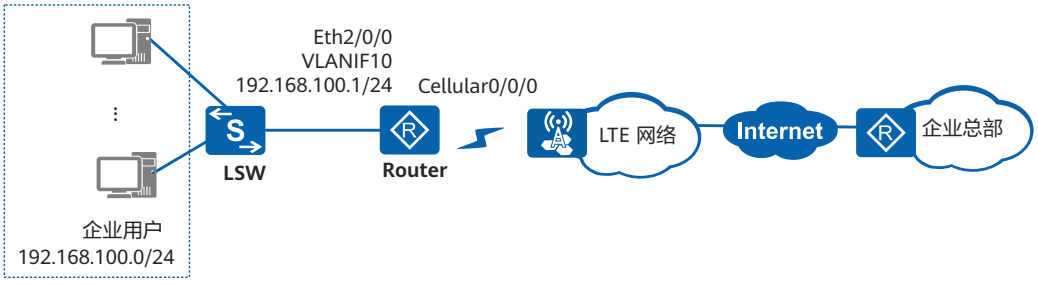
企业的某个分支位于偏远区域，无法获取有线广域接入服务，但该分支需要与外界进行较大流量的业务传输。如图5-8所示，为了满足业务传输的需求，该分支使用Router作为出口网关，使用LTE Cellular接口通过LTE网络接入Internet。

分支内网所属网段为192.168.100.0/24，主机都加入VLAN10，该分支希望Router能够为该分支内网用户分配IP地址，并且希望内网用户可以访问外网。

该企业分支办理了包年业务，采用自动拨号方式接入Internet，从运营商获取到的信息如下：

- APN为3gnet
- 拨号串为*99#

图 5-8 企业通过 LTE 链路接入 Internet 组网图



版权所有 © 华为技术有限公司

操作步骤

步骤1 Router的配置

```
#
vlan batch 10    //创建VLAN10
#
dhcp enable    //使能DHCP功能
#
acl number 3002    //配置进行NAT的ACL
 rule 5 permit ip source 192.168.100.0 0.0.0.255
#
ip pool ltepool    //创建全局地址池ltepool
 gateway-list 192.168.100.1    //配置出口网关
 network 192.168.100.0 mask 255.255.255.0    //配置全局地址池的地址范围
#
interface Vlanif10
 ip address 192.168.100.1 255.255.255.0    //配置接口的IP地址
 dhcp select global    //使能接口采用全局地址池的DHCP服务器功能
#
interface Ethernet2/0/0    //将Eth2/0/0接口加入VLAN10
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface Cellular0/0/0
 dialer enable-circular    //使能轮询DCC功能
 apn-profile lteprofile    //在Cellular接口上绑定名称为lteprofile的APN模板
 dialer number *99# autodial    //配置到达对端的拨号串，接口根据拨号串自动拨号
 nat outbound 3002    //配置Easy IP方式的NAT Outbound
 ip address negotiate    //配置Cellular接口动态获取IP地址
#
apn profile lteprofile    //创建名称为lteprofile的APN模板
 apn 3gnet    //在APN模板中配置APN为3gnet
#
ip route-static 0.0.0.0 0.0.0.0 Cellular0/0/0    //配置缺省路由，指定出接口为Cellular0/0/0
#
return
```

步骤2 验证配置结果

在Router上执行命令**display interface cellular 0/0/0**查看接口的详细信息，当接口上有流量传送时，可以看到接口的物理状态和链路层协议状态都是Up。

在Router上执行命令**display cellular 0/0/0 all**查看LTE数据卡的呼叫连接信息，可以看到APN为3gnet、无线网络类型为Automatic以及网络连接方式为LTE(LTE)。

----结束

配置注意事项

- APN和拨号串的获取需要咨询当地运营商。
- 配置APN后，APN会记录在LTE数据卡中，以后会一直存在。如果APN值变化，需要重新配置。

5.9 配置 IPoA 实现局域网接入 Internet 的示例

规格

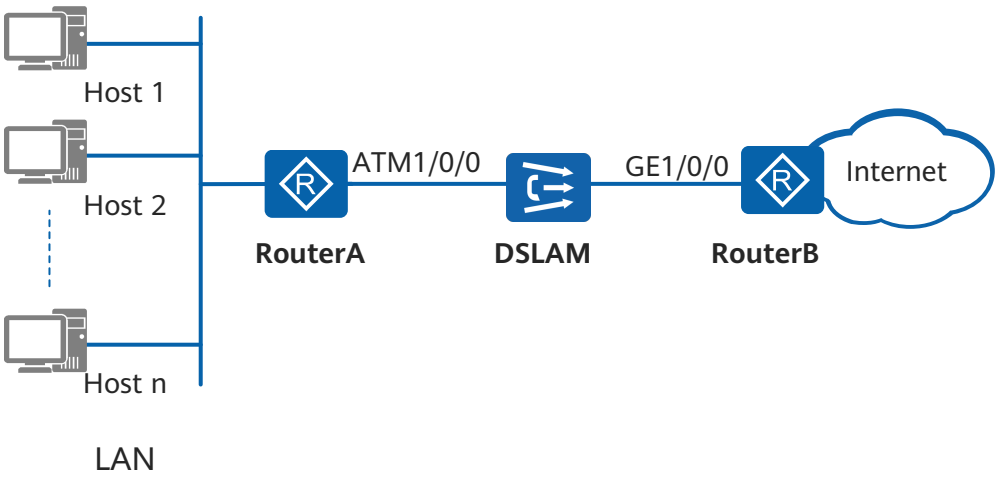
适用于所有版本的AR路由器。

 版权所有 © 华为技术有限公司

组网需求

RouterA的ATM1/0/0连接DSLAM设备。RouterB的GE1/0/0连接DSLAM设备。要求RouterA采用IPoA应用方式与RouterB通信。

图 5-9 配置 IPoA 组网图



操作步骤

步骤1 RouterA的配置

```
#
interface Atm1/0/0
 ip address 1.1.0.1 255.255.255.0 //配置RouterA ATM1/0/0的IP地址
 pvc 0/35 //创建PVC，进入PVC视图
  map ip 1.1.0.2 //配置PVC上的IPoA映射
#
return
```

步骤2 RouterB的配置

```
#
interface GigabitEthernet1/0/0
 ip address 1.1.0.2 255.255.255.0 //配置RouterB GE1/0/0的IP地址
#
return
```

步骤3 配置DSLAM设备

具体步骤请参考具体DSLAM设备的产品手册。

步骤4 验证配置结果

RouterA能ping通对端（即RouterB）。

----结束

5.10 配置 IPoEoA 实现局域网接入 Internet 的示例

规格

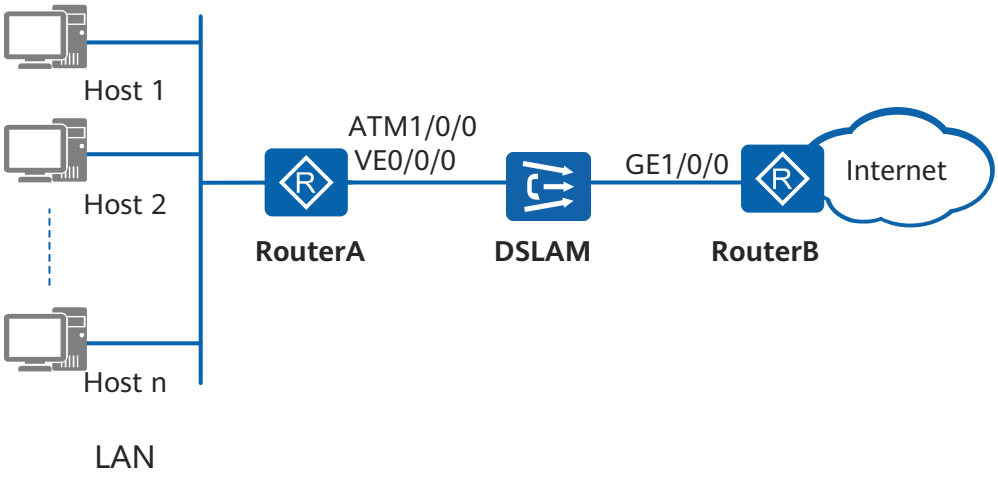
适用于所有版本的AR路由器。

版权所有 © 华为技术有限公司

组网需求

企业网内用户通过二层以太接口统一接入企业网关RouterA，RouterA通过ADSL接口上行接入DSLAM设备后接入RouterB。

图 5-10 配置 IPoEoA 组网图



操作步骤

步骤1 RouterA的配置

```
#
interface Virtual-Ethernet0/0/0 //创建并进入虚拟以太网接口
 ip address 1.1.0.1 255.255.255.0 //配置虚拟以太网接口的IP地址
#
interface Atm1/0/0
 pvc 25/45 //创建PVC，进入PVC视图
  map bridge Virtual-Ethernet 0/0/0 //配置PVC上的IPoEoA映射
#
return
```

步骤2 RouterB的配置

```
#
interface GigabitEthernet0/0/1
 ip address 1.1.0.2 255.255.255.0 //配置RouterB GE0/0/1的IP地址
#
return
```

步骤3 配置DSLAM设备

具体步骤请参考具体DSLAM设备的产品手册。

步骤4 验证配置结果

RouterA能ping通对端（即RouterB）。

----结束

版权所有 © 华为技术有限公司

5.11 配置 PPPoEoA 实现用户利用 PPP 协议接入 Internet 的示例

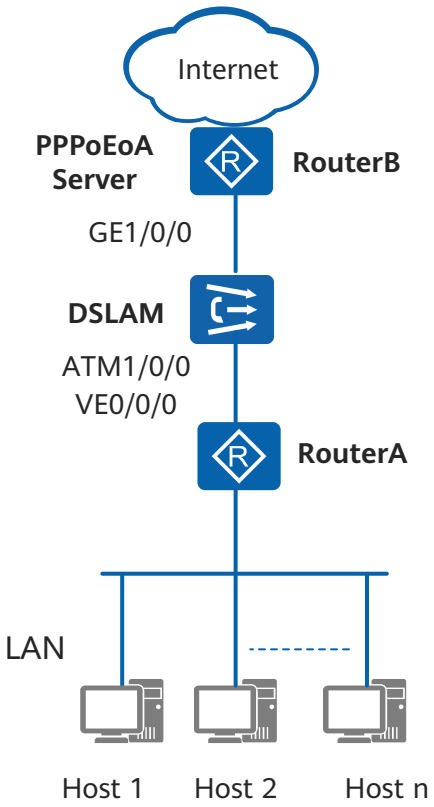
规格

适用于所有版本的AR路由器。

组网需求

如图1所示，企业内网用户需要访问Internet，要求高带宽、提供良好QoS、传送语音、数据和视频多媒体信息等要求，需要使用PPPoA实现接入Internet。企业网内所有用户以RouterA以太网口的IP地址为网关，通过ADSL接口连接DSLAM接入PPPoEoA服务器，RouterA作为PPPoEoA的客户端，通过CHAP来进行认证，IP地址均为PPP协商获取。

图 5-11 配置 PPPoEoA 组网图



操作步骤

步骤1 RouterA的配置

```
#
dialer-rule    //进入Dialer-rule视图
```


版权所有 © 华为技术有限公司

```
 dialer-rule 10 ip permit   //配置拨号访问控制列表，编号为10
#
acl 2000   //配置进行NAT的ACL
 rule 5 permit source 192.168.0.0 0.0.0.255
#
interface Dialer16   //进入Dialer接口
 link-protocol ppp   //配置Dialer接口的链路层协议
 ppp chap user user2@system   //配置CHAP认证的用户名，以便PPPoE Server对客户端进行认证
 ppp chap password cipher %@%@t^cV#p7O3JZd9oD{d3h8%ay3%@%@   //配置CHAP认证的密码，以便
PPPoE Server对客户端进行认证
 ip address ppp-negotiate   //配置通过PPP协议的地址协商功能为客户端接口分配IP地址
 dialer user user2@system   //使能共享DCC功能
 dialer bundle 14   //指定Dialer bundle的编号为14
 dialer-group 10   //配置拨号接口的拨号访问组，编号为10
 nat outbound 2000   //配置Easy IP方式的NAT Outbound
 tcp adjust-mss 1200   //配置TCP最大报文段长度
#
interface Virtual-Ethernet0/0/0   //创建并进入VE接口视图
 pppoe-client dial-bundle-number 14   //建立一个PPPoE会话，并且指定该会话所对应的Dialer Bundle
#
interface Atm1/0/0   //进入ATM接口视图
 pvc 30/90   //创建PVC，进入PVC视图
  map bridge Virtual-Ethernet0/0/0   //配置PVC上的PPPoEoA映射
#
 ip route-static 0.0.0.0 0 Dialer16   //配置Dialer0作为默认路由出口
```

步骤2 RouterB的配置

```
#
ip pool 1 //创建全局地址池
 gateway-list 1.1.1.1 //配置DHCP服务器全局地址池的出口网关地址
 network 1.1.1.2 mask 255.255.255.0 //配置全局地址池下可分配的网段地址
#
aaa //采用本地认证模式
 authentication-scheme system_a
 domain system
  authentication-scheme system_a
 local-user user2@system password cipher %@%@bko\D0<pFF#XozNHQ!70OC]<%@%@ //配置本地用户的
用户名和密码
 local-user user2@system privilege level 0
 local-user user2@system service-type ppp //配置本地用户使用的服务类型为PPP
#
interface Virtual-Template0 //创建并进入指定的虚拟接口模板
 ppp authentication-mode chap domain system  //配置验证方式为CHAP
 remote address pool 1 //配置为客户端分配IP地址或指定地址池
 ip address 1.1.1.1 255.255.255.0 //为虚拟接口模板分配IP地址
#
interface GigabitEthernet0/0/1 //进入接口视图
 pppoe-server bind Virtual-Template 0 //将指定的虚拟模板绑定到以太网接口上，并在以太网接口上启用PPPoE
协议
#
return
```

步骤3 配置DSLAM设备

具体步骤请参考具体DSLAM设备的产品手册。

步骤4 验证配置结果

使用**display interface dialer**命令查看Router上的拨号接口被分配到正确的IP地址。

显示信息中出现如下信息，说明拨号接口已经分配到了正确的IP地址：

```
Internet Address is negotiated, 1.1.1.254/32
```

使用**display virtual-access**命令查看拨号接口生成的VA的PPP协商状态。

显示信息中出现如下信息，说明VA的PPP协商状态为正常：

 版权所有 © 华为技术有限公司

```
LCP opened, IPCP opened
```

RouterA能ping通PPPoEoA服务器（即RouterB）。

----结束

配置注意事项

- 命令**dialer-rule**中的编号和命令**dialer-group**中的编号必须一致；命令**dialer bundle**中的编号和命令**pppoe-client dial-bundle-number**的编号必须一致。
- Dialer接口下的**dialer user**的用户名可以随便配置，**dialer user**只使能共享DCC功能。
- 当出现经过NAT后，可以Ping通公网但是无法打开网页，将公网接口上配置**tcp adjust-mss**命令。对于PPPoE应用，该值推荐为1200字节。

5.12 配置 PPPoA 实现用户利用 PPP 协议接入 Internet 的示例

规格

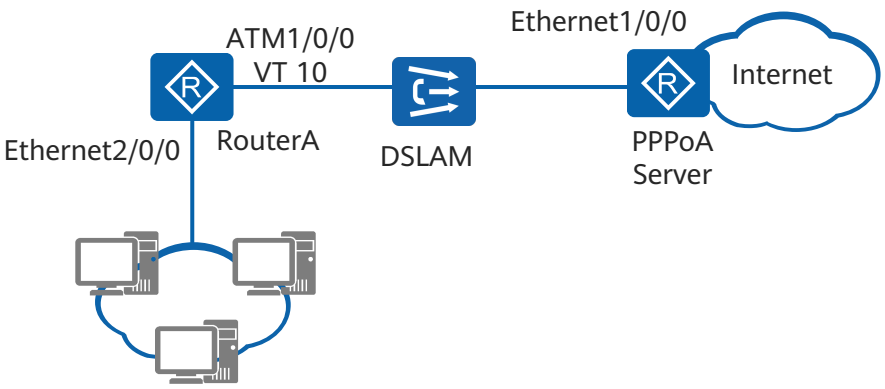
适用于所有版本的AR路由器。

组网需求

企业内网用户需要访问Internet，要求高带宽、提供良好QoS、传送语音、数据和视频多媒体信息等要求，需要使用PPPoA实现接入Internet。PPPoA的通讯过程由PPP协议管理，可以利用PPP协议的灵活性和丰富的应用实现接入Internet。PPPoA指的是在ATM上承载PPP协议报文：ATM信元封装PPP报文，IP或其它协议的报文则封装在PPP报文中。

如图1所示，企业网内用户通过三层以太接口统一接入企业网关RouterA，RouterA通过ADSL接口上行接入DSLAM设备后接入Internet。企业网内用户发出的IP报文封装在PPP报文中，再通过ADSL接口发送出去，实现了PPPoA应用。

图 5-12 配置 PPPoA 组网图



版权所有 © 华为技术有限公司

操作步骤

步骤1 配置RouterA

```
#
 sysname RouterA
#
interface Ethernet2/0/0  //配置LAN侧接口
 ip address 1.1.0.1 255.255.255.0
#  //配置WAN侧VT接口
interface Virtual-Template10
  ppp chap user huawei
  ppp chap password cipher %^%#;^p|F{9fb1IiN7U[7HoAFh8)%^%#
  ip address ppp-negotiate
#
interface Atm1/0/0  //配置WAN侧ATM接口
  pvc 35/53
   map ppp Virtual-Template10
#
return
```

步骤2 配置DSLAM设备

具体步骤请参考具体DSLAM设备的产品手册。

步骤3 配置PPPoA服务器

```
#  //配置IP地址池
ip pool 1
 gateway-list 2.1.1.1
 network 2.1.1.2 mask 255.255.255.0
#
aaa  //配置用户
 local-user huawei password cipher %^%#;3k`38}:/##N~BmPHev|;;rdS%^%#
 local-user huawei privilege level 0
 local-user huawei service-type ppp
#
interface Ethernet1/0/0  //配置WAN侧
 pppoe-server bind Virtual-Template 0
#
interface Virtual-Template0  //配置WAN侧VT接口
 ppp authentication-mode chap  //配置CHAP认证
 remote address pool 1
 ip address 2.1.1.1 255.255.255.0
#
return
```

步骤4 验证配置结果

使用**display interface virtual-template**命令查看RouterA上的VT接口被分配到正确的IP地址。RouterA能ping通PPPoA服务器。

----结束

配置注意事项

- 本端用户名和密码一定要和对端CHAP验证配置的用户名和密码一致。

5.13 配置帧中继专线利用 PPP 协议实现局域网互联的示例

规格

适用于所有版本的AR路由器。

 版权所有 © 华为技术有限公司

组网需求

RouterA与RouterB之间通过帧中继专线直连，由于帧中继网络不提供认证功能，无法确认接入用户的合法性。

考虑到PPP协议具有良好的认证功能和扩展性，本示例将通过配置PPPoFR方案，通过CHAP认证然后承载在帧中继网络上，实现在帧中继网上建立一个端到端的PPP会话，从而保证对接入用户的合法性验证。

图 5-13 配置 PPPoFR 组网图

操作步骤

步骤1 RouterA的配置

```
#
interface Virtual-Template10 //创建虚拟接口模板并进入相应视图
 ip address 10.1.0.5 255.255.255.0 //配置VT的IP地址
 ppp chap user huawei //配置CHAP认证的用户名
 ppp chap password cipher %@%@;^p|F{9fb1IiN7U[7HoAFh8)%@%@ //配置CHAP认证的密
码
#
interface Serial1/0/0
 link-protocol fr //封装接口链路层协议为帧中继
 fr interface-type dte //配置帧中继接口类型为DTE
 fr dlci 100 //配置帧中继链路的数据连接标识符
 fr map ppp interface Virtual-Template10 100 //将帧中继的一条虚电路映射到一条PPP链
路
#
return
```

步骤2 RouterB的配置

```
#
aaa //进入AAA视图
 local-user huawei password cipher %@%@3k`38}:/##N~BmPHev|;;rdS%@%@ //配置本地用户的用户名和密
码
 local-user huawei privilege level 0
 local-user huawei service-type ppp //配置本地用户使用的服务类型为PPP
#
interface Virtual-Template10 //创建虚拟接口模板并进入相应视图
 ip address 10.1.0.6 255.255.255.0 //配置VT的IP地址
 ppp authentication-mode chap //配置PPP认证方式为CHAP
#
interface Serial1/0/0
 link-protocol fr //封装接口链路层协议为帧中继
 fr interface-type dce //配置帧中继接口类型为DCE
 fr dlci 100 //配置帧中继链路的数据连接标识符
 fr map ppp interface Virtual-Template10 100 //将帧中继的一条虚电路映射到一条PPP链路
#
return
```

步骤3 验证配置结果

使用**display virtual-access vt** *vt-number*命令查看RouterB上虚拟模板接口对应的VA的状态。

版权所有 © 华为技术有限公司

使用**display fr map-info interface** *interface-type interface-number*命令查看RouterB上帧中继的地址映射信息。

----结束

5.14 配置帧中继专线利用 IP 协议实现局域网互联的示例

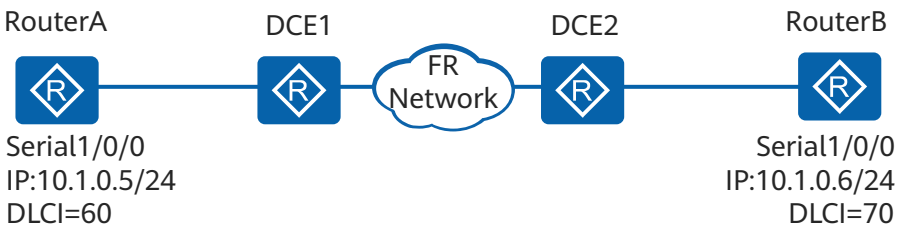
规格

适用于所有版本的AR路由器。

组网需求

在帧中继接入场景中，RouterA和RouterB作为DTE设备承载IP报文，通过公用帧中继网络实现局域网的互联。

图 5-14 配置 IPoFR 组网图



操作步骤

步骤1 RouterA的配置

```
#
interface Serial1/0/0
 link-protocol fr    //封装接口链路层协议为帧中继
 fr dlci 60    //配置帧中继链路的数据连接标识符
 fr map ip 10.1.0.6 60    //配置本端DLCI到对端IP地址的静态映射
 ip address 10.1.0.5 255.255.255.0    //配置本端设备的IP地址
#
return
```

步骤2 RouterB的配置

```
#
interface Serial1/0/0
 link-protocol fr    //封装接口链路层协议为帧中继
 fr dlci 70    //配置帧中继链路的数据连接标识符
 fr map ip 10.1.0.5 70    //配置本端DLCI到对端IP地址的静态映射
 ip address 10.1.0.6 255.255.255.0    //配置本端设备的IP地址
#
return
```

步骤3 验证配置结果

RouterA和RouterB能够互相Ping通。

----结束

版权所有 © 华为技术有限公司

5.15 配置采用 MP-Group 进行 MP 绑定示例

规格

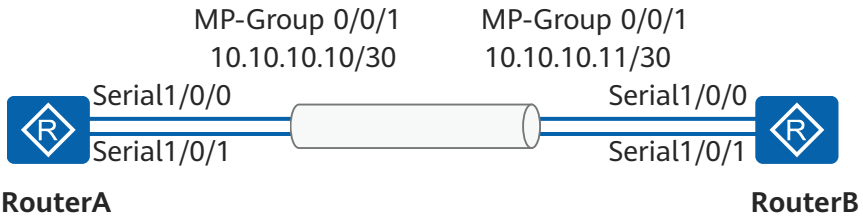
适用于所有版本的AR路由器。

组网需求

为了增加带宽，可以将多个PPP链路捆绑成MP使用。采用MP-Group进行MP绑定只是MP捆绑方式中的一种，使用这种绑定方式时，MP中包含的PPP链路是固定的，这种方式快速高效、配置简单、容易理解，在实际组网中应用较多。

如图5-15所示，路由器RouterA和RouterB的两对串口分别相连，使用MP-Group进行MP绑定，采用CHAP本地认证。

图 5-15 采用 MP-Group 进行 MP 绑定组网图



操作步骤

步骤1 配置RouterA

```
#
aaa  //配置本地用户
  authentication-scheme system_a
 domain system
  authentication-scheme system_a
 local-user userb password cipher %@%@3k`38}:/##N~BmPHev|;;rdS%@%@
 local-user userb privilege level 0
 local-user userb service-type ppp
#
interface Mp-group0/0/1
 ip address 10.10.10.10 255.255.255.252
#
interface Serial1/0/0
 link-protocol ppp
 ppp authentication-mode chap domain system //采用CHAP方式验证
 ppp chap user usera //配置对端的用户名和密码
 ppp chap password cipher %@%@3k`38}:/##N~BmPHev|;;rdS%@%@
 ppp mp mp-group 0/0/1 //捆绑MP
#
interface Serial1/0/1
 link-protocol ppp
 ppp authentication-mode chap domain system //采用CHAP方式验证
 ppp chap user usera //配置对端的用户名和密码
 ppp chap password cipher %@%@4k`38}:/##N~BmPHev|;;rdS%@%@
 ppp mp mp-group 0/0/1 //捆绑MP
return
```


版权所有 © 华为技术有限公司

步骤2 配置RouterB

```
#
aaa  //配置本地用户
  authentication-scheme system_b
 domain system
  authentication-scheme system_b
 local-user usera password cipher %@%@wSj=##g9INJIZ$Ip'6f7;rd!%@%@
 local-user usera privilege level 0
 local-user usera service-type ppp
#
interface Mp-group0/0/1
 ip address 10.10.10.11 255.255.255.252
#
interface Serial1/0/0
 link-protocol ppp
 ppp authentication-mode chap domain system //采用CHAP方式验证
 ppp chap user userb //配置对端的用户名和密码
 ppp chap password cipher %@%@3k`38}:/##N~BmPHev|;;ldS%@%@
 ppp mp mp-group 0/0/1 //捆绑MP
#
interface Serial1/0/1
 link-protocol ppp
 ppp authentication-mode chap domain system //采用CHAP方式验证
 ppp chap user userb  //配置对端的用户名和密码
 ppp chap password cipher %@%@3k`38}:/##N~BmPHev|;;mdS%@%@
 ppp mp mp-group 0/0/1  //捆绑MP
return
```

步骤3 验证配置结果。

在RouterA上执行命令**display ppp mp**查看绑定效果。根据显示信息可以看出MP子链路的物理状态和协议状态、子链路数及MP的成员等信息。

在RouterA上执行命令**display virtual-access**查看VA状态。

RouterB可以Ping通RouterA。

----结束

配置注意事项

- 为了保证配置生效，请在配置全部完成后，重启MP包含的所有成员接口。
- 本端用户名和密码一定要和对端CHAP验证配置的用户名和密码一致。

相关资料

视频：**如何捆绑多个E1线路**

5.16 配置将 PPP 链路直接绑定到 VT 上实现 MP 的示例

规格

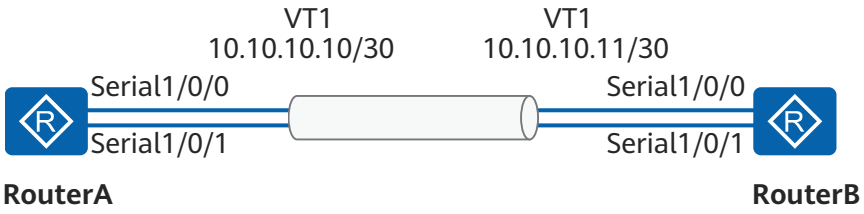
适用于所有版本的AR路由器。

组网需求

如图5-16所示，两台路由器通过串口线互连，通过MP互通，实现更高的可靠性和带宽。MP的绑定方式为链路直接绑定到VT上。

 版权所有 © 华为技术有限公司

图 5-16 采用虚拟接口模板进行 MP 直接绑定组网图



操作步骤

步骤1 RouterA的配置

```
#
sysname RouterA  //修改设备名称用于识别设备
interface serial 1/0/0
 link-protocol ppp  //配置链路协议为PPP
 ppp mp Virtual-Template 1  //串口工作在MP方式，绑定到虚拟接口模板VT1
#
interface serial 1/0/1
 link-protocol ppp  //配置链路协议为PPP
 ppp mp Virtual-Template 1  //串口工作在MP方式，绑定到虚拟接口模板VT1
#
interface Virtual-Template1
 ip address 10.10.10.10 255.255.255.252  //配置VT1的IP地址
return
```

步骤2 RouterB的配置

```
#
sysname RouterB  //修改设备名称用于识别设备
interface serial 1/0/0
 link-protocol ppp  //配置链路协议为PPP
 ppp mp Virtual-Template 1  //串口工作在MP方式，绑定到虚拟接口模板VT1
#
interface serial 1/0/1
 link-protocol ppp  //配置链路协议为PPP
 ppp mp Virtual-Template 1  //串口工作在MP方式，绑定到虚拟接口模板VT1
#
interface Virtual-Template1
 ip address 10.10.10.11 255.255.255.252  //配置VT1的IP地址
return
```

步骤3 验证配置结果

在RouterA上执行命令**display ppp mp**查看绑定状态，可在成员中看到两个串口。

在RouterB上执行命令**display ppp mp**查看绑定状态，可在成员中看到两个串口。

在RouterB上Ping对端，可以Ping通。

----结束

配置注意事项

- 为了使PPP协议重新协商，以保证所有物理接口成功绑定到MP，配置完成后，请重启所有物理接口。

版权所有 © 华为技术有限公司

5.17 配置按照用户名查找虚拟接口模板实现 MP 的示例

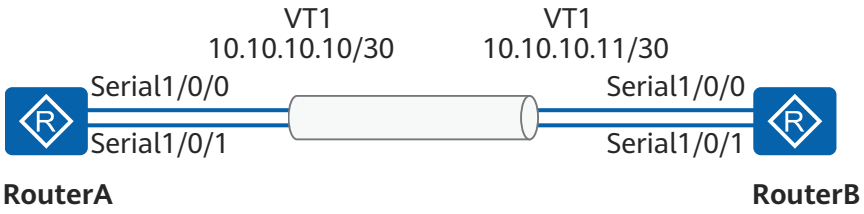
规格

适用于所有版本的AR路由器。

组网需求

如图5-17所示，两台AR路由器通过串口线互连，通过MP互通，实现更高的可靠性和带宽。MP的绑定方式为按照用户名查找虚拟接口模板进行绑定。

图 5-17 配置按照用户名查找虚拟接口模板进行 MP 绑定组网图



操作步骤

步骤1 配置RouterA

```
#
 sysname RouterA  //修改设备名称用于识别设备
 #
 ppp mp user userb bind Virtual-Template 1  //将对端用户名userb绑定到VT 1
#
aaa
  authentication-scheme system_a
 domain system
  authentication-scheme system_a
 local-user userb@system password cipher %@%@3k`38}:/##N~BmPHev|;;rdS%@%@
 local-user userb@system privilege level 0
 local-user userb@system service-type ppp  //创建对端的用户和密码，用于认证对端
#
interface Serial1/0/0
 link-protocol ppp
 ppp authentication-mode chap domain system
 ppp chap user usera@system
 ppp chap password cipher %@%@3k`38}:/##N~BmPHev|;;rdS%@%@  //创建被对端认证的用户名和密码，认证方式为CHAP
 ppp mp  //串口工作在MP方式
#
interface Serial1/0/1
 link-protocol ppp
 ppp authentication-mode chap domain system
 ppp chap user usera@system
 ppp chap password cipher %@%@4k`38}:/##N~BmPHev|;;rdS%@%@  //创建被对端认证的用户名和密码，认证方式为CHAP
 ppp mp  //串口工作在MP方式
#
interface Virtual-Template1
 ppp mp binding-mode authentication  //根据对端用户名进行MP绑定
 ip address 10.10.10.10 255.255.255.252
```


版权所有 © 华为技术有限公司

```
#
return
```

步骤2 配置RouterB

```
#
 sysname RouterB  //修改设备名称用于识别设备
 #
 ppp mp user usera bind Virtual-Template 1  //将对端用户名usera绑定到VT 1
#
aaa
 authentication-scheme system_b
 domain system
  authentication-scheme system_b
 local-user usera@system password cipher %@%@wSj=##g9INJIZ$Ip'6f7;rd!%@%@
 local-user usera@system privilege level 0
 local-user usera@system service-type ppp  //创建对端的用户和密码，用于认证对端
#
interface Serial1/0/0
 link-protocol ppp
 ppp authentication-mode chap domain system
 ppp chap user userb@system
 ppp chap password cipher %@%@3k`38}:/##N~BmPHev|;;ldS%@%@  //创建被对端认证的用户名和密码，认证方式为CHAP
 ppp mp
#
interface Serial1/0/1
 link-protocol ppp
 ppp authentication-mode chap domain system
 ppp chap user userb@system
 ppp chap password cipher %@%@3k`38}:/##N~BmPHev|;;mdS%@%@  //创建被对端认证的用户名和密码，认证方式为CHAP
 ppp mp
#
interface Virtual-Template1
 ppp mp binding-mode authentication  //根据对端用户名进行MP绑定
 ip address 10.10.10.11 255.255.255.252
#
return
```

步骤3 验证配置结果

在RouterA上执行命令**display ppp mp**查看绑定状态，可在成员中看到两个串口。

在RouterB上执行命令**display ppp mp**查看绑定状态，可在成员中看到两个串口。

在RouterB上Ping对端，可以Ping通。

----结束

配置注意事项

- 为了使PPP协议重新协商，以保证所有物理接口成功绑定到MP，配置完成后，请重启所有物理接口。
- 本端用户名和密码一定要和对端CHAP验证配置的用户名和密码一致。

5.18 配置设备作为 PPPoE Client，实现设备接入 Internet 的示例

规格

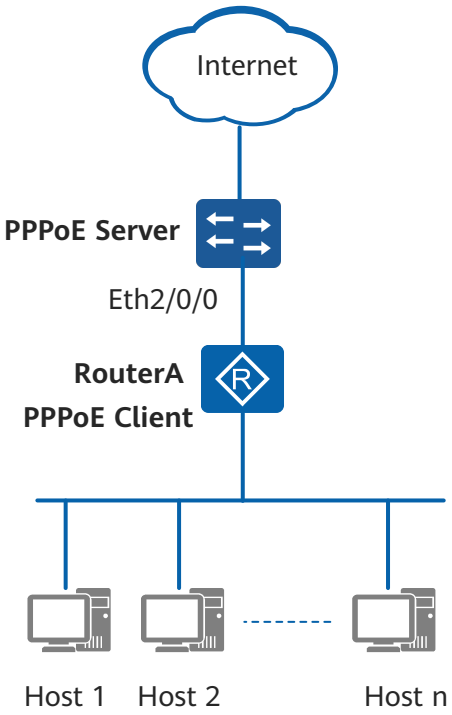
适用于所有版本的AR路由器。

 版权所有 © 华为技术有限公司

组网需求

企业用户希望把一个站点上的多台主机连接到同一台远程接入设备，同时接入设备能够提供与拨号上网类似的访问控制和计费功能。PPPoE利用以太网将大量主机组成网络，通过一个远端接入设备连入因特网，并运用PPP协议对接入的每个主机进行控制，具有适用范围广、安全性高、计费方便的特点。如图1所示，企业网内的主机使用相同的PPPoE客户端同PPPoE服务器建立连接，接入到Internet。其中，Router作为PPPoE客户端，并得到PPPoE服务器的认证。

图 5-18 配置 PPPoE Client 功能组网图



操作步骤

步骤1 配置Router

```
#
dialer-rule  //进入Dialer-rule视图
 dialer-rule 1 ip permit  //配置拨号访问控制列表，编号为1
#
acl 3002  //配置进行NAT的ACL
 rule 5 permit ip source 192.168.0.0 0.0.0.255
#
interface Dialer0  //进入Dialer接口
 link-protocol ppp  //配置Dialer接口的链路层协议
 ip address ppp-negotiate  //配置通过PPP协议的地址协商功能为客户端接口分配IP地址
 ppp chap user client  //配置CHAP认证的用户名，以便PPPoE Server对客户端进行认证
 ppp chap password cipher %@%@VGZIW'r|aGrQ"v8`<pEP$7uH%@%@  //配置CHAP认证的密码，以便PPPoE Server对客户端进行认证
 dialer user server  //使能共享DCC功能
 dialer bundle 1  //指定Dialer bundle的编号为1
 dialer-group 1  //配置拨号接口的拨号访问组，编号为1
 nat outbound 3002  //配置Easy IP方式的NAT Outbound
 tcp adjust-mss 1200  //配置TCP最大报文段长度
```


版权所有 © 华为技术有限公司

```
#
interface Ethernet2/0/0   //进入以太网接口
 pppoe-client dial-bundle-number 1   //在以太网接口上启用PPPoE Client功能
#
 ip route-static 0.0.0.0 0 Dialer0   //配置到PPPoE Server的静态路由，指定出接口为Dialer0
```

步骤2 验证配置结果

执行命令**display pppoe-client session summary**查看PPPoE会话的状态和配置信息。根据显示信息判断会话状态是否正常（状态为up表示正常）、配置是否正确（是否和之前的数据规划和组网一致）。

----结束

配置注意事项

- 命令**dialer-rule**中的编号和命令**dialer-group**中的编号必须一致；命令**dialer bundle**中的编号和命令**pppoe-client**的*dial-bundle-number*参数必须一致。
- Dialer接口下的**dialer user**的用户名可以随便配置，**dialer user**只使能共享DCC功能。
- Dialer接口的PPP认证的用户名和密码需要与PPPoE Server保持一致。
- 在以太网接口上启用PPPoE Client功能，选择**on-demand**参数表示按需拨号，当连接断开后，只有在数据需要传输时，设备才能建立拨号连接；不选择**on-demand**参数表示自动拨号，当连接断开后，每隔一段时间设备会自动再次尝试建立拨号连接。

相关资料

视频：**如何配置PPPoE Client**

5.19 配置设备作为 PPPoE Client（IPv6），实现设备接入 Internet 的示例

规格

适用于所有版本支持WAN接口的AR路由器。

设备支持配置为IPv6 PPPoE Client，不支持配置为IPv6 PPPoE Server。

组网需求

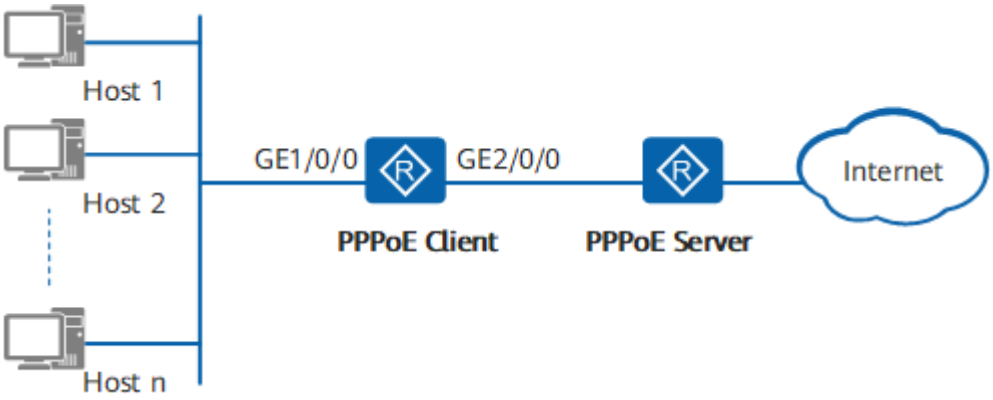
如**图1**所示，设备下行通过GE1/0/0连接局域网用户，上行通过GE2/0/0接入PPPoE Server。

用户希望局域网内主机共用一个上网帐号，在建立连接过程中，通过这个帐号到PPPoE Server进行认证，认证通过后，即建立了一个PPPoE会话。用户需求如下：

- 设备通过PPP认证与PPPoE Server建立IPv6连接。
- 当连接断开后，每隔一段时间设备会自动再次尝试建立拨号连接。

 版权所有 © 华为技术有限公司

图 5-19 设备作为 PPPoE Client 组网图



配置思路

采用如下的配置思路：

1. 为了实现以太网接口的接入，需要建立PPPoE会话并绑定在指定的以太网接口GigabitEthernet 2/0/0上。
2. 在拨号接口下配置CHAP认证，实现设备通过PPP认证与PPPoE Server建立连接。
3. 为了实现Dialer接口自动获得IPv6地址，需要开启设备的无状态地址自动配置功能。同时申请IPv6前缀，并将该前缀分发给局域网内Host。
4. 配置拨号方式为自动拨号方式，保证连接断开后根据设定时间设备会自动再次尝试建立拨号连接。

操作步骤

步骤1 全局使能IPv6功能

```
<Huawei> system-view
[Huawei] sysname Router
[Router] ipv6
```

步骤2 配置Dialer接口

```
[Router] interface dialer 1
[Router-Dialer1] dialer user user2
[Router-Dialer1] dialer bundle 1
[Router-Dialer1] ppp chap user user1@system
[Router-Dialer1] ppp chap password cipher YsHsjx_202206
[Router-Dialer1] ip address ppp-negotiate
```

步骤3 使能DHCPv6客户端功能，并向Host分配地址前缀

```
[Router-Dialer1] ipv6 enable //使能接口IPv6功能
[Router-Dialer1] ipv6 address auto link-local //接口配置自动生成链路本地地址
[Router-Dialer1] ipv6 address auto global //使能无状态自动生成IPv6全局地址功能
[Router-Dialer1] undo ipv6 nd ra halt //使能系统发布RA报文功能
[Router-Dialer1] quit
```

步骤4 建立PPPoE会话

```
[Router] interface gigabitethernet 2/0/0
[Router-GigabitEthernet-2/0/0] pppoe-client dial-bundle-number 1
[Router-GigabitEthernet-2/0/0] quit
```

步骤5 验证配置结果

- 在PPPoE Client上执行命令**display dhcpv6 client**，查看设备是否获取IPv6地址。

版权所有 © 华为技术有限公司

- 检查PPPoE Client是否能够访问IPv6网络。

----结束

配置文件

设备作为PPPoE Client的配置文件

```
#
 sysname Router
#
ipv6
#
interface Dialer1
 link-protocol ppp
 ppp chap user user1@system
 ppp chap password cipher %^%#LHG2'Q8n%8NSLn'4-i'Z18)-%eT"v*||t1Mh;NbH%^%#
 ipv6 enable
 ip address ppp-negotiate
 dialer user user2
 dialer bundle 1
 ipv6 address auto link-local
 ipv6 address auto global
 undo ipv6 nd ra halt
#
interface GigabitEthernet2/0/0
 pppoe-client dial-bundle-number 1
#
return
```

配置注意事项

- PPPoE Server需要配置认证方式、IP地址获取方式或设置为PPPoE Client分配的IP地址或地址池。不同设备作为IPv6 PPPoE Server的配置过程也不同，请参考具体设备的相关资料。
- 命令**dialer-rule**中的编号和命令**dialer-group**中的编号必须一致；命令**dialer bundle**中的编号和命令**pppoe-client**的*dial-bundle-number*参数必须一致。
- Dialer接口下的**dialer user**的用户名可以随便配置，**dialer user**只使能共享DCC功能。
- 使能接口IPv6功能需要先全局使能IPv6。
- Dialer接口的PPP认证的用户名和密码需要与PPPoE Server保持一致。Dialer接口要保证Up状态。
- 在以太网接口上启用PPPoE Client功能，选择**on-demand**参数表示按需拨号，当连接断开后，只有在数据需要传输时，设备才能建立拨号连接；不选择**on-demand**参数表示自动拨号，当连接断开后，每隔一段时间设备会自动再次尝试建立拨号连接。

5.20 配置设备作为 PPPoE Server，实现用户安全接入 Internet 的示例

规格

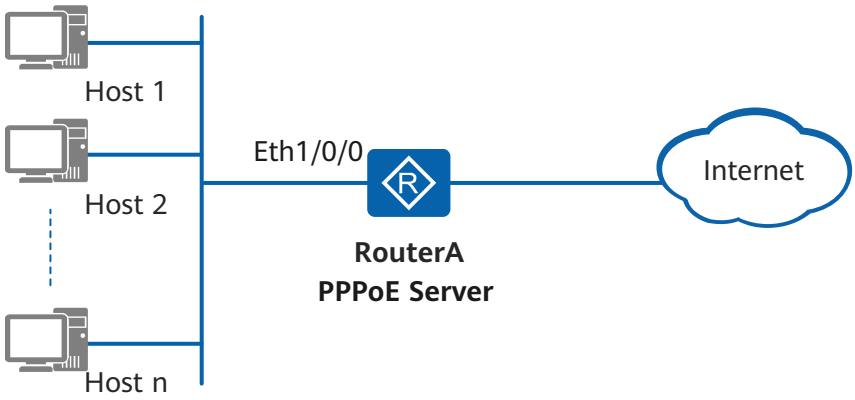
适用于所有版本的AR路由器。

 版权所有 © 华为技术有限公司

组网需求

如图5-20所示，企业网内的主机运行PPPoE Client，通过Router接入到Internet。Router作为PPPoE Server，配置本地认证，并通过地址池为用户主机分配IP地址。

图 5-20 配置 PPPoE Server 功能组网图



操作步骤

步骤1 配置Router

```
#
ip pool pool2  //创建IP地址池pool2
 gateway-list 192.168.10.1  //配置出口网关
 network 192.168.10.0 mask 255.255.255.0  //配置IP地址池的地址范围
#
aaa //配置本地认证
 local-user client password cipher %@%@N!}w4F\6;42P$A2'XqkP(Ix6%@%@  //配置PPPoE Client的用户名和密码
 local-user client privilege level 0
 local-user client service-type ppp  //配置PPPoE Client的接入类型
#
interface Virtual-Template1  //配置虚拟接口模板
 ppp authentication-mode chap  //配置虚拟接口模板的PPP认证方式，以便对PPPoE Client进行CHAP认证
 remote address pool pool2  //配置为PPPoE Client指定IP地址池，PPPoE Client将分配到IP地址池中的IP地址
 ip address 192.168.10.1 255.255.255.0  //配置虚拟接口模板的IP地址
#
interface Ethernet1/0/0  //进入以太网接口
 pppoe-server bind Virtual-Template 1  //在以太网接口上启用PPPoE Server功能
#
```

步骤2 验证配置结果

在Router上执行**display pppoe-server session all**命令，显示PPPoE会话的状态信息和配置信息。根据显示信息判断会话状态是否正常（状态为up表示正常）、配置是否正确（是否和之前的数据规划和组网一致）。

----结束

配置注意事项

局域网内各主机安装PPPoE客户端软件后，配置好用户名和密码（用户名为client，密码为YsHsjx_202206）就能使用PPPoE协议，通过Router接入到Internet。

版权所有 © 华为技术有限公司

相关资料

视频：**如何配置PPPoE Server**

5.21 配置设备利用 PPPoE 技术通过外置的 ADSL Modem 接入 Internet 的示例

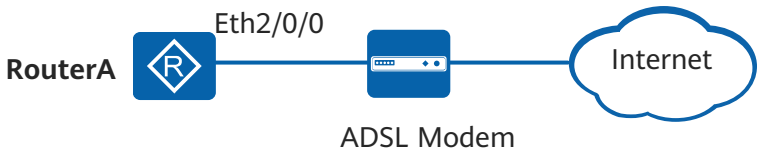
规格

适用于所有版本的AR路由器。

组网需求

如图5-21所示，Router的Ethernet接口与ADSL modem相连，使用PPPoE技术接入Internet。

图 5-21 配置路由器使用外置 ADSL modem 接入 Internet 组网图



操作步骤

步骤1 配置Router

```
#
dialer-rule  //进入Dialer-rule视图
 dialer-rule 1 ip permit  //配置拨号访问控制列表，编号为1
#
acl 2000  //配置进行NAT的ACL
 rule 5 permit source 192.168.0.0 0.0.0.255
#
interface Dialer0  //进入Dialer接口
 link-protocol ppp  //配置Dialer接口的链路层协议
 ip address ppp-negotiate  //配置通过PPP协议的地址协商功能为客户端接口分配IP地址
 ppp chap user client  //配置CHAP认证的用户名，以便PPPoE Server对客户端进行认证
 ppp chap password cipher %@%@ZpL+=<'bp;#yW'<oAkQA)%b0%@%@  //配置CHAP认证的密码，以便
PPPoE Server对客户端进行认证
 dialer user server  //使能共享DCC功能
 dialer timer idle 300  //配置闲置切断时间
 dialer bundle 1  //指定Dialer bundle的编号为1
 dialer-group 1  //配置拨号接口的拨号访问组，编号为1
 nat outbound 2000  //配置Easy IP方式的NAT Outbound
 tcp adjust-mss 1200  //配置TCP最大报文段长度
#
interface Ethernet2/0/0  //进入以太网接口
 pppoe-client dial-bundle-number 1 on-demand  //在以太网接口上启用PPPoE Client功能
#
 ip route-static 0.0.0.0 0 Dialer0  //配置Dialer0作为默认路由出口
```

步骤2 验证配置结果

版权所有 © 华为技术有限公司

执行命令**display pppoe-client session summary**查看PPPoE会话的状态和配置信息。根据显示信息判断会话状态是否正常（状态为up表示正常）、配置是否正确（是否和之前的数据规划和组网一致）。

显示信息中出现如下信息，说明信息判断会话状态已正常：

```
PPPoE Client Session:
ID   Bundle  Dialer  Intf          Client-MAC    Server-MAC    State
1    1       0       Eth2/0/0      00e0fc030201  0819a6cd0680  UP
```

----结束

配置注意事项

- 命令**dialer-rule**中的编号和命令**dialer-group**中的编号必须一致；命令**dialer bundle**中的编号和命令**pppoe-client dial-bundle-number**的编号必须一致。
- 如果选择**on-demand**参数，则需要在Dialer接口下执行**dialer timer idle**命令配置闲置切断时间。
- Dialer接口下的**dialer user**的用户名可以随便配置，**dialer user**只使能共享DCC功能。
- 当出现经过NAT后，可以Ping通公网但是无法打开网页，将公网接口上配置**tcp adjust-mss**命令。对于PPPoE应用，该值推荐为1200字节。

5.22 配置设备通过 Modem 拨号接入 PSTN 的示例(轮询 DCC 方式)

规格

适用于V200R001C01及更高版本的AR路由器。

组网需求

如图5-22所示，RouterA和RouterB通过PSTN互连，在路由器上配置轮循DCC，使RouterA和RouterB能够通过modem拨号互相连接到对端。

图 5-22 配置路由器通过 Modem 拨号接入 PSTN 组网图(轮询 DCC 方式)

操作步骤

步骤1 配置RouterA

```
#
dialer-rule   //进入Dialer-rule视图
 dialer-rule 1 ip permit   //配置拨号访问控制列表，编号为1
```


版权所有 © 华为技术有限公司

```
#
interface Async2/0/0  //进入Async接口
 link-protocol ppp  //配置Async接口的链路层协议
 ip address 10.1.1.1 255.255.255.0  //配置Async接口的IP地址
 dialer enable-circular  //使能轮询DCC功能
 dialer-group 1  //配置拨号接口的拨号访问组，编号为1
 dialer number 600152  //配置对端的拨号串，拨号串由PSTN网络的运营商分配
#
user-interface tty 9  //进入用户界面视图
 modem both  //配置允许Modem呼入和呼出
 modem auto-answer  //配置Modem为自动应答方式
#
 ip route-static 20.1.1.1 255.255.255.255 Async2/0/0  //配置到对端的静态路由
#
```

步骤2 配置RouterB

```
#
dialer-rule  //进入Dialer-rule视图
 dialer-rule 1 ip permit  //配置拨号访问控制列表，编号为1
#
interface Async2/0/0  //进入Async接口
 link-protocol ppp  //配置Async接口的链路层协议
 ip address 20.1.1.1 255.255.255.0  //配置Async接口的IP地址
 dialer enable-circular  //使能轮询DCC功能
 dialer-group 1  //配置拨号接口的拨号访问组，编号为1
 dialer number 600151  //配置对端的拨号串，拨号串由PSTN网络的运营商分配
#
user-interface tty 9  //进入用户界面视图
 shell  //V200R007C00及之后版本缺省情况下未启动TTY用户界面的终端服务，需要执行该命令启动TTY用户界面的终端服务
 modem both  //配置允许Modem呼入和呼出
 modem auto-answer  //配置Modem为自动应答方式
#
 ip route-static 10.1.1.1 255.255.255.255 Async2/0/0  //配置到对端的静态路由
#
```

步骤3 验证配置结果

执行**display user-interface**命令，查看物理接口对应的TTY用户接口编号。

配置完成后，RouterA和RouterB能够通过modem拨号互相连接到对端。

----结束

配置注意事项

- 本端设备、对端设备的Async接口的物理属性和链路层属性必须一致。建议不要改变设备的缺省情况。Async接口的工作模式为流模式时，链路层协议不能配置为PPP协议。
- 命令**dialer-rule**中的编号和命令**dialer-group**中的编号必须一致。
- 若要同时能够呼入呼出，则需要在相应的用户界面视图下配置**modem both**。
- Modem的应答方式分为两种：自动应答（Modem的AA灯亮）和非自动应答。Modem应答方式的配置主要取决于异步串口外接Modem的状态是否为自动应答方式（Modem的AA灯是否亮）。
  - 如果Modem是自动应答方式，用户需在使用拨号功能之前执行命令**modem auto-answer**。
  - 如果Modem不是自动应答方式，用户需执行命令**undo modem auto-answer**。

 版权所有 © 华为技术有限公司

5.23 配置设备通过 ISDN PRI 接口拨号接入 ISDN 的示例（共享 DCC 方式）

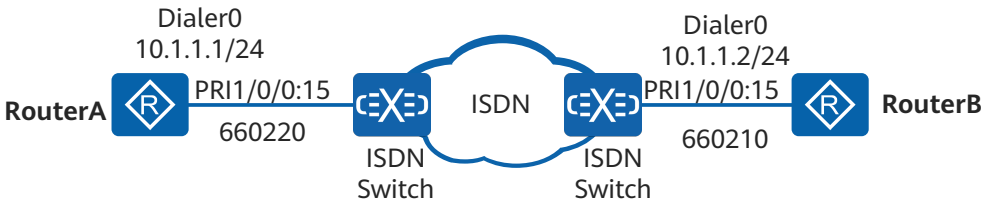
规格

适用于所有版本的AR路由器。

组网需求

如图5-23所示，RouterA和RouterB通过ISDN互连，在路由器上配置共享DCC，并配置CHAP认证互相认证对方。

图 5-23 配置路由器通过 ISDN PRI 接口拨号接入 ISDN 组网图（共享 DCC 方式）



操作步骤

步骤1 配置RouterA

```
#
dialer-rule  //进入Dialer-rule视图
 dialer-rule 1 ip permit  //配置拨号访问控制列表，编号为1
#
aaa  //配置本地认证
 local-user userb password cipher %@%@N!}w4F\6;42P$A2'XqkP(Ix6%@%@  //配置本地用户的用户名和密码
 local-user userb privilege level 0
 local-user userb service-type ppp  //配置本地用户的接入类型
#
interface Dialer0  //进入Dialer接口
 link-protocol ppp  //配置Dialer接口的链路层协议
 ppp authentication-mode chap  //配置PPP认证方式为CHAP，对对端进行CHAP认证
 ppp chap user usera  //配置CHAP认证的用户名
 ppp chap password cipher %@%@3k`38}:/##N~BmPHev|;;rdS%@%@  //配置CHAP认证的密码
 ip address 10.1.1.1 255.255.255.0  //配置Dialer接口的IP地址
 dialer user userb  //使能共享DCC功能，并设置对端用户名
 dialer bundle 1  //指定Dialer bundle的编号为1
 dialer number 660210  //配置呼叫对端的拨号串
 dialer-group 1  //配置拨号接口的拨号访问组，编号为1
#
controller E1 1/0/0  //配置ISDN PRI接口
 pri-set
#
interface Serial1/0/0:15  //进入ISDN PRI接口
 link-protocol ppp  //配置ISDN PRI接口的链路层协议
 ppp authentication-mode chap  //配置PPP认证方式为CHAP，对对端进行CHAP认证
 ppp chap user usera  //配置CHAP认证的用户名
 ppp chap password cipher %@%@4k`38}:/##N~BmPHev|;;rdS%@%@  //配置CHAP认证的密码
 dialer bundle-member 1  //配置ISDN PRI接口属于编号为1的Dialer bundle
#
```


版权所有 © 华为技术有限公司

步骤2 配置RouterB

```
#
dialer-rule  //进入Dialer-rule视图
 dialer-rule 1 ip permit  //配置拨号访问控制列表，编号为1
#
aaa  //配置本地认证
 local-user usera password cipher %@%@N!}w5F\6;42P$A2'XqkP(Ix6%@%@  //配置本地用户的用户名和密码
 local-user usera privilege level 0
 local-user usera service-type ppp  //配置本地用户的接入类型
#
interface Dialer0  //进入Dialer接口
 link-protocol ppp  //配置Dialer接口的链路层协议
 ppp authentication-mode chap  //配置PPP认证方式为CHAP，对对端进行CHAP认证
 ppp chap user userb  //配置CHAP认证的用户名
 ppp chap password cipher %@%@3k`38}:/##N~BmPHev|;;ldS%@%@  //配置CHAP认证的密码
 ip address 10.1.1.1 255.255.255.0  //配置Dialer接口的IP地址
 dialer user usera  //使能共享DCC功能，并设置对端用户名
 dialer bundle 1  //指定Dialer bundle的编号为1
 dialer number 660220  //配置呼叫对端的拨号串
 dialer-group 1  //配置拨号接口的拨号访问组，编号为1
#
controller E1 1/0/0  //配置ISDN PRI接口
 pri-set
#
interface Serial1/0/0:15  //进入ISDN PRI接口
 link-protocol ppp  //配置ISDN PRI接口的链路层协议
 ppp authentication-mode chap  //配置PPP认证方式为CHAP，对对端进行CHAP认证
 ppp chap user userb  //配置CHAP认证的用户名
 ppp chap password cipher %@%@3k`38}:/##N~BmPHev|;;mdS%@%@  //配置CHAP认证的密码
 dialer bundle-member 1  //配置ISDN PRI接口属于编号为1的Dialer bundle
#
```

步骤3 验证配置结果

配置完成后，RouterA和RouterB可以通过ISDN互相通信，且能互相认证。

----结束

配置注意事项

- 命令**dialer-rule**中的编号和命令**dialer-group**中的编号必须一致；命令**dialer bundle**中的编号和命令**dialer bundle-member**的编号必须一致。
- 在本端设备和对端设备，建议在物理接口和Dialer接口上都配置PAP或CHAP认证命令。
- 当Dialer接口封装PPP时，需要使用**dialer user**命令配置对端用户名，用该对端用户名与利用PPP认证得到的对端用户名进行比较，以决定接收呼叫的Dialer接口。

5.24 配置设备利用 HDLC 技术实现互通的示例

规格

适用于所有版本的AR路由器。

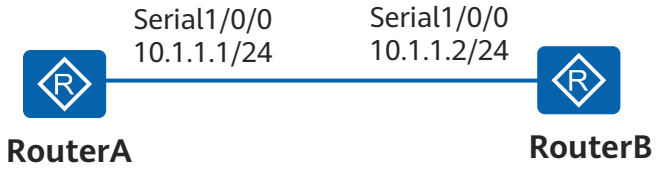
仅AR600系列不支持HDLC。

组网需求

RouterA和RouterB通过HDLC互通。

 版权所有 © 华为技术有限公司

图 5-24 HDLC 功能的典型配置组网图



操作步骤

步骤1 配置RouterA

```
#
 sysname RouterA
#
 interface Serial1/0/0
  link-protocol hdlc
  ip address 10.1.1.1 255.255.255.0
#
 return
```

步骤2 配置RouterB

```
#
 sysname RouterB
#
 interface Serial1/0/0
  link-protocol hdlc
  ip address 10.1.1.2 255.255.255.0
#
 return
```

步骤3 验证配置结果

在RouterA上通过命令**display interface serial 1/0/0**查看接口的配置信息，接口的物理层和链路层的状态都是**Up**状态。

RouterA和RouterB可以互相Ping通对方。

----结束

配置注意事项

- RouterA和RouterB的IP地址需要在同一网段，否则，两者不能互通。

版权所有 © 华为技术有限公司

6 通过 VPN 实现广域网互联

6.1 L2TP
6.2 GRE
6.3 DSVPN
6.4 IPSec
6.5 BGP/MPLS IP VPN
6.6 VLL
6.7 PWE3

6.1 L2TP

6.1.1 配置来自分支机构不同域的用户通过 L2TP 实现与总部互通的示例

规格

适用于所有版本、所有形态的AR路由器。

组网需求

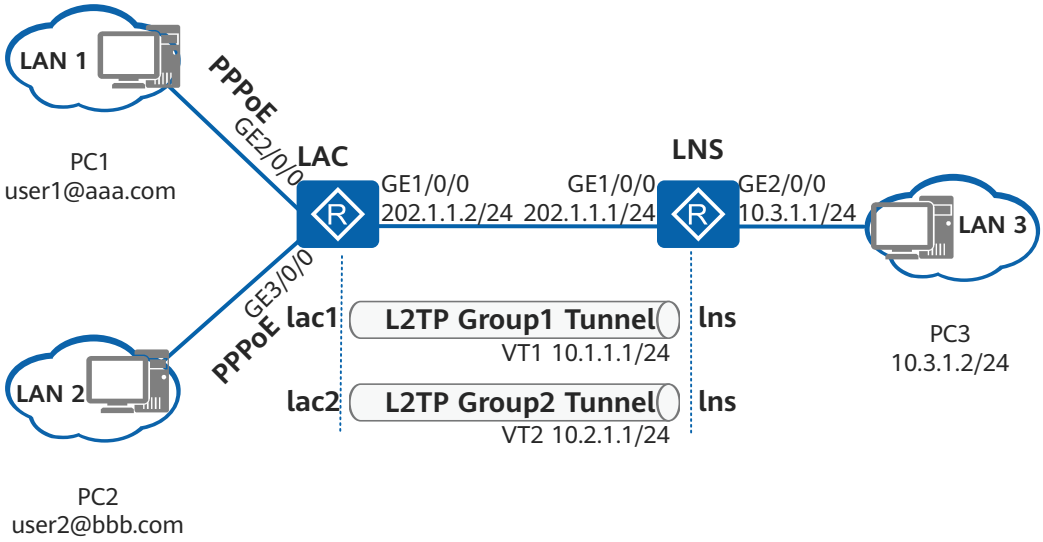
如**图6-1**所示，企业分支LAN1和LAN2的用户通过PPPoE连接LAC，发起到企业总部LAN3的连接。

路由器LAC上配置两个域aaa.com和bbb.com，分别对不同域的用户提供接入，aaa.com域的用户网段是10.1.1.0/24，bbb.com域的用户网段是10.2.1.0/24。

路由器LNS和LAC路由可达并建立L2TP隧道，对接入的用户认证通过后，为用户分配对应网段的IP地址和网关。

版权所有 © 华为技术有限公司

图 6-1 配置 L2TP 多域接入组网图



操作步骤

步骤1 配置LAC

```
#
 sysname LAC
#
 l2tp enable  //启用L2TP功能
#
aaa
 authentication-scheme lmt
 domain aaa.com
  authentication-scheme lmt
 domain bbb.com
  authentication-scheme lmt
 local-user user1@aaa.com password cipher %@%@/|S75*sxcH2@FQL=wn#2@I`a%@%@
 local-user user1@aaa.com privilege level 15
 local-user user1@aaa.com service-type ppp
 local-user user2@bbb.com password cipher %@%@qh-<X%_2QB+^!UR+UkxUA/6<%@%@
 local-user user2@bbb.com privilege level 15
 local-user user2@bbb.com service-type ppp  //配置PPPoE服务器的本地用户名和类型，用于认证接入的用户
#
interface Virtual-Template1  //创建虚拟接口模板VT1，为PPPoE服务器配置参数
 ppp authentication-mode chap  //对接入用户的认证方式为CHAP认证
#
interface GigabitEthernet1/0/0
 ip address 202.1.1.2 255.255.255.0
#
interface GigabitEthernet2/0/0
 pppoe-server bind Virtual-Template 1  //接口上启用PPPoE Server功能，引入VT1的配置参数，认证接入的拨号用户
#
interface GigabitEthernet3/0/0
 pppoe-server bind Virtual-Template 1
#
l2tp-group 1  //创建L2TP组，为建立L2TP隧道配置参数
 tunnel password cipher %@%@/-#)Lg[S4F:#2~ZNvqa$]\DL%@%@  //缺省使能隧道认证，配置密文密码为huawei，和对端认证一致
 tunnel name lac1  //隧道的名称为lac1，用于被对端LNS识别
 start l2tp ip 202.1.1.1 domain aaa.com  //如接入用户的域名为aaa.com，则发起到对端的L2TP隧道连接
#
l2tp-group 2
 tunnel password cipher %@%@EB~j7Je>;@>uNr''D=J<]\WL%@%@
```


版权所有 © 华为技术有限公司

```
 tunnel name lac2
 start l2tp ip 202.1.1.1 domain bbb.com
#
```

步骤2 配置LNS

```
#
 sysname LNS
#
 l2tp enable
#
ip pool 1  //创建IP地址池，名称为1，为接入用户分配IP地址
 gateway-list 10.1.1.1  //网关地址
 network 10.1.1.0 mask 255.255.255.0  //可分配IP地址范围
#
ip pool 2
 gateway-list 10.2.1.1
 network 10.2.1.0 mask 255.255.255.0
#
aaa
 local-user user1@aaa.com password cipher %@%@/|S75*sxcH2@FQL=wn#2@I`a%@%@
 local-user user1@aaa.com privilege level 15
 local-user user1@aaa.com service-type ppp
 local-user user2@bbb.com password cipher %@%@qh-<X%_2QB+^!UR+UkxUA/6<%@%@
 local-user user2@bbb.com privilege level 15
 local-user user2@bbb.com service-type ppp
#
interface Virtual-Template1
 ppp authentication-mode chap
 remote address pool 1  //引入IP地址池，PPP认证通过后，为用户分配IP地址
 ip address 10.1.1.1 255.255.255.0  //地址池的网关地址
#
interface Virtual-Template2
 ppp authentication-mode chap
 remote address pool 2
 ip address 10.2.1.1 255.255.255.0
#
interface GigabitEthernet1/0/0
 ip address 202.1.1.1 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 10.3.1.1 255.255.255.0
#
l2tp-group 1
 allow l2tp virtual-template 1 remote lac1  //允许和对端隧道lac1建立L2TP隧道连接，引入VT1的配置参数
 tunnel password cipher %@%@eS*)0t-0D!,~pa;IPll=3liC%@%@
 tunnel name lns
#
l2tp-group 2
 allow l2tp virtual-template 2 remote lac2
 tunnel password cipher %@%@Cyor,=OAk#tWwA;%2\!W3lwj%@%@
 tunnel name lns
#
```

步骤3 验证配置结果

在LNS上执行命令**display l2tp session**可以查看到建立会话数为**2**。

PC1和PC2可以ping通PC3。

----结束

配置注意事项

- LAC为每个域名创建L2TP组，不同L2TP组的隧道名称不同。
- L2TP组缺省使能隧道认证，隧道两端密码相同。

 版权所有 © 华为技术有限公司

6.1.2 配置分支与总部之间通过 L2TP 方式实现互通，且与总部服务器之间的数据通过 IPSec 加密传输的示例

规格

适用于所有版本、所有形态的AR路由器。

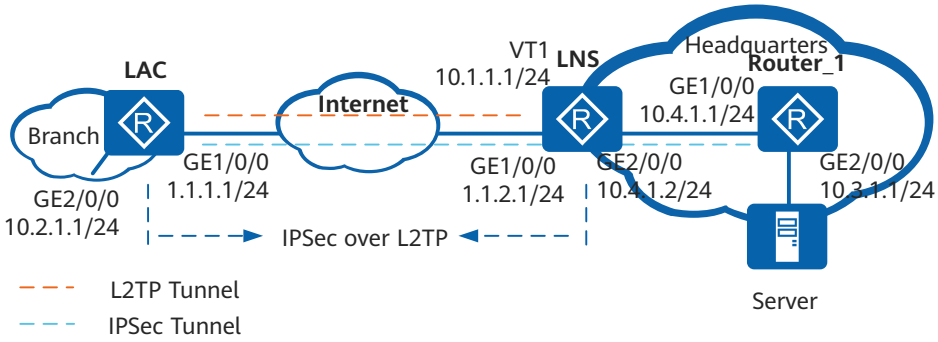
组网需求

如图6-2所示，企业总部在其他城市设有分支机构，分支机构部署为以太网络。

要求总部能为分支用户提供VPDN接入服务，允许分支内的任意用户接入。而且分支访问总部内网服务器时，需提供数据安全加密，防止数据被窃取。

配置LAC自拨号的方式，在LAC和LNS之间建立L2TP连接，实现总部为分支用户提供VPDN接入服务。然后配置IPSec，实现加密保护分支和总部内网服务器的交互数据，在LAC和LNS间IPSec加密数据通过L2TP隧道传输。

图 6-2 IPSec Over L2TP 组网图



操作步骤

步骤1 配置LAC

```
#
 sysname LAC
#
 l2tp enable  //使能L2TP
#
acl number 3000  //配置ACL
 rule 0 permit ip source 10.2.1.0 0.0.0.255 destination 10.3.1.0 0.0.0.255
#
ipsec proposal lac  //配置安全提议
 esp authentication-algorithm sha2-512
 esp encryption-algorithm aes-256
#
ike peer lac v1  //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
```


版权所有 © 华为技术有限公司

```
 pre-shared-key cipher %^%#JvZxR2g8c;a9~FPN~n'$7`DEV&=G(=Et02P/%\*!%^%#  //配置预共享密钥认证字为“huawei”，以密文显示，该命令在V2R3C00以前的版本中为“pre-shared-key huawei”，以明文显示
 remote-address 10.4.1.1  //指定IPSec对端的接口地址进行协商
#
ipsec policy lac 1 isakmp  //配置安全策略
 security acl 3000
 ike-peer lac
 proposal lac
#
interface Virtual-Template1  //创建VT虚拟接口模板
 ppp chap user huawei  //配置虚拟PPP用户的用户名为huawei
 ppp chap password cipher %@%@\;#%<c~6Y%cNZK/h.pK%:>Uo%@%@  //配置虚拟PPP用户的密码名为Huawei@1234
 ip address ppp-negotiate  //配置地址协商
 l2tp-auto-client enable  //L2TP自拨号方式
 ipsec policy lac  //绑定安全策略
#
interface GigabitEthernet1/0/0
 ip address 1.1.1.1 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 10.2.1.1 255.255.255.0
#
l2tp-group 1  //设置一个L2TP组并配置相关属性
 tunnel password cipher %@%@7v&1O#yr\#gl]w=Rk^uY:>@"%@%@  //使能隧道认证，配置密文密码为huawei，和对端认证一致
 tunnel name lac
 start l2tp ip 1.1.2.1 fullusername huawei
#
ip route-static 10.3.1.0 255.255.255.0 Virtual-Template1 10.1.1.1  //配置静态路由
ip route-static 10.4.1.0 255.255.255.0 Virtual-Template1
#
return
```

步骤2 配置LNS

```
#
 sysname LNS
#
 l2tp enable  //使能L2TP
#
ip pool 1  //配置IP地址池
 gateway-list 10.1.1.1
 network 10.1.1.0 mask 255.255.255.0
#
aaa  //配置本地用户，用户名为huawei，密码为Huawei@1234
 local-user huawei password cipher %^%#_<`.CO&(:LeS/$#F\H0Qv8B]KAZja3}3q'RNx;VI%^%#
 local-user huawei privilege level 15
 local-user huawei service-type ppp
#
interface Virtual-Template1  //创建VT虚拟接口模板
 ppp authentication-mode chap
 remote address pool 1
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/0
 ip address 1.1.2.1 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 10.4.1.2 255.255.255.0
#
l2tp-group 1 //设置一个L2TP组并配置相关属性
 allow l2tp virtual-template 1 remote lac
 tunnel password cipher %@%@FN15@5D_BGc=v"2~0=iJ,b+H%@%@  //使能隧道认证，配置密文密码为huawei，和对端认证一致
 tunnel name lns
#
ip route-static 10.2.1.0 255.255.255.0 Virtual-Template1  //配置静态路由
ip route-static 10.3.1.0 255.255.255.0 10.4.1.1
```

 版权所有 © 华为技术有限公司

```
#
return
```

步骤3 配置Router_1

```
#
 sysname Router_1
#
acl number 3000  //配置ACL
 rule 0 permit ip source 10.3.1.0 0.0.0.255 destination 10.2.1.0 0.0.0.255
#
ipsec proposal lac1 //配置安全提议
 esp authentication-algorithm sha2-512
 esp encryption-algorithm aes-256
#
ike peer lac1 v1  //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 pre-shared-key cipher %^%#K{JG:rWVHPMnf;5\|,GW(Luq'qi8BT4nOj%5W5=)%^%#  //配置预共享密钥认证字为“huawei”，以密文显示，该命令在V2R3C00以前的版本中为“pre-shared-key huawei”，以明文显示
#
ipsec policy-template temp 1  //配置IPSec策略模板
 security acl 3000
 ike-peer lac1
 proposal lac1
#
ipsec policy lac1 1 isakmp template temp  //配置IPSec策略
#
interface GigabitEthernet1/0/0
 ip address 10.4.1.1 255.255.255.0
 ipsec policy lac1  //绑定安全策略
#
interface GigabitEthernet2/0/0
 ip address 10.3.1.1 255.255.255.0
#
ip route-static 10.1.1.0 255.255.255.0 10.4.1.2  //配置静态路由
ip route-static 10.2.1.0 255.255.255.0 10.4.1.2
#
return
```

步骤4 验证配置结果

在LAC或者LNS上执行命令**display l2tp tunnel**可看到L2TP隧道及**Sessions**参数为**1**会话已建立。

在LAC或者Router_1上执行命令**display ike sa**可以查看到安全联盟建立成功，其中**Flag(s)**字段为**RD**表示SA已建立成功；**Phase**字段可以看到**1**和**2**两个阶段。

分支和总部可以相互Ping通。

----结束

配置注意事项

- LAC和LNS配置的验证用户名和密码必须统一。
- LAC的IPSec策略绑定在Virtual-Template1下。
- 配置LAC静态路由时，去往总部网段的路由的出接口必须为Virtual-Template1接口。

 版权所有 © 华为技术有限公司

6.1.3 配置分支机构与总部之间通过 L2TP over IPSec 方式实现安全互通的示例

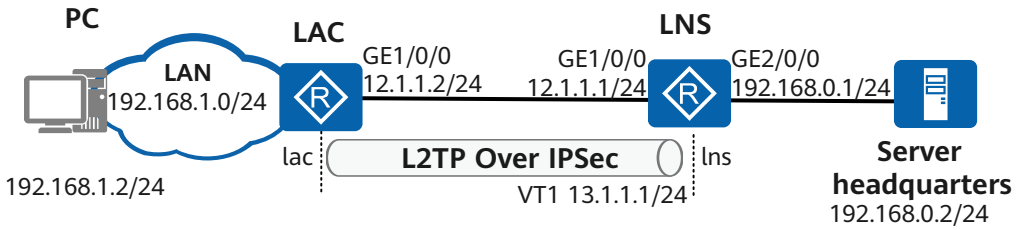
规格

适用于所有版本、所有形态的AR路由器。

组网需求

如图6-3所示，用户通过LAC接入LNS以访问总部内网，在LAC和LNS之间交互的数据通过IPSec加密后传输。

图 6-3 L2TP over IPSec 功能组网图



操作步骤

步骤1 配置LAC

```
#
 sysname LAC1
#
 l2tp enable  //使能L2TP
#
acl number 3000  //配置ACL规则，用于L2TP封装为外网地址后加
密
 rule 0 permit ip source 12.1.1.2 0 destination 12.1.1.1 0  //报文L2TP封装后，源地址和目的地址变为外网地
址
#
ipsec proposal lac  //配置安全提议
 esp authentication-algorithm sha2-512
 esp encryption-algorithm aes-256
#
ike peer lac v1  //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命
令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，
如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和
IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使
用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。
如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 pre-shared-key cipher %^%#JvZxR2g8c;a9~FPN~n'$7`DEV&=G(=Et02P/%\*!%^%#  //配置预共享密钥认证字
为“huawei”，以密文显示，该命令在V2R3C00以前的版本中为“pre-shared-key huawei”，以明文显示
 remote-address 12.1.1.1  //总部的外网地址
#
ipsec policy lac 1 isakmp  //配置安全策略
 security acl 3000
 ike-peer lac
 proposal lac
#
interface GigabitEthernet1/0/0  //外网接口
 ip address 12.1.1.2 255.255.255.0
 ipsec policy lac  //绑定安全策略
```


版权所有 © 华为技术有限公司

```
#
interface GigabitEthernet2/0/0  //内网接口
 ip address 192.168.1.1 255.255.255.0
#
interface Virtual-Template1  //配置虚拟PPP用户的用户名和密码，及PPP验证方式以及IP地址
 ppp chap user huawei
 ppp chap password cipher %@%@\;#%<c~6Y%cNZK/h.pK%:>Uo%@%@
 ip address ppp-negotiate  //配置地址协商
 l2tp-auto-client enable  //启用L2TP自拨号方式
#
l2tp-group 1  //设置一个L2TP组并配置相关属性
 tunnel password cipher %@%@d'o6Xpp(i/i:WRC)`'0#3nJ*%@%@      //缺省使能隧道认证，配置密文密码为
huawei，和对端认证一致
 tunnel LAC
 start l2tp ip 12.1.1.1 fullusername huawei
#
ip route-static 192.168.0.0 255.255.255.0 Virtual-Template1  //配置静态路由
#
return
```

步骤2 配置LNS

```
#
 sysname LNS1
#
 l2tp enable
#
acl number 3000  //配置ACL策略
 rule 0 permit ip source 12.1.1.1 0 destination 12.1.1.2 0
#
ipsec proposal lns  //配置安全提议
 esp authentication-algorithm sha2-512
 esp encryption-algorithm aes-256
#
ike peer lns v1  //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命
令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，
如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和
IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使
用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。
如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 pre-shared-key cipher %^%#K{JG:rWVHPMnf;5\|,GW(Luq'qi8BT4nOj%5W5=)%^%#  //配置预共享密钥认证
字为“huawei”，以密文显示，该命令在V2R3C00以前的版本中为“pre-shared-key huawei”，以明文显示
 remote-address 12.1.1.2
#
ipsec policy lns 1 isakmp  //配置安全策略
 security acl 3000
 ike-peer lns
 proposal lns
#
ip pool 1  //配置IP地址池
 gateway-list 13.1.1.1
 network 13.1.1.0 mask 255.255.255.0
#
aaa  //配置本地用户
 local-user huawei password cipher %^%#_<`.CO&(:LeS/$#F\H0Qv8B]KAZja3}3q'RNx;VI%^%#
 local-user huawei privilege level 15
 local-user huawei service-type ppp
#
interface Virtual-Template1  //创建虚模板Virtual-Template并配置认证方式、IP地址及接口地址
池
 ppp authentication-mode chap
 remote address pool 1
 ip address 13.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/0  //外网接口
 ip address 12.1.1.1 255.255.255.0
 ipsec policy lns  //绑定安全策略
#
interface GigabitEthernet2/0/0  //内网接口
 ip address 192.168.0.1 255.255.255.0
```

 版权所有 © 华为技术有限公司

```
#
l2tp-group 1  //设置一个L2TP组并配置相关属性
 allow l2tp virtual-template 1 remote LAC
 tunnel password cipher %@%@d'o6Xpp(i/i:WRC)`'0#3nJ*%@%@
 tunnel name LNS
#
ip route-static 192.168.1.0 255.255.255.0 Virtual-Template1  //配置静态路由
#
return
```

步骤3 验证配置结果

在LAC或者LNS上执行命令**display ike sa**可以查看到安全联盟的建立。

在LAC或者LNS上执行命令**display l2tp session**可以查看到L2TP会话的建立。

配置完后两侧用户可以互相ping通。

----结束

配置注意事项

- LAC和LNS配置的验证用户名和密码必须统一。
- 发起方和接收方IPSec策略绑定在外网接口，即L2TP封装后，再进行IPSEC封装。

6.1.4 配置远程拨号用户通过 L2TP 隧道接入总部的示例

规格

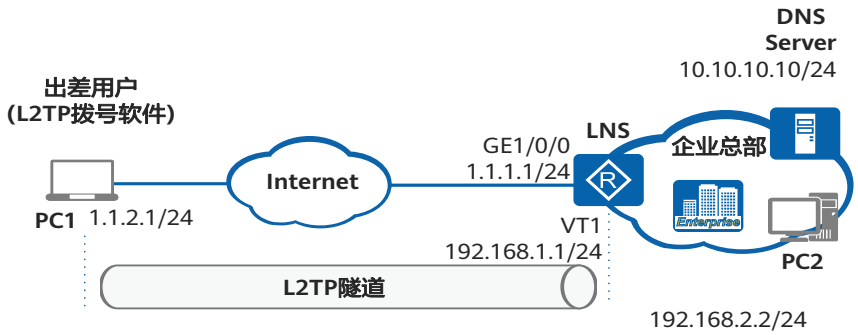
适用于所有版本、所有形态的AR路由器。

组网需求

如图6-4，企业出差员工的地理位置经常发生变动，并且随时需要和总部通信和访问总部内网资源。企业部署L2TP，出差员工通过拨号接入，实现总部网关对接入的用户进行辨别和管理。本示例在PC终端上以Windows 7为例。

建立L2TP连接之后，员工只能访问总部内网资源，为了满足企业出差员工拨号成功之后的外网访问需求，需要在LNS上部署NAT功能。

图 6-4 配置远程拨号用户发起 L2TP 隧道连接访问外网组网图



版权所有 © 华为技术有限公司

操作步骤

步骤1 配置LNS

```
#
 sysname LNS
#
 l2tp enable                          //启用L2TP功能
#
acl number 2001                       //配置ACL，进行NAT转换使用，将L2TP分配的地址进行NAT
 rule 5 permit source 192.168.1.0 0.0.0.255
#
ip pool lns                          //创建IP地址池，名称为lns，为接入用户分配IP地址
 gateway-list 192.168.1.1
 network 192.168.1.0 mask 255.255.255.0
#
aaa                                  //配置L2TP拨入的用户名密码
 local-user huawei password cipher %^%#_<`.CO&(:LeS/$#F\H0Qv8B]KAZja3}3q'RNx;VI%^%#
 local-user huawei privilege level 15
 local-user huawei service-type ppp
#
interface GigabitEthernet1/0/0
 ip address 1.1.1.1 255.255.255.0
 nat outbound 2001                   //配置NAT功能，实现公网访问功能
#
interface Virtual-Template1           //创建L2TP组，为建立L2TP隧道配置参数
 ppp authentication-mode chap
 remote address pool lns
 ppp ipcp dns 10.10.10.10             //分配DNS网关，以便员工使用域名访问外网资源
 ip address 192.168.1.1 255.255.255.0
#
l2tp-group 1
 undo tunnel authentication           //PC拨入，建议使用不认证的方式
 allow l2tp virtual-template 1
#
ip route-static 0.0.0.0 0.0.0.0 1.1.1.2
#
return
```

步骤2 配置Windows 7

修改Windows注册表，不使用数字证书认证功能。

单击“开始 > 运行”，输入**regedit**打开注册表，找到路径**HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters**，新建**DWORD**值，名称为**ProhibitIpSec**，取值为**1**，修改完成后重启PC。

创建L2TP网络连接。

打开“网络和共享中心”，单击“设置新的连接或网络”，选择“连接到工作区”，单击“下一步”。

单击“使用我的Internet连接”。

填入Internet地址，该地址为LNS的IP地址**1.1.1.1**，然后填入目标名称，作为网络连接的名称，可自行定义，此处填为**L2TP**，选中“现在不连接；仅进行设置以便稍后连接”，单击“下一步”。

填入用户名和密码，分别为**huawei**和**YsHsjx_202206**，单击“创建”。

说明

这里域无需配置。

 版权所有 © 华为技术有限公司

单击“关闭”。

配置L2TP连接的认证参数。

打开“网络和共享中心”，单击“连接到网络”，可以看到已创建的**L2TP**，右击**L2TP**选择“属性”，配置连接的参数。

如下“常规”页签中的参数不需要修改。

单击“选项”页签，勾选如下内容：“连接时显示进度”和“提示名称、密码和证书等(P)”。

说明

此页面如果单击“PPP设置”，采用默认方式，不需要进行设置。

单击“安全”页签，“VPN类型”可以选择默认的“自动”，也可以指定“使用IPsec的第2层隧道协议”。

在“运行这些协议”的复选项中，勾选如下内容：“未加密的密码(PAP)(U)”、“质询握手身份验证协议(CHAP)(H)”和“Microsoft CHAP 版本 2 (MS-CHAP v2)(C)”。

说明

此页面如果单击“高级设置”，会出现设置IPSec预共享密钥的窗体，请不要进行设置，此处并非真正设置IPSec预共享密钥的地方。

“网络”和“共享”这两个页签则无需修改。

打开“网络和共享中心”，单击“连接到网络”，可以看到已创建的**L2TP**，双击**L2TP**连接，输入用户名和密码，单击“连接”。

步骤3 验证配置结果

配置完成后PC1的**L2TP**连接正确获取私网IP地址**192.168.1.254**，和总部PC可以互通，也可以访问外网资源。

----结束

配置注意事项

配置过程中，需要注意以下几点：

- 配置L2TP组时，由于企业员工使用PC接入，不支持配置隧道认证功能。
- 对于需要访问外网的员工，需要将其所在网段加入ACL中，并对其进行NAT。
- 为了实现员工使用域名访问外网资源，需要在VT虚拟接口模板中配置LNS为对端设备指定DNS服务器的IP地址。

6.1.5 配置远程拨号用户通过认证域建立 L2TP 隧道接入总部的示例（Windows 7）

规格

适用于所有版本、所有形态的AR路由器。

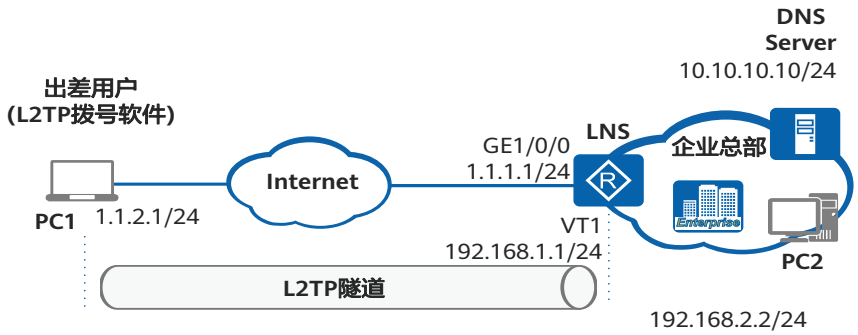
 版权所有 © 华为技术有限公司

组网需求

如图6-5，企业出差员工的地理位置经常发生变动，并且随时需要和总部通信。企业部署L2TP，出差员工通过拨号接入，实现总部网关对接入的用户进行认证和管理。本示例在PC终端上以Windows 7为例。

建立L2TP连接之后，员工只能访问总部内网资源，为了满足企业出差员工拨号成功之后的外网访问需求，需要在LNS上部署NAT功能。

图 6-5 配置远程拨号用户通过认证域建立 L2TP 隧道接入总部组网图



操作步骤

步骤1 配置LNS

```
#
 sysname LNS
#
 l2tp enable                          //启用L2TP功能
#
acl number 2001                       //配置ACL，进行NAT转换使用，将L2TP分配的地址进行NAT
 rule 5 permit source 192.168.1.0 0.0.0.255
#
ip pool lns                           //创建IP地址池，名称为lns，为接入用户分配IP地址
 gateway-list 192.168.1.1
 network 192.168.1.0 mask 255.255.255.0
#
aaa                                   //配置L2TP拨入的用户名密码
 authentication-scheme lmt
 domain huawei.com
  authentication-scheme lmt
 local-user 123456789@huawei.com password cipher %^%#_<`.CO&(:LeS/$#F\H0Qv8B]KAZja3}3q'RNx;VI%^
%#
 local-user 123456789@huawei.com privilege level 15
 local-user 123456789@huawei.com service-type ppp
#
interface GigabitEthernet1/0/0
 ip address 1.1.1.1 255.255.255.0
 nat outbound 2001                    //配置NAT功能，实现公网访问功能
#
interface Virtual-Template1           //创建VT虚拟接口模板，配置拨号参数
 ppp authentication-mode chap domain huawei.com   //配置认证方式时必须携带域名
 remote address pool lns
 ppp ipcp dns 10.10.10.10             //分配DNS网关，以便员工使用域名访问外网资源
 ip address 192.168.1.1 255.255.255.0
#
l2tp-group 1                          //创建L2TP组，配置L2TP连接参数
 undo tunnel authentication           //PC拨入，建议使用不认证的方式
 allow l2tp virtual-template 1
#
```


版权所有 © 华为技术有限公司

```
ip route-static 0.0.0.0 0.0.0.0 1.1.1.2
#
return
```

步骤2 配置Windows 7

1. 修改Windows注册表，不使用数字证书认证功能。

   单击“开始 > 运行”，输入**regedit**打开注册表，找到路径**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\RasMan\Parameters**，右击后选择**新建**，单击**DWORD（32 位）值**，填写名称为**ProhibitIpSec**，取值为**1**，修改完成后重启PC。

2. 创建L2TP网络连接。

   a. 打开“网络和共享中心”，单击“设置新的连接或网络”，选择“连接到工作区”，单击“下一步”。

   b. 单击“使用我的Internet连接”。

   c. 填入Internet地址，该地址为LNS的IP地址**1.1.1.1**，然后填入目标名称，作为网络连接的名称，可自行定义，此处填为**L2TP**，选中“现在不连接；仅进行设置以便稍后连接”，单击“下一步”。

   d. 填入用户名和密码，分别为**123456789@huawei.com**和**YsHsjx_202206**，单击“创建”。

      说明

      这里域无需配置。

   e. 单击“关闭”。

3. 配置L2TP连接的认证参数。

   a. 打开“网络和共享中心”，单击“连接到网络”，可以看到已创建的**L2TP**，右击**L2TP**选择“属性”，配置连接的参数。

      如下“常规”页签中的参数不需要修改。

   b. 单击“选项”页签，勾选如下内容：“连接时显示进度(D)”和“提示名称、密码和证书等(P)”。

      说明

      此页面如果单击“PPP设置”，采用默认方式，不需要进行设置。

   c. 单击“安全”页签，“VPN类型”可以选择默认的“自动”，也可以指定“使用IPsec的第 2 层隧道协议”。

      在“允许使用这些协议”的复选项中，勾选如下内容：“未加密的密码(PAP)(U)”、“质询握手身份验证协议(CHAP)(H)”和“Microsoft CHAP 版本 2(MS-CHAP v2)(C)”。

      说明

      此页面如果单击“高级设置”，会出现设置IPSec预共享密钥的窗体，请不要进行设置，此处并非真正设置IPSec预共享密钥的地方。

      “网络”和“共享”这两个页签则无需修改。

   d. 打开“网络和共享中心”，单击“连接到网络”，可以看到已创建的**L2TP**，双击**L2TP**连接，输入用户名和密码，单击“连接”。

 版权所有 © 华为技术有限公司

步骤3 验证配置结果

配置完成后，PC1能正确获取私网IP地址**192.168.1.254**，可以和总部PC互通，也可以访问外网资源。

----结束

配置注意事项

- 配置L2TP组时，由于企业员工使用PC接入，不支持配置隧道认证功能。
- 对于需要访问外网的员工，需要将其所在网段加入ACL中，并对其进行NAT。
- 为了实现员工使用域名访问外网资源，需要在VT虚拟接口模板中配置LNS为对端设备指定DNS服务器的IP地址。

6.1.6 配置移动办公用户通过认证域建立 L2TP 隧道接入总部的示例（Windows 10）

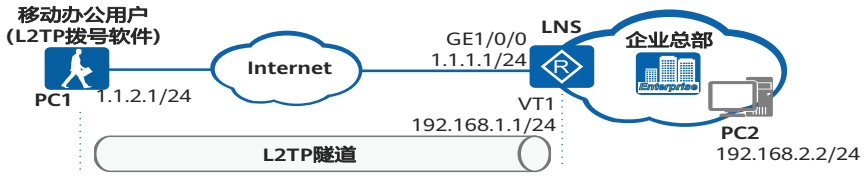
规格

适用于所有版本、所有形态的AR路由器。

组网需求

如图6-6，移动办公员工的地理位置经常发生变动，并且随时需要和总部通信。企业部署L2TP，将总部网关部署为LNS，移动办公用户在PC终端上使用L2TP拨号软件与企业总部建立L2TP隧道连接，实现总部网关对接入的用户进行认证和管理。本示例在PC终端上以Windows 10为例。建立L2TP连接之后，员工只能访问总部内网资源，为了满足企业出差员工拨号成功之后的外网访问需求，需要在LNS上部署NAT功能。

图 6-6 配置移动办公用户通过认证域建立 L2TP 隧道接入总部组网图



说明

1607(14393)版本的Windows 10系统不支持通过拨号建立L2TP连接，请使用Windows 10的其他版本。

操作步骤

步骤1 配置LNS

配置ACL、公网IP地址及路由，假设访问公网路由的下一跳地址为1.1.1.2。

```
<Huawei> system-view
[Huawei] sysname LNS
[LNS] acl number 2001
[LNS-acl-adv-2001] rule 5 permit source 192.168.1.0 0.0.0.255
```


版权所有 © 华为技术有限公司

```
[LNS-acl-adv-2001] quit
[LNS] interface gigabitethernet 1/0/0
[LNS-GigabitEthernet1/0/0] ip address 1.1.1.1 255.255.255.0
[LNS-GigabitEthernet1/0/0] nat outbound 2001
[LNS-GigabitEthernet1/0/0] quit
[LNS] ip route-static 0.0.0.0 0 1.1.1.2
```

配置L2TP用户的用户名为**huawei**，密码为**YsHsjx_202206**，用户类型固定为**ppp**。

```
[LNS] aaa
[LNS-aaa] local-user huawei password
Please configure the login password (8-128)
It is recommended that the password consist of at least 2 types of characters, i
ncluding lowercase letters, uppercase letters, numerals and special characters.
Please enter password:
Please confirm password:
Info: Add a new user.
Warning: The new user supports all access modes. The management user access mode
s such as Telnet, SSH, FTP, HTTP, and Terminal have security risks. You are advi
sed to configure the required access modes only.
[LNS-aaa] local-user huawei service-type ppp
[LNS-aaa] quit
```

定义一个地址池，为拨入用户分配地址。

```
[LNS] ip pool lns
[LNS-ip-pool-lns] network 192.168.1.0 mask 24
[LNS-ip-pool-lns] gateway-list 192.168.1.1
[LNS-ip-pool-lns] quit
```

配置虚拟接口模板。

```
[LNS] interface virtual-template 1
[LNS-Virtual-Template1] ip address 192.168.1.1 255.255.255.0
[LNS-Virtual-Template1] ppp authentication-mode chap
[LNS-Virtual-Template1] remote address pool lns
[LNS-Virtual-Template1] quit
```

使能L2TP功能，并创建L2TP组编号为**1**。

```
[LNS] l2tp enable
[LNS] l2tp-group 1
```

禁止隧道认证功能，Windows 10不支持隧道认证。

```
[LNS-l2tp1] undo tunnel authentication
```

配置LNS绑定虚拟接口模板。

```
[LNS-l2tp1] allow l2tp virtual-template 1
```

步骤2 配置Windows 10

1. 修改Windows注册表，不使用数字证书认证功能。

   单击“开始 > 运行”，输入**regedit**打开注册表，找到路径**HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters**，新建**DWORD**值，名称为**ProhibitIpSec**，取值为**1**，并选择基数为**十六进制**，修改完成后重启PC，配置生效。

2. 创建L2TP网络连接。

   a. 右键单击任务栏网络图标，选择“打开网络和共享中心”。

   b. 选择“设置新的连接或网络”，创建一个新的网络连接。

   c. 选择“连接到工作区”，单击“下一步”。

   d. 单击“使用我的Internet连接(VPN)(I)”。

 版权所有 © 华为技术有限公司

e. 选择“我将稍后设置Internet连接”。

f. 输入Internet地址，即LNS用于建立VPN隧道的接口的IP地址。该地址为LNS的IP地址**1.1.1.1**，填入目标名称为**L2TP**，作为网络连接的名称，单击“创建”。

g. 在“网络和共享中心”单击“更改适配器设置”。

h. 选中新建的连接后单击右键，选择“属性”。

i. 单击“安全”页签，“VPN类型”选择“使用IPsec的第 2 层隧道协议”。

在“允许使用这些协议(P)”的复选项中，勾选如下内容：“未加密的密码(PAP)(U)”、“质询握手身份验证协议(CHAP)(H)”和“Microsoft CHAP Version 2 (MS-CHAP v2)”。

说明

此页面如果单击“高级设置”，会出现设置IPSec预共享密钥的窗体，请不要进行设置，此处并非真正设置IPSec预共享密钥的地方。

j. 打开“网络和Internet”设置，选择“VPN > L2TP”，单击“连接”。

k. 输入用户名和密码，分别为**huawei**和**YsHsjx_202206**，单击“确定”。

l. L2TP拨号成功，系统显示已连接。

步骤3 验证配置结果。

配置完成后PC1的**L2TP**连接正确获取私网IP地址**192.168.1.254**，和总部PC可以互通。

----结束

配置注意事项

- 配置L2TP组时，由于移动办公用户使用PC接入，不支持配置隧道认证功能。
- 对于需要访问外网的员工，需要在LNS上配置IP地址池所在网段加入ACL，并对分配给用户的IP地址进行NAT转换。
- 为了实现员工使用域名访问外网资源，需要在VT虚拟接口模板中配置LNS为对端设备指定DNS服务器的IP地址。

6.1.7 配置远程拨号用户通过认证域建立 L2TP 隧道接入总部的示例（VPN Client）

规格

适用于所有版本、所有形态的AR路由器。

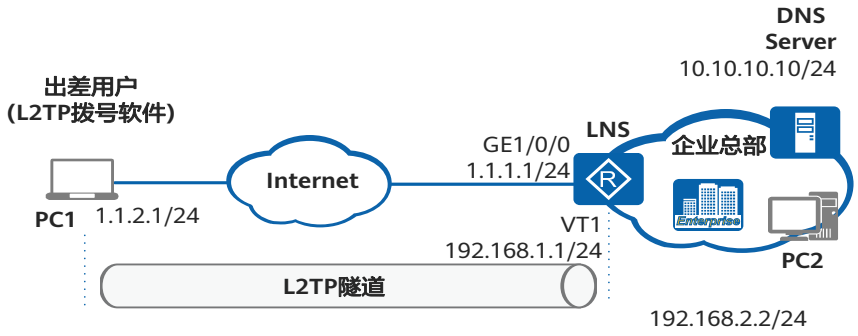
组网需求

如图6-7，企业出差员工的地理位置经常发生变动，并且随时需要和总部通信。企业部署L2TP，出差员工通过拨号接入，实现总部网关对接入的用户进行认证和管理。本示例在PC终端上以VPN Client为例。

建立L2TP连接之后，员工只能访问总部内网资源，为了满足企业出差员工拨号成功之后的外网访问需求，需要在LNS上部署NAT功能。

版权所有 © 华为技术有限公司

图 6-7 配置远程拨号用户通过认证域建立 L2TP 隧道接入总部组网图



操作步骤

步骤1 配置LNS

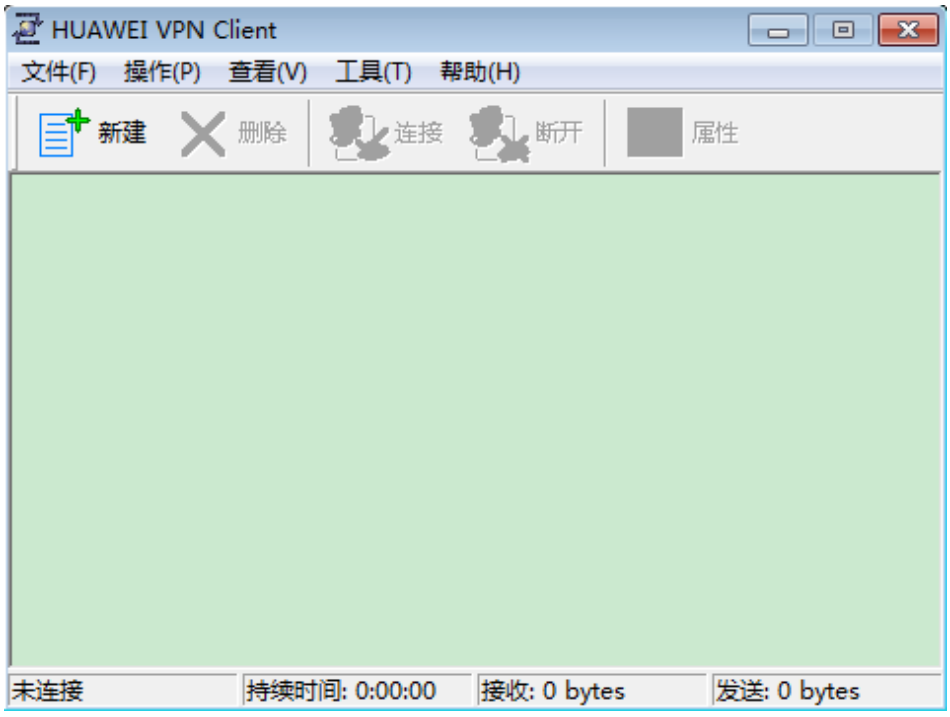
```
#
 sysname LNS
#
 l2tp enable                          //启用L2TP功能
#
acl number 2001                       //配置ACL，进行NAT转换使用，将L2TP分配的地址进行NAT
 rule 5 permit source 192.168.1.0 0.0.0.255
#
ip pool lns                           //创建IP地址池，名称为lns，为接入用户分配IP地址
 gateway-list 192.168.1.1
 network 192.168.1.0 mask 255.255.255.0
#
aaa                                   //配置L2TP拨入的用户名密码
 authentication-scheme lmt
 domain huawei.com
  authentication-scheme lmt
 local-user 123456789@huawei.com password cipher %^%#_<`.CO&(:LeS/$#F\H0Qv8B]KAZja3}3q'RNx;VI%^
%#
 local-user 123456789@huawei.com privilege level 15
 local-user 123456789@huawei.com service-type ppp
#
interface GigabitEthernet1/0/0
 ip address 1.1.1.1 255.255.255.0
 nat outbound 2001                    //配置NAT功能，实现公网访问功能
#
interface Virtual-Template1           //创建VT虚拟接口模板，配置拨号参数
 ppp authentication-mode chap domain huawei.com   //配置认证方式时必须携带域名
 remote address pool lns
 ppp ipcp dns 10.10.10.10             //分配DNS网关，以便员工使用域名访问外网资源
 ip address 192.168.1.1 255.255.255.0
#
l2tp-group 1                          //创建L2TP组，配置L2TP连接参数
 undo tunnel authentication           //PC拨入，建议使用不认证的方式
 allow l2tp virtual-template 1
#
ip route-static 0.0.0.0 0.0.0.0 1.1.1.2
#
return
```

步骤2 配置VPN Client

1. # 创建L2TP网络连接。

   a. 双击HUAWEI VPN Client，打开程序，单击“新建”，进入“新建连接向导”。

版权所有 © 华为技术有限公司



b. 选择“通过输入参数创建连接”，单击“下一步”。

c. 在“LNS服务器地址”填入**1.1.1.1**，输入用户名和密码，单击“下一步”。

版权所有 © 华为技术有限公司

d. “认证模式”选择“CHAP”，单击“下一步”。

说明

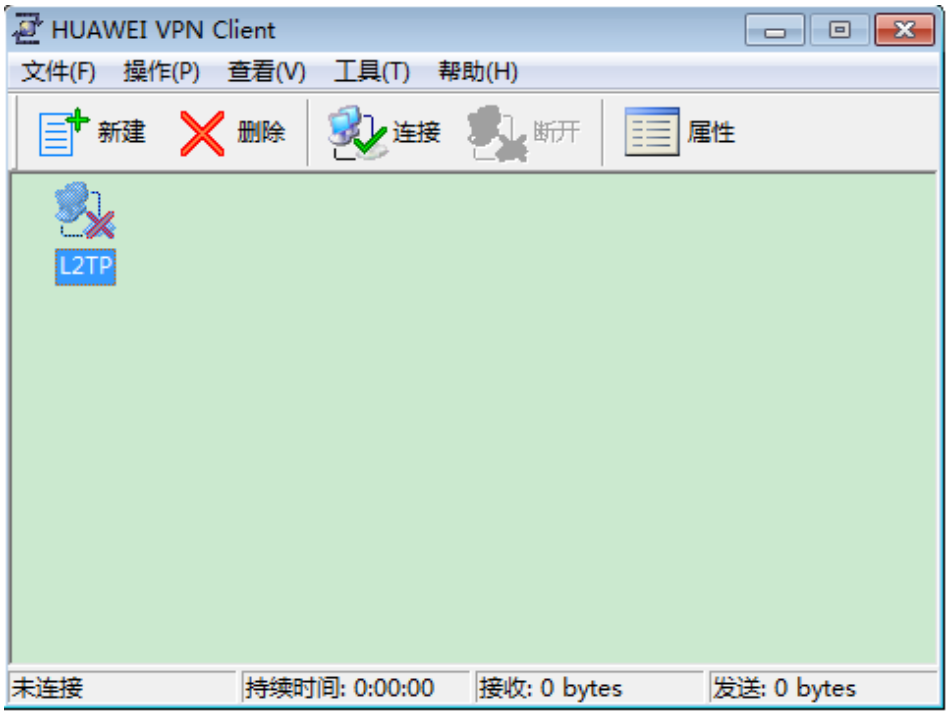
当LNS配置隧道名称时，这里需配置**隧道名称**。

当LNS配置隧道验证功能时，这里需选择**启用隧道验证功能**，并配置**隧道验证密码**。

e. 在“名字为”填入VPN连接的名称，可自行定义，此处填为**L2TP**，单击“完成”。

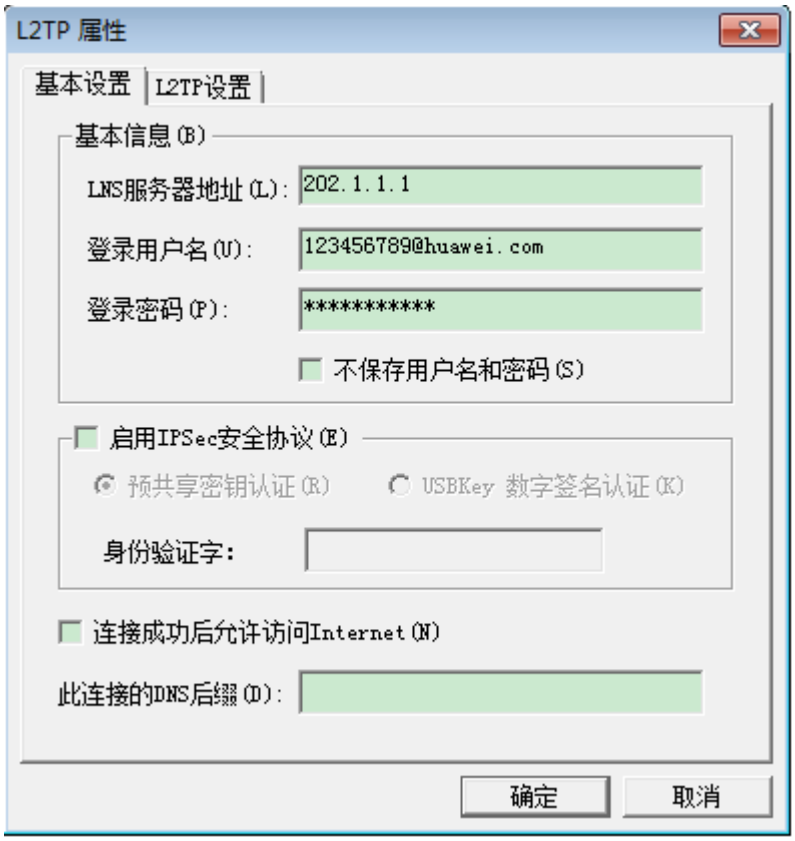
版权所有 © 华为技术有限公司

2. 修改L2TP连接的参数。
   a. 创建L2TP连接之后，选中需要修改的连接，此处以“L2TP”为例。
   选中“L2TP”，单击“属性”，打开“L2TP属性”。

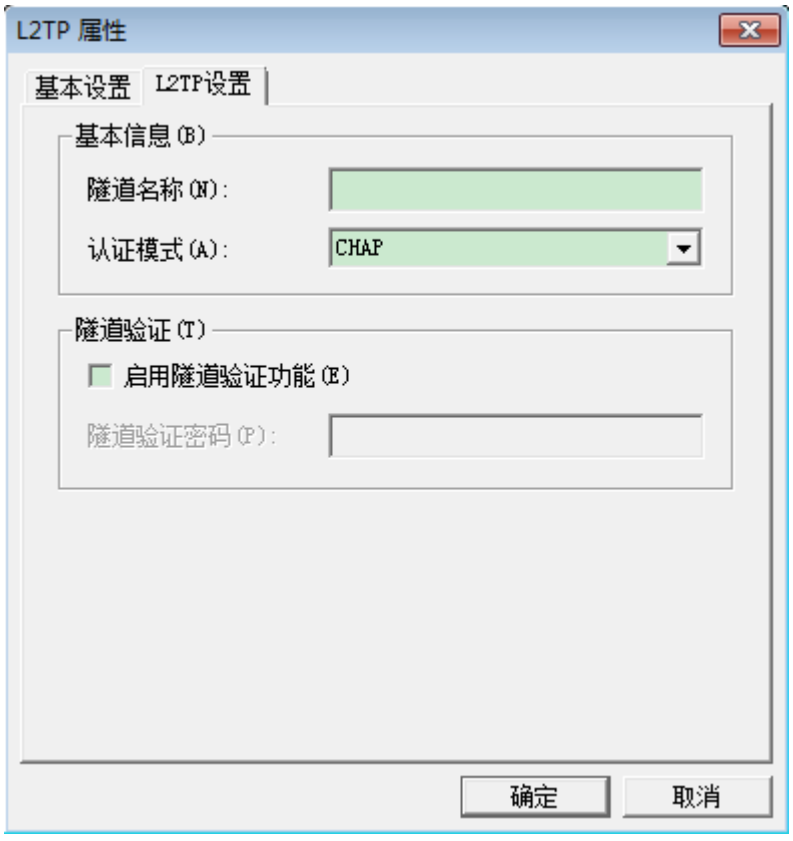


   b. 单击“基本设置”页签，如需修改用户名和密码，请根据实际情况进行配置。

版权所有 © 华为技术有限公司

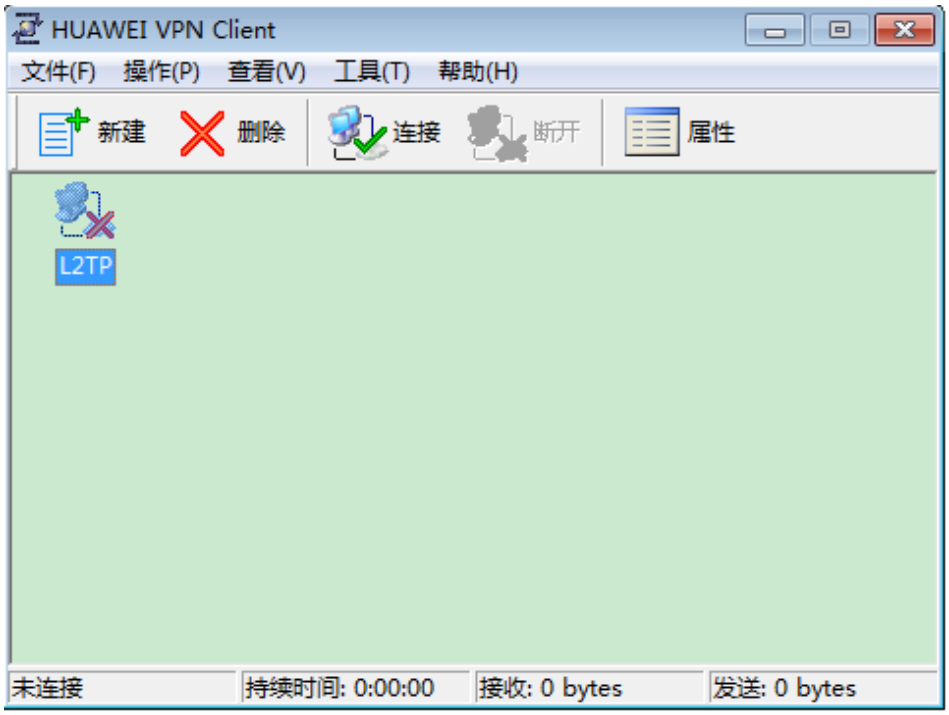


c. 如下“L2TP设置”页签中的参数，在LNS端没有修改配置的情况下不需要修改，与LNS配置保持一致即可。



版权所有 © 华为技术有限公司

d. 在“HUAWEI VPN Client”中，选择创建的**L2TP**，单击“连接”。



步骤3 验证配置结果

配置完成后，PC1能正确获取私网IP地址**192.168.1.254**，可以和总部PC互通，也可以访问外网资源。

----结束

配置注意事项

- 对于需要访问外网的员工，需要将其所在网段加入ACL中，并对其进行NAT。
- 为了实现员工使用域名访问外网资源，需要在VT虚拟接口模板中配置LNS为对端设备指定DNS服务器的IP地址。

6.1.8 配置远程拨号用户通过 L2TP over IPSec 方式接入总部的示例

规格

适用于所有版本、所有形态的AR路由器。

组网需求

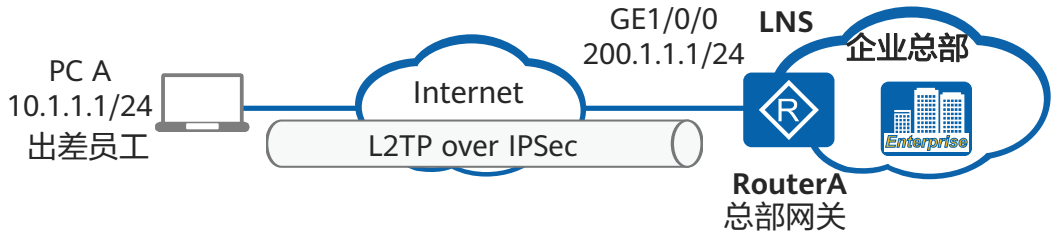
如图6-8所示，某企业使用RouterA作为总部网关。企业的出差员工用PC A通过L2TP拨号与总部建立通信。为了保证出差员工接入内网的安全性，企业希望在出差员工和总部网关之间建立一个IPSec隧道。

本示例配置步骤在PC终端上以Windows 7系统为例。

出差员工与总部之间是建立基于主机到网关的IPSec隧道，因此需要基于传输模式建立IPSec隧道。

版权所有 © 华为技术有限公司

图 6-8 配置 PC 与路由器进行 L2TP over IPSec 拨号组网图



操作步骤

步骤1 配置RouterA

```
#
 sysname RouterA  //配置设备名称
#
 l2tp enable  //启用L2TP功能
#
ipsec proposal prop  //配置IPSec安全提议
 encapsulation-mode transport
#
ike proposal 5  //配置IKE安全提议
#
ike peer peer1 v1  //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 pre-shared-key cipher %^%#JvZxR2g8c;a9~FPN~n'$7`DEV&=G(=Et02P/%\*!%^%#  //配置预共享密钥认证字为“YsHsjx_202206”，以密文显示，该命令在V2R3C00以前的版本中为“pre-shared-key huawei”，以明文显示
 ike-proposal 5
#
ipsec policy-template temp1 10  //配置策略模板
 ike-peer peer1
 proposal prop
#
ipsec policy policy1 1 isakmp template temp1  //配置安全策略
#
ip pool lns  //配置IP地址池，用于设备为接入PC分配私网IP地址
 gateway-list 192.168.1.1
 network 192.168.1.0 mask 255.255.255.0
#
aaa  //配置LNS的本地用户名和类型，用于认证接入的用户
 local-user huawei password cipher %^%#_<`.CO&(:LeS/$#F\H0Qv8B]KAZja3}3q'RNx;Vl%^%#
 local-user huawei privilege level 15
 local-user huawei service-type ppp
#
interface Virtual-Template1  //配置虚拟PPP用户的用户名和密码，PPP验证方式和IP地址
 ppp authentication-mode chap
 remote address pool lns
 ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet1/0/0
 ip address 200.1.1.1 255.255.255.0
 ipsec policy policy1
#
l2tp-group 1  //设置一个L2TP组并配置相关属性
 undo tunnel authentication
 allow l2tp virtual-template 1
#
```


版权所有 © 华为技术有限公司

```
ip route-static 0.0.0.0 0.0.0.0 200.1.1.2  //配置静态路由，保证两端路由可达
#
return
```

步骤2 配置PC A

修改Windows注册表，

单击“开始 > 运行”，输入regedit打开注册表，找到路径**HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\PolicyAgent**，新建DWORD值，名称为**AssumeUDPEncapsulationContextOnSendRule**，取值为2；找到路径**HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters**，新建DWORD值，名称为**ProhibitIpSec**，取值为1，修改完成后重启PC。

创建L2TP连接。

单击“开始 > 控制面板 > 网络和Internet > 网络和共享中心”，选择“设置新的连接或网络”。

出现“设置连接或网络”界面，选择“连接到工作区”，单击“下一步”。

选择“使用我的Internet连接(VPN)(I)”。

输入要连接的Internet地址（RouterA的IP地址），并单击“下一步”。

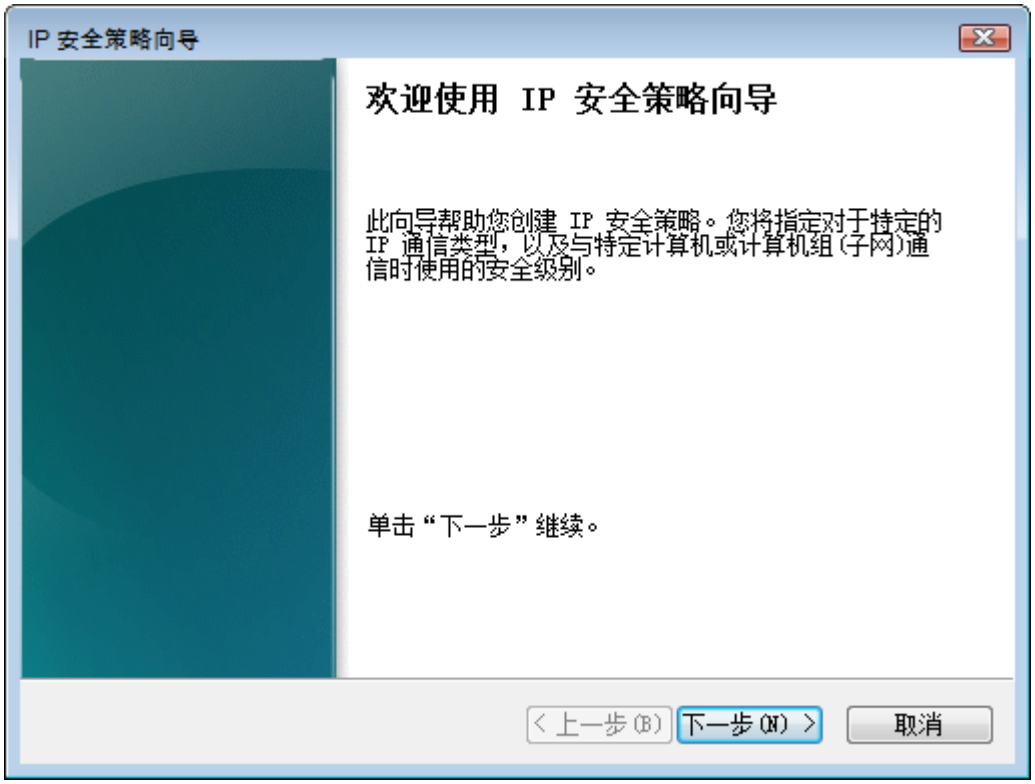
输入用户名和密码。

创建IP安全策略。

单击“控制面板”->“系统和安全”->“管理工具”->“本地安全策略”。

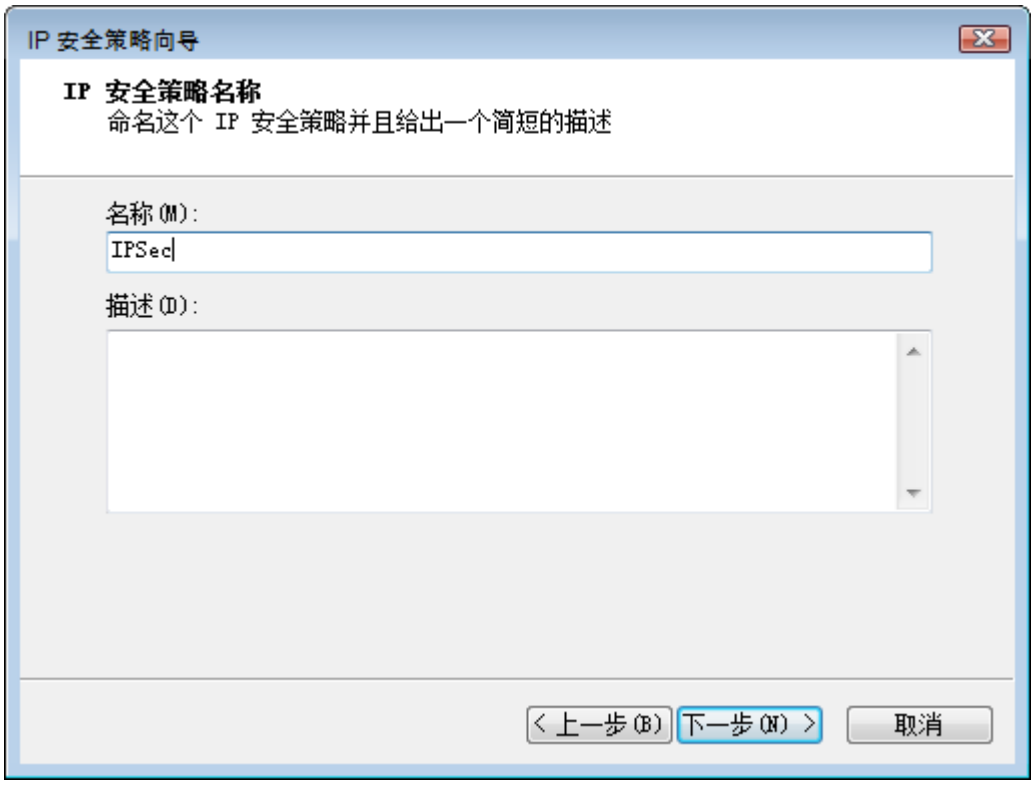
创建IP安全策略的向导步骤如图6-9、图6-10、图6-11和图6-12所示。

图 6-9 欢迎使用 IP 安全策略向导界面



版权所有 © 华为技术有限公司

图 6-10 编辑 IP 安全策略名称界面



版权所有 © 华为技术有限公司

图 6-11 指定 PC 对安全通讯作出响应界面

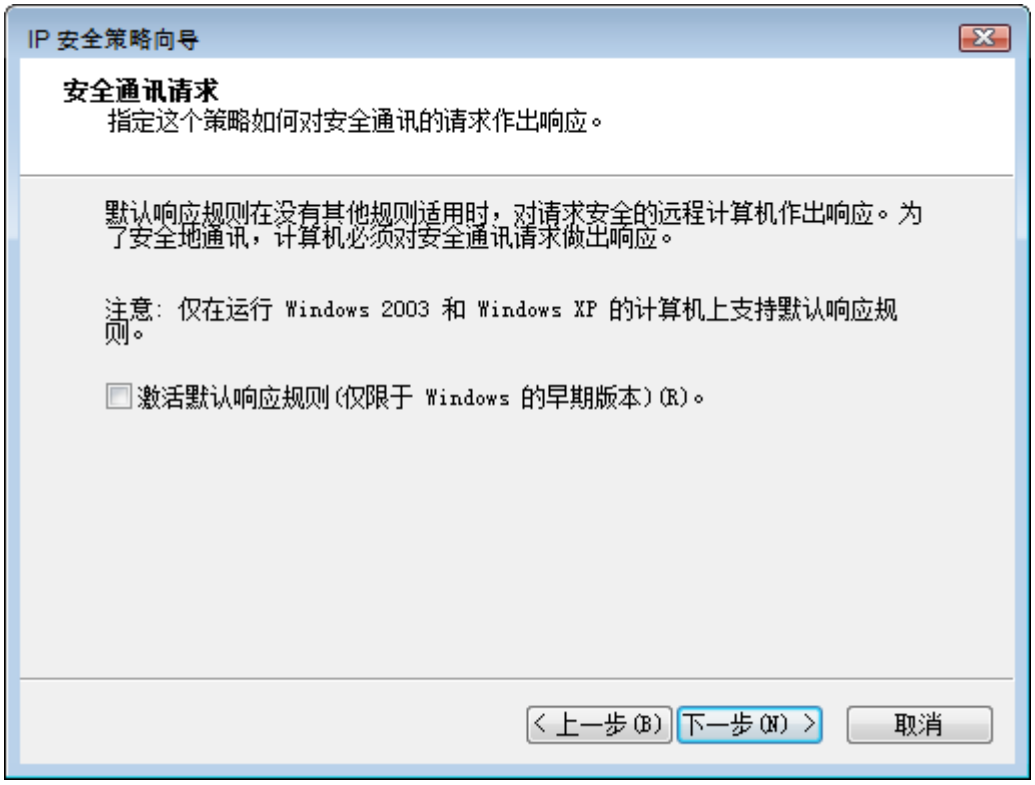
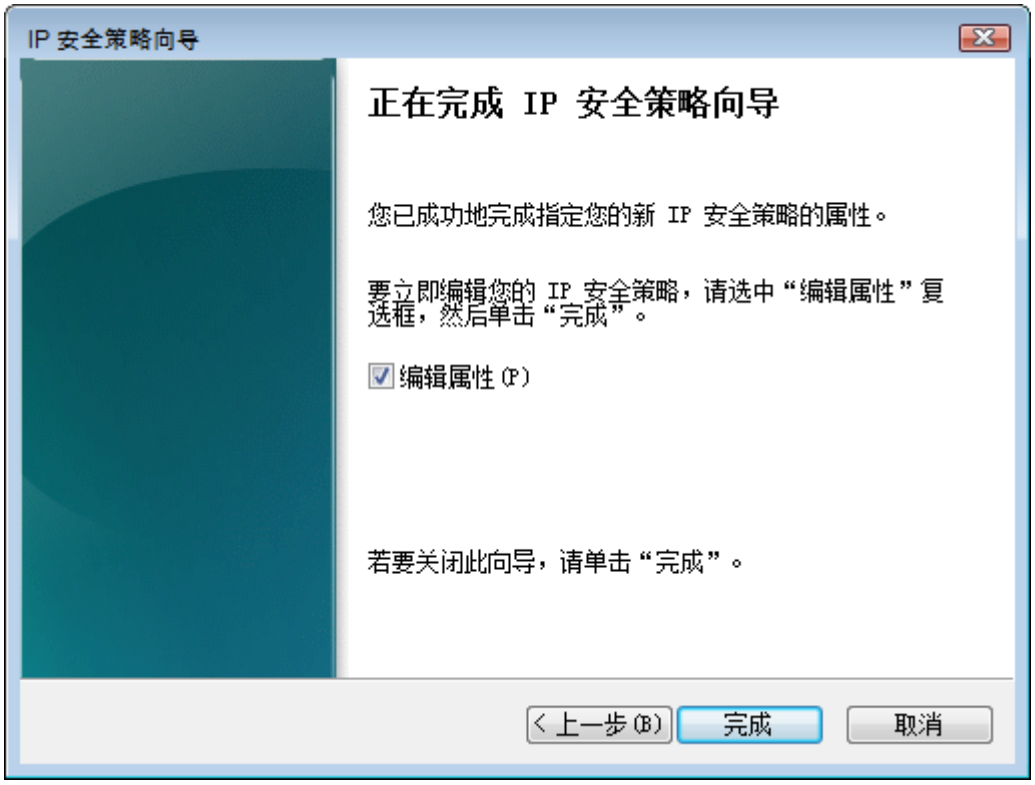


图 6-12 完成 IP 安全策略向导界面



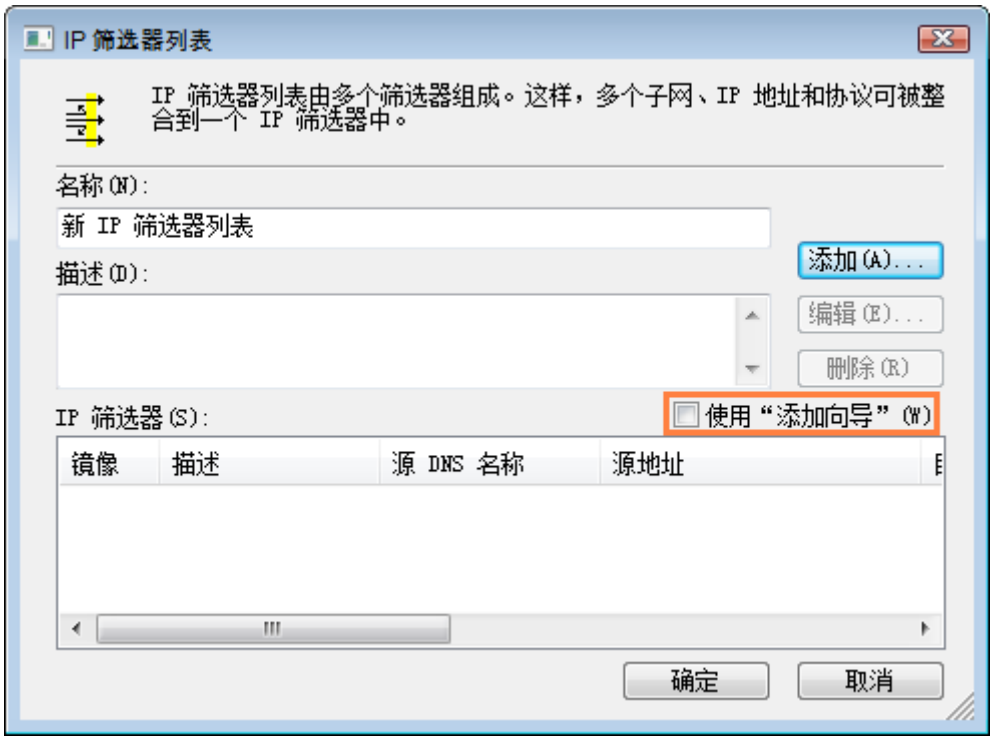
版权所有 © 华为技术有限公司

接下来进入IP安全策略的属性窗口的规则页，即将“使用‘添加向导’”的勾选取消，并选择“添加”以添加规则。

配置安全策略的属性。

1. 配置“IP筛选器列表”
   使用“添加向导”的勾选取消，并选择“添加”以添加IP筛选器。

   图 6-13 添加“IP 筛选器”界面



   接下来配置IP筛选器的属性，编辑“地址”页签，分别将“我的IP地址”作为源地址、总部网关的IP地址作为目标地址，选择数据流镜像匹配。
   编辑“协议”页签，选择数据的协议类型为“任何”。
   编辑“描述”页签，可以为该IP筛选器添加描述。
   单击“确定”，回到IP筛选器列表属性页，可看到新编辑的IP筛选器。
   单击“确定”回到IP安全策略的规则页面。
2. 配置“筛选器操作”
   选择“筛选器操作”页签，并单击“编辑”。
   出现筛选器操作的属性页面，并单击“添加”。
   出现“安全方法”属性页面，选择“自定义”的“设置”选项。
   出现“自定义安全方法”的属性页面，请进行设置。
   依次单击“确定”回到“筛选器操作”页签。

   说明

   MD5、SHA1、DES和3DES算法存在安全隐患，请谨慎使用。

版权所有 © 华为技术有限公司

3. 配置“身份验证方法”

   选择“身份验证方法”页签，并单击“编辑”。

   出现身份验证方法的属性页面，即选择“预共享密钥”方法，预共享密钥为huawei，

4. 配置“隧道设置”，即选择安全协议对数据的封装模式

   选择“隧道设置”页签，选择“此规则不指定IPSec隧道(T)”即传输模式。

5. 配置“连接类型”

   选择“连接类型”页签，保持原有选项“所有网络连接”。

6. 配置“密钥交换”，即配置IKE安全提议

   单击“应用”，回到IP安全策略属性界面，并选择“常规”页签，选择“设置”。

   进入“密钥交换设置”界面，选择“方法”。

   进入“密钥交换安全方法”界面，选择“添加”。

   添加下列安全方法，并单击“确定”。

   回到IP安全策略属性界面，单击“确定”，完成IP安全策略的配置。

   说明

   MD5、SHA1、DES和3DES算法存在安全隐患，请谨慎使用。

应用IP安全策略。

回到“本地安全策略”页面，右击配置好的IP安全策略，单击“分配”，即将IP安全策略在PC上应用。

在“网络连接”中选择已配置好的L2TP连接。输入用户名和密码，就可以进行L2TP连接了。

步骤3 验证配置结果

配置成功后，在PC A上执行**ping**操作仍然可以ping通RouterA，它们之间的数据传输将被加密，在RouterA上执行命令**display ipsec statistics esp**可以查看数据包的统计信息。

在RouterA上执行**display ike sa**和**display ipsec sa**命令，可以看到IPSec隧道配置成功的信息。

----结束

配置注意事项

PC上IPSec的配置相对路由器较复杂，请先熟悉路由器上IPSec的基本配置再在PC上操作。

6.1.9 配置 LAC 接入 PPPoE 用户发起 L2TP 隧道连接来实现分支与总部互通的示例

规格

适用于所有版本、所有形态的AR路由器。

 版权所有 © 华为技术有限公司

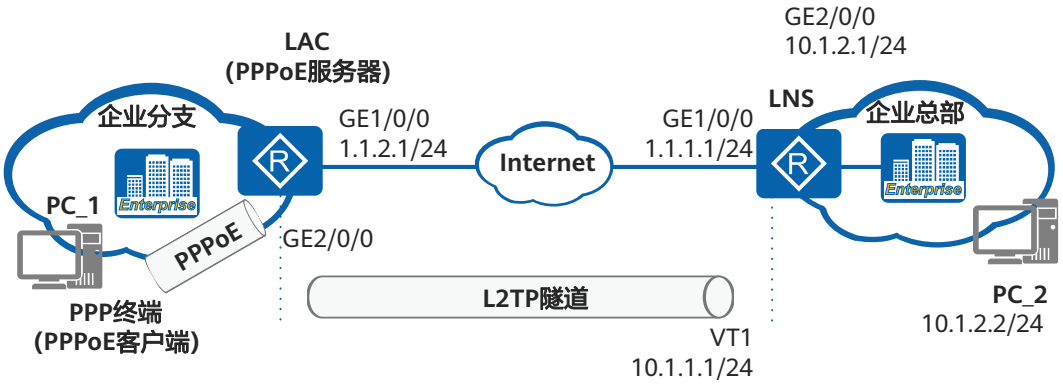
组网需求

如图6-14，企业总部在其他城市设有分支机构，分支机构内部使用以太网络。

分支用户需要和总部用户建立VPDN连接，在分支和总部之间部署L2TP，其中分支机构没有拨号网络，将分支的网关部署为PPPoE服务器，使分支用户的PPP拨号可以通过以太网络传输，同时分支网关也作为LAC，和总部建立L2TP隧道。

企业总部的网关部署为LNS，为分支用户提供接入服务，实现分支用户和总部网关之间的L2TP连接。

图 6-14 配置 LAC 接入 PPPoE 用户发起 L2TP 隧道连接来实现分支与总部互通组网图



操作步骤

步骤1 配置LAC

```
#
 sysname LAC
#
 l2tp enable   //启用L2TP功能
#
aaa    //配置L2TP的用户名和密码
 local-user huawei password cipher %^%#_<`.CO&(:LeS/$#F\H0Qv8B]KAZja3}3q'RNx;VI%^%#
 local-user huawei privilege level 15
 local-user huawei service-type ppp
#
interface Virtual-Template1
 ppp authentication-mode chap
#
interface GigabitEthernet1/0/0
 ip address 1.1.2.1 255.255.255.0
#
interface GigabitEthernet2/0/0
 pppoe-server bind Virtual-Template 1
#
l2tp-group 1   //创建L2TP组，配置L2TP连接参数
 tunnel password cipher %@%@/-#)Lg[S4F:#2~ZNvqa$]\DL%@%@
 tunnel name lac
 start l2tp ip 1.1.1.1 fullusername huawei
#
ip route-static 1.1.1.1 255.255.255.255 1.1.2.2
#
return
```

步骤2 配置LNS

```
#
 sysname LNS
```


版权所有 © 华为技术有限公司

```
#
 l2tp enable   //启用L2TP功能
#
ip pool 1   //创建IP地址池，为接入用户分配IP地址
 gateway-list 10.1.1.1
 network 10.1.1.0 mask 255.255.255.0
#
aaa      //配置L2TP的用户名和密码
 local-user huawei password cipher %^%#_<`.CO&(:LeS/$#F\H0Qv8B]KAZja3}3q'RNx;VI%^%#
 local-user huawei privilege level 15
 local-user huawei service-type ppp
#
interface Virtual-Template1   //创建VT虚拟接口模板，配置拨号参数
 ppp authentication-mode chap
 remote address pool 1
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/0
 ip address 1.1.1.1 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 10.1.2.1 255.255.255.0
#
l2tp-group 1   //创建L2TP组，配置L2TP连接参数
 allow l2tp virtual-template 1 remote lac
 tunnel password cipher %@%@EB~j7Je>;@>uNr''D=J<]\WL%@%@
 tunnel name lns
#
ip route-static 1.1.2.1 255.255.255.255 1.1.1.2
#
return
```

步骤3 验证配置结果

在LAC或者LNS上执行命令**display l2tp tunnel**可看到L2TP隧道及**Sessions**参数为**1**会话已建立。

企业分支与总部可以相互Ping通。

----结束

配置注意事项

- LAC和LNS配置的验证用户名和密码必须一致。
- 配置LAC静态路由时，去往总部网段的路由的出接口必须为Virtual-Template1接口。

6.1.10 配置 LAC 接入 PPPoE 用户发起 L2TP 隧道连接来实现分支与总部互通的示例（RADIUS 服务器）

规格

适用于所有版本、所有形态的AR路由器。

组网需求

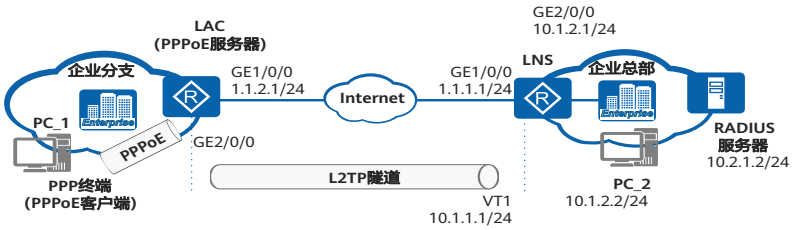
如图6-15，企业总部在其他城市设有分支机构，分支机构内部使用以太网络。

分支用户需要和总部用户建立VPDN连接，在分支和总部之间部署L2TP隧道，其中分支机构没有拨号网络，将分支的网关部署为PPPoE服务器，使分支用户的PPP拨号可以通过以太网络传输，同时分支网关也作为LAC和总部建立L2TP隧道。

 版权所有 © 华为技术有限公司

企业总部的网关部署为LNS，通过RADIUS服务器对用户进行认证和分配指定的IP地址，实现分支用户和总部网关之间的L2TP连接。

图 6-15 配置 LAC 接入 PPPoE 用户发起 L2TP 隧道连接来实现分支与总部互通组网图



操作步骤

步骤1 配置LAC

```
#
 sysname LAC
#
 l2tp enable  //启用L2TP功能
#
aaa  //配置拨号用户的用户名和密码
 local-user l2tp@huawei.com password cipher %^%#_<`.CO&(:LeS/$#F\H0Qv8B]KAZja3}3q'RNx;VI%^%#
 local-user l2tp@huawei.com privilege level 15
 local-user l2tp@huawei.com service-type ppp
#
interface Virtual-Template1  //创建VT虚拟接口模板，配置拨号参数
 ppp authentication-mode chap
#
interface GigabitEthernet1/0/0
 ip address 1.1.2.1 255.255.255.0
#
interface GigabitEthernet2/0/0
 pppoe-server bind Virtual-Template 1
#
l2tp-group 1  //创建L2TP组，配置L2TP连接参数
 tunnel password cipher %^%#/-#)Lg[S4F:#2~ZNvqa$]\DL%^%#
 start l2tp ip 1.1.1.1 fullusername l2tp1@huawei.com
#
ip route-static 1.1.1.1 255.255.255.255 1.1.2.2
#
return
```

步骤2 配置LNS

```
#
 sysname LNS
#
 l2tp enable  //启用L2TP功能
#
ip pool 1  //创建全局IP地址池
 gateway-list 10.1.1.1
 network 10.1.1.0 mask 255.255.255.0
#
radius-server template l2tp  //创建RADIUS服务器模板
 radius-server shared-key cipher %^%#}'|y>s-'m)@%$\X7QgS"Bc5M$iWmV:4aXREv:/~P%^%#
 radius-server authentication 10.2.1.2 1645 weight 80
#
aaa    //配置AAA采用RADIUS认证
 authentication-scheme l2tp
  authentication-mode radius
 domain huawei.com
  authentication-scheme l2tp
```


版权所有 © 华为技术有限公司

```
 radius-server l2tp
#
interface Virtual-Template1   //创建VT虚拟接口模板，配置拨号参数
 ppp authentication-mode chap domain huawei.com
 remote address pool 1
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/0
 ip address 1.1.1.1 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 10.1.2.1 255.255.255.0
#
l2tp-group 1   //创建L2TP组，配置L2TP连接参数
 allow l2tp virtual-template 1
 tunnel password cipher %^%#EB~j7Je>;@>uNr''D=J<]\WL%^%#
#
ip route-static 1.1.2.1 255.255.255.255 1.1.1.2
#
return
```

步骤3 验证配置结果

在LAC或者LNS上执行命令**display l2tp tunnel**可看到L2TP隧道及**Sessions**参数为**1**会话已建立。

企业分支与总部可以相互Ping通。

----结束

配置注意事项

- L2TP组缺省使能隧道认证，隧道两端密码相同。
- 配置LAC静态路由时，去往总部网段的路由的出接口必须为Virtual-Template1接口。
- 请根据实际情况在LNS上配置到RADIUS服务器的静态路由，这里未配置。

6.1.11 配置 LAC 自拨号发起 L2TP 隧道连接来实现分支与总部互通的示例

规格

适用于所有版本、所有形态的AR路由器。

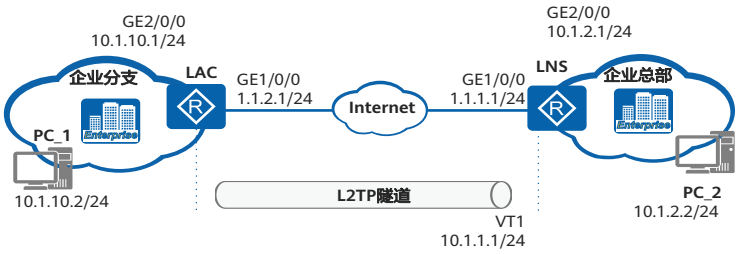
组网需求

如图6-16，企业总部在其他城市设有分支机构，分支机构内部使用以太网络。

总部为分支用户提供VPDN接入服务，允许分支内的任意用户接入，则LNS只需对LAC进行身份认证，此时可以通过在LAC配置自拨号的方式，在LAC和LNS之间建立L2TP连接。

 版权所有 © 华为技术有限公司

图 6-16 配置 LAC 自拨号发起 L2TP 隧道连接来实现分支与总部互通组网图



操作步骤

步骤1 配置LAC

```
#
 sysname LAC
#
 l2tp enable  //启用L2TP功能
#
interface Virtual-Template1  //创建VT虚拟接口模板，配置拨号参数
 ppp chap user huawei
 ppp chap password cipher %^%#U>upTZ}mQM:rhRL:4;s$,(xf%^%#
 ip address ppp-negotiate
 l2tp-auto-client enable
#
interface GigabitEthernet1/0/0
 ip address 1.1.2.1 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 10.1.10.1 255.255.255.0
#
l2tp-group 1  //创建L2TP组，配置L2TP连接参数
 tunnel password cipher %^%#/-#)Lg[S4F:#2~ZNvqa$]\DL%^%#
 tunnel name lac
 start l2tp ip 1.1.1.1 fullusername huawei
#
ip route-static 1.1.1.1 255.255.255.255 1.1.2.2
ip route-static 10.1.2.0 255.255.255.0 Virtual-Template1
#
return
```

步骤2 配置LNS

```
#
 sysname LNS
#
 l2tp enable  //启用L2TP功能
#
ip pool 1  //创建IP地址池，为接入用户分配IP地址
 gateway-list 10.1.1.1
 network 10.1.1.0 mask 255.255.255.0
#
aaa
 local-user huawei password cipher %^%#_<`.CO&(:LeS/$#F\H0Qv8B]KAZja3}3q'RNx;VI%^%#
 local-user huawei privilege level 15
 local-user huawei service-type ppp
#
interface Virtual-Template1  //创建VT虚拟接口模板，配置拨号参数
 ppp authentication-mode chap
 remote address pool 1
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/0
 ip address 1.1.1.1 255.255.255.0
```


版权所有 © 华为技术有限公司

```
#
interface GigabitEthernet2/0/0
 ip address 10.1.2.1 255.255.255.0
#
l2tp-group 1   //创建L2TP组，配置L2TP连接参数
 allow l2tp virtual-template 1 remote lac
 tunnel password cipher %^%#EB~j7Je>;@>uNr''D=J<]\WL%^%#
 tunnel name lns
#
ip route-static 1.1.2.1 255.255.255.255 1.1.1.2
ip route-static 10.1.10.0 255.255.255.0 Virtual-Template1
#
return
```

步骤3 验证配置结果

在LAC或者LNS上执行命令**display l2tp tunnel**可看到L2TP隧道及**Sessions**参数为**1**会话已建立。

企业分支与总部可以相互Ping通。

----结束

配置注意事项

- LAC和LNS配置的验证用户名和密码必须一致。
- 配置LAC静态路由时，去往总部网段的路由的出接口必须为Virtual-Template1接口。

6.1.12 配置 LAC 自拨号发起 L2TP 隧道连接来实现分支与总部互通的示例（RADIUS 服务器）

规格

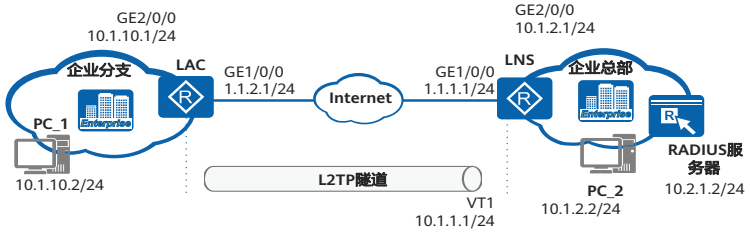
适用于所有版本、所有形态的AR路由器。

组网需求

如图6-17，企业总部在其他城市设有分支机构，分支机构内部使用以太网络。分支网关作为LAC和总部建立L2TP隧道。企业总部的网关部署为LNS，通过RADIUS务器对用户进行认证和分配指定的IP地址，实现分支用户和总部网关之间的L2TP连接。

总部为分支用户提供VPDN接入服务，允许分支内的任意用户接入，则LNS只需对LAC进行身份认证，此时可以通过在LAC配置自拨号的方式，在LAC和LNS之间建立L2TP连接。而且通过RADIUS服务器为用户进行认证和分配指定的IP地址。

图 6-17 配置 LAC 自拨号发起 L2TP 隧道连接来实现分支与总部互通组网图



版权所有 © 华为技术有限公司

操作步骤

步骤1 配置LAC

```
#
 sysname LAC
#
 l2tp enable  //启用L2TP功能
#
interface Virtual-Template1  //创建VT虚拟接口模板，配置拨号参数
 ppp chap user l2tp@huawei.com
 ppp chap password cipher %^%#U>upTZ}mQM:rhRL:4;s$,(xf%^%#
 ip address ppp-negotiate
 l2tp-auto-client enable
#
interface GigabitEthernet1/0/0
 ip address 1.1.2.1 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 10.1.10.1 255.255.255.0
#
l2tp-group 1  //创建L2TP组，配置L2TP连接参数
 tunnel password cipher %^%#/-#)Lg[S4F:#2~ZNvqa$]\DL%^%#
 start l2tp ip 1.1.1.1 fullusername l2tp@huawei.com
#
ip route-static 1.1.1.1 255.255.255.255 1.1.2.2
ip route-static 10.1.2.0 255.255.255.0 Virtual-Template1
#
return
```

步骤2 配置LNS

```
#
 sysname LNS
#
 l2tp enable  //启用L2TP功能
#
radius-server template l2tp  //创建RADIUS服务器模板
 radius-server shared-key cipher %^%#}'|y>s-'m)@%$\X7QgS''Bc5M$iWmV:4aXREv:/~P%^%#
 radius-server authentication 10.2.1.2 1645 weight 80
#
ip pool 1  //创建IP地址池，为接入用户分配IP地址
 gateway-list 10.1.1.1
 network 10.1.1.0 mask 255.255.255.0
#
aaa     //配置AAA采用RADIUS认证
 authentication-scheme l2tp
  authentication-mode radius
 domain huawei.com
  authentication-scheme l2tp
  radius-server l2tp
#
interface Virtual-Template1  //创建VT虚拟接口模板，配置拨号参数
 ppp authentication-mode chap domain huawei.com
 remote address pool 1
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/0
 ip address 1.1.1.1 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 10.1.2.1 255.255.255.0
#
l2tp-group 1  //创建L2TP组，配置L2TP连接参数
 allow l2tp virtual-template 1
 tunnel password cipher %^%#EB~j7Je>;@>uNr''D=J<]\WL%^%#
#
ip route-static 1.1.2.1 255.255.255.255 1.1.1.2
ip route-static 10.1.10.0 255.255.255.0 Virtual-Template1
```

 版权所有 © 华为技术有限公司

```
#
return
```

步骤3 验证配置结果

在LAC或者LNS上执行命令**display l2tp tunnel**可看到L2TP隧道及**Sessions**参数为**1**会话已建立。

企业分支与总部可以相互Ping通。

----结束

配置注意事项

- L2TP组缺省使能隧道认证，隧道两端密码相同。
- 配置LAC静态路由时，去往总部网段的路由的出接口必须为Virtual-Template1接口。
- 请根据实际情况在LNS上配置到RADIUS服务器的静态路由，这里未配置。

6.1.13 配置 LNS 多实例实现分支与总部互通的示例

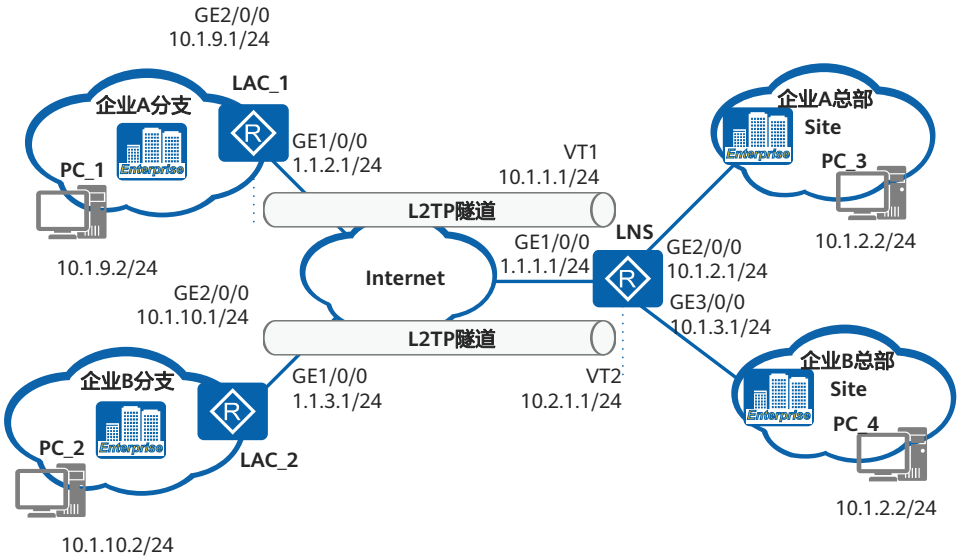
规格

适用于所有版本、所有形态的AR路由器。

组网需求

如图6-18，多个企业共用LNS，不同的企业用户分别连接LAC_1和LAC_2与各自的总部Site进行通讯。现要求：在LNS上配置L2TP多实例功能，使其能够为LAC_1和LAC_2同时提供L2TP接入服务，实现不同企业的用户能够远程访问企业内部网络。

图 6-18 配置 LNS 多实例实现分支与总部互通组网图



版权所有 © 华为技术有限公司

操作步骤

步骤1 配置LAC_1

```
#
 sysname LAC_1
#
 l2tp enable  //启用L2TP功能
#
interface Virtual-Template1  //创建VT虚拟接口模板，配置拨号参数
 ppp chap user l2tp1
 ppp chap password cipher %@%@U>upTZ}mQM:rhRL:4;s$,(xf%@%@
 ip address ppp-negotiate
 l2tp-auto-client enable
#
interface GigabitEthernet1/0/0
 ip address 1.1.2.1 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 10.1.9.1 255.255.255.0
#
l2tp-group 1  //创建L2TP组，配置L2TP连接参数
 tunnel password cipher %@%@/-#)Lg[S4F:#2~ZNvqa$]\DL%@%@
 tunnel name lac_1
 start l2tp ip 1.1.1.1 fullusername l2tp1
#
ip route-static 1.1.1.1 255.255.255.255 1.1.2.2  //配置静态路由
ip route-static 10.1.2.0 255.255.255.0 Virtual-Template1
#
return
```

步骤2 配置LAC_2

```
#
 sysname LAC_2
#
 l2tp enable  //启用L2TP功能
#
interface Virtual-Template1  //创建VT虚拟接口模板，配置拨号参数
 ppp chap user l2tp2
 ppp chap password cipher %@%@U>upTZ}mQM:rhRL:4;s$,(xf%@%@
 ip address ppp-negotiate
 l2tp-auto-client enable
#
interface GigabitEthernet1/0/0
 ip address 1.1.3.1 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 10.1.10.1 255.255.255.0
#
l2tp-group 1  //创建L2TP组，配置L2TP连接参数
 tunnel password cipher %@%@/-#)Lg[S4F:#2~ZNvqa$]\DL%@%@
 tunnel name lac_2
 start l2tp ip 1.1.1.1 fullusername l2tp2
#
ip route-static 1.1.1.1 255.255.255.255 1.1.3.2  //配置静态路由
ip route-static 10.1.3.0 255.255.255.0 Virtual-Template1
#
return
```

步骤3 配置LNS

```
#
 sysname LNS
#
 l2tp enable  //启用L2TP功能
#
ip vpn-instance vpn1  // 配置VPN实例VPN1
 ipv4-family
  route-distinguisher 100:1
  vpn-target 111:1 export-extcommunity
```

 版权所有 © 华为技术有限公司

```
 vpn-target 111:1 import-extcommunity
#
ip vpn-instance vpn2   // 配置VPN实例VPN2
 ipv4-family
  route-distinguisher 200:1
  vpn-target 222:1 export-extcommunity
  vpn-target 222:1 import-extcommunity
#
ip pool 1   //创建IP地址池，为接入用户分配IP地址
 vpn-instance vpn1
 gateway-list 10.1.1.1
 network 10.1.1.0 mask 255.255.255.0
#
ip pool 2
 vpn-instance vpn2
 gateway-list 10.2.1.1
 network 10.2.1.0 mask 255.255.255.0
#
aaa   //AAA视图下配置本地用户
 local-user l2tp1 password cipher %^%#_<`.CO&(:LeS/$#F\H0Qv8B]KAZja3}3q'RNx;VI%^%#
 local-user l2tp1 privilege level 15
 local-user l2tp1 service-type ppp
 local-user l2tp2 password cipher %^%#_<`.CO&(:LeS/$#F\H0Qv8B]KAZja3}3q'RNx;VI%^%#
 local-user l2tp2 privilege level 15
 local-user l2tp2 service-type ppp
#
interface Virtual-Template1   //创建VT1虚拟接口模板，配置拨号参数
 ppp authentication-mode chap
 remote address pool 1
 ip binding vpn-instance vpn1
 ip address 10.1.1.1 255.255.255.0
#
interface Virtual-Template2   //创建VT2虚拟接口模板，配置拨号参数
 ppp authentication-mode chap
 remote address pool 2
 ip binding vpn-instance vpn2
 ip address 10.2.1.1 255.255.255.0
#
interface GigabitEthernet1/0/0
 ip address 1.1.1.1 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip binding vpn-instance vpn1
 ip address 10.1.2.1 255.255.255.0
#
interface GigabitEthernet3/0/0
 ip binding vpn-instance vpn2
 ip address 10.1.3.1 255.255.255.0
#
l2tp-group 1   //创建L2TP组，配置L2TP连接参数
 allow l2tp virtual-template 1 remote lac_1 vpn-instance vpn1
 tunnel password cipher %@%@EB~j7Je>;@>uNr''D=J<]\WL%@%@
 tunnel name lns
#
l2tp-group 2   //创建L2TP组，配置L2TP连接参数
 allow l2tp virtual-template 2 remote lac_2 vpn-instance vpn2
 tunnel password cipher %@%@EB~j7Je>;@>uNr''D=J<]\WL%@%@
 tunnel name lns
#
ip route-static 1.1.2.1 255.255.255.255 1.1.1.2   //配置静态路由
ip route-static 1.1.3.1 255.255.255.255 1.1.1.2
ip route-static vpn-instance vpn1 10.1.9.0 255.255.255.0 Virtual-Template1
ip route-static vpn-instance vpn2 10.1.10.0 255.255.255.0 Virtual-Template2
#
return
```

步骤4 验证配置结果

 版权所有 © 华为技术有限公司

在LAC或者LNS上执行命令**display l2tp tunnel**可看到L2TP隧道及**Sessions**参数为**1**会话已建立。

企业分支与总部可以相互Ping通。

----结束

配置注意事项

- LAC和LNS配置的验证用户名和密码必须一致。
- 如果L2TP组编号为1，则可以不指定远端的隧道名称，表示允许接入任意LAC发起的L2TP连接请求；如果L2TP组编号不为1，则需要指定对端LAC的隧道名称。
- 配置LAC静态路由时，去往总部网段的路由的出接口必须为Virtual-Template接口。

6.1.14 配置 LNS 多实例实现分支与总部互通的示例（RADIUS 服务器）

规格

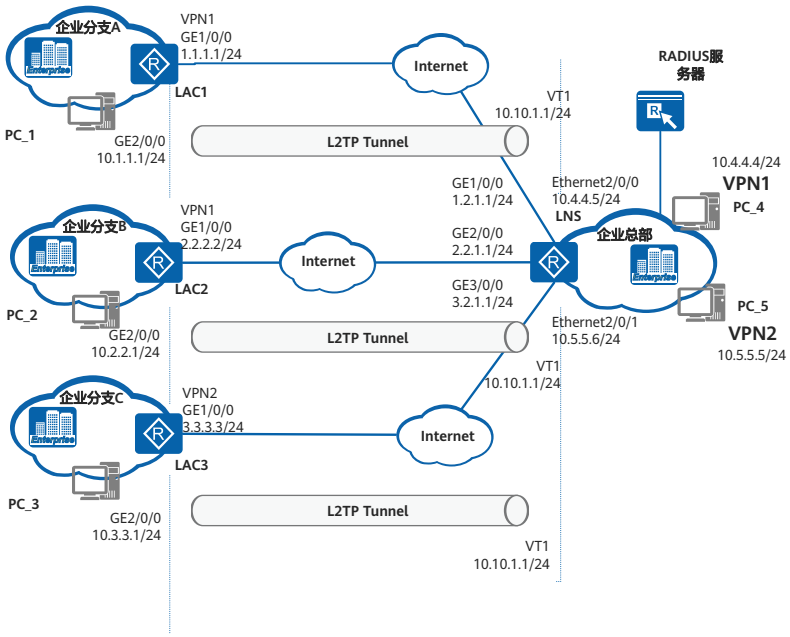
适用于V200R007C00、V200R008C50及更高版本、所有形态的AR路由器。

组网需求

如图6-19，企业总部在其他城市设有分支机构，多个分支共用LNS。企业分支A、企业分支B和企业分支C分别连接LAC1、LAC2和LAC3且与总部进行通讯。

具体需求如下：在LNS上配置L2TP多实例功能，使其能够为LAC1、LAC2和LAC3同时提供L2TP接入服务，实现不同企业分支的用户能够远程访问企业总部网络。由于限定了通讯范围，所属同一VPN实例的用户可相互通信。通过RADIUS服务器为用户进行认证，并通过VPN实例和下发IP地址等属性给用户分配地址。

图 6-19 配置 LNS 多实例实现分支与总部互通组网图



版权所有 © 华为技术有限公司

操作步骤

步骤1 配置LAC1

```
#
 sysname LAC1
#
 l2tp enable  //启用L2TP功能
#
interface Virtual-Template1  //创建VT虚拟接口模板，配置拨号参数
 ppp chap user lac1@huawei.com
 ppp chap password cipher %^%#U>upTZ}mQM:rhRL:4;s$,(xf%^%#
 ip address ppp-negotiate
 l2tp-auto-client enable
#
interface GigabitEthernet1/0/0
 ip address 1.1.1.1 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 10.1.1.1 255.255.255.0
#
l2tp-group 1  //创建L2TP组，配置L2TP连接参数
 tunnel password cipher %^%#/-#)Lg[S4F:#2~ZNvqa$]\DL%^%#
 tunnel name lac1
 start l2tp ip 1.2.1.1 fullusername lac1@huawei.com
#
ip route-static 1.2.1.0 255.255.255.0 1.1.1.2
ip route-static 10.4.4.0 255.255.255.0 Virtual-Template1
#
return
```

步骤2 配置LAC2

```
#
 sysname LAC2
#
 l2tp enable  //启用L2TP功能
#
interface Virtual-Template1  //创建VT虚拟接口模板，配置拨号参数
 ppp chap user lac2@huawei.com
 ppp chap password cipher %^%#/|S75*sxcH2@FQL=wn#2@I`a%^%#
 ip address ppp-negotiate
 l2tp-auto-client enable
#
interface GigabitEthernet1/0/0
 ip address 2.2.2.2 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 10.2.2.1 255.255.255.0
#
l2tp-group 1  //创建L2TP组，配置L2TP连接参数
 tunnel password cipher %^%#d'o6Xpp(i/i:WRC)`'0#3nJ*%^%#
 tunnel name lac2
 start l2tp ip 2.2.1.1 fullusername lac2@huawei.com
#
ip route-static 2.2.1.0 255.255.255.0 2.2.2.3
ip route-static 10.4.4.0 255.255.255.0 Virtual-Template1
#
return
```

步骤3 配置LAC3

```
#
 sysname LAC3
#
 l2tp enable  //启用L2TP功能
#
interface Virtual-Template1  //创建VT虚拟接口模板，配置拨号参数
 ppp chap user lac3@huawei.com
 ppp chap password cipher %^%#/|S75*sxcH2@FQL=wn#2@I`a%%^%#
 ip address ppp-negotiate
```

 版权所有 © 华为技术有限公司

```
 l2tp-auto-client enable
#
interface GigabitEthernet1/0/0
 ip address 3.3.3.3 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 10.3.3.1 255.255.255.0
#
l2tp-group 1   //创建L2TP组，配置L2TP连接参数
 tunnel password cipher %^%#d'o6Xpp(i/i:WRC)`'0#3nJ*%^%#
 tunnel name lac3
 start l2tp ip 3.2.1.1 fullusername lac3@huawei.com
#
ip route-static 3.2.1.0 255.255.255.0 3.3.3.4
ip route-static 10.5.5.0 255.255.255.0 Virtual-Template1
#
return
```

步骤4 配置LNS

```
#
 sysname LNS
#
 l2tp enable   //启用L2TP功能
#
ip vpn-instance vpn1   //配置VPN实例VPN1
ipv4-family
  route-distinguisher 200:1
  vpn-target 111:1 export-extcommunity
  vpn-target 111:1 import-extcommunity
#
ip vpn-instance vpn2   //配置VPN实例VPN2
 ipv4-family
  route-distinguisher 300:1
  vpn-target 222:1 export-extcommunity
  vpn-target 222:1 import-extcommunity
#
interface Ethernet2/0/0   //在LAN侧接口上配置VPN实例，将相应的接口与VPN实例绑定。
 ip binding vpn-instance vpn1
 ip address 10.4.4.5 255.255.255.0
#
interface Ethernet2/0/1   //在LAN侧接口上配置VPN实例，将相应的接口与VPN实例绑定。
 ip binding vpn-instance vpn2
 ip address 10.5.5.6 255.255.255.0
#
radius-server template l2tp   //创建RADIUS服务器模板
 radius-server shared-key cipher %^%#}'|y>s-'m)@%$\X7QgS''Bc5M$iWmV:4aXREv:/~P%^%#
 radius-server authentication 10.10.10.1 1645 weight 80
#
ip pool 1   //创建IP地址池，为接入用户分配IP地址
 gateway-list 10.10.1.1
 network 10.10.1.0 mask 255.255.255.0
#
aaa      //配置AAA采用RADIUS认证
 authentication-scheme l2tp
  authentication-mode radius
 domain huawei.com
  authentication-scheme l2tp
  radius-server l2tp
#
interface Virtual-Template1   //创建VT虚拟接口模板，配置拨号参数
 ppp authentication-mode chap domain huawei.com
 remote address pool 1
 ip address 10.10.1.1 255.255.255.0
#
interface GigabitEthernet1/0/0
 ip address 1.2.1.1 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 2.2.1.1 255.255.255.0
```

 版权所有 © 华为技术有限公司

```
#
interface GigabitEthernet3/0/0
 ip address 3.2.1.1 255.255.255.0
#
l2tp-group 1   //创建L2TP组，配置L2TP连接参数
 allow l2tp virtual-template 1
 tunnel password cipher %^%#5j*=S&AGXK'J}kG])REK]_-o%^%#
 tunnel name lns
#
ip route-static 1.1.1.0 255.255.255.0 1.2.1.2
ip route-static 2.2.2.0 255.255.255.255 2.2.1.2
ip route-static 3.3.3.0 255.255.255.255 3.2.1.2
ip route-static vpn-instance vpn1 10.1.1.0 255.255.255.255 10.10.1.100 public   //假设RADIUS服务器给LAC1侧用户的IP地址是10.10.1.100
ip route-static vpn-instance vpn1 10.2.2.0 255.255.255.255 10.10.1.101 public   //假设RADIUS服务器给LAC2侧用户的IP地址是10.10.1.101
ip route-static vpn-instance vpn2 10.3.3.0 255.255.255.255 10.10.1.102 public   //假设RADIUS服务器给LAC3侧用户的IP地址是10.10.1.102
#
return
```

步骤5 验证配置结果

在LAC或者LNS上执行命令**display l2tp tunnel**可看到L2TP隧道及**Sessions**参数为**1**会话已建立。

PC_1、PC_2和PC_4可以相互Ping通；PC_3和PC_5可以相互Ping通。

----结束

配置注意事项

- L2TP组缺省使能隧道认证，隧道两端密码相同。
- 配置LAC静态路由时，去往总部网段的路由的出接口必须为Virtual-Template1接口。
- 请根据实际情况在LNS上配置到RADIUS服务器的静态路由，这里未配置。
- 需要用户在RADIUS服务器上配置分配给LAC侧VT接口的IP地址，这里未配置。

6.1.15 配置 LAC 自拨号发起 L2TP 隧道连接来实现分支与总部互通示例（使用 3G 接口）

规格

适用于所有版本、所有形态的AR路由器。

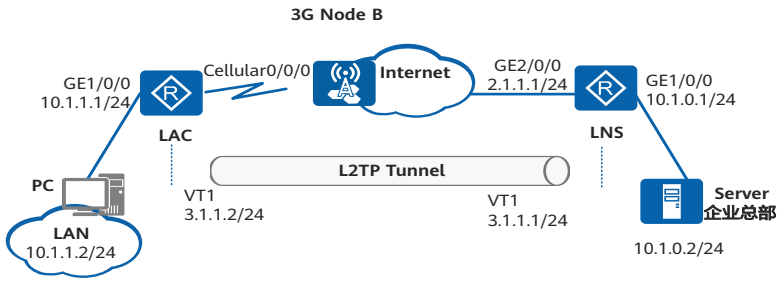
组网需求

如图6-20所示，企业总部在其他城市设有分支机构，分支机构部署为以太网络，并配备网关设备使用3G数据卡通过WCDMA网络接入Internet。

总部为分支用户提供VPDN接入服务，允许分支的任意用户接入，则LNS只对LAC进行身份认证，此时可以通过LAC自拨号的方式，在LAC和LNS之间建立L2TP连接。

 版权所有 © 华为技术有限公司

图 6-20 配置 LAC 自拨号发起 L2TP 隧道连接来实现分支与总部互通组网图（使用 3G 接口）



操作步骤

步骤1 配置LAC

```
#
 sysname LAC1
#
 l2tp enable  //启用L2TP功能
#
interface Virtual-Template1  //创建VT虚拟接口模板，配置拨号参数
 ppp chap user huawei
 ppp chap password cipher %^%#/|S75*sxcH2@FQL=wn#2@I`a%^%#
 ip address 3.1.1.2 255.255.255.0
 l2tp-auto-client enable
#
interface Cellular0/0/0  //配置3G接口
 link-protocol ppp
 ip address ppp-negotiate  //自动获取运营商分配的IP地址，接入公网
 dialer enable-circular  //使能DCC轮询功能
 dialer-group 1  //将此拨号口加入拨号控制列表，其编号和控制列表中的规则编号一致
 apn-profile 3GNET
 dialer timer autodial 60  //每隔60秒自动拨号
 dialer number *99# autodial  //按拨号串进行自动拨号
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.1 255.255.255.0
#
dialer-rule  //配置拨号控制列表
 dialer-rule 1 ip permit
#
apn profile 3GNET
 apn 3GNET
#
l2tp-group 1  //创建L2TP组，配置L2TP连接参数
 tunnel password cipher %^%#d'o6Xpp(i/i:WRC)`'0#3nJ*%^%#
 tunnel name LAC
 start l2tp ip 2.1.1.1 fullusername huawei
#
ip route-static 0.0.0.0 0.0.0.0 Cellular0/0/0  //配置静态路由
ip route-static 10.1.0.0 255.255.255.0 Virtual-Template1
#
return
```

步骤2 配置LNS

```
#
 sysname LNS1
#
 l2tp enable  //启用L2TP功能
#
ip pool 1  //创建IP地址池，为接入用户分配IP地址
 gateway-list 3.1.1.1
```


版权所有 © 华为技术有限公司

```
 network 3.1.1.0 mask 255.255.255.0
#
aaa   //配置L2TP的用户名和密码
 local-user huawei password cipher %^%#_<`.CO&(:LeS/$#F\H0Qv8B]KAZja3}3q'RNx;VI%^%#
 local-user huawei privilege level 15
 local-user huawei service-type ppp
#
interface Virtual-Template1   //创建VT虚拟接口模板，配置拨号参数
 ppp authentication-mode chap
 remote address pool 1
 ip address 3.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/0
 ip address 10.1.0.1 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 2.1.1.1 255.255.255.0
#
l2tp-group 1   //创建L2TP组，配置L2TP连接参数
 allow l2tp virtual-template 1 remote LAC
 tunnel password cipher %^%#5j*=S&AGXK'J}kG])REK]_-o%^%#
 tunnel name LNS
#
ip route-static 0.0.0.0 0.0.0.0 2.1.1.2   //配置静态路由
ip route-static 10.1.1.0 255.255.255.0 Virtual-Template1
#
return
```

步骤3 验证配置结果

在LAC或者LNS上执行命令**display l2tp tunnel**可看到L2TP隧道及**Sessions**参数为**1**会话已建立。

企业分支与总部可以相互Ping通。

----结束

配置注意事项

- LAC和LNS配置的验证用户名和密码必须统一。
- 配置LAC静态路由时，去往总部网段的路由的出接口必须为Virtual-Template1接口。

6.1.16 配置 LAC 自拨号发起 L2TP 隧道连接来实现分支与总部互通示例（使用 4G 接口）

规格

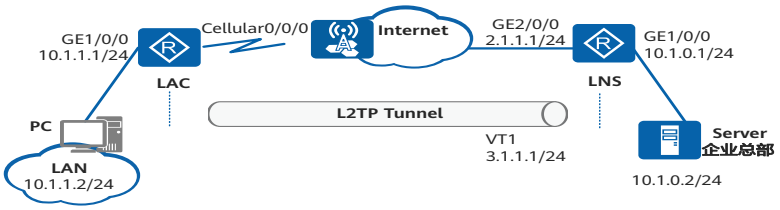
适用于所有版本、所有形态的AR路由器。

组网需求

如图6-21所示，企业总部在其他城市设有分支机构，分支机构部署为以太网络，并配备网关设备使用LTE数据卡通过LTE网络接入Internet。

总部为分支用户提供VPDN接入服务，允许分支的任意用户接入，则LNS只对LAC进行身份认证，此时可以通过LAC自拨号的方式，在LAC和LNS之间建立L2TP连接。

图 6-21 配置 LAC 自拨号发起 L2TP 隧道连接来实现分支与总部互通组网图（使用 4G 接口）



操作步骤

步骤1 配置LAC

```
#
 sysname LAC1
#
 l2tp enable  //启用L2TP功能
#
interface Virtual-Template1  //创建VT虚拟接口模板，配置拨号参数
 ppp chap user huawei
 ppp chap password cipher %^%#/|S75*sxcH2@FQL=wn#2@I`a%%^%#
 ip address ppp-negotiate
 l2tp-auto-client enable
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.1 255.255.255.0
#
interface Cellular0/0/0  //配置4G接口
 dialer enable-circular  //使能DCC轮询功能
 dialer-group 1  //将此拨号口加入拨号控制列表，其编号和控制列表中的规则编号一致
 apn-profile lteprofile
 dialer number *99# autodial  //按拨号串进行自动拨号
 ip address negotiate  //自动获取运营商分配的IP地址，接入公网
#
dialer-rule  //配置拨号控制列表
 dialer-rule 1 ip permit
#
apn profile lteprofile
apn ltenet
#
l2tp-group 1  //创建L2TP组，配置L2TP连接参数
 tunnel password cipher %^%#d'o6Xpp(i/i:WRC)`'0#3nJ*%^%#
 tunnel name LAC
 start l2tp ip 2.1.1.1 fullusername huawei
#
ip route-static 0.0.0.0 0.0.0.0 Cellular0/0/0  //配置静态路由
ip route-static 10.1.0.0 255.255.255.0 Virtual-Template1
#
return
```

步骤2 配置LNS

```
#
 sysname LNS1
#
 l2tp enable  //启用L2TP功能
#
ip pool 1  //创建IP地址池，为接入用户分配IP地址
 gateway-list 3.1.1.1
 network 3.1.1.0 mask 255.255.255.0
#
aaa  //配置L2TP的用户名和密码
 local-user huawei password cipher %^%#_<`.CO&(:LeS/$#F\H0Qv8B]KAZja3}3q'RNx;VI%^%#
```


版权所有 © 华为技术有限公司

```
 local-user huawei privilege level 15
 local-user huawei service-type ppp
#
interface Virtual-Template1   //创建VT虚拟接口模板，配置拨号参数
 ppp authentication-mode chap
 remote address pool 1
 ip address 3.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/0
 ip address 10.1.0.1 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 2.1.1.1 255.255.255.0
#
l2tp-group 1   //创建L2TP组，配置L2TP连接参数
 allow l2tp virtual-template 1 remote LAC
 tunnel password cipher %^%#5j*=S&AGXK'J}kG])REK]_-o%^%#
 tunnel name LNS
#
ip route-static 0.0.0.0 0.0.0.0 2.1.1.2   //配置静态路由
ip route-static 10.1.1.0 255.255.255.0 Virtual-Template1
#
return
```

步骤3 验证配置结果

在LAC或者LNS上执行命令**display l2tp tunnel**可看到L2TP隧道及**Sessions**参数为**1**会话已建立。

企业分支与总部可以相互Ping通。

----结束

配置注意事项

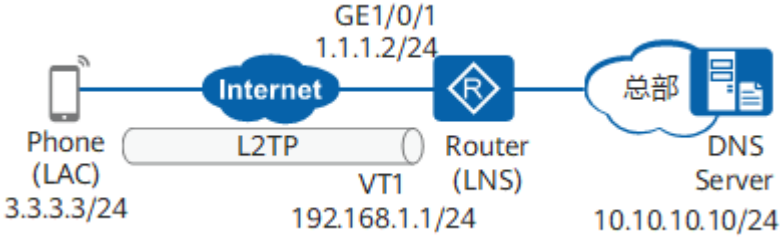
- LAC和LNS配置的验证用户名和密码必须一致。
- 配置LAC静态路由时，去往总部网段的路由的出接口必须为Virtual-Template1接口。

6.1.17 配置移动办公用户使用 Android 手机发起 L2TP 隧道连接示例

组网需求

如图6-22所示，企业出差员工的地理位置经常发生变动，并且随时需要和总部通信和访问总部内网资源，直接通过Internet网络虽然可以访问总部网关，但总部网关无法对接入的用户进行辨别和管理，这时将总部网关部署为LNS，出差员工通过Phone发起L2TP隧道连接，则可以在出差员工和总部网关之间建立虚拟的点到点连接。

图 6-22 配置移动办公用户使用 Phone 发起 L2TP 隧道连接组网图



版权所有 © 华为技术有限公司

说明

本举例使用8.0.0版本的Android手机系统。

Android手机发起L2TP隧道连接跟终端强相关，请确认手机是否支持。

配置思路

在Phone与总部上配置L2TP方式可以实现上述需求。可采用如下思路配置：

1. 在Router上配置接口的IP地址和到对端的静态路由，保证两端路由可达。
2. 在Router上配置L2TP，实现与Phone对接。
3. 在Phone上配置L2TP，实现与Router对接。Phone的配置参数需要与Router的参数对应。

操作步骤

步骤1 配置LNS

```
#
 sysname LNS
#
 l2tp enable                              //使能L2TP功能
#
acl number 2001                           //配置ACL，进行NAT转换使用，将L2TP分配的地址进行NAT转换
 rule 5 permit source 192.168.1.0 0.0.0.255
#
ip pool lns                               //创建IP地址池，名称为lns，为接入用户分配IP地址
 gateway-list 192.168.1.1
 network 192.168.1.0 mask 255.255.255.0
#
aaa                                       //配置L2TP拨入的用户名密码
 authentication-scheme lmt
 domain huawei.com
  authentication-scheme lmt
 local-user vpdnuser password cipher %^%#_<`.CO&(:LeS/$#F\H0Qv8B]KAZja3}3q'RNx;Vl%^%#
 local-user vpdnuser privilege level 15
 local-user vpdnuser service-type ppp
#
interface GigabitEthernet1/0/1
 ip address 1.1.1.2 255.255.255.0
 nat outbound 2001                        //配置NAT功能，实现公网访问功能
#
interface Virtual-Template1               //创建VT虚拟接口模板，配置拨号参数
 ppp authentication-mode chap domain huawei.com   //配置认证方式时必须携带域名
 remote address pool lns
 ppp ipcp dns 10.10.10.10                 //分配DNS网关，以便员工使用域名访问外网资源
 ip address 192.168.1.1 255.255.255.0
#
l2tp-group 1                              //创建L2TP组，配置L2TP连接参数
 undo tunnel authentication               //手机拨号拨入，使用不认证的方式
 allow l2tp virtual-template 1
#
ip route-static 0.0.0.0 0.0.0.0 1.1.1.3
#
return
```

步骤2 配置Phone

 版权所有 © 华为技术有限公司

说明

“L2TP密钥”填写Router上配置的密码YsHsjx_202206

----结束

结果验证

1. 在Phone上启用VPN连接，可以看到VPN连接成功。
2. 在Router上执行命令**display l2tp tunnel**，可以看到L2TP隧道建立成功。

```
[Router] display l2tp tunnel
 Total tunnel : 1
 LocalTID RemoteTID RemoteAddress    Port   Sessions RemoteName
 1        1         3.3.3.3          1701   1        -
```

6.1.18 配置分支机构与总部之间通过 L2TP over Bridge 方式建立二层网络互通的示例

规格

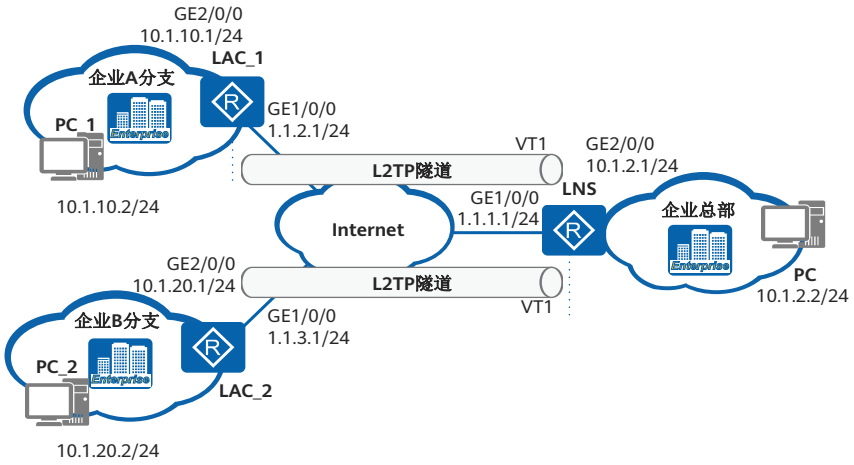
适用于所有版本、所有形态的AR路由器。

组网需求

如图6-23，企业总部LNS与企业用户LAC_1和LAC_2进行通讯，企业总部LNS为分支用户LAC_1和LAC_2提供VPDN接入服务，在LNS与LAC_1和LAC_2之间建立L2TP VPN隧道。企业可以通过配置L2TP over Bridge的方式建立总部与分支间的二层网络互通，实现LAC_1和LAC_2与LNS之间建立L2TP连接，分支内的任意用户接入和互相访问。L2TP隧道建立完成后，分支与总部之间的流量通过二层网络转发。

版权所有 © 华为技术有限公司

图 6-23 配置分支机构与总部之间通过 L2TP over Bridge 建立二层网络互通组网图



操作步骤

步骤1 配置LAC_1

```
#
 sysname LAC_1
#
 bridge 1
#
 l2tp enable  //使能L2TP功能
#
interface Virtual-Template1  //创建VT虚拟接口模板，配置拨号参数
 bridge 1  //创建网桥组1并将VT虚拟接口加入网桥组1
 bridge vlan-transmit enable  //使能网桥组接口透明传输VLAN ID功能
 ppp chap user huawei
 ppp chap password cipher %@%@U>upTZ}mQM:rhRL:4;s$,(xf%@%@
 l2tp-auto-client enable
#
interface GigabitEthernet1/0/0
 ip address 1.1.2.1 255.255.255.0
#
interface GigabitEthernet2/0/0
 bridge 1
 bridge vlan-transmit enable
#
l2tp-group 1  //创建L2TP组，配置L2TP连接参数
 tunnel password cipher %@%@/-#)Lg[S4F:#2~ZNvqa$]\DL%@%@
 tunnel name lac_1
 start l2tp ip 1.1.1.1 fullusername huawei
#
ip route-static 1.1.1.1 255.255.255.255 1.1.2.2  //配置静态路由
#
return
```

步骤2 配置LAC_2

```
#
 sysname LAC_2
#
 bridge 1
#
 l2tp enable  //使能L2TP功能
#
interface Virtual-Template1  //创建VT虚拟接口模板，配置拨号参数
 bridge 1  //创建网桥组1并将VT虚拟接口加入网桥组1
 bridge vlan-transmit enable  //使能网桥组接口透明传输VLAN ID功能
```


版权所有 © 华为技术有限公司

```
 ppp chap user huawei
 ppp chap password cipher %@%@U>upTZ}mQM:rhRL:4;s$,(xf%@%@
 ip address ppp-negotiate
 l2tp-auto-client enable
#
interface GigabitEthernet1/0/0
 ip address 1.1.3.1 255.255.255.0
#
interface GigabitEthernet2/0/0
 bridge 1
 bridge vlan-transmit enable
#
l2tp-group 1   //创建L2TP组，配置L2TP连接参数
 tunnel password cipher %@%@/-#)Lg[S4F:#2~ZNvqa$]\DL%@%@
 tunnel name lac_2
 start l2tp ip 1.1.1.1 fullusername huawei
#
ip route-static 1.1.1.1 255.255.255.255 1.1.3.2   //配置静态路由
#
return
```

步骤3 配置LNS

```
#
 sysname LNS
#
 l2tp enable   //使能L2TP功能
#
 bridge 1
#
aaa
 local-user huawei password cipher %^%#_<`.CO&(:LeS/$#F\H0Qv8B]KAZja3}3q'RNx;VI%^%#
 local-user huawei privilege level 15
 local-user huawei service-type ppp
#
interface Virtual-Template1
 bridge 1     //创建网桥组1并将VT虚拟接口加入网桥组1
 bridge vlan-transmit enable     //使能网桥组接口透明传输VLAN ID功能
 ppp authentication-mode chap
#
interface GigabitEthernet1/0/0
 ip address 1.1.1.1 255.255.255.0
#
interface GigabitEthernet2/0/0
 bridge 1
 bridge vlan-transmit enable
#
l2tp-group 1
 allow l2tp virtual-template 1
 tunnel password cipher %^%#_<`.CO&(:LeS/$#F\H0Qv8B]KAZja3}3q'RNx;VI%^%#
 tunnel name lns
#
ip route-static 1.1.2.1 255.255.255.255 1.1.1.2   //配置静态路由
ip route-static 1.1.3.1 255.255.255.255 1.1.1.2
#
return
```

步骤4 验证配置结果

企业分支与总部可以相互**Ping**通。

分别在LNS、LAC_1和LAC_2上查看L2TP隧道的建立情况，此处以LAC_1为例。

- 执行**display l2tp tunnel**命令，查看到有L2TP隧道信息，说明L2TP隧道建立成功。

```
[LAC_1] display l2tp tunnel

Total tunnel : 1
LocalTID RemoteTID RemoteAddress    Port   Sessions RemoteName
1        1         1.1.1.1          1701   1        LNS
```

 版权所有 © 华为技术有限公司

- 执行**display l2tp session**命令，查看到有L2TP会话信息，说明L2TP会话建立成功。

```
[LAC_1] display l2tp session

Total session : 1
LocalSID  RemoteSID  LocalTID
1         1          1
```

----结束

配置注意事项

- LAC和LNS配置的验证用户名和密码必须一致。
- 如果L2TP组编号为1，则可以不指定远端的隧道名称，表示允许接入任意LAC发起的L2TP连接请求；如果L2TP组编号不为1，则需要指定对端LAC的隧道名称。

6.2 GRE

6.2.1 配置 GRE 隧道，并在隧道上运行静态路由实现互通的示例

规格

适用于所有版本、所有形态的路由器。

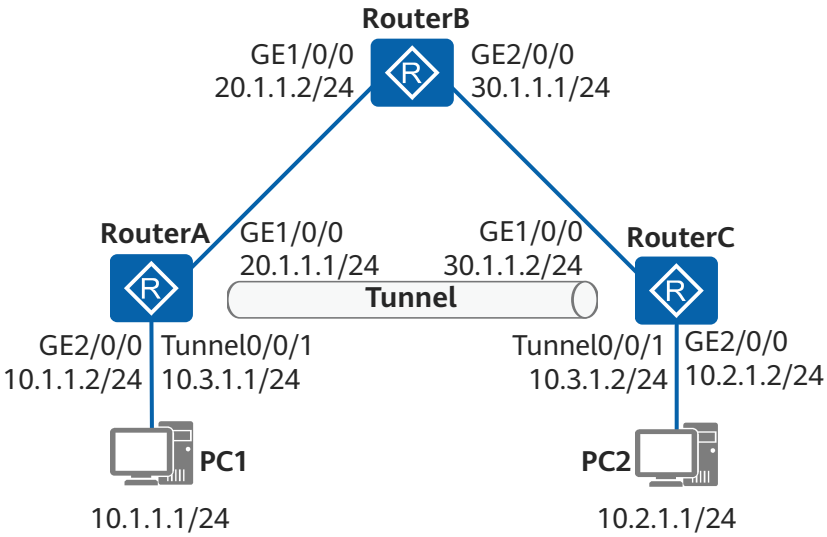
组网需求

如图6-24，RouterA、RouterB、RouterC属于VPN骨干网，它们之间运行OSPF。

RouterA和RouterC之间使用三层隧道协议GRE，实现PC1和PC2互联。

PC1和PC2上分别指定RouterA、RouterC为自己的缺省网关。

图 6-24 配置 GRE 使用静态路由组网图



版权所有 © 华为技术有限公司

操作步骤

步骤1 配置RouterA

```
#
 sysname RouterA
#
interface GigabitEthernet1/0/0  //配置公网出接口
 ip address 20.1.1.1 255.255.255.0
#
interface GigabitEthernet2/0/0  //配置私网出接口
 ip address 10.1.1.2 255.255.255.0
#
interface Tunnel0/0/1  //配置Tunnel接口，Tunnel的源地址是发出报文的实际接口IP地址，目的地址是接收报文的实际接口IP地址
 ip address 10.3.1.1 255.255.255.0
 tunnel-protocol gre
 source 20.1.1.1
 destination 30.1.1.2
#
ospf 1  //配置公网路由
 area 0.0.0.0
  network 20.1.1.0 0.0.0.255
#
ip route-static 10.2.1.0 255.255.255.0 Tunnel0/0/1  //配置私网静态路由，下一条接口为Tunnel接口
#
return
```

步骤2 配置RouterB

```
#
 sysname RouterB
#
interface GigabitEthernet1/0/0
ip address 20.1.1.2 255.255.255.0
#
interface GigabitEthernet2/0/0
ip address 30.1.1.1 255.255.255.0
#
ospf 1  //配置公网路由
 area 0.0.0.0
  network 20.1.1.0 0.0.0.255
  network 30.1.1.0 0.0.0.255
#
return
```

步骤3 配置RouterC

```
#
 sysname RouterC
#
interface GigabitEthernet1/0/0  //配置公网出接口
ip address 30.1.1.2 255.255.255.0
#
interface GigabitEthernet2/0/0  //配置私网出接口
 ip address 10.2.1.2 255.255.255.0
#
interface Tunnel0/0/1  //配置Tunnel接口，Tunnel的源地址是发出报文的实际接口IP地址，目的地址是接收报文的实际接口IP地址
 ip address 10.3.1.2 255.255.255.0
 tunnel-protocol gre
 source 30.1.1.2
 destination 20.1.1.1
#
ospf 1  //配置公网路由
 area 0.0.0.0
  network 30.1.1.0 0.0.0.255
#
ip route-static 10.1.1.0 255.255.255.0 Tunnel0/0/1  //配置私网静态路由，下一条接口为Tunnel接口
#
return
```

 版权所有 © 华为技术有限公司

步骤4 验证配置结果

在RouterA和RouterC上执行**display ip routing-table**命令，可以看到去往对端目的地址的出接口为Tunnel接口。

PC1和PC2能互相Ping通。

----结束

配置注意事项

- 两段需要配置到私网的路由，出接口为Tunnel接口。
- Tunnel源地址是发出报文的实际接口IP地址，目的地址是接收报文的实际接口IP地址。
- Tunnel接口的源IP和目的IP要和对端对应。

6.2.2 配置 GRE 隧道，并在隧道上运行 OSPF 实现互通的示例

规格

适用于所有版本、所有形态的路由器。

组网需求

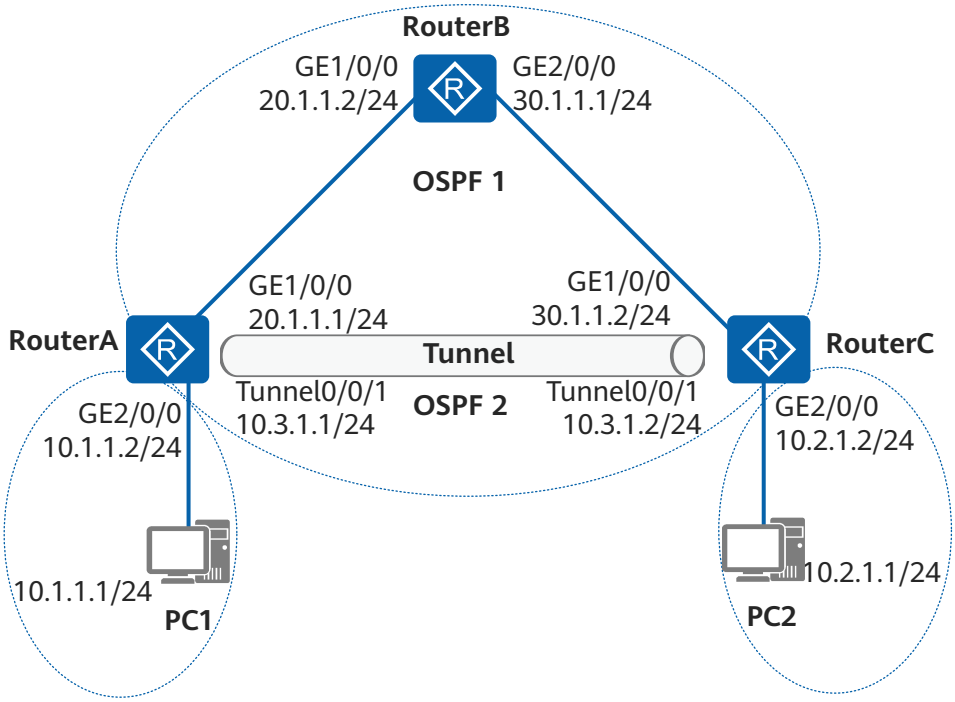
如图6-25，RouterA、RouterB、RouterC属于VPN骨干网，它们之间运行OSPF。

RouterA和RouterC之间使用三层隧道协议GRE，实现PC1和PC2互联。

PC1和PC2上分别指定RouterA、RouterC为自己的缺省网关。

Tunnel接口启用动态路由协议OSPF。VPN骨干网上使用OSPF进程1，用户接入部分使用OSPF进程2。

图 6-25 配置 GRE 使用动态路由协议组网图



版权所有 © 华为技术有限公司

操作步骤

步骤1 配置RouterA

```
#
 sysname RouterA
#
interface GigabitEthernet1/0/0  //配置公网出接口
ip address 20.1.1.1 255.255.255.0
#
interface GigabitEthernet2/0/0  //配置私网出接口
 ip address 10.1.1.2 255.255.255.0
#
interface Tunnel0/0/1  //配置Tunnel接口，源地址是发出报文的实际接口IP地址，目的地址是接收报文的实际接口IP地址
 ip address 10.3.1.1 255.255.255.0
 tunnel-protocol gre
 source 20.1.1.1
 destination 30.1.1.2
#
ospf 1  //配置公网路由
 area 0.0.0.0
  network 20.1.1.0 0.0.0.255
#
ospf 2
 area 0.0.0.0  //配置私网路由
  network 10.3.1.0 0.0.0.255
  network 10.1.1.0 0.0.0.255
#
return
```

步骤2 配置RouterB

```
#
 sysname RouterB
#
interface GigabitEthernet1/0/0
ip address 20.1.1.2 255.255.255.0
#
interface GigabitEthernet2/0/0
ip address 30.1.1.1 255.255.255.0
#
ospf 1  //配置公网路由
 area 0.0.0.0
  network 20.1.1.0 0.0.0.255
  network 30.1.1.0 0.0.0.255
#
return
```

步骤3 配置RouterC

```
#
 sysname RouterC
#
interface GigabitEthernet1/0/0  //配置公网出接口
ip address 30.1.1.2 255.255.255.0
#
interface GigabitEthernet2/0/0  //配置私网出接口
 ip address 10.2.1.2 255.255.255.0
#
interface Tunnel0/0/1  //配置Tunnel接口，源地址是发出报文的实际接口IP地址，目的地址是接收报文的实际接口IP地址
 ip address 10.3.1.2 255.255.255.0
 tunnel-protocol gre
 source 30.1.1.2
 destination 20.1.1.1
#
ospf 1  //配置公网路由
```

 版权所有 © 华为技术有限公司

```
 area 0.0.0.0
  network 30.1.1.0 0.0.0.255
#
ospf 2  //配置私网路由
 area 0.0.0.0
  network 10.3.1.0 0.0.0.255
  network 10.2.1.0 0.0.0.255
#
return
```

步骤4 验证配置结果

在RouterA和RouterC上执行**display ip routing-table**命令，可以看到去往对端目的地址的出接口为Tunnel接口。

PC1和PC2能互相Ping通。

----结束

配置注意事项

- 两段需要配置到私网的路由。
- Tunnel接口的源IP和目的IP要和对端对应。

6.2.3 配置 GRE over GRE 实现数据加密示例

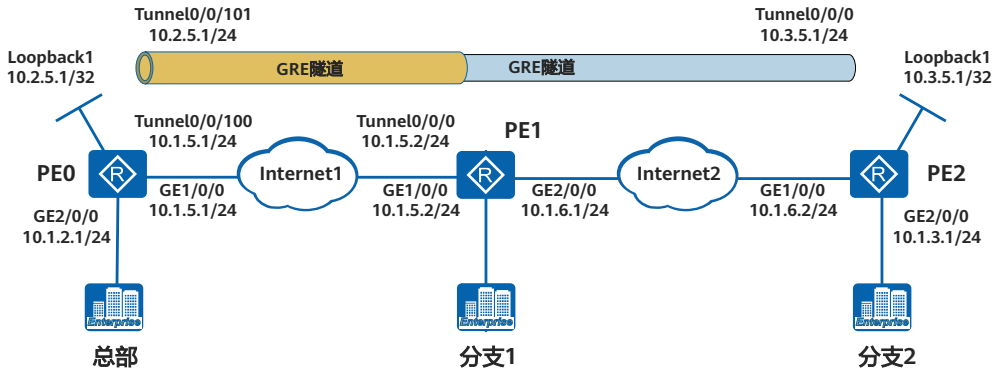
规格

适用于V200R006C10及更高版本、所有形态的路由器。

组网需求

如图6-26所示，PE0是银行总部网关，PE1和PE2是银行两分支网关。PE1通过运营商网络与PE0互通，PE2通过私有专用网络与PE1互通，但PE0与PE2不互通。现要求不仅在公网实现数据封装，在私网也实现数据封装，为实现PE0与PE1、PE2安全通信，可以在总部部署GRE over GRE。数据在PE0与PE1之间通过一层GRE隧道传输；数据在PE0与PE2之间传输时，经过PE0和PE1时通过两层GRE隧道传输。

图 6-26 通过 GRE over GRE 实现分支与总部互通的组网图



版权所有 © 华为技术有限公司

操作步骤

步骤1 配置PE0

```
#
 sysname PE0
#
interface GigabitEthernet1/0/0
 ip address 10.1.5.1 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 10.1.2.1 255.255.255.0
#
interface LoopBack1
 ip address 10.2.5.1 255.255.255.255
#
interface Tunnel0/0/100    //配置Tunnel接口
 ip address unnumbered interface GigabitEthernet1/0/0    //配置Tunnel0/0/100接口地址，借用GigabitEthernet1/0/0接口的IP地址
 tunnel-protocol gre    //配置Tunnel0/0/100接口的隧道模式为GRE
 source 10.1.5.1    //配置Tunnel源地址
 destination 10.1.5.2    //配置Tunnel目的地址
#
interface Tunnel0/0/101
 ip address unnumbered interface Loopback1    //配置Tunnel0/0/101接口地址，借用Loopback1接口的IP地址
 tunnel-protocol gre    //配置Tunnel0/0/101接口的隧道模式为GRE
 source 10.2.5.1    //配置Tunnel源地址
 destination 10.3.5.1    //配置Tunnel目的地址
#
ip route-static 10.3.5.1 255.255.255.255 Tunnel 0/0/100    //配置到PE2 Tunnel0/0/0目的地址的路由出接口为Tunnel0/0/100
ip route-static 10.1.3.0 255.255.255.0 Tunnel 0/0/101    //配置到PE2数据路由出接口为Tunnel0/0/101
#
return
```

步骤2 配置PE1

```
#
 sysname PE1
#
interface GigabitEthernet1/0/0
 ip address 10.1.5.2 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 10.1.6.1 255.255.255.0
#
interface Tunnel0/0/0    //配置Tunnel接口
 ip address unnumbered interface GigabitEthernet1/0/0    //配置Tunnel0/0/0接口地址，借用GigabitEthernet1/0/0接口的IP地址
 tunnel-protocol gre    //配置Tunnel0/0/100接口的隧道模式为GRE
 source 10.1.5.2    //配置Tunnel源地址
 destination 10.1.5.1    //配置Tunnel目的地址
#
ip route-static 10.2.5.1 255.255.255.255 Tunnel0/0/0    //配置到Tunnel0/0/101的源地址的路由出接口为Tunnel0/0/0
ip route-static 10.3.5.1 255.255.255.255 10.1.6.2    //配置到Tunnel0/0/101的目的地址的路由出接口IP地址是10.1.6.2
#
return
```

步骤3 配置PE2

```
#
 sysname PE2
#
interface GigabitEthernet1/0/0
 ip address 10.1.6.2 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 10.1.3.1 255.255.255.0
#
```

 版权所有 © 华为技术有限公司

```
interface Loopback1
 ip address 10.3.5.1 255.255.255.255
#
interface Tunnel0/0/0    //配置Tunnel接口
 ip address unnumbered interface Loopback1    //配置Tunnel0/0/0接口地址，借用Loopback1接口的IP地址
 tunnel-protocol gre    //配置Tunnel0/0/100接口的隧道模式为GRE
 source Loopback1    //配置Tunnel源地址
 destination 10.2.5.1    //配置Tunnel目的地址
#
ip route-static 10.2.5.1 255.255.255.255 10.1.6.1    //配置到Tunnel0/0/101的源地址的路由出接口IP地址是
10.1.6.1
ip route-static 10.1.2.0 255.255.255.0 Tunnel0/0/0    //配置到PE0的数据路由出接口为Tunnel0/0/0
#
return
```

步骤4 验证配置结果

总部分别和分支1、分支2能互相Ping通。

----结束

配置注意事项

1. Tunnel源地址是发出报文的实际接口IP地址，目的地址是接收报文的实际接口IP地址。
2. Tunnel两端的源IP地址和目的IP地址要对应。

6.2.4 配置分支机构与总部之间通过 IPSec Over GRE 方式实现安全互通的示例

规格

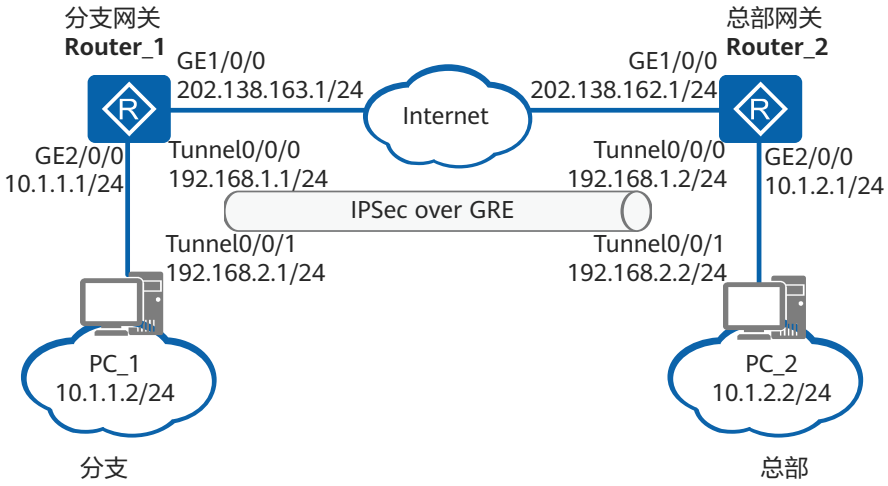
适用于V200R005C10及更高版本、所有形态的路由器。

组网需求

如图6-27所示，Router_1为公司分支网关，Router_2为公司总部网关，分支与总部通过公网建立通信。

原公司分支与总部通过GRE隧道实现私网互通，现要求对分支与总部之间相互访问的流量（不包括组播数据）进行安全保护。因此，可基于虚拟隧道接口方式建立IPSec over GRE，对分支和总部互通的流量进行保护。

图 6-27 IPSec Over GRE 组网



 版权所有 © 华为技术有限公司

操作步骤

步骤1 配置Router_1

```
#
 sysname Router_1
#
ipsec proposal tran1  //配置安全提议
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-128
#
ike proposal 5  //配置IKE提议
 encryption-algorithm aes-cbc-128
 authentication-algorithm sha2-256
#
ike peer spub v2  //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 pre-shared-key cipher %^%#JvZxR2g8c;a9~FPN~n'$7`DEV&=G(=Et02P/%\*!%^%#  //配置预共享密钥认证字为“huawei”，以密文显示，该命令在V2R3C00以前的版本中为“pre-shared-key huawei”，以明文显示
 ike-proposal 5
#
ipsec profile profile1  //配置安全框架
 ike-peer spub
 proposal tran1
#
interface Tunnel0/0/0  //配置GRE Tunnel接口
 ip address 192.168.1.1 255.255.255.0
 tunnel-protocol gre
 source 202.138.163.1
 destination 202.138.162.1
#
interface Tunnel0/0/1  //配置IPSec Tunnel接口
 ip address 192.168.2.1 255.255.255.0
 tunnel-protocol ipsec
 source Tunnel0/0/0  //指定Tunnel源接口为GRE Tunnel接口
 destination 192.168.1.2  //指定Tunnel的目的地址为GRE Tunnel地址
 ipsec profile profile1  //应用置安全框架
#
interface GigabitEthernet1/0/0
 ip address 202.138.163.1 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 10.1.1.1 255.255.255.0
#
ip route-static 10.1.2.0 255.255.255.0 tunnel0/0/1  //配置静态路由
ip route-static 202.138.162.0 255.255.255.0 202.138.163.2  //配置静态路由
#
return
```

步骤2 配置Router_2

```
#
 sysname Router_2
#
ipsec proposal tran1  //配置安全提议
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-128
#
ike proposal 5  //配置IKE提议
 encryption-algorithm aes-cbc-128  //V200R008及之后的版本，aes-cbc-128参数修改为aes-128
 authentication-algorithm sha2-256
#
ike peer spua v2  //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本
```

命令为**ike peer** *peer-name* [**v1** | **v2**]。V200R008及之后的版本命令为**ike peer** *peer-name*和**version** { **1** | **2** }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令**undo version 2**；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令**version 1**，再执行命令**undo version 2**。

```
 pre-shared-key cipher %^%#K{JG:rWVHPMnf;5\|,GW(Luq'qi8BT4nOj%5W5=)%^%#  //配置预共享密钥认证字为“huawei”，以密文显示，该命令在V2R3C00以前的版本中为“pre-shared-key huawei”，以明文显示
 ike-proposal 5
#
ipsec profile profile1  //配置安全框架
 ike-peer spua
 proposal tran1
#
interface Tunnel0/0/0  //配置GRE Tunnel接口
 ip address 192.168.1.2 255.255.255.0
 tunnel-protocol gre
 source 202.138.162.1
 destination 202.138.163.1
#
interface Tunnel0/0/1  //配置IPSec Tunnel接口
 ip address 192.168.2.2 255.255.255.0
 tunnel-protocol ipsec
 source Tunnel0/0/0  //指定Tunnel源接口为GRE Tunnel接口
 destination 192.168.1.1  //指定Tunnel的目的地址为GRE Tunnel地址
 ipsec profile profile1  //应用置安全框架
#
interface GigabitEthernet1/0/0
 ip address 202.138.162.1 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 10.1.2.1 255.255.255.0
#
ip route-static 10.1.1.0 255.255.255.0 tunnel0/0/1  //配置静态路由
ip route-static 202.138.163.0 255.255.255.0 202.138.162.2  //配置静态路由
#
return
```

步骤3 验证配置结果

在Router上执行命令**display ike sa**可以查看到安全联盟建立成功，其中**Flag(s)**字段为**RD**表示SA已建立成功；**Phase**字段可以看到**1**和**2**两个阶段。

PC_1和PC_2可以相互Ping通。

----结束

配置注意事项

配置IPSec Tunnel接口，将IPSec Tunnel的源接口配置为GRE Tunnel接口；且IPSec Tunnel的目的地址的路由必须从GRE Tunnel接口出去。

6.2.5 配置分支与总部通过 GRE 隧道实现互通的示例

规格

适用于所有版本、所有形态的路由器。

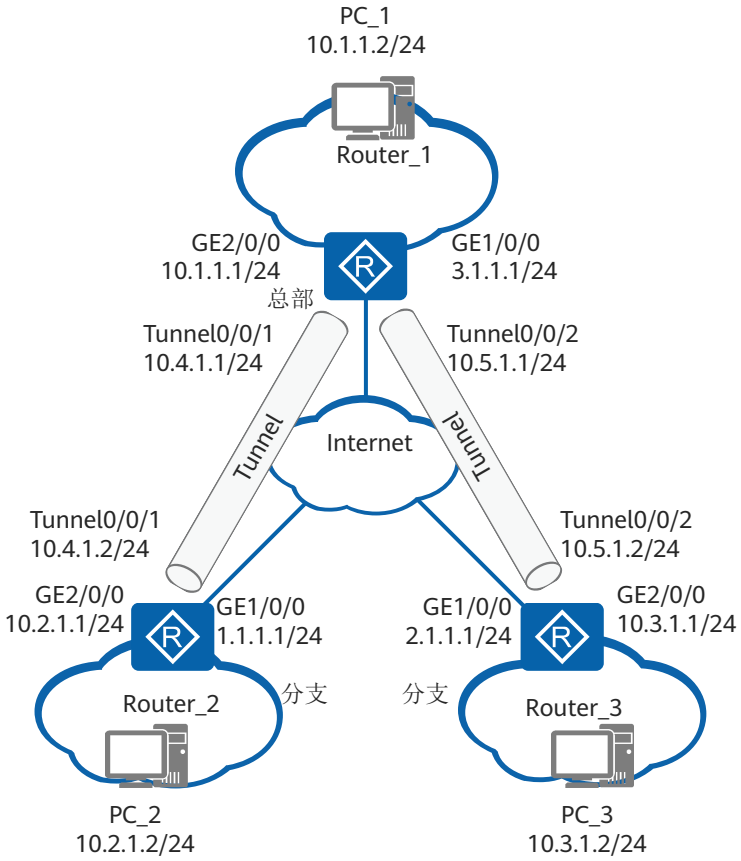
组网需求

如图6-28所示，Router_1为某企业总部网关，Router_2和Router_3为分支网关，服务提供商已经为各网关分配了公网IP地址，并保证网关之间可以通信，企业希望能实现企业总部和分支的私网互访，并且要求实现机制简单，成本低。

 版权所有 © 华为技术有限公司

此时，可以在总部和分支之间建立GRE隧道实现该需求。这里，配置OSPF协议使网关上存在通过Tunnel接口到达目的地址的路由表项。

图 6-28 配置分支与总部通过 GRE 隧道实现互通的组网图



操作步骤

步骤1 配置Router_1

```
#
 sysname Router_1
#
interface GigabitEthernet1/0/0   //配置公网出接口
 ip address 3.1.1.1 255.255.255.0
#
interface GigabitEthernet2/0/0   //配置私网出接口
 ip address 10.1.1.1 255.255.255.0
#
interface Tunnel0/0/1   //配置Tunnel接口，源地址是发出报文的实际接口IP地址，目的地址是接收报文的实际接口IP地址
 ip address 10.4.1.1 255.255.255.0
 tunnel-protocol gre
 source 3.1.1.1
 destination 1.1.1.1
#
interface Tunnel0/0/2
 ip address 10.5.1.1 255.255.255.0
 tunnel-protocol gre
 source 3.1.1.1
```


版权所有 © 华为技术有限公司

```
 destination 2.1.1.1
#
ospf 1   //配置公网路由
 area 0.0.0.0
  network 3.1.1.0 0.0.0.255
#
ospf 2
 area 0.0.0.0   //配置私网路由
  network 10.1.1.0 0.0.0.255
  network 10.4.1.0 0.0.0.255
  network 10.5.1.0 0.0.0.255
#
return
```

步骤2 配置Router_2

```
#
 sysname Router_2
#
interface GigabitEthernet1/0/0   //配置公网出接口
 ip address 1.1.1.1 255.255.255.0
#
interface GigabitEthernet2/0/0  //配置私网出接口
 ip address 10.2.1.1 255.255.255.0
#
interface Tunnel0/0/1   //配置Tunnel接口，源地址是发出报文的实际接口IP地址，目的地址是接收报文的实际接口IP地址
 ip address 10.4.1.2 255.255.255.0
 tunnel-protocol gre
 source 1.1.1.1
 destination 3.1.1.1
#
ospf 1   //配置公网路由
 area 0.0.0.0
  network 1.1.1.0 0.0.0.255
#
ospf 2   //配置私网路由
 area 0.0.0.0
  network 10.2.1.0 0.0.0.255
  network 10.4.1.0 0.0.0.255
#
return
```

步骤3 配置Router_3

```
#
 sysname Router_3
#
interface GigabitEthernet1/0/0   //配置公网出接口
 ip address 2.1.1.1 255.255.255.0
#
interface GigabitEthernet2/0/0  //配置私网出接口
 ip address 10.3.1.1 255.255.255.0
#
interface Tunnel0/0/2   //配置Tunnel接口，源地址是发出报文的实际接口IP地址，目的地址是接收报文的实际接口IP地址
 ip address 10.5.1.2 255.255.255.0
 tunnel-protocol gre
 source 2.1.1.1
 destination 3.1.1.1
#
ospf 1   //配置公网路由
 area 0.0.0.0
  network 2.1.1.0 0.0.0.255
#
ospf 2   //配置私网路由
 area 0.0.0.0
  network 10.3.1.0 0.0.0.255
  network 10.5.1.0 0.0.0.255
#
return
```

 版权所有 © 华为技术有限公司

步骤4 验证配置结果

在Router上执行**display ip routing-table**命令，可以看到去往对端目的地址的出接口为Tunnel接口。

PC_1分别和PC_2、PC_3互相Ping通。

----结束

配置注意事项

- 设备两端需要配置到私网的路由。
- 设备两端Tunnel接口的源IP和目的IP要相互对应。

6.2.6 配置 IPv6 over IPv4 GRE 隧道示例

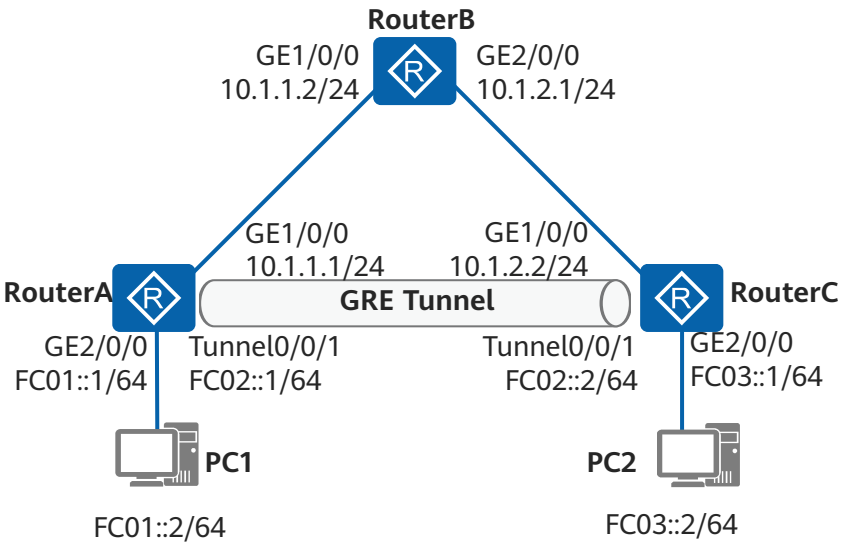
规格

适用于V200R003及V200R003以上版本、所有形态的路由器。

组网需求

如图6-29所示，RouterA、RouterB、RouterC之间通过IPv4网络互连。RouterA和RouterC分别连接到IPv6网络，且下挂IPv6主机PC1和PC2。客户希望在RouterA和RouterC之间配置IPv6 over IPv4 GRE隧道，实现PC1和PC2间互通。

图 6-29 配置 IPv6 over IPv4 GRE 隧道组网图



操作步骤

步骤1 配置RouterA

```
#
 sysname RouterA
#
```


版权所有 © 华为技术有限公司

```
ipv6
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.1 255.255.255.0     //配置接口的IPv4地址
#
interface GigabitEthernet2/0/0
 ipv6 enable
 ipv6 address FC01::1/64     //配置接口的IPv6地址
#
interface Tunnel0/0/1     //配置GRE隧道的Tunnel接口，隧道模式为GRE，Tunnel接口配置为IPv6地址，Tunnel接口的源地址和目的地址为IPv4地址
 ipv6 enable
 ipv6 address FC02::1/64
 tunnel-protocol gre
 source 10.1.1.1
 destination 10.1.2.2
#
ip route-static 10.1.2.0 255.255.255.0 10.1.1.2     //配置IPv4静态路由，确保RouterA到RouterC路由可达
#
ipv6 route-static FC03:: 64 Tunnel0/0/1     //配置IPv6静态路由，确保RouterA到PC2路由可达
#
return
```

步骤2 配置RouterB

```
#
 sysname RouterB
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 10.1.2.1 255.255.255.0
#
return
```

步骤3 配置RouterC

```
#
 sysname RouterC
#
ipv6
#
interface GigabitEthernet1/0/0
 ip address 10.1.2.2 255.255.255.0
#
interface GigabitEthernet2/0/0
 ipv6 enable
 ipv6 address FC03::1/64
#
interface Tunnel0/0/1
 ipv6 enable
 ipv6 address FC02::2/64
 tunnel-protocol gre
 source 10.1.2.2
 destination 10.1.1.1
#
ip route-static 10.1.1.0 255.255.255.0 10.1.2.1     //配置IPv4静态路由，确保RouterC到RouterA路由可达
#
ipv6 route-static FC01:: 64 Tunnel0/0/1     //配置IPv6静态路由，确保RouterC到PC1路由可达
#
return
```

步骤4 验证配置结果

PC1和PC2能互相Ping通。

----结束

 版权所有 © 华为技术有限公司

配置注意事项

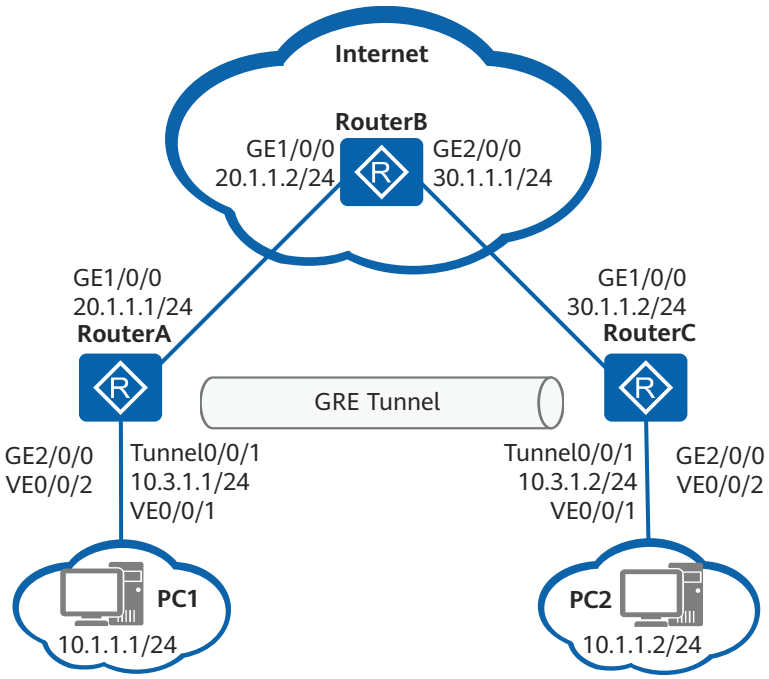
- IPv4网络需要路由可达。
- Tunnel两端必须配置隧道的源地址和目的地址，且本端配置的源端地址应该与对端配置的目的端地址相同，本端配置的目的端地址应该与对端配置的源端地址相同。

6.2.7 配置 Ethernet over GRE 隧道示例

组网需求

如图6-30，RouterA、B和C使用OSPF协议路由实现公网互通。分支以太网内的PC1和PC2属于同一网段，现需要PC1和PC2通过公网实现互通。

图 6-30 配置 Ethernet over GRE 组网图



配置思路

配置Ethernet over GRE实现以太网协议互通的思路如下：

1. 在所有设备之间运行OSPF路由协议实现设备间路由互通。
2. 在RouterA和RouterC之间使用GRE隧道直连，并在RouterA和RouterC上配置Ethernet over GRE，使PC1和PC2之间的流量通过GRE隧道传输，实现PC1和PC2互通。

版权所有 © 华为技术有限公司

操作步骤

步骤1 配置各物理接口IP地址。

配置RouterA。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 20.1.1.1 255.255.255.0
[RouterA-GigabitEthernet1/0/0] quit
```

配置RouterB。

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] ip address 20.1.1.2 255.255.255.0
[RouterB-GigabitEthernet1/0/0] quit
[RouterB] interface gigabitethernet 2/0/0
[RouterB-GigabitEthernet2/0/0] ip address 30.1.1.1 255.255.255.0
[RouterB-GigabitEthernet2/0/0] quit
```

配置RouterC。

```
<Huawei> system-view
[Huawei] sysname RouterC
[RouterC] interface gigabitethernet 1/0/0
[RouterC-GigabitEthernet1/0/0] ip address 30.1.1.2 255.255.255.0
[RouterC-GigabitEthernet1/0/0] quit
```

步骤2 配置设备间使用OSPF路由。

配置RouterA。

```
[RouterA] ospf 1
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] quit
```

配置RouterB。

```
[RouterB] ospf 1
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] network 30.1.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] quit
[RouterB-ospf-1] quit
```

配置RouterC。

```
[RouterC] ospf 1
[RouterC-ospf-1] area 0
[RouterC-ospf-1-area-0.0.0.0] network 30.1.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] quit
[RouterC-ospf-1] quit
```

配置完成后，在RouterA和RouterC上执行**display ip routing-table**命令，可以看到它们能够学到去往对端接口网段地址的OSPF路由。

以RouterA的显示为例。

```
[RouterA] display ip routing-table protocol ospf
Route Flags: R - relay, D - download to fib, T - to vpn-instance
------------------------------------------------------------------------------
Public routing table : OSPF
         Destinations : 1        Routes : 1
```

 版权所有 © 华为技术有限公司

```
OSPF routing table status : <Active>
        Destinations : 1        Routes : 1

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      30.1.1.0/24  OSPF    10   2           D   20.1.1.2        GigabitEthernet1/0/0

OSPF routing table status : <Inactive>
        Destinations : 0        Routes : 0
```

步骤3 配置Tunnel接口，建立GRE隧道。

配置RouterA。

```
[RouterA] interface tunnel 0/0/1
[RouterA-Tunnel0/0/1] tunnel-protocol gre
[RouterA-Tunnel0/0/1] ip address 10.3.1.1 255.255.255.0
[RouterA-Tunnel0/0/1] source 20.1.1.1
[RouterA-Tunnel0/0/1] destination 30.1.1.2
[RouterA-Tunnel0/0/1] quit
```

配置RouterC。

```
[RouterC] interface tunnel 0/0/1
[RouterC-Tunnel0/0/1] tunnel-protocol gre
[RouterC-Tunnel0/0/1] ip address 10.3.1.2 255.255.255.0
[RouterC-Tunnel0/0/1] source 30.1.1.2
[RouterC-Tunnel0/0/1] destination 20.1.1.1
[RouterC-Tunnel0/0/1] quit
```

配置完成后，Tunnel接口状态变为Up，Tunnel接口之间可以互相Ping通。

以RouterA的显示为例：

```
[RouterA] ping -a 10.3.1.1 10.3.1.2
  PING 10.3.1.2: 56  data bytes, press CTRL_C to break
    Reply from 10.3.1.2: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 10.3.1.2: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 10.3.1.2: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 10.3.1.2: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 10.3.1.2: bytes=56 Sequence=5 ttl=255 time=1 ms

  --- 10.3.1.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/1 ms
```

步骤4 配置Ethernet over GRE。

RouterC的配置与RouterA相同，以RouterA的配置为例。

配置二层VE接口VE0/0/2，并绑定到LAN侧物理以太网接口GE2/0/0。

```
[RouterA] vlan 100
[RouterA-vlan100] quit
[RouterA] interface virtual-ethernet 0/0/2
[RouterA-Virtual-Ethernet0/0/2] portswitch
[RouterA-Virtual-Ethernet0/0/2] port link-type access
[RouterA-Virtual-Ethernet0/0/2] port default vlan 100
[RouterA-Virtual-Ethernet0/0/2] quit
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet0/0/2] map interface virtual-ethernet 0/0/2
[RouterA-GigabitEthernet0/0/2] quit
```

配置二层VE接口VE0/0/1，并绑定到WAN侧Tunnel接口Tunnel0/0/1。

 版权所有 © 华为技术有限公司

```
[RouterA] interface virtual-ethernet 0/0/1
[RouterA-Virtual-Ethernet0/0/1] portswitch
[RouterA-Virtual-Ethernet0/0/1] port link-type trunk
[RouterA-Virtual-Ethernet0/0/1] port trunk allow-pass vlan 100
[RouterA-Virtual-Ethernet0/0/1] quit
[RouterA] interface tunnel 0/0/1
[RouterA-Tunnel0/0/1] map interface virtual-ethernet 0/0/1
[RouterA-Tunnel0/0/1] quit
```

步骤5 验证配置结果。

配置完成后，PC1和PC2可以互相Ping通。

----结束

配置文件

- RouterA的配置文件

```
#
 sysname RouterA
#
vlan batch 100
#
interface GigabitEthernet1/0/0
 ip address 20.1.1.1 255.255.255.0
#
interface GigabitEthernet2/0/0
 map interface Virtual-Ethernet0/0/2
#
interface Virtual-Ethernet0/0/1
 portswitch
 port link-type trunk
 port trunk allow-pass vlan 100
#
interface Virtual-Ethernet0/0/2
 portswitch
 port link-type access
 port default vlan 100
#
interface Tunnel0/0/1
 ip address 10.3.1.1 255.255.255.0
 tunnel-protocol gre
 source 20.1.1.1
 destination 30.1.1.2
 map interface Virtual-Ethernet0/0/1
#
ospf 1
 area 0.0.0.0
  network 20.1.1.0 0.0.0.255
#
return
```

- RouterB的配置文件

```
#
 sysname RouterB
#
interface GigabitEthernet1/0/0
 ip address 20.1.1.2 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 30.1.1.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 20.1.1.0 0.0.0.255
  network 30.1.1.0 0.0.0.255
#
return
```

 版权所有 © 华为技术有限公司

- RouterC的配置文件

```
#
 sysname RouterC
#
vlan batch 100
#
interface GigabitEthernet1/0/0
 ip address 30.1.1.2 255.255.255.0
#
interface GigabitEthernet2/0/0
 map interface Virtual-Ethernet0/0/2
#
interface Virtual-Ethernet0/0/1
 portswitch
 port link-type trunk
 port trunk allow-pass vlan 100
#
interface Virtual-Ethernet0/0/2
 portswitch
 port link-type access
 port default vlan 100
#
interface Tunnel0/0/1
 ip address 10.3.1.2 255.255.255.0
 tunnel-protocol gre
 source 30.1.1.2
 destination 20.1.1.1
 map interface Virtual-Ethernet0/0/1
#
ospf 1
 area 0.0.0.0
  network 30.1.1.0 0.0.0.255
#
return
```

6.3 DSVPN

6.3.1 配置分支机构之间相互路由学习，并通过 DSVPN 方式实现互通的示例（适用少量分支机构）

规格

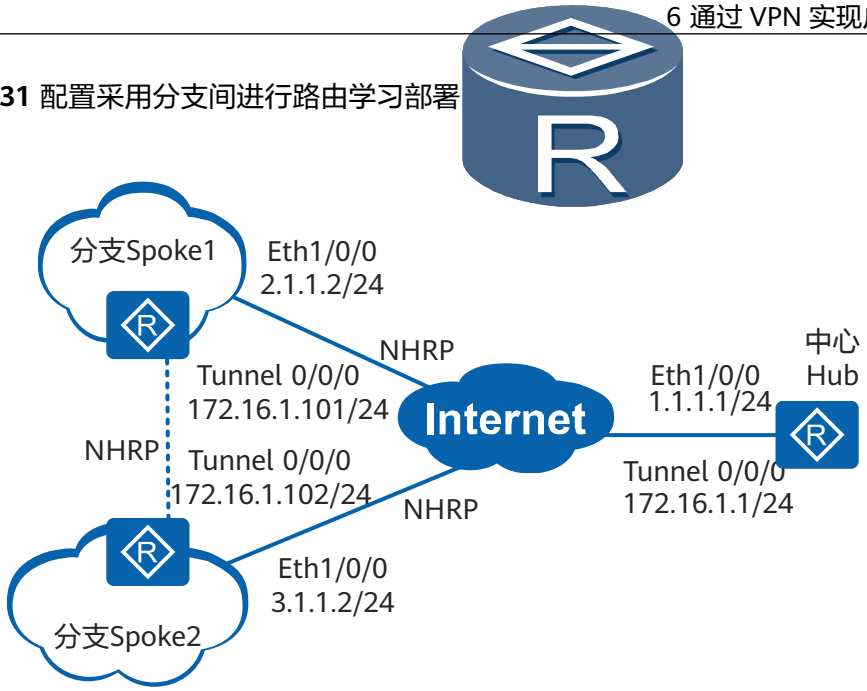
适用于所有版本、所有形态的路由器。

组网需求

如图6-31所示，中心Hub、分支Spoke1和Spoke2属于同一自治系统，他们之间通过路由协议可达到IP网络互连。

版权所有 © 华为技术有限公司

图 6-31 配置采用分支间进行路由学习部署



操作步骤

步骤1 配置spoke1

```
#
interface Ethernet1/0/0
 ip address 2.1.1.2 255.255.255.0
#
interface Tunnel0/0/0
 ip address 172.16.1.101 255.255.255.0
 tunnel-protocol gre p2mp  //配置隧道模式为MGRE
 source Ethernet1/0/0  //设置Tunnel接口的源地址或源接口
 nhrp entry 172.16.1.1 1.1.1.1 register  //配置NHRP地址映射表
 ospf network-type broadcast  //将接口的网络类型更改为广播
#
ospf 1  //配置OSPF协议
 area 0.0.0.1
  network 2.1.1.0 0.0.0.255
ospf 2
 area 0.0.0.0
  network 172.16.1.0 0.0.0.255
#
return
```

步骤2 配置spoke2

```
#
interface Ethernet1/0/0
 ip address 3.1.1.2 255.255.255.0
#
interface Tunnel0/0/0
 ip address 172.16.1.102 255.255.255.0
 tunnel-protocol gre p2mp  //配置隧道模式为MGRE
 source Ethernet1/0/0  //设置Tunnel接口的源地址或源接口
 nhrp entry 172.16.1.1 1.1.1.1 register  //配置NHRP地址映射表
 ospf network-type broadcast  //将接口的网络类型更改为广播
#
ospf 1  //配置OSPF协议
 area 0.0.0.1
  network 3.1.1.0 0.0.0.255
```


版权所有 © 华为技术有限公司

```
ospf 2
 area 0.0.0.0
  network 172.16.1.0 0.0.0.255
#
return
```

步骤3 配置Hub

```
#
interface Ethernet1/0/0
 ip address 1.1.1.1 255.255.255.0
#
interface Tunnel0/0/0
 ip address 172.16.1.1 255.255.255.0
 tunnel-protocol gre p2mp  //配置隧道模式为MGRE
 source Ethernet1/0/0  //设置Tunnel接口的源地址或源接口
 nhrp entry multicast dynamic  //配置动态注册的分支加入NHRP组播成员表
 ospf network-type broadcast  //将接口的网络类型更改为广播
#
ospf 1  //配置OSPF协议
 area 0.0.0.1
  network 1.1.1.0 0.0.0.255
ospf 2
 area 0.0.0.0
  network 172.16.1.0 0.0.0.255
#
return
```

步骤4 验证配置结果

在spoke1上ping分支spoke2的IP地址172.16.1.102，则在spoke1和spoke2上可以分别看到彼此的Peer表项。

----结束

配置注意事项

- 如果动态路由配置为OSPF，则在Tunnel接口下，OSPF网络类型配置为广播型。

6.3.2 配置分支机构只保存到总部的汇聚路由，并通过 DSVPN 方式实现分支机构之间互通的示例（适用多个分支机构）

规格

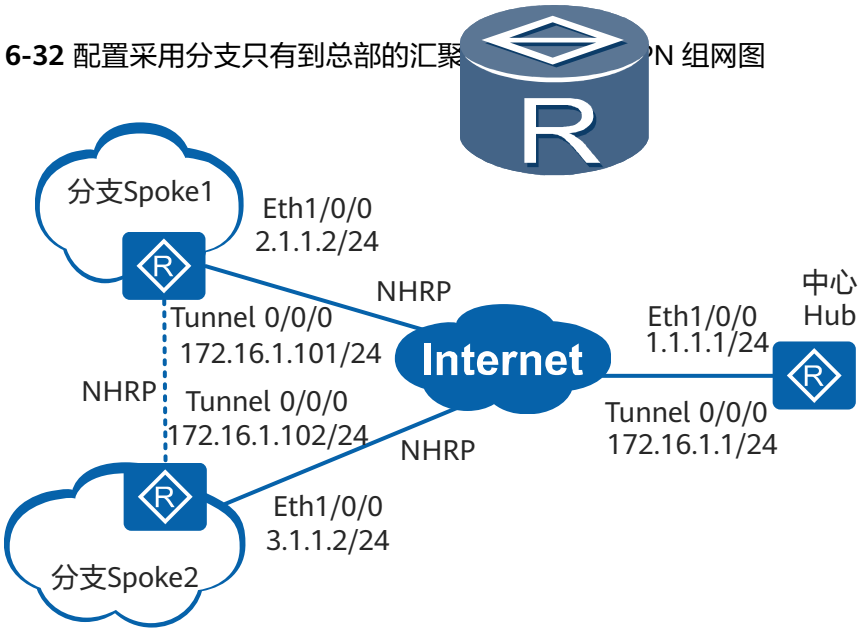
适用于所有版本、所有形态的路由器。

组网需求

如图6-32所示，中心Hub、分支Spoke1和Spoke2属于同一自治系统，他们之间通过路由协议可达到IP网络互连。

 版权所有 © 华为技术有限公司

图 6-32 配置采用分支只有到总部的汇聚[illegible]N 组网图



操作步骤

步骤1 配置spoke1

```
#
interface Ethernet1/0/0
 ip address 2.1.1.2 255.255.255.0
#
interface Tunnel0/0/0
 ip address 172.16.1.101 255.255.255.0
 tunnel-protocol gre p2mp  //配置隧道模式为MGRE
 source Ethernet1/0/0  //设置Tunnel接口的源地址或源接口
 nhrp entry 172.16.1.1 1.1.1.1 register  //配置NHRP地址映射表
 nhrp shortcut  //使能shortcut功能
#
rip 1  //配置路由功能
 version 2
 network 172.16.0.0
#
ospf 2
 area 0.0.0.1
  network 2.1.1.0 0.0.0.255
#
return
```

步骤2 配置spoke2

```
#
interface Ethernet1/0/0
 ip address 3.1.1.2 255.255.255.0
#
interface Tunnel0/0/0
 ip address 172.16.1.102 255.255.255.0
 tunnel-protocol gre p2mp  //配置隧道模式为MGRE
 source Ethernet1/0/0  //设置Tunnel接口的源地址或源接口
 nhrp entry 172.16.1.1 1.1.1.1 register  //配置NHRP地址映射表
 nhrp shortcut  //使能shortcut功能
#
rip 1  //配置路由功能
 version 2
 network 172.16.0.0
#
ospf 2
 area 0.0.0.1
  network 3.1.1.0 0.0.0.255
```


版权所有 © 华为技术有限公司

```
#
return
```

步骤3 配置Hub

```
#
interface Ethernet1/0/0
 ip address 1.1.1.1 255.255.255.0
#
interface LoopBack0
 ip address 192.168.0.1 255.255.255.0
#
interface Tunnel0/0/0
 ip address 172.16.1.1 255.255.255.0
 rip version 2 multicast
 rip summary-address 192.168.0.0 255.255.0.0
 tunnel-protocol gre p2mp  //配置隧道模式为MGRE
 source Ethernet1/0/0  //设置Tunnel接口的源地址或源接口
 nhrp redirect  //使能nhrp redirect功能
 nhrp entry multicast dynamic  //配置动态注册的分支加入NHRP组播成员表
#
rip 1  //配置路由功能
 version 2
 network 172.16.0.0
 network 192.168.0.0
#
ospf 2
 area 0.0.0.1
  network 1.1.1.0 0.0.0.255
#
return
```

步骤4 验证配置结果

在spoke1上ping分支spoke2的IP地址172.16.1.102，则在spoke1和spoke2上可以分别看到彼此的Peer表项。

----结束

配置注意事项

- 如果动态路由配置为RIP，则总部Hub的Tunnel接口上要开启水平分割和自动路由聚合功能。

6.3.3 配置利用总部 Hub 备份，分支机构之间通过 DSVPN 方式实现稳定互通的示例

规格

适用于所有版本、所有形态的路由器。

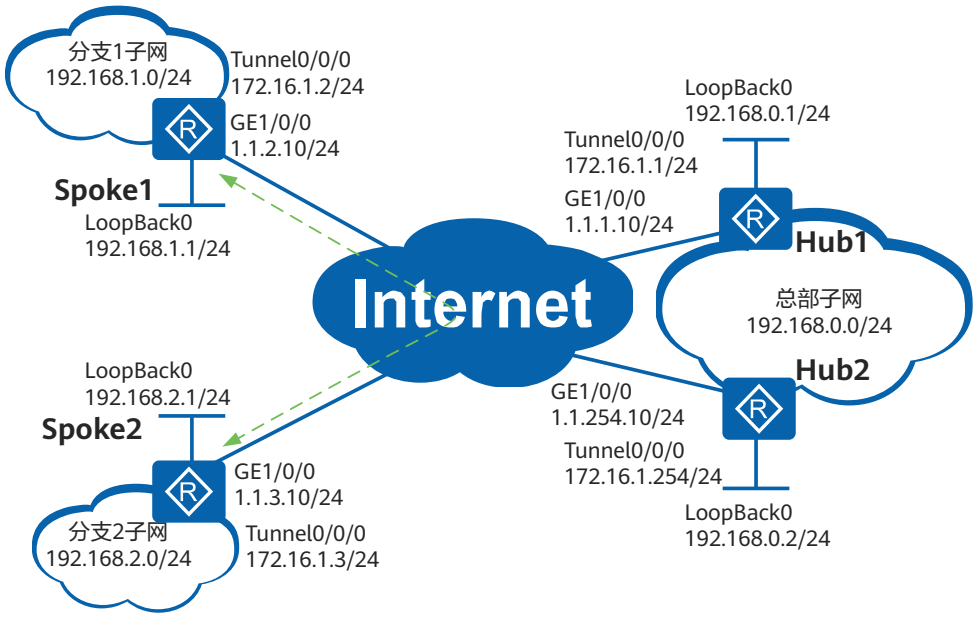
组网需求

某大型企业有总部（Hub1和Hub2）和多个分支（Spoke1、Spoke2……，举例中仅使用两个分支），分布在不同地域，总部和分支的子网环境会经常出现变动。分支采用动态地址接入公网。企业现网网络规划使用OSPF路由协议。

现在用户希望能够实现分支之间的VPN互联，Hub1作为主用Hub，Hub2作为备用Hub，在Hub1故障时接管协议报文的转发，在Hub1故障恢复后继续冗余备份。

 版权所有 © 华为技术有限公司

图 6-33 配置双 Hub DSVPN 组网图



操作步骤

步骤1 配置Hub1

```
#
sysname Hub1
#
interface GigabitEthernet1/0/0
 ip address 1.1.1.10 255.255.255.0
#
interface LoopBack0
 ip address 192.168.0.1 255.255.255.0
#
interface Tunnel0/0/0
 ip address 172.16.1.1 255.255.255.0
 tunnel-protocol gre p2mp
 source GigabitEthernet1/0/0
 ospf cost 1000  //与Hub2配置不同的ospf cost值是为了让Spoke优先选取Hub1作为路由的下一跳
 ospf network-type p2mp
 nhrp redirect  //shortcut场景总部必配
 nhrp entry multicast dynamic
#
ospf 1 router-id 172.16.1.1
 area 0.0.0.0
  network 172.16.1.0 0.0.0.255
#
ospf 2  //配置OSPF路由协议，实现公网路由可达
 area 0.0.0.1
  network 1.1.1.0 0.0.0.255
#
return
```

步骤2 配置Hub2

```
#
sysname Hub2
#
```


版权所有 © 华为技术有限公司

```
interface GigabitEthernet1/0/0
 ip address 1.1.254.10 255.255.255.0
#
interface LoopBack0
 ip address 192.168.0.2 255.255.255.0
#
interface Tunnel0/0/0
 ip address 172.16.1.254 255.255.255.0
 tunnel-protocol gre p2mp
 source GigabitEthernet1/0/0
 ospf cost 3000  //与Hub1配置不同的ospf cost值是为了让Spoke优先选取Hub1作为路由的下一跳
 ospf network-type p2mp
 nhrp redirect  //shortcut场景总部必配
 nhrp entry multicast dynamic
#
ospf 1 router-id 172.16.1.254
 area 0.0.0.0
  network 172.16.1.0 0.0.0.255
#
ospf 2  //配置OSPF路由协议，实现公网路由可达
 area 0.0.0.1
  network 1.1.1.0 0.0.0.255
#
return
```

步骤3 配置Spoke1

```
#
sysname Spoke1
#
interface GigabitEthernet1/0/0
 ip address 1.1.2.10 255.255.255.0
#
interface LoopBack0
 ip address 192.168.1.1 255.255.255.0
#
interface Tunnel0/0/0
 ip address 172.16.1.2 255.255.255.0
 tunnel-protocol gre p2mp
 source GigabitEthernet1/0/0
 ospf network-type p2mp  //配置OSPF网络类型为p2mp以实现分支到总部的路由
 nhrp shortcut  //shortcut场景分支必配
 nhrp registration interval 300  //在Hub1从故障中恢复之后，只有等到Spoke向其进行注册之后，才能重新学习到Hub1的路由。为了让Spoke快速感知Hub1，可以将Spoke的注册间隔调整到合适的值（默认注册间隔为1800秒）
 nhrp entry 172.16.1.1 1.1.1.10 register
 nhrp entry 172.16.1.254 1.1.254.10 register
#
ospf 1 router-id 172.16.1.2  //分支间子网路由学习
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
  network 172.16.1.0 0.0.0.255
#
ospf 2  //配置OSPF路由协议，实现公网路由可达
 area 0.0.0.1
  network 1.1.2.0 0.0.0.255
#
return
```

步骤4 配置Spoke2

```
#
sysname Spoke2
#
interface GigabitEthernet1/0/0
 ip address 1.1.3.10 255.255.255.0
#
interface LoopBack0
 ip address 192.168.2.1 255.255.255.0
#
interface Tunnel0/0/0
```

 版权所有 © 华为技术有限公司

```
 ip address 172.16.1.3 255.255.255.0
 tunnel-protocol gre p2mp
 source GigabitEthernet1/0/0
 ospf network-type p2mp  //配置OSPF网络类型为p2mp以实现分支到总部的路由
 nhrp shortcut  //shortcut场景分支必配
 nhrp registration interval 300      //在Hub1从故障中恢复之后，只有等到Spoke向其进行注册之后，才能重新学习到Hub1的路由。为了让Spoke快速感知Hub1，可以将Spoke的注册间隔调整到合适的值（默认注册间隔为1800秒）
nhrp entry 172.16.1.1 1.1.1.10 register
 nhrp entry 172.16.1.254 1.1.254.10 register
#
ospf 1 router-id 172.16.1.3  //分支间子网路由学习
 area 0.0.0.0
  network 192.168.2.0 0.0.0.255
  network 172.16.1.0 0.0.0.255
#
ospf 2  //配置OSPF路由协议，实现公网路由可达
 area 0.0.0.1
  network 1.1.3.0 0.0.0.255
#
return
```

步骤5 验证配置结果

- 检查DSVPN配置结果

  配置完成后，检查Spoke上的NHRP peer信息。

  # 在Spoke1上执行**display nhrp peer all**操作，结果如下。

```
[Huawei] display nhrp peer all
--------------------------------------------------------------------------------
Protocol-addr   Mask  NBMA-addr      NextHop-addr    Type        Flag
--------------------------------------------------------------------------------
172.16.1.1      32    1.1.1.10       172.16.1.1      static      hub
--------------------------------------------------------------------------------
Tunnel interface: Tunnel0/0/0
Created time    : 05:35:50
Expire time     : --
--------------------------------------------------------------------------------
Protocol-addr   Mask  NBMA-addr      NextHop-addr    Type        Flag
--------------------------------------------------------------------------------
172.16.1.254    32    1.1.254.10     172.16.1.254    static      hub
--------------------------------------------------------------------------------
Tunnel interface: Tunnel0/0/0
Created time    : 04:32:49
Expire time     : --

Number of nhrp peers: 2
```

  # 在Spoke2上执行**display nhrp peer all**操作，结果如下。

```
[Huawei] display nhrp peer all
--------------------------------------------------------------------------------
Protocol-addr   Mask  NBMA-addr      NextHop-addr    Type        Flag
--------------------------------------------------------------------------------
172.16.1.1      32    1.1.1.10       172.16.1.1      static      hub
--------------------------------------------------------------------------------
Tunnel interface: Tunnel0/0/0
Created time    : 05:36:30
Expire time     : --
--------------------------------------------------------------------------------
Protocol-addr   Mask  NBMA-addr      NextHop-addr    Type        Flag
--------------------------------------------------------------------------------
172.16.1.254    32    1.1.254.10     172.16.1.254    static      hub
--------------------------------------------------------------------------------
Tunnel interface: Tunnel0/0/0
Created time    : 04:33:14
Expire time     : --

Number of nhrp peers: 2
```

 版权所有 © 华为技术有限公司

说明

完成上述配置后，执行**display nhrp peer all**命令，spoke1和spoke2上只能看到Hub1和Hub2的静态NHRP peer表项。

检查Hub上Spoke1和Spoke2的注册信息。

在Hub1上执行**display nhrp peer all**操作，结果如下。

```
[Huawei] display nhrp peer all
--------------------------------------------------------------------------------
Protocol-addr   Mask  NBMA-addr      NextHop-addr    Type        Flag
--------------------------------------------------------------------------------
172.16.1.3      32    1.1.3.10       172.16.1.3      dynamic     route tunnel
--------------------------------------------------------------------------------
Tunnel interface: Tunnel0/0/0
Created time    : 02:59:52
Expire time     : 01:59:12
--------------------------------------------------------------------------------
Protocol-addr   Mask  NBMA-addr      NextHop-addr    Type        Flag
--------------------------------------------------------------------------------
172.16.1.2      32    1.1.2.10       172.16.1.2      dynamic     route tunnel
--------------------------------------------------------------------------------
Tunnel interface: Tunnel0/0/0
Created time    : 02:59:32
Expire time     : 01:59:09

Number of nhrp peers: 2
```

在Hub2上执行**display nhrp peer all**操作，结果如下。

```
[Huawei] display nhrp peer all
--------------------------------------------------------------------------------
Protocol-addr   Mask  NBMA-addr      NextHop-addr    Type        Flag
--------------------------------------------------------------------------------
172.16.1.3      32    1.1.3.10       172.16.1.3      dynamic     route tunnel
--------------------------------------------------------------------------------
Tunnel interface: Tunnel0/0/0
Created time    : 00:21:09
Expire time     : 01:59:51
--------------------------------------------------------------------------------
Protocol-addr   Mask  NBMA-addr      NextHop-addr    Type        Flag
--------------------------------------------------------------------------------
172.16.1.2      32    1.1.2.10       172.16.1.2      dynamic     route tunnel
--------------------------------------------------------------------------------
Tunnel interface: Tunnel0/0/0
Created time    : 00:14:13
Expire time     : 01:59:48

Number of nhrp peers: 2
```

- 检查OSPF路由信息

  检查Hub上的OSPF路由信息。

  # 在Hub1上执行**display ospf 1 routing**操作，结果如下。

```
[Huawei] display ospf 1 routing

        OSPF Process 1 with Router ID 172.16.1.1
              Routing Tables

 Routing for Network
 Destination        Cost  Type       NextHop         AdvRouter       Area
 172.16.1.1/32      0     Stub       172.16.1.1      172.16.1.1      0.0.0.0
 172.16.1.2/32      1000  Stub       172.16.1.2      172.16.1.2      0.0.0.0
 172.16.1.3/32      5562  Stub       172.16.1.2      172.16.1.3      0.0.0.0
 172.16.1.254/32    2562  Stub       172.16.1.2      172.16.1.254    0.0.0.0
 192.168.1.1/32     1000  Stub       172.16.1.2      172.16.1.2      0.0.0.0
 192.168.2.1/32     5562  Stub       172.16.1.2      172.16.1.3      0.0.0.0

 Total Nets: 6
```

 版权所有 © 华为技术有限公司

```
Intra Area: 6  Inter Area: 0  ASE: 0  NSSA: 0
```

在Hub2上执行**display ospf 1 routing**操作，结果如下。

```
[Huawei] display ospf 1 routing

        OSPF Process 1 with Router ID 172.16.1.254
                Routing Tables

 Routing for Network
 Destination        Cost  Type       NextHop         AdvRouter       Area
 172.16.1.254/32    0     Stub       172.16.1.254    172.16.1.254    0.0.0.0
 172.16.1.1/32      4562  Stub       172.16.1.3      172.16.1.1      0.0.0.0
 172.16.1.2/32      5562  Stub       172.16.1.3      172.16.1.2      0.0.0.0
 172.16.1.3/32      3000  Stub       172.16.1.3      172.16.1.3      0.0.0.0
 192.168.1.1/32     5562  Stub       172.16.1.3      172.16.1.2      0.0.0.0
 192.168.2.1/32     3000  Stub       172.16.1.3      172.16.1.3      0.0.0.0

 Total Nets: 6
 Intra Area: 6  Inter Area: 0  ASE: 0  NSSA: 0
```

检查Spoke上的OSPF路由信息。

在Spoke1上执行**display ospf 1 routing**操作，结果如下。

```
[Huawei] display ospf 1 routing

        OSPF Process 1 with Router ID 172.16.1.2
                Routing Tables

 Routing for Network
 Destination        Cost  Type       NextHop         AdvRouter       Area
 172.16.1.2/32      0     Stub       172.16.1.2      172.16.1.2      0.0.0.0
 192.168.1.1/32     0     Stub       192.168.1.1     172.16.1.2      0.0.0.0
 172.16.1.1/32      1562  Stub       172.16.1.1      172.16.1.1      0.0.0.0
 172.16.1.3/32      2562  Stub       172.16.1.1      172.16.1.3      0.0.0.0
 172.16.1.254/32    1562  Stub       172.16.1.254    172.16.1.254    0.0.0.0
 192.168.2.1/32     2562  Stub       172.16.1.1      172.16.1.3      0.0.0.0

 Total Nets: 6
 Intra Area: 6  Inter Area: 0  ASE: 0  NSSA: 0
```

在Spoke2上执行**display ospf 1 routing**操作，结果如下。

```
[Huawei] display ospf 1 routing

        OSPF Process 1 with Router ID 172.16.1.3
                Routing Tables

 Routing for Network
 Destination        Cost  Type       NextHop         AdvRouter       Area
 172.16.1.3/32      0     Stub       172.16.1.3      172.16.1.3      0.0.0.0
 192.168.2.1/32     0     Stub       192.168.2.1     172.16.1.3      0.0.0.0
 172.16.1.1/32      1562  Stub       172.16.1.1      172.16.1.1      0.0.0.0
 172.16.1.2/32      2562  Stub       172.16.1.1      172.16.1.2      0.0.0.0
 172.16.1.254/32    1562  Stub       172.16.1.254    172.16.1.254    0.0.0.0
 192.168.1.1/32     2562  Stub       172.16.1.1      172.16.1.2      0.0.0.0

 Total Nets: 6
 Intra Area: 6  Inter Area: 0  ASE: 0  NSSA: 0
```

- 执行**ping**操作，查看配置结果

  在Spoke1上ping分支Spoke2的子网地址192.168.2.1，则在Spoke1和Spoke2上可以分别看到彼此的动态NHRP peer表项。

  # 在Spoke1上执行**ping -a 192.168.1.1 192.168.2.1**操作，结果如下。

```
[Huawei] ping -a 192.168.1.1 192.168.2.1
  PING 192.168.2.1: 56  data bytes, press CTRL_C to break
```

 版权所有 © 华为技术有限公司

```
  Reply from 192.168.2.1: bytes=56 Sequence=1 ttl=254 time=3 ms
  Reply from 192.168.2.1: bytes=56 Sequence=2 ttl=255 time=2 ms
  Reply from 192.168.2.1: bytes=56 Sequence=3 ttl=255 time=2 ms
  Reply from 192.168.2.1: bytes=56 Sequence=4 ttl=255 time=2 ms
  Reply from 192.168.2.1: bytes=56 Sequence=5 ttl=255 time=2 ms

--- 192.168.2.1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 2/2/3 ms
```

在Spoke1上执行**display nhrp peer all**操作，结果如下。

```
[Huawei] display nhrp peer all
------------------------------------------------------------------------------
Protocol-addr   Mask  NBMA-addr      NextHop-addr    Type        Flag
------------------------------------------------------------------------------
172.16.1.1      32    1.1.1.10       172.16.1.1      static      hub
------------------------------------------------------------------------------
Tunnel interface: Tunnel0/0/0
Created time    : 05:42:50
Expire time     : --
------------------------------------------------------------------------------
Protocol-addr   Mask  NBMA-addr      NextHop-addr    Type        Flag
------------------------------------------------------------------------------
172.16.1.254    32    1.1.254.10     172.16.1.254    static      hub
------------------------------------------------------------------------------
Tunnel interface: Tunnel0/0/0
Created time    : 04:39:49
Expire time     : --
------------------------------------------------------------------------------
Protocol-addr   Mask  NBMA-addr      NextHop-addr    Type        Flag
------------------------------------------------------------------------------
192.168.2.1     32    1.1.3.10       172.16.1.3      dynamic     route network
------------------------------------------------------------------------------
Tunnel interface: Tunnel0/0/0
Created time    : 00:00:19
Expire time     : 01:59:41
------------------------------------------------------------------------------
Protocol-addr   Mask  NBMA-addr      NextHop-addr    Type        Flag
------------------------------------------------------------------------------
172.16.1.3      32    1.1.3.10       172.16.1.3      dynamic     route tunnel
------------------------------------------------------------------------------
Tunnel interface: Tunnel0/0/0
Created time    : 00:00:19
Expire time     : 01:59:41
------------------------------------------------------------------------------
Protocol-addr   Mask  NBMA-addr      NextHop-addr    Type        Flag
------------------------------------------------------------------------------
192.168.1.1     32    1.1.2.10       172.16.1.2      dynamic     local
------------------------------------------------------------------------------
Tunnel interface: Tunnel0/0/0
Created time    : 00:00:19
Expire time     : 01:59:41

Number of nhrp peers: 5
```

在Spoke2上执行**display nhrp peer all**操作，结果如下。

```
[Huawei] display nhrp peer all
------------------------------------------------------------------------------
Protocol-addr   Mask  NBMA-addr      NextHop-addr    Type        Flag
------------------------------------------------------------------------------
172.16.1.1      32    1.1.1.10       172.16.1.1      static      hub
------------------------------------------------------------------------------
Tunnel interface: Tunnel0/0/0
Created time    : 05:43:19
Expire time     : --
------------------------------------------------------------------------------
Protocol-addr   Mask  NBMA-addr      NextHop-addr    Type        Flag
```

 版权所有 © 华为技术有限公司

```
--------------------------------------------------------------------------------
172.16.1.254    32    1.1.254.10    172.16.1.254    static       hub
--------------------------------------------------------------------------------
Tunnel interface: Tunnel0/0/0
Created time    : 04:40:03
Expire time     : --
--------------------------------------------------------------------------------
Protocol-addr   Mask  NBMA-addr      NextHop-addr    Type        Flag
--------------------------------------------------------------------------------
192.168.1.1     32    1.1.2.10       172.16.1.2      dynamic     route network
--------------------------------------------------------------------------------
Tunnel interface: Tunnel0/0/0
Created time    : 00:00:45
Expire time     : 01:59:15
--------------------------------------------------------------------------------
Protocol-addr   Mask  NBMA-addr      NextHop-addr    Type        Flag
--------------------------------------------------------------------------------
172.16.1.2      32    1.1.2.10       172.16.1.2      dynamic     route tunnel
--------------------------------------------------------------------------------
Tunnel interface: Tunnel0/0/0
Created time    : 00:00:45
Expire time     : 01:59:15
--------------------------------------------------------------------------------
Protocol-addr   Mask  NBMA-addr      NextHop-addr    Type        Flag
--------------------------------------------------------------------------------
192.168.2.1     32    1.1.3.10       172.16.1.3      dynamic     local
--------------------------------------------------------------------------------
Tunnel interface: Tunnel0/0/0
Created time    : 00:00:45
Expire time     : 01:59:15

Number of nhrp peers: 5
```

- Hub1故障，shutdown Hub1的公网物理接口GE1/0/0，检查OSPF路由信息

  # 在Hub1上shutdown接口GE1/0/0。

  ```
  [Huawei] interface gigabitethernet 1/0/0
  [Huawei-GigabitEthernet1/0/0] shutdown
  [Huawei-GigabitEthernet1/0/0] quit
  ```

  Hub1故障之后，检查Spoke的路由表项，下一跳变成Hub2。

  # 在Spoke1上执行**display ospf 1 routing**操作，结果如下。

  ```
  [Huawei] display ospf 1 routing

          OSPF Process 1 with Router ID 172.16.1.2
                  Routing Tables

   Routing for Network
   Destination        Cost  Type       NextHop         AdvRouter       Area
   172.16.1.2/32      0     Stub       172.16.1.2      172.16.1.2      0.0.0.0
   192.168.1.1/32     0     Stub       192.168.1.1     172.16.1.2      0.0.0.0
   172.16.1.3/32      4562  Stub       172.16.1.254    172.16.1.3      0.0.0.0
   172.16.1.254/32    1562  Stub       172.16.1.254    172.16.1.254    0.0.0.0
   192.168.2.1/32     4562  Stub       172.16.1.254    172.16.1.3      0.0.0.0

   Total Nets: 5
   Intra Area: 5  Inter Area: 0  ASE: 0  NSSA: 0
  ```

  # 在Spoke2上执行**display ospf 1 routing**操作，结果如下。

  ```
  [Huawei] display ospf 1 routing

          OSPF Process 1 with Router ID 172.16.1.3
                  Routing Tables

   Routing for Network
   Destination        Cost  Type       NextHop         AdvRouter       Area
   172.16.1.3/32      0     Stub       172.16.1.3      172.16.1.3      0.0.0.0
   192.168.2.1/32     0     Stub       192.168.2.1     172.16.1.3      0.0.0.0
  ```


版权所有 © 华为技术有限公司

```
172.16.1.2/32      4562  Stub       172.16.1.254    172.16.1.2      0.0.0.0
172.16.1.254/32    1562  Stub       172.16.1.254    172.16.1.254    0.0.0.0
192.168.1.1/32     4562  Stub       172.16.1.254    172.16.1.2      0.0.0.0

Total Nets: 5
Intra Area: 5  Inter Area: 0  ASE: 0  NSSA: 0
```

- 再次执行**ping**操作，查看配置结果

  在Spoke1上ping分支Spoke2的子网地址192.168.2.1，则在Spoke1和Spoke2上可以分别看到彼此的动态NHRP peer表项。

须知

执行ping操作前，需要确认本地没有到Hub1的默认路由，确保到Hub1不可达。

在Spoke1上执行**ping -a 192.168.1.1 192.168.2.1**操作，结果如下。

```
[Huawei] ping -a 192.168.1.1 192.168.2.1
  PING 192.168.2.1: 56  data bytes, press CTRL_C to break
    Reply from 192.168.2.1: bytes=56 Sequence=1 ttl=254 time=2 ms
    Reply from 192.168.2.1: bytes=56 Sequence=2 ttl=255 time=2 ms
    Reply from 192.168.2.1: bytes=56 Sequence=3 ttl=255 time=2 ms
    Reply from 192.168.2.1: bytes=56 Sequence=4 ttl=255 time=2 ms
    Reply from 192.168.2.1: bytes=56 Sequence=5 ttl=255 time=2 ms

  --- 192.168.2.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 2/2/2 ms
```

在Spoke1上执行**display nhrp peer all**操作，结果如下。

```
[Huawei] display nhrp peer all
--------------------------------------------------------------------------------
Protocol-addr   Mask  NBMA-addr      NextHop-addr    Type        Flag
--------------------------------------------------------------------------------
172.16.1.1      32    1.1.1.10       172.16.1.1      static      hub
--------------------------------------------------------------------------------
Tunnel interface: Tunnel0/0/0
Created time    : 05:46:29
Expire time     : --
--------------------------------------------------------------------------------
Protocol-addr   Mask  NBMA-addr      NextHop-addr    Type        Flag
--------------------------------------------------------------------------------
172.16.1.254    32    1.1.254.10     172.16.1.254    static      hub
--------------------------------------------------------------------------------
Tunnel interface: Tunnel0/0/0
Created time    : 04:43:28
Expire time     : --
--------------------------------------------------------------------------------
Protocol-addr   Mask  NBMA-addr      NextHop-addr    Type        Flag
--------------------------------------------------------------------------------
192.168.2.1     32    1.1.3.10       172.16.1.3      dynamic     route network
--------------------------------------------------------------------------------
Tunnel interface: Tunnel0/0/0
Created time    : 00:00:22
Expire time     : 01:59:38
--------------------------------------------------------------------------------
Protocol-addr   Mask  NBMA-addr      NextHop-addr    Type        Flag
--------------------------------------------------------------------------------
172.16.1.3      32    1.1.3.10       172.16.1.3      dynamic     route tunnel
--------------------------------------------------------------------------------
Tunnel interface: Tunnel0/0/0
Created time    : 00:00:22
```


版权所有 © 华为技术有限公司

```
Expire time     : 01:59:38
--------------------------------------------------------------------------------
Protocol-addr   Mask  NBMA-addr       NextHop-addr    Type        Flag
--------------------------------------------------------------------------------
192.168.1.1     32    1.1.2.10        172.16.1.2      dynamic     local
--------------------------------------------------------------------------------
Tunnel interface: Tunnel0/0/0
Created time    : 00:00:22
Expire time     : 01:59:38

Number of nhrp peers: 5
```

在Spoke2上执行**display nhrp peer all**操作，结果如下。

```
[Huawei] display nhrp peer all
--------------------------------------------------------------------------------
Protocol-addr   Mask  NBMA-addr       NextHop-addr    Type        Flag
--------------------------------------------------------------------------------
172.16.1.1      32    1.1.1.10        172.16.1.1      static      hub
--------------------------------------------------------------------------------
Tunnel interface: Tunnel0/0/0
Created time    : 05:46:54
Expire time     : --
--------------------------------------------------------------------------------
Protocol-addr   Mask  NBMA-addr       NextHop-addr    Type        Flag
--------------------------------------------------------------------------------
172.16.1.254    32    1.1.254.10      172.16.1.254    static      hub
--------------------------------------------------------------------------------
Tunnel interface: Tunnel0/0/0
Created time    : 04:43:38
Expire time     : --
--------------------------------------------------------------------------------
Protocol-addr   Mask  NBMA-addr       NextHop-addr    Type        Flag
--------------------------------------------------------------------------------
192.168.1.1     32    1.1.2.10        172.16.1.2      dynamic     route network
--------------------------------------------------------------------------------
Tunnel interface: Tunnel0/0/0
Created time    : 00:00:43
Expire time     : 01:59:17
--------------------------------------------------------------------------------
Protocol-addr   Mask  NBMA-addr       NextHop-addr    Type        Flag
--------------------------------------------------------------------------------
172.16.1.2      32    1.1.2.10        172.16.1.2      dynamic     route tunnel
--------------------------------------------------------------------------------
Tunnel interface: Tunnel0/0/0
Created time    : 00:00:43
Expire time     : 01:59:17
--------------------------------------------------------------------------------
Protocol-addr   Mask  NBMA-addr       NextHop-addr    Type        Flag
--------------------------------------------------------------------------------
192.168.2.1     32    1.1.3.10        172.16.1.3      dynamic     local
--------------------------------------------------------------------------------
Tunnel interface: Tunnel0/0/0
Created time    : 00:00:43
Expire time     : 01:59:17

Number of nhrp peers: 5
```

说明

执行**ping**操作之前，需要清除Spoke上已经存在的NHRP peer表项。

----结束

配置注意事项

正常情况下，需要在Hub1和Hub2的mGRE接口上配置不同的ospf cost值，使得Spoke学习到cost值较小的路由，在进行分支间子网通信时优先选择主用Hub。如果主Hub配置的ospf cost值大于备用Hub的，分支Spoke将会优先选用备用Hub发送报文。

 版权所有 © 华为技术有限公司

FAQ

- Q：配置DSVPN时，必须保证所有设备公网路由可达吗?
  A：是的，这点是实现DSVPN功能的前提。
- Q：配置双Hub DSVPN时，主备Hub可以配置在同一个网段吗?
  A：不能。配置双Hub DSVPN，进行网络规划时，不能将主备Hub配置在同一个网段。
- Q：在主Hub状态正常时，备用Hub相当于一直处于冗余状态，算是对资源的一种浪费，是否可以将其配置成Spoke?
  A：可以。在主Hub状态正常时，备用Hub一直处于冗余状态。在企业资源有限的情况下，可以选择将其配置成Spoke，跟其他分支Spoke一样，向主Hub进行注册。在主Hub故障时，会接替主Hub角色，保证分支间相互通信。

6.4 IPSec

6.4.1 配置采用手工方式建立 IPSec 隧道示例

规格

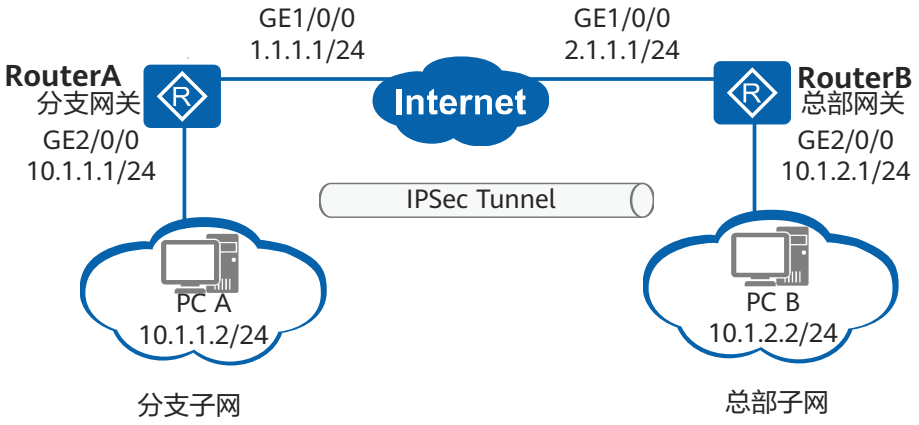
适用于所有版本、所有形态的路由器。

组网需求

如图6-34所示，RouterA为企业分支网关，RouterB为企业总部网关，分支与总部通过公网建立通信。分支子网为10.1.1.0/24，总部子网为10.1.2.0/24。

企业希望对分支子网与总部子网之间相互访问的流量进行安全保护。分支与总部通过公网建立通信，可以在分支网关与总部网关之间建立一个IPSec隧道来实施安全保护。由于维护网关较少，可以考虑采用手工方式建立IPSec隧道。

图 6-34 配置采用手工方式建立 IPSec 隧道组网图



版权所有 © 华为技术有限公司

操作步骤

步骤1 RouterA的配置

```
#
 sysname RouterA
#
acl number 3101  //配置ACL 3101，匹配从分支子网到总部子网的流量
 rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
#
ipsec proposal tran1  //配置IPSec安全提议
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-128
#
ipsec policy map1 10 manual  //配置手动方式安全策略
 security acl 3101
 proposal tran1
 tunnel local 1.1.1.1
 tunnel remote 2.1.1.1
 sa spi inbound esp 54321
 sa string-key inbound esp cipher %^%#JvZxR2g8c;a9~FPN~n'$7`DEV&=G(=Et02P/%\*!%^%#  //配置入方向SA的认证密钥为YsHsjx_202206
 sa spi outbound esp 12345
 sa string-key outbound esp cipher %^%#K{JG:rWVHPMnf;5\|,GW(Luq'qi8BT4nOj%5W5=)%^%#  //配置出方向SA的认证密钥为YsHsjx_202206
#
interface GigabitEthernet1/0/0
 ip address 1.1.1.1 255.255.255.0
 ipsec policy map1
#
interface GigabitEthernet2/0/0
 ip address 10.1.1.1 255.255.255.0
#
ip route-static 2.1.1.0 255.255.255.0 1.1.1.2  //配置一条目的地址是总部外网出口的静态路由
ip route-static 10.1.2.0 255.255.255.0 1.1.1.2  //配置一条目的地址是总部内网的静态路由
#
return
```

步骤2 RouterB的配置

```
#
 sysname RouterB
#
acl number 3101  //配置ACL 3101，匹配从总部子网到分支子网的流量
 rule 5 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
#
ipsec proposal tran1  //配置IPSec安全提议
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-128
#
ipsec policy use1 10 manual  //配置手动方式安全策略
 security acl 3101
 proposal tran1
 tunnel local 2.1.1.1
 tunnel remote 1.1.1.1
 sa spi inbound esp 12345
 sa string-key inbound esp cipher %^%#IRFGEiFPJ1$&a'Qy,L*XQL_+*Grq-=yMb}ULZdS6%^%#  //配置入方向SA的认证密钥为YsHsjx_202206
 sa spi outbound esp 54321
 sa string-key outbound esp cipher %^%#(3fr1!&6O=)!GN#~{)n,2fq>4#4+%;lMTs5(]:c)%^%#  //配置出方向SA的认证密钥为YsHsjx_202206
#
interface GigabitEthernet1/0/0
 ip address 2.1.1.1 255.255.255.0
 ipsec policy use1
#
interface GigabitEthernet2/0/0
 ip address 10.1.2.1 255.255.255.0
#
ip route-static 1.1.1.0 255.255.255.0 2.1.1.2  //配置一条目的地址是分支外网出口的静态路由
```

 版权所有 © 华为技术有限公司

```
ip route-static 10.1.1.0 255.255.255.0 2.1.1.2  //配置一条目的地址是分支内网的静态路由
#
return
```

步骤3 验证配置结果

在RouterA上执行**display ipsec sa**命令，可以查看IPSec隧道上配置的信息。

----结束

配置注意事项

- 分支的ACL需要与总部ACL互为镜像。
- 总部和分支之间的外网地址路由可达。
- 所有的IPSec策略都绑定在对应的外网出接口上。
- 总部和各个分支之间都采用相同的pre-shared-key。

6.4.2 配置设备之间通过 IKE 动态协商方式建立 IPSec 隧道的示例（不对对等体存活进行检测）

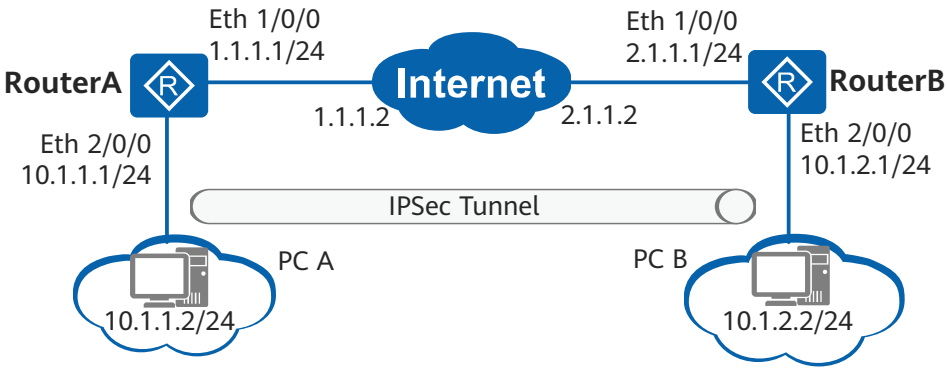
规格

适用于所有版本、所有形态的路由器。

组网需求

如图6-35所示，在RouterA和RouterB之间建立一个安全隧道，对PC A代表的子网（10.1.1.x）与PC B代表的子网（10.1.2.x）之间的数据流进行安全保护。安全协议采用ESP协议，加密算法采用DES，认证算法采用SHA1。

图 6-35 配置采用 IKE 协商方式建立安全联盟组网图



版权所有 © 华为技术有限公司

操作步骤

步骤1 配置RouterA

```
#
acl number 3101  //配置ACL
 rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
#
ipsec proposal tran1  //配置IPSec安全提议
 esp authentication-algorithm sha2-256
#
ike proposal 1  //配置IPSec IKE提议
 encryption-algorithm aes-cbc-128  //V200R008及之后的版本，aes-cbc-128参数修改为aes-128
 dh group14
 authentication-algorithm sha2-256
#
 ike local-name huawei01
#
ike peer spub v1  //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 exchange-mode aggressive
 pre-shared-key cipher %^%#JvZxR2g8c;a9~FPN~n'$7`DEV&=G(=Et02P/%\*!%^%#  //配置预共享密钥认证字为“YsHsjx_202206”，以密文显示，该命令在V2R3C00以前的版本中为“pre-shared-key YsHsjx_202206”，以明文显示
 ike-proposal 1
 local-id-type name  //配置IKE协商时本端的ID类型。V200R008及之后的版本，name参数修改为fqdn
 remote-name huawei02  //配置对端IKE peer名称。V200R008及之后的版本，设备不支持命令remote-name，其命令功能等同于命令remote-id
 local-address 1.1.1.1
 remote-address 2.1.1.1
#
ipsec policy map1 10 isakmp  //配置IPSec策略
 security acl 3101
 ike-peer spub
 proposal tran1
#
 ip route-static 10.1.2.0 255.255.255.0 1.1.1.2
 ip route-static 2.1.1.0 255.255.255.0 1.1.1.2
#
interface Ethernet1/0/0  //配置外网接口
 ip address 1.1.1.1 255.255.255.0
 ipsec policy map1
#
interface Ethernet2/0/0  //配置私网接口
 ip address 10.1.1.1 255.255.255.0
#
return
```

步骤2 配置RouterB

```
#
acl number 3101  //配置ACL
  rule 5 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
#
ipsec proposal tran1  //配置IPSec安全提议
 esp authentication-algorithm sha2-256
#
ike proposal 1  //配置IKE提议
 encryption-algorithm aes-cbc-128  //V200R008及之后的版本，aes-cbc-128参数修改为aes-128
 dh group14
 authentication-algorithm sha2-256
#
 ike local-name huawei02
#
ike peer spua v1  //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 |
```

 版权所有 © 华为技术有限公司

```
2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 exchange-mode aggressive
 pre-shared-key cipher %^%#K{JG:rWVHPMnf;5\|,GW(Luq'qi8BT4nOj%5W5=)%^%#  //配置预共享密钥认证字为“YsHsjx_202206”，以密文显示，该命令在V2R3C00以前的版本中为“pre-shared-key YsHsjx_202206”，以明文显示
 ike-proposal 1
 local-id-type name   //配置IKE协商时本端的ID类型。V200R008及之后的版本，name参数修改为fqdn
 remote-name huawei01   //配置对端IKE peer名称。V200R008及之后的版本，设备不支持命令remote-name，其命令功能等同于命令remote-id
 local-address 2.1.1.1
 remote-address 1.1.1.1
#
ipsec policy use1 10 isakmp  //配置IPSec策略
 security acl 3101
 ike-peer spua
 proposal tran1
#
 ip route-static 10.1.1.0 255.255.255.0 2.1.1.2
 ip route-static 1.1.1.0 255.255.255.0 2.1.1.2
#
interface Ethernet1/0/0  //配置外网接口
 ip address 2.1.1.1 255.255.255.0
 ipsec policy use1
#
interface Ethernet2/0/0  //配置私网接口
 ip address 10.1.2.1 255.255.255.0
#
return
```

----结束

配置注意事项

- 分支的ACL需要与总部ACL互为镜像。
- 总部和各分支之间的外网地址路由可达。

6.4.3 配置设备之间通过 IKE 动态协商方式建立 IPSec 隧道的示例（对对等体存活进行检测）

规格

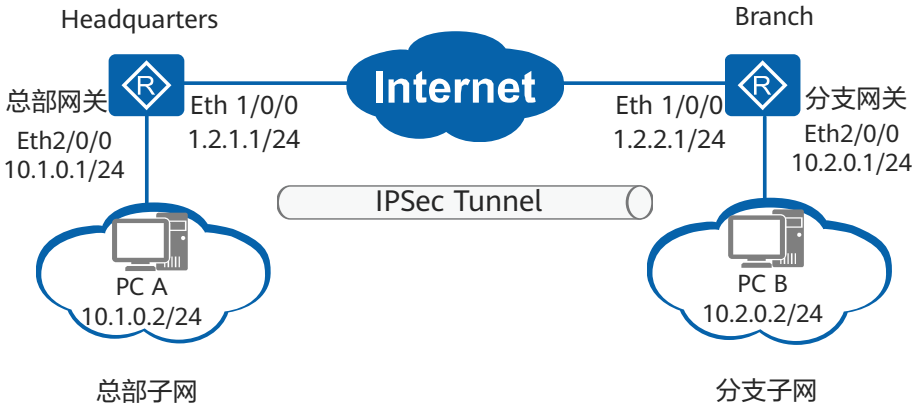
适用于所有版本、所有形态的路由器。

组网需求

Headquarters和Branch建立IPSec连接，Headquarters和Branch都配置DPD。通过配置DPD技术来检测Headquarters与Branch间IPSEC对等体的存活情况，或者Headquarters上针对该分支相应的IPSEC SA被异常删除后，Branch继续将加密数据发往Headquarters，导致Headquarters无法对这部分数据正常解密，数据通信中断。

 版权所有 © 华为技术有限公司

图 6-36 IKE DPD 功能组网图



操作步骤

步骤1 Headquarters的配置

```
#
 sysname Headquarters
#
acl number 3000  //配置ACL 3000，匹配从总部子网到分支子网的流量
 rule 0 permit ip source 10.1.0.0 0.0.0.255 destination 10.2.0.0 0.0.0.255
#
ipsec proposal def  //配置IPSec提议
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-192
#
ike proposal 5   //配置IKE提议
 encryption-algorithm aes-cbc-128   //V200R008及之后的版本，aes-cbc-128参数修改为aes-128
 dh group14
 authentication-algorithm sha2-256
#
ike peer Center v1  //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 pre-shared-key cipher %^%#JvZxR2g8c;a9~FPN~n'$7`DEV&=G(=Et02P/%\*!%^%#  //配置预共享密钥认证字为“YsHsjx_202206”，以密文显示，该命令在V2R3C00以前的版本中为“pre-shared-key YsHsjx_202206”，以明文显示
 remote-address 1.2.2.1  //配置对端IP地址
 dpd type on-demand  //配置DPD检测模式为根据需要进行检测
 ike-proposal 5
#
ipsec policy center 1 isakmp  //配置IPSec策略
 security acl 3000
 ike-peer Center
 proposal def
#
interface Ethernet1/0/0
 ip address 1.2.1.1 255.255.255.0
 ipsec policy center
#
interface Ethernet2/0/0
 ip address 10.1.0.1 255.255.255.0
#
ip route-static 1.2.2.0 255.255.255.0 1.2.1.2  //配置一条目的地址是Branch外网出口的静态路由
ip route-static 10.2.0.0 255.255.255.0 1.2.1.2  //配置一条目的地址是Branch内网的静态路由
```


版权所有 © 华为技术有限公司

```
#
return
```

步骤2 Branch的配置

```
#
 sysname Branch
#
acl number 3000  //配置ACL 3000，匹配从分支子网到总部子网的流量
 rule 0 permit ip source 10.2.0.0 0.0.0.255 destination 10.1.0.0 0.0.0.255
#
ipsec proposal def  //配置IPSec提议
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-192
#
ike proposal 5   //配置IKE提议
 encryption-algorithm aes-cbc-128   //V200R008及之后的版本，aes-cbc-128参数修改为aes-128
 dh group14
 authentication-algorithm sha2-256
#
ike peer Branch v1  //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 pre-shared-key cipher %^%#K{JG:rWVHPMnf;5\|,GW(Luq'qi8BT4nOj%5W5=)%^%#   //配置预共享密钥认证字为“YsHsjx_202206”，以密文显示，该命令在V2R3C00以前的版本中为“pre-shared-key YsHsjx_202206”，以明文显示
 remote-address 1.2.1.1  //配置对端IP地址
 dpd type on-demand  //配置DPD检测模式为根据需要进行检测
 ike-proposal 5
#
ipsec policy branch 1 isakmp  //配置IPSec策略
 security acl 3000
 ike-peer Branch
 proposal def
#
interface Ethernet1/0/0
 ip address 1.2.2.1 255.255.255.0
 ipsec policy branch
#
interface Ethernet2/0/0
 ip address 10.2.0.1 255.255.255.0
#
ip route-static 1.2.1.0 255.255.255.0 1.2.2.2  //配置一条目的地址是Headquarters外网出口的静态路由
ip route-static 10.1.0.0 255.255.255.0 1.2.2.2  //配置一条目的地址是Headquarters内网的静态路由
#
return
```

步骤3 检查配置结果

1. 在Headquarters上执行**display ike sa verbose**和**display ipsec sa**命令，可以查看IPSec隧道上配置的信息。
2. 如果Branch上的链路断掉，在Headquarters上执行Ping操作，可以看到Headquarters设备发出的DPD请求。

----结束

6.4.4 配置穿越 NAT 设备建立 IPSec 隧道的示例

规格

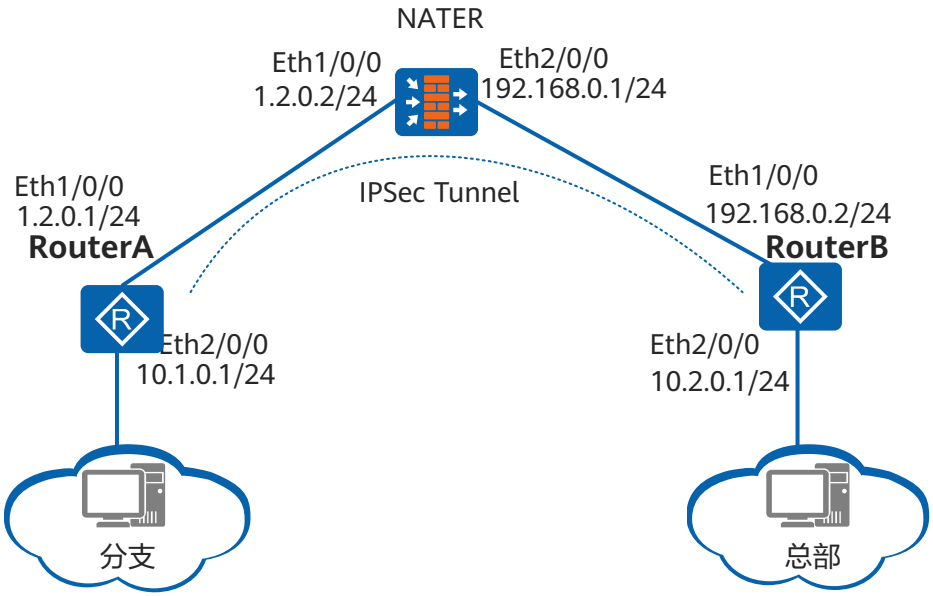
适用于所有版本、所有形态的路由器。

组网需求

当进行IPSec协商的两个对端设备之间存在NAT网关时，建立IPSec隧道的两端需要进行NAT穿越能力协商，因此两端设备都必须具备NAT穿越的能力。

如图6-37所示，分支网络出口网关RouterA、总部网络出口网关RouterB之间通过NATER进行地址转换，RouterA、RouterB之间建立支持NAT穿越的野蛮模式IPSec。

图 6-37 IPSec 穿越 NAT 功能组网图



操作步骤

步骤1 RouterA的配置

```
#
 sysname RouterA  //设置设备的主机名
#
 ike local-name RouterA  //设置IKE协商时本设备的ID
#
ipsec proposal rta  //创建一个IPSec提议
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-192
#
ike proposal 5  //配置IKE提议
 encryption-algorithm aes-cbc-128  //V200R008及之后的版本，aes-cbc-128参数修改为aes-128
 dh group14
 authentication-algorithm sha2-256
#
ike peer rta v1  //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 exchange-mode aggressive  //配置IKE的协商模式为野蛮模式
 pre-shared-key cipher %^%#JvZxR2g8c;a9~FPN~n'$7`DEV&=G(=Et02P/%\*!%^%#  //配置预共享密钥认证字为“YsHsjx_202206”，以密文显示，该命令在V2R3C00以前的版本中为“pre-shared-key YsHsjx_202206”，以明文显示
 ike-proposal 5
 local-id-type name  //配置IKE协商时本端的ID类型。V200R008及之后的版本，name参数修改为fqdn
```


版权所有 © 华为技术有限公司

```
 remote-name RouterB  //配置对端IKE peer名称,//配置对端IKE peer名称。V200R008及之后的版本，设备不支持命令remote-name，其命令功能等同于命令remote-id
 nat traversal  //使能NAT穿越功能。V200R008版本，设备默认使能NAT穿越功能，不支持配置此命令；但V200R008之后版本，支持配置此命令
#
ipsec policy-template rta_temp 1  //建一个安全策略模板
 ike-peer rta
 proposal rta
#
ipsec policy rta 1 isakmp template rta_temp  //指定采用策略模板创建安全联盟
#
interface Ethernet1/0/0
 ip address 1.2.0.1 255.255.255.0
 ipsec policy rta
#
interface Ethernet2/0/0
 ip address 10.1.0.1 255.255.255.0
#
ip route-static 10.2.0.0 255.255.255.0 1.2.0.2  //配置到10.2.0.0网段的静态路由
#
return
```

步骤2 RouterB的配置

```
#
 sysname RouterB  //设置设备的主机名
#
 ike local-name RouterB  //设置IKE协商时本设备的ID
#
acl number 3000  //配置ACL
 rule 0 permit ip source 10.2.0.0 0.255.255.255 destination 10.1.0.0 0.255.255.255
#
ipsec proposal rtb  //创建一个IPSec提议
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-192
#
ike proposal 5  //配置IKE提议
 encryption-algorithm aes-cbc-128  //V200R008及之后的版本，aes-cbc-128参数修改为aes-128
 dh group14
 authentication-algorithm sha2-256
#
ike peer rtb v1  //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 exchange-mode aggressive  //配置IKE的协商模式为野蛮模式
 pre-shared-key cipher %^%#K{JG:rWVHPMnf;5\|,GW(Luq'qi8BT4nOj%5W5=)%^%#  //配置预共享密钥认证字为“YsHsjx_202206”，以密文显示，该命令在V2R3C00以前的版本中为“pre-shared-key YsHsjx_202206”，以明文显示
 ike-proposal 5
 local-id-type name  //配置IKE协商时本端的ID类型。V200R008及之后的版本，name参数修改为fqdn
 remote-name RouterA  //配置对端IKE peer名称。V200R008及之后的版本，设备不支持命令remote-name，其命令功能等同于命令remote-id
 remote-address 1.2.0.1  //配置对端IKE peer地址
 nat traversal  //使能NAT穿越功能。V200R008版本，设备默认使能NAT穿越功能，不支持配置此命令；但V200R008之后版本，支持配置此命令
#
ipsec policy rtb 1 isakmp  //配置IPSec策略
 security acl 3000
 ike-peer rtb
 proposal rtb
#
interface Ethernet1/0/0
 ip address 192.168.0.2 255.255.255.0
 ipsec policy rtb
#
interface Ethernet2/0/0
 ip address 10.2.0.1 255.255.255.0
```

 版权所有 © 华为技术有限公司

```
#
ip route-static 0.0.0.0 0.0.0.0 192.168.0.1  //配置静态路由
#
return
```

步骤3 NATER的配置

```
#
 sysname NATER  //设置设备的主机名
#
acl number 3000  //配置ACL
 rule 0 permit ip source 192.168.0.0 0.0.0.255 destination 1.2.0.0 0.0.0.255
#
interface Ethernet1/0/0
 ip address 1.2.0.2 255.255.255.0
 nat outbound 3000  //接口下配置nat outbound
#
interface Ethernet2/0/0
 ip address 192.168.0.1 255.255.255.0
#
return
```

步骤4 验证配置结果

通过Ping触发建立IPSec会话，在RouterA上执行**display ike sa verbose**和**display ipsec sa**命令，可以查看IPSec隧道上配置的信息。

----结束

配置注意事项

- 配置NATER，保证RouterA和RouterB经过NATER可以互通。
- RouterA作为IPSec协商的响应方，需要使用安全策略模板方式。
- RouterA和RouterB都需要使能NAT穿越功能。

6.4.5 配置分支机构与总部利用 IPSec 隧道实现总部多个访问资源独立保护的示例

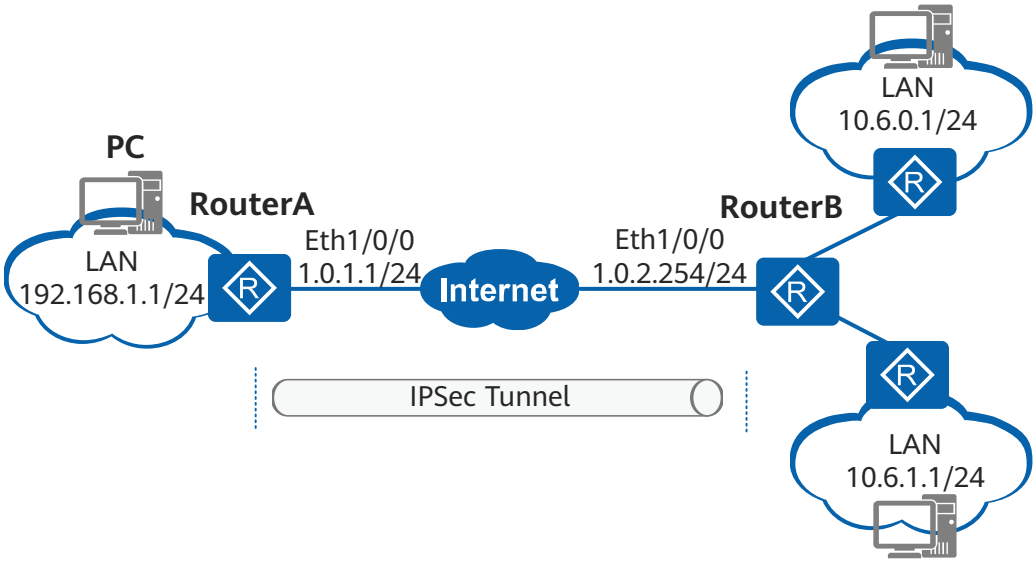
规格

适用于所有版本、所有形态的路由器。

组网需求

如图6-38所示，总部内部有多个网段，要求分支内网访问总部不同网段时使用独立的加密密钥。

图 6-38 IPSec 多网段独立保护功能的配置组网图



操作步骤

步骤1 配置RouterA

```
#
 sysname RouterA
#
acl number 3000  //配置ACL 3000，匹配从192.168.1.0/24到10.6.0.0/24的流量
 rule 0 permit ip source 192.168.1.0 0.0.0.255 destination 10.6.0.0 0.0.0.255
#
acl number 3001  //配置ACL 3001，匹配从192.168.1.0/24到的流量10.6.1.0/24
 rule 0 permit ip source 192.168.1.0 0.0.0.255 destination 10.6.1.0 0.0.0.255
#
ipsec proposal default  //配置IPSec提议
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-192
#
ike proposal 5   //配置IKE提议
 encryption-algorithm aes-cbc-128   //V200R008及之后的版本，aes-cbc-128参数修改为aes-128
 dh group14
 authentication-algorithm sha2-256
#
ike peer center1 v1  //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 pre-shared-key cipher %^%#pf$s.~E0h*hws%-7cwv&ItP3Bfw7DN`{)~~Sh'H'%^%# //配置预共享密钥认证字为“YsHsjx_202206”，以密文显示，该命令在V2R3C00以前的版本中为“pre-shared-key YsHsjx_202206”，以明文显示
 ike-proposal 5
 local-address 1.0.1.1
 remote-address 1.0.2.254
#
ike peer center2 v1  //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
```


版权所有 © 华为技术有限公司

```
 pre-shared-key cipher %^%#19+-M|4}f2,%g3/9IT#C46mnQm+@3;,Eh^"3>eVI%^%# //配置预共享密钥认证字为“YsHsjx_202206”，以密文显示，该命令在V2R3C00以前的版本中为“pre-shared-key YsHsjx_202206”，以明文显示
 ike-proposal 5
 local-address 1.0.1.1
 remote-address 1.0.2.254
#
ipsec policy center 10 isakmp  //建立IPSec策略center，序号10，用于保护分支与10.6.0.0/24的流量
 security acl 3000
 ike-peer center1
 proposal default
#
ipsec policy center 20 isakmp  //建立IPSec策略center，序号20，用于保护分支与10.6.1.0/24的流量
 security acl 3001
 ike-peer center2
 proposal default
#
interface Ethernet1/0/0  //配置分支外网出口
 ip address 1.0.1.1255.255.255.0
 ipsec policy center  //绑定IPSec策略
#
interface GigabitEthernet0/0/1  //配置分支内网接口
 ip address 192.168.1.1 255.255.255.0
#
ip route-static 10.0.0.0 255.0.0.0 1.0.1.2  //配置一条目的地址是总部内网的静态路由
#
return
```

步骤2 配置RouterB

```
#
 sysname RouterB
#
acl number 3000  //配置ACL 3000，匹配从10.6.0.0/24到192.168.1.0/24的流量
 rule 0 permit ip source 10.6.0.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
#
acl number 3001  //配置ACL 3001，匹配从10.6.1.0/24到192.168.1.0/24的流量
 rule 0 permit ip source 10.6.1.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
#
ipsec proposal default  //配置IPSec提议
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-192
#
ike proposal 5   //配置IKE提议
 encryption-algorithm aes-cbc-128   //V200R008及之后的版本，aes-cbc-128参数修改为aes-128
 dh group14
 authentication-algorithm sha2-256
#
ike peer branch1 v1  //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 pre-shared-key cipher %^%#&,/=<KeGs@/vTKYku>`HM:$CU,_!P<Ijhb~*U[PU%^%#  //配置预共享密钥认证字为“YsHsjx_202206”，以密文显示，该命令在V2R3C00以前的版本中为“pre-shared-key YsHsjx_202206”，以明文显示
 ike-proposal 5
 local-address 1.0.2.254
 remote-address 1.0.1.1
#
ike peer branch2 v1      //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 pre-shared-key cipher %^%#e6'U*sl_&<I-qIL>}zr9W-r8(RR:#A*{4WC~j2|W%^%#  //配置预共享密钥认证字为“YsHsjx_202206”，以密文显示，该命令在V2R3C00以前的版本中为“pre-shared-key YsHsjx_202206”，以明文显示
```

```
 ike-proposal 5
 local-address 1.0.2.254
 remote-address 1.0.1.1
#
ipsec policy branch 10 isakmp  //配置IPSec策略branch，序号10，用于保护分支与10.6.0.0/24的流量
 security acl 3000
 ike-peer branch1
 proposal default
#
ipsec policy branch 20 isakmp  //配置IPSec策略branch，序号20，用于保护分支与10.6.1.0/24的流量
 security acl 3001
 ike-peer branch2
 proposal default
#
interface Ethernet1/0/0  //配置总部外网出口
 ip address 1.0.2.254 255.255.255.0
 ipsec policy branch  //配置IPSec策略
#
interface GigabitEthernet0/0/1  //配置公司总部内网接口1
 ip address 10.6.0.1 255.255.255.0
#
interface GigabitEthernet0/0/2
 ip address 10.6.1.1 255.255.255.0  //配置公司总部内网接口2
#
ip route-static 192.168.1.0 255.255.255.0 1.0.2.2  //配置一条目的地址为分支内网的静态路由
#
return
```

步骤3 验证配置结果

在设备上执行命令**display ike sa**可以查看到安全联盟的相关信息。

配置完后两侧用户可以实现数据加密互访。

----结束

配置注意事项

- 分支的ACL需要与总部ACL互为镜像。
- 两端路由器都需要配置多序号安全策略。
- 所有的IPSec策略都绑定在对应的外网出接口上。
- 必须保证总部和分支出接口能互通。

6.4.6 配置远程拨号用户通过 IPSec 隧道接入总部的示例

规格

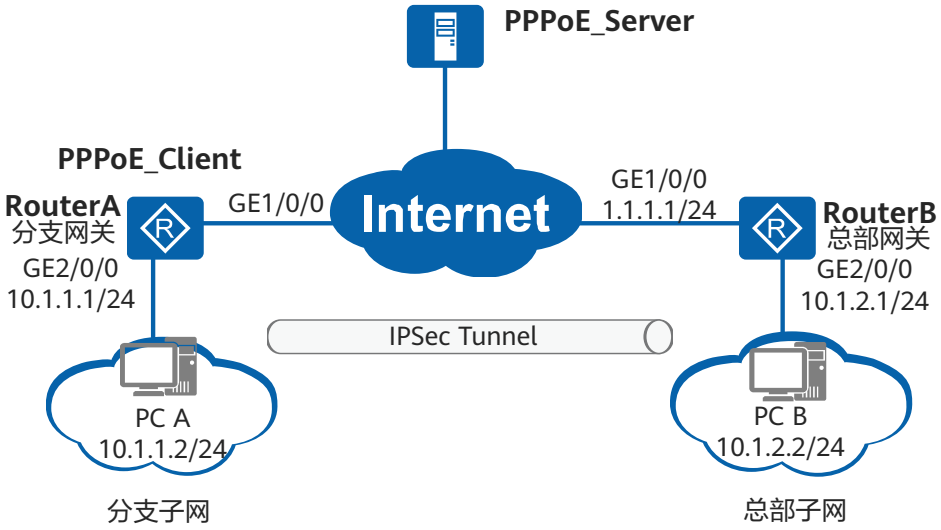
适用于所有版本、所有形态的路由器。

组网需求

某企业由于业务拓展，在各地建立了若干分支机构，分支网关通过PPPoE方式接入公网。如图6-39所示，RouterA为企业分支网关，RouterB为企业总部网关，分支与总部通过公网建立通信。分支机构在业务开展过程中需要访问位于总部的业务服务器，同时需要对分支与总部间通信的数据进行加密，保证业务安全。

 版权所有 © 华为技术有限公司

图 6-39 采用拨号接口上配置 IPSec 功能组网图



说明

如果分支网关和总部网关都通过PPPoE方式接入公网，则分支网关和总部网关必须执行命令**remote-address** *host-name*指定域名进行IPSec协商，否则IPSec隧道无法建立。

操作步骤

步骤1 配置RouterA

```
#
 sysname RouterA
#
acl number 3003   //配置ACL 3003，匹配从分支到总部的流量
 rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
#
ipsec proposal prop1   //配置IPSec提议
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-128
#
ike proposal 5   //配置IKE提议
 encryption-algorithm aes-cbc-128   //V200R008及之后的版本，aes-cbc-128参数修改为aes-128
 dh group14
 authentication-algorithm sha2-256
#
ike peer rut1 v1   //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 pre-shared-key cipher %^%#JvZxR2g8c;a9~FPN~n'$7`DEV&=G(=Et02P/%\*!%^%#   //配置预共享密钥认证字为“YsHsjx_202206”，以密文显示，该命令在V2R3C00以前的版本中为“pre-shared-key YsHsjx_202206”，以明文显示
 ike-proposal 5
 remote-address 1.1.1.1
#
ipsec policy policy1 10 isakmp   //配置IPSec策略
 security acl 3003
 ike-peer rut1
```


版权所有 © 华为技术有限公司

```
 proposal prop1
#
interface Dialer1   //配置拨号口
 link-protocol ppp
 ppp chap user user@huawei.com   //配置CHAP认证
 ppp chap password cipher %@%@^_PfANXK0(,Jr-(3p]"R,eOL%@%@   //配置CHAP验证的口令为
“YsHsjx_202206”
 ip address ppp-negotiate
 dialer user huawei   //配置Dialer接口对应的对端用户名
 dialer bundle 1   //配置所属的拨号绑定组
 dialer-group 1   //配置所属的拨号访问控制列表
 ipsec policy policy1   //绑定IPSec策略
#
interface GigabitEthernet1/0/0
 pppoe-client dial-bundle-number 1   //配置PPPoe_Client使用绑定组1
#
interface GigabitEthernet2/0/0
 ip address 10.1.1.1 255.255.255.0   //配置内部网络接口
#
dialer-rule   //配置拨号访问控制列表
 dialer-rule 1 ip permit
#
ip route-static 0.0.0.0 0.0.0.0 dialer1   //配置默认路由指向拨号口
#
return
```

步骤2 配置RouterB

```
#
 sysname RouterB
#
ipsec proposal prop1   //配置IPSec提议
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-128
#
ike proposal 5   //配置IKE提议
 encryption-algorithm aes-cbc-128   //V200R008及之后的版本，aes-cbc-128参数修改为aes-128
 dh group14
 authentication-algorithm sha2-256
#
ike peer rut1 v1   //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 pre-shared-key cipher %^%#K{JG:rWVHPMnf;5\|,GW(Luq'qi8BT4nOj%5W5=)%^%#   //配置预共享密钥认证字为“YsHsjx_202206”，以密文显示，该命令在V2R3C00以前的版本中为“pre-shared-key YsHsjx_202206”，以明文显示
 ike-proposal 5
#
ipsec policy-template temp1   //配置IPSec策略模板
 ike-peer rut1
 proposal prop1
#
ipsec policy policy1 10 isakmp template temp1   //配置IPSec策略，引入策略模板

#
interface GigabitEthernet1/0/0   //配置公网接口
 ip address 1.1.1.1 255.255.255.0
 ipsec policy policy1
#
interface GigabitEthernet2/0/0   //配置内部网络接口
 ip address 10.1.2.1 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 1.1.1.254   //配置访问对端内网的静态路由
#
return
```

步骤3 验证配置结果

 版权所有 © 华为技术有限公司

在设备上执行命令**display ike sa**和**display ipsec sa**，可以查看IPSec隧道上配置的信息。

----结束

配置注意事项

- IKE发起方PPPoE_Client必须指定接收方PPPoE_Server的地址。
- PPPoE客户端使用IPSec策略指定IKE对端地址，PPPoE服务端通过绑定IPSec策略模板到IPSec，不需要指定IKE对端地址。

6.4.7 配置设备之间建立 IPSec 隧道时需要通过 PKI 方式的身份认证的示例

规格

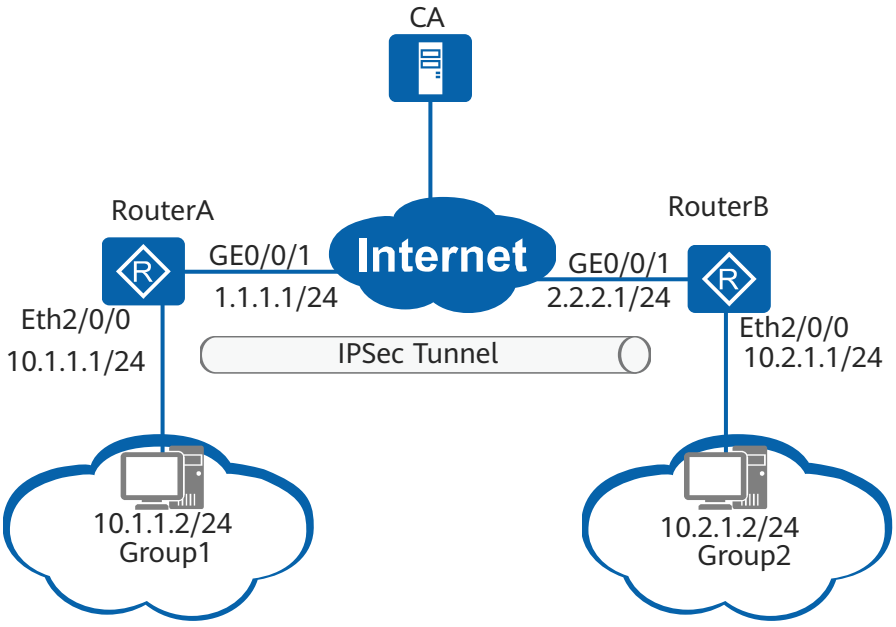
适用于V200R002C00及更高版本、所有形态的AR路由器。

组网需求

如图6-40所示，两个子网通过各自的网关设备与外部网络互联，希望通过IPsec隧道建立数据流的安全通道，具体需求如下：

- 在网关设备之间建立一个IPsec安全隧道，对子网Group1（10.1.1.0/24）与子网Group2（10.2.1.0/24）之间的数据流进行安全保护。
- 在网关设备之间使用IKE自动协商建立安全通道，IKE自动协商采用基于PKI证书的身份认证方式。

图 6-40 配置 IPSec 应用 PKI 的组网图



版权所有 © 华为技术有限公司

表 6-1 RouterA 数据规划表

配置项	数据
PKI实体	PKI实体名：routera ● 实体通用名：helloa ● 国家代码：CN ● 所在的州或者省：jiangsu ● 所在的组织：huawei ● 所在的组织部门：info
PKI域名	PKI域名：testa ● 信任的CA：ca_root ● 注册证书的URL：http://10.137.145.158:8080/certsrv/mscep/mscep.dll ● 绑定的实体:routera ● CA的指纹：采用安全散列算法2 指纹值：17A34D94624B1C1BCBF6D763C4A67035D17A34D94624B1C1BCBF6D763C4A67035D
IKE安全提议	● 加密算法：AES-CBC-128 ● 认证模式：rsa-signature ● 认证算法：AES-XCBC-MAC-96
IKE Peer	● IKE Peer名：routera ● 本地Peer的ID类型：IP ● 本端地址：1.1.1.1 ● 远端地址：2.2.2.1 ● 协商模式：主模式
IPSec安全提议	● 传输协议：ESP ● 认证算法：SHA2-256 ● 加密算法：AES-128 ● 封装模式：隧道模式
IPSec安全策略	SA触发模式：自动

版权所有 © 华为技术有限公司

表 6-2 RouterB 数据规划表

配置项	数据
PKI实体	PKI实体名：routerb ● 实体通用名：hellob ● 国家代码：CN ● 所在的州或者省：jiangsu ● 所在的组织：huawei ● 所在的组织部门：marketing
PKI域名	PKI域名：testb ● 信任的CA：ca_root ● 注册证书的URL：http://10.137.145.158:8080/certsrv/mscep/mscep.dll ● 绑定的实体:routerb ● CA的指纹：采用安全散列算法2 指纹值：17A34D94624B1C1BCBF6D763C4A67035D17A34D94624B1C1BCBF6D763C4A67035D
IKE安全提议	● 加密算法：AES-CBC-128 ● 认证模式：rsa-signature ● 认证算法：AES-XCBC-MAC-96
IKE Peer	● IKE Peer名：routerb ● 协商模式：主模式 ● 本地Peer的ID类型：IP ● 本端地址：2.2.2.1 ● 远端地址：1.1.1.1
IPSec安全提议	● 传输协议：esp ● 认证算法：sha2-256 ● 加密算法：aes-128 ● 封装模式：隧道模式
IPSec安全策略	SA触发模式：自动

操作步骤

步骤1 配置RouterA

```
#
router id 10.1.1.1
#
pki entity routera  //配置PKI实体
 country CN
 state jiangsu
 organization huawei
```


版权所有 © 华为技术有限公司

```
 organization-unit info
 common-name helloa
#
pki realm testa    //配置PKI域
 ca id ca_root
 enrollment-url http://10.137.145.158:8080/certsrv/mscep/mscep.dll ra
 entity routera
 fingerprint sha2 7a34d94624b1c1bcbf6d763c4a67035d7a34d94624b1c1bcbf6d763c4a67035d
 certificate-check none
 rsa local-key-pair rsa_scep   //配置使用SCEP方式申请证书时使用的RSA密钥对，该密钥对由pki rsa local-key-pair create命令提前创建。该命令适用于V200R008及之后的版本
 password cipher %$%$\1HN-bn(k;^|O85OAtYF3(M4%$%$   //配置SCEP证书申请时使用的挑战密码为6AE73F21E6D3571D，该命令适用于V200R008及之后的版本
 auto-enroll 60 regenerate  //开启证书自动注册和更新功能，该命令适用于V200R008及之后的版本
#
acl number 3000  //配置ACL，定义受保护的数据流
 rule 15 permit ip source 10.1.1.0 0.0.0.255 destination 10.2.1.0 0.0.0.255
#
ipsec proposal routera  //配置IPSec提议
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-128
#
ike proposal 1  //配置IKE，使用数字签名进行身份认证。
 encryption-algorithm aes-cbc-128   //V200R008及之后的版本，aes-cbc-128参数修改为aes-128
 dh group14
 authentication-algorithm aes-xcbc-mac-96
 authentication-method rsa-signature
#
ike peer routera v2   //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 ike-proposal 1
 local-address 1.1.1.1
 remote-address 2.2.2.1
 pki realm testa
#
ipsec policy routera 1 isakmp  //配置IPSec策略
 security acl 3000
 ike-peer routera
 proposal routera
#
interface Ethernet2/0/0  //配置外网接口
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1  //配置内网接口
 ip address 1.1.1.1 255.255.255.0
 ipsec policy routera
#
ospf 1
 area 0.0.0.0
  network 1.1.1.0 0.0.0.255
  network 10.1.1.0 0.0.0.255
#
return
```

步骤2 配置RouterB

```
#
router id 10.2.1.1
#
pki entity routerb  //配置PKI实体
 country CN
 state jiangsu
 organization huawei
 organization-unit marketing
 common-name hellob
#
```

```
pki realm testb  //配置PKI域
 ca id ca_root
 enrollment-url http://10.137.145.158:8080/certsrv/mscep/mscep.dll ra
 entity routerb
 fingerprint sha2 7a34d94624b1c1bcbf6d763c4a67035d7a34d94624b1c1bcbf6d763c4a67035d
 certificate-check none
 rsa local-key-pair rsa_scep   //配置使用SCEP方式申请证书时使用的RSA密钥对，该密钥对由pki rsa local-key-pair create命令提前创建。该命令适用于V200R008及之后的版本
 password cipher %$%$\1HN-bn(k;^|O85OAtYF3(M4%$%$   //配置SCEP证书申请时使用的挑战密码为6AE73F21E6D3571D，该命令适用于V200R008及之后的版本
 auto-enroll 60 regenerate  //开启证书自动注册和更新功能，该命令适用于V200R008及之后的版本
# //配置ACL，定义受保护的数据流
acl number 3000
 rule 10 permit ip source 10.2.1.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
#
ipsec proposal routerb  //配置IPSec提议
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-128
#
ike proposal 1  //配置IKE，使用数字签名进行身份认证。
 encryption-algorithm aes-cbc-128   //V200R008及之后的版本，aes-cbc-128参数修改为aes-128
 dh group14
 authentication-algorithm aes-xcbc-mac-96
 authentication-method rsa-signature
#
ike peer routerb v2  //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 ike-proposal 1
 local-address 2.2.2.1
 remote-address 1.1.1.1
 pki realm testb
#
ipsec policy routerb 1 isakmp  //配置IPSec策略
 security acl 3000
 ike-peer routerb
 proposal routerb
#
interface Ethernet2/0/0    //配置外网接口
 ip address 10.2.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1  //配置内网接口
 ip address 2.2.2.1 255.255.255.0
 ipsec policy routerb
#
ospf 1
 area 0.0.0.0
  network 2.2.2.0 0.0.0.255
  network 10.2.1.0 0.0.0.255
#
return
```

----结束

配置注意事项

- IKE协商的时候，如果RouterA和RouterB还未获得CA证书和本地证书，则会出现IKE初次协商失败的情况。
- 分支的ACL需要与总部ACL互为镜像。

 版权所有 © 华为技术有限公司

6.4.8 配置总部部署 VRRP 的场景下，分支机构利用 VRRP 虚地址与总部建立 IPSec 隧道的示例

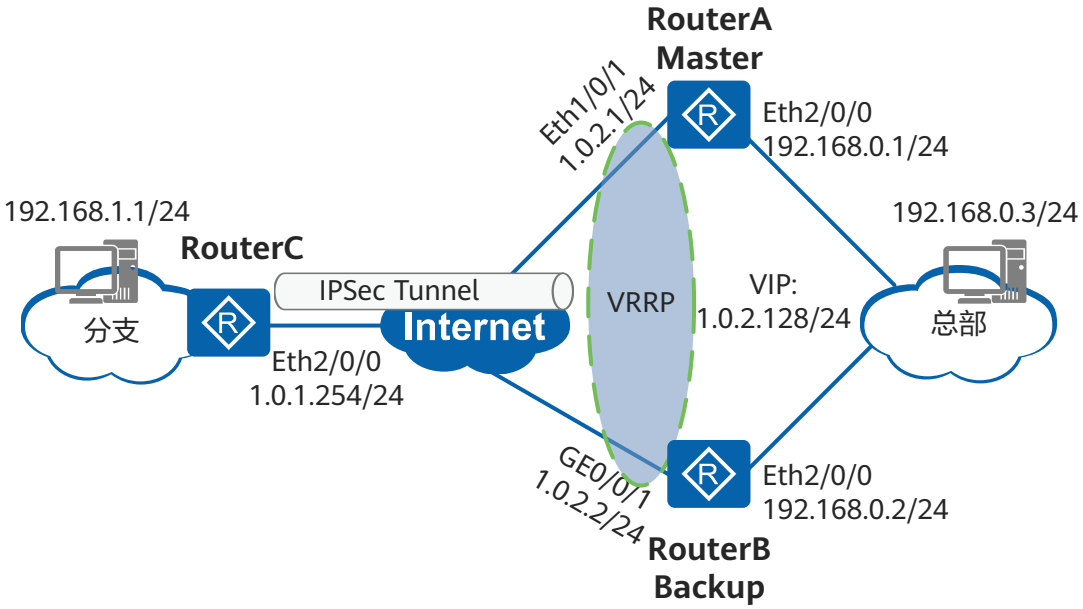
规格

适用于所有版本、所有形态的路由器。

组网需求

如图6-41所示，RouterA、RouterB、RouterC都连接在一台交换机上，RouterA和RouterB组VRRP，虚地址是1.0.2.128，RouterA作为VRRP Master，RouterB作为Backup，RouterC和VRRP虚地址之间建立基于IKE的IPSec。

图 6-41 VRRP 虚地址建立 IPSec 功能的配置组网图



操作步骤

步骤1 配置RouterA

```
#
 sysname RouterA
#
acl number 3000  //ACL配置
 rule 0 permit ip source 192.168.0.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
#
ipsec proposal def  //IPSec提议配置
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-192
#
ike proposal 5   //配置IKE提议
 encryption-algorithm aes-cbc-128   //V200R008及之后的版本，aes-cbc-128参数修改为aes-128
 dh group14
 authentication-algorithm sha2-256
#
```


版权所有 © 华为技术有限公司

```
ike peer branch v1  //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 pre-shared-key cipher %^%#JvZxR2g8c;a9~FPN~n'$7`DEV&=G(=Et02P/%\*!%^%#  //配置预共享密钥认证字为“YsHsjx_202206”，以密文显示，该命令在V2R3C00以前的版本中为“pre-shared-key YsHsjx_202206”，以明文显示
 ike-proposal 5
 local-address 1.0.2.128
 remote-address 1.0.1.254
#
ipsec policy branch 1 isakmp  //IPSec策略配置
 security acl 3000
 ike-peer branch
 proposal def
#
interface Ethernet1/0/1  //对接接口
 ip address 1.0.2.1 255.255.255.0
 vrrp vrid 1 virtual-ip 1.0.2.128  //配置VRRP组1的虚地址1.0.2.128，使用默认优先级
 ipsec policy branch  //绑定IPSec策略
#
interface GigabitEthernet0/0/1  //内网接口
 ip address 192.168.0.1 255.255.255.0
#
ip route-static 1.0.1.0 255.255.255.0 1.0.2.3    //配置到分支网关的静态路由
ip route-static 192.168.1.0 255.255.255.0 1.0.2.3 //配置到分支网络的静态路由
#
return
```

步骤2 配置RouterB

```
#
 sysname RouterB
#
acl number 3000  //ACL配置
 rule 0 permit ip source 192.168.0.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
#
ipsec proposal def  //IPSec提议配置
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-192
#
ike proposal 5  //配置IKE提议
 encryption-algorithm aes-cbc-128  //V200R008及之后的版本，aes-cbc-128参数修改为aes-128
 dh group14
 authentication-algorithm sha2-256
#
ike peer branch v1  //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 pre-shared-key cipher %^%#K{JG:rWVHPMnf;5\|,GW(Luq'qi8BT4nOj%5W5=)%^%#  //配置预共享密钥认证字为“YsHsjx_202206”，以密文显示，该命令在V2R3C00以前的版本中为“pre-shared-key YsHsjx_202206”，以明文显示
 ike-proposal 5
 local-address 1.0.2.128
 remote-address 1.0.1.254
#
ipsec policy branch 1 isakmp  //IPSec策略配置
 security acl 3000
 ike-peer branch
 proposal def
#
interface Ethernet2/0/0  //内网接口
 ip address 192.168.0.2 255.255.255.0
#
```

 版权所有 © 华为技术有限公司

```
interface GigabitEthernet0/0/1  //对接接口
 ip address 1.0.2.2 255.255.255.0
 vrrp vrid 1 virtual-ip 1.0.2.128  //配置VRRP组1的虚地址1.0.2.128
 vrrp vrid 1 priority 80  //配置VRRP组1的优先级为80，使RouterB成为
Backup
 ipsec policy branch  //绑定IPSec策略
#
ip route-static 1.0.1.0 255.255.255.0 1.0.2.4      //配置到分支网关的静态路由
ip route-static 192.168.1.0 255.255.255.0 1.0.2.4  //配置到分支网络的静态路由
#
return
```

步骤3 配置RouterC

```
#
 sysname RouterC
#
acl number 3000  //ACL配置
 rule 0 permit ip source 192.168.1.0 0.0.0.255 destination 192.168.0.0 0.0.0.255
#
ipsec proposal def  //IPSec提议配置
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-192
#
ike proposal 5   //配置IKE提议
 encryption-algorithm aes-cbc-128   //V200R008及之后的版本，aes-cbc-128参数修改为aes-128
 dh group14
 authentication-algorithm sha2-256
#
ike peer center v1  //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 pre-shared-key cipher %^%#IRFGEiFPJ1$&a'Qy,L*XQL_+*Grq-=yMb}ULZdS6%^%#  //配置预共享密钥认证字为“YsHsjx_202206”，以密文显示，该命令在V2R3C00以前的版本中为“pre-shared-key YsHsjx_202206”，以明文显示
 ike-proposal 5
 local-address 1.0.1.254
 remote-address 1.0.2.128
#
ipsec policy center 1 isakmp  //IPSec策略配置
 security acl 3000
 ike-peer center
 proposal def
#
interface Ethernet2/0/0  //对接接口
 ip address 1.0.1.254 255.255.255.0
 ipsec policy center  //绑定IPSec策略
#
interface GigabitEthernet0/0/1  //内网接口
 ip address 192.168.1.1 255.255.255.0
#
ip route-static 1.0.2.0 255.255.255.0 1.0.1.2       //配置到总部网关的静态路由
ip route-static 192.168.0.0 255.255.255.0 1.0.2.128  //配置到总部网络的静态路由
#
return
```

步骤4 验证配置结果

在RouterA、RouterB或者RouterC上执行命令**display ike sa**可以查看到安全联盟的相关信息。

在RouterA或者RouterB上执行命令**display vrrp**命令，可以看到VRRP的相关状态信息。

分部可以ping通VRRP虚拟网关。

----结束

 版权所有 © 华为技术有限公司

配置注意事项

- 分支的ACL需要与总部ACL互为镜像。

6.4.9 配置总部采用 IPSec 策略模板与分支建立多条 IPSec 隧道的示例

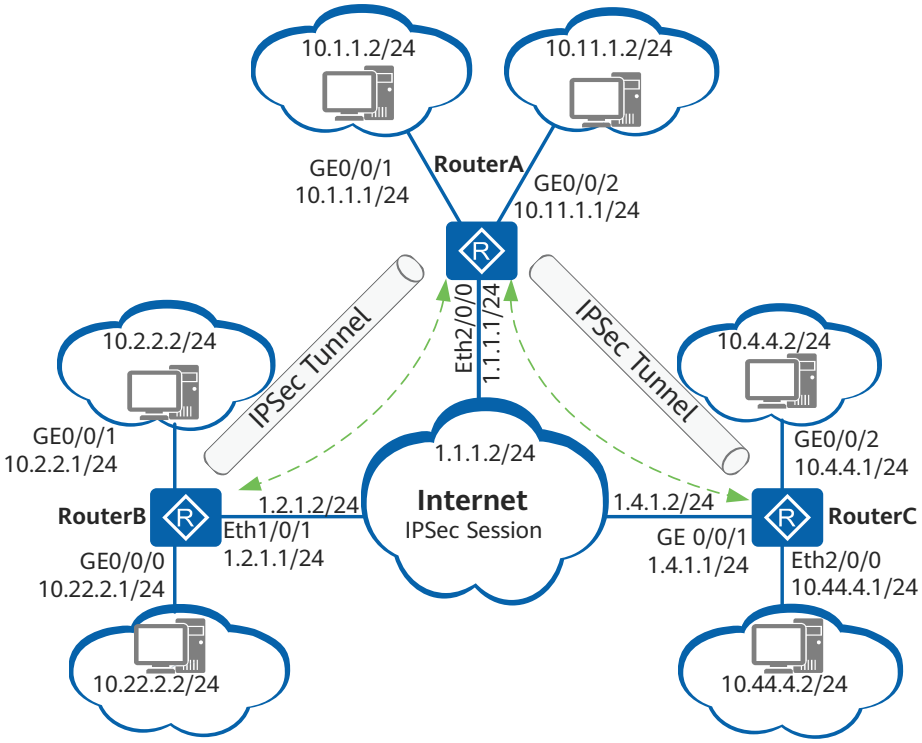
规格

适用于所有版本、所有形态的路由器。

组网需求

如图6-42所示，RouterA为总部网关，RouterB和RouterC为分支网关。分支连接有多个私网网络，需要和总部建立安全的通信连接。在RouterA上部署IPSec策略模板，配置一个IPSec策略引用策略模板，就可以接入各分支发起的IPSec协商，完成多条IPSec隧道的建立。

图 6-42 配置中心单 IKE Peer、单 IPSec 策略及序号、多分支功能组网图



操作步骤

步骤1 配置RouterA

```
#
 sysname RouterA
#
ipsec proposal def
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-192
```


版权所有 © 华为技术有限公司

```
#
ike proposal 5  //配置IKE提议
 encryption-algorithm aes-cbc-128  //V200R008及之后的版本，aes-cbc-128参数修改为aes-128
 dh group14
 authentication-algorithm sha2-256
#
ike peer branch v1  //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 pre-shared-key cipher %^%#JvZxR2g8c;a9~FPN~n'$7`DEV&=G(=Et02P/%\*!%^%#  //配置预共享密钥认证字为“YsHsjx_202206”，以密文显示，该命令在V2R3C00以前的版本中为“pre-shared-key YsHsjx_202206”，以明文显示
 ike-proposal 5
 local-address 1.1.1.1
#
ipsec policy-template branch 1  //配置IPSec策略模板
 ike-peer branch
 proposal def
#
ipsec policy hk 1 isakmp template branch  //配置IPSec策略
#
interface Ethernet2/0/0  //配置互联接口，用于建立IKE连接和隧道封装外层IP地址
 ip address 1.1.1.1 255.255.255.0
 ipsec policy hk  //配置接口下绑定IPSec策略
#
interface GigabitEthernet0/0/1
 ip address 10.1.1.1 255.255.255.0  //配置连接业务网段的接口1
#
interface GigabitEthernet0/0/2
 ip address 10.11.1.1 255.255.255.0  //配置连接业务网段的接口2
#
ip route-static 0.0.0.0 0.0.0.0 1.1.1.2  //配置静态路由
#
return
```

步骤2 配置RouterB

```
#
 sysname RouterB
#
acl number 3000  //配置ACL 3000，定义了两条数据流
 rule 0 permit ip source 10.2.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
 rule 5 permit ip source 10.22.2.0 0.0.0.255 destination 10.11.1.0 0.0.0.255
#
ipsec proposal def
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-192
#
ike proposal 5  //配置IKE提议
 encryption-algorithm aes-cbc-128  //V200R008及之后的版本，aes-cbc-128参数修改为aes-128
 dh group14
 authentication-algorithm sha2-256
#
ike peer center v1  //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 pre-shared-key cipher %^%#K{JG:rWVHPMnf;5\|,GW(Luq'qi8BT4nOj%5W5=)%^%#  //配置预共享密钥认证字为“YsHsjx_202206”，以密文显示，该命令在V2R3C00以前的版本中为“pre-shared-key YsHsjx_202206”，以明文显示
 ike-proposal 5
 local-address 1.2.1.1
 remote-address 1.1.1.1
#
ipsec policy hk 1 isakmp  //配置IPSec策略
```

 版权所有 © 华为技术有限公司

```
 security acl 3000
 ike-peer center
 proposal def
#
interface Ethernet1/0/1  //配置互联网接口，用于建立IKE和IPSec隧道外层封装IP地址
 ip address 1.2.1.1 255.255.255.0
 ipsec policy hk
#
interface GigabitEthernet0/0/0
 ip address 10.22.2.1 255.255.255.0  //配置连接业务网段的接口1
#
interface GigabitEthernet0/0/1
 ip address 10.2.2.1 255.255.255.0  //配置连接业务网段的接口2
#
 ip route-static 0.0.0.0 0.0.0.0 1.2.1.2  //配置静态路由
#
return
```

步骤3 配置RouterC

```
#
 sysname RouterC
#
acl number 3000  //ACL 3000配置，定义了两条数据流
 rule 0 permit ip source 10.4.4.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
 rule 5 permit ip source 10.44.4.0 0.0.0.255 destination 10.11.1.0 0.0.0.255
#
ipsec proposal def
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-192
#
ike proposal 5   //配置IKE提议
 encryption-algorithm aes-cbc-128   //V200R008及之后的版本，aes-cbc-128参数修改为aes-128
 dh group14
 authentication-algorithm sha2-256
#
ike peer center v1  //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 pre-shared-key cipher %^%#IRFGEiFPJ1$&a'Qy,L*XQL_+*Grq-=yMb}ULZdS6%^%#  //配置预共享密钥认证字为“YsHsjx_202206”，以密文显示，该命令在V2R3C00以前的版本中为“pre-shared-key YsHsjx_202206”，以明文显示
 ike-proposal 5
 local-address 1.4.1.1
 remote-address 1.1.1.1
#
ipsec policy hk 1 isakmp  //配置IPSec策略
 security acl 3000
 ike-peer center
 proposal def
#
interface GigabitEthernet0/0/1  //配置互联网接口，用于建立IKE和IPSec隧道外层封装IP地址
 ip address 1.4.1.1 255.255.255.0
 ipsec policy hk
#
interface Ethernet2/0/0
 ip address 10.44.4.1 255.255.255.0  //配置连接业务网段的接口1
#
interface GigabitEthernet0/0/2
 ip address 10.4.4.1 255.255.255.0  //配置连接业务网段的接口2
#
 ip route-static 0.0.0.0 0.0.0.0 1.4.1.2  //配置静态路由
#
return
```

步骤4 验证配置结果

 版权所有 © 华为技术有限公司

在LAC或者LNS上执行命令**display ike sa**可以查看到安全联盟的相关信息。

配置完后两侧用户可以实现数据加密互访。

----结束

配置注意事项

- 总部采用策略模板方式建立IPSec，在IKE对等体的配置中不要指定对端的名称或IP地址。
- 总部和各个分支之间都采用相同的Pre-share-key。

6.4.10 配置分支机构通过 3G 接口访问 Internet，总部利用 IPSec 策略模板与分支建立 IPSec 隧道的示例

规格

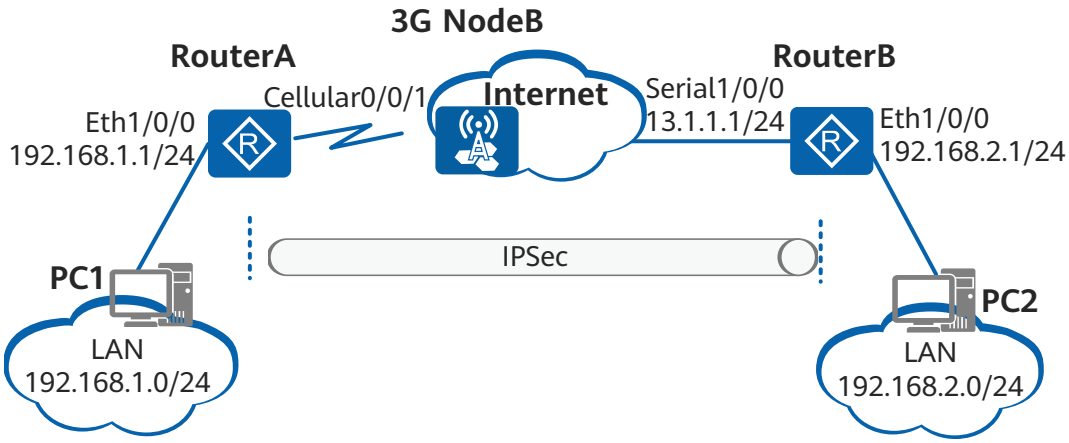
适用于所有版本、所有形态的路由器。

组网需求

企业总部需要和分支建立安全的IPSec连接。总部网关RouterB使用静态公网地址；分支规模较小，网关RouterA使用3G接口从服务商处动态获取IP地址访问公网。总部部署IPSec策略时需要知道分支的IP地址，但分支的IP地址经常发生变化，难以维护。此时可在总部使用IPSec策略模板，无需知道分支的IP地址，即可接入各分支发起的IPSec协商，且配置简单。

建立IPSec后，分支员工只能访问总部内网资源，为了满足分支员工的外网访问需求，需要在RouterA上部署NAT功能。

图 6-43 使用 IPSec 策略模板建立安全联盟组网图



操作步骤

步骤1 配置RouterA

```
#
 sysname RouterA
```


版权所有 © 华为技术有限公司

```
#
acl number 3000  //配置IPSec保护的数据流
 rule 5 permit ip source 192.168.1.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
acl number 3001  //配置外网访问的数据流
 rule 1 deny ip source 192.168.1.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
 rule 2 permit ip source 192.168.1.0 0.0.0.255
#
ipsec proposal rta  //配置IPSec的安全提议
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-192
#
ike proposal 5  //配置IKE的安全提议
 encryption-algorithm aes-cbc-128  //V200R008及之后的版本，aes-cbc-128参数修改为aes-128
 authentication-algorithm sha2-256
#
ike peer rta v1  //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 pre-shared-key cipher %^%#JvZxR2g8c;a9~FPN~n'$7`DEV&=G(=Et02P/%\*!%^%#  //配置预共享密钥认证字为“YsHsjx_202206”，以密文显示，该命令在V2R3C00以前的版本中为“pre-shared-key YsHsjx_202206”，以明文显示
 ike-proposal 5
 remote-address 13.1.1.1  //配置对等体的IP地址，向对端发起IKE协商
#
ipsec policy rta 1 isakmp  //配置IPSec策略
 security acl 3000
 ike-peer rta
 proposal rta
#
dialer-rule  //创建拨号控制列表，符合条件则触发拨号
 dialer-rule 1 ip permit
#
apn profile 3gprofile      //创建APN模板
 user name 3guser password cipher %@%@,)AK/L"R0'^5%YUBDqKP#^y>%@%@ authentication-mode
auto
 apn 3GNET
#
interface Cellular0/0/1  //配置3G接口拨号参数
 link-protocol ppp
 ip address ppp-negotiate  //自动获取运营商分配的IP地址，接入公网
 dialer enable-circular  //使能DCC轮询功能
 dialer-group 1  //将此拨号口加入拨号控制列表，其编号和控制列表中的规则编号一致
 apn-profile 3gprofile
 dialer timer autodial 60  //每隔60秒自动拨号
 dialer number *99# autodial  //按拨号串进行自动拨号
 mode wcdma wcdma-precedence //配置3G数据卡连接WCDMA网络的方式
 ipsec policy rta  //在接口上绑定IPSec策略，发起IPSec协商
 nat outbound 3001  //配置NAT功能，实现公网访问功能
#
ip route-static 0.0.0.0 0.0.0.0 Cellular0/0/1
#
return
```

步骤2 配置RouterB

```
#
 sysname RouterB
#
ipsec proposal rtb
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-192
#
ike proposal 5  //配置IKE的安全提议
 encryption-algorithm aes-cbc-128  //V200R008及之后的版本，aes-cbc-128参数修改为aes-128
 authentication-algorithm sha2-256
#
ike peer rtb v1  //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命
```

令为**ike peer** *peer-name* [**v1** | **v2**]。V200R008及之后的版本命令为**ike peer** *peer-name*和**version** { **1** | **2** }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令**undo version 2**；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令**version 1**，再执行命令**undo version 2**。

```
 pre-shared-key cipher %^%#K{JG:rWVHPMnf;5\|,GW(Luq'qi8BT4nOj%5W5=)%^%#  //配置预共享密钥认证字为“YsHsjx_202206”，以密文显示，该命令在V2R3C00以前的版本中为“pre-shared-key YsHsjx_202206”，以明文显示
 ike-proposal 5
#
ipsec policy-template temp 1  //配置IPSec策略模板，引入各参数
 ike-peer rtb
 proposal rtb
#
ipsec policy rtb 1 isakmp template temp  //配置IPSec策略，引入策略模板
#
interface Serial1/0/0  //配置公网接口，使用固定IP地址
 link-protocol ppp
 ip address 13.1.1.1 255.255.255.0
 ipsec policy rtb
#
ip route-static 0.0.0.0 0.0.0.0 Serial1/0/0
#
return
```

步骤3 验证配置结果

配置完后总部和分支的用户可以互相ping通。

----结束

配置注意事项

- 两端用于IKE协商的预共享密钥保持一致。
- 使用IPSec策略模板的一端，IKE参数中不需要指定对端的IP地址。
- 使用IPSec策略模板的一端，可以不配置ACL规则，如果配置ACL规则对数据流进行保护，则目的地址需要包含所有对端ACL中的源地址。
- 3G接口的拨号参数，各3G网络有所区别，具体需咨询3G网络的服务商。

6.4.11 配置设备之间通过 GRE Over IPSec 方式实现互通的示例

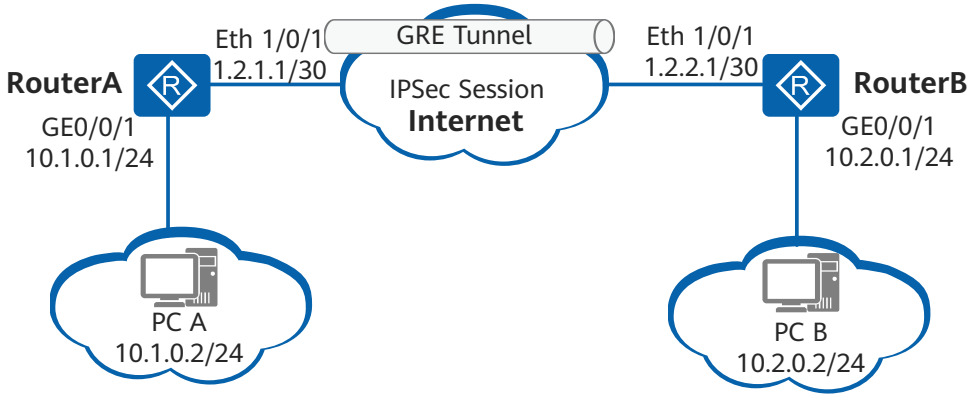
规格

适用于所有版本、所有形态的路由器。

组网需求

如图6-44所示，RouterA和RouterB先建立IPSec会话，在会话接口上建立GRE隧道，将GE0/0/1所连网段的流量引入到GRE隧道上。

图 6-44 GRE Over IPSec 功能的配置组网图



操作步骤

步骤1 配置RouterA

```
#
 sysname RouterA
#
acl number 3000  //配置安全ACL
 rule 0 permit ip source 1.2.1.1 0 destination 1.2.2.1 0
#
ipsec proposal rtb  //配置IPSec提议
 encapsulation-mode transport  //定义封装模式为传输模式
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-192
#
ike proposal 1  //配置IKE提议
 encryption-algorithm aes-cbc-128  //V200R008及之后的版本，aes-cbc-128参数修改为aes-128
 dh group14
 authentication-algorithm sha2-256
#
ike peer rtb v1  //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 ike-proposal 1
 pre-shared-key cipher %^%#JvZxR2g8c;a9~FPN~n'$7`DEV&=G(=Et02P/%\*!%^%#  //配置预共享密钥认证字为“YsHsjx_202206”，以密文显示，该命令在V2R3C00以前的版本中为“pre-shared-key YsHsjx_202206”，以明文显示
 remote-address 1.2.2.1
#
ipsec policy rtb 1 isakmp  //配置IPSec策略，协商方式为isakmp，即使用IKE协商
 security acl 3000  //配置需要加密传送的ACL
 ike-peer rtb  //选择使用的IKE对等体
 proposal rtb  //选择IPSec提议
#
interface Ethernet1/0/1
 ip address 1.2.1.1 255.255.255.252
 ipsec policy rtb  //将安全策略绑定在端口下
#
interface GigabitEthernet0/0/1
 ip address 10.1.0.1 255.255.255.0
#
interface Tunnel0/0/1  //配置GRE隧道
 ip address 1.3.1.1 255.255.255.252
```


版权所有 © 华为技术有限公司

```
 tunnel-protocol gre
 source 1.2.1.1  //指定隧道的源
 destination 1.2.2.1  //指定隧道的目的
#
ip route-static 10.2.0.0 255.255.255.0 Tunnel0/0/1  //定义静态路由
ip route-static 0.0.0.0 0.0.0.0 1.2.1.2
#
return
```

步骤2 配置RouterB

```
#
 sysname RouterB
#
acl number 3000  //配置安全ACL
 rule 0 permit ip source 1.2.2.1 0 destination 1.2.1.1 0
#
ipsec proposal rta  //配置IPSec提议
 encapsulation-mode transport  //定义封装模式为传输模式
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-192
#
ike proposal 1  //配置IKE提议
 encryption-algorithm aes-cbc-128  //V200R008及之后的版本，aes-cbc-128参数修改为aes-128
 dh group14
 authentication-algorithm sha2-256
#
ike peer rta v1  //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 ike-proposal 1
 pre-shared-key cipher %^%#K{JG:rWVHPMnf;5\|,GW(Luq'qi8BT4nOj%5W5=)%^%#  //配置预共享密钥认证字为“YsHsjx_202206”，以密文显示，该命令在V2R3C00以前的版本中为“pre-shared-key YsHsjx_202206”，以明文显示
 remote-address 1.2.1.1
#
ipsec policy rta 1 isakmp  //配置IPSec策略，协商方式为isakmp，即使用IKE协商
 security acl 3000  //定义需要加密传送的ACL
 ike-peer rta  //选择使用的IKE对等体
 proposal rta  //选择IPSec提议
#
interface Ethernet1/0/1
 ip address 1.2.2.1 255.255.255.252
 ipsec policy rta  //将安全策略绑定在端口下
#
interface GigabitEthernet0/0/1
 ip address 10.2.0.1 255.255.255.0
#
interface Tunnel0/0/1  //配置GRE隧道
 ip address 1.3.1.2 255.255.255.252
 tunnel-protocol gre
 source 1.2.2.1  //指定隧道的源
 destination 1.2.1.1  //指定隧道的目的
#
ip route-static 10.1.0.0 255.255.255.0 Tunnel0/0/1  //配置静态路由
ip route-static 0.0.0.0 0.0.0.0 1.2.2.2
#
return
```

步骤3 验证配置结果

在RouterA或者RouterB上执行命令**display ike sa**可以查看到安全联盟的相关信息。

在RouterA或者RouterB上执行命令**display ip routing-table**命令，可以看到经过Tunnel接口去往对端用户侧的路由信息。

 版权所有 © 华为技术有限公司

两端用户可以实现互通。

----结束

配置注意事项

- ACL保护公网接口的数据。
- IPSec Proposal中指定封装模式为传输模式。
- 注意GRE隧道的源和目的，要和IPSec保护流（即IPSec策略引用的ACL定义的数据流）吻合。

6.4.12 配置分支机构与总部之间运行 OSPF，并通过 GRE Over IPSec 方式实现互通的示例

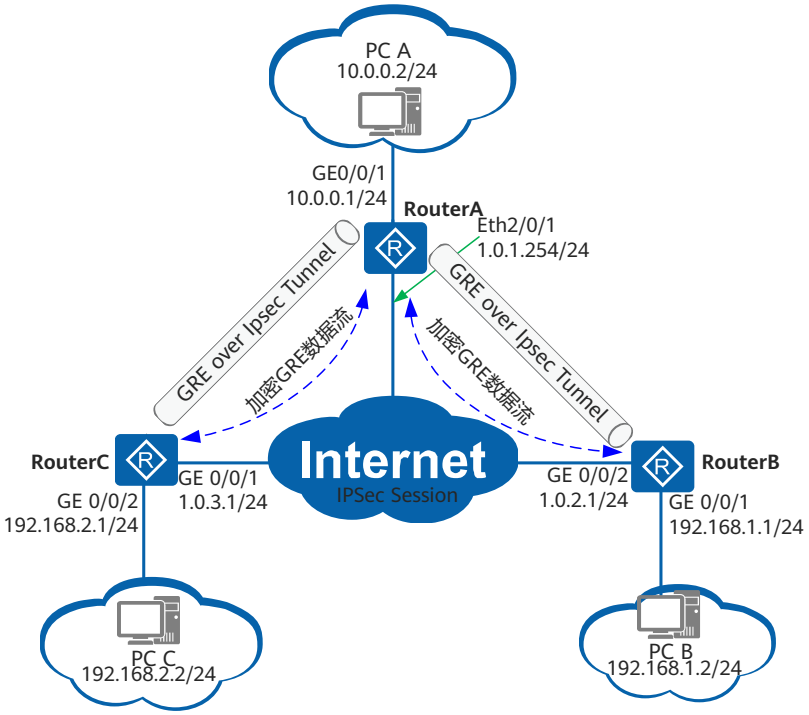
规格

适用于所有版本、所有形态的路由器。

组网需求

如图6-45所示，其中RouterA作为总部网络的出口路由器，对2个分支提供GRE Over IPSec的接入，另外两台RouterB和RouterC分别是2个企业分支网络的出口路由器，通过GRE Over IPSec方式接入到总部。总部与各个分支在GRE隧道上启动OSPF路由协议，实现所有总部与分支之间的流量进行加密。

图 6-45 采用 GRE Over IPSec+OSPF 组网图



版权所有 © 华为技术有限公司

操作步骤

步骤1 配置RouterA

```
#
 sysname RouterA
#
router id 192.168.255.255  //配置OSPF的Router ID
#
acl number 3000  //配置ACL 3000，精确匹配总部路由器和分支1路由器的出口地址
 rule 0 permit ip source 1.0.1.254 0 destination 1.0.2.1 0
#
acl number 3001  //配置ACL 3001，精确匹配总部路由器和分支2路由器的出口地址
 rule 0 permit ip source 1.0.1.254 0 destination 1.0.3.1 0
#
ipsec proposal default
 encapsulation-mode transport
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-192
#
ike proposal 5   //配置IKE提议
 encryption-algorithm aes-cbc-128   //V200R008及之后的版本，aes-cbc-128参数修改为aes-128
 dh group14
 authentication-algorithm sha2-256
#
ike peer branch1 v1  //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 pre-shared-key cipher %^%#JvZxR2g8c;a9~FPN~n'$7`DEV&=G(=Et02P/%\*!%^%#  //配置预共享密钥认证字为“YsHsjx_202206”，以密文显示，该命令在V2R3C00以前的版本中为“pre-shared-key YsHsjx_202206”，以明文显示
 ike-proposal 5
 local-address 1.0.1.254
 remote-address 1.0.2.1
#
ike peer branch2 v1  //配置分支2的IKE Peer
 pre-shared-key cipher %^%#K{JG:rWVHPMnf;5\|,GW(Luq'qi8BT4nOj%5W5=)%^%#  //配置预共享密钥认证字为“YsHsjx_202206”，以密文显示，该命令在V2R3C00以前的版本中为“pre-shared-key YsHsjx_202206”，以明文显示
 ike-proposal 5
 local-address 1.0.1.254
 remote-address 1.0.3.1
#
ipsec policy branch 10 isakmp  //建立IPSec策略branch，序号10，用于与分支1的GRE连接
 security acl 3000
 ike-peer branch1
 proposal default
#
ipsec policy branch 20 isakmp  //建立IPSec策略branch，序号20，用于与分支2的GRE连接
 security acl 3001
 ike-peer branch2
 proposal default
#
interface Ethernet2/0/1  //配置总部外网出口
 ip address 1.0.1.254 255.255.255.0
  ipsec policy branch
#
interface GigabitEthernet0/0/1  //配置公司总部内网接口
 ip address 10.0.0.1 255.255.255.0
#
interface LoopBack0  //配置用于Router ID的环回地址
 ip address 192.168.255.255 255.255.255.255
#
interface Tunnel0/0/0  //配置用于与分支1建立GRE连接的隧道接口
 ip address 192.168.0.1 255.255.255.252
 tunnel-protocol gre
 source Ethernet2/0/1
```

 版权所有 © 华为技术有限公司

```
 destination 1.0.2.1
#
interface Tunnel0/0/1  //配置用于与分支2建立GRE连接的隧道接口
 ip address 192.168.0.5 255.255.255.252
 tunnel-protocol gre
 source Ethernet2/0/1
 destination 1.0.3.1
#
ospf 1  //配置启用OSPF路由
 area 0.0.0.0
  network 10.0.0.0 0.0.0.255
  network 192.168.255.255 0.0.0.0
  network 192.168.0.0 0.0.0.3
  network 192.168.0.4 0.0.0.3
#
ip route-static 0.0.0.0 0.0.0.0 1.0.1.253
#
return
```

步骤2 配置RouterB

```
#
 sysname RouterB
#
router id 192.168.255.1  //配置OSPF的Router ID
#
acl number 3000  //配置ACL 3000，需要与总部路由器的ACL 3000互为镜像
 rule 0 permit ip source 1.0.2.1 0 destination 1.0.1.254 0
#
ipsec proposal default   //配置IPSec提议，也需要与总部配置一致
 encapsulation-mode transport
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-192
#
ike proposal 5   //配置IKE提议
 encryption-algorithm aes-cbc-128   //V200R008及之后的版本，aes-cbc-128参数修改为aes-128
 dh group14
 authentication-algorithm sha2-256
#
ike peer center v1  //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 pre-shared-key cipher %^%#IRFGEiFPJ1$&a'Qy,L*XQL_+*Grq-=yMb}ULZdS6%^%#  //配置预共享密钥认证字为“YsHsjx_202206”，以密文显示，该命令在V2R3C00以前的版本中为“pre-shared-key YsHsjx_202206”，以明文显示
 ike-proposal 5
 local-address 1.0.2.1
 remote-address 1.0.1.254
#
ipsec policy center 1 isakmp  //配置IPSec策略center，需要1，使用ISAKMP方式
 security acl 3000
 ike-peer center
 proposal default
#
interface GigabitEthernet0/0/1  //配置公司总部内网接口
 ip address 192.168.1.1 255.255.255.0
 #
interface GigabitEthernet0/0/2  //配置分支1外网出接口
 ip address 1.0.2.1 255.255.255.0
 ipsec policy center
#
interface LoopBack0  //配置用于Router ID的环回口
 ip address 192.168.255.1 255.255.255.255
#
interface Tunnel0/0/0  //配置用于连接总部的GRE隧道接口
 ip address 192.168.0.2 255.255.255.252
 tunnel-protocol gre
```

 版权所有 © 华为技术有限公司

```
 source GigabitEthernet0/0/2
 destination 1.0.1.254
#
#
ospf 1  //配置OSPF路由
 area 0.0.0.0
  network 192.168.255.1 0.0.0.0
  network 192.168.0.0 0.0.0.3
  network 192.168.1.0 0.0.0.255
#
ip route-static 0.0.0.0 0.0.0.0 1.0.2.2
#
return
```

步骤3 配置RouterC

```
#
 sysname RouterC
#
router id 192.168.255.2  //配置OSPF的Router ID
#
acl number 3001  //配置ACL 3001，需要与总部路由器的ACL 3001互为镜像
 rule 0 permit ip source 1.0.3.1 0 destination 1.0.1.254 0
#
ipsec proposal default   //配置IPSec提议，也需要与总部配置一致
 encapsulation-mode transport
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-192
#
ike proposal 5   //配置IKE提议
 encryption-algorithm aes-cbc-128   //V200R008及之后的版本，aes-cbc-128参数修改为aes-128
 dh group14
 authentication-algorithm sha2-256
#
ike peer center v1  //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 pre-shared-key cipher %^%#(3fr1!&6O=)!GN#~{)n,2fq>4#4+%;lMTs5(]:c)%^%#  //配置预共享密钥认证字为“YsHsjx_202206”，以密文显示，该命令在V2R3C00以前的版本中为“pre-shared-key YsHsjx_202206”，以明文显示
 ike-proposal 5
 local-address 1.0.3.1
 remote-address 1.0.1.254
#
ipsec policy center 1 isakmp  //配置IPSec策略center，需要1，使用ISAKMP方式
 security acl 3001
 ike-peer center
 proposal default
#
interface GigabitEthernet0/0/2  //配置公司总部内网接口
 ip address 192.168.2.1 255.255.255.0
 #
interface GigabitEthernet0/0/1  //配置分支1外网出接口
 ip address 1.0.3.1 255.255.255.0
 ipsec policy center
#
interface LoopBack0  //配置用于Router ID的环回口
 ip address 192.168.255.2 255.255.255.255
#
interface Tunnel0/0/1  //配置用于连接总部的GRE隧道接口
 ip address 192.168.0.6 255.255.255.252
 tunnel-protocol gre
 source GigabitEthernet0/0/1
 destination 1.0.1.254
#
ospf 1  //配置OSPF路由
 area 0.0.0.0
```

 版权所有 © 华为技术有限公司

```
 network 192.168.255.2 0.0.0.0
 network 192.168.0.4 0.0.0.3
 network 192.168.2.0 0.0.0.255
#
ip route-static 0.0.0.0 0.0.0.0 1.0.3.2
#
return
```

步骤4 验证配置结果

在RouterA或者RouterB上执行命令**display ike sa**可以查看到安全联盟的相关信息。

在RouterA或者RouterB上执行命令**display ip routing-table**命令，可以看到经过Tunnel接口去往对端用户侧的路由信息。

分部和总部之间用户可以实现互通。

----结束

配置注意事项

- 总部ACL配置需要注意不能配置Deny的规则，否则会导致业务流不走IPSec隧道。
- 分支的ACL需要与总部ACL互为镜像。
- 总部的IPSec策略只能创建一个，在不同的序号中指定不同IKE Peer。
- 总部和各分支之间的外网地址可以互通。

6.4.13 配置分支机构与总部之间通过 GRE Over IPSec 方式实现互通，并穿越 NAT 设备实现分支之间互通的示例（运行 OSPF）

规格

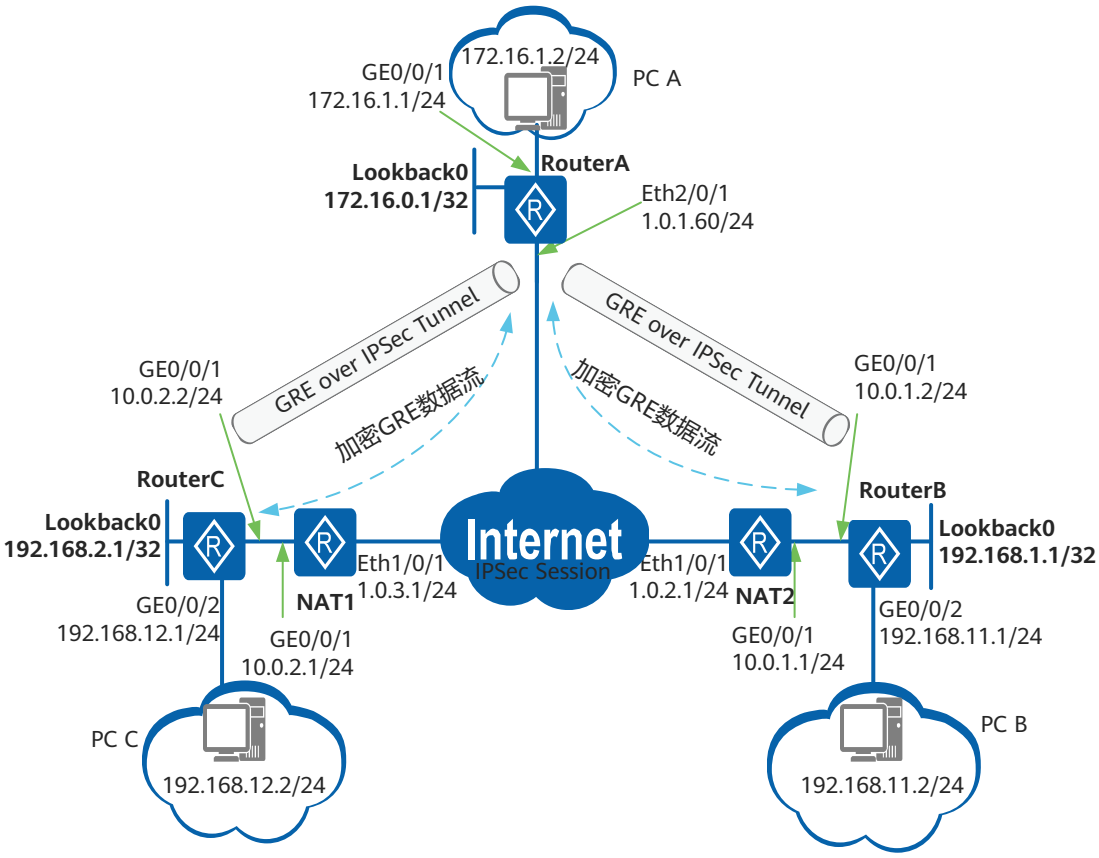
适用于所有版本、所有形态的路由器。

组网需求

如图6-46所示，总部对多个分支提供IPSec VPN接入，分支出口存在NAT设备，因此总部与分支之间配置成野蛮模式和NAT穿越，总部路由器不配置ACL，而使用安全模板，总部和分支之间通过内网Loopback建立GRE隧道，分支通过建立ACL使分支Loopback和总部Loopback之间的GRE通过IPSec互通，建立好GRE隧道后，在隧道上运行OSPF，使各内部路由互通，分支之间的流量通过总部转发。

 版权所有 © 华为技术有限公司

图 6-46 采用 GRE Over IPSec+OSPF 穿越 NAT 多分支互通功能组网图



操作步骤

步骤1 配置RouterA

```
#
 sysname RouterA
#
router id 172.16.0.1  //配置OSPF的Router ID
#
 ike local-name rta
#
ipsec proposal default  //配置默认安全提议
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-192
#
ike proposal 5   //配置IKE提议
 encryption-algorithm aes-cbc-128   //V200R008及之后的版本，aes-cbc-128参数修改为aes-128
 dh group14
 authentication-algorithm sha2-256
#
ike peer branch v1  //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 exchange-mode aggressive  //配置成野蛮模式
```


版权所有 © 华为技术有限公司

```
 pre-shared-key cipher %^%#JvZxR2g8c;a9~FPN~n'$7`DEV&=G(=Et02P/%\*!%^%#  //配置预共享密钥认证字为“YsHsjx_202206”，以密文显示，该命令在V2R3C00以前的版本中为“pre-shared-key YsHsjx_202206”，以明文显示
 ike-proposal 5
 local-id-type name   //配置IKE协商时本端的ID类型。V200R008及之后的版本，name参数修改为fqdn
 nat traversal   //使能NAT穿越功能。V200R008版本，设备默认使能NAT穿越功能，不支持配置此命令；但V200R008之后版本，支持配置此命令
#
ipsec policy-template branch 1  //配置分支的安全模板，序号1
 ike-peer branch
 proposal default
#
ipsec policy policy1 1 isakmp template branch    //根据安全模板branch创建安全策略policy1序号1
#
interface Ethernet2/0/1  //配置总部外网接口
 ip address 1.0.1.60 255.255.255.0
 ipsec policy policy1
#
interface GigabitEthernet0/0/1  //配置总部内网接口地址
 ip address 172.16.1.1 255.255.255.0
#
interface LoopBack0  //配置用于建立GRE连接和OSPF Router ID的Loopback接口
 ip address 172.16.0.1 255.255.255.255
#
interface Tunnel0/0/0  //配置连接分支1的GRE隧道
 ip address 192.168.0.1 255.255.255.252
 tunnel-protocol gre
 source LoopBack0
 destination 192.168.1.1
#
interface Tunnel0/0/1  //配置连接分支2的GRE隧道
 ip address 192.168.0.5 255.255.255.252
 tunnel-protocol gre
 source LoopBack0
 destination 192.168.2.1
#
ospf 1  //配置路由
 area 0.0.0.0
  network 192.168.0.4 0.0.0.3
  network 172.16.1.0 0.0.0.255
  network 192.168.0.0 0.0.0.3
#
ip route-static 0.0.0.0 0.0.0.0 1.0.1.61  //配置默认路由
#
return
```

步骤2 配置RouterB

```
#
 sysname RouterB
#
 router id 192.168.1.1  //配置OSPF的Router ID
#
 ike local-name rtb
#
acl number 3000
 rule 0 permit gre source 192.168.1.1 0 destination 172.16.0.1 0
#
ipsec proposal default  //默认的安全提议
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-192
#
ike proposal 5   //配置IKE提议
 encryption-algorithm aes-cbc-128   //V200R008及之后的版本，aes-cbc-128参数修改为aes-128
 dh group14
 authentication-algorithm sha2-256
#
ike peer center v1  //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 |
```

 版权所有 © 华为技术有限公司

2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令**undo version 2**；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令**version 1**，再执行命令**undo version 2**。
 exchange-mode aggressive //配置使用野蛮模式
 pre-shared-key cipher %^%#K{JG:rWVHPMnf;5\|,GW(Luq'qi8BT4nOj%5W5=)%^%# //配置预共享密钥认证字为“YsHsjx_202206”，以密文显示，该命令在V2R3C00以前的版本中为“pre-shared-key YsHsjx_202206”，以明文显示
 ike-proposal 5
 local-id-type name //配置IKE协商时本端的ID类型。V200R008及之后的版本，**name**参数修改为**fqdn**
 remote-name rta //配置对端IKE peer名称。V200R008及之后的版本，设备不支持命令**remote-name**，其命令功能等同于命令**remote-id**
 nat traversal //使能NAT穿越功能。V200R008版本，设备默认使能NAT穿越功能，不支持配置此命令；但V200R008之后版本，支持配置此命令
 remote-address 1.0.1.60
#
ipsec policy center 1 isakmp //配置到总部的安全策略，序号1
 security acl 3000
 ike-peer center
 proposal default
#
interface GigabitEthernet0/0/1 //配置分支1的外网出接口
 ip address 10.0.1.2 255.255.255.0
 ipsec policy center
#
interface GigabitEthernet0/0/2 //配置分支1内网接口
 ip address 192.168.11.1 255.255.255.0
#
interface LoopBack0 //配置用于创建于总部连接的GRE源和OSPF的Router ID的Loopback接口
 ip address 192.168.1.1 255.255.255.255
#
interface Tunnel0/0/0 //配置连接总部的GRE隧道
 ip address 192.168.0.2 255.255.255.252
 tunnel-protocol gre
 source LoopBack0
 destination 172.16.0.1
//配置OSPF路由
ospf 1
 area 0.0.0.0
  network 192.168.11.0 0.0.0.255
  network 192.168.0.0 0.0.0.3
#
ip route-static 0.0.0.0 0.0.0.0 10.0.1.1 //配置默认路由
#
return

步骤3 配置RouterC

```
#
 sysname RouterC
#
 router id 192.168.2.1  //配置OSPF的Router ID
#
 ike local-name rtc
#
acl number 3000
 rule 0 permit gre source 192.168.2.1 0 destination 172.16.0.1 0
#
ipsec proposal default  //配置默认的安全提议
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-192
#
ike proposal 5  //配置IKE提议
 encryption-algorithm aes-cbc-128  //V200R008及之后的版本，aes-cbc-128参数修改为aes-128
 dh group14
 authentication-algorithm sha2-256
#
ike peer center v1  //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协
```

 版权所有 © 华为技术有限公司

```
议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 exchange-mode aggressive  //配置使用野蛮模式
 pre-shared-key cipher %^%#IRFGEiFPJ1$&a'Qy,L*XQL_+*Grq-=yMb}ULZdS6%^%#  //配置预共享密钥认证字为“YsHsjx_202206”，以密文显示，该命令在V2R3C00以前的版本中为“pre-shared-key YsHsjx_202206”，以明文显示
 ike-proposal 5
 local-id-type name   //配置IKE协商时本端的ID类型。V200R008及之后的版本，name参数修改为fqdn
 remote-name rta   //配置对端IKE peer名称。V200R008及之后的版本，设备不支持命令remote-name，其命令功能等同于命令remote-id
 nat traversal   //使能NAT穿越功能。V200R008版本，设备默认使能NAT穿越功能，不支持配置此命令；但V200R008之后版本，支持配置此命令
 remote-address 1.0.1.60
#
ipsec policy center 1 isakmp  //配置到总部的安全策略，序号1
 security acl 3000
 ike-peer center
 proposal default
#
interface GigabitEthernet0/0/1  //配置分支2的外网出接口
 ip address 10.0.2.2 255.255.255.0
 ipsec policy center
#
interface GigabitEthernet0/0/2  //配置分支2内网接口
 ip address 192.168.12.1 255.255.255.0
#
interface LoopBack0  //配置用于创建于总部连接的GRE源和OSPF的Router ID的Loopback接口
 ip address 192.168.2.1 255.255.255.255
#
interface Tunnel0/0/1  //配置连接总部的GRE隧道
 ip address 192.168.0.6 255.255.255.252
 tunnel-protocol gre
 source LoopBack0
 destination 172.16.0.1
#  //配置OSPF路由
ospf 1
 area 0.0.0.0
  network 192.168.0.4 0.0.0.3
  network 192.168.12.0 0.0.0.255
#
ip route-static 0.0.0.0 0.0.0.0 10.0.2.1  //配置默认路由
#
return
```

步骤4 配置NAT1

```
#
 sysname NAT1
#
acl number 2000  //配置需要被NAT处理的地址
 rule 0 permit source 10.0.2.0 0.0.0.255
#
 nat address-group 0 11.0.0.1 11.0.0.10  //配置NAT地址池
#
interface Ethernet1/0/1  //NAT设备外网接口
 ip address 1.0.3.1 255.255.255.0
 nat outbound 2000 address-group 0
#
interface GigabitEthernet0/0/1  //连接分支2路由器的接口地址
 ip address 10.0.2.1 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 1.0.3.2  //配置默认路由
#
return
```

步骤5 配置NAT2

```
#
 sysname NAT2
#
```

 版权所有 © 华为技术有限公司

```
acl number 2000  //配置需要被NAT处理的地址
 rule 0 permit source 10.0.1.0 0.0.0.255
#
 nat address-group 0 12.0.0.1 12.0.0.10  //配置NAT地址池
#
interface Ethernet1/0/1  //NAT设备外网接口
 ip address 1.0.2.1 255.255.255.0
 nat outbound 2000 address-group 0
#
interface GigabitEthernet0/0/1  //连接分支1路由器的接口地址
 ip address 10.0.1.1 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 1.0.2.2  //配置默认路由
#
return
```

步骤6 验证配置结果

在RouterA、RouterB或者RouterC上执行命令**display ike sa**可以查看到安全联盟的相关信息。

在RouterA或者RouterB上执行命令**display ip routing-table**命令，可以看到经过Tunnel接口去往对端用户侧的路由信息。

分部和总部之间用户可以实现互通。

----结束

配置注意事项

- 总部ACL配置需要注意不能配置Deny的规则，否则会导致业务流不走IPSec隧道。
- 总部的IPSec策略只能创建一个，在不同的序号中指定不同IKE Peer。
- 总部和各分支之间的外网地址路由可达。
- 配置NAT地址池时，请确保其他设备到NAT地址池中地址段的路由可达。

6.4.14 配置分支与总部之间建立 IPSec over GRE 隧道示例（基于 ACL 方式）

规格

适用于V200R008C50及更高版本、所有形态的AR路由器。

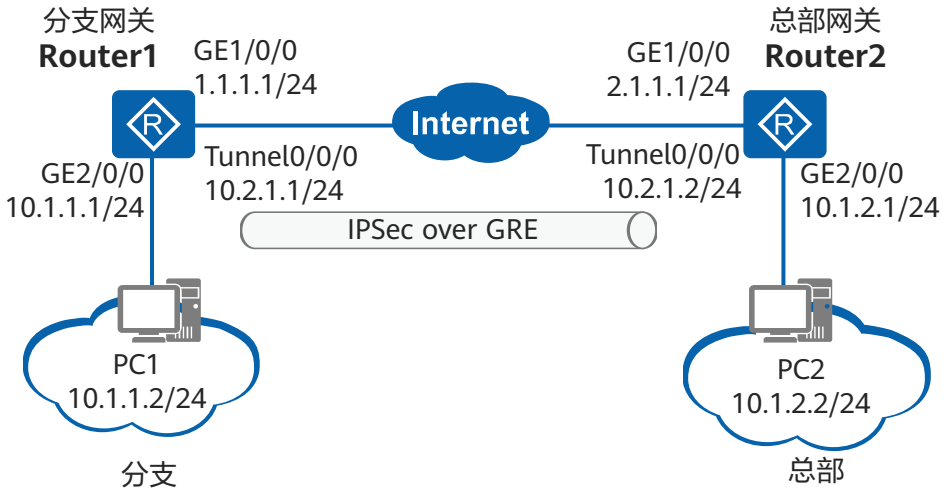
组网需求

如图6-47所示，Router1为公司分支网关，Router2为公司总部网关，分支与总部通过公网建立通信。

原公司分支与总部通过GRE隧道实现私网互通，现要求对分支与总部之间相互访问的流量（不包括组播数据）进行安全保护。因此，可基于ACL方式建立IPSec over GRE，对分支和总部互通的流量进行保护。

 版权所有 © 华为技术有限公司

图 6-47 配置分支与总部之间建立 IPSec over GRE 隧道组网图



操作步骤

步骤1 配置Router1

```
#
 sysname Router1
#
acl number 3101   //配置允许进行IPSec加密的地址网段
 rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
#
ipsec proposal tran1   //配置IPSec的安全提议的认证和加密算法
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-128
#
ike proposal 5   //配置IKE的安全提议的认证、加密和DH组算法
 encryption-algorithm aes-128
 dh group14
 authentication-algorithm sha2-256
#
ike peer spub   //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 pre-shared-key cipher %^%#JvZxR2g8c;a9~FPN~n'$7`DEV&=G(=Et02P/%\*!%^%#   //配置预共享密钥为YsHsjx_202206
 ike-proposal 5
 remote-address 10.2.1.2   //配置对端Tunnel接口的IP地址
#
ipsec policy map1 10 isakmp   //配置安全策略，引入各参数
 security acl 3101
 ike-peer spub
 proposal tran1
#
interface GigabitEthernet1/0/0
 ip address 1.1.1.1 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 10.1.1.1 255.255.255.0
#
interface Tunnel0/0/0   //配置GRE Tunnel接口
```


版权所有 © 华为技术有限公司

```
 ip address 10.2.1.1 255.255.255.0
 tunnel-protocol gre
 source 1.1.1.1
 destination 2.1.1.1
 ipsec policy map1   //在接口应用安全策略，开启IPSec保护功能
#
ip route-static 2.1.1.0 255.255.255.0 1.1.1.2   //配置公网的静态路由
ip route-static 10.1.2.0 255.255.255.0 Tunnel0/0/0   //配置私网的静态路由
#
return
```

步骤2 配置Router2

```
#
 sysname Router2
#
acl number 3101   //配置允许进行IPSec加密的地址网段
 rule 5 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
#
ipsec proposal tran1   //配置IPSec的安全提议的认证和加密算法
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-128
#
ike proposal 5   //配置IKE的安全提议的认证、加密和DH组算法
 encryption-algorithm aes-128
 dh group14
 authentication-algorithm sha2-256
#
ike peer spua   //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 pre-shared-key cipher %^%#K{JG:rWVHPMnf;5\|,GW(Luq'qi8BT4nOj%5W5=)%^%#   //配置预共享密钥为YsHsjx_202206
 ike-proposal 5
 remote-address 10.2.1.1   //配置对端Tunnel接口的IP地址
#
ipsec policy use1 10 isakmp   //配置安全策略，引入各参数
 security acl 3101
 ike-peer spua
 proposal tran1
#
interface GigabitEthernet1/0/0
 ip address 2.1.1.1 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 10.1.2.1 255.255.255.0
#
interface Tunnel0/0/0   //配置GRE Tunnel接口
 ip address 10.2.1.2 255.255.255.0
 tunnel-protocol gre
 source 2.1.1.1
 destination 1.1.1.1
 ipsec policy use1   //在接口应用安全策略，开启IPSec保护功能
#
ip route-static 1.1.1.0 255.255.255.0 2.1.1.2   //配置公网的静态路由
ip route-static 10.1.1.0 255.255.255.0 Tunnel0/0/0   //配置私网的静态路由
#
return
```

步骤3 验证配置结果

在Router上执行命令**display ike sa**，可以看到SA建立成功。

 版权所有 © 华为技术有限公司

分支Ping总部后，在Router上执行命令**display ipsec statistics**查看IPSec报文的统计信息，**input/output security packets**字段的计数值不为0，表明分支和总部之间的通信被加密传输。

----结束

注意事项

- 两端用于IKE协商的预共享密钥保持一致。
- IKE对等体中配置的对端地址为Tunnel接口的IP地址。

6.4.15 配置分支与总部之间建立 IPSec over DSVPN 隧道示例（基于 ACL 方式）

规格

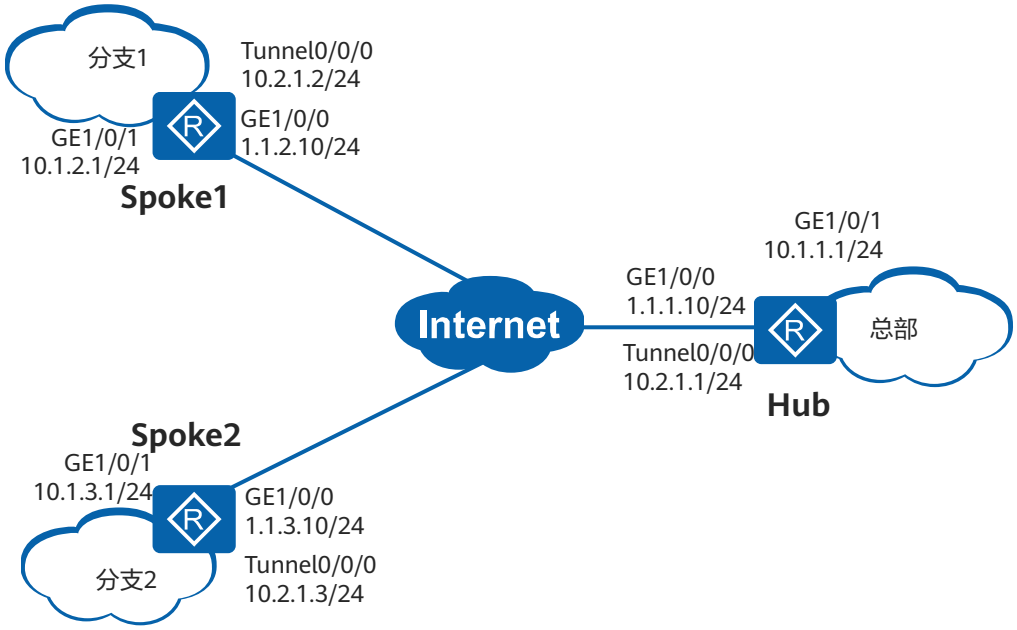
适用于V200R008C50及更高版本、所有形态的AR路由器。

组网需求

如图6-48所示，某大型企业有总部（Hub）和多个分支（Spoke1、Spoke2……，举例中仅使用两个分支），分布在不同地域，分支通过DHCP获取动态地址接入公网，并且分支间、分支和总部通过部署DSVPN实现互联。

现在用户希望对总部和分支以及分支间传输的数据进行加密保护，此时可以在分支和总部上部署IPSec over DSVPN，实现对他们互通的流量进行保护。

图 6-48 配置分支与总部之间建立 IPSec over DSVPN 隧道组网图



假设Spoke1和Spoke2获取的动态地址分别为1.1.2.10和1.1.3.10。

版权所有 © 华为技术有限公司

操作步骤

步骤1 配置Hub

```
#
 sysname Hub
#
ipsec proposal pro1   //配置IPSec的安全提议的认证和加密算法
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256
#
ike proposal 1   //配置IKE的安全提议的认证、加密、PRF和DH组算法
 encryption-algorithm aes-256
 dh group14
 authentication-algorithm sha2-256
 prf aes-xcbc-128
#
ike peer hub   //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 pre-shared-key cipher %@%@6vn$NdN1M+5]huX8YT'B|'*5%@%@%^%#O3uIP\/YNF
+`AcJhbZ&C7y*iVlOOU@DraF58J4=;%^%#   //配置预共享密钥为YsHsjx_202206
 ike-proposal 1
 dpd type periodic
 dpd idle-time 40
#
ipsec policy-template use1 10   //配置IPSec策略模板，引入各参数
 ike-peer hub
 proposal pro1
#
ipsec policy policy1 10 isakmp template use1   //配置IPSec策略，引入策略模板
#
interface GigabitEthernet1/0/0
 ip address 1.1.1.10 255.255.255.0
#
interface GigabitEthernet1/0/1
 ip address 10.1.1.1 255.255.255.0
#
interface Tunnel0/0/0   //配置mGRE Tunnel接口
 ip address 10.2.1.1 255.255.255.0
 tunnel-protocol gre p2mp
 source GigabitEthernet1/0/0
 ospf network-type p2mp   //配置OSPF网络类型为点到多点型
 ipsec policy policy1   //在接口应用安全策略，开启IPSec保护功能
 nhrp entry multicast dynamic   //配置动态注册的分支加入NHRP组播成员表
#
ospf 1 router-id 10.2.1.1   //配置私网路由
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 10.2.1.0 0.0.0.255
#
ospf 2   //配置公网路由
 area 0.0.0.1
  network 1.1.1.0 0.0.0.255
#
return
```

步骤2 配置Spoke1

```
#
 sysname Spoke1
#
acl number 3101   //配置允许进行IPSec加密的地址网段
 rule 5 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
 rule 10 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.3.0 0.0.0.255
#
ipsec proposal pro1   //配置IPSec的安全提议的认证和加密算法
```

 版权所有 © 华为技术有限公司

```
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256
#
ike proposal 1   //配置IKE的安全提议的认证、加密、PRF和DH组算法
 encryption-algorithm aes-256
 dh group14
 authentication-algorithm sha2-256
 prf aes-xcbc-128
#
ike peer spoke1   //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 pre-shared-key cipher %@%@6vn$NdN1M+5]huX8YT'B|'*5%@%@%^%#O3uIP\/YNF
+`AcJhbZ&C7y*iVlOOU@DraF58J4=;%^%#   //配置预共享密钥为YsHsjx_202206
 ike-proposal 1
 dpd type periodic   //配置DPD检测模式为周期型
 dpd idle-time 40   //对等体存活检测空闲时间
 remote-address 10.2.1.1   //配置对端Tunnel接口的IP地址
#
ipsec policy policy1 10 isakmp   //配置安全策略，引入各参数
 security acl 3101
 ike-peer spoke1
 proposal pro1
#
interface GigabitEthernet1/0/0
 ip address dhcp-alloc
#
interface GigabitEthernet1/0/1
 ip address 10.1.2.1 255.255.255.0
#
interface Tunnel0/0/0   //配置mGRE Tunnel接口
 ip address 10.2.1.2 255.255.255.0
 tunnel-protocol gre p2mp
 source GigabitEthernet1/0/0
 ospf network-type p2mp   //配置OSPF网络类型为点到多点型
 ipsec policy policy1   //在接口应用安全策略，开启IPSec保护功能
 nhrp entry 10.2.1.1 1.1.1.10 register   //配置NHRP映射表
#
ospf 1 router-id 10.2.1.2   //配置私网路由
 area 0.0.0.0
  network 10.1.2.0 0.0.0.255
  network 10.2.1.0 0.0.0.255
#
ospf 2   //配置公网路由
 area 0.0.0.1
  network 1.1.2.0 0.0.0.255
#
return
```

步骤3 配置Spoke2

```
#
 sysname Spoke2
#
acl number 3101   //配置允许进行IPSec加密的地址网段
 rule 5 permit ip source 10.1.3.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
 rule 10 permit ip source 10.1.3.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
#
ipsec proposal pro1   //配置IPSec的安全提议的认证和加密算法
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256
#
ike proposal 1   //配置IKE的安全提议的认证、加密、PRF和DH组算法
 encryption-algorithm aes-256
 dh group14
 authentication-algorithm sha2-256
 prf aes-xcbc-128
```

 版权所有 © 华为技术有限公司

```
#
ike peer spoke2  //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 pre-shared-key cipher %@%@6vn$NdN1M+5]huX8YT'B|'*5%@%@%^%#O3uIP\/YNF
+`AcJhbZ&C7y*iVlOOU@DraF58J4=;%^%#  //配置预共享密钥为YsHsjx_202206
 ike-proposal 1
 dpd type periodic  //配置DPD检测模式为周期型
 dpd idle-time 40  //对等体存活检测空闲时间
 remote-address 10.2.1.1  //配置对端Tunnel接口的IP地址
#
ipsec policy policy1 10 isakmp  //配置安全策略，引入各参数
 security acl 3101
 ike-peer spoke2
 proposal pro1
#
interface GigabitEthernet1/0/0
 ip address dhcp-alloc
#
interface GigabitEthernet1/0/1
 ip address 10.1.3.1 255.255.255.0
#
interface Tunnel0/0/0  //配置mGRE Tunnel接口
 ip address 10.2.1.3 255.255.255.0
 tunnel-protocol gre p2mp
 source GigabitEthernet1/0/0
 ospf network-type p2mp  //配置OSPF网络类型为点到多点型
 ipsec policy policy1  //在接口应用安全策略，开启IPSec保护功能
 nhrp entry 10.2.1.1 1.1.1.10 register  //配置NHRP映射表
#
ospf 1 router-id 10.2.1.3  //配置私网路由
 area 0.0.0.0
  network 10.1.3.0 0.0.0.255
  network 10.2.1.0 0.0.0.255
#
ospf 2  //配置公网路由
 area 0.0.0.1
  network 1.1.3.0 0.0.0.255
#
return
```

步骤4 验证配置结果

在Spoke和Hub上执行命令**display ike sa**，可以看到SA建立成功。

Spoke1分支Ping Hub总部后，在Spoke1上执行命令**display ipsec statistics**查看IPSec报文的统计信息，**input/output security packets**字段的计数值不为0，表明分支和总部之间的通信被加密传输。

Spoke2分支Ping Spoke1分支后，在Spoke2上执行命令**display ipsec statistics**查看IPSec报文的统计信息，**input/output security packets**字段的计数值不为0，表明分支间的通信被加密传输。

----结束

注意事项

- 两端用于IKE协商的预共享密钥保持一致。
- IKE对等体中配置的对端地址为Tunnel接口的IP地址。

 版权所有 © 华为技术有限公司

6.4.16 配置分支机构与总部之间采用域名进行 IKE 自动协商，建立 IPSec 隧道的示例

规格

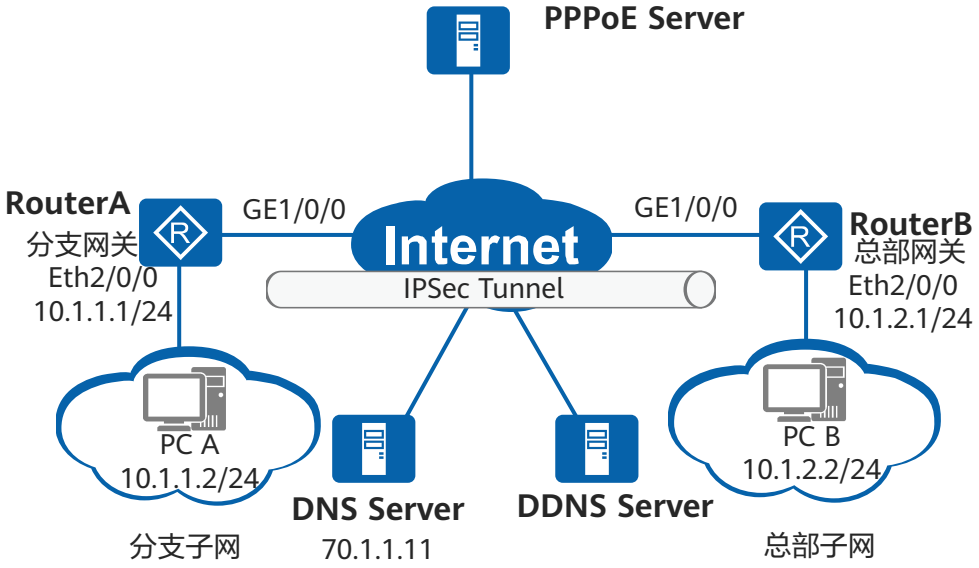
适用于所有版本、所有形态的路由器。

组网需求

如图6-49所示，RouterA为企业远程分支网关，RouterB为企业总部网关，分支与总部均通过PPPoE方式接入公网建立通信。分支子网为10.1.1.0/24，总部子网为10.1.2.0/24。DNS Server为解析域名的服务器，DDNS Server为更新域名对应IP地址的服务器，PPPoE Server为分配IP地址的服务器。

企业希望对分支子网与总部子网之间的流量进行安全保护。分支与总部通过公网建立通信，可以在分支网关与总部网关之间建立一个IPSec隧道来实施安全保护。由于分支与总部的IP地址均为动态地址，可以采用域名形式进行IKE协商。

图 6-49 配置分支与总部协商采用动态地址进行 IKE 协商的 IPSec 隧道组网图



操作步骤

步骤1 配置RouterA

```
#
 sysname RouterA  //配置设备名称
#
 dns resolve  //使能DNS域名解析功能
 dns server 70.1.1.11  //配置DNS服务器的IP地址
 ddns policy ddnspolicy1  //配置DDNS策略
 url oray://<username>:<password>@phddnsdev.oray.net username username1 password password1  //配置DDNS服务器的URL
#
acl number 3003  //配置ACL，定义由子网10.1.1.0/24去子网10.1.2.0/24的数据流
 rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
#
```


版权所有 © 华为技术有限公司

```
ipsec proposal prop1  //配置IPSec安全提议
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-192
#
ike proposal 5  //配置IKE安全提议
 encryption-algorithm aes-cbc-128  //V200R008及之后的版本，aes-cbc-128参数修改为aes-128
 dh group14
 authentication-algorithm sha2-256
#
ike peer rut1 v1  //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 pre-shared-key cipher %^%#JvZxR2g8c;a9~FPN~n'$7`DEV&=G(=Et02P/%\*!%^%#  //配置预共享密钥认证字为“YsHsjx_202206”，以密文显示，该命令在V2R3C00以前的版本中为“pre-shared-key YsHsjx_202206”，以明文显示
 ike-proposal 5
 remote-address www.huaweib.com  //该域名已向DDNS服务提供商申请注册
#
ipsec policy policy1 10 isakmp  //配置安全策略
 security acl 3003
 ike-peer rut1
 proposal prop1
#
interface Dialer1  //配置拨号口相关参数
 link-protocol ppp
 ppp chap user user@huawei.com
 ppp chap password cipher %@%@l$S'&"Sm7!j4F#)i{{G#L3Wu%@%@
 ip address ppp-negotiate
 dialer user huawei
 dialer bundle 1
 dialer-group 1
 ddns policy ddnspolicy1  //拨号口上应用DDNS策略，使其接口IP地址发生变化时，能向DDNS服务器发送动态更新
 ipsec policy policy1  //拨号口上应用安全策略，使接口具有IPSec的保护功能
#
interface GigabitEthernet1/0/0  //在物理接口下绑定拨号口，建立PPPoE会话
 pppoe-client dial-bundle-number 1
#
interface Ethernet2/0/0
 ip address 10.1.1.1 255.255.255.0
#
dialer-rule  //配置拨号访问组，指定允许所有的IPv4报文通过
 dialer-rule 1 ip permit
#
ip route-static 0.0.0.0 255.255.255.255 dialer1
#
return
```

步骤2 配置RouterB

```
#
 sysname RouterB  //配置设备名称
#
 dns resolve  //使能DNS域名解析功能
 dns server 70.1.1.11  //配置DNS服务器的IP地址
 ddns policy ddnspolicy1  //配置DDNS策略
 url oray://<username>:<password>@phddnsdev.oray.net username username2 password password2  //配置DDNS服务器的URL
#
acl number 3003  //配置ACL，定义由子网10.1.2.0/24去子网10.1.1.0/24的数据流
 rule 5 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
#
ipsec proposal prop1  //配置IPSec安全提议
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-192
#
ike proposal 5  //配置IKE安全提议
```

```
 encryption-algorithm aes-cbc-128  //V200R008及之后的版本，aes-cbc-128参数修改为aes-128
 dh group14
 authentication-algorithm sha2-256
#
ike peer rut1 v1  //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 pre-shared-key cipher %^%#K{JG:rWVHPMnf;5\|,GW(Luq'qi8BT4nOj%5W5=)%^%#  //配置预共享密钥认证字为“YsHsjx_202206”，以密文显示，该命令在V2R3C00以前的版本中为“pre-shared-key YsHsjx_202206”，以明文显示
 ike-proposal 5
 remote-address www.huaweia.com  //该域名已向DDNS服务提供商申请注册
#
ipsec policy policy1 10 isakmp  //配置安全策略
 security acl 3003
 ike-peer rut1
 proposal prop1
#
interface Dialer1  //配置拨号口相关参数
 link-protocol ppp
 ppp chap user user@huawei.com
 ppp chap password cipher %@%@l$S'&"Sm7!j4F#)i{{G#L3Wu%@%@
 ip address ppp-negotiate
 dialer user huawei
 dialer bundle 1
 dialer-group 1
 ddns policy ddnspolicy1  //拨号口上应用DDNS策略，使其接口IP地址发生变化时，能向DDNS服务器发送动态更新
 ipsec policy policy1  //拨号口上应用安全策略，使接口具有IPSec的保护功能
#
interface GigabitEthernet1/0/0   //在物理接口下绑定拨号口，建立PPPoE会话
 pppoe-client dial-bundle-number 1
#
interface Ethernet2/0/0
 ip address 10.1.2.1 255.255.255.0
#
dialer-rule  //配置拨号访问组，指定允许所有的IPv4报文通过
 dialer-rule 1 ip permit
#
ip route-static 0.0.0.0 255.255.255.0  dialer1
#
return
```

步骤3 验证配置结果

配置成功后，在PC A上执行**ping**操作仍然可以ping通PC B，它们之间的数据传输将被加密，执行命令**display ipsec statistics**可以查看数据包的统计信息。

分别在RouterA和RouterB上执行**display ike sa**和**display ipsec sa**命令，可以看到IPSec隧道上配置的信息。

----结束

配置注意事项

如果PPPoE拨号链路有震荡现象，即拨号口IP地址经常变化，导致拨号口IP地址变化后无法重新建立IPSec隧道，可以采用以下方法：

- 如果两端都配置了安全策略，需要在两端设备上配置对等体存活检测DPD功能，通过DPD检测对端故障，重新建立IPSec隧道。
- 如果一端配置了安全策略，一端配置了策略模板，可以在配置了策略模板的那端执行**ipsec remote traffic-identical accept**命令（该命令从V2R3C00版本开始支

持），使能保护相同数据流的新用户接入总部功能，使分支网关与总部网关之前的建立IPSec SA迅速老化，以重新建立IPSec隧道。

6.4.17 配置出差用户利用 L2TP over IPSec 隧道接入总部的示例

规格

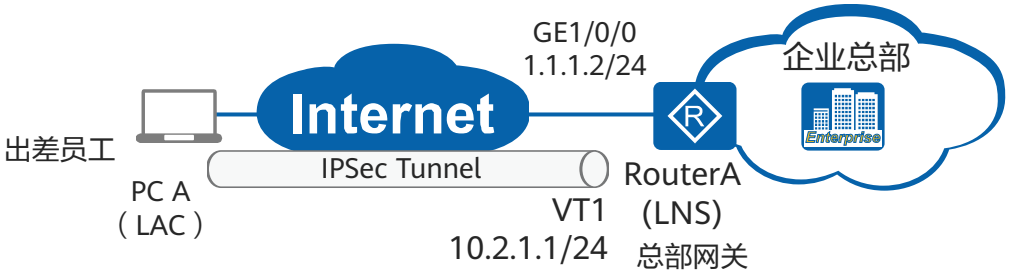
适用于所有版本、所有形态的路由器。

组网需求

如图6-50所示，某企业使用RouterA作为总部网关。企业的出差员工用PC A通过公网与总部建立通信。为了保证出差员工接入内网的安全性，企业希望在出差员工和总部网关之间建立一个L2TP over IPSec隧道。

本示例配置步骤在PC终端上以Windows 7系统为例。

图 6-50 配置 PC 与路由器建立 L2TP over IPSec 隧道组网图



操作步骤

步骤1 配置RouterA

```
#
 sysname RouterA  //配置设备名称
#
 l2tp enable  //开启L2TP功能
#
ipsec proposal prop  //配置IPSec安全提议
 encapsulation-mode transport
#
ike proposal 5  //配置IKE安全提议
 encryption-algorithm aes-cbc-128  //V200R008及之后的版本，aes-cbc-128参数修改为aes-128
 authentication-algorithm sha2-256
#
ike peer peer1 v1  //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 pre-shared-key cipher %^%#JvZxR2g8c;a9~FPN~n'$7`DEV&=G(=Et02P/%\*!%^%#  //配置预共享密钥
 ike-proposal 5
#
ipsec policy-template temp1 10  //配置策略模板
 ike-peer peer1
 proposal prop
```


版权所有 © 华为技术有限公司

```
#
ipsec policy policy1 10 isakmp template temp1  //配置安全策略
#
ip pool 1  //配置IP地址池为L2TP客户端分配地址
 gateway-list 10.2.1.1
 network 10.2.1.0 mask 255.255.255.0
#
aaa  //配置AAA本地认证，用户名为vpdnuser，密码为YsHsjx_202206
 authentication-scheme l2tp
  authentication-mode local
 domain l2tp
  authentication-scheme l2tp
 local-user vpdnuser password cipher %^%#!~$GMN5Gj=j&f)IjQ8\>~b\-1"i^b@~.)+,2gi9K%^%#
 local-user vpdnuser privilege level 0
 local-user vpdnuser service-type ppp
#
interface GigabitEthernet1/0/0
 ip address 1.1.1.2 255.255.255.0
 ipsec policy policy1
#
interface Virtual-Template1  //创建VT虚拟接口模板，配置拨号参数
 ppp authentication-mode chap domain l2tp  //配置认证方式时必须携带域名
 remote address pool 1  //引用IP地址池
 ip address 10.2.1.1 255.255.255.0
#
l2tp-group 1  //创建L2TP组，配置L2TP连接参数
 undo tunnel authentication  //手机拨号接入，建议关闭隧道验证功能
 allow l2tp virtual-template 1
#
ip route-static 0.0.0.0 0.0.0.0 1.1.1.1  //配置静态路由，保证两端路由可达
ip route-static 10.2.1.0 255.255.255.0 Virtual-Template1
#
return
```

步骤2 配置出差用户的个人PC。以下为Windows 7系统的示例。

1. 查看IPSec服务状态，保证IPSec服务开启。
   a. 在“开始 > 运行”中，输入**services.msc**命令，单击“确定”，进入“服务”界面。
   b. 在“名称”一列中，查看“IPsec Policy Agent”的状态，确保状态为“已启用”。如果不为“已启用”，请右键单击“IPsec Policy Agent”，选择“属性”，在“属性”中设置“启动类型”为**自动**，单击“应用”。之后在“服务状态”中选择“启动”。
   c. 关闭“服务”界面。
2. 创建L2TP over IPSec连接。
   a. 选择“开始 > 控制面板”。
   b. 选择“网络和Internet”。
   c. 打开“网络和共享中心”。
   d. 选择“设置新的连接或网络”。
   e. 选择“连接到工作区”。
   f. 选择“使用我的Internet连接”。
   g. 设置Internet地址和目标名称。

      Internet地址设置为RouterA外网接口的IP地址（域名固定的情况下，可以填写固定域名）。
   h. 设置用户名、密码。
   i. 设置完成后，单击“连接”。

 版权所有 © 华为技术有限公司

j. 单击“跳过”，跳过验证过程。显示“连接已经可用”后，单击“关闭”。

3. 设置IKE连接参数。
   a. 在“网络和共享中心”左侧区域中选择“更改适配器设置”。
   b. 在新建的VPN连接处，单击鼠标右键并选择“属性”。
   c. 设置“选项”，选择“连接时显示进度”。
   d. 设置“安全”，在“VPN类型”中选择“使用IPsec的第2层隧道协议”，在“数据加密”中选择“需要加密”，并点击“高级设置”，选择“使用预共享的密钥作身份验证”，并输入密钥。
   e. 设置“网络”，选择“Internet 协议版本 4”。

步骤3 验证配置结果

配置成功后，PC A使用系统自带软件进行拨号，拨号成功。

在RouterA上执行命令**display l2tp tunnel**，可以看到L2TP隧道建立成功。

在RouterA上执行命令**display ike sa**，可以看到SA建立成功。

----结束

配置注意事项

- 两端用于IKE协商的预共享密钥保持一致。
- L2TP客户端软件不支持隧道验证时，需在设备上关闭隧道验证功能。
- 出差员工与总部之间是建立基于主机到网关的IPSec隧道，因此需要基于传输模式建立IPSec隧道。

6.4.18 配置手工和 IKE 协商混合建立 IPSec 隧道示例

规格

适用于所有版本、所有形态的AR路由器。

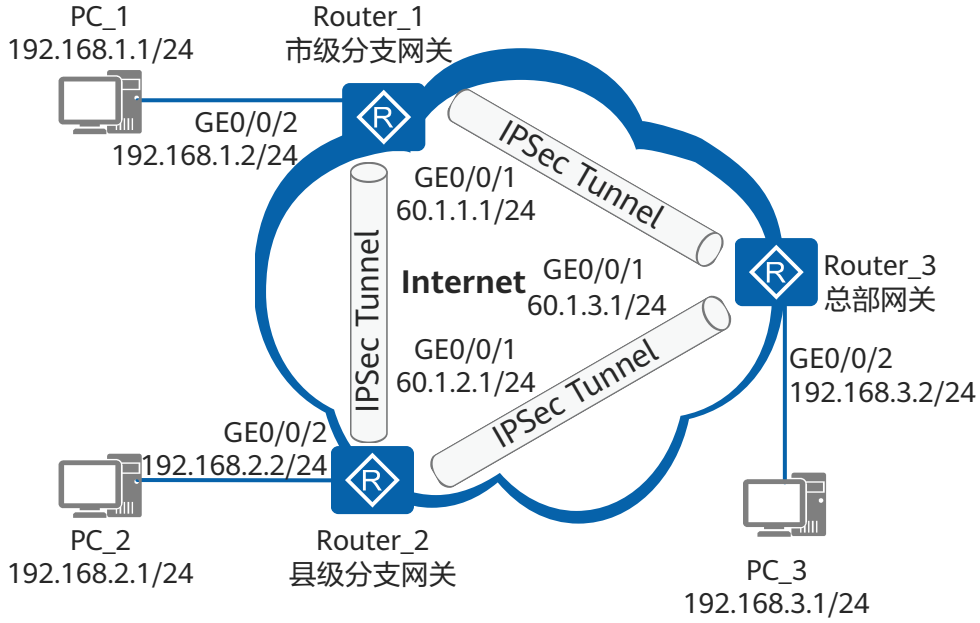
组网需求

如图6-51所示，Router_1和Router_2分别为某企业的市级分支网关和县级分支网关，Router_3为企业总部网关，分支与总部通过公网建立通信。市级分支少，县级分支多。

企业希望县级分支可直接与总部和市级分支互通、市级分支与总部互通，并且对分支与总部之间相互访问的流量进行安全保护。

 版权所有 © 华为技术有限公司

图 6-51 配置手工和 IKE 协商混合建立 IPSec 隧道示例组网图



操作步骤

步骤1 配置市级分支网关Router_1

```
#
 sysname Router_1
#
acl number 3001   //采用策略模板方式时，引用ACL是可选操作,因此只需在Router_1上定义到总部的数据流
 rule 5 permit ip source 192.168.1.0 0.0.0.255 destination 192.168.3.0 0.0.0.255
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256
#
ipsec policy policy1 10 manual   //配置手工方式安全策略，用于与总部建立IPSec隧道
 security acl 3001
 proposal tran1
 tunnel local 60.1.1.1
 tunnel remote 60.1.3.1
 sa spi inbound esp 12345    //配置入方向SA的安全参数索引，需与总部出方向SA的安全参数索引一致
 sa string-key inbound esp cipher %^%#zxX++-NU.;$%h;BB9zu1|7(EKNwdZAHC"EPP1y{S%^%#    //配置入方向SA的认证密钥为“YsHsjx_202206”，需与总部出方向SA的认证密钥一致
 sa spi outbound esp 54321   //配置出方向SA的安全参数索引，需与总部入方向SA的安全参数索引一致
 sa string-key outbound esp cipher %^%#$~1!;0~-Z8a5n\2'#~J'L`eOO>i7iMm*mY173mG7%^%#   //配置出方向SA的认证密钥为“YsHsjx_202206”，需与总部入方向SA的认证密钥一致
#
ike proposal 5
 encryption-algorithm aes-cbc-256   //V200R008及之后的版本，aes-cbc-256参数修改为aes-256
 dh group2
 authentication-algorithm sha2-256
 prf hmac-sha2-256
#
ike peer rut1 v2   //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 pre-shared-key cipher %^%#]%qh%KV&]('NP)+OE3VF"nAn7VF%/+EgfmX3BE|*%^%#   //配置预共享密钥为“YsHsjx_202206”，以密文显示；在V2R3C00以前版本中以明文显示，显示为“pre-shared-key
```


版权所有 © 华为技术有限公司

```
YsHsjx_202206”
 ike-proposal 5
#
ike identity identity1   //配置身份过滤集，指定符合条件的县级分支接入
 name huaweirt2   //V200R008及之后的版本，设备不支持命令name，其命令功能等同于命令fqdn
 ip address 60.1.2.0 255.255.255.0
#
ipsec policy-template use1 20
 ike-peer rut1
 proposal tran1
 match ike-identity identity1
#
ipsec policy policy1 20 isakmp template use1  //配置策略模板方式安全策略，用于与县级分支建立IPSec隧道
#
interface GigabitEthernet0/0/1     //配置互联接口，用于建立IKE连接和隧道封装外层IP地址
 ip address 60.1.1.1 255.255.255.0
 ipsec policy policy1     //在接口绑定安全策略组，开启IPSec保护功能
#
interface GigabitEthernet0/0/2    //配置连接业务网段的接口
 ip address 192.168.1.2 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 60.1.1.2   //配置静态路由
#
return
```

步骤2 配置县级分支网关Router_2

```
#
 sysname Router_2
#
 ike local-name huaweirt2
#
acl number 3001
 rule 5 permit ip source 192.168.2.0 0.0.0.255 destination 192.168.3.0 0.0.0.255
acl number 3002
 rule 5 permit ip source 192.168.2.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256
#
ike proposal 5
 encryption-algorithm aes-cbc-256   //V200R008及之后的版本，aes-cbc-256参数修改为aes-256
 dh group2
 authentication-algorithm sha2-256
 prf hmac-sha2-256
#
ike peer rut1 v2  //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 pre-shared-key cipher %^%#bkSqG8J"h(w42U.X6W!C@P.f3tfZB3.&|V04Q}(O%^%#   //配置预共享密钥为“YsHsjx_202206”，以密文显示；在V2R3C00以前版本中以明文显示，显示为“pre-shared-key YsHsjx_202206”
 ike-proposal 5
 remote-address 60.1.3.1
#
ike peer rut2 v2   //配置IKE对等体，用于与市级分支协商建立IPSec隧道，须配置remote address
 pre-shared-key cipher %^%#F[de7*vUZ9ZT)V5UEqX(g|)XG`S)xT}:C."&>c].%^%#   //配置预共享密钥为“YsHsjx_202206”，以密文显示；在V2R3C00以前版本中以明文显示，显示为“pre-shared-key YsHsjx_202206”
 ike-proposal 5
 remote-address 60.1.1.1
#
ipsec policy policy1 10 isakmp  //配置安全策略，用于与总部建立IPSec隧道
 security acl 3001
 ike-peer rut1
 proposal tran1
```

 版权所有 © 华为技术有限公司

```
ipsec policy policy1 20 isakmp  //配置安全策略，用于与市级分支建立IPSec隧道
 security acl 3002
 ike-peer rut2
 proposal tran1
#
interface GigabitEthernet0/0/1    //配置互联接口，用于建立IKE连接和隧道封装外层IP地址
 ip address 60.1.2.1 255.255.255.0
 ipsec policy policy1   //在接口绑定安全策略组，开启IPSec保护功能
#
interface GigabitEthernet0/0/2    //配置连接业务网段的接口
 ip address 192.168.2.2 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 60.1.2.2   //配置静态路由
#
return
```

步骤3 配置总部网关Router_3

```
#
 sysname Router_3
#
acl number 3001   //采用策略模板方式时，引用ACL是可选操作,因此只需在Router_3上定义到市级分支的数据流
 rule 5 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256
#
ipsec policy policy1 10 manual     //配手工方式安全策略，用于与市级分支建立IPSec隧道
 security acl 3001
 proposal tran1
 tunnel local 60.1.3.1
 tunnel remote 60.1.1.1
 sa spi inbound esp 54321      //配置入方向SA的安全参数索引，需与市级分支出方向SA的安全参数索引一致
 sa string-key inbound esp cipher %^%#$~1!;0~-Z8a5n\2'#~J'L`eOO>i7iMm*mY173mG7%^%#      //配置入方向SA的认证密钥为“YsHsjx_202206”，需与市级分支出方向SA的认证密钥一致
 sa spi outbound esp 12345     //配置出方向SA的安全参数索引，需与市级分支入方向SA的安全参数索引一致
 sa string-key outbound esp cipher %^%#zxX++-NU.;$%h;BB9zu1|7(EKNwdZAHC"EPP1y{S%^%#     //配置出方向SA的认证密钥为“YsHsjx_202206”，需与市级分支入方向SA的认证密钥一致
#
ike proposal 5
 encryption-algorithm aes-cbc-256   //V200R008及之后的版本，aes-cbc-256参数修改为aes-256
 dh group2
 authentication-algorithm sha2-256
 prf hmac-sha2-256
#
ike peer rut1 v2  //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 pre-shared-key cipher %^%#SNMkBqDAZOwo!9=MwR{+h;Bp"JEU.-s!Z=Wdu7_@%^%#   //配置预共享密钥为“YsHsjx_202206”，以密文显示；在V2R3C00以前版本中以明文显示，显示为“pre-shared-key YsHsjx_202206”
 ike-proposal 5
#
ike identity identity1     //配置身份过滤集，指定符合条件的县级分支接入
 name huaweirt2   //V200R008及之后的版本，设备不支持命令name，其命令功能等同于命令fqdn
 ip address 60.1.2.0 255.255.255.0
#
ipsec policy-template use1 20
 ike-peer rut1
 proposal tran1
 match ike-identity identity1
#
ipsec policy policy1 20 isakmp template use1  //配置策略模板方式安全策略，用于与县级分支建立IPSec隧道
#
interface GigabitEthernet0/0/1    //配置互联接口，用于建立IKE连接和隧道封装外层IP地址
 ip address 60.1.3.1 255.255.255.0
```

 版权所有 © 华为技术有限公司

```
 ipsec policy policy1    //在接口绑定安全策略组，开启IPSec保护功能
#
interface GigabitEthernet0/0/2    //配置连接业务网段的接口
 ip address 192.168.3.2 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 60.1.3.2    //配置静态路由
#
return
```

步骤4 验证配置结果

配置成功后：

- 分别在主机PC_1和主机PC_2执行**ping**操作仍然可以ping通主机PC_3，执行命令**display ipsec statistics**查看IPSec处理报文的统计信息，“Inpacket decap count/Outpacket encap count”（V200R008之前的版本）或者“input/output security packets”（V200R008及之后的版本）字段的计数值不为0，表明分支和总部之间的数据传输被加密。
- 分别在Router_1、Router_2和Router_3上执行**display ipsec sa**命令查看建立的SA，可以看到输出信息中“Tunnel remote”字段（即隧道目的地址）和“Mode”字段（即建立IPSec隧道的安全策略模式）的取值如下：
  - Router_1上，隧道目的地址为60.1.3.1的安全策略模式为“Manual”；隧道目的地址为60.1.2.1的安全策略模式为“Template”。
  - Router_2上，隧道目的地址为60.1.1.1和60.1.3.1的安全策略模式均为“ISAKMP”。
  - Router_3上，隧道目的地址为60.1.1.1的安全策略模式为“Manual”；隧道目的地址为60.1.2.1的安全策略模式为“Template”。
- 分别在Router_1、Router_2和Router_3上执行**display ike sa v2**（V200R008及之后的版本不支持配置**V2**参数）命令查看通过IKE协商建立的SA，可以看到：
  - Router_1上只有“Peer”为“60.1.2.1”的表项。
  - Router_2上有“Peer”为“60.1.1.1”和“60.1.3.1”的表项。
  - Router_3上只有“Peer”为“60.1.2.1”的表项。

----结束

配置注意事项

- 采用策略模板方式建立IPSec隧道时，在IKE对等体的配置中不要指定对端的名称或IP地址。
- IKE对等体之间要采用相同的pre-share-key。
- 在配置手工方式安全策略时，用户必须配置入方向和出方向SA的SPI。并且本端的入方向SA的SPI必须和对端的出方向SA的SPI一样、本端的出方向SA的SPI必须和对端的入方向的SPI一样。

6.4.19 配置分支采用多链路共享功能与总部建立 IPSec 隧道示例

规格

适用于所有版本、所有形态的路由器。

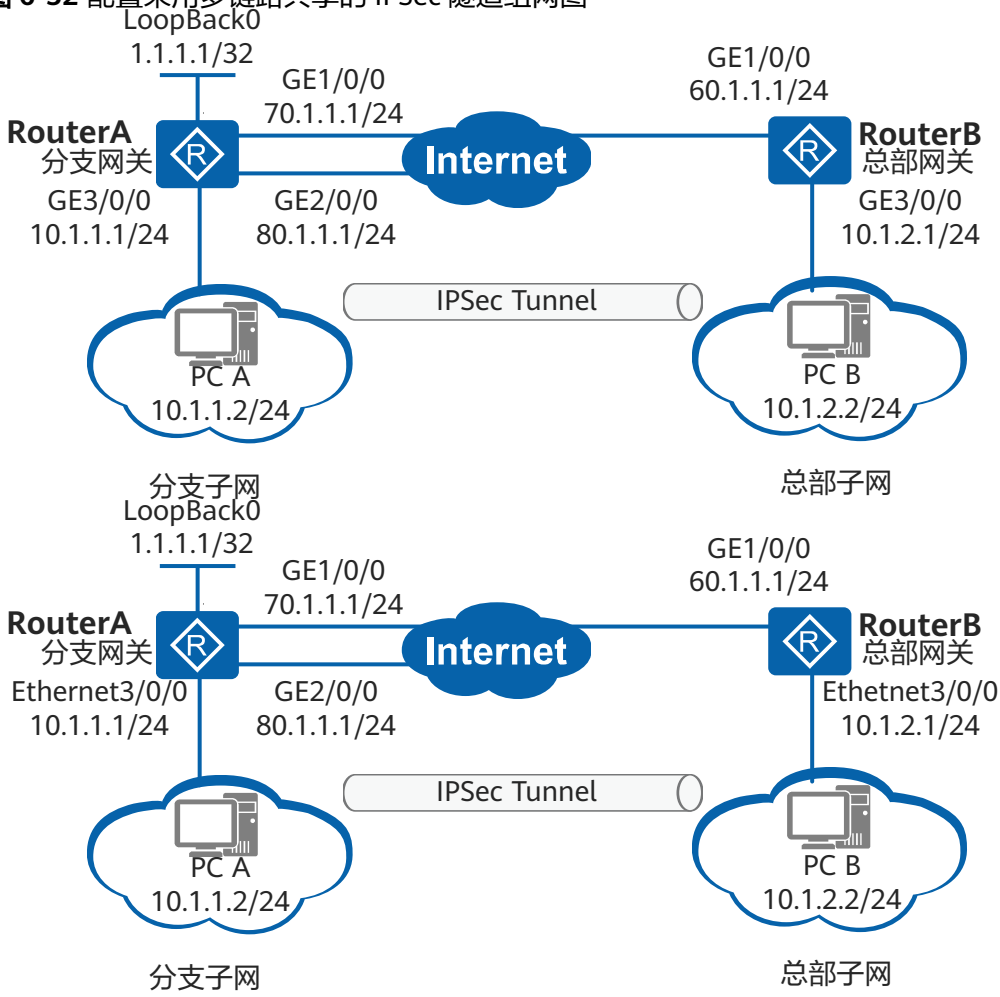
 版权所有 © 华为技术有限公司

组网需求

如图6-52所示，RouterA为企业分支网关，RouterB为企业总部网关，分支采用两条出口链路互为备份或者负载分担，与总部通过公网建立通信。分支子网为10.1.1.0/24，总部子网为10.1.2.0/24。

企业希望对分支子网与总部子网之间相互访问的流量进行安全保护，并且若主备链路切换或某条出口链路故障时，要求安全保护不中断。

图 6-52 配置采用多链路共享的 IPSec 隧道组网图



操作步骤

步骤1 RouterA的配置

```
#
 sysname RouterA
#
acl number 3101  //配置ACL 3101，匹配从分支子网到总部子网的流量
 rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
#
ipsec proposal prop  //配置IPSec安全提议
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-128
#
```


版权所有 © 华为技术有限公司

```
ike proposal 5  //配置IPSec IKE安全提议
 encryption-algorithm aes-cbc-128  //V200R008及之后的版本，aes-cbc-128参数修改为aes-128
 dh group2
 authentication-algorithm sha2-256
 prf hmac-sha2-256
#
ike peer rut v1  //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 pre-shared-key cipher %^%#JvZxR2g8c;a9~FPN~n'$7`DEV&=G(=Et02P/%\*!%^%#  //配置预共享密钥认证字为“YsHsjx_202206”，以密文显示，该命令在V2R3C00以前的版本中为“pre-shared-key YsHsjx_202206”，以明文显示
 ike-proposal 5
 remote-address 60.1.1.1
#
ipsec policy policy1 10 isakmp  //配置IPSec策略
 security acl 3101
 ike-peer rut
 proposal prop
#
ipsec policy policy1 shared local-interface LoopBack0  //配置安全策略组为共享安全策略组
#
interface GigabitEthernet1/0/0
 ip address 70.1.1.1 255.255.255.0
 ipsec policy policy1  //绑定IPSec安全策略组
#
interface GigabitEthernet2/0/0
 ip address 80.1.1.1 255.255.255.0
 ipsec policy policy1  //绑定IPSec安全策略组
#
interface GigabitEthernet3/0/0  ip address 10.1.1.1 255.255.255.0
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
ip route-static 10.1.2.0 255.255.255.0 70.1.1.2 preference 10  //配置一条RouterA的GE1/0/0接口到目的地址是总部内网的静态路由
ip route-static 10.1.2.0 255.255.255.0 80.1.1.2 preference 20  //配置一条RouterA的GE2/0/0接口到目的地址是总部内网的静态路由
ip route-static 60.1.1.0 255.255.255.0 70.1.1.2 preference 10  //配置一条RouterA的GE1/0/0接口到目的地址是总部外网出口的静态路由
ip route-static 60.1.1.0 255.255.255.0 80.1.1.2 preference 20  //配置一条RouterA的GE2/0/0接口到目的地址是总部外网出口的静态路由
#
return
```

步骤2 RouterB的配置

```
#
 sysname RouterB
#
acl number 3101  //配置ACL 3101，匹配从总部子网到分支子网的流量
 rule 5 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
#
ipsec proposal prop  //配置IPSec安全提议
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-128
#
ike proposal 5  //配置IPSec IKE安全提议
 encryption-algorithm aes-cbc-128  //V200R008及之后的版本，aes-cbc-128参数修改为aes-128
 dh group2
 authentication-algorithm sha2-256
 prf hmac-sha2-256
#
ike peer rut v1  //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和
```

```
IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 pre-shared-key cipher %^%#K{JG:rWVHPMnf;5\|,GW(Luq'qi8BT4nOj%5W5=)%^%#  //配置预共享密钥认证字为“YsHsjx_202206”，以密文显示，该命令在V2R3C00以前的版本中为“pre-shared-key YsHsjx_202206”，以明文显示
 ike-proposal 5
 remote-address 1.1.1.1
#
ipsec policy policy1 10 isakmp  //配置IPSec策略
 security acl 3101
 ike-peer rut
 proposal prop
#
interface GigabitEthernet1/0/0
 ip address 60.1.1.1 255.255.255.0
 ipsec policy policy1
#
interface GigabitEthernet3/0/0  ip address 10.1.2.1 255.255.255.0
#
ip route-static 1.1.1.1 255.255.255.255 60.1.1.2  //配置一条目的地址是对端设备LoopBack接口的静态路由
ip route-static 10.1.1.0 255.255.255.0 60.1.1.2  //配置一条目的地址是分支内网的静态路由
ip route-static 70.1.1.0 255.255.255.0 60.1.1.2  //配置一条目的地址是分支外网出口GE1/0/0的静态路由
ip route-static 80.1.1.0 255.255.255.0 60.1.1.2  //配置一条目的地址是分支外网出口GE2/0/0的静态路由
#
return
```

步骤3 验证配置结果

在RouterA上执行**display ike sa verbose**和**display ipsec sa**命令，可以查看IPSec隧道上配置的信息。

----结束

配置注意事项

- 分支的ACL需要与总部ACL互为镜像。
- 总部和分支之间的外网地址路由可达。
- 所有的IPSec策略都绑定在对应的外网出接口上。
- 总部和各个分支之间都采用相同的pre-shared-key。

6.4.20 配置 IPSec 反向路由注入功能示例

规格

适用于V200R002C00及更高版本、所有形态的AR路由器。

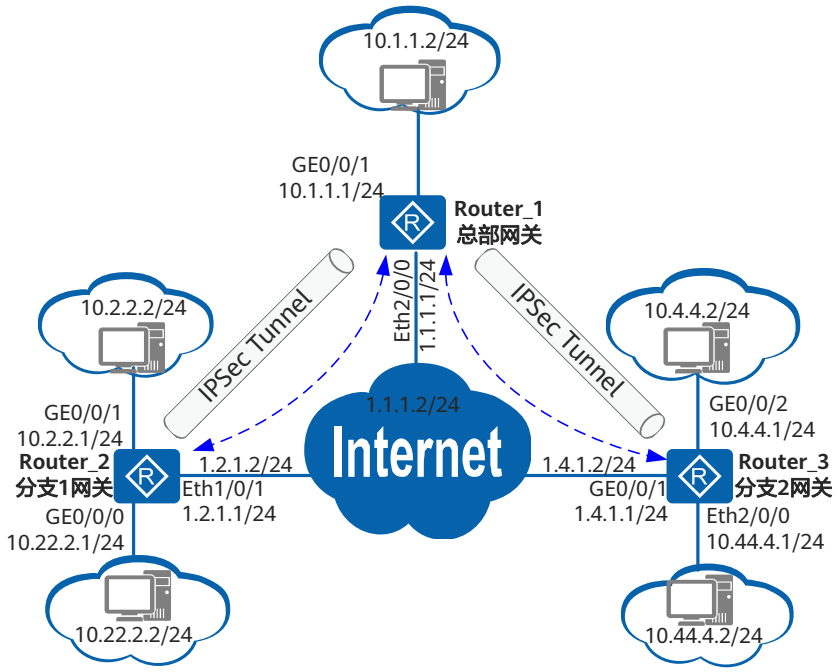
组网需求

如图6-53所示，某企业分支与总部通过公网建立通信，Router_1为总部网关，Router_2和Router_3分别为分支1和分支2的网关。分支连接有多个私网网络，企业总部网关需要配置大量静态路由，以便将总部发往分支的数据引到IPSec隧道上来，并且当企业分支内部网络规划发生变化时，需要调整总部网关上的静态路由配置，工作量大且容易出现配置错误。

企业希望分支与总部之间相互访问的流量进行安全保护，且减少总部网关配置和维护的工作量。

 版权所有 © 华为技术有限公司

图 6-53 配置 IPSec 反向路由注入功能组网图



操作步骤

步骤1 配置Router_1

```
#
 sysname Router_1
#
ipsec proposal def
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256
#
ike proposal 5
 encryption-algorithm aes-cbc-256   //V200R008及之后的版本，aes-cbc-256参数修改为aes-256
 dh group2
 authentication-algorithm sha2-256
 prf hmac-sha2-256
#
ike peer center v1    //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 pre-shared-key cipher %^%#bkSqG8J"h(w42U.X6W!C@P.f3tfZB3.&|V04Q}(O%^%#    //配置预共享密钥为“YsHsjx_202206”，以密文显示；在V2R3C00以前版本中以明文显示，显示为“pre-shared-key YsHsjx_202206”
 ike-proposal 5
 local-address 1.1.1.1
#
ipsec policy-template center 1     //配置IPSec策略模板
 ike-peer center
 proposal def
```


版权所有 © 华为技术有限公司

```
 route inject dynamic     //配置动态路由注入功能，自动添加总部到分支子网的静态路由
#
ipsec policy hk 1 isakmp template center  //配置IPSec策略
#
interface Ethernet2/0/0       //配置互联接口，用于建立IKE连接和隧道封装外层IP地址
 ip address 1.1.1.1 255.255.255.0
 ipsec policy hk      //配置接口下绑定IPSec策略
#
interface GigabitEthernet0/0/1
 ip address 10.1.1.1 255.255.255.0  //配置连接业务网段的接口
#
 ip route-static 1.2.1.0 255.255.255.0 1.1.1.2  //配置总部到分支1外网的静态路由
 ip route-static 1.4.1.0 255.255.255.0 1.1.1.2  //配置总部到分支2外网的静态路由
#
return
```

步骤2 配置Router_2

```
#
 sysname Router_2
#
acl number 3000  //配置ACL 3000，定义了两条数据流
 rule 0 permit ip source 10.2.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
 rule 5 permit ip source 10.22.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
#
ipsec proposal def
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256
#
ike proposal 5
 encryption-algorithm aes-cbc-256   //V200R008及之后的版本，aes-cbc-256参数修改为aes-256
 dh group2
 authentication-algorithm sha2-256
 prf hmac-sha2-256
#
ike peer branch v1  //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 pre-shared-key cipher %^%#bkSqG8J"h(w42U.X6W!C@P.f3tfZB3.&|V04Q}(O%^%#    //配置预共享密钥为“YsHsjx_202206”，以密文显示;在V2R3C00以前版本中以明文显示，显示为“pre-shared-key YsHsjx_202206”
 ike-proposal 5
 local-address 1.2.1.1
 remote-address 1.1.1.1
#
ipsec policy hk 1 isakmp  //配置IPSec策略
 security acl 3000
 ike-peer branch
 proposal def
#
interface Ethernet1/0/1  //配置互联网接口，用于建立IKE和IPSec隧道外层封装IP地址
 ip address 1.2.1.1 255.255.255.0
 ipsec policy hk
#
interface GigabitEthernet0/0/0
 ip address 10.22.2.1 255.255.255.0  //配置连接业务网段的接口1
#
interface GigabitEthernet0/0/1
 ip address 10.2.2.1 255.255.255.0  //配置连接业务网段的接口2
#
 ip route-static 1.1.1.0 255.255.255.0 1.2.1.2  //配置分支1到总部外网的静态路由
 ip route-static 10.1.1.0 255.255.255.0 1.2.1.2  //配置分支1到总部内网静态路由
#
return
```

步骤3 配置Router_3

```
#
 sysname Router_3
#
acl number 3000  //ACL 3000配置，定义了两条数据流
 rule 0 permit ip source 10.4.4.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
 rule 5 permit ip source 10.44.4.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
#
ipsec proposal def
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256
#
ike proposal 5
 encryption-algorithm aes-cbc-256   //V200R008及之后的版本，aes-cbc-256参数修改为aes-256
 dh group2
 authentication-algorithm sha2-256
 prf hmac-sha2-256
#
ike peer branch v1  //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 pre-shared-key cipher %^%#bkSqG8J"h(w42U.X6W!C@P.f3tfZB3.&|V04Q}(O%^%#    //配置预共享密钥为“YsHsjx_202206”，以密文显示;在V2R3C00以前版本中以明文显示，显示为“pre-shared-key YsHsjx_202206”
 ike-proposal 5
 local-address 1.4.1.1
 remote-address 1.1.1.1
#
ipsec policy hk 1 isakmp  //配置IPSec策略
 security acl 3000
 ike-peer branch
 proposal def
#
interface GigabitEthernet0/0/1  //配置互联网接口，用于建立IKE和IPSec隧道外层封装IP地址
 ip address 1.4.1.1 255.255.255.0
 ipsec policy hk
#
interface Ethernet2/0/0
 ip address 10.44.4.1 255.255.255.0  //配置连接业务网段的接口1
#
interface GigabitEthernet0/0/2
 ip address 10.4.4.1 255.255.255.0  //配置连接业务网段的接口2
#
 ip route-static 1.1.1.0 255.255.255.0 1.4.1.2  //配置分支2到总部外网的静态路由
 ip route-static 10.1.1.0 255.255.255.0 1.4.1.2  //配置分支2到总部内网静态路由
#
return
```

步骤4 验证配置结果

配置成功后：

- 分支主机上执行**ping**操作仍然可以ping通总部主机，执行命令**display ipsec statistics**查看IPSec处理报文的统计信息，“Inpacket decap count/Outpacket encap count”（V200R008之前的版本）或者“input/output security packets”（V200R008及之后的版本）字段的计数值不为0，表明分支和总部之间的数据传输被加密。
- 在分支网关和总部网关上执行命令**display ike sa**，可以查看到安全联盟的相关信息。
- 在总部网关上执行命令**display ip routing-table**，可以看到总部到分支子网的路由表项，目的地址分别为10.2.2.0/24、10.22.2.0/24、10.4.4.0/24、

 版权所有 © 华为技术有限公司

10.44.4.0/24，下一跳地址为1.1.1.1，且“Proto”字段的取值为**Unr**，表明为注入路由。

----结束

配置注意事项

- 总部采用策略模板方式建立IPSec隧道时，在IKE对等体的配置中不要指定对端的名称或IP地址。
- 总部和各个分支之间都采用相同的pre-share-key。
- 总部和各分支之间的外网地址路由可达。
- 只有IKE动态协商的SA才支持路由注入功能，手工方式生成的SA不支持路由注入功能。

6.4.21 配置对 IPSec 隧道内流量进行 QoS 保证示例

规格

适用于V200R003C00及更高版本、所有形态的AR路由器。

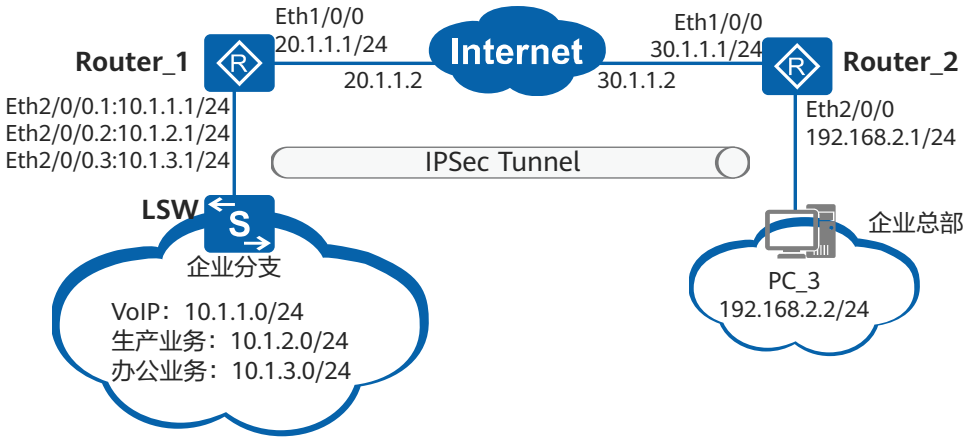
组网需求

如图6-54所示，某企业分支与总部通过公网进行通信，Router_1为分支网关，Router_2为总部的网关，分支出口到公网的带宽为2M。企业总部与分支间主要有VoIP、生产、办公三种业务流。

企业希望分支与总部之间相互访问的流量得到安全保护，且对VoIP、生产、办公三种业务流按照如下规划进行QoS保证：

- 对于VoIP业务流，需要确保低延时，并保障500Kbps带宽，设置IP优先级为5。
- 对于生产业务流，需要保障600Kbps带宽，设置IP优先级为4。
- 对于办公业务流，需要保障800Kbps带宽，设置IP优先级为2。

图 6-54 配置对 IPSec 隧道内流量进行 QoS 保证示例组网图



版权所有 © 华为技术有限公司

操作步骤

步骤1 配置Router_1

说明

LSW下行连接终端的接口配置为Access类型，并加入VoIP、生产业务、办公业务所属的VLAN；上行连接Router_1的接口配置为Trunk类型，并允许VoIP、生产业务、办公业务所属VLAN通过。具体配置请参考使用产品的配置手册。

```
#
 sysname Router_1
#
 ike local-name huawei01
#
acl number 3001  //配置ACL，定义VoIP业务流
 rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
acl number 3002  //配置ACL，定义生产业务流
 rule 5 permit ip source 10.1.2.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
acl number 3003  //配置ACL，定义办公业务流
 rule 5 permit ip source 10.1.3.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
#
ipsec proposal tran1  //配置IPSec安全提议
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256
#
ike proposal 1  //配置IKE安全提议
 encryption-algorithm aes-cbc-256   //V200R008及之后的版本，aes-cbc-256参数修改为aes-256
 dh group2
 authentication-algorithm sha2-256
 prf hmac-sha2-256
#
ike peer branch v1  //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 exchange-mode aggressive
 pre-shared-key cipher %^%#bkSqG8J"h(w42U.X6W!C@P.f3tfZB3.&|V04Q}(O%^%#    //配置预共享密钥为“YsHsjx_202206”，以密文显示；在V2R3C00以前版本中以明文显示，显示为“pre-shared-key YsHsjx_202206”
 ike-proposal 1
 local-id-type name   //配置IKE协商时本端的ID类型。V200R008及之后的版本，name参数修改为fqdn
 remote-name huawei02   //配置对端IKE peer名称。V200R008及之后的版本，设备不支持命令remote-name，其命令功能等同于命令remote-id
 local-address 20.1.1.1
 remote-address 30.1.1.1
#
ipsec policy map1 10 isakmp  //配置VoIP业务流的IPSec策略
 security acl 3001
 ike-peer branch
 proposal tran1
 qos pre-classify
ipsec policy map1 20 isakmp  //配置生产业务流的IPSec策略
 security acl 3002
 ike-peer branch
 proposal tran1
 qos pre-classify
ipsec policy map1 30 isakmp  //配置办公业务流的IPSec策略
 security acl 3003
 ike-peer branch
 proposal tran1
 qos pre-classify
#
traffic classifier tc2 operator or
 if-match acl 3001
traffic classifier tc1 operator or
 if-match acl 3002
```

 版权所有 © 华为技术有限公司

```
traffic classifier tc3 operator or
 if-match acl 3003
#
traffic behavior tb1
 car cir 500 cbs 94000 pbs 156500 mode color-blind green pass yellow pass red discard
 remark local-precedence ef
traffic behavior tb3
 car cir 800 cbs 150400 pbs 250400 mode color-blind green pass yellow pass red discard
 remark local-precedence af2
traffic behavior tb2
 car cir 600 cbs 112800 pbs 187800 mode color-blind green pass yellow pass red discard
 remark local-precedence af4
#
traffic policy tp1
 classifier tc1 behavior tb1 precedence 5
 classifier tc2 behavior tb2 precedence 10
 classifier tc3 behavior tb3 precedence 15
#
interface Ethernet1/0/0  //配置外网接口
 ip address 20.1.1.1 255.255.255.0
 traffic-policy tp1 outbound
 ipsec policy map1
#
interface Ethernet2/0/0   //配置私网接口
#
interface Ethernet2/0/0.1
 dot1q termination vid 10           //终结VoIP业务流所属VLAN，并使用arp broadcast enable使能子接口的ARP
广播功能（缺省已使能）
 ip address 10.1.1.1 255.255.255.0
#
interface Ethernet2/0/0.2
 dot1q termination vid 20          //终结生产业务流所属VLAN，并使用arp broadcast enable使能子接口的ARP
广播功能（缺省已使能）
 ip address 10.1.2.1 255.255.255.0
#
interface Ethernet2/0/0.3
 dot1q termination vid 30         //终结办公业务流所属VLAN，并使用arp broadcast enable使能子接口的ARP广
播功能（缺省已使能）
 ip address 10.1.3.1 255.255.255.0
#
 ip route-static 192.168.2.0 255.255.255.0 20.1.1.2   //配置分支到总部内网的静态路由
 ip route-static 30.1.1.0 255.255.255.0 20.1.1.2      //配置分支到总部外网的静态路由
#
return
```

步骤2 配置Router_2

```
#
 sysname Router_2
#
 ike local-name huawei02
#
acl number 3001  //配置ACL，定义VoIP业务流
 rule 5 permit ip source 192.168.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
acl number 3002  //配置ACL，定义生产业务流
 rule 5 permit ip source 192.168.2.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
acl number 3003  //配置ACL，定义办公业务流
 rule 5 permit ip source 192.168.2.0 0.0.0.255 destination 10.1.3.0 0.0.0.255
#
ipsec proposal tran1  //配置IPSec安全提议
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-256
#
ike proposal 1  //配置IKE安全提议
 encryption-algorithm aes-cbc-256   //V200R008及之后的版本，aes-cbc-256参数修改为aes-256
 dh group2
 authentication-algorithm sha2-256
 prf hmac-sha2-256
#
ike peer center v1  //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本
```

命令为**ike peer** *peer-name* [**v1** | **v2**]。V200R008及之后的版本命令为**ike peer** *peer-name*和**version** { **1** | **2** }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令**undo version 2**；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令**version 1**，再执行命令**undo version 2**。

```
 exchange-mode aggressive
 pre-shared-key cipher %^%#bkSqG8J"h(w42U.X6W!C@P.f3tfZB3.&|V04Q}(O%^%#    //配置预共享密钥为“YsHsjx_202206”，以密文显示；在V2R3C00以前版本中以明文显示，显示为“pre-shared-key YsHsjx_202206”
 ike-proposal 1
 local-id-type name   //配置IKE协商时本端的ID类型。V200R008及之后的版本，name参数修改为fqdn
 remote-name huawei01   //配置对端IKE peer名称。V200R008及之后的版本，设备不支持命令remote-name，其命令功能等同于命令remote-id
 local-address 30.1.1.1
 remote-address 20.1.1.1
#
ipsec policy map1 10 isakmp  //配置VoIP业务流的IPSec策略
 security acl 3001
 ike-peer center
 proposal tran1
ipsec policy map1 20 isakmp  //配置生产业务流的IPSec策略
 security acl 3002
 ike-peer center
 proposal tran1
ipsec policy map1 30 isakmp  //配置办公业务流的IPSec策略
 security acl 3003
 ike-peer center
 proposal tran1
#
interface Ethernet1/0/0  //配置外网接口
 ip address 30.1.1.1 255.255.255.0
 ipsec policy map1
#
interface Ethernet2/0/0  //配置私网接口
 ip address 192.168.2.1 255.255.255.0
#
 ip route-static 10.1.1.0 255.255.255.0 30.1.1.2   //配置总部到分支内网VoIP业务网段的静态路由
 ip route-static 10.1.2.0 255.255.255.0 30.1.1.2   //配置总部到分支内网生产业务网段的静态路由
 ip route-static 10.1.3.0 255.255.255.0 30.1.1.2   //配置总部到分支内网办公业务网段的静态路由
 ip route-static 20.1.1.0 255.255.255.0 30.1.1.2   //配置总部到分支外网的静态路由
#
return
```

步骤3 验证配置结果

配置成功后，分别往Router_1的接口ETH2/0/0发送10000Kbps的VoIP、生产和办公业务流：

- 从接口ETH1/0/0发出的VoIP业务流带宽不低于500Kbps、生产业务流带宽不低于600Kbps、办公业务流带宽不低于800Kbps。
- 在Router_1的系统视图执行命令**capture-packet interface ethernet 1/0/0 destination terminal**，分别捕获接口ETH1/0/0发出的VoIP、生产和办公业务流，可以看到报文中的DSCP值分别为5、4、2。
- 在Router_1、Router_2上执行命令**display ipsec statistics**查看IPSec处理报文的统计信息，“Inpacket decap count/Outpacket encap count”（V200R008之前的版本）或者“input/output security packets”（V200R008及之后的版本）字段的计数值不为0，表明分支和总部之间的数据传输被加密。

----结束

配置注意事项

- 分支的ACL需要与总部ACL互为镜像。

 版权所有 © 华为技术有限公司

- 总部和各分支之间的外网地址路由可达。

6.4.22 配置分支机构通过 4G 接口访问 Internet，总部利用 IPSec 策略模板与分支建立 IPSec 隧道的示例

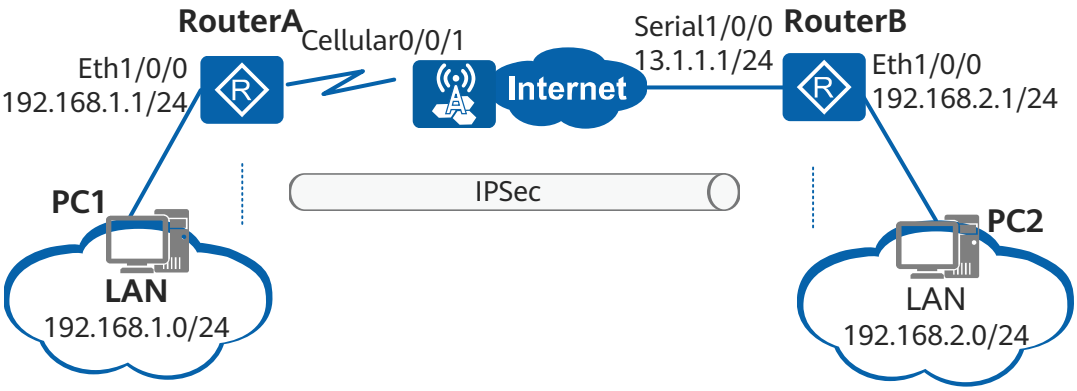
规格

适用于V200R002C00及更高版本、所有形态的AR路由器。

组网需求

企业总部需要和分支建立安全的IPSec连接。总部网关RouterB使用静态公网地址；分支规模较小，网关RouterA使用4G接口从服务商处动态获取IP地址访问公网。总部部署IPSec策略时需要知道分支的IP地址，但分支的IP地址经常发生变化，难以维护。此时可在总部使用IPSec策略模板，无需知道分支的IP地址，即可接入各分支发起的IPSec协商，且配置简单。

图 6-55 配置分支机构通过 4G 接口访问 Internet，总部利用 IPSec 策略模板与分支建立 IPSec 隧道的示例组网图



操作步骤

步骤1 配置RouterA

```
#
 sysname RouterA
#
acl number 3000  //配置IPSec保护的数据流
 rule 5 permit ip source 192.168.1.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
#
ipsec proposal rta  //配置IPSec的安全提议
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-192
#
ike proposal 5  //配置IKE提议
 encryption-algorithm aes-cbc-128  //V200R008及之后的版本，aes-cbc-128参数修改为aes-128
 dh group14
 authentication-algorithm sha2-256
#
ike peer rta v1  //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 },
```


版权所有 © 华为技术有限公司

```
如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 pre-shared-key cipher %^%#JvZxR2g8c;a9~FPN~n'$7`DEV&=G(=Et02P/%\*!%^%#  //配置预共享密钥认证字为“YsHsjx_202206”，以密文显示，该命令在V2R3C00以前的版本中为“pre-shared-key YsHsjx_202206”，以明文显示
 ike-proposal 5
 remote-address 13.1.1.1  //配置对等体的IP地址，向对端发起IKE协商
#
ipsec policy rta 1 isakmp  //配置IPSec策略
 security acl 3000
 ike-peer rta
 proposal rta
#
interface Ethernet1/0/0
 ip address 192.168.1.1 255.255.255.0
#
interface Cellular0/0/1  //配置4G接口拨号参数
 dialer enable-circular  //使能DCC轮询功能
 dialer-group 1  //将此拨号口加入拨号控制列表，其编号和控制列表中的规则编号一致
 apn-profile lteprofile
 dialer number *99# autodial  //按拨号串进行自动拨号
 ip address negotiate  //自动获取运营商分配的IP地址，接入公网
 ipsec policy rta  //在接口上绑定IPSec策略，发起IPSec协商
#
dialer-rule  //创建拨号控制列表，符合条件则触发拨号
 dialer-rule 1 ip permit
#
apn profile lteprofile  //创建APN模板
 apn ltenet
#
ip route-static 0.0.0.0 0.0.0.0 Cellular0/0/1
#
return
```

步骤2 配置RouterB

```
#
 sysname RouterB
#
ipsec proposal rtb
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-192
#
ike proposal 5  //配置IKE提议
 encryption-algorithm aes-cbc-128  //V200R008及之后的版本，aes-cbc-128参数修改为aes-128
 dh group14
 authentication-algorithm sha2-256
#
ike peer rtb v1  //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 pre-shared-key cipher %^%#K{JG:rWVHPMnf;5\|,GW(Luq'qi8BT4nOj%5W5=)%^%#  //配置预共享密钥认证字为“YsHsjx_202206”，以密文显示，该命令在V2R3C00以前的版本中为“pre-shared-key YsHsjx_202206”，以明文显示
 ike-proposal 5
#
ipsec policy-template temp 1  //配置IPSec策略模板，引入各参数
 ike-peer rtb
 proposal rtb
#
ipsec policy rtb 1 isakmp template temp  //配置IPSec策略，引入策略模板
#
interface Ethernet1/0/0
 ip address 192.168.2.1 255.255.255.0
#
```

 版权所有 © 华为技术有限公司

```
interface Serial1/0/0  //配置公网接口，使用固定IP地址
 link-protocol ppp
 ip address 13.1.1.1 255.255.255.0
 ipsec policy rtb
#
ip route-static 0.0.0.0 0.0.0.0 Serial1/0/0
#
return
```

步骤3 验证配置结果

在设备上执行命令**display ike sa**可以查看到安全联盟的相关信息。

配置完后总部和分支的用户可以实现数据加密互访。

----结束

配置注意事项

- 两端用于IKE协商的预共享密钥保持一致。
- 使用IPSec策略模板的一端，IKE参数中不需要指定对端的IP地址。
- 使用IPSec策略模板的一端，可以不配置ACL规则，如果配置ACL规则对数据流进行保护，则目的地址需要包含所有对端ACL中的源地址。

6.4.23 配置分支通过主备链路与总部建立 IPSec 隧道的示例

规格

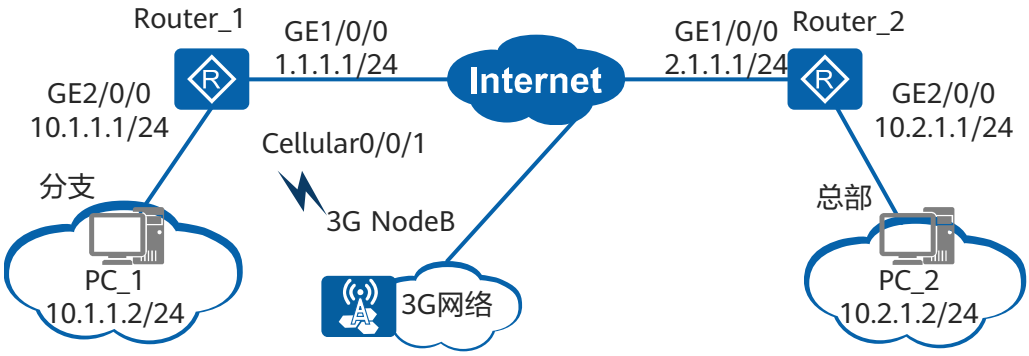
适用于V200R002C00及更高版本、所有形态的AR路由器。

组网需求

如图6-56所示，Router_1和Router_2分别作为企业分支和总部网关，分支通过Internet与总部建立通信，同时分支使用3G作为备份链路，在主链路故障时，流量能切换到备份链路，保证流量不中断。

企业希望对分支与总部之间相互访问的流量进行安全保护。分支与总部通过公网建立通信，可以在分支网关与总部网关之间建立一个IPSec隧道来实施安全保护。同时，要求分支用户可以访问外网，则可以在Router_1上部署NAT功能来实现该需求。

图 6-56 配置分支通过主备链路与总部建立 IPSec 隧道的组网图



版权所有 © 华为技术有限公司

操作步骤

步骤1 配置Router_1

```
#
 sysname Router_1
#
acl number 3000   //配置允许进行NAT转换的地址网段
 rule 1 deny ip source 10.1.1.0 0.0.0.255 destination 10.2.1.0 0.0.0.255
 rule 2 permit ip source 10.1.1.0 0.0.0.255
acl number 3010   //配置允许进行IPSec加密的地址网段
 rule 2 permit ip source 10.1.1.0 0.0.0.255 destination 10.2.1.0 0.0.0.255
#
ipsec proposal rta   //配置IPSec的安全提议
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-192
#
ike proposal 5   //配置IKE的安全提议
 encryption-algorithm aes-cbc-128   //V200R008及之后的版本，aes-cbc-128参数修改为aes-128
 dh group14
 authentication-algorithm sha2-256
#
ike peer rta v1   //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 pre-shared-key cipher %^%#JvZxR2g8c;a9~FPN~n'$7`DEV&=G(=Et02P/%\*!%^%#
 ike-proposal 5
 dpd msg seq-hash-notify
 dpd type periodic
 dpd idle-time 40
 remote-address 2.1.1.1
#
ipsec policy rt1 1 isakmp   //配置IPSec策略
 security acl 3010
 ike-peer rta
 proposal rta
ipsec policy rt2 1 isakmp
 security acl 3010
 ike-peer rta
 proposal rta
#
interface GigabitEthernet1/0/0
 ip address 1.1.1.1 255.255.255.0
 ipsec policy rt1   //在接口上绑定IPSec策略，发起IPSec协商
 standby interface Cellular0/0/1   //配置主接口的备份接口
 nat outbound 3000   //配置NAT功能，实现用户访问外网
#
interface GigabitEthernet2/0/0
 ip address 10.1.1.1 255.255.255.0
#
interface Cellular0/0/1   //配置3G接口拨号参数
 link-protocol ppp
 ip address ppp-negotiate   //自动获取运营商分配的IP地址，接入Internet
 dialer enable-circular   //使能DCC轮询功能
 dialer-group 1   //将此拨号口加入拨号控制列表，其编号和控制列表中的规则编号一致
 dialer timer autodial 15
 dialer number *99# autodial   //按拨号串进行自动拨号
 ipsec policy rt2   //在接口上绑定IPSec策略，发起IPSec协商
 nat outbound 3000
#
dialer-rule
 dialer-rule 1 ip permit
#
ip route-static 0.0.0.0 0.0.0.0 1.1.1.2 preference 40   //配置静态路由，使得该链路成为主链路
ip route-static 0.0.0.0 0.0.0.0 Cellular0/0/1 preference 80
#
return
```

 版权所有 © 华为技术有限公司

步骤2 配置Router_2

```
#
 sysname Router_2
#
acl number 3010   //配置允许进行IPSec加密的地址网段
 rule permit ip source 10.2.1.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
#
ipsec proposal rtb   //配置IPSec的安全提议
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-192
#
ike proposal 5   //配置IKE的安全提议
 encryption-algorithm aes-cbc-128   //V200R008及之后的版本，aes-cbc-128参数修改为aes-128
 dh group14
 authentication-algorithm sha2-256
#
ike peer rtb v1   //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 pre-shared-key cipher %^%#K{JG:rWVHPMnf;5\|,GW(Luq'qi8BT4nOj%5W5=)%^%#
 ike-proposal 5
 dpd msg seq-hash-notify
 dpd type periodic
 dpd idle-time 40
#
ipsec policy-template temp 1   //配置IPSec策略模板，引入各参数
 security acl 3010
 ike-peer rtb
 proposal rtb
#
ipsec policy rtb 1 isakmp template temp   //配置IPSec策略，引入策略模板
#
interface GigabitEthernet1/0/0
 ip address 2.1.1.1 255.255.255.0
 ipsec policy rtb   //在接口上绑定IPSec策略
#
interface GigabitEthernet2/0/0
 ip address 10.2.1.1 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 2.1.1.2   //配置静态路由
#
return
```

步骤3 验证配置结果

在设备上执行命令**display ike sa**可以查看到安全联盟的相关信息。

配置完后总部和分支的用户可以实现数据加密互访。同时，分支用户也可以访问外网。

----结束

配置注意事项

- 两端用于IKE协商的预共享密钥保持一致。
- 使用IPSec策略模板的一端，IKE参数中不需要指定对端的IP地址。
- 使用IPSec策略模板的一端，可以不配置ACL规则，如果配置ACL规则对数据流进行保护，则目的地址需要包含所有对端ACL中的源地址。
- 3G接口的拨号参数，各3G网络有所区别，具体需咨询3G网络的服务商。

 版权所有 © 华为技术有限公司

- 当IPSec与NAT配置在同一台设备时，由于设备优先处理NAT流程，故在IPSec封装之前，PC访问对端的数据流会首先进行NAT转换。所以这里需将NAT的ACL中要将经过IPSec隧道的数据流的动作配置为Deny。

6.4.24 配置分支使用有线线路和总部之间建立 IPSec 隧道的示例

规格

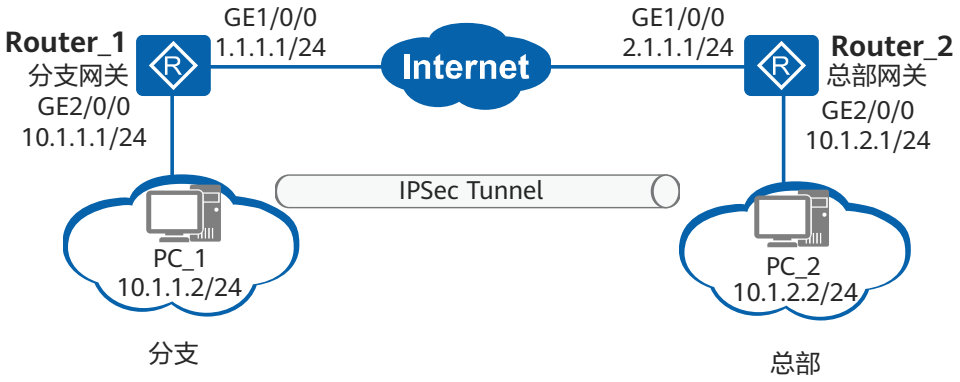
适用于V200R002C00及更高版本、所有形态的AR路由器。

组网需求

如图6-57所示，Router_1为企业分支网关，Router_2为企业总部网关，分支与总部通过公网建立通信。

企业希望对分支与总部之间相互访问的流量进行安全保护。分支与总部通过公网建立通信，可以在分支网关与总部网关之间建立一个IPSec隧道来实施安全保护。同时，要求分支用户可以访问外网，则可以在Router_1上部署NAT功能来实现该需求。

图 6-57 配置分支使用有线线路和总部之间建立 IPSec 隧道的组网图



操作步骤

步骤1 配置Router_1

```
#
 sysname Router_1
#
acl number 3000   //配置允许进行NAT转换的地址
 rule 1 deny ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
 rule 2 permit ip source 10.1.1.0 0.0.0.255
acl number 3101   //配置允许进行IPSec加密的地址网段
 rule 5 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
#
ipsec proposal tran1   //配置IPSec的安全提议
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-128
#
ike proposal 5   //配置IKE的安全提议
 encryption-algorithm aes-cbc-128   //V200R008及之后的版本，aes-cbc-128参数修改为aes-128
 dh group14
 authentication-algorithm sha2-256
```


版权所有 © 华为技术有限公司

```
#
ike peer spub v1  //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 pre-shared-key cipher %^%#JvZxR2g8c;a9~FPN~n'$7`DEV&=G(=Et02P/%\*!%^%#
 ike-proposal 5
 remote-address 2.1.1.1
#
ipsec policy map1 10 isakmp  //配置IPSec策略
 security acl 3101
 ike-peer spub
 proposal tran1
#
interface GigabitEthernet1/0/0
 ip address 1.1.1.1 255.255.255.0
 ipsec policy map1  //在接口上绑定IPSec策略，发起IPSec协商
 nat outbound 3000  //配置NAT功能，实现用户访问外网
#
interface GigabitEthernet2/0/0
 ip address 10.1.1.1 255.255.255.0
#
ip route-static 2.1.1.0 255.255.255.0 1.1.1.2  //配置静态路由
ip route-static 10.1.2.0 255.255.255.0 1.1.1.2
#
return
```

步骤2 配置Router_2

```
#
 sysname Router_2
#
acl number 3101  //配置允许进行IPSec加密的地址网段
 rule 5 permit ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
#
ipsec proposal tran1  //配置IPSec的安全提议
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-128
#
ike proposal 5  //配置IKE的安全提议
 encryption-algorithm aes-cbc-128  //V200R008及之后的版本，aes-cbc-128参数修改为aes-128
 dh group14
 authentication-algorithm sha2-256
#
ike peer spua v1  //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 pre-shared-key cipher %^%#K{JG:rWVHPMnf;5\|,GW(Luq'qi8BT4nOj%5W5=)%^%#
 ike-proposal 5
 remote-address 1.1.1.1
#
ipsec policy use1 10 isakmp  //配置IPSec策略
 security acl 3101
 ike-peer spua
 proposal tran1
#
interface GigabitEthernet1/0/0
 ip address 2.1.1.1 255.255.255.0
 ipsec policy use1  //在接口上绑定IPSec策略
#
interface GigabitEthernet2/0/0
 ip address 10.1.2.1 255.255.255.0
#
ip route-static 1.1.1.0 255.255.255.0 2.1.1.2  //配置静态路由
ip route-static 10.1.1.0 255.255.255.0 2.1.1.2
```

 版权所有 © 华为技术有限公司

```
#
return
```

步骤3 验证配置结果

在设备上执行命令**display ike sa**可以查看到安全联盟的相关信息。

配置完后总部和分支的用户可以实现数据加密互访。同时，分支用户也可以访问外网。

----结束

配置注意事项

- 两端用于IKE协商的预共享密钥保持一致。
- 总部和各分支之间的外网地址路由可达。
- 分支的ACL需要与总部ACL互为镜像。
- 当IPSec与NAT配置在同一台设备时，由于设备优先处理NAT流程，故在IPSec封装之前，PC访问对端的数据流会首先进行NAT转换。所以这里需将NAT的ACL中要将经过IPSec隧道的数据流的动作配置为Deny。

6.5 BGP/MPLS IP VPN

6.5.1 配置设备之间部署 BGP/MPLS IP VPN 实现互通的示例

适用产品和版本

适用于所有版本。

AR611E-S、AR611、AR631I-LTE4CN、AR631I-LTE4EA、AR611-LTE4EA、AR611-S、AR611W-S、AR611W、AR611W-LTE4CN、AR611W-LTE6EA、AR617VW、AR617VW-LTE4EA、AR617VW-LTE4、AR651C和AR651F-Lite不支持此功能。

AR303和AR303W不支持此功能。

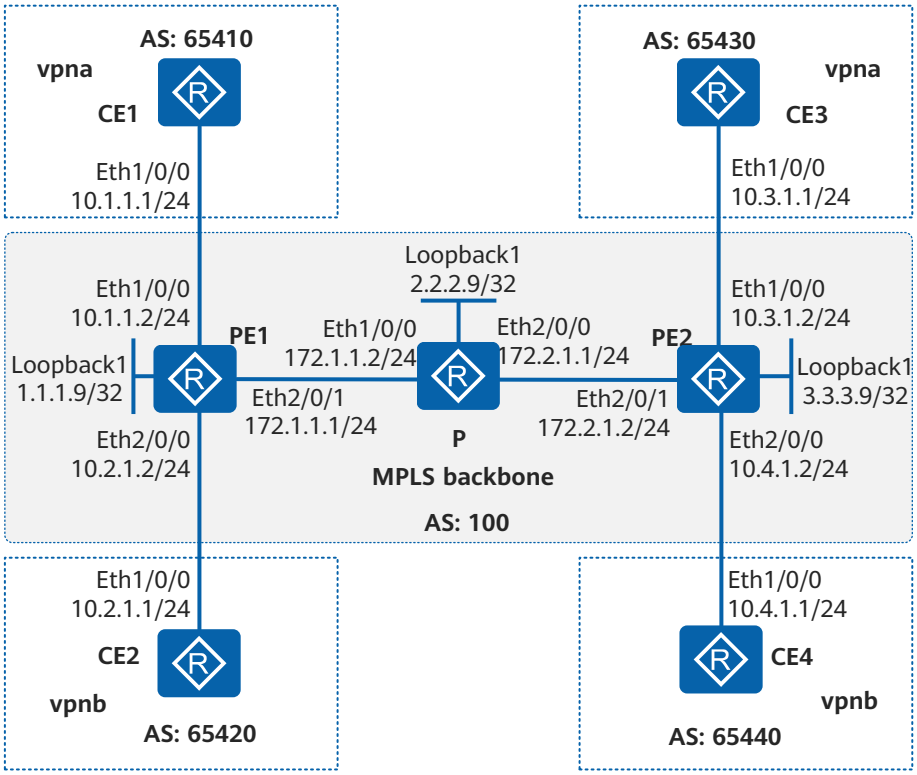
组网需求

如图6-58:

- CE1、CE3属于vpna。
- CE2、CE4属于vpnb。
- vpna使用的VPN-target属性为111:1，vpnb为222:2。
- 不同VPN用户之间不能互相访问。

版权所有 © 华为技术有限公司

图 6-58 配置 BGP/MPLS IP VPN 组网图



操作步骤

步骤1 配置PE1

```
#
 sysname PE1
#
ip vpn-instance vpna  //创建VPN实例vpna
 ipv4-family
  route-distinguisher 100:1
  vpn-target 111:1 export-extcommunity
  vpn-target 111:1 import-extcommunity
#
ip vpn-instance vpnb  //创建VPN实例vpnb
 ipv4-family
  route-distinguisher 100:2
  vpn-target 222:2 export-extcommunity
  vpn-target 222:2 import-extcommunity
#
mpls lsr-id 1.1.1.9  //配置MPLS
mpls
#
mpls ldp  //建立LDP
#
interface Ethernet1/0/0  //绑定VPN实例
 ip binding vpn-instance vpna
 ip address 10.1.1.2 255.255.255.0
#
interface Ethernet2/0/0
 ip binding vpn-instance vpnb  //绑定VPN实例
 ip address 10.2.1.2 255.255.255.0
#
interface Ethernet2/0/1  //接口使能MPLS
```


版权所有 © 华为技术有限公司

```
 ip address 172.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface LoopBack1
 ip address 1.1.1.9 255.255.255.255
#
bgp 100  //配置MP-IBGP对等体
 peer 3.3.3.9 as-number 100
 peer 3.3.3.9 connect-interface LoopBack1
 #
 ipv4-family unicast
  undo synchronization
  peer 3.3.3.9 enable
 #
 ipv4-family vpnv4  //使能对等体交换VPNv4路由信息的能力
  policy vpn-target
  peer 3.3.3.9 enable
 #
 ipv4-family vpn-instance vpna  //配置PE与CE之间建立EBGP对等体关系，引入VPN路由
  peer 10.1.1.1 as-number 65410
  import-route direct
 #
 ipv4-family vpn-instance vpnb  //配置PE与CE之间建立EBGP对等体关系，引入VPN路由
  peer 10.2.1.1 as-number 65420
  import-route direct
#
ospf 1  //配置公网路由
 area 0.0.0.0
  network 172.1.1.0 0.0.0.255
  network 1.1.1.9 0.0.0.0
#
return
```

步骤2 配置P

```
#
 sysname P
#
mpls lsr-id 2.2.2.9  //配置MPLS
mpls
#
mpls ldp
#
interface Ethernet1/0/0
 ip address 172.1.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface Ethernet2/0/0
 ip address 172.2.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface LoopBack1
 ip address 2.2.2.9 255.255.255.255
#
ospf 1  //配置公网路由
 area 0.0.0.0
  network 172.1.1.0 0.0.0.255
  network 172.2.1.0 0.0.0.255
  network 2.2.2.9 0.0.0.0
#
return
```

步骤3 配置PE2

```
#
 sysname PE2
#
ip vpn-instance vpna  //创建VPN实例vpna
```

 版权所有 © 华为技术有限公司

```
 ipv4-family
  route-distinguisher 200:1
  vpn-target 111:1 export-extcommunity
  vpn-target 111:1 import-extcommunity
#
ip vpn-instance vpnb  //创建VPN实例vpnb
 ipv4-family
  route-distinguisher 200:2
  vpn-target 222:2 export-extcommunity
  vpn-target 222:2 import-extcommunity
#
mpls lsr-id 3.3.3.9  //配置MPLS LSR
mpls
#
mpls ldp
#
interface Ethernet1/0/0 //绑定VPN实例
 ip binding vpn-instance vpna
 ip address 10.3.1.2 255.255.255.0
#
interface Ethernet2/0/0  //绑定VPN实例
 ip binding vpn-instance vpnb
 ip address 10.4.1.2 255.255.255.0
#
interface Ethernet2/0/1  //接口使能MPLS
 ip address 172.2.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface LoopBack1
 ip address 3.3.3.9 255.255.255.255
#
bgp 100  //配置MP-IBGP对等体
 peer 1.1.1.9 as-number 100
 peer 1.1.1.9 connect-interface LoopBack1
 #
 ipv4-family unicast
  undo synchronization
  peer 1.1.1.9 enable
 #
 ipv4-family vpnv4  //使能对等体交换VPNv4路由信息的能力
  policy vpn-target
  peer 1.1.1.9 enable
 #
 ipv4-family vpn-instance vpna  //配置PE与CE之间建立EBGP对等体关系，引入VPN路由
  peer 10.3.1.1 as-number 65430
  import-route direct
 #
 ipv4-family vpn-instance vpnb  //配置PE与CE之间建立EBGP对等体关系，引入VPN路由
  peer 10.4.1.1 as-number 65440
  import-route direct
#
ospf 1  //配置公网路由
 area 0.0.0.0
  network 172.2.1.0 0.0.0.255
  network 3.3.3.9 0.0.0.0
#
return
```

步骤4 配置CE1

```
#
 sysname CE1
#
interface Ethernet1/0/0
 ip address 10.1.1.1 255.255.255.0
#
bgp 65410  //在PE与CE之间建立EBGP对等体关系
 peer 10.1.1.2 as-number 100
 #
```

 版权所有 © 华为技术有限公司

```
 ipv4-family unicast
  undo synchronization
  import-route direct  //引入直连路由
  peer 10.1.1.2 enable
#
return
```

步骤5 配置CE2

```
#
 sysname CE2
#
interface Ethernet1/0/0
 ip address 10.2.1.1 255.255.255.0
#
bgp 65420  //在PE与CE之间建立EBGP对等体关系
 peer 10.2.1.2 as-number 100
 #
 ipv4-family unicast
  undo synchronization
  import-route direct  //引入直连路由
  peer 10.2.1.2 enable
#
return
```

步骤6 配置CE3

```
#
 sysname CE3
#
interface Ethernet1/0/0
 ip address 10.3.1.1 255.255.255.0
#
bgp 65430  //在PE与CE之间建立EBGP对等体关系
 peer 10.3.1.2 as-number 100
 #
 ipv4-family unicast
  undo synchronization
  import-route direct  //引入直连路由
  peer 10.3.1.2 enable
#
return
```

步骤7 配置CE4

```
#
 sysname CE4
#
interface Ethernet1/0/0
 ip address 10.4.1.1 255.255.255.0
#
bgp 65440  //在PE与CE之间建立EBGP对等体关系
 peer 10.4.1.2 as-number 100
 #
 ipv4-family unicast
  undo synchronization
  import-route direct  //引入直连路由
  peer 10.4.1.2 enable
#
return
```

----结束

配置注意事项

- PE之间必须使用32位掩码的Loopback接口地址来建立MP-IBGP对等体关系，以便能够迭代到隧道。

 版权所有 © 华为技术有限公司

6.5.2 配置分支机构与总部之间部署 BGP/MPLS IP VPN 实现互通，并通过总部实现分支之间互通的示例

适用产品和版本

适用于所有版本。

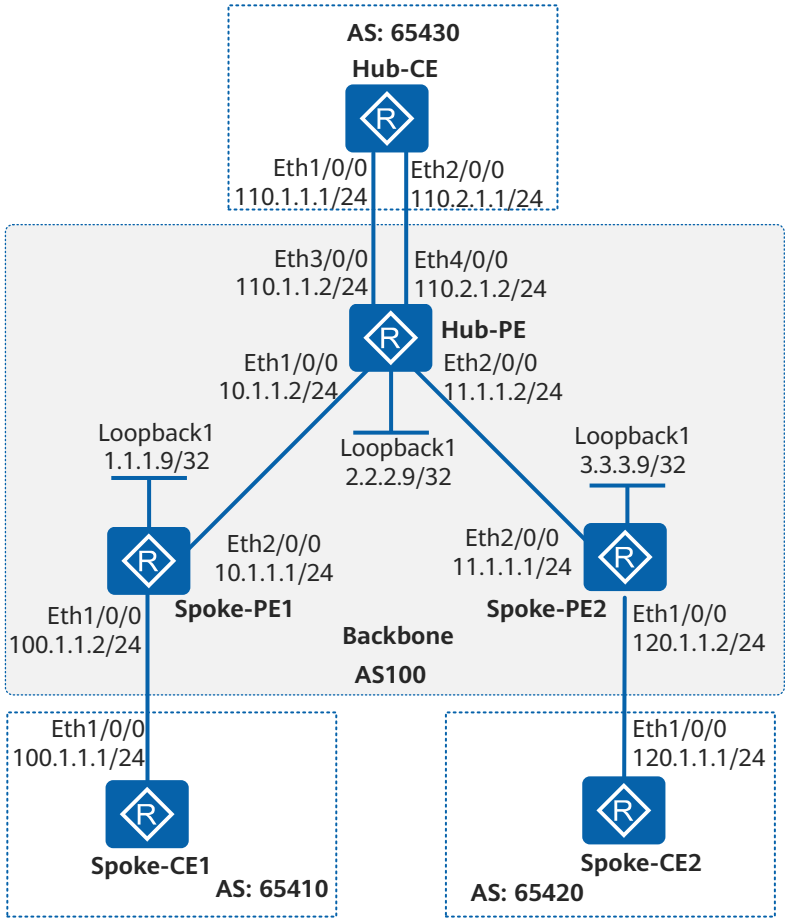
AR611E-S、AR611、AR631I-LTE4CN、AR631I-LTE4EA、AR611-LTE4EA、AR611-S、AR611W-S、AR611W、AR611W-LTE4CN、AR611W-LTE6EA、AR617VW、AR617VW-LTE4EA、AR617VW-LTE4、AR651C和AR651F-Lite不支持此功能。

AR303和AR303W不支持此功能。

组网需求

如图6-59，Spoke-CE之间的通信通过中心站点Hub-CE控制，即Spoke-CE之间的流量经过Hub-CE转发，而不是只经过Hub-PE转发。

图 6-59 配置 Hub and Spoke 组网图



版权所有 © 华为技术有限公司

操作步骤

步骤1 配置Spoke-CE1

```
#
 sysname Spoke-CE1
#
interface Ethernet1/0/0
 ip address 100.1.1.1 255.255.255.0
#
bgp 65410  //Spoke-PE与CE之间建立EBGP对等体关系
 peer 100.1.1.2 as-number 100
 #
 ipv4-family unicast
  undo synchronization
  import-route direct  //引入直连路由
  peer 100.1.1.2 enable
#
return
```

步骤2 配置Spoke-PE1

```
#
 sysname Spoke-PE1
#
ip vpn-instance vpna  //配置VPN实例
 ipv4-family
  route-distinguisher 100:1
  vpn-target 100:1 export-extcommunity
  vpn-target 200:1 import-extcommunity
#
mpls lsr-id 1.1.1.9  //建立MPLS LSR
mpls
#
mpls ldp
#
interface Ethernet1/0/0  //接口绑定VPN
 ip binding vpn-instance vpna
 ip address 100.1.1.2 255.255.255.0
#
interface Ethernet2/0/0  //使能接口MPLS
 ip address 10.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface LoopBack1
 ip address 1.1.1.9 255.255.255.255
#
bgp 100  //在PE之间建立MP-IBGP对等体关系
 peer 2.2.2.9 as-number 100
 peer 2.2.2.9 connect-interface LoopBack1
 #
 ipv4-family unicast
  undo synchronization
  peer 2.2.2.9 enable
 #  //在PE之间建立MP-IBGP对等体关系
 ipv4-family vpnv4
  policy vpn-target
  peer 2.2.2.9 enable
 #  //在Spoke-PE与CE之间建立EBGP对等体关系
 ipv4-family vpn-instance vpna
  peer 100.1.1.1 as-number 65410
  import-route direct//引入直连路由
#
ospf 1  //配置公网路由
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 1.1.1.9 0.0.0.0
#
return
```

 版权所有 © 华为技术有限公司

步骤3 配置Spoke-PE2

```
#
 sysname Spoke-PE2
#
ip vpn-instance vpna  //配置VPN实例
 ipv4-family
  route-distinguisher 100:3
  vpn-target 100:1 export-extcommunity
  vpn-target 200:1 import-extcommunity
#
mpls lsr-id 3.3.3.9  //建立MPLS LSR
mpls
#
mpls ldp
#
interface Ethernet1/0/0
 ip binding vpn-instance vpna
 ip address 120.1.1.2 255.255.255.0
#
interface Ethernet2/0/0  //使能接口MPLS
 ip address 11.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface LoopBack1
 ip address 3.3.3.9 255.255.255.255
#
bgp 100  //在PE之间建立MP-IBGP对等体关系
 peer 2.2.2.9 as-number 100
 peer 2.2.2.9 connect-interface LoopBack1
 #
 ipv4-family unicast
  undo synchronization
  peer 2.2.2.9 enable
 #  //在PE之间建立MP-IBGP对等体关系
 ipv4-family vpnv4
  policy vpn-target
  peer 2.2.2.9 enable
 #  //在Spoke-PE与CE之间建立EBGP对等体关系
 ipv4-family vpn-instance vpna
  peer 120.1.1.1 as-number 65420
  import-route direct  //引入直连路由
#
ospf 1  //配置公网路由
 area 0.0.0.0
  network 3.3.3.9 0.0.0.0
  network 11.1.1.0 0.0.0.255
#
return
```

步骤4 配置Spoke-CE2

```
#
 sysname Spoke-CE2
#
interface Ethernet1/0/0
 ip address 120.1.1.1 255.255.255.0
#
bgp 65420  //Spoke-PE与CE之间建立EBGP对等体关系
 peer 120.1.1.2 as-number 100
 #
 ipv4-family unicast
  undo synchronization
  import-route direct  //引入直连路由
  peer 120.1.1.2 enable
#
return
```

步骤5 配置Hub-CE

 版权所有 © 华为技术有限公司

```
#
 sysname Hub-CE
#
interface Ethernet1/0/0
 ip address 110.1.1.1 255.255.255.0
#
interface Ethernet2/0/0
 ip address 110.2.1.1 255.255.255.0
#
bgp 65430  //Spoke-PE与CE之间建立EBGP对等体关系
 peer 110.1.1.2 as-number 100
 peer 110.2.1.2 as-number 100
 #
 ipv4-family unicast
  undo synchronization
  import-route direct  //引入直连路由
  peer 110.2.1.2 enable
  peer 110.1.1.2 enable
#
return
```

步骤6 配置Hub-PE

```
#
 sysname Hub-PE
#
ip vpn-instance vpn_in  //配置VPN实例vpn_in
 ipv4-family
  route-distinguisher 100:21
  vpn-target 100:1 import-extcommunity
#
ip vpn-instance vpn_out  //配置VPN实例vpn_out
 ipv4-family
  route-distinguisher 100:22
  vpn-target 200:1 export-extcommunity
#
mpls lsr-id 2.2.2.9  //配置MPLS LSR
mpls
#
mpls ldp
#
interface Ethernet1/0/0
 ip address 10.1.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface Ethernet2/0/0  //使能接口MPLS
 ip address 11.1.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface Ethernet3/0/0  //接口绑定VPN
 ip binding vpn-instance vpn_in
 ip address 110.1.1.2 255.255.255.0
#
interface Ethernet4/0/0  //接口绑定VPN
 ip binding vpn-instance vpn_out
 ip address 110.2.1.2 255.255.255.0
#
interface LoopBack1
 ip address 2.2.2.9 255.255.255.255
#
bgp 100  //在Hub-PE与CE之间建立EBGP对等体关系
 peer 1.1.1.9 as-number 100
 peer 1.1.1.9 connect-interface LoopBack1
 peer 3.3.3.9 as-number 100
 peer 3.3.3.9 connect-interface LoopBack1
 #
 ipv4-family unicast
  undo synchronization
```

 版权所有 © 华为技术有限公司

```
 peer 1.1.1.9 enable
 peer 3.3.3.9 enable
#
ipv4-family vpnv4
 policy vpn-target
 peer 1.1.1.9 enable
 peer 3.3.3.9 enable
#
ipv4-family vpn-instance vpn_in  //引入VPN路由
 peer 110.1.1.1 as-number 65430
 import-route direct
#
ipv4-family vpn-instance vpn_out  //引入VPN路由
 peer 110.2.1.1 as-number 65430
 peer 110.2.1.1 allow-as-loop
 import-route direct
#
ospf 1  //配置公网路由
 area 0.0.0.0
  network 2.2.2.9 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 11.1.1.0 0.0.0.255
#
return
```

----结束

配置注意事项

- PE之间必须使用32位掩码的Loopback接口地址来建立MP-IBGP对等体关系，以便能够迭代到隧道。

6.5.3 配置在层次化网络中设备之间部署 BGP/MPLS IP VPN 实现互通的示例

适用产品和版本

适用于所有版本。

AR611E-S、AR611、AR631I-LTE4CN、AR631I-LTE4EA、AR611-LTE4EA、AR611-S、AR611W-S、AR611W、AR611W-LTE4CN、AR611W-LTE6EA、AR617VW、AR617VW-LTE4EA、AR617VW-LTE4、AR651C和AR651F-Lite不支持此功能。

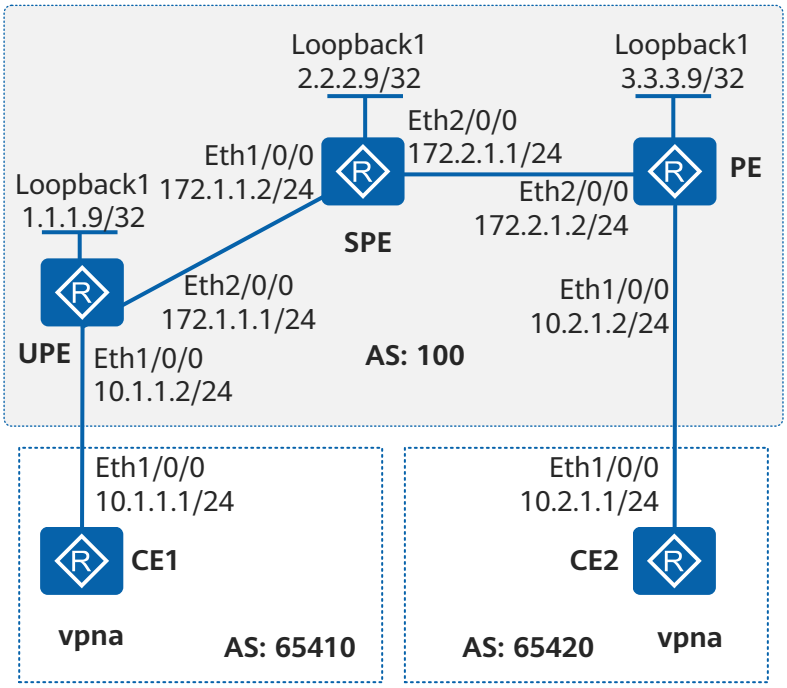
AR303和AR303W不支持此功能。

组网需求

如图6-60，CE1、CE2属于同一个VPN，使用的VPN-target属性也一样；CE1通过UPE接入，CE2通过普通PE接入。UPE、SPE与PE之间配置OSPF实现互通。

 版权所有 © 华为技术有限公司

图 6-60 配置 HoVPN 组网图



操作步骤

步骤1 配置CE1

```
#
 sysname CE1
#
interface Ethernet1/0/0
 ip address 10.1.1.1 255.255.255.0
#  //配置PE和CE间使用EBGP
bgp 65410
 peer 10.1.1.2 as-number 100
 #
 ipv4-family unicast
  undo synchronization
  import-route direct
  peer 10.1.1.2 enable
#
return
```

步骤2 配置UPE

```
#
 sysname UPE
#  //创建并配置VPN实例
ip vpn-instance vpna
 ipv4-family
  route-distinguisher 100:1
  vpn-target 1:1 export-extcommunity
  vpn-target 1:1 import-extcommunity
#  //使能MPLS
mpls lsr-id 1.1.1.9
mpls
#
mpls ldp
#  //接口绑定VPN实例
interface Ethernet1/0/0
```


版权所有 © 华为技术有限公司

```
 ip binding vpn-instance vpna
 ip address 10.1.1.2 255.255.255.0
#
interface Ethernet2/0/0
 ip address 172.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface LoopBack1
 ip address 1.1.1.9 255.255.255.255
#  //配置UPE与SPE的MP-IBGP对等体关系
bgp 100
 peer 2.2.2.9 as-number 100
 peer 2.2.2.9 connect-interface LoopBack1
 #
 ipv4-family unicast
  undo synchronization
  peer 2.2.2.9 enable
 #
 ipv4-family vpnv4
  policy vpn-target
  peer 2.2.2.9 enable
 #
 ipv4-family vpn-instance vpna
  peer 10.1.1.1 as-number 65410
  import-route direct
#  //配置路由
ospf 1
 area 0.0.0.0
  network 1.1.1.9 0.0.0.0
  network 172.1.1.0 0.0.0.255
#
return
```

步骤3 配置SPE

```
#
 sysname SPE
#  //创建并配置VPN实例
ip vpn-instance vpna
 ipv4-family
  route-distinguisher 200:1
  vpn-target 1:1 export-extcommunity
  vpn-target 1:1 import-extcommunity
#  //使能MPLS
mpls lsr-id 2.2.2.9
mpls
#
mpls ldp
#
interface Ethernet1/0/0
 ip address 172.1.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface Ethernet2/0/0
 ip address 172.2.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface LoopBack1
 ip address 2.2.2.9 255.255.255.255
#  //配置UPE与SPE、PE与SPE的MP-IBGP对等体关系
bgp 100
 peer 1.1.1.9 as-number 100
 peer 1.1.1.9 connect-interface LoopBack1
 peer 3.3.3.9 as-number 100
 peer 3.3.3.9 connect-interface LoopBack1
 #
 ipv4-family unicast
```

 版权所有 © 华为技术有限公司

```
 undo synchronization
 peer 1.1.1.9 enable
 peer 3.3.3.9 enable
#
ipv4-family vpnv4
 policy vpn-target
 peer 1.1.1.9 enable
 peer 1.1.1.9 upe
 peer 1.1.1.9 default-originate vpn-instance vpna
 peer 3.3.3.9 enable
#  //配置路由
ospf 1
 area 0.0.0.0
  network 2.2.2.9 0.0.0.0
  network 172.1.1.0 0.0.0.255
  network 172.2.1.0 0.0.0.255
#
return
```

步骤4 配置PE

```
#
 sysname PE
#  //创建并配置VPN实例
ip vpn-instance vpna
 ipv4-family
  route-distinguisher 100:2
  vpn-target 1:1 export-extcommunity
  vpn-target 1:1 import-extcommunity
#  //配置MPLS
mpls lsr-id 3.3.3.9
mpls
#
mpls ldp
#
interface Ethernet1/0/0
 ip binding vpn-instance vpna
 ip address 10.2.1.2 255.255.255.0
#
interface Ethernet2/0/0
 ip address 172.2.1.2 255.255.255.0
 mpls  //使能接口MPLS
 mpls ldp
#  //配置PE与SPE的MP-IBGP对等体关系
interface LoopBack1
 ip address 3.3.3.9 255.255.255.255
#
bgp 100
 peer 2.2.2.9 as-number 100
 peer 2.2.2.9 connect-interface LoopBack1
 #
 ipv4-family unicast
  undo synchronization
  peer 2.2.2.9 enable
 #
 ipv4-family vpnv4
  policy vpn-target
  peer 2.2.2.9 enable
 #
 ipv4-family vpn-instance vpna
  peer 10.2.1.1 as-number 65420
  import-route direct
#  //配置路由
ospf 1
 area 0.0.0.0
  network 3.3.3.9 0.0.0.0
  network 172.2.1.0 0.0.0.255
#
return
```

 版权所有 © 华为技术有限公司

步骤5 配置CE2

```
#
 sysname CE2
#
interface Ethernet1/0/0
 ip address 10.2.1.1 255.255.255.0
#  //配置PE接入CE，PE与CE之间使用BGP
bgp 65420
 peer 10.2.1.2 as-number 100
 #
 ipv4-family unicast
  undo synchronization
  import-route direct
  peer 10.2.1.2 enable
#
return
```

----结束

6.5.4 配置采用 OptionA 方式实现跨域的 BGP/MPLS IP VPN 示例

适用产品和版本

适用于所有版本。

AR611E-S、AR611、AR631I-LTE4CN、AR631I-LTE4EA、AR611-LTE4EA、AR611-S、AR611W-S、AR611W、AR611W-LTE4CN、AR611W-LTE6EA、AR617VW、AR617VW-LTE4EA、AR617VW-LTE4、AR651C和AR651F-Lite不支持此功能。

AR303和AR303W不支持此功能。

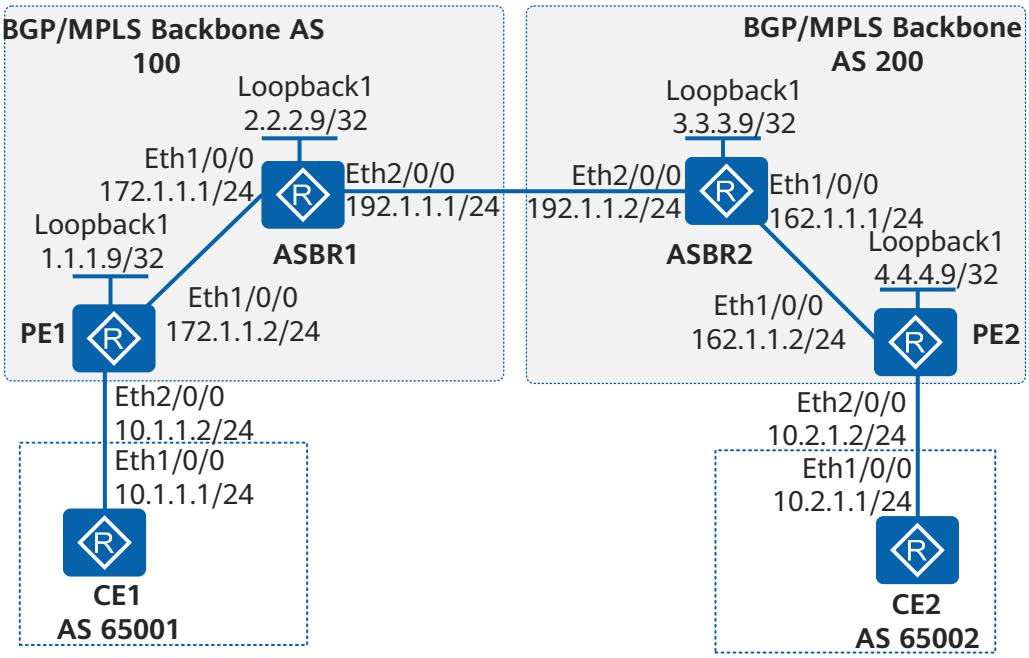
组网需求

如图6-61，CE1和CE2属于同一个VPN。CE1通过AS100的PE1接入，CE2通过AS200的PE2接入。

采用OptionA方式实现跨域的BGP/MPLS IP VPN，即采用VRF-to-VRF方式管理VPN路由。

版权所有 © 华为技术有限公司

图 6-61 配置 OptionA 方式跨域 VPN 组网图



操作步骤

步骤1 配置CE1

```
#
 sysname CE1
#
interface Ethernet1/0/0
 ip address 10.1.1.1 255.255.255.0
#  //配置CE与PE建立EBGP对等体
bgp 65001
 peer 10.1.1.2 as-number 100
#
ipv4-family unicast
 undo synchronization
 import-route direct
 peer 10.1.1.2 enable
#
return
```

步骤2 配置PE1

```
#
sysname PE1
#  //创建并配置VPN实例
ip vpn-instance vpn1
 ipv4-family
  route-distinguisher 100:1
  vpn-target 1:1 export-extcommunity
  vpn-target 1:1 import-extcommunity
#  //使能MPLS
mpls lsr-id 1.1.1.9
mpls
#
mpls ldp
#  //使能接口MPLS功能
interface Ethernet1/0/0
 ip address 172.1.1.2 255.255.255.0
```


版权所有 © 华为技术有限公司

```
 mpls
 mpls ldp
#  //接口绑定VPN实例
interface Ethernet2/0/0
 ip binding vpn-instance vpn1
 ip address 10.1.1.2 255.255.255.0
#
interface LoopBack1
 ip address 1.1.1.9 255.255.255.255
#  //配置PE与ASBR建立MP-IBGP对等体关系
bgp 100
 peer 2.2.2.9 as-number 100
 peer 2.2.2.9 connect-interface LoopBack1
 #
 ipv4-family unicast
  undo synchronization
  peer 2.2.2.9 enable
 #
 ipv4-family vpnv4  //使能对等体交换VPNv4路由信息的能力
  policy vpn-target
  peer 2.2.2.9 enable
 #
 ipv4-family vpn-instance vpn1  //配置PE与CE建立EBGP对等体关系
  peer 10.1.1.1 as-number 65001
#  //配置OSPF路由
ospf 1
 area 0.0.0.0
  network 1.1.1.9 0.0.0.0
  network 172.1.1.0 0.0.0.255
#
return
```

步骤3 配置ASBR1

```
#
sysname ASBR1
#  //创建并配置VPN实例
ip vpn-instance vpn1
 ipv4-family
  route-distinguisher 100:2
  vpn-target 1:1 export-extcommunity
  vpn-target 1:1 import-extcommunity
#  //配置MPLS功能
mpls lsr-id 2.2.2.9
mpls
#
mpls ldp
#
interface Ethernet1/0/0
 ip address 172.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface Ethernet2/0/0
 ip binding vpn-instance vpn1
 ip address 192.1.1.1 255.255.255.0
#
interface LoopBack1
 ip address 2.2.2.9 255.255.255.255
#  //配置PE与ASBR建立MP-IBGP对等体关系
bgp 100
 peer 1.1.1.9 as-number 100
 peer 1.1.1.9 connect-interface LoopBack1
 #
 ipv4-family unicast
  undo synchronization
  peer 1.1.1.9 enable
 #
 ipv4-family vpnv4  //使能对等体交换VPNv4路由信息的能力
  policy vpn-target
```

 版权所有 © 华为技术有限公司

```
 peer 1.1.1.9 enable
 #
 ipv4-family vpn-instance vpn1  //配置ASBR1与ASBR2建立EBGP对等体关系
  peer 192.1.1.2 as-number 200
#  //配置OSPF路由
ospf 1
 area 0.0.0.0
  network 2.2.2.9 0.0.0.0
  network 172.1.1.0 0.0.0.255
#
return
```

步骤4 配置ASBR2

```
#
 sysname ASBR2
#  //创建并配置VPN实例
ip vpn-instance vpn1
 ipv4-family
  route-distinguisher 200:2
  vpn-target 2:2 export-extcommunity
  vpn-target 2:2 import-extcommunity
#  //配置MPLS LSR
mpls lsr-id 3.3.3.9
mpls
#
mpls ldp
#  //使能接口MPLS功能
interface Ethernet1/0/0
 ip address 162.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface Ethernet2/0/0
 ip binding vpn-instance vpn1
 ip address 192.1.1.2 255.255.255.0
#
interface LoopBack1
 ip address 3.3.3.9 255.255.255.255
#  //配置PE与ASBR建立MP-IBGP对等体关系
bgp 200
 peer 4.4.4.9 as-number 200
 peer 4.4.4.9 connect-interface LoopBack1
 #
 ipv4-family unicast
  undo synchronization
  peer 4.4.4.9 enable
 #
 ipv4-family vpnv4  //使能对等体交换VPNv4路由信息的能力
  policy vpn-target
  peer 4.4.4.9 enable
 #
 ipv4-family vpn-instance vpn1    //配置ASBR1与ASBR2建立EBGP对等体关系
  peer 192.1.1.1 as-number 100
#  //配置OSPF路由
ospf 1
 area 0.0.0.0
  network 3.3.3.9 0.0.0.0
  network 162.1.1.0 0.0.0.255
#
return
```

步骤5 配置PE2

```
#
 sysname PE2
#  //创建并配置VPN实例
ip vpn-instance vpn1
 ipv4-family
  route-distinguisher 200:1
  vpn-target 2:2 export-extcommunity
```

 版权所有 © 华为技术有限公司

```
 vpn-target 2:2 import-extcommunity
#  //配置MPLS
mpls lsr-id 4.4.4.9
mpls
#
mpls ldp
#  //使能接口MPLS功能
interface Ethernet1/0/0
 ip address 162.1.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface Ethernet2/0/0
 ip binding vpn-instance vpn1
 ip address 10.2.1.2 255.255.255.0
#
interface LoopBack1
 ip address 4.4.4.9 255.255.255.255
#  //配置PE与ASBR建立MP-IBGP对等体关系
bgp 200
 peer 3.3.3.9 as-number 200
 peer 3.3.3.9 connect-interface LoopBack1
 #
 ipv4-family unicast
  undo synchronization
  peer 3.3.3.9 enable
 #
 ipv4-family vpnv4  //使能对等体交换VPNv4路由信息的能力
  policy vpn-target
  peer 3.3.3.9 enable
#
ipv4-family vpn-instance vpn1  //配置PE与CE建立EBGP对等体关系
 peer 10.2.1.1 as-number 65002
#  //配置OSPF路由
ospf 1
 area 0.0.0.0
  network 4.4.4.9 0.0.0.0
  network 162.1.1.0 0.0.0.255
#
return
```

步骤6 配置CE2

```
#
sysname CE2
#
interface Ethernet1/0/0
 ip address 10.2.1.1 255.255.255.0
#  //配置CE与PE建立EBGP对等体
bgp 65002
 peer 10.2.1.2 as-number 200
 #
 ipv4-family unicast
  undo synchronization
  import-route direct
  peer 10.2.1.2 enable
#
return
```

----结束

6.5.5 配置采用 OptionB 方式实现跨域的 BGP/MPLS IP VPN 示例

适用产品和版本

适用于所有版本。

AR611E-S、AR611、AR631I-LTE4CN、AR631I-LTE4EA、AR611-LTE4EA、AR611-S、AR611W-S、AR611W、AR611W-LTE4CN、AR611W-LTE6EA、AR617VW、AR617VW-LTE4EA、AR617VW-LTE4、AR651C和AR651F-Lite不支持此功能。

AR303和AR303W不支持此功能。

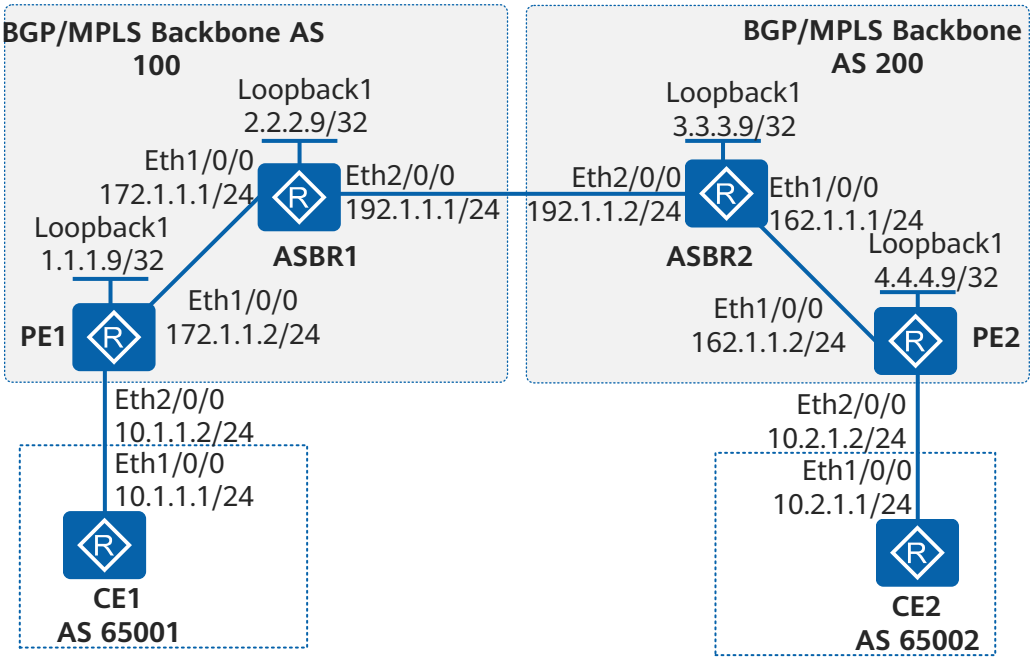
组网需求

如图6-62，CE1和CE2属于同一个VPN。CE1通过AS100的PE1接入，CE2通过AS200的PE2接入。

采用OptionB方式实现跨域的BGP/MPLS IP VPN：

- ASBR1与ASBR2间通过MP-EBGP交换VPNv4路由；
- ASBR不对接收的VPNv4路由进行VPN-Target过滤。

图 6-62 配置 OptionB 方式跨域 VPN 组网图



操作步骤

步骤1 配置CE1

```
#
 sysname CE1
#
interface Ethernet1/0/0
 ip address 10.1.1.1 255.255.255.0
#  //配置CE与PE建立EBGP对等体
bgp 65001
 peer 10.1.1.2 as-number 100
 #
 ipv4-family unicast
  undo synchronization
  import-route direct
  peer 10.1.1.2 enable
```


版权所有 © 华为技术有限公司

```
#
return
```

步骤2 配置PE1

```
#
 sysname PE1
#  //创建并配置VPN实例
ip vpn-instance vpn1
 ipv4-family
  route-distinguisher 100:1
  apply-label per-instance
  vpn-target 1:1 export-extcommunity
  vpn-target 1:1 import-extcommunity
#  //使能MPLS
mpls lsr-id 1.1.1.9
mpls
#
mpls ldp
#  //使能接口MPLS功能
interface Ethernet1/0/0
 ip address 172.1.1.2 255.255.255.0
 mpls
 mpls ldp
#  //接口绑定VPN实例
interface Ethernet2/0/0
 ip binding vpn-instance vpn1
 ip address 10.1.1.2 255.255.255.0
#
interface LoopBack1
 ip address 1.1.1.9 255.255.255.255
#  //配置PE与ASBR建立MP-IBGP对等体关系
bgp 100
 peer 2.2.2.9 as-number 100
 peer 2.2.2.9 connect-interface LoopBack1
 #
 ipv4-family unicast
  undo synchronization
  peer 2.2.2.9 enable
 #
 ipv4-family vpnv4  //使能对等体交换VPNv4路由信息的能力
  policy vpn-target
  peer 2.2.2.9 enable
 #
 ipv4-family vpn-instance vpn1  //配置PE与CE建立EBGP对等体关系
  peer 10.1.1.1 as-number 65001
  import-route direct
#  //配置OSPF路由
ospf 1
 area 0.0.0.0
  network 1.1.1.9 0.0.0.0
  network 172.1.1.0 0.0.0.255
#
return
```

步骤3 配置ASBR1

```
#
 sysname ASBR1
#  //配置MPLS功能
mpls lsr-id 2.2.2.9
mpls
#
mpls ldp
#
interface Ethernet1/0/0
 ip address 172.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface Ethernet2/0/0
```

 版权所有 © 华为技术有限公司

```
 ip address 192.1.1.1 255.255.255.0
 mpls
#
interface LoopBack1
 ip address 2.2.2.9 255.255.255.255
#  //配置PE与ASBR建立MP-IBGP对等体关系
bgp 100
 peer 192.1.1.2 as-number 200
 peer 1.1.1.9 as-number 100
 peer 1.1.1.9 connect-interface LoopBack1
 #
 ipv4-family unicast
  undo synchronization
  peer 192.1.1.2 enable
  peer 1.1.1.9 enable
 #
 ipv4-family vpnv4  //不对接收的VPNv4路由进行VPN-target过滤，并且使能ASBR1按下一跳分标签
  undo policy vpn-target
  apply-label per-nexthop
  peer 1.1.1.9 enable
  peer 192.1.1.2 enable
#  //配置OSPF路由
ospf 1
 area 0.0.0.0
  network 2.2.2.9 0.0.0.0
  network 172.1.1.0 0.0.0.255
#
return
```

步骤4 配置ASBR2

```
#
 sysname ASBR2
#  //配置MPLS功能
mpls lsr-id 3.3.3.9
mpls
#
mpls ldp
#
interface Ethernet1/0/0
 ip address 162.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface Ethernet2/0/0
 ip address 192.1.1.2 255.255.255.0
 mpls
#
interface LoopBack1
 ip address 3.3.3.9 255.255.255.255
#  //配置PE与ASBR建立MP-IBGP对等体关系
bgp 200
 peer 192.1.1.1 as-number 100
 peer 4.4.4.9 as-number 200
 peer 4.4.4.9 connect-interface LoopBack1
 #
 ipv4-family unicast
  undo synchronization
  peer 192.1.1.1 enable
  peer 4.4.4.9 enable
 #
 ipv4-family vpnv4  //不对接收的VPNv4路由进行VPN-target过滤，并且使能ASBR1按下一跳分标签
  undo policy vpn-target
  apply-label per-nexthop
  peer 4.4.4.9 enable
  peer 192.1.1.1 enable
#
ospf 1
 area 0.0.0.0
  network 3.3.3.9 0.0.0.0
```

 版权所有 © 华为技术有限公司

```
 network 162.1.1.0 0.0.0.255
#
return
```

步骤5 配置PE2

```
#
 sysname PE2
#  //创建并配置VPN实例
ip vpn-instance vpn1
 ipv4-family
  route-distinguisher 200:1
  apply-label per-instance
  vpn-target 1:1 export-extcommunity
  vpn-target 1:1 import-extcommunity
#  //配置MPLS LSR
mpls lsr-id 4.4.4.9
mpls
#
mpls ldp
#  //使能接口MPLS功能
interface Ethernet1/0/0
 ip address 162.1.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface Ethernet2/0/0
 ip binding vpn-instance vpn1
 ip address 10.2.1.2 255.255.255.0
#
interface LoopBack1
 ip address 4.4.4.9 255.255.255.255
#  //配置PE与ASBR建立MP-IBGP对等体关系
bgp 200
 peer 3.3.3.9 as-number 200
 peer 3.3.3.9 connect-interface LoopBack1
 #
 ipv4-family unicast
  undo synchronization
  peer 3.3.3.9 enable
 #
 ipv4-family vpnv4  //使能对等体交换VPNv4路由信息的能力
  policy vpn-target
  peer 3.3.3.9 enable
 #
 ipv4-family vpn-instance vpn1  //配置PE与CE建立EBGP对等体关系
  peer 10.2.1.1 as-number 65002
  import-route direct
#  //配置OSPF路由
ospf 1
 area 0.0.0.0
  network 4.4.4.9 0.0.0.0
  network 162.1.1.0 0.0.0.255
#
return
```

步骤6 配置CE2

```
#
 sysname CE2
#
interface Ethernet1/0/0
 ip address 10.2.1.1 255.255.255.0
#
bgp 65002  //配置CE与PE建立EBGP对等体
 peer 10.2.1.2 as-number 200
 #
 ipv4-family unicast
  undo synchronization
  import-route direct
  peer 10.2.1.2 enable
```

 版权所有 © 华为技术有限公司

```
#
return
```

----结束

6.5.6 配置采用 OptionC 方式实现跨域的 BGP/MPLS IP VPN 示例

适用产品和版本

适用于所有版本。

AR611E-S、AR611、AR631I-LTE4CN、AR631I-LTE4EA、AR611-LTE4EA、AR611-S、AR611W-S、AR611W、AR611W-LTE4CN、AR611W-LTE6EA、AR617VW、AR617VW-LTE4EA、AR617VW-LTE4、AR651C和AR651F-Lite不支持此功能。

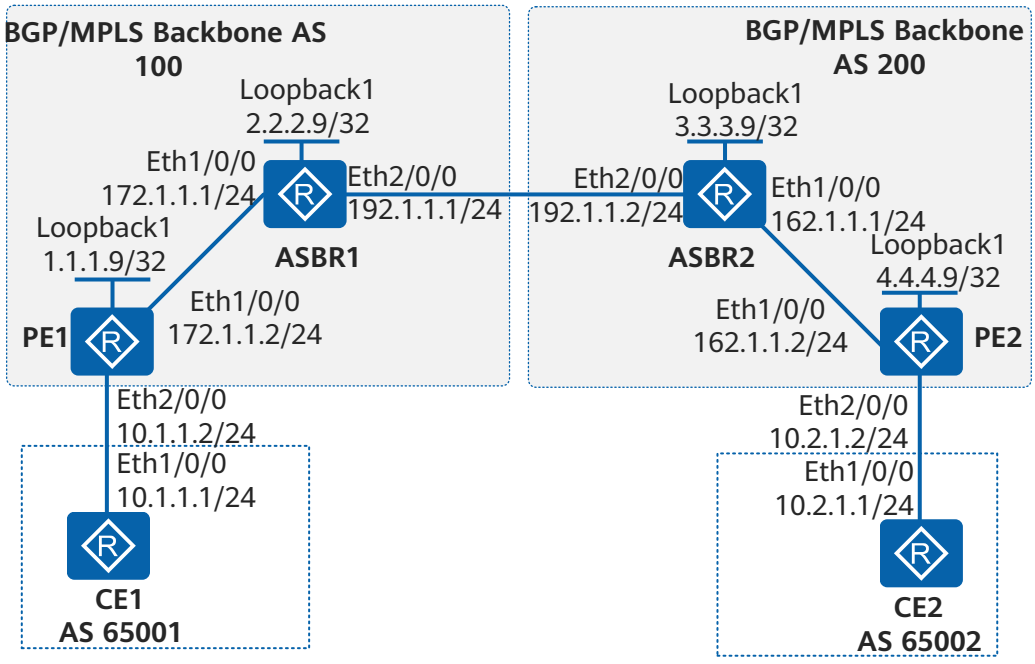
AR303和AR303W不支持此功能。

组网需求

如图6-63，CE1和CE2属于同一个VPN。CE1通过AS100的PE1接入，CE2通过AS200的PE2接入。

采用OptionC方式实现跨域的BGP/MPLS IP VPN。

图 6-63 配置 OptionC 方式跨域 VPN 组网图



操作步骤

步骤1 配置CE1

```
#
 sysname CE1
#
interface Ethernet1/0/0
```


版权所有 © 华为技术有限公司

```
 ip address 10.1.1.1 255.255.255.0
#
bgp 65001  //配置CE与PE建立EBGP对等体
 peer 10.1.1.2 as-number 100
 #
 ipv4-family unicast
  undo synchronization
  import-route direct
  peer 10.1.1.2 enable
#
return
```

步骤2 配置PE1

```
#
 sysname PE1
#  //创建并配置VPN实例
ip vpn-instance vpn1
 ipv4-family
  route-distinguisher 100:1
  vpn-target 1:1 export-extcommunity
  vpn-target 1:1 import-extcommunity
#  //使能MPLS
mpls lsr-id 1.1.1.9
mpls
#
mpls ldp
#  //使能接口MPLS功能
interface Ethernet1/0/0
 ip address 172.1.1.2 255.255.255.0
 mpls
 mpls ldp
#  //接口绑定VPN实例
interface Ethernet2/0/0
 ip binding vpn-instance vpn1
 ip address 10.1.1.2 255.255.255.0
#
interface LoopBack1
 ip address 1.1.1.9 255.255.255.255
#
bgp 100
 peer 2.2.2.9 as-number 100  //PE1与ASBR1建立IBGP对等体关系
 peer 2.2.2.9 connect-interface LoopBack1
 peer 4.4.4.9 as-number 200  //PE1与PE2建立MP-EBGP对等体关系
 peer 4.4.4.9 ebgp-max-hop 10
 peer 4.4.4.9 connect-interface LoopBack1
 #
 ipv4-family unicast
  undo synchronization
  peer 2.2.2.9 enable
  peer 2.2.2.9 label-route-capability  //使能与ASBR1交换标签IPv4路由的能力
  peer 4.4.4.9 enable
 #
 ipv4-family vpnv4  //使能对等体交换VPNv4路由信息的能力
  policy vpn-target
  peer 4.4.4.9 enable
 #
 ipv4-family vpn-instance vpn1    //PE1与CE建立EBGP对等体关系,引入VPN路由
  peer 10.1.1.1 as-number 65001
  import-route direct
#
ospf 1
 area 0.0.0.0
  network 1.1.1.9 0.0.0.0
  network 172.1.1.0 0.0.0.255
#
return
```

步骤3 配置ASBR1

 版权所有 © 华为技术有限公司

```
#
 sysname ASBR1
#
mpls lsr-id 2.2.2.9
mpls
#
mpls ldp
#
interface Ethernet1/0/0
 ip address 172.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface Ethernet2/0/0
 ip address 192.1.1.1 255.255.255.0
 mpls
#
interface LoopBack1
 ip address 2.2.2.9 255.255.255.255
#
bgp 100
 peer 192.1.1.2 as-number 200  //ASBR1与ASBR2建立EBGP对等体关系
 peer 1.1.1.9 as-number 100  //ASBR1与PE1建立IBGP对等体关系
 peer 1.1.1.9 connect-interface LoopBack1
 #
 ipv4-family unicast
  undo synchronization
  network 1.1.1.9 255.255.255.255
  peer 192.1.1.2 enable
  peer 192.1.1.2 route-policy policy1 export  //对向ASBR2发布的路由应用路由策略，并使能与ASBR2交换标签IPv4路由的能力
  peer 192.1.1.2 label-route-capability
  peer 1.1.1.9 enable
  peer 1.1.1.9 route-policy policy2 export  //对向PE1发布的路由应用路由策略，并使能与PE1交换标签IPv4路由的能力
  peer 1.1.1.9 label-route-capability
#  //配置路由
ospf 1
 area 0.0.0.0
  network 2.2.2.9 0.0.0.0
  network 172.1.1.0 0.0.0.255
#  //创建路由策略
route-policy policy1 permit node 1
 apply mpls-label
route-policy policy2 permit node 1
 if-match mpls-label
 apply mpls-label
#
return
```

步骤4 配置ASBR2

```
#
 sysname ASBR2
#  //使能MPLS功能
mpls lsr-id 3.3.3.9
mpls
#
mpls ldp
#
interface Ethernet1/0/0
 ip address 162.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface Ethernet2/0/0
 ip address 192.1.1.2 255.255.255.0
 mpls
#
interface LoopBack1
```

 版权所有 © 华为技术有限公司

```
 ip address 3.3.3.9 255.255.255.255
#
bgp 200
 peer 192.1.1.1 as-number 100  //ASBR2与ASBR1建立EBGP对等体关系
 peer 4.4.4.9 as-number 200  //ASBR2与PE2建立IBGP对等体关系
 peer 4.4.4.9 connect-interface LoopBack1
 #
 ipv4-family unicast
  undo synchronization
  network 4.4.4.9 255.255.255.255
  peer 192.1.1.1 enable
  peer 192.1.1.1 route-policy policy1 export  //对向ASBR1发布的路由应用路由策略，并使能与ASBR1交换标签IPv4路由的能力
  peer 192.1.1.1 label-route-capability
  peer 4.4.4.9 enable
  peer 4.4.4.9 route-policy policy2 export  //对向PE2发布的路由应用路由策略，并使能与PE2交换标签IPv4路由的能力
  peer 4.4.4.9 label-route-capability
#  //配置路由
ospf 1
 area 0.0.0.0
  network 3.3.3.9 0.0.0.0
  network 162.1.1.0 0.0.0.255
#  //创建路由策略
route-policy policy1 permit node 1
 apply mpls-label
route-policy policy2 permit node 1
 if-match mpls-label
 apply mpls-label
#
return
```

步骤5 配置PE2

```
#
 sysname PE2
#  //创建并配置VPN实例
ip vpn-instance vpn1
 ipv4-family
  route-distinguisher 200:1
  vpn-target 1:1 export-extcommunity
  vpn-target 1:1 import-extcommunity
#  //使能MPLS功能
mpls lsr-id 4.4.4.9
mpls
#
mpls ldp
#
interface Ethernet1/0/0
 ip address 162.1.1.2 255.255.255.0
 mpls
 mpls ldp
#  //接口绑定VPN实例
interface Ethernet2/0/0
 ip binding vpn-instance vpn1
 ip address 10.2.1.2 255.255.255.0
#
interface LoopBack1
 ip address 4.4.4.9 255.255.255.255
#
bgp 200
 peer 1.1.1.9 as-number 100  //PE1与PE2建立MP-EBGP对等体关系
 peer 1.1.1.9 ebgp-max-hop 10
 peer 1.1.1.9 connect-interface LoopBack1
 peer 3.3.3.9 as-number 200
 peer 3.3.3.9 connect-interface LoopBack1
 #
 ipv4-family unicast
  undo synchronization
  peer 1.1.1.9 enable
```

 版权所有 © 华为技术有限公司

```
 peer 3.3.3.9 enable
 peer 3.3.3.9 label-route-capability
#
ipv4-family vpnv4  //使能对等体交换VPNv4路由信息的能力
 policy vpn-target
 peer 1.1.1.9 enable
#
ipv4-family vpn-instance vpn1  //PE1与CE建立EBGP对等体关系,引入VPN路由
 peer 10.2.1.1 as-number 65002
 import-route direct
#  //配置路由功能
ospf 1
 area 0.0.0.0
  network 4.4.4.9 0.0.0.0
  network 162.1.1.0 0.0.0.255
#
return
```

步骤6 配置CE2

```
#
 sysname CE2
#
interface Ethernet1/0/0
 ip address 10.2.1.1 255.255.255.0
#
bgp 65002  //配置CE与PE建立EBGP对等体
 peer 10.2.1.2 as-number 200
 #
 ipv4-family unicast
  undo synchronization
  import-route direct
  peer 10.2.1.2 enable
#
return
```

----结束

6.5.7 配置设备之间部署 BGP/MPLS IP VPN 实现互通的示例（PE 和 CE 之间使用 ISIS）

适用产品和版本

适用于所有版本。

AR611E-S、AR611、AR631I-LTE4CN、AR631I-LTE4EA、AR611-LTE4EA、AR611-S、AR611W-S、AR611W、AR611W-LTE4CN、AR611W-LTE6EA、AR617VW、AR617VW-LTE4EA、AR617VW-LTE4、AR651C和AR651F-Lite不支持此功能。

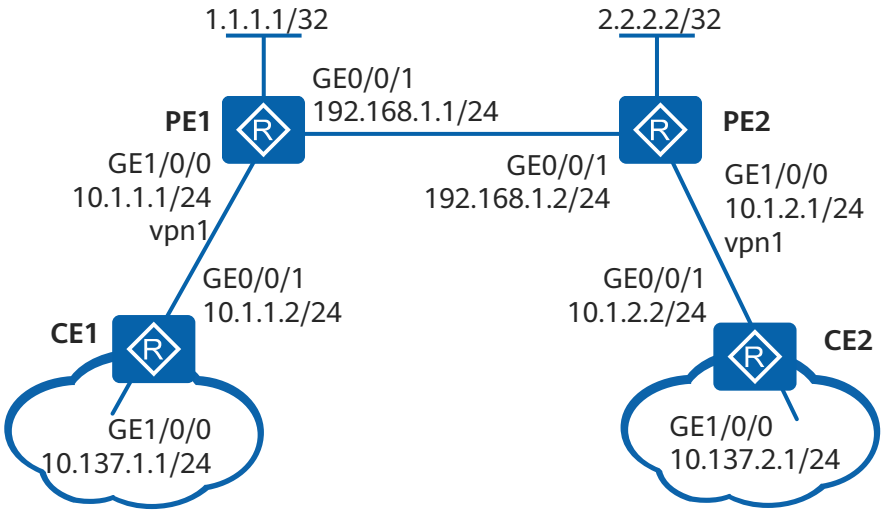
AR303和AR303W不支持此功能。

组网需求

PE1连接CE1，PE2连接CE2，CE1和CE2均属于vpn1，PE与CE通过ISIS进行路由交互。

 版权所有 © 华为技术有限公司

图 6-64 配置 BGP MPLS/IP VPN 组网图



操作步骤

步骤1 CE1上的配置

```
#
 sysname CE1
#
isis 1  //配置ISIS进程
 network-entity 10.0000.1111.1112.00
#
interface GigabitEthernet0/0/1
 ip address 10.1.1.2 255.255.255.0
 isis enable 1  //接口下使能ISIS
#
interface GigabitEthernet1/0/0
 ip address 10.137.1.1 255.255.255.0
 isis enable 1  //接口下使能ISIS
#
return
```

步骤2 CE2上的配置

```
#
 sysname CE2
#
isis 1  //配置ISIS进程
 network-entity 10.0000.1111.0001.00
#
interface GigabitEthernet0/0/1
 ip address 10.1.2.2 255.255.255.0
 isis enable 1  //接口下使能ISIS
#
interface GigabitEthernet1/0/0
 ip address 10.137.2.1 255.255.255.0
 isis enable 1  //接口下使能ISIS
#
return
```

步骤3 PE1上的配置

```
#
 sysname PE1
#
ip vpn-instance vpn1  //创建VPN实例
```


版权所有 © 华为技术有限公司

```
 ipv4-family
  route-distinguisher 1:1
  vpn-target 1:1 export-extcommunity
  vpn-target 1:1 import-extcommunity
#
mpls lsr-id 1.1.1.1  //配置MPLS能力
mpls
#
mpls ldp
#
isis 1 vpn-instance vpn1  //创建ISIS进程与VPN实例绑定
 network-entity 10.0000.1111.1111.00
 import-route bgp  //本端PE把从对端PE学到的VPNv4路由引入到ISIS
#
interface GigabitEthernet0/0/1
 ip address 192.168.1.1 255.255.255.0
 mpls
 mpls ldp  //公网侧接口使能mpls能力
#
interface GigabitEthernet1/0/0
 ip binding vpn-instance vpn1  //私网侧接口与VPN绑定
 ip address 10.1.1.1 255.255.255.0
 isis enable 1  //私网接口上使能ISIS进程
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
bgp 100
 peer 2.2.2.2 as-number 100
 peer 2.2.2.2 connect-interface LoopBack0  //使用32位掩码的Loopback接口地址来建立MP-IBGP对等体关
系
 #
 ipv4-family unicast
  undo synchronization
  peer 2.2.2.2 enable
 #
 ipv4-family vpnv4  //使能对等体交换VPNv4路由信息的能力
  policy vpn-target
  peer 2.2.2.2 enable
 #
 ipv4-family vpn-instance vpn1
  import-route isis 1  //将本端ISIS私网路由引入BGP-VPN实例IPv4地址族路由
表
#
ospf 1  //使用OSPF发布PE之间的路由，到达Loopback接口的路由
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
  network 192.168.1.0 0.0.0.255
#
return
```

步骤4 PE2上的配置

```
#
 sysname PE2
#
ip vpn-instance vpn1  //创建VPN实例
 ipv4-family
  route-distinguisher 1:1
  vpn-target 1:1 export-extcommunity
  vpn-target 1:1 import-extcommunity
#
mpls lsr-id 2.2.2.2  //配置MPLS能力
mpls
#
mpls ldp
#
isis 1 vpn-instance vpn1  //创建ISIS进程与VPN实例绑定
 network-entity 10.0000.1111.0002.00
 import-route bgp  //本端PE把从对端PE学到的VPNv4路由引入到ISIS
```

```
#
interface GigabitEthernet0/0/1
 ip address 192.168.1.2 255.255.255.0
 mpls
 mpls ldp  //公网侧接口使能mpls能力
#
interface GigabitEthernet1/0/0
 ip binding vpn-instance vpn1  //私网侧接口与VPN绑定
 ip address 10.1.2.1 255.255.255.0
 isis enable 1  //私网侧接口使能ISIS进程
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
bgp 100
 peer 1.1.1.1 as-number 100
 peer 1.1.1.1 connect-interface LoopBack0  //使用32位掩码的Loopback接口地址来建立MP-IBGP对等体关
系
 #
 ipv4-family unicast
  undo synchronization
  peer 1.1.1.1 enable
 #
 ipv4-family vpnv4  //使能对等体交换VPNv4路由信息的能力
  policy vpn-target
  peer 1.1.1.1 enable
 #
 ipv4-family vpn-instance vpn1
  import-route isis 1  //将本端ISIS私网路由引入BGP-VPN实例IPv4地址族路由表
#
ospf 1  //使用OSPF发布PE之间的路由，到达Loopback接口的路由
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
  network 2.2.2.2 0.0.0.0
#
return
```

步骤5 验证配置结果

1. 在PE上执行**display ip routing-table vpn-instance vpn1**命令，本端PE的VPN路由表中有达到对端PE私网的路由。

   PE1上的关键信息：

   ```
   Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

       10.1.2.0/24    IBGP    255  0           RD   2.2.2.2         GigabitEthernet0/0/1
     10.137.2.0/24    IBGP    255  20          RD   2.2.2.2         GigabitEthernet0/0/1
   ```

   PE2上的关键信息：

   ```
   Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

       10.1.1.0/24    IBGP    255  0           RD   1.1.1.1         GigabitEthernet0/0/1
     10.137.1.0/24    IBGP    255  20          RD   1.1.1.1         GigabitEthernet0/0/1
   ```

2. 在CE上执行**display ip routing-table protocol isis**，CE1，CE2学习到彼此的路由。

   CE1上的关键信息：

   ```
   Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

       10.1.2.0/24  ISIS-L2 15   74          D    10.1.1.1        GigabitEthernet0/0/1
     10.137.2.0/24  ISIS-L2 15   74          D    10.1.1.1        GigabitEthernet0/0/1
   ```

   CE2上的关键信息：

 版权所有 © 华为技术有限公司

```
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

  10.1.1.0/24     ISIS-L2 15   74          D   10.1.2.1        GigabitEthernet0/0/1
10.137.1.0/24     ISIS-L2 15   74          D   10.1.2.1        GigabitEthernet0/0/1
```

CE2上可以Ping通10.137.1.1，CE1上可以Ping通10.137.2.1。

----结束

配置注意事项

- 使用ISIS实现PE和CE间路由间交互时，需要给ISIS进程绑定VPN实例。
- PE上BGP和ISIS发布的路由需要相互引入。

6.5.8 配置设备之间部署 BGP/MPLS IP VPN 实现互通的示例（PE 和 CE 之间使用 BGP）

适用产品和版本

适用于所有版本。

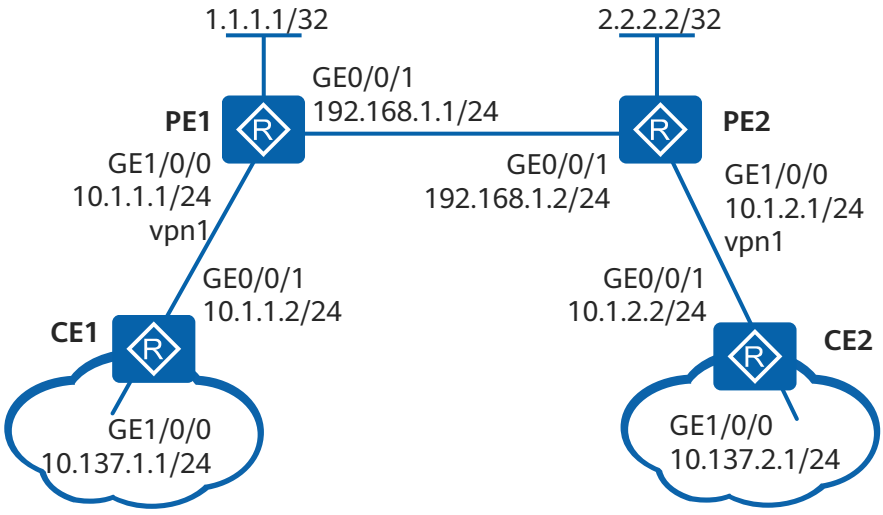
AR611E-S、AR611、AR631I-LTE4CN、AR631I-LTE4EA、AR611-LTE4EA、AR611-S、AR611W-S、AR611W、AR611W-LTE4CN、AR611W-LTE6EA、AR617VW、AR617VW-LTE4EA、AR617VW-LTE4、AR651C和AR651F-Lite不支持此功能。

AR303和AR303W不支持此功能。

组网需求

PE1连接CE1，PE2连接CE2，CE1和CE2均属于vpn1，PE与CE通过BGP进行路由交互。

图 6-65 配置 BGP MPLS/IP VPN 组网图



版权所有 © 华为技术有限公司

操作步骤

步骤1 CE1上的配置

```
#
 sysname CE1
#
interface GigabitEthernet0/0/1
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/0
 ip address 10.137.1.1 255.255.255.0
#
bgp 65101
 peer 10.1.1.1 as-number 100  //和本端PE建立EBGP邻居关系
 #
 ipv4-family unicast
  undo synchronization
  import-route direct
  peer 10.1.1.1 enable
#
return
```

步骤2 CE2上的配置

```
#
 sysname CE2
#
interface GigabitEthernet0/0/1
 ip address 10.1.2.2 255.255.255.0
#
interface GigabitEthernet1/0/0
 ip address 10.137.2.1 255.255.255.0
#
bgp 65102
 peer 10.1.2.1 as-number 100  //和本端PE建立EBGP邻居关系
 #
 ipv4-family unicast
  undo synchronization
  import-route direct
  peer 10.1.2.1 enable
#
return
```

步骤3 PE1上的配置

```
#
 sysname PE1
#
ip vpn-instance vpn1  //创建VPN实例
 ipv4-family
  route-distinguisher 1:1
  vpn-target 1:1 export-extcommunity
  vpn-target 1:1 import-extcommunity
#
mpls lsr-id 1.1.1.1  //配置MPLS能力
mpls
#
mpls ldp
#
interface GigabitEthernet0/0/1
 ip address 192.168.1.1 255.255.255.0
 mpls
 mpls ldp  //公网侧接口使能mpls能力
#
interface GigabitEthernet1/0/0
 ip binding vpn-instance vpn1  //私网侧接口与VPN绑定
 ip address 10.1.1.1 255.255.255.0
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
```

 版权所有 © 华为技术有限公司

```
#
bgp 100
 peer 2.2.2.2 as-number 100
 peer 2.2.2.2 connect-interface LoopBack0  //使用32位掩码的Loopback接口地址来建立MP-IBGP对等体关
系
 #
 ipv4-family unicast
  undo synchronization
  peer 2.2.2.2 enable
 #
 ipv4-family vpnv4  //使能对等体交换VPNv4路由信息的能力
  policy vpn-target
  peer 2.2.2.2 enable

#
 ipv4-family vpn-instance vpn1
  import-route direct
  peer 10.1.1.2 as-number 65101  //将本端CE配置为VPN私网对等体
#
ospf 1  //使用OSPF发布PE之间的路由，到达Loopback接口的路由
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
  network 192.168.1.0 0.0.0.255
#
return
```

步骤4 PE2上的配置

```
#
 sysname PE2
#
ip vpn-instance vpn1  //创建VPN实例
 ipv4-family
  route-distinguisher 1:1
  vpn-target 1:1 export-extcommunity
  vpn-target 1:1 import-extcommunity
#
mpls lsr-id 2.2.2.2  //配置MPLS能力
mpls
#
mpls ldp
#
interface GigabitEthernet0/0/1
 ip address 192.168.1.2 255.255.255.0
 mpls
 mpls ldp  //公网侧接口使能mpls能力
#
interface GigabitEthernet1/0/0
 ip binding vpn-instance vpn1  //私网侧接口与VPN绑定
 ip address 10.1.2.1 255.255.255.0
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
bgp 100
 peer 1.1.1.1 as-number 100
 peer 1.1.1.1 connect-interface LoopBack0  //使用32位掩码的Loopback接口地址来建立MP-IBGP对等体关
系
 #
 ipv4-family unicast
  undo synchronization
  peer 1.1.1.1 enable
 #
 ipv4-family vpnv4  //使能对等体交换VPNv4路由信息的能力
  policy vpn-target
  peer 1.1.1.1 enable
 #
 ipv4-family vpn-instance vpn1
  import-route direct
  peer 10.1.2.2 as-number 65102  //将本端CE配置为VPN私网对等体
```

 版权所有 © 华为技术有限公司

```
#
ospf 1  //使用OSPF发布PE之间的路由，到达Loopback接口的路由
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
  network 2.2.2.2 0.0.0.0
#
return
```

步骤5 验证配置结果

1. 在PE上执行**display ip routing-table vpn-instance vpn1**命令，本端PE的VPN路由表中有达到对端PE私网的路由。

   PE1上的关键信息：

   ```
   Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

       10.1.2.0/24     IBGP    255  0           RD   2.2.2.2         GigabitEthernet
   0/0/1
     10.137.2.0/24     IBGP    255  0           RD   2.2.2.2         GigabitEthernet
   0/0/1
   ```

   PE2上的关键信息：

   ```
   Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

       10.1.1.0/24     IBGP    255  0           RD   1.1.1.1         GigabitEthernet
   0/0/1
     10.137.1.0/24     IBGP    255  0           RD   1.1.1.1         GigabitEthernet
   0/0/1
   ```

2. 在CE上执行**display ip routing-table protocol bgp**，CE1，CE2学习到彼此的路由。

   CE1上的关键信息：

   ```
   Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

       10.1.2.0/24   EBGP    255  0           D   10.1.1.1      GigabitEthernet
   0/0/1
     10.137.2.0/24   EBGP    255  0           D   10.1.1.1      GigabitEthernet
   0/0/2
   ```

   CE2上的关键信息：

   ```
   Destination/Mask  Proto   Pre  Cost      Flags NextHop         Interface

       10.1.1.0/24   EBGP    255  0           D   10.1.2.1    GigabitEthernet
   0/0/1
     10.137.1.0/24   EBGP    255  0           D   10.1.2.1    GigabitEthernet
   0/0/2
   ```

   CE2上可以Ping通10.137.1.1，CE1上可以Ping通10.137.2.1。

----结束

配置注意事项

- PE和CE间的路由交互即可以使用IBGP，也可以使用EBGP，本例使用的是EBGP。
- 需要在PE的BGP-VPN实例IPv4地址族视图下，将CE配置为私网对等体。

 版权所有 © 华为技术有限公司

6.5.9 配置设备之间部署 BGP/MPLS IP VPN 实现互通的示例（PE 和 CE 之间使用 OSPF）

适用产品和版本

适用于所有版本。

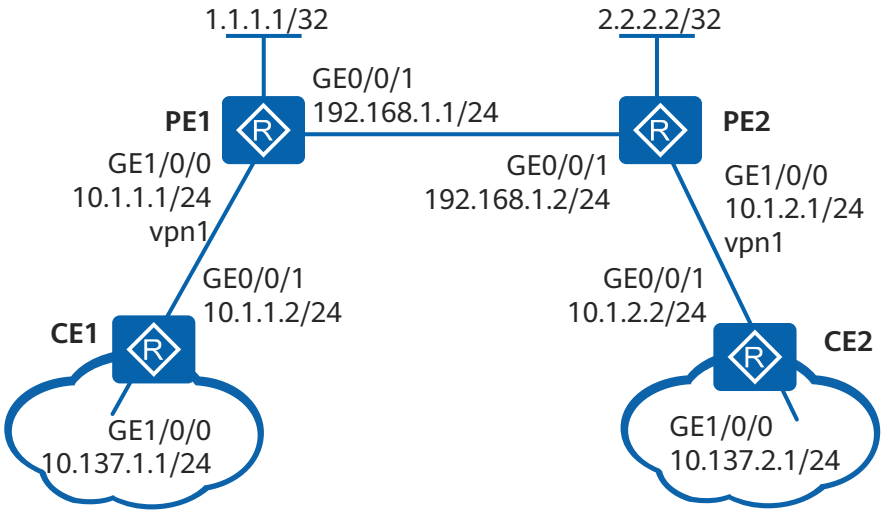
AR611E-S、AR611、AR631I-LTE4CN、AR631I-LTE4EA、AR611-LTE4EA、AR611-S、AR611W-S、AR611W、AR611W-LTE4CN、AR611W-LTE6EA、AR617VW、AR617VW-LTE4EA、AR617VW-LTE4、AR651C和AR651F-Lite不支持此功能。

AR303和AR303W不支持此功能。

组网需求

PE1连接CE1，PE2连接CE2，CE1和CE2均属于vpn1，PE与CE通过OSPF进行路由交互。

图 6-66 配置 BGP MPLS/IP VPN 组网图



操作步骤

步骤1 CE1上的配置

```
#
 sysname CE1
#
interface GigabitEthernet0/0/1
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/0
 ip address 10.137.1.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 10.137.1.0 0.0.0.255
#
return
```


版权所有 © 华为技术有限公司

步骤2 CE2上的配置

```
#
 sysname CE2
#
interface GigabitEthernet0/0/1
 ip address 10.1.2.2 255.255.255.0
#
interface GigabitEthernet1/0/0
 ip address 10.137.2.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.1.2.0 0.0.0.255
  network 10.137.2.0 0.0.0.255
#
return
```

步骤3 PE1上的配置

```
#
 sysname PE1
#
ip vpn-instance vpn1  //创建VPN实例
 ipv4-family
  route-distinguisher 1:1
  vpn-target 1:1 export-extcommunity
  vpn-target 1:1 import-extcommunity
#
mpls lsr-id 1.1.1.1  //配置MPLS能力
mpls
#
mpls ldp
#
interface GigabitEthernet0/0/1
 ip address 192.168.1.1 255.255.255.0
 mpls
 mpls ldp  //公网侧接口使能mpls能力
#
interface GigabitEthernet1/0/0
 ip binding vpn-instance vpn1  //私网侧接口与VPN绑定
 ip address 10.1.1.1 255.255.255.0
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
bgp 100
 peer 2.2.2.2 as-number 100
 peer 2.2.2.2 connect-interface LoopBack0  //使用32位掩码的Loopback接口地址来建立MP-IBGP对等体关
系
 #
 ipv4-family unicast
  undo synchronization
  peer 2.2.2.2 enable
 #
 ipv4-family vpnv4  //使能对等体交换VPNv4路由信息的能力
  policy vpn-target
  peer 2.2.2.2 enable
 #
 ipv4-family vpn-instance vpn1
  import-route ospf 3  //将本端OSPF私网路由引入BGP-VPN实例IPv4地址族路由
表
#
ospf 1  //使用OSPF发布PE之间的路由，到达Loopback接口的路由
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
  network 192.168.1.0 0.0.0.255
#
ospf 3 vpn-instance vpn1  //创建OSPF进程，并于VPN实例绑定
 import-route bgp  //本端PE把从对端PE学到的VPNv4路由引入到
OSPF
```

 版权所有 © 华为技术有限公司

```
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
#
return
```

步骤4 PE2上的配置

```
#
 sysname PE2
#
ip vpn-instance vpn1  //创建VPN实例
 ipv4-family
  route-distinguisher 1:1
  vpn-target 1:1 export-extcommunity
  vpn-target 1:1 import-extcommunity
#
mpls lsr-id 2.2.2.2  //配置MPLS能力
mpls
#
mpls ldp
#
interface GigabitEthernet0/0/1
 ip address 192.168.1.2 255.255.255.0
 mpls
 mpls ldp  //公网侧接口使能mpls能力
#
interface GigabitEthernet1/0/0
 ip binding vpn-instance vpn1  //私网侧接口与VPN绑定
 ip address 10.1.2.1 255.255.255.0
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
bgp 100
 peer 1.1.1.1 as-number 100
 peer 1.1.1.1 connect-interface LoopBack0  //使用32位掩码的Loopback接口地址来建立MP-IBGP对等体关
系
 #
 ipv4-family unicast
  undo synchronization
  peer 1.1.1.1 enable
 #
 ipv4-family vpnv4  //使能对等体交换VPNv4路由信息的能力
  policy vpn-target
  peer 1.1.1.1 enable
 #
 ipv4-family vpn-instance vpn1
  import-route ospf 2  //将本端OSPF私网路由引入BGP-VPN实例IPv4地址族路由
表
#
ospf 1  //使用OSPF发布PE之间的路由，到达Loopback接口的路由
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
  network 2.2.2.2 0.0.0.0
#
ospf 2 vpn-instance vpn1
 import-route bgp  //本端PE把从对端PE学到的VPNv4路由引入到
OSPF
 area 0.0.0.0
  network 10.1.2.0 0.0.0.255
#
return
```

步骤5 验证配置结果

1. 在PE上执行**display ip routing-table vpn-instance vpn1**命令，本端PE的VPN路由表中有达到对端PE私网的路由。

   PE1上的关键信息：

 版权所有 © 华为技术有限公司

```
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

    10.1.2.0/24     IBGP    255  0           RD   2.2.2.2         GigabitEthernet
0/0/1
   10.137.2.0/24    IBGP    255  3           RD   2.2.2.2         GigabitEthernet
0/0/1
```

PE2上的关键信息：

```
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

    10.1.1.0/24     IBGP    255  0           RD   1.1.1.1         GigabitEthernet
0/0/1
   10.137.1.0/24    IBGP    255  3           RD   1.1.1.1         GigabitEthernet
0/0/1
```

2. 在CE上执行**display ip routing-table protocol ospf**，CE1，CE2学习到彼此的路由。

   CE1上的关键信息：

```
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

     10.1.2.0/24    O_ASE   150  1           D   10.1.1.1        GigabitEthernet
0/0/1
    10.137.2.0/24   OSPF    10   4           D   10.1.1.1        GigabitEthernet
0/0/1
```

   CE2上的关键信息：

```
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

     10.1.1.0/24    O_ASE   150  1           D   10.1.2.1        GigabitEthernet
0/0/1
    10.137.1.0/24   OSPF    10   4           D   10.1.2.1        GigabitEthernet
0/0/1
```

   CE2上可以Ping通10.137.1.1，CE1上可以Ping通10.137.2.1。

----结束

配置注意事项

- 使用OSPF实现PE和CE间路由间交互时，需要给OSPF进程绑定VPN实例。
- PE上BGP和OSPF发布的路由需要相互引入。

6.5.10 配置 OSPF 伪连接，避免在同一个 OSPF 区域内属于同一个 VPN 的用户之间的通信总是通过 OSPF 区域内路由转发示例

适用产品和版本

适用于所有版本。

AR611E-S、AR611、AR631I-LTE4CN、AR631I-LTE4EA、AR611-LTE4EA、AR611-S、AR611W-S、AR611W、AR611W-LTE4CN、AR611W-LTE6EA、AR617VW、AR617VW-LTE4EA、AR617VW-LTE4、AR651C和AR651F-Lite不支持此功能。

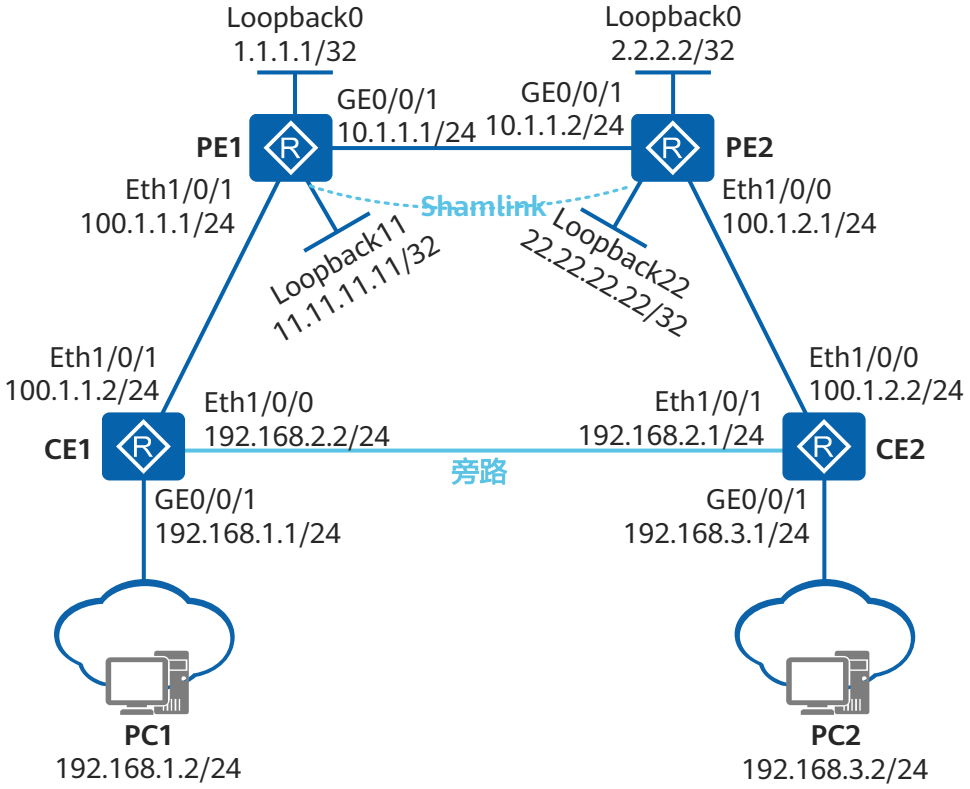
AR303和AR303W不支持此功能。

 版权所有 © 华为技术有限公司

组网需求

PE1连接CE1，PE2连接CE2，CE1和CE2均属于vpn1，PE与CE通过OSPF进行路由交互。CE1和CE2在同一个OSPF区域，要求CE1与CE2之间的VPN流量通过MPLS骨干网转发，不使用OSPF的区域内路由。

图 6-67 配置 BGP MPLS/IP VPN + OSPF 虚连接组网图



操作步骤

步骤1 CE1上的配置

```
#
 sysname CE1
#
interface Ethernet1/0/0
 ip address 192.168.2.2 255.255.255.0
 ospf cost 10
#
interface Ethernet1/0/1
 ip address 100.1.1.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 ip address 192.168.1.1 255.255.255.0
#

ospf 1
 area 0.0.0.0
  network 100.1.1.0 0.0.0.255
  network 192.168.1.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
#
return
```


版权所有 © 华为技术有限公司

步骤2 CE2上的配置

```
#
 sysname CE2
#
interface GigabitEthernet0/0/1
 ip address 192.168.3.1 255.255.255.0
#
interface Ethernet1/0/0
 ip address 100.1.2.2 255.255.255.0
#

interface Ethernet1/0/1
 ip address 192.168.2.1 255.255.255.0
 ospf cost 10
#

ospf 1
 area 0.0.0.0
  network 100.1.2.0 0.0.0.255
  network 192.168.3.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
#
return
```

步骤3 PE1上的配置

```
#
 sysname PE1
#
ip vpn-instance vpn1
 ipv4-family
  route-distinguisher 1:1
  vpn-target 1:1 export-extcommunity
  vpn-target 1:1 import-extcommunity
#
mpls lsr-id 1.1.1.1
mpls
#
mpls ldp
#

interface Ethernet1/0/1
 ip binding vpn-instance vpn1
 ip address 100.1.1.1 255.255.255.0
#

interface GigabitEthernet0/0/1
 ip address 10.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
interface LoopBack11
 ip binding vpn-instance vpn1  //用于建立伪连接的Loopback接口绑定到VPN实
例
 ip address 11.11.11.11 255.255.255.255
#

bgp 100
 peer 2.2.2.2 as-number 100
 peer 2.2.2.2 connect-interface LoopBack0
 #
 ipv4-family unicast
  undo synchronization
  peer 2.2.2.2 enable
 #
 ipv4-family vpnv4
  policy vpn-target
```

 版权所有 © 华为技术有限公司

```
 peer 2.2.2.2 enable
 #
 ipv4-family vpn-instance vpn1
  import-route direct  //引入伪连接端点地址的路由，伪连接端点地址将被作为VPN-IPv4地址发
布
  import-route ospf 2
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 1.1.1.1 0.0.0.0
#
ospf 2 vpn-instance vpn1
 import-route bgp
 area 0.0.0.0
  network 100.1.1.0 0.0.0.255
  sham-link 11.11.11.11 22.22.22.22  //指定伪连接的源地址和目的地址
#
return
```

步骤4 PE2上的配置

```
#
 sysname PE2
#
ip vpn-instance vpn1
 ipv4-family
  route-distinguisher 1:1
  vpn-target 1:1 export-extcommunity
  vpn-target 1:1 import-extcommunity
#
mpls lsr-id 2.2.2.2
mpls
#
mpls ldp
#
interface Ethernet1/0/0
 ip binding vpn-instance vpn1
 ip address 100.1.2.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 ip address 10.1.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#

interface LoopBack22
 ip binding vpn-instance vpn1  //用于建立伪连接的Loopback接口绑定到VPN实
例
 ip address 22.22.22.22 55.255.255.255
#

bgp 100
 peer 1.1.1.1 as-number 100
 peer 1.1.1.1 connect-interface LoopBack0
 #
 ipv4-family unicast
  undo synchronization
  peer 1.1.1.1 enable
 #
 ipv4-family vpnv4
  policy vpn-target
  peer 1.1.1.1 enable
 #
 ipv4-family vpn-instance vpn1
  import-route direct  //引入伪连接端点地址的路由，伪连接端点地址将被作为VPN-IPv4地址发
布
```

 版权所有 © 华为技术有限公司

```
 import-route ospf 2
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 2.2.2.2 0.0.0.0
#
ospf 2 vpn-instance vpn1
 import-route bgp
 area 0.0.0.0
  network 100.1.2.0 0.0.0.255
  sham-link 22.22.22.22 11.11.11.11  //指定伪连接的源地址和目的地址
#
return
```

步骤5 验证配置结果

1. 在PE上执行**display ospf 2 sham-link**查看伪连接的建立情况。

   以PE2上显示为例：

   ```
   Area          NeighborId      Source-IP       Destination-IP  State Cost
   0.0.0.0       100.1.1.1       22.22.22.22     11.11.11.11     P-2-P 1
   ```

2. 在PE上执行**display ip routing-table vpn-instance vpn1**命令，本端PE的VPN路由表中有达到对端PE私网的路由。

   PE1上的关键信息：

   ```
   Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

    11.11.11.11/32    Direct  0    0           D   127.0.0.1       LoopBack0
    22.22.22.22/32    IBGP    255  0           RD  2.2.2.2         GigabitEthernet
   0/0/1
      100.1.1.0/24    Direct  0    0           D   100.1.1.1       Ethernet1/0/1
      100.1.1.1/32    Direct  0    0           D   127.0.0.1       Ethernet1/0/1
    100.1.1.255/32    Direct  0    0           D   127.0.0.1       Ethernet1/0/1
      100.1.2.0/24    IBGP    255  0           RD  2.2.2.2         GigabitEthernet
   0/0/1
    192.168.1.0/24    OSPF    10   2           D   100.1.1.2       Ethernet1/0/1
    192.168.2.0/24    OSPF    10   11          D   100.1.1.2       Ethernet1/0/1
    192.168.3.0/24    IBGP    255  3           RD  2.2.2.2         GigabitEthernet
   0/0/1
   255.255.255.255/32 Direct  0    0           D   127.0.0.1       InLoopBack0
   ```

   PE2上的关键信息：

   ```
   Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

    11.11.11.11/32    IBGP    255  0           RD  1.1.1.1         GigabitEthernet
   0/0/1
    22.22.22.22/32    Direct  0    0           D   127.0.0.1       LoopBack0
      100.1.1.0/24    IBGP    255  0           RD  1.1.1.1         GigabitEthernet
   0/0/1
      100.1.2.0/24    Direct  0    0           D   100.1.2.1       Ethernet1/0/0
      100.1.2.1/32    Direct  0    0           D   127.0.0.1       Ethernet1/0/0
    100.1.2.255/32    Direct  0    0           D   127.0.0.1       Ethernet1/0/0
    192.168.1.0/24    IBGP    255  3           RD  1.1.1.1         GigabitEthernet
   0/0/1
      192.168.2.0/24  OSPF    10   11          D   100.1.2.2       Ethernet1/0/0
      192.168.3.0/24  OSPF    10   2           D   100.1.2.2       Ethernet1/0/0
   255.255.255.255/32 Direct  0    0           D   127.0.0.1       InLoopBack0
   ```

3. 在CE上执行**display ip routing-table protocol ospf**，CE1，CE2学习到彼此的路由，出接口为连接PE的接口。

   CE1上的关键信息：

 版权所有 © 华为技术有限公司

```
  100.1.2.0/24  OSPF    10   3          D   100.1.1.1     Ethernet1/0/1
192.168.3.0/24  OSPF    10   4          D   100.1.1.1     Ethernet1/0/1
```

CE2上的关键信息：

```
  100.1.1.0/24  OSPF    10   3          D   100.1.2.1     Ethernet1/0/0
192.168.1.0/24  OSPF    10   4          D   100.1.2.1     Ethernet1/0/0
```

----结束

配置注意事项

- 伪连接端点地址的路由不能通过私网的OSPF进程发布到对端PE上。如果伪连接端点地址的路由通过私网的OSPF进程发布到对端PE上，则对端PE将同时存在两条到该伪连接端点地址的路由。其中一条是通过私网OSPF学习到的，另一条是通过MP-BGP学习到的。OSPF路由比BGP路由优先级高，对端PE将选择OSPF路由，伪连接无法建立成功。
- PE上需要使用掩码为32位的Loopback接口建立伪连接。
- 为了使VPN流量通过MPLS骨干网转发，在配置sham-link时，应保证sham link的cost值小于通过用户网络转发时OSPF路由的cost值。因此，常常需要调整旁路转发接口的cost值，使它比sham link的cost值大。

6.5.11 配置设备之间部署 BGP/MPLS IP VPN 实现互通的示例（PE 和 CE 之间使用静态路由）

适用产品和版本

适用于所有版本。

AR611E-S、AR611、AR631I-LTE4CN、AR631I-LTE4EA、AR611-LTE4EA、AR611-S、AR611W-S、AR611W、AR611W-LTE4CN、AR611W-LTE6EA、AR617VW、AR617VW-LTE4EA、AR617VW-LTE4、AR651C和AR651F-Lite不支持此功能。

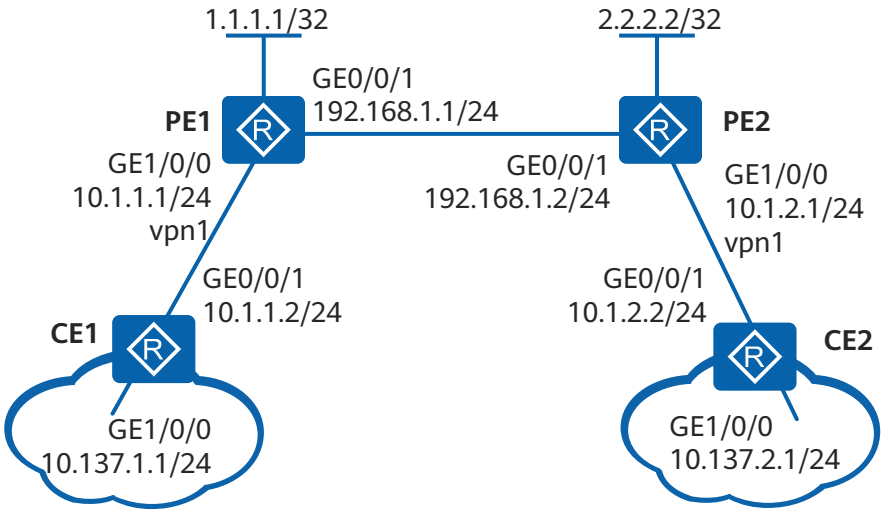
AR303和AR303W不支持此功能。

组网需求

PE1连接CE1，PE2连接CE2，CE1和CE2均属于vpn1，PE与CE之间配置静态路由实现互访。

 版权所有 © 华为技术有限公司

图 6-68 配置 BGP MPLS/IP VPN 组网图



操作步骤

步骤1 CE1上的配置

```
#
 sysname CE1
#
interface GigabitEthernet0/0/1
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/0
 ip address 10.137.1.1 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 10.1.1.1
#
return
```

步骤2 CE2上的配置

```
#
 sysname CE2
#
interface GigabitEthernet0/0/1
 ip address 10.1.2.2 255.255.255.0
#
interface GigabitEthernet1/0/0
 ip address 10.137.2.1 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 10.1.2.1
#
return
```

步骤3 PE1上的配置

```
#
 sysname PE1
#
ip vpn-instance vpn1  //创建VPN实例
 ipv4-family
  route-distinguisher 1:1
  vpn-target 1:1 export-extcommunity
  vpn-target 1:1 import-extcommunity
#
mpls lsr-id 1.1.1.1  //配置MPLS能力
```


版权所有 © 华为技术有限公司

```
mpls
#
mpls ldp
#
interface GigabitEthernet0/0/1
 ip address 192.168.1.1 255.255.255.0
 mpls
 mpls ldp  //公网侧接口使能mpls能力
#
interface GigabitEthernet1/0/0
 ip binding vpn-instance vpn1  //私网侧接口与VPN绑定
 ip address 10.1.1.1 255.255.255.0
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
bgp 100
 peer 2.2.2.2 as-number 100
 peer 2.2.2.2 connect-interface LoopBack0  //使用32位掩码的Loopback接口地址来建立MP-IBGP对等体关
系
 #
 ipv4-family unicast
  undo synchronization
  peer 2.2.2.2 enable
 #
 ipv4-family vpnv4  //使能对等体交换VPNv4路由信息的能力
  policy vpn-target
  peer 2.2.2.2 enable

#
 ipv4-family vpn-instance vpn1
  import-route static  //引入私网的静态路由
#
ospf 1  //使用OSPF发布PE之间的路由，到达Loopback接口的路由
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
  network 192.168.1.0 0.0.0.255
#
ip route-static vpn-instance vpn1 10.137.1.0 255.255.255.0 10.1.1.2
#
return
```

步骤4 PE2上的配置

```
#
 sysname PE2
#
ip vpn-instance vpn1  //创建VPN实例
 ipv4-family
  route-distinguisher 1:1
  vpn-target 1:1 export-extcommunity
  vpn-target 1:1 import-extcommunity
#
mpls lsr-id 2.2.2.2  //配置MPLS能力
mpls
#
mpls ldp
#
interface GigabitEthernet0/0/1
 ip address 192.168.1.2 255.255.255.0
 mpls
 mpls ldp  //公网侧接口使能mpls能力
#
interface GigabitEthernet1/0/0
 ip binding vpn-instance vpn1  //私网侧接口与VPN绑定
 ip address 10.1.2.1 255.255.255.0
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
```

 版权所有 © 华为技术有限公司

```
bgp 100
 peer 1.1.1.1 as-number 100
 peer 1.1.1.1 connect-interface LoopBack0  //使用32位掩码的Loopback接口地址来建立MP-IBGP对等体关
系
 #
 ipv4-family unicast
  undo synchronization
  peer 1.1.1.1 enable
 #
 ipv4-family vpnv4  //使能对等体交换VPNv4路由信息的能力
  policy vpn-target
  peer 1.1.1.1 enable
 #
 ipv4-family vpn-instance vpn1
  import-route static  //引入私网的静态路由
#
ospf 1  //使用OSPF发布PE之间的路由，到达Loopback接口的路由
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
  network 2.2.2.2 0.0.0.0
#
ip route-static vpn-instance vpn1 10.137.2.0 255.255.255.0 10.1.2.2
#
return
```

步骤5 验证配置结果

在PE上执行**display ip routing-table vpn-instance vpn1**命令，本端PE的VPN路由表中有达到对端PE私网的路由。 CE2上可以Ping通10.137.1.1，CE1上可以Ping通10.137.2.1。

PE1上的关键信息：

```
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

    10.1.2.0/24     IBGP    255  0           RD  2.2.2.2         GigabitEthernet
0/0/1
   10.137.2.0/24    IBGP    255  20          RD  2.2.2.2         GigabitEthernet
0/0/1
```

PE2上的关键信息：

```
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

    10.1.1.0/24     IBGP    255  0           RD  1.1.1.1         GigabitEthernet
0/0/1
   10.137.1.0/24    IBGP    255  20          RD  1.1.1.1         GigabitEthernet
0/0/1
```

----结束

配置注意事项

- PE上的BGP需要引入静态VPN路由。
- CE上需要配置访问其他私网的静态路由，

6.5.12 配置设备之间部署 BGP/MPLS IP VPN 实现互通的示例（PE 和 CE 之间使用 RIP）

适用产品和版本

适用于所有版本。

 版权所有 © 华为技术有限公司

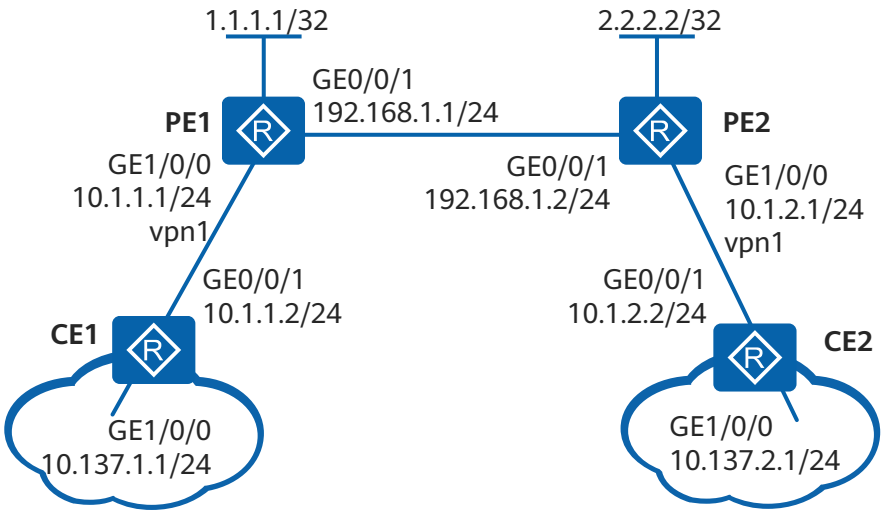
AR611E-S、AR611、AR631I-LTE4CN、AR631I-LTE4EA、AR611-LTE4EA、AR611-S、AR611W-S、AR611W、AR611W-LTE4CN、AR611W-LTE6EA、AR617VW、AR617VW-LTE4EA、AR617VW-LTE4、AR651C和AR651F-Lite不支持此功能。

AR303和AR303W不支持此功能。

组网需求

PE1连接CE1，PE2连接CE2，CE1和CE2均属于vpn1，PE与CE通过RIP进行路由交互。

图 6-69 配置 BGP MPLS/IP VPN 组网图



操作步骤

步骤1 CE1上的配置

```
#
 sysname CE1
#
interface GigabitEthernet0/0/1
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/0
 ip address 10.137.1.1 255.255.255.0
#
rip 1  //创建RIP进程
 version 2
 network 10.0.0.0
#
return
```

步骤2 CE2上的配置

```
#
 sysname CE2
#
interface GigabitEthernet0/0/1
 ip address 10.1.2.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 ip address 10.137.2.1 255.255.255.0
#
```


版权所有 © 华为技术有限公司

```
rip 1    //创建RIP进程
 version 2
 network 10.0.0.0
#
return
```

步骤3 PE1上的配置

```
#
 sysname PE1
#
ip vpn-instance vpn1  //创建VPN实例
 ipv4-family
  route-distinguisher 1:1
  vpn-target 1:1 export-extcommunity
  vpn-target 1:1 import-extcommunity
#
mpls lsr-id 1.1.1.1  //配置MPLS能力
mpls
#
mpls ldp
#
interface GigabitEthernet0/0/1
 ip address 192.168.1.1 255.255.255.0
 mpls
 mpls ldp  //公网侧接口使能mpls能力
#
interface GigabitEthernet1/0/0
 ip binding vpn-instance vpn1  //私网侧接口与VPN绑定
 ip address 10.1.1.1 255.255.255.0
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
bgp 100
 peer 2.2.2.2 as-number 100
 peer 2.2.2.2 connect-interface LoopBack0  //使用32位掩码的Loopback接口地址来建立MP-IBGP对等体关
系
 #
 ipv4-family unicast
  undo synchronization
  peer 2.2.2.2 enable
 #
 ipv4-family vpnv4  //使能对等体交换VPNv4路由信息的能力
  policy vpn-target
  peer 2.2.2.2 enable
 #
 ipv4-family vpn-instance vpn1
  import-route rip 1  //将本端RIP私网路由引入BGP-VPN实例IPv4地址族路由
表
#
ospf 1  //使用OSPF发布PE之间的路由，到达Loopback接口的路由
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
  network 192.168.1.0 0.0.0.255
#
rip 1 vpn-instance vpn1  //创建RIP进程，并与VPN实例绑定
 import-route bgp  //PE把从对端PE学到的VPNv4路由引入到RIP
 version 2
 network 10.0.0.0
#
return
```

步骤4 PE2上的配置

```
#
 sysname PE2
#
ip vpn-instance vpn1  //创建VPN实例
 ipv4-family
  route-distinguisher 1:1
```

 版权所有 © 华为技术有限公司

```
  vpn-target 1:1 export-extcommunity
  vpn-target 1:1 import-extcommunity
#
mpls lsr-id 2.2.2.2  //配置MPLS能力
mpls
#
mpls ldp
#
interface GigabitEthernet0/0/1
 ip address 192.168.1.2 255.255.255.0
 mpls
 mpls ldp  //公网侧接口使能mpls能力
#
interface GigabitEthernet1/0/0
 ip binding vpn-instance vpn1  //私网侧接口与VPN绑定
 ip address 10.1.2.1 255.255.255.0
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
bgp 100
 peer 1.1.1.1 as-number 100
 peer 1.1.1.1 connect-interface LoopBack0  //使用32位掩码的Loopback接口地址来建立MP-IBGP对等体关
系
 #
 ipv4-family unicast
  undo synchronization
  peer 1.1.1.1 enable
 #
 ipv4-family vpnv4  //使能对等体交换VPNv4路由信息的能力
  policy vpn-target
  peer 1.1.1.1 enable
 #
 ipv4-family vpn-instance vpn1
  import-route rip 1  //将本端RIP私网路由引入BGP-VPN实例IPv4地址族路由表
#
ospf 1  //使用OSPF发布PE之间的路由，到达Loopback接口的路由
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
  network 2.2.2.2 0.0.0.0
#
rip 1 vpn-instance vpn1
 import-route bgp  //PE把从对端PE学到的VPNv4路由引入到RIP
 version 2
 network 10.0.0.0
#
return
```

步骤5 验证配置结果

1. 在PE上执行**display ip routing-table vpn-instance vpn1**命令，本端PE的VPN路由表中有达到对端PE私网的路由。

   PE1上的关键信息：

   ```
   Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      10.1.2.0/24     IBGP    255  0           RD   2.2.2.2         GigabitEthernet
   0/0/1
    10.137.2.0/24     IBGP    255  1           RD   2.2.2.2         GigabitEthernet
   0/0/1
   ```

   PE2上的关键信息：

   ```
   Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      10.1.1.0/24     IBGP    255  0           RD   1.1.1.1         GigabitEthernet
   0/0/1
   ```

 版权所有 © 华为技术有限公司

```
 10.137.1.0/24    IBGP   255  1          RD   1.1.1.1         GigabitEthernet
0/0/1
```

2. 在CE上执行**display ip routing-table protocol rip**，CE1，CE2学习到彼此的路由。

   CE1上的关键信息：

```
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

    10.1.2.0/24    RIP     100  1           D   10.1.1.1    GigabitEthernet
0/0/2
  10.137.2.0/24    RIP     100  1           D   10.1.1.1    GigabitEthernet
0/0/2
```

   CE2上的关键信息：

```
Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

    10.1.1.0/24    RIP     100  1           D   10.1.2.1    GigabitEthernet
0/0/2
  10.137.1.0/24    RIP     100  1           D   10.1.2.1    GigabitEthernet
0/0/2
```

   CE2上可以Ping通10.137.1.1，CE1上可以Ping通10.137.2.1。

----结束

配置注意事项

- 使用RIP实现PE和CE间路由间交互时，需要给RIP进程指定VPN实例。
- PE上BGP和RIP发布的路由需要相互引入。

6.5.13 配置路由反射器优化 VPN 骨干层的示例

适用产品和版本

适用于所有版本。

AR611E-S、AR611、AR631I-LTE4CN、AR631I-LTE4EA、AR611-LTE4EA、AR611-S、AR611W-S、AR611W、AR611W-LTE4CN、AR611W-LTE6EA、AR617VW、AR617VW-LTE4EA、AR617VW-LTE4、AR651C和AR651F-Lite不支持此功能。

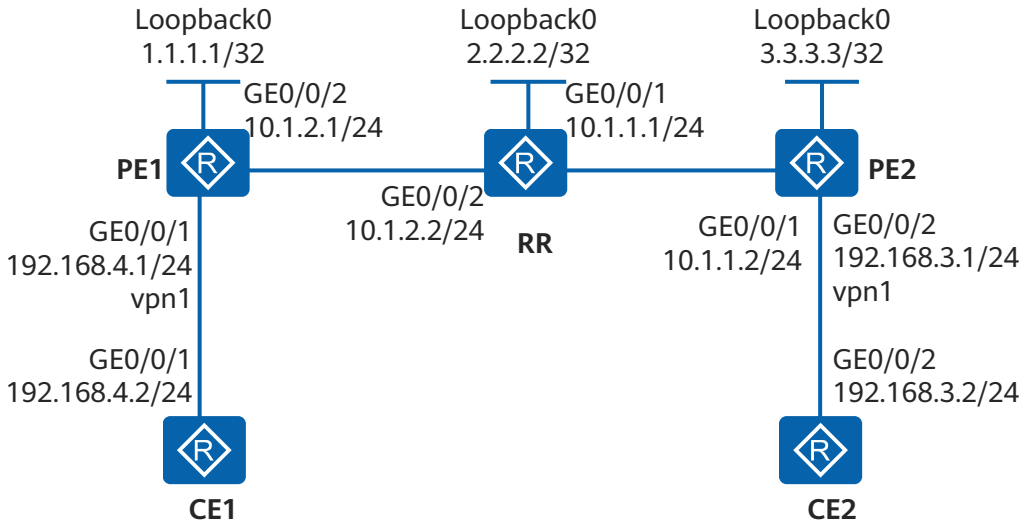
AR303和AR303W不支持此功能。

组网需求

PE1连接CE1，PE2连接CE2，CE1和CE2均属于vpn1。PE1、PE2分别和反射器RR建立MP-IBGP连接，VPN路由都由RR反射传播。

 版权所有 © 华为技术有限公司

图 6-70 配置路由反射器优化 VPN 骨干层组网图



操作步骤

步骤1 CE1上的配置

```
#
 sysname CE1
#
interface GigabitEthernet0/0/1
 ip address 192.168.4.2 255.255.255.0
#
bgp 65001  //和PE1建立EBGP邻居
 peer 192.168.4.1 as-number 100
 #
 ipv4-family unicast
  undo synchronization
  import-route direct
  peer 192.168.4.1 enable
#
return
```

步骤2 CE2上的配置

```
#
 sysname CE2
#
interface GigabitEthernet0/0/2
 ip address 192.168.3.2 255.255.255.0
#
bgp 65002  //和PE2建立EBGP邻居
 peer 192.168.3.1 as-number 100
 #
 ipv4-family unicast
  undo synchronization
  import-route direct
  peer 192.168.3.1 enable
#
return
```

步骤3 PE1上的配置

```
#
 sysname PE1
#
```


版权所有 © 华为技术有限公司

```
ip vpn-instance vpn1
 ipv4-family
  route-distinguisher 1:1
  vpn-target 1:1 export-extcommunity
  vpn-target 1:1 import-extcommunity
#
mpls lsr-id 1.1.1.1
mpls
#
mpls ldp
#
interface GigabitEthernet0/0/1
 ip binding vpn-instance vpn1
 ip address 192.168.4.1 255.255.255.0
#
interface GigabitEthernet0/0/2
 ip address 10.1.2.1 255.255.255.0
 mpls
 mpls ldp
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
bgp 100
 peer 2.2.2.2 as-number 100  //指定RR为IBGP对等体
 peer 2.2.2.2 connect-interface LoopBack0
 #
 ipv4-family unicast
  undo synchronization
  peer 2.2.2.2 enable
 #
 ipv4-family vpnv4
  policy vpn-target
  peer 2.2.2.2 enable
 #
 ipv4-family vpn-instance vpn1
  peer 192.168.4.2 as-number 65001
#
ospf 1
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
  network 10.1.2.0 0.0.0.255
#
return
```

步骤4 PE2上的配置

```
#
 sysname PE2
#
ip vpn-instance vpn1
 ipv4-family
  route-distinguisher 1:1
  vpn-target 1:1 export-extcommunity
  vpn-target 1:1 import-extcommunity
#
mpls lsr-id 3.3.3.3
mpls
#
mpls ldp
#
interface GigabitEthernet0/0/1
 ip address 10.1.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet0/0/2
 ip binding vpn-instance vpn1
 ip address 192.168.3.1 255.255.255.0
#
```

 版权所有 © 华为技术有限公司

```
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
#
bgp 100
 peer 2.2.2.2 as-number 100  //指定RR为IBGP对等体
 peer 2.2.2.2 connect-interface LoopBack0
 #
 ipv4-family unicast
  undo synchronization
  peer 2.2.2.2 enable
 #
 ipv4-family vpnv4
  policy vpn-target
  peer 2.2.2.2 enable
 #
 ipv4-family vpn-instance vpn1
  import-route direct
#
ospf 1
 area 0.0.0.0
  network 3.3.3.3 0.0.0.0
  network 10.1.1.0 0.0.0.255
#
return
```

步骤5 RR上的配置

```
#
 sysname RR
#
mpls lsr-id 2.2.2.2
mpls
#
mpls ldp
#

interface GigabitEthernet0/0/1
 ip address 10.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet0/0/2
 ip address 10.1.2.2 255.255.255.0
 mpls
 mpls ldp
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
bgp 100
 peer 3.3.3.3 as-number 100  //指定PE2为RR的IBGP对等体
 peer 3.3.3.3 connect-interface LoopBack0
 peer 1.1.1.1 as-number 100  //指定PE1为RR的IBGP对等体
 peer 1.1.1.1 connect-interface LoopBack0
 #
 ipv4-family unicast
  undo synchronization
  peer 3.3.3.3 enable
  peer 1.1.1.1 enable
 #
 ipv4-family vpnv4
  undo policy vpn-target  //配置RR不对接收的VPNv4路由使能VPN-Target进行过
滤。
  peer 3.3.3.3 enable
  peer 3.3.3.3 reflect-client  //使能RR的BGP-VPNv4路由反射功能，PE2为客户机
  peer 1.1.1.1 enable
  peer 1.1.1.1 reflect-client  //使能RR的BGP-VPNv4路由反射功能，PE1为客户机
#
ospf 1
 area 0.0.0.0
```

 版权所有 © 华为技术有限公司

```
 network 2.2.2.2 0.0.0.0
 network 10.1.1.0 0.0.0.255
 network 10.1.2.0 0.0.0.255
#
return
```

步骤6 验证配置结果

1. 在PE上或者RR上执行**dis bgp vpnv4 all peer** 查看BGP VPNv4对等体的建立情况。

   PE1上的关键信息：

   ```
    Peer            V          AS  MsgRcvd  MsgSent  OutQ  Up/Down       State Pre
   fRcv

    2.2.2.2 4         100       13       11     0 00:08:10 Established
     1
   ```

   PE2上的关键信息：

   ```
    Peer            V          AS  MsgRcvd  MsgSent  OutQ  Up/Down       State Pre
   fRcv

    2.2.2.2 4         100       18       19     0 00:13:44 Established
     1
   ```

   RR上的关键信息：

   ```
    Peer            V          AS  MsgRcvd  MsgSent  OutQ  Up/Down       State Pre
   fRcv

    3.3.3.3 4         100       19       19     0 00:14:13 Established
     1
    1.1.1.1 4         100       16       19     0 00:13:36 Established
     1
   ```

2. 在PE上执行**display ip routing-table vpn-instance vpn1**命令，本端PE的VPN路由表中有达到对端PE私网的路由。

   PE1上的关键信息：

   ```
   Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      192.168.3.0/24  IBGP   255  0           RD   3.3.3.3 GigabitEthernet
   0/0/2
   ```

   PE2上的关键信息：

   ```
   Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface
   ...
      192.168.4.0/24  IBGP   255  0           RD   1.1.1.1 GigabitEthernet
   0/0/1
   ...
   ```

----结束

配置注意事项

- PE只需要与RR建立MP-IBPG邻居关系。
- 反射器上无需配置VPN实例。

6.6 VLL

 版权所有 © 华为技术有限公司

6.6.1 配置设备之间部署 Martini 方式 VLL 实现互通的示例

规格

AR300系列不支持此功能。

AR611E-S、AR611、AR631I-LTE4CN、AR631I-LTE4EA、AR611-LTE4EA、AR611-S、AR611W-S、AR611W、AR611W-LTE4CN、AR611W-LTE6EA、AR617VW、AR617VW-LTE4EA、AR617VW-LTE4、AR651C和AR651F-Lite不支持此功能。

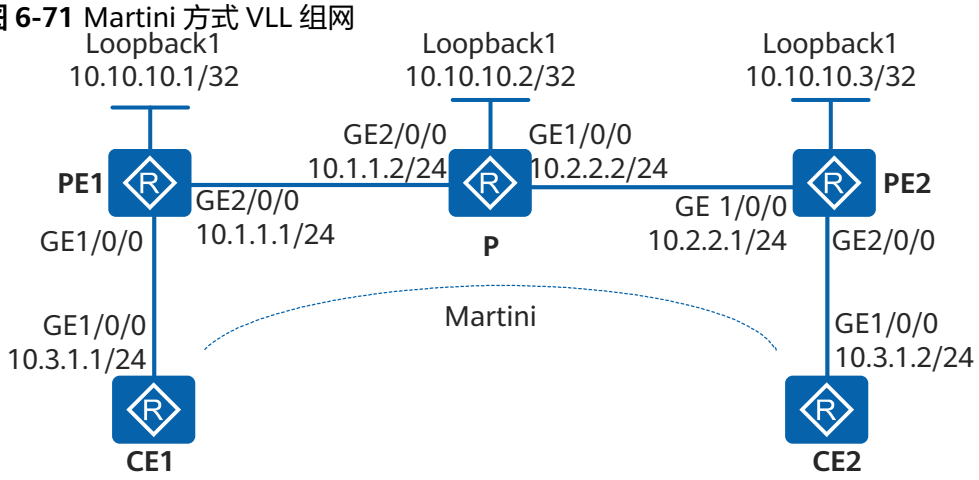
RU-5G-101不支持此功能。

组网需求

如图6-71所示，运营商MPLS网络为用户提供L2VPN服务，其中PE1和PE2作为用户接入设备，接入的用户数量较多且经常变化。现要求一种适当的VPN方案，为用户提供安全的VPN服务，在接入新用户时配置简单。

CE1和CE2之间建议采用建立Martini方式的VLL方式进行连接。

图 6-71 Martini 方式 VLL 组网



操作步骤

步骤1 配置CE1

```
#
 sysname CE1
#
interface GigabitEthernet1/0/0
 ip address 10.3.1.1 255.255.255.0
#
return
```

步骤2 配置PE1

```
#
 sysname PE1
#
mpls lsr-id 10.10.10.1  //配置MPLS LSR ID
mpls  //使能全局MPLS
#
mpls l2vpn  //使能MPLS L2VPN功能
```


版权所有 © 华为技术有限公司

```
#
mpls ldp  //使能全局MPLS LDP
#
mpls ldp remote-peer 10.10.10.3  //配置远端LDP会话
 remote-ip 10.10.10.3
#
interface GigabitEthernet1/0/0  //创建Martini方式的VLL连接
 mpls l2vc 10.10.10.3 101
#
interface GigabitEthernet2/0/0  //接口使能MPLS LDP
 ip address 10.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface LoopBack1
 ip address 10.10.10.1 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 10.10.10.1 0.0.0.0
#
return
```

步骤3 配置P

```
#
 sysname P
#
mpls lsr-id 10.10.10.2  //配置MPLS LSR ID
mpls  //使能全局MPLS
#
mpls ldp  //使能全局MPLS LDP
#
interface GigabitEthernet2/0/0  //接口使能MPLS LDP
 ip address 10.1.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet1/0/0
 ip address 10.2.2.2 255.255.255.0
 mpls
 mpls ldp
#
interface LoopBack1
 ip address 10.10.10.2 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 10.2.2.0 0.0.0.255
  network 10.10.10.2 0.0.0.0
#
return
```

步骤4 配置PE2

```
#
 sysname PE2
#
mpls lsr-id 10.10.10.3  //配置MPLS LSR ID
mpls  //使能全局MPLS
#
mpls l2vpn  //使能MPLS L2VPN功能
#
mpls ldp  //使能全局MPLS LDP
#
mpls ldp remote-peer 10.10.10.1  //配置远端LDP会话
 remote-ip 10.10.10.1
#
interface GigabitEthernet1/0/0  //接口使能MPLS LDP
```

 版权所有 © 华为技术有限公司

```
 ip address 10.2.2.1 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet2/0/0  //创建Martini方式的VLL连接
 mpls l2vc 10.10.10.1 101
#
interface LoopBack1
 ip address 10.10.10.3 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 10.2.2.0 0.0.0.255
  network 10.10.10.3 0.0.0.0
#
return
```

步骤5 配置CE2

```
#
 sysname CE2
#
interface GigabitEthernet1/0/0
 ip address 10.3.1.2 255.255.255.0
#
return
```

步骤6 验证配置结果

在PE上执行命令**display mpls l2vc brief**查看L2VPN连接信息，可以看到建立了一条LDP VC，状态为UP。

CE1和CE2能够相互Ping通。

----结束

6.6.2 配置设备之间部署 VLL 采用 GRE 隧道实现互通的示例

规格

AR300系列不支持此功能。

AR611E-S、AR611、AR631I-LTE4CN、AR631I-LTE4EA、AR611-LTE4EA、AR611-S、AR611W-S、AR611W、AR611W-LTE4CN、AR611W-LTE6EA、AR617VW、AR617VW-LTE4EA、AR617VW-LTE4、AR651C和AR651F-Lite不支持此功能。

RU-5G-101不支持此功能。

组网需求

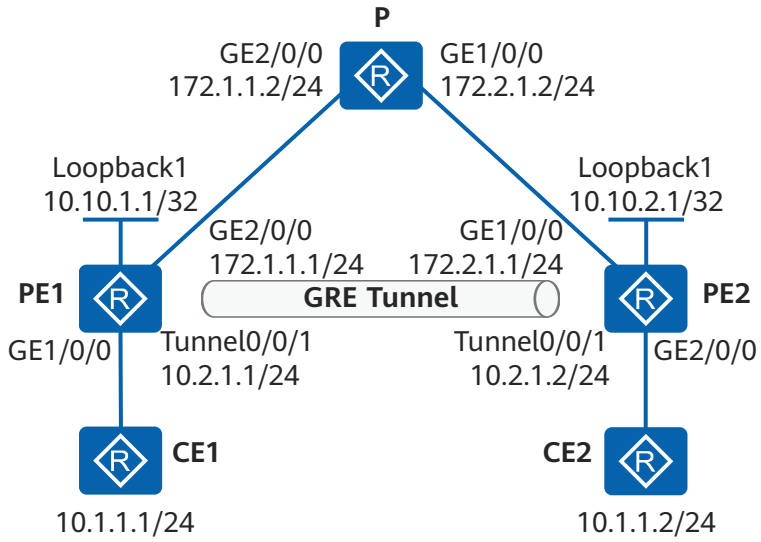
运营商网络为用户提供L2VPN服务，其中PE1和PE2作为用户接入设备，接入的用户数量较多且经常变化。现要求一种适当的VPN方案，为用户提供安全的VPN服务，在接入新用户时配置简单。

CE1和CE2之间建议采用建立Martini方式的VLL方式进行连接。在缺省情况下，系统为Martini方式的VLL选择的隧道类型为LSP，且不进行隧道的负载分担。在P节点设备不支持MPLS功能时，无法实现VLL功能。

为了解决上述问题，可以对Martini方式的VLL应用隧道策略，保证VLL业务承载在GRE隧道上。

 版权所有 © 华为技术有限公司

图 6-72 VLL 采用 GRE 隧道组网



操作步骤

步骤1 配置CE1

```
#
 sysname CE1
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.1 255.255.255.0
#
return
```

步骤2 配置PE1

```
#
 sysname PE1
#
mpls lsr-id 10.10.1.1  //配置MPLS LSR ID
mpls  //使能全局MPLS
#
mpls l2vpn  //使能MPLS L2VPN功能
#
mpls ldp  //使能全局MPLS LDP
#
mpls ldp remote-peer 10.10.2.1  //配置远端LDP会话
 remote-ip 10.10.2.1
#
interface GigabitEthernet1/0/0
 mpls l2vc 10.10.2.1 39 tunnel-policy gre1  //创建Martini方式的VLL连接并指定隧道策略名
#
interface GigabitEthernet2/0/0
 ip address 172.1.1.1 255.255.255.0
#
interface LoopBack1
 ip address 10.10.1.1 255.255.255.255
#
interface Tunnel0/0/1  //配置GRE Tunnel接口
 ip address 10.2.1.1 255.255.255.0
 tunnel-protocol gre
 source 10.10.1.1
 destination 10.10.2.1
#
```


版权所有 © 华为技术有限公司

```
ospf 1
 area 0.0.0.0
  network 10.10.1.1 0.0.0.0
  network 172.1.1.0 0.0.0.255
#
tunnel-policy gre1  //配置隧道策略
 tunnel select-seq gre load-balance-number 1
#
return
```

步骤3 配置P

```
#
 sysname P
#
interface GigabitEthernet2/0/0
 ip address 172.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/0
 ip address 172.2.1.2 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 172.1.1.0 0.0.0.255
  network 172.2.1.0 0.0.0.255
#
return
```

步骤4 配置PE2

```
#
 sysname PE2
#
mpls lsr-id 10.10.2.1  //配置MPLS LSR ID
mpls  //使能全局MPLS
#
mpls l2vpn  //使能MPLS L2VPN功能
#
mpls ldp  //使能全局MPLS LDP
#
mpls ldp remote-peer 10.10.1.1  //配置远端LDP会话
 remote-ip 10.10.1.1
#
interface GigabitEthernet1/0/0
 ip address 172.2.1.1 255.255.255.0
#
interface GigabitEthernet2/0/0  //创建Martini方式的VLL连接并指定隧道策略名
 mpls l2vc 10.10.1.1 39 tunnel-policy gre1
#
interface LoopBack1
 ip address 10.10.2.1 255.255.255.255
#
interface Tunnel0/0/1  //配置GRE Tunnel接口
 ip address 10.2.1.2 255.255.255.0
 tunnel-protocol gre
 source 10.10.2.1
 destination 10.10.1.1
#
ospf 1
 area 0.0.0.0
  network 10.10.2.1 0.0.0.0
  network 172.2.1.0 0.0.0.255
#
tunnel-policy gre1  //配置隧道策略
 tunnel select-seq gre load-balance-number 1
#
return
```

步骤5 配置CE2

```
#
 sysname CE2
```

 版权所有 © 华为技术有限公司

```
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.2 255.255.255.0
#
return
```

步骤6 验证配置结果

在PE上执行命令**display mpls l2vc brief**查看L2VPN连接信息，可以看到建立了一条VC，状态为UP。

CE1和CE2能够相互Ping通。

----结束

6.7 PWE3

6.7.1 配置空中交通管制场景中使用 E&M 接口传输甚高频业务（骨干网使用双链路保护）

规格

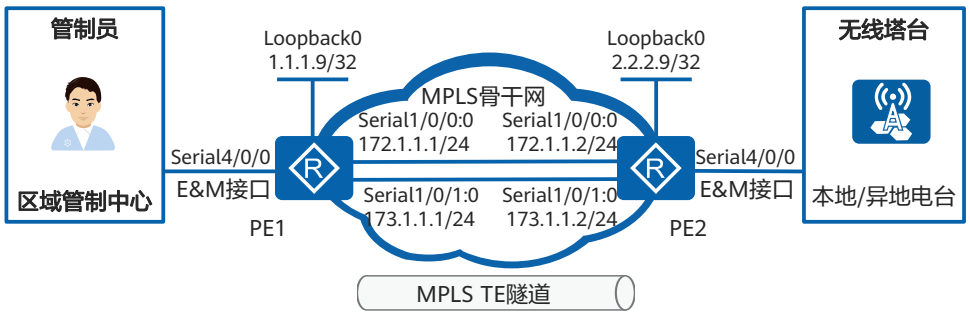
AR300系列和AR600系列不支持。

组网需求

如图6-73所示，在空中交通管制场景中，区域管制中心和电台通过骨干网相连。骨干网设备PE1使用E&M接口与区域管制中心的内话系统相连，PE2使用E&M接口与电台相连。客户希望区域管制中心和电台之间的甚高频业务正常传输，实现地面和空中通话。

另外，由于区域管制中心和电台之间的通信非常重要，不允许出现通信中断的情况，所以客户迫切希望保障其通信的稳定和可靠，使用了两条E1链路。

图 6-73 配置空中交通管制场景中使用 E&M 接口传输甚高频业务组网图



需求分析

- 区域管制中心和电台之间的甚高频业务需要通过E&M接口进行传输，在穿越骨干网的时候，需要使用PWE3技术建立业务数据传输隧道。

 版权所有 © 华为技术有限公司

- 客户为了保障通信的稳定和可靠，使用了两条E1链路接入骨干网。而目前的隧道技术中，MPLS TE隧道的可靠性和主备切换性能最为优异，而且还可与BFD检测一起使用，提供更快的路径故障感知和主备CR-LSP切换功能。使用MPLS TE技术建立主备CR-LSP，分别使用其中一条E1链路（显式路径技术），主链路故障之后，业务数据流量转发路径立刻切换到热备份CR-LSP上，不会造成流量丢失和时延。

说明

PWE3功能使用License授权，缺省情况下设备的PWE3功能受限无法使用。如果需要使用PWE3功能，请联系华为办事处申请并购买相应的License。

操作步骤

步骤1 配置PE1

```
#
 sysname PE1
#
bfd
#
mpls lsr-id 1.1.1.9
mpls
 mpls te
 mpls rsvp-te
 mpls te cspf           //使能CSPF功能，建立MPLS TE隧道
#
mpls l2vpn
#
explicit-path backup    //使用显式路径指定备份CR-LSP使用的链路
 next hop 173.1.1.2
 next hop 2.2.2.9
#
explicit-path main      //使用显式路径指定主CR-LSP使用的链路
 next hop 172.1.1.2
 next hop 2.2.2.9
#
pw-template pe2pe       //使用PW模板建立PWE3
 peer-address 2.2.2.9   //指定远端PW的地址
 jitter-buffer depth 8  //设置Jitter Buffer深度。取值越大，抗抖动能力越大，但在数据流重建的时候会引入较大的传输延时，过大或过小的Jitter Buffer都不利于业务的高质量传输
 tdm-encapsulation-number 8 //根据需要选择每个PW包所封装的TDM帧数，配置较少的打包帧数可以获得较小的网络时延，但是会有更多的封装开销；而配置较多的打包帧数可以获得更高的带宽利用率，但是会引入更大的打包时延
#
mpls ldp
#
mpls ldp remote-peer 2.2.2.9 //指定远端对等体
 remote-ip 2.2.2.9
#
controller E1 1/0/0
 using e1
 clock master               //为保证能够准确无误的进行数据交换，需要配置接口工作在主时钟模式
#
controller E1 1/0/1
 using e1
 clock master
#
interface Serial1/0/0:0
 link-protocol ppp
 ip address 172.1.1.1 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
 mpls ldp
#
interface Serial1/0/1:0
```

 版权所有 © 华为技术有限公司

```
 link-protocol ppp
 ip address 173.1.1.1 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
 mpls ldp
#
interface Serial4/0/0   //配置AC接口，创建传输甚高频业务的隧道
 link-protocol tdm
 mpls l2vc pw-template pe2pe 300 tunnel-policy te
 em passthrough enable  //使能数据透传功能，以便E&M数据可以通过MPLS隧道传输
#
interface LoopBack0
 ip address 1.1.1.9 255.255.255.255
#
interface Tunnel0/0/0   //创建MPLS TE隧道
 ip address unnumbered interface LoopBack0
 tunnel-protocol mpls te
 destination 2.2.2.9
 mpls te tunnel-id 100
 mpls te record-route
 mpls te path explicit-path main   //配置主CR-LSP使用的显示路径
 mpls te path explicit-path backup secondary   //配置备CR-LSP使用的显示路径
 mpls te backup hot-standby mode revertive wtr 15
 mpls te backup ordinary best-effort
 mpls te commit
#
ospf 1 router-id 1.1.1.9   //发布路由信息，以便建立MPLS TE隧道
 opaque-capability enable
 area 0.0.0.0
  network 1.1.1.9 0.0.0.0
  network 172.1.1.0 0.0.0.255
  network 173.1.1.0 0.0.0.255
  mpls-te enable
#
tunnel-policy te        //配置隧道策略，以便PWE3使用MPLS TE和LDP LSP隧道
 tunnel select-seq cr-lsp lsp load-balance-number 1
#
bfd a bind mpls-te interface Tunnel0/0/0 te-lsp   //配置BFD检测，以便业务数据更快速的在主备CR-LSP之间进
行切换
 discriminator local 10
 discriminator remote 10
 min-tx-interval 10
 min-rx-interval 10
 process-pst
 notify neighbor-down
 commit
#
return
```

步骤2 配置PE2

```
#
 sysname PE2
#
bfd
#
mpls lsr-id 2.2.2.9
mpls
 mpls te
 mpls rsvp-te
 mpls te cspf
#
mpls l2vpn
#
explicit-path backup
 next hop 173.1.1.1
 next hop 1.1.1.9
#
explicit-path main
```

 版权所有 © 华为技术有限公司

```
 next hop 172.1.1.1
 next hop 1.1.1.9
#
pw-template pe2pe
 peer-address 1.1.1.9
 jitter-buffer depth 8
 tdm-encapsulation-number 8
#
mpls ldp
#
#
mpls ldp remote-peer 1.1.1.9
 remote-ip 1.1.1.9
#
controller E1 1/0/0
 using e1
#
controller E1 1/0/1
 using e1
#
interface Serial1/0/0:0
 link-protocol ppp
 ip address 172.1.1.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
 mpls ldp
#
interface Serial1/0/1:0
 link-protocol ppp
 ip address 173.1.1.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
 mpls ldp
#
interface Serial4/0/0
 link-protocol tdm
 mpls l2vc pw-template pe2pe 300 tunnel-policy te
 em passthrough enable
#
interface LoopBack0
 ip address 2.2.2.9 255.255.255.255
#
interface Tunnel0/0/0
 ip address unnumbered interface LoopBack0
 tunnel-protocol mpls te
 destination 1.1.1.9
 mpls te tunnel-id 100
 mpls te record-route
 mpls te path explicit-path main
 mpls te path explicit-path backup secondary
 mpls te backup hot-standby mode revertive wtr 15
 mpls te backup ordinary best-effort
 mpls te commit
#
ospf 1 router-id 2.2.2.9
 opaque-capability enable
 area 0.0.0.0
  network 2.2.2.9 0.0.0.0
  network 172.1.1.0 0.0.0.255
  network 173.1.1.0 0.0.0.255
  mpls-te enable
#
tunnel-policy te
 tunnel select-seq cr-lsp lsp load-balance-number 1
#
bfd a bind mpls-te interface Tunnel0/0/0 te-lsp
 discriminator local 10
```

 版权所有 © 华为技术有限公司

```
 discriminator remote 10
 min-tx-interval 10
 min-rx-interval 10
 process-pst
 notify neighbor-down
 commit
#
return
```

步骤3 验证配置结果

#配置完成后，检查PE设备之间的MPLS TE隧道建立成功，VC状态为Up。以PE1为例：

```
[PE1] display mpls te tunnel-interface tunnel 0/0/0
  ------------------------------------------------------------------------------
                          Tunnel0/0/0
  ------------------------------------------------------------------------------
  Tunnel State Desc   :  UP
  Active LSP          :  Primary LSP
  Session ID          :  100
  Ingress LSR ID      :  1.1.1.9          Egress LSR ID:  2.2.2.9
  Admin State         :  UP               Oper State    :  UP
  Primary LSP State      : UP
    Main LSP State       : READY              LSP ID  : 10
  Hot-Standby LSP State  : UP
    Main LSP State       : READY              LSP ID  : 32773
[PE1] display mpls l2vc interface serial 4/0/0
 *client interface       : Serial4/0/0 is up
  Administrator PW       : no
  session state          : up
  AC status              : up
  Ignore AC state        : disable
  VC state               : up
  Label state            : 0
  Token state            : 0
  VC ID                  : 300
  VC type                : CESoPSN basic mode
  destination            : 2.2.2.9
......
```

区域管制中心播放音乐，电台放音正常且清晰。切断E1主链路，链路快速切换到备份链路，无感知音乐中断，无卡音；恢复E1主链路，链路快速切换到主链路，无感知音乐中断，无卡音。

----结束

 版权所有 © 华为技术有限公司

7 部署 5G

7.1 5G拨号上网场景
7.2 5G2B专线场景
7.3 5G冗余保护场景

7.1 5G 拨号上网场景

7.1.1 配置企业通过 5G 链路接入 Internet 示例

场景介绍

5G Cellular接口是路由器用来实现5G技术的物理接口，它为用户提供了企业级的无线广域网接入服务，主要用于eMBB场景。与LTE相比，5G系统可以为企业用户提供更大带宽的无线广域接入服务。

路由器的5G功能，可以实现企业分支机构或中小企业的无线宽带接入及互联的需求。5G功能不仅为企业提供了灵活、高效、快速部署网络的解决方案，也为企业提供了一种有线广域链路的备份方法。与LTE相比，5G具备更大带宽的无线广域接入能力，可以为企业用户提供更为丰富的3D高清视频、云桌面和智慧办公等业务。

组网需求

如**图1**所示，企业分支和总部之间通过Internet网络互通。企业分支使用AR企业路由器作为出口网关，AR企业路由器通过5G链路接入Internet，与企业总部建立连接。该企业分支办理了包年业务，采用自动拨号方式接入Internet。

图 7-1 配置企业通过 5G 链路接入 Internet 组网图

版权所有 © 华为技术有限公司

数据准备

表 7-1 数据准备表

项目	数据	说明
运营商分配给企业分支的APN名称	5gnet	APN名称需提前从运营商处获取。
运营商分配给分支的5G Cellular接口的IP地址	1.1.1.1/32	5G Cellular接口拨号接入运营商后，运营商给5G Cellular接口自动分配的IP地址。
分支AR1 LAN侧接口信息	所属VLAN：20 网关地址：VLANIF20（10.1.1.1/24） LAN侧物理接口：GE0/0/1	VLAN 20为分支子网用户所在的VLAN，且分支子网用户的网关为VLANIF20接口。
NQA探测的目的地址	公网DNS服务器地址：114.114.114.114	NQA测试例的测试类型必须为ICMP测试，且到NQA测试例的目的地址必须路由可达。本例中选择公网的DNS服务器地址为探测目的地址，也可以选择其他路由可达的公网地址。 114.114.114.114是国内通用的DNS地址，国内用户使用较多，本例中用该地址来测试5G链路的连通性。8.8.8.8是全球通用的DNS地址，如果是国外用户，可以用8.8.8.8地址来测试5G链路的连通性。

配置思路

1. 配置5G Cellular接口的连接参数及NQA测试例，实现5G Cellular接口接入5G网络。
2. 配置企业子网，为内部用户自动分配IP地址。
3. 配置NAT功能，实现分支的内网用户可以访问Internet。
4. 配置缺省路由，指定出接口为5G Cellular接口，使该企业分支内网的流量通过5G Cellular接口上行传输到Internet。

   说明

   在5G Cellular接口下执行命令**dialer enable-circular**配置轮询拨号功能时，设备会同时下发自动拨号、IP地址协商和5G Modem自愈的相关配置，无需再重复配置。

操作步骤

1. 配置5G Cellular接口的连接参数及NQA测试例，实现5G Cellular接口接入5G网络。

 版权所有 © 华为技术有限公司

a. 创建APN模板。

```
<Huawei> system-view
[Huawei] sysname AR1
[AR1] apn profile 5gprofile
[AR1-apn-profile-5gprofile] apn 5gnet
[AR1-apn-profile-5gprofile] quit
```

b. 使能轮询DCC功能，配置自动拨号连接。

```
[AR1] interface Cellular 1/0/0
[AR1-Cellular1/0/0] dialer enable-circular
```

c. 配置NQA功能，探测5G链路的连通性。

```
[AR1] nqa test-instance user test
[AR1-nqa-user-test] test-type icmp
[AR1-nqa-user-test] frequency 30
[AR1-nqa-user-test] destination-address ipv4 114.114.114.114
[AR1-nqa-user-test] start now
[AR1-nqa-user-test] quit
```

d. 在5G Cellular接口上绑定APN模板及NQA测试例。

```
[AR1-Cellular1/0/0] apn-profile 5gprofile
Info: The configuration will become effective after link reset.
[AR1-Cellular1/0/0] modem auto-recovery track nqa user test probe-cycle seconds 30
[AR1-Cellular1/0/0] modem auto-recovery track action modem-reboot fail-times 10
[AR1-Cellular1/0/0] shutdown
[AR1-Cellular1/0/0] undo shutdown
[AR1-Cellular1/0/0] quit
```

2. 配置企业子网，为内部用户自动分配IP地址。

   # 配置分支子网，创建VLAN20，将GE0/0/1接口加入VLAN20，并配置DHCP功能。

```
[AR1] vlan 20
[AR1-vlan20] quit
[AR1] interface GigabitEthernet 0/0/1
[AR1-GigabitEthernet0/0/1] port link-type trunk
[AR1-GigabitEthernet0/0/1] port trunk allow-pass vlan 20
[AR1-GigabitEthernet0/0/1] quit
[AR1] dhcp enable
[AR1] interface vlanif 20
[AR1-Vlanif20] ip address 10.1.1.1 24
[AR1-Vlanif20] dhcp select interface
[AR1-Vlanif20] quit
```

3. 配置分支的NAT功能。

```
[AR1] acl number 3000
[AR1-acl-adv-3000] rule 5 permit ip
[AR1-acl-adv-3000] quit
[AR1] interface cellular 1/0/0
[AR1-Cellular1/0/0] nat outbound 3000
[AR1-Cellular1/0/0] quit
```

4. 配置静态路由，使企业分支和总部的内网流量可以上行传输到Internet。

   # 配置分支的缺省路由，指定出接口为5G Cellular接口。

```
[AR1] ip route-static 0.0.0.0 0.0.0.0 cellular 1/0/0
```

验证

1. 在AR1上执行命令**display ip interface brief Cellular 1/0/0**查看5G Cellular接口的详细信息，当接口上有流量传送时，可以看到接口获取到的IP地址，接口的物理状态和链路层协议状态都是Up。

```
<AR1> display ip interface brief Cellular 1/0/0
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
(E): E-Trunk down
Interface                   IP Address/Mask      Physical   Protocol
```

 版权所有 © 华为技术有限公司

```
Cellular1/0/0                1.1.1.1/32      up       up
```

2. 在AR1上执行命令**display cellular 1/0/0 all**查看5G数据卡的呼叫连接信息，可以看到APN为5gnet、无线网络类型为Automatic以及网络连接方式为5G(NSA)。

```
<AR1> display Cellular 1/0/0 all
Modem State:
Hardware Information.
=====================
Model = RG801
Modem Type = 5G module
Modem Firmware Version = RG801HEAAAR01A07M8G
Hardware Version = HiB5000_MODEM Ver.A
Integrate circuit card identity (ICCID) = 98681020100202000069
International Mobile Subscriber Identity (IMSI) = 460070075591996
Mobile Station International ISDN Number (MSISDN) = None
International Mobile Equipment Identity (IMEI) = 867147050004457
Factory Serial Number (FSN) = 0123456789ABCDEF
Modem Status = Online
Profile Information.
====================
Profile 1
--------
PDP Type = IPv4, Header Compression = OFF
Data Compression = OFF
Access Point Name (APN) = 5gnet
Packet Session Status = Active
* - Default profile
Network Information.
====================
Current Service Status = Service available
Service Domain = Combined
Current Service = PS
Packet Service = Attached
Packet Session Status = Active
Current Roaming Status = Roaming
Network Selection Mode = Automatic
Network Connection Mode = LTE-NR
Current Network Connection = 5G(NSA)
Mobile Country Code (MCC) = 369
Mobile Network Code (MNC) = 77
Mobile Operator Information = Unknown
Tracking Area Code (TAC) = 1002
Cell ID = 9881858
Radio Information.
==================
Current Bands :
  WCDMA: AUTO
  LTE: B3
  NR: AUTO
LTE:
Current Band = B3
Current RSSI >= -51 dBm
Current RSRP = -71 dBm (strong)
Current RSRQ = -6 dB
Current SINR = 6 dB
NR:
Current Band = N78
Current RSRP = -65 dBm (strong)
Current RSRQ = -10 dB
Current SINR = 38 dB
Bands supported :
  WCDMA: WCDMA850 WCDMA900 WCDMA2100
  FDD LTE: B1 B3 B5 B7 B8 B20 B28
  TDD LTE: B34 B38 B39 B40 B41
  FDD NR: N1 N3 N28
  TDD NR: N41 N77 N78 N79
Modem Security Information.
===========================
SIM ID = 1
```

 版权所有 © 华为技术有限公司

```
PIN Verification = Disabled
PIN Status = Ready
Number of Retries remaining = 3
SIM Status = OK
```

配置脚本

AR1配置文件

```
#
 sysname AR1
#
vlan batch 20
#
dhcp enable
#
acl number 3000
 rule 5 permit ip
#
interface Vlanif20
 ip address 10.1.1.1 255.255.255.0
 dhcp select interface
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 20
#
interface Cellular1/0/0
 dialer enable-circular
 apn-profile 5gprofile
 dialer timer autodial 10
 nat outbound 3000
 modem auto-recovery dial action modem-reboot fail-times 128
 modem auto-recovery track action modem-reboot fail-times 10
 modem auto-recovery icmp-unreachable action modem-reboot
 modem auto-recovery services-unavailable action modem-reboot test-times 0 interval 3600
 modem auto-recovery track nqa user test probe-cycle seconds 30
 ip address negotiate
#
apn profile 5gprofile
 apn 5gnet
#
ip route-static 0.0.0.0 0.0.0.0 Cellular1/0/0
#
nqa test-instance user test
 test-type icmp
 destination-address ipv4 114.114.114.114
 frequency 30
 start now
#
return
```

7.1.2 配置企业通过 5G IPv6 链路接入 Internet 示例

场景介绍

5G Cellular接口是路由器用来实现5G技术的物理接口，它为用户提供了企业级的无线广域网接入服务，主要用于eMBB场景。IPv6可以为海量机器类通信提供足够的IP地址，相比于IPv4，IPv6协议新增的扩展报文头、端到端分片等功能，有助于提升网络的可靠性、降低网络时延。IPv6推进了5G网络的发展，相反，5G的部署也将激发基于IPv6的技术创新。

路由器的5G功能，可以实现企业分支机构或中小企业的无线宽带接入及互联的需求。5G功能不仅为企业提供了灵活、高效、快速部署网络的解决方案，也为企业提供了一种有线广域链路的备份方法。与LTE相比，5G具备更大带宽的无线广域接入能力，可以为企业用户提供更为丰富的3D高清视频、云桌面和智慧办公等业务。

 版权所有 © 华为技术有限公司

组网需求

如图1所示，企业分支和总部之间通过Internet网络互通。企业分支使用AR企业路由器作为出口网关，AR企业路由器通过5G IPv6链路接入Internet，与企业总部建立连接。该企业分支办理了包年业务，采用自动拨号方式接入Internet。

图 7-2 配置企业通过 5G IPv6 链路接入 Internet 组网图

数据准备

表 7-2 数据准备表

项目	数据	说明
运营商分配给企业分支的APN名称	5gnet	APN名称需提前从运营商处获取。
运营商分配给分支的5G Cellular接口的IPv6地址	2408:843E:C00:8E4:2E0:FC20:19:2020/64	5G Cellular接口拨号接入运营商后，运营商给5G Cellular接口自动分配的IPv6地址。
分支AR1 LAN侧接口信息	所属VLAN：20 网关地址：VLANIF20（280d::1/64） LAN侧物理接口：GE0/0/1	VLAN 20为分支子网用户所在的VLAN，且分支子网用户的网关为VLANIF20接口。 **说明** AR不支持IPv6 NAT, 为了使回程报文能够在网络侧被正确转发，LAN侧网段必须由运营商提供。运营商设备通过配置Frame-Route可以为无线用户指定LAN侧网段。
NQA探测的目的地址	公网DNS服务器地址：240c::6666	NQA测试例的测试类型必须为ICMP测试，且到NQA测试例的目的地址必须路由可达。本例中选择公网的DNS服务器地址为探测目的地址，也可以选择其他路由可达的公网地址。 240c::6666是国内通用的DNS地址，国内用户使用较多，本例中用该地址来测试5G链路的连通性。 2001:4860:4860::8888是全球通用的DNS地址，如果是国外用户，可以用2001:4860:4860::8888地址来测试5G链路的连通性。

版权所有 © 华为技术有限公司

配置思路

1. 配置5G Cellular接口的连接参数及NQA测试例，实现5G Cellular接口接入5G网络。
2. 配置企业子网，为内部用户自动分配IP地址。
3. 配置NAT功能，实现分支的内网用户可以访问Internet。
4. 配置缺省路由，指定出接口为5G Cellular接口，使该企业分支内网的流量通过5G Cellular接口上行传输到Internet。

说明

在5G Cellular接口下执行命令**dialer enable-circular**配置轮询拨号功能时，设备会默认下发IPv4地址协商功能，如果不需要获取IPv4地址，可以执行undo ip address negotiate命令删除IPv4地址协商功能。

操作步骤

1. 配置5G Cellular接口的连接参数及NQA测试例，实现5G Cellular接口接入5G网络。

   a. 创建APN模板。

   ```
   <Huawei> system-view
   [Huawei] sysname AR1
   [AR1] apn profile 5gprofile
   [AR1-apn-profile-5gprofile] apn 5gnet
   [AR1-apn-profile-5gprofile] quit
   ```

   b. 使能IPv6功能。

   ```
   [AR1] ipv6
   [AR1] interface Cellular 2/0/0
   [AR1-Cellular2/0/0] ipv6 enable
   [AR1-Cellular2/0/0] ipv6 address auto link-local
   [AR1-Cellular2/0/0] ipv6 address auto global
   ```

   c. 使能轮询DCC功能，配置自动拨号连接。

   ```
   [AR1] interface Cellular 2/0/0
   [AR1-Cellular2/0/0] dialer enable-circular
   [AR1-Cellular2/0/0] undo ip address negotiate
   [AR1-Cellular2/0/0] quit
   ```

   d. 配置NQA功能，探测5G链路的连通性。

   ```
   [AR1] nqa test-instance user test
   [AR1-nqa-user-test] test-type icmp
   [AR1-nqa-user-test] frequency 30
   [AR1-nqa-user-test] destination-address ipv6 240c::6666
   [AR1-nqa-user-test] start now
   [AR1-nqa-user-test] quit
   ```

   e. 在5G Cellular接口上绑定APN模板及NQA测试例。

   ```
   [AR1-Cellular2/0/0] apn-profile 5gprofile
   Info: The configuration will become effective after link reset.
   [AR1-Cellular2/0/0] modem auto-recovery track nqa user test probe-cycle seconds 30
   [AR1-Cellular2/0/0] modem auto-recovery track action modem-reboot fail-times 10
   [AR1-Cellular2/0/0] shutdown
   [AR1-Cellular2/0/0] undo shutdown
   [AR1-Cellular2/0/0] quit
   ```

2. 配置企业子网，为内部用户自动分配IPv6地址。

   # 配置分支子网，创建VLAN20，将GE0/0/1接口加入VLAN20。

   ```
   [AR1] vlan 20
   [AR1-vlan20] quit
   [AR1] interface GigabitEthernet 0/0/1
   [AR1-GigabitEthernet0/0/1] port link-type trunk
   [AR1-GigabitEthernet0/0/1] port trunk allow-pass vlan 20
   ```

 版权所有 © 华为技术有限公司

```
[AR1-GigabitEthernet0/0/1] quit
[AR1] interface vlanif 20
[AR1-Vlanif20] ipv6 enable
[AR1-Vlanif20] ipv6 address 280D::1/64
[AR1-Vlanif20] undo ipv6 nd ra halt
[AR1-Vlanif20] quit
```

3. 配置静态路由，使企业分支和总部的内网流量可以上行传输到Internet。

   # 配置分支的缺省路由，指定出接口为5G Cellular接口。

```
[AR1] ip route-static :: 0 cellular 2/0/0
```

验证

1. 在AR1上执行命令**display ipv6 interface brief**查看5G Cellular接口的详细信息，当接口上有流量传送时，可以看到接口获取到的IP地址，接口的物理状态和链路层协议状态都是Up。

```
<AR1> display ipv6 interface brief
*down: administratively down
(l): loopback
(s): spoofing
Interface                  Physical            Protocol
Cellular2/0/0                up                up
[IPv6 Address] 2408:843E:C00:8E4:2E0:FC20:19:2020
```

2. 在AR1上执行命令**display cellular 2/0/0 all**查看5G数据卡的呼叫连接信息，可以看到APN为5gnet、无线网络类型为Automatic以及网络连接方式为5G(SA)。

```
<AR1> display Cellular 2/0/0 all
Modem State:
Hardware Information.
======================
Model = RG801
Modem Type = 5G module
Modem Firmware Version = RG801HEAAAR03A03M8G
Hardware Version = HiB5000_MODEM Ver.A
Integrate circuit card identity (ICCID) = 89860120801472630356
International Mobile Subscriber Identity (IMSI) = 460012285508496
Mobile Station International ISDN Number (MSISDN) = None
International Mobile Equipment Identity (IMEI) = 867147050005231
Factory Serial Number (FSN) = 0123456789ABCDEF
Modem Status = Online
Profile Information.
====================
Profile 1
--------
PDP Type = IPv6, Header Compression = OFF
Data Compression = OFF
Access Point Name (APN) = 5gnet
Packet Session Status = Active
* - Default profile
Network Information.
====================
Current Service Status = Service available
Service Domain = Combined
Current Service = PS
Packet Service = Attached
Packet Session Status = Active
Current Roaming Status = Home
Network Selection Mode = Automatic
Network Connection Mode = Automatic
Current Network Connection = 5G(SA)
Mobile Country Code (MCC) = 460
Mobile Network Code (MNC) = 01
Mobile Operator Information = CHN-UNICOM
Tracking Area Code (TAC) = 13608193
Cell ID = 55740145665
Radio Information.
```

 版权所有 © 华为技术有限公司

```
==================
Current Bands : AUTO
Current Band = N78
Current RSRP = -84 dBm (strong)
Current RSRQ = -10 dB
Current SINR = 18 dB
Bands supported :
  WCDMA: WCDMA850 WCDMA900 WCDMA2100
  FDD LTE: B1 B3 B5 B7 B8 B20 B28
  TDD LTE: B34 B38 B39 B40 B41
  FDD NR: N1 N3 N28
  TDD NR: N41 N77 N78 N79
Modem Security Information.
==========================
SIM ID = 1
PIN Verification = Disabled
PIN Status = Ready
Number of Retries remaining = 3
SIM Status = OK
```

配置脚本

AR1配置文件

```
#
 sysname AR1
#
ipv6
#
vlan batch 20
#
interface Vlanif20
 ipv6 enable
 ipv6 address 280D::1/64
 undo ipv6 nd ra halt
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 20
#
interface Cellular2/0/0
 ipv6 enable
 dialer enable-circular
 apn-profile 5gprofile
 dialer timer autodial 10
 ipv6 address auto link-local
 ipv6 address auto global
 modem auto-recovery track nqa user test probe-cycle seconds 30
 modem auto-recovery track action modem-reboot fail-times 10
 modem auto-recovery dial action modem-reboot fail-times 128
 modem auto-recovery icmp-unreachable action modem-reboot
 modem auto-recovery services-unavailable action modem-reboot test-times 0 interval 3600
#
apn profile 5gprofile
 apn 5gnet
#
ipv6 route-static :: 0 Cellular2/0/0
#
nqa test-instance user test
 test-type icmp
 destination-address ipv6 240C::6666
 frequency 30
 start now
#
return
```

 版权所有 © 华为技术有限公司

7.1.3 配置企业通过 5G 双 DNN 同时接入 Internet 和 IMS 示例

场景介绍

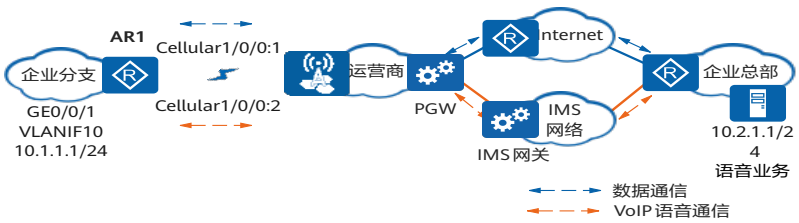
在5G网络中，DNN（Data Network Name）等同于4G网络中的APN（Access Point Name）， 标识一个外部数据网络。用户可以在AR上配置DNN接入到相应的数据网络。AR1支持多DNN技术，每个DNN都可以会获取到独立的IP地址，不同DNN接入到不同的数据网络，例如DNN1接入Internet网络进行数据通信，DNN2接入到IMS数据网络进行VoIP语音通信。

由于AR2的5G功能同时兼容LTE和3G，虽然外部数据网络的概念在5G网络里叫做DNN，但配置还是沿用原来LTE和3G里的APN，所以举例里还是写配置APN。

组网需求

如图1所示，为了接入不同的网络，AR1的一个Cellular接口包含多个Cellular通道接口，每个Cellular通道接口等同于一个逻辑的业务接口，可以获取独立IP地址、并独立配置所要应用的业务，如语音、数据等。每个APN绑定一个Cellular通道接口，多个APN共用一个Cellular接口。路由器通过APN1接入Internet进行数据通信；通过APN2接入IMS网络进行VoIP语音通信。企业使用5G多APN进行数据通信和VoIP语音通信。

图 7-3 配置企业通过 5G 双 DNN 同时接入 Internet 和 IMS 组网图



数据准备

表 7-3 数据准备表

项目	数据	说明
运营商分配给企业分支的APN名称	5gnet、voicenet	APN名称需提前从运营商处获取。
运营商分配给分支的5G Cellular通道接口的IP地址	Cellular1/0/0:1接口：1.1.1.1/32 Cellular1/0/0:2接口：2.2.2.2/32	5G Cellular通道接口拨号接入运营商后，运营商给5G Cellular通道接口自动分配的IP地址。本例中，假设运营商为两个5G Cellular通道接口分配的IP地址分别为1.1.1.1和2.2.2.2。

版权所有 © 华为技术有限公司

项目	数据	说明
分支AR1 LAN侧接口信息	所属VLAN：10 网关地址：VLANIF10（10.1.1.1/24） LAN侧物理接口：GE0/0/1	VLAN 10为分支子网用户所在的VLAN，且分支子网用户的网关为VLANIF10接口。
总部语音业务所在的子网网段	10.2.1.0/24	总部语音业务所在的子网网段用于配置路由信息，使语言业务和数据业务走不同的路由。

配置思路

1. 创建两个APN模板，一个APN模板接入Internet，另一个APN模板接入IMS网络。
2. 在5G Cellular接口上使能多APN功能，并配置5G下行流量异常时发送ICMP报文检测DNS服务器是否可达。
3. 在5G Cellular通道接口上配置轮询DCC拨号连接，并绑定APN模板。
4. 配置分支内网，由AR1为该企业分支内网用户分配IP地址。
5. 配置NAT功能，指定5G Cellular通道接口的IP地址作为该企业分支公网地址。
6. 配置静态路由，指定出接口为5G Cellular通道接口，使数据业务和语音业务可以通过不同的5G Cellular通道接口上行传输到5G网络。

说明

在5G Cellular接口下执行命令**dialer enable-circular**配置轮询拨号功能时，设备会同时下发自动拨号、IP地址协商和5G Modem自愈的相关配置，无需再重复配置。

操作步骤

1. 配置APN模板

   # 配置APN模板5gnet，该模板用来接入Internet。

   ```
   <Huawei> system-view
   [Huawei] sysname AR1
   [AR1] apn profile 5gnet
   [AR1-apn-profile-5gnet] apn 5gnet
   [AR1-apn-profile-5gnet] quit
   ```

   # 配置APN模板voicenet，该模板用来接入IMS网络。

   ```
   [AR1] apn profile voicenet
   [AR1-apn-profile-voicenet] apn voicenet
   [AR1-apn-profile-voicenet] quit
   ```

2. 在5G Cellular接口上使能多APN功能。

   ```
   [AR1] interface cellular 1/0/0
   [AR1-Cellular1/0/0] multi-apn enable
   [AR1-Cellular1/0/0] quit
   ```

3. 在5G Cellular通道接口上配置轮询DCC拨号连接，绑定APN模板。

   # 在5G Cellular通道接口1上配置轮询DCC拨号连接，绑定APN模板5gnet。

   ```
   [AR1] interface cellular 1/0/0:1
   [AR1-Cellular1/0/0:1] dialer enable-circular
   [AR1-Cellular1/0/0:1] apn-profile 5gnet
   ```

 版权所有 © 华为技术有限公司

```
[AR1-Cellular1/0/0:1] shutdown
[AR1-Cellular1/0/0:1] undo shutdown
[AR1-Cellular1/0/0:1] quit
```

在5G Cellular通道接口2上配置轮询DCC拨号连接，绑定APN模板voicenet。

```
[AR1] interface cellular 1/0/0:2
[AR1-Cellular1/0/0:2] dialer enable-circular
[AR1-Cellular1/0/0:2] apn-profile voicenet
[AR1-Cellular1/0/0:2] shutdown
[AR1-Cellular1/0/0:2] undo shutdown
[AR1-Cellular1/0/0:2] quit
```

4. 配置分支内网，为该企业分支内网用户分配IP地址。

   # 创建VLAN10，将GE0/0/1接口加入VLAN10。

   ```
   [AR1] vlan 10
   [AR1-vlan10] quit
   [AR1] interface GigabitEthernet 0/0/1
   [AR1-GigabitEthernet0/0/1] port link-type access
   [AR1-GigabitEthernet0/0/1] port default vlan 10
   [AR1-GigabitEthernet0/0/1] quit
   ```

   # 使能DHCP功能，并配置接口工作在接口地址池模式。

   ```
   [AR1] dhcp enable
   [AR1] interface Vlanif 10
   [AR1-Vlanif10] ip address 10.1.1.1 255.255.255.0
   [AR1-Vlanif10] dhcp select interface
   [AR1-Vlanif10] quit
   ```

5. 配置NAT功能。

   ```
   [AR1] acl number 3000
   [AR1-acl-adv-3000] rule 5 permit ip
   [AR1-acl-adv-3000] quit
   [AR1] interface cellular 1/0/0:1
   [AR1-Cellular1/0/0:1] nat outbound 3000
   [AR1-Cellular1/0/0:1] quit
   [AR1] interface cellular 1/0/0:2
   [AR1-Cellular1/0/0:2] nat outbound 3000
   [AR1-Cellular1/0/0:2] quit
   ```

6. 配置静态路由，数据业务走缺省路由，出接口为Cellular1/0/0:1；语音业务走另一条静态路由，出接口为Cellular1/0/0:2。

   ```
   [AR1] ip route-static 0.0.0.0 0.0.0.0 Cellular 1/0/0:1
   [AR1] ip route-static 10.2.1.0 255.255.255.0 Cellular 1/0/0:2
   [AR1] quit
   ```

验证

1. 在AR1上执行命令**display ip interface brief Cellular 1/0/0:1**，查看Cellular1/0/0:1接口获取到的IP地址。

   ```
   <AR1> display ip interface brief Cellular 1/0/0:1
   *down: administratively down
   ^down: standby
   (l): loopback
   (s): spoofing
   (E): E-Trunk down
   Interface                   IP Address/Mask      Physical   Protocol

   Cellular1/0/0:1               1.1.1.1/32         up         up
   ```

2. 在AR1上执行命令**display cellular 1/0/0 all**，查看Cellular1/0/0接口的状态信息。

   ```
   <AR1> display Cellular 1/0/0 all
   Modem State:
   Hardware Information.
   =====================
   Model = RG801
   Modem Type = 5G module
   ```

 版权所有 © 华为技术有限公司

```
Modem Firmware Version = RG801HEAAAR01A07M8G
Hardware Version = HiB5000_MODEM Ver.A
Integrate circuit card identity (ICCID) = 98610201001020200069
International Mobile Subscriber Identity (IMSI) = 460070075591996
Mobile Station International ISDN Number (MSISDN) = None
International Mobile Equipment Identity (IMEI) = 867147050004457
Factory Serial Number (FSN) = 0123456789ABCDEF
Modem Status = Online
Profile Information.
====================
Profile 1
--------
PDP Type = IPv4, Header Compression = OFF
Data Compression = OFF
Access Point Name (APN) = 5gnet
Packet Session Status = Active
* - Default profile
Network Information.
====================
Current Service Status = Service available
Service Domain = Combined
Current Service = PS
Packet Service = Attached
Packet Session Status = Active
Current Roaming Status = Roaming
Network Selection Mode = Automatic
Network Connection Mode = LTE-NR
Current Network Connection = 5G(NSA)
Mobile Country Code (MCC) = 369
Mobile Network Code (MNC) = 77
Mobile Operator Information = Unknown
Tracking Area Code (TAC) = 1002
Cell ID = 9881858
Radio Information.
==================
Current Bands :
  WCDMA: AUTO
  LTE: B3
  NR: AUTO
LTE:
Current Band = B3
Current RSSI >= -51 dBm
Current RSRP = -71 dBm (strong)
Current RSRQ = -6 dB
Current SINR = 6 dB
NR:
Current Band = N78
Current RSRP = -65 dBm (strong)
Current RSRQ = -10 dB
Current SINR = 38 dB
Bands supported :
  WCDMA: WCDMA850 WCDMA900 WCDMA2100
  FDD LTE: B1 B3 B5 B7 B8 B20 B28
  TDD LTE: B34 B38 B39 B40 B41
  FDD NR: N1 N3 N28
  TDD NR: N41 N77 N78 N79
Modem Security Information.
===========================
SIM ID = 1
PIN Verification = Disabled
PIN Status = Ready
Number of Retries remaining = 3
SIM Status = OK
```

配置文件

AR1配置文件

```
#
 sysname AR1
```

 版权所有 © 华为技术有限公司

```
#
vlan batch 10
#
dhcp enable
#
acl number 3000
 rule 5 permit ip
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
 dhcp select interface
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 10
#
interface Cellular1/0/0
 multi-apn enable
 modem auto-recovery icmp-unreachable action modem-reboot
#
interface Cellular1/0/0:1
 dialer enable-circular
 apn-profile 5gnet
 dialer timer autodial 10
 nat outbound 3000
 modem auto-recovery dial action modem-reboot fail-times 128
 modem auto-recovery services-unavailable action modem-reboot test-times 0 interval 3600
 ip address negotiate
#
interface Cellular1/0/0:2
 dialer enable-circular
 apn-profile voicenet
 dialer timer autodial 10
 nat outbound 3000
 modem auto-recovery dial action modem-reboot fail-times 128
 modem auto-recovery services-unavailable action modem-reboot test-times 0 interval 3600
 ip address negotiate
#
apn profile 5gnet
 apn 5gnet
apn profile voicenet
 apn voicenet
#
ip route-static 0.0.0.0 0.0.0.0 Cellular1/0/0:1
ip route-static 10.2.1.0 255.255.255.0 Cellular1/0/0:2
#
return
```

7.2 5G2B 专线场景

7.2.1 配置分支使用 5G 链路和总部建立 GRE 隧道互联示例

场景介绍

VPN是一种解决企业分支和总部之间通过公有网络实现私有数据通信的技术。VPN在企业分支和总部之间，跨公有网络建立一个私有的、专用的虚拟通信隧道，实现分支和总部之间跨公网的私有通信。VPN由于安全、可靠、可信赖、灵活、价格便宜等众多优势，在企业网络中得到广泛应用。VPN加上5G链路的大带宽、低时延、易部署等优点，更能满足远程用户、企业分支和企业总部之间快速、安全、高效的互联需求。

企业分支通过5G链路接入到Internet，然后与企业总部建立VPN，使得分支可以通过Internet接入总部。根据企业分支和总部之间的业务诉求，可以在5G链路上建立不同的VPN隧道。例如GRE是一种三层隧道封装技术，当企业分支和总部之间需要交互三

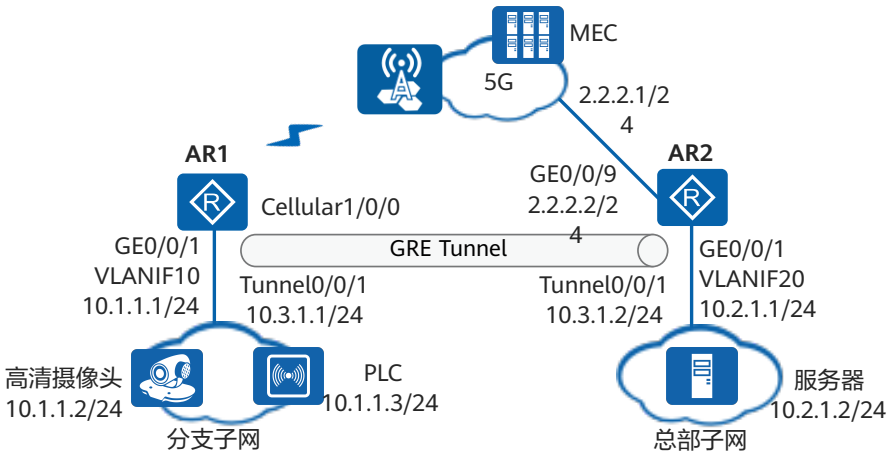
 版权所有 © 华为技术有限公司

层业务时，可以在总部和分支之间建立GRE隧道，转发分支和总部之间的L3业务流量，满足企业分支用户快速、安全、高效接入总部的需求。

组网需求

如图1所示，企业分支和总部之间通过Internet网络互通。企业分支使用AR1企业路由器作为出口网关，AR1企业路由器通过5G链路接入Internet。企业分支和总部之间在5G链路上构建GRE隧道，转发它们之间的三层流量。

图 7-4 配置分支使用 5G 链路和总部建立 GRE 隧道互联组网图



数据准备

表 7-4 数据准备表

项目	数据	说明
运营商给分支分配的APN名称	5gnet	APN名称需提前从运营商处获取。
运营商给分支5G Cellular接口分配的IP地址	1.1.1.1/32	5G Cellular接口拨号接入运营商后，运营商给5G Cellular接口自动分配的IP地址。 **说明** 使用GRE隧道时，要求运营商给5G Cellular接口分配的IP地址为固定IP地址。本例中，假设运营商为5G Cellular接口分配的固定IP地址为1.1.1.1。
运营商给总部GE0/0/9接口分配的IP地址	2.2.2.2/24	总部AR2通过有线的方式接入Internet，该有线接口GE0/0/9采用静态方式配置IP地址。

 版权所有 © 华为技术有限公司

项目	数据	说明
运营商对接总部GE0/0/9接口的IP地址	2.2.2.1/24	运营商对接总部AR2 GE0/0/9接口的IP地址用于配置路由信息，使总部和Internet之间的路由互通。
分支AR1 LAN侧接口信息	所属VLAN：10 网关地址：VLANIF10（10.1.1.1/24） LAN侧物理接口：GE0/0/1	VLAN 10为分支子网用户所在的VLAN，且分支子网用户的网关为VLANIF10接口。
总部AR2 LAN侧接口信息	所属VLAN：20 网关地址：VLANIF20（10.2.1.1/24） LAN侧物理接口：GE0/0/1	VLAN 20为总部子网用户所在的VLAN，且总部子网用户的网关为VLANIF20接口。
分支AR1 Tunnel接口的IP地址	10.3.1.1/24	分支GRE隧道的地址。
总部AR2 Tunnel接口的IP地址	10.3.1.2/24	总部GRE隧道的地址。

TCP MSS 参数配置说明

为了减少网络传输中不必要的分片和重组，网络规划时需要合理设置终端发出的报文大小。对于TCP报文，可以配置5G AR设备的TCP MSS值，通过修改应用层报文数据包的长度来避免报文分片。在5G 2B专线场景中，TCP MSS取值比较简单，在隧道两端AR设备的LAN侧接入物理口或VLANIF口上配置TCP MSS为推荐值1200。

配置思路

1. 配置5G Cellular接口的连接参数，实现5G Cellular接口接入5G网络。
2. 配置企业子网，为内部用户自动分配IP地址。
3. 配置Tunnel接口，创建GRE隧道，使分支和总部之间的业务流量通过GRE隧道传输。
4. 配置静态路由，使企业分支和总部子网的用户可以互通。

说明

在5G Cellular接口下执行命令**dialer enable-circular**配置轮询拨号功能时，设备会同时下发自动拨号、IP地址协商和5G Modem自愈的相关配置，无需再重复配置。

操作步骤

1. 配置5G Cellular接口的连接参数，实现5G Cellular接口接入5G网络。
   a. 创建APN模板。

```
<Huawei> system-view
[Huawei] sysname AR1
```

```
[AR1] apn profile 5gprofile
[AR1-apn-profile-5gprofile] apn 5gnet
[AR1-apn-profile-5gprofile] quit
```

b. 使能轮询DCC功能，配置自动拨号连接。

```
[AR1] interface Cellular 1/0/0
[AR1-Cellular1/0/0] dialer enable-circular
```

c. 在5G Cellular接口上绑定APN模板。

```
[AR1-Cellular1/0/0] apn-profile 5gprofile
Info: The configuration will become effective after link reset.
[AR1-Cellular1/0/0] shutdown
[AR1-Cellular1/0/0] undo shutdown
[AR1-Cellular1/0/0] quit
```

2. 配置企业子网，为内部用户自动分配IP地址。

a. 配置分支子网，创建VLAN10，将GE0/0/1接口加入VLAN10。配置VLANIF 10接口TCP最大报文段长度为1200字节并配置DHCP功能。

```
[AR1] vlan 10
[AR1-vlan10] quit
[AR1] interface GigabitEthernet 0/0/1
[AR1-GigabitEthernet0/0/1] port link-type access
[AR1-GigabitEthernet0/0/1] port default vlan 10
[AR1-GigabitEthernet0/0/1] quit
[AR1] dhcp enable
[AR1] interface Vlanif 10
[AR1-Vlanif10] ip address 10.1.1.1 24
[AR1-Vlanif10] dhcp select interface
[AR1-Vlanif10] tcp adjust-mss 1200
[AR1-Vlanif10] quit
```

b. 配置总部子网，创建VLAN20，将GE0/0/1接口加入VLAN20。配置VLANIF 20接口TCP最大报文段长度为1200字节并配置DHCP功能。

```
<Huawei> system-view
[Huawei] sysname AR2
[AR2] vlan 20
[AR2-vlan20] quit
[AR2] interface GigabitEthernet 0/0/1
[AR2-GigabitEthernet0/0/1] port link-type access
[AR2-GigabitEthernet0/0/1] port default vlan 20
[AR2-GigabitEthernet0/0/1] quit
[AR2] dhcp enable
[AR2] interface Vlanif 20
[AR2-Vlanif20] ip address 10.2.1.1 24
[AR2-Vlanif20] dhcp select interface
[AR2-Vlanif20] tcp adjust-mss 1200
[AR2-Vlanif20] quit
```

3. 配置Tunnel接口，创建GRE隧道。

a. 配置总部WAN侧接口GE0/0/9的IP地址。

```
[AR2] interface GigabitEthernet 0/0/9
[AR2-GigabitEthernet0/0/9] ip address 2.2.2.2 24
[AR2-GigabitEthernet0/0/9] quit
```

b. 配置总部的Tunnel接口。

```
[AR2] interface Tunnel0/0/1
[AR2-Tunnel0/0/1] tunnel-protocol gre
Warning: After this tunnel encapsulation protocol was configured, the MTU and other
parameter settings of the tunnel were deleted.
[AR2-Tunnel0/0/1] ip address 10.3.1.2 255.255.255.0
[AR2-Tunnel0/0/1] source GigabitEthernet 0/0/9
[AR2-Tunnel0/0/1] destination 1.1.1.1
[AR2-Tunnel0/0/1] quit
```

c. 配置分支的Tunnel接口。

```
[AR1] interface Tunnel0/0/1
[AR1-Tunnel0/0/1] tunnel-protocol gre
Warning: After this tunnel encapsulation protocol was configured, the MTU and other
parameter settings of the tunnel were deleted.
```

 版权所有 © 华为技术有限公司

```
[AR1-Tunnel0/0/1] ip address 10.3.1.1 255.255.255.0
[AR1-Tunnel0/0/1] source Cellular 1/0/0
[AR1-Tunnel0/0/1] destination 2.2.2.2
[AR1-Tunnel0/0/1] quit
```

4. 配置静态路由，使企业分支和总部子网的用户可以互通。

   a. 配置两条分支静态路由，一条静态路由的出接口为5G Cellular1/0/0，一条静态路由的出接口为Tunnel0/0/1。

   ```
   [AR1] ip route-static 2.2.2.2 32 Cellular 1/0/0
   [AR1] ip route-static 10.2.1.0 255.255.255.0 Tunnel 0/0/1
   [AR1] quit
   ```

   b. 配置两条总部静态路由，一条静态路由的下一跳地址为对端运营商接口的IP地址，一条静态路由的出接口为Tunnel0/0/1。

   ```
   [AR2] ip route-static 1.1.1.0 255.255.255.0 2.2.2.1
   [AR2] ip route-static 10.1.1.0 255.255.255.0 Tunnel 0/0/1
   [AR2] quit
   ```

验证

1. 在AR1上执行命令**display ip interface brief Cellular 1/0/0**，查看Cellular1/0/0接口获取到的IP地址。

   ```
   <AR1> display ip interface brief Cellular 1/0/0
   *down: administratively down
   ^down: standby
   (l): loopback
   (s): spoofing
   (E): E-Trunk down
   Interface                   IP Address/Mask      Physical   Protocol

   Cellular1/0/0               1.1.1.1/32           up         up
   ```

2. 在AR1上执行命令**display Cellular 1/0/0 all**，查看Cellular1/0/0接口的状态信息。

   ```
   <AR1> display Cellular 1/0/0 all
   Modem State:
   Hardware Information.
   =====================
   Model = RG801
   Modem Type = 5G module
   Modem Firmware Version = RG801HEAAAR01A07M8G
   Hardware Version = HiB5000_MODEM Ver.A
   Integrate circuit card identity (ICCID) = 98681020100202000069
   International Mobile Subscriber Identity (IMSI) = 460070075591996
   Mobile Station International ISDN Number (MSISDN) = None
   International Mobile Equipment Identity (IMEI) = 867147050004457
   Factory Serial Number (FSN) = 0123456789ABCDEF
   Modem Status = Online
   Profile Information.
   ====================
   Profile 1
   --------
   PDP Type = IPv4, Header Compression = OFF
   Data Compression = OFF
   Access Point Name (APN) = 5gnet
   Packet Session Status = Active
   * - Default profile
   Network Information.
   ====================
   Current Service Status = Service available
   Service Domain = Combined
   Current Service = PS
   Packet Service = Attached
   Packet Session Status = Active
   Current Roaming Status = Roaming
   Network Selection Mode = Automatic
   Network Connection Mode = LTE-NR
   ```

 版权所有 © 华为技术有限公司

```
Current Network Connection = 5G(NSA)
Mobile Country Code (MCC) = 369
Mobile Network Code (MNC) = 77
Mobile Operator Information = Unknown
Tracking Area Code (TAC) = 1002
Cell ID = 9881858
Radio Information.
==================
Current Bands :
  WCDMA: AUTO
  LTE: B3
  NR: AUTO
LTE:
Current Band = B3
Current RSSI >= -51 dBm
Current RSRP = -71 dBm (strong)
Current RSRQ = -6 dB
Current SINR = 6 dB
NR:
Current Band = N78
Current RSRP = -65 dBm (strong)
Current RSRQ = -10 dB
Current SINR = 38 dB
Bands supported :
  WCDMA: WCDMA850 WCDMA900 WCDMA2100
  FDD LTE: B1 B3 B5 B7 B8 B20 B28
  TDD LTE: B34 B38 B39 B40 B41
  FDD NR: N1 N3 N28
  TDD NR: N41 N77 N78 N79
Modem Security Information.
===========================
SIM ID = 1
PIN Verification = Disabled
PIN Status = Ready
Number of Retries remaining = 3
SIM Status = OK
```

3. 在AR1上执行命令**ping -a 10.1.1.1 10.2.1.1**，模拟分支用户访问总部用户的流量，流量能Ping通。

```
<AR1> ping -a 10.1.1.1 10.2.1.1
  PING 10.2.1.1: 56  data bytes, press CTRL_C to break
    Reply from 10.2.1.1: bytes=56 Sequence=1 ttl=255 time=51 ms
    Reply from 10.2.1.1: bytes=56 Sequence=2 ttl=255 time=35 ms
    Reply from 10.2.1.1: bytes=56 Sequence=3 ttl=255 time=45 ms
    Reply from 10.2.1.1: bytes=56 Sequence=4 ttl=255 time=40 ms
    Reply from 10.2.1.1: bytes=56 Sequence=5 ttl=255 time=37 ms

  --- 10.2.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 35/41/51 ms
```

配置文件

AR1配置文件

```
#
 sysname AR1
#
vlan batch 10
#
dhcp enable
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
 dhcp select interface
 tcp adjust-mss 1200
#
interface GigabitEthernet0/0/1
```

 版权所有 © 华为技术有限公司

```
 port link-type access
 port default vlan 10
#
interface Cellular1/0/0
 dialer enable-circular
 apn-profile 5gprofile
 dialer timer autodial 10
 modem auto-recovery dial action modem-reboot fail-times 128
 modem auto-recovery icmp-unreachable action modem-reboot
 modem auto-recovery services-unavailable action modem-reboot test-times 0 interval 3600
 ip address negotiate
#
interface Tunnel0/0/1
 ip address 10.3.1.1 255.255.255.0
 tunnel-protocol gre
 source Cellular1/0/0
 destination 2.2.2.2
#
apn profile 5gprofile
 apn 5gnet
#
ip route-static 2.2.2.2 255.255.255.255 Cellular1/0/0
ip route-static 10.2.1.0 255.255.255.0 Tunnel0/0/1
#
return
```

AR2配置文件

```
#
 sysname AR2
#
vlan batch 20
#
dhcp enable
#
interface Vlanif20
 ip address 10.2.1.1 255.255.255.0
 dhcp select interface
 tcp adjust-mss 1200
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 20
#
interface GigabitEthernet0/0/9
 ip address 2.2.2.2 255.255.255.0
#
interface Tunnel0/0/1
 ip address 10.3.1.2 255.255.255.0
 tunnel-protocol gre
 source GigabitEthernet0/0/9
 destination 1.1.1.1
#
ip route-static 1.1.1.0 255.255.255.0 2.2.2.1
ip route-static 10.1.1.0 255.255.255.0 Tunnel0/0/1
#
return
```

7.2.2 配置分支使用 5G 链路和总部建立 IPSec 加密隧道示例

场景介绍

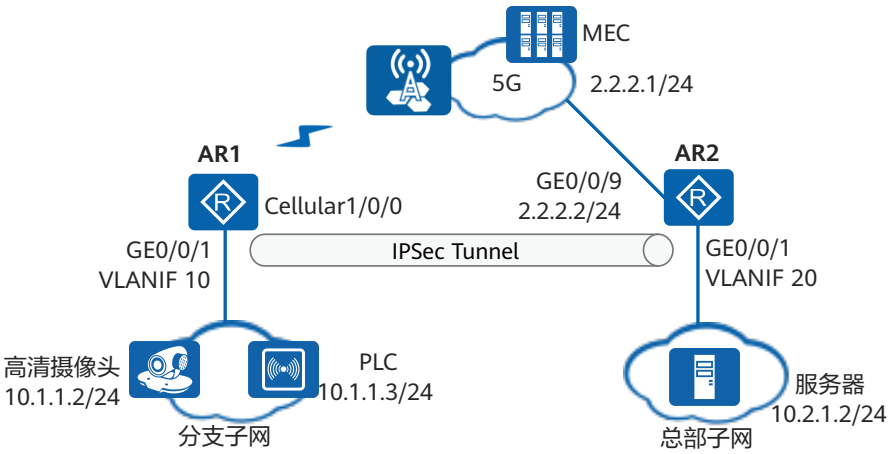
企业分支通过5G链路接入到Internet，然后与企业总部建立VPN，使得分支可以通过Internet接入总部。根据企业分支和总部之间的业务诉求，可以在5G链路上建立不同的VPN隧道，例如GRE、L2TP、IPSec VPN、DSVPN。其中，IPSec VPN隧道可以对链路上传输的数据进行加密，防止数据被拦截或篡改，非常适用于那些业务安全性和保密性要求较高的行业，例如金融的离行ATM、政府机构等。

 版权所有 © 华为技术有限公司

组网需求

如图1所示，企业分支使用AR1企业路由器作为出口网关，AR2企业路由器通过5G链路接入Internet，企业分支和总部在5G链路上通过配置IPSec实现企业分支与总部的业务安全互通，对互相访问的流量进行安全保护。

图 7-5 配置分支使用 5G 链路和总部建立 IPSec 加密隧道组网图



数据准备

表 7-5 数据准备表

项目	数据	说明
运营商分配给企业分支的APN名称	5gnet	APN名称需提前从运营商处获取。
运营商分配给分支的5G Cellular接口的IP地址	1.1.1.1/32	5G Cellular接口拨号接入运营商后，运营商给5G Cellular接口自动分配的IP地址。
运营商分配给总部的GE0/0/9接口的IP地址	2.2.2.2/24	总部AR2通过有线的方式接入Internet，该有线接口GE0/0/9采用静态方式获取IP地址。
分支AR1 LAN侧接口信息	VLAN：10 VLANIF10：10.1.1.1	VLAN 10为分支子网用户所在的VLAN，且分支子网用户的网关为VLANIF10接口。
总部AR2 LAN侧接口信息	VLAN：20 VLANIF20：10.2.1.1	VLAN 20为总部子网用户所在的VLAN，且总部子网用户的网关为VLANIF20接口。

版权所有 © 华为技术有限公司

项目	数据	说明
总部AR2对端运营商接口的IP地址	2.2.2.1/24	总部AR2对端运营商接口的IP地址用于配置路由信息，使分支和总部之间的路由互通。

TCP MSS 参数配置说明

为了减少网络传输中不必要的分片和重组，网络规划时需要合理设置终端发出的报文大小。对于TCP报文，可以配置5G AR设备的TCP MSS值，通过修改应用层报文数据包的长度来避免报文分片。在5G 2B专线场景中，TCP MSS取值比较简单，在隧道两端AR设备的LAN侧接入物理口或VLANIF口上配置TCP MSS为推荐值1200。

配置思路

1. 配置5G Cellular接口的连接参数，实现5G Cellular接口接入5G网络。
2. 配置企业子网，为内部用户自动分配IP地址。
3. 配置分支NAT功能，实现分支的内部用户可以访问Internet。
4. 配置ACL，以定义IPSec保护的数据流。
5. 配置IPSec安全提议，定义IPSec的保护方法。
6. 配置IKE对等体，定义对等体间IKE协商时的属性。
7. 配置安全策略，确定对何种数据流采取何种保护方法。其中总部AR采用策略模板方式创建安全策略。
8. 在接口上应用安全策略组，使接口具有IPSec的保护功能。
9. 配置静态路由，使企业分支和总部的内网流量可以上行传输到Internet.

说明

自动拨号和按需拨号只需配置一种即可，即如果执行命令**dialer enable-circular**配置自动拨号，设备会自动配置拨号串和IP地址协商，则无需再配置拨号控制列表进行按需拨号。

操作步骤

1. 配置5G Cellular接口的连接参数，实现5G Cellular接口接入5G网络。
   a. 创建APN模板。
   ```
   <Huawei> system-view
   [Huawei] sysname AR1
   [AR1] apn profile 5gprofile
   [AR1-apn-profile-5gprofile] apn 5gnet
   [AR1-apn-profile-5gprofile] quit
   ```
   b. 使能轮询DCC功能，配置自动拨号连接。
   ```
   [AR1] interface Cellular 1/0/0
   [AR1-Cellular1/0/0] dialer enable-circular
   ```
   c. 在5G Cellular接口上绑定APN模板。
   ```
   [AR1-Cellular1/0/0] apn-profile 5gprofile
   Info: The configuration will become effective after link reset.
   [AR1-Cellular1/0/0] shutdown
   [AR1-Cellular1/0/0] undo shutdown
   [AR1-Cellular1/0/0] quit
   ```
2. 配置企业子网，为内部用户自动分配IP地址。

 版权所有 © 华为技术有限公司

a. 配置分支子网，创建VLAN10，将GE0/0/1接口加入VLAN10。配置VLANIF 10接口TCP最大报文段长度为1200字节并配置DHCP功能。

```
[AR1] vlan 10
[AR1-vlan10] quit
[AR1] interface GigabitEthernet 0/0/1
[AR1-GigabitEthernet0/0/1] port link-type access
[AR1-GigabitEthernet0/0/1] port default vlan 10
[AR1-GigabitEthernet0/0/1] quit
[AR1] dhcp enable
[AR1] interface Vlanif 10
[AR1-Vlanif10] ip address 10.1.1.1 24
[AR1-Vlanif10] dhcp select interface
[AR1-Vlanif10] tcp adjust-mss 1200
[AR1-Vlanif10] quit
```

b. 配置总部子网，创建VLAN20，将GE0/0/1接口加入VLAN20。配置VLANIF 20接口TCP最大报文段长度为1200字节并配置DHCP功能。

```
<Huawei> system-view
[Huawei] sysname AR2
[AR2] vlan 20
[AR2-vlan20] quit
[AR2] interface GigabitEthernet 0/0/1
[AR2-GigabitEthernet0/0/1] port link-type access
[AR2-GigabitEthernet0/0/1] port default vlan 20
[AR2-GigabitEthernet0/0/1] quit
[AR2] dhcp enable
[AR2] interface Vlanif 20
[AR2-Vlanif20] ip address 10.2.1.1 24
[AR2-Vlanif20] dhcp select interface
[AR2-Vlanif20] tcp adjust-mss 1200
[AR2-Vlanif20] quit
```

3. 配置分支NAT功能

```
[AR1] acl number 3000
[AR1-acl-adv-3000] rule 5 deny ip destination 10.2.1.0 0.0.0.255
[AR1-acl-adv-3000] rule 10 permit ip
[AR1-acl-adv-3000] quit
[AR1] interface Cellular 1/0/0
[AR1-Cellular1/0/0] nat outbound 3000
[AR1-Cellular1/0/0] quit
```

4. 配置总部接口IP地址。

```
[AR2] interface gigabitethernet 0/0/9
[AR2-GigabitEthernet0/0/9] ip address 2.2.2.2 255.255.255.0
[AR2-GigabitEthernet0/0/9] quit
```

5. 配置ACL，定义各自要保护的数据流。

配置分支ACL，定义由子网10.1.1.0/24去子网10.2.1.0/24的数据流。

```
[AR1] acl number 3101
[AR1-acl-adv-3101] rule permit ip destination 10.2.1.0 0.0.0.255
[AR1-acl-adv-3101] quit
```

配置总部ACL，定义由子网10.2.1.0/24去子网10.1.1.0/24的数据流。

```
[AR2] acl number 3101
[AR2-acl-adv-3101] rule permit ip source 10.2.1.0 0.0.0.255
[AR2-acl-adv-3101] quit
```

6. 配置IPSec安全提议。

配置分支IPSec安全提议。

```
[AR1] ipsec proposal tran1
[AR1-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
[AR1-ipsec-proposal-tran1] esp encryption-algorithm aes-128
[AR1-ipsec-proposal-tran1] quit
```

配置总部IPSec安全提议。

```
[AR2] ipsec proposal tran1
[AR2-ipsec-proposal-tran1] esp authentication-algorithm sha2-256
[AR2-ipsec-proposal-tran1] esp encryption-algorithm aes-128
[AR2-ipsec-proposal-tran1] quit
```

 版权所有 © 华为技术有限公司

7. 配置IKE对等体。
   a. 配置分支IKE安全提议。
   ```
   [AR1] ike proposal 5
   [AR1-ike-proposal-5] authentication-algorithm sha2-256
   [AR1-ike-proposal-5] encryption-algorithm aes-128
   [AR1-ike-proposal-5] dh group14
   [AR1-ike-proposal-5] quit
   ```
   b. 配置分支IKE对等体。
   ```
   [AR1] ike peer spub
   [AR1-ike-peer-spub] ike-proposal 5
   [AR1-ike-peer-spub] pre-shared-key cipher YsHsjx_202206
   [AR1-ike-peer-spub] remote-address 2.2.2.2
   [AR1-ike-peer-spub] quit
   ```
   c. 配置总部IKE安全提议。
   ```
   [AR2] ike proposal 5
   [AR2-ike-proposal-5] authentication-algorithm sha2-256
   [AR2-ike-proposal-5] encryption-algorithm aes-128
   [AR2-ike-proposal-5] dh group14
   [AR2-ike-proposal-5] quit
   ```
   d. 配置总部IKE对等体。
   ```
   [AR2] ike peer spua
   [AR2-ike-peer-spua] ike-proposal 5
   [AR2-ike-peer-spua] pre-shared-key cipher YsHsjx_202206
   [AR2-ike-peer-spua] remote-address 1.1.1.1
   [AR2-ike-peer-spua] quit
   ```
8. 配置安全策略。
   a. 配置分支IKE动态协方式安全策略。
   ```
   [AR1] ipsec policy policy1 10 isakmp
   [AR1-ipsec-policy-isakmp-policy1-10] proposal tran1
   [AR1-ipsec-policy-isakmp-policy1-10] ike-peer spub
   [AR1-ipsec-policy-isakmp-policy1-10] security acl 3101
   [AR1-ipsec-policy-isakmp-policy1-10] quit
   ```
   b. 配置总部以策略模板方式配置IKE动态协商方式安全策略。
   ```
   [AR2] ipsec policy policy1 10 isakmp
   [AR2-ipsec-policy-templet-use1-10] proposal tran1
   [AR2-ipsec-policy-templet-use1-10] ike-peer spua
   [AR2-ipsec-policy-templet-use1-10] security acl 3101
   [AR2-ipsec-policy-templet-use1-10] quit
   ```
9. 配置分支和总部在接口上应用各自的安全策略组，使接口具有IPSec的保护功能。
   a. 在分支接口上应用安全策略组。
   ```
   [AR1] interface cellular 1/0/0
   [AR1-Cellular1/0/0] ipsec policy policy1
   [AR1-Cellular1/0/0] quit
   ```
   b. 在总部接口上应用安全策略组。
   ```
   [AR2] interface gigabitethernet 0/0/9
   [AR2-GigabitEthernet0/0/9] ipsec policy policy1
   [AR2-GigabitEthernet0/0/9] quit
   ```
10. 配置静态路由，使企业分支和总部的内网流量可以上行传输到Internet。

    # 配置分支的缺省路由，指定出接口为5G Cellular接口。
    ```
    [AR1] ip route-static 0.0.0.0 0.0.0.0 cellular 1/0/0
    ```
    # 配置总部的路由参数，确保企业总部与企业分支用户网络互通。
    ```
    [AR2] ip route-static 0.0.0.0 0.0.0.0 2.2.2.1
    ```

验证

1. 分别在AR1和AR2上执行**display ike sa**会显示所配置的信息，以AR1为例。
   ```
   [AR1] display ike sa
    Conn-ID  Peer                    VPN            Flag(s)            Phase  RemoteType
   ```

 版权所有 © 华为技术有限公司

```
RemoteID
------------------------------------------------------------------------------------------------------------------------
-------------
 16        2.1.1.1:500                                     RD|ST             v1:2    IP         2.1.1.1
 14        2.1.1.1:500                                     RD|ST             v1:1    IP
2.1.1.1
  Number of IKE SA : 2
------------------------------------------------------------------------------------------------------------------------
-------------

 Flag Description:
 RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--
TIMEOUT
 HRT--HEARTBEAT   LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED
UP
 M--ACTIVE   S--STANDBY   A--ALONE  NEG--NEGOTIATING
```

2. 在AR1上执行命令**display ip interface brief Cellular 1/0/0**，查看Cellular1/0/0接口获取到的IP地址。

```
<AR1> display ip interface brief Cellular 1/0/0
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
(E): E-Trunk down
Interface                   IP Address/Mask      Physical   Protocol

Cellular1/0/0               1.1.1.1/32           up         up
```

3. 在AR1上执行命令**display Cellular 1/0/0 all**，查看Cellular1/0/0接口的状态信息。

```
<AR1> display Cellular 1/0/0 all
Modem State:
Hardware Information.
=====================
Model = RG801
Modem Type = 5G module
Modem Firmware Version = RG801HEAAAR01A07M8G
Hardware Version = HiB5000_MODEM Ver.A
Integrate circuit card identity (ICCID) = 98681020100202000069
International Mobile Subscriber Identity (IMSI) = 460070075591996
Mobile Station International ISDN Number (MSISDN) = None
International Mobile Equipment Identity (IMEI) = 867147050004457
Factory Serial Number (FSN) = 0123456789ABCDEF
Modem Status = Online
Profile Information.
====================
Profile 1
--------
PDP Type = IPv4, Header Compression = OFF
Data Compression = OFF
Access Point Name (APN) = 5gnet
Packet Session Status = Active
* - Default profile
Network Information.
====================
Current Service Status = Service available
Service Domain = Combined
Current Service = PS
Packet Service = Attached
Packet Session Status = Active
Current Roaming Status = Roaming
Network Selection Mode = Automatic
Network Connection Mode = LTE-NR
Current Network Connection = 5G(NSA)
Mobile Country Code (MCC) = 369
Mobile Network Code (MNC) = 77
Mobile Operator Information = Unknown
Tracking Area Code (TAC) = 1002
Cell ID = 9881858
```

 版权所有 © 华为技术有限公司

```
Radio Information.
==================
Current Bands :
  WCDMA: AUTO
  LTE: B3
  NR: AUTO
LTE:
Current Band = B3
Current RSSI >= -51 dBm
Current RSRP = -71 dBm (strong)
Current RSRQ = -6 dB
Current SINR = 6 dB
NR:
Current Band = N78
Current RSRP = -65 dBm (strong)
Current RSRQ = -10 dB
Current SINR = 38 dB
Bands supported :
  WCDMA: WCDMA850 WCDMA900 WCDMA2100
  FDD LTE: B1 B3 B5 B7 B8 B20 B28
  TDD LTE: B34 B38 B39 B40 B41
  FDD NR: N1 N3 N28
  TDD NR: N41 N77 N78 N79
Modem Security Information.
==========================
SIM ID = 1
PIN Verification = Disabled
PIN Status = Ready
Number of Retries remaining = 3
SIM Status = OK
```

4. 在AR1上执行命令**ping -a 10.1.1.1 10.2.1.1**，模拟分支用户访问总部用户的流量，流量能Ping通。

```
<AR1> ping -a 10.1.1.1 10.2.1.1
  PING 10.2.1.1: 56  data bytes, press CTRL_C to break
    Reply from 10.2.1.1: bytes=56 Sequence=1 ttl=255 time=51 ms
    Reply from 10.2.1.1: bytes=56 Sequence=2 ttl=255 time=35 ms
    Reply from 10.2.1.1: bytes=56 Sequence=3 ttl=255 time=45 ms
    Reply from 10.2.1.1: bytes=56 Sequence=4 ttl=255 time=40 ms
    Reply from 10.2.1.1: bytes=56 Sequence=5 ttl=255 time=37 ms

  --- 10.2.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 35/41/51 ms
```

配置脚本

AR1配置文件

```
#
 sysname AR1
#
vlan batch 10
#
dhcp enable
#
acl number 3000
 rule 5 deny ip destination 10.2.1.0 0.0.0.255
rule 10 permit ip
acl number 3101
 rule permit ip destination 10.2.1.0 0.0.0.255
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
 dhcp select interface
 tcp adjust-mss 1200
#
interface GigabitEthernet0/0/1
```

 版权所有 © 华为技术有限公司

```
 port link-type access
 port default vlan 10
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-128
#
ike proposal 5
 encryption-algorithm aes-128
 dh group14
 authentication-algorithm sha2-256
#
ike peer spub
 pre-shared-key cipher %^%#JvZxR2g8c;a9~FPN~n'$7`DEV&=G(=Et02P/%\*!%^%#
 remote-address 2.2.2.2
 ike-proposal 5
#
ipsec policy policy1 10 isakmp
 security acl 3101
 ike-peer spub
 proposal tran1
#
interface Cellular1/0/0
 dialer enable-circular
 apn-profile 5gprofile
 dialer timer autodial 10
 nat outbound 3000
 modem auto-recovery dial action modem-reboot fail-times 128
 modem auto-recovery icmp-unreachable action modem-reboot
 modem auto-recovery services-unavailable action modem-reboot test-times 0 interval 3600
 ip address negotiate
 ipsec policy policy1
#
apn profile 5gprofile
 apn 5gnet
#
ip route-static 0.0.0.0 0.0.0.0 Cellular 1/0/0
#
return
```

AR2配置文件

```
#
 sysname AR2
#
vlan batch 20
#
dhcp enable
#
interface Vlanif20
 ip address 10.2.1.1 255.255.255.0
 dhcp select interface
 tcp adjust-mss 1200
#
acl number 3101
 rule permit ip source 10.2.1.0 0.0.0.255
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 20
#
ipsec proposal tran1
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-128
#
ike proposal 5
 encryption-algorithm aes-128
 dh group14
 authentication-algorithm sha2-256
#
ike peer spua
```

 版权所有 © 华为技术有限公司

```
 pre-shared-key cipher %^%#K{JG:rWVHPMnf;5\|,GW(Luq'qi8BT4nOj%5W5=)%^%#
 remote-address 1.1.1.1
 ike-proposal 5
#
ipsec policy policy1 10 isakmp
 security acl 3101
 ike-peer spua
 proposal tran1
#
interface GigabitEthernet0/0/9
 ip address 2.2.2.2 255.255.255.0
 ipsec policy policy1
#
ip route-static 0.0.0.0 0.0.0.0 2.2.2.1
#
return
```

7.2.3 配置分支使用 5G 链路和总部建立 L2TP 隧道互联示例

场景介绍

随着企业的发展和业务的增加，在不同地域成立的分支机构和出差的员工，需要和总部建立快速、安全和可靠的网络连接。传统的拨号网络需要租用因特网服务提供商ISP（Internet Service Provider）的电话线路，申请公共的号码或IP地址，不仅产生高额的费用，而且无法为远程用户尤其是出差员工提供便利的接入服务。L2TP技术出现以后，使用L2TP隧道承载PPP报文在Internet上传输成为了解决上述问题的一种途径。无论出差员工是通过传统拨号方式接入Internet，还是通过以太网方式接入Internet，L2TP都可以提供远程接入服务。

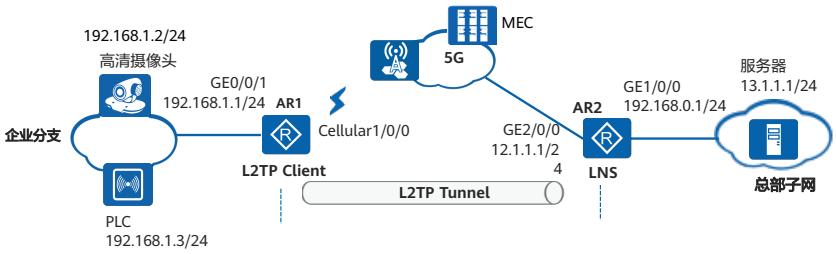
根据企业分支和总部之间的业务诉求，可以在5G链路上建立不同的VPN隧道。L2TP是一种二层隧道协议，企业分支配置拨号LAC，与企业总部LNS设备建立L2TP隧道。企业总部可以对分支设备接入账号密码做安全认证，也可以通过L2TP over IPSec保证数据传输安全。

组网需求

企业总部在其他城市设有分支机构，分支机构部署为以太网络，并配备网关设备通过5G链路接入到Internet。

企业总部的网关部署为LNS，为分支用户提供接入服务，LNS只对L2TP Client进行身份认证，此时可以通过在L2TP Client配置主动拨号的方式，在L2TP Client和LNS之间建立L2TP连接。

图 7-6 配置分支使用 5G 链路和总部建立 L2TP 隧道互联



 版权所有 © 华为技术有限公司

数据准备

表 7-6 数据准备表

项目	数据	说明
运营商分配给企业分支的APN名称	5gnet	APN名称需提前从运营商处获取。
运营商分配给分支的5G Cellular接口的IP地址	1.1.1.1/32	5G Cellular接口拨号接入运营商后，运营商给5G Cellular接口自动分配的IP地址。
运营商对接总部GE2/0/0接口的IP地址	12.1.1.1/24	运营商对接总部AR2 GE2/0/0接口的IP地址用于配置路由信息，使总部和Internet之间的路由互通。

TCP MSS 参数配置说明

为了减少网络传输中不必要的分片和重组，网络规划时需要合理设置终端发出的报文大小。对于TCP报文，可以配置5G AR设备的TCP MSS值，通过修改应用层报文数据包的长度来避免报文分片。在5G 2B专线场景中，TCP MSS取值比较简单，在隧道两端AR设备的LAN侧接入物理口或VLANIF口上配置TCP MSS为推荐值1200。

配置思路

1. 配置5G Cellular接口的连接参数，实现5G Cellular接口接入5G网络。
2. 配置企业子网，为内部用户自动分配IP地址。
3. 配置L2TP功能，PPP用户通过L2TP隧道向总部发出接入请求，总部认证成功后建立隧道。
4. 配置访问公网的路由，路由出接口为5G接口，并使能L2TP Client的主动拨号功能。
5. 在LNS上配置L2TP功能及PPP用户，并配置访问公网的路由。

   说明

   在5G Cellular接口下执行命令**dialer enable-circular**配置轮询拨号功能时，设备会同时下发自动拨号、IP地址协商和5G Modem自愈的相关配置，无需再重复配置。

操作步骤

1. 配置L2TP Client
   a. 配置5G Cellular接口的连接参数，实现5G Cellular接口接入5G网络。
      i. 创建APN模板。

```
<Huawei> system-view
[Huawei] sysname AR1
[AR1] apn profile 5gprofile
[AR1-apn-profile-5gprofile] apn 5gnet
[AR1-apn-profile-5gprofile] quit
```

      ii. 使能轮询DCC功能，配置自动拨号连接。

```
[AR1] interface Cellular 1/0/0
[AR1-Cellular1/0/0] dialer enable-circular
```

 版权所有 © 华为技术有限公司

iii. 在5G Cellular接口上绑定APN模板。

```
[AR1-Cellular1/0/0] apn-profile 5gprofile
Info: The configuration will become effective after link reset.
[AR1-Cellular1/0/0] shutdown
[AR1-Cellular1/0/0] undo shutdown
[AR1-Cellular1/0/0] quit
```

b. 配置用户侧IP地址。

```
[AR1] interface gigabitethernet 0/0/1
[AR1-GigabitEthernet0/0/1] ip address 192.168.1.1 255.255.255.0
[AR1-GigabitEthernet0/0/1] tcp adjust-mss 1200
[AR1-GigabitEthernet0/0/1] quit
```

c. 设置一个L2TP组并配置相关属性。

```
[AR1] l2tp enable
[AR1] l2tp-group 1
[AR1-l2tp1] tunnel name L2TPClient
[AR1-l2tp1] start l2tp ip 12.1.1.1 fullusername huawei
[AR1-l2tp1] tunnel password cipher 123
[AR1-l2tp1] quit
```

d. 配置虚拟PPP用户的用户名和密码，PPP认证方式以及IP地址。

```
[AR1] interface virtual-template 1
[AR1-Virtual-Template1] ppp chap user huawei
[AR1-Virtual-Template1] ppp chap password cipher YsHsjx_202206
[AR1-Virtual-Template1] ip address 13.1.1.2 255.255.255.0
[AR1-Virtual-Template1] quit
```

e. 配置公网路由，访问公司总部的报文将通过5G接口转发。

```
[AR1] ip route-static 12.1.1.1 255.255.255.255 Cellular1/0/0
```

f. 触发L2TP Client建立L2TP隧道。

```
[AR1] interface virtual-template 1
[AR1-virtual-template1] l2tp-auto-client enable
[AR1-virtual-template1] quit
```

g. 配置私网路由，使企业分支用户与总部子网互通。

```
[AR1] ip route-static 192.168.0.0 255.255.255.0 Virtual-Template1
```

2. 配置LNS

a. 配置IP地址。

```
<Huawei> system-view
[Huawei] sysname AR2
[AR2] interface GigabitEthernet 1/0/0
[AR2-GigabitEthernet1/0/0] ip address 192.168.0.1 255.255.255.0
[AR2-GigabitEthernet1/0/0] tcp adjust-mss 1200
[AR2-GigabitEthernet1/0/0] quit
[AR2] interface gigabitethernet 0/0/2
[AR2-GigabitEthernet0/0/2] ip address 12.1.1.1 255.255.255.0
[AR2-GigabitEthernet0/0/2] quit
```

b. 创建虚拟模板Virtual-Template并配置相关信息。

```
[AR2] interface virtual-template 1
[AR2-Virtual-Template1] ppp authentication-mode chap
[AR2-Virtual-Template1] ip address 13.1.1.1 255.255.255.0
[AR2-Virtual-Template1] quit
```

c. 使能L2TP服务，并设置一个L2TP组。

```
[AR2] l2tp enable
[AR2] l2tp-group 1
```

d. 配置LNS侧本端名称及接收的通道对端名称。

```
[AR2-l2tp1] tunnel name LNS
[AR2-l2tp1] allow l2tp virtual-template 1 remote L2TPClient
```

e. 设置通道验证密码。

```
[AR2-l2tp1] tunnel password cipher 123
[AR2-l2tp1] quit
```

f. 设置用户名及口令分别为**huawei**和**YsHsjx_202206**（应与L2TP Client侧的设置一致）。

 版权所有 © 华为技术有限公司

```
[AR2] aaa
[AR2-aaa] local-user huawei password
Please configure the login password (8-128)
It is recommended that the password consist of at least 2 types of characters, i
ncluding lowercase letters, uppercase letters, numerals and special characters.
Please enter password:
Please confirm password:
Info: Add a new user.
Warning: The new user supports all access modes. The management user access mode
s such as Telnet, SSH, FTP, HTTP, and Terminal have security risks. You are advi
sed to configure the required access modes only.
[AR2-aaa] local-user huawei service-type ppp
[AR2-aaa] quit
```

g. 配置公网路由，假设访问公网的路由下一跳地址为12.1.1.2。

```
[AR2] ip route-static 0.0.0.0 0 12.1.1.2
```

配置私网路由，使得企业总部与企业分支用户私网互通。

```
[AR2] ip route-static 192.168.1.0 255.255.255.0 13.1.1.2
```

3. 验证配置结果

配置成功后，分别在L2TP Client和LNS上执行**display l2tp tunnel**命令可发现隧道建立成功，以L2TP Client侧的显示为例：

```
[AR1] display l2tp tunnel

 Total tunnel : 1
 LocalTID RemoteTID RemoteAddress    Port   Sessions RemoteName
 1        1         12.1.1.1         1701   1        LNS
```

执行**display l2tp session**命令可看到会话连接建立情况，以LNS侧的显示为例：

```
[AR2] display l2tp session

Total session : 1
 LocalSID  RemoteSID  LocalTID  Interface           LclTAddr        RmtTAddr        LclSAddr
RmtSAddr
 1         1          1         Virtual-Template1:1   12.1.1.1        1.1.1.1         13.1.1.1
13.1.1.2
```

分支机构的PC可以访问公司总部服务器。

配置脚本

AR1配置文件

```
#
 sysname AR1
#
 l2tp enable
#
apn profile 5gnet
 apn 5gnet
#
interface Virtual-Template1
 ppp chap user huawei
 ppp chap password cipher %^%#'&=6Q(|7-#|.]EB`mK$(h7[CY`2m}-YT)Q=Oh2~2%^%#
 ip address 13.1.1.2 255.255.255.0
 l2tp-auto-client enable
#
interface GigabitEthernet0/0/1
 ip address 192.168.1.1 255.255.255.0
 tcp adjust-mss 1200
#
interface Cellular0/0/1
 dialer enable-circular
 apn-profile 5gnet
 dialer timer autodial 10
 modem auto-recovery dial action modem-reboot fail-times 128
```

 版权所有 © 华为技术有限公司

```
 modem auto-recovery icmp-unreachable action modem-reboot
 modem auto-recovery services-unavailable action modem-reboot test-times 0 interval 3600
 ip address negotiate
#
l2tp-group 1
 tunnel password cipher %@%@d'o6Xpp(i/i:WRC)`'0#3nJ*%@%@
 tunnel name L2TPClient
 start l2tp ip 12.1.1.1 fullusername huawei
#
ip route-static 12.1.1.1 255.255.255.255 Cellular1/0/0
ip route-static 192.168.0.0 255.255.255.0 Virtual-Template1
#
return
```

AR2配置文件

```
#
 sysname AR2
#
 l2tp enable
#
aaa
 local-user huawei password cipher %^%#_<`.CO&(:LeS/$#F\H0Qv8B]KAZja3}3q'RNx;VI%^%#
 local-user huawei privilege level 0
 local-user huawei service-type ppp
#
interface Virtual-Template1
 ppp authentication-mode chap
 ip address 13.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/0
 ip address 192.168.0.1 255.255.255.0
 tcp adjust-mss 1200
#
interface GigabitEthernet2/0/0
 ip address 12.1.1.1 255.255.255.0
#
l2tp-group 1
 allow l2tp virtual-template 1 remote L2TPClient
 tunnel password cipher %@%@5j*=S&AGXK'J}kG])REK]_-o%@%@
 tunnel name LNS
#
ip route-static 0.0.0.0 0.0.0.0 12.1.1.2
ip route-static 192.168.1.0 255.255.255.0 13.1.1.2
#
return
```

7.2.4 配置分支使用 5G 链路和总部建立 DSVPN over IPSec 互连示例

场景介绍

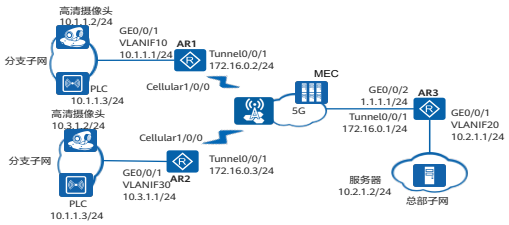
分布在不同地域的企业分支可以通过5G链路拨号接入到Internet，再与企业总部建立DSVPN，实现分支站点接口动态获取IP地址，支持NAT穿越以及企业分支之间、企业分支与总部之间快速、安全、高效互连功能。用户可以通过部署DSVPN over IPSec对总部和分支以及分支间传输的数据进行加密保护。

组网需求

如图7-7所示，企业分支使用AR1接入Internet，在AR1上配置DSVPN over IPSec实现企业分支与总部的业务互通。

 版权所有 © 华为技术有限公司

图 7-7 配置分支与总部之间建立 IPSec over DSVPN 隧道组网图



数据准备

表 7-7 数据准备表

项目	数据	说明
运营商分配给企业分支1的APN名称	5gnet1	APN名称需提前从运营商处获取。
运营商分配给企业分支1的5G Cellular接口的IP地址	2.2.2.2/32	5G Cellular接口拨号接入运营商后，运营商给5G Cellular接口自动分配的IP地址。
分支AR1 LAN侧接口信息	VLAN：10 VLANIF10：10.1.1.1	VLAN 10为分支子网用户所在的VLAN，且分支子网用户的网关为VLANIF10接口。
运营商分配给企业分支2的APN名称	5gnet2	APN名称需提前从运营商处获取。
运营商分配给企业分支2的5G Cellular接口的IP地址	3.3.3.3/32	5G Cellular接口拨号接入运营商后，运营商给5G Cellular接口自动分配的IP地址。
分支AR2 LAN侧接口信息	VLAN：30 VLANIF30：10.3.1.1	VLAN 30为分支子网用户所在的VLAN，且分支子网用户的网关为VLANIF30接口。
运营商分配给总部的GE0/0/2接口的IP地址	1.1.1.1/24	总部AR3通过有线的方式接入Internet，该有线接口GE0/0/2采用静态方式配置IP地址。
总部AR3 LAN侧接口信息	VLAN：20 VLANIF20：10.2.1.1	VLAN 20为总部子网用户所在的VLAN，且总部子网用户的网关为VLANIF20接口。

版权所有 © 华为技术有限公司

项目	数据	说明
总部AR3对端运营商接口的IP地址	2.2.2.1/24	总部AR3对端运营商接口的IP地址用于配置路由信息，使分支和总部之间的路由互通。

TCP MSS 参数配置说明

为了减少网络传输中不必要的分片和重组，网络规划时需要合理设置终端发出的报文大小。对于TCP报文，可以配置5G AR设备的TCP MSS值，通过修改应用层报文数据包的长度来避免报文分片。在5G 2B专线场景中，TCP MSS取值比较简单，在隧道两端AR设备的LAN侧接入物理口或VLANIF口上配置TCP MSS为推荐值1200。

配置思路

1. 配置5G Cellular接口的连接参数，实现5G Cellular接口接入5G网络。
2. 配置企业子网，为内部用户自动分配IP地址。
3. 配置IKE对等体。
4. 创建IPSec安全提议。
5. 配置IPSec安全框架。
6. 配置Tunnel接口。
7. 部署路由协议来实现分支/总部间的通信。

操作步骤

1. 配置5G Cellular接口的连接参数，实现5G Cellular接口接入5G网络。

   # 配置分支1的连接参数

   a. 创建APN模板。

   ```
   <Huawei> system-view
   [Huawei] sysname AR1
   [AR1] apn profile 5gprofile1
   [AR1-apn-profile-5gprofile1] apn 5gnet1
   [AR1-apn-profile-5gprofile1] quit
   ```

   b. 使能轮询DCC功能，配置自动拨号连接。

   ```
   [AR1] interface Cellular 1/0/0
   [AR1-Cellular1/0/0] dialer enable-circular
   ```

   c. 在5G Cellular接口上绑定APN模板。

   ```
   [AR1-Cellular1/0/0] apn-profile 5gprofile1
   Info: The configuration will become effective after link reset.
   [AR1-Cellular1/0/0] shutdown
   [AR1-Cellular1/0/0] undo shutdown
   [AR1-Cellular1/0/0] quit
   ```

   # 配置分支2的连接参数

   a. 创建APN模板。

   ```
   <Huawei> system-view
   [Huawei] sysname AR2
   [AR2] apn profile 5gprofile2
   [AR2-apn-profile-5gprofile2] apn 5gnet2
   [AR2-apn-profile-5gprofile2] quit
   ```

   b. 使能轮询DCC功能，配置自动拨号连接。

   ```
   [AR2] interface Cellular 1/0/0
   [AR2-Cellular1/0/0] dialer enable-circular
   ```

 版权所有 © 华为技术有限公司

c. 在5G Cellular接口上绑定APN模板。

```
[AR2-Cellular1/0/0] apn-profile 5gprofile2
Info: The configuration will become effective after link reset.
[AR2-Cellular1/0/0] shutdown
[AR2-Cellular1/0/0] undo shutdown
[AR2-Cellular1/0/0] quit
```

2. 配置企业子网，为内部用户自动分配IP地址。

a. 配置分支1子网，创建VLAN10，将GE0/0/1接口加入VLAN10，并配置DHCP功能。配置VLANIF 10接口TCP最大报文段长度为1200字节并配置DHCP功能。

```
[AR1] vlan 10
[AR1-vlan10] quit
[AR1] interface GigabitEthernet 0/0/1
[AR1-GigabitEthernet0/0/1] port link-type access
[AR1-GigabitEthernet0/0/1] port default vlan 10
[AR1-GigabitEthernet0/0/1] quit
[AR1] dhcp enable
[AR1] interface Vlanif 10
[AR1-Vlanif10] ip address 10.1.1.1 24
[AR1-Vlanif10] dhcp select interface
[AR1-Vlanif10] tcp adjust-mss 1200
[AR1-Vlanif10] quit
```

b. 配置分支2子网，创建VLAN30，将GE0/0/1接口加入VLAN30，并配置DHCP功能。配置VLANIF 30接口TCP最大报文段长度为1200字节并配置DHCP功能。

```
[AR2] vlan 30
[AR2-vlan30] quit
[AR2] interface GigabitEthernet 0/0/1
[AR2-GigabitEthernet0/0/1] port link-type access
[AR2-GigabitEthernet0/0/1] port default vlan 30
[AR2-GigabitEthernet0/0/1] quit
[AR2] dhcp enable
[AR2] interface Vlanif 30
[AR2-Vlanif30] ip address 10.3.1.1 24
[AR2-Vlanif30] dhcp select interface
[AR2-Vlanif20] tcp adjust-mss 1200
[AR2-Vlanif30] quit
```

c. 配置总部子网，创建VLAN20，将GE0/0/1接口加入VLAN20，并配置DHCP功能。配置VLANIF 20接口TCP最大报文段长度为1200字节并配置DHCP功能。

```
<Huawei> system-view
[Huawei] sysname AR3
[AR3] vlan 20
[AR3-vlan20] quit
[AR3] interface GigabitEthernet 0/0/1
[AR3-GigabitEthernet0/0/1] port link-type access
[AR3-GigabitEthernet0/0/1] port default vlan 20
[AR3-GigabitEthernet0/0/1] quit
[AR3] dhcp enable
[AR3] interface Vlanif 20
[AR3-Vlanif20] ip address 10.2.1.1 24
[AR3-Vlanif20] dhcp select interface
[AR3-Vlanif20] tcp adjust-mss 1200
[AR3-Vlanif20] quit
```

3. 配置总部接口IP地址。

```
[AR3] interface gigabitethernet 0/0/2
[AR3-GigabitEthernet0/0/2] ip address 1.1.1.1 255.255.255.0
[AR3-GigabitEthernet0/0/2] quit
```

4. 配置IKE对等体。

a. 配置分支1的IKE安全提议。

```
[AR1] ike proposal 5
[AR1-ike-proposal-5] authentication-algorithm sha2-256
[AR1-ike-proposal-5] encryption-algorithm aes-128
```

 版权所有 © 华为技术有限公司

```
[AR1-ike-proposal-5] dh group14
[AR1-ike-proposal-5] quit
```

b. 配置分支1的IKE对等体。

```
[AR1] ike peer spu1
[AR1-ike-peer-spu1] ike-proposal 5
[AR1-ike-peer-spu1] pre-shared-key cipher YsHsjx_202206
[AR1-ike-peer-spu1] quit
```

c. 配置分支2的IKE安全提议。

```
[AR2] ike proposal 5
[AR2-ike-proposal-5] authentication-algorithm sha2-256
[AR2-ike-proposal-5] encryption-algorithm aes-128
[AR2-ike-proposal-5] dh group14
[AR2-ike-proposal-5] quit
```

d. 配置分支2的IKE对等体。

```
[AR2] ike peer spu2
[AR2-ike-peer-spu2] ike-proposal 5
[AR2-ike-peer-spu2] pre-shared-key cipher YsHsjx_202206
[AR2-ike-peer-spu2] quit
```

e. 配置总部的IKE安全提议。

```
[AR3] ike proposal 5
[AR3-ike-proposal-5] authentication-algorithm sha2-256
[AR3-ike-proposal-5] encryption-algorithm aes-128
[AR3-ike-proposal-5] dh group14
[AR3-ike-proposal-5] quit
```

f. 配置总部的IKE对等体。

```
[AR3] ike peer spu3
[AR3-ike-peer-spu3] ike-proposal 5
[AR3-ike-peer-spu3] pre-shared-key cipher YsHsjx_202206
[AR3-ike-peer-spu3] quit
```

5. 配置IPSec安全提议。

a. 配置分支1的安全提议。

```
[AR1] ipsec proposal pro1
[AR1-ipsec-proposal-pro1] transform ah-esp
[AR1-ipsec-proposal-pro1] ah authentication-algorithm sha2-256
[AR1-ipsec-proposal-pro1] esp authentication-algorithm sha2-256
[AR1-ipsec-proposal-pro1] esp encryption-algorithm aes-192
[AR1-ipsec-proposal-pro1] quit
```

b. 配置分支2的安全提议。

```
[AR2] ipsec proposal pro1
[AR2-ipsec-proposal-pro1] transform ah-esp
[AR2-ipsec-proposal-pro1] ah authentication-algorithm sha2-256
[AR2-ipsec-proposal-pro1] esp authentication-algorithm sha2-256
[AR2-ipsec-proposal-pro1] esp encryption-algorithm aes-192
[AR2-ipsec-proposal-pro1] quit
```

c. 配置总部安全提议。

```
[AR3] ipsec proposal pro1
[AR3-ipsec-proposal-pro1] transform ah-esp
[AR3-ipsec-proposal-pro1] ah authentication-algorithm sha2-256
[AR3-ipsec-proposal-pro1] esp authentication-algorithm sha2-256
[AR3-ipsec-proposal-pro1] esp encryption-algorithm aes-192
[AR3-ipsec-proposal-pro1] quit
```

6. 配置IPSec安全框架。

a. 配置分支1安全框架。

```
[AR1] ipsec profile profile1
[AR1-ipsec-profile-profile1] proposal pro1
[AR1-ipsec-profile-profile1] ike-peer spu1
[AR1-ipsec-profile-profile1] quit
```

b. 配置分支2安全框架。

```
[AR2] ipsec profile profile1
[AR2-ipsec-profile-profile1] proposal pro1
```

 版权所有 © 华为技术有限公司

```
[AR2-ipsec-profile-profile1] ike-peer spu2
[AR2-ipsec-profile-profile1] quit
```

c. 配置总部安全框架。

```
[AR3] ipsec profile profile1
[AR3-ipsec-profile-profile1] proposal pro1
[AR3-ipsec-profile-profile1] ike-peer spu3
[AR3-ipsec-profile-profile1] quit
```

7. 配置Tunnel接口。

a. 配置分支1的Tunnel接口和OSPF相关属性以及总部的静态NHRP peer表项，应用安全框架。

```
[AR1] interface tunnel 0/0/1
[AR1-Tunnel0/0/1] ip address 172.16.0.2 255.255.255.0
[AR1-Tunnel0/0/1] tunnel-protocol gre p2mp
[AR1-Tunnel0/0/1] source Cellular 1/0/0
[AR1-Tunnel0/0/1] nhrp entry 172.16.0.1 1.1.1.1 register
[AR1-Tunnel0/0/1] nhrp registration no-unique
[AR1-Tunnel0/0/1] ospf network-type p2mp
[AR1-Tunnel0/0/1] nhrp shortcut
[AR1-Tunnel0/0/1] ipsec profile profile1
[AR1-Tunnel0/0/1] quit
```

b. 配置分支2的Tunnel接口和OSPF相关属性以及总部的静态NHRP peer表项，应用安全框架。

```
[AR2] interface tunnel 0/0/1
[AR2-Tunnel0/0/1] ip address 172.16.0.3 255.255.255.0
[AR2-Tunnel0/0/1] tunnel-protocol gre p2mp
[AR2-Tunnel0/0/1] source Cellular 1/0/0
[AR2-Tunnel0/0/1] nhrp entry 172.16.0.1 1.1.1.1 register
[AR2-Tunnel0/0/1] nhrp registration no-unique
[AR2-Tunnel0/0/1] ospf network-type p2mp
[AR2-Tunnel0/0/1] nhrp shortcut
[AR2-Tunnel0/0/1] ipsec profile profile1
[AR2-Tunnel0/0/1] quit
```

c. 配置总部的Tunnel接口和OSPF相关属性，应用安全框架。

```
[AR3] interface tunnel 0/0/1
[AR3-Tunnel0/0/1] ip address 172.16.0.1 255.255.255.0
[AR3-Tunnel0/0/1] tunnel-protocol gre p2mp
[AR3-Tunnel0/0/1] source GigabitEthernet 0/0/2
[AR3-Tunnel0/0/1] nhrp entry multicast dynamic
[AR3-Tunnel0/0/1] ospf network-type p2mp
[AR3-Tunnel0/0/1] nhrp redirect
[AR3-Tunnel0/0/1] ipsec profile profile1
[AR3-Tunnel0/0/1] quit
```

8. 配置公网路由，使企业分支和总部子网的用户可以互通。

在分支1配置静态路由。

```
[AR1] ip route-static 1.1.1.0 255.255.255.0 Cellular1/0/0
```

在分支2配置静态路由。

```
[AR2] ip route-static 1.1.1.0 255.255.255.0 Cellular1/0/0
```

在总部配置静态路由。

```
[AR3] ip route-static 0.0.0.0 0.0.0.0 1.1.1.2
```

9. 配置OSPF基本功能。

配置分支1。

```
[AR1] ospf 1 router-id 172.16.0.2
[AR1-ospf-1] area 0.0.0.0
[AR1-ospf-1-area-0.0.0.0] network 172.16.0.0 0.0.0.255
[AR1-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[AR1-ospf-1-area-0.0.0.0] quit
[AR1-ospf-1] quit
```

配置分支2。

 版权所有 © 华为技术有限公司

```
[AR2] ospf 1 router-id 172.16.0.3
[AR2-ospf-1] area 0.0.0.0
[AR2-ospf-1-area-0.0.0.0] network 172.16.0.0 0.0.0.255
[AR2-ospf-1-area-0.0.0.0] network 10.3.1.0 0.0.0.255
[AR2-ospf-1-area-0.0.0.0] quit
[AR2-ospf-1] quit
```

配置总部。

```
[AR3] ospf 1 router-id 172.16.0.1
[AR3-ospf-1] area 0.0.0.0
[AR3-ospf-1-area-0.0.0.0] network 172.16.0.0 0.0.0.255
[AR3-ospf-1-area-0.0.0.0] network 10.2.1.0 0.0.0.255
[AR3-ospf-1-area-0.0.0.0] quit
[AR3-ospf-1] quit
```

验证

1. 在分支1和分支2上执行**display nhrp peer all**命令，可以看到总部的注册信息。以分支1的显示为例：

```
[AR1] display nhrp peer all
--------------------------------------------------------------------------------
Protocol-addr   Mask  NBMA-addr       NextHop-addr    Type        Flag
--------------------------------------------------------------------------------
172.16.0.1      32    1.1.1.1         172.16.0.1      AR          up
--------------------------------------------------------------------------------
Tunnel interface: Tunnel0/0/1
Created time    : 00:10:58
Expire time     : --

Number of nhrp peers: 1
```

2. 检查IPSec SA信息，在总部和分支上查看进行注册后生成的IPSec SA信息。以分支1的显示为例：

```
[AR1] display ipsec sa

ipsec sa information:

===============================

Interface: Tunnel0/0/1
===============================


 ----------------------------
 IPSec profile name: "1"
 Mode              : PROF-ISAKMP
 ----------------------------
   Connection ID     : 16092
   Encapsulation mode: Tunnel
   Holding time      : 0d 0h 17m 3s
   Tunnel local      : 2.2.2.2/500
   Tunnel remote     : 1.1.1.1/500
   Flow source       : 2.2.2.2/255.255.255.255
0/0-65535
   Flow destination  : 1.1.1.1/255.255.255.255
0/0-65535

   [Outbound ESP SAs]
     SPI: 3064365 (0x2ec22d)
     Proposal: ESP-ENCRYPT-AES-256 ESP-AUTH-
SHA2-256-128
     SA remaining soft duration (kilobytes/sec):
1345536/2588
     SA remaining hard duration (kilobytes/sec):
1843200/3560
     Outpacket count       : 0
     Outpacket encap count : 0
     Outpacket drop count  : 0
```

 版权所有 © 华为技术有限公司

```
    Max sent sequence-number: 0
    UDP encapsulation used for NAT traversal:
N

  [Outbound AH SAs]
    SPI: 710278 (0xad686)
    Proposal: AH-SHA1-96
    SA remaining soft duration (kilobytes/sec):
1345536/2517
    SA remaining hard duration (kilobytes/sec):
1843200/3560
    Outpacket count      : 0
    Outpacket encap count : 0
    Outpacket drop count  : 0
    Max sent sequence-number: 0
    UDP encapsulation used for NAT traversal:
N

  [Inbound AH SAs]
    SPI: 11203890 (0xaaf532)
    Proposal: AH-SHA1-96
    SA remaining soft duration (kilobytes/sec):
1290240/2408
    SA remaining hard duration (kilobytes/sec):
1843200/3560
    Inpacket count       : 0
    Inpacket decap count  : 0
    Inpacket drop count   : 0
    Max received sequence-number:
0
    UDP encapsulation used for NAT traversal:
N
    Anti-replay : Enable
    Anti-replay window size: 1024

  [Inbound ESP SAs]
    SPI: 6901571 (0x694f43)
    Proposal: ESP-ENCRYPT-AES-256 ESP-AUTH-
SHA2-256-128
    SA remaining soft duration (kilobytes/sec):
1290240/2480
    SA remaining hard duration (kilobytes/sec):
1843200/3560
    Inpacket count       : 0
    Inpacket decap count  : 0
    Inpacket drop count   : 0
    Max received sequence-number:
0
    UDP encapsulation used for NAT traversal:
N
    Anti-replay : Enable
    Anti-replay window size: 1024
```

配置文件

AR1配置文件

```
#
 sysname AR1
#
apn profile 5gprofile1
 apn 5gnet1
#
ipsec proposal pro1
 transform ah-esp
 ah authentication-algorithm sha2-256
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-128
#
ike proposal 5
```

 版权所有 © 华为技术有限公司

```
 encryption-algorithm aes-128
 authentication-algorithm sha2-256
 dh group14
#
ike peer spu1
 pre-shared-key cipher %^%#JvZxR2g8c;a9~FPN~n'$7`DEV&=G(=Et02P/%\*!%^%#
 ike-proposal 5
#
ipsec profile profile1
 ike-peer spu1
 proposal pro1
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
 dhcp select interface
 tcp adjust-mss 1200
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 10
#
interface Cellular1/0/0
 dialer enable-circular
 apn-profile 5gprofile1
 dialer timer autodial 10
 modem auto-recovery dial action modem-reboot fail-times 128
 modem auto-recovery icmp-unreachable action modem-reboot
 modem auto-recovery services-unavailable action modem-reboot test-times 0 interval 3600
 ip address negotiate
#
interface Tunnel0/0/1
 ip address 172.16.0.2 255.255.255.0
 tunnel-protocol gre p2mp
 source Cellular1/0/0
 ospf network-type p2mp
 nhrp shortcut
 nhrp entry 172.16.0.1 1.1.1.1 register
 nhrp registration no-unique
 ipsec profile profile1
#
ospf 1 router-id 172.16.0.2
 area 0.0.0.0
 network 172.16.0.0 0.0.0.255
 network 10.1.1.0 0.0.0.255
#
ip route-static 1.1.1.1 255.255.255.0 Cellular1/0/0
#
return
```

AR2配置文件

```
#
 sysname AR2
#
apn profile 5gprofile2
 apn 5gnet2
#
ipsec proposal pro1
 transform ah-esp
 ah authentication-algorithm sha2-256
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-128
#
ike proposal 5
 encryption-algorithm aes-128
 authentication-algorithm sha2-256
 dh group14
#
ike peer spu2
 pre-shared-key cipher %^%#JvZxR2g8c;a9~FPN~n'$7`DEV&=G(=Et02P/%\*!%^%#
 ike-proposal 5
```

 版权所有 © 华为技术有限公司

```
#
ipsec profile profile1
 ike-peer spu2
 proposal pro1
#
interface Vlanif30
 ip address 10.3.1.1 255.255.255.0
 dhcp select interface
 tcp adjust-mss 1200
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 30
#
interface Cellular1/0/0
 dialer enable-circular
 apn-profile 5gprofile2
 dialer timer autodial 10
 modem auto-recovery dial action modem-reboot fail-times 128
 modem auto-recovery icmp-unreachable action modem-reboot
 modem auto-recovery services-unavailable action modem-reboot test-times 0 interval 3600
 ip address negotiate
#
interface Tunnel0/0/1
 ip address 172.16.0.3 255.255.255.0
 tunnel-protocol gre p2mp
 source Cellular1/0/0
 ospf network-type p2mp
 nhrp shortcut
 nhrp entry 172.16.0.1 1.1.1.1 register
 nhrp registration no-unique
 ipsec profile profile1
#
ospf 1 router-id 172.16.0.3
 area 0.0.0.0
 network 172.16.0.0 0.0.0.255
 network 10.3.1.0 0.0.0.255
#
ip route-static 1.1.1.1 255.255.255.0 Cellular1/0/0
#
return
```

AR3配置文件

```
#
 sysname AR3
#
ipsec proposal pro1
 ah authentication-algorithm sha2-256
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-128
#
ike proposal 5
 encryption-algorithm aes-128
 authentication-algorithm sha2-256
 dh group14
#
ike peer spu3
 pre-shared-key cipher %^%#K{JG:rWVHPMnf;5\|,GW(Luq'qi8BT4nOj%5W5=)%^%#
 ike-proposal 5
#
ipsec profile profile1
 ike-peer spu3
 proposal pro1
#
interface GigabitEthernet0/0/2
 ip address 1.1.1.1 255.255.255.0
#
interface Tunnel0/0/1
 ip address 172.16.0.1 255.255.255.0
 tunnel-protocol gre p2mp
```

 版权所有 © 华为技术有限公司

```
 source GigabitEthernet0/0/2
 ospf network-type p2mp
 nhrp redirect
 nhrp entry multicast dynamic
 ipsec profile profile1
#
interface Vlanif20
 ip address 10.2.1.1 255.255.255.0
 dhcp select interface
 tcp adjust-mss 1200
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 20
#
ospf 1 router-id 172.16.0.1
 area 0.0.0.0
 network 172.16.0.0 0.0.0.255
 network 10.2.1.0 0.0.0.255
#
ip route-static 0.0.0.0 0.0.0.0 1.1.1.2
#
return
```

7.2.5 配置分支使用 5G 链路和总部建立 VPDN 互联示例

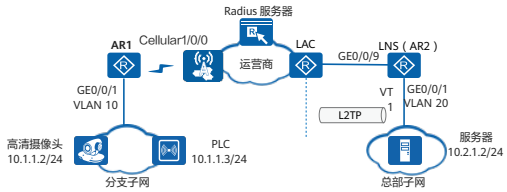
场景介绍

VPDN是基于拨号网络发展出来的一种虚拟私有拨号网络。VPDN在企业分支和总部网关之间，建立一条透明的点到点虚拟链路来转发流量，是应用于远程办公场景中为出差员工远程访问企业内网资源提供接入服务的一种重要VPN技术。二层隧道协议L2TP是VPDN隧道协议的一种，L2TP通过拨号网络（PSTN/ISDN），基于点到点协议PPP，在L2TP访问集中器LAC和L2TP网络服务器LNS之间建立隧道，实现分支与总部互联。

组网需求

如图1所示，企业分支通过AR1企业路由器与总部建立VPDN连接，AR1企业路由器通过5G链路拨号与运营商提供的LAC建立PPP连接，运营商的LAC与企业总部LNS设备建立L2TP隧道转发业务流量，实现企业分支用户和总部之间的L2TP连接。

图 7-8 配置分支使用 5G 链路和总部建立 VPDN 互联组网图



 版权所有 © 华为技术有限公司

数据准备

表 7-8 数据准备表

项目	数据	说明
运营商分配给企业分支的APN名称	5gnet	APN名称需提前从运营商处获取。
运营商分配给企业分支接入认证的用户名	huawei	用户名、密码以及认证方式需要咨询运营商。
运营商分配给企业分支接入认证的密码	YsHsjx_202206	用户名、密码以及认证方式需要咨询运营商。
运营商分配给企业分支接入认证时的认证方式	chap	用户名、密码以及认证方式需要咨询运营商。
LNS分配给分支5G Cellular接口的IP地址	1.1.1.2/32	5G Cellular接口拨号接入运营商后，运营商给5G Cellular接口自动分配的IP地址。
运营商给总部GE0/0/9接口分配的IP地址	2.2.2.2/24	总部AR2通过有线的方式接入Internet，该有线接口GE0/0/9采用静态方式配置IP地址。
分支AR1 LAN侧接口信息	所属VLAN：VLAN：10 网关地址：VLANIF10（10.1.1.1/24） LAN侧物理接口：GE0/0/1	VLAN 10为分支子网用户所在的VLAN，且分支子网用户的网关为VLANIF10接口。
总部AR2 LAN侧接口信息	所属VLAN：20 网关地址：VLANIF20（10.2.1.1/24） LAN侧物理接口：GE0/0/1	VLAN 20为总部子网用户所在的VLAN，且总部子网用户的网关为VLANIF20接口。
总部AR2的虚拟接口IP地址	VT1接口：1.1.1.1/24	为对端LAC分配IP地址，接入L2TP连接。

TCP MSS 参数配置说明

为了减少网络传输中不必要的分片和重组，网络规划时需要合理设置终端发出的报文大小。对于TCP报文，可以配置5G AR设备的TCP MSS值，通过修改应用层报文数据包的长度来避免报文分片。在5G 2B专线场景中，TCP MSS取值比较简单，在隧道两端AR设备的LAN侧接入物理口或VLANIF口上配置TCP MSS为推荐值1200。

 版权所有 © 华为技术有限公司

配置思路

1. 配置5G Cellular接口的连接参数，实现5G Cellular接口接入5G网络。
2. 配置企业子网，为内部用户自动分配IP地址。
3. 配置总部LNS功能，对分支用户进行L2TP接入认证。
4. 配置静态路由，使企业分支和总部的内网流量可以上行传输到Internet。

说明

在5G Cellular接口下执行命令**dialer enable-circular**配置轮询拨号功能时，设备会同时下发自动拨号、IP地址协商和5G Modem自愈的相关配置，无需再重复配置。

操作步骤

1. 配置5G Cellular接口的连接参数，实现5G Cellular接口接入5G网络。
   a. 创建APN模板。
   ```
   <Huawei> system-view
   [Huawei] sysname AR1
   [AR1] apn profile 5gprofile
   [AR1-apn-profile-5gprofile] apn 5gnet
   [AR1-apn-profile-5gprofile] quit
   ```
   b. 使能轮询DCC功能，配置自动拨号连接。
   ```
   [AR1] interface Cellular 1/0/0
   [AR1-Cellular1/0/0] dialer enable-circular
   ```
   c. 在5G Cellular接口上绑定APN模板。
   ```
   [AR1-Cellular1/0/0] apn-profile 5gprofile
   Info: The configuration will become effective after link reset.
   [AR1-Cellular1/0/0] shutdown
   [AR1-Cellular1/0/0] undo shutdown
   [AR1-Cellular1/0/0] quit
   ```
2. 配置企业子网，为内部用户自动分配IP地址。
   a. 配置分支子网，创建VLAN10，将GE0/0/1接口加入VLAN10。配置VLANIF 10接口TCP最大报文段长度为1200字节并配置DHCP功能。
   ```
   [AR1] vlan 10
   [AR1-vlan10] quit
   [AR1] interface GigabitEthernet 0/0/1
   [AR1-GigabitEthernet0/0/1] port link-type access
   [AR1-GigabitEthernet0/0/1] port default vlan 10
   [AR1-GigabitEthernet0/0/1] quit
   [AR1] dhcp enable
   [AR1] interface Vlanif 10
   [AR1-Vlanif10] ip address 10.1.1.1 24
   [AR1-Vlanif10] dhcp select interface
   [AR1-Vlanif10] tcp adjust-mss 1200
   [AR1-Vlanif10] quit
   ```
   b. 配置总部子网，创建VLAN20，将GE0/0/1接口加入VLAN20。配置VLANIF 20接口TCP最大报文段长度为1200字节并配置DHCP功能。
   ```
   <Huawei> system-view
   [Huawei] sysname AR2
   [AR2] vlan 20
   [AR2-vlan20] quit
   [AR2] interface GigabitEthernet 0/0/1
   [AR2-GigabitEthernet0/0/1] port link-type access
   [AR2-GigabitEthernet0/0/1] port default vlan 20
   [AR2-GigabitEthernet0/0/1] quit
   [AR2] dhcp enable
   [AR2] interface Vlanif 20
   [AR2-Vlanif20] ip address 10.2.1.1 24
   [AR2-Vlanif20] dhcp select interface
   [AR2-Vlanif20] tcp adjust-mss 1200
   [AR2-Vlanif20] quit
   ```

 版权所有 © 华为技术有限公司

3. 配置总部LNS功能

   a. # 在与通道相连接的物理接口上配置IP地址。
   ```
   <AR2> system-view
   [AR2] interface gigabitEthernet 0/0/9
   [AR2-GigabitEthernet0/0/9] ip address 2.2.2.2 255.255.255.0
   [AR2-GigabitEthernet0/0/9] quit
   ```

   b. # 配置地址池。
   ```
   [AR2] ip pool 1
   [AR2-ip-pool-1] network 1.1.1.0 mask 24
   [AR2-ip-pool-1] gateway-list 1.1.1.1
   [AR2-ip-pool-1] quit
   ```

   c. # 创建虚模板Virtual-Template并配置相关信息。
   ```
   [AR2] interface virtual-template 1
   [AR2-Virtual-Template1] ppp authentication-mode chap
   [AR2-Virtual-Template1] ip address 1.1.1.1 255.255.255.0
   [AR2-Virtual-Template1] remote address pool 1
   [AR2-Virtual-Template1] quit
   ```

   d. # 使能L2TP服务，并设置一个L2TP组。
   ```
   [AR2] l2tp enable
   [AR2] l2tp-group 1
   ```

   e. # 配置LNS侧本端名称及接收的通道对端名称。
   ```
   [AR2-l2tp1] tunnel name LNS
   [AR2-l2tp1] allow l2tp virtual-template 1 remote LAC
   ```

   f. # 启用通道验证并设置通道验证密码。
   ```
   [AR2-l2tp1] tunnel authentication
   [AR2-l2tp1] tunnel password cipher YsHsjx_202206
   [AR2-l2tp1] quit
   ```

   g. # 设置用户名及口令分别为**huawei**和**YsHsjx_202206**（应与LAC侧的设置一致）。
   ```
   [AR2] aaa
   [AR2-aaa] local-user huawei password
   Please configure the login password (8-128)It is recommended that the password consist of at least 2 types of characters, including lowercase letters, uppercase letters, numerals and special characters.
   Please enter password:
   Please confirm password:
   Info: Add a new user.
   Warning: The new user supports all access modes. The management user access modes such as Telnet, SSH, FTP, HTTP, and Terminal have security risks. You are advised to configure the required access modes only.
   [AR2-aaa] local-user huawei service-type ppp
   [AR2-aaa] quit
   ```

4. 配置静态路由，使企业分支和总部子网的用户可以互通。

   a. 配置分支缺省路由，出接口为5G Cellular1/0/0。
   ```
   [AR1] ip route-static 0.0.0.0 0 Cellular 1/0/0
   [AR1] quit
   ```

   b. 配置两条总部静态路由，一条缺省路由的下一跳地址为对端运营商接口的IP地址，一条静态路由的下一跳地址为1.1.1.2。
   ```
   [AR2] ip route-static 0.0.0.0 0 2.2.2.1
   [AR2] ip route-static 10.1.1.0 255.255.255.0 1.1.1.2
   [AR2] quit
   ```

验证

1. 在AR1上执行命令**display ip interface brief Cellular 1/0/0**，查看Cellular1/0/0接口获取到的IP地址。
   ```
   <AR1> display ip interface brief Cellular 1/0/0
   *down: administratively down
   ^down: standby
   (l): loopback
   ```

 版权所有 © 华为技术有限公司

```
(s): spoofing
(E): E-Trunk down
Interface                   IP Address/Mask      Physical   Protocol

Cellular1/0/0               1.1.1.2/32           up         up
```

2. 在AR1上执行命令**display Cellular 1/0/0 all**，查看Cellular1/0/0接口的状态信息。

```
<AR1> display Cellular 1/0/0 all
Modem State:
Hardware Information.
=====================
Model = RG801
Modem Type = 5G module
Modem Firmware Version = RG801HEAAAR01A07M8G
Hardware Version = HiB5000_MODEM Ver.A
Integrate circuit card identity (ICCID) = 98681020100202000069
International Mobile Subscriber Identity (IMSI) = 460070075591996
Mobile Station International ISDN Number (MSISDN) = None
International Mobile Equipment Identity (IMEI) = 867147050004457
Factory Serial Number (FSN) = 0123456789ABCDEF
Modem Status = Online
Profile Information.
====================
Profile 1
--------
PDP Type = IPv4, Header Compression = OFF
Data Compression = OFF
Access Point Name (APN) = 5gnet
Packet Session Status = Active
* - Default profile
Network Information.
====================
Current Service Status = Service available
Service Domain = Combined
Current Service = PS
Packet Service = Attached
Packet Session Status = Active
Current Roaming Status = Roaming
Network Selection Mode = Automatic
Network Connection Mode = LTE-NR
Current Network Connection = 5G(NSA)
Mobile Country Code (MCC) = 369
Mobile Network Code (MNC) = 77
Mobile Operator Information = Unknown
Tracking Area Code (TAC) = 1002
Cell ID = 9881858
Radio Information.
==================
Current Bands :
  WCDMA: AUTO
  LTE: B3
  NR: AUTO
LTE:
Current Band = B3
Current RSSI >= -51 dBm
Current RSRP = -71 dBm (strong)
Current RSRQ = -6 dB
Current SINR = 6 dB
NR:
Current Band = N78
Current RSRP = -65 dBm (strong)
Current RSRQ = -10 dB
Current SINR = 38 dB
Bands supported :
  WCDMA: WCDMA850 WCDMA900 WCDMA2100
  FDD LTE: B1 B3 B5 B7 B8 B20 B28
  TDD LTE: B34 B38 B39 B40 B41
  FDD NR: N1 N3 N28
  TDD NR: N41 N77 N78 N79
```

 版权所有 © 华为技术有限公司

```
Modem Security Information.
=========================
SIM ID = 1
PIN Verification = Disabled
PIN Status = Ready
Number of Retries remaining = 3
SIM Status = OK
```

3. 在AR1上执行命令**ping -a 10.1.1.1 10.2.1.1**，模拟分支用户访问总部用户的流量，流量能Ping通。

```
<AR1> ping -a 10.1.1.1 10.2.1.1
  PING 10.2.1.1: 56  data bytes, press CTRL_C to break
    Reply from 10.2.1.1: bytes=56 Sequence=1 ttl=255 time=51 ms
    Reply from 10.2.1.1: bytes=56 Sequence=2 ttl=255 time=35 ms
    Reply from 10.2.1.1: bytes=56 Sequence=3 ttl=255 time=45 ms
    Reply from 10.2.1.1: bytes=56 Sequence=4 ttl=255 time=40 ms
    Reply from 10.2.1.1: bytes=56 Sequence=5 ttl=255 time=37 ms

  --- 10.2.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 35/41/51 ms
```

配置脚本

AR1配置文件

```
#
 sysname AR1
#
vlan batch 10
#
dhcp enable
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
 tcp adjust-mss 1200
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 10
#
interface Cellular1/0/0
 dialer enable-circular
 apn-profile 5gprofile
 dialer timer autodial 10
 modem auto-recovery dial action modem-reboot fail-times 128
 modem auto-recovery icmp-unreachable action modem-reboot
 modem auto-recovery services-unavailable action modem-reboot test-times 0 interval 3600
 ip address negotiate
#
apn profile 5gprofile
 apn 5gnet
#
ip route-static 0.0.0.0 0.0.0.0 Cellular1/0/0
#
return
```

AR2配置文件

```
#
 sysname AR2
#
vlan batch 20
#
 l2tp enable
#
interface Vlanif20
 ip address 10.1.1.1 255.255.255.0
```

 版权所有 © 华为技术有限公司

```
 tcp adjust-mss 1200
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 20
#
ip pool 1
 gateway-list 1.1.1.0
 network 1.1.1.1 mask 255.255.255.0
#
aaa
 local-user huawei password cipher %^%#_<`.CO&(:LeS/$#F\H0Qv8B]KAZja3}3q'RNx;VI%^%#
 local-user huawei privilege level 0
 local-user huawei service-type ppp
#
interface Virtual-Template1
 ppp authentication-mode chap
 remote address pool 1
 ip address 1.1.1.1 255.255.255.0
#
interface GigabitEthernet0/0/9
 ip address 2.2.2.2 255.255.255.0
#
l2tp-group 1
 allow l2tp virtual-template 1 remote LAC
 tunnel password cipher %@%@5j*=S&AGXK'J}kG])REK]_-o%@%@
 tunnel name LNS
#
ip route-static 0.0.0.0 0.0.0.0 2.2.2.1
ip route-static 10.1.1.0 255.255.255.0 1.1.1.2
#
return
```

7.2.6 配置分支使用 5G 链路和总部建立 Ethernet over GRE 隧道互联示例

场景介绍

Ethernet over GRE是一种将以太网协议报文通过GRE封装后，在另一个网络中传输的隧道技术，属于一种L2VPN。为了转发Ethernet报文，配置Ethernet over GRE功能时，需在设备LAN侧的物理以太网接口和WAN侧的Tunnel接口上分别绑定二层VE接口，让LAN侧物理以太网接口收到的以太报文通过设备两侧绑定的VE接口进行转发，然后从WAN侧Tunnel接口进行GRE封装后发送出去，最终实现以太报文通过GRE隧道进行透传。

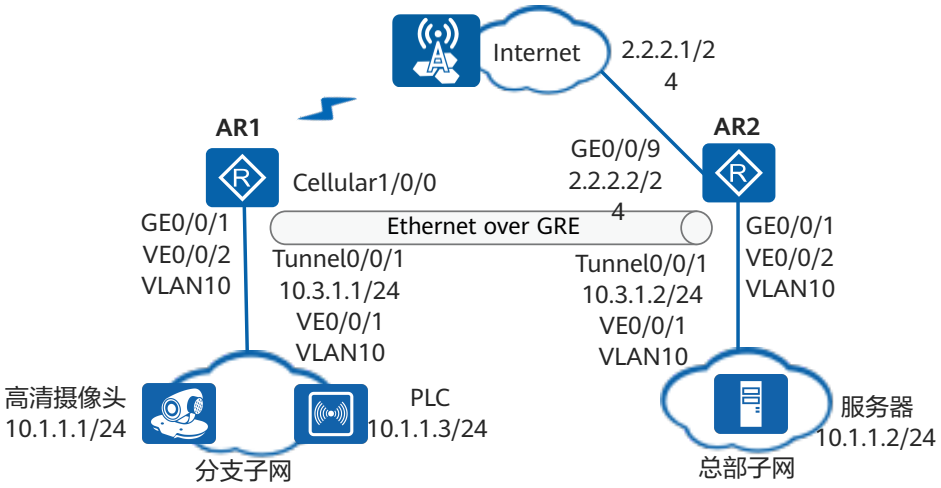
企业分支通过5G链路接入到Internet，然后与企业总部建立VPN，使得分支可以通过Internet接入总部。根据企业分支和总部之间的业务诉求，可以在5G链路上建立不同的VPN隧道。当企业总部和分支的网络都是以太网络，且总部和分支之间需要交互二层业务时，可以在分支的5G链路上构建一条Ethernet over GRE隧道来承载它们之间的L2业务流量，达到在5G链路上传递Ethernet报文的目的。

组网需求

如图1所示，企业分支和总部之间通过Internet网络互通。企业分支使用AR1企业路由器作为出口网关，AR1企业路由器通过5G链路接入Internet。企业分支和总部之间在5G链路上构建Ethernet over GRE隧道，转发它们之间的二层以太报文。

 版权所有 © 华为技术有限公司

图 7-9 配置分支使用 5G 链路和总部建立 Ethernet over GRE 隧道互联组网图



数据准备

表 7-9 数据准备表

项目	数据	说明
运营商给分支分配的APN名称	5gnet	APN名称需提前从运营商处获取。
运营商给分支5G Cellular接口分配的IP地址	1.1.1.1/32	5G Cellular接口拨号接入运营商后，运营商给5G Cellular接口自动分配的IP地址。 **说明** 使用GRE隧道时，要求运营商给5G Cellular接口分配的IP地址为固定IP地址。本例中，假设运营商为5G Cellular接口分配的固定IP地址为1.1.1.1。
运营商给总部GE0/0/9接口分配的IP地址	2.2.2.2/24	总部AR2通过有线的方式接入Internet，该有线接口GE0/0/9采用静态方式获取IP地址。
运营商对接总部GE0/0/9接口的IP地址	2.2.2.1/24	运营商对接总部AR2 GE0/0/9接口的IP地址用于配置路由信息，使总部和Internet之间的路由互通。
分支AR1 LAN侧接口信息	LAN侧物理接口：GE0/0/1 绑定的VE接口：VE0/0/2 所属VLAN：10	分支和总部用户都在同一个网段，所属的VLAN都为VLAN 10。

版权所有 © 华为技术有限公司

项目	数据	说明
总部AR2 LAN侧接口信息	LAN侧物理接口：GE0/0/1 绑定的VE接口：VE0/0/2 所属VLAN：10	
分支AR1 Tunnel接口信息	IP地址：10.3.1.1/24 绑定的VE接口：VE0/0/1 所属VLAN：10	分支GRE隧道的地址。
总部AR2 Tunnel接口信息	IP地址：10.3.1.2/24 绑定的VE接口：VE0/0/1 所属VLAN：10	总部GRE隧道的地址。

MTU 及 TCP MSS 参数配置说明

为了减少网络传输中不必要的分片和重组，网络规划时需要合理设置终端发出的报文大小，设置依据如下：

- 对于UDP报文，可以调节发送端的MTU值，如果发送端不支持调节MTU值，则需要在5G AR设备上调节MTU值，以确保报文在网络中传输时不会产生二次分片。
- 对于TCP报文，可以配置5G AR设备的TCP MSS值，通过修改应用层报文数据包的长度来避免报文分片。

在5G 2B专线场景中，TCP MSS取值比较简单，在隧道两端AR设备的LAN侧接入物理口或VLANIF口上配置TCP MSS为推荐值1200。MTU取值相对复杂，与如下三个参数有关，具体的配置方法请参见**表2** 。

- 单层GRE隧道组网，报文经过5G AR设备后会增加28字节，即单层GRE头长度为28字节。
- 双层GRE隧道组网，报文经过5G AR设备后会增加56字节，即双层GRE头长度为56字节。
- 5G网络中GTP封装会增加至少40字节，其中IP头20字节，UDP头8字节，GTP消息封装12字节。考虑到GTP支持扩展消息头，建议多预留1至2个扩展消息头长度（4或8字节）作为缓冲，即GTP封装头长度最大为48字节。

 版权所有 © 华为技术有限公司

表 7-10 MTU 参数配置方法

组网场景	在发送端调节MTU方值	或者在5G AR上调节MTU值
单层GRE隧道组网	发送端MTU值=网络中设备允许通过MTU值减去单层GRE头长度28，再减去GTP封装头长度48，即发送端MTU值=MTU-28-48。	5G接口MTU值=网络中设备允许通过MTU值减去GTP封装头长度，即5G接口MTU值=MTU-48。本例中，MTU取值为1500。
双层GRE隧道组网	发送端MTU值=网络中设备允许通过MTU值减去双层GRE头长度56，再减去GTP封装头长度48，即发送端MTU值=MTU-56-48。	最外层L3 GRE隧道接口MTU值=网络中设备允许通过MTU值减去单层GRE头长度28，再减去GTP封装头长度48，即最外层L3 GRE隧道接口MTU值=MTU-28-48。

配置思路

1. 配置5G Cellular接口的连接参数，实现5G Cellular接口接入5G网络。
2. 配置Ethernet over GRE，创建VE接口。
3. 配置Tunnel接口，建立GRE隧道，使分支AR1及总部AR2之间可以通过GRE隧道直连。
4. 将二层VE接口绑定到WAN侧Tunnel接口和LAN侧物理接口，使企业分支和总部之间的以太报文可以通过GRE隧道传输。
5. 配置静态路由，使企业分支和总部子网的用户可以互通。

说明

在5G Cellular接口下执行命令**dialer enable-circular**配置轮询拨号功能时，设备会同时下发自动拨号、IP地址协商和5G Modem自愈的相关配置，无需再重复配置。

操作步骤

1. 配置5G Cellular接口的连接参数，实现5G Cellular接口接入5G网络。
   a. 创建APN模板。
   ```
   <Huawei> system-view
   [Huawei] sysname AR1
   [AR1] apn profile 5gprofile
   [AR1-apn-profile-5gprofile] apn 5gnet
   [AR1-apn-profile-5gprofile] quit
   ```
   b. 使能轮询DCC功能，配置自动拨号连接。
   ```
   [AR1] interface Cellular 1/0/0
   [AR1-Cellular1/0/0] dialer enable-circular
   [AR1-Cellular1/0/0] mtu 1452
   ```
   c. 在5G Cellular接口上绑定APN模板。
   ```
   [AR1-Cellular1/0/0] apn-profile 5gprofile
   Info: The configuration will become effective after link reset.
   [AR1-Cellular1/0/0] shutdown
   [AR1-Cellular1/0/0] undo shutdown
   [AR1-Cellular1/0/0] quit
   ```
2. 配置Ethernet over GRE，创建VE接口。
   a. 创建分支的二层VE接口VE0/0/1和VE0/0/2。
   ```
   [AR1] vlan 10
   [AR1-vlan10] quit
   ```

 版权所有 © 华为技术有限公司

```
[AR1] interface Virtual-Ethernet 0/0/1
[AR1-Virtual-Ethernet0/0/1] portswitch
Vlan Info: The operation may take a few seconds. Please wait for a moment...done
[AR1-Virtual-Ethernet0/0/1] port link-type access
[AR1-Virtual-Ethernet0/0/1] port default vlan 10
[AR1-Virtual-Ethernet0/0/1] quit
[AR1] interface Virtual-Ethernet 0/0/2
[AR1-Virtual-Ethernet0/0/2] portswitch
Vlan Info: The operation may take a few seconds. Please wait for a moment...done
[AR1-Virtual-Ethernet0/0/2] port link-type access
[AR1-Virtual-Ethernet0/0/2] port default vlan 10
[AR1-Virtual-Ethernet0/0/2] quit
```

b. 创建总部的二层VE接口VE0/0/1和VE0/0/2。

```
<Huawei> system-view
[Huawei] sysname AR2
[AR2] vlan 10
[AR2-vlan10] quit
[AR2] interface Virtual-Ethernet 0/0/1
[AR2-Virtual-Ethernet0/0/1] portswitch
Vlan Info: The operation may take a few seconds. Please wait for a moment...done
[AR2-Virtual-Ethernet0/0/1] port link-type access
[AR2-Virtual-Ethernet0/0/1] port default vlan 10
[AR2-Virtual-Ethernet0/0/1] quit
[AR2] interface Virtual-Ethernet 0/0/2
[AR2-Virtual-Ethernet0/0/2] portswitch
Vlan Info: The operation may take a few seconds. Please wait for a moment...done
[AR2-Virtual-Ethernet0/0/2] port link-type access
[AR2-Virtual-Ethernet0/0/2] port default vlan 10
[AR2-Virtual-Ethernet0/0/2] quit
```

3. 配置Tunnel接口，创建GRE隧道。

a. 配置总部WAN侧接口GE0/0/9的IP地址。

```
[AR2] interface GigabitEthernet 0/0/9
[AR2-GigabitEthernet0/0/9] ip address 2.2.2.2 24
[AR2-GigabitEthernet0/0/9] quit
```

b. 配置总部的Tunnel接口。

```
[AR2] interface Tunnel0/0/1
[AR2-Tunnel0/0/1] tunnel-protocol gre
Warning: After this tunnel encapsulation protocol was configured, the MTU and other
parameter settings of the tunnel were deleted.
[AR2-Tunnel0/0/1] ip address 10.3.1.2 255.255.255.0
[AR2-Tunnel0/0/1] source GigabitEthernet 0/0/9
[AR2-Tunnel0/0/1] destination 1.1.1.1
[AR2-Tunnel0/0/1] quit
```

c. 配置分支的Tunnel接口。

```
[AR1] interface Tunnel0/0/1
[AR1-Tunnel0/0/1] tunnel-protocol gre
Warning: After this tunnel encapsulation protocol was configured, the MTU and other
parameter settings of the tunnel were deleted.
[AR1-Tunnel0/0/1] ip address 10.3.1.1 255.255.255.0
[AR1-Tunnel0/0/1] source Cellular 1/0/0
[AR1-Tunnel0/0/1] destination 2.2.2.2
[AR1-Tunnel0/0/1] quit
```

4. 将二层VE接口绑定到WAN侧Tunnel接口和LAN侧物理接口。

a. 配置分支的VE0/0/1绑定到Tunnel0/0/1接口，VE0/0/2绑定到GE0/0/1接口。

```
[AR1] interface Tunnel0/0/1
[AR1-Tunnel0/0/1] map interface Virtual-Ethernet 0/0/1
[AR1-Tunnel0/0/1] quit
[AR1] interface GigabitEthernet 0/0/1
[AR1-GigabitEthernet0/0/1] undo portswitch  //GE0/0/1如果不是三层物理以太网接口，则需要执
行undo portswitch命令切换
[AR1-GigabitEthernet0/0/1] map interface Virtual-Ethernet 0/0/2
Warnning: The interface is being bound to Virtual-Ethernet.Other services are unavailable on
the interface.
[AR1-GigabitEthernet0/0/1] tcp adjust-mss 1200
[AR1-GigabitEthernet0/0/1] quit
```

 版权所有 © 华为技术有限公司

b. 配置总部的VE0/0/1绑定到Tunnel0/0/1接口，VE0/0/2绑定到GE0/0/1接口。

```
[AR2] interface Tunnel0/0/1
[AR2-Tunnel0/0/1] map interface Virtual-Ethernet 0/0/1
[AR2-Tunnel0/0/1] quit
[AR2] interface GigabitEthernet 0/0/1
[AR2-GigabitEthernet0/0/1] undo portswitch
[AR2-GigabitEthernet0/0/1] map interface Virtual-Ethernet 0/0/2
Warnning: The interface is being bound to Virtual-Ethernet.Other services are unavailable on the interface.
[AR2-GigabitEthernet0/0/1] tcp adjust-mss 1200
[AR2-GigabitEthernet0/0/1] quit
```

5. 配置静态路由，使企业分支和总部的内部主机HostA和HostB可以互通。

a. 配置分支的缺省路由，指定出接口为5G Cellular接口。

```
[AR1] ip route-static 0.0.0.0 0 Cellular 1/0/0
[AR1] quit
```

b. 配置总部的明细路由，指定下一跳地址为对端运营商接口的IP地址。

```
[AR2] ip route-static 1.1.1.1 255.255.255.255 2.2.2.1
[AR2] quit
```

验证

1. 在AR1上执行命令**display ip interface brief Cellular 1/0/0**，查看Cellular1/0/0接口获取到的IP地址。

```
<AR1> display ip interface brief Cellular 1/0/0
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
(E): E-Trunk down
Interface                   IP Address/Mask      Physical   Protocol

Cellular1/0/0               1.1.1.1/32           up         up
```

2. 在AR1上执行命令**display Cellular 1/0/0 all**，查看Cellular1/0/0接口的状态信息。

```
<AR1> display Cellular 1/0/0 all
Modem State:
Hardware Information.
=====================
Model = RG801
Modem Type = 5G module
Modem Firmware Version = RG801HEAAAR01A07M8G
Hardware Version = HiB5000_MODEM Ver.A
Integrate circuit card identity (ICCID) = 98610201000202000069
International Mobile Subscriber Identity (IMSI) = 460070075591996
Mobile Station International ISDN Number (MSISDN) = None
International Mobile Equipment Identity (IMEI) = 867147050004457
Factory Serial Number (FSN) = 0123456789ABCDEF
Modem Status = Online
Profile Information.
====================
Profile 1
--------
PDP Type = IPv4, Header Compression = OFF
Data Compression = OFF
Access Point Name (APN) = 5gnet
Packet Session Status = Active
* - Default profile
Network Information.
====================
Current Service Status = Service available
Service Domain = Combined
Current Service = PS
Packet Service = Attached
Packet Session Status = Active
Current Roaming Status = Roaming
```

 版权所有 © 华为技术有限公司

```
Network Selection Mode = Automatic
Network Connection Mode = LTE-NR
Current Network Connection = 5G(NSA)
Mobile Country Code (MCC) = 369
Mobile Network Code (MNC) = 77
Mobile Operator Information = Unknown
Tracking Area Code (TAC) = 1002
Cell ID = 9881858
Radio Information.
==================
Current Bands :
  WCDMA: AUTO
  LTE: B3
  NR: AUTO
LTE:
Current Band = B3
Current RSSI >= -51 dBm
Current RSRP = -71 dBm (strong)
Current RSRQ = -6 dB
Current SINR = 6 dB
NR:
Current Band = N78
Current RSRP = -65 dBm (strong)
Current RSRQ = -10 dB
Current SINR = 38 dB
Bands supported :
  WCDMA: WCDMA850 WCDMA900 WCDMA2100
  FDD LTE: B1 B3 B5 B7 B8 B20 B28
  TDD LTE: B34 B38 B39 B40 B41
  FDD NR: N1 N3 N28
  TDD NR: N41 N77 N78 N79
Modem Security Information.
===========================
SIM ID = 1
PIN Verification = Disabled
PIN Status = Ready
Number of Retries remaining = 3
SIM Status = OK
```

3. 在AR1上执行命令**ping -a 10.1.1.1 10.2.1.1**，模拟分支用户访问总部用户的流量，流量能Ping通。

```
<AR1> ping -a 10.1.1.1 10.2.1.1
  PING 10.2.1.1: 56  data bytes, press CTRL_C to break
    Reply from 10.2.1.1: bytes=56 Sequence=1 ttl=255 time=51 ms
    Reply from 10.2.1.1: bytes=56 Sequence=2 ttl=255 time=35 ms
    Reply from 10.2.1.1: bytes=56 Sequence=3 ttl=255 time=45 ms
    Reply from 10.2.1.1: bytes=56 Sequence=4 ttl=255 time=40 ms
    Reply from 10.2.1.1: bytes=56 Sequence=5 ttl=255 time=37 ms

  --- 10.2.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 35/41/51 ms
```

配置文件

AR1配置文件

```
#
 sysname AR1
#
vlan batch 10
#
interface GigabitEthernet0/0/1
 undo portswitch
 map interface Virtual-Ethernet0/0/2
 tcp adjust-mss 1200
#
interface Cellular1/0/0
```

 版权所有 © 华为技术有限公司

```
 dialer enable-circular
 apn-profile 5gprofile
 dialer timer autodial 10
 modem auto-recovery dial action modem-reboot fail-times 128
 modem auto-recovery icmp-unreachable action modem-reboot
 modem auto-recovery services-unavailable action modem-reboot test-times 0 interval 3600
 ip address negotiate
 mtu 1452
#
interface Virtual-Ethernet0/0/1
 portswitch
 port link-type access
 port default vlan 10
#
interface Virtual-Ethernet0/0/2
 portswitch
 port link-type access
 port default vlan 10
#
interface Tunnel0/0/1
 ip address 10.3.1.1 255.255.255.0
 tunnel-protocol gre
 source Cellular1/0/0
 destination 2.2.2.2
 map interface Virtual-Ethernet0/0/1
#
apn profile 5gprofile
 apn 5gnet
#
ip route-static 0.0.0.0 0.0.0.0 Cellular 1/0/0
#
return
```

AR2配置文件

```
#
 sysname AR2
#
vlan batch 10
#
interface GigabitEthernet0/0/1
 undo portswitch
 map interface Virtual-Ethernet0/0/2
 tcp adjust-mss 1200
#
interface GigabitEthernet0/0/9
 ip address 2.2.2.2 255.255.255.0
#
interface Virtual-Ethernet0/0/1
 portswitch
 port link-type access
 port default vlan 10
#
interface Virtual-Ethernet0/0/2
 portswitch
 port link-type access
 port default vlan 10
#
interface Tunnel0/0/1
 ip address 10.3.1.2 255.255.255.0
 tunnel-protocol gre
 source GigabitEthernet0/0/9
 destination 1.1.1.1
 map interface Virtual-Ethernet0/0/1
#
ip route-static 1.1.1.1 255.255.255.255 2.2.2.1
#
return
```

 版权所有 © 华为技术有限公司

7.2.7 配置双网关多发选收示例（5G CPE 场景）

组网需求

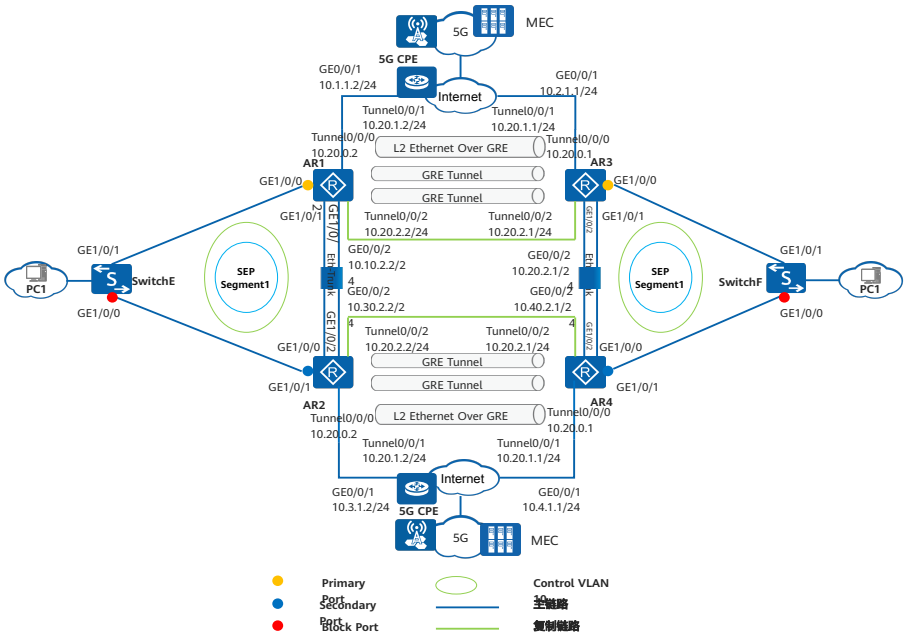
说明

AR设备配置多个GE子接口与5G CPE（N5368X）桥接模式对接时，由于CPE使用场景约束，AR设备需要使用子接口下的MAC地址修改功能保证CPE学习MAC地址的唯一性。

如图7-10所示，AR1和AR3之间的链路作为主链路进行业务传输，AR2和AR4之间的链路作为备链路进行业务传输，AR1和AR3之间、AR2和AR4之间通过Tunnel0/0/1接口和Tunnel0/0/2接口连接通信，在Tunnel0/0/1接口配置多发选收功能，将Tunnel0/0/1接口下的报文复制到Tunnel0/0/2接口发送出去，防止出现业务中断的现象。此外：

- 在接入层、汇聚层运行SEP协议，当环网上没有故障链路时，SEP能够消除以太网冗余环路。当环网上发生链路故障时，SEP能够迅速恢复环网上各节点间通信通路。
- 双设备之间存在报文复制后MAC地址漂移的问题和WAN侧环网的问题，因此配置VRRP备份且使用虚地址建立Tunnel0/0/0接口来传递以太报文。
- 配置AR1和AR3之间的BFD会话，检测WAN侧连通性，联动VRRP保证AR1和AR3的VRRP同步切换。
- 双设备之间使用Eth-Trunk连接，保证连接的可靠性，否则中间链路Down后，在非直连场景会造成VRRP双主，造成二层网络出现环路。

图 7-10 配置多发选收组网图



版权所有 © 华为技术有限公司

数据准备

表 7-11 数据准备表

项目	数据	说明
运营商给分支分配的APN名称	5gnet	APN名称需提前从运营商处获取。
分支AR1 接口信息	WAN侧物理接口：GE0/0/1，GE0/0/2 IP地址：10.1.1.2/24，10.10.2.2/24 LAN侧物理接口：GE1/0/0 互联接口：GE1/0/1，GE1/0/2	LAN侧物理接口所属VLAN为20和30；互联接口所属VLAN为20和30。30为以太数据转发VLAN，20为VRRP业务VLAN，10为SEP的控制VLAN。
分支AR2 接口信息	WAN侧物理接口：GE0/0/1，GE0/0/2 IP地址：10.3.1.2/24，10.30.2.2/24 LAN侧物理接口：GE1/0/0 互联接口：GE1/0/1，GE1/0/2	LAN侧物理接口所属VLAN为20和30；互联接口所属VLAN为20和30。30为以太数据转发VLAN，20为VRRP业务VLAN，10为SEP的控制VLAN。
分支AR3 接口信息	WAN侧物理接口：GE0/0/1，GE0/0/2 IP地址：10.2.1.1/24，10.20.2.1/24 LAN侧物理接口：GE1/0/0 互联接口：GE1/0/1，GE1/0/2	LAN侧物理接口所属VLAN为20和30；互联接口所属VLAN为20和30。30为以太数据转发VLAN，20为VRRP业务VLAN，10为SEP的控制VLAN。
分支AR4 接口信息	WAN侧物理接口：GE0/0/1，GE0/0/2 IP地址：10.4.1.1/24，10.40.2.1/24 LAN侧物理接口：GE1/0/0 互联接口：GE1/0/1，GE1/0/2	LAN侧物理接口所属VLAN为20和30；互联接口所属VLAN为20和30。30为以太数据转发VLAN，20为VRRP业务VLAN，10为SEP的控制VLAN。

 版权所有 © 华为技术有限公司

项目	数据	说明
分支AR1 Tunnel接口的IP地址	外层隧道： Tunnel0/0/1：10.20.1.2/24 Tunnel0/0/2：10.20.2.2/24 内层隧道： Tunnel0/0/0：10.20.0.2	分支隧道的信息。
分支AR2 Tunnel接口的IP地址	外层隧道： Tunnel0/0/1：10.20.1.2/24 Tunnel0/0/2：10.20.2.2/24 内层隧道： Tunnel0/0/0：10.20.0.2	分支隧道的信息。
分支AR3 Tunnel接口的IP地址	外层隧道： Tunnel0/0/1：10.20.1.1/24 Tunnel0/0/2：10.20.2.1/24 内层隧道： Tunnel0/0/0：10.20.0.1	分支隧道的信息。
分支AR4 Tunnel接口的IP地址	外层隧道： Tunnel0/0/1：10.20.1.1/24 Tunnel0/0/2：10.20.2.1/24 内层隧道： Tunnel0/0/0：10.20.0.1	分支隧道的信息。

MTU 及 TCP MSS 参数配置说明

为了减少网络传输中不必要的分片和重组，网络规划时需要合理设置终端发出的报文大小，设置依据如下：

- 对于UDP报文，可以调节发送端的MTU值，如果发送端不支持调节MTU值，则需要在5G AR设备上调节MTU值，以确保报文在网络中传输时不会产生二次分片。
- 对于TCP报文，可以配置5G AR设备的TCP MSS值，通过修改应用层报文数据包的长度来避免报文分片。

在5G2B专线场景中，TCP MSS取值比较简单，在隧道两端AR设备的LAN侧接入物理口或VLANIF口上配置TCP MSS为推荐值1200。MTU取值相对复杂，与如下三个参数有关，具体的配置方法请参见**表2** 。

- 单层GRE隧道组网，报文经过5G AR设备后会增加28字节，即单层GRE头长度为28字节。

 版权所有 © 华为技术有限公司

- 双层GRE隧道组网，报文经过5G AR设备后会增加56字节，即双层GRE头长度为56字节。
- 5G网络中GTP封装会增加至少40字节，其中IP头20字节，UDP头8字节，GTP消息封装12字节。考虑到GTP支持扩展消息头，建议多预留1至2个扩展消息头长度（4或8字节）作为缓冲，即GTP封装头长度最大为48字节。

表 7-12 MTU 参数配置方法

组网场景	在发送端调节MTU方值	或者在5G AR上调节MTU值
单层GRE隧道组网	发送端MTU值=网络中设备允许通过MTU值减去单层GRE头长度28，再减去GTP封装头长度48，即发送端MTU值=MTU-28-48。	5G接口MTU值=网络中设备允许通过MTU值减去GTP封装头长度，即5G接口MTU值=MTU-48。
双层GRE隧道组网	发送端MTU值=网络中设备允许通过MTU值减去双层GRE头长度56，再减去GTP封装头长度48，即发送端MTU值=MTU-56-48。	最外层L3 GRE隧道接口MTU值=网络中设备允许通过MTU值减去单层GRE头长度28，再减去GTP封装头长度48，即最外层L3 GRE隧道接口MTU值=MTU-28-48。本例中，MTU取值为1500。

配置思路

本例配置主要思路是：

1. 在二层网络上配置SEP协议。
2. 配置设备间的网络互连。
3. 配置VRRP主备备份。
4. 配置BFD会话，实现设备间链路故障的快速检测。
5. 配置双设备之间使用Eth-Trunk连接。
6. 配置Tunnel接口并配置多发选收功能，将Tunnel0/0/1接口下的报文复制到Tunnel0/0/2接口。
7. 配置静态路由。

操作步骤

1. 在二层网络上配置SEP协议。

   # 配置AR1。

```
<Huawei> system-view
[Huawei] sysname AR1
[AR1] vlan batch 20 30
[AR1] sep segment 1
[AR1-sep-segment1] control-vlan 10
[AR1-sep-segment1] protected-instance all
[AR1-sep-segment1] quit
[AR1] interface gigabitethernet 1/0/0
[AR1-GigabitEthernet1/0/0] port hybrid tagged vlan 10 20 30
[AR1-GigabitEthernet1/0/0] stp disable
[AR1-GigabitEthernet1/0/0] sep segment 1 edge primary
[AR1-GigabitEthernet1/0/0] quit
```

 版权所有 © 华为技术有限公司

配置AR2。

```
<Huawei> system-view
[Huawei] sysname AR2
[AR2] vlan batch 20 30
[AR2] sep segment 1
[AR2-sep-segment1] control-vlan 10
[AR2-sep-segment1] protected-instance all
[AR2-sep-segment1] quit
[AR2] interface gigabitethernet 1/0/1
[AR2-GigabitEthernet1/0/1] port hybrid tagged vlan 10 20 30
[AR2-GigabitEthernet1/0/1] stp disable
[AR2-GigabitEthernet1/0/1] sep segment 1 edge secondary
[AR2-GigabitEthernet1/0/1] quit
```

配置SwitchE。

```
<Huawei> system-view
[Huawei] sysname SwitchE
[SwitchE] vlan batch 20 30
[SwitchE] sep segment 1
[SwitchE-sep-segment1] control-vlan 10
[SwitchE-sep-segment1] protected-instance all
[SwitchE-sep-segment1] quit
[SwitchE] interface gigabitethernet 1/0/0
[SwitchE-GigabitEthernet1/0/0] port hybrid tagged vlan 10 20 30
[SwitchE-GigabitEthernet1/0/0] stp disable
[SwitchE-GigabitEthernet1/0/0] sep segment 1 priority 128
[SwitchE-GigabitEthernet1/0/0] quit
[SwitchE] interface gigabitethernet 1/0/1
[SwitchE-GigabitEthernet1/0/1] port hybrid tagged vlan 10 20 30
[SwitchE-GigabitEthernet1/0/1] stp disable
[SwitchE-GigabitEthernet1/0/1] sep segment 1
[SwitchE-GigabitEthernet1/0/1] quit
```

配置AR3、AR4和SwitchF。

AR3与AR1的配置相同，AR4与AR2的配置相同，SwitchF与SwitchE的配置相同。具体配置过程略。请参见本示例的**配置文件**。

2. 配置设备间的网络互连。

配置AR1。

```
[AR1] interface Virtual-Ethernet 0/0/0
[AR1-Virtual-Ethernet0/0/0] portswitch
[AR1-Virtual-Ethernet0/0/0] port link-type access
[AR1-Virtual-Ethernet0/0/0] port default vlan 30
[AR1-Virtual-Ethernet0/0/0] quit
[AR1] interface Virtual-Ethernet 0/0/1
[AR1-Virtual-Ethernet0/0/1] portswitch
[AR1-Virtual-Ethernet0/0/1] port link-type trunk
[AR1-Virtual-Ethernet0/0/1] port trunk allow-pass vlan 30
[AR1-Virtual-Ethernet0/0/1] quit
[AR1] interface gigabitethernet 0/0/1
[AR1-GigabitEthernet0/0/1] ip address 10.1.1.2 255.255.255.0
[AR1-GigabitEthernet0/0/1] quit
[AR1] interface gigabitethernet 0/0/2
[AR1-GigabitEthernet0/0/2] ip address 10.10.2.2 255.255.255.0
[AR1-GigabitEthernet0/0/2] quit
[AR1] interface vlanif 30
[AR1-Vlanif30] tcp adjust-mss 1200
[AR1-Vlanif30] map interface Virtual-Ethernet0/0/0
[AR1-Vlanif30] quit
```

配置AR3。

```
[AR3] interface Virtual-Ethernet 0/0/0
[AR3-Virtual-Ethernet0/0/0] portswitch
[AR3-Virtual-Ethernet0/0/0] port link-type access
[AR3-Virtual-Ethernet0/0/0] port default vlan 30
[AR3-Virtual-Ethernet0/0/0] quit
[AR3] interface Virtual-Ethernet 0/0/1
```

 版权所有 © 华为技术有限公司

```
[AR3-Virtual-Ethernet0/0/1] portswitch
[AR3-Virtual-Ethernet0/0/1] port link-type trunk
[AR3-Virtual-Ethernet0/0/1] port trunk allow-pass vlan 30
[AR3-Virtual-Ethernet0/0/1] quit
[AR3] interface gigabitethernet 0/0/1
[AR3-GigabitEthernet0/0/1] ip address 10.2.1.1 255.255.255.0
[AR3-GigabitEthernet0/0/1] quit
[AR3] interface gigabitethernet 0/0/2
[AR3-GigabitEthernet0/0/2] ip address 10.20.2.1 255.255.255.0
[AR3-GigabitEthernet0/0/2] quit
[AR3] interface vlanif 30
[AR3-Vlanif30] tcp adjust-mss 1200
[AR3-Vlanif30] map interface Virtual-Ethernet0/0/0
[AR3-Vlanif30] quit
```

配置AR2和AR4。

AR2与AR1的配置相同，AR4与AR3的配置相同。

具体配置过程略。请参见本示例的**配置文件**。

3. 配置VRRP主备备份。

在AR1上创建VRRP备份组1，配置AR1在该备份组中的优先级为120。

```
[AR1] interface vlanif 20
[AR1-Vlanif20] ip address 172.16.1.1 255.255.255.0
[AR1-Vlanif20] vrrp vrid 1 virtual-ip 172.16.1.100
[AR1-Vlanif20] vrrp vrid 1 priority 120
[AR1-Vlanif20] vrrp vrid 1 track bfd-session 3 reduced 15
[AR1-Vlanif20] vrrp vrid 1 track bfd-session 5 reduced 15
[AR1-Vlanif20] quit
[AR1] interface tunnel 0/0/0
[AR1-Tunnel0/0/0] tunnel-protocol gre
[AR1-Tunnel0/0/0] ip address 10.20.0.2 255.255.255.0
[AR1-Tunnel0/0/0] source 172.16.1.100
[AR1-Tunnel0/0/0] destination 172.17.1.100
[AR1-Tunnel0/0/0] map interface Virtual-Ethernet0/0/1
[AR1-Tunnel0/0/0] quit
```

在AR2上创建VRRP备份组1，其在该备份组中的优先级为缺省值100。

```
[AR2] interface vlanif 20
[AR2-Vlanif20] ip address 172.16.1.2 255.255.255.0
[AR2-Vlanif20] vrrp vrid 1 virtual-ip 172.16.1.100
[AR2-Vlanif20] quit
[AR2] interface tunnel 0/0/0
[AR2-Tunnel0/0/0] tunnel-protocol gre
[AR2-Tunnel0/0/0] ip address 10.20.0.2 255.255.255.0
[AR2-Tunnel0/0/0] source 172.16.1.100
[AR2-Tunnel0/0/0] destination 172.17.1.100
[AR2-Tunnel0/0/0] map interface Virtual-Ethernet0/0/1
[AR2-Tunnel0/0/0] quit
```

在AR3上创建VRRP备份组1，配置AR3在该备份组中的优先级为120。

```
[AR3] interface vlanif 20
[AR3-Vlanif20] ip address 172.17.1.1 255.255.255.0
[AR3-Vlanif20] vrrp vrid 1 virtual-ip 172.17.1.100
[AR3-Vlanif20] vrrp vrid 1 priority 120
[AR3-Vlanif20] vrrp vrid 1 track bfd-session 4 reduced 15
[AR3-Vlanif20] vrrp vrid 1 track bfd-session 6 reduced 15
[AR3-Vlanif20] quit
[AR3] interface tunnel 0/0/0
[AR3-Tunnel0/0/0] tunnel-protocol gre
[AR3-Tunnel0/0/0] ip address 10.20.0.1 255.255.255.0
[AR3-Tunnel0/0/0] source 172.17.1.100
[AR3-Tunnel0/0/0] destination 172.16.1.100
[AR3-Tunnel0/0/0] map interface Virtual-Ethernet0/0/1
[AR3-Tunnel0/0/0] quit
```

在AR4上创建VRRP备份组1，其在该备份组中的优先级为缺省值100。

```
[AR4] interface vlanif 20
[AR4-Vlanif20] ip address 172.17.1.2 255.255.255.0
```

 版权所有 © 华为技术有限公司

```
[AR4-Vlanif20] vrrp vrid 1 virtual-ip 172.17.1.100
[AR4-Vlanif20] quit
[AR4] interface tunnel 0/0/0
[AR4-Tunnel0/0/0] tunnel-protocol gre
[AR4-Tunnel0/0/0] ip address 10.20.0.1 255.255.255.0
[AR4-Tunnel0/0/0] source 172.17.1.100
[AR4-Tunnel0/0/0] destination 172.16.1.100
[AR4-Tunnel0/0/0] map interface Virtual-Ethernet0/0/1
[AR4-Tunnel0/0/0] quit
```

4. 配置BFD会话，实现设备间链路故障的快速检测。

   # 配置AR1。

   ```
   [AR1] bfd
   [AR1-bfd] quit
   [AR1] bfd tunnel1 bind peer-ip 10.20.1.1 source-ip 10.20.1.2
   [AR1-bfd-session-atob] discriminator local 3
   [AR1-bfd-session-atob] discriminator remote 4
   [AR1-bfd-session-atob] commit
   [AR1-bfd-session-atob] quit
   [AR1] bfd tunnel2 bind peer-ip 10.20.2.1 source-ip 10.20.2.1
   [AR1-bfd-session-atob] discriminator local 5
   [AR1-bfd-session-atob] discriminator remote 6
   [AR1-bfd-session-atob] commit
   [AR1-bfd-session-atob] quit
   ```

   # 配置AR3。

   ```
   [AR3] bfd
   [AR3-bfd] quit
   [AR3] bfd tunnel1 bind peer-ip 10.20.1.2 source-ip 10.20.1.1
   [AR3-bfd-session-atob] discriminator local 4
   [AR3-bfd-session-atob] discriminator remote 3
   [AR3-bfd-session-atob] commit
   [AR3-bfd-session-atob] quit
   [AR3] bfd tunnel2 bind peer-ip 10.20.2.1 source-ip 10.20.2.1
   [AR3-bfd-session-atob] discriminator local 6
   [AR3-bfd-session-atob] discriminator remote 5
   [AR3-bfd-session-atob] commit
   [AR3-bfd-session-atob] quit
   ```

5. 配置双设备之间使用Eth-Trunk连接。

   # 配置AR1。

   ```
   [AR1] interface GigabitEthernet 1/0/1
   [AR1-GigabitEthernet1/0/1] Eth-Trunk 1
   [AR1-GigabitEthernet1/0/1] quit
   [AR1] interface GigabitEthernet 1/0/2
   [AR1-GigabitEthernet1/0/2] Eth-Trunk 1
   [AR1-GigabitEthernet1/0/2] quit
   [AR1] interface Eth-Trunk1
   [AR1-Eth-Trunk1] port hybrid tagged vlan 10 20 30
   [AR1-Eth-Trunk1] stp disable
   [AR1-Eth-Trunk1] sep segment 1
   [AR1-Eth-Trunk1] quit
   ```

   # 配置AR2。

   ```
   [AR2] interface GigabitEthernet 1/0/0
   [AR2-GigabitEthernet1/0/1] Eth-Trunk 1
   [AR2-GigabitEthernet1/0/1] quit
   [AR2] interface GigabitEthernet 1/0/2
   [AR2-GigabitEthernet1/0/2] Eth-Trunk 1
   [AR2-GigabitEthernet1/0/2] quit
   [AR2] interface Eth-Trunk1
   [AR2-Eth-Trunk1] port hybrid tagged vlan 10 20 30
   [AR2-Eth-Trunk1] stp disable
   [AR2-Eth-Trunk1] sep segment 1
   [AR2-Eth-Trunk1] quit
   ```

   # 配置AR3和AR4。

   AR3与AR1的配置相同，AR4与AR2的配置相同。

 版权所有 © 华为技术有限公司

具体配置过程略。请参见本示例的**配置文件**。

6. 配置Tunnel接口并配置多发选收功能，将Tunnel0/0/1接口下的报文复制到Tunnel0/0/2接口。

   # 配置AR1。

```
[AR1] interface tunnel 0/0/1
[AR1-Tunnel0/0/1] tunnel-protocol gre
[AR1-Tunnel0/0/1] ip address 10.20.1.2 255.255.255.0
[AR1-Tunnel0/0/1] source 10.1.1.2
[AR1-Tunnel0/0/1] destination 10.2.1.1
[AR1-Tunnel0/0/1] mtu 1424
[AR1-Tunnel0/0/1] quit
[AR1] interface tunnel 0/0/2
[AR1-Tunnel0/0/2] tunnel-protocol gre
[AR1-Tunnel0/0/2] ip address 10.20.2.2 255.255.255.0
[AR1-Tunnel0/0/2] source 10.10.2.2
[AR1-Tunnel0/0/2] destination 10.20.2.1
[AR1-Tunnel0/0/2] quit
[AR1] replication path-group g1
[AR1-replication-path-group-g1] path Tunnel 0/0/2 priority 1
[AR1-replication-path-group-g1] quit
[AR1] interface tunnel 0/0/1
[AR1-Tunnel0/0/1] replication path-group g1
[AR1-Tunnel0/0/1] quit
```

   # 配置AR3。

```
[AR3] interface tunnel 0/0/1
[AR3-Tunnel0/0/1] tunnel-protocol gre
[AR3-Tunnel0/0/1] ip address 10.20.1.1 255.255.255.0
[AR3-Tunnel0/0/1] source 10.2.1.1
[AR3-Tunnel0/0/1] destination 10.1.1.2
[AR3-Tunnel0/0/1] mtu 1424
[AR3-Tunnel0/0/1] quit
[AR3] interface tunnel 0/0/2
[AR3-Tunnel0/0/2] tunnel-protocol gre
[AR3-Tunnel0/0/2] ip address 10.20.2.1 255.255.255.0
[AR3-Tunnel0/0/2] source 10.20.2.1
[AR3-Tunnel0/0/2] destination 10.10.2.2
[AR3-Tunnel0/0/2] quit
[AR3] replication path-group g1
[AR3-replication-path-group-g1] path Tunnel 0/0/2 priority 1
[AR3-replication-path-group-g1] quit
[AR3] interface tunnel 0/0/1
[AR3-Tunnel0/0/1] replication path-group g1
[AR3-Tunnel0/0/1] quit
```

   # 配置AR2和AR4。

   AR2与AR1的配置相同，AR4与AR3的配置相同。

   具体配置过程略。请参见本示例的**配置文件**。

7. 配置静态路由。

   # 配置AR1。

```
[AR1] ip route-static 172.17.1.0 255.255.255.0 Tunnel 0/0/1
[AR1] ip route-static 172.17.1.0 255.255.255.0 Tunnel 0/0/2 preference 100
[AR1] ip route-static 10.2.1.0 255.255.255.0 10.1.1.1
[AR1] ip route-static 10.20.2.0 255.255.255.0 10.10.2.1
```

   # 配置AR3。

```
[AR3] ip route-static 172.16.1.0 255.255.255.0 Tunnel 0/0/1
[AR3] ip route-static 172.16.1.0 255.255.255.0 Tunnel 0/0/2 preference 100
[AR3] ip route-static 10.1.1.0 255.255.255.0 10.2.1.2
[AR3] ip route-static 10.10.2.0 255.255.255.0 10.20.2.2
```

   # 配置AR2和AR4。

   AR2与AR1的配置相同，AR4与AR3的配置相同。

 版权所有 © 华为技术有限公司

具体配置过程略。请参见本示例的**配置文件**。

配置文件

- AR1的配置文件

```
#
vlan batch 20 30
sep segment 1
 control-vlan 10
 protected-instance all
#
interface GigabitEthernet1/0/1
 Eth-Trunk 1
#
interface GigabitEthernet1/0/2
 Eth-Trunk 1
#
interface Eth-Trunk1
 port hybrid tagged vlan 10 20 30
 stp disable
 sep segment 1
#
interface GigabitEthernet1/0/0
 port hybrid tagged vlan 10 20 30
 stp disable
 sep segment 1 edge primary
#
interface Virtual-Ethernet0/0/0
 portswitch
 port link-type access
 port default vlan 30
#
interface Virtual-Ethernet0/0/1
 portswitch
 port link-type trunk
 port trunk allow-pass vlan 30
#
interface GigabitEthernet0/0/1
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet0/0/2
 ip address 10.10.2.2 255.255.255.0
#
interface Tunnel0/0/0
 ip address 10.20.0.2 255.255.255.0
 tunnel-protocol gre
 source 172.16.1.100
 destination 172.17.1.100
 map interface Virtual-Ethernet0/0/1
#
interface Tunnel0/0/1
 ip address 10.20.1.2 255.255.255.0
 tunnel-protocol gre
 source 10.1.1.2
 destination 10.2.1.1
 mtu 1424
 replication path-group g1
#
interface Tunnel0/0/2
 ip address 10.20.2.2 255.255.255.0
 tunnel-protocol gre
 source 10.10.2.2
 destination 10.20.2.1
 mtu 1424
#
interface Vlanif20
 ip address 172.16.1.1 255.255.255.0
 vrrp vrid 1 virtual-ip 172.16.1.100
 vrrp vrid 1 priority 120
```

 版权所有 © 华为技术有限公司

```
 vrrp vrid 1 track bfd-session 3 reduced 15
 vrrp vrid 1 track bfd-session 5 reduced 15
#
interface vlanif 30
 tcp adjust-mss 1200
 map interface Virtual-Ethernet0/0/0
#
ip route-static 172.17.1.0 255.255.255.0 Tunnel0/0/1
ip route-static 172.17.1.0 255.255.255.0 Tunnel0/0/2 preference 100
ip route-static 10.2.1.0 255.255.255.0 10.1.1.1
ip route-static 10.20.2.0 255.255.255.0 10.10.2.1
#
replication path-group g1
 path Tunnel0/0/2 priority 1
#
bfd tunnel1 bind peer-ip 10.20.1.1 source-ip 10.20.1.2
 discriminator local 3
 discriminator remote 4
 commit
bfd tunnel2 bind peer-ip 10.20.2.1 source-ip 10.20.2.2
 discriminator local 5
 discriminator remote 6
 commit
#
return
```

- AR2的配置文件

```
#
vlan batch 20 30
sep segment 1
 control-vlan 10
 protected-instance all
#
interface GigabitEthernet1/0/0
 Eth-Trunk 1
#
interface GigabitEthernet1/0/2
 Eth-Trunk 1
#
interface Eth-Trunk1
 port hybrid tagged vlan 10 20 30
 stp disable
 sep segment 1
#
interface GigabitEthernet1/0/1
 port hybrid tagged vlan 10 20 30
 stp disable
 sep segment 1 edge secondary
#
interface Virtual-Ethernet0/0/0
 portswitch
 port link-type access
 port default vlan 30
#
interface Virtual-Ethernet0/0/1
 portswitch
 port link-type trunk
 port trunk allow-pass vlan 30
#
interface GigabitEthernet0/0/1
 ip address 10.3.1.2 255.255.255.0
#
interface GigabitEthernet0/0/2
 ip address 10.30.2.2 255.255.255.0
#
interface Tunnel0/0/0
 ip address 10.20.0.2 255.255.255.0
 tunnel-protocol gre
 source 172.16.1.100
 destination 172.17.1.100
```

 版权所有 © 华为技术有限公司

```
 map interface Virtual-Ethernet0/0/1
#
interface Tunnel0/0/1
 ip address 10.20.1.2 255.255.255.0
 tunnel-protocol gre
 source 10.3.1.2
 destination 10.4.1.1
 mtu 1424
 replication path-group g1
#
interface Tunnel0/0/2
 ip address 10.20.2.2 255.255.255.0
 tunnel-protocol gre
 source 10.30.2.2
 destination 10.40.2.1
 mtu 1424
#
interface Vlanif20
 ip address 172.16.1.2 255.255.255.0
 vrrp vrid 1 virtual-ip 172.16.1.100
#
interface vlanif 30
 tcp adjust-mss 1200
 map interface Virtual-Ethernet0/0/0
#
ip route-static 172.16.1.0 255.255.255.0 Tunnel0/0/1
ip route-static 172.16.1.0 255.255.255.0 Tunnel0/0/2 preference 100
ip route-static 10.4.1.0 255.255.255.0 10.3.1.1
ip route-static 10.40.2.0 255.255.255.0 10.30.2.1
#
replication path-group g1
 path Tunnel0/0/2 priority 1
#
return
```

- AR3的配置文件

```
#
vlan batch 20 30
sep segment 1
 control-vlan 10
 protected-instance all
#
interface GigabitEthernet1/0/0
 Eth-Trunk 1
#
interface GigabitEthernet1/0/2
 Eth-Trunk 1
#
interface Eth-Trunk1
 port hybrid tagged vlan 10 20 30
 stp disable
 sep segment 1
#
interface GigabitEthernet1/0/0
 port hybrid tagged vlan 10 20 30
 stp disable
 sep segment 1 edge primary
#
interface Virtual-Ethernet0/0/0
 portswitch
 port link-type access
 port default vlan 30
#
interface Virtual-Ethernet0/0/1
 portswitch
 port link-type trunk
 port trunk allow-pass vlan 30
#
interface GigabitEthernet0/0/1
 ip address 10.2.1.1 255.255.255.0
```

 版权所有 © 华为技术有限公司

```
#
interface GigabitEthernet0/0/2
 ip address 10.20.2.1 255.255.255.0
#
interface Tunnel0/0/0
 ip address 10.20.0.1 255.255.255.0
 tunnel-protocol gre
 source 172.17.1.100
 destination 172.16.1.100
 map interface Virtual-Ethernet0/0/1
#
interface Tunnel0/0/1
 ip address 10.20.1.1 255.255.255.0
 tunnel-protocol gre
 source 10.2.1.1
 destination 10.1.1.2
 mtu 1424
 replication path-group g1
#
interface Tunnel0/0/2
 ip address 10.20.2.1 255.255.255.0
 tunnel-protocol gre
 source 10.20.2.1
 destination 10.10.2.2
 mtu 1424
#
interface Vlanif20
 ip address 172.17.1.1 255.255.255.0
 vrrp vrid 1 virtual-ip 172.17.1.100
 vrrp vrid 1 priority 120
 vrrp vrid 1 track bfd-session 4 reduced 15
 vrrp vrid 1 track bfd-session 6 reduced 15

#
interface vlanif 30
 tcp adjust-mss 1200
 map interface Virtual-Ethernet0/0/0
#
ip route-static 172.16.1.0 255.255.255.0 Tunnel0/0/1
ip route-static 172.16.1.0 255.255.255.0 Tunnel0/0/2 preference 100
ip route-static 10.1.1.0 255.255.255.0 10.2.1.2
ip route-static 10.10.2.0 255.255.255.0 10.20.2.2
#
replication path-group g1
 path Tunnel0/0/2 priority 1
#
bfd tunnel1 bind peer-ip 10.20.1.2 source-ip 10.20.1.1
 discriminator local 4
 discriminator remote 3
 commit
bfd tunnel2 bind peer-ip 10.20.2.2 source-ip 10.20.2.1
 discriminator local 6
 discriminator remote 5
 commit
#
return
```

- AR4的配置文件

```
#
vlan batch 20 30
sep segment 1
 control-vlan 10
 protected-instance all
#
interface GigabitEthernet1/0/0
 Eth-Trunk 1
#
interface GigabitEthernet1/0/2
 Eth-Trunk 1
#
```

 版权所有 © 华为技术有限公司

```
interface Eth-Trunk1
 port hybrid tagged vlan 10 20 30
 stp disable
 sep segment 1
#
interface GigabitEthernet1/0/1
 port hybrid tagged vlan 10 20 30
 stp disable
 sep segment 1 edge secondary
#
interface Virtual-Ethernet0/0/0
 portswitch
 port link-type access
 port default vlan 30
#
interface Virtual-Ethernet0/0/1
 portswitch
 port link-type trunk
 port trunk allow-pass vlan 30
#
interface GigabitEthernet0/0/1
 ip address 10.4.1.1 255.255.255.0
#
interface GigabitEthernet0/0/2
 ip address 10.40.2.1 255.255.255.0
#
interface Tunnel0/0/0
 ip address 10.20.0.1 255.255.255.0
 tunnel-protocol gre
 source 172.17.1.100
 destination 172.16.1.100
 map interface Virtual-Ethernet0/0/1
#
interface Tunnel0/0/1
 ip address 10.20.1.1 255.255.255.0
 tunnel-protocol gre
 source 10.4.1.1
 destination 10.3.1.2
 mtu 1424
 replication path-group g1
#
interface Tunnel0/0/2
 ip address 10.20.2.1 255.255.255.0
 tunnel-protocol gre
 source 10.40.2.1
 destination 10.30.2.2
 mtu 1424
#
interface Vlanif20
 ip address 172.17.1.2 255.255.255.0
 vrrp vrid 1 virtual-ip 172.17.1.100
#
interface vlanif 30
 tcp adjust-mss 1200
 map interface Virtual-Ethernet0/0/0
#
ip route-static 172.16.1.0 255.255.255.0 Tunnel0/0/1
ip route-static 172.16.1.0 255.255.255.0 Tunnel0/0/2 preference 100
ip route-static 10.3.1.0 255.255.255.0 10.4.1.2
ip route-static 10.30.2.0 255.255.255.0 10.40.2.2
#
replication path-group g1
 path Tunnel0/0/2 priority 1
#
return
```

- SwitchE的配置文件

```
#
vlan batch 20 30
sep segment 1
```

 版权所有 © 华为技术有限公司

```
 control-vlan 10
 protected-instance all
#
interface GigabitEthernet1/0/0
 port hybrid tagged vlan 10 20 30
 stp disable
 sep segment 1 priority 128
#
interface GigabitEthernet1/0/1
 port hybrid tagged vlan 10 20 30
 stp disable
 sep segment 1
#
return
```

- SwitchF的配置文件

```
#
vlan batch 20 30
sep segment 1
 control-vlan 10
 protected-instance all
#
interface GigabitEthernet1/0/0
 port hybrid tagged vlan 10 20 30
 stp disable
 sep segment 1 priority 128
#
interface GigabitEthernet1/0/1
 port hybrid tagged vlan 10 20 30
 stp disable
 sep segment 1
#
return
```

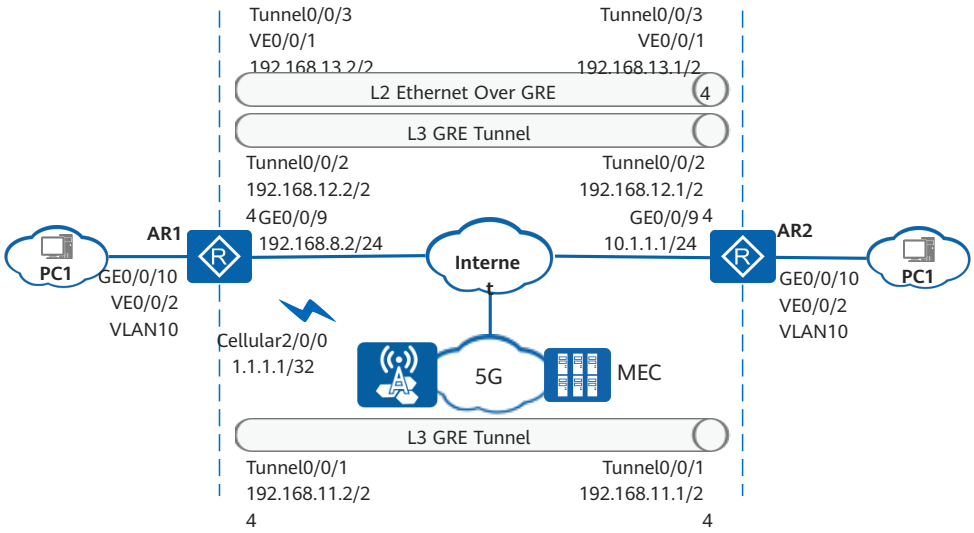
7.2.8 配置 5G 场景二层多发选收示例

组网需求

如图7-11所示，AR1和AR2之间通过Internet网络互通，为了提高链路可靠性，AR1部署了两条上行链路接入Internet。其中5G链路作为主链路，以太有线链路作为备链路。用户希望将5G链路的报文复制到以太链路发送出去，防止出现业务中断的现象。并且分支和总部可以传输原始以太报文（如工业控制的PLC报文），采用二层隧道封装。

 版权所有 © 华为技术有限公司

图 7-11 配置 5G 场景二层多发选收组网图



数据准备

表 7-13 数据准备表

项目	数据	说明
分支AR1 LAN侧接口信息	LAN侧物理接口：GE0/0/10 绑定的VE接口：VE0/0/2 所属VLAN：10	分支AR1与分支用户之间的链路信息。
分支AR1 WAN侧接口信息	主链路5G Cellular接口：Cellular2/0/0 IP地址：1.1.1.1/32 绑定VPN实例：vpn1 备链路物理接口：GE0/0/9 IP地址：192.168.8.2/24 绑定VPN实例：vpn2	分支AR1和总部AR2之间的链路信息。
分支AR1 Tunnel0/0/1接口信息	IP地址：192.168.11.2/24 源接口：Cellular2/0/0	分支AR1和总部AR2之间的L3 GRE隧道信息。
分支AR1 Tunnel0/0/2接口信息	IP地址：192.168.12.2/24 源接口：GE0/0/9	分支AR1和总部AR2之间的L3 GRE隧道信息。
分支AR1 Tunnel0/0/3接口信息	IP地址：192.168.13.2/24 源接口：LoopBack1 绑定的VE接口：VE0/0/1	分支AR1和总部AR2之间的Ethernet over GRE隧道信息。

版权所有 © 华为技术有限公司

项目	数据	说明
总部AR2 LAN侧接口信息	LAN侧物理接口：GE0/0/10 绑定的VE接口：VE0/0/2 所属VLAN：10	总部AR2与总部用户之间的链路信息。
总部AR2 WAN侧接口信息	WAN侧物理接口：GE0/0/9 IP地址：10.1.1.1/24	总部AR2与分支AR1之间的链路信息。
总部AR2 Tunnel0/0/1接口信息	IP地址：192.168.11.1/24 源接口：GE0/0/9	总部AR2和分支AR1之间的L3 GRE隧道信息。
总部AR2 Tunnel0/0/2接口信息	IP地址：192.168.12.1/24 源接口：GE0/0/9	总部AR2和分支AR1之间的L3 GRE隧道信息。
总部AR2 Tunnel0/0/3接口信息	IP地址：192.168.13.1/24 源接口：LoopBack1 绑定的VE接口：VE0/0/1	总部AR2和分支AR1之间的Ethernet over GRE隧道信息。

MTU 及 TCP MSS 参数配置说明

为了减少网络传输中不必要的分片和重组，网络规划时需要合理设置终端发出的报文大小，设置依据如下：

- 对于UDP报文，可以调节发送端的MTU值，如果发送端不支持调节MTU值，则需要在5G AR设备上调节MTU值，以确保报文在网络中传输时不会产生二次分片。
- 对于TCP报文，可以配置5G AR设备的TCP MSS值，通过修改应用层报文数据包的长度来避免报文分片。

在5G2B专线场景中，TCP MSS取值比较简单，在隧道两端AR设备的LAN侧接入物理口或VLANIF口上配置TCP MSS为推荐值1200。MTU取值相对复杂，与如下三个参数有关，具体的配置方法请参见**表2** 。

- 单层GRE隧道组网，报文经过5G AR设备后会增加28字节，即单层GRE头长度为28字节。
- 双层GRE隧道组网，报文经过5G AR设备后会增加56字节，即双层GRE头长度为56字节。
- 5G网络中GTP封装会增加至少40字节，其中IP头20字节，UDP头8字节，GTP消息封装12字节。考虑到GTP支持扩展消息头，建议多预留1至2个扩展消息头长度（4或8字节）作为缓冲，即GTP封装头长度最大为48字节。

版权所有 © 华为技术有限公司

表 7-14 MTU 参数配置方法

组网场景	在发送端调节MTU方值	或者在5G AR上调节MTU值
单层GRE隧道组网	发送端MTU值=网络中设备允许通过MTU值减去单层GRE头长度28，再减去GTP封装头长度48，即发送端MTU值=MTU-28-48。	5G接口MTU值=网络中设备允许通过MTU值减去GTP封装头长度，即5G接口MTU值=MTU-48。
双层GRE隧道组网	发送端MTU值=网络中设备允许通过MTU值减去双层GRE头长度56，再减去GTP封装头长度48，即发送端MTU值=MTU-56-48。	最外层L3 GRE隧道接口MTU值=网络中设备允许通过MTU值减去单层GRE头长度28，再减去GTP封装头长度48，即最外层L3 GRE隧道接口MTU值=MTU-28-48。本例中，MTU取值为1500。

配置思路

在5G链路上构建Tunnel0/0/1接口，在以太链路上构建Tunnel0/0/2接口，在Tunnel0/0/1接口配置多发选收功能，将Tunnel0/0/1接口下的报文复制到Tunnel0/0/2接口发送出去，同时配置联动BFD会话，实现设备间链路故障的快速检测。

本例配置主要思路是：

1. 在AR1上配置不同的VPN实例，与AR1相连的接口和相应的VPN实例绑定，接入VPN用户。
2. 配置设备间网络互连。
3. 配置BFD会话，实现设备间链路故障的快速检测。
4. 配置Tunnel接口并配置多发选收功能。
5. 配置静态路由，并联动BFD会话。

说明

用户可以根据现网实际情况配置BFD报文的接收和发送间隔。

操作步骤

1. 在AR1上配置不同的VPN实例，与AR1相连的接口和相应的VPN实例绑定，接入VPN用户。

```
[AR1] ip vpn-instance vpn1
[AR1-vpn-instance-vpn1] ipv4-family
[AR1-vpn-instance-vpn1-af-ipv4] route-distinguisher 1:1
[AR1-vpn-instance-vpn1-af-ipv4] vpn-target 1:1 export-extcommunity
[AR1-vpn-instance-vpn1-af-ipv4] vpn-target 1:1 import-extcommunity
[AR1-vpn-instance-vpn1-af-ipv4] quit
[AR1-vpn-instance-vpn1] quit
[AR1] ip vpn-instance vpn2
[AR1-vpn-instance-vpn2] ipv4-family
[AR1-vpn-instance-vpn2-af-ipv4] route-distinguisher 2:2
[AR1-vpn-instance-vpn2-af-ipv4] vpn-target 2:2 export-extcommunity
[AR1-vpn-instance-vpn2-af-ipv4] vpn-target 2:2 import-extcommunity
[AR1-vpn-instance-vpn2-af-ipv4] quit
[AR1-vpn-instance-vpn2] quit
[AR1] dialer-rule
[AR1-dialer-rule] dialer-rule 1 ip permit
```

 版权所有 © 华为技术有限公司

```
[AR1-dialer-rule] quit
[AR1] apn profile 3gnet
[AR1-apn-profile-3gnet] quit
[AR1] interface Cellular 2/0/0
[AR1-Cellular2/0/0] ip binding vpn-instance vpn1
[AR1-Cellular2/0/0] dialer enable-circular
[AR1-Cellular2/0/0] dialer-group 1
[AR1-Cellular2/0/0] dialer timer autodial 10
[AR1-Cellular2/0/0] apn-profile 3gnet
[AR1-Cellular2/0/0] profile create default 3gnet
[AR1-Cellular2/0/0] ip address negotiate
[AR1-Cellular2/0/0] quit
[AR1] interface GigabitEthernet 0/0/9
[AR1-GigabitEthernet0/0/9] ip binding vpn-instance vpn2
[AR1-GigabitEthernet0/0/9] ip address 192.168.8.2 255.255.255.0
[AR1-GigabitEthernet0/0/9] quit
[AR1] ip route-static vpn-instance vpn1 0.0.0.0 0.0.0.0 Cellular2/0/0
[AR1] ip route-static vpn-instance vpn2 0.0.0.0 0.0.0.0 192.168.8.1
```

配置AR2。

```
[AR2] interface GigabitEthernet 0/0/9
[AR2-GigabitEthernet0/0/9] ip address 10.1.1.1 24
[AR2-GigabitEthernet0/0/9] quit
[AR2] ip route-static 0.0.0.0 0.0.0.0 10.1.1.2
```

2. 配置设备间网络互连。

配置AR1。

```
[AR1] interface LoopBack1
[AR1-LoopBack1] ip address 2.2.2.2 255.255.255.255
[AR1-LoopBack1] quit
[AR1] vlan batch 10
[AR1] interface Virtual-Ethernet 0/0/1
[AR1-Virtual-Ethernet0/0/1] portswitch
[AR1-Virtual-Ethernet0/0/1] port link-type trunk
[AR1-Virtual-Ethernet0/0/1] port trunk allow-pass vlan 10
[AR1-Virtual-Ethernet0/0/1] quit
[AR1] interface Virtual-Ethernet 0/0/2
[AR1-Virtual-Ethernet0/0/2] portswitch
[AR1-Virtual-Ethernet0/0/2] port link-type access
[AR1-Virtual-Ethernet0/0/2] port default vlan 10
[AR1-Virtual-Ethernet0/0/2] quit
[AR1] interface Tunnel 0/0/3
[AR1-Tunnel0/0/3] ip address 192.168.13.2 255.255.255.0
[AR1-Tunnel0/0/3] tunnel-protocol gre
[AR1-Tunnel0/0/3] gre key plain 3
[AR1-Tunnel0/0/3] source LoopBack1
[AR1-Tunnel0/0/3] destination 11.11.11.11
[AR1-Tunnel0/0/3] map interface Virtual-Ethernet 0/0/1
[AR1-Tunnel0/0/3] quit
[AR1] interface gigabitethernet 0/0/10
[AR1-GigabitEthernet0/0/10] map interface Virtual-Ethernet 0/0/2
[AR1-GigabitEthernet0/0/10] tcp adjust-mss 1200
[AR1-GigabitEthernet0/0/10] quit
```

配置AR2。

```
[AR2] interface LoopBack1
[AR2-LoopBack1] ip address 11.11.11.11 255.255.255.255
[AR2-LoopBack1] quit
[AR2] vlan batch 10
[AR2] interface Virtual-Ethernet 0/0/1
[AR2-Virtual-Ethernet0/0/1] portswitch
[AR2-Virtual-Ethernet0/0/1] port link-type trunk
[AR2-Virtual-Ethernet0/0/1] port trunk allow-pass vlan 10
[AR2-Virtual-Ethernet0/0/1] quit
[AR2] interface Virtual-Ethernet 0/0/2
[AR2-Virtual-Ethernet0/0/2] portswitch
[AR2-Virtual-Ethernet0/0/2] port link-type access
[AR2-Virtual-Ethernet0/0/2] port default vlan 10
[AR2-Virtual-Ethernet0/0/2] quit
```

 版权所有 © 华为技术有限公司

```
[AR2] interface Tunnel 0/0/3
[AR2-Tunnel0/0/3] ip address 192.168.13.1 255.255.255.0
[AR2-Tunnel0/0/3] tunnel-protocol gre
[AR2-Tunnel0/0/3] gre key plain 3
[AR2-Tunnel0/0/3] source LoopBack1
[AR2-Tunnel0/0/3] destination 2.2.2.2
[AR2-Tunnel0/0/3] map interface Virtual-Ethernet 0/0/1
[AR2-Tunnel0/0/3] quit
[AR2] interface gigabitethernet 0/0/10
[AR2-GigabitEthernet0/0/10] map interface Virtual-Ethernet 0/0/2
[AR2-GigabitEthernet0/0/10] tcp adjust-mss 1200
[AR2-GigabitEthernet0/0/10] quit
```

3. 配置BFD会话，实现设备间链路故障的快速检测。

   # 配置AR1。

   ```
   [AR1] bfd
   [AR1-bfd] quit
   [AR1] bfd atob1 bind peer-ip 192.168.11.1 source-ip 192.168.11.2
   [AR1-bfd-session-atob1] discriminator local 2
   [AR1-bfd-session-atob1] discriminator remote 1
   [AR1-bfd-session-atob1] commit
   [AR1-bfd-session-atob1] quit
   [AR1] bfd atob2 bind peer-ip 192.168.12.1 source-ip 192.168.12.2
   [AR1-bfd-session-atob2] discriminator local 4
   [AR1-bfd-session-atob2] discriminator remote 3
   [AR1-bfd-session-atob2] commit
   [AR1-bfd-session-atob2] quit
   ```

   # 配置AR2。

   ```
   [AR2] bfd
   [AR2-bfd] quit
   [AR2] bfd btoa1 bind peer-ip 192.168.11.2 source-ip 192.168.11.1
   [AR2-bfd-session-btoa1] discriminator local 1
   [AR2-bfd-session-btoa1] discriminator remote 2
   [AR2-bfd-session-btoa1] commit
   [AR2-bfd-session-btoa1] quit
   [AR2] bfd btoa2 bind peer-ip 192.168.12.2 source-ip 192.168.12.1
   [AR2-bfd-session-btoa2] discriminator local 3
   [AR2-bfd-session-btoa2] discriminator remote 4
   [AR2-bfd-session-btoa2] commit
   [AR2-bfd-session-btoa2] quit
   ```

4. 配置Tunnel接口并配置多发选收功能。

   # 配置AR1。

   ```
   [AR1] interface tunnel 0/0/1
   [AR1-Tunnel0/0/1] tunnel-protocol gre
   [AR1-Tunnel0/0/1] ip address 192.168.11.2 255.255.255.0
   [AR1-Tunnel0/0/1] gre key plain 1
   [AR1-Tunnel0/0/1] source Cellular2/0/0
   [AR1-Tunnel0/0/1] destination vpn-instance vpn1 10.1.1.1
   [AR1-Tunnel0/0/1] mtu 1424
   [AR1-Tunnel0/0/1] quit
   [AR1] interface tunnel 0/0/2
   [AR1-Tunnel0/0/2] tunnel-protocol gre
   [AR1-Tunnel0/0/2] ip address 192.168.12.2 255.255.255.0
   [AR1-Tunnel0/0/2] gre key plain 2
   [AR1-Tunnel0/0/2] source GigabitEthernet0/0/9
   [AR1-Tunnel0/0/2] destination vpn-instance vpn2 10.1.1.1
   [AR1-Tunnel0/0/2] mtu 1424
   [AR1-Tunnel0/0/2] quit
   [AR1] replication path-group g1
   [AR1-replication-path-group-g1] path Tunnel 0/0/1 priority 1 track bfd-session atob1
   [AR1-replication-path-group-g1] path Tunnel 0/0/2 priority 2 track bfd-session atob2
   [AR1-replication-path-group-g1] quit
   [AR1] interface tunnel 0/0/1
   [AR1-Tunnel0/0/1] replication path-group g1
   [AR1-Tunnel0/0/1] quit
   [AR1] interface tunnel 0/0/2
   ```

 版权所有 © 华为技术有限公司

```
[AR1-Tunnel0/0/2] replication path-group g1
[AR1-Tunnel0/0/2] quit
```

配置AR2。

```
[AR2] interface tunnel 0/0/1
[AR2-Tunnel0/0/1] tunnel-protocol gre
[AR2-Tunnel0/0/1] ip address 192.168.11.1 255.255.255.0
[AR2-Tunnel0/0/1] gre key plain 1
[AR2-Tunnel0/0/1] source GigabitEthernet0/0/9
[AR2-Tunnel0/0/1] destination 1.1.1.1
[AR2-Tunnel0/0/1] mtu 1424
[AR2-Tunnel0/0/1] quit
[AR2] interface tunnel 0/0/2
[AR2-Tunnel0/0/2] tunnel-protocol gre
[AR2-Tunnel0/0/2] ip address 192.168.12.1 255.255.255.0
[AR2-Tunnel0/0/2] gre key plain 2
[AR2-Tunnel0/0/2] source GigabitEthernet0/0/9
[AR2-Tunnel0/0/2] destination 192.168.8.2
[AR2-Tunnel0/0/2] mtu 1424
[AR2-Tunnel0/0/2] quit
[AR2] replication path-group g1
[AR2-replication-path-group-g1] path Tunnel 0/0/1 priority 1 track bfd-session btoa1
[AR2-replication-path-group-g1] path Tunnel 0/0/2 priority 2 track bfd-session btoa2
[AR2-replication-path-group-g1] quit
[AR2] interface tunnel 0/0/1
[AR2-Tunnel0/0/1] replication path-group g1
[AR2-Tunnel0/0/1] quit
[AR2] interface tunnel 0/0/2
[AR2-Tunnel0/0/2] replication path-group g1
[AR2-Tunnel0/0/2] quit
```

5. 配置静态路由，5G链路和以太链路的隧道作为等价路由，并联动BFD会话。

   # 配置AR1。

   ```
   [AR1] ip route-static 11.11.11.11 255.255.255.255 Tunnel0/0/1 track bfd-session atob1
   [AR1] ip route-static 11.11.11.11 255.255.255.255 Tunnel0/0/2 track bfd-session atob2
   ```

   # 配置AR2。

   ```
   [AR2] ip route-static 2.2.2.2 255.255.255.255 Tunnel0/0/1 track bfd-session btoa1
   [AR2] ip route-static 2.2.2.2 255.255.255.255 Tunnel0/0/2 track bfd-session btoa2
   ```

配置文件

- AR1的配置文件

```
#
ip vpn-instance vpn1
 ipv4-family
 route-distinguisher 1:1
 vpn-target 1:1 export-extcommunity
 vpn-target 1:1 import-extcommunity
#
ip vpn-instance vpn2
 ipv4-family
 route-distinguisher 2:2
 vpn-target 2:2 export-extcommunity
 vpn-target 2:2 import-extcommunity
#
dialer-rule
 dialer-rule 1 ip permit
#
apn profile 3gnet
#
interface Cellular2/0/0
 ip binding vpn-instance vpn1
 dialer enable-circular
 dialer-group 1
 dialer timer autodial 10
 apn-profile 3gnet
 profile create default 3gnet
```

 版权所有 © 华为技术有限公司

```
 ip address negotiate
#
interface GigabitEthernet0/0/9
 ip binding vpn-instance vpn2
 ip address 192.168.8.2 255.255.255.0
#
ip route-static vpn-instance vpn1 0.0.0.0 0.0.0.0 Cellular2/0/0
ip route-static vpn-instance vpn2 0.0.0.0 0.0.0.0 192.168.8.1
#
interface Tunnel0/0/1
 ip address 192.168.11.2 255.255.255.0
 tunnel-protocol gre
 gre key plain 1
 source Cellular2/0/0
 destination vpn-instance vpn1 10.1.1.1
 replication path-group g1
 mtu 1424
#
interface Tunnel0/0/2
 ip address 192.168.12.2 255.255.255.0
 tunnel-protocol gre
 gre key plain 2
 source GigabitEthernet0/0/9
 destination vpn-instance vpn2 10.1.1.1
 replication path-group g1
 mtu 1424
#
bfd
#
bfd atob1 bind peer-ip 192.168.11.1 source-ip 192.168.11.2
 discriminator local 2
 discriminator remote 1
 commit
#
bfd atob2 bind peer-ip 192.168.12.1 source-ip 192.168.12.2
 discriminator local 4
 discriminator remote 3
 commit
#
replication path-group g1
 path Tunnel0/0/1 priority 1 track bfd-session atob1
 path Tunnel0/0/2 priority 2 track bfd-session atob2
#
interface LoopBack1
 ip address 2.2.2.2 255.255.255.255
#
ip route-static 11.11.11.11 255.255.255.255 Tunnel0/0/1 track bfd-session atob1
ip route-static 11.11.11.11 255.255.255.255 Tunnel0/0/2 track bfd-session atob1
#
vlan batch 10
#
interface Virtual-Ethernet0/0/1
 portswitch
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface Virtual-Ethernet0/0/2
 portswitch
 port link-type access
 port default vlan 10
#
interface Tunnel0/0/3
 ip address 192.168.13.2 255.255.255.0
 tunnel-protocol gre
 gre key plain 3
 source LoopBack1
 destination 11.11.11.11
 map interface Virtual-Ethernet0/0/1
#
```

 版权所有 © 华为技术有限公司

```
interface GigabitEthernet0/0/10
 map interface Virtual-Ethernet0/0/2
 tcp adjust-mss 1200
#
```

- AR2的配置文件

```
#
interface GigabitEthernet0/0/9
 ip address 10.1.1.1 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 10.1.1.2
#
interface Tunnel0/0/1
 ip address 192.168.11.1 255.255.255.0
 tunnel-protocol gre
 gre key plain 1
 source GigabitEthernet0/0/9
 destination 20.20.20.20
 replication path-group g1
 mtu 1424
#
interface Tunnel0/0/2
 ip address 192.168.12.1 255.255.255.0
 tunnel-protocol gre
 gre key plain 2
 source GigabitEthernet0/0/9
 destination 192.168.8.2
 replication path-group g1
 mtu 1424
#
bfd
#
bfd btoa1 bind peer-ip 192.168.11.2 source-ip 192.168.11.1
 discriminator local 1
 discriminator remote 2
 commit
#
bfd btoa2 bind peer-ip 192.168.12.2 source-ip 192.168.12.1
 discriminator local 3
 discriminator remote 4
 commit
#
replication path-group g1
 path Tunnel0/0/1 priority 1 track bfd-session btoa1
 path Tunnel0/0/2 priority 2 track bfd-session btoa2
#
interface LoopBack1
 ip address 11.11.11.11 255.255.255.255
#
ip route-static 2.2.2.2 255.255.255.255 Tunnel0/0/1 track bfd-session btoa1
ip route-static 2.2.2.2 255.255.255.255 Tunnel0/0/2 track bfd-session btoa2
#
vlan batch 10
#
interface Virtual-Ethernet0/0/1
 portswitch
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface Virtual-Ethernet0/0/2
 portswitch
 port link-type access
 port default vlan 10
#
interface Tunnel0/0/3
 ip address 192.168.13.1 255.255.255.0
 tunnel-protocol gre
 gre key plain 3
 source LoopBack1
 destination 2.2.2.2
```

 版权所有 © 华为技术有限公司

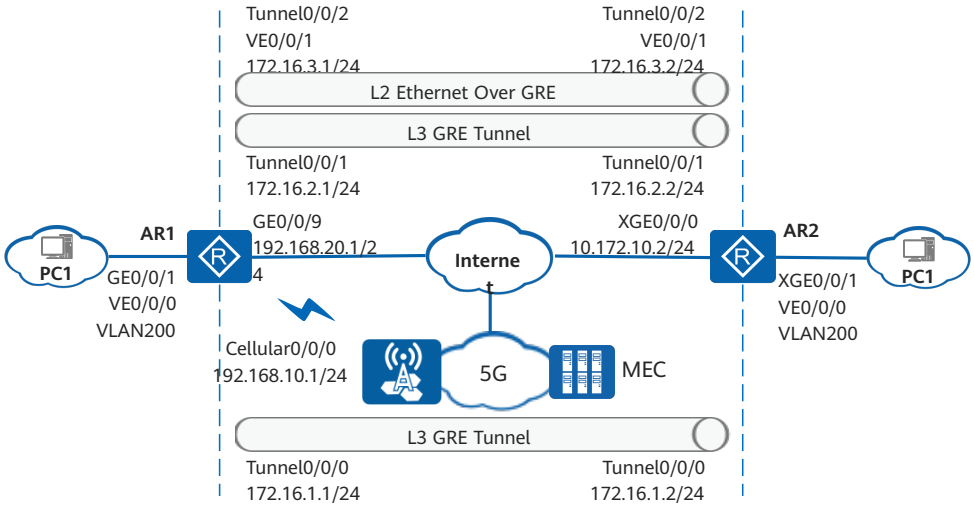
```
 map interface Virtual-Ethernet0/0/1
#
interface GigabitEthernet0/0/10
 map interface Virtual-Ethernet0/0/2
 tcp adjust-mss 1200
#
```

7.2.9 配置 5G 场景二层重定向多发选收示例

组网需求

如图7-12所示，企业分支和总部之间通过Internet网络互通，企业分支使用AR1作为出口网关。为了提高链路可靠性，AR1部署了两条上行链路接入Internet。其中5G链路作为主链路，以太有线链路作为备链路。用户希望将5G链路的报文复制到以太链路发送出去，报文复制过程忽略接口状态和路由状态，最大程度保证业务连续性。并且分支和总部可以传输原始以太报文（如工业控制的PLC报文，采用二层隧道封装。

图 7-12 配置 5G 场景二层重定向多发选收组网图



数据准备

表 7-15 数据准备表

项目	数据	说明
分支AR1 LAN侧接口信息	LAN侧物理接口：GE0/0/1 绑定的VE接口：VE0/0/0 所属VLAN：200	分支AR1与分支用户之间的链路信息。

版权所有 © 华为技术有限公司

项目	数据	说明
分支AR1 WAN侧接口信息	主链路5G Cellular接口：Cellular0/0/0 IP地址：192.168.10.1/24 绑定VPN实例：wan1 备链路物理接口：GE0/0/9 IP地址：192.168.20.1/24 绑定VPN实例：wan2	分支AR1和总部AR2之间的链路信息。
分支AR1 Tunnel0/0/0接口信息	IP地址：172.16.1.1/24 源接口：Cellular0/0/0	分支AR1和总部AR2之间的L3 GRE隧道信息。
分支AR1 Tunnel0/0/1接口信息	IP地址：172.16.2.1/24 源接口：GE0/0/9	分支AR1和总部AR2之间的L3 GRE隧道信息。
分支AR1 Tunnel0/0/2接口信息	IP地址：172.16.3.1/24 源接口：LoopBack0 绑定的VE接口：VE0/0/1	分支AR1和总部AR2之间的Ethernet over GRE隧道信息。
总部AR2 LAN侧接口信息	LAN侧物理接口：XGE0/0/1 绑定的VE接口：VE0/0/0 所属VLAN：200	总部AR2与总部用户之间的链路信息。
总部AR2 WAN侧接口信息	WAN侧物理接口：XGE0/0/0 IP地址：10.172.10.2/24	总部AR2与分支AR1之间的链路信息。
总部AR2 Tunnel0/0/0接口信息	IP地址：172.16.1.2/24 源接口：XGE0/0/0	总部AR2和分支AR1之间的L3 GRE隧道信息。
总部AR2 Tunnel0/0/1接口信息	IP地址：172.16.2.2/24 源接口：XGE0/0/0	总部AR2和分支AR1之间的L3 GRE隧道信息。
总部AR2 Tunnel0/0/2接口信息	IP地址：172.16.3.2/24 源接口：LoopBack0 绑定的VE接口：VE0/0/1	总部AR2和分支AR1之间的Ethernet over GRE隧道信息。

MTU 及 TCP MSS 参数配置说明

为了减少网络传输中不必要的分片和重组，网络规划时需要合理设置终端发出的报文大小，设置依据如下：

- 对于UDP报文，可以调节发送端的MTU值，如果发送端不支持调节MTU值，则需要在5G AR设备上调节MTU值，以确保报文在网络中传输时不会产生二次分片。
- 对于TCP报文，可以配置5G AR设备的TCP MSS值，通过修改应用层报文数据包的长度来避免报文分片。

 版权所有 © 华为技术有限公司

在5G2B专线场景中，TCP MSS取值比较简单，在隧道两端AR设备的LAN侧接入物理口或VLANIF口上配置TCP MSS为推荐值1200。MTU取值相对复杂，与如下三个参数有关，具体的配置方法请参见**表2** 。

- 单层GRE隧道组网，报文经过5G AR设备后会增加28字节，即单层GRE头长度为28字节。
- 双层GRE隧道组网，报文经过5G AR设备后会增加56字节，即双层GRE头长度为56字节。
- 5G网络中GTP封装会增加至少40字节，其中IP头20字节，UDP头8字节，GTP消息封装12字节。考虑到GTP支持扩展消息头，建议多预留1至2个扩展消息头长度（4或8字节）作为缓冲，即GTP封装头长度最大为48字节。

表 7-16 MTU 参数配置方法

组网场景	在发送端调节MTU方值	或者在5G AR上调节MTU值
单层GRE隧道组网	发送端MTU值=网络中设备允许通过MTU值减去单层GRE头长度28，再减去GTP封装头长度48，即发送端MTU值=MTU-28-48。	5G接口MTU值=网络中设备允许通过MTU值减去GTP封装头长度，即5G接口MTU值=MTU-48。
双层GRE隧道组网	发送端MTU值=网络中设备允许通过MTU值减去双层GRE头长度56，再减去GTP封装头长度48，即发送端MTU值=MTU-56-48。	最外层L3 GRE隧道接口MTU值=网络中设备允许通过MTU值减去单层GRE头长度28，再减去GTP封装头长度48，即最外层L3 GRE隧道接口MTU值=MTU-28-48。本例中，MTU取值为1500。

配置思路

本例配置主要思路是：

1. 配置设备物理接口的IP地址及静态路由，实现设备之间三层网络互通，同时，在AR1上创建不同的VPN实例，实现不同VPN间的业务隔离。
2. 在AR1和AR2之间部署GRE隧道，通过静态路由指定到达对端的报文通过GRE隧道转发，实现Underlay传输网络互通，用于三层报文多发选收。
3. 配置Overlay业务网络互通。在LAN侧的接口和WAN侧的Tunnel接口上分别绑定二层VE接口，实现以太报文通过GRE隧道进行透传，且配置WAN侧Tunnel源接口为Loopback接口用于实现二层报文多发选收。
4. 在源接口为Loopback接口的内层Ethernet Over GRE隧道上配置重定向多发选收功能，并指定链路组不根据链路状态刷新选路信息，避免路由切换过程中出现的丢包现象，最大程度保证业务连续性。
5. 配置OSPF路由。

 版权所有 © 华为技术有限公司

说明

- 对丢包有特殊要求的业务，比如金融、安全等相关业务，在多发选收功能仍然无法满足其要求时，可以通过引入Loopback接口的内层GRE隧道配置重定向多发选收实现报文转发，不再依赖于路由。同时通过配置链路组选路刷新的抑制周期，避免路由切换过程中出现的丢包现象，最大程度保证业务连续性。
- 多发选收功能只支持转发IPinIP、TCP、UDP、GRE、ESP和AH六种类型的报文。对于LAN侧为Ethernet二层报文的场景，可使用Loopback接口创建Ethernet Over GRE再进行多发选收功能配置，实现二层报文的多发选收。

操作步骤

1. 配置设备物理接口的IP地址及静态路由，实现设备之间三层网络互通。

   # 配置AR1。在AR1上创建不同的VPN实例，实现不同VPN间的业务隔离。

```
<Huawei> system-view
[Huawei] sysname AR1
[AR1] router id 1.1.1.1
[AR1] ip vpn-instance wan1
[AR1-vpn-instance-wan1] ipv4-family
[AR1-vpn-instance-wan1-af-ipv4] route-distinguisher 192.168.10.1:0
[AR1-vpn-instance-wan1-af-ipv4] quit
[AR1-vpn-instance-wan1] quit
[AR1] ip vpn-instance wan2
[AR1-vpn-instance-wan2] ipv4-family
[AR1-vpn-instance-wan2-af-ipv4] route-distinguisher 192.168.20.1:0
[AR1-vpn-instance-wan2-af-ipv4] quit
[AR1-vpn-instance-wan2] quit
[AR1] interface gigabitethernet 0/0/9
[AR1-GigabitEthernet0/0/9] ip binding vpn-instance wan2
[AR1-GigabitEthernet0/0/9] ip address 192.168.20.1 255.255.255.0
[AR1-GigabitEthernet0/0/9] quit
[AR1] interface Cellular 0/0/0
[AR1-Cellular0/0/0] ip binding vpn-instance wan1
[AR1-Cellular0/0/0] dialer enable-circular
[AR1-Cellular0/0/0] dialer timer autodial 10
[AR1-Cellular0/0/0] modem auto-recovery dial action modem-reboot fail-times 128
[AR1-Cellular0/0/0] modem auto-recovery services-unavailable action modem-reboot test-times
0 interval 3600
[AR1-Cellular0/0/0] ip address negotiate
[AR1-Cellular0/0/0] quit
[AR1] route-static vpn-instance wan1 10.172.0.0 255.255.0.0 Cellular0/0/0
[AR1] ip route-static vpn-instance wan2 10.172.0.0 255.255.0.0 192.168.20.254
```

   # 配置AR2。

```
<Huawei> system-view
[Huawei] sysname AR2
[AR2] router id 2.2.2.2
[AR2] interface XGigabitEthernet0/0/0
[AR2-XGigabitEthernet0/0/0] ip address 10.172.10.2 255.255.255.0
[AR2-XGigabitEthernet0/0/0] quit
[AR2] ip route-static 192.168.0.0 255.255.0.0 10.172.10.1
```

2. 在AR1和AR2之间部署GRE隧道，通过静态路由指定到达对端的报文通过GRE隧道转发，实现Underlay传输网络互通，用于三层报文多发选收。

   # 配置AR1。

```
[AR1] interface Tunnel0/0/0
[AR1-Tunnel0/0/0] description key1
[AR1-Tunnel0/0/0] ip address 172.16.1.1 255.255.255.0
[AR1-Tunnel0/0/0] tunnel-protocol gre
[AR1-Tunnel0/0/0] keepalive period 1
[AR1-Tunnel0/0/0] gre key plain 1
[AR1-Tunnel0/0/0] source Cellular0/0/0
[AR1-Tunnel0/0/0] destination vpn-instance wan1 10.172.10.2
[AR1-Tunnel0/0/0] ospf enable 1 area 0.0.0.0
[AR1-Tunnel0/0/0] mtu 1424
```

 版权所有 © 华为技术有限公司

```
[AR1-Tunnel0/0/0] quit
[AR1] interface Tunnel0/0/1
[AR1-Tunnel0/0/1] description key2
[AR1-Tunnel0/0/1] ip address 172.16.2.1 255.255.255.0
[AR1-Tunnel0/0/1] tunnel-protocol gre
[AR1-Tunnel0/0/1] keepalive period 1
[AR1-Tunnel0/0/1] gre key plain 2
[AR1-Tunnel0/0/1] source GigabitEthernet0/0/9
[AR1-Tunnel0/0/1] destination vpn-instance wan2 10.172.10.2
[AR1-Tunnel0/0/1] ospf enable 1 area 0.0.0.0
[AR1-Tunnel0/0/1] mtu 1424
[AR1-Tunnel0/0/1] quit
```

配置AR2。

```
[AR2] interface Tunnel0/0/0
[AR2-Tunnel0/0/0] description key1
[AR2-Tunnel0/0/0] ip address 172.16.1.2 255.255.255.0
[AR2-Tunnel0/0/0] tunnel-protocol gre
[AR2-Tunnel0/0/0] keepalive period 1
[AR2-Tunnel0/0/0] gre key plain 1
[AR2-Tunnel0/0/0] source XGigabitEthernet0/0/0
[AR2-Tunnel0/0/0] destination 192.168.10.1
[AR2-Tunnel0/0/0] ospf enable 1 area 0.0.0.0
[AR2-Tunnel0/0/0] mtu 1424
[AR2-Tunnel0/0/0] quit
[AR2] interface Tunnel0/0/1
[AR2-Tunnel0/0/1] description key2
[AR2-Tunnel0/0/1] ip address 172.16.2.2 255.255.255.0
[AR2-Tunnel0/0/1] tunnel-protocol gre
[AR2-Tunnel0/0/1] gre key plain 2
[AR2-Tunnel0/0/1] source XGigabitEthernet0/0/0
[AR2-Tunnel0/0/1] destination 192.168.20.1
[AR2-Tunnel0/0/1] mtu 1424
[AR2-Tunnel0/0/1] ospf enable 1 area 0.0.0.0
[AR2-Tunnel0/0/1] quit
```

配置完成后Tunnel接口状态变为Up，Tunnel接口之间可以Ping通，直连隧道建立。以AR1的显示为例。

```
<AR1> ping 172.16.1.2
  PING 172.16.1.2: 56  data bytes, press CTRL_C to break
    Reply from 172.16.1.2: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 172.16.1.2: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 172.16.1.2: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 172.16.1.2: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 172.16.1.2: bytes=56 Sequence=5 ttl=255 time=1 ms
  --- 172.16.1.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/1 ms
```

3. 配置Overlay业务网络互通。在LAN侧的接口和WAN侧的Tunnel接口上分别绑定二层VE接口，实现以太报文通过GRE隧道进行透传，且配置WAN侧Tunnel源接口为Loopback接口用于实现二层报文多发选收。

   # 配置AR1。

```
[AR1] interface LoopBack0
[AR1-LoopBack0] ip address 1.1.1.1 255.255.255.0
[AR1-LoopBack0] quit
[AR1] vlan batch 200
[AR1] interface Virtual-Ethernet0/0/0
[AR1-Virtual-Ethernet0/0/0] portswitch
[AR1-Virtual-Ethernet0/0/0] port link-type access
[AR1-Virtual-Ethernet0/0/0] port default vlan 200
[AR1-Virtual-Ethernet0/0/0] quit
[AR1] interface Virtual-Ethernet0/0/1
[AR1-Virtual-Ethernet0/0/1] portswitch
[AR1-Virtual-Ethernet0/0/1] port link-type trunk
[AR1-Virtual-Ethernet0/0/1] undo port trunk allow-pass vlan 1
```

 版权所有 © 华为技术有限公司

```
[AR1-Virtual-Ethernet0/0/1] port trunk allow-pass vlan 200
[AR1-Virtual-Ethernet0/0/1] quit
[AR1] interface gigabitethernet 0/0/1
[AR1-GigabitEthernet0/0/1] undo portswitch
[AR1-GigabitEthernet0/0/1] tcp adjust-mss 1200
[AR1-GigabitEthernet0/0/1] map interface Virtual-Ethernet0/0/0
[AR1-GigabitEthernet0/0/1] quit
[AR1] interface Tunnel0/0/2
[AR1-Tunnel0/0/2] ip address 172.16.3.1 255.255.255.0
[AR1-Tunnel0/0/2] tunnel-protocol gre
[AR1-Tunnel0/0/2] gre key plain 3
[AR1-Tunnel0/0/2] source LoopBack0
[AR1-Tunnel0/0/2] destination 2.2.2.2
[AR1-Tunnel0/0/2] map interface Virtual-Ethernet0/0/1
[AR1-Tunnel0/0/2] quit
```

配置AR2。

```
[AR2] interface LoopBack0
[AR2-LoopBack0] ip address 2.2.2.2 255.255.255.0
[AR2-LoopBack0] quit
[AR2] vlan batch 200
[AR2] interface XGigabitEthernet0/0/1
[AR2-XGigabitEthernet0/0/1] portswitch
[AR2-XGigabitEthernet0/0/1] port link-type trunk
[AR2-XGigabitEthernet0/0/1] undo port trunk allow-pass vlan 1
[AR2-XGigabitEthernet0/0/1] port trunk allow-pass vlan 200
[AR2-XGigabitEthernet0/0/1] quit
[AR2] interface Virtual-Ethernet0/0/0
[AR2-Virtual-Ethernet0/0/0] portswitch
[AR2-Virtual-Ethernet0/0/0] port link-type trunk
[AR2-Virtual-Ethernet0/0/0] undo port trunk allow-pass vlan 1
[AR2-Virtual-Ethernet0/0/0] port trunk allow-pass vlan 200
[AR2-Virtual-Ethernet0/0/0] quit
[AR2] interface Virtual-Ethernet0/0/1
[AR2-Virtual-Ethernet0/0/1] portswitch
[AR2-Virtual-Ethernet0/0/1] port link-type trunk
[AR2-Virtual-Ethernet0/0/1] undo port trunk allow-pass vlan 1
[AR2-Virtual-Ethernet0/0/1] port trunk allow-pass vlan 200
[AR2-Virtual-Ethernet0/0/1] quit
[AR2] interface Tunnel0/0/2
[AR2-Tunnel0/0/2] ip address 172.16.3.2 255.255.255.0
[AR2-Tunnel0/0/2] tunnel-protocol gre
[AR2-Tunnel0/0/2] gre key plain 3
[AR2-Tunnel0/0/2] source LoopBack0
[AR2-Tunnel0/0/2] destination 1.1.1.1
[AR2-Tunnel0/0/2] map interface Virtual-Ethernet0/0/1
[AR2-Tunnel0/0/2] quit
[AR2] interface Vlanif200
[AR2-Vlanif200] map interface Virtual-Ethernet0/0/0
[AR2-Vlanif200] tcp adjust-mss 1200
[AR2-Vlanif200] quit
```

4. 在源接口为Loopback接口的内层Ethernet Over GRE隧道上配置重定向多发选收功能，并指定链路组不根据链路状态刷新选路信息，避免路由切换过程中出现的丢包现象，最大程度保证业务连续性。

   # 配置AR1。

   ```
   [AR1] replication path-group 1
   [AR1-replication-path-group-1] path Tunnel0/0/0 priority 1
   [AR1-replication-path-group-1] path Tunnel0/0/1 priority 2
   [AR1-replication-path-group-1] quit
   [AR1] interface tunnel 0/0/2
   [AR1-Tunnel0/0/2] redirect-replication path-group 1
   [AR1-Tunnel0/0/2] quit
   [AR1] replication if-down-delay 65535
   ```

   # 配置AR2。

   ```
   [AR2] replication path-group 1
   [AR2-replication-path-group-1] path Tunnel 0/0/0 priority 1
   [AR2-replication-path-group-1] path Tunnel 0/0/1 priority 2
   ```

 版权所有 © 华为技术有限公司

```
[AR2-replication-path-group-1] quit
[AR2] interface tunnel0/0/2
[AR2-Tunnel0/0/2] redirect-replication path-group 1
[AR2-Tunnel0/0/2] quit
[AR2] replication if-down-delay 65535
```

5. 配置OSPF路由。

   # 配置AR1。

```
[AR1] ospf 1
[AR1-ospf-1] area 0.0.0.0
[AR1-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[AR1-ospf-1-area-0.0.0.0] quit
[AR1-ospf-1] quit
```

   # 配置AR2。

```
[AR2] ospf 1
[AR2-ospf-1] area 0.0.0.0
[AR2-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[AR2-ospf-1-area-0.0.0.0] quit
[AR2-ospf-1] quit
```

配置文件

- AR1的配置文件

```
#
sysname AR1
#
router id 1.1.1.1
#
vlan batch 200
#
 replication if-down-delay 65535
#
ip vpn-instance wan1
 ipv4-family
  route-distinguisher 192.168.10.1:0
#
ip vpn-instance wan2
 ipv4-family
  route-distinguisher 192.168.20.1:0
#
interface GigabitEthernet0/0/1
 undo portswitch
 tcp adjust-mss 1200
 map interface Virtual-Ethernet0/0/0
#
interface GigabitEthernet0/0/9
 ip binding vpn-instance wan2
 ip address 192.168.20.1 255.255.255.0
#
interface Cellular0/0/0
 ip binding vpn-instance wan1
 dialer enable-circular
 dialer timer autodial 10
 modem auto-recovery dial action modem-reboot fail-times
128
 modem auto-recovery services-unavailable action modem-reboot test-times 0 interval
3600
 ip address negotiate
#
interface Virtual-Ethernet0/0/0
 portswitch
 port link-type access
 port default vlan 200
#
interface Virtual-Ethernet0/0/1
 portswitch
 port link-type trunk
```

 版权所有 © 华为技术有限公司

```
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 200
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.0
#
interface Tunnel0/0/0
 description key1
 ip address 172.16.1.1 255.255.255.0
 tunnel-protocol gre
 keepalive period 1
 gre key plain 1
 source Cellular0/0/0
 destination vpn-instance wan1 10.172.10.2
 ospf enable 1 area 0.0.0.0
 mtu 1424
#
interface Tunnel0/0/1
 description key2
 ip address 172.16.2.1 255.255.255.0
 tunnel-protocol gre
 keepalive period 1
 gre key plain 2
 source GigabitEthernet0/0/9
 destination vpn-instance wan2 10.172.10.2
 ospf enable 1 area 0.0.0.0
 mtu 1424
#
interface Tunnel0/0/2
 ip address 172.16.3.1 255.255.255.0
 tunnel-protocol gre
 gre key plain 3
 source LoopBack0
 destination 2.2.2.2
 redirect-replication path-group 1
 map interface Virtual-Ethernet0/0/1
#
ospf 1
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
#
ip route-static vpn-instance wan1 10.172.0.0 255.255.0.0 Cellular0/0/0
ip route-static vpn-instance wan2 10.172.0.0 255.255.0.0 192.168.20.254
#
replication path-group 1
 path Tunnel0/0/0 priority 1
 path Tunnel0/0/1 priority 2
#
```

- AR2的配置文件

```
#
sysname AR2
#
router id 2.2.2.2
#
vlan batch  200
#
 replication if-down-delay 65535
#
interface Vlanif200
 map interface Virtual-Ethernet0/0/0
 tcp adjust-mss 1200
#
interface XGigabitEthernet0/0/0
 ip address 10.172.10.2 255.255.255.0
#
interface XGigabitEthernet0/0/1
 portswitch
 port link-type trunk
 undo port trunk allow-pass vlan 1
```

 版权所有 © 华为技术有限公司

```
 port trunk allow-pass vlan 200
 #
interface Virtual-Ethernet0/0/0
 portswitch
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 200
#
interface Virtual-Ethernet0/0/1
 portswitch
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 200
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
interface Tunnel0/0/0
 description key1
 ip address 172.16.1.2 255.255.255.0
 tunnel-protocol gre
 keepalive period 1
 gre key plain 1
 source XGigabitEthernet0/0/0
 destination 192.168.10.1
 ospf enable 1 area 0.0.0.0
 mtu 1424
#
interface Tunnel0/0/1
 description key2
 ip address 172.16.2.2 255.255.255.0
 tunnel-protocol gre
 keepalive period 1
 gre key plain 2
 source XGigabitEthernet0/0/0
 destination 192.168.20.1
 ospf enable 1 area 0.0.0.0
 mtu 1424
#
interface Tunnel0/0/2
 ip address 172.16.3.2 255.255.255.0
 tunnel-protocol gre
 gre key plain 3
 source LoopBack0
 destination 1.1.1.1
 redirect-replication path-group 1
 map interface Virtual-Ethernet0/0/1
#
ospf 1
 area 0.0.0.0
  network 2.2.2.2 0.0.0.0
#
ip route-static 192.168.0.0 255.255.0.0 10.172.10.1
#
replication path-group 1
 path Tunnel0/0/0 priority 1
 path Tunnel0/0/1 priority 2
#
```

7.2.10 配置二层多发选收示例（5G CPE 场景）

组网需求

说明

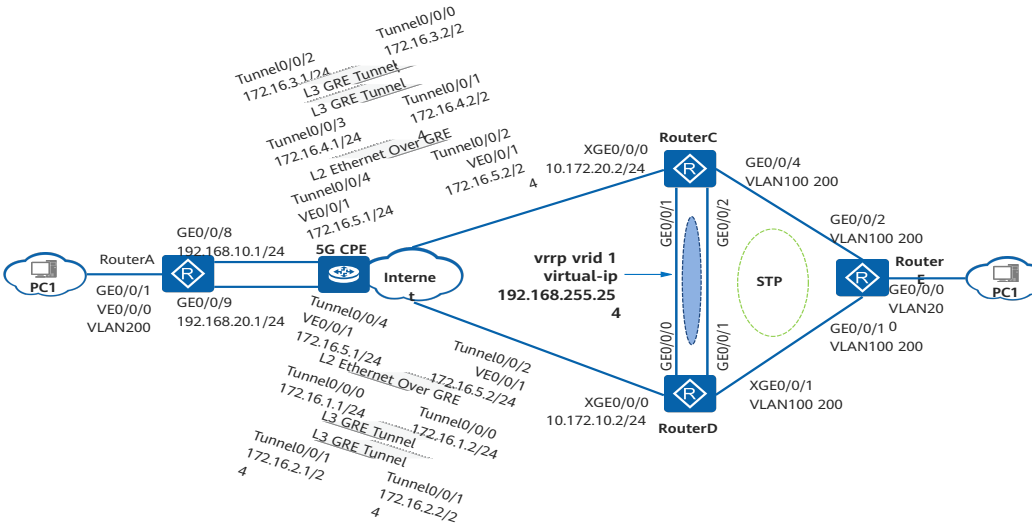
AR设备配置多个GE子接口与5G CPE（N5368X）桥接模式对接时，由于CPE使用场景约束，AR设备需要使用子接口下的MAC地址修改功能保证CPE学习MAC地址的唯一性。

 版权所有 © 华为技术有限公司

如图7-13所示，RouterA为企业分支网关，RouterC和RouterD为企业总部网关，用户希望实现：

- 正常情况下，RouterD为Master设备承担流量转发，当RouterD故障时，RouterC接替作为网关继续进行工作，实现网关的冗余备份。
- 分支和总部可以传输原始以太报文（如工业控制的PLC报文），采用二层隧道封装。
- 对于可靠性要求很高并且流量较小的业务，如果分支RouterA其中一条链路故障，将报文复制到另外一条链路发送出去，防止出现业务中断的现象。

图 7-13 配置二层多发选收组网图



数据准备

表 7-17 数据准备表

项目	数据	说明
分支RouterA LAN侧接口信息	LAN侧物理接口：GE0/0/1 绑定的VE接口：VE0/0/0 所属VLAN：200	分支RouterA与分支用户之间的链路信息。
分支RouterA WAN侧接口信息	主链路物理接口：GE0/0/8 IP地址：192.168.10.1/24 绑定VPN实例：wan1 复制链路物理接口：GE0/0/9 IP地址：192.168.20.1/24 绑定VPN实例：wan2	分支RouterA与5G CPE之间的链路信息。

版权所有 © 华为技术有限公司

项目	数据	说明
分支RouterA Tunnel0/0/0接口信息	IP地址：172.16.1.1/24 源接口：GE0/0/8	分支RouterA和总部RouterD之间的L3 GRE隧道信息。
分支RouterA Tunnel0/0/1接口信息	IP地址：172.16.2.1/24 源接口：GE0/0/9	分支RouterA和总部RouterD之间的L3 GRE隧道信息。
分支RouterA Tunnel0/0/2接口信息	IP地址：172.16.3.1/24 源接口：GE0/0/8	分支RouterA和总部RouterC之间的L3 GRE隧道信息。
分支RouterA Tunnel0/0/3接口信息	IP地址：172.16.4.1/24 源接口：GE0/0/9	分支RouterA和总部RouterC之间的L3 GRE隧道信息。
分支RouterA Tunnel0/0/4接口信息	IP地址：172.16.5.1/24 源接口：LoopBack0 绑定的VE接口：VE0/0/1	分支RouterA和总部RouterC以及RouterD之间的Ethernet over GRE隧道信息。
总部RouterC LAN侧接口信息	LAN侧物理接口：GE0/0/4 所属VLAN：100、200	总部RouterC与分支RouterE之间的链路信息。
总部RouterC WAN侧接口信息	WAN侧物理接口：XGE0/0/0 IP地址：10.172.20.2/24	总部RouterC与Internet之间的链路信息。
总部RouterC Tunnel0/0/0接口信息	IP地址：172.16.3.2/24 源接口：XGE0/0/0	总部RouterC和分支RouterA之间的L3 GRE隧道信息。
总部RouterC Tunnel0/0/1接口信息	IP地址：172.16.4.2/24 源接口：XGE0/0/0	总部RouterC和分支RouterA之间的L3 GRE隧道信息。
总部RouterC Tunnel0/0/2接口信息	IP地址：172.16.5.2/24 源地址：192.168.255.254（VRRP备份组的虚拟IP地址） 绑定的VE接口：VE0/0/1	总部RouterC和分支RouterA之间的Ethernet over GRE隧道信息。
总部RouterD LAN侧接口信息	LAN侧物理接口：XGE0/0/1 所属VLAN：100、200	总部RouterD与分支RouterE之间的链路信息。
总部RouterD WAN侧接口信息	WAN侧物理接口：XGE0/0/0 IP地址：10.172.10.2/24	总部RouterD与Internet之间的链路信息。
总部RouterD Tunnel0/0/0接口信息	IP地址：172.16.1.2/24 源接口：XGE0/0/0	总部RouterD和分支RouterA之间的L3 GRE隧道信息。
总部RouterD Tunnel0/0/1接口信息	IP地址：172.16.2.2/24 源接口：XGE0/0/0	总部RouterD和分支RouterA之间的L3 GRE隧道信息。

 版权所有 © 华为技术有限公司

项目	数据	说明
总部RouterD Tunnel0/0/2接口信息	IP地址：172.16.5.2/24 源地址：192.168.255.254（VRRP备份组的虚拟IP地址） 绑定的VE接口：VE0/0/1	总部RouterD和分支RouterA之间的Ethernet over GRE隧道信息。
分支RouterE LAN侧接口信息	LAN侧物理接口1：GE0/0/0 所属VLAN：200 LAN侧物理接口2：GE0/0/1 所属VLAN：100、200 LAN侧物理接口3：GE0/0/2 所属VLAN：100、200	GE0/0/0为分支RouterE与分支用户之间的接口。 GE0/0/1为分支RouterE与总部RouterD之间的接口。 GE0/0/2为分支RouterE与总部RouterC之间的接口。

配置思路

本例配置的主要思路是：

1. 配置设备物理接口的IP地址及静态路由，实现设备之间三层网络互通，同时，在RouterA上创建不同的VPN实例，实现不同VPN间的业务隔离。
2. 在RouterA和RouterC、RouterD之间部署GRE隧道，通过静态路由指定到达对端的报文通过GRE隧道转发，实现Underlay传输网络互通，用于三层报文多发选收。
3. 配置Overlay业务网络互通。
   - 在LAN侧的接口和WAN侧的Tunnel接口上分别绑定二层VE接口，实现以太报文通过GRE隧道进行透传，且配置WAN侧Tunnel接口的源接口为Loopback接口用于实现二层报文多发选收。
   - RouterC和RouterD配置RSTP功能，破除二层网络中的环路。
   - RouterC和RouterD配置Eth-Trunk保证连接的可靠性。
4. 在RouterC和RouterD上配置VRRP备份组。其中，RouterD上配置较高优先级，作为Master设备承担流量转发；RouterC作为备用路由器，实现网关冗余备份。
5. 在RouterA、RouterC和RouterD上分别配置BFD会话，实现设备间链路故障的快速检测。
6. 在Tunnel接口上配置多发选收。
7. 配置静态路由，并联动BFD会话。

操作步骤

1. 配置设备物理接口的IP地址及静态路由，实现设备之间三层网络互通。

   # 配置RouterA物理接口的IP地址及静态路由，在RouterA上创建不同的VPN实例，实现不同VPN间的业务隔离。

   ```
   <Huawei> system-view
   [Huawei] sysname RouterA
   ```

 版权所有 © 华为技术有限公司

```
[RouterA] ip vpn-instance wan1
[RouterA-vpn-instance-wan1] ipv4-family
[RouterA-vpn-instance-wan1-af-ipv4] route-distinguisher 192.168.10.1:0
[RouterA-vpn-instance-wan1-af-ipv4] quit
[RouterA-vpn-instance-wan1] quit
[RouterA] ip vpn-instance wan2
[RouterA-vpn-instance-wan2] ipv4-family
[RouterA-vpn-instance-wan2-af-ipv4] route-distinguisher 192.168.20.1:0
[RouterA-vpn-instance-wan2-af-ipv4] quit
[RouterA-vpn-instance-wan2] quit
[RouterA] interface gigabitethernet 0/0/8
[RouterA-GigabitEthernet0/0/8] ip binding vpn-instance wan1
[RouterA-GigabitEthernet0/0/8] ip address 192.168.10.1 255.255.255.0
[RouterA-GigabitEthernet0/0/8] quit
[RouterA] interface gigabitethernet 0/0/9
[RouterA-GigabitEthernet0/0/9] ip binding vpn-instance wan2
[RouterA-GigabitEthernet0/0/9] ip address 192.168.20.1 255.255.255.0
[RouterA-GigabitEthernet0/0/9] quit
[RouterA] ip route-static vpn-instance wan1 10.172.0.0 255.255.0.0 192.168.10.254
[RouterA] ip route-static vpn-instance wan2 10.172.0.0 255.255.0.0 192.168.20.254
```

配置RouterC物理接口的IP地址及静态路由。

```
<Huawei> system-view
[Huawei] sysname RouterC
[RouterC] interface XGigabitEthernet0/0/0
[RouterC-XGigabitEthernet0/0/0] ip address 10.172.20.2 255.255.255.0
[RouterC-XGigabitEthernet0/0/0] quit
[RouterC] ip route-static 192.168.0.0 255.255.0.0 10.172.20.1
```

配置RouterD物理接口的IP地址及静态路由。

```
<Huawei> system-view
[Huawei] sysname RouterD
[RouterD] interface XGigabitEthernet0/0/0
[RouterD-XGigabitEthernet0/0/0] ip address 10.172.10.2 255.255.255.0
[RouterD-XGigabitEthernet0/0/0] quit
[RouterD] ip route-static 192.168.0.0 255.255.0.0 10.172.10.1
```

2. 在RouterA和RouterC、RouterD之间部署GRE隧道，通过静态路由指定到达对端的报文通过GRE隧道转发，实现Underlay传输网络互通，用于三层报文多发选收。

   # 在RouterA上创建Tunnel接口，并配置接口路由。

```
[RouterA] interface Tunnel0/0/0
[RouterA-Tunnel0/0/0] description key1
[RouterA-Tunnel0/0/0] ip address 172.16.1.1 255.255.255.0
[RouterA-Tunnel0/0/0] tunnel-protocol gre
[RouterA-Tunnel0/0/0] gre key plain 1
[RouterA-Tunnel0/0/0] source GigabitEthernet0/0/8
[RouterA-Tunnel0/0/0] destination vpn-instance wan1 10.172.10.2
[RouterA-Tunnel0/0/0] quit
[RouterA] interface Tunnel0/0/1
[RouterA-Tunnel0/0/1] description key2
[RouterA-Tunnel0/0/1] ip address 172.16.2.1 255.255.255.0
[RouterA-Tunnel0/0/1] tunnel-protocol gre
[RouterA-Tunnel0/0/1] gre key plain 2
[RouterA-Tunnel0/0/1] source GigabitEthernet0/0/9
[RouterA-Tunnel0/0/1] destination vpn-instance wan2 10.172.10.2
[RouterA-Tunnel0/0/1] quit
[RouterA] interface Tunnel0/0/2
[RouterA-Tunnel0/0/2] ip address 172.16.3.1 255.255.255.0
[RouterA-Tunnel0/0/2] tunnel-protocol gre
[RouterA-Tunnel0/0/2] gre key plain 3
[RouterA-Tunnel0/0/2] source GigabitEthernet0/0/8
[RouterA-Tunnel0/0/2] destination vpn-instance wan1 10.172.20.2
[RouterA-Tunnel0/0/2] quit
[RouterA] interface Tunnel0/0/3
[RouterA-Tunnel0/0/3] ip address 172.16.4.1 255.255.255.0
[RouterA-Tunnel0/0/3] tunnel-protocol gre
[RouterA-Tunnel0/0/3] gre key plain 4
[RouterA-Tunnel0/0/3] source GigabitEthernet0/0/9
```

 版权所有 © 华为技术有限公司

```
[RouterA-Tunnel0/0/3] destination vpn-instance wan2 10.172.20.2
[RouterA-Tunnel0/0/3] quit
```

在RouterC上创建Tunnel接口，并配置接口路由。

```
[RouterC] interface Tunnel0/0/0
[RouterC-Tunnel0/0/0] ip address 172.16.3.2 255.255.255.0
[RouterC-Tunnel0/0/0] tunnel-protocol gre
[RouterC-Tunnel0/0/0] gre key plain 3
[RouterC-Tunnel0/0/0] source XGigabitEthernet0/0/0
[RouterC-Tunnel0/0/0] destination 192.168.10.1
[RouterC-Tunnel0/0/0] quit
[RouterC] interface Tunnel0/0/1
[RouterC-Tunnel0/0/1] ip address 172.16.4.2 255.255.255.0
[RouterC-Tunnel0/0/1] tunnel-protocol gre
[RouterC-Tunnel0/0/1] gre key plain 4
[RouterC-Tunnel0/0/1] source XGigabitEthernet0/0/0
[RouterC-Tunnel0/0/1] destination 192.168.20.1
[RouterC-Tunnel0/0/1] quit
```

在RouterD上创建Tunnel接口，并配置接口路由。

```
[RouterD] interface Tunnel0/0/0
[RouterD-Tunnel0/0/0] description key1
[RouterD-Tunnel0/0/0] ip address 172.16.1.2 255.255.255.0
[RouterD-Tunnel0/0/0] tunnel-protocol gre
[RouterD-Tunnel0/0/0] gre key plain 1
[RouterD-Tunnel0/0/0] source XGigabitEthernet0/0/0
[RouterD-Tunnel0/0/0] destination 192.168.10.1
[RouterD-Tunnel0/0/0] quit
[RouterD] interface Tunnel0/0/1
[RouterD-Tunnel0/0/1] description key2
[RouterD-Tunnel0/0/1] ip address 172.16.2.2 255.255.255.0
[RouterD-Tunnel0/0/1] tunnel-protocol gre
[RouterD-Tunnel0/0/1] gre key plain 2
[RouterD-Tunnel0/0/1] source XGigabitEthernet0/0/0
[RouterD-Tunnel0/0/1] destination 192.168.20.1
[RouterD-Tunnel0/0/1] quit
```

配置完成后Tunnel接口状态变为Up，Tunnel接口之间可以Ping通，直连隧道建立。以RouterA的显示为例。

```
<RouterA> ping 172.16.1.2
  PING 172.16.1.2: 56  data bytes, press CTRL_C to break
    Reply from 172.16.1.2: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 172.16.1.2: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 172.16.1.2: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 172.16.1.2: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 172.16.1.2: bytes=56 Sequence=5 ttl=255 time=1 ms
  --- 172.16.1.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/1 ms
```

3. 配置Overlay业务网络互通。在LAN侧的接口和WAN侧的Tunnel接口上分别绑定二层VE接口，实现以太报文通过GRE隧道进行透传，且配置WAN侧Tunnel接口的源接口为Loopback接口用于实现二层报文多发选收。

   # 配置RouterA。

```
[RouterA] interface LoopBack0
[RouterA-LoopBack0] ip address 1.1.1.1 255.255.255.0
[RouterA-LoopBack0] quit
[RouterA] vlan batch 100 200
[RouterA] interface Virtual-Ethernet0/0/0
[RouterA-Virtual-Ethernet0/0/0] portswitch
[RouterA-Virtual-Ethernet0/0/0] port link-type access
[RouterA-Virtual-Ethernet0/0/0] port default vlan 200
[RouterA-Virtual-Ethernet0/0/0] quit
[RouterA] interface Virtual-Ethernet0/0/1
[RouterA-Virtual-Ethernet0/0/1] portswitch
[RouterA-Virtual-Ethernet0/0/1] port link-type trunk
```

 版权所有 © 华为技术有限公司

```
[RouterA-Virtual-Ethernet0/0/1] undo port trunk allow-pass vlan 1
[RouterA-Virtual-Ethernet0/0/1] port trunk allow-pass vlan 200
[RouterA-Virtual-Ethernet0/0/1] quit
[RouterA] interface gigabitethernet 0/0/1
[RouterA-GigabitEthernet0/0/1] undo portswitch
[RouterA-GigabitEthernet0/0/1] tcp adjust-mss 1200
[RouterA-GigabitEthernet0/0/1] map interface Virtual-Ethernet0/0/0
[RouterA-GigabitEthernet0/0/1] quit
[RouterA] interface Tunnel0/0/4
[RouterA-Tunnel0/0/4] ip address 172.16.5.1 255.255.255.0
[RouterA-Tunnel0/0/4] tunnel-protocol gre
[RouterA-Tunnel0/0/4] gre key plain 5
[RouterA-Tunnel0/0/4] source LoopBack0
[RouterA-Tunnel0/0/4] destination 192.168.255.254
[RouterA-Tunnel0/0/4] map interface Virtual-Ethernet0/0/1
[RouterA-Tunnel0/0/4] quit
```

配置RouterC。

- 配置RSTP功能，破除二层网络中的环路。
- 配置Eth-Trunk保证连接的可靠性。

```
[RouterC] vlan batch 100 200
[RouterC] interface Eth-Trunk0
[RouterC-Eth-Trunk0] port link-type trunk
[RouterC-Eth-Trunk0] undo port trunk allow-pass vlan 1
[RouterC-Eth-Trunk0] port trunk allow-pass vlan 100 200
[RouterC-Eth-Trunk0] quit
[RouterC] interface gigabitethernet0/0/1
[RouterC-GigabitEthernet0/0/1] portswitch
[RouterC-GigabitEthernet0/0/1] eth-trunk 0
[RouterC-GigabitEthernet0/0/1] quit
[RouterC] interface gigabitethernet0/0/2
[RouterC-GigabitEthernet0/0/2] portswitch
[RouterC-GigabitEthernet0/0/2] eth-trunk 0
[RouterC-GigabitEthernet0/0/2] quit
[RouterC] interface gigabitethernet0/0/4
[RouterC-GigabitEthernet0/0/4] portswitch
[RouterC-GigabitEthernet0/0/4] port link-type trunk
[RouterC-GigabitEthernet0/0/4] port trunk allow-pass vlan 100 200
[RouterC-GigabitEthernet0/0/4] quit
[RouterC] interface Virtual-Ethernet0/0/0
[RouterC-Virtual-Ethernet0/0/0] portswitch
[RouterC-Virtual-Ethernet0/0/0] port link-type trunk
[RouterC-Virtual-Ethernet0/0/0] undo port trunk allow-pass vlan 1
[RouterC-Virtual-Ethernet0/0/0] port trunk allow-pass vlan 200
[RouterC-Virtual-Ethernet0/0/0] quit
[RouterC] interface Virtual-Ethernet0/0/1
[RouterC-Virtual-Ethernet0/0/1] portswitch
[RouterC-Virtual-Ethernet0/0/1] port link-type trunk
[RouterC-Virtual-Ethernet0/0/1] undo port trunk allow-pass vlan 1
[RouterC-Virtual-Ethernet0/0/1] port trunk allow-pass vlan 200
[RouterC-Virtual-Ethernet0/0/1] quit
[RouterC] interface Vlanif200
[RouterC-Vlanif200] map interface Virtual-Ethernet0/0/0
[RouterC-Vlanif200] quit
[RouterC] interface Tunnel0/0/2
[RouterC-Tunnel0/0/2] ip address 172.16.5.2 255.255.255.0
[RouterC-Tunnel0/0/2] tunnel-protocol gre
[RouterC-Tunnel0/0/2] gre key plain 5
[RouterC-Tunnel0/0/2] source 192.168.255.254
[RouterC-Tunnel0/0/2] destination 1.1.1.1
[RouterC-Tunnel0/0/2] map interface Virtual-Ethernet0/0/1
[RouterC-Tunnel0/0/2] quit
```

配置RouterD。

- 配置RSTP功能，破除二层网络中的环路。
- 配置Eth-Trunk保证连接的可靠性。

 版权所有 © 华为技术有限公司

```
[RouterD] stp instance 0 root primary
[RouterD] vlan batch 100 200
[RouterD] interface Eth-Trunk0
[RouterD-Eth-Trunk0] port link-type trunk
[RouterD-Eth-Trunk0] undo port trunk allow-pass vlan 1
[RouterD-Eth-Trunk0] port trunk allow-pass vlan 100 200
[RouterD-Eth-Trunk0] quit
[RouterD] interface gigabitethernet0/0/0
[RouterD-GigabitEthernet0/0/0] portswitch
[RouterD-GigabitEthernet0/0/0] eth-trunk 0
[RouterD-GigabitEthernet0/0/0] quit
[RouterD] interface gigabitethernet0/0/1
[RouterD-GigabitEthernet0/0/1] portswitch
[RouterD-GigabitEthernet0/0/1] eth-trunk 0
[RouterD-GigabitEthernet0/0/1] quit
[RouterD] interface XGigabitEthernet0/0/1
[RouterD-XGigabitEthernet0/0/1] portswitch
[RouterD-XGigabitEthernet0/0/1] port link-type trunk
[RouterD-XGigabitEthernet0/0/1] undo port trunk allow-pass vlan 1
[RouterD-XGigabitEthernet0/0/1] port trunk allow-pass vlan 100 200
[RouterD-XGigabitEthernet0/0/1] quit
[RouterD] interface Virtual-Ethernet0/0/0
[RouterD-Virtual-Ethernet0/0/0] portswitch
[RouterD-Virtual-Ethernet0/0/0] port link-type trunk
[RouterD-Virtual-Ethernet0/0/0] undo port trunk allow-pass vlan 1
[RouterD-Virtual-Ethernet0/0/0] port trunk allow-pass vlan 200
[RouterD-Virtual-Ethernet0/0/0] quit
[RouterD] interface Virtual-Ethernet0/0/1
[RouterD-Virtual-Ethernet0/0/1] portswitch
[RouterD-Virtual-Ethernet0/0/1] port link-type trunk
[RouterD-Virtual-Ethernet0/0/1] undo port trunk allow-pass vlan 1
[RouterD-Virtual-Ethernet0/0/1] port trunk allow-pass vlan 200
[RouterD-Virtual-Ethernet0/0/1] quit
[RouterD] interface Vlanif200
[RouterD-Vlanif200] map interface Virtual-Ethernet0/0/0
[RouterD-Vlanif200] quit
[RouterD] interface Tunnel0/0/2
[RouterD-Tunnel0/0/2] ip address 172.16.5.2 255.255.255.0
[RouterD-Tunnel0/0/2] tunnel-protocol gre
[RouterD-Tunnel0/0/2] gre key plain 5
[RouterD-Tunnel0/0/2] source 192.168.255.254
[RouterD-Tunnel0/0/2] destination 1.1.1.1
[RouterD-Tunnel0/0/2] map interface Virtual-Ethernet0/0/1
[RouterD-Tunnel0/0/2] quit
```

配置RouterE的接口加入VLAN。

```
<Huawei> system-view
[Huawei] sysname RouterE
[RouterE] interface gigabitethernet 0/0/0
[RouterE-GigabitEthernet0/0/0] stp disable
[RouterE-GigabitEthernet0/0/0] port link-type trunk
[RouterE-GigabitEthernet0/0/0] undo port trunk allow-pass vlan 1
[RouterE-GigabitEthernet0/0/0] port trunk allow-pass vlan 200
[RouterE-GigabitEthernet0/0/0] quit
[RouterE] interface gigabitethernet 0/0/1
[RouterE-GigabitEthernet0/0/1] port link-type trunk
[RouterE-GigabitEthernet0/0/1] undo port trunk allow-pass vlan 1
[RouterE-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 200
[RouterE-GigabitEthernet0/0/1] quit
[RouterE] interface gigabitethernet 0/0/2
[RouterE-GigabitEthernet0/0/2] port link-type trunk
[RouterE-GigabitEthernet0/0/2] undo port trunk allow-pass vlan 1
[RouterE-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 200
[RouterE-GigabitEthernet0/0/2] quit
```

4. 配置VRRP主备备份。RouterD上配置较高优先级，作为Master设备承担流量转发；RouterC作为备用路由器，实现网关冗余备份。

   # 配置RouterC。

 版权所有 © 华为技术有限公司

```
[RouterC] interface Vlanif100
[RouterC-Vlanif100] ip address 192.168.255.2 255.255.255.0
[RouterC-Vlanif100] vrrp vrid 1 virtual-ip 192.168.255.254
[RouterC-Vlanif100] quit
```

配置RouterD。

```
[RouterD] interface Vlanif100
[RouterD-Vlanif100] ip address 192.168.255.1 255.255.255.0
[RouterD-Vlanif100] vrrp vrid 1 virtual-ip 192.168.255.254
[RouterD-Vlanif100] vrrp vrid 1 priority 120
[RouterD-Vlanif100] vrrp vrid 1 track interface GigabitEthernet0/0/0 reduced 40
[RouterD-Vlanif100] quit
```

5. 配置BFD会话，实现设备间链路故障的快速检测。

   # 配置RouterA。

```
[RouterA] bfd
[RouterA-bfd] quit
[RouterA] bfd 1 bind peer-ip 172.16.1.2 source-ip 172.16.1.1
[RouterA-bfd-session-1] discriminator local 1
[RouterA-bfd-session-1] discriminator remote 2
[RouterA-bfd-session-1] commit
[RouterA-bfd-session-1] quit
[RouterA] bfd 2 bind peer-ip 172.16.2.2 source-ip 172.16.2.1
[RouterA-bfd-session-2] discriminator local 3
[RouterA-bfd-session-2] discriminator remote 4
[RouterA-bfd-session-2] commit
[RouterA-bfd-session-2] quit
[RouterA] bfd 3 bind peer-ip 172.16.3.2 source-ip 172.16.3.1
[RouterA-bfd-session-3] discriminator local 5
[RouterA-bfd-session-3] discriminator remote 6
[RouterA-bfd-session-3] commit
[RouterA-bfd-session-3] quit
[RouterA] bfd 4 bind peer-ip 172.16.4.2 source-ip 172.16.4.1
[RouterA-bfd-session-4] discriminator local 7
[RouterA-bfd-session-4] discriminator remote 8
[RouterA-bfd-session-4] commit
[RouterA-bfd-session-4] quit
```

   # 配置RouterC。

```
[RouterC] bfd
[RouterC-bfd] quit
[RouterC] bfd 1 bind peer-ip 172.16.3.1 source-ip 172.16.3.2
[RouterC-bfd-session-1] discriminator local 6
[RouterC-bfd-session-1] discriminator remote 5
[RouterC-bfd-session-1] commit
[RouterC-bfd-session-1] quit
[RouterC] bfd 2 bind peer-ip 172.16.4.1 source-ip 172.16.4.2
[RouterC-bfd-session-2] discriminator local 8
[RouterC-bfd-session-2] discriminator remote 7
[RouterC-bfd-session-2] commit
[RouterC-bfd-session-2] quit
```

   # 配置RouterD。

```
[RouterD] bfd
[RouterD-bfd] quit
[RouterD] bfd 1 bind peer-ip 172.16.1.1 source-ip 172.16.1.2
[RouterD-bfd-session-1] discriminator local 2
[RouterD-bfd-session-1] discriminator remote 1
[RouterD-bfd-session-1] commit
[RouterD-bfd-session-1] quit
[RouterD] bfd 2 bind peer-ip 172.16.2.1 source-ip 172.16.2.2
[RouterD-bfd-session-2] discriminator local 4
[RouterD-bfd-session-2] discriminator remote 3
[RouterD-bfd-session-2] commit
[RouterD-bfd-session-2] quit
```

   # 配置完成后，执行**display bfd session all**命令，可以看到建立了BFD会话，且状态为Up。以RouterA上的显示为例。

 版权所有 © 华为技术有限公司

```
<RouterA> display bfd session all
--------------------------------------------------------------------------------
Local Remote     PeerIpAddr      State     Type        InterfaceName
--------------------------------------------------------------------------------
1     2          172.16.1.2      Up        S_IP_PEER       -
3     4          172.16.2.2      Up        S_IP_PEER       -
5     6          172.16.3.2      Up        S_IP_PEER       -
7     8          172.16.4.2      Up        S_IP_PEER       -
--------------------------------------------------------------------------------
    Total UP/DOWN Session Number : 4/0
```

6. 在Tunnel接口上配置多发选收。

   # 配置RouterA。

```
[RouterA] replication path-group 1
[RouterA-replication-path-group-1] path Tunnel 0/0/1 priority 1
[RouterA-replication-path-group-1] quit
[RouterA] replication path-group 2
[RouterA-replication-path-group-2] path Tunnel 0/0/3 priority 1
[RouterA-replication-path-group-2] quit
[RouterA] interface tunnel 0/0/0
[RouterA-Tunnel0/0/0] replication path-group 1
[RouterA-Tunnel0/0/0] quit
[RouterA] interface tunnel0/0/2
[RouterA-Tunnel0/0/2] replication path-group 2
[RouterA-Tunnel0/0/2] quit
```

   # 配置RouterC。

```
[RouterC] replication path-group 1
[RouterC-replication-path-group-1] path Tunnel 0/0/1 priority 1
[RouterC-replication-path-group-1] quit
[RouterC] interface tunnel0/0/0
[RouterC-Tunnel0/0/0] replication path-group 1
[RouterC-Tunnel0/0/0] quit
```

   # 配置RouterD。

```
[RouterD] replication path-group 1
[RouterD-replication-path-group-1] path Tunnel 0/0/1 priority 1
[RouterD-replication-path-group-1] quit
[RouterD] interface tunnel0/0/0
[RouterD-Tunnel0/0/0] replication path-group 1
[RouterD-Tunnel0/0/0] quit
```

   # 配置完成后，执行**display replication path-group**命令可以看到链路组的所有链路状态和选路结果。以RouterA的显示为例。

```
[RouterA] display replication path-group 1
------------------------------------------------------------
Path member       Priority     Track info     Path state
Tunnel0/0/1       1            -              UP
------------------------------------------------------------
[RouterA] display replication path-group
--------------------------------------------------------------------------------
Group name                    Replication link1     Replication link2
1                             Tunnel0/0/1           -
--------------------------------------------------------------------------------
```

7. 配置静态路由，并联动BFD会话。

   # 配置RouterA。

```
[RouterA] ip route-static 192.168.255.254 255.255.255.255 Tunnel0/0/0 track bfd-session 1
[RouterA] ip route-static 192.168.255.254 255.255.255.255 Tunnel0/0/1 preference 70 track bfd-session 2
[RouterA] ip route-static 192.168.255.254 255.255.255.255 Tunnel0/0/2 preference 80 track bfd-session 3
[RouterA] ip route-static 192.168.255.254 255.255.255.255 Tunnel0/0/3 preference 90 track bfd-session 4
```

   # 配置RouterC。

```
[RouterC] ip route-static 1.1.1.1 255.255.255.255 Tunnel0/0/0 track bfd-session 1
[RouterC] ip route-static 1.1.1.1 255.255.255.255 Tunnel0/0/1 preference 70 track bfd-session 2
```

 版权所有 © 华为技术有限公司

配置RouterD。

```
[RouterD] ip route-static 1.1.1.1 255.255.255.255 Tunnel0/0/0 track bfd-session 1
[RouterD] ip route-static 1.1.1.1 255.255.255.255 Tunnel0/0/1 preference 70 track bfd-session 2
```

配置文件

- RouterA的配置文件

```
#
vlan batch 100 200
#
ip vpn-instance wan1
 ipv4-family
  route-distinguisher 192.168.10.1:0
#
ip vpn-instance wan2
 ipv4-family
  route-distinguisher 192.168.20.1:0
#
bfd
#
interface GigabitEthernet0/0/1
 undo portswitch
 tcp adjust-mss 1200
 map interface Virtual-Ethernet0/0/0
#
interface GigabitEthernet0/0/8
 ip binding vpn-instance wan1
 ip address 192.168.10.1 255.255.255.0
#
interface GigabitEthernet0/0/9
 ip binding vpn-instance wan2
 ip address 192.168.20.1 255.255.255.0
#
interface Virtual-Ethernet0/0/0
 portswitch
 port link-type access
 port default vlan 200
#
interface Virtual-Ethernet0/0/1
 portswitch
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 200
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.0
#
interface Tunnel0/0/0
 description key1
 ip address 172.16.1.1 255.255.255.0
 tunnel-protocol gre
 gre key plain 1
 source GigabitEthernet0/0/8
 destination vpn-instance wan1 10.172.10.2
 replication path-group 1
#
interface Tunnel0/0/1
 description key2
 ip address 172.16.2.1 255.255.255.0
 tunnel-protocol gre
 gre key plain 2
 source GigabitEthernet0/0/9
 destination vpn-instance wan2 10.172.10.2
#
interface Tunnel0/0/2
 ip address 172.16.3.1 255.255.255.0
 tunnel-protocol gre
 gre key plain 3
```

 版权所有 © 华为技术有限公司

```
 source GigabitEthernet0/0/8
 destination vpn-instance wan1 10.172.20.2
 replication path-group 2
#
interface Tunnel0/0/3
 ip address 172.16.4.1 255.255.255.0
 tunnel-protocol gre
 gre key plain 4
 source GigabitEthernet0/0/9
 destination vpn-instance wan2 10.172.20.2
#
interface Tunnel0/0/4
 ip address 172.16.5.1 255.255.255.0
 tunnel-protocol gre
 gre key plain 5
 source LoopBack0
 destination 192.168.255.254
 map interface Virtual-Ethernet0/0/1
#
bfd 1 bind peer-ip 172.16.1.2 source-ip 172.16.1.1
 discriminator local 1
 discriminator remote 2
 commit
#
bfd 2 bind peer-ip 172.16.2.2 source-ip 172.16.2.1
 discriminator local 3
 discriminator remote 4
 commit
#
bfd 3 bind peer-ip 172.16.3.2 source-ip 172.16.3.1
 discriminator local 5
 discriminator remote 6
 commit
#
bfd 4 bind peer-ip 172.16.4.2 source-ip 172.16.4.1
 discriminator local 7
 discriminator remote 8
 commit
#
ip route-static 192.168.255.254 255.255.255.255 Tunnel0/0/0 track bfd-session 1
ip route-static 192.168.255.254 255.255.255.255 Tunnel0/0/1 preference 70 track bfd-session 2
ip route-static 192.168.255.254 255.255.255.255 Tunnel0/0/2 preference 80 track bfd-session 3
ip route-static 192.168.255.254 255.255.255.255 Tunnel0/0/3 preference 90 track bfd-session 4
ip route-static vpn-instance wan1 10.172.0.0 255.255.0.0 192.168.10.254
ip route-static vpn-instance wan2 10.172.0.0 255.255.0.0 192.168.20.254
#
replication path-group 1
 path Tunnel0/0/1 priority 1
replication path-group 2
 path Tunnel0/0/3 priority 1
#
```

- RouterC的配置文件

```
#
vlan batch 100 200
#
bfd
#
interface Vlanif100
 ip address 192.168.255.2 255.255.255.0
 vrrp vrid 1 virtual-ip 192.168.255.254
#
interface Vlanif200
 map interface Virtual-Ethernet0/0/0
#
interface Eth-Trunk0
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 100 200
#
```

 版权所有 © 华为技术有限公司

```
interface GigabitEthernet0/0/1
 portswitch
 eth-trunk 0
#
interface GigabitEthernet0/0/2
 portswitch
 eth-trunk 0
#
interface GigabitEthernet0/0/4
 portswitch
 port link-type trunk
 port trunk allow-pass vlan 100 200
#
interface XGigabitEthernet0/0/0
 ip address 10.172.20.2 255.255.255.0
#
interface Virtual-Ethernet0/0/0
 portswitch
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 200
#
interface Virtual-Ethernet0/0/1
 portswitch
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 200
#
interface Tunnel0/0/0
 ip address 172.16.3.2 255.255.255.0
 tunnel-protocol gre
 gre key plain 3
 source XGigabitEthernet0/0/0
 destination 192.168.10.1
 replication path-group 1
#
interface Tunnel0/0/1
 ip address 172.16.4.2 255.255.255.0
 tunnel-protocol gre
 gre key plain 4
 source XGigabitEthernet0/0/0
 destination 192.168.20.1
#
interface Tunnel0/0/2
 ip address 172.16.5.2 255.255.255.0
 tunnel-protocol gre
 gre key plain 5
 source 192.168.255.254
 destination 1.1.1.1
 map interface Virtual-Ethernet0/0/1
#
bfd 1 bind peer-ip 172.16.3.1 source-ip 172.16.3.2
 discriminator local 6
 discriminator remote 5
 commit
#
bfd 2 bind peer-ip 172.16.4.1 source-ip 172.16.4.2
 discriminator local 8
 discriminator remote 7
 commit
#
ip route-static 1.1.1.1 255.255.255.255 Tunnel0/0/0 track bfd-session 1
ip route-static 1.1.1.1 255.255.255.255 Tunnel0/0/1 preference 70 track bfd-session 2
ip route-static 192.168.0.0 255.255.0.0 10.172.20.1
#
replication path-group 1
 path Tunnel0/0/1 priority 1
#
```

- RouterD的配置文件

 版权所有 © 华为技术有限公司

```
#
vlan batch 100 200
#
stp instance 0 root primary
#
interface Vlanif100
 ip address 192.168.255.1 255.255.255.0
 vrrp vrid 1 virtual-ip 192.168.255.254
 vrrp vrid 1 priority 120
 vrrp vrid 1 track interface XGigabitEthernet0/0/0 reduced 40
#
interface Vlanif200
 map interface Virtual-Ethernet0/0/0
#
interface Eth-Trunk0
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 100 200
#
interface GigabitEthernet0/0/0
 portswitch
 eth-trunk 0
#
interface GigabitEthernet0/0/1
 portswitch
 eth-trunk 0
#
interface XGigabitEthernet0/0/0
 ip address 10.172.10.2 255.255.255.0
#
interface XGigabitEthernet0/0/1
 portswitch
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 100 200
#
interface Virtual-Ethernet0/0/0
 portswitch
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 200
#
interface Virtual-Ethernet0/0/1
 portswitch
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 200
#
interface Tunnel0/0/0
 description key1
 ip address 172.16.1.2 255.255.255.0
 tunnel-protocol gre
 gre key plain 1
 source XGigabitEthernet0/0/0
 destination 192.168.10.1
 replication path-group 1
#
interface Tunnel0/0/1
 description key2
 ip address 172.16.2.2 255.255.255.0
 tunnel-protocol gre
 gre key plain 2
 source XGigabitEthernet0/0/0
 destination 192.168.20.1
#
interface Tunnel0/0/2
 ip address 172.16.5.2 255.255.255.0
 tunnel-protocol gre
 gre key plain 5
```

 版权所有 © 华为技术有限公司

```
 source 192.168.255.254
 destination 1.1.1.1
 map interface Virtual-Ethernet0/0/1
#
bfd 1 bind peer-ip 172.16.1.1 source-ip 172.16.1.2
 discriminator local 2
 discriminator remote 1
 commit
#
bfd 2 bind peer-ip 172.16.2.1 source-ip 172.16.2.2
 discriminator local 4
 discriminator remote 3
 commit
#
ip route-static 1.1.1.1 255.255.255.255 Tunnel0/0/0 track bfd-session 1
ip route-static 1.1.1.1 255.255.255.255 Tunnel0/0/1 preference 70 track bfd-session 2
ip route-static 192.168.0.0 255.255.0.0 10.172.10.1
#
replication path-group 1
 path Tunnel0/0/1 priority 1
#
```

- RouterE的配置文件

```
#
interface GigabitEthernet0/0/0
 stp disable
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 200
#
interface GigabitEthernet0/0/1
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 100 200
#
interface GigabitEthernet0/0/2
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 100 200
#
```

7.2.11 配置二层重定向多发选收示例（5G CPE 场景）

组网需求

说明

AR设备配置多个GE子接口与5G CPE（N5368X）桥接模式对接时，由于CPE使用场景约束，AR设备需要使用子接口下的MAC地址修改功能保证CPE学习MAC地址的唯一性。

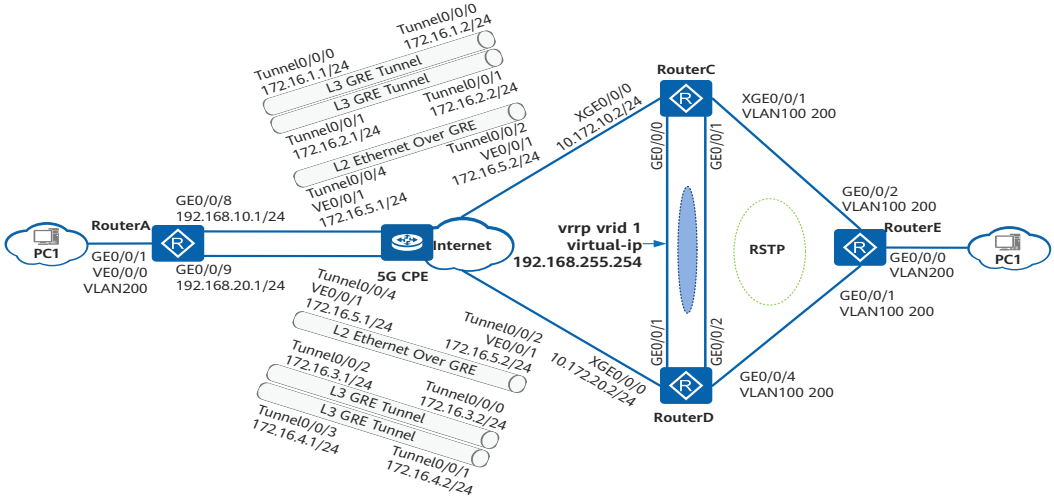
如图7-14所示，RouterA为企业分支网关，RouterC和RouterD为企业总部网关，用户希望实现：

- 正常情况下，RouterC为Master设备承担流量转发，当RouterC故障时，RouterD接替作为网关继续进行工作，实现网关的冗余备份。
- 分支和总部可以传输原始以太报文（如工业控制的PLC报文），采用二层隧道封装。
- 分支网关RouterA接口GE0/0/8所在链路作为主链路，GE0/0/9所在链路作为复制链路。
- 如果RouterA主链路故障，通过复制链路转发报文，优选RouterC进行流量转发。如果总部RouterC网关LAN侧网络或中间链路故障，RouterA选择RouterD进行流量转发。

 版权所有 © 华为技术有限公司

- 报文复制过程忽略接口状态和路由状态，最大程度保证业务连续性。

图 7-14 配置二层重定向多发选收组网图



数据准备

表 7-18 数据准备表

项目	数据	说明
分支RouterA LAN侧接口信息	LAN侧物理接口：GE0/0/1 绑定的VE接口：VE0/0/0 所属VLAN：200	分支RouterA与分支用户之间的链路信息。
分支RouterA WAN侧接口信息	主链路物理接口：GE0/0/8 IP地址：192.168.10.1/24 绑定VPN实例：wan1 复制链路物理接口：GE0/0/9 IP地址：192.168.20.1/24 绑定VPN实例：wan2	分支RouterA与5G CPE之间的链路信息。
分支RouterA Tunnel0/0/0接口信息	IP地址：172.16.1.1/24 源接口：GE0/0/8	分支RouterA和总部RouterC之间的L3 GRE隧道信息。
分支RouterA Tunnel0/0/1接口信息	IP地址：172.16.2.1/24 源接口：GE0/0/9	分支RouterA和总部RouterC之间的L3 GRE隧道信息。
分支RouterA Tunnel0/0/2接口信息	IP地址：172.16.3.1/24 源接口：GE0/0/8	分支RouterA和总部RouterD之间的L3 GRE隧道信息。

版权所有 © 华为技术有限公司

项目	数据	说明
分支RouterA Tunnel0/0/3接口信息	IP地址：172.16.4.1/24 源接口：GE0/0/9	分支RouterA和总部RouterD之间的L3 GRE隧道信息。
分支RouterA Tunnel0/0/4接口信息	IP地址：172.16.5.1/24 源接口：LoopBack0 绑定的VE接口：VE0/0/1	分支RouterA和总部RouterC以及RouterD之间的Ethernet over GRE隧道信息。
总部RouterC LAN侧接口信息	LAN侧物理接口：XGE0/0/1 所属VLAN：100、200	总部RouterC与分支RouterE之间的链路信息。
总部RouterC WAN侧接口信息	WAN侧物理接口：XGE0/0/0 IP地址：10.172.10.2/24	总部RouterC与Internet之间的链路信息。
总部RouterC Tunnel0/0/0接口信息	IP地址：172.16.1.2/24 源接口：XGE0/0/0	总部RouterC和分支RouterA之间的L3 GRE隧道信息。
总部RouterC Tunnel0/0/1接口信息	IP地址：172.16.2.2/24 源接口：XGE0/0/0	总部RouterC和分支RouterA之间的L3 GRE隧道信息。
总部RouterC Tunnel0/0/2接口信息	IP地址：172.16.5.2/24 源地址：192.168.255.254（VRRP备份组的虚拟IP地址） 绑定的VE接口：VE0/0/1	总部RouterC和分支RouterA之间的Ethernet over GRE隧道信息。
总部RouterD LAN侧接口信息	LAN侧物理接口：GE0/0/4 所属VLAN：100、200	总部RouterD与分支RouterE之间的链路信息。
总部RouterD WAN侧接口信息	WAN侧物理接口：XGE0/0/0 IP地址：10.172.20.2/24	总部RouterD与Internet之间的链路信息。
总部RouterD Tunnel0/0/0接口信息	IP地址：172.16.3.2/24 源接口：XGE0/0/0	总部RouterD和分支RouterA之间的L3 GRE隧道信息。
总部RouterD Tunnel0/0/1接口信息	IP地址：172.16.4.2/24 源接口：XGE0/0/0	总部RouterD和分支RouterA之间的L3 GRE隧道信息。
总部RouterD Tunnel0/0/2接口信息	IP地址：172.16.5.2/24 源地址：192.168.255.254（VRRP备份组的虚拟IP地址） 绑定的VE接口：VE0/0/1	总部RouterD和分支RouterA之间的Ethernet over GRE隧道信息。

版权所有 © 华为技术有限公司

项目	数据	说明
分支RouterE LAN侧接口信息	LAN侧物理接口1：GE0/0/0 所属VLAN：200 LAN侧物理接口2：GE0/0/1 所属VLAN：100、200 LAN侧物理接口3：GE0/0/2 所属VLAN：100、200	GE0/0/0为分支RouterE与分支用户之间的接口。 GE0/0/1为分支RouterE与总部RouterD之间的接口。 GE0/0/2为分支RouterE与总部RouterC之间的接口。

配置思路

本例配置的主要思路是：

1. 配置设备物理接口的IP地址及静态路由，实现设备之间三层网络互通，同时，在RouterA上创建不同的VPN实例，实现不同VPN间的业务隔离。
2. 在RouterA和RouterC、RouterD之间部署GRE隧道，通过静态路由指定到达对端的报文通过GRE隧道转发，实现Underlay传输网络互通，用于三层报文多发选收。
3. 配置Overlay业务网络互通。
   - 在LAN侧的接口和WAN侧的Tunnel接口上分别绑定二层VE接口，实现以太报文通过GRE隧道进行透传，且配置WAN侧Tunnel接口的源接口为Loopback接口用于实现二层报文多发选收。
   - RouterC和RouterD配置RSTP功能，破除二层网络中的环路。
   - RouterC和RouterD配置Eth-Trunk保证连接的可靠性。
4. 在RouterA、RouterC和RouterD上分别配置BFD会话，实现设备间链路故障的快速检测。
5. 在RouterC和RouterD上配置VRRP备份组。RouterC上配置较高优先级，作为Master设备承担流量转发；RouterD作为备用路由器，实现网关冗余备份，同时，配置VRRP与BFD联动，实现链路故障时VRRP备份组快速切换。
6. 在源接口为Loopback接口的内层Ethernet Over GRE隧道上配置重定向多发选收功能，并指定链路组不根据链路状态刷新选路信息，避免路由切换过程中出现的丢包现象，最大程度保证业务连续性。
7. 配置设备间使用OSPF路由，且使能OSPF BFD检测机制，当链路出现故障时，BFD能够快速检测到故障并通告给OSPF协议，使业务流量使用等价链路传送。

说明

用户可以根据现网实际情况配置BFD报文的接收和发送间隔。

操作步骤

1. 配置设备物理接口的IP地址及静态路由，实现设备之间三层网络互通。

   # 配置RouterA物理接口的IP地址及静态路由，在RouterA上创建不同的VPN实例，实现不同VPN间的业务隔离。

 版权所有 © 华为技术有限公司

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] router id 1.1.1.1
[RouterA] ip vpn-instance wan1
[RouterA-vpn-instance-wan1] ipv4-family
[RouterA-vpn-instance-wan1-af-ipv4] route-distinguisher 192.168.10.1:0
[RouterA-vpn-instance-wan1-af-ipv4] quit
[RouterA-vpn-instance-wan1] quit
[RouterA] ip vpn-instance wan2
[RouterA-vpn-instance-wan2] ipv4-family
[RouterA-vpn-instance-wan2-af-ipv4] route-distinguisher 192.168.20.1:0
[RouterA-vpn-instance-wan2-af-ipv4] quit
[RouterA-vpn-instance-wan2] quit
[RouterA] interface gigabitethernet 0/0/8
[RouterA-GigabitEthernet0/0/8] ip binding vpn-instance wan1
[RouterA-GigabitEthernet0/0/8] ip address 192.168.10.1 255.255.255.0
[RouterA-GigabitEthernet0/0/8] quit
[RouterA] interface gigabitethernet 0/0/9
[RouterA-GigabitEthernet0/0/9] ip binding vpn-instance wan2
[RouterA-GigabitEthernet0/0/9] ip address 192.168.20.1 255.255.255.0
[RouterA-GigabitEthernet0/0/9] quit
[RouterA] ip route-static vpn-instance wan1 10.172.0.0 255.255.0.0 192.168.10.254
[RouterA] ip route-static vpn-instance wan2 10.172.0.0 255.255.0.0 192.168.20.254
```

配置RouterC物理接口的IP地址及静态路由。

```
<Huawei> system-view
[Huawei] sysname RouterC
[RouterC] router id 10.172.10.2
[RouterC] interface XGigabitEthernet0/0/0
[RouterC-XGigabitEthernet0/0/0] ip address 10.172.10.2 255.255.255.0
[RouterC-XGigabitEthernet0/0/0] quit
[RouterC] ip route-static 192.168.0.0 255.255.0.0 10.172.10.1
```

配置RouterD物理接口的IP地址及静态路由。

```
<Huawei> system-view
[Huawei] sysname RouterD
[RouterD] router id 10.172.20.2
[RouterD] interface XGigabitEthernet0/0/0
[RouterD-XGigabitEthernet0/0/0] ip address 10.172.20.2 255.255.255.0
[RouterD-XGigabitEthernet0/0/0] quit
[RouterD] ip route-static 192.168.0.0 255.255.0.0 10.172.20.1
```

2. 在RouterA和RouterC、RouterD之间部署GRE隧道，通过静态路由指定到达对端的报文通过GRE隧道转发，实现Underlay传输网络互通，用于三层报文多发选收。

   # 在RouterA上创建Tunnel接口，并配置接口路由。

```
[RouterA] interface Tunnel0/0/0
[RouterA-Tunnel0/0/0] description key1
[RouterA-Tunnel0/0/0] ip address 172.16.1.1 255.255.255.0
[RouterA-Tunnel0/0/0] tunnel-protocol gre
[RouterA-Tunnel0/0/0] keepalive period 1
[RouterA-Tunnel0/0/0] gre key plain 1
[RouterA-Tunnel0/0/0] source GigabitEthernet0/0/8
[RouterA-Tunnel0/0/0] destination vpn-instance wan1 10.172.10.2
[RouterA-Tunnel0/0/0] ospf enable 1 area 0.0.0.0
[RouterA-Tunnel0/0/0] quit
[RouterA] interface Tunnel0/0/1
[RouterA-Tunnel0/0/1] description key2
[RouterA-Tunnel0/0/1] ip address 172.16.2.1 255.255.255.0
[RouterA-Tunnel0/0/1] tunnel-protocol gre
[RouterA-Tunnel0/0/1] keepalive period 1
[RouterA-Tunnel0/0/1] gre key plain 2
[RouterA-Tunnel0/0/1] source GigabitEthernet0/0/9
[RouterA-Tunnel0/0/1] destination vpn-instance wan2 10.172.10.2
[RouterA-Tunnel0/0/1] ospf enable 1 area 0.0.0.0
[RouterA-Tunnel0/0/1] quit
[RouterA] interface Tunnel0/0/2
[RouterA-Tunnel0/0/2] ip address 172.16.3.1 255.255.255.0
[RouterA-Tunnel0/0/2] tunnel-protocol gre
```

 版权所有 © 华为技术有限公司

```
[RouterA-Tunnel0/0/2] gre key plain 3
[RouterA-Tunnel0/0/2] source GigabitEthernet0/0/8
[RouterA-Tunnel0/0/2] destination vpn-instance wan1 10.172.20.2
[RouterA-Tunnel0/0/2] ospf enable 1 area 0.0.0.0
[RouterA-Tunnel0/0/2] quit
[RouterA] interface Tunnel0/0/3
[RouterA-Tunnel0/0/3] ip address 172.16.4.1 255.255.255.0
[RouterA-Tunnel0/0/3] tunnel-protocol gre
[RouterA-Tunnel0/0/3] gre key plain 4
[RouterA-Tunnel0/0/3] source GigabitEthernet0/0/9
[RouterA-Tunnel0/0/3] destination vpn-instance wan2 10.172.20.2
[RouterA-Tunnel0/0/3] ospf enable 1 area 0.0.0.0
[RouterA-Tunnel0/0/3] quit
```

在RouterC上创建Tunnel接口，并配置接口路由。

```
[RouterC] interface Tunnel0/0/0
[RouterC-Tunnel0/0/0] description key1
[RouterC-Tunnel0/0/0] ip address 172.16.1.2 255.255.255.0
[RouterC-Tunnel0/0/0] tunnel-protocol gre
[RouterC-Tunnel0/0/0] gre key plain 1
[RouterC-Tunnel0/0/0] source XGigabitEthernet0/0/0
[RouterC-Tunnel0/0/0] destination 192.168.10.1
[RouterC-Tunnel0/0/0] ospf enable 1 area 0.0.0.0
[RouterC-Tunnel0/0/0] quit
[RouterC] interface Tunnel0/0/1
[RouterC-Tunnel0/0/1] description key2
[RouterC-Tunnel0/0/1] ip address 172.16.2.2 255.255.255.0
[RouterC-Tunnel0/0/1] tunnel-protocol gre
[RouterC-Tunnel0/0/1] gre key plain 2
[RouterC-Tunnel0/0/1] source XGigabitEthernet0/0/0
[RouterC-Tunnel0/0/1] destination 192.168.20.1
[RouterC-Tunnel0/0/1] ospf enable 1 area 0.0.0.0
[RouterC-Tunnel0/0/1] quit
```

在RouterD上创建Tunnel接口，并配置接口路由。

```
[RouterD] interface Tunnel0/0/0
[RouterD-Tunnel0/0/0] ip address 172.16.3.2 255.255.255.0
[RouterD-Tunnel0/0/0] tunnel-protocol gre
[RouterD-Tunnel0/0/0] gre key plain 3
[RouterD-Tunnel0/0/0] source XGigabitEthernet0/0/0
[RouterD-Tunnel0/0/0] destination 192.168.10.1
[RouterD-Tunnel0/0/0] ospf enable 1 area 0.0.0.0
[RouterD-Tunnel0/0/0] quit
[RouterD] interface Tunnel0/0/1
[RouterD-Tunnel0/0/1] ip address 172.16.4.2 255.255.255.0
[RouterD-Tunnel0/0/1] tunnel-protocol gre
[RouterD-Tunnel0/0/1] gre key plain 4
[RouterD-Tunnel0/0/1] source XGigabitEthernet0/0/0
[RouterD-Tunnel0/0/1] destination 192.168.20.1
[RouterD-Tunnel0/0/1] ospf enable 1 area 0.0.0.0
[RouterD-Tunnel0/0/1] quit
```

配置完成后Tunnel接口状态变为Up，Tunnel接口之间可以Ping通，直连隧道建立。以RouterA的显示为例。

```
<RouterA> ping 172.16.1.2
  PING 172.16.1.2: 56  data bytes, press CTRL_C to break
    Reply from 172.16.1.2: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 172.16.1.2: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 172.16.1.2: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 172.16.1.2: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 172.16.1.2: bytes=56 Sequence=5 ttl=255 time=1 ms
  --- 172.16.1.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/1 ms
```

 版权所有 © 华为技术有限公司

3. 配置Overlay业务网络互通。在LAN侧的接口和WAN侧的Tunnel接口上分别绑定二层VE接口，实现以太报文通过GRE隧道进行透传，且配置WAN侧Tunnel接口的源接口为Loopback接口用于实现二层报文多发选收。

   # 配置RouterA。

```
[RouterA] interface LoopBack0
[RouterA-LoopBack0] ip address 1.1.1.1 255.255.255.0
[RouterA-LoopBack0] quit
[RouterA] vlan batch 100 200
[RouterA] interface Virtual-Ethernet0/0/0
[RouterA-Virtual-Ethernet0/0/0] portswitch
[RouterA-Virtual-Ethernet0/0/0] port link-type access
[RouterA-Virtual-Ethernet0/0/0] port default vlan 200
[RouterA-Virtual-Ethernet0/0/0] quit
[RouterA] interface Virtual-Ethernet0/0/1
[RouterA-Virtual-Ethernet0/0/1] portswitch
[RouterA-Virtual-Ethernet0/0/1] port link-type trunk
[RouterA-Virtual-Ethernet0/0/1] undo port trunk allow-pass vlan 1
[RouterA-Virtual-Ethernet0/0/1] port trunk allow-pass vlan 200
[RouterA-Virtual-Ethernet0/0/1] quit
[RouterA] interface gigabitethernet 0/0/1
[RouterA-GigabitEthernet0/0/1] undo portswitch
[RouterA-GigabitEthernet0/0/1] tcp adjust-mss 1200
[RouterA-GigabitEthernet0/0/1] map interface Virtual-Ethernet0/0/0
[RouterA-GigabitEthernet0/0/1] quit
[RouterA] interface Tunnel0/0/4
[RouterA-Tunnel0/0/4] ip address 172.16.5.1 255.255.255.0
[RouterA-Tunnel0/0/4] tunnel-protocol gre
[RouterA-Tunnel0/0/4] gre key plain 5
[RouterA-Tunnel0/0/4] source LoopBack0
[RouterA-Tunnel0/0/4] destination 192.168.255.254
[RouterA-Tunnel0/0/4] map interface Virtual-Ethernet0/0/1
[RouterA-Tunnel0/0/4] quit
```

   # 配置RouterC。

   - 配置RSTP功能，破除二层网络中的环路。
   - 配置Eth-Trunk保证连接的可靠性。

```
[RouterC] stp mode rstp
[RouterC] stp instance 0 root primary
[RouterC] stp pathcost-standard legacy
[RouterC] vlan batch 100 200
[RouterC] interface Eth-Trunk0
[RouterC-Eth-Trunk0] port link-type trunk
[RouterC-Eth-Trunk0] undo port trunk allow-pass vlan 1
[RouterC-Eth-Trunk0] port trunk allow-pass vlan 100 200
[RouterC-Eth-Trunk0] quit
[RouterC] interface gigabitethernet0/0/0
[RouterC-GigabitEthernet0/0/0] portswitch
[RouterC-GigabitEthernet0/0/0] eth-trunk 0
[RouterC-GigabitEthernet0/0/0] quit
[RouterC] interface gigabitethernet0/0/1
[RouterC-GigabitEthernet0/0/1] portswitch
[RouterC-GigabitEthernet0/0/1] eth-trunk 0
[RouterC-GigabitEthernet0/0/1] quit
[RouterC] interface XGigabitEthernet0/0/1
[RouterC-GigabitEthernet0/0/1] portswitch
[RouterC-GigabitEthernet0/0/1] port link-type trunk
[RouterC-GigabitEthernet0/0/1] undo port trunk allow-pass vlan 1
[RouterC-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 200
[RouterC-GigabitEthernet0/0/1] stp root-protection
[RouterC-GigabitEthernet0/0/1] quit
[RouterC] interface Virtual-Ethernet0/0/0
[RouterC-Virtual-Ethernet0/0/0] portswitch
[RouterC-Virtual-Ethernet0/0/0] port link-type trunk
[RouterC-Virtual-Ethernet0/0/0] undo port trunk allow-pass vlan 1
[RouterC-Virtual-Ethernet0/0/0] port trunk allow-pass vlan 200
[RouterC-Virtual-Ethernet0/0/0] quit
```

 版权所有 © 华为技术有限公司

```
[RouterC] interface Virtual-Ethernet0/0/1
[RouterC-Virtual-Ethernet0/0/1] portswitch
[RouterC-Virtual-Ethernet0/0/1] port link-type trunk
[RouterC-Virtual-Ethernet0/0/1] undo port trunk allow-pass vlan 1
[RouterC-Virtual-Ethernet0/0/1] port trunk allow-pass vlan 200
[RouterC-Virtual-Ethernet0/0/1] quit
[RouterC] interface Vlanif200
[RouterC-Vlanif200] map interface Virtual-Ethernet0/0/0
[RouterC-Vlanif200] quit
[RouterC] interface Tunnel0/0/2
[RouterC-Tunnel0/0/2] ip address 172.16.5.2 255.255.255.0
[RouterC-Tunnel0/0/2] tunnel-protocol gre
[RouterC-Tunnel0/0/2] gre key plain 5
[RouterC-Tunnel0/0/2] source 192.168.255.254
[RouterC-Tunnel0/0/2] destination 1.1.1.1
[RouterC-Tunnel0/0/2] map interface Virtual-Ethernet0/0/1
[RouterC-Tunnel0/0/2] quit
```

配置RouterD。

- 配置RSTP功能，破除二层网络中的环路。
- 配置Eth-Trunk保证连接的可靠性。

```
[RouterD] stp mode rstp
[RouterD] stp pathcost-standard legacy
[RouterD] vlan batch 100 200
[RouterD] interface Eth-Trunk0
[RouterD-Eth-Trunk0] port link-type trunk
[RouterD-Eth-Trunk0] undo port trunk allow-pass vlan 1
[RouterD-Eth-Trunk0] port trunk allow-pass vlan 100 200
[RouterD-Eth-Trunk0] quit
[RouterD] interface gigabitethernet0/0/1
[RouterD-GigabitEthernet0/0/1] portswitch
[RouterD-GigabitEthernet0/0/1] eth-trunk 0
[RouterD-GigabitEthernet0/0/1] quit
[RouterD] interface gigabitethernet0/0/2
[RouterD-GigabitEthernet0/0/2] portswitch
[RouterD-GigabitEthernet0/0/2] eth-trunk 0
[RouterD-GigabitEthernet0/0/2] quit
[RouterD] interface GigabitEthernet0/0/4
[RouterD-GigabitEthernet0/0/4] portswitch
[RouterD-GigabitEthernet0/0/4] port link-type trunk
[RouterD-GigabitEthernet0/0/4] port trunk allow-pass vlan 100 200
[RouterD-GigabitEthernet0/0/4] quit
[RouterD] interface Virtual-Ethernet0/0/0
[RouterD-Virtual-Ethernet0/0/0] portswitch
[RouterD-Virtual-Ethernet0/0/0] port link-type trunk
[RouterD-Virtual-Ethernet0/0/0] undo port trunk allow-pass vlan 1
[RouterD-Virtual-Ethernet0/0/0] port trunk allow-pass vlan 200
[RouterD-Virtual-Ethernet0/0/0] quit
[RouterD] interface Virtual-Ethernet0/0/1
[RouterD-Virtual-Ethernet0/0/1] portswitch
[RouterD-Virtual-Ethernet0/0/1] port link-type trunk
[RouterD-Virtual-Ethernet0/0/1] undo port trunk allow-pass vlan 1
[RouterD-Virtual-Ethernet0/0/1] port trunk allow-pass vlan 200
[RouterD-Virtual-Ethernet0/0/1] quit
[RouterD] interface Vlanif200
[RouterD-Vlanif200] map interface Virtual-Ethernet0/0/0
[RouterD-Vlanif200] quit
[RouterD] interface Tunnel0/0/2
[RouterD-Tunnel0/0/2] ip address 172.16.5.2 255.255.255.0
[RouterD-Tunnel0/0/2] tunnel-protocol gre
[RouterD-Tunnel0/0/2] gre key plain 5
[RouterD-Tunnel0/0/2] source 192.168.255.254
[RouterD-Tunnel0/0/2] destination 1.1.1.1
[RouterD-Tunnel0/0/2] map interface Virtual-Ethernet0/0/1
[RouterD-Tunnel0/0/2] quit
```

配置RouterE的接口加入VLAN。

 版权所有 © 华为技术有限公司

```
<Huawei> system-view
[Huawei] sysname RouterE
[RouterE] stp mode rstp
[RouterE] stp pathcost-standard legacy
[RouterE] interface gigabitethernet 0/0/0
[RouterE-GigabitEthernet0/0/0] description lan
[RouterE-GigabitEthernet0/0/0] port link-type trunk
[RouterE-GigabitEthernet0/0/0] undo port trunk allow-pass vlan 1
[RouterE-GigabitEthernet0/0/0] port trunk allow-pass vlan 200
[RouterE-GigabitEthernet0/0/0] stp disable
[RouterE-GigabitEthernet0/0/0] quit
[RouterE] interface gigabitethernet 0/0/1
[RouterE-GigabitEthernet0/0/1] port link-type trunk
[RouterE-GigabitEthernet0/0/1] undo port trunk allow-pass vlan 1
[RouterE-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 200
[RouterE-GigabitEthernet0/0/1] quit
[RouterE] interface gigabitethernet 0/0/2
[RouterE-GigabitEthernet0/0/2] port link-type trunk
[RouterE-GigabitEthernet0/0/2] undo port trunk allow-pass vlan 1
[RouterE-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 200
[RouterE-GigabitEthernet0/0/2] quit
```

4. 配置BFD会话，实现设备间链路故障的快速检测。

   # 配置RouterA。

```
[RouterA] bfd
[RouterA-bfd] quit
[RouterA] bfd 1 bind peer-ip 172.16.1.2 source-ip 172.16.1.1
[RouterA-bfd-session-1] discriminator local 1
[RouterA-bfd-session-1] discriminator remote 2
[RouterA-bfd-session-1] commit
[RouterA-bfd-session-1] quit
[RouterA] bfd 2 bind peer-ip 172.16.2.2 source-ip 172.16.2.1
[RouterA-bfd-session-2] discriminator local 3
[RouterA-bfd-session-2] discriminator remote 4
[RouterA-bfd-session-2] commit
[RouterA-bfd-session-2] quit
[RouterA] bfd tohub bind peer-ip 192.168.255.254 source-ip 1.1.1.1
[RouterA-bfd-session-tohub] discriminator local 5
[RouterA-bfd-session-tohub] discriminator remote 6
[RouterA-bfd-session-tohub] commit
[RouterA-bfd-session-tohub] quit
```

   # 配置RouterC。

```
[RouterC] bfd
[RouterC-bfd] quit
[RouterC] bfd 1 bind peer-ip 172.16.1.1 source-ip 172.16.1.2
[RouterC-bfd-session-1] discriminator local 2
[RouterC-bfd-session-1] discriminator remote 1
[RouterC-bfd-session-1] description 1
[RouterC-bfd-session-1] commit
[RouterC-bfd-session-1] quit
[RouterC] bfd 2 bind peer-ip 172.16.2.1 source-ip 172.16.2.2
[RouterC-bfd-session-2] discriminator local 4
[RouterC-bfd-session-2] discriminator remote 3
[RouterC-bfd-session-2] commit
[RouterC-bfd-session-2] quit
[RouterC] bfd tospoke bind peer-ip 1.1.1.1 source-ip 192.168.255.254
[RouterC-bfd-session-tospoke] discriminator local 6
[RouterC-bfd-session-tospoke] discriminator remote 5
[RouterC-bfd-session-tospoke] commit
[RouterC-bfd-session-tospoke] quit
```

   # 配置完成后，在RouterA执行**display bfd session all**命令，可以看到建立了BFD会话，且状态为Up。

```
<RouterA> display bfd session all
--------------------------------------------------------------------------------
Local Remote     PeerIpAddr       State     Type        InterfaceName
--------------------------------------------------------------------------------
1     2          172.16.1.2       Up        S_IP_PEER   -
```

 版权所有 © 华为技术有限公司

```
3    4         172.16.2.2        Up       S_IP_PEER         -
5    6         192.168.255.254   Up       S_IP_PEER         -
------------------------------------------------------------------------------
    Total UP/DOWN Session Number : 3/0
```

配置完成后，在RouterC执行**display bfd session all**命令，可以看到建立了BFD会话，且状态为Up。

```
<RouterC> display bfd session all
------------------------------------------------------------------------------

Local Remote     PeerIpAddr       State     Type
InterfaceName
------------------------------------------------------------------------------

2     1          172.16.1.1       Up        S_IP_PEER         -
4     3          172.16.2.1       Up        S_IP_PEER         -
6     5          1.1.1.1          Up        S_IP_PEER         -
------------------------------------------------------------------------------

    Total UP/DOWN Session Number :
3/0
```

5. 配置VRRP主备备份。RouterC上配置较高优先级，作为Master设备承担流量转发；RouterD作为备用路由器，实现网关冗余备份。同时，配置VRRP与BFD联动，实现链路故障时VRRP备份组快速切换。

   # 配置RouterC。

   ```
   [RouterC] interface Vlanif100
   [RouterC-Vlanif100] ip address 192.168.255.1 255.255.255.0
   [RouterC-Vlanif100] vrrp vrid 1 virtual-ip 192.168.255.254
   [RouterC-Vlanif100] vrrp vrid 1 priority 120
   [RouterC-Vlanif100] vrrp vrid 1 track bfd-session 2 reduced 15
   [RouterC-Vlanif100] vrrp vrid 1 track bfd-session 4 reduced 15
   [RouterC-Vlanif100] vrrp vrid 1 track interface XGigabitEthernet0/0/0 reduced 30
   [RouterC-Vlanif100] quit
   ```

   # 配置RouterD。

   ```
   [RouterD] interface Vlanif100
   [RouterD-Vlanif100] ip address 192.168.255.2 255.255.255.0
   [RouterD-Vlanif100] vrrp vrid 1 virtual-ip 192.168.255.254
   [RouterD-Vlanif100] quit
   ```

6. 在源接口为Loopback接口的内层Ethernet Over GRE隧道上配置重定向多发选收功能，并指定链路组不根据链路状态刷新选路信息，避免路由切换过程中出现的丢包现象，最大程度保证业务连续性。

   # 配置RouterA。

   ```
   [RouterA] replication path-group 1
   [RouterA-replication-path-group-1] path Tunnel0/0/0 priority 1 track bfd tohub
   [RouterA-replication-path-group-1] path Tunnel0/0/1 priority 2 track bfd tohub
   [RouterA-replication-path-group-1] path Tunnel0/0/2 priority 3
   [RouterA-replication-path-group-1] path Tunnel0/0/3 priority 4
   [RouterA-replication-path-group-1] quit
   [RouterA] interface tunnel 0/0/4
   [RouterA-Tunnel0/0/4] redirect-replication path-group 1
   [RouterA-Tunnel0/0/4] quit
   [RouterA] replication if-down-delay 65535
   ```

   # 配置RouterC。

   ```
   [RouterC] replication path-group 1
   [RouterC-replication-path-group-1] path Tunnel 0/0/0 priority 1
   [RouterC-replication-path-group-1] path Tunnel 0/0/1 priority 2
   [RouterC-replication-path-group-1] quit
   [RouterC] interface tunnel0/0/2
   [RouterC-Tunnel0/0/2] redirect-replication path-group 1
   [RouterC-Tunnel0/0/2] quit
   [RouterC] replication if-down-delay 65535
   ```

   # 配置RouterD。

 版权所有 © 华为技术有限公司

```
[RouterD] replication path-group 1
[RouterD-replication-path-group-1] path Tunnel 0/0/0 priority 1
[RouterD-replication-path-group-1] path Tunnel 0/0/1 priority 2
[RouterD-replication-path-group-1] quit
[RouterD] interface tunnel0/0/2
[RouterD-Tunnel0/0/2] redirect-replication path-group 1
[RouterD-Tunnel0/0/2] quit
[RouterD] replication if-down-delay 65535
```

配置完成后，执行**display replication path-group**命令可以看到链路组的所有链路状态和选路结果。以RouterA的显示为例。

```
[RouterA] display replication path-group 1
------------------------------------------------------------
Path member       Priority     Track info      Path state
Tunnel0/0/0       1            BFD             UP
Tunnel0/0/1       2            BFD             UP
Tunnel0/0/2       3            -               UP
Tunnel0/0/3       4            -               UP
------------------------------------------------------------
[RouterA] display replication path-group
------------------------------------------------------------------------------
Group name                    Replication link1     Replication link2
1                          Tunnel0/0/0           Tunnel0/0/1
------------------------------------------------------------------------------
```

7. 配置设备间使用OSPF路由，且使能OSPF BFD检测机制，当链路出现故障时，BFD能够快速检测到故障并通告给OSPF协议，使业务流量使用备份链路传送。

   # 配置RouterA。

   ```
   [RouterA] ospf 1
   [RouterA-ospf-1] bfd all-interfaces enable
   [RouterA-ospf-1] bfd all-interfaces min-tx-interval 50 min-rx-interval 50
   [RouterA-ospf-1] filter-policy ip-prefix fromhub import
   [RouterA-ospf-1] area 0.0.0.0
   [RouterA-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
   [RouterA-ospf-1-area-0.0.0.0] quit
   [RouterA-ospf-1] quit
   [RouterA] ip ip-prefix fromhub index 10 permit 192.168.255.254 32
   ```

   # 配置RouterC。

   ```
   [RouterC] ospf 1
   [RouterC-ospf-1] bfd all-interfaces enable
   [RouterC-ospf-1] bfd all-interfaces min-tx-interval 50 min-rx-interval 50
   [RouterC-ospf-1] filter-policy ip-prefix fromspoke import
   [RouterC-ospf-1] import-route direct route-policy tospoke
   [RouterC-ospf-1] area 0.0.0.0
   [RouterC-ospf-1-area-0.0.0.0] quit
   [RouterC-ospf-1] quit
   [RouterC] route-policy tospoke permit node 0
   [RouterC-route-policy] if-match ip-prefix tospoke
   [RouterC-route-policy] quit
   [RouterC] ip ip-prefix fromspoke index 10 permit 1.1.1.1 32
   [RouterC] ip ip-prefix tospoke index 10 permit 192.168.255.254 32
   ```

   # 配置RouterD。

   ```
   [RouterD] ospf 1
   [RouterD-ospf-1] bfd all-interfaces enable
   [RouterD-ospf-1] bfd all-interfaces min-tx-interval 50 min-rx-interval 50
   [RouterD-ospf-1] filter-policy ip-prefix fromspoke import
   [RouterD-ospf-1] import-route direct route-policy tospoke
   [RouterD-ospf-1] area 0.0.0.0
   [RouterD-ospf-1-area-0.0.0.0] quit
   [RouterD-ospf-1] quit
   [RouterD] route-policy tospoke permit node 0
   [RouterD-route-policy] if-match ip-prefix tospoke
   [RouterD-route-policy] quit
   [RouterD] ip ip-prefix fromspoke index 10 permit 1.1.1.1 32
   [RouterD] ip ip-prefix tospoke index 10 permit 192.168.255.254 32
   ```

 版权所有 © 华为技术有限公司

配置文件

- RouterA的配置文件

```
#
sysname RouterA
#
router id 1.1.1.1
#
vlan batch 100 200
#
 replication if-down-delay 65535
#
ip vpn-instance wan1
 ipv4-family
  route-distinguisher 192.168.10.1:0
#
ip vpn-instance wan2
 ipv4-family
  route-distinguisher 192.168.20.1:0
#
bfd
#
interface GigabitEthernet0/0/1
 undo portswitch
 tcp adjust-mss 1200
 map interface Virtual-Ethernet0/0/0
#
interface GigabitEthernet0/0/8
 ip binding vpn-instance wan1
 ip address 192.168.10.1 255.255.255.0
#
interface GigabitEthernet0/0/9
 ip binding vpn-instance wan2
 ip address 192.168.20.1 255.255.255.0
#
interface Virtual-Ethernet0/0/0
 portswitch
 port link-type access
 port default vlan 200
#
interface Virtual-Ethernet0/0/1
 portswitch
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 200
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.0
#
interface Tunnel0/0/0
 description key1
 ip address 172.16.1.1 255.255.255.0
 tunnel-protocol gre
 keepalive period 1
 gre key plain 1
 source GigabitEthernet0/0/8
 destination vpn-instance wan1 10.172.10.2
 ospf enable 1 area 0.0.0.0
#
interface Tunnel0/0/1
 description key2
 ip address 172.16.2.1 255.255.255.0
 tunnel-protocol gre
 keepalive period 1
 gre key plain 2
 source GigabitEthernet0/0/9
 destination vpn-instance wan2 10.172.10.2
 ospf enable 1 area 0.0.0.0
#
```

 版权所有 © 华为技术有限公司

```
interface Tunnel0/0/2
 ip address 172.16.3.1 255.255.255.0
 tunnel-protocol gre
 gre key plain 3
 source GigabitEthernet0/0/8
 destination vpn-instance wan1 10.172.20.2
 ospf enable 1 area 0.0.0.0
#
interface Tunnel0/0/3
 ip address 172.16.4.1 255.255.255.0
 tunnel-protocol gre
 gre key plain 4
 source GigabitEthernet0/0/9
 destination vpn-instance wan2 10.172.20.2
 ospf enable 1 area 0.0.0.0
#
interface Tunnel0/0/4
 ip address 172.16.5.1 255.255.255.0
 tunnel-protocol gre
 gre key plain 5
 source LoopBack0
 destination 192.168.255.254
 redirect-replication path-group 1
 map interface Virtual-Ethernet0/0/1
#
bfd 1 bind peer-ip 172.16.1.2 source-ip 172.16.1.1
 discriminator local 1
 discriminator remote 2
 commit
#
bfd 2 bind peer-ip 172.16.2.2 source-ip 172.16.2.1
 discriminator local 3
 discriminator remote 4
 commit
#
bfd tohub bind peer-ip 192.168.255.254 source-ip
1.1.1.1
 discriminator local 5
 discriminator remote 6
 commit
#
ospf 1
 bfd all-interfaces enable
 bfd all-interfaces min-tx-interval 50 min-rx-interval 50
 filter-policy ip-prefix fromhub import
 area 0.0.0.0
  network 1.1.1.1 0.0.0.0
#
ip ip-prefix fromhub index 10 permit 192.168.255.254 32
#
ip route-static vpn-instance wan1 10.172.0.0 255.255.0.0 192.168.10.254
ip route-static vpn-instance wan2 10.172.0.0 255.255.0.0 192.168.20.254
#
replication path-group 1
 path Tunnel0/0/0 priority 1 track bfd tohub
 path Tunnel0/0/1 priority 2 track bfd tohub
 path Tunnel0/0/2 priority 3
 path Tunnel0/0/3 priority 4
#
```

- RouterC的配置文件

```
#
sysname RouterC
#
router id 10.172.10.2
#
vlan batch 100 200
#
stp mode rstp
stp instance 0 root primary
```

 版权所有 © 华为技术有限公司

```
stp pathcost-standard legacy
#
 replication if-down-delay 65535
#
bfd
#
interface Vlanif100
 ip address 192.168.255.1 255.255.255.0
 vrrp vrid 1 virtual-ip 192.168.255.254
 vrrp vrid 1 priority 120
 vrrp vrid 1 track bfd-session 2 reduced 15
 vrrp vrid 1 track bfd-session 4 reduced 15
 vrrp vrid 1 track interface XGigabitEthernet0/0/0 reduced 30
#
interface Vlanif200
 map interface Virtual-Ethernet0/0/0
#
interface Eth-Trunk0
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 100 200
#
interface GigabitEthernet0/0/0
 portswitch
 eth-trunk 0
#
interface GigabitEthernet0/0/1
 portswitch
 eth-trunk 0
#
interface XGigabitEthernet0/0/0
 ip address 10.172.10.2 255.255.255.0
#
interface XGigabitEthernet0/0/1
 portswitch
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 100 200
 stp root-protection
#
interface Virtual-Ethernet0/0/0
 portswitch
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 200
#
interface Virtual-Ethernet0/0/1
 portswitch
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 200
#
interface Tunnel0/0/0
 description key1
 ip address 172.16.1.2 255.255.255.0
 tunnel-protocol gre
 gre key plain 1
 source XGigabitEthernet0/0/0
 destination 192.168.10.1
 ospf enable 1 area 0.0.0.0
#
interface Tunnel0/0/1
 description key2
 ip address 172.16.2.2 255.255.255.0
 tunnel-protocol gre
 gre key plain 2
 source XGigabitEthernet0/0/0
 destination 192.168.20.1
 ospf enable 1 area 0.0.0.0
```

 版权所有 © 华为技术有限公司

```
#
interface Tunnel0/0/2
 ip address 172.16.5.2 255.255.255.0
 tunnel-protocol gre
 gre key plain 5
 source 192.168.255.254
 destination 1.1.1.1
 redirect-replication path-group 1
 map interface Virtual-Ethernet0/0/1
#
bfd 1 bind peer-ip 172.16.1.1 source-ip 172.16.1.2
 discriminator local 2
 discriminator remote 1
 description 1
 commit
#
bfd 2 bind peer-ip 172.16.2.1 source-ip 172.16.2.2
 discriminator local 4
 discriminator remote 3
 commit
#
bfd tospoke bind peer-ip 1.1.1.1 source-ip
192.168.255.254
 discriminator local 6
 discriminator remote 5
 commit
#
ospf 1
 bfd all-interfaces enable
 bfd all-interfaces min-tx-interval 50 min-rx-interval 50
 filter-policy ip-prefix fromspoke import
 import-route direct route-policy tospoke
 area 0.0.0.0
#
route-policy tospoke permit node 0
 if-match ip-prefix tospoke
#
ip ip-prefix fromspoke index 10 permit 1.1.1.1 32
ip ip-prefix tospoke index 10 permit 192.168.255.254 32
#
ip route-static 192.168.0.0 255.255.0.0 10.172.10.1
#
replication path-group 1
 path Tunnel0/0/0 priority 1
 path Tunnel0/0/1 priority 2
#
```

- RouterD的配置文件

```
#
sysname RouterD
#
router id 10.172.20.2
#
vlan batch 100 200
#
stp mode rstp
stp pathcost-standard legacy
#
 replication if-down-delay 65535
#
interface Vlanif100
 ip address 192.168.255.2 255.255.255.0
 vrrp vrid 1 virtual-ip 192.168.255.254
#
interface Vlanif200
 map interface Virtual-Ethernet0/0/0
#
interface Eth-Trunk0
 port link-type trunk
 undo port trunk allow-pass vlan 1
```

 版权所有 © 华为技术有限公司

```
 port trunk allow-pass vlan 100 200
#
interface GigabitEthernet0/0/1
 portswitch
 eth-trunk 0
#
interface GigabitEthernet0/0/2
 portswitch
 eth-trunk 0
#
interface GigabitEthernet0/0/4
 portswitch
 port link-type trunk
 port trunk allow-pass vlan 100 200
#
interface XGigabitEthernet0/0/0
 ip address 10.172.20.2 255.255.255.0
#
interface Virtual-Ethernet0/0/0
 portswitch
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 200
#
interface Virtual-Ethernet0/0/1
 portswitch
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 200
#
interface Tunnel0/0/0
 ip address 172.16.3.2 255.255.255.0
 tunnel-protocol gre
 gre key plain 3
 source XGigabitEthernet0/0/0
 destination 192.168.10.1
 ospf enable 1 area 0.0.0.0
 replication path-group 1
#
interface Tunnel0/0/1
 ip address 172.16.4.2 255.255.255.0
 tunnel-protocol gre
 gre key plain 4
 source XGigabitEthernet0/0/0
 destination 192.168.20.1
 ospf enable 1 area 0.0.0.0
#
interface Tunnel0/0/2
 ip address 172.16.5.2 255.255.255.0
 tunnel-protocol gre
 gre key plain 5
 source 192.168.255.254
 destination 1.1.1.1
 redirect-replication path-group 1
 map interface Virtual-Ethernet0/0/1
#
ospf 1
 bfd all-interfaces enable
 bfd all-interfaces min-tx-interval 50 min-rx-interval 50
 filter-policy ip-prefix fromspoke import
 import-route direct route-policy tospoke
 area 0.0.0.0
#
route-policy tospoke permit node 0
 if-match ip-prefix tospoke
#
ip ip-prefix fromspoke index 10 permit 1.1.1.1 32
ip ip-prefix tospoke index 10 permit 192.168.255.254 32
#
```

 版权所有 © 华为技术有限公司

```
ip route-static 192.168.0.0 255.255.0.0 10.172.20.1
#
replication path-group 1
 path Tunnel0/0/0 priority 1
 path Tunnel0/0/1 priority 2
#
```

- RouterE的配置文件

```
#
sysname RouterE
#
stp mode rstp
stp pathcost-standard legacy
#
interface GigabitEthernet0/0/0
 description lan
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 200
 stp disable
#
interface GigabitEthernet0/0/1
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 100
200
#
interface GigabitEthernet0/0/2
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 100
200
#
```

7.3 5G 冗余保护场景

7.3.1 配置企业使用 5G 主备双 SIM 卡上网示例

场景介绍

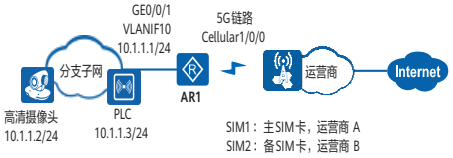
提高5G链路的可靠性有多种方式，例如5G双上行、5G+有线双上行等，其中双SIM卡主备也是比较简单且常用的一种。特别是对于一些单5G链路上行场景，可以通过在AR1上插入2个SIM卡来提高5G链路的可靠性。2个SIM卡通常分属于不同的运营商，防止某一个运营商无线侧发生故障后，整条5G链路断掉。同时，还可以配置SIM卡切换策略，当主SIM卡费用不足、或运营商无线链路故障导致5G拨号失败时，流量可以自动切换到备份SIM卡上转发，保证业务的快速恢复。目前双SIM卡备份场景下切换的时间为分钟级。

组网方式

如图1所示，企业分支和总部之间通过Internet网络互联。企业分支使用AR1企业路由器作为出口网关。为了提高链路可靠性，AR1企业路由器上插了两张不同运营商的5G SIM卡。两张SIM卡关联到不同优先级的APN模板，关联主SIM卡的APN模板的优先级高于关联备SIM卡的APN模板的优先级，并使能NQA探测功能。当主SIM卡所在的链路NQA探测失败时，5G链路切换到备SIM卡上重新拨号连接。

 版权所有 © 华为技术有限公司

图 7-15 配置企业使用 5G 主备双 SIM 卡上网组网图



数据准备

表 7-19 数据准备表

项目	数据	说明
运营商给分支分配的APN名称	主SIM1卡：运营商A、5gneta 备SIM2卡：运营商B、5gnetb	APN名称需提前从运营商处获取。
运营商给分支5G Cellular接口分配的IP地址	运营商A：1.1.1.1/32 运营商B：2.2.2.2/32	5G Cellular接口拨号接入运营商后，运营商给5G Cellular接口自动分配的IP地址。
分支AR1 LAN侧接口信息	所属VLAN：10 网关地址：VLANIF10（10.1.1.1/24） LAN侧物理接口：GE0/0/1	VLAN 10为分支子网用户所在的VLAN，且分支子网用户的网关为VLANIF10接口。
NQA探测的目的地址	公网DNS服务器地址：114.114.114.114	NQA测试例的测试类型必须为ICMP测试，且到NQA测试例的目的地址必须路由可达。本例中选择公网的DNS服务器地址为探测目的地址，也可以选择其他路由可达的公网地址。 114.114.114.114是国内通用的DNS地址，国内用户使用较多，本例中用该地址来测试5G链路的连通性。8.8.8.8是全球通用的DNS地址，如果是国外用户，可以用8.8.8.8地址来测试5G链路的连通性。

配置思路

1. 配置5G Cellular接口的连接参数及NQA测试例，实现5G Cellular接口接入5G网络。
2. 配置分支企业子网，为内部用户自动分配IP地址。

版权所有 © 华为技术有限公司

3. 配置分支NAT功能，实现分支的内部用户可以访问Internet。
4. 配置静态路由，使企业分支和Internet之间的路由互通。

说明

在5G Cellular接口下执行命令**dialer enable-circular**配置轮询拨号功能时，设备会同时下发自动拨号、IP地址协商和5G Modem自愈的相关配置，无需再重复配置。

操作步骤

1. 配置5G Cellular接口的连接参数及NQA测试例，实现5G Cellular接口接入5G网络。
   a. 创建APN模板。
   ```
   <Huawei> system-view
   [Huawei] sysname AR1
   [AR1] apn profile 5gprofilea
   [AR1-apn-profile-5gprofilea] apn 5gneta
   [AR1-apn-profile-5gprofilea] quit
   [AR1] apn profile 5gprofileb
   [AR1-apn-profile-5gprofileb] apn 5gnetb
   [AR1-apn-profile-5gprofileb] sim-id 2
   [AR1-apn-profile-5gprofileb] quit
   ```
   b. 使能轮询DCC功能，配置自动拨号连接。
   ```
   [AR1] interface Cellular 1/0/0
   [AR1-Cellular1/0/0] dialer enable-circular
   [AR1-Cellular1/0/0] quit
   ```
   c. 配置NQA功能，探测5G主SIM卡对应链路的连通性。
   ```
   [AR1] nqa test-instance user test
   [AR1-nqa-user-test] test-type icmp
   [AR1-nqa-user-test] frequency 30
   [AR1-nqa-user-test] destination-address ipv4 114.114.114.114
   [AR1-nqa-user-test] start now
   [AR1-nqa-user-test] quit
   ```
   d. 在5G Cellular接口上绑定APN模板，同时绑定NQA测试例。
   ```
   [AR1-Cellular1/0/0] apn-profile 5gprofilea priority 120 track nqa user test
   Info: The configuration will become effective after link reset.
   [AR1-Cellular1/0/0] apn-profile 5gprofileb priority 110
   Info: The configuration will become effective after link reset.
   [AR1-Cellular1/0/0] shutdown
   [AR1-Cellular1/0/0] undo shutdown
   [AR1-Cellular1/0/0] quit
   ```
2. 配置企业分支子网，为内部用户自动分配IP地址。创建VLAN10，将GE0/0/1接口加入VLAN10，并配置DHCP功能。
   ```
   [AR1] vlan 10
   [AR1-vlan10] quit
   [AR1] interface GigabitEthernet 0/0/1
   [AR1-GigabitEthernet0/0/1] port link-type access
   [AR1-GigabitEthernet0/0/1] port default vlan 10
   [AR1-GigabitEthernet0/0/1] quit
   [AR1] dhcp enable
   [AR1] interface Vlanif 10
   [AR1-Vlanif10] ip address 10.1.1.1 24
   [AR1-Vlanif10] dhcp select interface
   [AR1-Vlanif10] quit
   ```
3. 配置分支NAT功能。
   ```
   [AR1] acl number 3000
   [AR1-acl-adv-3000] rule 5 permit ip
   [AR1-acl-adv-3000] quit
   [AR1] interface Cellular 1/0/0
   [AR1-Cellular1/0/0] nat outbound 3000
   [AR1-Cellular1/0/0] quit
   ```

 版权所有 © 华为技术有限公司

4. 配置静态路由，出接口为5G Cellular1/0/0，使企业分支和Internet之间的路由互通。

```
[AR1] ip route-static 0.0.0.0 0.0.0.0 Cellular 1/0/0
[AR1] quit
```

验证

1. 在AR1上执行命令**display ip interface brief Cellular 1/0/0**，查看Cellular1/0/0接口获取到的IP地址。

```
<AR1> display ip interface brief Cellular 1/0/0
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
(E): E-Trunk down
Interface                   IP Address/Mask      Physical   Protocol

Cellular1/0/0               1.1.1.1/32           up         up
```

2. 在AR1上执行命令**display Cellular 1/0/0 all**，查看Cellular1/0/0接口的状态信息。

```
<AR1> display Cellular 1/0/0 all
Modem State:
Hardware Information.
=====================
Model = RG801
Modem Type = 5G module
Modem Firmware Version = RG801HEAAAR01A07M8G
Hardware Version = HiB5000_MODEM Ver.A
Integrate circuit card identity (ICCID) = 98681020100202000069
International Mobile Subscriber Identity (IMSI) = 460070075591996
Mobile Station International ISDN Number (MSISDN) = None
International Mobile Equipment Identity (IMEI) = 867147050004457
Factory Serial Number (FSN) = 0123456789ABCDEF
Modem Status = Online
Profile Information.
====================
Profile 1
--------
PDP Type = IPv4, Header Compression = OFF
Data Compression = OFF
Access Point Name (APN) = 5gneta
Packet Session Status = Active
* - Default profile
Network Information.
====================
Current Service Status = Service available
Service Domain = Combined
Current Service = PS
Packet Service = Attached
Packet Session Status = Active
Current Roaming Status = Roaming
Network Selection Mode = Automatic
Network Connection Mode = Automatic
Current Network Connection = 5G(NSA)
Mobile Country Code (MCC) = 369
Mobile Network Code (MNC) = 77
Mobile Operator Information = Unknown
Tracking Area Code (TAC) = 1002
Cell ID = 9881858
Radio Information.
==================
Current Bands : AUTO
LTE:
Current Band = B3
Current RSSI >= -51 dBm
Current RSRP = -71 dBm (strong)
Current RSRQ = -6 dB
```

 版权所有 © 华为技术有限公司

```
Current SINR = 14 dB
NR:
Current Band = N78
Current RSRP = -65 dBm (strong)
Current RSRQ = -10 dB
Current SINR = 36 dB
Bands supported :
  WCDMA: WCDMA850 WCDMA900 WCDMA2100
  FDD LTE: B1 B3 B5 B7 B8 B20 B28
  TDD LTE: B34 B38 B39 B40 B41
  FDD NR: N1 N3 N28
  TDD NR: N41 N77 N78 N79
  SUL NR: N80
Modem Security Information.
============================
SIM ID = 1
PIN Verification = Disabled
PIN Status = Ready
Number of Retries remaining = 3
SIM Status = OK
```

3. 当主SIM卡故障时，执行命令**display ip interface brief Cellular 1/0/0**，查看Cellular1/0/0接口可以获取到运营商B分配的IP地址。

```
<AR1> display ip interface brief Cellular 1/0/0
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
(E): E-Trunk down
Interface                   IP Address/Mask      Physical   Protocol

Cellular1/0/0               2.2.2.2/32           up         up
```

配置文件

AR1配置文件

```
#
 sysname AR1
#
vlan batch 10
#
dhcp enable
#
acl number 3000
 rule 5 permit ip
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
 dhcp select interface
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 10
#
interface Cellular1/0/0
 dialer enable-circular
 apn-profile 5gprofilea priority 120 track nqa user test
 apn-profile 5gprofileb priority 110
 dialer timer autodial 10
 nat outbound 3000
 modem auto-recovery dial action modem-reboot fail-times 128
 modem auto-recovery icmp-unreachable action modem-reboot
 modem auto-recovery services-unavailable action modem-reboot test-times 0 interval 3600
 ip address negotiate
#
apn profile 5gprofilea
 apn 5gneta
apn profile 5gprofileb
 apn 5gnetb
```

 版权所有 © 华为技术有限公司

```
 sim-id 2
#
ip route-static 0.0.0.0 0.0.0.0 Cellular1/0/0
#
nqa test-instance user test
 test-type icmp
 destination-address ipv4 114.114.114.114
 frequency 30
 start now
#
return
```

7.3.2 配置企业使用有线和 5G 主备双链路上网示例

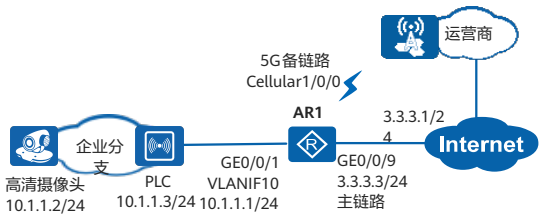
场景介绍

典型的企业分支通常还是采用有线链路作为主链路，例如以太链路、MPLS专线等。为了提升分支站点的可靠性，企业一般都会部署两条上行链路，一条为主链路，一条为备链路。如果两条上行链路都采用有线，成本会比较高，因为要租用两条专线。因此，在5G链路出现以前，一般使用有线链路为主链路，4G无线链路作为备份链路。5G链路出现以后，由于5G链路开通快、带宽大、成本低等优点，企业可以选择使用5G链路作为有线链路的备份链路。

组网方式

如图1所示，企业分支和总部之间通过Internet网络互通，企业分支使用AR1企业路由器作为出口网关。为了提高链路可靠性，AR1企业路由器部署了两条上行链路接入Internet。其中以太有线链路作为主链路，5G无线链路作为备链路。

图 7-16 配置企业使用有线和 5G 主备双链路上网组网图



数据准备

表 7-20 数据准备表

项目	数据	说明
运营商给分支分配的APN名称	5gnet	APN名称需提前从运营商处获取。
运营商给分支5G Cellular接口分配的IP地址	1.1.1.1/32	5G Cellular接口拨号接入运营商后，运营商给5G Cellular接口自动分配的IP地址。

 版权所有 © 华为技术有限公司

项目	数据	说明
运营商给分支GE0/0/9接口分配的IP地址	3.3.3.3/24	分支AR1的主链路为以太链路，接口GE0/0/9通过静态方式配置IP地址。分支用户优先通过该链路接入Internet。
运营商对接分支GE0/0/9接口的IP地址	3.3.3.1/24	运营商对接分支GE0/0/9接口的IP地址用于配置路由信息，使分支和Internet之间的路由互通。
分支AR1 LAN侧接口信息	所属VLAN：10 网关地址：VLANIF10（10.1.1.1/24） LAN侧物理接口：GE0/0/1	VLAN 10为分支子网用户所在的VLAN，且分支子网用户的网关为VLANIF10接口。

配置思路

1. 配置5G Cellular接口的连接参数，实现5G Cellular接口接入5G网络。
2. 配置企业子网，为内部用户自动分配IP地址。
3. 配置分支NAT功能，实现分支的内部用户可以访问Internet。
4. 配置静态路由，使有线链路的优先级高于5G无线链路。当有线主链路故障后，流量可以快速切换到5G备链路上转发。

说明

在5G Cellular接口下执行命令**dialer enable-circular**配置轮询拨号功能时，设备会同时下发自动拨号、IP地址协商和5G Modem自愈的相关配置，无需再重复配置。

操作步骤

1. 配置5G Cellular接口的连接参数，实现5G Cellular接口接入5G网络。
   a. 创建APN模板。
   ```
   <Huawei> system-view
   [Huawei] sysname AR1
   [AR1] apn profile 5gprofile
   [AR1-apn-profile-5gprofile] apn 5gnet
   [AR1-apn-profile-5gprofile] quit
   ```
   b. 使能轮询DCC功能
   ```
   [AR1] interface Cellular 1/0/0
   [AR1-Cellular1/0/0] dialer enable-circular
   ```
   c. 在5G Cellular接口上绑定APN模板。
   ```
   [AR1-Cellular1/0/0] apn-profile 5gprofile
   Info: The configuration will become effective after link reset.
   [AR1-Cellular1/0/0] shutdown
   [AR1-Cellular1/0/0] undo shutdown
   [AR1-Cellular1/0/0] quit
   ```
2. 配置分支子网，创建VLAN10，将GE0/0/1接口加入VLAN10，并配置DHCP功能。
   ```
   [AR1] vlan 10
   [AR1-vlan10] quit
   [AR1] interface GigabitEthernet 0/0/1
   [AR1-GigabitEthernet0/0/1] port link-type access
   [AR1-GigabitEthernet0/0/1] port default vlan 10
   ```

 版权所有 © 华为技术有限公司

```
[AR1-GigabitEthernet0/0/1] quit
[AR1] dhcp enable
[AR1] interface Vlanif 10
[AR1-Vlanif10] ip address 10.1.1.1 24
[AR1-Vlanif10] dhcp select interface
[AR1-Vlanif10] quit
```

3. 配置分支WAN侧接口GE0/0/9的IP地址。

```
[AR1] interface GigabitEthernet 0/0/9
[AR1-GigabitEthernet0/0/9] ip address 3.3.3.3 24
[AR1-GigabitEthernet0/0/9] quit
```

4. 配置分支NAT功能。

```
[AR1] acl number 3000
[AR1-acl-adv-3000] rule 5 permit ip
[AR1-acl-adv-3000] quit
[AR1] interface Cellular 1/0/0
[AR1-Cellular1/0/0] nat outbound 3000
[AR1-Cellular1/0/0] quit
[AR1] interface GigabitEthernet 0/0/9
[AR1-GigabitEthernet0/0/9] nat outbound 3000
[AR1-GigabitEthernet0/0/9] quit
```

5. 配置两条分支缺省路由，有线链路路由优先级高，5G链路路由优先级低。

```
[AR1] ip route-static 0.0.0.0 0 Cellular 1/0/0
[AR1] ip route-static 0.0.0.0 0.0.0.0 3.3.3.1 preference 30
[AR1] quit
```

验证

1. 在AR1上执行命令**display ip interface brief Cellular 1/0/0**，查看Cellular1/0/0接口获取到的IP地址。

```
<AR1> display ip interface brief Cellular 1/0/0
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
(E): E-Trunk down
Interface                   IP Address/Mask      Physical   Protocol

Cellular1/0/0               1.1.1.1/32           up         up
```

2. 在AR1上执行命令**display Cellular 1/0/0 all**，查看Cellular1/0/0接口的状态信息。

```
<AR1> display Cellular 1/0/0 all
Modem State:
Hardware Information.
=====================
Model = RG801
Modem Type = 5G module
Modem Firmware Version = RG801HEAAAR01A07M8G
Hardware Version = HiB5000_MODEM Ver.A
Integrate circuit card identity (ICCID) = 98681020100202000069
International Mobile Subscriber Identity (IMSI) = 460070075591996
Mobile Station International ISDN Number (MSISDN) = None
International Mobile Equipment Identity (IMEI) = 867147050004457
Factory Serial Number (FSN) = 0123456789ABCDEF
Modem Status = Online
Profile Information.
====================
Profile 1
--------
PDP Type = IPv4, Header Compression = OFF
Data Compression = OFF
Access Point Name (APN) = 5gnet
Packet Session Status = Active
* - Default profile
Network Information.
====================
```

 版权所有 © 华为技术有限公司

```
Current Service Status = Service available
Service Domain = Combined
Current Service = PS
Packet Service = Attached
Packet Session Status = Active
Current Roaming Status = Roaming
Network Selection Mode = Automatic
Network Connection Mode = LTE-NR
Current Network Connection = 5G(NSA)
Mobile Country Code (MCC) = 369
Mobile Network Code (MNC) = 77
Mobile Operator Information = Unknown
Tracking Area Code (TAC) = 1002
Cell ID = 9881858
Radio Information.
==================
Current Bands :
  WCDMA: AUTO
  LTE: B3
  NR: AUTO
LTE:
Current Band = B3
Current RSSI >= -51 dBm
Current RSRP = -71 dBm (strong)
Current RSRQ = -6 dB
Current SINR = 6 dB
NR:
Current Band = N78
Current RSRP = -65 dBm (strong)
Current RSRQ = -10 dB
Current SINR = 38 dB
Bands supported :
  WCDMA: WCDMA850 WCDMA900 WCDMA2100
  FDD LTE: B1 B3 B5 B7 B8 B20 B28
  TDD LTE: B34 B38 B39 B40 B41
  FDD NR: N1 N3 N28
  TDD NR: N41 N77 N78 N79
Modem Security Information.
===========================
SIM ID = 1
PIN Verification = Disabled
PIN Status = Ready
Number of Retries remaining = 3
SIM Status = OK
```

3. 在AR1的GE0/0/9接口上执行命令**shutdown**，模拟以太主链路故障。

```
<AR1> system-view
[AR1] interface GigabitEthernet 0/0/9
[AR1-GigabitEthernet0/0/9] shutdown
[AR1-GigabitEthernet0/0/9] quit
[AR1] quit
```

4. 在AR1上执行命令**ping -a 10.1.1.1 10.2.1.1**，模拟分支用户访问总部用户的流量，流量能Ping通。

```
<AR1> ping -a 10.1.1.1 10.2.1.1
  PING 10.2.1.1: 56  data bytes, press CTRL_C to break
    Reply from 10.2.1.1: bytes=56 Sequence=1 ttl=255 time=51 ms
    Reply from 10.2.1.1: bytes=56 Sequence=2 ttl=255 time=35 ms
    Reply from 10.2.1.1: bytes=56 Sequence=3 ttl=255 time=45 ms
    Reply from 10.2.1.1: bytes=56 Sequence=4 ttl=255 time=40 ms
    Reply from 10.2.1.1: bytes=56 Sequence=5 ttl=255 time=37 ms

  --- 10.2.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 35/41/51 ms
```

 版权所有 © 华为技术有限公司

配置文件

AR1配置文件

```
#
 sysname AR1
#
vlan batch 10
#
dhcp enable
#
acl number 3000
 rule 5 permit ip
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
 dhcp select interface
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 10
#
interface GigabitEthernet0/0/9
 ip address 3.3.3.3 255.255.255.0
 nat outbound 3000
#
interface Cellular1/0/0
 dialer enable-circular
 apn-profile 5gprofile
 dialer timer autodial 10
 nat outbound 3000
 modem auto-recovery dial action modem-reboot fail-times 128
 modem auto-recovery icmp-unreachable action modem-reboot
 modem auto-recovery services-unavailable action modem-reboot test-times 0 interval 3600
 ip address negotiate
#
apn profile 5gprofile
 apn 5gnet
#
ip route-static 0.0.0.0 0.0.0.0 Cellular1/0/0
ip route-static 0.0.0.0 0.0.0.0 3.3.3.1 preference 30
#
return
```

7.3.3 配置分支使用 5G 双链路和总部建立 GRE 主备隧道互联示例

场景介绍

可靠性是企业组网中必须考虑的一个重要因素，特别是对于那些大型企业，业务一旦中断，可能会损失惨重。为了增强企业分支接入Internet的可靠性，分支与总部互联时一般都会部署两条广域上行链路，一条为主链路，一条为备链路。当主链路发生故障后，流量可以切换到备链路上转发，保证业务的连续性。在某些场景，不仅需要高可靠性，还需要链路之间可以快速切换。例如工业控制场景，需要亚秒级甚至毫秒级的切换。还有一些场景，对上行带宽的要求比较高，例如视频监控回传场景。

为了满足这些多样化的需求，企业可以选择使用两条5G链路作为广域上行链路，并配置BFD功能。由于5G链路开通快、带宽大、成本低，加上BFD快速检测机制，当主链路发生故障时，业务可以立即切换到5G备份链路上转发，减少业务中断时间，提高网络的可靠性。

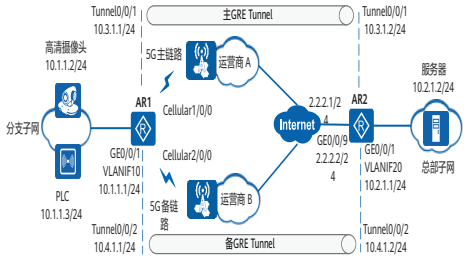
组网方式

如图1所示，企业分支和总部之间通过Internet网络互联。企业分支使用AR1企业路由器作为出口网关。为了提高链路可靠性，AR1企业路由器上插了两块5G单板，提供两

 版权所有 © 华为技术有限公司

条5G链路接入Internet。当企业分支和总部之间需要交互三层业务时，分支和总部之间要在两条5G链路上分别构建GRE隧道，通过配置不同的静态路由优先级实现业务主备。BFD检测并监控主GRE隧道的连通状态，实现分支及总部之间三层业务的快速收敛。

图 7-17 配置分支使用 5G 双链路和总部建立 GRE 主备隧道互联组网图



数据准备

表 7-21 数据准备表

项目	数据	说明
运营商A给分支分配的APN名称	5gneta	APN名称需提前从运营商处获取。
运营商B给分支分配的APN名称	5gnetb	
运营商A给分支主5G Cellular1/0/0接口分配的IP地址	1.1.1.1/32	5G Cellular接口拨号接入运营商后，运营商给5G Cellular接口自动分配的IP地址。 **说明** 使用GRE隧道时，要求运营商给5G Cellular接口分配的IP地址为固定IP地址。本例中，假设运营商为5G Cellular接口分配的固定IP地址为1.1.1.1和3.3.3.3。
运营商B给分支备5G Cellular2/0/0接口分配的IP地址	3.3.3.3/32	
运营商给总部GE0/0/9接口分配的IP地址	2.2.2.2/24	总部AR2通过有线的方式接入Internet，该有线接口GE0/0/9采用静态方式配置IP地址。
运营商对接总部GE0/0/9接口的IP地址	2.2.2.1/24	运营商对接总部AR2 GE0/0/9接口的IP地址用于配置路由信息，使总部和Internet之间的路由互通。
分支AR1主Tunnel0/0/1接口的IP地址	10.3.1.1/24	分支和总部主备GRE隧道的Tunnel接口地址。
分支AR1备Tunnel0/0/2接口的IP地址	10.4.1.1/24	

 版权所有 © 华为技术有限公司

项目	数据	说明
总部AR2主Tunnel0/0/1接口的IP地址	10.3.1.2/24	
总部AR2备Tunnel0/0/2接口的IP地址	10.4.1.2/24	
分支AR1 LAN侧接口信息	所属VLAN：10 网关地址：VLANIF10（10.1.1.1/24） LAN侧物理接口：GE0/0/1	VLAN 10为分支子网用户所在的VLAN，且分支子网用户的网关为VLANIF10接口。
总部AR2 LAN侧接口信息	所属VLAN：20 网关地址：VLANIF20（10.2.1.1/24） LAN侧物理接口：GE0/0/1	VLAN 20为总部子网用户所在的VLAN，且总部子网用户的网关为VLANIF20接口。

TCP MSS 参数配置说明

为了减少网络传输中不必要的分片和重组，网络规划时需要合理设置终端发出的报文大小。对于TCP报文，可以配置5G AR设备的TCP MSS值，通过修改应用层报文数据包的长度来避免报文分片。在5G 2B专线场景中，TCP MSS取值比较简单，在隧道两端AR设备的LAN侧接入物理口或VLANIF口上配置TCP MSS为推荐值1200。

配置思路

1. 配置5G Cellular接口的连接参数，实现5G Cellular接口接入5G网络。
2. 配置企业子网，为内部用户自动分配IP地址。
3. 配置Tunnel接口，创建主备GRE隧道，使分支和总部之间的业务流量通过GRE隧道传输。
4. 配置BFD会话，探测分支和总部之间主GRE隧道的连通性。
5. 配置静态路由，使企业分支和总部子网的用户可以互通。

说明

在5G Cellular接口下执行命令**dialer enable-circular**配置轮询拨号功能时，设备会同时下发自动拨号、IP地址协商和5G Modem自愈的相关配置，无需再重复配置。

操作步骤

1. 配置5G Cellular接口的连接参数，实现5G Cellular接口接入5G网络。
   a. 创建APN模板。

```
<Huawei> system-view
[Huawei] sysname AR1
```

```
[AR1] apn profile 5gprofilea
[AR1-apn-profile-5gprofilea] apn 5gneta
[AR1-apn-profile-5gprofilea] quit
[AR1] apn profile 5gprofileb
[AR1-apn-profile-5gprofileb] apn 5gnetb
[AR1-apn-profile-5gprofileb] quit
```

b. 使能轮询DCC功能，配置自动拨号连接。

```
[AR1] interface Cellular 1/0/0
[AR1-Cellular1/0/0] dialer enable-circular
[AR1-Cellular1/0/0] quit
[AR1] interface Cellular 2/0/0
[AR1-Cellular2/0/0] dialer enable-circular
[AR1-Cellular2/0/0] quit
```

c. 在5G Cellular接口上绑定APN模板。

```
[AR1] interface Cellular 1/0/0
[AR1-Cellular1/0/0] apn-profile 5gprofilea
Info: The configuration will become effective after link reset.
[AR1-Cellular1/0/0] shutdown
[AR1-Cellular1/0/0] undo shutdown
[AR1-Cellular1/0/0] quit
[AR1] interface Cellular 2/0/0
[AR1-Cellular2/0/0] apn-profile 5gprofileb
Info: The configuration will become effective after link reset.
[AR1-Cellular2/0/0] shutdown
[AR1-Cellular2/0/0] undo shutdown
[AR1-Cellular2/0/0] quit
```

2. 配置企业子网，为内部用户自动分配IP地址。

a. 配置分支子网，创建VLAN10，将GE0/0/1接口加入VLAN10。配置VLANIF 10接口TCP最大报文段长度为1200字节并配置DHCP功能。

```
[AR1] vlan 10
[AR1-vlan10] quit
[AR1] interface GigabitEthernet 0/0/1
[AR1-GigabitEthernet0/0/1] port link-type access
[AR1-GigabitEthernet0/0/1] port default vlan 10
[AR1-GigabitEthernet0/0/1] quit
[AR1] dhcp enable
[AR1] interface Vlanif 10
[AR1-Vlanif10] ip address 10.1.1.1 24
[AR1-Vlanif10] dhcp select interface
[AR1-Vlanif10] tcp adjust-mss 1200
[AR1-Vlanif10] quit
```

b. 配置总部子网，创建VLAN20，将GE0/0/1接口加入VLAN20。配置VLANIF 20接口TCP最大报文段长度为1200字节并配置DHCP功能。

```
<Huawei> system-view
[Huawei] sysname AR2
[AR2] vlan 20
[AR2-vlan20] quit
[AR2] interface GigabitEthernet 0/0/1
[AR2-GigabitEthernet0/0/1] port link-type access
[AR2-GigabitEthernet0/0/1] port default vlan 20
[AR2-GigabitEthernet0/0/1] quit
[AR2] dhcp enable
[AR2] interface Vlanif 20
[AR2-Vlanif20] ip address 10.2.1.1 24
[AR2-Vlanif20] dhcp select interface
[AR2-Vlanif20] tcp adjust-mss 1200
[AR2-Vlanif20] quit
```

3. 配置Tunnel接口，创建GRE隧道。

a. 配置总部WAN侧接口GE0/0/9的IP地址。

```
[AR2] interface GigabitEthernet 0/0/9
[AR2-GigabitEthernet0/0/9] ip address 2.2.2.2 24
[AR2-GigabitEthernet0/0/9] quit
```

b. 配置总部的两个Tunnel接口。

 版权所有 © 华为技术有限公司

```
[AR2] interface Tunnel0/0/1
[AR2-Tunnel0/0/1] tunnel-protocol gre
Warning: After this tunnel encapsulation protocol was configured, the MTU and other parameter settings of the tunnel were deleted.
[AR2-Tunnel0/0/1] ip address 10.3.1.2 255.255.255.0
[AR2-Tunnel0/0/1] source GigabitEthernet 0/0/9
[AR2-Tunnel0/0/1] destination 1.1.1.1
[AR2-Tunnel0/0/1] quit
[AR2] interface Tunnel0/0/2
[AR2-Tunnel0/0/2] tunnel-protocol gre
Warning: After this tunnel encapsulation protocol was configured, the MTU and other parameter settings of the tunnel were deleted.
[AR2-Tunnel0/0/2] ip address 10.4.1.2 255.255.255.0
[AR2-Tunnel0/0/2] source GigabitEthernet 0/0/9
[AR2-Tunnel0/0/2] destination 3.3.3.3
[AR2-Tunnel0/0/2] quit
```

c. 配置分支的两个Tunnel接口。

```
[AR1] interface Tunnel0/0/1
[AR1-Tunnel0/0/1] tunnel-protocol gre
Warning: After this tunnel encapsulation protocol was configured, the MTU and other parameter settings of the tunnel were deleted.
[AR1-Tunnel0/0/1] ip address 10.3.1.1 255.255.255.0
[AR1-Tunnel0/0/1] source Cellular 1/0/0
[AR1-Tunnel0/0/1] destination 2.2.2.2
[AR1-Tunnel0/0/1] quit
[AR1] interface Tunnel0/0/2
[AR1-Tunnel0/0/2] tunnel-protocol gre
Warning: After this tunnel encapsulation protocol was configured, the MTU and other parameter settings of the tunnel were deleted.
[AR1-Tunnel0/0/2] ip address 10.4.1.1 255.255.255.0
[AR1-Tunnel0/0/2] source Cellular 2/0/0
[AR1-Tunnel0/0/2] destination 2.2.2.2
[AR1-Tunnel0/0/2] quit
```

4. 配置BFD会话，探测分支和总部之间主GRE隧道的连通性。

a. 配置分支的BFD会话。

```
[AR1] bfd
[AR1-bfd] quit
[AR1] bfd aa bind peer-ip 10.3.1.2 source-ip 10.3.1.1
[AR1-bfd-session-aa] discriminator local 10
[AR1-bfd-session-aa] discriminator remote 20
[AR1-bfd-session-aa] commit
Info: The configuration succeeds, but BFD session cannot be created for the moment because the route cannot be found.
[AR1-bfd-session-aa] quit
```

b. 配置总部的BFD会话。

```
[AR2] bfd
[AR2-bfd] quit
[AR2] bfd bb bind peer-ip 10.3.1.1 source-ip 10.3.1.2
[AR2-bfd-session-bb] discriminator local 20
[AR2-bfd-session-bb] discriminator remote 10
[AR2-bfd-session-bb] commit
Info: The configuration succeeds, but BFD session cannot be created for the moment because the route cannot be found.
[AR2-bfd-session-bb] quit
```

5. 配置静态路由，使企业分支和总部子网的用户可以互通。

a. 配置分支的静态路由，两条静态路由的出接口为5G Cellular接口，两条到总部子网的静态路由的出接口为Tunnel接口，并在主隧道接口Tunnel0/0/1所在的路由上绑定BFD会话。

```
[AR1] ip route-static 2.2.2.2 32 Cellular 1/0/0
[AR1] ip route-static 2.2.2.2 32 Cellular 2/0/0 preference 70
[AR1] ip route-static 10.2.1.0 255.255.255.0 Tunnel 0/0/1 track bfd-session aa
[AR1] ip route-static 10.2.1.0 255.255.255.0 Tunnel 0/0/2 preference 70
[AR1] quit
```

 版权所有 © 华为技术有限公司

b. 配置总部的静态路由，并在主隧道接口Tunnel0/0/1所在的路由上绑定BFD会话。

```
[AR2] ip route-static 0.0.0.0 0.0.0.0 2.2.2.1
[AR2] ip route-static 10.1.1.0 255.255.255.0 Tunnel 0/0/1 track bfd-session bb
[AR2] ip route-static 10.1.1.0 255.255.255.0 Tunnel 0/0/2 preference 70
[AR2] quit
```

验证

1. 在AR1上执行命令**display ip interface brief Cellular 1/0/0**，查看Cellular1/0/0接口获取到的IP地址。

```
<AR1> display ip interface brief Cellular 1/0/0
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
(E): E-Trunk down
Interface                   IP Address/Mask      Physical   Protocol

Cellular1/0/0               1.1.1.1/32           up         up
```

2. 在AR1上执行命令**display ip interface brief Cellular 2/0/0**，查看Cellular2/0/0接口获取到的IP地址。

```
<AR1> display ip interface brief Cellular 2/0/0
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
(E): E-Trunk down
Interface                   IP Address/Mask      Physical   Protocol

Cellular2/0/0               3.3.3.3/32           up         up
```

3. 在AR1上执行命令**display Cellular 1/0/0 all**，查看Cellular1/0/0接口的状态信息。

```
<AR1> display Cellular 1/0/0 all
Modem State:
Hardware Information.
=====================
Model = RG801
Modem Type = 5G module
Modem Firmware Version = RG801HEAAAR01A07M8G
Hardware Version = HiB5000_MODEM Ver.A
Integrate circuit card identity (ICCID) = 98681020100202000069
International Mobile Subscriber Identity (IMSI) = 460070075591996
Mobile Station International ISDN Number (MSISDN) = None
International Mobile Equipment Identity (IMEI) = 867147050004457
Factory Serial Number (FSN) = 0123456789ABCDEF
Modem Status = Online
Profile Information.
====================
Profile 1
--------
PDP Type = IPv4, Header Compression = OFF
Data Compression = OFF
Access Point Name (APN) = 5gneta
Packet Session Status = Active
* - Default profile
Network Information.
====================
Current Service Status = Service available
Service Domain = Combined
Current Service = PS
Packet Service = Attached
Packet Session Status = Active
Current Roaming Status = Roaming
Network Selection Mode = Automatic
Network Connection Mode = LTE-NR
```

 版权所有 © 华为技术有限公司

```
Current Network Connection = 5G(NSA)
Mobile Country Code (MCC) = 369
Mobile Network Code (MNC) = 77
Mobile Operator Information = Unknown
Tracking Area Code (TAC) = 1002
Cell ID = 9881858
Radio Information.
==================
Current Bands :
  WCDMA: AUTO
  LTE: B3
  NR: AUTO
LTE:
Current Band = B3
Current RSSI >= -51 dBm
Current RSRP = -68 dBm (strong)
Current RSRQ >= -3 dB
Current SINR = 6 dB
NR:
Current Band = N78
Current RSRP = -64 dBm (strong)
Current RSRQ = -10 dB
Current SINR = 35 dB
Bands supported :
  WCDMA: WCDMA850 WCDMA900 WCDMA2100
  FDD LTE: B1 B3 B5 B7 B8 B20 B28
  TDD LTE: B34 B38 B39 B40 B41
  FDD NR: N1 N3 N28
  TDD NR: N41 N77 N78 N79
  SUL NR: N80
Modem Security Information.
===========================
SIM ID = 1
PIN Verification = Disabled
PIN Status = Ready
Number of Retries remaining = 3
SIM Status = OK
```

4. 在AR1上执行**display bfd session all**命令，可以看到BFD会话已经建立，且状态为UP。

```
<AR1> display bfd session all
--------------------------------------------------------------------------------
Local Remote     PeerIpAddr      State     Type        InterfaceName
--------------------------------------------------------------------------------
10    20         10.3.1.2        Up        S_IP_PEER         -
--------------------------------------------------------------------------------
    Total UP/DOWN Session Number : 1/0
```

5. 在AR1的Cellular1/0/0接口上执行命令**shutdown**，模拟5G主链路故障。

```
<AR1> system-view
[AR1] interface Cellular 1/0/0
[AR1-Cellular1/0/0] shutdown
[AR1-Cellular1/0/0] quit
[AR1] quit
```

6. 在AR1上执行命令**ping -a 10.1.1.1 10.2.1.1**，模拟分支用户访问总部用户的流量，流量能Ping通。

```
<AR1> ping -a 10.1.1.1 10.2.1.1
  PING 10.2.1.1: 56  data bytes, press CTRL_C to break
    Reply from 10.2.1.1: bytes=56 Sequence=1 ttl=255 time=51 ms
    Reply from 10.2.1.1: bytes=56 Sequence=2 ttl=255 time=35 ms
    Reply from 10.2.1.1: bytes=56 Sequence=3 ttl=255 time=45 ms
    Reply from 10.2.1.1: bytes=56 Sequence=4 ttl=255 time=40 ms
    Reply from 10.2.1.1: bytes=56 Sequence=5 ttl=255 time=37 ms

  --- 10.2.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 35/41/51 ms
```

 版权所有 © 华为技术有限公司

配置文件

AR1配置文件

```
#
 sysname AR1
#
vlan batch 10
#
dhcp enable
#
bfd
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
 dhcp select interface
 tcp adjust-mss 1200
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 10
#
interface Cellular1/0/0
 dialer enable-circular
 apn-profile 5gprofilea
 dialer timer autodial 10
 modem auto-recovery dial action modem-reboot fail-times 128
 modem auto-recovery icmp-unreachable action modem-reboot
 modem auto-recovery services-unavailable action modem-reboot test-times 0 interval 3600
 ip address negotiate
#
interface Cellular2/0/0
 dialer enable-circular
 apn-profile 5gprofileb
 dialer timer autodial 10
 modem auto-recovery dial action modem-reboot fail-times 128
 modem auto-recovery icmp-unreachable action modem-reboot
 modem auto-recovery services-unavailable action modem-reboot test-times 0 interval 3600
 ip address negotiate
#
interface Tunnel0/0/1
 ip address 10.3.1.1 255.255.255.0
 tunnel-protocol gre
 source Cellular1/0/0
 destination 2.2.2.2
#
interface Tunnel0/0/2
 ip address 10.4.1.1 255.255.255.0
 tunnel-protocol gre
 source Cellular2/0/0
 destination 2.2.2.2
#
apn profile 5gprofilea
 apn 5gneta
apn profile 5gprofileb
 apn 5gnetb
#
bfd aa bind peer-ip 10.3.1.2 source-ip 10.3.1.1
 discriminator local 10
 discriminator remote 20
 commit
#
ip route-static 2.2.2.2 255.255.255.255 Cellular1/0/0
ip route-static 2.2.2.2 255.255.255.255 Cellular2/0/0 preference 70
ip route-static 10.2.1.0 255.255.255.0 Tunnel0/0/1 track bfd-session aa
ip route-static 10.2.1.0 255.255.255.0 Tunnel0/0/2 preference 70
#
return
```

AR2配置文件

 版权所有 © 华为技术有限公司

```
#
 sysname AR2
#
vlan batch 20
#
dhcp enable
#
bfd
#
interface Vlanif20
 ip address 10.2.1.1 255.255.255.0
 dhcp select interface
 tcp adjust-mss 1200
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 20
#
interface GigabitEthernet0/0/9
 ip address 2.2.2.2 255.255.255.0
#
interface Tunnel0/0/1
 ip address 10.3.1.2 255.255.255.0
 tunnel-protocol gre
 source GigabitEthernet0/0/9
 destination 1.1.1.1
#
interface Tunnel0/0/2
 ip address 10.4.1.2 255.255.255.0
 tunnel-protocol gre
 source GigabitEthernet0/0/9
 destination 3.3.3.3
#
bfd bb bind peer-ip 10.3.1.1 source-ip 10.3.1.2
 discriminator local 20
 discriminator remote 10
 commit
#
ip route-static 0.0.0.0 0.0.0.0 2.2.2.1
ip route-static 10.1.1.0 255.255.255.0 Tunnel0/0/1 track bfd-session bb
ip route-static 10.1.1.0 255.255.255.0 Tunnel0/0/2 preference 70
#
return
```

7.3.4 配置分支使用 5G 双链路和总部建立 Ethernet over GRE 主备隧道互联示例

场景介绍

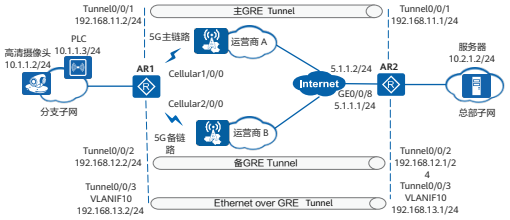
Ethernet over GRE是将以太网协议的报文通过GRE封装后，在另一个网络层协议（如IPv4）的网络中传输。当企业总部和分支的网络都是以太网络，且总部和分支之间需要交互二层业务时，AR可以通过插入两个5G单板，与对端设备建立两个GRE隧道形成两条承载链路。再采用Ethernet over GRE技术，将以太业务封装在GRE隧道中，通过GRE链路进行主备切换，达到双5G上行快速倒换或负载分担的目的。

组网需求

如图1所示，企业分支和总部之间通过Internet网络互通。企业分支使用AR1企业路由器作为出口网关，为了提高链路可靠性，AR1企业路由器上插了两块5G单板，提供两条5G链路接入Internet。企业分支和总部之间需要交互二层业务时，分支和总部之间构建Ethernet over GRE隧道，通过配置不同的静态路由优先级实现业务主备。BFD检测并监控主Ethernet over GRE隧道的连通状态，实现分支及总部之间二层业务的快速收敛。

 版权所有 © 华为技术有限公司

图 7-18 配置分支使用 5G 双链路和总部建立 Ethernet over GRE 主备隧道互联组网图



数据准备

表 7-22 数据准备表

项目	数据	说明
运营商A给分支分配的APN名称	5gneta	APN名称需提前从运营商处获取。
运营商B给分支分配的APN名称	5gnetb	
运营商A给分支主5G Cellular1/0/0接口分配的IP地址	1.1.1.1/32	5G Cellular接口拨号接入运营商后，运营商给5G Cellular接口自动分配的IP地址。 **说明** 使用GRE隧道时，要求运营商给5G Cellular接口分配的IP地址为固定IP地址。本例中，假设运营商为5G Cellular接口分配的固定IP地址为1.1.1.1和3.3.3.3。
运营商B给分支备5G Cellular2/0/0接口分配的IP地址	3.3.3.3/32	
运营商给总部GE0/0/8接口分配的IP地址	5.1.1.1/24	总部AR2通过有线的方式接入Internet，该有线接口GE0/0/8采用静态方式配置IP地址。
运营商对接总部GE0/0/8接口的IP地址	5.1.1.2/24	运营商对接总部GE0/0/8接口的IP地址用于配置路由信息，使总部和Internet之间的路由互通。
分支AR1主Tunnel0/0/1接口的IP地址	192.168.11.2/24	分支和总部主备GRE隧道的Tunnel接口地址。
分支AR1备Tunnel0/0/2接口的IP地址	192.168.12.2/24	
总部AR2主Tunnel0/0/1接口的IP地址	192.168.11.1/24	
总部AR2备Tunnel0/0/2接口的IP地址	192.168.12.1/24	

版权所有 © 华为技术有限公司

项目	数据	说明
分支AR1 LAN侧接口信息	LAN侧物理接口：GE0/0/1 绑定的VE接口：VE0/0/2 所属VLAN：10	分支和总部用户都在同一个网段，所属的VLAN都为VLAN 10。
总部AR2 LAN侧接口信息	LAN侧物理接口：GE0/0/1 绑定的VE接口：VE0/0/2 所属VLAN：10	
分支AR1 Tunnel0/0/3接口信息	IP地址：192.168.13.2/24 绑定的VE接口：VE0/0/1 所属VLAN：10	分支Ethernet over GRE隧道的地址。
总部AR2 Tunnel0/0/3接口信息	IP地址：192.168.13.1/24 绑定的VE接口：VE0/0/1 所属VLAN：10	总部Ethernet over GRE隧道的地址。

MTU 及 TCP MSS 参数配置说明

为了减少网络传输中不必要的分片和重组，网络规划时需要合理设置终端发出的报文大小，设置依据如下：

- 对于UDP报文，可以调节发送端的MTU值，如果发送端不支持调节MTU值，则需要在5G AR设备上调节MTU值，以确保报文在网络中传输时不会产生二次分片。
- 对于TCP报文，可以配置5G AR设备的TCP MSS值，通过修改应用层报文数据包的长度来避免报文分片。

在5G2B专线场景中，TCP MSS取值比较简单，在隧道两端AR设备的LAN侧接入物理口或VLANIF口上将配置TCP MSS配置为推荐值1200。MTU取值相对复杂，与如下三个参数有关，具体的配置方法请参见**表2** 。

- 单层GRE隧道组网，报文经过5G AR设备后会增加28字节，即单层GRE头长度为28字节。
- 双层GRE隧道组网，报文经过5G AR设备后会增加56字节，即双层GRE头长度为56字节。
- 5G网络中GTP封装会增加至少40字节，其中IP头20字节，UDP头8字节，GTP消息封装12字节。考虑到GTP支持扩展消息头，建议多预留1至2个扩展消息头长度（4或8字节）作为缓冲，即GTP封装头长度最大为48字节。

 版权所有 © 华为技术有限公司

表 7-23 MTU 参数配置方法

组网场景	在发送端调节MTU方值	或者在5G AR上调节MTU值
单层GRE隧道组网	发送端MTU值=网络中设备允许通过MTU值减去单层GRE头长度28，再减去GTP封装头长度48，即发送端MTU值=MTU-28-48。	5G接口MTU值=网络中设备允许通过MTU值减去GTP封装头长度，即5G接口MTU值=MTU-48。
双层GRE隧道组网	发送端MTU值=网络中设备允许通过MTU值减去双层GRE头长度56，再减去GTP封装头长度48，即发送端MTU值=MTU-56-48。	最外层L3 GRE隧道接口MTU值=网络中设备允许通过MTU值减去单层GRE头长度28，再减去GTP封装头长度48，即最外层L3 GRE隧道接口MTU值=MTU-28-48。本例中，MTU取值为1500。

配置思路

1. 配置5G Cellular接口的连接参数，实现5G Cellular接口接入5G网络。
2. 配置企业子网，为内部用户自动分配IP地址。
3. 配置Tunnel接口，创建主备GRE隧道，使企业分支和总部之间的业务流量通过GRE隧道传输。
4. 配置Ethernet over GRE功能，将二层VE接口绑定到WAN侧Tunnel接口和LAN侧物理接口，使企业分支和总部之间的以太报文可以通过Ethernet over GRE隧道传输。
5. 配置BFD会话，探测分支和总部之间主Ethernet over GRE隧道的连通性。
6. 配置静态路由，使企业分支和总部子网的用户可以互通。

说明

在5G Cellular接口下执行命令**dialer enable-circular**配置轮询拨号功能时，设备会同时下发自动拨号、IP地址协商和5G Modem自愈的相关配置，无需再重复配置。

操作步骤

1. 配置5G Cellular接口的连接参数，实现5G Cellular接口接入5G网络。
   a. 创建APN模板。

```
<Huawei> system-view
[Huawei] sysname AR1
[AR1] apn profile 5gprofilea
[AR1-apn-profile-5gprofilea] apn 5gneta
[AR1-apn-profile-5gprofilea] quit
[AR1] apn profile 5gprofileb
[AR1-apn-profile-5gprofileb] apn 5gnetb
[AR1-apn-profile-5gprofileb] quit
```

   b. 使能轮询DCC功能，配置自动拨号连接。

```
[AR1] interface Cellular 1/0/0
[AR1-Cellular1/0/0] dialer enable-circular
[AR1-Cellular1/0/0] quit
[AR1] interface Cellular 2/0/0
[AR1-Cellular2/0/0] dialer enable-circular
[AR1-Cellular2/0/0] quit
```

 版权所有 © 华为技术有限公司

c. 在5G Cellular接口上绑定APN模板。

```
[AR1] interface Cellular 1/0/0
[AR1-Cellular1/0/0] apn-profile 5gprofilea
Info: The configuration will become effective after link reset.
[AR1-Cellular1/0/0] shutdown
[AR1-Cellular1/0/0] undo shutdown
[AR1-Cellular1/0/0] quit
[AR1] interface Cellular 2/0/0
[AR1-Cellular2/0/0] apn-profile 5gprofileb
Info: The configuration will become effective after link reset.
[AR1-Cellular2/0/0] shutdown
[AR1-Cellular2/0/0] undo shutdown
[AR1-Cellular2/0/0] quit
```

2. 配置Tunnel接口，创建GRE隧道。

a. 配置总部WAN侧接口GE0/0/8的IP地址。

```
<Huawei> system-view
[Huawei] sysname AR2
[AR2] interface GigabitEthernet 0/0/8
[AR2-GigabitEthernet0/0/8] ip address 5.1.1.1 255.255.255.0
[AR2-GigabitEthernet0/0/8] quit
```

b. 配置总部的三个Tunnel接口。

```
[AR2] interface loopback 1
[AR2-loopback1] ip address 6.6.6.6 255.255.255.255
[AR2-loopback1] quit
[AR2] interface Tunnel0/0/1
[AR2-Tunnel0/0/1] tunnel-protocol gre
Warning: After this tunnel encapsulation protocol was configured, the MTU and other
parameter settings of the tunnel were deleted.
[AR2-Tunnel0/0/1] ip address 192.168.11.1 255.255.255.0
[AR2-Tunnel0/0/1] gre key plain 1
[AR2-Tunnel0/0/1] source GigabitEthernet 0/0/8
[AR2-Tunnel0/0/1] destination 1.1.1.1
[AR2-Tunnel0/0/1] mtu 1424
[AR2-Tunnel0/0/1] quit
[AR2] interface Tunnel0/0/2
[AR2-Tunnel0/0/2] tunnel-protocol gre
Warning: After this tunnel encapsulation protocol was configured, the MTU and other
parameter settings of the tunnel were deleted.
[AR2-Tunnel0/0/2] ip address 192.168.12.1 255.255.255.0
[AR2-Tunnel0/0/2] gre key plain 2
[AR2-Tunnel0/0/2] source GigabitEthernet 0/0/8
[AR2-Tunnel0/0/2] destination 3.3.3.3
[AR2-Tunnel0/0/2] mtu 1424
[AR2-Tunnel0/0/2] quit
[AR2] interface Tunnel0/0/3
[AR2-Tunnel0/0/3] tunnel-protocol gre
Warning: After this tunnel encapsulation protocol was configured, the MTU and other
parameter settings of the tunnel were deleted.
[AR2-Tunnel0/0/3] ip address 192.168.13.1 255.255.255.0
[AR2-Tunnel0/0/3] source 6.6.6.6
[AR2-Tunnel0/0/3] destination 5.5.5.5
[AR2-Tunnel0/0/3] quit
```

c. 配置分支的三个Tunnel接口。

```
[AR1] interface loopback 1
[AR1-loopback1] ip address 5.5.5.5 255.255.255.255
[AR1-loopback1] quit
[AR1] interface Tunnel0/0/1
[AR1-Tunnel0/0/1] tunnel-protocol gre
Warning: After this tunnel encapsulation protocol was configured, the MTU and other
parameter settings of the tunnel were deleted.
[AR1-Tunnel0/0/1] ip address 192.168.11.2 255.255.255.0
[AR1-Tunnel0/0/1] source Cellular 1/0/0
[AR1-Tunnel0/0/1] gre key plain 1
[AR1-Tunnel0/0/1] destination 5.5.5.1
[AR1-Tunnel0/0/1] mtu 1424
[AR1-Tunnel0/0/1] quit
[AR1] interface Tunnel0/0/2
```

 版权所有 © 华为技术有限公司

```
[AR1-Tunnel0/0/2] tunnel-protocol gre
Warning: After this tunnel encapsulation protocol was configured, the MTU and other parameter settings of the tunnel were deleted.
[AR1-Tunnel0/0/2] ip address 192.168.12.2 255.255.255.0
[AR1-Tunnel0/0/2] source Cellular 2/0/0
[AR1-Tunnel0/0/2] gre key plain 2
[AR1-Tunnel0/0/2] destination 5.5.5.1
[AR1-Tunnel0/0/2] mtu 1424
[AR1-Tunnel0/0/2] quit
[AR1] interface Tunnel0/0/3
[AR1-Tunnel0/0/3] tunnel-protocol gre
Warning: After this tunnel encapsulation protocol was configured, the MTU and other parameter settings of the tunnel were deleted.
[AR1-Tunnel0/0/3] ip address 192.168.13.2 255.255.255.0
[AR1-Tunnel0/0/3] source 5.5.5.5
[AR1-Tunnel0/0/3] destination 6.6.6.6
[AR1-Tunnel0/0/3] quit
```

3. 配置Ethernet over GRE，创建VE接口。

   a. 创建分支的二层VE接口VE0/0/1和VE0/0/2。

   ```
   [AR1] vlan 10
   [AR1-vlan10] quit
   [AR1] interface Virtual-Ethernet 0/0/1
   [AR1-Virtual-Ethernet0/0/1] portswitch
   Vlan Info: The operation may take a few seconds. Please wait for a moment...done
   [AR1-Virtual-Ethernet0/0/1] port link-type trunk
   [AR1-Virtual-Ethernet0/0/1] undo port trunk allow-pass vlan 1
   [AR1-Virtual-Ethernet0/0/1] port trunk allow-pass vlan 10
   [AR1-Virtual-Ethernet0/0/1] quit
   [AR1] interface Virtual-Ethernet 0/0/2
   [AR1-Virtual-Ethernet0/0/2] portswitch
   Vlan Info: The operation may take a few seconds. Please wait for a moment...done
   [AR1-Virtual-Ethernet0/0/2] port link-type trunk
   [AR1-Virtual-Ethernet0/0/2] undo port trunk allow-pass vlan 1
   [AR1-Virtual-Ethernet0/0/2] port trunk allow-pass vlan 10
   [AR1-Virtual-Ethernet0/0/2] quit
   ```

   b. 创建总部的二层VE接口VE0/0/1和VE0/0/2。

   ```
   [AR2] vlan 10
   [AR2-vlan10] quit
   [AR2] interface Virtual-Ethernet 0/0/1
   [AR2-Virtual-Ethernet0/0/1] portswitch
   Vlan Info: The operation may take a few seconds. Please wait for a moment...done
   [AR2-Virtual-Ethernet0/0/1] port link-type trunk
   [AR2-Virtual-Ethernet0/0/1] undo port trunk allow-pass vlan 1
   [AR2-Virtual-Ethernet0/0/1] port trunk allow-pass vlan 10
   [AR2-Virtual-Ethernet0/0/1] quit
   [AR2] interface Virtual-Ethernet 0/0/2
   [AR2-Virtual-Ethernet0/0/2] portswitch
   Vlan Info: The operation may take a few seconds. Please wait for a moment...done
   [AR2-Virtual-Ethernet0/0/2] port link-type trunk
   [AR2-Virtual-Ethernet0/0/2] undo port trunk allow-pass vlan 1
   [AR2-Virtual-Ethernet0/0/2] port trunk allow-pass vlan 10
   [AR2-Virtual-Ethernet0/0/2] quit
   ```

4. 将二层VE接口绑定到WAN侧Tunnel接口和LAN侧物理接口。

   a. 配置分支的VE0/0/1绑定到Tunnel0/0/3接口，VE0/0/2绑定到GE0/0/1接口。

   ```
   [AR1] interface Tunnel0/0/3
   [AR1-Tunnel0/0/1] map interface Virtual-Ethernet 0/0/1
   [AR1-Tunnel0/0/1] quit
   [AR1] interface GigabitEthernet 0/0/1
   [AR1-GigabitEthernet0/0/1] undo portswitch  //GE0/0/1如果不是三层物理以太网接口，则需要执行undo portswitch命令切换
   [AR1-GigabitEthernet0/0/1] map interface Virtual-Ethernet 0/0/2
   Warnning: The interface is being bound to Virtual-Ethernet.Other services are unavailable on the interface.
   [AR1-GigabitEthernet0/0/1] tcp adjust-mss 1200
   [AR1-GigabitEthernet0/0/1] quit
   ```

 版权所有 © 华为技术有限公司

b. 配置总部的VE0/0/1绑定到Tunnel0/0/3接口，VE0/0/2绑定到GE0/0/1接口。

```
[AR2] interface Tunnel0/0/3
[AR2-Tunnel0/0/1] map interface Virtual-Ethernet 0/0/1
[AR2-Tunnel0/0/1] quit
[AR2] interface GigabitEthernet 0/0/1
[AR2-GigabitEthernet0/0/1] undo portswitch
[AR2-GigabitEthernet0/0/1] map interface Virtual-Ethernet 0/0/2
Warnning: The interface is being bound to Virtual-Ethernet.Other services are unavailable on the interface.
[AR2-GigabitEthernet0/0/1] tcp adjust-mss 1200
[AR2-GigabitEthernet0/0/1] quit
```

5. 配置BFD会话，探测分支和总部之间主Ethernet over GRE隧道的连通性。

a. 配置分支的BFD会话。

```
[AR1] bfd
[AR1-bfd] quit
[AR1] bfd 1 bind peer-ip 192.168.11.1 source-ip 192.168.11.2
[AR1-bfd-session-aa] discriminator local 2
[AR1-bfd-session-aa] discriminator remote 1
[AR1-bfd-session-aa] commit
Info: The configuration succeeds, but BFD session cannot be created for the moment because the route cannot be found.
[AR1-bfd-session-aa] quit
```

b. 配置总部的BFD会话。

```
[AR2] bfd
[AR2-bfd] quit
[AR2] bfd 1 bind peer-ip 192.168.11.2 source-ip 192.168.11.1
[AR2-bfd-session-bb] discriminator local 1
[AR2-bfd-session-bb] discriminator remote 2
[AR2-bfd-session-bb] commit
Info: The configuration succeeds, but BFD session cannot be created for the moment because the route cannot be found.
[AR2-bfd-session-bb] quit
```

6. 配置静态路由，使企业分支和总部子网的用户可以互通。

a. 配置分支的静态路由，两条静态路由的出接口为5G Cellular接口，两条到总部子网的静态路由的出接口为Tunnel接口，并在主隧道接口Tunnel0/0/1所在的路由上绑定BFD会话。

```
[AR1] ip route-static 5.1.1.1 255.255.255.255 Cellular 1/0/0
[AR1] ip route-static 5.1.1.1 255.255.255.255 Cellular 2/0/0 preference 70
[AR1] ip route-static 5.5.5.5 255.255.255.255 Tunnel 0/0/1 track bfd-session 1
[AR1] ip route-static 5.5.5.5 255.255.255.255 Tunnel 0/0/2 preference 70
[AR1] quit
```

b. 配置总部的静态路由，并在主隧道接口Tunnel0/0/1所在的路由上绑定BFD会话。

```
[AR2] ip route-static 0.0.0.0 0.0.0.0 5.1.1.2
[AR2] ip route-static 6.6.6.6 255.255.255.255 Tunnel 0/0/1 track bfd-session 1
[AR2] ip route-static 6.6.6.6 255.255.255.255 Tunnel 0/0/2 preference 70
[AR2] quit
```

验证

1. 在AR1上执行命令**display ip interface brief Cellular 1/0/0**，查看Cellular1/0/0接口获取到的IP地址。

```
<AR1> display ip interface brief Cellular 1/0/0
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
(E): E-Trunk down
Interface                   IP Address/Mask      Physical   Protocol

Cellular1/0/0               1.1.1.1/32           up         up
```

 版权所有 © 华为技术有限公司

2. 在AR1上执行命令**display ip interface brief Cellular 2/0/0**，查看Cellular2/0/0接口获取到的IP地址。

```
<AR1> display ip interface brief Cellular 2/0/0
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
(E): E-Trunk down
Interface                   IP Address/Mask      Physical   Protocol

Cellular2/0/0               3.3.3.3/32           up         up
```

3. 在AR1上执行命令**display Cellular 1/0/0 all**，查看Cellular1/0/0接口的状态信息。

```
<AR1> display Cellular 1/0/0 all
Modem State:
Hardware Information.
=====================
Model = RG801
Modem Type = 5G module
Modem Firmware Version = RG801HEAAAR01A07M8G
Hardware Version = HiB5000_MODEM Ver.A
Integrate circuit card identity (ICCID) = 98681020100202000069
International Mobile Subscriber Identity (IMSI) = 460070075591996
Mobile Station International ISDN Number (MSISDN) = None
International Mobile Equipment Identity (IMEI) = 867147050004457
Factory Serial Number (FSN) = 0123456789ABCDEF
Modem Status = Online
Profile Information.
====================
Profile 1
--------
PDP Type = IPv4, Header Compression = OFF
Data Compression = OFF
Access Point Name (APN) = 5gneta
Packet Session Status = Active
* - Default profile
Network Information.
====================
Current Service Status = Service available
Service Domain = Combined
Current Service = PS
Packet Service = Attached
Packet Session Status = Active
Current Roaming Status = Roaming
Network Selection Mode = Automatic
Network Connection Mode = LTE-NR
Current Network Connection = 5G(NSA)
Mobile Country Code (MCC) = 369
Mobile Network Code (MNC) = 77
Mobile Operator Information = Unknown
Tracking Area Code (TAC) = 1002
Cell ID = 9881858
Radio Information.
==================
Current Bands :
  WCDMA: AUTO
  LTE: B3
  NR: AUTO
LTE:
Current Band = B3
Current RSSI >= -51 dBm
Current RSRP = -68 dBm (strong)
Current RSRQ >= -3 dB
Current SINR = 6 dB
NR:
Current Band = N78
Current RSRP = -64 dBm (strong)
Current RSRQ = -10 dB
```

 版权所有 © 华为技术有限公司

```
Current SINR = 35 dB
Bands supported :
  WCDMA: WCDMA850 WCDMA900 WCDMA2100
  FDD LTE: B1 B3 B5 B7 B8 B20 B28
  TDD LTE: B34 B38 B39 B40 B41
  FDD NR: N1 N3 N28
  TDD NR: N41 N77 N78 N79
  SUL NR: N80
Modem Security Information.
============================
SIM ID = 1
PIN Verification = Disabled
PIN Status = Ready
Number of Retries remaining = 3
SIM Status = OK
```

4. 在AR1上执行**display bfd session all**命令，可以看到BFD会话已经建立，且状态为Up。

```
<AR1> display bfd session all
--------------------------------------------------------------------------------
Local Remote     PeerIpAddr      State     Type        InterfaceName
--------------------------------------------------------------------------------
1     2          192.168.11.1    Up        S_IP_PEER   -
--------------------------------------------------------------------------------
    Total UP/DOWN Session Number : 1/0
```

配置文件

AR1配置文件

```
#
 sysname AR1
#
apn profile 5gprofilea
 apn 5gneta
apn profile 5gprofileb
 apn 5gnetb
#
vlan batch 10
#
interface Virtual-Ethernet0/0/1
 portswitch
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 10
#
interface Virtual-Ethernet0/0/2
 portswitch
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/1
 undo portswitch
 map interface Virtual-Ethernet0/0/2
 tcp adjust-mss 1200
#
interface Cellular1/0/0
 dialer enable-circular
 apn-profile 5gprofilea
 dialer timer autodial 10
 modem auto-recovery dial action modem-reboot fail-times 128
 modem auto-recovery icmp-unreachable action modem-reboot
 modem auto-recovery services-unavailable action modem-reboot test-times 0 interval 3600
 ip address negotiate
#
interface Cellular2/0/0
 dialer enable-circular
 apn-profile 5gprofileb
 dialer timer autodial 10
```

 版权所有 © 华为技术有限公司

```
 modem auto-recovery dial action modem-reboot fail-times 128
 modem auto-recovery icmp-unreachable action modem-reboot
 modem auto-recovery services-unavailable action modem-reboot test-times 0 interval 3600
 ip address negotiate
#
interface LoopBack1
 ip address 6.6.6.6 255.255.255.255
#
interface Tunnel0/0/1
 ip address 192.168.11.2 255.255.255.0
 tunnel-protocol gre
 gre key plain 1
 source Cellular1/0/0
 destination 5.5.5.1
 mtu 1424
#
interface Tunnel0/0/2
 ip address 192.168.12.2 255.255.255.0
 tunnel-protocol gre
 gre key plain 2
 source Cellular2/0/0
 destination 5.5.5.1
 mtu 1424
#
interface Tunnel0/0/3
 ip address 192.168.13.2 255.255.255.0
 tunnel-protocol gre
 source 6.6.6.6
 destination 5.5.5.5
 map interface Virtual-Ethernet0/0/1
#
bfd
#
bfd 1 bind peer-ip 192.168.11.1 source-ip 192.168.11.2
 discriminator local 2
 discriminator remote 1
 commit
#
ip route-static 5.1.1.1 255.255.255.255 Cellular1/0/0
ip route-static 5.1.1.1 255.255.255.255 Cellular2/0/0 preference 70
ip route-static 5.5.5.5 255.255.255.255 Tunnel0/0/1 track bfd-session 1
ip route-static 5.5.5.5 255.255.255.255 Tunnel0/0/2 preference 70
#
return
```

AR2配置文件

```
#
 sysname AR2
#
interface GigabitEthernet0/0/8
 ip address 5.1.1.1 255.255.255.0
#
interface Virtual-Ethernet0/0/1
 portswitch
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 10
#
interface Virtual-Ethernet0/0/2
 portswitch
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/1
 undo portswitch
 map interface Virtual-Ethernet0/0/2
 tcp adjust-mss 1200
#
```

 版权所有 © 华为技术有限公司

```
interface Tunnel0/0/1
 ip address 192.168.11.1 255.255.255.0
 tunnel-protocol gre
 gre key plain 1
 source GigabitEthernet0/0/8
 destination 1.1.1.1
 mtu 1424
#
interface Tunnel0/0/2
 ip address 192.168.12.1 255.255.255.0
 tunnel-protocol gre
 gre key plain 2
 source GigabitEthernet0/0/8
 destination 3.3.3.3
 mtu 1424
#
interface LoopBack1
 ip address 5.5.5.5 255.255.255.255
#
interface Tunnel0/0/3
 ip address 192.168.13.1 255.255.255.0
 tunnel-protocol gre
 source 5.5.5.5
 destination 6.6.6.6
 map interface Virtual-Ethernet0/0/1
#
bfd
#
bfd 1 bind peer-ip 192.168.11.2 source-ip 192.168.11.1
 discriminator local 1
 discriminator remote 2
 commit
#
ip route-static 0.0.0.0 0.0.0.0 32.1.1.1
ip route-static 6.6.6.6 255.255.255.255 Tunnel0/0/1 track bfd-session 1
ip route-static 6.6.6.6 255.255.255.255 Tunnel0/0/2 preference 70
#
return
```

 版权所有 © 华为技术有限公司

8 获取 IP 地址

8.1 配置设备作为DHCP Server，为用户分配IP地址的示例
8.2 配置设备作为DHCP Client，动态获取IP地址的示例
8.3 配置用户通过DHCP Relay功能从DHCP Server获取IP地址的示例
8.4 配置用户自动获取IPv6地址的示例
8.5 配置用户通过IPv6方式上网

8.1 配置设备作为 DHCP Server，为用户分配 IP 地址的示例

规格

适用于所有版本、所有形态的AR路由器。

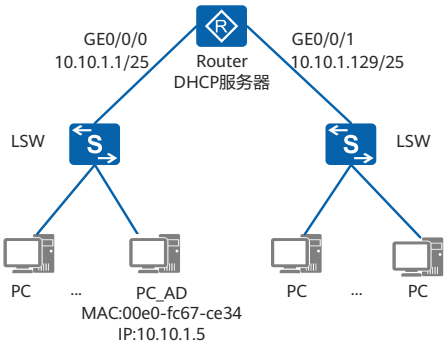
组网需求

如**图8-1**所示，某企业为办公终端规划了两个网段，网段10.10.1.0/25内PC为员工固定办公终端，网段10.10.1.128/25供企业出差人员临时接入网络。为方便管理员统一管理，希望企业终端能够自动获取IP地址和DNS服务器IP地址（当用户希望以域名方式访问时需要配置域名解析的DNS服务器）。其中，企业管理者的办公PC（PC_AD）由于业务需要，希望使用固定IP地址为10.10.1.5。

配置思路如下：Router作为DHCP服务器为网段10.10.1.0/24中的客户端动态分配IP地址，该地址池网段分为两个子网网段：10.10.1.0/25和10.10.1.128/25。Router的两个以太网接口GE0/0/0和GE0/0/1的IP地址分别为10.10.1.1/25和10.10.1.129/25。
10.10.1.0/25网段内的地址租用期限为10天12小时，域名为huawei.com，DNS服务器地址为10.10.1.2，NetBIOS服务器地址为10.10.1.4，网关地址为10.10.1.1，其中企业管理者的办公PC（PC_AD）由于业务需要，希望使用固定IP地址为10.10.1.5。
10.10.1.128/25网段内的地址租用期限为5天，域名为huawei.com，DNS服务器地址为10.10.1.2，无NetBIOS服务器地址，出口网关的地址为10.10.1.129。

版权所有 © 华为技术有限公司

图 8-1 配置 DHCP Server 功能组网图



操作步骤

步骤1 Router上的配置

```
#
 sysname Router
#
dhcp enable //使能dhcp功能
#
ip pool ip-pool1
 gateway-list 10.10.1.1 //配置网关地址
 network 10.10.1.0 mask 255.255.255.128 //配置全局地址池可动态分配的IP地址范
围
 excluded-ip-address 10.10.1.2 //配置地址池中10.10.1.2不参与自动分配
 excluded-ip-address 10.10.1.4 //配置地址池中10.10.1.4不参与自动分配
 dns-list 10.10.1.2 //配置DHCP客户端使用的DNS服务器的IP地址
 nbns-list 10.10.1.4 //配置DHCP客户端的NetBIOS服务器地址
 lease day 10 hour 12 minute 0 //配置IP地址租期为10天12小时
 domain-name huawei.com //配置域名为huawei.com
 static-bind ip-address 10.10.1.5 mac-address 00e0-fc67-ce34 //为PC_AD分配固定的IP地址
#
ip pool ip-pool2
 gateway-list 10.10.1.129 //配置网关地址
 network 10.10.1.128 mask 255.255.255.128 //配置全局地址池可动态分配的IP地址范围
 dns-list 10.10.1.2 //配置DHCP客户端使用的DNS服务器的IP地址
 lease day 5 hour 0 minute 0 //配置IP地址租期为5天
 domain-name huawei.com //配置域名为huawei.com
#
interface GigabitEthernet0/0/0
 ip address 10.10.1.1 255.255.255.128
 dhcp select global //接口工作在全局地址池模式
#
interface GigabitEthernet0/0/1
 ip address 10.10.1.129 255.255.255.128
 dhcp select global //接口工作在全局地址池模式
#
```


版权所有 © 华为技术有限公司

步骤2 验证配置结果

在Router上使用命令**display ip pool**，可以查看IP地址池配置情况。

----结束

8.2 配置设备作为 DHCP Client，动态获取 IP 地址的示例

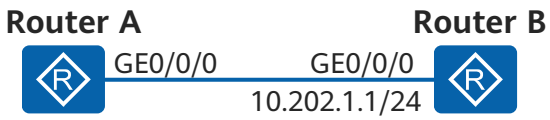
规格

适用于所有版本、所有形态的AR路由器。

组网需求

RouterA作为DHCP Client，动态获取接口的IP地址。

图 8-2 配置 DHCP Client 功能



操作步骤

步骤1 RouterA上的配置

```
#
dhcp enable //使能dhcp功能
#
interface GigabitEthernet0/0/0
 ip address dhcp-alloc
#
```

步骤2 Router B上的配置

```
#
dhcp enable //使能dhcp功能
#
ip pool ip-pool1
 gateway-list 10.202.1.1 //配置网关地址
 network 10.202.1.0 mask 255.255.255.0 //配置全局地址池可动态分配的IP地址范围
#
interface GigabitEthernet0/0/0
 ip address 10.202.1.1 255.255.255.0
 dhcp select global //配置接口工作在全局地址池模式下
#
```

步骤3 验证配置结果

在Router A上使用命令**display ip interface brief**，可以查看GE0/0/0获得IP地址的情况。

----结束

版权所有 © 华为技术有限公司

8.3 配置用户通过 DHCP Relay 功能从 DHCP Server 获取 IP 地址的示例

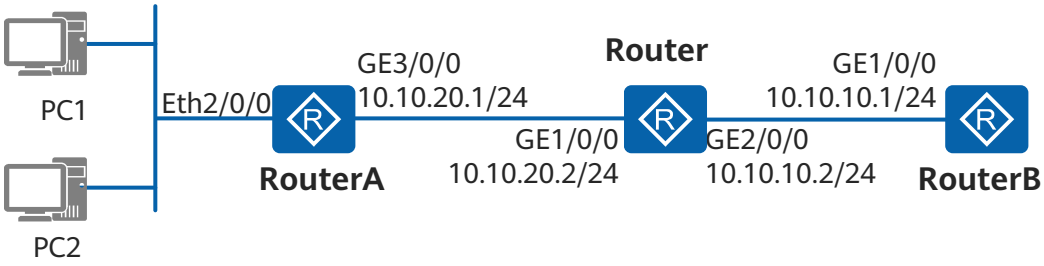
规格

适用于所有版本、所有形态的AR路由器。

组网需求

如图8-3所示，RouterA作为DHCP Relay，RouterB作为DHCP Server。需要通过具有DHCP中继功能的路由器RouterA转发DHCP报文，使PC可以从DHCP服务器上申请到IP地址等相关配置信息。

图 8-3 配置 DHCP Relay 功能



操作步骤

步骤1 配置RouterA

```
#
 vlan batch 100
#
 dhcp enable    //使能全局DHCP功能
#
dhcp server group dhcpgroup1    //创建DHCP服务器组
 dhcp-server 10.10.10.1    //在DHCP服务器组中添加DHCP服务器
#
interface Vlanif100
 ip address 10.20.20.1 255.255.255.0
 dhcp select relay    //在接口下使能DHCP中继功能
 dhcp relay server-select dhcpgroup1    //指定接口对应的DHCP服务器组
#
interface Ethernet 2/0/0
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface GigabitEthernet3/0/0
 ip address 10.10.20.1 255.255.255.0
#
 ip route-static 0.0.0.0 0.0.0.0 10.10.20.2    //配置缺省路由，下一跳为10.10.20.2
```

步骤2 配置RouterB

版权所有 © 华为技术有限公司

```
#
dhcp enable    //使能全局DHCP功能
#
ip pool pool1    //创建全局地址池
 network 10.20.20.0 mask 255.255.255.0    //配置全局地址池可动态分配的IP地址范围
 gateway-list 10.20.20.1    //配置DHCP客户端的出口网关地址
#
interface GigabitEthernet1/0/0
 ip address 10.10.10.1 255.255.255.0
 dhcp select global    //配置接口工作在全局地址池模式
#
 ip route-static 0.0.0.0 0.0.0.0 10.10.10.2    //配置缺省路由，下一跳为10.10.10.2
```

步骤3 验证配置结果

在RouterA上使用**display dhcp relay**命令用来查看接口的DHCP中继配置情况。

```
[RouterA] display dhcp relay interface vlanif 100
 **  Vlanif100 DHCP Relay Configuration  **
  DHCP server group name : dhcpgroup1
   DHCP server IP [0] :10.10.10.1
```

内网PC可以通过DHCP中继从DHCP服务器上申请到IP地址等相关配置信息。

```
[RouterB] display ip pool
  ------------------------------------------------------------------------------
  Pool-name      : pool1
  Pool-No        : 0
  Position       : Local          Status          : Unlocked
  Gateway-0      : 10.20.20.1
  Mask           : 255.255.255.0
  Vpn instance   : --


 IP address Statistic
    Total       :250
    Used        :0          Idle        :248
    Expired     :0          Conflict    :0          Disable   :2
```

----结束

配置注意事项

- PC、DHCP Relay分别与DHCP Server之间路由可达。
- DHCP Relay与DHCP Client处于同一网段。

8.4 配置用户自动获取 IPv6 地址的示例

规格

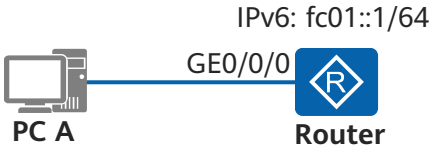
适用于V200R002C00及以上版本、所有形态的AR路由器。

适用于所有版本、所有形态的AR路由器。

组网需求

PC直连Router的接口后可通过协议自动获取IPv6地址，并自动生成默认网关，从而使PC与路由器可以自动连通。具体到该试验中，在路由器使能RA（Router Advertisement，路由器通告）后，PC能够根据接收到的RA报文自动配置地址，且能生成指向该路由器的默认路由。

图 8-4 配置路由器 IPv6 无状态地址自动配置功能



操作步骤

步骤1 Router上的配置

```
#
ipv6  //使能IPv6功能
#
interface GigabitEthernet0/0/0
 ipv6 enable
 ipv6 address fc01::1/64
 undo ipv6 nd ra halt
#
```

步骤2 验证配置结果

进入PC A的CMD命令窗口，通过**ipconfig**命令查看当前PC的地址状态，显示如下：

```
C:\> ipconfig

Windows IP Configuration


Ethernet adapter 本地连接:

      Connection-specific DNS Suffix  . :
      IP Address. . . . . . . . . . . . : 0.0.0.0
      Subnet Mask . . . . . . . . . . . : 0.0.0.0
      IP Address. . . . . . . . . . . . : fc01::bdc5:2448:dc6b:bbe0   – ①
      IP Address. . . . . . . . . . . . : fc01::215:e9ff:feac:2df2    – ②
      IP Address. . . . . . . . . . . . : fe80::215:e9ff:feac:2df2%5  – ③
      Default Gateway . . . . . . . . . : fe80::a19:a6ff:fecd:a896%5  – ④
```

说明

① IPv6自动配置的本地IP地址，前缀与GE0/0/0接口的IPv6地址相同；

② 用本地Mac地址生成的EUI-64地址；

③ 链路本地地址；

④ 自动生成的默认网关，此处为直连路由器接口的链路层地址。

通过CMD命令窗口，ping Router的GE0/0/0接口，可以ping通。

```
C:\> ping fc01::1

Pinging fc01::1 with 32 bytes of data:

Reply from fc01::1: time<1ms
Reply from fc01::1: time<1ms
Reply from fc01::1: time<1ms
Reply from fc01::1: time<1ms

Ping statistics for fc01::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```


版权所有 © 华为技术有限公司

从以上信息可以看出路由自动通告成功，地址自动配置完成。

----结束

8.5 配置用户通过 IPv6 方式上网

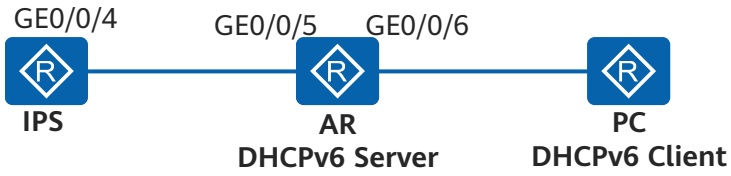
规格

适用于所有版本、所有形态的AR路由器。

组网需求

运营商为企业分配了WAN侧的IPv6地址1111:2222:A0EE:6::2/64和LAN侧的IPv6地址1111:3333:E840:2::1/64，企业通过运营商提供的IPv6地址配置上网。

图 8-5 配置用户通过 IPv6 方式上网



操作步骤

步骤1 IPS上的配置

```
#
interface GigabitEthernet0/0/4
 ipv6 enable
 ipv6 address 1111:2222:A0EE:6::1/64
#
ipv6 route-static :: 0 1111:2222:A0EE:6::2   //配置运营商网关到AR设备的路由
#
```

步骤2 AR上的配置

```
#
interface GigabitEthernet0/0/5   //GE0/0/5为连接运营商网关设备的WAN口
 undo portswitch
 description IPS
 ipv6 enable
 ipv6 address 1111:2222:A0EE:6::2/64
#
interface GigabitEthernet0/0/6   //GE0/0/6为连接内网设备并为外网设备分配地址的LAN口
 undo portswitch
 description LAN
 ipv6 enable
 ipv6 address 1111:3333:E840:2::1/64
 ipv6 nd ra prefix default no-advertise
 undo ipv6 nd ra halt
 ipv6 nd autoconfig managed-address-flag
 ipv6 nd autoconfig other-flag
 dhcpv6 server pool1
#
ipv6 route-static :: 0 1111:2222:A0EE:6::1
#
```


版权所有 © 华为技术有限公司

步骤3 PC上的配置

```
#
interface GigabitEthernet0/0/6
 undo portswitch
 ipv6 enable
 ipv6 address auto link-local
 ipv6 address auto global default
 ipv6 address auto dhcp
#
```

步骤4 验证配置结果

1. 在PC上查看DHCPv6客户端信息、AR和IPS网关地址是否可达。

   # 在PC上执行命令**display dhcpv6 client**查看DHCPv6客户端的信息。

   # 在PC上执行命令**ping ipv6 1111:3333:E840:2::1**查看LAN侧网关地址是否可达。

   # 在PC上执行命令**ping ipv6 1111:2222:A0EE:6::2**查看WAN侧网关地址是否可达。

   # 在PC上执行命令**ping ipv6 1111:2222:A0EE:6::1**查看IPS网关地址是否可达。
2. 在AR上查看DHCPv6服务器端信息。

   # 在AR上执行命令**display dhcpv6 server**查看DHCPv6服务器端的信息。

   # 在AR上执行命令**display dhcpv6 pool**查看IPv6地址池信息。
3. 在AR上查看PC被分配的网关地址是否可达。

   # 在PC上执行命令**display dhcpv6 pool**查看PC被分配的IPv6地址。

   # 在AR上执行命令**ping ipv6 1111:3333:E840:2::2**查看PC被分配的网关地址是否可达。

----结束

 版权所有 © 华为技术有限公司

9 部署路由

9.1 静态路由协议
9.2 RIP路由协议
9.3 RIPng路由协议
9.4 OSPF路由协议
9.5 OSPFv3路由协议
9.6 IS-IS（IPv4）路由协议
9.7 IS-IS（IPv6）路由协议
9.8 BGP路由协议
9.9 策略路由
9.10 路由策略

9.1 静态路由协议

9.1.1 配置 IPv4 静态路由基本功能示例

规格

适用于所有版本、所有形态的AR路由器。

组网需求

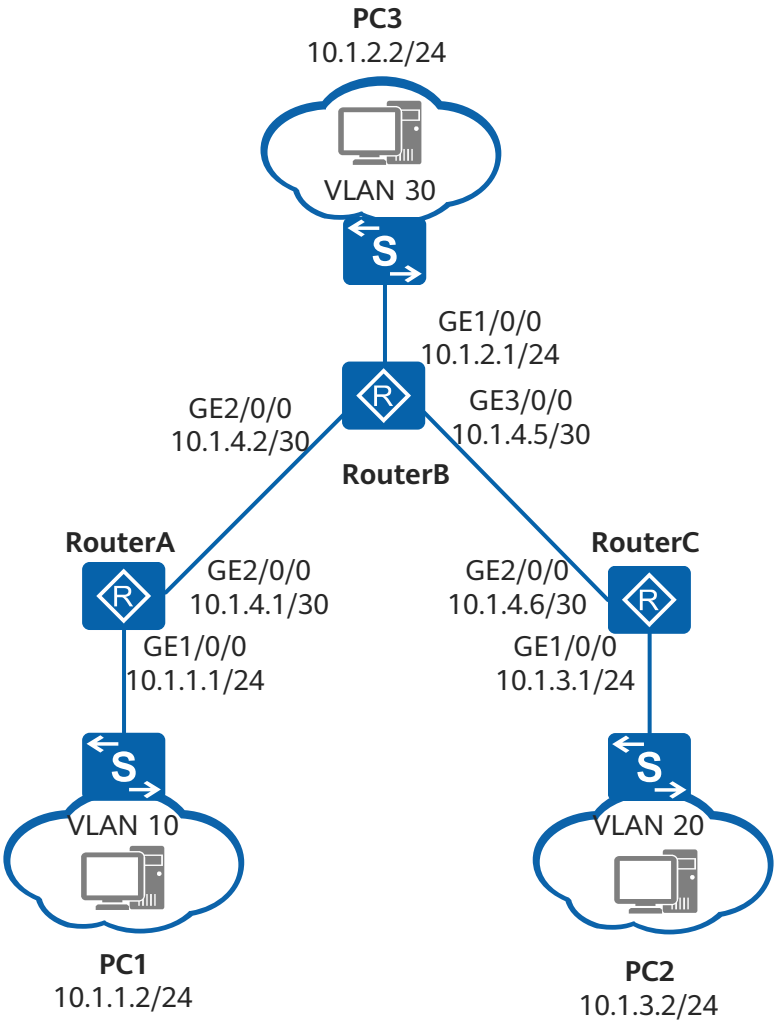
如**图1**所示，某企业网内用户因业务需要划分了不同网段，不同网段用户想能够实现互访。由于企业网规模不大，且要求网络简单，安全，可靠以及转发效率高，所以采用配置静态路由实现组网中任意两台主机之间都能互通。

在配置IPv4静态路由之前，需完成以下任务：

配置接口的链路层协议参数和IP地址，使相邻节点网络层可达。

 版权所有 © 华为技术有限公司

图 9-1 配置静态路由组网图



操作步骤

步骤1 RouterA的配置

```
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 10.1.4.1 255.255.255.252
#
ip route-static 10.1.2.0 255.255.255.0 10.1.4.2
ip route-static 10.1.3.0 255.255.255.0 10.1.4.2  //配置RouterA到不同网段的静态路由
#
return
```

步骤2 RouterB的配置

```
#
interface GigabitEthernet1/0/0
 ip address 10.1.2.1 255.255.255.0
#
interface GigabitEthernet2/0/0
```


版权所有 © 华为技术有限公司

```
 ip address 10.1.4.2 255.255.255.252
#
interface GigabitEthernet3/0/0
 ip address 10.1.4.5 255.255.255.252
#
ip route-static 10.1.1.0 255.255.255.0 10.1.4.1
ip route-static 10.1.3.0 255.255.255.0 10.1.4.6  //配置RouterB到不同网段的静态路由
#
return
```

步骤3 RouterC的配置

```
#
interface GigabitEthernet1/0/0
 ip address 10.1.3.1 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 10.1.4.6 255.255.255.252
#
ip route-static 10.1.1.0 255.255.255.0 10.1.4.5
ip route-static 10.1.2.0 255.255.255.0 10.1.4.5  //配置RouterC到不同网段的静态路由
#
return
```

步骤4 配置主机

配置VLAN10内主机的缺省网关为10.1.1.1，VLAN20内主机的缺省网关为10.1.3.1，VLAN30内主机的缺省网关为10.1.2.1。

步骤5 配置交换机

配置各交换机，使得各主机能与其网关路由器互通。

步骤6 验证配置结果

使用**display ip routing-table**命令查看路由器的IP路由表。

使用**Ping**命令验证连通性。

----结束

配置注意事项

- 正确配置各路由器各接口的IPv4地址，使网络互通。
- 保证两个路由器互连接口地址配置在同一网段，并且可以正常互通。
- 在各主机上配置IPv4缺省网关。

9.1.2 配置 NQA for IPv4 静态路由示例

规格

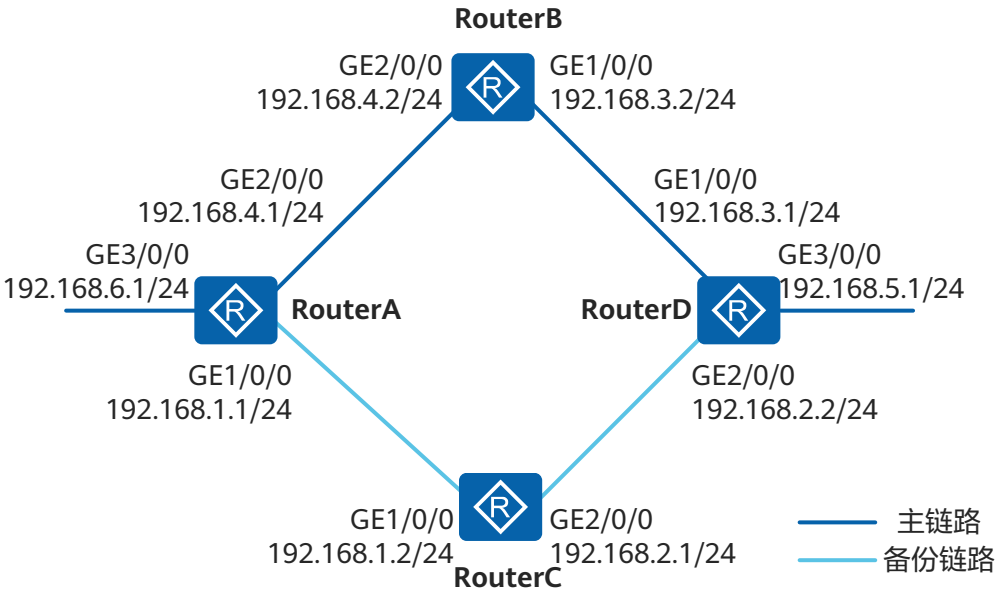
适用于所有版本、所有形态的AR路由器。

组网需求

通过配置NQA for IPv4静态路由可以快速检测到网络的故障，控制静态路由的发布。如图9-2所示，RouterA通过接口GE2/0/0连接RouterB到RouterD作为主链路，RouterA通过接口GE1/0/0连接RouterC到RouterD作为备份链路。在RouterA上配置NQA ICMP测试例，以检测主链路的网络状况。当主链路出现故障时，从RouterA发送到RouterD的报文就会切换到备份链路进行转发。

 版权所有 © 华为技术有限公司

图 9-2 配置 NQA for IPv4 静态路由组网图



操作步骤

步骤1 RouterA的配置

```
#
 sysname RouterA
#
interface GigabitEthernet1/0/0
 ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 192.168.4.1 255.255.255.0
#
interface GigabitEthernet3/0/0
 ip address 192.168.6.1 255.255.255.0
#
ip route-static 192.168.2.0 255.255.255.0 192.168.1.2
ip route-static 192.168.3.0 255.255.255.0 192.168.4.2
ip route-static 192.168.5.0 255.255.255.0 192.168.1.2 preference 100  //配置静态路由优先级为100，用来做备用路由
ip route-static 192.168.5.0 255.255.255.0 GigabitEthernet2/0/0 192.168.4.2 track nqa admin icmp  //配置与NQA测试例联动的静态路由
#
nqa test-instance admin icmp  //配置名为admin icmp的NQA测试例
 test-type icmp  //配置测试例类型为ICMP
 destination-address ipv4 192.168.3.1  //配置NQA测试例的目的地址为192.168.3.1
 frequency 10  //配置NQA测试例两次测试之间间隔10秒
 probe-count 2  //配置NQA测试例的测试探针数目为2
 start now  //立即开始执行当前的NQA测试例
#
```

步骤2 RouterB的配置

```
#
 sysname RouterB
#
interface GigabitEthernet1/0/0
 ip address 192.168.3.2 255.255.255.0
#
interface GigabitEthernet2/0/0
```


版权所有 © 华为技术有限公司

```
 ip address 192.168.4.2 255.255.255.0
#
ip route-static 192.168.5.0 255.255.255.0 192.168.3.1
ip route-static 192.168.6.0 255.255.255.0 192.168.4.1
#
```

步骤3 RouterC的配置

```
#
 sysname RouterC
#
interface GigabitEthernet1/0/0
 ip address 192.168.1.2 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 192.168.2.1 255.255.255.0
#
ip route-static 192.168.5.0 255.255.255.0 192.168.2.2
ip route-static 192.168.6.0 255.255.255.0 192.168.1.1
#
```

步骤4 RouterD的配置

```
#
 sysname RouterD
#
interface GigabitEthernet1/0/0
 ip address 192.168.3.1 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 192.168.2.2 255.255.255.0
#
interface GigabitEthernet3/0/0
 ip address 192.168.5.1 255.255.255.0
#
ip route-static 192.168.1.0 255.255.255.0 192.168.2.1
ip route-static 192.168.4.0 255.255.255.0 192.168.3.2
ip route-static 192.168.6.0 255.255.255.0 192.168.3.2
ip route-static 192.168.6.0 255.255.255.0 192.168.2.1
#
```

步骤5 验证配置结果

在RouterA上执行命令**display nqa results test-instance admin icmp**查看NQA测试结果，其中可以看到“Lost packet ratio: 0 %”，这说明链路状态完好。然后执行命令**display ip routing-table**查看路由表，可以看到到目的网段192.168.5.0/24，下一条为192.168.4.2的静态路由存在于路由表中，而配置的优先级为100的静态路由不存在与路由表中。

在RouterB的两个接口的任一接口视图下执行命令**shutdown**，来模拟链路出现故障。然后在RouterA上执行命令**display nqa results test-instance admin icmp**，查看NQA测试结果，其中可以看到“Completion:failed”和“Lost packet ratio: 100 %”，这说明检测到链路出现故障。接着执行命令**display ip routing-table**查看路由表，可以看到之前到目的网段192.168.5.0/24，下一条为192.168.4.2的静态路由被优先级为100的静态路由在路由表中所取代。

----结束

配置注意事项

- NQA测试例使用**display nqa results**命令查看测试结果，只有当测试完成状态为测试失败时，与NQA联动的静态路由才会在路由表中被删除。
- 修改NQA测试例的配置时，要先停止当前运行的NQA测试例。
- 配置同一条静态路由与其它NQA测试例联动时，会解除与当前NQA测试例的联动关系。

 版权所有 © 华为技术有限公司

- 此案例中的NQA仅做PING检测，对对端设备没有配置要求。目的是让RouterA通过检测结果来切换链路，从而增强RouterA对报文转发的可靠性。

9.1.3 配置 IPv6 静态路由基本功能示例

规格

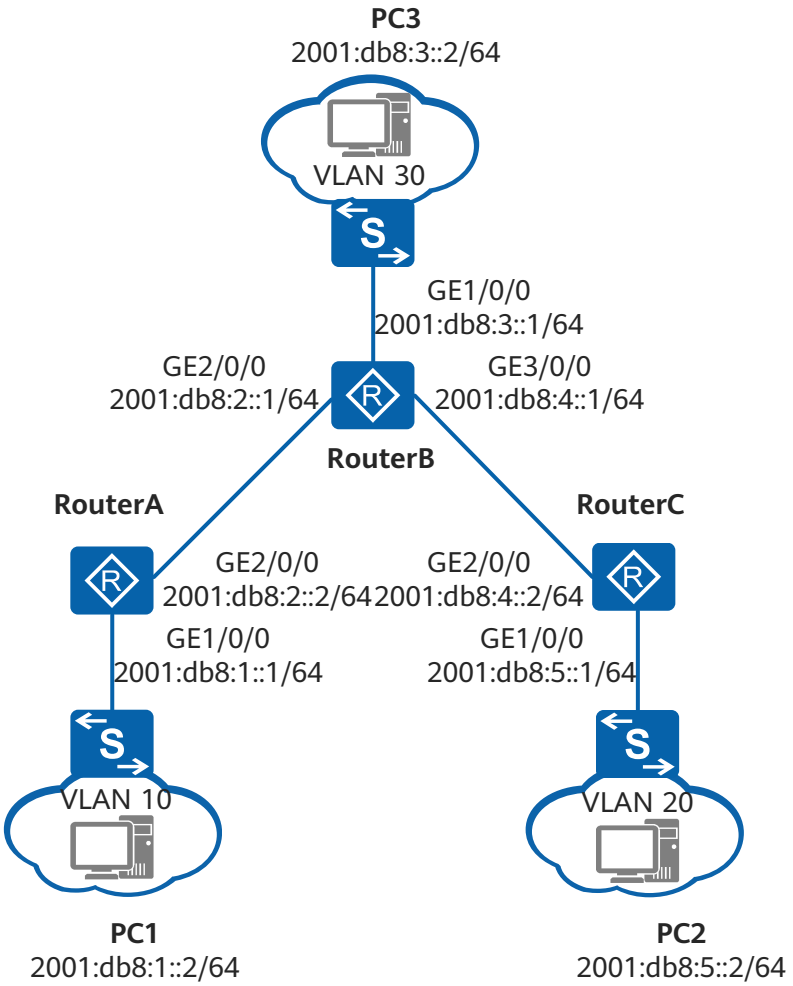
适用于ARV200R002C00及更高版本、所有形态的AR路由器。

适用于所有版本、所有形态的AR路由器。

组网需求

路由器各接口及主机的IPv6地址和掩码如图9-3所示。要求采用静态路由，使图中任意两台主机之间都能互通。

图 9-3 配置 IPv6 静态路由组网图



 版权所有 © 华为技术有限公司

操作步骤

步骤1 RouterA的配置

```
#
ipv6  //使能路由器IPv6报文转发能力
#
interface GigabitEthernet1/0/0
 ipv6 enable  //在接口上使能IPv6功能
 ipv6 address 2001:db8:1::1 64
#
interface GigabitEthernet2/0/0
 ipv6 enable
 ipv6 address 2001:db8:2::2 64
#
ipv6 route-static 3:: 64 2001:db8:2::1
ipv6 route-static 4:: 64 2001:db8:2::1
ipv6 route-static 5:: 64 2001:db8:2::1  //配置RouterA到不同网段的静态路由
#
return
```

步骤2 RouterB的配置

```
#
ipv6
#
interface GigabitEthernet1/0/0
 ipv6 enable
 ipv6 address 2001:db8:3::1 64
#
interface GigabitEthernet2/0/0
 ipv6 enable
 ipv6 address 2001:db8:2::1 64
#
interface GigabitEthernet3/0/0
 ipv6 enable
 ipv6 address 2001:db8:4::1 64
#
ipv6 route-static 1:: 64 2001:db8:2::2
ipv6 route-static 5:: 64 2001:db8:4::2
#
return
```

步骤3 RouterC的配置

```
#
ipv6
#
interface GigabitEthernet1/0/0
 ipv6 enable
 ipv6 address 2001:db8:5::1 64
#
interface GigabitEthernet2/0/0
 ipv6 enable
 ipv6 address 2001:db8:4::2 64
#
ipv6 route-static 1:: 64 2001:db8:4::1
ipv6 route-static 2:: 64 2001:db8:4::1
ipv6 route-static 3:: 64 2001:db8:4::1
#
return
```

步骤4 配置主机

配置VLAN10内主机的缺省网关为2001:db8:1::1，VLAN20内主机的缺省网关为2001:db8:5::1，VLAN30内主机的缺省网关为2001:db8:3::1。

步骤5 配置交换机

配置各交换机，使得各主机能与其网关路由器互通。

 版权所有 © 华为技术有限公司

步骤6 验证配置结果

使用**display ipv6 routing-table**命令查看路由器的IP路由表。

使用**Ping ipv6**命令验证连通性。

----结束

配置注意事项

- 配置IPv6路由协议前，一定要先使能路由设备转发IPv6单播报文。在接口下配置关于IPv6特性的命令前必须先在接口上使能IPv6功能。
- 正确配置各路由器各接口的IPv6地址，使网络互通。
- 在各主机上配置缺省网关。

9.1.4 配置 IPv4 静态路由与 BFD 联动配置

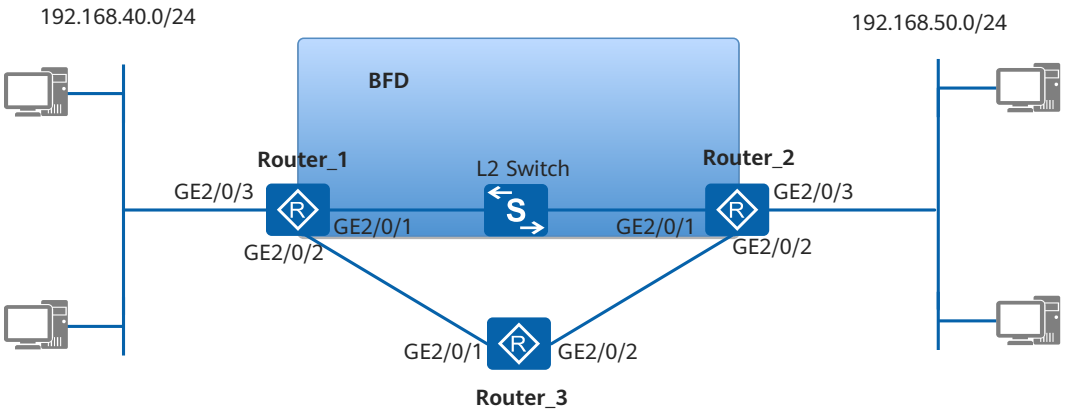
规格

适用于所有版本、所有形态的AR路由器。

组网需求

某公司内部网络如图9-4所示，从Router_1到Router_2有两条转发路径，下一跳分别为Router_2和Router_3。由于Router_1和Router_2之间物理距离较远，通过一个二层交换机L2 Switch作为中继。假设Router_2不支持BFD，要求在Router_1上使用静态路由与BFD联动技术，实现当Router_2与二层交换机L2 Switch之间的链路出现故障（如链路down）时，Router_1能快速感知，并将流量切换到Router_3的链路上。

图 9-4 IPv4 静态路由与 BFD 联动配置组网图



设备	接口	IP地址
Router_1	GE2/0/1	10.10.10.101/24
	GE2/0/2	10.10.20.101/24
	GE2/0/3	10.10.40.101/24

 版权所有 © 华为技术有限公司

设备	接口	IP地址
Router_2	GE2/0/1	10.10.10.102/24
	GE2/0/2	10.10.30.101/24
	GE2/0/3	10.10.50.101/24
Router_3	GE2/0/1	10.10.20.102/24
	GE2/0/2	10.10.30.102/24

操作步骤

步骤1 Router_1的配置文件

```
#
 sysname Router_1
#
bfd
#
interface GigabitEthernet2/0/1     //配置Router_1 GigabitEthernet2/0/1的IP地址
 ip address 10.10.10.101 255.255.255.0
#
interface GigabitEthernet2/0/2
 ip address 10.10.20.101 255.255.255.0
#
interface GigabitEthernet2/0/3
 ip address 10.10.40.101 255.255.255.0
#
bfd aa bind peer-ip 10.10.10.102 interface GigabitEthernet2/0/1 one-arm-echo    //在Router_1上配置与Router_2之间的BFD会话
 discriminator local 1
 min-echo-rx-interval 100
 commit
#
 ip route-static 10.10.50.0 24 GigabitEthernet2/0/1 10.10.10.102 track bfd-session aa    //配置Router_1到10.10.50.0/24网段的静态路由，Router_1到Router_2的流量优先走Router_1 –> L2 Switch–> Router_2链路，当此链路发生故障时，流量切换到Router_1 –> Router_3–> Router_2链路上
 ip route-static 10.10.50.0 24 GigabitEthernet2/0/2 10.10.20.102 preference 65
#
return
```

步骤2 Router_2的配置文件

```
#
 sysname Router_2
#
interface GigabitEthernet2/0/1    //配置Router_2 GigabitEthernet2/0/1的IP地址
 ip address 10.10.10.102 255.255.255.0
#
interface GigabitEthernet2/0/2
 ip address 10.10.30.101 255.255.255.0
#
interface GigabitEthernet2/0/3
 ip address 10.10.50.101 255.255.255.0
#
ip route-static 10.10.40.0 24 GigabitEthernet2/0/1 10.10.10.101   //配置Router_2到10.10.40.0/24网段的静态路由，Router_2到Router_1的流量优先走Router_2 –> L2 Switch–> Router_1链路，当此链路发生故障时，流量切换到Router_2 –> Router_3–> Router_1链路上。
ip route-static 10.10.40.0 24 GigabitEthernet2/0/2 10.10.30.102 preference 65
#
return
```

步骤3 Router_3的配置文件

 版权所有 © 华为技术有限公司

```
#
 sysname Router_3
#
interface GigabitEthernet2/0/1    //配置Router_3 GigabitEthernet2/0/1的IP地址
 ip address 10.10.20.102 255.255.255.0
#
interface GigabitEthernet2/0/2
 ip address 10.10.30.102 255.255.255.0
#
ip route-static 10.10.40.0 24 GigabitEthernet2/0/1 10.10.20.101    //配置Router_3到10.10.40.0/24和10.10.50.0/24网段的静态路由
ip route-static 10.10.50.0 24 GigabitEthernet2/0/2 10.10.30.101
#
return
```

步骤4 验证配置结果

Router_1和Router_2设备及之间的链路均正常工作时：

- 在Router_1执行命令**display ip routing-table protocol static**查看静态路由信息，可以看到Router_1和Router_2之间路由可达。
- 在Router_1执行命令**display bfd session all**查看BFD会话已经创建。

Router_2与L2 Switch之间的链路出现故障时，在Router_1执行命令**display ip routing-table protocol static**查看静态路由信息，可以看到Router_1和Router_3之间路由可达。

----结束

9.1.5 配置路由器通过 IPv4 静态路由与三层交换机对接示例

规格

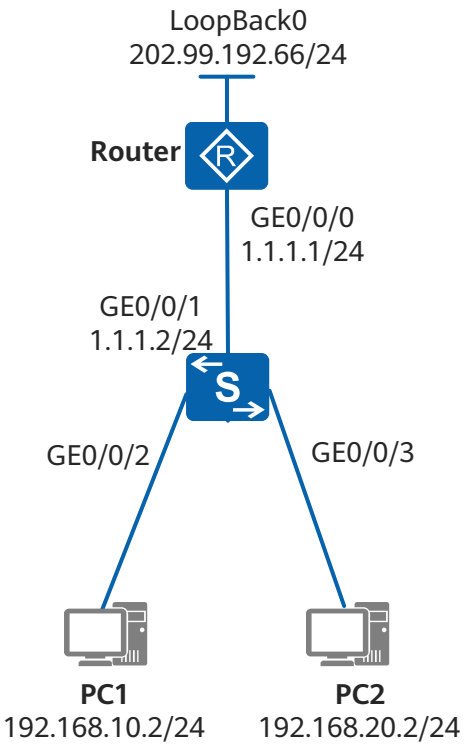
适用于所有版本、所有形态的AR路由器。

组网需求

路由器各接口及主机的IP地址和掩码如图9-5所示。配置Loopback接口模拟外网，要求采用静态路由，使图中任意两台主机都连接到外网。

 版权所有 © 华为技术有限公司

图 9-5 配置静态路由组网图



操作步骤

步骤1 物理交换机的配置

```
#
vlan batch 10 20 100
#
interface vlanif 10
 ip address 192.168.10.1 255.255.255.0
#
interface vlanif 20
 ip address 192.168.20.1 255.255.255.0
#
interface vlanif 100
 ip address 1.1.1.2 255.255.255.0
#
interface gigabitEthernet0/0/1
 port link-type access
 port default vlan 100  //配置GigabitEthernet0/0/1接口以access方式加入vlan100,该接口和路由器进行对接
#
interface gigabitEthernet0/0/2
 port link-type access
 port default vlan 10
```

 版权所有 © 华为技术有限公司

```
#
interface gigabitEthernet0/0/3
 port link-type access
 port default vlan 20
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.1  //配置默认静态路由
#
  return
```

步骤2 Router的配置

```
#
interface gigabitEthernet0/0/0
  ip address 1.1.1.1 255.255.255.0  //配置GigabitEthernet0/0/0接口的IP地址,该接口和交换机进行对接
#
interface loopback 0
 ip address 202.99.192.66 255.255.255.0  //配置本地回环接口地址,以做测试用
#
ip route-static 192.168.0.0 255.255.0.0 1.1.1.2  //配置Router的静态路由,使数据可以到达交换
机
#
return
```

步骤3 配置主机

执行route add 1.1.1.0 mask 24 192.168.10.1配置PC1主机的IP地址，执行route add 1.1.1.0 mask 24 192.168.20.1配置PC2主机的IP地址。

步骤4 验证配置结果

使用**display ip routing-table**命令查看路由器的IP路由表。

使用**Ping**命令验证连通性。

----结束

配置注意事项

- 正确配置各路由器各接口的IPv4地址，使网络互通。
- 在各主机上配置IPv4缺省网关。

9.1.6 配置 IPv4 静态路由双出口固定地址的案例

规格

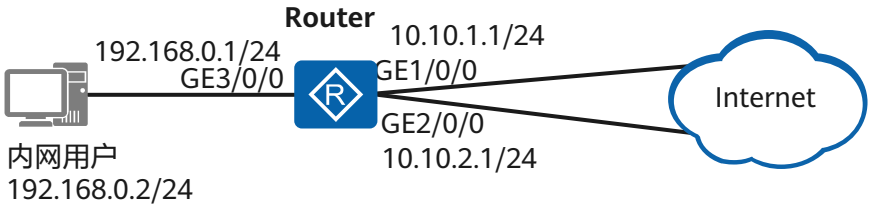
适用于所有版本、所有形态的AR路由器。

组网需求

为了保证企业网网络稳定和可靠性，可以通过配置路由双出口固定地址，一旦某一条路由丢失，用户也能通过其他备份路由继续上网。用户可以通过静态路由的优先级区分主备链路，以此保证数据能正常切换，用户顺利上网。

 版权所有 © 华为技术有限公司

图 9-6 配置 IPv4 静态路由双出口固定地址组网图



操作步骤

步骤1 Router的配置

```
#
 sysname Router  //修改设备名称
#
acl number 2000
 rule 5 permit
#
acl number 2001
 rule 5 permit
#
interface gigabitethernet 1/0/0
 ip address 10.10.1.1 24 //配置外网口1
 nat outbound 2000
#
interface gigabitethernet 2/0/0
 ip address 10.10.2.1 24 //配置外网口2
 nat outbound 2001
#
interface gigabitethernet 3/0/0
 ip address 192.168.0.1 24 //配置内网网口3
#
ip route-static 0.0.0.0 0.0.0.0 10.10.1.2
ip route-static 0.0.0.0 0.0.0.0 10.10.2.2
#
```

步骤2 配置主机

配置主机PC1的缺省网关为192.168.0.1。

步骤3 验证配置结果

使用**display ip routing-table**命令查看路由器的IP路由表。

使用**Ping**命令验证连通性。

----结束

配置注意事项

- 配置ACL，确定对哪些网段进行NAT转换。
- 在出接口视图下配置NAT转换，注意转换方向。

9.2 RIP 路由协议

版权所有 © 华为技术有限公司

9.2.1 配置 RIP 路由协议基本功能示例

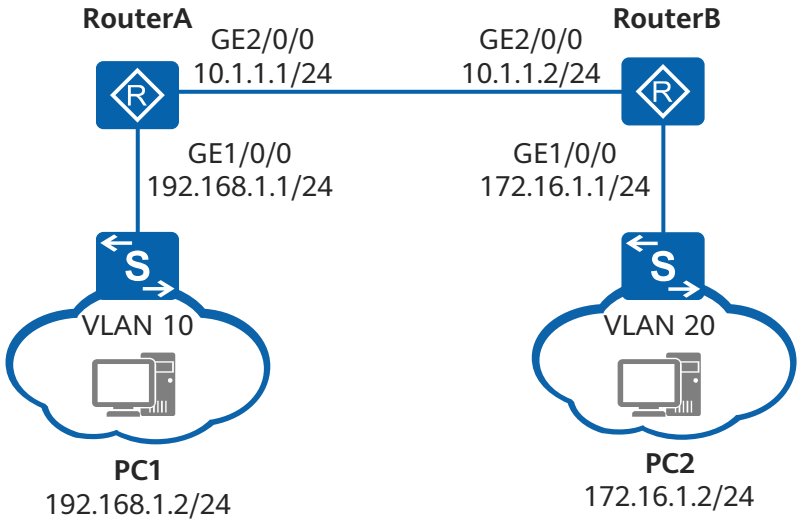
规格

适用于所有版本、所有形态的AR路由器。

组网需求

路由器各接口及主机的IP地址和掩码如图9-7所示。要求采用RIP路由协议，使图中两台主机之间互通。

图 9-7 配置 RIP 路由组网图



操作步骤

步骤1 RouterA的配置

```
#
interface GigabitEthernet1/0/0
 ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 10.1.1.1 255.255.255.0
#
rip 1
 version 2 //指定全局RIP版本
 network 192.168.1.0 //在指定网段使能RIP
 network 10.0.0.0
#
return
```

步骤2 RouterB的配置

```
#
interface GigabitEthernet1/0/0
 ip address 172.16.1.1 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 10.1.1.2 255.255.255.0
#
```


版权所有 © 华为技术有限公司

```
rip 1
 version 2
 network 172.16.0.0
 network 10.0.0.0
#
return
```

步骤3 配置主机

配置VLAN10内主机的缺省网关为192.168.1.1，VLAN20内主机的缺省网关为172.16.1.1。

步骤4 配置交换机

配置各交换机，使得各主机能与其网关路由器互通。

步骤5 验证配置结果

使用**display rip** *process-id* **route**命令查看路由器的IP路由表。从路由表中可以看出，RIP-2发布的路由中带有更为精确的子网掩码信息。

使用**Ping**命令验证连通性。

----结束

配置注意事项

- 正确配置各路由器各接口的IPv4地址，使网络互通。
- 保证两个路由器互连接口地址配置在同一网段，并且可以正常互通。
- 在各主机上配置IPv4缺省网关。
- 使用**network**命令使能RIP的网络地址时，必须是自然网段的地址。

9.2.2 配置 RIP 路由协议与 BFD 联动示例

规格

适用于所有版本、所有形态的AR路由器。

组网需求

如图9-8所示，某公司通过一台二层交换机作为中继将两个相距较远的部门连接。Router_1、Router_2、Router_3上运行RIP，建立RIP邻居关系，保证网络层相互可达。

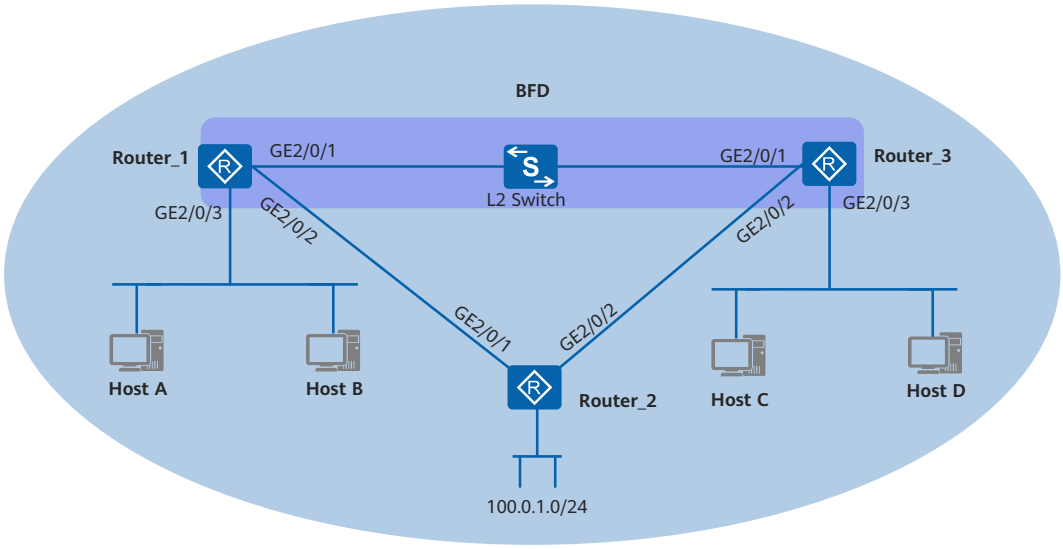
已知Router_3不支持BFD功能。公司希望在Router_1上使用RIP与BFD联动技术，采用BFD echo报文方式实现当Router_1或Router_3与二层交换机之间的链路出现故障时，BFD能够快速感知并通告RIP协议。

现要求通过在Router_1和Router_3上配置RIP与BFD联动功能，实现：

- 监测通过L2 Switch通信的链路。
- 当链路出现故障时设备能够快速感知并通告RIP协议，快速切换到Router_2链路进行通信。

 版权所有 © 华为技术有限公司

图 9-8 RIP 与 BFD 联动配置组网图



设备	接口	IP地址
Router_1	GE2/0/1	10.1.0.101/24
	GE2/0/2	10.10.0.101/24
	GE2/0/3	10.20.1.1/24
Router_2	GE2/0/1	10.10.0.102/24
	GE2/0/2	10.40.1.101/24
Router_3	GE2/0/1	10.1.0.102/24
	GE2/0/2	10.40.1.102/24
	GE2/0/3	10.30.1.1/24

操作步骤

步骤1 Router_1的配置文件

```
#
 sysname Router_1
#
bfd
#
interface GigabitEthernet2/0/1
 ip address 10.1.0.101 255.255.255.0
 rip bfd static
#
interface GigabitEthernet2/0/2
 ip address 10.10.0.101 255.255.255.0
#
interface GigabitEthernet2/0/3
 ip address 10.20.1.1 255.255.255.0
#
rip 1    //配置Router_1的RIP基本功能
```


版权所有 © 华为技术有限公司

```
 version 2
 network 10.0.0.0
#
bfd 1 bind peer-ip 10.10.0.102 interface GigabitEthernet2/0/1 one-arm-echo    //配置Router_1的单臂BFD特性
 discriminator local 1
 min-echo-rx-interval 200
commit
#
return
```

步骤2 Router_2的配置文件

```
#
 sysname Router_2
#
interface GigabitEthernet2/0/1
 ip address 10.10.0.102 255.255.255.0
#
interface GigabitEthernet2/0/2
 ip address 10.40.1.101 255.255.255.0
#
rip 1    //配置Router_2的RIP基本功能
 version 2
 network 10.0.0.0

#
return
```

步骤3 Router_3的配置文件

```
#
 sysname Router_3
#
interface GigabitEthernet2/0/1
 ip address 10.1.0.102 255.255.255.0
#
interface GigabitEthernet2/0/2
 ip address 10.40.1.102 255.255.255.0
#
interface GigabitEthernet2/0/3
 ip address 10.30.1.1 255.255.255.0
#
rip 1    //配置Router_3的RIP基本功能
 version 2
 network 10.0.0.0

#
return
```

步骤4 验证配置结果

在Router_1上执行命令**display rip 1 bfd session all**查看BFD会话信息，显示BFD会话已被创建，且状态为Up。

在Router_1上执行命令**display ip routing-table**查看学到的路由10.30.1.0/24，可以看到Router_1经过L2 Switch到达Router_3。

----结束

9.3 RIPng 路由协议

 版权所有 © 华为技术有限公司

9.3.1 配置 RIPng 路由协议基本功能示例

规格

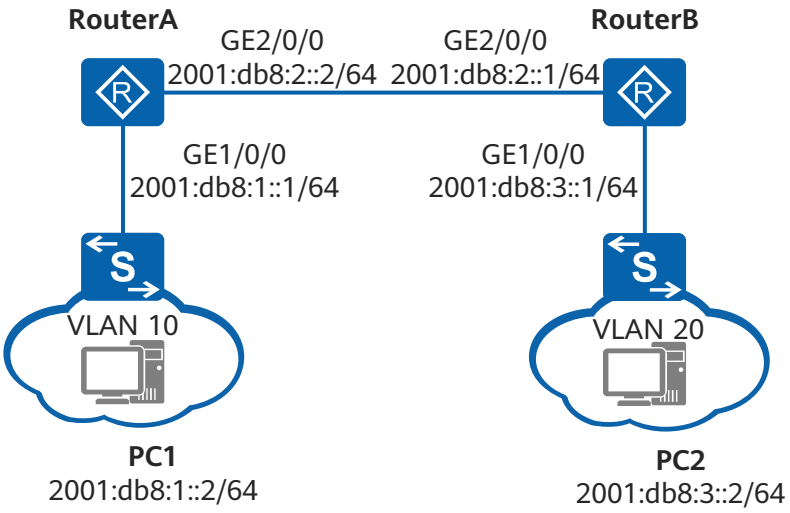
适用于ARV200R002C00及更高版本、所有形态的AR路由器。

适用于所有版本、所有形态的AR路由器。

组网需求

路由器各接口及主机的IPv6地址和掩码如图9-9所示。要求采用RIPng路由协议，使图中两台主机之间都能互通。

图 9-9 配置 RIPng 路由协议基本功能组网图



操作步骤

步骤1 RouterA的配置

```
#
ipv6  //使能路由器IPv6报文转发能力
#
interface GigabitEthernet1/0/0
 ipv6 enable  //在接口上使能IPv6功能
 ipv6 address 2001:db8:1::1 64
 ripng 1 enable  //在指定接口上使能RIPng
#
interface GigabitEthernet2/0/0
 ipv6 enable
 ipv6 address 2001:db8:2::2 64
 ripng 1 enable
#
ripng 1  //使能RIPng路由进程
#
return
```

步骤2 RouterB的配置

```
#
ipv6
```


版权所有 © 华为技术有限公司

```
#
interface GigabitEthernet1/0/0
 ipv6 enable
 ipv6 address 2001:db8:3::1 64
 ripng 1 enable
#
interface GigabitEthernet2/0/0
 ipv6 enable
 ipv6 address 2001:db8:2::1 64
 ripng 1 enable
#
ripng 1
#
return
```

步骤3 配置主机

配置VLAN10内主机的缺省网关为2001:db8:1::1，VLAN20内主机的缺省网关为2001:db8:3::1。

步骤4 配置交换机

配置各交换机，使得各主机能与其网关路由器互通。

步骤5 验证配置结果

使用**display ripng** *process-id* **route**命令查看路由器的IP路由表。从路由表中可以看出发布的路由信息。

使用**ping ipv6**命令验证连通性。

----结束

配置注意事项

- 配置IPv6路由协议前，一定要先使能路由设备转发IPv6单播报文。在接口下配置关于IPv6特性的命令前必须先在接口上使能IPv6功能。
- 正确配置各路由器各接口的IPv6地址，使网络互通。
- 保证两个路由器互连接口地址配置在同一网段，并且可以正常互通。
- 在各主机上配置缺省网关。

9.4 OSPF 路由协议

9.4.1 配置 OSPF 路由协议基本功能示例

规格

适用于所有版本、所有形态的AR路由器。

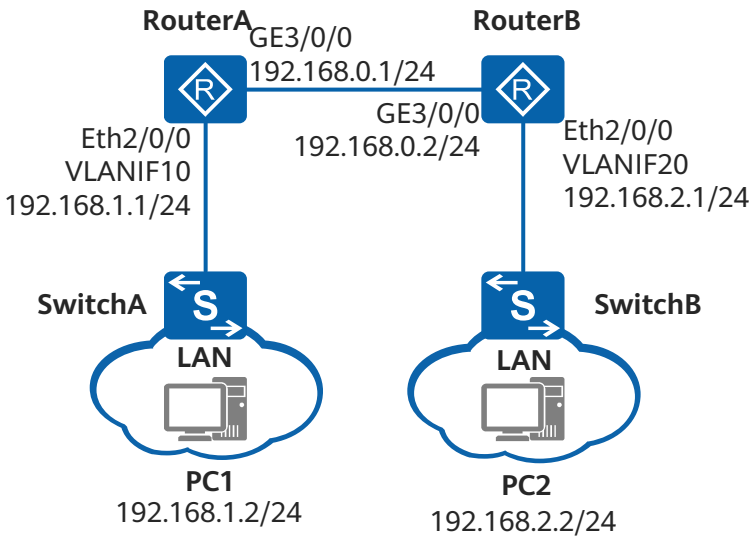
组网需求

企业用户要求不需要花费大量人力去维护网络性能，当网络中出现网络拓扑变动时，可以通过路由更新，计算出新的路由。因此需要使用OSPF动态路由协议保证网络的稳定，实现互连互通。

在配置OSPF的基本功能之前，需完成以下任务：配置接口的网络层地址，使各相邻节点网络层可达。

 版权所有 © 华为技术有限公司

图 9-10 配置 OSPF 路由协议组网图



操作步骤

步骤1 RouterA的配置

```
#
 sysname RouterA
#
router id 1.1.1.1  //Router ID，建议配置为LoopBack0的IP地址
#
vlan batch 10
#
interface Vlanif10
 ip address 192.168.1.1 255.255.255.0
#
interface Ethernet2/0/0
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface GigabitEthernet3/0/0
 ip address 192.168.0.1 255.255.255.0
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
ospf 2
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255  //指定运行OSPF 2协议的接口的IP地址位于192.168.1.0/24网段，接口所属的区域为area 0
  network 192.168.0.0 0.0.0.255
#
```

步骤2 RouterB的配置

```
#
 sysname RouterB
#
router id 2.2.2.2
#
vlan batch 20
#
interface Vlanif20
 ip address 192.168.2.1 255.255.255.0
```


版权所有 © 华为技术有限公司

```
#
interface Ethernet2/0/0
 port link-type trunk
 port trunk allow-pass vlan 20
#
interface GigabitEthernet3/0/0
 ip address 192.168.0.2 255.255.255.0
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
ospf 2
 area 0.0.0.0
  network 192.168.2.0 0.0.0.255
  network 192.168.0.0 0.0.0.255
#
```

步骤3 配置主机

配置PC1的缺省网关为192.168.1.1，PC2的缺省网关为192.168.2.1。

步骤4 配置交换机

配置各交换机，使得各主机能与其网关路由器互通。

步骤5 验证配置结果

在PC1上能成功Ping通PC2的IP地址。

----结束

配置注意事项

- 请配置SwitchA与RouterA对接的接口为Trunk类型接口，并加入VLAN10。
- 请配置SwitchB与RouterB对接的接口为Trunk类型接口，并加入VLAN20。
- 每个OSPF进程的Router ID要保证全网唯一，否则会导致邻居不能正常建立、路由信息不正确的问题。
- RouterA的接口GE3/0/0和RouterB的GE3/0/0所属的OSPF区域一致。

相关资料

视频：**AR系列路由器配置OSPF基本功能**

9.4.2 配置 OSPF 虚连接且验证的示例

规格

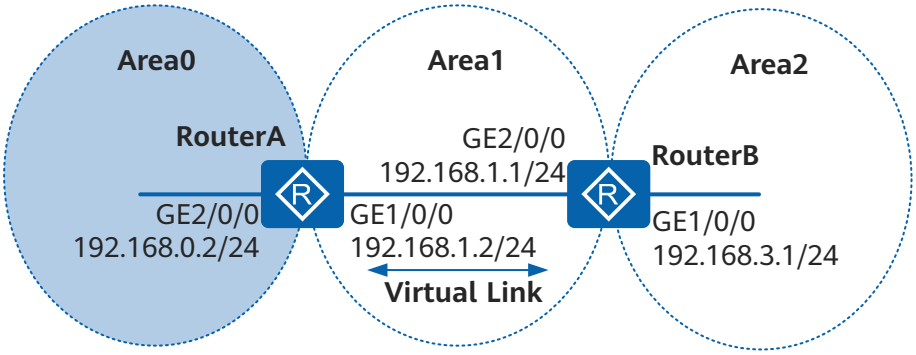
适用于所有版本、所有形态的AR路由器。

组网需求

Area2没有与Area0直接相连。Area1被用作传输区域（Transit Area）来连接Area2和Area0。RouterA和RouterB之间配置一条虚连接，配置完成后，RouterA能够学到Area2中的路由。同时要求所有OSPF邻居之间都要进行OSPF区域验证，所有接口都要进行OSPF接口验证。

 版权所有 © 华为技术有限公司

图 9-11 配置 OSPF 虚连接组网图



操作步骤

步骤1 RouterA的配置

```
#
 sysname RouterA
#
router id 1.1.1.1  //Router ID，建议配置为LoopBack0的IP地址
#
interface GigabitEthernet1/0/0
 ip address 192.168.1.2 255.255.255.0
 ospf authentication-mode hmac-sha256  //配置OSPF接口的验证模式为hmac-sha256验证
#
interface GigabitEthernet2/0/0
 ip address 192.168.0.2 255.255.255.0
 ospf authentication-mode hmac-sha256
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
ospf 2
 area 0.0.0.0
  authentication-mode hmac-sha256  //配置OSPF区域的验证模式为hmac-sha256验证
  network 192.168.0.0 0.0.0.255  //指定运行OSPF 2协议的接口的IP地址位于192.168.0.0/24网段，接口所属的区域为area 0
 area 0.0.0.1
  authentication-mode hmac-sha256
  network 192.168.1.0 0.0.0.255
  vlink-peer 2.2.2.2  //创建对端路由器ID为2.2.2.2的虚连接
#
```

步骤2 RouterB的配置

```
#
 sysname RouterB
#
router id 2.2.2.2
#
interface GigabitEthernet1/0/0
 ip address 192.168.3.1 255.255.255.0
 ospf authentication-mode hmac-sha256
#
interface GigabitEthernet2/0/0
 ip address 192.168.1.1 255.255.255.0
 ospf authentication-mode hmac-sha256
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
ospf 2
```


版权所有 © 华为技术有限公司

```
area 0.0.0.1
 authentication-mode hmac-sha256
 network 192.168.1.0 0.0.0.255
 vlink-peer 1.1.1.1
area 0.0.0.2
 authentication-mode hmac-sha256
 network 192.168.3.0 0.0.0.255
#
```

步骤3 验证配置结果

在RouterA上执行命令**display ip routing-table**，会查看到路由表中有到192.168.3.0/24网段的OSPF路由信息。

----结束

配置注意事项

- 每个OSPF进程的Router ID要保证全网唯一，否则会导致邻居不能正常建立、路由信息不正确的问题。
- 使用OSPF区域验证时，一个区域中所有的路由器在该区域下的验证模式和口令必须一致。
- 使用OSPF接口验证时，同一网段的路由器接口下配置的验证模式和口令必须一致。接口验证方式优先级高于区域验证方式。
- 配置虚连接验证时，两端的路由器配置的验证模式和口令必须一致。

9.4.3 配置 OSPF 的 STUB 区域示例

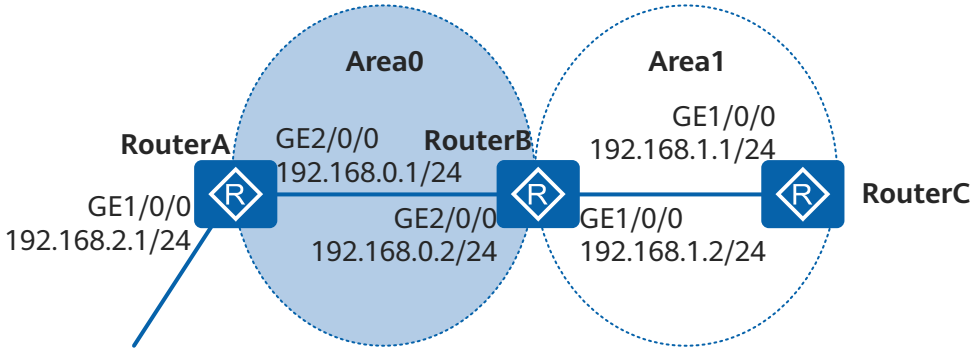
规格

适用于所有版本、所有形态的AR路由器。

组网需求

RouterA、RouterB运行在Area0，RouterB、RouterC运行在Area1，RouterB为ABR。将Area1配置成为STUB区域，RouterC通过ABR发布的缺省路由来访问区域外的网络。

图 9-12 配置 OSPF Stub 区域组网图



 版权所有 © 华为技术有限公司

操作步骤

步骤1 RouterA的配置

```
#
 sysname RouterA
#
router id 1.1.1.1  //Router ID，建议配置为LoopBack0的IP地址
#
interface GigabitEthernet1/0/0
 ip address 192.168.2.1 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 192.168.0.1 255.255.255.0
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
ospf 2
 import-route direct  //配置引入直连路由
 area 0.0.0.0
  network 192.168.0.0 0.0.0.255  //指定运行OSPF 2协议的接口的IP地址位于192.168.0.0/24网段，接口所属的区域为area 0
#
```

步骤2 RouterB的配置

```
#
 sysname RouterB
#
router id 2.2.2.2
#
interface GigabitEthernet1/0/0
 ip address 192.168.1.2 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 192.168.0.2 255.255.255.0
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
ospf 2
 area 0.0.0.0
  network 192.168.0.0 0.0.0.255
 area 0.0.0.1
  network 192.168.1.0 0.0.0.255
  stub  //将Area1设置为Stub区域
#
```

步骤3 RouterC的配置

```
#
 sysname RouterC
#
router id 3.3.3.3
#
interface GigabitEthernet1/0/0
 ip address 192.168.1.1 255.255.255.0
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
#
ospf 2
 area 0.0.0.1
  network 192.168.1.0 0.0.0.255
  stub
#
```

步骤4 验证配置结果

 版权所有 © 华为技术有限公司

运用**Ping**验证，RouterC可以成功和192.168.0.0/24网段以及192.168.2.0/24网段进行通信。

在RouterB上执行命令**display ip routing-table**，会查看到由RouterA引入的外部直连路由信息。

----结束

配置注意事项

- 每个OSPF进程的Router ID要保证全网唯一，否则会导致邻居不能正常建立、路由信息不正确的问题。
- Stub区域中的所有路由器都必须配置Stub属性。

9.4.4 配置 OSPF 的 NSSA 区域示例

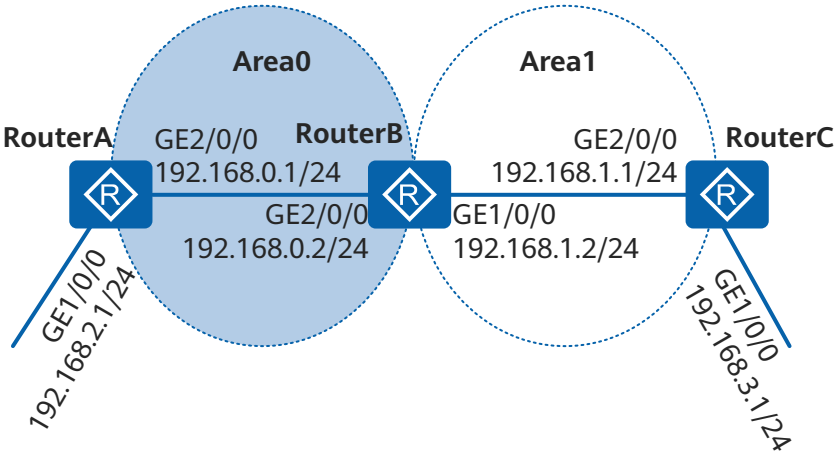
规格

适用于所有版本、所有形态的AR路由器。

组网需求

RouterA、RouterB运行在Area0，RouterB、RouterC运行在Area1，RouterB为ABR。将Area1配置成为NSSA区域，RouterC通过ABR发布的缺省路由来访问区域外的网络。

图 9-13 配置 OSPF NSSA 区域组网图



操作步骤

步骤1 RouterA的配置

```
#
 sysname RouterA
#
router id 1.1.1.1  //Router ID，建议配置为LoopBack0的IP地址
#
interface GigabitEthernet1/0/0
 ip address 192.168.2.1 255.255.255.0
#
```

 版权所有 © 华为技术有限公司

```
interface GigabitEthernet2/0/0
 ip address 192.168.0.1 255.255.255.0
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
ospf 2
 import-route direct  //配置引入直连路由
 area 0.0.0.0
  network 192.168.0.0 0.0.0.255  //指定运行OSPF 2协议的接口的IP地址位于192.168.0.0/24网段，接口所属的区域为area 0
#
```

步骤2 RouterB的配置

```
#
 sysname RouterB
#
router id 2.2.2.2
#
interface GigabitEthernet1/0/0
 ip address 192.168.1.2 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 192.168.0.2 255.255.255.0
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
ospf 2
 area 0.0.0.0
  network 192.168.0.0 0.0.0.255
 area 0.0.0.1
  network 192.168.1.0 0.0.0.255
  nssa default-route-advertise  //将Area1设置为NSSA区域，并在ABR上配置产生缺省的Type7 LSA到NSSA区域
#
```

步骤3 RouterC的配置

```
#
 sysname RouterC
#
router id 3.3.3.3
#
interface GigabitEthernet1/0/0
 ip address 192.168.3.1 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 192.168.1.1 255.255.255.0
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
#
ospf 2
 import-route direct
 area 0.0.0.1
  network 192.168.1.0 0.0.0.255
  nssa  //将Area1设置为NSSA区域
#
```

步骤4 验证配置结果

利用**Ping**验证，RouterC可以成功和192.168.0.0/24，192.168.2.0/24网段进行通信。

在RouterB上执行命令**display ip routing-table**，会查看到由RouterA和RouterC引入的外部直连路由信息。

----结束

 版权所有 © 华为技术有限公司

配置注意事项

- 每个OSPF进程的Router ID要保证全网唯一，否则会导致邻居不能正常建立、路由信息不正确的问题。
- NSSA区域中的所有路由器都必须配置NSSA属性。

9.4.5 配置 OSPF 区域路由聚合功能示例

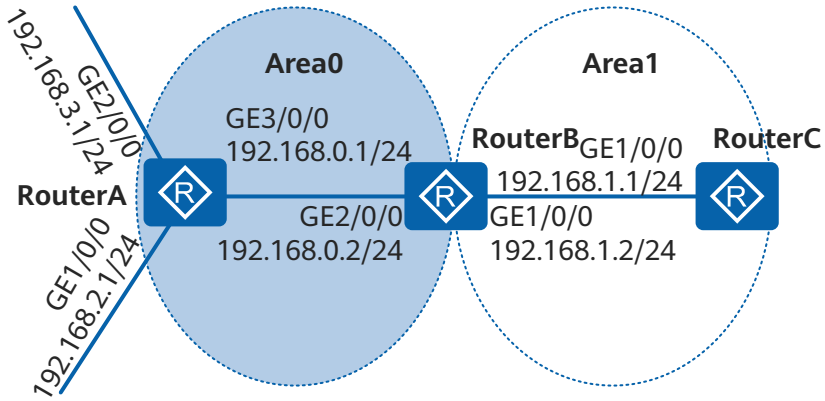
规格

适用于所有版本、所有形态的AR路由器。

组网需求

RouterA、RouterB运行在Area0；RouterB、RouterC运行在Area1，RouterB为ABR。要求RouterB对来自RouterA的某些网段的路由经过聚合后发布给RouterC。

图 9-14 配置 OSPF 区域路由聚合组网图



操作步骤

步骤1 RouterA的配置

```
#
 sysname RouterA
#
router id 1.1.1.1  //Router ID，建议配置为LoopBack0的IP地址
#
interface GigabitEthernet1/0/0
 ip address 192.168.2.1 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 192.168.3.1 255.255.255.0
#
interface GigabitEthernet3/0/0
 ip address 192.168.0.1 255.255.255.0
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
ospf 2
```

 版权所有 © 华为技术有限公司

```
 area 0.0.0.0
  network 192.168.0.0 0.0.0.255  //指定运行OSPF 2协议的接口的IP地址位于192.168.0.0/24网段，接口所属的区域为area 0
  network 192.168.2.0 0.0.0.255
  network 192.168.3.0 0.0.0.255
#
```

步骤2 RouterB的配置

```
#
 sysname RouterB
#
router id 2.2.2.2
#
interface GigabitEthernet1/0/0
 ip address 192.168.1.2 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 192.168.0.2 255.255.255.0
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
ospf 2
 area 0.0.0.0
  abr-summary 192.168.2.0 255.255.254.0  //在区域边界路由器（ABR）上配置路由聚合
  network 192.168.0.0 0.0.0.255
 area 0.0.0.1
  network 192.168.1.0 0.0.0.255
#
```

步骤3 RouterC的配置

```
#
 sysname RouterC
#
router id 3.3.3.3
#
interface GigabitEthernet1/0/0
 ip address 192.168.1.1 255.255.255.0
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
#
ospf 2
 area 0.0.0.1
  network 192.168.1.0 0.0.0.255
#
```

步骤4 验证配置结果

在RouterC上执行命令**display ip routing-table**，会查看到由RouterB发布的到192.168.2.0/23网段以及到192.168.0.0/24网段的OSPF路由信息。

----结束

配置注意事项

- 每个OSPF进程的Router ID要保证全网唯一，否则会导致邻居不能正常建立、路由信息不正确的问题。

9.4.6 配置 OSPF 引入路由聚合功能示例

规格

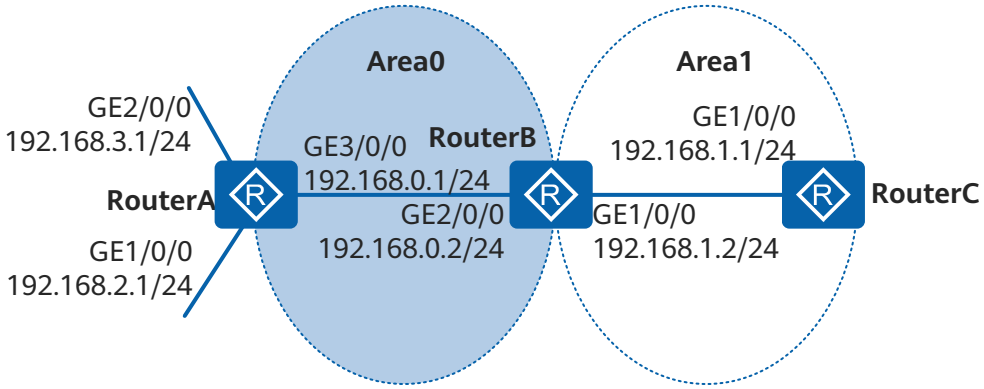
适用于所有版本、所有形态的AR路由器。

 版权所有 © 华为技术有限公司

组网需求

RouterA、RouterB运行在Area0；RouterB、RouterC运行在Area1，RouterA为ASBR，RouterB为ABR。要求RouterA对引入的外部直连路由经过聚合后发布到OSPF自治系统中的其他路由器。

图 9-15 配置 OSPF 引入路由聚合组网图



操作步骤

步骤1 RouterA的配置

```
#
 sysname RouterA
#
router id 1.1.1.1  //Router ID，建议配置为LoopBack0的IP地址
#
interface GigabitEthernet1/0/0
 ip address 192.168.2.1 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 192.168.3.1 255.255.255.0
#
interface GigabitEthernet3/0/0
 ip address 192.168.0.1 255.255.255.0
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
ospf 2
 asbr-summary 192.168.2.0 255.255.254.0  //配置ASBR对引入的路由进行聚合
 import-route direct  //配置引入直连路由
 area 0.0.0.0
  network 192.168.0.0 0.0.0.255  //指定运行OSPF 2协议的接口的IP地址位于192.168.0.0/24网段，接口所属的区域为area 0
#
```

步骤2 RouterB的配置

```
#
 sysname RouterB
#
router id 2.2.2.2
#
interface GigabitEthernet1/0/0
 ip address 192.168.1.2 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 192.168.0.2 255.255.255.0
```


版权所有 © 华为技术有限公司

```
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
ospf 2
 area 0.0.0.0
  network 192.168.0.0 0.0.0.255
 area 0.0.0.1
  network 192.168.1.0 0.0.0.255
#
```

步骤3 RouterC的配置

```
#
 sysname RouterC
#
router id 3.3.3.3
#
interface GigabitEthernet1/0/0
 ip address 192.168.1.1 255.255.255.0
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
#
ospf 2
 area 0.0.0.1
  network 192.168.1.0 0.0.0.255
#
```

步骤4 验证配置结果

在RouterB上执行命令**display ip routing-table**，会查看到由RouterA发布的到192.168.2.0/23网段的引入外部直连路由信息。

在RouterC上执行命令**display ip routing-table**，会查看到由RouterA发布的到192.168.2.0/23网段的引入外部直连路由信息。

----结束

配置注意事项

- 每个OSPF进程的Router ID要保证全网唯一，否则会导致邻居不能正常建立、路由信息不正确的问题。
- 对于普通区域，不能在ABR上对区域内的引入路由进行聚合，只能由ASBR进行聚合。

9.4.7 配置 OSPF 路由信息过滤功能示例

规格

适用于所有版本、所有形态的AR路由器。

组网需求

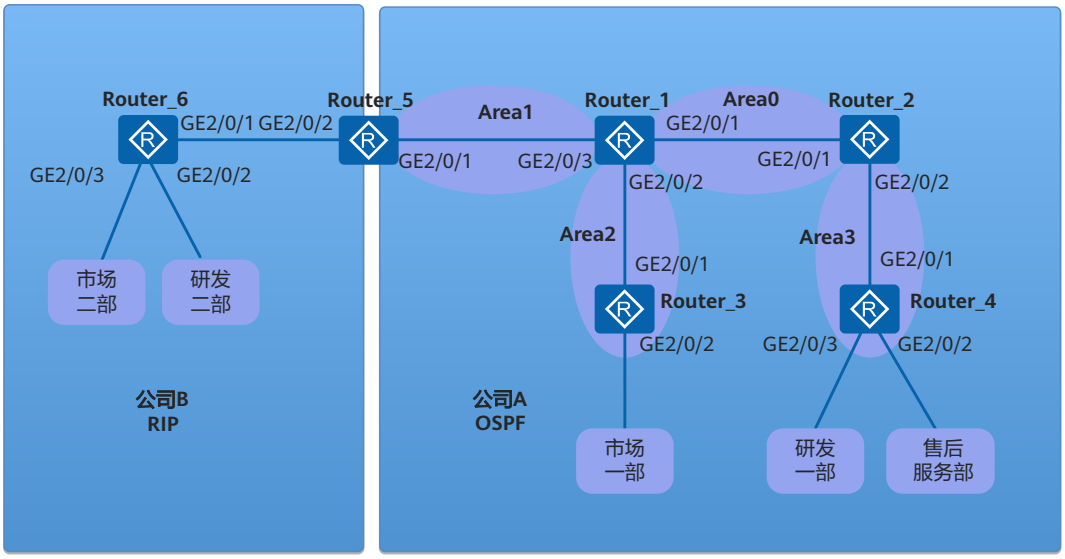
如图9-16所示，公司A使用OSPF路由协议实现公司设备全网互通，后来公司A扩张兼并了公司B，要求将公司B采用的RIP路由协议与公司A的OSPF协议互相引入，使得各个部门可以实现互通。Router_1和Router_2作为公司核心设备负责各个部门间的通信。由于业务需要，现要求通过下列措施控制并调整网络中的路由信息：

- 在Router_5上对引入的路由信息进行过滤，使得研发二部所在网段无法访问市场一部、研发一部和售后服务部所在网段。

 版权所有 © 华为技术有限公司

- 在Router_3上使用路由信息的过滤功能，使得市场一部所在网段无法访问研发一部。
- 在Router_4上使用路由信息的过滤功能，使得研发一部和售后服务部所在网段无法访问市场二部。

图 9-16 OSPF 路由信息过滤组网图



设备	接口	IP地址	设备	接口	IP地址
Router_1	GE2/0/1	10.1.1.1/24	Router_2	GE2/0/1	10.1.1.2/24
	GE2/0/2	10.2.1.1/24		GE2/0/2	10.3.1.1/24
	GE2/0/3	10.4.1.1/24			
Router_3	GE2/0/1	10.2.1.2/24	Router_4	GE2/0/1	10.3.1.2/24
	GE2/0/2	10.10.3.1/24（市场一部所在网段）		GE2/0/2	10.10.1.1/24（售后服务部所在网段）
				GE2/0/3	10.10.2.1/24（研发一部所在网段）
Router_5	GE2/0/1	10.4.1.2/24	Router_6	GE2/0/1	10.5.1.2/24
	GE2/0/2	10.5.1.1/24		GE2/0/2	10.10.4.1/24（研发二部所在网段）

版权所有 © 华为技术有限公司

设备	接口	IP地址	设备	接口	IP地址
				GE2/0/3	10.10.5.1/24（市场二部所在网段）

操作步骤

步骤1 Router_1的配置

```
#
 sysname Router_1
#
interface GigabitEthernet2/0/1
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet2/0/2
 ip address 10.2.1.1 255.255.255.0
#
interface GigabitEthernet2/0/3
 ip address 10.4.1.1 255.255.255.0
#
ospf 1    //使能指定网段的OSPF路由功能
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
 area 0.0.0.1
  network 10.4.1.0 0.0.0.255
 area 0.0.0.2
  network 10.2.1.0 0.0.0.255
#
return
```

步骤2 Router_2的配置

```
#
 sysname Router_2
#
interface GigabitEthernet2/0/1
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet2/0/2
 ip address 10.3.1.1 255.255.255.0
#
ospf 1    //使能指定网段的OSPF路由功能
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
 area 0.0.0.3
  network 10.3.1.0 0.0.0.255
#
return
```

步骤3 Router_3的配置

```
#
 sysname Router_3
#
acl number 2000    //创建基本ACL并匹配需要拒绝访问的源IP地址10.10.2.0/24
 rule 0 deny source 10.10.2.0 0.0.0.255
 rule 5 permit
#
interface GigabitEthernet2/0/1
 ip address 10.2.1.2 255.255.255.0
#
interface GigabitEthernet2/0/2
 ip address 10.10.3.1 255.255.255.0
```

 版权所有 © 华为技术有限公司

```
#
ospf 1    //使能指定网段的OSPF路由功能
 filter-policy 2000 import    //通过指定访问控制列表ACL2000来对要加入到路由表的路由信息进行过滤
 area 0.0.0.2
  network 10.2.1.0 0.0.0.255
  network 10.10.3.0 0.0.0.255
#
return
```

步骤4 Router_4的配置

```
#
 sysname Router_4
#
acl number 2000    //创建基本ACL并匹配需要拒绝访问的源IP地址10.10.5.0/24
 rule 0 deny source 10.10.5.0 0.0.0.255
 rule 5 permit
#
interface GigabitEthernet2/0/1
 ip address 10.3.1.2 255.255.255.0
#
interface GigabitEthernet2/0/2
 ip address 10.10.1.1 255.255.255.0
#
interface GigabitEthernet2/0/3
 ip address 10.10.2.1 255.255.255.0
#
ospf 1    //使能指定网段的OSPF路由功能
 filter-policy 2000 import    //通过指定访问控制列表ACL2000来对要加入到路由表的路由信息进行过滤
 area 0.0.0.3
  network 10.3.1.0 0.0.0.255
  network 10.10.1.0 0.0.0.255
  network 10.10.2.0 0.0.0.255
#
return
```

步骤5 Router_5的配置

```
#
 sysname Router_5
#
acl number 2000    //创建基本ACL并匹配需要拒绝访问的源IP地址10.10.4.0/24
 rule 0 deny source 10.10.4.0 0.0.0.255
 rule 5 permit
#
interface GigabitEthernet2/0/1
 ip address 10.4.1.2 255.255.255.0
#
interface GigabitEthernet2/0/2
 ip address 10.5.1.1 255.255.255.0
#
ospf 1    //使能指定网段的OSPF路由功能
 import-route direct    //将直连路由引入到OSPF网络中
 import-route rip 1    //将RIP路由引入到OSPF网络中
 filter-policy 2000 export rip 1    //通过指定访问控制列表ACL2000来对引入OSPF的RIP路由信息进行过滤
 area 0.0.0.1
  network 10.4.1.0 0.0.0.255
#
rip 1    //使能指定网段的RIP功能
 undo summary
 version 2
 network 10.5.1.0
 import-route direct    //将直连路由引入到RIP网络中
 import-route ospf 1    //和OSPF路由引入到RIP网络中
#
return
```

步骤6 Router_6的配置

```
#
 sysname Router_6
#
```

 版权所有 © 华为技术有限公司

```
interface GigabitEthernet2/0/1
 ip address 10.5.1.2 255.255.255.0
#
interface GigabitEthernet2/0/2
 ip address 10.10.4.1 255.255.255.0
#
interface GigabitEthernet2/0/3
 ip address 10.10.5.1 255.255.255.0
#
rip 1    //使能指定网段的RIP功能
 undo summary
 version 2
 network 10.5.1.0
 network 10.10.4.0
 network 10.10.5.0
#
return
```

步骤7 验证配置结果

在Router_3上使用源地址10.10.3.1Ping目标地址10.10.2.1不通，说明市场一部所在网段无法访问研发一部所在网段。

在Router_4上使用源地址10.10.1.1和10.10.2.1分别Ping目标地址10.10.5.1均不通，说明研发一部和售后服务部所在网段无法访问市场二部所在网段。

查看Router_3和Router_4的路由表信息中均没有10.10.4.0/24网段路由信息，说明研发二部所在网段无法访问市场一部、研发一部和售后服务部所在网段。

----结束

配置注意事项

- 路由信息过滤功能中对于引入外部路由信息时采用**export**关键字进行过滤，该参数只能在ASBR上生效。
- 路由信息过滤功能只是对路由表中相关路由信息过滤，并不是过滤掉OSPF中通告的LSA。
- 由于路由通信是双向的，使用路由信息过滤功能将某一目的网段过滤后，该路由器下联的其它网段无法访问这个目的网段的设备，这个目的网段的设备也不能访问源地址网段的设备。
- 使用路由信息过滤功能配合ACL使用时，必须将最后一条规则设置为允许所有源地址通过才能避免将所有网段路由全部过滤掉。

9.4.8 配置 OSPF 路由协议与 BFD 联动示例

规格

适用于所有版本、所有形态的AR路由器。

组网需求

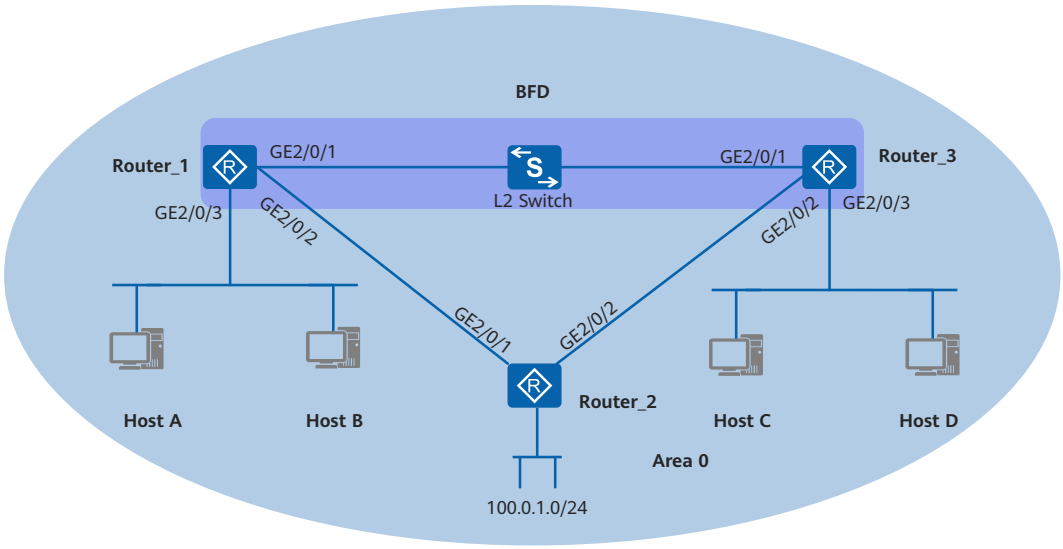
图1为某公司的部门网络架构。公司希望保证网络层相互可达，达到快速检测、监控网络中链路或者IP路由的转发连通状况的目的，因此可以采用OSPF与BFD联动技术，采用BFD控制报文方式实现当Router_1或Router_3与二层交换机之间的链路出现故障（如链路down）时，BFD能够快速感知并通告OSPF协议。

现要求通过在Router_1和Router_3上配置OSPF与BFD联动功能，实现如下要求：

 版权所有 © 华为技术有限公司

- 监测通过L2 Switch通信的链路。
- 当链路出现故障时设备能够快速感知并通告OSPF协议，快速切换到Router_2链路进行通信。

图 9-17 OSPF 与 BFD 联动配置组网图



设备	接口	IP地址
Router_1	GE2/0/1	10.1.0.101/24
	GE2/0/2	10.10.0.101/24
	GE2/0/3	10.20.1.1/24
Host A	-	10.20.1.2/24
Router_2	GE2/0/1	10.10.0.102/24
	GE2/0/2	10.40.1.101/24
Router_3	GE2/0/1	10.1.0.102/24
	GE2/0/2	10.40.1.102/24
	GE2/0/3	10.30.1.1/24
Host C	-	10.30.1.2/24

操作步骤

步骤1 Router_1的配置文件

```
#
 sysname Router_1
#
bfd
#
```


版权所有 © 华为技术有限公司

```
interface GigabitEthernet2/0/1
 ip address 10.1.0.101 255.255.255.0
 ospf bfd enable    //配置接口的BFD特性
 ospf bfd min-tx-interval 100 min-rx-interval 100
#
interface GigabitEthernet2/0/2
 ip address 10.10.0.101 255.255.255.0
#
interface GigabitEthernet2/0/3
 ip address 10.20.1.1 255.255.255.0
#
ospf 1    //配置Router_1的OSPF基本功能，并使能OSPF的BFD功能
 bfd all-interfaces enable
 area 0.0.0.0
  network 10.1.0.0 0.0.0.255
  network 10.10.0.0 0.0.0.255
  network 10.20.1.0 0.0.0.255
#
return
```

步骤2 Router_2的配置文件

```
#
 sysname Router_2
#
bfd
#
acl number 2000    //创建ACL 2000，允许源IP地址为10.20.0.0/24的报文通过
 rule 0 permit source 10.20.0.0 0.0.0.255
#
interface GigabitEthernet2/0/1
 ip address 10.10.0.102 255.255.255.0
#
interface GigabitEthernet2/0/2
 ip address 10.40.1.101 255.255.255.0
#
ospf 1    //配置Router_2的OSPF基本功能
 bfd all-interfaces enable
 area 0.0.0.0
  network 10.10.0.0 0.0.0.255
  network 10.40.1.0 0.0.0.255
#
return
```

步骤3 Router_3的配置文件

```
#
 sysname Router_3
#
bfd
#
interface GigabitEthernet2/0/1
 ip address 10.1.0.102 255.255.255.0
 ospf bfd enable    //配置接口的BFD特性
 ospf bfd min-tx-interval 100 min-rx-interval 100
#
interface GigabitEthernet2/0/2
ip address 10.40.1.102 255.255.255.0
#
interface GigabitEthernet2/0/3
ip address 10.30.1.1 255.255.255.0
#
ospf 1    //配置Router_3的OSPF基本功能，并使能OSPF的BFD功能
 bfd all-interfaces enable
 area 0.0.0.0
  network 10.1.0.0 0.0.0.255
  network 10.30.1.0 0.0.0.255
  network 10.40.1.0 0.0.0.255
#
return
```

 版权所有 © 华为技术有限公司

步骤4 验证配置结果

执行**Ping**命令检查Router_1连接的主机host A（10.20.1.2）到Router_3连接的主机host C（10.30.1.2）路由可达。

执行**display ospf peer**命令查看Router_1 上OSPF邻居信息，显示Router_1和Router_3已建立OSPF邻居关系。

分别在Router_1和Router_3上执行**display ospf bfd session all**命令查看Router_1和Router_3上BFD会话已被创建，且状态为UP。

在Router_1上执行**display ip routing-table 10.30.1.0 verbose**命令查看10.30.1.0/24的路由信息，可以看出Router_1和Router_3是通过L2 Switch进行通信的。

----结束

9.5 OSPFv3 路由协议

9.5.1 配置 OSPFv3 路由协议基本功能示例

规格

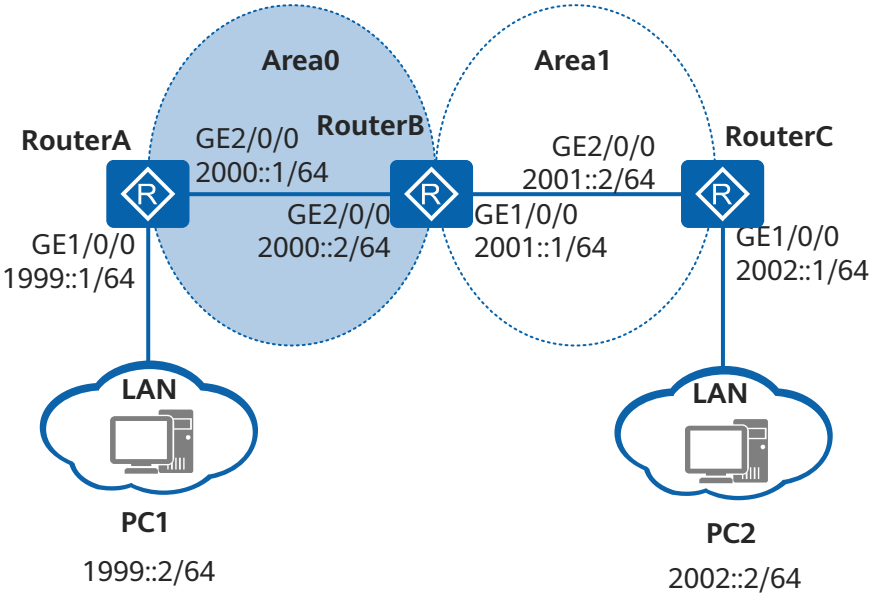
适用于ARV200R002C00及更高版本、所有形态的AR路由器。

适用于所有版本、所有形态的AR路由器。

组网需求

在RouterA，RouterB和RouterC上启用OSPFv3路由协议。RouterA，RouterC引入外部直连路由来与PC连接，要求PC1与PC2能够互相ping通。

图 9-18 配置 OSPFv3 路由协议组网图



版权所有 © 华为技术有限公司

操作步骤

步骤1 RouterA的配置

```
#
 sysname RouterA
#
ipv6  //配置使能路由设备转发IPv6单播报文
#
ospfv3 2
 router-id 10.10.10.10  //配置运行OSPFv3 2协议路由的路由器ID为10.10.10.10
 import-route direct  //配置引入外部路由
#
interface GigabitEthernet1/0/0
 ipv6 enable  //配置在接口上使能IPv6功能
 ipv6 address 1999::1/64
#
interface GigabitEthernet2/0/0
 ipv6 enable  //配置在接口上使能IPv6功能
 ipv6 address 2000::1/64
 ospfv3 2 area 0.0.0.0  //配置在接口上使能OSPFv3 2的进程，并指定所属Area0
#
```

步骤2 RouterB的配置

```
#
 sysname RouterB
#
ipv6
#
ospfv3 2
 router-id 20.20.20.20
#
interface GigabitEthernet1/0/0
 ipv6 enable
 ipv6 address 2001::1/64
 ospfv3 2 area 0.0.0.1
#
interface GigabitEthernet2/0/0
 ipv6 enable
 ipv6 address 2000::2/64
 ospfv3 2 area 0.0.0.0
#
```

步骤3 RouterC的配置

```
#
 sysname RouterC
#
ipv6
#
ospfv3 2
 router-id 30.30.30.30
 import-route direct
#
interface GigabitEthernet1/0/0
 ipv6 enable
 ipv6 address 2002::1/64
#
interface GigabitEthernet2/0/0
 ipv6 enable
 ipv6 address 2001::2/64
 ospfv3 2 area 0.0.0.1
#
```

步骤4 验证配置结果

 版权所有 © 华为技术有限公司

PC1和PC2能够互相Ping通。

----结束

配置注意事项

- OSPFv3的Router ID必须手工配置，如果没有配置ID号，OSPFv3无法正常运行。
- 手工配置Router ID时，必须保证自治系统中任意两台路由器的Router ID都不相同。如果在同一台路由器上运行了多个OSPFv3进程，必须为不同的进程指定不同的Router ID。
- 配置IPv6路由协议前，一定要先使能路由设备转发IPv6单播报文。在接口下配置关于IPv6特性的命令前必须先在接口上使能IPv6功能。

9.5.2 配置 OSPFv3 双进程路由互通功能示例

规格

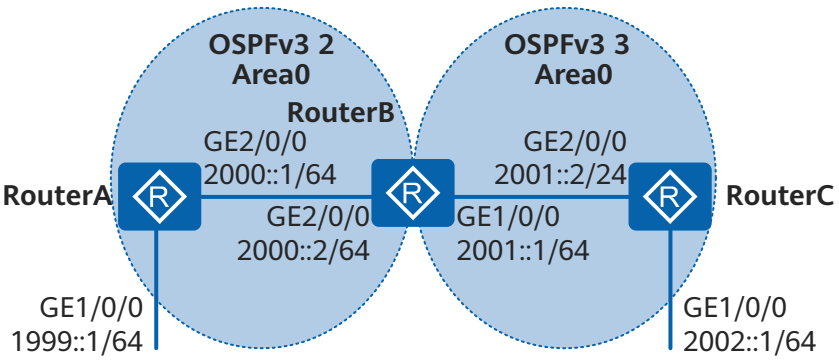
适用于ARV200R002C00及更高版本、所有形态的AR路由器。

适用于所有版本、所有形态的AR路由器。

组网需求

在RouterA，RouterB启用OSPFv3 2进程路由协议，在RouterB，RouterC启用OSPFv3 3进程路由协议。要求RouterA的GE1/0/0接口地址与RouterC的GE1/0/0接口地址能够互相Ping通。

图 9-19 配置 OSPFv3 双进程路由互通功能组网图



操作步骤

步骤1 RouterA的配置

```
#
 sysname RouterA
#
ipv6  //配置使能路由设备转发IPv6单播报文
#
ospfv3 2
 router-id 10.10.10.10  //配置运行OSPFv3 2协议路由的路由器ID为10.10.10.10
#
interface GigabitEthernet1/0/0
```

 版权所有 © 华为技术有限公司

```
 ipv6 enable  //配置在接口上使能IPv6功能
 ipv6 address 1999::1/64
 ospfv3 2 area 0.0.0.0  //配置在接口上使能OSPFv3 2的进程，并指定所属Area0
#
interface GigabitEthernet2/0/0
 ipv6 enable
 ipv6 address 2000::1/64
 ospfv3 2 area 0.0.0.0
#
```

步骤2 RouterB的配置

```
#
 sysname RouterB
#
ipv6
#
ospfv3 2
 router-id 22.22.22.22
 import-route ospfv3 3  //配置引入OSPFv3进程3路由
#
ospfv3 3
 router-id 23.23.23.23
 import-route ospfv3 2
#
interface GigabitEthernet1/0/0
 ipv6 enable
 ipv6 address 2001::1/64
 ospfv3 3 area 0.0.0.0
#
interface GigabitEthernet2/0/0
 ipv6 enable
 ipv6 address 2000::2/64
 ospfv3 2 area 0.0.0.0
#
```

步骤3 RouterC的配置

```
#
 sysname RouterC
#
ipv6
#
ospfv3 3
 router-id 30.30.30.30
#
interface GigabitEthernet1/0/0
 ipv6 enable
 ipv6 address 2002::1/64
 ospfv3 3 area 0.0.0.0
#
interface GigabitEthernet2/0/0
 ipv6 enable
 ipv6 address 2001::2/64
 ospfv3 3 area 0.0.0.0
#
```

步骤4 验证配置结果

在RouterA上执行命令**ping ipv6 -a 1999::1 2002::1**，可以实现RouterA的GE1/0/0接口地址与RouterC的GE1/0/0接口地址能够互相Ping通。

----结束

配置注意事项

- OSPFv3的Router ID必须手工配置，如果没有配置ID号，OSPFv3无法正常运行。

 版权所有 © 华为技术有限公司

- 手工配置Router ID时，必须保证自治系统中任意两台路由器的Router ID都不相同。如果在同一台路由器上运行了多个OSPFv3进程，必须为不同的进程指定不同的Router ID。
- 配置IPv6路由协议前，一定要先使能路由设备转发IPv6单播报文。在接口下配置关于IPv6特性的命令前必须先在接口上使能IPv6功能。

9.5.3 配置 OSPFv3 路由信息过滤功能示例

规格

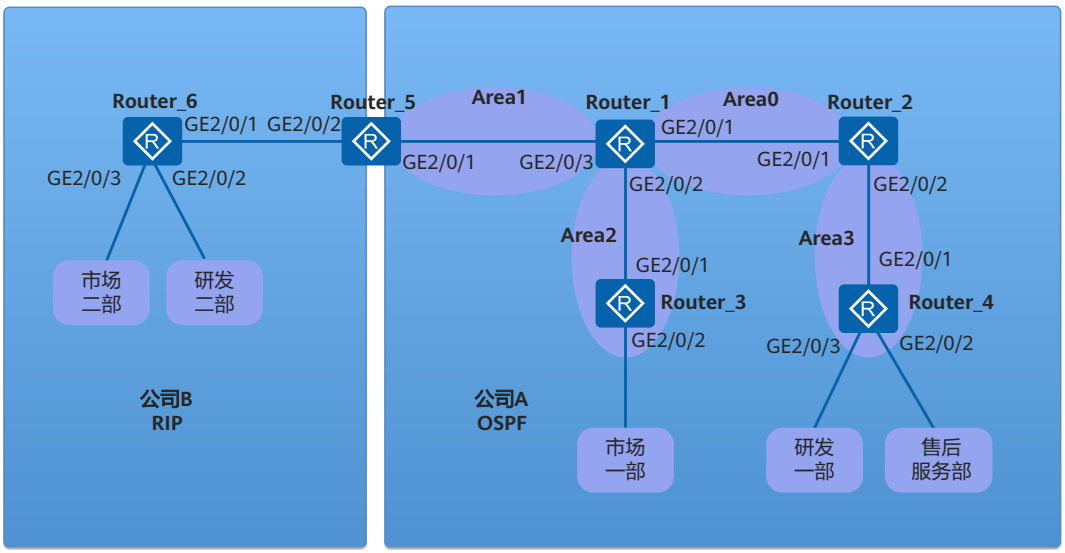
适用于所有版本、所有形态的AR路由器。

组网需求

如图9-20所示，公司A使用OSPFv3路由协议实现公司设备全网互通，后来公司A扩张兼并了公司B，要求将公司B采用的RIPng路由协议与公司A的OSPFv3协议互相引入，使得各个部门可以实现互通。Router_1和Router_2作为公司核心设备负责各个部门间的通信。由于业务需要，现要求通过下列措施控制并调整网络中的路由信息：

- 在Router_5上对引入的路由信息进行过滤，使得研发二部所在网段无法访问市场一部、研发一部和售后服务部所在网段。
- 在Router_3上使用路由信息的过滤功能，使得市场一部所在网段无法访问研发一部。
- 在Router_4上使用路由信息的过滤功能，使得研发一部和售后服务部所在网段无法访问市场二部。

图 9-20 OSPFv3 路由信息过滤组网图



设备	接口	IPv6地址	设备	接口	IPv6地址
Router_1	GE2/0/1	FC01::1/64	Router_2	GE2/0/1	FC01::2/64
	GE2/0/2	FC02::1/64		GE2/0/2	FC03::1/64

版权所有 © 华为技术有限公司

设备	接口	IPv6地址	设备	接口	IPv6地址
	GE2/0/3	FC04::1/64			
Router_3	GE2/0/1	FC02::2/64	Router_4	GE2/0/1	FC03::2/64
	GE2/0/2	FC13::1/64（市场一部所在网段）		GE2/0/2	FC11::1/64（售后服务部所在网段）
				GE2/0/3	FC12::1/64（研发一部所在网段）
Router_5	GE2/0/1	FC04::2/64	Router_6	GE2/0/1	FC05::2/64
	GE2/0/2	FC05::1/64		GE2/0/2	FC14::1/64（研发二部所在网段）
				GE2/0/3	FC15::1/64（市场二部所在网段）

操作步骤

步骤1 Router_1的配置

```
#
 sysname Router_1
#
ipv6
#
interface GigabitEthernet2/0/1
 ipv6 enable
 ipv6 address FC01::1/64
 ospfv3 1 area 0.0.0.0
#
interface GigabitEthernet2/0/2
 ipv6 enable
 ipv6 address FC02::1/64
 ospfv3 1 area 0.0.0.2
#
interface GigabitEthernet2/0/3
 ipv6 enable
 ipv6 address FC04::1/64
 ospfv3 1 area 0.0.0.1
#
ospfv3 1    //创建OSPFv3进程，并在Router_1的接口上使能OSPFv3路由功能
 router-id 6.6.6.6
 area 0.0.0.0
 area 0.0.0.1
 area 0.0.0.2
#
return
```

步骤2 Router_2的配置

```
#
 sysname Router_2
#
```

 版权所有 © 华为技术有限公司

```
ipv6
#
interface GigabitEthernet2/0/1
 ipv6 enable
 ipv6 address FC01::2/64
 ospfv3 1 area 0.0.0.0
#
interface GigabitEthernet2/0/2
 ipv6 enable
 ipv6 address FC03::1/64
 ospfv3 1 area 0.0.0.3
#
ospfv3 1    //创建OSPFv3进程，并在Router_2的接口上使能OSPFv3路由功能
 router-id 5.5.5.5
 area 0.0.0.0
 area 0.0.0.3
#
return
```

步骤3 Router_3的配置

```
#
 sysname Router_3
#
acl ipv6 number 2000    //创建基本IPv6 ACL并匹配需要拒绝访问的源网段FC12::1/64
 rule 0 deny source FC12::/64
 rule 5 permit
#
ipv6
#
interface GigabitEthernet2/0/1
 ipv6 enable
 ipv6 address FC02::2/64
 ospfv3 1 area 0.0.0.2
#
interface GigabitEthernet2/0/2
 ipv6 enable
 ipv6 address FC13::1/64
 ospfv3 1 area 0.0.0.2
#
ospfv3 1    //创建OSPFv3进程，并在Router_3的接口上使能OSPFv3路由功能
 router-id 4.4.4.4
 filter-policy 2000 import    //通过指定访问控制列表IPv6 ACL2000来对要加入到路由表的路由信息进行过滤
 area 0.0.0.2
#
return
```

步骤4 Router_4的配置

```
#
 sysname Router_4
#
acl ipv6 number 2000    //创建基本IPv6 ACL并匹配需要拒绝访问的源网段FC15::1/64
 rule 0 deny source FC15::/64
 rule 5 permit
#
ipv6
#
interface GigabitEthernet2/0/1
 ipv6 enable
 ipv6 address FC03::2/64
 ospfv3 1 area 0.0.0.3
#
interface GigabitEthernet2/0/2
 ipv6 enable
 ipv6 address FC11::1/64
 ospfv3 1 area 0.0.0.3
#
interface GigabitEthernet2/0/3
 ipv6 enable
 ipv6 address FC12::1/64
```

 版权所有 © 华为技术有限公司

```
 ospfv3 1 area 0.0.0.3
#
ospfv3 1    //创建OSPFv3进程，并在Router_4的接口上使能OSPFv3路由功能
 router-id 3.3.3.3
 filter-policy 2000 import    //通过指定访问控制列表IPv6 ACL2000来对要加入到路由表的路由信息进行过滤
 area 0.0.0.3
#
return
```

步骤5 Router_5的配置

```
#
 sysname Router_5
#
acl ipv6 number 2000    //创建基本IPv6 ACL并匹配需要拒绝访问的源网段FC14::1/64
 rule 0 deny source FC14::/64
 rule 5 permit
#
ipv6
#
interface GigabitEthernet2/0/1
 ipv6 enable
 ipv6 address FC04::2/64
 ospfv3 1 area 0.0.0.1
#
interface GigabitEthernet2/0/2
 ipv6 enable
 ipv6 address FC05::1/64
 ripng 1 enable
#
ospfv3 1    //创建OSPFv3进程，并在Router_5的接口上使能OSPFv3路由功能
 router-id 2.2.2.2
 filter-policy 2000 export ripng 1    //通过指定访问控制列表IPv6 ACL2000来对引入OSPFv3的RIPng路由信息进
行过滤
 import-route direct    //将直连路由引入到OSPFv3网络中
 import-route ripng 1    //将RIPng路由引入到OSPFv3网络中
 area 0.0.0.1
#
ripng 1    //创建RIPng进程，并在Router_5的接口上使能RIPng路由功能
 import-route direct    //将直连路由引入到RIPng网络中
 import-route ospfv3 1    //将OSPFv3路由引入到RIPng网络中
#
return
```

步骤6 Router_6的配置

```
#
 sysname Router_6
#
ipv6
#
interface GigabitEthernet2/0/1
 ipv6 enable
 ipv6 address FC05::2/64
 ripng 1 enable
#
interface GigabitEthernet2/0/2
 ipv6 enable
 ipv6 address FC14::1/64
 ripng 1 enable
#
interface GigabitEthernet2/0/3
 ipv6 enable
 ipv6 address FC15::1/64
 ripng 1 enable
#
ripng 1    //创建RIPng进程，并在Router_6的接口上使能RIPng路由功能
#
return
```

 版权所有 © 华为技术有限公司

步骤7 验证配置结果

在Router_3上使用源地址FC13::1Ping目标地址FC12::1不通，说明市场一部所在网段无法访问研发一部所在网段。

在Router_4上使用源地址FC11::1和FC12::1分别Ping目标地址FC15::1均不通，说明研发一部和售后服务部所在网段无法访问市场二部所在网段。

查看Router_3和Router_4的路由表信息中均没有FC14::/64网段路由信息，说明研发二部所在网段无法访问市场一部、研发一部和售后服务部所在网段。

----结束

配置注意事项

- 路由信息过滤功能中对于引入外部路由信息时采用**export**关键字进行过滤，该参数只能在ASBR上生效。
- 路由信息过滤功能只是对路由表中相关路由信息过滤，并不是过滤掉OSPFv3中通告的LSA。
- 由于路由通信是双向的，使用路由信息过滤功能将某一目的网段过滤后，该路由器下联的其它网段无法访问这个目的网段的设备，这个目的网段的设备也不能访问源地址网段的设备。
- 使用路由信息过滤功能配合ACL使用时，必须将最后一条规则设置为允许所有源地址通过才能避免将所有网段路由被全部过滤掉。
- 配置OSPFv3时必须手工指定Router ID。

9.6 IS-IS（IPv4）路由协议

9.6.1 配置 IS-IS 的路由渗透功能示例

规格

适用于所有版本、所有形态的AR路由器。

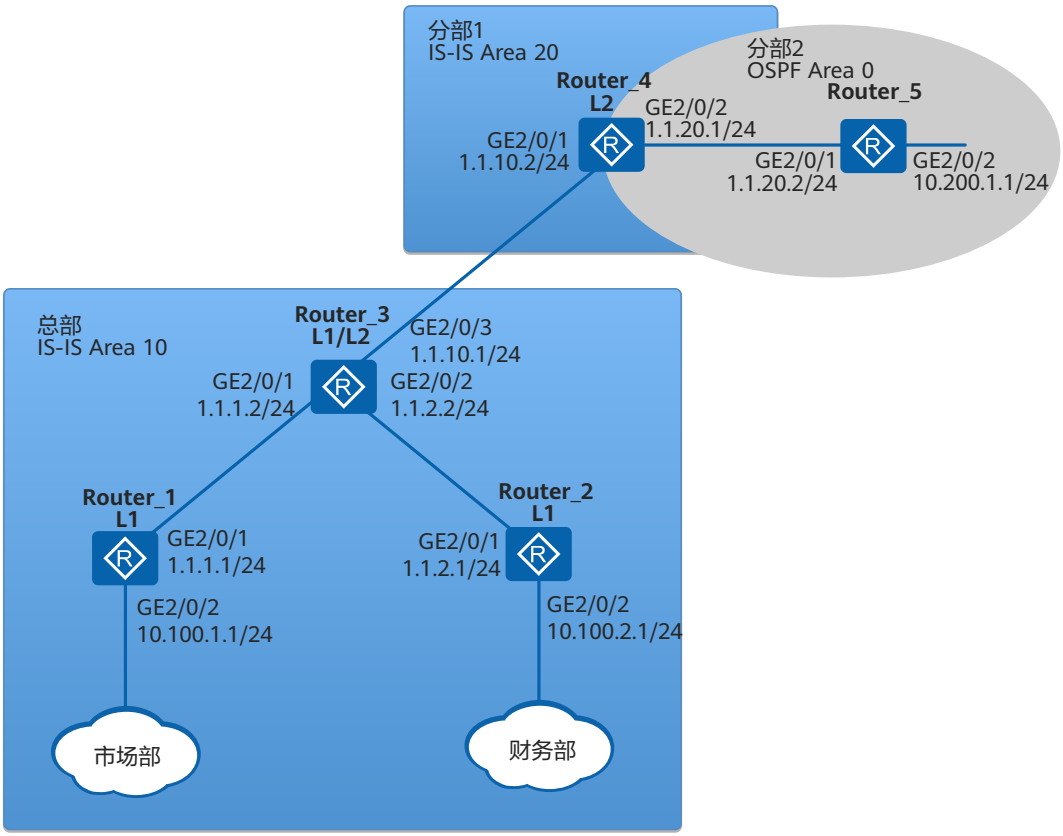
组网需求

如图9-21所示，某公司总部和分部1使用IS-IS路由协议进行互联。公司总部内为市场部和财务部设置了独立的网络。该公司的分部2使用的是OSPF路由协议。现要求：

- 公司总部内市场部和财务部可以通信；并通过配置路由渗透功能，实现总部与分部间、市场部与分部可以正常通信，财务部与分部无法通信，且分部无法查看到财务部的路由信息。
- 将分部2的OSPF路由引入公司分部的网络中，并保证市场部与分部2可以通信。
- 当总部的网关设备Router_3 IS-IS协议进程重启时，原有的通信不中断。

 版权所有 © 华为技术有限公司

图 9-21 IS-IS 的典型配置组网图



操作步骤

步骤1 Router_1的配置

```
#
 sysname Router_1
#
isis 1    //配置IS-IS基本功能
 is-level level-1
 network-entity 10.0000.0000.1001.00
#
interface GigabitEthernet2/0/1
 ip address 1.1.1.1 255.255.255.0
 isis enable 1
#
interface GigabitEthernet2/0/2
 ip address 10.100.1.1 255.255.255.0
 isis enable 1
#
return
```

步骤2 Router_2的配置

```
#
 sysname Router_2
#
isis 1    //配置IS-IS基本功能
 is-level level-1
 network-entity 10.0000.0000.2001.00
#
interface GigabitEthernet2/0/1
```


版权所有 © 华为技术有限公司

```
 ip address 1.1.2.1 255.255.255.0
 isis enable 1
#
interface GigabitEthernet2/0/2
 ip address 10.100.2.1 255.255.255.0
 isis enable 1
#
return
```

步骤3 Router_3的配置

```
#
 sysname Router_3
#
isis 1    //配置IS-IS基本功能
 graceful-restart    //使能IS-IS协议的GR能力
 network-entity 10.0000.0001.0001.00
 import-route isis level-1 into level-2 filter-policy ip-prefix 1    //配置IS-IS路由渗透，并引用名为1的地址前缀列表，实现Level-1区域只将10.100.1.0/24网段的路由信息向Level-2发布
#
interface GigabitEthernet2/0/1
 ip address 1.1.1.2 255.255.255.0
 isis enable 1
#
interface GigabitEthernet2/0/2
 ip address 1.1.2.2 255.255.255.0
 isis enable 1
#
interface GigabitEthernet2/0/3
 ip address 1.1.10.1 255.255.255.0
 isis enable 1
#
ip ip-prefix 1 index 10 permit 10.100.1.0 24
#
return
```

步骤4 Router_4的配置

```
#
 sysname Router_4
#
isis 1    //配置IS-IS基本功能
 is-level level-2
 network-entity 20.0000.0002.0001.00
 import-route direct    //配置IS-IS进程引入直连路由
 import-route ospf 1    //配置IS-IS进程引入OSPF进程的路由
#
interface GigabitEthernet2/0/1
 ip address 1.1.10.2 255.255.255.0
 isis enable 1
#
interface GigabitEthernet2/0/2
 ip address 1.1.20.1 255.255.255.0
 isis enable 1
#
ospf 1    //配置OSPF基本功能
 import-route direct    //配置OSPF进程引入直连路由
 import-route isis 1    //配置OSPF进程引入IS-IS进程的路由
 area 0.0.0.0
  network 1.1.20.0 0.0.0.255
#
return
```

步骤5 Router_5的配置

```
#
 sysname Router_5
#
interface GigabitEthernet2/0/1
 ip address 1.1.20.2 255.255.255.0
#
interface GigabitEthernet2/0/2
```

 版权所有 © 华为技术有限公司

```
 ip address 10.200.1.1 255.255.255.0
#
ospf 1    //配置OSPF基本功能
 area 0.0.0.0
  network 10.200.1.0 0.0.0.255
  network 1.1.20.0 0.0.0.255
#
return
```

步骤6 验证配置结果

在Router_4上查看IS-IS路由表，可以查看到市场部（10.100.1.0/24）的路由，无法查看到财务部（10.100.2.0/24）的路由，说明公司分部只能与市场部通信。

在Router_3上查看IS-IS路由表，可以看到10.200.1.0/24的路由，并且执行**ping**命令到10.200.1.1地址，路由可达，说明本公司的市场部与分部2可以正常通信。

在Router_1上持续执行**ping**命令到Router_2，期间在Router_3上重启IS-IS进程，查看Router_3的IS-IS协议重启时，通信未中断。并使用**display isis graceful-restart status**命令，可查看Router_3上IS-IS协议的GR状态。

----结束

配置注意事项

在设备平滑重启过程中，请勿变更拓扑，否则可能导致路由黑洞。

9.6.2 配置 IS-IS 的路由聚合功能示例

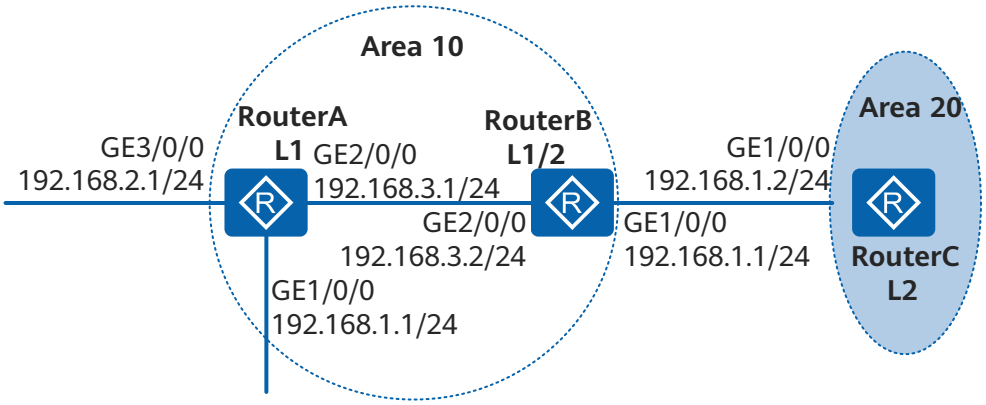
规格

适用于所有版本、所有形态的AR路由器。

组网需求

如图9-22所示，网络中的三台路由器都配置了IS-IS路由协议。其中RouterA作为Level-1路由器、RouterB作为Level-1–2路由器都属于Area10，RouterC作为Level-2路由器属于Area20。要求将Area10中所有的路由信息聚合后发送给RouterC。

图 9-22 配置 IS-IS 的路由聚合功能组网图



 版权所有 © 华为技术有限公司

操作步骤

步骤1 RouterA的配置

```
#
 sysname RouterA
#
isis 10  //启动IS-IS路由进程10
 is-level level-1  //配置路由器级别为Level-1
 network-entity 10.0000.0000.0001.00  //配置IS-IS路由进程的网络实体名称NET
#
interface GigabitEthernet1/0/0
 ip address 192.168.1.1 255.255.255.0
 isis enable 10  //在接口上使能IS-IS
#
interface GigabitEthernet2/0/0
 ip address 192.168.3.1 255.255.255.0
 isis enable 10
#
interface GigabitEthernet3/0/0
 ip address 192.168.2.1 255.255.255.0
 isis enable 10
#
```

步骤2 RouterB的配置

```
#
 sysname RouterB
#
isis 10
 network-entity 10.0000.0000.0002.00
 summary 192.168.0.0 255.255.0.0 level-1-2  //配置IS-IS生成聚合路由
#
interface GigabitEthernet1/0/0
 ip address 192.168.1.1 255.255.255.0
 isis enable 10
#
interface GigabitEthernet2/0/0
 ip address 192.168.3.2 255.255.255.0
 isis enable 10
#
```

步骤3 RouterC的配置

```
#
 sysname RouterC
#
isis 10
 is-level level-2
 network-entity 20.0000.0000.0003.00
#
interface GigabitEthernet1/0/0
 ip address 192.168.1.2 255.255.255.0
 isis enable 10
#
```

步骤4 验证配置结果

在RouterC上执行命令**display isis route**，发现到Area10中所有网段的路由信息都聚合成了到目的网段192.168.0.0/16的一条路由信息。

----结束

配置注意事项

- 使用命令**network-entity**设置IS-IS路由进程的网络实体名称NET时，同一个区域内的路由器设备区域ID必须相同。

 版权所有 © 华为技术有限公司

9.6.3 配置 IS-IS 路由协议与 BFD 联动示例

规格

适用于所有版本、所有形态的AR路由器。

组网需求

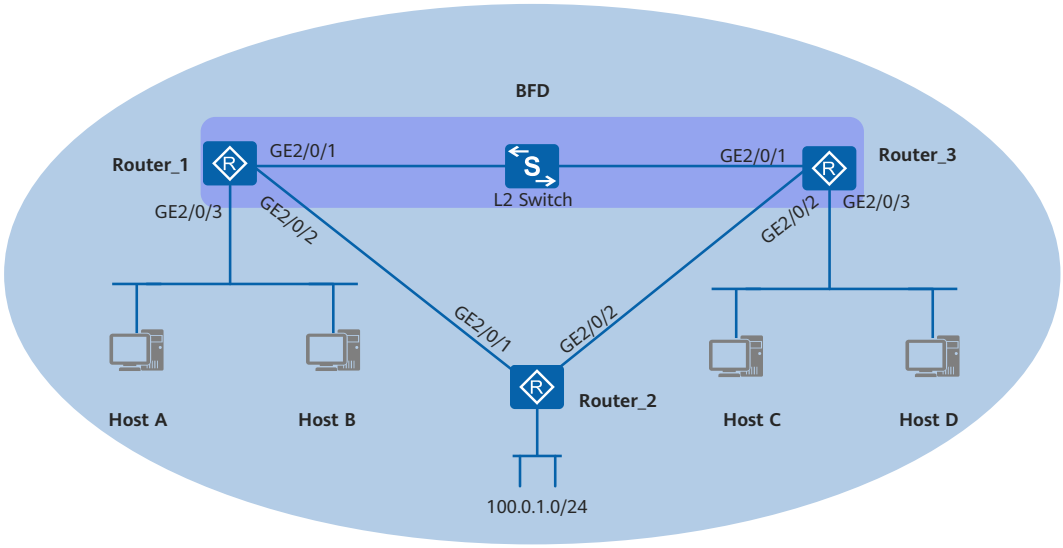
如图9-23所示，某公司通过一台二层交换机作为中继将两个相距较远的部门连接。Router_1、Router_2、Router_3上运行IS-IS，建立IS-IS邻居关系，保证网络层相互可达。

已知Router_1、Router_2和Router_3都支持BFD功能，公司希望使用IS-IS与BFD联动技术，采用BFD控制报文方式实现当Router_1或Router_3与二层交换机之间的链路出现故障（如链路down）时，BFD能够快速感知并通告IS-IS协议。

现要求通过在Router_1和Router_3上配置IS-IS与BFD联动功能，实现：

- 监测通过L2 Switch通信的链路。
- 当链路出现故障时设备能够快速感知并通告IS-IS协议，快速切换到Router_2链路进行通信。

图 9-23 IS-IS 与 BFD 联动配置组网图



设备	接口	IP地址
Router_1	GE2/0/1	10.1.0.101/24
	GE2/0/2	10.10.0.101/24
	GE2/0/3	10.20.1.1/24
Router_2	GE2/0/1	10.10.0.102/24
	GE2/0/2	10.40.1.101/24

版权所有 © 华为技术有限公司

设备	接口	IP地址
Router_3	GE2/0/1	10.1.0.102/24
	GE2/0/2	10.40.1.102/24
	GE2/0/3	10.30.1.1/24

操作步骤

步骤1 Router_1的配置文件

```
#
 sysname Router_1
#
bfd
#
isis 1    //配置Router_1的IS-IS基本功能，并使能IS-IS的BFD功能
 is-level level-2
 bfd all-interfaces enable
 network-entity 10.0000.0000.0001.00
#
interface GigabitEthernet2/0/1
 ip address 10.1.0.101 255.255.255.0
 isis enable 1
 isis cost 5
 isis bfd enable
 isis bfd min-tx-interval 100 min-rx-interval 100    //配置发送和接收单跳BFD控制报文的最小时间间隔都为
100ms
#
interface GigabitEthernet2/0/2
 ip address 10.10.0.101 255.255.255.0
 isis enable 1
#
interface GigabitEthernet2/0/3
 ip address 10.20.1.1 255.255.255.0
#
return
```

步骤2 Router_2的配置文件

```
#
 sysname Router_2
#
bfd
#
isis 1
 is-level level-2
 bfd all-interfaces enable
 network-entity 10.0000.0000.0003.00
#
interface GigabitEthernet2/0/1
 ip address 10.10.0.102 255.255.255.0
 isis enable 1
#
interface GigabitEthernet2/0/2
 ip address 10.40.1.101 255.255.255.0
 isis enable 1
#
return
```

步骤3 Router_3的配置文件

```
#
 sysname Router_3
#
```

 版权所有 © 华为技术有限公司

```
bfd
#
isis 1
 is-level level-2
 bfd all-interfaces enable
 network-entity 10.0000.0000.0002.00
#
interface GigabitEthernet2/0/1
 ip address 10.1.0.102 255.255.255.0
 isis enable 1
 isis cost 5
 isis bfd enable
 isis bfd min-tx-interval 100 min-rx-interval 100    //配置发送和接收单跳BFD控制报文的最小时间间隔都为
100ms
#
interface GigabitEthernet2/0/2
 ip address 10.40.1.102 255.255.255.0
 isis enable 1
#
interface GigabitEthernet2/0/3
 ip address 10.30.1.1 255.255.255.0
 isis enable 1
#
return
```

步骤4 验证配置结果

在Router_1上执行**display isis peer verbose**命令查看Router_1上IS-IS邻居信息，当“State”的状态显示为“Up”时表示Router_1和Router_3已建立IS-IS邻居关系。

在Router_1和Router_3上分别执行**display isis bfd session all**，查看BFD会话，显示BFD会话已被创建，且**Session State**状态为**UP**。

在Router_1上执行**display ip routing-table 10.30.1.0 verbose** 命令查看10.30.1.0/24的路由信息，可以看出Router_1和Router_3是通过L2 Switch进行通信的。

----结束

9.7 IS-IS（IPv6）路由协议

9.7.1 配置 IS-IS IPv6 的基本功能示例

规格

适用于ARV200R002C00及更高版本、所有形态的AR路由器。

适用于所有版本、所有形态的AR路由器。

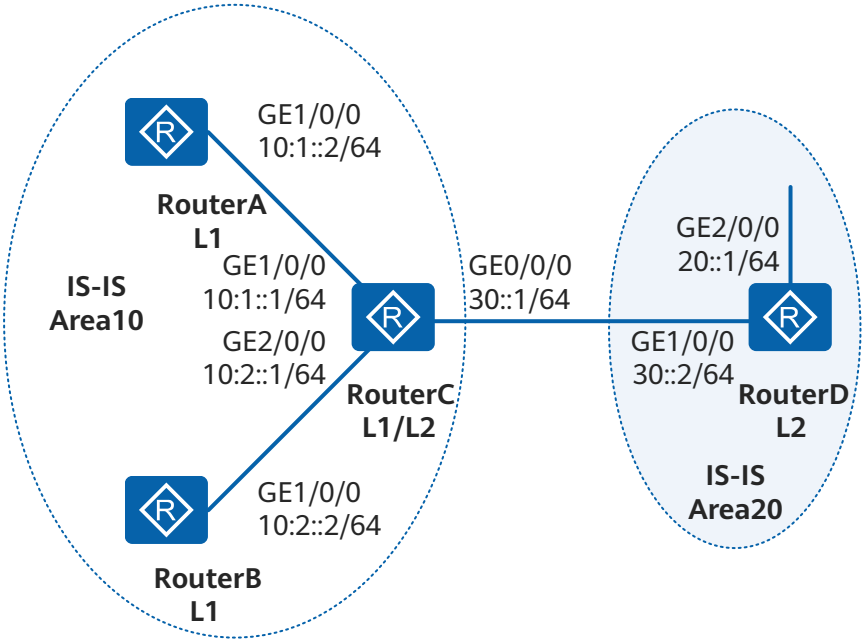
组网需求

如图9-24所示：

- RouterA、RouterB、RouterC和RouterD属于同一自治系统，要求它们之间通过IS-IS协议达到IPv6网络互连的目的。
- RouterA、RouterB和RouterC属于区域10，RouterD属于区域20。
- RouterA和RouterB是Level-1路由器，RouterC是Level-1-2路由器，RouterD是Level-2路由器。

 版权所有 © 华为技术有限公司

图 9-24 配置 IS-IS IPv6 的基本功能示例的组网图



操作步骤

步骤1 RouterA的配置

```
#
 sysname RouterA
#
 ipv6  //配置使能路由设备转发IPv6单播报文
#
isis 1  //启动IS-IS路由进程1
 is-level level-1  //设置当前路由器工作在Level-1
 network-entity 10.0000.0000.0001.00  //设置IS-IS路由进程的网络实体名称NET
 #
 ipv6 enable topology standard  //使能IS-IS进程的IPv6能力
 #
#
interface GigabitEthernet1/0/0
 ipv6 enable  //在接口下使能IPv6功能
 ipv6 address 10:1::2/64  //配置接口的全球单播IPv6地址
 isis ipv6 enable 1  //激活接口上IS-IS路由进程1的IPv6能力
#
return
```

步骤2 RouterB的配置

```
#
 sysname RouterB
#
 ipv6
#
isis 1
 is-level level-1
 network-entity 10.0000.0000.0002.00  //设置IS-IS路由进程的网络实体名称NET
 #
 ipv6 enable topology standard
 #
#
interface GigabitEthernet1/0/0
 ipv6 enable
```


版权所有 © 华为技术有限公司

```
 ipv6 address 10:2::2/64  //配置接口的全球单播IPv6地址
 isis ipv6 enable 1
#
return
```

步骤3 RouterC的配置

```
#
 sysname RouterC
#
 ipv6
#
isis 1
 network-entity 10.0000.0000.0003.00  //设置IS-IS路由进程的网络实体名称NET
 #
 ipv6 enable topology standard
 #
#
interface GigabitEthernet0/0/0
 ipv6 enable
 ipv6 address 30::1/64  //配置接口的全球单播IPv6地址
 isis ipv6 enable 1
 isis circuit-level level-2  //设置接口链路类型为Level-2，即在本接口只能建立Level-2邻接关系
#
interface GigabitEthernet1/0/0
 ipv6 enable
 ipv6 address 10:1::1/64  //配置接口的全球单播IPv6地址
 isis ipv6 enable 1
#
interface GigabitEthernet2/0/0
 ipv6 enable
 ipv6 address 10:2::1/64  //配置接口的全球单播IPv6地址
 isis ipv6 enable 1
#
return
```

步骤4 RouterD的配置

```
#
 sysname RouterD
#
 ipv6
#
isis 1
 is-level level-2  //设置当前路由器工作在Level-2
 network-entity 20.0000.0000.0004.00  //设置IS-IS路由进程的网络实体名称NET
 #
 ipv6 enable topology standard
 #
#
interface GigabitEthernet1/0/0
 ipv6 enable
 ipv6 address 30::2/64  //配置接口的全球单播IPv6地址
 isis ipv6 enable 1
#
interface GigabitEthernet2/0/0
 ipv6 enable
 ipv6 address 20::1/64  //配置接口的全球单播IPv6地址
 isis ipv6 enable 1
#
return
```

步骤5 验证配置结果

在各路由器上执行**display isis route**，可以看到对应的IS-IS路由信息。

RouterA、RouterB、RouterC、RouterD的接口互相之间可以**ping**通。

----结束

 版权所有 © 华为技术有限公司

配置注意事项

- 需要在系统视图和接口视图下使能IPv6功能。
- 需要在接口上使能接口IS-IS的IPv6能力。
- 使用命令**network-entity**设置IS-IS路由进程的网络实体名称NET时，同一个区域内的路由器设备区域ID必须相同。

9.8 BGP 路由协议

9.8.1 配置 BGP 路由协议基本功能示例

规格

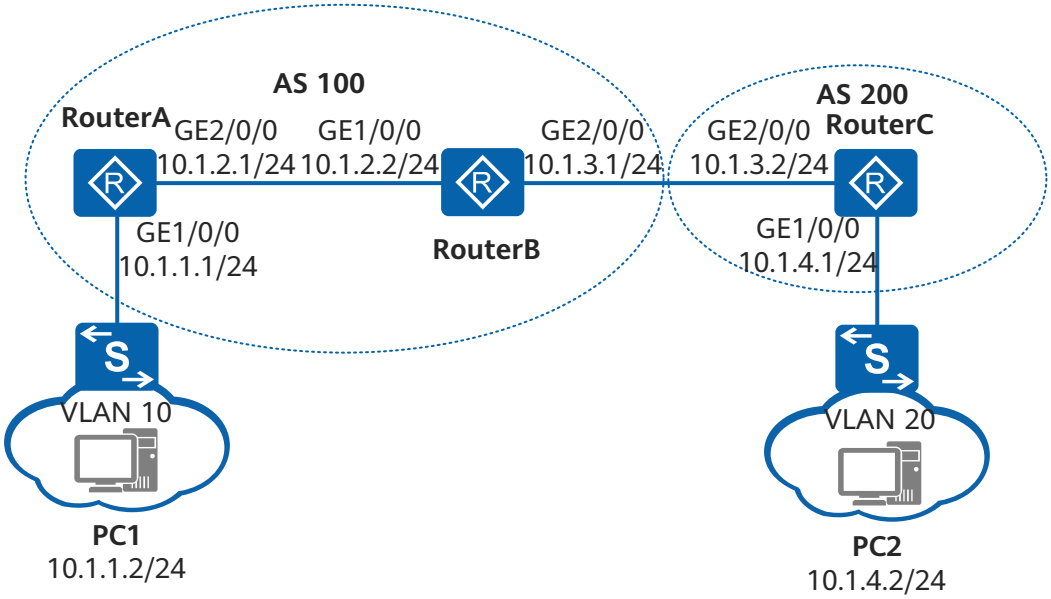
适用于所有版本、所有形态的AR路由器。

组网需求

某个地区拥有多个AS，AS之间有相互访问的需求，因此需要AS之间相互交换本AS内部的路由。由于AS内路由器数量众多，导致路由数量较大，路由变化频繁，如何高效率的在AS之间传递大量路由，并且不占用大量带宽成为一个难题。为解决上述问题，可以使用BGP协议。

路由器各接口及主机的IP地址和掩码如图9-25所示。RouterC处于AS200，RouterA和RouterB处于AS100。在这几个路由器上部署BGP协议之后，路由器之间可以相互传递路由，并且当任何一个路由器有路由更新时，只需发送路由更新信息给邻居路由器，而无须发送整个路由表，大大节约了网络带宽。

图 9-25 配置 BGP 路由协议基本功能组网图



版权所有 © 华为技术有限公司

操作步骤

步骤1 RouterA的配置

```
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 10.1.2.1 255.255.255.0
#
bgp 100 //进入BGP视图
 router-id 1.1.1.1  //配置路由管理中的Router ID
 peer 10.1.2.2 as-number 100  //指定对等体的IP地址及其所属的AS编号
 #
 ipv4-family unicast  //进入IPv4单播地址族视图
  undo synchronization
  network 10.1.1.0 24  //将本地路由表中的路由以静态方式加入到BGP路由表中，并发布给对等体
  peer 10.1.2.2 enable
#
return
```

步骤2 RouterB的配置

```
#
interface GigabitEthernet1/0/0
 ip address 10.1.2.2 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 10.1.3.1 255.255.255.0
#
bgp 100
 router-id 2.2.2.2
 peer 10.1.2.1 as-number 100
 peer 10.1.3.2 as-number 200
 #
 ipv4-family unicast
  undo synchronization
  peer 10.1.2.1 enable
  peer 10.1.2.1 next-hop-local
  peer 10.1.3.2 enable
#
return
```

步骤3 RouterC的配置

```
#
interface GigabitEthernet1/0/0
 ip address 10.1.4.1 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 10.1.3.2 255.255.255.0
#
bgp 200
 router-id 3.3.3.3
 peer 10.1.3.1 as-number 100
 #
 ipv4-family unicast
  undo synchronization
  network 10.1.4.0 24
  peer 10.1.3.1 enable
#
return
```

步骤4 配置主机

配置VLAN10内主机的缺省网关为10.1.1.1，VLAN20内主机的缺省网关为10.1.4.1。

步骤5 验证配置结果

使用**display bgp routing-table**命令查看路由器的IP路由表。

 版权所有 © 华为技术有限公司

使用**Ping**命令验证连通性。

----结束

配置注意事项

- 保证两个路由器互连接口地址配置在同一网段，并且可以正常互通。
- 在各主机上配置IPv4缺省网关。
- 执行命令**network**配置路由器发布路由，如果没有指定掩码或掩码长度，则按有类地址处理。
- 缺省情况下，同步功能是关闭的。
- 缺省情况下，BGP-IPv4单播地址族的对等体是自动使能的。

9.8.2 配置 BGP 路由反射器功能示例

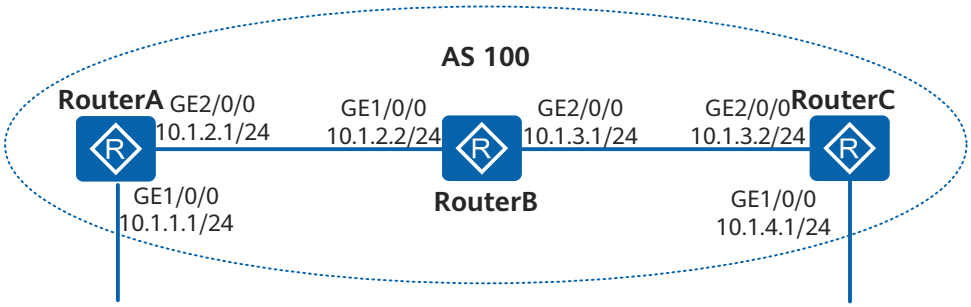
规格

适用于所有版本、所有形态的AR路由器。

组网需求

路由器各接口及主机的IP地址和掩码如图9-26所示。其中RouterB为路由反射器（RR），RouterC是它的客户机，RouterA是非客户机。RouterC与RouterA之间没有建立BGP连接，但是RouterC可以通过路由反射器RouterB学到RouterA通告的路由。

图 9-26 配置 BGP 路由反射器功能组网图



操作步骤

步骤1 RouterA的配置

```
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 10.1.2.1 255.255.255.0
#
bgp 100 //进入BGP视图
 router-id 1.1.1.1  //配置路由管理中的Router ID
 peer 10.1.2.2 as-number 100  //指定对等体的IP地址及其所属的AS编号
 #
 ipv4-family unicast  //进入IPv4单播地址族视图
```

 版权所有 © 华为技术有限公司

```
 undo synchronization
 network 10.1.1.0 24 //将本地路由表中的路由以静态方式加入到BGP路由表中，并发布给对等体
 peer 10.1.2.2 enable
#
return
```

步骤2 RouterB的配置

```
#
interface GigabitEthernet1/0/0
 ip address 10.1.2.2 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 10.1.3.1 255.255.255.0
#
bgp 100
 router-id 2.2.2.2
 peer 10.1.2.1 as-number 100
 peer 10.1.3.2 as-number 100
 #
 ipv4-family unicast
  undo synchronization
  peer 10.1.2.1 enable
  peer 10.1.3.2 enable
  peer 10.1.3.2 reflect-client //配置RR及其客户机
#
return
```

步骤3 RouterC的配置

```
#
interface GigabitEthernet1/0/0
 ip address 10.1.4.1 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 10.1.3.2 255.255.255.0
#
bgp 100
 router-id 3.3.3.3
 peer 10.1.3.1 as-number 100
 #
 ipv4-family unicast
  undo synchronization
  peer 10.1.3.1 enable
#
return
```

步骤4 验证配置结果

在RouterC上使用命令**display bgp routing-table**查看路由器的BGP路由表。从路由表中可以看到，RouterC从RouterB那里学到了RouterA通告的路由，通过显示指定路由的详细信息还可以看到该路由的Originator和Cluster_ID属性。

----结束

配置注意事项

- 保证两个路由器互连接口地址配置在同一网段，并且可以正常互通。
- 执行命令**network**配置路由器发布路由，如果没有指定掩码或掩码长度，则按有类地址处理。
- 缺省情况下，同步功能是关闭的。
- 缺省情况下，BGP-IPv4单播地址族的对等体是自动使能的。

 版权所有 © 华为技术有限公司

9.8.3 配置 BGP 路由策略应用本地优先级和团体属性功能示例

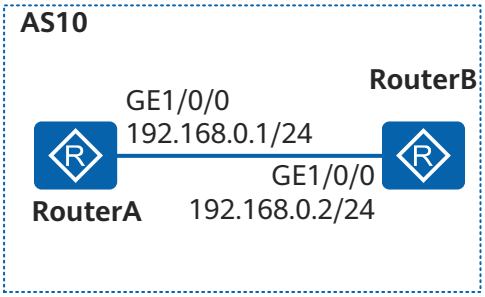
规格

适用于所有版本、所有形态的AR路由器。

组网需求

在RouterA，RouterB启用BGP路由协议，在RouterA上引入两条静态黑洞路由。要求RouterB对192.168.10.0/24范围内的路由进行修改本地优先级和团体属性添加操作。

图 9-27 配置 BGP 路由策略应用本地优先级、团体属性功能组网图



操作步骤

步骤1 RouterA的配置

```
#
 sysname RouterA
#
interface GigabitEthernet1/0/0
 ip address 192.168.0.1 255.255.255.0
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
bgp 10
 router-id 1.1.1.1  //Router ID，建议配置为LoopBack0的IP地址
 peer 192.168.0.2 as-number 10  //指定对等体的IP地址及其所属的AS编号
 #
 ipv4-family unicast
  undo synchronization
  import-route static  //配置引入静态路由
  peer 192.168.0.2 enable
#
ip route-static 192.168.10.0 255.255.255.0 NULL0  //配置静态黑洞路由
ip route-static 192.168.20.0 255.255.255.0 NULL0
#
```

步骤2 RouterB的配置

```
#
 sysname RouterB
#
acl number 2001
 rule 2 permit source 192.168.10.0 0.0.0.255  //配置在ACL 2001中增加一条规则2，允许源地址是192.168.10.0/24的报文通过。
#
interface GigabitEthernet1/0/0
 ip address 192.168.0.2 255.255.255.0
```


版权所有 © 华为技术有限公司

```
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
bgp 10
 router-id 2.2.2.2
 peer 192.168.0.1 as-number 10
 #
 ipv4-family unicast
  undo synchronization
  peer 192.168.0.1 enable
  peer 192.168.0.1 route-policy admin import  //配置对来自对等体的路由指定路由策略admin
#
route-policy admin permit node 10  //配置名为admin的路由策略，其节点号为10，匹配模式为允许
 if-match acl 2001  //配置基于acl 2001的匹配规则
 apply local-preference 120  //配置指定BGP路由的本地优先级为120
 apply community 10:1  //配置指定BGP路由的BGP团体属性为10：1
#
route-policy admin permit node 20  //配置名为admin的路由策略，其节点号为20，匹配模式为允许
#
```

步骤3 验证配置结果

在RouterB上执行命令**display bgp routing-table**，可以查看到192.168.10.0/24和192.168.20.0/24目的网段的路由信息。执行命令**display bgp routing-table 192.168.10.0 24**可以查看到192.168.10.0/24目的网段的路由的具体信息，其中本地优先级为120，团体属性为10：1。

----结束

配置注意事项

- 缺省情况下，同步功能是关闭的。
- 缺省情况下，BGP-IPv4单播地址族的对等体是自动使能的。
- 路由策略最后要添加一个空的Permit节点，否则许多没有匹配之前节点的路由就不会被添加到BGP路由表中。
- 本地优先级仅用于同一个AS域内的选路，不向域外发布这个属性，所以用于配置EBGP邻居策略时，**apply local-preference**命令的设置不生效。

9.8.4 配置 BGP 路由策略应用 AS_Path 属性功能示例

规格

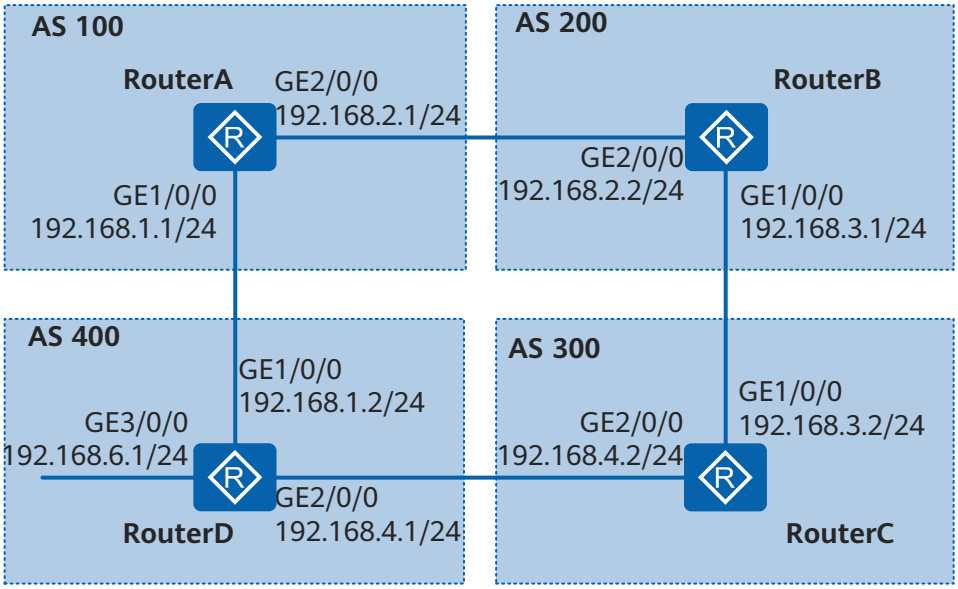
适用于所有版本、所有形态的AR路由器。

组网需求

如图9-28所示，四台路由器分别属于不同自治系统，它们之间建立EBGP连接。要求在RouterD上对RouterA发送路由时改变AS-Path属性，以改变RouterA到192.168.6.1/24的路由。

 版权所有 © 华为技术有限公司

图 9-28 配置 BGP 路由协议的 AS_Path 属性功能组网图



操作步骤

步骤1 RouterA的配置

```
#
 sysname RouterA
#
interface GigabitEthernet1/0/0
 ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 192.168.2.1 255.255.255.0
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
bgp 100
 router-id 1.1.1.1  //Router ID，建议配置为LoopBack0的IP地址
 peer 192.168.1.2 as-number 400  //指定对等体的IP地址及其所属的AS编号
 peer 192.168.2.2 as-number 200
 #
 ipv4-family unicast
  undo synchronization
  peer 192.168.1.2 enable
  peer 192.168.2.2 enable
#
```

步骤2 RouterB的配置

```
#
 sysname RouterB
#
interface GigabitEthernet1/0/0
 ip address 192.168.3.1 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 192.168.2.2 255.255.255.0
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
```


版权所有 © 华为技术有限公司

```
bgp 200
 router-id 2.2.2.2
 peer 192.168.2.1 as-number 100
 peer 192.168.3.2 as-number 300
 #
 ipv4-family unicast
  undo synchronization
  peer 192.168.2.1 enable
  peer 192.168.3.2 enable
#
```

步骤3 RouterC的配置

```
#
 sysname RouterC
#
interface GigabitEthernet1/0/0
 ip address 192.168.3.2 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 192.168.4.2 255.255.255.0
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
#
bgp 300
 router-id 3.3.3.3
 peer 192.168.3.1 as-number 200
 peer 192.168.4.1 as-number 400
 #
 ipv4-family unicast
  undo synchronization
  peer 192.168.3.1 enable
  peer 192.168.4.1 enable
#
```

步骤4 RouterD的配置

```
#
 sysname RouterD
#
interface GigabitEthernet1/0/0
 ip address 192.168.1.2 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 192.168.4.1 255.255.255.0
#
interface GigabitEthernet3/0/0
 ip address 192.168.6.1 255.255.255.0
#
interface LoopBack0
 ip address 4.4.4.4 255.255.255.255
#
bgp 400
 router-id 4.4.4.4
 peer 192.168.1.1 as-number 100
 peer 192.168.4.2 as-number 300
 #
 ipv4-family unicast
  undo synchronization
  network 192.168.6.0 255.255.255.0  //配置BGP发布本地网络路由
  peer 192.168.1.1 enable
  peer 192.168.1.1 route-policy t1 export  //对发送到对等体的路由应用路由策略
  peer 192.168.4.2 enable
#
route-policy t1 permit node 5  //创建路由策略
 apply as-path 400 400 400 additive  //在原有的AS-Path属性列表中追加AS号400 400 400
#
```

步骤5 验证配置结果

 版权所有 © 华为技术有限公司

在RouterD上应用路由策略之前，在RouterA上执行命令**display bgp routing-table**查看到网段192.168.6.0/24的两条BGP路由，其中下一跳为192.168.2.2的路由AS路径属性为200 300 400，而下一跳为192.168.1.2的路由AS路径属性为400。然后执行命令**display ip routing-table**可以看到经过AS少的路由，即下一跳为192.168.1.2的路由被优选。

在RouterD上应用路由策略之后，在RouterA上执行命令**display bgp routing-table**查看到网段192.168.6.0/24的两条BGP路由，其中下一跳为192.168.2.2的路由的AS路径属性还为200 300 400，但下一跳为192.168.1.2的路由AS路径属性则变为400 400 400 400。然后执行命令**display ip routing-table**可以看到经过AS少的路由，即下一跳为192.168.2.2的路由被优选。

----结束

配置注意事项

- 执行命令**network**配置路由器发布路由，如果没有指定掩码或掩码长度，则按有类地址处理。
- 缺省情况下，同步功能是关闭的。
- 缺省情况下，BGP-IPv4单播地址族的对等体是自动使能的。

9.8.5 配置 BGP4+路由反射器功能示例

规格

适用于ARV200R002C00及更高版本、所有形态的AR路由器。

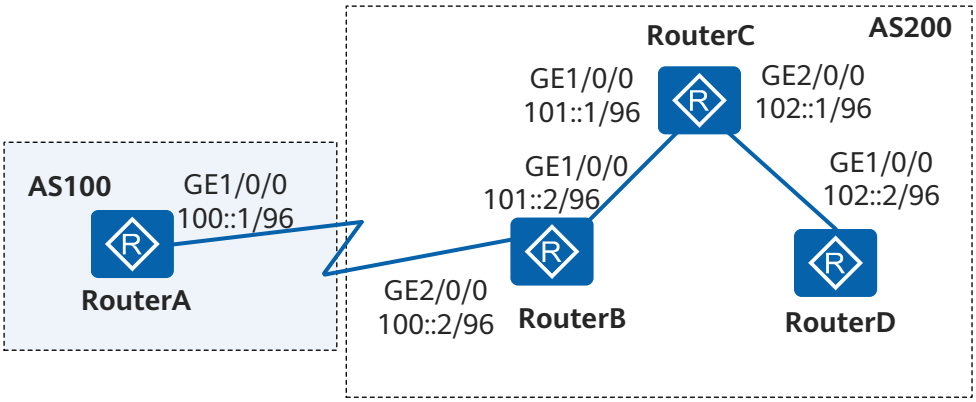
适用于所有版本、所有形态的AR路由器。

组网需求

如图9-29所示，RouterB接收了一个经过EBGP的更新报文并将之传给RouterC。RouterC被配置为路由反射器，它有两个客户机：RouterB和RouterD。

RouterB和RouterD间不需要建立IBGP连接，当RouterC接收了来自RouterB的路由更新时，它将此信息反射给RouterD；反之，接收到的RouterD的路由信息也会被反射给RouterB。

图 9-29 配置 BGP4+路由反射器功能组网图



 版权所有 © 华为技术有限公司

操作步骤

步骤1 RouterA的配置

```
#
ipv6  //使能路由器IPv6报文转发能力
#
interface GigabitEthernet1/0/0
 ipv6 enable  //配置在接口上使能IPv6功能
 ipv6 address 100::1 96
#
bgp 100 //进入BGP视图
 router-id 1.1.1.1  //配置路由管理中的Router ID
 peer 100::2 as-number 200  //指定对等体的IPv6地址及其所属的AS编号
 #
 ipv6-family unicast  //进入IPv6单播地址族视图
  undo synchronization
  network 100:: 96  //将本地路由表中的路由以静态方式加入到BGP路由表中，并发布给对等体
  peer 100::2 enable  //使能与指定对等体之间交换相关的路由信息
#
return
```

步骤2 RouterB的配置

```
#
ipv6
#
interface GigabitEthernet1/0/0
 ipv6 enable
 ipv6 address 101::2 96
#
interface GigabitEthernet2/0/0
 ipv6 enable
 ipv6 address 100::2 96
#
bgp 200
 router-id 2.2.2.2
 peer 100::1 as-number 100
 peer 101::1 as-number 200
 #
 ipv6-family unicast
  undo synchronization
  network 100:: 96
  network 101:: 96
  peer 100::1 enable
  peer 101::1 enable
#
return
```

步骤3 RouterC的配置

```
#
ipv6
#
interface GigabitEthernet1/0/0
 ipv6 enable
 ipv6 address 101::1 96
#
interface GigabitEthernet2/0/0
 ipv6 enable
 ipv6 address 102::1 96
#
bgp 200
 router-id 3.3.3.3
 peer 101::2 as-number 200
 peer 102::2 as-number 200
 #
 ipv6-family unicast
  undo synchronization
  network 101:: 96
  network 102:: 96
```

 版权所有 © 华为技术有限公司

```
 peer 101::2 enable
 peer 101::2 reflect-client //配置RouterC作为路由反射器，RouterB作为客户机
 peer 102::2 enable
 peer 102::2 reflect-client
#
return
```

步骤4 RouterD的配置

```
#
ipv6
#
interface GigabitEthernet1/0/0
 ipv6 enable
 ipv6 address 102::2 96
#
bgp 200
 router-id 4.4.4.4
 peer 102::1 as-number 200
 #
 ipv6-family unicast
  undo synchronization
  network 102:: 96
  peer 102::1 enable
#
return
```

步骤5 验证配置结果

在RouterD上使用**display bgp ipv6 routing-table**命令查看路由器的IPv6 BGP路由表。从路由表中可以看到，RouterD从RouterC那里学到了RouterA通告的路由。

----结束

配置注意事项

- 保证两个路由器互连接口地址配置在同一网段，并且可以正常互通。
- 执行命令**network**配置路由器发布路由，如果没有指定掩码或掩码长度，则按有类地址处理。
- 缺省情况下，同步功能是关闭的。
- 在BGP视图下配置BGP4+对等体之后，还需要在IPv6单播地址族视图使能该对等体。

9.8.6 配置 BGP4+负载分担功能示例

规格

适用于ARV200R002C00及更高版本、所有形态的AR路由器。

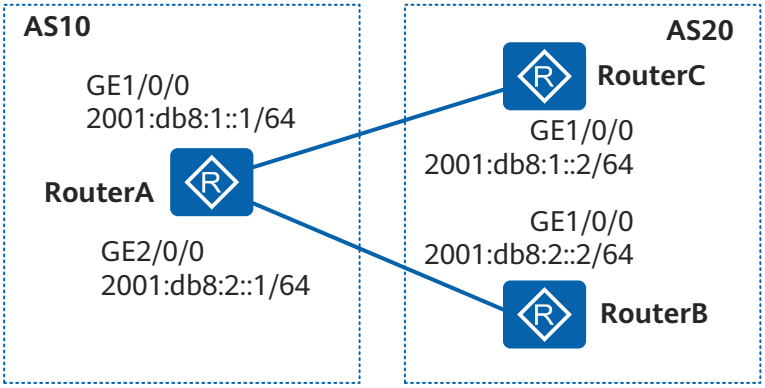
适用于所有版本、所有形态的AR路由器。

组网需求

RouterA与RouterB、RouterC建立EBGP连接。分别在RouterB、RouterC中引入到2001:db8::/64的静态路由。要求RouterB和RouterC实现负载分担。

 版权所有 © 华为技术有限公司

图 9-30 配置 BGP4+负载分担功能组网图



操作步骤

步骤1 RouterA的配置

```
#
 sysname RouterA
#
ipv6  ////配置使能路由设备转发IPv6单播报文
#
interface GigabitEthernet1/0/0
 ipv6 enable  //在接口下使能IPv6功能
 ipv6 address 2001:db8:1::1/64
#
interface GigabitEthernet2/0/0
 ipv6 enable
 ipv6 address 2001:db8:2::1/64
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
bgp 10
 router-id 1.1.1.1  //Router ID，建议配置为LoopBack0的IP地址
 peer 2001:db8:1::2 as-number 20  //指定对等体的IP地址及其所属的AS编号
 peer 2001:db8:2::2 as-number 20
 #
 ipv6-family unicast
  undo synchronization
  maximum load-balancing 2  //配置等价路由的最大条数为2
  peer 2001:db8:1::2 enable  //使能与指定对等体之间交换相关的路由信息
  peer 2001:db8:2::2 enable
#
```

步骤2 RouterB的配置

```
#
 sysname RouterB
#
ipv6
#
interface GigabitEthernet1/0/0
 ipv6 enable
 ipv6 address 2001:db8:2::2/64
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
bgp 20
 router-id 2.2.2.2
```


版权所有 © 华为技术有限公司

```
 peer 2001:db8:2::1 as-number 10
 #
 ipv6-family unicast
  undo synchronization
  import-route static  //配置引入IPv6静态路由
  peer 2001:db8:2::1 enable
#
ipv6 route-static 2001:db8:: 64 NULL0  //配置IPv6静态路由
#
```

步骤3 RouterC的配置

```
#
 sysname RouterC
#
ipv6
#
interface GigabitEthernet1/0/0
 ipv6 enable
 ipv6 address 2001:db8:1::2/64
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
#
bgp 20
 router-id 3.3.3.3
 peer 2001:db8:1::1 as-number 10
 #
 ipv6-family unicast
  undo synchronization
  import-route static
  peer 2001:db8:1::1 enable
#
ipv6 route-static 2001:db8:: 64 NULL0  //配置IPv6静态路由
#
```

步骤4 验证配置结果

在RouterA上执行命令**display bgp ipv6 routing-table**，可以查看到网络地址为2001:db8::/64有两条路由，下一跳地址分别为2001:db8:1::2和2001:db8:2::2。

----结束

配置注意事项

- 在BGP视图下配置BGP4+对等体之后，还需要在IPv6单播地址族视图使能该对等体。
- 配置IPv6路由协议前，一定要先使能路由设备转发IPv6单播报文。在接口下配置关于IPv6特性的命令前必须先在接口上使能IPv6功能。

9.8.7 配置 BGP4+路由协议联盟功能示例

规格

适用于ARV200R002C00及更高版本、所有形态的AR路由器。

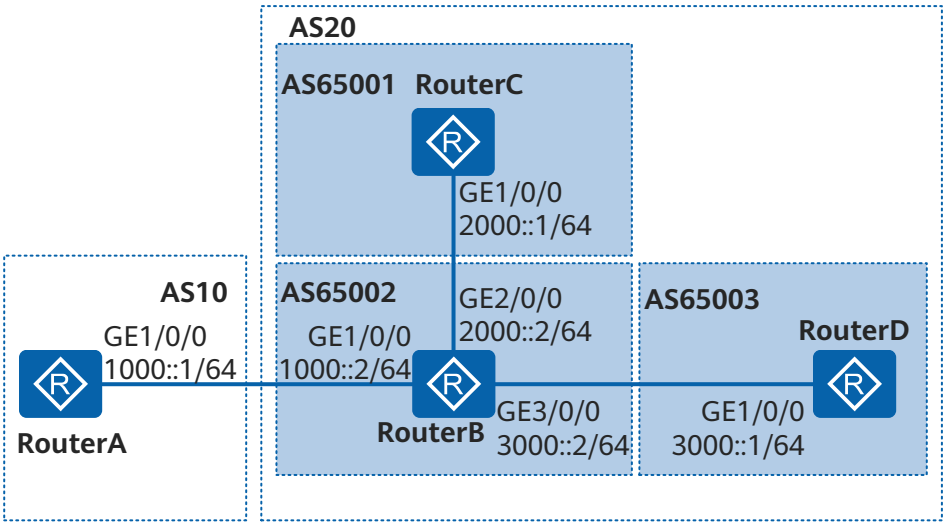
适用于所有版本、所有形态的AR路由器。

组网需求

如图9-31所示，将自治系统AS20划分为3个子自治系统AS65001，AS65002，AS65003，配置EBGP和IBGP。使各自治系统可以互通。

 版权所有 © 华为技术有限公司

图 9-31 配置 BGP4+路由协议联盟功能组网图



操作步骤

步骤1 RouterA的配置

```
#
 sysname RouterA
#
ipv6  //配置使能路由设备转发IPv6单播报文
#
interface GigabitEthernet1/0/0
 ipv6 enable  //在接口下使能IPv6功能
 ipv6 address 1000::1/64
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
bgp 10
 router-id 1.1.1.1  //Router ID，建议配置为LoopBack0的IP地址
 peer 1000::2 as-number 20  //指定对等体的IP地址及其所属的AS编号
 #
 ipv6-family unicast
  undo synchronization
  peer 1000::2 enable  //使能与指定对等体之间交换相关的路由信息
#
```

步骤2 RouterB的配置

```
#
 sysname RouterB
#
ipv6
#
interface GigabitEthernet1/0/0
 ipv6 enable
 ipv6 address 1000::2/64
#
interface GigabitEthernet2/0/0
 ipv6 enable
 ipv6 address 2000::2/64
#
interface GigabitEthernet3/0/0
 ipv6 enable
 ipv6 address 3000::2/64
#
```


版权所有 © 华为技术有限公司

```
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
bgp 65002
 router-id 2.2.2.2
 confederation id 20  //配置联盟ID为20
 confederation peer-as 65001 65003  //配置与本地AS连接的联盟内其他对等体的子自治系统号
 peer 1000::1 as-number 10
 peer 2000::1 as-number 65001
 peer 3000::1 as-number 65003
 #
 ipv6-family unicast
  undo synchronization
  import-route direct  //配置引入直连路由
  peer 1000::1 enable
  peer 2000::1 enable
  peer 3000::1 enable
#
```

步骤3 RouterC的配置

```
#
 sysname RouterC
#
ipv6
#
interface GigabitEthernet1/0/0
 ipv6 enable
 ipv6 address 2000::1/64
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
#
bgp 65001
 router-id 3.3.3.3
 confederation id 20
 confederation peer-as 65002
 peer 2000::2 as-number 65002
 #
 ipv6-family unicast
  undo synchronization
  peer 2000::2 enable
#
```

步骤4 RouterD的配置

```
#
 sysname RouterD
#
ipv6
#
interface GigabitEthernet1/0/0
 ipv6 enable
 ipv6 address 3000::1/64
#
interface LoopBack0
 ip address 4.4.4.4 255.255.255.255
#
bgp 65003
 router-id 4.4.4.4
 confederation id 20
 confederation peer-as 65002
 peer 3000::2 as-number 65002
 #
 ipv6-family unicast
  undo synchronization
  peer 3000::2 enable
#
```

步骤5 验证配置结果

 版权所有 © 华为技术有限公司

在RouterD上执行命令**ping ipv6 2000::1**，可以成功与RouterC互通。在RouterD上执行命令**ping ipv6 1000::1**，可以成功与RouterA互通。

----结束

配置注意事项

- 配置IPv6路由协议前，一定要先使能路由设备转发IPv6单播报文。在接口下配置关于IPv6特性的命令前必须先在接口上使能IPv6功能。
- 在BGP视图下配置BGP4+对等体之后，还需要在IPv6单播地址族视图使能该对等体。
- 由于RouterB只发布自己本地路由表中已有的路由，所以要在RouterB的BGP4+路由协议中引入直连路由，否则RouterA，RouterC，RouterD之间不能互通。

9.8.8 配置 BGP 路由协议与 BFD 联动示例

规格

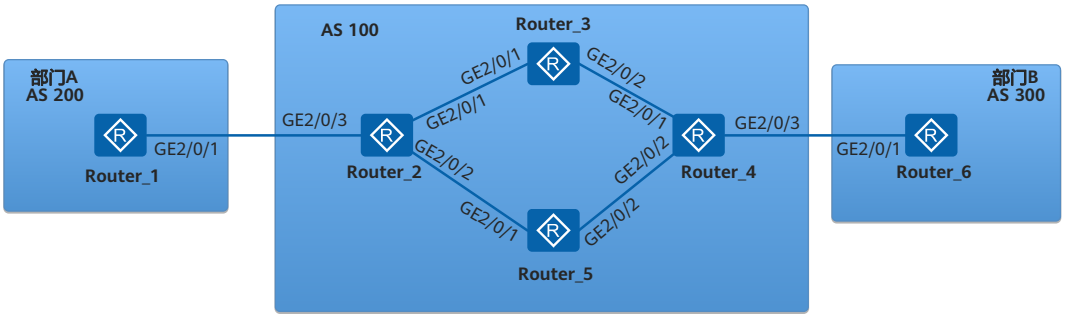
适用于所有版本、所有形态的AR路由器。

组网需求

如图9-32所示，某公司的部门A和部门B相距较远，Router_1和Router_6分别作为这两个部门的出口设备，现通过部署BGP，使两个部门可以进行业务通信。已知Router_2和Router_4都支持BFD功能，公司希望使用BGP与BFD联动技术，采用BFD控制报文方式检测AS 200与AS 300之间通信的主链路状态，实现当Router_2与Router_4之间的链路出现故障（如链路down）时，BFD能够快速感知并通告BGP协议。具体要求如下：

- 在AS 100内使用OSPF作为IGP。
- 配置Router_2 <-> Router_3 <-> Router_4链路作为主链路，负责转发Router_1和Router_6之间的流量，并采用BFD控制报文的方式检测主链路。

图 9-32 BGP 与 BFD 联动配置组网图



设备	接口	IP地址	设备	接口	IP地址
Router_1	GE2/0/1	10.20.0.1/24	Router_4	GE2/0/1	10.2.0.101/24
Router_2	GE2/0/1	10.1.0.101/24		GE2/0/2	10.40.1.101/24

 版权所有 © 华为技术有限公司

设备	接口	IP地址	设备	接口	IP地址
	GE2/0/2	10.30.0.101/24		GE2/0/3	10.50.0.2/24
	GE2/0/3	10.20.0.2/24	Router_5	GE2/0/1	10.30.0.102/24
Router_3	GE2/0/1	10.1.0.102/24		GE2/0/2	10.40.1.102/24
	GE2/0/2	10.2.0.102/24	Router_6	GE2/0/1	10.50.0.1/24

操作步骤

步骤1 Router_1的配置文件

```
#
 sysname Router_1
#
interface GigabitEthernet2/0/1
 ip address 10.20.0.1 255.255.255.0
#
bgp 200    //启动BGP，指定本地AS号为200
 router-id 1.1.1.1
 peer 10.20.0.2 as-number 100    //配置Router_1和Router_2建立EBGP连接
 #
 ipv4-family unicast
  undo synchronization
  network 10.20.0.0 255.255.255.0
  peer 10.20.0.2 enable
#
return
```

步骤2 Router_2的配置文件

```
#
 sysname Router_2
#
bfd
#
acl number 2000
 rule 0 permit source 10.20.0.0 0.0.0.255
#
interface GigabitEthernet2/0/1
 ip address 10.1.0.101 255.255.255.0
#
interface GigabitEthernet2/0/2
 ip address 10.30.0.101 255.255.255.0
#
interface GigabitEthernet2/0/3
 ip address 10.20.0.2 255.255.255.0
#
bgp 100    //启动BGP，指定本地AS号为100
 router-id 2.2.2.2
 peer 10.2.0.101 as-number 100
 peer 10.2.0.101 bfd enable
 peer 10.20.0.1 as-number 200    //配置Router_2和Router_1建立EBGP连接
 peer 10.40.1.101 as-number 100    //配置Router_2和Router_4建立IBGP连接
#
 ipv4-family unicast
  undo synchronization
  preference 255 100 130
```

 版权所有 © 华为技术有限公司

```
 import-route ospf 1
 peer 10.2.0.101 enable
 peer 10.2.0.101 route-policy local-pre export
 peer 10.2.0.101 next-hop-local
 peer 10.20.0.1 enable
 peer 10.40.1.101 enable
 peer 10.40.1.101 next-hop-local
#
ospf 1    //在AS 100内配置OSPF功能，保证设备间路由可达
import-route bgp
 area 0.0.0.0
  network 10.1.0.0 0.0.0.255
  network 10.30.0.0 0.0.0.255
#
route-policy local-pre permit node 10    // 配置向对等体10.2.0.101发布的路由设置本地优先级为200
 if-match ip route-source acl 2000
 apply local-preference 200
#
return
```

步骤3 Router_3的配置文件

```
#
 sysname Router_3
#
interface GigabitEthernet2/0/1
 ip address 10.1.0.102 255.255.255.0
#
interface GigabitEthernet2/0/2
 ip address 10.2.0.102 255.255.255.0
#
ospf 1    //在AS 100内配置OSPF功能，保证设备间路由可达
 area 0.0.0.0
  network 10.1.0.0 0.0.0.255
  network 10.2.0.0 0.0.0.255
#
return
```

步骤4 Router_4的配置文件

```
#
 sysname Router_4
#
bfd
#
acl number 2000    //创建ACL2000，允许源IP地址为10.50.0.0/24的报文通过
 rule 0 permit source 10.50.0.0 0.0.0.255
#
interface GigabitEthernet2/0/1
 ip address 10.2.0.101 255.255.255.0
#
interface GigabitEthernet2/0/2
 ip address 10.40.1.101 255.255.255.0
#
interface GigabitEthernet2/0/3
 ip address 10.50.0.2 255.255.255.0
#
bgp 100    //启动BGP，指定本地AS号为100
 router-id 4.4.4.4
 peer 10.1.0.101 as-number 100    //配置Router_4和Router_2建立IBGP连接
 peer 10.1.0.101 bfd min-tx-interval 100 min-rx-interval 100
 peer 10.1.0.101 bfd enable    //配置BFD功能
 peer 10.30.0.101 as-number 100
 peer 10.50.0.1 as-number 300    //配置Router_4和Router_6建立EBGP连接
 peer 10.50.0.1 ebgp-max-hop 255
 #
 ipv4-family unicast
  undo synchronization
  preference 255 100 130
  peer 10.1.0.101 enable
  peer 10.1.0.101 route-policy local-pre export
```

 版权所有 © 华为技术有限公司

```
 peer 10.1.0.101 next-hop-local    //在BGP IPv4单播地址族视图下，配置向对等体10.1.0.101发布BGP路由时，将下一跳属性修改为自身的地址
 peer 10.30.0.101 enable
 peer 10.30.0.101 next-hop-local    //在BGP IPv4单播地址族视图下，配置向对等体10.30.0.101发布BGP路由时，将下一跳属性修改为自身的地址
 peer 10.50.0.1 enable
#
ospf 1    //在AS 100内配置OSPF功能，保证设备间路由可达
 import-route direct
 area 0.0.0.0
  network 10.2.0.0 0.0.0.255
  network 10.40.1.0 0.0.0.255
#
route-policy local-pre permit node 10    //配置向对等体10.1.0.101发布的路由设置本地优先级为200
 if-match ip route-source acl 2000
 apply local-preference 200
#
return
```

步骤5 Router_5的配置文件

```
#
 sysname Router_5
#
interface GigabitEthernet2/0/1
 ip address 10.30.0.102 255.255.255.0
#
interface GigabitEthernet2/0/2
 ip address 10.40.1.102 255.255.255.0
#
ospf 1    //在AS 100内配置OSPF功能，保证设备间路由可达
 area 0.0.0.0
  network 10.30.0.0 0.0.0.255
  network 10.40.1.0 0.0.0.255
#
return
```

步骤6 Router_6的配置文件

```
#
 sysname Router_6
#
interface GigabitEthernet2/0/1
 ip address 10.50.0.1 255.255.255.0
#
bgp 300    //启动BGP，指定本地AS号为300
 router-id 6.6.6.6
 peer 10.50.0.2 as-number 100    //配置Router_6和Router_4建立EBGP连接
 peer 10.50.0.2 ebgp-max-hop 255
 #
 ipv4-family unicast
  undo synchronization
  network 10.50.0.0 255.255.255.0
  peer 10.50.0.2 enable
#
return
```

步骤7 验证配置结果

在Router_1上执行**Ping**命令检查Router_1到Router_6的路由可达。

在Router_2上通过命令**display bgp peer**查看BGP对等体信息，可以看到Router_2与Router_4建立IBGP连接，Router_2与Router_1建立EBGP连接，且均处于Established状态。

在Router_2上执行命令**display bgp bfd session all**查看BFD会话信息，显示BFD会话已被创建，且**Session State**状态为**Up**。

 版权所有 © 华为技术有限公司

在Router_2上执行命令**display ip routing-table**查看10.50.0.0/24的路由信息，可以看出Router_2通过Router_2 <-> Router_3 <-> Router_4这条路径与10.50.0.0/24网段通信。

----结束

9.9 策略路由

9.9.1 配置接口策略路由的基本功能示例

规格

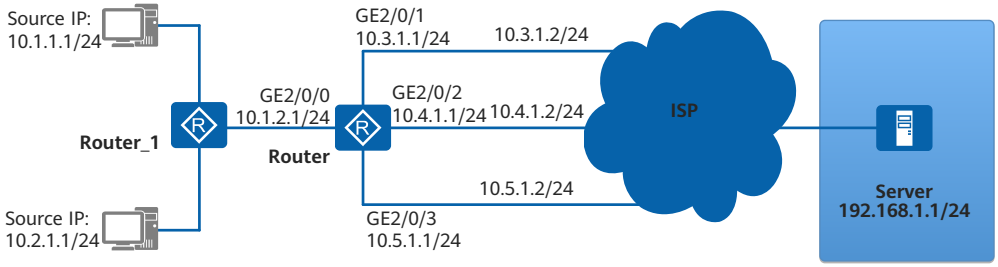
适用于所有版本、所有形态的AR路由器。

组网需求

如图9-33所示，缺省情况下，Router的接口GE2/0/0上收到的所有访问Server的报文根据路由表转发的下一跳均为10.4.1.2。现要求在Router上配置接口策略路由，对于访问Server的报文实现如下要求：

- 匹配接口GE2/0/0上收到的源IP地址为10.2.1.1的报文，将该报文的下一跳重定向到10.5.1.2，此接口的流策略调用优先级较高。
- 匹配接口GE2/0/0上收到的HTTP报文，将该报文的下一跳重定向到10.3.1.2。

图 9-33 接口策略路由典型功能组网图



操作步骤

步骤1 Router的配置

```
#
 sysname Router
#
acl number 3005    //定义访问控制列表ACL3005，用于匹配源IP地址为10.2.1.1的报文
 rule 0 permit ip source 10.2.1.1 0
#
acl number 3006    //定义访问控制列表ACL3006，用于匹配HTTP报文
 rule 0 permit tcp destination-port eq www
#
traffic classifier 10.2.1.1 operator or
 if-match acl 3005
traffic classifier www operator or
 if-match acl 3006
#
```


版权所有 © 华为技术有限公司

```
traffic behavior 10.2.1.1
 redirect ip-nexthop 10.5.1.2
traffic behavior www
  redirect ip-nexthop 10.3.1.2
#
Traffic policy pbr
  Classifier 10.2.1.1 behavior 10.2.1.1 precedence 5
  Classifier www behavior www precedence 10
#
interface GigabitEthernet2/0/0    //配置接口的IP地址
 ip address 10.1.2.1 255.255.255.0
 traffic-policy pbr inbound
#
interface GigabitEthernet2/0/1
 ip address 10.3.1.1 255.255.255.0
#
interface GigabitEthernet2/0/2
 ip address 10.4.1.1 255.255.255.0
#
interface GigabitEthernet2/0/3
 ip address 10.5.1.1 255.255.255.0
#
ip route-static 192.168.1.0 24 10.3.1.2    //配置静态路由，保证三条路径都可达，并且缺省下一跳为10.4.1.2
ip route-static 192.168.1.0 24 10.4.1.2 preference 40
ip route-static 192.168.1.0 24 10.5.1.2
#
return
```

步骤2 验证配置结果

通过**display traffic classifier user-defined** [*classifier-name*]命令查看已配置的流分类信息。

通过**display traffic behavior** { **system-defined** | **user-defined** } [*behavior-name*]命令查看已配置的流行为信息。

通过**display traffic policy user-defined** [*policy-name* [**classifier** *classifier-name*]]命令查看流策略的配置信息。

通过**display traffic-policy applied-record** [*policy-name*]命令查看指定流策略的应用记录。

----结束

9.9.2 配置策略路由示例

规格

适用于所有版本、所有形态的AR路由器。

组网需求

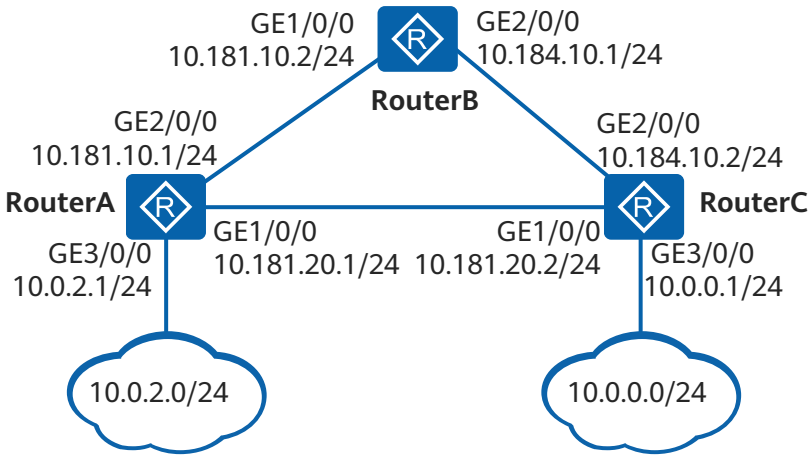
企业用户希望根据用户实际需求制定策略进行路由选择，使不同的数据流通过不同的链路进行发送，增强路由选择的灵活性和可控性，提高链路的利用效率和降低企业成本。为实现上述需求，可以使用策略路由。

如图9-34所示，RouterA、RouterB和RouterC使用OSPF保证全网路由可达，并且在RouterA上察看路由表可以发现到10.0.0.0的下一跳为RouterC的GE1/0/0接口地址。

在RouterA的上应用策略路由，使从10.0.2.0/24到10.0.0.0/24的流量重定向到RouterB上。

 版权所有 © 华为技术有限公司

图 9-34 配置策略路由示例



操作步骤

步骤1 配置RouterA

```
#
acl number 3001    //定义ACL匹配目的源地址是10.0.2.0/24，目的地址是10.0.0.0/24
 rule 5 permit ip source 10.0.2.0 0.0.0.255 destination 10.0.0.0 0.0.0.255
#
traffic classifier rdt operator or  //定义需要重定向的数据流分类
 if-match acl 3001
#
traffic behavior rdt  //定义流行为为重定向到RouterB的GE1/0/0的接口地址
 redirect ip-nexthop 10.181.10.2
#
traffic policy rdt  //绑定流策略
 classifier rdt behavior rdt precedence 5
#
interface GigabitEthernet 1/0/0
 ip address 10.181.20.1 255.255.255.0
#
interface GigabitEthernet 2/0/0
 ip address 10.181.10.1 255.255.255.0
#
interface GigabitEthernet 3/0/0
 ip address 10.0.2.1 255.255.255.0
 traffic-policy rdt inbound  //从10.0.2.0/24到10.0.0.0/24的流量重定向到RouterB上
#
ospf 1    //配置OSPF路由协议
 area 0.0.0.0
  network 10.0.2.0 0.0.0.255
  network 10.181.20.0 0.0.0.255
  network 10.181.10.0 0.0.0.255
#
return
```

步骤2 配置RouterB

```
#
interface GigabitEthernet 1/0/0
 ip address 10.181.10.2 255.255.255.0
#
interface GigabitEthernet 2/0/0
 ip address 10.184.10.1 255.255.255.0
#
ospf 1    //配置OSPF路由协议
```


版权所有 © 华为技术有限公司

```
 area 0.0.0.0
  network 10.181.10.0 0.0.0.255
  network 10.184.10.0 0.0.0.255
#
return
```

步骤3 配置RouterC

```
#
interface GigabitEthernet 1/0/0
 ip address 10.181.20.2 255.255.255.0
#
interface GigabitEthernet 2/0/0
 ip address 10.184.10.2 255.255.255.0
#
ospf 1        //配置OSPF路由协议
 area 0.0.0.0
  network 10.184.10.0 0.0.0.255
  network 10.181.20.0 0.0.0.255
  network 10.0.0.0 0.0.0.255
#
return
```

步骤4 验证配置结果

在10.0.2.0/24网段的主机上执行**tracert**命令，检测从10.0.2.0/24到10.0.0.0/24的路径。发现从10.0.2.0/24到10.0.0.0/24的流量重定向到RouterB上。

----结束

9.10 路由策略

9.10.1 配置路由策略基本功能示例

规格

适用于所有版本、所有形态的AR路由器。

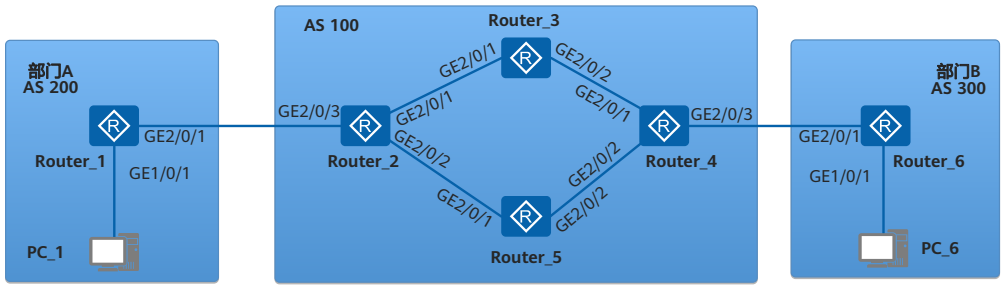
组网需求

如图9-35所示，某公司的部门A和部门B相距较远，Router_1和Router_6分别作为这两个部门的出口设备，AS 100内部使用OSPF作为IGP。现要求：

- 通过部署BGP，使部门A和部门B可以通信。
- 通过配置路由策略，将Router_2 <-> Router_3 <-> Router_4链路作为主链路，负责转发Router_1和Router_6之间的流量；当主链路断开时，自动切换到Router_2 <-> Router_5 <-> Router_4这条路径进行通信。

 版权所有 © 华为技术有限公司

图 9-35 配置路由策略基本功能组网图



设备	接口	IP地址	设备	接口	IP地址
Router_1	GE1/0/1	10.10.0.1/24	Router_4	GE2/0/1	10.2.0.101/24
	GE2/0/1	10.20.0.1/24		GE2/0/2	10.40.1.101/24
Router_2	GE2/0/1	10.1.0.101/24		GE2/0/3	10.50.0.2/24
	GE2/0/2	10.30.0.101/24	Router_5	GE2/0/1	10.30.0.102/24
	GE2/0/3	10.20.0.2/24		GE2/0/2	10.40.1.102/24
Router_3	GE2/0/1	10.1.0.102/24	Router_6	GE1/0/1	10.60.0.1/24
	GE2/0/2	10.2.0.102/24		GE2/0/1	10.50.0.1/24

操作步骤

步骤1 Router_1的配置

```
#
 sysname Router_1
#
interface GigabitEthernet1/0/1
 ip address 10.10.0.1 255.255.255.0
#
interface GigabitEthernet2/0/1
 ip address 10.20.0.1 255.255.255.0
#
bgp 200    //启动BGP，指定本地AS号为200，指定BGP路由器的Router ID为1.1.1.1
 router-id 1.1.1.1
 peer 10.20.0.2 as-number 100    //配置Router_1和Router_2建立EBGP连接
 #
 ipv4-family unicast
  undo synchronization
  network 10.10.0.0 255.255.255.0    //在BGP IPv4单播地址族视图下，将本地路由表中到达10.10.0.0/24网段的路由添加到BGP路由表中
  peer 10.20.0.2 enable
```


版权所有 © 华为技术有限公司

```
#
return
```

步骤2 Router_2的配置

```
#
 sysname Router_2
#
acl number 2000    //创建ACL 2000，允许源IP地址为10.20.0.0/24的报文通过
 rule 0 permit source 10.20.0.0 0.0.0.255
#
interface GigabitEthernet2/0/1
 ip address 10.1.0.101 255.255.255.0
#
interface GigabitEthernet2/0/2
 ip address 10.30.0.101 255.255.255.0
#
interface GigabitEthernet2/0/3
 ip address 10.20.0.2 255.255.255.0
#
bgp 100    //启动BGP，指定本地AS号为100，指定BGP路由器的Router ID为2.2.2.2
 router-id 2.2.2.2
 peer 10.2.0.101 as-number 100    //配置Router_2和Router_4建立IBGP连接
 peer 10.40.1.101 as-number 100
 peer 10.20.0.1 as-number 200    //配置Router_2和Router_1建立EBGP连接
#
 ipv4-family unicast
  undo synchronization
  preference 255 100 130    //配置EBGP路由优先级为255，配置IBGP路由优先级为100，配置本地路由优先级为130，使IBGP路由优先级优于OSPF路由
  peer 10.2.0.101 enable
  peer 10.2.0.101 route-policy local-pre export    //指定向对等体10.2.0.101发布的路由策略为local-pre
  peer 10.2.0.101 next-hop-local    //在BGP IPv4单播地址族视图下，配置向对等体10.2.0.101发布BGP路由时，将下一跳属性修改为自身的地址
  peer 10.20.0.1 enable
  peer 10.40.1.101 enable
  peer 10.40.1.101 next-hop-local    //在BGP IPv4单播地址族视图下，配置向对等体10.40.1.101发布BGP路由时，将下一跳属性修改为自身的地址
#
ospf 1
 import-route direct
 import-route bgp
 area 0.0.0.0
  network 10.1.0.0 0.0.0.255
  network 10.30.0.0 0.0.0.255
#
route-policy local-pre permit node 10    //配置路由策略，将从对等体10.20.0.1学习到的路由发布给对等体10.2.0.101时，设置本地优先级为200
 if-match ip route-source acl 2000
 apply local-preference 200
#
return
```

步骤3 Router_3的配置

```
#
 sysname Router_3
#
interface GigabitEthernet2/0/1
 ip address 10.1.0.102 255.255.255.0
#
interface GigabitEthernet2/0/2
 ip address 10.2.0.102 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.1.0.0 0.0.0.255
  network 10.2.0.0 0.0.0.255
#
return
```

 版权所有 © 华为技术有限公司

步骤4 Router_4的配置

```
#
 sysname Router_4
#
acl number 2000    //创建ACL 2000，允许源IP地址为10.50.0.0/24的报文通过
 rule 0 permit source 10.50.0.0 0.0.0.255
#
interface GigabitEthernet2/0/1
 ip address 10.2.0.101 255.255.255.0
#
interface GigabitEthernet2/0/2
 ip address 10.40.1.101 255.255.255.0
#
interface GigabitEthernet2/0/3
 ip address 10.50.0.2 255.255.255.0
#
bgp 100    //启动BGP，指定本地AS号为100，指定BGP路由器的Router ID为4.4.4.4
 router-id 4.4.4.4
 peer 10.1.0.101 as-number 100    //配置Router_4和Router_2建立IBGP连接
 peer 10.50.0.1 as-number 300    //配置Router_4和Router_6建立EBGP连接
 peer 10.30.0.101 as-number 100    //配置Router_4和Router_2建立IBGP连接
 #
 ipv4-family unicast
  undo synchronization
  preference 255 100 130    //配置EBGP路由优先级为255，配置IBGP路由优先级为100，配置本地路由优先级为130，使IBGP路由优先级优于OSPF路由
  peer 10.1.0.101 enable
  peer 10.1.0.101 next-hop-local    //在BGP IPv4单播地址族视图下，配置向对等体10.1.0.101发布BGP路由时，将下一跳属性修改为自身的地址
  peer 10.1.0.101 route-policy local-pre export
  peer 10.30.0.101 enable
  peer 10.30.0.101 next-hop-local    //在BGP IPv4单播地址族视图下，配置向对等体10.30.0.101发布BGP路由时，将下一跳属性修改为自身的地址
  peer 10.50.0.1 enable
#
ospf 1
 import-route direct
 import-route bgp
 area 0.0.0.0
  network 10.2.0.0 0.0.0.255
  network 10.40.1.0 0.0.0.255
#
route-policy local-pre permit node 10    //配置路由策略，将从对等体10.50.0.1学习到的路由发布给对等体10.1.0.101时，设置本地优先级为200
 if-match ip route-source acl 2000
 apply local-preference 200
#
return
```

步骤5 Router_5的配置

```
#
 sysname Router_5
#
interface GigabitEthernet2/0/1
 ip address 10.30.0.102 255.255.255.0
#
interface GigabitEthernet2/0/2
 ip address 10.40.1.102 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.40.1.0 0.0.0.255
  network 10.30.0.0 0.0.0.255
#
return
```

步骤6 Router_6的配置

```
#
 sysname Router_6
```

 版权所有 © 华为技术有限公司

```
#
interface GigabitEthernet2/0/1
 ip address 10.50.0.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 ip address 10.60.0.1 255.255.255.0
#
bgp 300    //启动BGP，指定本地AS号为300，指定BGP路由器的Router ID为6.6.6.6
 router-id 6.6.6.6
 peer 10.50.0.2 as-number 100    //配置Router_6和Router_4建立EBGP连接
 #
 ipv4-family unicast
  undo synchronization
  network 10.60.0.0 255.255.255.0    //在BGP IPv4单播地址族视图下，将本地路由表中到达10.60.0.0/24网段的路由添加到BGP路由表中
  peer 10.50.0.2 enable
#
return
```

步骤7 验证配置结果

在PC_1上可以执行**ping**命令到PC_6的IP地址路由可达，证明PC_1和PC_6可以通信。

在Router_2上使用**display bgp routing-table**命令查看BGP路由表，可以看到2条10.60.0.0/24的路由，本地路由优先级分别为100和200。

在PC_1上**tracert** PC_6，查看到报文传输路径是Router_1 <-> Router_2 <-> Router_3 <-> Router_4 <-> Router_6。

主链路断开后再查看Router_2的BGP路由表，存在1条10.60.0.0/24的路由。

再次在PC_1上**tracert** PC_6，查看到报文传输路径是Router_1 <-> Router_2 <-> Router_5 <-> Router_4 <-> Router_6，表明主备链路切换成功。

----结束

 版权所有 © 华为技术有限公司

10 部署 IP 组播

说明

RU-5G-101不支持此功能。

10.1 配置通过IGMP实现用户主机接收组播视频信息的示例
10.2 配置通过PIM-SM实现组播数据在网络中传输的示例
10.3 配置组播数据通过GRE隧道实现跨单播网段交换的示例
10.4 配置基于VLAN的IGMP Snooping策略以实现用户接收特定的组播组数据示例
10.5 配置使用静态端口实现二层组播示例

10.1 配置通过 IGMP 实现用户主机接收组播视频信息的示例

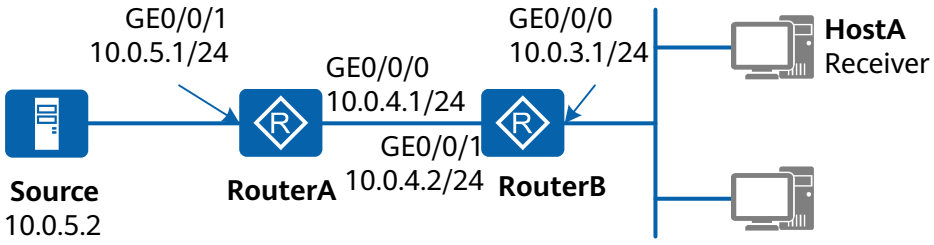
规格

适用于所有版本、所有形态的AR路由器。

组网需求

RouterA的GE0/0/1连接组播源，GE0/0/0连接RouterB。RouterB的GE0/0/1连接RouterA，GE0/0/0连接用户侧主机HostA。要求在该网络中部署组播功能，使HostA能够接收视频点播信息。

图 10-1 IGMP 功能组网图



版权所有 © 华为技术有限公司

操作步骤

步骤1 RouterA的配置

```
#
multicast routing-enable  //全局启动组播协议
#
interface GigabitEthernet0/0/0
 ip address 10.0.4.1 255.255.255.0  //连接RouterB的接口地址
 pim dm  //使能PIM-DM
#
interface GigabitEthernet0/0/1
 ip address 10.0.5.1 255.255.255.0  //连接组播源的接口的IP地址
 pim dm  //使能PIM-DM
#
 ip route-static 10.0.3.0 255.255.255.0 10.0.4.2   //配置到达接收者网段的路由
#
```

步骤2 RouterB的配置

```
#
multicast routing-enable  //全局启动组播协议
#
interface GigabitEthernet0/0/0
 ip address 10.0.3.1 255.255.255.0  //连接HostA的接口的IP地址
 igmp enable  //连接HostA的接口使能igmp
#
interface GigabitEthernet0/0/1
 ip address 10.0.4.2 255.255.255.0  //连接RouterA的接口的IP地址
 pim dm  //使能PIM-DM
#
 ip route-static 10.0.5.0 255.255.255.0 10.0.4.1   //配置到达组播源路由，用于组播RPF检查
#
```

步骤3 验证配置结果

在RouterB上执行**display igmp interface**命令可以查看各路由器接口上IGMP的配置和运行情况。其中“IGMP state”为**up**，HostA能够接收视频点播信息。

----结束

配置注意事项

- 全局使能组播功能。
- 组播源与接收者之间路由可达，接口上全部使能PIM-DM，保证RPF检查正确。
- 连接receiver的接口使能IGMP协议。

10.2 配置通过 PIM-SM 实现组播数据在网络中传输的示例

规格

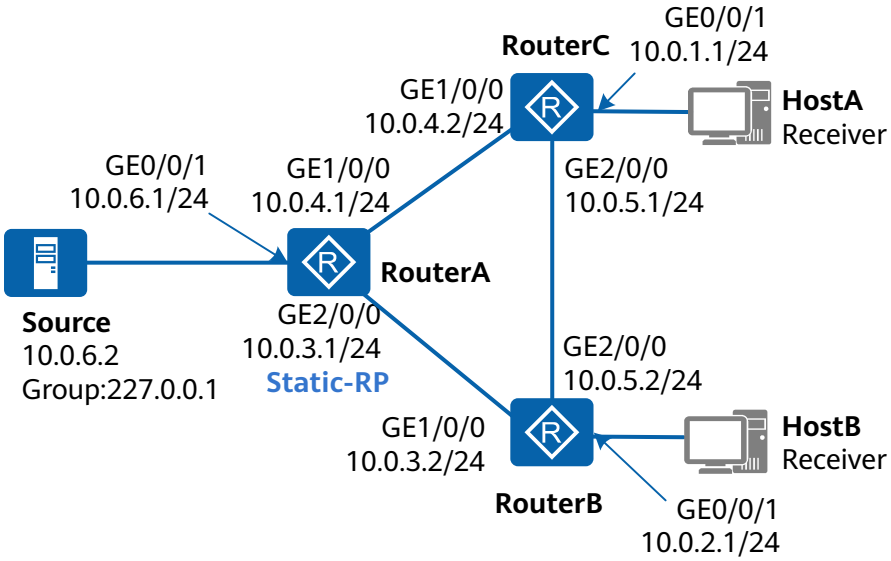
适用于所有版本、所有形态的AR路由器。

组网需求

RouterA连接组播源，RouterB和RouterC连接组播接收者。在RouterA与组播源连接的接口，RouterA、RouterB和RouterC互连的接口上使能PIM SM功能，RouterB和RouterC连接接收者的接口上使能IGMP功能，使接收者能够接收组播源发送的组播数据信息。

 版权所有 © 华为技术有限公司

图 10-2 配置 PIM-SM 功能组网图



操作步骤

步骤1 RouterA的配置

```
#
multicast routing-enable
#
interface GigabitEthernet0/0/1
 ip address 10.0.6.1 255.255.255.0
 pim sm  //连接组播源的接口使能PIM-SM
#
interface GigabitEthernet1/0/0
 ip address 10.0.4.1 255.255.255.0
 pim sm  //使能PIM-SM
#
interface GigabitEthernet2/0/0
 ip address 10.0.3.1 255.255.255.0
 pim sm  //使能PIM-SM
#
ospf 1
 area 0
  network 10.0.3.0 0.0.0.255
  network 10.0.4.0 0.0.0.255
  network 10.0.6.0 0.0.0.255
#
pim
 static-rp 10.0.3.1  //配置静态RP
#
```

步骤2 RouterB的配置

```
#
multicast routing-enable
#
interface GigabitEthernet0/0/1
 ip address 10.0.2.1 255.255.255.0
 pim sm  //使能PIM-SM
 igmp enable  //连接接收者的接口使能igmp
#
interface GigabitEthernet1/0/0
 ip address 10.0.3.2 255.255.255.0
 pim sm  //使能PIM-SM
```


版权所有 © 华为技术有限公司

```
#
interface GigabitEthernet2/0/0
 ip address 10.0.5.2 255.255.255.0
 pim sm  //使能PIM-SM
#
ospf 1
 area 0
  network 10.0.2.0 0.0.0.255
  network 10.0.3.0 0.0.0.255
  network 10.0.5.0 0.0.0.255
#
pim
 static-rp 10.0.3.1  //配置静态RP
#
```

步骤3 RouterC的配置

```
#
multicast routing-enable
#
interface GigabitEthernet0/0/1
 ip address 10.0.1.1 255.255.255.0
 pim sm  //使能PIM-SM
 igmp enable  //连接接收者的接口使能igmp
#
interface GigabitEthernet1/0/0
 ip address 10.0.4.2 255.255.255.0
 pim sm  //使能PIM-SM
#
interface GigabitEthernet2/0/0
 ip address 10.0.5.1 255.255.255.0
 pim sm  //使能PIM-SM
#
ospf 1
 area 0
  network 10.0.1.0 0.0.0.255
  network 10.0.4.0 0.0.0.255
  network 10.0.5.0 0.0.0.255
#
pim
 static-rp 10.0.3.1  //配置静态RP
#
```

步骤4 验证配置结果

在路由器上使用**display pim interface**命令可以查看路由器接口上PIM的配置和运行情况，“State”为“up”。

在路由器上执行**display pim routing-table**命令可以看到(10.0.6.2, 227.0.0.1)表项。

----结束

配置注意事项

- 连接receiver的接口需要使能IGMP协议。
- 配置动态RP时，在有可能成为RP的路由器上配置C-BSR和C-RP。
- 配置静态RP时，PIM-SM域内所有路由器都必须配置完全相同的静态RP。

10.3 配置组播数据通过 GRE 隧道实现跨单播网段交换的示例

规格

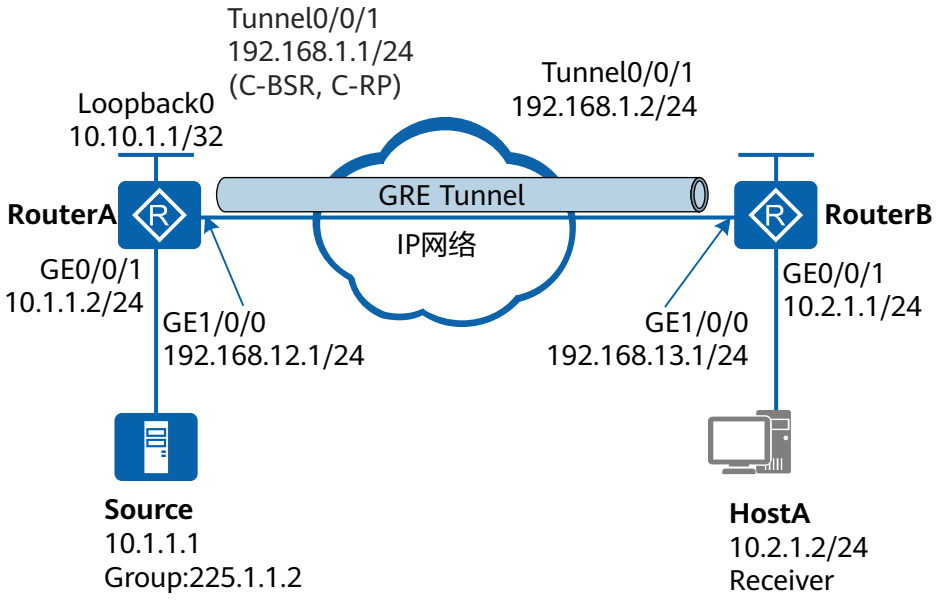
适用于所有版本、所有形态的AR路由器。

 版权所有 © 华为技术有限公司

组网需求

RouterA连接组播源，RouterB连接组播接收者。RouterA和RouterB使用loopback接口建立一条GRE隧道，在GRE隧道接口配置PIM SM协议，使组播流通过GRE隧道发送给组播接收者。

图 10-3 组播 Over GRE 功能组网图



操作步骤

步骤1 RouterA的配置

```
#
multicast routing-enable
#
interface GigabitEthernet0/0/1
 ip address 10.1.1.2 255.255.255.0  //连接组播源的接口的IP地址
 pim sm  //使能PIM-SM
#
interface GigabitEthernet1/0/0
 ip address 192.168.12.1  255.255.255.0
#
interface loopback0
 ip address 10.10.1.1 255.255.255.255
#
interface tunnel0/0/1
 tunnel-protocol gre  //tunnel封装为GRE隧道
 ip address 192.168.1.1 255.255.255.0
 source 10.10.1.1
 destination 10.10.1.2
 pim sm  //在Tunnel接口使能PIM-SM
#
ospf 1
 area 0
  network 10.10.1.1 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 192.168.1.0 0.0.0.255
#  //配置C-RP和C-BSR，使用tunnel接口的IP地址作为候选RP的IP地址
pim
```


版权所有 © 华为技术有限公司

```
 c-bsr Tunnel0/0/1
 c-rp Tunnel0/0/1
#
```

步骤2 RouterB的配置

```
#
multicast routing-enable
#
interface GigabitEthernet0/0/1
 ip address 10.2.1.1 255.255.255.0  //连接组播接收者的接口的IP地址
 pim sm  //使能PIM-SM
 igmp enable  //使能IGMP
#
interface GigabitEthernet1/0/0
 ip address 192.168.13.1  255.255.255.0
#
interface loopback0
 ip address 10.10.1.2 255.255.255.255
#
interface tunnel0/0/1
 tunnel-protocol gre  //tunnel封装为GRE隧道
 ip address 192.168.1.2 255.255.255.0
 source 10.10.1.2
 destination 10.10.1.1
 pim sm  //在GRE Tunnel接口使能PIM-SM
#
ospf 1
 area 0
  network 10.10.1.2 0.0.0.0
  network 10.2.1.0 0.0.0.255
  network 192.168.1.0 0.0.0.255
#
```

步骤3 验证配置结果

在路由器上使用**display pim interface**命令可以查看路由器接口上PIM的配置和运行情况，“State”为“up”。

在RouterB上使用**display igmp group**命令可以看到接收者已经加入到组播组。

```
Interface group report information
 GigabitEthernet0/0/1(10.2.1.1):
  Total 1 IGMP Group reported
   Group Address   Last Reporter   Uptime      Expires
   225.1.1.2       10.2.1.2        00:02:04    00:01:17
```

在路由器上执行**display pim routing-table**命令可以看到(10.1.1.1, 225.1.1.2)表项。

```
 (10.1.1.1, 225.1.1.2)
     RP: 192.168.1.1
     Protocol: pim-sm, Flag: ACT
     UpTime: 00:04:32
     Upstream interface: Tunnel0/0/1
         Upstream neighbor: 192.168.1.1
         RPF prime neighbor: 192.168.1.1
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet0/0/1
             Protocol: pim-sm, UpTime: 00:04:32, Expires: -
```

----结束

配置注意事项

- 使用Loopback接口建立GRE隧道，并在Tunnel接口上使能PIM SM。
- 连接receiver的接口需要使能IGMP协议。

 版权所有 © 华为技术有限公司

- 配置C-RP和C-BSR时，使用tunnel接口的IP地址作为候选RP的IP地址。

10.4 配置基于 VLAN 的 IGMP Snooping 策略以实现用户接收特定的组播组数据示例

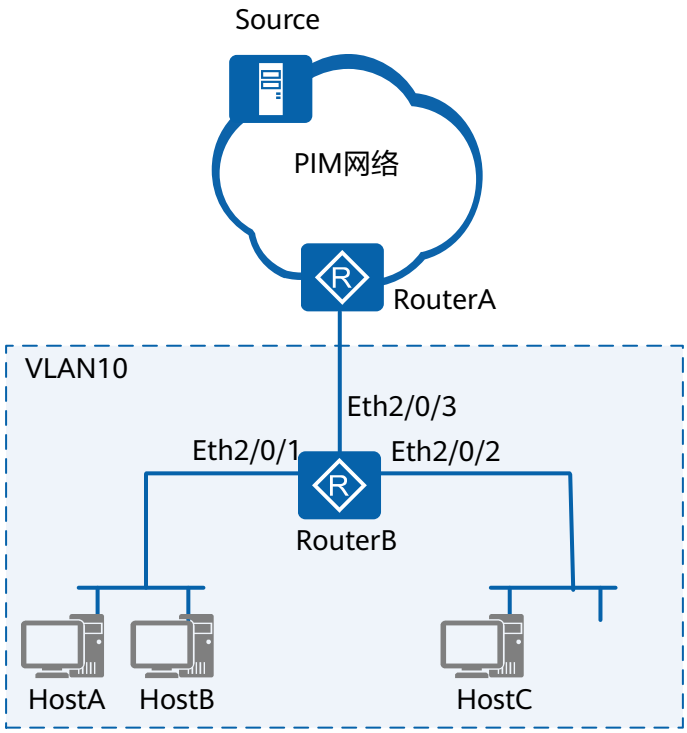
规格

适用于所有版本、所有形态的AR路由器。

组网需求

如图10-4所示，用户网络VLAN 10通过RouterB接入到PIM网络。组播源Source向组播组225.1.1.1～225.1.1.5发送数据。要求通过在RouterB开启IGMP Snooping功能并配置组播组过滤策略，实现用户网络VLAN 10内的组播接收者HostA、HostB和HostC拒收组播组225.1.1.4跟225.1.1.5的数据，只能接收发往组播组225.1.1.1～225.1.1.3的组播数据。

图 10-4 配置 IGMP Snooping 策略组网图



操作步骤

步骤1 RouterB的配置

```
#
 sysname RouterB  //配置设备名称
#
```


版权所有 © 华为技术有限公司

```
vlan batch 10  //创建VLAN10
#
 igmp-snooping enable  //使能全局IGMP Snooping功能
#
vlan 10  //使能VLAN10的IGMP Snooping功能
 igmp-snooping enable
 igmp-snooping group-policy 2000  //在VLAN10内应用组播组过滤策略2000
#
acl number 2000  //配置组播组过滤策略2000，拒收组播组225.1.1.4和225.1.1.5的数据，只能接收发往组播组225.1.1.1～225.1.1.3的组播数据
 rule 5 deny source 225.1.1.4 0
 rule 10 deny source 225.1.1.5 0
 rule 15 permit source 225.1.1.1 0
 rule 20 permit source 225.1.1.2 0
 rule 25 permit source 225.1.1.3 0
#
interface Ethernet2/0/1  //配置接口Eth2/0/1加入VLAN10
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface Ethernet2/0/2  //配置接口Eth2/0/2加入VLAN10
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface Ethernet2/0/3  //配置接口Eth2/0/3加入VLAN10
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
return
```

步骤2 验证配置结果

在RouterB上执行命令**display igmp-snooping port-info**查看组播组的成员端口信息。可以看到组播组225.1.1.1～225.1.1.3已在RouterB上动态生成的成员端口Eth2/0/1和Eth2/0/2上。

在RouterB上执行命令**display l2-multicast forwarding-table vlan 10**查看指定VLAN的IGMP Snooping转发表信息。可以看到转发表中只有225.1.1.1～225.1.1.3的组播数据。225.1.1.4～225.1.1.5的组播数据不会转发给Host。

----结束

配置注意事项

- RouterB的接口Eth2/0/1，Eth2/0/2和Eth2/0/3加入VLAN10。
- 全局和VLAN10使能IGMP Snooping功能。

10.5 配置使用静态端口实现二层组播示例

规格

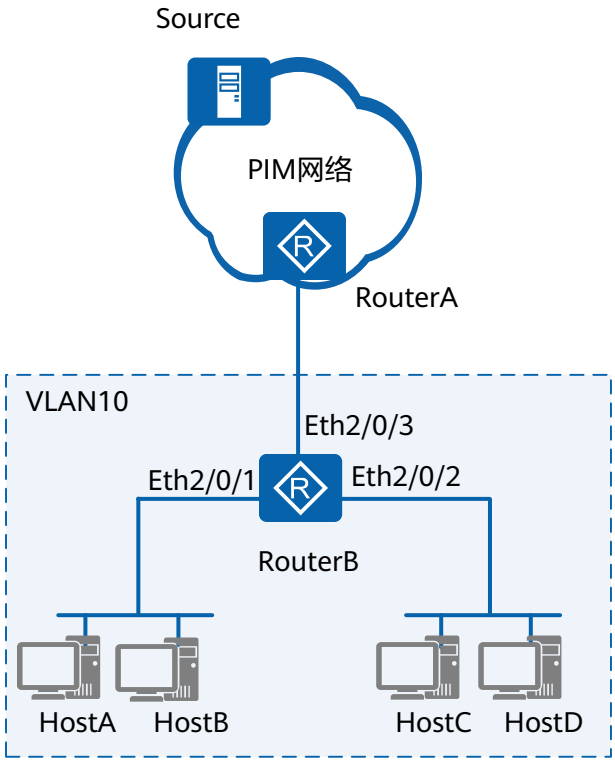
适用于所有版本、所有形态的AR路由器。

组网需求

如图10-5所示，路由器RouterA通过二层设备RouterB连接用户网络VLAN10，RouterA的用户侧三层VLANIF接口配置了225.1.1.1～225.1.1.5的IGMP静态组，没有运行IGMP协议。网络中有HostA、HostB、HostC、HostD四个接收者，其中HostA和HostB希望长期稳定接收组播组225.1.1.1～225.1.1.3的数据，HostC和HostD希望长期稳定接收组播组225.1.1.4～225.1.1.5的数据。

 版权所有 © 华为技术有限公司

图 10-5 配置静态端口实现二层组播组网图



操作步骤

步骤1 RouterB的配置

```
#
 sysname RouterB  //配置设备名称
#
vlan batch 10  //创建VLAN10
#
igmp-snooping enable  //使能全局的IGMP Snooping功能
#
vlan 10  //使能VLAN10的IGMP Snooping功能
 igmp-snooping enable
#
interface Ethernet2/0/1  //配置端口Eth2/0/1加入VLAN10
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
 l2-multicast static-group group-address 225.1.1.1 to 225.1.1.3 vlan 10  //配置端口Eth2/0/1静态加入组播组225.1.1.1～225.1.1.3
#
interface Ethernet2/0/2  //配置端口Ethernet2/0/2加入VLAN10
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
 l2-multicast static-group group-address 225.1.1.4 to 225.1.1.5 vlan 10  //配置端口Eth2/0/2静态加入组播组225.1.1.4，225.1.1.5
#
interface Ethernet2/0/3  //配置端口Eth2/0/3加入VLAN10
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
 igmp-snooping static-router-port vlan 10  //配置端口Eth2/0/3为静态路由器端口
#
return
```


版权所有 © 华为技术有限公司

步骤2 验证配置结果

在RouterB上执行命令**display igmp-snooping router-port**查看VLAN内IGMP Snooping的路由器端口信息。可以看到Eth2/0/3已成为静态路由器端口。

在RouterB上执行命令**display igmp-snooping port-info**查看组播组的成员端口信息。可以看到组播组225.1.1.1～225.1.1.3在RouterB上有静态成员端口Eth2/0/1，组播组225.1.1.4～225.1.1.5在RouterB上有静态成员端口Eth2/0/2。

在RouterB上执行命令**display l2-multicast forwarding-table vlan 10**查看指定VLAN的IGMP Snooping转发表信息。可以看到组播组225.1.1.1～225.1.1.5在RouterB上已生成转发表。

----结束

配置注意事项

- RouterB的接口Eth2/0/1，Eth2/0/2和Eth2/0/3加入VLAN10。
- 全局和VLAN10使能IGMP Snooping功能。

 版权所有 © 华为技术有限公司

11 部署 MPLS

11.1 配置骨干网设备MPLS本地会话功能实现数据在MPLS网络中转发示例
11.2 配置骨干网设备MPLS远端会话功能实现VPN数据在MPLS网络中承载示例
11.3 配置静态LSP实现分支和总部的互通示例
11.4 配置LDP LSP实现分支和总部的互通示例
11.5 配置MPLS TE实现分支和总部的互通示例

11.1 配置骨干网设备 MPLS 本地会话功能实现数据在 MPLS 网络中转发示例

规格

AR611E-S、AR611、AR631I-LTE4CN、AR631I-LTE4EA、AR611-LTE4EA、AR611-S、AR611W-S、AR611W、AR611W-LTE4CN、AR611W-LTE6EA、AR617VW、AR617VW-LTE4EA、AR617VW-LTE4、AR651C和AR651F-Lite不支持MPLS。

仅AR300系列不支持MPLS。

RU-5G-101不支持MPLS。

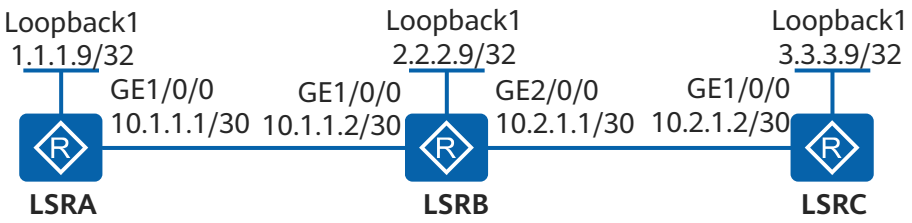
组网需求

如**图11-1**所示，LSRA、LSRB、LSRC是MPLS网络的核心设备。数据流量从PE设备进入MPLS网络。要实现数据流在MPLS域内的转发，则需要在LSRA、LSRB、LSRC之间配置LDP本地会话，从而进行标签交换，建立LDP LSP。

按照**图11-1**所示，对LSRA、LSRB、LSRC进行地址规划。

版权所有 © 华为技术有限公司

图 11-1 配置 LDP 本地会话组网图



操作步骤

步骤1 LSRA的配置

```
#
 sysname LSRA
#
mpls lsr-id 1.1.1.9  //配置Loopback1接口的地址做为LSR ID
mpls                 //全局使能MPLS
#
mpls ldp             //全局使能MPLS LDP
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.1 255.255.255.252
 mpls                //接口使能MPLS
 mpls ldp            //接口使能MPLS LDP
#
interface LoopBack1
 ip address 1.1.1.9 255.255.255.255
#
ospf 1               //OSPF保证全网互通
 area 0.0.0.0
  network 1.1.1.9 0.0.0.0
  network 10.1.1.0 0.0.0.3
#
```

步骤2 LSRB的配置

```
#
 sysname LSRB
#
mpls lsr-id 2.2.2.9  //配置Loopback1接口的地址做为LSR ID
mpls                 //全局使能MPLS
#
mpls ldp             //全局使能MPLS LDP
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.2 255.255.255.252
 mpls                //接口使能MPLS
 mpls ldp            //接口使能MPLS LDP
#
interface GigabitEthernet2/0/0
 ip address 10.2.1.1 255.255.255.252
 mpls                //接口使能MPLS
 mpls ldp            //接口使能MPLS LDP
#
interface LoopBack1
 ip address 2.2.2.9 255.255.255.255
#
ospf 1               //OSPF保证全网互通
 area 0.0.0.0
```


版权所有 © 华为技术有限公司

```
 network 2.2.2.9 0.0.0.0
 network 10.1.1.0 0.0.0.3
 network 10.2.1.0 0.0.0.3
#
```

步骤3 LSRC的配置

```
#
 sysname LSRC
#
mpls lsr-id 3.3.3.9  //配置Loopback1接口的地址做为LSR ID
mpls                 //全局使能MPLS
#
mpls ldp             //全局使能MPLS LDP
#
interface GigabitEthernet1/0/0
 ip address 10.2.1.2 255.255.255.252
 mpls                //接口使能MPLS
 mpls ldp            //接口使能MPLS LDP
#
interface LoopBack1
 ip address 3.3.3.9 255.255.255.255
#
ospf 1               //OSPF保证全网互通
 area 0.0.0.0
  network 3.3.3.9 0.0.0.0
  network 10.2.1.0 0.0.0.3
#
```

步骤4 验证配置结果

配置完成后，在节点上执行**display mpls ldp session**命令，可以看到LSRA和LSRB、LSRB和LSRC之间的LDP本地会话状态为“Operational”。

----结束

配置注意事项

- 配置LSR ID是配置其它MPLS命令的前提。

11.2 配置骨干网设备 MPLS 远端会话功能实现 VPN 数据在 MPLS 网络中承载示例

规格

AR611E-S、AR611、AR631I-LTE4CN、AR631I-LTE4EA、AR611-LTE4EA、AR611-S、AR611W-S、AR611W、AR611W-LTE4CN、AR611W-LTE6EA、AR617VW、AR617VW-LTE4EA、AR617VW-LTE4、AR651C和AR651F-Lite不支持MPLS。

仅AR300系列不支持MPLS。

RU-5G-101不支持MPLS。

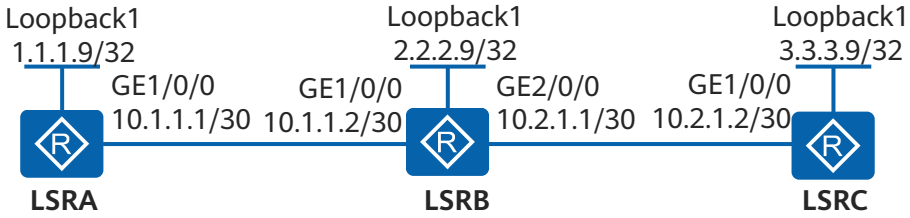
组网需求

如图11-2所示，LSRA、LSRC是骨干网的边缘设备。在该网络中部署VPN业务，建立跨越VPN区域的LDP LSP，则需要在LSRA和LSRC之间建立远端LDP会话，从而为VPN业务提供服务。

按照图11-2所示，对LSRA、LSRB、LSRC进行地址规划。

 版权所有 © 华为技术有限公司

图 11-2 配置 LDP 远端会话组网图



操作步骤

步骤1 LSRA的配置

```
#
 sysname LSRA
#
mpls lsr-id 1.1.1.9  //配置Loopback1接口的地址做为LSR ID
mpls                 //全局使能MPLS
#
mpls ldp             //全局使能MPLS LDP
#
 mpls ldp remote-peer LSRC  //在LSRA上指定远端对等体为LSRC
 remote-ip 3.3.3.9          //在LSRA上指定远端对等体的IP地址
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.1 255.255.255.252
 mpls
 mpls ldp
#
interface LoopBack1
 ip address 1.1.1.9 255.255.255.255
#
ospf 1               //OSPF保证全网互通
 area 0.0.0.0
  network 1.1.1.9 0.0.0.0
  network 10.1.1.0 0.0.0.3
#
```

步骤2 LSRB的配置

```
#
 sysname LSRB
#
mpls lsr-id 2.2.2.9  //配置Loopback1接口的地址做为LSR ID
mpls                 //全局使能MPLS
#
mpls ldp             //全局使能MPLS LDP
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.2 255.255.255.252
 mpls
 mpls ldp
#
interface GigabitEthernet2/0/0
 ip address 10.2.1.1 255.255.255.252
 mpls
 mpls ldp
#
interface LoopBack1
 ip address 2.2.2.9 255.255.255.255
#
ospf 1               //OSPF保证全网互通
 area 0.0.0.0
  network 2.2.2.9 0.0.0.0
  network 10.1.1.0 0.0.0.3
```


版权所有 © 华为技术有限公司

```
 network 10.2.1.0 0.0.0.3
#
```

步骤3 LSRC的配置

```
#
 sysname LSRC
#
mpls lsr-id 3.3.3.9  //配置Loopback1接口的地址做为LSR ID
mpls                 //全局使能MPLS
#
mpls ldp             //全局使能MPLS LDP
#
 mpls ldp remote-peer LSRA  //在LSRC上指定远端对等体为LSRA
 remote-ip 1.1.1.9          //在LSRC上指定远端对等体的IP地址
#
interface GigabitEthernet1/0/0
 ip address 10.2.1.2 255.255.255.252
 mpls
 mpls ldp
#
interface LoopBack1
 ip address 3.3.3.9 255.255.255.255
#
ospf 1               //OSPF保证全网互通
 area 0.0.0.0
  network 3.3.3.9 0.0.0.0
  network 10.2.1.0 0.0.0.3
#
```

步骤4 验证配置结果

配置完成后，在节点上执行**display mpls ldp session**命令，可以看到LSRA和LSRB、LSRB和LSRC之间的LDP本地会话状态为“Operational”；也可以看到LSRA和LSRC远端会话状态为“Operational”。

在LDP远端会话两端LSR上执行**display mpls ldp remote-peer**命令，可以看到LSR的远端对等体信息。

----结束

配置注意事项

- 配置LSR ID是配置其它MPLS命令的前提。

11.3 配置静态 LSP 实现分支和总部的互通示例

规格

AR611E-S、AR611、AR631I-LTE4CN、AR631I-LTE4EA、AR611-LTE4EA、AR611-S、AR611W-S、AR611W、AR611W-LTE4CN、AR611W-LTE6EA、AR617VW、AR617VW-LTE4EA、AR617VW-LTE4、AR651C和AR651F-Lite不支持MPLS。

仅AR300系列不支持MPLS。

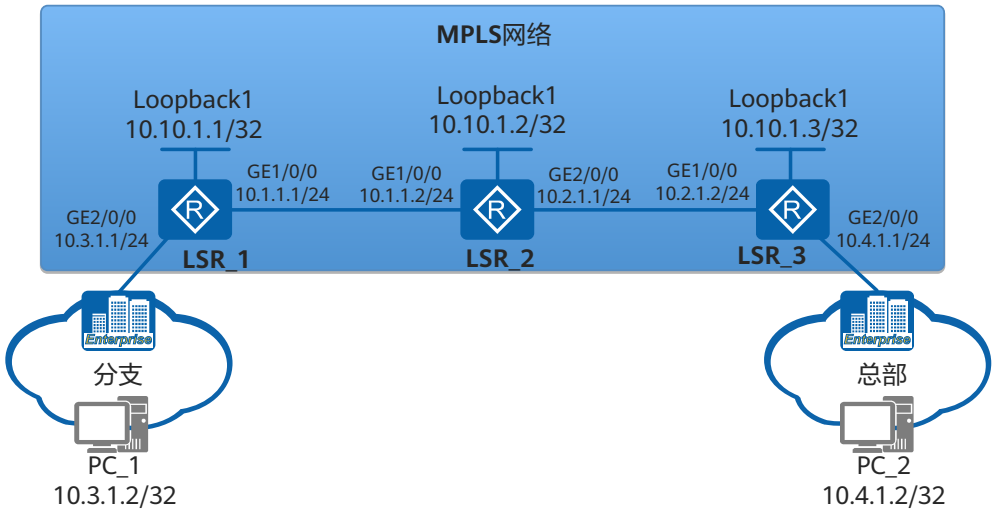
RU-5G-101不支持MPLS。

组网需求

如图11-3所示，LSR_1、LSR_2、LSR_3为MPLS骨干网设备。要求通过配置静态LSP隧道，使这分支和总部互访的报文能够通过LSP在MPLS网络中进行传输。

 版权所有 © 华为技术有限公司

图 11-3 配置静态 LSP 实现分支和总部的互通组网



操作步骤

步骤1 配置LSR_1

```
#
 sysname LSR_1
#
mpls lsr-id 10.10.1.1   //配置MPLS LSR ID
mpls   //使能全局MPLS功能
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.1 255.255.255.0
 mpls   //使能接口MPLS功能
#
interface GigabitEthernet2/0/0
 ip address 10.3.1.1 255.255.255.0
#
interface LoopBack1
 ip address 10.10.1.1 255.255.255.255
#
ospf 1   //配置路由
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 10.3.1.0 0.0.0.255
  network 10.10.1.1 0.0.0.0
#
static-lsp ingress LSP1 destination 10.4.1.0 24 nexthop 10.1.1.2 out-label 20   //配置本节点为指定LSP1的
Ingress
static-lsp egress LSP2 incoming-interface GigabitEthernet1/0/0 in-label 60   //配置本节点为指定LSP2的Egress
#
return
```

步骤2 配置LSR_2

```
#
 sysname LSR_2
#
mpls lsr-id 10.10.1.2
mpls
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.2 255.255.255.0
 mpls
#
```


版权所有 © 华为技术有限公司

```
interface GigabitEthernet2/0/0
 ip address 10.2.1.1 255.255.255.0
 mpls
#
interface LoopBack1
 ip address 10.10.1.2 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 10.2.1.0 0.0.0.255
  network 10.10.1.2 0.0.0.0
#
static-lsp transit LSP1 incoming-interface GigabitEthernet1/0/0 in-label 20 nexthop 10.2.1.2 out-label 40   //配置本节点为指定LSP1的Transit
static-lsp transit LSP2 incoming-interface GigabitEthernet2/0/0 in-label 30 nexthop 10.1.1.1 out-label 60   //配置本节点为指定LSP2的Transit
#
return
```

步骤3 配置LSR_3

```
#
 sysname LSR_3
#
mpls lsr-id 10.10.1.3
mpls
#
interface GigabitEthernet1/0/0
 ip address 10.2.1.2 255.255.255.0
 mpls
#
interface LoopBack1
 ip address 10.10.1.3 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 10.2.1.0 0.0.0.255
  network 10.3.1.0 0.0.0.255
  network 10.10.1.3 0.0.0.0
#
static-lsp ingress LSP2 destination 10.3.1.0 24 nexthop 10.2.1.1 out-label 30   //配置本节点为指定LSP2的Ingress
static-lsp egress LSP1 incoming-interface GigabitEthernet1/0/0 in-label 40   //配置本节点为指定LSP1的Egress
#
return
```

步骤4 配置LSR_3验证配置结果

在LSR上执行命令**display mpls static-lsp**，可以看到LSP的**Status**为**Up**。

企业分支与总部可以相互Ping通。

----结束

配置注意事项

- 配置静态LSP时需要遵循的原则是：前一节点出标签的值等于下一个节点入标签的值。
- 配置静态LSP时，需要注意配置的静态LSP的路由一定要和路由信息完全匹配。如下面所示：
  - 如果在配置静态LSP时指定了下一跳，则在配置IP静态路由时也必须指定下一跳，否则不能建立静态LSP。
  - 如果LSR之间使用动态路由协议互通，则LSP的下一跳IP地址必须与路由表中的下一跳IP地址一致。

 版权所有 © 华为技术有限公司

11.4 配置 LDP LSP 实现分支和总部的互通示例

规格

AR611E-S、AR611、AR631I-LTE4CN、AR631I-LTE4EA、AR611-LTE4EA、AR611-S、AR611W-S、AR611W、AR611W-LTE4CN、AR611W-LTE6EA、AR617VW、AR617VW-LTE4EA、AR617VW-LTE4、AR651C和AR651F-Lite不支持MPLS。

仅AR300系列不支持MPLS。

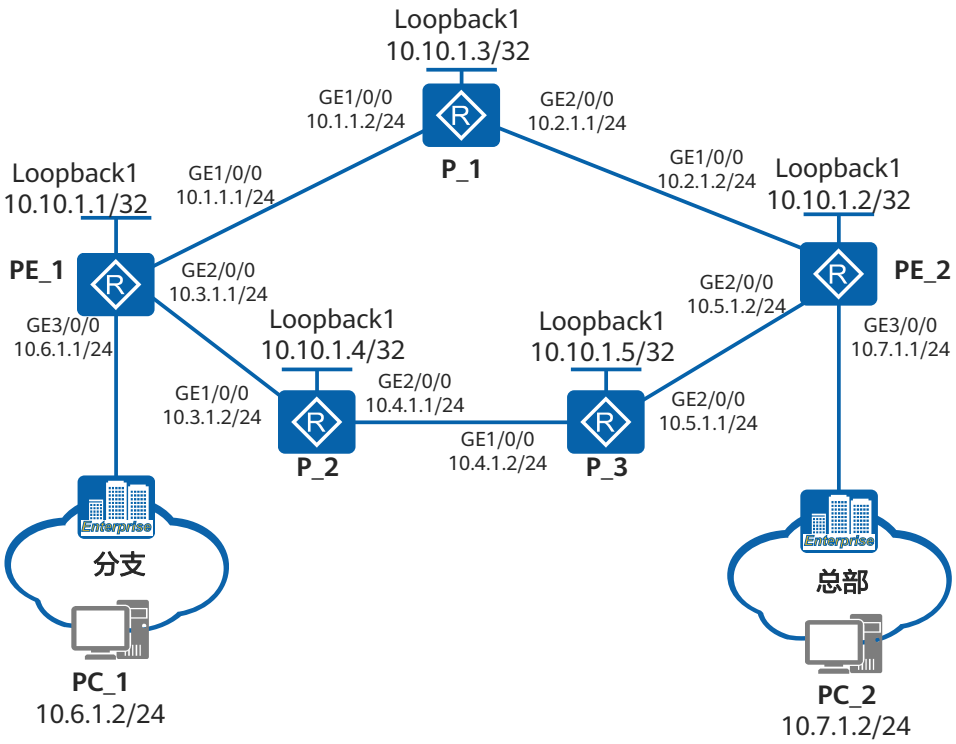
RU-5G-101不支持MPLS。

组网需求

如图11-4所示，PE和P为MPLS骨干网设备，PE_1和PE_2之间路由可达。

企业现要求分支和总部之间的流量通过MPLS转发，并且当主用LSP故障时，流量能够快速切换到备份LSP，尽可能地避免流量的丢失。另外，为了避免建立的LSP数量过多，影响设备性能，所有设备上只允许目的地址为10.10.1.x/32、10.6.1.0/24和10.7.1.0/24的路由表项触发建立LSP，其他路由表项不能触发建立LSP。

图 11-4 配置 LDP LSP 实现分支和总部的互通组网



操作步骤

步骤1 配置PE_1

版权所有 © 华为技术有限公司

```
#
 sysname PE_1
#
bfd   //全局使能BFD功能
#
mpls lsr-id 10.10.1.1   //配置MPLS LSR ID
mpls   //使能全局MPLS功能
 lsp-trigger ip-prefix pe1    //根据IP地址前缀列表触发LDP建立LSP
 mpls bfd enable   //使能BFD功能
 mpls bfd-trigger fec-list tortc  //指定LDP BFD以FEC列表方式触发
 mpls bfd min-tx-interval 100 min-rx-interval 100
#
fec-list tortc   //创建FEC列表
 fec-node 10.10.1.2
#
mpls ldp   //使能全局MPLS LDP功能
#
interface GigabitEthernet1/0/0   //使能接口MPLS LDP功能
 ip address 10.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet2/0/0
 ip address 10.3.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet3/0/0
 ip address 10.6.1.1 255.255.255.0
#
interface LoopBack1
 ip address 10.10.1.1 255.255.255.255
#
ospf 1   //配置OSPF路由
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 10.3.1.0 0.0.0.255
  network 10.6.1.0 0.0.0.255
  network 10.10.1.1 0.0.0.0
#
ip ip-prefix pe1 index 10 permit 10.10.1.1 32   //创建IP地址前缀列表
ip ip-prefix pe1 index 20 permit 10.10.1.2 32
ip ip-prefix pe1 index 30 permit 10.10.1.3 32
ip ip-prefix pe1 index 40 permit 10.10.1.4 32
ip ip-prefix pe1 index 50 permit 10.10.1.5 32
ip ip-prefix pe1 index 60 permit 10.6.1.0 24
ip ip-prefix pe1 index 70 permit 10.7.1.0 24
#
return
```

步骤2 配置P_1

```
#
 sysname P_1
#
mpls lsr-id 10.10.1.3   //配置MPLS LSR ID
mpls   //使能全局MPLS功能
#
mpls ldp   //使能全局MPLS LDP功能
#
interface GigabitEthernet1/0/0   //使能接口MPLS LDP功能
 ip address 10.1.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet2/0/0
 ip address 10.2.1.1 255.255.255.0
 mpls
 mpls ldp
#
```

 版权所有 © 华为技术有限公司

```
interface LoopBack1
 ip address 10.10.1.3 255.255.255.255
#
ospf 1   //配置OSPF路由
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 10.2.1.0 0.0.0.255
  network 10.10.1.3 0.0.0.0
#
return
```

步骤3 配置P_2

```
#
 sysname P_2
#
mpls lsr-id 10.10.1.4   //配置MPLS LSR ID
mpls   //使能全局MPLS功能
#
mpls ldp   //使能全局MPLS LDP功能
#
interface GigabitEthernet1/0/0   //使能接口MPLS LDP功能
 ip address 10.3.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet2/0/0
 ip address 10.4.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface LoopBack1
 ip address 10.10.1.4 255.255.255.255
#
ospf 1   //配置OSPF路由
 area 0.0.0.0
  network 10.3.1.0 0.0.0.255
  network 10.4.1.0 0.0.0.255
  network 10.10.1.4 0.0.0.0
#
return
```

步骤4 配置P_3

```
#
 sysname P_3
#
mpls lsr-id 10.10.1.5   //配置MPLS LSR ID
mpls   //使能全局MPLS功能
#
mpls ldp   //使能全局MPLS LDP功能
#
interface GigabitEthernet1/0/0   //使能接口MPLS LDP功能
 ip address 10.4.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet2/0/0
 ip address 10.5.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface LoopBack1
 ip address 10.10.1.5 255.255.255.255
#
ospf 1   //配置OSPF路由
 area 0.0.0.0
  network 10.4.1.0 0.0.0.255
  network 10.5.1.0 0.0.0.255
  network 10.10.1.5 0.0.0.0
```

 版权所有 © 华为技术有限公司

```
#
return
```

步骤5 配置PE_2

```
#
 sysname PE_2
#
bfd   //全局使能BFD功能
 mpls-passive   //使能被动创建BFD会话功能
#
mpls lsr-id 10.10.1.2   //配置MPLS LSR ID
mpls   //使能全局MPLS功能
 lsp-trigger ip-prefix pe2   //根据IP地址前缀列表触发LDP建立LSP
#
mpls ldp   //使能全局MPLS LDP功能
#
interface GigabitEthernet1/0/0   //使能接口MPLS LDP功能
 ip address 10.2.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet2/0/0
 ip address 10.5.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface GigabitEthernet3/0/0
 ip address 10.7.1.1 255.255.255.0
#
interface LoopBack1
 ip address 10.10.1.2 255.255.255.255
#
ospf 1   //配置OSPF路由
 area 0.0.0.0
  network 10.2.1.0 0.0.0.255
  network 10.5.1.0 0.0.0.255
  network 10.7.1.0 0.0.0.255
  network 10.10.1.2 0.0.0.0
#
ip ip-prefix pe2 index 10 permit 10.10.1.1 32   //创建IP地址前缀列表
ip ip-prefix pe2 index 20 permit 10.10.1.2 32
ip ip-prefix pe2 index 30 permit 10.10.1.3 32
ip ip-prefix pe2 index 40 permit 10.10.1.4 32
ip ip-prefix pe2 index 50 permit 10.10.1.5 32
ip ip-prefix pe2 index 60 permit 10.6.1.0 24
ip ip-prefix pe2 index 70 permit 10.7.1.0 24
#
return
```

步骤6 验证配置结果

在LSR上执行命令**display mpls ldp lsp**，可以看到去往对应目的地址的LSP已经建立。将同一台测试仪的两个接口（Port1和Port2）分别接入PE_1和PE_2，从Port1向Port2打MPLS流。当对P_1的GE1/0/0接口进行shutdown操作来模拟主用LSP故障时，发现流量快速切换到备份LSP。

企业分支与总部可以相互Ping通。

----结束

配置注意事项

- 配置LSR ID是配置其它MPLS命令的前提。
- MPLS是基于路由来建立LSP，需确保路由可达。

 版权所有 © 华为技术有限公司

11.5 配置 MPLS TE 实现分支和总部的互通示例

规格

AR611E-S、AR611、AR631I-LTE4CN、AR631I-LTE4EA、AR611-LTE4EA、AR611-S、AR611W-S、AR611W、AR611W-LTE4CN、AR611W-LTE6EA、AR617VW、AR617VW-LTE4EA、AR617VW-LTE4、AR651C和AR651F-Lite不支持MPLS。

仅AR300系列不支持MPLS。

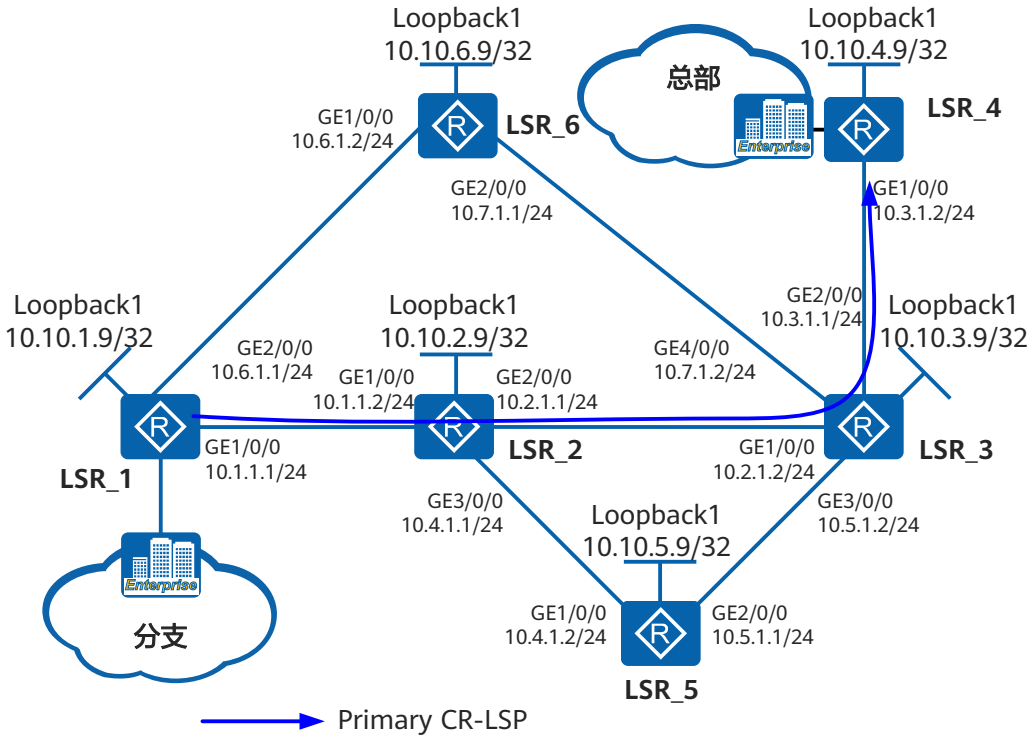
RU-5G-101不支持MPLS。

组网需求

如图11-5所示，企业分支和总部通过MPLS网络进行互联。要求创建一条沿显式路径：LSR_1→LSR_2→LSR_3→LSR_4的主隧道。在中间节点LSR_2上配置一条TE FRR的旁路保护隧道，路径为LSR_2→LSR_5→LSR_3，并在入节点LSR_1上配置普通备份CR-LSP，路径为LSR_1→LSR_6→LSR_3→LSR_4。

当LSR_2和LSR_3之间的链路出现故障后，设备启用TE FRR旁路保护隧道（即主CR-LSP处于Frr-in-use状态）并尝试恢复主CR-LSP的同时，也会尝试创建备份CR-LSP。

图 11-5 配置 MPLS TE 实现分支和总部的互通组网图



版权所有 © 华为技术有限公司

操作步骤

步骤1 配置LSR_1

```
#
 sysname LSR_1
#
bfd   //使能BFD功能
#
mpls lsr-id 10.10.1.9
mpls   //使能MPLS TE
 mpls te
 mpls rsvp-te
 mpls te cspf
#
explicit-path backup-path   //配置备份CR-LSP的显式路径
 next hop 10.6.1.2
 next hop 10.7.1.2
 next hop 10.3.1.2
 next hop 10.10.4.9
#
explicit-path pri-path   //配置主CR-LSP的显式路径
 next hop 10.1.1.2
 next hop 10.2.1.2
 next hop 10.3.1.2
 next hop 10.10.4.9
#
interface GigabitEthernet1/0/0   //使能接口MPLS TE
 ip address 10.1.1.1 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet2/0/0
 ip address 10.6.1.1 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface LoopBack1
 ip address 10.10.1.9 255.255.255.255
#
interface Tunnel0/0/1   //配置主CR-LSP的MPLS TE隧道接口
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 10.10.4.9
 mpls te tunnel-id 100
 mpls te bfd enable   //配置动态BFD for CR-LSP功能
 mpls te bfd min-tx-interval 500 min-rx-interval 500
 mpls te record-route label
 mpls te path explicit-path pri-path
 mpls te path explicit-path backup-path secondary
 mpls te fast-reroute   //使能TE FRR功能
 mpls te backup ordinary
 mpls te backup frr-in-use
 mpls te commit
#
ospf 1   //配置OSPF路由
 opaque-capability enable
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 10.6.1.0 0.0.0.255
  network 10.10.1.9 0.0.0.0
  mpls-te enable
#
return
```

步骤2 配置LSR_2

 版权所有 © 华为技术有限公司

```
#
 sysname LSR_2
#
mpls lsr-id 10.10.2.9
mpls   //使能MPLS TE
 mpls te
 mpls rsvp-te
 mpls te cspf
#
explicit-path by-path   //配置Bypass CR-LSP的显式路径
 next hop 10.4.1.2
 next hop 10.5.1.2
 next hop 10.10.3.9
#
interface GigabitEthernet1/0/0   //使能接口MPLS TE
 ip address 10.1.1.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet2/0/0
 ip address 10.2.1.1 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet3/0/0
 ip address 10.4.1.1 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface LoopBack1
 ip address 10.10.2.9 255.255.255.255
#
interface Tunnel0/0/2   //配置Bypass CR-LSP的隧道接口
 ip address unnumbered interface LoopBack1
 tunnel-protocol mpls te
 destination 10.10.3.9
 mpls te tunnel-id 300
 mpls te record-route
 mpls te path explicit-path by-path
 mpls te bypass-tunnel
 mpls te protected-interface GigabitEthernet2/0/0
 mpls te commit
#
ospf 1   //配置OSPF路由
 opaque-capability enable
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 10.2.1.0 0.0.0.255
  network 10.4.1.0 0.0.0.255
  network 10.10.2.9 0.0.0.0
  mpls-te enable
#
return
```

步骤3 配置LSR_3

```
#
 sysname LSR_3
#
bfd   //使能被动创建BFD会话
 mpls-passive
#
mpls lsr-id 10.10.3.9
mpls   //使能MPLS TE
 mpls te
 mpls rsvp-te
#
```

 版权所有 © 华为技术有限公司

```
interface GigabitEthernet1/0/0   //使能接口MPLS TE
 ip address 10.2.1.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet2/0/0
 ip address 10.3.1.1 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet3/0/0
 ip address 10.5.1.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet4/0/0
 ip address 10.7.1.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface LoopBack1
 ip address 10.10.3.9 255.255.255.255
#
ospf 1   //配置OSPF路由
 opaque-capability enable
 area 0.0.0.0
  network 10.2.1.0 0.0.0.255
  network 10.3.1.0 0.0.0.255
  network 10.5.1.0 0.0.0.255
  network 10.7.1.0 0.0.0.255
  network 10.10.3.9 0.0.0.0
  mpls-te enable
#
return
```

步骤4 配置LSR_4

```
#
 sysname LSR_4
#
mpls lsr-id 10.10.4.9
mpls   //使能MPLS TE
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet1/0/0   //接口使能MPLS TE
 ip address 10.3.1.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface LoopBack1
 ip address 10.10.4.9 255.255.255.255
#
ospf 1   //配置OSPF路由
 opaque-capability enable
 area 0.0.0.0
  network 10.3.1.0 0.0.0.255
  network 10.10.4.9 0.0.0.0
  mpls-te enable
#
return
```

步骤5 配置LSR_5

```
#
 sysname LSR_5
```

 版权所有 © 华为技术有限公司

```
#
mpls lsr-id 10.10.5.9
mpls   //使能MPLS TE
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet1/0/0   //接口使能MPLS TE
 ip address 10.4.1.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet2/0/0
 ip address 10.5.1.1 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface LoopBack1
 ip address 10.10.5.9 255.255.255.255
#
ospf 1   //配置OSPF路由
 opaque-capability enable
 area 0.0.0.0
  network 10.4.1.0 0.0.0.255
  network 10.5.1.0 0.0.0.255
  network 10.10.5.9 0.0.0.0
  mpls-te enable
#
return
```

步骤6 配置LSR_6

```
#
 sysname LSR_6
#
mpls lsr-id 10.10.6.9
mpls   //使能MPLS TE
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet1/0/0   //接口使能MPLS TE
 ip address 10.6.1.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface GigabitEthernet2/0/0
 ip address 10.7.1.1 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface LoopBack1
 ip address 10.10.6.9 255.255.255.255
#
ospf 1   //配置OSPF路由
 opaque-capability enable
 area 0.0.0.0
  network 10.6.1.0 0.0.0.255
  network 10.7.1.0 0.0.0.255
  network 10.10.6.9 0.0.0.0
  mpls-te enable
#
return
```

步骤7 验证配置结果

将LSR_2的GE2/0/0接口Shutdown后，在LSR_1上执行**display mpls te tunnel-interface**命令，可以看到隧道状态为“Up”，说明主隧道处于Frr-in-use状态的同

 版权所有 © 华为技术有限公司

时，正在创建普通备份的CR-LSP和恢复主CR-LSP。即当主CR-LSP故障后，系统启用TE FRR旁路保护隧道（即主CR-LSP处于Frr-in-use状态）并尝试恢复主CR-LSP的同时，也会尝试创建备份CR-LSP。

----结束

配置注意事项

- 在采用RSVP-TE动态建立CR-LSP时，必须配置IGP的TE扩展（目前支持OSPF TE和ISIS TE）。在不配置IGP的TE扩展时计算出的路径是由IGP路由得到的，而不是CSPF计算出来的。
- 只有使用RSVP-TE信令协议建立的MPLS TE隧道支持FRR功能。
- 同一个Tunnel接口不能同时作为旁路隧道和备份隧道。
- 同一个Tunnel接口不能同时作为旁路隧道和主隧道。
- 配置旁路隧道时，需要先规划好它所保护的链路或节点，并确保该旁路隧道不会经过它所保护的链路或节点，否则不能真正起到保护作用。

 版权所有 © 华为技术有限公司

12 部署 WLAN AP

12.1 配置无线用户接入WLAN示例
12.2 配置安全策略为WEP认证（open-system+WEP加密）的业务示例
12.3 配置安全策略为WPA认证（PSK认证+TKIP加密）的业务示例
12.4 配置安全策略为WPA2认证（PSK认证+CCMP加密）的业务示例
12.5 配置安全策略为WAPI认证的业务示例
12.6 配置WLAN QoS策略的业务示例

12.1 配置无线用户接入 WLAN 示例

规格

仅适用于AR651W-X4、AR651W-8P、AR651W、AR657W、AR303W、AR611W-S、AR611W、AR611W-LTE4CN、AR611W-LTE6EA、AR617VW、AR617VW-LTE4、AR617VW-LTE4EA和AR6120-VW路由器。

组网需求

如**图12-1**所示，企业使用WLAN技术为用户提供方便的无线上网服务。其中，设备作为FAT AP，同时作为DHCP Server给无线用户分配IP地址，并以NAT转换方式提供无线用户接入Network功能。

在GigabitEthernet1/0/0接口上配置NAT转换，并配置其公网地址为1.1.1.1/24，对端运营商侧地址为1.1.1.2/24。

图 12-1 配置 WLAN 基本业务示例图

版权所有 © 华为技术有限公司

操作步骤

步骤1 Router上的配置

```
#
dhcp enable
#
vlan batch 100
#
dot1x enable       //使能802.1X功能，V200R008及之后版本不再需要配置该命令
#
interface Vlanif100
 ip address 192.168.0.1 255.255.255.0
 dhcp select interface  //使能VLANIF 100接口的DHCP服务功能
#
interface Wlan-Bss1  //配置WLAN-BSS虚接口
 port hybrid tagged vlan 100
#
wlan
 wmm-profile name wmm id 0              //创建WMM模板，采用缺省配置
 traffic-profile name traffic id 0      //创建流量模板，采用缺省配置
 security-profile name security id 0    //创建安全模板
  security-policy wpa2                  //配置安全策略为WPA2
  wpa2 authentication-method psk pass-phrase cipher %^%#Q-%d~;.Aj!
<@qOUJ=vMG~rie2vkWOOUq>`5f73RU%^%# encryption-method ccmp            //配置CCMP数据加密方式
 service-set name huawei id 0           //创建服务集
  Wlan-Bss 1                           //配置服务集绑定WLAN-BSS 1接口
  ssid huawei                          //指定服务集SSID
  traffic-profile id 0                 //配置服务集绑定流量模板
  security-profile id 0                //配置服务集绑定安全模板
 radio-profile name radio-1 id 1        //创建射频模板
  wmm-profile id 1                      //配置射频模板绑定WMM模板
#
interface Wlan-Radio0/0/0
 radio-profile id 0       //将射频口绑定射频模板，设备出厂时，默认已在WLAN视图下创建ID为0的射频模板，且在wlan-radio0/0/0接口下已绑定该射频模板。如果设备以默认的出厂配置启动，则无法在wlan-radio0/0/0接口上删除该射频模板。
 service-set id 0 wlan 1  //将射频口绑定服务集
#
acl number 2000                         //配置编号为2000的编号型访问控制列表
 rule 1 permit source 192.168.0.0 0.0.0.255  //配置规则1，指定源地址为192.168.0.0网段的为符合条件的数据包
#
 nat address-group 1 1.1.1.100 1.1.1.200  //配置公网地址池
#
interface GigabitEthernet1/0/0
 ip address 1.1.1.1 255.255.255.0  //配置公网IP地址
 nat outbound 2000 address-group 1      //配置ACL和地址池关联
#
ip route-static 0.0.0.0 0.0.0.0 1.1.1.2  //配置缺省路由
#
```

步骤2 验证配置结果

无线接入用户可以搜索到SSID标识为huawei的WLAN网络，可以正常使用WLAN上网服务。

在Router上执行**display station assoc-info interface wlan-radio0/0/0** [**service-set** *service-set-id*]命令，可查询Radio上或Radio上指定service-set上所有关联的无线终端接入信息。

----结束

配置注意事项

- 路由器的缺省国家码为CN，用户可以根据实际情况重新设置，方便识别和管理。
- 创建WMM模板后，模板内的参数均自动配置为缺省值，用户可以根据实际情况重新进行配置。

 版权所有 © 华为技术有限公司

- 创建流量模板后，模板内的参数均自动配置为缺省值，用户可以根据实际情况重新进行配置。
- 配置安全模板时，用户可以根据实际需求选择安全策略，安全策略包括WEP、WPA、WPA2和WAPI。

12.2 配置安全策略为 WEP 认证（open-system+WEP 加密）的业务示例

规格

仅适用于AR651W-X4、AR651W-8P、AR651W、AR657W、AR303W、AR611W-S、AR611W、AR611W-LTE4CN、AR611W-LTE6EA、AR617VW、AR617VW-LTE4、AR617VW-LTE4EA和AR6120-VW路由器。

组网需求

如图12-2所示，设备作为FAT AP，为用户提供WLAN服务，用户可以搜索到SSID为huawei的无线网络，采用的安全策略为WEP认证（open-system+WEP加密）。

图 12-2 配置安全策略为 WEP 认证（open-system+WEP 加密）的业务示例图

操作步骤

步骤1 Router上的配置

```
#
vlan 10
#
dhcp enable  //使能DHCP功能
#
interface Vlanif10
 ip address 192.168.1.1 255.255.255.0
 dhcp select interface  //使能VLANIF 10接口的DHCP服务功能
#
interface Wlan-Bss0  //配置WLAN-BSS虚接口
 port hybrid tagged vlan 10
#
wlan
 wmm-profile name wmm id 1              //创建WMM模板，模板参数采用缺省值
 traffic-profile name traffic id 1      //创建流量模板，模板参数采用缺省值
 security-profile name security id 1    //创建安全模板security采用开放式系统认证+WEP-40加密
  wep authentication-method open-system data-encrypt
  wep key wep-40 pass-phrase 0 cipher %^%#Q-%d~;.Aj!<@qOUJ=vMG~rie2vkWOOUq>`5f73RU%^%#    //
配置WEP加密采用WEP-40方式，仅ARV200R002C01以后版本支持关键字cipher
 service-set name service-set id 0  //创建服务集
  Wlan-Bss 0               //配置服务集绑定WLAN-BSS 0接口
  ssid huawei              //指定服务集SSID
  traffic-profile id 1     //配置服务集绑定流量模板
```


版权所有 © 华为技术有限公司

```
 security-profile id 1      //配置服务集绑定安全模板
 radio-profile name radio-1 id 1  //创建射频模板
  wmm-profile id 1                //配置射频模板绑定WMM模板
#
interface Wlan-Radio0/0/0
 radio-profile id 1       //将射频口绑定射频模板
 service-set id 0 wlan 1  //将射频口绑定服务集
```

步骤2 验证配置结果

无线接入用户可以搜索到SSID为huawei的WLAN网络，用户输入密钥即可以正常使用WLAN服务。

在Router上执行**display station assoc-info interface wlan-radio0/0/0** [**service-set** *service-set-id*]命令，可查询Radio上或Radio上指定service-set上所有关联的无线终端接入信息。

----结束

配置注意事项

- 路由器的缺省国家码为CN，用户可以根据实际情况重新设置，方便识别和管理。

12.3 配置安全策略为 WPA 认证（PSK 认证+TKIP 加密）的业务示例

规格

仅适用于AR651W-X4、AR651W-8P、AR651W、AR657W、AR303W、AR611W-S、AR611W、AR611W-LTE4CN、AR611W-LTE6EA、AR617VW、AR617VW-LTE4、AR617VW-LTE4EA和AR6120-VW路由器。

组网需求

如图12-3所示，设备作为FAT AP，为用户提供WLAN服务，用户可以搜索到名为huawei的无线网络，采用的安全策略为WPA-PSK认证+TKIP加密的方式。

图 12-3 配置安全策略为 WPA 认证（PSK 认证+TKIP 加密）的业务示例

操作步骤

步骤1 Router上的配置

```
#
vlan 102
#
dhcp enable  //使能DHCP功能
#
```


版权所有 © 华为技术有限公司

```
dot1x enable //使能802.1x功能（PSK密钥交互承载在EAPOL报文之上，所以需要开启dot1x），V200R008及之后版本不再需要配置该命令
#
interface Vlanif102
 ip address 192.168.1.1 255.255.255.0
 dhcp select interface  //使能VLANIF接口的DHCP服务功能
#
interface Wlan-Bss1     //配置WLAN-BSS虚接口
 port hybrid tagged vlan 102
#
wlan
 wmm-profile name wmm id 1              //创建WMM模板，模板参数采用缺省值
 traffic-profile name traffic id 1      //创建流量模板，模板参数采用缺省值
 security-profile name security id 1    //创建安全模板security采用wpa+psk+tkip安全策略
                                  也可以采用（wpa+psk+CCMP）安全策略，只需将encryption-method后面的加密方式改为CCMP即可
  security-policy wpa
  wpa authentication-method psk pass-phrase cipher %^%#Q-%d~;.Aj!<@qOUJ=vMG~rie2vkWOOUq>`5f73RU%^%# encryption-method tkip
 service-set name ss-1 id 0  //创建服务集
  Wlan-Bss 1                 //配置服务集绑定WLAN-BSS 1接口
  ssid huawei                //指定服务集ID
  traffic-profile id 1       //配置服务集绑定流量模板
  security-profile id 1      //配置服务集绑定安全模板
 radio-profile name radio-1 id 1  //创建射频模板
  wmm-profile id 1                //配置射频模板绑定WMM模板
#
interface Wlan-Radio0/0/0
 radio-profile id 1       //将射频口绑定射频模板
 service-set id 0 wlan 1  //将射频口绑定服务集
```

步骤2 验证配置结果

无线用户可以搜索到SSID为huawei的WLAN网络，用户需要输入PSK预共享密钥0123456789才能正常使用WLAN服务。

在Router上执行**display security-profile** { **id** *profile-id* | **name** *profile-name* }命令，可以查询到接入安全的配置策略。

在Router上执行**display station assoc-info interface wlan-radio0/0/0** [**service-set** *service-set-id*]命令，可查询Radio上或Radio上指定service-set上所有关联的无线终端接入信息。

----结束

配置注意事项

- 路由器的缺省国家码为CN，用户可以根据实际情况重新设置，方便识别和管理。

12.4 配置安全策略为 WPA2 认证（PSK 认证+CCMP 加密）的业务示例

规格

仅适用于AR651W-X4、AR651W-8P、AR651W、AR657W、AR303W、AR611W-S、AR611W、AR611W-LTE4CN、AR611W-LTE6EA、AR617VW、AR617VW-LTE4、AR617VW-LTE4EA和AR6120-VW路由器。

 版权所有 © 华为技术有限公司

组网需求

如图12-4所示，设备作为FAT AP，为用户提供WLAN服务，用户可以搜索到名为huawei的无线网络，采用的安全策略为WPA2-PSK认证+CCMP加密的方式。

图 12-4 配置安全策略为 WPA2 认证（PSK 认证+CCMP 加密）的业务示例

操作步骤

步骤1 Router上的配置

```
#
vlan 101
#
dhcp enable  //使能DHCP功能
#
dot1x enable //使能802.1x功能（PSK密钥交互承载在EAPOL报文之上，所以需要开启dot1x），V200R008及之后版本不再需要配置该命令
#
interface Vlanif101
 ip address 192.168.0.1 255.255.255.0
 dhcp select interface  //使能VLANIF接口的DHCP服务功能
#
interface Wlan-Bss1  //配置WLAN-BSS虚接口
 port hybrid tagged vlan 101
#
wlan
 wmm-profile name wmm id 1              //创建WMM模板，模板参数采用缺省值
 traffic-profile name traffic id 1      //创建流量模板，模板参数采用缺省值
 security-profile name security id 1    //创建安全模板security采用wpa2+psk+CCMP安全策略
                                        也可以采用（wpa2+psk+TKIP）安全策略，只需将encryption-method后面的加密方式改为TKIP即可
  security-policy wpa2
  wpa2 authentication-method psk pass-phrase cipher %^%#Q-%d~;.Aj!<@qOUJ=vMG~rie2vkWOOUq>`5f73RU%^%# encryption-method ccmp
 service-set name ss-1 id 0  //创建服务集
  Wlan-Bss 1                //配置服务集绑定WLAN-BSS 1接口
  ssid huawei               //指定服务集ID
  traffic-profile id 1      //配置服务集绑定流量模板
  security-profile id 1     //配置服务集绑定安全模板
 radio-profile name radio-1 id 1  //创建射频模板
  wmm-profile id 1              //配置射频模板绑定WMM模板
#
interface Wlan-Radio0/0/0
 radio-profile id 1       //将射频口绑定射频模板
 service-set id 0 wlan 1  //将射频口绑定服务集
```

步骤2 验证配置结果

无线用户可以搜索到SSID为huawei的WLAN网络，用户需要输入PSK预共享密钥才能正常使用WLAN服务。

在Router上执行**display security-profile** { **id** *profile-id* | **name** *profile-name* }命令，可以查询到接入安全的配置策略。

版权所有 © 华为技术有限公司

在Router上执行**display station assoc-info interface wlan-radio0/0/0** [**service-set** *service-set-id*]命令，可查询Radio上或Radio上指定service-set上所有关联的无线终端接入信息。

----结束

配置注意事项

- 路由器的缺省国家码为CN，用户可以根据实际情况重新设置，方便识别和管理。

12.5 配置安全策略为 WAPI 认证的业务示例

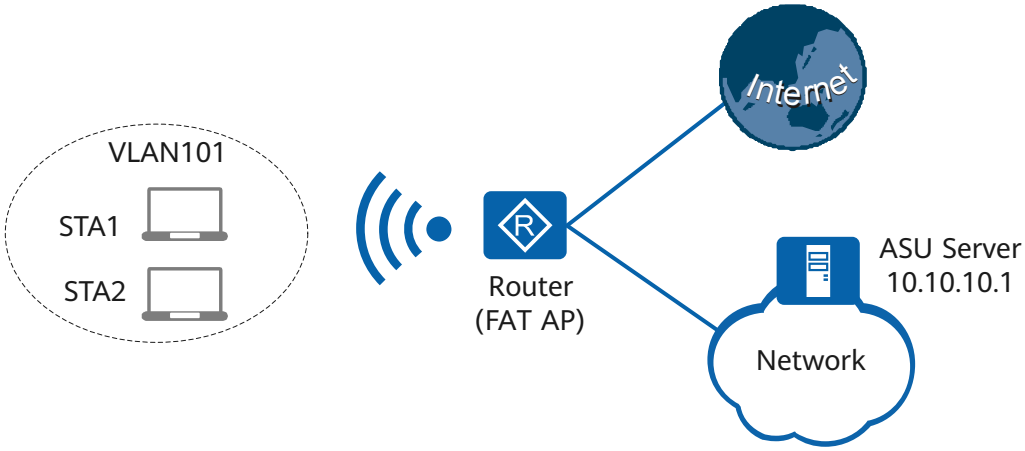
规格

仅适用于AR651W-X4、AR651W-8P、AR651W、AR657W、AR303W、AR611W-S、AR611W、AR611W-LTE4CN、AR611W-LTE6EA、AR617VW、AR617VW-LTE4、AR617VW-LTE4EA和AR6120-VW路由器。

组网需求

如图12-5所示，设备作为FAT AP，为用户提供WLAN服务，用户需要搜索到名为huawei的无线网络，采用的安全策略为WAPI方式。

图 12-5 配置安全策略为 WAPI 认证的业务示例



操作步骤

步骤1 Router上的配置

```
#
vlan batch 101
#
dhcp enable  //使能DHCP功能
#
interface Vlanif101
 ip address 192.168.0.1 255.255.255.0
 dhcp select interface  //使能VLANIF接口的DHCP服务功能
#
interface Wlan-Bss1  //配置WLAN-BSS虚接口
 port hybrid tagged vlan 101
#
wlan
```


版权所有 © 华为技术有限公司

```
 wmm-profile name wmm id 1              //创建WMM模板，模板参数采用缺省值
 traffic-profile name traffic id 1      //创建流量模板，模板参数采用缺省值
 security-profile name security id 0    //创建安全模板security
  security-policy wapi                  //配置安全模板采用WAPI方式认证
  wapi asu ip 10.10.10.1                //配置ASU服务器的IP地址为10.10.10.1
  wapi import certificate ap file-name flash:/huawei-ap.cer          //指定认证证书路径和文件名
  wapi import certificate asu file-name flash:/huawei-asu.cer        //指定ASU认证证书路径和文件名
  wapi import certificate issuer file-name flash:/huawei-issuer.cer  //指定Issuer认证证书路径和文件名
  wapi import private-key file-name flash:/huawei-ap.cer             //指定私钥证书路径和文件名
  service-set name ss-1 id 0  //创建服务集
  Wlan-Bss 1                  //配置服务集绑定WLAN-BSS 1接口
  ssid huawei                 //指定服务集ID
  traffic-profile id 1        //配置服务集绑定流量模板
  security-profile id 1       //配置服务集绑定安全模板
 radio-profile name radio-1 id 1  //创建射频模板
  wmm-profile id 1                //配置射频模板绑定WMM模板
#
interface Wlan-Radio0/0/0
 radio-profile id 1       //将射频口绑定射频模板
 service-set id 0 wlan 1  //将射频口绑定服务集
```

步骤2 验证配置结果

在Router上执行**display security-profile** { **id** *profile-id* | **name** *profile-name* }命令，可以查询到接入安全的配置策略。

在Router上执行**display station assoc-info interface wlan-radio0/0/0** [**service-set** *service-set-id*]命令，可查询Radio上或Radio上指定service-set上所有关联的无线终端接入信息。

----结束

配置注意事项

- 路由器的缺省国家码为CN，用户可以根据实际情况重新设置，方便识别和管理。
- 配置前请确保Router与ASU Server之间路由可达。
- ASU服务器也需做相关配置，这里不做介绍。
- 配置安全模板security的安全策略时，请确保AP的认证证书为huawei-ap.cer，ASU认证证书为huawei-asu.cer，Issuer认证证书为huawei-issuer.cer，私钥证书为huawei-ap.cer均已保存在设备上。

12.6 配置 WLAN QoS 策略的业务示例

规格

仅适用于AR651W-X4、AR651W-8P、AR651W、AR657W、AR303W、AR611W-S、AR611W、AR611W-LTE4CN、AR611W-LTE6EA、AR617VW、AR617VW-LTE4、AR617VW-LTE4EA和AR6120-VW路由器。

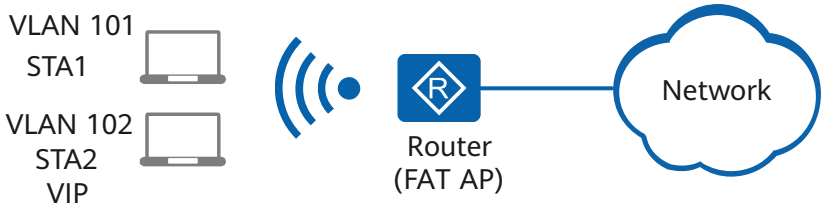
组网需求

如图12-6所示，STA1、STA2通过设备连接到网络。设备作为FAT AP，其中STA2为VIP客户。要求：

- 优先满足接入用户的视频需求。
- 当网络带宽不足时，优先满足VIP客户的使用需求。

 版权所有 © 华为技术有限公司

图 12-6 配置 WLAN QoS 策略示例图



操作步骤

步骤1 Router上的配置

```
#
dhcp enable  //使能DHCP服务功能
#
vlan batch 101 to 102
#
interface Vlanif101
 ip address 192.168.0.1 255.255.255.0
 dhcp select interface  //使能VLANIF接口的DHCP服务功能
#
interface Vlanif102
 ip address 192.168.1.1 255.255.255.0
 dhcp select interface
#
interface Wlan-Bss1  //配置WLAN-BSS虚接口
 port hybrid tagged vlan 101
#
interface Wlan-Bss2
 port hybrid tagged vlan 102
#
wlan
 wmm-profile name wmmf id 0
 wmm-profile name huawei-vi id 1  //创建名为“huawei-vi”的WMM模板
  wmm edca ap ac-vi aifsn 1 ecw ecwmin 1 ecwmax 1 txoplimit 36  //修改AP发送报文时视频队列的EDCA参数，提高视频业务的优先级
  wmm edca client ac-vi aifsn 1 ecw ecwmin 1 ecwmax 3 txoplimit 36  //修改STA发送报文时视频队列的EDCA参数，提高视频业务的优先级
 traffic-profile name traf id 0
 traffic-profile name huawei id 1      //创建名为“huawei”的流量模板
  rate-limit client up 512             //配置STA上行限速为512Kbps
  rate-limit vap up 1024               //配置VAP上行限速为1024Kbps
 traffic-profile name huawei-vip id 2  //创建名为“huawei-vip”的流量模板
  rate-limit client up 1024            //配置STA上行限速为1024Kbps
  rate-limit vap up 2048               //配置VAP上行限速为2048Kbps
 security-profile name secf id 0
 security-profile name huawei id 1  //创建名为“huawei”的安全模板，采用缺省参数
 service-set name huawei-1 id 0  //创建名为“huawei-1”的服务集
  Wlan-Bss 1
  ssid huawei-1         //配置服务集的网络标识符为“huawei-1”
  traffic-profile id 1  //配置服务集绑定的流量模板为“huawei”
  security-profile id 1
 service-set name huawei-2 id 1  //创建名为“huawei-2”的服务集
  Wlan-Bss 2
  ssid huawei-2         //配置服务集的网络标识符为“huawei-2”
  traffic-profile id 2  //配置服务集绑定的流量模板为“huawei-vip”
  security-profile id 1
 radio-profile name radiof id 0
  wmm-profile id 0
 radio-profile name huawei-vi id 1
  wmm-profile id 1
#
interface Wlan-Radio0/0/0
 radio-profile id 1       //配置AP的射频口绑定射频模板“huawei-vi”
```


版权所有 © 华为技术有限公司

```
service-set id 0 wlan 1  //配置AP的射频口绑定服务集“huawei-1”
service-set id 1 wlan 2  //配置AP的射频口绑定服务集“huawei-2”
```

步骤2 验证配置结果

无线用户可以搜索到2个WLAN网络，其网络标识分别为huawei-1和huawei-2。STA1、STA2分别选择huawei-1和huawei-2的WLAN网络。

在Router上执行**display station assoc-info interface wlan-radio0/0/0** [**service-set** *service-set-id*]命令，可查询Radio上或Radio上指定service-set上所有关联的无线终端接入信息。

----结束

配置注意事项

- 路由器的缺省国家码为CN，用户可以根据实际情况重新设置，方便识别和管理。
- 通过修改WMM模板中AC_VI(视频)队列的AIFSN（Arbitration Inter Frame Spacing Number，仲裁帧间隙数）、ECWmin（Exponent form of CWmin，最小竞争窗口指数形式）、ECWmax（Exponent form of CWmax，最大竞争窗口指数形式）和TXOPLimit（Transmission Opportunity Limit，传输机会限制）四个参数可以提升视频业务的优先级。

 版权所有 © 华为技术有限公司

13 部署 WLAN AC

13.1 配置小型网络WLAN基本业务示例（AC通过二层口管理AP）
13.2 配置中型网络WLAN基本业务示例（AC通过二层口管理AP）
13.3 配置大型网络WLAN基本业务示例（AC通过二层口管理AP）
13.4 配置小型网络WLAN基本业务示例（AC通过三层口管理AP）
13.5 配置中型网络WLAN基本业务示例（AC通过三层口管理AP）
13.6 配置家庭消费用户无线上网示例（AC通过三层口管理AP）
13.7 配置安全策略为Portal认证的业务示例
13.8 配置安全策略为802.1X认证的业务示例
13.9 配置安全策略为MAC认证的业务示例

13.1 配置小型网络 WLAN 基本业务示例（AC 通过二层口管理 AP）

规格

适用于支持WLAN AC功能的款型，V200R008C00及更高版本。

组网需求

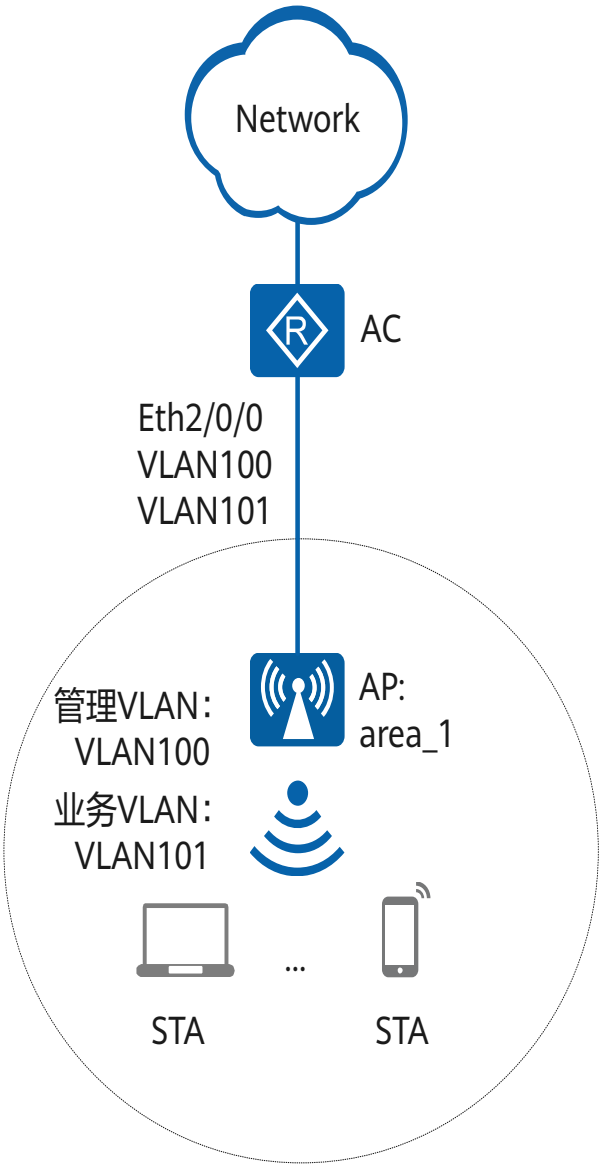
如**图13-1**所示，AC直接与AP连接。现某企业分支机构为了保证工作人员可以随时随地的访问公司网络，需要通过部署WLAN基本业务实现移动办公。

具体要求如下：

- 提供名为“wlan-net”的无线网络，密码为“YsHsjx_202206”。
- 工作人员分配到的IP地址网段为10.10.11.0/24。

版权所有 © 华为技术有限公司

图 13-1 配置小型网络 WLAN 基本业务组网图



操作步骤

步骤1 AC上的配置

```
#
 sysname AC
#
vlan batch 100 to 101     //创建VLAN100（管理VLAN）和VLAN101（业务VLAN）
#
dhcp enable          //使能DHCP功能
#
interface Vlanif100
 ip address 10.10.10.1 255.255.255.0
 dhcp select interface     //使能VLANIF100接口的DHCP服务功能，以便AC能够为AP分配IP地址
#
interface Vlanif101
```


版权所有 © 华为技术有限公司

```
 ip address 10.10.11.1 255.255.255.0
 dhcp select interface    //使能VLANIF101接口的DHCP服务功能，以便AC能够为AP下的STA分配IP地址
#
interface Ethernet2/0/0
 port link-type trunk
 port trunk pvid vlan 100                  //配置Eth2/0/0接口的缺省VLAN是
VLAN100
 port trunk allow-pass vlan 100 to 101     //配置Eth2/0/0接口加入VLAN100和
VLAN101
 port-isolate enable group 1
#
capwap source interface vlanif100      //指定AC的源接口
#
wlan ac
 security-profile name wlan-security  //创建安全模板
  security wpa2 psk pass-phrase %^%#m"tz0f>~7.[`^6RWdzwCy16hJj/Mc!,}s`X*B]}A%^%# aes   //配置采用
PSK认证方式和AES加密方式，并且以密文形式显示用户口令
 ssid-profile name wlan-ssid  //创建SSID模板
  ssid wlan-net               //指定无线网络名称为wlan-net
 vap-profile name wlan-vap    //创建VAP模板
  service-vlan vlan-id 101    //配置业务VLAN为VLAN101
  ssid-profile wlan-ssid      //引用SSID模板至VAP模板
  security-profile wlan-security            //引用安全模板至VAP模板
 regulatory-domain-profile name domain1      //创建域管理模板，配置国家码标识，默认情况下是中国CN，如
果无变化，可以不配置
 ap-group name ap-group1                    //创建AP组
  regulatory-domain-profile domain1          //引用域模板至AP组
  radio 0
   vap-profile wlan-vap wlan 1              //引用VAP模板至射频
  radio 1
   vap-profile wlan-vap wlan 1              //引用VAP模板至射频
  radio 2
   vap-profile wlan-vap wlan 1              //引用VAP模板至射频
 ap-id 0 type-id 19 ap-mac 00e0-fc76-e360 ap-sn 210235554710CB000042       //离线添加AP设备
  ap-name area_1           //配置AP名称
  ap-group ap-group1       //配置AP加入AP组
#
return
```

步骤2 验证配置结果

WLAN业务配置完成后，通过执行命令**display ap all**查看AP上线信息，当“State”项显示为“nor”时，表示AP已成功上线。

WLAN业务配置完成后，通过执行命令**display vap ssid wlan-net**查看VAP信息，当“Status”项显示为“ON”时，表示AP对应的射频上的VAP已创建成功。

STA搜索到名为“wlan-net”的无线网络，输入密码“YsHsjx_202206”并正常关联后，在AC上执行**display station ssid wlan-net**命令，可以查看到用户已经接入到无线网络“wlan-net”中。

STA接入到无线网络“wlan-net”后，可以在系统视图下，执行命令**display access-user**查看接入用户分配到的IP地址。

----结束

配置注意事项

- WLAN业务配置完成后，需要通过**commit all**命令，提交AP的配置。
- 路由器的缺省国家码为CN，用户可以根据实际情况重新设置，方便识别和管理。
- 离线添加AP后，需要保证AP状态是**normal**，如果AP状态不是**normal**，请排查故障并最终使AP状态为**normal**。

 版权所有 © 华为技术有限公司

13.2 配置中型网络 WLAN 基本业务示例（AC 通过二层口管理 AP）

规格

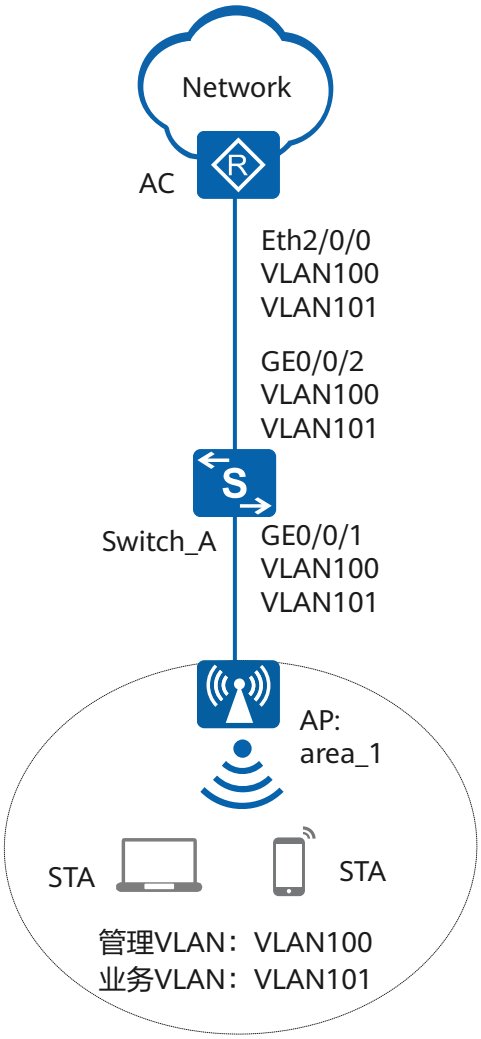
适用于支持WLAN AC功能的款型，V200R008C00及更高版本。

组网需求

如图13-2，AC通过接入交换机Switch_A与AP连接，并管理AP。

某中型企业存在无线办公的业务需求，需要在办公区的每个办公室内都部署WLAN网络，用户希望能够在AC上对用户进行集中控制和管理。

图 13-2 配置中型网络 WLAN 基本业务组网图



版权所有 © 华为技术有限公司

操作步骤

步骤1 交换机上的配置

```
#
sysname Switch_A
#
vlan batch 100 to 101        //创建VLAN100（管理VLAN）和VLAN101（业务VLAN）
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk pvid vlan 100    //配置GE0/0/1接口的缺省VLAN是VLAN100
 port trunk allow-pass vlan 100 to 101    //配置GE0/0/1接口加入VLAN100和VLAN101
 port-isolate enable group 1              //配置GE0/0/1接口的端口隔离功能
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 100 to 101    //配置GE0/0/2接口加入VLAN100和VLAN101
#
return
```

步骤2 AC上的配置

```
#
 sysname AC
#
vlan batch 100 to 101        //创建VLAN100（管理VLAN）和VLAN101（业务VLAN）
#
dhcp enable                  //使能DHCP功能
#
interface Vlanif100
 ip address 10.10.10.1 255.255.255.0
 dhcp select interface       //使能VLANIF100接口的DHCP服务功能，以便AC能够为AP分配IP地址
#
interface Vlanif101
 ip address 10.10.11.1 255.255.255.0
 dhcp select interface       //使能VLANIF101接口的DHCP服务功能，以便AC能够为AP下的STA分配IP地址
#
interface Ethernet2/0/0
 port link-type trunk
 port trunk allow-pass vlan 100 to 101    //配置Eth2/0/0接口加入VLAN100和VLAN101
 port-isolate enable group 1              //配置Eth2/0/0接口的端口隔离功能
#
capwap source interface vlanif100       //指定AC的源接口
#
wlan ac
 security-profile name wlan-security   //创建安全模板
  security wpa2 psk pass-phrase %^%#m"tz0f>~7.[`^6RWdzwCy16hJj/Mc!,}s`X*B]}A%^%# aes   //配置采用
PSK认证方式和AES加密方式，并且以密文形式显示用户口令
 ssid-profile name wlan-ssid  //创建SSID模板
  ssid wlan-net               //指定无线网络名称为wlan-net
 vap-profile name wlan-vap    //创建VAP模板
  service-vlan vlan-id 101    //配置业务VLAN为VLAN101
  ssid-profile wlan-ssid      //引用SSID模板至VAP模板
  security-profile wlan-security            //引用安全模板至VAP模板
 regulatory-domain-profile name domain1      //创建域管理模板，配置国家码标识，默认情况下是中国CN，如
果无变化，可以不配置
 ap-group name ap-group1                    //创建AP组
  regulatory-domain-profile domain1          //引用域模板至AP组
  radio 0
   vap-profile wlan-vap wlan 1               //引用VAP模板至射频
  radio 1
   vap-profile wlan-vap wlan 1               //引用VAP模板至射频
  radio 2
   vap-profile wlan-vap wlan 1               //引用VAP模板至射频
 ap-id 0 type-id 19 ap-mac 00e0-fc76-e360 ap-sn 210235554710CB000042       //离线添加AP设备
  ap-name area_1             //配置AP名称
  ap-group ap-group1         //配置AP加入AP组
#
return
```

 版权所有 © 华为技术有限公司

步骤3 验证配置结果

WLAN业务配置完成后，通过执行命令**display ap all**查看AP上线信息，当“State”项显示为“nor”时，表示AP已成功上线。

WLAN业务配置完成后，通过执行命令**display vap ssid wlan-net**查看VAP信息，当“Status”项显示为“ON”时，表示AP对应的射频上的VAP已创建成功。

STA搜索到名为“wlan-net”的无线网络，输入密码“YsHsjx_202206”并正常关联后，在AC上执行**display station ssid wlan-net**命令，可以查看到用户已经接入到无线网络“wlan-net”中。

STA接入到无线网络“wlan-net”后，可以在系统视图下，执行命令**display access-user**查看接入用户分配到的IP地址。

----结束

配置注意事项

- WLAN业务配置完成后，需要通过**commit all**命令，提交AP的配置。
- 路由器的缺省国家码为CN，用户可以根据实际情况重新设置，方便识别和管理。
- 离线添加AP后，需要保证AP状态是**normal**，如果AP状态不是**normal**，请排查故障并最终使AP状态为**normal**。

13.3 配置大型网络 WLAN 基本业务示例（AC 通过二层口管理 AP）

规格

适用于支持WLAN AC功能的款型，V200R008C00及更高版本。

组网需求

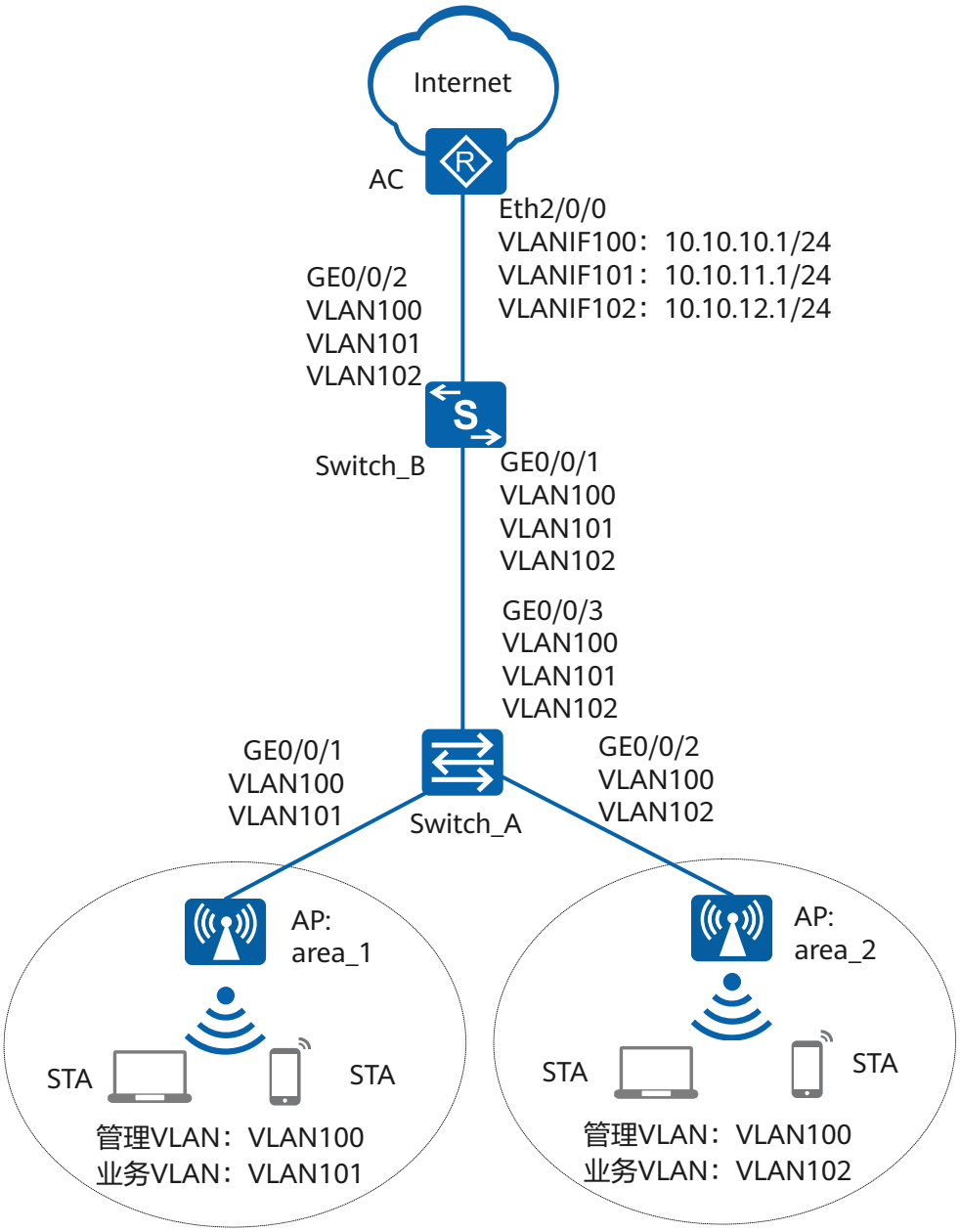
如图13-3所示，某大型企业的现网中，汇聚交换机Switch_B下行连接接入交换机Switch_A，上行连接Router。用户希望能在尽可能少的更改现有组网架构的情况下部署WLAN网络。

用户的具体需求为：

- 企业办公楼的前台大厅部署SSID为“guest”的无线网络，为来访的客户提供无线网络接入。
- 办公区域部署SSID为“employee”的无线网络，为企业员工提供无线网络接入。

 版权所有 © 华为技术有限公司

图 13-3 配置大型网络 WLAN 基本业务组网图



操作步骤

步骤1 交换机A上的配置

```
#
sysname SwitchA
#
vlan batch 100 to 102            //创建VLAN100（管理VLAN）、VLAN101（业务VLAN）和VLAN102（业务VLAN）
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk pvid vlan 100        //配置GE0/0/1接口的缺省VLAN是VLAN100
 port trunk allow-pass vlan 100 to 101    //配置GE0/0/1接口加入VLAN100和VLAN101
 port-isolate enable group 1             //配置GE0/0/1接口的端口隔离功能
#
interface GigabitEthernet0/0/2
```


版权所有 © 华为技术有限公司

```
 port link-type trunk
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100 102       //配置GE0/0/2接口加入VLAN100和VLAN102
 port-isolate enable group 1
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 100 to 102    //配置GE0/0/3接口加入VLAN100、VLAN101和VLAN102
#
return
```

步骤2 交换机B上的配置

```
#
sysname SwitchB
#
vlan batch 100 to 102             //创建VLAN100（管理VLAN）、VLAN101（业务VLAN）和VLAN102（业务
VLAN）
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100 to 102    //配置GE0/0/1接口加入VLAN100、VLAN101和
VLAN102
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 100 to 102    //配置GE0/0/2接口加入VLAN100、VLAN101和VLAN102
#
return
```

步骤3 AC上的配置

```
#
 sysname AC
#
vlan batch 100 to 102     //创建VLAN100（管理VLAN）、VLAN101（业务VLAN）和VLAN102（业务VLAN）
#
dhcp enable               //使能DHCP功能
#
interface Vlanif100
 ip address 10.10.10.1 255.255.255.0
 dhcp select interface    //使能VLANIF100接口的DHCP服务功能，以便AC能够为AP分配IP地
址
#
interface Vlanif101
 ip address 10.10.11.1 255.255.255.0
 dhcp select interface    //使能VLANIF101接口的DHCP服务功能，以便AC能够为AP下的STA分配IP地址
#
interface Vlanif102
 ip address 10.10.12.1 255.255.255.0
 dhcp select interface    //使能VLANIF102接口的DHCP服务功能，以便AC能够为AP下的STA分配IP地
址
#
interface Ethernet2/0/0
 port link-type trunk
 port trunk allow-pass vlan 100 to 102      //配置Eth2/0/0接口加入VLAN100、VLAN101和VLAN102
#
capwap source interface vlanif100      //指定AC的源接口
#
wlan ac
 security-profile name guest        //创建安全模板
  security wep share-key            //配置认证方式为share-key
  wep key 0 wep-40 pass-phrase %^%#z*z]6]#!|%n:n}Xz'mhKE{PfN|cIj*eU$jJYH48S%^%#        //配置WEP的
密钥
 security-profile name employee     //创建安全模板
  security wpa2 psk pass-phrase %^%#H{1<-b]4~'"*+Y:4-'/URy;$+,33UgQf)@9I(Yl]V%^%# aes   //配置采用
PSK认证方式和AES加密方式，并且以密文形式显示用户口令
 ssid-profile name guest  //创建SSID模板
  ssid guest              //指定无线网络名称为guest
 ssid-profile name employee  //创建SSID模板
  ssid employee              //指定无线网络名称为employee
```

 版权所有 © 华为技术有限公司

```
vap-profile name guest      //创建VAP模板
 service-vlan vlan-id 101   //配置业务VLAN为VLAN101
 ssid-profile guest         //引用SSID模板至VAP模板
 security-profile guest     //引用安全模板至VAP模板
vap-profile name employee      //创建VAP模板
 service-vlan vlan-id 102      //配置业务VLAN为VLAN102
 ssid-profile employee         //引用SSID模板至VAP模板
 security-profile employee     //引用安全模板至VAP模板
regulatory-domain-profile name domain1      //创建域管理模板
ap-group name guest                         //创建AP组
 regulatory-domain-profile domain1          //引用域模板至AP组
 radio 0
  vap-profile guest wlan 1              //引用VAP模板至射频
 radio 1
  vap-profile guest wlan 1              //引用VAP模板至射频
 radio 2
  vap-profile guest wlan 1              //引用VAP模板至射频
ap-group name default                       //创建AP组
ap-group name employee                      //创建AP组
 regulatory-domain-profile domain1          //引用域模板至AP组
 radio 0
  vap-profile employee wlan 1           //引用VAP模板至射频
 radio 1
  vap-profile employee wlan 1           //引用VAP模板至射频
 radio 2
  vap-profile employee wlan 1           //引用VAP模板至射频
ap-id 0 type-id 19 ap-mac 00e0-fc76-e360 ap-sn 210235554710CB000042       //离线添加AP设备
 ap-name area_1          //配置AP名称
 ap-group guest          //配置AP加入AP组
ap-id 1 type-id 19 ap-mac 00e0-fc74-9640 ap-sn 210235554710CB000075       //离线添加AP设备
 ap-name area_2          //配置AP名称
 ap-group employee       //配置AP加入AP组
#
return
```

步骤4 验证配置结果

WLAN业务配置完成后，通过执行命令**display vap ssid guest**和**display vap ssid employee**查看如下信息，当“Status”项显示为“ON”时，表示AP对应的射频上的VAP已创建成功。

STA搜索到名为“guest”和“employee”的无线网络，分别输入密码“YsHsjx_202206”和“YsHsjx_202207”并正常关联后，在AC上执行**display station ssid guest**和**display station ssid employee**命令，可以查看到用户已经分别接入到无线网络“guest”和“employee”中。

----结束

配置注意事项

- WLAN业务配置完成后，需要通过**commit all**命令，提交AP的配置。
- 路由器的缺省国家码为CN，用户可以根据实际情况重新设置，方便识别和管理。
- 离线添加AP后，需要保证AP状态是**normal**，如果AP状态不是**normal**，请排查故障并最终使AP状态为**normal**。

13.4 配置小型网络 WLAN 基本业务示例（AC 通过三层口管理 AP）

规格

适用于支持WLAN AC功能的款型，V200R008C00及更高版本。

 版权所有 © 华为技术有限公司

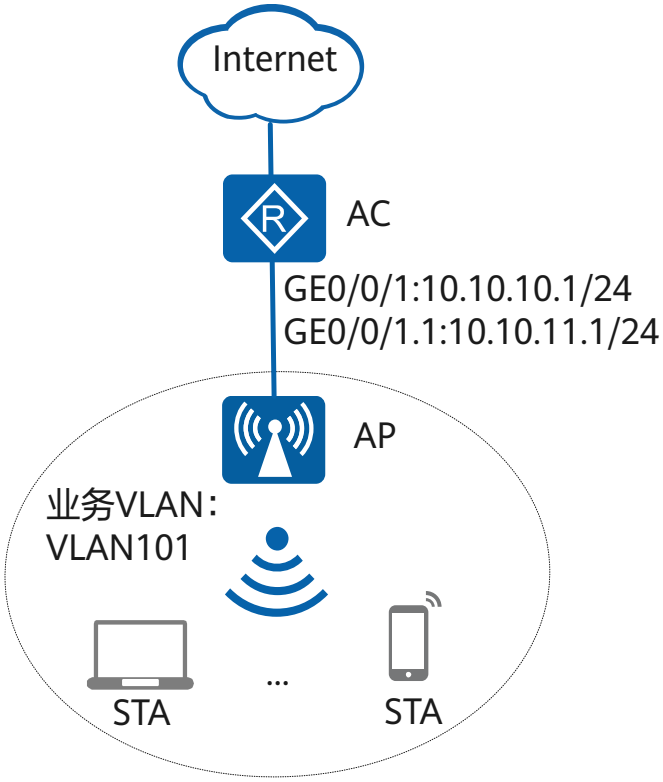
组网需求

如图13-4所示，某小型企业由于业务需要，希望员工能在企业内部随时随地的访问Internet，进行移动办公。该企业部署了一台AR路由器作为出口网关，希望同时在AR路由器上部署WLAN功能，为企业员工提供无线网络接入服务，实现移动办公。

在提供无线网络接入服务上，主要有如下需求：

- AR路由器作为AC，通过下挂AP的方式，为企业员工提供无线网络接入服务。
- 由于企业规模较小，终端用户数较少，AC下只需直连一台AP，即可满足所有终端用户的无线上网需求。AR路由器的二层接口已部署了其他业务，AP设备只能通过三层接口接入AC。
- AR路由器同时作为DHCP服务器，为AP设备及接入的STA分配IP地址。

图 13-4 小型网络 WLAN 基本业务（AC 通过三层口管理 AP）



数据准备

表 13-1 数据准备表

项目	数据	说明
DHCP服务器	AC作为DHCP服务器为AP和STA分配IP地址	采用接口地址池方式为AP和STA分配IP地址。

版权所有 © 华为技术有限公司

项目	数据	说明
AP的IP地址池	10.10.10.2～10.10.10.254/24	选择三层接口GE0/0/1下的地址池为AP分配IP地址。
STA的IP地址池	10.10.11.2～10.10.11.254/24	选择三层子接口GE0/0/1.1下的地址池为STA分配IP地址。
AC的源接口IP地址	LoopBack0：1.1.1.1/32	无。
AP组	• 名称：ap-group1 • 引用模板：VAP模板wlan-vap、域管理模板domain1	无。
域管理模板	• 名称：domain1 • 国家码：CN	本例中，国家码配置成CN，也可以根据实际情况配置。
SSID模板	• 名称：wlan-ssid • SSID名称：wlan-net	本例中，无线网络的名称为“wlan-net”，员工打开STA的WLAN开关后，即可搜索到该无线网络。
安全模板	• 名称：wlan-security • 安全策略：WPA2+PSK+AES • 密码：YsHsjx_202206	本例中，安全策略为WPA2+PSK+AES，员工搜索到“wlan-net”无线网络后，输入密码“YsHsjx_202206”，即可接入该无线网络。
VAP模板	• 名称：wlan-vap • 业务VLAN：VLAN101 • 引用模板：SSID模板wlan-ssid、安全模板wlan-security	本例中，AP通过三层接口方式接入AC，AC上只需要配置业务VLAN，不需要配置管理VLAN。

配置思路

- 配置AC设备，实现AC、AP之间三层网络互通。
- 配置AC作为DHCP服务器为STA和AP分配IP地址。
- 配置AP上线。具体操作如下：
  - 创建AP组，用于将需要进行相同配置的AP都加入到AP组，实现统一配置。
  - 配置AC的系统参数，包括国家码、AC与AP之间通信的源接口。
  - 配置AP上线的认证方式并离线导入AP，实现AP正常上线。
- 配置WLAN业务参数，实现STA访问WLAN网络功能。

版权所有 © 华为技术有限公司

操作步骤

步骤1 配置AC三层接口及对应子接口的IP地址，实现AC与AP之间三层网络互通。

```
<Huawei> system-view
[Huawei] sysname AC
[AC] vlan batch 101
Info: This operation may take a few seconds. Please wait for a moment...done.
[AC] interface gigabitethernet 0/0/1
[AC-GigabitEthernet0/0/1] ip address 10.10.10.1 255.255.255.0
[AC-GigabitEthernet0/0/1] quit
[AC] interface gigabitethernet 0/0/1.1
[AC-GigabitEthernet0/0/1.1] ip address 10.10.11.1 255.255.255.0
[AC-GigabitEthernet0/0/1.1] quit
```

步骤2 配置AC作为DHCP服务器，为STA和AP分配IP地址。

```
[AC] dhcp enable
[AC] interface gigabitethernet 0/0/1
[AC-GigabitEthernet0/0/1] dhcp select interface //三层接口为AP分配IP地址，接口地址池为10.10.10.2～10.10.10.254/24
[AC-GigabitEthernet0/0/1] quit
[AC] interface gigabitethernet 0/0/1.1
[AC-GigabitEthernet0/0/1.1] dhcp select interface  //三层子接口为STA分配IP地址，接口地址池为10.10.11.2～10.10.11.254/24
[AC-GigabitEthernet0/0/1.1] dot1q termination vid 101 //三层子接口上需要配置终结业务VLAN101，剥掉报文里VLAN Tag 101的标签，使三层接口上可以接收二层报文
[AC-GigabitEthernet0/0/1.1] quit
```

步骤3 配置AP上线。

1. 创建AP组，用于将相同配置的AP都加入同一AP组中。

   ```
   [AC] wlan ac
   [AC-wlan-view] ap-group name ap-group1
   Info: This operation may take a few seconds. Please wait for a moment.done. [AC-wlan-ap-group-ap-group1] quit
   ```

2. 创建域管理模板，在域管理模板下配置AC的国家码并在AP组下引用域管理模板。

   ```
   [AC-wlan-view] regulatory-domain-profile name domain1
   [AC-wlan-regulate-domain-domain1] country-code cn  //国家码配置成CN
   Info: The current country code is same with the input country code. [AC-wlan-regulate-domain-domain1] quit
   [AC-wlan-view] ap-group name ap-group1
   [AC-wlan-ap-group-ap-group1] regulatory-domain-profile domain1
   Warning: Modifying the country code will clear channel, power and antenna gain configurations of the radio and reset the AP. Continu
   e?[Y/N]:y
   [AC-wlan-ap-group-ap-group1] quit
   [AC-wlan-view] quit
   ```

3. 配置AC源接口。

   ```
   [AC] interface loopback 0
   [AC-LoopBack0] ip address 1.1.1.1 255.255.255.255
   [AC-LoopBack0] quit
   [AC] capwap source interface loopback0  //配置loopback0口为AC的源接口
   ```

4. 在AC上离线导入AP，并将AP加入AP组“ap-group1”中。离线添加AP后，需要保证AP状态是**normal**，如果AP状态不是**normal**，请排查故障并最终使AP状态为**normal**。原因很大一部分是VLAN没有配置正确。

   ```
   [AC] wlan ac
   [AC-wlan-view] ap auth-mode mac-auth
   [AC-wlan-view] ap-id 1 ap-mac 00e0-fcbc-2420
   [AC-wlan-ap-1] ap-name area_1
   [AC-wlan-ap-1] ap-group ap-group1
   Warning: This operation may cause AP reset. If the country code changes, it will clear channel, power and antenna gain configuration
   s of the radio, Whether to continue? [Y/N]:y
   Info: This operation may take a few seconds. Please wait for a moment.. done. [AC-wlan-ap-1] quit
   ```

 版权所有 © 华为技术有限公司

5. 将AP上电后，检查AP的上线情况，当“State”项显示为“nor”时，表示AP已成功上线。

```
[AC-wlan-view] display ap all
Info: This operation may take a few seconds. Please wait for a moment.done.
Total AP information:
nor  : normal         [1]
-------------------------------------------------------------------------------------------------
ID   MAC          Name          Group     IP          Type          State STA Uptime
-------------------------------------------------------------------------------------------------
1    00e0-fcbc-2420 area_1        ap-group1 10.10.10.105 AP3010DN-AGN    nor   1   24M:51S
-------------------------------------------------------------------------------------------------
Total: 1
```

步骤4 配置WLAN的业务参数。

1. 创建名为“wlan-security”的安全模板，并配置安全策略。

```
[AC-wlan-view] security-profile name wlan-security
[AC-wlan-sec-prof-wlan-security] security wpa2 psk pass-phrase YsHsjx_202206 aes
[AC-wlan-sec-prof-wlan-security] quit
```

2. 创建名为“wlan-ssid”的SSID模板，并配置SSID名称为“wlan-net”。

```
[AC-wlan-view] ssid-profile name wlan-ssid
[AC-wlan-ssid-prof-wlan-ssid] ssid wlan-net
Warning: This action may cause service interruption. Continue?[Y/N]y
Info: This operation may take a few seconds, please wait.done.
[AC-wlan-ssid-prof-wlan-ssid] quit
```

3. 创建名为“wlan-vap”的VAP模板，配置业务VLAN，并且引用安全模板和SSID模板。

```
[AC-wlan-view] vap-profile name wlan-vap
[AC-wlan-vap-prof-wlan-vap] service-vlan vlan-id 101
Info: This operation may take a few seconds, please wait.done.
[AC-wlan-vap-prof-wlan-vap] security-profile wlan-security
Info: This operation may take a few seconds, please wait.done.
[AC-wlan-vap-prof-wlan-vap] ssid-profile wlan-ssid
Info: This operation may take a few seconds, please wait.done.
[AC-wlan-vap-prof-wlan-vap] quit
```

4. 配置AP组引用VAP模板，AP上射频都使用VAP模板“wlan-vap”的配置。

```
[AC-wlan-view] ap-group name ap-group1
[AC-wlan-ap-group-ap-group1] vap-profile wlan-vap wlan 1 radio all
Info: This operation may take a few seconds, please wait.done.
[AC-wlan-ap-group-ap-group1] quit
```

5. 提交配置，在AC上配置完WLAN的配置之后，必须使用**commit**命令将配置下发到AP上，否则WLAN的配置不生效。

```
[AC-wlan-view] commit all
Warning: Committing configuration may cause service interruption, continue?[Y/N]:y
```

步骤5 验证配置结果。

1. 在AC上，执行命令**display vap ssid wlan-net**查看如下信息，当“Status”项显示为“ON”时，表示AP对应的射频上的VAP已创建成功。

```
[AC-wlan-view] display vap ssid wlan-net
Info: This operation may take a few seconds, please wait.
WID : WLAN ID
-------------------------------------------------------------------------------
AP ID AP name       RfID WID  BSSID          Status  Auth type  STA   SSID
-------------------------------------------------------------------------------
1     area_1        0    1    00E0-FCBC-2420 ON      WPA2-PSK   0     wlan-net
1     area_1        1    1    00E0-FCBC-2430 ON      WPA2-PSK   1     wlan-net
-------------------------------------------------------------------------------
Total: 2
```

2. STA搜索到名为“wlan-net”的无线网络，输入密码“YsHsjx_202206”并正常接入后，在AC上执行**display station ssid wlan-net**命令，可以查看到用户已经接入到无线网络“wlan-net”中。

 版权所有 © 华为技术有限公司

```
[AC-wlan-view] display station ssid wlan-net
Rf/WLAN: Radio ID/WLAN ID
Rx/Tx: link receive rate/link transmit rate(Mbps)
--------------------------------------------------------------------------------
STA MAC         AP ID Ap name  Rf/WLAN  Band  Type  Rx/Tx     RSSI  VLAN  IP address
--------------------------------------------------------------------------------
00e0-fc03-bcef  1     area_1   1/1      5G    11n   92/122    -55   101   10.10.11.164
--------------------------------------------------------------------------------
Total: 1 2.4G: 0 5G: 1
```

----结束

配置文件

AC配置文件

```
#
 sysname AC
#
vlan batch 101
#
dhcp enable
#
interface GigabitEthernet0/0/1
 ip address 10.10.10.1 255.255.255.0
 dhcp select interface
#
interface GigabitEthernet0/0/1.1
 dot1q termination vid 101
 ip address 10.10.11.1 255.255.255.0
 dhcp select interface
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
capwap source interface loopback0
#
wlan ac
 security-profile name wlan-security
  security wpa2 psk pass-phrase %^%#m"tz0f>~7.[`^6RWdzwCy16hJj/Mc!,}s`X*B]}A%^%# aes
 ssid-profile name wlan-ssid
  ssid wlan-net
 vap-profile name wlan-vap
  service-vlan vlan-id 101
  ssid-profile wlan-ssid
  security-profile wlan-security
 regulatory-domain-profile name domain1
 ap-group name ap-group1
  regulatory-domain-profile domain1
  radio 0
   vap-profile wlan-vap wlan 1
  radio 1
   vap-profile wlan-vap wlan 1
  radio 2
   vap-profile wlan-vap wlan 1
 ap-id 1 type-id 31 ap-mac ac85-3dbc-2420 ap-sn 2102355829W0E5009170
  ap-name area_1
  ap-group ap-group1
#
return
```

 版权所有 © 华为技术有限公司

13.5 配置中型网络 WLAN 基本业务示例（AC 通过三层口管理 AP）

规格

适用于支持WLAN AC功能的款型，V200R008C00及更高版本。

组网需求

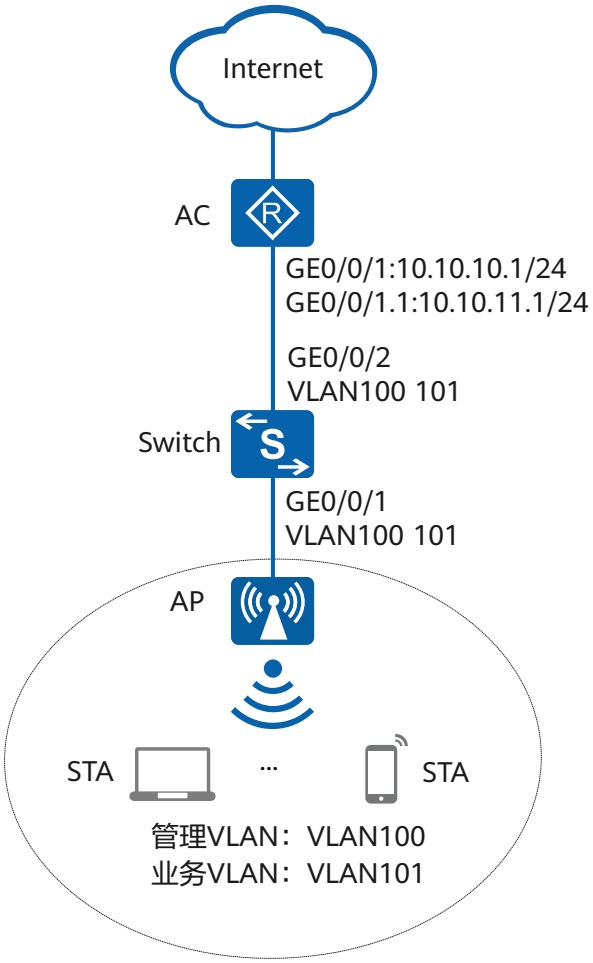
如图13-5所示，某中型企业由于业务需要，希望员工能在企业内部随时随地的访问Internet，进行移动办公。该企业部署了一台AR路由器作为出口网关，希望同时在AR路由器上部署WLAN功能，为企业员工提供无线网络接入服务，实现移动办公。

在提供无线网络接入服务上，主要有如下需求：

- AR路由器作为AC，通过下挂AP的方式，为企业员工提供无线网络接入服务。
- 由于企业规模不大，终端用户数较少，目前只需要一台AP，即可满足所有终端用户的无线上网需求。
- AR路由器主要作出口网关，下接一个二层交换机作数据转发。该AR路由器上无可用的二层接口，只能通过一个三层接口连接交换机。由于二层交换机上接口较多，为了防止公司后期规模扩张，企业员工增加，需要接入更多的AP，现将AP设备通过二层交换机接入AC。
- AR路由器同时作为DHCP服务器，为AP设备及接入的STA分配IP地址。

版权所有 © 华为技术有限公司

图 13-5 中型网络 WLAN 基本业务（AC 通过三层口管理 AP）



数据准备

表 13-2 数据准备表

项目	数据	说明
DHCP服务器	AC作为DHCP服务器为AP和STA分配IP地址	采用接口地址池方式为AP和STA分配IP地址。
AP的IP地址池	10.10.10.2～10.10.10.254/24	选择三层接口GE0/0/1下的地址池为AP分配IP地址。
STA的IP地址池	10.10.11.2～10.10.11.254/24	选择三层子接口GE0/0/1.1下的地址池为STA分配IP地址。
AC的源接口IP地址	LoopBack0：1.1.1.1/32	无。

版权所有 © 华为技术有限公司

项目	数据	说明
AP组	● 名称：ap-group1 ● 引用模板：VAP模板 wlan-vap、域管理模板 domain1	无。
域管理模板	● 名称：domain1 ● 国家码：CN	本例中，国家码配置成CN，也可以根据实际情况配置。
SSID模板	● 名称：wlan-ssid ● SSID名称：wlan-net	本例中，无线网络的名称为“wlan-net”，员工打开STA的WLAN开关后，即可搜索到该无线网络。
安全模板	● 名称：wlan-security ● 安全策略：WPA2+PSK+AES ● 密码：YsHsjx_202206	本例中，安全策略为WPA2+PSK+AES，员工搜索到“wlan-net”无线网络后，输入密码“YsHsjx_202206”，即可接入该无线网络。
VAP模板	● 名称：wlan-vap ● 业务VLAN：VLAN101 ● 管理VLAN：VLAN100 ● 引用模板：SSID模板 wlan-ssid、安全模板 wlan-security	本例中，AP通过三层接口方式接入AC，AC上只需要配置业务VLAN，不需要配置管理VLAN。但是为了AP发送的管理报文可以通过二层交换机转发到AC，建议在二层交换机上配置一个管理VLAN，管理VLAN和业务VLAN不能相同。

配置思路

- 配置AC设备，实现AC、交换机和AP之间三层网络互通。
- 配置交换机设备，实现AC、交换机和AP之间二层网络互通。
- 配置AC作为DHCP服务器为STA和AP分配IP地址。
- 配置AP上线。具体操作如下：
  - 创建AP组，用于将需要进行相同配置的AP都加入到AP组，实现统一配置。
  - 配置AC的系统参数，包括国家码、AC与AP之间通信的源接口。
  - 配置AP上线的认证方式并离线导入AP，实现AP正常上线。
- 配置WLAN业务参数，实现STA访问WLAN网络功能。

操作步骤

步骤1 配置AC三层接口及对应子接口的IP地址，实现AC与AP之间三层网络互通。

```
<Huawei> system-view
[Huawei] sysname AC
```

 版权所有 © 华为技术有限公司

```
[AC] vlan batch 101
Info: This operation may take a few seconds. Please wait for a moment...done.
[AC] interface gigabitethernet 0/0/1
[AC-GigabitEthernet0/0/1] ip address 10.10.10.1 255.255.255.0
[AC-GigabitEthernet0/0/1] quit
[AC] interface gigabitethernet 0/0/1.1
[AC-GigabitEthernet0/0/1.1] ip address 10.10.11.1 255.255.255.0
[AC-GigabitEthernet0/0/1.1] quit
```

步骤2 配置交换机接口加入VLAN100和VLAN101，实现AC、交换机和AP之间二层网络互通。

```
<Huawei> system-view
[Huawei] sysname Switch
[Switch] vlan batch 100 101
Info: This operation may take a few seconds. Please wait for a moment...done.
[Switch] interface gigabitethernet 0/0/1
[Switch-GigabitEthernet0/0/1] port link-type trunk
[Switch-GigabitEthernet0/0/1] port trunk pvid vlan 100 //配置缺省VLAN是VLAN100，为AP发送的管理报文打上VLAN Tag 100的标签
[Switch-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 101
[Switch-GigabitEthernet0/0/1] port-isolate enable //建议在连接AP的接口GE0/0/1上配置端口隔离，如果不配置端口隔离，可能会在VLAN内存在不必要的广播报文，或者导致不同AP间的WLAN用户二层互通的问题
[Switch-GigabitEthernet0/0/1] quit
[Switch] interface gigabitethernet 0/0/2
[Switch-GigabitEthernet0/0/2] port link-type trunk
[Switch-GigabitEthernet0/0/2] port trunk pvid vlan 100//配置缺省VLAN是VLAN100，剥掉AP发送的管理报文中VLAN Tag 100的标签
[Switch-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 101
[Switch-GigabitEthernet0/0/2] quit
```

步骤3 配置AC作为DHCP服务器，为STA和AP分配IP地址。

```
[AC] dhcp enable
[AC] interface gigabitethernet 0/0/1
[AC-GigabitEthernet0/0/1] dhcp select interface //三层接口为AP分配IP地址，接口地址池为10.10.10.2～10.10.10.254/24
[AC-GigabitEthernet0/0/1] quit
[AC] interface gigabitethernet 0/0/1.1
[AC-GigabitEthernet0/0/1.1] dhcp select interface  //三层子接口为STA分配IP地址，接口地址池为10.10.11.2～10.10.11.254/24
[AC-GigabitEthernet0/0/1.1] dot1q termination vid 101 //三层子接口上需要配置终结业务VLAN101，剥掉报文里VLAN Tag 101的标签，使三层接口上可以接收二层报文
[AC-GigabitEthernet0/0/1.1] quit
```

步骤4 配置AP上线。

1. 创建AP组，用于将相同配置的AP都加入同一AP组中。

   ```
   [AC] wlan ac
   [AC-wlan-view] ap-group name ap-group1
   Info: This operation may take a few seconds. Please wait for a moment.done. [AC-wlan-ap-group-ap-group1] quit
   ```

2. 创建域管理模板，在域管理模板下配置AC的国家码并在AP组下引用域管理模板。

   ```
   [AC-wlan-view] regulatory-domain-profile name domain1
   [AC-wlan-regulate-domain-domain1] country-code cn  //国家码配置成CN
   Info: The current country code is same with the input country code. [AC-wlan-regulate-domain-domain1] quit
   [AC-wlan-view] ap-group name ap-group1
   [AC-wlan-ap-group-ap-group1] regulatory-domain-profile domain1
   Warning: Modifying the country code will clear channel, power and antenna gain configurations of the radio and reset the AP. Continu
   e?[Y/N]:y
   [AC-wlan-ap-group-ap-group1] quit
   [AC-wlan-view] quit
   ```

3. 配置AC源接口。

   ```
   [AC] interface loopback 0
   [AC-LoopBack0] ip address 1.1.1.1 255.255.255.255
   [AC-LoopBack0] quit
   [AC] capwap source interface loopback0  //配置loopback0口为AC的源接口
   ```

 版权所有 © 华为技术有限公司

4. 在AC上离线导入AP，并将AP加入AP组“ap-group1”中。离线添加AP后，需要保证AP状态是**normal**，如果AP状态不是**normal**，请排查故障并最终使AP状态为**normal**。原因很大一部分是VLAN没有配置正确。

```
[AC] wlan ac
[AC-wlan-view] ap auth-mode mac-auth
[AC-wlan-view] ap-id 1 ap-mac 00e0-fcbc-2420
[AC-wlan-ap-1] ap-name area_1
[AC-wlan-ap-1] ap-group ap-group1
Warning: This operation may cause AP reset. If the country code changes, it will clear channel, power and antenna gain configuration
s of the radio, Whether to continue? [Y/N]:y
Info: This operation may take a few seconds. Please wait for a moment.. done. [AC-wlan-ap-1] quit
```

5. 将AP上电后，检查AP的上线情况，当“State”项显示为“nor”时，表示AP已成功上线。

```
[AC-wlan-view] display ap all
Info: This operation may take a few seconds. Please wait for a moment.done.
Total AP information:
nor  : normal         [1]
------------------------------------------------------------------------------------------------------
ID   MAC            Name          Group     IP          Type           State STA Uptime
------------------------------------------------------------------------------------------------------
1    00e0-fcbc-2420 area_1        ap-group1 10.10.10.105 AP3010DN-AGN    nor   1   24M:51S
------------------------------------------------------------------------------------------------------
Total: 1
```

步骤5 配置WLAN的业务参数。

1. 创建名为“wlan-security”的安全模板，并配置安全策略。

```
[AC-wlan-view] security-profile name wlan-security
[AC-wlan-sec-prof-wlan-security] security wpa2 psk pass-phrase YsHsjx_202206 aes
[AC-wlan-sec-prof-wlan-security] quit
```

2. 创建名为“wlan-ssid”的SSID模板，并配置SSID名称为“wlan-net”。

```
[AC-wlan-view] ssid-profile name wlan-ssid
[AC-wlan-ssid-prof-wlan-ssid] ssid wlan-net
Warning: This action may cause service interruption. Continue?[Y/N]y
Info: This operation may take a few seconds, please wait.done.
[AC-wlan-ssid-prof-wlan-ssid] quit
```

3. 创建名为“wlan-vap”的VAP模板，配置业务VLAN，并且引用安全模板和SSID模板。

```
[AC-wlan-view] vap-profile name wlan-vap
[AC-wlan-vap-prof-wlan-vap] service-vlan vlan-id 101
Info: This operation may take a few seconds, please wait.done.
[AC-wlan-vap-prof-wlan-vap] security-profile wlan-security
Info: This operation may take a few seconds, please wait.done.
[AC-wlan-vap-prof-wlan-vap] ssid-profile wlan-ssid
Info: This operation may take a few seconds, please wait.done.
[AC-wlan-vap-prof-wlan-vap] quit
```

4. 配置AP组引用VAP模板，AP上射频都使用VAP模板“wlan-vap”的配置。

```
[AC-wlan-view] ap-group name ap-group1
[AC-wlan-ap-group-ap-group1] vap-profile wlan-vap wlan 1 radio all
Info: This operation may take a few seconds, please wait.done.
[AC-wlan-ap-group-ap-group1] quit
```

5. 提交配置，在AC上配置完WLAN的配置之后，必须使用**commit**命令将配置下发到AP上，否则WLAN的配置不生效。

```
[AC-wlan-view] commit all
Warning: Committing configuration may cause service interruption, continue?[Y/N]:y
```

步骤6 验证配置结果。

1. 在AC上，执行命令**display vap ssid wlan-net**查看如下信息，当“Status”项显示为“ON”时，表示AP对应的射频上的VAP已创建成功。

```
[AC-wlan-view] display vap ssid wlan-net
Info: This operation may take a few seconds, please wait.
```

 版权所有 © 华为技术有限公司

```
WID : WLAN ID
-------------------------------------------------------------------------------
AP ID AP name       RfID WID  BSSID          Status  Auth type  STA   SSID
-------------------------------------------------------------------------------
1     area_1        0    1    00E0-FCBC-2420 ON      WPA2-PSK   0     wlan-net
1     area_1        1    1    00E0-FCBC-2430 ON      WPA2-PSK   1     wlan-net
-------------------------------------------------------------------------------
Total: 2
```

2. STA搜索到名为“wlan-net”的无线网络，输入密码“YsHsjx_202206”并正常接入后，在AC上执行**display station ssid wlan-net**命令，可以查看到用户已经接入到无线网络“wlan-net”中。

```
[AC-wlan-view] display station ssid wlan-net
Rf/WLAN: Radio ID/WLAN ID
Rx/Tx: link receive rate/link transmit rate(Mbps)
-------------------------------------------------------------------------------------------
STA MAC         AP ID AP name  Rf/WLAN  Band  Type  Rx/Tx     RSSI  VLAN  IP address
-------------------------------------------------------------------------------------------
00e0-fc03-bcef  1     area_1   1/1      5G    11n   92/122    -55   101   10.10.11.164
-------------------------------------------------------------------------------------------
Total: 1 2.4G: 0 5G: 1
```

----结束

配置文件

- AC配置文件

```
#
 sysname AC
#
vlan batch 101
#
dhcp enable
#
interface GigabitEthernet0/0/1
 ip address 10.10.10.1 255.255.255.0
 dhcp select interface
#
interface GigabitEthernet0/0/1.1
 dot1q termination vid 101
 ip address 10.10.11.1 255.255.255.0
 dhcp select interface
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
capwap source interface loopback0
#
wlan ac
 security-profile name wlan-security
  security wpa2 psk pass-phrase %^%#m"tz0f>~7.[`^6RWdzwCy16hJj/Mc!,}s`X*B]}A%^%# aes
 ssid-profile name wlan-ssid
  ssid wlan-net
 vap-profile name wlan-vap
  service-vlan vlan-id 101
  ssid-profile wlan-ssid
  security-profile wlan-security
 regulatory-domain-profile name domain1
 ap-group name ap-group1
  regulatory-domain-profile domain1
  radio 0
   vap-profile wlan-vap wlan 1
  radio 1
   vap-profile wlan-vap wlan 1
  radio 2
   vap-profile wlan-vap wlan 1
 ap-id 1 type-id 31 ap-mac 00e0-fcbc-2420 ap-sn 2102355829W0E5009170
  ap-name area_1
```

 版权所有 © 华为技术有限公司

```
 ap-group ap-group1
#
return
```

- Switch配置文件

```
#
sysname Switch
#
vlan batch 100 to 101
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100 101
 port-isolate enable group 1
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100 101
#
return
```

13.6 配置家庭消费用户无线上网示例（AC 通过三层口管理 AP）

规格

适用于支持WLAN AC功能的款型，V200R008C00及更高版本。

组网需求

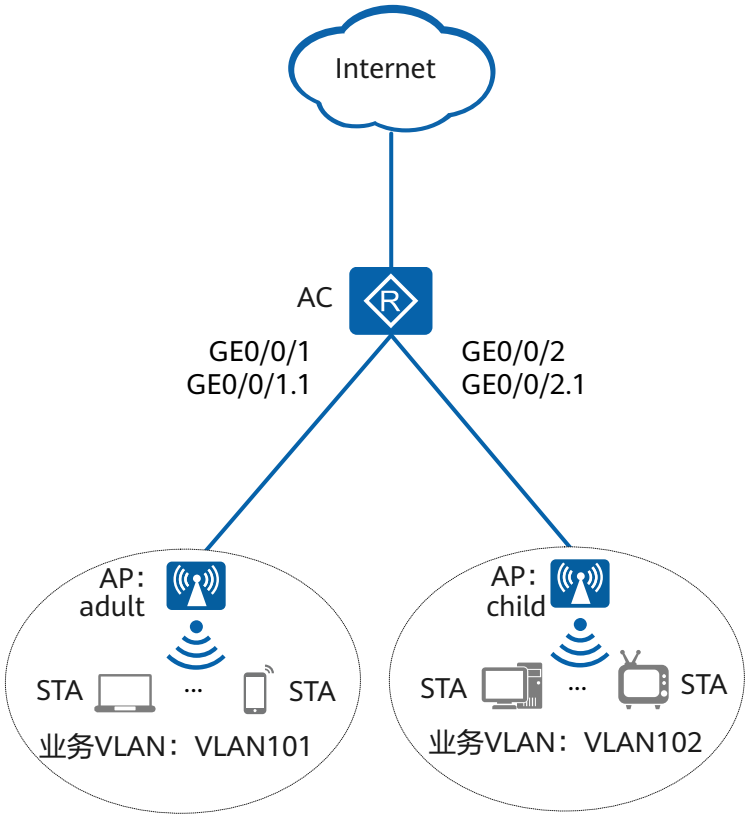
图13-6为一个典型的家庭消费用户使用的网络架构。该家庭消费用户的上网流量大多是低速流量，例如浏览网页、玩游戏、看视频等。家庭成员使用的无线终端主要为手机、PC、电视机等。终端接入的数量正常情况下在10个以内，偶尔有家庭聚会等特殊情况，终端接入的数量可能会达到30～40个。用户希望部署WLAN功能，为家庭成员提供良好的无线网络接入服务。

在提供无线网络接入服务上，主要有如下需求：

- AR路由器作为AC，通过下挂AP的方式，为家庭成员提供无线网络接入服务。
- 为了满足家庭聚会时所有成员的无线上网需求，需要部署多台AP，同时为了提升家庭成员的无线上网体验，AP需要同时支持2.4G频段和5G频段。
- 该家庭成员里有成年人与未成年人，为了限制不同家庭成员的上网行为，需要部署不同的SSID，供不同的成员接入。其中部署SSID为“adult”的无线网络供成年人接入，部署SSID为“child”的无线网络供未成年人接入，并对“child”无线网络进行WLAN QoS限速，防止未成年人浪费太多时间上网。
- AR路由器同时作为DHCP服务器，为AP设备及接入的STA分配IP地址。
- 本例中，AR路由器有2个WAN侧GE电接口（三层接口），用户可以直接使用该接口连接AP。

 版权所有 © 华为技术有限公司

图 13-6 家庭消费用户无线上网示例



数据准备

表 13-3 数据准备表

项目	数据	说明
DHCP服务器	AC作为DHCP服务器为AP和STA分配IP地址	采用接口地址池方式为AP和STA分配IP地址。
adult区域内AP的IP地址池	10.10.10.2～10.10.10.254/24	选择三层接口GE0/0/1下的地址池为adult区域内的AP分配IP地址。
adult区域内STA的IP地址池	10.10.11.2～10.10.11.254/24	选择三层子接口GE0/0/1.1下的地址池为adult区域内的STA分配IP地址。
child区域内AP的IP地址池	10.10.12.2～10.10.12.254/24	选择三层接口GE0/0/2下的地址池为child区域内的AP分配IP地址。

版权所有 © 华为技术有限公司

项目	数据	说明
child区域内STA的IP地址池	10.10.13.2～10.10.13.254/24	选择三层子接口GE0/0/2.1下的地址池为child区域内的STA分配IP地址。
AC的源接口IP地址	LoopBack0：1.1.1.1/32	无。
AP组	• 名称：adult • 引用模板：VAP模板adult、域管理模板domain1	无。
	• 名称：child • 引用模板：VAP模板child、域管理模板domain1	无。
域管理模板	• 名称：domain1 • 国家码：CN	本例中，国家码配置成CN，也可以根据实际情况配置。
SSID模板	• 名称：adult • SSID名称：adult	无线网络“adult”为成年家庭成员提供网络接入服务。
	• 名称：child • SSID名称：child	无线网络“child”为未成年家庭成员提供网络接入服务。
安全模板	• 名称：adult • 安全策略：WPA2+PSK+AES • 密码：YsHsjx_202206	安全策略为WPA2+PSK+AES，成年家庭成员搜索到“adult”无线网络后，输入密码“YsHsjx_202206”，即可接入该无线网络。
	• 名称：child • 安全策略：WPA2+PSK+AES • 密码：YsHsjx_202207	安全策略为WPA2+PSK+AES，未成年家庭成员搜索到“child”无线网络后，输入密码“YsHsjx_202207”，即可接入该无线网络。
流量模板	• 名称：child • 限速策略：STA上行限速为1024kbit/s、VAP上行限速为2048kbit/s	对未成年人接入的无线网络“child”进行WLAN QoS限速，防止未成年人浪费太多的时间上网。
VAP模板	• 名称：adult • 业务VLAN：VLAN101 • 引用模板：SSID模板adult、安全模板adult	本例中，AP通过三层接口接入AC，AC上只需要配置业务VLAN，不需要配置管理VLAN。

版权所有 © 华为技术有限公司

项目	数据	说明
	● 名称：child ● 业务VLAN：VLAN102 ● 引用模板：SSID模板child、安全模板child、流量模板child	

配置思路

- 配置AC设备，实现AC、AP之间三层网络互通。
- 配置AC作为DHCP服务器为STA和AP分配IP地址。
- 配置AP上线。具体操作如下：
  - 创建AP组，用于将需要进行相同配置的AP都加入到AP组，实现统一配置。
  - 配置AC的系统参数，包括国家码、AC与AP之间通信的源接口。
  - 配置AP上线的认证方式并离线导入AP，实现AP正常上线。
- 配置WLAN业务参数，实现STA访问WLAN网络功能。

操作步骤

步骤1 配置AC三层接口及对应子接口的IP地址，实现AC与AP之间三层网络互通。

```
<Huawei> system-view
[Huawei] sysname AC
[AC] vlan batch 101 102
Info: This operation may take a few seconds. Please wait for a moment...done.
[AC] interface gigabitethernet 0/0/1
[AC-GigabitEthernet0/0/1] ip address 10.10.10.1 255.255.255.0
[AC-GigabitEthernet0/0/1] quit
[AC] interface gigabitethernet 0/0/1.1
[AC-GigabitEthernet0/0/1.1] ip address 10.10.11.1 255.255.255.0
[AC-GigabitEthernet0/0/1.1] quit
[AC] interface gigabitethernet 0/0/2
[AC-GigabitEthernet0/0/2] ip address 10.10.12.1 255.255.255.0
[AC-GigabitEthernet0/0/2] quit
[AC] interface gigabitethernet 0/0/2.1
[AC-GigabitEthernet0/0/2.1] ip address 10.10.13.1 255.255.255.0
[AC-GigabitEthernet0/0/2.1] quit
```

步骤2 配置AC作为DHCP服务器，为STA和AP分配IP地址。

```
[AC] dhcp enable
Info: The operation may take a few seconds. Please wait for a moment.done.
[AC] interface gigabitethernet 0/0/1
[AC-GigabitEthernet0/0/1] dhcp select interface //三层接口为adult区域的AP分配IP地址，接口地址池为10.10.10.2～10.10.10.254/24
[AC-GigabitEthernet0/0/1] quit
[AC] interface gigabitethernet 0/0/1.1
[AC-GigabitEthernet0/0/1.1] dhcp select interface  //三层子接口为adult区域的STA分配IP地址，接口地址池为10.10.11.2～10.10.11.254/24
[AC-GigabitEthernet0/0/1.1] dot1q termination vid 101 //三层子接口上需要配置终结业务VLAN101，剥掉报文里VLAN Tag 101的标签，使三层接口上可以接收二层报文
[AC-GigabitEthernet0/0/1.1] quit
[AC] interface gigabitethernet 0/0/2
[AC-GigabitEthernet0/0/2] dhcp select interface //三层接口为child区域的AP分配IP地址，接口地址池为10.10.12.2～10.10.12.254/24
[AC-GigabitEthernet0/0/2] quit
[AC] interface gigabitethernet 0/0/2.1
```

 版权所有 © 华为技术有限公司

```
[AC-GigabitEthernet0/0/2.1] dhcp select interface  //三层子接口为child区域的STA分配IP地址，接口地址池为10.10.13.2～10.10.13.254/24
[AC-GigabitEthernet0/0/2.1] dot1q termination vid 102 //三层子接口上需要配置终结业务VLAN102，剥掉报文里VLAN Tag 102的标签，使三层接口上可以接收二层报文
[AC-GigabitEthernet0/0/2.1] quit
```

步骤3 配置AP上线。

1. 创建AP组，用于将相同配置的AP都加入同一AP组中。

```
[AC] wlan ac
[AC-wlan-view] ap-group name adult
Info: This operation may take a few seconds. Please wait for a moment.done. [AC-wlan-ap-group-adult] quit
[AC-wlan-view] ap-group name child
Info: This operation may take a few seconds. Please wait for a moment.done. [AC-wlan-ap-group-child] quit
```

2. 创建域管理模板，在域管理模板下配置AC的国家码并在AP组下引用域管理模板。

```
[AC-wlan-view] regulatory-domain-profile name domain1
[AC-wlan-regulate-domain-domain1] country-code cn  //国家码配置成CN
Info: The current country code is same with the input country code.
[AC-wlan-regulate-domain-domain1] quit
[AC-wlan-view] ap-group name adult
[AC-wlan-ap-group-adult] regulatory-domain-profile domain1
Warning: Modifying the country code will clear channel, power and antenna gain configurations of the radio and reset the AP. Continu
e?[Y/N]:y
[AC-wlan-ap-group-adult] quit
[AC-wlan-view] ap-group name child
[AC-wlan-ap-group-child] regulatory-domain-profile domain1
Warning: Modifying the country code will clear channel, power and antenna gain configurations of the radio and reset the AP. Continu
e?[Y/N]:y
[AC-wlan-ap-group-child] quit
[AC-wlan-view] quit
```

3. 配置AC源接口。

```
[AC] interface loopback 0
[AC-LoopBack0] ip address 1.1.1.1 255.255.255.255
[AC-LoopBack0] quit
[AC] capwap source interface loopback0  //配置loopback0口为AC的源接口
```

4. 在AC上离线导入AP，并分别将AP加入AP组“adult”和“child”中。离线添加AP后，需要保证AP状态是**normal**，如果AP状态不是**normal**，请排查故障并最终使AP状态为**normal**。

```
[AC] wlan ac
[AC-wlan-view] ap auth-mode mac-auth
[AC-wlan-view] ap-id 0 ap-mac 00e0-fc05-e5a0
[AC-wlan-ap-0] ap-name adult
[AC-wlan-ap-0] ap-group adult
Warning: This operation may cause AP reset. If the country code changes, it will clear channel, power and antenna gain configuration
s of the radio, Whether to continue? [Y/N]:y
Info: This operation may take a few seconds. Please wait for a moment.. done. [AC-wlan-ap-0] quit
[AC-wlan-view] ap-id 1 ap-mac 00e0-fc06-1160
[AC-wlan-ap-1] ap-name child
[AC-wlan-ap-1] ap-group child
Warning: This operation may cause AP reset. If the country code changes, it will clear channel, power and antenna gain configuration
s of the radio, Whether to continue? [Y/N]:y
Info: This operation may take a few seconds. Please wait for a moment.. done. [AC-wlan-ap-1] quit
```

5. 将AP上电后，检查AP的上线情况，当“State”项显示为“nor”时，表示AP已成功上线。

```
[AC-wlan-view] display ap all
Info: This operation may take a few seconds. Please wait for a moment.done.
Total AP information:
nor  : normal          [2]
--------------------------------------------------------------------------------
```

```
---------
ID   MAC            Name  Group IP          Type           State STA Uptime
------------------------------------------------------------------------------
---------
0    00e0-fc05-e5a0 adult adult 10.10.10.212 AP6010DN-AGN    nor   0   39M:19S
1    00e0-fc06-1160 child child 10.10.12.40  AP6010DN-AGN    nor   0   17S
------------------------------------------------------------------------------
---------
Total: 2
```

步骤4 配置WLAN的业务参数。

1. 创建名为“adult”和“child”的安全模板，并配置安全策略。

```
[AC-wlan-view] security-profile name adult
[AC-wlan-sec-prof-adult] security wpa2 psk pass-phrase YsHsjx_202206 aes
[AC-wlan-sec-prof-adult] quit
[AC-wlan-view] security-profile name child
[AC-wlan-sec-prof-child] security wpa2 psk pass-phrase YsHsjx_202207 aes
[AC-wlan-sec-prof-child] quit
```

2. 创建名为“adult”和“child”的SSID模板，并配置SSID名称为“adult”和“child”。

```
[AC-wlan-view] ssid-profile name adult
[AC-wlan-ssid-prof-adult] ssid adult
Warning: This action may cause service interruption. Continue?[Y/N]y
Info: This operation may take a few seconds, please wait.done.
[AC-wlan-ssid-prof-adult] quit
[AC-wlan-view] ssid-profile name child
[AC-wlan-ssid-prof-child] ssid child
Warning: This action may cause service interruption. Continue?[Y/N]y
Info: This operation may take a few seconds, please wait.done.
[AC-wlan-ssid-prof-child] quit
```

3. 创建名为“child”的流量模板，并配置限速策略，STA上行限速为1024kbit/s、VAP上行限速为2048kbit/s。

```
[AC-wlan-view] traffic-profile name child
[AC-wlan-traffic-prof-child] rate-limit client up 1024
[AC-wlan-traffic-prof-child] rate-limit vap up 2048
[AC-wlan-traffic-prof-child] quit
```

4. 创建名为“adult”和“child”的VAP模板，配置业务VLAN，并且引用安全模板和SSID模板，“child”还需引用流量模板。

```
[AC-wlan-view] vap-profile name adult
[AC-wlan-vap-prof-adult] service-vlan vlan-id 101
Info: This operation may take a few seconds, please wait.done.
[AC-wlan-vap-prof-adult] security-profile adult
Info: This operation may take a few seconds, please wait.done.
[AC-wlan-vap-prof-adult] ssid-profile adult
Info: This operation may take a few seconds, please wait.done.
[AC-wlan-vap-prof-adult] quit
[AC-wlan-view] vap-profile name child
[AC-wlan-vap-prof-child] service-vlan vlan-id 102
Info: This operation may take a few seconds, please wait.done.
[AC-wlan-vap-prof-child] security-profile child
Info: This operation may take a few seconds, please wait.done.
[AC-wlan-vap-prof-child] ssid-profile child
Info: This operation may take a few seconds, please wait.done.
[AC-wlan-vap-prof-child] traffic-profile child
Warning: This action may cause service interruption. Continue?[Y/N]y
Info: This operation may take a few seconds, please wait.done.
[AC-wlan-vap-prof-child] quit
```

5. 配置AP组引用VAP模板，并在AP射频0和射频1上都使用VAP模板“adult”和“child”的配置。

```
[AC-wlan-view] ap-group name adult
[AC-wlan-ap-group-adult] vap-profile adult wlan 1 radio all
Info: This operation may take a few seconds, please wait.done.
[AC-wlan-ap-group-adult] quit
```

 版权所有 © 华为技术有限公司

```
[AC-wlan-view] ap-group name child
[AC-wlan-ap-group-child] vap-profile child wlan 1 radio all
Info: This operation may take a few seconds, please wait.done.
[AC-wlan-ap-group-child] quit
```

6. 提交配置，在AC上配置完WLAN的配置之后，必须使用**commit**命令将配置下发到AP上，否则WLAN的配置不生效。

```
[AC-wlan-view] commit all
Warning: Committing configuration may cause service interruption, continue?[Y/N]:y
```

步骤5 验证配置结果。

1. 在AC上，执行命令**display vap ssid wlan-net**和**display vap ssid child**查看如下信息，当“Status”项显示为“ON”时，表示AP对应的射频上的VAP已创建成功。

```
[AC-wlan-view] display vap ssid adult
Info: This operation may take a few seconds, please wait.
WID : WLAN ID
--------------------------------------------------------------------------------
AP ID AP name RfID WID  BSSID         Status  Auth type  STA   SSID
--------------------------------------------------------------------------------
0     adult   0    1    88CF-9805-E5A0 ON      WPA2-PSK   0     adult
0     adult   1    1    88CF-9805-E5B0 ON      WPA2-PSK   0     adult
--------------------------------------------------------------------------------
Total: 2
[AC-wlan-view] display vap ssid child
Info: This operation may take a few seconds, please wait.
WID : WLAN ID
--------------------------------------------------------------------------------
AP ID AP name RfID WID  BSSID         Status  Auth type  STA   SSID
--------------------------------------------------------------------------------
1     child   0    1    88CF-9806-1160 ON      WPA2-PSK   0     child
1     child   1    1    88CF-9806-1170 ON      WPA2-PSK   0     child
--------------------------------------------------------------------------------
Total: 2
```

2. STA搜索到名为“adult”和“child”的无线网络，输入密码“YsHsjx_202206”和“YsHsjx_202207”即可正常接入无线网络。

----结束

配置文件

AC配置文件

```
#
 sysname AC
#
vlan batch 101 to 102
#
dhcp enable
#
interface GigabitEthernet0/0/1
 ip address 10.10.10.1 255.255.255.0
 dhcp select interface
#
interface GigabitEthernet0/0/1.1
 dot1q termination vid 101
 ip address 10.10.11.1 255.255.255.0
 dhcp select interface
#
interface GigabitEthernet0/0/2
 ip address 10.10.12.1 255.255.255.0
 dhcp select interface
#
interface GigabitEthernet0/0/2.1
 dot1q termination vid 102
 ip address 10.10.13.1 255.255.255.0
```

 版权所有 © 华为技术有限公司

```
 dhcp select interface
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
capwap source interface loopback0
#
wlan ac
 traffic-profile name child
  rate-limit client up 1024
  rate-limit vap up 2048
 traffic-profile name default
 security-profile name adult
  security wpa2 psk pass-phrase %^%#}6UoO#|fz,cF!+ZhgM$3g3m&G|(@YN|l"lUpGG7-%^%#
 aes
 security-profile name child
  security wpa2 psk pass-phrase %^%#hus&<9SU`TihmU%.+{+(5e6cXdr/YE>x/q";drf)%^%#
 aes
 security-profile name default
 security-profile name default-wds
  security wpa2 psk pass-phrase %^%#=gC6'\D5*Q4;i)&s[{-/zaDWE!c\|C*'QDJt]2x5%^%#
 aes
 ssid-profile name adult
  ssid adult
 ssid-profile name child
  ssid child
 ssid-profile name default
 vap-profile name adult
  service-vlan vlan-id 101
  ssid-profile adult
  security-profile adult
 vap-profile name child
  service-vlan vlan-id 102
  ssid-profile child
  security-profile child
  traffic-profile child
 vap-profile name default
 wds-profile name default
 regulatory-domain-profile name default
 regulatory-domain-profile name domain1
 air-scan-profile name default
 rrm-profile name default
 radio-2g-profile name default
 radio-5g-profile name default
 wids-spoof-profile name default
 wids-profile name default
 ap-system-profile name default
 port-link-profile name default
 wired-port-profile name default
 ap-group name adult
  regulatory-domain-profile domain1
  radio 0
   vap-profile adult wlan 1
  radio 1
   vap-profile adult wlan 1
  radio 2
   vap-profile adult wlan 1
 ap-group name child
  regulatory-domain-profile domain1
  radio 0
   vap-profile child wlan 1
  radio 1
   vap-profile child wlan 1
  radio 2
   vap-profile child wlan 1
 ap-group name default
 ap-id 0 type-id 19 ap-mac 88cf-9805-e5a0 ap-sn 2102354196W0FB001727
  ap-name adult
  ap-group adult
```

 版权所有 © 华为技术有限公司

```
 ap-id 1 type-id 19 ap-mac 88cf-9806-1160 ap-sn 2102354196W0FB002038
  ap-name child
  ap-group child
#
return
```

13.7 配置安全策略为 Portal 认证的业务示例

规格

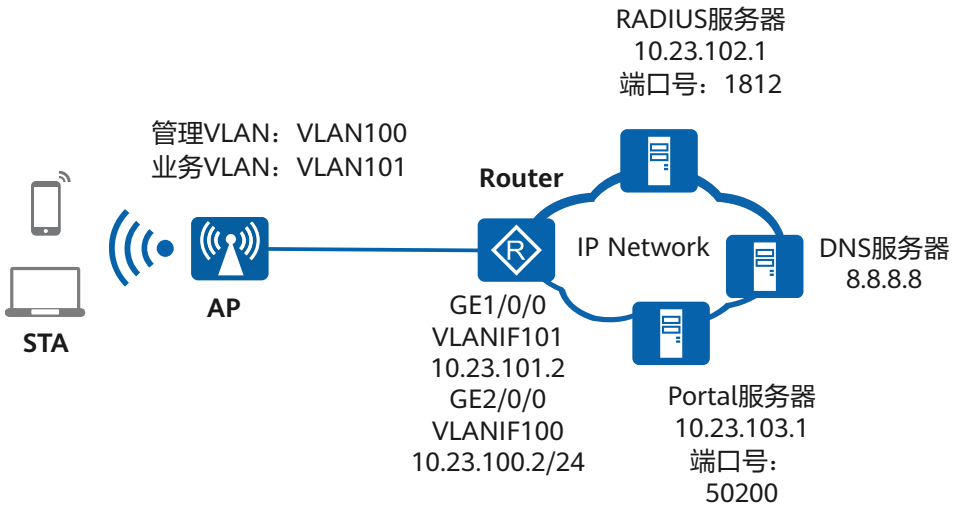
仅适用于AR651W-X4、AR651W-8P、AR651W、AR657W、AR303W、AR611W-S、AR611W、AR611W-LTE4CN、AR611W-LTE6EA、AR617VW、AR617VW-LTE4、AR617VW-LTE4EA和AR6120-VW路由器。

组网需求

某企业为了提高WLAN网络的安全性，采用外置Portal认证方式，实现对用户的接入控制。如下图所示。

- AR组网方式：旁挂二层组网
- DHCP部署方式：AR作为DHCP服务器为AP和STA分配IP地址。
- 业务数据转发方式：隧道转发。
- 认证方式：外置Portal认证。
- 安全策略：开放认证。

图 13-7 配置安全策略为 Portal 认证的业务组网图



版权所有 © 华为技术有限公司

数据准备

表 13-4 数据准备表

项目	数据
AP管理VLAN	VLAN100
STA业务VLAN	VLAN101
DHCP服务器	AR作为DHCP服务器为AP分配IP地址，为STA分配IP地址，STA的默认网关为10.23.101.2
AP的IP地址池	10.23.100.2~10.23.100.254/24
STA的IP地址池	10.23.101.3~10.23.101.254/24
AC的源接口IP地址	VLANIF100：10.23.100.1/24
AP组	● 名称：ap-group1 ● 绑定模板：VAP模板wlan-net、域管理模板default
域管理模板	● 名称：default ● 国家码：中国
SSID模板	● 名称：wlan-net ● SSID名称：wlan-net
安全模板	● 名称：wlan-net ● 安全策略：开放认证
RADIUS认证参数	RADIUS认证方案名称：wlan-net RADIUS服务器模板名称：wlan-net，其中： ● IP地址：10.23.102.1 ● 认证端口号：1812 ● 共享密钥：YsHsjx_202206
Portal服务器模板	● 名称：wlan-net ● IP地址：10.23.102.1 ● AC向Portal服务器主动发送报文时使用的目的端口号：50200 ● Portal认证共享密钥：YsHsjx_202206
Portal接入模板	● 名称：wlan-net ● 绑定的模板：Portal服务器模板wlan-net

版权所有 © 华为技术有限公司

项目	数据
免认证规则模板	● 名称：default_free_rule ● 免认证资源：DNS服务器的地址（8.8.8.8）
认证模板	● 名称：wlan-net ● 绑定的模板和认证方案：Portal接入模板wlan-net、RADIUS服务器模板wlan-net、免认证规则模板default_free_rule、认证方案wlan-net
VAP模板	● 名称：wlan-net ● 转发模式：隧道转发 ● 业务VLAN：VLAN101 ● 绑定模板：SSID模板wlan-net、安全模板wlan-net、认证模板wlan-net

配置思路

1. 配置网络互通，为AP和STA分配IP地址。
2. 配置AP上线。
3. 配置AC上的外置Portal认证参数。
   a. 配置RADIUS服务器参数。
   b. 配置针对外置Portal服务器的Portal接入模板，管理Portal接入控制参数。
   c. 配置免认证规则模板，实现AC放行访问DNS服务器的报文。
   d. 配置认证模板，管理外置Portal认证的相关配置。
4. 配置WLAN业务参数。
5. 配置第三方服务器参数。

操作步骤

步骤1 配置网络互通，为AP和STA分配IP地址

配置Router的接口GE1/0/0加入VLAN101，创建接口VLANIF101并配置IP地址为10.23.101.2/24，GE2/0/0加入VLAN100，创建接口VLANIF100并配置IP地址10.23.100.2/24，为STA和AP分配IP地址。

```
<Huawei> system-view
[Huawei] sysname Router
[Router] dhcp enable
[Router] vlan batch 100 101
[Router] interface gigabitethernet 1/0/0
[Router-GigabitEthernet1/0/0] port link-type trunk
[Router-GigabitEthernet1/0/0] port trunk allow-pass vlan 101
[Router-GigabitEthernet1/0/0] quit
[Router] interface vlanif 101
[Router-Vlanif101] ip address 10.23.101.2 24
[Router-Vlanif101] dhcp select interface
[Router-Vlanif101] dhcp server gateway-list 10.23.101.2
```

 版权所有 © 华为技术有限公司

```
[Router-Vlanif101] dhcp server dns-list 8.8.8.8
[Router-Vlanif101] quit
[Router] interface gigabitethernet 2/0/0
[Router-GigabitEthernet2/0/0] port link-type trunk
[Router-GigabitEthernet2/0/0] port trunk allow-pass vlan 100
[Router-GigabitEthernet2/0/0] quit
[Router] interface vlanif 100
[Router-Vlanif100] ip address 10.23.100.2 24
[Router-Vlanif100] dhcp select interface
[Router-Vlanif100] quit
```

步骤2 配置AP上线

创建AP组，用于将相同配置的AP都加入同一AP组中。

```
[Router] wlan ac
[Router-wlan-view] ap-group name ap-group1
Info: This operation may take a few seconds. Please wait for a moment.done.
[Router-wlan-ap-group-ap-group1] quit
```

创建域管理模板，在域管理模板下配置AC的国家码并在AP组下引用域管理模板。

```
[Router-wlan-view] regulatory-domain-profile name default
[Router-wlan-regulate-domain-default] country-code cn
Info: The current country code is same with the input country code.
[Router-wlan-regulate-domain-default] quit
[Router-wlan-view] ap-group name ap-group1
[Router-wlan-ap-group-ap-group1] regulatory-domain-profile default
Warning: Modifying the country code will clear channel, power and antenna gain configurations of the radio and reset the AP. Continue?[Y/N]:y
[Router-wlan-ap-group-ap-group1] quit
[Router-wlan-view] quit
```

配置AC的源接口。

```
[Router] capwap source interface vlanif 100
```

在AC上离线导入AP，并将AP加入AP组“ap-group1”中。假设AP的MAC地址为60de-4476-e360，并且根据AP的部署位置为AP配置名称，便于从名称上就能够了解AP的部署位置。例如MAC地址为60de-4476-e360的AP部署在1号区域，命名此AP为area_1。

说明

ap auth-mode命令缺省情况下为MAC认证，如果之前没有修改其缺省配置，可以不用执行**ap auth-mode mac-auth**。

举例中使用的AP为AP5030DN，具有射频0和射频1两个射频。AP5030DN的射频0为2.4GHz射频，射频1为5GHz射频。

```
[Router] wlan ac
[Router-wlan-view] ap auth-mode mac-auth
[Router-wlan-view] ap-id 0 ap-mac 60de-4476-e360
[Router-wlan-ap-0] ap-name area_1
[Router-wlan-ap-0] ap-group ap-group1
Warning: This operation may cause AP reset. If the country code changes, it will clear channel, power and antenna gain configuration s of the radio, Whether to continue? [Y/N]:y
Info: This operation may take a few seconds. Please wait for a moment.. done.
[Router-wlan-ap-0] quit
```

将AP上电后，当执行命令display ap all查看到AP的“State”字段为“nor”时，表示AP正常上线。

```
[Router-wlan-view] display ap all
Total AP information:
nor  : normal          [1]
Extra information:
P  : insufficient power supply
------------------------------------------------------------------------------------------------
```

 版权所有 © 华为技术有限公司

```
ID  MAC            Name   Group     IP            Type          State STA Uptime    ExtraInfo
-------------------------------------------------------------------------------------------
0   60de-4476-e360 area_1 ap-group1 10.23.100.254 AP5030DN      nor   0   10S       -
-------------------------------------------------------------------------------------------
Total: 1
```

步骤3 配置RADIUS服务器模板、RADIUS认证方案

说明

请确保AC上的RADIUS服务器地址、端口号、共享密钥配置正确，并且和RADIUS服务器保持一致。

配置RADIUS服务器模板。

```
[Router] radius-server template wlan-net
[Router-radius-wlan-net] radius-server authentication 10.23.102.1 1812
[Router-radius-wlan-net] radius-server shared-key cipher YsHsjx_202206
[Router-radius-wlan-net] quit
```

创建认证方案并配置认证方式为RADIUS。

```
[Router] aaa
[Router-aaa] authentication-scheme wlan-net
[Router-aaa-authen-wlan-net] authentication-mode radius
[Router-aaa-authen-wlan-net] quit
```

创建认证域“wlan-net”，并在其上绑定AAA认证方案“wlan-net”与RADIUS服务器模板“wlan-net”。

```
[Router-aaa] domain wlan-net
[Router-aaa-domain-wlan-net] authentication-scheme wlan-net
[Router-aaa-domain-wlan-net] radius-server wlan-net
[Router-aaa-domain-wlan-net] quit
[Router-aaa] quit
```

步骤4 配置Portal服务器模板

说明

请确保AC上Portal服务器地址、URL地址、端口号、共享密钥配置正确，并且和Portal服务器保持一致。

```
[Router] web-auth-server wlan-net
[Router-web-auth-server-wlan-net] server-ip 10.23.102.1
[Router-web-auth-server-wlan-net] port 50200
[Router-web-auth-server-wlan-net] url http://10.23.102.1:8080/webagent
[Router-web-auth-server-wlan-net] shared-key cipher YsHsjx_202206
[Router-web-auth-server-wlan-net] quit
```

步骤5 配置Portal接入模板“wlan-net”，并配置Portal认证为二层Portal认证

```
[Router] portal-access-profile name wlan-net
[Router-portal-access-profile-wlan-net] web-auth-server wlan-net direct
[Router-portal-access-profile-wlan-net] quit
```

步骤6 配置免认证规则模板

```
[Router] free-rule-template name default_free_rule
[Router-free-rule-default_free_rule] free-rule 1 destination ip 8.8.8.8 mask 32
[Router-free-rule-default_free_rule] quit
```

步骤7 配置认证模板“wlan-net”

```
[Router] authentication-profile name wlan-net
[Router-authentication-profile-wlan-net] portal-access-profile wlan-net
[Router-authen-profile-profile-wlan-net] access-domain wlan-net force
[Router-authentication-profile-wlan-net] free-rule-template default_free_rule
[Router-authentication-profile-wlan-net] quit
```

 版权所有 © 华为技术有限公司

步骤8 配置WLAN业务参数

创建名为“wlan-net”的安全模板，并配置安全策略为open方式的开放认证。缺省情况下，安全策略为open方式的开放认证。

```
[Router] wlan ac
[Router-wlan-view] security-profile name wlan-net
[Router-wlan-sec-prof-wlan-net] security open
[Router-wlan-sec-prof-wlan-net] quit
```

创建名为“wlan-net”的SSID模板，并配置SSID名称为“wlan-net”。

```
[Router-wlan-view] ssid-profile name wlan-net
[Router-wlan-ssid-prof-wlan-net] ssid wlan-net
Warning: This action may cause service interruption. Continue?[Y/N]y
Info: This operation may take a few seconds, please wait.done.
[Router-wlan-ssid-prof-wlan-net] quit
```

创建名为“wlan-net”的VAP模板，配置业务数据转发模式、业务VLAN，并且引用安全模板、SSID模板和认证模板。

```
[Router-wlan-view] vap-profile name wlan-net
[Router-wlan-vap-prof-wlan-net] forward-mode tunnel
Warning: This action may cause service interruption. Continue?[Y/N]y
Info: This operation may take a few seconds, please wait.done.
[Router-wlan-vap-prof-wlan-net] service-vlan vlan-id 101
Info: This operation may take a few seconds, please wait.done.
[Router-wlan-vap-prof-wlan-net] security-profile wlan-net
Info: This operation may take a few seconds, please wait..done.
[Router-wlan-vap-prof-wlan-net] ssid-profile wlan-net
Info: This operation may take a few seconds, please wait..done.
[Router-wlan-vap-prof-wlan-net] authentication-profile wlan-net
[Router-wlan-vap-prof-wlan-net] quit
```

配置AP组引用VAP模板，AP上射频0和射频1都使用VAP模板“wlan-net”的配置。

```
[Router-wlan-view] ap-group name ap-group1
[Router-wlan-ap-group-ap-group1] vap-profile wlan-net wlan 1 radio 0
[Router-wlan-ap-group-ap-group1] vap-profile wlan-net wlan 1 radio 1
[Router-wlan-ap-group-ap-group1] quit
[Router-wlan-view] quit
```

步骤9 配置第三方服务器

具体配置方法建议参考相应的产品手册。

步骤10 检查配置结果

- 完成配置后，STA可以搜索到SSID为wlan-net的无线网络。
- STA关联到无线网络上后，能够被分配相应的IP地址。
- STA上打开浏览器访问网络时，会自动跳转到Portal服务器提供的认证页面，在页面上输入正确的用户名和密码后，STA认证成功并可以访问网络。

----结束

配置文件

Router的配置文件

```
#
sysname Router
#
dhcp enable
#
vlan batch 100 101
#
```

 版权所有 © 华为技术有限公司

```
interface Vlanif101
 ip address 10.23.101.2 255.255.255.0
 dhcp select interface
 dhcp server gateway-list 10.23.101.2
 dhcp server dns-list 8.8.8.8
#
interface GigabitEthernet1/0/0
 port link-type trunk
 port trunk allow-pass vlan 101
#
interface Vlanif100
 ip address 10.23.100.2 255.255.255.0
 dhcp select interface
#
interface GigabitEthernet2/0/0
 port link-type trunk
 port trunk allow-pass vlan 100
#
authentication-profile name wlan-net
 portal-access-profile wlan-net
 access-domain wlan-net force
 free-rule-template default_free_rule
#
aaa
 authentication-scheme wlan-net
  authentication-mode radius
 domain wlan-net
  authentication-scheme wlan-net
  radius-server wlan-net
#
capwap source interface vlanif100
#
radius-server template wlan-net
 radius-server shared-key cipher %^%#Oc6_BMCw#9gZ2@SMVtk!PAC6>Ou*eLW/"qLp+f#$%^%#
 radius-server authentication 10.23.102.1 1812 weight 80
#
free-rule-template name default_free_rule
 free-rule 1 destination ip 8.8.8.8 mask 255.255.255.255
#
web-auth-server wlan-net
 server-ip 10.23.102.1
 port 50200
 url http://10.23.102.1:8080/webagent
 shared-key cipher %^%#4~ZXE3]6@BXu;2;aw}hA{rSb,@"L@T#e{%6G1AiD%^%#
#
portal-access-profile name wlan-net
 web-auth-server wlan-net direct
#
wlan ac
 security-profile name wlan-net
 ssid-profile name wlan-net
  ssid wlan-net
 vap-profile name wlan-net
  forward-mode tunnel
  service-vlan vlan-id 101
  ssid-profile wlan-net
  security-profile wlan-net
  authentication-profile wlan-net
 ap-group name ap-group1
  regulatory-domain-profile default
  radio 0
   vap-profile wlan-net wlan 1
  radio 1
   vap-profile wlan-net wlan 1
 ap-id 0 type-id 35 ap-mac 60de-4476-e360 ap-sn 210235554710CB000042
  ap-name area_1
  ap-group ap-group1
#
return
```

 版权所有 © 华为技术有限公司

配置注意事项

- 纯组播报文由于协议要求在无线空口没有ACK机制保障，且无线空口链路不稳定，为了纯组播报文能够稳定发送，通常会以低速报文形式发送。如果网络侧有大量异常组播流量涌入，则会造成无线空口拥堵。为了减小大量低速组播报文对无线网络造成的冲击，建议配置组播报文抑制功能。配置前请确认是否有组播业务，如果有，请谨慎配置限速值。
  - 业务数据转发方式采用直接转发时，建议在直连AP的交换机接口上配置组播报文抑制。
  - 业务数据转发方式采用隧道转发时，建议在AC的流量模板下配置组播报文抑制。
- 建议在与AP直连的设备接口上配置端口隔离，如果不配置端口隔离，尤其是业务数据转发方式采用直接转发时，可能会在VLAN内形成大量不必要的广播报文，导致网络阻塞，影响用户体验。
- 隧道转发模式下，管理VLAN和业务VLAN不能配置为同一VLAN，且AP和AC之间只能放通管理VLAN，不能放通业务VLAN。

13.8 配置安全策略为 802.1X 认证的业务示例

规格

仅适用于AR651W-X4、AR651W-8P、AR651W、AR657W、AR303W、AR611W-S、AR611W、AR611W-LTE4CN、AR611W-LTE6EA、AR617VW、AR617VW-LTE4、AR617VW-LTE4EA和AR6120-VW路由器。

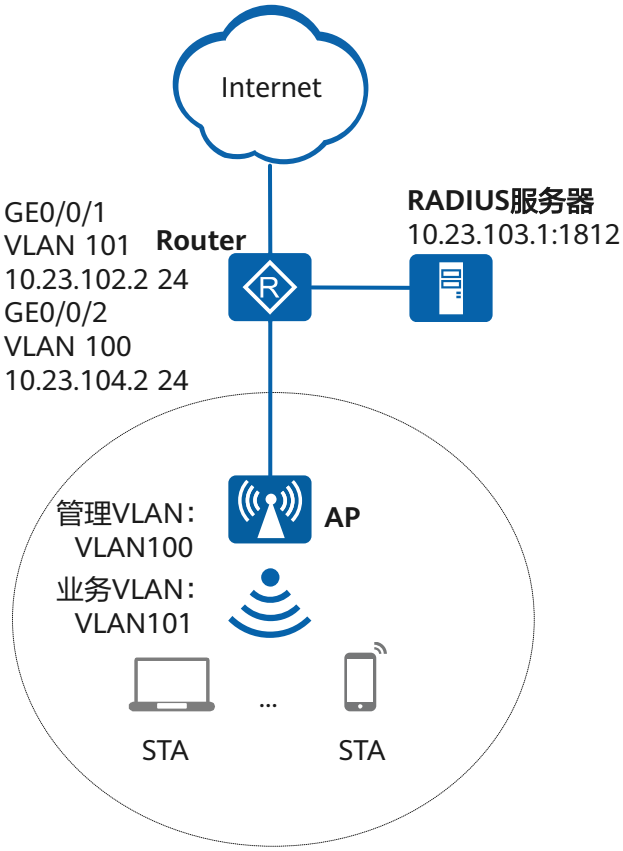
组网需求

用户接入WLAN网络，使用802.1X客户端进行认证，输入正确的用户名和密码后可以无线上网。且在覆盖区域内移动发生漫游时，不影响用户的业务使用。如下图所示。

- AC组网方式：旁挂二层组网
- DHCP部署方式：AR作为DHCP服务器为AP和STA分配IP地址。
- 业务数据转发方式：直接转发。
- WLAN认证方式：WPA-WPA2+802.1X+AES。

 版权所有 © 华为技术有限公司

图 13-8 配置安全策略为 802.1X 认证的业务组网图



数据准备

表 13-5 数据准备表

项目	数据
管理VLAN	VLAN100
业务VLAN	VLAN101
AC的源接口	VLANIF100：10.23.100.1/24
DHCP服务器	AR作为DHCP服务器为AP和STA分配IP地址。
AP的IP地址池	10.23.100.2~10.23.100.254/24
STA的IP地址池	10.23.101.3~10.23.101.254/24

版权所有 © 华为技术有限公司

项目	数据
RADIUS认证参数	RADIUS服务器模板名称：wlan-net ● IP地址：10.23.103.1 ● 认证端口号：1812 ● 共享密钥：YsHsjx_202206 ● 认证方案：wlan-net
802.1X接入模板	● 名称：wlan-net ● 认证方式：EAP
认证模板	● 名称：wlan-net ● 引用模板和认证方案：802.1X接入模板wlan-net、RADIUS服务器模板wlan-net、认证方案wlan-net
AP组	● 名称：ap-group1 ● 引用模板：VAP模板wlan-net、域管理模板default
域管理模板	● 名称：default ● 国际码：中国
SSID模板	● 名称：wlan-net ● SSID名称：wlan-net
安全模板	● 名称：wlan-net ● 安全策略：WPA-WPA2+802.1X+AES
VAP模板	● 名称：wlan-net ● 转发模式：直接转发 ● 业务VLAN：VLAN101 ● 引用模板：SSID模板wlan-net、安全模板wlan-net、认证模板wlan-net

配置思路

1. 配置网络互通，为AP和STA分配IP地址。
2. 配置AP上线。
3. 配置AC上的802.1X认证。
4. 配置第三方服务器。

说明

AC侧配置的RADIUS共享密钥需要和服务器侧保持一致。

版权所有 © 华为技术有限公司

操作步骤

步骤1 配置网络互通，为AP和STA分配IP地址

配置Router的接口GE0/0/1加入VLAN101，创建接口VLANIF101并配置IP地址为10.23.102.2/24，GE0/0/2加入VLAN100，创建接口VLANIF100并配置IP地址为10.23.104.2/24，并配置指向RADIUS服务器和STA网段的静态路由。

说明

DNS服务器地址请根据实际需要配置。常用配置方法如下：

- 接口地址池场景，需要在VLANIF接口视图下执行命令**dhcp server dns-list** *ip-address* &<1-8>。
- 全局地址池场景，需要在IP地址池视图下执行命令**dns-list** *ip-address* &<1-8>。

```
<Huawei> system-view
[Huawei] sysname Router
[Huawei] dhcp enable
[Router] vlan batch 100 101
[Router] interface gigabitethernet 0/0/1
[Router-GigabitEthernet0/0/1] port link-type trunk
[Router-GigabitEthernet0/0/1] port trunk allow-pass vlan 101
[Router-GigabitEthernet0/0/1] quit
[Router] interface vlanif 101
[Router-Vlanif101] ip address 10.23.102.2 24
[Router-Vlanif101] dhcp select interface
[Router-Vlanif101] quit
[Router] interface gigabitethernet 0/0/2
[Router-GigabitEthernet0/0/2] port link-type trunk
[Router-GigabitEthernet0/0/2] port trunk allow-pass vlan 100
[Router-GigabitEthernet0/0/2] quit
[Router] interface vlanif 100
[Router-Vlanif100] ip address 10.23.104.2 24
[Router-Vlanif100] dhcp select interface
[Router-Vlanif100] quit
[Router] ip route-static 10.23.103.0 24 10.23.102.1
[Router] ip route-static 10.23.101.0 24 10.23.104.1
```

步骤2 配置AP上线

创建AP组，用于将相同配置的AP都加入同一AP组中。

```
[Router] wlan ac
[Router-wlan-view] ap-group name ap-group1
Info: This operation may take a few seconds. Please wait for a moment.done.
[Router-wlan-ap-group-ap-group1] quit
```

创建域管理模板，在域管理模板下配置AC的国家码并在AP组下引用域管理模板。

```
[Router-wlan-view] regulatory-domain-profile name default
[Router-wlan-regulate-domain-default] country-code cn
Info: The current country code is same with the input country code.
[Router-wlan-regulate-domain-default] quit
[Router-wlan-view] ap-group name ap-group1
[Router-wlan-ap-group-ap-group1] regulatory-domain-profile default
Warning: Modifying the country code will clear channel, power and antenna gain configurations of the radio and reset the AP. Continue?[Y/N]:y
[Router-wlan-ap-group-ap-group1] quit
[Router-wlan-view] quit
```

配置AC的源接口。

```
[Router] capwap source interface vlanif 100
```

在AC上离线导入AP，并将AP加入AP组“ap-group1”中。假设AP的MAC地址为60de-4476-e360，并且根据AP的部署位置为AP配置名称，便于从名称上就能够了解

 版权所有 © 华为技术有限公司

AP的部署位置。例如MAC地址为60de-4476-e360的AP部署在1号区域，命名此AP为area_1。

说明

ap auth-mode命令缺省情况下为MAC认证，如果之前没有修改其缺省配置，可以不用执行**ap auth-mode mac-auth**。

举例中使用的AP为AP5030DN，具有射频0和射频1两个射频。AP5030DN的射频0为2.4GHz射频，射频1为5GHz射频。

```
[Router] wlan ac
[Router-wlan-view] ap auth-mode mac-auth
[Router-wlan-view] ap-id 0 ap-mac 60de-4476-e360
[Router-wlan-ap-0] ap-name area_1
[Router-wlan-ap-0] ap-group ap-group1
Warning: This operation may cause AP reset. If the country code changes, it will clear channel, power and antenna gain configuration s of the radio, Whether to continue? [Y/N]:y
Info: This operation may take a few seconds. Please wait for a moment.. done.
[Router-wlan-ap-0] quit
```

将AP上电后，当执行命令display ap all查看到AP的“State”字段为“nor”时，表示AP正常上线。

```
[Router-wlan-view] display ap all
Total AP information:
nor  : normal          [1]
-------------------------------------------------------------------------------------------------
ID   MAC           Name   Group     IP           Type           State STA Uptime   ExtraInfo
-------------------------------------------------------------------------------------------------
0    60de-4476-e360 area_1 ap-group1 10.23.100.254 AP5030DN       nor   0   10S      -
-------------------------------------------------------------------------------------------------
Total: 1
```

步骤3 配置AP射频的信道和功率

说明

射频的信道和功率自动调优功能默认开启，如果不关闭此功能则会导致手动配置不生效。举例中AP射频的信道和功率仅为示例，实际配置中请根据AP的国家码和网规结果进行配置。

创建名称为“radio-profile1”的2G射频模板，名称为“radio-profile2”的5G射频模板， 并在名为“ap-group1”的AP组中引用“radio-profile1”和“radio-profile2”。

```
[Huawei-wlan-view] radio-2g-profile name radio-profile1
[Huawei-wlan-radio-2g-prof-radio-profile1] quit
[Huawei-wlan-view] radio-5g-profile name radio-profile2
[Huawei-wlan-radio-5g-prof-radio-profile2] quit
[Huawei-wlan-view] ap-group name ap-group1
Info: This operation may take a few seconds. Please wait for a moment.done.
[Huawei-wlan-ap-group-ap-group1] radio-2g-profile radio-profile1 radio 0
Warning: This action may cause service interruption. Continue?[Y/N]y
[Huawei-wlan-ap-group-ap-group1] radio-5g-profile radio-profile2 radio 1
Warning: This action may cause service interruption. Continue?[Y/N]y
[Huawei-wlan-ap-group-ap-group1] quit
```

关闭AP射频0和射频1的信道和功率自动调优功能。

```
[Huawei-wlan-view] rrm-profile name wlan-net
[Huawei-wlan-rrm-prof-wlan-net] calibrate auto-channel-select disable
[Huawei-wlan-rrm-prof-wlan-net] calibrate auto-txpower-select disable
[Huawei-wlan-rrm-prof-wlan-net] quit
[Huawei-wlan-view] radio-2g-profile name radio-profile1
[Huawei-wlan-radio-2g-prof-radio-profile1] rrm-profile wlan-net
Warning: This action may cause service interruption. Continue?[Y/N]y
[Huawei-wlan-radio-2g-prof-radio-profile1] quit
[Huawei-wlan-view] radio-5g-profile name radio-profile2
```

 版权所有 © 华为技术有限公司

```
[Huawei-wlan-radio-5g-prof-radio-profile2] rrm-profile wlan-net
Warning: This action may cause service interruption. Continue?[Y/N]y
[Huawei-wlan-radio-5g-prof-radio-profile2] quit
```

配置AP射频0的信道和功率。

```
[Router-wlan-view] ap-id 0
[Router-wlan-ap-0] radio 0
[Router-wlan-radio-0/0] channel 20mhz 6
Warning: This action may cause service interruption. Continue?[Y/N]y
[Router-wlan-radio-0/0] eirp 127
[Router-wlan-radio-0/0] quit
```

配置AP射频1的信道和功率。

```
[Router-wlan-ap-0] radio 1
[Router-wlan-radio-0/1] channel 80mhz 149
Warning: This action may cause service interruption. Continue?[Y/N]y
[Router-wlan-radio-0/1] eirp 127
[Router-wlan-radio-0/1] quit
[Router-wlan-ap-0] quit
```

步骤4 配置802.1X认证

1. 配置RADIUS认证参数

   # 创建RADIUS服务器模板。

   ```
   [Router-wlan-view] quit
   [Router] radius-server template wlan-net
   [Router-radius-wlan-net] radius-server authentication 10.23.103.1 1812
   [Router-radius-wlan-net] radius-server shared-key cipher huawei@123
   [Router-radius-wlan-net] quit
   ```

   # 创建RADIUS方式的认证方案。

   ```
   [Router] aaa
   [Router-aaa] authentication-scheme wlan-net
   [Router-aaa-authen-wlan-net] authentication-mode radius
   [Router-aaa-authen-wlan-net] quit
   [Router-aaa] quit
   ```

   # 创建认证域“wlan-net”，并在其上绑定AAA认证方案“wlan-net”与RADIUS服务器模板“wlan-net”。

   ```
   [Router-aaa] domain wlan-net
   [Router-aaa-domain-wlan-net] authentication-scheme wlan-net
   [Router-aaa-domain-wlan-net] radius-server wlan-net
   [Router-aaa-domain-wlan-net] quit
   [Router-aaa] quit
   ```

2. 配置802.1X接入模板，管理802.1X接入控制参数。

   # 创建名为“wlan-net”的802.1X接入模板。

   ```
   [Router] dot1x-access-profile name wlan-net
   ```

   # 配置认证方式为EAP中继模式。

   ```
   [Router-dot1x-access-profile-wlan-net] dot1x authentication-method eap
   [Router-dot1x-access-profile-wlan-net] quit
   ```

3. 创建名为“wlan-net”的认证模板，并引用802.1X接入模板。

   ```
   [Router] authentication-profile name wlan-net
   [Router-authen-profile-wlan-net] dot1x-access-profile wlan-net
   [Router-authen-profile-wlan-net] access-domain wlan-net force
   [Router-authen-profile-wlan-net] quit
   ```

4. 在接口GE0/0/2上绑定认证模板“wlan-net”，使能802.1X认证。

 版权所有 © 华为技术有限公司

```
[Router] interface gigabitethernet 0/0/2
[Router-GigabitEthernet0/0/2] authentication-profile wlan-net
[Router-GigabitEthernet0/0/2] quit
```

5. 配置WLAN业务参数

   # 创建名为“wlan-net”的安全模板，并配置安全策略。

   ```
   [Router] wlan ac
   [Router-wlan-view] security-profile name wlan-net
   [Router-wlan-sec-prof-wlan-net] security wpa-wpa2 dot1x aes
   [Router-wlan-sec-prof-wlan-net] quit
   ```

   # 创建名为“wlan-net”的SSID模板，并配置SSID名称为“wlan-net”。

   ```
   [Router-wlan-view] ssid-profile name wlan-net
   [Router-wlan-ssid-prof-wlan-net] ssid wlan-net
   Warning: This action may cause service interruption. Continue?[Y/N]y
   Info: This operation may take a few seconds, please wait.done.
   [Router-wlan-ssid-prof-wlan-net] quit
   ```

   # 创建名为“wlan-net”的VAP模板，配置业务数据转发模式为直接转发、业务VLAN，并且引用安全模板、认证模板和SSID模板。

   ```
   [Router-wlan-view] vap-profile name wlan-net
   [Router-wlan-vap-prof-wlan-net] forward-mode direct-forward
   Warning: This action may cause service interruption. Continue?[Y/N]y
   Info: This operation may take a few seconds, please wait.done.
   [Router-wlan-vap-prof-wlan-net] service-vlan vlan-id 101
   Info: This operation may take a few seconds, please wait.done.
   [Router-wlan-vap-prof-wlan-net] security-profile wlan-net
   Info: This operation may take a few seconds, please wait..done.
   [Router-wlan-vap-prof-wlan-net] ssid-profile wlan-net
   Info: This operation may take a few seconds, please wait..done.
   [Router-wlan-vap-prof-wlan-net] authentication-profile wlan-net
   [Router-wlan-vap-prof-wlan-net] quit
   ```

   # 配置AP组引用VAP模板，AP上射频0和射频1都使用VAP模板“wlan-net”的配置。

   ```
   [Router-wlan-view] ap-group name ap-group1
   [Router-wlan-ap-group-ap-group1] vap-profile wlan-net wlan 1 radio 0
   [Router-wlan-ap-group-ap-group1] vap-profile wlan-net wlan 1 radio 1
   [Router-wlan-ap-group-ap-group1] quit
   [Router-wlan-view] quit
   ```

步骤5 配置第三方服务器。

具体配置方法建议参考相应的产品手册。

步骤6 检查配置结果

- 完成配置后，用户可通过无线终端搜索到SSID为**wlan-net**的无线网络。
- 用户关联到无线网络上后，无线PC能够被分配相应的IP地址。
- 在STA上使用802.1X客户端进行认证，输入正确的用户名和密码后，STA认证成功，正常访问WLAN网络。需要根据设置的认证方式**PEAP**对客户端进行相应的配置。
  - Windows 7系统下的配置
    i. 进入管理无线网络页面，单击“添加”，选择手动创建网络配置文件，添加SSID为**wlan-net**，并选择认证方式为**WPA2-企业**，加密使用的算法**AES**，单击“下一步”。
    ii. 单击“更改连接设置”，进入“无线网络属性”界面，选择“安全”页签，单击“设置”，取消勾选“验证服务器证书”（此处不验证服务器

 版权所有 © 华为技术有限公司

证书），单击“配置”，取消勾选“自动使用Windows登录名和密码”，单击“确定”。

iii. 单击“确定”，返回“无线网络属性”界面，单击“高级设置”，在“高级设置”界面，勾选“指定身份验证模式”，并选择身份验证模式为“用户身份验证”，单击“确定”。

- 无线用户接入后，在AR上执行命令**display access-user access-type dot1x**，可以查看到认证类型为“802.1X”的用户中，名为“huawei”的用户已成功上线。

```
[Router] display access-user access-type dot1x
--------------------------------------------------------------------------------
UserID Username              IP address      MAC           Status
--------------------------------------------------------------------------------
460    huawei                10.23.101.254   8000-6e74-e78a Success
--------------------------------------------------------------------------------
Total: 1, printed: 1
```

----结束

配置文件

Router的配置文件

```
#
sysname Router
#
dhcp enable
#
vlan batch 100 101
#
interface Vlanif101
 ip address 10.23.102.2 255.255.255.0
 dhcp select interface
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 101
#
interface Vlanif100
 ip address 10.23.104.2 255.255.255.0
 dhcp select interface
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 100
 authentication-profile wlan-net
#
ip route-static 10.23.103.0 24 10.23.102.1
ip route-static 10.23.101.0 24 10.23.104.1
#
#
authentication-profile name wlan-net
 dot1x-access-profile wlan-net
 access-domain wlan-net force
#
radius-server template wlan-net
 radius-server shared-key cipher %^%#*7d1;XNof/|Q0:DsP!,W51DIYPx}`AARBdJ'0B^$%^%#
 radius-server authentication 10.23.103.1 1812 weight 80
#
aaa
 authentication-scheme wlan-net
  authentication-mode radius
 domain wlan-net
  authentication-scheme wlan-net
  radius-server wlan-net
#
capwap source interface vlanif100
```

 版权所有 © 华为技术有限公司

```
#
wlan ac
 security-profile name wlan-net
  security wpa-wpa2 dot1x aes
 ssid-profile name wlan-net
  ssid wlan-net
 vap-profile name wlan-net
  service-vlan vlan-id 101
  ssid-profile wlan-net
  security-profile wlan-net
  authentication-profile wlan-net
 regulatory-domain-profile name default
 rrm-profile name wlan-net
  calibrate auto-channel-select disable
  calibrate auto-txpower-select disable
 radio-2g-profile name radio-profile1
  rrm-profile wlan-net
 radio-5g-profile name radio-profile2
  rrm-profile wlan-net
 ap-group name ap-group1
  radio 0
   vap-profile wlan-net wlan 1
   radio-2g-profile radio-profile1
  radio 1
   vap-profile wlan-net wlan 1
   radio-5g-profile radio-profile2
 ap-id 0 type-id 35 ap-mac 60de-4476-e360 ap-sn 210235554710CB000042
  ap-name area_1
  ap-group ap-group1
  radio 0
   channel 20mhz 6
   eirp 127
  radio 1
   channel 80mhz 149
   eirp 127
#
dot1x-access-profile name wlan-net
#
return
```

配置注意事项

- 纯组播报文由于协议要求在无线空口没有ACK机制保障，且无线空口链路不稳定，为了纯组播报文能够稳定发送，通常会以低速报文形式发送。如果网络侧有大量异常组播流量涌入，则会造成无线空口拥堵。为了减小大量低速组播报文对无线网络造成的冲击，建议配置组播报文抑制功能。配置前请确认是否有组播业务，如果有，请谨慎配置限速值。
  - 业务数据转发方式采用直接转发时，建议在直连AP的交换机接口上配置组播报文抑制。
  - 业务数据转发方式采用隧道转发时，建议在AC的流量模板下配置组播报文抑制。
- 建议在与AP直连的设备接口上配置端口隔离，如果不配置端口隔离，尤其是业务数据转发方式采用直接转发时，可能会在VLAN内形成大量不必要的广播报文，导致网络阻塞，影响用户体验。
- 隧道转发模式下，管理VLAN和业务VLAN不能配置为同一VLAN，且AP和AC之间只能放通管理VLAN，不能放通业务VLAN。

13.9 配置安全策略为 MAC 认证的业务示例

 版权所有 © 华为技术有限公司

规格

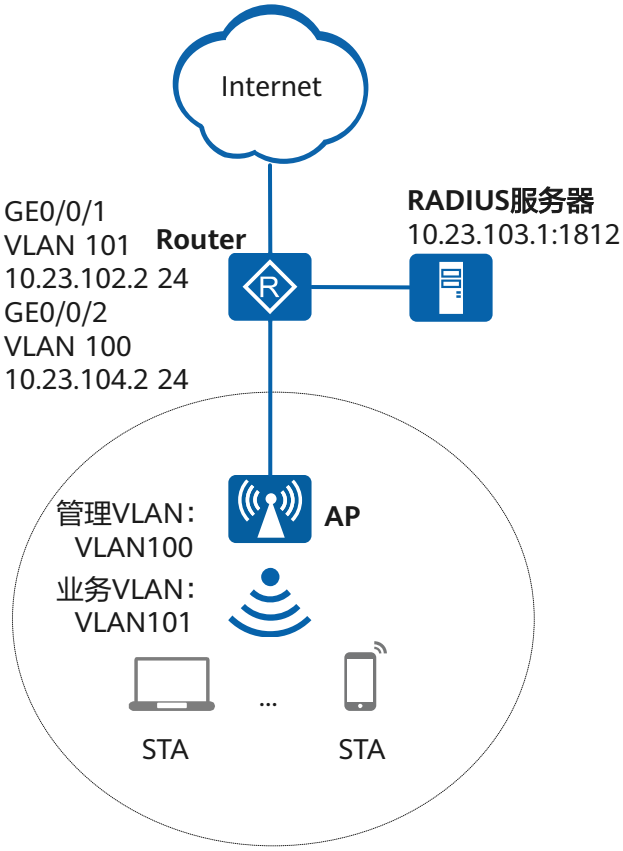
仅适用于AR651W-X4、AR651W-8P、AR651W、AR657W、AR303W、AR611W-S、AR611W、AR611W-LTE4CN、AR611W-LTE6EA、AR617VW、AR617VW-LTE4、AR617VW-LTE4EA和AR6120-VW路由器。

组网需求

无线网络打印机、无线网络电话等哑终端接入WLAN网络，由于无法安装认证客户端，使用MAC认证。如下图所示。

- AC组网方式：旁挂二层组网
- DHCP部署方式：AR作为DHCP服务器为AP和STA分配IP地址。
- 业务数据转发方式：直接转发。
- WLAN认证方式：开放式系统认证。

图 13-9 配置安全策略为 MAC 认证的业务组网图



版权所有 © 华为技术有限公司

数据准备

表 13-6 数据准备表

项目	数据
管理VLAN	VLAN100
业务VLAN	VLAN101
AC的源接口	VLANIF100：10.23.100.1/24
DHCP服务器	AR作为DHCP服务器为AP和STA分配IP地址。
AP的IP地址池	10.23.100.2~10.23.100.254/24
STA的IP地址池	10.23.101.3~10.23.101.254/24
RADIUS认证参数	RADIUS服务器模板名称：wlan-net ● IP地址：10.23.103.1 ● 认证端口号：1812 ● 共享密钥：YsHsjx_202206 ● 认证方案：wlan-net
MAC接入模板	名称：wlan-net
认证模板	● 名称：wlan-net ● 引用模板和认证方案：MAC接入模板wlan-net、RADIUS服务器模板wlan-net、认证方案wlan-net
AP组	● 名称：ap-group1 ● 引用模板：VAP模板wlan-net、域管理模板default
域管理模板	● 名称：default ● 国际码：中国
SSID模板	● 名称：wlan-net ● SSID名称：wlan-net
安全模板	● 名称：wlan-net ● 安全策略：开放式系统认证
VAP模板	● 名称：wlan-net ● 转发模式：直接转发 ● 业务VLAN：VLAN101 ● 引用模板：SSID模板wlan-net、安全模板wlan-net、认证模板wlan-net

版权所有 © 华为技术有限公司

配置思路

1. 配置网络互通，为AP和STA分配IP地址。
2. 配置AP上线。
3. 配置AC上的MAC认证。
4. 配置第三方服务器。

说明

AC侧配置的RADIUS共享密钥需要和服务器侧保持一致。

操作步骤

步骤1 配置网络互通，为AP和STA分配IP地址

配置Router的接口GE0/0/1加入VLAN101，创建接口VLANIF101并配置IP地址为10.23.102.2/24，GE0/0/2加入VLAN100，创建接口VLANIF100并配置IP地址为10.23.104.2/24，并配置指向RADIUS服务器和STA网段的静态路由。

说明

DNS服务器地址请根据实际需要配置。常用配置方法如下：

- 接口地址池场景，需要在VLANIF接口视图下执行命令**dhcp server dns-list** *ip-address* &<1-8>。
- 全局地址池场景，需要在IP地址池视图下执行命令**dns-list** *ip-address* &<1-8>。

```
<Huawei> system-view
[Huawei] sysname Router
[Huawei] dhcp enable
[Router] vlan batch 100 101
[Router] interface gigabitethernet 0/0/1
[Router-GigabitEthernet0/0/1] port link-type trunk
[Router-GigabitEthernet0/0/1] port trunk allow-pass vlan 101
[Router-GigabitEthernet0/0/1] quit
[Router] interface vlanif 101
[Router-Vlanif101] ip address 10.23.102.2 24
[Router-Vlanif101] dhcp select interface
[Router-Vlanif101] quit
[Router] interface gigabitethernet 0/0/2
[Router-GigabitEthernet0/0/2] port link-type trunk
[Router-GigabitEthernet0/0/2] port trunk allow-pass vlan 100
[Router-GigabitEthernet0/0/2] quit
[Router] interface vlanif 100
[Router-Vlanif100] ip address 10.23.104.2 24
[Router-Vlanif100] dhcp select interface
[Router-Vlanif100] quit
[Router] ip route-static 10.23.103.0 24 10.23.102.1
[Router] ip route-static 10.23.101.0 24 10.23.104.1
```

步骤2 配置AP上线

创建AP组，用于将相同配置的AP都加入同一AP组中。

```
[Router] wlan ac
[Router-wlan-view] ap-group name ap-group1
Info: This operation may take a few seconds. Please wait for a moment.done.
[Router-wlan-ap-group-ap-group1] quit
```

创建域管理模板，在域管理模板下配置AC的国家码并在AP组下引用域管理模板。

```
[Router-wlan-view] regulatory-domain-profile name default
[Router-wlan-regulate-domain-default] country-code cn
Info: The current country code is same with the input country code.
```

 版权所有 © 华为技术有限公司

```
[Router-wlan-regulate-domain-default] quit
[Router-wlan-view] ap-group name ap-group1
[Router-wlan-ap-group-ap-group1] regulatory-domain-profile default
Warning: Modifying the country code will clear channel, power and antenna gain configurations of the radio and reset the AP. Continue?[Y/N]:y
[Router-wlan-ap-group-ap-group1] quit
[Router-wlan-view] quit
```

配置AC的源接口。

```
[Router] capwap source interface vlanif 100
```

在AC上离线导入AP，并将AP加入AP组“ap-group1”中。假设AP的MAC地址为60de-4476-e360，并且根据AP的部署位置为AP配置名称，便于从名称上就能够了解AP的部署位置。例如MAC地址为60de-4476-e360的AP部署在1号区域，命名此AP为area_1。

说明

ap auth-mode命令缺省情况下为MAC认证，如果之前没有修改其缺省配置，可以不用执行**ap auth-mode mac-auth**。

举例中使用的AP为AP5030DN，具有射频0和射频1两个射频。AP5030DN的射频0为2.4GHz射频，射频1为5GHz射频。

```
[Router] wlan ac
[Router-wlan-view] ap auth-mode mac-auth
[Router-wlan-view] ap-id 0 ap-mac 60de-4476-e360
[Router-wlan-ap-0] ap-name area_1
[Router-wlan-ap-0] ap-group ap-group1
Warning: This operation may cause AP reset. If the country code changes, it will clear channel, power and antenna gain configuration s of the radio, Whether to continue? [Y/N]:y
[Router-wlan-ap-0] quit
```

将AP上电后，当执行命令display ap all查看到AP的“State”字段为“nor”时，表示AP正常上线。

```
[Router-wlan-view] display ap all
Total AP information:
nor  : normal          [1]
--------------------------------------------------------------------------------------------------
ID   MAC            Name   Group     IP            Type           State STA Uptime   ExtraInfo
--------------------------------------------------------------------------------------------------
0    60de-4476-e360 area_1 ap-group1 10.23.100.254 AP5030DN       nor   0   10S      -
--------------------------------------------------------------------------------------------------
Total: 1
```

步骤3 配置AP射频的信道和功率

说明

射频的信道和功率自动调优功能默认开启，如果不关闭此功能则会导致手动配置不生效。举例中AP射频的信道和功率仅为示例，实际配置中请根据AP的国家码和网规结果进行配置。

创建名称为“radio-profile1”的2G射频模板，名称为“radio-profile2”的5G射频模板， 并在名为“ap-group1”的AP组中引用“radio-profile1”和“radio-profile2”。

```
[Huawei-wlan-view] radio-2g-profile name radio-profile1
[Huawei-wlan-radio-2g-prof-radio-profile1] quit
[Huawei-wlan-view] radio-5g-profile name radio-profile2
[Huawei-wlan-radio-5g-prof-radio-profile2] quit
[Huawei-wlan-view] ap-group name ap-group1
Info: This operation may take a few seconds. Please wait for a moment.done.
[Huawei-wlan-ap-group-ap-group1] radio-2g-profile radio-profile1 radio 0
Warning: This action may cause service interruption. Continue?[Y/N]y
[Huawei-wlan-ap-group-ap-group1] radio-5g-profile radio-profile2 radio 1
```

 版权所有 © 华为技术有限公司

```
Warning: This action may cause service interruption. Continue?[Y/N]y
[Huawei-wlan-ap-group-ap-group1] quit
```

关闭AP射频0和射频1的信道和功率自动调优功能。

```
[Huawei-wlan-view] rrm-profile name wlan-net
[Huawei-wlan-rrm-prof-wlan-net] calibrate auto-channel-select disable
[Huawei-wlan-rrm-prof-wlan-net] calibrate auto-txpower-select disable
[Huawei-wlan-rrm-prof-wlan-net] quit
[Huawei-wlan-view] radio-2g-profile name radio-profile1
[Huawei-wlan-radio-2g-prof-radio-profile1] rrm-profile wlan-net
Warning: This action may cause service interruption. Continue?[Y/N]y
[Huawei-wlan-radio-2g-prof-radio-profile1] quit
[Huawei-wlan-view] radio-5g-profile name radio-profile2
[Huawei-wlan-radio-5g-prof-radio-profile2] rrm-profile wlan-net
Warning: This action may cause service interruption. Continue?[Y/N]y
[Huawei-wlan-radio-5g-prof-radio-profile2] quit
```

配置AP射频0的信道和功率。

```
[Router-wlan-view] ap-id 0
[Router-wlan-ap-0] radio 0
[Router-wlan-radio-0/0] channel 20mhz 6
Warning: This action may cause service interruption. Continue?[Y/N]y
[Router-wlan-radio-0/0] eirp 127
[Router-wlan-radio-0/0] quit
```

配置AP射频1的信道和功率。

```
[Router-wlan-ap-0] radio 1
[Router-wlan-radio-0/1] channel 80mhz 149
Warning: This action may cause service interruption. Continue?[Y/N]y
[Router-wlan-radio-0/1] eirp 127
[Router-wlan-radio-0/1] quit
[Router-wlan-ap-0] quit
```

步骤4 在AC上配置MAC认证

1. 配置RADIUS认证参数

   # 创建RADIUS服务器模板。

   ```
   [Router-wlan-view] quit
   [Router] radius-server template wlan-net
   [Router-radius-wlan-net] radius-server authentication 10.23.103.1 1812
   [Router-radius-wlan-net] radius-server shared-key cipher huawei@123
   [Router-radius-wlan-net] quit
   ```

   # 创建RADIUS方式的认证方案。

   ```
   [Router] aaa
   [Router-aaa] authentication-scheme wlan-net
   [Router-aaa-authen-wlan-net] authentication-mode radius
   [Router-aaa-authen-wlan-net] quit
   [Router-aaa] quit
   ```

   # 创建认证域“wlan-net”，并在其上绑定AAA认证方案“wlan-net”与RADIUS服务器模板“wlan-net”。

   ```
   [Router-aaa] domain wlan-net
   [Router-aaa-domain-wlan-net] authentication-scheme wlan-net
   [Router-aaa-domain-wlan-net] radius-server wlan-net
   [Router-aaa-domain-wlan-net] quit
   [Router-aaa] quit
   ```

2. 配置MAC接入模板

   说明

   MAC接入模板中，MAC认证用户的用户名和密码默认均为不带分隔符“-”的MAC地址。

 版权所有 © 华为技术有限公司

创建名为“wlan-net”的MAC接入模板。

```
[Router] mac-access-profile name wlan-net
[Router-mac-access-profile-wlan-net] quit
```

3. 创建名为“wlan-net”的认证模板，并引用MAC接入模板、认证方案和RADIUS服务器模板。

```
[Router] authentication-profile name wlan-net
[Router-authen-profile-wlan-net] mac-access-profile wlan-net
[Router-authen-profile-wlan-net] access-domain isp1 force
[Router-authentication-profile-wlan-net] quit
```

4. 在接口GE0/0/2上绑定认证模板“wlan-net”，使能MAC认证。

```
[Router] interface gigabitethernet 0/0/2
[Router-GigabitEthernet0/0/2] authentication-profile wlan-net
[Router-GigabitEthernet0/0/2] quit
```

5. 配置WLAN业务参数

   # 创建名为“wlan-net”的安全模板，并配置安全策略。缺省情况下，安全策略为open方式的开放认证。

```
[Router] wlan ac
[Router-wlan-view] security-profile name wlan-net
[Router-wlan-sec-prof-wlan-net] security open
[Router-wlan-sec-prof-wlan-net] quit
```

   # 创建名为“wlan-net”的SSID模板，并配置SSID名称为“wlan-net”。

```
[Router-wlan-view] ssid-profile name wlan-net
[Router-wlan-ssid-prof-wlan-net] ssid wlan-net
Warning: This action may cause service interruption. Continue?[Y/N]y
Info: This operation may take a few seconds, please wait.done.
[Router-wlan-ssid-prof-wlan-net] quit
```

   # 创建名为“wlan-net”的VAP模板，配置业务数据转发模式为直接转发、业务VLAN，并且引用安全模板、认证模板和SSID模板。

```
[Router-wlan-view] vap-profile name wlan-net
[Router-wlan-vap-prof-wlan-net] forward-mode direct-forward
Info: This operation may take a few seconds, please wait.done.
[Router-wlan-vap-prof-wlan-net] service-vlan vlan-id 101
Info: This operation may take a few seconds, please wait.done.
[Router-wlan-vap-prof-wlan-net] security-profile wlan-net
Info: This operation may take a few seconds, please wait..done.
[Router-wlan-vap-prof-wlan-net] authentication-profile wlan-net
[Router-wlan-vap-prof-wlan-net] ssid-profile wlan-net
Info: This operation may take a few seconds, please wait..done.
[Router-wlan-vap-prof-wlan-net] quit
```

   # 配置AP组引用VAP模板，AP上射频0和射频1都使用VAP模板“wlan-net”的配置。

```
[Router-wlan-view] ap-group name ap-group1
[Router-wlan-ap-group-ap-group1] vap-profile wlan-net wlan 1 radio 0
[Router-wlan-ap-group-ap-group1] vap-profile wlan-net wlan 1 radio 1
[Router-wlan-ap-group-ap-group1] quit
[Router-wlan-view] quit
```

步骤5 配置第三方服务器。

具体配置方法建议参考相应的产品手册。

步骤6 检查配置结果

- 哑终端关联到无线网络后，自动完成认证，认证成功后能够访问网络。

 版权所有 © 华为技术有限公司

- 哑终端接入后，在AC上执行命令**display access-user access-type mac-authen**，可以查看到认证类型为“mac-authen”的用户中，名为“huawei”的用户已成功上线。

```
[Router] display access-user access-type mac-authen
--------------------------------------------------------------------------------
UserID Username              IP address      MAC            Status
--------------------------------------------------------------------------------
460    huawei                10.23.101.254   8000-6e74-e78a Success
--------------------------------------------------------------------------------
Total: 1, printed: 1
```

----结束

配置文件

Router的配置文件

```
#
 sysname Router
#
dhcp enable
#
vlan batch 100 101
#
interface Vlanif101
 ip address 10.23.102.2 255.255.255.0
 dhcp select interface
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 101
#
interface Vlanif100
 ip address 10.23.104.2 255.255.255.0
 dhcp select interface
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 100
 authentication-profile wlan-net
#
ip route-static 10.23.103.0 24 10.23.102.1
ip route-static 10.23.101.0 24 10.23.104.1
#
authentication-profile name wlan-net
 mac-access-profile wlan-net
 access-domain wlan-net force
#
radius-server template wlan-net
 radius-server shared-key cipher %^%#*7d1;XNof/|Q0:DsP!,W51DIYPx}`AARBdJ'0B^$%^%#
 radius-server authentication 10.23.103.1 1812 weight 80
#
aaa
 authentication-scheme wlan-net
  authentication-mode radius
 domain wlan-net
  authentication-scheme wlan-net
  radius-server wlan-net
#
capwap source interface vlanif100
#
wlan ac
 security-profile name wlan-net
 ssid-profile name wlan-net
  ssid wlan-net
 vap-profile name wlan-net
  service-vlan vlan-id 101
  ssid-profile wlan-net
```

 版权所有 © 华为技术有限公司

```
 security-profile wlan-net
 authentication-profile wlan-net
regulatory-domain-profile name default
rrm-profile name wlan-net
  calibrate auto-channel-select disable
  calibrate auto-txpower-select disable
 radio-2g-profile name radio-profile1
  rrm-profile wlan-net
 radio-5g-profile name radio-profile2
  rrm-profile wlan-net
ap-group name ap-group1
 radio 0
  vap-profile wlan-net wlan 1
  radio-2g-profile radio-profile1
 radio 1
  vap-profile wlan-net wlan 1
  radio-5g-profile radio-profile2
ap-id 0 type-id 35 ap-mac 60de-4476-e360 ap-sn 210235554710CB000042
 ap-name area_1
 ap-group ap-group1
 radio 0
  channel 20mhz 6
  eirp 127
 radio 1
  channel 80mhz 149
  eirp 127
#
mac-access-profile name wlan-net
#
return
```

配置注意事项

- 纯组播报文由于协议要求在无线空口没有ACK机制保障，且无线空口链路不稳定，为了纯组播报文能够稳定发送，通常会以低速报文形式发送。如果网络侧有大量异常组播流量涌入，则会造成无线空口拥堵。为了减小大量低速组播报文对无线网络造成的冲击，建议配置组播报文抑制功能。配置前请确认是否有组播业务，如果有，请谨慎配置限速值。
  - 业务数据转发方式采用直接转发时，建议在直连AP的交换机接口上配置组播报文抑制。
  - 业务数据转发方式采用隧道转发时，建议在AC的流量模板下配置组播报文抑制。
- 建议在与AP直连的设备接口上配置端口隔离，如果不配置端口隔离，尤其是业务数据转发方式采用直接转发时，可能会在VLAN内形成大量不必要的广播报文，导致网络阻塞，影响用户体验。
- 隧道转发模式下，管理VLAN和业务VLAN不能配置为同一VLAN，且AP和AC之间只能放通管理VLAN，不能放通业务VLAN。

 版权所有 © 华为技术有限公司

14 部署语音

14.1 配置AR作为分支网关接入UC示例
14.2 配置不同企业间共享PBX示例
14.3 配置现网PBX扩容示例
14.4 配置分布式组网示例
14.5 配置中小企业语音业务示例

14.1 配置 AR 作为分支网关接入 UC 示例

组网需求

- 中心节点与AR本地节点连接正常时：
  - 总部和分支机构的所有用户均注册到中心节点统一网关。
  - 企业内呼叫全部由中心节点统一网关处理。
- 中心节点和AR本地节点断连或中心节点设备故障时：本地节点的本地用户能实现本地再生。即本地用户注册到本地节点AR上，实现本地用户的局内通话、出入局呼叫。

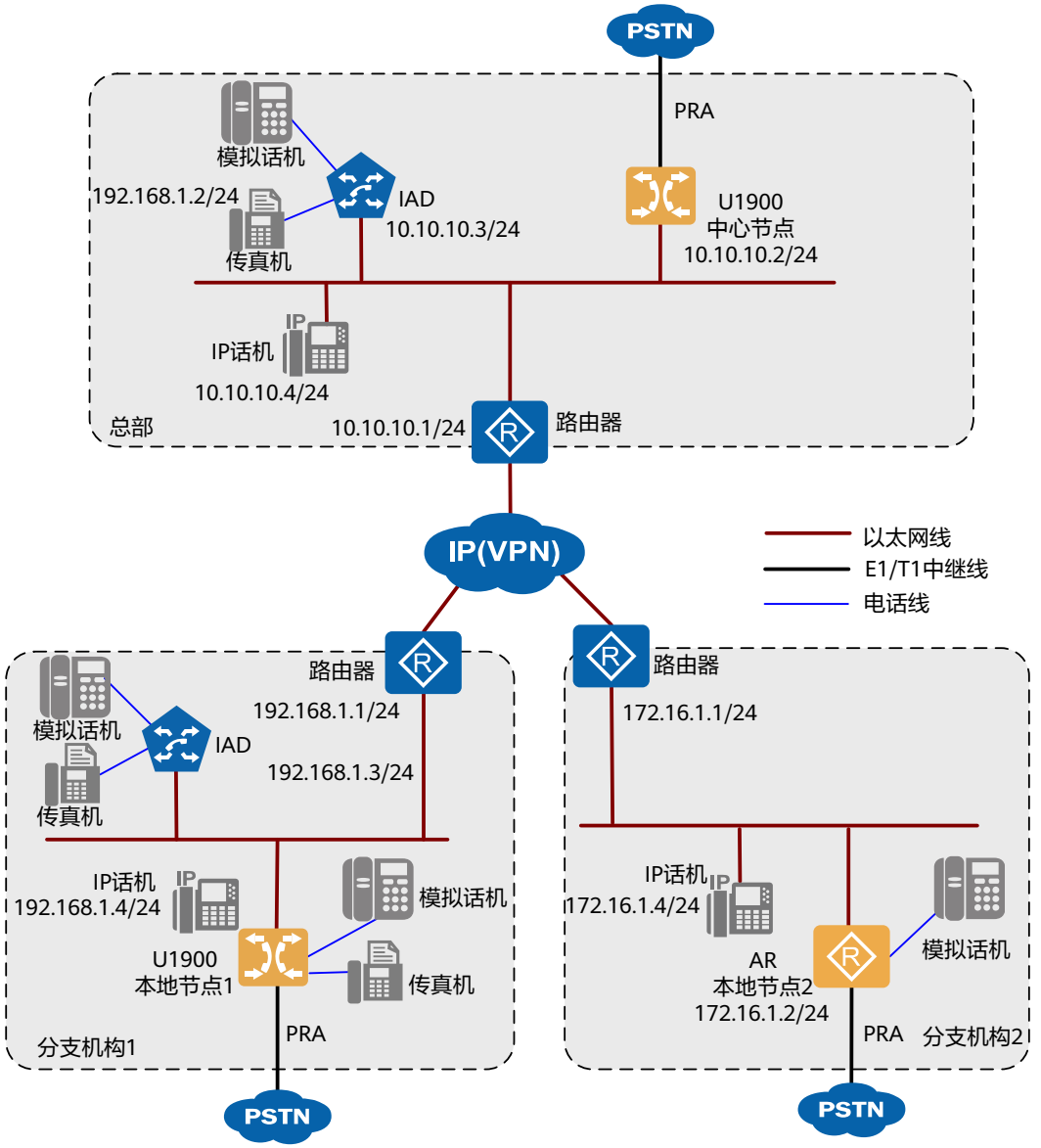
典型场景组网**图14-1**所示。

通过统一网关与AR间的对接配置后，实现的配置目标为：

- 总部、分支机构1和分支机构2之间的IP话机、POTS话机和传真机，通过拨打短号实现局内互通。
- 完成中心节点与本地节点的SIP中继对接以及与PSTN的对接，实现出局/入局呼叫。

版权所有 © 华为技术有限公司

图 14-1 现网方案



数据规划

本例中数据规划为举例说明，实际配置需要与用户和运营商协商确定。

表 14-1 用户号码

终端接入设备	短号	长号
IP话机	86000	28886000
模拟话机	88001	-
自动总机接入码	-	28888999

版权所有 © 华为技术有限公司

表 14-2 SIP 中继群

所属位置	网元	对局	中继类型	中继群名称	媒体和信令IP地址	本局端口号	对局端口号
分支机构2	本地节点2	中心节点	SIP IP	sipip	172.16.1.2	5063	5060
			SIP AT0	sipat0	172.16.1.2	5061	

表 14-3 PRA 中继群

所属位置	网元	对局	中继类型	槽位号/子卡号/端口号	路由
分支结构2	本地节点2	PSTN	PRA DSS1	1/0/0	0

表 14-4 字冠和号码变换

所属位置	网元	字冠类型	字冠	局向选择码	被叫号码变换	主叫号码变换	备注
分支机构2	本地节点2	局内字冠	8	-	-	-	用户局内字冠
		局内字冠	2888	-	-	-	用户局内字冠
		国内长途字冠	90	路由：1	删除号码第1位	将号码修改为分支机构2的自动总机接入码28888999	出局到本地PSTN
		国际长途字冠	900				
		出局字冠	9				
		出局字冠	9021				

表 14-5 单板

所属位置	网元	单板类型	槽位号
分支机构2	本地节点2	2E1/T1–F	1
		4FXS1FXO	2

版权所有 © 华为技术有限公司

操作步骤

步骤1 配置业务模式为PBX。

```
<Huawei> system-view
[Huawei] voice
[huawei-voice] service-mode pbx
[huawei-voice] return
[Huawei] save
The current configuration will be written to the device.
  Are you sure to continue? (y/n)[n]:yIt will take several minutes to save configuration file, please wait.....
  Configuration file had been saved successfully
  Note: The configuration file will take effect after being activated
<Huawei> reboot
Info: The system is comparing the configuration, please wait.
System will reboot! Continue ? [y/n]:yInfo: system is rebooting, please wait...
```

步骤2 配置接口0/0/0的以太网IP地址为172.16.1.2，并把172.16.1.2加入到该接口的媒体IP地址池和信令IP地址池。

```
<Huawei> system-view
[Huawei] interface gigabitethernet 0/0/0
[Huawei-GigabitEthernet0/0/0] ip address 172.16.1.2 24
[Huawei-GigabitEthernet0/0/0] quit
[Huawei] voice
[Huawei-voice] voip-address media interface gigabitethernet 0/0/0 172.16.1.2
[Huawei-voice] voip-address signalling interface gigabitethernet 0/0/0 172.16.1.2
```

步骤3 配置SIP服务器。

```
[Huawei-voice] sipserver
[Huawei-voice-sipserver] signalling-address ip 172.16.1.2 port 5060
[Huawei-voice-sipserver] media-ip 172.16.1.2
[Huawei-voice-sipserver] register-uri abcd.com
[Huawei-voice-sipserver] home-domain abcd.com
[Huawei-voice-sipserver] reset
[Huawei-voice-sipserver] quit
```

步骤4 配置默认国家码为86，默认地区码为021，并开启国家码地区码变换。

```
[Huawei-voice] pbx default-country-code 86 default-area-code 021
[Huawei-voice] pbx enable-country-area-transform enable
```

步骤5 配置字冠。

1. 配置呼叫属性为0的局内字冠8。

   局内字冠2888的配置方法参考此配置，将最小号长修改为8位即可。

   ```
   [Huawei-voice] callprefix 8
   [Huawei-voice-callprefix-8] prefix 8
   [Huawei-voice-callprefix-8] call-type category basic-service attribute 0
   [Huawei-voice-callprefix-8] digit-length 5 32
   [Huawei-voice-callprefix-8] quit
   ```

2. 配置呼叫属性为1的出局字冠9，路由为1。

   参考此配置方法，配置呼叫属性为1的出局字冠9021、呼叫属性为2的国内长途字冠90、呼叫属性为3的国际长途字冠900。

   ```
   [Huawei-voice] callprefix 9
   [Huawei-voice-callprefix-9] prefix 9
   [Huawei-voice-callprefix-9] call-type category basic-service attribute 1
   [Huawei-voice-callprefix-9] digit-length 1 32
   [Huawei-voice-callprefix-9] quit
   [Huawei-voice] callroute 1
   [Huawei-voice-callroute-1] quit
   [Huawei-voice] callprefix 9
   [Huawei-voice-callprefix-9] callroute 1
   [Huawei-voice-callprefix-9] quit
   ```

 版权所有 © 华为技术有限公司

3. 配置自动总机。自动总机名字为ivr，总机号码为28888999。

说明

在配置自动总机前，请参考《AR接入路由器产品文档》完成IVR配置。自动总机配置的“vu-service-name”为IVR配置的“业务名称”。

```
[Huawei-voice] callprefix ivr
[Huawei-voice-callprefix-ivr] prefix 28888999
[Huawei-voice-callprefix-ivr] call-type category vu-service vu-service-name vudefault
[Huawei-voice-callprefix-ivr] digit-length 8 32
[Huawei-voice-callprefix-ivr] save
[Huawei-voice-callprefix-ivr] quit
```

步骤6 配置用户号码。

1. 配置用户号码为86000的SIP用户。

   分支机构的SIP用户已经在中心节点配置，并通过“数据同步”将SIP用户号码同步到本地节点，所以不用在本地节点上SIP放号。

2. 配置用户号码为88001的POTS用户，用户的呼入呼出权限为all。

```
[Huawei-voice] pbxuser 88001 pots
[Huawei-voice-pbxuser-88001] port 2/0/1
[Huawei-voice-pbxuser-88001] telno 88001
[Huawei-voice-pbxuser-88001] proxyreg-id 88001
[Huawei-voice-pbxuser-88001] proxyreg-password cipher
Please input user password(8-64 chars):*********
//该密码与U1900中心节点添加本地节点AR的POTS用户的鉴权密码保持一致。
[Huawei-voice-pbxuser-88001] call-right in all
[Huawei-voice-pbxuser-88001] call-right out all
[Huawei-voice-pbxuser-88001] quit
//POTS用户通过AR本地节点代理注册到中心节点时，需要在AR上配置代理注册的头域信息，以便中心节点统一网关识别该POTS用户为通过AR代理注册的用户。
[Huawei-voice] sip
[Huawei-voice-sip] field-header user-agent HUAWEI-eSpace-UCExpress
```

步骤7 配置中继群。

1. 配置PRA中继群。

```
<Huawei> system-view
[Huawei] set workmode slot 1 e1t1 e1-voice
Changing the working mode will reset the board in slot 1. Continue? [y/n]:y
INFO: Resetting board[1] succeeded.
[Huawei] voice
[Huawei-voice] port ve1 1/0/0
[Huawei-voice-ve1-1/0/0] signal ccs
  Set signal type successfully
[Huawei-voice-ve1-1/0/0] quit
[Huawei-voice] quit
[Huawei] clock source 0 1/0/0
[Huawei] voice
[Huawei-voice] callroute 1
[Huawei-voice-callroute-1] quit
[Huawei-voice] trunk-group pra dss1-user
[Huawei-voice-trunkgroup-pra] trunk-pra 1/0/0
[Huawei-voice-trunkgroup-pra] callroute 1
[Huawei-voice-trunkgroup-pra] quit
```

2. 配置SIP AT0中继群。

```
[Huawei-voice] trunk-group sipat0 sip trunk-circuit
[Huawei-voice-trunkgroup-sipat0] signalling-address ip 172.16.1.2 port 5061
[Huawei-voice-trunkgroup-sipat0] media-ip 172.16.1.2
[Huawei-voice-trunkgroup-sipat0] peer-address static 10.10.10.2 5060
[Huawei-voice-trunkgroup-sipat0] register-uri abcd.com
[Huawei-voice-trunkgroup-sipat0] home-domain abcd.com
[Huawei-voice-trunkgroup-sipat0] trunk-sipat0 28888001 default-called-telno 88001
[Huawei-voice-trunkgroup-sipat0] reset
 Note: Trunkgroup reset succeeds.
[Huawei-voice-trunkgroup-sipat0] quit
```

 版权所有 © 华为技术有限公司

3. 配置SIP IP中继群。

```
[Huawei-voice] callroute 2
[Huawei-voice-callroute-2] quit
[Huawei-voice] trunk-group sipip sip no-register
[Huawei-voice-trunkgroup-sipip] callroute 2
[Huawei-voice-trunkgroup-sipip] signalling-address ip 172.16.1.2 port 5063
[Huawei-voice-trunkgroup-sipip] media-ip 172.16.1.2
[Huawei-voice-trunkgroup-sipip] peer-address static 10.10.10.2 5060
[Huawei-voice-trunkgroup-sipip] home-domain abcd.com
[Huawei-voice-trunkgroup-sipip] register-uri abcd.com
[Huawei-voice-trunkgroup-sipip] reset
 Note: Trunkgroup reset succeeds.
[Huawei-voice-trunkgroup-sipip] quit
```

步骤8 配置路由后号码变换。

```
[Huawei-voice] afterroute-change 9
[Huawei-voice-afterroute-change-9] callprefix 9
[Huawei-voice-afterroute-change-9] trunk-group pra
[Huawei-voice-afterroute-change-9] caller del-then-insert 1 32 28888999
[Huawei-voice-afterroute-change-9] called del 1 1
[Huawei-voice-afterroute-change-9] quit
```

步骤9 配置本地再生。

```
[Huawei-voice] local-survival
[Huawei-voice-local-survival] dataserver ip 10.10.10.2 port 8099
[Huawei-voice-local-survival] dataservertype u1900
[Huawei-voice-local-survival] primary-trunk-group sipip proxyreg-trunk-group sipat0
[Huawei-voice-local-survival] local-address ip 172.16.1.2 port 8000
[Huawei-voice-local-survival] password cipher
 Please input user password(16-32 chars):*********
//假设本地再生BIN通道鉴权密码为YsHsjx_202206，该密码与U1900中心节点添加本地节点AR的鉴权密码保持一致。
[Huawei-voice-local-survival] sync-interval 2
[Huawei-voice-local-survival] transfer tls
[Huawei-voice-local-survival] reset
[Huawei-voice-local-survival] save
```

步骤10 导入证书和私钥文件。

说明

若步骤9中的传输模式配置为TCP，请略过本配置步骤。但TCP传输模式为非加密传输，存在安全隐患，建议将传输模式配置为TLS加密传输。

1. 在U1900系列统一网关主机软件包（若没有，请登录https://support.huawei.com/enterprise/后获取）中获取证书“servercert.pem”和私钥文件“serverkey.pem”。

   证书和私钥是TLS传输双方认证的凭据。U1900系列统一网关出厂时已预置配套的证书和私钥。

   建议开局后，更换为客户自行生成或向官方机构申请的证书和私钥。在AR上更换为用户的证书和私钥文件后，请在U1900系列统一网关上导入与之配套的证书和私钥文件。

2. 将证书和私钥文件上传到AR设备上。

3. 配置策略。

```
[Huawei] pki realm u1900
[Huawei-pki-realm-u1900] quit
[Huawei] ssl policy u1900 type server
[Huawei-ssl-policy-u1900] pki-realm u1900
[Huawei-ssl-policy-u1900] quit
```

4. 导入文件。

```
[Huawei] pki import-certificate local u1900 pem
Please enter the name of certificate file <length 1-127>: servercert.pem
```

 版权所有 © 华为技术有限公司

```
You are importing a local certificate, the current private keyis required.
Please enter the name of private key file <length 1-127>: serverkey.pem
Please enter the type of private key file(pem , p12): pem
The current password is required, please enter your password <length 1-31 >:********
Successfully imported the certificate.
```

说明

U1900系列统一网关自带的私钥文件的解密密码，请从eSpace U1900系列的《产品文档》中的“配置 > 配置指南 > 高级配置 > 配置信令加密”章节中获取。

5. 进入local-survival视图，绑定策略。

```
[Huawei-voice] local-survival
[Huawei-voice-local-survival] transfer tls
[Huawei-voice-local-survival] ssl-server-policy u1900
[Huawei-voice-local-survival] reset
[Huawei-voice-local-survival] save
```

步骤11 验证配置结果

步骤	操作	预期结果
1	局内SIP用户、模拟用户短号互拨验证： 1. 分支机构2的IP话机86000摘机，拨打总部IP话机81000 2. 分支机构2的IP话机86000摘机，拨打分支机构2的模拟话机88001	1. 81000 IP话机振铃，摘机接听后开始通话。 2. 88001 模拟话机振铃，摘机接听后开始通话。
2	出局呼叫验证： 1. 分支机构2的IP话机86000摘机，拨打9XXXXXXXX呼叫分支机构2的PSTN用户B 2. 分支机构2的IP话机86000摘机，拨打9010XXXXXXXX呼叫总部PSTN用户A	1. PSTN用户B振铃，摘机接听后开始通话。 2. PSTN用户A振铃，摘机接听后开始通话。
3	入局呼叫验证： 1. 分支机构2的PSTN用户B，拨打28886000长号，呼叫分支机构1的IP话机 2. 分支机构2的PSTN用户B，拨打企业总机28888999，再拨打分机号88001	1. 28886000 IP话机振铃，摘机接听后开始通话。 2. 88001模拟话机振铃，摘机接听后开始通话。

 版权所有 © 华为技术有限公司

步骤	操作	预期结果
4	将中心节点统一网关的网络断开，模拟本地再生场景验证： 1. 分支机构2的IP话机86000摘机，拨打分支机构1的模拟话机88001 2. 分支机构2的IP话机86000摘机，拨打9XXXXXXXX呼叫分支机构2的PSTN用户B 3. 分支机构2的PSTN用户B，拨打28886000长号，呼叫分支机构2的IP话机 4. 分支机构2的PSTN用户B，拨打企业总机28888999，再拨打分机号88001	对应用户的话机振铃，摘机接听后开始通话。 1. 88001模拟话机振铃，摘机接听后开始通话。 2. PSTN用户B振铃，摘机接听后开始通话。 3. 28886000 IP话机振铃，摘机接听后开始通话。 4. 88001模拟话机振铃，摘机接听后开始通话。

----结束

配置文件

- Router的配置文件

```
#
 clock source 0 1/0/0 priority 9
#
 set workmode slot 1 e1t1 e1-voice
#
pki realm u1900
#
ssl policy u1900 type server
 pki-realm u1900
#
interface GigabitEthernet0/0/0
 ip address 172.16.1.2 255.255.255.0
#
voice
 voip-address media interface GigabitEthernet 0/0/0 172.16.1.2
 voip-address signalling interface GigabitEthernet 0/0/0 172.16.1.2
 pbx default-area-code 021
 pbx enable-country-area-transform enable
 #
 port ve1 1/0/0
  signal CCS
 #
 sip
  field-header user-agent HUAWEI-eSpace-UCExpress
 #
 callroute 1
 #
 callroute 2
 #
 sipserver
  signalling-address ip 172.16.1.2 port 5060
  media-ip 172.16.1.2
  register-uri abcd.com
  home-domain abcd.com
 #
 trunk-group pra dss1-user
  trunk-pra 1/0/0
  callroute 1
```

 版权所有 © 华为技术有限公司

```
#
trunk-group sipat0 sip trunk-circuit
 signalling-address ip 172.16.1.2 port 5061
 media-ip 172.16.1.2
 peer-address static 10.10.10.2 5060
 register-uri abcd.com
 home-domain abcd.com
 trunk-sipat0 28888001 default-called-telno 88001
#
trunk-group sipip sip no-register
 callroute 2
 signalling-address ip 172.16.1.2 port 5063
 media-ip 172.16.1.2
 peer-address static 10.10.10.2 5060
 register-uri abcd.com
 home-domain abcd.com
#
callprefix 8
 prefix 8
 call-type category basic-service attribute 0
 digit-length 5 32
#
callprefix 9
 prefix 9
 call-type category basic-service attribute 1
 digit-length 1 32
 callroute 1
#
callprefix ivr
 prefix 28888999
 call-type category vu-service vu-service-name vudefault
 digit-length 8 32
#
local-survival
 dataserver ip 10.10.10.2
 dataservertype u1900
 local-address ip 172.16.1.2
 sync-interval 2
 password cipher %^%#nw@y%OP0$#],HR"wQH/3`|.@A7+ZttF2*1D!)C~.or3f~>0ZB#EX,3dEoR%^%#
 ssl-server-policy u1900
 primary-trunk-group sipip proxyreg-trunk-group sipat0
#
pbxuser 88001 pots
 telno 88001
 port 2/0/1
 call-right out all
#
afterroute-change 9
 callprefix 9
 trunk-group pra
 caller del-then-Insert 1 32 28888999
 called del 1 1
#
```

14.2 配置不同企业间共享 PBX 示例

组网需求

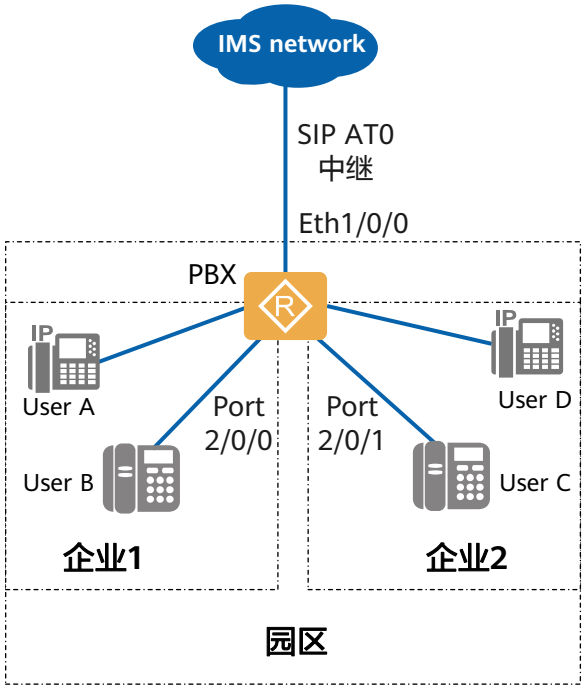
User A、User B属于企业1，User C、User D属于企业2。企业1和企业2都在同一个工业园区，通过在设备上配置不同的企业来实现企业1和企业2在逻辑上语音业务的隔离，从而实现了共用PBX。企业1和企业2既可以通过虚拟PBX实现企业内用户之间的语音业务，又可以通过统一出口实现与外部用户的语音业务。这样既节约企业成本又减少了运营商的接入点。PBX共享组网如**图14-2**所示。

本节以实现以下功能来举例：

 版权所有 © 华为技术有限公司

- 运营商为企业1分配的外部号码为56623000，外部用户拨打56623000时，User B振铃，外部用户呼叫局内非User B用户时可以通过User B转接。
- 运营商为企业2分配的外部号码为56623001，外部用户拨打56623001时，User C振铃，外部用户呼叫局内非User C用户时可以通过User C转接。
- 国家码为86，地区码为571。
- 用户A的局内号码为7100，用户B的局内号码为7000。用户C的局内号码为6000，用户D的局内号码为6100。
- 信令IP地址和媒体IP地址是192.168.1.2。
- 用户A、用户B所属的企业为hw、号首集为local、本局呼叫字冠为7，出局呼叫字冠为8。用户C、用户D所属的企业为hw1、号首集为local1、本局呼叫字冠为6，出局呼叫字冠为9。
- 中继使用SIP AT0中继出局，IMS的IP地址为192.168.10.10，端口为5060。
- 企业1从SIP AT0中继出局时，配置路由后号码变换方案8，主叫号码不变换，被叫删除第一位；企业2从SIP AT0中继出局时，配置路由后号码变换方案9，主叫号码不变换，被叫删除第一位。

图 14-2 PBX 共享组网



配置思路

1. 配置Router的业务模式为PBX模式，配置公共参数。配置企业1和企业2，实现不同企业接入Router。
2. 在企业1下配置用户、呼叫字冠、中继群、呼叫路由和路由后号码变换，企业1内用户可以实现本局呼叫和出局呼叫。
3. 在企业2下配置用户、呼叫字冠、中继群、呼叫路由和路由后号码变换，企业2内用户可以实现本局呼叫和出局呼叫。

版权所有 © 华为技术有限公司

数据规划

本例中数据规划为举例说明，实际配置需要与用户和运营商协商确定。

表 14-6 用户号码规划

短号号段	长号号段	备注
7000–7004	-	企业1
7100–7104	-	
-	56623000	
6000–6004	-	企业2
6100–6104	-	
-	56623001	

表 14-7 SIP AT0 中继规划

信令IP地址	端口号	媒体IP地址	对局IP地址	对局端口号	路由	备注	注册ID	注册密码
192.168.1.2	5061	192.168.1.2	192.168.1.10	5060	0	企业1	56623000	YsHsjx_202206
192.168.1.2	5062	192.168.1.2	192.168.1.10	5060	0	企业2	56623001	YsHsjx_202206

表 14-8 字冠规划

字冠	类型	路由	备注
7	局内	-	企业1
8	出局	0	
6	局内	-	企业2
9	出局	0	

表 14-9 路由后号码变换规划

字冠	中继出局	被叫号码变换	备注
8	SIP AT0	删除第一位	企业1

 版权所有 © 华为技术有限公司

字冠	中继出局	被叫号码变换	备注
9	SIP AT0	删除第一位	企业2

操作步骤

步骤1 配置业务模式为PBX

```
<Huawei> system-view
[Huawei] voice
[huawei-voice] service-mode pbx
[huawei-voice] quit
[Huawei] save
The current configuration will be written to the device.
  Are you sure to continue? (y/n)[n]:y It will take several minutes to save configuration file, please wait.....
  Configuration file had been saved successfully
  Note: The configuration file will take effect after being activated
<Huawei>reboot
Info: The system is comparing the configuration, please wait.
System will reboot! Continue ? [y/n]:y Info: system is rebooting, please wait...
```

步骤2 配置接口0/0/0的以太网IP地址为192.168.1.2，并把192.168.1.2加入到该接口的媒体IP地址池和信令IP地址池。

```
<Huawei> system-view
[Huawei] interface gigabitethernet 0/0/0
[Huawei-GigabitEthernet0/0/0] ip address 192.168.1.2 24
[Huawei-GigabitEthernet0/0/0] quit
[Huawei] voice
[Huawei-voice] voip-address media interface gigabitethernet 0/0/0 192.168.1.2
[Huawei-voice] voip-address signalling interface gigabitethernet 0/0/0 192.168.1.2
[Huawei-voice] quit
```

步骤3 配置默认国家码为86，默认地区码为571，并开启国家码地区码变换。

```
[Huawei] voice
[Huawei-voice] pbx default-country-code 86 default-area-code 571
[Huawei-voice] pbx enable-country-area-transform enable
```

步骤4 配置SIP服务器。

```
[Huawei-voice] sipserver
[Huawei-voice-sipserver] signalling-address ip 192.168.1.2 port 5060
[Huawei-voice-sipserver] media-ip 192.168.1.2
[Huawei-voice-sipserver] register-uri abcd.com
[Huawei-voice-sipserver] home-domain abcd.com
[Huawei-voice-sipserver] reset
[Huawei-voice-sipserver] quit
```

步骤5 配置号码归属的企业、号首集。

```
[Huawei-voice] enterprise hw
[Huawei-voice-enterprise-hw] dn-set local
[Huawei-voice-enterprise-hw] quit
[Huawei-voice] enterprise hw1
[Huawei-voice-enterprise-hw1] dn-set local1
[Huawei-voice-enterprise-hw1] quit
```

步骤6 用户A、用户B所属的企业为hw、号首集为local、本局呼叫字冠为7，出局呼叫字冠为8。

说明

用户C、用户D所属的企业为hw1、号首集为local1、本局呼叫字冠为6，出局呼叫字冠为9。

```
[Huawei-voice] callprefix 7
[Huawei-voice-callprefix-7] enterprise hw dn-set local
```

 版权所有 © 华为技术有限公司

```
[Huawei-voice-callprefix-7] prefix 7
[Huawei-voice-callprefix-7] call-type category basic-service attribute 0
[Huawei-voice-callprefix-7] digit-length 4 32
[Huawei-voice-callprefix-7] quit
[Huawei-voice] callprefix 8
[Huawei-voice-callprefix-8] enterprise hw dn-set local
[Huawei-voice-callprefix-8] prefix 8
[Huawei-voice-callprefix-8] call-type category basic-service attribute 1
[Huawei-voice-callprefix-8] digit-length 1 32
[Huawei-voice-callprefix-8] quit
[Huawei-voice] callroute 8
[Huawei-voice-callroute-8] quit
[Huawei-voice] callprefix 8
[Huawei-voice-callprefix-8] callroute 8
[Huawei-voice-callprefix-8] quit
```

步骤7 配置用户号码为7100的SIP用户A，鉴权密码为YsHsjx_202206。

说明

配置用户D所属的企业为hw1，用户号码为6100的用户，配置方法参见7100的配置。

```
[Huawei-voice] pbxuser 7100 sipue enterprise hw
[Huawei-voice-pbxuser-7100] dn-set local
[Huawei-voice-pbxuser-7100] sipue 7100
[Huawei-voice-pbxuser-7100] telno 7100
[huawei-voice-pbxuser-7100] eid-para password cipher
 Please input user password(6-64 chars): *******
[Huawei-voice-pbxuser-7100] quit
```

步骤8 配置用户B号码为7000。

说明

配置用户C所属的企业为hw1，用户号码为6000的用户，配置方法参见7000的配置。

```
[Huawei-voice] pbxuser 7000 pots enterprise hw
[Huawei-voice-pbxuser-7000] dn-set local
[Huawei-voice-pbxuser-7000] port 2/0/0
[Huawei-voice-pbxuser-7000] telno 7000
[Huawei-voice-pbxuser-7000] call-right in idd enable
[Huawei-voice-pbxuser-7000] call-right out idd enable
[Huawei-voice-pbxuser-7000] quit
```

步骤9 配置SIP AT0中继群。

```
[Huawei-voice] trunk-group sipat0 sip trunk-circuit
[Huawei-voice-trunkgroup-sipat0] signalling-address ip 192.168.1.2 port 5061
[Huawei-voice-trunkgroup-sipat0] enterprise hw dn-set local
[Huawei-voice-trunkgroup-sipat0] media-ip 192.168.1.2
[Huawei-voice-trunkgroup-sipat0] peer-address static 192.168.10.10 5060
[Huawei-voice-trunkgroup-sipat0] register-uri abcd.com
[Huawei-voice-trunkgroup-sipat0] home-domain abcd.com
[Huawei-voice-trunkgroup-sipat0] trunk-sipat0 56623000 default-called-telno 7000 password cipher
 Please input user password(1-32 chars):********
[Huawei-voice-trunkgroup-sipat0] number-parameter 19 0
[Huawei-voice-trunkgroup-sipat0] reset
 Note: Trunkgroup reset succeeds.
[Huawei-voice-trunkgroup-sipat0] quit
[Huawei-voice] trunk-group sipat01 sip trunk-circuit
[Huawei-voice-trunkgroup-sipat01] signalling-address ip 192.168.1.2 port 5062
[Huawei-voice-trunkgroup-sipat01] enterprise hw1 dn-set local1
[Huawei-voice-trunkgroup-sipat01] media-ip 192.168.1.2
[Huawei-voice-trunkgroup-sipat01] peer-address static 192.168.10.10 5060
[Huawei-voice-trunkgroup-sipat01] register-uri abcd.com
[Huawei-voice-trunkgroup-sipat01] home-domain abcd.com
[Huawei-voice-trunkgroup-sipat01] trunk-sipat0 56623001 default-called-telno 6000 password cipher
 Please input user password(1-32 chars):********
[Huawei-voice-trunkgroup-sipat0] number-parameter 19 0
[Huawei-voice-trunkgroup-sipat01] reset
 Note: Trunkgroup reset succeeds.
```

 版权所有 © 华为技术有限公司

```
[Huawei-voice-trunkgroup-sipat0] quit
```

步骤10 配置呼叫路由和路由后号码变换。

企业1从SIP AT0中继出局时，配置路由后号码变换方案8，主叫号码不变换，被叫删除第一位。

说明

配置企业2从SIP AT0中继出局路由后号码变换方案9，主叫号码不变换，被叫删除第一位。

```
[Huawei-voice] callprefix 8
[Huawei-voice-callprefix-8] callroute 8
[Huawei-voice-callprefix-8] quit
[Huawei-voice] trunk-group sipat0
[Huawei-voice-trunkgroup-sipat0] callroute 8
[Huawei-voice-trunkgroup-sipat0] quit
[Huawei-voice] afterroute-change 8
[Huawei-voice-afterroute-change-8] callprefix 8
[Huawei-voice-afterroute-change-8] trunk-group sipat0
[Huawei-voice-afterroute-change-8] caller no-change
[Huawei-voice-afterroute-change-8] called del 1 1
[Huawei-voice-afterroute-change-8] save
```

步骤11 验证配置结果

验证项	正常结果	可能的异常原因
局内呼叫	比如用户7000拨打用户7100能够正常通话，7100用户显示主叫号码为7000。	局内字冠配置问题。
出局呼叫	能正常通话，并且号码显示正常。比如用户7000从SIP AT0出局呼叫，被叫用户显示主叫号码为56623000。	• 出局字冠配置问题。 • 出局中继问题。
入局呼叫	能正常通话，比如局外用户拨打PBX的自动总机56623000，通过7000转接到其他用户。	-

----结束

配置文件

- Router的配置文件

```
#
interface GigabitEthernet0/0/0
 ip address 192.168.1.2 255.255.255.0
#
voice
 voip-address media interface GigabitEthernet 0/0/0 192.168.1.2
 voip-address signalling interface GigabitEthernet 0/0/0 192.168.1.2
 pbx default-area-code 571
 pbx enable-country-area-transform enable
 #
 callroute 8
 #
```

 版权所有 © 华为技术有限公司

```
enterprise hw
 dn-set local
#
enterprise hw1
 dn-set local1
#
sipserver
 signalling-address ip 192.168.1.2 port 5060
 media-ip 192.168.1.2
 register-uri abcd.com
 home-domain abcd.com
#
trunk-group sipat0 sip trunk-circuit
 enterprise hw dn-set local
 callroute 8
 signalling-address ip 192.168.1.2 port 5061
 media-ip 192.168.1.2
 peer-address static 192.168.10.10 5060
 register-uri abcd.com
 home-domain abcd.com
 trunk-sipat0 56623000 default-called-telno 7000
 trunk-sipat0 56623000 password cipher %^%#wlyf~LstT9[[t|HjP*N3>t{Q3!f8>2e#PDM@Ga-:%^%#
#
trunk-group sipat1 sip trunk-circuit
 enterprise hw1 dn-set local1
 signalling-address ip 192.168.1.2 port 5062
 media-ip 192.168.1.2
 peer-address static 192.168.10.10 5060
 register-uri abcd.com
 home-domain abcd.com
 trunk-sipat0 56623001 default-called-telno 6000
 trunk-sipat0 56623001 password cipher %^%##;d~MTyB}'|b2:@A=Rg25*=-5s^[<12[K8-M9pm5%^%#
#
callprefix 7
 enterprise hw dn-set local
 prefix 7
 call-type category basic-service attribute 0
 digit-length 4 32
#
callprefix 8
 enterprise hw dn-set local
 prefix 8
 call-type category basic-service attribute 1
 digit-length 1 32
 callroute 8
#
pbxuser 7000 pots enterprise hw
 telno 7000
 port 2/0/0
 dn-set local
 call-right out idd enable
#
pbxuser 7100 sipue enterprise hw
 sipue 7100
 telno 7100
 dn-set local
 eid-para password cipher %^%#Y;QQB*rk9,$7=K5av']G_[YWC~knl!4X[%Dvz%Q<%^%#
#
afterroute-change 8
 callprefix 8
 trunk-group sipat0
 caller no-change
 called del 1 1
#
```

14.3 配置现网 PBX 扩容示例

 版权所有 © 华为技术有限公司

组网需求

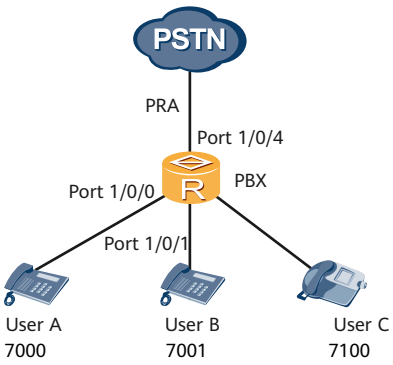
基于现网PBX扩容，并保留原先的用户长短号、自动总机和用户拨号习惯的需求，将现网PBX接入到新增的PBX来实现扩容目标。现网PBX接入PBX的典型场景组网图14-3所示。

本场景以实现以下需求为例：

- 配置国家码为86，地区码571。
- 配置企业为hw，号首集为hwdnset。
- 实现PBX和现网PBX下的短号互拨。
- PBX通过H.323中继现网PBX对接，路由为2。
- 现网PBX通过H.323与PBX对接，路由为3。
- PBX通过AT0中继与A运营商对接，通过PRA中继与B运营商对接。配置两个中继出局基于负荷分担的路由方式，都绑定路由0。
- 从PRA中继出局到PSTN，有长号的出局显示长号，没有长号的主叫变换为28980808。
- 从AT0中继出局到PSTN，有长号的出局显示长号，没有长号的主叫变换为83780808。
- A运营商或者B运营商的用户拨打PBX的自动总机。

 版权所有 © 华为技术有限公司

图 14-3 现网 PBX 扩容场景



企业用户通过PBX实现内部用户之间的语音业务，通过PRA中继实现与企业外部用户之间的语音业务。
1、PSTN给PBX放多个号码，PBX可以用一个作为自动总机，其他用作专线。
2、PBX给用户放号。
3、PBX用户局内短号互拨；出局专线的显示专线号码，没有专线的对外显示为自动总机号码。

前提条件

已经完成IVR配置，自动总机配置的“vu-service-name”为IVR配置的“业务名称”。

版权所有 © 华为技术有限公司

数据规划

本例中数据规划为举例说明，实际配置需要与用户和运营商协商确定。

表 14-10 用户号码规划

短号号段	长号号段	备注
7000–7004	28987000–28987004	新增PBX的用户
7100–7104	-	
-	28980808	新增PBX的自动总机
6000–6004	83786000–83786004	现网PBX的用户
6100–6104	-	
-	83780808	现网PBX的自动总机

表 14-11 IP 地址规划

网元	IP地址	子网掩码
新增PBX	192.168.1.2	255.255.255.0
现网PBX	192.168.1.3	255.255.255.0

表 14-12 PRA 中继规划

槽位号/子卡号/端口号	路由	对局
1/0/0	0	PSTN

表 14-13 AT0 中继规划

槽位号/子卡号/端口号	默认接入号码	路由号
3/0/4	83780808	0

表 14-14 H.323 中继规划

媒体IP地址	端口号	对局IP地址	对局端口号	路由号
192.168.1.2	1720	192.168.1.3	1720	2

 版权所有 © 华为技术有限公司

表 14-15 字冠规划

字冠	类型	路由	所属设备
6	出局	2	新增PBX
7	局内	-	
2898	局内	-	
8378	出局	2	
6	局内	-	现网PBX
7	出局	3	
9	出局	3	
8378	局内	-	

表 14-16 路由后号码变换规划

字冠	中继出局	主叫号码变换	被叫号码变换
9	PRA	28980808	删除第一位
	AT0	-	删除第一位

操作步骤

步骤1 配置业务模式为PBX。

```
<Huawei> system-view
[Huawei] voice
[huawei-voice] service-mode pbx
[huawei-voice] return
[Huawei] save
The current configuration will be written to the device.
  Are you sure to continue? (y/n)[n]:y It will take several minutes to save configuration file, please wait.....
  Configuration file had been saved successfully
  Note: The configuration file will take effect after being activated
<Huawei>reboot
Info: The system is comparing the configuration, please wait.
System will reboot! Continue ? [y/n]:yInfo: system is rebooting, please wait...
```

步骤2 配置接口0/0/0的以太网IP地址为192.168.1.2，并把192.168.1.2加入到该接口的媒体IP地址池和信令IP地址池。

```
<Huawei> system-view
[Huawei] interface gigabitethernet 0/0/0
[Huawei-GigabitEthernet0/0/0] ip address 192.168.1.2 24
[Huawei-GigabitEthernet0/0/0] quit
[Huawei] voice
[Huawei-voice] voip-address media interface gigabitethernet 0/0/0 192.168.1.2
[Huawei-voice] voip-address signalling interface gigabitethernet 0/0/0 192.168.1.2
```

步骤3 配置SIP服务器。

```
[Huawei-voice] sipserver
[Huawei-voice-sipserver] signalling-address ip 192.168.1.2 port 5060
[Huawei-voice-sipserver] media-ip 192.168.1.2
```

 版权所有 © 华为技术有限公司

```
[Huawei-voice-sipserver] register-uri abcd.com
[Huawei-voice-sipserver] home-domain abcd.com
[Huawei-voice-sipserver] reset
[Huawei-voice-sipserver] quit
```

步骤4 配置默认国家码为86，默认地区码为571，并开启国家码地区码变换。

```
[Huawei-voice] pbx default-country-code 86 default-area-code 571
[Huawei-voice] pbx enable-country-area-transform enable
```

步骤5 配置号码归属的企业、号首集。

```
[Huawei-voice] enterprise hw
[Huawei-voice-enterprise-hw] dn-set hwdnset
[Huawei-voice-enterprise-hw] save
[Huawei-voice-enterprise-hw] quit
```

步骤6 配置字冠。

1. 配置字冠的企业为hw、号首集为hwdnset、字冠为7的呼叫属性为0的本局呼叫。

   说明

   局内字冠2898的配置方法参考此配置，只要修改最小号长为8位即可。

   ```
   [Huawei-voice] callprefix 7
   [Huawei-voice-callprefix-7] enterprise hw dn-set hwdnset
   [Huawei-voice-callprefix-7] prefix 7
   [Huawei-voice-callprefix-7] call-type category basic-service attribute 0
   [Huawei-voice-callprefix-7] digit-length 4 32
   [Huawei-voice-callprefix-7] quit
   ```

2. 配置字冠6的呼叫属性为1的字冠，字冠的路由为2。

   说明

   出局字冠8378的配置方法参考此配置，只要修改最小号长为8位即可。

   ```
   [Huawei-voice] callprefix 6
   [Huawei-voice-callprefix-6] enterprise hw dn-set hwdnset
   [Huawei-voice-callprefix-6] prefix 6
   [Huawei-voice-callprefix-6] call-type category basic-service attribute 1
   [Huawei-voice-callprefix-6] digit-length 4 32
   [Huawei-voice-callprefix-6] quit
   [Huawei-voice] callroute 2
   [Huawei-voice-calldroute-2] quit
   [Huawei-voice] callprefix 6
   [Huawei-voice-callprefix-6] callroute 2
   [Huawei-voice-callprefix-6] quit
   ```

3. 配置字冠9的呼叫属性为1的字冠，字冠的路由为0。

   说明

   配置90的呼叫属性为2的国内长途字冠、900的呼叫属性为3的国际长途字冠，字冠的路由为0，配置方法参见字冠9的配置。

   ```
   [Huawei-voice] callprefix 9
   [Huawei-voice-callprefix-9] enterprise hw dn-set hwdnset
   [Huawei-voice-callprefix-9] prefix 9
   [Huawei-voice-callprefix-9] call-type category basic-service attribute 1
   [Huawei-voice-callprefix-9] digit-length 1 32
   [Huawei-voice-callprefix-9] quit
   [Huawei-voice] callroute 0
   [Huawei-voice-calldroute-0] quit
   [Huawei-voice] callprefix 9
   [Huawei-voice-callprefix-9] callroute 0
   [Huawei-voice-callprefix-9] quit
   ```

4. 配置自动总机。

   自动总机名字为ivr，总机号码为28980808。

 版权所有 © 华为技术有限公司

```
[Huawei-voice] callprefix ivr
[Huawei-voice-callprefix-ivr] prefix 28980808
[Huawei-voice-callprefix-ivr] enterprise hw dn-set hwdnset
[Huawei-voice-callprefix-ivr] call-type category vu-service vu-service-name vudefault
[Huawei-voice-callprefix-ivr] digit-length 8 32
[Huawei-voice-callprefix-ivr] save
[Huawei-voice-callprefix-ivr] quit
```

步骤7 配置用户号码。

1. 配置用户号码为7000的SIP用户，鉴权密码为YsHsjx_202206，用户的呼入呼出权限为all。

```
[Huawei-voice] pbxuser 7000 sipue enterprise hw
[Huawei-voice-pbxuser-7000] dn-set hwdnset
[Huawei-voice-pbxuser-7000] sipue 7000
[Huawei-voice-pbxuser-7000] telno 7000 long-telno 28987000
[Huawei-voice-pbxuser-7000] call-right in all
[Huawei-voice-pbxuser-7000] call-right out all
[Huawei-voice-pbxuser-7000] eid-para password cipher
 Please input user password(6-64 chars): *******
[Huawei-voice-pbxuser-7000] quit
```

2. 配置用户号码为7100的POTS用户，用户的呼入呼出权限为all。

```
[Huawei-voice] pbxuser 7100 pots enterprise hw
[Huawei-voice-pbxuser-7100] dn-set hwdnset
[Huawei-voice-pbxuser-7100] port 3/0/0
[Huawei-voice-pbxuser-7100] telno 7100
[Huawei-voice-pbxuser-7100] call-right in all
[Huawei-voice-pbxuser-7100] call-right out all
[Huawei-voice-pbxuser-7100] return
```

步骤8 配置中继群。

1. 配置PRA中继群。

```
<Huawei> system-view
[Huawei] set workmode slot 1 e1t1 e1-voice
Changing the working mode will reset the board in slot 1. Continue? [y/n]:y
INFO: Resetting board[1] succeeded.
[Huawei] voice
[Huawei-voice] port ve1 1/0/0
[Huawei-voice-ve1-1/0/0] signal ccs
  Set signal type successfully
[Huawei-voice-ve1-1/0/0] quit
[Huawei-voice] quit
[Huawei] clock source 0 1/0/0
[Huawei] voice
[Huawei-voice] callroute 0
[Huawei-voice-calldroute-0] quit
[Huawei-voice] trunk-group pra dss1-user
[Huawei-voice-trunkgroup-pra] trunk-pra 1/0/0
[Huawei-voice-trunkgroup-pra] enterprise hw dn-set hwdnset
[Huawei-voice-trunkgroup-pra] quit
```

2. 配置AT0中继群。

```
[Huawei-voice] trunk-group AT0 fxo
[Huawei-voice-trunkgroup-AT0] trunk-AT0 3/0/4 default-called-telno 83780808
[Huawei-voice-trunkgroup-AT0] enterprise hw dn-set hwdnset
[Huawei-voice-trunkgroup-AT0] quit
```

3. 配置H.323中继群。

```
[Huawei-voice] h323-attribute
[Huawei-voice-h323-attribute] localip 192.168.1.2
 Note: Mandatory parameter of h323 system completed, please reset h323 system.
[Huawei-voice-h323-attribute] reset
 H323 system parameters reset successfully!
[Huawei-voice-h323-attribute] quit
[Huawei-voice] trunk-group h323 h323 symmetrical
[Huawei-voice-trunkgroup-h323] media-ip 192.168.1.2
```

 版权所有 © 华为技术有限公司

```
[Huawei-voice-trunkgroup-h323] peer-address static 192.168.1.3 1720
 Note: Mandatory parameter of the trunkgroup completed, please reset the trunkgroup.
[Huawei-voice-trunkgroup-h323] enterprise hw dn-set hwdnset
[Huawei-voice-trunkgroup-h323] callroute 2
[Huawei-voice-trunkgroup-h323] reset
[Huawei-voice-trunkgroup-h323] save
[Huawei-voice-trunkgroup-h323] quit
```

步骤9 配置基于负荷分担的智能路由。

```
[Huawei-voice] callroute 0
[Huawei-voice-callroute-0] selecttype loadshare
[Huawei-voice-callroute-0] quit
[Huawei-voice] trunk-group pra
[Huawei-voice-trunkgroup-pra] callroute 0
[Huawei-voice-trunkgroup-pra] quit
[Huawei-voice] trunk-group AT0
[Huawei-voice-trunkgroup-AT0] callroute 0
[Huawei-voice-trunkgroup-AT0] quit
```

步骤10 配置路由后号码变换。

```
[Huawei-voice] afterroute-change 9_6xxx_pra
[Huawei-voice-afterroute-change-9_6xxx_pra] callprefix 9
[Huawei-voice-afterroute-change-9_6xxx_pra] trunk-group pra
[Huawei-voice-afterroute-change-9_6xxx_pra] condition caller-telno 6xxx
[Huawei-voice-afterroute-change-9_6xxx_pra] caller del-then-insert 1 32 28980808
[Huawei-voice-afterroute-change-9_6xxx_pra] called del 1 1
[Huawei-voice-afterroute-change-9_6xxx_pra] quit
[Huawei-voice] afterroute-change 9_71xx_pra
[Huawei-voice-afterroute-change-9_7xxx_pra] callprefix 9
[Huawei-voice-afterroute-change-9_7xxx_pra] trunk-group pra
[Huawei-voice-afterroute-change-9_7xxx_pra] condition caller-telno 71xx
[Huawei-voice-afterroute-change-9_7xxx_pra] caller del-then-insert 1 32 28980808
[Huawei-voice-afterroute-change-9_7xxx_pra] called del 1 1
[Huawei-voice-afterroute-change-9_7xxx_pra] quit
[Huawei-voice] afterroute-change 9_at0
[Huawei-voice-afterroute-change-9_at0] callprefix 9
[Huawei-voice-afterroute-change-9_at0] trunk-group AT0
[Huawei-voice-afterroute-change-9_at0] caller no-change
[Huawei-voice-afterroute-change-9_at0] called del 1 1
[Huawei-voice-afterroute-change-9_at0] quit
[Huawei-voice] afterroute-change 9_pra
[Huawei-voice-afterroute-change-9_at0] callprefix 9
[Huawei-voice-afterroute-change-9_at0] trunk-group pra
[Huawei-voice-afterroute-change-9_at0] caller no-change
[Huawei-voice-afterroute-change-9_at0] called del 1 1
[Huawei-voice-afterroute-change-9_at0] quit
```

步骤11 验证配置结果

验证项	正常结果	可能的异常原因
局内呼叫	比如用户7000拨打用户7100能够正常通话，7100用户显示主叫号码为7000。	局内字冠配置问题。

 版权所有 © 华为技术有限公司

验证项	正常结果	可能的异常原因
配置长号的用户出局呼叫	能正常通话，并且号码显示正常。 ● 比如用户7000拨打用户6000能够正常通话，6000用户显示主叫号码为7000。 ● 比如用户7000从PRA出局呼叫，被叫用户显示主叫号码为28987000。 ● 比如用户7000从AT0出局呼叫，被叫用户显示主叫号码为28987000。	● 出局字冠配置问题。 ● 出局中继问题或者配置完成后没有执行**reset**命令。
没有配置长号的用户出局呼叫	能正常通话，并且号码显示正常。 ● 比如用户7100拨打用户6000能够正常通话，6000用户显示主叫号码为7100。 ● 比如用户7100从PRA出局呼叫，被叫用户显示主叫号码为28980808。 ● 比如用户7100从AT0出局呼叫，被叫用户显示主叫号码为83780808。	-
入局呼叫	能正常通话，比如局外用户拨打PBX的自动总机28980808，主叫根据语音提示，再拨打分机号码7000转接到7000用户。	-

----结束

配置文件

- Router的配置文件

```
#
 clock source 0 1/0/0 priority 9
#
 set workmode slot 1 e1t1 e1-voice
#
interface GigabitEthernet0/0/0
 ip address 192.168.1.2 255.255.255.0
#
voice
 voip-address media interface GigabitEthernet 0/0/0 192.168.1.2
```

 版权所有 © 华为技术有限公司

```
voip-address signalling interface GigabitEthernet 0/0/0 192.168.1.2
pbx default-area-code 571
pbx enable-country-area-transform enable
#
port ve1 1/0/0
 signal CCS
#
h323-attribute
 localip 192.168.1.2
#
callroute 0
 selecttype loadshare
#
callroute 2
#
enterprise hw
 dn-set hwdnset
#
sipserver
 signalling-address ip 192.168.1.2 port 5060
 media-ip 192.168.1.2
 register-uri abcd.com
 home-domain abcd.com
#
trunk-group at0 fxo
 trunk-AT0 3/0/4 default-called-telno 83780808
 enterprise hw dn-set hwdnset
 callroute 0
#
trunk-group h323 h323 symmetrical
 enterprise hw dn-set hwdnset
 callroute 2
 media-ip 192.168.1.2
 peer-address static 192.168.1.3 1720
#
trunk-group pra dss1-user
 trunk-pra 1/0/0
 enterprise hw dn-set hwdnset
 callroute 0
#
callprefix 6
 enterprise hw dn-set hwdnset
 prefix 6
 call-type category basic-service attribute 1
 digit-length 4 32
 callroute 2
#
callprefix 7
 enterprise hw dn-set hwdnset
 prefix 7
 call-type category basic-service attribute 0
 digit-length 4 32
#
callprefix 9
 enterprise hw dn-set hwdnset
 prefix 9
 call-type category basic-service attribute 1
 digit-length 1 32
 callroute 0
#
callprefix ivr
 enterprise hw dn-set hwdnset
 prefix 28980808
 call-type category vu-service vu-service-name vudefault
 digit-length 8 32
#
pbxuser 7000 sipue enterprise hw
 sipue 7000
 telno 7000 long-telno 28987000
```

 版权所有 © 华为技术有限公司

```
 dn-set hwdnset
 call-right out all
 eid-para password cipher %^%#"(sq-~Wu6YD^RCIcKx:'6]z--N|iKU6DyrM4m&*X%^%#
#
pbxuser 7100 pots enterprise hw
 telno 7100
 port 3/0/0
 dn-set hwdnset
 call-right out all
#
afterroute-change 9_6xxx_pra
 callprefix 9
 trunk-group pra
 condition caller-telno 6xxx
 caller del-then-Insert 1 32 28980808
 called del 1 1
#
afterroute-change 9_71xx_pra
 callprefix 9
 trunk-group pra
 condition caller-telno 71xx
 caller del-then-Insert 1 32 28980808
 called del 1 1
#
afterroute-change 9_at0
 callprefix 9
 trunk-group AT0
 caller no-change
 called del 1 1
#
afterroute-change 9_pra
 callprefix 9
 trunk-group pra
 caller no-change
 called del 1 1
#
```

14.4 配置分布式组网示例

组网需求

企业为了节省长途电话成本，在多个城市分部间通过SIP中继对接，各分部本地经SIP AT0接入IMS或者PRA中继接入PSTN网络。

当A市用户拨打B市的PSTN市话时，呼叫经SIP IP中继由PBX拨打到IP PBX，再经IP PBX的PRA中继出局到PSTN网络，最终打通B市企业外用户。B市用户拨打A市的市话，呼叫流程和A市拨打B市的市话类似，先将呼叫汇接到PBX再出局。

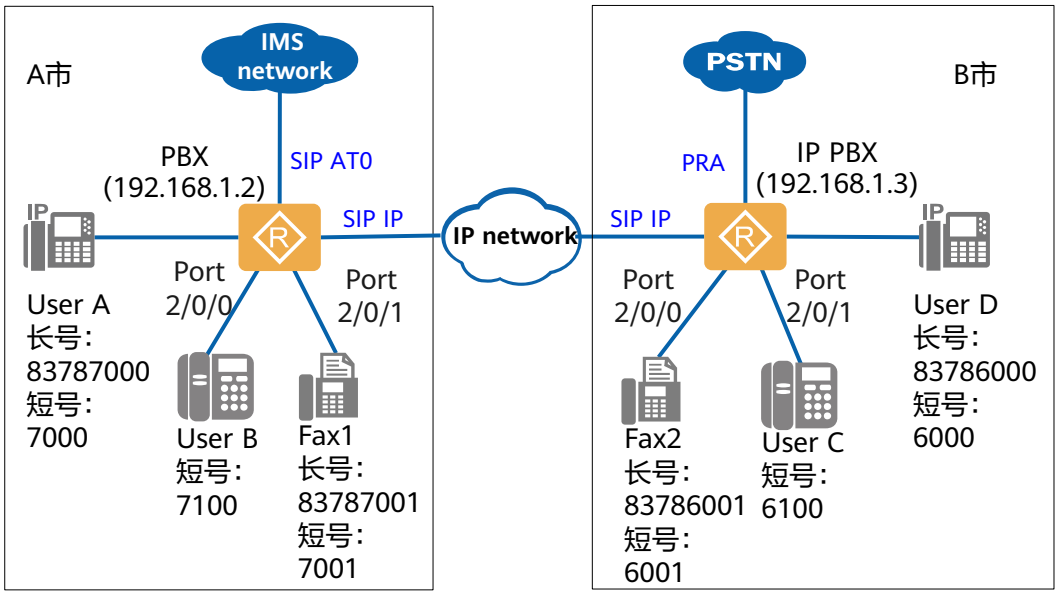
这种场景即可以节约长途成本的经济，分布式组网如图1所示。

本节以实现以下功能为例：

- 国家码为86，A市的地区码为571，B市的地区码577。
- IMS网络的IP地址为192.168.1.4，服务端口为5060。
- PBX的自动总机为83787005，IP PBX的自动总机为83786005。
- PBX下用户和IP PBX下用户以短号互拨。
- PBX下的用户或者IP PBX下的用户拨打B市的市话，从IP PBX出局，有长号的出局显示长号，没有长号的主叫变换为83786005。
- IP PBX下的用户或者PBX下的用户拨打A市的市话，从PBX出局，有长号的出局显示长号，没有长号的主叫变换为83787005。

 版权所有 © 华为技术有限公司

图 14-4 分布式组网



前提条件

已经完成IVR配置，自动总机配置的“vu-service-name”为IVR配置的“业务名称”。

数据规划

本例中数据规划为举例说明，实际配置需要与用户和运营商协商确定。

表 14-17 号码规划

短号号段	长号号段	所属设备
7000–7004	83787000–83787004	PBX
7100–7104	-	
-	83786005	PBX的自动总机
6000–6004	83786000–83786004	IP PBX
6100–6104	-	
-	83787005	IP PBX的自动总机

表 14-18 IP 地址规划

网元	IP地址	子网掩码
PBX	192.168.1.2	255.255.255.0
IP PBX	192.168.1.3	255.255.255.0

版权所有 © 华为技术有限公司

表 14-19 PRA 中继规划

槽位号/子卡号/端口号	路由	对局
3/0/0	0	PSTN

表 14-20 SIP IP 中继规划

信令IP地址	端口号	媒体IP地址	对局IP地址	对局端口号	路由
192.168.1.2	5062	192.168.1.2	192.168.1.3	5062	1

表 14-21 SIP AT0 中继规划

信令IP地址	端口号	媒体IP地址	对局IP地址	对局端口号	路由	注册ID	注册密码
192.168.1.2	5061	192.168.1.2	192.168.1.4	5060	3	+8620837870005@abcd.com	YsHsjx_202206

表 14-22 字冠规划

字冠	类型	路由	主叫号码变换	被叫号码变换	所属设备
7	局内	-	-	-	PBX
83787	局内	-	-	-	
9	出局	3	变换为83786005	删除第一位	
6	出局	1	-	-	
90577	出局	1	-	-	
6	局内	-	-	-	IP PBX
83786	局内	-	-	-	
9	出局	0	变换为83787005	删除第一位	
7	出局	2	-	-	
90571	出局	2	-	-	

版权所有 © 华为技术有限公司

表 14-23 路由后号码变换规划

字冠	中继出局	主叫号码变换	被叫号码变换
9	PRA	83786005	删除第一位
	SIP AT0	83787005	删除第一位

操作步骤

步骤1 配置业务模式为PBX。

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] service-mode pbx
[Huawei-voice] return
[Huawei] save
The current configuration will be written to the device.
  Are you sure to continue? (y/n)[n]:y It will take several minutes to save configuration file, please wait.....
  Configuration file had been saved successfully
  Note: The configuration file will take effect after being activated
<Huawei> reboot
Info: The system is comparing the configuration, please wait.
System will reboot! Continue ? [y/n]:y Info: system is rebooting, please wait...
```

步骤2 配置接口GE0/0/0的以太网IP地址为192.168.1.2，并把192.168.1.2加入到该接口的媒体IP地址池和信令IP地址池。

```
<Huawei> system-view
[Huawei] interface gigabitethernet 0/0/0
[Huawei-GigabitEthernet0/0/0] ip address 192.168.1.2 24
[Huawei-GigabitEthernet0/0/0] quit
[Huawei] voice
[Huawei-voice] voip-address media interface gigabitethernet 0/0/0 192.168.1.2
[Huawei-voice] voip-address signalling interface gigabitethernet 0/0/0 192.168.1.2
```

步骤3 配置SIP服务器。

```
[Huawei-voice] sipserver
[Huawei-voice-sipserver] signalling-address ip 192.168.1.2 port 5060
[Huawei-voice-sipserver] media-ip 192.168.1.2
[Huawei-voice-sipserver] register-uri abcd.com
[Huawei-voice-sipserver] home-domain abcd.com
[Huawei-voice-sipserver] reset
[Huawei-voice-sipserver] quit
```

步骤4 配置默认国家码为86，默认地区码为571，并开启国家码地区码变换。

```
[Huawei-voice] pbx default-country-code 86 default-area-code 571
[Huawei-voice] pbx enable-country-area-transform enable
```

步骤5 配置号码归属的企业、号首集。

```
[Huawei-voice] enterprise hw
[Huawei-voice-enterprise-hw] dn-set hwdnset
[Huawei-voice-enterprise-hw] save
[Huawei-voice-enterprise-hw] quit
```

步骤6 配置字冠。

1. 配置字冠为7的呼叫属性为0的本局呼叫。

   出局字冠83787的配置方法参考此配置，只要修改最小号长为8位即可。

   ```
   [Huawei-voice] callprefix 7
   [Huawei-voice-callprefix-7] prefix 7
   [Huawei-voice-callprefix-7] call-type category basic-service attribute 0
   ```

 版权所有 © 华为技术有限公司

```
[Huawei-voice-callprefix-7] digit-length 4 32
[Huawei-voice-callprefix-7] quit
```

2. 配置字冠9的呼叫属性为1的字冠，字冠的路由为3。

   配置90的呼叫属性为2的国内长途字冠、900的呼叫属性为3的国际长途字冠，字冠的路由为0，配置方法参见字冠9的配置。

```
[Huawei-voice] callprefix 9
[Huawei-voice-callprefix-9] prefix 9
[Huawei-voice-callprefix-9] call-type category basic-service attribute 1
[Huawei-voice-callprefix-9] digit-length 1 32
[Huawei-voice-callprefix-9] quit
[Huawei-voice] callroute 3
[Huawei-voice-calldroute-3] quit
[Huawei-voice] callprefix 9
[Huawei-voice-callprefix-9] callroute 3
[Huawei-voice-callprefix-9] quit
```

3. 配置字冠6的呼叫属性为1的字冠，字冠的路由为1。

   出局字冠90577的呼叫属性为1的字冠，字冠的路由为1，配置方法参见字冠6的配置。

```
[Huawei-voice] callprefix 6
[Huawei-voice-callprefix-6] prefix 6
[Huawei-voice-callprefix-6] call-type category basic-service attribute 1
[Huawei-voice-callprefix-6] digit-length 4 32
[Huawei-voice-callprefix-6] quit
[Huawei-voice] callroute 1
[Huawei-voice-calldroute-1] quit
[Huawei-voice] callprefix 6
[Huawei-voice-callprefix-6] callroute 1
[Huawei-voice-callprefix-6] quit
```

4. 配置自动总机。

   自动总机名字为ivr，总机号码为83786005。

```
[Huawei-voice] callprefix ivr
[Huawei-voice-callprefix-ivr] prefix 83786005
[Huawei-voice-callprefix-ivr] enterprise hw dn-set hwdnset
[Huawei-voice-callprefix-ivr] call-type category vu-service vu-service-name vudefault
[Huawei-voice-callprefix-ivr] digit-length 8 32
[Huawei-voice-callprefix-ivr] save
[Huawei-voice-callprefix-ivr] quit
```

步骤7 配置用户号码。

1. 配置用户号码为7000的SIP用户，鉴权密码为YsHsjx_202206，用户的呼入呼出权限为all。

```
[Huawei-voice] pbxuser 7000 sipue
[Huawei-voice-pbxuser-7000] sipue 7000
[Huawei-voice-pbxuser-7000] telno 7000 long-telno 83787000
[Huawei-voice-pbxuser-7000] call-right in all
[Huawei-voice-pbxuser-7000] call-right out all
[Huawei-voice-pbxuser-7000] eid-para password cipher
 Please input user password(6-64 chars): *******
[Huawei-voice-pbxuser-7000] quit
```

2. 配置用户号码为7100的POTS用户，用户的呼入呼出权限为all。

```
[Huawei-voice] pbxuser 7100 pots
[Huawei-voice-pbxuser-7100] port 2/0/0
[Huawei-voice-pbxuser-7100] telno 7100 long-telno 83787100
[Huawei-voice-pbxuser-7100] call-right in all
[Huawei-voice-pbxuser-7100] call-right out all
[Huawei-voice-pbxuser-7100] quit
```

 版权所有 © 华为技术有限公司

步骤8 配置中继群。

1. 配置PRA中继群。

```
<Huawei> system-view
[Huawei] set workmode slot 3 e1t1 e1-voice
Changing the working mode will reset the board in slot 3. Continue? [y/n]:y
INFO: Resetting board[3] succeeded.
[Huawei] voice
[Huawei-voice] port ve1 3/0/0
[Huawei-voice-ve1-3/0/0] signal ccs
  Set signal type successfully
[Huawei-voice-ve1-3/0/0] quit
[Huawei-voice] quit
[Huawei] clock source 0 3/0/0
[Huawei] voice
[Huawei-voice] callroute 0
[Huawei-voice-calldroute-0] quit
[Huawei-voice] trunk-group pra dss1-user
[Huawei-voice-trunkgroup-pra] trunk-pra 3/0/0
[Huawei-voice-trunkgroup-pra] callroute 0
[Huawei-voice-trunkgroup-pra] quit
```

2. 配置SIP AT0中继群。

```
[Huawei-voice] trunk-group sipat0 sip trunk-circuit
[Huawei-voice-trunkgroup-sipat0] signalling-address ip 192.168.1.2 port 5061
[Huawei-voice-trunkgroup-sipat0] media-ip 192.168.1.2
[Huawei-voice-trunkgroup-sipat0] peer-address static 192.168.1.4 5060
[Huawei-voice-trunkgroup-sipat0] register-uri abcd.com
[Huawei-voice-trunkgroup-sipat0] home-domain abcd.com
[Huawei-voice-trunkgroup-sipat0] trunk-sipat0 +862083787005@abcd.com default-called-telno
83787005 password cipher
 Please input user password(1-32 chars):********
[Huawei-voice-trunkgroup-sipat0] number-parameter 19 1
[Huawei-voice-trunkgroup-sipat0] callroute 3
[Huawei-voice-trunkgroup-sipat0] reset
 Note: Trunkgroup reset succeeds.
[Huawei-voice-trunkgroup-sipat0] quit
```

3. 配置SIP IP中继群。

```
[Huawei-voice] trunk-group sipip01 sip no-register
[Huawei-voice-trunkgroup-sipip01] signalling-address ip 192.168.1.2 port 5062
[Huawei-voice-trunkgroup-sipip01] media-ip 192.168.1.2
[Huawei-voice-trunkgroup-sipip01] peer-address static 192.168.1.3 5062
[Huawei-voice-trunkgroup-sipip01] home-domain abcd.com
[Huawei-voice-trunkgroup-sipip01] register-uri abcd.com
[Huawei-voice-trunkgroup-sipip01] callroute 1
[Huawei-voice-trunkgroup-sipip01] reset
 Note: Trunkgroup reset succeeds.
[Huawei-voice-trunkgroup-sipat0] quit
```

步骤9 配置PBX的路由后号码变换。

IP PBX的路由后号码变换参考PBX的配置，只要将中继修改为pra中继、主叫号码为83786005即可。

```
[Huawei-voice] afterroute-change 9_6xxx_sipat0
[Huawei-voice-afterroute-change-9_6xxx_sipat0] callprefix 9
[Huawei-voice-afterroute-change-9_6xxx_sipat0] trunk-group sipat0
[Huawei-voice-afterroute-change-9_6xxx_sipat0] condition caller-telno 6xxx
[Huawei-voice-afterroute-change-9_6xxx_sipat0] caller del-then-insert 1 32 83786005
[Huawei-voice-afterroute-change-9_6xxx_sipat0] called del 1 1
[Huawei-voice-afterroute-change-9_6xxx_sipat0] quit
[Huawei-voice] afterroute-change 9_7xxx_sipat0
[Huawei-voice-afterroute-change-9_7xxx_sipat0] callprefix 9
[Huawei-voice-afterroute-change-9_7xxx_sipat0] trunk-group sipat0
[Huawei-voice-afterroute-change-9_7xxx_sipat0] condition caller-telno 7xxx
[Huawei-voice-afterroute-change-9_7xxx_sipat0] caller del-then-insert 1 32 83787005
[Huawei-voice-afterroute-change-9_7xxx_sipat0] called del 1 1
[Huawei-voice-afterroute-change-9_7xxx_sipat0] quit
```

 版权所有 © 华为技术有限公司

步骤10 验证配置结果

验证项	正常结果	可能的异常原因
局内呼叫	比如用户7000拨打用户7100能够正常通话，7100用户显示主叫号码为7000。	局内字冠配置问题。
配置长号的用户出局呼叫	能正常通话，并且号码显示正常。 ● 比如用户7000拨打用户6000能够正常通话，6000用户显示主叫号码为7000。 ● 比如用户7000从SIP AT0出局呼叫，被叫用户显示主叫号码为83787000。 ● 比如用户7000从PRA出局呼叫，被叫用户显示主叫号码为83787000。	● 出局字冠配置问题。 ● 出局中继问题或者配置完成后没有执行**reset**命令。
没有配置长号的用户出局呼叫	能正常通话，并且号码显示正常。 ● 比如用户7100拨打用户6000能够正常通话，6000用户显示主叫号码为7100。 ● 比如用户7100从SIP AT0出局呼叫，被叫用户显示主叫号码为83787005。 ● 比如用户7100从PRA出局呼叫，被叫用户显示主叫号码为83786005。	-
入局呼叫	能正常通话，比如局外用户拨打PBX的自动总机83787005，主叫根据语音提示，再拨打分机号码7000转接到7000用户。	-

----结束

配置文件

- Router的配置文件

```
#
 clock source 0 3/0/0 priority 9
```

 版权所有 © 华为技术有限公司

```
#
 set workmode slot 3 e1t1 e1-voice
#
interface GigabitEthernet0/0/0
 ip address 192.168.1.2 255.255.255.0
#
voice
 voip-address media interface GigabitEthernet 0/0/0 192.168.1.2
 voip-address signalling interface GigabitEthernet 0/0/0 192.168.1.2
 pbx default-area-code 571
 pbx enable-country-area-transform enable
 #
 port ve1 3/0/0
  signal CCS
 #
 callroute 0
 #
 callroute 1
 #
 callroute 3
 #
 enterprise hw
  dn-set hwdnset
 #
 sipserver
  signalling-address ip 192.168.1.2 port 5060
  media-ip 192.168.1.2
  register-uri abcd.com
  home-domain abcd.com
 #
 trunk-group pra dss1-user
  callroute 0
  trunk-pra 3/0/0
 #
 trunk-group sipat0 sip trunk-circuit
  callroute 3
  signalling-address ip 192.168.1.2 port 5061
  media-ip 192.168.1.2
  peer-address static 192.168.1.4 5060
  register-uri abcd.com
  home-domain abcd.com
  number-parameter 19 1
  trunk-sipat0 +862083787005@abcd.com password cipher %^%#sh1hK7Y[vIDIo]@
%y)"(^`xyQQLvuFT&:]Fob_b5%^%#
 #
 trunk-group sipip01 sip no-register
  callroute 1
  signalling-address ip 192.168.1.2 port 5062
  media-ip 192.168.1.2
  peer-address static 192.168.1.3 5062
  register-uri abcd.com
  home-domain abcd.com
 #
 callprefix 6
  prefix 6
  call-type category basic-service attribute 1
  digit-length 4 32
  callroute 1
 #
 callprefix 7
  prefix 7
  call-type category basic-service attribute 0
  digit-length 4 32
 #
 callprefix 9
  prefix 9
  call-type category basic-service attribute 1
  digit-length 1 32
  callroute 3
```

 版权所有 © 华为技术有限公司

```
#
callprefix ivr
 enterprise hw dn-set local
 prefix 83786005
 call-type category vu-service vu-service-name vudefault
 digit-length 8 32
#
 pbxuser 7000 sipue
  sipue 7000
  telno 7000 long-telno 83787000
  call-right out all
  eid-para password cipher %^%#%')'%i~C[2>B0.~$l6E@D)H|+:L0I!`Dg@,2>qjJ%^%#
 #
 pbxuser 7100 pots
  port 2/0/0
  telno 7100 long-telno 83787100
  call-right out all
 #
 afterroute-change 9_6xxx_sipat0
  callprefix 9
  trunk-group sipat0
  condition caller-telno 6xxx
  caller del-then-Insert 1 32 83786005
  called del 1 1
 #
 afterroute-change 9_7xxx_sipat0
  callprefix 9
  trunk-group sipat0
  condition caller-telno 7xxx
  caller del-then-Insert 1 32 83787005
  called del 1 1
 #
```

14.5 配置中小企业语音业务示例

组网需求

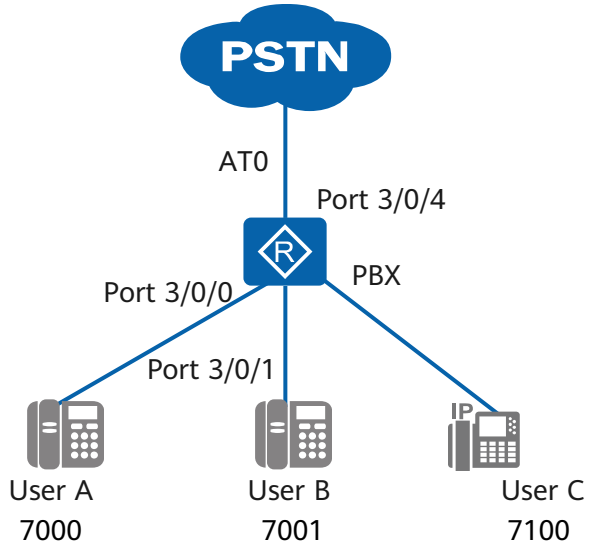
某中小企业因业务需求，需要实现内部用户在PBX注册，从而进行通话和视频。PBX将运营商给企业分配外部号码配置为自动总机，局外用户拨打该号码后根据语音提示，再拨打分机号码转接到局内用户；局内用户短号互拨。语音业务组网如图1所示。

本节以实现以下功能为例：

- 国家码为86，地区码为571。
- User A的局内号码为7000，User B的局内号码为7001，User C的局内号码为7100。
- User A、User B和User C所属的企业为hw、号首集为local、本局呼叫字冠为7，出局呼叫字冠为9，所有的用户呼入呼出权限均为all。
- 信令IP地址和媒体IP地址是192.168.1.2。
- 配置自动总机名为ivr，将PSTN分配的一个号码作为总机的号码，如28980808。
- PBX上从FXO口出局时，配置路由后号码变换方案9，主叫号码不变换，被叫删除第一位。

 版权所有 © 华为技术有限公司

图 14-5 语音业务组网



前提条件

已经完成IVR配置，自动总机配置的“vu-service-name”为IVR配置的“业务名称”。

数据规划

本例中数据规划为举例说明，实际配置需要与用户和运营商协商确定。

表 14-24 用户号码规划

POTS用户	SIP用户	备注
7000–7004	7100–7104	PBX用户

表 14-25 AT0 中继规划

槽位号/子卡号/端口号	默认接入号码	路由号
3/0/4	28980808	0

表 14-26 字冠规划

字冠	类型	路由
7	局内	-
9	出局	0

版权所有 © 华为技术有限公司

表 14-27 路由后号码变换规划

字冠	中继出局	被叫号码变换
9	AT0	删除第一位

操作步骤

步骤1 配置业务模式为PBX。

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] service-mode pbx
[Huawei-voice] return
[Huawei] save
The current configuration will be written to the device.
  Are you sure to continue? (y/n)[n]:y It will take several minutes to save configuration file, please wait.....
  Configuration file had been saved successfully
  Note: The configuration file will take effect after being activated
<Huawei>reboot
Info: The system is comparing the configuration, please wait.
System will reboot! Continue ? [y/n]:y Info: system is rebooting, please wait...
```

步骤2 配置接口GE0/0/0的以太网IP地址为192.168.1.2，并把192.168.1.2加入到该接口的媒体IP地址池和信令IP地址池。

```
<Huawei> system-view
[Huawei] interface gigabitethernet 0/0/0
[Huawei-GigabitEthernet0/0/0] ip address 192.168.1.2 24
[Huawei-GigabitEthernet0/0/0] quit
[Huawei] voice
[Huawei-voice] voip-address media interface gigabitethernet 0/0/0 192.168.1.2
[Huawei-voice] voip-address signalling interface gigabitethernet 0/0/0 192.168.1.2
```

步骤3 配置SIP服务器。

```
[Huawei-voice] sipserver
[Huawei-voice-sipserver] signalling-address ip 192.168.1.2 port 5060
[Huawei-voice-sipserver] media-ip 192.168.1.2
[Huawei-voice-sipserver] register-uri abcd.com
[Huawei-voice-sipserver] home-domain abcd.com
[Huawei-voice-sipserver] reset
[Huawei-voice-sipserver] quit
```

步骤4 配置默认国家码为86，默认地区码为571，并开启国家码地区码变换。

```
[Huawei-voice] pbx default-country-code 86 default-area-code 571
```

步骤5 配置号码归属的企业、号首集。

```
[Huawei-voice] enterprise hw
[Huawei-voice-enterprise-hw] dn-set local
[Huawei-voice-enterprise-hw] quit
```

步骤6 配置字冠的企业为hw、号首集为local、字冠为7的呼叫属性为0的本局呼叫，字冠9的呼叫属性为1的本地呼叫，字冠90呼叫属性为2的国内长途，900呼叫属性为3的国际长途。

```
[Huawei-voice] callprefix 7
[Huawei-voice-callprefix-7] enterprise hw dn-set local
[Huawei-voice-callprefix-7] prefix 7
[Huawei-voice-callprefix-7] call-type category basic-service attribute 0
[Huawei-voice-callprefix-7] digit-length 3 32
[Huawei-voice-callprefix-7] quit
[Huawei-voice] callprefix 9
[Huawei-voice-callprefix-9] enterprise hw dn-set local
[Huawei-voice-callprefix-9] prefix 9
[Huawei-voice-callprefix-9] call-type category basic-service attribute 1
```

 版权所有 © 华为技术有限公司

```
[Huawei-voice-callprefix-9] digit-length 1 32
[Huawei-voice-callprefix-9] quit
[Huawei-voice] callprefix 90
[Huawei-voice-callprefix-90] enterprise hw dn-set local
[Huawei-voice-callprefix-90] prefix 90
[Huawei-voice-callprefix-90] call-type category basic-service attribute 2
[Huawei-voice-callprefix-90] digit-length 2 32
[Huawei-voice-callprefix-90] quit
[Huawei-voice] callprefix 900
[Huawei-voice-callprefix-900] enterprise hw dn-set local
[Huawei-voice-callprefix-900] prefix 900
[Huawei-voice-callprefix-900] call-type category basic-service attribute 3
[Huawei-voice-callprefix-900] digit-length 3 32
[Huawei-voice-callprefix-900] quit
```

步骤7 配置自动总机。

自动总机名字为ivr，总机号码为28980808。

```
[Huawei-voice] callprefix ivr
[Huawei-voice-callprefix-ivr] prefix 28980808
[Huawei-voice-callprefix-ivr] enterprise hw dn-set local
[Huawei-voice-callprefix-ivr] call-type category vu-service vu-service-name vudefault
[Huawei-voice-callprefix-ivr] digit-length 8 32
[Huawei-voice-callprefix-ivr] save
[Huawei-voice-callprefix-ivr] quit
```

步骤8 配置用户号码为7100的SIP用户，鉴权密码为YsHsjx_202206，用户的呼入呼出权限为all。

```
[Huawei-voice] pbxuser 7100 sipue enterprise hw
[Huawei-voice-pbxuser-7100] dn-set local
[Huawei-voice-pbxuser-7100] sipue 7100
[Huawei-voice-pbxuser-7100] telno 7100
[Huawei-voice-pbxuser-7100] call-right in all
[Huawei-voice-pbxuser-7100] call-right out all
[Huawei-voice-pbxuser-7100] eid-para password cipher
 Please input user password(6-64 chars): *******
[Huawei-voice-pbxuser-7100] quit
```

步骤9 配置用户号码为7000和7001的POTS用户，用户的呼入呼出权限为all。

```
[Huawei-voice] pbxuser 7000 pots enterprise hw
[Huawei-voice-pbxuser-7000] dn-set local
[Huawei-voice-pbxuser-7000] port 3/0/0
[Huawei-voice-pbxuser-7000] telno 7000
[Huawei-voice-pbxuser-7000] call-right in all
[Huawei-voice-pbxuser-7000] call-right out all
[Huawei-voice-pbxuser-7000] quit
[Huawei-voice] pbxuser 7001 pots enterprise hw
[Huawei-voice-pbxuser-7001] dn-set local
[Huawei-voice-pbxuser-7001] port 3/0/1
[Huawei-voice-pbxuser-7001] telno 7001
[Huawei-voice-pbxuser-7001] call-right in all
[Huawei-voice-pbxuser-7001] call-right out all
[Huawei-voice-pbxuser-7001] quit
```

步骤10 配置AT0中继群。

```
[Huawei-voice] trunk-group at0 fxo
[Huawei-voice-trunkgroup-at0] enterprise hw dn-set local
[Huawei-voice-trunkgroup-at0] trunk-at0 3/0/4 default-called-telno 28980808
[Huawei-voice-trunkgroup-at0] quit
```

步骤11 配置呼叫路由和路由后号码变换。

```
[Huawei-voice] callroute 9
[Huawei-voice-calldroute-9] quit
[Huawei-voice] callprefix 9
[Huawei-voice-callprefix-9] callroute 9
[Huawei-voice-callprefix-9] quit
```

 版权所有 © 华为技术有限公司

```
[Huawei-voice] trunk-group at0
[Huawei-voice-trunkgroup-at0] callroute 9
[Huawei-voice-trunkgroup-at0] quit
[Huawei-voice] afterroute-change 9
[Huawei-voice-afterroute-change-9] callprefix 9
[Huawei-voice-afterroute-change-9] trunk-group at0
[Huawei-voice-afterroute-change-9] caller no-change
[Huawei-voice-afterroute-change-9] called del 1 1
[Huawei-voice-afterroute-change-9] save
```

步骤12 验证配置结果

验证项	正常结果	可能的异常原因
局内呼叫	比如用户7000拨打用户7100能够正常通话，7100用户显示主叫号码为7000。	局内字冠配置问题。
出局呼叫	能正常通话，并且号码显示正常。比如用户7000从AT0出局呼叫，被叫用户显示主叫号码为28980808。	• 出局字冠配置问题。 • 出局中继问题。
入局呼叫	能正常通话，比如局外用户拨打PBX的自动总机28980808，主叫根据语音提示，再拨打分机号码7000转接到7000用户。	-

----结束

配置文件

- Router的配置文件

```
#
interface GigabitEthernet0/0/0
ip address 192.168.1.2 255.255.255.0
#
voice
voip-address media interface GigabitEthernet 0/0/0 192.168.1.2
voip-address signalling interface GigabitEthernet 0/0/0 192.168.1.2
pbx default-area-code 571
#
callroute 9
#
enterprise hw
 dn-set local
#
sipserver
 signalling-address ip 192.168.1.2 port 5060
 media-ip 192.168.1.2
 register-uri abcd.com
 home-domain abcd.com
#
trunk-group at0 fxo
 enterprise hw dn-set local
 trunk-at0 3/0/4 default-called-telno 28980808
 callroute 9
#
callprefix 7
```

 版权所有 © 华为技术有限公司

```
 enterprise hw dn-set local
 prefix 7
 call-type category basic-service attribute 0
 digit-length 3 32
#
callprefix 9
 enterprise hw dn-set local
 prefix 9
 call-type category basic-service attribute 1
 digit-length 1 32
 callroute 9
#
callprefix 90
 enterprise hw dn-set local
 prefix 90
 call-type category basic-service attribute 2
 digit-length 2 32
#
callprefix 900
 enterprise hw dn-set local
 prefix 900
 call-type category basic-service attribute 3
 digit-length 3 32
#
callprefix ivr
 enterprise hw dn-set local
 prefix 28980808
 call-type category vu-service vu-service-name vudefault
 digit-length 8 32
#
pbxuser 7000 pots enterprise hw
 telno 7000
 dn-set local
 port 3/0/0
 call-right out all
#
pbxuser 7001 pots enterprise hw
 telno 7001
 dn-set local
 port 3/0/0
 call-right out all
#
pbxuser 7100 sipue enterprise hw
 sipue 7100
 telno 7100
 dn-set local
 call-right out all
 eid-para password cipher %@%@nGE1Y)%q*~n14{5/1l2@,._1TrX7Eeq(Y>/,=AT'V"\~._4,%@%@
#
 afterroute-change 9
 callprefix 9
 trunk-group at0
 caller no-change
 called del 1 1
#
```

 版权所有 © 华为技术有限公司

15 部署可靠性

15.1 配置接口备份的示例（3G+3G）
15.2 配置接口备份的示例（ADSL+3G）
15.3 配置接口备份的示例（以太网+以太网）
15.4 配置通过动态路由备份，实现ISDN网络对IP网络备份的示例
15.5 配置BFD单跳检测链路的示例
15.6 配置BFD多跳检测链路的示例
15.7 配置通过部署VRRP，实现设备网关冗余备份的示例
15.8 配置通过部署VRRP，实现主备设备共同分担用户业务的示例

15.1 配置接口备份的示例（3G+3G）

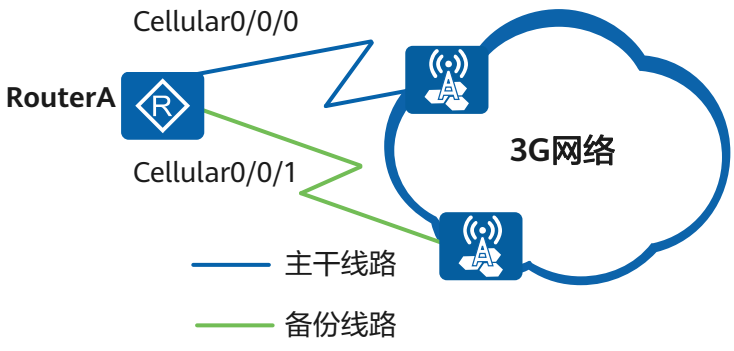
规格

适用于V200R001C01及更高版本、支持3G Cellular接口的路由器。

组网需求

在没有有线网络的情况下，使用RouterA的Cellular0/0/0接口作为主用接口，Cellular0/0/1接口作为备用接口，实现无线网络的中的数据传输备份。

图 15-1 通过接口备份和 3G 网络实现干线链路备份组网图



版权所有 © 华为技术有限公司

操作步骤

步骤1 RouterA的配置

```
# //主接口的配置
interface Cellular0/0/0
 link-protocol ppp
 ip address ppp-negotiate
 dialer enable-circular  //使能轮询DCC功能
 dialer-group 1
 dialer timer autodial 60  //配置DCC自动拨号间隔
 dialer number *99# autodial  //接口根据拨号串*99#进行自动拨号
 standby interface Cellular0/0/1  //配置Cellular0/0/1接口作为备份接口
#
interface Cellular0/0/1  //备份3G接口的配置
 link-protocol ppp
 ip address ppp-negotiate
 dialer enable-circular
 dialer-group 1
 dialer timer autodial 60
 dialer number *99# autodial
#
dialer-rule
 dialer-rule 1 ip permit
#
 ip route-static 0.0.0.0 0.0.0.0 Cellular0/0/0 preference 40
 ip route-static 0.0.0.0 0.0.0.0 Cellular0/0/1 preference 80
#
```

步骤2 验证配置结果

执行**display ip interface brief**检查接口状态，Cellular0/0/0接口的物理状态为“up”，并且已经通过协商获取到IP地址，作为备份的Cellular0/0/1接口的物理状态为“^down”，IP地址“unassigned”。在RouterA上Ping网关时，Cellular0/0/0接口通过的报文数增加。

shutdown主端口Cellular0/0/0后，Cellular0/0/1接口的物理状态为“up”，协商到IP地址，在RouterA上Ping网关时，Cellular0/0/1接口通过的报文数增加。

----结束

配置注意事项

- 3G接口只能用于轮询DCC。
- 主接口、备份接口到目的网段之间需要路由可达。
- 3G接口拨号时间较长，主备链路切换的过程中可能出现数据丢包。

15.2 配置接口备份的示例（ADSL+3G）

规格

适用于所有版本、所有形态的AR路由器。

组网需求

用户通过RouterA接入IP网络，业务对网络的连通性要求很高，短时间的网络中断都可能影响业务，因此需要通过接口备份的方式保证链路连通性。由于有线方式的网络接

 版权所有 © 华为技术有限公司

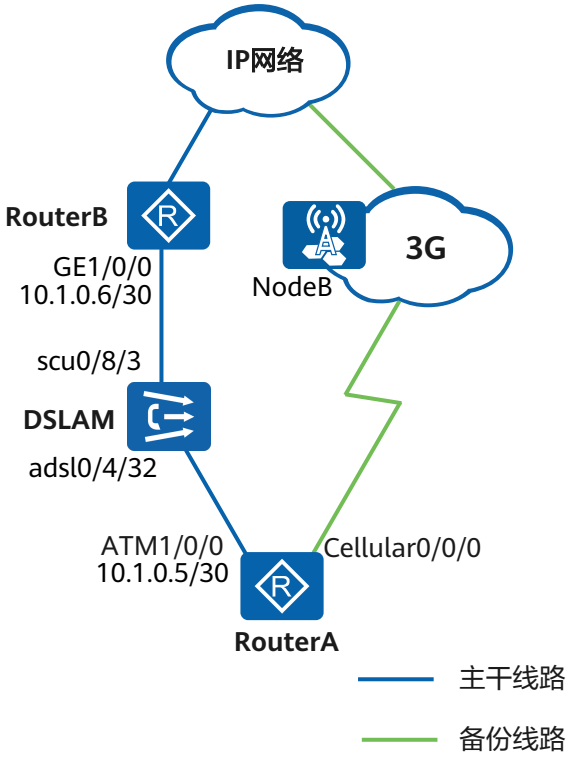
入安装周期长、费用高，而3G接入部署简单、灵活，该用户决定采用3G接口作为备份接口接入IP网络，当主链路发生故障时，流量切换到备份链路，以增强接入IP网络的可靠性。RouterA通过两条链路接入IP网络，具体需求如下：

- 主用链路：RouterA通过ADSL接口（普通电话线）连接至DSLAM的ADPD业务板，DSLAM通过主控上的接口与RouterB相连。
- 备用链路：RouterA通过Cellular接口接入NodeB。然后接入IP网络。

说明

该举例中的DSLAM设备为MA5600T设备，给出的配置仅供参考。

图 15-2 ADSL+3G 接口备份组网图



操作步骤

步骤1 RouterA的配置

```
#
interface Atm1/0/0  //连接ADSL的ATM接口
 ip address 10.1.0.5 255.255.255.252  //ATM接口的IP地址，与RouterB的GE1/0/0接口在同一网段
 pvc ipoa 20/80  //创建PVC，VPI为20，VCI为80
  map ip 10.1.0.6  //配置PVC上IPoA映射
 standby interface Cellular0/0/0  //配置3G接口作为备份接口
#
interface Cellular0/0/0  //做为备份的3G接口
 link-protocol ppp
 ip address ppp-negotiate
 dialer enable-circular  //使能轮询DCC功能
 dialer-group 1
 dialer timer autodial 60  //配置DCC自动拨号间隔
 dialer number *99# autodial  //接口根据拨号串*99#进行自动拨号
#
```


版权所有 © 华为技术有限公司

```
dialer-rule  //配置拨号访问控制列表
 dialer-rule 1 ip permit
#  //配置到网关的出口路由，不清楚网关地址时可以配置缺省路由
 ip route-static 200.168.2.0 255.255.255.0 10.1.0.6 preference 40
 ip route-static 200.168.2.0 255.255.255.0 Cellular0/0/0 preference 80
#
```

步骤2 DSLAM的配置

```
#
 vlan 100 smart
 port vlan 100 0/8 3  //将上行连接RouterB的接口加入VLAN
#
 interface scu 0/8
 native-vlan 3 vlan 100  //配置上行端口的Native VLAN
#
 service-port 40 vlan 100 adsl 0/4/32 vpi 20 vci 80  //加入业务虚端口
#
 mac-pool 3 00e0-fc12-3456  //配置3号MAC地址池，该地址池的起始地址为00e0-fc12-3456
 ipoa enable
 encapsulation 0/4/32 vpi 20 vci 80 type ipoa llc srcIP 10.1.0.5 dstIP 10.1.0.6
// 设置ADSL端口0/4/32的IPoA业务封装方式。VPI、VCI的值与RouterA上ATM接口VPI、VCI的值对应
#
```

步骤3 RouterB的配置

```
#
interface GigabitEthernet1/0/0
 ip address 10.1.0.6 255.255.255.252
#
```

步骤4 验证配置结果

执行**display ip interface brief**检查接口状态，ATM1/0/0接口的物理状态为“up”，作为备份的Cellular0/0/0接口的物理状态为“^down”。在RouterA上Ping网关时，ATM接口通过的报文数增加。

shutdown主端口ATM1/0/0后，Cellular0/0/0接口的物理状态为“up”，在RouterA上Ping网关时，Cellular接口通过的报文数增加。

----结束

配置注意事项

- 3G接口只能用于轮询DCC。
- 主接口、备份接口到目的网段之间需要路由可达。
- DSLAM设备上VPI，VCI的值需要与使能接口备份的设备上VPI，VCI值一致。首次在DSLAM进行IPoA的配置时，必须配置MAC地址池。
- 3G接口拨号时间较长，主备链路切换的过程中可能出现数据丢包。

15.3 配置接口备份的示例（以太网+以太网）

规格

适用于所有版本、所有形态的AR路由器。

组网需求

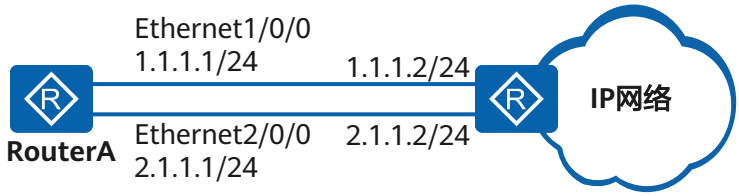
如图15-3所示，RouterA通过接口Ethernet1/0/0和Ethernet2/0/0连接到IP网络。

接口Ethernet1/0/0作为主接口。

 版权所有 © 华为技术有限公司

Ethernet2/0/0作为备份接口。

图 15-3 接口备份组网图



操作步骤

步骤1 RouterA的配置

```
#
interface Ethernet1/0/0
 ip address 1.1.1.1 255.255.255.0  //连接IP网络的主接口的IP地址
 standby interface Ethernet2/0/0 30  //指定Ethernet2/0/0为备份接口，优先级为30
#
interface Ethernet2/0/0
 ip address 2.1.1.1 255.255.255.0  //连接IP网络的备份接口的IP地址
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.2
 ip route-static 0.0.0.0 0.0.0.0 2.1.1.2
#
```

步骤2 验证配置结果

在RouterA上执行**display standby state**查看主备接口的状态信息。其中，Ethernet1/0/0的“Interfacestate”为**UP**，Ethernet2/0/0的“Interfacestate”为**STANDBY**。

----结束

配置注意事项

- 路由器支持的主备接口均为WAN侧接口。
- 一个主接口最多可以配置3个备份接口。
- 一个备份接口只能为一个主接口提供备份。
- 一台设备最多允许同时存在10个主接口。
- 当主接口出现故障时，多个备份接口根据优先级来决定接替工作的顺序。当优先级相同时，根据配置的先后来决定接替工作的顺序。

15.4 配置通过动态路由备份，实现 ISDN 网络对 IP 网络备份的示例

规格

适用于所有版本。

版权所有 © 华为技术有限公司

组网需求

如图15-4所示，RouterA和RouterB分别作为分支和总部的出口网关。

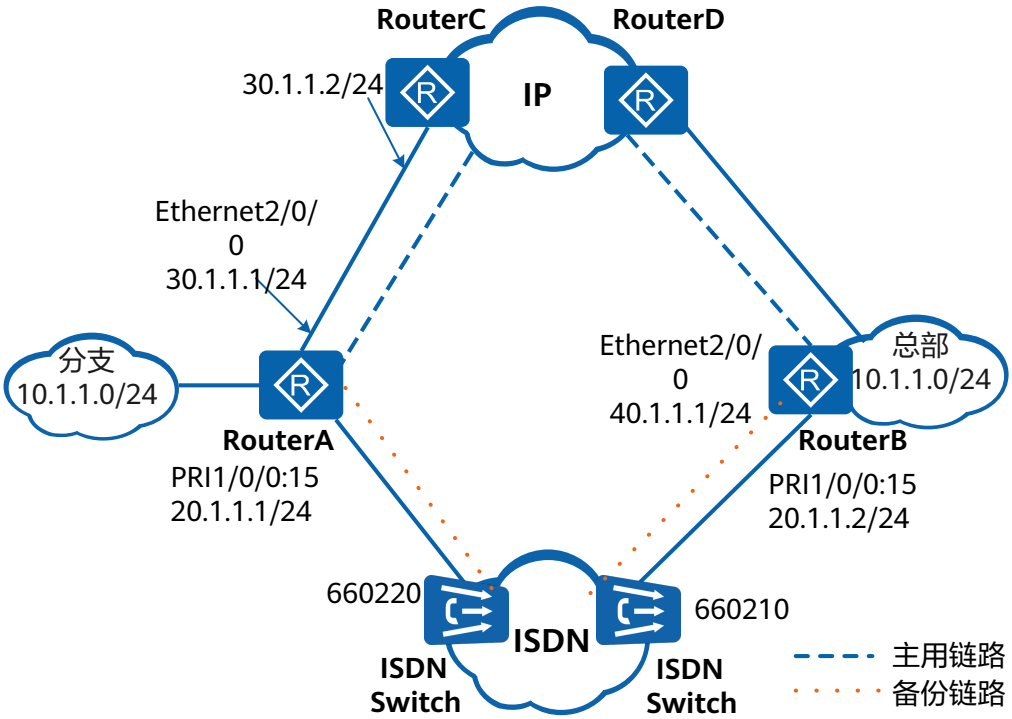
分支和总部通过IP网络连接作为主用链路。

分支和总部通过ISDN网络连接作为备份链路。

分支的接入号码是660220，总部的接入号码是660210。

分支对到达总部的路由10.1.2.0/24进行监控，当主用链路Down掉时，分支检测到路由失效，启用拨号链路进行备份。

图 15-4 动态路由备份组网图



操作步骤

步骤1 RouterA的配置

```
#
 standby routing-rule 1 ip 10.1.2.0 255.255.255.0  //创建动态路由备份组，并将被监控网段加入动态路由备份组
#
controller E1 1/0/0  //配置物理接口
 pri-set
#
interface Serial1/0/0:15
 link-protocol ppp
 ip address 20.1.1.1 255.255.255.0  //配置拨号接口的IP地址
 dialer enable-circular  //使能轮询DCC功能
 dialer-group 1  //配置拨号接口的拨号访问组1
 dialer route ip 20.1.1.2 broadcast 660210  //配置呼叫对端的目的地址及拨号串
 standby routing-group 1  //在拨号备份接口上启用动态路由备份功能
```


版权所有 © 华为技术有限公司

```
#
interface Ethernet2/0/0
 ip address 30.1.1.1 255.255.255.0  //配置主用链路分支出接口的IP地址
#
dialer-rule
 dialer-rule 1 ip permit  //配置拨号接口的拨号访问组1对应的拨号访问控制列表，指定引发DCC呼叫的条件
#
ospf 1 router-id 1.1.1.1   //配置OSPF动态路由协议
 area 0.0.0.0
  network 20.1.1.0 0.0.0.255
  network 30.1.1.0 0.0.0.255
  network 10.1.1.0 0.0.0.255
#
```

步骤2 RouterB的配置

```
#
controller E1 1/0/0  //配置物理接口
 pri-set
#
interface Serial1/0/0:15
 link-protocol ppp
 ip address 20.1.1.2 255.255.255.0  //配置拨号接口的IP地址
 dialer enable-circular  //使能轮询DCC功能
 dialer-group 1  //配置拨号接口的拨号访问组1
 dialer route ip 20.1.1.1 broadcast 660220  //配置呼叫对端的目的地址及拨号
串
#
interface Ethernet2/0/0
 ip address 40.1.1.1 255.255.255.0  //配置主用链路总部出接口的IP地址
#
 dialer-rule
 dialer-rule 1 ip permit  //配置拨号接口的拨号访问组1对应的拨号访问控制列表，指定引发DCC呼叫的条件
#
ospf 1 router-id 2.2.2.2   //配置OSPF动态路由协议
 area 0.0.0.0
  network 20.1.1.0 0.0.0.255
  network 40.1.1.0 0.0.0.255
  network 10.1.2.0 0.0.0.255
#
```

步骤3 RouterC、RouterD等中间设备的配置

具体配置步骤请参见RouterA或RouterB的OSPF动态路由协议的配置。配置完成后，确保RouterA和RouterB之间路由可达。

步骤4 验证配置结果

当主用链路路由可达时，在RouterA上查看路由表中对应目的网段（10.1.2.0/24）的出接口为Ethernet2/0/0，拨号接口Serial1/0/0:15上没有数据流量。

当主用链路路由失效时，启用备份链路，RouterA上查看路由表中对应目的网段（10.1.2.0/24）的出接口为Serial1/0/0:15，拨号接口Serial1/0/0:15上有数据流量通过。

----结束

配置注意事项

- 路由器最多支持创建255个动态路由备份组，且每个动态路由备份组只能监控一个网段地址。

15.5 配置 BFD 单跳检测链路的示例

 版权所有 © 华为技术有限公司

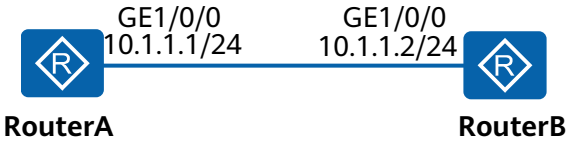
规格

适用于所有版本、所有形态的AR路由器。

组网需求

如图1所示，RouterA和RouterB之间通过三层物理链路直连。在IP链路上建立BFD会话，利用BFD检测机制检测两台设备之间的IP单跳路径，实现设备间链路故障的快速检测。

图 15-5 配置三层物理链路单跳检测组网图



操作步骤

步骤1 RouterA的配置

```
#
 sysname RouterA
#
 bfd
#
interface GigabitEthernet 1/0/0
 ip address 10.1.1.1 255.255.255.0
#
bfd atob bind peer-ip 10.1.1.2 interface GigabitEthernet 1/0/0  //创建三层链路单跳检测的BFD会话atob
 discriminator local 1  //配置本地标识符为1
 discriminator remote 2  //配置远端标识符为2
 commit
#
return
```

步骤2 RouterB的配置

```
#
 sysname RouterB
#
 bfd
#
interface GigabitEthernet 1/0/0
 ip address 10.1.1.2 255.255.255.0
#
bfd atob bind peer-ip 10.1.1.1 interface GigabitEthernet 1/0/0  //创建三层链路单跳检测的BFD会话atob
 discriminator local 2  //配置本地标识符为2
 discriminator remote 1  //配置远端标识符为1
 commit
#
return
```

步骤3 验证配置结果

配置完成后，在RouterA和RouterB上执行**display bfd session all verbose**命令，可以看到建立了一个单跳（One Hop）的BFD Session，且状态为Up。

----结束

 版权所有 © 华为技术有限公司

配置注意事项

- 第一次创建单跳BFD会话时，必须绑定对端IP地址和本端相应接口。
- 配置标识符时，本端的本地标识符与对端的远端标识符必需相同。

15.6 配置 BFD 多跳检测链路的示例

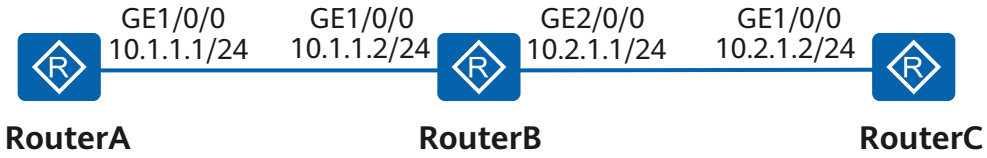
规格

适用于所有版本、所有形态的AR路由器。

组网需求

如图1所示，RouterA和RouterC为非直连设备，通过配置静态路由互通。用户希望可以实现对设备间链路故障的快速检测。

图 15-6 配置 BFD 多跳检测组网图



操作步骤

步骤1 RouterA的配置

```
#
 sysname RouterA
#
 bfd
#
interface GigabitEthernet1/0/0
ip address 10.1.1.1 255.255.255.0  //配置RouterA的接口IP地址
#
bfd atoc bind peer-ip 10.2.1.2  //配置多跳检测BFD会话
 discriminator local 10  //配置本地标识符为10
 discriminator remote 20  //配置远端标识符为20
 commit
#
 ip route-static 10.2.1.0 255.255.255.0 10.1.1.2  //配置静态路由使路由互通
#
return
```

步骤2 RouterB的配置

```
#
 sysname RouterB
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.2 255.255.255.0  //配置RouterB的接口IP地址
#
interface GigabitEthernet2/0/0  //配置RouterB的接口IP地址
 ip address 10.2.1.1 255.255.255.0
#
return
```

步骤3 RouterC的配置

版权所有 © 华为技术有限公司

```
#
 sysname RouterC
#
 bfd
#
interface GigabitEthernet1/0/0
 ip address 10.2.1.2 255.255.255.0  //配置RouterC的接口IP地址
#
bfd ctoa bind peer-ip 10.1.1.1  //配置多跳检测BFD会话
 discriminator local 20  //配置本端标识符为20
 discriminator remote 10  //配置远端标识符为10
 commit
#
ip route-static 10.1.1.0 255.255.255.0 10.2.1.1  //配置静态路由使路由互通
#
return
```

步骤4 验证配置结果

配置完成后，在RouterA和RouterC上执行display bfd session all verbose命令，可以看到建立了一个多跳BFD会话，且“(Multi Hop) State”状态为Up。

----结束

配置注意事项

- 在第一次创建多跳BFD会话时，必须绑定对端IP地址。
- BFD会话两端设备的本地标识符和远端标识符需要分别对应，否则会话无法正确建立。

15.7 配置通过部署 VRRP，实现设备网关冗余备份的示例

规格

适用于所有版本、所有形态的AR路由器。

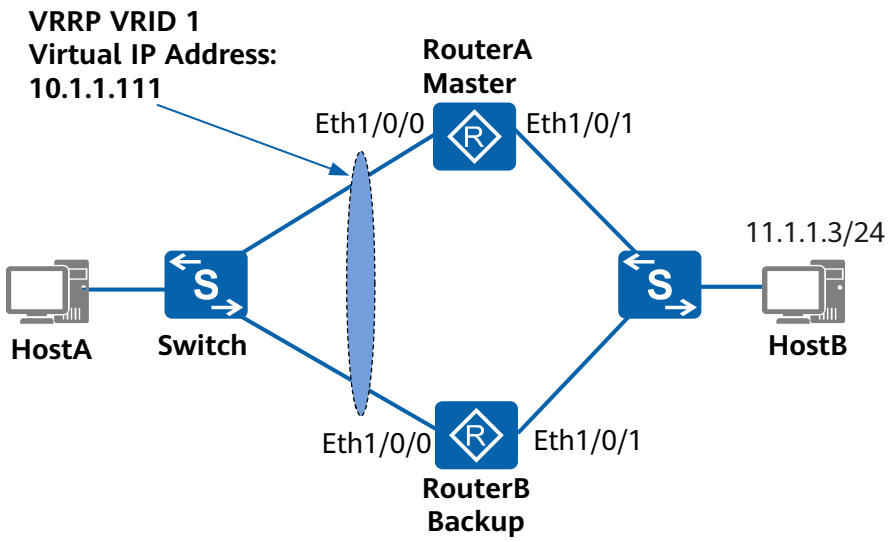
组网需求

如图15-7所示，HostA通过Switch双归属到RouterA和RouterB。主机HostA通过缺省网关访问主机HostB。RouterA和RouterB组成VRRP备份组，RouterA为主设备，RouterB为备用设备。用户希望实现：

- 正常情况下，主机以RouterA为默认网关接入Internet，当RouterA故障时，RouterB接替作为网关继续进行工作，实现网关的冗余备份。
- RouterA故障恢复后，能在20秒内抢占成为Master，重新成为网关。

 版权所有 © 华为技术有限公司

图 15-7 主备备份 VRRP 组网图



操作步骤

步骤1 RouterA的配置

```
#
interface Ethernet1/0/0
 ip address 10.1.1.1 255.255.255.0  //连接HostA的接口的IP地址
 vrrp vrid 1 virtual-ip 10.1.1.111  //配置虚拟网关地址
 vrrp vrid 1 priority 120  //配置RouterA在备份组中的优先级为120，缺省情况下，优先级为100，越大越优先
 vrrp vrid 1 preempt-mode timer delay 20  //配置抢占方式下的延迟时间
#
interface Ethernet1/0/1
 ip address 11.1.1.1 255.255.255.0  //连接HostB的接口的IP地址
#
```

步骤2 RouterB的配置

```
#
interface Ethernet1/0/0
 ip address 10.1.1.2 255.255.255.0  //连接HostA的接口的IP地址
 vrrp vrid 1 virtual-ip 10.1.1.111  //配置虚拟网关地址
#
interface Ethernet1/0/1
 ip address 11.1.1.2 255.255.255.0  //连接HostB的接口的IP地址
#
```

步骤3 验证配置结果

在RouterA上执行**display vrrp**命令可以查看RouterA上接口Ethernet1/0/0在VRRP备份组中的状态。其中“state”为**Master**。

在RouterB上执行**display vrrp**命令可以查看RouterB上接口Ethernet1/0/0在VRRP备份组中的状态。其中“state”为**Backup**。

----结束

配置注意事项

- RouterA和RouterB的虚拟网关地址要配置成一致。
- 需要配置RouterA和RouterB在备份组中的优先级，以确定主从关系。缺省情况下，优先级为100，越大越优先。

版权所有 © 华为技术有限公司

- 确保HostB与RouterA之间、HostB与RouterB之间分别路由可达。

15.8 配置通过部署 VRRP，实现主备设备共同分担用户业务的示例

规格

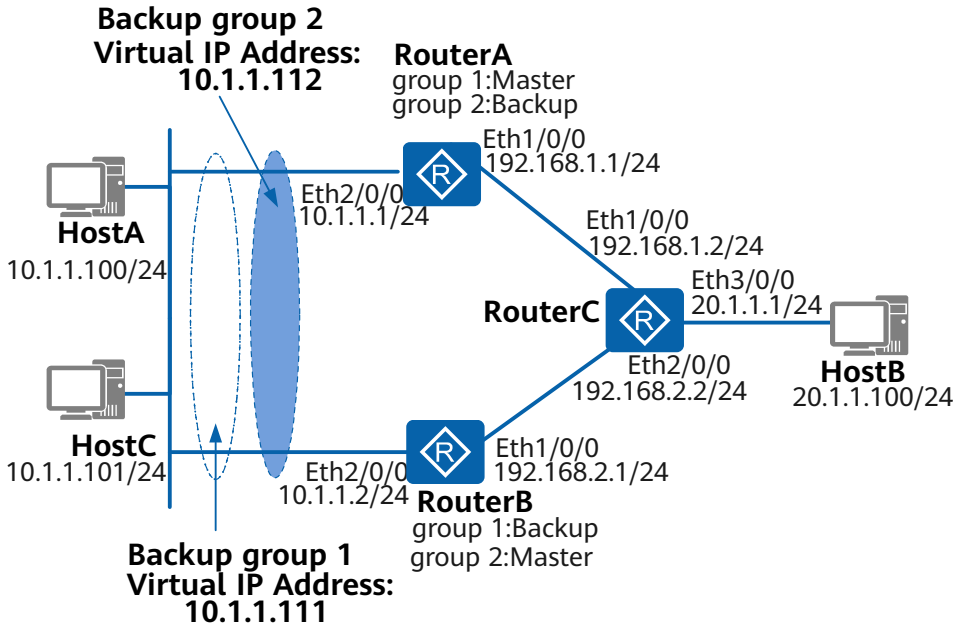
适用于所有版本、所有形态的AR路由器。

组网需求

如图15-8所示，RouterA和RouterB加入两个VRRP备份组以实现备份组中RouterA和RouterB既能相互备份，又能分担网络流量。用户希望HostA以RouterA为默认网关接入Internet，RouterB作为备份网关；HostC以RouterB为默认网关接入Internet，RouterA作为备份网关，以实现流量的负载均衡。具体需求如下：

- 在RouterA和RouterB上创建VRRP备份组1和VRRP备份组2。
- 在备份组1中，配置RouterA为Master设备，RouterB为Backup设备。
- 在备份组2中，配置RouterB为Master设备，RouterA为Backup设备。
- HostA使用备份组1作网关，HostC主机使用备份组2作为网关。

图 15-8 负载分担 VRRP 组网图



操作步骤

步骤1 RouterA的配置

```
#
interface Ethernet1/0/0
```


版权所有 © 华为技术有限公司

```
 ip address 192.168.1.1 255.255.255.0
#
interface Ethernet2/0/0
 ip address 10.1.1.1 255.255.255.0  //连接HostA的接口的IP地址
 vrrp vrid 1 virtual-ip 10.1.1.111  //配置备份组1的虚拟网关地址
 vrrp vrid 1 priority 120           //配置RouterA在备份组1中的优先级为120
 vrrp vrid 2 virtual-ip 10.1.1.112  //配置备份组2的虚拟网关地址
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
  network 10.1.1.0 0.0.0.255
#
```

步骤2 RouterB的配置

```
#
interface Ethernet1/0/0
 ip address 192.168.2.1 255.255.255.0
#
interface Ethernet2/0/0
 ip address 10.1.1.2 255.255.255.0  //连接HostC的接口的IP地址
 vrrp vrid 1 virtual-ip 10.1.1.111  //配置备份组1的虚拟网关地址
 vrrp vrid 2 virtual-ip 10.1.1.112  //配置备份组2的虚拟网关地址
 vrrp vrid 2 priority 120           //配置RouterB在备份组2中的优先级为120
#
ospf 1
 area 0.0.0.0
  network 192.168.2.0 0.0.0.255
  network 10.1.1.0 0.0.0.255
#
```

步骤3 RouterC的配置

```
#
interface Ethernet1/0/0
 ip address 192.168.1.2 255.255.255.0
#
interface Ethernet2/0/0
 ip address 192.168.2.2 255.255.255.0
#
interface Ethernet3/0/0
 ip address 20.1.1.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
  network 20.1.1.0 0.0.0.255
#
```

步骤4 验证配置结果

在HostA上对HostB进行**tracert**测试，可以看到HostA经过RouterA和RouterC到达HostB。显示信息看如下：

```
<HostA> tracert 20.1.1.100
 traceroute to  20.1.1.100(20.1.1.100), max hops: 30, packet length: 40
 1   10.1.1.1      120ms   50 ms   60 ms
 2   192.168.1.2   100 ms  60 ms   60 ms
 3   20.1.1.100    130 ms  90 ms   90 ms
```

在HostC上对HostB进行**tracert**测试，可以看到HostC经过RouterB和RouterC到达HostB。显示信息看如下：

```
<HostC> tracert 20.1.1.100
 traceroute to  20.1.1.100(20.1.1.100), max hops: 30, packet length: 40
 1   10.1.1.2     30 ms  60 ms  40 ms
 2   192.168.2.2  90 ms  60 ms  60 ms
 3   20.1.1.100   70 ms  60 ms  90 ms
```

 版权所有 © 华为技术有限公司

在RouterA上执行**display vrrp**命令，可以看到RouterA分别作为备份组1的Master和备份组2的Backup。其中备份组1的“state”为**Master**，备份组2的“state”为**Backup**。

```
<RouterA> display vrrp
  Ethernet2/0/0 | Virtual Router 1
    state          : Master
    Virtual IP     : 10.1.1.111
    Master IP      : 10.1.1.1
    PriorityRun    : 120
    PriorityConfig : 120
    MasterPriority : 120
    Preempt        : YES     Delay Time : 0 s
    TimerRun       : 1 s
    TimerConfig    : 1 s
    Auth Type      : NONE
    Virtual Mac    :  0000-5e00-0101
    Check TTL      : YES
    Config type    : normal-vrrp
    Backup-forward : disabled
    Create time    : 2007-11-22 16:02:21
    Last change time : 2007-11-22 16:02:25
  Ethernet2/0/0 | Virtual Router 2
    state          : Backup
    Virtual IP     : 10.1.1.112
    Master IP      : 10.1.1.2
    PriorityRun    : 100
    PriorityConfig : 100
    MasterPriority : 100
    Preempt        : YES     Delay Time : 0 s
    TimerRun       : 1 s
    TimerConfig    : 1 s
    Auth Type      : NONE
    Virtual Mac    :  0000-5e00-0102
    Check TTL      : YES
    Config type    : normal-vrrp
    Backup-forward : disabled
    Create time    : 2007-11-22 16:03:05
    Last change time : 2007-11-22 16:03:09
```

在RouterB的Ethernet2/0/0接口上执行**shutdown**命令，模拟备份组2的网关故障。在RouterA上执行**display vrrp**命令，可以看到RouterA分别作为备份组1的Master和备份组2的Master。其中，备份组1和备份组2的“state”均为**Master**。此时，两个VRRP备份组的虚拟网关都在RouterA上。

```
<RouterA> display vrrp
  Ethernet2/0/0 | Virtual Router 1
    state          : Master
    Virtual IP     : 10.1.1.111
    Master IP      : 10.1.1.1
    PriorityRun    : 120
    PriorityConfig : 120
    MasterPriority : 120
    Preempt        : YES     Delay Time : 0 s
    TimerRun       : 1 s
    TimerConfig    : 1 s
    Auth Type      : NONE
    Virtual Mac    :  0000-5e00-0101
    Check TTL      : YES
    Config type    : normal-vrrp
    Backup-forward : disabled
    Create time    : 2007-11-22 16:02:21
    Last change time : 2007-11-22 16:02:25
  Ethernet2/0/0 | Virtual Router 2
    state          : Master
    Virtual IP     : 10.1.1.112
    Master IP      : 10.1.1.1
    PriorityRun    : 100
    PriorityConfig : 100
    MasterPriority : 100
```

 版权所有 © 华为技术有限公司

```
Preempt       : YES     Delay Time : 0 s
TimerRun      : 1 s
TimerConfig   : 1 s
Auth Type     : NONE
Virtual Mac   :  0000-5e00-0102
Check TTL     : YES
Config type   : normal-vrrp
Backup-forward : disabled
Create time   : 2007-11-22 16:03:05
Last change time : 2007-11-22 16:03:09
```

----结束

配置注意事项

- RouterA和RouterB在同一个备份组中的虚拟网关地址要配置成一致。
- 需要配置路由器在不同备份组中的优先级，以确定主从关系。缺省情况下，优先级为100。
- 执行tracert测试前，需要分别在RouterA、RouterB和RouterC上分别执行命令**icmp port-unreachable send**使能ICMP端口不可达报文的发送功能。

 版权所有 © 华为技术有限公司

16 用户接入与认证

16.1 配置802.1x本地认证，以识别用户身份的示例
16.2 配置802.1x远端认证，由Radius服务器识别用户身份的示例
16.3 配置802.1x远端认证，由Radius主备服务器识别用户身份的示例
16.4 配置采用HWTACACS协议对Telnet用户进行命令行授权示例
16.5 配置用户通过STelnet登录设备的身份认证示例（RADIUS认证）
16.6 配置用户通过Telnet登录设备的身份认证示例（HWTACACS认证）

16.1 配置 802.1x 本地认证，以识别用户身份的示例

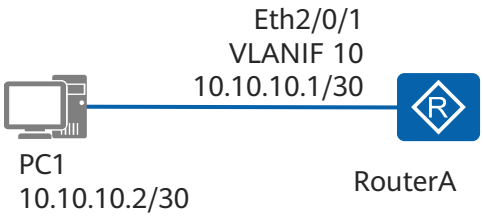
规格

适用于所有版本、所有形态的AR路由器。

组网需求

PC1(10.10.10.2/30)直接连接到RouterA的Eth2/0/1端口，RouterA的VLANIF10接口IP地址10.10.10.1/30（为PC1上的网关IP地址），配置802.1x协议进行访问控制，认证方式采用本地认证。

图 16-1 802.1x 本地认证组网图



版权所有 © 华为技术有限公司

操作步骤

步骤1 RouterA的配置

```
#
vlan batch 10
#
authentication-profile name p1
 dot1x-access-profile d1    //在认证模板p1上绑定802.1x接入模板d1
#
aaa
 local-user huawei password cipher %^%#3jJfL9#LQ>AIDJY~":3P^52}G"!M:/faAYTy,Z/ybp^0/"9i,tFOpPe4Lq!c"pn=%^%#  //添加本地用户密码为“YsHsjx_202206”
 local-user huawei privilege level 0
 local-user huawei service-type 8021x  //添加本地接入用户
#
interface Ethernet2/0/1
 port link-type access
 port default vlan 10
 authentication-profile p1  //接口下绑定认证模板p1
#
interface Vlanif10
 ip address 10.10.10.1 255.255.255.252
#
dot1x-access-profile name d1
 dot1x authentication-method pap
#
```

步骤2 验证配置结果

客户端认证软件输入用户名“huawei”，密码“YsHsjx_202206”可以成功上线，执行**display access-user**可以查看上线用户的信息。

----结束

配置注意事项

缺省情况下，接口下接入用户的认证方式为基于MAC，该接口下的所有用户上线时均需要单独认证。配置认证方式为基于接口时，只要该接口下的第一个用户认证成功后，其他802.1x用户无须认证。

16.2 配置 802.1x 远端认证，由 Radius 服务器识别用户身份的示例

规格

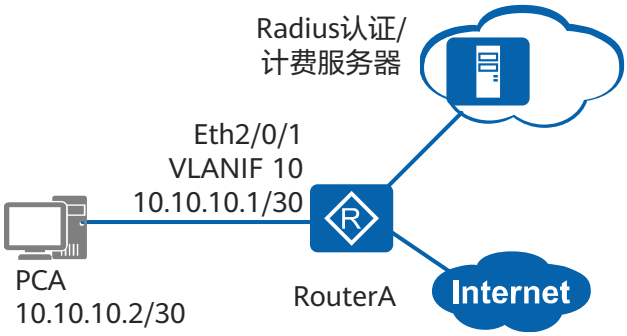
适用于所有版本、所有形态的AR路由器。

组网需求

用户通过RouterA访问网络。RouterA与RADIUS服务器之间路由可达。为了保证网络的安全性，要求在用户接入网络时进行认证。认证成功后可以正常访问网络。

 版权所有 © 华为技术有限公司

图 16-2 802.1x 远端认证组网图



操作步骤

步骤1 RouterA的配置

```
#
vlan batch 10
#
authentication-profile name p1
 dot1x-access-profile d1    //在认证模板p1上绑定802.1x接入模板d1
#
radius-server template radius1  //配置RADIUS服务器模板
 radius-server shared-key cipher %^%#,$*=V^v:!CNN#VE:5'p;tpY,G"!M:/faAYTy,Z/ybp^0/"9i,tFOpPe4Lq!c"pn=
%^%#  //配置路由器和RADIUS服务器之间的共享密钥为YsHsjx_202206
 radius-server authentication 10.11.1.1 1645  //配置RADIUS认证服务器
 radius-server accounting 10.11.1.1 1646  //配置RADIUS计费服务器
#
aaa
 authentication-scheme radius1  //配置认证方案
  authentication-mode radius  //指定认证方式为RADIUS认证
 accounting-scheme radius1  //配置计费方案
  accounting-mode radius  //指定计费模式为RADIUS模式
 domain huawei  //创建用户域
  authentication-scheme radius1  //指定该域用户的RADIUS认证方案
  accounting-scheme radius1  //指定该域用户的RADIUS计费方案
  radius-server  radius1  //指定该域用户的RADIUS服务器模板
#
interface Ethernet2/0/1
 port link-type access
 port default vlan 10
 authentication-profile p1  //接口下绑定认证模板p1
#
interface Vlanif10
 ip address 10.10.10.1 255.255.255.252
#
dot1x-access-profile name d1
#
```

步骤2 验证配置结果

RADIUS服务器添加用户**user1@huawei**，密码**YsHsjx_202206**，共享密钥与路由器保持一致配置为**YsHsjx_202206**。客户端认证成功后，执行**display access-user**可以查看**Username**字段里有用户名为**user1@huawei**，并且相应**Status**字段显示为**Success**。

----结束

版权所有 © 华为技术有限公司

配置注意事项

- RADIUS服务器认证端口缺省为1645或者1812，计费端口缺省为1646或者1813。路由器与RADIUS服务器上认证、计费端口的值需要保持一致。
- 路由器和RADIUS服务器上共享密钥需要保持一致。
- 路由器与RADIUS服务器间需要路由可达。

相关信息

视频

配置802.1x认证

16.3 配置 802.1x 远端认证，由 Radius 主备服务器识别用户身份的示例

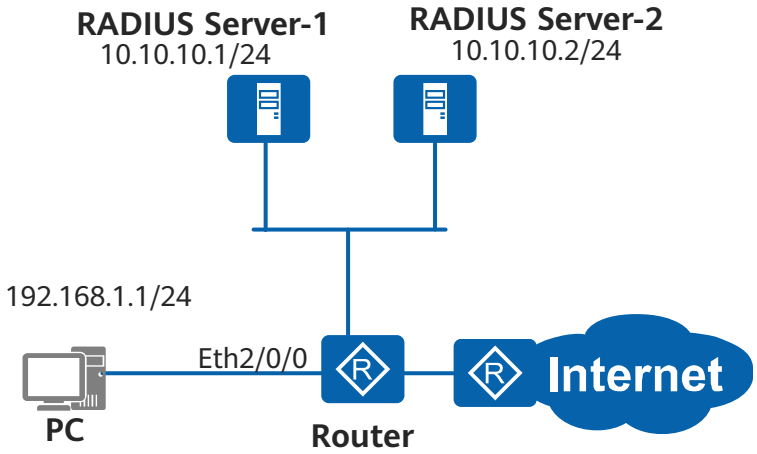
规格

适用于所有版本、所有形态的AR路由器。

组网需求

PC通过Router访问网络。为了保证网络的安全性，要求在用户接入网络时进行802.1x认证。认证服务器为两台Radius服务器，IP为10.10.10.1/24服务器作为主认证服务器，IP为10.10.10.2/24的服务器为备用认证服务器。当主用服务器不可用时，Router可以实现最快3s内切换到备用服务器。

图 16-3 配置采用 Radius 主备服务器的 802.1x 认证组网图



操作步骤

步骤1 Router上的配置

```
#
vlan batch 10
#
```


版权所有 © 华为技术有限公司

```
authentication-profile name p1
 dot1x-access-profile d1    //在认证模板p1上绑定802.1x接入模板d1
#
radius-server template shiva  //配置RADIUS服务器模板shiva
 radius-server shared-key cipher %^%#Q75cNQ6IF(e#L4WMxP~%^7'u17,]D87GO{"[o]`D%^
%#
 radius-server authentication 10.10.10.1 1812 //配置RADIUS主用认证服务器
 radius-server authentication 10.10.10.2 1812 //配置RADIUS备用认证服务器
#
aaa
 authentication-scheme scheme0 //创建名为scheme0的认证方案
  authentication-mode radius
 domain huawei //配置名为huawei的域
  authentication-scheme scheme0
  radius-server shiva
#
interface Vlanif10
 ip address 192.168.1.2 255.255.255.0
#
interface Ethernet2/0/0
 port link-type access
 port default vlan 10
 authentication-profile p1  //接口下绑定认证模板p1
#
dot1x-access-profile name d1
#
```

步骤2 验证配置结果

RADIUS服务器添加用户**user1@huawei**，密码**YsHsjx_202206**，共享密钥与路由器保持一致配置为**radius**。客户端认证成功后，执行**display access-user**可以查看**Username**字段里有用户名为**user1@huawei**，并且相应**Status**字段显示为**Success**。

----结束

配置注意事项

- 路由器与RADIUS服务器上认证端口的值需要保持一致。
- 路由器和RADIUS服务器上共享密钥需要保持一致。
- 路由器与RADIUS服务器间需要路由可达。

16.4 配置采用 HWTACACS 协议对 Telnet 用户进行命令行授权示例

规格

适用于所有版本、所有形态的AR路由器。

组网需求

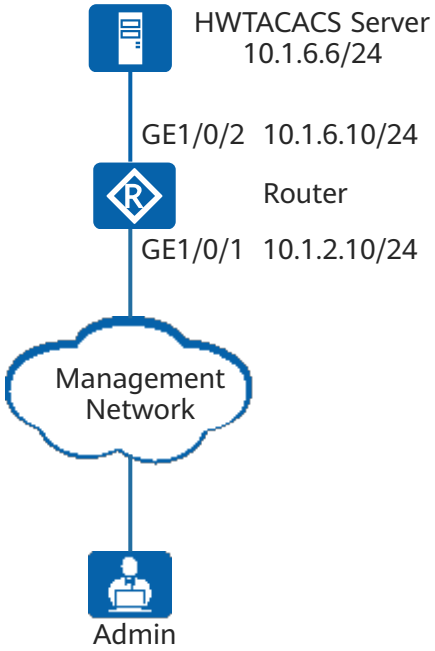
如图16-4所示，在某企业网内，部署一台AR路由器和一台HWTACACS服务器，用户通过设备访问网络，企业通过HWTACACS服务器对用户授权。为了实现精细化管理和保证设备环境的安全性，企业希望通过HWTACACS服务器对不同级别的接入用户进行命令授权，以实现部分用户不需要执行高级别的全部命令即可访问总部，并且记录用户在设备上执行过的命令。具体要求如下：

- HWTACACS服务器IP地址为10.1.6.6/24，认证端口号为49，授权端口号为49。

 版权所有 © 华为技术有限公司

- 用户处于huawei.com域，用户名为user1@huawei.com，用户密码为YsHsjx_202206。
- 对级别为3的用户实现按命令行授权。

图 16-4 基于 HWTACACS 系统的命令行授权



操作步骤

步骤1 Router上的配置

```
#
 sysname Router
#
hwtacacs-server template 1  //配置HWTACACS服务器模板
 hwtacacs-server authentication 10.1.6.6 weight 80  //配置HWTACACS认证服务器
 hwtacacs-server authorization 10.1.6.6 weight 80  //配置HWTACACS授权服务器
 hwtacacs-server shared-key cipher %^%#BS'$!w:u7H.lu:/&W9A5=pUtz3#CA>MtbD=>A]Ts;au$;&I!<sN~"B!+
+2S8'--;%^%#  //配置路由器和HWTACACS服务器之间的共享密钥为YsHsjx_202206
#
aaa
 authentication-scheme sch1  //创建名为sch1的认证方案
  authentication-mode hwtacacs
 authorization-scheme ht  //创建名为ht的授权方案
  authorization-mode hwtacacs
  authorization-cmd 3 hwtacacs  //指定对级别为3的用户实现按命令行授权
 recording-scheme scheme0  //创建名为scheme0的记录方案
  recording-mode hwtacacs 1  //指定与记录方案scheme0相关联的HWTACACS服务器模
板
 cmd recording-scheme scheme0  //指定记录方案scheme0的记录策略为记录用户在设备上执行过的命令
 service-scheme sch1  //创建名为sch1的业务方案
  admin-user privilege level 15
 domain huawei.com  //配置名为huawei.com的域
  authentication-scheme sch1  //指定该域用户采用的HWTACACS认证方案
  authorization-scheme ht  //指定该域用户采用的HWTACACS授权方案
```

 版权所有 © 华为技术有限公司

```
 service-scheme sch1  //指定该域用户采用的业务方案
 hwtacacs-server 1  //指定该域用户采用的HWTACACS服务器模板
#
interface GigabitEthernet1/0/1
 ip address 10.1.2.10 255.255.255.0
#
interface GigabitEthernet1/0/2
 ip address 10.1.6.10 255.255.255.0
#
 telnet server permit interface all          //配置Telnet服务器允许客户端连接的接口，否则无法使能Telnet服务。
 telnet server enable  //使能Telnet服务器功能
#
user-interface maximum-vty 15  //配置VTY用户界面的登录用户最大数目为15
user-interface vty 0 14
 authentication-mode aaa  //配置VTY类型用户界面的认证方式为AAA
#
return
```

步骤2 验证配置结果

管理员在PC上单击“运行”->输入“cmd”，进入Windows的命令行提示符界面，执行**telnet**命令，并输入用户名user1@huawei.com和密码YsHsjx_202206，通过Telnet方式登录设备成功。

```
C:\Documents and Settings\Administrator> telnet 10.1.2.10
Username:user1@huawei.com
Password:**********
<Router>//管理员登录设备成功
```

在设备上执行**display authorization-scheme ht**命令后，可以看到对级别为3的用户按命令行进行授权。

```
<Huawei> display authorization-scheme ht
------------------------------------------------------------------------------
 Authorization-scheme-name              : ht
 Authorization-method                   : HWTACACS
 Authorization-cmd level  0             : Disabled
 Authorization-cmd level  1             : Disabled
 Authorization-cmd level  2             : Disabled
 Authorization-cmd level  3             : Enabled  ( HWTACACS  )
 Authorization-cmd level  4             : Disabled
 Authorization-cmd level  5             : Disabled
 Authorization-cmd level  6             : Disabled
 Authorization-cmd level  7             : Disabled
 Authorization-cmd level  8             : Disabled
 Authorization-cmd level  9             : Disabled
 Authorization-cmd level 10             : Disabled
 Authorization-cmd level 11             : Disabled
 Authorization-cmd level 12             : Disabled
 Authorization-cmd level 13             : Disabled
 Authorization-cmd level 14             : Disabled
 Authorization-cmd level 15             : Disabled
 Authorization-cmd no-response-policy    : Online
------------------------------------------------------------------------------
```

----结束

配置注意事项

- 路由器与HWTACACS服务器上认证端口的值需要保持一致。
- 路由器和HWTACACS服务器上共享密钥需要保持一致。
- 路由器与HWTACACS服务器间需要路由可达。

 版权所有 © 华为技术有限公司

相关信息

视频

配置AAA用户

16.5 配置用户通过 STelnet 登录设备的身份认证示例（RADIUS 认证）

规格

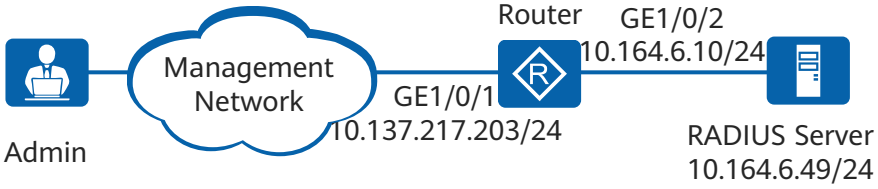
适用于所有版本、所有形态的AR路由器。

组网需求

用户使用STelnet方式连接Router，要求在SSH认证过程中，配置Router支持SSH用户通过RADIUS服务器进行远端认证。

RADIUS服务器认证该用户，将认证结果返回给Router。Router根据认证结果决定是否允许用户建立连接。

图 16-5 配置 SSH 支持 RADIUS 认证组网图



操作步骤

步骤1 在Router上生成本地密钥对

```
<Huawei> system-view
[Huawei] sysname Router
[Router] rsa local-key-pair create
The key name will be: Host
RSA keys defined for Host already exist.
Confirm to replace them? (y/n):y
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is less than 2048,
       It will introduce potential security risks.
Input the bits in the modulus[default = 2048]:2048
Generating keys...
.....+++
....+++
.....++++++++
.............++++++++
```

步骤2 在Router上配置AAA

```
#
radius-server template ssh  //指定服务器端的RADIUS模板为ssh
```


版权所有 © 华为技术有限公司

```
 radius-server shared-key cipher %^%#b8M{Q8]h|Xf(7*;+<N@IIq{c*g6x9%o`~R&/ok/X%^%  //配置RADIUS服务器密钥为密文密码YsHsjx_202206
 radius-server authentication 10.164.6.49 1812 weight 80  //配置RADIUS认证服务器的IP地址和端口号
#
aaa
 authentication-scheme newscheme  //配置SSH服务器端认证方案newscheme
  authentication-mode radius  //指定newscheme的认证方法为RADIUS
 domain ssh.com  //配置SSH服务端的RADIUS域名为ssh.com
  authentication-scheme newscheme  //指定该域用户的RADIUS认证方案
  radius-server ssh  //指定该域用户的RADIUS服务器模板
 local-user admin password irreversible-cipher $1a$QjpV-qYo;E$Eq,ZXUKmiBQsnn@#V_8H'XFcN/OEaVdFQ/%#$St;$  //配置SSH用户admin，密码为YsHsjx_202206
 local-user admin privilege level 15  //配置SSH用户的用户级别
 local-user admin service-type ssh  //配置SSH用户的服务类型
#
 domain ssh.com admin //配置ssh.com为全局默认管理域
#
interface GigabitEthernet1/0/1
 ip address 10.137.217.203 255.255.255.0
#
interface GigabitEthernet1/0/2
 ip address 10.164.6.10 255.255.255.0
#
 ssh user admin authentication-type password  //配置SSH用户的认证方式为password
 ssh server permit interface all              // 配置SSH服务器允许客户端连接的接口，否则无法使能STelnet服务。
 stelnet server enable //在SSH服务器端使能Stelnet服务器功能
#
user-interface vty 0 4
 authentication-mode aaa  //指定配置VTY0～4用户的认证方式为AAA，此时会要求输入本地用户的旧密码
 user privilege level 15  //配置VTY 0～VTY 4的用户级别为15级
 protocol inbound ssh  //配置VTY类型用户只支持SSH协议
#
return
```

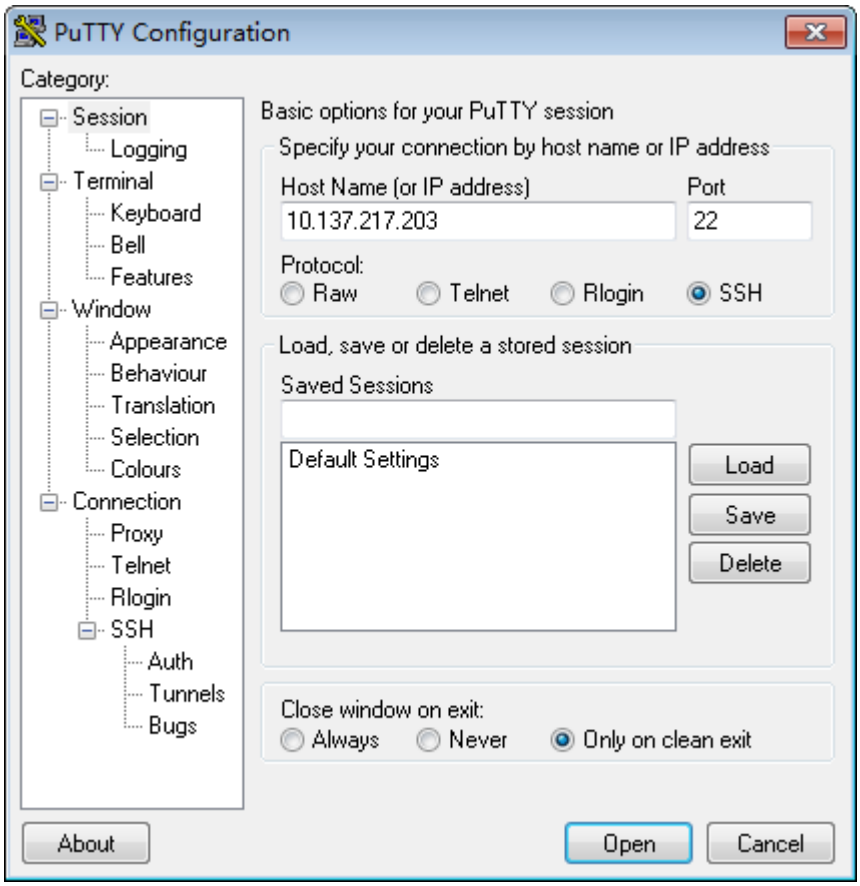
步骤3 验证配置结果

从终端通过STelnet登录设备，此处使用第三方软件putty为例进行介绍。

通过putty软件登录设备，输入设备的IP地址，选择协议类型为SSH。

 版权所有 © 华为技术有限公司

图 16-6 通过 putty 软件用 password 认证方式连接 SSH 服务器示意图



单击“Open”，出现如下界面，输入用户名admin和密码YsHsjx_202206，并按“Enter”键，至此已登录到Router。（以下显示信息仅为示意）

```
login as: admin
Sent username "admin"

admin@10.137.217.203's password:

<SSH Server>
```

----结束

配置注意事项

- 路由器与RADIUS服务器上认证端口的值需要保持一致。
- 路由器和RADIUS服务器上共享密钥需要保持一致。
- 配置SSH用户使用password验证，只需在SSH服务器端生成本地RSA密钥。
- 路由器与RADIUS服务器间需要路由可达。

相关信息

视频

配置AAA用户

版权所有 © 华为技术有限公司

配置RADIUS认证和计费

16.6 配置用户通过 Telnet 登录设备的身份认证示例（HWTACACS 认证）

规格

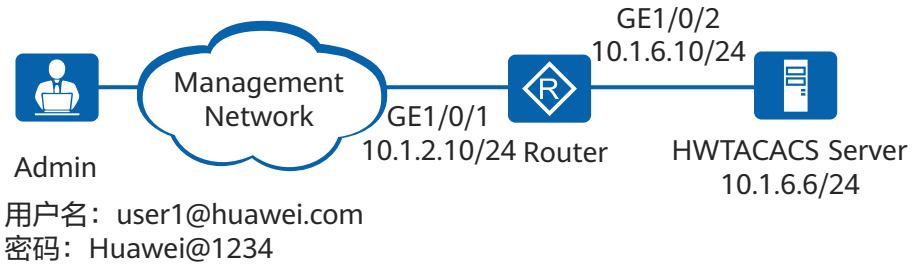
适用于所有版本、所有形态的AR路由器。

组网需求

如图16-7所示，网络中部署了HWTACACS服务器，企业希望管理员通过Telnet登录设备来远程管理设备：

1. 管理员输入正确的用户名和密码才能通过Telnet登录设备。
2. 管理员通过Telnet登录设备后，可以执行命令级别为0～15的所有命令行。

图 16-7 配置用户通过 Telnet 登录设备的身份认证示例（HWTACACS 认证）



操作步骤

步骤1 Router上的配置

```
#
 sysname Router
#
hwtacacs-server template 1  //配置HWTACACS服务器模板
 hwtacacs-server authentication 10.1.6.6 weight 80  //配置HWTACACS认证服务器
 hwtacacs-server shared-key cipher %^%#BS'$!w:u7H.lu:/&W9A5=pUtz3#CA>MtbD=>A]Ts;au$;&I!<sN~"B!+
+2S8'--;%^%#  //配置路由器和HWTACACS服务器之间的共享密钥为YsHsjx_202206
#
aaa
 authentication-scheme sch1  //创建名为sch1的认证方案
  authentication-mode hwtacacs  //指定认证方式为HWTACACS认证
 service-scheme sch1  //创建名为sch1的业务方案
  admin-user privilege level 15
 domain huawei.com  //配置名为huawei.com的域
  authentication-scheme sch1  //指定该域用户采用的HWTACACS认证方案
  service-scheme sch1  //指定该域用户采用的业务方案
  hwtacacs-server 1  //指定该域用户采用的HWTACACS服务器模板
#
interface GigabitEthernet1/0/1
 ip address 10.1.2.10 255.255.255.0
#
interface GigabitEthernet1/0/2
 ip address 10.1.6.10 255.255.255.0
```


版权所有 © 华为技术有限公司

```
#
 telnet server permit interface all          //配置Telnet服务器允许客户端连接的接口，否则无法使能Telnet服务。
 telnet server enable  //使能Telnet服务器功能
#
user-interface maximum-vty 15  //配置VTY用户界面的登录用户最大数目为15
user-interface vty 0 14
 authentication-mode aaa  //配置VTY类型用户界面的认证方式为AAA
#
return
```

步骤2 验证配置结果

管理员在PC上单击“运行”->输入“cmd”，进入Windows的命令行提示符界面，执行**telnet**命令，并输入用户名user1@huawei.com和密码YsHsjx_202206，通过Telnet方式登录设备成功。

```
C:\Documents and Settings\Administrator> telnet 10.1.2.10
Username:user1@huawei.com
Password:**********
<Router>//管理员登录设备成功
```

----结束

配置注意事项

- 路由器与HWTACACS服务器上认证端口的值需要保持一致。
- 路由器和HWTACACS服务器上共享密钥需要保持一致。
- 路由器与HWTACACS服务器间需要路由可达。

相关资料

视频

配置AAA用户

 版权所有 © 华为技术有限公司

17 部署设备或网络安全

17.1 配置本机防攻击的综合示例
17.2 配置通过部署ASPF，使内网仅提供FTP服务的示例
17.3 配置通过基于ACL规则的包过滤，使内网用户无法访问所有外网的示例
17.4 如何限制外网用户访问WEB网管
17.5 配置通过部署DHCP Snooping，使用户与合法的DHCP服务器进行通信的示例

17.1 配置本机防攻击的综合示例

规格

适用于所有版本、所有形态路由器。

组网需求

如图17-1所示，位于不同局域网的用户通过RouterA与RouterB连接访问Internet。为分析RouterA受攻击情况，需要配置攻击溯源检查功能记录攻击源信息。管理员发现存在以下现象：

- 通过攻击溯源检查功能分析可知，Net1网段中的某个用户经常会发生攻击行为。
- 攻击者发送大量的ARP Request报文，影响CPU的正常工作。
- 管理员需要以FTP方式上传文件到RouterA，此时需要建立管理员主机与RouterA之间的数据连接。
- 大多数局域网用户通过DHCP方式动态获取IP地址，但RouterA不优先处理上送CPU的DHCP Client报文。

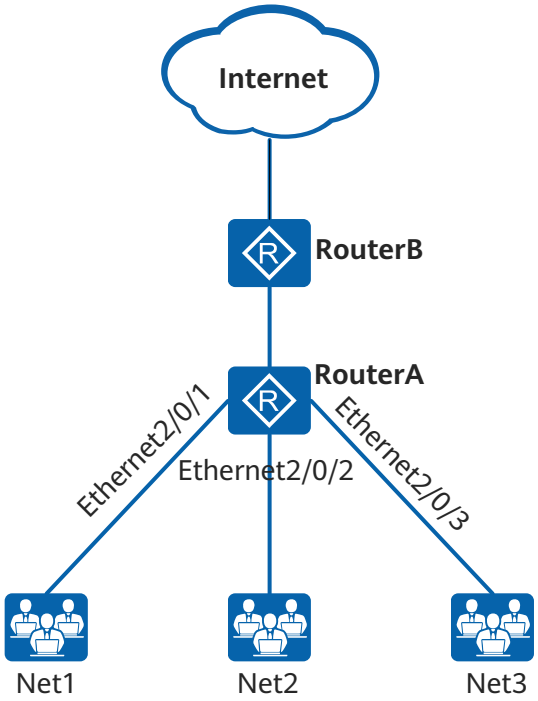
管理员希望通过在RouterA进行配置，以便解决上述问题，从而保证网络畅通。

说明

以下仅给出本机防攻击特性的配置步骤，关于路由的配置请参见相关手册。

 版权所有 © 华为技术有限公司

图 17-1 配置防攻击策略组网图



操作步骤

步骤1 Router上的配置

```
#
 sysname RouterA
#
acl number 4001 //配置本机防攻击黑名单引用的ACL
 rule 5 permit source-mac 00e0-fc01-0101
#
cpu-defend policy devicesafety //创建本机防攻击策略
 blacklist 1 acl 4001 //指定黑名单
 packet-type arp-request rate-limit 68 //限制上送CPU的ARP Request报文的速率为68pps
 packet-type dhcp-client priority 3  //配置上送CPU的dhcp-client的报文优先级为3
 application-apperceive packet-type ftp rate-limit 2000  //配置FTP报文动态链路保护功能的限制速率为
2000pps
 auto-defend enable  //使能攻击溯源功能
 auto-defend threshold 50  //配置攻击溯源检查阈值为50pps
#
 cpu-defend-policy devicesafety  //在主控板上应用防攻击策略
#
return
```

步骤2 验证配置结果

在RouterA上执行**display cpu-defend policy**命令，查看防攻击策略的配置信息。

在RouterA上执行**display cpu-defend configuration**命令，查看设备对协议报文限速的配置信息。

----结束

 版权所有 © 华为技术有限公司

17.2 配置通过部署 ASPF，使内网仅提供 FTP 服务的示例

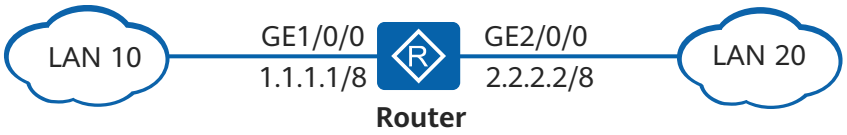
规格

适用于所有版本、所有形态的AR路由器。

组网需求

AR作为LAN10和LAN20的网关，要求除了LAN10访问LAN20中FTP服务器的流量，禁止任何LAN20到LAN10的流量。

图 17-2 配置 ASPF 防火墙功能组网图



操作步骤

步骤1 Router上的配置

```
#
firewall-nat session ftp aging-time 300 //配置FTP控制连接的超时时间为300秒
#
acl number 3102
 rule 5 deny ip //定义ACL3102拒绝所有流量
#
firewall zone trust
 priority 15 //设置安全区域trust的优先级为15
#
firewall zone untrust
 priority 1 //设置安全区域untrust的优先级为1
#
firewall interzone trust untrust //创建由安全区域trust和安全区域untrust构成的安全域
间
 firewall enable //使能安全域间的防火墙功能
 packet-filter 3102 inbound //在安全域间的入方向上根据ACL3102进行包过滤
 detect aspf ftp //在安全域间对FTP协议进行ASPF检测
#
interface GigabitEthernet1/0/0
 ip address 1.1.1.1 255.0.0.0
 zone trust //将接口加入到安全域trust中
#
interface GigabitEthernet2/0/0
 ip address 2.2.2.2 255.0.0.0
 zone untrust //将接口加入到安全域untrust中
#
```

步骤2 验证配置结果

在Router上执行**display firewall interzone**命令，查看安全域间的配置。

在Router上执行**display firewall zone**命令，查看安全区域的配置。

----结束

版权所有 © 华为技术有限公司

FAQ

- 安全域间的入方向是怎么定义的?

  入方向是指从优先级低的安全区域到优先级高的安全区域，出方向反之。本例中入方向是指从untrust区域到trust区域。

17.3 配置通过基于 ACL 规则的包过滤，使内网用户无法访问所有外网的示例

规格

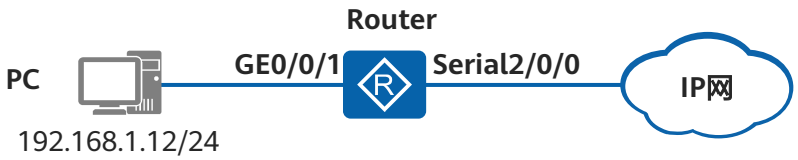
适用于所有版本、所有形态的路由器。

组网需求

在某企业网中，企业内用户通过Router接入IP网络，为了避免非法用户访问网络或者合法用户随意访问外网引发网络安全隐患，通过配置ACL过滤策略，对企业内的某些用户限制访问外网的所有Web界面。具体要求如下：

- 在Router的入方向接口拒绝指定用户访问IP网络。
- 在Router的入方向接口允许指定用户所在网段的其余用户访问IP网络。

图 17-3 配置通过基于 ACL 规则的包过滤，使内网用户无法访问所有外网的组网图



操作步骤

步骤1 Router上的配置

```
#
 dhcp enable //使能DHCP功能
#
acl number 2000 //配置ACL规则，允许源地址192.168.1.0/24网段的用户
 rule 5 permit source 192.168.1.0 0.0.0.255
#
acl number 3005 //定义用于报文过滤的访问控制的ACL
 description deny_souce_ip_www
 rule 5 deny tcp source 192.168.1.12 0 destination-port eq www
 rule 10 permit tcp source 192.168.1.12 0
#
ip pool pool1 //创建全局地址池
 gateway-list 192.168.1.2 //配置DHCP客户端的出口网关地址
 network 192.168.1.0 mask 255.255.255.0 //配置全局地址池可动态分配的IP地址范围
 dns-list 10.106.0.20 10.106.46.151 //配置DHCP客户端使用的DNS服务器的IP地址
#
interface Serial2/0/0
 link-protocol ppp
 ip address 219.143.125.234 255.255.255.252
 nat outbound 2000 //允许192.168.1.0/24网段的主机进行地址转换
```


版权所有 © 华为技术有限公司

```
#
interface GigabitEthernet0/0/1
 ip address 192.168.1.2 255.255.255.0
 traffic-filter inbound acl 3005 //在接口上应用ACL，进行报文过滤
 dhcp select global //配置接口工作在全局地址池模式
#
 ip route-static 0.0.0.0 0.0.0.0 Serial2/0/0 //配置缺省路由
#
```

步骤2 验证配置结果

在Router上执行**display traffic-filter statistics**命令，查看流量统计信息。

----结束

相关资料

视频：**配置基于时间的ACL**

17.4 如何限制外网用户访问 WEB 网管

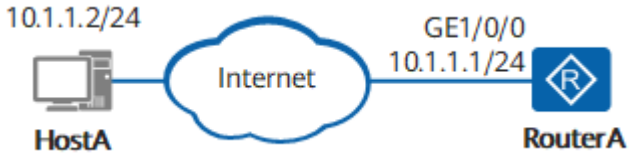
规格

适用于所有版本、所有形态的AR路由器。

组网需求

RouterA的GE1/0/0与用户侧主机HostA相连。要求允许10.1.1.0/24网段的主机访问WEB网管设备，并限制其他网段主机访问。

图 17-4 访问 WEB 网管组网图



操作步骤

步骤1 RouterA的配置

```
#
acl number 2000     //匹配可以访问WEB网管的主机地址
  rule 5 permit source 10.1.1.0 0.0.0.255
  rule 10 deny
#
aaa
 local-user huawei password cipher %@%@Dyb;#tOxsEBO@H@Jy'IX_:HK%@%@  //创建本地用户，用户名为huawei、密文密码为YsHsjx_202206
 local-user huawei service-type http  //配置本地用户huawei的接入类型为http
 local-user huawei privilege level 3  //配置本地用户huawei的优先级为3
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.1 255.255.255.0  //配置连接HostA接口的IP地址
#
```

 版权所有 © 华为技术有限公司

```
http acl 2000
http server permit interface GigabitEthernet1/0/0
http server enable
http secure-server enable
#
```

步骤2 验证配置结果

在HostA上可以访问WEB网管设备RouterA，其他网段的主机不可以访问RouterA。

----结束

配置注意事项

HostA访问WEB设备使用的用户名和密码要和RouterA的配置保持一致。

17.5 配置通过部署 DHCP Snooping，使用户与合法的 DHCP 服务器进行通信的示例

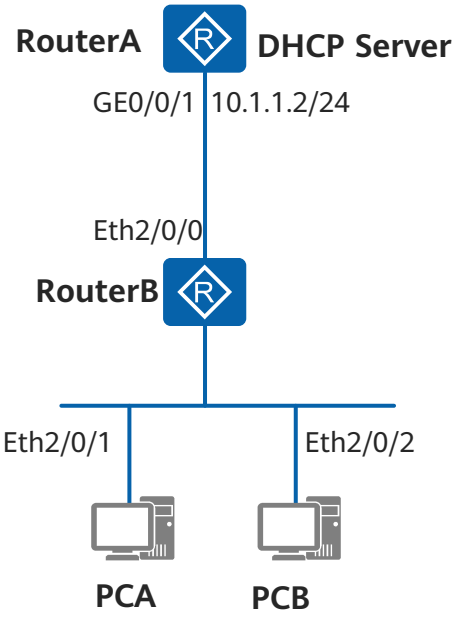
规格

适用于所有版本、所有形态的AR路由器。

组网需求

RouterB上的接口Eth2/0/0上使能dhcp snooping trusted，表示该接口所连接的DHCP服务器是受信的，其DHCP应答等消息会被正常转发，如果是从非受信端口收到的DHCP应答等消息会被丢弃。

图 17-5 配置 DHCP Snooping 功能组网图



版权所有 © 华为技术有限公司

操作步骤

步骤1 RouterA上的配置

```
#
 dhcp enable
#
ip pool pool1 //设置全局地址池
 gateway-list 10.1.1.2
 network 10.1.1.0 mask 255.255.255.0
#
interface GigabitEthernet0/0/1
 ip address 10.1.1.2 255.255.255.0
 dhcp select global
#
```

步骤2 RouterB上的配置

```
#
 dhcp enable //使能dhcp功能
 dhcp snooping enable //使能DHCP Snooping功能
#
interface Ethernet2/0/0
 dhcp snooping trusted //配置接口为“信任”状态
#
interface Ethernet2/0/1
 dhcp snooping enable
#
interface Ethernet2/0/2
 dhcp snooping enable
#
```

步骤3 验证配置结果

在RouterB上执行**display dhcp snooping global**命令，查看全局下DHCP Snooping相关信息。

在RouterB上执行**display dhcp snooping interface**命令，查看接口下DHCP Snooping的配置信息和丢弃报文的统计信息。

----结束

配置注意事项

无

 版权所有 © 华为技术有限公司

18 部署 QoS

18.1 配置流量整形综合示例
18.2 配置流量整形，对内网IP限速的示例
18.3 配置流量监管，对网段总流量限速的示例
18.4 配置流量监管，对网段的每个IP单独限速的示例
18.5 配置拥塞管理和拥塞避免的示例
18.6 配置禁止BT下载的示例
18.7 配置基于源MAC地址控制访问的示例
18.8 配置双出口实现内部互访和重定向的示例
18.9 配置队列模板实现拥塞管理和拥塞避免的示例
18.10 配置CBQ综合示例
18.11 带宽管理

18.1 配置流量整形综合示例

规格

适用于所有版本、所有形态的AR路由器。

组网需求

如**图18-1**所示，企业网内部LAN侧的语音、视频和数据业务通过Switch连接到RouterA的Eth2/0/0上，并通过RouterA的GE3/0/0连接到WAN侧网络。

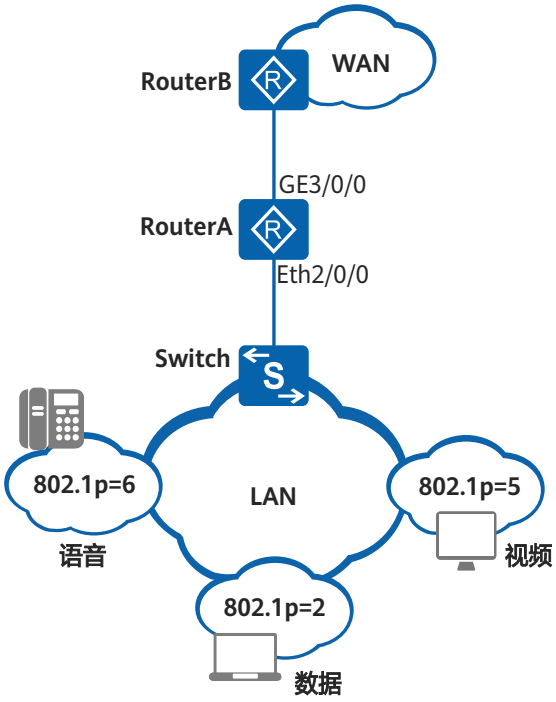
不同业务的报文在LAN侧使用802.1p优先级进行标识，在RouterA上根据报文的802.1p优先级入队列，当报文从GE3/0/0到达WAN侧时可能会发生带宽抖动。为了减少带宽抖动，同时保证各类业务带宽要求，现要求如下：

- 端口保证带宽为8000kbit/s，承诺突发尺寸为200000byte。
- 语音保证带宽为256kbit/s，承诺突发尺寸为6400byte。

 版权所有 © 华为技术有限公司

- 视频保证带宽为4000kbit/s，承诺突发尺寸为100000byte。
- 数据保证带宽为2000kbit/s，承诺突发尺寸为50000byte。

图 18-1 配置流量整形的组网图



操作步骤

步骤1 RouterA的配置

```
#
 sysname RouterA
#
vlan batch 10
#
qos queue-profile qp1  //创建队列模板qp1
  queue 2 gts cir 2000 cbs 50000  //配置队列2的承诺信息速率为2000kbit/s，承诺突发尺寸为50000byte
  queue 5 gts cir 4000 cbs 100000  //配置队列5的承诺信息速率为4000kbit/s，承诺突发尺寸为100000byte
  queue 6 gts cir 256 cbs 6400  //配置队列6的承诺信息速率为256kbit/s，承诺突发尺寸为6400byte
  schedule wfq 0 to 5 pq 6 to 7  //配置队列0～5的调度方式为WFQ（加权公平调度模式），队列6～7的调度方式为PQ（严格优先级调度模式）
#
interface Vlanif10
 ip address 192.168.1.1 255.255.255.0
#
interface Ethernet2/0/0
 port link-type trunk  //配置接口的链路类型为Trunk
 port trunk allow-pass vlan 10  //配置Trunk类型接口加入vlan 10
 trust 8021p  //配置接口信任报文的802.1p优先级
#
interface GigabitEthernet3/0/0
 ip address 192.168.4.1 255.255.255.0
 qos queue-profile qp1      //在接口上应用队列模板qp1
 qos gts cir 8000 cbs 200000  //配置接口承诺信息速率为8000kbit/s，承诺突发尺寸为200000byte
#
```


版权所有 © 华为技术有限公司

步骤2 验证配置结果

执行**display qos queue statistics interface gigabitethernet 3/0/0**命令查看接口GE3/0/0下各队列的统计信息，可以看到队列的输出速率被限制在规定范围内，队列满后，无法缓存的报文被丢弃。

----结束

配置注意事项

- 请配置Switch与RouterA对接的接口为Trunk类型接口，并加入相应的VLAN。
- 根据实际情况配置RouterB，确保RouterB与RouterA间路由可达。
- 接口整形的*cir-value*必须大于或等于接口上所有队列整形的*cir-value*之和；否则可能会造成某些高优先级队列得不到及时调度。

18.2 配置流量整形，对内网 IP 限速的示例

规格

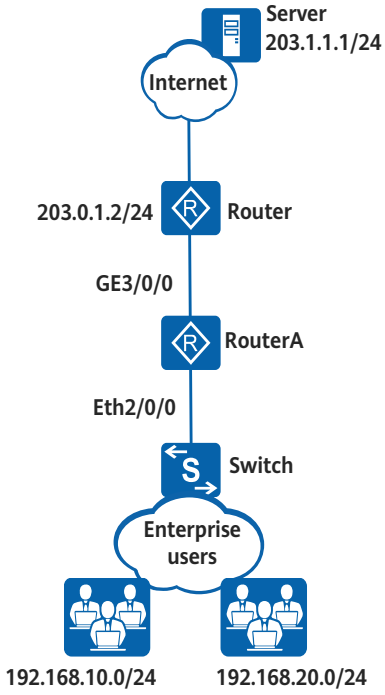
适用于所有版本、所有形态的AR路由器。

组网需求

企业网络中，总部与分支机构通过ISP网络使用专线相连。分支机构想要访问服务器必须通过总部。如果所有分支机构同时访问服务器，可能导致访问服务器的流量产生拥塞，从而被丢弃。为了防止流量的丢失，可以在企业分支机构的流量进入企业总部之前配置流量整形。如图18-2所示，针对内网用户192.168.10.0/24对服务器203.1.1.1/24的访问，要求控制速率在64kbit/s。

 版权所有 © 华为技术有限公司

图 18-2 配置基于内网 IP 进行限速的组网图



操作步骤

步骤1 RouterA的配置

```
#
 sysname RouterA
#
vlan batch 10 20
#
acl number 3001  //配置编号为3001的编号型访问控制列表
 rule 5 permit ip source 192.168.10.0 0.0.0.255  //配置规则5，允许源地址为192.168.10.0网段的报文通过
 rule 10 permit ip source 192.168.20.0 0.0.0.255  //配置规则10，允许源地址为192.168.20.0网段的报文通过
acl number 3002  //配置编号为3002的编号型访问控制列表
 rule 5 permit ip source 192.168.10.0 0.0.0.255  //配置规则5，允许源地址为192.168.10.0网段的报文通过
#
qos queue-profile limit  //创建队列模板limit
  queue 3 gts cir 64 cbs 1600  //配置队列3的承诺信息速率为64kbit/s
#
traffic classifier c1 operator or
 if-match acl 3002  //配置流分类c1：匹配规则为ACL 3002
#
traffic behavior b1
 remark local-precedence af3  //配置流行为b1：对匹配流分类的报文重标记本地优先级为AF3，不指定流行为为permit或deny时，默认为permit。
#
traffic policy p1
 classifier c1 behavior b1 precedence 5 //配置流策略p1:绑定流分类c1与流行为b1
#
interface Vlanif10
 ip address 192.168.10.1 255.255.255.0
#
interface Vlanif20
 ip address 192.168.20.1 255.255.255.0
#
interface Ethernet2/0/0
```


版权所有 © 华为技术有限公司

```
 port link-type trunk  //配置接口的链路类型为Trunk
 port trunk allow-pass vlan 10 20  //配置Trunk类型接口加入vlan 10和vlan 20
 traffic-policy p1 inbound  //在接口入方向上应用流策略p1
#
interface GigabitEthernet3/0/0
 ip address 203.0.1.1 255.255.255.0
 qos queue-profile limit  //在接口上应用队列模板limit
 nat outbound 3001  //在接口上对匹配ACL 3001的报文做NAT
#
ip route-static 0.0.0.0 0.0.0.0 203.0.1.2
#
return
```

步骤2 验证配置结果

执行**display qos queue statistics interface gigabitethernet 3/0/0**命令检查GE3/0/0接口上应用了队列模板limit后的报文统计信息，可以看到接口3号队列的输出速率被限制在规定范围内，队列满后，无法缓存的报文被丢弃。

----结束

配置注意事项

- 请配置Switch与不同的网段用户对接的接口为Access类型接口，并将其加入对应VLAN。
- 请配置Switch与RouterA对接的接口为Trunk类型接口，并加入对应VLAN。

相关资料

视频：配置基于接口的限速

18.3 配置流量监管，对网段总流量限速的示例

规格

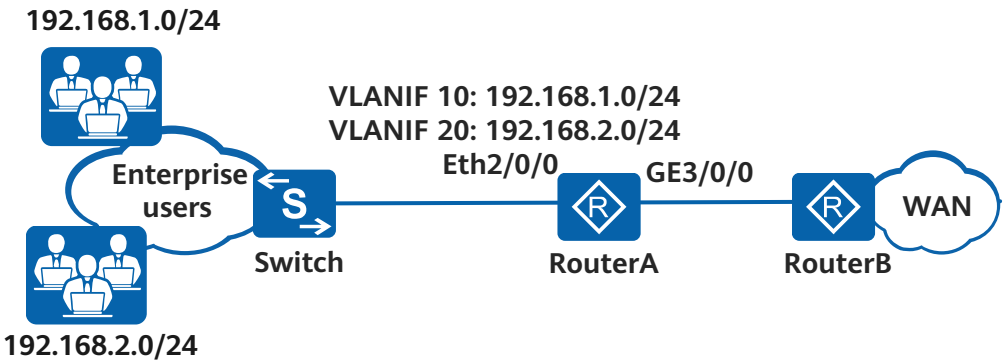
适用于所有版本、所有形态的AR路由器。

组网需求

RouterA部署在企业网的出口处，企业用户通过2个不同的网段连接到RouterA从而访问互联网。现要求对192.168.1.0/24网段访问互联网的**总流量**限制为512kbit/s，对192.168.2.0/24网段访问互联网的**总流量**限制为128kbit/s。

 版权所有 © 华为技术有限公司

图 18-3 配置流量监管的组网图



操作步骤

步骤1 RouterA的配置

```
#
 sysname RouterA
#
vlan batch 10 20
#
acl number 2000  //配置编号为2000的编号型访问控制列表
 rule 0 permit source 192.168.1.0 0.0.0.255  //配置规则0，允许源地址为192.168.1.0网段的报文通过
acl number 2001  //配置编号为2001的编号型访问控制列表
 rule 0 permit source 192.168.2.0 0.0.0.255  //配置规则0，允许源地址为192.168.2.0网段的报文通过
#
interface Vlanif10
 ip address 192.168.1.1 255.255.255.0
#
interface Vlanif20
 ip address 192.168.2.1 255.255.255.0
#
interface Ethernet2/0/0
 port link-type trunk  //配置接口的链路类型为Trunk
 port trunk allow-pass vlan 10 20  //配置Trunk类型接口加入vlan 10和vlan 20
#
interface GigabitEthernet3/0/0
 ip address 1.1.1.1 255.255.255.0
 qos car outbound acl 2000 cir 512 cbs 96256 pbs 160256 green pass yellow pass red discard
 //配置在接口出方向对符合ACL 2000规则的报文做流量监管，指定承诺信息速率为512kbit/s
 qos car outbound acl 2001 cir 128 cbs 24064 pbs 40064 green pass yellow pass red discard
 //配置在接口出方向对符合ACL 2001规则的报文做流量监管，指定承诺信息速率为128kbit/s
#
```

步骤2 验证配置结果

执行**display qos car statistics interface GigabitEthernet 3/0/0 outbound**命令检查GE3/0/0接口上应用了流量监管后的报文统计信息，可以看到接口的输出速率被限制在规定范围内，超出部分流量被丢弃。

----结束

版权所有 © 华为技术有限公司

配置注意事项

- 请配置Switch与不同的网段用户对接的接口为Access类型接口，并将其加入对应VLAN。
- 请配置Switch与RouterA对接的接口为Trunk类型接口，并加入对应VLAN。
- 根据实际情况配置RouterB，确保RouterB与RouterA间路由可达。
- 在本例中的案例是在路由器上行接入WAN的接口的出方向上配置流量监管，也可以根据需要在路由器下行接入LAN接口的入方向配置流量监管。

相关资料

视频：配置基于某网段的限速

18.4 配置流量监管，对网段的每个 IP 单独限速的示例

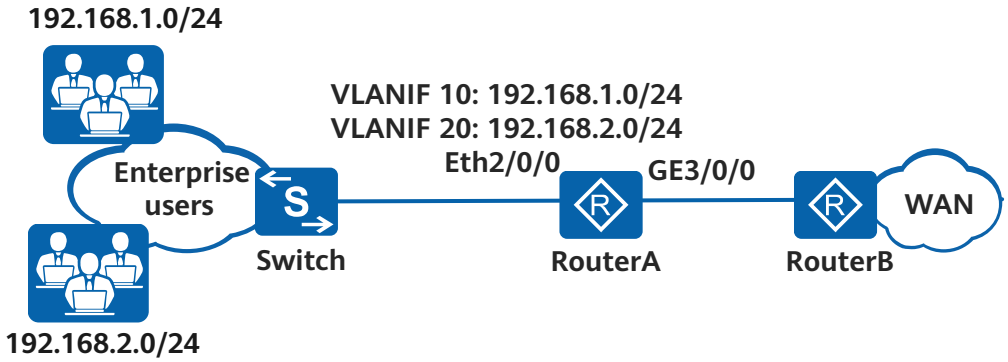
规格

适用于所有版本、所有形态的AR路由器。

组网需求

RouterA部署在企业网的出口处，企业用户通过2个不同的网段连接到RouterA从而访问互联网。现要求对192.168.1.0/24网段**每个IP地址**访问互联网流量限制为64kbit/s，对192.168.2.0/24网段**每个IP地址**访问互联网流量限制为128kbit/s。

图 18-4 配置流量监管的组网图



操作步骤

步骤1 RouterA的配置

```
#
 sysname RouterA
#
vlan batch 10 20
#
```

 版权所有 © 华为技术有限公司

```
interface Vlanif10
 ip address 192.168.1.1 255.255.255.0
 qos car inbound source-ip-address range 192.168.1.2 to 192.168.1.254 per-address cir 64 cbs 12032 pbs 20032 green pass yellow pass red discard
 //配置在接口入方向对源地址为192.168.1.2到192.168.1.254范围内的报文做流量监管，指定各IP地址发送报文的承诺信息速率为64kbit/s
#
interface Vlanif20
 ip address 192.168.2.1 255.255.255.0
 qos car inbound source-ip-address range 192.168.2.2 to 192.168.2.254 per-address cir 128 cbs 24064 pbs 40064 green pass yellow pass red discard
 //配置在接口入方向对源地址为192.168.2.2到192.168.2.254范围内的报文做流量监管，指定各IP地址发送报文承诺信息速率为128kbit/s
#
interface Ethernet2/0/0
 port link-type trunk  //配置接口的链路类型为Trunk
 port trunk allow-pass vlan 10 20  //配置Trunk类型接口加入VLAN 10和VLAN 20
#
interface GigabitEthernet3/0/0
 ip address 1.1.1.1 255.255.255.0
#
```

步骤2 验证配置结果

执行**display qos car statistics interface Vlanif 10 inbound**和**display qos car statistics interface Vlanif 20 inbound**命令检查接口上应用了流量监管后的报文统计信息，可以看到接口的输出速率被限制在规定范围内，超出部分流量被丢弃。

----结束

配置注意事项

- 请配置Switch与不同的网段用户对接的接口为Access类型接口，并将其加入对应VLAN。
- 请配置Switch与RouterA对接的接口为Trunk类型接口，并加入对应VLAN。
- 根据实际情况配置RouterB，确保RouterB与RouterA间路由可达。
- 若在**qos car**命令中不配置**per-address**参数，则对源IP在指定范围内的所有报文聚合起来做流量监管，即对该地址段发送报文的总流量做流量监管。

相关资料

视频：配置基于IP地址的限速

18.5 配置拥塞管理和拥塞避免的示例

规格

适用于所有版本、所有形态的AR路由器(以8个队列的接口举例)。

组网需求

如图18-5所示，企业网内部LAN侧的语音、视频和数据业务通过SwitchA和SwitchB连接到RouterA的Eth2/0/0和Eth2/0/1上，并通过RouterA的GE3/0/0接口连接到WAN侧网络。

各类报文被SwitchA和SwitchB打上不同的DSCP优先级，语音、视频和数据分别为ef（46）、af43（38）、af32（28）和af31（26），在RouterA上根据报文的DSCP优先

 版权所有 © 华为技术有限公司

级入队列，由于上行服务商提供的带宽有限，在接口GE3/0/0出方向处可能会发生拥塞。为了减轻网络拥塞造成的影响，保证用户对于高优先级、低延迟业务的服务要求，配置需求如下表所述：

表 18-1 拥塞避免配置参数

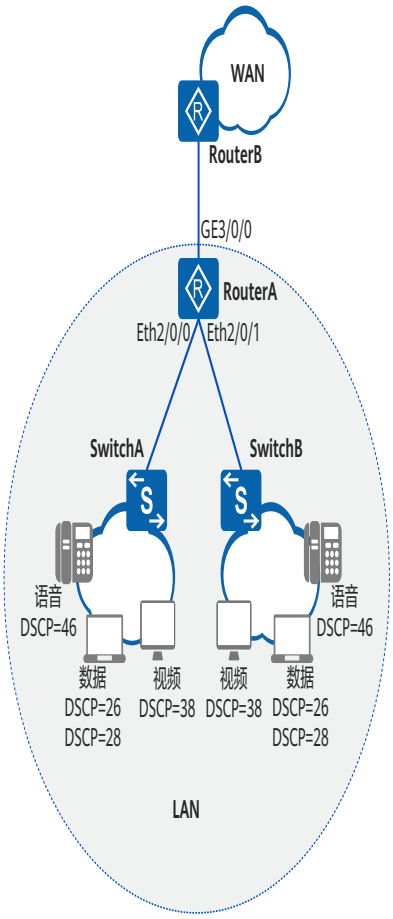
业务类型	DSCP优先级	队列索引	调度方式	丢弃方式
语音	46	5	PQ	尾丢弃
视频	38	4	WFQ	WRED： • 阈值下限(%)：60 • 阈值上限(%)：80 • 丢弃概率(%)：20

 版权所有 © 华为技术有限公司

业务类型	DSCP优先级	队列索引	调度方式	丢弃方式
数据	28 26	3	WFQ	WRED： ● DSCP=28 – 阈值下限(%)：50 – 阈值上限(%)：70 – 丢弃概率(%)：30 ● DSCP=26 – 阈值下限(%)：40 – 阈值上限(%)：60 – 丢弃概率(%)：40

版权所有 © 华为技术有限公司

图 18-5 配置拥塞避免和拥塞管理的组网图



操作步骤

步骤1 RouterA的配置

```
#
 sysname RouterA
#
vlan batch 20 30
#
drop-profile data  //创建WRED丢弃模板data
wred dscp  //配置当前WRED丢弃模板基于DSCP优先级进行丢弃
  dscp af31 low-limit 40 high-limit 60 discard-percentage 40  //配置对DSCP优先级为26的报文的丢弃下限为40%，丢弃上限为60%，最大丢弃概率为40%
  dscp af32 low-limit 50 high-limit 70 discard-percentage 30  //配置对DSCP优先级为28的报文的丢弃下限为50%，丢弃上限为70%，最大丢弃概率为30%
#
drop-profile video  //创建WRED丢弃模板video
wred dscp  //配置当前WRED丢弃模板基于DSCP优先级进行丢弃
  dscp af43 low-limit 60 high-limit 80 discard-percentage 20  //配置对DSCP优先级为38的报文的丢弃下限为60%，丢弃上限为80%，最大丢弃概率为20%
#
qos queue-profile queue-profile1  //创建队列模板queue-profile1
  schedule wfq 3 to 4 pq 5  //配置队列3～4的调度模式为wfq，队列5的调度模式为pq
  queue 3 drop-profile data  //配置队列3绑定名称为data的丢弃模板
  queue 4 drop-profile video  //配置队列4绑定名称为video的丢弃模板
```


版权所有 © 华为技术有限公司

```
#
interface Vlanif20
 ip address 192.168.2.1 255.255.255.0
#
interface Vlanif30
 ip address 192.168.3.1 255.255.255.0
#
interface Ethernet2/0/0
 port link-type trunk
 port trunk allow-pass vlan 20
 trust dscp  //配置接口信任报文的dscp优先级
#
interface Ethernet2/0/1
 port link-type trunk
 port trunk allow-pass vlan 30
 trust dscp  //配置接口信任报文的dscp优先级
#
interface GigabitEthernet3/0/0
 ip address 192.168.4.1 255.255.255.0
 qos queue-profile queue-profile1  //在接口下应用队列模板queue-profile1
#
```

步骤2 验证配置结果

执行**display qos queue statistics interface gigabitethernet 3/0/0**命令查看接口GE3/0/0下各队列的统计信息，执行**display qos queue statistics interface gigabitethernet 3/0/0 queue 3**命令查看接口GE3/0/0下队列3的统计信息，可以看到不同DSCP优先级报文通过和丢弃的统计信息。

----结束

配置注意事项

- 请配置SwitchA、SwitchB与RouterA对接的接口为Trunk类型接口，并加入对应VLAN。
- 请配置RouterB，确保RouterB与RouterA间路由可达。
- 使用队列模板时，通过**trust**命令指定对报文按照其自身携带的某类优先级进行优先级映射，并根据映射后的本地优先级值进入不同的队列。若不配置此命令报文按照端口优先级入队列。
- 使用CBQ时，设备根据IP优先级或者DSCP优先级、输入接口、IP报文的五元组等规则来对报文进行分类，然后让匹配流分类规则的报文进入对应的EF、AF队列。对于不匹配任何类别的报文，送入系统定义的缺省类，并按照按流的“会话”信息进入BE队列。
- AR路由器不同接口支持不同的调度模式：

表 18-2 各接口支持的调度模式

接口	调度模式
LAN接口	• PQ • DRR • WRR • PQ+DRR • PQ+WRR

 版权所有 © 华为技术有限公司

接口	调度模式
WAN接口	• PQ • WFQ • PQ+WFQ

18.6 配置禁止 BT 下载的示例

规格

适用于所有版本、所有形态的AR路由器。

说明

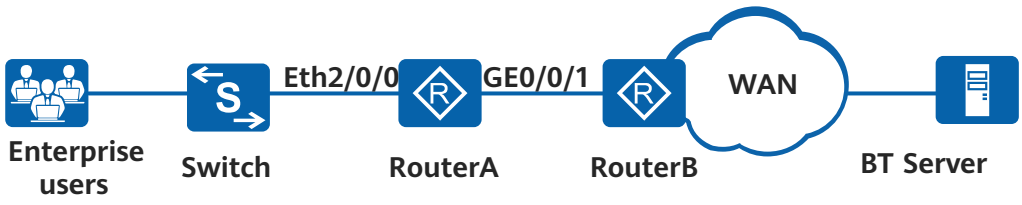
SAC功能使用License授权，缺省情况下，设备的SAC功能受限无法使用。如果需要使用SAC功能，请根据设备款型联系华为办事处申请并购买License。

组网需求

如图18-6所示，企业内用户通过交换机连接到RouterA的Eth2/0/0，并通过RouterA的GE0/0/1接口连接到WAN侧网络。

现在要求在RouterA上通过配置基于智能应用控制SAC（Smart Application Control）的流分类，禁止企业用户进行BT下载。

图 18-6 配置禁止 BT 下载的组网图



操作步骤

步骤1 RouterA的配置

```
#
 sysname RouterA
#
vlan batch 20
#
engine enable  //开启深度安全防御功能
#
update restore sdb-default sa-sdb  //将特征库恢复到出厂默认版本
#
traffic classifier c1 operator or  //创建流分类c1
 if-match application BT  //匹配BT应用协议
#
traffic behavior b1  //创建流行为b1
 deny  //禁止匹配指定规则的报文流通过
```


版权所有 © 华为技术有限公司

```
#
traffic policy p1  //创建流策略p1
 classifier c1 behavior b1 precedence 5 //将流分类和对应的流行为进行绑定
#
interface Vlanif20
 ip address 192.168.2.1 255.255.255.0
 sa application-statistic enable  //使能接口基于SA的统计功能
 traffic-policy p1 inbound  //将流策略p1应用到接口入方向
#
interface Ethernet2/0/0
 port link-type trunk  //配置接口的链路类型为Trunk
 port trunk allow-pass vlan 20  //配置Trunk类型接口加入vlan 20
#
interface GigabitEthernet0/0/1
 ip address 192.168.4.1 255.255.255.0
 sa application-statistic enable  //使能接口基于SA的统计功能
 traffic-policy p1 inbound  //将流策略p1应用到接口入方向
#
```

步骤2 验证配置结果

执行**display sa application-statistic**命令检查Eth2/0/0和GE0/0/1接口上查看基于不同SA应用协议的报文统计信息。

----结束

配置注意事项

- 请配置Switch与RouterA对接的接口为Trunk类型接口，并加入对应VLAN。
- 请配置RouterB，确保RouterB与RouterA间路由可达。
- 指定特征库名称时，一般要求用户输入完整的路径和名称，防止恢复配置时出错。

18.7 配置基于源 MAC 地址控制访问的示例

规格

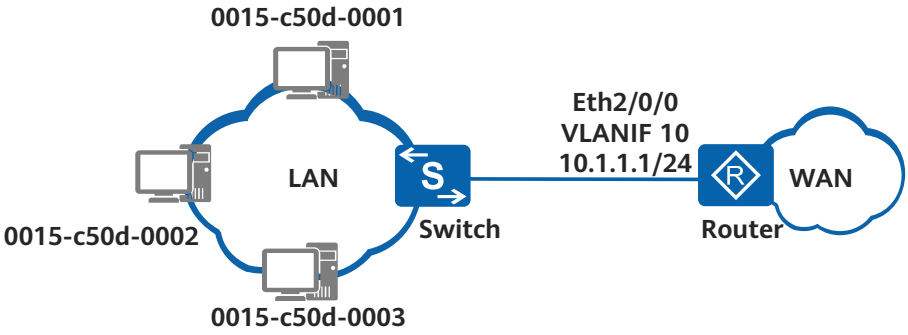
适用于所有版本、所有形态的AR路由器。

组网需求

如图18-7所示，Router为企业网关，企业内用户通过Router访问互联网。现要求限制局域网内某些主机访问互联网，但是由于这些主机可以变换IP地址，所以通过防火墙限制不能有效防范，最合适的做法是基于源MAC地址进行限制。在本例中可以实现限制某些主机访问互联网，但是可以访问网关。

 版权所有 © 华为技术有限公司

图 18-7 配置组网图



操作步骤

步骤1 Router的配置

```
#
 sysname Router
#
vlan batch 10
#
acl number 3001  //配置编号为3001的编号型访问控制列表
 rule 1 permit ip destination 10.1.1.0 0.0.0.255  //配置规则1，指定匹配目的地址为10.1.1.1/24（即网关地址）
#
traffic classifier gate operator and
 if-match acl 3001  //配置流分类gate，指定匹配ACL 3001
traffic classifier mac1 operator and
 if-match source-mac 0015-c50d-0001  //配置流分类mac1，指定匹配源地址为0015-c50d-0001
traffic classifier mac2 operator and
 if-match source-mac 0015-c50d-0002  //配置流分类mac2，指定匹配源地址为0015-c50d-0002
traffic classifier mac3 operator and
 if-match source-mac 0015-c50d-0003  //配置流分类mac3，指定匹配源地址为0015-c50d-0003
#
traffic behavior p1
 permit  //配置流行为p1为允许通过
traffic behavior d1
 deny  //配置流行为d1为拒绝并丢弃
#
traffic policy myqos  //配置流策略myqos
 classifier gate behavior p1 precedence 5 //绑定流分类gate与流行为p1
 classifier mac1 behavior d1 precedence 10 //绑定流分类mac1与流行为d1
 classifier mac2 behavior d1 precedence 15 //绑定流分类mac2与流行为d1
 classifier mac3 behavior d1 precedence 20 //绑定流分类mac3与流行为d1
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
 traffic-policy myqos inbound  //在接口入方向应用流策略myqos
#
interface Ethernet2/0/0
 port link-type trunk  //配置接口的链路类型为Trunk
 port trunk allow-pass vlan 10  //配置Trunk类型接口加入vlan 10
#
```

步骤2 验证配置结果

执行**display traffic policy user-defined** 命令查看配置的流策略信息。

版权所有 © 华为技术有限公司

在被限制的主机上可以成功Ping通网关地址，但不能Ping通非LAN内的IP地址。

----结束

配置注意事项

- 请配置Switch与Router对接的接口为Trunk类型接口，并加入VLAN10。
- 由于在接口下应用流策略后，报文依次匹配流策略中的流分类，所以在配置流策略**myqos**时，必须先配置允许访问网关的流分类和流行为，再配置禁止访问互联网的流分类和流行为。

相关资料

视频：**通过配置MAC地址过滤，限制指定用户上网**

18.8 配置双出口实现内部互访和重定向的示例

规格

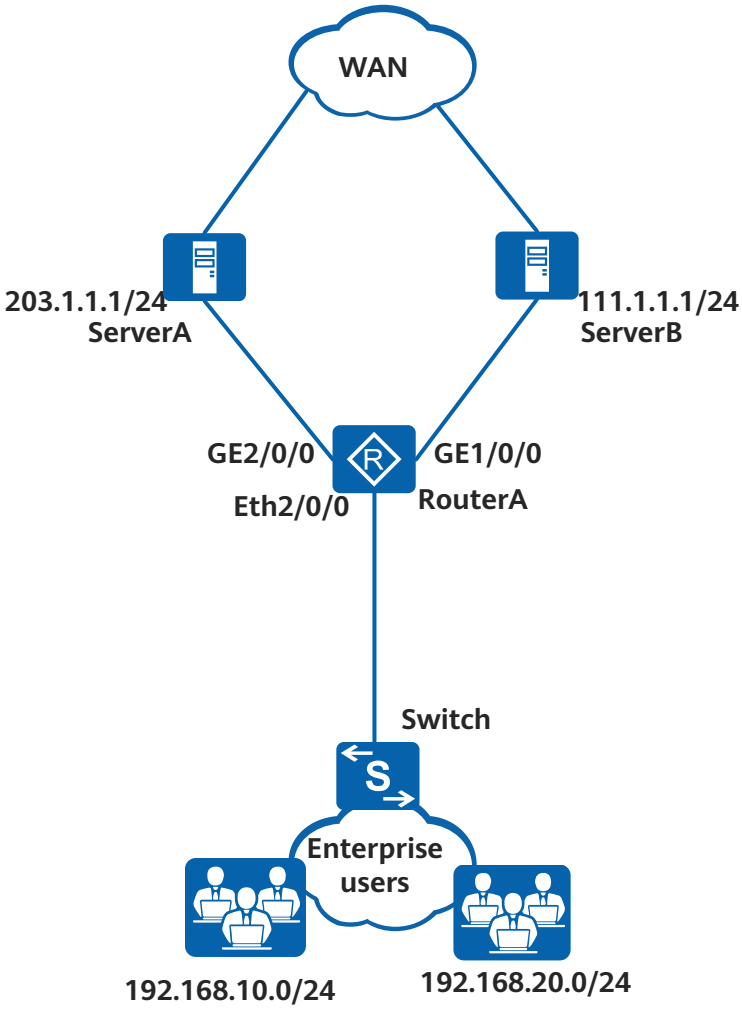
适用于所有版本、所有形态的AR路由器。

组网需求

RouterA部署在企业网的出口处，企业网中有2个不同的网段连接到RouterA从而访问两台服务器ServerA（203.1.1.1/24）和ServerB（111.1.1.1/24）。现要求将来自192.168.10.0/24用户组的数据流强制通过ServerB访问WAN，并实现企业网内用户组192.168.10.0/24与192.168.20.0/24的互访。

 版权所有 © 华为技术有限公司

图 18-8 双出口实现内部互访及重定向的组网图



操作步骤

步骤1 RouterA的配置

```
#
 sysname RouterA
#
vlan batch 10 20
#
acl number 3001  //配置编号为3001的编号型访问控制列表
 rule 5 permit ip source 192.168.10.0 0.0.0.255  //配置规则5，允许源地址为192.168.10.0网段的报文通过
 rule 10 permit ip source 192.168.20.0 0.0.0.255  //配置规则10，允许源地址为192.168.20.0网段的报文通过
acl number 3002  //配置编号为3002的编号型访问控制列表
 rule 5 permit ip source 192.168.10.0 0.0.0.255 destination 192.168.20.0 0.0.0.255  //配置规则5，允许源地址为192.168.10.0网段且目的地址为192.168.20.0网段的报文通过
 rule 10 permit ip source 192.168.10.0 0.0.0.255 destination 192.168.10.0 0.0.0.255  //配置规则10，允许源/目的地址均为192.168.10.0网段的报文通过
acl number 3003  //配置编号为3003的编号型访问控制列表
 rule 5 permit ip source 192.168.10.0 0.0.0.255  //配置规则5，允许源地址为192.168.10.0网段的报文通过
#
traffic classifier c2 operator or
```


版权所有 © 华为技术有限公司

```
 if-match acl 3003  //配置流分类c2：匹配规则为ACL 3003
traffic classifier c1 operator or
 if-match acl 3002  //配置流分类c1：匹配规则为ACL 3002
#
traffic behavior b2
 redirect ip-nexthop 111.1.1.1  //配置流行为b2：对匹配流分类的报文重定向到111.1.1.1，实现重定向
traffic behavior b1  //配置流行为b1：默认为允许通过，实现部门内互访
#
traffic policy pp
 classifier c1 behavior b1 precedence 5
 classifier c2 behavior b2 precedence 10 //配置流策略pp：绑定流分类c1与流行为b1，流分类c2与流行为b2
#
interface Vlanif10
 ip address 192.168.10.1 255.255.255.0
#
interface Vlanif20
 ip address 192.168.20.1 255.255.255.0
#
interface Ethernet2/0/0
 port link-type trunk  //配置接口的链路类型为Trunk
 port trunk allow-pass vlan 10 20  //配置Trunk类型接口加入vlan 10和vlan 20
 traffic-policy pp inbound  //在接口入方向上应用流策略pp
#
interface GigabitEthernet2/0/0
 ip address 203.1.1.2 255.255.255.0
 nat outbound 3001  //在接口上对匹配ACL 3001的报文做NAT
#
interface GigabitEthernet1/0/0
 ip address 111.1.1.2 255.255.255.0
 nat outbound 3001  //在接口上对匹配ACL 3001的报文做NAT
#
ip route-static 0.0.0.0 0.0.0.0 203.1.1.1
#
```

步骤2 验证配置结果

执行**display traffic policy user-defined**命令查看配置的流策略信息，执行**display traffic-policy applied-record**命令查看流策略是否应用成功。

企业内192.168.10.0/24网段的用户组之间可以互访并且可以与192.168.20.0/24的用户组互访。

----结束

配置注意事项

- 请配置Switch与不同的网段用户对接的接口为Access类型接口，并将其加入对应VLAN。
- 请配置Switch与RouterA对接的接口为Trunk类型接口，并加入对应VLAN。
- 由于在接口下应用流策略后，报文依次匹配流策略中的流分类，所以在配置流策略pp时，必须先配置内部互访的流分类与流行为，再配置重定向的流分类和流行为。

相关资料

视频：

- **配置双出口的重定向**
- **配置通过ACL禁止两个网段互访**

 版权所有 © 华为技术有限公司

18.9 配置队列模板实现拥塞管理和拥塞避免的示例

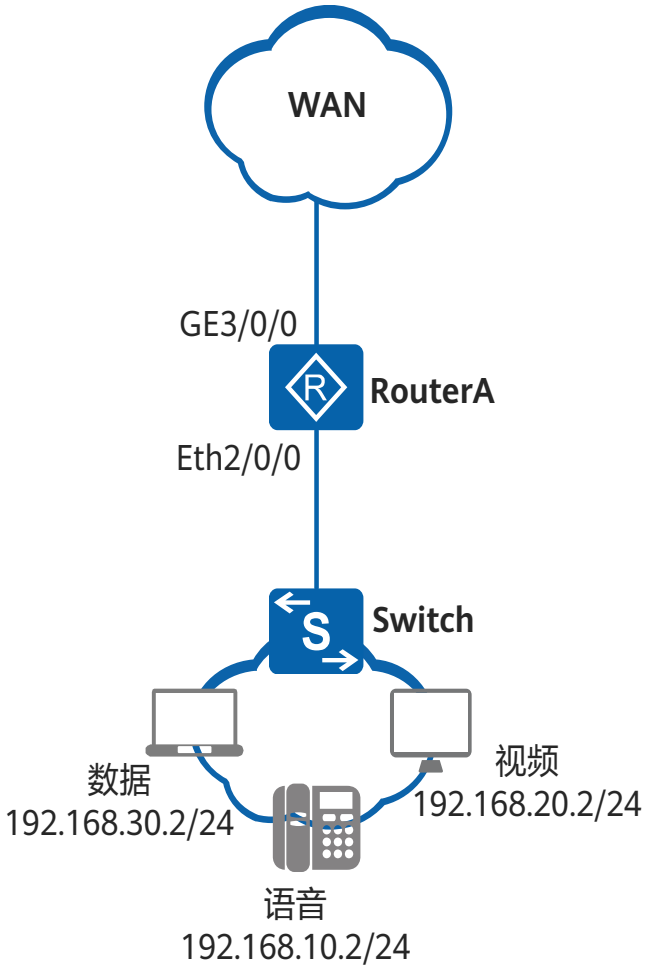
规格

适用于所有版本、所有形态的AR路由器。

组网需求

企业网内部的语音、视频和数据业务通过Switch连接到RouterA的Eth2/0/0上，并通过RouterA的GE3/0/0接口连接到WAN侧网络。各类报文以源IP地址进行区分，语音报文来自192.168.10.2/24，视频报文来自192.168.20.2/24，数据报文来自192.168.30.2/24，现在用户希望对三类报文分别进行带宽限制，语音报文占接口实际可用带宽的50%，视频报文占接口实际可用带宽的40%，数据报文占接口实际可用带宽的5%。

图 18-9 配置队列实现拥塞避免与拥塞管理的组网图



版权所有 © 华为技术有限公司

操作步骤

步骤1 RouterA的配置

```
#
 sysname RouterA
#
vlan batch 10 20 30
#
acl number 3001  //配置编号3001的编号型访问控制列表
 rule 5 permit ip source 192.168.10.0 0.0.0.255  //配置规则5，允许源地址为192.168.10.0网段的报文通过
 rule 10 permit ip source 192.168.20.0 0.0.0.255 //配置规则10，允许源地址为192.168.20.0网段的报文通过
 rule 15 permit ip source 192.168.30.0 0.0.0.255 //配置规则15，允许源地址为192.168.30.0网段的报文通过
acl number 3002  //配置编号3002的编号型访问控制列表
 rule 5 permit ip source 192.168.10.0 0.0.0.255  //配置规则5，允许源地址为192.168.10.0网段的报文通过
acl number 3003  //配置编号3003的编号型访问控制列表
 rule 5 permit ip source 192.168.20.0 0.0.0.255  //配置规则5，允许源地址为192.168.20.0网段的报文通过
acl number 3004  //配置编号3004的编号型访问控制列表
 rule 5 permit ip source 192.168.30.0 0.0.0.255  //配置规则5，允许源地址为192.168.30.0网段的报文通过
#
traffic classifier c3 operator or
 if-match acl 3004  //配置流分类c3：匹配规则为ACL 3004
traffic classifier c2 operator or
 if-match acl 3003  //配置流分类c2：匹配规则为ACL 3003
traffic classifier c1 operator or
 if-match acl 3002  //配置流分类c1：匹配规则为ACL 3002
traffic classifier data operator or
 if-match dscp af31  //配置流分类data：匹配规则为DSCP值为AF31
traffic classifier video operator or
 if-match dscp af41  //配置流分类video：匹配规则为DSCP值为AF41
traffic classifier voice operator or
 if-match dscp ef  //配置流分类voice：匹配规则为DSCP值为EF
#
traffic behavior b3
 remark dscp af31  //配置流行为b3：对匹配流分类的报文重标记DSCP为AF31
traffic behavior b2
 remark dscp af41  //配置流行为b2：对匹配流分类的报文重标记DSCP为AF41
traffic behavior b1
 remark dscp ef  //配置流行为b1：对匹配流分类的报文重标记DSCP为EF
traffic behavior data
 queue af bandwidth pct 5  //配置流行为data：对匹配流分类的报文配置确保转发并配置可确保的最小带宽占接口实际可用带宽的5%
traffic behavior video
 queue af bandwidth pct 40  //配置流行为video：对匹配流分类的报文配置确保转发并配置可确保的最小带宽占接口实际可用带宽的40%
traffic behavior voice
 queue ef bandwidth pct 50  //配置流行为voice：对匹配流分类的报文配置确保转发并配置可确保的最小带宽占接口实际可用带宽的50%
#
traffic policy schedule
 classifier data behavior data precedence 5
 classifier video behavior video precedence 10
 classifier voice behavior voice precedence 15 //配置流策略schedule:绑定流分类data与流行为data，流分类video与流行为video，流分类voice与流行为voice
traffic policy p1
 classifier c1 behavior b1 precedence 5
 classifier c2 behavior b2 precedence 10
 classifier c3 behavior b3 precedence 15 //配置流策略p1:绑定流分类c1与流行为b1，流分类c2与流行为b2，流分类c3与流行为b3
#
interface Vlanif10
 ip address 192.168.10.1 255.255.255.0
#
interface Vlanif20
 ip address 192.168.20.1 255.255.255.0
#
interface Vlanif30
 ip address 192.168.30.1 255.255.255.0
#
interface Ethernet2/0/0
```

 版权所有 © 华为技术有限公司

```
 port link-type trunk
 port trunk allow-pass vlan 10 20 30
 traffic-policy p1 inbound  //在接口入方向上应用流策略p1
#
interface GigabitEthernet3/0/0
 ip address 222.1.1.2 255.255.255.0
 traffic-policy schedule outbound  //在接口出方向上应用流策略schedule
 nat outbound 3001  //在接口上对匹配ACL 3001的报文做NAT
#
ip route-static 0.0.0.0 0.0.0.0 222.1.1.1
#
```

步骤2 验证配置结果

执行**display traffic policy user-defined**命令查看配置的流策略信息，执行**display traffic-policy applied-record**命令查看流策略是否应用成功。

执行**display traffic policy statistics interface GigabitEthernet3/0/0 outbound verbose classifer**查看接口上基于流分类的报文统计信息。

----结束

配置注意事项

- 请配置Switch与不同的网段用户对接的接口为Access类型接口，并将其加入对应VLAN。
- 请配置Switch与RouterA对接的接口为Trunk类型接口，并加入对应VLAN。

18.10 配置 CBQ 综合示例

规格

仅支持MPLS特性的设备支持该示例。

组网需求

如图18-10所示，企业内用户通过交换机连接到RouterA和RouterB，并通过RouterA和RouterB连接到WAN侧网络，实现互通。

现要求：

- LAN侧：

  交换机和路由器之间使用FE口连接，通过VLAN区分实时业务和非实时业务。重标记实时业务报文的EXP优先级为4，非实时业务报文的EXP优先级为3。

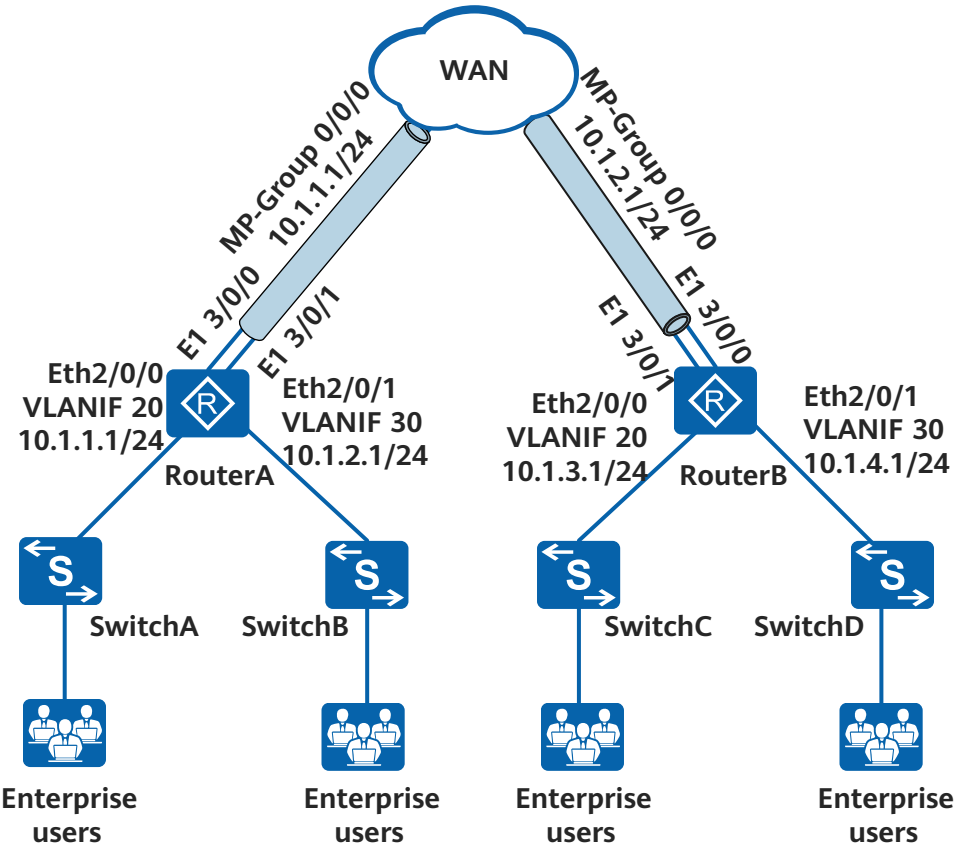
- WAN侧：

  将路由器上工作在E1模式的2个CE1/PRI接口和MP-Group绑定，接入WAN侧网络。

  实时业务和非实时业务通过VPN实例vpn-rt和VPN实例vpn-nrt隔离。实时业务既保证带宽，又保证时延，保证60%接口带宽；非实时业务保证30%接口带宽。

 版权所有 © 华为技术有限公司

图 18-10 配置 CBQ 的组网图



操作步骤

步骤1 RouterA的配置

```
#
 sysname RouterA
#
router id 1.1.1.1  //Router ID，建议配置为LoopBack0的IP地址
#
vlan batch 20 30
#
ip vpn-instance vpn-nrt  //配置VPN实例vpn-nrt，用于通过非实时业务报文
 ipv4-family
  route-distinguisher 21825:2
  vpn-target 21825:200 export-extcommunity
  vpn-target 21825:200 import-extcommunity
#
ip vpn-instance vpn-rt  //配置VPN实例vpn-rt，用于通过实时业务报文
 ipv4-family
  route-distinguisher 21825:1
  vpn-target 21825:100 export-extcommunity
  vpn-target 21825:100 import-extcommunity
#
 mpls lsr-id 1.1.1.1  //配置MPLS的LSR ID为LoopBack0的IP地址
 mpls  //全局使能MPLS
#
mpls ldp  //全局使能MPLS LDP
#
traffic classifier vpn-nrt operator or  //配置流分类，匹配EXP优先级为3的报文
```


版权所有 © 华为技术有限公司

```
 if-match mpls-exp 3
traffic classifier lan-rt operator or  //配置流分类，匹配所有通过的报文
 if-match any
traffic classifier vpn-rt operator or  //配置流分类，匹配EXP优先级为4的报文
 if-match mpls-exp 4
traffic classifier lan-nrt operator or  //配置流分类，匹配所有通过的报文
 if-match any
#
traffic behavior vpn-nrt  //配置流行为，对符合要求报文进行确保转发，配置可确保的最小带宽占接口可用带宽的30%
 queue af bandwidth pct 30
traffic behavior lan-rt  //配置流行为，重新标记符合要求报文中的EXP优先级为4
 remark mpls-exp 4
traffic behavior vpn-rt  //配置流行为，对符合要求报文进行低延时转发，并配置允许的最大带宽占接口可用带宽的60%
 queue llq bandwidth pct 60
traffic behavior lan-nrt  //配置流行为，重新标记符合要求报文中的EXP优先级为3
 remark mpls-exp 3
#
traffic policy lan-rt  //创建流策略lan-rt
 classifier lan-rt behavior lan-rt precedence 5  //将流分类和对应的流行为进行绑定：将接口下所有通过的报文的EXP优先级重标记为3
traffic policy vpn  //创建流策略vpn
 classifier vpn-nrt behavior vpn-nrt precedence 5  //将流分类和对应的流行为进行绑定：对EXP优先级为3的报文进行确保转发，可确保的最小带宽占接口可用带宽的30%
 classifier vpn-rt behavior vpn-rt precedence 10  //将流分类和对应的流行为进行绑定：对EXP优先级为4的报文进行加速转发，允许的最大带宽占接口可用带宽的60%
traffic policy lan-nrt  //创建流策略lan-nrt
 classifier lan-nrt behavior lan-nrt precedence 5 //将流分类和对应的流行为进行绑定：将接口下所有通过的报文的EXP优先级重标记为4
#
controller E1 3/0/0
 using e1  //配置CE1/PRI接口的工作方式为E1
#
controller E1 3/0/1
 using e1  //配置CE1/PRI接口的工作方式为E1
#
interface Vlanif20
 ip binding vpn-instance vpn-nrt  //将接口Vlanif20与名为vpn-nrt的VPN实例绑定
 ip address 10.1.1.1 255.255.255.0
#
interface Vlanif30
 ip binding vpn-instance vpn-rt  //将接口Vlanif30与名为vpn-rt的VPN实例绑定
 ip address 10.1.2.1 255.255.255.0
#
interface Mp-group0/0/0
 ip address 10.1.1.1 255.255.255.0
 qos gts cir 400 cbs 100000  //限制Mp-group0/0/0接口向外发送数据的承诺信息速率为400kbit/s，承诺突发尺寸为100000字节
 traffic-policy vpn outbound  //将流策略vpn应用到接口出方向
 mpls  //接口使能MPLS
 mpls ldp  //接口使能MPLS LDP
#
interface Serial3/0/0:0
 link-protocol ppp  //配置接口封装的链路层协议为PPP
 ppp mp Mp-group 0/0/0  //配置接口Serial3/0/0:0加入Mp-group 0/0/0
#
interface Serial3/0/1:0
 link-protocol ppp  //配置接口封装的链路层协议为PPP
 ppp mp Mp-group 0/0/0  //配置接口Serial3/0/0:1加入Mp-group 0/0/0
#
interface Ethernet2/0/0
 port link-type trunk
 port trunk allow-pass vlan 20
 traffic-policy lan-nrt inbound  //将流策略lan-nrt应用到接口入方向
#
interface Ethernet2/0/1
 port link-type trunk
 port trunk allow-pass vlan 30
```

 版权所有 © 华为技术有限公司

```
 traffic-policy lan-rt inbound  //将流策略lan-rt应用到接口入方向
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
bgp 100
 peer 2.2.2.2 as-number 100  //配置IPv4对等体2.2.2.2的对端AS号为100
 peer 2.2.2.2 connect-interface LoopBack0  //指定BGP报文的源接口和源地址
 #
 ipv4-family unicast
  undo synchronization
  peer 2.2.2.2 enable
 #
 ipv4-family vpnv4  //使能BGP的vpnv4路由能力
  policy vpn-target  //对收到的vpnv4路由进行VPN-Target过滤
  peer 2.2.2.2 enable  //使能与指定对等体2.2.2.2之间交换vpnv4路由信息
 #
 ipv4-family vpn-instance vpn-nrt
  network 10.1.1.0 255.255.255.0  //指定vpn-nrt发布本地路由10.1.1.0/24
  import-route direct  //引入直连路由
 #
 ipv4-family vpn-instance vpn-rt
  network 10.1.2.0 255.255.255.0  //指定vpn-rt发布本地路由10.1.2.0/24
  import-route direct  //引入直连路由
#
ospf 100  //配置OSPF，保证RouterA和RouterB之间路由可达
 import-route direct
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
#
return
```

步骤2 RouterB的配置

```
#
 sysname RouterB
#
router id 2.2.2.2  //Router ID，建议配置为LoopBack0的IP地址
#
vlan batch 20 30
#
ip vpn-instance vpn-nrt
 ipv4-family
  route-distinguisher 21825:2
  vpn-target 21825:200 export-extcommunity
  vpn-target 21825:200 import-extcommunity
#
ip vpn-instance vpn-rt
 ipv4-family
  route-distinguisher 21825:1
  vpn-target 21825:100 export-extcommunity
  vpn-target 21825:100 import-extcommunity
#
 mpls lsr-id 2.2.2.2  //配置MPLS的LSR ID为LoopBack0的IP地址
 mpls
#
mpls ldp
#
traffic classifier vpn-nrt operator or
 if-match mpls-exp 3
traffic classifier lan-rt operator or
 if-match any
traffic classifier vpn-rt operator or
 if-match mpls-exp 4
traffic classifier lan-nrt operator or
 if-match any
#
traffic behavior vpn-nrt
 queue af bandwidth pct 30
traffic behavior lan-rt
```

 版权所有 © 华为技术有限公司

```
 remark mpls-exp 4
traffic behavior vpn-rt
 queue llq bandwidth pct 60
traffic behavior lan-nrt
 remark mpls-exp 3
#
traffic policy lan-rt
 classifier lan-rt behavior lan-rt precedence 5
traffic policy vpn
 classifier vpn-nrt behavior vpn-nrt precedence 5
 classifier vpn-rt behavior vpn-rt precedence 10
traffic policy lan-nrt
 classifier lan-nrt behavior lan-nrt precedence 5
#
controller E1 3/0/0
 using e1
#
controller E1 3/0/1
 using e1
#
interface Vlanif20
 ip binding vpn-instance vpn-nrt
 ip address 10.1.3.1 255.255.255.0
#
interface Vlanif30
 ip binding vpn-instance vpn-rt
 ip address 10.1.4.1 255.255.255.0
#
interface Mp-group0/0/0
 ip address 10.1.2.1 255.255.255.0
 qos gts cir 400 cbs 100000
 traffic-policy vpn outbound
 mpls
 mpls ldp
#
interface Serial3/0/0:0
 link-protocol ppp
 ppp mp Mp-group 0/0/0
#
interface Serial3/0/1:0
 link-protocol ppp
 ppp mp Mp-group 0/0/0
#
interface Ethernet2/0/0
 port link-type trunk
 port trunk allow-pass vlan 20
 traffic-policy lan-nrt inbound
#
interface Ethernet2/0/1
 port link-type trunk
 port trunk allow-pass vlan 30
 traffic-policy lan-rt inbound
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
bgp 100
 peer 1.1.1.1 as-number 100  //配置IPv4对等体1.1.1.1的对端AS号为100
 peer 1.1.1.1 connect-interface LoopBack0  //指定BGP报文的源接口和源地址
 #
 ipv4-family unicast
  undo synchronization
  peer 1.1.1.1 enable
 #
 ipv4-family vpnv4
  policy vpn-target
  peer 1.1.1.1 enable
 #
 ipv4-family vpn-instance vpn-nrt
```

 版权所有 © 华为技术有限公司

```
 network 10.1.3.0 255.255.255.0  //指定vpn-nrt发布本地路由10.1.3.0/24
 import-route direct  //引入直连路由
#
ipv4-family vpn-instance vpn-rt
 network 10.1.4.0 255.255.255.0  //指定vpn-rt发布本地路由10.1.4.0/24
 import-route direct  //引入直连路由
#
ospf 100  //配置OSPF，保证RouterA和RouterB之间路由可达
 import-route direct
 area 0.0.0.0
  network 10.1.2.0 0.0.0.255
#
return
```

步骤3 验证配置结果

执行**display mpls ldp session**检查LDP对等体间的会话信息，可以看到LDP会话的状态为**Operational**。

执行**display bgp vpnv4 all peer**检查vpnv4的对等体信息，可以看到对等体的状态为**Established**。

执行**display traffic-policy vpn applied-record**、**display traffic-policy lan-nrt applied-record**和**display traffic-policy lan-rt applied-record**检查流策略的应用记录，可以看到流策略的配置信息和在接口下的应用的状态为**success**。

----结束

配置注意事项

- Router ID和MPLS的LSR ID最好都使用同一个LoopBack口的地址。
- 在系统视图和接口视图下都需要使能MPLS和MPLS LDP。
- 配置BGP时注意使用接口LoopBack0建立连接。
- 请配置SwitchA、SwitchB、SwitchC和SwitchD与路由器对接的接口为Trunk类型接口，并加入相应VLAN。
- 使用队列模板时，通过**trust**命令指定对报文按照其自身携带的某类优先级进行优先级映射，并根据映射后的本地优先级值进入不同的队列。若不配置此命令报文按照端口优先级入队列。
- 低延时队列（LLQ）是一种特殊的加速转发队列（EF），LLQ队列较EF队列而言，时延更低。
- 使用CBQ时，设备根据IP优先级或者DSCP优先级、输入接口、IP报文的五元组等规则来对报文进行分类，然后让匹配流分类规则的报文进入对应的EF、AF队列。对于不匹配任何类别的报文，送入系统定义的缺省类，并按照按流的“会话”信息进入BE队列。

18.11 带宽管理

18.11.1 配置禁止 P2P 软件下载的示例

规格

适用于所有版本、所有形态的AR路由器。

 版权所有 © 华为技术有限公司

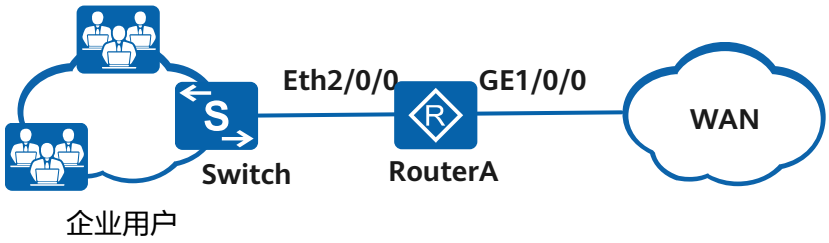
说明

SAC功能使用License授权，缺省情况下，设备的SAC功能受限无法使用。如果需要使用SAC功能，请根据设备款型联系华为办事处申请并购买License。

组网需求

企业内用户通过交换机连接到RouterA的接口Eth2/0/0，并通过RouterA的接口GE1/0/0连接到WAN侧网络。为了保障企业网络带宽资源的合理利用，企业希望能够禁止内部用户使用P2P软件BT、迅雷或电驴进行下载。

图 18-11 配置禁止 P2P 下载的组网图



操作步骤

步骤1 RouterA的配置

```
#
sysname RouterA
#
vlan batch 20
#
engine enable  //开启深度安全防御功能
#
update restore sdb-default sa-sdb  //将特征库恢复到出厂默认版本
#
traffic classifier c1 operator or  //创建流分类c1
 if-match category FileShare_P2P  //在流分类中创建基于SA应用组进行分类的匹配规则
#
traffic behavior b1
 deny  //对匹配规则的报文配置禁止动作
#
traffic policy p1
 classifier c1 behavior b1 precedence 5 //配置流策略p1，绑定流分类c1和流行为b1
#
interface Vlanif20
 ip address 192.168.2.1 255.255.255.0
 sa application-statistic enable  //使能接口Vlanif20的SA统计功能
 traffic-policy p1 inbound  //将流策略p1应用在接口VLANIF20的入方向
#
interface GigabitEthernet1/0/0
 ip address 192.168.4.1 255.255.255.0
 sa application-statistic enable  //使能接口GE1/0/0的SA统计功能
 traffic-policy p1 inbound  //将流策略p1应用在接口GE1/0/0的入方向
#
interface Ethernet2/0/0
 port link-type trunk
 port trunk allow-pass vlan 20
```

 版权所有 © 华为技术有限公司

```
#
return
```

步骤2 验证配置结果

执行**display sa application-statistic**命令检查VLANIF20和GE1/0/0接口上查看基于不同SA应用协议的报文统计信息。

----结束

18.11.2 配置流量整形，对内网 IP 限速的示例

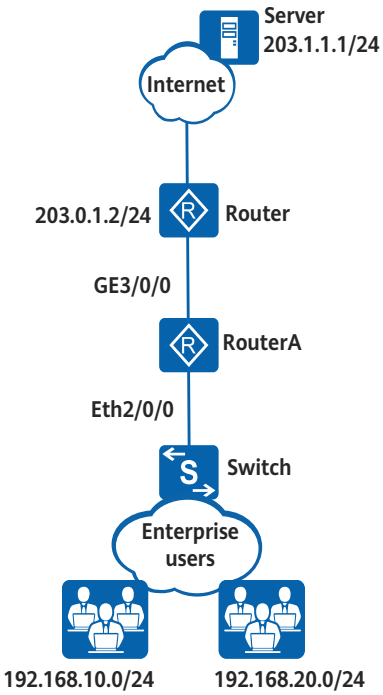
规格

适用于所有版本、所有形态的AR路由器。

组网需求

企业网络中，总部与分支机构通过ISP网络使用专线相连。分支机构想要访问服务器必须通过总部。如果所有分支机构同时访问服务器，可能导致访问服务器的流量产生拥塞，从而被丢弃。为了防止流量的丢失，可以在企业分支机构的流量进入企业总部之前配置流量整形。如图18-12所示，针对内网用户192.168.10.0/24对服务器203.1.1.1/24的访问，要求控制速率在64kbit/s。

图 18-12 配置基于内网 IP 进行限速的组网图



操作步骤

步骤1 RouterA的配置

 版权所有 © 华为技术有限公司

```
#
 sysname RouterA
#
vlan batch 10 20
#
acl number 3001  //配置编号为3001的编号型访问控制列表
 rule 5 permit ip source 192.168.10.0 0.0.0.255  //配置规则5，允许源地址为192.168.10.0网段的报文通过
 rule 10 permit ip source 192.168.20.0 0.0.0.255  //配置规则10，允许源地址为192.168.20.0网段的报文通过
acl number 3002  //配置编号为3002的编号型访问控制列表
 rule 5 permit ip source 192.168.10.0 0.0.0.255  //配置规则5，允许源地址为192.168.10.0网段的报文通过
#
qos queue-profile limit  //创建队列模板limit
  queue 3 gts cir 64 cbs 1600  //配置队列3的承诺信息速率为64kbit/s
#
traffic classifier c1 operator or
 if-match acl 3002  //配置流分类c1：匹配规则为ACL 3002
#
traffic behavior b1
 remark local-precedence af3  //配置流行为b1：对匹配流分类的报文重标记本地优先级为AF3，不指定流行为为
permit或deny时，默认为permit。
#
traffic policy p1
 classifier c1 behavior b1 precedence 5 //配置流策略p1:绑定流分类c1与流行为b1
#
interface Vlanif10
 ip address 192.168.10.1 255.255.255.0
#
interface Vlanif20
 ip address 192.168.20.1 255.255.255.0
#
interface Ethernet2/0/0
 port link-type trunk  //配置接口的链路类型为Trunk
 port trunk allow-pass vlan 10 20  //配置Trunk类型接口加入vlan 10和vlan 20
 traffic-policy p1 inbound  //在接口入方向上应用流策略p1
#
interface GigabitEthernet3/0/0
 ip address 203.0.1.1 255.255.255.0
 qos queue-profile limit  //在接口上应用队列模板limit
 nat outbound 3001  //在接口上对匹配ACL 3001的报文做NAT
#
ip route-static 0.0.0.0 0.0.0.0 203.0.1.2
#
return
```

步骤2 验证配置结果

执行**display qos queue statistics interface gigabitethernet 3/0/0**命令检查GE3/0/0接口上应用了队列模板limit后的报文统计信息，可以看到接口3号队列的输出速率被限制在规定范围内，队列满后，无法缓存的报文被丢弃。

----结束

配置注意事项

- 请配置Switch与不同的网段用户对接的接口为Access类型接口，并将其加入对应VLAN。
- 请配置Switch与RouterA对接的接口为Trunk类型接口，并加入对应VLAN。

相关资料

视频：配置基于接口的限速

 版权所有 © 华为技术有限公司

19 网络管理与监控

19.1 配置通过部署SNMP，使设备与网管进行通信的示例
19.2 配置通过部署Netstream，对用户流量进行统计方便计费的示例
19.3 配置UDP Jitter测试示例
19.4 配置TCP测试示例
19.5 配置通过RMON功能实现对设备的远程监控和管理
19.6 配置通过带验证的单播NTP服务器/客户端模式实现时钟同步示例
19.7 配置通过带验证的NTP广播模式实现时钟同步示例
19.8 配置通过NTP组播模式实现时钟同步示例
19.9 配置本地端口镜像，对用户的行为进行监控的示例

19.1 配置通过部署 SNMP，使设备与网管进行通信的示例

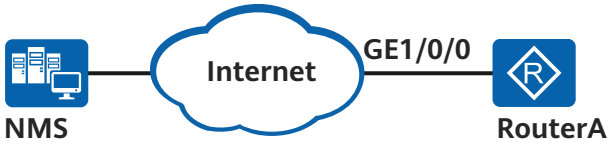
规格

适用于所有版本、所有形态的AR路由器。

组网需求

如图19-1所示，通过部署RouterA由NMS网管设备管理用于监控网络是否畅通和业务是否正常。为了保证NMS和RouterA之间有一个数据传输安全、接入方式灵活、链路传输可靠的网络，并且可以实时监控设备的运行情况，网络中的RouterA通过网管实时监控运行状况，并提供告警报告，以分析出现过的异常并及时解决故障问题。用户在通过网管管理设备时，需要部署SNMP协议，保证网管和被管理设备间的正常通信。

图 19-1 配置 SNMP 功能组网图



 版权所有 © 华为技术有限公司

操作步骤

步骤1 RouterA的配置

```
#
interface GigabitEthernet1/0/0
 ip address 10.1.2.1 255.255.255.0
#
 snmp-agent local-engineid 000007DB7FFFFFFF00001AA7
 snmp-agent community read %@%@$X!5#d+t+OJOXL1[{O2!&0UZv'@a;R/`Y+kK$4BUGFe)&2YLuM/kMF!HPG5Mzz3DXe223%@%@    //配置团体名为admin@123（此处以密文的方式显示），并且只允许进行只读访问
 snmp-agent sys-info version v3    //配置SNMP版本为v3
 snmp-agent target-host trap-hostname nms address 10.1.1.2 udp-port 162 trap-paramsname trapnms2  //配置Trap目的地址为10.1.1.2，主机名为nms，使用的Trap报文发送参数信息列表名为trapnms2
 snmp-agent target-host trap-paramsname trapnms2 v3 securityname %@%@_=XqAFC_94uCS,3'<gYC*ZU6%@%@ privacy //配置Trap报文的发送参数信息列表：列表名为trapnms2，SNMP版本为v3，生成Trap报文的安全名为admin@123（此处以密文的方式显示），对报文进行认证和加密。
 snmp-agent trap enable  //使能RouterA对NMS发送Trap报文的功能
 snmp-agent
#
```

步骤2 验证配置结果

执行命令**display snmp-agent target-host**查看Trap报文的目标主机列表。

当有告警信息产生时，执行命令**display trapbuffer**查看告警信息。

----结束

配置注意事项

- 保证网管NMS配置的SNMP版本和团体名与RouterA一致。

19.2 配置通过部署 Netstream，对用户流量进行统计方便计费的示例

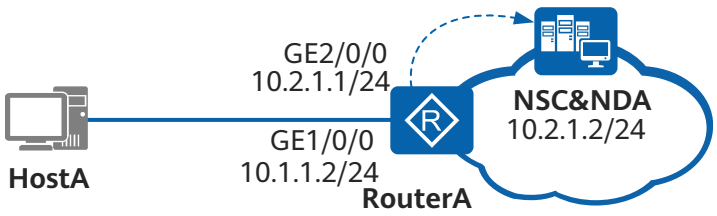
规格

适用于所有版本、所有形态的AR路由器。

组网需求

如图19-2所示，HostA与RouterA的GE1/0/0相连，在RouterA上使能NetStream统计功能。NSC&NDA通过对流入和流出RouterA上GE1/0/0接口的流量进行统计，为网络计费提供依据。

图 19-2 配置 Netstream 功能组网图



版权所有 © 华为技术有限公司

操作步骤

步骤1 RouterA的配置

```
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.2 255.255.255.0
 ip netstream inbound                  //使能RouterA的NetStream入统计功能
 ip netstream outbound                  //使能RouterA的NetStream出统计功能
#
interface GigabitEthernet2/0/0
 ip address 10.2.1.1 255.255.255.0
#
 ip netstream export version 9          //配置RouterA的原始IPv4流按照版本9进行输出
 ip netstream export source 10.2.1.1     //配置RouterA上统计信息输出的源地址
 ip netstream export host 10.2.1.2 6000  //配置RouterA上统计信息输出的目的地址为NSC&NDA（10.2.1.2），端口号为6000
#
```

步骤2 验证配置结果

执行命令**display ip netstream all**，查看NetStream统计的所有配置信息。

----结束

配置注意事项

- 保证RouterA上配置的统计信息端口号与NSC&NDA的一致。

19.3 配置 UDP Jitter 测试示例

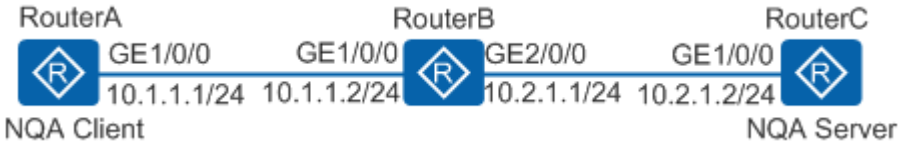
规格

适用于所有版本、所有形态的AR路由器。

组网需求

如图19-3所示，RouterA作为NQA客户端，RouterC作为NQA服务端。使用UDP Jitter测试RouterA与RouterC之间传送报文的抖动时间。

图 19-3 配置 UDP Jitter 测试组网图



操作步骤

步骤1 RouterA的配置

```
#
 sysname RouterA  //配置设备名称
#
```

 版权所有 © 华为技术有限公司

```
interface GigabitEthernet1/0/0
 ip address 10.1.1.1 255.255.255.0  //配置RouterA GE1/0/0的IP地址
#
ip route-static 10.2.1.0 255.255.255.0 10.1.1.2  //配置RouterA到指定网段的静态路由
#
nqa test-instance admin jitter  //创建NQA测试例并进入NQA测试例视图
 test-type jitter  //配置测试例类型为Jitter
 destination-address ipv4 10.2.1.2  //配置目的地址
 destination-port 9000  //配置目的端口号
#
return
```

步骤2 RouterB的配置

```
#
 sysname RouterB  //配置设备名称
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.2 255.255.255.0  //配置RouterB GE1/0/0的IP地址
#
interface GigabitEthernet2/0/0
 ip address 10.2.1.1 255.255.255.0  //配置RouterB GE2/0/0的IP地址
#
return
```

步骤3 RouterC的配置

```
#
 sysname RouterC  //配置设备名称
#
interface GigabitEthernet1/0/0
 ip address 10.2.1.2 255.255.255.0  //配置RouterC GE1/0/0的IP地址
#
nqa-server udpecho 10.2.1.2 9000  //配置NQA服务端的地址和端口号
#
ip route-static 10.1.1.0 255.255.255.0 10.2.1.1  //配置RouterC到指定网段的静态路由
#
return
```

步骤4 验证配置结果

在RouterA的NQA测试例视图下执行命令**start now**启动测试。

在RouterA的任意视图下执行命令**display nqa results test-instance admin jitter**查看抖动时间，其中Average of Jitter表示平均抖动值。

----结束

19.4 配置 TCP 测试示例

规格

适用于所有版本、所有形态的AR路由器。

组网需求

如图19-4所示，RouterA作为NQA客户端，RouterC作为NQA服务端。使用NQA TCP测试功能测试RouterA到RouterC之间建立TCP连接的时间。

 版权所有 © 华为技术有限公司

图 19-4 配置 TCP 测试组网图

操作步骤

步骤1 RouterA的配置

```
#
 sysname RouterA  //配置设备名称
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.1 255.255.255.0  //配置RouterA GE1/0/0的IP地址
#
ip route-static 10.2.1.0 255.255.255.0 10.1.1.2  //配置RouterA到指定网段的静态路由
#
nqa test-instance admin tcp  //创建NQA测试例并进入NQA测试例视图
 test-type tcp  //配置测试例类型为TCP
 destination-address ipv4 10.2.1.2  //配置目的地址
 destination-port 9000  //配置目的端口号
#
return
```

步骤2 RouterB的配置

```
#
 sysname RouterB  //配置设备名称
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.2 255.255.255.0  //配置RouterB GE1/0/0的IP地址
#
interface GigabitEthernet2/0/0
 ip address 10.2.1.1 255.255.255.0  //配置RouterB GE2/0/0的IP地址
#
return
```

步骤3 RouterC的配置

```
#
 sysname RouterC  //配置设备名称
#
interface GigabitEthernet1/0/0
 ip address 10.2.1.2 255.255.255.0  //配置RouterC GE1/0/0的IP地址
#
nqa-server tcpconnect 10.2.1.2 9000  //配置NQA服务端的地址和端口号
#
ip route-static 10.1.1.0 255.255.255.0 10.2.1.1  //配置RouterC到指定网段的静态路由
#
return
```

步骤4 验证配置结果

在RouterA的NQA测试例视图下执行命令**start now**启动测试。

在RouterA的任意视图下执行命令**display nqa results test-instance admin tcp**查看NQA测试结果，其中Min/Max/Average Completion Time表示TCP连接的最小/最大/平均完成时间。

----结束

 版权所有 © 华为技术有限公司

19.5 配置通过 RMON 功能实现对设备的远程监控和管理

规格

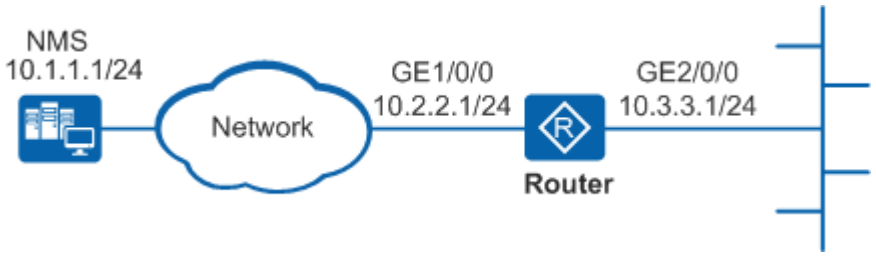
适用于所有版本、所有形态的AR路由器。

组网需求

如图19-5所示，现有一段子网通过Router的接口GE2/0/0接入网络中，需要网管NMS对子网进行监控，包括：

- 流量和各种类型包数量的实时和历史统计信息。
- 当流量超过设定值时，记录日志。
- 监控此子网的广播和组播信息流量，当超过设定值时，主动向NMS上报告警信息。

图 19-5 配置 RMON 组网图



操作步骤

步骤1 Router的配置

```
#
 sysname Router
#
interface GigabitEthernet1/0/0
 ip address 10.2.2.1 255.255.255.0  //配置接口GE1/0/0的IP地址
#
interface GigabitEthernet2/0/0
 ip address 10.3.3.1 255.255.255.0  //配置接口GE2/0/0的IP地址
 rmon-statistics enable  //使能接口GE2/0/0的RMON统计功能
 rmon statistics 1 owner Test300 //配置统计表，表的索引为1，创建者为Test300
 rmon history 1 buckets 10 interval 30 owner Test300  //配置历史控制表，设置RMON对子网中的流量信息采样，采样间隔为30秒钟，并保存最近10次数据
#
ospf 1  //创建并运行OSPF进程
 area 0.0.0.0 //创建并进入OSPF区域视图
  network 10.2.2.0 0.0.0.255 //配置运行OSPF协议区域所包含的网段
  network 10.3.3.0 0.0.0.255  //配置运行OSPF协议区域所包含的网段
#
 snmp-agent target-host trap-hostname hwnm address 10.1.1.1 udp-port 162 trap-paramsname hw //配置向指定的网管发送Trap
 snmp-agent target-host trap-paramsname hw v1 securityname %@%@_=XqAFC_94uCS,3'<gYC*ZU6%@%@
 snmp-agent trap enable //使能SNMP发送Trap的功能
#
 rmon event 1 description null log owner Test300  //配置RMON的1号事件处理方式为记录日志
 rmon event 2 description forUseofPrialarm trap public owner Test300  //配置RMON的2号事件处理方式为向
```


版权所有 © 华为技术有限公司

```
网管站发送Trap消息
 rmon alarm 1 1.3.6.1.2.1.16.1.1.1.6.1 30 absolute rising-threshold 500 1 falling-threshold 100 1 owner Test300  //配置告警表，设置采样间隔时间和触发告警事件1（告警OID为1.3.6.1.2.1.16.1.1.1.6.1）的阈值
 rmon prialarm 1 .1.3.6.1.2.1.16.1.1.1.6.1+.1.3.6.1.2.1.16.1.1.1.7.1 sumofbroadandmulti 30 delta rising-threshold 1000 2 falling-threshold 0 2 entrytype forever owner Test300  //配置扩展告警表，设置RMON对统计表中广播和组播总数每30秒钟进行1次采样，当采样变化值高于最大阈值1000或低于最小阈值0时触发事件2，向网管站发送Trap信息
#
return
```

步骤2 验证配置结果

执行命令**display rmon statistics gigabitethernet 2/0/0**查看子网的数据流量信息。

执行命令**display rmon history gigabitethernet 2/0/0**查看历史统计信息。

执行命令**display rmon event**查看RMON事件的配置信息。

执行命令**display rmon alarm 1**查看RMON告警的配置信息。

执行命令**display rmon prialarm 1**查看RMON扩展告警的配置信息。

执行命令**display rmon eventlog**查看事件日志信息。

----结束

19.6 配置通过带验证的单播 NTP 服务器/客户端模式实现时钟同步示例

规格

适用于所有版本、所有形态的AR路由器。

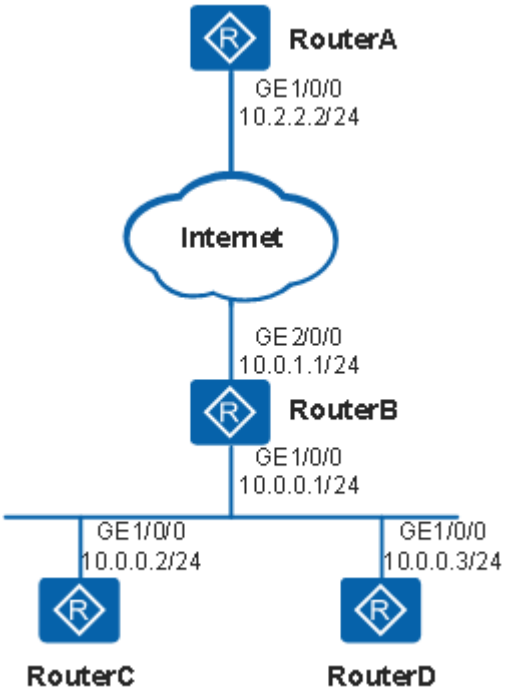
组网需求

在某企业网中，为了保证整个组网的数据传输的灵活性，需要在网络中部署时钟同步业务，为维持整个组网数据保证稳定速率收发不会发生乱序等问题，为整个网络提高了稳定性。如图19-6所示，RouterB、RouterC和RouterD在同一个局域网中并且通过网络和RouterA相连。用户由于业务需要，希望局域网中的所有路由器的系统时间同步到标准时钟。具体要求如下：

- RouterA作为主时钟服务器，层级数为2。
- RouterA和RouterB之间采用单播NTP服务器/客户端模实现时钟同步。RouterA作为服务器，RouterB作为客户端。
- RouterB分别和RouterC、RouterD之间采用单播NTP服务器/客户端模实现时钟同步。其中RouterB作为服务器，RouterC和RouterD均作为客户端。
- 通过使能NTP认证功能加强网络安全。

 版权所有 © 华为技术有限公司

图 19-6 单播 NTP 客户端/服务器模式组网图



操作步骤

步骤1 RouterA的配置

```
#
 sysname RouterA
#
interface GigabitEthernet1/0/0
 ip address 10.2.2.2 255.255.255.0 //配置接口GE1/0/0的IP地址
#
ospf 1  //创建并运行OSPF进程
 area 0.0.0.0  //创建并进入OSPF区域视图
  network 10.2.2.0 0.0.0.255  //配置运行OSPF协议区域所包含的网段
#
 ntp-service authentication enable  //使能NTP认证功能
 ntp-service authentication-keyid 42 authentication-mode hmac-sha256 cipher %^%#$h,(9nViD-B<~\<`rN
+#d1_Y7QHW\(s`_Q%0#L3'%^%#  //配置NTP认证密钥
 ntp-service reliable authentication-keyid 42  //声明NTP认证密钥是可信的
 ntp-service refclock-master 2  //配置RouterA为NTP主时钟且层级数为2
#
return
```

步骤2 RouterB的配置

```
#
 sysname RouterB
#
interface GigabitEthernet1/0/0
 ip address 10.0.0.1 255.255.255.0  //配置接口GE1/0/0的IP地址
#
interface GigabitEthernet2/0/0
 ip address 10.0.1.1 255.255.255.0  //配置接口GE2/0/0的IP地址
#
ospf 1  //创建并运行OSPF进程
 area 0.0.0.0  //创建并进入OSPF区域视图
  network 10.0.0.0 0.0.0.255  //配置运行OSPF协议区域所包含的网段
```


版权所有 © 华为技术有限公司

```
 network 10.0.1.0 0.0.0.255  //配置运行OSPF协议区域所包含的网段
#
 ntp-service authentication enable  //使能NTP认证功能
 ntp-service authentication-keyid 42 authentication-mode hmac-sha256 cipher %^%#$h,(9nViD-B<~\<`rN
+#d1_Y7QHW\(s`_Q%0#L3'%^%#  //配置NTP认证密钥
 ntp-service reliable authentication-keyid 42  //声明NTP认证密钥是可信的
 ntp-service unicast-server 10.2.2.2 authentication-keyid 42  //配置RouterA作为RouterB的NTP服务器，并使用
已配置的验证密钥
#
return
```

步骤3 RouterC的配置

```
#
 sysname RouterC
#
interface GigabitEthernet1/0/0
 ip address 10.0.0.2 255.255.255.0  //配置接口GE1/0/0的IP地址
#
ospf 1  //创建并运行OSPF进程
 area 0.0.0.0  //创建并进入OSPF区域视图
  network 10.0.0.0 0.0.0.255  //配置运行OSPF协议区域所包含的网段
#
 ntp-service authentication enable  //使能NTP认证功能
 ntp-service authentication-keyid 42 authentication-mode hmac-sha256 cipher %^%#$h,(9nViD-B<~\<`rN
+#d1_Y7QHW\(s`_Q%0#L3'%^%#  //配置NTP认证密钥
 ntp-service reliable authentication-keyid 42  //声明NTP认证密钥是可信的
 ntp-service unicast-server 10.0.0.1 authentication-keyid 42  //配置RouterB作为RouterC的NTP服务器，并使用
已配置的验证密钥
#
return
```

步骤4 RouterD的配置

```
#
 sysname RouterD
#
interface GigabitEthernet1/0/0
 ip address 10.0.0.3 255.255.255.0  //配置接口GE1/0/0的IP地址
#
ospf 1  //创建并运行OSPF进程
 area 0.0.0.0  //创建并进入OSPF区域视图
  network 10.0.0.0 0.0.0.255  //配置运行OSPF协议区域所包含的网段
#
 ntp-service authentication enable  //使能NTP认证功能
 ntp-service authentication-keyid 42 authentication-mode hmac-sha256 cipher %^%#$h,(9nViD-B<~\<`rN
+#d1_Y7QHW\(s`_Q%0#L3'%^%#  //配置NTP认证密钥
 ntp-service reliable authentication-keyid 42  //声明NTP认证密钥是可信的
 ntp-service unicast-server 10.0.0.1 authentication-keyid 42  //配置RouterB作为RouterD的NTP服务器，并使用
已配置的验证密钥
#
return
```

步骤5 验证配置结果

在RouterB上执行命令**display ntp-service status**查看NTP状态信息，其中“clock status”显示为“synchronized”，说明已经完成时钟同步。“clock stratum”显示为“3”，比服务器RouterA低1级，说明RouterB同步了RouterA的时钟。

在RouterC上执行命令**display ntp-service status**查看NTP状态信息，其中“clock status”显示为“synchronized”，说明已经完成时钟同步。“clock stratum”显示为“4”，比服务器RouterB低1级，说明RouterC同步了RouterB的时钟。

在RouterD上执行命令**display ntp-service status**查看NTP状态信息，其中“clock status”显示为“synchronized”，说明已经完成时钟同步。“clock stratum”显示为“4”，比服务器RouterB低1级，说明RouterD同步了RouterB的时钟。

----结束

 版权所有 © 华为技术有限公司

配置注意事项

- 在单播服务器/客户端模式下配置NTP认证时，必须在客户端先使能NTP认证，然后再指定NTP服务器地址，并同时指定发给服务器的验证密钥。否则将不进行验证，直接同步。
- 服务器端和客户端必须配置相同的认证密钥。
- 客户端和服务器端都需要进行完整的配置，才能验证通过。

19.7 配置通过带验证的 NTP 广播模式实现时钟同步示例

规格

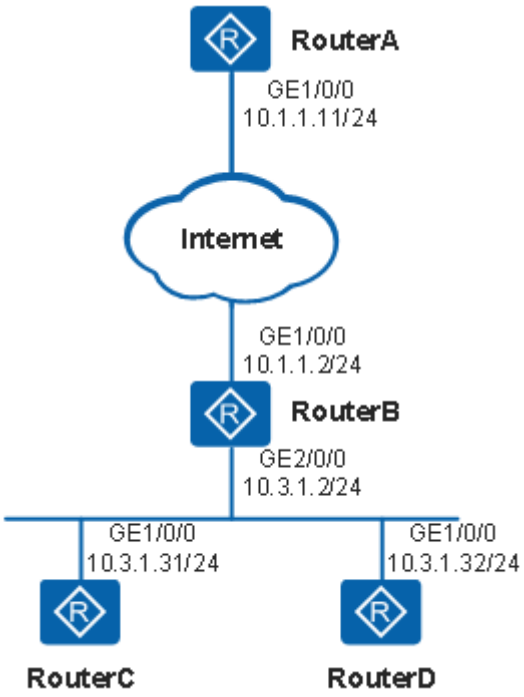
适用于所有版本、所有形态的AR路由器。

组网需求

如图19-7所示，RouterB、RouterC和RouterD在同一个局域网中。RouterA和RouterB直连。RouterC通过无线电直接同步到标准时钟。用户由于业务需要，要求局域网中的所有路由器的时间同步到标准时钟，但是不影响RouterA的系统时钟。具体要求如下：

- RouterC作为主时钟服务器，使用本地时钟作为NTP主时钟，层级数为3。
- RouterC为NTP广播服务器，从接口GE1/0/0向外发送广播报文。
- RouterA、RouterD和RouterB为NTP广播客户端。RouterA使用GE1/0/0接口侦听广播报文。RouterD使用GE1/0/0接口侦听广播报文。RouterB使用GE2/0/0接口侦听广播报文。
- 通过使能NTP认证功能加强网络安全。

图 19-7 NTP 广播模式组网图



版权所有 © 华为技术有限公司

操作步骤

步骤1 RouterA的配置

```
#
 sysname RouterA
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.11 255.255.255.0  //配置接口GE1/0/0的IP地址
 ntp-service broadcast-client  //配置RouterA为NTP广播客户端
#
ospf 1  //创建并运行OSPF进程
 area 0.0.0.0  //创建并进入OSPF区域视图
  network 10.1.1.0 0.0.0.255  //配置运行OSPF协议区域所包含的网段
#
 ntp-service authentication enable  //使能NTP认证功能
 ntp-service authentication-keyid 16 authentication-mode hmac-sha256 cipher %@%@,1_MBtq@`IsY6$Xkl|
J<"6P(%@%@  //配置NTP认证密钥
 ntp-service reliable authentication-keyid 16  //声明NTP认证密钥是可信的
#
return
```

步骤2 RouterB的配置

```
#
 sysname RouterB
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.2 255.255.255.0  //配置接口GE1/0/0的IP地址
#
interface GigabitEthernet2/0/0
 ip address 10.3.1.2 255.255.255.0  //配置接口GE2/0/0的IP地址
 ntp-service broadcast-client  //配置RouterB为NTP广播客户端
#
ospf 1  //创建并运行OSPF进程
 area 0.0.0.0  //创建并进入OSPF区域视图
  network 10.1.1.0 0.0.0.255  //配置运行OSPF协议区域所包含的网段
  network 10.3.1.0 0.0.0.255  //配置运行OSPF协议区域所包含的网段
#
 ntp-service authentication enable  //使能NTP认证功能
 ntp-service authentication-keyid 16 authentication-mode hmac-sha256 cipher %@%@,1_MBtq@`IsY6$Xkl|
J<"6P(%@%@  //配置NTP认证密钥
 ntp-service reliable authentication-keyid 16  //声明NTP认证密钥是可信的
#
return
```

步骤3 RouterC的配置

```
#
 sysname RouterC
#
interface GigabitEthernet1/0/0
 ip address 10.3.1.31 255.255.255.0  //配置接口GE1/0/0的IP地址
 ntp-service broadcast-server authentication-keyid 16  //配置RouterC为NTP广播服务器
#
ospf 1  //创建并运行OSPF进程
 area 0.0.0.0  //创建并进入OSPF区域视图
  network 10.3.1.0 0.0.0.255  //配置运行OSPF协议区域所包含的网段
#
 ntp-service authentication enable  //使能NTP认证功能
 ntp-service authentication-keyid 16 authentication-mode hmac-sha256 cipher %@%@,1_MBtq@`IsY6$Xkl|
J<"6P(%@%@  //配置NTP认证密钥
 ntp-service reliable authentication-keyid 16  //声明NTP认证密钥是可信的
 ntp-service refclock-master 3  //配置RouterC为NTP主时钟且层级数为3
#
return
```

 版权所有 © 华为技术有限公司

步骤4 RouterD的配置

```
#
 sysname RouterD
#
interface GigabitEthernet1/0/0
 ip address 10.3.1.32 255.255.255.0  //配置接口GE1/0/0的IP地址
 ntp-service broadcast-client  //配置RouterD为NTP广播客户端
#
ospf 1  //创建并运行OSPF进程
 area 0.0.0.0  //创建并进入OSPF区域视图
  network 10.3.1.0 0.0.0.255  //配置运行OSPF协议区域所包含的网段
#
 ntp-service authentication enable  //使能NTP认证功能
 ntp-service authentication-keyid 16 authentication-mode hmac-sha256 cipher %@%@,1_MBtq@`IsY6$XkI|J<"6P(%@%@  //配置NTP认证密钥
 ntp-service reliable authentication-keyid 16  //声明NTP认证密钥是可信的
#
return
```

步骤5 验证配置结果

在RouterA上执行命令**display ntp-service status**查看NTP状态信息，其中“clock status”显示为“unsynchronized”，说明未同步RouterC的时钟。因为RouterA和RouterC不在同一个网段，收不到RouterC发出的广播报文。

在RouterD上执行命令**display ntp-service status**查看NTP状态信息，其中“clock status”显示为“synchronized”，说明已经完成时钟同步。“clock stratum”显示为“4”，比服务器RouterC低1级，说明RouterD同步了RouterC的时钟。因为RouterD和RouterC在同一个网段，能够收到RouterC发出的广播报文。

----结束

19.8 配置通过 NTP 组播模式实现时钟同步示例

规格

适用于所有版本、所有形态的AR路由器。

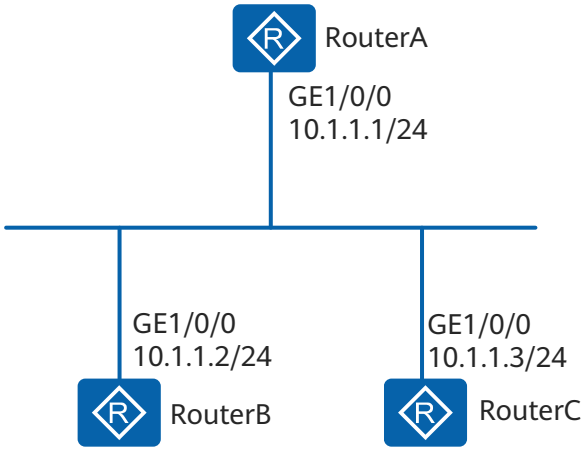
组网需求

如图19-8所示，RouterA、RouterB和RouterC在同一个局域网中。RouterA通过无线电直接同步到标准时钟。用户由于业务需要，要求组网中所有路由器的时钟同步到标准时钟。具体要求如下：

- RouterA作为主时钟服务器，使用本地时钟作为NTP主时钟，层级数为2。
- RouterA为NTP组播服务器，从接口GE1/0/0向外发送组播报文。
- RouterB和RouterC为NTP组播客户端。RouterB使用GE1/0/0接口侦听组播报文。RouterC使用GE1/0/0接口侦听组播报文。

 版权所有 © 华为技术有限公司

图 19-8 NTP 组播模式组网图



操作步骤

步骤1 RouterA的配置

```
#
 sysname RouterA
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.1 255.255.255.0  //配置接口GE1/0/0的IP地址
 ntp-service multicast-server  //配置RouterA为NTP组播服务器
#
 ntp-service refclock-master  2  //配置RouterA为NTP主时钟且层级数为2
#
return
```

步骤2 RouterB的配置

```
#
 sysname RouterB
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.2 255.255.255.0  //配置接口GE1/0/0的IP地址
 ntp-service multicast-client  //配置RouterB为NTP组播客户端
#
return
```

步骤3 RouterC的配置

```
#
 sysname RouterC
#
interface GigabitEthernet1/0/0
 ip address 10.1.1.3 255.255.255.0  //配置接口GE1/0/0的IP地址
 ntp-service multicast-client  //配置RouterC为NTP组播客户端
#
return
```

步骤4 验证配置结果

在RouterB上执行命令**display ntp-service status**查看NTP状态信息，其中“clock status”显示为“synchronized”，说明已经完成时钟同步。“clock stratum”显示为“3”，比服务器RouterA低1级，说明RouterB同步了RouterA的时钟。

版权所有 © 华为技术有限公司

在RouterC上执行命令**display ntp-service status**查看NTP状态信息，其中“clock status”显示为“synchronized”，说明已经完成时钟同步。“clock stratum”显示为“3”，比服务器RouterA低1级，说明RouterC同步了RouterA的时钟。

----结束

19.9 配置本地端口镜像，对用户的行为进行监控的示例

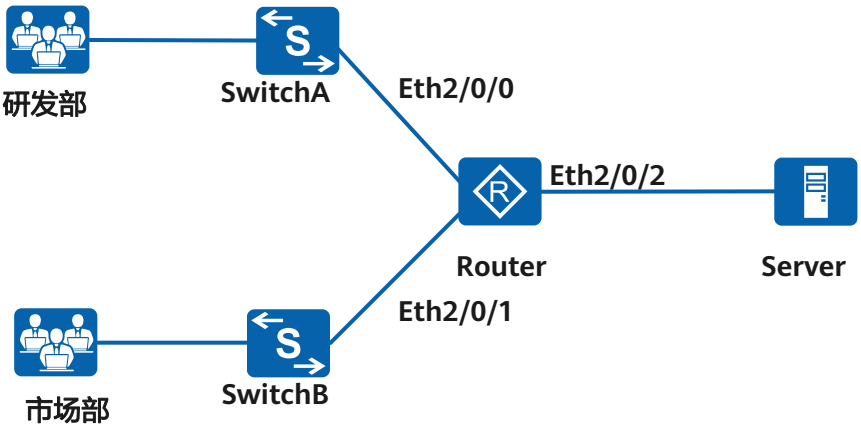
规格

适用于所有版本、所有形态的AR路由器。

组网需求

如图19-9所示，Router作为某企业的出口网关，研发部和市场部用户分别通过接口Eth2/0/0和Eth2/0/1接入网关。一台数据检测设备Server接在网关的接口Eth2/0/2上，Server上安装了监控软件，用于对抓取的数据进行分析。为保证企业的信息安全，要求借助本地端口镜像功能来实现Server对研发部和市场部发送的所有报文的监控。

图 19-9 本地端口镜像配置组网图



操作步骤

步骤1 Router的配置

```
#
 observe-port interface Ethernet2/0/2  //配置本地观察端口
#
interface Ethernet2/0/0
 mirror to observe-port inbound  //将Ethernet2/0/0配置为本地镜像端口，并指定对端口入方向的报文进行镜像。
#
interface Ethernet2/0/1
 mirror to observe-port inbound  //将Ethernet2/0/1配置为本地镜像端口，并指定对端口入方向的报文进行镜像。
#
```

步骤2 验证配置结果

在Router上执行display observe-port命令，查看观察端口的配置情况。其中，“Interface:”字段显示为Ethernet2/0/2

版权所有 © 华为技术有限公司

在Router上执行display mirror-port命令，查看镜像端口的配置情况。其中，“Mirror-port:”字段显示为Ethernet2/0/0和Ethernet2/0/1。

在Router上执行display interface命令，查看接口Ethernet2/0/0、Ethernet2/0/1和Ethernet2/0/2的报文计数，可以看到接口Ethernet2/0/2的出方向的报文计数为接口Ethernet2/0/0与接口Ethernet2/0/1的入方向的报文计数之和，或者通过Server可以看到接口Ethernet2/0/0和Ethernet2/0/1收到的所有报文，说明接口Ethernet2/0/0和Ethernet2/0/1上的报文已经被Router镜像过来。

----结束

配置注意事项

- 路由器仅可以配置一个观察端口，且观察端口仅支持LAN侧和WAN侧以太口。
- 路由器支持将多个端口的报文镜像到一个观察端口。
- 配置观察端口和镜像端口时，需要注意接口的带宽关系。例如将GigabitEthernet接口作为镜像端口，将Ethernet接口作为观察端口时，观察端口的接收能力不够，可能会造成镜像报文的丢失。
- 如果接口被配置为观察端口后，建议不要在该接口上进行其他配置，否则影响镜像功能：若观察端口上不仅有镜像报文还有其他业务流量，将无法区分报文来源；若观察端口发生拥塞时，由于镜像报文的优先级比较低，可能导致镜像报文被丢弃。

 版权所有 © 华为技术有限公司

20 综合案例

20.1 配置DHCP和NAT，实现用户动态获取IP地址并访问Internet公网的示例
20.2 IPSec与NQA联动实现主备对等体和主备链路快速切换
20.3 配置SPR实现语音业务智能选路示例

20.1 配置 DHCP 和 NAT，实现用户动态获取 IP 地址并访问 Internet 公网的示例

规格

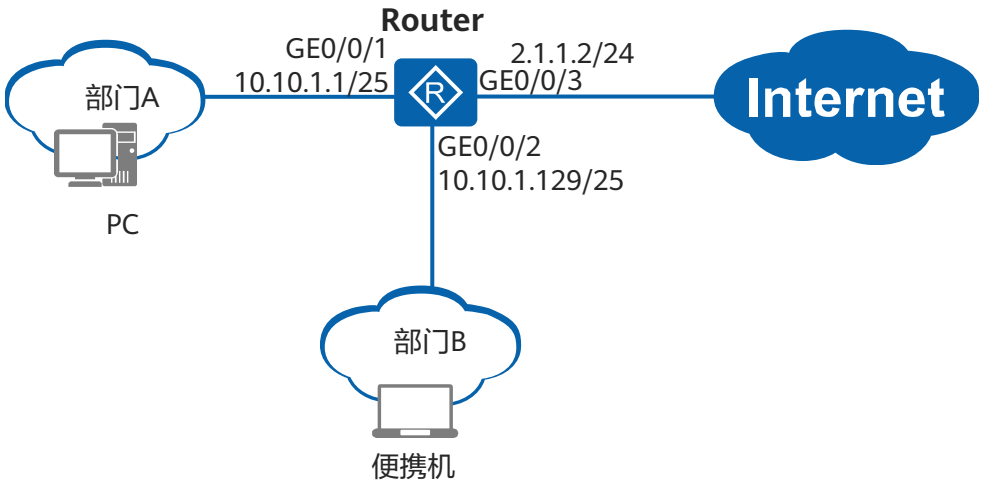
适用于所有版本、所有形态的AR路由器。

组网需求

Router作为某企业出口网关。该企业包括两个部门A和B，分别为部门A和B内终端规划两个地址网段：10.10.1.0/25和10.10.1.128/25，网关地址分别为10.10.1.1/25和10.10.1.129/25。部门A内PC为办公终端，地址租用期限为30天，域名为huawei.com，DNS服务器地址为10.10.1.2。部门B内大部分是出差人员所用便携机，地址租用期限为2天，域名为huawei.com，DNS服务器地址为10.10.1.2。企业内地址规划为私网地址，且需要访问Internet公网，因此，需要通过配置NAT实现私网地址到公网地址的转换。连接Router出接口GE0/0/3的对端IP地址为2.1.1.1/24。

 版权所有 © 华为技术有限公司

图 20-1 配置 DHCP 和 NAT，实现用户动态获取 IP 地址并访问 Internet 公网的组网图



操作步骤

步骤1 Router上的配置

```
#
 sysname Router  //修改设备名称
#
dhcp enable //使能DHCP功能
#
acl number 2000  //配置允许进行NAT转换的内网地址段10.10.1.0/24
 rule 5 permit source 10.10.1.0 0.0.0.255
#
ip pool ip-pool1
 gateway-list 10.10.1.1 //配置网关地址
 network 10.10.1.0 mask 255.255.255.128 //配置全局地址池可动态分配的IP地址范
围
 excluded-ip-address 10.10.1.2 //配置地址池中10.10.1.2不参与自动分配
 dns-list 10.10.1.2 //配置DHCP客户端使用的DNS服务器的IP地址
 lease day 30 hour 0 minute 0 //配置IP地址租期为30天
 domain-name huawei.com //配置域名为huawei.com
#
ip pool ip-pool2
 gateway-list 10.10.1.129 //配置网关地址
 network 10.10.1.128 mask 255.255.255.128 //配置全局地址池可动态分配的IP地址范围
 dns-list 10.10.1.2 //配置DHCP客户端使用的DNS服务器的IP地址
 lease day 2 hour 0 minute 0 //配置IP地址租期为2天
 domain-name huawei.com //配置域名为huawei.com
#
interface GigabitEthernet0/0/1
 ip address 10.10.1.1 255.255.255.128
 dhcp select global //接口工作在全局地址池模式
#
interface GigabitEthernet0/0/2
 ip address 10.10.1.129 255.255.255.128
 dhcp select global //接口工作在全局地址池模式
#
interface GigabitEthernet0/0/3
 ip address 2.1.1.2 255.255.255.0
 nat outbound 2000  //在出接口GE0/0/3上做Easy IP方式的NAT，实现私网地址到公网地址的转换
#
ip route-static 0.0.0.0 0.0.0.0 2.1.1.1  //配置默认路由，保证出接口到对端路由可达
#
return
```


版权所有 © 华为技术有限公司

步骤2 验证配置结果

在Router上执行命令**display ip pool**，可以查看IP地址池的分配情况。执行命令**display nat outbound**，可以查看GE0/0/3上NAT的配置信息。配置成功后，终端可以动态获取IP地址，并能访问Internet。

----结束

配置注意事项

配置ACL，确定对哪些网段进行NAT转换。

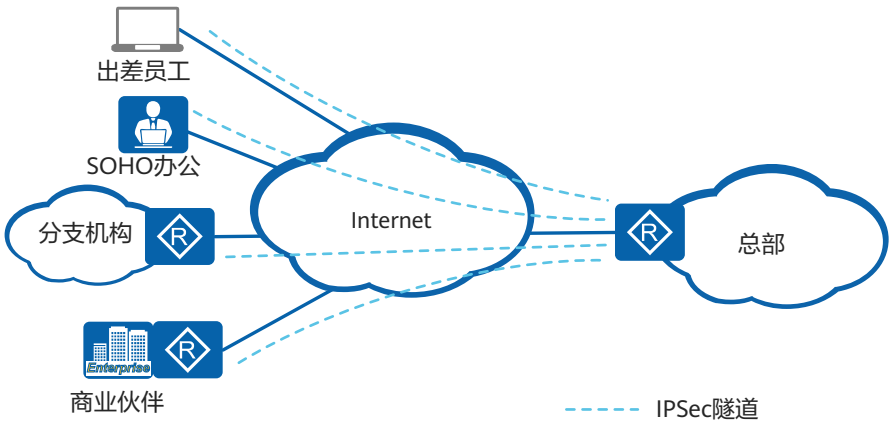
20.2 IPSec 与 NQA 联动实现主备对等体和主备链路快速切换

IPSec 简介

如图20-2所示，IPSec VPN利用Internet构建VPN的方式，允许用户以任意方式接入VPN，并且不受地理因素的限制，无论用户在哪里，只需要从当地接入Internet即可。IPSec VPN不仅适用于移动办公用户、商业伙伴接入，而且适用于企业总部和分支机构之间互连互通。

站点之间的数据流通过IPSec隧道进行安全保护传送，虽然是在公网上传输，但都得到加密保护。

图 20-2 IPSec VPN 基本组网图



如图20-3所示，为了保证总部设备的可靠性，总部使用两台或两台以上的设备进行VRRP组网，总部与分支建立IPSec隧道。分支网关需在一个对等体下配置2个地址或域名与总部网关建立IPSec。分支网关首先采用第一个地址或域名与总部网关建立IPSec，若第一个IPSec建立失败或对等体存活检测结果为失败，采用第二个地址或域名建立IPSec。但是，这个切换过程耗时较长，且当故障恢复后，流量也无法回切到原对等体。

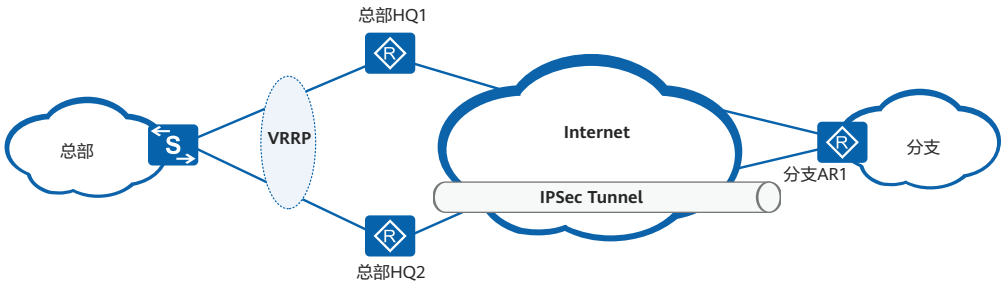
此时，可以通过部署IPSec与NQA联动，根据探测结果确定对等体地址是否失效，如果失效，则触发流量快速向另一个地址的对等体切换，进而实现对等体的快速切换，确

 版权所有 © 华为技术有限公司

保一个总部网关故障时流量能及时切换到另一个总部网关。另外，也可配置对等体回切功能，使原总部网关故障恢复后流量能够回切回来。

同时，为了提高分支链路的可靠性，分支网关使用两个接口接入Internet进行主备链路组网。分支网关首先使用主链路与总部网关建立IPSec，若主链路故障，采用备份链路与总部网关建立IPSec。由于这个切换过程也耗时较长，且故障恢复后，流量也无法回切到主链路。因此，也可以通过部署IPSec与NQA联动，根据探测结果确主链路否失效，如果失效，则触发流量快速向备份链路切换。而且，主链路故障恢复后流量能够回切回来。

图 20-3 IPSec 与 NQA 联动实现主备快速切换组网图



配置注意事项

1. 保证同一备份组的设备上配置相同的备份组号。
2. 分支和总部的认证算法和加密算法需一致。
3. 分支的ACL需要与总部ACL互为镜像，当对等体间ACL规则非互为镜像时，只有发起方的ACL规则定义的范围是响应方的子集时，SA才能成功建立。
4. 当IPSec与NAT配置在同一台设备时，要确认经过IPSec封装的数据流是否还需要进行NAT转换。
   - 如果需要进行NAT转换，则Security ACL要匹配NAT后的地址。
   - 如果不需要进行NAT转换，则Security ACL要匹配NAT前的地址，且NAT的ACL中要将经过IPSec隧道的数据流的动作配置为**Deny**。
5. 配置IPSec时需保证公网路由可达，这里不详细介绍。

组网需求

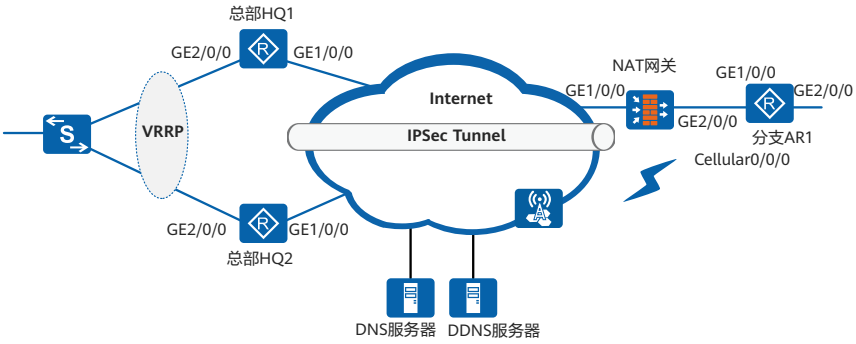
如图20-4所示，HQ1和HQ2都为总部网关，AR1为分支网关。DNS服务器为解析域名的服务器，DDNS服务器为更新域名对应IP地址的服务器。

为了提高企业总部网关的可靠性，企业总部HQ1和HQ2进行VRRP组网，其中HQ1为Master。同时，为了提高分支链路的可靠性和业务的安全性，分支AR1接入两条链路与总部建立IPSec VPN，其中3G拨号链路为备份链路。现企业要求如下：

- 企业希望当总部主链路（HQ1到AR1之间的链路）故障时，VRRP备份组可以感知并进行主备切换，启用HQ2承担业务转发，以减小链路故障对业务转发的影响。
- 企业希望HQ1故障时，AR1能快速切换与HQ2协商建立IPSec隧道，以减少流量的丢失，同时HQ1故障恢复后流量能够回切回来。
- 企业希望AR1主链路故障时，IPSec隧道能快速切换到备份链路，以减少业务流量的丢失，同时当主链路恢复后流量能快速回切回来。

 版权所有 © 华为技术有限公司

图 20-4 IPSec 与 NQA 联动实现主备快速切换组网图



配置思路

为了满足企业上述需求，采用如下思路进行配置：

1. 为了实现网关的主备备份，需在HQ1和HQ2上配置VRRP备份组。其中HQ1的优先级为120，抢占延时为20秒，作为Master设备；HQ2的优先级为90，作为Backup设备。
2. 为了保证VRRP备份组及时切换，减少业务丢失，可以配置VRRP与NQA联动功能，实时监测总部主链路的连通状况。当NQA探测失败时，数据流量及时从HQ1切换到HQ2进行转发。
3. 为了实现分支和总部的业务安全互通，需在HQ1、HQ2和AR1上配置IPSec。
4. 为了实现分支与总部主备对等体快速切换，减少业务丢失，需在AR1配置IPSec与NQA联动功能，实时监测对等体地址是否失效，确保一个总部网关故障时流量能及时切换到另一个总部网关。另外，也可配置对等体回切功能，使原总部网关故障恢复后流量能够回切回来。
5. 为了分支主备链路快速切换，减少业务丢失，需在AR1上配置IPSec与NQA联动功能，实时监测IPSec隧道联通状况，确保分支主链路故障时，流量能快速切换到备份链路。当主链路故障恢复后流量能够回切回来。

版权所有 © 华为技术有限公司

数据规划

表 20-1 数据规划表

业务	参数	说明
IP地址	HQ1： ● GE2/0/0：10.1.0.1/24 HQ2： ● GE2/0/0：10.1.0.2/24 AR1： ● GE1/0/0：10.2.1.2/24 ● GE2/0/0：10.0.1.1/24 ● Cellular0/0/0：2.1.1.2/24 NAT： ● GE1/0/0：1.0.3.1/24 ● GE2/0/0：10.2.1.1/24 DNS服务器：5.1.1.2/24	HQ1和HQ2的GE1/0/0接口都是通过PPPoE拨号获得地址 HQ1对应的域名为store1.huawei.com，对应地址为3.1.1.1/24 HQ2对应的域名为store2.7huawei.com，对应地址为4.1.1.1/24
VRRP备份组	虚地址：10.1.0.10/24 Master：HQ1，优先级：120，抢占延迟时间：20秒 Backup：HQ2，优先级：90	无
IKE安全提议	认证算法：sha2-256 加密算法：aes-cbc-128	总部与分支的配置需一致
IPSec安全提议	认证算法：sha2-256 加密算法：aes-192	
预共享密钥	认证字：huawei1234	
NQA测试例	管理者：user 测试例名：test、test1 测试类型：ICMP 一次测试的探针数：5 发送报文时间间隔：20秒	无

配置文件

- 配置HQ1

```
#
 sysname HQ1
#
 dns resolve  //使能DNS域名解析功能来解析总部网关地址
```

 版权所有 © 华为技术有限公司

```
 dns server 5.1.1.2  //配置DNS服务器的IP地址
#
ddns policy ddnspolicy1  //配置DDNS策略来更新域名对应IP地址
 url oray://username1:password1@phddnsdev.oray.net  //配置DDNS服务器的URL
#
ipsec proposal def  //配置IPSec提议
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-192
#
ike proposal 1  //配置IPSec IKE提议
 encryption-algorithm aes-cbc-128  //V200R008及之后的版本，aes-cbc-128参数修改为aes-128
 authentication-algorithm sha2-256
#
ike peer branch v2  //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 pre-shared-key cipher %^%#JvZxR2g8c;a9~FPN~n'$7`DEV&=G(=Et02P/%\*!%^%#  //配置预共享密钥认证字为“YsHsjx_202206”，以密文显示，该命令在V2R3C00以前的版本中为“pre-shared-key YsHsjx_202206”，以明文显示
 ike-proposal 1
 nat traversal  //使能NAT穿越功能。V200R008版本，设备默认使能NAT穿越功能，不支持配置此命令；但V200R008之后版本，支持配置此命令
 dpd type periodic  //指定检测模式为周期性地进行检测
 dpd retransmit-interval 10  //设置DPD报文重传间隔为10秒
#
ipsec policy-template use1 10  //配置IPSec策略模板
 ike-peer branch
 proposal def
#
ipsec policy branch 1 isakmp template use1 //指定安全策略中引用策略模板
#
interface Dialer0 //配置拨号口相关参数
 link-protocol ppp
 ppp pap local-user user@huawei.com password cipher %@%@ZX}=YK.{rUa.K#7W\==O)+[c%@%@
 ip address ppp-negotiate
 dialer user huawei
 dialer bundle 1  //指定共享DCC的Dialer接口使用的Dialer bundle
 dialer-group 1  //将接口置于一个拨号访问组中
 ddns policy ddnspolicy1  //拨号口上应用DDNS策略，使其接口IP地址发生变化时，能向DDNS服务器发送动态更新
 ipsec policy branch  //绑定IPSec策略
#
interface GigabitEthernet1/0/0
 pppoe-client dial-bundle-number 1 //绑定拨号口，建立PPPoE会话
#
interface GigabitEthernet2/0/0
 ip address 10.1.0.1 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.0.10  //配置VRRP组1的虚地址10.1.0.10
 vrrp vrid 1 priority 120  //配置路由器在备份组中的优先级
 vrrp vrid 1 preempt-mode timer delay 20 //配置备份组中路由器的抢占延迟时间
 vrrp vrid 1 track nqa user test reduced 40 //配置VRRP与NQA联动功能来快速检测总部主链路的连通性
#
dialer-rule  //配置拨号访问组，指定允许所有的IPv4报文通过
 dialer-rule 1 ip permit
#
ip route-static 0.0.0.0 0.0.0.0 Dialer0  //配置静态路由
#
nqa test-instance user test  //NQA测试例
 test-type icmp  //配置NQA测试例的测试类型为ICMP
 destination-address ipv4 5.1.1.2
 frequency 20  //配置NQA测试例自动执行测试的时间间隔
 probe-count 5  //配置一次测试的探针数
 source-interface Dialer0  //配置发送测试报文的源接口
 start now  //立即启动执行当前测试例
```

 版权所有 © 华为技术有限公司

```
#
return
```

- 配置HQ2

```
#
 sysname HQ2
#
 dns resolve  //使能DNS域名解析功能来解析总部网关地址
 dns server 5.1.1.2  //配置DNS服务器的IP地址
#
ddns policy ddnspolicy1  //配置DDNS策略来更新域名对应IP地址
 url oray://username1:password1@phddnsdev.oray.net  //配置DDNS服务器的URL
#
ipsec proposal def  //配置IPSec提议
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-192
#
ike proposal 1  //配置IPSec IKE提议
 encryption-algorithm aes-cbc-128
 authentication-algorithm sha2-256
#
ike peer branch v2  //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 pre-shared-key cipher %^%#JvZxR2g8c;a9~FPN~n'$7`DEV&=G(=Et02P/%\*!%^%#  //配置预共享密钥认证字为“YsHsjx_202206”，以密文显示，该命令在V2R3C00以前的版本中为“pre-shared-key YsHsjx_202206”，以明文显示
 ike-proposal 1
 nat traversal  //使能NAT穿越功能。V200R008版本，设备默认使能NAT穿越功能，不支持配置此命令；但V200R008之后版本，支持配置此命令
 dpd type periodic  //指定检测模式为周期性地进行检测
 dpd retransmit-interval 10  //设置DPD报文重传间隔为10秒
#
ipsec policy-template use1 10  //配置IPSec策略模板
 ike-peer branch
 proposal def
#
ipsec policy branch 1 isakmp template use1 //指定安全策略中引用策略模板
#
interface Dialer0 //配置拨号口相关参数
 link-protocol ppp
 ppp pap local-user user@huawei.com password cipher %@%@ZX}=YK.{rUa.K#7W\==O)+[c%@%@
 ip address ppp-negotiate
 dialer user huawei
 dialer bundle 1  //指定共享DCC的Dialer接口使用的Dialer bundle
 dialer-group 1  //将接口置于一个拨号访问组中
 ddns policy ddnspolicy1  //拨号口上应用DDNS策略，使其接口IP地址发生变化时，能向DDNS服务器发送动态更新
 ipsec policy branch  //绑定IPSec策略
#
interface GigabitEthernet1/0/0
 pppoe-client dial-bundle-number 1 //绑定拨号口，建立PPPoE会话
#
interface GigabitEthernet2/0/0
 ip address 10.1.0.2 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.0.10  //配置VRRP组1的虚地址10.1.0.10
 vrrp vrid 1 priority 90  //配置VRRP组1的优先级为90，使HQ2成为Backup
 vrrp vrid 1 track nqa user test reduced 40 //配置VRRP与NQA联动功能来检测总部备链路的连通性
#
dialer-rule  //配置拨号访问组，指定允许所有的IPv4报文通过
 dialer-rule 1 ip permit
#
ip route-static 0.0.0.0 0.0.0.0 Dialer0  //配置静态路由
#
nqa test-instance user test  //NQA测试例
 test-type icmp  //配置NQA测试例的测试类型为ICMP
```

 版权所有 © 华为技术有限公司

```
 destination-address ipv4 5.1.1.2
 frequency 20  //配置NQA测试例自动执行测试的时间间隔
 probe-count 5  //配置一次测试的探针数
 source-interface Dialer0  //配置发送测试报文的源接口
 start now  //立即启动执行当前测试例
#
return
```

- 配置AR1

```
#
 sysname AR1
#
 dns resolve  //使能DNS域名解析功能来解析总部网关地址
 dns server 5.1.1.2  //配置DNS服务器的IP地址
#
acl number 3000  //配置ACL
 rule 0 permit ip source 10.1.1.0 0.0.0.255 destination 10.1.0.0 0.0.0.255
#
ipsec proposal def  //配置IPSec提议
 esp authentication-algorithm sha2-256
 esp encryption-algorithm aes-192
#
ike proposal 1  //配置IPSec IKE提议
 encryption-algorithm aes-cbc-128
 authentication-algorithm sha2-256
#
ike peer center v2  //配置IKE对等体及其使用的协议时，不同的软件版本间的配置有差异：V200R008之前的版本命令为ike peer peer-name [ v1 | v2 ]。V200R008及之后的版本命令为ike peer peer-name和version { 1 | 2 }，如果对等体IKEv1和IKEv2版本同时启用，设备发起协商时会使用IKEv2协议，响应协商时则同时支持IKEv1协议和IKEv2协议。自V200R008版本到V200R021版本，缺省情况下，对等体IKEv1和IKEv2同时启用。如果设备需要使用IKEv1协议，则可以执行命令undo version 2；V200R021及之后版本，缺省情况下，启用对等体IKEv2版本。如果设备需要使用IKEv1协议，需要先执行命令version 1，再执行命令undo version 2。
 pre-shared-key cipher %^%#IRFGEiFPJ1$&a'Qy,L*XQL_+*Grq-=yMb}ULZdS6%^%#  //配置预共享密钥认证字为“YsHsjx_202206”，以密文显示，该命令在V2R3C00以前的版本中为“pre-shared-key YsHsjx_202206”，以明文显示
 ike-proposal 1
 nat traversal  //使能NAT穿越功能。V200R008版本，设备默认使能NAT穿越功能，不支持配置此命令；但V200R008之后版本，支持配置此命令
 dpd type periodic  //指定检测模式为周期性地进行检测
 dpd retransmit-interval 10  //设置DPD报文重传间隔为10秒
 remote-address store1.huawei.com track nqa user test1 up //指定当NQA测试例状态为Up时，可使用本域名作为对端的地址进行协商
 remote-address store2.huawei.com track nqa user test1 down //指定当NQA测试例状态为Down时，可使用本域名作为对端的地址进行协商
 switch-back enable
#
ipsec policy center1 1 isakmp  //配置IPSec策略
 security acl 3000
 ike-peer center
 proposal def
 connect track nqa user test up  //指定当NQA测试例的状态为Up时，使用此安全策略建立IPSec隧道
 disconnect track nqa user test down //指定当NQA测试例的状态为Down时，拆除使用该安全策略建立的IPSec隧道
#
ipsec policy center2 1 isakmp  //配置IPSec策略
 security acl 3000
 ike-peer center
 proposal def
 connect track nqa user test down  //指定当NQA测试例的状态为Down时，使用此安全策略建立IPSec隧道
 disconnect track nqa user test up //指定当NQA测试例的状态为Up时，拆除使用该安全策略建立的IPSec隧道
#
interface GigabitEthernet1/0/0
 ip address 10.2.1.2 255.255.255.0
 ipsec policy center1  //绑定IPSec策略
#
interface GigabitEthernet2/0/0
 ip address 10.1.1.1 255.255.255.0
```

 版权所有 © 华为技术有限公司

```
#
interface Cellular0/0/0
 dialer enable-circular
 dialer-group 1
 dialer timer idle 180
 dialer timer autodial 10
 dialer number *99#
 ipsec policy center2
 ip address negotiate
#
ip route-static 0.0.0.0 0.0.0.0 Cellular0/0/0 preference 200 //配置静态路由使其为备份路由
ip route-static 0.0.0.0 0.0.0.0 10.2.1.1 track nqa user test //配置静态路由使其为主路由，并配置NQA检测
ip route-static 5.1.1.2 255.255.255.0 10.2.1.1 //配置静态路由使得与5.1.1.2地址互通
#
dialer-rule  //配置拨号访问组，指定允许所有的IPv4报文通过
 dialer-rule 1 ip permit
#
nqa test-instance user test  //NQA测试例
 test-type icmp   //配置NQA测试例的测试类型为ICMP
 destination-address ipv4 5.1.1.2  //指定公网稳定的IP地址用于检测连通性
 frequency 20   //配置NQA测试例自动执行测试的时间间隔
 probe-count 5  //配置一次测试的探针数
 source-interface GigabitEthernet1/0/0   //配置发送测试报文的源接口
nqa test-instance user test1
 test-type icmp
 destination-address ipv4 3.1.1.1 // 指定HQ1公网地址
 frequency 20
 probe-count 5
#
return
```

20.3 配置 SPR 实现语音业务智能选路示例

智能策略路由简介

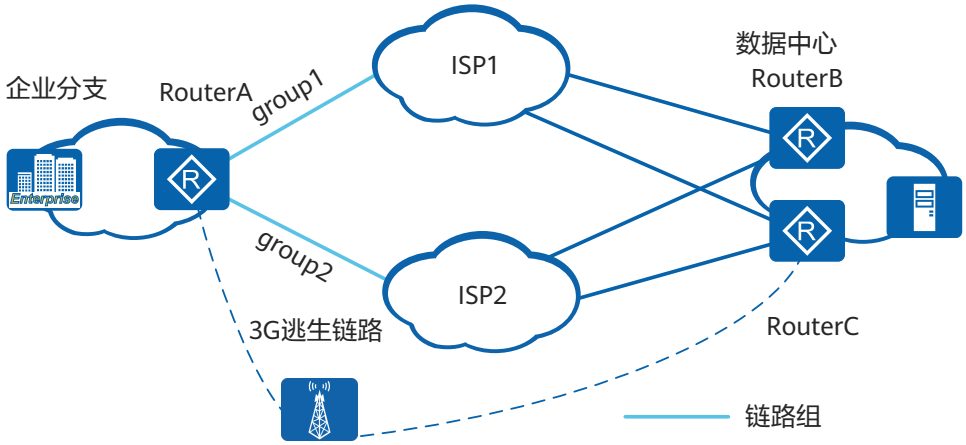
智能策略路由SPR（Smart Policy Routing）是基于业务需求的策略路由。随着网络业务需求的多样化，业务数据的集中放置，链路质量对网络业务越来越重要。越来越多的用户把关注点从网络的连通性转移到业务的可用性上，如响应速度和业务质量等。这些复杂的业务需求给传统的基于逐跳的路由协议提出了挑战，这些传统的路由协议无法感知链路质量和业务需求，即使链路质量已经很差甚至无法正常转发报文，只要路由可达，也会继续选择该链路转发报文，所以无法保障业务的用户体验。

智能策略路由就是在这一背景下产生的一种策略路由，它可以主动探测链路质量并匹配业务的需求，从而选择一条最优链路转发业务数据，可以有效的避免网络黑洞、网络震荡等问题。

智能策略路由常见场景是基于链路质量信息为不同业务数据流（比如数据、语音或视频业务）选择最佳链路。如图1所示，企业分支和数据中心通过ISP1、ISP2的网络互连，并且配置了3G出口作为逃生链路。其中，RouterA通过链路组group1与ISP1网络相连，ISP1提供优质的网络服务价格昂贵；RouterA通过链路组group2与ISP2网络相连，ISP2提供的网络服务价格相对较便宜，但网络质量相对较差。企业分支和数据中心交互的业务有语音、视频、FTP和HTTP四种业务。语音和视频业务对链路质量要求较高，因而选用group1链路组作为主链路组，group2链路组作为备用链路组；FTP和HTTP业务对链路质量要求较低，因而选用group2链路组作为主链路组，group1链路组作为备用链路组。当语音、视频、FTP和HTTP等业务无法从group1和group2链路组找到合适的链路，可以启用3G逃生链路。

 版权所有 © 华为技术有限公司

图 20-5 智能策略路由场景图



接口备份与NQA、BFD或路由联动功能根据链路连通性来选择链路，它们无法感知链路的质量和业务的需求，只要链路可通，即使链路质量很差也可用于业务传输。而智能策略路由则根据不同业务对时延、抖动、丢包率的需求来选择链路，它可以主动探测链路质量，并且依据链路质量来匹配不同业务的质量需求，从而选择一条最优链路转发相应业务的数据。

配置注意事项

1. 本例适用于V300R003C00及其之后版本的所有AR路由器。
2. 只有ADSL接口、工作在ATM模式的VDSL接口和工作在ATM模式的G.SHDSL接口支持ATM特性，这些接口可以作为ATM接口配置IPoA、IPoEoA、PPPoA或PPPoEoA等业务。
   - 1ADSL-A/M、1ADSL-B/J单板可以提供ADSL接口，4G.SHDSL、1GBIS4W单板可以提供G.SHDSL接口，VDSL2单板可以提供VDSL接口。

   说明

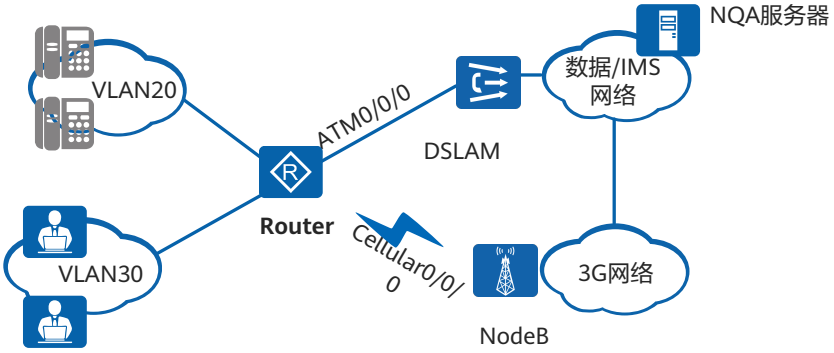
   本例不涉及接口自身属性的配置。

组网需求

如图2所示，Router作为企业出口网关，下接用户PC和IP话机，上行通过一个ATM接口和一个3G接口接入数据/IMS网络。

版权所有 © 华为技术有限公司

图 20-6 有线、无线融合智能选路示例图



为了满足企业发展需要，企业希望Router能同时传输数据业务和语音业务。由于租用的ATM链路质量不稳定，为了保证语音业务和数据业务的传输质量，企业还有如下需求：

1. Router能够为企业内网中的用户PC和IP话机分配IP地址。
2. 数据流量和语音流量都有各自的备份链路，以保证流量传输的可靠性。
3. 语音流量能够及时根据链路的时延、抖动、丢包率的变化情况动态切换传输链路，以满足语音流量高质量链路要求。
4. 数据流量能够根据链路的连通状态动态切换传输链路，以提高数据流量传输的可靠性。

配置思路

为了满足企业上述需求，采用如下思路进行配置：

1. 在Router上配置DHCP服务器功能，为企业内网中的用户PC和IP话机分配IP地址。
2. 为了节省成本，可以配置两个ATM子接口，让两个ATM子接口都作为主链路来分别承载数据报文和语音报文。
3. 由于语音业务可靠性要求比较高，可以对语音业务配置智能策略路由功能进行智能选路，并在SPR业务模板中配置时延、抖动、丢包率和CMI的阈值作为链路质量指标。当ATM语音子接口的时延、抖动、丢包率或CMI不满足链路质量指标时，流量自动切换到3G语音通道口；当ATM语音子接口的时延、抖动、丢包率和CMI恢复正常后，Router自动对3G语音通道口执行shutdown操作，这样语音业务又切换到ATM语音子接口。
4. 由于数据业务实时性要求相对较低，可以采用3G数据通道口配置接口备份与NQA联动功能，实时监测主链路的连通状况。当NQA探测失败时，数据流量从ATM数据子接口切换到3G数据通道口；当NQA探测成功后，3G数据通道口设置为standby状态，数据业务又切换到ATM数据子接口。

版权所有 © 华为技术有限公司

数据规划

表 20-2 数据规划表

业务	参数	说明
DHCP	• IP话机划分在VLAN20，网段为10.1.2.0/24，DNS服务器地址为4.4.4.4。 • 用户PC划分在VLAN30，网段为10.1.3.0/24，DNS服务器地址为5.5.5.5。	配置全局地址池方式。
QoS	• ACL3000匹配语音报文，语音报文重标记DSCP为加速转发ef。 • ATM链路传输语音报文最大允许带宽120kbit/s，切换到3G链路时，传输语音报文最大允许带宽128kbit/s。 • 数据报文重标记DSCP为af31。	企业根据自身网络规划调整QoS流行为参数。
ATM(IPoEoA)	• ATM0/0/0.1作为语音通道，vpi/vci是10/35；VE0/0/1的IP地址是1.1.1.1/24。 • ATM0/0/0.2作为数据通道，vpi/vci是10/36；VE0/0/2的IP地址是2.2.2.2/24。	ATM子接口使能NAT Outbound功能，进行内外网地址替换；同时，配置NAT预分类功能，将NAT转换前的私网IP信息携带到出接口。
3G	• 3G语音通道口Cellular0/0/0:1的拨号串是*99***1#，APN是imsbackup，采用PPP拨号方式。 • 3G数据通道口Cellular0/0/0:2的拨号串是*99***1#，APN是webdsl，采用WWAN拨号方式。	ATM子接口使能NAT Outbound功能，进行内外网地址替换；同时，配置NAT预分类功能，将NAT转换前的私网IP信息携带到出接口。 3G数据通道口使能接口备份联动NQA功能，联动的NQA测试例名称为data wan_connected_check。

版权所有 © 华为技术有限公司

业务	参数	说明
NQA	• NQA测试例data wan_connected_check：探测类型是ICMP，探测目的地址是11.11.11.11，探测失败比是33%，发送报文时间间隔是4秒，探测超时时间是2秒，探针是15个，自动执行时间间隔是35秒。 • NQA测试例voice wan_connected_check：探测类型是ICMP，探测目的地址是10.10.10.10，探测失败比是33%，发送报文时间间隔是4秒，探测超时时间是2秒，探针是15个，自动执行时间间隔是35秒。 • NQA测试例degrad voice_linkcheck：探测类型是UDP jitter，目的地址是22.22.22.22，目的端口是10000，使能硬件转发引擎进行发包及打时间戳，模拟语音测试编码类型是g729a，探测报文大小是64字节，源接口VE0/0/1，自动执行时间间隔是900秒。 • NQA测试例degrad voice_linkcheck_3G：探测类型是UDP jitter，目的地址是22.22.22.22，目的端口是10000，使能硬件转发引擎进行发包及打时间戳，模拟语音测试编码类型g729a，探测报文大小是64字节，源接口是Cellular0/0/0:1，自动执行时间间隔是900秒。	NQA测试例data wan_connected_check用于3G数据通道口ATM0/0/0.2联动NQA。 NQA测试例voice wan_connected_check用于语音数据通道口Cellular0/0/0:2联动NQA，作为ATM0/0/0.2的备份接口。 语音有线探测链路ATM0/0/0.1关联NQA测试例degrad voice_linkcheck；语音无线探测链路Cellular0/0/0:1关联NQA测试例degrad voice_linkcheck_3G。
智能策略路由SPR	SPR切换周期1200秒，震荡抑制周期2400秒，SPR中链路未被选中时接口自动关闭的延迟时间600秒，时延阈值是100，丢包率阈值是30，抖动阈值是30。	VE0/0/1加入主链路组，关联NQA测试例degrad voice_linkcheck；Cellular0/0/0:1加入备份链路组，关联NQA测试例degrad voice_linkcheck_3G。 SPR业务模板中配置时延、抖动、丢包率和CMI的阈值，作为链路质量指标定义链路质量。

版权所有 © 华为技术有限公司

配置文件

```
#
 sysname Router
#
dhcp enable     //使能DHCP功能
#
vlan 20     //创建划分IP话机的VLAN
vlan 30     //创建划分用户PC的VLAN
#
acl 3000    //配置匹配语音报文的ACL，表明来自10.1.2.0/24网段、目的端口范围为10000～32766的UDP报文为语音报文
 rule 0 permit udp source 10.1.2.0 0.0.0.255 destination-port range 10000 32766
acl 3001    //配置NAT Outbound引用的ACL，该ACL定义了NAT地址转换的规则
 rule 0 permit ip
#
traffic classifier 3G_voice operator or   //配置3G语音流分类
 if-match acl 3000
traffic classifier voice operator or      //配置ATM语音流分类
 if-match acl 3000
traffic classifier default-class operator or      //配置默认语音流分类
 if-match acl 3001
#
traffic behavior voice_behavior         //配置ATM语音流行为
 remark dscp ef             //重标记IP报文的DSCP优先级为加速转发ef
 statistic enable
 queue ef bandwidth 120 cbs 3000  //配置ATM语音流量最大允许带宽为120kbit/s
traffic behavior 3G_voice_behavior      //配置3G语音流行为
 remark dscp ef          //重标记IP报文的DSCP优先级为加速转发ef
 statistic enable
 queue ef bandwidth 128 cbs 3200  //配置3G语音流量最大允许带宽为128kbit/s
traffic behavior default_behavior       //配置数据流行为
 remark dscp af31        //重标记IP报文的DSCP优先级为af31
 statistic enable
#
traffic policy traffic_policy      //配置ATM流策略
 classifier voice behavior voice_behavior precedence 5 //匹配语音流分类和流行为
 classifier default-class behavior default_behavior precedence 10 //匹配数据流分类和流行为，其中数据流分类为系统缺省流分类default-class
traffic policy 3G_policy       //配置3G流策略
 classifier 3G_voice behavior 3G_voice_behavior precedence 5 //匹配语音流分类和流行为
 classifier default-class behavior default_behavior precedence 10 //匹配数据流分类和流行为，其中数据流分类为系统缺省流分类default-class
#
ip pool pool_voice         //配置IP地址池，以便为IP话机分配IP地址
 gateway-list 10.1.2.1
 network 10.1.2.0 mask 255.255.255.0   //地址池范围为10.1.2.0/24
 lease day 0 hour 0 minute 30         //IP地址租期为30分钟
 dns-list 4.4.4.4   //配置DNS服务器地址为4.4.4.4
 domain-name ims.it    //配置域名后缀
#
ip pool pool_data        //配置IP地址池，以便为用户PC分配IP地址
 gateway-list 10.1.3.1
 network 10.1.3.0 mask 255.255.255.0  //地址池范围为10.1.3.0/24
 lease day 5 hour 0 minute 0      //IP地址租期为5天
 dns-list 5.5.5.5   //配置DNS服务器地址为5.5.5.5
#
interface Vlanif20      //创建VLANIF20接口
 description *** VLAN VOICE***
 ip address 10.1.2.1 255.255.255.0
 dhcp select global       //使能采用全局地址池的DHCP服务器功能
#
interface Vlanif30       //创建VLANIF30接口
 description *** VLAN DATA ***
 ip address 10.1.3.1 255.255.255.0
 dhcp select global      //使能采用全局地址池的DHCP服务器功能
#
interface Cellular0/0/0    //进入3G接口
 link-protocol ppp
 traffic-policy 3G_policy outbound  //在3G接口出方向应用3G流策略
```

 版权所有 © 华为技术有限公司

```
 multi-apn enable              //使能多APN功能
#
interface Cellular0/0/0:1   //进入编号为1的3G通道接口
 description *** 3G VOICE ***
 link-protocol ppp
 ip address ppp-negotiate    //采用PPP协商方式动态获取IP地址
 dialer enable-circular   //使能轮询DCC功能
 dialer-group 1        //配置编号为1的拨号控制列表关联3G通道接口
 dialer timer idle 20
 dialer timer autodial 10     //配置自动拨号间隔
 dialer number *99***1#     //配置到达对端的拨号串
 qos pre-nat       //使能NAT预分类功能
 apn-profile imsbackup    //在3G通道接口下绑定APN模板
 nat outbound 3001    //配置NAT Outbound功能
#
interface Cellular0/0/0:2
 description *** 3G DATA***
 ip address negotiate   //采取WWAN协商方式动态获取IP地址
 dialer enable-circular   //使能轮询DCC功能
 dialer-group 1     //配置拨号控制列表关联3G通道接口
 dialer timer idle 20
 dialer timer autodial 10
 dialer number *99***1#    //配置到达对端的拨号串
 qos pre-nat   //使能NAT预分类功能
 standby track nqa data wan_connected_check   //配置接口备份与NQA联动功能，实时监测主链路的网络状况
 apn-profile webdsl     //在3G通道接口下绑定APN模板
 nat outbound 3001     //配置NAT Outbound功能
#
interface Atm0/0/0       //进入ATM接口
 traffic-policy traffic_policy outbound   //在ATM接口出方向应用ATM流策略
#
interface Atm0/0/0.1 p2p   //进入ATM子接口，该子接口传输语音流量
 description *** PVC ADSL VOICE ***
 pvc 10/35    //创建VPI/VCI为10/35的PVC
  map bridge Virtual-Ethernet0/0/1 //在PVC视图下引用VE0/0/1创建IPoEoA映射
#
interface Atm0/0/0.2 p2p       //进入ATM子接口，该子接口传输数据
 description *** PVC ADSL DATA***
 pvc 10/36  //创建VPI/VCI为10/36的PVC
  map bridge Virtual-Ethernet0/0/2 //在PVC视图下引用VE0/0/2创建IPoEoA映射
#
interface Virtual-Ethernet0/0/1    //配置VE0/0/1
 description *** WAN VOICE ***
 ip address 1.1.1.1 255.255.255.0
 qos pre-nat      //使能NAT预分类功能
 nat outbound 3001    //配置NAT Outbound功能
#
interface Virtual-Ethernet0/0/2    //配置VE0/0/2
 description *** WAN DATA ***
 ip address 2.2.2.2 255.255.255.0
 qos pre-nat    //使能NAT预分类功能
 nat outbound 3001  //配置NAT Outbound功能
#
dialer-rule
 dialer-rule 1 ip permit    //配置编号为1的拨号控制列表，允许所有IP报文通过
#
apn profile webdsl  //创建数据流的APN模板，模板名webdsl就是APN
apn profile imsbackup  //创建语音流的APN模板，模板名imsbackup就是APN
#
nqa test-instance data wan_connected_check      //用于3G数据通道口ATM0/0/0.2联动NQA
 test-type icmp     //配置测试例类型为ICMP
 destination-address ipv4 11.11.11.11   //配置NQA测试例的目的地址
 probe-failtimes 5
 fail-percent 33
 frequency 30
 interval seconds 4
 timeout 2
 probe-count 5
 source-interface Virtual-Ethernet0/0/2   //配置测试例源接口是VE0/0/2
```

 版权所有 © 华为技术有限公司

```
 start now
#
nqa test-instance voice wan_connected_check      //用于语音数据通道口Cellular0/0/0:2联动NQA，作为ATM0/0/0.2的备份接口
 test-type icmp     //配置测试例类型为ICMP
 destination-address ipv4 10.10.10.10   //配置NQA测试例的目的地址
 probe-failtimes 5
 fail-percent 33
 frequency 30
 interval seconds 4
 timeout 2
 probe-count 5
 source-interface Virtual-Ethernet0/0/2   //配置测试例源接口是VE0/0/2
 start now
#
nqa test-instance degrad voice_linkcheck    //创建ATM语音的NQA测试例
 test-type jitter           //配置测试例类型为Jitter
 destination-address ipv4 22.22.22.22    //配置NQA测试例的目的地址
 destination-port 10000
 hardware-based enable     //使能在进行Jitter测试时，采用接口板上的硬件转发引擎进行发包及打时间戳
 frequency 900
 jitter-codec g729a
 datasize 64
 source-interface Virtual-Ethernet0/0/1   //配置测试例源接口是VE0/0/1
 start now
#
nqa test-instance degrad voice_linkcheck_3G    //创建3G语音的NQA测试例
 test-type jitter   //配置测试例类型为Jitter
 destination-address ipv4 22.22.22.22  /配置NQA测试例的目的地址
 destination-port 10000
 hardware-based enable   //使能在进行Jitter测试时，采用接口板上的硬件转发引擎进行发包及打时间戳
 frequency 900
 jitter-codec g729a
 datasize 64
 source-interface Cellular0/0/0:1    //配置测试例源接口是编号为1的3G通道口
 start now
#
smart-policy-route    //创建智能策略路由，并进入智能策略路由视图
 period 1200
 wtr period hours 2 //配置SPR从备份链路回切到主链路的时间
 route flapping suppression 2400
 prober Virtual-Ethernet0/0/1 nqa degrad voice_linkcheck    //配置SPR中探测链路，将VE0/0/1关联名为degrad voice_linkcheck的NQA测试例
 prober Cellular0/0/0:1 nqa degrad voice_linkcheck_3G    //配置SPR中探测链路，将Cellular0/0/0:1关联名为degrad voice_linkcheck_3G的NQA测试例
 standby-interface Cellular0/0/0:1   // 配置接口Cellular0/0/0:1在SPR中链路未被选中时可以自动关闭
 standby-limit-time 600
 link-group group1    //创建名为group1的链路组
  link-member Virtual-Ethernet0/0/1   //将探测链路接口VE0/0/1加入链路组group1
 link-group group2     //创建名为group2的链路组
  link-member Cellular0/0/0:1  //将探测链路接口Cellular0/0/0:1加入链路组group2
 service-map voice      // 创建SPR的业务模板并进入业务模板视图
  cmi-method d+l+j      //配置CMI计算公式，该CMI值取决于链路的时延、抖动和丢包率。其中，d代表时延，j代表抖动时间，l代表丢包率
  match acl 3000    //配置将ACL3000与业务模板绑定，表明区分出语音业务流
  set delay threshold 100   //配置SPR中业务的时延阈值。当链路的时延大于业务时延阈值时，则链路不满足业务对时延的要求
  set loss threshold 30   //配置SPR中业务的丢包率阈值。当链路的丢包率大于业务丢包率阈值时，则链路不满足该业务对丢包率的要求
  set jitter threshold 30    //配置SPR中业务的抖动阈值。当链路的抖动大于业务的抖动阈值时，则链路不满足业务对抖动时间的要求
  set cmi threshold 8840   //配置CMI阈值，当CMI值小于该阈值时，则认为链路的综合度量指标不满足业务的需求
  set link-group group1   //配置group1为主链路组
  set link-group group2 backup   //配置group2为备份链路组
#
```

 版权所有 © 华为技术有限公司