

配置手册

MTS 系列交换机

即使没有特别说明，本手册中对版权商标的命名也不应该被认为是指这些名称在商标和商号保护法的意义上被认为是免费的，因此也不得认为它们可以被任何人自由使用。

© 2020, Belden Singapore Pte Ltd

手册和软件受版权保护。保留所有权利。不得全部或部分复制、复印、翻译、转换成任何电子媒体或机器可扫描格式。为您自己使用而制作备份软件是例外。对于具有嵌入式软件的设备，适用随附的CD/DVD上的最终用户许可协议。

本文描述的性能特点只有在合同签订时已经明确商定时才具有约束力。本文件由 Belden 尽可能根据本公司所掌握的情况制作而成。Belden 保留更改本文件内容的权利，恕不另行通知。Belden 不保证本文件中信息的正确性或准确性。

对于因使用网络组件或相关操作软件而导致的损害，Belden 不承担任何责任。另外，我们还援引许可合同中规定的使用条件。

您可以通过Internet 在 Hirschmann IT 产品网站上获得本手册的最新版本

(网址为 www.belden.com) 。

安全约定

安全管理

默认的，设备应当放置在安全、可靠的位置；所有的物理访问者都应是得到授权的操作员；使用的命令行脚本应当得到妥善的保管、更新和审核。

安全传输

Hirschmann IT 设备支持多种管理方式，包括 Telnet, SSH, HTTP, HTTPS 等，任何非加密的管理方式都是不推荐的。我们强烈建议我们的用户仅使用 SSH 和 HTTPS 作为管理途径，以确保所有的管理流量都是加密的。

安全存储

登录设备使用的凭据、设备的配置和状态数据，应当被保管在合适的地方并定期更新，并且仅有有限的人可以查阅和管理。

目录

安全约定	3
安全指示	37
关于本手册	38
系统基础及管理	39
1 系统操作基础	39
1.1 系统操作基础简介	39
1.2 系统操作基础功能	39
1.2.1 设备配置方式 -B -S -E -A	40
1.2.2 命令运行模式 -B -S -E -A	40
1.2.3 命令行接口 -B -S -E -A	43
2 系统登录	47
2.1 系统登录简介	47
2.2 系统登录功能配置	48
2.2.1 通过 CONSOLE 口登录设备 -B -S -E -A	48
2.2.2 配置 TELNET 远程登录 -B -S -E -A	51
2.2.3 配置 SSH 远程登录 -B -S -E -A	52
2.2.4 系统登录监控与维护 -B -S -E -A	54
2.3 系统登录典型配置举例	55
2.3.1 配置本地终端 TELNET 登录设备 -B -S -E -A	55
2.3.2 配置通过本地设备 TELNET 登录到远端设备 -B -S -E -A	56
2.3.3 配置通过本地设备 SSH 登录到远端设备 -B -S -E -A	58
2.3.4 配置设备作为 SFTP 客户端 -B -S -E -A	59
2.3.5 配置设备作为 SFTP 服务器 -B -S -E -A	61
3 登录控制与管理	62
3.1 登录控制与管理简介	63
3.2 登录控制与管理功能配置	63

3.2.1	切换用户级别 -B -S -E -A	64
3.2.2	配置命令级别 -B -S -E -A	66
3.2.3	配置 ENABLE 密码 -B -S -E -A	67
3.2.4	配置 LINE 属性 -B -S -E -A	67
3.2.5	登录控制与管理监控与维护 -B -S -E -A	74
4	FTP、FTPS、TFTP 和 SFTP 简介	74
4.1	FTP、FTPS、TFTP 和 SFTP 功能配置	76
4.1.1	配置 FTP 服务器 -B -S -E -A	76
4.1.2	配置 FTP 客户端 -B -S -E -A	77
4.1.3	配置 TFTP 客户端 -B -S -E -A	79
4.1.4	配置 TFTP 服务器 -B -S -E -A	80
4.1.5	配置 SFTP 服务器 -B -S -E -A	80
4.1.6	配置 SFTP 客户端 -B -S -E -A	81
4.1.7	FTP 和 TFTP 监控与维护 -B -S -E -A	82
4.2	FTP 和 TFTP 典型配置举例	82
4.2.1	配置设备作为 FTP 客户端 -B -S -E -A	82
4.2.2	配置设备作为 FTP 服务器 -B -S -E -A	83
4.2.3	配置设备作为 TFTP 客户端 -B -S -E -A	87
4.2.4	配置设备作为 SFTP 客户端 -B -S -E -A	88
4.2.5	配置设备作为 SFTP 服务器 -B -S -E -A	89
4.2.6	配置设备作为 FTPS 客户端 -B -S -E -A	91
5	文件系统管理	95
5.1	文件系统管理简介	95
5.2	文件系统管理功能配置	96
5.2.1	存储设备管理 -B -S -E -A	96
5.2.2	文件目录管理 -B -S -E -A	98
5.2.3	文件操作管理 -B -S -E -A	100
5.2.4	从 FTP 下载文件 -B -S -E -A	102

5.2.5	配置启动参数 -B -S -E -A	103
5.2.6	文件系统管理监控与维护 -B -S -E -A	103
5.3	文件系统管理典型配置举例	104
5.3.1	配置启动参数 -B -S -E -A	104
6	配置文件管理	105
6.1	配置文件管理简介	105
6.2	配置文件管理功能配置	106
6.2.1	保存当前配置 -B -S -E -A	106
6.2.2	备份系统配置 -B -S -E -A	107
6.2.3	恢复启动配置 -B -S -E -A	109
6.2.4	配置文件管理监控与维护 -B -S -E -A	110
6.2.5	配置文件加密 -B -S -E -A	111
7	系统管理	112
7.1	系统管理简介	113
7.2	系统管理功能配置	113
7.2.1	配置设备名称 -B -S -E -A	114
7.2.2	配置系统时间和时区 -B -S -E -A	114
7.2.3	配置登录欢迎信息 -B -S -E -A	115
7.2.4	配置系统异常处理方式 -B -S -E -A	116
7.2.5	配置设备重启 -B -S -E -A	117
7.2.6	配置历史命令保存功能 -B -S -E -A	118
7.2.7	配置登录安全服务 -B -S -E -A	119
7.2.8	配置 CPU 监控 -B -S -E -A	120
7.2.9	配置分页显示属性 -B -S -E -A	121
7.2.10	操作记录文件管理 -B -S -E -A	122
7.2.11	系统管理监控与维护 -B -S -E -A	122
7.3	系统管理典型配置举例	124
7.3.1	配置基于用户、IP 的登陆限制 -B -S -E -A	124

7.3.2	配置快速登陆限制 -B -S -E -A	127
8	系统告警	128
8.1	系统告警简介	128
8.2	系统告警功能配置	128
8.2.1	配置系统温度告警 -B -S -E -A	129
8.2.2	配置系统 CPU 告警 -B -S -E -A	130
8.2.3	配置内存使用门限低值 -B -S -E -A	130
8.2.4	配置系统内存告警 -B -S -E -A	131
8.2.5	配置系统电源告警 -B -S -E -A	132
8.2.6	配置系统风扇告警 -B -S -E -A	132
9	系统日志配置	133
9.1	日志简介	133
9.2	日志功能配置	135
9.2.1	配置日志输出功能 -B -S -E -A	135
9.2.2	配置日志时间戳 -B -S -E -A	141
9.2.3	配置操作日志发送到日志主机 -B -S -E -A	142
9.2.4	配置日志重复抑制 -B -S -E -A	143
9.2.5	配置日志文件容量 -B -S -E -A	144
9.2.6	配置日志文件加密 -B -S -E -A	144
9.2.7	配置日志显示颜色 -B -S -E -A	145
9.2.8	日志监控与维护 -B -S -E -A	146
10	软件升级	147
10.1	软件升级简介	147
10.2	软件升级功能配置	148
10.2.1	IMAGE 程序包升级 -B -S -E -A	148
10.2.2	BOOTLOADER 程序升级 -B -S -E -A	150
10.2.3	打包文件升级 -B -S -E -A	154
10.3	软件升级典型配置举例	156

目录

10.3.1	升级软件版本 -B -S -E -A	156
10.3.2	全面升级所有软件版本 -B -S -E -A	158
10.3.3	使用 CONSOLE 口升级 BOOTLOADER -B -S -E -A	161
11	BOOTLOADER	163
11.1	BOOTLOADER 简介	163
11.2	BOOTLOADER 功能配置	163
11.2.1	BOOTLOADER 功能配置前准备 -B -S -E -A	164
11.2.2	进入 BOOTLOADER 配置模式 -B -S -E -A	164
11.2.3	设置 BOOTLOADER 启动参数 -B -S -E -A	165
11.2.4	升级 BOOTLOADER 程序 -B -S -E -A	166
11.2.5	BOOTLOADER 监控与维护 -B -S -E -A	168
11.3	BOOTLOADER 典型配置举例	168
11.3.1	配置 BOOTLOADER 通过网络启动 IMAGE 程序 -B -S -E -A	168
12	POE 管理	169
12.1	PoE 简介	169
12.1.1	PSE/PD 接口标准 -S -E -A	170
12.1.2	PoE 供电过程 -S -E -A	171
12.2	PoE 功能配置	172
12.2.1	配置 PoE 基本功能 -S -E -A	173
12.2.2	配置 PoE 功率 -S -E -A	176
12.2.3	配置供电优先级 -S -E -A	179
12.2.4	配置 PD 上电断电参数 -S -E -A	180
12.2.5	配置异常恢复功能 -S -E -A	184
12.2.6	配置 PoE 功率告警阈值 -S -E -A	186
12.2.7	PoE 监控与维护 -S -E -A	186
13	LUM	187
13.1	LUM 简介	187
13.2	LUM 功能配置	188

目录

13.2.1	配置角色 -B-S-E-A	188
13.2.2	配置本地用户 -B-S-E-A	190
13.2.3	配置管理员用户属性 -B-S-E-A	191
13.2.4	配置接入用户属性 -B-S-E-A	194
13.2.5	配置本地用户组 -B-S-E-A	195
13.2.6	配置密码策略 -B-S-E-A	197
13.2.7	LUM 监控与维护 -B-S-E-A	200
13.3	LUM 典型配置举例	200
13.3.1	配置网络管理员用户 -B-S-E-A	200
	接口	203
14	接口基础	203
14.1	接口基础简介	203
14.2	接口基础功能配置	204
14.2.1	配置接口基本功能 -B-S-E-A	204
14.2.2	配置接口组功能 -B-S-E-A	208
14.2.3	配置接口状态 SNMP 代理关心层次 -B-S-E-A	209
14.2.4	接口基础监控与维护 -B-S-E-A	210
15	以太网接口	211
15.1	以太网接口简介	211
15.2	以太网接口功能配置	212
15.2.1	配置以太网接口基本功能 -B-S-E-A	213
15.2.2	配置以太网接口检测功能 -B-S-E-A	222
15.2.3	配置二层以太网接口风暴抑制 -B-S-E-A	224
15.2.4	配置 UNI/NNI 类型 -B-S-E-A	226
15.2.5	配置三层以太网接口基本功能 -B-S-E-A	228
15.2.6	以太网接口监控与维护 -B-S-E-A	230
15.3	以太网接口典型配置举例	231
15.3.1	配置风暴抑制功能 -B-S-E-A	231

16	汇聚组接口	233
16.1	汇聚组接口简介	233
16.2	汇聚组接口功能配置	233
16.2.1	配置汇聚组接口基本功能 -B -S -E -A	233
16.2.2	汇聚组接口监控与维护 -B -S -E -A	235
17	VLAN 接口	236
17.1	VLAN 接口简介	236
17.2	VLAN 接口功能配置	236
17.2.1	配置 VLAN 接口基本功能 -B -S -E -A	236
17.2.2	VLAN 接口监控与维护 -B -S -E -A	239
17.3	VLAN 接口典型配置举例	239
17.3.1	配置 VLAN 接口 -B -S -E -A	239
18	LOOPBACK 接口	241
18.1	LOOPBACK 接口简介	242
18.2	LOOPBACK 接口功能配置	242
18.2.1	配置 LOOPBACK 接口基本功能 -B -S -E -A	242
19	NULL 接口	244
19.1	NULL 接口简介	244
19.2	NULL 接口功能配置	245
19.2.1	配置 NULL 接口基本功能 -S -E -A	245
20	虚拟交换链路接口	246
20.1	虚拟交换链路接口简介	246
20.2	虚拟交换链路接口功能配置	246
20.2.1	配置虚拟交换链路接口功能 -B -S -E -A	246
20.2.2	虚拟交换链路接口监控与维护 -B -S -E -A	247
	以太网交换	248
21	链路汇聚	248
21.1	链路汇聚简介	248

21.1.1	基本概念	248
21.1.2	链路汇聚的模式 -B -S -E -A	250
21.2	负载均衡模板简介	251
21.2.1	负载均衡 -B -S -E -A	251
21.2.2	HASH KEY -B -S -E -A	252
21.2.3	负载均衡模板 -B -S -E -A	254
21.3	负载均衡模板功能配置	254
21.3.1	创建负载均衡模板 -B -S -E -A	255
21.3.2	配置负载均衡模板的 HASH KEY -B -S -E -A	255
21.3.3	删除负载均衡模板 -B -S -E -A	258
21.4	链路汇聚功能配置	258
21.4.1	配置汇聚组 -B -S -E -A	259
21.4.2	配置汇聚组引用负载均衡模板 -B -S -E -A	262
21.4.3	配置 LACP 优先级 -B -S -E -A	262
21.4.4	配置热插拔快速切换根端口 -B -S -E -A	263
21.4.5	链路汇聚监控与维护 -B -S -E -A	264
21.5	链路汇聚典型配置举例	265
21.5.1	配置静态汇聚组 -B -S -E -A	265
21.5.2	配置动态汇聚组 -B -S -E -A	268
22	端口隔离	273
22.1	端口隔离简介	273
22.2	端口隔离功能配置	273
22.2.1	配置端口隔离基本功能 -B -S -E -A	274
22.2.2	配置汇聚组成员端口隔离功能 -B -S -E -A	275
22.2.3	端口隔离监控与维护 -B -S -E -A	276
22.3	端口隔离典型配置举例	277
22.3.1	配置端口隔离 -B -S -E -A	277
23	VLAN	279

23.1 VLAN 简介	279
23.2 VLAN 功能配置	280
23.2.1 配置 VLAN 基本属性 -B -S -E -A.....	281
23.2.2 配置基于端口的 VLAN -B -S -E -A.....	283
23.2.3 配置基于 MAC 的 VLAN -B -S -E -A.....	288
23.2.4 配置基于 IP 子网的 VLAN -B -S -E -A.....	289
23.2.5 配置基于协议的 VLAN -B -S -E -A.....	291
23.2.6 配置端口的可接收帧类型 -B -S -E -A.....	292
23.2.7 VLAN 监控与维护 -B -S -E -A.....	293
23.3 VLAN 典型配置举例	294
23.3.1 配置基于端口的 VLAN -B -S -E -A.....	294
23.3.2 配置基于 MAC 的 VLAN -B -S -E -A.....	296
23.3.3 配置基于 IP 子网的 VLAN -B -S -E -A.....	298
23.3.4 配置基于协议的 VLAN -B -S -E -A.....	300
24 SUPER-VLAN	302
24.1 SUPER-VLAN 简介	302
24.2 SUPER-VLAN 功能配置	303
24.2.1 配置 SUPER-VLAN -S -E -A.....	303
24.2.2 配置 SUPER-VLAN 的 SUB-VLAN 成员 -S -E -A.....	304
24.2.3 使能 ARP 代理功能 -S -E -A.....	305
24.2.4 SUPER-VLAN 监控与维护 -S -E -A.....	306
24.3 SUPER-VLAN 典型配置举例	306
24.3.1 配置 SUPER-VLAN -S -E -A.....	306
25 VOICE-VLAN	309
25.1 VOICE-VLAN 简介	309
25.2 VOICE-VLAN 功能配置	310
25.2.1 配置 VOICE-VLAN -B -S -E -A.....	310
25.2.2 配置 OUI 地址 -B -S -E -A.....	311

25.2.3	使能端口的 VOICE-VLAN 功能 -B -S -E -A	312
25.2.4	配置端口的 VOICE-VLAN 工作模式 -B -S -E -A	313
25.2.5	使能 VOICE-VLAN 的安全模式 -B -S -E -A	315
25.2.6	使能 VOICE-VLAN 的 LLDP-MED 认证模式 -B -S -E -A	316
25.2.7	VOICE-VLAN 监控与维护 -B -S -E -A	317
25.3	VOICE-VLAN 典型配置举例	318
25.3.1	配置 VOICE-VLAN 手动模式 -B -S -E -A	318
25.3.2	配置 VOICE-VLAN 自动模式 -B -S -E -A	320
25.3.3	配置 VOICE-VLAN 安全模式 -B -S -E -A	322
25.3.4	配置 VOICE-VLAN LLDP-MED 认证模式 -B -S -E -A	324
26	MAC 地址表管理	326
26.1	MAC 地址管理简介	326
26.2	MAC 地址管理功能配置	327
26.2.1	配置 MAC 地址管理属性 -B -S -E -A	328
26.2.2	配置 MAC 地址学习限制 -B -S -E -A	331
26.2.3	配置静态 MAC 地址 -B -S -E -A	334
26.2.4	MAC 地址管理监控与维护 -B -S -E -A	336
26.3	MAC 地址迁移日志功能配置	337
26.3.1	MAC 地址迁移日志功能配置 -B -S -E -A	337
26.3.2	MAC 地址迁移日志功能监控与维护 -B -S -E -A	338
27	生成树	339
27.1	生成树简介	339
27.2	生成树功能配置	343
27.2.1	配置生成树基本功能 -B -S -E -A	345
27.2.2	配置网桥属性 -B -S -E -A	347
27.2.3	配置生成树端口属性 -B -S -E -A	350
27.2.4	配置生成树工作模式 -B -S -E -A	359
27.2.5	配置生成树保护功能 -B -S -E -A	360

27.2.6	生成树监控与维护 -B -S -E -A	366
27.3	生成树典型配置举例	367
27.3.1	MSTP 典型应用 -B -S -E -A	367
28	环回检测	373
28.1	环回检测简介	373
28.2	环回检测功能配置	374
28.2.1	配置环回检测基本功能 -B -S -E -A	374
28.2.2	配置环回检测基本参数 -B -S -E -A	376
28.2.3	环回检测监控与维护 -B -S -E -A	378
28.3	环回检测典型配置举例	378
28.3.1	配置远端环回检测 -B -S -E -A	378
28.3.2	配置本端环回检测 -B -S -E -A	382
29	ERROR-DISABLE 管理	385
29.1	ERROR-DISABLE 管理简介	385
29.2	ERROR-DISABLE 管理功能配置	386
29.2.1	配置 ERROR-DISABLE 管理基本功能 -B -S -E -A	386
29.2.2	配置 ERROR-DISABLE 自动恢复 -B -S -E -A	387
29.2.3	ERROR-DISABLE 管理监控与维护 -B -S -E -A	388
29.3	ERROR-DISABLE 管理典型配置举例	389
29.3.1	ERROR-DISABLE 与风暴抑制联用 -B -S -E -A	389
IP 协议及业务		392
30	ARP	392
30.1	ARP 简介	392
30.2	ARP 功能配置	392
30.2.1	配置 ARP 基本功能 -B -S -E -A	393
30.2.2	ARP 监控与维护 -B -S -E -A	398
30.3	ARP 典型配置举例	398
30.3.1	配置 ARP 代理 -B -S -E -A	398

30.3.2 配置静态 ARP -B -S -E -A	399
31 IP 基础	401
31.1 IP 基础简介	401
31.2 IP 基础功能配置	402
31.2.1 配置 IP 地址 -B -S -E -A	403
31.2.2 配置 IP 协议基本功能 -B -S -E -A	406
31.2.3 配置 ICMP 协议基本功能 -B -S -E -A	409
31.2.4 配置 TCP 协议基本功能 -B -S -E -A	413
31.2.5 配置 TCP 协议防攻击功能 -B -S -E -A	418
31.2.6 配置 UDP 协议基本功能 -B -S -E -A	419
31.2.7 IP 基础监控与维护 -B -S -E -A	422
32 DHCP	423
32.1 DHCP 简介	423
32.2 DHCP 功能配置	424
32.2.1 配置 DHCP 地址池 -S -E -A	426
32.2.2 配置 DHCP 服务器其它参数 -S -E -A	431
32.2.3 配置 DHCP 客户端功能 -S -E -A	433
32.2.4 配置 DHCP 中继功能 -S -E -A	435
32.2.5 DHCP 监控与维护 -S -E -A	439
32.3 DHCP 典型配置举例	440
32.3.1 配置 DHCP 服务器静态分配 IP 地址 -S -E -A	440
32.3.2 配置 DHCP 服务器动态分配 IP 地址 -S -E -A	442
32.3.3 配置 DHCP 中继 -S -E -A	444
32.3.4 配置 DHCP 中继支持 OPTION82 选项 -S -E -A	446
33 DNS	448
33.1 DNS 简介	448
33.2 DNS 功能配置	449
33.2.1 配置 DNS 缓存规格 -B -S -E -A	449

33.2.2	配置 DNS 客户端功能 -B -S -E -A	450
33.2.3	配置 DNS 探测功能 -B -S -E -A	451
33.2.4	DNS 监控与维护 -B -S -E -A	453
33.3	DNS 典型配置举例	453
33.3.1	配置静态域名解析 -B -S -E -A	453
33.3.2	配置动态域名解析 -B -S -E -A	454
34	IPV6 基础	456
34.1	IPv6 基础简介	456
34.2	IPv6 基础功能配置	456
34.2.1	配置接口 IPv6 地址 -B -S -E -A	457
34.2.2	配置 IPv6 基本功能 -B -S -E -A	461
34.2.3	配置 IPv6 邻居发现协议 -B -S -E -A	463
34.2.4	配置 ICMPV6 功能 -B -S -E -A	470
34.2.5	配置 IPv6 TCP 防攻击功能 -B -S -E -A	471
34.2.6	IPv6 基础监控与维护 -B -S -E -A	473
34.3	IPv6 基础配置举例	474
34.3.1	配置接口的 IPv6 地址 -B -S -E -A	474
34.3.2	配置 IPv6 邻居发现 -B -S -E -A	476
35	DHCPV6	479
35.1	DHCPv6 简介	479
35.2	DHCPv6 功能配置	480
35.2.1	配置 DHCPV6 地址池 -S -E -A	481
35.2.2	配置 DHCPV6 服务器其它参数 -S -E -A	485
35.2.3	配置 DHCPV6 客户端功能 -S -E -A	487
35.2.4	配置 DHCPV6 中继功能 -S -E -A	488
35.2.5	DHCPv6 监控与维护 -S -E -A	491
35.3	DHCPv6 典型配置举例	492
35.3.1	配置 DHCPV6 服务器静态分配 IPv6 地址 -S -E -A	492

35.3.2	配置 DHCPv6 服务器动态分配 IPv6 地址 -S -E -A	494
35.3.3	配置 DHCPv6 中继 -S -E -A	495
	单播路由	498
36	路由基础	498
36.1	路由基础简介	498
36.2	路由基础功能配置	498
36.2.1	配置路由负载均衡 -B -S -E -A	499
36.2.2	配置 VRF 路由容量 -E -A	499
36.2.3	路由基础监控与维护 -B -S -E -A	500
37	IPv6 路由基础	502
37.1	IPv6 路由基础简介	502
37.2	IPv6 路由基础功能配置	502
37.2.1	配置 IPv6 路由负载均衡 -B -S -E -A	503
37.2.2	IPv6 路由基础监控与维护 -B -S -E -A	503
38	静态路由	504
38.1	静态路由简介	504
38.2	静态路由功能配置	505
38.2.1	配置静态路由 -B -S -E -A	506
38.2.2	配置缺省管理距离 -B -S -E -A	508
38.2.3	配置递归功能 -B -S -E -A	508
38.2.4	配置负载均衡路由 -B -S -E -A	509
38.2.5	配置浮动路由 -B -S -E -A	510
38.2.6	配置静态路由与 BFD 联动 -E -A	511
38.2.7	配置静态路由与 TRACK 联动 -B -S -E -A	512
38.2.8	静态路由监控与维护 -B -S -E -A	513
38.3	静态路由典型配置举例	514
38.3.1	配置静态路由基本功能 -B -S -E -A	514
38.3.2	配置静态浮动路由 -B -S -E -A	516

38.3.3	配置静态 NULL0 接口路由 -S -E -A	518
38.3.4	配置静态递归路由 -B -S -E -A	520
38.3.5	配置静态路由与 BFD 联动 -E -A	522
39	RIP	525
39.1	RIP 简介	525
39.2	RIP 功能配置	526
39.2.1	配置 RIP 基本功能 -S -E -A	527
39.2.2	配置 RIP 路由生成 -S -E -A	531
39.2.3	配置 RIP 路由控制 -S -E -A	533
39.2.4	配置 RIP 网络认证 -S -E -A	539
39.2.5	配置 RIP 网络优化 -S -E -A	540
39.2.6	配置 RIP 与 BFD 联动 -E -A	546
39.2.7	RIP 监控与维护 -S -E -A	547
39.3	RIP 典型配置举例	548
39.3.1	配置 RIP 的版本 -S -E -A	548
39.3.2	配置 RIP 路由重分发 -S -E -A	550
39.3.3	配置 RIP 度量偏移 -S -E -A	553
39.3.4	配置 RIP 路由过滤 -S -E -A	556
39.3.5	配置 RIP 路由汇总 -S -E -A	558
39.3.6	配置 RIP 与 BFD 联动 -E -A	560
39.3.7	配置 RIP 备份接口 -S -E -A	563
39.3.8	配置 RIP 被动接口 -S -E -A	565
40	RIPNG	568
40.1	RIPNG 简介	568
40.2	RIPNG 功能配置	568
40.2.1	配置 RIPNG 基本功能 -E -A	569
40.2.2	配置 RIPNG 路由生成 -E -A	570
40.2.3	配置 RIPNG 路由控制 -E -A	572

40.2.4	配置 RIPNG 网络优化 -E -A	577
40.2.5	配置 RIPNG 与 BFD 联动 -E -A	581
40.2.6	RIPNG 监控与维护 -E -A	582
40.3	RIPNG 典型配置举例	583
40.3.1	配置 RIPNG 基本功能 -E -A	583
40.3.2	配置 RIPNG 路由重分发 -E -A	584
40.3.3	配置 RIPNG 度量偏移 -E -A	587
40.3.4	配置 RIPNG 路由过滤 -E -A	590
40.3.5	配置 RIPNG 路由汇总 -E -A	592
40.3.6	配置 RIPNG 被动接口 -E -A	595
41	OSPF	597
41.1	OSPF 简介	598
41.2	OSPF 功能配置	598
41.2.1	配置 OSPF 基本功能 -S -E -A	601
41.2.2	配置 OSPF 区域 -S -E -A	603
41.2.3	配置 OSPF 网络类型 -S -E -A	606
41.2.4	配置 OSPF 网络认证 -S -E -A	610
41.2.5	配置 OSPF 路由生成 -S -E -A	613
41.2.6	配置 OSPF 路由控制 -S -E -A	616
41.2.7	配置 OSPF 网络优化 -S -E -A	623
41.2.8	配置 OSPF 与 BFD 联动 -E -A	631
41.2.9	配置 OSPF GR -S -E -A	632
41.2.10	OSPF 监控与维护 -S -E -A	634
41.3	OSPF 典型配置举例	636
41.3.1	配置 OSPF 基本功能 -S -E -A	636
41.3.2	配置 OSPF 认证 -S -E -A	640
41.3.3	配置 OSPF 路由重分发 -S -E -A	645
41.3.4	配置 OSPF 多进程 -S -E -A	648

目录

41.3.5	配置 OSPF 外部路由汇总 -S -E -A	653
41.3.6	配置 OSPF 区域间路由汇总 -S -E -A	657
41.3.7	配置 OSPF 区域间路由过滤 -S -E -A	662
41.3.8	配置 OSPF 完全 STUB 区域 -S -E -A	666
41.3.9	配置 OSPF NSSA 区域 -S -E -A	669
41.3.10	配置 OSPF 与 BFD 联动 -E -A	674
42	OSPFV3	677
42.1	OSPFV3 简介	677
42.2	OSPFV3 功能配置	677
42.2.1	配置 OSPFV3 基本功能 -E -A	679
42.2.2	配置 OSPFV3 区域 -E -A	681
42.2.3	配置 OSPFV3 网络类型 -E -A	684
42.2.4	配置 OSPFV3 网络认证 -E -A	688
42.2.5	配置 OSPFV3 路由生成 -E -A	689
42.2.6	配置 OSPFV3 路由控制 -E -A	691
42.2.7	配置 OSPFV3 网络优化 -E -A	698
42.2.8	配置 OSPFV3 GR -E -A	704
42.2.9	配置 OSPFV3 与 BFD 联动 -E -A	706
42.2.10	OSPFV3 监控与维护 -E -A	707
42.3	OSPFV3 典型配置举例	709
42.3.1	配置 OSPFV3 基本功能 -E -A	709
42.3.2	配置 OSPFV3 使用 IPSEC 加密认证 -E -A	715
42.3.3	配置 OSPFV3 与 BFD 的联动 -E -A	723
43	IS-IS	727
43.1	IS-IS 简介	727
43.2	IS-IS 功能配置	727
43.2.1	配置 IS-IS 基本功能 -E -A	729
43.2.2	配置 IS-IS 层属性 -E -A	731

目录

43.2.3	配置 IS-IS 路由生成 -E -A	732
43.2.4	配置 IS-IS 路由控制 -E -A	734
43.2.5	配置 IS-IS 网络优化 -E -A	739
43.2.6	配置 IS-IS 网络认证 -E -A	750
43.2.7	配置 IS-IS 与 BFD 联动 -E -A	751
43.2.8	配置 IS-IS GR -E -A	752
43.2.9	IS-IS 监控与维护 -E -A	754
43.3	IS-IS 典型配置举例	755
43.3.1	配置 IS-IS 基本功能 -E -A	755
43.3.2	配置 IS-IS 的 DIS 选举 -E -A	759
43.3.3	配置 IS-IS 层间路由泄露 -E -A	761
43.3.4	IS-IS 路由重分发 -E -A	766
43.3.5	配置 IS-IS 邻居认证 -E -A	769
43.3.6	配置 IS-IS 与 BFD 联动 -E -A	772
44	BGP	775
44.1	BGP 简介	775
44.2	BGP 功能配置	776
44.2.1	配置 BGP 邻居 -E -A	778
44.2.2	配置 BGP 路由生成 -E -A	786
44.2.3	配置 BGP 路由控制 -E -A	789
44.2.4	配置 BGP 路由属性 -E -A	796
44.2.5	配置 BGP 网络优化 -E -A	808
44.2.6	配置 BGP 大型网络 -E -A	814
44.2.7	配置 BGP GR -E -A	817
44.2.8	配置 BGP 与 BFD 联动 -E -A	819
44.2.9	BGP 监控与维护 -E -A	821
44.2.10	BGP 监控与维护 -E -A	825
44.3	BGP 典型配置举例	828

目录

44.3.1	配置 BGP 基本功能 -E -A	828
44.3.2	配置 BGP 路由重分发 -E -A	831
44.3.3	配置 BGP 团体属性 -E -A	833
44.3.4	配置 BGP 路由反射器 -E -A	836
44.3.5	配置 BGP 路由聚合 -E -A	840
44.3.6	配置 BGP 路由优选 -E -A	844
44.3.7	配置 BGP 联盟 -E -A	851
44.3.8	配置 BGP 与 BFD 联动 -E -A	856
45	IPV6 BGP	861
45.1	IPV6 BGP 简介	861
45.2	IPV6 BGP 功能配置	861
45.2.1	配置 IPv6 BGP 邻居 -E -A	863
45.2.2	配置 IPv6 BGP 路由生成 -E -A	870
45.2.3	配置 IPv6 BGP 路由控制 -E -A	874
45.2.4	配置 IPv6 BGP 路由属性 -E -A	881
45.2.5	配置 IPv6 BGP 网络优化 -E -A	893
45.2.6	配置 IPv6 BGP 大型网络 -E -A	899
45.2.7	配置 IPv6 BGP GR -E -A	902
45.2.8	配置 IPv6 BGP 与 BFD 联动 -E -A	905
45.2.9	IPv6 BGP 监控与维护 -E -A	908
45.3	IPV6 BGP 典型配置举例	910
45.3.1	配置 IPv6 BGP 基本功能 -E -A	910
45.3.2	配置 IPv6 BGP 路由重分发 -E -A	914
45.3.3	配置 IPv6 BGP 团体属性 -E -A	917
45.3.4	配置 IPv6 BGP 路由反射器 -E -A	921
45.3.5	配置 IPv6 BGP 路由聚合 -E -A	926
45.3.6	配置 IPv6 BGP 路由优选 -E -A	930
45.3.7	配置 IPv6 BGP 与 BFD 联动 -E -A	939

46 策略路由	945
46.1 策略路由简介	945
46.2 策略路由功能配置	945
46.2.1 配置策略路由 -S -E -A	946
46.2.2 配置策略路由的应用 -S -E -A	950
46.2.3 策略路由监控与维护 -S -E -A	953
46.3 策略路由典型配置举例	954
46.3.1 配置策略路由 -S -E -A	954
47 路由策略工具	958
47.1 路由策略工具简介	958
47.2 路由策略工具功能配置	958
47.2.1 配置前缀列表 -S -E -A	959
47.2.2 配置 AS-PATH 列表 -E -A	960
47.2.3 配置团体属性列表 -E -A	962
47.2.4 配置扩展团体属性列表 -E -A	963
47.2.5 配置路由图 -S -E -A	965
47.2.6 配置密码链 -S -E -A	971
47.2.7 路由策略工具监控与维护 -S -E -A	972
47.3 路由策略工具典型配置举例	973
47.3.1 配置路由重分发关联路由策略 -S -E -A	973
47.3.2 配置 BGP 关联路由策略 -E -A	977
QOS	986
48 硬件 QOS	986
48.1 硬件 QoS 简介	986
48.1.1 背景	986
48.1.2 服务模型	986
48.1.3 QoS 功能组成介绍 -B -S -E -A	987
48.2 硬件 QoS 功能配置	991
配置手册	

48.2.1	配置优先级映射 -B -S -E -A	992
48.2.2	配置流分类 -B -S -E -A	995
48.2.3	配置流量监管 -B -S -E -A	1001
48.2.4	配置流量整形 -B -S -E -A	1002
48.2.5	配置拥塞管理 -B -S -E -A	1003
48.2.6	配置拥塞避免 -B -S -E -A	1005
48.2.7	配置 VFP 动作组 -B -S -E -A	1006
48.2.8	硬件 QoS 监控与维护 -B -S -E -A	1009
48.3	硬件 QoS 典型配置举例	1010
48.3.1	配置优先级映射 -B -S -E -A	1010
48.3.2	配置重标记 -B -S -E -A	1012
48.3.3	配置流量整形 -B -S -E -A	1014
48.3.4	配置速率限制 -B -S -E -A	1017
48.3.5	配置 WRED -B -S -E -A	1019
48.3.6	配置 SP -B -S -E -A	1021
48.3.7	配置 WDRR -B -S -E -A	1023
48.3.8	配置 SP+WRR -B -S -E -A	1026
48.3.9	配置流镜像 -B -S -E -A	1029
安全		1032
49 CPU 保护		1032
49.1 CPU 保护简介		1032
49.2 CPU 保护功能配置		1032
49.2.1	配置协议报文的 CPU 队列 -B -S -E -A	1033
49.2.2	配置 CPU 所有队列总的速率限制 -B -S -E -A	1034
49.2.3	配置 CPU 每个队列的速率限制 -B -S -E -A	1034
49.2.4	配置用户自定义协议报文交由 CPU 处理 -B -S -E -A	1035
49.2.5	CPU 保护监控与维护 -B -S -E -A	1037
49.3 CPU 保护典型配置举例		1038

49.3.1	配置 CPU 保护基本功能 -B -S -E -A	1038
49.3.2	配置 CPU 保护自定义规则 -B -S -E -A	1041
50	端口安全	1042
50.1	端口安全简介	1042
50.1.1	端口安全概述 -B -S -E -A	1042
50.1.2	端口安全规则 -B -S -E -A	1043
50.1.3	端口安全工作原理	1043
50.2	端口安全功能配置	1044
50.2.1	配置端口安全基本功能 -B -S -E -A	1044
50.2.2	配置端口安全规则 -B -S -E -A	1046
50.2.3	配置 STICKY 规则学习模式 -B -S -E -A	1050
50.2.4	配置静态 MAC 地址老化功能 -B -S -E -A	1051
50.2.5	配置收到非法报文时的处理模式 -B -S -E -A	1053
50.2.6	配置收到非法报文时发送日志的时间间隔 -B -S -E -A	1054
50.2.7	配置 MAC+IP 规则使用 ACL 功能 -B -S -E -A	1055
50.2.8	端口安全监控与维护 -B -S -E -A	1056
50.3	端口安全典型配置举例	1056
50.3.1	配置端口安全 MAC 及 IP 规则 -B -S -E -A	1056
50.3.2	配置端口安全 MAX 规则 -B -S -E -A	1058
50.3.3	配置端口安全 STICKY 规则 -B -S -E -A	1060
51	IP SOURCE GUARD	1062
51.1	IP SOURCE GUARD 简介	1062
51.2	IP SOURCE GUARD 功能配置	1063
51.2.1	配置端口 IP SOURCE GUARD 静态绑定表项 -B -S -E -A	1063
51.2.2	配置端口 IP SOURCE GUARD 功能 -B -S -E -A	1065
51.2.3	配置端口 IP SOURCE GUARD 过滤报文类型 -B -S -E -A	1066
51.2.4	配置端口 MAC 静态表项绑定功能 -B -S -E -A	1067
51.2.5	配置全局 IP SOURCE GUARD 功能 -B -S -E -A	1068

51.2.6	IP SOURCE GUARD 监控与维护 -B -S -E -A	1070
51.3	IP SOURCE GUARD 典型配置举例	1070
51.3.1	配置基于 IP+VLAN 的端口 IP SOURCE GUARD 功能 -B -S -E -A	1070
51.3.2	配置基于 MAC+VLAN 的端口 IP SOURCE GUARD 功能 -B -S -E -A	1072
51.3.3	配置基于 IP+MAC+VLAN 的端口 IP SOURCE GUARD 功能 -B -S -E -A	1074
52	DHCP SNOOPING	1077
52.1	DHCP SNOOPING 简介	1077
52.1.1	DHCP SNOOPING 基本功能简介 -B -S -E -A	1077
52.1.2	DHCP SNOOPING OPTION82 选项简介 -B -S -E -A	1078
52.2	DHCP SNOOPING 功能配置	1079
52.2.1	配置 DHCP SNOOPING 基本功能 -B -S -E -A	1080
52.2.2	配置 DHCP SNOOPING OPTION82 选项 -B -S -E -A	1082
52.2.3	配置 DHCP SNOOPING 绑定表项存储 -B -S -E -A	1087
52.2.4	DHCP SNOOPING 监控与维护 -B -S -E -A	1089
52.3	DHCP SNOOPING 典型配置举例	1090
52.3.1	配置 DHCP SNOOPING 的基本功能 -B -S -E -A	1090
53	DYNAMIC ARP INSPECTION	1092
53.1	DYNAMIC ARP INSPECTION 简介	1093
53.2	DYNAMIC ARP INSPECTION 功能配置	1093
53.2.1	配置端口 DYNAMIC ARP INSPECTION 功能 -B -S -E -A	1094
53.2.2	配置全局 DYNAMIC ARP INSPECTION 功能 -B -S -E -A	1097
53.2.3	配置 DYNAMIC ARP INSPECTION ARP 攻击检测 -B -S -E -A	1097
53.2.4	DYNAMIC ARP INSPECTION 监控与维护 -B -S -E -A	1098
53.3	DAI 典型配置举例	1099
53.3.1	配置 DAI 基本功能 -B -S -E -A	1099
53.3.2	DAI 与 DHCP SNOOPING 联用 -B -S -E -A	1101
54	HOST GUARD	1104
54.1	HOST GUARD 简介	1104

54.2	HOST GUARD 功能配置	1105
54.2.1	配置 HOST GUARD 功能 -B -S -E -A.....	1105
54.2.2	HOST GUARD 监控与维护 -B -S -E -A.....	1107
55	AAA	1108
55.1	AAA 简介	1108
55.2	AAA 功能配置	1109
55.2.1	配置 AAA 域 -B -S -E -A.....	1110
55.2.2	配置 AAA 域下认证功能 -B -S -E -A.....	1111
55.2.3	配置 AAA 域下授权功能 -B -S -E -A.....	1113
55.2.4	配置 AAA 域下统计功能 -B -S -E -A.....	1114
55.2.5	配置进入特权模式认证方法 -B -S -E -A.....	1116
55.2.6	配置开启命令行授权 -B -S -E -A.....	1117
55.2.7	配置系统事件统计功能 -B -S -E -A.....	1118
55.2.8	配置统计相关属性 -B -S -E -A.....	1119
55.2.9	配置 RADIUS 方案 -B -S -E -A.....	1120
55.2.10	配置 TACACS 方案 -B -S -E -A.....	1125
55.2.11	AAA 监控与维护 -B -S -E -A.....	1127
55.3	AAA 典型配置举例	1128
55.3.1	配置 TELNET 用户登录使用本地认证 -B -S -E -A.....	1128
55.3.2	配置 TELNET 用户登录使用 RADIUS 认证、授权与统计 -B -S -E -A.....	1129
55.3.3	配置 TELNET 用户级别切换使用 RADIUS 认证 -B -S -E -A.....	1130
55.3.4	配置 SHELL 命令的 TACACS 授权与统计 -B -S -E -A.....	1132
56	802.1X	1134
56.1	802.1X 简介	1134
56.1.1	802.1X -B -S -E -A.....	1134
56.1.2	安全通道认证 -B -S -E -A.....	1139
56.1.3	MAC 地址认证 -B -S -E -A.....	1139
56.2	802.1X 功能配置	1140

目录

56.2.1	配置 802.1X 认证功能 -B -S -E -A	1142
56.2.2	配置安全通道认证 -B -S -E -A	1144
56.2.3	配置 802.1X 认证及安全通道认证属性 -B -S -E -A	1147
56.2.4	配置 MAC 地址认证 -B -S -E -A	1154
56.2.5	配置公共属性 -B -S -E -A	1160
56.2.6	802.1X 监控与维护 -B -S -E -A	1180
56.3	802.1X 典型配置举例	1182
56.3.1	配置 802.1X 的 PORTBASED 认证 -B -S -E -A	1182
56.3.2	配置 802.1X 的 MACBASED 认证 -B -S -E -A	1185
56.3.3	配置 802.1X 透传模式 -B -S -E -A	1188
56.3.4	配置 802.1X 免客户端认证 -B -S -E -A	1190
56.3.5	配置安全通道 -B -S -E -A	1192
56.3.6	配置 IP 授权 DHCP SERVER 模式 -B -S -E -A	1195
56.3.7	配置 802.1X CRITICAL VLAN -B -S -E -A	1198
56.3.8	配置 802.1X 与端口安全共用 -B -S -E -A	1201
57	ACL 配置	1204
57.1	ACL 简介	1204
57.1.1	ACL 简介	1204
57.1.2	时间域简介	1205
57.2	ACL 功能配置	1205
57.2.1	配置 IP 标准 ACL -B -S -E -A	1207
57.2.2	配置 IP 扩展 ACL -B -S -E -A	1211
57.2.3	配置 MAC 标准 ACL -B -S -E -A	1216
57.2.4	配置 MAC 扩展 ACL -B -S -E -A	1219
57.2.5	配置 HYBRID 扩展 ACL -B -S -E -A	1223
57.2.6	配置 IPv6 标准 ACL -B -S -E -A	1226
57.2.7	配置 IPv6 扩展 ACL -B -S -E -A	1230
57.2.8	配置 ACL 规则条目数限制 -B -S -E -A	1234

目录

57.2.9	配置时间域 -B -S -E -A	1234
57.2.10	配置 ACL 的应用 -B -S -E -A	1240
57.2.11	ACL 监控与维护 -B -S -E -A	1247
57.3	ACL 典型配置举例	1248
57.3.1	配置 IP 标准 ACL -B -S -E -A	1248
57.3.2	配置带时间域的 IP 扩展 ACL -B -S -E -A	1250
57.3.3	配置 MAC 标准 ACL -B -S -E -A	1253
57.3.4	配置 MAC 扩展 ACL -B -S -E -A	1255
57.3.5	配置 HYBRID 扩展 ACL -B -S -E -A	1257
58	URPF	1259
58.1	URPF 简介	1260
58.2	URPF 功能配置	1260
58.2.1	配置 URPF 功能 -E -A	1260
58.2.2	URPF 监控与维护 -E -A	1261
58.3	URPF 典型配置举例	1262
58.3.1	配置 URPF 严格模式 -E -A	1262
58.3.2	配置 URPF 松散模式 -E -A	1263
59	攻击检测	1266
59.1	攻击检测简介	1266
59.2	攻击检测功能配置	1266
59.2.1	配置软件攻击检测功能 -B -S -E -A	1268
59.2.2	配置硬件攻击检测功能 -B -S -E -A	1275
59.2.3	攻击检测监控与维护 -B -S -E -A	1281
59.3	攻击检测典型配置举例	1282
59.3.1	配置防 DDOS 攻击检测 -B -S -E -A	1282
59.3.2	配置拦截源、目的 IP 地址相同的攻击检测 -B -S -E -A	1284
	可靠性	1286
60	HA	1286

60.1 HA 简介	1286
60.2 HA 功能配置	1286
60.2.1 HA 监控与维护 <i>-B -S -E -A</i>	1286
61 ULFD	1287
61.1 ULFD 简介	1287
61.2 ULFD 功能配置	1288
61.2.1 配置 ULFD 基本功能 <i>-B -S -E -A</i>	1288
61.2.2 配置 ULFD 参数 <i>-B -S -E -A</i>	1290
61.2.3 ULFD 监控与维护 <i>-B -S -E -A</i>	1291
61.3 ULFD 典型配置举例	1291
61.3.1 配置 ULFD 基本功能 <i>-B -S -E -A</i>	1291
62 VRRP	1295
62.1 VRRP 简介	1295
62.2 VRRP 功能配置	1295
62.2.1 配置 VRRP 基本功能 <i>-S -E -A</i>	1296
62.2.2 配置 VRRP 联动组 <i>-S -E -A</i>	1299
62.2.3 配置 VRRP 网络认证 <i>-S -E -A</i>	1300
62.2.4 配置 VRRP 与 TRACK 联动 <i>-S -E -A</i>	1301
62.2.5 VRRP 监控与维护 <i>-S -E -A</i>	1304
62.3 VRRP 典型配置举例	1305
62.3.1 配置 VRRP 单备份组 <i>-S -E -A</i>	1305
62.3.2 配置 VRRP 联动组 <i>-S -E -A</i>	1307
62.3.3 配置 VRRP 与 TRACK 联动 <i>-S -E -A</i>	1312
62.3.4 配置 VRRP 与 BFD 联动 <i>-S -E -A</i>	1315
62.3.5 配置 VRRP 负载均衡 <i>-S -E -A</i>	1318
63 VRRPV3	1322
63.1 VRRPv3 简介	1322
63.2 VRRPv3 功能配置	1322

63.2.1	配置 VRRPV3 基本功能 -E -A	1323
63.2.2	配置 VRRPV3 与 TRACK 联动 -E -A	1326
63.2.3	VRRPV3 监控与维护 -E -A	1329
63.3	VRRPV3 典型配置举例	1330
63.3.1	配置基于 IPV6 的 VRRP 单备份组 -E -A	1330
63.3.2	配置基于 IPV6 的 VRRP 与 TRACK 联动 -E -A	1332
63.3.3	配置基于 IPV6 的 VRRP 负载均衡 -E -A	1336
64	TRACK	1339
64.1	TRACK 简介	1339
64.2	TRACK 功能配置	1339
64.2.1	配置 TRACK 组 -B -S -E -A	1340
64.2.2	配置监控对象 -B -S -E -A	1341
64.2.3	TRACK 监控与维护 -B -S -E -A	1345
65	BFD	1346
65.1	BFD 简介	1346
65.2	BFD 功能配置	1347
65.2.1	配置 BFD 基本功能 -E -A	1347
65.2.2	BFD 监控与维护 -E -A	1350
65.3	BFD 典型配置举例	1351
65.3.1	配置 BFD 基本功能 -E -A	1351
66	ERPS	1355
66.1	ERPS 简介	1355
66.2	ERPS 功能配置	1356
66.2.1	配置 ERPS 环 -B -S -E -A	1356
66.2.2	配置 ERPS 环定时器 -B -S -E -A	1360
66.2.3	配置 ERPS 网络优化 -B -S -E -A	1361
66.2.4	配置 ERPS 与 CFM 联动 -B -S -E -A	1364
66.2.5	ERPS 监控与维护 -B -S -E -A	1365

66.3 ERPS 典型配置举例	1365
66.3.1 配置 ERPS 基本功能 -B -S -E -A	1365
66.3.2 配置 ERPS 负载 -B -S -E -A	1371
66.3.3 配置 ERPS 相交环 -B -S -E -A	1380
网络管理及监控	1391
67 网络测试和故障诊断	1391
67.1 网络测试和故障诊断简介	1391
67.2 网络测试和故障诊断应用	1391
67.2.1 PING 功能 -B -S -E -A	1392
67.2.2 TRACEROUTE 功能 -B -S -E -A	1397
67.2.3 系统调试功能 -B -S -E -A	1400
67.2.4 网络测试和故障诊断监控与维护 -B -S -E -A	1401
67.3 网络测试和故障诊断典型配置举例	1402
67.3.1 PING 的应用 -B -S -E -A	1402
67.3.2 TRACEROUTE 的应用 -B -S -E -A	1403
68 网关保活	1405
68.1 网关保活简介	1405
68.2 网关保活功能配置	1405
68.2.1 配置网关保活功能 -S -E -A	1406
68.2.2 网关保活监控与维护 -S -E -A	1407
68.3 网关保活典型配置举例	1408
68.3.1 配置网关保活 -S -E -A	1408
69 SLA	1411
69.1 SLA 简介	1411
69.2 SLA 功能配置	1412
69.2.1 使能 RTR -S -E -A	1413
69.2.2 配置 RTR 实体 -S -E -A	1413
69.2.3 配置 RTR 实体组 -S -E -A	1427

目录

69.2.4	配置 RTR 应答器 -S -E -A	1429
69.2.5	配置 RTR 调度器 -S -E -A	1430
69.2.6	配置暂停调度实体 -S -E -A	1431
69.2.7	配置恢复调度实体 -S -E -A	1431
69.2.8	SLA 监控与维护 -S -E -A	1432
69.3	SLA 典型配置举例	1432
69.3.1	配置 ICMP-ECHO 实体检测网络基本通信情况 -S -E -A	1432
69.3.2	配置 ICMP-PATH-ECHO 实体检测网络通信情况 -S -E -A	1436
69.3.3	配置 ICMP-PATH-JITTER 实体检测网络通信情况 -S -E -A	1438
69.3.4	配置 VOIP-JITTER 实体检测网络传输语音报文的情况 -S -E -A	1441
69.3.5	配置 UDP-ECHO 实体检测网络传输 UDP 报文的情况 -S -E -A	1444
69.3.6	配置 FLOW-STATISTICS 实体检测接口流量 -S -E -A	1447
69.3.7	配置 TRACK 与 SLA 联动 -S -E -A	1449
70	NTP	1452
70.1	NTP 简介	1452
70.2	NTP 功能配置	1453
70.2.1	配置 NTP 基本功能 -B -S -E -A	1454
70.2.2	配置 NTP 可选参数 -B -S -E -A	1457
70.2.3	配置 NTP 认证功能 -B -S -E -A	1460
70.2.4	配置 NTP 访问控制 -B -S -E -A	1465
70.2.5	NTP 监控与维护 -B -S -E -A	1466
70.3	NTP 典型配置举例	1466
70.3.1	配置 NTP 服务器端与客户端 -B -S -E -A	1466
70.3.2	配置 NTP 服务器端与多级客户端 -B -S -E -A	1468
70.3.3	配置带 MD5 认证的 NTP 服务器端与客户端 -B -S -E -A	1470
70.3.4	配置 NTP 对等体模式 -B -S -E -A	1472
70.3.5	配置 NTP 广播模式 -B -S -E -A	1474
70.3.6	配置 NTP 广播模式认证功能 -B -S -E -A	1477

71 端口镜像	1480
71.1 端口镜像简介	1481
71.1.1 端口镜像简介	1481
71.1.2 基本概念 -B -S -E -A	1481
71.2 SPAN 功能配置	1483
71.2.1 配置 LOCAL SPAN -B -S -E -A	1483
71.2.2 配置 RSPAN -B -S -E -A	1484
71.2.3 配置 VLAN SPAN -B -S -E -A	1487
71.2.4 SPAN 监控与维护 -B -S -E -A	1489
71.3 端口镜像典型配置举例	1490
71.3.1 配置 LOCAL SPAN -B -S -E -A	1490
71.3.2 配置 RSPAN -B -S -E -A	1491
71.3.3 配置 VLAN SPAN -B -S -E -A	1494
72 SFLOW	1495
72.1 sFLOW 简介	1496
72.2 sFLOW 功能配置	1496
72.2.1 配置 sFLOW 基本功能 -B -S -E -A	1497
72.2.2 配置 sFLOW 采样方式 -B -S -E -A	1498
72.2.3 sFLOW 监控与维护 -B -S -E -A	1500
72.3 sFLOW 典型配置举例	1500
72.3.1 配置 sFLOW 基本功能 -B -S -E -A	1500
73 LLDP	1502
73.1 LLDP 简介	1503
73.1.1 LLDP 协议概述 -B -S -E -A	1503
73.1.2 TLV 类型信息 -B -S -E -A	1503
73.1.3 LLDP 工作机制 -B -S -E -A	1507
73.2 LLDP 功能配置	1508
73.2.1 配置 LLDP 基本功能 -B -S -E -A	1509

目录

73.2.2	配置 LLDP 工作模式 -B-S-E-A	1510
73.2.3	配置 LLDP 允许发布的 TLV -B-S-E-A	1511
73.2.4	配置 LLDP 参数 -B-S-E-A	1514
73.2.5	LLDP 监控与维护 -B-S-E-A	1517
73.3	LLDP 典型配置举例	1518
73.3.1	配置 LLDP 的基本功能 -B-S-E-A	1518
74	SNMP	1521
74.1	SNMP 简介	1521
74.2	SNMP 功能配置	1524
74.2.1	配置 SNMP 基本功能 -B-S-E-A	1525
74.2.2	配置 SNMPV1/V2 -B-S-E-A	1527
74.2.3	配置 SNMPV3 -B-S-E-A	1528
74.2.4	配置 SNMP TRAP -B-S-E-A	1532
74.2.5	SNMP 监控与维护 -B-S-E-A	1534
74.3	SNMP 典型配置举例	1535
74.3.1	配置 SNMP v1/v2c 代理服务器 -B-S-E-A	1535
74.3.2	配置 SNMP v3 代理服务器 -B-S-E-A	1537
74.3.3	配置 SNMP v3 TRAP 通告 -B-S-E-A	1538
74.3.4	配置 SNMP v3 INFORM 通告 -B-S-E-A	1540
74.3.5	配置 SNMP v3 代理转发 -B-S-E-A	1542
75	RMON	1545
75.1	RMON 简介	1545
75.2	RMON 功能配置	1546
75.2.1	使能 RMON 功能 -B-S-E-A	1546
75.2.2	配置 RMON 告警组 -B-S-E-A	1547
75.2.3	配置 RMON 扩展告警组 -B-S-E-A	1548
75.2.4	配置 RMON 事件组 -B-S-E-A	1549
75.2.5	配置 RMON 历史组 -B-S-E-A	1550

75.2.6	配置 RMON 统计组 -B -S -E -A	1551
75.2.7	RMON 监控与维护 -B -S -E -A	1552
75.3	RMON 典型配置举例	1552
75.3.1	配置 RMON 基本功能 -B -S -E -A	1552
	虚拟化	1556
76	VST	1556
76.1	VST 简介	1556
76.1.1	基本概念	1557
76.2	VST 功能配置	1558
76.2.1	配置虚拟交换成员设备 -B -S -E -A	1559
76.2.2	配置虚拟交换链路接口 -B -S -E -A	1562
76.2.3	配置设备运行模式 -B -S -E -A	1564
76.2.4	VST 监控与维护 -B -S -E -A	1565
76.3	VST 典型配置举例	1565
76.3.1	配置设备形成链形堆叠系统 -B -S -E -A	1565
77	MAD	1568
77.1	MAD 简介	1568
77.2	MAD 功能配置	1569
77.2.1	配置 MAD LACP 功能 -B -S -E -A	1569
77.2.2	配置 MAD FAST-HELLO 功能 -B -S -E -A	1570
77.2.3	配置保留口 -B -S -E -A	1572
77.2.4	配置恢复 MAD 状态为 ACTIVE 状态 -B -S -E -A	1573
77.2.5	MAD 监控与维护 -B -S -E -A	1574
77.3	MAD 典型配置举例	1575
77.3.1	配置 MAD LACP 功能 -B -S -E -A	1575
77.3.2	配置 MAD FAST-HELLO 功能 -B -S -E -A	1577

安全指示

警告

不受控制的机器行为

为避免由于数据丢失而导致出现不受控制的机器行为，请单独配置所有的数据传输设备。

在启动任何通过数据传输控制的机器之前，请务必完成所有数据传输设备的配置。

不遵守这些指示可能会导致死亡、严重伤害或设备损坏。

关于本手册

“图形用户界面”参考手册包含使用图形界面操作设备的各个功能的详细信息。

以下图形用户界面将被称为基于 WEB 的界面。

配置说明:

-B -S -E -A 分别代表不同的软件版本，如下:

-B: *Basic*

-S: *Standard*

-E: *Enhanced*

-A: *Advanced*

注意: 8000 系列产品和 -A 产品的软件性能除 MPLS QoS 外完全一样。

维护

Hirschmann IT 一直致力于改进和发展软件。您可定期检查是否有能为您提供额外好处的软件更新版本。您能在 www.belden.com 的 Hirschmann IT 产品页面上找到信息并下载软件。

系统基础及管理

1 系统操作基础

1.1 系统操作基础简介

系统操作基础主要讲述设备操作的基础知识，包括主要讲述设备操作的基础知识，包括设备配置方式、命令运行模式及命令行接口等相关内容。

1.2 系统操作基础功能

表 1-1 系统操作基础功能配置列表

配置任务	
设备配置方式	设备配置方式
命令运行模式	命令运行模式
命令行接口	命令行接口

1.2.1 设备配置方式 **-B -S -E -A**

用户可以通过不同的方式登录到设备进行配置和管理（详细的登录方式请参见配置手册“系统登录”相关章节），设备为用户提供了四种典型的配置方式：

- 通过 Console 口本地登录设备进行配置，缺省情况下，用户可以直接通过这种方式进行配置；
- 通过 Modem 远程拨号登录设备进行配置，缺省情况下，不能直接用这种方式进行配置，需要做一些准备配置工作；
- 通过 Telnet 远程登录到设备进行配置，缺省情况下，不能直接用这种方式进行配置，需要做一些准备配置工作；
- 通过 SSH 远程登录到设备进行配置，缺省情况下，不能直接用这种方式进行配置，需要做一些准备配置工作。

1.2.2 命令运行模式 **-B -S -E -A**

设备为系统命令的管理及执行提供了一个命令处理子系统，称为 shell，其主要功能包括：

- 系统命令的注册
- 系统配置命令的用户编辑
- 用户输入命令的语法分析
- 系统命令的执行

用户通过 shell 命令配置设备时，系统为命令的执行提供了多种运行模式，每种命令模式分别支持特定的配置命令，从而达到分级保护系统的目的，确保系统不受未经授权的访问。

shell 子系统当前为配置命令的运行提供了以下多种模式，不同的模式对应于不同的系统提示符，用于提示用户当前所处的系统模式。常见的几种配置模式如下：

- 普通用户模式 (user EXEC)
- 特权用户模式 (privilege EXEC)
- 全局配置模式 (global configuration)
- 接口配置模式 (interface configuration)
- 文件系统配置模式 (file system configuration)

- 访问列表配置模式 (access list configuration)
- 其他配置模式 (在其他相关章节中进行介绍)

下表描述了几种常见命令模式的进入方法及模式间的切换方法。

表 1-2 系统模式及其相互切换的方法

模式名称	模式进入方法	系统提示符	退出方法	功能说明
普通用户模式	登录设备	Hostname>	执行 exit 命令退出	·改变终端设置 ·执行基本测试 ·显示系统信息
特权用户模式	在普通用户模式下执行 enable 命令	Hostname#	执行 disable 或者 exit 命令退回到普通用户模式	·配置设备运行参数 ·显示设备运行信息
全局配置模式	在特权用户模式下执行 configure terminal 命令	Hostname(config)#	执行 exit 命令退回到特权用户模式	·配置设备运行所需的全局参数
接口配置模式	在全局模式下执行 interface 命令 (同时指定相应的接口或者接口组)	Hostname(config-if-xxx[number])# 或者 Hostname(config-if-group[number])#	执行 exit 命令退回到全局配置模式 执行 end 命令退回到特权用户模式	在该模式下配置设备接口, 包括: ·配置各种类型的接口 ·配置接口组

模式名称	模式进入方法	系统提示符	退出方法	功能说明
文件系统配置模式	在特权用户模式执行 filesystem 命令	Hostname(configuration)#	执行 exit 命令退回到特权用户模式	进行设备的文件系统的管理
访问列表配置模式	在全局配置模式下，执行 ip access-list standard 命令或者 ip access-list extended 命令	Hostname(configuration-std-nacl)# Hostname(configuration-ext-nacl)#	执行 exit 命令退回到全局配置模式 执行 end 命令退回到特权用户模式	配置 ACL 访问列表，其任务包括： ·配置标准访问列表 ·配置扩展访问列表

说明：

- Hostname 是系统名称，用户可以在全局配置模式下运行 **hostname** 命令修改系统名称，并且这种修改是立即生效的。
- 如果用户需要执行的命令是在特权用户模式下，但是当前模式又在特权用户模式之外，那么可以通过 do 命令来执行需要执行的命令（详见技术手册“系统操作基础”相关章节），无需回到特权用户模式下。但是注意不包括模式切换的命令如 do configure terminal。

1.2.3 命令行接口 **-B -S -E -A**

命令行接口是 shell 子系统为用户配置、使用设备而提供的一个人机交互界面，用户通过命令行接口可以输入、编辑命令来完成相应的配置任务，同时也可以通过该接口查看系统信息，了解系统运行情况。

命令行接口为用户提供了如下功能：

- 系统帮助信息管理
- 系统命令输入、编辑
- 历史命令管理
- 终端显示系统管理

命令行在线帮助

命令行提供了如下几种在线帮助：

- help
- 完全帮助
- 部分帮助

通过上述的帮助手段，用户可以获取到各种帮助信息，分别举例如下：

- 在任意一种命令模式下，执行 **help** 命令可以获取有关帮助系统的简单描述。

```
Hostname#help
Help may be requested at any point in a command by entering
a question mark '?'. If nothing matches, the help list will
be empty and you must backup until entering a '?' shows the
available options.
Two styles of help for command are provided:
1. Full help is available when you are ready to enter a
  command argument (e.g. 'show ?') and describes each possible
  argument.
2. Partial help is provided when an abbreviated argument is entered
  and you want to know what arguments match the input
  (e.g. 'show pr?'.)
And "Edit key" usage is the following:
CTRL+A -- go to home of current line
CTRL+E -- go to end of current line
CTRL+U -- erase all character from home to current cursor
CTRL+K -- erase all character from current cursor to end
CTRL+W -- erase a word on the left of current cursor
CTRL+R -- erase a word on the right of current cursor
CTRL+D,DEL -- erase a character on current cursor
BACKSPACE -- erase a character on the left of current cursor
CTRL+B,LEFT -- current cursor backward a character
CTRL+F,RIGHT -- current cursor forward a character
```

- 在任一命令模式下，键入 “?” 获取该命令模式下所有命令及其简单描述。

```

Hostname#configure terminal
Hostname(config)#?
aaa          Authentication, Authorization and Accounting
access-list  Access List
alarm        Set alarm option of system
arl          Address translation item
arp          Set a static ARP entry
arp-security To CPU arp security
autosave    Auto save the startup configuration
banner       Define a login banner
bgp          BGP information
cable-diagnostics Cable Diagnostics on physical interface
.....
    
```

- 键入一命令，后接以空格分隔的 “?” ，则显示出所有该命令在当前模式下可以执行的子命令。

```

Hostname#show ?
access-list  List access lists
acl-object   Show acl object
arl          Address translation item
arp          Command arp
arp-security To CPU arp security
bfd          BFD Protocol information
bgp          BGP information
cable-diagnostics Cable Diagnostics on physical interface
card_list    Show information of hardware modules
clock        Print system clock information
cluster      Config cluster
cpu          Show CPU use per process
.....
    
```

- 键入一字符串，后紧接 “?” ，列出以该字符串开始的所有关键字及其描述。

```

Hostname#show a?
access-list  List access lists
acl-object   Show acl object
arl          Address translation item
arp          Command arp
arp-security To CPU arp security
    
```

命令行错误信息

用户键入的所有命令，命令行都要进行语法检查，如果检查通过，则正确执行，否则向用户报告错误信息，常见错误信息参见下表：

表 1-3 命令行错误信息

错误信息	错误原因
% Invalid input detected at '^' marker.	没有查找到命令、关键字，或者参数类型错误、参数值越界

错误信息	错误原因
Type "**** ?" for a list of subcommands 或者 % Incomplete command	输入命令不完整
Hostname#wh % Ambiguous command: wh % Please select: whoami who	输入的字符串是一个模糊命令

历史命令

命令行接口提供类似 Doskey 功能，系统将用户输入的命令自动保存到历史命令缓冲区，用户可以随时调用命令行接口保存的历史命令，并重复执行，从而减少用户不必要的重复输入工作。命令行接口为每个连接到设备的用户最多保存 10 条命令，随后新的命令将覆盖掉旧的命令。

表 1-4 访问命令行接口历史命令

操作	按键	执行结果
访问上一条历史命令	上光标键↑或 Ctrl+P	如果还有更早的历史命令，取出显示；否则响铃告警
访问下一条历史命令	下光标键↓或 Ctrl+N	如果还有更晚的历史命令，取出显示；否则清空命令行并响铃告警

说明：

- 用上下光标键对历史命令进行访问时，在 windows 98/NT 系统下，运行 telnet 登录到设备上时，需要将终端->首选选项->模拟选项设为 VT-100/ANSI 类型。
- 历史命令以当前模式为范围显示，比如在特权模式下，只显示特权模式的历史命令。

编辑特性

命令行接口提供了基本的命令编辑功能，支持多行编辑，每行命令最多可达 256 个字符，下表即是 shell 子系统为命令行接口提供的基本编辑功能。

表 1-5 基本编辑功能表

按键	功能
普通按键	如编辑缓冲区未滿，则插入当前光标位置处，并向右移动光标；否则响铃告警
退格键 Backspace	删除光标前一字符，光标前移，若已到达命令首，则响铃告警
删除键 Delete	删除光标处的字符，若已到达命令尾，则响铃告警
左光标键←或 Ctrl+B	光标向左移动一个字符位置，若已到达命令首，则响铃告警
右光标键→或 Ctrl+F	光标向右移动一个字符位置，若已到达命令尾，则响铃告警
上下光标键↑↓	显示历史命令
Ctrl+A	光标移到命令行首
Ctrl+E	光标移到命令行尾
Ctrl+U	删除光标左边的所有字符直到命令行首

显示特性

为方便用户，命令行接口提供如下的显示特性：

在所需显示的信息超过一屏时，提供了暂停功能，并在屏幕左下角显示提示符“---MORE---”，此时用户可以有如下表中的几种选择：

表 1-6 显示特性表

按键	功能
空格键 Space 或下光标键↓或 Ctrl-F	继续显示下一屏信息
上光标键↑或 Ctrl-B	显示上一屏信息
回车键 Enter 或右光标键→或等于号键=	显示信息向下翻滚一行
或左光标键←或减号键-	显示信息向上翻滚一行
Ctrl-H	回到显示内容的最前面
其余任意按键	退出显示，不再显示未完的信息

2 系统登录

2.1 系统登录简介

设备支持的系统登录方式有以下几种：

- 通过 Console 口登录设备进行管理和维护；
- Telnet（远程登录），用户可以通过这种方式对设备进行远程管理和维护；
- SSH（Secure Shell）安全外壳的简称。SSH 通过加密和认证技术，为用户提供安全的远程登录管理服务。

2.2 系统登录功能配置

表 2-1 系统登录功能配置列表

配置任务	
通过 Console 口登录设备	-
通过 AUX 口登录设备	-
配置 Telnet 远程登录	使能设备 Telnet 服务
	设备作为 Telnet 客户端远程登录
配置 SSH 远程登录	使能设备 SSH 服务
	设备作为 SSH 客户端远程登录

说明：

- Telnet 和 SSH 远程登录相关用户配置，请参见登录控制与管理手册。

2.2.1 通过 Console 口登录设备 **-B -S -E -A**

通过 Console 口连接终端配置设备，需要以下几个步骤：

步骤 1： 选择一台终端。

终端既可以是标准的具有 RS-232 串口的终端，也可以是一台普通的 PC 机，更常用的是后者。如果要通过远程拨号登录，则还需两台 Modem。

步骤 2： Console 口的物理连接方式。

在确认终端或带有 Console 口的设备至少有一方是关电的情况下，再将终端的 RS-232 串口与设备 Console 口相连。连接关系如下图所示：



图 2-1 通过 Console 口登录设备的连接图

步骤 3： 配置超级终端。

给终端上电后，需要设置终端的通信参数：即波特率为 9600bps、8 位数据位、1 位停止位、无校验和无数据流控制。如果是 Windows XP/NT 操作系统的 PC，则运行 HyperTerminal（超级终端）程序，并按照以上参数设置超级终端程序的串口通信参数。下面以 Windows NT 的终端超级终端程序为例图示说明：

- 创建连接：

首先输入一个连接名称，并为该连接选择一个 Windows 图标。



图 2-2 创建连接图

- 选择串行通信口：

根据所连接的串行通信口，可以选择 COM1 或 COM2。



图 2-3 选择串行通信口

- 配置串行通信口参数：

波特率——9600bps

数据位——8 位

奇偶校验——无

停止位——1 位

数据流控制——无



图 2-4 配置串行通信口参数

- 登录成功检验：

给带有 Console 口的设备上电后，设备启动时的信息将会在终端上显示出来。当启动完成后会显示：

“Press any key to start the shell!” 信息。如果配置了登录需要认证，则输入用户名和密码，否则

按任意键直接登录。登录成功后在终端上会显示“Hostname>”提示符，就可以对设备进行配置了。

2.2.2 配置 Telnet 远程登录 -B -S -E -A

配置条件

无

使能设备 Telnet 服务

用户可以通过 Telnet 方式远程登录到设备上进行管理，但在使用 Telnet 服务之前，需要先使能设备的 Telnet 服务。当设备的 Telnet 服务启动后，会监听 Telnet 服务端口 23。

表 2-2 使能设备 Telnet 服务

步骤	命令	说明
进入全局配置模式	configure terminal	-
使能设备 Telnet 服务	telnet server enable	必选 缺省情况下，Telnet 服务已使能

设备作为 Telnet 客户端远程登录

设备作为 Telnet 客户端进行远程登录是指用户可以把一台设备作为 Telnet 客户端，然后远程登录到指定的 Telnet 服务器端，对其进行配置与管理。

表 2-3 设备作为 Telnet 客户端远程登录

步骤	命令	说明
进入全局配置模式	configure terminal	-
使能设备 Telnet 客户端	telnet client enable	可选

步骤	命令	说明
		缺省情况下, Telnet 客户端已使能
设备作为 Telnet 客户端远程登录	telnet [vrf <i>vrf-name</i>] { <i>hostname</i> <i>remote-host</i> } [<i>port-number</i>] [ipv4 ipv6] [source-interface <i>interface-name</i>]	必选

说明:

- 只有当远程设备开启 Telnet 服务器功能, 且 Telnet 客户端与远程设备网络可达时, Telnet 客户端才能登录到远程设备。

2.2.3 配置 SSH 远程登录 **-B -S -E -A**

配置条件

无

使能设备 SSH 服务

设备在使能 SSH 服务后, 会接受用户通过 SSHv1 或 SSHv2 客户端发起的连接请求, 在对客户端进行认证通过后, 则允许客户端登录到设备。当设备使能 SSH 服务后, 会监听 SSH 服务端口 22。配置 **ip ssh server** 如果没有带参数 **sshv1-compatible**, 则表示仅支持 SSH 客户端采用 SSHv2 登录。

表 2-4 使能设备 SSH 服务

步骤	命令	说明
进入全局配置模式	config terminal	-
使能设备 SSH 服务	ip ssh server [<i>listen-port</i>] [sshv1-compatible] [<i>listen-port</i>]	必选 缺省情况下, SSH 服务关闭

设备作为 SSH 客户端远程登录

设备作为 SSH 客户端, 可采用 SSHv1 或 SSHv2 协议远程登录到指定 SSH 服务器, 登录时需输入用户名、密码用于 SSH 服务器进行认证。

表 2-5 设备作为 SSH 客户端远程登录

步骤	命令	说明
设备作为 SSH 客户端远程登录	ssh [<i>vrf vrf-name</i>] version { 1 2 } <i>remote-host port-number</i> [source-interface <i>interface-name</i>] user auth-method 1 password	必选

说明:

- 只有当远程设备开启 SSH 服务, 且 SSH 客户端与远程设备网络可达时, SSH 客户端才能登录到远程设备。

设备作为 SFTP 客户端访问 SFTP 服务器

设备作为 SFTP 客户端, 使用 SSHv2 协议远程连接到指定 SFTP 服务器, 连接时需输入用户名、密码用于 SFTP 服务器进行认证, SFTP 客户端连接到 SFTP 服务器后下载或者上传服务器上的文件。

表 2-6 设备作为 SFTP 客户端访问 SFTP 服务器

步骤	命令	说明
设备作为 SFTP 客户端访问 SFTP 服务器	sftp {get put} [vrf vrf-name] remote-host port-number [source-interface interface-name] user password src-filename dst-filename [compress]	必选

说明：

- 只有当远程设备开启 SSH 服务，且 SFTP 客户端与远程设备网络可达时，SFTP 客户端才能连接到远程设备。

2.2.4 系统登录监控与维护

-B -S -E -A

表 2-7 系统登录监控与维护

命令	说明
show fingerprint	显示 SSH 公钥指纹信息。

2.3 系统登录典型配置举例

2.3.1 配置本地终端 Telnet 登录设备

-B -S -E -A

网络需求

- 使用 PC 作为本地终端 Telnet 登录到设备。
- PC 和设备必须路由可达。

网络拓扑



图 2-5 配置本地终端 Telnet 登录设备组网图

配置步骤

步骤 1： 创建 VLAN，并将端口加入对应的 VLAN。（略）

步骤 2： 配置各接口的 IP 地址。（略）

步骤 3： 配置 enable 密码。

```
Device#configure terminal
Device(config)#enable password admin
```

步骤 4： Telnet 登录设备。

#在 PC 上运行 Telnet 程序，输入接口 VLAN2 的 IP 地址。



图 2-6 在 PC 上 Telnet 登录设备

步骤 5: 检测结果。

#登录成功后弹出下面的窗口。

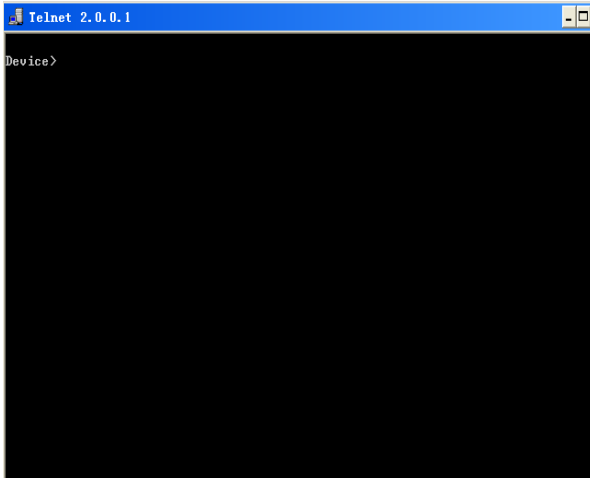


图 2-7 Telnet 登录成功的界面

成功登录设备 Device 后，输入正确的 enable 密码，获取到对设备相应的操作权限。如果要退出登录的可以连续使用 “exit” 命令。

说明：

- 如果出现 “Too many clients or invalid access” 则表示登录的用户已经超过设备允许登录的最大用户数。可等一会儿再进行登录。
 - 如果出现 “%enable operation is locked by login-secure service” 则表示输入错误的 enable 密码超过了用户连续登录认证失败次数，达到系统设定次数后，系统就会在设定的时间内禁止来自该 IP 地址的登录连接。
 - 如果出现 “Password required, but none set” 则表示未配置 “login password” 。
-

2.3.2 配置通过本地设备 Telnet 登录到远端设备

-B -S -E -A

网络需求

- 本端设备 Device1 作为 Telnet 客户端，对端设备 Device2 作为 Telnet 服务器端。
- 两台设备必须路由可达。
- PC 能够正常登录 Device1。

网络拓扑

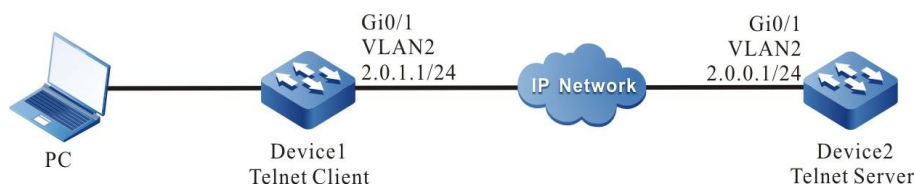


图 2-8 配置本地设备 Telnet 登录远端设备图

配置步骤

步骤 1： 创建 VLAN，并将端口加入对应的 VLAN。（略）

步骤 2： 配置各接口的 IP 地址。（略）

步骤 3： 使用 PC 登录到 Device1 上。（略）

步骤 4： 在 Device1 上使用命令远程登录到 Device2 上。

```
Device1#telnet 2.0.0.1
```

#进入到 Device2 的 shell 界面。

```
Connect to 2.0.0.1 ...done  
Device2>
```

成功登录设备 Device2 后输入正确的 enable 密码，获取到对设备操作的相应权限。如果要退出登录可以连续使用 “exit” 命令。

说明：

- 如果出现 “Too many clients or invalid access” 则表示登录的用户已经超过设备允许登录的最大用户数。可等一会儿再进行登录。
- 如果出现 “%enable operation is locked by login-secure service” 则表示输入错误的 enable 密码超过了用户连续登录认证失败次数，达到系统设定次数后，系统就会在设定的时间内禁止来自该 IP 地址的登录连接。

- 如果出现 “Password required, but none set” 则表示未配置 login password。

2.3.3 配置通过本地设备 SSH 登录到远端设备

-B -S -E -A

网络需求

- 本端设备 Device1 作为 SSH 客户端，对端设备 Device2 作为 SSH 服务器端。
- 两台设备必须路由可达。
- PC 能够正常登录到 Device1 上。

网络拓扑

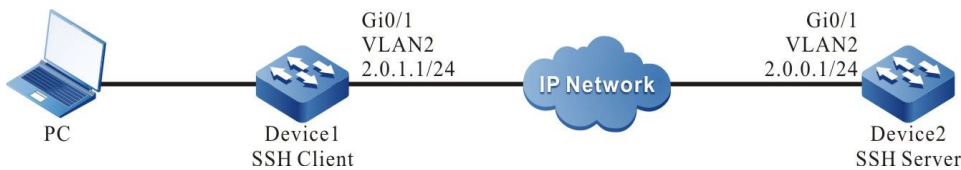


图 2-9 配置通过本地设备 SSH 登录到远端设备图

配置步骤

步骤 1： 创建 VLAN，并将端口加入对应的 VLAN。（略）

步骤 2： 配置各接口的 IP 地址。（略）

步骤 3： 配置本地用户和相关属性。

#配置 Device2 的用户名和密码。

```
Device2#configure terminal
Device2(config)#user admin password 0 admin
```

步骤 4： 启用 Device2 SSH 服务器功能。

```
Device2(config)#ip ssh server
```

步骤 5： 配置登录认证方式使用本地认证。

```
Device2(config)#line vty 0 15
Device2(config-line)#login local
Device2(config-line)#exit
```

步骤 6： 在设备 Device1 上 SSH 登录到 Device2 上。

#配置 Device1 SSH 登陆到 Device2 上。

```
Device1#ssh version 2 2.0.0.1 22 admin auth-method 1 admin
The authenticity of host '2.0.0.1' can't be established
RSA key fingerprint is 7b:ed:cc:81:cf:12:36:6f:f7:ff:29:15:63:75:64:10.
Are you sure you want to continue connecting (yes/no)? yes
Device2>
```

步骤 7： 检验结果。

登录成功后会进入到设备 Device2 的 shell 界面。

说明：

- 如果出现 “Connection closed by foreign host” 则表示对端未开启 SSH 服务功能或者输入的用户名和密码不正确。
 - SSH 服务器端可以配置不使用认证，当 SSH 服务器端不使用认证的时候，在客户端登录的时候用户名和密码可以用任意字符代替。
-

2.3.4 配置设备作为 SFTP 客户端

-B -S -E -A

网络需求

- PC 作为 SFTP 服务器，设备 Device 作为 SFTP 客户端；服务器和设备网络连通。
- SFTP 服务器上设置设备登录 FTP 服务器的用户名为 admin，密码为 admin；将需要下载的文件放到 SFTP 服务器的目录下。
- 设备作为 SFTP 客户端，与 SFTP 服务器之间上传、下载文件。

网络拓扑



图 2-10 配置设备作为 SFTP 客户端组网图

配置步骤

步骤 1: 创建 VLAN, 并将端口加入对应的 VLAN。 (略)

步骤 2: 配置 SFTP 服务器, 将需要下载的文件放到 SFTP 服务器的目录下。 (略)

步骤 3: 配置各设备 IP 地址, 使客户端与服务器网络连通。 (略)

步骤 4: Device 作为 SFTP 客户端, 与 SFTP 服务器之间上传、下载文件。

#从 SFTP 服务器下载一个文件到设备的文件系统中

```
Device#sftp get 2.0.0.1 22 admin admin sp8-g-6.6.7(46)-dbg.pck sp8-g-6.6.7(46)-dbg.pck
The authenticity of host '2.0.0.1 (2.0.0.1)' can't be established.
RSA key fingerprint is e4:dd:11:2e:82:34:ab:62:59:1c:c8:62:1d:4b:48:99.
Are you sure you want to continue connecting (yes/no)? yes

Downloading#####
#####OK!
```

#将 Device 文件系统下的 startup 文件上传到 SFTP 服务器

```
Device#sftp put 2.0.0.1 22 admin admin startup startup.txt
The authenticity of host '2.0.0.1 (2.0.0.1)' can't be established.
RSA key fingerprint is e4:dd:11:2e:82:34:ab:62:59:1c:c8:62:1d:4b:48:99.
Are you sure you want to continue connecting (yes/no)? yes

Uploading#####
#####OK!
```

步骤 5: 检验结果。

#拷贝完成后, 可以在 Device 文件系统中查看下载的文件是否存在; 在 SFTP 服务器上查看上传的文件是否存在 (略)。

```
Device(config-fs)#dir
size    date    time    name
-----  -
101526  MAR-01-2015 01:17:18 logging
10147   MAR-26-2015 07:58:50 startup
10207   MAR-01-2015 01:17:54 history
11676148 MAR-26-2013 07:51:32 sp8-g-6.6.7(46)-dbg.pck
2048    JAN-10-2015 17:30:20 snmp          <DIR>
```

2.3.5 配置设备作为 SFTP 服务器

-B -S -E -A

网络需求

- Device 作为 SFTP 服务器，PC 作为 SFTP 客户端；客户端和服务器网络连通。
- SFTP 服务器 Device 上设置用户名为 admin，密码为 admin，Device 的文件系统目录作为 SFTP 服务器根目录。
- PC 作为 SFTP 客户端，与 SFTP 服务器 Device 之间上传、下载文件。

网络拓扑



图 2-11 配置设备作为 SFTP 服务器组网图

配置步骤

- 步骤 1： 创建 VLAN，并将端口加入对应的 VLAN。（略）
- 步骤 2： 配置各接口的 IP 地址，使 PC 与 Device 网络连通。（略）
- 步骤 3： 在 Device 上，使能 SFTP 服务，配置授权的用户名和密码。

#在 SFTP 服务器 Device 上配置授权的用户名和密码

```
Device#configure terminal
Device(config)#user admin password 0 admin
```

#在 Device 上开启 SSH 服务（SFTP 是 SSH 协议的一个子模块）

```
Device(config)#ip ssh server
```

- 步骤 4： 使用 PC 作为 SFTP 客户端，上传、下载一个文件到 SFTP 服务器 Device 上。

#如下以 Linux 系统为例描述相关过程

#输入正确的 IP 地址和用户名、密码登录到 SFTP 服务器上

```
[root@aas ~]# sftp admin@2.1.1.1
Connecting to 2.1.1.1...
admin@2.1.1.1's password:
sftp>
```

#获取 SFTP 服务器 Device 文件系统中的 startup 文件

```
sftp> get startup startup
Fetching /flash/startup to startup
/flash/startup                                100% 13KB 12.9KB/s 00:00
```

#文件复制完成后，可以在操作的目录下找到相关文件

```
sftp> ls
sp8-g-6.6.7(74)-dbg.pck sp8-g-6.6.7(76)-dbg.pck startup      tech      test_pc
sftp>
```

#将 PC 中的文件上传到 SFTP 服务器 Device 文件系统中。

```
sftp> put sp8-g-6.6.7(76)-dbg.pck sp8-g-6.6.7(76)-dbg.pck
Uploading sp8-g-6.6.7(76)-dbg.pck to /flash/ sp8-g-6.6.7(76)-dbg.pck
sp8-g-6.6.7(76)-dbg.pck                       100% 11424KB 16.0KB/s 00:00
```

#文件上传完成后，可以在 Device 的文件系统中找到对应的文件

```
Device(config-fs)#dir
  size      date       time      name
-----
2048       JUN-30-2015 16:35:50 tech      <DIR>
10229      JUN-12-2015 14:31:22 history
101890     JUN-30-2015 17:46:40 logging
39755      JUN-30-2015 16:33:56 startup
740574     MAY-27-2014 18:55:14 web-Spl-1.1.243.rom
2048       JUN-27-2015 16:26:10 snmp      <DIR>
11698172   JUN-30-2015 10:36:18 sp8-g-6.6.7(76)-dbg.pck
```

3 登录控制与管理

3.1 登录控制与管理简介

为了加强设备的操作安全性，在用户登录或者 enable 操作时提供了多种类型的认证管理（包括 AAA，参考《AAA 配置手册章节》），只有拥有相应权限的用户登录或者 enable 操作才会成功。

为了给不同级别的用户授权不同级别的可执行命令集合，设备的命令分为 0~15 级，用户级别分为 0~15 级。其中级别 0 的权限最低，级别 15 的权限最高。

3.2 登录控制与管理功能配置

表 3-1 登录控制与管理配置列表

配置任务	
切换用户级别	切换用户级别
配置命令级别	配置命令级别
配置 enable 密码	配置 enable 密码
配置用户及相关属性	配置自动执行命令
	配置登录时无需密码验证
	配置用户密码
	配置用户授权级别
配置 line 属性	进入 Console 口 line 配置模式
	进入 Telnet 或 SSH 用户 line 配置模式
	配置登录用户操作绝对时间
	配置登录用户被授权级别

配置任务	
	配置用户登录自动执行命令
	配置用户登录自动执行命令选项
	配置登录用户空闲超时时间
	配置 line 密码
	配置登录认证方式
	配置 line 授权方式
	配置 line 统计方式
	启用 Console 口 Modem 功能
	配置用户登录超时时间

3.2.1 切换用户级别

-B -S -E -A

如果配置了相应级别的用户密码，就可以用 enable level (0~15) 命令输入正确的密码后进入相应的用户等级。同时拥有小于等于相应命令等级的执行权限。

如果当前用户级别高于要进入的用户级别，则不需要任何认证，直接进入相应级别。如果要进入的级别高于当前用户的级别，则根据当前配置会需要认证，认证方法根据配置的情况来选择。

如果配置了相应级别的 enable 密码（通过命令 **enable password level** 来配置），假如没有配置 AAA 的 enable 认证或者 AAA 的 enable 认证使用 enable 方法，则使用该密码进行验证。

如果没有配置相应级别的 enable 密码，但是 enable 认证方法是使用本地 enable 密码认证，分为 2 种情况：

a) 如果是 Telnet 用户，则不能成功，没有配置 AAA 会提示：% No password set，配置了 AAA 会提示：% Error in authentication。

b) 如果是 Console 口用户，配置了 AAA，则 enable 登录会先试着使用 enable 密码进行验证，如果没有设置 enable 密码，则使用 none 认证方法，即缺省通过。没有配置 AAA，则提示：% No password set，认证不成功。

如果 enable 认证成功，则进入刚才指定的用户级别，且当前用户拥有相应级别。通过命令 **show privilege** 可以看到当前的用户级别。

如果配置了 `aaa authentication enable default method`，使用相应的方法列表来进行 enable 认证，则需要使用相应的方法来认证，分为：

a) 如果配置：`aaa authentication enable default none`，则无需任何密码。

b) 如果配置：`aaa authentication enable default line`，并且配置了 line 密码，，则使用该密码，否则提示：% Error in authentication，认证失败。

c) 如果配置：`aaa authentication enable default radius`，使用 radius 认证。注意，radius 的 enable 认证用户名是固定的，就是 `$enab+level$`，level 是 1~15 的数字，就是要进入的级别。考虑到 radius 使用的是固定规则的用户名，认证时不需要输入用户名，只需要输入密码就可以了。如果 radius 服务器上为相应级别的用户名设置了密码，则输入相应的密码登录成功，否则失败。比如执行命令 `enable 10`，则使用的固定用户名为 `$enab10$`，如果 radius 服务器上有该用户名，则输入该用户名对应的密码就认证成功。

d) 如果配置：`aaa authentication enable default tacacs`，使用 tacacs 认证。如果登录时有用户名，则不用另外输入用户名，直接使用登录的用户名，输入该用户名的 enable 密码；否则要求输入用户名和该用户名的 enable 密码。如果输入的用户名在 tacacs 服务器上存在，并且设置了 tacacs 的 enable 密码，则认证成功，否则失败。

说明：

- 上面的几种 enable 认证方法可组合使用。
-

配置条件

无

切换用户级别

如果用户有相应的权限，则能够在普通用户模式下，通过命令切换用户级别进入特权用户模式，并且拥有对应级别的用户权限。如果在特权用户模式下执行该命令，将会根据命令的参数切换用户的级别。

表 3-2 切换用户级别

步骤	命令	说明
切换用户级别	enable [<i>level-number</i>]	必选 缺省情况下，用户级别为 15 级

3.2.2 配置命令级别

-B -S -E -A

配置条件

无

配置命令级别

在应用程序中的每个 shell 命令都有一个缺省级别，但是可以通过命令 **privilege** 来修改命令的缺省级别。当前用户只能执行级别小于等于自己级别的命令。比如用户级别为 12 的用户，只能执行 0 ~ 12 级别的命令。配置命令级别时，需要借助命令所在的模式，可以修改指定模式下具体的命令或者所有命令的级别。

表 3-3 配置命令级别

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置命令级别	privilege <i>privilege-mode</i> level <i>level-number</i> [all command <i>command-line</i>]	必选

3.2.3 配置 enable 密码

-B -S -E -A**配置条件**

无

配置 enable 密码

配置 enable 密码是指配置各级别用户进入本地的 enable 密码，如果命令中没有指定 enable 的级别，那么缺省情况下就是 15 级别的 enable 密码。

表 3-4 配置 enable 密码

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 enable 密码	enable password [level level-number] [0] password	必选 缺省情况下，没有配置 enable 密码

3.2.4 配置 line 属性

-B -S -E -A

设备中最多可以支持一个 Console 口用户、16 个 Telnet 用户或者 SSH 用户同时登录，line 命令可以为这些登录用户设置不同的认证、授权等属性。

配置条件

无

进入 Console 口 line 配置模式

当需要配置 Console 口的属性的时候，需要先进入 Console 口 line 配置模式。

表 3-5 进入 Console 口 line 配置模式

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 Console 口 line 配置模式	line con 0	必选

进入 Telnet 或 SSH 用户 line 配置模式

当需要配置 Telnet 或 SSH 的属性的时候，需要先进入 Telnet 或 SSH 的 line 配置模式。

表 3-6 进入 Telnet 或 ssh 用户的 line 配置模式

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 Telnet 或 SSH 用户的 line 配置模式	line vty { vty-min-number } [vty-max-number]	必选

配置登录用户操作绝对时间

登录用户操作的绝对时间是指从用户登录成功到自动退出的超时时间，单位为分钟。如果配置为 0，则表示不限制时间长短。缺省情况下，该时间配置是 0。其中，当到达配置时间之前的 5 秒钟时会给出一个提示：Line timeout expired。

表 3-7 配置允许登录用户操作的绝对时间

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 Console 口或者 vty 的 line 配置模式	line { con 0 vty vty-min-number [vty-max-number] }	必选

步骤	命令	说明
配置允许登录用户操作的绝对时间	absolute-timeout <i>absolute-timeout-number</i>	必选 缺省情况下，操作的绝对时间为 0，即无限长时间

配置登录用户授权级别

配置登录用户被授权的级别，缺省级别为 1。用户只能执行级别小于等于当前用户级别的命令。

表 3-8 配置登录用户被授权的级别

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 Console 口或者 vty 的 line 配置模式	line { con 0 vty vty-min-number [vty-max-number] }	必选
配置登录用户被授权的级别	privilege level level-number	必选 缺省情况下，被授权的用户级别为 1

配置访问控制列表

设置用户访问控制列表，只有访问控制列表允许的主机才能对设备进行登录。

表 3-9 配置 line 访问控制列表

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
进入者 vty 的 line 配置模式	line { vty <i>vty-min-number</i> [<i>vty-max-number</i>] }	必选
配置访问控制列表	access-class { <i>access-list-number</i> <i>access-list-name</i> } { in out }	必选
配置 ipv6 ACL 控制列表	ipv6 access-class { <i>access-list-number</i> <i>access-list-name</i> }{ in out }	可选

配置用户登录自动执行命令

设置登录用户登录成功后自动执行的命令，缺省为不执行任何命令。

表 3-10 配置登录用户登录成功后自动执行的命令

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 Console 口或者 vty 的 line 配置模式	line { con 0 vty <i>vty-min-number</i> [<i>vty-max-number</i>] }	必选
配置登录用户登录成功后自动执行的命令	autocommand <i>command-line</i>	必选

配置用户登录自动执行命令选项

用户可以对自动执行命令配置延迟执行的时间，还可以配置自动执行完后是否断开用户连接。缺省情况下，对命令自动执行的时间不进行延迟，自动执行完后断开用户连接。

配置用户执行自动命令的选项有延迟执行及执行后不断开连接等选项。

表 3-11 配置用户登录自动执行命令选项

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 Console 口或者 vty 的 line 配置模式	line { con 0 vty vty-min-number [vty-max-number] }	必选
配置登录用户执行自动命令的选项	autocommand-option { nohangup [delay delay-time-number] delay delay-time-number [nohangup] }	必选

说明：

- **autocommand-option** 命令只有配置了 **autocommand** 功能后才能生效。

配置登录用户空闲超时时间

当登录用户没有对设备进行操作的时间大于空闲超时时间时，设备将退出当前登录用户。缺省的空闲超时退出时间为 5 分钟。如果配置时间为 0，则空闲超时不退出。

表 3-12 配置空闲超时退出时间

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
进入 Console 口或者 vty 的 line 配置模式	line { con 0 vty vty-min-number [vty-max-number] }	必选
配置空闲超时退出时间	exec-timeout <i>exec-timeout-minute_number [exec-timeout-second_number]</i>	必选 缺省情况下，空闲超时退出时间为 5 分钟

配置 line 密码

对于配置 line 的密码内容是明文还是密文，用 0 和 7 来区分，0 对应的密码为明文，7 对应的密码为密文。在交互模式下，只能设置密码为明文，即只能使用参数 0。

表 3-13 配置 line 密码

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 Console 口或者 vty 的 line 配置模式	line { con 0 vty vty-min-number [vty-max-number] }	必选
配置 line 密码	password 0 password	必选

配置登录认证方式

设备中的登录认证方式包括以下几种：

login password 登录认证方式：使用的是 line 密码认证；

login aaa 登录认证方式：使用的是 AAA 认证；

no login 表示不需要认证就可以登录；

Telnet 缺省使用 no login 登录认证方式，SSH 缺省使用本地用户认证方式。

表 3-14 配置登录认证方式

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 Console 口或者 vty 的 line 配置模式	line { con 0 vty vty-min-number [vty-max-number] }	必选
配置登录认证方式	login {aaa [domain-name default] password}	这个命令会同时影响 AAA 认证、授权、计费

配置用户登录超时时间

当用户登录设备的时候，如果输入用户名或密码的等待时间超时，那么系统会提示登录失败，缺省情况下，登录超时时间是 30 秒。当用户需要修改等待超时时间时，可以使用该功能进行配置。

表 3-15 配置等待用户登录的超时时间

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 Console 口或者 vty 的 line 配置模式	line { con 0 vty vty-min-number [vty-max-number] }	必选
配置等待用户登录的超时时间	timeout login respond respond-time-value	必选 缺省情况下，等待输入用户名或者密码的时间为 30 秒

表 3-16 登录控制与管理监控与维护

命令	说明
clear line { con <i>con-number</i> vty <i>vty-number</i> }	清除某个终端服务
show privilege	查看当前用户的级别
show users	查看配置的用户信息

4 FTP、FTPS、TFTP 和 SFTP 简介

FTP 用于在服务器和客户机之间传输文件，目的是提高文件的共享性，为用户与远程计算机之间提供了一种高效、可靠传送数据的方式。FTP 协议一般使用 TCP 端口 20 和 21 进行传输。端口 20 用于主动模式下传输数据，端口 21 用于传输控制消息。

同大多数 Internet 服务一样，FTP 也是采用的客户/服务器通信机制。要连上 FTP 服务器一般要有该 FTP 服务器授权的帐号，互联网中有很一部分 FTP 服务器是匿名 FTP 服务器，这类服务器的目的是向公众提供文件拷贝服务，不要求用户事先在该服务器进行登记注册，也不用取得 FTP 服务器的授权。

FTP 有两种文件传输模式：

- ASCII 传输模式，用于传输文本文件；
- 二进制传输模式，用于传输程序文件。

设备作为 FTP 客户端时只使用二进制传输模式，作为 FTP 服务器时两种传输模式都支持。

FTP 有两种工作方式：

- 主动方式：FTP 客户端首先和 FTP 服务器的 TCP21 端口建立连接，通过这个通道发送命令，客户端需要接收数据的时候在这个通道上发送 PORT 命令。PORT 命令包含了客户端用什么端口接收数据。在传送数据的时候，服务器端通过自己的 TCP20 端口连接至客户端的指定端口发送数据。FTP 服务器必须和客户端建立一个新的连接用来传送数据；
- 被动方式：在建立控制通道时和主动方式类似，但建立连接后发送的不是 PORT 命令，而是 PASV 命令。FTP 服务器收到 PASV 命令后，随机打开一个高端端口（端口号大于 1024）并且通知客户端在这个端口上传送数据，客户端连接 FTP 服务器此端口，然后 FTP 服务器将通过这个端口进行数据的传送。

许多内网的客户端不能用主动模式登陆 FTP 服务器，因为服务器无法和内部网络的客户端建立一个新的连接，从而导致无法工作。

设备作为 FTP 客户端时采用主动模式与服务器建立数据连接。

FTPS 是在安全套接层使用标准的 FTP 协议和指令的一种增强型 FTP 协议，为 FTP 协议和数据通道增加了 SSL 安全功能。FTPS 也称作“FTP-SSL”和“FTP-over-SSL”。SSL 是一个在客户机和具有 SSL 功能的服务器之间的安全连接中对数据进行加密和解密的协议。设备上只有 FTP 客户端支持该功能。TFTP 是一个简单的文件传输协议，它基于 UDP 协议实现，使用 UDP 端口 69 进行数据传输。此协议是为进行小文件传输而设计的，因此它不具备 FTP 协议的许多功能，不能列出目录，不能进行认证等。设备上只实现了 TFTP 客户端功能。

SFTP（Secure File Transfer Protocol /Secure FTP）安全文件传送协议，是 SSH 2.0 中新增的功能。SFTP 建立在 SSH 连接的基础之上，它使得远程用户可以安全地登录设备，进行文件管理和文件传送等操作，为数据传输提供了更高的安全保障。SFTP 为传输文件提供一种安全方法。SFTP 是 SSH 的子功能，实现了文件的安全传输。SFTP 要加密传输认证信息和传输的数据，所以使用 SFTP 是非常安全的，如果对网络安全性要求较高时，可以使用 SFTP 代替 FTP。但是由于 SFTP 文件传输使用了加密/解密技术，所以传输效率比 FTP 文件传输要低。

4.1 FTP、FTPS、TFTP 和 SFTP 功能配置

表 4-1 FTP 和 TFTP 功能配置列表

配置任务	
配置 FTP 服务器	配置 FTP 服务器功能
配置 FTP 客户端	配置 FTP 客户端功能
配置 TFTP 客户端	配置 TFTP 客户端功能
配置 SFTP 服务器	配置 SFTP 服务器功能
配置 SFTP 客户端	配置 SFTP 客户端功能

4.1.1 配置 FTP 服务器

-B -S -E -A

配置条件

无

配置 FTP 服务器功能

配置设备作为 FTP 服务器，需要首先开启 FTP 服务器功能，FTP 客户端才能访问。出于安全考虑，设备只对授权用户提供 FTP 服务，并且限制了允许同时登录的最大用户数。

表 4-2 配置 FTP 服务器功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
开启 FTP 服务器功能	ftp enable	必选

步骤	命令	说明
		缺省情况下，没有开启 FTP 服务器功能
配置授权的用户名和密码	user <i>username</i> password 0 <i>password</i>	必选 缺省情况下，没有授权的配置用户名和密码 该命令的详细使用请参见“登录控制与管理”相关章节
配置 FTP 服务监听端口号	ftp listen-port [<i>port-num</i>]	可选 缺省情况下，FTP 服务的监听端口号为 21
配置允许同时登录的最大用户数	ftp max-user-num <i>user-num</i>	可选 缺省情况下，允许同时登录的最大用户数为 1
配置连接超时时间	ftp timeout <i>time</i>	可选 缺省情况下，连接超时时间为 300 秒

4.1.2 配置 FTP 客户端

-B -S -E -A

配置条件

无

配置 FTP 客户端功能

在设备上采用 **copy** 命令复制文件（请参见“文件系统管理”相关章节）或者采用 **sysupdate** 命令升级软件版本（请参见“软件升级”相关章节）时，可以触发设备作为 FTP 客户端，与远程的 FTP 服务器建立连接。

FTP 客户端与 FTP 服务器建立连接时，系统缺省情况下，使用到 FTP 服务器的路由出接口地址作为源地址。用户也可以通过 **ip ftp source-address**、**ip ftp source-interface** 命令来指定 FTP 客户端源地址或者源接口。

表 4-3 配置 FTP 客户端功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 FTP 客户端源地址	ip ftp { source-interface <i>interface-name</i> source-address <i>ip-address</i> }	可选 缺省情况下，使用到 FTP 服务器的路由出接口地址，作为源地址与 FTP 服务器通信
配置 FTP 客户端优先使用 port 模式	ip ftp port-first	可选 缺省情况下，优先使用 passive 模式与服务器建立数据连接

说明：

- 在某些网络环境下，因为安全因素，可能限制了设备到 FTP 服务器的路由出接口地址与 FTP 服务器之间通信，但其它业务接口地址可通，此时可以采用 **ip ftp source-address**、**ip ftp source-interface** 命令指定 FTP 客户端源地址或者源接口。

4.1.3 配置 TFTP 客户端 **-B -S -E -A****配置条件**

无

配置 TFTP 客户端功能

在设备上采用 **copy** 命令复制文件（请参见“文件系统管理”相关章节）或者采用 **sysupdate** 命令升级软件版本（请参见“软件升级”相关章节）时，可以触发设备作为 TFTP 客户端，与远程的 TFTP 服务器建立连接。

TFTP 客户端与 TFTP 服务器建立连接时，系统缺省情况下，使用到 TFTP 服务器的路由出接口地址作为源地址。用户也可以通过 **ip tftp source-address**、**ip tftp source-interface** 命令来指定 TFTP 客户端源地址或者源接口。

表 4-4 配置 TFTP 客户端功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 TFTP 客户端源地址	ip tftp { source-interface <i>interface-name</i> source-address <i>ip-address</i> }	可选 缺省情况下，使用到 TFTP 服务器的路由出接口地址，作为源地址与 TFTP 服务器通信

说明：

- 在某些网络环境下，因为安全因素，可能限制了设备到 TFTP 服务器的路由出接口地址与 TFTP 服务器之间的通信，但其它业务接口地址可通，此时可以采用 **ip tftp source-address**、**ip tftp source-interface** 命令指定 TFTP 客户端源地址或者源接口。

4.1.4 配置 TFTP 服务器 **-B -S -E -A**

配置条件

无

配置 TFTP 服务器功能

配置设备作为 TFTP 服务器，需要首先开启 TFTP 服务器功能，TFTP 客户端才能访问。

表 4-5 配置 TFTP 服务器功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
开启 TFTP 服务器功能	tftp enable	必选 缺省情况下，没有开启 TFTP 服务器功能

4.1.5 配置 SFTP 服务器 **-B -S -E -A**

配置条件

无

配置 SFTP 服务器功能

配置设备作为 SFTP 服务器，需要首先开启 SFTP 服务器功能，SFTP 客户端才能访问。由于 SFTP 属于 SSH 的一个附属子功能，开启 SFTP 服务与开启 SSH 远程登陆服务的配置相同。

表 4-6 配置 SFTP 服务器功能

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
开启 SFTP 服务器功能	ip ssh server [sshv1-compatible] [listen-port]	必选 缺省情况下，没有开启 SFTP 服务器功能

4.1.6 配置 SFTP 客户端 *-B -S -E -A*

配置条件

无

配置 SFTP 客户端功能

设备作为 SFTP 客户端，连接 SFTP 服务器，从 SFTP 服务器下载文件或向 SFTP 服务器上传文件。

表 4-7 配置 SFTP 客户端功能

步骤	命令	说明
配置设备作为 SFTP 客户端向 SFTP 服务器上传或下载文件	sftp { get put } [vrf vrf-name] host-ip-address port-number [source-interface interface-name] user password src-filename dest-filename [compress]	可选

4.1.7 FTP 和 TFTP 监控与维护 **-B -S -E -A**

无

4.2 FTP 和 TFTP 典型配置举例

4.2.1 配置设备作为 FTP 客户端 **-B -S -E -A**

网络需求

- PC 作为 FTP 服务器，设备 Device 作为 FTP 客户端；服务器和设备网络连通。
- FTP 服务器上设置设备登录 FTP 服务器的用户名为 admin，密码为 admin；将需要下载的文件放到 FTP 服务器的目录下。
- 设备作为 FTP 客户端，与 FTP 服务器之间上传、下载文件。

网络拓扑



图 4-1 配置设备作为 FTP 客户端组网图

配置步骤

- 步骤 1： 创建 VLAN，并将端口加入对应的 VLAN。（略）
- 步骤 2： 配置 FTP 服务器，将需要下载的文件放到 FTP 服务器的目录下。（略）
- 步骤 3： 配置各设备 IP 地址，使客户端与服务器网络连通。（略）
- 步骤 4： Device 作为 FTP 客户端，与 FTP 服务器之间上传、下载文件。

#在 Device 的文件系统模式下从 FTP 服务器 copy 一个文件到 Device 的文件系统中。

```
Device#filesystem
Device(config-fs)#copy ftp 2.0.0.1 admin admin sp4-g-6.5.0(41).pck file-system sp4-g-6.5.0(41).pck
```

```
Device (config-fs)#exit
```

#在 Device 文件系统模式下将 Device 的 startup 文件 copy 到 FTP 服务器。

```
Device#filesystem
Device(config-fs)#copy file-system startup ftp 2.0.0.1 admin admin startup.txt
```

步骤 5: 检验结果。

#copy 完成后, 可以在 Device 文件系统中查看下载的文件是否存在; 在 FTP 服务器上查看上传的文件是否存在 (略)。

```
Device(config-fs)#dir
size      date      time      name
-----
101526    MAR-01-2013 01:17:18 logging
10147     MAR-26-2013 07:58:50 startup
10207     MAR-01-2013 01:17:54 history
1372      MAR-23-2013 08:18:38 devInfo
6598624   MAR-26-2013 07:51:32 sp4-g-6.5.0(41).pck
1024      JAN-10-2013 17:30:20 snmp          <DIR>
0         JAN-31-2013 14:29:50 syslog
736512    MAR-27-2013 10:30:48 web-Spl-1.1.168.rom
```

说明:

- 如果打印 “FTP: Ctrl socket connect error(0x3c): Operation timed out” 表示不能正常连接到服务器, 可能原因是路由不可达或者服务器未开启。
 - 如果打印 “Downloading##OK!” 的提示信息, 表示 copy 文件成功。
-

4.2.2 配置设备作为 FTP 服务器 **-B -S -E -A**

网络需求

- Device1 作为 FTP 服务器, PC、Device2 作为 FTP 客户端; 客户端和服务器网络连通。
- FTP 服务器 Device1 上设置用户名为 admin, 密码为 admin, Device1 的文件系统目录作为 FTP 服务器根目录。
- PC、Device2 作为 FTP 客户端, 与 FTP 服务器 Device1 之间上传、下载文件。

网络拓扑

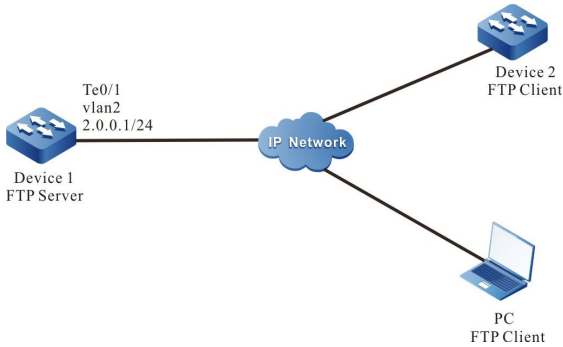


图 4-2 设备作为 FTP 服务器组网图

配置步骤

步骤 1: 创建 VLAN, 并将端口加入对应的 VLAN。 (略)

步骤 2: 配置各接口的 IP 地址, 使 PC、Device2 与 Device1 网络连通。 (略)

步骤 3: 在 Device1 上, 使能 FTP 服务, 配置授权的用户名和密码。

#在 FTP 服务器 Device1 上配置授权的用户名和密码。

```
Device1#configure terminal
Device1(config)#user admin password 0 admin
```

#在 Device1 上开启 FTP 服务。

```
Device1(config)#ftp enable
```

#在 Device1 上配置最大同时连接的用户数为 2。

```
Device1(config)#ftp max-user-num 2
```

步骤 4: 检验结果。

#查看 Device1 的 FTP 服务功能是否开启。

```
Device#show ip sockets
Active Internet connections (including servers)
PCB Proto Recv-Q Send-Q Local Address Foreign Address vrf (state)
-----
27cf8a4 TCP 0 0 0.0.0.0.80 0.0.0.0 all LISTEN
27ce0a4 TCP 0 0 130.255.104.43.22 130.255.98.2.3590 global ESTABLISHED
27d0be4 TCP 0 0 0.0.0.0.21 0.0.0.0 all LISTEN
27d0824 TCP 0 0 127.0.0.1.2622 127.0.0.1.1026 global ESTABLISHED
```

如果 FTP 服务功能已经开启，可以看到端口号 21 处于 listen 状态。

步骤 5： 使用 Device2 作为 FTP 客户端，从 FTP 服务器 Device1 上 copy 一个 startup 文件到本地。

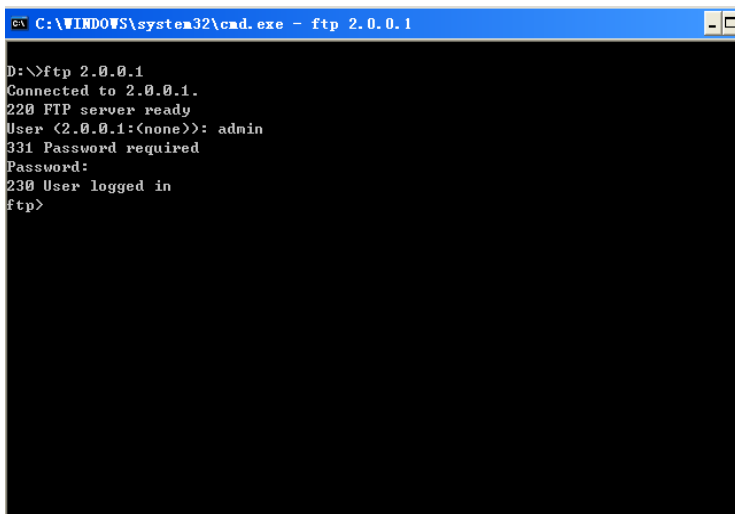
```
Device2#filesystem
Device2(config-fs)#copy ftp 2.0.0.1 admin admin startup file-system startup
```

步骤 6： 使用 PC 作为 FTP 客户端，从 FTP 服务器 Device1 上 copy 一个 startup 文件到 PC。

#如下以 Windows DOS 界面为例描述相关过程。

#在 DOS 界面上输入正确的 IP 地址和用户名、密码登录到 FTP 服务器上。

```
D:\>ftp 2.0.0.1
Connected to 2.0.0.1.
220 FTP server ready
User (2.0.0.1:(none)): admin
331 Password required
Password:
230 User logged in
ftp>
```



```
C:\WINDOWS\system32\cmd.exe - ftp 2.0.0.1
D:\>ftp 2.0.0.1
Connected to 2.0.0.1.
220 FTP server ready
User (2.0.0.1:(none)): admin
331 Password required
Password:
230 User logged in
ftp>
```

图 4-3 在 DOS 界面上登录到 FTP 服务器上

#配置 PC 和 FTP 服务器以二进制方式进行数据传输。

```
ftp>binary
```

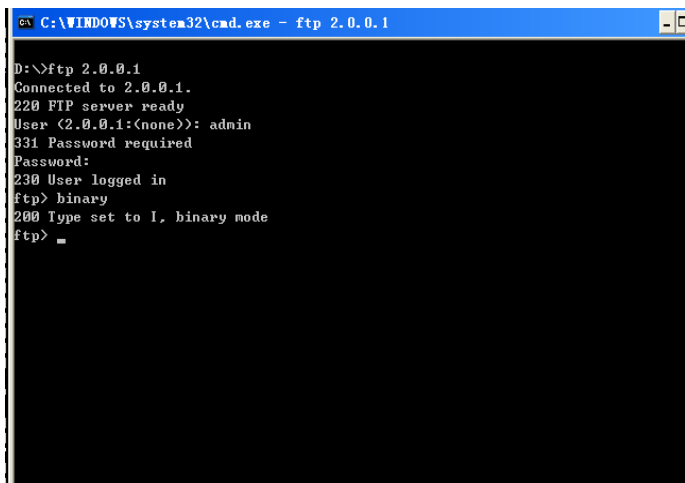


图 4-4 设置 PC 和 FTP 服务器以二进制方式进行传输

#获取 FTP 服务器 Device1 文件系统中的 startup 文件。

ftp>get startup

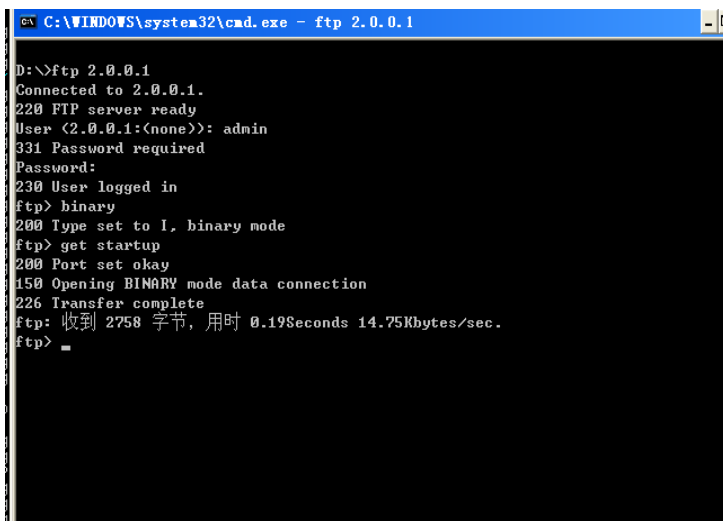


图 4-5 从 FTP 服务器复制一个配置文件

文件复制完成后，可以在操作的 Windows 目录下找到相关文件。

说明：

- 如果打印 “421 Session limit reached, closing control connection” 表示已经超过服务器允许的最大连接数。
- 使用设备 copy 文件的时候，如果打印 “FTP: Ctrl socket connect error(0x3c): Operation timed out” 可能是由于服务器端未开启服务器功能或者服务器和客户端

路由不可达。

- 在客户端 PC 上操作 FTP 连接服务器的时候，如果打印 “> FTP: connect :未知错误号” 可能是由于服务器端未开启服务器功能或者服务器端和客户端路由不可达。

4.2.3 配置设备作为 TFTP 客户端

-B -S -E -A

网络需求

- PC 作为 TFTP 服务器，设备 Device 作为 TFTP 客户端；服务器和设备网络连通。将需要下载的文件放到 TFTP 服务器的目录下。
- 设备作为 TFTP 客户端，与 TFTP 服务器之间上传、下载文件。

网络拓扑



图 4-6 设备作为 TFTP 客户端组网图

配置步骤

- 步骤 1： 创建 VLAN，并将端口加入对应的 VLAN。（略）
- 步骤 2： 配置各接口的 IP 地址，使客户端与服务器网络连通。（略）
- 步骤 3： 在 PC 上使能 TFTP 服务器功能，将需要下载的文件放到 TFTP 服务器的目录下。（略）
- 步骤 4： Device 作为 TFTP 客户端，与 TFTP 服务器之间上传、下载文件。

#在 Device 上从 TFTP 服务器 copy 一个文件到 Device 的文件系统中。

```
Device#filesystem
Device(config-fs)#copy tftp 2.1.2.1 sp4-g-6.5.0(41).pck file-system sp4-g-6.5.0(41).pck
Device(config-fs)#exit
```

#在 Device 上将 Device 的 startup 文件 copy 到 TFTP 服务器。

```
Device#filesystem
Device(config-fs)#copy startup-config tftp 2.1.2.1 startup.txt
```

步骤 5: 检验结果。

copy 完成后, 可以在 Device 文件系统中查看下载的文件是否存在; 在 TFTP 服务器上查看上传的文件是否存在。(略)

```
Device(config-fs)#dir
size      date      time      name
-----
102227    MAR-01-2013 05:24:32 logging
10147     MAR-26-2013 07:58:50 startup
10202     MAR-01-2013 05:26:46 history
6598624   MAR-26-2013 07:51:32 sp4-g-6.5.0(41).pck
1024      JAN-10-2013 17:30:20 snmp          <DIR>
0         JAN-31-2013 14:29:50 syslog
736512    MAR-27-2013 10:30:48 web-Spl-1.1.168.rom
```

说明:

- 如果打印 “Downloading####OK!” 的提示信息, 表示 copy 文件成功, 打印信息显示的文件大小, 跟文件实际大小相关。
 - 使用设备进行 copy 文件的时候, 如果打印 “tftp: Failed! ErrorNum: 0x41, ErrorType: Host unreach.” 可能是由于服务器未开启 TFTP 服务功能或者服务器和客户端路由不可达。
-

4.2.4 配置设备作为 SFTP 客户端

-B -S -E -A

网络需求

- PC 作为 SFTP 服务器, 设备 Device 作为 SFTP 客户端; 服务器和设备网络连通。
- SFTP 服务器上设置设备登录 SFTP 服务器的用户名为 admin, 密码为 admin; 将需要下载的文件放到 SFTP 服务器的目录下。
- 设备作为 SFTP 客户端, 与 SFTP 服务器之间上传、下载文件。

网络拓扑



图 4-7 配置设备作为 SFTP 客户端组网图

配置步骤

- 步骤 1: 配置 SFTP 服务器，将需要下载的文件放到 SFTP 服务器的目录下。（略）
- 步骤 2: 配置各设备 IP 地址，使客户端与服务器网络连通。（略）
- 步骤 3: Device 作为 SFTP 客户端，与 SFTP 服务器之间上传、下载文件。

#从 SFTP 服务器下载一个文件到设备的文件系统中

```

Device#sftp get 2.0.0.1 22 admin admin sp8-g-6.6.7(46)-dbg.pck sp8-g-6.6.7(46)-dbg.pck
The authenticity of host '2.0.0.1 (2.0.0.1)' can't be established.
RSA key fingerprint is e4:dd:11:2e:82:34:ab:62:59:1c:c8:62:1d:4b:48:99.
Are you sure you want to continue connecting (yes/no)? yes

Downloading#####
#####
    
```

#将 Device 文件系统下的 startup 文件上传到 SFTP 服务器

```

Device#sftp put 2.0.0.1 22 admin admin startup startup.txt
The authenticity of host '2.0.0.1 (2.0.0.1)' can't be established.
RSA key fingerprint is e4:dd:11:2e:82:34:ab:62:59:1c:c8:62:1d:4b:48:99.
Are you sure you want to continue connecting (yes/no)? yes
Uploading#####
#####
###
    
```

- 步骤 4: 检验结果。

#拷贝完成后，可以在 Device 文件系统中查看下载的文件是否存在；在 SFTP 服务器上查看上传的文件是否存在（略）。

```

Device(config-fs)#dir
size      date      time      name
-----
101526    MAR-01-2015 01:17:18 logging
10147     MAR-26-2015 07:58:50 startup
10207     MAR-01-2015 01:17:54 history
11676148  MAR-26-2013 07:51:32 sp8-g-6.6.7(46)-dbg.pck
2048     JAN-10-2015 17:30:20 snmp          <DIR>
    
```

4.2.5 配置设备作为 SFTP 服务器

-B -S -E -A

网络需求

配置手册

- • Device 作为 SFTP 服务器，PC 作为 SFTP 客户端；客户端和服务器网络连通。
- • SFTP 服务器 Device 上设置用户名为 admin，密码为 admin，Device 的文件系统目录作为 SFTP 服务器根目录。
- • PC 作为 SFTP 客户端，与 SFTP 服务器 Device 之间上传、下载文件。

网络拓扑



图 4-8 配置设备作为 SFTP 服务器组网图

配置步骤

步骤 1： 配置各接口的 IP 地址，使 PC 与 Device 网络连通。（略）

步骤 2： 在 Device 上，使能 SFTP 服务，配置授权的用户名和密码。

#在 SFTP 服务器 Device 上配置授权的用户名和密码

```
Device#configure terminal
Device(config)#user admin password 0 admin
```

#在 Device 上开启 SSH 服务（SFTP 是 SSH 协议的一个子模块）

```
Device(config)#ip ssh server
```

步骤 3： 使用 PC 作为 SFTP 客户端，上传、下载一个文件到 SFTP 服务器 Device 上。

#如下以 Linux 系统为例描述相关过程

#输入正确的 IP 地址和用户名、密码登录到 SFTP 服务器上

```
[root@aas ~]# sftp admin@2.1.1.1
Connecting to 2.1.1.1...
admin@2.1.1.1's password:
sftp>
```

#获取 SFTP 服务器 Device 文件系统中的 startup 文件

```
sftp> get startup startup
Fetching /flash/startup to startup
/flash/startup 100% 13KB 12.9KB/s 00:00
```

#文件复制完成后，可以在操作的目录下找到相关文件

```
sftp> ls
sp8-g-6.6.7(74)-dbg.pck sp8-g-6.6.7(76)-dbg.pck startup          tech          test_pc
sftp>
```

#将 PC 中的文件上传到 SFTP 服务器 Device 文件系统中。

```
sftp> put sp8-g-6.6.7(76)-dbg.pck sp8-g-6.6.7(76)-dbg.pck
Uploading sp8-g-6.6.7(76)-dbg.pck to /flash/ sp8-g-6.6.7(76)-dbg.pck
sp8-g-6.6.7(76)-dbg.pck                               100% 11424KB 16.0KB/s 00:00
```

#文件上传完成后，可以在 Device 的文件系统中找到对应的文件

```
Device(config-fs)#dir
size      date       time      name
-----
2048      JUN-30-2015 16:35:50 tech      <DIR>
10229     JUN-12-2015 14:31:22 history
101890    JUN-30-2015 17:46:40 logging
39755     JUN-30-2015 16:33:56 startup
740574    MAY-27-2014 18:55:14 web-Spl-1.1.243.rom
2048      JUN-27-2015 16:26:10 snmp      <DIR>
11698172  JUN-30-2015 10:36:18 sp8-g-6.6.7(76)-dbg.pck
```

4.2.6 配置设备作为 FTPS 客户端

-B -S -E -A

网络需求

- • PC 作为 FTP Server，设备 Device 作为 FTP Client；Server 和 Client 网络连通。
- • 在 FTP Server 端和 FTP Client 通过建立安全数据通道，为数据传输提供安全保障。
- • FTP Client 与 FTP Server 之间能够上传、下载文件。

网络拓扑



图 4-9 配置设备为 FTPS Client 组网图

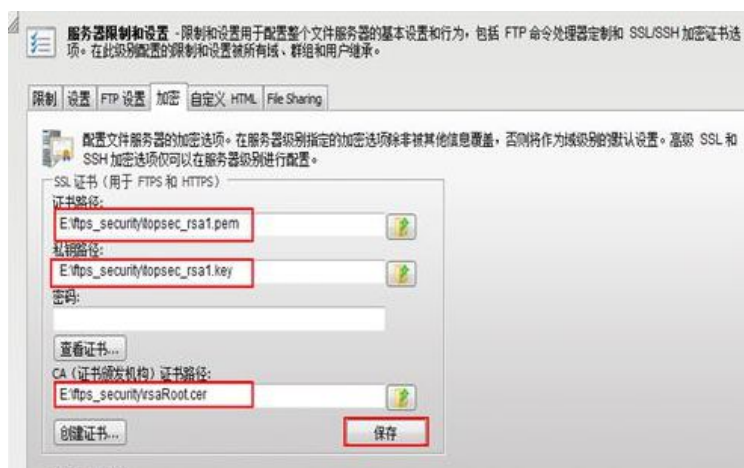
配置步骤

配置手册

发布 1.1 04/2020

步骤 1: 配置各接口 IPv4 地址。（略）

步骤 2: FTP Server 端安装证书并设置 FTP 用户证书路径、私钥路径、CA 证书路径:



步骤 3: FTP Client 导入 FTP CA 证书、用户证书、私钥。

#在设备上创建一个域 test:

```
Device#configure terminal
Device(config)#crypto ca identity test
Device(ca-identity)#exit
```

#ftp 绑定域 test:

```
Device(config)#ip ftp secure-identity test
```

#把 CA 证书(rsaRoot.cer)用记事本打开,再拷贝里面的内容,在 shell 上输入 crypto ca import certificate to test,按照提示把证书导入到设备域 test:

```
Device(config)#crypto ca import certificate to test
% Input the certificate data, press <Enter> twice to finish:
-----BEGIN CERTIFICATE-----
MIIDBzCCAnCgAwIBAgIItpXH17Hj/AswDQYJKoZIhvcNAQEFBQAwYjELMAkGA1UE
BhMCQ04xEDA0BgNVBAGMB0JFSUpJTkcxDjAMBGNVBAoMBUNJRUNDMDQ8wDQYDVQQL
DAZHRkEgQ0ExIDAEbgNVBAMMF01pbmlDQSBGcmVU0QgUm9vdCBDZXJ0MjB4XDTA5
MDgwMzA2MDY1MloXDTE5MDgwMzA2MDY1MlowYjELMAkGA1UEBhMCQ04xEDA0BgNV
BAGMB0JFSUpJTkcxDjAMBGNVBAoMBUNJRUNDMDQ8wDQYDVQQLDAZHRkEgQ0ExIDAE
BgNVBAMMF01pbmlDQSBGcmVU0QgUm9vdCBDZXJ0MjB4XDTA5MDgwMzA2MDY1MloX
A4GMADCBiAKBgHXZMtpxzH8p0uUt6QomUhuJNcy9iyYhoJVx4l3T6kpmx9cdzapM
RoKUa9eB/jCzhgctQc7ZDUkP+gafHWgZtbzwwSVksVsNmFqBivixveGx9dCrtequ
+vDiXVvDVPNSDDTmamMGyYcb0N7aSOzdg6BYyQYy/Y0FK6/vv4NUxAgMBAAGj
gcYwgcmwPQYDVR0fBDYwNDAYoDCgLoYsaHR0cDovLzE2OC4xNjguMTCuNDY6OTAw
MC9nZmEvY3JsL2dmYWwFwC5jcmwwSAYDVR0gBEEwPzA9BggrBgEEAYcrMjAxMC8G
CCsGAQUFBwIBFiNodHRvOi8vd3d3LmdmYXBRa5S5jb20uY24vcG9saWN5LmRvY2E1
BgNVHQ8EBAMCAuQwDAYDVR0TBAUwAwEB/zAdBgNVHQ4EFgQUhny8uZXbE2iX1mXO
ipvfUdUgAeswDQYJKoZIhvcNAQEFBQADgYEAkNPdTE+YpfOQn8lW1oF7TkgJ/Vzd
c0O5UUB+jPhYkj+fxUX8WyxabOxgl3u+7DJ/3gHw1r08ZcDO94Wz+nBsile5tFv7
/bHz0yqJVoUJMlaWODmLXj5f15GeBCprzLM88RJCv6LBHfg4ThOC4Ds80Ssive1
eAod+7kbmVPOZg8=
-----END CERTIFICATE-----
```

% Input the private key data, press <Enter> twice after data to finish or press <Enter> without data to ignore:

% The Root CA Certificate has the following attributes:

Serial Number: 4e95c7d7b1e3fc0b
Subject: C=CN, ST=BEIJING, O=CIECC, OU=GFA CA, CN=MiniCA FreBSD Root Cert
Issuer: C=CN, ST=BEIJING, O=CIECC, OU=GFA CA, CN=MiniCA FreBSD Root Cert
Validity
Start date: 2009-08-03 06:06:52
End date: 2019-08-03 06:06:52
Usage: General
Fingerprint(sm3) :18d39e4c50c9ad8b11446ac7ac1736f853ac92e769994b98233b48787562429c
Fingerprint(sha1):ab3559e26384539ffcac3c76b5a5e7a1f7073dfb

% Do you accept this root ca-certificate[yes]/[no]:

% Please answer 'yes' or 'no'.

% Do you accept this root ca-certificate[yes]/[no]:

Nov 11 2015 19:06:04: %PKI-CERTIFICATE_STATECHG-5: Certificate(issuer:C=CN, ST=BEIJING, O=CIECC, OU=GFA CA, CN=MiniCA FreBSD Root Cert, sn:4E95C7D7B1E3FC0B, subject:C=CN, ST=BEIJING, O=CIECC, OU=GFA CA, CN=MiniCA FreBSD Root Cert) state valid
% PKI: Import Certificate success.

#把用户证书(topsec_rsa2_myself.pem)、私钥证书(topsec_rsa2_myself.key)用记事本打开，再拷贝里面的内容，在 shell 上输入命令 `crypto ca import certificate to test` 按照提示，把证书依次导入到设备域 test:

```
Device(config)#crypto ca import certificate to test
% Input the certificate data, press <Enter> twice to finish:
-----BEGIN CERTIFICATE-----
MIIDVTCCAr6gAwIBAgIQEJ7twbl3pDlZz99DFOKOzANBqkqhkiG9w0BAQUFADBiMQswCQYDVQQGEwJDTJJEQ
MA4GA1UECAwHQkvJskIORzEOMAwGA1UECgwFQ0IFQ0MxZmZANBgNVBAsMBkdGQSBDDQTEgMB4GA1UEA
wwXTWluaUNBIEZyZUJTRCBSb290IENlcnQwHhcNMjIwMDUwMTIzWhcNMzIwMDUwMTIzWjB/MQs
wCQYDVQQGEwJDTJJEQMA4GA1UECAwHYmVpamluZzESMBAGA1UEBwwJZG9uZ2NoZW5nMQ4wDAYDVQQ
KDAVjaWVjYzEMMAoGA1UECwwDZ2ZzMR0wGwYJKoZIhvcNAQkBFg50ZXN0QGVjLmNvbS55bjENMAsGA1UE
AwwEcnNhMjBzANBgkqhkiG9w0BAQEFAAOBjQAwYkCgYEA6AlNqTnNsV9Yyjt2TmPpB9C5VCLtkPh9Kllq/
ZTIVhrJED+N5HVfQqYzYS/z4JWAip50dyP1+NP+bpP+pb9CfEaJ8+ObYQnfUH6qiPccLkWO3XYanu6Dw5EMJY
ntwglSKmk1Pcc+j+yzWnwYMDfcbSsQ+8J5UzlesFhU7GnXacAAwEAAoB7jCB6zA+BgNVHR8ENzA1MDOgM
aAvhi1odHRwczovLzlxMS44OC4yNS4xODo4NDQ0L2dmYS9jcmwwUINBMTAyNC5jcmwwUQYDVROgBEowSD
BGBggrBgEEAYcrMjA6MDgGCCsGAQUFBwIBFixodHRwczovLzlxMS44OC4yNS4xODo4NDQ0L2dmYS9jcmwwU
INBMTAyNC5wbDALBgNVHQ8EBAMCA/gwCQYDVROTBAlwADAdBgNVHQ4EFgQUUp/9/ODGLR84syxPaBkLG3
mCpU5YHwHwYDVR0jBBgwFoAUhnY8uZXbE2iX1mXOipvfUDUgAeswDQYJKoZIhvcNAQEFBQADgYEAyrFZQrIN
HoLN9odcGctzTRGvmMcv9sJ0ncgUEfbrLu6QUodQy3jjxWFlxheJK1btff66/ShuKtZpqj1WE9I92tflHwLpXt0guit
xNi02TOPBNEU7P9nUgxfDG+uhyPTeufSkfn3LCTHmGfVORF2soGSLaUPV1Zy5E9hmFZOMhs=
-----END CERTIFICATE-----
```

% Input the private key data, press <Enter> twice after data to finish or press <Enter> without data to ignore:

```
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQDoCU2pOc2xX1jKkPa1MymkH0LIUlu2Q+H0qUir9IOVWgskQP43kdV9BDJlH/PglYCKnnR3I
/X40/5u8/6lv0J8RonZ45thCd9QfqqI9xwuRY7ddhqe7oPDkQwlie3CCVlqaTU9xz6P7LNafBgmVxtKxD7wnlTOV
6wWFTsaddpwIDAQABAoGBAMnJNwliJFgI4+1CvHGN4buhmApWBnnmBL1A7jrlh4CMGPi5MJrgzvjEsnlwfWI
XJXbSu4feujT1UFqMkuyIm9l+k8Rm3hjCIXlIfNV/ykG6a6GIVFYGxQWwHaL50Pm6S7xXL9Ryd6hnOHUUtwwLvkp
BTx/4qvrIABDtXRjVglvApAkeA9BN1ZxM31BOyeB6KXvmmXD6/+dGaDfE4Dbcijy1LgKliaEBJ00e/0R9ekg6myGT
U2asJvPtkaXPqcvwU6+e2mwJBAPNfRTk9LzUlNmTV2DrsE9k3rbPnqqS9wb/mLUNdV2FQeoY/Zf4qh0Wxsug2q
/6GpsvLUA7mbdArGFUwwQbw3+UCQC8r25LSOGX40JM6g8+bq4fEcOHdSoLLTeQlStstC9yP3/75/cqhoUjPY
z2jK0SriB+RWM53X46p4nPdo4b8P2RAkBGjoBLL+nXxooWgcjGjFrUxsedOLTIphtFvz2wliWx2NsswSZQ0skae5
8VB1ZFSJvguoa58M+bsAHMnrNdH+HhAkBcNAjKBDDvW0ll6bNoRgugEvuo3Z300kbVczjZld+4aVG4DzvEp1Zb
sYRv9YPMtpnzmb7WZUshAL99nHnHxtbh
-----END RSA PRIVATE KEY-----
```

Nov 11 2015 19:06:56: %PKI-CERTIFICATE_STATECHG-5: Certificate(issuer:C=CN, ST=BEIJING, O=CIECC, OU=GFA CA, CN=MiniCA FreBSD Root Cert, sn:109EEDC1B977A43973273F7D0C538A3B, subject:C=CN, ST=beijing, L=dongcheng, O=ciecc, OU=gfa, E=test@ec.com.cn, CN=rsa2) state valid
% PKI: Import Certificate success.

#证书导入成功后，通过 show crypto ca certificates 可以查看状态为 Valid：

```
Device#show crypto ca certificates
Root CA Certificate:
  Status: Valid
  Serial Number: 4e95c7d7b1e3fc0b
  Subject: C=CN, ST=BEIJING, O=CIECC, OU=GFA CA, CN=MiniCA FreBSD Root Cert
  Issuer : C=CN, ST=BEIJING, O=CIECC, OU=GFA CA, CN=MiniCA FreBSD Root Cert
  Validity
    Start date: 2009-08-03 06:06:52
    End date: 2019-08-03 06:06:52
  Key Type: RSA(1023 bit)
  Usage: General
  Fingerprint(sm3):18d39e4c50c9ad8b11446ac7ac1736f853ac92e769994b98233b48787562429c
  Fingerprint(sha1):ab3559e26384539ffcac3c76b5a5e7a1f7073dfb
  Associated Identity: test
    index: 3

My Certificate:
  Status: Valid
  Serial Number: 109eedc1b977a43973273f7d0c538a3b
  Subject: C=CN, ST=beijing, L=dongcheng, O=ciecc, OU=gfa, E=test@ec.com.cn, CN=rsa2
  Issuer : C=CN, ST=BEIJING, O=CIECC, OU=GFA CA, CN=MiniCA FreBSD Root Cert
  Validity
    Start date: 2012-06-26 05:01:23
    End date: 2032-06-26 05:01:23
  Key Type: RSA(1024 bit)
  Usage: General
  Fingerprint(sm3):504599a2f170c51b62b2f8b0850f33a5595bc9e592d14eae9c90b1e59de35a89
  Fingerprint(sha1):080614a82cc4f3786458c585f9a58edf19da19bd
  Associated Identity: test
    index: 4
```

步骤 4： FTP Client 与 FTP Server 之间上传、下载文件。

#FTP Client 向 FTP Server 上传文件：

```
Device#filesystem
Device1(config-fs)#copy file-system startup ftps 2.0.0.1 a a startup VerifyType peer

Copying!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Total 103440 bytes copying completed.
```

#FTP Client 从 FTP Server 下载文件：

```
Device(config-fs)#ftpscopy 2.0.0.1 a a test.doc test.doc VerifyType peer

Downloading#####
#####
##### OK!
```

步骤 5： 检验结果。

#下载完成后，在 Device 文件系统中查看下载的文件：

```
Device(config-fs)#dir
  size      date       time      name
-----
10189      NOV-04-2015 20:27:03 history
```

5 文件系统管理

5.1 文件系统管理简介

设备有以下几种存储介质，其用途如下：

- SDRAM：用作设备应用程序的执行空间；
- FLASH：用于存放设备应用程序、配置文件及 BootROM 程序等；
- EEPROM：用于存放经常改动的系统配置文件、用户信息等；
- USB：用于存放用户数据。

设备所管理的文件包括以下几种：

- BootROM 文件——存放系统初始化的基本数据；
- 设备应用程序——用于完成路由转发、文件管理、系统管理等工作；
- 配置文件——存放用户对系统配置的参数；
- 日志文件——存放系统日志信息。

说明：

- **filesystem** 命令是用于进入文件系统的命令，在主用主控和备用主控上都可以使用。
-

5.2 文件系统管理功能配置

表 5-1 文件系统管理功能配置列表

配置任务	
存储设备管理	显示存储设备信息
	格式化存储设备
文件目录管理	显示文件目录信息
	显示当前工作路径
	改变当前工作路径
	创建目录
	删除目录
文件操作管理	复制文件
	重命名文件
	显示文件内容
	删除文件
手动执行配置文件	手动执行配置文件
配置启动参数	配置启动参数

5.2.1 存储设备管理

-B -S -E -A

配置条件

在对存储设备操作之前，首先完成以下任务：

- 系统正常启动。

显示存储设备信息

通过显示存储设备的信息，能够详细的看到存储设备的特征信息以及所剩余空间的大小。

表 5-2 显示存储设备信息

步骤	命令	说明
进入文件系统配置模式	filesystem	-
显示存储设备信息	volume	必选

格式化存储设备

当相应存储设备的某些空间不可用时，可以通过格式化命令来格式化相应的存储设备。

表 5-3 格式化存储设备

步骤	命令	说明
进入文件系统配置模式	filesystem	-
格式化存储设备	format { /flash /syslog /usb }	可选

注意：

- 格式化存储设备操作需要谨慎使用，它会导致存储设备上的所有文件永久性丢失，不能恢复。
-

5.2.2 文件目录管理

-B -S -E -A

配置条件

在文件目录操作之前，首先完成以下任务：

- 系统正常启动。

显示文件目录信息

通过显示文件目录信息，能够详细的看到指定目录路径下的文件信息。

表 5-4 显示文件目录信息

步骤	命令	说明
进入文件系统配置模式	filesystem	-
显示目录信息	dir [path]	必选

显示当前工作路径

通过显示当前工作路径，能够详细的看到当前所在的路径信息。

表 5-5 显示当前工作路径

步骤	命令	说明
进入文件系统配置模式	filesystem	-
显示当前工作路径	pwd	必选

改变当前工作路径

通过改变当前工作路径，可以使用户切换到指定的目录下。

表 5-6 改变当前工作路径

步骤	命令	说明
进入文件系统配置模式	filesystem	-
改变当前工作路径	cd path	必选

创建目录

当需要在文件系统中创建一个目录时，可以使用创建目录的操作完成。

表 5-7 创建目录

步骤	命令	说明
进入文件系统配置模式	filesystem	-
创建目录	mkdir directory	必选

删除目录

当通过该操作删除指定目录后，该目录下的子目录以及目录中的所有文件会一并被删除。

表 5-8 删除目录

步骤	命令	说明
进入文件系统配置模式	filesystem	-
删除目录	rmdir directory	必选

说明：

- 删除目录的操作需要谨慎使用，它会导致删除的目录、该目录下的目录以及目录中所

有文件永久性丢失，不能恢复。

5.2.3 文件操作管理 **-B -S -E -A**

配置条件

在对文件操作之前，首先完成以下任务：

- 系统正常启动。

复制文件

在文件系统中，可以通过文件复制的操作将一个文件复制到指定的目录位置。

表 5-9 复制文件

步骤	命令	说明
进入文件系统配置模式	filesystem	-
复制文件	copy <i>src-parameter</i> <i>dest-parameter</i>	必选

说明：

- **copy** 命令可以在文件系统、FTP 服务器、TFTP 服务器间进行文件拷贝，具体操作请参见技术手册 **copy** 命令使用方法。
-

重命名文件

在文件系统中，可以通过重命名文件的操作将该文件的名称重命名为指定的文件名称。

表 5-10 重命名文件

步骤	命令	说明
进入文件系统配置模式	filesystem	-
重命名文件	rename <i>src-filename</i> <i>dest-filename</i>	必选

显示文件内容

在文件系统中，可以通过显示文件内容的操作来查看文件的内容信息。

表 5-11 显示文件内容

步骤	命令	说明
进入文件系统配置模式	filesystem	-
显示文件内容	type <i>path/filename</i>	必选

删除文件

在文件系统中，可以通过删除文件的操作来删除不需要的文件信息。

表 5-12 删除文件

步骤	命令	说明
进入文件系统配置模式	filesystem	-
删除文件	delete <i>path/filename</i>	必选

说明：

- **delete** 命令需要谨慎使用，它会使文件永久性删除，不能恢复。

5.2.4 从 FTP 下载文件

-B -S -E -A

配置条件

在手动执行从 FTP 下载文件之前，首先完成以下任务：

- 系统正常启动；
- 保证 FTP 服务器和设备接口的路由可达，能互相 ping 通。

从 FTP 服务器下载文件

通过从 FTP 下载文件命令，可以将 FTP 服务器上的相关文件从 FTP 服务器下载到文件系统中。

表 5-13 从 FTP 服务器下载文件

步骤	命令	说明
进入文件系统配置模式	filesystem	-
从 FTP 服务器下载文件	{ftpcopy ftpscopy}[vrf vrf-name] host-ip-address username password src-filename { /flash /syslog usb dest-filename }	可选

说明：

- **ftpcopy** 命令、**ftpscopy** 命令可以从 FTP 服务器上下载文件到文件系统，具体操作请参见技术手册 **ftpcopy** 命令、**ftpscopy** 命令使用方法。

5.2.5 配置启动参数 **-B -S -E -A**

配置条件

在配置启动参数之前，首先完成以下任务：

- 系统正常启动。

配置启动参数

配置系统启动参数是指定系统下一次启动使用的应用程序文件。

表 5-14 配置启动参数

步骤	命令	说明
进入文件系统配置模式	filesystem	-
配置启动参数	boot-loader <i>path/filename</i> [<i>bootline-number</i>]	必选

5.2.6 文件系统管理监控与维护 **-B -S -E -A**

表 5-15 文件系统管理监控与维护

命令	说明
clear boot-loader [<i>bootline-number</i>]	清除指定索引的启动参数
show filesystem	显示文件系统信息

命令	说明
show file descriptor	显示系统文件在文件系统中的文件描述符信息
show boot-loader	显示系统启动参数信息

5.3 文件系统管理典型配置举例

5.3.1 配置启动参数 **-B -S -E -A**

网络需求

无

网络拓扑

无

配置步骤

步骤 1: 进入文件系统配置模式。

步骤 2: 配置系统启动项。

#查看系统启动参数。

```
Device#filesystem
Device(config-fs)#show boot-loader
The app to boot at the next time is: yflash0: /yflash/sp9b-g-8.1.0.7(R).pck
The app to boot at the this time is: yflash0: /yflash/sp9b-g-8.1.0.7(R).pck

Boot-loader0: yflash0: /yflash/sp9b-g-8.1.0.7(R).pck

Device(config-fs)#exit
```

#将文件 sp9b-g-8.1.0.7(R).pck 通过 ftp 方式拷贝到 flash 中，再修改 flash 中的 sp9b-g-8.1.0.7(R).pck 文件为系统下次启项，并且优先级设置为 0。

```
Device#filesystem
Device(config-fs)#boot-loader /yflash/sp9b-g-8.1.0.7(R).pck 0
Device(config-fs)#exit
```


#查看配置结果。

```
Device(config-fs)#show boot-loader
The app to boot at the next time is: yflash0: /yflash/sp9b-g-8.1.0.7(R).pck
The app to boot at the this time is: yflash0: /yflash/sp9b-g-8.1.0.7(R).pck

Boot-loader0: yflash0: yflash/sp9b-g-8.1.0.7(R).pck
Boot-loader4: backupramfs0: /backupramfs/sp9b-g-8.1.0.7(R).pck

Device(config-fs)#exit
```

6 配置文件管理

6.1 配置文件管理简介

配置文件管理是用于管理设备配置文件的一项功能。用户可以根据设备提供的命令行接口，十分方便地进行配置文件的管理。如果设备在重启后需要自动加载用户的当前配置，那么在设备重启之前需要将当前配置命令保存到配置文件中。另外用户还可以通过 FTP 或 TFTP 将配置文件上传或下载到其他设备上，快速实现设备的批量配置。其中设备的配置包括以下两种：

启动配置：

当设备启动时，会默认去加载文件名称为 startup 的启动配置文件，并完成对设备的初始化配置工作，这种配置称为启动配置。其中，设备上存在两个启动配置文件，一个是默认的启动配置文件，一个是备份的启动配置文件，设备在启动时，如果默认的启动配置文件不存在，那么系统将会把备份的启动配置文件复制到默认启动配置文件的存放位置，并且加载这个启动配置文件。

当前配置：

当前配置是设备当前生效命令的集合，它包括启动配置和启动之后用户增加或修改的配置内容。由于当前配置信息存放在内存数据库中，如果没有把当前配置保存到启动配置文件中，那么设备重启后会造造成配置信息丢失。

另外设备中配置文件的内容及格式说明如下：

- 配置文件以文本文件的形式存在于文件系统中。
- 配置文件内容是以配置命令的格式存在，并且只保存非缺省配置。
- 配置文件以命令模式为标准，同一命令模式下的命令组织在一起形成一个段落。
- 段落之间的顺序按照一定规则排列：即系统配置模式、接口配置模式、各种协议配置模式。
- 按照命令之间的相互关系分类，相关的命令形成组，组与组之间通过空行分隔。

6.2 配置文件管理功能配置

表 6-1 配置文件管理列表

配置任务	
保存当前配置	保存当前配置
备份设备配置	备份当前配置
	备份启动配置
恢复启动配置	恢复启动配置

6.2.1 保存当前配置

-B -S -E -A

配置条件

无

保存当前配置

如果用户的当前配置需要在设备重启之后继续生效，那么就应该将当前配置保存到启动配置文件中。

表 6-2 保存当前配置

步骤	命令	说明
保存当前配置到启动配置文件中	write	必选

说明：

- 如果在配置文件保存过程中设备出现重启或是断电的等问题，这样可能会造成配置信息丢失。
- 保存当前配置不仅会保存到默认的启动配置文件，同时也会把当前配置保存到备份的启动配置文件中。

6.2.2 备份系统配置

-B -S -E -A

配置条件

在备份系统配置之前，首先完成以下任务：

- 保证设备和服务器之间路由可达。
- 确认需要备份的配置文件是否存在，不存在备份会失败。

备份当前配置

备份当前配置主要是通过命令将当前的配置备份到 FTP 服务器上。

表 6-3 备份当前配置

步骤	命令	说明
进入文件系统模式	filesystem	-

步骤	命令	说明
利用 FTP 协议将当前配置备份到远端主机上	<pre> copy running-config { file-system <i>dest- filename</i> ftp [vrf <i>vrf- name</i>] { <i>hostname</i> <i>ip- address</i> } <i>username</i> <i>password</i> <i>dest-filename</i> startup-config tftp [vrf <i>vrf-name</i>] { <i>hostname</i> <i>ip- address</i> } <i>dest-filename</i> ftps [vrf <i>vrf-name</i>] { <i>hostname</i> <i>ip- address</i> } <i>username</i> <i>password</i> <i>dest-filename</i> VerifyType { none peer } }</pre>	必选

备份启动配置

备份启动配置主要是通过命令将启动配置备份到 FTP 服务器上。

表 6-4 备份启动配置

步骤	命令	说明
进入文件系统模式	enable	-
利用 FTP 协议将启动配置保存到远端主机上	<pre> copy startup-config { file-system <i>dest- filename</i> ftp [vrf <i>vrf- name</i>] { <i>hostname</i> <i>ip- address</i> } <i>username</i></pre>	必选

步骤	命令	说明
	<pre>password dest-filename ftps [vrf vrf-name] { hostname ip- address } username password dest-filename VerifyType { none peer } tftp [vrf vrf- name] { hostname ip- address } dest- filename }</pre>	

6.2.3 恢复启动配置

-B -S -E -A

配置条件

在恢复启动配置之前，首先完成以下任务：

- 保证设备和服务器之间路由可达。
- 确认需要恢复的配置文件是否存在。

恢复启动配置

恢复启动配置主要是通过命令将 FTP 服务器上的启动配置文件下载到设备中，并且设置为重启后的启动配置文件，这样设备在重启之后，就可以加载这个启动配置文件。

表 6-5 恢复启动配置

步骤	命令	说明
进入文件系统模式	filesystem	-
恢复启动配置	copy { file-system src-filename ftp [vrf vrf-name] { hostname ip-	必选

步骤	命令	说明
	<pre> address } username password src-filename ftps [vrf vrf-name] { hostname ip-address } username password src- filename tftp [vrf vrf- name] { hostname ip- address } src-filename } { file-system dest- filename startup-config } </pre>	

说明：

- 在覆盖本地启动配置之前一定要确定这个配置文件是否和设备类型匹配，是否跟当前系统版本匹配。
- 执行完恢复启动配置操作后，当前的配置没有改变，需要等到重启之后，才能执行恢复的启动配置。

6.2.4 配置文件管理监控与维护 **-B -S -E -A**

表 6-6 配置文件管理监控与维护

命令	说明
<pre> show running-config [after- interface before-interface interface [interface-name] [configuration] [[{ begin exclude include } expression] </pre>	查看当前配置信息

命令	说明
<pre> redirect { file <i>file-name</i> ftp [vrf <i>vrf-name</i>] { <i>hostname</i> <i>ip-address</i> } <i>user-name password file-name</i> } } ftps [vrf <i>vrf-name</i>] { <i>hostname</i> <i>ip-address</i> } <i>user-name password file-name</i> } }] </pre>	
<pre> show startup-config [<i>file-number</i> { { begin exclude include [context] } <i>expression</i> redirect { file <i>filename</i> ftp { [vrf <i>vrf-name</i>] { <i>hostname</i> <i>ip-address</i> } <i>user-name</i> <i>password file-name</i> } } ftps { [vrf <i>vrf-name</i>] { <i>hostname</i> <i>ip-address</i> } <i>user-name password file-name</i> } }] </pre>	查看启动配置信息

6.2.5 配置文件加密

-B -S -E -A

配置条件

- 配置文件加密需要插入 USB 设备。

配置配置文件加密

配置文件加密是指使用国密 SM4 算法对配置文件加密，密钥由用户指定，当用户指定密钥后，将会在下一次执行 write 动作时将配置文件加密。

操作记录加密是指使用国密 SM4 算法对配置文件加密，密钥由用户指定，当用户指定密钥后，对之后的操作记录开始加密。

表 6-7 配置文件加密、操作记录加密

步骤	命令	说明
进入全局配置模式	config terminal	-
配置文件加密	service encryption startup algorithms SM4 key password	配置文件加密，用户指定密钥
操作记录加密	service encryption history algorithms SM4 key password	操作记录加密，用户指定密钥

说明：

- 配置文件的加密在配置加密功能后执行的下一次 write 动作时生效。操作记录的加密在配置加密功能后即刻生效。
- 配置加密功能必须插入外部 USB 设备。操作记录加密功能不需要 USB 设备。

7 系统管理

7.1 系统管理简介

通过系统管理，用户可以查看系统当前的工作状态，配置设备基础功能参数，对设备进行基本的维护和管理。系统管理提供的功能主要有：配置设备名称、配置系统时间和时区、配置登录欢迎信息、配置系统异常处理方式、重启设备、配置密码加密服务、配置历史命令保存功能、配置登录安全服务、配置监视 CPU、配置分页显示属性。

7.2 系统管理功能配置

表 7-1 系统管理功能配置列表

配置任务	
配置设备名称	配置设备名称
配置系统时间和时区	配置系统时间和时区
配置登录欢迎信息	配置登录欢迎信息
配置系统异常处理方式	配置系统异常处理方式
配置设备重启	配置设备重启
配置加密服务	配置加密服务
配置历史命令保存功能	配置历史命令保存功能
配置登录安全服务	配置登录安全服务
配置 CPU 监控	配置 CPU 监控
配置分页显示属性	配置分页显示属性

7.2.1 配置设备名称 **-B -S -E -A****配置条件**

无

配置设备名称

设备名称用于标识设备，在使用过程中，用户可以根据自己的需要，随时改变设备的名称，并且这种改动是立即生效的，即新的设备名称将会在下一次系统提示符中出现。

表 7-2 配置设备名称

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置设备名称	hostname <i>host-name</i>	必选

7.2.2 配置系统时间和时区 **-B -S -E -A****配置条件**

无

配置系统时间和时区

系统时间和时区是系统信息时间戳显示的时间。该时间由配置的时间和时区决定的，通过 **show clock** 可以查看系统的时间信息。为了能让设备与其他设备协调工作，需要将系统时间和时区配置准确。

表 7-3 配置系统时间和时区

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
配置系统时区	clock timezone <i>timezone-name-string</i> <i>hour-offset-number</i> [<i>minute</i> <i>offset-number</i>]	必选 缺省情况下, UTC (universal time coordinated) 时区
进入特权用户模式	exit	-
配置系统时间	clock <i>year-number</i> [<i>month-number</i> [<i>day-number</i> [<i>hour-number</i> [<i>minute-number</i> [<i>second-number</i>]]]]]	必选

7.2.3 配置登录欢迎信息 **-B -S -E -A**

配置条件

无

配置登录欢迎信息

登录欢迎信息是用户在登录到设备, 进行登录验证时系统显示的一段信息, 这些欢迎信息可以根据需要, 通过配置登录欢迎信息来实现。

表 7-4 配置登录欢迎信息

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置登录欢迎消息	banner motd <i>banner-line</i>	必选

7.2.4 配置系统异常处理方式

-B -S -E -A

配置条件

无

配置系统异常处理方式

系统异常处理是指当系统出现异常后，系统会通过直接重启的方式进行恢复。配置系统异常处理的方式包括三方面内容：首先是使能周期性异常检测，系统会周期性的检测任务状态、代码段、信号量死锁情况，其检测的周期分别为 10 秒、10 秒、30 秒。其次是配置某种异常等级，该等级及其以上等级出现异常时，设备会重启。异常等级包括以下几种：alert、critical、emergency、error、warn。还可以通过配置健康监测异常处理方式，处理方式包括忽略和重启方式。

表 7-5 配置系统异常处理方式

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置异常处理方式	exception { period-detect enable reboot [level { alert critical emergency error warn }] detect-health { ignore reload } }	必选 缺省情况下 周期性异常检测已开启， 异常出现时设备重启的异常等级为 critical ； 缺省情况下健康监测已经开启，设备健康监测异常后默认为忽略
堆叠模式下配置异常处理方式	exception { period-detect enable reboot { device device-num level device device-num { alert critical	必选 缺省情况下

步骤	命令	说明
	<code> emergency error warn } } detect-health {ignore reload} }</code>	<p>周期性异常检测已开启，</p> <p>异常出现时设备重启的异常等级为 critical；</p> <p>缺省情况下健康监测已经开启，设备健康监测异常后默认为忽略</p>

说明：

- 如果配置了一种异常等级重启，那么这个等级及其以上的异常出现时都会使设备重启。
- 异常等级从高到低为 emergency、alert、critical、error、warn。

7.2.5 配置设备重启

-B -S -E -A

配置条件

无

设备重启

当设备出现故障时，用户可以根据实际的情况，通过重启整机来排除故障。其中，重启设备的方式包括冷重启和热重启两种方式：冷重启是指用户直接对设备断电后再重新上电来实现重启。热重启是指用户通过重启命令对设备重启，该重启过程设备不会断电。

表 7-6 设备重启

步骤	命令	说明
使用命令重启设备或堆叠模式下使用命令重启堆叠域内所有在位虚拟交换成员设备	reload	必选

说明：

- 如果对正在工作的设备进行强制断电重启，可能会造成硬件上的损坏或数据丢失，一般情况下，建议不使用该方式。
- 当使用 reload 命令重启整个设备后，整个设备的所有业务将会被中断，请谨慎使用。

7.2.6 配置历史命令保存功能

-B -S -E -A

配置条件

无

配置历史命令保存功能

历史命令保存功能就是将历史命令保存起来便于查看和收集相关执行过的命令信息。在配置历史命令保存功能前，历史命令是保存在内存文件系统中，配置了这个功能后，系统会自动将历史命令保存到 flash 文件系统中。

表 7-7 配置历史命令保存功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置保存历史命令	shell-history save	必选

步骤	命令	说明
		缺省情况下, 历史命令保存功能开启

7.2.7 配置登录安全服务 **-B -S -E -A**

配置条件

无

开启系统登录安全服务

为了增强系统的安全性, 设备提供了系统登录安全服务功能。主要功能包括:

- 防止暴力破解登录用户密码功能;
- 防止快速连接功能。

防止暴力破解登录用户密码功能主要为了预防存在恶意非法用户对登录设备所用的用户名和密码进行暴力破解。当系统发现有用户连续登录认证失败次数达到系统设定次数后, 系统就会在设定的时间内禁止来自该 IP 地址的登录连接或者来自该用户的登陆请求。

防止快速连接功能主要为了预防非法用户短时间内对设备发起大量的登录请求, 导致占用大量的系统和网络资源。当在规定的时间内如果用户反复连接登录设备的次数达到设定次数后, 系统在设定时间内将禁止来自该 IP 地址的登录连接请求。

表 7-8 配置启动系统登录安全服务

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置启动系统服务登录安全服务	service login-secure { telnet ssh ftp snmp}	必选 缺省情况下, 系统登录安全服务开启

配置系统登录安全服务参数

表 7-9 配置系统登录安全服务参数

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 Telnet 模块禁止违规 IP 地址登录的时间	login-secure telnet ip-addr forbid-time forbid-time-number	必选 缺省情况下为 10 分钟
配置 Telnet 模块禁止违规 IP 地址连续登录认证失败的最大次数	login-secure telnet ip-addr max-try-time max-try-time-number	必选 缺省情况下为 5 次
配置 Telnet 模块禁止违规 IP 地址记录信息的老化时间	login-secure telnet ip-addr record-aging-time record-aging-time-number	必选 缺省情况下为 15 分钟

7.2.8 配置 CPU 监控

-B -S -E -A**配置条件**

无

配置 CPU 监控

CPU 监控是系统针对 CPU 的占用率信息进行监控，这样可以方便了解 CPU 当前运行的状态。CPU 监控的内容如下：

- 监视系统中各个进程的 CPU 占用率，配置后可以通过 **show cpu** 进行相关信息查看开启 CPU 占用率的历史统计功能，配置后可以通过 **show cpu monitor** 进行相关信息的查看。

表 7-10 配置 CPU 监控

步骤	命令	说明
进入特权模式	enable	-
开启各进程 CPU 占用率的监视	spy cpu	必选 缺省情况下，未开启 CPU 占用率的监视功能
开启 CPU 占用率的历史统计功能	monitor cpu	必选 缺省情况下，已开启 CPU 占用率的历史统计功能

7.2.9 配置分页显示属性 **-B -S -E -A**

配置条件

无

配置分页显示的属性

分页显示是指系统的显示信息可以分页进行显示，方便用户查看。用户可以根据需要对设备的显示信息进行分页显示设置。

表 7-11 配置分页显示的属性

步骤	命令	说明
进入特权模式	enable	-
配置分页显示的属性	more { on off discipline [num] }	必选 缺省情况下，分页功能已开启， displine 缺省显示 24 行

7.2.10 操作记录文件管理

-B -S -E -A

配置条件

无

配置操作记录文件

操作记录默认保存在 flash 中，操作记录文件管理主要是更改操作记录的保存位置。

表 7- 13 配置文件加密、操作记录加密

步骤	命令	说明
进入全局配置模式	config terminal	-
操作记录文件管理	shell-history location <i>device-name</i>	用户指定操作记录的保存位置
操作记录文件大小指定	shell-history file max-size <i>num</i>	用户指定操作记录的文件大小

7.2.11 系统管理监控与维护

-B -S -E -A

表 7-12 系统管理监控与维护

命令	说明
show clock	查看系统时钟信息
show cpu	查看 CPU 使用率信息

命令	说明
show device	查看系统设备信息
show environment	查看板卡温度信息
show history { begin <i>expression</i> exclude <i>expression</i> include <i>expression</i> redirect { file <i>file-name</i> ftp [vrf <i>vrf-name</i>] { <i>hostname</i> <i>ip-address</i> } <i>user-name password file-name</i> ftps [vrf <i>vrf-name</i>] { <i>hostname</i> <i>ip-address</i> } <i>user-name password file-name</i> }	查看历史命令信息
show language	查看系统语言版本信息
show login-secure { telnet ssh ftp snmp } { ip-addr user quick-connect }	查看系统登录安全服务信息
show login-secure quick-connect	查看系统登录安全的快速连接信息
show mbuf allocated [<i>pool-name</i>]	查看 mbuf 信息
show memory	查看内存信息
show pool [detail information]	查看系统内存池信息
show process [<i>task-name</i>]	查看系统中主要任务及其运行状态
show semaphore { <i>sem-name</i> all binary counting list mutex } [any pended unpended]	查看系统信号量信息

命令	说明
show spy	查看监视开关状态
show stack	查看系统中各个任务堆栈的使用情况
show system fan [brief]	查看风扇信息
show system lpu [lpu-num brief]	查看 LPU 信息
show system module brief	查看设备所有模块部件摘要信息
show system mpu [brief mpu-num]	查看 MPU 信息
show system power [power-num brief]	查看电源信息
show tech-support { sys-base [detail] drv-base [detail] l2-base [detail] l3-base [detail] all } [page to-memory to-flash]	查看技术支持信息
show version [detail]	查看系统版本信息

7.3 系统管理典型配置举例

7.3.1 配置基于用户、IP 的登陆限制

-B -S -E -A

网络需求

- • PC1、PC2 作为本地终端，可以通过 Telnet、ssh 登录到 Device。
- • Device 可以通过用户和 IP 对 PC1、PC2 进行登录限制。

网络拓扑

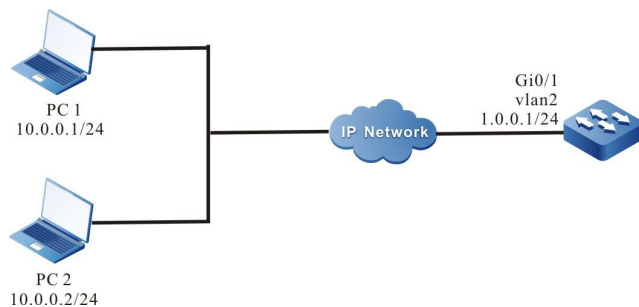


图 7-1 配置基于用户、IP 的登陆限制组网图

配置步骤

步骤 1： 配置各接口的 IP 地址，配置路由协议使 PC1、PC2 和 Device 互通。（略）

步骤 2： 配置基于用户、IP 的登陆限制功能。

#开启 telnet、ssh 登陆安全功能。

```
Device#configure terminal
Device(config)#service login-secure telnet
Device(config)#service login-secure ssh
```

#分别配置 telnet 和 ssh 的 IP 地址的最大重试次数为 5，用户的最大重试次数为 5。

```
Device(config)#login-secure telnet ip-addr max-try-time 5
Device(config)#login-secure telnet user max-try-time 5
Device(config)#login-secure ssh ip-addr max-try-time 5
Device(config)#login-secure ssh user max-try-time 5
```

步骤 3： 开启 Device 的 ssh 服务，配置用户名和密码，并设置使用本地认证登陆

```
Device(config)#ip ssh server
Device(config)#user user1 password 0 admin
Device(config)#line vty 0 15
Device(config-line)#login local
Device(config-line)#exit
```

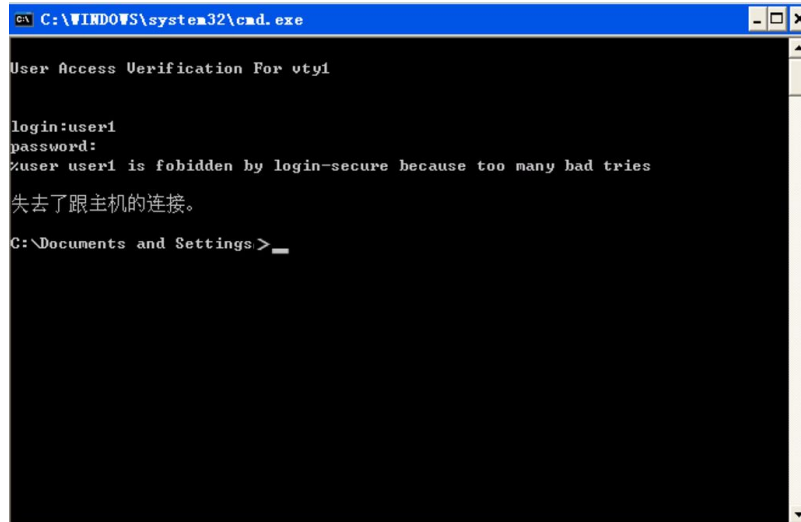
步骤 4： 检验结果。

#PC1 通过 telnet 尝试登陆 Device，用户名 user1，连续输入 6 次错误的密码后，Device 上查看 telnet 登陆安全统计的 user 信息：

```
Device#show login-secure telnet user
telnet module forbidden user information:
user      try-time  forbid-time  wd-id      number  record-time
-----  -
user1     6         00:09:00    0x167f9c20  0       00:01:00
```

可以看到 user1 被认为登陆攻击用户，10 分钟内不允许 user1 通过 telnet 登陆设备。

此时 PC1 再次使用 user1 通过 telnet 登陆 Device，将提示登陆被禁止。



```
C:\WINDOWS\system32\cmd.exe
User Access Verification For vty1

login:user1
password:
user user1 is forbidden by login-secure because too many bad tries
失去了跟主机的连接。
C:\Documents and Settings>
```

#PC2 通过 ssh 尝试登陆 Device，使用 Device 未配置的用户名，连续登陆 6 次后，查看 ssh 登陆安全统计的 ip 信息：

```
Device#show login-secure ssh ip-addr
ssh module forbidden login address:
client address try-time forbid-time wd-id type number record-time
-----
10.0.0.2 6 00:09:00 0x167f9c80 login 0 00:01:00
```

可以看到 PC2 的 IP 地址被认为登陆攻击地址，10 分钟内不允许 PC2 通过 ssh 登陆设备。

此时 PC2 再次通过 ssh 登陆 Device，将提示登陆被禁止。

说明：

- 只有当登陆次数超过所配置的最大重试次数后，才会被认为登陆攻击，并被禁止，登陆次数等于所配置的最大次数不会被禁止。
 - PC 上的部分 ssh 客户端在登陆失败时，会内部重试，此种情况设备依然会记录为多次登陆。
 - 缺省情况下，设备开启 telnet、ssh 的登陆安全功能。
-

7.3.2 配置快速登陆限制 *-B -S -E -A*

网络需求

- • • PC1、PC2 作为本地终端，可以通过 Telnet 登录到 Device。
- • • PC1 反复快速登陆 Device 后登陆被限制，PC2 不受影响。

网络拓扑

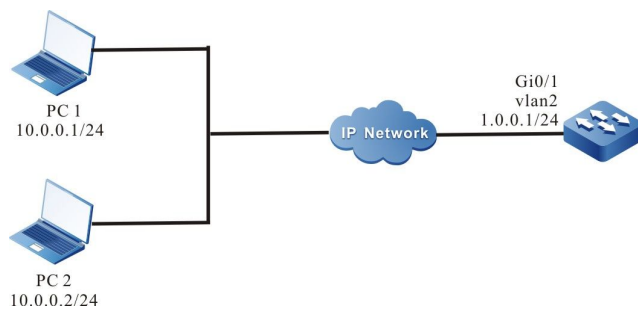


图 7-2 配置快速登录限制组网图

配置步骤

步骤 1： 配置各接口的 IP 地址，配置路由协议使 PC1、PC2 和 Device 互通。（略）

步骤 2： 配置 telnet 的快速登陆限制功能。

#开启 telnet 登陆安全功能，并配置快速登陆最大次数为 20、禁止时间为 10。

```
Device#configure terminal
Device(config)#service login-secure telnet
Device(config)#login-secure telnet quick-connect max-times 20
Device(config)#login-secure telnet quick-connect forbid-time 10
```

步骤 3： 配置 Device 的登陆用户名和密码，并设置使用本地认证登陆。

```
Device(config)#user user1 password 0 admin
Device(config)#line vty 0 15
Device(config-line)#login local
Device(config-line)#exit
```

步骤 4： 检验结果

PC1 通过 telnet，使用 user1 反复登陆退出 21 次，登陆时间间隔不超过 30 秒，查看 telnet 登陆安全统计的快速连接信息：

```
Device#show login-secure telnet quick-connect
```

```
telnet module quick connect info:
connect ip    connect times  last connect time    forbid-time  record-time
-----
10.0.0.1    21          TUE AUG 11 20:22:38 2015  00:09:00    00:01:00
```

可以看到 PC1 被认为登陆攻击地址，10 分钟内不允许 PC1 通过 telnet 登陆设备。

通过 PC2 通过 telnet 可以成功登陆 Device。

8 系统告警

8.1 系统告警简介

系统告警功能是在系统异常时发出的告警提示信息，以便第一时间让用户关注到设备的异常情况，并采取相应的措施来排除异常，让设备继续稳定运行。其中系统告警包含有：温度告警、电源异常告警以及风扇异常告警等功能。其中在系统温度告警中，CPU 或环境温度达到门限值时，会产生异常的系统告警日志信息。缺省情况下的 CPU 温度告警门限值为 110 度，环境告警温度门限值为 80 度。当在电源和风扇异常之后，也会产生异常的系统告警日志信息。

8.2 系统告警功能配置

表 8-1 系统告警功能配置列表

配置任务	
配置系统温度告警	配置系统温度告警
配置系统 CPU 告警	配置系统 CPU 告警

配置任务	
配置系统内存告警	配置系统内存告警
配置系统电源告警	配置系统电源告警
配置系统风扇告警	配置系统风扇告警

8.2.1 配置系统温度告警 **-B -S -E -A**

配置条件

在配置系统告警之前，首先完成以下任务：

- 系统启动稳定后，所有的板卡加载成功。
- 系统启动稳定后，电源和风扇正常工作。

配置系统温度告警

配置系统温度告警是指配置系统交换芯片和主板告警的温度，当交换芯片或主板温度达到一定门限值时，会产生系统告警日志信息。缺省情况下交换芯片告警温度门限值为 115 度，主板告警温度门限值为 115 度。

表 8-2 配置系统温度告警

步骤	命令	说明
进入全局配置模式	config terminal	-
配置交换芯片或主板温度告警门限	alarm temperature mpu { switch mainboard} <i>temperature</i>	必选

步骤	命令	说明
堆叠环境下配置某台在位虚拟交换成员设备交换芯片或主板温度告警门限	alarm temperature device <i>device-num</i> mpu { switch mainboard } <i>temperature</i>	必选

8.2.2 配置系统 CPU 告警

-B -S -E -A

配置条件

在配置系统告警之前，首先完成以下任务：

- 系统启动稳定后，所有的板卡加载成功。

配置系统 CPU 告警

配置系统 CPU 告警是指通过配置 CPU 利用率监测门限后，当超过监测门限后就会发出 CPU 利用率异常的告警功能。

表 8-3 配置系统 CPU 告警

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置系统 CPU 利用率告警门限	cpu utilization warning-threshold [<i>rate-value</i>]	可选

8.2.3 配置内存使用门限低值

-B -S -E -A

配置条件

在配置系统门限告警之前，首先完成以下任务：

- 系统启动稳定后，所有的板卡加载成功。

配置系统内存使用门限低值

配置系统内存使用门限低值是指通过配置系统内存门限低值后，当系统内存低于门限低值之后进入内存短缺状态的功能。

表 8-4 配置系统内存门限告警

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置系统内存门限告警	memory threshold low <i>low-value</i>	可选 缺省情况下，系统内存门限低值为 32M。

8.2.4 配置系统内存告警 **-B -S -E -A**

配置条件

在配置系统告警之前，首先完成以下任务：

- 系统启动稳定后，所有的板卡加载成功。

配置系统内存告警

配置系统内存告警是指通过配置系统内存利用率监测门限后，当超过监测门限后就会发出系统内存利用率异常的告警功能。

表 8-5 配置系统内存告警

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
配置系统内存利用率告警门限	memory utilization warner-threshold [<i>rate-value</i>]	可选 缺省情况下，系统内存利用率告警门限值为 95%。

8.2.5 配置系统电源告警 **-B -S -E -A**

配置条件

无

配置系统电源告警

当电源出现故障或异常时，系统会立即产生系统电源告警日志信息，以便提示让用户关注设备电源的异常情况，并采取相应的措施来排除异常，让设备稳定运行。缺省情况下，系统电源告警功能已开启。

8.2.6 配置系统风扇告警 **-B -S -E -A**

配置条件

无

配置系统风扇告警

当系统风扇出现故障或异常时，系统会立即产生系统风扇告警日志信息，以便提示让用户关注设备风扇的异常情况，并采取相应的措施来排除异常，让设备稳定运行。缺省情况下，系统风扇告警功能已开启。

9 系统日志配置

9.1 日志简介

日志信息共有八类级别，分别是：**emergencies**、**alerts**、**critical**、**errors**、**warnings**、**notifications**、**informational**、**debugging**，其中，0~6 级是日志信息，7 级是调试信息，详见下表所示。

表 9-1 日志级别字段描述

字段	级别	描述
emergencies	0	致命错误，系统不可用，设备停止，需要重启
alerts	1	严重错误，某类功能不可用，业务停止
critical	2	紧急错误，某类功能出现不可逆转问题，少许功能受影响
errors	3	错误信息
warnings	4	警告信息
notifications	5	事件通知信息
informational	6	信息提示及通知信息
debugging	7	调试信息

日志信息分为五个输出方向，包括控制台（Console 终端）、监控台（Telnet 或 SSH 终端）、日志服务器、日志文件（内存日志文件与 flash 日志文件）、email 邮箱，并且五个输出方向都有相应的配置命令对输出进行控制。调试信息主要向控制台与监控台两个输出方向进行输出，也可以配置日志信息输出到日志服务器或日志文件。

表 9-2 日志输出方向

输出方向	描述
控制台	向 Console 终端输出日志信息
监控台	向 Telnet 或 SSH 终端输出日志信息
日志服务器	向日志服务器发送日志信息 缺省情况下，级别在 0~5 级的日志信息将会输出到日志服务器
日志文件	向系统内存或 Flash 存储器输出日志信息 缺省情况下，级别在 0~5 级的日志信息将会输出到系统内存，级别在 0~5 级的日志信息将会输出到 Flash 存储器
email	向 email 邮箱输出日志信息 缺省情况下，级别在 0~4 级的日志信息将会输出到日志邮箱

日志模块运行于独立的 syslog 进程，syslog 进程的主线程接收到系统发送过来的日志信息，首先对日志数据进行处理并分配缓存空间，然后按配置的输出动作分别挂载到各个输出终端对应的缓存队列。由于缓存队列存在长度限制，故大量日志信息输出时，存在日志信息丢失的情况，此时日志模块会对丢失的消息进行统计。日志调度输出共有 2 个线程（日志信息输出到控制台、监控台、日志服务器和日志文件运行于同一个子线程，日志信息输出到 email 运行于另外一个子线程），在调度线程中为每一个输出方向开启了一个定时器，定时器每次响应后，就从终端对应的队列中获取日志信息数据并按用户配置输出到对应的终端。

9.2 日志功能配置

表 9-3 日志功能配置列表

配置任务	
配置日志输出功能	配置日志输出到控制台
	配置日志输出到监控台
	配置日志输出到服务器
	配置日志输出到文件
	配置日志输出到 email 邮箱
配置日志时间戳	配置日志时间戳
配置操作日志发送到日志服务器	配置操作日志发送到日志服务器
配置日志重复抑制功能	配置日志重复抑制
配置日志文件容量	配置日志文件容量
配置日志文件加密功能	配置日志文件加密
配置日志显示颜色	配置日志显示颜色

9.2.1 配置日志输出功能

-B -S -E -A

配置条件

无

配置日志输出到控制台

配置手册

发布 1.1 04/2020

控制台是指 Console 终端，它是用于系统向控制台输出日志信息的一个通道。

表 9-4 配置日志输出到控制台

步骤	命令	说明
进入全局配置模式	configure terminal	-
开启日志输出功能	logging enable	可选 缺省情况下，日志输出功能处于开启状态
开启控制台的日志显示	logging source { <i>module-name</i> default } console { level severity deny }	可选 缺省情况下，已启用控制台的日志显示功能

配置日志输出到监控台

监控台是指 Telnet 或 SSH 终端，它适用于远程设备管理。当配置日志输出到监控台显示时，需要开启当前终端显示日志。

表 9-5 配置日志输出到监控台

步骤	命令	说明
进入全局配置模式	configure terminal	-
开启日志输出功能	logging enable	可选 缺省情况下，日志输出功能处于开启状态
开启监控台的日志显示	logging source { <i>module-name</i> default } monitor { level severity deny }	可选 缺省情况下，全局监控台的日志显示功能处于开启状态

步骤	命令	说明
开启当前监控台显示日志	terminal monitor	必选 缺省情况下，当前监控台未开启日志显示功能

配置日志输出到服务器

为了更全面的记录日志信息，可以配置日志信息输出到日志服务器，以便于系统的维护与管理。当配置日志输出到日志服务器时，需要配置日志服务器的主机地址或者域名。

表 9-6 配置日志发送到日志服务器

步骤	命令	说明
进入全局配置模式	configure terminal	-
开启日志输出功能	logging enable	可选 缺省情况下，日志输出功能处于开启状态
配置日志输出到日志服务器	logging server <i>server-name</i> [vrf <i>vrf-name</i>] { ip <i>ip-address</i> ipv6 <i>ipv6-address</i> / hostname <i>host-name</i> } [port <i>port-num</i>] [facility <i>facility-name</i>] [level <i>severity</i>]	必选 缺省情况下，未配置日志输出到日志服务器
配置日志信息发送的 IP 源地址	logging server source { ip <i>ip-address</i> ipv6 <i>ipv6-address</i>	可选 缺省情况下，将根据路由来确定发送日志信息的出接口，使用

步骤	命令	说明
	interface <i>interface-name</i> }	出接口的主 IP 地址作为发送的日志信息的源 IP 地址
配置指定级别的日志信息输出到日志服务器	logging source { <i>module-name</i> default } server [<i>server-name</i> &<1-8>] { level <i>severity</i> deny }	可选 缺省情况下, 0~5 级别的日志信息可输出到日志主机

配置日志输出到文件

日志文件同时有两种存储方式, 一种方式是储存在内存, 另一种方式是储存在 Flash 存储器。储存在内存中的日志信息仅保留设备从 syslog 启动之后到系统重启或者 syslog 进程重启之前的内容, 在缺省情况下保存的是 5 级 (**notifications**) 及以上级别的日志信息。储存在 Flash 存储器中的日志信息在缺省情况下保存级别为 5 级 (**notifications**) 及以上级别的日志信息, 日志级别请详见表 9-1 中的详细定义。两种形式的日志文件的容量都有一定的容量大小限制, 当日志文件大小达到配置的最大容量时, 新增一条日志时将会先删除最老的一个日志文件 (日志信息由多个日志文件记录), 然后新建一个日志文件并将新增日志信息记录到新建的日志文件中。

表 9-7 配置日志输出到文件

步骤	命令	说明
进入全局配置模式	configure terminal	-
开启日志输出功能	logging enable	可选 缺省情况下, 日志输出功能处于开启状态
配置日志保存到 Flash	logging source { <i>module-name</i>	可选

步骤	命令	说明
	default } file { level severity deny }	缺省情况下，0~5 级别的日志信息保存到 Flash
配置日志保存到内存	logging source { module-name default } buffer { level severity deny }	可选 缺省情况下，0~5 级别的日志信息保存到内存
配置日志文件容量告警	logging { buffer file } warning warning-value recover-value	可选 缺省情况下，日志信息告警水位线为 90%，恢复水位线为 70%
配置日志文件压缩	logging compress [gunzip] logging compress max-num value	可选 缺省情况下，未开启日志压缩功能

配置日志输出到邮箱

为了更全面的记录日志信息，可以配置日志信息通过 email 输出到对应的接收者和抄送者的邮箱中去。

表 9-8 配置日志输出到邮箱

步骤	命令	说明
进入全局配置模式	configure terminal	-
开启日志输出功能	logging enable	可选

步骤	命令	说明
		缺省情况下，日志输出功能处于开启状态
配置 email 模板	logging email <i>email-profile</i>	必选 缺省情况下，未配置日志输出到邮箱的模板
配置接受日志信息接受者的邮箱地址	mail recipient mail-address	必选 缺省情况下，未配置日志信息接收者的邮箱地址
配置接受日志信息抄送者的邮箱地址	mail copyto mail-address	可选 缺省情况下，未配置日志信息抄送者的邮箱地址
配置日志信息发送者的邮箱地址	mail sender <i>mail-address</i>	必选 缺省情况下，未配置日志信息发送者的邮箱地址
配置日志信息发送者的邮箱密码	mail sender password <i>password-string</i>	必选 缺省情况下，未配置日志信息发送者的邮箱密码
配置日志信息接收者的邮箱域名地址	mail server <i>server-name</i>	可选

步骤	命令	说明
		缺省情况下, 以发送者的邮箱地址@符之后的字符作为发送者的域名地址
配置日志信息发送的邮箱主题	mail subject <i>subject-name</i>	可选 缺省情况下, 未配置日志信息发送的邮箱主题
配置指定级别的日志信息通过 email 输出到对应的接收者和抄送者的邮箱中去	logging source { <i>module-name</i> default } email { level <i>severity</i> deny }	可选 缺省情况下, 0~4 级别的日志信息会输出到 email

9.2.2 配置日志时间戳

-B -S -E -A

配置条件

无

配置日志时间戳

日志时间戳可以详细记录日志所生成的时间。缺省情况下, 日志时间戳采用的是绝对时间形式, 但也可以支持 Uptime(相对时间)形式。当配置绝对时间时, 可以指定记录年份及毫秒级精度, 能详细输出日志的时间。

表 9-9 配置日志时间戳

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
配置日志信息时间戳类型	logging timestamps uptime	可选 缺省情况下，日志信息采用绝对戳类型
配置日志信息时间戳格式	logging timestamp-format { msec timezone year }	可选 缺省情况下，日志信息采用带有年份的时间戳格式显示

9.2.3 配置操作日志发送到日志主机 **-B -S -E -A**

配置条件

需要先配置日志输出到主机

配置操作日志发送到日志服务器

当配置了操作日志发送到日志服务器时，就可以在日志服务器上查看用户产生的操作日志。

表 9-10 配置操作日志发送到日志主机

步骤	命令	说明
进入全局配置模式	configure terminal	-
开启日志输出功能	logging enable	可选 缺省情况下，日志输出功能处于开启状态
配置日志主机	logging server <i>server-name</i> [vrf <i>vrf-name</i>] { ip <i>ip-address</i> ipv6 <i>ipv6-</i>	必选

步骤	命令	说明
	<i>address / hostname host-name</i> [port port-num] [facility facility-name] [level severity]	缺省情况下，日志信息发送到日志服务器功能未开启
配置操作日志发送到日志服务器	logging operation to-server	必选 缺省情况下操作日志发送到日志服务器功能未开启

9.2.4 配置日志重复抑制

-B -S -E -A

配置条件

无

配置日志重复信息抑制

由于在某种情况下模块可能会一直不停的输出相同的日志，影响对其他日志的观察，此时可以通过开启日志信息重复抑制功能。重复的日志信息在每次抑制周期之内输出一次，并在抑制周期结束的时候输出抑制周期内此条日志被抑制的次数。

表 9-11 配置日志重复抑制

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置日志重复信息抑制功能	logging suppress duplicates interval interval-num	必选 缺省情况下，日志抑制功能开启

9.2.5 配置日志文件容量

-B -S -E -A**配置条件**

无

配置日志文件容量

由于受 Flash 存储器容量限制，日志文件容量可以配置的范围是 1M ~ 32M，当日志信息存储量超过配置的最大容量限制时，新增的日志将会覆盖掉旧的日志信息（以文件为单位覆盖旧的日志信息文件）。

表 9-12 配置日志文件容量

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置日志文件容量	logging file size <i>file-max-size</i>	可选 缺省情况下，日志文件容量为 1M 字节

9.2.6 配置日志文件加密

-B -S -E -A**配置条件**

无

配置日志文件容量

考虑到日志信息安全，可以对储存在 flash 中的日志文件进行加密。当配置日志文件加密功能后，后续产生的日志会以密文的形式存到日志文件中，如果日志文件的密码发生改变，那么之前以密文存储的日志将无法以明文显示出来，只有重新把密码配置为产生日志时的密码时，日志信息才可以明文的形式显示出来。

表 9-13 配置日志文件加密

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置日志文件加密	logging file encryption algorithms SMV4 key <i>password</i>	可选 缺省情况下，未对 Flash 中的日志文件配置加密功能

9.2.7 配置日志显示颜色

-B -S -E -A

配置条件

无

配置日志显示颜色

当日志信息显示时，可以对不同级别的日志信息通过修改，配置不同的显示颜色以突显信息重要程度。缺省情况下，日志显示颜色的功能是开启的，并且各种日志级别对应的缺省日志显示颜色，请参见下表：

表 9-14 日志颜色描述

字段	描述
emergencies	红色(red)
alerts	紫色(purple)
alerts	蓝色(blue)
errors	棕色(brown)
warnings	青色(cyan)
notifications	白色(white)

字段	描述
informational	绿色(green)
debugging	绿色(green)

表 9-15 配置日志显示颜色

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置对应日志级别下的日志显示颜色	logging color [<i>logging-level logging-color</i>]	可选 缺省情况下, 各种日志级别具有缺省日志显示颜色

说明:

- 当控制台或监控台需要输出日志信息的颜色时, 需要配置显示终端的颜色选项, 否则, 日志信息的颜色不能显示出来。

9.2.8 日志监控与维护

-B -S -E -A

表 9-16 日志监控与维护

命令	说明
clear logging [buffer file]	清除储存在内存或者是 Flash 中的日志信息
show logging [buffer file]	显示储存在内存或者是 Flash 中的日志信息
show logging { file buffer } desc	逆向显示储存在内存或者是 Flash 中的日志信息

命令	说明
show logging operation	显示存储在操作日志文件中的日志信息
show logging [{ file buffer } [begin-level <i>level-value</i> / [start-time <i>stime</i> [end-time <i>etime</i>]] [detail]]]	显示存储在日志文件中的日志信息，可带时间以及级别过滤选项过滤显示日志信息
show logging { file buffer } message-counter	显示本设备储在 Flash 存储器或者内存中的日志文件大小以及日志信息条目数

10 软件升级

10.1 软件升级简介

软件升级，可以为用户提供更加稳定的软件版本和更多的软件特性。

软件升级成功后的程序以文件或者数据块形式存储在设备各个存储介质中，各种对应功能的软件模块相互配合，使设备整体保持稳定工作的状态，从而支持设备的硬件特性和用户的应用业务。

用户可以通过 TFTP/FTP 网络传输方式，或者通过 Console 口 Xmodem 传输方式升级软件。升级不同类型的软件时，用户必须认真阅读软件升级相关手册的操作步骤、说明和注意事项，以保证设备正常运行。

软件升级时，通常需要对各个类型的软件都升级，如果升级过程中某类型软件版本未更新，可以不用重复升级该软件。通常将所有对应版本升级完毕后才能重启设备。

软件有如下几种类型：

- image 程序包：后缀名为 pck 的程序包，包含了系统正常运行的程序集合（操作系统和应用程序等）；
- bootloader 程序：后缀名为 pck 的程序，类似于 PC 机的 BIOS 程序，固化在主板 ROM 中，在系统上电时最先执行。这段程序对基本系统进行初始化，并实现如升级、下载、引导、调试及测试等功能，主控板和交换板卡可以升级 bootloader 程序。
- Package 打包程序：包含 image, bootloader, 程序的打包文件，可一次性升级多种类型软件程序，方便省时。

10.2 软件升级功能配置

表 10-1 软件升级功能配置列表

配置任务	
image 程序包升级	通过 TFTP/FTP 方式升级 image 程序包
bootloader 程序升级	通过 TFTP/FTP 方式升级 bootloader 程序
	通过 Console 口升级 bootloader 程序
Package 打包程序升级	通过 TFTP/FTP 方式升级 package 打包程序

10.2.1 image 程序包升级 **-B -S -E -A**

配置条件

在进行 image 程序包升级之前，需完成以下任务：

- 保证 TFTP/FTP 服务器和设备接口的路由可达，能互相 ping 通；
- TFTP/FTP 服务器配置正确，且 image 程序正确的存放在 TFTP/FTP 指定目录下；
- 保证对应存储路径剩余空间足够，如果空间不足，可以手动删除对应存储路径上不需要的文件；
- 备份配置文件。

通过 TFTP/FTP 方式升级 image 程序包

进入特权用户模式，保证设备可以从外部 TFTP/FTP 服务器获取升级程序，然后通过 sysupdate image 命令升级。

表 10-2 通过 TFTP/FTP 方式升级 image 程序包

步骤	命令	说明
进入特权用户模式	无	必选
升级 image 程序包	sysupdate image [device {memberId all}] mpu [vrf vrf-name] dest-ip-address filename [ftp ftp-username ftp-password] [reload]	必选 如果未指定 FTP 选项，缺省使用 TFTP 升级

举例说明：堆叠模式下，通过 FTP 服务器 130.255.168.45，从设备接口升级镜像文件名为 sp35-g-9.4.0.12(R).pck 的 image 程序包。

```

Hostname# sysupdate image device all mpu 130.255.168.45 sp35-g-9.4.0.12(R).pck ftp a 123456
#设备会提示如下信息：

Hostname #sysupdate image device all mpu 130.255.168.45 sp9b-g-6.6.6.1.2(R).pck ftp a 123456
checking "sp35-g-9.4.0.12(R).pck" : ... OK
downloading "sp35-g-9.4.0.12(R).pck" : #####OK
Download "sp35-g-9.4.0.12(R).pck" (40175300 Bytes) successfully

Sysupdate start to write image sp35-g-9.4.0.12(R).pck:
Verify the image...valid!
Writing file /flash/ sp35-g-9.4.0.12(R).pck .....OK!
write ios to backup file-system.....OK!

%Sysupdate image is in process, please wait...
%Sysupdate image finished...

sysupdate image result information list:
    
```

```
-----  
Card          result information  
-----  
Device 0 - Mpu  sysupdate successfully!  
  
Hostname #
```

#以上信息说明设备的 image 程序升级成功，升级完成后会输出升级结果的报表及日志信息。

说明：

- 如果加上命令选项 reload，则会提示是否需要保存配置、是否立即重启设备。一般情况下需要升级完各种程序后才重启设备，所以 reload 选项一般不建议使用。
- 升级前应保证对应存储路径有足够的剩余空间，否则升级失败。此时用户可以通过手动删除对应存储路径上不需要的文件，释放空间后重新升级应用程序。
- 升级 image 程序包需要较长的时间，如果对应存储路径剩余空间越小升级时间越长。
- 升级完成后，如果需要运行新 image 程序，则需要重启设备。
- 如果设备无法正常启动，可以进入 bootloader 界面，修改启动方式为网络启动，启动成功后再升级。具体方法请参考“bootloader”配置手册、技术手册相关章节。

警告：

- 升级过程中保证设备不能断电，并且禁止做重启以及拔插板卡操作；否则可能导致系统或者板卡无法启动，可能会对板卡的对应存储路径文件系统造成损坏。
-

10.2.2 bootloader 程序升级

-B -S -E -A

配置条件

在进行 monitor 程序升级之前，需完成以下任务：

- 保证 TFTP/FTP 服务器和设备接口的路由可达，能互相 ping 通；
- TFTP/FTP 服务器配置正确，且 bootloader 程序正确的存放在 TFTP/FTP 指定目录下；

- 备份配置文件。

通过 TFTP/FTP 方式升级 bootloader 程序

进入特权用户模式，保证设备可以从外部 TFTP/FTP 服务器获取升级程序，然后通过 `sysupdate bootloader` 命令升级。

表 10-3 通过 TFTP/FTP 方式升级 bootloader 程序

步骤	命令	说明
进入特权用户模式	无	必选
升级 monitor 程序	sysupdate bootloader [device {memberId all}] mpu [vrf vrf- name] dest-ip-address filename [ftp ftp- username ftp- password] [reload]	必选 如果未指定 FTP 选项，缺省使用 TFTP 升级

举例说明：堆叠模式下，通过 FTP 服务器 130.255.168.45，升级文件名为 `sz03-tboots1-rtk93-1.0.0.10.pck` 的 bootloader 程序。

```

Hostname# sysupdate bootloader device all mpu 128.255.21.170 sz03-tboots1-rtk93-1.0.0.10.pck ftp a 123456
#设备会提示以下信息：
checking "sz03-tboots1-rtk93-1.0.0.10.pck" : ...OK
downloading "sz03-tboots1-rtk93-1.0.0.10.pck" : ##OK
Download "sz03-tboots1-rtk93-1.0.0.10.pck" (1849684 Bytes) successfully

Sysupdate start to write bootloader sz03-tboots1-rtk93-1.0.0.10.pck:
Update bootloader start.....OK.
Bootloader write successfully.
%Sysupdate bootloader is in process, please wait...
%Sysupdate bootloader finished...

sysupdate bootloader result information list:
-----
Card          result information
-----
Device 0 - Mpu  sysupdate successfully!
    
```

#以上信息说明设备的 bootloader 程序升级成功，升级完成后会输出升级结果的报表及日志信息。

说明：

- 如果加上命令选项 reload，则会提示是否需要保存配置、是否立即重启设备。一般情况下需要升级完各种程序后才重启设备，所以 reload 选项一般不建议使用。
 - 升级完成后，如果需要运行新 bootloader 程序，则需要重启设备。
 - 请选择正确的 bootloader 版本进行升级，避免出现异常情况。
-

说明：

- 升级过程中保证设备不能断电，并且禁止做重启操作；否则可能导致系统无法启动，可能会对设备的 bootloader 文件造成损坏。
-

通过 Console 口升级 bootloader 程序

保证超级终端能通过 Console 口访问设备，进入 bootloader 模式，调整波特率，通过超级终端的 ymodem 升级。

具体命令的详细说明，请参照“bootloader”命令手册相关章节。

表 10-4 通过 Console 口升级 bootloader 程序

步骤	命令	说明
设置超级终端	无	必选 运行超级终端程序，并选择相应的串口(如 com1)，设置其属性：波特率为 9600 bps，软流控，数据

步骤	命令	说明
		位是 8 位, 无奇偶校验, 1 位停止位
进入 bootloader 模式	无	必选 设备重启时, 按下 CTRL+C, 进入 bootloader 模式
修改 Console 口和超级终端的波特率, 加快升级速度	srate { <i>speed</i> }	可选 修改设备 Console 口波特率为 115200bps, 然后超级终端断开连接, 修改超级终端的波特率为 115200bps, 重新连接
升级 bootloader 程序	mupdate bootloader	必选 在 bootloader 模式下输入 mupdate bootloader 命令, 然后选择超级终端的 y modem 协议, 选定 bootloader 程序后开始发送

举例说明: 通过 Console 口升级主用主控卡的 bootloader 程序。

```
#设备会提示如下信息:
RTL9310# # mupdate bootloader
Download bootloader start...
## Ready for binary (ymodem) download to 0x80000000 at 9600 bps...
CCC
Starting ymodem transfer. Press Ctrl+C to cancel.
Transferring sz03-tboots1-rtk9310-1.0.0.10.bin...
100% 904 KB 872 bytes/sec 00:17:41 0 Errors

## Total Size = 0x000e2130 = 926000 Bytes
Download bootloader OK.
Loader Chip: 93100000
Loader CRC: 98ba8309
Loader Size: e2058
```

```
Loader Tail CRC: 85eed660
Program flash start...
1048576 bytes written, 0 bytes skipped
Program flash OK.
Update bootloader OK.
RTL9310# #
```

#以上信息说明设备的 bootloader 程序升级成功。

说明：

- 升级 bootloader 程序时保证超级终端的速率和设备 Console 口速率一致。
 - 升级 bootloader 程序时建议设置传输速率值为 115200bps，这样升级传输时间更短。
 - 升级 bootloader 程序时，如果修改了 Console 口的缺省速率，加载 image 程序包时，设备的 Console 口速率自动恢复到 9600bps，此时超级终端的速率需要同步修改。
 - 建议尽量通过 TFTP/FTP 方式升级 bootloader，当第一种升级方式条件不满足的时候，才使用 Console 口升级 bootloader 程序。
-

警告：

- 升级过程中保证设备不能断电，否则可能导致系统无法启动，可能会对设备的 bootloader 文件造成损坏。
-

10.2.3 打包文件升级

-B -S -E -A

打包文件中包含 image,bootloader 文件，通过打包文件可以一次性升级这些文件。

配置准备

在进行打包文件升级之前，需完成以下任务：

- 保证 TFTP/FTP 服务器和设备接口的路由可达，能互相 ping 通。
- TFTP/FTP 服务器配置正确，且打包文件正确的存放在 TFTP/FTP 指定目录下。
- 备份配置文件。

通过 TFTP/FTP 方式升级打包文件

进入特权用户模式，保证设备可以从外部 TFTP/FTP 服务器获取升级程序，然后通过 `sysupdate package` 命令升级。

表 10-5 通过 TFTP/FTP 方式升级打包文件

步骤	命令	说明
进入特权用户模式	无	必选
升级 package 打包文件	sysupdate package [<i>vrf vrf-name</i>] <i>dest-ip-address filename</i> [ftp <i>ftp-username ftp-password</i>][no-comparision][reload]	必选 如果未指定 FTP 选项，缺省使用 TFTP 升级

#通过 FTP 服务器 130.255.168.45，升级设备 sp35-g-9.4.0.17(R)-001.pkg 文件。

```
Hostname# sysupdate package 130.255.168.45 sp35-g-9.4.0.17(R)-001.pkg FTP a a
```

说明：

- 如果加上命令选项 `reload`，则会提示是否需要保存配置、是否立即重启设备。一般情况下需要升级完各种程序后才重启设备，所以 `reload` 选项一般不建议使用。

警告：

- 升级过程中保证设备不能断电，否则可能导致系统无法正确启动，可能会对文件造成损坏。

10.3 软件升级典型配置举例

10.3.1 升级软件版本

-B -S -E -A

网络需求

- PC 作为 FTP 服务器，设备 Device 作为 FTP 客户端；服务器和设备网络连通。
- FTP 服务器上设置设备登录 FTP 服务器的用户名为 admin，密码为 admin；将需要升级的打包升级程序放在 FTP 服务器目录下，全面升级设备支持打包升级的所有软件版本。

网络拓扑



图 10-1 打包升级所有支持的软件版本组网图

配置步骤

- 步骤 1：配置 FTP 服务器，并将打包升级程序放到 FTP 服务器的目录下。（略）
- 步骤 2：备份设备配置文件。（略）
- 步骤 3：配置接口的 IP 地址，使设备与 FTP 服务器网络连通。（略）
- 步骤 4：升级打包升级程序。

#使用 sysupdate 升级打包升级程序。

```
Device#sysupdate package device all 128.255.21.170 sp35-g-9.4.0.12(R)-001.pkg ftp a 123456 no-comparision
```

在升级结束之后，会打印升级结果列表，供用户判断打包升级文件中包含的所有升级程序在设备上的升级结果：

```
package sysupdate result information list:
-----
sysupdate sp35-g-9.4.0.12(R).pck result information list:
-----
```

```
Card          result information
-----
Device 0 - Mpu device is not online,skipped!
Device 1 - Mpu device is not online,skipped!
Device 2 - Mpu device is not online,skipped!
Device 3 - Mpu device is not online,skipped!
Device 4 - Mpu sysupdate successfully!
Device 5 - Mpu device is not online,skipped!
Device 6 - Mpu device is not online,skipped!
Device 7 - Mpu device is not online,skipped!

sysupdate sz03-tboots2-rtk93-1.0.0.10,pck result information list:
-----
Card          result information
-----
Device 0 - Mpu device is not online,skipped!
Device 1 - Mpu device is not online,skipped!
Device 2 - Mpu device is not online,skipped!
Device 3 - Mpu device is not online,skipped!
Device 4 - Mpu sysupdate successfully!
Device 5 - Mpu device is not online,skipped!
Device 6 - Mpu device is not online,skipped!
Device 7 - Mpu device is not online,skipped!
```

说明:

- 打包升级前请确保所有板卡在位且状态为 Start OK。升级过程中请勿进行板卡拔插操作，避免板卡升级异常影响板卡后续启动。
-

说明:

- 此处选择 “no-comparision” 参数则不进行 image 的版本比较而直接升级打包升级程序中的版本。如果不选择该参数则会进行 image 的版本比较，如果打包升级程序中的 image 版本低于设备运行版本或者和设备运行版本相同则设备会提示用户，并等待用户确认是否要升级包中的该 image 升级程序。无论用户选择升级该程序与否，都不会影响升级包中其他升级文件的升级。如果打包升级包中只有该 image 文件，如果用户选择不升级，则打包升级结束。
 - 该命令还可以添加 “reload” 参数，添加该参数则升级完成之后直接重启设备。
-

步骤 5: 命令重启设备

#使用 reload 命令重启设备。

```
Device #reload
Save current configuration to startup-config(Yes|No)?y
```

Please confirm system to reload(Yes|No)?y

在重启前是否要保存配置由用户根据实际需要决定。

说明:

- 如果升级命令中包含了 “reload” 参数, 则此步骤省略。
-

步骤:6: 检验结果。

#升级完成并重启设备后, 通过 show package version 查看打包升级程序中升级的文件版本信息。

```
Device #show package version
package      :sp35-g-9.4.0.12(R)-001.pkg
image       :sp35-g-9.4.0.12(R).pck
bootloader  :sz03-tboots2-rtk93-1.0.0.10.pck
```

#通过 show system verison brief 查看各个程序的版本号来检查是否更新。

```
Device #show system version brief
Device 4:
Module      Online State  Name                BootLoader IOS          CMM PCB CPLD FPGA
-----
```

说明:

- 通过 show package version 查看打包升级程序中升级文件的版本, 对应 show system verison brief 查看最终升级结果。
-

10.3.2 全面升级所有软件版本

-B -S -E -A

网络需求

- PC 作为 FTP 服务器, 设备 Device 作为 FTP 客户端, 服务器和客户端网络连通。
- FTP 服务器上设置设备登录 FTP 服务器的用户名为 admin, 密码为 admin; 将需要升级的 image 程序、bootloader 程序放在 FTP 服务器目录下。

网络拓扑



图 10-2 全面升级所有软件版本组网图

配置步骤

步骤 1： 配置 FTP 服务器，并将 image 程序、bootloader 程序放到 FTP 服务器的目录下。

(略)

步骤 2： 备份设备配置文件。(略)

步骤 3： 创建 VLAN，并将端口加入对应的 VLAN。(略)

步骤 4： 配置接口的 IP 地址，使 Device 与 FTP 服务器网络连通。(略)

步骤 5： 升级 image 程序。

#升级 image 程序之前查看文件系统中是否有足够的剩余空间。

```
Device#filesystem
Device(config-fs)#volume
Device(config-fs)#exit
```

#使用 sysupdate 升级设备的 image 程序。

```
Device# sysupdate image mpu all 130.255.98.2 sp9b-g-6.6.6.1.2(R).pck ftp admin admin
```

image 程序的升级过程和升级是否成功的打印信息，可参考“软件升级功能配置”中“image 程序包升级”的相关内容。

步骤 6： 升级 bootloader 程序。

#使用 sysupdate 升级设备所有板卡的 bootloader 程序。

```
Device#sysupdate bootloader all 2.0.0.1 sz03-tboots1-rtk93-1.0.0.10.pck ftp admin admin
```

bootloader 程序的升级过程和升级是否成功的打印信息，可参考“软件升级功能配置”中“bootloader 升级”的相关内容。

步骤 7： 命令重启设备。

#使用 reload 命令重启设备。

```
Device#reload
Save current configuration to startup-config(Yes|No)?yes
Building Configuration...done
Write to mode file... OK
Write to startup file ... OK
Please confirm system to reload(Yes|No)?yes
```

在重启前是否要保存配置由用户根据实际需要决定。

步骤 8: 检验结果。

#升级完成并重启设备后，通过查看各种程序的版本号来检验版本是否更新。

#检验设备的 image、bootloader 程序升级是否成功。

```
Hostname#show system mpu
System Card Information(Mpu 0 - ONLINE)
-----
      Type: MTS2848-6X-E
      Status: Start Ok
      Last-Alarm: Normal
      Card-Port-Num: 54
      Card-SubSlot-Num: 0
      Power-INTF-Status: Normal
      Power-Card-Status: On
      Serial No.: ser_dev_mpu1/0
      Card-Name: MTS2848-6X-E
      Description: jkjkjk
Hardware-Information:
      PCB-Version: 001
Software-Information:
      Bootloader-Version:
      Software-Version: 9.4.0.11(integrity)
Temperature-Information:
      Temperature-State:
          Switch-Temperature = 73 C
          Last-Alarm = Normal.
          Mainboard-Temperature = 43 C
          Last-Alarm = Normal.
CPU-On-Card-Information: < 1 CPUs>
      CPU-Idx: 00
      Status: Normal
      Core-Num: 0001
      Core-State:
      Core-Idx-00
          Core-Status: 0000
          Core-Utilization: 9%
MEM-On-Card-Information: <1 MEMs>
      MEM-Idx: 00
      MEM-State:
          BytesFree = 638988288 bytes
          BytesAlloc = 321507328 bytes
          BlocksFree = 4 blocks
          BlocksAlloc = 10652 blocks
          MaxBlockSizeFree = 31457280 bytes
          SizeTotal = 960495616 bytes
DISK-On-Card-Information: <1 DISKs>
      DISK-Idx: 00
      Type: Flash
      Status: Online
      DISK-State:
```


SizeTotal = 162299904 bytes
SizeFree = 95928320 bytes

STATISTICS: 1 IN, 0 OUT, 0 IERR, 0 OERR

说明:

- 上述升级 image、bootloader 程序的顺序，并没有严格的要求，但切记，需要升级完所有程序后才重启整机。

在升级之前应保证设备的对应存储路径文件系统中有足够的剩余空间用于保存升级的 image 文件。如果设备的空间不足，可以删除设备文件系统中不需要的文件；建议升级前保证设备的对应存储路径剩余空间大于 24M。

10.3.3 使用 Console 口升级 bootloader

-B -S -E -A

网络需求

- PC 与设备 Console 口直接连接。
- 使用 Console 口升级设备的 bootloader 程序。

网络拓扑

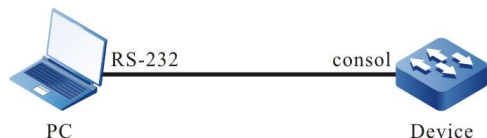


图 10-3 使用 Console 口升级 bootloader

配置步骤

步骤 1: PC 与设备的 Console 口正确连接。(略)

步骤 2: 进入 bootloader 界面。

在设备刚启动打印 “Press ctrl+c to enter bootloader mode: 0 ” 的时候长按 “ctrl+c” 进入 bootloader 界面。

步骤 3: 设置传输速率为 115200bps, 加快升级速度。

```
RTL9310# # srate 115200
```

#设置完 bootloader 下 Console 口的传输速率后, 应将超级终端的传输速率同样设置为 115200bps。

步骤 4: 在 bootloader 界面下升级 bootloader 版本。

```
RTL9310# # mupdate bootloader
```

#输入 “mupdate bootloader” 命令, 使用 ymodem 传输保存在 PC 上的 bootloader 文件。

#检验结果

#升级完成后在 bootloader 界面下会打印下面的信息。

```
Program flash OK.  
Update bootloader OK.
```

步骤 5: 检验结果。

#升级完成后重启设备, 会打印系统由新的 bootloader 引导加载。

```
1.0.0.4 compiled at May 01 2019 - 01:32:36  
warm boot from master sector  
Press ctrl+c to enter bootloader mode: 0
```

说明:

- 由于用 Console 升级 bootloader 程序较复杂且较慢, 所以通常情况建议使用 TFTP/FTP 方式升级 bootloader 程序, 当第一种升级方式条件不满足的时候, 才使用 Console 口升级 bootloader 程序。
 - 升级完成后用 “reset” 命令退出 bootloader, 由新的 bootloader 程序引导 image 程序加载。
 - 升级 bootloader 程序时, 如果修改了 Console 口的缺省波特率, 加载 image 程序包时, 设备的 Console 口速率自动恢复到 9600bps, 此时超级终端的速率需要同步修改。
-

11 Bootloader

11.1 bootloader 简介

在嵌入式系统中，bootloader 在操作系统内核运行之前运行，用于初始化硬件设备（包括 Console 口、以太接口、flash 等）、建立内存空间映射，从而将系统的软硬件环境带到一个合适状态，以便为最终引导操作系统内核准备好正确的环境。在嵌入式系统中，通常并没有像 BIOS 那样的固件程序，整个系统的加载启动任务就由 bootloader 来完成。

bootloader 系统主要包含如下功能：

- 设置启动参数通过网络或者内部 flash 存储设备加载 IOS
- 升级 bootloader 程序。
- 备份 bootloader 程序

11.2 bootloader 功能配置

表 11-1 bootloader 功能配置列表

配置任务	
进入 bootloader 配置模式	启动时进入 bootloader 配置模式
设置 bootloader 启动参数	设置 bootloader 启动参数从 flash 裸区启动 image 程序

配置任务	
配置 bootloader 管理以太口 IP 地址	配置 bootloader 管理以太口 IP 地址。
通过网络启动 image 程序	通过网络启动 image 程序。
升级 bootloader 程序	升级 bootloader 程序

11.2.1 bootloader 功能配置前准备

-B -S -E -A

在进行 bootloader 配置前，需要建立本地配置环境。需将主机（或终端）的串口通过配置线缆与设备的 Console 口连接，要求主机（或终端）的通信参数配置和设备 Console 口的缺省配置保持一致。设备端 Console 口的缺省配置为：

- 传输速率：9600bps
- 流控方式：无
- 校验方式：无
- 停止位：1bit
- 数据位：8bit

11.2.2 进入 bootloader 配置模式

-B -S -E -A

配置条件

无

进入 bootloader 配置模式

表 11-2 进入 bootloader 配置模式

步骤	命令	说明
进入 bootloader 配置模式	无	必选 设备上电后，按住按键“ctrl+c”即可进入 bootloader 配置模式；进入后提示信息为：“RTL93xx#”

说明：

- 进入 bootloader 配置模式后，可以执行 bootloader 模式提供的功能。

11.2.3 设置 bootloader 启动参数

-B -S -E -A

配置条件

无

设置 bootloader 的启动参数

表 11-3 设置 bootloader 的启动参数

步骤	命令	说明
进入 bootloader 配置模式	无	必选 设备上电后，按住按键“ctrl+c”即可进入

步骤	命令	说明
		bootloader 配置模式；进入后提示信息为：“RTL93xx#”
设置 bootloader 下 IOS 的启动参数	<pre> change index[0~3] ge0 filename local-ip- addr host-ip-addr [gatewayip] [netmask] change index[0~3] flash0 filename </pre>	必选 第一行命令为网络启动配置参数，如果跨网段升级，则需要添加网关和掩码 第二行命令为 flash 存储设备启动配置参数

说明：

- 国产交换机的 bootloader 程序目前可设置启动参数持通过网络启动 image 程序。

11.2.4 升级 bootloader 程序

-B -S -E -A

配置条件

无

升级 bootloader 程序

表 11-4 升级 bootloader 程序

步骤	命令	说明
进入 bootloader 配置模式	无	必选 设备上电后，按住按键“ctrl+c”即可进入 bootloader 配置模式； 进入后提示信息为：“RTL93xx#”
在 PC 机上启动 tftp 服务器		必选 将用于升级的新 bootloader 版本拷贝到 tftp 的 root 目录，用于设备通过 tftp 下载版本文件。
升级 bootloader 程序	update bootloader filename ge0 local-ip-addr host-ip-addr [gatewayip] [netmask]	必选 通过 tftp 服务器升级 bootloader 的 PCK 文件
备份 bootloader 程序	bootloaderbak	可选

说明：

- bootloader 系统程序采取了双 bootloader 备份的方式，即分为主 bootloader 程序与备份 bootloader 程序，使用升级命令只能对主 bootloader 进行版本升级，而备份 bootloader 程序将保持不变。

- 升级 bootloader 系统程序后，使用命令 **reset** 或断电重启设备，即可使用最新的 bootloader 系统程序。
- 当系统加载成功后，可以通过 **sysupdate** 命令升级

11.2.5 bootloader 监控与维护

-B -S -E -A

表 11-5 bootloader 监控与维护

命令	说明
version	显示 bootloader 程序版本号
print index[0~4]	显示 index 所指定的启动参数信息

11.3 bootloader 典型配置举例

11.3.1 配置 bootloader 通过网络启动 Image 程序

-B -S -E -A

网络需求

- PC 作为 TFTP 服务器，设备 Device 作为 TFTP 客户端；服务器和设备网络连通。
- TFTP 服务器上需将需要升级的 image 程序、bootloader 程序放在 TFTP 服务器目录下。

网络拓扑

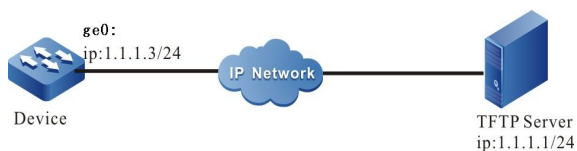


图 11-1 配置 bootloader 通过网络启动 image 程序

配置步骤

步骤 1: 配置 TFTP 服务器, 并将 image 程序程序放到 TFTP 服务器的目录下。(略)

步骤 2: 设备上电后, 按住按键 “ctrl+c” 进入 bootloader 配置模式。

步骤 3: 配置启动行参数, 从网络启动 Image 程序

```
RTL93xx# change 0 ge0 sp35-g-9.4.0.12(R).pck 1.1.1.3 1.1.1.1
```

```
RTL93xx# boot
```

说明:

- 将设备的第一个端口与 tftp 服务器连接。
 - 在设置完以上启动信息后, 执行 run 之前设备能与 ftp 服务器正常通信。
-

12 PoE 管理

12.1 PoE 简介

PoE (Power Over Ethernet, 以太网供电) 指的是在现有的以太网 Cat.5 布线基础架构不做任何改动的情况下, 在为一些基于 IP 的终端 (如 IP 电话机、无线局域网接入点、网络摄像机等) 传输数据信号的同时, 还能为此类设备提供直流供电的技术。PoE 技术能在确保现有结构化布线安全的同时保证现有网络的正常运作, 最大限度地降低成本。

PoE 也被称为基于局域网的供电系统(PoL, Power Over LAN)或有源以太网(Active Ethernet), 有时也被简称为以太网供电, 这是利用现存标准以太网传输电缆的同时传送数据和电功率的最新标准规范, 并保持了与现存以太网系统和用户的兼容性。IEEE 802.3af 和 IEEE802.3at 标准是所有 PoE 设计需要遵循的技术标准, IEEE802.3af 是 PoE 技术的基础性标准, 它在 IEEE 802.3 的基础上增加了通过网线直接供电的相关标准, 是现有以太网标准的扩展。而 IEEE802.3at 标准是在 IEEE802.3af 基础上的扩展。

按照 IEEE802.3af 标准的定义, 一个完整的 PoE 供电系统包含 PSE 和 PD 两种类型的设备:

- PSE (Power Sourcing Equipment, 供电设备): 主要是用来给其他设备进行供电的设备。
- PD (Power Device, 受电设备): 接受供电的设备, 这些设备一般功率都不大。

12.1.1 PSE/PD 接口标准 **-S -E -A**

IEEE802.3af 标准针对 10BASE-T 与 100BASE-TX 网络还定义了 PI (Power Interface, PSE/PD 与网线的接口), 目前已经定义了 Alternative A (1、2、3、6 信号线对) 和 Alternative B (4、5、7、8 空闲线对) 两种供电模式, 其说明如下:

1、通过信号线对供电 (Alternative A)

如下图所示, PSE 可通过信号线对给 PD 供电。由于 DC 和数据频率互不干扰, 所以可以在同一线对同时传输电流和数据。其实, 对电缆来说可以看作是一种“复用”。可以把 1、2 链接形成正 (或负) 极, 把 3、6 链接形成负 (或正) 极。

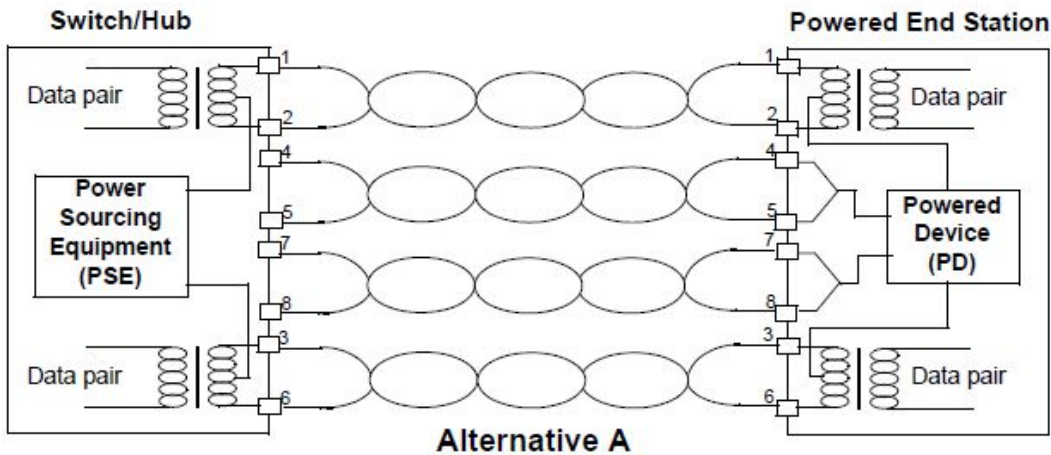


图 12-1 10BASE-T 与 100BASE-TX Alternative A 供电模式

2、通过空闲线对供电 (Alternative B)

如下图所示，PSE 通过空闲线对给 PD 供电。4、5 链接形成正极，7、8 链接形成负极。

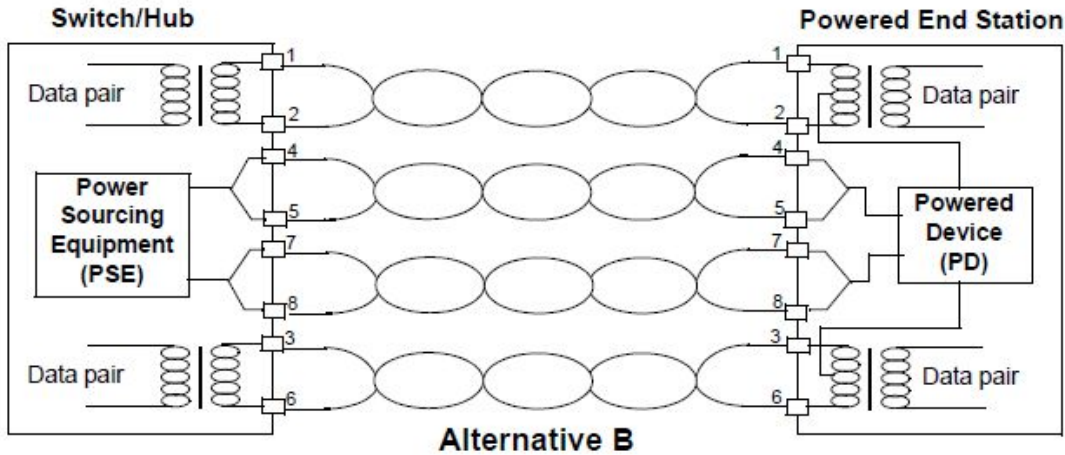


图 12-2 10BASE-T 与 100BASE-TX Alternative B 供电模式

根据 IEEE802.3af 标准，标准的 PD 必须支持信号线对供电和空闲线对供电两种受电方式，但 PSE 只需支持其中一种即可。

12.1.2 PoE 供电过程 **-S -E -A**

当在一个网络中布置 PSE 供电端设备时，PoE 以太网供电工作过程如下所示：

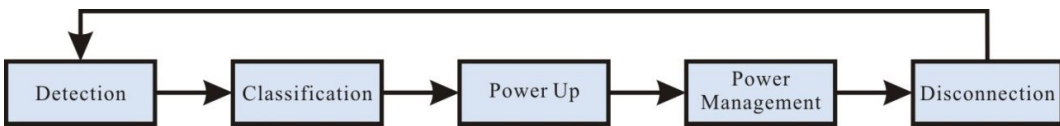


图 12-3 PSE 供电过程

- Detection (检测)：在把任何网络设备连接到 PSE 时，PSE 必须先检测设备是不是 PD，以保证不会给非 PD 提供电流，否则可能会损坏连接的设备。PSE 通过检测电源输出线对之间的阻容值来判断 PD 是否存在，只有检测到 PD，PSE 才会进入下一个步骤。
- Classification (分级)：当检测到 PD 之后，PSE 可能需要对 PD 进行分类，PSE 通过检测电源输出电流来确定 PD 功率等级。供电过程中，分级是可选的。
- Power Up (上电)：在一个可配置时间（一般小于 15us）的启动期内，PSE 开始从低电压向 PD 供电，直至提供 48V 的直流电源。

- Power Management (电源管理和实时监控)：PSE 为 PD 提供稳定可靠的 48V 直流电源。一旦 PSE 开始提供电源，它会持续监测 PD 电流输入，当 PD 电流消耗下降到最低值以下，如在拔下 PD 时或遇到 PD 功率消耗过载、短路、超过 PSE 供电负荷等，则认为 PD 不在位或者 PD 异常，PSE 会停止给 PD 供电。
- Disconnection (断电检测和断电)：PSE 通过检测 PD 的电流来判断 PD 是否断开，如果 PD 断开，PSE 就会快速地（一般在 300~400ms 之内）停止为 PD 供电，PSE 将重新回到 Detection 状态。

12.2 PoE 功能配置

表 12-1 PoE 功能配置列表

配置任务	
配置 PoE 基本功能	使能全局 PoE 功能
	使能接口 PoE 功能
	使能接口强制供电功能
	使能接口自动供电功能
配置 PoE 功率	配置 PoE 电源总功率
	配置 PoE 电源保护功率
	配置接口最大输出功率限制模式
	配置接口最大输出功率
配置供电优先级	配置 PoE 功率管理模式
	配置接口供电优先级
配置 PD 上电断电参数	配置接口 PD 检测模式

配置任务	
	配置接口分级模式
	配置接口上电冲击电流模式
	配置接口供电线对
	配置接口断电检测模式
配置异常恢复功能	配置接口供电异常恢复时间
	重启 PoE 电源
配置 PoE 功率告警功能	配置 PoE 功率告警阈值

12.2.1 配置 PoE 基本功能

-S -E -A

PoE 功能需要通过配置全局 PoE 使能和接口 PoE 使能来控制，也就是说全局和接口的 PoE 功能必须同时使能，才能使用 PoE 功能。使用全局 PoE 功能禁用命令，可以方便的禁用所有接口 PoE 功能。使用接口 PoE 功能禁用命令，可以选择性的禁用一些接口的 PoE 功能。使能接口 PoE 功能是一种标准的供电方式，而接口强制供电功能是一种特殊的供电方式，同一时刻只能选择其中一种，但这两种供电方式都必须在使能全局 PoE 功能时才能生效。

配置条件

无

使能全局 PoE 功能

表 12-2 使能全局 PoE 功能

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
使能全局 PoE 功能	power enable	可选 缺省情况下，全局 PoE 功能已开启

使能接口 PoE 功能

表 12-3 使能接口 PoE 功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
使能全局 PoE 功能	power enable	可选 缺省情况下，全局 PoE 功能已开启
进入二/三层以太网接口配置模式	interface <i>interface-name</i>	-
使能接口 PoE 功能	power enable	可选 缺省情况下，接口 PoE 功能已开启

使能接口强制供电功能

表 12-4 使能接口强制供电功能

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
使能全局 PoE 功能	power enable	可选 缺省情况下, 全局 PoE 功能已开启
进入二/三层以太接口配置模式	interface interface-name	-
使能接口强制供电功能	power force { always once }	必选 缺省情况下, 接口强制供电功能未开启

说明:

强制供电属于一种特殊的供电模式, 不需要配置使能接口 PoE 功能。

使能接口自动供电功能

表 12-5 使能接口自动供电功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
使能全局 PoE 功能	power enable	可选 缺省情况下, 全局 PoE 功能已开启
进入二/三层以太接口配置模式	interface interface-name	-

步骤	命令	说明
使能接口自动供电功能	power auto-enable	必选 缺省情况下，接口自动供电功能未开启

说明：

接口自动供电功能，在手动功率管理模式下才起作用。

12.2.2 配置 PoE 功率

-S -E -A

配置条件

在配置 PoE 功率之前，首先完成以下任务：

- 使能全局 PoE 功能。
- 使能接口 PoE 功能。

配置 PoE 电源总功率

通过配置 PoE 电源总功率，来限制设备最大供电输出功率。当所有的 PD 所需总功率超过配置的电源总功率时，会根据当前供电优先级的模式来选择停止为某些 PD 供电。

表 12-6 配置 PoE 电源总功率

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 PoE 电源总功率		可选

步骤	命令	说明
	power total-power { all <i>system-id</i> { all <i>subsystem-id</i> } } power-value	缺省情况下，电源总功率为设备电源能够提供的最大总功率

配置 PoE 电源保护功率

PD 正常受电过程中，所消耗的功率会在一定的范围内波动，为了避免功率波动导致 PD 断电，需要从设备总功率中预留一部分功率作为保护功率，当 PD 消耗功率增长时，增长的部分会从保护功率中分配。

保护功率也可能被分配用于正常供电，当设备可分配功率不足以为新连接的 PD 供电时，如果此时设备可分配功率加上保护功率的值大于或等于新连接 PD 的接口最大输出功率值，会从保护功率中分配足够的功率来为新连接的 PD 供电。

表 12-7 配置 PoE 电源保护功率

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 PoE 电源保护功率	power guard-band { all <i>system-id</i> { all <i>subsystem-id</i> } } guard-band-value	可选 缺省情况下，电源保护功率为 40.0 瓦特

配置接口最大输出功率限制模式

接口输出的最大功率，可以根据 PD 分级类型来确定，也可以通过用户自定义配置的方式指定接口最大输出功率值。

表 12-8 配置接口最大输出功率限制模式

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二/三层以太网接口配置模式	interface <i>interface-name</i>	-
配置接口最大输出功率限制模式	power threshold-mode { classification user }	可选 缺省情况下，最大输出功率限制模式为用户配置模式

配置接口最大输出功率

限制 PSE 对接口连接的 PD 分配的最大功率值。对所需功率超过接口最大输出功率的 PD，PSE 将不会对其供电。

表 12-9 配置接口最大输出功率

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二/三层以太网接口配置模式	interface <i>interface-name</i>	-
配置接口最大输出功率限制模式为用户配置模式	power threshold-mode user	必选 缺省情况下，最大输出功率限制模式为用户配置模式
配置接口最大输出功率	power port-max-power <i>max-power-value</i>	可选

步骤	命令	说明
		缺省情况下，最大输出功率为 30.0 瓦特

12.2.3 配置供电优先级

-S -E -A

供电优先级功能是在设备能够提供的总功率不足以为所有的 PD 供电时，保证关键 PD 能够优先得到供电的手段。可以通过该命令来配置以何种方式优先为关键 PD 供电。

配置条件

在配置供电优先级之前，首先完成以下任务：

- 使能全局 PoE 功能。
- 使能接口 PoE 功能。

配置 PoE 功率管理模式

表 12-10 配置 PoE 功率管理模式

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 PoE 功率管理模式	power manage { all system-id { all subsystem-id } } { dynamic-fifs dynamic-priority static-fifs static-priority }	可选 缺省情况下，功率管理模式为动态先来先服务

配置接口供电优先级

如果 PoE 功率管理模式为动态优先级模式，当 PSE 的供电功率不足时，优先保证对接口供电优先级较高的 PD 供电。如果接口供电优先级都相同，则优先对接口编号较小的 PD 供电。

表 12-11 配置接口供电优先级

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 PoE 功率管理模式为动态优先级	power manage { all system-id { all subsystem-id } } dynamic-priority	必须 缺省情况下，功率管理模式为动态先来先服务
进入二/三层以太网接口配置模式	interface interface-name	-
配置接口供电优先级	power priority { critical high medium low }	可选 缺省情况下，供电优先级为低优先级

12.2.4 配置 PD 上电断电参数 **-S -E -A**

PoE 上电过程分为几个阶段：

1. Detection：检测，PSE 检测 PD 是否存在。
2. Classification：分级，PSE 对 PD 进行分级并确定 PD 功耗。该阶段可选。
3. Power-Up：上电，PSE 给 PD 供电。

可以通过调整以上几个阶段的参数，来为不同类型的 PD 进行供电。

配置条件

在配置 PD 上电参数之前，首先完成以下任务：

- 使能全局 PoE 功能。

- 使能接口 PoE 功能。

配置接口 PD 检测模式

接口使能 PoE 功能后，PSE 通过检测电源输出线对之间的阻容值来判断 PD 是否存在。标准检测模式只能够检测到符合 IEEE802.3af 和 IEEE802.3at 标准的 PD。标准对 PD 和非 PD 进行了定义，但还有一种设备的阻容值介于 PD 和非 PD 之间，兼容模式就是检测这种设备。

表 12-12 配置接口 PD 检测模式

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二/三层以太接口配置模式	interface <i>interface-name</i>	-
配置接口 PD 检测模式	power detect-mode { compatible standard }	可选 缺省情况下，PD 检测模式为标准模式

配置接口分级模式

接口使能 PoE 功能后，PSE 通过检测电源输出电流来确定 PD 的功率等级。根据 PD 的功率等级来为 PD 分配对应的功率。PD 分级在整个上电流程中是可选步骤，可以配置为不分级模式来跳过该步骤。

表 12-13 配置接口分级模式

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二/三层以太接口配置模式	interface <i>interface-name</i>	-

步骤	命令	说明
配置接口分级模式	power class-mode { standard never }	可选 缺省情况下，分级模式为不分级

说明：

某些非标准 PD 可能不支持分级，这种情况该 PD 默认分级为 class0，接口最大输出功率为 15.4 瓦特。

配置接口上电冲击电流模式

PoE 标准规范了为 PD 上电时的冲击电流。该参数与 PSE、PD 的（寄生）电容、PD 功率相关。对于某些符合或者不符合规范的 PD，所需的上电冲击电流可能会有差异，需要为不同的 PD 配置相应的上电冲击电流模式。

表 12-14 配置接口上电冲击电流模式

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二/三层以太网接口配置模式	interface <i>interface-name</i>	-
配置接口上电冲击电流模式	power power-up-mode { 802.3af high Pre-802.3at 802.3at }	可选 缺省情况下，上电冲击电流模式为高冲击电流

配置接口供电线对

PoE 标准规范了空闲线和数据线对两种供电模式，标准的 PD 需要支持信号线对供电和空闲线对供电两种受电方式，但 PSE 只需支持其中一种即可。

表 12-15 配置接口供电线对模式

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二/三层以太接口配置模式	interface interface-name	-
配置接口供电线对模式	power power-pair{pair-A pair-B }	可选 缺省情况下，供电线对模式为数据线

说明：

PSE 设备只支持数据线供电模式。

配置接口断电检测模式

PSE 交换机可根据供电的电流类型直流或交流，提供不同的断电检测模式。

表 12-16 配置接口断电检测模式

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二/三层以太接口配置模式	interface interface-name	-

步骤	命令	说明
配置接口断电检测模式	power disconnect{ ac dc }	可选 缺省情况下，断电检测模式为直流

说明：

PSE 设备的 PoE 功能集成到交换机内，以直流方式供电，只支持接口断电检测模式为直流模式。

12.2.5 配置异常恢复功能 **-S -E -A**

PoE 供电异常时，支持异常恢复功能，包括自动恢复和手动恢复两种方式。

配置条件

在配置异常恢复功能之前，首先完成以下任务：

- 使能全局 PoE 功能。
- 使能接口 PoE 功能。

配置接口供电异常恢复时间

PSE 为 PD 供电过程中检测到接口供电状态异常时，会自动禁用接口 PoE 功能，然后在指定的异常恢复时间间隔后，重新使能接口 PoE 功能，尝试恢复对该接口的 PD 供电。

表 12-17 配置接口供电异常恢复时间

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
进入二/三层以太接口配置模式	interface <i>interface-name</i>	-
配置接口供电异常恢复时间	power recover-time <i>time-value</i>	可选 缺省情况下，供电异常恢复时间为 0 分钟，表示异常后立即恢复

重启 PoE 电源

当出现 PoE 供电异常，或者 PoE 电源工作异常时，可以通过手动热重启 PoE 电源的方式尝试从异常状态中恢复。

表 12-18 配置接口供电异常恢复时间

步骤	命令	说明
重启 PoE 电源	power reload { all <i>system-id</i> }	必选

说明：

在电源重启过程中，再次执行 **power reload** 命令会提示执行失败。

12.2.6 配置 PoE 功率告警阈值

-S -E -A

配置条件

在配置 PoE 功率之前，首先完成以下任务：

- 使能全局 PoE 功能；
- 使能接口 PoE 功能。

配置 PoE 功率告警阈值

当 PoE 功率利用率达到或低于设置的功率阈值时，会发送 Trap 告警提示。

表 12-19 配置 PoE 功率告警阈值

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 PoE 功率告警阈值	power alarm-threshold { all <i>system-id</i> { all <i>subsystem-id</i> } } <i>threshold-value</i>	可选 缺省情况下，电源功率告警阈值为 99%

12.2.7 PoE 监控与维护

-S -E -A

表 12-20 PoE 监控与维护

命令	说明
show power { manage summary configure interface <i>interface-name</i> detect interface <i>interface-name</i> pd-status interface <i>interface-name</i> /	显示 PoE 配置、供电状态及端口对应关系信息

命令	说明
<code>system-to-port [<i>system-id</i>] / version }</code>	

13 LUM

13.1 LUM 简介

LUM: 本地用户 LUM (Local User Manager) 是用于提供 aaa 的本地认证的本地用户数据库。

RBAC: (Role Based Access Control, 基于角色的访问控制) 通过建立“权限<->角色”的关联实现将权限赋予给角色, 并通过建立“角色<->用户”的关联实现为用户指定角色, 从而使用户获得相应角色所具有的权限。RBAC 的基本思想就是给用户指定角色, 这些角色中定义了允许用户操作哪些系统功能以及资源对象。

由于权限与用户的分离, RBAC 具有以下优势:

- 管理员不需要针对用户去逐一指定权限, 只需要预先定义具有相应权限的角色, 再将角色赋予用户即可。因此RBAC 更能适应用户的变化, 提高了用户权限分配的灵活性。
- 由于角色与用户的关系常常会发生变化, 但是角色和权限的关系相对稳定, 因此利用这种稳定的关联可减小用户授权管理的复杂性, 降低管理开销。

角色: 规则的集合。

规则：指定特性或所有特性的命令的permit/deny权限。

特性：模块。

13.2 LUM 功能配置

表 13-1 LUM 功能配置列表

配置任务	
配置用户角色	配置用户角色
配置管理员方案	配置管理员
	配置管理员用户组
配置接入用户方案	配置接入用户
	配置用户组

13.2.1 配置角色 **-B -S -E -A**

默认有安全管理员角色（Security-admin）、网络管理员角色(Network-admin)、审计员角色(Audit-admin)和网络监控管理员角色（Network-operator）四种角色，这四种角色的权限不能修改。

自定义角色权限为网络管理员角色权限的子集，不允许配置已经被赋予安全管理员角色（Security-admin）、审计员角色(Audit-admin)的模块权限。具体的权限请参见下表。

	日志	History	用户管理、用户认证	其他模块
--	----	---------	-----------	------

公共	NO	NO	修改自身密码	Show running、exit 等
安全管理员	操作日志查看以及相关配置命令	Histry 配置以及操作	OK	lai 模块、line、service、AAA
审计管理员	数据日志查看以及配置命令	NO	NO	NO
网络管理员	操作日志和数据日志以外其他所有命令	History 配置以及操作	NO	OK
网络监控管理员	网络管理员权限内的所有 show 命令	show 命令	NO	网络管理员权限内的所有 show 命令

默认情况下，用户没有配置 role 属性。当 role 属性生效时，用户等级不再生效，角色代替用户等级成为指令授权的基本标准：用户根据各自角色的不同拥有不同指令的执行权限。

配置条件

无

配置用户角色

表 13-2 配置用户角色

步骤	命令	说明
进入全局配置模式	configure terminal	-
创建用户角色同时 进入用户角色模式	role <i>role-name</i>	必选 默认有安全管理员 (Security-admin)、网络管理员(Network-admin)、审计员(Audit-admin)和网络监控管理员 (Network-operator) 四种角色，这四种角色的权限不能修改。
为用户角色创建一条规则	rule <i>number</i> { deny permit } feature { all <i>feature-name</i> }	缺省情况下，新创建的用户角色未定义规则，即当前用户角色无任何权限。 规则修改，对于当前在线的用户不生效，对于以后登录使用该角色的规则的用户生效。 规则 ID 小的规则优先级高

13.2.2 配置本地用户

-B -S -E -A

本地用户为存储在设备的用户：包括本地管理员和本地接入用户。只有当认证方式为本地时才生效。创建本地用户时就会指定其类型是管理员还是接入用户。

配置条件

无

配置本地管理员用户

表 13-3 配置管理员

步骤	命令	说明
进入全局配置模式	configure terminal	-
创建管理员用户同时进入管理员用户模式	local-user <i>user-name</i> class manager	必选。 缺省情况下，未配置管理员用户。

配置本地接入用户

表 13-4 配置接入用户

步骤	命令	说明
进入全局配置模式	configure terminal	-
创建接入用户同时进入接入用户模式	local-user <i>user-name</i> class network	必选。 缺省情况下，未配置接入用户。

13.2.3 配置管理员用户属性**-B -S -E -A**

管理员就是指登录设备的用户。

配置本地管理员用户属性时，有以下配置限制和指导：

- 如果用户登录的时候通过 AAA 授权了角色，则用户登录设备后是否执行的命令由角色决定，如果用户登录的时候 AAA 没有授权角色，则用户登录后是否可以执行命令由用户级别决定。
- 对于 SSH 用户，使用公钥认证时，在用户线视图下未配置登录设备的认证方式的时候，其所能使用的命令以与 SSH 用户同名的本地管理员用户视图中设置的用户角色或者用户级别（用户角色的优先级高于用户级别）为准。关于用户角色的详细介绍请参见“LUM 配置指导”中的“配置角色”。
- 用户的密码最大尝试次数属性均可以在本地管理员用户视图和管理员用户组视图下配置，各视图下的配置优先级顺序从高到底依次为：本地管理员用户视图-->管理员用户组视图。
- 用户的密码生存周期属性均可以在本地管理员用户视图、管理员用户组视图和全局视图下配置，各视图下的配置优先级顺序从高到底依次为：本地管理员用户视图-->管理员用户组视图-->全局视图。

配置条件

无

配置管理员用户属性

表 13-5 配置管理员

步骤	命令	说明
进入全局配置模式	configure terminal	-
创建管理员用户同时进入管理员用户模式	local-user <i>user-name</i> class manager	必选。 缺省情况下，没有创建管理员用户。
配置管理员用户密码	password 0 <i>password</i>	必选。 缺省状态下，用户没有密码。
设置用户可以使用服务器类型	service-type { ssh telnet console ftp web }	必选。 缺省状态下，用户不支持任何的 service-type

步骤	命令	说明
设置本地用户所属用户角色	user-role <i>role-name</i>	可选。 缺省情况下未配置管理员角色。 管理员角色优先级高于管理员级别，即当管理员用户配置了角色，管理员权限将以管理员角色为准
设置管理员用户所属的用户组	group <i>group-name</i>	可选。 缺省情况下，未配置用户组。
配置登录用户授权的级别	privilege <i>privilege-level-number</i>	可选。 缺省情况下，默认级别为 1
配置用户要自动执行的命令	autocommand <i>command-line</i>	可选。 默认情况下，用户没有配置自动执行的命令
配置用户自动执行命令的选项	autocommand-option { nohangup [delay <i>delay-time-number</i>] delay <i>delay-time-number</i> [nohangup] }	可选。 缺省情况下，自动执行完命令后断开连接，自动执行命令的延时时间为 0

步骤	命令	说明
配置用户生存周期	password-control livetime <i>user-live-time</i>	可选。 缺省情况下不限制用户的生存周期。
配置管理员用户连续登录认证失败的最大次数	password-control max-try-time <i>max-try-time-number</i>	可选。 默认情况下用户管理不会限制最大尝试次数。
配置同一用户的最大在线数目	max-online-num <i>user-number</i>	可选。 缺省情况下不限制同一用户的最大在线数目。
配置用户可使用的文件权限	filesys-control{read write execute none}	可选。 缺省情况下用户拥有 read、write、execute 的文件权限。
配置设备提供的可供管理员访问或管理的目录	work-directory <i>directory</i>	可选。 缺省情况下为 /flash 目录。该属性当前只作用配置 ftp 用户登录设备的文件目录。

13.2.4 配置接入用户属性 **-B -S -E -A**

接入用户就是通过设备接入网络的用户。

配置条件

无

配置接入用户

表 13-6 配置接入用户

步骤	命令	说明
进入全局配置模式	configure terminal	
创建接入用户同时 进入接入用户模式	local-user <i>user-name</i> class network	必选。 缺省状态下，未配置接入用户。
配置接入用户密码	password 0 <i>password</i>	必选。 缺省状态下，用户没有密码，这可能导致用户无法登录设备
设置接入用户可以 使用的服务器类型	service-type { <i>xauth</i> }	必选。 缺省状态下，用户不支持任何的 service-type
设置接入用户所属 的用户组	group <i>group-name</i>	可选。 缺省状态下，未配置接入用户所属的用户组。
配置用户状态	stat { <i>active / block</i> }	可选。 缺省情况下，用户状态状态为活跃状态。

13.2.5 配置本地用户组

-B -S -E -A

本地用户分为管理员用户组和接入用户组。

配置手册

发布 1.1 04/2020

管理员用户组是管理员用户属性的集合，支持配置密码生存周期，连续登录认证失败的最大次数。

接入用户组是管理接入用户，有层级嵌套，更为形象的体现出公司或者部门的组织架构关系。接入用户组下暂时不支持任何接入用户属性。

配置条件

无

配置管理员用户组

表 13-7 配置管理员用户组

步骤	命令	说明
进入全局配置模式	configure terminal	-
创建管理员用户组并进入其模式	manager-group <i>group-name</i>	必选。 缺省情况下，未配置管理员用户组。
配置管理员用户组下的用户密码生存周期	password-control lifetime <i>user-live-time</i>	可选。 缺省情况下不限制该用户组下管理员用户的生存周期，即以管理员用户视图下配置的密码生存周期为主。
配置管理员用户组下的用户连续登录认证失败的最大次数	password-control max-try-time <i>max-try-time-number</i>	可选。 缺省情况下，管理员用户组下用户连续登录认证失败的次数不限制，即以管理员用户视图下配置的连续登录认证失败的最大次数为主。

配置接入用户组

表 13-8 配置接入用户组

步骤	命令	说明
进入全局配置模式	configure terminal	
创建接入用户组并进入其模式	user-group <i>group-name</i>	必选。 缺省情况下，未配置接入用户组。
配置接入用户组的父组	parent <i>group-name</i>	可选。 缺省情况下，默认父组即为组名路径中的父路径。

13.2.6 配置密码策略

-B -S -E -A

对于我们的系统设计有强大的密码安全策略。从密码复杂度、首次登录强制修改密码和密码的最大尝试次数三部分来保证。密码安全策略仅针对本地管理员用户有效。

密码复杂度：

(1) 密码最小长度限制，管理员可以限制管理员用户密码的最小长度。当设置用户密码的时候，如果输入的密码长度小于设置的最小长度，系统将不允许设置该密码。并提示："Bad password:it is too short."

(2) 密码组合检测功能，管理员可以设置用户密码的组成元素的组合类型。密码的组成元素包括以下 4 种类型：

- 大写字母：[A ~ Z]
- 小写字母：[a ~ z]
- 十进制数字：[0 ~ 9]

- 31 个特殊字符(~!@\$%^&*()_+ -={}|\:;“ ’ <> ,/ ’)

密码元素的组合类型有 4 种，具体涵义如下：

- 组合类型为 1 表示密码中至少包含 1 种元素；
- 组合类型为 2 表示密码中至少包含 2 种元素；
- 组合类型为 3 表示密码中至少包含 3 种元素；
- 组合类型为 4 表示密码中必须包含所有 4 种元素。

当用户设置密码时，系统会检查设定的密码是否符合配置要求，只有符合要求的密码才能设置成功。

(3) 密码不能与用户名相同。当设置管理员用户密码的时候，如果输入的密码与用户名相同，系统将不允许设置该密码。

首次登录强制修改密码：

当启用“用户首次登录强制修改密码”功能后，用户首次登录设备时，系统会输出相应的提示信息要求用户修改密码，否则不允许登录设备。当管理员用户名为“admin”的时候，无论是否开启“首次登录强制修改密码”的功能，该用户首次登录都会强制要求修改密码才能登录设备。

密码生存周期：

密码生存周期用来限制用户密码的使用时间。当密码的使用时间超过密码生存周期后，需要用户更换密码。当用户登录时，如果用户输入已经过期的密码，系统将提示该密码已经过期，本地登录前必须重新设置密码方可继续。如果输入的密码不符合要求，或者连续两次输入的新密码不一致，系统将拒绝此次登录。对于非交互模式下的登录方式，例如 FTP 用户，在密码生存周期到期后，只能由管理员修改 FTP 用户的密码方可登录；但在登录的时间段内恰好密码过期，不会影响本次登录的本次操作，但下一个 FTP 命令将触发下线。特别的，如果首次登录要求修改密码，密码事实上也到了失效时间，登录时只会统一要求修改一次密码。

密码最大尝试次数：

用户最大尝试次数限制可以用来防止恶意用户通过不断尝试来破解密码。密码尝试错误失败超出最大尝试次数以后，系统会将该用户加入 login-secure 模块的黑名单，该用户账号会被锁定一段时间。

配置条件

无

配置条件

表 13-9 配置密码策略

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置密码的复杂度	password-control complexity {min-length <i>len</i> with user-name-check composition type-number <i>type-number</i>}	可选。 缺省情况下，用户密码最小长度为 6，密码元素的组合类型包含 2 种，不允许用户名与密码相同。
配置用户第一次登录强制修改密码	password-control firstmodify enable	可选。 缺省情况下，用户的第一次登录不强制修改密码。 管理员用户名为“admin”的用户再未开启该命令的时候，在首次登录的时候也会强制要求修改密码。
配置用户生存周期	password-control lifetime user-live-time	可选。 缺省情况下不限制用户的生存周期
配置管理员用户连续登录认证失败的最大次数	password-control max-try-time max-try-time-number	可选。 该命令在管理员用户组和管理员用户的视图下配置。 缺省情况下，管理员用户组下用户连续登录认证失

步骤	命令	说明
		败的未配置，即以管理员用户视图下配置的连续登录认证失败的最大次数为主。

13.2.7 LUM 监控与维护

-B -S -E -A

表 13-10 LUM 监控与维护

命令	说明
debug user { manager network }	开启用户管理的 debug 信息
show users class { manager network } [username]	显示用户的配置信息
show role [rolename]	显示所有角色或指定角色的配置信息

13.3 LUM 典型配置举例

13.3.1 配置网络管理员用户

-B -S -E -A

网络需求

- 配置网络管理员用户，验证其具有网路管理员权限。

网络拓扑

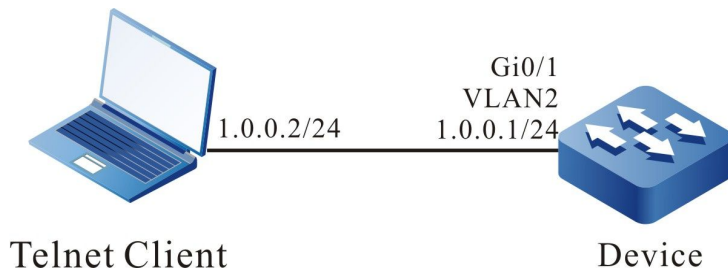


图 13-1 配置网络管理员用户组网图

配置步骤

步骤 1: 配置各接口的 IP 地址。 (略)

步骤 2: 配置管理员属性。

#配置用户 admin, 密码为 admin。

```
Device#configure terminal
Device(config)#local-user admin class manager
Device(config-user-manager-admin)#password 0 admin
```

#配置服务类型

```
Device(config-user-manager-admin)#service-type telnet ftp web console ssh
```

#配置本地用户所属用户角色为网络管理员

```
Device(config-user-manager-admin)#user-role network-admin
```

#配置 local 授权, 使得角色生效

```
Device(config-user-manager-admin)#exit
Device(config)#domain system
Device(config-isp-system)#aaa authentication login local
Device(config-isp-system)#aaa authorization login local
Device(config-isp-system)#exit
```

#配置 line vty 下使用 login aaa 认证

```
Device(config)#line vty 0 15
Device(config-line)#login aaa
```

步骤 3: Telnet 客户端输入用户名 admin, 密码 admin, 成功登录设备。

#验证管理员用户能执行管理员命令 show logging 查看日志

```
Device#show logging
Logging source configurations
console is enabled,level: 7(debugging)
monitor is enabled,level: 7(debugging)
buffer is enabled,level: 5(notifications)
```

file is enabled,level: 7(debugging)
The Context of logging file:

#验证网络管理员不能执行其他管理员的命令

Device#show role
You may not be authorized to perform this operation,please check.

说明:

- 管理员默认角色有 security-admin、network-operator、audit-admin、network-admin 可以根据需要自行设置管理员角色，也可以使用自定义角色
-

接口

14 接口基础

14.1 接口基础简介

设备支持的接口分为物理接口和逻辑接口两大类，其中物理接口为二层以太网接口、三层以太网接口；逻辑接口包括汇聚组接口、VLAN 接口、Loopback 接口、Null 接口、Tunnel 接口等。

二层以太网接口，又被称为端口，是一种物理接口，工作在 OSI 参考模型中的第二层——数据链路层，主要用于数据帧转发和 MAC 地址学习。

三层以太网接口，是一种物理接口，工作在 OSI 参考模型中的第三层——网络层，可以配置 IP 地址，主要用于报文转发。

汇聚组接口，是一种逻辑接口，通过将两台设备间的多条物理链路进行捆绑形成，同样工作在数据链路层，主要用于扩展链路带宽和提高链路可靠性。

VLAN 接口，是一种逻辑接口，用于同 VLAN 绑定，完成不同 VLAN 之间的报文转发。

Loopback 接口，也称本地环回接口，是一种逻辑接口，对于发送到 Loopback 接口的报文，设备都认为其是发往本身，不会将报文转发。

Null 接口，是一种逻辑接口，任何发送往 Null 接口的报文，都将被丢弃。

Tunnel 接口，是一种逻辑接口，为点对点模式提供了传输链路。

对于不同的接口，存在对应的配置模式，接口相关配置模式包括：

- 接口配置模式，对应 VLAN 接口、Loopback 接口、Null 接口、Tunnel 接口。

- 二层以太接口配置模式，对应二层以太接口。
- 三层以太接口配置模式，对应三层以太接口。
- 汇聚组配置模式，对应汇聚组接口。

本章主要介绍各类接口共性的功能配置，各类接口的特性功能配置参见相应的接口章节。

14.2 接口基础功能配置

表 14-1 接口基础功能配置列表

配置任务	
配置接口基本功能	开启/关闭接口
	配置接口描述
	配置接口流量统计时间间隔
配置接口组功能	配置接口组
配置接口状态 SNMP 代理关心层次	配置接口状态 SNMP 代理关心层次

14.2.1 配置接口基本功能 *-B -S -E -A*

配置条件

无

开启/关闭接口

当以太接口被关闭之后，不能接收和发送报文。但是，当以太接口被启用之后，是否可以接收和发送报文还与其它设置相关，例如，对端以太接口是否是启用的、本端与对端以太接口的速率、双工模式和 MDIX (Media Dependent Interface Crossover) 模式等是否匹配。

当汇聚组接口被关闭之后，所有成员端口都被关闭；当汇聚组接口被启用之后，可以单独地关闭或者启用其中的某个成员端口。

表 14-2 开启/关闭接口

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	必选其一 进入接口配置模式后，后续配置只在当前接口生效；
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	进入汇聚组配置模式后，后续配置只在汇聚组接口生效；
进入二/三层以太接口配置模式	interface <i>interface-name</i>	进入二/三层以太接口配置模式后，后续配置只在当前接口生效；
进入虚拟交换链路接口配置模式	vsi-channel <i>vsi-channel-id</i>	进入虚拟交换链路接口模式后，后续配置只在当前虚拟交换链路接口生效
开启接口	no shutdown	必选 缺省情况下，接口为启用状态
关闭接口	shutdown	必选 缺省情况下，接口为启用状态

说明：

- 配置接口描述功能，在 Null 接口上不支持。

配置接口描述

接口描述用于为不同的接口进行命名，帮助用户区分不同接口的类型和实际业务功能，便于用户更好地管理各种接口。

表 14-3 配置接口描述信息

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	必选其一 进入接口配置模式后，后续配置只在当前接口生效；进入汇聚组配置模式后，后续配置只在汇聚组接口生效；进入二/三层以太接口配置模式后，后续配置只在当前接口生效；
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	
进入二/三层以太接口配置模式	interface <i>interface-name</i>	
进入虚拟交换链路接口配置模式	vsl-channel <i>vsl-channel-id</i>	进入虚拟交换链路接口模式后，后续配置只在当前虚拟交换链路接口生效
配置接口描述信息	description <i>description-name</i>	必选 缺省情况下，没有配置接口描述信息
	peer-description <i>description-name</i>	必选 缺省情况下，没有配置对端接口描述信息

说明：

- 配置接口描述功能，在 Null 接口上不支持。

配置接口流量统计时间间隔

不同的接口承载的业务流量不同，通过调整接口的流量统计时间间隔，帮助用户有选择性地关注接口流量历史记录，更加准确地预计接口流量的未来趋势，便于用户分析和调整接口的承载业务。

表 14-4 配置接口流量统计时间间隔

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	必选其一
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	进入接口配置模式后，后续配置只在当前接口生效；进入汇聚组配置模式后，后续配置只在汇聚组接口生效；进入二层以太接口配置模式后，后续配置只在当前端口生效；进入虚拟交换链路接口模式
进入二层以太接口配置模式	interface <i>interface-name</i>	后，后续配置只在当前虚拟交换链路接口生效
进入虚拟交换链路接口模式	vsl-channel <i>vsl-channel-id</i>	
配置接口流量统计时间间隔	load-interval <i>load-interval-value</i>	必选 缺省情况下，接口流量统计时间间隔为 300 秒。

说明：

- 配置接口描述功能，在 Null 接口上不支持。

14.2.2 配置接口组功能 **-B -S -E -A**

将多个接口绑定为一个接口组，在接口组配置各项接口命令，就相当于在接口组内的所有接口上进行配置，而不需要在每个接口上重复配置。显示某个接口组的信息，即显示该接口组内所有接口的信息。

配置条件

接口组覆盖的接口必须已经存在。

配置接口组

表 14-5 配置接口组

步骤	命令	说明
进入全局配置模式	configure terminal	-
以列举方式创建接口组	interface group <i>group-id</i> enum <i>interface-name1 interface-name2 ... interface-nameN</i> [point-to-point multipoint]	必选 缺省情况下，没有创建接口组。
进入全局配置模式	exit	-
以指定范围方式创建接口组	interface group <i>group-id</i> range <i>start-interface-name end-interface-</i>	必选

步骤	命令	说明
	<code>name [point-to-point multipoint]</code>	缺省情况下，没有创建接口组。

说明：

- 接口组下的接口类型必须相同，用户可以根据需要配置多组接口组。
- 接口组下可以配置所有类型接口支持的命令，但如果接口组覆盖的接口并不支持，则相应命令不会生效，且可能没有错误提示，请通过查看配置来检查是否生效。
- 接口组如果覆盖了逻辑接口，当逻辑接口被删除时，接口组下面的逻辑接口也将自动删除。

14.2.3 配置接口状态 SNMP 代理关心层次

-B -S -E -A

接口 UP/DOWN 状态在系统中实际上有两个层次的状态，一个是 L2 链路层状态，一个是 L3 协议层 (protocol) 状态，采用命令 `show ip interface brief` 可以看到。一般情况下这两个状态都随着物理接口 UP/DOWN 变化，但是当以太类接口上配置 `keepalive gateway` 保活时，L3 协议层状态将受到 `keepalive` 保活检测状态的控制。

如果设备上启用了 SNMP 代理功能，则网管服务器可通过公共 `mib` 获取到接口状态信息，并在 SNMP Trap 启用的情况下还可以把接口状态变化信息发送给网管服务器。

通过本功能命令可以设置 SNMP 代理关心的接口状态层次。缺省情况下 SNMP 代理关心的接口状态层次是 L2 链路层，但在以太类接口配置 `keepalive gateway` 保活的情况下，为实现网管服务器呈现的接口状态与 `keepalive` 保活检测状态联动一致，则需要设置 SNMP 代理关心的接口状态层次为 L3 协议层。因此在启用 `keepalive` 检测的环境中（如 MSTP 广域网线路环境），建议配置 `link-status-care l3`。

配置条件

无

配置接口组

表 14-6 配置接口状态 SNMP 代理关心层次

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置接口状态网管层次	link-status-care { l2 l3 }	必选 缺省情况下，接口状态 SNMP 代理关心层次是 L2 链路层
进入全局配置模式	exit	-

14.2.4 接口基础监控与维护

-B -S -E -A

表 14-7 接口基础监控与维护

命令	说明
clear interface group <i>group-id</i>	清除接口组下所有接口的统计信息
interface group <i>group-id</i> display	显示当前接口组所包含的所有接口
show interface group <i>group-id</i>	显示接口组下所有接口的信息

15 以太网接口

15.1 以太网接口简介

以太网接口，包括二层以太网接口和三层以太网接口。

二层以太网接口，又被称为端口，是一种物理接口，工作在 OSI 参考模型中的第二层——数据链路层。它主要用于执行两个基本操作：

数据帧转发：根据数据帧的 MAC (Media Access Control) 地址（即物理地址）进行数据帧的转发操作。二层以太网接口只能对接收到的报文进行二层交换转发，即只能接收和发送源 IP 和目的 IP 处于同一网段的报文。

MAC 地址学习：构造和维护 MAC 地址表，用于支持数据帧的转发操作。

三层以太网接口，是一种物理接口，工作在 OSI 参考模型中的第三层——网络层。它主要用于执行的基本操作：

报文转发：根据报文的 IP (Internet Protocol) 地址（即网络地址）进行报文的路由转发。三层以太网接口只能对接收到的报文进行三层路由转发，即可以接收和发送源 IP 和目的 IP 处于不同网段的报文。

按照以太网接口支持的最大速率，以太网接口类型可以分为以下四种：

fastethernet：百兆以太网接口，可以简称为 Fa，例如 fastethernet0/1 或者 Fa0/1；

gigabitethernet：千兆以太网接口，可以简称为 Gi，例如：gigabitethernet0/25 或者 Gi0/25；

tengigabitethernet：万兆以太网接口，可以简称为 Te，例如：tengigabitethernet1/1 或者 Te1/1；

按照以太网接口的介质类型，以太网接口类型可以分为以下两种：copper（电口）和 fiber（光口）。

15.2 以太接口功能配置

表 15-1 以太接口功能配置列表

配置任务	
配置以太接口基本功能	进入以太接口配置模式
	进入二层以太接口批量配置模式
	配置速率和双工模式
	配置 MDIX (Media Dependent Interface Crossover) 模式
	配置介质类型
	配置 MTU (Maximum Transmission Unit)
	配置流控
	配置延迟时间
	配置自动节能
	配置能效以太网功能
配置以太接口检测功能	配置状态震荡检测
	启用环回测试
配置二层以太接口风暴抑制	配置风暴抑制参数
	配置在发生风暴抑制后执行的动作

配置任务	
配置 UNI/NNI 属性	配置 UNI/NNI 属性
	配置 uni 端口连通性
配置三层以太接口基本功能	配置三层以太接口

15.2.1 配置以太接口基本功能 **-B -S -E -A**

配置条件

无

进入以太接口配置模式

为了在指定以太接口上进行配置，首先进入这个以太接口的二层以太接口配置模式或者三层以太接口配置模式，然后执行相应的配置命令。

表 15-2 进入以太接口配置模式

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二/三层以太接口配置模式	interface interface-name	必选其一 进入二/三层以太接口配置模式后，后续配置只在当前接口生效

说明：

- 以太网接口编号命名规则为 U/S/P (Unit/Slot/Port)，其中 Unit：指在堆叠状态中的设备，从 0 开始编号，设备初始化的时候需要明确是否在堆叠状态中，如果没有，则设备号缺省为 0 并且隐藏。Slot：指设备上的插槽，从 0 开始编号，如果有固定以太网接口，则插槽号 0 预留给固定以太网接口使用，业务插槽从 1 开始编号。Port：指设备上或者接口卡上的以太网接口，每个设备上和接口卡上的以太网接口都是从 1 开始编号。
- 以太网接口名称 *interface-name* 的命名规则为以太网接口类型+以太网接口编号，例如 `gigabitethernet0/1`，表示编号为 1 的千兆以太网接口；`tengigabitethernet1/2`，表示在编号为 1 的业务插槽上编号为 2 的万兆以太网接口；在堆叠模式下，`gigabitethernet0/1/2`，表示成员编号为 0，业务插槽编号为 1 上的编号为 2 的千兆以太网接口。

进入二层以太网接口批量配置模式

当在多个端口上进行相同的配置时，为了提高配置效率，减少相同的重复步骤，选择进入二层以太网接口批量配置模式，包括以下三种的情况：单个端口，例如 `gigabitethernet 0/1`；连续端口，使用“-”表示一段连续端口，例如 `“gigabitethernet 0/3-0/5”`，代表端口 0/3、0/4、0/5；既包括单个端口，又包括连续端口，使用逗号分隔。例如 `“gigabitethernet 0/1, 0/3-0/4, 0/6”`，代表端口 0/1、0/3、0/4、0/6。

表 15-3 进入二层以太网接口批量配置模式

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太网接口批量配置模式	interface interface-list	必选

说明：

- 三层以太网接口不支持批量配置模式。

配置速率和双工模式

设置以太接口的速率，可以分为两类情况：

一类是根据以太接口速率能力集合设置固定速率，可选参数包括：**10**（10M）、**100**（100M）、**1000**（1000M）、**10000**（10000M）；

一类是设置速率为 **auto**（自动协商），指定速率通过本端与对端以太接口自动协商决定。

类似地，设置以太接口的双工模式，也可以分为两类情况：

一类是根据以太接口双工模式能力集合设置双工模式，可选参数包括：**full**（全双工模式）以太接口在接收报文的同时可以发送报文；**half**（半双工模式）以太接口在某一时刻只能接收或者发送报文，但是不能同时进行；

一类是设置双工模式为 **auto**（自动协商），指定双工模式通过本端与对端以太接口自动协商决定。

表 15-4 配置速率和双工模式

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二/三层以太接口配置模式	interface interface-name	必选其一 进入二/三层以太接口配置模式后，后续配置只在当前接口生效
配置以太接口的速率	speed { 10 100 1000 10000 auto }	必选
配置以太接口的双工模式	duplex { auto full half }	必选

说明：

- 当以太接口为百兆光口时，支持的速率为 100M 和自动协商模式，支持的双工模式为

自动协商模式和全双工模式；当以太接口为千兆光口时，支持的速率为 100M、1000M 和自动协商模式，支持的双工模式为自动协商模式和全双工模式；当以太接口为万兆光口时，支持的速率为 1000M、10000M，支持的双工模式为自动协商模式和全双工模式。

配置 MDIX 模式

只有将本端与对端以太接口连接之后才能发送和接收信号，因此 MDIX 模式是和连接线缆配合使用的。

连接以太接口的线缆分为两类：直通线缆（straight-through cable）和交叉线缆（crossover cable）。为了支持使用这两类线缆，提供三种 MDIX 模式：**normal**、**cross** 和 **auto**。

光口只支持直通线缆。

电口由 8 个引脚组成，通过设置 MDIX 模式，可以改变各个引脚的角色。当设置为 **normal** 时，使用引脚 1、2 发送信号，使用引脚 3、6 接收信号；当设置为 **cross** 时，使用引脚 1、2 接收信号，使用 3、6 发送信号；当设置为 **auto** 时，本端和对端电口通过在线缆连接之后自动协商决定各个引脚的作用。

当使用直通线缆时，本端与对端以太接口的 MDIX 模式不能相同。

当使用交叉线缆时，本端与对端以太接口的 MDIX 模式必须相同或者至少有一端为 **auto**。

表 15-5 配置 MDIX 模式

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二/三层以太接口配置模式	interface interface-name	必选其一 进入二/三层以太接口配置模式后，后续配置只在当前接口生效

步骤	命令	说明
配置通过网线接收和发送信号的方式	mdix { auto cross normal }	必选 缺省情况下, 电口的 MDIX 模式为 auto (自动协商), 光口的 MDIX 模式为 normal

说明:

- 光口不支持该配置。

配置介质类型

通过配置以太接口介质类型, 在 Combo 口上切换使用其中的光口或者电口。光口与其对应的电口是光电复用关系, 两者不能同时工作, 当在 Combo 口上指定其中一种介质类型时, 另一种介质类型就自动处于禁用状态。

表 15-6 配置介质类型

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二/三层以太接口配置模式	interface interface-name	必选其一 进入二/三层以太接口配置模式后, 后续配置只在当前接口生效
配置介质类型	media-type { auto copper fiber }	必选

步骤	命令	说明
		缺省情况下，电口的介质类型为 copper ，光口的介质类型为 fiber ，Combo 口的介质类型为 copper

说明：

- 当在 Combo 口上进行光电切换时，切换之后的以太接口配置如速率、双工模式、MDIX 模式等，初始化为缺省值。

配置 MTU

在二层以太接口上配置的 MTU，对于入方向和出方向报文是同时生效的，并且设置的值是相同的。当接收和发送报文的长度超过设置的值时，报文直接丢弃。

与之对比，在三层以太接口上配置的 MTU，对于入方向和出方向的转发报文是同时生效的。当从本机发送报文的长度超过设置的值时，报文首先进行 IP 分片，使得分片报文的长度不超过设置的值，然后再发送出去。

表 15-7 配置 MTU

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二/三层以太接口配置模式	interface <i>interface-name</i>	必选其一 进入二/三层以太接口配置模式后，后续配置只在当前接口生效

步骤	命令	说明
配置 MTU	mtu <i>mtu-value</i>	必选 缺省情况下，二层以太接口的 MTU 为 1824 字节，三层以太接口的 MTU 为 1500 字节

配置流控

在发送或者接收缓冲区满的情况下，如果端口的双工模式为半双工，端口通过背压方式将阻塞信号发回源端；如果端口的双工模式为全双工，端口通过流控报文方式通知源端停止发送。

表 15-9 配置流控

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface <i>interface-name</i>	-
配置流控	flowcontrol { on off }	必选 缺省情况下，端口的流控功能处于关闭状态

说明：

- 只有本端与对端都启用了流控功能，才能实现对本端的流控。
- 三层以太接口不支持配置流控。

配置延迟时间

配置手册

发布 1.1 04/2020

端口由 Up 变为 Down，首先进入设定的抑制时间区间，这时端口状态的切换，不会被系统感知；然后在经过设定的抑制时间后，再向系统报告端口状态变化。这样可以避免由于端口状态在较短时间内频繁切换，给系统带来不必要的运行开销。

表 15-10 配置延迟时间

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太网接口配置模式	interface <i>interface-name</i>	-
配置延迟时间	link-delay <i>link-delay-value</i>	必选 缺省情况下，端口由 Up 变为 Down 的延迟上报时间为 0 秒，即是关闭延迟上报功能，当端口由 Up 变为 Down 时，立即上报并且处理

说明：

- 三层以太网接口不支持配置延迟时间。

配置自动节能

在关闭或者启用但是没有连接线缆的情况下，端口内部始终在轮询端口状态。为了减少这种不必要的能耗，可以通过配置端口自动节能，当端口闲置时，自动切换为低能耗状态。

表 15-11 配置自动节能

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface interface-name	-
配置自动节能	auto-power-down enable	必选 缺省情况下，端口的自动节能功能处于关闭状态

说明：

- 三层以太接口不支持配置自动节能。

配置能效以太网功能

没有数据流量经过的情况下，以太接口内部始终在轮询端口状态。为了减少这种不必要的能耗，可以通过配置能效以太网功能，当以太接口空闲时，自动切换为低能耗状态，正常传输数据时则恢复供电。

表 15-12 配置能效以太网功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二/三层以太接口配置模式	interface interface-name	必选其一

步骤	命令	说明
		进入二/三层以太网接口配置模式后，后续配置只在当前接口生效
配置能效以太网功能	energy-efficient-ethernet enable	必选 缺省情况下，以太网接口的能效以太网功能处于关闭状态

说明：

- 连接在线缆两端的以太网接口都开启能效以太网功能后，功能才生效。
- 光口不支持能效以太网功能。
- 速率为 10Mbps 且双工模式为任意模式的以太网接口、速率为 100Mbps 且双工模式不为自动协商模式的以太网接口不支持能效以太网功能。

15.2.2 配置以太网接口检测功能

-B -S -E -A

配置状态震荡检测

以太网接口由 Down 变为 Up，如果已经配置以太网接口的状态震荡检测，并且满足检测条件，那么就认为指定以太网接口发生状态震荡或称为 Link-Flap，以太网接口将被系统自动关闭并且设置为 Error-Disabled 状态。

表 15-15 配置状态震荡检测

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置震荡检测	errdisable flap-setting cause link-flap max- flaps <i>max-flaps-number</i> time <i>time-value</i>	必选 缺省情况下，执行 Link-Flap 功能的触发条件为，在 10 秒的时间间隔内，检测以太网接口 Up 的次数达到 5 次

说明：

- 当以太网接口被 Link-Flap 功能关闭并且设置为 Error-Disabled 状态之后，如果需要自动恢复，可以通过配置命令 **errdisable recovery cause** 对上述功能进行设置。

启用环回测试

在进行某些故障排除时，例如初步定位以太网接口故障，可以启用以太网接口的环回测试功能。已经启用环回测试功能的以太网接口不能正常转发报文。

以太网接口的环回测试功能包括内部环回测试和外部环回测试两种方式。

内部环回测试，是将指定以太网接口内部的接收端和发送端换接，使得从这个以太网接口发出的报文在设备内部环回，并且又被这个以太网接口接收。如果内部环回测试成功，则表明以太网接口内部工作正常。以太网接口未插光模块时将处于 OMM-disabled 状态，配置内部环回无法 UP，此时需要首先取消端口 OMM-disabled 状态。

外部环回测试，首先在以太网接口上插入一个自环线缆，从指定以太网接口发出的报文通过自环线缆又回到这个以太网接口，并且又被这个以太网接口接收。如果外部环回测试成功，则表明以太网接口工作正常。

表 15-16 启用环回测试

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二/三层以太网接口配置模式	interface interface-name	必选其一 进入二/三层以太网接口配置模式后，后续配置只在当前接口生效
启用环回测试	loopback { internal external }	必选 缺省情况下，没有启用以太接口的环回测试功能

说明：

- 本设备不支持外部环回测试功能。

15.2.3 配置二层以太网接口风暴抑制

-B -S -E -A

配置风暴抑制参数

通过配置风暴抑制参数，限制在端口上允许通过的广播、未知组播或未知单播流量。当端口上的广播、组播或未知单播流量超过设置的阈值时，系统将丢弃超出限制的报文，从而使通过端口的广播、组播或未知单播流量所占的比例降低到限定的范围，保证网络业务的正常运行。

表 15-18 配置风暴抑制参数

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
进入二层以太网接口配置模式	interface <i>interface-name</i>	-
配置风暴抑制参数	storm-control { broadcast multicast unicast } { <i>percent-value</i> bps <i>bps-value</i> pps <i>pps-value</i> }	必选 缺省情况下，没有配置端口的风暴抑制参数

说明：

- 三层以太网接口不支持配置风暴抑制参数。

配置在风暴抑制后执行的动作

当在特定端口上检测到风暴且启用风暴抑制时，可以选择在这个端口上处理风暴的三种策略：

一种是在设备上记录并且在终端上打印输出检测到风暴的告警信息。在这种方式下，由于端口仍然是启用的，端口可以接收后续流量，在端口上发生的风暴不能消除。

一种是关闭端口，在设备上记录并且在终端上打印输出检测到风暴的告警信息，将检测到风暴和关闭端口的告警信息通过 trap 方式发送到配置的日志服务器。在这种方式下，由于端口被关闭，端口不能接收后续流量，在端口上发生的风暴立即消除。

一种是在设备上记录并且在终端上打印输出检测到风暴的告警信息，将检测到风暴的告警信息通过 trap 方式发送到配置的日志服务器。在这种方式下，由于端口仍然是启用的，端口可以接收后续流量，在端口上发生的风暴不能消除。

表 15-19 配置在发生风暴抑制后执行的动作

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface interface-name	-
配置在发生风暴抑制后执行的动作	storm-control action { shutdown trap logging }	必选 缺省情况下，端口在检测到风暴后执行的动作为在设备上记录并且在终端上打印输出检测到风暴的告警信息

说明：

- 当端口被风暴抑制功能关闭并且设置为 Error-Disabled 状态之后，如果需要自动恢复，可以通过配置命令 **errdisable recovery cause** 对上述功能进行设置。
- 三层以太接口不支持配置在发生风暴抑制后执行的动作。

15.2.4 配置 UNI/NNI 类型 **-B -S -E -A**

配置 UNI/NNI 类型

uni 端口，是用户设备与网络之间的连接端口；nni 端口，是网络与网络之间的连接接口。在同一台设备上，nni 端口与 uni 端口或者 nni 端口之间相互连通，没有隔离；uni 端口之间相互隔离。

表 15-20 配置 UNI/NNI 属性

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface interface-name	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation link-aggregation-id	
配置 UNI/NNI 属性	port-type { nni uni }	必选 缺省情况下，二层以太接口和汇聚组的 UNI/NNI 类型为 nni

说明：

- 三层以太接口不支持配置 UNI/NNI 类型。

配置 uni 端口连通性

在缺省情况下，同一台设备的所有 uni 端口之间相互隔离。但是，当其中特定的多个 uni 端口之间为了实现互通，但是又不改变这些 uni 端口与其它 uni 端口之间的隔离关系时，可以配置 uni 端口连通性。

在特定 uni 端口上配置连通性，只能设置这个 uni 端口是否可以转发报文到其它 uni 端口，不影响其它 uni 端口是否可以转发报文到指定 uni 端口。因此，为了实现多个 uni 端口之间互通，必须在这些 uni 端口上分别配置为 community。

表 15-21 配置 uni 端口连通性

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface interface-name	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation link-aggregation-id	
配置 uni 端口连通性	uni-isolate { community isolated }	必选 缺省情况下，uni 端口不能转发报文到其它 uni 端口

说明：

- 这个命令只能在 uni 端口上起效。
- 三层以太接口不支持配置 uni 端口连通性。

15.2.5 配置三层以太接口基本功能

-B -S -E -A

根据以太接口对数据包处理层次的不同，以太接口可工作在二层模式或三层模式。如果将以太接口工作模式设置为二层模式，则作为一个二层以太接口使用；如果将以太接口工作模式设置为三层模式，则作为一个三层以太接口使用，其角色等同于与 VLAN 接口。

配置条件

无

配置三层以太网接口

表 15-22 配置三层以太网接口

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二/三层以太网接口配置模式	interface interface-name	-
配置三层以太网接口	no switchport	必选 缺省情况下，以太网接口工作在二层模式，作为一个二层以太网接口使用

说明：

- 以太网接口的工作模式切换后，该以太网接口下除 `description`、`shutdown`、`speed`、`duplex`、`media-type`、`mdix`、`eee` 配置外其它所有配置都将恢复到新模式下的缺省配置。
- 以太网接口作为一个三层接口使用时，对三层以太网接口基本功能的配置请参照对 VLAN 接口基本功能的配置。

表 15-23 以太接口监控与维护

命令	说明
clear interface <i>interface-name</i>	清除指定三层以太接口的统计信息
clear interface { <i>interface-list</i> switchport } statistics	清除端口的报文和流量统计信息
clear optical { all interface <i>interface-list</i> } exception statistic	清除在以太接口上插入的光模块的异常统计信息
show errdisable flap-values	显示触发执行 Link-Flap 功能的当前设置
show interface { <i>interface-list</i> [group] switchport [brief [down up vsl]] }	显示以太接口或者虚拟交换链路成员端口的全部信息或者摘要信息
show interface <i>interface-list</i> statistics	显示端口的报文和流量统计信息
show interface switchport statistics [packet rate ratio]	显示设备所有端口的报文和流量统计信息
show optical { all interface <i>interface-list</i> } [detail exception statistic]	显示在以太接口上插入的光模块的信息
show port-type [<i>interface-list</i> { uni nni } [interface <i>interface-list</i>]]	显示端口的 UNI/NNI 属性信息

命令	说明
show interface <i>interface-list</i> rate-peak [input / output]	显示指定端口的流量监控信息
show storm-control [interface <i>interface-list</i>]	显示指定端口的风暴抑制设置

15.3 以太接口典型配置举例

15.3.1 配置风暴抑制功能 **-B -S -E -A**

网络需求

- 在 Device 的端口上配置风暴抑制功能，对广播、未知单播、未知组播报文进行抑制，实现当 PC1 发送大量广播、未知单播、未知组播报文时，PC2 也能正常访问网络。

网络拓扑

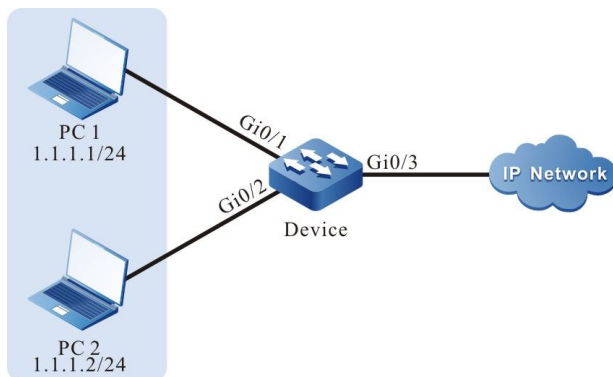


图 15-1 配置风暴抑制组网图

配置步骤

- 步骤 1： 在 Device 上配置 VLAN 和端口的链路类型。

#在 Device 上创建 VLAN2。

配置手册

发布 1.1 04/2020

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#在 Device 上配置端口 gigabitethernet0/1 和 gigabitethernet0/2 的链路类型为 Access，允许 VLAN2 的业务通过。

```
Device(config)#interface gigabitethernet 0/1,0/2
Device(config-if-range)#switchport mode access
Device(config-if-range)#switchport access vlan 2
Device(config-if-range)#exit
```

#在 Device 上配置端口 gigabitethernet0/3 链路类型为 Trunk，允许 VLAN2 的业务通过。

```
Device(config)#interface gigabitethernet 0/3
Device(config-if-gigabitethernet0/3)#switchport mode trunk
Device(config-if-gigabitethernet0/3)#switchport trunk allowed vlan add 2
Device(config-if-gigabitethernet0/3)#exit
```

- 步骤 2： 配置风暴抑制功能。

#在端口 gigabitethernet0/1 上采用 bps 限制方式对广播、未知单播、未知组播报文进行抑制，抑制速率为 1024Kbps。

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#storm-control broadcast bps 1024
Device(config-if-gigabitethernet0/1)#storm-control unicast bps 1024
Device(config-if-gigabitethernet0/1)#storm-control multicast bps 1024
Device(config-if-gigabitethernet0/1)#exit
```

- 步骤 3： 检验结果。

#在 Device 上查看端口 gigabitethernet0/1 的风暴抑制信息。

```
Device#show storm-control interface gigabitethernet 0/1
Interface          Unicast  Broadcast  Multicast  Action
-----
gi0/1              enable   enable     enable     logging
```

#当 PC1 发送大量广播、未知单播、未知组播报文时，PC2 也能正常访问网络。

16 汇聚组接口

16.1 汇聚组接口简介

汇聚组接口，是一种逻辑接口。当在多个端口上启用链路汇聚功能时，具有相同链路汇聚特征的多个端口组成汇聚组，并且抽象为汇聚组接口；同时，这些具有相同属性的多个端口称为汇聚组的成员端口。它主要用于扩展链路带宽和增加连接可靠性。

16.2 汇聚组接口功能配置

表 16-1 汇聚组接口功能配置列表

配置任务	
配置汇聚组接口基本功能	进入汇聚组配置模式
	配置汇聚组转发模式

16.2.1 配置汇聚组接口基本功能 **-B -S -E -A**

配置条件

无

进入汇聚组配置模式

配置手册

发布 1.1 04/2020

表 16-2 进入汇聚组配置模式

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	必选

说明：

- 在进入指定的汇聚组配置模式之前，必须首先创建对应的汇聚组。

配置汇聚组转发模式

在 VST 环境中，为减轻 VSL 链路的负担，缺省情况下，成员设备收到的业务流量优先从本设备的其它以太接口转发出去，即采用本地优先转发策略，在跨设备链路汇聚情况下，汇聚组内各成员链路业务流量的负载是不均衡的。用户可根据实际网络场景，设置汇聚组的转发模式。当转发模式设置为全局负载均衡时，在跨设备链路汇聚情况下，汇聚组内各成员链路业务流量的负载是均衡分布的。

表 16-3 配置汇聚组转发模式

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置汇聚组转发模式	link-aggregation forward-mode { global-fair local-prior }	必选 缺省情况下，汇聚组转发模式为全局负载均衡

说明：

- 当设备工作在 VST 模式下，才支持配置命令 **link-aggregation forward-mode { global-fair | local-prior }**。

16.2.2 汇聚组接口监控与维护

-B -S -E -A

表 16-4 汇聚组接口监控与维护

命令	说明
clear link-aggregation <i>link-aggregation-id</i> statistics	清除指定汇聚组的报文和流量统计信息
show link-aggregation [<i>link-aggregation-id</i> brief]	显示汇聚组的全部信息
show link-aggregation <i>link-aggregation-id</i> statistics	显示指定汇聚组的报文和流量统计信息
show link-aggregation <i>link-aggregation-id</i> rate-peak [input output]	显示指定聚合组的流量监控信息
show port-type link-aggregation <i>link-aggregation-id</i> { uni nni } link-aggregation <i>link-aggregation-id</i>	显示汇聚组的 UNI/NNI 属性信息

17 VLAN 接口

17.1 VLAN 接口简介

VLAN 接口是一个逻辑接口，用于同 VLAN 绑定，完成不同 VLAN 之间的报文转发。一个 VLAN 只能绑定到一个 VLAN 接口上，一个 VLAN 接口也只能绑定一个 VLAN。

17.2 VLAN 接口功能配置

表 17-1 VLAN 接口功能配置列表

配置任务	
配置 VLAN 接口基本功能	配置 VLAN 接口
	配置接口逻辑带宽
	配置接口时延
	配置接口 MTU

17.2.1 配置 VLAN 接口基本功能

-B -S -E -A

配置条件

无

配置 VLAN 接口

表 17-2 配置 VLAN 接口

步骤	命令	说明
进入全局配置模式	configure terminal	-
创建 VLAN 接口	interface vlan <i>vlan-id</i>	必选 缺省情况下，没有创建 VLAN 接口

说明：

- VLAN 接口是一个逻辑接口，它要正常工作，需要创建相应的 VLAN 并把物理端口加入 VLAN。如何创建 VLAN 并把物理端口加入 VLAN，参见配置手册 VLAN 相关章节。
- 创建 VLAN 接口和创建 VLAN 并把物理端口加入 VLAN 没有先后顺序要求。

配置接口逻辑带宽

接口逻辑带宽会影响路由耗费值及 QoS 的计算，不会影响接口的物理带宽。一般情况下，当接口连接广域网时，建议用户配置接口逻辑带宽与租用的线路实际带宽一致。

表 17-3 配置接口逻辑带宽

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface vlan <i>vlan-id</i>	-

接口

步骤	命令	说明
配置 VLAN 接口逻辑带宽	bandwidth <i>width-value</i>	可选 缺省情况下, VLAN 接口逻辑带宽为 100,000Kbps

配置接口时延

接口时延配置会影响路由协议耗费值的计算, 不会影响接口实际传输时延。用户可通过配置接口时延改变路由协议的耗费值。

表 17-4 配置接口时延

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface vlan <i>vlan-id</i>	-
配置 VLAN 接口时延	delay <i>delay-time</i>	可选 缺省情况下, VLAN 接口的时延是 10, 单位为 10 微秒

配置接口 MTU

接口 MTU 决定 IP 分片报文的最大长度, 用户可手动配置。

表 17-5 配置接口 MTU

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
进入接口配置模式	interface vlan <i>vlan-id</i>	-
配置 VLAN 接口 MTU	mtu <i>mtu-size</i>	必选 缺省情况下, VLAN 接口 MTU 为 1500 字节

17.2.2 VLAN 接口监控与维护

-B -S -E -A

表 17-6 VLAN 接口监控与维护

命令	说明
clear interface vlan <i>vlan-id</i>	清除指定 VLAN 接口的统计信息
show interface vlan <i>vlan-id</i>	查看指定 VLAN 接口的信息
show interface vlan <i>vlan-id</i> original statistics	查看指定 VLAN 接口的统计信息

17.3 VLAN 接口典型配置举例

17.3.1 配置 VLAN 接口

-B -S -E -A

网络需求

- 在 Device 上配置 VLAN 接口, 实现属于不同 VLAN 的 PC1 与 PC2 互通。

网络拓扑

配置手册

发布 1.1 04/2020

接口



图 17-1 配置 VLAN 接口组网图

配置步骤

- 步骤 1： 在 Device 上配置 VLAN 和端口的链路类型。

#在 Device 上创建 VLAN2 和 VLAN3。

```
Device#configure terminal
Device(config)#vlan 2-3
```

#在 Device 上配置端口 gigabitethernet0/1 和 gigabitethernet0/2 的链路类型为 Access，gigabitethernet0/1 允许 VLAN2 的业务通过，gigabitethernet0/2 允许 VLAN3 的业务通过。

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
Device(config-if-gigabitethernet0/1)#exit
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode access
Device(config-if-gigabitethernet0/2)#switchport access vlan 3
Device(config-if-gigabitethernet0/2)#exit
```

- 步骤 2： 在 Device 上配置 VLAN 接口及 IP 地址。

#在 Device 上创建 VLAN2 接口，IP 地址为 1.1.1.1，子网掩码为 255.255.255.0；创建 VLAN3 接口，IP 地址为 2.1.1.1，子网掩码为 255.255.255.0。

```
Device(config)#interface vlan 2
Device(config-if-vlan2)#ip address 1.1.1.1 255.255.255.0
Device(config-if-vlan2)#exit
Device(config)#interface vlan 3
Device(config-if-vlan3)#ip address 2.1.1.1 255.255.255.0
Device(config-if-vlan3)#exit
```

- 步骤 3： 检验结果。

#在 Device 上查看 VLAN 接口的信息。

```
Device#show interface vlan 2
vlan2:
  line protocol is up
```



```
Flags: (0xc008063) BROADCAST MULTICAST ARP RUNNING
Type: ETHERNET_CSMACD
Internet address: 1.1.1.1/24
Broadcast address: 1.1.1.255
Metric: 0, MTU: 1500, BW: 100000 Kbps, DLY: 100 usec, VRF: global
Reliability 255/255, Txload 1/255, Rxload 1/255
Ethernet address is 0012.2355.9913
5 minutes input rate 0 bits/sec, 0 packets/sec
5 minutes output rate 0 bits/sec, 0 packets/sec
0 packets received; 1 packets sent
0 multicast packets received
1 multicast packets sent
0 input errors; 0 output errors
0 collisions; 0 dropped
Unknown protocol 0
Device#show interface vlan 3
vlan3:
line protocol is up
Flags: (0xc008063) BROADCAST MULTICAST ARP RUNNING
Type: ETHERNET_CSMACD
Internet address: 2.1.1.1/24
Broadcast address: 2.1.1.255 Metric: 0, MTU: 1500, BW: 100000 Kbps, DLY: 100 usec, VRF: global
Reliability 255/255, Txload 1/255, Rxload 1/255
Ethernet address is 0012.2355.9913
5 minutes input rate 0 bits/sec, 0 packets/sec
5 minutes output rate 0 bits/sec, 0 packets/sec
0 packets received; 1 packets sent
0 multicast packets received
1 multicast packets sent
0 input errors; 0 output errors
0 collisions; 0 dropped
Unknown protocol 0
```

#PC1 能 ping 通 PC2。

18

Loopback 接口

接口

18.1 Loopback 接口简介

Loopback 接口也称本地环回接口，是软件实现的逻辑虚拟接口。此接口不受物理状态的影响，只要不手动关闭，它的状态一直为启用状态。在动态路由协议如 OSPF 中，可以选取 Loopback 接口的 IP 地址作为 Router ID，作为设备的标识。对于发送到 Loopback 接口的报文，设备都认为其是发往本身，不会将报文转发。

18.2 Loopback 接口功能配置

表 18-1 Loopback 接口功能配置列表

配置任务	
配置 Loopback 接口基本功能	配置 Loopback 接口
	配置接口逻辑带宽
	配置接口时延

18.2.1 配置 Loopback 接口基本功能

-B -S -E -A

配置条件

无

配置 Loopback 接口

表 18-2 配置 Loopback 接口

步骤	命令	说明
进入全局配置模式	configure terminal	-
创建 Loopback 接口	interface loopback <i>unit</i> <i>-number</i>	必选

步骤	命令	说明
		缺省情况下，没有创建 Loopback 接口

配置接口逻辑带宽

接口逻辑带宽会影响路由耗费值及 QoS 的计算，不会影响接口的物理带宽。一般情况下，当接口连接广域网时，建议用户配置接口逻辑带宽与租用的线路实际带宽一致。

表 18-3 配置接口逻辑带宽

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置接口逻辑带宽	bandwidth <i>width-value</i>	可选 缺省情况下，Loopback 接口逻辑带宽为 8,000,000 Kbps

配置接口时延

接口时延配置会影响路由协议耗费值的计算，不会影响接口实际传输时延。用户可通过配置接口时延改变路由协议的耗费值。

表 18-4 配置接口时延

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
进入接口配置模式	interface <i>interface-name</i>	-
配置接口时延	delay <i>delay-time</i>	可选 缺省情况下，Loopback 接口的时延是 5000，单位为 10 微秒

19 Null 接口

19.1 Null 接口简介

Null 接口是软件实现的逻辑虚拟接口。任何发送往 Null 接口的报文，都将被丢弃。动态路由协议如 OSPF 会产生自动汇总的路由，外出接口指向 Null 接口，可以有效避免路由环路。Null0 接口由设备默认创建，用户无法关闭或删除。

19.2 Null 接口功能配置

表 19-1 Null 接口功能配置列表

配置任务	
配置 Null 接口基本功能	配置 Null 接口基本功能

19.2.1 配置 Null 接口基本功能 **-S -E -A**

配置条件

无

配置 Null 接口基本功能

表 19-2 配置 Null 接口基本功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 Null 接口配置模式	interface null 0	必选
配置禁止发送 ICMP 不可达差错报文	no ip unreachable	可选 缺省情况下，禁止发送 ICMP 不可达差错报文

说明：

- Null 接口仅支持配置允许或禁止发送 ICMP 不可达差错报文。
- 到达 Null 接口的报文会被丢弃，不需要发送 ICMP 不可达差错。

20 虚拟交换链路接口

20.1 虚拟交换链路接口简介

将多个物理端口捆绑在一起形成一个虚拟交换链路接口（VSL-Channel）。虚拟交换链路接口是堆叠系统中各成员交换机之间进行协议报文交互以及业务数据转发的逻辑链路通道，其中的每个物理端口都称为虚拟交换链路的成员端口。

各成员交换机加入同一个交换域，相互之间通过虚拟交换链路接口进行互联，最后形成一台虚拟的交换机。

20.2 虚拟交换链路接口功能配置

表 7-1 虚拟交换链路接口功能配置列表

配置任务	
配置虚拟交换链路接口功能	进入虚拟交换链路接口配置模式

20.2.1 配置虚拟交换链路接口功能

-B -S -E -A

配置条件

无

进入虚拟交换链路接口配置模式

表 7-2 进入虚拟交换链路接口配置模式

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
进入虚拟交换链路接口配置模式	<code>vsl-channel vsl-channel-id</code>	必选 在单机模式下 <i>vsl-channel-id</i> 为一维值表示虚拟交换链路接口编号，堆叠模式下为二维值，第一维为虚拟交换成员编号，第二维为虚拟交换链路接口编号

说明：

- 在进入虚拟交换链路接口配置模式之前，必须首先创建对应的虚拟交换链路接口。

20.2.2 虚拟交换链路接口监控与维护

-B -S -E -A

表 7-3 虚拟交换链路接口监控与维护

命令	说明
<code>clear vsl-channel vsl-channel-id statistics</code>	清除指定虚拟交换链路接口的报文和流量统计信息
<code>show vsl-channel vsl-channel-id rate-peak [input output]</code>	显示指定虚拟交换链路接口的流量监控信息
<code>show vsl-channel vsl-channel-id statistics</code>	显示指定虚拟交换链路接口的报文和流量统计信息

以太网交换

21 链路汇聚

21.1 链路汇聚简介

链路汇聚，即 Link Aggregation，将两台设备间多条物理链路捆绑在一起形成一个逻辑链路，以扩展链路带宽。逻辑链路内各条物理链路彼此互为冗余和动态备份，以提供更高的网络连接可靠性。

21.1.1 基本概念

汇聚组和成员端口

将多个物理端口捆绑在一起所形成的组合称为汇聚组，而这些被捆绑在一起的物理端口称为汇聚组的成员端口。

成员端口的状态

汇聚组的成员端口有以下两种状态：

- 选中状态：处于这个状态下的端口可以参与用户业务流量转发，处于此状态的成员端口简称为“选中端口”；
- 非选中状态：处于这个状态下的端口不能参与用户业务流量转发，处于此状态的成员端口简称为“非选中端口”。

汇聚组的速率和双工模式取决于汇聚组内的选中端口。汇聚组的速率等于所有选中端口的速率之和，汇聚组的双工模式与选中端口的双工模式相同。

操作 key

操作 key 是成员端口的属性配置，由速率、双工模式及管理 key（即汇聚组编号）组成。属性配置中，双工模式或者速率的变化都会引起操作 key 重新计算。

同一汇聚组中，如果成员端口的双工模式或者速率不同，生成的操作 key 必定不同，但处于选中状态的成员端口一定有相同的操作 key。

LACP 协议

LACP 协议（Link Aggregation Control Protocol，链路汇聚控制协议）是一种基于 IEEE802.3ad 标准的协议。LACP 协议通过 LACPDU（Link Aggregation Control Protocol Data Unit，链路汇聚控制协议数据单元）与对端交互信息。

LACP 优先级

LACP 优先级分为系统 LACP 优先级和端口 LACP 优先级两类：

- 系统 LACP 优先级：用于区分两端设备 LACP 优先级的高低；
- 端口 LACP 优先级：用于决定本端设备成员端口被选中的优先顺序。

系统 ID 和端口 ID

系统 ID：设备的汇聚属性，由设备的系统 LACP 优先级和系统 MAC 地址构成。系统 LACP 优先级越高，则设备的系统 ID 越优。在系统 LACP 优先级相同的情况下，系统 MAC 地址越小，则设备的系统 ID 越优。

端口 ID：端口的汇聚属性，由端口 LACP 优先级和端口编号构成。端口 LACP 优先级越高，端口 ID 越优。在端口 LACP 优先级相同的情况下，端口编号越小，端口 ID 越优。

汇聚组的根端口

汇聚组上应用的协议都是通过汇聚组的根端口接收和发送协议报文。汇聚组根端口从汇聚组成员端口中选出。根端口的物理链路状态必须是 up 的。

链路汇聚模式分为静态汇聚模式和动态汇聚模式。汇聚组类型分为静态汇聚组和动态汇聚组。

静态汇聚模式

静态汇聚模式下，两端设备成员端口的 LACP 协议为禁用状态。静态汇聚组中，本端设备按照以下原则设置成员端口的选中状态：

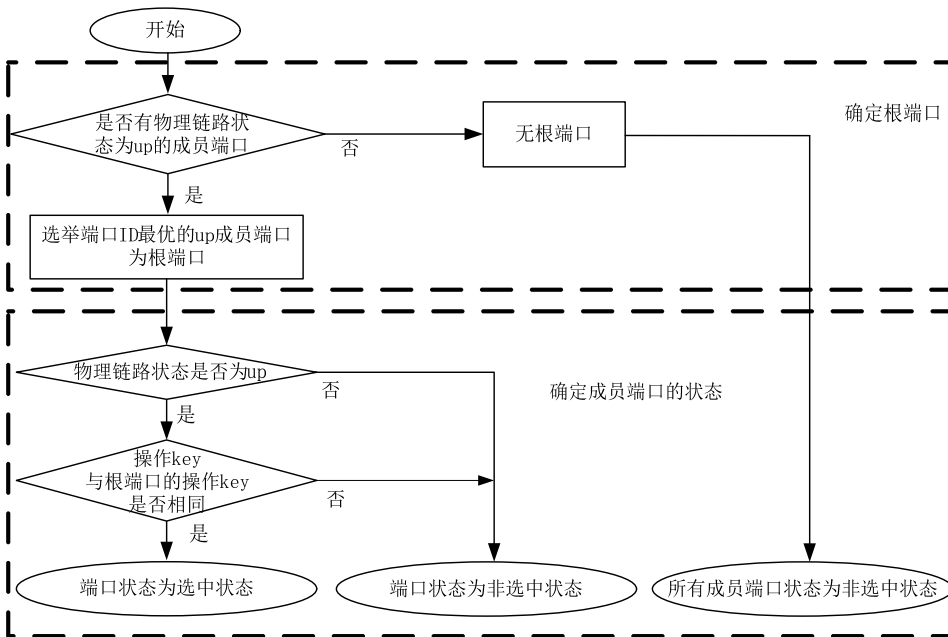


图 21-1 静态汇聚模式下成员端口的选择原则

动态汇聚模式

动态汇聚模式下，端口可以通过两种方式（Active 或者 Passive）加入动态汇聚组。

- 端口的双工模式为全双工：

以 Active（主动）方式加入动态汇聚组，端口的 LACP 协议为开启状态；

以 Passive（被动）方式加入动态汇聚组后，LACP 协议为禁用状态，当收到对端端口发送的 LACPDU 报文时，LACP 协议变为开启状态。

- 端口的双工模式为半双工，无论端口以何种方式加入动态汇聚组，端口的 LACP 协议都处于关闭状态。

动态汇聚组中，系统按照以下原则设置成员端口的选中状态：

确定系统 ID 较优的设备，由该设备决定两端成员端口的状态。系统 ID 较优的设备按照以下原则设置成员端口的选中状态：

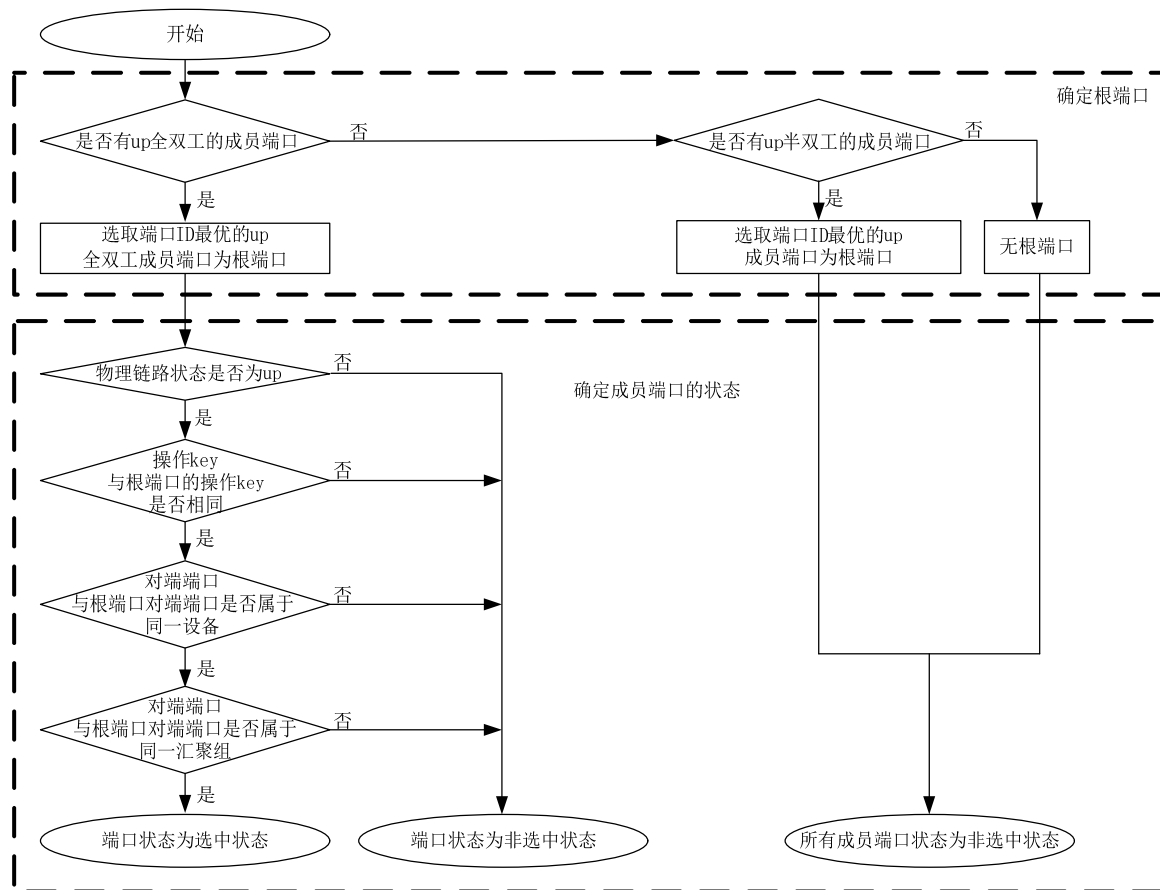


图 21-2 动态汇聚模式下成员端口的选择原则

21.2 负载均衡模板简介

21.2.1 负载均衡 **-B -S -E -A**

负载均衡 (Load-Balance) ，是指当流量的出口是汇聚组时，芯片可根据当前的 HASH 配置条件，使流量在汇聚组内各个成员端口间实现流量的负载均衡，提高聚合组的带宽利用率。

21.2.2 HASH KEY

-B -S -E -A

HASH KEY，是指流量选择汇聚组的具体出端口时，芯片进行 HASH 计算出端口使用的 KEY 值。通常来说，对于不同的报文类型支持的 HASH KEY 会有不同，且不同的交换芯片支持的 HASH KEY 值也有所不同。不同的报文支持的 HASH KEY 的情况如表 1-1 所示。

表 21-1 不同的报文类型支持的 HASH KEY 值及其含义

HASH KEY 类型	说明
dst-mac	基于目的 MAC 地址：按报文的的目的 MAC 地址实现汇聚负载均衡。
src-mac	基于源 MAC 地址：按报文的源 MAC 地址实现汇聚负载均衡。
src-interface	基于接收源接口：按报文的接收源接口实现汇聚负载均衡。
vlan	基于 VLAN：按报文的 VLAN 实现汇聚负载均衡。
dst-ip	基于目的 IP 地址：按报文的的目的 IP 地址实现汇聚负载均衡。
l4-dst-port	基于四层目的端口号：按报文的四层目的端口号实现汇聚负载均衡。
flow-label	基于 IPv6 流标签：按报文的 IPv6 流标签实现汇聚负载均衡。
protocol	基于 IP 协议：按报文的 IP 协议实现汇聚负载均衡。
src-ip	基于源 IP 地址：按报文的源 IP 地址实现汇聚负载均衡。

HASH KEY 类型	说明
I4-src-port	基于四层源端口号：按报文的四层源端口号实现汇聚负载均衡。

本设备中，不同报文支持的 HASH KEY 情况如表 1-2 所示：

表 21-2 不同报文支持的 HASH KEY 情况

报文类型	HASH KEY 支持情况
L2 已知单播报文	dst-mac、src-mac、src-interface、vlan
L3 已知单播报文	dst-ip、I4-dst-port、dst-mac、flow-label、protocol、src-ip、I4-src-port、src-mac、src-interface、vlan
其他 L2 报文	dst-mac、src-mac、src-interface
其他 L3 (IPv4/IPv6) 报文	dst-ip、src-ip、src-interface

说明：

- L2 已知单播报文的 HASH KEY 可以支持一个或者多个 HASH KEY 的组合。
- L3 已知单播报文的 HASH KEY 可以支持一个或者多个 HASH KEY 的组合。
- 其他 L2 报文的 HASH KEY 是固定的，不可配置，固定使用 dst-mac、src-mac、src-interface 进行负载均衡。
- 其他 L3 (IPv4/IPv6) 报文的 HASH KEY 是固定的，不可配置，固定使用 dst-ip、src-ip、src-interface 进行负载均衡。

21.2.3 负载均衡模板

-B -S -E -A

负载均衡模板，是为了屏蔽不同芯片厂商的芯片差异，专门引入的一种“用户-模板”概念。其中，“用户”指的是所有需要使用芯片的负载均衡的业务（即业务模块，如汇聚 LAC）；“模板”则是将底层 HASH 资源抽象出来的一个可以复用 HASH 配置方案。

负载均衡模板通过模板名进行区分，模板名长度不超过 31 个字符。系统默认都会存在一个名为“default”的默认 HASH 模板。除此以外，根据当前的运行模式（单机、堆叠模式）和芯片资源情况，可能还可以为用户提供可以自定义的模板。每个模板，一般由 L2 报文 HASH KEY 配置和 L3 报文 HASH KEY 配置组合而成。

用户可根据实际需要，灵活配置负载均衡模板和对应模板的 HASH KEY。配置完成后，再通过引用或绑定对应的模板即可按照相应的模板配置，实现流量的负载均衡。

说明：

- 负载均衡模板的名字长度不超过 31 个字符。
- 默认负载均衡模板名字“default”不可修改。
- 默认负载均衡模板“default”不可删除，但可以配置。

21.3 负载均衡模板功能配置

表 21-3 负载均衡模板功能配置列表

配置任务	
负载均衡模板配置功能	创建负载均衡模板，并进入模板配置模式
	配置负载均衡模板的 HASH KEY
	删除负载均衡模板

21.3.1 创建负载均衡模板 **-B -S -E -A**

创建负载均衡模板成功后，会进入对应的负载均衡模板配置模式。

说明：

- 单机模式下，最多可以创建 1 个用户自定义模板。
- 堆叠模式下，不支持创建用户自定义模板。

配置条件

无

创建负载均衡模板

表 21-4 创建负载均衡模板

步骤	命令	说明
进入全局配置模式	configure terminal	-
创建负载均衡模板	load-balance profile { <i>profile-name</i> default }	必选

说明：

- 系统默认已经创建了“default”模板，用户可以直接通过创建命令进入到“default”模板的配置模式。
- 创建的模板名字仅支持英文，长度不超过 31 个字符。

21.3.2 配置负载均衡模板的 HASH KEY **-B -S -E -A**

创建负载均衡模板并成功进入模板配置模式后，可以配置对应负载均衡模板的 HASH KEY 值。

说明：

- 系统默认创建的“default”模板会配置一套默认的 HASH KEY，用户也可以按照实际需求修改其配置。
- “default”模板的默认配置为：L2:src-mac、dst-mac；lp:src-ip、dst-ip。

说明：

- 新建的用户自定义模板后，新模板默认没有配置任何 HASH KEY 值，用户须正确配置 HASH KEY 后，才能够被业务的绑定。

配置条件

无

配置负载均衡模板 HASH KEY

表 21-5 配置负载均衡模板 HASH KEY

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入负载均衡模板配置模式	load-balance profile { <i>profile-name</i> default }	必选 与创建负载均衡模板命令相同
配置 L2 已知单播报文负载使用的 HASH KEY	l2 { [dst-mac] [src-mac] [src-interface] [vlan] }	必选 可以一个或多个 HASH KEY 组合
配置 L3 已知单播报文负载使用的 HASH KEY	ip { [dst-ip] [l4-src-port] [l4-dst-port] }	必选

步骤	命令	说明
	[protocol] [src-interface] [src-ip] [src-mac] [vlan] [dst-mac] [flow-label] }	可以一个或多个 HASH KEY 组合
激活当前 HASH KEY 配置	active configuration pending	必选
取消当前 HASH KEY 配置	abort configuration pending	必选

说明：

- 通过 l2 或者 ip 命令配置 HASH KEY 值，处于 pending 状态，不会立即生效，必须通过 active configuration pending 之后才能够生效。
- 通过 l2 或者 ip 命令配置 HASH KEY 值，处于 pending 状态，不会立即生效，用户可以通过 abort configuration pending 命令取消当前的配置。
- 配置新的 HASH KEY 时，不会覆盖原有的 HASH KEY，通过 active 命令激活后的结果是原有 HASH KEY 和新配置的 HASH KEY 合并后的组合。
- 通过 abort 命令取消当前处于 pending 状态的 HASH KEY 时，不会修改原有的 HASH KEY。
- 激活失败时，不会清除 pending 状态的 HASH KEY，激活失败一般都是由于配置的 HASH KEY 不符合要求所致。
- 用户自定义的负载均衡模板可以配置任意 HASH KEY，但是在业务绑定使用时，要求被绑定的模板的 L2 和 L3 都至少有一个生效的 HASH KEY。
- “default” 模板要求：L2 和 L3 的 HASH KEY 都至少配置一个 HASH KEY。

21.3.3 删除负载均衡模板

-B -S -E -A

删除负载均衡模板。

说明：

- 系统默认创建的“default”无法删除。
- 有业务引用或者绑定的模板无法删除，需要先解除所有的引用绑定关系后才能删除。
- 不存在的模板无法删除。

配置条件

无

删除负载均衡模板

表 21-6 删除负载均衡模板

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入负载均衡模板配置模式	no load-balance profile { profile-name }	必选

21.4 链路汇聚功能配置

表 21-7 链路汇聚功能配置列表

配置任务	
配置汇聚组	创建汇聚组
	配置端口加入汇聚组

配置任务	
配置汇聚组引用负载均衡模板	配置汇聚组引用负载均衡模板
配置 LACP 优先级	配置系统 LACP 优先级
	配置端口 LACP 优先级
配置热插拔快速切换根端口	配置热插拔快速切换根端口

21.4.1 配置汇聚组

-B -S -E -A

配置汇聚组后，可以实现对多个物理端口的集中管理，任何对汇聚组的配置都会同时作用到每个成员端口。

说明：

- 每个汇聚组最多可以支持 8 个端口同时加入，最多只能有 8 个端口同时处于选中状态。
-

配置条件

无

创建汇聚组

汇聚链路的两端应配置相同类型的汇聚组。为汇聚组配置描述信息，可以方便网络管理员根据这些信息来区分汇聚组的作用。

表 21-8 配置创建汇聚组

步骤	命令	说明
进入全局配置模式	configure terminal	-
创建汇聚组	link-aggregation link-aggregation-id mode { manual lacp }	必选 缺省情况下，未创建指定汇聚组
进入汇聚组配置模式	link-aggregation link-aggregation-id	-
配置汇聚组描述信息	description <i>description-name</i>	可选 缺省情况下，汇聚组无描述信息
配置汇聚组对端描述信息	peer-description <i>description-name</i>	可选 缺省情况下，汇聚组无对端描述信息

注意：

- 汇聚组上应用的协议都是通过根端口发送和接收协议报文。静态汇聚模式下，两端设备的成员端口之间不交互 LACPDU 报文，可能出现两端设备根端口不在同一条物理链路上的问题，导致汇聚组上应用的其他协议报文收发不正常，因此需要确保两端根端口在同一条物理链路上。动态汇聚模式下，两端设备的成员端口之间交互 LACPDU 报文，通过协商，使根端口在同一条物理链路上。
- 删除某个汇聚组时，汇聚组内所有成员端口将全部离开汇聚组，成员端口的所有配置为缺省情况，可能导致网络出现环路。因此必须确认已使能生成树功能或者确认网络中不会出现环路。

配置端口加入汇聚组

汇聚组最初被创建时，只是一个逻辑接口，无实际物理端口，因此汇聚功能不生效。将端口加入静态汇聚组，汇聚功能即可生效。本端和对端的端口都加入了动态汇聚组，汇聚功能才能生效。

表 21-9 配置端口加入汇聚组

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface interface-name	-
配置端口加入汇聚组	link-aggregation link-aggregation-id { manual active passive }	必选 缺省情况下，端口不加入任何汇聚组

说明：

- 将端口加入指定汇聚组时，要先在系统中创建该汇聚组，否则会出现错误提示信息。
- 一个端口同一时刻只能加入一个汇聚组。
- 端口加入汇聚组后，端口上原有的某些配置（如环回检测、VLAN 等）将会被清除。
- 不能直接对汇聚组内的成员端口进行某些功能（如环回检测）配置，否则会提示错误信息。
- 以 Passive 方式加入动态汇聚组的端口，其对端端口应以 Active 方式加入动态汇聚组。否则这两个端口的选中状态都为非选中状态，不能参与用户业务流量转发。

21.4.2 配置汇聚组引用负载均衡模板

-B -S -E -A

通过配置汇聚组引用的负载均衡模板，可以灵活地实现汇聚组内业务流量的负载均衡。

配置条件

无

配置汇聚组引用负载均衡模板

表 21-10 配置汇聚组引用负载均衡模板

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	-
配置汇聚组引用负载均衡模式	load-balance profile <i>profile-name</i>	必选 缺省情况下，汇聚组引用默认模板实现汇聚负载均衡

21.4.3 配置 LACP 优先级

-B -S -E -A**配置条件**

无

配置系统 LACP 优先级

配置系统 LACP 优先级，会影响系统 ID，最终影响动态汇聚组成员端口的选中/非选中状态。

表 21-11 配置系统 LACP 优先级

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置系统 LACP 优先级	lacp system-priority <i>system-priority-value</i>	必选 缺省情况下，系统 LACP 优先级为 32768

配置端口 LACP 优先级

配置端口 LACP 优先级，会影响端口 ID，最终将会影响汇聚组成员端口的选中/非选中状态。

表 21-12 配置端口 LACP 优先级

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface <i>interface-name</i>	-
配置端口 LACP 优先级	lacp port-priority <i>port-priority-value</i>	必选 缺省情况下，端口 LACP 优先级为 32768

21.4.4 配置热插拔快速切换根端口

-B -S -E -A

配置热插拔快速切换根端口，可以实现热插拔根端口所在板卡时，快速通知对端重新选择根端口，便于汇聚组快速稳定和收敛。

说明：

- 拔出根端口所在板卡时，才会发送快速切换通知。
- 静态汇聚组不会发送快速切换通知。

配置条件

无

配置热插拔快速切换根端口

表 21-13 配置热插拔快速切换根端口

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置热插拔快速切换根端口	link-aggregation hotswap fast-change- rootport	必选 缺省情况下，热插拔快速切换根端口未配置

21.4.5 链路汇聚监控与维护

-B -S -E -A

表 21-14 链路汇聚监控与维护

命令	说明
show link-aggregation group [link-aggregation-id]	显示指定汇聚组或者所有已创建汇聚组的摘要信息

命令	说明
show link-aggregation interface [<i>interface-name</i>]	显示汇聚组指定成员端口的详细信息或者所有已创建汇聚组的所有成员端口的详细信息

21.5 链路汇聚典型配置举例

21.5.1 配置静态汇聚组

-B -S -E -A

网络需求

- Device1 连接 PC1, Device2 连接 PC2、PC3, 3 台 PC 在同一网段, Device1 和 Device2 之间通过 Trunk 端口互联。
- Device1 和 Device2 之间配置静态汇聚组, 以实现增加带宽、负载均衡和业务备份。

网络拓扑

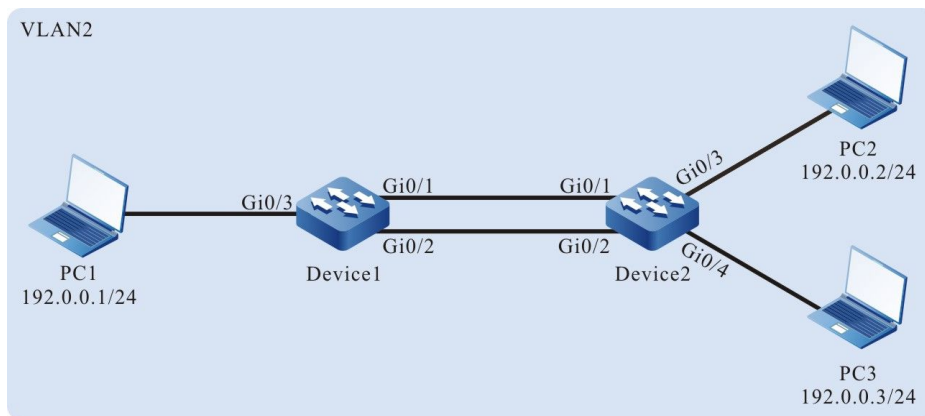


图 21-3 配置静态汇聚组组网图

配置步骤

- 步骤 1: 创建静态汇聚组。

#在 Device1 上创建静态汇聚组 1。

```
Device1#configure terminal
Device1(config)#link-aggregation 1 mode manual
```

#在 Device2 上创建静态汇聚组 1。

```
Device2#configure terminal
Device2(config)#link-aggregation 1 mode manual
```

- 步骤 2: 配置端口加入汇聚组。

#在 Device1 上分别将端口 gigabitethernet0/1、gigabitethernet0/2 以 Manual 方式加入汇聚组 1 中。

```
Device1(config)#interface gigabitethernet 0/1,0/2
Device1(config-if-range)#link-aggregation 1 manual
Device1(config-if-range)#exit
```

#在 Device2 上分别将端口 gigabitethernet0/1、gigabitethernet0/2 以 Manual 方式加入汇聚组 1 中。

```
Device2(config)#interface gigabitethernet 0/1,0/2
Device2(config-if-range)#link-aggregation 1 manual
Device2(config-if-range)#exit
```

#配置完成后，在设备上查看汇聚组 1 状态。

以 Device1 为例：

```
Device1#show link-aggregation group 1
Link Aggregation 1
Mode: Manual
User: LAC
Description:
Peer-description:
Load balance profile: default
Number of ports in total: 2
Number of ports attached: 2
Root port: gigabitethernet0/1
gigabitethernet0/1: ATTACHED
gigabitethernet0/2: ATTACHED
```

可以看到，Device1 上的端口 gigabitethernet0/1、gigabitethernet0/2 在汇聚组 1 中都为 ATTACHED 状态，汇聚组 1 汇聚成功。

说明：

- Device2 的检查方法请参照 Device1。
-

- 步骤 3: 配置汇聚组引用负载均衡模板。

#在 Device1 上创建负载均衡模板 linkagg-profile。

```
Device1(config)#load-balance profile linkagg-profile
```

#在 Device1 上负载均衡模板 linkagg-profile 下配置报文负载 hash-key，配置 L2 报文按照目的 MAC 负载，配置 IP 报文按照目的 IP 负载。

```
Device1(config-hashprofile)#l2 dst-mac
Device1(config-hashprofile)#ip dst-ip
Device1(config-hashprofile)#active configuration pending
```

#在 Device1 上配置汇聚组 1 引用的负载均衡模板为 linkagg-profile。

```
Device1(config)#link-aggregation 1
```

```
Device1(config-link-aggregation1)#load-balance profile linkagg-profile
```

- 步骤 4: 配置 VLAN 及汇聚组和端口的链路类型。

#在 Device1 上创建 VLAN2，配置汇聚组 1 的链路类型为 Trunk，允许 VLAN2 的业务通过，PVID 配置为 2。

```
Device1(config)#vlan 2
Device1(config-vlan2)#exit
Device1(config)#link-aggregation 1
Device1(config-link-aggregation1)#switchport mode trunk
Device1(config-link-aggregation1)#switchport trunk allowed vlan add 2
Device1(config-link-aggregation1)#switchport trunk pvid vlan 2
Device1(config-link-aggregation1)#exit
```

#在 Device1 上配置端口 gigabitethernet0/3 的链路类型为 Access，允许 VLAN2 的业务通过。

```
Device1(config)#interface gigabitethernet 0/3
Device1(config-if-gigabitethernet0/3)#switchport mode access
Device1(config-if-gigabitethernet0/3)#switchport access vlan 2
Device1(config-if-gigabitethernet0/3)#exit
```

#在 Device2 上创建 VLAN2，配置汇聚组 1 的链路类型为 Trunk，允许 VLAN2 的业务通过，PVID 配置为 2。（略）

#在 Device2 上配置端口 gigabitethernet0/3、gigabitethernet0/4 的链路类型为 Access，允许 VLAN2 的业务通过。（略）

- 步骤 5: 检验结果。

#在设备上查看汇聚组 1 的汇聚带宽。

以 Device1 为例:

```
Device1#show link-aggregation 1
link-aggregation 1 configuration information
  Description      :
  Peer-description :
  Status           : Enabled
  Link             : Up
  Act Speed        : 2000
  Act Duplex       : Full
  Port Type        : Nni
  Pvid             : 2
```

可以看到, Device1 上汇聚组 1 的接口带宽为 2000M。

说明:

- Device2 的检查方法请参照 Device1。
-

#在 Device1 上查看汇聚组 1 当前生效的负载均衡模板。

```
Device1#show link-aggregation group 1
Link Aggregation 1
Mode: Manual
User: LAC
Description:
Peer-description :
Load balance profile: linkagg-profile
Number of ports in total: 2
Number of ports attached: 2
Root port: gigabitethernet0/1
gigabitethernet0/1: ATTACHED
gigabitethernet0/2: ATTACHED
```

可以看到, 汇聚组 1 当前的负载均衡模板为 linkagg-profile。

#在 PC1 与 PC2、PC3 进行业务交互的过程中, 数据能在汇聚链路上实现负载均衡。当汇聚组的某条链路出现故障时, 剩余链路能够进行业务备份。

21.5.2 配置动态汇聚组

-B -S -E -A

网络需求

- Device1 连接 PC1, Device2 连接 PC2、PC3, 3 台 PC 在同一网段, Device1 和 Device2 之间通过 Trunk 端口互联。
- Device1 和 Device2 之间配置动态汇聚组, 以实现增加带宽、负载均衡和业务备

份。

网络拓扑

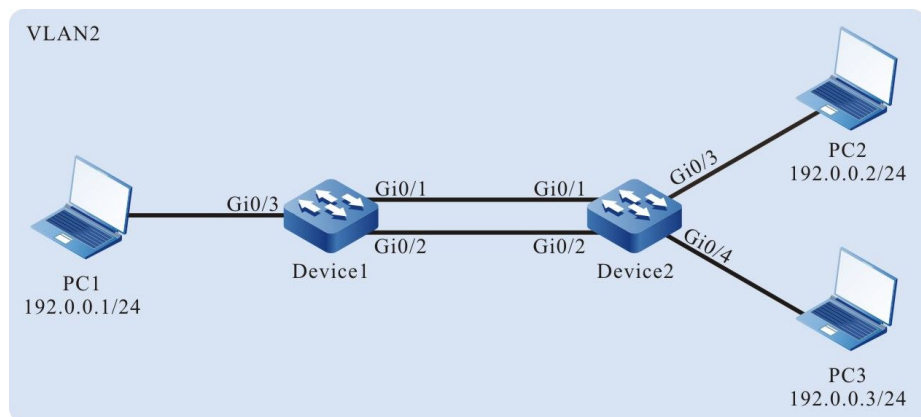


图 21-4 配置动态汇聚组组网图

配置步骤

- 步骤 1: 创建动态汇聚组。

#在 Device1 上创建动态汇聚组 1。

```
Device1#configure terminal
Device1(config)#link-aggregation 1 mode lacp
```

#在 Device2 上创建动态汇聚组 1。

```
Device2#configure terminal
Device2(config)#link-aggregation 1 mode lacp
```

- 步骤 2: 配置端口加入汇聚组。

#在 Device1 上将端口 gigabitethernet0/1、gigabitethernet0/2 以 Active 方式加入汇聚组 1 中。

```
Device1(config)#interface gigabitethernet 0/1,0/2
Device1(config-if-range)#link-aggregation 1 active
Device1(config-if-range)#exit
```

#在 Device2 上将端口 gigabitethernet0/1、gigabitethernet0/2 以 Active 方式加入汇聚组 1 中。

```
Device2(config)#interface gigabitethernet 0/1,0/2
Device2(config-if-range)#link-aggregation 1 active
Device2(config-if-range)#exit
```

#配置完成后，在设备上查看汇聚组 1 状态。

以 Device1 为例:

```
Device1#show link-aggregation group 1
Link Aggregation 1
Mode: LACP
User: LAC
Description:
Peer-description:
Load balance profile: default
Number of ports in total: 2
Number of ports attached: 2
Root port: gigabitethernet0/1
gigabitethernet0/1: ATTACHED
gigabitethernet0/2: ATTACHED
```

可以看到，Device1 上的端口 gigabitethernet0/1、gigabitethernet0/2 在汇聚组 1 中都为 ATTACHED 状态，汇聚组 1 汇聚成功。

说明:

- Device2 的检查方法请参照 Device1。
-

- 步骤 3: 配置汇聚组引用负载均衡模板。

#在 Device1 上创建负载均衡模板 linkagg-profile。

```
Device1(config)#load-balance profile linkagg-profile
```

#在 Device1 上负载均衡模板 linkagg-profile 下配置报文负载 hash-key，配置 L2 报文按照目的 MAC 负载，配置 IP 报文按照目的 IP 负载。

```
Device1(config-hashprofile)#l2 dst-mac
Device1(config-hashprofile)#ip dst-ip
Device1(config-hashprofile)#active configuration pending
```

#在 Device1 上配置汇聚组 1 引用的负载均衡模板为 linkagg-profile。

```
Device1(config)#link-aggregation 1
Device1(config-link-aggregation1)#load-balance profile linkagg-profile
```

#在 Device2 上创建负载均衡模板 linkagg-profile。（略）

#在 Device2 上负载均衡模板 linkagg-profile 下配置报文负载 hash-key，配置 L2 报文按照目的 MAC 负载，配置 IP 报文按照目的 IP 负载。（略）

#在 Device2 上配置汇聚组 1 引用的负载均衡模板为 linkagg-profile。（略）

- 步骤 4: 配置 VLAN 及汇聚组、端口的链路类型。

#在 Device1 上创建 VLAN2，配置汇聚组 1 的链路类型为 Trunk，允许 VLAN2 的业务通过，PVID 配置为 2。

```
Device1(config)#vlan 2
Device1(config-vlan2)#exit
Device1(config)#link-aggregation 1
Device1(config-link-aggregation1)#switchport mode trunk
Device1(config-link-aggregation1)#switchport trunk allowed vlan add 2
Device1(config-link-aggregation1)#switchport trunk pvid vlan 2
Device1(config-link-aggregation1)#exit
```

#在 Device1 上配置端口 gigabitethernet0/3 的链路类型为 Access，允许 VLAN2 的业务通过。

```
Device1(config)#interface gigabitethernet 0/3
Device1(config-if-gigabitethernet0/3)#switchport mode access
Device1(config-if-gigabitethernet0/3)#switchport access vlan 2
Device1(config-if-gigabitethernet0/3)#exit
```

#在 Device2 上创建 VLAN2，配置汇聚组 1 的链路类型为 Trunk，允许 VLAN2 的业务通过，PVID 配置为 2。（略）

#在 Device2 上配置端口 gigabitethernet0/3、gigabitethernet0/4 的链路类型为 Access，允许 VLAN2 的业务通过。（略）

- 步骤 5: 检验结果。

#在设备上查看汇聚组 1 的汇聚带宽。

以 Device1 为例：

```
Device1#show link-aggregation 1
link-aggregation 1 configuration information
  Description      :
  Peer-description :
  Status           : Enabled
  Link             : Up
  Act Speed        : 2000
  Act Duplex       : Full
  Port Type        : Nni
  Pvid             : 2
```

可以看到，Device1 汇聚组接口带宽为 2000M。

说明：

- Device2 的检查方法请参照 Device1。
-

#配置完成后，在 Device1 上查看配置的负载均衡模板。

```
Device1#show load-balance configuration

Profile:default
  Configuration Valid currently:
    L2: src-mac dst-mac
    Ip: src-ip dst-ip
  Configuration Valid-pending to be applied:
    L2:
    Ip:
  Configuration Invalid-pending to be applied:
    L2:
    Ip:
Profile:linkagg-profile
  Configuration Valid currently:
    L2: dst-mac
    Ip: dst-ip
  Configuration Valid-pending to be applied:
    L2:
    Ip:
  Configuration Invalid-pending to be applied:
    L2:
    Ip:
```

#配置完成后，在 Device1 上查看当前生效的负载均衡模板。

```
Device1#show link-aggregation group 1
Link Aggregation 1
Mode: LACP
User: LAC
Description:
Peer-description :
Load balance profile: linkagg-profile
Number of ports in total: 2
Number of ports attached: 2
Root port: gigabitethernet0/1
gigabitethernet0/1: ATTACHED
gigabitethernet0/2: ATTACHED
```

可以看到，汇聚组 1 当前的负载均衡模板为 linkagg-profile。

#在 PC1 与 PC2、PC3 进行业务交互的过程中，数据能在汇聚链路上实现负载均衡。当汇聚组的某条链路出现故障时，剩余链路能够进行业务备份。

22 端口隔离

22.1 端口隔离简介

端口隔离是基于端口的安全特性之一。用户可根据需要，配置指定端口与某些端口隔离，即配置它的被隔离端口，这样，指定端口接收的报文不能转发到被隔离端口，既增强了网络的安全性，也为用户提供了更灵活的组网方案。

22.2 端口隔离功能配置

表 22-1 端口隔离功能配置列表

配置任务	
配置端口隔离基本功能	配置端口隔离
配置汇聚组成员端口隔离功能	配置汇聚组成员端口隔离

22.2.1 配置端口隔离基本功能

-B -S -E -A

端口隔离功能实现的是单方向的报文隔离，假设配置端口 A 的被隔离端口为 B，那么从端口 A 进入的报文，若其目的端口为 B，则报文会被直接丢弃，但是从端口 B 进入的报文，若其目的端口为 A，则报文能正常转发。被隔离端口既可以是端口，也可以是汇聚组。

端口隔离，基于隔离组配置。

- 同隔离组内的端口相互隔离。

隔离组内的端口可配置为 ingress、egress、both 模式，解析如下：

表 22-2 配置模式转发表

报文入端口模式	报文出端口模式	是否能正常转发
ingress 模式	ingress 模式	正常转发
ingress 模式	egress 模式	禁止转发
ingress 模式	both 模式	禁止转发
egress 模式	ingress 模式	正常转发
egress 模式	egress 模式	正常转发
egress 模式	both 模式	正常转发
both 模式	ingress 模式	正常转发
both 模式	egress 模式	禁止转发
both 模式	both 模式	禁止转发

- 隔离组内的端口与未加入隔离组的端口正常通信

不同隔离组内的端口能正常通信

配置条件

隔离组已经被创建

配置端口隔离

表 22-3 配置端口隔离

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入隔离组配置模式	isolate group <i>group-id</i>	必选
端口加入隔离组	interface <i>interface-list</i> [ingress egress both]	必选 缺省情况下，端口未加入隔离组
汇聚组加入隔离组	link-aggregation <i>link-aggregation-id</i> [ingress egress both]	必选 缺省情况下，汇聚组未加入隔离组

说明：

- 端口加入隔离组时，隔离组需要被创建。

22.2.2 配置汇聚组成员端口隔离功能

-B -S -E -A

端口隔离支持汇聚组成员端口隔离功能，使得汇聚组某一成员端口收到的报文不会转发到汇聚组其它成员端口中。

配置条件

配置手册

发布 1.1 04/2020

无

配置汇聚组成员端口隔离

表 22-4 配置汇聚组成员端口隔离

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	-
使能汇聚组成员端口隔离功能	link-aggregation member-isolate	必选 缺省情况下，未使能汇聚组成员端口隔离功能

说明：

- 一般情况下，汇聚组某个成员端口收到的报文不会转发到其他成员端口，但是在 VLAN N: 1 这种特殊的环境不支持汇聚组的这个特性，可以通过使能汇聚组成员端口隔离功能来支持这个特性。

22.2.3 端口隔离监控与维护

-B -S -E -A

表 22-5 端口隔离监控与维护

命令	说明
show isolate { group [<i>group-id</i>] interface <i>interface-list</i> link-aggregation <i>link-aggregation-id</i> }	显示端口隔离信息

22.3 端口隔离典型配置举例

22.3.1 配置端口隔离

-B -S -E -A

网络需求

- PC1 和 PC2 连接到 Device 上，并在同一个 VLAN2 内。
- 在 Device 上配置端口隔离，实现 PC1 与 PC2 之间不能通信。

网络拓扑

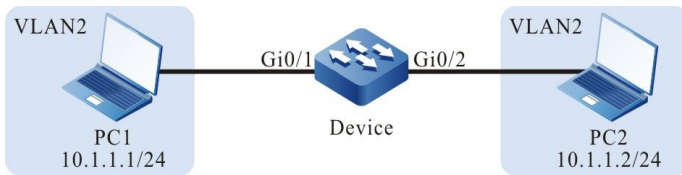


图 22-1 配置端口隔离组网图

配置步骤

步骤 1： 配置 VLAN 及端口的链路类型。

#在 Device 上创建 VLAN2。

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#在 Device 上配置端口 gigabitethernet0/1 和端口 gigabitethernet0/2 的链路类型为 Access，允许 VLAN2 的业务通过。

```
Device(config)#interface gigabitethernet 0/1-0/2
Device(config-if-range)#switchport mode access
Device(config-if-range)#switchport access vlan 2
Device(config-if-range)#exit
```

步骤 2： 配置端口隔离。

#在 Device 上配置隔离组

配置手册

发布 1.1 04/2020

```
Device#config terminal
Device(config)#isolate group 1
Device(config-isolate-group1)#
Device(config-isolate-group1)#end
Device#show isolate group 1
```

```
-----
isolate group 1
ingress member:
egress member :
both member  :
```

#在 Device 上配置端口 gigabitethernet0/1 和端口 gigabitethernet0/2 之间相互隔离。

```
Device#config terminal
Device(config)#isolate group 1
Device(config-isolate-group1)#interface gigabitethernet 0/1-0/2
```

```
Device#show isolate group 1
```

```
-----
isolate group 1
ingress member:
egress member :
both members  : gi0/1-0/2
```

#在 Device 上查看端口隔离信息。

```
Device#show isolate interface gigabitethernet 0/1-0/2
interface gigabitethernet0/1 isolated information
isolate group 1 mode: both
isolated interface:
    gi0/2
interface gigabitethernet0/2 isolated information
isolate group 1 mode: both
isolated interface:
    gi0/1
```

步骤 3: 检验结果。

#PC1 与 PC2 之间不能通信。

23 VLAN

23.1 VLAN 简介

在交换式以太网中，设备的每个端口都是独立的冲突域，但所有端口都属于一个广播域，当一台终端设备发送广播报文时，局域网中所有设备都能收到，既造成了网络带宽浪费，又埋下了安全隐患。

VLAN (Virtual Local Area Network, 虚拟局域网) 是一种将同一局域网中的设备进行逻辑划分的技术，划分在同一 VLAN 内的设备能够相互二层通信，不同 VLAN 内的设备相互二层隔离，这样，广播报文被限制在一个 VLAN 内。

VLAN 遵循 IEEE 802.1Q 协议标准，该标准定义了一种新的帧封装格式，即在传统数据帧的源 MAC 地址后添加 4 字节的 VLAN Tag，用于保存 VLAN 信息。

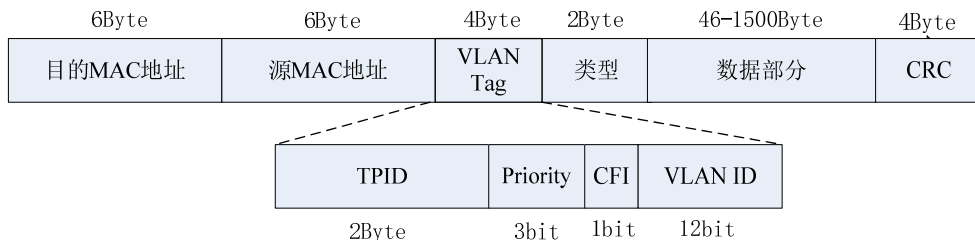


图 23-1 IEEE 802.1Q 帧封装格式

VLAN Tag 包含以下四个字段：

- TPID (Tag Protocol Identifier, 标签协议标识符)：用来判断本数据帧是否携带 VLAN Tag，长度为 2Byte，其值固定为 0x8100，表示为 802.1Q 标准的 Tag；
- Priority: 表示报文的 802.1p 优先级，长度为 3bit，取值范围为 0~7，不同优先级的报文可以得到不同级别的服务；

- CFI (Canonical Format Indicator, 规范格式指示符)：表示 MAC 地址在不同传输介质中是否以标准格式封装，长度为 1bit，取值为 0 表示 MAC 地址以标准格式进行封装，为 1 表示以非标准格式封装；
- VLAN ID：表示报文所属的 VLAN，长度为 12bit，取值范围为 0~4095，其中 0 和 4095 是协议保留值，实际可用的 VLAN ID 范围为 1~4094。

VLAN 具有以下优点：

- 灵活构建虚拟工作组。相同需求的用户可划分为一个 VLAN，不受其物理位置的限制；
- 限制广播域。一个 VLAN 是一个广播域，二层的单播、组播和广播帧只能在本 VLAN 内转发，不能直接进入其他 VLAN，有助于防止广播风暴；
- 提高网络安全性。不同 VLAN 间相互二层隔离，不能直接通信。

VLAN 根据应用的不同可以分为以下四种类型：

- 基于端口的 VLAN；
- 基于 MAC 的 VLAN；
- 基于 IP 子网的 VLAN；
- 基于协议的 VLAN。

缺省情况下，四种 VLAN 划分的优先级别从高到低依次为：基于 MAC 的 VLAN，基于 IP 子网的 VLAN，基于协议的 VLAN，基于端口的 VLAN。在同一端口上，VLAN 划分按优先级别生效，且只有一个 VLAN 划分生效。

23.2 VLAN 功能配置

表 23-1 VLAN 功能配置列表

配置任务	
配置 VLAN 基本属性	配置 VLAN
	配置 VLAN 名称

配置任务	
配置基于端口的 VLAN	配置端口链路类型
	配置 Access 端口加入 VLAN
	配置 Trunk 端口允许 VLAN 通过
	配置 Hybrid 端口加入 VLAN
	配置端口的 PVID
配置基于 MAC 的 VLAN	配置基于 MAC 的 VLAN
配置基于 IP 子网的 VLAN	配置基于 IP 子网的 VLAN
配置基于协议的 VLAN	配置基于协议的 VLAN
配置端口的可接收帧类型	配置端口的可接收帧类型

23.2.1 配置 VLAN 基本属性

-B -S -E -A

配置条件

无

配置 VLAN

每个 VLAN 都是独立的广播域，同一 VLAN 内的用户可以相互二层通信，不同 VLAN 内的用户相互二层隔离。

表 23-2 配置 VLAN

步骤	命令	说明
进入全局配置模式	configure terminal	-
创建 VLAN	vlan <i>vlan-list</i>	必选 缺省情况下，系统自动创建 VLAN1 如果创建单个 VLAN，创建后会进入 VLAN 配置模式，如果创建多个 VLAN，创建后仍在当前配置模式

配置 VLAN 名称

为便于记忆和管理，可以根据 VLAN 的业务类型、功能、连接情况等来配置 VLAN 名称。

表 23-3 配置 VLAN 名称

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 VLAN 配置模式	vlan <i>vlan-id</i>	-
配置 VLAN 名称	name <i>vlan-name</i>	必选 缺省情况下，VLAN1 的名称为“DEFAULT”，其他 VLAN 的名称为“VLAN <i>vlan-id</i> ”，例如“VLAN0100”

23.2.2 配置基于端口的 VLAN

-B -S -E -A

基于端口的 VLAN，又称为端口 VLAN，是最简单的一种 VLAN 划分方式，将端口加入 VLAN，该端口就能够转发所属 VLAN 的报文。

配置条件

无

配置端口链路类型

根据端口转发报文时对 VLAN Tag 的不同处理方式，分为以下三种链路类型：

- Access 类型：转发出去的报文不携带 VLAN Tag，该类型端口一般与用户设备相连；
- Trunk 类型：转发出去的 PVID 所在 VLAN 报文不携带 VLAN Tag，其他 VLAN 的报文保留 VLAN Tag，该类型端口一般用于网络设备间互联；
- Hybrid 类型：可以配置转发出去的指定 VLAN 报文不携带 VLAN Tag 或保留 VLAN Tag，该类型端口既可用于与用户设备相连，也可用于网络设备间互联。

Trunk 类型和 Hybrid 类型端口之间不能直接转换，需先转换为 Access 类型，再转换为其他类型。

表 23-4 配置端口链路类型

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface <i>interface-name</i>	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	进入汇聚组配置模式后，后续配置只在汇聚组生效

步骤	命令	说明
配置端口链路类型	switchport mode { access hybrid trunk }	必选 缺省情况下，端口链路类型为 Access 类型

注意：

- 某些命令只能在指定链路类型的端口上配置，切换端口链路类型会导致原链路类型端口上配置的功能失效。

配置 Access 端口加入 VLAN

Access 端口只能属于一个 VLAN，当配置 Access 端口加入指定 VLAN 时，会退出 Access 端口当前所在 VLAN，再加入指定 VLAN。如果 Access 端口加入的 VLAN 未创建，会自动创建该 VLAN。

表 23-5 配置 Access 端口加入 VLAN

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface <i>interface-name</i>	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	
配置端口链路类型为 Access 类型	switchport mode access	必选

步骤	命令	说明
		缺省情况下，端口链路类型为 Access 类型
配置 Access 端口加入指定 VLAN	switchport access vlan <i>vlan-id</i>	必选 缺省情况下，Access 端口加入 VLAN1

配置 Trunk 端口允许 VLAN 通过

如果 Trunk 端口允许通过的 VLAN 已经创建，则端口允许该 VLAN 数据报文转发；如果 Trunk 端口允许通过的 VLAN 未创建，不会自动创建该 VLAN，需要创建相应的 VLAN 后，端口才允许该 VLAN 数据报文转发。

表 23-6 配置 Trunk 端口允许 VLAN 通过

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface <i>interface-name</i>	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	
配置端口链路类型为 Trunk 类型	switchport mode trunk	必选 缺省情况下，端口链路类型为 Access 类型

步骤	命令	说明
配置 Trunk 端口允许指定 VLAN 通过	switchport trunk allowed vlan { all add vlan-list }	必选 缺省情况下, Trunk 端口允许 VLAN1 通过
配置从 Trunk 端口转发出去的 PVID 所在 VLAN 报文保留 VLAN Tag	vlan dot1q tag pvid	可选 缺省情况下, 从 Trunk 端口转发出去的 PVID 所在 VLAN 报文不携带 VLAN Tag

配置 Hybrid 端口加入 VLAN

如果 Hybrid 端口加入的 VLAN 未创建, 会自动创建该 VLAN。

表 23-7 配置 Hybrid 端口加入 VLAN

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface interface-name	必选其一 进入二层以太接口配置模式后, 后续配置只在当前端口生效; 进入汇聚组配置模式后, 后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation link-aggregation-id	
配置端口链路类型为 Hybrid 类型	switchport mode hybrid	必选

步骤	命令	说明
		缺省情况下，端口链路类型为 Access 类型
配置 Hybrid 端口以指定方式加入指定 VLAN	switchport hybrid { untagged tagged } vlan <i>vlan-list</i>	必选 缺省情况下，Hybrid 端口以 Untagged 方式加入 VLAN1

配置端口的 PVID

PVID (Port VLAN ID, 端口缺省 VLAN) 是端口的一个重要参数，当端口收到 Untag 报文时，会为其添加 VLAN Tag，VLAN Tag 的 VLAN ID 为该端口的 PVID。

Access 端口的 PVID 是它所属 VLAN 的 ID，只能通过配置它所属的 VLAN 来改变 PVID。Trunk 端口和 Hybrid 端口可属于多个 VLAN，其 PVID 可根据需要配置。

Trunk 端口和 Hybrid 端口必须加入其 PVID 所在 VLAN，否则不能转发 PVID 所在 VLAN 的报文，该端口收到的 Untag 报文会被丢弃。

表 23-8 配置端口的 PVID

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface <i>interface-name</i>	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	

步骤	命令	说明
配置 Trunk 端口的 PVID	switchport trunk pvid vlan <i>vlan-id</i>	必选，根据端口链路类型选择其一
配置 Hybrid 端口的 PVID	switchport hybrid pvid vlan <i>vlan-id</i>	缺省情况下，端口的 PVID 为 VLAN1

说明：

- 配置端口的 PVID，PVID 所在 VLAN 必须已经创建，否则无法配置成功，会输出错误提示信息。

23.2.3 配置基于 MAC 的 VLAN

-B -S -E -A

基于 MAC 的 VLAN，又称为 MAC VLAN，是根据报文的源 MAC 地址来划分 VLAN。配置 MAC VLAN 后，如果端口收到 Untag 报文，且报文的源 MAC 地址与某条 MAC VLAN 表项匹配，则系统为报文添加 VLAN Tag，其 VLAN ID 为该匹配表项中的 VLAN ID。

当用户的物理位置改变时，只要用户的 MAC 地址不改变，就不需要重新配置连接用户的端口所属的 VLAN。

配置条件

无

配置基于 MAC 的 VLAN

表 23-9 配置基于 MAC 的 VLAN

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 MAC VLAN 表项	mac-vlan mac-address mac-address vlan vlan- id	必选 缺省情况下，没有 MAC VLAN 表项
进入二层以太接口配置模式	interface interface- name	必选其一 进入二层以太接口配置模 式后，后续配置只在当前 端口生效；进入汇聚组配 置模式后，后续配置只在 汇聚组生效
进入汇聚组配置模式	link-aggregation link- aggregation-id	
使能端口的 MAC VLAN 功能	mac-vlan enable	必选 缺省情况下，端口未使能 MAC VLAN 功能

说明：

- 使能 MAC VLAN 功能的端口需要加入匹配表项的 VLAN，否则不能转发该 VLAN 的报文，源 MAC 地址匹配的报文将被丢弃。

23.2.4 配置基于 IP 子网的 VLAN **-B -S -E -A**

基于 IP 子网的 VLAN，又称为 IP 子网 VLAN，是根据报文的源 IP 地址来划分 VLAN。配置 IP 子网 VLAN 后，如果端口收到 Untag 报文，且报文的源 IP 地址与某条 IP 子网 VLAN 表项匹配，则系统为报文添加 VLAN Tag，其 VLAN ID 为该匹配表项中的 VLAN ID。

当用户的物理位置改变时，只要用户的 IP 地址不改变，就不需要重新配置连接用户的端口所属的 VLAN。

配置条件

无

配置基于 IP 子网的 VLAN

表 23-10 配置基于 IP 子网的 VLAN

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 IP 子网 VLAN 表项	ip-subnet-vlan ipv4 ip-address mask mask vlan vlan-id	必选 缺省情况下，没有 IP 子网 VLAN 表项
进入二层以太接口配置模式	interface interface-name	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation link-aggregation-id	
使能端口的 IP 子网 VLAN 功能	ip-subnet-vlan enable	必选 缺省情况下，端口未使能 IP 子网 VLAN 功能

说明：

- 使能 IP 子网 VLAN 的端口需要加入匹配表项的 VLAN，否则不能转发该 VLAN 的报

文，源 IP 匹配的报文将被丢弃。

23.2.5 配置基于协议的 VLAN -B -S -E -A

基于协议的 VLAN，又称为协议 VLAN，是根据报文的帧封装格式和协议类型来划分 VLAN。定义协议模板，配置端口匹配某一协议模板，且使能端口的协议 VLAN 功能后，如果端口收到 Untag 报文匹配该协议模板，则系统为报文添加 VLAN Tag，其 VLAN ID 为该匹配模板对应的 VLAN ID。

当用户的物理位置改变时，只要用户发送报文的帧封装格式、协议类型不改变，就不需要重新配置连接用户的端口所属的 VLAN。

配置条件

无

配置基于协议的 VLAN

表 23-11 配置基于协议的 VLAN

步骤	命令	说明
进入全局配置模式	configure terminal	-
定义协议模板	protocol-vlan profile <i>profile-index</i> frame-type <i>frame-type</i> ether-type <i>ether-type</i>	必选 缺省情况下，没有定义协议模板
进入二层以太接口配置模式	interface <i>interface-name</i>	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	

步骤	命令	说明
配置端口匹配的协议模板	protocol-vlan profile <i>profile-index</i> vlan <i>vlan-id</i>	必选 缺省情况下，端口未匹配任何协议模板
使能端口的协议 VLAN 功能	protocol-vlan enable	必选 缺省情况下，端口未使能协议 VLAN 功能

说明：

- 配置有匹配协议模板，且使能协议 VLAN 功能的端口，需要加入该匹配协议模板对应的 VLAN，否则不能转发该 VLAN 的报文，协议匹配的报文将被丢弃。

23.2.6 配置端口的可接收帧类型

-B -S -E -A

配置条件

无

配置端口的可接收帧类型

可以通过配置端口的可接收帧类型，使端口只接收 Untag 报文，或只接收 Tag 报文，或两者都接收，不符合要求的报文将被丢弃。

表 23-12 配置端口的可接收帧类型

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
进入二层以太接口配置模式	interface <i>interface-name</i>	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	
配置端口的可接收帧类型	switchport accept frame-type { all untag tag }	必选 缺省情况下，端口的可接收帧类型为 all，即接收所有 Untag 报文和 Tag 报文

23.2.7 VLAN 监控与维护

-B -S -E -A

表 23-13 VLAN 监控与维护

命令	说明
show ip-subnet-vlan	显示 IP 子网 VLAN 信息
show mac-vlan	显示 MAC VLAN 信息
show protocol-vlan [profile]	显示协议 VLAN 信息
show running-config vlan	显示 VLAN 配置信息
show vlan [vlan-id]	显示指定 VLAN 或全部已创建 VLAN 的信息

命令	说明
show vlan statistics	显示已创建 VLAN 的数目
show vlan summary	显示静态创建和动态学习的 VLAN 信息
show { interface <i>interface-name</i> link-aggregation <i>link-aggregation-id</i> } vlan status	显示指定端口或汇聚组的 VLAN 信息

23.3 VLAN 典型配置举例

23.3.1 配置基于端口的 VLAN -B -S -E -A

网络需求

- Server1、PC1 为办公网络的服务器和 PC，Server2、PC2 为生产网络的服务器和 PC。
- 配置基于端口的 VLAN 功能，实现 PC1 和 PC2 相互隔离，PC1 只能访问 Server1，PC2 只能访问 Server2。

网络拓扑

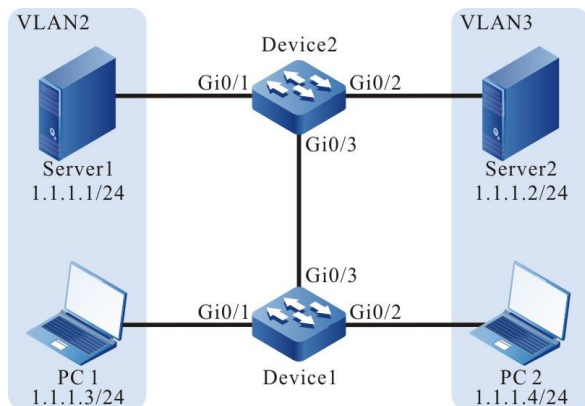


图 23-2 配置基于端口的 VLAN 组网图

配置步骤

- 步骤 1: 在 Device1 上配置 VLAN 及端口的链路类型。

#在 Device1 上创建 VLAN2 和 VLAN3。

```
Device1#configure terminal
Device1(config)#vlan 2-3
```

#在 Device1 上配置端口 gigabitethernet0/1 和 gigabitethernet0/2 的链路类型为 Access, gigabitethernet0/1 允许 VLAN2 的业务通过, gigabitethernet0/2 允许 VLAN3 的业务通过。

```
Device1(config)#interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#switchport mode access
Device1(config-if-gigabitethernet0/1)#switchport access vlan 2
Device1(config-if-gigabitethernet0/1)#exit
Device1(config)#interface gigabitethernet0/2
Device1(config-if-gigabitethernet0/2)#switchport mode access
Device1(config-if-gigabitethernet0/2)#switchport access vlan 3
Device1(config-if-gigabitethernet0/2)#exit
```

#在 Device1 上配置端口 gigabitethernet0/3 的链路类型为 Trunk, 允许 VLAN2 和 VLAN3 的业务通过。

```
Device1(config)#interface gigabitethernet 0/3
Device1(config-if-gigabitethernet0/3)#switchport mode trunk
Device1(config-if-gigabitethernet0/3)#switchport trunk allowed vlan add 2-3
Device1(config-if-gigabitethernet0/3)#exit
```

- 步骤 2: 在 Device2 上配置 VLAN 及端口的链路类型。

#在 Device2 上创建 VLAN2 和 VLAN3。

```
Device2#configure terminal
Device2(config)#vlan 2-3
```

#在 Device2 上配置端口 gigabitethernet0/1 和 gigabitethernet0/2 的链路类型为 Access, gigabitethernet0/1 允许 VLAN2 的业务通过, gigabitethernet0/2 允许 VLAN3 的业务通过。

```
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#switchport mode access
Device2(config-if-gigabitethernet0/1)#switchport access vlan 2
Device2(config-if-gigabitethernet0/1)#exit
Device2(config)#interface gigabitethernet0/2
Device2(config-if-gigabitethernet0/2)#switchport mode access
Device2(config-if-gigabitethernet0/2)#switchport access vlan 3
Device2(config-if-gigabitethernet0/2)#exit
```

#在 Device2 上配置端口 gigabitethernet0/3 的链路类型为 Trunk，允许 VLAN2 和 VLAN3 的业务通过。

```
Device2(config)#interface gigabitethernet 0/3
Device2(config-if-gigabitethernet0/3)#switchport mode trunk
Device2(config-if-gigabitethernet0/3)#switchport trunk allowed vlan add 2-3
Device2(config-if-gigabitethernet0/3)#exit
```

- 步骤 3: 检验结果。

#查看 Device1 上的 VLAN 信息。

```
Device1#show vlan 2
-----
NO. VID VLAN-Name          Owner Mode  Interface
-----
1  2  VLAN0002                static Tagged  gi0/3
                               Untagged gi0/1
Device1#show vlan 3
-----
NO. VID VLAN-Name          Owner Mode  Interface
-----
1  3  VLAN0003                static Tagged  gi0/3
                               Untagged gi0/2
```

#查看 Device2 上的 VLAN 信息。

```
Device2#show vlan 2
-----
NO. VID VLAN-Name          Owner Mode  Interface
-----
1  2  VLAN0002                static Tagged  gi0/3
                               Untagged gi0/1
Device2#show vlan 3
-----
NO. VID VLAN-Name          Owner Mode  Interface
-----
1  3  VLAN0003                static Tagged  gi0/3
                               Untagged gi0/2
```

#PC1 和 PC2 不能互通，PC1 只能访问 Server1，PC2 只能访问 Server2。

23.3.2 配置基于 MAC 的 VLAN

-B -S -E -A

网络需求

- PC1 和 PC2 可以从 Device 的不同端口接入到网络。
- 配置基于 MAC 的 VLAN 功能，使指定 MAC 的 PC 在不同端口进行迁移均可访问服务器；非指定 MAC 的 PC 只能在特定的端口访问服务器。

网络拓扑

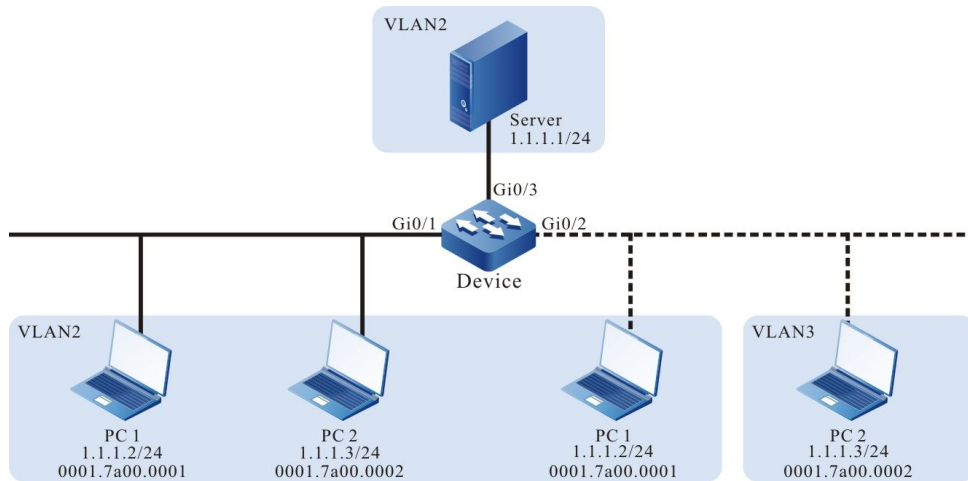


图 23-3 配置基于 MAC 的 VLAN 组网图

配置步骤

- 步骤 1: 在 Device 上配置 VLAN 及端口的链路类型。

在 Device 上创建 VLAN2 和 VLAN3。

```
Device#configure terminal
Device(config)#vlan 2-3
```

#在 Device 上配置端口 gigabitethernet0/1 和 gigabitethernet0/3 的链路类型为 Access，允许 VLAN2 的业务通过。

```
Device(config)#interface gigabitethernet 0/1,0/3
Device(config-if-range)#switchport mode access
Device(config-if-range)#switchport access vlan 2
Device(config-if-range)#exit
```

#在 Device 上配置端口 gigabitethernet0/2 的链路类型为 Hybrid，允许 VLAN2 和 VLAN3 的业务通过，并且 PVID 为 3。

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode hybrid
Device(config-if-gigabitethernet0/2)#switchport hybrid untagged vlan 2-3
Device(config-if-gigabitethernet0/2)#switchport hybrid pvid vlan 3
Device(config-if-gigabitethernet0/2)#exit
```

- 步骤 2: 配置基于 MAC 的 VLAN 功能。

#在 Device 上配置基于 MAC 的 VLAN 表项，使源 MAC 地址为 0001.7a00.0001 的报文在 VLAN2 中转发。

```
Device(config)#mac-vlan mac-address 0001.7a00.0001 vlan 2
```

#在 Device 的端口 gigabitethernet0/2 上使能基于 MAC 的 VLAN 功能。

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#mac-vlan enable
Device(config-if-gigabitethernet0/2)#exit
```

- 步骤 3: 检验结果。

#在 Device 上查看 MAC VLAN 的表项信息和端口的使能情况。

```
Device#show mac-vlan
                total 128,  used 1,  left 127

-----MAC-VLAN-----
NO.  Mac Address  Dynamic Vlan  Static Vlan  Current Pri  Static Pri
-----
1   0001.7a00.0001  0           2           0           0

-----ENABLE MAC-VLAN-----
gi0/2
```

#PC1 从端口 gigabitethernet0/1 或 gigabitethernet0/2 接入时都能访问服务器，PC2 只能从端口 gigabitethernet0/1 上接入时才能访问服务器。

23.3.3 配置基于 IP 子网的 VLAN **-B -S -E -A**

网络需求

- Server1 为办公网服务器，Server2 为生产网服务器。
- 配置基于 IP 子网的 VLAN 功能，使 PC1 只能访问 Server1，PC2 只能访问 Server2。

网络拓扑

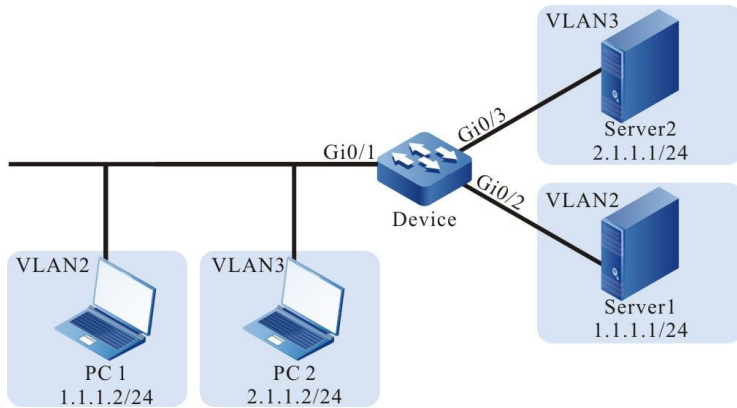


图 23-4 配置基于 IP 子网的 VLAN 组网图

配置步骤

- 步骤 1: 在 Device 上配置 VLAN 及端口的链路类型。

#在 Device 上创建 VLAN2 和 VLAN3。

```
Device#configure terminal
Device(config)#vlan 2-3
```

#在 Device 上配置端口 gigabitethernet0/1 的链路类型为 Hybrid，允许 VLAN2 和 VLAN3 的业务通过，并且 PVID 为 2。

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode hybrid
Device(config-if-gigabitethernet0/1)#switchport hybrid untagged vlan 2-3
Device(config-if-gigabitethernet0/1)#switchport hybrid pvid vlan 2
Device(config-if-gigabitethernet0/1)#exit
```

#在 Device 上配置端口 gigabitethernet0/2 和 gigabitethernet0/3 的链路类型为 Access，gigabitethernet0/2 允许 VLAN2 的业务通过，gigabitethernet0/3 允许 VLAN3 的业务通过。

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode access
Device(config-if-gigabitethernet0/2)#switchport access vlan 2
Device(config)#interface gigabitethernet 0/3
Device(config-if-gigabitethernet0/3)#switchport mode access
Device(config-if-gigabitethernet0/3)#switchport access vlan 3
Device(config-if-gigabitethernet0/3)#exit
```

- 步骤 2: 配置基于 IP 子网的 VLAN 功能。

#在 Device 上配置基于 IP 子网的 VLAN 表项，使源 IP 地址属于 2.1.1.0/24 网段的报文在 VLAN3 中转发。

```
Device(config)#ip-subnet-vlan ipv4 2.1.1.0 mask 255.255.255.0 vlan 3
```

#在 Device 的端口 gigabitethernet0/1 上使能基于 IP 子网的 VLAN 功能。

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#ip-subnet-vlan enable
Device(config-if-gigabitethernet0/1)#exit
```

- 步骤 3: 检验结果。

#在 Device 上查看 IP 子网 VLAN 的表项信息和端口的使能情况。

```
Device(config)#show ip-subnet-vlan
-----IP-SUBNET-VLAN-----
NO.  IP          MASK          VLAN  PRI
-----
1    2.1.1.0      255.255.255.0  3    0
-----
-----Enable SUBNET-VLAN-----
gi0/1
-----Enable SUBNET-VLAN Priority-----
```

#PC1 只能访问 Server1, PC2 只能访问 Server2。

23.3.4 配置基于协议的 VLAN *-B -S -E -A*

网络需求

- PC 为以太网中一台主机, Server1、Server2 为以太网中的两台服务器。
- 配置基于协议的 VLAN 功能, 使 Device 上的端口在未使能基于协议的 VLAN 功能时, PC 只能访问 Server1; 端口使能基于协议的 VLAN 功能时, PC 只能访问 Server2。

网络拓扑

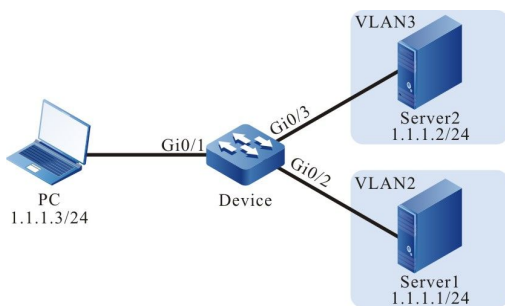


图 23-5 配置基于协议的 VLAN 组网图

配置步骤

- 步骤 1: 在 Device 上配置 VLAN 及端口的链路类型。

#在 Device 上创建 VLAN2 和 VLAN3。

```
Device#configure terminal
Device(config)#vlan 2-3
```

#在 Device 上配置端口 gigabitethernet0/1 链路类型为 Hybrid，允许 VLAN2 和 VLAN3 的业务通过，并且 PVID 为 VLAN 2。

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport hybrid untagged vlan 2-3
Device(config-if-gigabitethernet0/1)#switchport hybrid pvid vlan 2
```

#在 Device 上配置端口 gigabitethernet0/2 和 gigabitethernet0/3 链路类型为 Access，gigabitethernet0/2 允许 VLAN2 的业务通过，gigabitethernet0/3 允许 VLAN3 的业务通过。

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode access
Device(config-if-gigabitethernet0/2)#switchport access vlan 2
Device(config-if-gigabitethernet0/2)#exit
Device(config)#interface gigabitethernet 0/3
Device(config-if-gigabitethernet0/3)#switchport mode access
Device(config-if-gigabitethernet0/3)#switchport access vlan 3
Device(config-if-gigabitethernet0/3)#exit
```

- 步骤 2: 配置基于协议的 VLAN 功能。

#在 Device 上配置基于 ETHERII 封装的 IP(0x0800)报文的协议模版。

```
Device(config)#protocol-vlan profile 1 frame-type ETHERII ether-type 0x0800
```

#在 Device 的端口 gigabitethernet0/1 上应用匹配上述协议模板的报文在 VLAN3 中转发，并使能协议 VLAN 功能。

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#protocol-vlan profile 1 vlan 3
Device(config-if-gigabitethernet0/1)#protocol-vlan enable
Device(config-if-gigabitethernet0/1)#exit
```

- 步骤 3: 检验结果。

#在 Device 上查看协议 VLAN 的表项信息和端口的使能情况。

```
Device#show protocol-vlan profile
-----PROTOCOL-VLAN-TEMPLATE-----
Profile  Frame-type  Ether-type
-----
1        ETHERII    0x800

-----Enable PROTOCOL-VLAN-----
gi0/1

-----Enable PROTOCOL-VLAN Profile-----
gi0/1: total-profiles 1
      vlan 3, profile 1
Device#show protocol-vlan
-----PROTOTOCL-VLAN-----
Interface      Profile      VLAN
-----
gi0/1          1            3

-----Enable PROTOCOL-VLAN-----
gi0/1

-----Enable PROTOCOL-VLAN Profile-----
gi0/1: total-profiles 1
      vlan 3, profile 1
```

#端口 gigabitethernet0/1 未使能基于协议的 VLAN 功能时，PC 只能访问 Server1；端口 gigabitethernet0/1 使能基于协议的 VLAN 功能时，PC 只能访问 Server2。

24 Super-VLAN

24.1 Super-VLAN 简介

不同 VLAN 之间会相互二层隔离，如果想要它们之间能够相互通信，就必须为每个 VLAN 配置 VLAN 接口和 IP 地址，但这种方式会消耗较多本就稀缺的 IP 地址资源。Super-VLAN 又称为 VLAN 聚合，能够有效解决这个问题。普通 VLAN 加入 Super-VLAN 后就成为它的 Sub-VLAN 成员，只要使能

Super-VLAN 的 ARP 代理功能，其 Sub-VLAN 就能共享 Super-VLAN 的 VLAN 接口，以它的 IP 地址作为网关进行三层通信，节省了 IP 地址资源。

24.2 Super-VLAN 功能配置

表 24-1 Super-VLAN 功能配置列表

配置任务	
配置 Super-VLAN	配置 Super-VLAN
配置 Super-VLAN 的 Sub-VLAN 成员	配置 Super-VLAN 的 Sub-VLAN 成员
使能 ARP 代理功能	使能 ARP 代理功能

24.2.1 配置 Super-VLAN **-S -E -A**

配置条件

无

配置 Super-VLAN

Super-VLAN 上可以配置 VLAN 接口，但不能添加端口。创建的 Super-VLAN 不能是已存在的 VLAN、Sub-VLAN。

表 24-2 配置 Super-VLAN

步骤	命令	说明
进入全局配置模式	configure terminal	-
创建 Super-VLAN	super-vlan <i>vlan-id</i>	必选

步骤	命令	说明
		缺省情况下，没有创建 Super-VLAN 创建 Super-VLAN 后会自 动进入 Super-VLAN 配置 模式
配置 Super-VLAN 的描述 信息	description <i>description</i>	可选 缺省情况下， Super- VLAN 的描述信息为 "SuperVLAN <i>vlan- id</i> "，例如 "SuperVLAN0100"

24.2.2 配置 Super-VLAN 的 Sub-VLAN 成员 **-S -E -A**

配置条件

无

配置 Super-VLAN 的 Sub-VLAN 成员

一个 Super-VLAN 最多支持 128 个 Sub-VLAN 成员，一个 VLAN 只能成为一个 Super-VLAN 的 Sub-VLAN 成员。Sub-VLAN 上不能配置 VLAN 接口，但可以添加端口，端口加入 Sub-VLAN 的方式与加入普通 VLAN 的方式相同。Sub-VLAN 的 VLAN ID 不能与已存在的 Super-VLAN 的 VLAN ID 相同。

表 24-3 配置 Super-VLAN 的 Sub-VLAN 成员

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
进入 Super-VLAN 配置模式	super-vlan <i>vlan-id</i>	-
配置 Super-VLAN 的 Sub-VLAN 成员	sub-vlan <i>vlan-list</i>	必选 缺省情况下, Super-VLAN 没有 Sub-VLAN 成员

注意:

- 已配置为 Sub-VLAN 则不可以配置为独占类型的 EIPS 控制 vlan。

24.2.3 使能 ARP 代理功能 **-S -E -A**

配置条件

在使能 ARP 代理功能前, 首先完成以下任务:

- 配置 Super-VLAN 对应的 VLAN 接口及 IP 地址。

配置 ARP 代理功能

使能 Super-VLAN 的 ARP 代理功能后, Sub-VLAN 之间能够通过 ARP 代理实现三层互通。

表 24-4 使能 ARP 代理功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 Super-VLAN 配置模式	super-vlan <i>vlan-id</i>	-

步骤	命令	说明
使能 ARP 代理功能	arp proxy enable	必选 缺省情况下，未使能 ARP 代理功能

说明：

- ARP 代理功能依赖于三层转发功能，如果设备不支持三层转发功能，则 ARP 代理功能不生效。

24.2.4 Super-VLAN 监控与维护 **-S -E -A**

表 24-5 Super-VLAN 监控与维护

命令	说明
show super-vlan [<i>vlan-id</i>]	显示指定的 Super-VLAN 信息

24.3 Super-VLAN 典型配置举例

24.3.1 配置 Super-VLAN **-S -E -A**

网络需求

- PC1 和 PC2 为 Sub-VLAN2 内的两台主机，PC3 为 Sub-VLAN3 内的主机，Server 为 VLAN5 内的服务器。

- 在 Device 上配置 Super-VLAN 功能，实现 PC1、PC2 之间能够二层互通，PC1、PC2 和 PC3 之间能够三层互通，且均能访问服务器。

网络拓扑

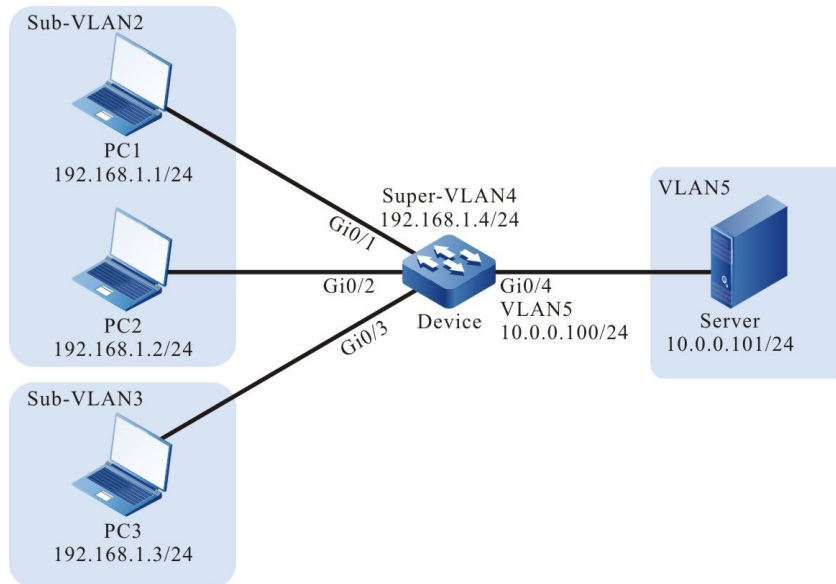


图 24-1 配置 Super-VLAN 组网图

配置步骤

步骤 1： 在 Device 上配置 VLAN 及端口的链路类型。

#在 Device 上创建 VLAN 2,VLAN3,VLAN5。

```
Device#configure terminal
Device(config)#vlan 2-3,5
```

#在 Device 上配置 VLAN 接口 4 的 IP 地址为 192.168.1.4，掩码为 255.255.255.0，VLAN 接口 5 的 IP 地址为 10.0.0.100，掩码为 255.255.255.0。

```
Device(config)#interface vlan 4
Device(config-if-vlan4)#ip address 192.168.1.4 255.255.255.0
Device(config-if-vlan4)#exit
Device(config)#interface vlan 5
Device(config-if-vlan5)#ip address 10.0.0.100 255.255.255.0
Device(config-if-vlan5)#exit
```

#配置 Device 端口 gigabitethernet0/1~gigabitethernet0/2 的链路类型为 Access，并允许 VLAN2 的业务通过。

```
Device(config)#interface gigabitethernet 0/1,0/2
Device(config-if-range)#switchport mode access
Device(config-if-range)#switchport access vlan 2
```

```
Device(config-if-range)#exit
```

#配置 Device 端口 gigabitethernet0/3 的链路类型为 Access，并允许 VLAN3 的业务通过。

```
Device(config)#interface gigabitethernet 0/3
Device(config-if-gigabitethernet0/3)#switchport mode access
Device(config-if-gigabitethernet0/3)#switchport access vlan 3
Device(config-if-gigabitethernet0/3)#exit
```

#配置 Device 端口 gigabitethernet0/4 的链路类型为 Access，并允许 VLAN5 的业务通过。

```
Device(config)#interface gigabitethernet 0/4
Device(config-if-gigabitethernet0/4)#switchport mode access
Device(config-if-gigabitethernet0/4)#switchport access vlan 5
Device(config-if-gigabitethernet0/4)#exit
```

#查看 Device 的 VLAN 及端口信息。

```
Device#show vlan 2
-----
NO. VID VLAN-Name          Owner Mode  Interface
-----
1  2  VLAN0002                static Untagged gi0/1 gi0/2
Device#show vlan 3
-----
NO. VID VLAN-Name          Owner Mode  Interface
-----
1  3  VLAN0003                static Untagged gi0/3
Device#show vlan 5
-----
NO. VID VLAN-Name          Owner Mode  Interface
-----
1  5  VLAN0005                static Untagged gi0/4
```

步骤 2: 在 Device 上配置 Super-VLAN 功能。

#在 Device 上配置 VLAN4 为 Super-VLAN,VLAN2 和 VLAN3 为 Sub-VLAN，并使能 ARP 代理。

```
Device(config)#super-vlan 4
Device(config-super-vlan4)#sub-vlan 2,3
Device(config-super-vlan4)#arp proxy enable
Device(config-super-vlan4)#exit
```

#查看 Device 上的 Super-VLAN 信息。

```
Device#show super-vlan
-----
NO. SuperVlan Description          Arp Proxy SubVlan Member
-----
1  4  SuperVLAN0004        enable  2-3
```

说明:

- 实现不同 Sub-VLAN 内的主机之间三层互通，必须开启 ARP 代理功能。
 - Super-VLAN 与 Sub-VLAN 必须在同一个生成树实例中。
-

步骤 3: 检验结果，用 ping 命令验证 PC1、PC2、PC3 和服务器之间的连通性。

#Sub-VLAN2 内的两台主机 PC1、PC2 之间可以互相 ping 通。

#Sub-VLAN2 内的主机 PC1、PC2 与 Sub-VLAN3 的主机 PC3 之间可以互相 ping 通。

#Sub-VLAN 内的主机 PC1、PC2 和 PC3 均能与服务器互相 ping 通。

25 Voice-VLAN

25.1 Voice-VLAN 简介

Voice-VLAN 是为语音数据流提供安全和 QOS 保障的一种机制，网络中通常同时存在语音数据和业务数据两种流量，语音数据在传输时需要具有比业务数据更高的优先级，以减少传输过程中可能产生的时延和丢包现象。Voice-VLAN 能够自动识别出语音流量，将其分发到具有 QOS 保障的特定 VLAN 中传输。

25.2 Voice-VLAN 功能配置

表 6-1 Voice-VLAN 功能配置列表

配置任务	
配置 Voice-VLAN	配置 Voice-VLAN
配置 OUI 地址	配置 OUI 地址
使能端口的 Voice-VLAN 功能	使能端口的 Voice-VLAN 功能
配置端口的 Voice-VLAN 工作模式	配置 Voice-VLAN 自动模式
	配置 Voice-VLAN 手动模式
使能 Voice-VLAN 的安全模式	使能 Voice-VLAN 的安全模式
使能 Voice-VLAN 的 Ildp-med 认证模式	使能 Voice-VLAN 的 Ildp-med 认证模式

25.2.1 配置 Voice-VLAN *-B -S -E -A*

Voice-VLAN 用于传输语音报文。被识别为语音报文的 802.1p 优先级将被替换为 Voice-VLAN 对应的优先级，划分到 Voice-VLAN 中转发。设备最多支持一个 Voice-VLAN。

配置条件

在配置 Voice-VLAN 前，首先完成以下任务：

- 创建指定为 Voice-VLAN 的 VLAN。

配置 Voice-VLAN

表 6-2 配置 Voice-VLAN

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置指定 VLAN 为 Voice-VLAN	voice vlan <i>vlan-id</i> cos <i>priority</i>	必选 缺省情况下，没有配置 Voice-VLAN，即未全局使能 Voice-VLAN 功能

25.2.2 配置 OUI 地址

-B -S -E -A

配置条件

在配置 OUI 地址前，首先完成以下任务：

- 全局使能 Voice-VLAN 功能；
- 端口使能 Voice-VLAN 功能。

配置 OUI 地址

OUI (Organizationally Unique Identifier, 全球统一标识符) 用来标识各厂商的语音设备发送的语音报文。工作在 Voice-VLAN 自动模式下的端口收到 Untag 报文后，将取出其源 MAC 地址和 OUI 的掩码相与，得到的地址范围如果和 OUI 地址相同，则匹配了该 OUI 地址，该报文被识别为语音报文。

表 6-3 配置 OUI 地址

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
配置 OUI 地址	voice vlan oui-mac <i>oui-mac-address mask</i> mask name <i>oui-name</i>	必选 缺省情况下，有 5 个缺省 OUI 地址 设备最多支持 32 个 OUI 地址

25.2.3 使能端口的 Voice-VLAN 功能

-B -S -E -A

端口使能 Voice-VLAN 功能后，会根据端口的 Voice-VLAN 工作模式，采用相应的方式对收到的报文进行自动识别。

配置条件

在使能端口的 Voice-VLAN 功能前，首先要完成以下任务：

- 全局使能 Voice-VLAN 功能；
- 配置端口加入 Voice-VLAN。

使能端口的 Voice-VLAN 功能

表 6-4 使能端口的 Voice-VLAN 功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface <i>interface-name</i>	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	

步骤	命令	说明
		置模式后，后续配置只在汇聚组生效
使能端口的 Voice-VLAN 功能	voice vlan enable	必选 缺省情况下，端口未使能 Voice-VLAN 功能

说明：

- Voice-VLAN 的安全模式不支持汇聚组，即当设备使能了 Voice-VLAN 的安全模式后，则汇聚组无法使能 Voice-VLAN 功能；或者当设备有汇聚组使能了 Voice-VLAN 功能，则无法使能 Voice-VLAN 的安全模式。
- Voice-VLAN 的 Ildp-med 认证模式不支持汇聚组，即当设备使能了 Voice-VLAN 的 Ildp-med 认证模式后，则汇聚组无法使能 Voice-VLAN 功能；或者当设备有汇聚组使能了 Voice-VLAN 功能，则无法使能 Voice-VLAN 的 Ildp-med 认证模式。

25.2.4 配置端口的 Voice-VLAN 工作模式

-B -S -E -A

端口的 Voice-VLAN 工作模式分为自动模式和手动模式两种类型，工作在不同 Voice-VLAN 模式下的端口识别语音报文的方式不同：

- 自动模式：端口收到的是 Untag 报文或 VLAN ID 为 Voice-VLAN ID 的 Tag 报文，且报文源 MAC 地址与某个 OUI 地址匹配，则认为是语音报文；
- 手动模式：端口收到的报文都认为是语音报文。

配置条件

在配置端口的 Voice-VLAN 工作模式前，首先要完成以下任务：

- 全局使能 Voice-VLAN 功能；
- 使能端口的 Voice-VLAN 功能。

配置 Voice-VLAN 自动模式

表 6-5 配置 Voice-VLAN 自动模式

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface <i>interface-name</i>	必选其一 进入二层以太接口配置模式后, 后续配置只在当前端口生效; 进入汇聚组配置模式后, 后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	
配置端口工作在 Voice-VLAN 自动模式	voice vlan mode auto	必选 缺省情况下, 端口工作在 Voice-VLAN 自动模式

配置 Voice-VLAN 手动模式

表 6-6 配置 Voice-VLAN 手动模式

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface <i>interface-name</i>	必选其一 进入二层以太接口配置模式后, 后续配置只在当前端口生效; 进入汇聚组配置模式后, 后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	

步骤	命令	说明
配置端口工作在 Voice-VLAN 手动模式	no voice vlan mode auto	必选 缺省情况下，端口工作在 Voice-VLAN 自动模式

说明：

- 如果端口用于传输 Tagged 语音数据，则端口类型只能配置为 Trunk 或 Hybrid，且 PVID 不能为 Voice-VLAN。
- 如果端口工作在 Voice-VLAN 手工模式，且用于传输 untagged 语音数据，则 PVID 必须为 Voice-VLAN。
- Voice-VLAN 的 Ildp-med 认证模式不支持端口的手动模式，即当设备使能了 Voice-VLAN 的 Ildp-med 认证模式后，则端口无法配置为 Voice-VLAN 的手动模式；或者当有端口配置为 Voice-VLAN 的手动模式，则无法使能 Voice-VLAN 的 Ildp-med 认证模式。

25.2.5 使能 Voice-VLAN 的安全模式

-B -S -E -A

使能 Voice-VLAN 的安全模式后，设备将对每一个要进入 Voice-VLAN 传输的报文进行源 MAC 地址匹配检查，对于不能匹配 OUI 地址的报文，则将其丢弃。

配置条件

在使能 Voice-VLAN 的安全模式前，首先要完成以下任务：

- 全局使能 Voice-VLAN 功能；

使能 Voice-VLAN 的安全模式

表 6-7 使能 Voice-VLAN 的安全模式

步骤	命令	说明
进入全局配置模式	configure terminal	-
使能 Voice-VLAN 的安全模式	voice vlan security enable	必选 缺省情况下，未使能 Voice-VLAN 的安全模式

说明：

- Voice-VLAN 的安全模式不支持汇聚组，即当设备有汇聚组使能了 Voice-VLAN 功能，则无法使能 Voice-VLAN 的安全模式；或者当设备使能了 Voice-VLAN 的安全模式后，则汇聚组无法使能 Voice-VLAN 功能。

25.2.6 使能 Voice-VLAN 的 Ildp-med 认证模式

-B -S -E -A

使能 Voice-VLAN 的 Ildp-med 认证模式后，设备将用户配置的 OUI 或默认 OUI 作为认证白名单，对 Ildp-med 通告的语音设备源 MAC 地址进行匹配检查，能匹配白名单的语音设备发出的语音报文才能进入 Voice-VLAN 进行传输。

配置条件

在使能 Voice-VLAN 的 Ildp-med 认证模式前，首先要完成以下任务：

- 全局使能 Voice-VLAN 功能；

使能 Voice-VLAN 的 Ildp-med 认证模式

表 6-8 使能 Voice-VLAN 的 Ildp-med 认证模式

步骤	命令	说明
进入全局配置模式	configure terminal	-
使能 Voice-VLAN 的 Ildp-med 认证模式	voice vlan Ildp-med authentication	必选 缺省情况下, 未使能 Voice-VLAN 的 Ildp-med 认证模式

说明:

- Voice-VLAN 的 Ildp-med 认证模式不支持汇聚组, 即当设备有汇聚组使能了 Voice-VLAN 功能, 则无法使能 Voice-VLAN 的 Ildp-med 认证模式; 或者当设备使能了 Voice-VLAN 的 Ildp-med 认证模式后, 则汇聚组无法使能 Voice-VLAN 功能。
- Voice-VLAN 的 Ildp-med 认证模式不支持端口的手动模式, 即当有端口配置为 Voice-VLAN 的手动模式, 则无法使能 Voice-VLAN 的 Ildp-med 认证模式; 或者当设备使能了 Voice-VLAN 的 Ildp-med 认证模式后, 则端口无法配置为 Voice-VLAN 的手动模式。

25.2.7 Voice-VLAN 监控与维护

-B -S -E -A

表 6-9 Voice-VLAN 监控与维护

命令	说明
show voice vlan { all interface [<i>interface-name</i>] link-aggregation [<i>link-aggregation-id</i>] oui Ildp-med authenticated-mac }	显示 Voice-VLAN 信息

25.3 Voice-VLAN 典型配置举例

25.3.1 配置 Voice-VLAN 手动模式

-B -S -E -A

网络需求

- IP Phone 和 PC 通过 Device 接入 IP Network。
- 在 Device 上配置 Voice-VLAN 手动模式，实现在网络通畅的情况下，IP Phone 和 PC 都可以正常访问 IP Network；在网络拥塞的情况下，IP Phone 优先于 PC 访问 IP Network。

网络拓扑

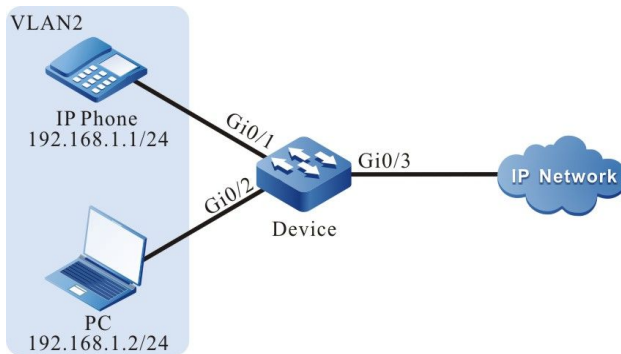


图 6-1 配置 Voice-VLAN 手动模式组网图

配置步骤

步骤 1： 配置 VLAN 和端口的链路类型。

#在 Device 上创建 VLAN2。

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#在 Device 上配置端口 gigabitethernet0/1 和 gigabitethernet0/2 的链路类型为 Access，允许 VLAN2 的业务通过。

```
Device(config)#interface gigabitethernet 0/1,0/2
Device(config-if-range)#switchport mode access
```

```
Device(config-if-range)#switchport access vlan 2
Device(config-if-range)#exit
```

#在 Device 上配置端口 gigabitethernet0/3 的链路类型为 Trunk，允许 VLAN2 的业务通过。

```
Device(config)#interface gigabitethernet 0/3
Device(config-if-gigabitethernet0/3)#switchport mode trunk
Device(config-if-gigabitethernet0/3)#switchport trunk allowed vlan add 2
Device(config-if-gigabitethernet0/3)#exit
```

步骤 2： 配置 Voice-VLAN 功能。

#在 Device 上配置 VLAN2 为 Voice-VLAN，Cos 值为 7。

```
Device(config)#voice vlan 2 cos 7
```

#在 Device 的端口 gigabitethernet0/1 上配置 Voice-VLAN 手动模式。

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#voice vlan enable
Device(config-if-gigabitethernet0/1)#no voice vlan mode auto
Device(config-if-gigabitethernet0/1)#exit
```

#在 Device 上查看 Voice-VLAN 信息。

```
Device#show voice vlan all
Voice Vlan Global Information: Voice Vlan enable
Voice Vlan security: disable
Voice Vlan lldp-med authentication: disable
Voice Vlan VID: 2, Cos: 7
Default OUI number: 5
User config OUI number: 0

Voice vlan interface information:
Interface      Mode
-----
gi0/1          Manual-Mode

Voice Vlan OUI information: Total: 5
MacAddr      Mask      Name
-----
0003.6b00.0000 ffff.ff00.0000 Cisco-phone default
006b.e200.0000 ffff.ff00.0000 H3C-Aolynk-phone default
00d0.1e00.0000 ffff.ff00.0000 Pingtel-phone default
00e0.7500.0000 ffff.ff00.0000 Polycom-phone default
00e0.bb00.0000 ffff.ff00.0000 3Com-phone default
```

步骤 3： 检验结果。

#IP Phone 发往 IP Network 的报文 802.1P 优先级被修改为 7，PC 发往 IP Network 的报文 802.1P 优先级不会被修改。

#在网络通畅的情况下，IP Phone 和 PC 都可以正常访问 IP Network。

#在网络拥塞的情况下，IP Phone 可以优先于 PC 访问 IP Network。

25.3.2 配置 Voice-VLAN 自动模式

-B -S -E -A

网络需求

- IP Phone 和 PC 通过 Device 的端口 gigabitethernet0/1 接入 IP Network，IP Phone 的 MAC 地址为 0001.0001.0001，PC 的 MAC 地址为 0002.0002.0002。
- 在 Device 上配置 Voice-VLAN 自动模式，实现在网络通畅的情况下，IP Phone 和 PC 都可以正常访问 IP Network，在网络拥塞的情况下，IP Phone 优先于 PC 访问 IP Network。

网络拓扑

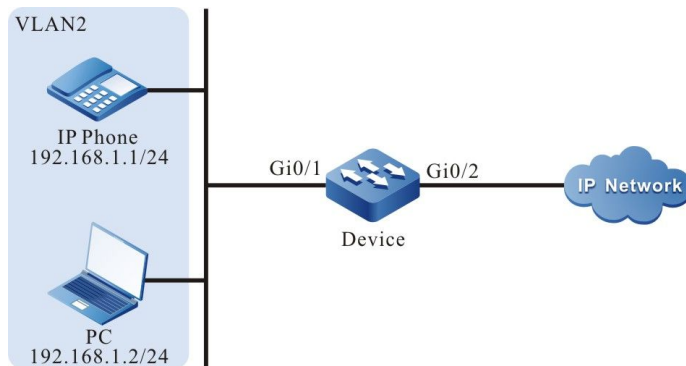


图 6-2 配置 Voice-VLAN 自动模式组网图

配置步骤

步骤 1： 配置 VLAN 和端口的链路类型。

#在 Device 上创建 VLAN2。

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#在 Device 上配置端口 gigabitethernet0/1 的链路类型为 Trunk，允许 VLAN2 的业务通过。

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)# switchport mode trunk
Device(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2
```



```
Device(config-if-gigabitethernet0/1)#exit
```

#在 Device 上配置端口 gigabitethernet0/2 的链路类型为 Trunk，允许 VLAN2 的业务通过。

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode trunk
Device(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 2
Device(config-if-gigabitethernet0/2)#exit
```

步骤 2: 配置 Voice-VLAN 功能。

#在 Device 上配置 VLAN2 为 Voice-VLAN，且对应的 Cos 值修改为 7。

```
Device(config)#voice vlan 2 cos 7
```

#在 Device 的端口 gigabitethernet0/1 上配置 Voice-VLAN 自动模式。

```
Device(config)# interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#voice vlan enable
Device(config-if-gigabitethernet0/1)#voice vlan mode auto
Device(config-if-gigabitethernet0/1)#exit
```

#在 Device 上配置 IP Phone 的 MAC 地址 0001.0001.0001 对应的 OUI 地址。

```
Device(config)#voice vlan oui-mac 0001.0001.0001 mask ffff.ffff.0000 name voice-vlan
```

#在 Device 上查看 Voice-VLAN 信息。

```
Device#show voice vlan all
Voice Vlan Global Information: Voice Vlan enable
Voice Vlan security: disable
Voice Vlan lldp-med authentication: disable
Voice Vlan VID: 2, Cos: 7
Default OUI number: 5
User config OUI number: 1

Voice vlan interface information:
Interface      Mode
-----
gi0/1          Auto-Mode

Voice Vlan OUI information: Total: 6
MacAddr      Mask      Name
-----
0001.0001.0000 ffff.ffff.0000 voice-vlan
0003.6b00.0000 ffff.ff00.0000 Cisco-phone default
006b.e200.0000 ffff.ff00.0000 H3C-Aolynk-phone default
00d0.1e00.0000 ffff.ff00.0000 Pingtel-phone default
00e0.7500.0000 ffff.ff00.0000 Polycom-phone default
00e0.bb00.0000 ffff.ff00.0000 3Com-phone default
```

步骤 3: 检验结果。

#IP Phone 发往 IP Network 的报文 802.1P 优先级被修改为 7, PC 发往 IP Network 的报文 802.1P 优先级不会被修改。

#在网络通畅的情况下, IP Phone 和 PC 都可以正常访问 IP Network。

#在网络拥塞的情况下, IP Phone 可以优先于 PC 访问 IP Network。

25.3.3 配置 Voice-VLAN 安全模式

-B -S -E -A

网络需求

- IP Phone 和 PC 通过 Device 的端口 gigabitethernet0/1 接入 IP Network, IP Phone 的 MAC 地址为 0001.0001.0001, PC 的 MAC 地址为 0002.0002.0002。
- 在 Device 上配置 Voice-VLAN 安全模式, 实现 IP Phone 可以正常访问 IP Network, PC 不能访问 IP Network。

网络拓扑

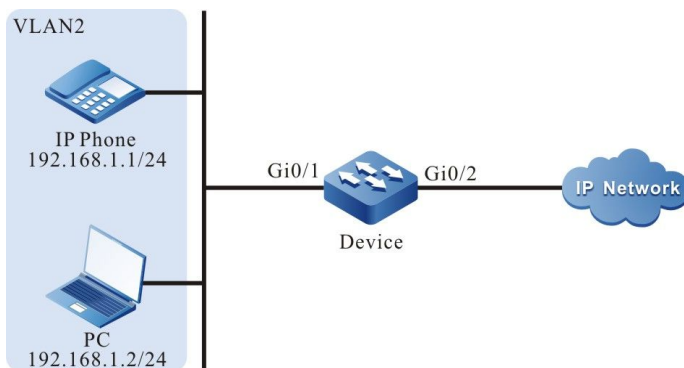


图 6-3 配置 Voice-VLAN 安全模式组网图

配置步骤

步骤 1: 配置 VLAN 和端口的链路类型。

#在 Device 上创建 VLAN2。

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#在 Device 上配置端口 gigabitethernet0/1 的链路类型为 trunk，允许 VLAN2 的业务通过。

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode trunk
Device(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2
Device(config-if-gigabitethernet0/1)#exit
```

#在 Device 上配置端口 gigabitethernet0/2 的链路类型为 Trunk，允许 VLAN2 的业务通过。

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode trunk
Device(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 2
Device(config-if-gigabitethernet0/2)#exit
```

步骤 2: 配置 Voice-VLAN 功能。

#在 Device 上配置 VLAN2 为 Voice-VLAN，且对应的 Cos 值修改为 7。

```
Device(config)#voice vlan 2 cos 7
```

#在 Device 上配置全局使能 Voice-VLAN 安全模式。

```
Device(config)# voice vlan security enable
```

#在 Device 的端口 gigabitethernet0/1 上配置 Voice-VLAN 自动模式。

```
Device(config)# interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#voice vlan enable
Device(config-if-gigabitethernet0/1)#voice vlan mode auto
Device(config-if-gigabitethernet0/1)#exit
```

#在 Device 上配置 IP Phone 的 MAC 地址 0001.0001.0001 对应的 OUI 地址。

```
Device(config)#voice vlan oui-mac 0001.0001.0001 mask ffff.ffff.0000 name voice-vlan
```

#在 Device 上查看 Voice-VLAN 信息。

```
Device#show voice vlan all
Voice Vlan Global Information: Voice Vlan enable
Voice Vlan security: enable
Voice Vlan lldp-med authentication: disable
Voice Vlan VID: 2, Cos: 7
Default OUI number: 5
User config OUI number: 1

Voice vlan interface information:
Interface      Mode
-----
gi0/1          Auto-Mode

Voice Vlan OUI information: Total: 6
MacAddr      Mask      Name
-----
0001.0001.0000 ffff.ffff.0000 voice-vlan
0003.6b00.0000 ffff.ff00.0000 Cisco-phone default
006b.e200.0000 ffff.ff00.0000 H3C-Aolynk-phone default
00d0.1e00.0000 ffff.ff00.0000 Pingtel-phone default
00e0.7500.0000 ffff.ff00.0000 Polycom-phone default
00e0.bb00.0000 ffff.ff00.0000 3Com-phone default
```

步骤 3: 检验结果。

#IP Phone 发往 IP Network 的报文 802.1P 优先级被修改为 7。

#PC 不可以访问 IP Network。

25.3.4 配置 Voice-VLAN lldp-med 认证模式 *-B -S -E -A*

网络需求

- IP Phone(该 IP Phone 可发送携带语音字段的 LLDP 报文)和 PC 通过 Device 的端口 gigabitethernet0/1 接入 IP Network, IP Phone 的 MAC 地址为 0001.0001.0001, PC 的 MAC 地址为 0002.0002.0002。
- 在 Device 上配置 Voice-VLAN lldp-med 认证模式, 实现 IP Phone 可以正常访问 IP Network, PC 不能访问 IP Network。

网络拓扑

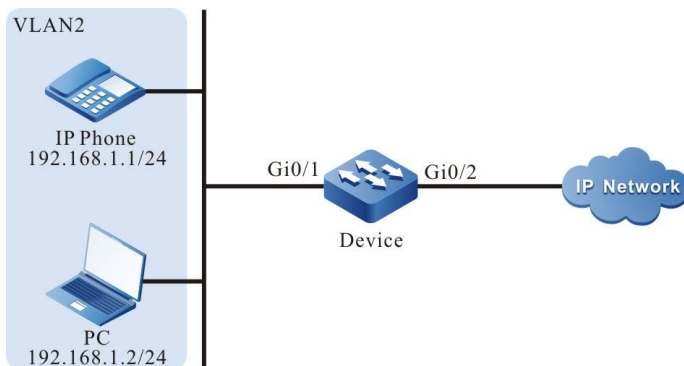


图 6-4 配置 Voice-VLAN lldp-med 认证模式组网图

配置步骤

步骤 1: 配置 VLAN 和端口的链路类型。

#在 Device 上创建 VLAN2。

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#在 Device 上配置端口 gigabitethernet0/1 的链路类型为 trunk，允许 VLAN2 的业务通过。

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode trunk
Device(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2
Device(config-if-gigabitethernet0/1)#exit
```

#在 Device 上配置端口 gigabitethernet0/2 的链路类型为 Trunk，允许 VLAN2 的业务通过。

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode trunk
Device(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 2
Device(config-if-gigabitethernet0/2)#exit
```

步骤 2: 配置 Voice-VLAN 功能。

#在 Device 上配置 VLAN2 为 Voice-VLAN，且对应的 Cos 值修改为 7。

```
Device(config)#voice vlan 2 cos 7
```

#在 Device 上配置全局使能 Voice-VLAN lldp-med 认证模式。

```
Device(config)#voice vlan lldp-med authentication
```

#在 Device 的端口 gigabitethernet0/1 上配置 Voice-VLAN 自动模式。

```
Device(config)# interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#voice vlan enable
Device(config-if-gigabitethernet0/1)#voice vlan mode auto
Device(config-if-gigabitethernet0/1)#exit
```

#在 Device 上配置 IP Phone 的 MAC 地址 0001.0001.0001 对应的 OUI 地址。

```
Device(config)#voice vlan oui-mac 0001.0001.0001 mask ffff.ffff.0000 name voice-vlan
```

#在 Device 上查看 Voice-VLAN 信息。

```
Device#show voice vlan all
Voice Vlan Global Information: Voice Vlan enable
Voice Vlan security: disable
Voice Vlan lldp-med authentication: enable
Voice Vlan VID: 2, Cos: 7
Default OUI number: 5
User config OUI number: 1

Voice vlan interface information:
Interface      Mode
-----
gi0/1          Auto-Mode

Voice Vlan OUI information: Total: 6
MacAddr      Mask      Name
-----
0001.0001.0000 ffff.ffff.0000 voice-vlan
0003.6b00.0000 ffff.ff00.0000 Cisco-phone default
006b.e200.0000 ffff.ff00.0000 H3C-Aolynk-phone default
00d0.1e00.0000 ffff.ff00.0000 Pingtel-phone default
00e0.7500.0000 ffff.ff00.0000 Polycom-phone default
00e0.bb00.0000 ffff.ff00.0000 3Com-phone default
```

```
Voice Vlan Ildp-med authenticated mac information:
MacAddr      Interface
-----
0001.0001.0001  gi0/1
```

步骤 3: 检验结果。

#IP Phone 发往 IP Network 的报文 802.1P 优先级被修改为 7。

#PC 不可以访问 IP Network。

26 MAC 地址表管理

26.1 MAC 地址管理简介

MAC 地址表项由终端的 MAC 地址、与终端相连的设备端口及该端口所属 VLAN ID 组成。设备接收到数据报文时，会将报文的目地 MAC 地址与设备中保存的 MAC 地址表项进行匹配，用来快速定位报文的转发端口。

MAC 地址可以分为两类，动态 MAC 地址和静态 MAC 地址。静态 MAC 地址又分为静态转发 MAC 地址和静态过滤 MAC 地址。

动态 MAC 地址学习是设备最基本的 MAC 地址学习方式。每一个动态 MAC 地址表项都存在一个老化时间，若在老化时间到期时，在相应 VLAN 和端口下仍然没有接收到源 MAC 地址与 MAC 地址表项匹配的报文，则设备会将这条 MAC 地址表项删除。

动态 MAC 地址学习/转发过程：

- 当设备接收到报文时，在相应的 VLAN 中查找 MAC 地址表是否有匹配报文的源 MAC 地址表项，如果没有相应的匹配表项，则将报文的源 MAC 地址写入 MAC 地址表，并开启这条新增表项的老化时间定时器，如果查找到匹配的 MAC 地址表项，则更新此 MAC 地址表项的老化时间；
- 在相应的 VLAN 中，查找 MAC 地址表是否存在匹配报文的目的 MAC 地址表项，如果没有相应的匹配表项，则报文会向相同 VLAN ID 里的其它端口洪泛，如果查找到匹配目的 MAC 地址表项，则从指定端口转发报文。

静态过滤 MAC 地址用于隔离带有攻击性质的设备，阻止其与外界设备进行通信。

静态过滤 MAC 地址的配置/转发过程：

- 静态过滤 MAC 地址只能由用户配置；
- 若报文的源 MAC 地址或目的 MAC 地址在相应的 VLAN 中匹配到静态过滤 MAC 地址表项，则报文被丢弃。

静态转发 MAC 地址用于控制报文的选路原则，同时防止 MAC 地址表项在设备中出现频繁 MAC 地址迁移现象。MAC 地址迁移是指：设备从端口 A 学习到某 MAC 地址，又从端口 B 接收到了以此 MAC 地址为源 MAC 地址的报文，且端口 B 与端口 A 属于相同的 VLAN，此时 MAC 地址表项保存的转发端口从端口 A 更新到端口 B。

静态转发 MAC 地址的配置/转发过程：

- 静态转发 MAC 地址由用户配置；
- 若报文的目的 MAC 地址在相应的 VLAN 中匹配到了静态 MAC 地址表项，则报文从指定端口转发。

同一个端口在不同 VLAN 中可以学习到相同的 MAC 地址，同一个 MAC 地址在同一个 VLAN 中只能被一个端口学习。

26.2 MAC 地址管理功能配置

表 26-1 MAC 地址管理功能配置列表

配置任务	
配置 MAC 地址管理属性	配置 MAC 地址老化时间
	配置 MAC 地址学习能力
配置 MAC 地址学习限制	配置基于端口的动态 MAC 地址学习限制
	配置基于 VLAN 的动态 MAC 地址学习限制
	配置基于系统的动态 MAC 地址学习限制
配置静态 MAC 地址	配置静态过滤 MAC 地址
	配置绑定在端口下的静态转发 MAC 地址
	配置绑定在汇聚组下的静态转发 MAC 地址

26.2.1 配置 MAC 地址管理属性

-B -S -E -A

MAC 地址管理属性包含：配置 MAC 地址的老化时间和配置端口的 MAC 地址学习能力。

动态 MAC 地址表项存在一个老化时间，若在老化时间到期时，在指定的 VLAN 中仍然没有接收到源 MAC 地址与 MAC 地址表项匹配的报文，则该 MAC 地址表项将会被删除。若指定的 VLAN 中接收到源 MAC 地址与 MAC 地址表项匹配的报文，则重置相应表项的老化时间。

静态 MAC 地址只能由用户配置、删除，静态 MAC 地址不会被老化。

在网络中如果设备有闲置端口并且该端口是不允许随意使用，可以在端口上配置关闭 MAC 地址学习能力，使端口接收的报文全部被丢弃，来限制指定端口接入网络，提高网络的安全性。

配置条件

无

配置 MAC 地址老化时间

设备中设置的动态 MAC 地址老化时间全局生效，MAC 地址老化时间取值范围如下：

- 0 设置 MAC 地址不老化，即学习到的动态 MAC 地址不会老化；
- 60~1000000 设置动态 MAC 地址老化时间，单位为秒，缺省值为 300。

配置老化时间过长时，设备中的 MAC 地址表中可能存在大量不再使用的 MAC 地址表项，造成无效表项过多，会将 MAC 地址表资源耗尽，使设备无法新增有效 MAC 地址表项；配置老化时间过短时，设备会频繁删除有效 MAC 地址表项，影响设备转发性能；所以老化时间要根据实际环境配置一个相对合理的值。

表 26-2 配置 MAC 地址老化时间

步骤	命令	说明
进入全局配置模式	config terminal	-
配置 MAC 地址老化时间	mac-address aging-time <i>aging-time-value</i>	必选 缺省情况下，MAC 地址老化时间为 300 秒

配置 MAC 地址学习能力

开启/关闭 MAC 地址学习能力仅对学习动态 MAC 地址有效。缺省情况下，端口下开启 MAC 地址学习能力，此时该端口正常学习到 MAC 地址表项并转发相应报文；若端口下关闭 MAC 地址学习能力，此时该端口不再学习动态 MAC 地址且接收的报文会被丢弃。

表 26-3 配置 MAC 地址学习能力

步骤	命令	说明
进入全局配置模式	config terminal	-
进入二层以太接口配置模式	interface <i>interface-name</i>	必选其一

步骤	命令	说明
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	进入二层以太接口配置模式后, 后续配置只在当前端口生效; 进入汇聚组配置模式后, 后续配置只在汇聚组生效
使能端口或者汇聚组 MAC 地址学习能力	mac-address learning	必选 缺省情况下, 端口开启 MAC 地址学习能力

配置 MAC 地址学习功能

开启/关闭 MAC 地址学习功能对学习动态 MAC 地址和转发报文有效。缺省情况下, 端口下开启 MAC 地址学习功能, 此时该端口可以学习到 MAC 地址表项, 并转发报文; 若端口下关闭 MAC 地址学习功能, 此时该端口不再学习动态 MAC 地址, 但是仍然可以转发报文。

表 26-4 配置 MAC 地址学习功能

步骤	命令	说明
进入全局配置模式	config terminal	-
进入二层以太接口配置模式	interface <i>interface-name</i>	必选其一 进入二层以太接口配置模式后, 后续配置只在当前端口生效; 进入汇聚组配置模式后, 后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	
使能端口或者汇聚组 MAC 地址学习功能	mac-address learning action forward	必选

步骤	命令	说明
		缺省情况下，端口开启 MAC 地址学习功能

26.2.2 配置 MAC 地址学习限制

-B -S -E -A

MAC 地址学习限制可以分为 3 类：基于端口的动态 MAC 地址学习限制、基于 VLAN 的动态 MAC 地址学习限制和基于系统的动态 MAC 地址学习限制。

设备中学习到的动态 MAC 地址表项越多，报文转发查找 MAC 地址表的时间越长，可能导致设备性能下降。可在设备中配置动态 MAC 地址学习能力限制，从而提高设备性能，在相应端口下或相应 VLAN 中配置动态 MAC 地址学习能力限制，可以控制终端接入的数量。

配置条件

无

配置基于端口的动态 MAC 地址学习限制

指定端口下学习到的 MAC 地址表项已经达到上限值后，此端口接收到源 MAC 地址不在 MAC 地址转发表里的报文将被丢弃。

表 26-5 配置基于端口的动态 MAC 地址学习限制

步骤	命令	说明
进入全局配置模式	config terminal	-
进入二层以太接口配置模式	interface interface-name	必选其一
进入汇聚组配置模式	link-aggregation link-aggregation-id	进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效

步骤	命令	说明
配置基于端口的动态 MAC 地址学习限制	mac-address max-mac-count <i>max-mac-count-value</i>	必选 缺省情况下，端口下动态 MAC 地址学习不受限制 配置学习动态 MAC 地址上限值的取值范围为 1~硬件芯片支持的允许学习的最大地址表项条数

说明：

- 配置基于端口的动态 MAC 地址学习限制时，若配置的限制小于当前端口下已经存在的动态 MAC 地址条数，设备会提示用户需要手动清除已存在的动态 MAC 地址表项。手动清除后，配置即时生效。

配置基于 VLAN 的动态 MAC 地址学习限制

指定 VLAN 中学习到的 MAC 地址表项已经达到上限值后，此 VLAN 中接收到源 MAC 地址不在 MAC 地址转发表里的报文将被丢弃。

表 26-6 配置基于 VLAN 的动态 MAC 地址学习限制

步骤	命令	说明
进入全局配置模式	config terminal	-
配置基于 VLAN 的动态 MAC 地址学习限制	mac-address vlan <i>vlan-id</i> max-mac-count <i>max-mac-count-value</i>	必选 缺省情况下，VLAN 中动态 MAC 地址学习不受限制

步骤	命令	说明
		配置学习动态 MAC 地址上限值的取值范围为 1~硬件芯片支持的允许学习的最大地址表项条数

说明:

- 配置基于 VLAN 的动态 MAC 地址学习限制时, 若配置的限制小于当前 VLAN 中已经存在的动态 MAC 地址条数, 设备会提示用户需要手动清除已存在的 MAC 地址表项。手动清除后, 配置即时生效。

配置基于系统的动态 MAC 地址学习限制

系统中学习到的 MAC 地址表项已经达到上限值后, 此系统接收到源 MAC 地址不在 MAC 地址转发表里的报文将被丢弃。

表 26-7 配置基于系统的动态 MAC 地址学习限制

步骤	命令	说明
进入全局配置模式	config terminal	-
配置基于系统的动态 MAC 地址学习限制	mac-address system max-mac-count <i>max-mac-count-value</i>	<p>必选</p> <p>缺省情况下, MAC 地址学习不受限制</p> <p>配置学习动态 MAC 地址上限值的取值范围的范围为 1~硬件芯片支持的允许学习的最大地址表项条数</p>

说明：

- 配置基于系统的动态 MAC 地址学习限制时，若配置的限制小于当前系统中已经存在的动态 MAC 地址条数，设备会提示用户需要手动清除已存在的 MAC 地址表项。手动清除后，配置即时生效。

26.2.3 配置静态 MAC 地址

-B -S -E -A

静态 MAC 地址可以分为两类：静态转发 MAC 地址和静态过滤 MAC 地址。

配置的 MAC 地址必须是合法单播 MAC 地址，不能是广播、组播。

同一个 MAC 地址在同一个 VLAN 中只能配置成静态转发 MAC 地址或者是静态过滤 MAC 地址。

配置条件

无

配置静态过滤 MAC 地址

配置静态过滤 MAC 地址表项后，在相应的 VLAN 中接收到的报文源或目的 MAC 地址值与静态过滤 MAC 地址表项匹配时，报文将被丢弃。此功能用于防止不信任设备接入网络，防止非法用户进行欺骗、攻击活动。

表 26-8 配置静态过滤 MAC 地址

步骤	命令	说明
进入全局配置模式	config terminal	-
配置静态过滤 MAC 地址	mac-address static <i>mac-address-value</i> vlan <i>vlan-id</i> drop	必选 缺省情况下，设备中没有配置静态过滤 MAC 地址

配置绑定在端口下的静态转发 MAC 地址

配置静态转发 MAC 地址表项后，端口在相应 VLAN 中接收到报文时，将报文的目地 MAC 地址与设备中配置的静态转发 MAC 地址表项匹配，如果匹配成功则将报文从指定的端口转发出去。此功能可以更加灵活地控制报文的选路原则，同时防止 MAC 地址表项在设备中出现频繁迁移现象。

表 26-9 配置绑定在端口下的静态转发 MAC 地址

步骤	命令	说明
进入全局配置模式	config terminal	-
配置绑定在端口下的静态转发 MAC 地址	mac-address static <i>mac-address-value</i> vlan <i>vlan-id</i> interface <i>interface-name</i>	必选 缺省情况下，设备中没有配置静态转发 MAC 地址

配置绑定在汇聚组下的静态转发 MAC 地址

配置静态转发 MAC 地址表项后，汇聚组在相应 VLAN 中接收到报文时，将报文的目地 MAC 地址与设备中配置的静态转发 MAC 地址表项匹配，如果匹配成功则将报文从指定的汇聚组转发出去。此功能可以更加灵活地控制报文的选路原则，同时防止 MAC 地址表项在设备中出现频繁迁移现象。

表 26-10 配置绑定在汇聚组下的静态转发 MAC 地址

步骤	命令	说明
进入全局配置模式	config terminal	-
配置绑定在汇聚组下的静态转发 MAC 地址	mac-address static <i>mac-address-value</i> vlan <i>vlan-id</i> link- aggregation <i>link-</i> <i>aggregation-id</i>	必选 缺省情况下，设备中没有配置静态转发 MAC 地址

说明：

- 配置此命令时需要保证指定的汇聚组已经被创建。

26.2.4 MAC 地址管理监控与维护 **-B -S -E -A**

表 26-11 MAC 地址管理监控与维护

命令	说明
clear mac-address dynamic { <i>mac-address-value</i> all / interface <i>interface-list</i> link-aggregation <i>link-aggregation-id</i> vlan <i>vlan-id</i> [<i>mac-address-value</i> / interface <i>interface-list</i> link-aggregation <i>link-aggregation-id</i>] }	清除动态学习到的 MAC 地址表项
show mac-address interface <i>interface-list</i> { all dynamic static [config] }	显示端口下 MAC 地址表项信息
show mac-address link-aggregation <i>link-aggregation-id</i> { all dynamic static [config] }	显示汇聚组下 MAC 地址表项信息
show mac-address vlan <i>vlan-id</i> { all dynamic static [config] }	显示 VLAN 中 MAC 地址表项信息
show mac-address drop [<i>mac-address-value</i> config]	显示系统中静态过滤 MAC 地址表项信息

命令	说明
show mac-address dynamic [<i>mac-address-value</i>]	显示系统中动态 MAC 地址表项信息
show mac-address static [<i>mac-address-value</i> config]	显示系统中静态转发 MAC 地址表项信息
show mac-address system-mac	显示系统使用的 MAC 地址
show mac-address { <i>mac-address-value</i> all }	显示系统中 MAC 地址表项信息或指定 MAC 地址表项信息
show mac-address aging-time	显示动态 MAC 地址表项老化时间信息
show mac-address max-mac-count { interface [<i>interface-name</i>] link-aggregation [<i>link-aggregation-id</i>] system vlan { <i>vlan-id</i> all } }	显示系统中动态 MAC 地址学习限制信息
show mac-address count [interface <i>interface-name</i> link-aggregation <i>link-aggregation-id</i> vlan <i>vlan-id</i>]	显示系统中 MAC 地址表项统计信息

26.3 MAC 地址迁移日志功能配置

26.3.1 MAC 地址迁移日志功能配置

-B -S -E -A

MAC 地址迁移日志功能可以手动开启和关闭，开启 MAC 地址迁移日志功能后，当 MAC 地址表项发生地址迁移时，会记录一条相应的地址迁移日志。

配置条件

无

开启 MAC 地址迁移日志功能

表 26-12 开启 MAC 地址迁移日志功能

步骤	命令	说明
进入全局配置模式	config terminal	-
开启地址迁移日志功能	mac-address move log	默认开启

关闭 MAC 地址迁移日志功能

表 26-13 关闭 MAC 地址迁移日志功能

步骤	命令	说明
进入全局配置模式	config terminal	-
关闭地址迁移日志功能	no mac-address move log	关闭地址迁移日志功能后，MAC 地址表项发生地址迁移时不再记录日志信息。

26.3.2 MAC 地址迁移日志功能监控与维护**-B -S -E -A**

表 26-14 MAC 地址迁移监控与维护

命令	说明
clear mac-address move log{mac-address}	清除 MAC 地址迁移日志

命令	说明
show mac-address move config	查看 MAC 地址迁移日志功能配置信息。
show mac-address move log { <i>mac-address-value</i> count <i>count</i> hardlearn start-time [<i>time</i>] end-time [<i>time</i>] }	查看 MAC 地址迁移日志。

27 生成树

27.1 生成树简介

IEEE 802.1D 协议标准定义的 STP（Spanning Tree Protocol，生成树协议）用于消除网络环路，避免数据帧在环路中不断循环和增生，导致网络拥塞，影响网络正常通信。STP 通过生成树算法，能够判断网络中存在环路的地方，阻塞冗余链路上的端口，把网络修剪成无环路的树型结构，避免设备重复接收相同数据帧，当活动路径发生故障时，能够恢复被阻塞冗余链路的连通性，保证业务正常运行。之后，在 STP 的基础上发展出 RSTP（Rapid Spanning Tree Protocol，快速生成树协议）、MSTP（Multiple Spanning Tree Protocol，多生成树协议），这三者的基本原理相同，后者是前者的改进版。

STP 中定义了以下几个基本概念：

- 根桥 (Root Bridge) : 最终形成的树型网络结构的树根。根桥由具有最高优先级的设备担任;
- 根端口 (RP, Root Port) : 非根桥设备上离根桥最近的端口, 负责与根桥进行通信;
- 指定桥 (Designated Bridge) : 本设备向直连设备或直连局域网转发 BPDU (Bridge Protocol Data Unit, 桥协议数据单元) 配置消息, 则称为该直连设备或直连局域网的指定桥;
- 指定端口 (DP, Designated Port) : 指定桥转发 BPDU 配置消息的端口称为指定端口;
- 路径开销 (Path Cost) : 表示链路的优劣, 与链路速率有关。一般情况下, 链路速率越高, 路径开销越小, 链路越优。

运行 STP 的设备通过交互 BPDU 报文来完成生成树的计算, 最终形成稳定的拓扑结构。BPDU 报文分为以下两种类型:

- 配置 BPDU (Configuration BPDU) : 又称为 BPDU 配置消息, 用来计算和维护生成树拓扑;
- TCN BPDU (Topology Change Notification BPDU) : 当拓扑结构发生变化时, 用来通知其他设备网络拓扑结构发生变化。

BPDU 报文中包含了生成树计算需要的所有信息, 比较重要的几个如下:

- 根桥 ID: 由根桥的优先级和 MAC 地址组成;
- 根路径开销: 到根桥的最小路径开销;
- 指定桥 ID: 由指定桥的优先级和 MAC 地址组成;
- 指定端口 ID: 由指定端口的优先级和端口号组成;
- Message Age: BPDU 配置消息在网络中传播的生存期;
- Hello Time: BPDU 配置消息的发送周期;
- Forward Delay: 端口状态迁移延时;
- Max Age: 配置消息在设备中能够保存的最大生存期。

STP 的选举过程如下:

- 初始状态。

本设备以自己为根桥生成 BPDU 配置消息向外发送，BPDU 报文中根桥 ID 和指定桥 ID 为本设备网桥 ID，根路径开销为 0，指定端口为发送端口。

本设备的每个端口生成端口配置消息用于生成树计算，端口配置消息中根桥 ID 和指定桥 ID 为本设备网桥 ID，根路径开销为 0，指定端口为本端口。

- 更新端口配置消息。

本设备收到来自其他设备的 BPDU 配置消息后，与接收端口的端口配置消息对比，如果接收的配置消息更优，则用 BPDU 配置消息替换端口配置消息，如果端口配置消息更优，则不作任何处理。

比较的原则为：依次比较根桥 ID、根路径开销、指定桥 ID、指定端口 ID、接收端口 ID，值小的更优，前一项相等时才会比较后一项。

- 根桥的选择。

全网中发送最优配置消息的设备被选为根桥。

- 端口角色和端口状态的选择。

根桥的所有端口都是指定端口，处于 Forwarding 状态。指定桥会在所有端口中选出最优的端口配置消息，该消息的接收端口被选为根端口，处于 Forwarding 状态。其它端口根据根端口配置消息计算指定端口配置消息。

计算方式为：根桥 ID 为根端口配置消息的根桥 ID，根路径开销为根端口配置消息的根路径开销与根端口路径开销之和，指定桥 ID 为本设备网桥 ID，指定端口为本端口。

对比端口配置消息和计算出的指定端口配置消息来决定端口角色：如果指定端口配置消息更优，则本端口被选为指定端口，处于 Forwarding 状态，用指定端口配置消息替换端口配置消息，指定端口会以 Hello Time 时间为间隔定期对外发送端口配置消息；如果端口配置消息更优，则端口被阻塞，处于 Discarding 状态，不修改端口配置消息。

只要根桥、根端口、指定端口选举完成，树型网络拓扑就已成功建立。只有根端口和指定端口可以转发数据，其他端口都处于 Discarding 状态，只能接收配置消息，不能发送配置消息和转发数据。

如果某台非根桥的根端口没有定期收到配置消息，则认为这条活动路径发生了故障，设备会重新生成以自己为根桥的 BPDU 配置消息和 TCN BPDU 并对外发送，从而引发生成树的重新计算，得到新的活动路径。

其他设备在收到新的配置消息前，由于没有发现网络拓扑变化，其根端口和指定端口仍会按原来的路径转发数据，新选出的根端口和指定端口必须经过 2 倍 Forward Delay 时间后才会迁移到

Forwarding 状态，以保证新的配置消息传遍全网，避免新旧根端口和指定端口都转发数据而引起暂时性的环路。

IEEE 802.1w 协议标准定义的 RSTP 由 STP 发展而来，是 STP 的优化版，能够实现端口状态的快速迁移，缩短网络最终达到稳定拓扑需要的时间。RSTP 的改进点如下：

- 为根端口设置了备份端口，即 Alternate 端口，当根端口被阻塞，Alternate 端口能够快速切换为新的根端口；
- 为指定端口设置了备份端口，即 Backup 端口，当指定端口被阻塞，Backup 端口能够快速切换为新的指定端口；
- 在两台设备直连的点对点链路中，指定端口只需与下游网桥进行一次握手就可以无时延的进入 Forwarding 状态；
- 将没有连接到其他网桥设备或共享链路上，而直接与用户终端相连的端口定义为边缘端口。边缘端口的状态变化不影响网络连通性，可以无时延的进入 Forwarding 状态。

但是 RSTP 和 STP 形成的都是单生成树，存在以下不足：

- 由于全网只有一颗生成树，网络规模较大时，网络收敛时间较长；
- 所有 VLAN 的报文都沿着一颗生成树进行转发，不能实现负载均衡。

IEEE 802.1s 协议标准定义的 MSTP 在 STP、RSTP 的基础上进行了改善，向下兼容 STP、RSTP，引入了区域、实例的概念，把网络划分为多个区域，一个区域可以包含多个实例，一个实例可以和一个或多个 VLAN 建立映射关系，一个实例对应一棵生成树，一个端口在不同实例里可以有不同的端口角色和端口状态，从而实现了不同 VLAN 的报文按各自的路径转发。

MSTP 中增加了以下几个概念的定义：

- MST 域：由交换网络内的多台设备及它们之间的网络组成。同一 MST 域的设备必须满足的条件为：已使能全局生成树功能，具有相同 MST 域名、MSTP 级别、VLAN 映射表，且物理直连；
- IST (Internal Spanning Tree, 内部生成树)：是每个域内实例 0 上的生成树；
- CST (Common Spanning Tree, 公共生成树)：如果把每个 MST 域看作是一台设备，连接这些 MST 域的单生成树称为 CST；
- CIST (Common and Internal Spanning Tree, 公共和内部生成树)：由 MST 域内的 IST 和 MST 域间的 CST 共同组成，是连接全网所有设备的一棵单生成树；

- MSTI (Multiple Spanning Tree Instance) : MST 域内的生成树, 每个实例生成一个独立的 MSTI;
- 总根: CIST 中的树根;
- 域根: MST 域内每个 IST 和 MSTI 的根桥, MST 域内每个实例拥有独立的生成树, 域根也可能不同。实例 0 的根桥为区域的域根;
- 域边缘端口: 位于 MST 域的边缘, 用于连接不同 MST 域的端口;
- 外部路径开销: 端口到总根的最小路径开销;
- 内部路径开销: 端口到域根的最小路径开销;
- Master 端口: 是 MST 域中到达总根路径开销最小的域边缘端口。Master 端口在 MSTI 中的角色跟 CIST 中的角色相同。

MSTP 的选举规则与 STP 基本相同, 通过对比配置消息, 选举出全网中优先级最高的网桥作为 CIST 的根桥, 每个 MST 域内计算出 IST, MST 域间计算出 CST, 构成了整个网络的 CIST, 每个 MST 域内根据 VLAN 和生成树实例的映射关系, 在每个实例中计算出独立的生成树 MSTI。

27.2 生成树功能配置

表 27-1 生成树功能配置列表

配置任务	
配置生成树基本功能	使能生成树功能
	配置 MST 域
配置网桥属性	配置网桥优先级
	配置 Hello Time 时间
	配置 Forward Delay 时间
	配置 Max Age 时间
	配置 MST 域最大跳数

配置任务	
配置生成树端口属性	配置端口优先级
	配置端口缺省路径开销标准
	配置端口路径开销
	配置 BPDU 报文长度检查
	配置 BPDU 报文最大长度值
	配置 BPDU 报文最大发送速率
	配置 BPDU 报文源 mac 检查
	配置 BPDU 报文的超时因子
	配置边缘端口
	配置边缘端口自动检测
	强制边缘端口自动检测
	配置端口链路类型
配置生成树工作模式	配置生成树工作模式
配置生成树保护功能	配置 BPDU Guard 功能
	配置 BPDU Filter 功能
	配置 Flap Guard 功能
	配置 Loop Guard 功能

配置任务	
	配置 Root Guard 功能
	配置 TC Guard 功能
	配置 TC 保护功能

27.2.1 配置生成树基本功能

-B -S -E -A

配置条件

无

使能生成树功能

使能生成树功能后，设备开始运行生成树协议，通过与其他设备交互 BPDU 报文，最终形成稳定的树型网络拓扑，消除网络环路。

表 27-2 使能生成树功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
使能全局的生成树功能	spanning-tree enable	必选 缺省情况下，未使能全局生成树功能
进入二层以太接口配置模式	interface interface-name	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配
进入汇聚组配置模式	link-aggregation link-aggregation-id	

步骤	命令	说明
		置模式后, 后续配置只在 汇聚组生效
使能端口的生成树功能	spanning-tree enable	可选 缺省情况下, 已使能端口 的生成树功能

配置 MST 域

将整个网络划分为多个 MST 域, 可以缩短网络收敛时间, VLAN 报文在 MST 域内沿着对应的 MSTI 转发, MST 域间沿着 CST 转发。

表 27-3 配置 MST 域

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 MST 域配置模式	spanning-tree mst configuration	-
配置 MST 域名	region-name <i>region- name</i>	必选 缺省情况下, MST 域名为 本设备的 MAC 地址
配置 MSTP 修订级别	revision-level <i>revision- level</i>	必选 缺省情况下, MSTP 修订 级别为 0
配置 VLAN 映射表	instance <i>instance-id</i> vlan <i>vlan-list</i>	必选

步骤	命令	说明
		缺省情况下，所有 VLAN 都映射到实例 0
激活 MST 域参数配置	active configuration pending	必选 缺省情况下，MST 域参数修改后不会立即生效

说明：

- MST 域参数修改后不会立即生效，需要使用 **active configuration pending** 命令激活，触发生成树重新计算，可以使用 **abort configuration pending** 命令取消 MST 域参数配置。

27.2.2 配置网桥属性

-B -S -E -A

配置条件

无

配置网桥优先级

网桥优先级和 MAC 地址共同组成网桥 ID，网桥 ID 的值越小，表示优先级越高，具有最高优先级别的设备会被选为根桥。同一设备在不同生成树实例中可以拥有不同的网桥优先级。

表 27-4 配置网桥优先级

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
配置网桥优先级	spanning-tree mst instance <i>instance-id</i> priority <i>priority-value</i>	必选 缺省情况下，设备在每个生成树实例中的网桥优先级都为 32768

说明：

- 网桥优先级数值的配置步长是 4096，即可配置值有：0、4096、8192、12288、16384、20480、24576、28672、32768、36864、40960、45056、49152、53248、57344、61440。

配置 Hello Time 时间

网络拓扑稳定后，根桥每隔 Hello Time 时间会向外发送 BPDU 报文，通知其他网桥自己现在是根桥，以使其他网桥对自身的根桥地位给予认可。指定桥根据该 BPDU 报文来维护已有的生成树拓扑并向其他设备转发。如果指定桥在 3 倍 Hello Time 时间内没有收到来自根桥的 BPDU 报文，则认为链路出现故障，会引发生成树重新计算网络拓扑以得到新的活动路径，保证网络连通性。

表 27-5 配置 Hello Time 时间

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 Hello Time 时间	spanning-tree mst hello-time <i>seconds</i>	必选 缺省情况下，Hello Time 时间为 2 秒

说明：

- Forward Delay、Hello Time、Max Age 这三个时间参数的配置应满足以下条件，否则会引起网络频繁震荡：

$$2 \times (\text{Forward_Delay} - 1.0\text{seconds}) \geq \text{Max_Age}$$

$$\text{Max_Age} \geq 2 \times (\text{Hello_Time} + 1.0\text{seconds})$$

配置 Forward Delay 时间

在 STP 中，根端口或指定端口由 Discarding 状态迁移到 Forwarding 状态时，由于拓扑变化不能立即传遍全网，为避免引入临时环路，会等待 Forward Delay 时间迁移到 Learning 状态作为过渡，再等待 Forward Delay 时间才最终迁移到 Forwarding 状态。

表 27-6 配置 Forward Delay 时间

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 Forward Delay 时间	spanning-tree mst forward-time <i>seconds</i>	必选 缺省情况下，Forward Delay 时间为 15 秒

配置 Max Age 时间

Max Age 时间是 BPDU 配置消息在网络中传播的生存期。配置消息跨域传递时，每经过一个 MST 域，配置消息中 Message Age 的值加一，如果设备收到的配置消息中 Message Age 的值加 1 等于 Max Age 的值，则会丢弃该配置消息，不用于生成树计算。

表 27-7 配置 Max Age 时间

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 Max Age 时间	spanning-tree mst max-age seconds	必选 缺省情况下，Max Age 时间为 20 秒

配置 MST 域的最大跳数

可以通过配置 MST 域的最大跳数来限制 MST 域的规模。MST 域的最大跳数越大，表示 MST 域的规模越大。同一 MST 域中，从域根开始，配置消息每经过一台设备转发，跳数减一，设备将丢弃跳数为 0 的配置消息，因此处于最大跳数外的设备无法参与同一域内生成树的计算。

表 27-8 配置 MST 域的最大跳数

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 MST 域的最大跳数	spanning-tree mst max-hops max-hops- value	必选 缺省情况下，MST 域的最大跳数为 20

27.2.3 配置生成树端口属性

-B -S -E -A

配置条件

无

配置端口优先级

端口优先级和端口索引共同组成端口 ID，端口 ID 会影响端口角色的选举，端口 ID 的值越小，表示优先级越高。同一端口在不同生成树实例中可以拥有不同的端口优先级。

表 27-9 配置端口优先级

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface <i>interface-name</i>	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	
配置端口优先级	spanning-tree mst instance <i>instance-id</i> port-priority <i>priority-value</i>	必选 缺省情况下，端口在所有生成树实例中的端口优先级都为 128

说明：

- 端口优先级的配置步长是 16，即可配置值有：0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、240。

配置端口缺省路径开销标准

与 IEEE 802.1D-1998 标准计算的路径开销相比，IEEE 802.1T-2001 标准计算的路径开销值更大，随着链路速率增大，路径开销值减小得更快。

表 27-10 配置端口缺省路径开销标准

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置端口缺省路径开销标准	spanning-tree pathcost method { dot1D-1998 dot1T-2001 }	必选 缺省情况下，采用 IEEE 802.1T-2001 标准计算端口的缺省路径开销

配置端口路径开销

端口路径开销会影响端口角色的选举，端口路径开销的值越小，表示链路越优。同一端口在不同生成树实例中可以拥有不同的端口路径开销。

表 27-11 配置端口路径开销

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface <i>interface-name</i>	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	
配置端口的路径开销	spanning-tree mst instance <i>instance-id</i> cost <i>cost-value</i>	必选 缺省情况下，根据端口速率自动计算

配置 BPDU 报文长度检查

配置 BPDU 报文长度检查，可以让端口对接收到的 BPDU 报文的长度进行检查，从而防止非法长度的 BPDU 报文攻击。

表 27-12 配置 BPDU 报文长度检查

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 BPDU 报文长度检查	spanning-tree bpdu length-check	必选 缺省情况下，未开启 BPDU 报文长度检查

配置 BPDU 报文最大长度值

配置进行 BPDU 报文长度检查时，合法 BPDU 报文的最大长度值。

表 27-13 配置 BPDU 报文最大长度值

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 BPDU 报文最大长度值	spanning-tree bpdu max-length <i>max-length</i>	必选 缺省情况下，最大长度值为 1500 字节

配置 BPDU 报文最大发送速率

BPDU 报文最大发送速率限制了设备在 Hello Time 时间内可发送的 BPDU 报文数，避免发送过多 BPDU 报文，造成其他设备频繁进行生成树计算。

表 27-14 配置 BPDU 报文最大发送速率

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 BPDU 报文最大发送速率	spanning-tree transmit hold-count <i>hold-count-number</i>	缺省情况下，端口在 Hello Time 时间内最多可发送 6 个 BPDU 报文

配置 BPDU 报文源 MAC 地址检查

配置 BPDU 报文源 MAC 地址检查，可以让端口对接收到的 BPDU 报文的源 MAC 地址进行检查，从而防止非法设备的 BPDU 报文的攻击。

表 27-15 配置 BPDU 报文源 mac 检查

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface <i>interface-name</i>	必选其一
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
配置 BPDU 报文源 mac 检查	spanning-tree bpdu src-mac-match <i>src-mac</i>	必选

步骤	命令	说明
		缺省情况下，端口未开启 BPDU 报文源 MAC 地址检查

配置 BPDU 报文超时因子

网络拓扑稳定情况下，指定端口都会每 HELLO TIME 时间间隔向相邻设备发送一个 BPDU 报文。通常情况下如果设备在 3 倍超时时间(3*HELLO TIME)间隔内未收到上游设备发送的 BPDU，则会认为网络拓扑已经发生变化，触发生成树重新选举。

但在网络拓扑稳定情况下，上游设备如果比较繁忙或者其它原因导致下游设备没有及时收到 BPDU，引发重新选举，在这种情况下，可以通过配置超时因子避免这种不需要的计算。

表 27-16 配置 BPDU 报文超时因子

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 BPDU 报文时间因子	spanning-tree timer-factor times-number	缺省情况下，设备在 3 倍超时时间(3*HELLO TIME)间隔内未收到上游设备发送的 BPDU，则会认为网络拓扑已经发生变化，触发生成树重新选举。堆叠环境下，建议将超时因子配置为 6。

配置边缘端口

边缘端口是指直接与用户终端直连的端口，边缘端口出现 UP/DOWN 不可能产生临时环路，因此边缘端口可以实现 Discarding 状态到 Forwarding 状态的快速迁移，无需等待延迟时间，且边缘端口出现 UP/DOWN 时不会发送 TC BPDU，避免引起不必要的生成树重新计算。

边缘端口如果收到 BPDU 报文，会重新变为非边缘端口，只有重启该端口才能恢复为边缘端口。

表 27-17 配置边缘端口

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface <i>interface-name</i>	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	
配置边缘端口	spanning-tree portfast edgeport	必选 缺省情况下，端口为非边缘端口

说明：

- 在将端口指定为边缘端口前，请确认端口是与用户终端直接相连，否则配置为边缘端口后，可能会引入临时环路。

配置边缘端口自动检测

可以通过配置边缘端口自动检测，让与终端相连的端口自动识别为边缘端口，从而防止终端设备上下线造成生成树重新计算引起网络震荡。

识别为边缘端口后如果收到 BPDU 报文，会重新变为非边缘端口。

表 27-18 配置边缘端口自动检测

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface interface-name	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation link-aggregation-id	
配置边缘端口自动检测	spanning-tree portfast autoedge	必选 缺省情况下，端口边缘端口自动检测功能在单机模式下默认开启，在堆叠模式下自动关闭

强制边缘端口自动检测

由于配置或者环境的原因，当前端口可能会被错误的识别为边缘端口或非边缘端口，此时用户可以执行该命令触发端口进行边缘端口检测，使端口正确识别自身是否为边缘端口。

表 27-19 配置边缘端口自动检测

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface interface-name	必选其一

步骤	命令	说明
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
强制边缘端口自动检测	spanning-tree portfast autoedge force	必选

说明：

- 该命令只有在端口已经使能自动边缘端口检测的情况下，才会生效

配置端口链路类型

如果两台设备直接相连，可将其端口链路类型配置为点到点链路，点到点链路类型的端口能够实现由 Discarding 状态到 Forwarding 状态的快速迁移，无需等待延迟时间。

表 27-20 配置端口链路类型

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface <i>interface-name</i>	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	后，后续配置只在当前端口生效；进入汇聚组配置模式

步骤	命令	说明
		后，后续配置只在汇聚组生效
配置端口链路类型	spanning-tree link-type { point-to-point shared }	必选 缺省情况下，根据端口双工模式自动设置链路类型，如果端口工作在全双工模式，会设置为点到点链路类型，如果端口工作在半双工模式，会设置为共享链路类型

说明：

- 端口的链路类型应根据实际物理链路来配置，如果端口实际物理链路不是点到点链路，错误配置为点到点链路，可能会引入临时环路。
- 当本端端口链路类型为共享链路类型时，本端端口不支持边缘端口自动识别功能，若对端端口进行边缘端口自动识别，将可能导致对端端口错误识别为边缘端口。

27.2.4 配置生成树工作模式

-B -S -E -A

生成树工作模式决定了设备运行的模式及对外发送的 BPDU 报文的封装格式。工作在 MSTP 模式下的端口，当发现与运行 RSTP 的设备相连时，会自动迁移到 RSTP 模式下工作，工作在 RSTP 模式或 MSTP 模式下的端口，当发现与运行 STP 的设备相连时，会自动迁移到 STP 兼容模式下工作。

配置条件

无

配置生成树工作模式

表 27-21 配置生成树工作模式

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置生成树工作模式	spanning-tree mode { stp rstp mstp }	必选 缺省情况下，生成树工作模式为 MSTP 模式

27.2.5 配置生成树保护功能

-B -S -E -A

配置条件

无

配置 BPDU Guard 功能

对于接入层设备，接入端口一般直接与用户终端或文件服务器相连，此时该端口会被设置为边缘端口以实现端口状态的快速迁移，当边缘端口收到 BPDU 报文时，会自动变为非边缘端口，引起生成树重新计算。正常情况下，边缘端口不会收到 BPDU 报文，但如果有人伪造 BPDU 报文恶意攻击设备，就会导致网络震荡。BPDU Guard 功能用于防止这类攻击，开启 BPDU Guard 功能的边缘端口，如果收到了 BPDU 报文，会被关闭。

表 27-22 配置 BPDU Guard 功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface <i>interface-name</i>	必选其一

步骤	命令	说明
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
配置 BPDU Guard 功能	spanning-tree bpdu guard	必选 缺省情况下，端口未开启 BPDU Guard 功能

配置 BPDU Filter 功能

边缘端口开启 BPDU Filter 功能的后，将不发送、也不接收 BPDU 报文。

表 27-23 配置 BPDU Filter 功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface <i>interface-name</i>	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	
配置 BPDU Filter 功能	spanning-tree bpdu filter	必选 缺省情况下，端口未开启 BPDU Filter 功能

配置 Flap Guard 功能

稳定的拓扑环境中，根端口一般不会发生变化，但当网络中链路不稳定或收到外部 BPDU 报文攻击时，可能会造成根端口的频繁切换，导致网络震荡。

Flap Guard 功能能够防止根端口的频繁切换。开启 Flap Guard 功能后，如果某个生成树实例根端口角色变化频率超过阈值，该实例的根端口会进入 Flap Guard 状态，即根端口的端口状态始终处于 Discarding 状态，直到恢复时间超时后，根端口才开始正常的生成树计算。

表 27-24 配置 Flap Guard 功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
使能 Flap Guard 功能	spanning-tree flap-guard enable	必选 缺省情况下，未使能 Flap Guard 功能
配置在探测周期内允许发生根端口变化的最大次数	spanning-tree flap-guard max-flaps <i>max-flaps-number</i> time seconds	可选 缺省情况下，使能 Flap Guard 功能后，某个实例如果 10 秒钟内发生 5 次根端口角色变化，就会进入 Flap Guard 状态
配置 Flap Guard 恢复时间	spanning-tree flap-guard recovery-time <i>seconds</i>	可选 缺省情况下，Flap Guard 恢复时间为 30 秒

配置 Loop Guard 功能

本设备根据上游设备定期发送的 BPDU 报文维持根端口和其他阻塞端口的状态。但当链路拥塞或者单向链路故障时，这些端口收不到上游设备的 BPDU 报文，端口上的生成树信息超时，此时下游设备会

重新选择端口角色，收不到 BPDU 报文的下游设备端口会转变为指定端口，而阻塞端口会迁移到 Forwarding 状态，从而导致交换网络产生环路。

Loop Guard 功能能够抑制这种环路的产生。开启 Loop Guard 功能后，当端口因没收到上游设备发送的 BPDU 报文而超时，在重新计算端口角色的时候，会将该端口设置为 Discarding 状态，且该端口不参与生成树计算。如果该端口上的实例再次收到 BPDU 报文，则重新参与生成树计算。

表 27-25 配置 Loop Guard 功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface <i>interface-name</i>	必选其一
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
配置 Loop Guard 功能	spanning-tree guard { loop root none }	必选 缺省情况下，未开启端口的 Loop Guard 功能

说明：

- 端口的 Root Guard 功能和 Loop Guard 功能，同时只能有一项功能开启。

配置 Root Guard 功能

生成树的根桥及备份根桥应该处于同一个域内，特别是 CIST 的根桥和备份根桥，网络设计时一般会把 CIST 的根桥和备份根桥放在一个高带宽的核心域内。但由于维护人员的错误配置或网络中的恶意攻击，网络中的合法根桥可能会收到优先级更高的 BPDU 报文，这样当前合法根桥会失去根桥的地

位，引起网络拓扑结构的错误变动。这种不合法的变动会导致原来应该通过高速链路的流量被牵引到低速链路上，导致网络拥塞。

Root Guard 功能能够防止这种情况发生，开启 Root Guard 功能的端口，在所有实例上的端口角色只能保持为指定端口，只要端口收到更优的 BPDU 配置消息，会被设置为 Discarding 状态，一段时间内没再收到更优的 BPDU 配置消息，则会恢复。建议在指定端口上开启 Root Guard 功能。

表 27-26 配置 Root Guard 功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface <i>interface-name</i>	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	
配置 Root Guard 功能	spanning-tree guard { loop root none }	必选 缺省情况下，未开启端口的 Root Guard 功能

说明：

- 端口的 Root Guard 功能和 Loop Guard 功能，同时只能有一项功能开启。

配置 TC Guard 功能

当设备检测到网络拓扑变化时，会产生 TC 报文，通知环境中其他设备网络拓扑发生变化，当设备在接收到 TC 报文后会进行地址刷新操作。在拓扑不稳定的情况下或人为构造 TC 报文进行攻击，网络中会频繁产生 TC，导致设备反复进行地址刷新，影响生成树计算，导致 CPU 占用率高。

TC GUARD 能够有效防止这种情况发生，在当前端口上配置了 TC GUARD 后，当设备收到 TC 报文后，不会再对其中的 TC 标志进行处理，也不再传播 TC，从而有效的防止 TC 报文对网络的冲击。

表 27-27 配置 TC Guard 功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface interface-name	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation link-aggregation-id	
配置 TC Guard 功能	spanning-tree tc-guard enable	必选 缺省情况下，未开启端口的 TC Guard 功能

配置 TC 保护功能

网络拓扑变化时，为确保拓扑变化过程中用户数据的正常转发，设备处理 TC 报文时，会刷新 MAC 地址。如果有人伪造 TC 报文进行攻击，使设备频繁进行地址刷新，会影响生成树计算，导致 CPU 占用率高。

TC 保护功能能够防止这种情况发生，使能 TC 保护功能后，在 TC 保护的间隔时间内，每收到一个 TC 报文，TC 计数器加一，如果 TC 计数器等于或大于阈值，则进入抑制状态，之后的 TC 报文处理时不会进行地址刷新。超过这个间隔时间后，会从抑制状态恢复为正常状态且 TC 计数器清零，重新开始计数。

表 27-28 配置 TC 保护功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
使能 TC 保护功能	spanning-tree tc-protection enable	可选 缺省情况下, TC 保护功能未使能
配置 TC 保护的间隔时间	spanning-tree tc-protection interval <i>seconds</i>	必选 缺省情况下, TC 保护的间隔时间为 2 秒
配置 TC 保护的阈值	spanning-tree tc-protection threshold <i>threshold-value</i>	必选 缺省情况下, TC 保护的阈值为 3

27.2.6 生成树监控与维护

-B -S -E -A

表 27-29 生成树监控与维护

命令	说明
clear spanning-tree detected-protocols	执行全局或指定端口上的 mCheck 操作
clear spanning-tree bpdu statistics [interface <i>interface-name</i> link-aggregation <i>link-aggregation-id</i>]	执行全部或指定端口上的 BPDU 相关统计信息清除操作

命令	说明
show spanning-tree detail	显示生成树详细状态信息
show spanning-tree guard [current [interface <i>interface-name</i> link-aggregation <i>link-aggregation-id</i>]	显示端口上生成树保护功能的配置、状态信息
show spanning-tree { interface <i>interface-name</i> link-aggregation <i>link-aggregation-id</i> } [detail]	显示指定端口或汇聚组的生成树状态信息
show spanning-tree mst [configuration [current pending] detail instance <i>instance-id</i> [detail] { interface <i>interface-name</i> link-aggregation <i>link-aggregation-id</i> } [instance <i>instance-id</i>]]	显示生成树配置、状态信息
show configuration { current pending }	显示 MST 域的相关配置

27.3 生成树典型配置举例

27.3.1 MSTP 典型应用

-B -S -E -A

网络需求

- 网络中的 4 台设备都在同一个 MST 域内，Device1 和 Device2 为汇聚层设备，Device3 和 Device4 为接入层设备。
- 为了合理均衡各条链路上的流量，实现不同 VLAN 数据的负载分担和冗余备份，配置 VLAN2 的报文沿着实例 1 转发，实例 1 的根桥为 Device1；VLAN3 的报文

沿着实例 2 转发，实例 2 的根桥为 Device2；VLAN4 沿着实例 0 转发。

网络拓扑

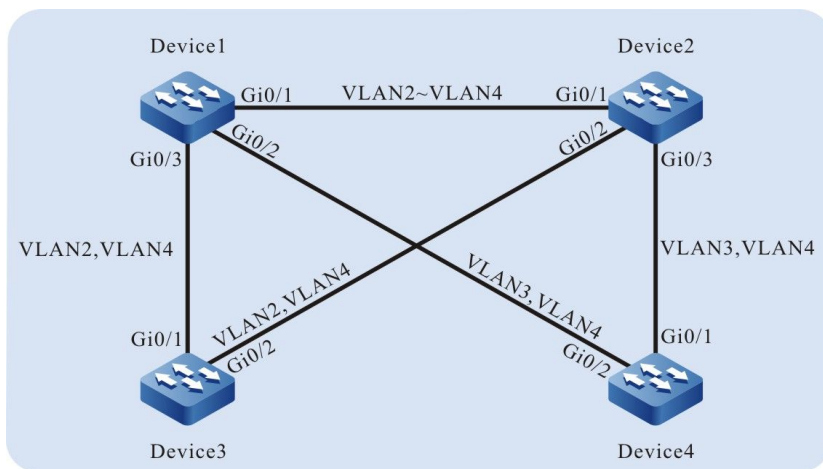


图 27-1 MSTP 典型应用组网图

配置步骤

- 步骤 1： 配置 VLAN 及端口链路类型。

#在 Device1 上创建 VLAN2~VLAN4，配置端口 gigabitethernet0/1 的链路类型为 Trunk，允许 VLAN2~VLAN4 业务通过。

```
Device1(config)#vlan 2-4
Device1(config)#interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#switchport mode trunk
Device1(config-if-gigabitethernet0/1)#switchport trunk allowed vlan add 2-4
Device1(config-if-gigabitethernet0/1)#exit
```

#在 Device1 上配置端口 gigabitethernet0/2 链路类型为 Trunk，允许 VLAN3、VLAN4 的业务通过；gigabitethernet0/3 链路类型为 Trunk，允许 VLAN2、VLAN4 的业务通过。（略）

#在 Device2 上创建 VLAN2~VLAN4，配置端口 gigabitethernet0/1~gigabitethernet0/3 的链路类型为 Trunk，gigabitethernet0/1 允许 VLAN2~VLAN4 业务通过，gigabitethernet0/2 允许 VLAN2、VLAN4 的业务通过，gigabitethernet0/3 允许 VLAN3、VLAN4 的业务通过。（略）

#在 Device3 上创建 VLAN2、VLAN4，配置端口 gigabitethernet0/1~gigabitethernet0/2 的链路类型为 Trunk，允许 VLAN2、VLAN4 的业务通过。（略）

#在 Device4 上创建 VLAN3、VLAN4，配置端口 gigabitethernet0/1~gigabitethernet0/2 的链路类型为 Trunk，允许 VLAN3、VLAN4 的业务通过。（略）

- 步骤 2: 配置 MST 域。

#在 Device1 上进行 MST 域配置, 配置域名为 admin, 修订级别为 1, 实例 1 映射 VLAN2、实例 2 映射 VLAN3, 进行 MST 域激活。

```
Device1#configure terminal
Device1(config)#spanning-tree mst configuration
Device1(config-mst)#region-name admin
Device1(config-mst)#revision-level 1
Device1(config-mst)#instance 1 vlan 2
Device1(config-mst)#instance 2 vlan 3
Device1(config-mst)#active configuration pending
Device1(config-mst)#exit
```

说明:

- Device2、Device3 和 Device4 的 MST 域配置与 Device1 完全相同。(略)
-

#在 Device1 上配置 MSTI 1 的优先级为 0, 在 Device2 上配置 MSTI 2 的优先级为 0。

```
Device1(config)#spanning-tree mst instance 1 priority 0
Device2(config)#spanning-tree mst instance 2 priority 0
```

#在 Device1 上全局使能生成树。

```
Device1(config)#spanning-tree enable
```

说明:

- Device2、Device3 和 Device4 全局使能生成树的配置与 Device1 完全相同。(略)
-

- 步骤 3: 检验结果。

#待网络拓扑稳定后, 在 Device1 上查看所有生成树实例的计算结果。

```
Device1#show spanning-tree mst
Spanning-tree enabled protocol mstp
MST Instance 00      vlans mapped: 1,4-4094
Bridge              address 0000.0000.008b priority 32768
Region root         address 0000.0000.008b priority 32768
Designated root     address 0000.0000.008b priority 32768
                    root: 0, rpc: 0, epc: 0, hop: 20
```

```

Operational hello time 2, forward time 15, max age 20
Configured hello time 2, forward time 15, max age 20, max hops 20, hold count 6
Flap guard : admin false, max count 5, detect period 10s, recovery period 30s
Tc protection: admin true, threshold 3, interval 2s, rxTcCnt 0, status:NORMAL
Bpdu length-check: false, bpdu illegal length packets count: 0
Autoedge swap-check: true
Swap-delay time: 30
Configured timer factor: 3
Topology Change Count:4, last change occurred:0 hour 1 minute 0 second(60 seconds)
  Interface Role Sts Cost Prio.Nbr Type
-----
gi0/1      Desg FWD  20000 128.001 P2P
gi0/2      Desg FWD  20000 128.002 P2P
gi0/3      Desg FWD  20000 128.003 P2P
MST Instance 01 vlans mapped: 2
Bridge ID address 0000.0000.008b priority 1/0
Designated root address 0000.0000.008b priority 1
                root: 0, rpc: 0, hop: 20
Topology Change Count:4, last change occurred:0 hour 1 minute 0 second(60 seconds)
  Interface Role Sts Cost Prio.Nbr Type
-----
gi0/1      Desg FWD  20000 128.001 P2P
gi0/3      Desg FWD  20000 128.003 P2P
MST Instance 02 vlans mapped: 3
Bridge ID address 0000.0000.008b priority 32770/32768
Designated root address 0001.7a54.5c96 priority 2
                root: 32769, rpc: 20000, hop: 19
Topology Change Count:4, last change occurred:0 hour 1 minute 0 second(60 seconds)
  Interface Role Sts Cost Prio.Nbr Type
-----
gi0/1      Root FWD  20000 128.001 P2P
gi0/2      Desg FWD  20000 128.002 P2P

```

#在 Device2 上查看所有生成树实例的计算结果。可以看到，Device2 上的端口 gigabitethernet0/2 在实例 0、实例 1 中都被阻塞。

```

Device2#show spanning-tree mst
Spanning-tree enabled protocol mstp
MST Instance 00 vlans mapped: 1,4-4094
Bridge address 0001.7a54.5c96 priority 32768
Region root address 0000.0000.008b priority 32768
Designated root address 0000.0000.008b priority 32768
                root: 32769, rpc: 20000, rpc: 0, hop: 19
Operational hello time 2, forward time 15, max age 20
Configured hello time 2, forward time 15, max age 20, max hops 20, hold count 6
Flap guard : admin false, max count 5, detect period 10s, recovery period 30s
Tc protection: admin true, threshold 3, interval 2s, rxTcCnt 0, status:NORMAL
Bpdu length-check: false, bpdu illegal length packets count: 0
Autoedge swap-check: true
Swap-delay time: 30
Configured timer factor: 3
Topology Change Count:4, last change occurred:0 hour 1 minute 0 second(60 seconds)
  Interface Role Sts Cost Prio.Nbr Type
-----
gi0/1      Root FWD  20000 128.001 P2P
gi0/2      Alte DIS  20000 128.002 P2P
gi0/3      Desg FWD  20000 128.003 P2P
MST Instance 01 vlans mapped: 2
Bridge ID address 0001.7a54.5c96 priority 32769/32768
Designated root address 0000.0000.008b priority 1
                root: 32769, rpc: 20000, hop: 19
Topology Change Count:4, last change occurred:0 hour 1 minute 0 second(60 seconds)
  Interface Role Sts Cost Prio.Nbr Type
-----
gi0/1      Root FWD  20000 128.001 P2P
gi0/2      Alte DIS  20000 128.002 P2P

```

以太网交换

```
MST Instance 02      vlans mapped: 3
Bridge ID           address 0001.7a54.5c96 priority 2/0
Designated root    address 0001.7a54.5c96 priority 2
                    root: 0, rpc: 0, hop: 20
Topology Change Count:4, last change occurred:0 hour 1 minute 0 second(60 seconds)
  Interface Role Sts   Cost Prio.Nbr Type
-----
gi0/1           Desg FWD   20000 128.001 P2P
gi0/3           Desg FWD   20000 128.003 P2P
```

#在 Device3 上查看所有生成树实例的计算结果。

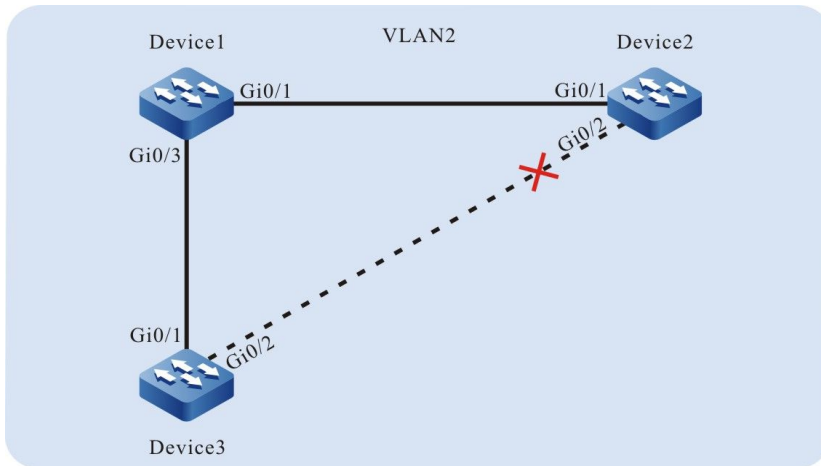
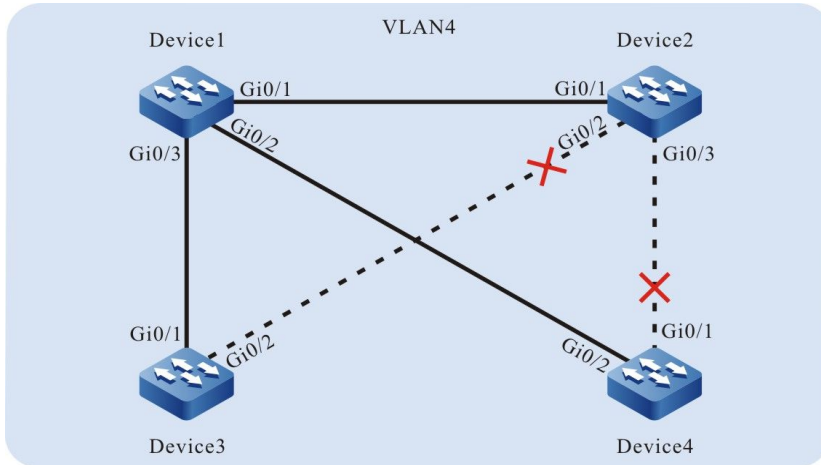
```
Device3#show spanning-tree mst
Spanning-tree enabled protocol mstp
MST Instance 00      vlans mapped: 1,4-4094
Bridge              address 0000.0305.070a priority 32768
Region root         address 0000.0000.008b priority 32768
  Designated root    address 0000.0000.008b priority 32768
                    root: 32769, rpc: 20000, epc: 0, hop: 19
Operational hello time 2, forward time 15, max age 20
Configured hello time 2, forward time 15, max age 20, max hops 20, hold count 6
Flap guard : admin false, max count 5, detect period 10s, recovery period 30s
Tc protection: admin true, threshold 3, interval 2s, rxTcCnt 0, status:NORMAL
Bpdu length-check: false, bpdu illegal length packets count: 0
Autoedge swap-check: true
Swap-delay time: 30
Configured timer factor: 3
Topology Change Count:4, last change occurred:0 hour 1 minute 0 second(60 seconds)
  Interface Role Sts   Cost Prio.Nbr Type
-----
gi0/1           Root FWD   20000 128.001 P2P
gi0/2           Desg FWD   20000 128.002 P2P
MST Instance 01      vlans mapped: 2
Bridge ID           address 0000.0305.070a priority 32769/32768
Designated root    address 0000.0000.008b priority 1
                    root: 32769, rpc: 20000, hop: 19
Topology Change Count:4, last change occurred:0 hour 1 minute 0 second(60 seconds)
  Interface Role Sts   Cost Prio.Nbr Type
-----
gi0/1           Root FWD   20000 128.001 P2P
gi0/2           Desg FWD   20000 128.002 P2P
```

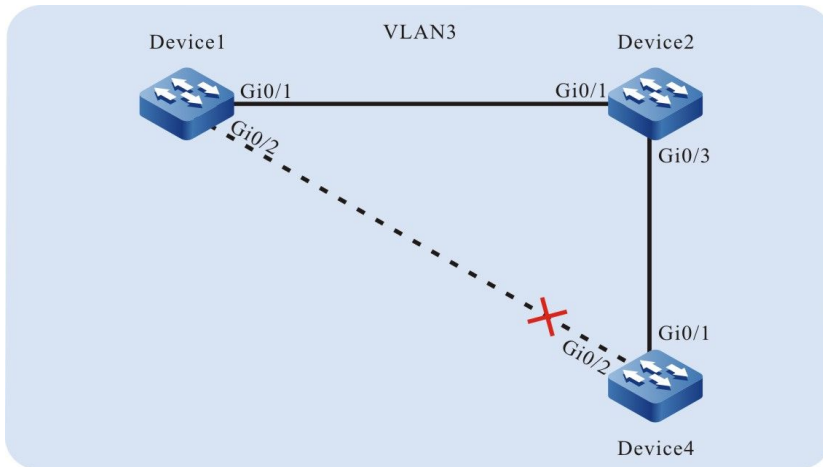
#在 Device4 上查看所有生成树实例的计算结果。可以看到，Device4 上的端口 gigabitethernet0/1 在实例 0 中被阻塞，端口 gigabitethernet0/2 在实例 2 中被阻塞。

```
Device4#show spanning-tree mst
Spanning-tree enabled protocol mstp
MST Instance 00      vlans mapped: 1,4-4094
Bridge              address 0001.7a58.dc0c priority 32768
Region root         address 0000.0000.008b priority 32768
  Designated root    address 0000.0000.008b priority 32768
                    root: 32769, rpc: 20000, epc: 0, hop: 19
Operational hello time 2, forward time 15, max age 20
Configured hello time 2, forward time 15, max age 20, max hops 20, hold count 6
Flap guard : admin false, max count 5, detect period 10s, recovery period 30s
Tc protection: admin true, threshold 3, interval 2s, rxTcCnt 0, status:NORMAL
Bpdu length-check: false, bpdu illegal length packets count: 0
Autoedge swap-check: true
Swap-delay time: 30
Configured timer factor: 3
Topology Change Count:4, last change occurred:0 hour 1 minute 0 second(60 seconds)
  Interface Role Sts   Cost Prio.Nbr Type
-----
gi0/1           Alte DIS  20000 128.001 P2P
gi0/2           Root FWD   20000 128.002 P2P
MST Instance 02      vlans mapped: 3
```

```
Bridge ID      address 0001.7a58.dc0c priority 32770/32768
Designated root address 0001.7a54.5c96 priority 2
                root: 32769, rpc: 20000, hop: 19
Topology Change Count:4, last change occurred:0 hour 1 minute 0 second(60 seconds)
Interface Role Sts Cost Prio.Nbr Type
-----
gi0/1      Root FWD  20000 128.001 P2P
gi0/2      Alte DIS  20000 128.002 P2P
```

根据以上 4 台设备的生成树计算信息，可以分别得出 MSTI 0（映射 VLAN4）、MSTI 1（映射 VLAN2）、MSTI 2（映射 VLAN3）所对应的树图。





28 环回检测

28.1 环回检测简介

在以太网中，当报文无法识别目的地时，会在同一 VLAN 内进行洪泛。当网络存在环路时，报文就会在网络中无限循环增生，最终导致将带宽耗尽，网络无法正常通信。

出现环路有两种情况：一种是在设备的不同以太接口之间存在环路，另一种是在设备的同一个以太接口上存在环回。这两种情况都可以采用环回检测来进行环路的检测。

通过启动环回检测功能，以太接口每隔一段时间发送环回检测报文，检查网络是否存在环路。当以太接口接收到本设备发送出去的环回检测报文时，认为网络中出现环路，关闭相应以太接口，消除局部环路对整网的影响。

28.2 环回检测功能配置

表 9-1 环回检测功能配置列表

配置任务	
配置环回检测基本功能	使能全局环回检测控制开关
	使能以太接口或汇聚组环回检测控制开关
配置环回检测基本参数	配置环回检测报文发送周期
	配置以太接口 Error-Disable 动作

28.2.1 配置环回检测基本功能

-B -S -E -A

配置条件

无

使能全局环回检测控制开关

全局环回检测控制开关用于使能全局环回检测功能，只有使能全局环回检测控制开关，以太接口的环回检测配置才能生效。

表 9-2 使能全局环回检测控制开关

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
使能全局环回检测控制开关	loopback-detection enable	必选 缺省情况下，未使能环回检测全局控制开关

使能以太接口或汇聚组环回检测控制开关

使能环回检测功能后，会在以太接口每隔一段时间发送环回检测报文，检查网络是否存在环路。

表 9-3 使能以太接口或汇聚组环回检测控制开关

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层/三层以太接口配置模式	interface <i>interface-name</i>	必选其一 进入二层/三层以太接口配置模式后，后续配置只在当前以太接口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	
使能以太接口或汇聚组环回检测控制开关	loopback-detection enable	必选 缺省情况下，未使能以太接口或汇聚组环回检测控制开关

说明：

- 在环回检测的配置任务中，必须先使能全局环回检测控制开关，以太接口的环回检测配置才能生效。

28.2.2 配置环回检测基本参数

-B -S -E -A

配置条件

无

配置环回检测报文发送周期

环回检测会周期性地发送环回检测报文，来探测网络是否存在环路。可以根据网络的实际情况来修改环回检测报文的发送周期。

表 9-4 配置环回检测报文发送周期

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层/三层以太网接口配置模式	interface <i>interface-name</i>	必选其一 进入二层/三层以太网接口配置模式后，后续配置只在当前以太网接口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	
配置环回检测报文发送周期	loopback-detection enable interval-time <i>interval-time-value</i>	必选

步骤	命令	说明
		缺省情况下，环回检测报文的发送周期为 30 秒

配置以太接口 Error-Disable 动作

若以太接口允许 Error-Disable 动作即以太接口受控，当以太接口在检测到环回后，会执行 Error-Disable 动作，将以太接口关闭，以消除环路。若以太接口为非受控状态，以太接口只打印环回提示信息，不关闭以太接口，此时环路未消除。

表 9-5 配置以太接口 Error-Disable 动作

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层/三层以太接口配置模式	interface <i>interface-name</i>	必选其一
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	进入二层/三层以太接口配置模式后，后续配置只在当前以太接口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
配置以太接口是否允许 Error-Disable 动作	loopback-detection enable control	必选 缺省情况下，以太接口检测到环路执行 Error-Disable 动作

28.2.3 环回检测监控与维护

-B -S -E -A

表 9-6 环回检测监控与维护

命令	说明
show loopback-detection [interface <i>interface-name</i> link-aggregation <i>link-aggregation-id</i>]	显示环回检测全部以太接口配置信息或指定以太接口配置信息

28.3 环回检测典型配置举例

28.3.1 配置远端环回检测

-B -S -E -A

网络需求

- Device1 与 Device2 直连，Device2 上有两个二层以太接口自环。
- 在 Device1 上开启环回检测。
- Device1 检测到环路后，对互联以太接口执行关闭操作，阻断环路。

网络拓扑

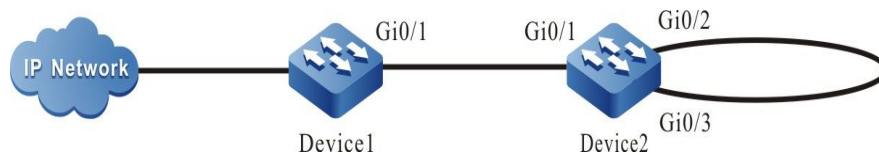


图 9-1 配置远端环回检测功能组网图

二层以太接口配置步骤

- 步骤 1: 配置 VLAN 及二层以太接口链路类型。

#在 Device1 上创建 VLAN2。

```
Device1#configure terminal
Device1(config)#vlan 2
Device1(config-vlan2)#exit
```

#在 Device1 上配置二层以太接口 gigabitethernet0/1 链路类型为 Trunk, 允许 VLAN2 的业务通过。

```
Device1(config)#interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#switchport mode trunk
Device1(config-if-gigabitethernet0/1)#switchport trunk allowed vlan add 2
Device1(config-if-gigabitethernet0/1)#exit
```

#在 Device2 上创建 VLAN2。

```
Device2#configure terminal
Device2(config)#vlan 2
Device2(config-vlan2)#exit
```

#在 Device2 上配置二层以太接口 gigabitethernet0/1、gigabitethernet0/2、gigabitethernet0/3 链路类型为 Trunk, 允许 VLAN2 的业务通过, 二层以太接口 gigabitethernet0/2、gigabitethernet0/3 关闭生成树。

```
Device2(config)#interface gigabitethernet 0/1-0/3
Device2(config-if-range)#switchport mode trunk
Device2(config-if-range)#no switchport trunk allowed vlan 1
Device2(config-if-range)#switchport trunk allowed vlan add 2
Device2(config-if-range)#exit
Device2(config)#interface gigabitethernet 0/2-0/3
Device2(config-if-range)#no spanning-tree enable
Device2(config-if-range)#exit
```

- 步骤 2: 使能环回检测功能。

#在 Device1 上全局使能环回检测功能。

```
Device1(config)#loopback-detection enable
```

#在 Device1 上, 查看环回检测状态。

```
Device1#show loopback-detection
-----
Global loopback-detection : ENABLE
-----
Interface      Loopback  Time(s)  State    Control
-----
gi0/1          DISABLE   30       NORMAL   TRUE
gi0/2          DISABLE   30       NORMAL   TRUE
```

#在 Device1 上的二层以太接口 gigabitethernet0/1 使能环回检测功能。

以太网交换

```
Device1(config)#interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#loopback-detection enable
Device1(config-if-gigabitethernet0/1)#exit
```

- 步骤 3: 检验结果。

#在 Device1 上, 查看环回检测状态。

```
检测到环路之后:
Device1#show loopback-detection
-----
Global loopback-detection : ENABLE
-----
Interface      Loopback  Time(s)  State      Control
-----
gi0/1          ENABLE    30       ERR-DISABLE TRUE
gi0/2          DISABLE   30       NORMAL     TRUE
```

#Device1 上检测到环路, 二层以太接口 gigabitethernet0/1 执行关闭操作, 在设备上输出如下提示信息。

```
Jul 30 2014 03:30:30: %LOOP-BACK-DETECTED : loop-back send tag packet in vlan2 on gigabitethernet0/1,
detected in vlan2 from gigabitethernet0/1
Jul 30 2014 03:30:30: %LINK-INTERFACE_DOWN-4: interface gigabitethernet0/1, changed state to down
Jul 30 2014 03:30:30: %LINEPROTO-5-UPDOWN : gigabitethernet0/1 link-status changed to err-disable
```

#在 Device1 上查看二层以太接口 gigabitethernet0/1 的状态, 可以看到二层以太接口 gigabitethernet0/1 链路状态变为 Down。

```
Device1#show interface gigabitethernet 0/1
gigabitethernet0/1 configuration information
Description      :
Status           : Enabled
Link             : Down (Err-disabled)
Set Speed        : Auto
Act Speed        : Unknown
Set Duplex       : Auto
Act Duplex       : Unknown
Set Flow Control : Off
Act Flow Control : Off
Mdix             : Auto
Mtu              : 1824
Port mode        : LAN
Port ability     : 10M HD,10M FD,100M HD,100M FD,1000M FD
Link Delay       : No Delay
Storm Control    : Unicast Disabled
Storm Control    : Broadcast Disabled
Storm Control    : Multicast Disabled
Storm Action     : None
Port Type        : Nni
Pvid             : 1
Set Medium       : Copper
Act Medium       : Copper
Mac Address      : 0000.0000.008b
```

三层以太接口配置步骤

- 步骤 1: 配置 VLAN 及二层以太接口链路类型。

以太网交换

#在 Device2 上创建 VLAN2。

```
Device2#configure terminal
Device2(config)#vlan 2
Device2(config-vlan2)#exit
```

#在 Device2 上配置二层以太接口 gigabitethernet0/1、gigabitethernet0/2、gigabitethernet0/3 链路类型为 Trunk，允许 VLAN2 的业务通过；二层以太接口 gigabitethernet0/2、gigabitethernet0/3 关闭生成树。

```
Device2(config)#interface gigabitethernet 0/1-0/3
Device2(config-if-range)#switchport mode trunk
Device2(config-if-range)#no switchport trunk allowed vlan 1
Device2(config-if-range)#switchport trunk allowed vlan add 2
Device2(config-if-range)#switchport trunk pvid vlan 2
Device2(config-if-range)#exit
Device2(config)#interface gigabitethernet 0/2-0/3
Device2(config-if-range)#no spanning-tree enable
Device2(config-if-range)#exit
```

- 步骤 2： 使能环回检测功能。

#在 Device1 上全局使能环回检测功能。

```
Device1(config)#loopback-detection enable
```

#在 Device1 上，查看环回检测状态。

```
Device1#show loopback-detection
-----
Global loopback-detection : ENABLE
-----
Interface      Loopback Time(s) State    Control
-----
gi0/1          DISABLE  30    NORMAL  TRUE
gi0/2          DISABLE  30    NORMAL  TRUE
```

#在 Device1 上配置二层以太接口 gigabitethernet0/1 为三层以太接口。

```
Device1(config)#interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#no switchport
```

```
#在 Device1 上的三层以太接口 gigabitethernet0/1 使能环回检测功能
Device1(config-if-gigabitethernet0/1)#loopback-detection enable
Device1(config-if-gigabitethernet0/1)#exit
```

- 步骤 3： 检验结果。

#在 Device1 上，查看环回检测状态。

检测到环路之后：

配置手册

发布 1.1 04/2020

以太网交换

```
Device1#show loopback-detection
-----
Global loopback-detection : ENABLE
-----
Interface      Loopback Time(s) State    Control
-----
gi0/1          ENABLE   30    ERR-DISABLE  TRUE
gi0/2          DISABLE  30    NORMAL      TRUE
```

#Device1 上检测到环路，三层以太接口 gigabitethernet0/1 执行关闭操作，在设备上输出如下提示信息。

```
Jul 31 2014 11:29:30: %LOOP-BACK-DETECTED : loop-back send packet on gigabitethernet0/1, detected from
gigabitethernet0/1
Jul 31 2014 11:29:30: %LINEPROTO-5-UPDOWN : gigabitethernet0/1 link-status changed to err-disable
Jul 31 2014 11:29:30: %LINK-INTERFACE_DOWN-3: Interface gigabitethernet0/1, changed state to down.
Jul 31 2014 11:29:30: %LINK-LINEPROTO_DOWN-3: Line protocol on interface gigabitethernet0/1, changed
state to down.
```

#在 Device1 上查看三层以太接口 gigabitethernet0/1 的状态，可以看到三层以太接口状态变为 err-disabled。

```
Device1#show interface gigabitethernet 0/1 status err-disabled
-----
Interface      Status      Reason
-----
gi0/1          err-disabled  loopback-detect
```

28.3.2 配置本端环回检测 **-B -S -E -A**

网络需求

- Device1 和 Device2 设备通过 2 条链路环接，所有环接的三层以太接口在同一 VLAN 内。
- 在 Device1 上开启环回检测。
- Device1 上检测到环路后，对互联三层以太接口执行关闭操作，阻断环路。

网络拓扑

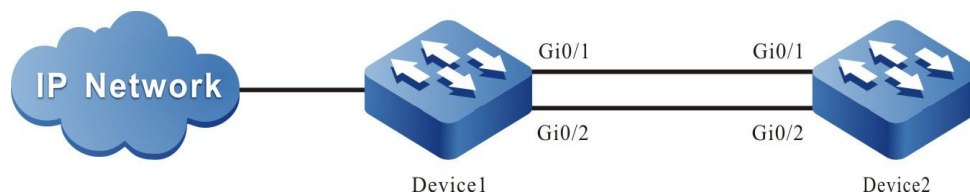


图 9-2 配置本端环回检测功能组网图

二层以太接口配置步骤

- 步骤 1: 配置 VLAN 及二层以太接口链路类型。

#在 Device1 上创建 VLAN2。

```
Device1#configure terminal
Device1(config)#vlan 2
Device1(config-vlan2)#exit
```

#在 Device1 上, 配置二层以太接口 gigabitethernet0/1 和 gigabitethernet0/2 链路类型为 Trunk, 允许 VLAN2 的业务通过。

```
Device1(config)# interface gigabitethernet 0/1-0/2
Device1(config-if-range)#switchport mode trunk
Device1(config-if-range)#switchport trunk allowed vlan add 2
Device1(config-if-range)#exit
```

#在 Device2 上创建 VLAN2。

```
Device2#configure terminal
Device2(config)#vlan 2
Device2(config-vlan2)#exit
```

#配置二层以太接口 gigabitethernet0/1 和 gigabitethernet0/2 链路类型为 Trunk, 允许 VLAN2 的业务通过, 并且关闭生成树。

```
Device2(config)# interface gigabitethernet 0/1-0/2
Device2(config-if-range)#switchport mode trunk
Device2(config-if-range)#no switchport trunk allowed vlan 1
Device2(config-if-range)#switchport trunk allowed vlan add 2
Device2(config-if-range)#no spanning-tree enable
Device2(config-if-range)#exit
```

- 步骤 2: 使能环回检测功能。

#在 Device1 上全局使能环回检测功能。

```
Device1(config)#loopback-detection enable
```

#在 Device1 上, 查看环回检测状态。

```
Device1#show loopback-detection
-----
Global loopback-detection : ENABLE
-----
Interface      Loopback  Time(s)  State    Control
-----
gi0/1          DISABLE   30       NORMAL   TRUE
gi0/2          DISABLE   30       NORMAL   TRUE
```

#在 Device1 的二层以太接口 gigabitethernet0/1 使能环回检测功能。

```
Device1(config)#interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#loopback-detection enable
Device1(config-if-gigabitethernet0/1)#exit
```

以太网交换

- 步骤 3: 检验结果。

#在 Device1 上, 查看环回检测状态。

```
检测到环路之后:
Device1#show loopback-detection
-----
Global loopback-detection : ENABLE
-----
Interface      Loopback Time(s) State      Control
-----
gi0/1          ENABLE   30    ERR-DISABLE TRUE
gi0/2          DISABLE  30    NORMAL    TRUE
```

Device1 上检测到环路, 二层以太网接口 gigabitethernet0/1 执行关闭操作, 在设备上输出如下提示信息。

```
Jul 30 2014 03:29:59: %LOOP-BACK-DETECTED : loop-back send tag packet in vlan2 on gigabitethernet0/1,
detected in vlan2 from gigabitethernet0/2
Jul 30 2014 03:29:59: %LINK-INTERFACE_DOWN-4: interface gigabitethernet0/1, changed state to down
Jul 30 2014 03:29:59: %LINEPROTO-5-UPDOWN : gigabitethernet0/1 link-status changed to err-disable
```

#在 Device1 上查看二层以太网接口 gigabitethernet0/1 的状态, 可以看到二层以太网接口 gigabitethernet0/1 链路状态变为 Down。

```
Device1#show interface gigabitethernet 0/1
gigabitethernet0/1 configuration information
Description      :
Status           : Enabled
Link             : Down (Err-disabled)
Set Speed        : Auto
Act Speed        : Unknown
Set Duplex       : Auto
Act Duplex       : Unknown
Set Flow Control : Off
Act Flow Control : Off
Mdx              : Auto
Mtu              : 1824
Port mode        : LAN
Port ability     : 10M HD,10M FD,100M HD,100M FD,1000M FD
Link Delay       : No Delay
Storm Control    : Unicast Disabled
Storm Control    : Broadcast Disabled
Storm Control    : Multicast Disabled
Storm Action     : None
Port Type       : Nni
Pvid             : 1
Set Medium       : Copper
Act Medium       : Copper
Mac Address      : 0000.0000.008b
```

说明:

- Device1 的 gigabitethernet 0/1 或者 gigabitethernet 0/2 为三层以太网接口时, 这种组网环境不存在环路。
-

29 Error-Disable 管理

29.1 Error-Disable 管理简介

Error-Disable 功能是一种端口上的错误检测与故障恢复机制。

在端口上出现的异常情况，可能会导致整个网络性能下降或者瘫痪。使用 Error-Disable 功能可以把这些异常情况限制在单台设备或者局部网络范围内，避免影响其它正常工作的端口以及扩散异常情况。

在一个端口处于开启状态的情况下，当在这个端口上检测到异常情况时，这个端口会被自动关闭，使得这个端口不再继续转发报文。换句话说，当在这个端口上触发某种错误条件(error condition)时，这个端口会被自动禁用 (disable)。这种情况被称为 Error-Disable 管理功能，并且这时的端口状态被称为 Error-Disabled 状态。

当前支持以下功能，风暴抑制、端口安全、链路震荡、DHCP 限速、BPDU Guard、ARP 检测、L2 协议隧道、环回检测、OAM 网管、Monitor Link、fabric-failure。

当上述功能在端口上检测到异常情况时，这个端口会被自动关闭并且设置为 Error-Disabled 状态。但是，这种状态不能一直持续下去，等到故障解除之后需要重新启用这个端口，并且清除端口的 Error-Disabled 状态，使得这个端口继续转发报文。这里就涉及 Error-Disable 管理功能的自动恢复机制。

29.2 Error-Disable 管理功能配置

表 29-1 Error-Disable 管理功能配置列表

配置任务	
配置 Error-Disable 基本功能	配置 Error-Disable 错误检测
配置 Error-Disable 自动恢复	配置 Error-Disable 自动恢复
	配置 Error-Disable 自动恢复的时间间隔

29.2.1 配置 Error-Disable 管理基本功能

-B -S -E -A

配置条件

无

配置 Error-Disable 错误检测

通过配置指定功能的 Error-Disable 错误检测，当端口上检测到异常情况时，系统自动关闭这个端口并且设置端口状态为 Error-Disabled。

表 29-2 配置 Error-Disable 错误检测

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 Error-Disable 错误检测	errdisable detect cause { all bpduguard dai dhcp-snooping storm-control link-flap port-security loopback-detect	必选 缺省情况下，允许列出的所有功能将端口关闭并且设置为 Error-Disabled 状态

步骤	命令	说明
	transceiver-power-low }	

29.2.2 配置 Error-Disable 自动恢复

-B -S -E -A

配置 Error-Disable 自动恢复

由于 Error-Disable 错误检测机制使得指定功能可以关闭端口，为了使端口尽快恢复并且继续转发报文，提供自动恢复机制，可在指定的时间间隔之后，自动地重新启用这个端口。

表 29-3 配置 Error-Disable 自动恢复

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 Error-Disable 自动恢复	errdisable recovery cause { all bpduguard dai dhcp-snooping eips-udld link-flap loopback-detect port-security storm-control transceiver-power-low ulfd }	必选 缺省情况下，不能自动启用端口和清除被列出的所有功能设置的 Error-Disabled 状态。例外地，允许自动启用端口并且清除被 Link-Flap 功能设置的 Error-Disabled 状态

配置 Error-Disable 自动恢复的时间间隔

配置端口在被 Error-Disable 错误检测机制关闭之后自动恢复的时间间隔。

表 29-4 配置 Error-Disable 自动恢复的时间间隔

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 Error-Disable 自动恢复的时间间隔	errdisable recovery interval <i>interval-value</i>	必选 缺省情况下, 自动启用端口并且清除 Error-Disabled 状态的时间间隔为 300 秒

29.2.3 Error-Disable 管理监控与维护

-B -S -E -A

表 29-5 Error-Disable 管理监控与维护

命令	说明
show errdisable detect	显示是否允许列出的所有功能将端口关闭和设置为 Error-Disabled 状态
show errdisable recovery	显示是否允许自动启用端口和清除被列出的所有功能设置的 Error-Disabled 状态
show { interface <i>interface-list</i> link-aggregation <i>link-aggregation-id</i> } status err-disabled	显示指定端口或汇聚组被设置为 Error-Disabled 状态的相关信息

29.3 Error-Disable 管理典型配置举例

29.3.1 Error-Disable 与风暴抑制联用

-B -S -E -A

网络需求

- PC 通过 Device 接入 IP Network，在 Device 上使能风暴抑制功能和 Error-Disable 功能。
- 当设备上端口收到大量广播报文时可以通过 Error-Disable 将端口关闭，且 Error-Disable 可根据策略重新启用该端口。

网络拓扑

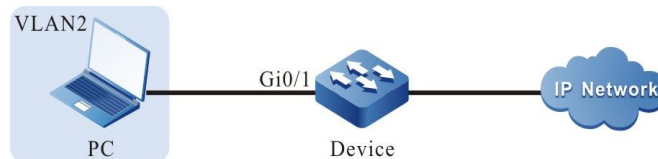


图 29-1 Error-Disable 与风暴抑制联用组网图

配置步骤

- 步骤 1：配置 VLAN 和端口的链路类型。

#在 Device 上创建 VLAN2。

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#配置 Device 端口 gigabitethernet0/1 的链路类型为 Access，允许 VLAN2 的业务通过。

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
Device(config-if-gigabitethernet0/1)#exit
```

- 步骤 2：配置风暴抑制功能。

#在 Device 端口 gigabitethernet0/1 上使能风暴抑制功能，并采用 pps 限制方式对广播报文进行抑制，抑制速率为 20pps，发生风暴时采取的动作是 shutdown 端口。

以太网交换

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#storm-control action shutdown
Device(config-if-gigabitethernet0/1)#storm-control broadcast pps 20
Device(config-if-gigabitethernet0/1)#exit
```

- 步骤 3: 配置 Error-Disable 功能。

#使能 Error-Disable 中风暴抑制的恢复功能, 并配置恢复时间为 30 秒。

```
Device(config)#errdisable recovery cause storm-control
Device(config)#errdisable recovery interval 30
```

- 步骤 4: 检验结果。

#查看 Error-Disable 相关配置。

```
Device#show errdisable recovery

Error disable auto recovery config
interval:30 seconds
ErrDisable Reason  Timer Status
-----
bpduguard          Disabled
dai                 Disabled
dhcp-snooping      Disabled
erps-udld          Disabled
link-flap           Enabled
loopback-detect    Disabled
port-security      Disabled
storm-control       Enabled
ulfd                Disabled
transceiver-power-low Disabled
```

#当 PC 发送大量广播报文时, 端口 gigabitethernet0/1 将被关闭, 并打印以下提示信息。

```
Nov 24 2014 15:37:13: %STORM_CONTROL-3: A storm detected on interface gigabitethernet0/1,
ActionType:shutdown, StormType: broadcast storm
```

```
Nov 24 2014 15:37:13: %PORTMGR-LINEPROTO_DOWN-3: Line protocol on interface
gigabitethernet0/1, changed state to down
```

.#查看端口 gigabitethernet0/1 状态。

```
Device#show interface gigabitethernet 0/1

gigabitethernet0/1 configuration information
Description      :
Status           : Enabled
Link             : Down (Err-disabled)
Set Speed        : Auto
Act Speed        : Unknown
Set Duplex       : Auto
```

```
Act Duplex      : Unknown
Set Flow Control : Off
Act Flow Control : Off
Mdix           : Auto
Mtu            : 1824
Port mode      : LAN
Port ability   : 10M HD,10M FD,100M HD,100M FD,1000M FD
Link Delay     : No Delay
Storm Control  : Unicast Pps 1500
Storm Control  : Broadcast Pps 20
Storm Control  : Multicast Pps 1500
Storm Action   : Shutdown
Port Type      : Nni
Pvid           : 2
Set Medium     : Copper
Act Medium     : Copper
Mac Address    : 0001.7a54.5ca5
```

#30 秒后端口 gigabitethernet0/1 将启用，并打印以下提示信息。

```
Nov 24 2014 15:37:43: %PORTMGR-AUTO_RECOVERY-5: auto recovery timer expired on interface
gigabitethernet0/1, module: STROM CONTROL ACTION.
Nov 24 2014 15:37:45: %PORTMGR-LINEPROTO_UP-5: Line protocol on interface gigabitethernet0/1,
changed state to up.
```

#查看端口 gigabitethernet0/1 状态。

```
Device#show interface gigabitethernet 0/1

gigabitethernet0/1 configuration information
Description      :
Status          : Enabled
Link            : Up
Set Speed       : Auto
Act Speed       : 1000
Set Duplex      : Auto
Act Duplex      : Full
Set Flow Control : Off
Act Flow Control : Off
Mdix           : Auto
Mtu            : 1824
Port mode      : LAN
Port ability   : 10M HD,10M FD,100M HD,100M FD,1000M FD
Link Delay     : No Delay
Storm Control  : Unicast Pps 1500
Storm Control  : Broadcast Pps 20
Storm Control  : Multicast Pps 1500
Storm Action   : Shutdown
Port Type      : Nni
Pvid           : 2
Set Medium     : Copper
Act Medium     : Copper
Mac Address    : 0001.7a54.5ca5
```

IP 协议及业务

30 ARP

30.1 ARP 简介

ARP (Address Resolution Protocol, 地址解析协议) 提供 IP 地址到对应 MAC 地址的动态映射。在以太网中传输的以太帧需要指定 MAC 地址才能够正确封装, ARP 协议用于获取 IP 地址对应的 MAC 地址。

30.2 ARP 功能配置

表 30-1 ARP 功能配置列表

配置任务	
配置 ARP 基本功能	配置静态 ARP
	配置本地 ARP 通告
	配置动态 ARP 最大条目数
	配置动态 ARP 老化时间
	使能动态 ARP 学习功能
	使能动态 ARP 被动学习功能

配置任务	
	配置 ARP 报文接收队列长度
	配置 ARP 代理

30.2.1 配置 ARP 基本功能 **-B -S -E -A**

配置条件

无

配置静态 ARP

配置静态 ARP 是指用户手动指定 IP 地址与 MAC 地址的映射关系。

表 30-2 配置静态 ARP

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置静态 ARP	arp [vrf vrf-name] { ip-address / host-name } mac-address [alias [advertise] advertise [alias]] [vlan vlan-id] {{ interface if-name } { link-aggregation link-aggregation-id }}	必选

说明：

- 当配置的静态 ARP 带有 alias 选项时，如果收到该 IP 地址的 ARP 请求，则使用该静态 ARP 中的 MAC 地址进行应答。
- 当配置的静态 ARP 带有 advertise 选项时，在使能静态 ARP 通告的情况下，则会定期通告该静态 ARP。
- 当静态 ARP 绑定到具体的端口或者汇聚组时，则静态 ARP 只在这个端口或者汇聚组生效。

配置本地 ARP 通告

ARP 请求报文是广播报文，当网络中存在大量 ARP 请求时，容易在网络上产生广播风暴，导致正常的 ARP 请求报文可能被淹没，无法学习到 ARP。这种情况下，可以通过配置本地 ARP 通告功能来减少 ARP 请求，降低广播风暴的可能性。

表 30-3 配置本地 ARP 通告

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置本地 ARP 通告	arp local-announce enable	必选
配置本地 ARP 通告时间间隔	arp local-announce interval seconds	可选 缺省值为 10 秒
配置本地 ARP 通告的速率	arp local-announce rate speed	可选 缺省值为 1 个报文每秒

配置动态 ARP 最大条目数

配置动态 ARP 最大条目数是为了避免动态学习的 ARP 占用过多系统资源。

表 30-4 配置动态 ARP 最大条目数

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置动态 ARP 最大条目数	arp limited max-entries	必选 缺省最大条目数为 2000

配置动态 ARP 老化时间

动态学习的 ARP 存在生存周期，即老化时间。在老化时间内，设备会定期发送 ARP 请求，如果收到 ARP 应答则重置老化时间，当老化时间超时，则删除该动态 ARP 表项。

表 30-5 配置动态 ARP 老化时间

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface interface-name	-
配置动态 ARP 老化时间	arp timeout { second / disable }	必选 缺省老化时间为 1200 秒

使能动态 ARP 被动学习功能

设备缺省可以进行动态 ARP 被动学习，为了避免动态学习的 ARP 占用过多系统资源，用户可以关闭动态 ARP 被动学习功能。关闭动态 ARP 被动学习功能后，当收到请求本设备 MAC 地址的 ARP 请求时，只进行 ARP 应答，但本设备不生成相关 ARP 表项。只有当本设备主动请求对端设备 MAC 地址时，才生成相关 ARP 表项。

表 30-6 使能动态 ARP 被动学习功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
使能动态 ARP 被动学习功能	arp learn-active	必选 缺省情况下，使能动态 ARP 被动学习功能

使能接口动态 ARP 学习功能

接口缺省可以进行动态 ARP 学习，为了获得更可靠的安全性，用户可关闭接口动态 ARP 学习功能，并使用静态 ARP，可有效防止 ARP 欺骗。

表 30-7 使能动态 ARP 学习功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface interface-name	-
使能动态 ARP 学习功能	arp dynamic-learn	必选 缺省情况下，使能动态 ARP 学习功能

配置 ARP 报文接收队列长度

设备收到的 ARP 报文会首先被缓存到 ARP 接收队列，系统从该队列依次读取报文进行处理。当缓存的 ARP 报文达到队列长度后，后续接收的 ARP 报文将被丢弃。用户可根据网络突发 ARP 情况，调整 ARP 报文接收队列长度。

表 30-8 配置 ARP 报文接收队列长度

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 ARP 报文接收队列长度	arp queue-length <i>length</i>	必选 缺省 ARP 报文接收队列长度为 200

配置 ARP 代理

ARP 的请求是从一个网络的主机发往另一个网络，并且连接这两个网络的中间设备可以应答该 ARP 请求，这个过程称为 ARP 代理。

表 30-9 配置 ARP 代理

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置 ARP 代理	ip proxy-arp	必选 缺省情况下，已开启 ARP 代理功能

30.2.2 ARP 监控与维护

-B -S -E -A

表 30-10 ARP 监控与维护

命令	说明
show arp [vrf vrf-name]	查看 ARP 表
show arp attack-detection	查看 ARP 攻击嫌疑主机信息

30.3 ARP 典型配置举例

30.3.1 配置 ARP 代理

-B -S -E -A

网络需求

- Device 分别与 PC1、PC2 直连。PC1、PC2 所在局域网的网络号一样，均为 10.0.0.0/16。
- Device 的接口 VLAN2 的 MAC 地址为 0001.7a13.0102。
- 通过 Device 的 ARP 代理，PC1 能 ping 通 PC2，且 PC1 能学习到 PC2 的 MAC 地址。

网络拓扑

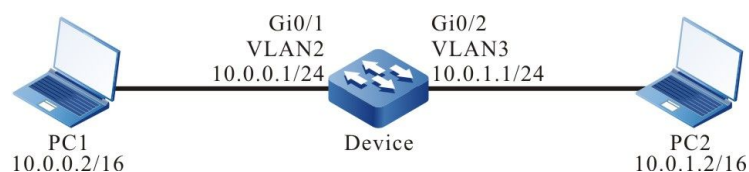


图 30-1 配置 ARP 代理组网图

配置步骤

步骤 1：配置 VLAN，并将端口加入对应 VLAN。（略）

步骤 2: 配置各接口的 IP 地址。 (略)

步骤 3: 检验结果。

PC1 ping PC2 的地址 10.0.1.2。

```
C:\Documents and Settings>ping 10.0.1.2

Pinging 10.0.1.2 with 32 bytes of data:

Reply from 10.0.1.2: bytes=32 time<1ms TTL=255
Reply from 10.0.1.2: bytes=32 time<1ms TTL=255
Reply from 10.0.1.2: bytes=32 time<1ms TTL=255
Reply from 10.0.1.2: bytes=32 time<1ms TTL=255

Ping statistics for 10.0.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

#查看 Device 的 ARP 表项。

```
Device#show arp
Protocol Address Age (min) Hardware Addr Type Interface Swithport
Internet 10.0.0.1 - 0001.7a13.0102 ARPA vlan2 ---
Internet 10.0.0.2 1 B8AC.6F2D.4498 ARPA vlan2 gigabitethernet0/1
Internet 10.0.1.1 - 0001.7a13.0103 ARPA vlan3 ---
Internet 10.0.1.2 1 4437.e603.0d63 ARPA vlan3 gigabitethernet0/2
```

#查看 PC1 的 ARP 表项。

```
C:\Documents and Settings>arp -a

Interface: 10.0.0.2 --- 0x5
Internet Address Physical Address Type
10.0.0.1 00-01-7a-13-01-02 dynamic
10.0.1.2 00-01-7a-13-01-02 dynamic
```

PC1 能 ping 通 PC2, 且 PC1 学习到了 PC2 的 MAC 地址。

说明:

- 设备缺省启用了 ARP 代理。
-

30.3.2 配置静态 ARP

-B -S -E -A

网络需求

- Device 与 PC 直连。
- PC 的 MAC 地址为 4437.e603.0d63。
- Device 上绑定 PC 的 IP 和 MAC 地址。
- PC 能 ping 通 Device 的接口 VLAN2 的地址。

网络拓扑

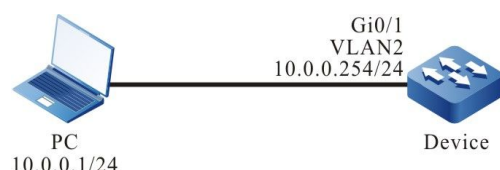


图 30-2 配置静态 ARP 组网图

配置步骤

步骤 1: 配置 VLAN,并将端口加入对应 VLAN。(略)

步骤 2: 配置各接口的 IP 地址。(略)

步骤 3: Device 上绑定 PC 的 IP 和 MAC 地址。

#配置 Device。

Device 绑定 PC 的 IP 和 MAC 地址。

```
Device(config)#arp 10.0.0.1 4437.e603.0d63
```

步骤 4: 检验结果。

#查看 Device 的 ARP 表项。

```
Device1#show arp
Protocol Address  Age (min) Hardware Addr  Type  Interface  Switchport
Internet 10.0.0.1  -   4437.e603.0d63  ARPA  vlan2  gigabitethernet0/1
Internet 10.0.0.254 -   0001.7a13.0102  ARPA  vlan2  ---
```

#PC ping Device 的接口 VLAN2 的地址 10.0.0.254。

```
C:\Documents and Settings>ping 10.0.0.254

Pinging 10.0.0.254 with 32 bytes of data:

Reply from 10.0.0.254: bytes=32 time<1ms TTL=255
```



```
Reply from 10.0.0.254: bytes=32 time<1ms TTL=255
Reply from 10.0.0.254: bytes=32 time<1ms TTL=255
Reply from 10.0.0.254: bytes=32 time<1ms TTL=255
```

```
Ping statistics for 10.0.0.254:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

PC 能 ping 通 Device 的接口 VLAN2 的地址 10.0.0.254。

31 IP 基础

31.1 IP 基础简介

Internet 网络协议 (IP) 是以数据包为基础的协议，用于在计算机网络之间交互数据。设备支持的协议包括：IP 协议、ICMP 协议、TCP 协议、UDP 协议和 Socket 等。

其中 IP 报文是整个 TCP/IP 协议栈的基础。IP 层负责处理 IP 报文的寻址、分片、重组、和协议信息的分解。作为网络层协议，IP 进行路由寻址和控制数据包的传递。

传输控制协议 (TCP) 和用户数据报协议 (UDP) 建立在 IP 协议的基础之上，分别提供基于连接的、可靠的数据传输服务和基于非连接的、不可靠的数据传输服务。

Internet 控制报文协议 (ICMP) 主要用于提供网络检测服务，并在网络层或传输层协议出现异常时提供差错报告，通知相应设备，以便进行网络的控制管理。

31.2 IP 基础功能配置

表 31-1 IP 基础功能配置列表

配置任务	
配置 IP 地址	配置接口 IP 地址
	配置接口无编号 IP 地址
配置 IP 协议基本功能	配置 IP 报文接收队列深度
	配置发送 IP 报文 TTL
	配置报文重组超时时间
	使能 IP 报文接收校验和检查
	配置发送 IP 报文计算校验和
	使能 IP 路由缓存
配置 ICMP 协议基本功能	使能全局 ICMP 重定向
	使能接口 ICMP 重定向
	使能 ICMP 目的不可达
	配置 ICMP 限速
配置 TCP 协议基本功能	配置 TCP 接收缓存大小
	配置 TCP 发送缓存大小
	配置 TCP 最大重传次数

配置任务	
	配置 TCP 最大报文段长度
	配置 TCP 最大往返时间
	配置 TCP 连接空闲时间
	配置 TCP 连接建立等待时间
	配置 TCP 最大保活次数
	使能 TCP 时间戳
	使能 TCP 选择性重传
配置 UDP 协议基本功能	配置 UDP 报文 TTL
	配置 UDP 接收缓存大小
	配置 UDP 发送缓存大小
	使能 UDP 校验和检查
	填充 UDP 报文校验和

31.2.1 配置 IP 地址

-B -S -E -A

IP 地址是一个 32 位数字，它用来唯一标识连接到 Internet 上运行 IP 协议的网络设备。

IP 地址由两部分组成：

- 网络号 (Net-id)：指定设备所在的网络；
- 主机号 (Host-id)：指定设备所在网络的主机编号。

为了便于 IP 地址的管理，IP 地址被分作五类，每类 IP 地址有其各自特有的功能：A~C 类 IP 地址用于地址分配、D 类 IP 地址用于组播应用、E 类 IP 地址用于试验目的。IP 地址分类及其范围如下表所示。

表 31-2 IP 地址分类及其范围

地址类型	可用网络地址范围	说明
A	1.0.0.0 ~ 127.0.0.0	网络号 127 用于环回接口
B	128.0.0.0 ~ 191.255.0.0	-
C	192.0.0.0 ~ 223.255.255.0	-
D	224.0.0.0 ~ 239.255.255.255	D 类地址用于组播
E	240.0.0.0 ~ 255.255.255.254	E 类地址用于试验目的

随着 Internet 的发展，IP 地址资源逐渐被消耗殆尽，而按类方式分配地址存在许多浪费的情况。于是出现了“子网”的概念。“子网”把 IP 地址中部分主机号用做子网号，这样一个大的网络就能够被划分为多个更小的子网，方便网络的规划和部署。

10.0.0.0 ~ 10.255.255.255、172.16.0.0 ~ 172.31.255.255 和 192.168.0.0 ~ 192.168.255.255 这三个地址段属于私有保留地址，不能分配到公网。

本节介绍配置接口 IP 地址和配置接口无编号 IP 地址。

配置条件

无

配置接口 IP 地址

IP 地址只能配置在支持 IP 协议的接口上。一个接口只允许配置一个主 IP 地址，但可以配置多个从 IP 地址。

表 31-3 配置接口 IP 地址

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
为接口配置 IP 地址	ip address <i>ip-address</i> { <i>network-mask</i> / <i>mask-len</i> } [secondary]	必选

说明：

- 一个接口只能配置一个主 IP 地址，新配置的主 IP 地址将替换原有的主 IP 地址。
- 配置从 IP 地址前，接口必须已经配置了主 IP 地址，最多可配置 100 个从 IP 地址。
- 不同接口的 IP 地址不能在同一网段，但同一接口的主从 IP 地址可以在同一网段。

配置接口无编号 IP 地址

IP 无编号是节省 IP 地址的一种方法。它可以借用其它接口的 IP 地址而不必单独分配。无编号的接口产生一个 IP 报文时，此报文的源 IP 地址是借用接口的主 IP 地址。为接口配置无编号 IP 地址时，需指定借用的接口，从而借用该接口的 IP 地址。

表 31-4 配置接口无编号 IP 地址

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-

步骤	命令	说明
配置接口无编号 IP 地址	ip unnumbered <i>reference-interface</i>	必选

说明：

- 所借用的接口必须已经配置了主 IP 地址，并且该接口不能配置无编号地址。
- 一个接口的主地址可以被多个接口借用，并且只有主 IP 地址能被借用。

31.2.2 配置 IP 协议基本功能

-B -S -E -A

在 TCP/IP 协议栈中，IP 协议是负责网络互连的网络层核心协议。IP 协议是一种无连接的协议，发送数据前，并不先建立连接。它尽最大努力交付报文，并不保证所有报文按序到达目的地。

配置条件

无

配置 IP 报文接收队列深度

设备收到的 IP 报文首先会被缓存到接口的 IP 接收队列，系统从该队列依次读取报文进行处理。当缓存的 IP 报文达到队列深度后，后续接收的 IP 报文将被丢弃。用户可根据网络突发 IP 报文情况，调整 IP 报文接收队列深度。

表 31-5 配置 IP 报文接收队列深度

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 IP 报文接收队列深度为指定值	ip option queue-length <i>queue-size</i>	必选

步骤	命令	说明
		缺省情况下，报文接收队列深度值为 200
配置 IP 报文接收队列深度为缺省值	default ip option queue-length	可选

配置发送 IP 报文 TTL

IP 报文头部包含生存时间 (TTL: Time-To-Live) 字段，每经过一个路由设备 TTL 减 1。当 TTL 为零时，设备丢弃这个 IP 报文。缺省情况下，设备发送 IP 报文的 TTL 值为 255，即该报文最多可经过 255 次转发。如果用户希望限制报文转发的次数，可以调整发送 IP 报文的 TTL 值。

表 31-6 配置发送 IP 报文 TTL

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置发送 IP 报文的 TTL 为指定值	ip option default-ttl ttl -value	必选 缺省情况下，发送 IP 报文的 TTL 值为 255
配置发送 IP 报文的 TTL 为缺省值	default ip option default-ttl	可选

配置报文重组超时时间

当 IP 报文在传输过程中被分片，并且分片报文到达目的地后，需要重组为一个完整的 IP 报文。在没有接收到所有分片之前，接收到的分片会被暂时缓存。如果重组超时并且所有分片还没有完全到达目的地，那么所属分片将会被丢弃。

表 31-7 配置报文重组超时时间

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置报文重组超时时间为指定值	ip option fragment-ttl <i>tvl-value</i>	必选 缺省情况下，报文重组超时时间值为 60，单位是 0.5 秒
配置分片报文重组超时时间为缺省值	default ip option fragment-ttl	可选

说明：

- 分片重组超时时间的单位是 0.5 秒。

使能 IP 报文校验和检查

对接收到的 IP 报文进行校验和检查。如果校验和错误，丢弃该报文。

表 31-8 使能 IP 报文校验和检查

步骤	命令	说明
进入全局配置模式	configure terminal	-
使能 IP 报文接收校验和检查	ip option rcv-checksum	必选 缺省情况下，该功能开启
配置接收到 IP 报文校验和检查处理方式为缺省	default ip option rcv-checksum	可选

使能 IP 路由缓存

当报文从 socket 发送到 IP 层时，如果目的地址与上一次一样，且路由是有效的，可以直接使用缓存中的路由，不用再进行路由查找。

表 31-9 使能 IP 路由缓存

步骤	命令	说明
进入全局配置模式	configure terminal	-
使能 IP 路由缓存	ip upper-cache	必选 缺省情况下，IP 路由缓存功能已开启

31.2.3 配置 ICMP 协议基本功能 **-B -S -E -A**

在 TCP/IP 协议栈中，Internet 控制报文协议（Internet Control Message Protocol）主要用于提供网络检测服务，并在网络层或传输层协议出现异常时，提供差错报告，通知相应设备，以便进行网络的控制管理。

配置条件

无

使能全局 ICMP 重定向

设备接收到需要转发的 IP 报文后，通过选路发现该报文的接收接口与发送接口相同，此时设备将此报文转发，并向源端回送 ICMP 重定向报文，通知源端重新选择正确的下一跳，进行后续报文的发送。缺省情况下，设备能够发送 ICMP 重定向报文，但在一些特定情况下，用户可以禁止设备发送 ICMP 重定向报文。

表 31-10 使能全局 ICMP 重定向

步骤	命令	说明
进入全局配置模式	configure terminal	-
使能全局 ICMP 重定向	ip redirect	必选 缺省情况下，全局 ICMP 重定向功能已关闭

使能接口 ICMP 重定向

在发送 ICMP 重定向报文时，如果要从接口上发送 ICMP 重定向报文，那么需要使能接口 ICMP 重定向功能。

表 31-11 使能接口 ICMP 重定向

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface interface-name	-
使能接口 ICMP 重定向	ip redirects	必选 缺省情况下，接口 ICMP 重定向功能已开启

说明：

- 需要同时使能全局 ICMP 重定向和接口 ICMP 重定向功能，才能发送 ICMP 重定向报文。

使能全局 ICMP 目的网络不可达

设备收到 IP 数据报文后，如果发生目的网络不可达的差错，则将该报文丢弃并向源端回送 ICMP 目的网络不可达差错报文。

- 对于转发的 IP 报文，如果查找路由失败，则向源端回送“网络不可达” ICMP 差错报文

表 31-12 使能 ICMP 目的网络不可达

步骤	命令	说明
进入全局配置模式	configure terminal	-
使能 ICMP 目的网络不可达	ip network unreachable reply	可选 缺省情况下，不开启 ICMP 目的网络不可达功能

使能 ICMP 目的不可达

设备收到 IP 数据报文后，如果发生目的不可达的差错，则将该报文丢弃并向源端回送 ICMP 目的不可达差错报文。

- 对于转发的 IP 报文，如果查找路由失败，则向源端回送“主机不可达” ICMP 差错报文。
- 对于可以进行转发的 IP 报文，如果需要将该 IP 报文分片，但该报文设置了不分片比特，则向源端发送“需要进行分片但设置了不可分片比特” ICMP 差错报文。
- 对于目的地址是本机的 IP 报文，如果设备不支持该报文的上一层协议，则向源端回送“协议不可达” ICMP 差错报文。
- 对于目的地址是本机的 IP 报文，如果该报文的传输层端口号与设备的进程监听的端口号不匹配，则向源端回送“端口不可达” ICMP 差错报文。

如果设备遭受到需要发送大量 ICMP 目的不可达报文的恶意攻击，会造成设备性能降低，并增大网络流量。为了避免这种情况，可以关闭设备的 ICMP 目的不可达报文发送功能。

表 31-13 使能 ICMP 目的不可达

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface interface-name	-
使能 ICMP 目的不可达	ip unreachable	可选 缺省情况下, ICMP 目的不可达功能已开启

配置 ICMP 限速

如果设备遭受到需要发送大量 ICMP 差错报文的恶意攻击时, 会造成设备性能降低, 并增大网络流量。为避免这种情况, 可以通过配置 ICMP 报文限速来处理。其中, ICMP 差错报文类型包括: 不可达报文、重定向报文、TTL 超时报文、参数错误报文, 这些报文的缺省限速速率为 10pps, 其他类型报文的缺省发送速率为 0, 即不限速。另外用户可单独配置各种不同类型的发送速率, 如没有配置则以缺省值为准。

表 31-14 配置 ICMP 限速

步骤	命令	说明
进入全局配置模式	configure terminal	-
开启 ICMP 限速	ip icmp ratelimit enable	必选 缺省情况下, 该功能开启
配置 ICMP 限速速率	ip icmp ratelimit { default pps / echo-reply { pps unlimit } 	必选

步骤	命令	说明
	mask-reply { <i>pps</i> unlimit } param-problem { <i>pps</i> unlimit } redirect { <i>pps</i> unlimit } time-exceed { <i>pps</i> unlimit } time-stamp-reply { <i>pps</i> unlimit } unreach { <i>pps</i> unlimit }	缺省情况下，ICMP 限速功能已开启

31.2.4 配置 TCP 协议基本功能

-B -S -E -A

在 TCP/IP 协议栈中，传输控制协议（Transmission Control Protocol）是面向连接的传输层协议。它在发送数据之前，需先建立连接，提供拥塞控制并保证可靠的数据传输。

配置条件

无

配置 TCP 接收缓存大小

在一些特定的网络环境中，可以通过同时配置 TCP 连接的接收和发送缓存大小，以使网络性能达到最佳。当没有配置 TCP 接收缓存大小时，接收缓存大小为缺省值。

表 31-15 配置 TCP 接收缓存大小

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 TCP 接收缓存大小	ip tcp rcvbufs <i>buff-size</i>	必选 缺省情况下，接收缓存大小为 8192 字节

配置 TCP 发送缓存大小

在一些特定的网络环境中，可以通过同时配置 TCP 连接的接收和发送缓存大小，以使网络性能达到最佳。当没有配置 TCP 发送缓存大小时，发送缓存大小为缺省值。

表 31-16 配置 TCP 发送缓存大小

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 TCP 发送缓存大小	ip tcp sendbuffers buff-size	可选 缺省情况下，发送缓存大小为 8192 字节

配置 TCP 最大重传次数

服务器发送 SYN-ACK 报文后，如果未收到客户端的应答报文，服务器将会重传此报文，如果重传次数超过系统规定的最大重传次数，系统将 TCP 连接断开。

表 31-17 配置 TCP 最大重传次数

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 TCP 最大重传次数	ip tcp retransmits retransmits-count	必选 缺省情况下，TCP 最大重传此为 3 次

配置 TCP 最大报文段长度

TCP 最大报文段长度是指 TCP 连接发送端传往接收端的最大数据块长度。当一个连接建立时，以双方各自通告的最大报文段长度的最小值，作为双方发送 TCP 报文时的最大报文段长度。当 TCP 报文超过最大报文段长度时，发送端需要进行分段发送。

表 31-18 配置 TCP 最大报文段长度

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 TCP 最大报文段长度	ip tcp segment-size <i>seg-size</i>	可选 缺省情况下，TCP 最大报文段长度为 512 字节

配置 TCP 最大往返时间

TCP 往返时间是指发送端从发送 TCP 报文开始到接收到应答报文所耗费的时间。当 TCP 连接建立时，配置的 TCP 最大往返时间将作为 TCP 往返时间的初始值。后续的 TCP 往返时间会根据实际的往返时间重新进行计算。缺省情况下，TCP 最大往返时间为 3 秒。

表 31-19 配置 TCP 最大往返时间

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 TCP 最大往返时间	ip tcp round-trip <i>round-trip-time</i>	必选 缺省情况下，TCP 最大往返时间为 3 秒

配置 TCP 连接空闲时间

TCP 连接建立后，如果一直没有数据交互，连接空闲时间超时后，TCP 将需要进行保活测试，当达到最大保活次数后，TCP 连接断开。缺省情况下，TCP 连接空闲时间为 2 小时。

表 31-20 配置 TCP 连接空闲时间

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 TCP 连接空闲时间	ip tcp idle-timeout <i>idle-time</i>	必选 缺省情况下，TCP 连接空闲时间为 14400，单位为 0.5 秒

说明：

- TCP 连接空闲时间单位为 0.5 秒。

配置 TCP 连接建立等待时间

TCP 连接建立需要进行三次握手，TCP 客户端在发送连接请求报文后需要等待 TCP 服务端的应答，以完成连接的建立。当建立连接的等待时间超时时，还没有收到应答，连接建立将被终止。缺省情况下，建立 TCP 连接的等待时间为 75 秒。

表 31-21 配置 TCP 连接建立等待时间

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 TCP 连接建立等待时间	ip tcp init-timeout <i>init-time</i>	必选 缺省情况下，建立 TCP 连接的等待时间为 150，单位为 0.5 秒

说明：

- TCP 连接建立等待时间单位为 0.5 秒。

配置 TCP 最大保活次数

当 TCP 连接没有数据交互的时间超过 TCP 连接空闲时间后，会发送 TCP 保活报文进行保活测试。如果保活测试失败，会再次进行保活测试，直到超过 TCP 最大保活次数时，该 TCP 连接将断开。缺省情况下，TCP 最大保活次数为 3 次。

表 31-22 配置 TCP 最大保活次数

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 TCP 最大保活次数	ip tcp keep-count <i>keep-count</i>	必选 缺省情况下，TCP 最大保活次数为 3 次

使能 TCP 时间戳

TCP 根据请求报文和应答报文的序列号会自动计算报文的往返时间，但是，这种计算方式存在不精确的缺陷。而 TCP 时间戳可以修正该问题。即发送端在报文中加入时间戳，接收端在应答报文中将该时间戳发回，发送端根据返回的时间戳计算报文往返时间。缺省情况下，该功能未启用。

表 31-23 使能 TCP 时间戳

步骤	命令	说明
进入全局配置模式	configure terminal	-
使能 TCP 时间戳	ip tcp timestamp	必选

步骤	命令	说明
		缺省情况下，该功能未启用

使能 TCP 选择性重传

如果 TCP 发送了一系列报文后，有一个报文传输失败，那么就需要将这一系列报文重传。而开启了 TCP 选择性重传后，则仅重新传输失败的那个报文，可以减小系统和线路的开销。缺省情况下，该功能未启用。

表 31-24 使能 TCP 选择性重传

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 TCP 选择性重传	ip tcp selective-ack	必选 缺省情况下，该功能未启用

31.2.5 配置 TCP 协议防攻击功能 **-B -S -E -A**

如果 TCP 服务器收到了大量的 SYN 报文但是对端不响应服务器的 SYN+ACK 回应。就会导致服务器的内存大量消耗，占用服务器的半连接队列，导致 TCP 服务器无法为正常的请求服务。针对这种攻击可以通过配置 TCP 防攻击功能来避免。

配置条件

无

使能 TCP syncache 功能

该功能是在收到 SYN 数据报文时不急于去分配 TCB，而是先回应一个 SYN ACK 报文，并在一个专用 HASH 表 (Cache) 中保存这种半开连接信息，直到收到正确的回应 ACK 报文再分配 TCB。

表 2-25 使能 TCP syncache 功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 TCP syncache 功能	ip tcp syncache	必选 缺省情况下，该功能未启用

使能 TCP syncookies 功能

该功能完全不使用任何存储资源，它使用一种特殊的算法生成 Sequence Number，这种算法考虑到了对方的 IP、端口、己方 IP、端口的固定信息，以及对方无法知道而己方比较固定的一些信息，如 MSS、时间等，在收到对方的 ACK 报文后，重新计算一遍，看其是否与对方回应报文中的 (Sequence Number-1) 相同，从而决定是否分配 TCB 资源

表 2-26 使能 TCP syncookies 功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 TCP syncookies 功能	ip tcp syncookies	必选 缺省情况下，该功能未启用

31.2.6 配置 UDP 协议基本功能

-B -S -E -A

在 TCP/IP 协议栈中，用户数据报协议 (User Datagram Protocol) 是面向无连接的传输层协议。它在发送数据之前，不需要建立连接，提供没有拥塞控制的不可靠的数据传输。

配置条件

无

配置手册

发布 1.1 04/2020

配置 UDP 报文 TTL

配置 UDP 报文 TTL 是指填充 UDP 报文 IP 头部的 TTL 值。IP 报文头部包含生存时间 (TTL: Time-To-Live) 字段, 每经过一个路由设备 TTL 减 1。当 TTL 为零时, 设备丢弃这个 IP 报文。缺省情况下, UDP 报文的 IP 头部 TTL 值为 64。

表 31-27 配置 UDP 报文 TTL

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 UDP 报文 TTL	ip udp default-ttl <i>time-to-live</i>	必选 缺省情况下, UDP 报文的 IP 头部 TTL 值为 64

配置 UDP 接收缓存大小

在一些特定的网络环境中, 可以通过同时配置 UDP 的接收和发送缓存大小, 以使网络性能达到最佳。当没有配置 UDP 接收缓存大小时, 接收缓存大小的缺省值为 41600 字节。

表 31-28 配置 UDP 接收缓存大小

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 UDP 接收缓存大小	ip udp rcvbufs <i>buffer-size</i>	必选 缺省情况下, UDP 接收缓存大小为 41600 字节

配置 UDP 发送缓存大小

在一些特定的网络环境中，可以通过同时配置 UDP 的接收和发送缓存大小，以使网络性能达到最佳。当没有配置 UDP 发送缓存大小时，发送缓存大小的缺省值为 9216 字节。

表 31-29 配置 UDP 发送缓存大小

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 UDP 发送缓存大小	ip udp sendbuffers buffer-size	必选 缺省情况下，UDP 发送缓存大小为 9216 字节

使能 UDP 校验和检查

为防止 UDP 报文在传输过程中出错，接收到 UDP 报文后，需进行 UDP 校验和检查。通过比较接收端计算的 UDP 报文校验和与 UDP 报文首部校验和字段，如果二者值不同，则认为传输出现错误，将该报文丢弃。缺省情况下，该功能已开启。

表 31-30 使能 UDP 校验和检查

步骤	命令	说明
进入全局配置模式	configure terminal	-
使能 UDP 接收校验和检查	ip udp recv-checksum	必选 缺省情况下，该功能已开启

填充 UDP 报文校验和

为防止 UDP 报文在传输过程中出错，发送 UDP 报文时，发送端需要将计算的 UDP 报文校验和填充到 UDP 报文首部校验和字段中，用以接收端进行校验和检查。缺省情况下，该功能已开启。

表 31-31 填充 UDP 报文校验和

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置发送 UDP 报文时填充报文校验和	ip udp send-checksum	必选 缺省情况下, 该功能已开启

31.2.7 IP 基础监控与维护

-B -S -E -A

表 31-32 IP 基础监控与维护

命令	说明
clear ip icmpstat	清除 ICMP 协议统计信息
clear ip statistics	清除 IP 协议统计信息
clear ip tcp syncache statistics	清除 TCP 协议 syncache 统计信息
clear ip tcpstat	清除 TCP 协议统计信息
clear ip udpstat	清除 UDP 协议统计信息
show ip icmpstat	显示 ICMP 协议统计信息
show ip interface [interface-name] brief]	显示接口 IP 地址信息
show ip sockets	显示 Socket 详细信息

命令	说明
show ip statistics	显示 IP 协议统计信息
show ip tcpstat	显示 TCP 协议统计信息
show ip tcp syncache statistics	显示 TCP syncache 统计信息
show ip udpstat	显示 UDP 协议统计信息
show ip tcp syncache detail	显示 TCP 协议 syncache 表项信息
show tcp tcb [detail]	显示 TCP 协议控制块信息

32 DHCP

32.1 DHCP 简介

当一个网络比较庞大时，它是很难以管理的，比如 IP 地址通过手工分配的网络环境中最常见的问题是 IP 地址冲突。处理这个问题的唯一方法是为主机动态分配 IP 地址。动态主机配置协议 DHCP 从一个地址池中把 IP 地址分配给请求主机。同时 DHCP 也能提供其它信息，如网关 IP、DNS 服务器地址等。DHCP 减轻了管理员跟踪记录手工分配 IP 地址的负担。

DHCP 是一个基于 UDP 广播的协议。DHCP 客户端从 DHCP 服务器端获取 IP 地址和其它配置信息的过程，主要通过四个阶段进行：

DISCOVER 阶段，当 DHCP 客户端第一次登录网络时，它会向网络发出一个 DHCP DISCOVER 报文，报文的源地址为 0.0.0.0，目的地址为 255.255.255.255；

OFFER 阶段，当 DHCP 服务器接收到客户端发出的 DHCP DISCOVER 广播报文后，它会根据策略，从对应的地址池中选择一个 IP 地址，与其它参数一起通过 DHCP OFFER 报文发送给客户端；

REQUEST 阶段，如果 DHCP 客户端收到网络上多台 DHCP 服务器的回应，只会挑选其中一个 DHCP OFFER（通常是最先抵达的那个），并且会向网络发送一个 DHCP REQUEST 报文，告诉所有 DHCP 服务器它将接受哪一台服务器提供的 IP 地址。

ACK 阶段，当 DHCP 服务器收到 DHCP 客户端的 DHCP REQUEST 请求报文后，它便向 DHCP 客户端发送一个包含它所提供的 IP 地址和其它配置的 DHCP ACK 确认信息，告诉 DHCP 客户端可以使用它所提供的 IP 地址。

DHCP 服务器分配给 DHCP 客户端的 IP 地址都有一个租约，期满后 DHCP 服务器便会收回分配的 IP 地址。当 DHCP 客户端的 IP 地址租约剩余一半时，DHCP 客户端会向 DHCP 服务器发送更新其 IP 租约的 DHCP REQUEST 报文。如果 DHCP 客户端可以继续使用该 IP 地址，则 DHCP 服务器回应 DHCP ACK 报文，通知 DHCP 客户端更新租约；如果 DHCP 客户端不可以继续使用该 IP 地址，则 DHCP 服务器回应 DHCP NAK 报文。

由于在 IP 地址动态获取过程中是采用广播方式发送请求报文，因此 DHCP 只适用于 DHCP 客户端与 DHCP 服务器处于同一子网内的情况。如果在一个网络中存在多个子网，而多个子网的主机都需要通过 DHCP 服务器来提供 IP 地址等配置信息时，则这些子网的主机可以通过 DHCP 中继设备来与 DHCP 服务器进行通信，最终获得 IP 地址及其它配置信息。

32.2 DHCP 功能配置

表 32-1 DHCP 功能配置列表

配置任务	
配置 DHCP 地址池	创建 DHCP 地址池可以指定 VRF 属性
	配置 IP 地址范围

	配置 DNS 服务器地址
	配置默认路由
	配置 IP 地址租期
	配置 IP、MAC 地址绑定
	配置用户自定义选项
	配置特定厂商地址池
配置 DHCP 服务器其它参数	配置 DHCP 服务器
	配置保留的 IP 地址范围
	配置 DHCP ping 探测参数
	配置 DHCP 数据日志功能
配置 DHCP 客户端功能	配置 DHCP 客户端
	配置厂商 ID
	配置 DHCP 路由距离
	配置 DHCP 60 选项功能
	配置 DHCP 客户端不请求默认路由选项
配置 DHCP 中继功能	配置接口 DHCP 中继
	配置 Option 82 功能
	配置接口 DHCP 中继报文源地址

	配置 DHCP 服务器地址
--	---------------

32.2.1 配置 DHCP 地址池

-S -E -A

配置条件

无

创建 DHCP 地址池

DHCP 服务器从 DHCP 地址池中为客户端选择并分配 IP 地址及其它相关参数，因此，DHCP 服务器必须先创建 DHCP 地址池。

表 32-2 创建 DHCP 地址池

步骤	命令	说明
进入全局配置模式	configure terminal	-
创建 DHCP 地址池并进入 DHCP 配置模式	ip dhcp pool <i>pool-name</i> [vrf <i>vrf-name</i>]	必选 缺省情况下，系统没有创建 DHCP 地址池

说明：

- 地址池有 Network 和 Range 两种地址池类型，可以分别通过 network 和 range 命令进行配置。

配置 IP 地址范围

在 DHCP 服务器上，每个 DHCP 地址池都应该配置相应的 IP 地址范围，以给 DHCP 客户端分配 IP 地址。

表 32-3 配置 IP 地址范围

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 DHCP 配置模式	ip dhcp pool <i>pool-name</i> [vrf <i>vrf-name</i>]	-
配置 Network 类型 IP 地址范围	network <i>ip-address</i> [<i>network-mask</i> <i>mask-len</i>]	可选 缺省情况下，地址池没有配置 IP 地址范围
配置 Range 类型 IP 地址范围	range <i>low-ip-address</i> <i>high-ip-address</i> [<i>network-mask</i> <i>mask-len</i>]	可选 缺省情况下，地址池没有配置 IP 地址范围

说明：

- 如果地址池先用 **network** 或 **range** 命令配置了地址池的 IP 地址范围，再执行 **network** 或 **range** 命令时会覆盖先前的 IP 地址范围配置。
- 修改地址池的 network 类型改为 range 类型(或者将 range 类型地址池改为 network 类型)，若新配置的地址范围和旧配置的地址范围存在交集，命令行会提示用户是否执行该操作，若是，会删除地址池下所有的地址配置(静态绑定、vendor 子池)和动态租约；若新配置的地址实际生效范围包含旧配置的地址实际生效范围，地址池会保留地址池下所有的地址配置(静态绑定、vendor 子池)，但是会删除 vendor 子池配置的 ip range 和动态租约。

配置 DNS 服务器地址

在 DHCP 服务器上，可以为每个 DHCP 地址池分别配置 DNS 服务器地址。DHCP 服务器在给 DHCP 客户端分配 IP 地址时，也将 DNS 服务器地址发送给客户端。

DHCP 客户端进行动态域名解析时，将向 DNS 服务器进行查询。

表 32-4 配置 DNS 服务器地址

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 DHCP 配置模式	ip dhcp pool <i>pool-name</i> [vrf <i>vrf-name</i>]	-
配置 DNS 服务器地址	dns-server { <i>ip-address</i> &<1-8> / autoconfig }	必选 缺省情况下，没有配置 DNS 服务器地址

配置默认路由

在 DHCP 服务器上，可以为每个 DHCP 地址池分别指定客户端对应的网关地址。在给客户端分配 IP 地址的同时，也将网关地址发送给客户端。

DHCP 客户端访问本网段以外的服务器或主机时，数据通过网关进行转发。

表 32-5 配置默认路由

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 DHCP 配置模式	ip dhcp pool <i>pool-name</i> [vrf <i>vrf-name</i>]	-
配置默认路由	default-router <i>ip-address</i> &<1-8>	必选 缺省情况下，没有配置默认路由

配置 IP 地址租期

DHCP 服务器分配给 DHCP 客户端的 IP 地址有一定的租借期限，当租借期满后服务器会收回该 IP 地址。如果 DHCP 客户端希望继续使用该地址，需要更新 IP 地址租约。

在 DHCP 服务器上，可以为每个 DHCP 地址池分别配置 IP 地址租期。

表 32-6 配置 IP 地址租期

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 DHCP 配置模式	ip dhcp pool <i>pool-name</i> [vrf <i>vrf-name</i>]	-
配置 IP 地址租期	lease <i>days</i> [<i>hours</i> [<i>minutes</i>]]	必选 缺省情况下， <i>days</i> 为 1， <i>hours</i> 为 6， <i>minutes</i> 为 0

配置 IP、MAC 地址绑定

配置 IP、MAC 地址绑定，当指定 MAC 地址的客户端向 DHCP 服务器请求分配 IP 地址时，DHCP 服务器将分配其绑定的 IP 地址。只要该客户端的 MAC 地址不变（如换网卡等），客户端每次从服务器获取的 IP 地址都是相同的。

表 32-7 配置 IP、MAC 地址绑定

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 DHCP 配置模式	ip dhcp pool <i>pool-name</i> [vrf <i>vrf-name</i>]	-

配置 IP、MAC 地址绑定	bind { <i>ip-address mac-address</i> automatic }	必选 缺省情况下，没有配置 IP、MAC 地址绑定
----------------	--	------------------------------

配置用户自定义选项

有些选项的内容，RFC 中没有做统一规定，因此用户根据自己的需要可以自定义选项及其内容。

表 32-8 配置用户自定义选项

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 DHCP 配置模式	ip dhcp pool <i>pool-name</i> [vrf <i>vrf-name</i>]	-
配置用户自定义选项	option <i>option-code</i> { ascii <i>ascii-string</i> hex <i>hex-string</i> ip <i>ip-address</i> &<1-8> }	必选 缺省情况下，没有配置用户自定义选项

配置 DHCP 厂商地址池

在客户端请求 ip 地址时，可能会携带 option60 选项，其中指明了厂商 ID。客户可以为不同的厂商指定不同的 ip 地址段。

表 32-9 配置 DHCP 厂商地址池

步骤	命令	说明
进入全局配置模式	configure terminal	-

进入 DHCP 配置模式	ip dhcp pool <i>pool-name</i> [vrf <i>vrf-name</i>]	-
配置厂商地址池, 进入 DHCP 厂商地址池配置模式	vendor-class-identifier <i>vendor_id</i>	缺省情况下, 没有配置厂商地址池
配置厂商地址池范围	ip range <i>low-ip-address</i> <i>high-ip-address</i>	缺省情况没有配置范围
配置为指定的厂商返回的 option 43 的内容	option 43 { ascii <i>ascii-string</i> hex <i>hex-string</i> ip <i>ip-address</i> &<1-8> }	缺省情况没有配置

32.2.2 配置 DHCP 服务器其它参数

-S -E -A

配置条件

无

配置 DHCP 服务器

配置在接口工作在 DHCP 服务器模式后, 当接口收到 DHCP 客户端发来的 DHCP 请求报文时, DHCP 服务器会为客户端分配 IP 地址和其他网络参数。

表 32-10 配置 DHCP 服务器

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-

配置 DHCP 服务器功能	ip dhcp server	必选 缺省情况下，没有配置 DHCP 服务器功能
---------------	-----------------------	-----------------------------

配置保留的 IP 地址范围

在 DHCP 地址池中，有一些 IP 地址是为某些特定设备预留的，有一些 IP 地址与网络上其他主机 IP 地址冲突，因此这些 IP 地址不能用于动态分配。

表 32-11 配置保留的 IP 地址范围

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置保留的 IP 地址范围	ip dhcp excluded-address <i>low-ip-address</i> [<i>high-ip-address</i>] [vrf <i>vrf-name</i>]	必选 缺省情况下，没有配置保留的 IP 地址范围 保留的 IP 地址范围内的 IP 地址不参与地址分配

配置 DHCP ping 探测参数

为防止 IP 地址冲突，DHCP 服务器在为 DHCP 客户端动态分配 IP 地址前，需要先对该 IP 地址进行探测。而探测是通过 ping 操作来进行的，根据检测能否在指定时间内收到 ICMP 回显响应报文来判断是否有 IP 地址冲突。

表 32-12 配置 DHCP ping 探测参数

步骤	命令	说明
进入全局配置模式	configure terminal	-

配置 DHCP ping 探测参数	ip dhcp ping { packets packet-num timeout milliseconds }	必选 缺省情况下, ping 包的个数为 1, 超时时间是 500ms
-------------------	---	--

配置 DHCP 数据日志功能

开启 DHCP 服务器的数据日志功能后, DHCP 服务器上地址池分配的情况将被记录至数据日志中。

表 32-13 配置 DHCP 服务开关

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 DHCP 服务器的数据日志功能开关	ip dhcp logging security-data	必选 缺省情况下, 未开启数据日志功能

32.2.3 配置 DHCP 客户端功能

-S -E -A

配置条件

无

配置 DHCP 客户端

DHCP 客户端的接口可以通过 DHCP 获取 IP 地址及其它参数。

表 32-14 配置 DHCP 客户端

步骤	命令	说明
进入全局配置模式	configure terminal	-

进入接口配置模式	interface <i>interface-name</i>	-
配置 DHCP 客户端获取地址	ip address dhcp [request-ip-address <i>ip-address</i>]	必选 缺省情况下, 没有配置 DHCP 客户端获取 IP 地址

配置 DHCP 路由距离

在 IP 路由表中各个协议都有控制选路的管理距离, 即路由距离。路由距离用于对来自不同协议的相同网段路由进行路由决策, 路由距离小的路由优先。

表 32-15 配置 DHCP 路由距离

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 DHCP 路由距离	ip dhcp route-distance <i>distance</i>	必选 缺省情况下, DHCP 路由距离为 254

配置 Option 60 功能

DHCP option 60 选项内容为厂商 ID, 在 DHCP 客户端请求过程中, 可以携带 option 60 选项。服务器可以根据该选项制定 ip 地址分配策略。

表 32-16 配置 DHCP option 60 功能

步骤	命令	说明
进入全局配置模式	configure terminal	-

进入接口配置模式	interface <i>interface-name</i>	-
配置 option 60 功能	ip dhcp vendor-class-identifier {disable content <i>hex-string</i>}	缺省情况为携带 option 60 选项

配置 DHCP 客户端不请求默认路由选项

在 DHCP 客户端请求 IP 地址的过程中默认会请求默认路由，用户可以指定 DHCP 客户端不请求默认路由从而自己配置路由。

表 32-17 配置 DHCP 客户端不请求默认路由选项

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 DHCP 客户端不请求默认路由选项	ip dhcp router-option disable	必选 缺省情况下，DHCP 客户端要请求默认路由选项

32.2.4 配置 DHCP 中继功能

-S -E -A

配置条件

无

配置 DHCP 中继

如果在一个网络中存在多个子网，而多个子网的主机都需要通过 DHCP 服务器来提供 IP 地址等配置信息时，则这些子网的主机可以通过 DHCP 中继设备来与 DHCP 服务器进行通信，最终获得 IP 地址及其它配置信息。如果配置接口工作在 DHCP 中继模式后，当接口收到 DHCP 客户端发来的 DHCP 报文时，会将报文中继到配置的 DHCP 服务器，由 DHCP 服务器来分配 IP 地址。

表 32-18 配置 DHCP 中继

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface interface-name	-
配置 DHCP 中继功能	ip dhcp relay	必选 缺省情况下，没有配置 DHCP 中继功能

配置 Option 82 功能

Option 82 选项称为中继信息选项，该选项记录了 DHCP 客户端的位置信息。如果配置开启 DHCP 中继支持 Option 82 选项功能，DHCP 中继收到 DHCP 客户端发送给 DHCP 服务器的请求报文后，并且该请求报文中没有带有 Option 82 选项，则在该请求报文中添加 Option 82 选项，并转发给 DHCP 服务器；如果配置开启 DHCP 中继支持 Option 82 选项功能，并且请求报文中已经携带了 Option 82 选项，则会根据 **ip dhcp relay information strategy** 命令配置的动作进行下一步处理，然后再将报文转发给服务器；如果 DHCP 中继收到的 DHCP 应答报文中含有 Option 82 选项，则会将 Option 82 选项删除后再转发给 DHCP 客户端。

表 32-19 配置 Option 82 功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置开启 DHCP 中继支持 Option 82 选项功能	ip dhcp relay information option	必选 缺省情况下，没有开启 DHCP 中继支持 Option 82 选项功能
配置 DHCP 中继收到来自客户端发来的含	ip dhcp relay information	可选

有 Option82 选项的请求报文时的处理策略	strategy {drop keep replace}	对于含有 Option 82 选项的报文使用 replace 动作
配置 Option 82 功能	ip dhcp relay information option remote-id { <i>ascii</i> <i>ascii-string</i> <i>hex</i> <i>hex-string</i> } / circuit-id { <i>ascii</i> <i>ascii-string</i> <i>hex</i> <i>hex-string</i> }	必选 缺省情况下, 没有配置 Option 82 功能

配置 DHCP 中继报文源地址

DHCP 中继 DHCP 客户端到服务器报文的源地址, 默认使用到 DHCP 服务器的路由出接口地址, 在某些特殊环境中 DHCP 服务器是不能与该地址通信的, 因此允许用户可以通过 **ip dhcp relay source-address** 命令用于配置 DHCP 中继发往 DHCP 服务器报文的源地址和报文中的 giaddr 字段; 也允许用户通过 **ip dhcp relay source-address relay-address** 命令配置 DHCP 中继源地址为收到 DHCP 客户端报文的接口地址。

表 32-20 配置 DHCP 中继报文源地址

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 DHCP 中继报文源地址	ip dhcp relay source-address relay-address	必选 缺省情况下, DHCP 中继报文源地址为到 DHCP 服务器的路由出接口地址
进入接口配置模式	interface <i>interface-name</i>	-

配置 DHCP 中继报 文源地址	ip dhcp relay source-address <i>ip- address</i>	必选 缺省情况下, DHCP 中继报文源地址为到 DHCP 服务器的路由 出接口地址
---------------------	--	--

说明:

- **ip dhcp relay source-address** *ip-address* 配置的源地址必须是本设备的接口地址, 同时接口地址必须与中继接口属于同一 vrf 下, 否则中继报文会发送失败。
- 若接口模式下配置了 **ip dhcp relay source-address** *ip-address* 命令以及全局模式下配置了 **ip dhcp relay source-address relay-address** 命令, 前者的优先级高于后者, DHCP 中继会将配置的 *ip-address* 填充 DHCP 中继发往 DHCP 服务器报文的源地址。

配置 DHCP 服务器地址

当接口收到 DHCP 客户端发来的 DHCP 报文时, 会将报文中继到配置的 DHCP 服务器, 由 DHCP 服务器来分配 IP 地址。

表 32-21 配置 DHCP 服务器地址

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface- name</i>	-
配置 DHCP 服务器地 址	ip dhcp relay server -address <i>ip-address</i>	必选 缺省情况下, 没有配 置 DHCP 服务器地址

表 32-22 DHCP 监控与维护

命令	说明
clear ip dhcp pool <i>pool-name</i> { lease conflict [<i>ip-address</i>] }	清除地址池下的动态租约信息或者出现地址冲突的地址信息
clear ip dhcp server interface [<i>interface-name</i>] statistics	清除 DHCP 服务器与客户端或者中继进行报文交互时的关键信息统计
clear ip dhcp relay statistics	清除 DHCP 中继设备上的统计信息
show ip dhcp server interface <i>interface-name</i> [statistics]	显示指定接口下关联的地址池信息或者显示指定接口下 DHCP 服务器与客户端或者中继进行报文交互时的关键信息统计
show ip dhcp pool <i>pool-name</i> { summary ping_list offer_list excluded_list conflict_list lease binding }	显示指定地址池的概要信息或者正在做 ping 检查的地址信息或者已经发送 OFFER 报文, 正在等待 DHCP 客户端回应 REQUEST 报文的地址信息或者显示地址池下被排除的地址信息或者显示地址池下出现地址冲突的地址信息或者显示地址池下动态租约信息或者显示地址池下静态绑定信息
show ip dhcp pool <i>pool-name</i> specific { ip-address <i>ip-</i>	显示地址池下指定 ip 地址或者 mac 地址的相关信息

<code>address mac-address mac-address }</code>	
<code>show ip dhcp relay [interface interface-name]</code>	显示 DHCP 中继设备上的报文统计信息。

32.3 DHCP 典型配置举例

32.3.1 配置 DHCP 服务器静态分配 IP 地址

-S -E -A

网络需求

- Device2 作为 DHCP 服务器，采用静态方式为客户端分配 IP 地址、网关 IP 地址、DNS 服务器 IP 地址。
- DHCP 服务器以 MAC 绑定方式为 PC 分配 IP 地址。

网络拓扑

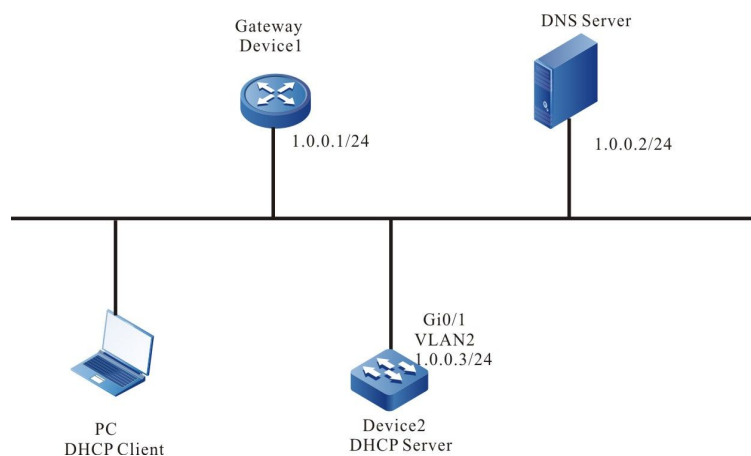


图 32-1 配置 DHCP 服务器静态分配 IP 地址组网图

配置步骤

步骤 1：配置 Device2 接口的 IP 地址并工作在 dhcp 服务器模式。

```
Device2#configure terminal
```



```
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ip address 1.0.0.3 255.255.255.0
Device2(config-if-vlan2)#ip dhcp server
Device2(config-if-vlan2)#exit
```

步骤 2: 配置静态绑定地址池及参数。

#配置地址池 mac-binding, 采用静态 mac 绑定方式为 PC 分配 IP 地址。

```
Device2(config)#ip dhcp pool mac-binding
Device2(dhcp-config)#range 1.0.0.4 1.0.0.254 255.255.255.0
Device2(dhcp-config)#bind 1.0.0.11 00e0.00c1.013d
Device2(dhcp-config)#default-router 1.0.0.1
Device2(dhcp-config)#dns-server 1.0.0.2
Device2(dhcp-config)#exit
```

步骤 3: 检验结果

#在 Device2 上通过 show ip dhcp server interface vlan2 命令查看接口关联地址池情况

```
Device2(config)#exit
Device2#show ip dhcp server interface vlan2
DHCP server status information:
DHCP server is enabled on interface: vlan2
Vrf : global
DHCP server pool information:
Available directly-connected pool:
Interface IP      Pool name      Pool Range      Pool utilization
-----
1.0.0.3/24      mac-binding    1.0.0.4 – 1.0.0.254    0.00%
```

#在 Device2 上通过 show ip dhcp pool mac-binding binding 命令查看为 PC 分配的绑定

IP 地址。

```
Device2#show ip dhcp pool mac-binding binding
IP Address      MAC Address      Vendor Id      Type      Time Left(s)
-----
1.0.0.11      00e0.00c1.013d    Global      Binding    NA
```

#在 Device2 上通过 show ip dhcp pool mac-binding lease 命令查看为 PC 分配的地址。

```
Device#show ip dhcp pool danymic-pool2 lease
IP Address      MAC Address      Vendor Id      Type      Time Left(s)
-----
1.0.0.11      00e0.00c1.013d    Global      Lease    107980
```

在 PC 上检查获取到的 IP 地址、网关 IP 地址、DNS 服务器地址正确。

网络需求

- Device 的两个接口 vlan2、vlan3 分别配置 IP 地址 1.0.0.3/24 和 2.0.0.3/24。
- DHCP 服务器 Device 为两个直连物理网络内的客户端分别动态分配 1.0.0.0/24 和 2.0.0.0/24 网段的 IP 地址。
- 网段 1.0.0.0/24 内的地址租期为 1 天，网关为 1.0.0.3，DNS 服务器地址为 2.0.0.4；网段 2.0.0.0/24 内的地址租期为 3 天，网关地址为 2.0.0.3，DNS 服务器地址为 2.0.0.4。
- 网段 1.0.0.0/24 和网段 2.0.0.0/24 内前 10 个 IP 地址保留不被分配

网络拓扑

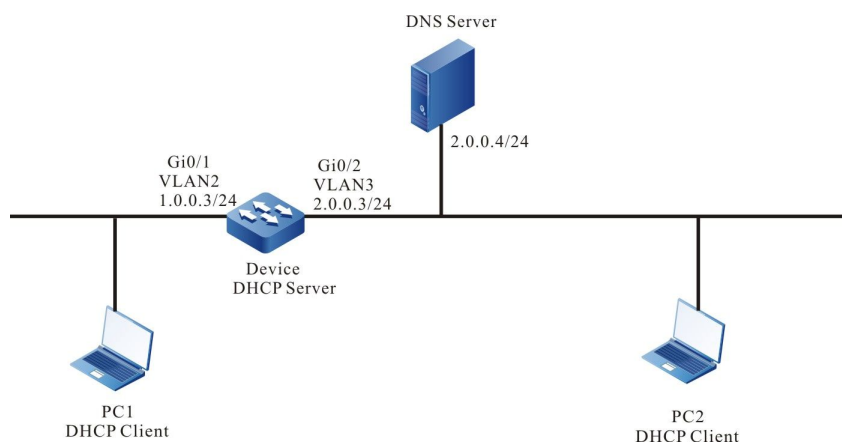


图 32-2 DHCP 动态分配 IP 地址组网图

配置步骤

步骤 1：配置 Device 各接口的 IP 地址并使接口工作在 dhcp 服务器模式。

```
Device(config)#interface vlan2
Device(config-if- vlan2)#ip address 1.0.0.3 255.255.255.0
Device(config-if- vlan2)#ip dhcp server
Device(config-if- vlan2)#exit
Device(config)#interface vlan3
Device(config-if- vlan3)#ip address 2.0.0.3 255.255.255.0
Device(config-if- vlan3)#ip dhcp server
Device(config-if- vlan3)#exit
```

步骤 2：在 DHCP 服务器 Device 上配置 2 个动态地址池及其参数。

#配置两个地址池中前 10 个 IP 地址作为保留地址

```
Device(config)#ip dhcp excluded-address 1.0.0.1 1.0.0.10
Device(config)#ip dhcp excluded-address 2.0.0.1 2.0.0.10
```

#配置名为 dynamic-pool1 的地址池及参数（地址范围、网关、dns 地址、地址租期）。

```
Device(config)#ip dhcp pool dynamic-pool1
Device(dhcp-config)#network 1.0.0.0 255.255.255.0
Device(dhcp-config)#default-router 1.0.0.3
Device(dhcp-config)#dns-server 2.0.0.4
Device(dhcp-config)#lease 1 0 0
Device(dhcp-config)#exit
```

#配置名为 dynamic-pool2 的地址池及参数（地址范围、网关、dns 地址、地址租期）。

```
Device(config)#ip dhcp pool dynamic-pool2
Device(dhcp-config)#network 2.0.0.0 255.255.255.0
Device(dhcp-config)#default-router 2.0.0.3
Device(dhcp-config)#dns-server 2.0.0.4
Device(dhcp-config)#lease 3 0 0
Device(dhcp-config)#exit
```

步骤 3: 检验结果

#查看 Device 上服务器关联地址池的信息。

```
Device(config)#exit
Device#show ip dhcp server interface vlan2
DHCP server status information:
DHCP server is enabled on interface: vlan2
Vrf : global
DHCP server pool information:
Available directly-connected pool:
Interface IP      Pool name      Pool Range      Pool utilization
-----
1.0.0.3/24      dynamic-pool1  1.0.0.0 – 1.0.0.255  0.00%
Device#show ip dhcp server interface vlan3
DHCP server status information:
DHCP server is enabled on interface: vlan3
Vrf : global
DHCP server pool information:
Available directly-connected pool:
Interface IP      Pool name      Pool Range      Pool utilization
-----
1.0.0.3/24      dynamic-pool2  2.0.0.0 – 2.0.0.255  0.00%
```

#查看 Device 上为客户端分配的 IP 地址信息。

```
Device#show ip dhcp pool danymic-pool1 lease
IP Address      MAC Address      Vendor Id      Type      Time Left(s)
-----
1.0.0.11       0001.7a6a.0268   Global        Lease    86390
Device#show ip dhcp pool danymic-pool2 lease
IP Address      MAC Address      Vendor Id      Type      Time Left(s)
-----
2.0.0.11       0001.7a6a.0269   Global        Lease    259194
```

#查看 Device 上配置的 IP 地址池的分配统计信息。

```
Device#show ip dhcp pool dynamic-pool1 summary
Pool: dynamic-pool1
Pool Configuration : 1.0.0.0 255.255.255.0
Pool Range       : 1.0.0.0 1.0.0.255
Pool Utilization : 0.39%
VRF              : global
DNS Server       : 2.0.0.4
Default Router   : 1.0.0.3
Lease Time       : 1 Days 0 Hours 0 Minutes
Free Addresses   : 243
Static Bind      : 0
Lease Count      : 1
PingList         : 0
OfferList        : 0
ConflictList     : 0
ExcludeList      : 12
```

```
Device#show ip dhcp pool dynamic-pool2 summary
Pool: dynamic-pool2
Pool Configuration : 2.0.0.0 255.255.255.0
Pool Range       : 2.0.0.0 2.0.0.255
Pool Utilization : 0.39%
VRF              : global
DNS Server       : 2.0.0.4
Default Router   : 2.0.0.3
Lease Time       : 3 Days 0 Hours 0 Minutes
Free Addresses   : 243
Static Bind      : 0
Lease Count      : 1
PingList         : 0
OfferList        : 0
ConflictList     : 0
ExcludeList      : 12
```

在 DHCP 客户端上查看 IP 地址获取正确。

说明:

- 地址池内的 IP 地址必须属于提供服务的接口的网段范围。
-

32.3.3 配置 DHCP 中继

-S -E -A

网络需求

- Device1 为 DHCP 服务器，Device2 接口启用 DHCP 中继功能。
- DHCP 服务器为 1.0.0.0/24 网段的客户端提供服务，保留前 10 个 IP 地址。
- DHCP 客户端通过 DHCP 中继获取 IP 地址。

网络拓扑

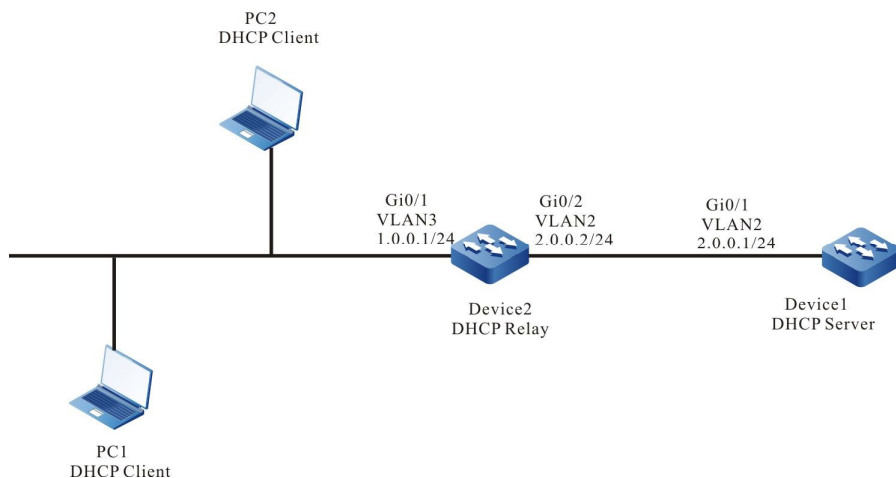


图 32-3 配置 DHCP 中继组网图

配置步骤

步骤 1: 配置 VLAN，并将端口加入对应的 VLAN。并配置各接口 IP 地址（略）

步骤 2: 配置 Device1 的 IP 地址池及保留的 IP 地址，并工作在 dhcp 服务器模式。

#配置 dhcp 服务器。

```
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip dhcp server
Device1(config-if-vlan2)#exit
```

#配置 1.0.0.1 至 1.0.0.10 的 IP 地址不被分配。

```
Device1#configure terminal
Device1(config)#ip dhcp excluded-address 1.0.0.1 1.0.0.10
```

#配置 Device1 的 IP 地址池 dynamic-pool。

```
Device1(config)#ip dhcp pool dynamic-pool
Device1(dhcp-config)#network 1.0.0.0 255.255.255.0
Device1(dhcp-config)#default-router 1.0.0.1
Device1(dhcp-config)#lease 1 0 0
Device1(dhcp-config)#exit
```

#配置到网段 1.0.0.0/24 的静态路由。

```
Device1(config)#ip route 1.0.0.0 255.255.255.0 2.0.0.2
```

步骤 3: 在 Device2 的 vlan3 接口上配置 DHCP 服务器地址为 2.0.0.1，并使接口工作在中继模式。

```
Device2(config)#interface vlan3
Device2(config-if-vlan3)#ip dhcp relay
Device2(config-if-vlan3)#ip dhcp relay server-address 2.0.0.1
Device2(config-if-vlan3)#exit
```

步骤 4: 检验结果

#查看 Device1 上分配的 IP 地址信息

```
Device1#show ip dhcp pool dynamic-pool lease
IP Address      MAC Address      Vendor Id      Type      Time Left(s)
-----
1.0.0.11       0001.7a6a.0268   Global         Lease     86387
```

使用 show ip dhcp pool dynamic-pool lease 命令查看为客户端分配的 IP 地址信息, 说

明客户端已经获取到 IP 地址 1.0.0.11。

32.3.4 配置 DHCP 中继支持 Option82 选项

-S -E -A

网络需求

- 在 DHCP 中继设备上启用 Option82 选项。
- 对于 Option82 子选项 Remote ID 内容指定为 0102030405。
- 中继设备 Device2 将在请求报文中添加 Option82 选项, 然后转发给 DHCP 服务器, 然后 DHCP 服务器为客户端分配 1.0.0.0/24 网段内的 IP 地址。

网络拓扑

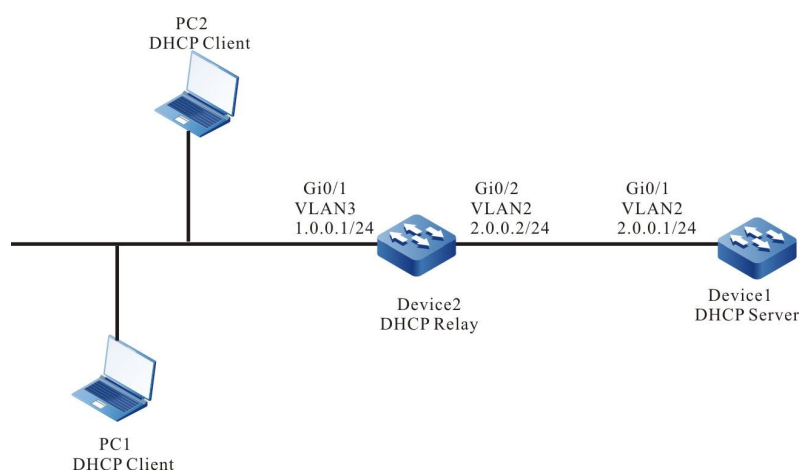


图 32-4 配置 DHCP 中继支持 Option82 选项组网图

配置步骤

步骤 1: 配置 VLAN, 并将端口加入对应的 VLAN。并配置各接口的 IP 地址。(略)

步骤 2: 配置 DHCP 服务器。

```
Device1# configure terminal
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip dhcp server
Device1(config-if-vlan2)#exit
Device1(config)#ip dhcp pool dynamic-pool
Device1(dhcp-config)#network 1.0.0.0 255.255.255.0
Device1(dhcp-config)#default-router 1.0.0.1
Device1(dhcp-config)#exit
```

#配置到网段 1.0.0.0/24 的静态路由。

```
Device1(config)#ip route 1.0.0.0 255.255.255.0 2.0.0.2
```

步骤 3: 配置 DHCP 中继设备 Device2 及 Option82 选项参数。

#配置 DHCP 中继服务器 IP 地址为 2.0.0.1。

```
Device2(config)#interface vlan3
Device2(config-if-vlan3)#ip dhcp relay
Device2(config-if-vlan3)#ip dhcp relay server-address 2.0.0.1
```

#启用 Option82 选项, 并配置子选项 remote-ID 为 0102030405。

```
Device2(config)#ip dhcp relay information option
Device2(config)#ip dhcp relay information remote-id hex 0102030405
```

步骤 4: 检验结果

查看 Device1 上为客户端分配的 IP 地址信息。

```
Device1#show ip dhcp pool danymic-pool1 lease
IP Address      MAC Address      Vendor Id      Type      Time Left(s)
-----
1.0.0.2         0001.7a6a.0268   Global         Lease     107992
```

在 DHCP 客户端上查看网卡已经获取到 1.0.0.0/24 网段的某个 IP 地址。

在 DHCP 服务器端抓包可以验证服务器收到的 discover 报文中 option82 的

remote-id 的填充值为 0102030405。

说明:

- 在启用 Option82 选项后, 其子选项 Circuit ID 填充内容为接收接口索引和中继设备系统 ID
-

33 DNS

33.1 DNS 简介

DNS 是域名系统 (Domain Name System) 的缩写, 是一个将域名和 IP 地址相互映射的分布式数据库, 并提供域名和 IP 地址之间的相互转换。通过 DNS, 用户访问互联网时, 可以直接使用便于记忆的、有意义的域名, 而由网络中的域名服务器将域名解析为正确的 IP 地址。域名解析分为静态域名解析和动态域名解析。

静态域名解析通过静态域名解析表进行, 即手动建立域名和 IP 地址之间的对应关系表, 将一些常用的域名加入表中, 当客户端需要域名所对应的 IP 地址时, 首先到静态域名解析表中进行查找, 获得所对应的 IP 地址, 从而提高域名解析的效率。

动态域名解析是通过查询域名服务器来完成的。DNS 客户端向域名服务器发出域名解析请求, 域名服务器收到域名解析请求后, 首先判断请求的域名是否处于自己被授权管理的子域内, 如果是, 就从数据库中查询域名对应的 IP 地址, 并将查询结果发送给客户端; 如果域名不处于自己被授权管理的子域内, 域名服务器或通过递归解析方式向其他域名服务器进行解析, 并将解析结果发送给客户端; 或在给客户端的响应报文指明下一个域名服务器的地址, 从而客户端再向该域名服务器发起域名解析请求, 即通常所说的迭代解析方式。

33.2 DNS 功能配置

表 33-1 DNS 功能配置列表

配置任务	
配置 DNS 缓存规格	配置静态缓存最大规格数
	配置动态缓存最大规格数
配置 DNS 客户端功能	配置静态域名解析
	配置动态域名解析
配置 DNS 探测功能	配置域名列表
	探测域名解析

33.2.1 配置 DNS 缓存规格

-B -S -E -A

配置条件

无

配置 DNS 规格

修改 DNS 最大支持的规格，若当前规格为 M,当前个数为 n；配置的规格为 N;有以下场景：

1. 静态规格，若 $N > M$ 或 $n < N < M$;则配置立即生效；若 $N < n$;则提示配置失败
2. 动态规格，若 $N > M$ 或 $n < N < M$;则配置立即生效；若 $N < n$;配置生效，等待动态个数老化。

表 33-2 配置特权模式认证方法列表

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置静态 dns 可支持配置的最大规格数	dns static max-count <i>number</i>	可选 缺省情况下，静态缓存最大支持 64
配置动态 dns 缓存可支持配置的最大规格数	dns dynamic max-count <i>number</i>	可选 缺省情况下，动态缓存最大支持 10K

33.2.2 配置 DNS 客户端功能

-B -S -E -A**配置条件**

无

配置静态域名解析

配置静态域名解析即是通过配置将域名与 IPv4 地址和 IPv6 地址相对应。

表 33-3 配置静态域名解析

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置域名和对应的 IPv4 地址	ip host [<i>vrf vrf-name</i>] <i>domain-name ip-address</i>	必选 缺省情况下，没有配置域名和对应的 IPv4 地址

步骤	命令	说明
配置静态域名对应的 IPv6 地址	ipv6 host [<i>vrf vrf-name</i>] <i>domain-name</i> <i>ipv6-address</i>	必选 缺省情况下, 没有配置域名和对应的 IPv6 地址

配置动态域名解析

配置动态域名解析, 需要配置域名服务器 IP 地址, 这样才能将域名解析请求发送到正确的域名服务器进行解析。

用户还可以先配置域名后缀, 当使用域名时, 可以只输入域名的部份字段, 由系统自动加上预先配置的域名后缀进行解析。

表 33-4 配置动态域名解析

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置域名后缀	ip domain-name [<i>vrf vrf-name</i>] <i>domain-name</i>	必选 缺省情况下, 没有配置域名后缀
配置 DNS 服务器地址	ip name-server [<i>vrf vrf-name</i>] <i>ip-address</i>	必选 缺省情况下, 没有配置 DNS 服务器地址

33.2.3 配置 DNS 探测功能

-B -S -E -A

配置条件

无

配置域名列表

通过配置域名列表，可以将一些常用的域名加入到域名列表中保存，需要使用时，直接指定域名列表的名称即可。

表 33-5 配置域名列表

步骤	命令	说明
进入全局配置模式	configure terminal	-
创建域名列表并进入域名列表配置模式	dns domain-list <i>list-name</i>	必选 缺省情况下，没有配置域名列表
配置域名	domain <i>domain-name</i>	必选 缺省情况下，域名列表下没有配置域名

探测域名解析

通过探测域名解析，可以检测 DNS 服务器能否正确解析指定的域名。

表 33-6 探测域名解析

步骤	命令	说明
探测域名解析	dns query [vrf <i>vrf-name</i>] <i>ip-address</i> [name <i>domain-name</i> name-list <i>list-name</i>] [timeout <i>time</i>]	必选 缺省情况下，不探测域名解析

33.2.4 DNS 监控与维护

-B -S -E -A

表 33-7 DNS 监控与维护

命令	说明
debug dns {all config event mpos packet timer}	打开 DNS 调试信息开关
show dns domain-list [list-name]	显示域名列表
show hosts	显示域名解析表表项
show name-server [vrf vrf-name]	显示 DNS 服务器信息

33.3 DNS 典型配置举例

33.3.1 配置静态域名解析

-B -S -E -A

网络需求

- Device 与 PC 互联，路由可达。
- PC 主机名为 host.xxyyz.com，对应 IP 地址为 1.0.0.2/24。
- 在 Device 上通过静态域名解析访问主机 host.xxyyz.com。

网络拓扑

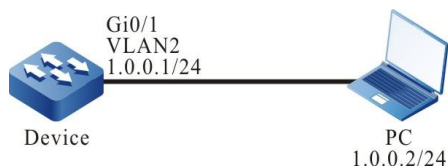


图 33-1 配置静态域名解析组网图

配置步骤

步骤 1: 配置 VLAN, 并将端口加入对应的 VLAN。 (略)

步骤 2: 配置各接口的 IP 地址。 (略)

步骤 3: 配置静态域名。

#在 Device 上配置主机名 host.xxyzz.com 对应的 IP 地址为 1.0.0.2。

```
Device#configure terminal
Device(config)#ip host host.xxyzz.com 1.0.0.2
Device(config)#exit
```

步骤 4: 检验结果。

#在 Device 上 ping 主机名 host.xxyzz.com, Device 通过本地域名解析出主机名对应 IP 地址为 1.0.0.2。

```
Device#ping host.xxyzz.com
Translating "host.xxyzz.com" for IPv6

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 1.0.0.2 , timeout is 2 seconds:
!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/6/16 ms.
```

说明:

- ping 主机名时首先会解析该主机名的 IPv6 地址, 然后解析 IPv4 地址。
-

33.3.2 配置动态域名解析

-B -S -E -A

网络需求

- DNS 服务器 IP 地址为 1.0.0.3/24, Device 的 IP 地址为 1.0.0.1/24, PC 的 IP 地址为 1.0.0.2/24。

- DNS 服务器、Device 和 PC 通过局域网互联，路由可达。DNS 服务器上设置 host.xxyzz.com 与 1.0.0.2 的 DNS 记录。
- Device 通过 DNS 服务器动态解析 host.xxyzz.com 访问 PC。

网络拓扑

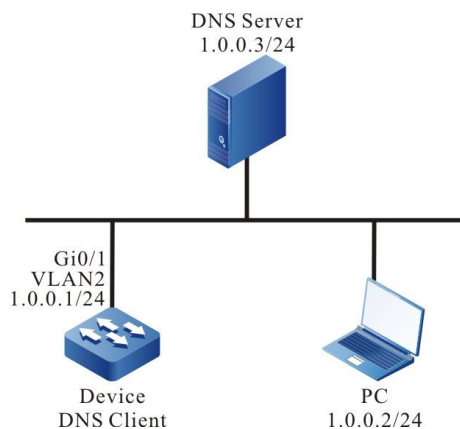


图 33-2 配置动态域名解析组网图

配置步骤

步骤 1： 配置 VLAN，并将端口加入对应的 VLAN。（略）

步骤 2： 配置各接口的 IP 地址。（略）

步骤 3： 配置 DNS 服务器。（略）

步骤 4： 配置 DNS 客户端。

#为客户端指定 DNS 服务器，IP 地址为 1.0.0.3。

```
Device#configure terminal
Device(config)#ip name-server 1.0.0.3
Device(config)#exit
```

步骤 5： 检验结果。

#在 Device 上 ping 主机名 host.xxyzz.com，Device 通过 DNS 服务器解析出主机名对应 IP 地址为 1.0.0.2。

```
Device#ping host.xxyzz.com
```

```
Press key (ctrl + shift + 6) interrupt it.  
Sending 5, 76-byte ICMP Echos to 1.0.0.2 , timeout is 2 seconds:  
!!!!  
Success rate is 100% (5/5). Round-trip min/avg/max = 0/6/16 ms.
```

34 IPv6 基础

34.1 IPv6 基础简介

IPv6 (Internet Protocol Version 6, 因特网协议版本 6) 是网络层协议的第二代标准协议, 也被称为 IPng (IP Next Generation, 下一代因特网), 它是 IETF (Internet Engineering Task Force, Internet 工程任务组) 设计的一套规范, 是 IPv4 的升级版本。

34.2 IPv6 基础功能配置

表 34-1 IPv6 基础功能配置列表

配置任务	
配置 IPv6 地址	配置接口 IPv6 地址
配置 IPv6 基本功能	开启 IPv6 单播转发功能
	开启接口 IPv6 功能
	配置 IPv6 报文跳数限制值
	配置接口的 IPv6 MTU

配置任务	
配置 IPv6 邻居发现协议	配置 IPv6 静态邻居
	配置 STALE 状态 IPv6 邻居表项的老化时间
	配置 NS 报文的重传时间间隔
	配置 IPv6 重复地址检测时发送 NS 报文的次数
	配置 RA 报文的相关参数
	开启接口发送重定向报文功能
配置 ICMPv6 功能	配置 ICMPv6 差错报文发送速率
	开启 ICMPv6 目的不可达报文的发送功能
配置 IPv6 TCP 防攻击功能	开启 TCP syncache 功能
	开启 TCP syncookies 功能

34.2.1 配置接口 IPv6 地址

-B -S -E -A

IPv6 和 IPv4 之间最显著的区别为：IP 地址的长度从 32 比特增加到 128 比特。IPv6 地址被表示为以冒号 (:) 分隔的一连串 16 比特的十六进制数。每个 IPv6 地址被分为 8 组，每组的 16 比特用 4 个十六进制数来表示，组和组之间用冒号隔开，比如：2000:0000:240F:0000:0000:0CB0:123A:15AB。

为了简化 IPv6 地址的表示，对于 IPv6 地址中的“0”可以有下面的处理方式：

- 每组中的前导“0”可以省略，即上述地址可表示为 2000:0:240F:0:0:CB0:123A:15AB。
- 如果地址中包含连续两个或多个均为 0 的组，则可以用双冒号“::”来代替，即上述地址可表示为 2000:0:240F::CB0:123A:15AB。

- 在一个 IPv6 地址中只能使用一次双冒号 "::"，否则当设备将 "::" 转变为 0 以恢复 128 位地址时，将无法确定 "::" 所代表的 0 的个数。

IPv6 地址由两部分组成：地址前缀与接口标识。其中，地址前缀相当于 IPv4 地址中的网络号字段，接口标识相当于 IPv4 地址中的主机号字段。

IPv6 地址前缀的表示方式为：IPv6 地址/前缀长度。其中，IPv6 地址是前面所列出的任一形式，而前缀长度是一个十进制数，表示 IPv6 地址前面多少位为地址前缀。

IPv6 地址分为三种类型：单播地址、组播地址和任播地址。

- 单播地址：用来唯一标识一个接口，类似于 IPv4 的单播地址。发送到单播地址的数据报文将被传送给此地址所标识的接口。
- 组播地址：用来标识一组接口，类似于 IPv4 的组播地址。发送到组播地址的数据报文被传送给此地址所标识的所有接口。
- 任播地址：用来标识一组接口，目标为一个任播地址的分组只会被送到那个组中的一个接口中去。根据路由选择协议，接收分组的接口是离源最近的接口。

IPv6 地址类型是由地址前面几位来指定的，称为格式前缀，主要地址类型与格式前缀的对应关系如表 1-2 所示。

表 34-2 IPv6 地址类型与格式前缀的对应关系

地址类型		格式前缀（二进制）	前缀标识
单播地址	未指定地址	00...0 (128 bits)	::/128
	环回地址	00...1 (128 bits)	::1/128
	链路本地地址	1111111010	FE80::/10
	站点本地地址	1111111011	FEC0::/10
	全球单播地址	其他形式	-

地址类型	格式前缀（二进制）	前缀标识
组播地址	11111111	FF00::/8
任播地址	从单播地址空间中进行分配，使用单播地址的格式	

IPv6 单播地址的类型可有多种，包括全球单播地址、链路本地地址和站点本地地址等。

- 全球单播地址等同于 IPv4 公网地址，提供给网络服务提供商。这种类型的地址允许路由前缀的聚合，从而限制了全球路由表项的数量。
- 链路本地地址用于邻居发现协议和无状态自动配置中链路本地节点之间的通信。使用链路本地地址作为源或目的地址的数据报文不会被转发到其他链路上。
- 站点本地地址与 IPv4 中的私有地址类似。使用站点本地地址作为源或目的地址的数据报文不会被转发到本站点外的其它站点。
- 环回地址：单播地址 0:0:0:0:0:0:0:1（简化表示为::1）称为环回地址，不能分配给任何物理接口。它的作用与在 IPv4 中的环回地址相同，即节点用来给自己发送 IPv6 报文。
- 未指定地址：地址 “::” 称为未指定地址，不能分配给任何节点。在节点获得有效的 IPv6 地址之前，可在发送的 IPv6 报文的源地址字段填入该地址，但不能作为 IPv6 报文中的目的地址。

IPv6 预留的特殊用途的组播地址如表 1-3 所示。

表 34-3 IPv6 特殊用途组播地址列表

地址	用途
FF01::1	表示节点本地范围所有节点的组播地址
FF02::1	表示链路本地范围所有节点的组播地址

地址	用途
FF01::2	表示节点本地范围所有路由器的组播地址
FF02::2	表示链路本地范围所有路由器的组播地址
FF05::2	表示站点本地范围所有路由器的组播地址

配置条件

无

配置接口 IPv6 地址

表 34-4 配置接口 IPv6 地址

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置接口 IPv6 地址	ipv6 address { <i>linklocal-address link-local</i> <i>prefix-address</i> [anycast eui-64] autoconfig }	必选 缺省情况下，接口没有配置 IPv6 地址

说明：

- 接口可以配置多个 IPv6 地址。

- 接口配置 IPv6 地址后，自动使能 IPv6 功能。

34.2.2 配置 IPv6 基本功能

-B -S -E -A

配置条件

无

开启 IPv6 单播转发功能

缺省情况下，IPv6 单播转发功能处于开启状态。在某些特定情况下，用户可以关闭 IPv6 单播转发功能，关闭该功能后，不转发 IPv6 报文。

表 34-5 开启 IPv6 单播转发功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
开启 IPv6 单播转发功能	ipv6 unicast-routing	必选 缺省情况下，IPv6 单播转发功能处于开启状态

开启接口 IPv6 功能

在接口上进行 IPv6 的相关配置前，必须先开启 IPv6 功能，否则可能导致某些配置不生效。

表 34-6 开启接口 IPv6 功能

步骤	命令	说明
进入全局配置模式	configure terminal	-

进入接口配置模式	interface <i>interface-name</i>	-
开启接口 IPv6 功能	ipv6 enable	必选 缺省情况下，接口 IPv6 功能处于关闭状态

配置 IPv6 报文跳数限制值

IPv6 报文头部包含跳数限制（Hop Limit）字段，该字段与 IPv4 头部中的 TTL 字段的作用一样，表示该报文在网络中可被路由器转发的次数。

可通过命令配置设备生成的 IPv6 报文头部中跳数限制的值。

表 34-7 配置 IPv6 报文跳数限制值

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 IPv6 报文跳数限制值	ipv6 hop-limit <i>value</i>	必选 缺省情况下，设备发送 IPv6 报文的跳数限制为 64

配置接口的 IPv6 MTU

表 34-8 配置接口的 IPv6 MTU

步骤	命令	说明
进入全局配置模式	configure terminal	-

进入接口配置模式	interface <i>interface-name</i>	-
配置接口的 IPv6 MTU	ipv6 mtu <i>value</i>	必选 缺省情况下，未配置接口的 IPv6 MTU

34.2.3 配置 IPv6 邻居发现协议

-B -S -E -A

IPv6 邻居发现 (ND: Neighbor Discovery) 协议包括以下功能: 地址解析、邻居不可达检测、重复地址检测、路由器发现/前缀发现、地址自动配置和重定向。

ND 协议使用的 ICMPv6 报文类型及作用如下表所示。

表 34-9 ND 协议使用的 ICMPv6 报文类型及作用

ICMPv6 报文类型	类型号	作用
路由器请求报文 (RS: Router Solicitation)	133	节点启动后, 通过 RS 报文向路由器发出请求, 请求前缀和其他配置信息, 用于节点的自动配置
路由器通告报文 (RA: Router Advertisement)	134	对 RS 报文进行响应 在没有抑制 RA 报文发送的条件下, 路由器会周期性地发送 RA 报文, 其中包括前缀信息选项和一些标志位的信息
邻居请求报文 (NS: Neighbor Solicitation)	135	获取邻居的链路层地址 验证邻居是否可达 进行重复地址检测

ICMPv6 报文类型	类型号	作用
邻居通告报文 (NA: Neighbor Advertisement)	136	对 NS 报文进行响应 节点在链路层变化时主动发送 NA 报文, 向邻居节点通告本节点的变化信息
重定向报文 (Redirect)	137	当满足一定的条件时, 缺省网关通过向源主机发送重定向报文, 使主机重新选择正确的下一跳地址进行后续报文的发送

- 地址解析

获取同一链路上邻居节点的链路层地址, 通过 NS 报文和 NA 报文实现。

- 邻居不可达检测

在获取到邻居节点的链路层地址后, 通过 NS 报文和 NA 报文可以验证邻居节点是否可达。

1) 节点发送 NS 报文, 其中目的地址是邻居节点的 IPv6 地址。

2) 如果收到邻居节点的确认报文, 则认为邻居可达; 否则认为邻居不可达。

- 重复地址检测

当节点获取到一个 IPv6 地址后, 需要使用重复地址检测功能确定该地址是否已被其他节点使用。

- 路由器发现/前缀发现及地址自动配置

路由器发现/前缀发现是指节点从收到的 RA 报文中获取邻居路由器及所在网络的前缀, 以及其他配置参数。

地址无状态自动配置是指节点根据路由器发现/前缀发现所获取的信息, 自动配置 IPv6 地址。

路由器发现/前缀发现通过 RS 报文和 RA 报文来实现。

- 重定向

当主机启动时，其路由表中可能只有一条到缺省网关的缺省路由。当满足一定的条件时，缺省网关会向源主机发送 ICMPv6 重定向报文，通知主机选择更好的下一跳进行后续报文的发送。

配置条件

无

配置 IPv6 静态邻居

将邻居节点的 IPv6 地址解析为链路层地址，可以通过 IPv6 ND 协议中的地址解析功能实现，也可以通过手工配置静态邻居来实现。

IPv6 邻居通过邻居节点的 IPv6 地址和与此邻居节点相连的三层接口来唯一标识。

表 34-10 配置 IPv6 静态邻居

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 IPv6 静态邻居	ipv6 neighbor ipv6-address interface-name mac-address	必选 缺省情况下，未配置 IPv6 静态邻居

配置处于 STALE 状态的 IPv6 邻居表项的老化时间

IPv6 邻居表项具有 5 种可达性状态：INCOMPLETE、REACHABLE、STALE、DELAY 和 PROBE，其中 STALE 状态表示不知道邻居是否可达，处于 STALE 状态的邻居表项存在一个老化时间，到达老化时间的 STALE 状态的邻居表项将迁移到 DELAY 状态。

表 34-11 配置处于 STALE 状态的 IPv6 邻居表项的老化时间

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置处于 STALE 状态的 IPv6 邻居表项的老化时间	ipv6 neighbor stale-aging aging-time	可选

		缺省情况下，处于 STALE 状态的 IPv6 邻居表项的老化时间为 7200 秒
--	--	---

配置 NS 报文的重传时间间隔

设备发送 NS 报文后，如果未在指定的时间间隔内收到响应，则会重新发送 NS 报文。通过以下命令可以配置发送 NS 报文重传的时间间隔。

表 34-12 配置 NS 报文重传时间间隔

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置 NS 报文重传时间间隔	ipv6 nd ns-interval <i>value</i>	必选 缺省情况下，接口发送 NS 报文的时间间隔为 1000 毫秒

配置 IPv6 重复地址检测发送 NS 报文的次数

接口配置 IPv6 地址后，发送 NS 报文进行重复地址检测，如果在一定时间内没有收到响应，则继续发送 NS 报文，当发送的 NS 报文数达到所设置的值后，仍未收到响应，则认为该地址可用。

表 34-13 配置 IPv6 重复地址检测 NS 报文的次数

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-

配置 IPv6 重复地址检测发送 NS 报文的次数	ipv6 nd dad attempts <i>value</i>	必选 缺省情况下，IPv6 重复地址检测发送 NS 报文的次数为 1
---------------------------	---	---

配置 RA 报文的相关参数

用户可以根据实际情况，配置接口是否发送 RA 报文及发送 RA 报文的时间间隔，同时可以配置 RA 报文中的相关参数以通告给主机。当主机接收到 RA 报文后，就可以采用这些参数进行相应操作。

表 34-14RA 报文中的参数及描述

参数	描述
跳数限制 (Hop Limit)	主机在发送 IPv6 报文时，将使用该参数值填充 IPv6 报文头中的 Hop Limit 字段。同时该参数值也作为设备应答报文中的 Hop Limit 字段值。
MTU	发布链路的 MTU，可以用于确保同一链路上的所有节点采用相同的 MTU 值。
路由器生存时间 (Router Lifetime)	用于设置发送 RA 报文的路由器作为主机的默认路由器的时间。主机根据接收到的 RA 报文中的路由器生存时间参数值，可以确定是否将发送该 RA 报文的路由器作为默认路由器。
邻居可达状态的保持时间 (Reachable Time)	当通过邻居不可达检测确认邻居可达后，在所设置的可达时间内，设备认为邻居可达；超过设置的时间后，如果需要向邻居发送报文，会重新确认邻居是否可达。

表 34-15RA 报文的相关参数

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置 RA 报文中的前缀选项信息	ipv6 nd prefix { <i>ipv6-prefix</i> default } [<i>valid-lifetime</i> infinite no-advertise no-autoconfig off-link] [<i>prefered-lifetime</i> infinite]	必选 缺省情况下，没有配置前缀选项信息。
配置接口发送的 RA 报文中 Hop Limit 字段的值从全局配置获取	ipv6 nd ra hop-limit	可选 缺省情况下，未配置接口发送的 RA 报文中 Hop Limit 字段的值从全局获取，Hop Limit 字段的值为 0。
配置发送 RA 报文的最大时间间隔和最小时间间隔	ipv6 nd ra interval <i>max-value</i> [<i>min-value</i>]	可选 缺省情况下，发送 RA 报文的最大时间间隔为 600 秒，最小时间间隔为 198 秒
配置 RA 报文中携带 MTU 选项	ipv6 nd ra mtu	可选 缺省情况下，RA 报文中不携带 MTU 选项

配置 RA 报文中路由器的生存时间	ipv6 nd ra-lifetime <i>value</i>	可选 缺省情况下，RA 报文中路由器的生存时间为 1800 秒
禁止接口周期性发送 RA 报文	ipv6 nd suppress-ra period	可选 缺省情况下，接口上不会周期性发送 RA 报文
禁止接口回应 RS 报文	ipv6 nd suppress-ra response	可选 缺省情况下，接口收到 RS 报文，不回应 RA 报文

开启接口发送重定向报文功能

设备接收到需要转发的 IPv6 报文后，通过选路发现该报文的接收接口与发送接口相同，此时设备将此报文转发，并向源端回送重定向报文，通知源端重新选择正确的下一跳，进行后续报文的发送。缺省情况下，设备能够发送重定向报文，但在一些特定情况下，用户可以禁止设备发送重定向报文。

表 34-16 接口发送重定向报文功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
开启接口发送重定向报文功能	ipv6 redirects	可选 缺省情况下，接口发送重定向报文功能处于开启状态

34.2.4 配置 ICMPv6 功能 -B -S -E -A

在 IPv6 协议栈中，Internet 控制报文协议（Internet Control Message Protocol）主要用于提供网络检测服务，并在网络层或传输层协议出现异常时，提供差错报告，通知相应设备，以便进行网络的控制管理。

配置条件

无

配置 ICMPv6 差错报文发送速率

如果网络中短时间内发送的 ICMPv6 差错报文过多，可能导致网络拥塞。为了避免这种情况，用户可以配置在指定时间内发送 ICMPv6 差错报文的最大个数。

表 34-17 ICMPv6 差错报文发送速率

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 ICMPv6 报文发送速率	ipv6 icmp error-interval interval [buckets]	可选 缺省情况下，计算 ICMPv6 差错报文发送速率的周期为 100 毫秒，在周期内发送 ICMPv6 差错报文的最大个数为 10

开启 ICMPv6 目的不可达报文的发送功能

ICMPv6 目的不可达报文发送功能是在设备收到 IPv6 数据报文后，如果目的不可达，则将报文丢弃并给源端发送 ICMPv6 目的不可达差错报文。

设备在满足下列条件时会发送 ICMPv6 目的不可达差错报文：

- 设备在转发报文时，如果查找路由失败，则向源端发送“没有到达目的地址的路由” ICMPv6 差

错报文；

- 设备在转发报文时，如果是因为管理策略（例如防火墙、ACL 等）导致无法发送报文时，则向源端发送“与目的地址的通信被管理策略禁止” ICMPv6 差错报文；
- 设备在转发报文时，如果报文的目的 IPv6 地址超出源 IPv6 地址的范围（例如，报文的源 IPv6 地址为链路本地地址，报文的目的 IPv6 地址为全球单播地址），会导致报文无法到达目的端，则向源端发送“超出源地址范围” ICMPv6 差错报文；
- 设备在转发报文时，如果不能解析目的 IPv6 地址对应的链路层地址，则向源端发送“地址不可达” ICMPv6 差错报文；
- 设备收到目的地址为本地、传输层协议为 UDP 的 IPv6 报文时，如果报文的目的端口号与正在使用的进程不匹配，则向源端发送“端口不可达” ICMPv6 差错报文。

由于 ICMPv6 目的不可达差错报文传递给用户进程的信息为不可达信息，如果存在恶意攻击，可能影响终端用户的正常使用。为了避免上述现象发生，可以关闭设备的 ICMPv6 目的不可达差错报文发送功能。

表 34-18 ICMPv6 目的不可达报文的发送功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
开启 ICMPv6 目的不可达报文的发送功能	ipv6 unreachable	可选 缺省情况下，ICMPv6 目的不可达报文发送功能处于开启状态

34.2.5 配置 IPv6 TCP 防攻击功能

-B -S -E -A

如果 IPv6 TCP 服务器收到了大量的 SYN 报文但是对端不响应服务器的 SYN+ACK 回应。就会导致服务器的内存大量消耗，占用服务器的半连接队列，导致 IPv6 TCP 服务器无法为正常的请求服务。针对这种攻击可以通过配置 IPv6 TCP 防攻击功能来避免。

配置条件

无

配置手册

发布 1.1 04/2020

开启 IPv6 TCP syncache 功能

该功能是在收到 SYN 数据报文时不急于去分配 TCB，而是先回应一个 SYN+ACK 报文，并在一个专用缓存中保存这种半开连接信息，直到收到正确的回应 ACK 报文再分配 TCB。

表 34-19 IPv6 TCP syncache 功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
开启 IPv6 TCP syncache 功能	ipv6 tcp syncache	必选 缺省情况下，IPv6 TCP syncache 功能处于关闭状态

开启 IPv6 TCP syncookies 功能

该功能完全不使用任何存储资源，它使用一种特殊的算法生成 Sequence Number，这种算法考虑到了对方的 IPv6 地址、端口、己方 IPv6 地址、端口的固定信息，以及对方无法知道而己方比较固定的一些信息，如 MSS、时间等，在收到对方的 ACK 报文后，重新计算一遍，看其是否与对方回应报文中的 (Sequence Number-1) 相同，从而决定是否分配 TCB 资源

表 34-20 IPv6 TCP syncookies 功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
开启 IPv6 TCP syncookies 功能	ipv6 tcp syncookies	必选 缺省情况下，IPv6 TCP syncookies 功能处于关闭状态

34.2.6 IPv6 基础监控与维护

-B -S -E -A

表 34-21 IPv6 基础监控与维护

命令	说明
clear ipv6 icmp6stat	清除 ICMPv6 统计信息
clear ipv6 interface statistics	清除接口 IPv6 报文统计信息
clear ipv6 mtu	清除 IPv6 路径 MTU 信息
clear ipv6 neighbors	清除 IPv6 动态邻居表项
clear ipv6 statistics	清除 IPv6 基础统计信息
clear ipv6 tcp syncache statistics	清除 IPv6 TCP 协议 syncache 统计信息
clear ipv6 tcp6stat	清除 IPv6 TCP 统计信息
clear ipv6 udp6stat	清除 IPv6 UDP 统计信息
show ipv6 hop-limit	显示 IPv6 全局 Hop Limit 值
show ipv6 frag-queue	显示缓存的 IPv6 分片报文
show ipv6 icmp6state	显示 ICMPv6 统计信息
show ipv6 interface	显示接口 IPv6 信息
show ipv6 interface statistics	显示接口 IPv6 统计信息
show ipv6 max-mtu	显示系统当前支持的 IPv6 MTU 最大值
show ipv6 mtu	显示 IPv6 路径 MTU 信息

命令	说明
show ipv6 neighbors	显示 IPv6 邻居信息
show ipv6 prefix	显示 IPv6 地址前缀信息
show ipv6 sockets	显示 IPv6 套接字信息
show ipv6 statistics	显示 IPv6 基本统计信息
show ipv6 tcp syncache detail	显示 IPv6 TCP 协议 syncache 表项信息
show ipv6 tcp syncache statistics	显示 IPv6 TCP 协议 syncache 统计信息
show ipv6 tcp6state	显示 IPv6 TCP 统计信息
show ipv6 udp6state	显示 IPv6 UDP 统计信息

34.3 IPv6 基础配置举例

34.3.1 配置接口的 IPv6 地址

-B -S -E -A

网络需求

- 两台设备通过以太网接口相连，给接口配置 IPv6 全球单播地址，验证它们之间的互通性。

网络拓扑

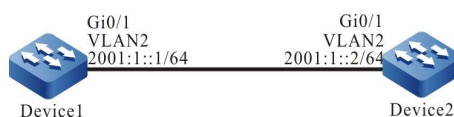


图 34-1 配置接口的 IPv6 地址组网图

配置步骤

步骤 1: 配置 VLAN，并将端口加入对应的 VLAN。（略）

步骤 2: 使能设备的 IPv6 转发能力。

#配置 Device1。

```
Device1#configure terminal
Device1(config)#ipv6 unicast-routing
```

#配置 Device2。

```
Device2#configure terminal
Device2(config)#ipv6 unicast-routing
```

步骤 3: 配置接口的全球单播地址。

#配置 Device1 接口 vlan 2 的全球单播地址为 2001:1::1/64。

```
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#ipv6 address 2001:1::1/64
Device1(config-if-vlan2)#exit
```

#配置 Device2 接口 vlan 2 的全球单播地址为 2001:1::2/64。

```
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#ipv6 address 2001:1::2/64
Device2(config-if-vlan2)#exit
```

步骤 4: 检验结果。

#查看 Device1 的接口信息。

```
Device1#show ipv6 interface vlan 2
vlan2 is up
VRF: global
IPv6 is enable, link-local address is fe80::0201:7aff:fe46:a64d
Global unicast address(es):
 2001:0001::0001, subnet is 2001:0001::/64
Joined group address(es):
 ff02::0001:ff00:0001
 ff02::0001:ff00:0
 ff02::0002
 ff02::0001
 ff02::0001:ff46:a64d
ND control flags: 0x1
MTU is 1500 bytes
ICMP redirects are enabled
ICMP unreachable are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
```

配置 IPv6 地址后，接口上会自动使能 IPv6 协议功能，自动生成链路本地地址，并加入对应的组播组。

#查看 Device2 的接口信息。

```
Device2#show ipv6 interface vlan 2
vlan2 is up
```

```
VRF: global
IPv6 is enable, link-local address is fe80::0201:7aff:fe22:e222
Global unicast address(es):
 2001:0001::0002, subnet is 2001:0001::/64
Joined group address(es):
 ff02::0001:ff00:0002
 ff02::0001:ff00:0
 ff02::0002
 ff02::0001
 ff02::0001:ff22:e222
ND control flags: 0x1
MTU is 1500 bytes
ICMP redirects are enabled
ICMP unreachable are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
```

#在 Device1 上 Ping Device2 的链路本地地址 fe80::0201:7aff:fe22:e222。

```
Device1#ping fe80::0201:7aff:fe22:e222

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to fe80::201:7aff:fe22:e222 , timeout is 2 seconds:

Output Interface: vlan 2
!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/96/483 ms.
```

说明：

- ping 链路本地地址时需要指定出接口，出接口为 ping 的链路本地地址同一链路上的接口。
-

#在 Device1 上 Ping Device2 的全球单播地址 2001:1::2。

```
Device1#ping 2001:1::2

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 2001:1::2 , timeout is 2 seconds:
!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/36/183 ms.
```

Device1 和 Device2 可以互相通信。

34.3.2 配置 IPv6 邻居发现

-B -S -E -A

网络需求

- Device 和 PC 属于同一个局域网。
- Device 的接口 VLAN2 配置 EUI-64 地址。
- PC 通过 IPv6 邻居发现协议获取到 IPv6 地址前缀，根据获取到的地址前缀自动配置 IPv6 地址。PC 和 Device 之间实现 IPv6 协议的通信。

网络拓扑

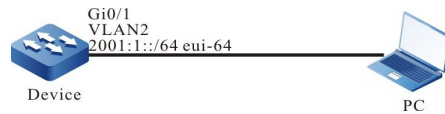


图 34-2 配置 IPv6 邻居发现组网图

配置步骤

步骤 1： 配置 VLAN，并将端口加入对应的 VLAN。（略）

步骤 2： 使能设备的 IPv6 转发能力。

```
Device#configure terminal
Device(config)#ipv6 unicast-routing
```

步骤 3： 配置 EUI-64 单播地址，并使能 RA 通告功能。

Device 的 vlan 2 配置 EUI-64 地址，使能 vlan 2 的 RA 通告功能。

```
Device(config)#interface vlan 2
Device(config-if-vlan 2)#ipv6 address 2001:1::/64 eui-64
Device(config-if-vlan 2)#no ipv6 nd suppress-ra period
Device(config-if-vlan 2)#no ipv6 nd suppress-ra response
Device(config-if-vlan 2)#exit
```

说明：

- 缺省情况下，RA 通告功能是关闭的。
-

查看 Device 的接口信息。

```
Device#show ipv6 interface vlan 2
vlan2 is up
VRF: global
IPv6 is enable, link-local address is fe80::0201:7aff:fe5d:e7d3
Global unicast address(es):
2001:0001::0201:7aff:fe5d:e7d3, subnet is 2001:0001::/64 [EUI]
```

```
Joined group address(es):
ff02::0001:ff00:0
ff02::0002
ff02::0001
ff02::0001:ff5d:e7d3
ND control flags: 0x85
MTU is 1500 bytes
ICMP redirects are enabled
ICMP unreachable are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
```

步骤 4: 配置 PC。

PC 上安装 IPv6 协议。IPv6 的配置因操作系统而异，本文仅以 Windows XP 为例进行说明。

```
C:\>ipv6 install
Installing...
Succeeded.
```

步骤 5: 检验结果。

#查看 PC 的接口信息。

```
C:\>ipconfig
..... (此处省略部分显示信息)
Ethernet adapter 130:

    Connection-specific DNS Suffix  . :
    IP Address. . . . . : 130.255.128.100
    Subnet Mask . . . . . : 255.255.0.0
    IP Address. . . . . : 2001:1::15b3:d4:f13d:c3da
    IP Address. . . . . : 2001:1::3a83:45ff:feef:c724
    IP Address. . . . . : fe80::3a83:45ff:feef:c724%6
    Default Gateway . . . . . : fe80::201:7aff:fe5e:cfc1%6
```

可看到 PC 获取到 IPv6 地址前缀 2001:1::/64，根据此前缀的自动生成全球单播地址。

说明：

- Windows XP 主机获取到地址前缀后会生成两个全球单播地址，其中一个地址的接口 ID 根据接口的 MAC 地址生成，另一个地址的接口 ID 随机生成。
-

#在 Device 上 Ping PC 的链路本地地址 fe80::3a83:45ff:feef:c724。

```
Device#ping fe80::3a83:45ff:feef:c724

Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to fe80::3a83:45ff:feef:c724 , timeout is 2 seconds:

Output Interface: vlan2
```

```
!!!!  
Success rate is 100% (5/5). Round-trip min/avg/max = 0/29/149 ms.
```

#在 Device 上 Ping PC 上自动生成的全球单播地址 2001:1::15b3:d4:f13d:c3da 和 2001:1::3a83:45ff:feef:c724。

```
Device#ping 2001:1::15b3:d4:f13d:c3da  
  
Press key (ctrl + shift + 6) interrupt it.  
Sending 5, 76-byte ICMP Echos to 2001:1::15b3:d4:f13d:c3da , timeout is 2 seconds:  
!!!!  
Success rate is 100% (5/5). Round-trip min/avg/max = 0/36/183 ms.  
  
Device#ping 2001:1::3a83:45ff:feef:c724  
  
Press key (ctrl + shift + 6) interrupt it.  
Sending 5, 76-byte ICMP Echos to 2001:1::3a83:45ff:feef:c724 , timeout is 2 seconds:  
!!!!  
Success rate is 100% (5/5). Round-trip min/avg/max = 0/26/133 ms.
```

PC 和 Device 之间能够互相通信。

说明：

- ping 链路本地地址时需要指定出接口，出接口为 ping 的链路本地地址同一链路上的接口。
-

35 DHCPv6

35.1 DHCPv6 简介

当一个网络比较庞大时，它是很难以管理的，比如 IPv6 地址通过手工分配的网络环境中最常见的问题是 IPv6 地址冲突。处理这个问题的唯一方法是为主机动态分配 IPv6 地址。动态主机配置协议 DHCPv6 从一个地址池中把 IPv6 地址分配给请求主机。同时 DHCPv6 也能提供其它信息，如 DNS 服务器地址等。DHCPv6 减轻了管理员跟踪记录手工分配 IPv6 地址的负担。

DHCPv6 是一个基于 UDP 广播的协议。DHCPv6 客户端从 DHCPv6 服务器端获取 IPv6 地址和其它配置信息的过程，主要通过四个阶段进行：

SOLICIT 阶段，当 DHCPv6 客户端第一次登录网络时，它会向网络发出一个 DHCP SOLICIT 报文，报文的源地址是客户端的 linklocal 地址，目的地址为 ff02::1:2；

ADVERTISE 阶段，当 DHCPv6 服务器接收到客户端发出的 DHCP SOLICIT 广播报文后，它会根据策略，从对应的地址池中选择一个 IPv6 地址，与其它参数一起通过 DHCP ADVERTISE 报文发送给客户端；

REQUEST 阶段，如果 DHCPv6 客户端收到网络上多台 DHCPv6 服务器的回应，只会挑选其中一个 DHCP ADVERTISE（通常是最先抵达的那个），并且会向网络发送一个 DHCP REQUEST 报文，告诉所有 DHCPv6 服务器它将接受哪一台服务器提供的 IPv6 地址；

REPLY 阶段，当 DHCPv6 服务器收到 DHCPv6 客户端的 DHCP REQUEST 请求报文后，它便向 DHCPv6 客户端发送一个包含它所提供的 IPv6 地址和其它配置的 DHCP REPLY 确认信息，告诉 DHCPv6 客户端可以使用它所提供的 IPv6 地址。

DHCPv6 服务器分配给 DHCPv6 客户端的 IPv6 地址都有一个租约，期满后 DHCPv6 服务器便会收回分配的 IPv6 地址。当 DHCPv6 客户端的 IPv6 地址租约剩余一半时，DHCPv6 客户端会向 DHCPv6 服务器发送更新其 IPv6 租约的 DHCP ENEW 报文。如果 DHCPv6 客户端可以继续使用该 IPv6 地址，则 DHCPv6 服务器回应 DHCP REPLY 报文，通知 DHCPv6 客户端更新租约；如果 DHCPv6 客户端不可以继续使用该 IPv6 地址，则 DHCPv6 服务器不予回应。

由于在 IPv6 地址动态获取过程中是采用组播方式发送请求报文，因此 DHCPv6 只适用于 DHCPv6 客户端与 DHCPv6 服务器处于同一子网内的情况。如果在一个网络中存在多个子网，而多个子网的主机都需要通过 DHCPv6 服务器来提供 IPv6 地址等配置信息时，则这些子网的主机可以通过 DHCPv6 中继设备来与 DHCPv6 服务器进行通信，最终获得 IPv6 地址及其它配置信息。

35.2 DHCPv6 功能配置

表 35-1 DHCPv6 功能配置列表

配置任务	
配置 DHCPv6 地址池	创建 DHCPv6 地址池可以指定 VRF 属性

	配置 IPv6 地址范围
	配置 DNS 服务器地址
	配置 IPv6 地址租期
	配置 IPv6 与 DUID、IAID 绑定
配置 DHCPv6 服务器其它参数	配置 DHCPv6 服务器
	配置保留的 IPv6 地址范围
	配置 DHCPv6 ping 探测参数
	配置 DHCPv6 服务器的数据日志功能
配置 DHCPv6 客户端功能	配置 DHCPv6 客户端
	配置 DHCPv6 Option 16 功能
配置 DHCPv6 中继功能	配置 DHCPv6 中继
	配置 DHCPv6 中继报文源地址
	配置 DHCPv6 服务器地址
	配置 DHCPv6 interface-id 选项

35.2.1 配置 DHCPv6 地址池

-S -E -A

配置条件

无

创建 DHCPv6 地址池

DHCPv6 服务器从 DHCPv6 地址池中为客户端选择并分配 IPv6 地址及其它相关参数，因此，DHCPv6 服务器必须先创建 DHCPv6 地址池。

表 35-2 创建 DHCPv6 地址池

步骤	命令	说明
进入全局配置模式	configure terminal	-
创建 DHCPv6 地址池并进入 DHCPv6 配置模式	ipv6 dhcp pool <i>pool-name</i> [vrf <i>vrf-name</i>]	必选 缺省情况下，系统没有创建 DHCPv6 地址池

说明：

- 地址池有 Network 和 Range 两种地址池类型，可以分别通过 network 和 range 命令进行配置。

配置 IPv6 地址范围

在 DHCPv6 服务器上，每个 DHCPv6 地址池都应该配置相应的 IPv6 地址范围，以给 DHCPv6 客户端分配 IPv6 地址。

表 35-3 配置 IPv6 地址范围

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 DHCPv6 配置模式	ipv6 dhcp pool <i>pool-name</i> [vrf <i>vrf-name</i>]	-
配置 Network 类型 IPv6 地址范围	network <i>ipv6-address/prefix-length</i>	可选

		缺省情况下，地址池没有配置 IPv6 地址范围
配置 Range 类型 IPv6 地址范围	range <i>low-ipv6-address high-ipv6-address prefix-length</i>	可选 缺省情况下，地址池没有配置 IPv6 地址范围

说明：

- 修改地址池的类型从 network 修改成 range(或者从 range 修改成 network)，若新配置的地址范围和旧配置的地址范围存在交集，命令行会提示用户是否执行该操作，若是，会删除地址池下相关的地址配置(静态绑定)和动态租约；若新配置的地址实际生效范围包含旧配置的地址实际生效范围，地址池会保留地址池下相关的地址配置(静态绑定)。但是会删除动态租约。

配置 DNS 服务器地址

在 DHCPv6 服务器上，可以为每个 DHCPv6 地址池分别配置 DNS 服务器地址。DHCPv6 服务器在给 DHCPv6 客户端分配 IPv6 地址时，也将 DNS 服务器地址发送给客户端。

DHCPv6 客户端进行动态域名解析时，将向 DNS 服务器进行查询。

表 35-4 配置 DNS 服务器地址

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 DHCPv6 配置模式	ipv6 dhcp pool <i>pool-name</i> [vrf <i>vrf-name</i>]	-

配置 DNS 服务器地址	dns-server { <i>ipv6-address</i> &<1-8> / autoconfig }	必选 缺省情况下，没有配置 DNS 服务器地址
--------------	--	----------------------------

配置 IPv6 地址租期

DHCPv6 服务器分配给 DHCPv6 客户端的 IPv6 地址有一定的租借期限，当租借期满后服务器会收回该 IPv6 地址。如果 DHCPv6 客户端希望继续使用该地址，需要更新 IPv6 地址租约。

在 DHCPv6 服务器上，可以为每个 DHCPv6 地址池分别配置 IPv6 地址租期。

表 35-5 配置 Ipv6 地址租期

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 DHCPv6 配置模式	ipv6 dhcp pool <i>pool-name</i> [vrf <i>vrf-name</i>]	-
配置 IPv6 地址租期	lease preferred-lifetime <i>preferred-lifetime</i> valid-lifetime <i>valid-lifetime</i>	必选 缺省情况下， preferred-lifetime 为 604800 秒 (7 天)， valid-lifetime 为 2592000 秒 (30 天)

配置 IPv6 与 DUID、IAID 绑定

配置 IPv6 与客户端 DUID、IAID 绑定，当指定 DUID、IAID 的客户端向 DHCPv6 服务器请求分配 IPv6 地址时，DHCPv6 服务器将分配其绑定的 IPv6 地址。只要该客户端的 DUID、IAID 不变，客户端每次从服务器获取的 IPv6 地址都是相同的。

表 35-6 配置 IPv6、DUID 和 IAID 地址绑定

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 DHCPv6 配置模式	ipv6 dhcp pool <i>pool-name</i> [vrf <i>vrf-name</i>]	-
配置 IPv6 与 DUID、IAID 绑定	bind <i>ipv6-address</i> duid <i>duid</i> [iaid <i>iaid</i>]	必选 缺省情况下，没有配置 IPv6 与 DUID、IAID 绑定

说明：

- 该命令只对 Range 类型和 Network 类型地址池有效。
- 配置相同的 duid 和 iaaid 的静态绑定时，地址池允许绑定五个 IPv6 地址。
- 配置的静态绑定只指定了 duid，没有指定 iaaid 时，地址池只允许绑定一个 IPv6 地址。

35.2.2 配置 DHCPv6 服务器其它参数

-S -E -A

配置条件

无

配置 DHCPv6 服务器

配置在接口工作在 DHCPv6 服务器模式后，当接口收到 DHCPv6 客户端发来的 DHCPv6 请求报文时，DHCPv6 服务器会为客户端分配 IPv6 地址和其他网络参数。

表 35-7 配置 DHCPv6 服务器

步骤	命令	说明
----	----	----

进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置 DHCPv6 服务器功能呢	ipv6 dhcp server	必选 缺省情况下，没有配置 DHCPv6 服务器功能

配置保留的 IPv6 地址范围

在 DHCPv6 地址池中，有一些 IPv6 地址是为某些特定设备预留的，有一些 IPv6 地址与网络上其他主机 IPv6 地址冲突，因此这些 IPv6 地址不能用于动态分配。

表 35-8 配置保留的 IPv6 地址范围

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置保留的 IPv6 地址范围	ipv6 dhcp excluded-address <i>low-ipv6-address</i> [<i>high-ipv6-address</i>] [vrf <i>vrf-name</i>]	必选 缺省情况下，没有配置保留的 IPv6 地址范围 保留的 IPv6 地址范围内的 IPv6 地址不参与地址分配

配置 DHCPv6 ping 探测参数

为防止 IPv6 地址冲突，DHCPv6 服务器在为 DHCPv6 客户端动态分配 IPv6 地址前，需要先对该 IPv6 地址进行探测。而探测是通过 ping 操作来进行的，根据检测能否在指定时间内收到 ICMPv6 回应响应报文来判断是否有 IPv6 地址冲突。

表 35-9 配置 DHCPv6 ping 探测参数

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 DHCPv6 ping 探测参数	ipv6 dhcp ping { packets <i>packet-num</i> timeout <i>milliseconds</i> }	必选 缺省情况下, ping 包的个数为 1, 超时时间是 500ms

配置 DHCPv6 服务器数据日志功能

开启 DHCPv6 服务器的数据日志功能后, DHCPv6 服务器上地址池分配的情况将被记录至数据日志中。

表 35-10 配置 DHCPv6 服务器数据日志功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 DHCPv6 服务器的数据日志功能开关	ipv6 dhcp logging security-data	必选 缺省情况下, 未开启数据日志功能

35.2.3 配置 DHCPv6 客户端功能 **-S -E -A**

配置条件

无

配置 DHCPv6 客户端

DHCPv6 客户端的接口可以通过 DHCPv6 获取 IPv6 地址及其它参数。

表 35-11 配置 DHCPv6 客户端

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置 DHCPv6 客户端获取 IPv6 地址	ipv6 dhcp client address [rapid-commit]	必选 缺省情况下，没有配置 DHCPv6 客户端请求获取 IPv6 地址
配置 DHCPv6 客户端获取 IPv6 前缀	ipv6 dhcp client pd pool-name [rapid-commit]	必选 缺省情况下，没有配置 DHCPv6 客户端请求获取 IPv6 前缀

35.2.4 配置 DHCPv6 中继功能

-S -E -A**配置条件**

无

配置 DHCPv6 中继

如果在一个网络中存在多个子网，而多个子网的主机都需要通过 DHCPv6 服务器来提供 IPv6 地址等配置信息时，则这些子网的主机可以通过 DHCPv6 中继设备来与 DHCPv6 服务器进行通信，最终获得 IPv6 地址及其它配置信息。如果配置接口工作在 DHCPv6 中继模式后，当接口收到 DHCPv6 客户端发来的 DHCPv6 报文时，会将报文中继到配置的 DHCPv6 服务器，由 DHCPv6 服务器来分配 IPv6 地址。

表 35-12 配置 DHCPv6 中继

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface interface-name	-
配置 DHCPv6 中继功能	ipv6 dhcp relay	必选 缺省情况下，没有配置 DHCPv6 中继功能

配置 DHCPv6 中继报文源地址

DHCPv6 中继 DHCPv6 客户端到服务器报文的源地址，默认使用到 DHCPv6 服务器的路由出接口地址，在某些特殊环境中 DHCPv6 服务器是不能与该地址通信的，因此允许用户可以通过 **ipv6 dhcp relay source-address** 命令用于配置 DHCPv6 中继发往 DHCPv6 服务器报文的源地址和报文中的 LinkAddr 字段；

表 35-13 配置 DHCPv6 中继报文源地址

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface interface-name	-
配置 DHCPv6 中继报文源地址	ipv6 dhcp relay source-address ipv6-address	必选 缺省情况下，没有配置 DHCPv6 中继报文源地址

配置 DHCPv6 服务器地址

当接口收到 DHCPv6 客户端发来的 DHCPv6 报文时，会将报文中继到配置的 DHCPv6 服务器，由 DHCPv6 服务器来分配 IPv6 地址。

表 35-14 配置 DHCPv6 服务器地址

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置 DHCPv6 服务器地址	ipv6 dhcp relay server -address <i>ipv6-address</i>	必选 缺省情况下，没有配置 DHCPv6 服务器地址

配置 DHCPv6 interface-id 选项

该命令用来配置 DHCPv6 中继支持的 interface-id 选项填充模式。

表 35-15 配置 DHCPv6 服务器地址

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 DHCPv6 interface-id 选项	ipv6 dhcp relay interface -id [interface]	必选 缺省情况下，没有配置 interface-id 选项填充模式

35.2.5 DHCPv6 监控与维护

-S -E -A

表 35-16 DHCPv6 监控与维护

命令	说明
clear ipv6 dhcp pool <i>pool-name</i> { lease conflict [<i>ipv6-address</i>] }	清除地址池下的动态租约信息或者出现地址冲突的地址信息
clear ipv6 dhcp server interface [<i>interface-name</i>] statistics	清除 DHCPv6 服务器与客户端或者中继进行报文交互时的关键信息统计
clear ipv6 dhcp relay statistics	清除 DHCPv6 中继设备上的统计信息
show ipv6 dhcp server interface <i>interface-name</i> [statistics]	显示指定接口下关联的地址池信息或者显示指定接口下 DHCPv6 服务器与客户端或者中继进行报文交互时的关键信息统计
show ipv6 dhcp pool <i>pool-name</i> { summary ping_list offer_list excluded_list conflict_list lease binding }	显示指定地址池的概要信息或者正在做 ping 检查的地址信息或者已经发送 OFFER 报文，正在等待 DHCPv6 客户端回应 REQUEST 报文的地址信息或者显示地址池下被排除的地址信息或者显示地址池下出现地址冲突的地址信息或者显示地址池下动态租约信息或者显示地址池下静态绑定信息

<pre>show ipv6 dhcp pool pool- name specific { ipv6-address ipv6-address duid duid }</pre>	显示地址池下指定 ip 地址或者客户端的 DUID 的相关信息
<pre>show ipv6 dhcp relay [interface interface-name]</pre>	显示 DHCPv6 中继设备上的报文统计信息。

35.3 DHCPv6 典型配置举例

35.3.1 配置 DHCPv6 服务器静态分配 IPv6 地址

-S -E -A

网络需求

- Device2 作为 DHCPv6 服务器，采用静态方式为客户端分配 IPv6 地址、DNS 服务器 IPv6 地址。
- DHCPv6 服务器以 DUID 绑定方式为 PC1 分配 IPv6 地址，以 DUID+IAID 绑定方式为 PC2 分配 IPv6 地址。

网络拓扑

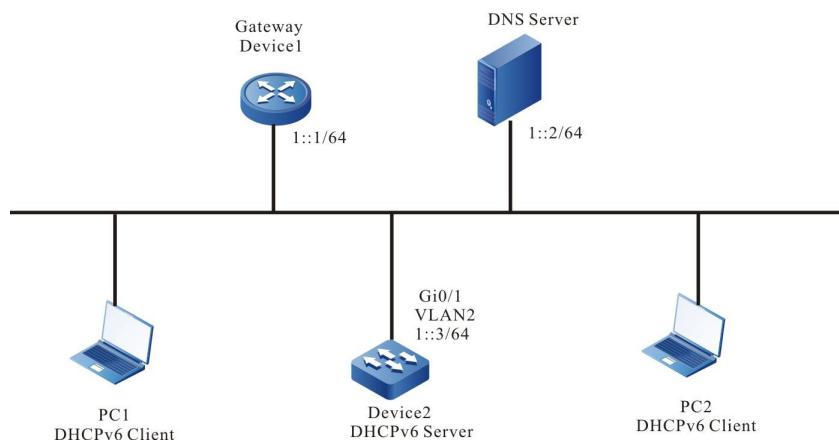


图 35-1 配置 DHCPv6 服务器静态分配 IPv6 地址组网图

配置步骤

步骤 1: 配置 Device2 接口的 IPv6 地址和 DHCPv6 服务器。

```
Device2#configure terminal
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ipv6 address 1::3/64
Device2(config-if-vlan2)#ipv6 dhcp server
Device2(config-if-vlan2)#exit
```

步骤 2: 配置静态绑定地址池及参数。

#配置地址池 binding, 采用静态 DUID 绑定方式为 PC1 分配 IPv6 地址。采用静态 DUID+IAID 的绑定方式为 PC2 分配 IPv6 地址

```
Device2(config)#ipv6 dhcp pool binding
Device2(dhcp6-config)#bind 1::11 duid 000200001613303030313761636635646634
Device2(dhcp6-config)#bind 1::12 duid 000200001613636364383166313037616239 iaid 00010071
Device2(dhcp6-config)#dns-server 1::2
Device2(dhcp6-config)#exit
```

步骤 3: 检验结果。

#检查服务器接口和地址的关联

```
Device2#show ipv6 dhcp server interface vlan2
DHCPv6 server status information:
DHCP server is enabled on interface: vlan2
Vrf : global
```

```
DHCPv6 server pool information:
Available directly-connected pool:
Interface IP: 1::1/64
Pool name: binding
Range:
min: 101::
max: 101::ffff:ffff:ffff:ffff
utilization: 0.00%
```

#检查服务器的静态绑定

```
Device2#show ipv6 dhcp pool binding binding
IPv6 Address      Duid              Iaid  Type  Time Left(s)
-----
1::11  000200001613303030313761636635646634  00000000 Binding NA
1::12  000200001613636364383166313037616239  00010071 Binding NA
```

#在 Device2 上通过 show ipv6 dhcp pool binding lease 命令查看为 PC1、PC2 分配的 IPv6 地址。

```
Device2#show ipv6 dhcp pool mac-binding lease
IPv6 Address      Duid              Iaid  Type  Time Left(s) -----
-----
1::11  000200001613303030313761636635646634  00000000 Lease 2591974
1::12  000200001613636364383166313037616239  00010071 Lease 2591974
```

在 PC1 和 PC2 上检查获取到的 IPv6 地址、DNS 服务器 IPv6 地址正确。

35.3.2 配置 DHCPv6 服务器动态分配 IPv6 地址

-S -E -A**网络需求**

- Device 的两个接口 vlan2、vlan3 分别配置 IPv6 地址 1::3/64 和 2::3/64。
- DHCPv6 服务器 Device 为两个直连物理网络内的客户端分别动态分配 1::/64 和 2::/64 网段的 IPv6 地址。
- 网段 1::/64 内的地址租期为 1 天，DNS 服务器地址为 2::4；网段 2::/64 内的地址租期为 3 天，网关地址为 2::3，DNS 服务器地址为 2::4。
- 网段 1::/64 和网段 2::/64 内前 10 个 IPv6 地址保留不被分配。

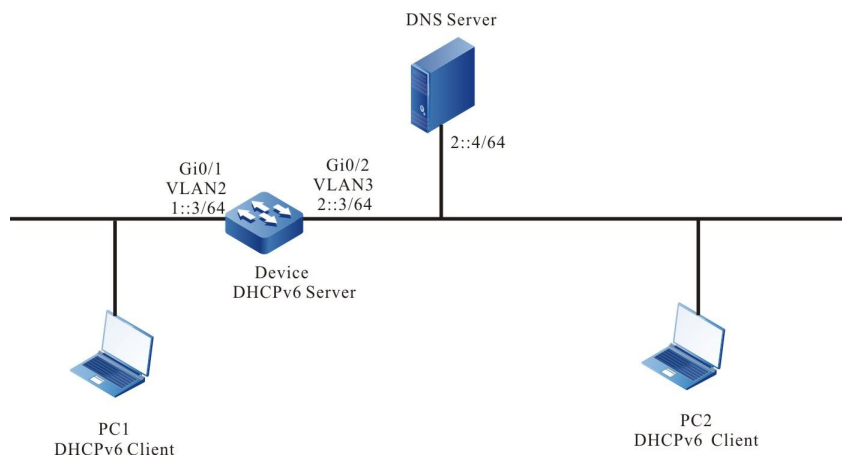
网络拓扑

图 35-2 配置 DHCPv6 动态分配 IPv6 地址组网图

配置步骤

步骤 1：配置 VLAN，并将端口加入对应的 VLAN。配置各接口的 IPv6 地址（略）

步骤 2：在 DHCPv6 服务器 Device1 上配置 2 个动态地址池及其参数。

#配置 DHCPv6 服务器

```
Device(config)#interface vlan2
Device(config-if-vlan2)#ipv6 dhcp server
Device(config-if-vlan2)#exit
Device(config)#interface vlan3
Device(config-if-vlan3)#ipv6 dhcp server
Device(config-if-vlan3)#exit
```

#配置两个地址池中前 10 个 IPv6 地址作为保留地址

```
Device(config)#ipv6 dhcp excluded-address 1::0 1::9
Device(config)#ipv6 dhcp excluded-address 2::0 2::9
```

#配置名为 dynamic-pool1 的地址池及参数（地址范围、dns 地址、地址租期）。

```
Device(config)#ipv6 dhcp pool dynamic-pool1
Device(dhcp6-config)#network 1::/64
Device(dhcp6-config)#dns-server 2::4
Device(dhcp6-config)#lease preferred-lifetime 86300 valid-lifetime 86400
Device(dhcp6-config)#exit
```

#配置名为 dynamic-pool2 的地址池及参数（地址范围、dns 地址、地址租期）。

```
Device(config)#ip DHCPv6 pool dynamic-pool2
Device(dhcp6-config)#network 2::/64
Device(dhcp6-config)#dns-server 2::4
Device(dhcp6-config)#lease preferred-lifetime 259100 valid-lifetime 259200
Device(dhcp6-config)#exit
```

步骤 3： 检验结果。

#查看 Device 上为客户端分配的 IPv6 地址信息。

```
Device#show ipv6 dhcp pool dynamic-pool1 lease
IPv6 Address      Duid              laid      Type      Time Left(s)
-----
1::a      000200001613303030313761636635646634  00000000  Lease    86390
Device2#show ipv6 dhcp pool dynamic-pool2 lease
IPv6 Address      Duid              laid      Type      Time Left(s)
-----
2::a      000200001613303030313761636635646634  00000000  Lease    2591974
```

在 DHCPv6 客户端上查看 IPv6 地址获取正确。

注意：

- 地址池内的 IPv6 地址必须属于提供服务的接口的网段范围。
-

35.3.3 配置 DHCPv6 中继

-S -E -A

网络需求

- Device1 为 DHCPv6 服务器，Device2 接口启用 DHCPv6 中继功能。
- DHCPv6 服务器为 1::/64 网段的客户端提供服务，保留前 10 个 IPv6 地址。
- DHCPv6 客户端通过 DHCPv6 中继获取 IPv6 地址。

网络拓扑

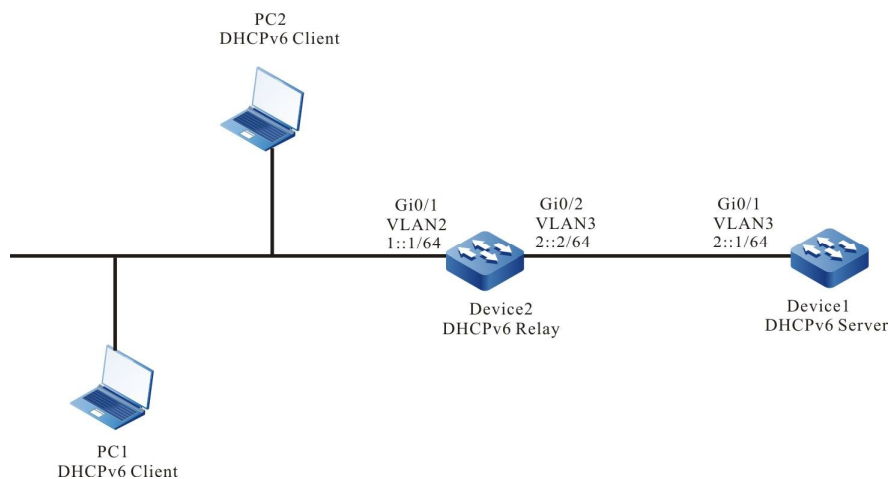


图 35-3 配置 DHCPv6 中继组网图

配置步骤

步骤 1: 配置 VLAN，并将端口加入对应的 VLAN。配置各接口的 IPv6 地址（略）。

步骤 2: 配置 Device1 的 IPv6 地址池及保留的 IPv6 地址。

#配置 Device1 为 DHCPv6 服务器。

```
Device1#configure terminal
Device1(config)#interface vlan3
Device2(config-if-vlan3)#ipv6 dhcp server
Device2(config-if-vlan3)#exit
```

#配置 1::0 至 1::9 的 IPv6 地址不被分配。

```
Device1(config)#ipv6 dhcp excluded-address 1::0 1::9
```

#配置 Device1 的 IPv6 地址池 dynamic-pool。

```
Device1(config)#ipv6 dhcp pool dynamic-pool
Device1(dhcp6-config)#network 1::/64
Device1(dhcp6-config)#lease preferred-lifetime 300 valid-lifetime 600
Device1(dhcp6-config)#exit
```

#配置到网段 1::/64 的静态路由。

```
Device1(config)#ipv6 route 1::0/64 2::2
```

步骤 3: 在 Device2 的 vlan2 接口上开启 DHCPv6 中继并配置 DHCPv6 服务器地址 2::1。

```
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ipv6 dhcp relay
Device2(config-if-vlan2)#ipv6 dhcp relay server-address 2::1
Device2(config-if-vlan2)#exit
```


步骤 4: 检验结果。

#查看 Device1 上分配的 IPv6 地址信息。

```
Device1#show ipv6 dhcp pool dynamic-pool lease
IPv6 Address      Duid              laid  Type  Time Left(s)
-----
1::0              000200001613303030313761636635646634  00000000 Lease  574
```

使用 `show ipv6 dhcp pool dynamic-pool lease` 命令查看为客户端分配的 IPv6 地址信息，说明客户端已经获取到 IPv6 地址 1::0。

单播路由

36 路由基础

36.1 路由基础简介

路由是指设备从一个接口收到报文，根据报文的目地址选路并转发到另一个接口的过程。在网络设备中，路由存储在一个叫做路由表数据库中，报文根据目的地址查找路由表确定该报文的下一跳和出接口。路由根据来源不同分为以下三类：

- 直连路由：由接口地址产生的路由。当用户配置接口的 IP 地址时，设备会根据该地址和掩码生成一条该网段的直连路由；
- 静态路由：自定义路由，由用户手动配置；
- 动态路由：通过动态路由协议发现到的路由。根据是否在一个自治域内部使用，动态路由协议分为内部网关协议（IGP）和外部网关协议（EGP）。这里的自治域指一个具有统一管理机构、统一路由策略的网络。自治域内部采用的路由选择协议称为内部网关协议，常用的有 RIP、OSPF；外部网关协议主要用于多个自治域之间的路由选择，常用的有 BGP。

路由支持负载均衡，即到同一个目的地有多条路由，报文转发时，设备根据路由表查找结果按照指定的负载均衡方式发送。

36.2 路由基础功能配置

表 36-1 路由基础功能配置列表

配置任务	
配置路由负载均衡	配置最大负载均衡条目数
配置 VRF 路由容量	配置 VRF 路由容量

36.2.1 配置路由负载均衡 **-B -S -E -A**

配置条件

无

配置最大负载均衡条目数

当到达某一目的地有几条路径开销相同，则形成负载均衡，配置最大负载均衡条目数，有助于提高链路的利用率并减少链路的负担。

表 36-2 配置最大负载均衡条目数

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置最大负载均衡条目数	route path-limit max-number	可选 缺省情况下，路由最大负载均衡条目数值为 4

36.2.2 配置 VRF 路由容量 **-E -A**

配置条件

无

配置 VRF 路由容量

为了保证设备的正常使用，防止大量路由消耗过多的资源，用户可以配置 **routing-table limit** 限制各 VRF 下路由的容量，并在路由量达到设定值时，产生告警信息。

表 36-3 配置 VRF 路由容量

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 VRF 配置模式	ip vrf vrf-name	-
配置 VRF 路由容量	routing-table limit limit-value { <i>threshold-value</i> syslog-alert }	可选 缺省情况下，路由容量为 220000，当路由数达到容量的 80% 时，打印告警信息

说明：

- 该命令无法限制全局 VRF 下的路由容量。
- 若路由条目超过容量，会导致新增路由信息丢失。

36.2.3 路由基础监控与维护**-B -S -E -A**

表 36-4 路由基础监控与维护

单播路由

命令	说明
clear ip route [vrf <i>vrf-name</i>] { <i>ip-address mask</i> all }	清除路由表中指定 IP 路由
show ip route [vrf <i>vrf-name</i>] [bgp connected irmp isis ospf rip static statistic [all] <i>ip-address</i> { <i>mask</i> <i>mask-len</i> }]	显示 IP 路由信息

37 IPv6 路由基础

37.1 IPv6 路由基础简介

路由是指设备从一个接口收到 IPv6 报文，根据 IPv6 报文的目地址选路并转发到另一个接口的过程。在网络设备中，路由存储在一个叫做路由表数据库中，报文根据目的地址查找路由表确定该报文的下一跳和出接口。路由根据来源不同分为以下三类：

- 直连路由：由接口地址产生的路由。当用户配置接口的 IPv6 地址时，设备会根据该地址和掩码生成一条该网段的直连路由。
- 静态路由：自定义路由，由用户手动配置。
- 动态路由：通过动态路由协议发现到的路由。根据是否在一个自治域内部使用，动态路由协议分为内部网关协议（IGP）和外部网关协议（EGP）。这里的自治域指一个具有统一管理机构、统一路由策略的网络。自治域内部采用的路由选择协议称为内部网关协议，常用的有 RIPng、OSPFv6；外部网关协议主要用于多个自治域之间的路由选择，常用的有 IPv6 BGP。

路由支持负载均衡，即到同一个目的地有多条路由，报文转发时，设备根据路由表查找结果按照指定的负载均衡方式发送。

37.2 IPv6 路由基础功能配置

表 37-1 IPv6 路由基础功能配置列表

配置任务	
配置 IPv6 路由负载均衡	配置 IPv6 最大负载均衡条目数
	配置 IPv6 负载均衡计算方式

37.2.1 配置 IPv6 路由负载均衡

-B -S -E -A**配置条件**

无

配置 IPv6 负载均衡计算方式

负载均衡存在如下三种计算方式：

- 基于源和目的地址的计算方式：用源地址和目的地址标识一条流，同一条流的报文走同一条路径，不会乱序。当各条流的负载不均衡时，可能导致线路负载不均衡。
- 基于源地址的计算方式：仅使用源地址标识一条流。同一条流的报文使用同一条路径，保证同一条流走同一条路径，不会乱序。当各条流的负载不均衡时，可能导致线路负载不均衡。
- 基于报文的计算方式：到同一目的地的报文，走不同的路径，尽可能达到各条路径上负载的均衡，但有可能乱序。

表 37-2 配置 IPv6 负载均衡计算方式

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 IPv6 报文负载均衡方式	ipv6 load-sharing { per-destination per-packet per-source }	可选 缺省情况下，使用基于源和目的地址的计算方式

37.2.2 IPv6 路由基础监控与维护

-B -S -E -A

表 37-3 IPv6 路由基础监控与维护

命令	说明
<code>clear ipv6 route { ipv6-address ipv6-prefix all }</code>	清除路由表中指定 IPv6 路由
<code>show ipv6 route [vrf vrf-name] [ipv6-address ipv6-prefix bgp brief connected isis linklocal local ospf rip static statistic all]</code>	显示 IPv6 路由信息

38 静态路由

38.1 静态路由简介

静态路由是自定义路由，由用户手动配置，它使去往指定目的地的 IP 数据包根据用户指定路径进行传输。

静态路由与动态路由协议相比较，它的优点在于安全性更高，设备资源占用率低。它的不足在于当网络拓扑改变时，需要用户手动进行配置，缺少自动重配置机制。

静态路由不需要占用线路带宽，及占用 CPU 周期去计算和通告路由，因此可以改进设备和网络性能。

单播路由

静态路由可用于对小型网络的安全性保障，例如只有一条路径连接到外部网络的情况。在大型网络中，静态路由也可以对某些类型的业务或链路进行安全控制，大多数网络采用动态路由协议，但可以配置少量静态路由用于特殊情况。

静态路由可以被重分发到动态路由协议，但动态路由协议产生的路由不能被重分发到静态路由，需要注意的是不合理的静态路由配置可能引起路由环路。

缺省路由是一种特殊的路由，可以通过静态路由配置。在路由表中，缺省路由以到网络 0.0.0.0、掩码 0.0.0.0 的路由形式出现。可通过命令 `show ip route` 查看是否生效。当接收报文的地址不能与路由表的任何表项匹配时，该报文将选取缺省路由。如果没有缺省路由且报文的目的地不在路由表中，那么该报文被丢弃的同时，将向源端返回一个 ICMP 报文报告该目的地或目的网络不可达。为了不使路由表过于庞大，可以设置一条缺省路由。凡遇到查找路由表失败后的数据包，就选择缺省路由转发。

Null0 路由也是一种特殊的路由，路由出接口为 Null0 接口。Null0 接口永远处于 UP 状态，但不能转发数据包，发往该接口的数据报文都会被丢弃。通过配置静态路由指定到达某一网段的出接口为 Null0 时，则任何发往该网段的报文都会被丢弃，因此可通过配置 Null0 静态路由实现报文过滤功能。

38.2 静态路由功能配置

表 38-1 静态路由配置功能列表

配置任务	
配置静态路由	配置静态路由
配置缺省管理距离	配置缺省管理距离
配置递归功能	配置递归功能
配置负载均衡路由	配置负载均衡路由
配置浮动路由	配置浮动路由

配置任务	
配置静态路由与 BFD 联动	配置静态路由与 BFD 联动
配置静态路由与 TRACK 联动	配置静态路由与 TRACK 联动

38.2.1 配置静态路由

-B -S -E -A

配置条件

在配置静态路由之前，首先完成以下任务：

- 配置链路层协议，保证链路层通信正常；
- 配置接口的 IP 地址，使各相邻节点网络层可达。

配置静态路由

静态路由按指定的参数不同，可分为如下三种：

- 接口路由：只指定路由的出接口；
- 网关路由：只指定路由的网关地址；
- 接口网关路由：同时指定路由的出接口和网关地址。

配置的静态路由在以下情况失效：

- 1) 目的地址为本地接口地址；
- 2) 目的网络为本地直连接口网络；
- 3) 路由的管理距离为 255；
- 4) 路由出接口 DOWN；
- 5) 路由出接口没有配置 IP 地址；
- 6) 网关地址不可达；
- 7) 路由出接口和网关冲突；
- 8) 路由出接口不存在；

9) 路由关联的 TRACK 对象为“假”；

10) 路由关联的 BFD 会话状态为 DOWN。

接口路由只要包含了•)、•)、•)、•)、•)、•)、••) 中的任意一条则路由无效；网关路由只要包含了•)、•)、•)、•)、•)、•)、••) 中的任意一条则路由无效；接口网关路由只要包含了上述所有条件中的任意一条则路由无效。

表 38-2 配置静态路由

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置静态路由	ip route [vrf vrf-name1] destination-ip-address destination-mask { interface-name / [nexthop-ip-address [vrf vrf-name2]] } [name nexthop-name] [tag tag-value] [track track-id] [administrative-distance]	必选 <i>administrative-distance</i> 为该静态路由的管理距离，未指定时使用缺省的管理距离

说明：

- 配置缺省路由时目的网络和掩码都应配置为 0.0.0.0。
- Null0 路由的出接口应配置为 Null0。
- Null0 路由的出接口不需要配置 ip 地址。

38.2.2 配置缺省管理距离

-B -S -E -A**配置条件**

无

配置缺省管理距离

配置静态路由时指定的管理距离越小路由的优先级越高，未指定管理距离时使用缺省的管理距离，用户可对缺省的管理距离进行动态的修改。重新设置缺省管理距离后，新设置的缺省管理距离仅对新增的静态路由生效。

表 38-3 配置缺省管理距离

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入静态路由配置模式	router static	-
配置缺省管理距离	distance <i>administration-distance</i>	可选 缺省管理距离的缺省值为 1

说明：

- 在使用 **ip route** 命令配置静态路由时可为其单独指定管理距离 (*administrative-distance* 参数)，未指定管理距离时使用缺省的管理距离。

38.2.3 配置递归功能

-B -S -E -A**配置条件**

单播路由

无

配置递归功能

如果配置的路由网关地址必须通过网关路由可达才能生效，则需要把静态路由的递归功能打开才能使该路由生效。缺省情况下静态路由的递归功能是打开的。

表 38-4 配置递归功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入静态路由配置模式	router static	-
配置静态路由支持递归功能	recursion	可选 缺省情况下，静态路由支持路由递归功能

38.2.4 配置负载均衡路由 *-B -S -E -A*

配置条件

无

配置负载均衡路由

负载均衡路由是指去往同一目的网络具有多条路由，这些路由的出接口不同或网关地址不同，但所有这些路由的管理距离（优先级）相同；通过配置这些路由负载均衡可以提高链路利用率。

表 38-5 配置负载均衡路由

步骤	命令	说明
进入全局配置模式	configure terminal	-

单播路由

步骤	命令	说明
配置第一条负载均衡路由	ip route <i>destination-ip-address destination-mask interface-name1 distance</i>	必选 出接口为 interface-name1
配置第二条负载均衡路由	ip route <i>destination-ip-address destination-mask interface-name2 distance</i>	必选 出接口为 <i>interface-name2</i>

说明：

- 配置负载均衡路由时 *distance* 的取值应相等。

38.2.5 配置浮动路由

-B -S -E -A

配置条件

无

配置浮动路由

浮动静态路由是指到达同一目的网络有多条路由，这些路由除了出接口不同或网关地址不同外，路由的优先级也不同，优先级高的为首选路由，优先级低的为浮动路由；在路由表中只能看到首选路由，只有在首选路由失效的情况下浮动路由才会出现在路由表中，因此浮动路由一般用来作为备份路由使用。

表 38-6 配置浮动路由

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
配置首选路由	ip route <i>destination-ip-address destination-mask interface-name1 distance1</i>	必选 首选路由的出接口为 <i>interface-name1</i> , 优先级为 <i>distance1</i>
配置浮动路由	ip route <i>destination-ip-address destination-mask interface-name2 distance2</i>	必选 浮动路由的出接口为 <i>interface-name2</i> , 优先级为 <i>distance2</i> , <i>distance2</i> 的值应大于 <i>distance1</i>

说明:

- 在指定路由的优先级时, *distance* 的值越小表示优先级越高。

38.2.6 配置静态路由与 BFD 联动 **-E -A**

配置条件

无

配置静态路由与 BFD 联动

BFD (Bidirectional Forwarding Detection, 双向转发检测) 协议提供一种轻负载、快速检测两台邻接路由器之间转发路径连通状态的方法。协议邻居通过该方式可以快速检测到转发路径的连通故障。静态路由不同于其他动态协议路由, 无法感知通信链路的故障, BFD 为静态路由提供了一个快速检测通信链路故障的方法, 配置静态路由与 BFD 联动后可快速实现路由的切换。目前静态路由只支持建立异步的 BFD 检测模式, 所以需要在链路两端的设备上配置与 BFD 联动。

当静态路由关联的 BFD 状态为 DOWN 时，配置的静态路由将失效。

表 38-7 配置静态路由与 BFD 联动

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置一条静态路由	ip route destination-ip-address destination-mask interface-name nexthop-ip-address	必选 只有同时指定了出接口和网关地址的静态路由才能和 BFD 联动
配置与 BFD 关联路由的出接口和下一跳地址	ip route static bfd interface-name nexthop-ip-address	必选 <i>nexthop-ip-address</i> 是直连的下一跳地址

说明：

- 有关 bfd 的介绍和基本功能配置，请参见 bfd 配置手册；

38.2.7 配置静态路由与 TRACK 联动

-B -S -E -A

配置条件

无

配置静态路由与 TRACK 联动

系统中有的模块需要监控一些系统信息，并根据这些信息确定自己的运行方式。这些被其它模块监控的对象，称之为监控对象。为了能够简化模块同监控对象之间的关系，可以使用 Track。一个 Track 对象可以容纳多个监控对象，并将这些监控对象的综合状态统一展现给外部模块。而外部模块仅仅同

单纯的 Track 对象关联，不再关心更细节的监控对象。Track 对象对外表现为两个状态“真”或者“假”，同 Track 对象关联的外部模块根据 Track 对象的状态来确定自己的运行方式。

静态路由可和 Track 对象进行关联来监控系统的信息，根据 Track 对象上报的状态来确定路由是否有效，当 Track 对象上报的状态为“真”时并且满足静态路由生效的条件，则将该路由添加到路由表中，当 Track 对象上报的状态为“假”时将该路由从路由表中删除。

表 38-8 配置静态路由与 TRACK 联动

步骤	命令	说明
进入全局配置模式	configure terminal	-
创建 Track 对象并进入该对象的配置模式	track track-id	必选
配置 Track 对象监控指定接口的链路状态	interface interface-name line-protocol	可选
返回全局配置模式	exit	-
配置一条静态路由并且与 Track 关联	ip route destination-ip-address destination-mask interface-name track track-id	必选 当监控接口的链路层 UP 时该路由生效，否则失效

38.2.8 静态路由监控与维护

-B -S -E -A

表 38-9 静态路由监控与维护

命令	说明
show ip route [vrf vrf-name] static	显示路由表中的静态路由

命令	说明
<code>show running-config ip route</code>	显示静态路由的配置信息

38.3 静态路由典型配置举例

38.3.1 配置静态路由基本功能

-B -S -E -A

网络需求

- Device1、Device2 和 Device3 配置静态路由，使得 PC1 和 PC2 之间能够互相通信。

网络拓扑



图 38-1 配置静态路由基本功能组网图

配置步骤

- 步骤 1：配置 VLAN，并将端口加入对应的 VLAN。（略）
- 步骤 2：配置各接口 IP 地址。（略）
- 步骤 3：配置静态路由。

#配置 Device1。

```
Device1#configure terminal
```

单播路由

```
Device1(config)#ip route 20.1.1.0 255.255.255.0 10.1.1.2
Device1(config)#ip route 100.1.1.0 255.255.255.0 10.1.1.2
```

#配置 Device2。

```
Device2#configure terminal
Device2(config)#ip route 110.1.1.0 255.255.255.0 10.1.1.1
Device2(config)#ip route 100.1.1.0 255.255.255.0 20.1.1.2
```

#配置 Device3。

```
Device3#configure terminal
Device3(config)#ip route 0.0.0.0 0.0.0.0 20.1.1.1
```

#查看 Device1 的路由表。

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C 10.1.1.0/24 is directly connected, 00:06:47, vlan3
S 20.1.1.0/24 [1/100] via 10.1.1.2, 00:00:13, vlan3
S 100.1.1.0/24 [1/100] via 10.1.1.2, 00:00:05, vlan3
C 110.1.1.0/24 is directly connected, 00:08:21, vlan2
C 127.0.0.0/8 is directly connected, 28:48:33, lo0
```

#查看 Device2 的路由表。

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C 10.1.1.0/24 is directly connected, 00:00:37, vlan2
C 20.1.1.0/24 is directly connected, 00:00:27, vlan3
S 100.1.1.0/24 [1/100] via 20.1.1.2, 00:00:05, vlan3
S 110.1.1.0/24 [1/100] via 10.1.1.1, 00:00:13, vlan2
C 127.0.0.0/8 is directly connected, 30:13:18, lo0
```

#查看 Device3 的路由表。

```
Device3#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is 20.1.1.2 to network 0.0.0.0

S 0.0.0.0/0 [1/100] via 20.1.1.1, 00:00:07, vlan2
C 20.1.1.0/24 is directly connected, 00:00:08, vlan2
C 100.1.1.0/24 is directly connected, 00:00:13, vlan3
C 127.0.0.0/8 is directly connected, 29:17:19, lo0
```

步骤 4: 检验结果, 用 **ping** 命令验证 PC1 与 PC2 的连通性。

#PC1 上使用 **ping** 命令验证连通性。

```
C:\Documents and Settings\Administrator>ping 100.1.1.2
```

Pinging 100.1.1.2 with 32 bytes of data:

```
Reply from 100.1.1.2: bytes=32 time<1ms TTL=125
Reply from 100.1.1.2: bytes=32 time<1ms TTL=125
Reply from 100.1.1.2: bytes=32 time<1ms TTL=125
Reply from 100.1.1.2: bytes=32 time<1ms TTL=125
```

Ping statistics for 100.1.1.2:

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

PC1 和 PC2 可以互相通信。

38.3.2 配置静态浮动路由 *-B -S -E -A*

网络需求

- Device1 配置两条静态路由通往 192.168.1.0/24 网段，一条通过 Device2 可达，另一条通过 Device3 可达。
- Device1 优先使用与 Device2 之间的线路转发报文；当该线路出现故障后切换到 Device3 进行通信。

网络拓扑

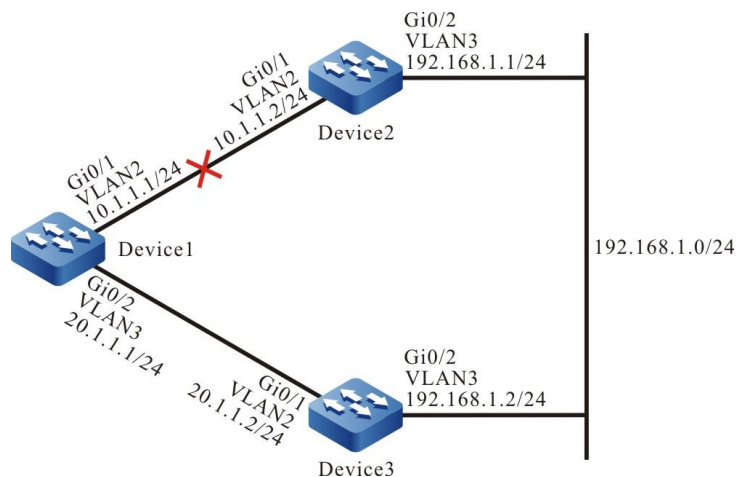


图 38-2 配置静态浮动路由组网图

配置步骤

步骤 1：配置 VLAN，并将端口加入对应的 VLAN。（略）

步骤 2：配置各接口 IP 地址。（略）

步骤 3: 配置静态路由。

#配置 Device1, 分别经过 Device2 和 Device3 通往 192.168.1.0/24 网段。

```
Device1#configure terminal
Device1(config)#ip route 192.168.1.0 255.255.255.0 10.1.1.2
Device1(config)#ip route 192.168.1.0 255.255.255.0 20.1.1.2
```

#查看 Device1 的路由表。

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C 10.1.1.0/24 is directly connected, 02:16:43, vlan2
C 20.1.1.0/24 is directly connected, 03:04:15, vlan3
C 127.0.0.0/8 is directly connected, 14:53:00, lo0
S 192.168.1.0/24 [1/100] via 10.1.1.2, 00:00:05, vlan2
  [1/100] via 20.1.1.2, 00:00:02, vlan3
```

可以看到, Device1 上存在两条可达 192.168.1.0/24 网段的路由, 并形成负载均衡。

步骤 4: 配置浮动路由。

#配置 Device1, 修改网关为 20.1.1.2 路由的管理距离为 15, 使其成为浮动路由。

```
Device1(config)#ip route 192.168.1.0 255.255.255.0 20.1.1.2 15
```

步骤 5: 检验结果。

#查看 Device1 的路由表。

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C 10.1.1.0/24 is directly connected, 02:28:25, vlan2
C 20.1.1.0/24 is directly connected, 03:15:58, vlan3
C 127.0.0.0/8 is directly connected, 15:04:42, lo0
S 192.168.1.0/24 [1/100] via 10.1.1.2, 00:11:47, vlan2
```

从路由表中可以看到, 由于管理距离为 1 的路由优先于管理距离为 15 的路由, 因此网关为 20.1.1.2 的路由被删除了。

#当 Device1 与 Device2 之间的线路出现故障后, 查看 Device1 的路由表。

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS
```

Gateway of last resort is not set

```
C 20.1.1.0/24 is directly connected, 03:23:44, vlan3
C 127.0.0.0/8 is directly connected, 15:12:28, lo0
S 192.168.1.0/24 [15/100] via 20.1.1.2, 00:00:02, vlan3
```

从路由表中可以看到，管理距离较大的路由会被添加至路由表，由 Device3 进行数据转发。

说明：

- 静态浮动路由最大的特点就是可以进行路由备份。
-

38.3.3 配置静态 Null0 接口路由

-S -E -A

网络需求

- Device1 和 Device2 上分别配置一条静态默认路由，网关地址分别为 2 台设备对端接口地址。Device1 配置静态 Null0 接口路由，仅过滤掉通往 PC2 的数据。

网络拓扑

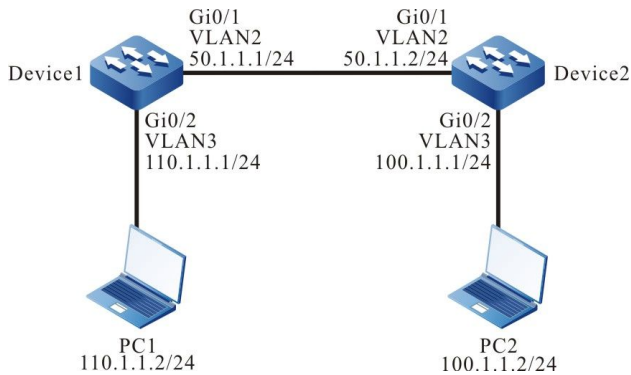


图 38-3 配置静态 Null0 接口路由组网图

配置步骤

步骤 1：配置 VLAN，并将端口加入对应的 VLAN。（略）

步骤 2：配置各接口 IP 地址。（略）

单播路由

步骤 3: 配置静态路由。

#配置 Device1。

```
Device1#configure terminal
Device1(config)#ip route 0.0.0.0 0.0.0.0 50.1.1.2
```

#配置 Device2。

```
Device2#configure terminal
Device2(config)#ip route 0.0.0.0 0.0.0.0 50.1.1.1
```

#PC1 用 ping 命令验证与 PC2 的连通性。

```
C:\Documents and Settings\Administrator>ping 100.1.1.2

Pinging 100.1.1.2 with 32 bytes of data:

Reply from 100.1.1.2: bytes=32 time<1ms TTL=126
Reply from 100.1.1.2: bytes=32 time<1ms TTL=126
Reply from 100.1.1.2: bytes=32 time<1ms TTL=126
Reply from 100.1.1.2: bytes=32 time<1ms TTL=126

Ping statistics for 100.1.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

步骤 4: 配置静态 Null0 接口路由。

#配置 Device1。

```
Device1(config)#ip route 100.1.1.2 255.255.255.255 null0
```

步骤 5: 检验结果。

#查看 Device1 路由表。

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is 50.1.1.2 to network 0.0.0.0

S 0.0.0.0/0 [1/100] via 50.1.1.2, 00:07:28, vlan2
C 50.1.1.0/24 is directly connected, 00:07:34, vlan2
C 110.1.1.0/24 is directly connected, 00:00:08, vlan3
C 127.0.0.0/8 is directly connected, 11:46:35, lo0
S 100.1.1.2/32 [1/1] is directly connected, 00:02:31, null0
```

路由表中已经添加了静态 Null0 接口路由。

单播路由

#PC1 上用 ping 命令验证与 PC2 的连通性。

```
C:\Documents and Settings\Administrator>ping 100.1.1.2

Pinging 100.1.1.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 100.1.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)
```

PC1 发送的 ICMP 报文在 Device1 上查找路由表后，发现出接口为 Null0，直接丢弃，因此，PC1 不能与 PC2 通信。

说明：

- 静态 Null0 接口路由是一种特殊的路由，发往该 Null0 接口的数据报文都会被丢弃；因此配置静态 Null0 接口路由可实现对报文过滤。
-

38.3.4 配置静态递归路由 *-B -S -E -A*

网络需求

- Device1 配置两条静态路由可达 192.168.1.1/32 网段，一条通过 Device2 可达，另一条通过 Device3 可达。Device1 优先使用与 Device3 之间的线路转发报文。
- Device1 配置一条静态递归路由可达 200.0.0.0/24 网段，网关地址为 Device3 的环回接口地址 192.168.1.1。Device1 与 Device3 之间的线路出现故障后，该路由会切换到 Device2 进行通信。

网络拓扑

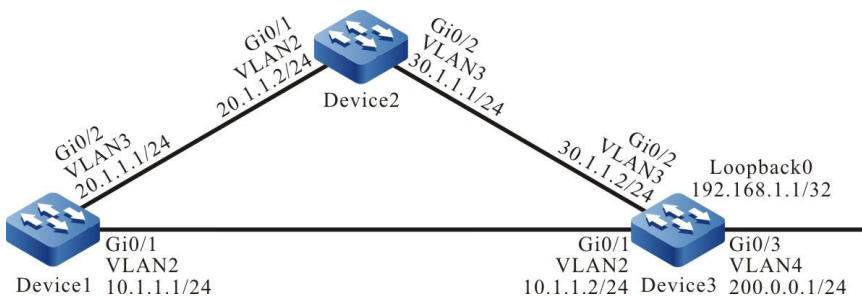


图 38-4 配置静态递归路由组网图

配置步骤

步骤 1: 配置 VLAN, 并将端口加入对应的 VLAN。 (略)

步骤 2: 配置各接口 IP 地址。 (略)

步骤 3: 配置静态路由。

#配置 Device1。

```
Device1#configure terminal
Device1(config)#ip route 192.168.1.1 255.255.255.255 10.1.1.2
Device1(config)#ip route 192.168.1.1 255.255.255.255 20.1.1.2 10
```

#配置 Device2。

```
Device2#configure terminal
Device2(config)#ip route 192.168.1.1 255.255.255.255 30.1.1.2
```

步骤 4: 配置静态递归路由。

#配置 Device1。

```
Device1(config)#ip route 200.0.0.0 255.255.255.0 192.168.1.1
```

#查看 Device1 的路由表。

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C 10.1.1.0/24 is directly connected, 00:04:07, vlan2
C 20.1.1.0/24 is directly connected, 00:03:58, vlan3
C 127.0.0.0/8 is directly connected, 73:10:12, lo0
S 200.0.0.0/24 [1/100] via 192.168.1.1, 00:00:08, vlan2
S 192.168.1.1/32 [1/100] via 10.1.1.2, 00:01:46, vlan2
```

从路由表中可以看到, 200.0.0.0/24 这条路由的网关地址为 192.168.1.1, 出接口为 VLAN2, 该路由依赖于 192.168.1.1/32 这条路由。

步骤 5: 检验结果。

#当 Device1 与 Device3 之间的线路出现故障后, 查看 Device1 的路由表。

```
Device1#show ip route
```

单播路由

Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

```
C 20.1.1.0/24 is directly connected, 00:09:04, vlan3
C 127.0.0.0/8 is directly connected, 73:15:18, lo0
S 200.0.0.0/24 [1/100] via 192.168.1.1, 00:00:02, vlan3
S 192.168.1.1/32 [10/100] via 20.1.1.2, 00:00:02, vlan3
```

对比步骤 3 的路由表可以看到，路由 200.0.0.0/24 的出接口为 VLAN3，表明已经切换到 Device2 进行通信。

38.3.5 配置静态路由与 BFD 联动 -E -A

网络需求

- Device1 配置两条静态路通往 201.0.0.0/24 网段，一条通过 Device2 可达，另一条通过 Device3 可达，Device1 优先使用与 Device3 之间的线路转发报文。同样的，Device3 配置两条静态路通往 200.0.0.0/24 网段，Device3 优先使用与 Device1 之间的线路转发报文。
- Device1 和 Device3 上配置静态路由与 BFD 联动，当 Device1 与 Device3 之间的线路发生故障后，快速切换到 Device2 进行通信。

网络拓扑

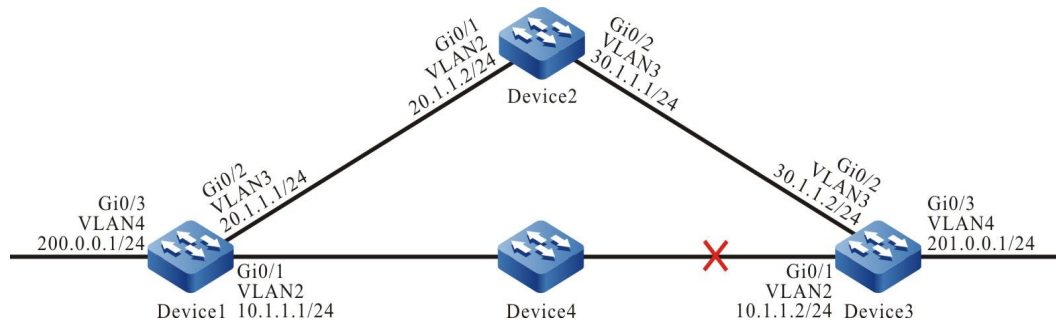


图 38-5 配置静态路由与 BFD 联动组网图

配置步骤

步骤 1：配置 VLAN，并将端口加入对应的 VLAN。（略）

步骤 2：配置各接口 IP 地址。（略）

步骤 3：配置静态路由。

单播路由

#配置 Device1，配置两条静态路由通往 201.0.0.0/24 网段。

```
Device1#configure terminal
Device1(config)#ip route 201.0.0.0 255.255.255.0 vlan2 10.1.1.2
Device1(config)#ip route 201.0.0.0 255.255.255.0 vlan3 20.1.1.2 10
```

#配置 Device2，分别配置静态路由通往 200.0.0.0/24 网段和 201.0.0.0/24 网段。

```
Device2#configure terminal
Device2(config)#ip route 200.0.0.0 255.255.255.0 20.1.1.1
Device2(config)#ip route 201.0.0.0 255.255.255.0 30.1.1.2
```

#配置 Device3，配置两条静态路由通往 200.0.0.0/24 网段。

```
Device3#configure terminal
Device3(config)#ip route 200.0.0.0 255.255.255.0 vlan2 10.1.1.1
Device3(config)#ip route 200.0.0.0 255.255.255.0 vlan3 30.1.1.1 10
```

#查看 Device1 的路由表。

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C 10.1.1.0/24 is directly connected, 00:07:41, vlan2
C 20.1.1.0/24 is directly connected, 00:07:29, vlan3
C 127.0.0.0/8 is directly connected, 101:56:14, lo0
C 200.0.0.0/24 is directly connected, 00:15:33, vlan4
S 201.0.0.0/24 [1/100] via 10.1.1.2, 00:02:23, vlan2
```

#查看 Device3 的路由表。

```
Device3#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C 10.1.1.0/24 is directly connected, 00:10:21, vlan2
C 30.1.1.0/24 is directly connected, 00:10:09, vlan3
C 127.0.0.0/8 is directly connected, 126:44:08, lo0
S 200.0.0.0/24 [1/100] via 10.1.1.1, 00:06:12, vlan2
C 201.0.0.0/24 is directly connected, 00:20:37, vlan4
```

步骤 4：配置静态路由与 BFD 联动。

#配置 Device1。

```
Device1(config)#bfd fast-detect
Device1(config)#ip route static bfd vlan2 10.1.1.2
```

#配置 Device3。

```
Device3(config)#bfd fast-detect
Device3(config)#ip route static bfd vlan2 10.1.1.1
```

步骤 5: 检验结果。

#查看 Device1 的 BFD 会话。

```
Device1#show bfd session
OurAddr      NeighAddr      LD/RD      State      Holddown      interface
10.1.1.1      10.1.1.2      15/22      UP         5000          vlan2
```

#查看 Device3 的 BFD 会话。

```
Device3#show bfd session
OurAddr      NeighAddr      LD/RD      State      Holddown      interface
10.1.1.2      10.1.1.1      22/15      UP         5000          vlan2
```

Device1、Device3 上 BFD 会话正常建立，表明静态路由与 BFD 联动成功。

#当 Device1 与 Device3 之间线路由出现故障时，BFD 会快速检测到线路故障，切换到 Device2 进行通信。查看 Device1 的 BFD 会话和路由表。

```
Device1#show bfd session
OurAddr      NeighAddr      LD/RD      State      Holddown      interface
10.1.1.1      10.1.1.2      15/0       DOWN      5000          vlan2
```

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNRP, B - BGP, i-ISIS
```

Gateway of last resort is not set

```
C 10.1.1.0/24 is directly connected, 00:29:07, vlan2
C 20.1.1.0/24 is directly connected, 00:28:55, vlan3
C 127.0.0.0/8 is directly connected, 102:17:40, lo0
C 200.0.0.0/24 is directly connected, 00:36:58, vlan4
S 201.0.0.0/24 [10/100] via 20.1.1.2, 00:00:09, vlan3
```

Device3 上 BFD 处理方式与 Device1 类似。

39 RIP

39.1 RIP 简介

在目前的 Internet 网上，运行一种网关协议是不可能的，我们要将它分成很多的自治系统 (Autonomous System - AS)，在每个自治系统有它自己的路由技术。我们称自治系统内部的路由协议为内部网关协议 (Interior gateway protocol - IGP)。RIP (Routing Information Protocol) 就是内部网关协议的一种，它采用的是矢量距离(Vector - Distance)算法。由于 RIP 简单易用的特点，因此被广泛应用于众多小型网络。

RIP 协议有 RIPv1 和 RIPv2 两个版本，两个版本的主要区别是 RIPv1 不支持无类别路由，而 RIPv2 支持无类别路由。一般情况下使用 RIPv2 版本。

RIP 协议具有协议简单、配置简单等优点，但 RIP 协议需要通告的路由信息和路由表的路由数量成正比，当路由比较多时，比较消耗设备资源与网络资源。同时 RIP 协议规定了路由路径经过路由器的最大跳数为 15，所有 RIP 协议只适用于比较简单的中小型网络。RIP 协议可用于大多数校园网及结构较简单的连续性强的地区性网络。对于更复杂的环境，一般不使用 RIP 协议。

RIPv1 被较早提出，最早的标准是 RFC1058，但其中有许多缺陷。为了改善 RIPv1 的不足，在 RFC1388 中提出了改进的 RIPv2，并在 RFC 1723 和 RFC 2453 中进行了修订。

39.2 RIP 功能配置

表 39-1 RIP 功能配置列表

配置任务	
配置 RIP 基本功能	全局使能 RIP 协议
	VRF 使能 RIP 协议
	配置 RIP 版本
配置 RIP 路由生成	配置 RIP 发布缺省路由
	配置 RIP 路由重分发
配置 RIP 路由控制	配置 RIP 管理距离
	配置 RIP 路由汇总
	配置 RIP 度量偏移
	配置 RIP 路由过滤
	配置 RIP 接口度量值
	配置 RIP 接口路由标记
	配置 RIP 最大负载均衡
配置 RIP 网络认证	配置 RIP 网络认证
配置 RIP 网络优化	配置 RIP 定时器
	配置 RIP 水平分割与毒性逆转

配置任务	
	配置源地址检查
	配置 RIP 静态邻居
	配置 RIP 被动接口
	配置 RIP 触发更新
	配置 RIP 备份接口
配置 RIP 与 BFD 联动	配置 RIP 与 BFD 联动

39.2.1 配置 RIP 基本功能

-S -E -A

配置条件

在配置 RIP 的基本功能之前，首先完成以下配置：

- 配置链路层协议，保证链路层通信正常；
- 配置接口的网络层地址，使相邻网络节点网络层可达。

全局使能 RIP 协议

使用 RIP 协议，需要进行如下配置：

- 创建 RIP 进程；
- 配置 RIP 覆盖直连网络或某接口。

表 39-2 全局使能 RIP 协议

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
创建 RIP 进程并进入 RIP 配置模式	router rip	必选 缺省情况下, 未启用 RIP 进程
覆盖指定网段或接口	network { ip-address interface-name }	必选 缺省情况下, 没有覆盖任何直连网络和接口

说明:

- 配置覆盖的网段将自动划分为有类地址。
- **network ip-address** 无法覆盖超网地址, 可以通过 **network interface-name** 覆盖超网地址。

VRF 使能 RIP 协议

RIP 支持 VRF 功能, 需要进行如下配置:

- 配置某 VRF, 并指定某接口加入到该 VRF 中;
- 指定在该 VRF 地址簇中启用 RIP 功能;
- 配置 RIP 覆盖某 VRF 直连网络或所属接口。

表 39-3 VRF 使能 RIP 协议

步骤	命令	说明
进入全局配置模式	configure terminal	-
创建 RIP 进程并进入 RIP 配置模式	router rip	必选

步骤	命令	说明
		缺省情况下，未启用 RIP 进程
进入 RIP 协议 VRF 地址簇配置模式	address-family { ipv4 vrf vrf-name }	必选 缺省情况下，不启用 VRF 地址簇模式
覆盖指定网段或接口	network { ip-address interface-name }	必选 缺省情况下，没有覆盖任何直连网络和接口

说明：

- VRF 模式下启用 RIP 协议，必须先创建 VRF 相关配置。

配置 RIP 版本

RIP 支持 RIPv1 与 RIPv2 两个版本，可以在全局、VRF、接口三种模式下配置：

- 缺省情况下，全局、VRF 模式下启用 RIPv1 版本，接口下未配置；
- 接口下配置的版本命令的优先级高于全局或 VRF 的版本配置命令；
- 接口下未配置版本命令时，将采用接口所在 VRF 或全局版本命令；
- 接口模式下，RIP 收发版本可以单独配置；
- 配置上版本后，RIP 具有严格的报文收发处理：当配置为 RIPv1 时，只收发 RIPv1 的广播或单播报文；为 RIPv2 时可收发 RIPv2 的单播、组播、或广播报文，仅在 RIPv1 兼容模式时，可发送 RIPv2 的单播、广播报文。

表 39-4 配置 RIP 版本

步骤	命令	说明
进入全局配置模式	configure terminal	-
创建 RIP 进程并进入 RIP 配置模式	router rip	必选 缺省情况下, 未启用 RIP 进程
配置全局 RIP 版本	version { 1 2 }	必选 缺省情况下, 启用 RIPv1
进入 RIP VRF 配置模式	address-family { ipv4 vrf vrf-name }	必选 缺省情况下, 不启用 VRF 地址簇
配置 RIP VRF 配置模式下的 RIP 版本	version { 1 / 2 }	必选 缺省情况下, 启用 RIPv1
退回 RIP 配置模式	exit-address-family	-
退回全局配置模式	exit	-
进入接口配置模式	interface interface_name	-
配置接口发送 RIP 版本	ip rip send version { { 1 / 2 } 1-compatible }	可选 缺省情况下, 根据 RIP 全局版本发送报文
配置接口接收 RIP 版本	ip rip receive version { 1 / 2 }	可选 缺省情况下, 根据 RIP 全局版本接收报文

39.2.2 配置 RIP 路由生成

-S -E -A**配置条件**

在配置 RIP 路由生成前，首先完成以下任务：

- 配置接口的 IP 地址，使各相邻节点网络层可达；
- 使能 RIP 协议。

配置 RIP 发布缺省路由

通过配置，设备可以在所有 RIP 接口下发送缺省路由，将自己设置为其他相邻设备的缺省网关。

表 39-5 配置 RIP 发布缺省路由

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 RIP 配置模式	router rip	必选 缺省情况下，未启用 RIP 进程
配置 RIP 发布缺省路由	default-information originate	必选 缺省情况下，RIP 不发布缺省路由

说明：

- 如果学习到一条默认路由（0.0.0.0/0），则会替换本设备发布的默认路由（0.0.0.0/0）。当网络存在环路时，可能会造成路由振荡。故使用该命令时应避免相同路由由域内多台设备同时启用该命令。

配置 RIP 路由重分发

可以通过配置路由重分发将其他协议产生的路由引入到 RIP 中。

表 39-6 配置 RIP 路由重分发

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 RIP 配置模式	router rip	必选 缺省情况下，未启用 RIP 进程
配置 RIP 引入其它路由协议路由的缺省度量值	default-metric <i>metric-value</i>	可选 缺省情况下，引入其它协议路由的缺省度量值为 1
配置 RIP 路由重分发	redistribute <i>protocol</i> [<i>protocol-id</i>] [metric <i>metric-value</i>] [route-map <i>route-map-name</i>] [match <i>route-sub-type</i>]	必选 缺省情况下，未配置路由重分发

说明：

- 重分发时指定 **metric** 命令选项后，相应重分发的路由将采用该度量值。
- RIP 配置路由重分发应用路由策略时，支持的 **match** 选项有 **ip address**、**route type**、**tag**，支持的 **set** 选项有 **interface**、**ip next-hop**、**route source**、**metric**。

配置条件

在配置 RIP 路由控制前，首先完成以下任务：

- 配置接口的 IP 地址，使各相邻节点网络层可达；
- 使能 RIP 协议。

配置 RIP 管理距离

设备中可以同时运行多个路由协议，设备通过管理距离对各个协议学习到的路由进行优选，管理距离越小路由越优先。

表 39-7 配置 RIP 管理距离

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 RIP 配置模式	router rip	-
配置 RIP 管理距离	distance <i>distance-value</i>	必选 缺省情况下，RIP 管理距离为 120

配置 RIP 路由汇总

RIP 路由汇总是指路由设备将同一自然网段内子网路由汇总成一条路由。汇总生成的路由与原子网路由同时存在于 RIP 路由表中。

配置 RIP 路由汇总后，设备只通告汇总路由，在大中型网络中可以显著减少相邻 RIP 路由表规模，同时减少路由协议报文对网络带宽的消耗。

汇总路由的 metric 将采用所有子网路由 metric 的最小值。

RIPv1 支持自动路由汇总方式，RIPv2 支持自动路由汇总和手动汇总两种方式。

1. RIP 自动路由汇总

自动路由汇总与手动路由汇总的区别在于，自动路由汇总由 RIP 根据同一自然网段内子网路由自动生成一条自然掩码路由。

表 39-8 配置自动路由汇总功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 RIP 配置模式	router rip	必选 缺省情况下，未启用 RIP 进程
配置自动路由汇总功能	auto-summary	必选 缺省情况下，未启用路由自动路由汇总功能

说明：

- RIPv1 不支持通过命令汇总路由。
- 汇总路由的 tag 为 0，路由度量值取明细路由中的最小值。在同时配置自动汇总功能的情况下，优先进行自动汇总。
- 在 RIPv2，要慎用路由自动路由汇总功能，确定网络中确实有路由自动路由汇总的必要，否则可能会产生路由环路。
- RIPv2 开启自动路由汇总的情况下，通告路由的接口所在网段和该路由在同一自然网段时，从该接口发出的更新报文不会对该自然网段下的所有子网路由进行汇总，否则会将路由汇总成自然网段通告出去。

2. 手动路由汇总

手动路由汇总需要配置一对目的地址和掩码的组合，这对组合将对所覆盖网段内的路由进行汇总。

表 39-9 配置手动路由汇总功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface interface-name	-
配置 RIPv2 在接口上的手动路由汇总功能	ip summary-address rip prefix-address	-

配置 RIP 度量偏移

缺省情况下，RIP 对接收到的路由采用相邻设备通告的路由度量值，在某些特殊应用场景中需要对度量值进行修改，可以通过配置 RIP 的度量偏移对指定路由度量值进行校正。

配置入方向上的度量值后，将会在 RIP 路由接收时进行路由度量值修改，再将路由存放于路由表中，当通告给相邻设备时将采用新的度量值；配置出方向上的度量值则只会在通告给相邻设备时修改。

表 39-10 配置 RIP 度量偏移

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 RIP 配置模式	router rip	必选 缺省情况下，未启用 RIP 进程
配置 RIP 对指定路由的度量进行修改	offset-list access-list-name { in out } metric-offset [interface-name]	必选 缺省情况下，没有配置任何接口的度量值

说明：

- 路由度量偏移仅支持匹配标准访问列表。

配置 RIP 路由过滤

路由器可以通过配置访问控制列表或前缀列表对接收或通告路由进行过滤。在接收 RIP 路由时，过滤某些学习到的路由，或者在通告 RIP 路由时，过滤某些向相邻设备通告的路由。

表 39-11 配置 RIP 路由过滤

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 RIP 配置模式	router rip	必选 缺省情况下，未启用 RIP 进程
配置 RIP 路由过滤功能	distribute-list { <i>access-list-name</i> prefix <i>prefix-list-name</i> } { in out } [<i>interface-name</i>]	必选 缺省情况下，未配置路由过滤功能，配置路由过滤功能时，如果不指定接口，将针对所有 RIP 覆盖接口接收或发送的启用路由过滤

说明：

- 使用 ACL 过滤时仅支持标准 ACL。

配置 RIP 接口度量值

接口在被覆盖到 RIP 进程中后，在数据库中会生成相应的直连路由，缺省度量值为 1，该路由在 RIP 数据库中或者将其通告给相邻设备时，如果该接口上配置了度量值，将采用接口度量值。

当接口度量值改变后，RIP 数据库中会立即更新 RIP 相应直连路由，并通告到相邻设备。

表 39-12 配置 RIP 接口度量值

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface interface-name	-
配置 RIP 接口度量	ip rip metric metric-value	必选 缺省情况下，RIP 接口度量值为 1

说明：

- 配置 RIP 接口度量值只会影响接口上直连子网的度量，不会影响路由学习的度量。

配置 RIP 接口路由标记

路由标记即路由 tag，是为了让网络管理员对一些路由打上标记，以便在应用路由策略时根据 tag 标记做路由过滤或路由属性通告。

仅 RIPv2 支持路由标记。

表 39-13 配置 RIP 接口路由标记

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置 RIP 在接口上直连子网的路由 tag	ip rip tag <i>tag-value</i>	-

配置 RIP 最大负载均衡条目数

通过配置该命令可以控制 RIP 路由的负载条目数。

表 39-14 配置 RIP 最大负载均衡条目数

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 RIP 配置模式	router rip	必选 缺省情况下，未启用 RIP 进程
配置 RIP 最大负载均衡条目数	maximum-paths <i>max-number</i>	可选 缺省情况下，RIP 最大负载均衡条目数为 4

39.2.4 配置 RIP 网络认证

-S -E -A

RIPv2 支持协议报文认证，因此满足对安全性要求较高的网络。目前支持明文认证方式和 MD5，SM3 认证方式，明文传输的特点安全性较低，后两者对认证码生成 MD5 码，或者 SM3 码进行传输，能提供较高安全保障。

受限于 RIPv2 报文特点，通告路由的报文单元仅有 16 个字节，所以，明文认证字符串长度不能超过 16 个字节，而所有字符串生成的 MD5 码都是标准的 16 字节，刚好满足长度要求。

表 39-15 配置 RIP 网络认证

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置 RIPv2 网络认证	ip rip authentication {{ key { 0 7 } <i>key-string</i> } { key-chain <i>key-chain-name</i> } { mode { text md5 sm3 } } }	必选 缺省情况下，未配置 RIPv2 认证功能

说明：

- 在使用 MD5 或 SM3 进行认证时，有下面几点需要注意：
- RIPv1 不支持网络认证功能。
- RIPv2 同一时间只能使用一种认证方式。
- MD5 或 SM3 认证信息里面需要携带 key ID。当使用 “**ip rip authentication key**” 配置密码时，key ID 为 1；当使用 “**ip rip authentication key-chain**” 配置密码时，key ID 是密码在 key-chain 上的 key ID。

- 在 Key-chain 上获取报文发送认证密码时，将按 Key ID 从小到大的顺序选择，所以 Key ID 最小的有效发送密码将会被选中。
- 在 Key-chain 上获取报文接收认证密码，取的是密码 Key ID 大于等于接收报文 Key ID 的第一个有效接收密码。所以，当认证的两端 Key ID 不一样时，Key ID 大的一边能够认证通过，而 Key ID 小的一边不能够认证通过。

39.2.5 配置 RIP 网络优化 -S -E -A

配置条件

在配置 RIP 网络优化前，首先完成以下任务：

- 配置接口的 IP 地址，使各相邻节点网络层可达；
- 使能 RIP 协议。

配置 RIP 定时器

由于 RIP 不维护邻居关系、不支持路由撤消，所以协议提供了四个可配置的定时器来控制网络收敛速度，分别是：路由更新时间、路由超时时间、路由抑制更新时间、路由清除时间。

路由超时时间取值应至少为路由更新时间的 3 倍，在路由超时时间内未收到路由更新报文时，路由将会变为无效状态并进入抑制周期，抑制周期的长短取决于抑制更新时间，在该周期内，路由将不会被更新，抑制周期结束后进入清除周期，在该周期内可接受路由更新，如果没有接收到路由更新报文，该路由将会被删除。

表 39-16 配置 RIP 定时器

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 RIP 配置模式	router rip	必选 缺省情况下，未启用 RIP 进程

步骤	命令	说明
配置 RIP 的定时器时间	timers basic <i>update-interval</i> <i>invalid-interval</i> <i>holddown-interval</i> <i>flush-interval</i>	可选 缺省情况下，RIP 更新间隔时间 30 秒、通告有效时间 180 秒、抑制时间 180 秒、清除时间 240 秒

说明：

- 在同一 RIP 路由域中，所有设备上 **timer basic** 配置必须一致，防止出现网络震荡。

配置 RIP 水平分割和毒性逆转

水平分割和毒性逆转均是防止路由环路的机制。

1. 配置水平分割

RIP 从某个接口学习到的路由将不再向该接口通告，避免环路。

表 39-17 配置 RIP 水平分割

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置 RIP 水平分割	ip split-horizon	必选 缺省情况下，不开启水平分割功能

2. 配置毒性逆转

RIP 从某接口学习到的路由会向该接口通告，但路由度量值为最大跳数 16，以避免环路。

表 39-18 配置 RIP 毒性逆转

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置 RIP 毒性逆转	ip split-horizon poisoned	可选 缺省情况下，开启毒性逆转功能

说明：

- 水平分割和毒性逆转只对学到的路由、RIP 覆盖网络的直连路由、重分发的直连和静态路由有效。
- 水平分割与毒性逆转不能同时使用。

配置 RIP 源地址检查

源地址检查是对 RIP 接收到报文的源地址进行检查，只有报文的源地址符合预期条件才会被 RIP 处理。检查项包括：报文源地址与入接口地址属于同一个网段；报文源地址与点对点（P2P）接口的对端地址匹配。

缺省情况下，已开启 RIP 在以太接口上检查接收报文的源地址是否与接口属于同一个网段，并且不能被取消。

表 39-19 配置 RIP 源地址检查

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 RIP 配置模式	router rip	必选 缺省情况下，未启用 RIP 进程
配置 RIP 在 P2P 接口上使用源地址检查	validate-update-source check-p2p-destination	必选 缺省情况下，对 P2P 接口不检查对端地址

配置 RIP 静态邻居

RIP 不维护邻接关系，故没有邻居的概念，这里描述配置的邻居指的是相邻 RIP 路由设备。指定 RIP 静态邻居后，RIP 会向该邻居以单播形式发送 RIP 报文。该配置应用于不支持广播或组播的网络，如点到点链路，在广播或组播网络中应用该配置会导致网络中存在多个重复的 RIP 报文。

表 39-20 配置 RIP 静态邻居

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 RIP 配置模式	router rip	必选 缺省情况下，未启用 RIP 进程
配置通过单播形式通告路由信息的邻居	neighbor ip-address	必选 参数 ip-address 为对端直连接口 ip 地址

说明：

- 向静态邻居通告路由信息只会在 RIP 覆盖的接口上进行，并且 “**passive-interface**” 不能阻止向静态邻居发送报文。

配置 RIP 被动接口

为减少路由协议消耗网络带宽，被动接口（Passive Interface）功能被动态路由协议采用。RIP 在被动接口上只接收路由更新报文，不发送路由更新报文。在带宽较窄的低速网络中，被动接口配合 Neighbor 功能能有效减少 RIP 的路由交互。

表 39-21 配置 RIP 被动接口

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 RIP 配置模式	router rip	必选 缺省情况下，未启用 RIP 进程
配置 RIP 被动接口	passive-interface { default <i>interface-name</i> }	必选 缺省情况下，未配置被动接口

说明：

- **passive-interface** 不会抑制向相邻设备发送单播路由更新，与 **neighbor** 命令配合使用时，**passive-interface** 不会抑制向相邻设备发送单播路由更新。故该应用方式可以控制路由器只针对某些相邻设备以单播方式发送路由更新，而不对接口上的所有相邻设备进行广播方式（RIPv2 为组播）路由更新。

配置 RIP 触发更新

在设备收到 RIP 更新报文后，为了减少设备间路由表差异而引入的环路问题，将立即向相邻设备通告该路由的更新报文，无需等到更新定时器超时后才更新。触发更新机制加快了网络的收敛速度。

表 39-22 配置 RIP 触发更新

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface interface-name	-
配置 RIP 在接口上启用触发更新	ip rip triggered	可选 缺省情况下，未启用触发更新功能

配置 RIP 备份接口

为加快备份路由收敛，RIP 新增备份接口（Standby Interface）功能，在 RIP 相应主路由接口上指定该主接口的备份接口，在特定应用环境中，RIP 只从某一条线路学习 RIP 路由，备份线路无路由信息交互，在主接口下线后，RIP 会定期（缺省 1 秒）从备份接口上发送 Request 报文向对方请求所有路由，备份接口收到对端路由 Response 报文后，取消 Request 报文发送，更新本地路由表，同时向备份接口通告本地路由表，如果在备份接口在规定的 Timeout 时间仍然没有收到对端 Response 报文，将取消 Request 报文发送。

表 39-23 配置 RIP 备份接口

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
进入接口配置模式	interface <i>interface-name</i>	-
配置 RIP 备份接口	ip rip standby <i>interface-name</i> [timeout <i>timeout-value</i>]	可选 缺省情况下，未启用备份接口功能， <i>timeout-value</i> 缺省值为 300s

39.2.6 配置 RIP 与 BFD 联动 -E -A

备份接口只能应用于特定应用环境下，并且不能满足实时备份的需求，此时，RIP 提供端到端保护的 BFD (Bidirectional Forwarding Detection, 双向转发检测) 功能，可以实现路由的快速收敛与切换。BFD 提供一种快速检测两台设备之间线路状态的方法。当相邻的两台 RIP 设备间启动 BFD 检测后，若设备之间发生线路故障，BFD 会快速检测到故障并通知 RIP 协议，RIP 将删除关联在 BFD 接口上的 RIP 路由，如果这些路由存在备份路由，将会在极短时间（受 BFD 配置影响）内切换到备份路由。目前，RIP 仅支持 BFD 单跳双向检测。

表 39-24 配置 RIP 与 BFD 联动

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 RIP 配置模式	router rip	必选 缺省情况下，未启用 RIP 进程
配置 RIP 进程覆盖的所有接口都启用 BFD 功能	bfd all-interfaces	必选

步骤	命令	说明
		缺省情况下，未启用所有 RIP 覆盖接口 BFD 功能
回到全局配置模式	exit	-
进入接口配置模式	interface interface-name	-
配置接口上启用 BFD 功能	ip rip bfd	必选 缺省情况下，未启用接口 BFD 功能

说明：

- BFD 相关配置，请参见可靠性技术-BFD 技术手册。

39.2.7 RIP 监控与维护

-S -E -A

表 39-25 配置 RIP 监控与维护

命令	说明
show ip rip [vrf vrf-name]	显示 RIP 协议基本信息
show ip rip [vrf vrf-name] database [detail prefix/mask [[detail longer-prefixes [detail]]]]	显示 RIP 路由数据库信息

命令	说明
show ip rip [vrf vrf-name] statistics	显示 RIP 协议统计信息
show ip rip interface [interface-name]	显示 RIP 接口信息
clear ip rip [vrf vrf-name] { process statistics }	清除 RIP 进程和统计信息

39.3 RIP 典型配置举例

39.3.1 配置 RIP 的版本

-S -E -A

网络需求

- Device1 和 Device2 间运行 RIPv2 进行路由交互。

网络拓扑

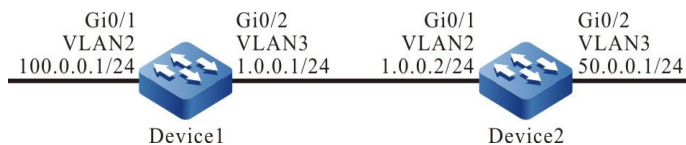


图 39-1 配置 RIP 版本组网图

配置步骤

步骤 1：配置 VLAN，并将端口加入对应的 VLAN。（略）

步骤 2：配置各接口的 IP 地址。（略）

步骤 3：配置 RIP。

#配置 Device1。

```
Device1#configure terminal
```

单播路由

```
Device1(config)#router rip
Device1(config-rip)#network 1.0.0.0
Device1(config-rip)#network 100.0.0.0
Device1(config-rip)#exit
```

#配置 Device2。

```
Device2#configure terminal
Device2(config)#router rip
Device2(config-rip)#network 1.0.0.0
Device2(config-rip)#network 50.0.0.0
Device2(config-rip)#exit
```

#查看 Device1 的路由表。

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C 1.0.0.0/24 is directly connected, 00:23:06, vlan3
R 50.0.0.0/8 [120/1] via 1.0.0.2, 00:13:26, vlan3
C 100.0.0.0/24 is directly connected, 00:23:06, vlan2
C 127.0.0.0/8 is directly connected, 76:51:00, lo0
```

#查看 Device2 的路由表。

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C 1.0.0.0/24 is directly connected, 00:23:06, vlan2
C 50.0.0.0/24 is directly connected, 00:23:06, vlan3
R 100.0.0.0/8 [120/1] via 1.0.0.1, 00:13:26, vlan2
C 127.0.0.0/8 is directly connected, 76:51:00, lo0
```

从路由表中可以看到设备通告的路由信息使用了 8 位自然掩码。

步骤 4： 配置 RIP 版本。

#配置 Device1。

```
Device1(config)#router rip
Device1(config-rip)#version 2
Device1(config-rip)#exit
```

#配置 Device2。

```
Device2(config)#router rip
Device2(config-rip)#version 2
Device2(config-rip)#exit
```

步骤 5： 检验结果。

单播路由

#查看 Device1 的路由表。

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C 1.0.0.0/24 is directly connected, 00:23:06, vlan3
R 50.0.0.0/24 [120/1] via 1.0.0.2, 00:13:26, vlan3
C 100.0.0.0/24 is directly connected, 00:23:06, vlan2
C 127.0.0.0/8 is directly connected, 76:51:00, lo0
```

#查看 Device2 的路由表。

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C 1.0.0.0/24 is directly connected, 00:23:06, vlan2
C 50.0.0.0/24 is directly connected, 00:23:06, vlan3
R 100.0.0.0/24 [120/1] via 1.0.0.1, 00:13:26, vlan2
C 127.0.0.0/8 is directly connected, 76:51:00, lo0
```

从路由表中可以看到设备通告的路由信息使用了 24 位精确掩码。

39.3.2 配置 RIP 路由重分发

-S -E -A

网络需求

- Device1 和 Device2 间运行 OSPF 协议，Device2 学习到 Device1 发布的 OSPF 路由 100.0.0.0/24，200.0.0.0/24。
- Device2 和 Device3 间运行 RIPv2 协议，Device2 仅将 OSPF 路由 100.0.0.0/24 重分发进 RIP，并把该路由通告给 Device3。

网络拓扑

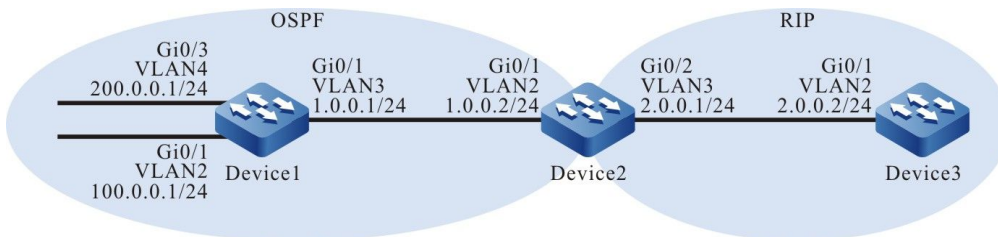


图 39-2 配置 RIP 路由重分发组网图

配置步骤

单播路由

步骤 1: 配置 VLAN, 并将端口加入对应的 VLAN。 (略)

步骤 2: 配置各接口的 IP 地址。 (略)

步骤 3: 配置 OSPF。

#配置 Device1。

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 1.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 100.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 200.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#配置 Device2。

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 1.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#查看 Device2 的路由表。

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C 1.0.0.0/24 is directly connected, 00:23:06, vlan2
C 2.0.0.0/24 is directly connected, 00:13:06, vlan3
O 100.0.0.0/24 [110/2] via 1.0.0.1, 00:04:12, vlan2
C 127.0.0.0/8 is directly connected, 76:51:00, lo0
O 200.0.0.0/24 [110/2] via 1.0.0.1, 00:04:12, vlan2
```

从路由表中可以看到 Device2 学习到了 Device1 通告的 OSPF 路由。

步骤 4: 配置 RIP。

#配置 Device2。

```
Device2(config)#router rip
Device2(config-rip)#version 2
Device2(config-rip)#network 2.0.0.0
Device2(config-rip)#exit
```

#配置 Device3。

```
Device3#configure terminal
Device3(config)#router rip
Device3(config-rip)#version 2
Device3(config-rip)#network 2.0.0.0
Device3(config-rip)#exit
```

单播路由

步骤 5: 配置路由策略。

#在 Device2 上配置 route-map 调用 ACL 匹配 100.0.0.0/24 并过滤 200.0.0.0/24。

```
Device2(config)#ip access-list standard 1
Device2(config-std-nacl)#permit 100.0.0.0 0.0.0.255
Device2(config-std-nacl)#exit
Device2(config)#route-map OSPFtoRIP
Device2(config-route-map)#match ip address 1
Device2(config-route-map)#exit
```

说明:

- 配置路由策略时, 前缀列表和 ACL 都可以创建过滤规则, 它们的区别在于前缀列表可以精确匹配路由掩码, 而 ACL 则不能匹配路由掩码。
-

步骤 6: 配置 RIP 重分发 OSPF 路由。

#配置 Device2。

```
Device2(config)#router rip
Device2(config-rip)#redistribute ospf 100 route-map OSPFtoRIP
Device2(config-rip)#exit
```

步骤 7: 检验结果。

#查看 Device2 的 RIP 路由表。

```
Device2#show ip rip database
Types: N - Network, L - Learn, R - Redistribute, D - Default config, S - Static config
Proto: C - connected, S - static, R - RIP, O - OSPF, E - IRMP,
       o - SNSP, B - BGP, i-ISIS

RIP routing database in VRF kernel (Counter 3):
T/P Network      ProID Metric Next-Hop   From      Time Tag  Interface
N/C 2.0.0.0/24   none 1    --      --      0    vlan3
R/O 100.0.0.0/24 1    1    1.0.0.1 --      0    vlan2
```

#查看 Device3 的路由表。

```
Device3#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set
```


单播路由

```
C 2.0.0.0/24 is directly connected, 00:23:06, vlan2
R 100.0.0.0/24 [120/1] via 2.0.0.1, 00:13:26, vlan2
C 127.0.0.0/8 is directly connected, 76:51:00, lo0
```

通过查看 Device2 的 RIP 路由表和 Device3 的路由表，发现在 Device2 上路由 100.0.0.0/24 被重分发至 RIP 并成功通告给 Device3，而路由 200.0.0.0/24 被成功过滤。

注意：

- 在实际应用中，如果自治系统边界路由器有 2 台及以上，建议不要直接在不同路由协议之间相互重分发路由，若必须配置时，需要在自治系统边界路由器上配置过滤、汇总等路由控制策略，防止产生路由环路。

39.3.3 配置 RIP 度量偏移

-S -E -A

网络需求

- Device1、Device2、Device3、Device4 间运行 RIPv2 协议进行互联。
- Device1 同时从 Device2 和 Device3 学习到路由 200.0.0.0/24。
- 要求在 Device1 上配置接收方向的路由度量偏移，使 Device1 优选 Device2 通告的路由。

网络拓扑

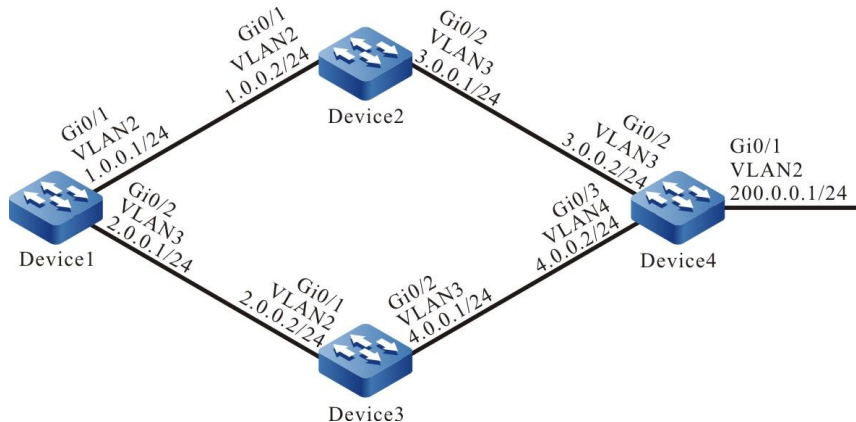


图 39-3 配置 RIP 度量偏移组网图

配置步骤

配置手册

发布 1.1 04/2020

单播路由

步骤 1: 配置 VLAN, 并将端口加入对应的 VLAN。 (略)

步骤 2: 配置各接口的 IP 地址。 (略)

步骤 3: 配置 RIP。

#配置 Device1。

```
Device1#configure terminal
Device1(config)#router rip
Device1(config-rip)#version 2
Device1(config-rip)#network 1.0.0.0
Device1(config-rip)#network 2.0.0.0
Device1(config-rip)#exit
```

#配置 Device2。

```
Device2#configure terminal
Device2(config)#router rip
Device2(config-rip)#version 2
Device2(config-rip)#network 1.0.0.0
Device2(config-rip)#network 3.0.0.0
Device2(config-rip)#exit
```

#配置 Device3。

```
Device3#configure terminal
Device3(config)#router rip
Device3(config-rip)#version 2
Device3(config-rip)#network 2.0.0.0
Device3(config-rip)#network 4.0.0.0
Device3(config-rip)#exit
```

#配置 Device4。

```
Device4#configure terminal
Device4(config)#router rip
Device4(config-rip)#version 2
Device4(config-rip)#network 3.0.0.0
Device4(config-rip)#network 4.0.0.0
Device4(config-rip)#network 200.0.0.0
Device4(config-rip)#exit
```

#查看 Device1 的路由表。

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C 1.0.0.0/24 is directly connected, 00:23:06, vlan2
C 2.0.0.0/24 is directly connected, 00:22:56, vlan3
R 3.0.0.0/24 [120/1] via 1.0.0.2, 00:13:26, vlan2
R 4.0.0.0/24 [120/1] via 2.0.0.2, 00:11:04, vlan3
C 127.0.0.0/8 is directly connected, 76:51:00, lo0
R 200.0.0.0/24 [120/2] via 1.0.0.2, 00:08:31, vlan2
   [120/2] via 2.0.0.2, 00:08:31, vlan3
```

单播路由

从 Device1 路由表中可以看到有两条到 200.0.0.0/24 的路由。

步骤 4: 配置访问列表。

#配置 Device1。

```
Device1(config)#ip access-list standard 1
Device1(config-std-nacl)#permit 200.0.0.0 0.0.0.255
Device1(config-std-nacl)#exit
```

步骤 5: 配置度量偏移。

#在 Device1 上配置偏移列表, 将从接口 VLAN3 学到且匹配 ACL 的路由度量值增加 3。

```
Device1(config)#router rip
Device1(config-rip)#offset-list 1 in 3 vlan3
Device1(config-rip)#exit
```

步骤 6: 检验结果。

#查看 Device1 的路由表。

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C 1.0.0.0/24 is directly connected, 00:33:59, vlan2
C 2.0.0.0/24 is directly connected, 00:33:50, vlan3
R 3.0.0.0/24 [120/1] via 1.0.0.2, 00:24:20, vlan2
R 4.0.0.0/24 [120/1] via 2.0.0.2, 00:21:57, vlan3
C 127.0.0.0/8 is directly connected, 77:01:54, lo0
R 200.0.0.0/24 [120/2] via 1.0.0.2, 00:19:25, vlan2
```

从 Device1 的路由表中看到路由 200.0.0.0/24 的下一跳出接口只有 VLAN2, 表明 Device1 优选了 Device2 通告的路由。

说明:

- 路由偏移列表可以使用在所有接口或指定接口上, 同时可以使用在设备的接收或通告方向。
-

39.3.4 配置 RIP 路由过滤 *-S -E -A*

网络需求

- Device1 和 Device2 间运行 RIPv2 进行路由交互。
- Device1 上学习到 Device2 通告的两条路由 2.0.0.0/24 和 3.0.0.0/24，之后在 Device2 的通告方向将路由 3.0.0.0/24 过滤。

网络拓扑

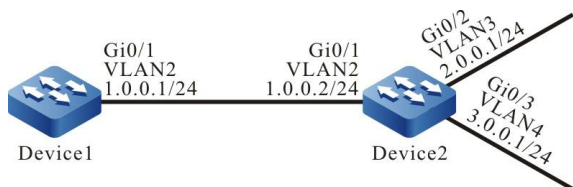


图 39-4 配置 RIP 路由过滤组网图

配置步骤

步骤 1：配置 VLAN，并将端口加入对应的 VLAN。（略）

步骤 2：配置各接口的 IP 地址。（略）

步骤 3：配置 RIP。

#配置 Device1。

```
Device1#configure terminal
Device1(config)#router rip
Device1(config-rip)#version 2
Device1(config-rip)#network 1.0.0.0
Device1(config-rip)#exit
```

#配置 Device2。

```
Device2#configure terminal
Device2(config)#router rip
Device2(config-rip)#version 2
Device2(config-rip)#network 1.0.0.0
Device2(config-rip)#network 2.0.0.0
Device2(config-rip)#network 3.0.0.0
Device2(config-rip)#exit
```

#查看 Device1 的路由表。

单播路由

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS
```

```
Gateway of last resort is not set
```

```
C 1.0.0.0/24 is directly connected, 00:23:06, vlan2
R 2.0.0.0/24 [120/1] via 1.0.0.2, 00:13:26, vlan2
R 3.0.0.0/24 [120/1] via 1.0.0.2, 00:13:26, vlan2
C 127.0.0.0/8 is directly connected, 76:51:00, lo0
```

可以看到 Device1 学习到 Device2 发布的两条路由。

步骤 4: 配置访问列表。

#配置 Device2。

```
Device2(config)#ip access-list standard 1
Device2(config-std-nacl)#permit 2.0.0.0 0.0.0.255
Device2(config-std-nacl)#exit
```

说明:

- 配置路由过滤时，前缀列表和 ACL 都可以创建过滤规则，它们的区别在于前缀列表可以精确匹配路由掩码，而 ACL 则不能匹配路由掩码。
-

步骤 5: 配置路由过滤。

#在 Device2 的接口 VLAN2 出方向配置路由过滤。

```
Device2(config)#router rip
Device2(config-rip)#distribute-list 1 out vlan2
Device2(config-rip)#exit
```

步骤 6: 检验结果。

#查看 Device1 的路由信息。

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS
```

```
Gateway of last resort is not set
```

```
C 1.0.0.0/24 is directly connected, 00:23:06, vlan2
R 2.0.0.0/24 [120/1] via 1.0.0.2, 00:13:26, vlan2
```

单播路由

C 127.0.0.0/8 is directly connected, 76:51:00, lo0

可以看到 Device2 不会给 Device1 通告路由 3.0.0.0/24，但需要等待路由超时后该路由才会从 Device1 的路由表中清除。

说明：

- **distribute-list** 可以使用在所有接口或指定接口上，同时可以使用在设备的接收或通告方向。

39.3.5 配置 RIP 路由汇总

-S -E -A

网络需求

- Device1、Device2、Device3、Device4 间运行 RIPv2 进行路由交互。
- Device1 从 Device2 学习到两条路由 100.1.0.0/24 和 100.2.0.0/24，为了减小 Device1 的路由表规模，需要 Device2 仅发布这两条路由的汇总路由给 Device1。

网络拓扑

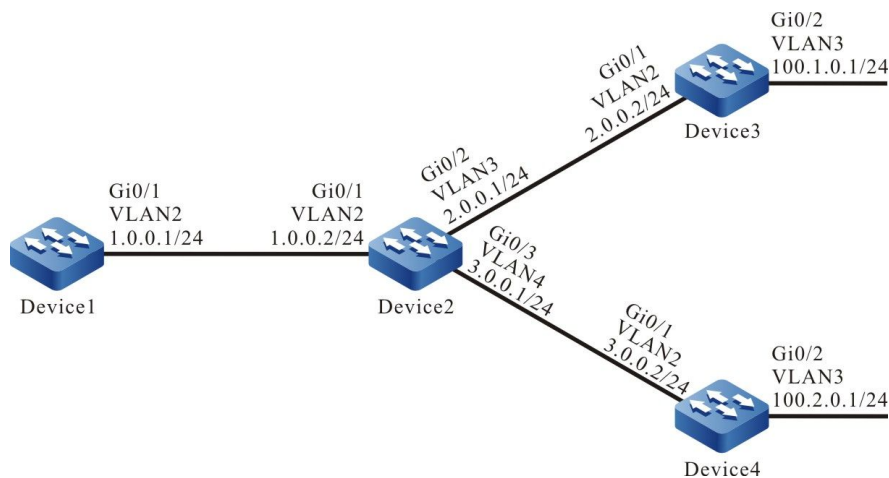


图 39-5 配置 RIP 路由汇总组网图

配置步骤

步骤 1：配置 VLAN，并将端口加入对应的 VLAN。（略）

单播路由

步骤 2: 配置各接口的 IP 地址。(略)

步骤 3: 配置 RIP。

#配置 Device1。

```
Device1#configure terminal
Device1(config)#router rip
Device1(config-rip)#version 2
Device1(config-rip)#network 1.0.0.0
Device1(config-rip)#exit
```

#配置 Device2。

```
Device2#configure terminal
Device2(config)#router rip
Device2(config-rip)#version 2
Device2(config-rip)#network 1.0.0.0
Device2(config-rip)#network 2.0.0.0
Device2(config-rip)#network 3.0.0.0
Device2(config-rip)#exit
```

#配置 Device3。

```
Device3#configure terminal
Device3(config)#router rip
Device3(config-rip)#version 2
Device3(config-rip)#network 2.0.0.0
Device3(config-rip)#network 100.0.0.0
Device3(config-rip)#exit
```

#配置 Device4。

```
Device4#configure terminal
Device4(config)#router rip
Device4(config-rip)#version 2
Device4(config-rip)#network 3.0.0.0
Device4(config-rip)#network 100.0.0.0
Device4(config-rip)#exit
```

#查看 Device1 的路由表。

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C 1.0.0.0/24 is directly connected, 00:23:06, vlan2
R 2.0.0.0/24 [120/1] via 1.0.0.2, 00:13:26, vlan2
R 3.0.0.0/24 [120/1] via 1.0.0.2, 00:13:26, vlan2
R 100.1.0.0/24 [120/2] via 1.0.0.2, 00:08:31, vlan2
R 100.2.0.0/24 [120/2] via 1.0.0.2, 00:08:31, vlan2
C 127.0.0.0/8 is directly connected, 76:51:00, lo0
```

步骤 4: 配置接口路由汇总。

单播路由

#在 Device2 上配置汇总路由 100.0.0.0/8。

```
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ip summary-address rip 100.0.0.0/8
Device2(config-if-vlan2)#exit
```

步骤 5: 检验结果。

#查看 Device1 的路由表。

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C 1.0.0.0/24 is directly connected, 00:24:06, vlan2
R 2.0.0.0/24 [120/1] via 1.0.0.2, 00:14:26, vlan2
R 3.0.0.0/24 [120/1] via 1.0.0.2, 00:14:26, vlan2
R 100.0.0.0/8 [120/2] via 1.0.0.2, 00:00:31, vlan2
C 127.0.0.0/8 is directly connected, 76:51:00, lo0
```

可以看到 Device1 学到 Device2 发布的汇总路由 100.0.0.0/8，但需要等待超时时两条明细路由才会从路由表中删除。

说明：

- RIP 支持全局自动汇总和接口手动汇总，RIPv2 的全局自动汇总缺省关闭。
-

39.3.6 配置 RIP 与 BFD 联动

-E -A

网络需求

- Device1、Device2、Device3 间运行 RIPv2 进行路由交互。
- Device1 从 Device2 和 Device3 均学习到 3.0.0.0/24 的路由，通过配置路由偏移使 Device1 优选 Device2 通告的路由，这时 Device1 到 Device2 间为该路由的主线路；Device1 到 Device3 间为该路由的备份线路。
- 在 Device1 与 Device2 间配置 BFD，当 Device1 与 Device2 间线路发生故障时，需要在 Device1 与 Device2 间配置 RIP 关联 BFD 以快速检测线路故障。当 BFD 检

测到主线路故障时会触发 RIP 进行路由更新，路由 3.0.0.0/24 切换到备份线路。

网络拓扑

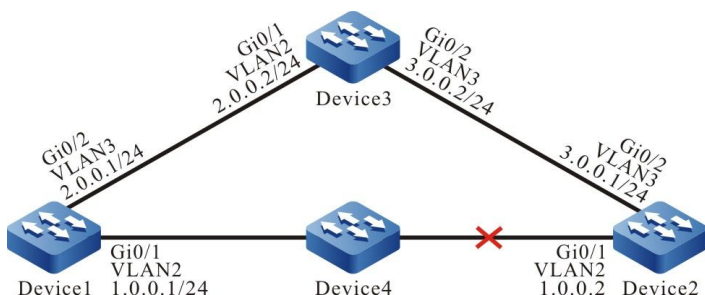


图 39-6 配置 RIP 与 BFD 联动组网图

配置步骤

步骤 1：配置 VLAN，并将端口加入对应的 VLAN。（略）

步骤 2：配置各接口的 IP 地址。（略）

步骤 3：配置 RIP。

#配置 Device1。

```
Device1#configure terminal
Device1(config)#router rip
Device1(config-rip)#version 2
Device1(config-rip)#network 1.0.0.0
Device1(config-rip)#network 2.0.0.0
Device1(config-rip)#exit
```

#配置 Device2。

```
Device2#configure terminal
Device2(config)#router rip
Device2(config-rip)#version 2
Device2(config-rip)#network 1.0.0.0
Device2(config-rip)#network 3.0.0.0
Device2(config-rip)#exit
```

#配置 Device3。

```
Device3#configure terminal
Device3(config)#router rip
Device3(config-rip)#version 2
Device3(config-rip)#network 2.0.0.0
Device3(config-rip)#network 3.0.0.0
Device3(config-rip)#exit
```

#查看 Device1 的路由表。

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
```

单播路由

D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

```
C 1.0.0.0/24 is directly connected, 01:30:23, vlan2
C 2.0.0.0/24 is directly connected, 01:30:14, vlan3
R 3.0.0.0/24 [120/1] via 1.0.0.2, 01:20:44, vlan2
   [120/1] via 2.0.0.2, 00:00:02, vlan3
C 127.0.0.0/8 is directly connected, 77:58:18, lo0
```

可以看到 Device1 同时从 Device2 和 Device3 学习到路由 3.0.0.0/24。

步骤 4： 配置路由偏移。

#在 Device1 的接口 VLAN3 的入方向配置路由偏移，使匹配 ACL 的路由度量值增大 3。

```
Device1(config)#ip access-list standard 1
Device1(config-std-nacl)#permit 3.0.0.0 0.0.0.255
Device1(config)#exit
Device1(config)#router rip
Device1(config-rip)#offset-list 1 in 3 vlan3
Device1(config-rip)#exit
```

#查看 Device1 的路由表。

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS
```

Gateway of last resort is not set

```
C 1.0.0.0/24 is directly connected, 01:30:23, vlan2
C 2.0.0.0/24 is directly connected, 01:30:14, vlan3
R 3.0.0.0/24 [120/1] via 1.0.0.2, 01:20:44, vlan2
C 127.0.0.0/8 is directly connected, 77:58:18, lo0
```

可以看到配置了路由偏移后 Device1 优选了 Device2 通告的路由 3.0.0.0/24。

步骤 5： 配置 BFD。

#配置 Device1。

```
Device1(config)#bfd fast-detect
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip rip bfd
Device1(config-if-vlan2)#exit
```

#配置 Device2。

```
Device2(config)#bfd fast-detect
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ip rip bfd
Device2(config-if-vlan2)#exit
```

步骤 6： 检验结果。

单播路由

#在 Device1 上查看 BFD 信息。

```
Device1#show bfd session
OurAddr      NeighAddr      LD/RD      State      Holddown      interface
1.0.0.1      1.0.0.2        2/4        UP         5000          vlan2
```

#当 Device1 与 Device2 间的线路出现故障后，路由能够快速切换到备份线路。

#在 Device1 上查看路由信息。

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C 2.0.0.0/24 is directly connected, 02:07:47, vlan3
R 3.0.0.0/24 [120/4] via 2.0.0.2, 00:01:14, vlan3
C 127.0.0.0/8 is directly connected, 78:35:51, lo0
```

39.3.7 配置 RIP 备份接口 *-S -E -A*

网络需求

- Device1、Device2、Device3 间运行 RIPv2 进行路由交互。
- Device1 同时从 Device2、Device3 学习到路由 3.0.0.0/24，在 Device1 上配置路由偏移使其优选 Device2 通告的路由，这时 Device1 到 Device2 间的线路为该路由的主线路；Device1 到 Device3 间的线路为该路由的备份线路。
- 在 Device1 配置 RIP 备份接口。在主线路正常的情况下，路由经过主线路，在主线路故障的情况下，路由能迅速切换至备份线路。

网络拓扑

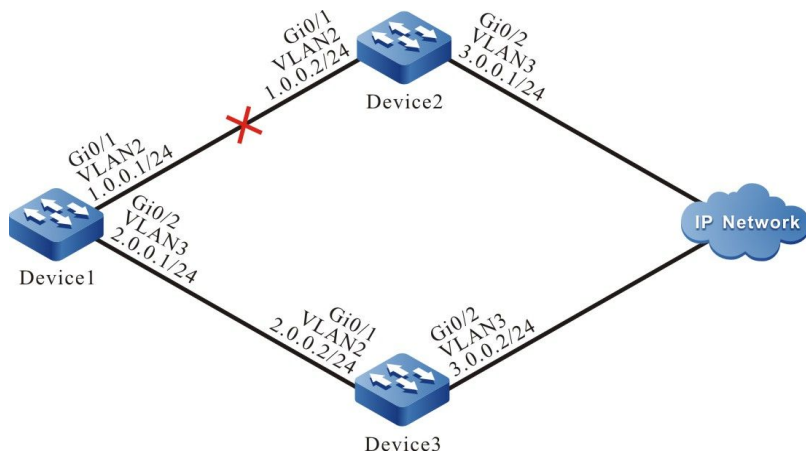


图 39-7 配置 RIP 备份接口组网图

配置步骤

步骤 1: 配置 VLAN, 并将端口加入对应的 VLAN。 (略)

步骤 2: 配置各接口的 IP 地址。 (略)

步骤 3: 配置 RIP。

#配置 Device1。

```
Device1#configure terminal
Device1(config)#router rip
Device1(config-rip)#version 2
Device1(config-rip)#network 1.0.0.0
Device1(config-rip)#network 2.0.0.0
Device1(config-rip)#exit
```

#配置 Device2。

```
Device2#configure terminal
Device2(config)#router rip
Device2(config-rip)#version 2
Device2(config-rip)#network 1.0.0.0
Device2(config-rip)#network 3.0.0.0
Device2(config-rip)#exit
```

#配置 Device3。

```
Device3#configure terminal
Device3(config)#router rip
Device3(config-rip)#version 2
Device3(config-rip)#network 2.0.0.0
Device3(config-rip)#network 3.0.0.0
Device3(config-rip)#exit
```

#查看 Device1 的路由表。

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C 1.0.0.0/24 is directly connected, 01:30:23, vlan2
C 2.0.0.0/24 is directly connected, 01:30:14, vlan3
R 3.0.0.0/24 [120/1] via 1.0.0.2, 01:20:44, vlan2
    [120/1] via 2.0.0.2, 00:00:02, vlan3
C 127.0.0.0/8 is directly connected, 77:58:18, lo0
```

可以看到 Device1 同时从 Device2 和 Device3 学习到路由 3.0.0.0/24。

步骤 4: 配置路由偏移。

#在 Device1 的接口 VLAN3 的入方向配置路由偏移, 使匹配 ACL 的路由度量值增大 3。

```
Device1(config)#ip access-list standard 1
```

单播路由

```
Device1(config-std-nacl)#permit 3.0.0.0 0.0.0.255
Device1(config)#exit
Device1(config)#router rip
Device1(config-rip)#offset-list 1 in 3 vlan3
Device1(config-rip)#exit
```

#查看 Device1 的路由表。

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C 1.0.0.0/24 is directly connected, 01:30:23, vlan2
C 2.0.0.0/24 is directly connected, 01:30:14, vlan3
R 3.0.0.0/24 [120/1] via 1.0.0.2, 01:20:44, vlan2
C 127.0.0.0/8 is directly connected, 77:58:18, lo0
```

可以看到配置了路由偏移后 Device1 优选了 Device2 通告的路由 3.0.0.0/24。

步骤 5： 配置备份接口。

#配置 Device1， 将接口 VLAN3 配置为 VLAN2 的 RIP 备份接口。

```
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip rip standby vlan3
Device1(config-if-vlan2)#exit
```

步骤 6： 检验结果。

#Device1 与 Device2 间的线路故障后， 路由能够快速切换到 Device1 与 Device3 间备份线路。

#在 Device1 上查看路由信息。

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C 2.0.0.0/24 is directly connected, 02:07:47, vlan3
R 3.0.0.0/24 [120/4] via 2.0.0.2, 00:01:14, vlan3
C 127.0.0.0/8 is directly connected, 78:35:51, lo0
```

39.3.8 配置 RIP 被动接口

-S -E -A

网络需求

- Device1 和 Device2 间运行 RIPv2 进行路由交互。
- 在 Device1 上配置被动接口， 不向 Device2 发送更新报文。

网络拓扑

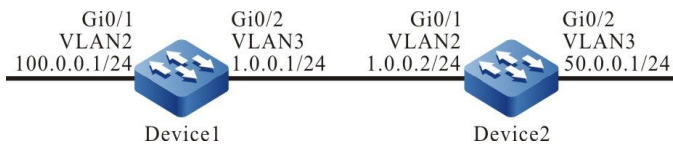


图 39-8 配置 RIP 被动接口组网图

配置步骤

步骤 1：配置 VLAN，并将端口加入对应的 VLAN。（略）

步骤 2：配置各接口的 IP 地址。（略）

步骤 3：配置 RIP。

#配置 Device1。

```
Device1#configure terminal
Device1(config)#router rip
Device1(config-rip)#version 2
Device1(config-rip)#network 1.0.0.0
Device1(config-rip)#network 100.0.0.0
Device1(config-rip)#exit
```

#配置 Device2。

```
Device2#configure terminal
Device2(config)#router rip
Device2(config-rip)#version 2
Device2(config-rip)#network 1.0.0.0
Device2(config-rip)#network 50.0.0.0
Device2(config-rip)#exit
```

#查看 Device1 的路由表。

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C 1.0.0.0/24 is directly connected, 00:23:06, vlan3
R 50.0.0.0/24 [120/1] via 1.0.0.2, 00:13:26, vlan3
C 100.0.0.0/24 is directly connected, 00:23:06, vlan2
C 127.0.0.0/8 is directly connected, 76:51:00, lo0
```

#查看 Device2 的路由表。

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C 1.0.0.0/24 is directly connected, 00:23:06, vlan2
```

单播路由

```
C 50.0.0/24 is directly connected, 00:23:06, vlan3
R 100.0.0.0/24 [120/1] via 1.0.0.1, 00:13:26, vlan2
C 127.0.0.0/8 is directly connected, 76:51:00, lo0
```

步骤 4: 配置被动接口。

#配置 Device1。

```
Device1(config)#router rip
Device1(config-rip)#passive-interface vlan3
Device1(config-rip)#exit
```

Device1 上配置 VLAN3 为被动接口，不向 Device2 发送更新报文，但仍然能接收更新报文。

步骤 5: 检验结果。

#查看 Device1 的路由表。

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C 1.0.0.0/24 is directly connected, 00:23:06, vlan3
R 50.0.0.0/24 [120/1] via 1.0.0.2, 00:13:26, vlan3
C 100.0.0.0/24 is directly connected, 00:23:06, vlan2
C 127.0.0.0/8 is directly connected, 76:51:00, lo0
```

Device1 上仍然会保存 50.0.0.0/24 的路由信息，而 Device2 上 RIP 路由超时删除后，路由表中会删除 100.0.0.0/24 的路由信息。

#查看 Device2 的路由表。

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C 1.0.0.0/24 is directly connected, 00:25:06, vlan2
C 50.0.0.0/24 is directly connected, 00:25:06, vlan3
C 127.0.0.0/8 is directly connected, 77:51:00, lo0
```

40 RIPng

40.1 RIPng 简介

RIPng 又称为下一代 RIP 协议 (RIP next generation)，它是一种用于 IPv6 网络为 IPv6 报文转发提供路由信息的动态路由协议。RIPng 在 RIP-2 上扩展而来，RIPng 协议的工作原理与 RIP 协议基本相同。为了适应 IPv6 网络，RIPng 对原有的 RIP 协议做了如下改动：

- UDP 端口号：RIPng 协议使用 UDP 的 521 端口号发送和接收协议报文；
- 组播地址：RIPng 协议使用 FF02::9 作为链路本地范围内的 RIPng 路由器组播地址，不支持广播；
- 前缀长度：RIPng 协议路由目的地址使用 128 比特的前缀长度；
- 下一跳地址：RIPng 协议使用 128 比特的 IPv6 地址；
- 源地址：RIPng 协议使用链路本地地址 FE80::/10 作为源地址发送 RIPng 协议报文。

RIPng 相关的协议规范有 RFC2080 和 RFC2081。

40.2 RIPng 功能配置

表 40-1 RIPng 功能配置列表

配置任务	
配置 RIPng 基本功能	全局使能 RIPng 协议
配置 RIPng 路由生成	配置 RIPng 发布缺省路由
	配置 RIPng 路由重分发

配置任务	
配置 RIPng 路由控制	配置 RIPng 管理距离
	配置 RIPng 路由汇总
	配置 RIPng 度量偏移
	配置 RIPng 路由过滤
	配置 RIPng 接口度量值
	配置 RIPng 接口路由标记
	配置 RIPng 最大负载均衡
配置 RIPng 网络优化	配置 RIPng 定时器
	配置 RIPng 水平分割与毒性逆转
	配置 RIPng 静态邻居
	配置 RIPng 被动接口

40.2.1 配置 RIPng 基本功能

-E -A

配置条件

在配置 RIPng 的基本功能之前，首先完成以下配置：

- 配置链路层协议，保证链路层通信正常；
- 配置使能接口的 IPv6 能力。

全局使能 RIPng 协议

使用 RIPng 协议，需要进行如下配置：

- 创建 RIPng 进程；

- 配置接口使能 RIPng 协议。

表 40-2 全局使能 RIPng 协议

步骤	命令	说明
进入全局配置模式	configure terminal	-
创建 RIPng 进程并进入 RIPng 配置模式	ipv6 router rip <i>process-id</i>	必选 缺省情况下, 未启用 RIPng 进程
退回全局配置模式	exit	-
进入接口配置模式	interface interface- <i>name</i>	-
接口使能 RIPng 协议	ipv6 rip enable <i>process-id</i>	必选 缺省情况下, 接口未使能 RIPng 协议

40.2.2 配置 RIPng 路由生成

-E -A

配置条件

在配置 RIPng 路由生成前, 首先完成以下任务:

- 配置使能接口的 IPv6 能力;
- 使能 RIPng 协议。

配置 RIPng 发布缺省路由

通过配置, 设备可以在所有 RIPng 接口下发送缺省路由, 将自己设置为其他相邻设备的缺省网关。

表 40-3 配置 RIPng 发布缺省路由

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 RIPng 配置模式	ipv6 router rip <i>process-id</i>	必选 缺省情况下, 未启用 RIPng 进程
配置 RIPng 发布缺省路由	default-information originate [metric <i>value</i>]	必选 缺省情况下, RIPng 不发 布缺省路由

说明:

- 如果学习到一条默认路由 (::/0), 则会替换本设备发布的默认路由 (::/0)。当网络存在环路时, 可能会造成路由振荡。故使用该命令时应避免相同路由域内多台设备同时启用该命令。

配置 RIPng 路由重分发

可以通过配置路由重分发将其他协议产生的路由引入到 RIPng 中。

表 40-4 配置 RIPng 路由重分发

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 RIPng 配置模式	ipv6 router rip <i>process-id</i>	必选 缺省情况下, 未启用 RIPng 进程

步骤	命令	说明
配置 RIPng 引入其它路由协议的缺省度量值	default-metric <i>metric-value</i>	可选 缺省情况下，引入其它协议的缺省度量值为 1
配置 RIPng 路由重分发	redistribute <i>protocol</i> [<i>protocol-id</i>] [metric <i>metric-value</i>] [route-map <i>route-map-name</i>] [match <i>route-sub-type</i>]	必选 缺省情况下，未配置路由重分发

说明：

- 重分发时指定 metric 命令选项后，相应重分发的路由将采用该度量值。
- RIPng 配置路由重分发应用路由图时，支持的 match 选项有 ipv6 address、route type、tag、interface、ipv6 nexthop、ipv6 route-source、metric，支持的 set 选项有 metric、tag。

40.2.3 配置 RIPng 路由控制

-E -A

配置条件

在配置 RIPng 路由控制前，首先完成以下任务：

- 配置接口使能 IPv6 能力；
- 使能 RIPng 协议。

配置 RIPng 管理距离

设备中可以同时运行多个路由协议，设备通过管理距离对各个协议学习到的路由进行优选，管理距离越小路由越优先。

表 40-5 配置 RIPng 管理距离

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 RIPng 配置模式	ipv6 router rip <i>process-id</i>	-
配置 RIPng 管理距离	distance <i>distance-value</i>	必选 缺省情况下, RIPng 管理距离为 120

配置 RIPng 路由汇总

RIPng 路由汇总是指配置一对目的地址和掩码的组合, 这对组合将对所覆盖网段内的路由进行汇总。

配置 RIPng 路由汇总后, 设备只通告汇总路由, 在大中型网络中可以显著减少相邻 RIPng 路由表规模, 同时减少路由协议报文对网络带宽的消耗。

汇总路由的 metric 将采用所有子网路由 metric 的最小值。

表 40-6 配置 RIPng 路由汇总功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置 RIPng 在接口上的路由汇总功能	ipv6 rip summary-address <i>prefix-address</i>	必选 缺省情况下未配置路由汇总功能

配置 RIPng 度量偏移

缺省情况下，RIPng 对接收到的路由采用相邻设备通告的路由度量值，在某些特殊应用场景中需要对度量值进行修改，可以通过配置 RIPng 的度量偏移对指定路由度量值进行校正。

配置入方向上的度量值后，将会在 RIPng 路由接收时进行路由度量值修改，再将路由存放于路由表中，当通告给相邻设备时将采用新的度量值；配置出方向上的度量值则只会在通告给相邻设备时修改。

表 40-7 配置 RIPng 度量偏移

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 RIPng 配置模式	ipv6 router rip <i>process-id</i>	必选 缺省情况下，未启用 RIPng 进程
配置 RIPng 对指定路由的度量进行修改	offset-list <i>access-list-name</i> { in out } <i>metric-offset</i> [<i>interface-name</i>]	必选 缺省情况下，没有配置任何接口的度量值

配置 RIPng 路由过滤

路由器可以通过配置访问控制列表、前缀列表、路由图对接收或通告路由进行过滤。在接收 RIPng 路由时，过滤某些学习到的路由，或者在通告 RIPng 路由时，过滤某些向相邻设备通告的路由。

表 40-8 配置 RIPng 路由过滤

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 RIPng 配置模式	ipv6 router rip <i>process-id</i>	必选 缺省情况下，未启用 RIPng 进程

步骤	命令	说明
配置 RIPng 路由过滤功能	distribute-list { <i>access-list-name</i> prefix <i>prefix-list-name</i> route-map <i>route-map-name</i> } { in out } [<i>interface-name</i>]	必选 缺省情况下，未配置路由过滤功能，配置路由过滤功能时，如果不指定接口，将针对所有 RIPng 接口启用路由过滤

配置 RIPng 接口度量值

接口在使能 RIPng 后，在数据库中会生成相应的直连路由，缺省度量值为 1，该路由在 RIPng 数据库中或者将其通告给相邻设备时，如果该接口上配置了度量值，将采用接口度量值。

当接口度量值改变后，RIPng 数据库中会立即更新 RIPng 相应直连路由，并通告到相邻设备。

表 40-9 配置 RIPng 接口度量值

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置 RIPng 接口度量	ipv6 rip metric <i>metric-value</i>	必选 缺省情况下，RIPng 接口度量值为 1

说明：

- 配置 RIPng 接口度量值只会影响接口上直连子网的度量，不会影响路由学习的度量。

配置 RIPng 接口路由标记

路由标记即路由 tag，是为了让网络管理员对一些路由打上标记，以便在应用路由策略时根据 tag 标记做路由过滤或路由属性通告。

表 40-10 配置 RIPng 接口路由标记

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置 RIPng 在接口上直连子网的路由 tag	ipv6 rip tag <i>tag-value</i>	必选 缺省情况下未配置路由标记

配置 RIPng 最大负载均衡条目数

通过配置该命令可以控制 RIPng 路由的负载条目数。

表 40-11 配置 RIPng 最大负载均衡条目数

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 RIPng 配置模式	ipv6 router rip <i>process-id</i>	必选 缺省情况下，未启用 RIPng 进程
配置 RIPng 最大负载均衡条目数	maximum-paths <i>max-number</i>	可选 缺省情况下，RIPng 最大负载均衡条目数为 4

配置条件

在配置 RIPng 网络优化前，首先完成以下任务：

- 配置接口使能 IPv6 能力；
- 使能 RIPng 协议。

配置 RIPng 定时器

由于 RIPng 不维护邻居关系、不支持路由撤消，所以协议提供了四个可配置的定时器来控制网络收敛速度，分别是：路由更新时间、路由超时时间、路由抑制更新时间、路由清除时间。

路由超时时间取值应至少为路由更新时间的 3 倍，在路由超时时间内未收到路由更新报文时，路由将会变为无效状态并进入抑制周期，抑制周期的长短取决于抑制更新时间，在该周期内，路由将不会被更新，抑制周期结束后进入清除周期，在该周期内可接受路由更新，如果没有接收到路由更新报文，该路由将会被删除。

表 40-12 配置 RIPng 定时器

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 RIPng 配置模式	ipv6 router rip <i>process-id</i>	必选 缺省情况下，未启用 RIPng 进程
配置 RIPng 的定时器时间	timers <i>update-interval</i> <i>invalid-interval</i> <i>holddown-interval</i> <i>flush-interval</i>	可选 缺省情况下，RIPng 更新 间隔时间 30 秒、通告有效 时间 180 秒、抑制时间 0 秒、清除时间 240 秒

说明：

- 在同一 RIPng 路由域中，所有设备上 **timer** 配置必须一致，防止出现网络震荡。

配置 RIPng 水平分割和毒性逆转

水平分割和毒性逆转均是防止路由环路的机制。

1. 配置水平分割

RIPng 从某个接口学习到的路由将不再向该接口通告，避免环路。

表 40-13 配置 RIPng 水平分割

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置 RIPng 水平分割	no ipv6 split-horizon [disable]	可选 缺省情况下，开启水平分割功能

2. 配置毒性逆转

RIPng 从某接口学习到的路由会向该接口通告，但路由度量值为最大跳数 16，以避免环路。

表 40-14 配置 RIPng 毒性逆转

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
进入接口配置模式	interface <i>interface-name</i>	-
配置 RIPng 毒性逆转	ipv6 split-horizon poison-reverse	必选 缺省情况下，未开启毒性 逆转功能

说明：

- 水平分割和毒性逆转只对学到的路由、RIPng 接口直连路由、重分发的直连和静态路由有效。
- 水平分割与毒性逆转不能同时使用。

配置 RIPng 静态邻居

RIPng 不维护邻接关系，故没有邻居的概念，这里描述配置的邻居指的是相邻 RIPng 路由设备。指定 RIPng 静态邻居后，RIPng 会向该邻居以单播形式发送 RIPng 报文。该配置应用于不支持广播或组播的网络，如点到点链路，在组播网络中应用该配置会导致网络中存在多个重复的 RIPng 报文。

表 40-15 配置 RIPng 静态邻居

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置通过单播形式通告路由信息的邻居	ipv6 rip neighbor <i>ipv6-address</i>	必选

步骤	命令	说明
		参数 ipv6-address 为对端直连接口 ipv6 地址

说明：

- 向静态邻居通告路由信息只会在 RIPng 接口上进行，并且 “**ipv6 rip passive**” 不能阻止向静态邻居发送报文。

配置 RIPng 被动接口

为减少路由协议消耗网络带宽，被动接口 (Passive Interface) 功能被动态路由协议采用。RIPng 在被动接口上只接收路由更新报文，不发送路由更新报文。在带宽较窄的低速网络中，被动接口配合 Neighbor 功能能有效减少 RIPng 的路由交互。

表 40-16 配置 RIPng 被动接口

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface interface-name	-
配置 RIPng 被动接口	ipv6 rip passive	必选 缺省情况下，未配置被动接口

说明：

- **ipv6 rip passive** 不会抑制向相邻设备发送单播路由更新，与 **neighbor** 命令配合使

用时，**ipv6 rip passive** 不会抑制向相邻设备发送单播路由更新。故该应用方式可以控制路由器只针对某些相邻设备以单播方式发送路由更新，而不对接口上的所有相邻设备进行组播方式路由更新。

40.2.5 配置 RIPng 与 BFD 联动

-E -A

备份接口只能应用于特定应用环境下，并且不能满足实时备份的需求，此时，RIPng 提供端到端保护的 BFD (Bidirectional Forwarding Detection, 双向转发检测) 功能，可以实现路由的快速收敛与切换。BFD 提供一种快速检测两台设备之间线路状态的方法。当相邻的两台 RIPng 设备间启动 BFD 检测后，若设备之间发生线路故障，BFD 会快速检测到故障并通知 RIPng 协议，RIP 将删除关联在 BFD 接口上的 RIPng 路由，如果这些路由存在备份路由，将会在极短时间（受 BFD 配置影响）内切换到备份路由。目前，RIPng 仅支持 BFD 单跳双向检测。

表 40-17 配置 RIPng 与 BFD 联动

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 RIPng 配置模式	ipv6 router rip 100	必选 缺省情况下，未启用 RIPng 进程
配置 RIPng 进程覆盖的所有接口都启用 BFD 功能	bfd all-interfaces	必选 缺省情况下，未启用所有 RIPng 覆盖接口 BFD 功能
回到全局配置模式	exit	-
进入接口配置模式	interface interface-name	-
配置接口上启用 BFD 功能	ipv6 rip bfd	必选

步骤	命令	说明
		缺省情况下, 未启用接口 BFD 功能

说明:

- BFD 相关配置, 请参见可靠性技术-BFD 技术手册。

40.2.6 RIPng 监控与维护

-E -A

表 40-18 配置 RIPng 监控与维护

命令	说明
clear ipv6 rip [<i>process-id</i>] { process statistics }	清除 RIPng 进程和统计信息
show ipv6 rip [<i>process-id</i>]	显示 RIPng 协议基本信息
show ipv6 rip [<i>process-id</i>] database [detail <i>ipv6-address/mask-length</i> [detail longer-prefixes]]	显示 RIPng 路由数据库信息
show ipv6 rip [<i>process-id</i>] statistics [<i>interface-name</i>]	显示 RIPng 接口统计信息
show ipv6 rip interface [<i>interface-name</i>]	显示 RIPng 接口信息

40.3 RIPng 典型配置举例

40.3.1 配置 RIPng 基本功能

-E -A

网络需求

- Device1 和 Device2 间运行 RIPng 进行路由交互。

网络拓扑

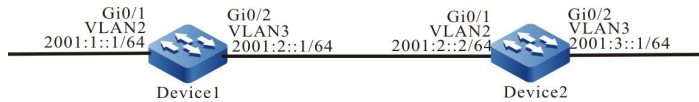


图 40-1 配置 RIPng 基本功能组网图

配置步骤

步骤 1： 配置 VLAN,并将端口加入对应的 VLAN。（略）

步骤 2： 配置各接口的 IPv6 地址。（略）

步骤 3： 配置 RIPng。

#配置 Device1。

```
Device1#configure terminal
Device1(config)#ipv6 router rip 100
Device1(config-ripng)#exit
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#ipv6 rip enable 100
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan 3
Device1(config-if-vlan3)#ipv6 rip enable 100
Device1(config-if-vlan3)#exit
```

#配置 Device2。

```
Device2#configure terminal
Device2(config)#ipv6 router rip 100
Device2(config-ripng)#exit
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#ipv6 rip enable 100
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan 3
Device2(config-if-vlan3)#ipv6 rip enable 100
Device2(config-if-vlan3)#exit
```

步骤 4： 检验结果。

#查看 Device1 的 IPv6 路由表。

```
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 2w4d:19:31:05, lo0
C 2001:1::/64 [0/0]
  via ::, 00:21:42, vlan2
L 2001:1::1/128 [0/0]
  via ::, 00:21:40, lo0
C 2001:2::/64 [0/0]
  via ::, 00:21:34, vlan3
L 2001:2::1/128 [0/0]
  via ::, 00:21:33, lo0
R 2001:3::/64 [120/2]
  via fe80::201:7aff:fec3:38a4, 00:11:19, vlan3
```

#查看 Device2 的 IPv6 路由表。

```
Device2#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 3d:22:39:31, lo0
R 2001:1::/64 [120/2]
  via fe80::201:7aff:fe01:204, 00:12:00, vlan2
C 2001:2::/64 [0/0]
  via ::, 00:30:46, vlan2
L 2001:2::2/128 [0/0]
  via ::, 00:30:45, lo0
C 2001:3::/64 [0/0]
  via ::, 00:29:12, vlan3
L 2001:3::1/128 [0/0]
  via ::, 00:29:11, lo0
```

从路由表中可以看到设备通告的路由信息使用了 64 位精确掩码。

40.3.2 配置 RIPng 路由重分发 **-E -A**

网络需求

- Device1 和 Device2 间运行 IPv6 OSPF 协议，Device2 学习到 Device1 发布的 IPv6 OSPF 路由 2001:1::/64，2001:2::/64。
- Device2 和 Device3 间运行 RIPng 协议，Device2 仅将 IPv6 OSPF 路由 2001:1::/64 重分发进 RIPng，并把该路由通告给 Device3。

网络拓扑

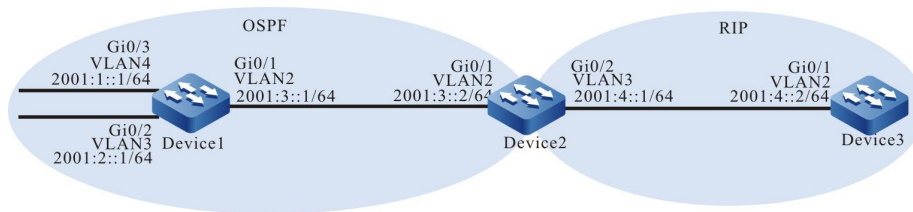


图 40-2 配置 RIPng 路由重分发组网图

配置步骤

步骤 1： 配置 VLAN,并将端口加入对应的 VLAN。（略）

步骤 2： 配置各接口的 IPv6 地址。（略）

步骤 3： 配置 IPv6 OSPF。

#配置 Device1。

```
Device1#configure terminal
Device1(config)#ipv6 router ospf 100
Device1(config-ospf6)# router-id 1.1.1.1
Device1(config-ospf6)#exit
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#ipv6 router ospf tag 100 area 0
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan 3
Device1(config-if-vlan3)#ipv6 router ospf tag 100 area 0
Device1(config-if-vlan3)#exit
Device1(config)#interface vlan 4
Device1(config-if-vlan4)#ipv6 router ospf tag 100 area 0
Device1(config-if-vlan4)#exit
```

#配置 Device2。

```
Device2#configure terminal
Device2(config)#ipv6 router ospf 100
Device2(config-ospf6)#router-id 2.2.2.2
Device2(config-ospf6)#exit
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#ipv6 router ospf tag 100 area 0
Device2(config-if-vlan2)#exit
```

#查看 Device2 的 IPv6 路由表。

```
Device2#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 4d:00:09:49, lo0
O 2001:1::/64 [110/2]
  via fe80::201:7aff:fe01:204, 00:12:16, vlan2
O 2001:2::/64 [110/2]
  via fe80::201:7aff:fe01:204, 00:12:16, vlan2
C 2001:3::/64 [0/0]
```

单播路由

```
via ::, 00:19:51, vlan2
L 2001:3::2/128 [0/0]
via ::, 00:19:50, lo0
C 2001:4::/64 [0/0]
via ::, 00:45:13, vlan3
L 2001:4::1/128 [0/0]
via ::, 00:45:12, lo0
```

从路由表中可以看到 Device2 学习到了 Device1 通告的 IPv6 OSPF 路由。

步骤 4: 配置 RIPng。

#配置 Device2。

```
Device2(config)#ipv6 router rip 100
Device2(config-ripng)#exit
Device2(config)#interface vlan 3
Device2(config-if-vlan3)#ipv6 rip enable 100
Device2(config-if-vlan3)#exit
```

#配置 Device3。

```
Device3#configure terminal
Device3(config)#ipv6 router rip 100
Device3(config-ripng)#exit
Device3(config)#interface vlan 2
Device3(config-if-vlan2)#ipv6 rip enable 100
Device3(config-if-vlan2)#exit
```

步骤 5: 配置路由策略。

#在 Device2 上配置 route-map 调用前缀列表匹配 2001:1::/64 并过滤 2001:2::/64。

```
Device2(config)#ipv6 prefix-list OSPF permit 2001:1::/64
Device2(config)#route-map OSPFtoRIP
Device2(config-route-map)#match ipv6 address prefix-list OSPF
Device2(config-route-map)#exit
```

说明:

- 配置路由策略时，前缀列表和 ACL 都可以创建过滤规则，它们的区别在于前缀列表可以精确匹配路由掩码，而 ACL 则不能匹配路由掩码。
-

步骤 6: 配置 RIPng 重分发 IPv6 OSPF 路由。

#配置 RIPng 重分发 IPv6 OSPF 路由。

```
Device2(config)#ipv6 router rip 100
Device2(config-ripng)#redistribute ospf 100 route-map OSPFtoRIP
Device2(config-ripng)#exit
```

步骤 7: 检验结果。

#查看 Device2 的 RIPng 数据库。

```
Device2#show ipv6 rip database
Type : N - Network interface, L - Learn, R - Redistribute, D - Default config,
      S - Static config
Proto: C - connected, S - static, R - RIP, O - OSPF, E - IRMP,
      o - SNSP, B - BGP, i-ISIS

RIPng process 100 routing database (VRF Kernel, Counter 2):
[Type/Proto]
[R/O] 2001:1::/64 metric 1
      via vlan2, fe80::201:7aff:fe01:204, no expires
[N/C] 2001:4::/64 metric 1, installed
      via vlan3, ::, no expires
```

#查看 Device3 的 IPv6 路由表。

```
Device3#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 2w0d:20:00:11, lo0
R 2001:1::/64 [120/2]
  via fe80::201:7aff:fec3:38a5, 02:50:14, vlan2
C 2001:4::/64 [0/0]
  via ::, 03:56:24, vlan2
L 2001:4::2/128 [0/0]
  via ::, 03:56:23, lo0
```

通过查看 Device2 的数据库和 Device3 的路由表，发现在 Device2 上路由 2001:1::/64 被重分发至 RIPng 并成功通告给 Device3，而路由 2001:2::/64 被成功过滤。

说明：

- 在实际应用中，如果自治系统边界路由器有 2 台及以上，建议不要直接在不同路由协议之间相互重分发路由，若必须配置时，需要在自治系统边界路由器上配置过滤、汇总等路由控制策略，防止产生路由环路。
-

40.3.3 配置 RIPng 度量偏移

-E -A

网络需求

- Device1、Device2、Device3、Device4 间运行 RIPng 协议进行互联。
- Device1 同时从 Device2 和 Device3 学习到路由 2001:5::/64。
- 要求在 Device1 上配置接收方向的路由度量偏移，使 Device1 优选 Device2 通告

的路由。

网络拓扑

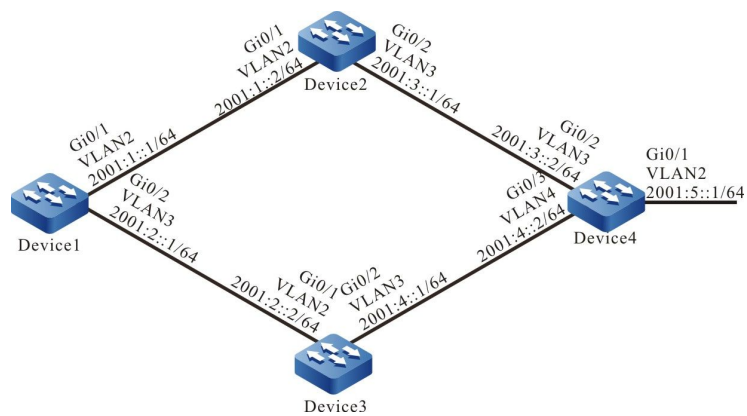


图 40-3 配置 RIPng 度量偏移组网图

配置步骤

步骤 1: 配置 VLAN，并将端口加入对应的 VLAN。（略）

步骤 2: 配置各接口的 IPv6 地址。（略）

步骤 3: 配置 RIPng。

#配置 Device1。

```
Device1#configure terminal
Device1(config)#ipv6 router rip 100
Device1(config-ripng)#exit
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#ipv6 rip enable 100
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan 3
Device1(config-if-vlan3)#ipv6 rip enable 100
Device1(config-if-vlan3)#exit
```

#配置 Device2。

```
Device2#configure terminal
Device2(config)#ipv6 router rip 100
Device2(config-ripng)#exit
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#ipv6 rip enable 100
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan 3
Device2(config-if-vlan3)#ipv6 rip enable 100
Device2(config-if-vlan3)#exit
```

#配置 Device3。

```
Device3#configure terminal
```

单播路由

```
Device3(config)#ipv6 router rip 100
Device3(config-ripng)#exit
Device3(config)#interface vlan 2
Device3(config-if-vlan2)#ipv6 rip enable 100
Device3(config-if-vlan2)#exit
Device3(config)#interface vlan 3
Device3(config-if-vlan3)#ipv6 rip enable 100
Device3(config-if-vlan3)#exit
```

#配置 Device4。

```
Device4#configure terminal
Device4(config)#ipv6 router rip 100
Device4(config-ripng)#exit
Device4(config)#interface vlan 2
Device4(config-if-vlan2)#ipv6 rip enable 100
Device4(config-if-vlan2)#exit
Device4(config)#interface vlan 3
Device4(config-if-vlan3)#ipv6 rip enable 100
Device4(config-if-vlan3)#exit
Device4(config)#interface vlan 4
Device4(config-if-vlan4)#ipv6 rip enable 100
Device4(config-if-vlan4)#exit
```

#查看 Device1 的 IPv6 路由表。

```
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
   via ::, 2w5d:06:21:24, lo0
C 2001:1::/64 [0/0]
   via ::, 00:02:05, vlan2
L 2001:1::1/128 [0/0]
   via ::, 00:02:04, lo0
C 2001:2::/64 [0/0]
   via ::, 00:02:02, vlan3
L 2001:2::1/128 [0/0]
   via ::, 00:02:01, lo0
R 2001:3::/64 [120/2]
   via fe80::201:7aff:fec3:38a4, 00:02:03, vlan2
R 2001:4::/64 [120/2]
   via fe80::201:7aff:fe11:2214, 00:00:48, vlan3
R 2001:5::/64 [120/3]
   via fe80::201:7aff:fec3:38a4, 00:02:03, vlan2
   [120/3]
   via fe80::201:7aff:fe11:2214, 00:00:48, vlan3
```

从 Device1 路由表中可以看到有两条到 2001:5::/64 的路由。

步骤 4: 配置访问列表。

```
Device1(config)#ipv6 access-list extended RIPng
Device1(config-v6-list)#permit 10 2001:5::/64 any
Device1(config-v6-list)#exit
```

步骤 5: 配置度量偏移。

#在 Device1 上配置偏移列表, 将从接口 vlan3 学到且匹配 ACL 的路由度量值增加 3。

```
Device1(config)# ipv6 router rip 100
```

单播路由

```
Device1(config-ripng)#offset-list RIPng in 3 vlan 3
Device1(config-ripng)#exit
```

步骤 6: 检验结果。

#查看 Device1 的 IPv6 路由表。

```
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 2w5d:06:34:28, lo0
C 2001:1::/64 [0/0]
  via ::, 00:15:09, vlan2
L 2001:1::1/128 [0/0]
  via ::, 00:15:08, lo0
C 2001:2::/64 [0/0]
  via ::, 00:15:06, vlan3
L 2001:2::1/128 [0/0]
  via ::, 00:15:05, lo0
R 2001:3::/64 [120/2]
  via fe80::201:7aff:fec3:38a4, 00:03:10, vlan2
R 2001:4::/64 [120/2]
  via fe80::201:7aff:fe11:2214, 00:03:10, vlan3
R 2001:5::/64 [120/3]
  via fe80::201:7aff:fec3:38a4, 00:03:10, vlan2
```

从 Device1 的路由表中看到路由 2001:5::/64 的下一跳出接口只有 vlan2，表明 Device1 优选了 Device2 通告的路由。

说明：

- 路由偏移列表可以使用在所有接口或指定接口上，同时可以使用在设备的接收或通告方向。
-

40.3.4 配置 RIPng 路由过滤

-E -A

网络需求

- Device1 和 Device2 间运行 RIPng 进行路由交互。
- Device1 上学习到 Device2 通告的两条路由 2001:2::/64 和 2001:3::/64，之后在 Device2 的通告方向将路由 2001:3::/64 过滤。

网络拓扑

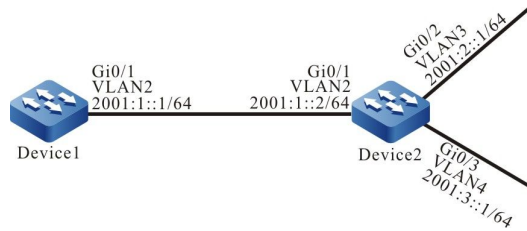


图 40-4 配置 RIPng 路由过滤组网图

配置步骤

- 步骤 1： 配置 VLAN，并将端口加入对应的 VLAN。（略）
- 步骤 2： 配置各接口的 IPv6 地址。（略）
- 步骤 3： 配置 RIPng。

#配置 Device1。

```
Device1#configure terminal
Device1(config)#ipv6 router rip 100
Device1(config-ripng)#exit
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#ipv6 rip enable 100
Device1(config-if-vlan2)#exit
```

#配置 Device2。

```
Device2#configure terminal
Device2(config)#ipv6 router rip 100
Device2(config-ripng)#exit
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#ipv6 rip enable 100
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan 3
Device2(config-if-vlan3)#ipv6 rip enable 100
Device2(config-if-vlan3)#exit
Device2(config)#interface vlan 4
Device2(config-if-vlan4)#ipv6 rip enable 100
Device2(config-if-vlan4)#exit
```

#查看 Device1 的 IPv6 路由表。

```
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 2w5d:02:47:44, lo0
C 2001:1::/64 [0/0]
  via ::, 00:56:34, vlan2
L 2001:1::1/128 [0/0]
  via ::, 00:56:32, lo0
R 2001:2::/64 [120/2]
  via fe80::201:7aff:fec3:38a4, 00:27:11, vlan2
R 2001:3::/64 [120/2]
```

单播路由

```
via fe80::201:7aff:fec3:38a4, 00:27:11, vlan2
```

可以看到 Device1 学习到 Device2 发布的两条路由。

步骤 4: 配置 IPv6 前缀列表。

```
Device2(config)#ipv6 prefix-list RIPng deny 2001:3::/64
```

步骤 5: 配置路由过滤。

#在 Device2 的接口 VLAN2 出方向配置路由过滤。

```
Device2(config)#ipv6 router rip 100
Device2(config-ripng)#distribute-list prefix RIPng out vlan 2
Device2(config-ripng)#exit
```

步骤 6: 检验结果。

#查看 Device1 的 IPv6 路由表。

```
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 2w5d:03:03:49, lo0
C 2001:1::/64 [0/0]
  via ::, 01:12:39, vlan2
L 2001:1::1/128 [0/0]
  via ::, 01:12:38, lo0
R 2001:2::/64 [120/2]
  via fe80::201:7aff:fec3:38a4, 00:43:16, vlan2
```

可以看到 Device2 不会给 Device1 通告路由 2001:3::/64，但需要等待路由超时后该路由才会从 Device1 的路由表中清除。

说明:

- distribute-list 可以使用在所有接口或指定接口上，同时可以使用在设备的接收或通告方向。
-

40.3.5 配置 RIPng 路由汇总

-E -A

网络需求

- Device1、Device2、Device3、Device4 间运行 RIPng 进行路由交互。
- Device1 从 Device2 学习到两条路由 2001:4:1:1::/64 和 2001:4:1:2::/64，为了减

小 Device1 的路由表规模，需要 Device2 仅发布这两条路由的汇总路由给 Device1。

网络拓扑

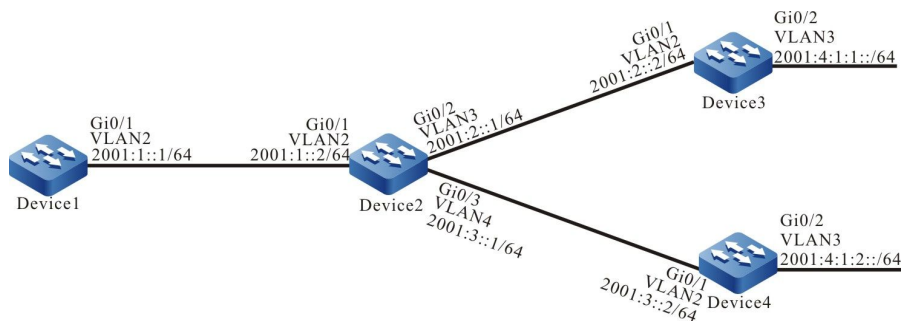


图 40-5 配置 RIPng 路由汇总组网图

配置步骤

步骤 1：配置 VLAN，并将端口加入对应的 VLAN。（略）

步骤 2：配置各接口的 IPv6 地址。（略）

步骤 3：配置 RIPng。

#配置 Device1。

```
Device1#configure terminal
Device1(config)#ipv6 router rip 100
Device1(config-ripng)#exit
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#ipv6 rip enable 100
Device1(config-if-vlan2)#exit
```

#配置 Device2。

```
Device2#configure terminal
Device2(config)#ipv6 router rip 100
Device2(config-ripng)#exit
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#ipv6 rip enable 100
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan 3
Device2(config-if-vlan3)#ipv6 rip enable 100
Device2(config-if-vlan3)#exit
Device2(config)#interface vlan 4
Device2(config-if-vlan4)#ipv6 rip enable 100
Device2(config-if-vlan4)#exit
```

#配置 Device3。

```
Device3#configure terminal
Device3(config)#ipv6 router rip 100
Device3(config-ripng)#exit
Device3(config)#interface vlan 2
Device3(config-if-vlan2)#ipv6 rip enable 100
```

单播路由

```
Device3(config-if-vlan2)#exit
Device3(config)#interface vlan 3
Device3(config-if-vlan3)#ipv6 rip enable 100
Device3(config-if-vlan3)#exit
```

#配置 Device4。

```
Device4#configure terminal
Device4(config)#ipv6 router rip 100
Device4(config-ripng)#exit
Device4(config)#interface vlan 2
Device4(config-if-vlan2)#ipv6 rip enable 100
Device4(config-if-vlan2)#exit
Device4(config)#interface vlan 3
Device4(config-if-vlan3)#ipv6 rip enable 100
Device4(config-if-vlan3)#exit
```

#查看 Device1 的 IPv6 路由表。

```
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 2w5d:02:27:40, lo0
C 2001:1::/64 [0/0]
  via ::, 00:36:29, vlan2
L 2001:1::1/128 [0/0]
  via ::, 00:36:28, lo0
R 2001:2::/64 [120/2]
  via fe80::201:7aff:fec3:38a4, 00:07:06, vlan2
R 2001:3::/64 [120/2]
  via fe80::201:7aff:fec3:38a4, 00:07:06, vlan2
R 2001:4:1:1::/64 [120/3]
  via fe80::201:7aff:fec3:38a4, 00:07:06, vlan2
R 2001:4:1:2::/64 [120/3]
  via fe80::201:7aff:fec3:38a4, 00:06:55, vlan2
```

步骤 4： 配置接口路由汇总。

#在 Device2 上配置汇总路由 2001:4:1::/48。

```
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#ipv6 rip summary-address 2001:4:1::/48
Device2(config-if-vlan2)#exit
```

步骤 5： 检验结果。

#查看 Device1 的 IPv6 路由表。

```
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 2w5d:02:35:44, lo0
C 2001:1::/64 [0/0]
  via ::, 00:44:33, vlan2
L 2001:1::1/128 [0/0]
  via ::, 00:44:32, lo0
R 2001:2::/64 [120/2]
```

```
via fe80::201:7aff:fec3:38a4, 00:15:10, vlan2
R 2001:3::/64 [120/2]
via fe80::201:7aff:fec3:38a4, 00:15:10, vlan2
R 2001:4:1::/48 [120/3]
via fe80::201:7aff:fec3:38a4, 00:05:19, vlan2
```

可以看到 Device1 学到 Device2 发布的汇总路由 2001:4:1::/48，但需要等待超时后两条明细路由才会从路由表中删除。

40.3.6 配置 RIPng 被动接口

-E -A

网络需求

- Device1 和 Device2 间运行 RIPng 进行路由交互。
- 在 Device1 上配置被动接口，不向 Device2 发送更新报文。

网络拓扑

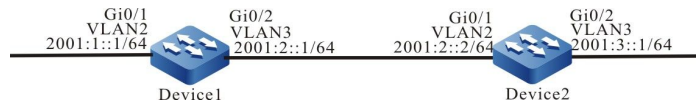


图 40-6 配置 RIPng 被动接口组网图

配置步骤

步骤 1：配置 VLAN，并将端口加入对应的 VLAN。（略）

步骤 2：配置各接口的 IPv6 地址。（略）

步骤 3：配置 RIPng。

#配置 Device1。

```
Device1#configure terminal
Device1(config)#ipv6 router rip 100
Device1(config-ripng)#exit
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#ipv6 rip enable 100
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan 3
Device1(config-if-vlan3)#ipv6 rip enable 100
Device1(config-if-vlan3)#exit
```

#配置 Device2。

```
Device2#configure terminal
Device2(config)#ipv6 router rip 100
Device2(config-ripng)#exit
Device2(config)#interface vlan 2
```

单播路由

```
Device2(config-if-vlan2)#ipv6 rip enable 100
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan 3
Device2(config-if-vlan3)#ipv6 rip enable 100
Device2(config-if-vlan3)#exit
```

#查看 Device1 的 IPv6 路由表。

```
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 2w4d:19:31:05, lo0
C 2001:1::/64 [0/0]
  via ::, 00:21:42, vlan2
L 2001:1::1/128 [0/0]
  via ::, 00:21:40, lo0
C 2001:2::/64 [0/0]
  via ::, 00:21:34, vlan3
L 2001:2::1/128 [0/0]
  via ::, 00:21:33, lo0
R 2001:3::/64 [120/2]
  via fe80::201:7aff:fec3:38a4, 00:11:19, vlan3
```

#查看 Device2 的 IPv6 路由表。

```
Device2#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 3d:22:39:31, lo0
R 2001:1::/64 [120/2]
  via fe80::201:7aff:fe01:204, 00:12:00, vlan2
C 2001:2::/64 [0/0]
  via ::, 00:30:46, vlan2
L 2001:2::2/128 [0/0]
  via ::, 00:30:45, lo0
C 2001:3::/64 [0/0]
  via ::, 00:29:12, vlan3
L 2001:3::1/128 [0/0]
  via ::, 00:29:11, lo0
```

步骤 4: 配置被动接口。

#配置 Device1。

```
Device1(config)#interface vlan 3
Device1(config-if-vlan3)#ipv6 rip passive
Device1(config-if-vlan3)#exit
```

Device1 上配置 vlan 3 为被动接口，不向 Device2 发送更新报文，但仍然能接收更新报文。

步骤 5: 检验结果。

#查看 Device1 的 IPv6 路由表。

```
Device1#show ipv6 route
```

单播路由

```
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 2w4d:19:55:37, lo0
C 2001:1::/64 [0/0]
  via ::, 00:46:14, vlan2
L 2001:1::1/128 [0/0]
  via ::, 00:46:12, lo0
C 2001:2::/64 [0/0]
  via ::, 00:46:06, vlan3
L 2001:2::1/128 [0/0]
  via ::, 00:46:05, lo0
R 2001:3::/64 [120/2]
  via fe80::201:7aff:fec3:38a4, 00:35:51, vlan3
```

Device1 上仍然会保存 2001:3::/64 的路由信息，而 Device2 上 RIPng 路由超时删除后，路由表中会删除 2001:1::/64 的路由信息。

#查看 Device2 的 IPv6 路由表。

```
Device2#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 3d:23:05:24, lo0
C 2001:2::/64 [0/0]
  via ::, 00:56:39, vlan2
L 2001:2::2/128 [0/0]
  via ::, 00:56:38, lo0
C 2001:3::/64 [0/0]
  via ::, 00:55:05, vlan3
L 2001:3::1/128 [0/0]
  via ::, 00:55:04, lo0
```

41 OSPF

41.1 OSPF 简介

OSPF 协议（Open Shortest Path First，开放最短路径优先）是一种基于链路状态的动态路由协议，使用 Dijkstra 的最短路径优先算法 SPF 在单一的自治系统（Autonomous System，简称 AS）内计算路由。

OSPF 协议由 IETF 开发，主要用于解决距离矢量路由存在的收敛慢、易形成环路的问题，适用于大中型网络。目前实现的 OSPF 版本 2，遵循 RFC2328，并且支持其它相关 RFC 定义的 OSPF 扩展功能。

在 OSPF 协议中，每台设备都维持一个描述 AS 网络的链路状态数据库，同一区域内设备的数据库相同，数据库完全同步之后，每台设备以自己为根，使用 SPF 算法计算出一个无环路的最短路径树，来描述它所知道的到达每一个目的地的最短路径，最后每台设备再从 SPF 树中构建出自己的路由表。

OSPF 主要特性有：

- 快速收敛：在网络的拓扑结构发生变化后立即发送更新报文，并使这一变化在自治系统中同步；
- 无自环：OSPF 根据链路状态数据库运行 SPF 计算路由，从算法本身保证了不会形成路由环路；
- 划分区域：OSPF 允许自治系统划分为多个区域，从而减少了网络带宽的占用，并使得构建层次化的网络成为可能；
- 支持认证：OSPF 设备每接收一个路由协议包，都会验证该包中的认证信息，以防止信息外泄或网络中的恶意攻击；
- 支持不同长度的子网：OSPF 通告的路由中携带网络掩码，以支持不同长度的子网；
- 支持负载均衡：支持到同一目的地址的多条等价路由。

41.2 OSPF 功能配置

表 41-1 OSPF 功能配置列表

配置任务	
配置 OSPF 基本功能	使能 OSPF 协议

配置任务	
配置 OSPF 区域	配置 OSPF NSSA 区域
	配置 OSPF Stub 区域
	配置 OSPF 虚链接
配置 OSPF 网络类型	配置 OSPF 接口网络类型为广播
	配置 OSPF 接口网络类型为 P2P
	配置 OSPF 接口网络类型为 NBMA
	配置 OSPF 接口网络类型为 P2MP
配置 OSPF 网络认证	配置 OSPF 区域认证
	配置 OSPF 接口认证
配置 OSPF 路由生成	配置 OSPF 路由重分发
	配置 OSPF 默认路由
	配置 OSPF 主机路由
配置 OSPF 路由控制	配置 OSPF 区域间路由汇总
	配置 OSPF 外部路由汇总
	配置 OSPF 区域间路由过滤
	配置 OSPF 外部路由过滤
	配置 OSPF 路由安装过滤

配置任务	
	配置 OSPF 接口 cost 值
	配置 OSPF 参考带宽
	配置 OSPF 管理距离
	配置 OSPF 最大负载均衡条目数
	配置 OSPF 兼容 RFC1583
配置 OSPF 网络优化	配置 OSPF 邻居保活时间
	配置 OSPF 被动接口
	配置 OSPF 需求电路
	配置 OSPF 接口优先级
	配置 OSPF 接口 MTU
	配置 OSPF 接口 LSA 传送时延
	配置 OSPF LSA 重传
	配置 OSPF 禁止 LSA 扩散
	配置 OSPF SPF 计算时间
配置 OSPF 数据库溢出	
配置 OSPF 与 BFD 联动	配置 OSPF 与 BFD 联动
配置 OSPF GR	配置 OSPF GR Restarter

配置任务

配置 OSPF GR Helper

41.2.1 配置 OSPF 基本功能

-S -E -A

在 OSPF 的各项配置任务中，必须先使能 OSPF 协议，其它功能特性的配置才能生效。

配置条件

在配置 OSPF 基本功能之前，首先完成以下任务：

- 配置链路层协议，保证链路层通信正常；
- 配置接口的 IP 地址，使各相邻节点网络层可达。

使能 OSPF 协议

启用 OSPF 功能，需先创建 OSPF 进程，指定该进程所关联的网络地址范围以及该地址范围所属的区域；如果某个接口 IP 地址在某个区域的网段内，则该接口属于这个区域并使能了 OSPF 功能，OSPF 将把这个接口的直连路由通告出去。

运行 OSPF 协议的设备，必须存在 Router ID，用于在一个 OSPF 自治系统内唯一的标识一台设备。需要保证自治系统内 Router ID 的唯一性，否则会影响邻居建立和路由学习。可在创建 OSPF 进程时指定 Router ID，若没有指定 Router ID，则根据以下规则进行选举：

- 首先从 Loopback 接口的 IP 地址中选择最大的作为 Router ID；
- 若没有配置 IP 地址的 Loopback 接口，则从其它接口的 IP 地址中选择最大的作为 Router ID；
- 只有接口处于 UP 状态时，该接口地址才可能被选作 Router ID。

OSPF 支持多进程，使用进程号标识一个进程，不同进程间相互独立，互不影响。

表 41-2 使能 OSPF 协议

步骤	命令	说明
进入全局配置模式	configure terminal	-
创建 OSPF 进程并进入 OSPF 配置模式	router ospf process-id [vrf vrf-name]	必选 启用或从 VRF 中启用 OSPF 进程，缺省情况下系统未使能 OSPF 协议 从 VRF 下启用 OSPF 时，属于某个 VRF 的 OSPF 进程只能管理属于该 VRF 的接口
配置 OSPF 区域覆盖的网段	network ip-address wildcard-mask area area-id	必选 缺省情况下，接口不属于任何 OSPF 进程和区域 一个接口只能属于一个 OSPF 进程和区域
配置 OSPF 进程的 Router ID	router-id ip-address	可选 缺省情况下，根据 Router ID 的选举规则生成 修改 Router ID 不会导致 OSPF 邻居失效，新配置 Router ID 生效需手动重置进程

41.2.2 配置 OSPF 区域

-S -E -A

为了减少大量数据库信息对 CPU 和内存的占用，将 OSPF 自治系统划分多个区域。区域通过 32 位的区域 ID 来标识，可以用 0~4294967295 范围的十进制数或者 0.0.0.0~255.255.255.255 范围的 IP 地址表示。区域 0 或 0.0.0.0 表示 OSPF 骨干区域，其它非 0 区域为非骨干区域。所有的区域间路由信息都需要通过骨干区域进行转发，非骨干区域之间不能直接交换路由信息。

OSPF 中定义了几种类型的路由器：

- 内部路由器 (Internal Router)：所有接口都属于一个区域的设备；
- 区域边界路由器 (Area Border Router, 简称 ABR)：连接到多个区域的设备；
- 自治系统边界路由器 (Autonomous System Boundary Router, 简称 ASBR)：为 OSPF 自治系统引入外部路由的设备。

配置条件

在配置 OSPF 区域前，首先完成以下任务：

- 配置接口的 IP 地址，使相邻节点网络层可达；
- 使能 OSPF 协议。

配置 OSPF NSSA 区域

非完全存根区域 (Not-So-Stub-Area, 简称 NSSA) 内不允许 Type-5 LSA 注入，但允许 Type-7 LSA 注入。通过配置重分发向 NSSA 区域引入外部路由，NSSA 区域的 ASBR 生成 Type-7 LSA，并泛洪到该 NSSA 区域。NSSA 区域的 ABR 会将 Type-7 LSA 转换为 Type-5 LSA，并把这些转换的 Type-5 LSA 泛洪到整个自治系统。

通过命令 **area area-id nssa no-summary** 配置的 OSPF NSSA 区域，称为完全 NSSA 区域。OSPF 完全 NSSA 区域禁止区域间路由在该区域内泛洪，此时 ABR 会生成一条默认路由，并泛洪到 NSSA 区域内，NSSA 区域内的设备将通过这条默认路由访问区域外的网络。

表 41-3 配置 OSPF NSSA 区域

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
进入 OSPF 配置模式	router ospf process-id [vrf vrf-name]	-
配置 NSSA 区域	area area-id nssa [[default-information-originate [metric metric-value / metric-type type-value] / no-redistribution / no-summary / translator-role { always candidate never }]] [translate-always translate-candidate translate-never]]	必选 缺省情况下，区域不为 NSSA 区域

说明：

- 骨干区域不能配置为 NSSA 区域。
- 同一个 NSSA 区域内的所有设备都必须配置为 NSSA 区域，区域类型不一致的设备间不能形成邻接关系。

配置 OSPF Stub 区域

存根区域 (Stub) 不允许 AS 外部路由在该区域内泛洪，以减少链路状态数据库的大小。配置区域为 Stub 后，位于 Stub 边界的 ABR 产生一条默认路由，并泛洪到该 Stub 区域内，Stub 区域内的设备将通过这条默认路由访问自治系统外的网络。

通过命令 **area area-id stub no-summary** 配置的 OSPF Stub 区域，称为完全 Stub 区域。OSPF 完全 Stub 区域禁止区域间路由、外部路由在该区域内泛洪，区域内的设备将通过默认路由访问该区域外以及 OSPF 自治系统外的网络。

表 41-4 配置 OSPF Stub 区域

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 OSPF 配置模式	router ospf <i>process-id</i> [vrf <i>vrf-name</i>]	-
配置 Stub 区域	area <i>area-id</i> stub [no-summary]	必选 缺省情况下，区域不为 Stub 区域
配置 Stub 区域 ABR 生成默认路由的 cost 值	area <i>area-id</i> default-cost <i>cost-value</i>	可选 缺省情况下，Stub 区域 ABR 生成默认路由的 cost 值为 1

说明：

- 骨干区域不能配置为 Stub 区域。
- 同一个 Stub 区域内的所有设备都必须配置为 Stub 区域，区域类型不一致的设备间不能形成邻接关系。

配置 OSPF 虚链接

OSPF 中非骨干区域间必须通过骨干区域来完成数据库的同步和数据的交互。因此，要求所有的非骨干区域必须和骨干区域保持连通。

当某些情况不能满足该要求时，可通过配置虚链接来解决这个问题。配置虚链接后，可以为该虚链接配置认证方式、修改 Hello 时间间隔等，这些参数的含义与一般 OSPF 接口参数的含义一致。

表 41-5 配置 OSPF 虚链接

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 OSPF 配置模式	router ospf process-id [vrf vrf-name]	-
配置 OSPF 虚链接	area transit-area-id virtual-link neighbor-id [[authentication [message-digest null] authentication-key key message-digest-key key-id md5 key] / dead-interval seconds hello-interval seconds / retransmit-interval seconds / transmit-delay seconds]	必选 缺省情况下，不会创建虚链接

说明：

- 虚链接必须配置在两台 ABR 之间。
- 配置虚链接的两个 ABR 必须处于同一个公共区域，该区域也称为虚链接的传输区域 (Transit Area)。
- 虚链接的传输区域不能是 Stub 区域或 NSSA 区域。

41.2.3 配置 OSPF 网络类型

-S -E -A

OSPF 根据链路协议类型将网络划分为四种类型：

- 广播网络 (Broadcast Networks) —— 链路协议是 Ethernet、FDDI 时，OSPF

缺省网络类型为广播；

- P2P (Point To Point Network) ——当链路协议是 PPP、LAPB、HDLC 时，OSPF 缺省网络类型为 P2P；
- NBMA 网络 (Non-Broadcast Multi-Access Network) ——当链路协议是 ATM、帧中继或 X.25 时，OSPF 缺省网络类型是 NBMA；
- P2MP (Point To Multi-Point Network) ——没有一种链路协议会被 OSPF 缺省认为是 P2MP 类型，通常将不是全联通的 NBMA 网络配置为 OSPF P2MP 网络。

可根据需要，修改 OSPF 接口的网络类型。建立 OSPF 邻居的接口网络类型需要一致，否则将影响路由的正常学习。

配置条件

在配置 OSPF 网络类型前，首先完成以下任务：

- 配置接口的 IP 地址，使相邻节点网络层可达；
- 使能 OSPF 协议。

配置 OSPF 接口网络类型为广播

广播网络支持多台（两个以上）设备，这些设备都有能力与网络上的所有设备交互信息。OSPF 使用 Hello 报文动态的发现邻居。

表 41-6 配置 OSPF 接口网络类型为广播

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置 OSPF 接口网络类型为广播	ip ospf network broadcast	必选 缺省情况下，OSPF 接口网络类型由链路层协议确定

配置 OSPF 接口网络类型为 P2P

单播路由

点到点网络，即由两台设备组成的网络，每台设备在点到点链路的一端。OSPF 使用 Hello 报文动态的发现邻居。

表 41-7 配置 OSPF 接口网络类型为 P2P

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置 OSPF 网络类型为 P2P	ip ospf network point-to-point	必选 缺省情况下，OSPF 接口网络类型由链路层协议确定

配置 OSPF 接口网络类型为 NBMA

NBMA 网络支持多台（两个以上）设备，但是没有广播能力，需要手动指定邻居。

表 41-8 配置 OSPF 接口网络类型为 NBMA

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置 OSPF 网络类型为 NBMA	ip ospf network non-broadcast	必选 缺省情况下，OSPF 接口网络类型由链路层协议确定
进入全局配置模式	exit	-

步骤	命令	说明
进入 OSPF 配置模式	router ospf <i>process-id</i> [vrf <i>vrf-name</i>]	-
配置 NBMA 网络邻居	neighbor <i>neighbor-ip-address</i> [cost <i>cost-value</i> / priority <i>priority-value</i> / poll-interval <i>interval-value</i>]	必选 NBMA 网络中，需手动指定邻居

配置 OSPF 接口网络类型为 P2MP

当 NBMA 不是全连通时，可配置网络类型为 P2MP，节省网络开销。配置网络类型为 P2MP 单播时，需手动指定邻居。

表 41-9 配置 OSPF 接口网络类型为 P2MP

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置 OSPF 网络类型为 P2MP	ip ospf network point-to-multipoint [non-broadcast]	必选 缺省情况下，OSPF 接口网络类型由链路层协议确定
进入全局配置模式	exit	-
进入 OSPF 配置模式	router ospf <i>process-id</i> [vrf <i>vrf-name</i>]	-

步骤	命令	说明
配置 P2MP 单播网络邻居	neighbor <i>neighbor-ip-address</i> [cost <i>cost-value</i> / priority <i>priority-value</i> / poll-interval <i>interval-value</i>]	如果配置接口网络类型为 P2MP 单播，则必选

41.2.4 配置 OSPF 网络认证

-S -E -A

为了防止信息外泄或对 OSPF 设备进行恶意的攻击，OSPF 邻居间所有报文的交互都具有认证能力。认证类型可以是：NULL(不认证)、简单文本认证、MD5 认证和 SM3 认证、key-chain 认证。

配置认证后，OSPF 接口在接收 OSPF 协议报文时，需要先认证，只有通过认证，才能接收该报文。因此建立邻接关系的 OSPF 接口，其认证方式、Key ID、认证密码必须一致。

认证方式和认证密码是独立配置的，当配置认证密码时，如果没有配置认证方式，将自动配置认证密码对应的认证方式。

OSPF 认证方式可以在区域、接口、接口地址上配置，其优先级从低到高为：区域认证、接口认证、接口地址认证。即优先使用接口地址的认证方式，然后使用接口的认证方式，最后使用区域的认证方式。

配置条件

在配置 OSPF 认证前，首先完成以下任务：

- 配置接口的 IP 地址，使相邻节点网络层可达；
- 使能 OSPF 协议。

配置 OSPF 区域认证

OSPF 区域认证只是配置认证方式，需要在接口下配置相应的认证密码，才完全生效。

表 41-10 配置 OSPF 区域认证

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 OSPF 配置模式	router ospf <i>process-id</i> [vrf <i>vrf-name</i>]	-
配置区域认证方式	area <i>area-id</i> authentication [message-digest key-chain]	必选 缺省情况下, 未配置区域认证 该命令中配置关键字 message-digest 表示 MD5 认证, 关键字 key-chain 表示 key-chain 认证, 否则为简单文本认证
进入接口配置模式	interface <i>interface-name</i>	-
配置简单文本认证密码	ip ospf [<i>ip-address</i>] authentication-key { 0 7 } <i>password</i>	必选 缺省情况下, 未配置简单文本认证密码
配置 MD5/SM3 认证密码	ip ospf [<i>ip-address</i>] message-digest-key <i>key-id</i> { md5 sm3 } { 0 7 } <i>password</i>	必选 缺省情况下, 未配置 MD5/SM3 认证密码
配置 key-chain 认证	ip ospf [<i>ip-address</i>] key-chain <i>key-chain name</i>	必选 缺省情况下, 未配置 key-chain 认证

配置 OSPF 接口认证

当一个 OSPF 接口上有多个 IP 地址时，可以为某一个接口地址单独指定认证方式或认证密码。没有指定接口地址时，则接口下所有地址都采用配置的认证方式或认证密码。

表 41-11 配置 OSPF 接口认证

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置接口认证方式	ip ospf [<i>ip-address</i>] authentication [key-chain message-digest null]	必选 缺省情况下，未配置接口认证方式 该命令中配置关键字 message-digest 表示 MD5 认证，关键字 key-chain 表示 key-chain 认证， null 表示不认证，否则为简单文本认证
配置简单文本认证密码	ip ospf [<i>ip-address</i>] authentication-key { 0 7 } <i>password</i>	必选 缺省情况下，未配置简单文本认证密码
配置 MD5/SM3 认证密码	ip ospf [<i>ip-address</i>] message-digest-key <i>key-id</i> { md5 sm3 } { 0 7 } <i>password</i>	必选 缺省情况下，未配置 MD5/SM3 认证密码
配置 key-chain 认证	ip ospf [<i>ip-address</i>] key-chain <i>key-chain name</i>	必选

步骤	命令	说明
		缺省情况下，未配置 key-chain 认证

41.2.5 配置 OSPF 路由生成

-S -E -A

OSPF 中通过 **network** 命令覆盖直连网段路由，也可重分发外部路由或通过 **host** 命令添加主机路由。

配置条件

在配置 OSPF 路由生成前，首先完成以下任务：

- 配置接口的 IP 地址，使相邻节点网络层可达；
- 使能 OSPF 协议。

配置 OSPF 路由重分发

当在一台设备上运行多种路由协议时，通过重分发将其它协议的路由引入到 OSPF 中，缺省生成 OSPF 第二类外部路由，路由 metric 值为 20。重分发引入外部路由时，可修改外部路由类型以及 metric、Tag 字段，并配置相应的路由策略，进行路由控制与管理。

表 41-12 配置 OSPF 路由重分发

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 OSPF 配置模式	router ospf <i>process-id</i> [vrf <i>vrf-name</i>]	-
配置 OSPF 路由重分发	redistribute <i>protocol</i> [<i>protocol-id</i>] [metric <i>metric-value</i> / metric-type <i>metric-type</i> / tag <i>tag-value</i>]	必选 缺省情况下，OSPF 未配置路由重分发

步骤	命令	说明
	<code>/ route-map route-map-name / match route-type]</code>	
配置 OSPF 外部路由 metric 值	<code>default-metric metric-value</code>	可选
配置 OSPF 重分发外部路由数目限制	<code>redistribute maximum-prefix maximum-prefix-value [threshold-value [warning-only] / warning-only]</code>	可选 缺省情况下，OSPF 无重分发外部路由数目限制

说明：

- 同时配置 `redistribute protocol [protocol-id] metric` 和 `default-metric` 设置外部路由的 metric 值时，前者优先级较高。

配置 OSPF 默认路由

配置 OSPF Stub 区域、完全 NSSA 区域后，会自动生成 Type-3 的默认路由。NSSA 区域不会自动生成默认路由，可通过 `area area-id nssa default-information-originate` 命令向 NSSA 区域引入一条 Type-7 的默认路由。

OSPF 不能通过 `redistribute` 命令引入 Type-5 的默认路由，若需要，可通过配置 `default-information originate [always]` 命令来实现。

表 41-13 配置 OSPF 默认路由

单播路由

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 OSPF 配置模式	router ospf <i>process-id</i> [vrf <i>vrf-name</i>]	-
配置 OSPF 引入默认路由	default-information originate [always / metric <i>metric-value</i> / metric-type <i>metric-type</i> / route-map <i>route-map-name</i>]	<p>必选</p> <p>缺省情况下，不会向 OSPF 自治系统引入外部默认路由</p> <p>引入默认路由的缺省 metric 值为 1，类型为外部类型 2</p> <p>always 表示强制向 OSPF 自治系统中生成默认路由，否则，只在本地路由表中有默认路由时才会生成</p>

配置 OSPF 主机路由

表 41-14 配置 OSPF 主机路由

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 OSPF 配置模式	router ospf <i>process-id</i> [vrf <i>vrf-name</i>]	-

步骤	命令	说明
配置 OSPF 主机路由	host <i>ip-address</i> area <i>area-id</i> [cost <i>cost</i>]	必选 缺省情况下，不生成主机路由

41.2.6 配置 OSPF 路由控制

-S -E -A

配置条件

在配置 OSPF 路由控制前，首先完成以下任务：

- 配置接口的 IP 地址，使相邻节点网络层可达；
- 使能 OSPF 协议。

配置 OSPF 区域间路由汇总

OSPF 中 ABR 在向其它区域通告区域间路由时，每条路由都是以 Type-3 LSA 单独通告的，可使用区域间路由汇总功能，将区域内一些连续的网段汇总为一条路由，只将汇总后的路由通告出去，以减少 OSPF 数据库的大小。

表 41-15 配置 OSPF 区域间路由汇总

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 OSPF 配置模式	router ospf <i>process-id</i> [vrf <i>vrf-name</i>]	-
配置 OSPF 区域间路由汇总	area <i>area-id</i> range <i>ip-address/mask-length</i> [advertise [cost <i>cost</i>] cost <i>cost</i> not-advertise]	必选 缺省情况下，ABR 不会进行区域间路由汇总

说明：

- OSPF 区域间路由汇总功能只在 ABR 上生效。
- 缺省情况下，选择明细路由中 cost 的最小值作为汇总路由的 cost 值。

配置 OSPF 外部路由汇总

OSPF 重分发外部路由时，每条路由在外部链路状态通告中均是单独通告的，可使用外部路由汇总功能，将自治系统外一些连续的网段汇总为一条路由，只将汇总后的路由通告出去，以减少 OSPF 数据库的大小。

在 ASBR 上配置 **summary-address** 命令后，可将汇总地址范围内的 Type-5 LSA 和 Type-7 LSA 进行汇总。

表 41-16 配置 OSPF 外部路由汇总

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 OSPF 配置模式	router ospf process-id [vrf vrf-name]	-
配置 OSPF 外部路由汇总	summary-address <i>ip-address mask</i> [not-advertise tag tag-value]	必选 缺省情况下，ASBR 不会进行外部路由汇总

说明：

- OSPF 外部路由汇总功能只在 ASBR 上生效。

配置 OSPF 区域间路由过滤

ABR 在接收区域间路由时，使用 ACL 或者前缀列表进行 in 方向的过滤，在通告区域间路由时使用 ACL 或者前缀列表进行 out 方向的过滤。

表 41-17 配置 OSPF 区域间路由过滤

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 OSPF 配置模式	router ospf process-id [vrf vrf-name]	-
配置 OSPF 区域间路由过滤	area area-id filter-list { access { access-list-name access-list-number } prefix prefix-list-name } { in out }	必选 缺省情况下，ABR 不会进行区域间路由过滤

说明：

- 匹配 ACL 过滤时仅支持标准 ACL。
- OSPF 区域间路由过滤功能只在 ABR 上生效。

配置 OSPF 外部路由过滤

配置外部路由过滤，即应用 ACL 或前缀列表来允许或禁止 OSPF 自治系统外的路由泛洪到 OSPF 自治系统内。

表 41-18 配置 OSPF 外部路由过滤

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 OSPF 配置模式	router ospf <i>process-id</i> [vrf <i>vrf-name</i>]	-
配置分布列表过滤外部路由	distribute-list { <i>access-list-name</i> <i>access-list-number</i> prefix <i>prefix-list-name</i> } out [<i>routing-protocol</i> [<i>process-id</i>]]	必选 缺省情况下, ASBR 不会进行外部路由过滤

说明:

- 匹配 ACL 过滤时仅支持标准 ACL。
- OSPF 外部路由过滤功能只在 ASBR 上生效。

配置 OSPF 路由安装过滤

OSPF 通过 LSA 计算出路由后, 为了防止某些路由加入路由表, 可对计算出的 OSPF 协议路由信息进行过滤。

有三种过滤方法:

- 基于前缀过滤, 使用 ACL、前缀列表对路由的目的地址进行过滤;
- 基于下一跳过滤, 使用前缀列表对路由的下一跳进行过滤。也可使用前缀列表, 同时对路由目的地址和下一跳进行过滤;
- 基于路由策略, 对路由进行过滤。

表 41-19 配置 OSPF 路由安装过滤

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 OSPF 配置模式	router ospf process-id [vrf vrf-name]	-
配置 OSPF 禁止安装路由	distribute-list { access-list-name access-list-number gateway prefix-list-name1 prefix prefix-list-name2 [gateway prefix-list-name3] route-map route-map-name } in [interface-name]	必选 缺省情况下，不会对安装的路由进行过滤

说明：

- 配置 **prefix**、**gateway**、**route-map** 过滤与配置 ACL 过滤互斥，如：先配置了 **prefix** 过滤，则不能再配置 ACL 过滤。
- 配置 **route-map**、**prefix** 过滤与配置 **gateway** 过滤互斥。
- 配置 **prefix** 过滤与配置 **gateway** 过滤相互覆盖。

配置 OSPF 接口 cost 值

缺省情况下，OSPF 接口开销的计算方法为：参考带宽/接口带宽。

表 41-20 配置 OSPF 接口 cost 值

步骤	命令	说明
进入全局配置模式	configure terminal	-

单播路由

步骤	命令	说明
进入接口配置模式	interface <i>interface-name</i>	-
配置 OSPF 接口 cost 值	ip ospf [<i>ip-address</i>] cost <i>cost-value</i>	可选 缺省情况下, 根据参考 带宽/接口带宽计算所得

配置 OSPF 参考带宽

接口参考带宽主要用于计算接口 cost 值, 缺省为 100Mbit/s, OSPF 接口 cost 的计算方法为: 参考带宽/接口带宽, 计算结果大于 1 时, 取整数部分; 小于 1 时, 则取 1。因此在带宽高于 100Mbit/s 的网络中, 将不能正确的选择出最优路由, 可使用 **auto-cost reference-bandwidth** 命令配置适当的参考带宽来解决这个问题。

表 41-21 配置 OSPF 参考带宽

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 OSPF 配置模式	router ospf <i>process-id</i> [vrf <i>vrf-name</i>]	-
配置 OSPF 接口参考带宽	auto-cost reference- bandwidth <i>reference-</i> <i>bandwidth</i>	可选 缺省情况下, 参考带宽 为 100Mbit/s

配置 OSPF 管理距离

管理距离用于表示路由协议的可信度, 当从不同路由协议学习到达同一目的网络的路由后, 根据管理距离进行选择, 优先选择管理距离小的路由。

表 41-22 配置 OSPF 管理距离

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 OSPF 配置模式	router ospf process-id [vrf vrf-name]	-
配置 OSPF 管理距离	distance { distance [ip-address wildcard-mask] [access-list-name access-list-number] ospf { external distance inter-area distance intra-area distance } }	可选 缺省情况下，OSPF 区域内路由、区域间路由管理距离为 110，外部路由管理距离为 150

配置 OSPF 最大负载均衡条目数

到达同一目的地址存在多条等价路径，则形成负载均衡，可提高链路的利用率并减少链路的负担。

表 41-23 配置 OSPF 最大负载均衡条目数

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 OSPF 配置模式	router ospf process-id [vrf vrf-name]	-
配置 OSPF 最大负载均衡条目数	maximum-path max-number	可选 缺省情况下，OSPF 最大负载均衡条目数为 4

配置 OSPF 兼容 RFC1583

当存在多条到达 ASBR 或外部路由转发地址的路径时，RFC1583 与 RFC2328 定义了不同的选路规则。配置兼容 RFC1583 时，优先选择骨干区域的区域内路径或区域间路径；不兼容 RFC1583 时，优先选择非骨干区域的区域内路径。

表 41-24 配置 OSPF 兼容 RFC1583

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 OSPF 配置模式	router ospf process-id [vrf vrf-name]	-
配置 OSPF 兼容 RFC1583	compatible rfc1583	必选 缺省情况下，不兼容 RFC1583

说明：

- OSPF 自治系统中，所有设备的选路规则需一致，即配置都兼容 RFC1583 或都不兼容 RFC1583，以防止形成路由环路。

41.2.7 配置 OSPF 网络优化

-S -E -A

配置条件

在配置 OSPF 网络优化前，首先完成以下任务：

- 配置接口的 IP 地址，使相邻节点网络层可达；
- 使能 OSPF 协议。

配置 OSPF 邻居保活时间

OSPF Hello 报文用来建立并保活邻居关系，Hello 报文缺省发送时间间隔由网络类型确定，广播网络、P2P 网络中 Hello 报文发送时间间隔缺省为 10 秒，P2MP、NBMA 网络中 Hello 报文发送时间间隔缺省为 30 秒。

邻居失效时间用来判断邻居的有效性，缺省是 Hello 时间间隔的 4 倍。若 OSPF 设备在邻居失效时间超时后还没有收到邻居的 Hello 报文，则认为邻居已经无效，并主动删除该邻居。

表 41-25 配置 OSPF 邻居保活时间

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置 OSPF Hello 时间间隔	ip ospf [<i>ip-address</i>] hello-interval <i>interval-value</i>	可选 缺省值根据网络类确定，广播网络、P2P 网络为 10 秒，P2MP、NBMA 网络为 30 秒
配置 OSPF 邻居失效时间	ip ospf [<i>ip-address</i>] dead-interval <i>interval-value</i>	可选 缺省为发送 Hello 时间间隔的 4 倍

说明：

- OSPF 相邻设备间 Hello 时间间隔和邻居失效时间必须一致，否则不能建立起邻居关系。
- 修改 Hello 时间间隔时，若当前邻居失效时间为 Hello 时间间隔的 4 倍，则邻居失效时间也会自动修改保持 4 倍关系；若当前邻居失效时间不是 Hello 时间间隔的 4 倍，则邻居失效时间保持不变。
- 修改邻居失效时间不会影响 Hello 时间间隔。

配置 OSPF 被动接口

动态路由协议采用被动接口（Passive Interface），可有效减少路由协议对网络带宽的消耗。配置 OSPF 被动接口，可通过 **network** 命令通告该接口所在直连网段的路由，但抑制 OSPF 协议报文在该接口上的接收和发送。

表 41-26 配置 OSPF 被动接口

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 OSPF 配置模式	router ospf process-id [vrf vrf-name]	-
配置 OSPF 被动接口	passive-interface { <i>interface-name</i> [<i>ip-address</i>] default }	必选 缺省情况下，未配置 OSPF 被动接口

配置 OSPF 需求电路

在 P2P、P2MP 链路上，为减少线路费用，可配置 OSPF 需求电路，抑制 Hello 报文的周期性发送和 LSA 报文的周期刷新。主要用在 ISDN、SVC、X.25 等收费链路上。

表 41-27 配置 OSPF 需求电路

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface interface-name	-
配置 OSPF 需求电路	ip ospf [ip-address] demand-circuit	必选

步骤	命令	说明
		缺省情况下，未使能 OSPF 需求电路

配置 OSPF 接口优先级

接口优先级主要用于广播网络、NBMA 网络中，指定路由器 DR (Designed Router)、备份指定路由器 BDR (Backup Designed Router) 的选举，取值范围 0~255，数值越大优先级越高，缺省为 1。

DR 和 BDR 是由同一网段中所有设备根据接口优先级、Router ID 通过 Hello 报文选举出来的，规则如下：

- 首先选举接口优先级最高的设备为 DR，选举接口优先级次高的为 BDR，优先级为 0，不参与选举；
- 如果接口优先级相同，则选举 Router ID 最高的设备为 DR，选举 Router ID 次高的为 BDR；
- 当 DR 失效后，BDR 会立即成为 DR，再选举新的 BDR。

表 41-28 配置 OSPF 接口优先级

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置 OSPF 接口优先级	ip ospf priority <i>priority-value</i>	可选 缺省情况下，OSPF 接口优先级为 1

说明：

- 优先级只影响选举过程，当网络中已经选举产生了 DR 和 BDR 时，修改接口优先级并不会影响本次选举结果，只影响下一次 DR 或 BDR 选举结果；故 DR 不一定是接口优先级最高的设备，BDR 不一定是接口优先级次高的设备。

配置 OSPF 接口 MTU

封装 OSPF 报文时，为了避免分片，报文的大小都限制为小于等于接口 MTU 值。当 OSPF 相邻设备间交互 DD 报文时，缺省情况下会检查 MTU 是否相同，若不相同则不能形成邻接关系。配置 OSPF 忽略接口 MTU 检查后，即使 MTU 不相同，也可以建立邻接关系。

表 41-29 配置 OSPF 接口 MTU

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置 OSPF 接口 MTU	ip ospf mtu <i>mtu-value</i>	可选
配置 OSPF 接口忽略 MTU 一致性检查	ip ospf [<i>ip-address</i>] mtu-ignore	必选 缺省情况下，会进行 MTU 一致性检查

配置 OSPF 接口 LSA 传送时延

LSA 传送时延表示 LSA 泛洪到其它设备所需花费的时间，发送 LSA 的设备会将接口传送时延加到待发送 LSA 的老化时间上。缺省情况下，当泛洪的 LSA 经过一台设备时老化时间会加 1。可根据网络状况配置 LSA 的传送时延，取值范围 1 ~ 840。一般用在低速链路上。

表 41-30 配置 OSPF 接口 LSA 传送时延

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置 OSPF 接口 LSA 传送时延	ip ospf transmit-delay <i>delay-value</i>	可选 缺省情况下, LSA 传送时延为 1 秒

配置 OSPF LSA 重传

为了保证数据交互的可靠性, OSPF 采用确认机制。当设备接口上泛洪一个 LSA 时, 会将该 LSA 加入到邻居的重传列表中, 若在重传时间超时后还没有收到邻居的确认信息, 则会重传该 LSA, 直到收到确认信息。

表 41-31 配置 OSPF LSA 重传

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置 OSPF LSA 重传时间间隔	ip ospf retransmit-interval <i>interval-value</i>	可选 缺省情况下, 重传时间间隔为 5 秒

配置 OSPF 禁止 LSA 扩散

在实际网络应用中, 某些情况下会在 OSPF 邻居间使用冗余链路, 使用该配置可减少 OSPF 更新报文在冗余链路上的扩散。

表 41-32 配置 OSPF 禁止 LSA 扩散

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置 OSPF 接口禁止扩散 LS-UPD	ip ospf database-filter all out	必选 缺省情况下, OSPF 接口不会禁止 LSA 扩散

说明:

- 配置 OSPF 禁止 LSA 扩散功能可能会导致部分路由信息丢失。

配置 OSPF SPF 计算时间

当 OSPF 网络拓扑发生变化时, 需要重新计算路由。网络不断变化时, 频繁的路由计算会占用大量的系统资源。通过调整 SPF 计算的时间参数, 来抑制网络频繁变化对系统资源的消耗。

表 41-33 配置 OSPF SPF 计算时间

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 OSPF 配置模式	router ospf <i>process-id</i> [vrf <i>vrf-name</i>]	-
配置 OSPF SPF 计算时间	timers throttle spf <i>delay-time hold-time max-time</i>	可选 缺省情况下, <i>delay-time</i> 为 5000ms, <i>hold-time</i> 为

步骤	命令	说明
		10000ms, max-time 为 10000ms

说明：

- 参数 *delay-time* 表示初始计算时延, *hold-time* 表示抑制时间, *max-time* 表示两次 SPF 计算的最大等待时间。在网络变化不频繁的情况下将连续路由计算的时间间隔缩小到 *delay-time*, 而在网络变化频繁的情况下可以进行相应调整, 增加 *hold-time* $\times 2^{n-2}$ (n 为连续触发路由计算的次数), 将等待时间按照配置的 *hold-time* 增量延长, 最大不超过 *max-time*。

配置 OSPF 数据库溢出

OSPF 数据库溢出用于限制数据库中 Type-5 LSA 的数量。

表 41-34 配置 OSPF 数据库溢出

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 OSPF 配置模式	router ospf process-id [vrf vrf-name]	-
配置 OSPF 数据库溢出	overflow database external max-number seconds	必选 缺省情况下, 未启用 OSPF 数据库溢出功能

说明：

- 使能数据库溢出功能后，可能会导致 OSPF 区域中的数据库不一致，部分路由丢失。

41.2.8 配置 OSPF 与 BFD 联动

-E -A

配置条件

在配置 OSPF 与 BFD 联动前，首先完成以下任务：

- 配置接口的 IP 地址，使相邻节点网络层可达；
- 使能 OSPF 协议。

配置 OSPF 与 BFD 联动

BFD(Bidirectional Forwarding Detection，双向转发检测)提供一种快速检测两台设备之间线路状态的方法。当相邻的两台 OSPF 设备间启动 BFD 检测后，若设备之间发生线路故障，BFD 会快速检测到故障并通知 OSPF 协议，触发 OSPF 进行路由计算并切换到备份线路，达到路由快速切换的目的。

表 41-35 配置 OSPF 与 BFD 联动

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置 OSPF 指定接口使能或禁用 BFD	ip ospf bfd [<i>ip-address</i> / disable]	必选 缺省情况下，未使能 BFD 功能
进入全局配置模式	exit	-
进入 OSPF 配置模式	router ospf <i>process-id</i> [vrf <i>vrf-name</i>]	-

步骤	命令	说明
配置 OSPF 进程的所有接口使能 BFD	bfd all-interface	可选

说明：

- 同时在 OSPF 配置模式、接口配置模式下配置 BFD 时，接口下配置优先级较高。

41.2.9 配置 OSPF GR

-S -E -A

GR (Graceful Restart, 优雅重启) 用于在设备主备切换过程中，保持本设备和邻居设备转发层面路由信息不变，转发不受影响；当切换设备重新运行后，两台设备协议层面同步路由信息并更新转发层，达到设备切换过程中数据转发不间断的目的。

GR 过程中有两种角色：

- GR Restarter 端——进行协议优雅重启的设备。
- GR Helper 端——协助协议优雅重启的设备。

分布式设备可以充当 GR Restarter 和 GR Helper，而集中式设备只能充当 GR Helper，协助 Restarter 端完成 GR。

配置条件

在配置 OSPF GR 前，首先完成以下任务：

- 配置接口的 IP 地址，使相邻节点可达。
- 使能 OSPF 协议。

配置 OSPF GR Restarter

表 41-36 配置 OSPF GR Restarter

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 OSPF 配置模式	router ospf <i>process-id</i> [vrf <i>vrf-name</i>]	-
配置 OSPF GR	nsf ietf	必选 缺省情况下，未启用 GR 功能 该功能生效，协议需支持 Opaque-LSA 功能，缺省支持 Opaque-LSA 功能
配置 OSPF GR 周期	nsf interval <i>grace-period</i>	可选 缺省情况下，GR 周期为 95 秒

说明：

- OSPF GR 功能只在堆叠环境或者存在双主控的环境中使用。

配置 OSPF GR Helper

GR Helper 协助 Restarter 端完成 GR，缺省情况下，设备都使能该功能，命令 **nsf ietf helper disable** 用来禁用 GR Helper 功能。命令 **nsf ietf helper strict-lsa-checking** 用来配置 Helper 端在 GR 过程中对 LSA 进行严格检查，若检查到 LSA 发生变化，则退出 GR Helper 模式。

表 41-37 配置 OSPF GR Helper

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 OSPF 配置模式	router ospf <i>process-id</i> [vrf <i>vrf-name</i>]	-
配置 OSPF GR Helper	nsf ietf helper [disable strict-lsa-checking]	可选 缺省情况下, 使能 Helper 功能, 不会对 LSA 进行严格检查

41.2.10 OSPF 监控与维护 **-S -E -A**

表 41-38 OSPF 监控与维护

命令	说明
clear ip ospf [<i>process-id</i>] process	重置 OSPF 进程
clear ip ospf <i>process-id</i> neighbor <i>neighbor-ip-address</i> [<i>neighbor-router-id</i>]	重置 OSPF 邻居
clear ip ospf statistics [<i>interface-name</i>]	清除 OSPF 接口统计信息
clear ip ospf [<i>process-id</i>] redistribution	重新通告外部路由
clear ip ospf [<i>process-id</i>] route	重新计算 OSPF 路由
show ip ospf [<i>process-id</i>]	显示 OSPF 基本信息

命令	说明
show ip ospf [<i>process-id</i>] border-routers	显示 OSPF 中到达边界设备的路由信息
show ip ospf [<i>process-id</i>] buffers	显示 OSPF 报文收发缓存大小
show ip ospf [<i>process-id</i>] database [<i>adv-router router-id</i> <i>age lsa_age</i> database-summary max-age [<i>asbr-summary</i> external network nssa-external opaque-area opaque-as opaque-link router self-originate summary] [[<i>link-state-id</i>] [<i>adv-router advertising-router-id</i>] self-originate summary]]	显示 OSPF 数据库信息
show ip ospf interface [<i>interface-name</i> [detail]]	显示 OSPF 接口信息
show ip ospf [<i>process-id</i>] neighbor [<i>neighbor-id</i> all detail [all] interface <i>ip-address</i> [detail] statistic]	显示 OSPF 邻居信息
show ip ospf [<i>process-id</i>] route [<i>ip-address mask</i> <i>ip-address/mask-length</i> external inter-area intra-area statistic]	显示 OSPF 协议路由信息
show ip ospf [<i>process-id</i>] virtual-links	显示 OSPF 虚链接信息

命令	说明
show ip ospf [process-id] sham-links	显示配置的 OSPF 伪链接接口信息，包括接口状态、cost 值、邻居状态

41.3 OSPF 典型配置举例

41.3.1 配置 OSPF 基本功能

-S -E -A

网络需求

- 所有设备配置 OSPF 协议，划分区域 0、区域 1 和区域 2 三个区域。配置完成后，所有设备能相互学习路由。
- 在背靠背的以太接口上，为了加快 OSPF 邻居建立，可将 OSPF 接口网络类型改为点对点。修改区域 2 的接口网络类型为点到点，配置完成后，所有设备能相互学习路由。

网络拓扑

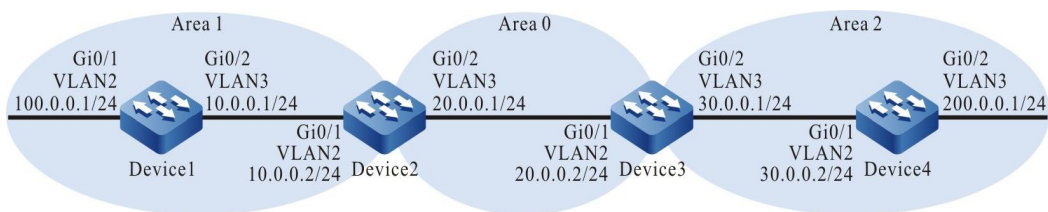


图 41-1 配置 OSPF 基本功能组网图

配置步骤

- 步骤 1: 配置 VLAN，并将端口加入对应的 VLAN。（略）
- 步骤 2: 配置各接口 IP 地址。（略）
- 步骤 3: 配置 OSPF 进程并将相应接口覆盖到不同区域中。

#配置 Device1，配置 OSPF 进程并将接口覆盖到区域 1 中。

单播路由

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#router-id 1.1.1.1
Device1(config-ospf)#network 10.0.0.0 0.0.0.255 area 1
Device1(config-ospf)#network 100.0.0.0 0.0.0.255 area 1
Device1(config-ospf)#exit
```

#配置 Device2，配置 OSPF 进程并将相应接口覆盖到区域 0 和区域 1 中。

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#router-id 2.2.2.2
Device2(config-ospf)#network 20.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 10.0.0.0 0.0.0.255 area 1
Device2(config-ospf)#exit
```

#配置 Device3，配置 OSPF 进程并将相应接口覆盖到区域 0 和区域 2 中。

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#router-id 3.3.3.3
Device3(config-ospf)#network 20.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 30.0.0.0 0.0.0.255 area 2
Device3(config-ospf)#exit
```

#配置 Device4，配置 OSPF 进程并将接口覆盖到区域 2 中。

```
Device4#configure terminal
Device4(config)#router ospf 100
Device4(config-ospf)#router-id 4.4.4.4
Device4(config-ospf)#network 30.0.0.0 0.0.0.255 area 2
Device4(config-ospf)#network 200.0.0.0 0.0.0.255 area 2
Device4(config-ospf)#exit
```

说明：

- Router ID 可以手工配置也可以自动生成，如果没有手工配置 Router ID，设备会自动选择 Router ID。首先选择 Loopback 接口中最大的 IP 地址作为 Router ID；如果设备没有配置 Loopback 接口地址，则会选择普通接口中最大的 IP 地址作为 Router ID。只有接口处于 up 状态时，该接口地址才可能被选作 Router ID。
 - 使用 **network** 命令时，反掩码可以不用精确匹配接口 IP 地址掩码长度，只要 **network** 网段覆盖接口 IP 地址即可。如：**network 0.0.0.0 255.255.255.255** 就表示覆盖所有接口。
-

#查看 Device1 的 OSPF 邻居信息和路由表。

```
Device1#show ip ospf neighbor
OSPF process 100:
Neighbor ID  Pri  State           Dead Time  Address      Interface
2.2.2.2      1  Full/DR        00:00:36  10.0.0.2    vlan3
```

```
Device1#show ip route
```

单播路由

Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

```
C 10.0.0.0/24 is directly connected, 02:26:21, vlan3
O 20.0.0.0/24 [110/2] via 10.0.0.2, 02:25:36, vlan3
O 30.0.0.0/24 [110/3] via 10.0.0.2, 02:25:36, vlan3
C 100.0.0.0/24 is directly connected, 02:26:23, vlan2
C 127.0.0.0/8 is directly connected, 18:09:44, lo0
O 200.0.0.0/24 [110/4] via 10.0.0.2, 02:25:36, vlan3
```

#查看 Device2 的 OSPF 邻居和路由表。

```
Device2#show ip ospf neighbor
OSPF process 100:
Neighbor ID Pri State Dead Time Address Interface
1.1.1.1 1 Full/Backup 00:00:37 10.0.0.1 vlan2
3.3.3.3 1 Full/DR 00:00:38 20.0.0.2 vlan3
```

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS
```

Gateway of last resort is not set

```
C 10.0.0.0/24 is directly connected, 02:31:15, vlan2
C 20.0.0.0/24 is directly connected, 02:31:50, vlan3
O 30.0.0.0/24 [110/2] via 20.0.0.2, 02:31:40, vlan3
O 100.0.0.0/24 [110/2] via 10.0.0.1, 02:30:29, vlan2
C 127.0.0.0/8 is directly connected, 240:21:34, lo0
O 200.0.0.0/24 [110/3] via 20.0.0.2, 02:31:40, vlan3
```

#查看 Device2 的 OSPF LSDB (链路状态数据库)。

```
Device2#show ip ospf database

OSPF Router with ID (2.2.2.2) (Process ID 100)

Router Link States (Area 0)

Link ID ADV Router Age Seq# CkSum Link count
2.2.2.2 2.2.2.2 1777 0x8000000c 0xcb20 1
3.3.3.3 3.3.3.3 309 0x8000000a 0x9153 1

Net Link States (Area 0)

Link ID ADV Router Age Seq# CkSum
20.0.0.2 3.3.3.3 369 0x80000006 0xec12

Summary Link States (Area 0)

Link ID ADV Router Age Seq# CkSum Route
10.0.0.0 2.2.2.2 1757 0x80000005 0xcc59 10.0.0.0/24
100.0.0.0 2.2.2.2 1356 0x80000005 0x408a 100.0.0.0/24
30.0.0.0 3.3.3.3 9 0x80000006 0xa765 30.0.0.0/24
200.0.0.0 3.3.3.3 149 0x80000006 0x075a 200.0.0.0/24

Router Link States (Area 1)

Link ID ADV Router Age Seq# CkSum Link count
1.1.1.1 1.1.1.1 1775 0x80000009 0xbbda 2
2.2.2.2 2.2.2.2 1737 0x80000008 0x2dd5 1

Net Link States (Area 1)

Link ID ADV Router Age Seq# CkSum
```

单播路由

```
10.0.0.2    2.2.2.2    34 0x80000006 0x39db
```

Summary Link States (Area 1)

Link ID	ADV Router	Age	Seq#	CkSum	Route
20.0.0.0	2.2.2.2	144	0x80000006	0x48d2	20.0.0.0/24
30.0.0.0	2.2.2.2	1186	0x80000005	0xd13f	30.0.0.0/24
200.0.0.0	2.2.2.2	14	0x80000006	0x2f35	200.0.0.0/24

对 Device2 来说，30.0.0.0/24、200.0.0.0/24 是区域间路由，从 Summary Link States (Area 0) 中可看到相关路由 LSA 信息；如果是区域内路由，则需要 **show ip ospf database router** 才能看到相关路由 LSA 信息。

步骤 4： 配置 OSPF 接口网络类型为点对点。

#配置 Device3，将接口 VLAN3 的 OSPF 网络类型改为点到点。

```
Device3(config)#interface vlan3
Device3(config-if-vlan3)#ip ospf network point-to-point
Device3(config-if-vlan3)#exit
```

#配置 Device4，将接口 VLAN2 的 OSPF 网络类型改为点到点。

```
Device4(config)#interface vlan2
Device4(config-if-vlan2)#ip ospf network point-to-point
Device4(config-if-vlan2)#exit
```

步骤 5： 检验结果。

#查看 Device3 的 OSPF 邻居和路由表。

```
Device3#show ip ospf neighbor
OSPF process 100:
Neighbor ID  Pri  State      Dead Time  Address    Interface
2.2.2.2      1  Full/Backup 00:00:36  20.0.0.1  vlan2
4.4.4.4      1  Full/-      00:00:39  30.0.0.2  vlan3

Device3#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

O  10.0.0.0/24 [110/2] via 20.0.0.1, 00:02:53, vlan2
C  20.0.0.0/24 is directly connected, 03:20:36, vlan2
C  30.0.0.0/24 is directly connected, 03:20:26, vlan3
O  100.0.0.0/24 [110/3] via 20.0.0.1, 00:01:51, vlan2
C  127.0.0.0/8 is directly connected, 262:01:24, lo0
O  200.0.0.0/24 [110/2] via 30.0.0.2, 00:00:11, vlan3
```

说明：

- 点对点网络建立 OSPF 邻接时，不会进行 DR 和 BDR 选举。
-

#查看 Device4 的 OSPF 邻居和路由表。

```
Device4#show ip ospf neighbor
OSPF process 100:
Neighbor ID   Pri  State           Dead Time  Address      Interface
3.3.3.3       1    Full/-         00:00:39  30.0.0.1    vlan2

Device4#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

O  10.0.0.0/24 [110/3] via 30.0.0.1, 00:01:04, vlan2
O  20.0.0.0/24 [110/2] via 30.0.0.1, 00:01:04, vlan2
C  30.0.0.0/24 is directly connected, 03:20:25, vlan2
O  100.0.0.0/24 [110/4] via 30.0.0.1, 00:01:04, vlan2
C  127.0.0.0/8 is directly connected, 22:52:36, lo0
C  200.0.0.0/24 is directly connected, 03:20:13, vlan3
```

可以看到，修改 OSPF 接口网络类型为点对点后，邻居能够正常建立，且能够正常学到路由。

说明：

- 配置 OSPF 接口网络类型时，邻居两端的 OSPF 接口网络类型必须一致，否则会影响路由的正常学习和泛洪。默认情况下，OSPF 接口的网络类型由物理接口的网络类型决定。
-

41.3.2 配置 OSPF 认证

-S -E -A

网络需求

- 所有设备运行 OSPF 并配置区域认证，区域 0 配置为简单文本认证，区域 1 配置为 MD5 认证。
- 配置 OSPF 接口认证，区域 0 的接口认证配置为简单文本认证，区域 1 的接口认证配置为 MD5 认证。
- 配置完成后，设备能够正常建立邻居并相互学习路由。

网络拓扑

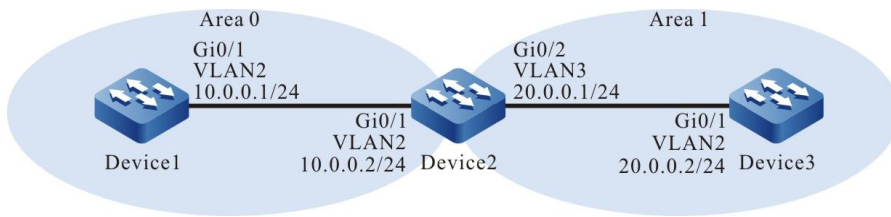


图 41-2 配置 OSPF 认证组网图

配置步骤

步骤 1: 配置 VLAN，并将端口加入对应的 VLAN。（略）

步骤 2: 配置各接口 IP 地址。（略）

步骤 3: 配置 OSPF 进程，将相应接口覆盖到不同区域中并开启区域认证，其中区域 0 采用简单文本认证方式，区域 1 采用 MD5 认证方式。

#配置 Device1，配置 OSPF 进程并配置区域认证功能。

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#router-id 1.1.1.1
Device1(config-ospf)#area 0 authentication
Device1(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#配置 Device2，配置 OSPF 进程并配置区域认证功能。

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#router-id 2.2.2.2
Device2(config-ospf)#area 0 authentication
Device2(config-ospf)#area 1 authentication message-digest
Device2(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 20.0.0.0 0.0.0.255 area 1
Device2(config-ospf)#exit
```

#配置 Device3，配置 OSPF 进程并配置区域认证功能。

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#router-id 3.3.3.3
Device3(config-ospf)#area 1 authentication message-digest
Device3(config-ospf)#network 20.0.0.0 0.0.0.255 area 1
Device3(config-ospf)#exit
```

#查看 Device1 的 OSPF 进程信息。

```
Device1#show ip ospf 100
Routing Process "ospf 100" with ID 1.1.1.1
Process bound to VRF default
Process uptime is 30 minutes
IETF NSF restarter support disabled
IETF NSF helper support enabled
Conforms to RFC2328, and RFC1583Compatibility flag is disabled
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Graceful Restart
Initial SPF schedule delay 5000 msec
Minimum hold time between two consecutive SPF 10000 msec
Maximum wait time between two consecutive SPF 10000 msec
Refresh timer 10 secs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of non-default external LSA is 0
External LSA database is unlimited.
Not Support Demand Circuit lsa number is 0, autonomy system support flood DoNotAge Lsa
Number of areas attached to this router: 1
  Area 0 (BACKBONE)   Number of interfaces in this area is 1(1)
    Number of fully adjacent neighbors in this area is 1
    Number of fully adjacent sham-link neighbors in this area is 0
    Area has simple password authentication
    SPF algorithm last executed 00:27:43.916 ago
    SPF algorithm executed 3 times
    Number of LSA 4. Checksum Sum 0x0160f7
    Not Support Demand Circuit lsa number is 0,
    Indication lsa (by other routers) number is: 0,
    Area support flood DoNotAge Lsa
```

可以看到，区域认证为简单文本方式。

#查看 Device1 的 OSPF 邻居信息和路由表。

```
Device1#show ip ospf neighbor
OSPF process 100:
Neighbor ID  Pri  State      Dead Time  Address      Interface
2.2.2.2      1  Full/DR   00:00:38  10.0.0.2    vlan2

Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C 10.0.0.0/24 is directly connected, 00:14:01, vlan2
O 20.0.0.0/24 [110/2] via 10.0.0.2, 00:10:38, vlan2
C 127.0.0.0/8 is directly connected, 20:55:08, lo0
```

Device1 上，邻居正常建立，路由学习正常。

#查看 Device3 的 OSPF 进程信息。

```
Device3#show ip ospf 100
Routing Process "ospf 100" with ID 3.3.3.3
Process bound to VRF default
Process uptime is 28 minutes
IETF NSF restarter support disabled
IETF NSF helper support enabled
Conforms to RFC2328, and RFC1583Compatibility flag is disabled
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Graceful Restart
Initial SPF schedule delay 5000 msec
Minimum hold time between two consecutive SPF 10000 msec
```

```
Maximum wait time between two consecutive SPFs 10000 msec
Refresh timer 10 secs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of non-default external LSA is 0
External LSA database is unlimited.
Not Support Demand Circuit lsa number is 0, autonomy system support flood DoNotAge Lsa
Number of areas attached to this router: 1
  Area 1    Number of interfaces in this area is 1(1)
            Number of fully adjacent neighbors in this area is 1
            Number of fully adjacent sham-link neighbors in this area is 0
            Number of fully adjacent virtual neighbors through this area is 0
            Area has message digest authentication
            SPF algorithm last executed 00:24:01.783 ago
            SPF algorithm executed 5 times
            Number of LSA 4. Checksum Sum 0x0337cf
            Not Support Demand Circuit lsa number is 0,
            Indication lsa (by other routers) number is: 0,
            Area support flood DoNotAge Lsa
```

可以看到，区域认证为 MD5 认证方式。

#查看 Device3 的 OSPF 邻居信息和路由表。

```
Device3#show ip ospf neighbor
OSPF process 100:
Neighbor ID Pri State Dead Time Address Interface
2.2.2.2 1 Full/Backup 00:00:33 20.0.0.1 vlan2

Device3#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

O 10.0.0.0/24 [110/2] via 20.0.0.1, 00:09:31, vlan2
C 20.0.0.0/24 is directly connected, 00:20:36, vlan2
C 127.0.0.0/8 is directly connected, 24:00:06, lo0
```

Device3 上，邻居正常建立，路由学习正常。

步骤 4：配置 OSPF 接口认证。

#配置 Device1，接口 VLAN2 采用简单文本认证，口令为 admin。

```
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip ospf authentication
Device1(config-if-vlan2)#ip ospf authentication-key 0 admin
Device1(config-if-vlan2)#exit
```

#配置 Device2，接口 VLAN2 采用简单文本认证，口令为 admin；接口 VLAN3 采用 MD5 认证，Key ID 为 1，口令为 admin。

```
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ip ospf authentication
Device2(config-if-vlan2)#ip ospf authentication-key 0 admin
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan3
Device2(config-if-vlan3)#ip ospf authentication message-digest
Device2(config-if-vlan3)#ip ospf message-digest-key 1 md5 0 admin
Device2(config-if-vlan3)#exit
```

#配置 Device3, 接口 VLAN2 采用 MD5 认证, Key ID 为 1, 口令为 admin。

```
Device3(config)#interface vlan2
Device3(config-if-vlan2)#ip ospf authentication message-digest
Device3(config-if-vlan2)#ip ospf message-digest-key 1 md5 0 admin
Device3(config-if-vlan2)#exit
```

步骤 5: 检验结果。

#查看 Device2 的 OSPF 邻居信息。

```
Device2#show ip ospf neighbor
OSPF process 100:
Neighbor ID Pri State Dead Time Address Interface
1.1.1.1 1 Full/Backup 00:00:33 10.0.0.1 vlan2
3.3.3.3 1 Full/DR 00:00:39 20.0.0.2 vlan3
```

#查看 Device2 的 OSPF 的接口信息。

```
Device2#show ip ospf interface vlan2
vlan2 is up, line protocol is up
Internet Address 10.0.0.2, 10.0.0.255( a[10.0.0.2] d[10.0.0.255]) Area 0, MTU 1500
Process ID 100, Router ID 2.2.2.2, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1, TE Metric 0
Designated Router (ID) 2.2.2.2, Interface Address 10.0.0.2
Backup Designated Router (ID) 1.1.1.1, Interface Address 10.0.0.1
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:04
Neighbor Count is 1, Adjacent neighbor count is 1
Crypt Sequence Number is 0
Graceful restart proxy id is 0x0
Hello received 406 sent 454, DD received 8 sent 6
LS-Req received 2 sent 2, LS-Upd received 11(LSA: 15) sent 10(LSA: 14)
LS-Ack received 10 sent 0, Discarded 0
```

```
Device2#show ip ospf interface vlan3
vlan3 is up, line protocol is up
Internet Address 20.0.0.1, 20.0.0.255( a[20.0.0.1] d[20.0.0.255]) Area 1, MTU 1500
Process ID 100, Router ID 2.2.2.2, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State Backup, Priority 1, TE Metric 0
Designated Router (ID) 3.3.3.3, Interface Address 20.0.0.2
Backup Designated Router (ID) 2.2.2.2, Interface Address 20.0.0.1
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:00
Neighbor Count is 1, Adjacent neighbor count is 1
Crypt Sequence Number is 485
Graceful restart proxy id is 0x0
Hello received 412 sent 454, DD received 9 sent 12
LS-Req received 3 sent 3, LS-Upd received 9(LSA: 10) sent 13(LSA: 16)
LS-Ack received 13 sent 8, Discarded 0
```

配置 MD5 认证后会生成认证序列号 (Crypt Sequence Number) ; 简单文本认证时, 不会生成该序列号。

说明:

- 配置 OSPF 认证时，可以只配置区域认证或者只配置接口认证，也可以同时配置区域认证和接口认证。
- 区域认证和接口认证同时配置时，接口认证优先生效。

41.3.3 配置 OSPF 路由重分发

-S -E -A

网络需求

- Device1 和 Device2 之间运行 OSPF 协议，Device2 和 Device3 之间运行 RIPv2 协议。
- Device2 将 RIP 路由重分发到 OSPF 中，并采用路由策略控制只重分发 100.0.0.0/24 这条路由。

网络拓扑

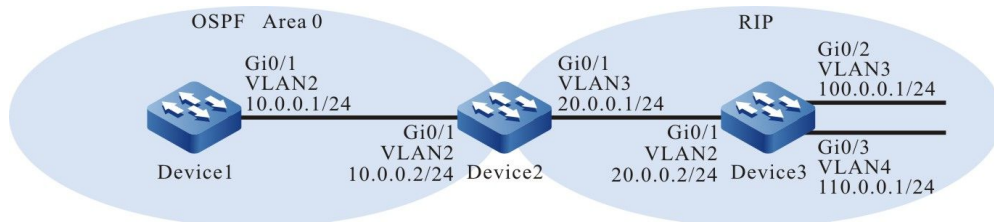


图 41-3 配置 OSPF 路由重分发组网图

配置步骤

- 步骤 1：配置 VLAN，并将端口加入对应的 VLAN。（略）
- 步骤 2：配置各接口 IP 地址。（略）
- 步骤 3：配置 Device 1 和 Device 2 的 OSPF 协议；配置 Device2 和 Device 3 的 RIPv2 协议。

#配置 Device1 的 OSPF 协议。

配置手册

发布 1.1 04/2020

单播路由

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#router-id 1.1.1.1
Device1(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#配置 Device2 的 OSPF 协议和 RIPv2 协议。

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#router-id 2.2.2.2
Device2(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
Device2(config)#router rip
Device2(config-rip)#version 2
Device2(config-rip)#network 20.0.0.0
Device2(config-rip)#exit
```

#配置 Device3 的 RIPv2 协议。

```
Device3#configure terminal
Device3(config)#router rip
Device3(config-rip)#version 2
Device3(config-rip)#network 20.0.0.0
Device3(config-rip)#network 100.0.0.0
Device3(config-rip)#network 110.0.0.0
Device3(config-rip)#exit
```

#查看 Device1 的 OSPF 邻居信息。

```
Device1#show ip ospf neighbor
OSPF process 100:
Neighbor ID  Pri  State           Dead Time  Address      Interface
2.2.2.2      1  Full/DR        00:00:32  10.0.0.2    vlan2
```

#查看 Device2 的 OSPF 邻居信息。

```
Device2#show ip ospf neighbor
OSPF process 100:
Neighbor ID  Pri  State           Dead Time  Address      Interface
1.1.1.1      1  Full/Backup    00:00:32  10.0.0.1    vlan2
```

#查看 Device2 的路由表。

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C 10.0.0.0/24 is directly connected, 00:21:17, vlan2
C 20.0.0.0/24 is directly connected, 00:21:33, vlan3
R 100.0.0.0/24 [120/1] via 20.0.0.2, 00:10:58, vlan3
R 110.0.0.0/24 [120/1] via 20.0.0.2, 00:10:58, vlan3
C 127.0.0.0/8 is directly connected, 30:20:17, lo0
```

Device2 上学到了 RIP 路由。

步骤 4: 配置路由策略。

#配置 Device2。

单播路由

```
Device2(config)#ip access-list standard 1
Device2(config-std-nacl)#permit 100.0.0.0 0.0.0.255
Device2(config-std-nacl)#exit
Device2(config)#route-map RIPtoOSPF
Device2(config-route-map)#match ip address 1
Device2(config-route-map)#exit
```

配置 route-map 调用 ACL 只匹配 100.0.0.0/24，而其它网段将被过滤掉，如 20.0.0.0/24 和 110.0.0.0/24。

步骤 5： 配置 OSPF 重分发 RIP 路由，并关联路由策略。

#配置 Device2。

```
Device2(config)#router ospf 100
Device2(config-ospf)#redistribute rip route-map RIPtoOSPF
Device2(config-ospf)#exit
```

重分发 RIP 路由时，调用 route-map 的匹配规则进行过滤。

步骤 6： 检验结果。

#查看 Device1 的路由表。

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C 10.0.0.0/24 is directly connected, 00:47:27, vlan2
OE 100.0.0.0/24 [150/20] via 10.0.0.2, 00:21:39, vlan2
C 127.0.0.0/8 is directly connected, 21:40:06, lo0
```

Device1 的路由表中只学到了 100.0.0.0/24 这条 OSPF 外部路由，而 20.0.0.0/24 和 110.0.0.0/24 这 2 条路由则被过滤掉了。

#查看 Device2 的 OSPF 进程信息及数据库。

```
Device2#show ip ospf 100
Routing Process "ospf 100" with ID 2.2.2.2
Process bound to VRF default
Process uptime is 1 hour 4 minutes
IETF NSF restarter support disabled
IETF NSF helper support enabled
Conforms to RFC2328, and RFC1583Compatibility flag is disabled
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Graceful Restart
This router is an ASBR (injecting external routing information)
Initial SPF schedule delay 5000 msec
Minimum hold time between two consecutive SPF 10000 msec
Maximum wait time between two consecutive SPF 10000 msec
Refresh timer 10 secs
Number of external LSA 2. Checksum Sum 0x0161F5
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of non-default external LSA is 2
External LSA database is unlimited.
```

```
Not Support Demand Circuit lsa number is 0, autonomy system support flood DoNotAge Lsa
Number of areas attached to this router: 1
Area 0 (BACKBONE)    Number of interfaces in this area is 1(1)
Number of fully adjacent neighbors in this area is 1
Number of fully adjacent sham-link neighbors in this area is 0
Area has no authentication
SPF algorithm last executed 00:37:52.833 ago
SPF algorithm executed 3 times
Number of LSA 3. Checksum Sum 0x00e746
Not Support Demand Circuit lsa number is 0,
Indication lsa (by other routers) number is: 0,
Area support flood DoNotAge Lsa
```

```
Device2#show ip ospf 100 database
```

```
OSPF Router with ID (2.2.2.2) (Process ID 100)

Router Link States (Area 0)

Link ID      ADV Router   Age Seq#     CkSum Link count
1.1.1.1      1.1.1.1      191 0x80000004 0x70a0 1
2.2.2.2      2.2.2.2      537 0x80000005 0x36ce 1

Net Link States (Area 0)

Link ID      ADV Router   Age Seq#     CkSum
10.0.0.2     2.2.2.2      818 0x80000003 0x3fd8

AS External Link States

Link ID      ADV Router   Age Seq#     CkSum Route
100.0.0.0    2.2.2.2      718 0x80000002 0x72be E2 100.0.0.0/24 [0x0]
```

从 OSPF 100 进程信息看到 Device2 的角色已经变成了 ASBR，且数据库中只产生了一条外部 LSA。

说明：

- 在实际应用中，如果自治系统边界路由器有 2 台及以上，建议不要直接在不同路由协议之间相互重分发路由，若必须配置时，需要配置路由策略，防止产生路由环路。
-

41.3.4 配置 OSPF 多进程 **-S -E -A**

网络需求

- 所有设备运行 OSPF 协议，Device2 上启用两个 OSPF 进程；Device1 与 Device2 的 OSPF 100 进程建立邻居；Device3 与 Device2 的 OSPF 200 进程建立邻居。
- Device2 上两个 OSPF 进程相互重分发路由，OSPF 100 进程采用路由策略控制只重分发 110.0.0.0/24 这条路由；OSPF 200 进程采用路由策略控制只重分发

100.0.0.0/24 这条路由。

网络拓扑

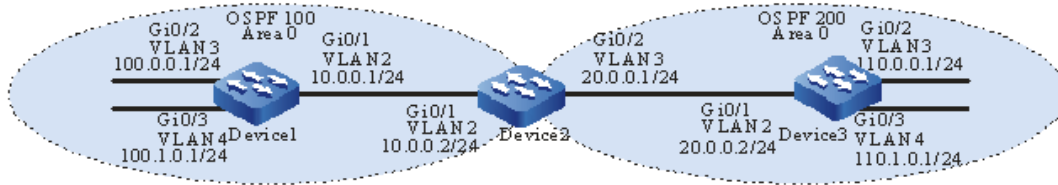


图 41-4 配置 OSPF 多进程组网图

配置步骤

- 步骤 1: 配置 VLAN, 并将端口加入对应的 VLAN。 (略)
- 步骤 2: 配置各接口 IP 地址。 (略)
- 步骤 3: 配置 OSPF 协议。

#配置 Device1。

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#router-id 1.1.1.1
Device1(config-ospf)#network 100.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 100.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 100.1.0.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#配置 Device2, 分别创建 2 个 OSPF 进程, 进程 100 和进程 200。

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#router-id 2.2.2.2
Device2(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
Device2(config)#router ospf 200
Device2(config-ospf)#router-id 2.2.2.3
Device2(config-ospf)#network 20.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#配置 Device3。

```
Device3#configure terminal
Device3(config)#router ospf 200
Device3(config-ospf)#router-id 3.3.3.3
Device3(config-ospf)#network 20.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 110.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 110.1.0.0 0.0.0.255 area 0
Device3(config-ospf)#exit
```

说明：

- 存在多个 OSPF 进程时，建议 OSPF 进程间配置不同的 Router ID，避免产生 Router ID 冲突的隐患。

#查看 Device2 LSDB 和邻居信息。

```
Device2#show ip ospf neighbor
OSPF process 100:
Neighbor ID Pri State Dead Time Address Interface
1.1.1.1 1 Full/Backup 00:00:30 10.0.0.1 vlan2
OSPF process 200:
Neighbor ID Pri State Dead Time Address Interface
3.3.3.3 1 Full/DR 00:00:33 20.0.0.2 vlan3

Device2#show ip ospf database

OSPF Router with ID (2.2.2.2) (Process ID 100)

Router Link States (Area 0)

Link ID ADV Router Age Seq# CkSum Link count
1.1.1.1 1.1.1.1 19 0x80000016 0x53bf 3
2.2.2.2 2.2.2.2 15 0x80000010 0x1ae1 1

Net Link States (Area 0)

Link ID ADV Router Age Seq# CkSum
10.0.0.2 2.2.2.2 21 0x80000001 0x43d6

OSPF Router with ID (2.2.2.3) (Process ID 200)

Router Link States (Area 0)

Link ID ADV Router Age Seq# CkSum Link count
2.2.2.3 2.2.2.3 14 0x8000000f 0xb235 1
3.3.3.3 3.3.3.3 15 0x8000001b 0x696b 3

Net Link States (Area 0)

Link ID ADV Router Age Seq# CkSum
20.0.0.2 3.3.3.3 15 0x80000002 0x03fe
```

Device2 的 OSPF 进程 100 和进程 200 分别建立了邻接关系，且单独拥有 OSPF 数据库。

#查看 Device2 的 OSPF 路由表。

```
Device2#show ip ospf route
OSPF process 100:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2

O 10.0.0.0/24 [1] is directly connected, vlan2, Area 0
O 100.0.0.0/24 [2] via 10.0.0.1, vlan2, Area 0
O 100.1.0.0/24 [2] via 10.0.0.1, vlan2, Area 0
```

单播路由

```
OSPF process 200:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

O 20.0.0.0/24 [1] is directly connected, vlan3, Area 0
O 110.0.0.0/24 [2] via 20.0.0.2, vlan3, Area 0
O 110.1.0.0/24 [2] via 20.0.0.2, vlan3, Area 0
```

OSPF 进程 100 和进程 200 分别计算出了各自的路由。

#查看 Device2 的路由表。

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C 10.0.0.0/24 is directly connected, 00:05:34, vlan2
C 20.0.0.0/24 is directly connected, 00:05:28, vlan3
O 100.0.0.0/24 [110/2] via 10.0.0.1, 00:04:42, vlan2
O 100.1.0.0/24 [110/2] via 10.0.0.1, 00:04:42, vlan2
O 110.0.0.0/24 [110/2] via 20.0.0.2, 00:04:41, vlan3
O 110.1.0.0/24 [110/2] via 20.0.0.2, 00:04:41, vlan3
C 127.0.0.0/8 is directly connected, 48:40:33, lo0
```

步骤 4： 配置路由策略。

#配置 Device2。

```
Device2(config)#ip prefix-list 1 permit 110.0.0.0/24
Device2(config)#ip prefix-list 2 permit 100.0.0.0/24
Device2(config)#route-map OSPF200to100
Device2(config-route-map)#match ip address prefix-list 1
Device2(config-route-map)#exit
Device2(config)#route-map OSPF100to200
Device2(config-route-map)#match ip address prefix-list 2
Device2(config-route-map)#exit
```

配置 route-map 分别调用前缀列表 1 和 2，匹配 110.0.0.0/24 网段和 100.0.0.0/24 网段。

说明：

- 配置路由策略时，前缀列表和 ACL 都可以创建过滤规则，它们的区别在于前缀列表可以精确匹配路由掩码，而 ACL 则不能匹配路由掩码。
-

步骤 5： 配置 OSPF 进程间相互重分发路由，并关联路由策略。

#配置 Device2。

```
Device2(config)#router ospf 100
Device2(config-ospf)#redistribute ospf 200 route-map OSPF200to100
Device2(config-ospf)#exit
Device2(config)#router ospf 200
Device2(config-ospf)#redistribute ospf 100 route-map OSPF100to200
Device2(config-ospf)#exit
```

步骤 6: 检验结果。

#查看 Device2 的 OSPF LSDB。

```
Device2#show ip ospf database

      OSPF Router with ID (2.2.2.2) (Process ID 100)

      Router Link States (Area 0)

Link ID      ADV Router   Age Seq#     CkSum Link count
1.1.1.1      1.1.1.1     1663 0x80000016 0x53bf 3
2.2.2.2      2.2.2.2     216 0x80000011 0x1eda 1

      Net Link States (Area 0)

Link ID      ADV Router   Age Seq#     CkSum
10.0.0.2     2.2.2.2     1664 0x80000001 0x43d6

      AS External Link States

Link ID      ADV Router   Age Seq#     CkSum Route
110.0.0.0    2.2.2.2     216 0x80000001 0x3dfc E2 110.0.0.0/24 [0x0]

      OSPF Router with ID (2.2.2.3) (Process ID 200)

      Router Link States (Area 0)

Link ID      ADV Router   Age Seq#     CkSum Link count
2.2.2.3      2.2.2.3     205 0x80000010 0xb62e 1
3.3.3.3      3.3.3.3     1658 0x8000001b 0x696b 3

      Net Link States (Area 0)

Link ID      ADV Router   Age Seq#     CkSum
20.0.0.2     3.3.3.3     1658 0x80000002 0x03fe

      AS External Link States

Link ID      ADV Router   Age Seq#     CkSum Route
100.0.0.0    2.2.2.3     205 0x80000001 0xb989 E2 100.0.0.0/24 [0x0]
```

可以看出，OSPF 进程 100 只有 110.0.0.0/24 这条外部路由的 LSA，其它路由 110.1.0.0/24、20.0.0.0/24 被路由策略 OSPF200to100 过滤掉了；同样，OSPF 进程 200 中只有 100.0.0.0/24 这条外部路由 LSA，其他路由 100.1.0.0/24、10.0.0.0/24 被路由策略 OSPF100to200 过滤掉了。

#查看 Device1 的路由表。

```
Device1#show ip route
```

单播路由

Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

```
C 10.0.0.0/24 is directly connected, 00:40:20, vlan2
C 100.0.0.0/24 is directly connected, 03:11:36, vlan3
C 100.1.0.0/24 is directly connected, 01:00:22, vlan4
OE 110.0.0.0/24 [150/2] via 10.0.0.2, 00:15:27, vlan2
C 127.0.0.0/8 is directly connected, 97:08:23, lo0
```

Device1 只学到了 110.0.0.0/24 路由。

#查看 Device3 的路由表。

```
Device3#show ip route
```

Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

```
C 20.0.0.0/24 is directly connected, 00:42:44, vlan2
OE 100.0.0.0/24 [150/2] via 20.0.0.1, 00:17:45, vlan2
C 110.0.0.0/24 is directly connected, 01:02:03, vlan3
C 110.1.0.0/24 is directly connected, 01:02:14, vlan4
C 127.0.0.0/8 is directly connected, 41:02:01, lo0
```

Device3 只学到了 100.0.0.0/24 路由。

说明：

- 在实际应用中，如果自治系统边界路由器有 2 台及以上，建议不要直接在不同的 OSPF 进程间相互重分发路由，若必须配置时，需要配置路由过滤策略，防止产生路由环路。
-

41.3.5 配置 OSPF 外部路由汇总 **-S -E -A**

网络需求

- Device1 和 Device2 之间运行 OSPF 协议，Device2 和 Device3 之间运行 RIPv2 协议。
- Device2 将 RIP 路由重分发到 OSPF，为减少 Device1 上的路由数量，在 ASBR 上将重分发的 RIP 路由做汇总，汇总为 20.0.0.0/16。

网络拓扑

单播路由

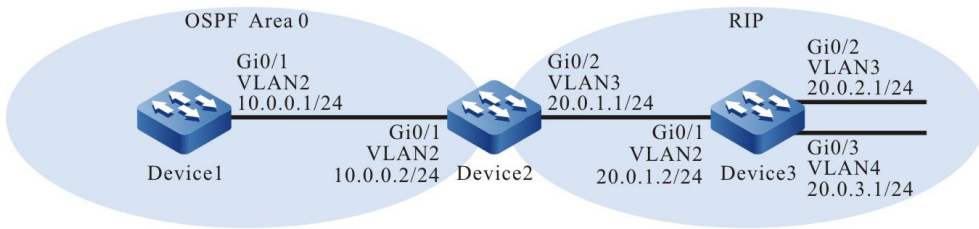


图 41-5 配置 OSPF 外部路由汇总组网图

配置步骤

- 步骤 1: 配置 VLAN, 并将端口加入对应的 VLAN。 (略)
- 步骤 2: 配置各接口 IP 地址。 (略)
- 步骤 3: 配置 OSPF 协议和 RIPv2 协议。

#配置 Device1 的 OSPF 协议。

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#router-id 1.1.1.1
Device1(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#配置 Device2 的 OSPF 协议和 RIPv2 协议。

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#router-id 2.2.2.2
Device2(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
Device2(config)#router rip
Device2(config-rip)#version 2
Device2(config-rip)#network 20.0.0.0
Device2(config-rip)#exit
```

#配置 Device3 的 RIPv2 协议。

```
Device3#configure terminal
Device3(config)#router rip
Device3(config-rip)#version 2
Device3(config-rip)#network 20.0.0.0
Device3(config-rip)#exit
```

#查看 Device2 的路由表。

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C 10.0.0.0/24 is directly connected, 00:15:46, vlan2
C 20.0.1.0/24 is directly connected, 00:15:23, vlan3
R 20.0.2.0/24 [120/1] via 20.0.1.2, 00:12:17, vlan3
```

单播路由

```
R 20.0.3.0/24 [120/1] via 20.0.1.2, 00:12:06, vlan3
C 127.0.0.0/8 is directly connected, 03:34:27, lo0
```

步骤 4: 配置 OSPF 重分发 RIP 路由。

#配置 Device2。

```
Device2(config)#router ospf 100
Device2(config-ospf)#redistribute rip
Device2(config-ospf)#exit
```

#查看 Device2 的 OSPF LSDB。

```
Device2#show ip ospf database

        OSPF Router with ID (2.2.2.2) (Process ID 100)

        Router Link States (Area 0)

Link ID      ADV Router   Age Seq#     CkSum Link count
1.1.1.1      1.1.1.1     1071 0x80000003 0x729f 1
2.2.2.2      2.2.2.2     873 0x80000004 0x38cd 1

        Net Link States (Area 0)

Link ID      ADV Router   Age Seq#     CkSum
10.0.0.2     2.2.2.2     1070 0x80000001 0x43d6

        AS External Link States

Link ID      ADV Router   Age Seq#     CkSum Route
20.0.1.0     2.2.2.2     365 0x80000001 0x7d04 E2 20.0.1.0/24 [0x0]
20.0.2.0     2.2.2.2     365 0x80000001 0x720e E2 20.0.2.0/24 [0x0]
20.0.3.0     2.2.2.2     365 0x80000001 0x6718 E2 20.0.3.0/24 [0x0]
```

从 OSPF 数据库中可以看到，已经产生了 3 条外部 LSA，表明 RIP 路由已经重分发到 OSPF 中。

#查看 Device1 的路由表。

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C 10.0.0.0/24 is directly connected, 00:56:40, vlan2
OE 20.0.1.0/24 [150/20] via 10.0.0.2, 00:02:40, vlan2
OE 20.0.2.0/24 [150/20] via 10.0.0.2, 00:02:40, vlan2
OE 20.0.3.0/24 [150/20] via 10.0.0.2, 00:02:40, vlan2
C 127.0.0.0/8 is directly connected, 115:12:28, lo0
```

Device1 学习到了重分发的 RIP 路由。

步骤 5: ASBR 上配置 OSPF 外部路由汇总，此时 Device2 为 ASBR。

#配置 Device2，将重分发的 RIP 路由汇总为 20.0.0.0/16。

单播路由

```
Device2(config)#router ospf 100
Device2(config-ospf)#summary-address 20.0.0.0 255.255.0.0
Device2(config-ospf)#exit
```

步骤 6: 检验结果。

#查看 Device2 的 OSPF LSDB。

```
Device2#show ip ospf database

      OSPF Router with ID (2.2.2.2) (Process ID 100)

      Router Link States (Area 0)

Link ID      ADV Router   Age Seq#      CkSum Link count
1.1.1.1      1.1.1.1     1437 0x80000003 0x729f 1
2.2.2.2      2.2.2.2     1240 0x80000004 0x38cd 1

      Net Link States (Area 0)

Link ID      ADV Router   Age Seq#      CkSum
10.0.0.2     2.2.2.2     144 0x80000002 0x41d7

      AS External Link States

Link ID      ADV Router   Age Seq#      CkSum Route
20.0.0.0     2.2.2.2     84 0x80000001 0x88f9 E2 20.0.0.0/16 [0x0]
```

对比步骤 3 可以看到，数据库中原来产生的 3 条外部 LSA 已经被删除了，重新生成了一条汇总后的外部 LSA。

#查看 Device2 的路由表。

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C 10.0.0.0/24 is directly connected, 00:28:03, vlan2
O 20.0.0.0/16 [110/1] is directly connected, 00:04:48, null0
C 20.0.1.0/24 is directly connected, 00:27:40, vlan3
R 20.0.2.0/24 [120/1] via 20.0.1.2, 00:24:34, vlan3
R 20.0.3.0/24 [120/1] via 20.0.1.2, 00:24:23, vlan3
C 127.0.0.0/8 is directly connected, 03:46:44, lo0
```

说明：

- 在 Device2 的路由表中会自动添加一条出接口指向 Null0 的汇总路由 20.0.0.0/16，该路由可以避免产生环路。
-

单播路由

#查看 Device1 的路由表。

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C 10.0.0.0/24 is directly connected, 00:58:40, vlan2
OE 20.0.0.0/16 [150/20] via 10.0.0.2, 00:15:26, vlan2
C 127.0.0.0/8 is directly connected, 115:17:28, lo0
```

Device1 的路由表中只会学到 20.0.0.0/16 这条汇总后的路由。

41.3.6 配置 OSPF 区域间路由汇总

-S -E -A

网络需求

- 所有设备配置 OSPF 协议，划分区域 0 和区域 1 两个区域。
- 为减少区域间路由数量，在 ABR 上做区域间路由汇总，将区域 0 路由汇总为 10.0.0.0/16；将区域 1 路由汇总为 20.0.0.0/16。

网络拓扑

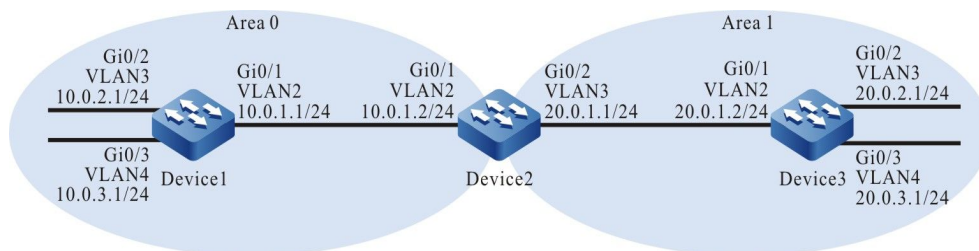


图 41-6 配置 OSPF 区域间路由汇总组网图

配置步骤

- 步骤 1：配置 VLAN，并将端口加入对应的 VLAN。（略）
- 步骤 2：配置各接口 IP 地址。（略）
- 步骤 3：配置 OSPF 进程并将相应的接口覆盖到不同区域中。

#配置 Device1。

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#router-id 1.1.1.1
Device1(config-ospf)#network 10.0.1.0 0.0.0.255 area 0
```

配置手册

发布 1.1 04/2020

单播路由

```
Device1(config-ospf)#network 10.0.2.0 0.0.0.255 area 0
Device1(config-ospf)#network 10.0.3.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#配置 Device2。

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#router-id 2.2.2.2
Device2(config-ospf)#network 10.0.1.0 0.0.0.255 area 0
Device2(config-ospf)#network 20.0.1.0 0.0.0.255 area 1
Device2(config-ospf)#exit
```

#配置 Device3。

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#router-id 3.3.3.3
Device3(config-ospf)#network 20.0.1.0 0.0.0.255 area 1
Device3(config-ospf)#network 20.0.2.0 0.0.0.255 area 1
Device3(config-ospf)#network 20.0.3.0 0.0.0.255 area 1
Device3(config-ospf)#exit
```

#查看 Device2 的 OSPF LSDB 和路由表。

```
Device2#show ip ospf database

      OSPF Router with ID (2.2.2.2) (Process ID 100)

      Router Link States (Area 0)

Link ID      ADV Router   Age Seq#     CkSum Link count
1.1.1.1      1.1.1.1     1419 0x80000007 0x4f81 3
2.2.2.2      2.2.2.2     1414 0x80000004 0x4bb9 1

      Net Link States (Area 0)

Link ID      ADV Router   Age Seq#     CkSum
10.0.1.2     2.2.2.2     1419 0x80000001 0x38e0

      Summary Link States (Area 0)

Link ID      ADV Router   Age Seq#     CkSum Route
20.0.1.0     2.2.2.2     1437 0x80000001 0x47d7 20.0.1.0/24
20.0.2.0     2.2.2.2     1363 0x80000001 0x46d6 20.0.2.0/24
20.0.3.0     2.2.2.2     1363 0x80000001 0x3be0 20.0.3.0/24

      Router Link States (Area 1)

Link ID      ADV Router   Age Seq#     CkSum Link count
2.2.2.2      2.2.2.2     1368 0x80000004 0xe70b 1
3.3.3.3      3.3.3.3     1341 0x80000006 0x6138 3

      Net Link States (Area 1)

Link ID      ADV Router   Age Seq#     CkSum
20.0.1.1     2.2.2.2     1368 0x80000001 0x24e3

      Summary Link States (Area 1)

Link ID      ADV Router   Age Seq#     CkSum Route
10.0.1.0     2.2.2.2     1442 0x80000001 0xc95f 10.0.1.0/24
10.0.2.0     2.2.2.2     1409 0x80000001 0xc85e 10.0.2.0/24
10.0.3.0     2.2.2.2     1409 0x80000001 0xbd68 10.0.3.0/24

Device2#show ip route
```

单播路由

Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

```
C 10.0.1.0/24 is directly connected, 00:30:31, vlan2
O 10.0.2.0/24 [110/2] via 10.0.1.1, 00:23:37, vlan2
O 10.0.3.0/24 [110/2] via 10.0.1.1, 00:23:37, vlan2
C 20.0.1.0/24 is directly connected, 02:09:10, vlan3
O 20.0.2.0/24 [110/2] via 20.0.1.2, 00:22:51, vlan3
O 20.0.3.0/24 [110/2] via 20.0.1.2, 00:22:51, vlan3
C 127.0.0.0/8 is directly connected, 05:28:14, lo0
```

Device2 的 OSPF 数据库中区域 0 和区域 1 中分别生成了 3 条区域间 LSA。各区域的区域内路由也加入到了路由表中。

#查看 Device1 的 OSPF LSDB 和路由表。

```
Device1#show ip ospf database
```

```
OSPF Router with ID (1.1.1.1) (Process ID 100)
```

```
Router Link States (Area 0)
```

Link ID	ADV Router	Age	Seq#	CkSum	Link count
1.1.1.1	1.1.1.1	249	0x80000008	0x4d82	3
2.2.2.2	2.2.2.2	191	0x80000005	0x49ba	1

```
Net Link States (Area 0)
```

Link ID	ADV Router	Age	Seq#	CkSum
10.0.1.2	2.2.2.2	471	0x80000002	0x36e1

```
Summary Link States (Area 0)
```

Link ID	ADV Router	Age	Seq#	CkSum	Route
20.0.1.0	2.2.2.2	251	0x80000002	0x45d8	20.0.1.0/24
20.0.2.0	2.2.2.2	1988	0x80000001	0x46d6	20.0.2.0/24
20.0.3.0	2.2.2.2	1988	0x80000001	0x3be0	20.0.3.0/24

```
Device1#show ip route
```

Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

```
C 10.0.1.0/24 is directly connected, 00:25:11, vlan2
C 10.0.2.0/24 is directly connected, 00:24:58, vlan3
C 10.0.3.0/24 is directly connected, 00:24:44, vlan4
O 20.0.1.0/24 [110/2] via 10.0.1.2, 00:14:59, vlan2
O 20.0.2.0/24 [110/3] via 10.0.1.2, 00:14:12, vlan2
O 20.0.3.0/24 [110/3] via 10.0.1.2, 00:14:12, vlan2
C 127.0.0.0/8 is directly connected, 116:19:42, lo0
```

Device1 的 OSPF 数据库中不存在 3 条区域间 LSA，路由表中也加入了这 3 条路由。

#查看 Device3 的 OSPF LSDB 和路由表。

```
Device3#show ip ospf database
```

```
OSPF Router with ID (3.3.3.3) (Process ID 100)
```

```
Router Link States (Area 1)
```

Link ID	ADV Router	Age	Seq#	CkSum	Link count
---------	------------	-----	------	-------	------------

单播路由

```
2.2.2.2 2.2.2.2 532 0x80000005 0xe50c 1
3.3.3.3 3.3.3.3 506 0x80000007 0x5f39 3
```

Net Link States (Area 1)

```
Link ID    ADV Router  Age Seq#    CkSum
20.0.1.1  2.2.2.2    532 0x80000002 0x22e4
```

Summary Link States (Area 1)

```
Link ID    ADV Router  Age Seq#    CkSum  Route
10.0.1.0  2.2.2.2    82 0x80000002 0xc760 10.0.1.0/24
10.0.2.0  2.2.2.2    382 0x80000002 0xc65f 10.0.2.0/24
10.0.3.0  2.2.2.2    262 0x80000002 0xbb69 10.0.3.0/24
```

```
Device3#show ip route
```

```
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
        D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS
```

```
Gateway of last resort is not set
```

```
O 10.0.1.0/24 [110/2] via 20.0.1.1, 00:24:04, vlan2
O 10.0.2.0/24 [110/3] via 20.0.1.1, 00:24:04, vlan2
O 10.0.3.0/24 [110/3] via 20.0.1.1, 00:24:04, vlan2
C 20.0.1.0/24 is directly connected, 02:09:51, vlan2
C 20.0.2.0/24 is directly connected, 02:07:21, vlan3
C 20.0.3.0/24 is directly connected, 02:07:09, vlan4
C 127.0.0.0/8 is directly connected, 360:20:45, lo0
```

同样，在 Device3 的 OSPF 数据库中存在 3 条区域间 LSA，路由表中也加入了这 3 条路由。

步骤 4： 在 ABR 上配置区域间路由汇总，此时 Device2 为 ABR。

#配置 Device2，将区域 0 路由汇总为 10.0.0.0/16，区域 1 路由汇总为 20.0.0.0/16。

```
Device2(config)#router ospf 100
Device2(config-ospf)#area 0 range 10.0.0.0/16
Device2(config-ospf)#area 1 range 20.0.0.0/16
Device2(config-ospf)#exit
```

步骤 5： 检验结果。

#查看 Device2 的 OSPF LSDB 和路由表。

```
Device2#show ip ospf database
```

```
OSPF Router with ID (2.2.2.2) (Process ID 100)
```

Router Link States (Area 0)

```
Link ID    ADV Router  Age Seq#    CkSum  Link count
1.1.1.1    1.1.1.1    305 0x80000009 0x4b83 3
2.2.2.2    2.2.2.2    297 0x80000006 0x47bb 1
```

Net Link States (Area 0)

```
Link ID    ADV Router  Age Seq#    CkSum
10.0.1.2  2.2.2.2    527 0x80000003 0x34e2
```

单播路由

```
Summary Link States (Area 0)

Link ID    ADV Router  Age Seq#    CkSum Route
20.0.0.0   2.2.2.2     23 0x80000001 0x52cd 20.0.0.0/16

Router Link States (Area 1)

Link ID    ADV Router  Age Seq#    CkSum Link count
2.2.2.2    2.2.2.2     277 0x80000006 0xe30d 1
3.3.3.3    3.3.3.3     332 0x80000008 0x5d3a 3

Net Link States (Area 1)

Link ID    ADV Router  Age Seq#    CkSum
20.0.1.1   2.2.2.2     317 0x80000003 0x20e5

Summary Link States (Area 1)

Link ID    ADV Router  Age Seq#    CkSum Route
10.0.0.0   2.2.2.2     26 0x80000001 0xd455 10.0.0.0/16

Device2#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

O 10.0.0.0/16 [110/1] is directly connected, 00:00:31, null0
C 10.0.1.0/24 is directly connected, 00:40:31, vlan2
O 10.0.2.0/24 [110/2] via 10.0.1.1, 00:33:37, vlan2
O 10.0.3.0/24 [110/2] via 10.0.1.1, 00:33:37, vlan2
O 20.0.0.0/16 [110/1] is directly connected, 00:00:27, null0
C 20.0.1.0/24 is directly connected, 02:19:10, vlan3
O 20.0.2.0/24 [110/2] via 20.0.1.2, 00:32:51, vlan3
O 20.0.3.0/24 [110/2] via 20.0.1.2, 00:32:51, vlan3
C 127.0.0.0/8 is directly connected, 05:38:14, lo0
```

对比步骤 2 可以看到，Device2 的 OSPF 数据库中区域 0 和区域 1 中各自只生成了 1 条汇总后的区域间 LSA。同样，路由表中会自动加入指向 Null0 接口的汇总路由。

#查看 Device1 的 OSPF LSDB 和路由表。

```
Device1#show ip ospf database

OSPF Router with ID (1.1.1.1) (Process ID 100)

Router Link States (Area 0)

Link ID    ADV Router  Age Seq#    CkSum Link count
1.1.1.1    1.1.1.1     1338 0x80000009 0x4b83 3
2.2.2.2    2.2.2.2     1332 0x80000006 0x47bb 1

Net Link States (Area 0)

Link ID    ADV Router  Age Seq#    CkSum
10.0.1.2   2.2.2.2     1563 0x80000003 0x34e2

Summary Link States (Area 0)

Link ID    ADV Router  Age Seq#    CkSum Route
20.0.0.0   2.2.2.2     90 0x80000001 0x52cd 20.0.0.0/16

Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS
```

Gateway of last resort is not set

```
C 10.0.1.0/24 is directly connected, 00:40:11, vlan2
C 10.0.2.0/24 is directly connected, 00:39:58, vlan3
C 10.0.3.0/24 is directly connected, 00:39:44, vlan4
O 20.0.0.0/16 [110/2] via 10.0.1.2, 00:02:18, vlan2
C 127.0.0.0/8 is directly connected, 116:44:42, lo0
```

在 Device1 上可以看到，OSPF 数据库中也只有汇总后的区域间 LSA，路由表中也只会学到区域 1 汇总后的路由 20.0.0.0/16；同样，Device3 上也只会学到区域 0 汇总后的路由 10.0.0.0/16。

41.3.7 配置 OSPF 区域间路由过滤

-S -E -A

网络需求

- 所有设备配置 OSPF 协议，划分区域 0 和区域 1 两个区域。
- 在 ABR 上做区域间路由过滤，区域 0 不允许路由 20.0.3.0/24 注入，同时也不允许路由 10.0.3.0/24 洪泛到其他区域。

网络拓扑

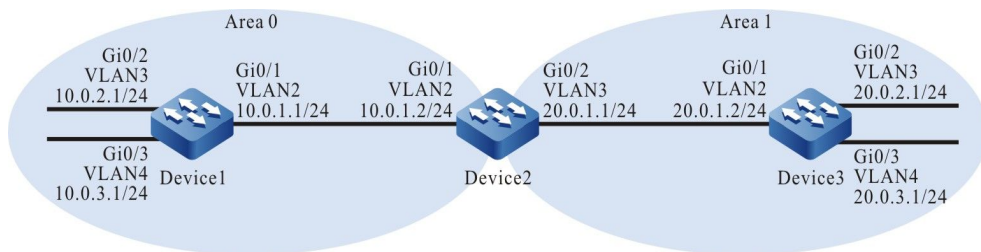


图 41-7 配置 OSPF 区域间路由过滤组网图

配置步骤

步骤 1：配置 VLAN，并将端口加入对应的 VLAN。（略）

步骤 2：配置各接口 IP 地址。（略）

步骤 3：配置 OSPF 进程并将相应接口覆盖到不同区域中。

#配置 Device1。

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#router-id 1.1.1.1
Device1(config-ospf)#network 10.0.1.0 0.0.0.255 area 0
Device1(config-ospf)#network 10.0.2.0 0.0.0.255 area 0
Device1(config-ospf)#network 10.0.3.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

单播路由

#配置 Device2.

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#router-id 2.2.2.2
Device2(config-ospf)#network 10.0.1.0 0.0.0.255 area 0
Device2(config-ospf)#network 20.0.1.0 0.0.0.255 area 1
Device2(config-ospf)#exit
```

#配置 Device3.

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#router-id 3.3.3.3
Device3(config-ospf)#network 20.0.1.0 0.0.0.255 area 1
Device3(config-ospf)#network 20.0.2.0 0.0.0.255 area 1
Device3(config-ospf)#network 20.0.3.0 0.0.0.255 area 1
Device3(config-ospf)#exit
```

#查看 Device2 的 OSPF LSDB 和路由表。

```
Device2#show ip ospf database
```

```
OSPF Router with ID (2.2.2.2) (Process ID 100)
```

```
Router Link States (Area 0)
```

Link ID	ADV Router	Age	Seq#	CkSum	Link count
1.1.1.1	1.1.1.1	329	0x8000005b	0xa6d5	3
2.2.2.2	2.2.2.2	324	0x80000051	0xb007	1

```
Net Link States (Area 0)
```

Link ID	ADV Router	Age	Seq#	CkSum
10.0.1.2	2.2.2.2	324	0x8000004e	0x9d2e

```
Summary Link States (Area 0)
```

Link ID	ADV Router	Age	Seq#	CkSum	Route
20.0.1.0	2.2.2.2	324	0x8000004e	0xac25	20.0.1.0/24
20.0.2.0	2.2.2.2	324	0x8000004d	0xad23	20.0.2.0/24
20.0.3.0	2.2.2.2	259	0x80000001	0x3be0	20.0.3.0/24

```
Router Link States (Area 1)
```

Link ID	ADV Router	Age	Seq#	CkSum	Link count
2.2.2.2	2.2.2.2	334	0x80000055	0x4f51	1
3.3.3.3	3.3.3.3	335	0x80000059	0xca7a	3

```
Net Link States (Area 1)
```

Link ID	ADV Router	Age	Seq#	CkSum
20.0.1.2	3.3.3.3	340	0x80000001	0xeb17

```
Summary Link States (Area 1)
```

Link ID	ADV Router	Age	Seq#	CkSum	Route
10.0.1.0	2.2.2.2	365	0x80000001	0xc95f	10.0.1.0/24
10.0.2.0	2.2.2.2	319	0x80000001	0xc85e	10.0.2.0/24
10.0.3.0	2.2.2.2	256	0x80000001	0xbd68	10.0.3.0/24

```
Device2#show ip route
```

```
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management  
D - Redirect, E - IRMP, EX - IRMP external, o - SNRP, B - BGP, i-ISIS
```

```
Gateway of last resort is not set
```

单播路由

```
C 10.0.1.0/24 is directly connected, 00:06:13, vlan2
O 10.0.2.0/24 [110/2] via 10.0.1.1, 00:05:22, vlan2
O 10.0.3.0/24 [110/2] via 10.0.1.1, 00:05:22, vlan2
C 20.0.1.0/24 is directly connected, 00:06:19, vlan3
O 20.0.2.0/24 [110/2] via 20.0.1.2, 00:05:32, vlan3
O 20.0.3.0/24 [110/2] via 20.0.1.2, 00:05:32, vlan3
C 127.0.0.0/8 is directly connected, 94:42:22, lo0
```

Device2 的 OSPF 数据库中区域 0 和区域 1 中分别生成了 3 条区域间 LSA。各区域内路由也加入到了路由表中。

#查看 Device1 的路由表。

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C 10.0.1.0/24 is directly connected, 00:08:41, vlan2
C 10.0.2.0/24 is directly connected, 37:59:10, vlan3
C 10.0.3.0/24 is directly connected, 38:05:36, vlan4
O 20.0.1.0/24 [110/2] via 10.0.1.2, 00:07:55, vlan2
O 20.0.2.0/24 [110/3] via 10.0.1.2, 00:07:55, vlan2
O 20.0.3.0/24 [110/3] via 10.0.1.2, 00:06:50, vlan2
C 127.0.0.0/8 is directly connected, 70:07:32, lo0
```

Device1 学到了区域 1 的路由。

#查看 Device3 的路由表。

```
Device3#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

O 10.0.1.0/24 [110/2] via 20.0.1.1, 00:08:44, vlan2
O 10.0.2.0/24 [110/3] via 20.0.1.1, 00:08:33, vlan2
O 10.0.3.0/24 [110/3] via 20.0.1.1, 00:07:30, vlan2
C 20.0.1.0/24 is directly connected, 00:09:31, vlan2
C 20.0.2.0/24 is directly connected, 37:59:57, vlan3
C 20.0.3.0/24 is directly connected, 38:03:35, vlan4
C 127.0.0.0/8 is directly connected, 61:26:38, lo0
```

Device3 学到了区域 0 的路由。

步骤 4: 配置路由过滤策略。

#配置 Device2。

```
Device2(config)#ip prefix-list 1 deny 10.0.3.0/24
Device2(config)#ip prefix-list 1 permit 0.0.0.0/0 le 32
Device2(config)#ip prefix-list 2 deny 20.0.3.0/24
Device2(config)#ip prefix-list 2 permit 0.0.0.0/0 le 32
Device2(config)#exit
```

前缀列表 1 表示过滤 10.0.3.0/24 网络，允许其它所有网络；2 表示过滤 20.0.3.0/24 网络，允许其它所有网络。

步骤 5: 在 ABR 上配置区域间路由过滤, 调用前缀列表的匹配规则。

#配置 Device2。

```
Device2(config)#router ospf 100
Device2(config-ospf)#area 0 filter-list prefix 1 out
Device2(config-ospf)#area 0 filter-list prefix 2 in
Device2(config-ospf)#exit
```

步骤 6: 检验结果。

#查看 Device2 的 OSPF LSDB。

```
Device2#show ip ospf database

        OSPF Router with ID (2.2.2.2) (Process ID 100)

        Router Link States (Area 0)

Link ID   ADV Router   Age Seq#    CkSum Link count
1.1.1.1   1.1.1.1     679 0x8000005b 0xa6d5 3
2.2.2.2   2.2.2.2     673 0x80000051 0xb007 1

        Net Link States (Area 0)

Link ID   ADV Router   Age Seq#    CkSum
10.0.1.2  2.2.2.2     673 0x8000004e 0x9d2e

        Summary Link States (Area 0)

Link ID   ADV Router   Age Seq#    CkSum Route
20.0.1.0  2.2.2.2     673 0x8000004e 0xac25 20.0.1.0/24
20.0.2.0  2.2.2.2     673 0x8000004d 0xad23 20.0.2.0/24

        Router Link States (Area 1)

Link ID   ADV Router   Age Seq#    CkSum Link count
2.2.2.2   2.2.2.2     683 0x80000055 0x4f51 1
3.3.3.3   3.3.3.3     684 0x80000059 0xca7a 3

        Net Link States (Area 1)

Link ID   ADV Router   Age Seq#    CkSum
20.0.1.2  3.3.3.3     689 0x80000001 0xeb17

        Summary Link States (Area 1)

Link ID   ADV Router   Age Seq#    CkSum Route
10.0.1.0  2.2.2.2     714 0x80000001 0xc95f 10.0.1.0/24
10.0.2.0  2.2.2.2     668 0x80000001 0xc85e 10.0.2.0/24
```

对比步骤 2 的结果, OSPF 数据库中 20.0.3.0/24 网络的 LSA 已经从区域 0 中删除了, 同样, 10.0.3.0/24 网络的 LSA 已经从区域 1 中删除了。

#查看 Device1 的路由表。

单播路由

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C 10.0.1.0/24 is directly connected, 00:12:57, vlan2
C 10.0.2.0/24 is directly connected, 38:03:25, vlan3
C 10.0.3.0/24 is directly connected, 38:09:52, vlan4
O 20.0.1.0/24 [110/2] via 10.0.1.2, 00:12:11, vlan2
O 20.0.2.0/24 [110/3] via 10.0.1.2, 00:12:11, vlan2
C 127.0.0.0/8 is directly connected, 70:11:48, lo0
```

Device1 的路由表中已经不存在 20.0.3.0/24 这条路由了。

#查看 Device3 的路由表。

```
Device3#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

O 10.0.1.0/24 [110/2] via 20.0.1.1, 00:13:09, vlan2
O 10.0.2.0/24 [110/3] via 20.0.1.1, 00:12:58, vlan2
C 20.0.1.0/24 is directly connected, 00:13:56, vlan2
C 20.0.2.0/24 is directly connected, 38:04:22, vlan3
C 20.0.3.0/24 is directly connected, 38:08:00, vlan4
C 127.0.0.0/8 is directly connected, 64:31:03, lo0
```

Device3 的路由表中也不存在 10.0.3.0/24 这条路由了。

41.3.8 配置 OSPF 完全 Stub 区域 **-S -E -A**

网络需求

- 所有设备配置 OSPF 协议，划分区域 0、区域 1 和区域 2 三个区域，其中区域 1 为完全 Stub 区域。
- 在 Device4 上重分发一条静态路由到 OSPF，配置完成后，完全 Stub 区域不能学到区域间路由和外部路由，其他区域设备可以学习区域间路由和外部路由。

网络拓扑

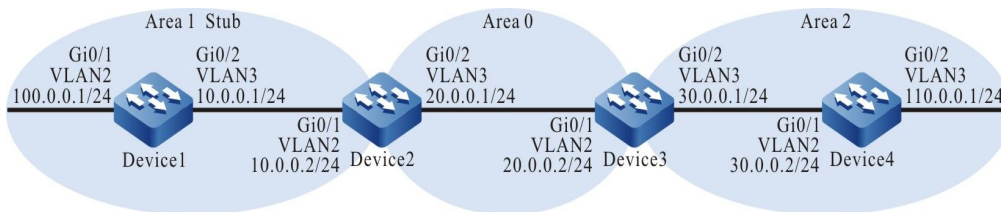


图 41-8 配置 OSPF 完全 Stub 区域组网图

配置步骤

单播路由

步骤 1: 配置 VLAN, 并将端口加入对应的 VLAN。 (略)

步骤 2: 配置各接口 IP 地址。 (略)

步骤 3: 配置 OSPF 进程, 将相应接口覆盖到对应的区域中。

#配置 Device1, 区域 1 配置为 Stub 区域。

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#router-id 1.1.1.1
Device1(config-ospf)#area 1 stub
Device1(config-ospf)#network 10.0.0.0 0.0.0.255 area 1
Device1(config-ospf)#network 100.0.0.0 0.0.0.255 area 1
Device1(config-ospf)#exit
```

#配置 Device2, 区域 1 配置为完全 Stub 区域。 Device2 为 ABR, no-summary 需要在 ABR 上配置才能生效。

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#router-id 2.2.2.2
Device2(config-ospf)#area 1 stub no-summary
Device2(config-ospf)#network 10.0.0.0 0.0.0.255 area 1
Device2(config-ospf)#network 20.0.1.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#配置 Device3。

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#router-id 3.3.3.3
Device3(config-ospf)#network 20.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 30.0.0.0 0.0.0.255 area 2
Device3(config-ospf)#exit
```

#配置 Device4。

```
Device4#configure terminal
Device4(config)#router ospf 100
Device4(config-ospf)#router-id 4.4.4.4
Device4(config-ospf)#network 30.0.0.0 0.0.0.255 area 2
Device4(config-ospf)#network 110.0.0.0 0.0.0.255 area 2
Device4(config-ospf)#exit
```

步骤 4: Device4 配置一条静态路由, 将该路由重分发到 OSPF 中。

#配置 Device4。

```
Device4(config)#ip route 200.1.1.0 255.255.255.0 110.0.0.2
Device4(config)#router ospf 100
Device4(config-ospf)#redistribute static
Device4(config-ospf)#exit
```

步骤 5: 检验结果。

#查看 Device1 的 OSPF LSDB 和路由表。

```
Device1#show ip ospf database

      OSPF Router with ID (1.1.1.1) (Process ID 100)

      Router Link States (Area 1 [Stub])

Link ID      ADV Router   Age Seq#     CkSum Link count
1.1.1.1      1.1.1.1      19 0x80000009 0x8513 2
2.2.2.2      2.2.2.2      22 0x80000005 0x51b6 1

      Net Link States (Area 1 [Stub])

Link ID      ADV Router   Age Seq#     CkSum
10.0.0.2     2.2.2.2      22 0x80000001 0x61ba

      Summary Link States (Area 1 [Stub])

Link ID      ADV Router   Age Seq#     CkSum Route
0.0.0.0      2.2.2.2      55 0x80000002 0x73c1 0.0.0.0/0

Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNRP, B - BGP, i-ISIS

Gateway of last resort is 10.0.0.2 to network 0.0.0.0

O  0.0.0.0/0 [110/2] via 10.0.0.2, 00:00:19, vlan3
C  10.0.0.0/24 is directly connected, 00:01:04, vlan3
C  100.0.0.0/24 is directly connected, 00:11:55, vlan2
C  127.0.0.0/8 is directly connected, 30:46:57, lo0
```

从 OSPF 数据库可以看到，除区域 1 有一条 0.0.0.0/0 的域间 LSA 外，没有其他的区域间 LSA 以及外部路由 LSA。Stub 区域的 ABR 会产生一条 0.0.0.0/0 的区域间路由，该路由在完全 Stub 区域内泛洪，通往区域外以及自治系统外的数据都依赖这条默认路由进行转发。

#查看 Device2 的路由表。

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNRP, B - BGP, i-ISIS

Gateway of last resort is not set

C  10.0.0.0/24 is directly connected, 00:01:02, vlan2
C  20.0.0.0/24 is directly connected, 00:00:59, vlan3
O  30.0.0.0/24 [110/2] via 20.0.0.2, 00:00:17, vlan3
O  100.0.0.0/24 [110/2] via 10.0.0.1, 00:00:10, vlan2
O  110.0.0.0/24 [110/3] via 20.0.0.2, 00:00:17, vlan3
C  127.0.0.0/8 is directly connected, 56:07:04, lo0
OE 200.1.1.0/24 [150/20] via 20.0.0.2, 00:00:16, vlan3
```

可以看到，Device2 可以学到区域间路由和外部路由。

说明:

- 只在 Stub 区域的 ABR 上配置命令 `area area-id stub`, 而不加 `no-summary` 时, 该区域内的设备可以学到区域间路由, 但是不能学到外部路由, 需要访问自治系统外的网络仍然是通过默认路由进行。

41.3.9 配置 OSPF NSSA 区域

-S -E -A

网络需求

- 所有设备配置 OSPF 协议, 划分区域 0、区域 1 和区域 2 三个区域, 其中区域 1 和区域 2 为 NSSA 区域。
- 在 Device4 上重分发一条静态路由到 OSPF, 配置完成后, 所有设备都能学到区域内、区域间路由, 但区域 1 不能注入外部路由。
- 在区域 1 的 ABR 上引入一条默认路由, 使 Device1 可以通过默认路由访问外部网络。

网络拓扑

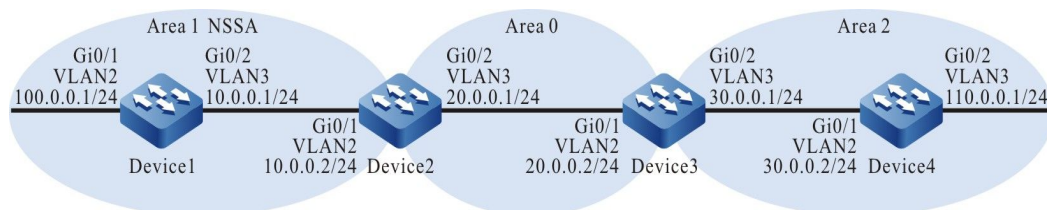


图 41-9 配置 OSPF NSSA 区域组网图

配置步骤

- 步骤 1: 配置 VLAN, 并将端口加入对应的 VLAN。(略)
- 步骤 2: 配置各接口 IP 地址。(略)
- 步骤 3: 配置 OSPF 进程, 将相应接口覆盖到对应的区域中。

#配置 Device1, 区域 1 配置为 NSSA 区域。

```
Device1#configure terminal
```

配置手册

单播路由

```
Device1(config)#router ospf 100
Device1(config-ospf)#router-id 1.1.1.1
Device1(config-ospf)#area 1 nssa
Device1(config-ospf)#network 10.0.0.0 0.0.0.255 area 1
Device1(config-ospf)#network 100.0.0.0 0.0.0.255 area 1
Device1(config-ospf)#exit
```

#配置 Device2, 区域 1 配置为 NSSA 区域。

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#router-id 2.2.2.2
Device2(config-ospf)#area 1 nssa
Device2(config-ospf)#network 10.0.0.0 0.0.0.255 area 1
Device2(config-ospf)#network 20.0.1.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#配置 Device3, 区域 2 配置为 NSSA 区域。

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#router-id 3.3.3.3
Device3(config-ospf)#area 2 nssa
Device3(config-ospf)#network 20.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 30.0.0.0 0.0.0.255 area 2
Device3(config-ospf)#exit
```

#配置 Device4, 区域 2 配置为 NSSA 区域。

```
Device4#configure terminal
Device4(config)#router ospf 100
Device4(config-ospf)#router-id 4.4.4.4
Device4(config-ospf)#area 2 nssa
Device4(config-ospf)#network 30.0.0.0 0.0.0.255 area 2
Device4(config-ospf)#network 110.0.0.0 0.0.0.255 area 2
Device4(config-ospf)#exit
```

步骤 4: Device4 配置一条静态路由, 将该路由重分发到 OSPF 中。

#配置 Device4。

```
Device4(config)#ip route 200.1.1.0 255.255.255.0 110.0.0.2
Device4(config)#router ospf 100
Device4(config-ospf)#redistribute static
Device4(config-ospf)#exit
```

#查看 Device3 的 OSPF LSDB。

```
Device3#show ip ospf database

      OSPF Router with ID (3.3.3.3) (Process ID 100)

      Router Link States (Area 0)

Link ID      ADV Router   Age Seq#      CkSum Link count
2.2.2.2      2.2.2.2     179 0x80000004 0xe110 1
3.3.3.3      3.3.3.3     177 0x80000004 0xa345 1

      Net Link States (Area 0)
```

单播路由

```
Link ID    ADV Router  Age Seq#   CkSum
20.0.0.2  3.3.3.3    182 0x80000001 0xf60d
```

Summary Link States (Area 0)

```
Link ID    ADV Router  Age Seq#   CkSum  Route
10.0.0.0   2.2.2.2    214 0x80000001 0xd455 10.0.0.0/24
100.0.0.0  2.2.2.2    173 0x80000001 0x4886 100.0.0.0/24
30.0.0.0   3.3.3.3    208 0x80000001 0xb160 30.0.0.0/24
110.0.0.0  3.3.3.3    171 0x80000001 0xa719 110.0.0.0/24
```

ASBR-Summary Link States (Area 0)

```
Link ID    ADV Router  Age Seq#   CkSum
4.4.4.4    3.3.3.3    171 0x80000001 0x72ac
```

Router Link States (Area 2 [NSSA])

```
Link ID    ADV Router  Age Seq#   CkSum  Link count
3.3.3.3    3.3.3.3    175 0x80000004 0x686f 1
4.4.4.4    4.4.4.4    177 0x80000005 0xe46a 2
```

Net Link States (Area 2 [NSSA])

```
Link ID    ADV Router  Age Seq#   CkSum
30.0.0.2   4.4.4.4    177 0x80000001 0xc827
```

Summary Link States (Area 2 [NSSA])

```
Link ID    ADV Router  Age Seq#   CkSum  Route
10.0.0.0   3.3.3.3    172 0x80000001 0xde48 10.0.0.0/24
20.0.0.0   3.3.3.3    214 0x80000001 0x52cb 20.0.0.0/24
100.0.0.0  3.3.3.3    172 0x80000001 0x5279 100.0.0.0/24
```

NSSA-external Link States (Area 2 [NSSA])

```
Link ID    ADV Router  Age Seq#   CkSum  Route
200.1.1.0  4.4.4.4    247 0x80000001 0x6cde N2 200.1.1.0/24 [0x0]
```

AS External Link States

```
Link ID    ADV Router  Age Seq#   CkSum  Route
200.1.1.0  3.3.3.3    176 0x80000001 0x0156 E2 200.1.1.0/24 [0x0]
```

从 OSPF 数据库可以看到，在 NSSA 区域 (area 2) 的 ABR 上会将 NSSA-external LSA 转换为 AS External LSA，因此其他区域可以正常学习到从 NSSA 区域 (area 2) 重分发的外部路由。

#查看 Device2 的路由表。

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS
```

Gateway of last resort is not set

```
C 10.0.0.0/24 is directly connected, 00:02:53, vlan2
C 20.0.0.0/24 is directly connected, 00:02:51, vlan3
O 30.0.0.0/24 [110/2] via 20.0.0.2, 00:02:04, vlan3
O 100.0.0.0/24 [110/2] via 10.0.0.1, 00:02:04, vlan2
O 110.0.0.0/24 [110/3] via 20.0.0.2, 00:02:02, vlan3
C 127.0.0.0/8 is directly connected, 06:47:22, lo0
OE 200.1.1.0/24 [150/20] via 20.0.0.2, 00:02:02, vlan3
```

Device2 上已经学到了从 NSSA 区域 (area 2) 重分发的外部路由。

单播路由

#查看 Device1 的路由表。

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C 10.0.0.0/24 is directly connected, 00:02:29, vlan3
O 20.0.0.0/24 [110/2] via 10.0.0.2, 00:01:44, vlan3
O 30.0.0.0/24 [110/3] via 10.0.0.2, 00:01:41, vlan3
C 100.0.0.0/24 is directly connected, 01:53:00, vlan2
O 110.0.0.0/24 [110/4] via 10.0.0.2, 00:01:40, vlan3
C 127.0.0.0/8 is directly connected, 383:45:55, lo0
```

可以看到，Device1 路由表中不存在路由 200.1.1.0/24，表明从 Device4 重分发的外部路由并没有被注入到 NSSA 区域（area 1）中，其它区域间路由已经添加到了路由表中。

步骤 5： 配置 Device2，为区域 1 引入默认路由。

#配置 Device2，此时 Device2 是区域 1 的 ABR。

```
Device2(config)#router ospf 100
Device2(config-ospf)#router-id 2.2.2.2
Device2(config-ospf)#area 1 nssa default-information-originate
Device2(config-ospf)#exit
```

说明：

- 在 NSSA 区域的 ABR 上配置命令 **area area-id nssa no-summary** 后，该区域又叫作完全 NSSA 区域。此时 ABR 也会生成一条默认路由，并且泛洪到 NSSA 区域内；配置该命令后可以进一步减少 summary LSA 和相应的区域间路由，此时访问区域外以及自治系统外的网络都通过这条默认路由进行。
-

步骤 6： 检验结果。

#查看 Device2 的 OSPF LSDB。

```
Device2#show ip ospf database

OSPF Router with ID (2.2.2.2) (Process ID 100)

Router Link States (Area 0)

Link ID      ADV Router   Age Seq#      CkSum Link count
2.2.2.2      2.2.2.2      455 0x80000004 0xe110 1
3.3.3.3      3.3.3.3      455 0x80000004 0xa345 1
```



```

Net Link States (Area 0)

Link ID    ADV Router  Age Seq#    CkSum
20.0.0.2   3.3.3.3    461 0x80000001 0xf60d

Summary Link States (Area 0)

Link ID    ADV Router  Age Seq#    CkSum Route
10.0.0.0   2.2.2.2    492 0x80000001 0xd455 10.0.0.0/24
100.0.0.0  2.2.2.2    449 0x80000001 0x4886 100.0.0.0/24
30.0.0.0   3.3.3.3    487 0x80000001 0xb160 30.0.0.0/24
110.0.0.0  3.3.3.3    449 0x80000001 0xa719 110.0.0.0/24

ASBR-Summary Link States (Area 0)

Link ID    ADV Router  Age Seq#    CkSum
4.4.4.4    3.3.3.3    449 0x80000001 0x72ac

Router Link States (Area 1 [NSSA])

Link ID    ADV Router  Age Seq#    CkSum Link count
1.1.1.1    1.1.1.1    456 0x80000005 0x8d0f 2
2.2.2.2    2.2.2.2    457 0x80000004 0x59ad 1

Net Link States (Area 1 [NSSA])

Link ID    ADV Router  Age Seq#    CkSum
10.0.0.2   2.2.2.2    457 0x80000001 0x61ba

Summary Link States (Area 1 [NSSA])

Link ID    ADV Router  Age Seq#    CkSum Route
20.0.0.0   2.2.2.2    492 0x80000001 0x70b1 20.0.0.0/24
30.0.0.0   2.2.2.2    449 0x80000001 0xf71f 30.0.0.0/24
110.0.0.0  2.2.2.2    448 0x80000001 0xedd7 110.0.0.0/24

NSSA-external Link States (Area 1 [NSSA])

Link ID    ADV Router  Age Seq#    CkSum Route
0.0.0.0    2.2.2.2    31 0x80000001 0x5b42 N2 0.0.0.0/0 [0x0]

AS External Link States

Link ID    ADV Router  Age Seq#    CkSum Route
200.1.1.0  3.3.3.3    454 0x80000001 0x0156 E2 200.1.1.0/24 [0x0]

```

OSPF 为默认路由生成了一条 NSSA-external LSA。

#查看 Device1 的路由表。

```

Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

OE 0.0.0.0/0 [150/1] via 10.0.0.2, 00:00:22, vlan3
C 10.0.0.0/24 is directly connected, 00:07:29, vlan3
O 20.0.0.0/24 [110/2] via 10.0.0.2, 00:06:44, vlan3
O 30.0.0.0/24 [110/3] via 10.0.0.2, 00:06:41, vlan3
C 100.0.0.0/24 is directly connected, 01:58:00, vlan2
O 110.0.0.0/24 [110/4] via 10.0.0.2, 00:06:40, vlan3
C 127.0.0.0/8 is directly connected, 383:50:55, lo0

```

Device1 的路由表中也学到了默认路由 0.0.0.0/0，与自治系统外部路由通信就通过这条默认路由进行。

41.3.10配置 OSPF 与 BFD 联动

-E -A

网络需求

- 所有设备配置 OSPF 协议。
- Device1 和 Device3 间的线路使能 BFD 检测功能，当线路出现故障时，BFD 会快速检测到故障并通知 OSPF，OSPF 将路由切换 Device2 进行通信。

网络拓扑

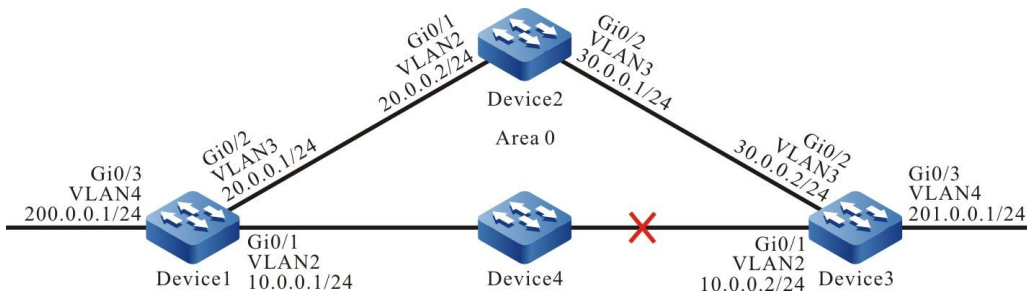


图 41-10 配置 OSPF 与 BFD 联动组网图

配置步骤

- 步骤 1：配置 VLAN，并将端口加入对应的 VLAN。（略）
- 步骤 2：配置各接口 IP 地址。（略）
- 步骤 3：配置 OSPF 进程。

#配置 Device1。

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#router-id 1.1.1.1
Device1(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 20.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 200.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#配置 Device2。

```
Device2#configure terminal
Device2(config)#router ospf 100
```

单播路由

```
Device2(config-ospf)#router-id 2.2.2.2
Device2(config-ospf)#network 20.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 30.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#配置 Device3。

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#router-id 3.3.3.3
Device3(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 30.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 201.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#exit
```

步骤 4： 配置 OSPF 与 BFD 联动。

#配置 Device1。

```
Device1(config)#bfd fast-detect
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip ospf bfd
Device1(config-if-vlan2)#exit
```

#配置 Device3。

```
Device3(config)#bfd fast-detect
Device3(config)#interface vlan2
Device3(config-if-vlan2)#ip ospf bfd
Device3(config-if-vlan2)#exit
```

步骤 5： 检验结果。

#查看 Device1 的 OSPF 邻居信息和路由表。

```
Device1#show ip ospf neighbor 3.3.3.3

OSPF process 100:
Neighbor 3.3.3.3, interface address 10.0.0.2
  In the area 0 via interface vlan2, BFD enabled
  Neighbor priority is 1, State is Full, 5 state changes
  DR is 10.0.0.2, BDR is 10.0.0.1
  Options is 0x42 (-|O|-|-|E|-)
  Dead timer due in 00:00:31
  Neighbor is up for 00:02:46
  Database Summary List 0
  Link State Request List 0
  Link State Retransmission List 0
  Crypt Sequence Number is 0
  Graceful restart proxy id is 0x0
  Thread Inactivity Timer on
  Thread Database Description Retransmission off, 0 times
  Thread Link State Request Retransmission off, 0 times
  Thread Link State Update Retransmission off, 0 times

Device1#show ip route
```

单播路由

```
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
        D - Redirect, E - IRMP, EX - IRMP external, o - SNRP, B - BGP, i-ISIS
```

```
Gateway of last resort is not set
```

```
C 10.0.0.0/24 is directly connected, 00:01:09, vlan2
C 20.0.0.0/24 is directly connected, 00:55:37, vlan3
O 30.0.0.0/24 [110/2] via 20.0.0.2, 00:02:50, vlan3
  [110/2] via 10.0.0.2, 00:01:30, vlan2
C 127.0.0.0/8 is directly connected, 05:51:09, lo0
C 200.0.0.0/24 is directly connected, 00:55:12, vlan4
O 201.0.0.0/24 [110/2] via 10.0.0.2, 00:01:30, vlan2
```

从 OSPF 邻居信息中看到 BFD 已经使能，路由 201.0.0.0/24 优选 Device1 和 Device3 之间的线路进行通信。

#查看 Device1 的 BFD 会话信息。

```
Device1#show bfd session detail
Total session number: 1
OurAddr      NeighAddr      LD/RD      State      Holddown      interface
10.0.0.1      10.0.0.2        7/14       UP         5000          vlan2
Type:direct
Local State:UP Remote State:UP Up for: 0h:2m:37s Number of times UP:1
Send Interval:1000ms Detection time:5000ms(1000ms*5)
Local Diag:0 Demand mode:0 Poll bit:0
MinTxInt:1000 MinRxInt:1000 Multiplier:5
Remote MinTxInt:1000 Remote MinRxInt:1000 Remote Multiplier:5
Registered protocols:OSPF
```

可以看到 OSPF 与 BFD 联动成功，会话正常建立。

#Device1 和 Device3 之间的线路出现故障后，BFD 会快速检测到故障并通知 OSPF，OSPF 将路由切换到 Device2 上进行通信，查看 Device1 的路由表。

```
%BFD-5-Session [10.0.0.2,10.0.0.1,vlan2,10] DOWN (Detection time expired)
%OSPF-5-ADJCHG: Process 100 Nbr [vlan2:10.0.0.1-3.3.3.3] from Full to Down,KillINbr: BFD session down
```

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
        D - Redirect, E - IRMP, EX - IRMP external, o - SNRP, B - BGP, i-ISIS
```

```
Gateway of last resort is not set
```

```
C 10.0.0.0/24 is directly connected, 00:01:59, vlan2
C 20.0.0.0/24 is directly connected, 00:56:13, vlan3
O 30.0.0.0/24 [110/2] via 20.0.0.2, 00:03:40, vlan3
C 127.0.0.0/8 is directly connected, 05:52:41, lo0
C 200.0.0.0/24 is directly connected, 00:56:02, vlan4
O 201.0.0.0/24 [110/3] via 20.0.0.2, 00:00:06, vlan3
```

Device3 的行为和 Device1 类似。

42 OSPFv3

42.1 OSPFv3 简介

OSPFv3 是 OSPF (Open Shortest Path First, 开放最短路径优先) 第 3 版的简称, 主要提供对 IPv6 的支持, 遵循 RFC2328, RFC2740, 并且支持其它相关 RFC 定义的 OSPF 扩展功能。

OSPFv3 原理与 OSPFv2 基本一样, 只是针对不同的 IP 协议及地址族, 有一些相应的修改。其不同之处主要表现在:

- OSPFv3 基于链路运行, OSPFv2 基于网段运行;
- OSPFv3 每链路上支持多个实例;
- OSPFv3 通过 Router ID 标志邻接的邻居, OSPFv2 通过 IP 地址标志邻接的邻居;

42.2 OSPFv3 功能配置

表 42-1 OSPFv3 功能配置列表

配置任务	
配置 OSPFv3 基本功能	使能 OSPFv3 协议
配置 OSPFv3 区域	配置 OSPFv3 NSSA 区域
	配置 OSPFv3 Stub 区域
	配置 OSPFv3 虚链接

配置任务	
配置 OSPFv3 网络类型	配置 OSPFv3 接口网络类型为广播
	配置 OSPFv3 接口网络类型为 P2P
	配置 OSPFv3 接口网络类型为 NBMA
	配置 OSPFv3 接口网络类型为 P2MP
配置 OSPFv3 网络认证	配置 OSPFv3 区域认证
	配置 OSPFv3 接口认证
配置 OSPFv3 路由生成	配置 OSPFv3 路由重分发
	配置 OSPFv3 默认路由
配置 OSPFv3 路由控制	配置 OSPFv3 区域间路由汇总
	配置 OSPFv3 外部路由汇总
	配置 OSPFv3 区域间路由过滤
	配置 OSPFv3 外部路由过滤
	配置 OSPFv3 路由安装过滤
	配置 OSPFv3 接口 cost 值
	配置 OSPFv3 参考带宽
	配置 OSPFv3 管理距离
配置 OSPFv3 最大负载均衡条目数	

配置任务	
配置 OSPFv3 网络优化	配置 OSPFv3 邻居保活时间
	配置 OSPFv3 被动接口
	配置 OSPFv3 需求电路
	配置 OSPFv3 接口优先级
	配置 OSPFv3 接口忽略 MTU
	配置 OSPFv3 接口 LSA 传送时延
	配置 OSPFv3 LSA 重传
	配置 OSPFv3 SPF 计算时间
配置 OSPFv3 GR	配置 OSPFv3 GR Restarter
	配置 OSPFv3 GR Helper
配置 OSPFv3 与 BFD 联动	配置 OSPFv3 与 BFD 联动

42.2.1 配置 OSPFv3 基本功能

-E -A

在 OSPFv3 的各项配置任务中，必须先使能 OSPFv3 协议，其它功能特性的配置才能生效。

配置条件

在配置 OSPFv3 基本功能之前，首先完成以下任务：

- 配置链路层协议，保证链路层通信正常。
- 使能 IPv6 转发功能。

使能 OSPFv3 协议

单播路由

启用 OSPFv3 功能，需先创建 OSPFv3 进程，指定该进程的 Router ID，并在接口上使能 OSPFv3 协议。

运行 OSPFv3 协议的设备，必须存在 Router ID，用于在一个 OSPFv3 自治系统内唯一的标识一台设备。需要保证自治系统内 Router ID 的唯一性，否则会影响邻居建立和路由学习。在 OSPFv3 中，需手动配置一个 IPv4 地址格式的 Router ID。

OSPFv3 支持多进程，使用进程号标识一个进程，不同进程间相互独立，互不影响。

表 42-2 使能 OSPFv3 协议

步骤	命令	说明
进入全局配置模式	configure terminal	-
创建 OSPFv3 进程并进入 OSPF 配置模式	ipv6 router ospf <i>process-id</i> [vrf <i>vrf-name</i>]	必选 启用或从 VRF 中启用 OSPFv3 进程，缺省情况下系统未使能 OSPFv3 协议 从 VRF 下启用 OSPFv3 时，属于某个 VRF 的 OSPFv3 进程只能管理属于该 VRF 的接口
配置 OSPFv3 进程 Router ID	router-id <i>ipv4-address</i>	必选
返回全局配置模式	exit	-
进入接口配置模式	interface <i>interface-name</i>	-
配置接口上使能 OSPFv3 协议	ipv6 router ospf <i>process-id</i> area <i>area-id</i>	必选

步骤	命令	说明
	[instance-id <i>instance-id</i>]	缺省情况下，接口上未使能 OSPFv3 协议

42.2.2 配置 OSPFv3 区域

-E -A

为了减少大量数据库信息对 CPU 和内存的占用，将 OSPFv3 自治系统划分多个区域。区域通过 32 位的区域 ID 来标识，可以用 0~4294967295 范围的十进制数或者 0.0.0.0~255.255.255.255 范围的 IP 地址表示。区域 0 或 0.0.0.0 表示 OSPFv3 骨干区域，其它非 0 区域为非骨干区域。所有的区域间路由信息都需要通过骨干区域进行转发，非骨干区域之间不能直接交换路由信息。

OSPF v3 中定义了几种类型的路由器：

- 内部路由器（Internal Router）：所有接口都属于一个区域的设备；
- 区域边界路由器（Area Border Router，简称 ABR）：连接到多个区域的设备；
- 自治系统边界路由器（Autonomous System Boundary Router，简称 ASBR）：为 OSPF v3 自治系统引入外部路由的设备。

配置条件

在配置 OSPFv3 区域前，首先完成以下任务：

- 使能 IPv6 转发功能。
- 使能 OSPFv3 协议。

配置 OSPFv3 NSSA 区域

非完全存根区域（Not-So-Stub-Area，简称 NSSA）内不允许 Type-5 LSA 注入，但允许 Type-7 LSA 注入。通过配置重分发向 NSSA 区域引入外部路由，NSSA 区域的 ASBR 生成 Type-7 LSA，并泛洪到该 NSSA 区域。NSSA 区域的 ABR 会将 Type-7 LSA 转换为 Type-5 LSA，并把这些转换的 Type-5 LSA 泛洪到整个自治系统。

通过命令 **area area-id nssa no-summary** 配置的 OSPFv3 NSSA 区域，称为完全 NSSA 区域。OSPFv3 完全 NSSA 区域禁止区域间路由在该区域内泛洪，此时 ABR 会生成一条默认路由，并泛洪到 NSSA 区域内，NSSA 区域内的设备将通过这条默认路由访问区域外的网络。

表 42-3 配置 OSPFv3 NSSA 区域

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 OSPFv3 配置模式	ipv6 router ospf <i>process-id</i> [vrf vrf-name]	-
配置 NSSA 区域	area area-id nssa [no- redistribution / no- summary / default- information-originate [metric metric-value / metric-type type- value]]	必选 缺省情况下, OSPFv3 区域不为 NSSA 区域

说明:

- 骨干区域不能配置为 NSSA 区域。
- 同一个 NSSA 区域内的所有设备都必须配置为 NSSA 区域, 区域类型不一致的设备间不能形成邻接关系。

配置 OSPFv3 Stub 区域

存根区域 (Stub) 不允许 AS 外部路由在该区域内泛洪, 以减少链路状态数据库的大小。配置区域为 Stub 后, 位于 Stub 边界的 ABR 产生一条默认路由, 并泛洪到该 Stub 区域内, Stub 区域内的设备将通过这条默认路由访问自治系统外的网络。

通过命令 **area area-id stub no-summary** 配置的 OSPFv3 Stub 区域, 称为完全 Stub 区域。OSPFv3 完全 Stub 区域禁止区域间路由、外部路由在该区域内泛洪, 区域内的设备将通过默认路由访问该区域外以及 OSPFv3 自治系统外的网络。

表 42-4 配置 OSPFv3 Stub 区域

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 OSPFv3 配置模式	ipv6 router ospf <i>process-id [vrf vrf-name]</i>	-
配置 Stub 区域	area area-id stub [no-summary]	必选 缺省情况下, OSPFv3 区域不为 Stub 区域

说明:

- 骨干区域不能配置为 Stub 区域。
- 同一个 Stub 区域内的所有设备都必须配置为 Stub 区域, 区域类型不一致的设备间不能形成邻接关系。

配置 OSPFv3 虚链接

OSPFv3 中非骨干区域间必须通过骨干区域来完成数据库的同步和数据的交互。因此, 要求所有的非骨干区域必须和骨干区域保持连通。

当某些情况不能满足该要求时, 可通过配置虚链接来解决这个问题。配置虚链接后, 可以为该虚链接配置认证方式、修改 Hello 时间间隔等, 这些参数的含义与一般 OSPFv3 接口参数的含义一致。

表 42-5 配置 OSPFv3 虚链接

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
进入 OSPFv3 配置模式	ipv6 router ospf <i>process-id</i> [vrf vrf-name]	-
配置虚链接	area <i>transit-area-id</i> virtual-link <i>neighbor-id</i> [dead-interval <i>seconds</i> / hello-interval <i>seconds</i> / retransmit-interval <i>seconds</i> / transmit-delay <i>seconds</i>]	必选 缺省情况下，不会创建虚链接

说明：

- 虚链接必须配置在两台 ABR 之间。
- 配置虚链接的两个 ABR 必须处于同一个公共区域，该区域也称为虚链接的传输区域 (Transit Area)。
- 虚链接的传输区域不能是 Stub 区域或 NSSA 区域。

42.2.3 配置 OSPFv3 网络类型

-E -A

OSPFv3 根据链路协议类型将网络划分为四种类型：

- 广播网络 (Broadcast Networks) ——链路协议是 Ethernet、FDDI 时，OSPFv3 缺省网络类型为广播。
- P2P (Point To Point Network) ——当链路协议是 PPP、LAPB、HDLC 时，OSPFv3 缺省网络类型为 P2P。
- NBMA 网络 (Non-Broadcast Multi-Access Network) ——当链路协议是 ATM、帧中继或 X.25 时，OSPFv3 缺省网络类型是 NBMA。
- P2MP (Point To Multi-Point Network) ——没有一种链路协议会被 OSPFv3 缺

省认为是 P2MP 类型，通常将不是全联通的 NBMA 网络配置为 OSPFv3 P2MP 网络。

可根据需要，修改 OSPFv3 接口的网络类型。建立 OSPFv3 邻居的接口网络类型需要一致，否则将影响路由的正常学习。

配置条件

在配置 OSPFv3 网络类型前，首先完成以下任务：

- 使能 IPv6 转发功能。
- 使能 OSPFv3 协议。

配置 OSPFv3 接口网络类型为广播

广播网络支持多台（两个以上）设备，这些设备都有能力与网络上的所有设备交互信息。OSPFv3 使用 Hello 报文动态发现邻居。

表 42-6 配置 OSPFv3 接口网络类型为广播

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置 OSPFv3 接口网络类型为广播	ipv6 ospf network broadcast	必选 缺省情况下，OSPFv3 接口网络类型由链路层协议确定

配置 OSPFv3 接口网络类型为 P2P

点到点网络，即由两台设备组成的网络，每台设备在点到点链路的一端。OSPFv3 使用 Hello 报文动态的发现邻居。

表 42-7 配置 OSPFv3 接口网络类型为 P2P

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置 OSPFv3 接口网络类型为 P2P	ipv6 ospf network point-to-point	必选 缺省情况下, OSPFv3 接口网络类型由链路层协议确定

配置 OSPFv3 接口网络类型为 NBMA

NBMA 网络支持多台（两个以上）设备，但是没有广播能力，需要手动指定邻居。

表 42-8 配置 OSPFv3 接口网络类型为 NBMA

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置 OSPFv3 接口网络类型为 NBMA	ipv6 ospf network non-broadcast	必选 缺省情况下, OSPFv3 接口网络类型由链路层协议确定
配置 NBMA 网络邻居	ipv6 ospf neighbor <i>neighbor-ipv6-address</i> [priority <i>priority-value</i> / poll-interval <i>interval-value</i> / cost <i>cost-value</i>]	必选 NBMA 网络中, 需手动指定邻居

单播路由

步骤	命令	说明
	[instance-id <i>instance-id</i>]	

配置 OSPFv3 接口网络类型为 P2MP

当 NBMA 不是全连通时，可配置网络类型为 P2MP，节省网络开销。配置网络类型为 P2MP 单播时，需手动指定邻居。

表 42-9 配置 OSPFv3 接口网络类型为 P2MP

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置 OSPFv3 接口网络类型为 P2MP	ipv6 ospf network point-to-multipoint [non-broadcast]	必选 缺省情况下，OSPFv3 接口网络类型由链路层协议确定
配置 P2MP 单播网络邻居	ipv6 ospf neighbor <i>neighbor-ipv6-address</i> [priority <i>priority-value</i> / poll-interval <i>interval-value</i> / cost <i>cost-value</i>] [instance-id <i>instance-id</i>]	如果配置接口网络类型为 P2MP 单播，则必选

为了防止信息外泄或对 OSPFv3 设备进行恶意的攻击，OSPFv3 邻居间所有报文的交互都具有加密认证能力。加密认证类型和算法可以是：NULL(没有认证)、SHA1 认证、MD5 认证由 IPsec 加密认证策略指定。

配置认证后，IPsec 安全特性会对 OSPFv3 协议报文进行加密认证，只有通过解密认证，OSPFv3 协议才能接收报文。因此建立邻接关系的 OSPFv3 接口，其认证方式、Spi ID、认证密码配置的 IPsec 加密认证策略必须一致。OSPFv3 认证方式可以在区域、接口上配置，其优先级从低到高为：区域认证、接口认证。即优先使用接口的认证方式，然后使用区域的认证方式。

配置条件

在配置 OSPFv3 网络认证前，首先完成以下任务：

- 使能 IPv6 转发功能。
- 使能 OSPFv3 协议。

配置 OSPFv3 区域认证

OSPFv3 进程区域下配置区域认证，可以使该区域下所有接口使用区域认证方式，能够有效避免接口下重复配置相同网络认证方式。

表 42-10 配置 OSPFv3 区域认证

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 OSPFv3 配置模式	ipv6 router ospf <i>process-id</i> [vrf <i>vrf-name</i>]	-
配置区域认证方式	area <i>area-id</i> ipsec-tunnel <i>tunnel-name</i>	必选 缺省情况下，OSPFv3 未配置区域认证

配置 OSPFv3 接口认证

当一个接口上有多个 OSPFv3 实例时，可以为某一个实例单独指定认证方式和密码。接口下未指定接口认证的实例，采用区域下指定的认证方式。

表 42-11 配置 OSPFv3 接口认证

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置接口认证方式	ipv6 ospf ipsec-tunnel <i>tunnel-name</i> { <i>instance-id</i> <i>instance-id</i> }	必选 缺省情况下，OSPFv3 未配置接口认证方式

42.2.5 配置 OSPFv3 路由生成

-E -A

配置条件

在配置 OSPFv3 路由生成前，首先完成以下任务：

- 使能 IPv6 转发功能。
- 使能 OSPFv3 协议。

配置 OSPFv3 路由重分发

当在一台设备上运行多种路由协议时，通过重分发将其它协议的路由引入到 OSPFv3 中，缺省生成 OSPFv3 第二类外部路由，路由 metric 值为 20。重分发引入外部路由时，可修改外部路由类型以及 metric、Tag 字段，并关联指定的路由策略，进行路由控制与管理。

表 42-12 配置 OSPFv3 路由重分发

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 OSPFv3 配置模式	ipv6 router ospf <i>process-id</i> [vrf vrf-name]	-
配置 OSPFv3 路由重分发	redistribute routing-protocol [<i>protocol-id-or-name</i>] [metric metric-value / metric-type type-value / tag tag-value / route-map map-name / match route-type]	必选 缺省情况下, OSPFv3 未配置路由重分发
配置 OSPFv3 外部路由 metric 值	default-metric metric-value	可选

说明:

- 同时配置 **redistribute protocol** [*protocol-id*] **metric** 和 **default-metric** 设置外部路由的 metric 值时, 前者优先级较高。

配置 OSPFv3 默认路由

配置 OSPFv3 Stub 区域、完全 NSSA 区域后, 会自动生成 Type-3 的默认路由。NSSA 区域不会自动生成默认路由, 可通过 **area area-id nssa default-information-originate** 命令向 NSSA 区域引入一条 Type-7 的默认路由。

OSPFv3 不能通过 **redistribute** 命令引入 Type-5 的默认路由, 若需要, 可通过配置 **default-information originate** [**always**] 命令来实现。

表 42-13 配置 OSPFv3 默认路由

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 OSPFv3 配置模式	ipv6 router ospf <i>process-id</i> [vrf <i>vrf-name</i>]	-
配置 OSPFv3 默认路由	default-information originate [always / metric <i>metric-value</i> / metric-type <i>metric-type</i> / route-map <i>route-map-name</i>]	<p>必选</p> <p>缺省情况下，不会向 OSPFv3 自治系统引入外部默认路由</p> <p>引入默认路由的缺省 metric 值为 1，类型为外部类型 2</p> <p>always 表示强制向 OSPFv3 自治系统中生成默认路由，否则，只在本地路由表中有默认路由时才会生成</p>

42.2.6 配置 OSPFv3 路由控制

-E -A

配置条件

在配置 OSPFv3 路由控制前，首先完成以下任务：

- 使能 IPv6 转发功能。
- 使能 OSPFv3 协议。

配置 OSPFv3 区域间路由汇总

单播路由

OSPFv3 中 ABR 在向其它区域通告区域间路由时，每条路由都是以 Type-3 LSA 单独通告的，可使用区域间路由汇总功能，将区域内一些连续的网段汇总为一条路由，只将汇总后的路由通告出去，以减少 OSPFv3 数据库的大小。

表 42-14 配置 OSPFv3 区域间路由汇总

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 OSPFv3 配置模式	ipv6 router ospf <i>process-id</i> [vrf vrf-name]	-
配置 OSPFv3 区域间路由汇总	area area-id range <i>ipv6-prefix/prefix-length</i> [advertise not-advertise]	必选 缺省情况下，ABR 不会进行区域间路由汇总

说明：

- OSPFv3 区域间路由汇总功能只在 ABR 上生效。
- 缺省情况下，选择明细路由中 cost 的最小值作为汇总路由的 cost 值。

配置 OSPFv3 外部路由汇总

OSPFv3 重分发外部路由时，每条路由在外部链路状态通告中均是单独通告的，可使用外部路由汇总功能，将自治系统外一些连续的网段汇总为一条路由，只将汇总后的路由通告出去，以减少 OSPFv3 数据库的大小。

在 ASBR 上配置 **summary-address** 命令后，可在在汇总地址范围内的 Type-5 LSA 和 Type-7 LSA 进行汇总。

表 42-15 配置 OSPFv3 外部路由汇总

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 OSPFv3 配置模式	ipv6 router ospf <i>process-id</i> [vrf vrf-name]	-
配置 OSPFv3 外部路由汇总	summary-prefix <i>ipv6-prefix/prefix-length</i> [not-advertise tag tag-value]	必选 缺省情况下, ASBR 不会进行外部路由汇总

说明:

- OSPFv3 外部路由汇总功能只在 ASBR 上生效。

配置 OSPFv3 区域间路由过滤

ABR 在接收区域间路由时, 使用 ACL 或者前缀列表进行 in 方向的过滤, 在通告区域间路由时使用 ACL 或者前缀列表进行 out 方向的过滤。

表 42-16 配置 OSPFv3 区域间路由过滤

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 OSPFv3 配置模式	ipv6 router ospf <i>process-id</i> [vrf vrf-name]	-
配置 OSPFv3 区域间路由过滤	area <i>area-id</i> filter-list { access { <i>access-list-name</i> / <i>access-list-</i>	必选

单播路由

步骤	命令	说明
	<code>number } prefix prefix-list-name } { in out }</code>	缺省情况下, ABR 不会进行区域间路由过滤

说明:

- OSPFv3 区域间路由过滤功能只在 ABR 上生效。

配置 OSPFv3 外部路由过滤

配置外部路由过滤, 即应用 ACL 或前缀列表来允许或禁止 OSPFv3 自治系统外的路由泛洪到 OSPFv3 自治系统内。

表 42-17 配置 OSPFv3 外部路由过滤

步骤	命令	说明
进入全局配置模式	<code>configure terminal</code>	-
进入 OSPFv3 配置模式	<code>ipv6 router ospf process-id [vrf vrf- name]</code>	-
配置 OSPFv3 外部路由过滤	<code>istribute-list { access { access-list-name / access-list-number } prefix prefix-list-name } out [routing-protocol [process-id]]</code>	必选 缺省情况下, ASBR 不会进行外部路由过滤

说明:

- OSPFv3 外部路由过滤功能只在 ASBR 上生效。

配置 OSPFv3 路由安装过滤

OSPFv3 通过 LSA 计算出路由后，为了防止某些路由加入路由表，可对计算出的 OSPFv3 协议路由信息进行过滤。

表 42-18 配置 OSPFv3 路由安装过滤

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 OSPFv3 配置模式	ipv6 router ospf <i>process-id</i> [vrf <i>vrf-name</i>]	-
配置 OSPFv3 路由安装过滤	distribute-list { access { <i>access-list-name</i> / <i>access-list-number</i> } gateway <i>prefix-list-name1</i> prefix <i>prefix-list-name2</i> [gateway <i>prefix-list-name3</i>] route-map <i>route-map-name</i> } in [<i>interface-name</i>]	必选 缺省情况下，未配置 OSPFv3 路由安装过滤

说明：

- 配置 **prefix**、**gateway**、**route-map** 过滤与配置 ACL 过滤互斥，如：先配置了 **prefix** 过滤，则不能再配置 ACL 过滤。

- 配置 **route-map**、**prefix** 过滤与配置 **gateway** 过滤互斥。
- 配置 **prefix** 过滤与配置 **gateway** 过滤相互覆盖。

配置 OSPFv3 接口 cost 值

缺省情况下，OSPFv3 接口开销的计算方法为：参考带宽/接口带宽。

表 42-19 配置 OSPFv3 接口 cost 值

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置 OSPFv3 接口 cost 值	ipv6 ospf cost <i>cost</i> [instance-id <i>instance-id</i>]	可选 缺省情况下，根据参考带宽/接口带宽计算所得

配置 OSPFv3 参考带宽

接口参考带宽主要用于计算接口 cost 值，缺省为 100Mbit/s，OSPFv3 接口 cost 的计算方法为：参考带宽/接口带宽，计算结果大于 1 时，取整数部分；小于 1 时，则取 1。因此在带宽高于 100Mbit/s 的网络中，将不能正确的选择出最优路由，可使用 **auto-cost reference-bandwidth** 命令配置适当的参考带宽来解决这个问题。

表 42-20 配置 OSPFv3 参考带宽

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 OSPFv3 配置模式	ipv6 router ospf <i>process-id</i> [vrf <i>vrf-name</i>]	-

步骤	命令	说明
配置 OSPFv3 参考带宽	auto-cost reference-bandwidth <i>reference-bandwidth</i>	可选 缺省情况下，参考带宽为 100Mbit/s

配置 OSPFv3 管理距离

管理距离用于表示路由协议的可信度，当从不同路由协议学习到达同一目的网络的路由后，根据管理距离进行选择，优先选择管理距离小的路由。

表 42-21 配置 OSPFv3 管理距离

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 OSPFv3 配置模式	ipv6 router ospf <i>process-id</i> [vrf <i>vrf-name</i>]	-
配置 OSPFv3 管理距离	distance [ospf { external <i>distance</i> / inter-area <i>distance</i> / intra-area <i>distance</i> } <i>distance</i>]	可选 缺省情况下，OSPFv3 区域内路由、区域间路由管理距离为 110，外部路由管理距离为 150

配置 OSPFv3 最大负载均衡条目数

到达同一目的地址存在多条等价路径，则形成负载均衡，可提高链路的利用率并减少链路的负担。

表 42-22 配置 OSPFv3 最大负载均衡条目数

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
进入 OSPFv3 配置模式	ipv6 router ospf <i>process-id [vrf vrf-name]</i>	-
配置 OSPFv3 最大负载均衡条目数	maximum-paths max-number	可选 缺省情况下, OSPFv3 最大负载均衡条目数为 4

42.2.7 配置 OSPFv3 网络优化

-E -A

配置条件

在配置 OSPFv3 网络优化前, 首先完成以下任务:

- 使能 IPv6 转发功能。
- 使能 OSPFv3 协议。

配置 OSPFv3 邻居保活时间

OSPFv3 Hello 报文用来建立并保活邻居关系, Hello 报文缺省发送时间间隔由网络类型确定, 广播网络、P2P 网络中 Hello 报文发送时间间隔缺省为 10 秒, P2MP、NBMA 网络中 Hello 报文发送时间间隔缺省为 30 秒。

邻居失效时间用来判断邻居的有效性, 缺省是 Hello 时间间隔的 4 倍。若 OSPFv3 设备在邻居失效时间超时后还没有收到邻居的 Hello 报文, 则认为邻居已经无效, 并主动删除该邻居。

表 42-23 配置 OSPFv3 邻居保活时间

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
进入接口配置模式	interface <i>interface-name</i>	-
配置 OSPFv3 Hello 时间间隔	ipv6 ospf hello-interval <i>interval-value</i> [instance-id <i>instance-id</i>]	可选 缺省值根据网络类确定，广播网络、P2P 网络为 10 秒，P2MP、NBMA 网络为 30 秒
配置 OSPFv3 邻居失效时间间隔	ipv6 ospf dead-interval <i>interval-value</i> [instance-id <i>instance-id</i>]	可选 缺省为发送 Hello 时间间隔的 4 倍

说明：

- OSPFv3 相邻设备间 Hello 时间间隔和邻居失效时间必须一致，否则不能建立起邻居关系。
- 修改 Hello 时间间隔时，若当前邻居失效时间为 Hello 时间间隔的 4 倍，则邻居失效时间也会自动修改保持 4 倍关系；若当前邻居失效时间不是 Hello 时间间隔的 4 倍，则邻居失效时间保持不变。
- 修改邻居失效时间不会影响 Hello 时间间隔。

配置 OSPFv3 被动接口

动态路由协议采用被动接口（Passive Interface），可有效减少路由协议对网络带宽的消耗。配置 OSPFv3 被动接口，可通过接口使能命令通告该接口所在直连网段的路由，但抑制 OSPFv3 协议报文在该接口上的接收和发送。

表 42-24 配置 OSPFv3 被动接口

单播路由

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 OSPFv3 配置模式	ipv6 router ospf <i>process-id</i> [vrf <i>vrf-name</i>]	-
配置 OSPFv3 被动接口	passive-interface { <i>interface-name/default</i> }	必选 缺省情况下, 未配置 OSPF 被动接口

配置 OSPFv3 需求电路

在 P2P、P2MP 链路上, 为减少线路费用, 可配置 OSPFv3 需求电路, 抑制 Hello 报文的周期性发送和 LSA 报文的周期刷新。主要用在 ISDN、SVC、X.25 等收费链路上。

表 42-25 配置 OSPFv3 需求电路

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置 OSPFv3 需求电路	ipv6 ospf demand-circuit [instance-id <i>instance-id</i>]	必选 缺省情况下, 未使能 OSPFv3 需求电路

配置 OSPFv3 接口优先级

接口优先级主要用于广播网络、NBMA 网络中, 指定路由器 DR (Designed Router)、备份指定路由器 BDR (Backup Designed Router) 的选举, 取值范围 0~255, 数值越大优先级越高, 缺省为 1。

单播路由

DR 和 BDR 是由同一网段中所有设备根据接口优先级、Router ID 通过 Hello 报文选举出来的，规则如下：

- 首先选举接口优先级最高的设备为 DR，选举接口优先级次高的为 BDR，优先级为 0，不参与选举。
- 如果接口优先级相同，则选举 Router ID 最高的设备为 DR，选举 Router ID 次高的为 BDR。

当 DR 失效后，BDR 会立即成为 DR，再选举新的 BDR。

表 42-26 配置 OSPFv3 接口优先级

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置 OSPFv3 接口优先级	ipv6 ospf priority <i>priority-value</i> [instance-id <i>instance-id</i>]	可选 缺省情况下，OSPFv3 接口优先级为 1

说明：

- 优先级只影响选举过程，当网络中已经选举产生了 DR 和 BDR 时，修改接口优先级并不会影响本次选举结果，只影响下一次 DR 或 BDR 选举结果；故 DR 不一定是接口优先级最高的设备，BDR 不一定是接口优先级次高的设备。

配置 OSPFv3 接口忽略 MTU

当 OSPFv3 相邻设备间交互 DD 报文时，缺省情况下会检查 MTU 是否相同，若不相同则不能形成邻接关系。配置 OSPFv3 忽略接口 MTU 检查后，即使 MTU 不相同，也可以建立邻接关系。

表 42-27 配置 OSPFv3 接口忽略 MTU

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置 OSPFv3 接口忽略 MTU	ipv6 ospf mtu-ignore [instance-id <i>instance-id</i>]	必选 缺省情况下，会进行 MTU 一致性检查

配置 OSPFv3 接口 LSA 传送时延

LSA 传送时延表示 LSA 泛洪到其它设备所需花费的时间，发送 LSA 的设备会将接口传送时延加到待发送 LSA 的老化时间上。缺省情况下，当泛洪的 LSA 经过一台设备时老化时间会加 1。可根据网络状况配置 LSA 的传送时延，取值范围 1~840。一般用在低速链路上。

表 42-28 配置 OSPFv3 接口 LSA 传送时延

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置 OSPFv3 接口 LSA 传送时延	ipv6 ospf transmit-delay <i>delay-value</i> instance-id [<i>instance-id</i>]	可选 缺省情况下，接口 LSA 传送时延为 1 秒

配置 OSPFv3 LSA 重传

为了保证数据交互的可靠性，OSPFv3 采用确认机制。当设备接口上泛洪一个 LSA 时，会将该 LSA 加入到邻居的重传列表中，若在重传时间超时后还没有收到邻居的确认信息，则会重传该 LSA，直到收到确认信息。

表 42-29 配置 OSPFv3 LSA 重传

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置 OSPFv3 LSA 重传时间间隔	ipv6 ospf retransmit-interval <i>interval-value</i> [instance-id <i>instance-id</i>]	可选 缺省情况下, LSA 重传时间间隔为 5 秒

配置 OSPFv3 SPF 计算时间

当 OSPFv3 网络拓扑发生变化时, 需要重新计算路由。网络不断变化时, 频繁的路由计算会占用大量的系统资源。通过调整 SPF 计算的时间参数, 来抑制网络频繁变化对系统资源的消耗。

表 42-30 配置 OSPFv3 SPF 计算时间

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 OSPFv3 配置模式	ipv6 router ospf <i>process-id</i> [vrf <i>vrf-name</i>]	-
配置 OSPFv3 SPF 计算时间	timers throttle spf <i>delay-time hold-time max-time</i>	可选 缺省情况下, <i>delay-time</i> 为 5000 毫秒, <i>hold-time</i> 为 10000 毫秒, <i>max-time</i> 为 10000 毫秒

说明：

- 参数 *delay-time* 表示初始计算时延，*hold-time* 表示抑制时间，*max-time* 表示两次 SPF 计算的最大等待时间。在网络变化不频繁的情况下将连续路由计算的时间间隔缩小到 *delay-time*，而在网络变化频繁的情况下可以进行相应调整，增加 $hold-time \times 2^{n-2}$ （n 为连续触发路由计算的次数），将等待时间按照配置的 *hold-time* 增量延长，最大不超过 *max-time*。

42.2.8 配置 OSPFv3 GR -E -A

GR（Graceful Restart，优雅重启）用于在设备主备切换过程中，保持本设备和邻居设备转发层面路由信息不变，转发不受影响；当切换设备重新运行后，两台设备协议层面同步路由信息并更新转发层，达到设备切换过程中数据转发不间断的目的。

GR 过程中有两种角色：

- GR Restarter 端——进行协议优雅重启的设备。
- GR Helper 端——协助协议优雅重启的设备。

分布式设备可以充当 GR Restarter 和 GR Helper，而集中式设备只能充当 GR Helper，协助 Restarter 端完成 GR。

配置条件

在配置 OSPFv3 GR 前，首先完成以下任务：

- 使能 IPv6 转发功能。
- 使能 OSPFv3 协议。

配置 OSPFv3 GR Restarter

表 42-31 配置 OSPFv3 GR Restarter

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
进入 OSPFv3 配置模式	ipv6 router ospf <i>process-id</i> [vrf <i>vrf-name</i>]	-
配置 OSPFv3 GR	nsf ietf	必选 缺省情况下，未启用 GR 功能 该功能生效，协议需支持 Opaque-LSA 功能，缺省支持 Opaque-LSA 功能
配置 OSPFv3 GR 周期	nsf interval <i>grace-period</i>	可选 缺省情况下，GR 周期为 95 秒

说明：

- OSPFv3 GR 功能只在堆叠环境或者存在双主控环境中能够使用。

配置 OSPFv3 GR Helper

GR Helper 协助 Restarter 端完成 GR，缺省情况下，设备都使能该功能，命令 **nsf ietf helper disable** 用来禁用 GR Helper 功能。命令 **nsf ietf helper strict-lsa-checking** 用来配置 Helper 端在 GR 过程中对 LSA 进行严格检查，若检查到 LSA 发生变化，则退出 GR Helper 模式。

表 42-32 配置 OSPFv3 GR Helper

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
进入 OSPFv3 配置模式	ipv6 router ospf <i>process-id</i> [vrf <i>vrf-name</i>]	-
配置 OSPFv3 GR Helper	nsf ietf helper [disable strict-lsa-checking]	可选 缺省情况下，使能 Helper 功能，不会对 LSA 进行严格检查

42.2.9 配置 OSPFv3 与 BFD 联动

-E -A

配置条件

在配置 OSPFv3 与 BFD 联动前，首先完成以下任务：

- 使能 IPv6 转发功能。
- 使能 OSPFv3 协议。

配置 OSPFv3 与 BFD 联动

BFD(Bidirectional Forwarding Detection，双向转发检测)提供一种快速检测两台设备之间线路状态的方法。当相邻的两台 OSPFv3 设备间启动 BFD 检测后，若设备之间发生线路故障，BFD 会快速检测到故障并通知 OSPFv3 协议，触发 OSPFv3 进行路由计算并切换到备份线路，达到路由快速切换的目的。

表 42-33 配置 OSPFv3 与 BFD 联动

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-

步骤	命令	说明
配置 OSPFv3 指定接口使能或禁用 BFD	ipv6 ospf bfd [disable] [instance-id instance-id]	必选 缺省情况下, 未使能 BFD 功能
进入全局配置模式	exit	-
进入 OSPFv3 配置模式	ipv6 router ospf process-id [vrf vrf-name]	-
配置 OSPFv3 进程的所有接口使能 BFD	bfd all-interfaces	可选

说明:

- 同时在 OSPFv3 配置模式、接口配置模式下配置 BFD 时, 接口下配置优先级较高。

42.2.10 OSPFv3 监控与维护

-E -A

表 42-34 OSPFv3 监控与维护

命令	说明
clear ipv6 ospf err-statistic	清除 OSPFv3 错误统计信息
clear ipv6 ospf [process-id] process	重置 OSPFv3 进程
clear ipv6 ospf [process-id] redistribution	重新通告外部路由

命令	说明
clear ipv6 ospf [<i>process-id</i>] route	重新计算 OSPFv3 路由
clear ipv6 ospf statistics [<i>interface-name</i>]	清除 OSPFv3 接口统计信息
show ipv6 ospf [<i>process-id</i>]	显示 OSPFv3 基本信息
show ipv6 ospf [<i>process-id</i>] border-routers	显示 OSPFv3 中到达边界设备的路由信息
show ipv6 ospf core-info	显示 OSPFv3 进程核心信息
show ipv6 ospf [<i>process-id</i>] database [database-summary external / inter-prefix inter-router intra-prefix link network nssa-external grace router adv-router <i>router-id</i> age <i>lsa_age</i> max-age self-originate]	显示 OSPFv3 数据库信息
show ipv6 ospf error-statistic	显示 OSPFv3 错误统计信息
show ipv6 ospf event-list	显示 OSPFv3 报文接收队列信息
show ipv6 ospf interface [<i>interface-name</i> [detail]]	显示 OSPFv3 接口信息
show ipv6 ospf [<i>process-id</i>] neighbor [<i>neighbor-id</i> / all / detail [all] interface <i>interface-name</i> [detail] statistics]	显示 OSPFv3 邻居信息

命令	说明
show ipv6 ospf [<i>process-id</i>] route [<i>ipv6-prefix/prefix-length</i> connected / external / inter-area / intra-area statistic]	显示 OSPFv3 路由信息
show ipv6 ospf [<i>process-id</i>] sham- links	显示配置的 OSPFv3 伪链接接口信息, 包括接口状态、cost 值、邻居状态
show ipv6 ospf [<i>process-id</i>] topology area [<i>area-id</i>]	显示 OSPFv3 拓扑信息
show ipv6 ospf [<i>process-id</i>] virtual-links	显示 OSPFv3 虚链接信息
show ipv6 ospf [vrf <i>vrf-name</i>]	显示指定 vrf 中所有 OSPFv3 进程信息和 参数
show running-config ipv6 router ospf	显示 OSPFv3 当前运行配置

42.3 OSPFv3 典型配置举例

42.3.1 配置 OSPFv3 基本功能

-E -A

网络需求

- 所有设备配置 OSPFv3 协议，划分区域 0、区域 1 和区域 2 三个区域。配置完成后，所有设备能相互学习路由。
- 在背靠背的以太接口上，为了加快 OSPFv3 邻居建立，可将 OSPFv3 接口网络类型改为点对点。修改区域 2 的接口网络类型为点到点，配置完成后，所有设备能相互学习路由。

网络拓扑

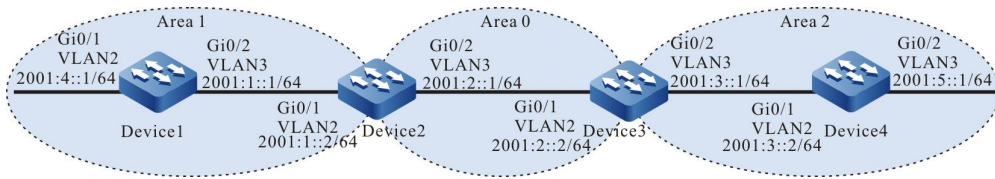


图 42-1 配置 OSPFv3 基本功能组网图

配置步骤

- 步骤 1: 配置 VLAN，并将端口加入对应的 VLAN。（略）
- 步骤 2: 配置各接口 IPv6 地址。（略）
- 步骤 3: 配置 OSPFv3 进程并将相应接口覆盖到不同区域中。

#配置 Device1，配置 OSPFv3 进程并将接口覆盖到区域 1 中。

```
Device1#configure terminal
Device1(config)#ipv6 router ospf 100
Device1(config-ospf6)#router-id 1.1.1.1
Device1(config-ospf6)#exit
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 router ospf 100 area 1
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan3
Device1(config-if-vlan3)#ipv6 router ospf 100 area 1
Device1(config-if-vlan3)#exit
```

#配置 Device2，配置 OSPFv3 进程并将相应接口覆盖到区域 0 和区域 1 中。

```
Device2#configure terminal
Device2(config)#ipv6 router ospf 100
Device2(config-ospf6)#router-id 2.2.2.2
Device2(config-ospf6)#exit
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ipv6 router ospf 100 area 1
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan3
Device2(config-if-vlan3)#ipv6 router ospf 100 area 0
Device2(config-if-vlan3)#exit
```

#配置 Device3，配置 OSPFv3 进程并将相应接口覆盖到区域 0 和区域 2 中。

```
Device3#configure terminal
Device3(config)#ipv6 router ospf 100
Device3(config-ospf6)#router-id 3.3.3.3
Device3(config-ospf6)#exit
Device3(config)#interface vlan2
Device3(config-if-vlan2)#ipv6 router ospf 100 area 0
Device3(config-if-vlan2)#exit
Device3(config)#interface vlan3
Device3(config-if-vlan3)#ipv6 router ospf 100 area 2
Device3(config-if-vlan3)#exit
```

#配置 Device4，配置 OSPFv3 进程并将接口覆盖到区域 2 中。

```
Device4#configure terminal
Device4(config)#ipv6 router ospf 100
Device4(config-ospf6)#router-id 4.4.4.4
Device4(config-ospf6)#exit
Device4(config)#interface vlan2
Device4(config-if-vlan2)#ipv6 router ospf 100 area 2
Device4(config-if-vlan2)#exit
Device4(config)#interface vlan3
Device4(config-if-vlan3)#ipv6 router ospf 100 area 2
Device4(config-if-vlan3)#exit
```

说明：

- 在 OSPFv3 中 Router ID 必须手工配置，而且必须保证自治系统中任意两台路由器的 Router ID 都不相同。
 - 接口使能到 OSPFv3 时，需要指定是哪个接口实例被使能到 OSPFv3 进程中，且两边实例号必须一致，默认在实例 0 中。
-

#查看 Device1 的 OSPFv3 邻居信息和路由表。

```
Device1#show ipv6 ospf neighbor
OSPFv3 Process (100)
Neighbor ID  Pri  State           Dead Time  Interface          Instance ID
2.2.2.2      1  Full/DR        00:00:38   vlan3              0
```

```
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
```

```
L  ::1/128 [0/0]
   via ::, 00:41:07, lo0
C  2001:1::/64 [0/0]
   via ::, 00:32:19, vlan3
L  2001:1::1/128 [0/0]
   via ::, 00:32:18, lo0
O  2001:2::/64 [110/2]
   via fe80::201:7aff:fe5e:6d45, 00:23:06, vlan3
O  2001:3::/64 [110/3]
   via fe80::201:7aff:fe5e:6d45, 00:23:00, vlan3
C  2001:4::/64 [0/0]
   via ::, 00:16:46, vlan2
L  2001:4::1/128 [0/0]
   via ::, 00:16:45, lo0
O  2001:5::/64 [110/4]
   via fe80::201:7aff:fe5e:6d45, 00:01:42, vlan3
```

#查看 Device2 的 OSPFv3 邻居和路由表。

```
Device2#show ipv6 ospf neighbor
OSPFv3 Process (100)
```

单播路由

```
Neighbor ID Pri State Dead Time Interface Instance ID
1.1.1.1 1 Full/Backup 00:00:34 vlan2 0
3.3.3.3 1 Full/DR 00:00:33 vlan3 0
```

```
Device2#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management
```

```
L ::1/128 [0/0]
via ::, 00:50:36, lo0
C 2001:1::/64 [0/0]
via ::, 00:43:05, vlan2
L 2001:1::2/128 [0/0]
via ::, 00:43:04, lo0
C 2001:2::/64 [0/0]
via ::, 00:40:01, vlan3
L 2001:2::1/128 [0/0]
via ::, 00:39:57, lo0
O 2001:3::/64 [110/2]
via fe80::2212:1ff:fe01:101, 00:34:00, vlan3
O 2001:4::/64 [110/2]
via fe80::201:7aff:fe61:7a24, 00:27:28, vlan2
O 2001:5::/64 [110/3]
via fe80::2212:1ff:fe01:101, 00:12:41, vlan3
```

#查看 Device2 的 OSPFv3 LSDB (链路状态数据库)。

```
Device2#show ipv6 ospf database

OSPFv3 Router with ID (2.2.2.2) (Process 100)

Link-LSA (Interface vlan2)
Link State ID ADV Router Age Seq# CkSum Prefix
0.0.0.1 1.1.1.1 81 0x80000001 0x8d18 1
0.0.0.1 2.2.2.2 78 0x80000001 0xf996 1

Link-LSA (Interface vlan3)
Link State ID ADV Router Age Seq# CkSum Prefix
0.0.0.2 2.2.2.2 71 0x80000003 0x2467 1
0.0.0.1 3.3.3.3 35 0x80000003 0xcd12 1

Router-LSA (Area 0.0.0.0)
Link State ID ADV Router Age Seq# CkSum Link
0.0.0.0 2.2.2.2 37 0x80000004 0x0dd6 1
0.0.0.0 3.3.3.3 25 0x80000007 0xda03 1

Network-LSA (Area 0.0.0.0)
Link State ID ADV Router Age Seq# CkSum
0.0.0.1 3.3.3.3 35 0x80000001 0x5790

Inter-Area-Prefix-LSA (Area 0.0.0.0)
Link State ID ADV Router Age Seq# CkSum Prefix
0.0.0.2 2.2.2.2 42 0x80000007 0x9e25 2001:1::/64
0.0.0.3 2.2.2.2 23 0x80000002 0xcef4 2001:4::/64
0.0.0.1 3.3.3.3 35 0x80000005 0xaa16 2001:3::/64
0.0.0.3 3.3.3.3 55 0x80000001 0xc0fe 2001:5::/64

Intra-Area-Prefix-LSA (Area 0.0.0.0)
Link State ID ADV Router Age Seq# CkSum Prefix Reference
0.0.0.3 3.3.3.3 34 0x80000001 0xb2d3 1 Network-LSA
```



```
Router-LSA (Area 0.0.0.1)
Link State ID  ADV Router   Age Seq#    CkSum  Link
0.0.0.0       1.1.1.1    41 0x80000004 0xc726  1
0.0.0.0       2.2.2.2    37 0x80000004 0xac3c  1
```

```
Network-LSA (Area 0.0.0.1)
Link State ID  ADV Router   Age Seq#    CkSum
0.0.0.1       2.2.2.2    42 0x80000001 0x21d2
```

```
Inter-Area-Prefix-LSA (Area 0.0.0.1)
Link State ID  ADV Router   Age Seq#    CkSum Prefix
0.0.0.1       2.2.2.2    42 0x80000004 0xbc0a 2001:2::/64
0.0.0.4       2.2.2.2    19 0x80000001 0xb80c 2001:3::/64
0.0.0.5       2.2.2.2    19 0x80000001 0xd0ef 2001:5::/64
```

```
Intra-Area-Prefix-LSA (Area 0.0.0.1)
Link State ID  ADV Router   Age Seq#    CkSum Prefix Reference
0.0.0.1       1.1.1.1    35 0x80000005 0xc4ce  1 Router-LSA
0.0.0.3       2.2.2.2    41 0x80000001 0x8807  1 Network-LSA
```

对 Device2 来说，2001:3::/64 和 2001:5::/64 是区域间路由，从 Inter-Area-Prefix-LSA (Area 0.0.0.0)中可看到相关路由 LSA 信息；如果是区域内路由，则需要 show ipv6 ospf database intra-prefix 才能看到相关路由 LSA 信息。

步骤 4： 配置 OSPFv3 接口网络类型为点对点。

#配置 Device3，将接口 vlan3 的 OSPFv3 网络类型改为点到点。

```
Device3(config)#interface vlan3
Device3(config-if-vlan3)#ipv6 ospf network point-to-point
Device3(config-if-vlan3)#exit
```

#配置 Device4，将接口 vlan2 的 OSPFv3 网络类型改为点到点。

```
Device4(config)#interface vlan2
Device4(config-if-vlan2)#ipv6 ospf network point-to-point
Device4(config-if-vlan2)#exit
```

步骤 5： 检验结果。

#查看 Device3 的 OSPFv3 邻居和路由表。

```
Device3#show ipv6 ospf neighbor
OSPFv3 Process (100)
Neighbor ID  Pri  State      Dead Time  Interface      Instance ID
2.2.2.2     1   Full/Backup 00:00:39  vlan2          0
4.4.4.4     1   Full/-      00:00:39  vlan3          0
```

```
Device3#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
```

```
L ::1/128 [0/0]
```

单播路由

```
via ::, 1d:09:10:10, lo0
O 2001:1::/64 [110/2]
  via fe80::201:7aff:fe5e:6d46, 02:07:25, vlan2
C 2001:2::/64 [0/0]
  via ::, 03:07:51, vlan2
L 2001:2::2/128 [0/0]
  via ::, 03:07:48, lo0
C 2001:3::/64 [0/0]
  via ::, 03:07:41, vlan3
L 2001:3::1/128 [0/0]
  via ::, 03:07:39, lo0
O 2001:4::/64 [110/3]
  via fe80::201:7aff:fe5e:6d46, 02:07:25, vlan2
O 2001:5::/64 [110/2]
  via fe80::201:2ff:fe03:405, 00:00:22, vlan3
```

说明:

- 点对点网络建立 OSPFv3 邻接时，不会进行 DR 和 BDR 选举。
-

#查看 Device4 的 OSPFv3 邻居和路由表。

```
Device4#show ipv6 ospf neighbor
OSPFv3 Process (100)
Neighbor ID  Pri  State           Dead Time  Interface        Instance ID
3.3.3.3      1   Full/-         00:00:38  vlan2            0

Device4#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 00:05:34, lo0
O 2001:1::/64 [110/3]
  via fe80::2212:1ff:fe01:102, 00:03:12, vlan2
O 2001:2::/64 [110/2]
  via fe80::2212:1ff:fe01:102, 00:03:12, vlan2
C 2001:3::/64 [0/0]
  via ::, 00:04:34, vlan2
L 2001:3::2/128 [0/0]
  via ::, 00:04:31, lo0
O 2001:4::/64 [110/4]
  via fe80::2212:1ff:fe01:102, 00:03:12, vlan2
C 2001:5::/64 [0/0]
  via ::, 00:03:14, vlan3
L 2001:5::1/128 [0/0]
  via ::, 00:03:13, lo0
```

可以看到，修改 OSPFv3 接口网络类型为点对点后，邻居能够正常建立，且能够正常学到路由。

网络需求

- 所有的路由器都运行 OSPFv3，整个自治系统划分为 2 个区域。
- Device1，Device2，Device3 使用 IPSec 隧道对 OSPFv3 协议报文进行加密认证，Device1 与 Device2 采用 ESP 传输封装方式，加密算法为 3des，认证算法为 sha1，Device2 与 Device3 采用 ESP 传输封装方式，加密算法为 aes128，ESP 认证算法为 sm3。
- 配置完成后，设备能够正常建立邻居并相互学习路由。

网络拓扑

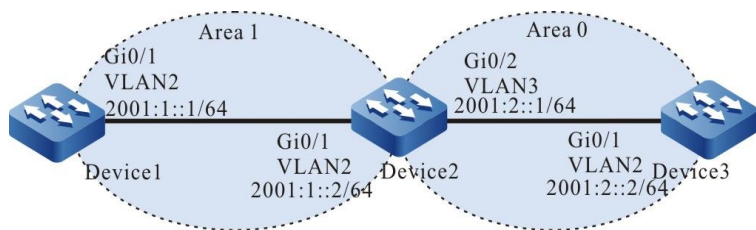


图 42-2 配置 OSPFv3 使用 IPSec 加密认证组网图

配置步骤

步骤 1：配置各接口 IPv6 地址。（略）

步骤 2：配置 OSPFv3 进程，在相应接口启用 OSPFv3 功能。

#配置 Device1，Device2，Device3 的 OSPFv3 进程，并在接口使能 OSPFv3。

```
Device1#configure terminal
Device1(config)#ipv6 router ospf 100
Device1(config-ospf6)#router-id 1.1.1.1
Device1(config-ospf6)#exit
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 router ospf 100 area 1
Device1(config-if-vlan2)#exit
```

```
Device2#configure terminal
Device2(config)#ipv6 router ospf 100
Device2(config-ospf6)#router-id 2.2.2.2
Device2(config-ospf6)#exit
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ipv6 router ospf 100 area 1
Device2(config-if-vlan2)#exit
```

配置手册

单播路由

```
Device2(config)#interface vlan3
Device2(config-if- vlan3)#ipv6 router ospf 100 area 0
Device2(config-if- vlan3)#exit
```

```
Device3#configure terminal
Device3(config)#ipv6 router ospf 100
Device3(config-ospf6)#router-id 3.3.3.3
Device3(config-ospf6)#exit
Device3(config)#interface vlan2
Device3(config-if-vlan2)#ipv6 router ospf 100 area 0
Device3(config-if-vlan2)#exit
```

步骤 3: 配置 IPsec 提议和手工隧道。

#配置 Device1, 创建 IPsec 提议 a, 采用 ESP 传输封装方式, 加密算法 3des, 认证算法 sha1, 创建 IPsec 手工隧道 a, 配置 SPI 和密钥。

```
Device1(config)#crypto ipsec proposal a
Device1(config-ipsec-prop)#mode transport
Device1(config-ipsec-prop)#esp 3des sha1
Device1(config-ipsec-prop)#exit
Device1(config)#crypto tunnel a manual
Device1(config-manual-tunnel)#set ipsec proposal a
Device1(config-manual-tunnel)#set inbound esp 1000 encryption 0 11111111111111111111 authentication
0 aaaaaaaaaaaaaaaaaaaaaa
Device1(config-manual-tunnel)#set outbound esp 1001 encryption 0 aaaaaaaaaaaaaaaaaaaaaa authentication
0 11111111111111111111
Device1(config-manual-tunnel)#exit
```

#配置 Device2, 创建 IPsec 提议 a, 采用 ESP 传输封装方式, 加密算法 3des, 认证算法 sha1, 创建 IPsec 手工隧道 a, 配置 SPI 和密钥; 创建 IPsec 提议 b, 采用 ESP 传输封装方式, 加密算法 aes128, 认证算法 sm3, 创建 IPsec 手工隧道 b, 配置 SPI 和密钥。

```
Device2(config)#crypto ipsec proposal a
Device2(config-ipsec-prop)#mode transport
Device2(config-ipsec-prop)#esp 3des sha1
Device2(config-ipsec-prop)#exit
Device2(config)#crypto tunnel a manual
Device2(config-manual-tunnel)#set ipsec proposal a
Device2(config-manual-tunnel)#set inbound esp 1001 encryption 0 aaaaaaaaaaaaaaaaaaaaaa authentication 0
11111111111111111111
Device2(config-manual-tunnel)#set outbound esp 1000 encryption 0 11111111111111111111 authentication
0 aaaaaaaaaaaaaaaaaaaaaa
Device2(config-manual-tunnel)#exit
Device2(config)#crypto ipsec proposal b
Device2(config-ipsec-prop)#mode transport
Device2(config-ipsec-prop)#esp aes128 sm3
Device2(config-ipsec-prop)#exit
Device2(config)#crypto tunnel b manual
Device2(config-manual-tunnel)#set ipsec proposal b
Device2(config-manual-tunnel)#set inbound esp 2001 encryption 0 1111111111111111 authentication 0 aaaaaa
aaaaaaaaaaaaaaaaaaaaa
Device2(config-manual-tunnel)#set outbound esp 2000 encryption 0 1111111111111111 authentication 0 11111
11111111111111111111
Device2(config-manual-tunnel)#exit
```

#配置 Device3, 创建 IPsec 提议 b, 采用 ESP 传输封装方式, 加密算法 aes128, 认证算法 sm3, 创建 IPsec 手工隧道 b, 配置 SPI 和密钥。

单播路由

```
Device3(config)#crypto ipsec proposal b
Device3(config-ipsec-prop)#mode transport
Device3(config-ipsec-prop)#esp aes128 sm3
Device3(config-ipsec-prop)#exit
Device3(config)#crypto tunnel b manual
Device3(config-manual-tunnel)#set ipsec proposal b
Device3(config-manual-tunnel)#set inbound esp 2000 encryption 0 1111111111111111 authentication 0 1111111
11111111111111111111111111111111
Device3(config-manual-tunnel)#set outbound esp 2001 encryption 0 1111111111111111 authentication 0 aaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaa
Device3(config-manual-tunnel)#exit
```

步骤 4: 在 OSPFv3 进程中各区域绑定相应的 IPsec 隧道。

#在 Device1 的 OSPFv3 进程中, 区域 1 绑定 IPsec 隧道 a。

```
Device1(config)#ipv6 router ospf 100
Device1(config-ospf6)#area 1 ipsec-tunnel a
Device1(config-ospf6)#exit
```

#在 Device2 的 OSPFv3 进程中, 区域 1 绑定 IPsec 隧道 a, 区域 0 绑定 IPsec 隧道 b。

```
Device2(config)#ipv6 router ospf 100
Device2(config-ospf6)#area 1 ipsec-tunnel a
Device2(config-ospf6)#area 0 ipsec-tunnel b
Device1(config-ospf6)#exit
```

#在 Device3 的 OSPFv3 进程中, 区域 0 绑定 IPsec 隧道 b。

```
Device3(config)#ipv6 router ospf 100
Device3(config-ospf6)#area 0 ipsec-tunnel b
Device3(config-ospf6)#exit
```

步骤 5: 检验结果。

#查看 Device1 的 OSPFv3 进程信息。

```
Device1#show ipv6 ospf 100
Routing Process "OSPFv3 (100)" with ID 1.1.1.1
Process bound to VRF default
IETF graceful-restarter support disabled
IETF gr helper support enabled
Initial SPF schedule delay 5000 msec
Minimum hold time between two consecutive SPFs 10000 msec
Maximum wait time between two consecutive SPFs 10000 msec
Minimum LSA interval 5 secs, Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x0000
Number of AS-Scoped Unknown LSA 0
Number of LSA originated 5
Number of LSA received 5
Number of areas in this router is 1
Not Support Demand Circuit lsa number is 0
Autonomy system support flood DoNotAge Lsa
Area 0.0.0.1
Number of interfaces in this area is 1
IPSec Tunnel Name:a , ID: 154
Number of fully adjacent neighbors in this area is 1
Number of fully adjacent sham-link neighbors in this area is 0
Number of fully adjacent virtual neighbors through this area is 0
SPF algorithm executed 4 times
LSA walker due in 00:00:02
Number of LSA 4. Checksum Sum 0x2FC53
```

单播路由

```
Number of Unknown LSA 0
Not Support Demand Circuit lsa number is 0
Indication lsa (by other routers) number is: 0,
area support flood DoNotAge lsa
```

可以看到，区域绑定 IPsec 隧道 a，ID 是 0~1023 之间的随机值。

#查看 Device1 的 IPsec 隧道信息。

```
Device1#show crypto tunnel a
get the manual tunnel
Crypto tunnel a : MANUAL
  policy name : (null)
  peer address :
  local interface : (null) address :
  ipsec proposal : a
  Inbound :
    esp spi: 1000 encryption key: ***** authentication key: *****
    ah spi: 0 authentication key: (null)
  Outbound :
    esp spi: 1001 encryption key: ***** authentication key: *****
    ah spi: 0 authentication key: (null)
  route ref : 1
  route asyn : 1
  route rt_id : 154
```

可以看到，route rt_id 与 show ipv6 ospf 100 中的 ID 相等。

#查看 Device1 的 IPsec 隧道加密类型信息。

```
Device1#show crypto ipsec sa tunnel a
route policy:
the pairs of ESP ipsec sa : id :0 , algorithm : 3DES HMAC-SHA1-96
  inbound esp ipsec sa : spi : 0x3e8(1000) crypto m_context(s_context) : 0x4cd3ba78 / 0x4cd3bae0
    current input 26 packets, 2 kbytes
    encapsulation mode : Transport
    replay protection : OFF
    remaining lifetime (seconds/kbytes) : 0/0
    uptime is 0 hour 4 minute 45 second
  outbound esp ipsec sa : spi : 0x3e9(1001) crypto m_context(s_context) : 0x4cd3bb48 / 0x4cd3bbb0
    current output 39 packets, 3 kbytes
    encapsulation mode : Transport
    replay protection : OFF
    remaining lifetime (seconds/kbytes) : 0/0
    uptime is 0 hour 4 minute 45 second
```

total sa and sa group is 1

可以看到，IPsec 隧道 a 采用 ESP 的传输封装方式，加密算法为 3des，认证算法为 sha1。

#查看 Device1 的 OSPFv3 的接口信息。

```
Device1#show ipv6 ospf interface vlan2
vlan2 is up, line protocol is up
Interface ID 50331913
IPv6 Prefixes
  fe80::201:7aff:fe80:10 (Link-Local Address)
  2001::1::1/64
Interface ID 13
OSPFv3 Process (100), Area 0.0.0.1, Instance ID 0, Enabled 00:41:10, MTU 1500
Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
IPsec tunnel(Area):a, ID:154
Transmit Delay is 1 sec, State Backup, 3 state change, Priority 1
Designated Router (ID) 2.2.2.2
```

单播路由

```
Interface Address fe80::200:1ff:fe7a:adf0
Backup Designated Router (ID) 1.1.1.1
Interface Address fe80::201:7aff:fecf:fbec
Timer interval configured, Hello 10, Dead 39, Wait 39, Retransmit 5
Hello due in 00:00:06
Neighbor Count is 1, Adjacent neighbor count is 1
Hello received 2 sent 3, DD received 3 sent 4
LS-Req received 1 sent 1, LS-Upd received 5 sent 3
LS-Ack received 3 sent 2, Discarded 0
```

可以看到，接口绑定 IPsec 隧道 a，ID 是 0~1023 之间的随机值。

#查看 Device1 的 OSPFv3 邻居信息和核心路由表。

```
Device1#show ipv6 ospf neighbor
OSPFv3 Process (100)
Neighbor ID Pri State Dead Time Interface Instance ID
2.2.2.2 1 Full/DR 00:00:39 vlan2 0
```

```
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management
```

```
L ::1/128 [0/0]
via ::, 4d:04:06:36, lo0
C 2001:1::/64 [0/0]
via ::, 03:00:53, vlan2
L 2001:1::1/128 [0/0]
via ::, 03:00:49, lo0
O 2001:2::/64 [110/2]
via fe80::201:7aff:fec9:1cdd, 2d:00:03:49, vlan2
```

Device1 上，邻居正常建立，路由学习正常。

#查看 Device3 的 OSPFv3 进程信息。

```
Device3#show ipv6 ospf 100
Routing Process "OSPFv3 (100)" with ID 3.3.3.3
Process bound to VRF default
IETF graceful-restarter support disabled
IETF gr helper support enabled
Initial SPF schedule delay 5000 msec
Minimum hold time between two consecutive SPF's 10000 msec
Maximum wait time between two consecutive SPF's 10000 msec
Minimum LSA interval 5 secs, Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x0000
Number of AS-Scoped Unknown LSA 0
Number of LSA originated 5
Number of LSA received 6
Number of areas in this router is 1
Not Support Demand Circuit lsa number is 0
Autonomy system support flood DoNotAge Lsa
Area BACKBONE(0)
Number of interfaces in this area is 1
IPSec Tunnel Name:b , ID: 2
Number of fully adjacent neighbors in this area is 1
Number of fully adjacent sham-link neighbors in this area is 0
SPF algorithm executed 4 times
LSA walker due in 00:00:02
Number of LSA 4. Checksum Sum 0x24272
Number of Unknown LSA 0
Not Support Demand Circuit lsa number is 0
Indication lsa (by other routers) number is: 0,
area support flood DoNotAge Lsa
```

可以看到，区域绑定 IPsec 隧道 b，ID 是 0~1023 之间的随机值。

#查看 Device3 的 IPsec 隧道信息。

```
Device3#show crypto tunnel b
get the manual tunnel
Crypto tunnel b : MANUAL
  policy name : (null)
  peer address :
  local interface : (null) address :
  Ipsec proposal : b
  Inbound :
    esp spi: 2000 encryption key: ***** authentication key: *****
    ah spi: 0 authentication key: (null)
  Outbound :
    esp spi: 2001 encryption key: ***** authentication key: *****
    ah spi: 0 authentication key: (null)
  route ref : 1
  route asyn : 1
  route rt_id : 2
```

可以看到，route rt_id 与 show ipv6 ospf 100 中的 ID 相等。

#查看 Device3 的 IPsec 隧道加密类型信息。

```
Device3#show crypto ipsec sa tunnel b
route policy:
  the pairs of ESP ipsec sa : id : 0, algorithm : AES128 HMAC-SM3
  inbound esp ipsec sa : spi : 0x7d0(2000) crypto m_context(s_context) : 0x6a0d9a98 /
  0x6a0d9a30
  current input 53 packets, 5 kbytes
  encapsulation mode : Transport
  replay protection : OFF
  remaining lifetime (seconds/kbytes) : 0/0
  uptime is 0 hour 6 minute 40 second
  outbound esp ipsec sa : spi : 0x7d1(2001) crypto m_context(s_context) : 0x6a0d99c8 /
  0x6a0d9960
  current output 52 packets, 5 kbytes
  encapsulation mode : Transport
  replay protection : OFF
  remaining lifetime (seconds/kbytes) : 0/0
  uptime is 0 hour 6 minute 40 second
```

total sa and sa group is 1

可以看到，IPsec 隧道采用 ESP 传输封装方式，加密算法为 aes128,认证算法为 sm3。

#查看 Device3 的 OSPFv3 的接口信息。

```
Device3#show ipv6 ospf interface vlan2
vlan2 is up, line protocol is up
Interface ID 50331899
IPv6 Prefixes
  fe80::200:1ff:fe7a:adf0/10 (Link-Local Address)
  2001::2::1/64
Interface ID 9
OSPFv3 Process (100), Area 0.0.0.1, Instance ID 0, Enabled 00:50:39, MTU 1500
Router ID 3.3.3.3, Network Type BROADCAST, Cost: 1
IPSec tunnel(Area):b, ID:2
Transmit Delay is 1 sec, State DR, 4 state change, Priority 1
Designated Router (ID) 2.2.2.2
  Interface Address fe80::200:1ff:fe7a:adf0
Backup Designated Router (ID) 1.1.1.1
  Interface Address fe80::201:7aff:fecf:fbec
```


单播路由

```
Timer interval configured, Hello 10, Dead 39, Wait 39, Retransmit 5
Hello due in 00:00:02
Neighbor Count is 1, Adjacent neighbor count is 1
Hello received 272 sent 316, DD received 12 sent 9
LS-Req received 3 sent 5, LS-Upd received 19 sent 18
LS-Ack received 11 sent 13, Discarded 0
```

可以看到，接口绑定 IPsec 隧道 b，ID 是 0~1023 之间的随机值。

#查看 Device3 的 OSPFv3 邻居信息和核心路由表。

```
Device3#show ipv6 ospf neighbor
OSPFv3 Process (100)
Neighbor ID Pri State Dead Time Interface Instance ID
2.2.2.2 1 Full/Backup 00:00:35 vlan2 0
```

```
Device3#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management
```

```
L ::1/128 [0/0]
via ::, 09:53:53, lo0
O 2001:1::/64 [110/2]
via fe80::ae9c:e4ff:fe77:889e, 00:23:36, vlan2
C 2001:2::/64 [0/0]
via ::, 03:05:16, vlan2
L 2001:2::2/128 [0/0]
via ::, 03:05:13, lo0
```

Device3 上，邻居正常建立，路由学习正常。

步骤 6： 在 OSPFv3 接口绑定相应的 IPsec 隧道。

#配置 Device1，接口 vlan2 绑定 IPsec 隧道 a。

```
Device1(config)#interface vlan2
Device1(config-if- vlan2)#ipv6 ospf ipsec-tunnel a
Device1(config-if- vlan2)#exit
```

#配置 Device2，接口 vlan2 绑定 IPsec 隧道 a；接口 vlan3 绑定 IPsec 隧道 b。

```
Device2(config)#interface vlan2
Device2(config-if- vlan2)#ipv6 ospf ipsec-tunnel a
Device2(config-if- vlan2)#exit
Device2(config)#interface vlan3
Device2(config-if-vlan3)#ipv6 ospf ipsec-tunnel b
Device2(config-if-vlan3)#exit
```

#配置 Device3，接口 vlan2 绑定 IPsec 隧道 b。

```
Device3(config)#interface vlan2
Device3(config-if- vlan2)#ipv6 ospf ipsec-tunnel b
Device3(config-if- vlan2)#exit
```

步骤 7： 检验结果。

#查看 Device1 的 OSPFv3 的接口信息。

单播路由

```
Device1#show ipv6 ospf interface vlan2
vlan2 is up, line protocol is up
Interface ID 50331913
IPv6 Prefixes
  fe80::201:7aff:fe7a:adf0/10 (Link-Local Address)
  2001:1::1/64
Interface ID 13
OSPFv3 Process (100), Area 0.0.0.1, Instance ID 0, Enabled 00:41:10, MTU 1500
Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
IPSec tunnel:a, ID:154
Transmit Delay is 1 sec, State Backup, 3 state change, Priority 1
Designated Router (ID) 2.2.2.2
  Interface Address fe80::200:1ff:fe7a:adf0
Backup Designated Router (ID) 1.1.1.1
  Interface Address fe80::201:7aff:fe7a:adf0
Timer interval configured, Hello 10, Dead 39, Wait 39, Retransmit 5
Hello due in 00:00:06
Neighbor Count is 1, Adjacent neighbor count is 1
Hello received 2 sent 3, DD received 3 sent 4
LS-Req received 1 sent 1, LS-Upd received 5 sent 3
LS-Ack received 3 sent 2, Discarded 0
```

可以看到，接口绑定 IPSec 隧道 a，ID 是 0~1023 之间的随机值。

#查看 Device1 的 OSPFv3 核心路由表。

```
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 4d:04:06:36, lo0
C 2001:1::/64 [0/0]
  via ::, 03:00:53, vlan2
L 2001:1::1/128 [0/0]
  via ::, 03:00:49, lo0
O 2001:2::/64 [110/2]
  via fe80::201:7aff:fe7a:adf0, 2d:00:03:49, vlan2
```

Device1 上，路由学习正常。

#查看 Device3 的 OSPFv3 的接口信息。

```
Device3#show ipv6 ospf interface vlan2
vlan2 is up, line protocol is up
Interface ID 50331899
IPv6 Prefixes
  fe80::200:1ff:fe7a:adf0/10 (Link-Local Address)
  2001:2::1/64
Interface ID 9
OSPFv3 Process (100), Area 0.0.0.1, Instance ID 0, Enabled 00:50:39, MTU 1500
Router ID 3.3.3.3, Network Type BROADCAST, Cost: 1
IPSec tunnel:b, ID:2
Transmit Delay is 1 sec, State DR, 4 state change, Priority 1
Designated Router (ID) 2.2.2.2
  Interface Address fe80::200:1ff:fe7a:adf0
Backup Designated Router (ID) 1.1.1.1
  Interface Address fe80::201:7aff:fe7a:adf0
Timer interval configured, Hello 10, Dead 39, Wait 39, Retransmit 5
Hello due in 00:00:02
Neighbor Count is 1, Adjacent neighbor count is 1
Hello received 272 sent 316, DD received 12 sent 9
LS-Req received 3 sent 5, LS-Upd received 19 sent 18
LS-Ack received 11 sent 13, Discarded 0
```

单播路由

可以看到，接口绑定 IPsec 隧道 b，ID 是 0~1023 之间的随机值。

#查看 Device3 的 OSPFv3 核心路由表。

```
Device3#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
```

```
L ::1/128 [0/0]
  via ::, 09:53:53, lo0
O 2001:1::/64 [110/2]
  via fe80::ae9c:e4ff:fe77:889e, 00:23:36, vlan2
C 2001:2::/64 [0/0]
  via ::, 03:05:16, vlan2
L 2001:2::2/128 [0/0]
  via ::, 03:05:13, lo0
```

Device3 上，路由学习正常。

说明：

- 配置 OSPFv3 绑定 IPsec 隧道时，可以只配置区域绑定或者只配置接口绑定，也可以同时配置区域和接口绑定。
- 区域绑定和接口绑定同时配置 IPsec 隧道时，接口绑定优先生效。

42.3.3 配置 OSPFv3 与 BFD 的联动 -E -A

网络需求

- 所有设备配置 OSPFv3 协议。
- Device1 和 Device3 间的线路使能 BFD 检测功能，当线路出现故障时，BFD 会快速检测到故障并通知 OSPFv3，OSPFv3 将路由切换 Device2 进行通信。

网络拓扑

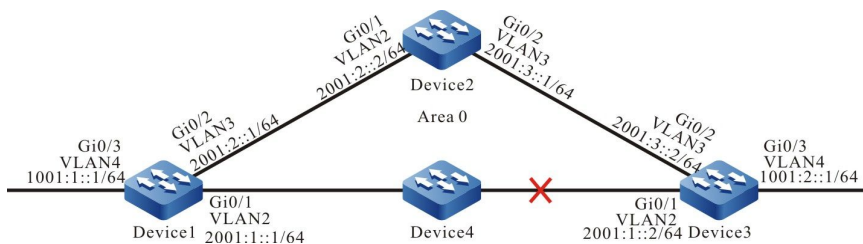


图 42-3 配置 OSPFv3 与 BFD 联动组网图

配置步骤

步骤 1: 配置 VLAN, 并将端口加入对应的 VLAN。 (略)

步骤 2: 配置各接口 IPv6 地址。 (略)

步骤 3: 配置 OSPFv3 进程。

#配置 Device1。

```
Device1#configure terminal
Device1(config)#ipv6 router ospf 100
Device1(config-ospf6)#router-id 1.1.1.1
Device1(config-ospf6)#exit
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 router ospf 100 area 0
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan3
Device1(config-if-vlan3)#ipv6 router ospf 100 area 0
Device1(config-if-vlan3)#exit
Device1(config)#interface vlan4
Device1(config-if-vlan4)#ipv6 router ospf 100 area 0
Device1(config-if-vlan4)#exit
```

#配置 Device2。

```
Device2#configure terminal
Device2(config)#ipv6 router ospf 100
Device2(config-ospf6)#router-id 2.2.2.2
Device2(config-ospf6)#exit
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ipv6 router ospf 100 area 0
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan3
Device2(config-if-vlan3)#ipv6 router ospf 100 area 0
Device2(config-if-vlan3)#exit
```

#配置 Device3。

```
Device3#configure terminal
Device3(config)#ipv6 router ospf 100
Device3(config-ospf6)#router-id 3.3.3.3
Device3(config-ospf6)#exit
Device3(config)#interface vlan2
Device3(config-if-vlan2)#ipv6 router ospf 100 area 0
Device3(config-if-vlan2)#exit
Device3(config)#interface vlan3
Device3(config-if-vlan3)#ipv6 router ospf 100 area 0
Device3(config-if-vlan3)#exit
Device3(config)#interface vlan4
Device3(config-if-vlan4)#ipv6 router ospf 100 area 0
Device3(config-if-vlan4)#exit
```

步骤 4: 配置 OSPFv3 与 BFD 联动。

#配置 Device1。

单播路由

```
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 ospf bfd
Device1(config-if-vlan2)#exit
```

#配置 Device3。

```
Device3(config)#interface vlan2
Device3(config-if-vlan2)#ipv6 ospf bfd
Device3(config-if-vlan2)#exit
```

步骤 5: 检验结果。

#查看 Device1 的 OSPFv3 邻居信息和路由表。

```
Device1#show ipv6 ospf neighbor 3.3.3.3
OSPFv3 Process (100)

Neighbor 3.3.3.3,interface address fe80::2212:1ff:fe01:104
In the area 0.0.0.0 via interface vlan4, BFD enabled
DR is 3.3.3.3 BDR is 1.1.1.1
Neighbor priority is 1, State is Full, 6 state changes
Options is 0x13 (-[R]-[E]V6)
Dead timer due in 00:00:37
Neighbor is up for 00:01:31
Database Summary List 0
Link State Request List 0
Link State Retransmission List 0
Thread Inactivity Timer on
Thread Database Description Retransmission off, 0 times
Thread Link State Request Retransmission off, 0 times
Thread Link State Update Retransmission off, 0 times

Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 01:15:27, lo0
C 1001:1::/64 [0/0]
  via ::, 01:15:27, vlan4
L 1001:1::1/128 [0/0]
  via ::, 01:15:27, lo0
O 1001:2::/64 [110/2]
  via fe80::2212:1ff:fe01:104, 00:02:40, vlan2
C 2001:1::/64 [0/0]
  via ::, 01:15:27, vlan2
L 2001:1::1/128 [0/0]
  via ::, 01:15:27, lo0
C 2001:2::/64 [0/0]
  via ::, 01:15:27, vlan3
L 2001:2::1/128 [0/0]
  via ::, 01:15:27, lo0
O 2001:3::/64 [110/2]
  via fe80::201:7aff:fe5e:6d45, 00:02:40, vlan3
  [110/2]
  via fe80::2212:1ff:fe01:104, 00:02:40, vlan2
```

从 OSPFv3 邻居信息中看到 BFD 已经使能，路由 1001:2::/64 优选 Device1 和 Device3 之间的线路进行通信。

#查看 Device1 的 BFD 会话信息。

```
Device1#show bfd session ipv6 detail
Total ipv6 session number: 1
OurAddr          NeighAddr          State   Holddown  Interface
fe80::201:7aff:fe61:7a25   fe80::2212:1ff:fe01:104   UP      5000      vlan2
Type:ipv6 direct
Local State:UP Remote State:UP Up for: 0h:0m:4s Number of times UP:1
Local Discriminator:5 Remote Discriminator:95
Send Interval:1000ms Detection time:5000ms(1000ms*5)
Local Diag:0 Demand mode:0 Poll bit:0
MinTxInt:1000 MinRxInt:1000 Multiplier:5
Remote MinTxInt:1000 Remote MinRxInt:1000 Remote Multiplier:5
Registered protocols:OSPFv3
```

可以看到 OSPFv3 与 BFD 联动成功，会话正常建立。

#Device1 和 Device3 之间的线路出现故障后，BFD 会快速检测到故障并通知 OSPFv3，OSPFv3 将路由切换到 Device2 上进行通信，查看 Device1 的路由表。

```
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L  ::1/128 [0/0]
   via ::, 01:16:10, lo0
C  1001:1::/64 [0/0]
   via ::, 01:16:10, vlan4
L  1001:1::1/128 [0/0]
   via ::, 01:16:10, lo0
O  1001:2::/64 [110/3]
   via fe80::201:7aff:fe5e:6d45, 00:00:07, vlan3
C  2001:1::/64 [0/0]
   via ::, 01:16:10, vlan2
L  2001:1::1/128 [0/0]
   via ::, 01:16:10, lo0
C  2001:2::/64 [0/0]
   via ::, 01:16:10, vlan3
L  2001:2::1/128 [0/0]
   via ::, 01:16:10, lo0
O  2001:3::/64 [110/2]
   via fe80::201:7aff:fe5e:6d45, 00:03:22, vlan3
```

Device3 的行为和 Device1 类似。

43 IS-IS

43.1 IS-IS 简介

IS-IS (Intermediate System to Intermediate System, 中间系统到中间系统) 是基于 SPF 算法的内部网关路由协议 (IGP)。IS-IS 协议的基本设计思想与算法和 OSPF 基本一致。IS-IS 协议是基于链路层的路由协议, 与网络层 (IPv4, IPv6, OSI) 无关, 不受网络层所约束, 因此有很好的扩展性。

IS-IS 协议能够同时支持多个协议栈的路由, 包括 IPv4、IPv6、OSI。IS-IS 协议最初是应用在 OSI 协议栈中 (ISO10589), 后来经过扩展用于 IPv4 协议栈 (RFC1195) 和 IPv6 协议栈 (RFC5308) 的路由。同时, 经过扩展能够支持 MPLS-TE (RFC3784) 的 CSPF 计算。

IS-IS 协议有兼容性好 (不同设备间实现的扩展功能不一致也可以很好的兼容)、网络容量大、同时支持多协议栈、能够平滑升级、协议相对 OSPF 较为简单不容易出问题等优点。因而, IS-IS 适用于大型的核心骨干网络。本节描述如何在设备上配置 IS-IS 动态路由协议进行网络互联。

43.2 IS-IS 功能配置

表 43-1 IS-IS 功能配置任务列表

配置任务	
配置 IS-IS 基本功能	使能 IS-IS 协议
	配置 IS-IS VRF 属性
配置 IS-IS 层属性	配置 IS-IS 层属性
配置 IS-IS 路由生成	配置 IS-IS 默认路由
	配置 IS-IS 路由重分发

配置任务	
配置 IS-IS 路由控制	配置 IS-IS 度量类型
	配置 IS-IS 接口 metric 值
	配置 IS-IS 管理距离
	配置 IS-IS 路由汇总
	配置 IS-IS 最大负载均衡条目数
	配置 IS-IS 层间路由泄露
	配置 IS-IS ATT 位
配置 IS-IS 网络优化	配置 IS-IS 接口优先级
	配置 IS-IS 被动接口
	配置 IS-IS Hello 报文参数
	配置 IS-IS LSP 报文参数
	配置 IS-IS SNP 报文参数
	配置 IS-IS SPF 计算间隔
	配置 IS-IS 最大区域数
	配置 IS-IS 主机名映射
配置 IS-IS 接口加入 Mesh 组	
配置 IS-IS 网络认证	配置 IS-IS 邻居认证

配置任务	
	配置 IS-IS 路由认证
配置 IS-IS 与 BFD 联动	配置 IS-IS 与 BFD 联动
配置 IS-IS GR	配置 IS-IS GR

43.2.1 配置 IS-IS 基本功能 **-E -A**

配置条件

用户使用 IS-IS 协议之前，首先完成以下任务：

- 配置链路层协议，保证链路层通信正常。

配置接口的网络层地址，使相邻网络节点网络层可达。

使能 IS-IS 协议

系统中可以同时运行多个 IS-IS 进程，每个进程使用不同的进程名进行区分。

表 43-2 使能 IS-IS 协议

步骤	命令	说明
进入全局配置模式	configure terminal	-
创建 IS-IS 进程并进入 IS-IS 配置模式	router isis [area-tag]	必选 缺省情况下，系统中没有运行 IS-IS 进程， <i>area-tag</i> 为进程名。
为 IS-IS 配置网络实体标题	net entry-title	必选 缺省情况下，IS-IS 没有网络实体标题

步骤	命令	说明
返回全局配置模式	exit	-
进入接口配置模式	interface <i>interface-name</i>	-
接口启用 IS-IS 协议	ip router isis [<i>area-tag</i>]	必选 缺省情况下，接口未启用 IS-IS 协议

说明：

- 在没有网络实体标题的情况下 IS-IS 协议不能运行。

配置 IS-IS VRF 属性

在同一个 VRF 中可以有多个 IS-IS 进程，但只能有一个 Level-2 属性的 IS-IS 进程。

表 43-3 配置 IS-IS VRF 属性

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 IS-IS 配置模式	router isis [<i>area-tag</i>]	-
配置 IS-IS 的 VRF 属性	vrf <i>vrf-name</i>	可选 缺省情况下，IS-IS 进程位于全局 VRF 中

43.2.2 配置 IS-IS 层属性 -E -A

配置条件

在配置 IS-IS 层属性前，首先完成以下任务：

- 配置接口的 IP 地址，使各相邻节点网络层可达。
- 使能 IS-IS 协议。

配置 IS-IS 层属性

IS-IS 层属性分为全局层属性和接口层属性；全局层属性即为 IS-IS 中间系统的类别，分为如下三类：

- Level-1 类型中间系统：只有 Level-1 的链路状态数据库，只能通告和学习 Level-1 区域的路由；
- Level-2 类型中间系统：只有 Level-2 的链路状态数据库，只能通告和学习 Level-2 区域的路由；
- Level-1-2 类型中间系统：同时拥有 Level-1 和 Level-2 的链路状态数据库，可以通告和学习 Level-1 和 Level-2 的路由，是 Level-1 和 Level-2 区域的互联设备。

IS-IS 接口的层属性也分为如下三类：

- Level-1 属性接口：只能发送和接收 IS-IS 协议 Level-1 报文，只能建立 Level-1 的邻居；
- Level-2 属性接口：只能发送和接收 IS-IS 协议 Level-2 报文，只能建立 Level-2 的邻居；
- Level-1-2 属性接口：可以同时发送和接收 IS-IS 协议 Level-1 与 Level-2 的报文，可以同时建立 Level-1 邻居和 Level-2 邻居。

IS-IS 接口层属性依赖于 IS-IS 全局层属性，Level-1 中间系统只能拥有 Level-1 属性的接口，Level-2 中间系统只能拥有 Level-2 属性的接口，Level-1-2 中间系统可以同时拥有所有属性的接口。

表 43-4 配置 IS-IS 全局层属性

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
进入 IS-IS 配置模式	router isis [<i>area-tag</i>]	-
配置 IS-IS 全局层属性	is-type { level-1 level-1-2 level-2-only }	可选 缺省情况下, IS-IS 全局层属性为 Level-1-2

表 43-5 配置 IS-IS 接口层属性

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置接口层属性	isis circuit-type [level-1 level-1-2 level-2]	可选 缺省情况下, 未指定接口层属性时, 接口层属性跟全局层属性一致

说明:

- 在同一个 VRF 中只能有一个 Level-2 属性的 IS-IS 进程。

43.2.3 配置 IS-IS 路由生成

-E -A

配置条件

在配置 IS-IS 路由生成前, 首先完成以下任务:

- 配置接口的 IP 地址，使各相邻节点网络层可达。
- 使能 IS-IS 协议。

配置 IS-IS 默认路由

IS-IS 协议的 Level-2 区域在运行时无法生成默认路由，可以通过配置在 Level-2 LSP 中增加一条默认路由（目的地址为 0.0.0.0/0 的路由）信息，并将其发布出去，其他中间系统相同级别的区域收到此信息后将会在路由表中增加一条默认路由。

表 43-6 配置 IS-IS 默认路由

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 IS-IS 配置模式	router isis [area-tag]	-
进入 IS-IS IPv4 地址族配置模式	address-family ipv4 unicast	-
配置 IS-IS 发布默认路由	default-information originate	必选 缺省情况下，不发布默认路由

配置 IS-IS 路由重分发

通过路由重分发可以将其他路由协议的路由信息引入到 IS-IS 协议中来，使运行 IS-IS 协议的自治系统和运行其他路由协议的自治系统或路由域实现互联。在引入外部路由时可指定路由引入的策略和引入后路由的层属性。

表 43-7 配置 IS-IS 路由重分发

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 IS-IS 配置模式	router isis [area-tag]	-

步骤	命令	说明
进入 IS-IS IPv4 地址族配置模式	address-family ipv4 unicast	-
配置 IS-IS 路由重分发	redistribute protocol [<i>protocol-id</i>] [level-1 / level-1-2 / level-2 / metric metric-value / metric-type { external internal } / route-map route-map-name / match route-sub-type]	必选 缺省情况下，不重分发其他路由协议的信息

43.2.4 配置 IS-IS 路由控制

-E -A

配置条件

在配置 IS-IS 路由特性前，首先完成以下任务：

- 配置接口的 IP 地址，使各相邻节点网络层可达。
- 使能 IS-IS 协议。

配置 IS-IS 度量类型

最初的 IS-IS 只有窄度量类型，使用窄度量类型时，接口的最大度量值为 63，随着网络规模的逐渐扩大，窄度量类型已经远远不能满足需求；于是后来对度量类型做了扩展，增加了宽度量类型，度量值可达到 16777214；使用不同度量类型的设备不能互相通告和学习路由信息，为了实现两种度量类型的过渡，提供了过渡度量类型的配置方法。

建议使用宽度量类型。

表 43-8 配置 IS-IS 度量类型

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 IS-IS 配置模式	router isis [<i>area-tag</i>]	-
配置接口度量类型	metric-style { <i>narrow</i> <i>narrow transition</i> <i>transition</i> <i>wide</i> <i>wide transition</i> } [<i>level-1</i> <i>level-1-2</i> <i>level-2</i>]	可选 缺省情况下, 使用窄度量类型

配置 IS-IS 接口 metric 值

接口在启用 IS-IS 协议后, IS-IS 路由的度量为全局的度量值, 可通过命令为每个接口单独指定度量值。

表 43-9 配置接口 metric 值

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 IS-IS 配置模式	router isis [<i>area-tag</i>]	-
配置 IS-IS 全局度量值	metric <i>metric-value</i> [<i>level-1</i> <i>level-2</i>]	可选 缺省情况下, 全局度量值为 10
返回全局配置模式	exit	-
进入接口配置模式	interface <i>interface-name</i>	-

单播路由

步骤	命令	说明
配置接口度量值	isis ipv4 metric { <i>metric-value</i> / maximum } [level-1 level-2]	可选 缺省情况下，使用全局的度量值

配置 IS-IS 管理距离

系统根据管理距离来优选路由，管理距离越小，路由越优先。

表 43-10 配置 IS-IS 管理距离

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 IS-IS 配置模式	router isis [<i>area-tag</i>]	-
进入 IS-IS IPv4 地址族配置模式	address-family ipv4 unicast	-
配置 IS-IS 路由管理距离	distance <i>distance-value</i>	可选 缺省情况下，管理距离为 115

配置 IS-IS 路由汇总

路由汇总是将多条路由信息汇总为一条路由信息，IS-IS 配置路由汇总后，可以有效地减少通告可达子网信息的数量，减小链路状态数据库和路由表的大小，从而能够有效地节省内存和 CPU 资源。该配置一般在 Level-1-2 边界设备上使用，以减少层间通告的路由信息。

表 43-11 配置 IS-IS 路由汇总

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
进入 IS-IS 配置模式	router isis [<i>area-tag</i>]	-
进入 IPv4 地址族配置模式	address-family ipv4 unicast	-
配置 IS-IS 路由汇总	summary-prefix <i>prefix-value</i> [metric <i>metric-value</i> / route-type { internal external } / metric-type { internal external } / tag <i>tag-value</i> / not-advertise / level-1 / level-2 / level-1-2]	必选 缺省情况下, 不进行路由汇总

配置 IS-IS 最大负载均衡条目数

去往同一目的地址可以有多个代价相同的路径, 通过这些等价路径可以提高链路利用率, 用户可控制 IS-IS 的等价路由最大条数。

表 43-12 配置 IS-IS 最大负载均衡条目数

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 IS-IS 配置模式	router isis [<i>area-tag</i>]	-
进入 IPv4 地址族配置模式	address-family ipv4 unicast	-
配置 IS-IS 最大负载均衡条目数	maximum-paths <i>max-number</i>	可选

单播路由

步骤	命令	说明
		缺省情况下，最大负载均衡条目数为 4

配置 IS-IS 层间路由泄露

在缺省情况下 IS-IS 只会将 Level-1 路由向 Level-2 泄露，Level-1 区域无法知道 Level-2 区域路由，可通过配置层间路由泄露将 Level-2 路由引入到 Level-1 区域中。在配置层间路由泄露时可指定路由策略，只泄露匹配条件的路由。

表 43-13 配置 IS-IS 层间路由泄露

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 IS-IS 配置模式	router isis [area-tag]	-
进入 IS-IS IPv4 地址族配置模式	address-family ipv4 unicast	-
配置 IS-IS 层间路由泄露	propagate { level-1 into level-2 level-2 into level-1 } [distribute-list access-list-name route-map route-map-name]	必选 缺省情况下，Level-1 向 Level-2 进行路由泄露

配置 IS-IS ATT 位

在 Level-1-2 设备中，ATT 位用来通告其他节点，本节点是否有到其他区域的连接，如果本节点有到其他区域的连接 ATT 位将会自动置 1，其他节点将会产生一条到本节点的默认路由，这样会增加本节点的业务负担，为了防止这种情况发生可将 ATT 位强制置为 0。

表 43-14 配置 IS-IS ATT 位

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 IS-IS 配置模式	router isis [area-tag]	-
进入 IS-IS IPv4 地址族配置模式	address-family ipv4 unicast	-
配置 IS-IS ATT 位	set-attached-bit { on off }	必选 缺省情况下，根据节点是否连接到其他区域来设置 ATT 位

43.2.5 配置 IS-IS 网络优化

-E -A

配置条件

在配置 IS-IS 调整和优化前，首先完成以下任务：

- 配置接口的 IP 地址，使各相邻节点网络层可达。
- 使能 IS-IS 协议。

配置 IS-IS 接口优先级

在广播链路上 IS-IS 需要选举一个节点作为 DIS，DIS 节点周期发送 CSNP 报文，同步全网的链路状态数据库；Level-1 和 Level-2 的 DIS 节点分别选举，接口优先级最高的被选举为 DIS 节点，优先级相同时选举 MAC 地址大的作为 DIS 节点。

表 43-15 配置 IS-IS 接口优先级

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
进入接口配置模式	interface <i>interface-name</i>	-
配置 IS-IS 接口优先级	isis priority <i>priority-value</i> [level-1 level-2]	可选 缺省情况下，接口优先级为 64

配置 IS-IS 被动接口

被动接口是指在此接口上不会发送和接收 IS-IS 协议的报文，但仍然发布此接口的直连网络路由信息；IS-IS 通过配置被动接口可以节省带宽和 CPU 的处理时间；在此配置基础之上还可指定 IS-IS 只发布被动接口的直连网络路由信息，而不发布非被动接口的直连网络路由信息。

表 43-16 配置 IS-IS 被动接口

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 IS-IS 配置模式	router isis [<i>area-tag</i>]	-
配置 IS-IS 被动接口	passive-interface <i>interface-name</i>	必选 缺省情况下，IS-IS 没有被动接口
配置 IS-IS 只发布被动接口的路由信息	advertise-passive-only	可选 缺省情况下，发布所有启用了 IS-IS 协议接口的直连网络路由信息

配置 IS-IS Hello 报文参数

1. 配置 Hello 报文发送间隔

启动了 IS-IS 协议的接口，会周期的发送 Hello 报文以保持和邻居的邻接关系，Hello 报文的发送间隔越小网络收敛越快，但占用的带宽也越大。

表 43-17 配置 Hello 报文的发送间隔

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置接口上 Hello 报文的发送间隔	isis hello-interval { <i>interval</i> minimal } [level-1 level-2]	可选 缺省情况下，Hello 报文的发送间隔为 10 秒

2. 配置 Hello 报文的失效数目

IS-IS 根据 Hello 报文失效数目计算出邻居关系的保持时间，并将保持时间通告给邻居设备，如果邻居设备在这个时间内没有收到此设备的 Hello 报文，认为此邻接关系失效，会重新进行路由计算。

表 43-18 配置 Hello 报文的失效数目

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置接口上 Hello 报文失效数目	isis hello-multiplier <i>multiplier</i> [level-1 level-2]	可选 缺省情况下，Hello 报文的失效数为 3

3. 配置取消 Hello 报文填充功能

为了防止链路两端接口的 MTU 值不一致，导致较小的报文能通过而较大的报文不能通过，IS-IS 采用填充 Hello 报文到接口 MTU 值的方法，使其在这种情况下不能建立邻居关系；但这种方法造成了带宽的浪费，在实际应用中可以配置不填充 Hello 报文，发送小型化的 Hello 报文。

表 43-19 配置取消 Hello 报文填充功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
取消 Hello 报文的填充功能	no isis hello padding	必选 缺省情况下，启用了 Hello 报文的填充功能

配置 IS-IS LSP 报文参数

1. 配置 LSP 报文最大生存时间

每个 LSP 报文都有一个最大生存时间，在 LSP 报文的生存时间减小到零后，会将其从链路状态数据库中删除。LSP 报文的最大生存时间应大于 LSP 报文的刷新间隔。

表 43-20 配置 IS-IS LSP 报文参数

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 IS-IS 配置模式	router isis [<i>area-tag</i>]	-
配置 LSP 报文的最大生存时间	max-lsp-lifetime <i>lifetime</i>	可选 缺省情况下，LSP 报文的最大生存时间为 1200 秒

2. 配置 LSP 报文刷新闻隔

IS-IS 协议通过交互各自的 LSP 报文来通告和学习路由，节点将收到的 LSP 报文存储在自己的链路状态数据库中，每个 LSP 报文都有一个最大生存时间，所以每个节点需要定期的更新自己的 LSP 报文，以防止 LSP 报文的最大生存时间减小到零，并且使整个区域中的 LSP 报文保持同步。减小 LSP 报文周期发送的时间间隔，可以加快网络的收敛速度，但会占用更多的带宽。

表 43-21 配置 LSP 报文刷新闻隔

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 IS-IS 配置模式	router isis [area-tag]	-
配置 LSP 报文刷新闻隔	lsp-refresh-interval <i>refresh-interval</i>	可选 缺省情况下，周期发送的时间间隔为 900 秒

3. 配置 LSP 报文生成间隔

除了周期更新会生成 LSP 报文外，接口状态变化，网络状态变化等都会触发生成新的 LSP 报文，为了防止频繁的生成 LSP 报文大量占用 CPU 资源，用户可配置 LSP 报文的最小生成间隔。

表 43-22 配置 LSP 报文生成间隔

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 IS-IS 配置模式	router isis [area-tag]	-
配置 LSP 报文生成间隔	lsp-gen-interval [level-1 level-2] <i>max-interval [initial-interval [secondary-interval]]</i>	可选 缺省情况下，LSP 报文的生成间隔的上限值为 10 秒，下限值缺省为 50 毫秒

4. 配置 LSP 报文发送时间间隔

每生成一次 LSP 报文便会在接口上进行发送，为了防止频繁的生成 LSP 报文而大量占用接口带宽，可为每个接口配置 LSP 报文的最小发送时间间隔。

表 43-23 配置 LSP 报文发送时间间隔

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置 LSP 报文发送时间间隔	isis lsp-interval <i>min-interval</i>	可选 缺省情况下，LSP 报文的发送间隔为 33 毫秒

5. 配置 LSP 报文重传时间

在点对点链路上，IS-IS 在发送 LSP 报文后需要对端发送 PSNP 的确认信息，如果没有收到对端的确认信息将重新发送该 LSP 报文。等待确认的时间即 LSP 报文的重传时间可由用户进行配置，防止在时延较大时因为没有收到确认而重传 LSP 报文。

表 43-24 配置 LSP 报文重传时间

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置 LSP 报文重传时间	isis retransmit-interval <i>interval</i> [level-1 level-2]	可选

步骤	命令	说明
		缺省情况下，重传时间为 5 秒

6. 配置 LSP MTU 值

IS-IS 协议的报文无法进行自动分片，为了不影响 LSP 报文的正常扩散，要求在一个路由域内 LSP 报文的最大长度不会超过所有设备 IS-IS 接口的最小 MTU 值；所以在路由域内设备接口的 MTU 值不一致时，建议将 LSP 报文的最大长度进行统一设置。

表 43-25 配置 LSP MTU 值

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 IS-IS 配置模式	router isis [area-tag]	-
配置 LSP 报文 MTU 值	lsp-mtu mtu-size [level-1 level-2]	可选 缺省情况下，LSP 报文 MTU 值为 1492 字节

配置 IS-IS SNP 报文参数

1. 配置 CSNP 报文发送时间间隔

在广播链路选举节点需要周期的发送 CSNP 报文来同步全网的链路状态数据库，CSNP 报文的周期发送间隔可根据实际情况进行调整。

表 43-26 配置 CSNP 报文发送时间间隔

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
进入接口配置模式	interface <i>interface-name</i>	-
配置 CSNP 报文发送间隔	isis csnp-interval <i>interval</i> [level-1 level-2]	可选 缺省情况下, CSNP 报文的周期发送间隔为 10 秒

2. 配置 PSNP 报文发送时间间隔

在广播链路上 PSNP 报文用来同步全网的链路状态数据库, 在点对点链路上 PSNP 报文用来确认收到的 LSP 报文。为了防止接口上大量发送 PSNP 报文, 为 PSNP 报文设置了一个最小发送时间间隔, 用户可以动态的修改这个间隔。PSNP 报文的发送间隔不宜设置过大, 设置过大对于广播链路, 将会影响全网链路状态数据库的同步, 对于点对点链路, 将会造成不能及时收到确认而重传 LSP 报文。

表 43-27 配置 PSNP 报文发送时间间隔

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置 PSNP 报文发送间隔	isis psnp-interval <i>min-interval</i> [level-1 level-2]	可选 缺省情况下, PSNP 报文发送间隔为 2 秒

配置 IS-IS SPF 计算间隔

IS-IS 的链路状态数据库发生变化时将会触发 SPF 路由计算, 频繁的 SPF 计算将会消耗大量的 CPU 资源, 用户可对 SPF 的计算间隔进行配置。

表 43-28 配置 IS-IS SPF 计算间隔

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 IS-IS 配置模式	router isis [area-tag]	-
进入 IS-IS IPv4 地址族配置模式	address-family ipv4 unicast	-
配置 IS-IS 的 SPF 计算间隔	spf-interval [level-1 level-2] maximum-interval [min-initial-delay [min-second-delay]]	可选

配置 IS-IS 最大区域数

在一个 IS-IS 进程中可以配置多个区域地址，多区域地址主要用于多个 Level-1 区域合并为一个 Level-1 区域，或者一个 Level-1 区域分割成多个 Level-1 区域的平滑过渡。

表 43-29 配置 IS-IS 最大区域数

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 IS-IS 配置模式	router isis [area-tag]	-
配置 IS-IS 最大区域数	max-area-addresses max-number	可选 缺省情况下，最大区域地址数为 3

说明：

- 该配置要求在整个 IS-IS Level-1 路由域内配置一致，否则将不能正常建立 Level-1 邻

居，对于 Level-2 邻居，则没有该影响。

配置 IS-IS 主机名映射

IS-IS 通过系统 ID 来唯一标识一个中间系统，系统 ID 的固定长度为 6 个字节，在查看系统信息时（邻居关系、链路状态数据库等），系统 ID 不能使用户很直观的将系统 ID 和主机名信息联系在一起；IS-IS 支持将系统 ID 和主机名进行映射，使用户在查看系统信息时更直观，方便。配置 IS-IS 主机名映射有两种方式：

1. 配置 IS-IS 静态主机名映射

IS-IS 静态主机名映射是用户手动为远端的设备建立系统 ID 和主机名的映射。

表 43-30 配置 IS-IS 静态主机名映射

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 IS-IS 配置模式	router isis [<i>area-tag</i>]	-
配置 IS-IS 静态主机名映射	hostname static <i>system-id host-name</i>	必选

2. 配置 IS-IS 动态主机名映射

静态主机名映射需要用户为网络中的每台设备配置其他设备的系统 ID 和主机名映射，工作量大；动态主机名映射只需用为每台设备配置主机名后，启用主机名通告功能，网络中的其他设备就能学习到该设备的主机名。

表 43-31 配置 IS-IS 动态主机名映射

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 IS-IS 配置模式	router isis [<i>area-tag</i>]	-

步骤	命令	说明
配置 IS-IS 动态主机名映射	hostname dynamic { <i>host-name</i> area-tag recv-only system-name }	必选 缺省情况下，只学习其他设备通告的主机名

配置 IS-IS 接口加入 Mesh 组

IS-IS 接口在未加入 Mesh 组的情况下，从一个接口收到 LSP 报文后将会把该 LSP 报文从所有的其他 IS-IS 接口发送出去，这在全网状连接的网络中将会造成很大的带宽浪费；可将几个 IS-IS 接口加入同一 Mesh 组，接口在收到 LSP 报文时只将该 LSP 报文发送到和该接口不在同一个 Mesh 组中的接口。

表 43-32 配置 IS-IS 接口加入 Mesh 组

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置 IS-IS 接口加入 Mesh 组	isis mesh-group { <i>group-number</i> blocked }	必选 缺省情况下，未加入 Mesh 组

说明：

- **isis mesh-group blocked** 将接口设置为阻塞型接口，阻塞型接口不会主动发送 LSP 报文，只有在收到 LSP 请求时才会发送 LSP 报文。

配置条件

在配置 IS-IS 网络认证前，首先完成以下任务：

- 配置接口的 IP 地址，使各相邻节点网络层可达。
- 使能 IS-IS 协议。

配置 IS-IS 邻居认证

配置 IS-IS 启用邻居关系认证后，将会在发送的 Hello 报文中添加认证消息，同时对收到的 Hello 报文进行认证，认证不通过的不会形成邻居关系，这样可以防止和不可信任的设备建立邻居关系。

表 43-33 配置 IS-IS 邻居认证

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置 Hello 报文的认证模式	isis authentication mode { md5 text } [level-1 level-2]	必选 缺省情况下，不启用认证功能
配置 Hello 报文的认证密码	isis authentication key { 0 7 } <i>password</i> [level-1 level-2]	二选一 缺省情况下，没有认证密码；认证密码可以使用密码链配置，关于密码链的配置可参见手册的密码链配置章节
	isis authentication key-chain <i>key-chain-name</i> [level-1 level-2]	

配置 IS-IS 路由认证

配置了 IS-IS 的路由信息认证后，将会在 LSP 和 SNP 报文中添加认证消息，同时对收到的 LSP 和 SNP 报文进行认证，认证不通过的报文直接丢弃，这样可以防止不可信任的路由信息扩散到 IS-IS 网络中。

表 43-34 配置 IS-IS 路由认证

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 IS-IS 配置模式	router isis [area-tag]	-
配置路由信息报文的认证模式	authentication mode { md5 text } [level-1 level-2]	必选 缺省情况下，不启用认证功能
配置路由信息报文的认证密码	authentication key { 0 7 } password [level-1 level-2]	二选一 缺省情况下，没有认证密码；认证密码可以使用密码链配置，关于密码链的配置可参见手册的密码链配置章节
	authentication key-chain key-chain-name [level-1 level-2]	

43.2.7 配置 IS-IS 与 BFD 联动 **-E -A**

配置 IS-IS 与 BFD 联动可快速的检测到链路故障，启用备份链路进行通信。配置 IS-IS 与 BFD 联动有两种方式，第一种是：所有启用了 IS-IS 协议的接口都关联 BFD；第二种是：指定接口关联 BFD。

关于 BFD 参数信息请参考 BFD 配置手册。

配置条件

在配置 IS-IS 与 BFD 联动前，首先完成以下任务：

- 配置接口的 IP 地址，使各相邻节点网络层可达。
- 使能 IS-IS 协议。

配置 IS-IS 与 BFD 联动

表 43-35 配置 IS-IS 与 BFD 联动

步骤	命令
进入全局配置模式	configure terminal
进入接口配置模式	interface <i>interface-name</i>
配置接口启用 BFD 链路检测功能	isis bfd
返回全局配置模式	exit
进入 IS-IS 配置模式	router isis [<i>area-tag</i>]
配置所有 IS-IS 接口启用 BFD 链路检测功能	bfd all-interfaces

43.2.8 配置 IS-IS GR **-E -A**

GR (Graceful Restart, 优雅重启) 用于在设备主备切换过程中, 保持本设备和邻居设备转发层面路由信息不变, 转发不受影响; 当切换设备重新运行后, 两台设备协议层面同步路由信息并更新转发层, 达到设备切换过程中数据转发不间断的目的。

GR 过程中有两种角色:

- GR Restarter 端——进行协议优雅重启的设备。
- GR Helper 端——协助协议优雅重启的设备。

分布式设备可以充当 GR Restarter 和 GR Helper, 而集中式设备只能充当 GR Helper, 协助 Restarter 端完成 GR。

配置条件

在配置 IS-IS GR 前, 首先完成以下任务:

- 配置接口的 IP 地址, 使各相邻节点网络层可达。

- 使能 IS-IS 协议。

配置 IS-IS GR Restarter

表 43-36 配置 IS-IS GR Restarter

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 IS-IS 配置模式	router isis [<i>area-tag</i>]	-
配置 IS-IS 启用优雅重启功能	nsf ietf	必选 缺省情况下，未启用 GR 功能
配置通告进入 GR 过程消息的重传次数	nsf interface-expire <i>resend-cnt</i>	可选 缺省情况下，重传次数为 3
配置进入 GR 过程消息的重传等待时间	nsf interface-timer <i>wait-time</i>	可选 缺省情况下，等待时间为 10 秒

配置 IS-IS GR Helper

GR Helper 协助 Restarter 端完成 GR，缺省情况下，设备都使能该功能，用户可通过命令关闭该功能。

表 43-37 配置 IS-IS GR Helper

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 IS-IS 配置模式	router isis [<i>area-tag</i>]	-

步骤	命令	说明
配置 IS-IS GR Helper 不具备 Helper 能力	nsf ietfhelper-disable	必选 配置 IS-IS GR Helper 不具备 Helper 能力

43.2.9 IS-IS 监控与维护

-E -A

表 43-38 IS-IS 监控与维护

命令	说明
clear isis [instance -null area-tag] statistics [interface_name]	清除 IS-IS 协议运行的统计信息
clear isis [instance -null area-tag] process	重启 IS-IS 协议进程
show isis [instance -null area-tag]	显示 IS-IS 进程的信息
show isis instance { -null area-tag } bfd-sessions	显示 IS-IS 进程的 BFD 会话信息
show isis [instance -null area-tag] database [lsp_id] [detail] [I1 / I2] [level-1 / level-2] [self] [verbose]	显示 IS-IS 链路状态数据库信息
show isis interface [interface-name] [detail]	显示运行 IS-IS 协议接口的信息
show isis [instance -null area-tag] ipv4 reach-info	显示 IS-IS 的 IPV4 子网可达信息

命令	说明
show isis [instance -null area-tag] ipv4 route	显示 IS-IS 的 IPV4 路由信息
show isis [instance -null area-tag] ipv4 topology	显示 IS-IS 的 IPV4 拓扑信息
show isis [instance - null area-tag] is-reach-info [level-1 level-2]	显示 IS-IS 的邻接节点信息
show isis [instance -null area-tag] mesh-groups	显示 IS-IS 的 mesh 组
show isis [instance -null area-tag] neighbors [interface-name] [detail]	显示 IS-IS 的邻居信息
show isis [instance -null area-tag] statistics [interface-name]	显示 IS-IS 协议运行的统计信息
show isis router	显示 IS-IS 主机名信息

43.3 IS-IS 典型配置举例

43.3.1 配置 IS-IS 基本功能

-E -A

网络需求

- 通过配置 IS-IS 协议使设备间达到网络互连。
- Device1 为 Level-1 路由器，Device2 为 Level-1-2 路由器，Device1 和 Device2 在同一区域内，区域号为 10。Device3 为 Level-2 路由器，区域号为 20。Device2 承担连接两个区域的功能。

网络拓扑

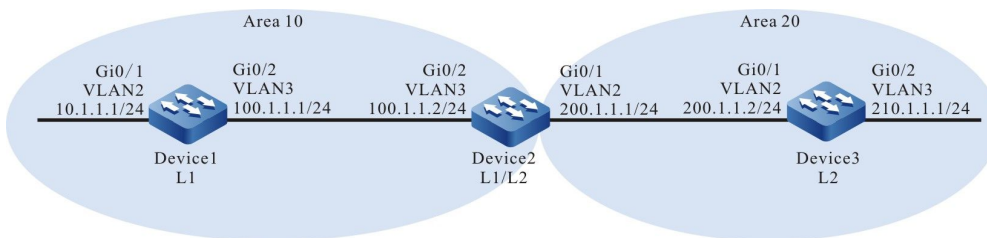


图 43-1 IS-IS 基本功能组网图

配置步骤

步骤 1: 配置各接口的 IP 地址。 (略)

步骤 2: 配置 IS-IS, 并在接口启用该进程。

#Device1 配置 IS-IS 进程 100, 区域号 10, 类型为 Level-1 并在接口上启用该进程。

```
Device1#configure terminal
Device1(config)#router isis 100
Device1(config-isis)#net 10.0000.0000.0001.00
Device1(config-isis)#is-type level-1
Device1(config-isis)#metric-style wide
Device1(config-isis)#exit
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip router isis 100
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan3
Device1(config-if-vlan3)#ip router isis 100
Device1(config-if-vlan3)#exit
```

#Device2 配置 IS-IS 进程 100, 区域号 10, 类型为 Level-1-2 并在接口上启用该进程。

```
Device2#configure terminal
Device2(config)#router isis 100
Device2(config-isis)#net 10.0000.0000.0002.00
Device2(config-isis)#metric-style wide
Device2(config-isis)#exit
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ip router isis 100
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan3
Device2(config-if-vlan3)#ip router isis 100
Device2(config-if-vlan3)#exit
```

#Device3 配置 IS-IS 进程 100, 区域号 20, 类型为 Level-2 并在接口上启用该进程。

```
Device3#configure terminal
Device3(config)#router isis 100
Device3(config-isis)#net 20.0000.0000.0003.00
Device3(config-isis)#is-type level-2
Device3(config-isis)#metric-style wide
Device3(config-isis)#exit
Device3(config)#interface vlan2
Device3(config-if-vlan2)#ip router isis 100
Device3(config-if-vlan2)#exit
```

单播路由

```
Device3(config)#interface vlan3
Device3(config-if-vlan3)#ip router isis 100
Device3(config-if-vlan3)#exit
```

步骤 3: 检验结果。

#查看 Device1 的 IS-IS 邻居信息。

```
Device1#show isis neighbors
IS-IS Instance 100 Neighbors (Counter 1):
Type System ID Interface State Holdtime Level IETF-NSF Priority Circuit ID
L1-LAN 0000.0000.0002 vlan3 Up 29 sec L1 capable 64 0000.0000.0001.01
```

#查看 Device2 的 IS-IS 邻居信息。

```
Device2#show isis neighbors
IS-IS Instance 100 Neighbors (Counter 2):
Type System ID Interface State Holdtime Level IETF-NSF Priority Circuit ID
L2-LAN 0000.0000.0003 vlan2 Up 9 sec L2 capable 64 0000.0000.0003.01
L1-LAN 0000.0000.0001 vlan3 Up 8 sec L1 capable 64 0000.0000.0001.01
```

Device2 分别与 Device1 和 Device3 建立 IS-IS 邻居。

#查看 Device3 的 IS-IS 邻居信息。

```
Device3#show isis neighbors
IS-IS Instance 100 Neighbors (Counter 1):
Type System ID Interface State Holdtime Level IETF-NSF Priority Circuit ID
L2-LAN 0000.0000.0002 vlan3 Up 22 sec L2 capable 64 0000.0000.0003.01
```

#查看 Device1 的路由信息。

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-IS-IS
```

```
Gateway of last resort is 100.1.1.2 to network 0.0.0.0
```

```
i 0.0.0.0/0 [115/10] via 100.1.1.2, 17:44:09, vlan3
C 10.1.1.0/24 is directly connected, 16:56:18, vlan2
C 100.1.1.0/24 is directly connected, 18:37:57, vlan3
C 127.0.0.0/8 is directly connected, 284:02:13, lo0
i 200.1.1.0/24 [115/20] via 100.1.1.2, 17:44:09, vlan3
```

```
Device1#show isis ipv4 route
IS-IS Instance 100, VRF Kernel, IPv4 routes table (Counter 4):
L1 0.0.0.0/0, flags none, metric 10, from learned, installed
via 100.1.1.2, vlan3, neighbor 0000.0000.0002
L1 10.1.1.0/24, flags none, metric 10, from network connected
via 0.0.0.0, vlan2
L1 100.1.1.0/24, flags none, metric 10, from network connected
via 0.0.0.0, vlan3
L1 200.1.1.0/24, flags none, metric 20, from learned, installed
via 100.1.1.2, vlan3, neighbor 0000.0000.0002
```

Device1 的路由表中有一条缺省路由，下一跳为 Device2。

#查看 Device2 的路由信息。

单播路由

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-IS-IS
```

Gateway of last resort is not set

```
i 10.1.1.0/24 [115/20] via 100.1.1.1, 16:58:26, vlan3
C 100.1.1.0/24 is directly connected, 18:39:58, vlan3
C 127.0.0.0/8 is directly connected, 20:16:34, lo0
C 200.1.1.0/24 is directly connected, 18:39:37, vlan2
i 210.1.1.0/24 [115/20] via 200.1.1.2, 16:57:56, vlan2
```

```
Device2#show isis ipv4 route
IS-IS Instance 100, VRF Kernel, IPv4 routes table (Counter 4):
L1 10.1.1.0/24, flags none, metric 20, from learned, installed
   via 100.1.1.1, vlan3, neighbor 0000.0000.0001
L1 100.1.1.0/24, flags none, metric 10, from network connected
   via 0.0.0.0, vlan3
L1 200.1.1.0/24, flags none, metric 10, from network connected
   via 0.0.0.0, vlan2
L2 210.1.1.0/24, flags none, metric 20, from learned, installed
   via 200.1.1.2, vlan2, neighbor 0000.0000.0003
Device2 中包含 Level-1 和 Level-2 的路由。
```

#查看 Device3 的路由信息。

```
Device3#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-IS-IS
```

Gateway of last resort is not set

```
i 10.1.1.0/24 [115/30] via 200.1.1.1, 16:59:29, vlan2
i 100.1.1.0/24 [115/20] via 200.1.1.1, 17:47:29, vlan2
C 127.0.0.0/8 is directly connected, 945:29:12, lo0
C 200.1.1.0/24 is directly connected, 18:40:27, vlan2
C 210.1.1.0/24 is directly connected, 16:59:04, vlan3
```

```
Device3#show isis ipv4 route
IS-IS Instance 100, VRF Kernel, IPv4 routes table (Counter 4):
L2 10.1.1.0/24, flags none, metric 30, from learned, installed
   via 200.1.1.1, vlan2, neighbor 0000.0000.0002
L2 100.1.1.0/24, flags none, metric 20, from learned, installed
   via 200.1.1.1, vlan2, neighbor 0000.0000.0002
L2 200.1.1.0/24, flags none, metric 10, from network connected
   via 0.0.0.0, vlan2
L2 210.1.1.0/24, flags none, metric 10, from network connected
   via 0.0.0.0, vlan3
```

Device3 学习到 Level-1 的路由，默认 Level-1 向 Level-2 泄露。

说明：

- 度量类型默认为窄度量，建议使用宽度量。
 - IS-IS 实体属性默认为 Level-1-2。
-

网络需求

- 通过修改优先级的方式将设备指定为 DIS。
- Device1 和 Device2 为 Level-1-2 设备，Device3 为 Level-1 设备，Device4 为 Level-2 设备。Device1、Device2、Device3、Device4 在同一广播网中并在同一区域内，区域号为 10。

网络拓扑

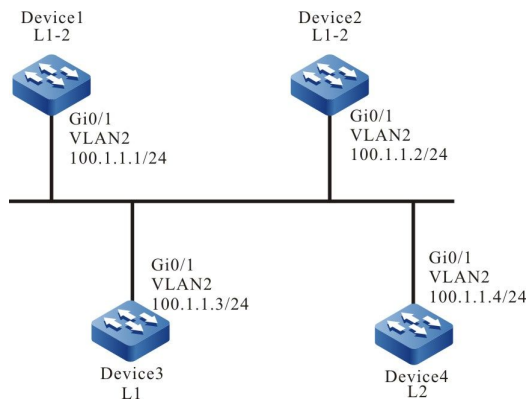


图 43-2 配置 IS-IS 的 DIS 选举组网图

配置步骤

步骤 1： 配置各接口的 IP 地址。（略）

步骤 2： 配置 IS-IS，并在接口启用该进程。

#Device1 配置 IS-IS 进程 100，区域号 10，类型为 Level-1-2 并在接口上启用该进程。

```
Device1#configure terminal
Device1(config)#router isis 100
Device1(config-isis)#net 10.0000.0000.0001.00
Device1(config-isis)#metric-style wide
Device1(config-isis)#exit
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip router isis 100
Device1(config-if-vlan2)#exit
```

#Device2 配置 IS-IS 进程 100，区域号 10，类型为 Level-1-2 并在接口上启用该进程。

```
Device2#configure terminal
Device2(config)#router isis 100
Device2(config-isis)#net 10.0000.0000.0002.00
Device2(config-isis)#metric-style wide
```

单播路由

```
Device2(config-isis)#exit
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ip router isis 100
Device2(config-if-vlan2)#exit
```

#Device3 配置 IS-IS 进程 100，区域号 10，类型为 Level-1 并在接口上启用该进程。

```
Device3#configure terminal
Device3(config)#router isis 100
Device3(config-isis)#net 10.0000.0000.0003.00
Device3(config-isis)#is-type level-1
Device3(config-isis)#metric-style wide
Device3(config-isis)#exit
Device3(config)#interface vlan2
Device3(config-if-vlan2)#ip router isis 100
Device3(config-if-vlan2)#exit
```

#Device4 配置 IS-IS 进程 100，区域号 20，类型为 Level-2 并在接口上启用该进程。

```
Device4#configure terminal
Device4(config)#router isis 100
Device4(config-isis)#net 20.0000.0000.0004.00
Device4(config-isis)#is-type level-2
Device4(config-isis)#metric-style wide
Device4(config-isis)#exit
Device4(config)#interface vlan2
Device4(config-if-vlan2)#ip router isis 100
Device4(config-if-vlan2)#exit
```

#查看 Device1 的 IS-IS 邻居信息。

```
Device1#show isis neighbors
IS-IS Instance 100 Neighbors (Counter 4):
Type System ID Interface State Holdtime Level IETF-NSF Priority Circuit ID
L1-LAN 0000.0000.0002 vlan2 Up 23 sec L1 capable 64 0000.0000.0003.01
L2-LAN 0000.0000.0002 vlan2 Up 23 sec L2 capable 64 0000.0000.0004.01
L1-LAN 0000.0000.0003 vlan2 Up 8 sec L1 capable 64 0000.0000.0003.01
L2-LAN 0000.0000.0004 vlan2 Up 8 sec L2 capable 64 0000.0000.0004.01
```

Level-1 的伪节点是 0000.0000.0003.01，Device3 是 Level-1 的 DIS。level-2 的伪节点是 0000.0000.0004.01，Device4 是 Level-2 的 DIS。

#使用命令 **show isis interface** 查看接口的 MAC 地址。在缺省优先级中，DIS 的选取按照物理接口的 MAC 地址越大越优先的原则。

步骤 3： 修改接口优先级。

#修改 Device1 接口优先级。

```
Device1(config)#interface vlan2
Device1(config-if-vlan2)#isis priority 100
Device1(config-if-vlan2)#exit
```

步骤 4： 检验结果。

#查看 Device1 的 IS-IS 邻居信息。

单播路由

```
Device1#show isis neighbors
IS-IS Instance 100 Neighbors (Counter 4):
Type System ID Interface State Holdtime Level IETF-NSF Priority Circuit ID
L1-LAN 0000.0000.0002 vlan2 Up 24 sec L1 capable 64 0000.0000.0001.01
L2-LAN 0000.0000.0002 vlan2 Up 23 sec L2 capable 64 0000.0000.0001.01
L1-LAN 0000.0000.0003 vlan2 Up 20 sec L1 capable 64 0000.0000.0001.01
L2-LAN 0000.0000.0004 vlan2 Up 24 sec L2 capable 64 0000.0000.0001.01
```

Level-1-2 的伪节点均为 0000.0000.0001.01，Device1 成为 Level-1-2 的 DIS。

说明：

- IS-IS 的接口优先级默认为 64，优先级越大越优先。

43.3.3 配置 IS-IS 层间路由泄露

-E -A

网络需求

- 通过在 Level-1-2 设备配置层间泄露将 Level-2 路由泄露到 Level-1 中。
- Device1 为 Level-1 路由器，Device2 为 Level-1-2 路由器，Device1 和 Device2 在同一区域内，区域号为 10。Device3 为 Level-2 路由器，区域号为 20。Device2 承担连接两个区域的功能。

网络拓扑

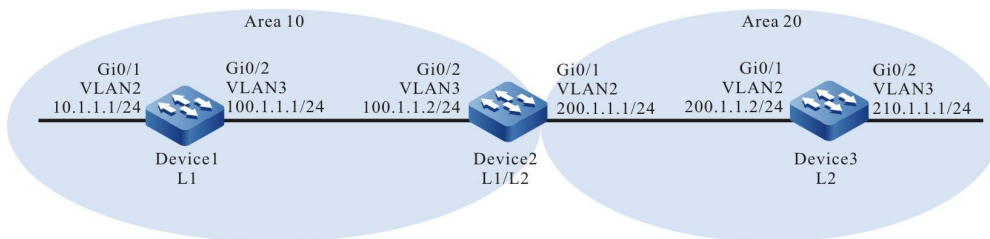


图 43-3 IS-IS 层间泄露组网图

配置步骤

步骤 1：配置各接口的 IP 地址。（略）

步骤 2：配置 IS-IS，并在接口启用该进程。

单播路由

#Device1 配置 IS-IS 进程 100，区域号 10，类型为 Level-1 并在接口上启用该进程。

```
Device1#configure terminal
Device1(config)#router isis 100
Device1(config-isis)#net 10.0000.0000.0001.00
Device1(config-isis)#is-type level-1
Device1(config-isis)#metric-style wide
Device1(config-isis)#exit
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip router isis 100
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan3
Device1(config-if-vlan3)#ip router isis 100
Device1(config-if-vlan3)#exit
```

#Device2 配置 IS-IS 进程 100，区域号 10，类型为 Level-1-2 并在接口上启用该进程。

```
Device2#configure terminal
Device2(config)#router isis 100
Device2(config-isis)#net 10.0000.0000.0002.00
Device2(config-isis)#metric-style wide
Device2(config-isis)#exit
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ip router isis 100
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan3
Device2(config-if-vlan3)#ip router isis 100
Device2(config-if-vlan3)#exit
```

#Device3 配置 IS-IS 进程 100，区域号 20，类型为 Level-2 并在接口上启用该进程。

```
Device3#configure terminal
Device3(config)#router isis 100
Device3(config-isis)#net 20.0000.0000.0003.00
Device3(config-isis)#is-type level-2
Device3(config-isis)#metric-style wide
Device3(config-isis)#exit
Device3(config)#interface vlan2
Device3(config-if-vlan2)#ip router isis 100
Device3(config-if-vlan2)#exit
Device3(config)#interface vlan3
Device3(config-if-vlan3)#ip router isis 100
Device3(config-if-vlan3)#exit
```

#查看 Device1 路由信息。

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNRP, B - BGP, i-IS-IS
```

```
Gateway of last resort is 100.1.1.2 to network 0.0.0.0
```

```
i 0.0.0.0/0 [115/10] via 100.1.1.2, 17:44:09, vlan3
C 10.1.1.0/24 is directly connected, 16:56:18, vlan2
C 100.1.1.0/24 is directly connected, 18:37:57, vlan3
C 127.0.0.0/8 is directly connected, 284:02:13, lo0
i 200.1.1.0/24 [115/20] via 100.1.1.2, 17:44:09, vlan3
```

```
Device1#show isis ipv4 route
IS-IS Instance 100, VRF Kernel, IPv4 routes table (Counter 4):
L1 0.0.0.0/0, flags none, metric 10, from learned, installed
   via 100.1.1.2, vlan3, neighbor 0000.0000.0002
L1 10.1.1.0/24, flags none, metric 10, from network connected
   via 0.0.0.0, vlan2
L1 100.1.1.0/24, flags none, metric 10, from network connected
   via 0.0.0.0, vlan3
```

```
L1 200.1.1.0/24, flags none, metric 20, from learned, installed
  via 100.1.1.2, vlan3, neighbor 0000.0000.0002

Device1#show isis database detail
IS-IS Instance 100 Level-1 Link State Database (Counter 3, LSP-MTU 1492):
LSPID          LSP Seq Num  LSP Checksum  LSP Holdtime  Length  ATT/P/OL
0000.0000.0001.00-00* 0x0000007E  0xD5DA      1067          71     0/0/0
NLPID: IPv4
Area Address: 10
IP Address: 100.1.1.1
Metric: 10     IS-Extended 0000.0000.0001.01
Metric: 10     IP-Extended 10.1.1.0/24
Metric: 10     IP-Extended 100.1.1.0/24
0000.0000.0001.01-00* 0x00000073  0xAAAF      471           51     0/0/0
Metric: 0      IS-Extended 0000.0000.0001.00
Metric: 0      IS-Extended 0000.0000.0002.00
0000.0000.0002.00-00 0x00000081  0x5926      887           71     1/0/0
NLPID: IPv4
Area Address: 10
IP Address: 200.1.1.1
Metric: 10     IS-Extended 0000.0000.0001.01
Metric: 10     IP-Extended 100.1.1.0/24
Metric: 10     IP-Extended 200.1.1.0/24
```

路由表中有一条缺省路由，下一跳为 Device2，没有 Device3 通告的 Level-2 路由。

#查看 Device2 路由信息。

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-IS-IS
```

Gateway of last resort is not set

```
i 10.1.1.0/24 [115/20] via 100.1.1.1, 16:58:26,vlan3
C 100.1.1.0/24 is directly connected, 18:39:58, vlan3
C 127.0.0.0/8 is directly connected, 20:16:34, lo0
C 200.1.1.0/24 is directly connected, 18:39:37, vlan2
i 210.1.1.0/24 [115/20] via 200.1.1.2, 16:57:56, vlan2
```

```
Device2#show isis ipv4 route
IS-IS Instance 100, VRF Kernel, IPv4 routes table (Counter 4):
L1 10.1.1.0/24, flags none, metric 20, from learned, installed
  via 100.1.1.1, vlan3, neighbor 0000.0000.0001
L1 100.1.1.0/24, flags none, metric 10, from network connected
  via 0.0.0.0, vlan3
L1 200.1.1.0/24, flags none, metric 10, from network connected
  via 0.0.0.0, vlan2
L2 210.1.1.0/24, flags none, metric 20, from learned, installed
  via 200.1.1.2, vlan2, neighbor 0000.0000.0003
```

```
Device2#show isis database detail
IS-IS Instance 100 Level-1 Link State Database (Counter 3, LSP-MTU 1492):
LSPID          LSP Seq Num  LSP Checksum  LSP Holdtime  Length  ATT/P/OL
0000.0000.0001.00-00 0x0000007E  0xD5DA      507           71     0/0/0
NLPID: IPv4
Area Address: 10
IP Address: 100.1.1.1
Metric: 10     IS-Extended 0000.0000.0001.01
Metric: 10     IP-Extended 10.1.1.0/24
Metric: 10     IP-Extended 100.1.1.0/24
0000.0000.0001.01-00 0x00000074  0xA8B0      799           51     0/0/0
Metric: 0      IS-Extended 0000.0000.0001.00
Metric: 0      IS-Extended 0000.0000.0002.00
0000.0000.0002.00-00* 0x00000082  0x5727     1146           71     1/0/0
NLPID: IPv4
Area Address: 10
```

单播路由

```
IP Address: 200.1.1.1
Metric: 10 IS-Extended 0000.0000.0001.01
Metric: 10 IP-Extended 100.1.1.0/24
Metric: 10 IP-Extended 200.1.1.0/24

IS-IS Instance 100 Level-2 Link State Database (Counter 3, LSP-MTU 1492):
LSPID          LSP Seq Num LSP Checksum LSP Holdtime Length ATT/P/OL
0000.0000.0002.00-00* 0x00000081 0x84C0      1047       79  0/0/0
NLPID: IPv4
Area Address: 10
IP Address: 200.1.1.1
Metric: 10 IS-Extended 0000.0000.0003.01
Metric: 20 IP-Extended 10.1.1.0/24
Metric: 10 IP-Extended 100.1.1.0/24
Metric: 10 IP-Extended 200.1.1.0/24
0000.0000.0003.00-00 0x00000315 0x9DC7      543        71  0/0/0
NLPID: IPv4
Area Address: 20
IP Address: 210.1.1.1
Metric: 10 IS-Extended 0000.0000.0003.01
Metric: 10 IP-Extended 200.1.1.0/24
Metric: 10 IP-Extended 210.1.1.0/24
0000.0000.0003.01-00 0x00000070 0xBF97      526        51  0/0/0
Metric: 0 IS-Extended 0000.0000.0002.00
Metric: 0 IS-Extended 0000.0000.0003.00
```

Device2 中包含 Level-1、Level-2 路由。

#查看 Device3 路由信息, Device3 中包含 Device1 通告的 Level-1 路由。

```
Device3#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNRP, B - BGP, i-IS-IS

Gateway of last resort is not set

i 10.1.1.0/24 [115/30] via 200.1.1.1, 16:59:29, vlan2
i 100.1.1.0/24 [115/20] via 200.1.1.1, 17:47:29, vlan2
C 127.0.0.0/8 is directly connected, 945:29:12, lo0
C 200.1.1.0/24 is directly connected, 18:40:27, vlan2
C 210.1.1.0/24 is directly connected, 16:59:04, vlan3
```

```
Device3#show isis ipv4 route
IS-IS Instance 100, VRF Kernel, IPv4 routes table (Counter 4):
L2 10.1.1.0/24, flags none, metric 30, from learned, installed
   via 200.1.1.1, vlan2, neighbor 0000.0000.0002
L2 100.1.1.0/24, flags none, metric 20, from learned, installed
   via 200.1.1.1, vlan2, neighbor 0000.0000.0002
L2 200.1.1.0/24, flags none, metric 10, from network connected
   via 0.0.0.0, vlan2
L2 210.1.1.0/24, flags none, metric 10, from network connected
   via 0.0.0.0, vlan3
```

```
Device3#show isis database detail
IS-IS Instance 100 Level-2 Link State Database (Counter 3, LSP-MTU 1492):
LSPID          LSP Seq Num LSP Checksum LSP Holdtime Length ATT/P/OL
0000.0000.0002.00-00 0x00000081 0x84C0      880        79  0/0/0
NLPID: IPv4
Area Address: 10
IP Address: 200.1.1.1
Metric: 10 IS-Extended 0000.0000.0003.01
Metric: 20 IP-Extended 10.1.1.0/24
Metric: 10 IP-Extended 100.1.1.0/24
Metric: 10 IP-Extended 200.1.1.0/24
0000.0000.0003.00-00* 0x00000316 0x9BC8      1197       71  0/0/0
NLPID: IPv4
Area Address: 20
```

单播路由

```
IP Address: 210.1.1.1
Metric: 10    IS-Extended 0000.0000.0003.01
Metric: 10    IP-Extended 200.1.1.0/24
Metric: 10    IP-Extended 210.1.1.0/24
0000.0000.0003.01-00* 0x00000070 0xBF97    359      51    0/0/0
Metric: 0     IS-Extended 0000.0000.0002.00
Metric: 0     IS-Extended 0000.0000.0003.00
```

步骤 3: 配置层间泄露。

#Device2 配置层间泄露。

```
Device2(config)#router isis 100
Device2(config-isis)#address-family ipv4 unicast
Device2(config-isis-af)#propagate level-2 into level-1
Device2(config-isis-af)#exit
Device2(config-isis)#exit
```

步骤 4: 检验结果。

#查看 Device1 的路由信息。

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-IS-IS
```

```
Gateway of last resort is 100.1.1.2 to network 0.0.0.0
```

```
i 0.0.0.0/0 [115/10] via 100.1.1.2, 17:44:09, vlan3
C 10.1.1.0/24 is directly connected, 16:56:18, vlan2
C 100.1.1.0/24 is directly connected, 18:37:57, vlan3
C 127.0.0.0/8 is directly connected, 284:02:13, lo0
i 200.1.1.0/24 [115/20] via 100.1.1.2, 17:44:09, vlan3
i 210.1.1.0/24 [115/30] via 100.1.1.2, 00:00:01, vlan3
```

```
Device1#show isis ipv4 route
L1 0.0.0.0/0, flags none, metric 10, from learned, installed
   via 100.1.1.2, vlan3, neighbor 0000.0000.0002
L1 100.1.1.0/24, flags none, metric 10, from network connected
   via 0.0.0.0, vlan3
L1 200.1.1.0/24, flags none, metric 20, from learned, installed
   via 100.1.1.2,vlan3, neighbor 0000.0000.0002
L1 210.1.1.0/24, flags inter-area, metric 30, from learned, installed
   via 100.1.1.2, vlan3, neighbor 0000.0000.0002
```

```
Device1#show isis database detail
IS-IS Instance 100 Level-1 Link State Database (Counter 3, LSP-MTU 1492):
LSPID      LSP Seq Num  LSP Checksum  LSP Holdtime  Length  ATT/P/OL
0000.0000.0001.00-00* 0x0000007F  0xD3DB      668          71    0/0/0
NLPID:     IPv4
Area Address: 10
IP Address: 100.1.1.1
Metric: 10    IS-Extended 0000.0000.0001.01
Metric: 10    IP-Extended 10.1.1.0/24
Metric: 10    IP-Extended 100.1.1.0/24
0000.0000.0001.01-00* 0x00000075  0xA6B1      995          51    0/0/0
Metric: 0     IS-Extended 0000.0000.0001.00
Metric: 0     IS-Extended 0000.0000.0002.00
0000.0000.0002.00-00 0x00000083  0x4DA6      984          79    1/0/0
NLPID:     IPv4
Area Address: 10
IP Address: 200.1.1.1
```

```
Metric: 10    IS-Extended 0000.0000.0001.01
Metric: 10    IP-Extended 100.1.1.0/24
Metric: 10    IP-Extended 200.1.1.0/24
Metric: 20    IP-Extended ia 210.1.1.0/24
```

Device1 除缺省路由外还学到了 Device3 通告的 Level-2 路由。

43.3.4 IS-IS 路由重分发 **-E -A**

网络需求

- 配置重分发将外部路由引入到 IS-IS 中使设备间达到网络互连。
- Device1、Device2 均为 Level-2 路由器，配置 IS-IS，区域号为 10。Device2 和 Device3 配置 OSPF。在 Device2 通过配置将 OSPF 路由重分发到 IS-IS 中。

网络拓扑

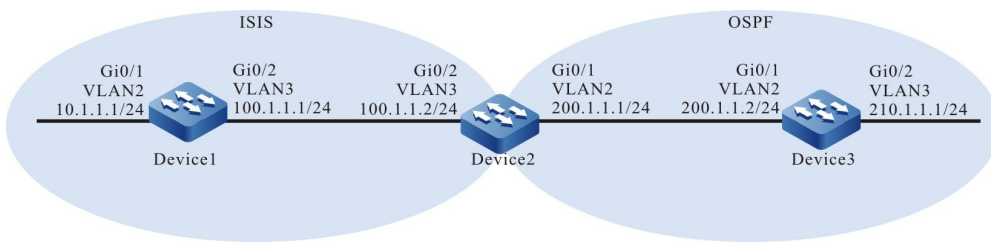


图 43-4 IS-IS 路由重分发组网图

配置步骤

步骤 1: 配置各接口的 IP 地址。（略）

步骤 2: 配置 IS-IS，并在接口启用该进程。

#Device1 配置 IS-IS 进程 100，区域号 10，类型为 Level-2 并在接口上启用该进程。

```
Device1#configure terminal
Device1(config)#router isis 100
Device1(config-isis)#net 10.0000.0000.0001.00
Device1(config-isis)#is-type level-2
Device1(config-isis)#metric-style wide
Device1(config-isis)#exit
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip router isis 100
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan3
Device1(config-if-vlan3)#ip router isis 100
Device1(config-if-vlan3)#exit
```

#Device2 配置 IS-IS 进程 100，区域号 10，类型为 Level-1-2 并在接口上启用该进程。

单播路由

```
Device2#configure terminal
Device2(config)#router isis 100
Device2(config-isis)#net 10.0000.0000.0002.00
Device2(config-isis)#is-type level-2
Device2(config-isis)#metric-style wide
Device2(config-isis)#exit
Device2(config)#interface vlan3
Device2(config-if-vlan3)#ip router isis 100
Device2(config-if-vlan3)#exit
```

步骤 3: 配置 OSPF。

#配置 Device2。

```
Device2(config)#router ospf 100
Device2(config-ospf)#network 200.1.1.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#配置 Device3。

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 210.1.1.0 0.0.0.255 area 0
Device3(config-ospf)#network 200.1.1.0 0.0.0.255 area 0
Device3(config-ospf)#exit
```

#查看 Device1 的路由表。Device1 没有学习到 Device2 重分发的 OSPF 路由。

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-IS-IS
```

Gateway of last resort is not set

```
C 10.1.1.0/24 is directly connected, 00:58:39, vlan2
C 100.1.1.0/24 is directly connected, 06:55:35, vlan3
C 127.0.0.0/8 is directly connected, 603:06:22, lo0
```

```
Device1#show isis ipv4 route
IS-IS Instance 100, VRF Kernel, IPv4 routes table (Counter 2):
L2 10.1.1.0/24, flags none, metric 10, from network connected
   via 0.0.0.0, vlan2
L2 100.1.1.0/24, flags none, metric 10, from network connected
   via 0.0.0.0, vlan3
```

```
Device1#show isis database detail
IS-IS Instance 100 Level-2 Link State Database (Counter 3, LSP-MTU 1492):
LSPID      LSP Seq Num  LSP Checksum  LSP Holdtime  Length  ATT/P/OL
0000.0000.0001.00-00* 0x00000046  0x489E       1123         71     0/0/0
  NLPID:    IPv4
  Area Address: 10
  IP Address: 100.1.1.1
  Metric: 10   IS-Extended 0000.0000.0001.01
  Metric: 10   IP-Extended 10.1.1.0/24
  Metric: 10   IP-Extended 100.1.1.0/24
0000.0000.0001.01-00* 0x00000045  0x097D       1103         51     0/0/0
  Metric: 0    IS-Extended 0000.0000.0001.00
  Metric: 0    IS-Extended 0000.0000.0002.00
0000.0000.0002.00-00 0x000000CB  0xEEA6       679          63     0/0/0
  NLPID:    IPv4
  Area Address: 10
  IP Address: 100.1.1.2
  Metric: 10   IS-Extended 0000.0000.0001.01
  Metric: 10   IP-Extended 100.1.1.0/24
```

单播路由

#查看 Device2 的路由表。Device2 分别学习到 ISIS 和 OSPF 路由。

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-IS-IS

Gateway of last resort is not set

i 10.1.1.0/24 [115/20] via 100.1.1.1, 15:45:37, vlan3
C 100.1.1.0/24 is directly connected, 22:38:58, vlan3
C 127.0.0.0/8 is directly connected, 300:03:03, lo0
C 200.1.1.0/24 is directly connected, 22:38:58, vlan2
O 210.1.1.1/32 [110/2] via 200.1.1.2, 15:43:35, vlan2

Device2#show isis ipv4 route
IS-IS Instance 100, VRF Kernel, IPv4 routes table (Counter 2):
L2 10.1.1.0/24, flags none, metric 20, from learned, installed
   via 100.1.1.1, vlan3, neighbor 0000.0000.0001
L2 100.1.1.0/24, flags none, metric 10, from network connected
   via 0.0.0.0, vlan3

Device2#show isis database detail
IS-IS Instance 100 Level-2 Link State Database (Counter 3, LSP-MTU 1492):
LSPID          LSP Seq Num  LSP Checksum  LSP Holdtime  Length  ATT/P/OL
0000.0000.0001.00-00 0x00000046  0x489E        911           71     0/0/0
  NLPID: IPv4
  Area Address: 10
  IP Address: 100.1.1.1
  Metric: 10    IS-Extended 0000.0000.0001.01
  Metric: 10    IP-Extended 10.1.1.0/24
  Metric: 10    IP-Extended 100.1.1.0/24
0000.0000.0001.01-00 0x00000045  0x097D        892           51     0/0/0
  Metric: 0     IS-Extended 0000.0000.0001.00
  Metric: 0     IS-Extended 0000.0000.0002.00
0000.0000.0002.00-00* 0x000000CB  0xEEA6        467           63     0/0/0
  NLPID: IPv4
  Area Address: 10
  IP Address: 100.1.1.2
  Metric: 10    IS-Extended 0000.0000.0001.01
  Metric: 10    IP-Extended 100.1.1.0/24
```

步骤 4: 配置 IS-IS 重分发 OSPF 路由。

#在 Device2 配置 OSPF 路由重分发至 IS-IS Level-2。

```
Device2(config)#router isis 100
Device2(config-isis)#address-family ipv4 unicast
Device2(config-isis-af)#redistribute ospf 100 level-2
Device2(config-isis-af)#exit
Device2(config-isis)#exit
```

步骤 5: 检验结果。

#查看 Device1 的路由信息。Device1 学习到 Device2 重分发的 OSPF 路由。

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-IS-IS

Gateway of last resort is not set
```



```
C 10.1.1.0/24 is directly connected, 16:47:30, vlan2
C 100.1.1.0/24 is directly connected, 22:44:27, vlan3
C 127.0.0.0/8 is directly connected, 618:55:13, lo0
i 200.1.1.0/24 [115/10] via 100.1.1.2, 00:00:05, vlan3
i 210.1.1.1/32 [115/10] via 100.1.1.2, 00:00:05, vlan3

Device1#show isis ipv4 route
IS-IS Instance 100, VRF Kernel, IPv4 routes table (Counter 4):
L2 10.1.1.0/24, flags none, metric 10, from network connected
   via 0.0.0.0, vlan2
L2 100.1.1.0/24, flags none, metric 10, from network connected
   via 0.0.0.0, vlan3
L2 200.1.1.0/24, flags none, metric 10, from learned, installed
   via 100.1.1.2, vlan3, neighbor 0000.0000.0002
L2 210.1.1.1/32, flags none, metric 10, from learned, installed
   via 100.1.1.2, vlan3, neighbor 0000.0000.0002

Device1#show isis database detail
IS-IS Instance 100 Level-2 Link State Database (Counter 3, LSP-MTU 1492):
LSPID          LSP Seq Num  LSP Checksum  LSP Holdtime  Length  ATT/P/OL
0000.0000.0001.00-00* 0x00000046  0x489E        626           71     0/0/0
NLPID:         IPv4
Area Address:  10
IP Address:    100.1.1.1
Metric: 10     IS-Extended 0000.0000.0001.01
Metric: 10     IP-Extended 10.1.1.0/24
Metric: 10     IP-Extended 100.1.1.0/24
0000.0000.0001.01-00* 0x00000045  0x097D        606           51     0/0/0
Metric: 0      IS-Extended 0000.0000.0001.00
Metric: 0      IS-Extended 0000.0000.0002.00
0000.0000.0002.00-00 0x000000CD  0xC6E2        1184          80     0/0/0
NLPID:         IPv4
Area Address:  10
IP Address:    100.1.1.2
Metric: 10     IS-Extended 0000.0000.0001.01
Metric: 10     IP-Extended 100.1.1.0/24
Metric: 0      IP-Extended 200.1.1.0/24
Metric: 0      IP-Extended 210.1.1.1/32
```

Device1 学习到重分发的 OSPF 路由。

43.3.5 配置 IS-IS 邻居认证

-E -A

网络需求

- 通过在接口上启用认证使配置相同密码的设备间建立邻居。
- Device1 为 Level-1 路由器，Device2 为 Level-1-2 路由器，Device1 和 Device2 在同一区域内，区域号为 10。Device3 为 Level-2 路由器，区域号为 20。Device2 承担连接两个区域的功能。

网络拓扑

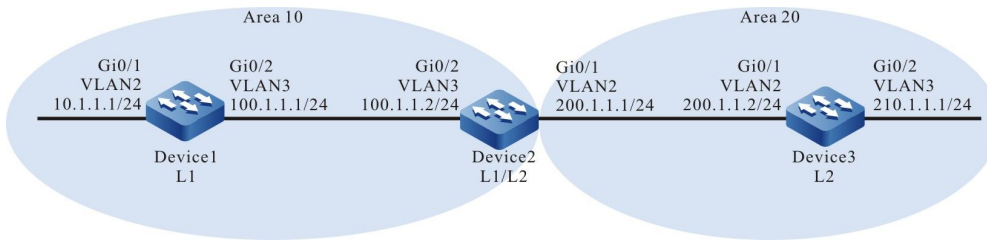


图 43-5 IS-IS 邻居认证组网图

配置步骤

步骤 1: 配置各接口的 IP 地址。(略)

步骤 2: 配置 IS-IS, 并在接口启用该进程。

#Device1 配置 IS-IS 进程 100, 区域号 10, 类型为 Level-1 并在接口上启用该进程。

```
Device1#configure terminal
Device1(config)#router isis 100
Device1(config-isis)#net 10.0000.0000.0001.00
Device1(config-isis)#is-type level-1
Device1(config-isis)#metric-style wide
Device1(config-isis)#exit
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip router isis 100
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan3
Device1(config-if-vlan3)#ip router isis 100
Device1(config-if-vlan3)#exit
```

#Device2 配置 IS-IS 进程 100, 区域号 10, 类型为 Level-1-2 并在接口上启用该进程。

```
Device2#configure terminal
Device2(config)#router isis 100
Device2(config-isis)#net 10.0000.0000.0002.00
Device2(config-isis)#metric-style wide
Device2(config-isis)#exit
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ip router isis 100
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan3
Device2(config-if-vlan3)#ip router isis 100
Device2(config-if-vlan3)#exit
```

#Device3 配置 IS-IS 进程 100, 区域号 20, 类型为 Level-2 并在接口上启用该进程。

```
Device3#configure terminal
Device3(config)#router isis 100
Device3(config-isis)#net 20.0000.0000.0003.00
Device3(config-isis)#is-type level-2
Device3(config-isis)#metric-style wide
Device3(config-isis)#exit
Device3(config)#interface vlan2
Device3(config-if-vlan2)#ip router isis 100
Device3(config-if-vlan2)#exit
Device3(config)#interface vlan3
Device3(config-if-vlan3)#ip router isis 100
Device3(config-if-vlan3)#exit
```

#查看 Device1 的 IS-IS 邻居信息。

```
Device1#show isis neighbors
IS-IS Instance 100 Neighbors (Counter 1):
Type System ID Interface State Holdtime Level IETF-NSF Priority Circuit ID
L1-LAN 0000.0000.0002 vlan3 Up 29 sec L1 capable 64 0000.0000.0001.01
```

#查看 Device2 的 IS-IS 邻居信息。

```
Device2#show isis neighbors
IS-IS Instance 100 Neighbors (Counter 2):
Type System ID Interface State Holdtime Level IETF-NSF Priority Circuit ID
L2-LAN 0000.0000.0003 vlan2 Up 9 sec L2 capable 64 0000.0000.0003.01
L1-LAN 0000.0000.0001 vlan3 Up 7 sec L1 capable 64 0000.0000.0001.01
```

#查看 Device3 的 IS-IS 邻居信息。

```
Device3#show isis neighbors
IS-IS Instance 100 Neighbors (Counter 1):
Type System ID Interface State Holdtime Level IETF-NSF Priority Circuit ID
L2-LAN 0000.0000.0002 vlan2 Up 24 sec L2 capable 64 0000.0000.0003.01
```

步骤 3: 配置认证。

#在 Device2 的接口上配置 MD5 认证, 密码为 admin。

```
Device2(config)#interface vlan2
Device2(config-if-vlan2)#isis authentication mode md5
Device2(config-if-vlan2)#isis authentication key 0 admin
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan3
Device2(config-if-vlan3)#isis authentication mode md5
Device2(config-if-vlan3)#isis authentication key 0 admin
Device2(config-if-vlan3)#exit
```

#查看 Device2 的 IS-IS 邻居。

```
Device2#show isis neighbors
IS-IS Instance 100 Neighbors (Counter 0):
Type System ID Interface State Holdtime Level IETF-NSF Priority Circuit ID
```

此时 Device1 和 Device3 尚未配置认证, Device2 没有建立 ISIS 邻居。

#在 Device1 的 vlan3 接口上配置 MD5 认证, 密码为 admin。

```
Device1(config)#interface vlan3
Device1(config-if-vlan3)#isis authentication mode md5
Device1(config-if-vlan3)#isis authentication key 0 admin
Device1(config-if-vlan3)#exit
```

#在 Device3 的 vlan2 接口上配置 MD5 认证, 密码为 admin。

```
Device3(config)#interface vlan2
Device3(config-if-vlan2)#isis authentication mode md5
Device3(config-if-vlan2)#isis authentication key 0 admin
Device3(config-if-vlan2)#exit
```

步骤 4: 检验结果。

单播路由

#查看 Device1 的 IS-IS 邻居信息。

```
Device1#show isis neighbors
IS-IS Instance 100 Neighbors (Counter 1):
Type System ID Interface State Holdtime Level IETF-NSF Priority Circuit ID
L1-LAN 0000.0000.0002 vlan3 Up 29 sec L1 capable 64 0000.0000.0001.01
```

可以看到 Device1 与 Device2 成功建立 ISIS 邻居，说明认证成功。

#查看 Device2 的 IS-IS 邻居信息。

```
Device2#show isis neighbors
IS-IS Instance 100 Neighbors (Counter 2):
Type System ID Interface State Holdtime Level IETF-NSF Priority Circuit ID
L2-LAN 0000.0000.0003 vlan2 Up 9 sec L2 capable 64 0000.0000.0003.01
L1-LAN 0000.0000.0001 vlan3 Up 7 sec L1 capable 64 0000.0000.0001.01
```

可以看到 Device2 与 Device1、Device3 成功建立 ISIS 邻居，说明认证成功。

#查看 Device3 的 IS-IS 邻居信息。

```
Device3#show isis neighbors
IS-IS Instance 100 Neighbors (Counter 1):
Type System ID Interface State Holdtime Level IETF-NSF Priority Circuit ID
L2-LAN 0000.0000.0002 vlan2 Up 24 sec L2 capable 64 0000.0000.0003.01
```

可以看到 Device3 与 Device2 成功建立 ISIS 邻居，说明认证成功。

#查看 Device2 的路由信息。能正常接收 Device1 和 Device3 通告的路由。

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-IS-IS
```

Gateway of last resort is not set

```
i 10.1.1.0/24 [115/20] via 100.1.1.1, 16:58:26, vlan3
C 100.1.1.0/24 is directly connected, 18:39:58, vlan3
C 127.0.0.0/8 is directly connected, 20:16:34, lo0
C 200.1.1.0/24 is directly connected, 18:39:37, vlan2
i 210.1.1.0/24 [115/20] via 200.1.1.2, 16:57:56, vlan2
```

```
Device2#show isis ipv4 route
IS-IS Instance 100, VRF Kernel, IPv4 routes table (Counter 4):
L1 10.1.1.0/24, flags none, metric 20, from learned, installed
via 100.1.1.1, vlan3, neighbor 0000.0000.0001
L1 100.1.1.0/24, flags none, metric 10, from network connected
via 0.0.0.0, vlan3
L1 200.1.1.0/24, flags none, metric 10, from network connected
via 0.0.0.0, vlan2
L2 210.1.1.0/24, flags none, metric 20, from learned, installed
via 200.1.1.2, vlan2, neighbor 0000.0000.0003
```

43.3.6 配置 IS-IS 与 BFD 联动

-E -A

网络需求

- 在设备间配置 BFD 关联，当主线路出现故障后业务能快速切换到备用线路。

- Device1、Device2、Device3 均为 Level-2 路由器且在同一区域内，区域号为 10。在 Device1 和 Device3 中配置 BFD 使其建立会话。当 Device1 和 Device3 中间线路出现异常断开时 Device1 能快速切换，从 Device2 上学习到 10.1.1.1/24 路由。

网络拓扑

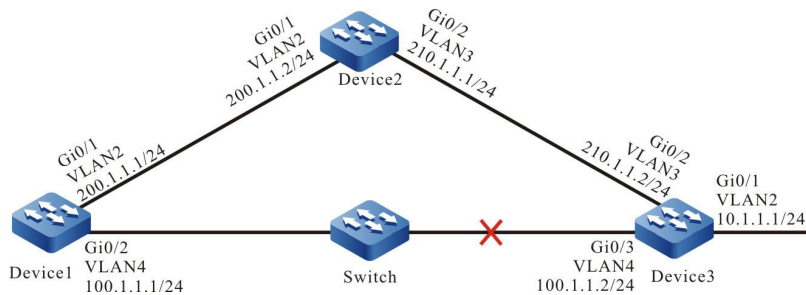


图 43-6 IS-IS 与 BFD 联动组网图

配置步骤

步骤 1： 配置各接口的 IP 地址。（略）

步骤 2： 配置 IS-IS，并在接口启用该进程。

#Device1 配置 IS-IS 进程 100，区域号 10，类型为 Level-2 并在接口上启用该进程。

```
Device1#configure terminal
Device1(config)#router isis 100
Device1(config-isis)#net 10.0000.0000.0001.00
Device1(config-isis)#is-type level-2
Device1(config-isis)#metric-style wide
Device1(config-isis)#exit
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip router isis 100
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan4
Device1(config-if-vlan4)#ip router isis 100
Device1(config-if-vlan4)#exit
```

#Device2 配置 IS-IS 进程 100，区域号 10，类型为 Level-2 并在接口上启用该进程。

```
Device2#configure terminal
Device2(config)#router isis 100
Device2(config-isis)#net 10.0000.0000.0002.00
Device2(config-isis)#is-type level-2
Device2(config-isis)#metric-style wide
Device2(config-isis)#exit
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ip router isis 100
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan3
Device2(config-if-vlan3)#ip router isis 100
Device2(config-if-vlan3)#exit
```

单播路由

#Device3 配置 IS-IS 进程 100，区域号 10，类型为 Level-2 并在接口上启用该进程。

```
Device3#configure terminal
Device3(config)#router isis 100
Device3(config-isis)#net 10.0000.0000.0003.00
Device3(config-isis)#is-type level-2
Device3(config-isis)#metric-style wide
Device3(config-isis)#exit
Device3(config)#interface vlan2
Device3(config-if-vlan2)#ip router isis 100
Device3(config-if-vlan2)#exit
Device3(config)#interface vlan3
Device3(config-if-vlan3)#ip router isis 100
Device3(config-if-vlan3)#exit
Device3(config)#interface vlan4
Device3(config-if-vlan4)#ip router isis 100
Device3(config-if-vlan4)#exit
```

#查看 Device1 的路由信息，Device1 优选从 Device3 通告的路由 10.1.1.0/24。

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-IS-IS

Gateway of last resort is not set

i 10.1.1.0/24 [115/20] via 100.1.1.2, 00:00:15, vlan4
C 100.1.1.0/24 is directly connected, 00:09:15, vlan4
C 127.0.0.0/8 is directly connected, 253:58:17, lo0
C 200.1.1.0/24 is directly connected, 00:11:29, vlan2
i 210.1.1.0/24 [115/20] via 100.1.1.2, 00:00:15, vlan4
  [115/20] via 200.1.1.2, 00:00:15, vlan2
Device1#show isis ipv4 route
IS-IS Instance 100, VRF Kernel, IPv4 routes table (Counter 4):
L2 10.1.1.0/24, flags none, metric 20, from learned, installed
   via 100.1.1.2, vlan4, neighbor 0000.0000.0003
L2 100.1.1.0/24, flags none, metric 10, from network connected
   via 0.0.0.0, vlan4
L2 200.1.1.0/24, flags none, metric 10, from network connected
   via 0.0.0.0, vlan2
L2 210.1.1.0/24, flags none, metric 20, from learned, installed
   via 100.1.1.2, vlan4, neighbor 0000.0000.0003
   via 200.1.1.2, vlan2, neighbor 0000.0000.0002
```

步骤 3: 配置 BFD。

#Device1 接口下启用 BFD。

```
Device1(config)#bfd fast-detect
Device1(config)#interface vlan4
Device1(config-if-vlan4)#isis bfd
Device1(config-if-vlan4)#exit
#Device3 接口下启用 BFD。
Device3(config)#bfd fast-detect
Device3(config)#interface vlan4
Device3(config-if-vlan4)#isis bfd
Device3(config-if-vlan4)#exit
```

#查看 Device1 的 BFD 信息。

```
Device1#show bfd session
OurAddr      NeighAddr      LD/RD      State
100.1.1.2    100.1.1.1      1/1        UP
```

```
Holddown      interface
5000          vlan4
```

步骤 4: 检验结果。

#当 Device1 与 Device3 间的线路出现故障后, BFD 会快速检测到故障并通知 ISIS, ISIS 将路由切换至 Device2 上进行通信。查看 Device1 的路由表。

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-IS-IS

Gateway of last resort is not set

i 10.1.1.0/24 [115/30] via 200.1.1.2, 00:00:14, vlan2
C 127.0.0.0/8 is directly connected, 112:55:25, lo0
C 200.1.1.0/24 is directly connected, 101:20:08, vlan2

Device1#show isis ipv4 route
IS-IS Instance 100, VRF Kernel, IPv4 routes table (Counter 2):
L2 10.1.1.0/24, flags none, metric 30, from l earned, installed
   via 200.1.1.2, vlan2, neighbor 0000.0000.0003
L2 200.1.1.0/24, flags none, metric 20, from network connected
   via 0.0.0.0, vlan2
```

#可以看到 Device1 到 10.1.1.0/24 网段的数据流优先 Device2。

44 BGP

44.1 BGP 简介

BGP (Border Gateway Protocol, 边界网关协议) 是一种用来在自治系统 (Autonomous System, AS) 之间交换网络层可达性信息 (Network Layer Reachability Information, NLRI) 的

路由选择协议。区别于内部网关协议（IGP, Internal Gateway Protocol），如常见的 RIP、OSPF、IS-IS 等，内部网关协议重点在于寻找确切的路径，以网络节点（路由器、三层交换机、多网卡主机等）为寻路单位，而外部网关协议（EGP, External Gateway Protocol）则重点在于控制路由方向，以 AS 网络为单位。

BGP 应用于 AS 网络之间的互联，提供 AS 间的路由信息交换，多用于大型网络汇聚和网络核心。这种应用层次决定 BGP 较 IGP 而言具有以下特征：

- BGP 使用 TCP 协议传输报文，服务端口号 179，TCP 保证了传输的可靠性，BGP 就不需要为保证信息的可靠而单独设计一套传输控制策略；
- BGP 通过增量的形式更新路由，即只有当路由属性发生变化或添删路由时才会向邻居通告这类路由变化，这种方式大大减少了 BGP 传播路由所占用的网络带宽；
- BGP 是一种基于 AS 的距离向量协议，通过在路由报文中携带 AS 路径属性以解决路由环路问题；
- BGP 路由具有丰富的属性，通过应用路由策略修改这些属性可以达到自由的控制路由过滤和选择；
- BGP 具有两种邻居类型，即 IBGP 与 EBGP，不同类型邻居之间具有不同的路由通告与选路策略。

44.2 BGP 功能配置

表 44-1 BGP 功能配置列表

配置任务	
配置 BGP 邻居	配置 IBGP 邻居
	配置 EBGP 邻居
	配置 BGP 被动邻居
	配置 MP-BGP 邻居
	配置 BGP 邻居 MD5 认证

配置任务	
配置 BGP 路由生成	配置 BGP 发布本地路由
	配置 BGP 路由重分发
	配置 BGP 发布缺省路由
配置 BGP 路由控制	配置 BGP 发布聚合路由
	配置 BGP 路由管理距离
	配置 BGP 邻居出方向路由策略
	配置 BGP 邻居入方向路由策略
	配置 BGP 邻居接收路由最大条目数
	配置 BGP 最大负载均衡条目数
配置 BGP 路由属性	配置 BGP 路由权重
	配置 BGP 路由 MED 属性
	配置 BGP 路由 Local-Preference 属性
	配置 BGP 路由 AS_PATH 属性
	配置 BGP 路由 NEXT-HOP 属性
	配置 BGP 路由团体属性
配置 BGP 网络优化	配置 BGP 邻居保活时间
	配置 BGP 路由检测时间

配置任务	
	配置 EBGp 邻居快速断连
	配置 BGP 路由抑制功能
	配置 BGP 邻居刷新能力
	配置 BGP 邻居软重置能力
	配置 BGP 邻居 ORF 能力
配置 BGP 大型网络	配置 BGP 对等体组
	配置 BGP 路由反射器
	配置 BGP 联盟
配置 BGP GR	配置 BGP GR Helper
配置 BGP 与 BFD 联动	配置 EBGp 与 BFD 联动
	配置 IBGP 与 BFD 联动

44.2.1 配置 BGP 邻居 -E -A

配置条件

在配置 BGP 邻居之前，首先完成以下任务：

- 配置链路层协议，保证链路层通信正常；
- 配置接口的网络层地址，使相邻网络节点网络层可达。

配置 IBGP 邻居

1、基本配置

单播路由

配置 IBGP 邻居需要指定邻居 AS 与本设备 AS 相同。可以对设备配置 Router ID，该 Router ID 用于建立 BGP 会话时，唯一标明一台 BGP 设备，未配置 Router ID 时将由设备根据接口地址进行优选，优先方式原则如下：

- 首先从 Loopback 接口的 IP 地址中选择最大的作为 Router ID；
- 若没有配置 IP 地址的 Loopback 接口，则从其它接口的 IP 地址中选择最大的作为 Router ID；
- 只有接口处于 UP 状态时，该接口地址才可能被选作 Router ID。

表 44-2 配置 IBGP 邻居

步骤	命令	说明
进入全局配置模式	configure terminal	-
启用 BGP 协议并进入 BGP 配置模式	router bgp <i>autonomous-system</i>	必选 缺省情况下，未启用 BGP
配置 BGP 设备标识	bgp router-id <i>router-id</i>	可选 缺省情况下，设备根据接口地址进行优选，优先方式采用 Loopback 接口优先与 IP 地址大优先原则
配置 IBGP 邻居	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } remote-as <i>as-number</i>	必选 缺省情况下，未创建任何 IBGP 邻居
激活 IBGP 邻居收发 IPv4 单播路由的能力	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } activate	可选

步骤	命令	说明
		缺省情况下，自动激活 IBGP 邻居收发 IPv4 单播路由的能力
配置 IBGP 邻居描述	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } description <i>description-string</i>	可选 缺省情况下，IBGP 邻居无描述信息

2、配置 TCP 会话的源地址

BGP 使用 TCP 作为其传输协议，TCP 具有传输可靠的特点，有效保证 BGP 协议报文能正确传输给邻居。

表 44-3 配置 TCP 会话的源地址

步骤	命令	说明
进入全局配置模式	configure terminal	-
启用 BGP 协议并进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
配置 IBGP 邻居	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } remote-as <i>as-number</i>	必选 缺省情况下，未创建任何 IBGP 邻居
配置 IBGP 邻居 TCP 会话的源地址	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } update-source { <i>interface-name</i> <i>ip-address</i> }	必选 缺省情况下，TCP 会话自动选择路由出接口的地址作为源地址

说明：

- 在存在负载均衡路由时需要 BGP 邻居之间明确配置 TCP 会话的源地址，未配置 TCP 源地址时，可能由于邻居的最优路由不同，而采用不同出接口作为各自的源地址，导致 BGP 会话一段时间内无法成功建立。

配置 EBGP 邻居

1、基本配置

配置 EBGP 邻居需要指定邻居 AS 与本设备 AS 不同。

表 44-4 配置 EBGP 邻居

步骤	命令	说明
进入全局配置模式	configure terminal	-
启用 BGP 协议并进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
配置 EBGP 邻居	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } remote-as <i>as-number</i>	必选 缺省情况下，未创建任何 EBGP 邻居

2、配置非直连 EBGP 邻居

EBGP 邻居各自处于不同的运营网络，通常由一条直连的物理链路进行连接，所以 EBGP 邻居间通信的 IP 报文缺省 TTL 值为 1，如果在非直连的运营网络之间，可以通过配置命令设置 IP 报文的 TTL 值，以达到允许 BGP 建连的目的。

表 44-5 配置非直连 EBGP 邻居

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
配置 EBGP 邻居	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } remote-as <i>as-number</i>	必选 缺省情况下，未创建任何 EBGP 邻居
配置 EBGP 邻居 TCP 会话的源地址	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } update-source { <i>interface-name</i> <i>ip-address</i> }	可选 缺省情况下，TCP 会话自动选择路由出接口的地址作为源地址
配置允许非直连 EBGP 邻居间建立连接	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } ebgp-multihop [<i>ttl-value</i>]	必选 缺省情况下，不允许非直连设备间形成 EBGP 邻居关系

配置 BGP 被动邻居

特殊应用环境中需要用到 BGP 的被动邻居功能。应用被动邻居后，BGP 不主动向邻居发起用于建立 BGP 邻居的 TCP 连接请求，只能等待邻居主动建连请求才能建立邻居关系。缺省情况下，邻居双方将相互主动发起连接，在连接存在冲突时将优选一条 TCP 连接形成 BGP 会话。在配置 BGP 被动邻居之前，需要配置 BGP 邻居。

表 44-6 配置 BGP 被动邻居

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
配置 BGP 邻居	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } remote-as <i>as-number</i>	必选 缺省情况下, 未创建任何 BGP 邻居
配置 BGP 被动邻居	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } passive	必选 缺省情况下, 未启用任何被动邻居

配置 MP-BGP 邻居

缺省情况下, BGP 邻居缺省在 IPv4 单播地址族下激活, 具备收发 IPv4 单播路由的能力, 而其他地址族下需要通过配置命令激活邻居, 使其具有收发对应路由的能力, 如组播地址簇、VRF 地址簇、LS 单播地址簇等。在配置 MP-BGP 邻居之前, 需要配置 BGP 邻居。

表 44-7 配置 MP-BGP 邻居

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
配置 BGP 邻居	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } remote-as <i>as-number</i>	必选 缺省情况下, 未创建任何 BGP 邻居

步骤	命令	说明
进入 BGP IPv4 组播配置模式	address-family ipv4 multicast	必选 缺省情况下，进入 BGP 配置模式后处于单播地址簇模式
BGP IPv4 组播地址簇下激活邻居	neighbor { neighbor-address peer-group-name } activate	必选 缺省情况下，全局邻居未在组播地址簇下激活
退出 BGP IPv4 组播配置模式	exit-address-family	-
进入 BGP IPv4 VRF 配置模式	address-family ipv4 vrf vrf-name	-
配置 BGP IPv4 VRF 地址簇下邻居	neighbor { neighbor-address peer-group-name } remote-as as-number	必选 缺省情况下，未创建任何 BGP 邻居
IPv4 VRF 地址簇下激活邻居	neighbor { neighbor-address peer-group-name } activate	可选 缺省情况下，BGP IPv4 VRF 配置模式的邻居已处于激活状态
退出 BGP IPv4 VRF 配置模式	exit-address-family	-
进入 BGP LS 配置模式	address-family link-state unicast	-

步骤	命令	说明
BGP LS 单播地址簇下激活邻居	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } activate	必选 缺省情况下，全局邻居未在 VPN 地址簇下激活
退出 BGP LS 配置模式	exit-address-family	-

说明：

- 在 BGP 配置模式和 BGP IPv4 单播配置模式下配置的邻居为全局邻居，在 BGP IPv4 VRF 配置模式下配置的邻居仅属于该 VRF 地址簇。

配置 BGP 邻居 MD5 认证

BGP 支持配置 MD5 认证对邻居间的信息交互进行保护，MD5 认证由 TCP 传输协议完成。邻居双方必须配置相同的 MD5 认证密码才能建立 TCP 连接，否则 TCP 传输协议对 MD5 认证失败后将不能建立 TCP 连接。配置 BGP 邻居 MD5 认证前，需要配置 BGP 邻居。

表 44-8 配置 BGP 邻居 MD5 认证

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
配置 BGP 邻居	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> }	必选 缺省情况下，未创建任何 BGP 邻居

步骤	命令	说明
	remote-as <i>as-number</i>	
配置 BGP 邻居 MD5 认证	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } password [0 7] <i>password-string</i>	必选 缺省情况下，BGP 邻居间不进行 MD5 认证

44.2.2 配置 BGP 路由生成

-E -A

配置条件

在配置 BGP 路由生成之前，首先完成以下任务：

- 启用 BGP 协议；
- 配置 BGP 邻居并使会话建立成功。

配置 BGP 发布本地路由

BGP 可以通过 **network** 命令引入 IP 路由表中的路由到 BGP 路由表中，仅当 IP 路由表中有与 **network** 前缀和掩码完全匹配的条目，才会将该路由引入到 BGP 路由表中并且将之发布。

在发布本地路由的同时，可以对路由应用路由图，也可以指定该路由为后门路由。后门路由将 EBGp 路由看作是本地 BGP 路由并使用本地路由的管理距离，这样允许 IGP 路由优先于 EBGp 路由，同时，后门路由不会通告给 EBGp 邻居。

表 44-9 配置 BGP 发布本地路由

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-

步骤	命令	说明
配置 BGP 发布本地路由	network <i>ip-address mask</i> [route-map <i>rtmap-name</i> [backdoor] backdoor]	必选 缺省情况下, BGP 不发布任何本地路由

说明:

- BGP 发布本地路由的路由 Origin 属性类型为 IGP。
- 使用 **network backdoor** 命令作用 EBGp 路由后, EBGp 路由管理距离将变成本地路由管理距离 (缺省情况下, EBGp 路由管理距离为 20, 本地路由管理距离为 200), 低于缺省 IGP 路由管理距离, 使 IGP 路由被优选, 这样 EBGp 邻居间形成后门链路。
- BGP 发布本地路由应用路由图支持的 match 选项有 as-path、community、extcommunity、ip address、ip nexthop、metric, 支持的 set 选项有 as-path、comm-list、community、extcommunity、ip next-hop、local-preference、metric、origin、weight。

配置 BGP 路由重分发

BGP 主要不负责学习路由, 而重点通过管理路由属性达到控制路由方向的目的, 因此 BGP 通过重分发 IGP 来产生 BGP 路由向邻居通告。BGP 重分发 IGP 路由的同时, 可以应用路由图。

表 44-10 配置 BGP 路由重分发

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
配置 BGP 重分发 IGP 路由	redistribute { connected irmp <i>as-number</i> isis	必选

步骤	命令	说明
	<code>[area-tag] [match isis-level] ospf as-number [match route-sub-type] rip static } [route-map map-name / metric value]</code>	缺省情况下，BGP 不重分发其它任何 IGP 路由

说明：

- BGP 重分发的 IGP 路由 Origin 属性类型为 INCOMPLETE。
- BGP 重分发其它协议应用路由图支持的 match 选项有 as-path、community、extcommunity、ip address、ip nexthop、metric，支持的 set 选项有 as-path、comm-list、community、extcommunity、ip next-hop、local-preference、metric、origin、weight。

配置 BGP 发布缺省路由

BGP 向邻居发布缺省路由前，需要引入缺省路由。引入缺省路由有两种方式：通过 **neighbor default-originate** 命令生成 BGP 的缺省路由；通过 **default-information originate** 命令重分发其它协议的缺省路由。

neighbor default-originate 命令生成的缺省路由是通过 BGP 自动产生一条 0.0.0.0/0 的路由，**default-information originate** 命令重分发的缺省路由是 BGP 引入被重分发协议的一条 0.0.0.0/0 的路由。

表 44-11 配置 BGP 发布缺省路由

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
配置 BGP 生成缺省路由	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } default-originate [route-map <i>rtmap-name</i>]	必选 缺省情况下, BGP 不产生缺省路由
配置 BGP 重分发其他协议的缺省路由	default-information originate	必选 缺省情况下, BGP 不重分发其它协议的缺省路由

说明:

- 配置 BGP 重分发其它协议的缺省路由同时需要配置路由重分发。
- 可以在配置 BGP 生成缺省路由时对该路由应用路由图。
- BGP 生成缺省路由应用路由图支持的 set 选项有 as-path、comm-list、community、extcommunity、ip next-hop、local-preference、metric、origin、weigh。

44.2.3 配置 BGP 路由控制

-E -A

配置条件

在配置 BGP 路由控制之前, 首先完成以下任务:

- 启用 BGP 协议;

- 配置 BGP 邻居并使会话建连成功。

配置 BGP 发布聚合路由

在大型 BGP 网络中，为了减少向邻居通告的路由数量或者有效控制 BGP 选路过程，需要配置 BGP 聚合路由。

表 44-12 配置 BGP 发布聚合路由

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
配置 BGP 发布聚合路由	aggregate-address <i>ip-address mask</i> [as-set / summary-only / route-map <i>rtmap-name</i>]	必选 缺省情况下，BGP 不会进行路由聚合

说明：

- BGP 发布聚合路由时，可以通过指定 **summary-only** 命令选项只通告聚合路由来达到减少路由通告规模的目的。
- 通过指定 **as-set** 命令选项可以生成具有 AS_PATH 属性的聚合路由。
- 通过对聚合路由应用路由图可以设置聚合路由更丰富的属性。

配置 BGP 路由管理距离

在 IP 路由表中各个协议都有控制选路的管理距离，该值越小越优先。BGP 通过对指定网段路由配置管理距离的方式来影响选路，覆盖到指定网段路由的管理距离都会被修改，同时可以应用 ACL 对覆盖网段进行有效过滤，仅 ACL 允许网段的管理距离才会被修改。

distance bgp 命令用于同时修改 BGP 外部、内部以及本地路由的管理距离，**distance** 命令仅用于修改指定网段路由的管理距离。**distance** 命令优先于 **distance bgp** 命令，配置 **distance** 覆盖的网段将采用该命令指定的管理距离，未覆盖的网段才采用 **distance bgp** 设置的管理距离。

表 44-13 配置 BGP 路由管理距离

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
配置 BGP 修改缺省管理距离	distance bgp <i>external-distance internal-distance local-distance</i>	可选 缺省情况下，EBGP 路由管理距离为 20，
配置指定网段的管理距离	distance administrative-distance <i>ip-address mask [acl-name]</i>	IBGP 路由管理距离为 200，本地路由管理距离为 200

配置 BGP 邻居出方向路由策略

BGP 路由通告或选路依赖其强大的路由属性完成，在通告路由给邻居时可以通过应用相应的策略对路由属性进行修改或者过滤掉部份路由。目前支持在出方向上应用的策略有：

- distribute-list: 分布列表；
- filter-list : AS_PATH 属性过滤列表；
- prefix-list: IP 前缀列表；
- route-map: 路由图。

表 44-14 配置 BGP 邻居出方向路由策略

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
指定在出方向上应用分布列表	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } distribute-list <i>access-list-name</i> out	<p>多选（分布列表与 IP 前缀列表不能同时配置）</p> <p>缺省情况下，未配置 BGP 邻居出方向路由策略</p>
指定在出方向上应用 AS_PATH 属性过滤列表	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } filter-list <i>aspath-list-name</i> out	
指定在出方向上应用 IP 前缀列表	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } prefix-list <i>prefix-list-name</i> out	
指定在出方向上应用路由图	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } route-map <i>rtmap-name</i> out	

说明：

- 配置 BGP 邻居出方向路由策略后，需要重置邻居才能生效。
- 配置路由反射器出方向上应用路由图时，只能改变 NEXT-HOP 属性。
- 配置过滤列表请参见策略工具-配置 AS-PATH 列表章节。
- 配置邻居出方向上的策略时，可以同时配置多个，BGP 按照 **distribute-list**、**filter-**

list、**prefix-list**、**route-map** 的先后顺序进行应用，排在前面的策略拒绝后不会进行后面策略的应用，只有配置的所有策略都通过后才通告路由信息。

- BGP 出方向上应用的路由图支持的 match 选项有 as-path、community、extcommunity、ip address、ip nexthop、metric，支持的 set 选项有 as-path、comm-list、community、extcommunity、ip next-hop、local-preference、metric、origin、weight。

配置 BGP 邻居入方向路由策略

BGP 可以应用策略对接收到的路由信息过滤或修改其属性，与出方向上应用策略相同，入方向上也支持四种策略：

- distribute-list：分布列表；
- filter-list：AS_PATH 属性过滤列表；
- prefix-list：IP 前缀列表；
- route-map：路由图。

表 44-15 配置 BGP 邻居入方向应用策略

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
指定在入方向上应用分布列表	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } distribute-list <i>access-list-name in</i>	多选（分布列表与 IP 前缀列表不能同时配置）
指定在入方向上应用 AS_PATH 属性过滤列表	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } filter-list <i>aspath-list-name in</i>	缺省情况下，在入方向上没有指定任何策略

步骤	命令	说明
指定在入方向上应用 IP 前缀列表	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } prefix-list <i>prefix-list-name</i> in	
指定在入方向上应用路由图	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } route-map <i>rtmap-name</i> in	

说明：

- 配置 BGP 邻居入方向路由策略后，需要重置邻居才能生效。
- 配置邻居入方向上的策略时，可以同时配置多个，BGP 按照 **distribute-list**、**filter-list**、**prefix-list**、**route-map** 的先后顺序进行应用，排在前面的策略拒绝后不会进行后面策略的应用，只有配置的所有策略都通过后才将路由加入到数据库中。
- BGP 入方向上应用的路由策略支持的 match 选项有 as-path、community、extcommunity、ip address、ip nexthop、metric，支持的 set 选项有 as-path、comm-list、community、extcommunity、ip next-hop、local-preference、metric、origin、weight。

配置 BGP 邻居接收路由最大条目数

BGP 设备支持对指定邻居限制接收路由的条目数，当从指定邻居接收到的路由达到一定阈值时进行告警或者断连。

表 44-16 配置 BGP 邻居接收路由最大条目数

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
配置邻居接收的最大路由条目数	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } maximum-prefix <i>prefix-num</i> [<i>threshold-value</i>] [warning-only]	必选 缺省情况下, 没有限制从邻居接收的前缀条目数

说明:

- 如果未指定 **warning-only** 命令选项, 在 BGP 从邻居接收的路由达到最大条目数时, 将自动断开 BGP 会话。
- 如果指定 **warning-only** 命令选项, 在 BGP 从邻居接收的路由达到最大条目数时, 仅给出告警信息, 不阻止路由继续学习。

配置 BGP 最大负载均衡条目数

在 BGP 组网环境中, 如果到达同一个目的地具有几条开销相同路径, 那么可以通过配置 BGP 负载条目数来形成负载均衡路由。

表 44-17 配置 BGP 最大负载均衡条目数

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-

步骤	命令	说明
配置 IBGP 最大负载条目数	maximum-paths ibgp <i>number</i>	必选 缺省情况下, IBGP 不进行负载均衡路由选路
配置 EBGP 最大负载条目数	maximum-paths <i>number</i>	必选 缺省情况下, EBGP 不进行负载均衡路由选路

说明:

- 配置 EBGP 最大负载均衡条目数后, 仅当 EBGP 路由被优选后才能形成负载。
- 配置最大负载均衡条目数在不同 BGP 配置模式下命令不同, 详见 BGP 技术手册对 **maximum-paths** 描述。

44.2.4 配置 BGP 路由属性 **-E -A**

配置条件

在配置 BGP 路由属性之前, 首先完成以下任务:

- 启用 BGP 协议;
- 配置 BGP 邻居并使会话建连成功。

配置 BGP 路由权重

BGP 选路第一条规则是比较路由的权重值, 路由权重值越大越优先。路由权重值是设备的本地属性, 不会传递给其它 BGP 邻居。路由权重值取值范围 0~65535, 缺省情况下, 从邻居学习到的路由权重值为 0, 本地设备产生的所有路由权重值都是 32768。

表 44-18 配置 BGP 路由权重

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
配置邻居或对等体组的路由权重	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } weight <i>weight-num</i>	必选 缺省情况下，邻居的路由权重值为 0

配置 BGP 路由 MED 属性

MED 属性用于对进入 AS 的流量选择最佳路由。在其它选路条件相同的情况下，BGP 从不同的 EBGP 邻居学习到具有相同目的地址但下一跳不同的路由时，BGP 将优选 MED 值最小者作为最佳入口。

MED 有时也被称为“外部度量”，并在 BGP 路由表中被标记为“度量 (Metric)”。BGP 会将从邻居学习到路由的 MED 属性通告给 IBGP 邻居，但不会通告给 EBGP 邻居，于是 MED 只适用于相邻 AS 之间。

1、配置 BGP 允许比较来自不同 AS 邻居路由的 MED

缺省情况下，BGP 只会对从同一个 AS 学习到的路由进行 MED 选路，但可以通过 **bgp always-compare-med** 命令来忽略 MED 选路时对相同 AS 要求的限制。

表 44-19 配置 BGP 允许比较来自不同 AS 邻居路由的 MED

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-

步骤	命令	说明
配置 BGP 允行比较来自不同 AS 邻居路由的 MED	bgp always-compare-med	必选 缺省情况下，BGP 只允许比较来自相同 AS 的路由 MED

2、配置 BGP 根据路由 AS_PATH 进行的分组对 MED 排序优选

缺省情况下，没有启用 BGP 根据路由 AS_PATH 进行的分组对 MED 排序优选，可以通过 **bgp deterministic-med** 命令开启该功能。在路由选择的时，将所有的路由都基于 AS_PATH 编排，在每一个 AS_PATH 组内，根据 MED 的大小对路由进行排序，MED 值最小的路由被选为该组的最佳路由。

表 44-20 配置 BGP 根据路由 AS_PATH 进行的分组对 MED 排序优选

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
BGP 根据路由 AS_PATH 进行的分组对 MED 排序优选	bgp deterministic-med	必选 缺省情况下，没有启用 BGP 根据路由 AS_PATH 进行的分组对 MED 排序优选

3、配置比较本地联盟路由的 MED

来自不同 AS 的 EBGp 路由缺省情况下不会比较 MED 属性，该原理同时对联盟的 EBGp 有效，命令 **bgp bestpath med confed** 用于启用对本地联盟的路由比较 MED 属性值。

表 44-21 配置 BGP 比较本地联盟路由的 MED

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
配置 BGP 用对本地联盟的路由比较 MED 属性值	bgp bestpath med confed	必选 缺省情况下，不会对本地联盟的路由比较 MED 属性值

4、配置路由图修改 MED 属性

在路由收发时，可以应用路由图修改 MED 属性值。

表 44-22 配置路由图修改 MED 属性

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
配置路由图修改 MED 属性	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } route-map <i>rtmap-name</i> in out	必选 缺省情况下，不对任何邻居应用路由图

说明：

- 配置路由图修改 MED 属性时，需要通过 **set metric** 命令对 MED 进行修改，请参见策略工具-技术手册-**set metric**。
- 配置 **neighbor attribute-unchanged** 命令后将不能通过路由图改变邻居 MED 属性。

配置 BGP 路由 Local-Preference 属性

Local-Preference 属性只会在 IBGP 邻居之间传递。Local-Preference 用于选择离开 AS 的最佳出口，Local-Preference 最大的路由将会被优选。

Local-Preference 属性取值范围 0~4294967295，数值越大，该路由优先级越高。缺省情况下，所有通告给 IBGP 邻居的路由 Local-Preference 属性为 100，可以通过 **bgp default local-preference** 或者路由图修改 Local-Preference 属性。

1、配置 BGP 修改缺省 Local-Preference 属性

表 44-23 配置 BGP 修改缺省 Local-Preference 属性

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
配置 BGP Local-Preference 属性缺省值	bgp default local-preference <i>local-value</i>	可选 缺省情况下，缺省本地优先级为 100

2、配置路由图修改 Local-Preference 属性

表 44-24 配置路由图修改 Local-Preference 属性

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
配置路由图修改 Local-Preference 属性	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } route-map <i>rtmap-name</i> in out	必选 缺省情况下, 不对任何邻居应用路由图

说明:

- 置路由图修改 Local-Preference 属性时, 需要通过 **set local-preference** 命令对 Local-Preference 属性进行修改, 请参见策略工具-技术手册-**set local-preference**。

配置 BGP 路由 AS_PATH 属性

1、配置 BGP 选路时忽略比较 AS_PATH

在其它条件相同条件下, BGP 选路时将优选 AS_PATH 最短的路由, 但可以通过 **bgp bestpath as-path ignore** 命令取消通过 AS_PATH 选路。

表 44-25 配置 BGP 选路时忽略比较 AS_PATH

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-

步骤	命令	说明
配置 BGP 选路时忽略比较 AS_PATH	bgp bestpath as-path ignore	必选 缺省情况下，选路时对 AS_PATH 属性值进行比较

2、配置 BGP 允许本地 AS 号重复出现次数

为了避免路由环路，BGP 会检查从邻居收到的路由 AS_PATH 属性，将丢弃包含本地 AS 号的路由，但可以通过 **neighbor allowas-in** 命令允许 BGP 接收到的路由 AS_PATH 属性中包含有本地 AS 号，并且可以配置包含本地 AS 号的个数。

表 44-26 配置 BGP 允许本地 AS 号重复出现次数

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
配置允许本地 AS 号重复	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } allowas-in [<i>as-num</i>]	必选 缺省情况下，不允许从邻居接收到的路由 AS_PATH 属性中含有本地 AS 号

3、配置 BGP 向邻居通告路由时移除私有 AS 号

在大型 BGP 网络中，路由 AS_PATH 属性具有联盟或团体属性，缺省情况下，BGP 向邻居通告时将携带这些私有 AS 属性信息，为了屏蔽私网信息，可以通过 **neighbor remove-private-AS** 移除私有 AS 号。

表 44-27 配置 BGP 向邻居通告路由时移除私有 AS 号

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
配置 BGP 向邻居通告路由时移除私有 AS 号	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } remove-private-AS	必选 缺省情况下，向邻居通告时将携带私有 AS 号

4、配置检测 EBGp 路由的第一个 AS 号合法性

BGP 向 EBGp 邻居通告路由时会将本地 AS 号压入到 AS_PATH 的开始位置，第一个通告该路由的 AS 将会处在最末位。通常情况下，从 EBGp 收到的路由第一个 AS 号应该与邻居的 AS 号相同，否则该路由将会被丢弃。

表 44-28 配置检测 EBGp 路由的第一个 AS 号合法性

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
配置检测 EBGp 路由的第一个 AS 号合法性	bgp enforce-first-as	必选 缺省情况下，BGP 未开启这种首 AS 号检查机制

5、配置路由图修改 AS_PATH 属性

BGP 支持配置路由图修改 AS_PATH 属性，可以通过 **set as-path prepend** 对路由属性进行追加，从而影响邻居选路。在使用 **set as-path prepend** 功能时，优先使用本地 AS 追加 AS_PATH，如果使用其它 AS，则必须足够重视，避免路由通告给该 AS 时遭到拒绝。

表 44-29 配置路由图修改 AS_PATH 属性

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
配置路由图修改 AS_PATH 属性	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } route-map <i>rtmap-name</i> in out	必选 缺省情况下，不对任何邻居应用路由图

说明：

- 配置路由图修改 AS_PATH 属性时，需要通过 **set as-path prepend** 命令对 AS_PATH 属性进行修改，请参见策略工具-技术手册-**set as-path**。

配置 BGP 路由 NEXT-HOP 属性

在 BGP 向 IBGP 邻居通告路由时不会改变路由属性（包括下一跳属性）。下一跳属性通常用于 BGP 将 EBGP 邻居学习到的路由通告给 IBGP 邻居时，通过 **neighbor next-hop-self** 命令修改向 BGP 邻居通告路由的下一跳属性采用本地 IP 地址。BGP 同时支持应用路由图修改下一跳属性。

1、配置 BGP 使用本地 IP 地址作为路由下一跳

表 44-30 配置 BGP 使用本地 IP 地址作为路由下一跳

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
配置向邻居通告路由时采用本地 IP 地址作为下一跳	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } next-hop-self	必选 缺省情况下，向 EBGP 邻居通告的路由下一跳属性为本地 IP 地址，向 IBGP 通告的路由下一跳属性将不会被修改，维持原有属性值

说明：

- 配置 BGP 使用本地 IP 地址作为路由下一跳时，如果使用 **neighbor update-source** 配置了 TCP 会话的源地址，则将采用该源地址作为下一跳地址，否则，将选取通告设备的出接口 IP 作为本地 IP 地址。

2、配置路由图修改 NEXT-HOP 属性

BGP 支持配置路由图修改 NEXT-HOP 属性，可以通过 **set ip next-hop** 修改下一跳属性。

表 44-31 配置路由图修改 NEXT-HOP 属性

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-

步骤	命令	说明
配置路由图修改 NEXT-HOP 属性	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } route-map <i>rtmap-name</i> in out	必选 缺省情况下, 不对任何邻居应用路由图

说明:

- 配置路由图修改 NEXT-HOP 属性时, 需要通过 **set ip next-hop** 命令对 NEXT-HOP 属性进行修改, 请参见策略工具-技术手册-**set ip next-hop**。

配置 BGP 路由团体属性

BGP 向邻居通告路由时支持配置发送团体属性, 可以在出入两个方向上对指定邻居应用路由图匹配团体属性。

团体属性用于标识一组路由, 以便对这组路由应用路由策略。团体属性具有标准与扩展两种形式, 标准团体属性 4 字节长, 具有 NO_EXPORT、LOCAL_AS、NO_ADVERTISE、INTERNET 等属性; 扩展团体属性 8 字节长, 具有路由目标 (Route Target, RT)、路由源 (Route Origin) 属性。

1、配置 BGP 向邻居通告路由团体属性

neighbor send-community 支持向邻居通告标准团体属性或扩展团体属性, 或者通告两者。

表 44-32 配置 BGP 向邻居通告路由团体属性

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-

配置向邻居通告路由团体属性	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } send-community [both extended standard]	必选 缺省情况下，不向任何邻居通告团体属性
---------------	--	--------------------------

说明：

- 在 VPNv4 地址簇下激活邻居后，将自动向邻居通告标准与扩展团体属性。

2、配置路由图修改路由团体属性

BGP 支持配置路由图修改路由团体属性，可以通过 **set communtiy** 修改团体属性。

表 44-33 配置路由图修改路由团体属性

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
配置路由图修改 BGP 路由团体属性	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } route-map <i>rtmap-name</i> in out	必选 缺省情况下，不对任何邻居应用路由图

说明：

- 配置路由图修改路由团体属性时，需要通过 **set communtiy** 命令对团体属性进行修

44.2.5 配置 BGP 网络优化

-E -A

配置条件

在配置 BGP 网络优化之前，首先完成以下任务：

- 启用 BGP 协议；
- 配置 BGP 邻居并使会话建连成功。

配置 BGP 邻居保活时间

在 BGP 会话成功建立之后，邻居之间将定时发送保活（Keepalive）消息维持 BGP 会话关系，如果在会话保持时间（Holdtime）内未收到邻居的保活消息或者路由更新报文（Update），BGP 会话就会超时断开。会话保活时间不会大于保持时间的三分之一。

表 44-34 配置 BGP 邻居保活时间

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
配置全局 BGP 保活时间与保持时间	timers bgp <i>keepalive-interval holdtime-interval</i>	可选
配置 BGP 邻居或对等体组的保活时间与保持时间	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } timers { <i>keepalive-interval holdtime-interval</i> connect <i>connect-interval</i> }	缺省情况下，保活定时器时间间隔为 60 秒，保持定时器时间间隔为 180 秒，会话重连定时器时间间隔为 120 秒

说明：

- 对指定邻居配置的保活时间与保持时间优先于全局 BGP 保活时间与保持时间。
- 邻居协商后将采用保持时间的最小者作为 BGP 会话的保持时间。
- 配置保活时间与保持时间同时为零时将取消邻居保活/保持功能。
- 保活时间间隔大于保持时间三分之一时，BGP 会话将采用保持时间的三分之一发送保活报文。

配置 BGP 路由检测时间

BGP 主要完成以 AS 为单位的寻路过程，AS 内部由 IGP 完成寻路，所以 BGP 路由通常依赖于 IGP 路由。在 BGP 依赖的 IGP 路由的下一跳或出接口发生变化后，BGP 通过定时检测 IGP 路由来更新 BGP 路由。在检测周期内同时完成对本地 BGP 路由更新等事务。

表 44-35 配置 BGP 路由检测时间

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
配置 BGP 路由检测时间	bgp scan-time <i>time</i>	可选 缺省情况下，BGP 路由检测时间为 60 秒

说明：

- 配置 BGP 路由检测时间过小将使 BGP 频繁检测路由，影响设备性能。

配置 EBGP 邻居快速断连

在 BGP 会话成功建立之后，邻居之间将相互定时发送保活（Keepalive）消息维持 BGP 会话关系，如果在会话保持时间（Holdtime）内未收到邻居的保活消息或者路由更新报文（Update），BGP 会话就会超时断开。可以通过配置直连 EBGP 邻居在相连接口 down 时，立刻断开 BGP 连接，而不需要等到 BGP 保活超时。取消 EBGP 邻居快速断连时，EBGP 会话将不会响应接口 down 事件，BGP 会话连接通过超时断开。

表 44-36 配置 EBGP 邻居快速断连

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
配置 EBGP 邻居快速断连	bgp fast-external-failover	可选 缺省情况下，已启用 EBGP 响应直连接口下线事件的快速处理能力

配置 BGP 路由抑制功能

网络中频繁震荡的路由会造成网络的不稳定，BGP 通过配置路由衰减抑制这类路由，减少震荡路由对网络的影响。

频繁震荡的路由将会分配增加惩罚值，当惩罚值超过抑制门限后，路由将不会被通告给邻居，惩罚值不能超过最大抑制时间。当路由在半衰期时间内没有发生震荡时，惩罚值将会减半，直到该值少于重用门限后，路由才会被重新通告给邻居。

- 半衰期：路由惩罚值减半的时间。
- 重用门限：路由恢复使用的门限值。
- 抑制门限：路由被抑制的门限值。
- 最大抑制时间：路由被抑制的最长时间。

表 44-37 配置 BGP 路由抑制功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
配置 BGP 路由衰减周期	bgp dampening [<i>reach-half-life</i> [<i>reuse-value suppress-value max-suppress-time</i> [<i>unreach-half-life</i>]] route-map <i>rtmap-name</i>]	必选 缺省情况下，未启用路由抑制功能，启用后的缺省路由抑制半衰期为 15 分钟，路由重用门限为 750，路由抑制门限为 2000，路由最大抑制时间为 60 分钟，路由惩罚的不可达半衰期为 15 分钟

说明：

- 路由震荡不仅有路由的增删，还包括路由属性的变化，如下一跳、MED 属性等。

配置 BGP 邻居刷新能力

当 BGP 邻居应用的路由策略或者选路策略发生变化时，需要重新对路由表进行刷新，一种方式是通过复位 BGP 连接使会话重新开始达到复位目的，这种方式会造成 BGP 路由震荡而影响业务运行。另一种更优雅的方式是配置本端 BGP 设备支持路由刷新能力，在其邻居需要对路由进行复位时，通过向本端通告 Route-Refresh 消息，本端收到 Route-Refresh 消息后会重新将路由发给该邻居，达到了不断开 BGP 会话的情况下就对路由表进行了动态刷新。

表 44-38 配置 BGP 邻居刷新能力

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
配置启用邻居刷新能力	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } capability route-refresh	可选 缺省情况下，已启用向邻居通告支持路由刷新能力

配置 BGP 邻居软重置能力

当 BGP 邻居应用的路由策略或者选路策略发生变化时，需要重新对路由表进行刷新，一种方式是通过复位 BGP 连接使会话重新开始达到复位目的，这种方式会造成 BGP 路由震荡而影响业务运行。另一种更优雅的方式是配置本端 BGP 设备支持路由刷新能力，还有一种方式是通过使能本端 BGP 设备的软重置能力。缺省情况下，BGP 设备保留各个邻居的路由信息，在使能其邻居软重置能力后，再次对本地保留邻居的路由进行刷新，此时不会断开 BGP 会话。

表 44-39 配置 BGP 邻居软重置能力

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
配置使能邻居软重置能力	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } soft-reconfiguration inbound	必选 缺省情况下，未启用邻居软重置功能

配置 BGP 邻居 ORF 能力

BGP 通过丰富的路由属性完成对路由的精确控制，通常在出入两个方向上应用路由策略达到该目的，这种方式是 BGP 本地的行为。BGP 同时也支持 ORF（Outbound Route Filtering，输出路由过滤）能力，通过 Route-refresh 报文将本地入口策略通告给邻居，由邻居向自己通告路由时应用该策略，可以大大减少 BGP 邻居之间路由更新报文的交互。

ORF 能力协商成功需要以下条件：

- 邻居双方都需要启用 ORF 能力；
- ORF send 与 ORF receive 必须配对，即某一方采用 ORF send，另一方必须是 ORF both 或 ORF receive；某一方采用 ORF receive，另一方必须是 ORF send 或 ORF both；
- 采用 ORF send 一方需要配置在入方向上应用前缀列表。

表 44-40 配置 BGP 邻居 ORF 能力

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
配置邻居在入方向上应用前缀列表	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } prefix-list <i>prefix-list-name</i> in	必选 缺省情况下，不对任何 BGP 邻居应用前缀列表
配置邻居支持 ORF 能力	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } capability orf prefix-list { both receive send }	必选 缺省情况下，未开启邻居通告支持 ORF 能力

44.2.6 配置 BGP 大型网络

-E -A**配置条件**

在配置 BGP 大型网络之前，首先完成以下任务：

- 启用 BGP 协议；
- 配置 BGP 邻居并使会话建连成功。

配置 BGP 对等体组

BGP 对等体组是具有相同配置策略的 BGP 邻居集合，任何对对等体组的配置都会同时作用到每个对等体成员，通过配置 BGP 对等体组便于对邻居进行集中管理与维护。

表 44-41 配置 BGP 对等体组

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
创建 BGP 对等体组	neighbor <i>peer-group-name</i> peer-group	必选
配置邻居加入对等体组	neighbor <i>neighbor-address</i> peer-group <i>peer-group-name</i>	缺省情况下，未配置对等体组，且邻居未加入任何对等体组

说明：

- 对等体组的配置将同时作用到所有对等体组成员。

- 邻居加入对等体组后原有邻居与对等体组相同的配置将会被删除。
- 配置对等体组出方向路由策略或入方向上路由策略时，在路由策略变化后，将不能对已加入对等体组的邻居生效，需要重置对等体组后，才能将变化后的路由策略作用到对等体组成员。

配置 BGP 路由反射器

在大型 BGP 组网环境中要求 IBGP 邻居全网连接，即每一个 BGP 与其它所有 IBGP 邻居建立连接关系，这样在 N 个 BGP 邻居的组网环境中 BGP 连接数为 $N*(N-1)/2$ 条，连接数越多，路由通告量越大。BGP 路由反射器是一种减少网络连接数的方法，它将若干个 IBGP 划分为一个群体，并指定某个 BGP 作为反射器 (RR)，其它 BGP 作为客户，非群体中的 BGP 作为非客户。客户只与 RR 建立对等关系，而不与其它 BGP 建立对等关系，从而降低了必要的 IBGP 连接数量，连接数降至 N-1 条。

BGP 路由反射器反射路由原则：

- 从非客户 IBGP 邻居学习到的路由，只反射给客户；
- 从客户学习到的路由，将反射给除发起该路由的客户之外的所有客户以及非客户；
- 从 EBGp 邻居学习到的路由，将反射给所有客户和非客户。

表 44-42 配置 BGP 路由反射器

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
配置反射器簇 ID	bgp cluster-id { <i>cluster-id-in-ip</i> <i>cluster-id-in-num</i> }	必选 缺省情况下，路由反射器簇 ID 使用设备 Router ID 值
配置邻居为反射器客户	neighbor { <i>neighbor-address</i> <i>peer-group-</i>	必选

步骤	命令	说明
	<i>name</i> } route-reflector-client	缺省情况下，未指定任何邻居作为反射器客户
配置 BGP 客户端之间路由反射功能	bgp client-to-client reflection	可选 缺省情况下，已启用 BGP 路由反射器客户端之间路由反射功能

说明：

- 反射器簇 ID 用于标识同一个反射器区域，该反射器区域中可以存在多个反射器，同时，这些反射器具有相同的反射簇 ID。

配置 BGP 联盟

在大型 BGP 组网环境中要求 IBGP 邻居全网连接，即每一个 BGP 与其它所有 IBGP 邻居建立连接关系，这样在 N 个 BGP 邻居的组网环境中 BGP 连接数为 $N*(N-1)/2$ 条，连接数越多，路由通告量越大。BGP 联盟是另外一种减少网络连接数的方法，它采用分而治之策略，将 AS 划分为若干个子 AS 区域，每个 AS 区域形成联盟，各联盟内部通过 IBGP 形成全连接，联盟子 AS 区域之间通过 EBGP 连接，有效减少了 BGP 连接数目。

配置 BGP 联盟时，需要为每一个联盟分配一个联盟 ID，并指定该联盟成员。与路由反射器不同，在路由反射器条件下，只要求路由反射器支持路由反射，而联盟则要求所有成员都要支持联盟功能。

表 44-43 配置 BGP 联盟

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
创建 BGP 联盟 ID	bgp confederation identifier <i>as-number</i>	必选 缺省情况下，未配置联盟自治系统号
配置联盟成员	bgp confederation peers <i>as-number-list</i>	必选 缺省情况下，未配置联盟的子自治系统号

说明：

- 联盟 ID 用于标识联盟子自治系统，联盟成员被划分到该子自治系统中。

44.2.7 配置 BGP GR -E -A

GR (Graceful Restart, 优雅重启) 用于在设备主备切换过程中，保持本设备和邻居设备转发层面路由信息不变，转发不受影响；当切换设备重新运行后，两台设备协议层面同步路由信息并更新转发层，达到设备切换过程中数据转发不间断的目的。

GR 过程角色：

- GR Restarter：进行协议优雅重启的设备；
- GR Helper：协助协议优雅重启的设备；
- GR Time：GR-Restarter 重启的最大时间，GR Helper 只在该时间内维持路由稳定。

双主控设备可以充当 GR Restarter 和 GR Helper，而集中式设备只能充当 GR Helper，协助 Restarter 端完成 GR。在 GR Restarter 进行 GR 时，GR Helper 维持其路由直到 GR Time 超时并协助其完成 GR 后，进行路由信息同步，在此期间，网络路由和报文转发维持 GR 前的状态，有效保证了网络稳定。

BGP GR 关系在邻居建连时通过 OPEN 报文协商建立，在 GR Restarter 邻居重启时，BGP 会话会断开，但是从该邻居学习的路由不会被删除，仍然在 IP 路由表中正常转发，这些路由只在 BGP 路由表中置上 Stale 标记，在 GR 完成或者超时后将会被更新。

GR Restarter 需要在最大允许时间内完成与 GR Helper 的建连，否则 GR Helper 将会消除保持的 GR 路由，解除 GR 过程。在邻居重建完成后，GR Helper 需要接收来自 GR Restarter 且带有 End-Of-RIB 标记的更新报文才能成功完成 GR 过程，否则未被更新的 GR 路由将会在最大保持时间后 (**stalepath-time**) 删除，GR 关系将解除。

配置条件

在配置 BGP GR 之前，首先完成以下任务：

- 启用 BGP 协议；
- 配置 BGP 邻居并使会话建连成功。

配置 BGP GR Restarter

表 44-44 配置 BGP GR Restarter

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
使能 BGP GR 能力	bgp graceful-restart [restart-time <i>time</i> stalepath-time <i>time</i>]	必选 缺省情况下，BGP 设备未启用 GR 能力，启用 GR 后的缺省邻居重建会话的最大允许时间为

步骤	命令	说明
		120 秒, GR 路由最大保持时间为 360 秒
配置向邻居通告 GR-Restarter 能力	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } capability graceful-restart	必选 缺省情况下, 不向邻居通告 GR Restarter 能力

配置 BGP GR Helper

表 44-45 配置 BGP GR Helper

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
使能 BGP GR 能力	bgp graceful-restart [restart-time <i>time</i> stalepath-time <i>time</i>]	必选 缺省情况下, BGP 设备未启用 GR 能力, 启用 GR 后的缺省邻居重建会话的最大允许时间为 120 秒, GR 路由最大保持时间为 360 秒

44.2.8 配置 BGP 与 BFD 联动 **-E -A**

通常在 BGP 邻居之间会运行有其它中间设备, 在这些中间设备出现故障时, BGP 会话在保持时间内仍然正常, 无法及时响应中间设备链路故障。BFD(Bidirectional Forwarding Detection, 双向转发

单播路由

检测)提供一种快速检测两台设备之间线路状态的方法。当 BGP 设备间启动 BFD 检测后,若设备之间线路发生故障,BFD 会快速检测到线路故障,并通知 BGP,触发 BGP 快速断开会话,并切换到备份线路,达到路由快速切换的目的。

配置条件

在配置 BGP 与 BFD 联动之前,首先完成以下任务:

- 启用 BGP 协议;
- 配置 BGP 邻居并使会话建连成功。

配置 EBGP 与 BFD 联动

EBGP 与 BFD 联动基于单跳 BFD 会话,需要在接口模式下配置 BFD 会话参数。

表 44-46 配置 EBGP 与 BFD 联动

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
配置 EBGP 与 BFD 联动	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } fall-over bfd	必选 缺省情况下,未启用邻居 BFD 功能
退出 BGP 配置模式	exit	-
进入接口配置模式	interface <i>interface-name</i>	-
配置 BFD 会话最小接收间隔时间	bfd min-receive-interval <i>milliseconds</i>	可选 缺省情况下,BFD 会话最小接收间隔时间为 1000 秒

步骤	命令	说明
配置 BFD 会话最小发送间隔时间	bfd min-transmit-interval <i>milliseconds</i>	可选 缺省情况下, BFD 会话最小发送间隔时间为 1000 秒
配置 BFD 会话检测超时倍数	bfd multiplier <i>number</i>	可选 缺省情况下, BFD 会话检测超时倍数为 5

说明:

- BFD 相关配置, 请参见可靠性技术-BFD 技术手册与 BFD 配置手册。

44.2.9 BGP 监控与维护

-E -A

表 44-47 BGP 监控与维护

命令	说明
clear ip bgp { * <i>neighbor-address</i> <i>as-number</i> / peer-group <i>peer-group-name</i> external } [vrf <i>vrf-name</i> ipv4 unicast ipv4 multicast vpnvp4 unicast mvpn]	重置 BGP 邻居
clear ip bgp [ipv4 unicast ipv4 multicast] dampening [<i>ip-</i>	清除抑制路由

命令	说明
<i>address</i> <i>ip-address/mask-length</i>]	
clear ip bgp [ipv4 unicast ipv4 multicast] flap-statistics [<i>ip-address</i> <i>ip-address/mask-length</i>]	清除抖动统计信息
clear ip bgp { * <i>neighbor-address</i> <i>as-number</i> / peer-group <i>peer-group-name</i> external } [ipv4 unicast ipv4 multicast vpn4 unicast vrf <i>vrf-name</i> mvpn] { [soft] [in out] }	软重置邻居
clear ip bgp { * <i>neighbor-address</i> } in { ecomm prefix-filter }	通告 ORF 给邻居
show ip bgp [vpn4 { all vrf <i>vrf-name</i> rd <i>route-distinguisher</i> }] [<i>ip-address</i> <i>ip-address/mask-length</i>]	显示 BGP 相应地址簇下的路由信息
show ip bgp attribute-info	显示 BGP 公共的路由属性信息
show ip bgp cidr-only	显示 BGP 所有有类网络路由
show ip bgp community [<i>community-number</i> / <i>aa:nn</i> / exact-match / local-AS / no-advertise / no-export]	显示匹配指定团体属性的路由信息

命令	说明
show ip bgp community-info	显示所有 BGP 的团体属性信息
show ip bgp community-list <i>community-list-name</i>	显示路由信息应用的团体属性列表
show ip bgp [vpnv4 { all vrf <i>vrf-name</i> rd route- <i>distinguisher</i> }] dampening { dampened-paths flap- statistics parameters }	显示路由衰减的详细信息
show ip bgp filter-list <i>filter-list-</i> <i>name</i> [exact-match]	显示 AS_PATH 访问列表匹配的路由
show ip bgp inconsistent-a	显示 AS_PATH 冲突的路由
show ip bgp ipv4 vpn-target [vpn-rt]	显示 BGP 的 VPN-TARGET 路由表
show ip bgp ipv4 vpn-target rt- filter [neighbor ip-address]	显示 BGP 邻居的 RT 过滤表
show ip bgp mvpn { all vrf <i>vrf-</i> <i>name</i> rd route-distinguisher } { all-type type { 1 [ip-address] 7[as:source-ip-address:group-ip- address] } }	显示 BGP MVPN 地址簇下的路由信息
show ip bgp mvpn { all vrf <i>vrf-</i> <i>name</i> rd route-distinguisher } { neighbors ip-address } { advertised-routes received-	显示 BGP MVPN 地址簇下指定邻居的路由信息

命令	说明
routes routes { all-type type { 1 [<i>ip-address</i>] 7 [<i>as:source-ip-address:group-ip-address</i>] } }	
show ip bgp mvpn { all vrf <i>vrf-name</i> rd <i>route-distinguisher</i> / neighbors <i>ip-address</i> } { all-type type { 1 7 } } { statistics }	显示 BGP MVPN 地址簇下的路由统计信息
show ip bgp [vpn4 { all vrf <i>vrf_name</i> rd <i>route-distinguisher</i> }] neighbors [<i>ip-address</i>]	显示 BGP 的邻居详细信息
show ip bgp orf ecomm	显示所有 BGP 邻居的 ORF 信息
show ip bgp paths	显示 BGP 路由 AS_PATH 信息
show ip bgp prefix-list <i>prefix-list-name</i>	显示前缀列表匹配的路由
show ip bgp quote-regexp <i>as-path-list-name</i>	显示 AS_PATH 列表匹配的路由
show ip bgp regexp <i>as-path-list-name</i>	显示 AS_PATH 列表匹配的路由
show ip bgp route-map <i>rtmap-name</i>	显示路由图匹配的对路由
show ip bgp scan	显示 BGP 的扫描信息

命令	说明
show ip bgp [vpn4 { all vrf <i>vrf-name</i> rd <i>route-distinguisher</i> } mvpn] summary	显示 BGP 的邻居汇总信息

44.2.10 BGP 监控与维护

-E -A

表 44-48 BGP 监控与维护

命令	说明
clear ip bgp { * [vrf <i>vrf-name</i>] <i>neighbor-address</i> [vrf <i>vrf-name</i>] <i>as-number</i> / peer-group <i>peer-group-name</i> external }	重置 BGP 邻居
clear ip bgp [ipv4 unicast ipv4 multicast] dampening [<i>ip-address</i> <i>ip-address/mask-length</i>]	清除抑制路由
clear ip bgp [ipv4 unicast ipv4 multicast] flap-statistics [<i>ip-address</i> <i>ip-address/mask-length</i>]	清除抖动统计信息
clear ip bgp { * <i>neighbor-address</i> <i>as-number</i> / peer-group <i>peer-group-name</i> external } [ipv4 unicast ipv4 multicast	软重置邻居

命令	说明
vpn4 unicast vrf <i>vrf-name</i>] { [soft] [in out] }	
clear ip bgp { * <i>neighbor-address</i> } in { ecomm prefix-filter }	通告 ORF 给邻居
show ip bgp [vpn4 { all vrf <i>vrf-name</i> rd <i>route-distinguisher</i> }] [<i>ip-address</i> <i>ip-address/mask-length</i>]	显示 BGP 相应地址簇下的路由信息
show ip bgp attribute-info	显示 BGP 公共的路由属性信息
show ip bgp cidr-only	显示 BGP 所有有类网络路由
show ip bgp community [<i>community-number / aa:nn / exact-match / local-AS / no-advertise / no-export</i>]	显示匹配指定团体属性的路由信息
show ip bgp community-info	显示所有 BGP 的团体属性信息
show ip bgp community-list <i>community-list-name</i>	显示路由信息应用的团体属性列表
show ip bgp [vpn4 { all vrf <i>vrf-name</i> rd <i>route-distinguisher</i> }] dampening { dampened-paths flap-statistics parameters }	显示路由衰减的详细信息

命令	说明
show ip bgp filter-list <i>filter-list-name</i> [exact-match]	显示 AS_PATH 访问列表匹配的路由
show ip bgp inconsistent-as	显示 AS_PATH 冲突的路由
show ip bgp [vpn4 all] neighbors [<i>ip-address</i>]	显示 BGP 的邻居详细信息
show ip bgp orf ecomm	显示所有 BGP 邻居的 ORF 信息
show ip bgp paths	显示 BGP 路由 AS_PATH 信息
show ip bgp prefix-list <i>prefix-list-name</i>	显示前缀列表匹配的路由
show ip bgp quote-regexp <i>as-path-list-name</i>	显示 AS_PATH 列表匹配的路由
show ip bgp regexp <i>as-path-list-name</i>	显示 AS_PATH 列表匹配的路由
show ip bgp route-map <i>rtmap-name</i>	显示路由图匹配的对路由
show ip bgp scan	显示 BGP 的扫描信息
show ip bgp [vpn4 { all vrf <i>vrf-name</i> rd <i>route-distinguisher</i> } vxlan] summary	显示 BGP 的邻居汇总信息
show ip bgp vxlan local-remote [<i>ip-address</i> neighbor <i>ip-address</i>]	显示 BGP 向邻居通告的本地 Session 信息

命令	说明
<code>show ip bgp vxlan session [ip-address active]</code>	显示 BGP 学习到的 Session 信息

44.3 BGP 典型配置举例

44.3.1 配置 BGP 基本功能 -E -A

网络需求

- Device1 和 Device2 间建立 EBGP 邻居，Device2 和 Device3 间建立 IBGP 邻居。
- Device1 学习到 Device3 的接口直连路由 200.0.0.0/24，Device3 学习到 Device1 的接口直连路由 100.0.0.0/24。

网络拓扑

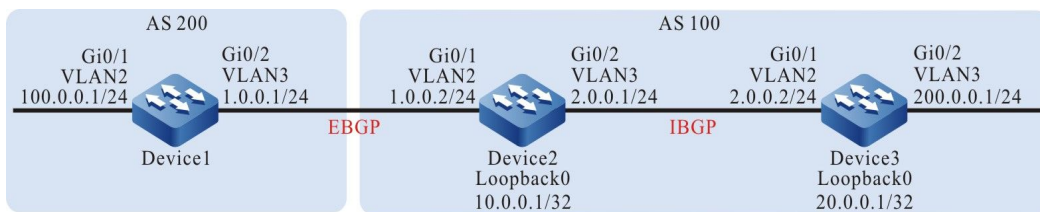


图 44-1 配置 BGP 基本功能组网图

配置步骤

- 步骤 1: 配置 VLAN，并将端口加入对应的 VLAN。（略）
- 步骤 2: 配置各接口的 IP 地址。（略）
- 步骤 3: 配置 OSPF，使设备间 Loopback 路由互相可达。

#配置 Device2。

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 10.0.0.1 0.0.0.0 area 0
```

单播路由

```
Device2(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#配置 Device3。

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 20.0.0.1 0.0.0.0 area 0
Device3(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#exit
```

#查看 Device2 的路由表。

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

O 20.0.0.1/32 [110/2] via 2.0.0.2, 00:27:09, vlan3
```

#查看 Device3 的路由表。

```
Device3#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

O 10.0.0.1/32 [110/2] via 2.0.0.1, 00:28:13, vlan2
```

可以看到 Device2 和 Device3 通过运行 OSPF 协议均学习到了对端环回口的路由，为下一步 Device2 和 Device3 通过环回口建立 IBGP 邻居做准备。

步骤 4： 配置 BGP。

#配置 Device1。

配置与 Device2 建立直连 EBGP 对等体，通过 network 的方式将 100.0.0.0/24 引入到 BGP 中。

```
Device1#configure terminal
Device1(config)#router bgp 200
Device1(config-bgp)#neighbor 1.0.0.2 remote-as 100
Device1(config-bgp)#network 100.0.0.0 255.255.255.0
Device1(config-bgp)#exit
```

#配置 Device2。

通过 Loopback0 与 Device3 建立非直连 IBGP 对等体关系，同时将通告路由的下一跳设置为自身，配置与 Device1 建立直连 EBGP 对等体。

```
Device2(config)#router bgp 100
Device2(config-bgp)#neighbor 20.0.0.1 remote-as 100
Device2(config-bgp)#neighbor 20.0.0.1 update-source loopback0
Device2(config-bgp)#neighbor 1.0.0.1 remote-as 200
Device2(config-bgp)#neighbor 20.0.0.1 next-hop-self
Device2(config-bgp)#exit
```

单播路由

#配置 Device3。

通过 Loopback0 与 Device2 建立非直连 IBGP 对等体关系，通过 network 的方式将 200.0.0.0/24 引入到 BGP 中。

```
Device3(config)#router bgp 100
Device3(config-bgp)#neighbor 10.0.0.1 remote-as 100
Device3(config-bgp)#neighbor 10.0.0.1 update-source loopback0
Device3(config-bgp)#network 200.0.0.0 255.255.255.0
Device3(config-bgp)#exit
```

说明：

- 为了防止路由动荡，所以 IBGP 邻居均是通过环回口建立，需要 OSPF 在 IBGP 邻居间同步环回口的路由信息。
-

步骤 5： 检验结果。

#查看 Device2 上 BGP 邻居状态。

```
Device2#show ip bgp summary
BGP router identifier 10.0.0.1, local AS number 100
BGP table version is 2
2 BGP AS-PATH entries
0 BGP community entries

Neighbor    V  AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
1.0.0.1     4 200    3    3     1  0  0 00:00:29 1
200.0.0.1  4 100    5    4     2  0  0 00:02:13 1
```

从 State/PfxRcd 这列的内容显示为数字（从邻居接收路由前缀的数目）可以看出 Device2 与 Device1、Device3 成功建立 BGP 邻居

#查看 Device1 的路由表。

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

B 200.0.0.0/24 [20/0] via 1.0.0.2, 00:15:52, vlan3
```

#查看 Device2 的路由表。

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set
```

```
B 100.0.0.0/24 [20/0] via 1.0.0.1, 00:14:11, vlan2
B 200.0.0.0/24 [200/0] via 20.0.0.1, 00:17:12, vlan3
```

#查看 Device3 的路由表。

```
Device3#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

B 100.0.0.0/24 [200/0] via 10.0.0.1, 00:14:50, vlan2
```

可以看到 Device1 学习到了 Device3 的接口直连路由 200.0.0.0/24，Device3 学习到 Device1 的接口直连路由 100.0.0.0/24。

44.3.2 配置 BGP 路由重分发 **-E -A**

网络需求

- Device3 与 Device2 间建立 OSPF 邻居，并向 Device2 通告接口直连路由 200.0.0.0/24。
- Device1 和 Device2 间建立 EBGP 邻居，Device2 将学习到的 OSPF 路由重分发到 BGP 中并通告给 Device1。

网络拓扑

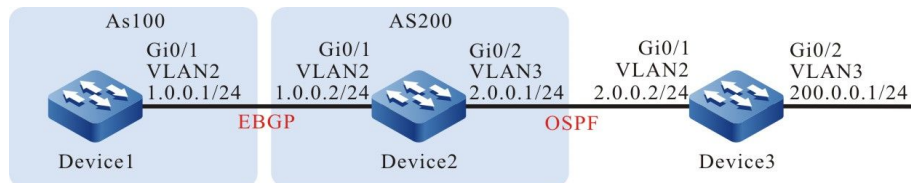


图 44-2 配置 BGP 路由重分发组网图

配置步骤

- 步骤 1：配置 VLAN，并将端口加入对应的 VLAN。（略）
- 步骤 2：配置各接口的 IP 地址。（略）
- 步骤 3：配置 OSPF，使设备间 Loopback 路由互相可达。

#配置 Device2。

```
Device2#configure terminal
```

单播路由

```
Device2(config)#router ospf 100
Device2(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#配置 Device3。

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 200.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#exit
```

#查看 Device2 的路由表。

```
Device2#show ip route ospf
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

O   200.0.0.0/24 [110/2] via 2.0.0.2, 00:01:45, vlan3
```

从路由表中可以看出 Device2 学习到了 Device3 通告的 OSPF 路由 200.0.0.0/24。

步骤 4： 配置 BGP。

#配置 Device1。

```
Device1#configure terminal
Device1(config)#router bgp 200
Device1(config-bgp)#neighbor 1.0.0.2 remote-as 100
Device1(config-bgp)#exit
```

#配置 Device2。

```
Device2(config)#router bgp 100
Device2(config-bgp)#neighbor 1.0.0.1 remote-as 200
Device2(config-bgp)#exit
```

#查看 Device2 上 BGP 邻居状态。

```
Device2#show ip bgp summary
BGP router identifier 2.0.0.1, local AS number 100
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor    V  AS MsgRcvd MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
1.0.0.1    4  200    2     2     2     0  00:00:42    0
```

可以看出 Device2 与 Device1 成功建立 BGP 邻居。

步骤 5： 配置 BGP 重分发 OSPF 路由。

#配置 Device2。

```
Device2(config)#router bgp 100
Device2(config-bgp)#redistribute ospf 100
Device2(config-bgp)#exit
```


步骤 6: 检验结果。

#查看 Device2 的 BGP 路由表。

```
Device2#show ip bgp
BGP table version is 6, local router ID is 2.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
                S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop        Metric LocPrf Weight Path
[O]*> 2.0.0.0/24   0.0.0.0          1     32768 ?
[O]*> 200.0.0.0/24 2.0.0.2          2     32768 ?
```

可以看到 OSPF 路由已经被成功重分发到 BGP 中。

#查看 Device1 的路由表。

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE - OSPF External, M - Management
        D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i - ISIS

Gateway of last resort is not set

B 2.0.0.0/24 [20/1] via 1.0.0.2, 00:06:14, vlan2
B 200.0.0.0/24 [20/2] via 1.0.0.2, 00:06:14, vlan2
```

可以看到 Device1 成功学习到路由 2.0.0.0/24 和 200.0.0.0/24。

说明:

- 在实际应用中，如果自治系统边界路由器有 2 台及以上，建议不要直接在不同路由协议之间相互重分发路由，若必须配置时，需要在自治系统边界路由器上配置过滤、汇总等路由控制策略，防止产生路由环路。
-

44.3.3 配置 BGP 团体属性

-E -A

网络需求

- Device1 与 Device2 间建立 EBGP 邻居。
- Device1 通过 network 的方式将两条直连路由 100.0.0.0/24 和 200.0.0.0/24 引入到 BGP 中，通告给 Device2 时分别对两条路由设置不同的团体属性。

- Device2 接收 Device1 通告的路由时，在邻居入方向通过匹配团体属性，过滤路由 100.0.0.0/24，而允许路由 200.0.0.0/24。

网络拓扑

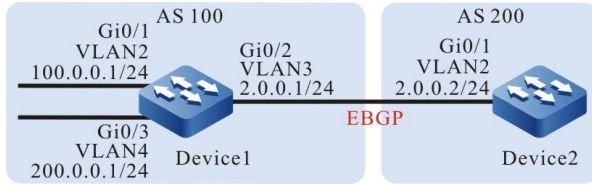


图 44-3 配置 BGP 团体属性组网图

配置步骤

步骤 1： 配置 VLAN，并将端口加入对应的 VLAN。（略）

步骤 2： 配置各接口的 IP 地址。（略）

步骤 3： 配置 BGP。

#配置 Device1。

```
Device1#configure terminal
Device1(config)#router bgp 100
Device1(config-bgp)#neighbor 2.0.0.2 remote-as 200
Device1(config-bgp)#network 100.0.0.0 255.255.255.0
Device1(config-bgp)#network 200.0.0.0 255.255.255.0
Device1(config-bgp)#exit
```

#配置 Device2。

```
Device2#configure terminal
Device2(config)#router bgp 200
Device2(config-bgp)#neighbor 2.0.0.1 remote-as 100
Device2(config-bgp)#exit
```

#查看 Device1 上 BGP 邻居状态。

```
Device1#show ip bgp summary
BGP router identifier 200.0.0.1, local AS number 100
BGP table version is 1
1 BGP AS-PATH entries
0 BGP community entries

Neighbor    V  AS MsgRcvd MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
2.0.0.2    4  200    2    3    1    0  00:00:04  0
```

可以看出 Device1 与 Device2 成功建立 BGP 邻居。

#查看 Device2 上的路由表。

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
```

```
D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS
```

```
Gateway of last resort is not set
```

```
B 100.0.0.0/24 [20/0] via 2.0.0.1, 00:07:47, vlan2
B 200.0.0.0/24 [20/0] via 2.0.0.1, 00:07:47, vlan2
```

可以看到 Device2 成功学习到路由 100.0.0.0/24 和 200.0.0.0/24。

步骤 4: 配置访问列表和路由策略, 设置 BGP 团体属性。

#配置 Device1。

```
Device1(config)#ip access-list standard 1
Device1(config-std-nacl)#permit 100.0.0.0 0.0.0.255
Device1(config-std-nacl)#exit
Device1(config)#ip access-list standard 2
Device1(config-std-nacl)#permit 200.0.0.0 0.0.0.255
Device1(config-std-nacl)#exit
Device1(config)#route-map CommunitySet 10
Device1(config-route-map)#match ip address 1
Device1(config-route-map)#set community 100:1
Device1(config-route-map)#exit
Device1(config)#route-map CommunitySet 20
Device1(config-route-map)#match ip address 2
Device1(config-route-map)#set community 100:2
Device1(config-route-map)#exit
```

通过配置访问列表和路由策略的方式对路由 100.0.0.0/24 和 200.0.0.0/24 分别设置不同的团体属性。

步骤 5: 配置 BGP 关联路由策略。

#配置 Device1。

```
Device1(config)#router bgp 100
Device1(config-bgp)#neighbor 2.0.0.2 route-map CommunitySet out
Device1(config-bgp)#neighbor 2.0.0.2 send-community
Device1(config-bgp)#exit
```

#查看 Device2 的 BGP 路由表。

```
Device2#show ip bgp 100.0.0.0
BGP routing table entry for 100.0.0.0/24
Paths: (1 available, best #1, table Default-IP-Routing-Table)
Not advertised to any peer
100
  2.0.0.1 (metric 10) from 2.0.0.1 (10.0.0.1)

  Origin IGP, metric 0, localpref 100, valid, external, best
  Community: 100:1
  Last update: 00:01:06 ago

Device2#show ip bgp 200.0.0.0
BGP routing table entry for 200.0.0.0/24
Paths: (1 available, best #1, table Default-IP-Routing-Table)
Not advertised to any peer
100
  2.0.0.1 (metric 10) from 2.0.0.1 (10.0.0.1)
```

```
Origin IGP, metric 0, localpref 100, valid, external, best
Community: 100:2
Last update: 00:01:10 ago
```

从 Device2 的 BGP 路由表中看出路由 100.0.0.0/24 的团体属性被设置为 100: 1, 200.0.0.0/24 的团体属性被设置为 100: 2。

步骤 6: 配置 BGP 路由过滤。

#配置 Device2。

```
Device2(config)#ip community-list 1 permit 100:2
Device2(config)#route-map communityfilter
Device2(config-route-map)#match community 1
Device2(config-route-map)#exit
Device2(config)#router bgp 200
Device2(config-bgp)#neighbor 2.0.0.1 route-map communityfilter in
Device2(config-bgp)#exit
```

步骤 7: 检验结果。

#查看 Device2 的路由表。

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

B 200.0.0.0/24 [20/0] via 2.0.0.1, 00:00:53, vlan2
```

从 Device2 的 BGP 路由表中看出路由 100.0.0.0/24 在入方向被过滤，而路由 200.0.0.0/24 被允许。

说明：

- 在对等体上配置了路由策略后需要重置 BGP 进程才能生效。
 - 需要配置 send-community 命令才能将团体属性通告给对等体。
-

44.3.4 配置 BGP 路由反射器

-E -A

网络需求

- Device3 和 Device4 间建立 EBGP 邻居，Device4 向 Device3 通告路由 100.0.0.0/24。
- Device2 分别和 Device3、Device1 间建立 IBGP 邻居，在 Device2 上配置路由反射器，Device1 和 Device3 为客户端，使得 Device1 能学习到 Device4 通告的路由 100.0.0.0/24。

网络拓扑

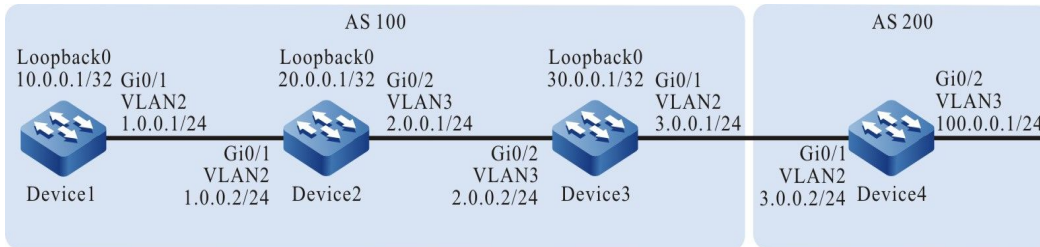


图 44-4 配置 BGP 路由反射器组网图

配置步骤

步骤 1： 配置 VLAN，并将端口加入对应的 VLAN。（略）

步骤 2： 配置各接口的 IP 地址。（略）

步骤 3： 配置 OSPF，使设备间 Loopback 路由互相可达。

#配置 Device1。

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 1.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 10.0.0.1 0.0.0.0 area 0
Device1(config-ospf)#exit
```

#配置 Device2。

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 1.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 20.0.0.1 0.0.0.0 area 0
Device2(config-ospf)#exit
```

#配置 Device3。

```
Device2#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 30.0.0.1 0.0.0.0 area 0
Device3(config-ospf)#exit
```

单播路由

#查看 Device1 的路由表。

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

O 2.0.0.0/24 [110/2] via 1.0.0.2, 01:12:00, vlan2
O 20.0.0.1/32 [110/2] via 1.0.0.2, 01:11:47, vlan2
O 30.0.0.1/32 [110/3] via 1.0.0.2, 01:07:47, vlan2
```

#查看 Device2 的路由表。

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

O 10.0.0.1/32 [110/2] via 1.0.0.1, 01:13:02, vlan2
O 30.0.0.1/32 [110/2] via 2.0.0.2, 01:08:58, vlan3
```

#查看 Device3 的路由表。

```
Device3#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

O 1.0.0.0/24 [110/2] via 2.0.0.1, 01:10:04, vlan2
O 10.0.0.1/32 [110/3] via 2.0.0.1, 01:10:04, vlan2
O 20.0.0.1/32 [110/2] via 2.0.0.1, 01:10:04, vlan2
```

可以看出 Device1、Device2、Device3 互相学习到对方环回口的路由。

步骤 4: 配置 BGP。

#配置 Device1。

```
Device1(config)#router bgp 100
Device1(config-bgp)#neighbor 20.0.0.1 remote-as 100
Device1(config-bgp)#neighbor 20.0.0.1 update-source loopback0
Device1(config-bgp)#exit
```

#配置 Device2。

```
Device2(config)#router bgp 100
Device2(config-bgp)#neighbor 30.0.0.1 remote-as 100
Device2(config-bgp)#neighbor 30.0.0.1 update-source loopback0
Device2(config-bgp)#neighbor 10.0.0.1 remote-as 100
Device2(config-bgp)#neighbor 10.0.0.1 update-source loopback0
Device2(config-bgp)#exit
```

#配置 Device3。

```
Device3(config)#router bgp 100
Device3(config-bgp)#neighbor 3.0.0.2 remote-as 200
Device3(config-bgp)#neighbor 20.0.0.1 remote-as 100
Device3(config-bgp)#neighbor 20.0.0.1 update-source loopback0
Device3(config-bgp)#neighbor 20.0.0.1 next-hop-self
```

```
Device3(config-bgp)#exit
```

#配置 Device4。

```
Device4#configure terminal
Device4(config)#router bgp 200
Device4(config-bgp)#neighbor 3.0.0.1 remote-as 100
Device4(config-bgp)#network 100.0.0.0 255.255.255.0
Device4(config-bgp)#exit
```

#查看 Device2 上 BGP 邻居状态。

```
Device2#show ip bgp summary
BGP router identifier 20.0.0.1, local AS number 100
BGP table version is 1
2 BGP AS-PATH entries
0 BGP community entries

Neighbor    V  AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
10.0.0.1    4 100    8     8    1  0  0 00:03:01  0
30.0.0.1    4 100    9     9    1  0  0 00:02:41  1
```

#查看 Device4 上 BGP 邻居状态。

```
Device4#show ip bgp summary
BGP router identifier 100.0.0.1, local AS number 200
BGP table version is 1
1 BGP AS-PATH entries
0 BGP community entries

Neighbor    V  AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
3.0.0.1     4 100   19    19    1  0  0 00:05:40  0
```

可以看出各设备间 BGP 邻居建立成功。

#查看 Device3 的 BGP 路由表。

```
Device3#show ip bgp
BGP table version is 2, local router ID is 30.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
              Network        Next Hop        Metric LocPrf Weight Path
[B]*> 100.0.0.0/24      3.0.0.2          0         0 200 i
```

#查看 Device2 的 BGP 路由表。

```
Device2#show ip bgp
BGP table version is 768, local router ID is 20.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
              Network        Next Hop        Metric LocPrf Weight Path
[B]*> 100.0.0.0/24      30.0.0.1        0      100  0 200 i
```

#查看 Device1 的 BGP 路由表。

```
Device1#show ip bgp
BGP table version is 2, local router ID is 10.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
              Network        Next Hop        Metric LocPrf Weight Path
```

单播路由

从上面结果可以看出 Device2 和 Device3 均学到路由 100.0.0.0/24，而 Device2 未将该路由通告给 Device1。

步骤 5： 配置 BGP 路由反射器。

#配置 Device2。

```
Device2(config)#router bgp 100
Device2(config-bgp)#neighbor 10.0.0.1 route-reflector-client
Device2(config-bgp)#neighbor 30.0.0.1 route-reflector-client
Device2(config-bgp)#exit
```

在 Device2 上将 Device1 和 Device3 配置为路由反射器的客户端。

步骤 6： 检验结果。

#查看 Device1 的路由表。

```
Device1#show ip bgp
BGP table version is 2, local router ID is 10.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop        Metric LocPrf Weight Path
[B]*>i100.0.0.0/24  30.0.0.1         0  100   0 200 i

Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

B 100.0.0.0/24 [200/0] via 30.0.0.1, 00:01:40, vlan2
```

在 Device2 的 BGP 中将 Device1 与 Device3 配置为路由反射器的客户端，Device2 将路由 100.0.0.0/24 成功地反射给客户端 Device1。

说明：

- 将某个对等体配置为路由反射器的客户端时，设备和该对等体的邻居会重置。
-

44.3.5 配置 BGP 路由聚合

-E -A

网络需求

- Device1 与 Device3 建立 OSPF 邻居，Device3 向 Device1 通告两条路由 100.1.0.0/24 和 100.2.0.0/24。
- Device1 与 Device2 建立 EBGP 邻居。
- 在 Device1 上将 100.1.0.0/24 和 100.2.0.0/24 聚合成路由 100.0.0.0/14 通告给 Device2。

网络拓扑

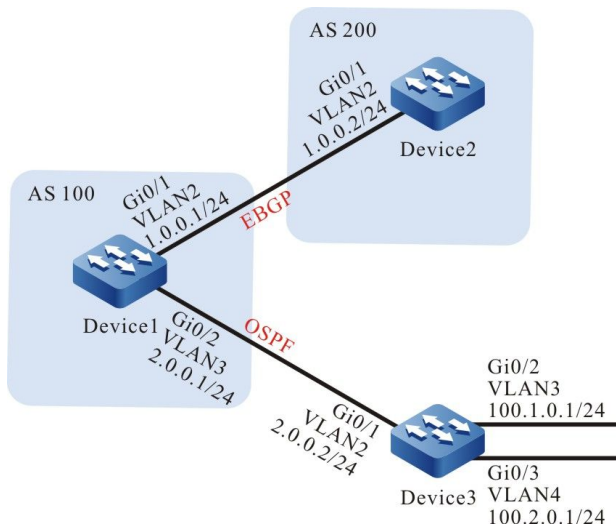


图 44-5 配置 BGP 路由聚合组网图

配置步骤

- 步骤 1：配置 VLAN，并将端口加入对应的 VLAN。（略）
- 步骤 2：配置各接口的 IP 地址。（略）
- 步骤 3：配置 OSPF，使设备间 Loopback 路由互相可达。

#配置 Device1。

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#配置 Device3。

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 100.1.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 100.2.0.0 0.0.0.255 area 0
```

单播路由

```
Device3(config-ospf)#exit
```

#查看 Device1 的路由表。

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNRP, B - BGP, i-ISIS

Gateway of last resort is not set

O 100.1.0.0/24 [110/2] via 2.0.0.2, 00:00:24, vlan3
O 100.2.0.0/24 [110/2] via 2.0.0.2, 00:00:24, vlan3
```

可以看到 Device1 学到 Device3 发布两条路由 100.1.0.0/24 和 100.2.0.0/24。

步骤 4: 配置 BGP。

#配置 Device1。

```
Device1(config)#router bgp 100
Device1(config-bgp)#neighbor 1.0.0.2 remote-as 200
Device1(config-bgp)#exit
```

#配置 Device2。

```
Device2#configure terminal
Device2(config)#router bgp 200
Device2(config-bgp)#neighbor 1.0.0.1 remote-as 100
Device2(config-bgp)#exit
```

#查看 Device1 上 BGP 邻居状态。

```
Device1#show ip bgp summary
BGP router identifier 1.0.0.1, local AS number 100
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor    V  AS MsgRcvd MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
1.0.0.2     4  200    2     2     2    0   00:00:42    0
```

Device1 与 Device2 成功建立 BGP 邻居。

步骤 5: 配置 BGP 路由聚合。

这里有两种方案可以完成网络需求：

方案一：通过配置指向 null0 的聚合静态路由并将其引入 BGP。

#配置 Device1。

```
Device1(config)#ip route 100.0.0.0 255.252.0.0 null0
Device1(config)#router bgp 100
Device1(config-bgp)#network 100.0.0.0 255.252.0.0
Device1(config-bgp)#exit
```

检验结果

单播路由

#查看 Device1 的 BGP 路由表。

```
Device1#show ip bgp
BGP table version is 2, local router ID is 10.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop          Metric LocPrf Weight Path
[B]*> 100.0.0.0/14  0.0.0.0              32768 i
```

可以看出 Device1 的 BGP 路由表中已经生成聚合路由 100.0.0.0/14。

#查看 Device2 的路由表。

```
Device2#show ip bgp
BGP table version is 3, local router ID is 20.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop          Metric LocPrf Weight Path
[B]*> 100.0.0.0/14  1.0.0.1              0      0 100 i

Device2#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

B 100.0.0.0/14 [20/0] via 1.0.0.1, 01:39:30, vlan2
```

可以看出 Device2 成功学习到 Device1 通告的聚合路由 100.0.0.0/14。

方案二：先将明细路由引入 BGP 再通过 **aggregate-address** 命令进行路由聚合。

#配置 Device1。

```
Device1(config)#router bgp 100
Device1(config-bgp)#redistribute ospf 100
Device1(config-bgp)#aggregate-address 100.0.0.0 255.252.0.0 summary-only
Device1(config-bgp)#exit
```

检验结果。

#查看 Device1 的 BGP 路由表。

```
Device1#show ip bgp
BGP table version is 2, local router ID is 10.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop          Metric LocPrf Weight Path
[B]*> 100.0.0.0/14  0.0.0.0              32768 i
[B]s> 100.1.0.0/24  2.0.0.2               2      32768 i
[B]s> 100.2.0.0/24  2.0.0.2               2      32768 i
```

可以看出 Device1 的 BGP 路由表中已经生成聚合路由 100.0.0.0/14。

#查看 Device2 的路由表。

单播路由

```
Device2#show ip bgp
BGP table version is 3, local router ID is 20.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
              Network        Next Hop          Metric LocPrf Weight Path
[B]*> 100.0.0.0/14      1.0.0.1           0         0 100 i

Device2#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

B 100.0.0.0/14 [20/0] via 1.0.0.1, 01:39:30, vlan2
```

可以看出 Device2 成功学习到 Device1 通告的聚合路由 100.0.0.0/14。

说明：

- 使用 aggregate-address 命令进行路由聚合的时候，若配置扩展命令 summary-only，设备将只通告聚合路由，否则将同时通告明细路由和聚合路由。
-

44.3.6 配置 BGP 路由优选

-E -A

网络需求

- Device1 分别与 Device2、Device3 建立 IBGP 邻居，Device4 分别与 Device2、Device3 建立 EBGP 邻居。
- Device1 向 Device4 通告两条路由分别是 55.0.0.0/24、65.0.0.0/24，Device4 向 Device1 通告两条路由分别是 75.0.0.0/24、85.0.0.0/24。
- 通过在 Device2 和 Device3 上修改路由的 Local-preference 属性，使得 Device1 优选 Device2 通告的路由 75.0.0.0/24 以及 Device3 通告的路由 85.0.0.0/24。
- 通过在 Device2 和 Device3 上修改路由的 MED 属性，使得 Device4 优选 Device2 通告的路由 55.0.0.0/24 以及 Device3 通告的路由 65.0.0.0/24。

网络拓扑

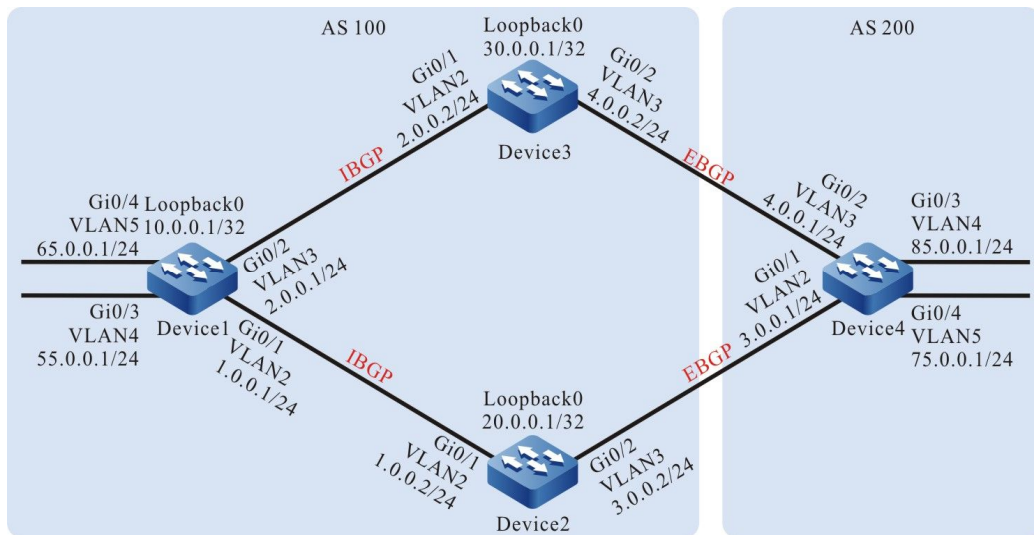


图 44-6 配置 BGP 路由优选组网图

配置步骤

- 步骤 1: 配置 VLAN，并将端口加入对应的 VLAN。（略）
- 步骤 2: 配置各接口的 IP 地址。（略）
- 步骤 3: 配置 OSPF，使设备间 Loopback 路由互相可达。

#配置 Device1。

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 1.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 10.0.0.1 0.0.0.0 area 0
Device1(config-ospf)#exit
```

#配置 Device2。

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 1.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 20.0.0.1 0.0.0.0 area 0
Device2(config-ospf)#exit
```

#配置 Device3。

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 30.0.0.1 0.0.0.0 area 0
Device3(config-ospf)#exit
```

#查看 Device1 的路由表。

单播路由

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

O 20.0.0.1/32 [110/2] via 1.0.0.2, 00:03:15, vlan2
O 30.0.0.1/32 [110/2] via 2.0.0.2, 00:01:40, vlan3
```

#查看 Device2 的路由表。

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

O 2.0.0.0/24 [110/2] via 1.0.0.1, 00:03:54, vlan2
O 10.0.0.1/32 [110/2] via 1.0.0.1, 00:03:54, vlan2
O 30.0.0.1/32 [110/3] via 1.0.0.1, 00:02:14, vlan2
```

#查看 Device3 的路由表。

```
Device3#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

O 1.0.0.0/24 [110/2] via 2.0.0.1, 00:02:35, vlan2
O 10.0.0.1/32 [110/2] via 2.0.0.1, 00:02:35, vlan2
O 20.0.0.1/32 [110/3] via 2.0.0.1, 00:02:35, vlan2
```

可以看出 Device1、Device2、Device3 互相学习到对方环回口的路由。

步骤 4: 配置 BGP。

#配置 Device1。

```
Device1(config)#router bgp 100
Device1(config-bgp)#neighbor 20.0.0.1 remote-as 100
Device1(config-bgp)#neighbor 20.0.0.1 update-source loopback0
Device1(config-bgp)#neighbor 30.0.0.1 remote-as 100
Device1(config-bgp)#neighbor 30.0.0.1 update-source loopback0
Device1(config-bgp)#network 55.0.0.0 255.255.255.0
Device1(config-bgp)#network 65.0.0.0 255.255.255.0
Device1(config-bgp)#exit
```

#配置 Device2。

```
Device2(config)#router bgp 100
Device2(config-bgp)#neighbor 10.0.0.1 remote-as 100
Device2(config-bgp)#neighbor 10.0.0.1 update-source loopback0
Device2(config-bgp)#neighbor 10.0.0.1 next-hop-self
Device2(config-bgp)#neighbor 3.0.0.1 remote-as 200
Device2(config-bgp)#exit
```

#配置 Device3。

```
Device3(config)#router bgp 100
Device3(config-bgp)#neighbor 10.0.0.1 remote-as 100
Device3(config-bgp)#neighbor 10.0.0.1 update-source loopback0
```

单播路由

```
Device3(config-bgp)#neighbor 10.0.0.1 next-hop-self
Device3(config-bgp)#neighbor 4.0.0.1 remote-as 200
Device3(config-bgp)#exit
```

#配置 Device4。

```
Device4#configure terminal
Device4(config)#router bgp 200
Device4(config-bgp)#neighbor 3.0.0.2 remote-as 100
Device4(config-bgp)#neighbor 4.0.0.2 remote-as 100
Device4(config-bgp)#network 75.0.0.0 255.255.255.0
Device4(config-bgp)#network 85.0.0.0 255.255.255.0
Device4(config-bgp)#exit
```

#查看 Device1 上 BGP 邻居状态。

```
Device1#show ip bgp summary
BGP router identifier 10.0.0.1, local AS number 100
BGP table version is 2
2 BGP AS-PATH entries
0 BGP community entries

Neighbor    V  AS MsgRcvd MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
20.0.0.1    4 100   11   11     2  0   0 00:07:40  2
30.0.0.1    4 100    7    7     2  0   0 00:03:59  2
```

#查看 Device4 上 BGP 邻居状态。

```
Device4#show ip bgp summary
BGP router identifier 85.0.0.1, local AS number 200
BGP table version is 2
2 BGP AS-PATH entries
0 BGP community entries

Neighbor    V  AS MsgRcvd MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
3.0.0.2     4 100    5    6     2  0   0 00:02:24  2
4.0.0.2     4 100    6    5     2  0   0 00:02:24  2
```

可以看到 Device1 分别与 Device2、Device3 成功建立 IBGP 邻居，Device4 分别与 Device2、Device3 成功建立 EBGP 邻居。

#查看 Device1 的路由表。

```
Device1#show ip bgp
BGP table version is 2, local router ID is 10.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop        Metric LocPrf Weight Path
[B]*> 55.0.0.0/24  0.0.0.0          0     32768 i
[B]*> 65.0.0.0/24  0.0.0.0          0     32768 i
[B]* i75.0.0.0/24  30.0.0.1         0 100  0 200 i
[B]*>i             20.0.0.1         0 100  0 200 i
[B]* i85.0.0.0/24  30.0.0.1         0 100  0 200 i
[B]*>i             20.0.0.1         0 100  0 200 i

Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

B 75.0.0.0/24 [200/0] via 20.0.0.1, 01:13:17, vlan2
B 85.0.0.0/24 [200/0] via 20.0.0.1, 01:13:17, vlan2
```

单播路由

可以看到 Device1 上路由 75.0.0.0/24 和 85.0.0.0/24 均选择了 Device2 为最优下一跳设备。

#查看 Device4 的路由表。

```
Device4#show ip bgp
BGP table version is 2, local router ID is 85.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop        Metric LocPrf Weight Path
[B]* 55.0.0.0/24   3.0.0.2         0      0 100 i
[B]*> 4.0.0.2     4.0.0.2         0      0 100 i
[B]* 65.0.0.0/24   3.0.0.2         0      0 100 i
[B]*> 4.0.0.2     4.0.0.2         0      0 100 i
[B]*> 75.0.0.0/24  0.0.0.0         0     32768 i
[B]*> 85.0.0.0/24  0.0.0.0         0     32768 i

Device4#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE - OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNRP, B - BGP, i - ISIS

Gateway of last resort is not set

B 55.0.0.0/24 [20/0] via 4.0.0.2, 01:25:19, vlan3
B 65.0.0.0/24 [20/0] via 4.0.0.2, 01:25:19, vlan3
```

可以看到 Device4 上路由 55.0.0.0/24 和 65.0.0.0/24 均选择了 Device3 为最优下一跳设备。

步骤 5: 配置访问控制列表和路由策略设置 local-preference 和 metric。

#配置 Device2。

```
Device2(config)#ip access-list standard 1
Device2(config-std-nacl)#permit 75.0.0.0 0.0.0.255
Device2(config-std-nacl)#exit
Device2(config)#ip access-list standard 2
Device2(config-std-nacl)#permit 65.0.0.0 0.0.0.255
Device2(config-std-nacl)#exit
Device2(config)#route-map SetPriority1 10
Device2(config-route-map)#match ip address 1
Device2(config-route-map)#set local-preference 110
Device2(config-route-map)#exit
Device2(config)#route-map SetPriority1 20
Device2(config-route-map)#exit
Device2(config)#route-map SetPriority2 10
Device2(config-route-map)#match ip address 2
Device2(config-route-map)#set metric 100
Device2(config-route-map)#exit
Device2(config)#route-map SetPriority2 20
Device2(config-route-map)#exit
```

在 Device2 上配置路由策略将路由 75.0.0.0/24 的 local-preference 设置为 110，同时将路由 65.0.0.0/24 的 metric 设置为 100。

#配置 Device3。

```
Device3(config)#ip access-list standard 1
Device3(config-std-nacl)#permit 85.0.0.0 0.0.0.255
Device3(config-std-nacl)#exit
Device3(config)#ip access-list standard 2
Device3(config-std-nacl)#permit 55.0.0.0 0.0.0.255
```


单播路由

```
Device3(config-std-nacl)#exit
Device3(config)#route-map SetPriority1 10
Device3(config-route-map)#match ip address 1
Device3(config-route-map)#set local-preference 110
Device3(config-route-map)#exit
Device3(config)#route-map SetPriority1 20
Device3(config-route-map)#exit
Device3(config)#route-map SetPriority2 10
Device3(config-route-map)#match ip address 2
Device3(config-route-map)#set metric 100
Device3(config-route-map)#exit
Device3(config)#route-map SetPriority2 20
Device3(config-route-map)#exit
```

在 Device3 上配置路由策略将路由 85.0.0.0/24 的 local-preference 设置为 110，同时将路由 55.0.0.0/24 的 metric 设置为 100。

说明：

- 配置路由策略时，前缀列表和 ACL 都可以创建过滤规则，它们的区别在于前缀列表可以精确匹配路由掩码，而 ACL 则不能匹配路由掩码。
-

步骤 6： 配置 BGP 关联路由策略。

#配置 Device2。

```
Device2(config)#router bgp 100
Device2(config-bgp)#neighbor 10.0.0.1 route-map SetPriority1 out
Device2(config-bgp)#neighbor 3.0.0.1 route-map SetPriority2 out
Device2(config-bgp)#exit
```

在 Device2 上配置邻居 10.0.0.1 的出方向修改 75.0.0.0/24 的 local-preference，同时配置邻居 3.0.0.1 的出方向修改 65.0.0.0/24 的 metric。

#配置 Device3。

```
Device3(config)#router bgp 100
Device3(config-bgp)#neighbor 10.0.0.1 route-map SetPriority1 out
Device3(config-bgp)#neighbor 4.0.0.1 route-map SetPriority2 out
Device3(config-bgp)#exit
```

在 Device3 上配置邻居 10.0.0.1 的出方向修改 85.0.0.0/24 的 local-preference，同时配置邻居 4.0.0.1 的出方向修改 55.0.0.0/24 的 metric。

在对等体上配置了路由策略后需要重置 BGP 进程才能生效。

步骤 7: 检验结果。

#查看 Device1 的路由表。

```
Device1#show ip bgp
BGP table version is 5, local router ID is 10.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop        Metric LocPrf Weight Path
[B]*> 55.0.0.0/24  0.0.0.0         0     32768 i
[B]*> 65.0.0.0/24  0.0.0.0         0     32768 i
[B]* i75.0.0.0/24  30.0.0.1        0    100   0 200 i
[B]*>i          20.0.0.1        0    110   0 200 i
[B]*>i85.0.0.0/24 30.0.0.1        0    110   0 200 i
[B]* i          20.0.0.1        0    100   0 200 i

Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

B 75.0.0.0/24 [200/0] via 20.0.0.1, 00:01:34, vlan2
B 85.0.0.0/24 [200/0] via 30.0.0.1, 00:00:51, vlan3
```

可以看出路由 75.0.0.0/24 及 85.0.0.0/24 的 local-preference 被成功修改, Device1 优选 Device2 通告的路由 75.0.0.0/24, 以及 Device3 通告的路由 85.0.0.0/24。

#查看 Device4 的路由表。

```
Device4#show ip bgp
BGP table version is 4, local router ID is 85.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop        Metric LocPrf Weight Path
[B]* 55.0.0.0/24  4.0.0.2         100    0 100 i
[B]*>          3.0.0.2         0      0 100 i
[B]*> 65.0.0.0/24  4.0.0.2         0      0 100 i
[B]*          3.0.0.2        100    0 100 i
[B]*> 75.0.0.0/24  0.0.0.0         0     32768 i
[B]*> 85.0.0.0/24  0.0.0.0         0     32768 i

Device4#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

B 55.0.0.0/24 [20/0] via 3.0.0.2, 00:15:02, vlan2
B 65.0.0.0/24 [20/0] via 4.0.0.2, 00:14:55, vlan3
```

可以看出路由 55.0.0.0/24 及 65.0.0.0/24 的 metric 被成功修改, Device4 优选 Device2 通告的路由 55.0.0.0/24, 以及 Device3 通告的路由 65.0.0.0/24。

说明：

- 路由策略可以使用在路由通告的出方向，同时也可以使用在路由接收的入方向。

44.3.7 配置 BGP 联盟

-E -A

网络需求

- Device2、Device3、Device4、Device5 在同一 BGP 自治系统 200 中，为了减少 IBGP 全连接，在同一个 BGP 联盟内将它们划到两个不同的 AS 中。
- Device1 与 Device2 建立 EBGP 邻居，并向自治系统 200 通告路由 100.0.0.0/24。

网络拓扑

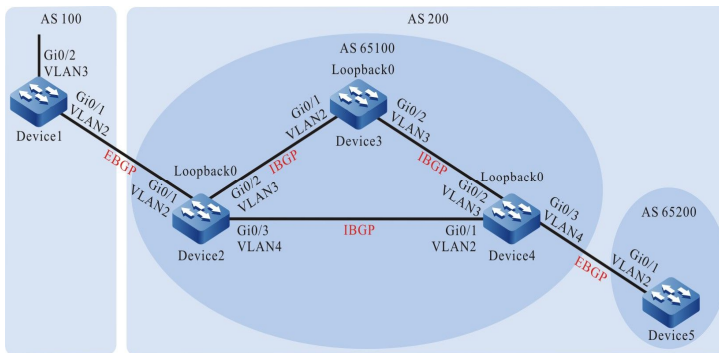


图 44-7 配置 BGP 联盟组网图

设备	接口	VLAN	IP 地址
Device1	Gi0/1	2	1.0.0.1/24
	Gi0/2	3	100.0.0.1/24
Device2	Gi0/1	2	1.0.0.2/24
	Gi0/2	3	2.0.0.2/24
	Gi0/3	4	3.0.0.2/24

设备	接口	VLAN	IP 地址
	Loopback0		20.0.0.1/32
Device3	Gi0/1	2	2.0.0.1/24
	Gi0/2	3	4.0.0.1/24
	Loopback0		30.0.0.1/32
Device4	Gi0/1	2	3.0.0.1/24
	Gi0/2	3	4.0.0.2/24
	Gi0/3	4	5.0.0.1/24
	Loopback0		40.0.0.1/32
Device5	Gi0/1	2	5.0.0.2/24

配置步骤

步骤 1: 配置 VLAN, 并将端口加入对应的 VLAN。 (略)

步骤 2: 配置各接口的 IP 地址。 (略)

步骤 3: 配置 OSPF, 使设备间 Loopback 路由互相可达。

#配置 Device2。

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 20.0.0.1 0.0.0.0 area 0
Device2(config-ospf)#exit
```

#配置 Device3。

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 4.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 30.0.0.1 0.0.0.0 area 0
```

单播路由

```
Device3(config-ospf)#exit
```

#配置 Device4。

```
Device4#configure terminal
Device4(config)#router ospf 100
Device4(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
Device4(config-ospf)#network 4.0.0.0 0.0.0.255 area 0
Device4(config-ospf)#network 5.0.0.0 0.0.0.255 area 0
Device4(config-ospf)#network 40.0.0.1 0.0.0.0 area 0
Device4(config-ospf)#exit
```

#配置 Device5。

```
Device5#configure terminal
Device5(config)#router ospf 100
Device5(config-ospf)#network 5.0.0.0 0.0.0.255 area 0
Device5(config-ospf)#exit
```

#查看 Device2 的路由表。

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

O 4.0.0.0/24 [110/2] via 2.0.0.1, 00:02:42, vlan3
   [110/2] via 3.0.0.1, 00:02:11, vlan4
O 30.0.0.1/32 [110/2] via 2.0.0.1, 00:02:32, vlan3
O 40.0.0.1/32 [110/2] via 3.0.0.1, 00:02:05, vlan4
```

#查看 Device3 的路由表。

```
Device3#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

O 3.0.0.0/24 [110/2] via 2.0.0.2, 00:03:24, vlan2
   [110/2] via 4.0.0.2, 00:02:38, vlan3
O 20.0.0.1/32 [110/2] via 2.0.0.2, 00:03:24, vlan2
O 40.0.0.1/32 [110/2] via 4.0.0.2, 00:02:38, vlan3
```

#查看 Device4 的路由表。

```
Device4#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

O 2.0.0.0/24 [110/2] via 3.0.0.2, 00:03:42, vlan2
   [110/2] via 4.0.0.1, 00:03:42, vlan3
O 20.0.0.1/32 [110/2] via 3.0.0.2, 00:03:42, vlan2
O 30.0.0.1/32 [110/2] via 4.0.0.1, 00:03:42, vlan3
```

#查看 Device5 的路由表。

```
Device5#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set
```

- 2.0.0.0/24 [110/3] via 5.0.0.1, 00:00:03, vlan2
- 3.0.0.0/24 [110/2] via 5.0.0.1, 00:00:03, vlan2
- 4.0.0.0/24 [110/2] via 5.0.0.1, 00:00:03, vlan2
- 20.0.0.1/32 [110/3] via 5.0.0.1, 00:00:03, vlan2
- 30.0.0.1/32 [110/3] via 5.0.0.1, 00:00:03, vlan2
- 40.0.0.1/32 [110/2] via 5.0.0.1, 00:00:03, vlan2

可以看出 Device2、Device3、Device4 互相学习到对方环回口的路由。

步骤 4: 配置联盟内 BGP 连接。

#配置联盟内 IBGP 连接。

#配置 Device2。

```
Device2(config)#router bgp 65100
Device2(config-bgp)#neighbor 30.0.0.1 remote-as 65100
Device2(config-bgp)#neighbor 30.0.0.1 update-source loopback0
Device2(config-bgp)#neighbor 40.0.0.1 remote-as 65100
Device2(config-bgp)#neighbor 40.0.0.1 update-source loopback0
Device2(config-bgp)#neighbor 30.0.0.1 next-hop-self
Device2(config-bgp)#neighbor 40.0.0.1 next-hop-self
Device2(config-bgp)#exit
```

#配置 Device3。

```
Device3(config)#router bgp 65100
Device3(config-bgp)#neighbor 20.0.0.1 remote-as 65100
Device3(config-bgp)#neighbor 20.0.0.1 update-source loopback0
Device3(config-bgp)#neighbor 40.0.0.1 remote-as 65100
Device3(config-bgp)#neighbor 40.0.0.1 update-source loopback0
Device3(config-bgp)#exit
```

#配置 Device4。

```
Device4(config)#router bgp 65100
Device4(config-bgp)#neighbor 20.0.0.1 remote-as 65100
Device4(config-bgp)#neighbor 20.0.0.1 update-source loopback0
Device4(config-bgp)#neighbor 30.0.0.1 remote-as 65100
Device4(config-bgp)#neighbor 30.0.0.1 update-source loopback0
Device4(config-bgp)#exit
```

#配置联盟内 EBGP 连接

#配置 Device4。

```
Device4(config)#router bgp 65100
Device4(config-bgp)#neighbor 5.0.0.2 remote-as 65200
Device4(config-bgp)#exit
```

#配置 Device5。

```
Device5(config)#router bgp 65200
Device5(config-bgp)#neighbor 5.0.0.1 remote-as 65100
Device5(config-bgp)#exit
```

#查看 Device4 上 BGP 邻居状态。

```
Device4#show ip bgp summary
```

单播路由

```
BGP router identifier 40.0.0.1, local AS number 65100
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries
```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
5.0.0.2	4	65200	15	15	2	0	0	00:09:40	0
20.0.0.1	4	65100	9	9	2	0	0	00:07:49	0
30.0.0.1	4	65100	7	7	2	0	0	00:05:39	0

Device4 与 Device2、Device3 建立 IBGP 邻居，Device4 与 Device5 建立 EBGP 邻居。

步骤 5： 配置 BGP 联盟。

#配置 Device1。

配置 EBGP 对等体，对等体 AS 号为联盟 ID 200。

```
Device1#configure terminal
Device1(config)#router bgp 100
Device1(config-bgp)#neighbor 1.0.0.2 remote-as 200
Device1(config-bgp)#network 100.0.0.0 255.255.255.0
Device1(config-bgp)#exit
```

#配置 Device2。

配置 BGP 联盟 ID 为 200，同时配置 EBGP 对等体，对等体 AS 号为 100。

```
Device2(config)#router bgp 65100
Device2(config-bgp)#bgp confederation identifier 200
Device2(config-bgp)#neighbor 1.0.0.1 remote-as 100
Device2(config-bgp)#exit
```

#配置 Device3。

配置 BGP 联盟 ID 为 200。

```
Device3(config)#router bgp 65100
Device3(config-bgp)#bgp confederation identifier 200
Device3(config-bgp)#exit
```

#配置 Device4。

配置 BGP 联盟 ID 为 200，并配置联盟包含区域 65100。

```
Device4#configure terminal
Device4(config)#router bgp 65100
Device4(config-bgp)#bgp confederation identifier 200
Device4(config-bgp)#bgp confederation peers 65200
Device4(config-bgp)#exit
```

#配置 Device5。

配置 BGP 联盟 ID 为 200，并配置联盟包含区域 65200。

```
Device5(config)#router bgp 65200
Device5(config-bgp)#bgp confederation identifier 200
Device5(config-bgp)#bgp confederation peers 65100
```

```
Device5(config-bgp)#exit
```

步骤 6: 检验结果。

#查看 Device1 上 BGP 邻居状态。

```
Device1#show ip bgp summary
BGP router identifier 100.0.0.1, local AS number 100
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor    V  AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down State/PfxRcd
1.0.0.2    4 200    6    6    2    0  00:02:20    0
```

可以看出 Device1 与 Device2 成功建立 EBGP 邻居关系。

#在 Device5 上查看路由信息。

```
Device5#show ip bgp
BGP table version is 49, local router ID is 5.0.0.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
              Network        Next Hop          Metric LocPrf Weight Path
[B]*> 100.0.0.0/24      20.0.0.1          0   100   0 (65100) 100 i

Device5#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE - OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i - ISIS

Gateway of last resort is not set

B 100.0.0.0/24 [200/0] via 20.0.0.1, 00:00:38, vlan2
```

Device5 成功学习到路由 100.0.0.0/24，同时可以看到该路由在联盟中传递的时候 next-hop 属性没有发生变化。Device2、Device3、Device4、Device5 均归属于同一联盟，所以不需要建立全连接关系，Device5 通过 Device4 来获取外部路由信息。

44.3.8 配置 BGP 与 BFD 联动 **-E -A**

网络需求

- Device1 分别与 Device2、Device3 建立 EBGP 邻居，Device2 与 Device3 建立 IBGP 邻居。
- Device1 同时从 Device2 和 Device3 学习到 EBGP 路由 3.0.0.0/24，Device1 优先选择通过 Device2 转发数据至 3.0.0.0/24 网段。
- 在 Device1 与 Device2 上配置 EBGP 关联 BFD，当 Device1 与 Device2 间的线路发生故障后 BFD 能迅速检测并通知 BGP，此时 Device1 选择通过 Device3 转发数据至 3.0.0.0/24 网段。

网络拓扑

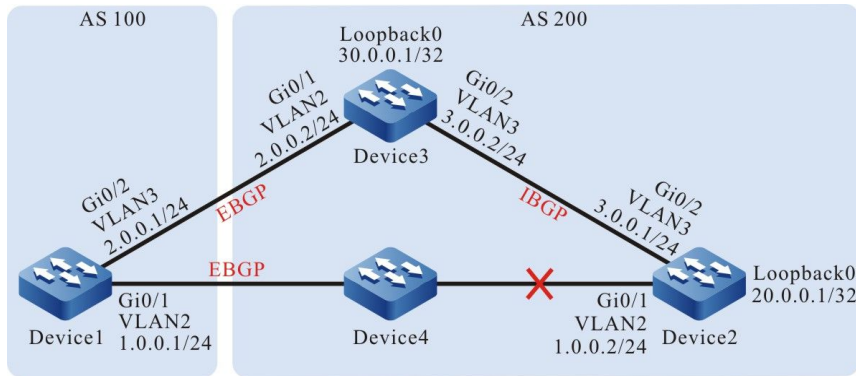


图 44-8 配置 BGP 与 BFD 联动组网图

配置步骤

步骤 1: 配置 VLAN, 并将端口加入对应的 VLAN。(略)

步骤 2: 配置各接口的 IP 地址。(略)

步骤 3: 配置 OSPF, 使设备间 Loopback 路由互相可达。

#配置 Device2。

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 20.0.0.1 0.0.0.0 area 0
Device2(config-ospf)#exit
```

#配置 Device3。

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 30.0.0.1 0.0.0.0 area 0
Device3(config-ospf)#exit
```

#查看 Device2 的路由表。

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

O 30.0.0.1/32 [110/2] via 3.0.0.2, 00:02:26, vlan3
```

#查看 Device3 的路由表。

```
Device3#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
```

单播路由

```
D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS
```

```
Gateway of last resort is not set
```

```
O 20.0.0.1/32 [110/2] via 3.0.0.1, 00:03:38, vlan3
```

可以看出 Device2、Device3 互相学习到对方环回口的路由。

步骤 4： 配置访问控制列表和路由策略，设置路由 metric。

#配置 Device1。

```
Device1#configure terminal
Device1(config)#ip access-list standard 1
Device1(config-std-nacl)#permit 3.0.0.0 0.0.0.255
Device1(config-std-nacl)#exit
Device1(config)#route-map SetMetric
Device1(config-route-map)#match ip address 1
Device1(config-route-map)#set metric 50
Device1(config-route-map)#exit
```

在 Device1 上配置路由策略将路由 3.0.0.0/24 的 metric 设置为 50。

步骤 5： 配置 BGP，同时在 Device1 关联路由策略。

#配置 Device1。

```
Device1(config)#router bgp 100
Device1(config-bgp)#neighbor 1.0.0.2 remote-as 200
Device1(config-bgp)#neighbor 2.0.0.2 remote-as 200
Device1(config-bgp)#neighbor 2.0.0.2 route-map SetMetric in
Device1(config-bgp)#exit
```

#配置 Device2。

```
Device2(config)#router bgp 200
Device2(config-bgp)#neighbor 1.0.0.1 remote-as 100
Device2(config-bgp)#neighbor 30.0.0.1 remote-as 200
Device2(config-bgp)#neighbor 30.0.0.1 update-source loopback0
Device2(config-bgp)#network 3.0.0.0 255.255.255.0
Device2(config-bgp)#exit
```

#配置 Device3。

```
Device3(config)#router bgp 200
Device3(config-bgp)#neighbor 2.0.0.1 remote-as 100
Device3(config-bgp)#neighbor 20.0.0.1 remote-as 200
Device3(config-bgp)#neighbor 20.0.0.1 update-source loopback0
Device3(config-bgp)#network 3.0.0.0 255.255.255.0
Device3(config-bgp)#exit
```

在对等体上配置了路由策略后需要重置 BGP 进程才能生效。

#查看 Device1 上 BGP 邻居状态。

```
Device1#show ip bgp summary
BGP router identifier 2.0.0.1, local AS number 100
BGP table version is 2
```

单播路由

```
2 BGP AS-PATH entries
0 BGP community entries
```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
1.0.0.2	4	200	2	2	2	0	0	00:01:32	1
2.0.0.2	4	200	2	2	2	0	0	00:01:43	1

#查看 Device2 上 BGP 邻居状态。

```
Device2#show ip bgp summary
BGP router identifier 20.0.0.1, local AS number 200
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries
```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
1.0.0.1	4	100	2	2	2	0	0	00:02:52	0
30.0.0.1	4	200	3	3	2	0	0	00:02:45	1

可以看到 Device1、Device2、Device3 间 BGP 邻居均成功建立。

#查看 Device1 的路由表。

```
Device1#show ip bgp
BGP table version is 3, local router ID is 1.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
```

```
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop           Metric LocPrf Weight Path
[B]* 3.0.0.0/24    2.0.0.2             50      0 200 i
[B]*> 1.0.0.2      1.0.0.2              0       0 200 i
```

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS
```

```
Gateway of last resort is not set
```

```
B 3.0.0.0/24 [20/0] via 1.0.0.2, 00:07:19, vlan2
```

可以看到 Device1 上路由 3.0.0.0/24 选择了 Device2 为最优下一跳设备。

步骤 6: 配置 BGP 与 BFD 联动。

#配置 Device1。

```
Device1(config)#bfd fast-detect
Device1(config)#router bgp 100
Device1(config-bgp)#neighbor 1.0.0.2 fall-over bfd
Device1(config-bgp)#exit
Device1(config)#interface vlan2
Device1(config-if-vlan2)#bfd min-receive-interval 500
Device1(config-if-vlan2)#bfd min-transmit-interval 500
Device1(config-if-vlan2)#bfd multiplier 4
Device1(config-if-vlan2)#exit
```

#配置 Device2。

```
Device2(config)#bfd fast-detect
Device2(config)#router bgp 200
Device2(config-bgp)#neighbor 1.0.0.1 fall-over bfd
Device2(config-bgp)#exit
```

单播路由

```
Device2(config)#interface vlan2
Device2(config-if-vlan2)#bfd min-receive-interval 500
Device2(config-if-vlan2)#bfd min-transmit-interval 500
Device2(config-if-vlan2)#bfd multiplier 4
Device2(config-if-vlan2)#exit
```

在 EBGP 邻居 Device1 与 Device2 间启用 BFD，并修改 BFD 控制报文的最小发送时间间隔和最小接收时间间隔及检测超时倍数。

步骤 7: 检验结果。

#在 Device1 上查看 BFD 会话状态。

```
Device1#show bfd session
OurAddr      NeighAddr      LD/RD      State      Holddown      interface
1.0.0.1      1.0.0.2      2/2      UP      2000      vlan2
```

可以看到 Device1 上的 BFD 状态正确 up，holddown 时间协商为 2000ms。

#当 Device1 与 Device2 间线路发生故障时，路由能够迅速切换至备份线路。

#查看 Device1 的路由表。

```
Device1#show ip bgp
BGP table version is 6, local router ID is 1.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
              Network      Next Hop      Metric LocPrf Weight Path
[B]*> 3.0.0.0/24      2.0.0.2      50      0 200 i

Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

B 3.0.0.0/24 [20/50] via 2.0.0.2, 00:00:05, vlan3
```

可以看出路由 3.0.0.0/24 的下一跳切换至 Device3。

45 IPv6 BGP

45.1 IPv6 BGP 简介

IPv6 BGP (BGP4+) 在 BGP-4 基础上扩展而来, BGP-4 只能管理 IPv4 路由信息, 为了实现对 IPv6 协议的支持, IETF 对 BGP-4 进行了扩展, 形成 IPv6 BGP, 目前的 IPv6 BGP 标准是 RFC 2858 (Multiprotocol Extensions for BGP-4, BGP-4 多协议扩展)。

IPv6 BGP 需要将 IPv6 网络层协议的信息反映到 NLRI (Network Layer Reachability Information, 网络层可达信息) 及 NEXT_HOP 属性中。IPv6 BGP 中引入的两个 NLRI 属性分别是:

- MP_REACH_NLRI: Multiprotocol Reachable NLRI, 多协议可达 NLRI。用于发布可达路由及下一跳信息。
- MP_UNREACH_NLRI: Multiprotocol Unreachable NLRI, 多协议不可达 NLRI。用于撤销不可达路由。

IPv6 BGP 中的 NEXT_HOP 属性用 IPv6 地址来表示, 可以是 IPv6 全球单播地址或者链路本地地址。

IPv6 BGP 是利用 BGP 的多协议扩展属性, 来达到在 IPv6 网络中应用的目的, BGP 协议原有的消息机制和路由机制并没有改变。

45.2 IPv6 BGP 功能配置

表 45-1 BGP 功能配置列表

配置任务	
配置 IPv6 BGP 邻居	配置 IBGP 邻居
	配置 EBGP 邻居

配置任务	
	配置 BGP 被动邻居
	配置 MP-BGP 邻居
	配置 BGP 邻居 MD5 认证
配置 BGP 路由生成	配置 BGP 发布本地路由
	配置 BGP 路由重分发
	配置 BGP 发布缺省路由
配置 BGP 路由控制	配置 BGP 发布聚合路由
	配置 BGP 路由管理距离
	配置 BGP 邻居出方向路由策略
	配置 BGP 邻居入方向路由策略
	配置 BGP 邻居接收路由最大条目数
	配置 BGP 最大负载均衡条目数
配置 BGP 路由属性	配置 BGP 路由权重
	配置 BGP 路由 MED 属性
	配置 BGP 路由 Local-Preference 属性
	配置 BGP 路由 AS_PATH 属性
	配置 BGP 路由 NEXT-HOP 属性

配置任务	
	配置 BGP 路由团体属性
配置 BGP 网络优化	配置 BGP 邻居保活时间
	配置 BGP 路由检测时间
	配置 EBGP 邻居快速断连
	配置 BGP 路由抑制功能
	配置 BGP 邻居刷新能力
	配置 BGP 邻居软重置能力
	配置 BGP 邻居 ORF 能力
配置 BGP 大型网络	配置 BGP 对等体组
	配置 BGP 路由反射器
	配置 BGP 联盟
配置 BGP GR	配置 BGP GR Restarter
	配置 BGP GR Helper
配置 BGP 与 BFD 联动	配置 EBGP 与 BFD 联动
	配置 IBGP 与 BFD 联动

45.2.1 配置 IPv6 BGP 邻居

-E -A**配置条件**

在配置 BGP 邻居之前，首先完成以下任务：

- 配置链路层协议，保证链路层通信正常。
- 配置接口的网络层地址，使相邻网络节点网络层可达。

配置 IBGP 邻居

1、基本配置

配置 IBGP 邻居需要指定邻居 AS 与本设备 AS 相同。可以对设备配置 Router ID，该 Router ID 用于建立 BGP 会话时，唯一标明一台 BGP 设备，未配置 Router ID 时将由设备根据接口地址进行优选，优先方式原则如下：

- 首先从 Loopback 接口的 IP 地址中选择最大的作为 Router ID；
- 若没有配置 IP 地址的 Loopback 接口，则从其它接口的 IP 地址中选择最大的作为 Router ID；
- 只有接口处于 UP 状态时，该接口地址才可能被选作 Router ID。

表 45-2 配置 IBGP 邻居

步骤	命令	说明
进入全局配置模式	configure terminal	-
启用 BGP 协议并进入 BGP 配置模式	router bgp <i>autonomous-system</i>	必选 缺省情况下，未启用 BGP
配置 BGP 设备标识	bgp router-id <i>router-id</i>	可选 缺省情况下，设备根据接口地址进行优选，优先方式采用 Loopback 接口优先与 IP 地址大优先原则
配置 IBGP 邻居	neighbor { <i>neighbor-address</i> <i>peer-group-</i>	必选

步骤	命令	说明
	<i>name</i> } remote-as <i>as-number</i>	缺省情况下, 未创建任何 IBGP 邻居
配置 IBGP 邻居描述	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } description <i>description-string</i>	可选 缺省情况下, IBGP 邻居无描述信息
进入 BGP IPv6 单播配置模式	address-family ipv6 unicast	-
激活 IBGP 邻居收发 IPv6 单播路由的能力	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } activate	可选 缺省情况下, 未激活 IBGP 邻居收发 IPv6 单播路由的能力

2、配置 TCP 会话的源地址

BGP 使用 TCP 作为其传输协议, TCP 具有传输可靠的特点, 有效保证 BGP 协议报文能正确传输给邻居。

表 45-3 配置 TCP 会话的源地址

步骤	命令	说明
进入全局配置模式	configure terminal	-
启用 BGP 协议并进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
配置 IBGP 邻居	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } remote-as <i>as-number</i>	必选 缺省情况下, 未创建任何 IBGP 邻居

步骤	命令	说明
配置 IBGP 邻居 TCP 会话的源地址	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } update-source { <i>interface-name</i> <i>ipv6-address</i> }	必选 缺省情况下，TCP 会话自动选择路由出接口的地址作为源地址

说明：

- 在存在负载均衡路由时需要 BGP 邻居之间明确配置 TCP 会话的源地址，未配置 TCP 源地址时，可能由于邻居的最优路由不同，而采用不同出接口作为各自的源地址，导致 BGP 会话一段时间内无法成功建立。

配置 EBGP 邻居

1、基本配置

配置 EBGP 邻居需要指定邻居 AS 与本设备 AS 不同。

表 45-4 配置 EBGP 邻居

步骤	命令	说明
进入全局配置模式	configure terminal	-
启用 BGP 协议并进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
配置 EBGP 邻居	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } remote-as <i>as-number</i>	必选 缺省情况下，未创建任何 EBGP 邻居

2、配置非直连 EBGP 邻居

EBGP 邻居各自处于不同的运营网络，通常由一条直连的物理链路进行连接，所以 EBGP 邻居间通信的 IP 报文缺省 TTL 值为 1，如果在非直连的运营网络之间，可以通过配置命令设置 IP 报文的 TTL 值，以达到允许 BGP 建连的目的。

表 45-5 配置非直连 EBGP 邻居

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
配置 EBGP 邻居	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } remote-as <i>as-number</i>	必选 缺省情况下，未创建任何 EBGP 邻居
配置 EBGP 邻居 TCP 会话的源地址	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } update-source { <i>interface-name</i> <i>ipv6-address</i> }	可选 缺省情况下，TCP 会话自动选择路由出接口的地址作为源地址
配置允许非直连 EBGP 邻居间建立连接	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } ebgp-multihop [<i>ttl-value</i>]	必选 缺省情况下，不允许非直连设备间形成 EBGP 邻居关系

配置 BGP 被动邻居

特殊应用环境中需要用到 BGP 的被动邻居功能。应用被动邻居后，BGP 不主动向邻居发起用于建立 BGP 邻居的 TCP 连接请求，只能等待邻居主动建连请求才能建立邻居关系。缺省情况下，邻居双方将相互主动发起连接，在连接存在冲突时将优选一条 TCP 连接形成 BGP 会话。在配置 BGP 被动邻居之前，需要配置 BGP 邻居。

表 45-6 配置 BGP 被动邻居

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
配置 BGP 邻居	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } remote-as <i>as-number</i>	必选 缺省情况下，未创建任何 BGP 邻居
配置 BGP 被动邻居	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } passive	必选 缺省情况下，未启用任何被动邻居

配置 MP-BGP 邻居

缺省情况下，BGP 邻居需要在 VRF 地址族、VPN 地址族激活才能具有收发对应路由的能力。在配置 MP-BGP 邻居之前，需要配置 BGP 邻居。

表 45-7 配置 MP-BGP 邻居

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
配置 BGP 邻居	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } remote-as <i>as-number</i>	必选 缺省情况下，未创建任何 BGP 邻居

步骤	命令	说明
进入 BGP IPv6 VRF 配置模式	address-family ipv6 vrf <i>vrf-name</i>	-
配置 BGP IPv6 VRF 地址簇下邻居	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } remote-as <i>as-number</i>	必选 缺省情况下, 未创建任何 BGP 邻居
IPv6 VRF 地址簇下激活邻居	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } activate	可选 缺省情况下, BGP IPv6 VRF 配置模式的邻居已处于激活状态
退出 BGP IPv6 VRF 配置模式	exit-address-family	-

说明:

- 在 BGP 配置模式和 BGP IPv6 单播配置模式下配置的邻居为全局邻居, 在 BGP IPv6 VRF 配置模式下配置的邻居仅属于该 VRF 地址簇。

配置 BGP 邻居 MD5 认证

BGP 支持配置 MD5 认证对邻居间的信息交互进行保护, MD5 认证由 TCP 传输协议完成。邻居双方必须配置相同的 MD5 认证密码才能建立 TCP 连接, 否则 TCP 传输协议对 MD5 认证失败后将不能建立 TCP 连接。配置 BGP 邻居 MD5 认证前, 需要配置 BGP 邻居。

表 45-8 配置 BGP 邻居 MD5 认证

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
配置 BGP 邻居	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } remote-as <i>as-number</i>	必选 缺省情况下，未创建任何 BGP 邻居
配置 BGP 邻居 MD5 认证	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } password [0 7] <i>password-string</i>	必选 缺省情况下，BGP 邻居间不进行 MD5 认证

45.2.2 配置 IPv6 BGP 路由生成 **-E -A**

配置条件

在配置 BGP 路由生成之前，首先完成以下任务：

- 启用 BGP 协议。
- 配置 IPv6 BGP 邻居并使会话建连成功。

配置 BGP 发布本地路由

BGP 可以通过 **network** 命令引入 IPv6 路由表中的路由到 BGP 路由表中，仅当 IPv6 路由表中有与 **network** 前缀和掩码完全匹配的条目，才会将该路由引入到 BGP 路由表中并且将之发布。

在发布本地路由的同时，可以对路由应用路由图，也可以指定该路由为后门路由。后门路由将 EBGP 路由看作是本地 BGP 路由并使用本地路由的管理距离，这样允许 IGP 路由优先于 EBGP 路由，同时，后门路由不会通告给 EBGP 邻居。

表 45-9 配置 BGP 发布本地路由

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
进入 BGP IPv6 单播配置模式	address-family ipv6 unicast	-
配置 BGP 发布本地路由	network <i>ipv6-prefix</i> [route-map <i>rtmap-name</i> [backdoor] backdoor]	必选 缺省情况下，BGP 不发布任何本地路由

说明：

- BGP 发布本地路由的路由 Origin 属性类型为 IGP。
- 使用 **network backdoor** 命令作用 EBGP 路由后，EBGP 路由管理距离将变成本地路由管理距离（缺省情况下，EBGP 路由管理距离为 20，本地路由管理距离为 200），低于缺省 IGP 路由管理距离，使 IGP 路由被优选，这样 EBGP 邻居间形成后门链路。
- BGP 发布本地路由由应用路由图支持的 match 选项有 as-path、community、extcommunity、ipv6 address、ipv6 nexthop、metric，支持的 set 选项有 as-path、comm-list、community、extcommunity、ipv6 next-hop、local-preference、metric、origin、weight。

配置 BGP 路由重分发

BGP 主要不负责学习路由，而重点通过管理路由属性达到控制路由方向的目的，因此 BGP 通过重分发 IGP 来产生 BGP 路由向邻居通告。BGP 重分发 IGP 路由的同时，可以应用路由图。

表 45-10 配置 BGP 路由重分发

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
进入 BGP IPv6 单播配置模式	address-family ipv6 unicast	-
配置 BGP 重分发 IGP 路由	redistribute { connected isis [<i>area-tag</i>] [match <i>isis-level</i>] ospf <i>as-number</i> [match <i>route-sub-type</i>] rip <i>process-id</i> static } [route-map <i>map-name</i> / metric <i>value</i>]	必选 缺省情况下，BGP 不重分发其它任何 IGP 路由

说明：

- BGP 重分发的 IGP 路由 Origin 属性类型为 INCOMPLETE。
- BGP 重分发其它协议应用路由图支持的 match 选项有 as-path、community、extcommunity、ipv6 address、ipv6 nexthop、metric，支持的 set 选项有 as-path、comm-list、community、extcommunity、ipv6 next-hop、local-preference、metric、origin、weight。

配置 BGP 发布缺省路由

BGP 向邻居发布缺省路由前，需要引入缺省路由。引入缺省路由有两种方式：通过 **neighbor default-originate** 命令生成 BGP 的缺省路由；通过 **default-information originate** 命令重分发其它协议的缺省路由。

neighbor default-originate 命令生成的缺省路由是通过 BGP 自动产生一条 0::/0 的路由，**default-information originate** 命令重分发的缺省路由是 BGP 引入被重分发协议的一条 0::/0 的路由。

表 45-11 配置 BGP 发布缺省路由

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
进入 BGP IPv6 单播配置模式	address-family ipv6 unicast	-
配置 BGP 生成缺省路由	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } default-originate [route-map <i>rtmap-name</i>]	必选 缺省情况下，BGP 不产生缺省路由
配置 BGP 重分发其他协议的缺省路由	default-information originate	必选 缺省情况下，BGP 不重分发其它协议的缺省路由

说明：

- 配置 BGP 重分发其它协议的缺省路由同时需要配置路由重分发。
- 可以在配置 BGP 生成缺省路由时对该路由应用路由图。
- BGP 生成缺省路由应用路由图支持的 set 选项有 as-path、comm-list、community、extcommunity、ipv6 next-hop、local-preference、metric、origin、weight。

45.2.3 配置 IPv6 BGP 路由控制 **-E -A****配置条件**

在配置 BGP 路由控制之前，首先完成以下任务：

- 启用 BGP 协议。
- 配置 IPv6 BGP 邻居并使会话建连成功。

配置 BGP 发布聚合路由

在大型 BGP 网络中，为了减少向邻居通告的路由数量或者有效控制 BGP 选路过程，需要配置 BGP 聚合路由。

表 45-12 配置 BGP 发布聚合路由

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
进入 BGP IPv6 单播配置模式	address-family ipv6 unicast	-
配置 BGP 发布聚合路由	aggregate-address <i>ipv6-prefix</i> [as-set / summary-only / route-map <i>rtmap-name</i>]	必选 缺省情况下，BGP 不会进行路由聚合

说明：

- BGP 发布聚合路由时，可以通过指定 **summary-only** 命令选项只通告聚合路由来达到减少路由通告规模的目的。

- 通过指定 **as-set** 命令选项可以生成具有 AS_PATH 属性的聚合路由。
- 通过对聚合路由由应用路由图可以设置聚合路由更丰富的属性。

配置 BGP 路由管理距离

在 IP 路由表中各个协议都有控制选路的管理距离，该值越小越优先。BGP 通过对指定网段路由配置管理距离的方式来影响选路，覆盖到指定网段路由的管理距离都会被修改，同时可以应用 ACL 对覆盖网段进行有效过滤，仅 ACL 允许网段的管理距离才会被修改。

distance bgp 命令用于同时修改 BGP 外部、内部以及本地路由的管理距离，**distance** 命令仅用于修改指定网段路由的管理距离。**distance** 命令优先于 **distance bgp** 命令，配置 **distance** 覆盖的网段将采用该命令指定的管理距离，未覆盖的网段才采用 **distance bgp** 设置的管理距离。

表 45-13 配置 BGP 路由管理距离

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
进入 BGP IPv6 单播配置模式	address-family ipv6 unicast	-
配置 BGP 修改缺省管理距离	distance bgp <i>external-distance internal-distance local-distance</i>	可选 缺省情况下，EBGP 路由管理距离为 20，
配置指定网段的管理距离	distance administrative-distance ipv6-prefix [<i>acl-num</i> <i>acl-name</i>]	IBGP 路由管理距离为 200，本地路由管理距离为 200

配置 BGP 邻居出方向路由策略

单播路由

BGP 路由通告或选路依赖其强大的路由属性完成，在通告路由给邻居时可以通过应用相应的策略对路由属性进行修改或者过滤掉部份路由。目前支持在出方向上应用的策略有：

- distribute-list: 分布列表；
- filter-list : AS_PATH 属性过滤列表；
- prefix-list: IP 前缀列表；
- route-map: 路由图。

表 45-14 配置 BGP 邻居出方向路由策略

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
进入 BGP IPv6 单播配置模式	address-family ipv6 unicast	-
指定在出方向上应用分布列表	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } distribute-list { <i>access-list-num</i> <i>access-list-name</i> } out	多选（分布列表与 IP 前缀列表不能同时配置） 缺省情况下，未配置 BGP 邻居出方向路由策略
指定在出方向上应用 AS_PATH 属性过滤列表	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } filter-list <i>aspath-list-name</i> out	
指定在出方向上应用 IP 前缀列表	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } prefix-list <i>prefix-list-name</i> out	

步骤	命令	说明
指定在出方向上应用路由图	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } route-map <i>rtmap-name</i> out	

说明：

- 配置 BGP 邻居出方向路由策略后，需要重置邻居才能生效。
- 配置路由反射器出方向上应用路由图时，只能改变 NEXT-HOP 属性。
- 配置过滤列表请参见策略工具-配置 AS-PATH 列表章节。
- 配置邻居出方向上的策略时，可以同时配置多个，BGP 按照 **distribute-list**、**filter-list**、**prefix-list**、**route-map** 的先后顺序进行应用，排在前面的策略拒绝后不会进行后面策略的应用，只有配置的所有策略都通过后才通告路由信息。
- BGP 出方向上应用的路由图支持的 match 选项有 as-path、community、extcommunity、ipv6 address、ipv6 nexthop、metric，支持的 set 选项有 as-path、comm-list、community、extcommunity、ipv6 next-hop、local-preference、metric、origin、weight。

配置 BGP 邻居入方向路由策略

BGP 可以应用策略对接收到的路由信息过滤或修改其属性，与出方向上应用策略相同，入方向上也支持四种策略：

- distribute-list: 分布列表；
- filter-list : AS_PATH 属性过滤列表；
- prefix-list: IPv6 前缀列表；
- route-map: 路由图。

表 45-15 配置 BGP 邻居入方向应用策略

单播路由

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
进入 BGP IPv6 单播配置模式	address-family ipv6 unicast	-
指定在入方向上应用分布列表	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } distribute-list { <i>access-list-num</i> <i>access-list-name</i> } in	<p>多选（分布列表与 IP 前缀列表不能同时配置）</p> <p>缺省情况下，在入方向上没有指定任何策略</p>
指定在入方向上应用 AS_PATH 属性过滤列表	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } filter-list <i>aspath-list-name in</i>	
指定在入方向上应用 IP 前缀列表	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } prefix-list <i>prefix-list-name in</i>	
指定在入方向上应用路由图	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } route-map <i>rtmap-name in</i>	

说明：

- 配置 BGP 邻居入方向路由策略后，需要重置邻居才能生效。
- 配置邻居入方向上的策略时，可以同时配置多个，BGP 按照 **distribute-list**、**filter-list**、**prefix-list**、**route-map** 的先后顺序进行应用，排在前面的策略拒绝后不会进行后面策略的应用，只有配置的所有策略都通过后才将路由加入到数据库中。
- BGP 入方向上应用的路由策略支持的 match 选项有 as-path、community、extcommunity、ipv6 address、ipv6 nexthop、metric，支持的 set 选项有 as-path、comm-list、community、extcommunity、ipv6 next-hop、local-preference、metric、origin、weight。

配置 BGP 邻居接收路由最大条目数

BGP 设备支持对指定邻居限制接收路由的条目数，当从指定邻居接收到的路由达到一定阈值时进行告警或者断连。

表 45-16 配置 BGP 邻居接收路由最大条目数

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
进入 BGP IPv6 单播配置模式	address-family ipv6 unicast	-
配置邻居接收的最大路由条目数	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } maximum-prefix <i>prefix-num</i> [<i>threshold-value</i>] [warning-only]	必选 缺省情况下，没有限制从邻居接收的前缀条目数

说明：

- 如果未指定 **warning-only** 命令选项，在 BGP 从邻居接收的路由达到最大条目数时，将

自动断开 BGP 会话。

- 如果指定 **warning-only** 命令选项，在 BGP 从邻居接收的路由达到最大条目数时，仅给出告警信息，不阻止路由继续学习。

配置 BGP 最大负载均衡条目数

在 BGP 组网环境中，如果到达同一个目的地具有几条开销相同路径，那么可以通过配置 BGP 负载条目数来形成负载均衡路由。

表 45-17 配置 BGP 最大负载均衡条目数

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
进入 BGP IPv6 单播配置模式	address-family ipv6 unicast	-
配置 IBGP 最大负载条目数	maximum-paths ibgp <i>number</i>	必选 缺省情况下，IBGP 不进行负载均衡路由选路
配置 EBGP 最大负载条目数	maximum-paths <i>number</i>	必选 缺省情况下，EBGP 不进行负载均衡路由选路

说明：

- 配置 EBGP 最大负载均衡条目数后，仅当 EBGP 路由被优选后才能形成负载。
- 配置最大负载均衡条目数在不同 BGP 配置模式下命令不同，详见 BGP 技术命令对 **maximum-paths** 描述。

45.2.4 配置 IPv6 BGP 路由属性 **-E -A**

配置条件

在配置 BGP 路由属性之前，首先完成以下任务：

- 启用 BGP 协议。
- 配置 IPv6 BGP 邻居并使会话建连成功。

配置 BGP 路由权重

BGP 选路第一条规则是比较路由的权重值，路由权重值越大越优先。路由权重值是设备的本地属性，不会传递给其它 BGP 邻居。路由权重值取值范围 0~65535，缺省情况下，从邻居学习到的路由权重值为 0，本地设备产生的所有路由权重值都是 32768。

表 45-18 配置 BGP 路由权重

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
配置邻居或对等体组的路由权重	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } weight <i>weight-num</i>	必选 缺省情况下，邻居的路由权重值为 0

配置 BGP 路由 MED 属性

MED 属性用于对进入 AS 的流量选择最佳路由。在其它选路条件相同的情况下，BGP 从不同的 EBGP 邻居学习到具有相同目的地址但下一跳不同的路由时，BGP 将优选 MED 值最小者作为最佳入口。

MED 有时也被称为“外部度量”，并在 BGP 路由表中被标记为“度量 (Metric)”。BGP 会将从邻居学习到路由的 MED 属性通告给 IBGP 邻居，但不会通告给 EBGP 邻居，于是 MED 只适用于相邻 AS 之间。

1、配置 BGP 允许比较来自不同 AS 邻居路由的 MED

缺省情况下，BGP 只会对从同一个 AS 学习到的路由进行 MED 选路，但可以通过 **bgp always-compare-med** 命令来忽略 MED 选路时对相同 AS 要求的限制。

表 45-19 配置 BGP 允许比较来自不同 AS 邻居路由的 MED

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
配置 BGP 允许比较来自不同 AS 邻居路由的 MED	bgp always-compare-med	必选 缺省情况下，BGP 只允许比较来自相同 AS 的路由 MED

2、配置 BGP 根据路由 AS_PATH 进行的分组对 MED 排序优选

缺省情况下，没有启用 BGP 根据路由 AS_PATH 进行的分组对 MED 排序优选，可以通过 **bgp deterministic-med** 命令开启该功能。在路由选择的时候，将所有的路由都基于 AS_PATH 编排，在每一个 AS_PATH 组内，根据 MED 的大小对路由进行排序，MED 值最小的路由被选为该组的最佳路由。

表 45-20 配置 BGP 根据路由 AS_PATH 进行的分组对 MED 排序优选

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
BGP 根据路由 AS_PATH 进行的分组对 MED 排序优选	bgp deterministic-med	必选 缺省情况下，没有启用 BGP 根据路由 AS_PATH 进行的分组对 MED 排序优选

3、配置比较本地联盟路由的 MED

来自不同 AS 的 EBGP 路由缺省情况下不会比较 MED 属性，该原理同时对联盟的 EBGP 有效，命令 **bgp bestpath med confed** 用于启用对本地联盟的路由比较 MED 属性值。

表 45-21 配置 BGP 比较本地联盟路由的 MED

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
配置 BGP 用对本地联盟的路由比较 MED 属性值	bgp bestpath med confed	必选 缺省情况下，不会对本地联盟的路由比较 MED 属性值

4、配置路由图修改 MED 属性

在路由收发时，可以应用路由图修改 MED 属性值。

表 45-22 配置路由图修改 MED 属性

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
进入 BGP IPv6 单播配置模式	address-family ipv6 unicast	-
配置路由图修改 MED 属性	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } route-map <i>rtmap-name</i> in out	必选 缺省情况下，不对任何邻居应用路由图

说明：

- 配置路由图修改 MED 属性时，需要通过 **set metric** 命令对 MED 进行修改，请参见策略工具-技术手册-**set metric**。
- 配置 **neighbor attribute-unchanged** 命令后将不能通过路由图改变邻居 MED 属性。

配置 BGP 路由 Local-Preference 属性

Local-Preference 属性只会在 IBGP 邻居之间传递。Local-Preference 用于选择离开 AS 的最佳出口，Local-Preference 最大的路由将会被优选。

Local-Preference 属性取值范围 0~4294967295，数值越大，该路由由优先级越高。缺省情况下，所有通告给 IBGP 邻居的路由 Local-Preference 属性为 100，可以通过 **bgp default local-preference** 或者路由图修改 Local-Preference 属性。

1、配置 BGP 修改缺省 Local-Preference 属性

表 45-23 配置 BGP 修改缺省 Local-Preference 属性

单播路由

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
配置 BGP Local-Preference 属性缺省值	bgp default local-preference <i>local-value</i>	可选 缺省情况下, 缺省本地优先级为 100

2、配置路由图修改 Local- Preference 属性

表 45-24 配置路由图修改 Local-Preference 属性

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
进入 BGP IPv6 单播配置模式	address-family ipv6 unicast	-
配置路由图修改 Local-Preference 属性	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } route-map <i>rtmap-name</i> in out	必选 缺省情况下, 不对任何邻居应用路由图

说明:

- 配置路由图修改 Local-Preference 属性时, 需要通过 **set local-preference** 命令对 Local-Preference 属性进行修改, 请参见策略工具-技术手册-**set local-preference**。

配置 BGP 路由 AS_PATH 属性

1、配置 BGP 选路时忽略比较 AS_PATH

在其它条件相同条件下，BGP 选路时将优选 AS_PATH 最短的路由，但可以通过 **bgp bestpath as-path ignore** 命令取消通过 AS_PATH 选路。

表 45-25 配置 BGP 选路时忽略比较 AS_PATH

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
配置 BGP 选路时忽略比较 AS_PATH	bgp bestpath as-path ignore	必选 缺省情况下，选路时对 AS_PATH 属性值进行比较

2、配置 BGP 允许本地 AS 号重复出现次数

为了避免路由环路，BGP 会检查从邻居收到的路由 AS_PATH 属性，将丢弃包含本地 AS 号的路由，但可以通过 **neighbor allowas-in** 命令允许 BGP 接收到的路由 AS_PATH 属性中包含有本地 AS 号，并且可以配置包含本地 AS 号的个数。

表 45-26 配置 BGP 允许本地 AS 号重复出现次数

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-

步骤	命令	说明
进入 BGP IPv6 单播配置模式	address-family ipv6 unicast	-
配置允许本地 AS 号重复	neighbor { neighbor-address peer-group-name } allowas-in [as-num]	必选 缺省情况下，不允许从邻居接收到的路由 AS_PATH 属性中含有本地 AS 号

3、配置 BGP 向邻居通告路由时移除私有 AS 号

在大型 BGP 网络中，路由 AS_PATH 属性具有联盟或团体属性，缺省情况下，BGP 向邻居通告时将携带这些私有 AS 属性信息，为了屏蔽私网信息，可以通过 **neighbor remove-private-AS** 移除私有 AS 号。

表 45-27 配置 BGP 向邻居通告路由时移除私有 AS 号

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp autonomous-system	-
进入 BGP IPv6 单播配置模式	address-family ipv6 unicast	-
配置 BGP 向邻居通告路由时移除私有 AS 号	neighbor { neighbor-address peer-group-name } remove-private-AS	必选 缺省情况下，向邻居通告时将携带私有 AS 号

4、配置检测 EBGP 路由的第一个 AS 号合法性

BGP 向 EBGP 邻居通告路由时会将本地 AS 号压入到 AS_PATH 的开始位置，第一个通告该路由的 AS 将会处在最末位。通常情况下，从 EBGP 收到的路由第一个 AS 号应该与邻居的 AS 号相同，否则该路由将会被丢弃。

表 45-28 配置检测 EBGP 路由的第一个 AS 号合法性

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
配置检测 EBGP 路由的第一个 AS 号合法性	bgp enforce-first-as	必选 缺省情况下，BGP 未开启这种首 AS 号检查机制

5、配置路由图修改 AS_PATH 属性

BGP 支持配置路由图修改 AS_PATH 属性，可以通过 **set as-path prepend** 对路由属性进行追加，从而影响邻居选路。在使用 **set as-path prepend** 功能时，优先使用本地 AS 追加 AS_PATH，如果使用其它 AS，则必须足够重视，避免路由通告给该 AS 时遭到拒绝。

表 45-29 配置路由图修改 AS_PATH 属性

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-

步骤	命令	说明
进入 BGP IPv6 单播配置模式	address-family ipv6 unicast	-
配置路由图修改 AS_PATH 属性	neighbor { neighbor-address peer-group-name } route-map rmap-name in out	必选 缺省情况下, 不对任何邻居应用路由图

说明:

- 配置路由图修改 AS_PATH 属性时, 需要通过 **set as-path prepend** 命令对 AS_PATH 属性进行修改, 请参见策略工具-技术手册-**set as-path**。

配置 BGP 路由 NEXT-HOP 属性

在 BGP 向 IBGP 邻居通告路由时不会改变路由属性（包括下一跳属性）。下一跳属性通常用于 BGP 将 EBGP 邻居学习到的路由通告给 IBGP 邻居时, 通过 **neighbor next-hop-self** 命令修改向 BGP 邻居通告路由的下一跳属性采用本地 IPv6 地址。BGP 同时支持应用路由图修改下一跳属性。

1、配置 BGP 使用本地 IP 地址作为路由下一跳

表 45-30 配置 BGP 使用本地 IP 地址作为路由下一跳

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp autonomous-system	-
进入 BGP IPv6 单播配置模式	address-family ipv6 unicast	-

步骤	命令	说明
配置向邻居通告路由时采用本地 IP 地址作为下一跳	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } next-hop-self	必选 缺省情况下，向 EBGP 邻居通告的路由下一跳属性为本地 IPv6 地址，向 IBGP 通告的路由下一跳属性将不会被修改，维持原有属性值

说明：

- 配置 BGP 使用本地 IPv6 地址作为路由下一跳时，如果使用 **neighbor update-source** 配置了 TCP 会话的源地址，则将采用该源地址作为下一跳地址，否则，将选取通告设备的出接口地址作为本地 IPv6 地址。

2、配置路由图修改 NEXT-HOP 属性

BGP 支持配置路由图修改 NEXT-HOP 属性，可以通过 **set ipv6 next-hop** 修改下一跳属性。

表 45-31 配置路由图修改 NEXT-HOP 属性

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
进入 BGP IPv6 单播配置模式	address-family ipv6 unicast	-
配置路由图修改 NEXT-HOP 属性	neighbor { <i>neighbor-address</i> <i>peer-group-</i>	必选

步骤	命令	说明
	<code>name } route-map rmap-name in out</code>	缺省情况下, 不对任何邻居应用路由图

说明:

- 配置路由图修改 NEXT-HOP 属性时, 需要通过 **set ipv6 next-hop** 命令对 NEXT-HOP 属性进行修改, 请参见策略工具-技术手册-**set ipv6 next-hop**。

配置 BGP 路由团体属性

BGP 向邻居通告路由时支持配置发送团体属性, 可以在出入两个方向上对指定邻居应用路由图匹配团体属性。

团体属性用于标识一组路由, 以便对这组路由应用路由策略。团体属性具有标准与扩展两种形式, 标准团体属性 4 字节长, 具有 NO_EXPORT、LOCAL_AS、NO_ADVERTISE、INTERNET 等属性; 扩展团体属性 8 字节长, 具有路由目标 (Route Target, RT)、路由源 (Route Origin) 属性。

1、配置 BGP 向邻居通告路由团体属性

neighbor send-community 支持向邻居通告标准团体属性或扩展团体属性, 或者通告两者。

表 45-32 配置 BGP 向邻居通告路由团体属性

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp autonomous-system	-
进入 BGP IPv6 单播配置模式	address-family ipv6 unicast	-

配置向邻居通告路由团体属性	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } send-community [both extended standard]	必选 缺省情况下，不向任何邻居通告团体属性
---------------	--	--------------------------

说明：

- 在 VPNv6 地址簇下激活邻居后，将自动向邻居通告标准与扩展团体属性。

2、配置路由图修改路由团体属性

BGP 支持配置路由图修改路由团体属性，可以通过 **set communtiy** 修改团体属性。

表 45-33 配置路由图修改路由团体属性

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
进入 BGP IPv6 单播配置模式	address-family ipv6 unicast	-
配置路由图修改 BGP 路由团体属性	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } route-map <i>rtmap-name</i> in out	必选 缺省情况下，不对任何邻居应用路由图

说明：

- 配置路由图修改路由团体属性时，需要通过 **set communitiy** 命令对团体属性进行修改，请参见策略工具-技术手册-**set communitiy**。

45.2.5 配置 IPv6 BGP 网络优化 -E -A

配置条件

在配置 BGP 网络优化之前，首先完成以下任务：

- 启用 BGP 协议。
- 配置 IPv6 BGP 邻居并使会话建连成功。

配置 BGP 邻居保活时间

在 BGP 会话成功建立之后，邻居之间将定时发送保活（Keepalive）消息维持 BGP 会话关系，如果在会话保持时间（Holdtime）内未收到邻居的保活消息或者路由更新报文（Update），BGP 会话就会超时断开。会话保活时间不会大于保持时间的三分之一。

表 45-34 配置 BGP 邻居保活时间

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
配置全局 BGP 保活时间与保持时间	timers bgp <i>keepalive-interval holdtime-interval</i>	可选
配置 BGP 邻居或对等体组的保活时间与保持时间	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } timers { <i>keepalive-interval holdtime-interval</i> connect <i>connect-interval</i> }	缺省情况下，保活定时器时间间隔为 60 秒，保持定时器时间间隔为 180 秒，会话重连定时器时间间隔为 120 秒

说明：

- 对指定邻居配置的保活时间与保持时间优先于全局 BGP 保活时间与保持时间。
- 邻居协商后将采用保持时间的最小者作为 BGP 会话的保持时间。
- 配置保活时间与保持时间同时为零时将取消邻居保活/保持功能。
- 保活时间间隔大于保持时间三分之一时，BGP 会话将采用保持时间的三分之一发送保活报文。

配置 BGP 路由检测时间

BGP 主要完成以 AS 为单位的寻路过程，AS 内部由 IGP 完成寻路，所以 BGP 路由通常依赖于 IGP 路由。在 BGP 依赖的 IGP 路由的下一跳或出接口发生变化后，BGP 通过定时检测 IGP 路由来更新 BGP 路由。在检测周期内同时完成对本地 BGP 路由更新等事务。

表 45-35 配置 BGP 路由检测时间

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
配置 BGP 路由检测时间	bgp scan-time <i>time</i>	可选 缺省情况下，BGP 路由检测时间为 60 秒

说明：

- 配置 BGP 路由检测时间过小将使 BGP 频繁检测路由，影响设备性能。

配置 EBGP 邻居快速断连

在 BGP 会话成功建立之后，邻居之间将相互定时发送保活（Keepalive）消息维持 BGP 会话关系，如果在会话保持时间（Holdtime）内未收到邻居的保活消息或者路由更新报文（Update），BGP 会话就会超时断开。可以通过配置直连 EBGP 邻居在相连接口 down 时，立刻断开 BGP 连接，而不需要等到 BGP 保活超时。取消 EBGP 邻居快速断连时，EBGP 会话将不会响应接口 down 事件，BGP 会话连接通过超时断开。

表 45-36 配置 EBGP 邻居快速断连

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
配置 EBGP 邻居快速断连	bgp fast-external-failover	可选 缺省情况下，已启用 EBGP 响应直连接口下线事件的快速处理能力

配置 BGP 路由抑制功能

网络中频繁震荡的路由会造成网络的不稳定，BGP 通过配置路由衰减抑制这类路由，减少震荡路由对网络的影响。

频繁震荡的路由将会分配增加惩罚值，当惩罚值超过抑制门限后，路由将不会被通告给邻居，惩罚值不能超过最大抑制时间。当路由在半衰期时间内没有发生震荡时，惩罚值将会减半，直到该值少于重用门限后，路由才会被重新通告给邻居。

- 半衰期：路由惩罚值减半的时间。
- 重用门限：路由恢复使用的门限值。
- 抑制门限：路由被抑制的门限值。

- 最大抑制时间：路由被抑制的最长时间。

表 45-37 配置 BGP 路由抑制功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
进入 BGP IPv6 单播配置模式	address-family ipv6 unicast	-
配置 BGP 路由衰减周期	bgp dampening [<i>reach-half-life</i> [<i>reuse-value suppress-value max-suppress-time</i> [<i>unreach-half-life</i>]]] route-map <i>rtmap-name</i>]	必选 缺省情况下，未启用路由抑制功能，启用后的缺省路由抑制半衰期为 15 分钟，路由重用门限为 750，路由抑制门限为 2000，路由最大抑制时间为 60 分钟，路由惩罚的不可达半衰期为 15 分钟

说明：

- 路由震荡不仅有路由的增删，还包括路由属性的变化，如下一跳、MED 属性等。

配置 BGP 邻居刷新能力

当 BGP 邻居应用的路由策略或者选路策略发生变化时，需要重新对路由表进行刷新，一种方式是通过复位 BGP 连接使会话重新开始达到复位目的，这种方式会造成 BGP 路由震荡而影响业务运行。另一

种更优雅的方式是配置本端 BGP 设备支持路由刷新能力，在其邻居需要对路由进行复位时，通过向本端通告 Route-Refresh 消息，本端收到 Route-Refresh 消息后会重新将路由发给该邻居，达到了不断开 BGP 会话的情况下就对路由表进行了动态刷新。

表 45-38 配置 BGP 邻居刷新能力

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
配置启用邻居刷新能力	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } capability route-refresh	可选 缺省情况下，已启用向邻居通告支持路由刷新能力

配置 BGP 邻居软重置能力

当 BGP 邻居应用的路由策略或者选路策略发生变化时，需要重新对路由表进行刷新，一种方式是通过复位 BGP 连接使会话重新开始达到复位目的，这种方式会造成 BGP 路由震荡而影响业务运行。另一种更优雅的方式是配置本端 BGP 设备支持路由刷新能力，还有一种方式是通过使能本端 BGP 设备的软重置能力。缺省情况下，BGP 设备保留各个邻居的路由信息，在使能其邻居软重置能力后，再次对本地保留邻居的路由进行刷新，此时不会断开 BGP 会话。

表 45-39 配置 BGP 邻居软重置能力

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-

步骤	命令	说明
进入 BGP IPv6 单播配置模式	address-family ipv6 unicast	-
配置使能邻居软重置能力	neighbor { neighbor-address peer-group-name } soft-reconfiguration inbound	必选 缺省情况下，未启用邻居软重置功能

配置 BGP 邻居 ORF 能力

BGP 通过丰富的路由属性完成对路由的精确控制，通常在出入两个方向上应用路由策略达到该目的，这种方式是 BGP 本地的行为。BGP 同时也支持 ORF（Outbound Route Filtering，输出路由过滤）能力，通过 Route-refresh 报文将本地入口策略通告给邻居，由邻居向自己通告路由时应用该策略，可以大大减少 BGP 邻居之间路由更新报文的交互。

ORF 能力协商成功需要以下条件：

- 邻居双方都需要启用 ORF 能力；
- ORF send 与 ORF receive 必须配对，即某一方采用 ORF send，另一方必须是 ORF both 或 ORF receive；某一方采用 ORF receive，另一方必须是 ORF send 或 ORF both；
- 采用 ORF send 一方需要配置在入方向上应用前缀列表。

表 45-40 配置 BGP 邻居 ORF 能力

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-

步骤	命令	说明
进入 BGP IPv6 单播配置模式	address-family ipv6 unicast	-
配置邻居在入方向上应用前缀列表	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } prefix-list <i>prefix-list-name</i> in	必选 缺省情况下，不对任何 BGP 邻居应用前缀列表
配置邻居支持 ORF 能力	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } capability orf prefix-list { both receive send }	必选 缺省情况下，未开启邻居通告支持 ORF 能力

45.2.6 配置 IPv6 BGP 大型网络 **-E -A**

配置条件

在配置 BGP 大型网络之前，首先完成以下任务：

- 启用 BGP 协议；
- 配置 IPv6 BGP 邻居并使会话建连成功。

配置 BGP 对等体组

BGP 对等体组是具有相同配置策略的 BGP 邻居集合，任何对对等体组的配置都会同时作用到每个对等体成员，通过配置 BGP 对等体组便于对邻居进行集中管理与维护。

表 45-41 配置 BGP 对等体组

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
进入 BGP IPv6 单播配置模式	address-family ipv6 unicast	-
创建 BGP 对等体组	neighbor <i>peer-group-name</i> peer-group	必选
配置邻居加入对等体组	neighbor <i>neighbor-address</i> peer-group <i>peer-group-name</i>	缺省情况下，未配置对等体组，且邻居未加入任何对等体组

说明：

- 对等体组的配置将同时作用到所有对等体组成员。
- 邻居加入对等体组后原有邻居与对等体组相同的配置将会被删除。
- 配置对等体组出方向路由策略或入方向上路由策略时，在路由策略变化后，将不能对已加入对等体组的邻居生效，需要重置对等体组后，才能将变化后的路由策略作用到对等体组成员。

配置 BGP 路由反射器

在大型 BGP 组网环境中要求 IBGP 邻居全网连接，即每一个 BGP 与其它所有 IBGP 邻居建立连接关系，这样在 N 个 BGP 邻居的组网环境中 BGP 连接数为 $N*(N-1)/2$ 条，连接数越多，路由通告量越大。BGP 路由反射器是一种减少网络连接数的方法，它将若干个 IBGP 划分为一个群体，并指定某个 BGP 作为反射器 (RR)，其它 BGP 作为客户，非群体中的 BGP 作为非客户。客户只与 RR 建立对等关系，而不与其它 BGP 建立对等关系，从而降低了必要的 IBGP 连接数量，连接数降至 N-1 条。

BGP 路由反射器反射路由原则：

- 从非客户 IBGP 邻居学习到的路由，只反射给客户；
- 从客户学习到的路由，将反射给除发起该路由的客户之外的所有客户以及非客户；

- 从 EBGP 邻居学习到的路由，将反射给所有客户和非客户。

表 45-42 配置 BGP 路由反射器

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
配置反射器簇 ID	bgp cluster-id { <i>cluster-id-in-ip</i> <i>cluster-id-in-num</i> }	必选 缺省情况下，路由反射器簇 ID 使用设备 Router ID 值
配置邻居为反射器客户	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } route-reflector-client	必选 缺省情况下，未指定任何邻居作为反射器客户
配置 BGP 客户端之间路由反射功能	bgp client-to-client reflection	可选 缺省情况下，已启用 BGP 路由反射器客户端之间路由反射功能

 说明：

- 反射器簇 ID 用于标识同一个反射器区域，该反射器区域中可以存在多个反射器，同时，这些反射器具有相同的反射簇 ID。

配置 BGP 联盟

在大型 BGP 组网环境中要求 IBGP 邻居全网连接，即每一个 BGP 与其它所有 IBGP 邻居建立连接关系，这样在 N 个 BGP 邻居的组网环境中 BGP 连接数为 $N*(N-1)/2$ 条，连接数越多，路由通告量越

大。BGP 联盟是另外一种减少网络连接数的方法，它采用分而治之策略，将 AS 划分为若干个子 AS 区域，每个 AS 区域形成联盟，各联盟内部通过 IBGP 形成全连接，联盟子 AS 区域之间通过 EBGP 连接，有效减少了 BGP 连接数目。

配置 BGP 联盟时，需要为每一个联盟分配一个联盟 ID，并指定该联盟成员。与路由反射器不同，在路由反射器条件下，只要求路由反射器支持路由反射，而联盟则要求所有成员都要支持联盟功能。

表 45-43 配置 BGP 联盟

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
创建 BGP 联盟 ID	bgp confederation identifier <i>as-number</i>	必选 缺省情况下，未配置联盟自治系统号
配置联盟成员	bgp confederation peers <i>as-number-list</i>	必选 缺省情况下，未配置联盟的子自治系统号

说明：

- 联盟 ID 用于标识联盟子自治系统，联盟成员被划分到该子自治系统中。

45.2.7 配置 IPv6 BGP GR -E -A

GR (Graceful Restart, 优雅重启) 用于在设备主备切换过程中，保持本设备和邻居设备转发层面路由信息不变，转发不受影响；当切换设备重新运行后，两台设备协议层面同步路由信息并更新转发层，达到设备切换过程中数据转发不间断的目的。

GR 过程角色：

- GR Restarter：进行协议优雅重启的设备。
- GR Helper：协助协议优雅重启的设备。
- GR Time：GR-Restarter 重启的最大时间，GR Helper 只在该时间内维持路由稳定。

双主控设备可以充当 GR Restarter 和 GR Helper，而集中式设备只能充当 GR Helper，协助 Restarter 端完成 GR。在 GR Restarter 进行 GR 时，GR Helper 维持其路由直到 GR Time 超时并协助其完成 GR 后，进行路由信息同步，在此期间，网络路由和报文转发维持 GR 前的状态，有效保证了网络稳定。

BGP GR 关系在邻居建连时通过 OPEN 报文协商建立，在 GR Restarter 邻居重启时，BGP 会话会断开，但是从该邻居学习的路由不会被删除，仍然在 IP 路由表中正常转发，这些路由只在 BGP 路由表中置上 Stale 标记，在 GR 完成或者超时后将会被更新。

GR Restarter 需要在最大允许时间内 (**restart-time**) 完成与 GR Helper 的建连，否则 GR Helper 将会消除保持的 GR 路由，解除 GR 过程。在邻居重建完成后，GR Helper 需要接收来自 GR Restarter 且带有 End-Of-RIB 标记的更新报文才能成功完成 GR 过程，否则未被更新的 GR 路由将会在最大保持时间后 (**stalepath-time**) 删除，GR 关系将解除。

配置条件

在配置 BGP GR 之前，首先完成以下任务：

- 启用 BGP 协议。
- 配置 IPv6 BGP 邻居并使会话建连成功。

配置 BGP GR Restarter

表 45-44 配置 BGP GR Restarter

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-

步骤	命令	说明
启用 BGP GR 能力	bgp graceful-restart [restart-time <i>time</i> stalepath-time <i>time</i>]	必选 缺省情况下，BGP 设备未启用 GR 能力，启用 GR 后的缺省邻居重建会话的最大允许时间为 120 秒，GR 路由最大保持时间为 360 秒
进入 BGP IPv6 单播配置模式	address-family ipv6 unicast	-
配置向邻居通告 GR-Restarter 能力	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } capability graceful-restart	必选 缺省情况下，不向邻居通告 GR Restarter 能力

配置 BGP GR Helper

表 45-45 配置 BGP GR Helper

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
启用 BGP GR 能力	bgp graceful-restart [restart-time <i>time</i> stalepath-time <i>time</i>]	必选 缺省情况下，BGP 设备未启用 GR 能力，启用 GR 后的缺省邻居重建会话的最大允许时间为

步骤	命令	说明
		120 秒，GR 路由最大保持时间为 360 秒

45.2.8 配置 IPv6 BGP 与 BFD 联动

-E -A

通常在 BGP 邻居之间会运行有其它中间设备，在这些中间设备出现故障时，BGP 会话在保持时间内仍然正常，无法及时响应中间设备链路故障。BFD(Bidirectional Forwarding Detection，双向转发检测)提供一种快速检测两台设备之间线路状态的方法。当 BGP 设备间启动 BFD 检测后，若设备之间线路发生故障，BFD 会快速检测到线路故障，并通知 BGP，触发 BGP 快速断开会话，并切换到备份线路，达到路由快速切换的目的。

配置条件

在配置 BGP 与 BFD 联动之前，首先完成以下任务：

- 启用 BGP 协议。
- 配置 IPv6 BGP 邻居并使会话建连成功。

配置 EBGP 与 BFD 联动

EBGP 与 BFD 联动基于单跳 BFD 会话，需要在接口模式下配置 BFD 会话参数。

表 45-46 配置 EBGP 与 BFD 联动

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
进入 BGP IPv6 单播配置模式	address-family ipv6 unicast	-

步骤	命令	说明
配置 EBGP 与 BFD 联动	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } fall-over bfd [single-hop]	必选 缺省情况下, 未启用邻居 BFD 功能
退出 BGP IPv6 单播配置模式	exit-address-family	-
退出 BGP 配置模式	exit	-
进入接口配置模式	interface <i>interface-name</i>	-
配置 BFD 会话最小接收间隔时间	bfd min-receive-interval <i>milliseconds</i>	可选 缺省情况下, BFD 会话最小接收间隔时间为 1000 秒
配置 BFD 会话最小发送间隔时间	bfd min-transmit-interval <i>milliseconds</i>	可选 缺省情况下, BFD 会话最小发送间隔时间为 1000 秒
配置 BFD 会话检测超时倍数	bfd multiplier <i>number</i>	可选 缺省情况下, BFD 会话检测超时倍数为 5

说明:

- BFD 相关配置, 请参见可靠性技术-BFD 命令与 BFD 配置相关章节。

配置 IBGP 与 BFD 联动

IBGP 与 BFD 联动基于多跳 BFD 会话，需要在 BGP 模式下配置 BFD 会话参数。

表 45-47 配置 IBGP 与 BFD 联动

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 BGP 配置模式	router bgp <i>autonomous-system</i>	-
进入 BGP IPv6 单播配置模式	address-family ipv6 unicast	-
配置 IBGP 与 BFD 联动	neighbor { <i>neighbor-address</i> <i>peer-group-name</i> } fall-over bfd [single-hop]	必选 缺省情况下，未启用邻居 BFD 功能
配置 BFD 会话最小接收间隔时间	bfd min-receive-interval <i>milliseconds</i>	可选 缺省情况下，BFD 会话最小接收间隔时间为 1000 秒
配置 BFD 会话最小发送间隔时间	bfd min-transmit-interval <i>milliseconds</i>	可选 缺省情况下，BFD 会话最小发送间隔时间为 1000 秒
配置 BFD 会话检测超时倍数	bfd multiplier <i>number</i>	可选 缺省情况下，BFD 会话检测超时倍数为 5

表 45-48 BGP 监控与维护

命令	说明
clear bgp ipv6 { * <i>as-number</i> / peer-group <i>peer-group-name</i> external <i>neighbor-address</i> } [vrf <i>vrf-name</i>]	重置 BGP 邻居
clear bgp [ipv6 unicast] dampening [<i>ipv6-address</i> <i>ipv6-address/mask-length</i>]	清除抑制路由
clear bgp [ipv6 unicast] flap-statistics [<i>ipv6-address</i> <i>ipv6-address/mask-length</i>]	清除抖动统计信息
clear bgp [ipv6] { * <i>as-number</i> peer-group <i>peer-group-name</i> external <i>neighbor-address</i> } [vrf <i>vrf-name</i>] { [soft] [in out] }	软重置邻居
clear bgp [ipv6] { * <i>neighbor-address</i> <i>as-number</i> / peer-group <i>peer-group-name</i> external } [vrf <i>vrf-name</i>] in prefix-filter	通告 ORF 给邻居
show bgp { ipv6 unicast vpn v6 unicast vrf <i>vrf-name</i> } [<i>ipv6-address</i> <i>ipv6-address/mask-length</i>]	显示 BGP 相应地址簇下的路由信息

命令	说明
show ip bgp attribute-info	显示 BGP 公共的路由属性信息
show bgp ipv6 unicast community [<i>community-number</i> / <i>aa:nn</i> / exact-match / local-AS / no-advertise / no-export]	显示匹配指定团体属性的路由信息
show bgp ipv6 unicast community-list <i>community-list-name</i>	显示路由信息应用的团体属性列表
show bgp { ipv6 unicast vpn6 unicast vrf <i>vrf-name</i> } dampening { dampened-paths flap-statistics parameters }	显示路由衰减的详细信息
show bgp ipv6 unicast filter-list <i>filter-list-name</i> [exact-match]	显示 AS_PATH 访问列表匹配的路由
show bgp ipv6 unicast inconsistent-as	显示 AS_PATH 冲突的路由
show bgp { ipv6 unicast vpn6 unicast vrf <i>vrf-name</i> } neighbors [<i>ipv6-address</i>]	显示 BGP 的邻居详细信息
show bgp ipv6 unicast prefix-list <i>prefix-list-name</i>	显示前缀列表匹配的路由

命令	说明
show bgp ipv6 unicast quote- regexp <i>as-path-list-name</i>	显示 AS_PATH 列表匹配的路由
show bgp ipv6 unicast regexp <i>as-path-list-name</i>	显示 AS_PATH 列表匹配的路由
show bgp ipv6 unicast route- map <i>rtmap-name</i>	显示路由图匹配的对路由
show ip bgp scan	显示 BGP 的扫描信息
show bgp {ipv6 unicast vpnv6 vrf vrf-name } summary	显示 BGP 的邻居汇总信息

45.3 IPv6 BGP 典型配置举例

45.3.1 配置 IPv6 BGP 基本功能 **-E -A**

网络需求

- Device1 和 Device2 间建立 EBGP 邻居，Device2 和 Device3 间建立 IBGP 邻居。
- Device1 学习到 Device3 的接口直连路由 2001:4::/64，Device3 学习到 Device1 的接口直连路由 2001:1::/64。

网络拓扑

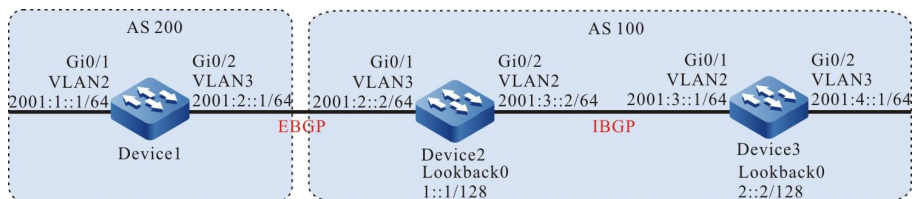


图 45-1 配置 IPv6 BGP 基本功能组网图

配置步骤

步骤 1: 配置各接口的 IPv6 全球单播地址。(略)

步骤 2: 配置 OSPFv3, 使设备间 Loopback 接口路由互相可达。

#配置 Device2。

Device2#configure terminal

```
Device2(config)#ipv6 router ospf 100
Device2(config-ospf6)#router-id 2.2.2.2
Device2(config-ospf6)#exit
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#ipv6 router ospf 100 area 0
Device2(config-if-vlan2)#exit
Device2(config)#interface loopback 0
Device2(config-if-loopback0)#ipv6 router ospf 100 area 0
Device2(config-if-loopback0)#exit
```

#配置 Device3。

Device3#configure terminal

```
Device3(config)#ipv6 router ospf 100
Device3(config-ospf6)#router-id 3.3.3.3
Device3(config-ospf6)#exit
Device3(config)#interface vlan 2
Device3(config-if-vlan2)#ipv6 router ospf 100 area 0
Device3(config-if-vlan2)#exit
Device3(config)#interface loopback 0
Device3(config-if-loopback0)#ipv6 router ospf 100 area 0
Device3(config-if-loopback0)#exit
```

#查看 Device2 的路由表。

```
Device2#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
```

```
L  ::1/128 [0/0]
   via ::, 1w1d:23:51:37, lo0
LC 1::1/128 [0/0]
   via ::, 00:09:34, loopback0
O  2::2/128 [110/2]
   via fe80::201:7aff:fec0:525a, 00:05:29, vlan2
C  2001:2::/64 [0/0]
   via ::, 00:09:41, vlan3
L  2001:2::2/128 [0/0]
   via ::, 00:09:39, vlan3
C  2001:3::/64 [0/0]
   via ::, 00:08:55, vlan2
L  2001:3::2/128 [0/0]
   via ::, 00:08:53, vlan2
```

#查看 Device3 的路由表。

配置手册

单播路由

```
Device3#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 1w5d:18:34:53, lo0
O 1::1/128 [110/2]
  via fe80::201:7aff:fe5e:6d2e, 00:29:59, vlan2
LC 2::2/128 [0/0]
  via ::, 00:32:36, loopback0
C 2001:3::/64 [0/0]
  via ::, 00:32:59, vlan2
L 2001:3::1/128 [0/0]
  via ::, 00:32:58, vlan2
C 2001:4::/64 [0/0]
  via ::, 00:32:44, vlan3
L 2001:4::1/128 [0/0]
  via ::, 00:32:43, vlan3
```

可以看到 Device2 和 Device3 通过运行 OSPFv3 协议均学习到了对端环回口的路由，为下一步 Device2 和 Device3 通过环回口建立 IBGP 邻居做准备。

步骤 3: 配置 IPv6 BGP 基本功能。

#配置 Device1。

配置与 Device2 建立直连 EBGP 对等体，通过 network 的方式将 2001:1::/64 引入到 BGP 中。

```
Device1#configure terminal
Device1(config)#router bgp 200
Device1(config-bgp)#bgp router-id 1.1.1.1
Device1(config-bgp)#address-family ipv6
Device1(config-bgp-af)#neighbor 2001:2::2 remote-as 100
Device1(config-bgp-af)#network 2001:1::/64
Device1(config-bgp-af)#exit-address-family
Device1(config-bgp)#exit
```

#配置 Device2。

配置与 Device1 建立直连 EBGP 对等体，通过 Loopback0 与 Device3 建立非直连 IBGP 对等体关系，同时将通告路由的下一跳设置为自身。

```
Device2(config)#router bgp 100
Device2(config-bgp)#bgp router-id 2.2.2.2
Device2(config-bgp)#address-family ipv6
Device2(config-bgp-af)#neighbor 2001:2::1 remote-as 200
Device2(config-bgp-af)#neighbor 2::2 remote-as 100
Device2(config-bgp-af)#neighbor 2::2 next-hop-self
Device2(config-bgp-af)#exit-address-family
Device2(config-bgp)#neighbor 2::2 update-source loopback 0
Device2(config-bgp)#exit
```

#配置 Device3。

通过 Loopback0 与 Device2 建立非直连 IBGP 对等体关系，通过 network 的方式将 2001:4::/64 引入到 BGP 中。


```
Device3(config)#router bgp 100
Device3(config-bgp)#bgp router-id 3.3.3.3
Device3(config-bgp)#address-family ipv6
Device3(config-bgp-af)#neighbor 1::1 remote-as 100
Device3(config-bgp-af)#network 2001:4::/64
Device3(config-bgp-af)#exit-address-family
Device3(config-bgp)#neighbor 1::1 update-source loopback 0
Device3(config-bgp)#exit
```

说明:

- 为了防止路由动荡，所以 IBGP 邻居均是通过环回口建立，需要 OSPFv3 在 IBGP 邻居间同步环回口的路由信息。
-

步骤 4: 检验结果。

#查看 Device2 上 IPv6 BGP 邻居状态。

```
Device2#show bgp ipv6 unicast summary
BGP router identifier 2.2.2.2, local AS number 100
BGP table version is 4
2 BGP AS-PATH entries
0 BGP community entries

Neighbor    V  AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down State/PfxRcd
2::2        4  100    8     6    3    0  0 00:04:12    1
2001:2::1   4  200   15    15    3    0  0 00:11:17    1

Total number of neighbors 2
```

从 State/PfxRcd 这列的内容显示为数字（从邻居接收路由前缀的数目）可以看出 Device2 与 Device1、Device3 成功建立 IPv6 BGP 邻居

#查看 Device1 的路由表。

```
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 1w2d:00:42:57, lo0
C 2001:1::/64 [0/0]
  via ::, 00:02:59, vlan2
L 2001:1::1/128 [0/0]
  via ::, 00:02:56, vlan2
C 2001:2::/64 [0/0]
  via ::, 00:52:17, vlan3
L 2001:2::1/128 [0/0]
  via ::, 00:52:16, vlan3
B 2001:4::/64 [20/0]
  via 2001:2::2, 00:06:13, vlan3
```

#查看 Device2 的路由表。

```
Device2#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 1w2d:00:34:53, lo0
LC 1::1/128 [0/0]
  via ::, 00:52:49, loopback0
O 2::2/128 [110/2]
  via fe80::201:7aff:fec0:525a, 00:48:45, vlan2
B 2001:1::/64 [20/0]
  via 2001:2::1, 00:03:18, vlan3
C 2001:2::/64 [0/0]
  via ::, 00:52:57, vlan3
L 2001:2::2/128 [0/0]
  via ::, 00:52:55, vlan3
C 2001:3::/64 [0/0]
  via ::, 00:52:10, vlan2
L 2001:3::2/128 [0/0]
  via ::, 00:52:09, lo0
B 2001:4::/64 [200/0]
  via 2::2, 00:07:27, vlan2
```

#查看 Device3 的路由表。

```
Device3#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 1w5d:18:54:38, lo0
O 1::1/128 [110/2]
  via fe80::201:7aff:fe5e:6d2e, 00:49:44, vlan2
LC 2::2/128 [0/0]
  via ::, 00:52:21, loopback0
B 2001:1::/64 [200/0]
  via 1::1, 00:03:54, vlan2
C 2001:3::/64 [0/0]
  via ::, 00:52:44, vlan2
L 2001:3::1/128 [0/0]
  via ::, 00:52:43, vlan2
C 2001:4::/64 [0/0]
  via ::, 00:52:29, vlan3
L 2001:4::1/128 [0/0]
  via ::, 00:52:28, vlan3
```

可以看到 Device1 学习到了 Device3 的接口直连路由 2001:4::/64，Device3 学习到 Device1 的接口直连路由 2001:1::/64。

45.3.2 配置 IPv6 BGP 路由重分发

-E -A

网络需求

- Device3 与 Device2 间建立 OSPFv3 邻居，并向 Device2 通告接口直连路由

2001:3::/64。

- Device1 和 Device2 间建立 EBGP 邻居，Device2 将学习到的 OSPFv3 路由重分发到 IPv6 BGP 中并通告给 Device1。

网络拓扑

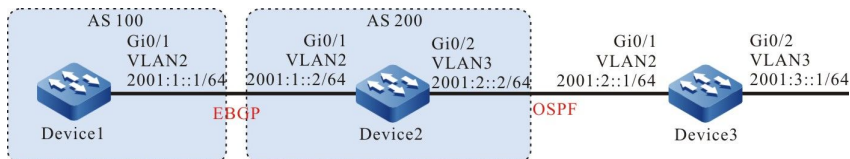


图 45-2 配置 IPv6 BGP 路由重分发组网图

配置步骤

步骤 1： 配置各接口的 IPv6 全球单播地址。（略）

步骤 2： 配置 OSPFv3，使 Device2 学习到 Device3 的直连接口路由 2001:3::/64。

#配置 Device2。

Device2#configure terminal

```
Device2(config)#ipv6 router ospf 100
Device2(config-ospf6)#router-id 2.2.2.2
Device2(config-ospf6)#exit
Device2(config)#interface vlan 3
Device2(config-if-vlan3)#ipv6 router ospf 100 area 0
Device2(config-if-vlan3)#exit
```

#配置 Device3。

Device3#configure terminal

```
Device3(config)#ipv6 router ospf 100
Device3(config-ospf6)#router-id 3.3.3.3
Device3(config-ospf6)#exit
Device3(config)#interface vlan 2
Device3(config-if-vlan2)#ipv6 router ospf 100 area 0
Device3(config-if-vlan2)#exit
Device3(config)#interface vlan 3
Device3(config-if-vlan3)#ipv6 router ospf 100 area 0
Device3(config-if-vlan3)#exit
```

#查看 Device2 的路由表。

```
Device2#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 1w2d:01:10:38, lo0
C 2001:1::/64 [0/0]
```

单播路由

```
via ::, 00:06:25, vlan2
L 2001:1::2/128 [0/0]
via ::, 00:06:24, vlan2
C 2001:2::/64 [0/0]
via ::, 00:05:46, vlan3
L 2001:2::2/128 [0/0]
via ::, 00:05:43, vlan3
O 2001:3::/64 [110/2]
via fe80::201:7aff:fec0:525a, 00:02:41, vlan3
```

从路由表中可以看出 Device2 学习到了 Device3 通告的 OSPFv3 路由 2001:3::/64。

步骤 3: 配置 IPv6 BGP 基本功能。

#配置 Device1。

Device1#configure terminal

```
Device1(config)#router bgp 100
Device1(config-bgp)#bgp router-id 1.1.1.1
Device1(config-bgp)#address-family ipv6
Device1(config-bgp-af)#neighbor 2001:1::2 remote-as 200
Device1(config-bgp-af)#exit-address-family
Device1(config-bgp-af)#exit
```

#配置 Device2。

```
Device2(config)#router bgp 200
Device2(config-bgp)#bgp router-id 2.2.2.2
Device2(config-bgp)#address-family ipv6
Device2(config-bgp-af)#neighbor 2001:1::1 remote-as 100
Device2(config-bgp-af)#exit-address-family
Device2(config-bgp-af)#exit
```

#查看 Device2 上 IPv6 BGP 邻居状态。

```
Device2#show bgp ipv6 unicast summary
BGP router identifier 2.2.2.2, local AS number 200
BGP table version is 1
1 BGP AS-PATH entries
0 BGP community entries

Neighbor    V  AS MsgRcvd MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
2001:1::1   4  100    2    2    1    0    0 00:00:50    0

Total number of neighbors 1
```

可以看出 Device2 与 Device1 成功建立 IPv6 BGP 邻居。

步骤 4: 配置 IPv6 BGP 重分发 OSPFv3 路由。

#配置 Device2。

```
Device2(config)#router bgp 200
Device2(config-bgp)#address-family ipv6
Device2(config-bgp-af)#redistribute ospf 100
Device2(config-bgp-af)#exit-address-family
Device2(config-bgp-af)#exit
```

步骤 5: 检验结果。

#查看 Device2 的 IPv6 BGP 路由表。

```
Device2#show bgp ipv6 unicast
BGP table version is 2, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
                S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop        Metric   LocPrf Weight Path
[O]*> 2001:2::/64  ::              1       32768 ?
[O]*> 2001:3::/64  ::              2       32768 ?
```

可以看到 OSPFv3 路由已经被成功重分发到 IPv6 BGP 中。

#查看 Device1 的路由表。

```
Device1#show bgp ipv6 unicast
BGP table version is 3, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
                S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop        Metric   LocPrf Weight Path
[B]*> 2001:2::/64  2001:1::2       1         0 200 ?
[B]*> 2001:3::/64  2001:1::2       2         0 200 ?
```

可以看到 Device1 成功学习到路由 2001:2::/64 和 2001:3::/64。

说明:

- 在实际应用中，如果自治系统边界设备有 2 台及以上，建议不要直接在不同路由协议之间相互重分发路由，若必须配置时，需要在自治系统边界设备上配置过滤、汇总等路由控制策略，防止产生路由环路。
-

45.3.3 配置 IPv6 BGP 团体属性 **-E -A**

网络需求

- Device1 与 Device2 间建立 EBGP 邻居。
- Device1 通过 network 的方式将两条直连路由 2001:1::/64 和 2001:2::/64 引入到 BGP 中，通告给 Device2 时分别对两条路由设置不同的团体属性。
- Device2 接收 Device1 通告的路由时，在邻居入方向通过匹配团体属性，过滤路由

2001:1::/64, 而允许路由 2001:2::/64。

网络拓扑

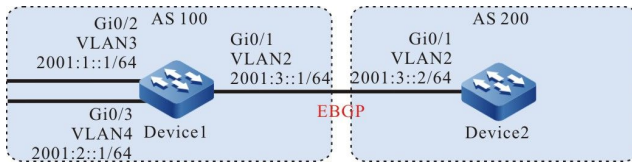


图 45-3 配置 IPv6 BGP 团体属性组网图

配置步骤

步骤 1: 配置各接口的 IPv6 全球单播地址。(略)

步骤 2: 配置 IPv6 BGP 基本功能。

#配置 Device1。

Device1#configure terminal

```
Device1(config)#router bgp 100
Device1(config-bgp)#bgp router-id 1.1.1.1
Device1(config-bgp)#address-family ipv6
Device1(config-bgp-af)#neighbor 2001:3::2 remote-as 200
Device1(config-bgp-af)#network 2001:1::/64
Device1(config-bgp-af)#network 2001:2::/64
Device1(config-bgp-af)#exit-address-family
Device1(config-bgp)#exit
```

#配置 Device2。

Device2#configure terminal

```
Device2(config)#router bgp 200
Device2(config-bgp)#bgp router-id 2.2.2.2
Device2(config-bgp)#address-family ipv6
Device2(config-bgp-af)#neighbor 2001:3::1 remote-as 100
Device2(config-bgp-af)#exit-address-family
Device2(config-bgp)#exit
```

#查看 Device1 上 IPv6 BGP 邻居状态。

```
Device1#show bgp ipv6 unicast summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 1
1 BGP AS-PATH entries
0 BGP community entries

Neighbor    V  AS MsgRcvd MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
2001:3::2  4  200    3    4    1    0  00:01:02    0

Total number of neighbors 1
```

可以看出 Device1 与 Device2 成功建立 IPv6 BGP 邻居。

#查看 Device2 上的路由表。

```
Device2#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 1w2d:05:45:34, lo0
B 2001:1::/64 [20/0]
  via 2001:3::1, 00:01:35, vlan2
B 2001:2::/64 [20/0]
  via 2001:3::1, 00:01:35, vlan2
C 2001:3::/64 [0/0]
  via ::, 00:04:09, vlan2
L 2001:3::2/128 [0/0]
  via ::, 00:04:08, vlan2
```

可以看到 Device2 成功学习到路由 2001:1::/64 和 2001:2::/64。

步骤 3: 配置访问列表和路由策略, 设置 IPv6 BGP 团体属性。

#配置 Device1。

```
Device1(config)#ipv6 access-list extended 7001
Device1(config-v6-list)#permit ipv6 2001:1::/64 any
Device1(config-v6-list)#exit
Device1(config)#ipv6 access-list extended 7002
Device1(config-v6-list)#permit ipv6 2001:2::/64 any
Device1(config-v6-list)#exit
Device1(config)#route-map CommunitySet 10
Device1(config-route-map)#match ipv6 address 7001
Device1(config-route-map)#set community 100:1
Device1(config-route-map)#exit
Device1(config)#route-map CommunitySet 20
Device1(config-route-map)#match ipv6 address 7002
Device1(config-route-map)#set community 100:2
Device1(config-route-map)#exit
```

通过配置访问列表和路由策略的方式对路由 2001:1::/64 和 2001:2::/64 分别设置不同的团体属性。

步骤 4: 配置 IPv6 BGP 关联路由策略。

#配置 Device1。

```
Device1(config)#router bgp 100
Device1(config-bgp)#address-family ipv6
Device1(config-bgp-af)#neighbor 2001:3::2 route-map CommunitySet out
Device1(config-bgp-af)#neighbor 2001:3::2 send-community
Device1(config-bgp-af)#exit-address-family
Device1(config-bgp)#exit
```

#查看 Device2 的 IPv6 BGP 路由表。

```
Device2#show bgp ipv6 unicast 2001:1::/64
BGP routing table entry for 2001:1::/64
Paths: (1 available, best #1, table Default-IP-Routing-Table)
Not advertised to any peer
100
```

```
2001:3::1 (metric 10) from 2001:3::1 (1.1.1.1)

Origin IGP, metric 0, localpref 100, valid, external, best
Community: 100:1
Last update: 00:00:24 ago
Device2#show bgp ipv6 unicast 2001:2::/64
BGP routing table entry for 2001:2::/64
Paths: (1 available, best #1, table Default-IP-Routing-Table)
Not advertised to any peer
100
2001:3::1 (metric 10) from 2001:3::1 (1.1.1.1)

Origin IGP, metric 0, localpref 100, valid, external, best
Community: 100:2
Last update: 00:00:30 ago
```

从 Device2 的 IPv6 BGP 路由表中看出路由 2001:1::/64 的团体属性被设置为 100:1，2001:2::/64 的团体属性被设置为 100:2。

步骤 5： 配置 IPv6 BGP 路由过滤。

#配置 Device2。

```
Device2(config)#ip community-list 1 permit 100:2
Device2(config)#route-map CommunityFilter
Device2(config-route-map)#match community 1
Device2(config-route-map)#exit
Device2(config)#router bgp 200
Device2(config-bgp)#address-family ipv6
Device2(config-bgp-af)#neighbor 2001:3::1 route-map CommunityFilter in
Device2(config-bgp-af)#exit-address-family
Device2(config-bgp)#exit
```

步骤 6： 检验结果。

#查看 Device2 的路由表。

```
Device2#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
via ::, 1w2d:05:58:57, lo0
B 2001:2::/64 [20/0]
via 2001:3::1, 00:00:05, vlan2
C 2001:3::/64 [0/0]
via ::, 00:17:32, vlan2
L 2001:3::2/128 [0/0]
via ::, 00:17:30, vlan2
```

从 Device2 的 IPv6 BGP 路由表中看出路由 2001:1::/64 在入方向被过滤，而路由 2001:2::/64 被允许。

说明:

- 在 IPv6 BGP 邻居上配置了路由策略后需要重置 IPv6 BGP 邻居才能生效。
- 需要配置 **send-community** 命令才能将团体属性通告给对等体。

45.3.4 配置 IPv6 BGP 路由反射器

-E -A

网络需求

- Device3 和 Device4 间建立 EBGP 邻居，Device4 向 Device3 通告路由 2001:4::/64。
- Device2 分别和 Device3、Device1 间建立 IBGP 邻居，在 Device2 上配置路由反射器，Device1 和 Device3 为客户端，使得 Device1 能学习到 Device4 通告的路由 2001:4::/64。

网络拓扑

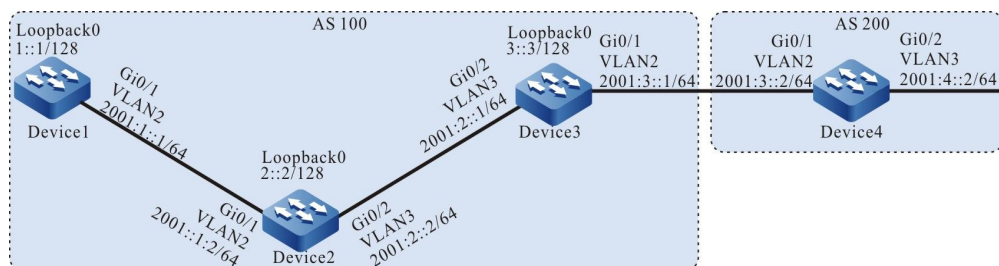


图 45-4 配置 IPv6 BGP 路由反射器组网图

配置步骤

步骤 1： 配置各接口的 IPv6 全球单播地址。（略）

步骤 2： 配置 OSPFv3，使设备间 Loopback 的接口路由互相可达。

#配置 Device1。

Device1#configure terminal

```
Device1(config)#ipv6 router ospf 100
Device1(config-ospf6)#router-id 1.1.1.1
Device1(config-ospf6)#exit
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#ipv6 router ospf 100 area 0
Device1(config-if-vlan2)#exit
```

配置手册

单播路由

```
Device1(config)#interface loopback 0
Device1(config-if-loopback0)#ipv6 router ospf 100 area 0
Device1(config-if-loopback0)#exit
```

#配置 Device2。

```
Device2#configure terminal
```

```
Device2(config)#ipv6 router ospf 100
Device2(config-ospf6)#router-id 2.2.2.2
Device2(config-ospf6)#exit
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#ipv6 router ospf 100 area 0
Device2(config-if-vlan2)#exit
Device2(config)#interface vlan 3
Device2(config-if-vlan3)#ipv6 router ospf 100 area 0
Device2(config-if-vlan3)#exit
Device2(config)#interface loopback 0
Device2(config-if-loopback0)#ipv6 router ospf 100 area 0
Device2(config-if-loopback0)#exit
```

#配置 Device3。

```
Device3#configure terminal
```

```
Device3(config)#ipv6 router ospf 100
Device3(config-ospf6)#router-id 3.3.3.3
Device3(config-ospf6)#exit
Device3(config)#interface vlan 3
Device3(config-if-vlan3)#ipv6 router ospf 100 area 0
Device3(config-if-vlan3)#exit
Device3(config)#interface loopback 0
Device3(config-if-loopback0)#ipv6 router ospf 100 area 0
Device3(config-if-loopback0)#exit
```

#查看 Device1 的路由表。

```
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
via ::, 1w2d:06:26:16, lo0
LC 1::1/128 [0/0]
via ::, 00:13:56, loopback0
O 2::2/128 [110/2]
via fe80::201:7aff:fec0:525a, 00:09:06, vlan2
O 3::3/128 [110/3]
via fe80::201:7aff:fec0:525a, 00:00:36, vlan2
C 2001:1::/64 [0/0]
via ::, 00:14:03, vlan2
L 2001:1::1/128 [0/0]
via ::, 00:14:02, vlan2
O 2001:2::/64 [110/2]
via fe80::201:7aff:fec0:525a, 00:09:06, vlan2
```

#查看 Device2 的路由表。

```
Device2#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
```

单播路由

```
via ::, 1w6d:00:46:09, lo0
O 1::1/128 [110/2]
  via fe80::201:7aff:fe5e:6d2e, 00:10:05, vlan2
LC 2::2/128 [0/0]
  via ::, 00:14:23, loopback0
O 3::3/128 [110/2]
  via fe80::201:7aff:fe62:bb80, 00:01:44, vlan3
C 2001:1::/64 [0/0]
  via ::, 00:14:48, vlan2
L 2001:1::2/128 [0/0]
  via ::, 00:14:47, vlan2
C 2001:2::/64 [0/0]
  via ::, 00:14:41, vlan3
L 2001:2::2/128 [0/0]
  via ::, 00:14:39, vlan3
```

#查看 Device3 的路由表。

```
Device3#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 1w2d:06:37:24, lo0
O 1::1/128 [110/3]
  via fe80::201:7aff:fec0:525b, 00:02:39, vlan3
O 2::2/128 [110/2]
  via fe80::201:7aff:fec0:525b, 00:02:39, vlan3
LC 3::3/128 [0/0]
  via ::, 00:14:45, loopback0
O 2001:1::/64 [110/2]
  via fe80::201:7aff:fec0:525b, 00:02:39, vlan3
C 2001:2::/64 [0/0]
  via ::, 00:15:03, vlan3
L 2001:2::1/128 [0/0]
  via ::, 00:15:02, vlan3
C 2001:3::/64 [0/0]
  via ::, 00:14:55, vlan2
L 2001:3::1/128 [0/0]
  via ::, 00:14:54, vlan2
```

可以看出 Device1、Device2、Device3 互相学习到对方环回口的接口路由。

步骤 3： 配置 IPv6 BGP 基本功能。

#配置 Device1。

```
Device1(config)#router bgp 100
Device1(config-bgp)#bgp router-id 1.1.1.1
Device1(config-bgp)#address-family ipv6
Device1(config-bgp-af)#neighbor 2::2 remote-as 100
Device1(config-bgp-af)#exit-address-family
Device1(config-bgp)#neighbor 2::2 update-source loopback 0
Device1(config-bgp)#exit
```

#配置 Device2。

```
Device2(config)#router bgp 100
Device2(config-bgp)#bgp router-id 2.2.2.2
Device2(config-bgp)#address-family ipv6
Device2(config-bgp-af)#neighbor 1::1 remote-as 100
Device2(config-bgp-af)#neighbor 3::3 remote-as 100
```

单播路由

```
Device2(config-bgp-af)#exit-address-family
Device2(config-bgp)#neighbor 1::1 update-source loopback 0
Device2(config-bgp)#neighbor 3::3 update-source loopback 0
Device2(config-bgp)#exit
```

#配置 Device3。

```
Device3(config)#router bgp 100
Device3(config-bgp)#bgp router-id 3.3.3.3
Device3(config-bgp)#address-family ipv6
Device3(config-bgp-af)#neighbor 2::2 remote-as 100
Device3(config-bgp-af)#neighbor 2::2 next-hop-self
Device3(config-bgp-af)#neighbor 2001:3::2 remote-as 200
Device3(config-bgp-af)#exit-address-family
Device3(config-bgp)#neighbor 2::2 update-source loopback 0
Device3(config-bgp)#exit
```

#配置 Device4。

Device4#configure terminal

```
Device4(config)#router bgp 200
Device4(config-bgp)#bgp router-id 4.4.4.4
Device4(config-bgp)#address-family ipv6
Device4(config-bgp-af)#neighbor 2001:3::1 remote-as 100
Device4(config-bgp-af)#network 2001:4::/64
Device4(config-bgp-af)#exit-address-family
Device4(config-bgp)#exit
```

#查看 Device2 上 IPv6 BGP 邻居状态。

```
Device2#show bgp ipv6 unicast summary
BGP router identifier 2.2.2.2, local AS number 100
BGP table version is 2
2 BGP AS-PATH entries
0 BGP community entries

Neighbor    V  AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
1::1       4 100    10    10     2  0  0 00:07:18  0
3::3       4 100    10     9     2  0  0 00:06:53  1

Total number of neighbors 2
```

#查看 Device4 上 IPv6 BGP 邻居状态。

```
Device4#show bgp ipv6 unicast summary
BGP router identifier 4.4.4.4, local AS number 200
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor    V  AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:3::1  4 100     3     4     2  0  0 00:01:45  0

Total number of neighbors 1
```

可以看出各设备间 IPv6 BGP 邻居建立成功。

#查看 Device3 的 IPv6 BGP 路由表。

```
Device3#show bgp ipv6 unicast
BGP table version is 3, local router ID is 3.3.3.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
```

单播路由

```
Network      Next Hop      Metric  LocPrf Weight Path
[B]*> 2001:4::/64    2001:3::2      0        0 200 i
```

#查看 Device2 的 IPv6 BGP 路由表。

```
Device2#show bgp ipv6 unicast
BGP table version is 7, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Network      Next Hop      Metric  LocPrf Weight Path
[B]*> i2001:4::/64    3::3          0    100  0 200 i
```

#查看 Device1 的 IPv6 BGP 路由表。

```
Device1#show bgp ipv6 unicast
```

从上面结果可以看出 Device2 和 Device3 均学到路由 2001:4::/64，而 Device2 未将该路由通告给 Device1。

步骤 4： 配置 IPv6 BGP 路由反射器。

#配置 Device2。

```
Device2(config)#router bgp 100
Device2(config-bgp)#address-family ipv6
Device2(config-bgp-af)#neighbor 1::1 route-reflector-client
Device2(config-bgp-af)#neighbor 3::3 route-reflector-client
Device2(config-bgp-af)#exit-address-family
Device2(config-bgp)#exit
```

在 Device2 上将 Device1 和 Device3 配置为路由反射器的客户端。

步骤 5： 检验结果。

#查看 Device1 的路由表。

```
Device1#show bgp ipv6 unicast
BGP table version is 2, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Network      Next Hop      Metric  LocPrf Weight Path
[B]*> i2001:4::/64    3::3          0    100  0 200 i
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L  ::1/128 [0/0]
   via ::, 1w2d:06:48:52, lo0
LC 1::1/128 [0/0]
   via ::, 00:36:32, loopback0
O  2::2/128 [110/2]
   via fe80::201:7aff:fec0:525a, 00:31:42, vlan2
O  3::3/128 [110/3]
   via fe80::201:7aff:fec0:525a, 00:23:12, vlan2
C  2001:1::/64 [0/0]
```

单播路由

```
via ::, 00:36:39, vlan2
L 2001:1::1/128 [0/0]
via ::, 00:36:38, vlan2
O 2001:2::/64 [110/2]
via fe80::201:7aff:fec0:525a, 00:31:42, vlan2
B 2001:4::/64 [200/0]
via 3::3, 00:01:16, vlan2
```

在 Device2 的 BGP 中将 Device1 与 Device3 配置为路由反射器的客户端，Device2 将路由 2001:4::/64 成功地反射给客户端 Device1。

说明：

- 将某个 IPv6 BGP 邻居配置为路由反射器的客户端时，该邻居会重置。

45.3.5 配置 IPv6 BGP 路由聚合 *-E -A*

网络需求

- Device1 与 Device3 建立 OSPFv3 邻居，Device3 向 Device1 通告两条路由 2002:1::/64 和 2002:2::/64。
- Device1 与 Device2 建立 EBGP 邻居。
- 在 Device1 上将 2002:1::/64 和 2002:2::/64 聚合成路由 2002::/30 通告给 Device2。

网络拓扑

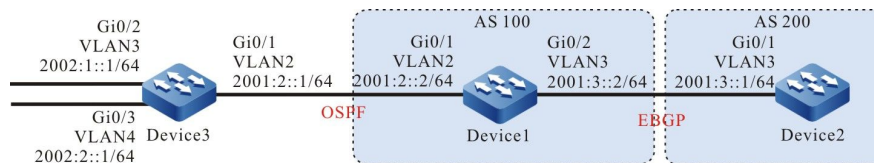


图 45-5 配置 IPv6 BGP 路由聚合组网图

配置步骤

- 步骤 1：配置各接口的 IPv6 全球单播地址。（略）
- 步骤 2：配置 OSPFv3，使 Device1 能够学习到 Device3 通告的两条路由 2002:1::/64 和 2002:2::/64。

单播路由

#配置 Device1。

Device1#configure terminal

```
Device1(config)#ipv6 router ospf 100
Device1(config-ospf6)#router-id 1.1.1.1
Device1(config-ospf6)#exit
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#ipv6 router ospf 100 area 0
Device1(config-if-vlan2)#exit
```

#配置 Device3。

Device3#configure terminal

```
Device3(config)#ipv6 router ospf 100
Device3(config-ospf6)#router-id 3.3.3.3
Device3(config-ospf6)#exit
Device3(config)#interface vlan 2
Device3(config-if-vlan2)#ipv6 router ospf 100 area 0
Device3(config-if-vlan2)#exit
Device3(config)#interface vlan 3
Device3(config-if-vlan3)#ipv6 router ospf 100 area 0
Device3(config-if-vlan3)#exit
Device3(config)#interface vlan 4
Device3(config-if-vlan4)#ipv6 router ospf 100 area 0
Device3(config-if-vlan4)#exit
```

#查看 Device1 的路由表。

```
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
```

```
L ::1/128 [0/0]
  via ::, 1w2d:07:35:38, lo0
C 2001:3::/64 [0/0]
  via ::, 00:01:11, vlan3
L 2001:3::2/128 [0/0]
  via ::, 00:01:10, vlan3
C 2001:2::/64 [0/0]
  via ::, 00:01:06, vlan2
L 2001:2::2/128 [0/0]
  via ::, 00:01:04, vlan2
O 2002:1::/64 [110/2]
  via fe80::201:7aff:fe62:bb7e, 00:01:54, vlan2
O 2002:2::/64 [110/2]
  via fe80::201:7aff:fe62:bb7e, 00:01:54, vlan2
```

可以看到 Device1 学到 Device3 发布的两条路由 2002:1:1::/64 和 2002:1:2::/64。

步骤 3: 配置 IPv6 BGP 基本功能。

#配置 Device1。

```
Device1(config)#router bgp 100
Device1(config-bgp)#bgp router-id 1.1.1.1
Device1(config-bgp)#address-family ipv6
Device1(config-bgp-af)#neighbor 2001:3::1 remote-as 200
Device1(config-bgp-af)#exit-address-family
Device1(config-bgp)#exit
```

单播路由

#配置 Device2。

Device2#configure terminal

```
Device2(config)#router bgp 200
Device2(config-bgp)#bgp router-id 2.2.2.2
Device2(config-bgp)#address-family ipv6
Device2(config-bgp-af)#neighbor 2001:3::2 remote-as 100
Device2(config-bgp-af)# xit-address-family
Device2(config-bgp)#exit
```

#查看 Device1 上 IPv6 BGP 邻居状态。

```
Device1#show bgp ipv6 unicast summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 1
1 BGP AS-PATH entries
0 BGP community entries

Neighbor      V  AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:3::1    4  200    3     3     1    0  0 00:01:16    0
```

Device1 与 Device2 成功建立 IPv6 BGP 邻居。

步骤 4: 配置 IPv6 BGP 路由聚合。

这里有两种方案可以完成网络需求:

方案一: 通过配置指向 null0 的 IPv6 静态路由并将其引入 BGP。

#配置 Device1。

```
Device1(config)#ipv6 route 2002::/30 null 0
Device1(config)#router bgp 100
Device1(config-bgp)#address-family ipv6
Device1(config-bgp-af)#network 2002::/30
Device1(config-bgp-af)#exit-address-family
Device1(config-bgp)#exit
```

检验结果

#查看 Device1 的 IPv6 BGP 路由表。

```
Device1#show bgp ipv6 unicast
BGP table version is 2, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Network        Next Hop      Metric  LocPrf  Weight Path
[B]*> 2002::/30  ::           0       32768  i
```

可以看出 Device1 的 IPv6 BGP 路由表中已经生成聚合路由 2002::/30。

#查看 Device2 的路由表。

```
Device2#show bgp ipv6 unicast
BGP table version is 2, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
```


单播路由

```
Origin codes: i - IGP, e - EGP, ? - incomplete
Network      Next Hop      Metric    LocPrf Weight Path
[B]*> 2002::/30    2001:3::2      0         0 100 i
Device2#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 1w6d:03:14:01, lo0
C 2001:3::/64 [0/0]
  via ::, 01:20:21, vlan3
L 2001:3::1/128 [0/0]
  via ::, 01:20:20, vlan3
B 2002::/30 [20/0]
  via 2001:3::2, 00:00:44, vlan3
```

可以看出 Device2 成功学习到 Device1 通告的聚合路由 2002::/30。

方案二：先将明细路由引入 BGP 再通过 aggregate-address 命令进行路由聚合。

#配置 Device1。

```
Device1(config)#router bgp 100
Device1(config-bgp)#address-family ipv6
Device1(config-bgp-af)#redistribute ospf 100
Device1(config-bgp-af)#aggregate-address 2002::/30 summary-only
Device1(config-bgp-af)#exit-address-family
Device1(config-bgp)#exit
```

检验结果

#查看 Device1 的 IPv6 BGP 路由表。

```
Device1#show bgp ipv6 unicast
BGP table version is 4, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Network      Next Hop      Metric    LocPrf Weight Path
[O]*> 2001:2::/64    ::            1         32768 ?
[B]*> 2002::/30     ::            0         32768 i
[O]s> 2002:1::/64   ::            2         32768 ?
[O]s> 2002:2::/64   ::            2         32768 ?
```

可以看出 Device1 的 IPv6 BGP 路由表中已经生成聚合路由 2002::/30。

#查看 Device2 的路由表。

```
Device2#show bgp ipv6 unicast
BGP table version is 4, local router ID is 2.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Network      Next Hop      Metric    LocPrf Weight Path
[B]*> 2001:2::/64    2001:3::2      1         0 100 ?
[B]*> 2002::/30     2001:3::2      0         0 100 i
Device2#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management
```

单播路由

```
L ::1/128 [0/0]
  via ::, 1w6d:03:16:42, lo0
B 2001:2::/64 [20/0]
  via 2001:3::2, 00:00:50, vlan3
C 2001:3::/64 [0/0]
  via ::, 01:23:01, vlan3
L 2001:3::1/128 [0/0]
  via ::, 01:23:00, vlan3
B 2002::/30 [20/0]
  via 2001:3::2, 00:00:50, vlan3
```

可以看出 Device2 成功学习到 Device1 通告的聚合路由 2002::/30。

说明：

- 使用 aggregate-address 命令进行路由聚合的时候，若配置扩展命令 summary-only，设备将只通告聚合路由，否则将同时通告明细路由和聚合路由。
-

45.3.6 配置 IPv6 BGP 路由优选 *-E -A*

网络需求

- Device1 分别与 Device2、Device3 建立 IBGP 邻居，Device4 分别与 Device2、Device3 建立 EBGP 邻居。
- Device1 向 Device4 通告两条路由分别是 2001:1::/64、2001:2::/64，Device4 向 Device1 通告两条路由分别是 2001:7::/64、2001:8::/64。
- 通过在 Device2 和 Device3 上修改路由的 Local-preference 属性，使得 Device1 优选 Device3 通告的路由 2001:7::/64 以及 Device2 通告的路由 2001:8::/64。
- 通过在 Device2 和 Device3 上修改路由的 MED 属性，使得 Device4 优选 Device3 通告的路由 2001:1::/64 以及 Device2 通告的路由 2001:2::/64。

网络拓扑

单播路由

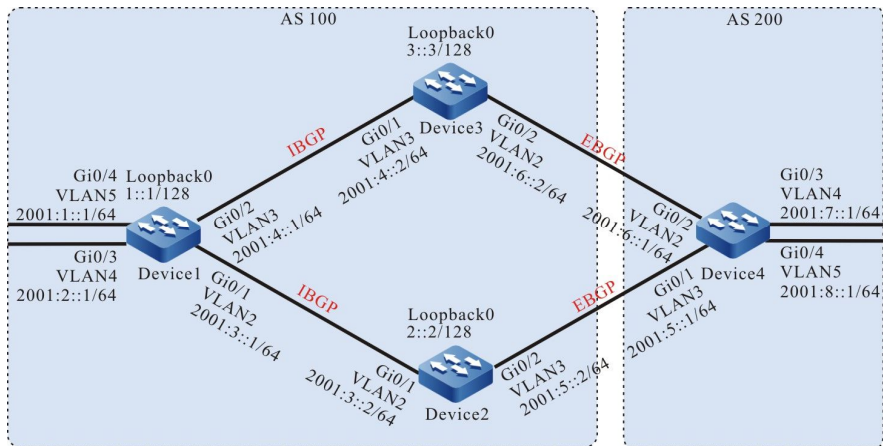


图 45-6 IPv6 BGP 路由优选组网图

配置步骤

步骤 1： 配置各接口的 IPv6 全球单播地址。（略）

步骤 2： 配置 OSPFv3，使设备间 Loopback 接口路由互相可达。

#配置 Device1。

Device1#configure terminal

```
Device1(config)#ipv6 router ospf 100
Device1(config-ospf6)#router-id 1.1.1.1
Device1(config-ospf6)#exit
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#ipv6 router ospf 100 area 0
Device1(config-if-vlan2)#exit
Device1(config)#interface vlan 3
Device1(config-if-vlan3)#ipv6 router ospf 100 area 0
Device1(config-if-vlan3)#exit
Device1(config)#interface loopback 0
Device1(config-if-loopback0)#ipv6 router ospf 100 area 0
Device1(config-if-loopback0)#exit
```

#配置 Device2。

Device2#configure terminal

```
Device2(config)#ipv6 router ospf 100
Device2(config-ospf6)#router-id 2.2.2.2
Device2(config-ospf6)#exit
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#ipv6 router ospf 100 area 0
Device2(config-if-vlan2)#exit
Device2(config)#interface loopback 0
Device2(config-if-loopback0)#ipv6 router ospf 100 area 0
Device2(config-if-loopback0)#exit
```

#配置 Device3。

Device3#configure terminal

配置手册

发布 1.1 04/2020

单播路由

```
Device3(config)#ipv6 router ospf 100
Device3(config-ospf6)#router-id 3.3.3.3
Device3(config-ospf6)#exit
Device3(config)#interface vlan 3
Device3(config-if-vlan3)#ipv6 router ospf 100 area 0
Device3(config-if-vlan3)#exit
Device3(config)#interface loopback 0
Device3(config-if-loopback0)#ipv6 router ospf 100 area 0
Device3(config-if-loopback0)#exit
```

#查看 Device1 的路由表。

```
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
```

```
L ::1/128 [0/0]
   via ::, 1w5d:04:03:11, lo0
LC 1::1/128 [0/0]
   via ::, 00:08:39, loopback0
O 2::2/128 [110/2]
   via fe80::201:7aff:fe5e:87da, 00:02:04, vlan2
O 3::3/128 [110/2]
   via fe80::201:7aff:fec0:525b, 00:00:38, vlan3
C 2001:1::/64 [0/0]
   via ::, 00:09:12, vlan5
L 2001:1::1/128 [0/0]
   via ::, 00:09:11, vlan5
C 2001:2::/64 [0/0]
   via ::, 00:08:26, vlan4
L 2001:2::1/128 [0/0]
   via ::, 00:08:26, vlan4
C 2001:3::/64 [0/0]
   via ::, 00:09:01, vlan2
L 2001:3::1/128 [0/0]
   via ::, 00:09:00, vlan2
C 2001:4::/64 [0/0]
   via ::, 00:08:55, vlan3
L 2001:4::1/128 [0/0]
   via ::, 00:08:53, vlan3
```

#查看 Device2 的路由表。

```
Device2#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
```

```
L ::1/128 [0/0]
   via ::, 2w4d:23:16:51, lo0
O 1::1/128 [110/2]
   via fe80::201:7aff:fe62:bb7f, 00:04:25, vlan2
LC 2::2/128 [0/0]
   via ::, 00:09:31, loopback0
O 3::3/128 [110/3]
   via fe80::201:7aff:fe62:bb7f, 00:02:52, vlan2
C 2001:3::/64 [0/0]
   via ::, 00:09:49, vlan2
L 2001:3::2/128 [0/0]
   via ::, 00:09:48, vlan2
O 2001:4::/64 [110/2]
   via fe80::201:7aff:fe62:bb7f, 00:04:25, vlan2
C 2001:5::/64 [0/0]
   via ::, 00:09:39, vlan3
```

单播路由

```
L 2001:5::2/128 [0/0]
  via ::, 00:09:38, vlan3
```

#查看 Device3 的路由表。

```
Device3#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
```

```
L ::1/128 [0/0]
  via ::, 2w1d:22:16:55, lo0
O 1::1/128 [110/2]
  via fe80::201:7aff:fe62:bb80, 00:04:27, vlan3
O 2::2/128 [110/3]
  via fe80::201:7aff:fe62:bb80, 00:04:27, vlan3
LC 3::3/128 [0/0]
  via ::, 00:10:48, loopback0
O 2001:3::/64 [110/2]
  via fe80::201:7aff:fe62:bb80, 00:04:27, vlan3
C 2001:4::/64 [0/0]
  via ::, 00:11:55, vlan3
L 2001:4::2/128 [0/0]
  via ::, 00:11:54, vlan3
C 2001:6::/64 [0/0]
  via ::, 00:11:48, vlan2
L 2001:6::2/128 [0/0]
  via ::, 00:11:47, vlan2
```

可以看出 Device1、Device2、Device3 互相学习到对方环回口的路由。

步骤 3: 配置 IPv6 BGP 基本功能。

#配置 Device1。

```
Device1(config)#router bgp 100
Device1(config-bgp)#bgp router-id 1.1.1.1
Device1(config-bgp)#address-family ipv6
Device1(config-bgp-af)#neighbor 2::2 remote-as 100
Device1(config-bgp-af)#neighbor 3::3 remote-as 100
Device1(config-bgp-af)#network 2001:1::/64
Device1(config-bgp-af)#network 2001:2::/64
Device1(config-bgp-af)#exit-address-family
Device1(config-bgp)#neighbor 2::2 update-source loopback 0
Device1(config-bgp)#neighbor 3::3 update-source loopback 0
Device1(config-bgp)#exit
```

#配置 Device2。

```
Device2(config)#router bgp 100
Device2(config-bgp)#bgp router-id 2.2.2.2
Device2(config-bgp)#address-family ipv6
Device2(config-bgp-af)#neighbor 1::1 remote-as 100
Device2(config-bgp-af)#neighbor 1::1 next-hop-self
Device2(config-bgp-af)#neighbor 2001:5::1 remote-as 200
Device2(config-bgp-af)#exit-address-family
Device2(config-bgp)#neighbor 1::1 update-source loopback 0
Device2(config-bgp)#exit
```

#配置 Device3。

```
Device3(config)#router bgp 100
```

单播路由

```
Device3(config-bgp)#bgp router-id 3.3.3.3
Device3(config-bgp)#address-family ipv6
Device3(config-bgp-af)#neighbor 1::1 remote-as 100
Device3(config-bgp-af)#neighbor 1::1 next-hop-self
Device3(config-bgp-af)#neighbor 2001:6::1 remote-as 200
Device3(config-bgp-af)#exit-address-family
Device3(config-bgp)#neighbor 1::1 update-source loopback 0
Device3(config-bgp)#exit
```

#配置 Device4。

Device4#configure terminal

```
Device4(config)#router bgp 200
Device4(config-bgp)#bgp router-id 4.4.4.4
Device4(config-bgp)#address-family ipv6
Device4(config-bgp-af)#neighbor 2001:5::2 remote-as 100
Device4(config-bgp-af)#neighbor 2001:6::2 remote-as 100
Device4(config-bgp-af)#network 2001:7::/64
Device4(config-bgp-af)#network 2001:8::/64
Device4(config-bgp-af)#exit-address-family
Device4(config-bgp)#exit
```

#查看 Device1 上 IPv6 BGP 邻居状态。

```
Device1#show bgp ipv6 unicast summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 4
2 BGP AS-PATH entries
0 BGP community entries

Neighbor      V  AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
2::2         4 100    9   10    4   0  0 00:06:18    2
3::3         4 100    7   8     4   0  0 00:04:29    2

Total number of neighbors 2
```

#查看 Device4 上 IPv6 BGP 邻居状态。

```
Device4#show bgp ipv6 unicast summary
BGP router identifier 4.4.4.4, local AS number 200
BGP table version is 4
2 BGP AS-PATH entries
0 BGP community entries

Neighbor      V  AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:5::2    4 100    6   5     4   0  0 00:02:43    2
2001:6::2    4 100    5   6     4   0  0 00:02:32    2

Total number of neighbors 2
```

可以看到 Device1 分别与 Device2、Device3 成功建立 IBGP 邻居，Device4 分别与 Device2、Device3 成功建立 EBGP 邻居。

#查看 Device1 的路由表。

```
Device1#show bgp ipv6 unicast
BGP table version is 4, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop        Metric  LocPrf  Weight Path
[B]*> 2001:1::/64  ::              0       32768  i
[B]*> 2001:2::/64  ::              0       32768  i
[B]* i2001:7::/64  3::3           0       100    0 200  i
```

单播路由

```
[B]*>i          2::2          0    100    0 200 i
[B]*>i2001:8::/64 2::2          0    100    0 200 i
[B]* i          3::3          0    100    0 200 i

Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
```

```
L ::1/128 [0/0]
   via ::, 1w5d:04:20:19, lo0
LC 1::1/128 [0/0]
   via ::, 00:25:47, loopback0
O 2::2/128 [110/2]
   via fe80::201:7aff:fe5e:87da, 00:19:12, vlan2
O 3::3/128 [110/2]
   via fe80::201:7aff:fec0:525b, 00:17:46, vlan3
C 2001:1::/64 [0/0]
   via ::, 00:26:20, vlan5
L 2001:1::1/128 [0/0]
   via ::, 00:26:19, vlan5
C 2001:2::/64 [0/0]
   via ::, 00:25:34, vlan4
L 2001:2::1/128 [0/0]
   via ::, 00:25:34, vlan4
C 2001:3::/64 [0/0]
   via ::, 00:26:09, vlan2
L 2001:3::1/128 [0/0]
   via ::, 00:26:08, vlan2
C 2001:4::/64 [0/0]
   via ::, 00:26:03, vlan3
L 2001:4::1/128 [0/0]
   via ::, 00:26:01, vlan3
B 2001:7::/64 [200/0]
   via 2::2, 00:03:21, vlan2
B 2001:8::/64 [200/0]
   via 2::2, 00:02:57, vlan2
```

可以看到 Device1 上路由 2001:7::/64 和 2001:8::/64 均选择了 Device2 为最优下一跳设备。

#查看 Device4 的路由表。

```
Device4#show bgp ipv6 unicast
BGP table version is 4, local router ID is 4.4.4.4
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop        Metric    LocPrf  Weight Path
[B]* 2001:1::/64   2001:6::2       0         0 100 i
[B]*> 2001:5::2   2001:5::2       0         0 100 i
[B]* 2001:2::/64   2001:6::2       0         0 100 i
[B]*> 2001:5::2   2001:5::2       0         0 100 i
[B]*> 2001:7::/64 ::              0        32768 i
[B]*> 2001:8::/64 ::              0        32768 i

Device4#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
```

```
L ::1/128 [0/0]
   via ::, 1w5d:04:14:15, lo0
B 2001:1::/64 [20/0]
   via 2001:5::2, 00:06:52, vlan2
B 2001:2::/64 [20/0]
```

```
via 2001:5::2, 00:06:52, vlan2
C 2001:5::/64 [0/0]
via ::, 00:26:17, vlan3
L 2001:5::1/128 [0/0]
via ::, 00:26:16, vlan3
C 2001:6::/64 [0/0]
via ::, 00:26:24, vlan2
L 2001:6::1/128 [0/0]
via ::, 00:26:23, vlan2
C 2001:7::/64 [0/0]
via ::, 00:25:53, vlan4
L 2001:7::1/128 [0/0]
via ::, 00:25:51, vlan4
C 2001:8::/64 [0/0]
via ::, 00:25:40, vlan5
L 2001:8::1/128 [0/0]
via ::, 00:25:40, vlan5
```

可以看到 Device4 上路由 2001:1::/64 和 2001:2::/64 均选择了 Device3 为最优下一跳设备。

步骤 4: 配置访问控制列表和路由策略设置 local-preference 和 metric。

#配置 Device2。

```
Device2(config)#ipv6 access-list extended 7001
Device2(config-v6-list)#permit ipv6 2001:8::/64 any
Device2(config-v6-list)#exit
Device2(config)#ipv6 access-list extended 7002
Device2(config-v6-list)#permit ipv6 2001:1::/64 any
Device2(config-v6-list)#exit
Device2(config)#route-map SetPriority1 10
Device2(config-route-map)#match ipv6 address 7001
Device2(config-route-map)#set local-preference 110
Device2(config-route-map)#exit
Device2(config)#route-map SetPriority1 20
Device2(config-route-map)#set local-preference 20
Device2(config-route-map)#exit
Device2(config)#route-map SetPriority2 10
Device2(config-route-map)#match ipv6 address 7002
Device2(config-route-map)#set metric 100
Device2(config-route-map)#exit
Device2(config)#route-map SetPriority2 20
Device2(config-route-map)#set metric 20
Device2(config-route-map)#exit
```

在 Device2 上配置路由策略将路由 2001:8::/64 的 local-preference 设置为 110，同时将路由 2001:1::/64 的 metric 设置为 100。

#配置 Device3。

```
Device3(config)#ipv6 access-list extended 7001
Device3(config-v6-list)#permit ipv6 2001:7::/64 any
Device3(config-v6-list)#exit
Device3(config)#ipv6 access-list extended 7002
Device3(config-v6-list)#permit ipv6 2001:2::/64 any
Device3(config-v6-list)#exit
Device3(config)#route-map SetPriority1 10
Device3(config-route-map)#match ipv6 address 7001
Device3(config-route-map)#set local-preference 110
Device3(config-route-map)#exit
Device3(config)#route-map SetPriority1 20
Device3(config-route-map)#exit
```


单播路由

```
Device3(config)#route-map SetPriority2 10
Device3(config-route-map)#match ipv6 address 7002
Device3(config-route-map)#set metric 100
Device3(config-route-map)#exit
Device3(config)#route-map SetPriority2 20
Device3(config-route-map)#exit
```

在 Device3 上配置路由策略将路由 2001:7::/64 的 local-preference 设置为 110，同时将路由 2001:2::/64 的 metric 设置为 100。

说明：

- 配置路由策略时，前缀列表和 ACL 都可以创建过滤规则，它们的区别在于前缀列表可以精确匹配路由掩码，而 ACL 则不能匹配路由掩码。
-

步骤 5： 配置 IPv6 BGP 关联路由策略。

#配置 Device2。

```
Device2(config)#router bgp 100
Device2(config-bgp)#address-family ipv6
Device2(config-bgp-af)#neighbor 1::1 route-map SetPriority1 out
Device2(config-bgp-af)#neighbor 2001:5::1 route-map SetPriority2 out
Device2(config-bgp-af)#exit-address-family
Device2(config-bgp)#exit
```

在 Device2 上配置邻居 1::1 的出方向修改 2001:8::/64 的 local-preference，同时配置邻居 2001:5::1 的出方向修改 2001:1::/64 的 metric。

#配置 Device3。

```
Device3(config)#router bgp 100
Device3(config-bgp)#address-family ipv6
Device3(config-bgp-af)#neighbor 1::1 route-map SetPriority1 out
Device3(config-bgp-af)#neighbor 2001:6::1 route-map SetPriority2 out
Device3(config-bgp-af)# exit-address-family
Device2(config-bgp)#exit
```

在 Device3 上配置邻居 10.0.0.1 的出方向修改 2001:7::/64 的 local-preference，同时配置邻居 2001:6::1 的出方向修改 2001:2::/64 的 metric。

在邻居上配置了路由策略后需要重置邻居才能生效。

步骤 6： 检验结果。

#查看 Device1 的路由表。

配置手册

单播路由

```
Device1#show bgp ipv6 unicast
BGP table version is 9, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop        Metric  LocPrf Weight Path
[B]*> 2001:1::/64      ::              0       32768 i
[B]*> 2001:2::/64      ::              0       32768 i
[B]* i2001:7::/64     2::2           0       100   0 200 i
[B]*>i                3::3           0       110   0 200 i
[B]*>i2001:8::/64     2::2           0       110   0 200 i
[B]* i                3::3           0       100   0 200 i

Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
```

```
L ::1/128 [0/0]
   via ::, 1w5d:04:59:59, lo0
LC 1::1/128 [0/0]
   via ::, 01:05:27, loopback0
O 2::2/128 [110/2]
   via fe80::201:7aff:fe5e:87da, 00:58:52, gigabitethernet1
O 3::3/128 [110/2]
   via fe80::201:7aff:fec0:525b, 00:57:26, gigabitethernet2
C 2001:1::/64 [0/0]
   via ::, 01:06:00, gigabitethernet0
L 2001:1::1/128 [0/0]
   via ::, 01:05:59, lo0
C 2001:2::/64 [0/0]
   via ::, 01:05:14, loopback1
L 2001:2::1/128 [0/0]
   via ::, 01:05:14, loopback1
C 2001:3::/64 [0/0]
   via ::, 01:05:49, gigabitethernet1
L 2001:3::1/128 [0/0]
   via ::, 01:05:48, lo0
C 2001:4::/64 [0/0]
   via ::, 01:05:43, gigabitethernet2
L 2001:4::1/128 [0/0]
   via ::, 01:05:41, lo0
B 2001:7::/64 [200/0]
   via 3::3, 00:09:05, gigabitethernet1
B 2001:8::/64 [200/0]
   via 2::2, 00:04:58, gigabitethernet0
```

可以看出路由 2001:7::/64 和 2001:8::/64 的 local-preference 被成功修改，Device1 优选 Device2 通告的路由 2001:8::/64，以及 Device3 通告的路由 2001:7::/64。

#查看 Device4 的路由表。

```
Device4#show bgp ipv6 unicast
BGP table version is 5, local router ID is 4.4.4.4
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop        Metric  LocPrf Weight Path
[B]* 2001:1::/64     2001:5::2       100     0 100 i
[B]*>                2001:6::2       0        0 100 i
[B]*> 2001:2::/64     2001:5::2       0        0 100 i
[B]* 2001:7::/64     2001:6::2       100     0 100 i
[B]*> 2001:7::/64     ::              0       32768 i
[B]*> 2001:8::/64     ::              0       32768 i
```

```
Device4#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L ::1/128 [0/0]
  via ::, 1w5d:04:53:45, lo0
B 2001:1::/64 [20/0]
  via 2001:6::2, 00:12:10, gigabitethernet1
B 2001:2::/64 [20/0]
  via 2001:5::2, 00:07:40, gigabitethernet0
C 2001:5::/64 [0/0]
  via ::, 01:05:47, gigabitethernet0
L 2001:5::1/128 [0/0]
  via ::, 01:05:46, lo0
C 2001:6::/64 [0/0]
  via ::, 01:05:54, gigabitethernet1
L 2001:6::1/128 [0/0]
  via ::, 01:05:52, lo0
C 2001:7::/64 [0/0]
  via ::, 01:05:22, gigabitethernet1/0
L 2001:7::1/128 [0/0]
  via ::, 01:05:21, lo0
C 2001:8::/64 [0/0]
  via ::, 01:05:09, gigabitethernet2
L 2001:8::1/128 [0/0]
  via ::, 01:05:09, gigabitethernet2
```

可以看出路由 2001:1::/64 及 2001:2::/64 的 metric 被成功修改，Device4 优选 Device2 通告的路由 2001:2::/64，以及 Device3 通告的路由 2001:1::/64。

说明：

- 路由策略可以使用在路由通告的出方向，同时也可以使用在路由接收的入方向。
-

45.3.7 配置 IPv6 BGP 与 BFD 联动

-E -A

网络需求

- Device1 分别与 Device2、Device3 建立 EBGP 邻居，Device2 与 Device3 建立 IBGP 邻居。
- Device1 同时从 Device2 和 Device3 学习到 EBGP 路由 2001:3::/64，Device1 优先选择通过 Device2 转发数据至 2001:3::/64 网段。
- 在 Device1 与 Device2 上配置 EBGP 关联 BFD，当 Device1 与 Device2 间的线路发生故障后 BFD 能迅速检测并通知 BGP，此时 Device1 选择通过 Device3 转发数

据至 2001:3::/64 网段。

网络拓扑

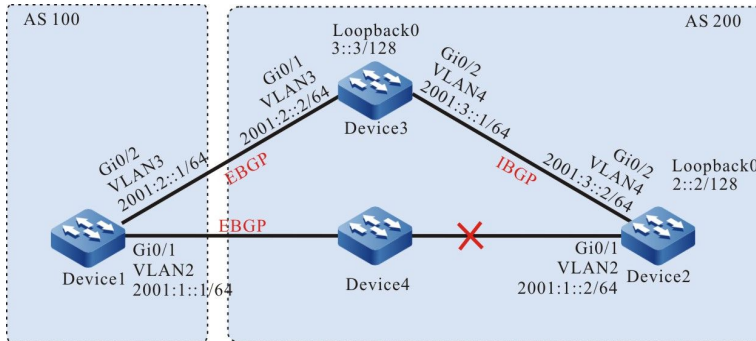


图 45-7 配置 IPv6 BGP 与 BFD 联动组网图

配置步骤

步骤 1: 配置各接口的 IPv6 全球单播地址。(略)

步骤 2: 配置 OSPFv3, 使设备间 Loopback 接口路由互相可达。

#配置 Device2。

Device2#configure terminal

```
Device2(config)#ipv6 router ospf 100
Device2(config-ospf6)#router-id 2.2.2.2
Device2(config-ospf6)#exit
Device2(config)# interface vlan 4
Device2(config-if-vlan4)#ipv6 router ospf 100 area 0
Device2(config-if-vlan4)#exit
Device2(config)#interface loopback 0
Device2(config-if-loopback0)#ipv6 router ospf 100 area 0
Device2(config-if-loopback0)#exit
```

#配置 Device3。

Device3#configure terminal

```
Device3(config)#ipv6 router ospf 100
Device3(config-ospf6)#router-id 3.3.3.3
Device3(config-ospf6)#exit
Device3(config)#interface vlan 4
Device3(config-if-vlan4)#ipv6 router ospf 100 area 0
Device3(config-if-vlan4)#exit
Device3(config)# interface loopback 0
Device3(config-if-loopback0)#ipv6 router ospf 100 area 0
Device3(config-if-loopback0)#exit
```

#查看 Device2 的路由表。

```
Device2#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
U - Per-user Static route
O - OSPF, OE-OSPF External, M - Management
```

```
L ::1/128 [0/0]
  via ::, 1w2d:09:31:22, lo0
LC 2::2/128 [0/0]
  via ::, 00:10:10, loopback0
O 3::3/128 [110/1]
  via fe80::201:7aff:fec0:525a, 00:00:12, vlan4
C 2001:1::/64 [0/0]
  via ::, 00:10:54, vlan2
L 2001:1::2/128 [0/0]
  via ::, 00:10:53, vlan2
C 2001:3::/64 [0/0]
  via ::, 00:10:17, vlan4
L 2001:3::2/128 [0/0]
  via ::, 00:10:16, vlan4
```

#查看 Device3 的路由表。

```
Device3#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
```

```
L ::1/128 [0/0]
  via ::, 1w6d:03:50:38, lo0
O 2::2/128 [110/2]
  via fe80::201:7aff:fe5e:6d2e, 00:02:40, vlan4
LC 3::3/128 [0/0]
  via ::, 00:00:49, loopback0
C 2001:2::/64 [0/0]
  via ::, 00:03:03, vlan3
L 2001:2::2/128 [0/0]
  via ::, 00:03:02, vlan3
C 2001:3::/64 [0/0]
  via ::, 00:03:18, vlan4
L 2001:3::1/128 [0/0]
  via ::, 00:03:17, vlan4
```

可以看出 Device2、Device3 互相学习到对方环回口的接口路由。

步骤 3： 配置访问控制列表和路由策略，设置路由 metric。

#配置 Device1。

Device1#configure terminal

```
Device1(config)#ipv6 access-list extended 7001
Device1(config-v6-list)#permit ipv6 2001:3::/64 any
Device1(config-v6-list)#exit
Device1(config)#route-map SetMetric
Device1(config-route-map)#match ipv6 address 7001
Device1(config-route-map)#set metric 50
Device1(config-route-map)#exit
```

在 Device1 上配置路由策略将路由 2001:3::/64 的 metric 设置为 50。

步骤 4： 配置 IPv6 BGP 基本功能，同时在 Device1 关联路由策略。

#配置 Device1。

配置手册

发布 1.1 04/2020

单播路由

```
Device1(config)#router bgp 100
Device1(config-bgp)#bgp router-id 1.1.1.1
Device1(config-bgp)#address-family ipv6
Device1(config-bgp-af)#neighbor 2001:1::2 remote-as 200
Device1(config-bgp-af)#neighbor 2001:2::2 remote-as 200
Device1(config-bgp-af)#neighbor 2001:2::2 route-map SetMetric in
Device1(config-bgp-af)#exit-address-family
Device1(config-bgp)#exit
```

#配置 Device2。

```
Device2(config)#router bgp 200
Device2(config-bgp)#bgp router-id 2.2.2.2
Device2(config-bgp)#address-family ipv6
Device2(config-bgp-af)#neighbor 2001:1::1 remote-as 100
Device2(config-bgp-af)#neighbor 3::3 remote-as 200
Device2(config-bgp-af)#network 2001:3::/64
Device2(config-bgp-af)#exit-address-family
Device2(config-bgp)#neighbor 3::3 update-source loopback 0
Device2(config-bgp)#exit
```

#配置 Device3。

```
Device3(config)#router bgp 200
Device3(config-bgp)#bgp router-id 3.3.3.3
Device3(config-bgp)#address-family ipv6
Device3(config-bgp-af)#neighbor 2001:2::1 remote-as 100
Device3(config-bgp-af)#neighbor 2::2 remote-as 200
Device3(config-bgp-af)#network 2001:3::/64
Device3(config-bgp-af)#exit-address-family
Device3(config-bgp)#neighbor 2::2 update-source loopback 0
Device3(config-bgp)#exit
```

在对等体上配置了路由策略后需要重置对等体才能生效。

#查看 Device1 上 IPv6 BGP 邻居状态。

```
Device1#show bgp ipv6 unicast summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 2
2 BGP AS-PATH entries
0 BGP community entries

Neighbor    V  AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
2001:1::2   4  200    7    6    2    0  0 00:04:00    1
2001:2::2   4  200    5    5    2    0  0 00:02:03    1

Total number of neighbors 2
```

#查看 Device2 上 IPv6 BGP 邻居状态。

```
Device2#show bgp ipv6 unicast summary
BGP router identifier 2.2.2.2, local AS number 200
BGP table version is 2
1 BGP AS-PATH entries
0 BGP community entries

Neighbor    V  AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
3::3        4  200    5    5    2    0  0 00:02:10    1
2001:1::1   4  100    6    7    2    0  0 00:04:38    0

Total number of neighbors 2
```

可以看到 Device1、Device2、Device3 间 IPv6 BGP 邻居均成功建立。

#查看 Device1 的路由表。

```
Device1#show bgp ipv6 unicast
BGP table version is 2, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop      Metric    LocPrf Weight Path
[B]* 2001:3::/64   2001:2::2     50         0 200 i
[B]*> 2001:1::2    2001:1::2     0          0 200 i
```

```
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management
```

```
L ::1/128 [0/0]
   via ::, 1w2d:09:53:27, lo0
C 2001:1::/64 [0/0]
   via ::, 00:24:05, vlan2
L 2001:1::1/128 [0/0]
   via ::, 00:24:02, vlan2
C 2001:2::/64 [0/0]
   via ::, 00:25:21, vlan3
L 2001:2::1/128 [0/0]
   via ::, 00:25:20, vlan3
B 2001:3::/64 [20/0]
   via 2001:1::2, 00:05:06, vlan2
```

可以看到 Device1 上路由 2001:3::/64 选择了 Device2 为最优下一跳设备。

步骤 5: 配置 IPv6 BGP 与 BFD 联动。

#配置 Device1。

```
Device1(config)#router bgp 100
Device1(config-bgp)#address-family ipv6
Device1(config-bgp-af)#neighbor 2001:1::2 fall-over bfd
Device1(config-bgp-af)#exit-address-family
Device1(config-bgp)#exit
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#bfd min-transmit-interval 500
Device1(config-if-vlan2)#bfd min-receive-interval 500
Device1(config-if-vlan2)#bfd multiplier 4
Device1(config-if-vlan2)#exit
```

#配置 Device2。

```
Device2(config)#router bgp 200
Device2(config-bgp)#address-family ipv6
Device2(config-bgp-af)#neighbor 2001:1::1 fall-over bfd
Device2(config-bgp-af)#exit-address-family
Device2(config-bgp)#exit
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#bfd min-transmit-interval 500
Device2(config-if-vlan2)#bfd min-receive-interval 500
Device2(config-if-vlan2)#bfd multiplier 4
Device2(config-if-vlan2)#exit
```

单播路由

在 Device1 与 Device2 间的 EBGP 邻居上启用 BFD，并修改 BFD 控制报文的最小发送时间间隔和最小接收时间间隔及检测超时倍数。

步骤 6: 检验结果。

#在 Device1 上查看 BFD 会话状态。

```
Device1#show bfd session ipv6
OurAddr           NeighAddr           State   Holddown  Interface
2001:1::1         2001:1::2           UP      2000      vlan2
```

可以看到 Device1 上的 BFD 状态正确 up，holddown 时间协商为 2000ms。

#当 Device1 与 Device2 间线路发生故障时，路由能够迅速切换至备份线路。

#查看 Device1 的路由表。

```
Device1#show bgp ipv6 unicast
BGP table version is 3, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop        Metric   LocPrf  Weight Path
[B]*> 2001:3::/64  2001:2::2       50        0 200 i
Device1#show ipv6 route
Codes: C - Connected, L - Local, S - static, R - RIP, B - BGP, i-ISIS
       U - Per-user Static route
       O - OSPF, OE-OSPF External, M - Management

L  ::1/128 [0/0]
   via ::, 1w2d:10:06:30, lo0
C  2001:1::/64 [0/0]
   via ::, 00:37:08, vlan2
L  2001:1::1/128 [0/0]
   via ::, 00:37:04, vlan2
C  2001:2::/64 [0/0]
   via ::, 00:38:24, vlan3
L  2001:2::1/128 [0/0]
   via ::, 00:38:23, vlan3
B  2001:3::/64 [20/0]
   via 2001:2::2, 00:00:16, vlan3
```

可以看出路由 2001 :3 ::/64 的下一跳切换至 Device3。

46 策略路由

46.1 策略路由简介

策略路由是根据用户定制策略进行报文转发的路由机制。报文在进行路由转发时，可根据 ACL 规则对报文进行匹配，匹配内容为 IP 协议号、源 IP 地址、目的 IP 地址、源 TCP/UDP 端口号、目的 TCP/UDP 端口号、报文优先级、TCP 标志等信息。对于满足匹配条件的报文，按指定的策略执行相应的操作（设置报文的下一跳），以完成对报文的转发控制。

策略路由与传统的仅根据目的地址进行报文转发的路由方式相比，具有更大的灵活性，可看作是对传统路由机制的有效补充和增强。

46.2 策略路由功能配置

表 46-1 策略路由配置列表

配置任务	
配置策略路由	配置报文转发下一跳 IP 地址
	配置报文转发下一跳 IPv6 地址
	配置 PBR 动作组与 ACL 的绑定

配置任务	
	配置 PBR 动作组与 ACL 规则的绑定
配置策略路由的应用	配置具有策略路由的 ACL 应用到二/三层以太接口
	配置具有策略路由的 ACL 应用到 VLAN
	配置具有策略路由的 ACL 应用到 Interface VLAN
	配置具有策略路由的 ACL 应用到全局

46.2.1 配置策略路由 **-S -E -A**

策略路由的实现是依赖于 ACL 规则对报文的过滤。ACL 规则首先过滤出符合条件的报文，然后再对报文执行策略路由转发到下一跳。

配置条件

在配置策略路由功能之前，首先完成以下任务：

- 配置 ACL 和 ACL 规则。

配置报文转发下一跳 IP 地址

配置报文转发的下一跳 IP 地址，以指定策略路由的目的地址。

报文转发的下一跳 IP 地址最多可以指定 6 个。如果用户同时配置多个下一跳 IP 地址，并且存在多个下一跳 IP 地址可达，则报文会采用负载均衡方式选择下一跳 IP 地址进行转发。

表 46-2 配置报文转发的下一跳 IP 地址

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 PBR 动作组配置模式	pbr-action-group <i>pbr-action-group-name</i>	-
配置报文转发的下一跳 IP 地址	redirect ipv4-nexthop <i>ip-address</i> [<i>ip-address</i>] [<i>ip-address</i>] [<i>ip-address</i>] [<i>ip-address</i>]	必选 缺省情况下, 未配置报文转发的下一跳 IP 地址

说明:

- 如果配置的所有转发的下一跳 IP 地址不可达, 则策略路由功能不会生效。
- 下一跳 IP 地址不能配置为本地 IP 地址、组播地址和广播地址。

配置报文转发下一跳 IPv6 地址

配置报文转发的下一跳 IPv6 地址, 以指定策略路由的目的地址。

报文转发的下一跳 IPv6 地址最多可以指定 6 个。如果用户同时配置多个下一跳 IPv6 地址, 并且存在多个下一跳 IPv6 地址可达, 则报文会采用负载均衡方式选择下一跳 IPv6 地址进行转发。

表 46-3 配置报文转发的下一跳 IPv6 地址

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 PBR 动作组配置模式	pbr-action-group <i>pb-action-group-name</i>	-

步骤	命令	说明
配置报文转发的下一跳 IPv6 地址	redirect ipv6-nexthop <i>ipv6-address</i> [<i>ipv6-address</i>] [<i>ipv6-address</i>] [<i>ipv6-address</i>] [<i>ipv6-address</i>] [<i>ipv6-address</i>]	必选 缺省情况下, 未配置报文转发的下一跳 IPv6 地址

说明:

- 如果配置的所有转发的下一跳 IPv6 地址不可达, 则策略路由功能不会生效。
- 下一跳 IPv6 地址不能配置为本地 IPv6 地址、组播地址和广播地址。

配置 PBR 动作组与 ACL 的绑定

配置 PBR 动作组与 ACL 的绑定, 实现 ACL 中所有规则与策略路由执行动作的关联。

PBR 动作组与 ACL 绑定后, ACL 中的所有规则都会与策略路由执行动作建立关联。只要端口接收的报文匹配到 ACL 中的规则, 报文就会转发到下一跳。

表 46-4 配置 PBR 动作组与 ACL 的绑定

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 PBR 动作组与 ACL 的绑定	ip pbr-action-group <i>pbr-action-group-name</i> access-list { <i>access-list-</i>	可选 缺省情况下, 未进行 PBR 动作组与 IP ACL 的绑定

步骤	命令	说明
	<i>number</i> <i>access-list-name</i> }	PBR 动作组支持 IP ACL 绑定, IP ACL 包含 IP 标准 ACL 和 IP 扩展 ACL
	ipv6 pbr-action-group <i>pbr-action-group-name</i> access-list { <i>access-list-number</i> <i>access-list-name</i> }	可选 缺省情况下, 未进行 PBR 动作组与 IPv6 ACL 的绑定 PBR 动作组支持 IPv6 ACL 绑定, IPv6 ACL 包含 IPv6 标准 ACL 和 IPv6 扩展 ACL

说明:

- 只有配置的下一跳 IP 地址可达时, 策略路由才会生效。
- 策略路由只能针对 ACL 中的允许规则生效。

配置 PBR 动作组与 ACL 规则的绑定

配置 PBR 动作组与 ACL 规则的绑定, 实现 ACL 规则与策略路由执行动作的关联。

PBR 动作组与 ACL 规则绑定后, ACL 规则会与策略路由执行动作建立关联。如果端口接收的报文匹配 ACL 规则, 则会按照动作组指定的下一跳进行转发。

表 46-5 配置 PBR 动作组与 ACL 规则的绑定

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
配置 PBR 动作组与 ACL 规则的绑定	请参见 “配置 IP 标准 ACL” 请参见 “配置 IP 扩展 ACL” 请参见 “配置 IPv6 标准 ACL” 请参见 “配置 IPv6 扩展 ACL”	在配置 IP 标准 ACL 和扩展 ACL 的允许规则中，必须指定 PBR 动作组才能使策略路由生效 在配置 IPv6 标准 ACL 和扩展 ACL 的允许规则中，必须指定 PBR 动作组才能使策略路由生效

说明：

- 只有配置的下一跳 IP 地址可达时，策略路由才会生效。
- 策略路由只能针对 ACL 中的允许规则生效。

46.2.2 配置策略路由的应用

-S -E -A

策略路由的应用实际上是具有策略路由的 ACL 的应用，策略路由的生效依赖于 ACL 规则。ACL 可以分别应用在二/三层以太网接口、VLAN、Interface VLAN 和全局。

具有策略路由的 ACL 分别应用到全局、VLAN、Interface VLAN、二/三层以太网接口时，可能会存在冲突。对于这种情况，高优先级对应的策略路由生效，优先级别从高到低依次为：端口，VLAN/Interface VLAN，全局。

配置条件

无

配置具有策略路由的 ACL 应用到二/三层以太网接口

具有策略路由的 ACL 应用到二/三以太接口后，对应二/三以太接口将具有策略路由功能。

表 46-6 配置策略路由应用到二/三以太接口

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二/三层以太接口配置模式	interface <i>interface-name</i>	必选其一 进入二/三层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	
配置策略路由应用到端口	ip policy-based-route { <i>access-list-number</i> <i>access-list-name</i> }	可选 缺省情况下，端口未应用具有策略路由的 IP ACL
	ipv6 policy-based-route { <i>access-list-number</i> <i>access-list-name</i> }	可选 缺省情况下，端口未应用具有策略路由的 IPv6 ACL

配置具有策略路由的 ACL 应用到 VLAN

具有策略路由的 ACL 应用到 VLAN 后，对应 VLAN 内的所有端口将具有策略路由功能。

表 46-7 配置策略路由应用到 VLAN

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 VLAN 配置模式	vlan <i>vlan-id</i>	-
配置策略路由应用到 VLAN	ip policy-based-route { <i>access-list-number</i> <i>access-list-name</i> }	可选 缺省情况下, VLAN 未应用具有策略路由的 IP ACL

配置具有策略路由的 ACL 应用到 Interface VLAN

具有策略路由的 ACL 应用到 Interface VLAN 后, 对应 Interface VLAN 接口将具有策略路由功能。

表 46-8 配置策略路由应用到 Interface VLAN

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 Interface VLAN 配置模式	Interface vlan <i>vlan-id</i>	-
配置策略路由应用到 Interface VLAN	ip policy-based-route { <i>access-list-number</i> <i>access-list-name</i> }	可选 缺省情况下, Interface VLAN 未应用具有策略路由的 IP ACL
	ipv6 policy-based-route { <i>access-list-number</i> <i>access-list-name</i> }	可选

单播路由

步骤	命令	说明
		缺省情况下, Interface VLAN 未应用具有策略路由的 IPv6 ACL

配置具有策略路由的 ACL 应用到全局

具有策略路由的 ACL 应用到全局后, 设备所有端口将具有策略路由功能。

表 46-9 配置策略路由应用到全局

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置策略路由应用到全局	global ip policy-based-route { <i>access-list-number</i> <i>access-list-name</i> }	必选 缺省情况下, 全局未应用具有策略路由的 ACL

46.2.3 策略路由监控与维护

-S -E -A

表 46-10 策略路由监控与维护

命令	说明
show pbr-action-group [<i>pbr-action-group-name</i>]	显示策略路由配置信息

命令	说明
show policy-based-route object [global interface/[vlan switchport]]vlan]	显示策略路由配置应用信息，若不指定参数则表示所有 PBR 的应用信息

46.3 策略路由典型配置举例

46.3.1 配置策略路由

-S -E -A

网络需求

- Device1 有默认路由，网关为 Device2。
- 通过在 Device1 上配置策略路由，实现 PC 访问网络 1.1.1.0/24 经过 Device3，访问网络 1.1.2.0/24 经过 Device2。

网络拓扑

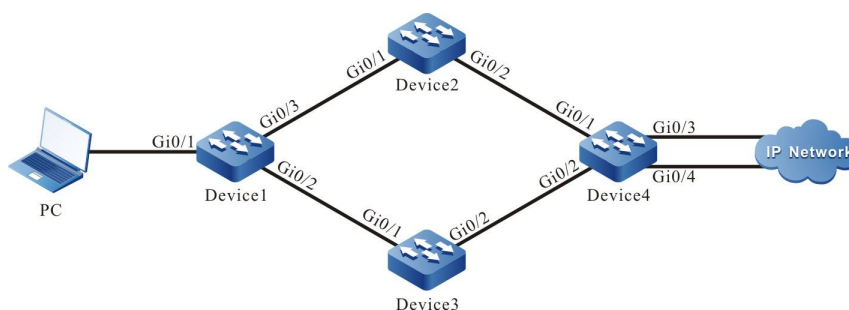


图 46-1 配置策略路由组网图

设备	端口	VLAN	IP 地址
PC			10.1.1.1/24
Device1	Gi0/1	2	10.1.1.2/24

设备	端口	VLAN	IP 地址
	Gi0/2	3	20.1.1.1/24
	Gi0/3	4	30.1.1.1/24
Device2	Gi0/1	2	30.1.1.2/24
	Gi0/2	3	50.1.1.1/24
Device3	Gi0/1	2	20.1.1.2/24
	Gi0/2	3	40.1.1.1/24
Device4	Gi0/1	2	50.1.1.2/24
	Gi0/2	3	40.1.1.2/24
	Gi0/3	4	1.1.1.1/24
	Gi0/4	5	1.1.2.1/24

配置步骤

步骤 1： 配置 VLAN，并将端口加入对应的 VLAN。（略）

步骤 2： 配置各接口 IP 地址。（略）

步骤 3： 配置静态路由。

#配置 Device1。

```
Device1#configure terminal
Device1(config)#ip route 0.0.0.0 0.0.0.0 30.1.1.2
```

#配置 Device2。

```
Device2#configure terminal
Device2(config)#ip route 10.1.1.0 255.255.255.0 30.1.1.1
```

单播路由

```
Device2(config)#ip route 1.1.0.0 255.255.0.0 50.1.1.2
```

#配置 Device3。

```
Device3#configure terminal
Device3(config)#ip route 10.1.1.0 255.255.255.0 20.1.1.1
Device3(config)#ip route 1.1.0.0 255.255.0.0 40.1.1.2
```

#配置 Device4。

```
Device4#configure terminal
Device4(config)#ip route 30.1.1.0 255.255.255.0 50.1.1.1
Device4(config)#ip route 20.1.1.0 255.255.255.0 40.1.1.1
Device4(config)#ip route 10.1.1.0 255.255.255.0 50.1.1.1
Device4(config)#ip route 10.1.1.0 255.255.255.0 40.1.1.1
```

#查看 Device1 的路由表。

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, Ex - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is 30.1.1.2 to network 0.0.0.0

S  0.0.0.0/0 [1/100] via 30.1.1.2, 00:26:24, vlan4
C  10.1.1.0/24 is directly connected, 00:00:59, vlan2
C  20.1.1.0/24 is directly connected, 00:00:50, vlan3
C  30.1.1.0/24 is directly connected, 00:00:39, vlan4
C  127.0.0.0/8 is directly connected, 03:47:36, lo0
```

步骤 4: Device1 上配置策略路由。

#配置 PBR 动作组，将报文重定向到下一跳 20.1.1.2。

```
Device1(config)#pbr-action-group pbr
Device1(config-action-group)#redirect ipv4-nexthop 20.1.1.2
Device1(config-action-group)#count all-colors
Device1(config-action-group)#exit
```

#查看 Device1 的 PBR 动作组信息。

```
Device1#show pbr-action-group pbr
pbr-action-group pbr
redirect ipv4-nexthop 20.1.1.2(valid)
```

#配置 ACL，将匹配目的 IP 网段为 1.1.1.0/24 的 ACL 规则绑定 L3 动作组 pbr。

```
Device1(config)#ip access-list extended 1001
Device1(config-std-nacl)#permit ip any 1.1.1.0 0.0.0.255 pbr-action-group pbr
Device1(config-std-nacl)#permit ip any 1.1.2.0 0.0.0.255
Device1(config-std-nacl)#exit
```

#查看 Device1 的 ACL 的信息。

```
Device1#show ip access-list 1001
ip access-list standard 1001
 10 permit ip any 1.1.1.0 0.0.0.255 pbr-action-group pbr (active)
 20 permit ip any 1.1.2.0 0.0.0.255
```

步骤 6: 应用 ACL。

#在 Device1 端口 vlan2 的上应用 ACL 1001。

```
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip policy-based-route 1001 in
Device1(config-if-vlan2)#exit
```

步骤 7: 检验结果。

#在 PC 上通过 Traceroute 查看到达目的网络 1.1.1.0/24 所经过的路径。

```
C:\Documents and Settings\Administrator>tracert 1.1.1.1

Tracing route to 1.1.1.1 over a maximum of 30 hops

  0  1 ms   1 ms   1 ms  10.1.1.2
  1  <1 ms  <1 ms  <1 ms 20.1.1.2
  2  <1 ms  <1 ms  <1 ms 1.1.1.1
Trace complete.
```

可以看出 PC 经过 Device1、Device3、Device4 到达网络 1.1.1.0/24。

#在 PC 上通过 Traceroute 查看到达目的网络 1.1.2.0/24 所经过的路径。

```
C:\Documents and Settings\Administrator>tracert 1.1.2.1

Tracing route to 1.1.2.1 over a maximum of 30 hops

  0  1 ms   1 ms   1 ms  10.1.1.2
  1  <1 ms  <1 ms  <1 ms 30.1.1.2
  2  <1 ms  <1 ms  <1 ms 1.1.2.1
Trace complete.
```

可以看出 PC 经过 Device1、Device2、Device4 到达网络 1.1.2.0/24。

说明:

- 在进行报文匹配时，根据引用的 ACL 规则进行灵活匹配，可以匹配报文源 IP 地址、目的 IP 地址、源端口、目的端口、协议、TCP 标志信息等。
 - 对于 ACL 的绑定，除了可以在二/三层以太网接口上绑定外，还可在 VLAN、Interface VLAN、全局进行绑定。
-

47 路由策略工具

47.1 路由策略工具简介

路由策略通过改变路由属性或路由可达性，以改变路由信息或数据流量所经过的途径。主要应用于以下几个方面：

- 设置路由属性：对通过路由策略匹配的路由设置相应的属性；
- 控制路由发布：路由协议在发布路由时，只发布满足条件的路由信息；
- 控制路由接收：路由协议在接收路由时，只接收满足条件的路由信息，以控制路由表项的数量，并提高网络的安全性；
- 控制路由重分发：路由协议在重分发引入外部路由时，只引入满足条件的路由信息，也可使用路由策略工具设置引入外部路由的某些属性。

密码链（Key-chain）则是一种密码管理工具，为路由协议在进行协议报文认证的时候提供认证密码。

47.2 路由策略工具功能配置

表 47-1 路由策略工具配置列表

配置任务	
配置前缀列表	配置前缀列表

配置任务	
配置 AS-PATH 列表	配置 AS-PATH 列表
配置团体属性列表	配置团体属性列表
配置扩展团体属性列表	配置扩展团体属性列表
配置路由图	创建路由图
	配置路由图 match 子句
	配置路由图 set 子句
配置密码链	配置密码链

47.2.1 配置前缀列表

-S -E -A

配置条件

无

配置前缀列表

前缀列表是针对前缀进行过滤，主要用于路由过滤。相对于 ACL 最初是被设计成用于数据包的过滤而后来才被应用在路由的过滤上，前缀列表被设计成用于路由的过滤。虽然它们在路由过滤的功能上有部分的重叠，但前缀列表在这方面要比 ACL 更灵活。

一个前缀列表由前缀列表名称标识。每个前缀列表可以包含多个表项，每个表项可以独立指定一个匹配范围。每个表项对应一个序号，用以指明前缀列表进行匹配检查的顺序。

前缀列表各个表项之间是“或”的关系，设备在匹配过程中，根据表项对应的序号按照从小到大的顺序进行检查，只要匹配上某一表项，就表示通过该前缀列表的过滤，不再检查下一个表项。

表 47-2 配置前缀列表

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 IPv4 前缀列表	ip prefix-list <i>prefix-list-name</i> [seq <i>seq-value</i>] { deny permit } <i>network / length</i> [ge <i>ge-value</i>] [le <i>le-value</i>]	必选 缺省情况下，未配置 IPv4 前缀列表

说明：

- **ge** 表示大于等于，**le** 表示小于等于，取值范围 $0 \leq \text{length} < \text{ge-value} \leq \text{le-value} \leq 32$ 。如配置 **ip prefix-list test permit 192.168.0.0/16 ge 18 le 24**，则表示允许地址为 192.168.0.0 掩码长度在 18（包含 18）到 24（包含 24）之间的路由项通过。
- 当 *network/length* 配置为 0.0.0.0/0 时，表示匹配默认路由；配置为 0.0.0.0/0 **le 32** 时，表示匹配所有路由。
- IPv4 前缀列表最后，含有隐式的禁止所有的表项：**deny 0.0.0.0/0 le 32**，当通过配置 **deny** 语句禁止某些路由时，建议在最后添加 **permit 0.0.0.0/0 le 32** 的语句，以允许其它 IPv4 路由通过。

47.2.2 配置 AS-PATH 列表

-E -A

配置条件

无

配置 AS-PATH 列表

AS-PATH 列表是针对 AS 号进行过滤的一种工具，用于 BGP 路由的过滤。BGP 路由的 AS 路径属性记录了此路由经过的所有 AS，BGP 在向本 AS 外部通告一条路由时，会把本自治系统的 AS 号加入到 AS 路径属性中，以记录此路由经过的 AS 路径信息。

一个 AS-PATH 列表可包含多个表项，各个表项之间是“或”的关系，匹配时根据配置的先后顺序进行检查，只要路由通过该 AS-PATH 列表中的某一个表项，就认为通过该 AS-PATH 列表。

表 47-3 配置 AS-PATH 列表

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 AS-PATH 列表	ip as-path access-list <i>path-list-number</i> { permit deny } <i>regular-expression</i>	必选 缺省情况下，未配置 AS-PATH 列表

AS-PATH 列表中使用正则表达式，用于指定符合规定的 AS 属性集合。正则表达式由一些普通字符和一些元字符 (Metacharacters) 组成。普通字符包括大小写的字母和数字，而元字符则具有特殊的含义，如下表所示。

表 47-4 正则表达式中元字符含义

符号	含义
.	匹配任意单字符
*	匹配模式中可跟 0 或更多位的序列
+	匹配模式中可跟 1 或更多位的序列
?	匹配模式中只能再跟 0 或 1 位序列
^	匹配输入字符串的开始
\$	匹配输入字符串的结束

符号	含义
-	匹配逗号, 括号, 字符串的开始和结束, 空格
[]	匹配一定范围中的单字符
-	把一个范围的结束点分开

47.2.3 配置团体属性列表 **-E -A**

配置条件

无

配置团体属性列表

团体属性列表 (Community-list) 用于针对路由的团体属性进行过滤。一般来说, 一个路由可以分为前缀和路由属性两个部分。其中路由属性在各个路由协议之间不一样, 在 IGP 协议中一般有 metric 等比较简单的属性, 在 BGP 中则比较繁多而复杂, 其中就有团体属性, Community-list 就是用于对这部分进行过滤的。团体属性列表过滤的结果是对这个团体属性所在整个路由而言的, 也就是说, 如果过滤的结果是 deny 的话, 那么是整条路由都会被 deny, 而不是仅仅 deny 这个团体属性。

Community-list 包括标准和扩展两种, 其中标准 Community-list 根据 BGP 路由的 local-AS、internet、no-advertise、no-export 属性进行过滤; 扩展 Community-list 则使用正则表达式对具有这些团体属性的 BGP 路由进行过滤。

在对 Community-list 的使用上, 带有团体属性的路由协议可以直接使用, 但常常都是通过把 Community-list 绑定到路由图上, 再由路由协议应用路由图的方式间接使用。

一个 Community-list 可包含多个表项, 各个表项之间是“或”的关系, 匹配时根据配置的先后顺序进行检查, 只要路由通过该 Community-list 中的某一个表项, 就认为通过该 Community-list。配置扩展 Community-list 时, 正则表达式的使用请参考配置 AS-PATH 列表部分。

表 47-5 配置团体属性列表

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置标准 Community-list	ip community-list { <i>community-list-number</i> standard <i>community-list-name</i> } { permit deny } [<i>community-number</i> / <i>aa: nn</i> / local-AS / internet / no-advertise / no-export]	必选 缺省情况下, 未配置标准 Community-list
配置扩展 Community-list	ip community-list { <i>community-list-number</i> expanded <i>community-list-name</i> } { permit deny } <i>regular-expression</i>	必选 缺省情况下, 未配置扩展 Community-list

47.2.4 配置扩展团体属性列表

-E -A

配置条件

无

配置扩展团体属性列表

Extcommunity-list 是针对扩展团体属性进行过滤, 主要用于 BGP 路由的过滤。Extcommunity-list 的性质和使用方法与 Community-list 基本是一样的, 主要区别在于扩展团体属性主要是在 MPLS L3VPN 中使用, 所以 Extcommunity-list 也主要使用在 MPLS L3VPN 中。

Extcommunity-list 包括标准和扩展两种，其中标准 Extcommunity-list 根据 BGP 路由的目标 (Router Target) 属性和源站点 (Site of Origin) 属性进行过滤；扩展 Extcommunity-list 则使用正则表达式对具有这些属性的 BGP 路由进行过滤。

一个扩展团体属性列表可包含多个表项，各个表项之间是“或”的关系，匹配时根据配置的先后顺序进行检查，只要路由通过该扩展团体属性列表中的某一个表项，就认为通过该扩展团体属性列表。配置扩展 Extcommunity-list 时，正则表达式的使用参考配置 AS-PATH 列表部分。

表 47-6 配置扩展团体属性列表

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置标准 Extcommunity-list	ip extcommunity-list { <i>extcommunity-list-number</i> standard <i>extcommunity-list-name</i> } { permit deny } [rt <i>extcommunity-number</i> / soo <i>extcommunity-number</i>]	必选 缺省情况下，未配置标准 Extcommunity-list
配置扩展 Extcommunity-list	ip extcommunity-list { <i>extcommunity-list-number</i> expanded <i>extcommunity-list-name</i> } { permit deny } <i>regular-expression</i>	必选 缺省情况下，未配置扩展 Extcommunity-list

47.2.5 配置路由图 **-S -E -A**

路由图是一种匹配路由、设置路由属性的工具。一个路由图由若干语句组成，每一语句由一些 match 子句和 set 子句组成。match 子句定义该语句的匹配规则，set 子句定义通过 match 子句匹配后进行的动作。match 子句之间是“与”的关系，即必须满足该语句的所有 match 子句。

路由图语句之间是“或”的关系，设备在匹配过程中，根据语句的序号按照从小到大的顺序进行检查，只要通过一个语句的检查就意味着匹配该路由图，不再检查下一个语句。若没有通过任一语句的检查，则不匹配该路由图。

配置条件

在配置路由图之前，首先完成以下任务：

- 配置路由图需要使用的 ACL、前缀列表、AS-PATH、团体属性列表或扩展团体属性列表。

创建路由图

创建路由图时，可指定路由图语句的匹配模式，有 **permit** 和 **deny** 两种：

permit 指定所创建路由图语句的匹配模式为允许。当路由项满足该语句的所有 match 子句时被允许通过，并执行该语句的 set 子句。若路由项不满足该语句的 match 子句，将会检查该路由图下一个语句；

deny 指定所创建路由图语句的匹配模式为禁止，仅当路由项满足该语句的所有 match 子句时将被禁止，并且不会进行下一个语句的检查。**deny** 模式下不会执行 set 子句。

表 47-7 创建路由图

步骤	命令	说明
进入全局配置模式	configure terminal	-
创建路由图	route-map <i>map-name</i> [{ permit deny } [<i>seq-number</i>]]	必选 缺省情况下，没有创建路由图

说明：

- 通过 `route-map` 命令创建路由图，当仅配置路由图的名称，而省略匹配模式和语句序号时，会自动增加一条匹配模式为 `permit`、序号为 10 的语句。
- 当路由协议应用路由图，但路由图未配置时，所有对象均匹配失败。

配置路由图 match 子句

路由图语句的 `match` 子句之间是“与”的关系，必须满足所有 `match` 子句才能通过。

表 47-8 配置路由图 match 子句

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入路由图配置模式	route-map <i>map-name</i> [{ permit deny } [<i>seq-number</i>]]	-
指定路由图匹配的 AS-PATH 列表	match as-path <i>path-list-number</i>	可选 缺省情况下，没有指定路由图匹配的 AS-PATH 列表
指定路由图匹配的 BGP 团体属性列表	match community <i>community-list-number</i> / <i>community-list-name</i> [exact-match]	可选 缺省情况下，没有指定路由图匹配的 BGP 团体属性列表
指定路由图匹配的 BGP 扩展团体属性列表	match extcommunity <i>extcommunity-list-number</i> /	可选

步骤	命令	说明
	<code>extcommunity-list-name</code>	缺省情况下, 没有指定路由图匹配的 BGP 扩展团体属性列表
指定路由图匹配的接口	match interface <code>interface-names</code>	可选 缺省情况下, 没有指定路由图匹配的接口
指定路由图匹配的路由前缀	match ip address { <code>access-list-number</code> <code>access-list-name</code> prefix-list <code>prefix-list-name</code> }	可选 缺省情况下, 没有指定路由图匹配的路由前缀
指定路由图匹配的下一跳地址	match ip next-hop { <code>access-list-name</code> prefix-list <code>prefix-list-name</code> }	可选 缺省情况下, 没有指定路由图匹配的下一跳地址
指定路由图匹配的路由源地址	match ip route-source { <code>access-list-name</code> prefix-list <code>prefix-list-name</code> }	可选 缺省情况下, 没有指定路由图匹配的路由源地址
指定路由图匹配的路由 metric 值	match metric <code>metric-value</code> [+ - <code>offset</code>]	可选 缺省情况下, 没有指定路由图匹配的路由 metric 值
指定路由图匹配的路由类型	match route-type { external / interarea / internal / level-1 /	可选 缺省情况下, 没有指定路由图匹配的路由类型

步骤	命令	说明
	level-2 / nssa-external / type-1 / type-2 }	
指定路由图匹配的 tag 值	match tag tag-value	可选 缺省情况下，没有指定路由图匹配的 tag 值

说明：

- 当路由图中没有配置 match 子句时，所有对象均能匹配成功。
- 当 match 子句关联的 ACL、前缀列表不存在时，所有对象均匹配失败。

配置路由图 set 子句

仅当路由图匹配模式为 permit，且所有 match 子句匹配通过后，才会执行 set 操作。匹配模式为 deny 时，不会执行 set 操作。

表 47-9 配置路由图 set 子句

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入路由图配置模式	route-map map-name [{ permit deny } [<i>seq-number</i>]]	-
设置 BGP 路由的 AS 路径属性	set as-path prepend as-path-number	可选 缺省情况下，未设置 BGP 路由的 AS 路径属性

步骤	命令	说明
设置 BGP 路由的团体属性	set communitiy { <i>community-number</i> additive local-AS internet no-advertise no-export none }	可选 缺省情况下, 未设置 BGP 路由的团体属性
删除指定的 BGP 团体属性列表	set comm-list { <i>community-list-number</i> / <i>community-list-name</i> } delete	可选 缺省情况下, 未删除 BGP 团体属性
设置 BGP 路由衰减参数	set dampening <i>half-life</i> <i>start-reusing</i> <i>start-suppress</i> <i>max-duration</i>	可选 缺省情况下, 未设置 BGP 路由衰减参数
设置 MPLS L3VPN 路由的扩展团体属性	set extcommunity { <i>rt</i> soo } <i>extcommunity</i>	可选 缺省情况下, 未设置 MPLS L3VPN 路由的扩展团体属性
设置路由下一跳	set ip default next-hop <i>ip-address</i>	可选 缺省情况下, 未设置路由下一跳 用于在 OSPF 路由重分发时, 设置路由下一跳
设置路由下一跳	set ip next-hop <i>ip-address</i>	可选 缺省情况下, 未设置路由下一跳

步骤	命令	说明
		用于 BGP 关联路由图设置路由下一跳
设置 BGP 路由的本地优先级	set local-preference <i>value</i>	可选 缺省情况下，未设置 BGP 路由的本地优先级
设置路由的 metric 值	set metric { <i>metric</i> + <i>metric</i> - <i>metric</i> <i>bandwidth delay reliable loading mtu</i> }	可选 缺省情况下，未设置路由的 metric 值
设置路由的 metric 类型	set metric-type { external internal type-1 type-2 }	可选 缺省情况下，未设置路由的 metric 类型
设置 BGP 路由的 Origin 属性	set origin { egp <i>as-number</i> igp incomplete }	可选 缺省情况下，未设置 BGP 路由的 Origin 属性
设置外部路由的 tag 选项字段	set tag <i>tag-value</i>	可选 缺省情况下，未设置外部路由的 tag 选项字段
设置 BGP 路由的权重	set weight <i>weight-value</i>	可选 缺省情况下，未设置 BGP 路由的权重

47.2.6 配置密码链

-S -E -A**配置条件**

无

配置密码链

密码链 (Key-chain) 是一个密码管理器，为路由协议在进行协议报文认证的时候提供认证密码。密码链能够针对报文的发送和接收提供不同的密码，并能够为不同的 Key ID 提供不同的密码。同时，密码链还能够根据配置 Key 的有效时间，定时自动切换密码，即在不同时间段使用不同的密码，大大加强了密码的安全性。

可以为一个密码链配置多个 Key ID，协议在使用密码链进行认证的时候，具体应用哪个 Key ID，根据以下规则获取：

- 获取发送密码的时候，获取的是 Key ID 最小的有效发送密码；
- 获取接收密码的时候，在 Key ID 大于等于协议给定 Key ID 的 Key 中，获取 Key ID 最小的有效接收密码；
- 当接收到的协议报文中带有 Key ID 时，会根据该 Key ID 在本端查找对应的有效接收密码；否则，将采用本端密码链中 Key ID 最小的有效接收密码。

表 47-10 配置密码链

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置产生一个密码链	key chain <i>keychain-name</i>	必选 缺省情况下，未配置密码链
配置 Key ID	key <i>key-id</i>	必选 缺省情况下，未配置 Key ID

步骤	命令	说明
配置密码	key-string [0 7] <i>password</i>	必选 缺省情况下，未配置密码 空格也被认为是密码字符，配置密码时需注意
设置 Key 作为接收密码的有效时间	accept-lifetime <i>time-start</i> { <i>time-end</i> duration <i>second</i> infinite }	必选 缺省情况下，接收密码一直有效
设置 Key 作为发送密码的有效时间	send-lifetime <i>time-start</i> { <i>time-end</i> duration <i>second</i> infinite }	必选 缺省情况下，发送密码一直有效

47.2.7 路由策略工具监控与维护

-S -E -A

表 47-11 路由策略工具监控与维护

命令	说明
clear ip prefix-list [<i>prefix-list-name</i> <i>network/length</i>]	清除前缀列表统计信息
show ip prefix-list [<i>prefix-list-name</i> [<i>network/length</i>] [first-match longer] seq <i>sep_value</i>] detail [<i>prefix-list-name</i>] orf-prefix summary [<i>prefix-list-name</i>]	显示前缀列表信息

命令	说明
show ip as-path-access-list [<i>list-name</i>]	显示 AS-PATH 列表信息
show ip community-list [<i>community-list-number</i> <i>community-list-name</i>]	显示团体属性列表信息
show ip extcommunity-list [<i>extcommunity-list-number</i> <i>extcommunity-list-name</i>]	显示扩展团体属性列表信息
show route-map [<i>route-map-name</i>]	显示路由图信息
show key chain [<i>keychain-name</i>]	显示密码链信息

47.3 路由策略工具典型配置举例

47.3.1 配置路由重分发关联路由策略 **-S -E -A**

网络需求

- Device1 和 Device2 间运行 OSPF 协议，Device2 和 Device3 间运行 RIP 协议。
- Device2 上配置 OSPF 重分发 RIP 路由，同时关联路由策略修改路由属性，要求路由 100.1.1.0/24 的 Tag 属性修改为 5，路由 110.1.1.0/24 的 Metric 值修改为 50，路由 120.1.1.0/24 的属性不变。

网络拓扑

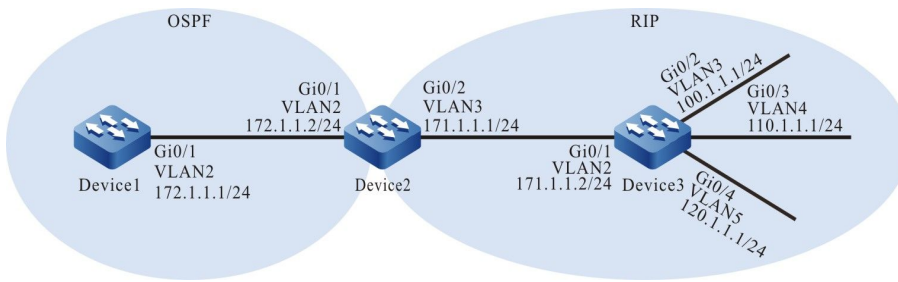


图 47-1 配置路由重分发关联路由策略组网图

配置步骤

步骤 1： 配置 VLAN，并将端口加入对应的 VLAN。（略）

步骤 2： 配置各接口的 IP 地址。（略）

步骤 3： 配置 OSPF。

#配置 Device1。

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 172.1.1.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#配置 Device2。

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 172.1.1.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

步骤 4： 配置 RIP。

#配置 Device2。

```
Device2(config)#router rip
Device2(config-rip)#version 2
Device2(config-rip)#network 171.1.1.0
Device2(config-rip)#exit
```

#配置 Device3。

```
Device3(config)#configure terminal
Device3(config)#router rip
Device3(config-rip)#version 2
Device3(config-rip)#network 171.1.1.0
Device3(config-rip)#network 100.1.1.0
Device3(config-rip)#network 110.1.1.0
Device3(config-rip)#network 120.1.1.0
```

```
Device3(config-rip)#exit
```

步骤 5: 配置 OSPF 重分发 RIP 路由。

#配置 Device2。

```
Device2(config)#router ospf 100
Device2(config-ospf)#redistribute rip
Device2(config-ospf)#exit
```

#查看 Device1 的路由表。

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

OE 100.1.1.0/24 [150/20] via 172.1.1.2, 02:22:08, vlan2
OE 110.1.1.0/24 [150/20] via 172.1.1.2, 00:49:57, vlan2
OE 120.1.1.0/24 [150/20] via 172.1.1.2, 02:22:08, vlan2
OE 171.1.1.0/24 [150/20] via 172.1.1.2, 02:22:41, vlan2
```

通过查看 Device1 的路由表，发现在 Device2 上的 RIP 路由 100.1.1.0/24、110.1.1.0/24、120.1.1.0/24 被重分发到了 OSPF 进程，并成功通告给 Device1。

步骤 6: 配置访问列表和路由策略。

#配置 Device2。

配置访问列表，允许 100.1.1.0/24、110.1.1.0/24 和 120.1.1.0/24 的路由通过。

```
Device2(config)#ip access-list standard 1
Device2(config-std-nacl)#permit 100.1.1.0 0.0.0.255
Device2(config-std-nacl)#exit
Device2(config)#ip access-list standard 2
Device2(config-std-nacl)#permit 110.1.1.0 0.0.0.255
Device2(config-std-nacl)#exit
Device2(config)#ip access-list standard 3
Device2(config-std-nacl)#permit 120.1.1.0 0.0.0.255
Device2(config-std-nacl)#exit
```

配置路由策略 rip_to_ospf，对匹配编号为 1 的访问列表允许的路由设置 tag 属性，对匹配编号为 2 的访问列表允许的路由设置 metric 属性，对匹配编号为 3 的访问列表允许的路由不改变路由属性。

```
Device2(config)#route-map rip_to_ospf 10
Device2(config-route-map)#match ip address 1
Device2(config-route-map)#set tag 5
Device2(config-route-map)#exit
Device2(config)#route-map rip_to_ospf 20
Device2(config-route-map)#match ip address 2
Device2(config-route-map)#set metric 50
Device2(config-route-map)#exit
Device2(config)#route-map rip_to_ospf 30
Device2(config-route-map)#match ip address 3
```

```
Device2(config-route-map)#exit
```

说明：

- 配置路由策略时，前缀列表和 ACL 都可以创建匹配规则，它们的区别在于前缀列表可以精确匹配路由掩码，而 ACL 则不能匹配路由掩码。
-

步骤 7： 配置 OSPF 重分发 RIP 路由关联路由策略。

#配置 Device2。

```
Device2(config)#router ospf 100
Device2(config-ospf)#redistribute rip route-map rip_to_ospf
Device2(config-ospf)#exit
```

步骤 8： 检验结果。

#查看 Device1 的 OSPF 数据库。

```
Device1#show ip ospf database external
      OSPF Router with ID (172.1.1.1) (Process ID 100)
```

```
      AS External Link States
```

```
      LS age: 1183
      Options: 0x22 (-|-|DC|-|-|E|-)
      LS Type: AS-external-LSA
      Link State ID: 100.1.1.0 (External Network Number)
      Advertising Router: 172.1.1.2
      LS Seq Number: 80000006
      Checksum: 0xbcc0
      Length: 36
      Network Mask: /24
      Metric Type: 2 (Larger than any link state path)
      TOS: 0
      Metric: 20
      Forward Address: 0.0.0.0
      External Route Tag: 5
```

```
      LS age: 1233
      Options: 0x22 (-|-|DC|-|-|E|-)
      LS Type: AS-external-LSA
      Link State ID: 110.1.1.0 (External Network Number)
      Advertising Router: 172.1.1.2
      LS Seq Number: 80000006
      Checksum: 0x0d4d
      Length: 36
      Network Mask: /24
```



```
Metric Type: 2 (Larger than any link state path)
TOS: 0
Metric: 50
Forward Address: 0.0.0.0
External Route Tag: 0
```

```
LS age: 1113
Options: 0x22 (-|DC|)|-|E|)
LS Type: AS-external-LSA
Link State ID: 120.1.1.0 (External Network Number)
Advertising Router: 172.1.1.2
LS Seq Number: 80000005
Checksum: 0x5f10
Length: 36
Network Mask: /24
  Metric Type: 2 (Larger than any link state path)
  TOS: 0
  Metric: 20
  Forward Address: 0.0.0.0
  External Route Tag: 0
```

#查看 Device1 的路由表。

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

OE 100.1.1.0/24 [150/20] via 172.1.1.2, 02:30:28, vlan2
OE 110.1.1.0/24 [150/50] via 172.1.1.2, 00:58:17, vlan2
OE 120.1.1.0/24 [150/20] via 172.1.1.2, 02:30:28, vlan2
```

通过查看 Device1 的 OSPF 数据库和路由表，发现 100.1.1.0/24 的路由 Tag 为 5，110.1.1.0/24 的路由 Metric 为 50，120.1.1.0/24 的路由属性没有改变。

说明：

- 重分发外部路由的时候，RIP 进程覆盖的直连接口路由也会被重分发到目标协议中。
-

47.3.2 配置 BGP 关联路由策略

-E -A

网络需求

- Device1 分别与 Device2、Device3 之间运行 IGP 协议 OSPF，建立 IBGP 邻居，Device4 分别与 Device2、Device3 之间建立 EBGP 邻居。
- 要求在 Device2 和 Device3 上配置路由策略，使得 Device1 将去往 100.1.1.0/24 网段的数据经过 Device2 到达，将去往 110.1.1.0/24 网段的数据经过 Device3 到

达, 使得 Device4 将去往 120.1.1.0/24 网段的数据经过 Device2 到达, 将去往 130.1.1.0/24 网段的数据经过 Device3 到达。

网络拓扑

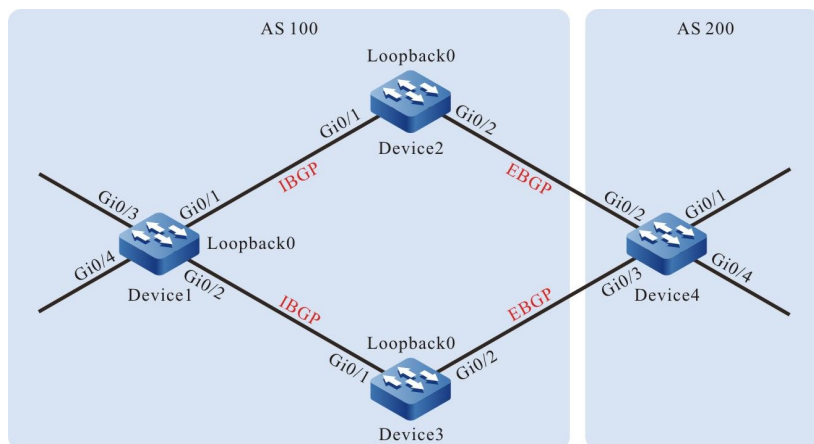


图 47-2 配置 BGP 关联路由策略组网图

设备	接口	VLAN	IP 地址
Device1	Gi0/1	2	1.0.0.1/24
	Gi0/2	3	2.0.0.1/24
	Gi0/3	4	120.1.1.1/24
	Gi0/4	5	130.1.1.1/24
	Loopback0		38.1.1.1/32
Device2	Gi0/1	2	1.0.0.2/24
	Gi0/2	3	3.0.0.1/24
	Loopback0		39.1.1.1/32
Device3	Gi0/1	2	2.0.0.2/24
	Gi0/2	3	4.0.0.1/24

设备	接口	VLAN	IP 地址
	Loopback0		40.1.1.1/32
Device4	Gi0/1	2	100.1.1.1/24
	Gi0/2	3	3.0.0.2/24
	Gi0/3	4	4.0.0.2/24
	Gi0/4	5	110.1.1.1/24

配置步骤

步骤 1： 配置 VLAN，并将端口加入对应的 VLAN。（略）

步骤 2： 配置各接口的 IP 地址。（略）

步骤 3： 配置 OSPF，使设备间 Loopback 路由互相可达。

#配置 Device1。

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 1.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 38.1.1.1 0.0.0.0 area 0
Device1(config-ospf)#exit
```

#配置 Device2。

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 1.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 39.1.1.1 0.0.0.0 area 0
Device2(config-ospf)#exit
```

#配置 Device3。

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 40.1.1.1 0.0.0.0 area 0
Device3(config-ospf)#exit
```

#查看 Device1 的路由表。

单播路由

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS
```

```
Gateway of last resort is not set
```

```
O 39.1.1.1/32 [110/2] via 1.0.0.2, 19:11:33, vlan2
O 40.1.1.1/32 [110/2] via 2.0.0.2, 18:56:32, vlan3
```

#查看 Device2 的路由表。

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS
```

```
Gateway of last resort is not set
```

```
O 2.0.0.0/24 [110/2] via 1.0.0.1, 19:19:10, vlan2
O 38.1.1.1/32 [110/2] via 1.0.0.1, 19:09:43, vlan2
O 40.1.1.1/32 [110/3] via 1.0.0.1, 18:56:49, vlan2
```

#查看 Device3 的路由表。

```
Device3#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS
```

```
Gateway of last resort is not set
```

```
O 1.0.0.0/24 [110/2] via 2.0.0.1, 19:17:33, vlan2
O 38.1.1.1/32 [110/2] via 2.0.0.1, 19:09:59, vlan2
O 39.1.1.1/32 [110/3] via 2.0.0.1, 19:12:06, vlan2
```

配置完成后，Device1 分别与 Device2、Device3 之间能建立 OSPF 邻居，并互相学习到对方 Loopback 路由。

步骤 4： 配置 BGP。

#配置 Device1。

配置 Device1 分别与 Device2、Device3 之间使用 Loopback 接口地址建立 IBGP 邻居，并将路由 120.1.1.0/24、130.1.1.0/24 通告到 BGP 路由表中。

```
Device1(config)#router bgp 100
Device1(config-bgp)#neighbor 39.1.1.1 remote-as 100
Device1(config-bgp)#neighbor 39.1.1.1 update-source loopback0
Device1(config-bgp)#neighbor 40.1.1.1 remote-as 100
Device1(config-bgp)#neighbor 40.1.1.1 update-source loopback0
Device1(config-bgp)#network 120.1.1.0 255.255.255.0
Device1(config-bgp)#network 130.1.1.0 255.255.255.0
Device1(config-bgp)#exit
```

#配置 Device2。

```
Device2(config)#router bgp 100
Device2(config-bgp)#neighbor 38.1.1.1 remote-as 100
Device2(config-bgp)#neighbor 38.1.1.1 update-source loopback0
Device2(config-bgp)#neighbor 38.1.1.1 next-hop-self
Device2(config-bgp)#neighbor 3.0.0.2 remote-as 200
Device2(config-bgp)#exit
```

#配置 Device3。

```
Device3(config)#router bgp 100
Device3(config-bgp)#neighbor 38.1.1.1 remote-as 100
Device3(config-bgp)#neighbor 38.1.1.1 update-source loopback0
Device3(config-bgp)#neighbor 38.1.1.1 next-hop-self
Device3(config-bgp)#neighbor 4.0.0.2 remote-as 200
Device3(config-bgp)#exit
```

#配置 Device4。

配置 Device4 分别与 Device2、Device3 之间建立 EBGP 邻居，并将路由 100.1.1.0/24、110.1.1.0/24 通告到 BGP 路由表中。

```
Device4#configure terminal
Device4(config)#router bgp 200
Device4(config-bgp)#neighbor 3.0.0.1 remote-as 100
Device4(config-bgp)#neighbor 4.0.0.1 remote-as 100
Device4(config-bgp)#network 100.1.1.0 255.255.255.0
Device4(config-bgp)#network 110.1.1.0 255.255.255.0
Device4(config-bgp)#exit
```

#查看 Device1 的 BGP 路由信息。

```
Device1#show ip bgp
BGP table version is 2, local router ID is 38.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop        Metric LocPrf Weight Path
[B]*>i100.1.1.0/24  39.1.1.1         0  100  0 200 i
[B]* i            40.1.1.1         0  100  0 200 i
[B]*>i110.1.1.0/24  39.1.1.1         0  100  0 200 i
[B]* i            40.1.1.1         0  100  0 200 i
[B]*> 120.1.1.0/24  0.0.0.0          0   32768 i
[B]*> 130.1.1.0/24  0.0.0.0          0   32768 i
```

#查看 Device1 的路由表。

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

B 100.1.1.0/24 [200/0] via 39.1.1.1, 19:03:19, vlan2
B 110.1.1.0/24 [200/0] via 39.1.1.1, 19:03:19, vlan2
```

从 Device1 的 BGP 路由表中可以看出，到 100.1.1.0/24 网段和 110.1.1.0/24 网段的数据分别有两条有效路由，因为 Device2 的路由器 ID 小，所以到 100.1.1.0/24 网段和 110.1.1.0/24 网段的数据 BGP 缺省都选择了经过 Device2 到达。

#查看 Device4 的 BGP 路由信息。

```
Device4#show ip bgp
BGP table version is 3, local router ID is 110.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop        Metric LocPrf Weight Path
[B]*> 100.1.1.0/24  0.0.0.0          0   32768 i
[B]*> 110.1.1.0/24  0.0.0.0          0   32768 i
[B]* 120.1.1.0/24  4.0.0.1          0     0 100 i
[B]*>              3.0.0.1          0     0 100 i
```

单播路由

```
[B]* 130.1.1.0/24 4.0.0.1 0 0 100 i
[B]*> 3.0.0.1 0 0 100 i
```

#查看 Device4 的路由表。

```
Device4#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

B 120.1.1.0/24 [20/0] via 3.0.0.1, 19:25:05, vlan3
B 130.1.1.0/24 [20/0] via 3.0.0.1, 19:25:05, vlan3
```

从 Device4 的 BGP 路由表中可以看出，到 120.1.1.0/24 网段和 130.1.1.0/24 网段的数据分别有两条有效路由，因为配置时 Device4 先和 Device2 建立邻居，从 Device2 学到这两条路由的时间长一些，所以到 120.1.1.0/24 网段和 130.1.1.0/24 网段的数据 BGP 缺省都选择了经过 Device2 到达。

步骤 5：配置前缀列表和路由策略。

#配置 Device2。

配置前缀列表，允许 100.1.1.0/24、130.1.1.0/24 的路由通过。

```
Device2(config)#ip prefix-list 1 permit 100.1.1.0/24
Device2(config)#ip prefix-list 2 permit 130.1.1.0/24
```

配置路由策略 Ip，使 Device2 对匹配编号为 1 的前缀列表允许的路由设置 local-preference 属性。

```
Device2(config)#route-map Ip 10
Device2(config-route-map)#match ip address prefix-list 1
Device2(config-route-map)#set local-preference 200
Device2(config-route-map)#exit
Device2(config)#route-map Ip 20
Device2(config-route-map)#exit
```

配置路由策略 med，使 Device2 对匹配编号为 2 的前缀列表允许的路由设置 MED 属性。

```
Device2(config)#route-map med 10
Device2(config-route-map)#match ip address prefix-list 2
Device2(config-route-map)#set metric 10
Device2(config-route-map)#exit
Device2(config)#route-map med 20
Device2(config-route-map)#exit
```

#配置 Device3。

配置前缀列表，允许 110.1.1.0/24、120.1.1.0/24 的路由通过。

```
Device3(config)#ip prefix-list 1 permit 110.1.1.0/24
Device3(config)#ip prefix-list 2 permit 120.1.1.0/24
```

配置路由策略 Ip，使 Device3 对匹配编号为 1 的前缀列表允许的路由设置 local-preference 属性。

```
Device3(config)#route-map Ip 10
Device3(config-route-map)#match ip address prefix-list 1
Device3(config-route-map)#set local-preference 200
Device3(config-route-map)#exit
```

单播路由

```
Device3(config)#route-map lp 20
Device3(config-route-map)#exit
```

配置路由策略 med，使 Device3 对匹配编号为 2 的前缀列表允许的路由设置 MED 属性。

```
Device3(config)#route-map med 10
Device3(config-route-map)# match ip address prefix-list 2
Device3(config-route-map)#set metric 10
Device3(config-route-map)#exit
Device3(config)#route-map med 20
Device3(config-route-map)#exit
```

说明：

- 配置路由策略时，前缀列表和 ACL 都可以创建匹配规则，它们的区别在于前缀列表可以精确匹配路由掩码，而 ACL 则不能匹配路由掩码。
-

步骤 6： 配置 BGP 关联路由策略。

#配置 Device2。

应用路由策略 lp 到邻居 38.1.1.1 的出方向路由上，应用路由策略 med 到邻居 3.0.0.2 的出方向路由上。

```
Device2(config)#router bgp 100
Device2(config-bgp)#neighbor 38.1.1.1 route-map lp out
Device2(config-bgp)#neighbor 3.0.0.2 route-map med out
Device2(config-bgp)#exit
```

#配置 Device3。

应用路由策略 lp 到邻居 38.1.1.1 的出方向路由上，应用路由策略 med 到邻居 4.0.0.2 的出方向路由上。

```
Device3(config)#router bgp 100
Device3(config-bgp)#neighbor 38.1.1.1 route-map lp out
Device3(config-bgp)#neighbor 4.0.0.2 route-map med out
Device3(config-bgp)#exit
```

步骤 7： 检验结果。

#查看 Device1 的 BGP 路由信息。

```
Device1#show ip bgp
BGP table version is 9, local router ID is 38.1.1.1
```

```
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Network      Next Hop      Metric LocPrf Weight Path
[B]* i100.1.1.0/24 40.1.1.1      0 100 0 200 i
[B]*>i      39.1.1.1      0 200 0 200 i
[B]*>i110.1.1.0/24 40.1.1.1      0 200 0 200 i
[B]* i      39.1.1.1      0 100 0 200 i
[B]*> 120.1.1.0/24 0.0.0.0       0 32768 i
[B]*> 130.1.1.0/24 0.0.0.0       0 32768 i
```

#查看 Device1 的路由表。

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

B 100.1.1.0/24 [200/0] via 39.1.1.1, 02:58:12, vlan2
B 110.1.1.0/24 [200/0] via 40.1.1.1, 02:58:10, vlan3
```

从 Device1 的 BGP 路由表中可以看出，路由 100.1.1.0/24 有两个下一跳，分别是 40.1.1.1 和 39.1.1.1，而下一跳为 39.1.1.1 的路由本地优先级变成了 200，从而到 100.1.1.0/24 网段的数据优选了经过 Device2 到达；路由 110.1.1.0/24 也存在两个下一跳，分别是 40.1.1.1 和 39.1.1.1，而下一跳为 40.1.1.1 的路由本地优先级变成了 200，从而到 110.1.1.0/24 网段的数据优选了经过 Device3 到达。

#查看 Device4 的 BGP 路由信息。

```
Device4#show ip bgp
BGP table version is 9, local router ID is 110.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Network      Next Hop      Metric LocPrf Weight Path
[B]*> 100.1.1.0/24 0.0.0.0       0 32768 i
[B]*> 110.1.1.0/24 0.0.0.0       0 32768 i
[B]* 120.1.1.0/24 4.0.0.1       10 0 100 i
[B]*>      3.0.0.1       0 0 100 i
[B]*> 130.1.1.0/24 4.0.0.1       0 0 100 i
[B]*      3.0.0.1       10 0 100 i
```

#查看 Device4 的路由表。

```
Device4#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

B 120.1.1.0/24 [20/0] via 3.0.0.1, 03:05:39, vlan3
B 130.1.1.0/24 [20/0] via 4.0.0.1, 03:05:37, vlan4
```

从 Device4 的 BGP 路由表中可以看出，路由 120.1.1.0/24 有两个下一跳，分别是 4.0.0.1 和 3.0.0.1，而下一跳为 4.0.0.1 的路由 metric 变成了 10，从而到 120.1.1.0/24 网段的数据优选了经过 Device2 到达；路由 130.1.1.0/24 也存在有两个下一跳，分别是 4.0.0.1 和 3.0.0.1，而下一跳为 3.0.0.1 的路由 metric 变成了 10，从而到 130.1.1.0/24 网段的数据优选了经过 Device3 到达。

说明:

- BGP 对等体或对等体组应用路由策略时, 可以使用在对等体或对等体组的接收或通告方向, 重置 BGP 后生效。
-

QoS

48 硬件 QoS

48.1 硬件 QoS 简介

48.1.1 背景

在传统的 IP 网络中，转发设备对所有需要转发的报文都是无区分的同等对待，采用先入先出（FIFO）的策略进行处理，尽最大的努力（Best-Effort）将报文送达到目的地，因此传送报文的可靠性、传输延迟等性能没有任何保证。

然而，随着 IP 网络的发展，基于 IP 网络的新应用也是层出不穷，这样对 IP 网络的服务质量也就提出了新的要求，特别是实时性要求比较高的业务报文的需求更为明显，例如网络流媒体、VoIP 语音等实时业务就对报文的传输延迟提出了较高要求，如果报文传输延时太长，用户将不能接受（相对而言，E-Mail 和 FTP 等业务对传输延迟并不敏感）。为了支持具有不同服务质量需求的通信业务，就要求网络能够智能地区分出不同的通信类别，进而为之提供相应的服务。而具备通信类别的区分能力正是为不同的通信提供不同服务质量的基本前提，所以说传统 IP 网络的尽力服务模式已不能满足现如今 IP 网络应用的需要。QoS（Quality of Service）技术的出现便致力于解决这个问题，以满足用户对网络的不同服务质量需求。

48.1.2 服务模型

通常 QoS 提供以下三种服务模型，即 Best-Effort service（尽力而为服务模型）、Integrated service（综合服务模型，简称 IntServ）、Differentiated service（区分服务模型，简称 DiffServ）。

Best-Effort 是一种单一的服务模型，也是最简单的服务模型。应用程序可以在任何时候，发出任意数量的报文，而且不需要获得批准，也不需要事先通知网络。对于 Best-Effort 服务，网络将尽最大的可能性来发送报文，但对报文的传输时延、可靠性等性能不提供任何保证。Best-Effort 服务是现在 Internet 的缺省服务模型，它适用于绝大多数网络应用，如 FTP、E-Mail 等，它通过 FIFO 队列机制来实现。

IntServ 是一种可以提供多种服务类别的服务模型，它可以满足多种 QoS 需求。这种服务模型在发送报文前，需要向网络申请特定的服务资源，这个请求是通过 RSVP 信令来完成的。RSVP 是在应用程序开始发送报文之前为该应用申请网络资源的，所以属于带外信令。应用程序在发送数据之前，首先通知网络它自己的流量参数和需要的特定服务质量请求，包括带宽、时延等。网络在收到应用程序的资源请求后，执行资源分配检查，即基于应用程序的资源申请和网络现有的资源情况，判断是否为应用程序分配资源。一旦网络确认为该应用程序分配资源，网络将为该特定的流（Flow，由两端的 IP 地址、端口号、协议号确定）维护一个状态，并基于这个状态执行报文的分类、流量监管、排队及调度。应用程序在收到网络的确认信息（即确认网络已经为这个应用程序的报文预留了资源）后，才可以发送报文。只要应用程序的报文控制在流量参数描述的范围内，网络将承诺满足应用程序的 QoS 需求。

DiffServ 是一种根据服务要求对通信进行分类，而后根据分类结果对流入或流出的报文进行不同的处理，以保证网络始终处于较好的通信连接状态。它是一种多通道服务模型，可以满足不同流的 QoS 请求。与 IntServ 最大的不同在于，区分服务不需要信令交互而达到在网络中预留资源的效果，它仅仅是作用于网络中某一个传输设备的某个端口上，对于流入或流出该端口的报文进行处理。对于区分服务而言，不需要为每一类通信维护状态信息，它根据配置好的 QoS 机制来区分每个报文的 QoS 级别并根据该级别为此报文提供服务。因此，有时也将提供此种 QoS 方案的机制称作 CoS。分类方法颇多，其常用的方式如：根据 IP 报文的优先级分类、根据报文的源、目的地址和端口分类、根据报文的协议分类、根据报文的大小、报文的入端口分类等。

优先级映射、流分类、流量监管、流量整形、拥塞管理和拥塞避免是构成区分服务的主要组成部件。流分类根据一定的匹配规则识别报文，是区分服务的基础和前提；而流量监管、流量整形、拥塞管理和拥塞避免从不同方面对网络流量进行资源分配和调度，是 DiffServ 服务思想的具体体现。

48.1.3 QoS 功能组成介绍

-B -S -E -A

优先级映射

优先级映射分入方向的映射和出方向的映射，入方向的映射是根据报文中的 802.1p 优先级和 DSCP 值映射到本地优先级（LP）；出方向的映射是根据报文的本地优先级（LP）映射到 802.1p 优先级和 DSCP 值。优先级映射是为队列调度和拥塞控制服务的。

设备支持六类优先级映射：报文的 DSCP 映射到本地优先级（LP）；报文入方向的 DSCP 值映射到报文出方向的 DSCP 值；报文的 802.1p 优先级映射到本地优先级（LP）；报文的 802.1p 优先级映射到出方向的 DSCP 值；报文的本地优先级（LP）映射到报文出方向的 802.1p 优先级；报文的本地优先级（LP）映射到报文出方向的 DSCP 值。优先级映射关系图如下：

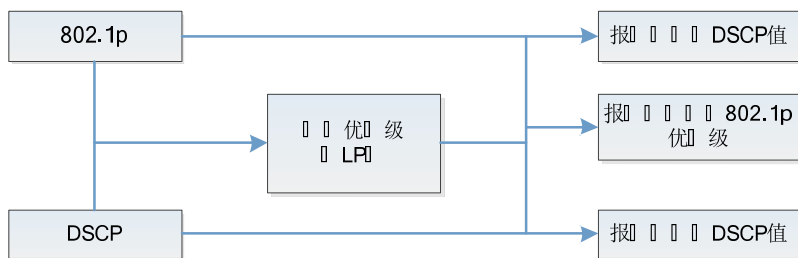


图 48-1 优先级映射关系图

流分类

流分类指采用一定的规则进行识别符合某类特征的报文，将满足不同特征的报文分为多个类别，然后利用相应的 QoS 机制对不同的类别提供不同的服务，因此流分类是提供不同服务的前提和基础。

流分类包括计数器、计量器、流镜像、重定向和重标记。

计数器和计量器分别是根据流分类的结果做计数和计量动作。

流镜像是将匹配的报文镜像到指定的端口。

重定向是将匹配的报文重定向到指定的端口或者指定的下一跳。

重标记指设置或者修改某一类报文的属性。通过流分类将报文分成了不同的类别后，重标记可以修改报文的属性，为后续对报文的处理作准备。

流量监管

流量监管通过令牌桶为进入端口的报文进行限速，为了保证流经网络的信息流量不出现过载并造成拥塞，设备提供了基于端口接收方向的速率限制，对端口接收方向上的总速率进行限制，超速流量将被丢弃。

流量整形

流量整形的典型作用是限制流出某一网络的流量，使报文以比较均匀的速率发送，通常分为端口的流量整形和队列的流量整形。当报文的发送速率超过整形的速率时，超速报文就暂时缓存在队列中，然后再以均匀的速率将这些报文发送出去。流量整形与流量监管的主要区别在于：利用流量监管进行报文流量控制时，对超速报文不会缓存，直接进行丢弃；而流量整形对于超速报文则进行缓存，减少了由突发流量造成的报文丢弃。但流量整形可能增加延迟，而流量监管几乎不增加延迟。

拥塞管理

当设备流量负载比较轻时，不会产生拥塞，报文到达端口就被转发出去了；当报文到达的速率大于端口的发送速率，超过了端口的处理限制或者设备资源不足时，设备会发生拥塞。拥塞的严重后果是导致整个网络的通信变得不再可靠，用于衡量网络服务质量的端到端延迟、抖动和包丢失率都会增加。如果启用了拥塞管理特性，当发生拥塞时报文就在端口排队，等待端口转发。拥塞管理一般采用队列技术，端口会根据报文的优先级别和队列机制确定哪些报文应放置在哪些队列里，以及如何调度并转发报文。

常用的调度有严格优先级调度 SP、轮询调度 RR、加权轮询调度 WRR 和加权赤字轮询调度 WDRR。

SP (Strict-Priority) 队列调度，端口上一共有 8 个队列，编号 0~7，队列 7 优先级最高，队列 0 优先级最低；

RR (Round Robin) 队列调度，每个队列调度出队一个报文，就转到下一个队列调度；WRR (Weighted Round Robin) 队列调度，配置每个队列调度出一定数量的报文，就转下一个队列调度；

WDRR (Weighted Deficit Round Robin) 调度。是对 WRR 算法的一种改进。该算法基于两个变量：配额 (quantum) 和余额 (credit counter)，配额代表权重，以字节为单位，是可配置的参数，余额用来表示配额的积累和消耗情况，是状态参数，不可配置。初始状态下，每个队列的余额等于其配额，当队列每发送一个报文的时候，余额就减去这个报文的字节数，当余额低于 0 的时候就停止这个队列的调度。当所有队列都停止调度的时候就为所有队列补充配额。

拥塞避免

拥塞避免技术监视网络的通信负荷量，以便尽量在网络拥塞产生之前避免拥塞的发生。常用的技术是加权随机早期检测模式 WRED (Weighted Random Early Detection)。与尾部丢弃方法不同的是 WRED 会根据 DSCP 或 IP 优先级值来选择丢弃数据包，可以为不同服务类别的数据提供具有区分的性能特征，还能避免 TCP 的全局同步现象。

在 WRED 算法中，队列丢弃报文的开始点记为 DropStartPoint，丢弃的结束点记为 DropEndPoint。当队列平均长度位于 DropStartPoint 和 DropEndPoint 之间时，WRED 按其对应

的丢弃率随机丢弃报文，而当队列长度超过 DropEndPoint 时按 100%的概率丢弃。当队列长度小于 DropStartPoint 时，WRED 不对这类报文进行丢弃。

下图是 WRED 的原理示意图：

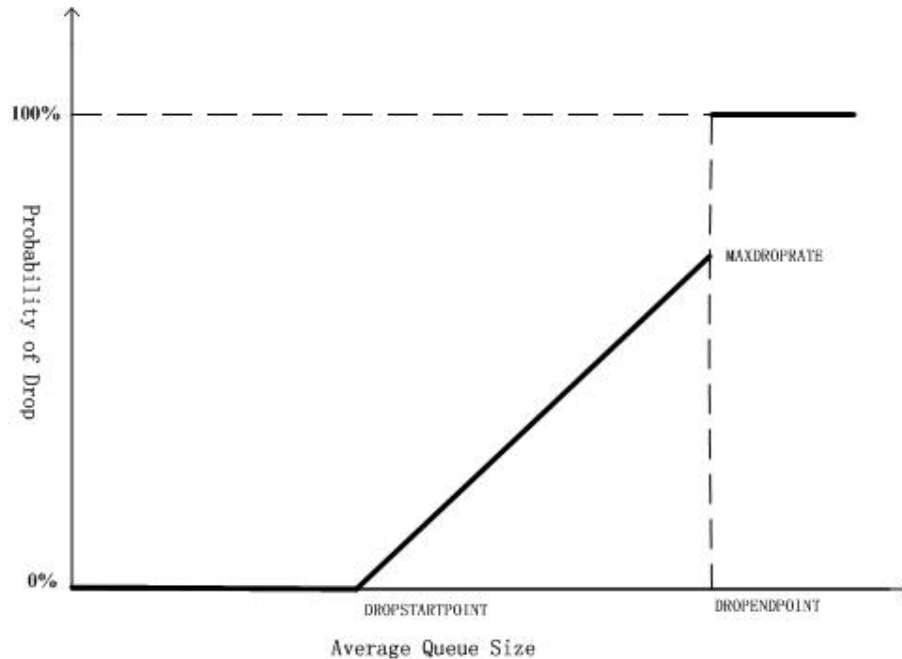


图 48-2 WRED 原理示意图

动作组功能

为了支持流分类和流量控制这样的应用，设备对传统的 ACL 进行了扩展，使 ACL 以及 ACL 规则都可以分别绑定一个动作组（Action Group），对匹配的报文采取相应的动作。动作组中包含计数器、计量器、流镜像、重定向和重标记方面的配置。

对各种 ACL 及 ACL 规则用于不同的作用域，各种动作组的配置不一样，对作用于入方向的 ACL，IP ACL 使用的动作组为 L3 动作组（l3-action-group），MAC ACL 使用的动作组为 L2 动作组（l2-action-group），作用于出方向的动作组（egr-action-group）用于 ACL 的出方向，VFP 动作组（vfp-action-group）用来实现基于流的 QinQ。每个 ACL 上可以同时绑定各种动作组，不过具体生效要看该 ACL 绑定的作用域，如：IP ACL 的一条规则上同时配置了 L3 动作组、出方向动作组和 VFP 动作组，这个 IP ACL 应用在入方向时，L3 动作组中的动作会生效，其他两个动作组中的动作不生效。

动作组中的策略路由是一种基于目的网络进行灵活路由的报文转发机制。策略路由是通过内容处理器（Content Aware Processor）对报文进行分类，并对符合分类规则的数据流按照指定的下一跳进行转发。当需要某些报文由其它路径而不是明确的最短路径路由时，就可以启用策略路由。策略路由的

优先级高于其他任何路由。所以一旦用户配置启用策略路由，报文发送就会先根据策略路由进行处理，只有访问列表匹配失败，才可能继续根据转发表查找结果进行转发；否则，根据路由策略指定的下一跳信息将报文转发出去。策略路由指定的下一跳应该为直连的下一跳。对于非直连的下一跳地址，虽然系统允许配置，实际上是无效的。

48.2 硬件 QoS 功能配置

表 48-1 硬件 QoS 功能配置列表

配置任务	
配置优先级映射	配置优先级映射
	配置缺省的优先级映射
配置流分类	配置计数器
	配置计量器
	配置流镜像
	配置重定向
	配置重标记 I2-priority
	配置重标记 I3-priority
配置流量监管	配置基于端口的速率限速
配置流量整形	配置基于队列的流量整形
	配置基于端口的流量整形
配置拥塞管理	配置端口队列的调度策略
配置拥塞避免	配置丢弃模式

配置任务	
配置 VFP 动作组	配置对单层 VLAN Tag 报文的处理
	配置对双层 VLAN Tag 报文的处理
	配置对不带 VLAN Tag 报文的处理
	配置在 VFP 动作组中绑定 VRF

48.2.1 配置优先级映射

-B -S -E -A

优先级映射是报文中的 802.1p 优先级、DSCP 值和本地优先级（LP）之间的相互映射，修改或者分配报文的优先级字段值，为拥塞避免和拥塞管理服务。

配置条件

无

配置优先级映射

优先级映射分入方向的映射和出方向的映射，入方向的映射是根据报文中的 802.1p 优先级和 DSCP 值映射到本地优先级（LP）；出方向映射是根据本地优先级（LP）映射到 802.1p 优先级和 DSCP 值。

表 48-2 配置优先级映射

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
配置优先级映射模板	qos map-table {ingress egress } <i>template-name</i>	必选 配置出方向和入方向的优先级模板
进入模板视图	{dot1p-dscp dot1p-lp dscp-dscp dscp-lp lp-dot1p lp-dscp } <i>index to value</i>	可选 缺省情况下，模板下优先级映射为默认映射关系
全局绑定优先级映射模板	map-table <i>template-name</i> { ingress egress }	必选 缺省情况下，未绑定优先级映射模板

说明：

- 对指定优先级报文进入相应的队列，最好不映射到第 7 队列，因为从 CPU 发出的报文都会进入第 7 队列，如果第 7 队列的报文太多，可能会丢掉 CPU 发出的报文。
- 模板下同时配置 dscp-lp 映射和 dot1p-lp 映射，dscp-lp 优先级要更高，优先生效。
- 配置 dscp-dscp 映射的任意一映射后，如果没有配置缺省的 dscp-dscp 优先级映射，模板下其他未配置 dscp-dscp 映射的表项都会映射到等值的 DSCP 值。如果配置了缺省的 dscp-dscp 映射值，未配置项都映射到缺省值。配置了 dscp-dscp 映射后会自动开启 dscp-lp 的映射，一旦模板上配置任意 dscp-lp 映射，未配置项会被分段映射到不同的本地优先级 (LP)，映射关系如下：DSCP 值 0~7 映射到本地优先级 (LP) 0，DSCP 值 8~15 映射到本地优先级 (LP) 1，依次类推。
- 开启入方向的 dot1p-lp 的映射后，转发报文的 802.1p 优先级不会根据本地优先级 (LP) 的值进行修改。如：dot1p-lp 的映射关系是 1 到 5，匹配入方向报文中的 VLAN Tag 的 802.1p 为 1 后，转发出去带 VLAN Tag 报文的 802.1p 优先级还是 1。
- 优先级映射对动作组重标记后的报文不生效。先在入方向的动作组重标记本地优先级 (LP)，然后在出方向通过本地优先级 (LP) 来映射到报文的 802.1p 优先级和 DSCP

值都是生效的。在入方向重标记 802.1p 优先级，然后通过 802.1p 优先级来映射本地优先级 (LP) 和 DSCP 值是不生效的，但重标记 802.1p 优先级本身是生效的。根据原始报文的 802.1p 优先级来映射也是生效的。也就是说重标记单独生效，优先级映射单独生效，根据重标记后的值来做优先级映射是不生效的。

- 同时在入方向配置 dscp-dscp 和在出方向配置 lp-dscp 映射，这两种映射以 lp-dscp 的映射生效为准。
- 端口上如果启用了 QinQ 功能，同时全局绑定的模板又包含了 dot1p-lp, dot1p-dscp, dscp-dscp 和 dscp-lp 映射，有可能不会得到用户想要的映射结果，因此建议用户不能在同一个端口上同时启用 QinQ 的同时全局绑定优先级映射功能。
- 配置 lp-dscp 映射后，lp-dscp 的默认映射是 0 映射到 0，1 映射到 8，2 映射到 16，3 映射到 24，4 映射到 32，5 映射到 40，6 映射到 48，7 映射到 56。

配置缺省的优先级映射

缺省的优先级映射和优先级映射一样，都有入方向的映射和出方向的映射。不同的是缺省的优先级映射把未配置优先级映射的表项都映射到缺省的值。

表 48-3 配置缺省的优先级映射

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置优先级映射模板	qos map-table {ingress egress} template-name	必选 配置出方向和入方向的优先级模板
配置缺省的优先级映射	{dot1p-dscp dot1p-lp dscp-dscp dscp-lp lp-dot1p lp-dscp} default value	必选 缺省情况下，未配置缺省的优先级映射

48.2.2 配置流分类

-B -S -E -A

流分类指采用一定的规则进行识别符合某类特征的报文，将满足不同特征的报文分为多个类别，然后利用相应的 QoS 机制对不同的类别提供不同的服务，因此流分类是提供不同服务的前提和基础。

配置条件

在配置流分类之前，首先完成以下任务：

- 配置 ACL。

配置计数器

在动作组中配置计数动作是为了对匹配的报文进行计数。

表 48-4 配置计数器

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 L3 动作组并进入 L3 动作组配置模式	l3-action-group <i>l3-action-group-name</i>	必选其一 进入 L3 动作组配置模式后，后续配置只在当前 L3 动作组中生效；进入 L2 动作组配置模式后，后续配置只在当前 L2 动作组中生效；进入出方向动作组配置模式后，后续配置只在当前出方向动作组中生效
配置 L2 动作组并进入 L2 动作组配置模式	l2-action-group <i>l2-action-group-name</i>	
配置出方向动作组并进入出方向动作组配置模式	egr-action-group <i>egr-action-group-name</i>	
配置计数器	count { all-colors green-other green-red green-yellow red-other red-yellow }	必选 缺省情况下，在动作组中不对报文进行计数

配置计量器

在动作组中配置绑定计量器是为了对匹配的报文进行限速或标记。配置不存在的计量器时，一旦指定的计量器配置完成则自动生效。当动作组没有配置计量器时，所有匹配的报文被当作绿色报文处理。当动作组中配置了计量器进行了报文着色后，会根据报文的流量将其分别标注为绿、黄两色，计数器才会对其进行分别计数。

表 48-5 配置计量器

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置计量器并进入计量器模式	traffic-meter <i>traffic-meter-name</i>	必选 缺省情况下，计量器中对黄色报文的动作为丢弃，未配置计量器模式 进入计量器配置后，一个完整的计量器配置包含黄色报文的计量器动作和计量器模式配置，不完整的配置不会生效
配置计量器的动作	meter action yellow { drop transmit [remark-dscp <i>dscp-value</i>] }	可选 缺省情况下，计量器中对黄色报文的动作为丢弃
配置计量器的模式	meter mode { srtcm <i>cir cbs ebs</i> trtcm <i>cir cbs pir pbs</i> }	必选 缺省情况下，未配置计量器的模式
进入全局配置模式	exit	-

步骤	命令	说明
配置 L3 动作组并进入 L3 动作组配置模式	l3-action-group <i>l3-action-group-name</i>	必选其一 进入 L3 动作组配置模式后，后续配置只在当前 L3 动作组中生效；进入 L2 动作组配置模式后，后续配置只在当前 L2 动作组中生效；进入出方向动作组配置模式后，后续配置只在当前出方向动作组中生效
配置 L2 动作组并进入 L2 动作组配置模式	l2-action-group <i>l2-action-group-name</i>	
配置出方向动作组并进入出方向动作组配置模式	egr-action-group <i>egr-action-group-name</i>	
配置绑定计量器	meter <i>traffic-meter-name</i>	必选 缺省情况下，未绑定任何计量器

说明：

- 在各对象上绑定的 ACL 如果配置有动作组，且在动作组上配置有用于限速的计量器（在限速应用时，对红黄报文的处理为丢弃），可能会存在冲突的限速动作。如：端口 0/1 属于 VLAN1，端口 0/1 上的 ACL 允许源 IP 地址 1.1.1.1 的报文通过，并配置将其流量限制 5Mbps 的动作。而 VLAN1 上的 ACL 允许 IP 地址为 1.1.1.1 的报文通过，并配置将其流量限制 1Mbps 的动作。对于这种情况，报文通路中的最小速率限制值将生效，速度被限制在 1Mbps。在此特别需要注意的是：由于硬件的限制，多级限速的实际流量会小于报文通路中的最小限速值。因此在需要精确限速的场合不推荐用户使用多级限速。
- 出方向动作组中的 meter 不支持 remark ip 和 remark dot1p-ip 动作。
- 计量器是基于芯片的，即每个芯片上的计量器限速这个芯片上的端口流量，如果计量器在链路汇聚下的端口分布在两个不同的芯片中，这时在每个芯片中都有一个计量器，这样限速的结果就是预想限速结果的 2 倍。
- 在 VLAN 对象上应用了计量器，该计量器对每个线卡上每块芯片生效。如在 VLAN 对象限速为 10M，如果设备上有 5 块单芯片的线卡，则该 10M 的流量是对一块线卡上

的流量起作用，也就是每块线卡上符合 VLAN 限速的流量都是 10M,, 如果其中一块线卡上有两块芯片，则该线卡上的每块芯片的流量为 10M。

配置流镜像

在动作组中配置流镜像动作是将匹配的报文镜像到指定的端口。

表 48-6 配置流镜像

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 L3 动作组并进入 L3 动作组配置模式	l3-action-group <i>l3-action-group-name</i>	必选其一 进入 L3 动作组配置模式
配置 L2 动作组并进入 L2 动作组配置模式	l2-action-group <i>l2-action-group-name</i>	后, 后续配置只在当前 L3 动作组中生效; 进入 L2 动作组配置模式后, 后续配置只在当前 L2 动作组中生效
配置流镜像	mirror interface <i>interface-name</i>	必选 缺省情况下, 未配置流镜像

配置重定向

在动作组中配置报文重定向动作是将匹配的报文重定向到指定的端口或者指定的下一跳。

表 48-7 配置重定向

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
配置 L3 动作组并进入 L3 动作组配置模式	I3-action-group <i>l3-action-group-name</i>	必选其一 进入 L3 动作组配置模式
配置 L2 动作组并进入 L2 动作组配置模式	I2-action-group <i>l2-action-group-name</i>	后, 后续配置只在当前 L3 动作组中生效; 进入 L2 动作组配置模式后, 后续配置只在当前 L2 动作组中生效
配置重定向	redirect { interface <i>interface-name</i> link- aggregation link- <i>aggregation-id</i> }	必选 缺省情况下, 未配置报文重定向

配置重标记 l2-priority

在动作组中配置报文重标记动作是为了对匹配的报文进行分类。以使用户在后续的数据通信中采取不同的 QoS 策略。

表 48-8 配置重标记 l2-priority

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 L3 动作组并进入 L3 动作组配置模式	I3-action-group <i>l3-action-group-name</i>	必选其一 进入 L3 动作组配置模式
配置 L2 动作组并进入 L2 动作组配置模式	I2-action-group <i>l2-action-group-name</i>	后, 后续配置只在当前 L3 动作组中生效; 进入 L2 动作组配置模式后, 后续配置只在当前 L2 动作组中生效
配置出方向动作组并进入出方向动作组配置模式	egr-action-group <i>egr-action-group-name</i>	置只在当前 L2 动作组中生效; 进入出方向动作组配

步骤	命令	说明
		置模式后, 后续配置只在当前出方向动作组中生效
配置重标记 l2-priority	remark l2-priority { dscp <i>dscp-value</i> {{ dot1p dot1p-lp lp } { <i>priority-value</i> precedence }}	必选 缺省情况下, 未配置重标记 l2-priority

配置重标记 l3-priority

在动作组中配置报文重标记动作是为了对匹配的报文进行分类。以使用户在后续的数据通信中采取不同的 QoS 策略。

表 48-9 配置重标记 l3-priority

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 L3 动作组并进入 L3 动作组配置模式	l3-action-group <i>l3-action-group-name</i>	必选其一 进入 L3 动作组配置模式后, 后续配置只在当前 L3 动作组中生效; 进入出方向动作组配置模式后, 后续配置只在当前出方向动作组中生效
配置出方向动作组并进入出方向动作组配置模式	egr-action-group <i>egr-action-group-name</i>	
配置重标记 l3-priority	remark l3-priority { dscp <i>dscp-value</i> precedence { <i>priority-value</i> dot1p }	必选 缺省情况下, 未配置重标记 l3-priority

说明:

- 在各对象上绑定的 ACL，如果配置有动作组，则可能会存在重标记冲突。如：端口 0/1 属于 VLAN1，端口 0/1 上的 ACL 允许源 IP 地址 1.1.1.1 的报文通过，并配置有重标记 DSCP 字段值为 5 的动作。而 VLAN1 上的 ACL 允许 IP 地址为 1.1.1.1 的报文通过，并重标记 DSCP 字段值为 4。对于这种情况，按端口 > VLAN > 全局以及 MAC ACL > IP ACL 的优先顺序进行处理，最终标记值为 5。
- 在各对象上绑定的 ACL 如果配置有动作组，可能会存在无冲突的重标记动作。如：端口 0/1 属于 VLAN1，端口 0/1 上的 ACL 允许源 IP 地址 1.1.1.1 的报文通过，并配置有重标记 DSCP 字段值为 5 的动作。而 VLAN1 上的 ACL 允许 IP 地址为 1.1.1.1 的报文通过，并重标记 802.1p 优先级为 4。对于这种无冲突的重标记动作，报文将会被标记 DSCP 为 5 的情况下同时标记 802.1p 优先级为 4。

48.2.3 配置流量监管

-B -S -E -A

为了保证流经网络的信息流量不出现过载并造成拥塞，设备提供了基于端口接收方向的速率限制，对端口接收方向上的总速率进行限制，超速流量将被丢弃。

配置条件

无

配置基于端口的速率限速

为满足不同时间段对端口提供不同的速率限制，每个端口可以配置 8 条不同优先级的速率限制，每条速率限制后可以绑定时间域，对同时生效的条目以优先级的级别来确定是哪条生效，优先级级别为 0 最高，7 优先级最低。对端口速率限制也能支持不带时间域，直接配置速率限制。

表 48-10 配置基于端口的速率限速

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
进入二/三层以太网接口配置模式	interface <i>interface-name</i>	-
配置基于端口的速率限制	rate-limit { default <i>rate</i> <i>burst-size</i> <i>priority</i> <i>rate</i> <i>burst-size</i> [time-range <i>time-range-name</i>] }	必选 缺省情况下，未配置端口的速率限制

48.2.4 配置流量整形

-B -S -E -A

流量整形使报文以比较均匀的速率发送出去。流量整形与流量监管的区别在于：流量监管在入方向生效，流量整形在出方向生效。在入方向超出的流量会被丢弃，而在出方向超出的流量会被缓存起来。

配置条件

无

配置基于队列的流量整形

基于队列的流量整形使队列上的流量以比较均匀的速率发送出去，可以根据需要在不同的队列上做不同的流量整形。

表 48-11 配置基于队列的流量整形

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二/三层以太网接口配置模式	interface <i>interface-name</i>	-
配置基于队列的流量整形	traffic-shape queue <i>queue-id</i> <i>cir</i> <i>cbs</i> <i>pir</i> <i>pbs</i>	必选

步骤	命令	说明
		缺省情况下，未配置基于队列的流量整形

配置基于端口的流量整形

基于端口的流量整形允许时间域的绑定，以达到不同时间段整形为不同带宽的目的。每个端口可以配置 8 条不同优先级的流量整形，每条流量整形可以绑定时间域，对同时生效的条目以优先级的级别来确定是哪条生效，优先级级别为 0 最高，优先级级别为 7 最低。

表 48-12 配置基于端口的流量整形

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太网接口配置模式	interface <i>interface-name</i>	-
配置基于端口的流量整形	traffic-shape { <i>rate burst-size</i> / <i>priority rate burst-size</i> [time-range <i>time-range-name</i>] }	必选 缺省情况下，未配置基于端口的流量整形

48.2.5 配置拥塞管理

-B -S -E -A

在比较复杂的网络中，拥塞是一种很常见的现象，主要是由于当前提供的带宽不能满足正常转发的需要导致的。发生拥塞会引起一系列的负面影响，如：会耗费大量的网络资源，导致系统崩溃；使网络的吞吐率降低，造成网络资源的利用率降低；增加报文传输的延迟和抖动。端口队列的调度策略是拥塞管理的一种方法。

配置条件

配置手册

发布 1.1 04/2020

无

配置端口队列的调度策略

基于队列的调度策略是用某种优先级别算法将之前分类好的流量发送出去。每种队列算法都是用以解决特定的网络流量问题，并对带宽资源的分配、延迟、抖动等有着十分重要的影响。队列调度对不同优先级的报文进行分级处理，优先级高的会得到优先发送。

常用的调度有严格优先级调度 SP、轮询调度 RR、加权轮询调度 WRR 和加权赤字轮询调度 WDRR。

SP (Strict-Priority) 队列调度，端口上一共有 8 个队列，编号 0~7，队列 7 优先级最高，队列 0 优先级最低；

RR (Round Robin) 队列调度，每个队列调度出队一个报文，就转到下一个队列调度；WRR (Weighted Round Robin) 队列调度，配置每个队列调度出一定数量的报文，就转下一个队列调度；

WDRR (Weighted Deficit Round Robin) 调度。是对 WRR 算法的一种改进。该算法基于两个变量：配额 (quantum) 和余额 (credit counter)，配额代表权重，以字节为单位，是可配置的参数，余额用来表示配额的积累和消耗情况，是状态参数，不可配置。初始状态下，每个队列的余额等于其配额，当队列每发送一个报文的时候，余额就减去这个报文的字节数，当余额低于 0 的时候就停止这个队列的调度。当所有队列都停止调度的时候就为所有队列补充配额。

表 48-13 配置端口队列的调度策略

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二/三层以太网接口配置模式	interface <i>interface-name</i>	-
配置端口队列的调度策略	queue-schedule { sp rr { wrr wdr } <i>weight0 weight1 weight2 weight3 weight4 weight5 weight6 weight7</i> }	必选 缺省情况下，端口队列的调度策略为严格优先级 (SP) 调度

48.2.6 配置拥塞避免

-B -S -E -A

拥塞避免技术是用来监视网络资源的使用情况和网络通信的负荷量，以便尽量在网络拥塞产生或有加剧趋势时，主动丢弃报文，避免拥塞的发生。过度的拥塞会对网络资源造成极大危害，必须采取某种措施加以解除，常用的措施是配置丢弃模式。

配置条件

无

配置丢弃模式

常用的丢弃模式有：尾部丢弃（tail-drop）模式和加权随机早期检测 WRED（Weighted Random Early Detection）模式。

尾部丢弃模式（tail-drop）：传统的丢包策略，当队列的长度达到最大值后，所有新到来的报文都将被丢弃。这种丢弃策略会引发 TCP 全局同步现象，当队列同时丢弃多个 TCP 连接的报文时，将造成多个 TCP 连接同时进入拥塞避免和慢启动状态以降低并调整流量，而后又会在某个时间同时出现流量高峰。如此反复，使网络流量忽大忽小，网络不停震荡。

加权随机早期检测 WRED（Weighted Random Early Detection）模式：当队列的长度超过队列本身长度时按 100% 的概率丢弃。当队列长度小于 start-value 时，不对报文进行丢弃。当队列的长度大于 start-value 时按照配置的值随机丢弃。WRED 生成的随机数是基于优先权的，它引入 IP 优先权区别丢弃策略，考虑了高优先权报文的利益，使高优先权的报文被丢弃的概率相对较小。

表 48-14 配置丢弃模式

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太网接口配置模式	interface <i>interface-name</i>	-
配置丢弃模式	drop-mode <i>cos-value</i> { tail-drop wred drop-	必选

步骤	命令	说明
	start start-value drop-rate drop-rate-value [only-tcp all] }	缺省情况下，端口队列的丢弃模式为尾部丢弃模式 (tail-drop)

48.2.7 配置 VFP 动作组 **-B -S -E -A**

VFP (VLAN Filter Processor) 动作组是对报文进行分类，重新指定单层 VLAN Tag 报文，双层 VLAN Tag 和不带 VLAN Tag 报文的动作。

配置条件

在配置 VFP 动作组之前，首先完成以下任务：

- 配置 ACL。

配置对单层 VLAN Tag 报文的处理

在 VFP 动作组中配置对单层 VLAN Tag 报文的处理，主要是对 VLAN Tag 中的 802.1p 优先级和 VLAN 编号的匹配和处理。

表 48-15 配置对单层 VLAN Tag 报文的处理

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 VFP 动作组并进入 VFP 动作组配置模式	vfp-action-group <i>vfp-action-group-name</i>	必选 缺省情况下，未配置 VFP 动作组
配置对单层 VLAN Tag 报文的处理	one-tag { match-vlan { any <i>vlan-id</i> } ovlan-act { add-ovlan <i>vlan-id</i>	必选 缺省情况下，未配置对单层 VLAN Tag 报文的处理

步骤	命令	说明
	[priority <i>priority-value</i>] replace-vlan <i>vlan-id</i> }	

配置对双层 VLAN Tag 报文的处理

在 VFP 动作组中配置对双层 VLAN Tag 报文的处理，主要是对内层和外层 VLAN Tag 中的 802.1p 优先级和 VLAN 编号的匹配和处理。

表 48-16 配置对双层 VLAN Tag 报文的处理

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 VFP 动作组并进入 VFP 动作组配置模式	vfp-action-group <i>vfp-action-group-name</i>	必选 缺省情况下，未配置 VFP 动作组
配置对双层 VLAN Tag 报文的处理	double-tag { invlan-act { delete-invlan replace-invlan <i>vlan-id</i> } match-invlan { any <i>vlan-id</i> } match-ovlan { any <i>vlan-id</i> } ovlan-act replace-ovlan <i>vlan-id</i> }	必选 缺省情况下，未配置对双层 VLAN Tag 报文的处理

配置对不带 VLAN Tag 报文的处理

在 VFP 动作组中配置对不带 VLAN Tag 报文的处理，主要是配置添加内层和外层 VLAN Tag 的动作。

表 48-17 配置对不带 VLAN Tag 报文的处理

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 VFP 动作组并进入 VFP 动作组配置模式	vfp-action-group <i>vfp-action-group-name</i>	必选 缺省情况下，未配置 VFP 动作组
配置对不带 VLAN Tag 报文的处理	untag { invlan-act add- invlan <i>vlan-id</i> } ovlan- act add-ovlan <i>vlan-id</i>	必选 缺省情况下，未配置对不带 VLAN Tag 报文的处理

配置在 VFP 动作组中绑定 VRF

表 48-18 配置在 VFP 动作组中绑定 VRF

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 VFP 动作组并进入 VFP 动作组配置模式	vfp-action-group <i>vfp-action-group-name</i>	必选 缺省情况下，未配置 VFP 动作组
配置在 VFP 动作组中绑定 VRF	vrfset <i>vrf-name</i>	必选 缺省情况下，未在 VFP 动作组中绑定 VRF

表 48-19 硬件 QoS 监控与维护

命令	说明
show drop-mode [interface <i>interface-name</i>]	显示端口队列的丢弃模式
show egr-action-group [<i>egr-action-group-name</i>]	显示出方向动作组的相关配置信息
show l2-action-group [<i>l2-action-group-name</i>]	显示 L2 动作组的相关配置信息
show l3-action-group [<i>l3-action-group-name</i>]	显示 L3 动作组的相关配置信息
show map-table user-name [<i>template name</i> { ingress egress }]	显示优先级映射模板信息
show queue-schedule [interface <i>interface-name</i>]	显示端口队列的调度策略
show rate-limit [interface <i>interface-name</i>]	显示端口上的速率限制信息
show traffic-count { inst-all inst-global { inst-interface <i>interface-name</i> / inst-interface-vlan <i>vlan-id</i> / inst-link-aggregation <i>link-aggregation-id</i> } { ip-in ip-out mac-in mac-out } inst-vlan <i>vlan-id</i> { ip-in ip-out } }	显示应用到指定对象上的 ACL 的计数器信息

命令	说明
show traffic-meter [<i>traffic-meter-name</i>]	显示计量器的所有信息
show traffic-shape [interface <i>interface-name</i>]	显示端口及队列上的流量整形信息
show vfp-action-group [<i>vfp-action-group-name</i>]	显示 VFP 动作组的相关配置信息

48.3 硬件 QoS 典型配置举例

48.3.1 配置优先级映射

-B -S -E -A

网络需求

- 网络中有两台服务器，分别是视频服务器（Video Server）和数据服务器（Data Server）；
- 视频流量报文中的 DSCP 值为 34，数据流量报文中的 DSCP 值为 38；
- 配置优先级映射功能，实现视频流量报文的 802.1p 优先级为 5，数据流量报文的 802.1p 优先级为 1。

网络拓扑

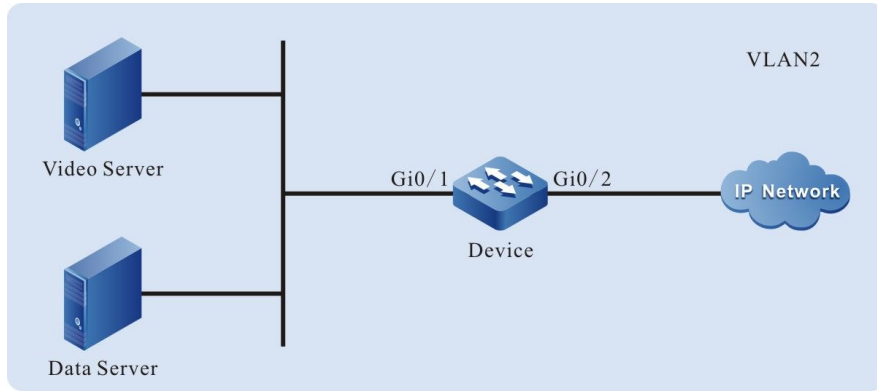


图 48-3 配置优先级映射组网图

配置步骤

- 步骤 1: 在 Device 上配置 VLAN 和端口的链路类型。

#创建 VLAN2。

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#配置端口 gigabitethernet0/1 的链路类型为 Access，允许 VLAN2 的业务通过。

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
```

#配置端口 gigabitethernet0/2 的链路类型为 Trunk，允许 VLAN2 的业务通过。

```
Device(config-if-gigabitethernet0/1)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode trunk
Device(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 2
Device(config-if-gigabitethernet0/2)#exit
```

- 步骤 2: 配置优先级映射功能。

#全局配置优先级映射功能，将 DSCP 值为 34 的报文映射到 2 队列，将 DSCP 值为 38 的报文映射到 3 队列。

```
Device(config)#qos map-table ingress a
Device(config-mactable-ingress)#dscp-lp 34 to 2
Device(config-if-gigabitethernet0/1)# dscp-lp 38 to 3
```

#全局配置优先级映射功能，将 2 队列报文的 802.1p 优先级映射为 5，将 3 队列报文的 802.1p 优先级映射为 1。

```
Device(config)#qos map-table egress b
```

```
Device(config-mactable-egress)#lp-dot1p 2 to 5
Device(config- mactable-egress)# lp-dot1p 3 to 1
```

#全局绑定模板

```
Device(config)#map-table a ingress
Device(config)#map-table b egress
```

#端口上配置信任

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#qos map-table trust dscp ingress
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#qos map-table trust dot1p egress
```

- 步骤 3: 检验结果。

#视频流量和数据流量经过 Device 处理后，从端口 gigabitethernet0/2 发出的视频流量报文的 802.1p 优先级为 5，数据流量报文的 802.1p 优先级为 1。

48.3.2 配置重标记

-B -S -E -A

网络需求

- 网络中有两台服务器，分别是视频服务器（Video Server）和数据服务器（Data Server）；
- 配置重标记功能，实现标记视频流量报文的 802.1p 优先级为 5，数据流量报文的 802.1p 优先级不变。

网络拓扑

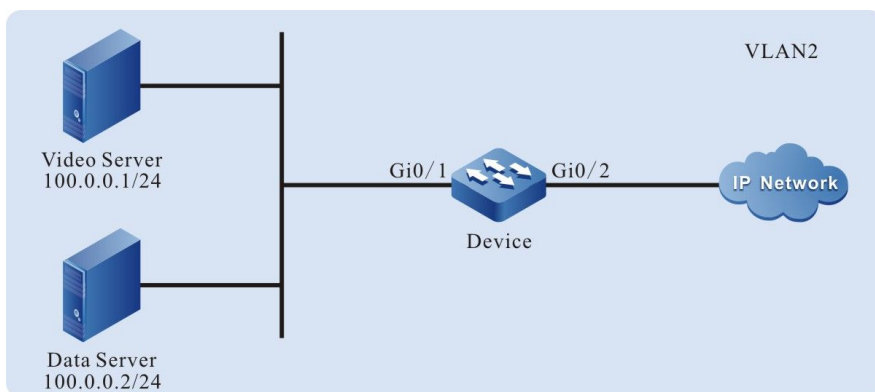


图 48-4 配置重标记组网图

配置步骤

- 步骤 1: 在 Device 上配置 VLAN 和端口的链路类型。

#创建 VLAN2。

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#配置端口 gigabitethernet0/1 的链路类型为 Access，允许 VLAN2 的业务通过。

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
```

#配置端口 gigabitethernet0/2 的链路类型为 Trunk，允许 VLAN2 的业务通过。

```
Device(config-if-gigabitethernet0/1)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode trunk
Device(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 2
Device(config-if-gigabitethernet0/2)#exit
```

- 步骤 2: 配置 L3 动作组。

#配置名称为 remark 的 L3 动作组，动作为重标记报文的 802.1p 优先级为 5。

```
Device(config)#l3-action-group remark
Device(config-action-group)#remark l2-priority dot1p 5
Device(config-action-group)#exit
```

- 步骤 3: 配置 IP 标准 ACL。

#在 Device 上配置编号为 1 的 IP 标准 ACL。

```
Device(config)#ip access-list standard 1
```

#配置规则与名称为 remark 的 L3 动作组绑定，实现重标记视频流量报文的 802.1p 优先级为 5。

```
Device(config-std-nacl)#permit host 100.0.0.1 l3-action-group remark
```

#配置规则，允许数据流量通过，并且不修改其报文的 802.1p 优先级。

```
Device(config-std-nacl)#permit host 100.0.0.2
Device(config-std-nacl)#exit
```

- 步骤 4: 配置应用 IP 标准 ACL。

#将编号为 1 的 IP 标准 ACL 应用于 Device 端口 gigabitethernet0/1 入方向。

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#ip access-group 1 in
Device(config-if-gigabitethernet0/1)#exit
```

#在 Device 上查看 ACL 应用于端口的信息。

```
Device#show acl-object interface
-----Interface-----Bind-----Instance-----
Interface-----Direction----AclType----AclName
gi0/1             IN      IP      1
```

- 步骤 5: 检验结果。

#视频流量和数据流量经过 Device 处理后，从端口 gigabitethernet0/2 发出的视频流量报文的 802.1p 优先级被修改为 5，数据流量报文的 802.1p 优先级保持不变。

48.3.3 配置流量整形 **-B -S -E -A**

网络需求

- 网络中有两台服务器，分别是视频服务器（Video Server）和数据服务器（Data Server）；
- 配置流量整形功能，保障视频流量速率为 20000kbps 但最大不能超过 20000kbps，视频流量速率和数据流量速率总和不超过 50000kbps。当视频流量速率大于 20000kbps 时，要限制视频流量速率为 20000kbps；当视频流量速率小于 20000kbps 时，剩余带宽可以被数据流量占用。

网络拓扑

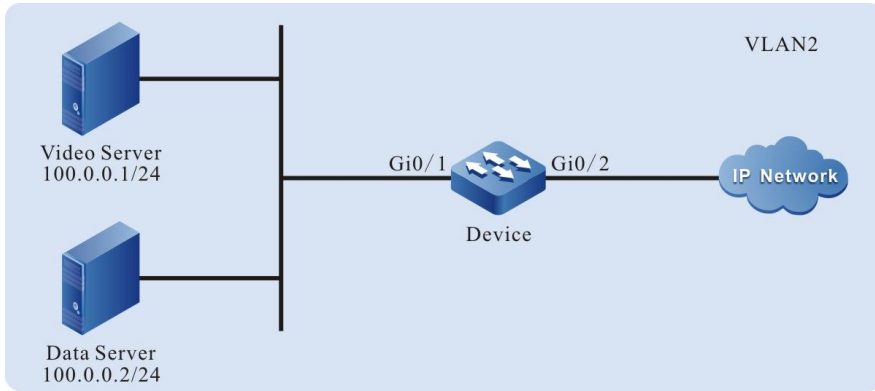


图 48-5 配置流量整形组网图

配置步骤

- 步骤 1: 在 Device 上配置 VLAN 和端口的链路类型。

#创建 VLAN2。

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#配置端口 gigabitethernet0/1 的链路类型为 Access，允许 VLAN2 的业务通过。

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
```

#配置端口 gigabitethernet0/2 的链路类型为 Trunk，允许 VLAN2 的业务通过。

```
Device(config-if-gigabitethernet0/1)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode trunk
Device(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 2
Device(config-if-gigabitethernet0/2)#exit
```

- 步骤 2: 配置 L3 动作组。

#配置名称为 LP7 的 L3 动作组，动作为重标记报文入 7 队列。

```
Device(config)#l3-action-group LP7
Device(config-action-group)#remark l2-priority 1p 7
Device(config-action-group)#exit
```

#配置名称为 LP6 的 L3 动作组，动作为重标记报文入 6 队列。

```
Device(config)#l3-action-group LP6
Device(config-action-group)#remark l2-priority 1p 6
Device(config-action-group)#exit
```

- 步骤 3: 配置 IP 标准 ACL。

#在 Device 上配置编号为 1 的 IP 标准 ACL。

```
Device(config)#ip access-list standard 1
```

#配置规则与名称为 LP7 的 L3 动作组绑定，实现重标记视频流量报文入 7 队列。

```
Device(config-std-nacl)#permit host 100.0.0.1 l3-action-group LP7
```

#配置规则与名称为 LP6 的 L3 动作组绑定，实现重标记数据流量报文入 6 队列。

```
Device(config-std-nacl)#permit host 100.0.0.2 l3-action-group LP6
Device(config-std-nacl)#exit
```

- 步骤 4: 配置应用 IP 标准 ACL。

#将编号为 1 的 IP 标准 ACL 应用于 Device 端口 gigabitethernet0/1 入方向。

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#ip access-group 1 in
Device(config-if-gigabitethernet0/1)#exit
```

#在 Device 上查看 ACL 应用于端口的信息。

```
Device#show acl-object interface
-----Interface-----Bind-----Instance-----
Interface-----Direction-----AclType----AclName
gi0/1             IN      IP      1
```

- 步骤 5: 配置流量整形功能。

#在端口 gigabitethernet0/2 上配置基于队列的流量整形，7 队列流量限速为 20000kbps。

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#traffic-shape queue 7 20000 4096 20000 4096
```

#在端口 gigabitethernet0/2 上配置基于端口的流量整形，整端口流量限速为 50000kbps。

```
Device(config-if-gigabitethernet0/2)#traffic-shape 50000 4096
Device(config-if-gigabitethernet0/2)#exit
```

- 步骤 6: 检验结果。

#视频流量和数据流量经过 Device 处理后，从端口 gigabitethernet0/2 发出的视频流量速率和数据流量速率总和不超过 50000kbps。当视频流量速率大于 20000kbps 时，限制视频流量速率为 20000kbps；当视频流量速率小于 20000kbps 时，剩余带宽可以被数据流量占用。

48.3.4 配置速率限制

-B -S -E -A

网络需求

- 网络中有两台服务器，分别是视频服务器（Video Server）和数据服务器（Data Server）；
- 配置速率限制功能，限制视频流量速率和数据流量速率总和不超过 50000kbps，其中数据流量速率不超过 20000kbps。

网络拓扑

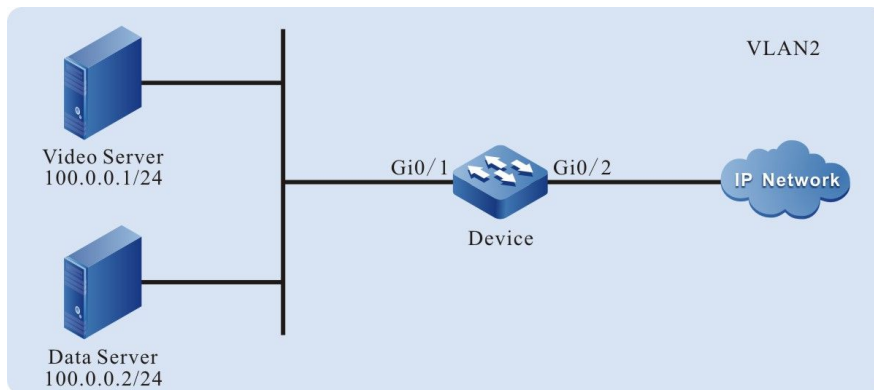


图 48-6 配置速率限制组网图

配置步骤

- 步骤 1： 在 Device 上配置 VLAN 和端口的链路类型。

#创建 VLAN2。

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#配置端口 gigabitethernet0/1 的链路类型为 Access，允许 VLAN2 的业务通过。

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
```

#配置端口 gigabitethernet0/2 的链路类型为 Trunk，允许 VLAN2 的业务通过。

```
Device(config-if-gigabitethernet0/1)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode trunk
Device(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 2
Device(config-if-gigabitethernet0/2)#exit
```

- 步骤 2: 配置速率限制功能。

#在端口 gigabitethernet0/1 上配置基于端口的速率限制，流量限速为 50000kbps。

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#rate-limit default 50000 4096
Device(config-if-gigabitethernet0/1)#exit
```

- 步骤 3: 配置计量器功能。

#配置名称为 data_stream 的计量器，流量限速为 20000kbps。

```
Device(config)#traffic-meter data_stream
Device(config-meter)#meter mode srtcm 20000 4096 4096
Device(config-meter)#exit
```

- 步骤 4: 配置出方向动作组。

#配置名称为 data_stream 的出方向动作组，并且在出方向动作组中应用计量器。

```
Device(config)#egr-action-group data_stream
Device(config-egract-group)#meter data_stream
Device(config-egract-group)#exit
```

- 步骤 5: 配置 IP 标准 ACL。

#在 Device 上配置编号为 1 的 IP 标准 ACL。

```
Device(config)#ip access-list standard 1
```

#配置规则与名称为 data_stream 的出方向动作组绑定，将数据流量限速为 20000kbps。

```
Device(config-std-nacl)#permit host 100.0.0.2 egr-action-group data_stream
```

#配置规则，允许视频流量通过。

```
Device(config-std-nacl)#permit host 100.0.0.1
```

```
Device(config-std-nacl)#exit
```

- 步骤 6: 配置应用 IP 标准 ACL。

#将编号为 1 的 IP 标准 ACL 应用于 Device 端口 gigabitethernet0/2 出方向。

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#ip access-group 1 out
Device(config-if-gigabitethernet0/2)#exit
```

#在 Device 上查看 ACL 应用于端口的信息。

```
Device#show acl-object interface
-----Interface-----Bind-----Instance-----
Interface-----Direction-----AclType-----AclName
gi0/2             OUT      IP      1
```

- 步骤 7: 检验结果。

#视频流量和数据流量经过 Device 处理后，从端口 gigabitethernet0/2 发出的视频流量速率和数据流量速率总和不超过 50000kbps，其中数据流量速率不超过 20000kbps。

48.3.5 配置 WRED

-B -S -E -A

网络需求

- 大量终端从 FTP 服务器上下载文件。
- 在 Device 上配置 WRED 功能，防止 TCP 的全局同步现象导致 FTP 连接时断时续。

网络拓扑

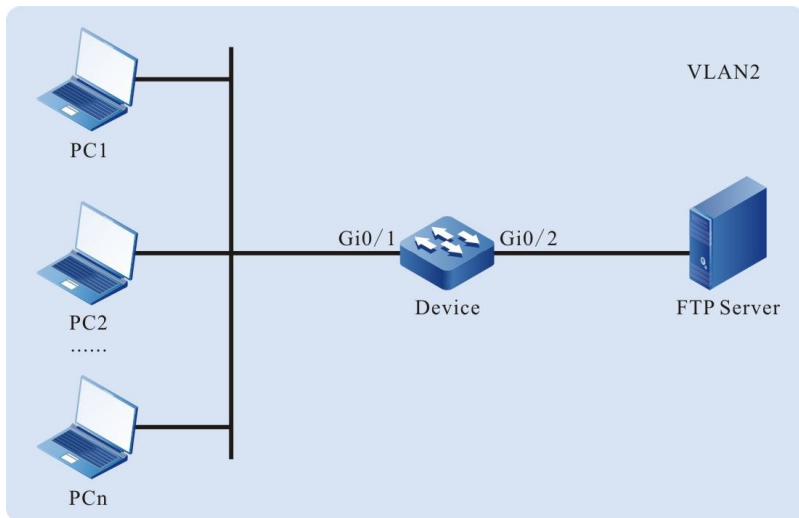


图 48-7 配置 WRED 组网图

配置步骤

- 步骤 1: 在 Device 上配置 VLAN 和端口的链路类型。

#创建 VLAN2。

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#配置端口 gigabitethernet0/1 的链路类型为 Access，允许 VLAN2 的业务通过。

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
```

#配置端口 gigabitethernet0/2 的链路类型为 Trunk，允许 VLAN2 的业务通过。

```
Device(config-if-gigabitethernet0/1)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode trunk
Device(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 2
Device(config-if-gigabitethernet0/2)#exit
```

- 步骤 2: 配置 WRED 功能。

#在端口 gigabitethernet0/2 上配置 0 队列报文的丢弃开始值为 80，丢弃几率为 45。

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#drop-mode 0 wred drop-start 80 drop-rate 45
Device(config-if-gigabitethernet0/2)#exit
```

说明：

- 由 PC 发出的报文均为 Untag 报文，默认进入 0 队列。

- 步骤 3： 检验结果。

#当大量终端从 FTP 服务器下载文件的时候，不会出现连接 FTP 时断时续的情况。

48.3.6 配置 SP **-B -S -E -A**

网络需求

- 网络中有认证服务器（AAA Server），视频服务器（Video Server）和一台终端设备（PC）；
- 配置 SP 功能，当出端口流量出现拥塞的时候，优先保障认证服务器的流量，其次保障视频流量，最后才保障终端流量。

网络拓扑

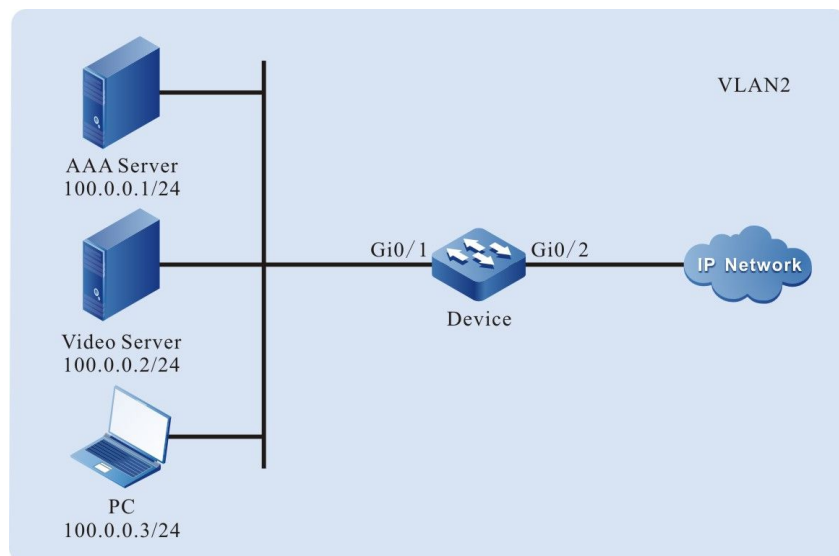


图 48-8 配置 SP 组网图

配置步骤

- 步骤 1: 在 Device 上配置 VLAN 和端口的链路类型。

#创建 VLAN2。

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#配置端口 gigabitethernet0/1 的链路类型为 Access，允许 VLAN2 的业务通过。

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
```

#配置端口 gigabitethernet0/2 的链路类型为 Trunk，允许 VLAN2 的业务通过。

```
Device(config-if-gigabitethernet0/1)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode trunk
Device(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 2
Device(config-if-gigabitethernet0/2)#exit
```

- 步骤 2: 配置 L3 动作组。

#配置名称为 LP7 的 L3 动作组，动作为重标记报文入 7 队列。

```
Device(config)#l3-action-group LP7
Device(config-action-group)#remark l2-priority 1p 7
Device(config-action-group)#exit
```

#配置名称为 LP6 的 L3 动作组，动作为重标记报文入 6 队列。

```
Device(config)#l3-action-group LP6
Device(config-action-group)#remark l2-priority 1p 6
Device(config-action-group)#exit
```

#配置名称为 LP5 的 L3 动作组，动作为重标记报文入 5 队列。

```
Device(config)#l3-action-group LP5
Device(config-action-group)#remark l2-priority 1p 5
Device(config-action-group)#exit
```

- 步骤 3: 配置 IP 标准 ACL。

#在 Device 上配置编号为 1 的 IP 标准 ACL。

```
Device(config)#ip access-list standard 1
```

#配置规则与名称为 LP7 的 L3 动作组绑定，实现重标记认证流量报文入 7 队列。

```
Device(config-std-nacl)#permit host 100.0.0.1 l3-action-group LP7
```

#配置规则与名称为 LP6 的 L3 动作组绑定，实现重标记视频流量报文入 6 队列。

```
Device(config-std-nacl)#permit host 100.0.0.2 l3-action-group LP6
```

#配置规则与名称为 LP5 的 L3 动作组绑定，实现重标记终端流量报文入 5 队列。

```
Device(config-std-nacl)#permit host 100.0.0.3 l3-action-group LP5
Device(config-std-nacl)#exit
```

- 步骤 4: 配置应用 IP 标准 ACL。

#将编号为 1 的 IP 标准 ACL 应用于 Device 端口 gigabitethernet0/1 入方向。

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#ip access-group 1 in
Device(config-if-gigabitethernet0/1)#exit
```

#在 Device 上查看 ACL 应用于端口的信息。

```
Device#show acl-object interface
-----Interface-----Bind-----Instance-----
Interface-----Direction-----AclType-----AclName
gi0/1           IN      IP      1
```

- 步骤 5: 配置 SP 功能。

#在端口 gigabitethernet0/2 上配置 SP 功能，对报文进行严格优先级调度。

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#queue-schedule sp
Device(config-if-gigabitethernet0/2)#exit
```

- 步骤 6: 检验结果。

#当出端口 gigabitethernet0/2 的流量出现拥塞的时候，认证流量被优先通过，其次是视频流量被允许通过，最后才是终端流量被允许通过。

48.3.7 配置 WDRR **-B -S -E -A**

网络需求

- 网络中有认证服务器 (AAA Server)，视频服务器 (Video Server) 和一台终端

设备 (PC) ；

- 配置 WDRR 功能，当出端口流量出现拥塞的时候，实现终端流量，视频流量和认证流量按照特定的比例通过。

网络拓扑

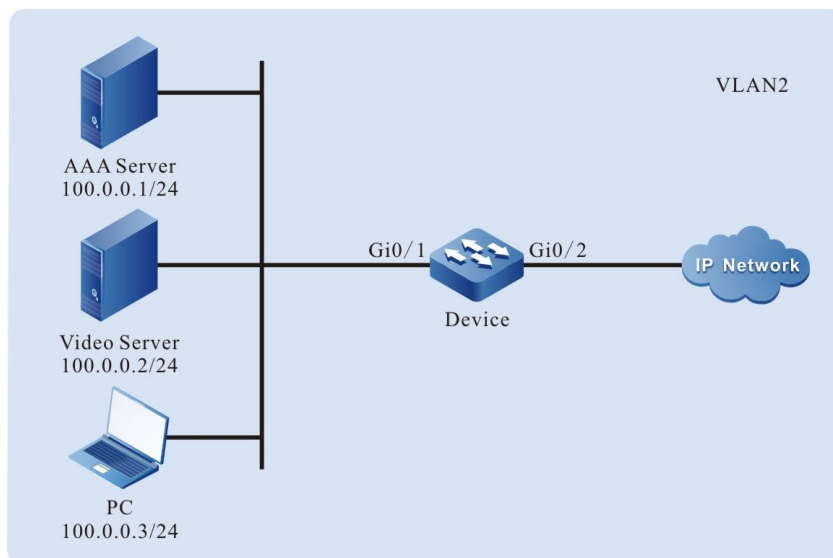


图 48-9 配置 WDRR 组网图

配置步骤

- 步骤 1： 在 Device 上配置 VLAN 和端口的链路类型。

#创建 VLAN2。

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#配置端口 gigabitethernet0/1 的链路类型为 Access，允许 VLAN2 的业务通过。

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
```

#配置端口 gigabitethernet0/2 的链路类型为 Trunk，允许 VLAN2 的业务通过。

```
Device(config-if-gigabitethernet0/1)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode trunk
Device(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 2
Device(config-if-gigabitethernet0/2)#exit
```


- 步骤 2: 配置 L3 动作组。

#配置名称为 LP7 的 L3 动作组，动作为重标记报文入 7 队列。

```
Device(config)#l3-action-group LP7
Device(config-action-group)#remark l2-priority 1p 7
Device(config-action-group)#exit
```

#配置名称为 LP6 的 L3 动作组，动作为重标记报文入 6 队列。

```
Device(config)#l3-action-group LP6
Device(config-action-group)#remark l2-priority 1p 6
Device(config-action-group)#exit
```

#配置名称为 LP5 的 L3 动作组，动作为重标记报文入 5 队列。

```
Device(config)#l3-action-group LP5
Device(config-action-group)#remark l2-priority 1p 5
Device(config-action-group)#exit
```

- 步骤 3: 配置 IP 标准 ACL。

#在 Device 上配置编号为 1 的 IP 标准 ACL。

```
Device(config)#ip access-list standard 1
```

#配置规则与名称为 LP7 的 L3 动作组绑定，实现重标记认证流量报文入 7 队列。

```
Device(config-std-nacl)#permit host 100.0.0.1 l3-action-group LP7
```

#配置规则与名称为 LP6 的 L3 动作组绑定，实现重标记视频流量报文入 6 队列。

```
Device(config-std-nacl)#permit host 100.0.0.2 l3-action-group LP6
```

#配置规则与名称为 LP5 的 L3 动作组绑定，实现重标记终端流量报文入 5 队列。

```
Device(config-std-nacl)#permit host 100.0.0.3 l3-action-group LP5
Device(config-std-nacl)#exit
```

- 步骤 4: 配置应用 IP 标准 ACL。

#将编号为 1 的 IP 标准 ACL 应用于 Device 端口 gigabitethernet0/1 入方向。

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#ip access-group 1 in
Device(config-if-gigabitethernet0/1)#exit
```

#在 Device 上查看 ACL 应用于端口的信息。

```
Device#show acl-object interface
-----Interface-----Bind-----Instance-----
```

Interface-----	Direction----	AcIType----	AcIName
gi0/1	IN	IP	1

- 步骤 5: 配置 WDRR 功能。

#在端口 gigabitethernet0/2 上配置 WDRR 功能，对 5 队列，6 队列，7 队列的报文分别按照 1: 2: 3 的比例进行调度。

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#queue-schedule wdr 1 1 1 1 1 2 3
Device(config-if-gigabitethernet0/2)#exit
```

- 步骤 6: 检验结果。

#当出端口 gigabitethernet0/2 的流量出现拥塞的时候，在报文字节数一致的情况下，终端流量，视频流量和认证流量按照 1: 2: 3 的比例通过；在报文字节数不一致的情况下，终端流量，视频流量和认证流量按照（1*认证报文字节数）：（2*视频报文字节数）：（3*终端报文字节数）的比例通过。

48.3.8 配置 SP+WRR *-B -S -E -A*

网络需求

- 网络中有认证服务器（AAA Server），视频服务器（Video Server）和一台终端设备（PC）。
- 配置 SP+WRR 功能，当出端口流量出现拥塞的时候，优先保障认证服务器的流量能够全部通过，终端流量和视频流量大小按照 1: 2 的比例通过。

网络拓扑

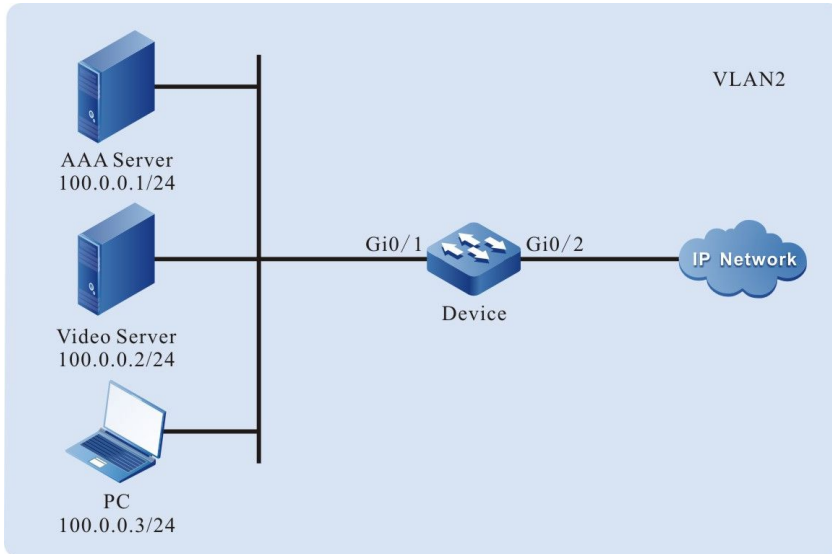


图 48-10 配置 SP+WRR 组网图

配置步骤

- 步骤 1: 在 Device 上配置 VLAN 和端口的链路类型。

#创建 VLAN2。

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#配置端口 gigabitethernet0/1 的链路类型为 Access，允许 VLAN2 的业务通过。

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
```

#配置端口 gigabitethernet0/2 的链路类型为 Trunk，允许 VLAN2 的业务通过。

```
Device(config-if-gigabitethernet0/1)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode trunk
Device(config-if-gigabitethernet0/2)#switchport trunk allowed vlan add 2
Device(config-if-gigabitethernet0/2)#exit
```

- 步骤 2: 配置 L3 动作组。

#配置名称为 LP7 的 L3 动作组，动作为重标记报文入 7 队列。

```
Device(config)#l3-action-group LP7
Device(config-action-group)#remark l2-priority 1p 7
Device(config-action-group)#exit
```

#配置名称为 LP6 的 L3 动作组，动作为重标记报文入 6 队列。

配置手册

发布 1.1 04/2020

```
Device(config)#l3-action-group LP6
Device(config-action-group)#remark l2-priority 1p 6
Device(config-action-group)#exit
```

#配置名称为 LP5 的 L3 动作组，动作为重标记报文入 5 队列。

```
Device(config)#l3-action-group LP5
Device(config-action-group)#remark l2-priority 1p 5
Device(config-action-group)#exit
```

- 步骤 3: 配置 IP 标准 ACL。

#在 Device 上配置编号为 1 的 IP 标准 ACL。

```
Device(config)#ip access-list standard 1
```

#配置规则与名称为 LP7 的 L3 动作组绑定，实现重标记认证流量报文入 7 队列。

```
Device(config-std-nacl)#permit host 100.0.0.1 l3-action-group LP7
```

#配置规则与名称为 LP6 的 L3 动作组绑定，实现重标记视频流量报文入 6 队列。

```
Device(config-std-nacl)#permit host 100.0.0.2 l3-action-group LP6
```

#配置规则与名称为 LP5 的 L3 动作组绑定，实现重标记终端流量报文入 5 队列。

```
Device(config-std-nacl)#permit host 100.0.0.3 l3-action-group LP5
Device(config-std-nacl)#exit
```

- 步骤 4: 配置应用 IP 标准 ACL。

#将编号为 1 的 IP 标准 ACL 应用于 Device 端口 gigabitethernet0/1 入方向。

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#ip access-group 1 in
Device(config-if-gigabitethernet0/1)#exit
```

#在 Device 上查看 ACL 应用于端口的信息。

```
Device#show acl-object interface
-----Interface----Bind----Instance-----
Interface-----Direction----AclType----AclName
gi0/1             IN      IP      1
```

- 步骤 5: 配置 SP+WRR 功能。

#在端口 gigabitethernet0/2 上配置 SP+WRR 功能，允许 7 队列的报文全部通过，5 队列和 6 队列的报文按照 1: 2 的比例进行调度。

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#queue-schedule wrr 1 1 1 1 1 1 2 0
Device(config-if-gigabitethernet0/2)#exit
```

- 步骤 6: 检验结果。

#当出端口 gigabitethernet0/2 的流量出现拥塞的时候，认证流量被优先全部通过。终端流量和视频流量大小按照 1: 2 的比例通过。

48.3.9 配置流镜像

-B -S -E -A

网络需求

- PC1、PC2 和 PC3 与 Device 相连，PC1 和 PC2 在 VLAN2 内通信；
- 在 Device 上配置流镜像功能，实现 PC3 对 Device 端口 gigabitethernet0/1 接收到的报文进行监控。

网络拓扑

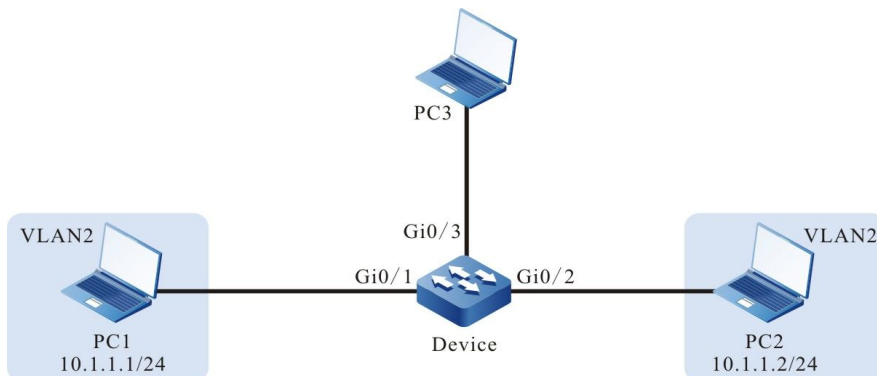


图 48-11 配置流镜像组网图

配置步骤

步骤 1: 配置 VLAN 及端口的链路类型。

#在 Device 上创建 VLAN2。

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#在 Device 上配置端口 gigabitethernet0/1 和端口 gigabitethernet0/2 的链路类型为 Access, 允许 VLAN2 的业务通过。

```
Device(config)#interface gigabitethernet 0/1-0/2
Device(config-if-range)#switchport mode access
Device(config-if-range)#switchport access vlan 2
Device(config-if-range)#exit
```

- 步骤 2: 配置流镜像功能。

#配置名称为 mirror 的 L3 动作组, 将报文镜像到端口 gigabitethernet0/3。

```
Device(config)#l3-action-group mirror
Device(config-action-group)#mirror interface gigabitethernet 0/3
Device(config-action-group)#exit
```

- 步骤 3: 配置计数器功能。

#配置名称为 count 的出方向动作组, 对报文个数进行计数。

```
Device(config)#egr-action-group count
Device(config-egract-group)#count all-colors
Device(config-egract-group)#exit
```

- 步骤 4: 配置 IP 标准 ACL。

#在 Device 上配置编号为 1 的 IP 标准 ACL。

```
Device(config)#ip access-list standard 1
```

#配置规则与名称为 mirror 的 L3 动作组绑定, 实现将所有报文都镜像到端口 gigabitethernet0/3。

```
Device(config-std-nacl)#permit any l3-action-group mirror
Device(config-std-nacl)#exit
```

#在 Device 上配置编号为 2 的 IP 标准 ACL。

```
Device(config)#ip access-list standard 2
```

#配置规则与名称为 count 的出方向动作组绑定, 实现将所有报文都进行计数。

```
Device(config-std-nacl)#permit any egr-action-group count
Device(config-std-nacl)#exit
```

- 步骤 5: 配置应用 IP 标准 ACL。

#将编号为 1 的 IP 标准 ACL 应用于 Device 端口 gigabitethernet0/1 入方向。

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#ip access-group 1 in
Device(config-if-gigabitethernet0/1)#exit
```

#将编号为 2 的 IP 标准 ACL 应用于 Device 端口 gigabitethernet0/3 出方向。

```
Device(config)#interface gigabitethernet 0/3
Device(config-if-gigabitethernet0/3)#ip access-group 2 out
Device(config-if-gigabitethernet0/3)#exit
```

#在 Device 上查看 ACL 应用于端口的信息。

```
Device#show acl-object interface
-----Interface----Bind----Instance-----
Interface-----Direction----AcIType----AcIName
gi0/1           IN      IP      1
gi0/3           OUT     IP      2
```

- 步骤 6: 检验结果。

#PC1 与 PC2 之间相互通信时，在 PC3 上能捕获到端口 gigabitethernet0/1 接收到的报文。

#在 Device 上查看计数器统计的报文个数。

```
Device#show traffic-count inst-interface gigabitethernet 0/3 ip-out
Interface      Instance_type      AcI_name      Frame_gap
gigabitethernet0/3  Ip AcI Bind Interface Out  2      Yes
-----
seq            :                10
counter_mode   :                count all color
all packets number :                5
all packets byte :                640
```

可以看出，在端口 gigabitethernet0/3 的出方向统计有 5 个报文。

安全

49 CPU 保护

49.1 CPU 保护简介

设备中有大量的协议报文需要交由 CPU 进行处理，需要为每种协议报文指定队列。CPU 保护功能对交由 CPU 的协议报文进行分类，按照协议的优先级不同，进入不同的 CPU 队列，并可以设置每个队列的速率限制。

设备共有 8 个 CPU 队列，编号从 0 到 7，它们采用严格优先级，编号越小，优先级越低，编号越大，优先级越高，也就是说，0 队列的优先级最低，7 队列的优先级最高。高优先级队列报文总是先于低优先级队列的报文被交由 CPU 进行处理。可以根据每种报文的重要性，将它们指定到不同的优先级队列，确保重要的报文优先交由 CPU 处理。

同时，设备能够对进入每个 CPU 队列的报文进行速率限制，防止网络中恶意的协议报文攻击，造成设备的 CPU 利用率过高，导致设备无法正常运行。

49.2 CPU 保护功能配置

表 49-1 CPU 保护功能配置列表

配置任务	
配置协议报文的 CPU 队列	配置协议报文的 CPU 队列
配置 CPU 队列的速率限制	配置 CPU 所有队列总的速率限制

配置任务	
	配置 CPU 每个队列的速率限制
配置用户自定义协议报文交由 CPU 处理	配置用户自定义协议报文交由 CPU 处理的匹配规则
	配置用户自定义协议报文交由 CPU 处理的方式

49.2.1 配置协议报文的 CPU 队列

-B -S -E -A

配置条件

无

配置协议报文的 CPU 队列

设备共有 8 个 CPU 队列，用户可以配置不同的协议报文进入不同的队列。设备会根据用户的配置，依次从高优先级队列到低优先级队列把协议报文交由 CPU 进行处理。如果协议报文在优先级高的队列中，那么会优先交由 CPU 处理，另外用户也可以指定重要的报文进入高优先级队列，来保证优先交由 CPU 处理。不同的协议报文在缺省情况下会进入到缺省的 CPU 队列，另外也可以通过命令修改其进入指定的 CPU 队列。

表 49-2 配置协议报文的 CPU 队列

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置协议报文进入的 CPU 队列	cpu-packet protocol cos cos-value	必选

步骤	命令	说明
		缺省情况下，不同的协议报文进入其缺省的 CPU 队列

49.2.2 配置 CPU 所有队列总的速率限制 **-B -S -E -A**

配置条件

无

配置 CPU 所有队列总的速率限制

为了防止网络恶意攻击，导致 CPU 利用率过高后设备无法运行，用户可以配置 CPU 所有队列总的速率限制。如果发生攻击，并且所有队列中总的报文速率超过了这个总的限制速率，报文将被丢弃，避免造成 CPU 利用率过高。

表 49-3 配置 CPU 所有队列总的速率限制

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 CPU 所有队列总的速率限制	cpu-packet cos global pps pps-value	必选 缺省情况下，所有队列总的限速速率为 2000PPS

49.2.3 配置 CPU 每个队列的速率限制 **-B -S -E -A**

配置条件

无

配置 CPU 每个队列的速率限制

为了防止网络恶意攻击，导致 CPU 利用率过高后设备无法运行，用户可以配置每个 CPU 队列的速率限制。如果发生攻击，并且队列中的报文速率超过了这个队列的限制速率，报文将被丢弃，避免造成 CPU 利用率过高。不同的 CPU 队列在缺省情况下设定了不同的限速值，用户可以根据实际需求修改 CPU 队列的限速值。

表 49-4 配置 CPU 每个队列的速率限制

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 CPU 每个队列的速率限制	cpu-packet cos cos-value pps pps-value	必选 缺省情况下，每个队列的限速值不一样

49.2.4 配置用户自定义协议报文交由 CPU 处理 **-B -S -E -A**

配置条件

无

配置用户自定义协议报文交由 CPU 处理的匹配规则

配置用户自定义协议报文交由 CPU 处理的匹配规则必须与用户自定义协议报文交由 CPU 处理的方式结合使用，它对满足匹配规则的报文会做相应的动作处理。其中匹配规则包括：dst-mac(目的 MAC 地址)，ingress(接口)，vlan-id(VLAN 号)，ether-type(以太类型)，IP (IPV4) ，IPV6，0x0000(自定义以太网类型)，ip-protocol(IP 协议，如 IGMP,TCP 等)，dst-ip(目的 IP)，src-port(源端口)，dst-port(目的端口)。根据用户的需求，可以把以上匹配规则组合使用。

表 49-5 配置用户自定义协议报文交由 CPU 的匹配规则

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置用户自定义协议匹配的规则	<pre> cpu-packet user-define <i>user-id</i> match { dst-mac <i>dst-mac</i> ether-type { <i>ether-type-value</i> ip [dst-ip <i>dst-ip-address</i> dst-mac <i>dst-mac</i> ingress <i>ingress-interface</i> ip-protocol <i>protocol-type</i> vlan-id <i>vlan-id</i> [dst-ip <i>dst-ip-address</i> ingress <i>ingress-interface</i> ip-protocol <i>protocol-type</i>]] ipv6 [dst-ip6 <i>dst-ipv6-address</i> dst-mac <i>dst-mac</i> / ingress <i>ingress-interface</i> ip-protocol <i>protocol-type</i> vlan-id <i>vlan-id</i> [dst-ip <i>dst-ip-address</i> ingress <i>ingress-interface</i> ip-protocol <i>protocol-type</i>]] } ingress <i>ingress-interface</i> vlan-id <i>vlan-id</i> [ingress <i>ingress-interface</i>] } </pre>	<p>必选</p> <p>缺省情况下，没有任何匹配规则。</p>

配置用户自定义协议报文交由 CPU 处理的方式

配置用户自定义协议报文交由 CPU 处理的匹配规则必须与用户自定义协议报文交由 CPU 处理的方式结合使用，它对满足匹配规则的报文会做相应的动作处理。例如：如果配置的方式为 copy，那么不会改变报文原始的转发流程，而是以拷贝的方式让报文交由 CPU 处理；如果配置的方式为 drop，那么不允许报文交由 CPU 处理，而是丢掉报文；如果配置的方式为 remark，那么修改报文交由 CPU 处理的优先级；如果配置的方式为 trap，那么改变报文原始的转发流程只交由 CPU 处理，不做转发。

表 49-6 配置用户自定义协议报文交由 CPU 的方式

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置用户自定义协议报文交由 CPU 处理的方式	cpu-packet user-define <i>user-id</i> action { drop { copy remark trap } cos <i>cos-value</i> }	<p>必选</p> <p>缺省情况下，对满足匹配规则的报文不做任何动作处理</p> <p>用户自定义协议交由 CPU 处理的方式为 copy、remark、trap 时可以指定 cos 值</p>

49.2.5 CPU 保护监控与维护

-B -S -E -A

表 49-7 CPU 保护监控与维护

命令	说明
show cpu-packet protocol-config-table	显示所有协议报文上送 CPU 的配置信息

命令	说明
show cpu-packet cos	显示协议报文交由 CPU 处理的当前和缺省队列信息
show cpu-packet pps	显示每个 CPU 队列的速率限制信息
show cpu-packet udf-table	显示所有通过 CPU 保护模块设置的用户自定义的 ACL 表项信息

49.3 CPU 保护典型配置举例

49.3.1 配置 CPU 保护基本功能

-B -S -E -A

网络需求

- PC 通过 Device 接入 IP Network。
- 在 Device 上配置 SVI-IP 报文入 5 队列，以实现到达本机的 SVI-IP 报文能够优先得到 CPU 处理。
- 在 Device 上对 ARP 所在的队列进行速率限制，以实现当 Device 的 CPU 利用率过高时，低优先级报文也能够正常得到处理。

网络拓扑

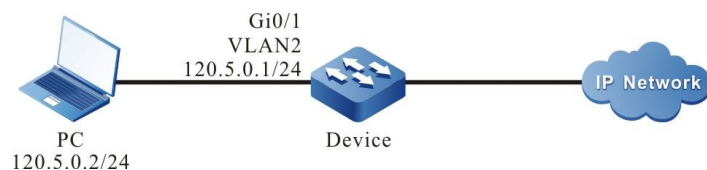


图 49-1 配置 CPU 保护基本功能组网图

配置步骤

步骤 1: 配置 VLAN, 并将端口加入对应的 VLAN。 (略)

步骤 2: 配置各接口 IP 地址。 (略)

步骤 3: 配置 SVI-IP 报文的 CPU 队列。

在 Device 上配置 SVI-IP 报文入 5 队列。

```
Device#configure terminal
Device(config)#cpu-packet svi-ip cos 5
```

步骤 4: 配置 CPU 队列的速率限制。

在 Device 上配置 CPU 队列的速率限制为 50pps。

```
Device(config)#cpu-packet cos 1 pps 50
```

步骤 5: 检验结果。

#在 Device 上查看各协议报文对应的 CPU 队列。

```
Device#show cpu-packet cos
Type          Current-CoS  [Default-CoS]
-----
random        0            [0]
ipv6-all     0            [0]
pppoe         0            [0]
udp-broadcast 0            [0]
icmp          0            [0]
ip-e-packet   0            [0]
ipsec-esp     0            [0]
ipsec-ah      0            [0]
ip            0            [0]
mpls-unicast  0            [0]
mpls-multicast 0            [0]
LBD_I2-src-miss 0            [0]
ipaddr-0      0            [0]
ipaddr-127    0            [0]
ipv4-all     0            [0]
src-martian-addr 0            [0]
arp           1            [1]
ip6-solicited-node 1            [1]
host-group    1            [1]
router-group  1            [1]
ND            1            [1]
trill-oam     1            [1]
lldp          2            [2]
dot1x         2            [2]
```

```

dhcp                2          [2]
dhcipv6             2          [2]
http                2          [2]
svi-ip              5          [2]
pim                 3          [3]
pim6                3          [3]
igmp-dvmrp          3          [3]
ip6-interface-multicast 3          [3]
ike                 3          [3]
ntp                 3          [3]
mld                 3          [3]
rsvp                4          [4]
ospf                4          [4]
ospfv3              4          [4]
irmp                4          [4]
rip                 4          [4]
ripng               4          [4]
is-is               4          [4]
bgp                 4          [4]
ldp                 4          [4]
mvst                5          [5]
l2-interface-unicast 5          [5]
gvrp                5          [5]
mvst-inspection     5          [5]
ulfd                5          [5]
l2pt                5          [5]
svi-icmp            5          [5]
ethernet-cfm        5          [5]
ethernet-lmi        5          [5]
bfd                 6          [6]
vbrp                6          [6]
vrrp                6          [6]
vrrp3               6          [6]
telnet-ssh          6          [6]
loopback-detect     6          [6]
slow-protocols      6          [6]
stp-bpdu            6          [6]
radius              6          [6]
trill               6          [6]
eips                7          [7]
ulpp                7          [7]
mad-fast-hello      7          [7]
erps                7          [7]

```

可以看到，Device 上 SVI-IP 所对应的 CPU 队列由缺省的 2 队列调整到了 5 队列。

#在 Device 上查看各队列的速率限制。

```

Device#show cpu-packet pps
CoS  Current-PPS  [Default-PPS]
-----
0    200           [200]
1    50            [250]
2    500           [500]
3    600           [600]
4    1000          [1000]
5    400           [400]
6    300           [300]
7    100           [100]
TOTAL 2000      [2000]

```

可以看到，Device 上 ARP 所在的 1 队列速率限制由缺省的 250pps 修改为 50pps。

49.3.2 配置 CPU 保护自定义规则 **-B -S -E -A**

网络需求

- Device 分别与 PC1、PC2 直连。
- 在 Device 上配置 CPU 保护自定义规则，将满足匹配条件的报文以 trap 的方式交由 CPU 处理，并进入相应队列。

网络拓扑

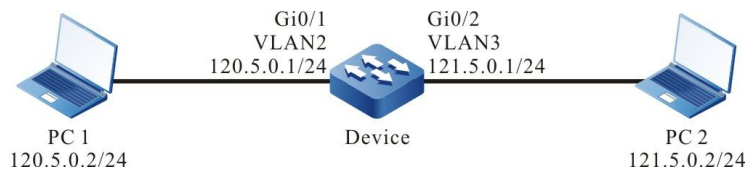


图 49-2 配置 CPU 保护自定义规则组网图

配置步骤

- 步骤 1：配置 VLAN 及将端口加入对应的 VLAN。（略）
- 步骤 2：配置各接口 IP 地址。（略）
- 步骤 3：配置 CPU 保护自定义规则。

#配置自定义规则，将目的地址为 121.5.0.2 的 IP 报文以 trap 的方式交由 CPU 处理，并设置 COS 值为 5。

```
Device#configure terminal
Device(config)#cpu-packet user-define 1 match ether-type ip dst-ip host 121.5.0.2
Device(config)#cpu-packet user-define 1 action trap cos 5
```

- 步骤 4：检验结果。

#在 Device 上查看自定义规则。

```
Device#show cpu-packet udf-table
user-define 1
ether-type: 0x0800(IPv4)
dst-ip: host 121.5.0.2
location: global
valid: yes
```

action: trap
CoS: 5

#当 PC1 访问 PC2 时，CPU 保护自定义规则生效，Device 上目的地址为 121.5.0.2 的 IP 报文以 trap 的方式交由 CPU 处理，并进入 5 队列。

说明：

- 自定义规则匹配其它条件和执行其它方式时，请参照此配置。
-

50 端口安全

50.1 端口安全简介

50.1.1 端口安全概述 *-B -S -E -A*

端口安全是对接入网络的设备进行控制的安全机制。一般应用在接入层，它能够对使用设备端口的主机进行限制，允许某些特定的主机访问网络，而其他主机均不能访问网络。

端口安全功能将用户的 MAC 地址、IP 地址、VLAN ID 以及端口号四个元素灵活绑定，杜绝非法用户接入网络，从而保证网络数据的安全性，并保证合法用户能够得到足够的带宽。

50.1.2 端口安全规则

-B -S -E -A

端口安全规则分为四类：

MAC 规则：主要是根据主机的 MAC 地址来控制主机是否能够通信，MAC 规则的绑定方式包含 MAC 绑定、MAC+VLAN 绑定和 MAC+IP 绑定；

IP 规则：主要是根据主机的 IP 地址来控制主机是否能够通信，IP 规则可以针对单一 IP 地址绑定，也可以针对 IP 地址段进行绑定；

MAX 规则：主要是通过限制端口可以自由学习到的 MAC 地址表项数目来控制主机的通信，这些 MAC 地址表项数目不包含 MAC 规则和 IP 规则产生的合法 MAC 地址表项；

STICKY 规则：主要根据主机的 MAC 地址来控制主机是否能够通信，STICKY 规则的绑定方式包含 MAC 绑定、MAC+VLAN 绑定和 MAC+IP 绑定。STICKY 规则既能自动学习，也能够手工配置，并保存于运行配置中。如果设备重启前保存运行配置，设备重启后，不需要再去配置，这些 STICKY 规则自动生效。当端口下开启 STICKY 功能且 STICKY 学习模式为 MAC 模式时，会将 MAX 规则学到的动态 MAC 表项转换为 STICKY 规则，并保存于运行配置中。

50.1.3 端口安全工作原理

如果只使能端口安全，那么端口安全将丢弃端口上收到的所有报文。端口安全的规则依靠终端设备的 ARP 报文和 IP 报文进行触发，当设备接收到 ARP 报文和 IP 报文时，端口安全从中提取各种报文信息，并与配置的规则进行匹配，匹配的顺序为先匹配 MAC 规则，再匹配 STICKY 规则，再匹配 IP 规则，最后匹配 MAX 规则，并根据匹配结果控制端口的二层转发表，以控制端口对报文的转发行为。匹配 MAX 规则或者 STICKY 规则的报文合法，将被转发。匹配 MAC 规则或 IP 规则的报文，如果规则对报文执行的动作为允许，那么报文属于合法报文将被转发，否则报文非法，将被丢弃。

动作为允许的 MAC 规则和 IP 规则，生效后将规则相应的 MAC 地址写入二层转发表，使得匹配规则的报文能够进行二层转发，动作为拒绝的 MAC 规则和 IP 规则，相应的 MAC 不被写入二层转发表，报文每次都需要经过端口安全作丢弃处理。

MAX 规则和 STICKY 规则，生效后通过写入 MAC 地址表项，形成生效表项，使得报文进行二层转发。

50.2 端口安全功能配置

表 2-1 端口安全基本功能配置列表

配置任务	
配置端口安全基本功能	使能端口安全功能
配置端口安全规则	配置 MAC 规则
	配置 IP 规则
	配置 MAX 规则
	配置 STICKY 规则
配置 STICKY 规则学习模式	配置 STICKY 规则学习模式
配置静态 MAC 地址老化功能	开启静态 MAC 地址老化功能
	配置静态 MAC 地址老化时间
配置收到非法报文时的处理模式	配置收到非法报文时的处理模式
配置收到非法报文时发送日志的时间间隔	配置收到非法报文时发送日志的时间间隔

50.2.1 配置端口安全基本功能

-B -S -E -A

在端口安全的各项配置任务中，必须先使能端口安全，其它功能特性的配置才能生效。

配置条件

无

使能端口安全功能

使能端口安全后，如果不配置任何端口安全规则，端口不能学习 MAC 地址。

表 2-2 配置端口安全基本功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface interface-name	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation link-aggregation-id	
使能端口安全功能	port-security enable	必选 缺省情况下，未使能端口安全功能

说明：

- 端口安全的 IP 规则与 MAX 规则和 802.1x 在同一端口不能同时使用。
- 端口安全的 IP 规则与 MAX 规则和 MAC 地址认证在同一端口不能同时使用。
- 端口安全和安全通道认证功能在同一端口下不能同时使用。
- 端口安全和 DAI (Dynamic ARP Inspection, 动态 ARP 检测) 在同一端口不能同时使用。

50.2.2 配置端口安全规则

-B -S -E -A**配置条件**

在配置端口安全规则之前，首先完成以下任务：

- 使能端口安全功能。

配置 MAC 规则

如果用户希望通过 MAC 地址来控制终端是否能够通信。可以使用 MAC 规则，匹配动作为允许规则的报文能够被转发，匹配动作为拒绝规则的报文将被丢弃。

表 2-3 配置 MAC 规则

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface <i>interface-name</i>	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	
配置动作为允许的 MAC 规则	port-security permit mac-address <i>mac-address-value</i> [desc security-rule-description ip-address <i>ip-address-value</i> [desc security-rule-description] vlan-id	必选其一 缺省情况下，端口下未配置 MAC 规则

步骤	命令	说明
	<i>vlan-id</i> [desc <i>security-rule-description</i>]]	
配置动作为拒绝的 MAC 规则	port-security deny mac-address <i>mac-address-value</i> [ip-address <i>ip-address-value</i> vlan-id <i>vlan-id</i>]	

配置 IP 规则

如果用户希望通过 IP 地址来控制终端是否能够通信。可以使用 IP 规则，匹配动作为允许规则的报文能够被转发，匹配动作为拒绝规则的报文将被丢弃。

表 2-4 配置 IP 规则

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface <i>interface-name</i>	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	
配置动作为允许的 IP 规则	port-security permit ip-address <i>ip-address-value</i> [to <i>ip-address-value</i>]	必选其一 缺省情况下，端口下未配置 IP 规则

步骤	命令	说明
配置动作为拒绝的 IP 规则	port-security deny ip-address <i>ip-address-value</i> [to <i>ip-address-value</i>]	

配置 MAX 规则

在使能端口安全功能的端口下，如果用户希望接入的终端不匹配 MAC 规则和 IP 规则也能通信，可以配置 MAX 规则，该规则会限定允许接入的终端数目。

表 2-5 配置 MAX 规则

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface <i>interface-name</i>	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	
配置 MAX 规则	port-security maximum <i>maximum-number</i>	必选 缺省情况下，MAX 规则允许学习的 MAC 地址数目为 0

说明：

- MAX 规则实际学习到的动态地址数目受到端口、VLAN 和系统的 MAC 地址数目限制。

配置 STICKY 规则

如果用户希望 MAX 规则允许的终端对应的 MAC 地址和 VLAN 信息能够保存在配置中，可以在设备上开启 STICKY 功能，使得设备通过 MAX 规则学到的表项能够被转化为 STICKY 规则。转化完后可以通过当前 STICKY 规则的数目来调整 MAX 规则数目，使得只有匹配 STICKY 规则的终端才能够通信。这样就能实现设备自动学习接入终端的 MAC 地址，并转化为 STICKY 规则，同时保存于配置中，免去了手动配置 MAC 规则的操作。

表 2-6 配置 STICKY 规则

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface <i>interface-name</i>	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	
配置 MAX 规则	port-security maximum <i>maximum-number</i>	必选 缺省情况下，MAX 规则允许学习的动态 MAC 地址数目为 0。只有先配置 MAX 规则的数目，才能够配置 STICKY 规则

步骤	命令	说明
开启 STICKY 功能	port-security permit mac-address sticky	必选 缺省情况下，STICKY 功能没有开启。只有先开启 STICKY 功能，才能够配置 STICKY 规则
配置 STICKY 规则	port-security permit mac-address sticky [<i>mac-address-value</i> [desc <i>security-rule-description</i> / vlan-id <i>vlan-id</i> [desc <i>security-rule-description</i>] ip-address <i>ip-address-value</i> [desc <i>security-rule-description</i>]]]	必选 缺省情况下，端口下未配置 STICKY 规则

50.2.3 配置 STICKY 规则学习模式

-B -S -E -A

配置条件

在配置 STICKY 规则学习模式之前，首先完成以下任务：

- 使能端口安全功能。

配置 STICKY 规则学习模式

如果用户希望按 MAC 或 MAC+VLAN 进行 STICKY 学习，则可以将 STICKY 规则学习模式配置为 MAC 模式，如果用户希望按 MAC+IP 进行 STICKY 规则学习，则可以将 STICKY 规则学习模式配置为 MAC+IP 模式。

表 2-7 配置 STICKY 规则学习模式

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface interface-name	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation link-aggregation-id	
配置 STICKY 规则学习模式	port-security permit mac-address sticky mode { mac mac-ip }	必选 缺省情况下，STICKY 规则学习模式为 MAC 模式

50.2.4 配置静态 MAC 地址老化功能

-B -S -E -A**配置条件**

在配置静态 MAC 地址老化功能之前，首先完成以下任务：

- 使能端口安全功能。

开启静态 MAC 地址老化功能

为了检测 MAC 规则或者 IP 规则生效表项对应的终端是否在线，可以开启静态 MAC 地址老化功能。开启静态 MAC 地址老化功能后，如果检测到终端已下线，会删除该终端对应的生效表项，使得芯片资源能够得到释放。

表 2-8 开启静态 MAC 地址老化功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface <i>interface-name</i>	必选其一 进入二层以太接口配置模式后, 后续配置只在当前端口生效; 进入汇聚组配置模式后, 后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	
开启静态 MAC 地址老化功能	port-security aging static	必选 缺省情况下, 静态 MAC 地址老化功能处于关闭状态

配置静态 MAC 地址老化时间

用户可以根据实际网络环境配置合理的老化时间。一般应用中, 保持缺省值即可。

表 2-9 配置静态 MAC 地址老化时间

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface <i>interface-name</i>	必选其一 进入二层以太接口配置模式后, 后续配置只在当前端口生效; 进入汇聚组配置模式后, 后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	

步骤	命令	说明
配置静态 MAC 地址老化时间	port-security aging time <i>time-value</i>	必选 缺省情况下，静态 MAC 地址老化时间为 1 分钟

50.2.5 配置收到非法报文时的处理模式

-B -S -E -A

配置条件

在配置收到非法报文时的处理模式之前，首先完成以下任务：

- 使能端口安全功能。

配置收到非法报文时的处理模式

端口安全提供三种对非法报文的处理模式，protect、restrict 和 shutdown，用户可以根据安全性的要求灵活选用，三种处理模式的具体功能如下：

- **protect**：收到非法报文后，丢弃报文；
- **restrict**：收到非法报文后，丢弃报文并将信息 trap 到网管；
- **shutdown**：收到非法报文后，丢弃报文，关闭收到报文的端口并将信息 trap 到网管。

表 2-10 配置收到非法报文时的处理模式

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface <i>interface-name</i>	必选其一

步骤	命令	说明
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	进入二层以太网接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
配置非法报文处理模式	port-security violation { protect restrict shutdown }	必选 缺省情况下，端口安全收到非法报文时的处理模式为 protect

50.2.6 配置收到非法报文时发送日志的时间间隔

-B -S -E -A

配置条件

在配置收到非法报文时发送日志的时间间隔之前，首先完成以下任务：

- 使能端口安全功能。

配置收到非法报文时发送日志的时间间隔

用户可以根据实际需要配置收到非法报文时发送日志的时间间隔。一般应用中，保持缺省值即可。

表 2-11 配置收到非法报文时的处理模式

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置收到非法报文时发送日志的时间间隔	port-security violation log-interval <i>log-interval-value</i>	必选

步骤	命令	说明
		缺省情况下，端口安全收到非法报文时发送日志的时间间隔为 5 秒

50.2.7 配置 MAC+IP 规则使用 ACL 功能

-B -S -E -A

配置条件

在配置 MAC+IP 规则使用 ACL 功能之前，首先完成以下任务：

- 使能端口安全功能。

配置 MAC+IP 规则使用 ACL 的功能

用户可以根据实际需要配置 MAC+IP 规则是否使用 ACL，使用 ACL 时 MAC+IP 规则可以精确匹配用户的源 MAC 地址和源 IP 地址，避免源 MAC 地址匹配，源 IP 地址不匹配的非法用户接入。

表 2-12 配置收到非法报文时的处理模式

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface interface-name	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation link-aggregation-id	
配置 MAC+IP 规则使用 ACL 的功能	port-security use-acl	必选 缺省情况下，MAC+IP 规则不使用 ACL。

50.2.8 端口安全监控与维护

-B -S -E -A

表 2-13 端口安全监控与维护

命令	说明
clear port-security statistics	清除报文收发统计信息
show port-security	显示有端口安全配置的端口概要信息
show port-security ip-address	显示配置的 IP 规则
show port-security mac-address	显示配置的 MAC 规则和 STICKY 规则
show port-security active-address	显示所有生效表项的信息
show port-security detect-mac	显示当前检测到的新 MAC 表项
show port-security violation log-interval	显示当前检测到非法 MAC 表项时的日志打印周期
show port-security violation-mac	显示当前检测到的非法 MAC 表项
show port-security statistics	显示报文收发统计信息

50.3 端口安全典型配置举例

50.3.1 配置端口安全 MAC 及 IP 规则

-B -S -E -A

网络需求

- PC1、PC2 以及网络打印机通过 Device 接入服务器。
- 在 Device 上配置端口安全功能，允许 PC1 通过，拒绝 PC2 通过，允许网络打印机执行服务器及 PC1 用户下发的打印任务。

网络拓扑

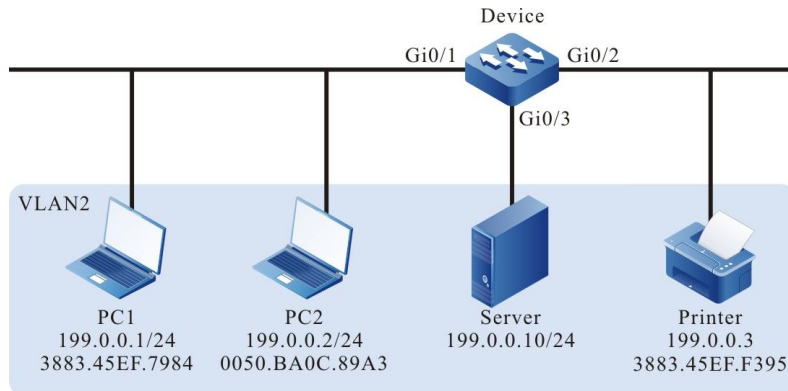


图 2-1 配置端口安全 MAC 及 IP 规则组网图

配置步骤

步骤 1： 配置 VLAN。

#创建 VLAN2。

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#在 Device 的 gigabitethernet0/1~gigabitethernet0/3 上配置端口链路类型为 Access，允许 VLAN2 的业务通过。

```
Device(config)#interface gigabitethernet 0/1-0/3
Device(config-if-range)#switchport mode access
Device(config-if-range)#switchport access vlan 2
Device(config-if-range)#exit
```

步骤 2： 配置端口安全功能。

#在 Device 的 gigabitethernet0/1 上配置 MAC+IP 规则允许 PC1 通过，配置 IP 规则拒绝 PC2 通过。

```
Device#config terminal
Device(config)#interface gigabitethernet 0/1
```

```
Device(config-if-gigabitethernet0/1)#port-security enable
Device(config-if-gigabitethernet0/1)#port-security permit mac-address 3883.45ef.7984 ip-address 199.0.0.1
Device(config-if-gigabitethernet0/1)#port-security deny ip-address 199.0.0.2
Device(config-if-gigabitethernet0/1)#exit
```

#在 Device 的 gigabitethernet0/2 上配置 MAC 规则，允许网络打印机接入网络。

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#port-security enable
Device(config-if-gigabitethernet0/2)#port-security permit mac-address 3883.45ef.f395
Device(config-if-gigabitethernet0/2)#exit
```

步骤 3: 检验结果。

#在 Device 上查看端口安全生效表项，可以看到 PC1 及网络打印机的 MAC 写入端口安全的生效表项中。

```
Device#show port-security active-address
-----
Entry Interface      MAC address      VID IP Addr      Derivation      Age(Sec)
-----
1 gi0/1              38:83:45:EF:79:84 2 199.0.0.1      MAC+IP          0
2 gi0/2              38:83:45:EF:F3:95 2 199.0.0.3      MAC              0
```

#通过验证可以看到，PC1 能够访问服务器并且网络打印机能够执行 PC1 及服务器下发的打印任务。

#通过验证可以看到，PC2 不能够 ping 通服务器及网络打印机。

50.3.2 配置端口安全 MAX 规则

-B -S -E -A

网络需求

- PC1、PC2 和 PC3 同时通过 Device 接入服务器，PC 和服务器在同一局域网内。
- 在 Device 上配置端口安全规则，允许 PC1 和 PC2 访问服务器，拒绝 PC3 访问服务器。

网络拓扑

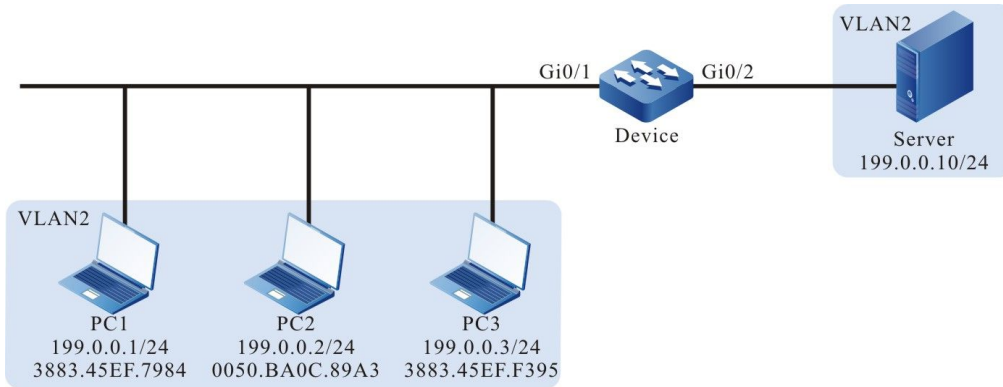


图 2-2 端口安全配置 MAX 规则组网图

配置步骤

步骤 1： 配置 VLAN。

#创建 VLAN2。

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#在 Device 的 gigabitEthernet0/1~gigabitEthernet0/2 上配置端口链路类型为 Access，允许 VLAN2 的业务通过。

```
Device(config)#interface gigabitEthernet 0/1-0/2
Device(config-if-range)#switchport mode access
Device(config-if-range)#switchport access vlan 2
Device(config-if-range)#exit
```

步骤 2： 在 Device 上配置端口安全规则。

#在 Device 的 gigabitEthernet0/1 上配置 MAX 规则，MAX 规则的最大数目为 3。

```
Device(config)#interface gigabitEthernet 0/1
Device(config-if-gigabitEthernet0/1)#port-security enable
Device(config-if-gigabitEthernet0/1)#port-security maximum 3
Device(config-if-gigabitEthernet0/1)#exit
```

#在 Device 的 giabitEthernet0/1 上拒绝 PC3 访问服务器。

```
Device(config)#interface gigabitEthernet 0/1
Device(config-if-gigabitEthernet0/1)#port-security deny mac-address 3883.45ef.f395
Device(config-if-gigabitEthernet0/1)#exit
```

步骤 3: 检验结果。

#三台 PC 分别尝试与服务器通信，可以看到 PC1 和 PC2 能够访问服务器，PC3 不能访问服务器。查看 Device 的 gigabitethernet0/1 端口安全生效表项，可以看到 PC1 和 PC2 的 MAC 地址写入端口安全生效表项。

```
Device#show port-security active-address
-----
Entry Interface      MAC address      VID IP Addr  Derivation  Age(Sec)
-----
1 gi0/1              00:50:ba:0c:89:a3 2 ---      FREE        0
2 gi0/1              38:83:45:EF:79:84 2 ---      FREE        0
Total Mac Addresses for this criterion: 2
```

50.3.3 配置端口安全 STICKY 规则

-B-S-E-A

网络需求

- PC1、PC2 和 PC3 通过 Device 接入服务器，PC 和服务器在同一局域网内。
- 在 Device 上配置端口安全规则，允许其中两台 PC 通过。
- 保存配置并重启 Device 后，重启前的 STICKY 规则能够立即生效。

网络拓扑

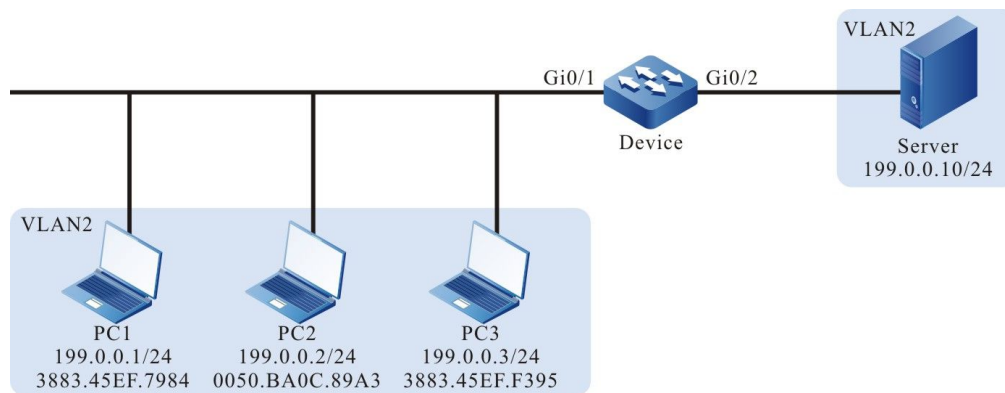


图 2-3 配置端口安全 STICKY 规则组网图

配置步骤

步骤 1: 配置 VLAN。

#创建 VLAN2。

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#在 Device 的 gigabitEthernet0/1~gigabitEthernet0/2 上配置端口链路类型为 Access，允许 VLAN2 的业务通过。

```
Device(config)#interface gigabitEthernet 0/1-0/2
Device(config-if-range)#switchport mode access
Device(config-if-range)#switchport access vlan 2
Device(config-if-range)#exit
```

步骤 2： 在 Device 上配置端口安全 MAX 规则。

#在 Device 的 gigabitEthernet0/1 上配置 MAX 规则，MAX 规则的最大数目为 2。

```
Device(config)#interface gigabitEthernet 0/1
Device(config-if-gigabitEthernet0/1)#port-security enable
Device(config-if-gigabitEthernet0/1)#port-security maximum 2
Device(config-if-gigabitEthernet0/1)#exit
```

步骤 3： 在 Device 上配置端口安全 STICKY 规则。

#在 Device 的 gigabitEthernet0/1 上使能 STICKY 功能。

```
Device(config)#interface gigabitEthernet 0/1
Device(config-if-gigabitEthernet0/1)#port-security permit mac-address sticky
Device(config-if-gigabitEthernet0/1)#exit
```

步骤 4： 检查配置结果。

#PC1、PC2 和 PC3 尝试与服务器通信，查看 Device 的 gigabitEthernet0/1 上的端口安全生效表项，可以看到 gigabitEthernet0/1 上的规则类型为 STICKY。

```
Device#show port-security active-address
-----
Entry Interface      MAC address      VID IP Addr      Derivation      Age(Sec)
-----
1   gi0/1             38:83:45:EF:79:84 2   199.0.0.1      STICKY          0
2   gi0/1             38:83:45:EF:F3:95 2   199.0.0.3      STICKY          0
Total Mac Addresses for this criterion: 2
```

#保存配置并重启设备后，重启前的 STICKY 规则存在并生效。

```
Device#show port-security active-address
```

Entry	Interface	MAC address	VID	IP Addr	Derivation	Age(Sec)
1	gi0/1	38:83:45:EF:79:84	2	199.0.0.1	STICKY	0
2	gi0/1	38:83:45:EF:F3:95	2	199.0.0.3	STICKY	0

Total Mac Addresses for this criterion: 2

51 IP Source Guard

51.1 IP Source Guard 简介

IP Source Guard 功能是一种报文过滤功能，可对端口转发的报文进行过滤控制，防止非法报文通过端口，提高端口的安全性。其功能分为两类：

1、端口 IP Source Guard 功能，即对指定端口接收到的 IP 报文进行过滤。过滤方式分为 IP、MAC 和 IP+MAC 三种，具体处理方式如下：

- IP 方式：如果报文中的源 IP 地址、VLAN ID 与绑定表项中记录的 IP 地址、VLAN 编号相同，端口将转发该报文；否则，将其丢弃；
- MAC 方式：如果报文中的源 MAC 和绑定表中记录的 MAC 地址、VLAN 编号相同，端口将转发该报文；否则，将其丢弃；
- IP+MAC 方式：如果报文中的源 IP 地址、源 MAC 地址、VLAN ID 与绑定表项中记录的 IP 地址、MAC 地址、VLAN 编号相同，端口将转发该报文；否则，将其丢弃。
- 过滤类型的设定只对动态绑定表项生效，对静态绑定表项不影响。
- 端口 IP Source Guard 的绑定表项包括两类：

- 静态绑定表项，手动配置的端口 IP Source Guard 静态绑定表项；
- 动态绑定表项，由 DHCP Snooping 功能的有效表项动态生成。

2、全局 IP Source Guard 功能，即对所有端口接收到的报文进行过滤，包括 ARP (Address Resolution Protocol, 地址解析协议) 和 IP 两种报文。具体过滤方式如下：

- 如果 IP 报文中的源 IP 地址与全局 IP Source Guard 绑定表项中的 IP 地址相同而源 MAC 地址不同、IP 报文中的源 MAC 地址与全局 IP Source Guard 绑定表项中的 MAC 地址相同而源 IP 地址不同时，该报文将被丢弃；
- 如果 ARP 报文中的发送端 IP 地址与绑定表项中的 IP 地址相同而源 MAC 地址不同、ARP 报文中的源 MAC 地址与绑定表项中的 MAC 地址相同而发送端 IP 地址不同时，该报文将被丢弃。

51.2 IP Source Guard 功能配置

表 3-1 IP Source Guard 功能配置列表

配置任务	
配置端口 IP Source Guard 静态绑定表项	配置端口 IP Source Guard 静态绑定表项
配置端口 IP Source Guard 功能	配置端口 IP Source Guard 功能
	配置端口 IP Source Guard 过滤报文类型
配置全局 IP Source Guard 功能	配置全局 IP Source Guard 功能

51.2.1 配置端口 IP Source Guard 静态绑定表项

-B -S -E -A

配置条件

在配置端口 IP Source Guard 静态绑定表项之前，首先完成以下任务：

- 使能端口 IP Source Guard 功能或使能端口 Dynamic ARP Inspection 功能。

配置端口 IP Source Guard 静态绑定表项

端口 IP Source Guard 静态绑定表项，作为对指定端口接收到的 IP 报文进行过滤的依据。

在使能端口 Dynamic ARP Inspection 功能情况下，端口 IP Source Guard 静态绑定表项，只有配置了 mac、ip、vlan 的静态表项才能作为对 ARP 报文进行合法性检测的依据。

表 3-2 配置端口 IP Source Guard 静态绑定表项

步骤	命令	说明
进入全局配置模式	config terminal	-
进入二层以太接口配置模式	interface <i>interface-name</i>	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	
配置端口 IP Source Guard 静态绑定表项	ip source binding { ip-address <i>ip-address</i> [mac-address <i>mac-address</i> [vlan <i>vlan-id</i>]] vlan <i>vlan-id</i>] mac-address <i>mac-address</i> [vlan <i>vlan-id</i>] }	必选 缺省情况，不存在端口 IP Source Guard 静态绑定表项

说明：

- 端口 Dynamic ARP Inspection 功能，参见配置手册 Dynamic ARP Inspection 相关章节。

51.2.2 配置端口 IP Source Guard 功能

-B -S -E -A**配置条件**

无

配置端口 IP Source Guard 功能

使能端口 IP Source Guard 功能后，首先将端口绑定表项写入芯片，包括静态绑定表项和动态绑定表项，静态绑定表项优先被写入。然后根据这些写入芯片的表项对端口接收到的 IP 报文进行安全控制，提高安全性。

表 3-3 配置端口 IP Source Guard 功能

步骤	命令	说明
进入全局配置模式	config terminal	-
进入二层以太接口配置模式	interface interface-name	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation link-aggregation-id	
使能端口 IP Source Guard 功能	ip verify source	必选 缺省情况，端口 IP Source Guard 功能处于禁用状态

说明：

- 使能端口 IP Source Guard 功能后，会将端口 IP Source Guard 绑定表项写入芯片，具体写入芯片的条数由可使用的芯片表项资源决定。如果芯片表项资源已用尽，还需添加绑定表项或使能其它端口上的端口 IP Source Guard 功能，则需要删除一些芯片表项资源相关的绑定表项。
 - 如果某些端口 IP Source Guard 绑定表项因为芯片表项资源不足，导致写入芯片失败，系统会每隔 60 秒自动地尝试将这些绑定表项再次写入芯片，直至所有写入芯片失败的绑定表项被写入芯片或被删除才结束。
 - 如果同时使能了端口 IP Source Guard 和全局 IP Source Guard 功能，则端口接收到的 IP 报文需要同时匹配端口 IP Source Guard 和全局 IP Source Guard 的绑定表项才能被转发，否则将被丢弃。
 - 使能端口 IP Source Guard 功能前，如果该端口所连接的终端设备为非 DHCP (Dynamic Host Configuration, 动态主机配置协议) 客户端，或终端设备是 DHCP 客户端但本设备未使能 DHCP Snooping 功能情况下，需将终端设备的 MAC 地址、IP 地址及对应 VLAN 编号配置成端口 IP Source Guard 静态绑定表项，来保证使能该功能后，终端设备通信正常。DHCP Snooping 功能，参见配置手册 DHCP Snooping 相关章节。
-

51.2.3 配置端口 IP Source Guard 过滤报文类型

-B -S -E -A

配置条件

在配置端口 IP Source Guard 过滤报文类型之前，首先完成以下任务：

- 使能端口 IP Source Guard 功能

配置端口 IP Source Guard 过滤报文类型

使能端口 IP Source Guard 功能后，以 ip 的方式对 IP 报文进行过滤。当端口接收到的 IPv4 报文中源 IP 地址和 VLAN 编号与端口 IP Source Guard 绑定表项中的源 IP 地址和 VLAN 编号都相同时，端口才转发该报文；若任意一个不相同，则丢弃。

使能端口 IP Source Guard 功能后，以 ip-mac 的方式对 IP 报文进行过滤。当端口接收到的 IP 报文中源 MAC 地址、源 IP 地址和 VLAN 编号与端口 IP Source Guard 绑定表项中的 MAC 地址、IP 地址和 VLAN 编号都相同时，端口才转发该报文；若任意一个不相同，则丢弃。

使能端口 IP Source Guard 功能后，以 mac 的方式对 IP 报文进行过滤。当端口接收到的 IP 报文中源 MAC 地址、VLAN 编号与端口 IP Source Guard 绑定表项中的 MAC 地址、IP 地址和 VLAN 编号都相同时，端口才转发该报文；若任意一个不相同，则丢弃。

表 3-4 配置端口 IP Source Guard 过滤报文类型

步骤	命令	说明
进入全局配置模式	config terminal	-
进入二层以太接口配置模式	interface interface-name	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation link-aggregation-id	
使能端口 IP Source Guard 功能	ip verify source type {ip ip-mac mac}	必选 缺省情况下，过滤方式为 ip 过滤类型，只对动态表项生效

51.2.4 配置端口 MAC 静态表项绑定功能 **-B -S -E -A**

配置条件

在配置端口 MAC 静态表项绑定功能之前，首先完成以下任务：

- 使能端口 IP Source Guard 功能

配置端口 MAC 静态表项绑定功能

在配置端口 MAC 静态表项绑定功能之后，就会在端口上配置的 IP Source Guard 静态表项和获取到的动态表项中，获取对应的 mac 地址、vlan 号、端口号下发对应的静态 MAC 表项

表 3-5 配置 MAC 静态表项绑定功能

步骤	命令	说明
进入全局配置模式	config terminal	-
进入二层以太接口配置模式	interface <i>interface-name</i>	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	
使能端口 IP Source Guard 功能	ip source sticky-mac	必选 缺省情况，端口 MAC 静态表项绑定功能处于禁用状态

51.2.5 配置全局 IP Source Guard 功能

-B -S -E -A

配置条件

无

配置全局 IP Source Guard 功能

为保护用户 IP 地址安全，避免其他用户盗用自己的 IP 地址，可通过配置全局 IP Source Guard 功能，将用户 IP 地址和 MAC 地址进行绑定。配置的用户 IP 地址与 MAC 地址的全局 IP Source Guard 绑定表项会被直接写入芯片，从而实现非法 IP 和 ARP 报文的过滤。

在使能全局 Dynamic ARP Inspection 功能情况下，配置的全局 IP Source Guard 绑定表项，作为全局 Dynamic ARP Inspection 功能对 ARP 报文进行合法性检测的依据。

表 3-6 配置全局 IP Source Guard 功能

步骤	命令	说明
进入全局配置模式	config terminal	-
配置全局 IP Source Guard 功能	source binding mac-address ip-address	<p>必选</p> <p>缺省情况，不存在全局 IP Source Guard 绑定表项，该功能处于关闭状态</p> <p>该命令使能全局 IP Source Guard 功能，同时也配置了一条全局 IP Source Guard 绑定表项</p>

说明：

- 如存在 Hybrid 扩展 ACL 应用在全局（所有端口）的入方向上，需取消该应用，才可配置全局 IP Source Guard 功能。否则，配置失败。参见配置手册 ACL 相关章节。
- 全局 IP Source Guard 绑定表项最大支持 40 条，超过 40 条后，配置会失败。
- 配置的全局 IP Source Guard 绑定表项会被直接写入芯片，具体写入芯片的条数由可使用的芯片表项资源决定。如果芯片表项资源已用尽的情况下，还需添加全局 IP Source Guard 绑定表项，则需要删除一些芯片表项资源相关的绑定表项。
- 如果同时使能了端口 IP Source Guard 和全局 IP Source Guard 功能，则端口接收到的 IP 报文需要同时匹配端口 IP Source Guard 和全局 IP Source Guard 的绑定表项才能被转发，否则将被丢弃。

说明：

- 全局 Dynamic ARP Inspection 功能，参见配置手册 Dynamic ARP Inspection 相关章节。

51.2.6 IP Source Guard 监控与维护

-B -S -E -A

表 3-7 IP Source Guard 监控与维护

命令	说明
show ip binding table [interface <i>interface-name</i> link-aggregation <i>link-aggregation-id</i> slot summary]	显示端口 IP Source Guard 绑定表项及绑定表项数目的统计信息
show ip source guard [interface <i>interface-name</i> link-aggregation <i>link-aggregation-id</i>]	显示端口 IP Source Guard 功能的配置信息
show source binding	显示全局 IP Source Guard 绑定表项及表项数目的统计信息

51.3 IP Source Guard 典型配置举例

51.3.1 配置基于 IP+VLAN 的端口 IP Source Guard 功能

-B -S -E -A

网络需求

- PC1、PC2 通过 Device 接入 IP Network。
- 配置基于 IP+VLAN 的端口 IP Source Guard 功能，实现 PC1 能正常访问 IP Network，PC2 不能访问 IP Network。

网络拓扑

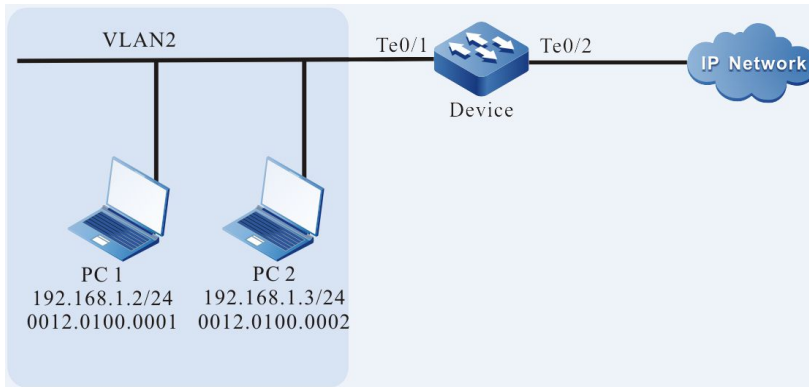


图 3-1 配置基于 IP+VLAN 的端口 IP Source Guard 功能组网图

配置步骤

步骤 1： 在 Device 上配置 VLAN 和端口的链路类型。

#创建 VLAN2。

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#配置端口 gigabitethernet0/1 的链路类型为 Access，允许 VLAN2 的业务通过。

```
Device(config)#interface tengigabitethernet0/1
Device(config-if-tengigabitethernet0/1)#switchport mode access
Device(config-if-tengigabitethernet0/1)#switchport access vlan 2
Device(config-if-tengigabitethernet0/1)#exit
```

步骤 2： 在 Device 上配置端口 IP Source Guard 功能。

#在端口 tengigabitethernet0/1 上使能基于 IP+VLAN 的端口 IP Source Guard 功能，并配置 IP 地址为 192.168.1.2，VLAN 为 2 的端口 IP Source Guard 绑定表项。

```
Device(config)#interface tengigabitethernet 0/1
Device(config-if-tengigabitethernet0/1)#ip verify source
Device(config-if-tengigabitethernet0/1)#ip source binding ip-address 192.168.1.2 vlan 2
Device(config-if-tengigabitethernet0/1)#exit
```

步骤 3: 检验结果。

#查看 IP Source Guard 相关配置信息。

```
Device#show ip source guard
-----
IP source guard interfaces on slot 0 :
  Total number of enabled interfaces : 1
-----
Interface Name      Status   Verify Type  L2 Status
-----
te0/1               Enabled  IP           Disabled
te0/2               Disabled IP           Disabled
te0/3               Disabled IP           Disabled
te0/4               Disabled IP           Disabled
.....
```

可以看到端口 tengigabitethernet0/1 已经使能了 IP Source Guard 功能，静态 IP Source Guard 表项是根据配置 IP+VLAN 表项生效，与 Verify Type 值无关。故上述例子是基于 IP+VLAN 生效。

#查看端口 IP Source Guard 绑定表项。

```
Device#show ip binding table
-----
IP Source Guard binding table on slot 0
  Total binding entries   : 1
  Static binding entries  : 1
  Static not write entries : 0
  Dynamic binding entries : 0
  Dynamic not write entries : 0
  PCE writing entries     : 1
-----
Interface-Name MAC-Address IP-Address VLAN-ID Type-Flag Writing-Flag L2-Flag
-----
te0/1          ---      192.168.1.2 2      Static  Wrote      Not Write
```

#PC1 能正常访问 IP Network, PC2 不能访问 IP Network。

51.3.2 配置基于 MAC+VLAN 的端口 IP Source Guard 功能

-B -S -E -A

网络需求

- PC1、PC2 通过 Device 接入 IP Network。
- 配置基于 MAC+VLAN 的端口 IP Source Guard 功能，实现 PC1 能正常访问 IP Network, PC2 不能访问 IP Network。

网络拓扑

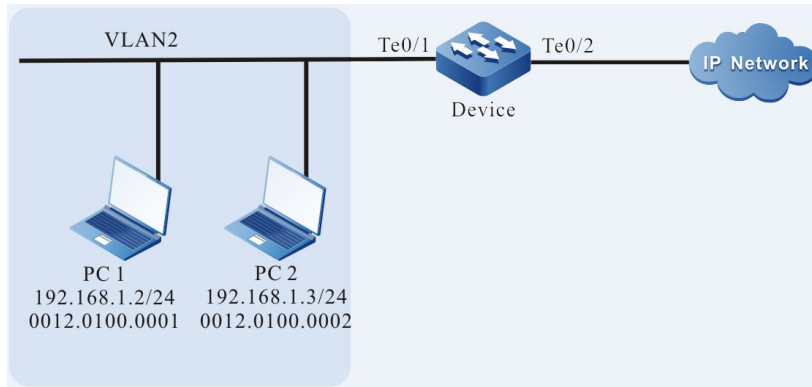


图 3-2 配置基于 MAC+VLAN 的端口 IP Source Guard 功能组网图

配置步骤

步骤 1： 在 Device 上配置 VLAN 和端口的链路类型。

#创建 VLAN2。

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#配置端口 tengigabitethernet0/1 的链路类型为 Access，允许 VLAN2 的业务通过。

```
Device(config)#interface tengigabitethernet 0/1
Device(config-if-tengigabitethernet0/1)#switchport mode access
Device(config-if-tengigabitethernet0/1)#switchport access vlan 2
Device(config-if-tengigabitethernet0/1)#exit
```

步骤 2： 在 Device 上配置端口 IP Source Guard 功能。

#在端口 tengigabitethernet0/1 上使能基于 MAC+VLAN 过滤方式的端口 IP Source Guard 功能，并配置 MAC 地址为 0012.0100.0001，VLAN 为 2 的端口 IP Source Guard 绑定表项。

```
Device(config)#interface tengigabitethernet 0/1
Device(config-if-tengigabitethernet0/1)#ip verify source
Device(config-if-tengigabitethernet0/1)#ip source binding mac-address 0012.0100.0001 vlan 2
Device(config-if-tengigabitethernet0/1)#exit
```

步骤 3： 检验结果。

#查看 IP Source Guard 相关配置信息。

```

Device#show ip source guard
-----
IP source guard interfaces on slot 0 :
  Total number of enabled interfaces : 1
-----
Interface Name      Status   Verify Type L2 Status
-----
te0/1               Enabled  IP         Disabled
te0/2               Disabled IP         Disabled
te0/3               Disabled IP         Disabled
te0/4               Disabled IP         Disabled
.....

```

可以看到端口 tengigabitethernet0/1 已经使能了 IP Source Guard 功能，静态 IP Source Guard 表项是根据配置 MAC+VLAN 表项生效，与 Verify Type 值无关。故上述例子是基于 MAC+VLAN 生效。

#查看端口 IP Source Guard 绑定表项。

```

Device#show ip binding table
-----
IP Source Guard binding table on slot 0
  Total binding entries   : 1
  Static binding entries  : 1
  Static not write entries : 0
  Dynamic binding entries : 0
  Dynamic not write entries : 0
  PCE writing entries     : 1
-----
Interface-Name MAC-Address IP-Address VLAN-ID Type-Flag Writing-Flag L2-Flag
-----
te0/1         0012.0100.0001 ---    2    Static   Wrote    Not Write

```

#PC1 能正常访问 IP Network，PC2 不能访问 IP Network。

51.3.3 配置基于 IP+MAC+VLAN 的端口 IP Source Guard 功能

-B -S -E -A

网络需求

- PC1、PC2 通过 Device 接入 IP Network。
- 配置基于 IP+MAC+VLAN 的端口 IP Source Guard 功能，实现 PC1 能正常访问 IP Network，PC2 不能访问 IP Network。

网络拓扑

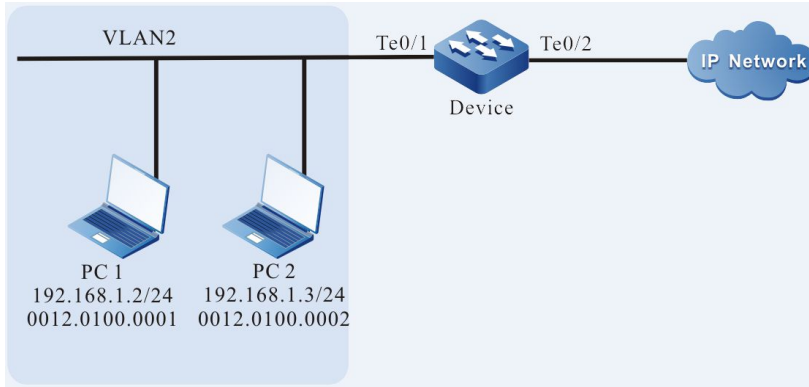


图 3-3 配置基于 IP+MAC+VLAN 的端口 IP Source Guard 功能组网图

配置步骤

步骤 1： 在 Device 上配置 VLAN 和端口的链路类型。

#创建 VLAN2。

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#配置端口 tengigabitethernet0/1 的链路类型为 Access，允许 VLAN2 的业务通过。

```
Device(config)#interface tengigabitethernet 0/1
Device(config-if-tengigabitethernet0/1)#switchport mode access
Device(config-if-tengigabitethernet0/1)#switchport access vlan 2
Device(config-if-tengigabitethernet0/1)#exit
```

步骤 2： 在 Device 上配置端口 IP Source Guard 功能。

#在端口 tengigabitethernet0/1 上使能基于 IP+MAC+VLAN 的端口 IP Source Guard 功能，并配置 MAC 地址为 0012.0100.0001，IP 地址为 192.168.1.2，VLAN 为 2 的端口 IP Source Guard 绑定表项。

```
Device(config)#interface tengigabitethernet 0/1
Device(config-if-tengigabitethernet0/1)#ip verify source
Device(config-if-tengigabitethernet0/1)#ip source binding ip-address 192.168.1.2 mac-address
0012.0100.0001 vlan 2
Device(config-if-tengigabitethernet0/1)#exit
```

步骤 3： 检验结果。

#查看 IP Source Guard 相关配置信息。

```
hostname#show ip source guard
-----
IP source guard interfaces on slot 0 :
  Total number of enabled interfaces : 1
-----
Interface Name      Status   Verify Type  L2 Status
-----
te0/1               Enabled  IP          Disabled
te0/2               Disabled IP          Disabled
te0/3               Disabled IP          Disabled
te0/4               Disabled IP          Disabled
.....
```

可以看到端口 tengigabitethernet0/1 已经使能了 IP Source Guard 功能，静态 IP Source Guard 表项是根据配置 IP+MAC+VLAN 表项生效，与 Verify Type 值无关。故上述例子是基于 IP+MAC+VLAN 生效。

#查看端口 IP Source Guard 绑定表项。

```
Device#show ip binding table
-----
IP Source Guard binding table on slot 0
  Total binding entries   : 1
  Static binding entries  : 1
  Static not write entries : 0
  Dynamic binding entries : 0
  Dynamic not write entries : 0
  PCE writing entries     : 1
-----
Interface-Name  MAC-Address  IP-Address  VLAN-ID  Type-Flag  Writing-Flag  L2-Flag
-----
te0/1          0012.0100.0001  192.168.1.2  2        Static     Wrote        Not Write
```

#PC1 能正常访问 IP Network, PC2 不能访问 IP Network。

52 DHCP snooping

52.1 DHCP snooping 简介

52.1.1 DHCP snooping 基本功能简介 *-B -S -E -A*

DHCP snooping 是 DHCP (Dynamic Host Configuration Protocol, 动态主机配置协议) 的一种安全特性, 主要具有如下两种功能:

1、记录 DHCP 客户端 MAC 地址与 IP 地址的对应关系:

出于安全性的考虑, 网络管理员可能需要记录用户上网时所用的 IP 地址, 确认用户主机 MAC 地址和从 DHCP 服务器获取的 IP 地址的对应关系。

DHCP snooping 通过监听 DHCP 请求报文和信任端口收到的 DHCP 应答报文, 记录 DHCP 客户端的 MAC 地址以及获取到的 IP 地址。管理员可以通过 DHCP snooping 记录的绑定表项, 来查看 DHCP 客户端获取的 IP 地址信息。

2、保证客户端从合法的服务器获取 IP 地址:

如果网络中存在私自架设的 DHCP 服务器, 则 DHCP 客户端可能获取到错误的 IP 地址, 导致通信异常或存在安全隐患。为保证 DHCP 客户端能通过合法的 DHCP 服务器获取 IP 地址, DHCP snooping 功能允许将端口配置为信任端口或非信任端口:

- 信任端口是与合法的 DHCP 服务器直接或间接连接的端口。信任端口对接收到的 DHCP 响应报文正常转发, 从而保证 DHCP 客户端可以获取正确的 IP 地址;
- 非信任端口是不与合法的 DHCP 服务器直接或间接连接的端口。如果从非信任端口

接收到 DHCP 服务器发送的 DHCP 响应报文，则会将其丢弃，从而防止 DHCP 客户端获取错误的 IP 地址。

52.1.2 DHCP snooping Option82 选项简介 *-B -S -E -A*

DHCP snooping 支持对 Option82 选项的添加、转发和管理。Option82 选项是一个 DHCP 报文选项，这个选项用于记录 DHCP 客户端的位置信息，管理员可以根据这个选项定位 DHCP 客户端，从而进行一些安全控制，比如限制某个端口或 VLAN 所能分配的 IP 地址个数等。根据 DHCP 报文类型的不同，对 Option82 选项的处理方式也不同：

1、当设备接收到 DHCP 请求报文后，将根据报文中是否包含 Option82 选项以及用户配置的处理策略及填充格式对报文进行相应的处理，并将处理后的报文转发给 DHCP 服务器；

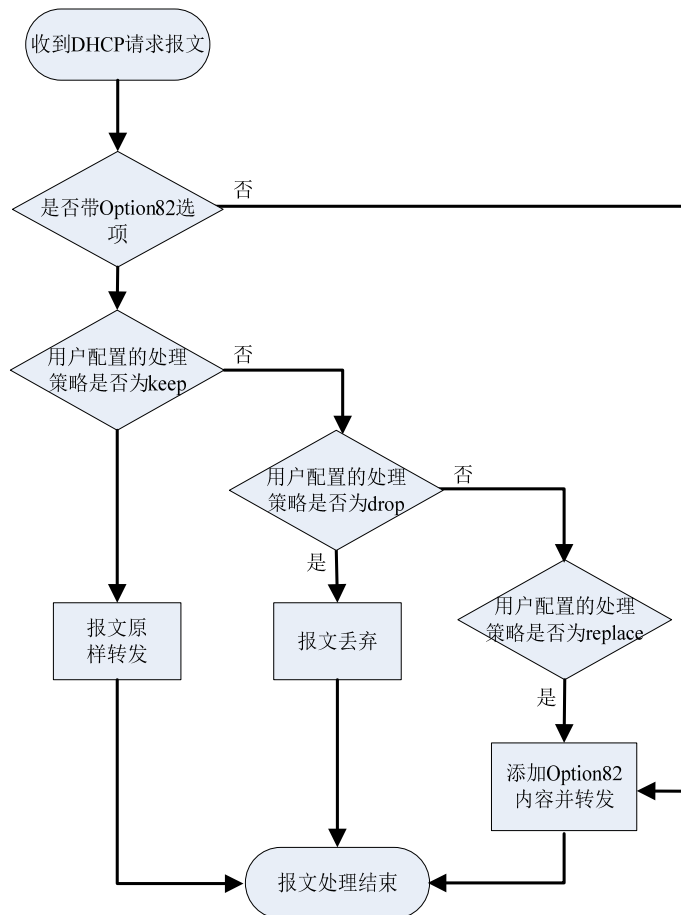


图 4-1 Option82 选项的处理流程

2、当设备接收到 DHCP 服务器的响应报文时，如果报文中包含 Option82 选项，则删除 Option82 选项，并转发给 DHCP 客户端；如果报文中不包含 Option82 选项，则直接转发给 DHCP 客户端。

52.2 DHCP snooping 功能配置

表 4-1 DHCP snooping 功能配置列表

配置任务	
配置 DHCP snooping 基本功能	配置 DHCP snooping 功能
	配置端口信任状态
	配置 DHCP snooping 限速功能
配置 DHCP snooping Option82 选项	配置 Option82 选项的处理策略
	配置 Remote ID 内容
	配置 Circuit ID 内容
	配置 Option82 选项填充格式
	配置 Option82 选项报文处理策略
配置 DHCP snooping 绑定表项存储	配置 DHCP snooping 绑定表项自动存储
	配置 DHCP snooping 绑定表项手动存储

52.2.1 配置 DHCP snooping 基本功能

-B -S -E -A

DHCP snooping 基本功能包括使能 DHCP snooping 功能、配置端口信任状态和 DHCP 报文限速功能。

配置条件

无

配置 DHCP snooping 功能

使能 DHCP snooping 功能后，会对设备所有端口接收到的 DHCP 报文进行监控：

- 对接收到的请求报文，会依据报文中的信息生成相应的绑定表项；
- 对从信任端口接收到的应答报文，会更新对应绑定表项的状态及租约时间；
- 对从非信任端口接收到的应答报文，会直接将其丢弃。

表 4-2 配置 DHCP snooping 功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
使能 DHCP snooping 功能	dhcp-snooping	必选 缺省情况下，DHCP snooping 功能处于禁用状态

配置端口信任状态

为防止 DHCP 客户端从非法 DHCP 服务器获取地址，可通过配置与合法服务器直接或间接连接的端口为信任端口。

当端口配置为信任端口后，才允许 DHCP 响应报文正常转发；否则，将 DHCP 响应报文丢弃。

表 4-3 配置端口信任状态

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface interface-name	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation link-aggregation-id	
配置端口信任状态	dhcp-snooping trust	必选 缺省情况，所有的端口均为非信任端口

说明：

- 与 DHCP 服务器相连的端口，需配置成信任端口，否则 DHCP 客户端无法获取到地址。
- 在端口被配置成信任端口后，就不会对通过该端口的 DHCP 报文速率进行限制。
- 将端口状态由信任端口改为非信任端口后，该端口的速率限制上限值为缺省值 40。

配置 DHCP snooping 限速功能

配置 DHCP snooping 限速功能可以对每秒处理的 DHCP 报文数目进行限制。避免系统由于长期处理 DHCP 报文，导致其他协议报文无法及时得到处理。

当一秒钟内收到的 DHCP 报文数目超过速率上限值时，后续 DHCP 报文会被丢弃。如果端口连续 20 秒收到的 DHCP 报文都超速，则会将相应端口关闭，来隔离报文冲击源。

表 4-4 配置 DHCP snooping 限速功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface <i>interface-name</i>	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	
配置 DHCP snooping 限速功能	dhcp-snooping rate-limit <i>limit-value</i>	必选 缺省情况，DHCP 报文速率上限值为 40pps

说明：

- 在汇聚组配置模式下配置 DHCP 报文速率上限值后，该汇聚组的每一个成员端口的 DHCP 报文速率上限值均为该值。
- DHCP 报文限速功能只对非信任端口生效，对信任端口不生效。
- 端口被自动关闭后，可通过配置 Error-Disable 将端口自动启用。缺省情况下，端口自动关闭功能处于使能状态；如果端口连续 20 秒收到的 DHCP 报文都超速，但未能将相应端口自动关闭，需查看 Error-Disable 配置。Error-Disable 功能，参见配置手册 Error-Disable 相关章节。

52.2.2 配置 DHCP snooping Option82 选项 **-B -S -E -A**

DHCP snooping 功能支持 Option82 选项，Option82 选项最多可以包含 255 个子选项。我司设备支持两个子选项：Circuit ID（电路 ID 子选项）和 Remote ID（远程 ID 子选项）。

配置条件

在配置 DHCP snooping Option82 选项之前，首先完成以下任务：

- 使能 DHCP snooping 功能。

配置 Option82 选项的处理策略

当端口上配置了去使能信息后，不管该端口收到什么样的选项报文，都原样转发。

表 4-5 配置 Circuit ID 内容

步骤	命令	说明
进入全局配置模式	configure terminal	-
使能 DHCP Snooping 功能的 Option82 选项	dhcp-snooping information enable	必选 缺省情况下，DHCP Snooping 功能的 Option82 选项处于禁用状态
进入二层以太接口配置模式	interface interface-name	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation link-aggregation-id	
配置 Option82 选项的处理策略	dhcp-snooping information disable	可选 缺省情况，对包含 Option82 选项的 DHCP 请求报文的处理策略为 replace，即替换后转发。

配置 Remote ID 内容

Remote ID 的内容分为默认内容和非默认内容两种。Remote ID 的默认内容填充格式如下图所示：

Remote ID Suboption Frame Format

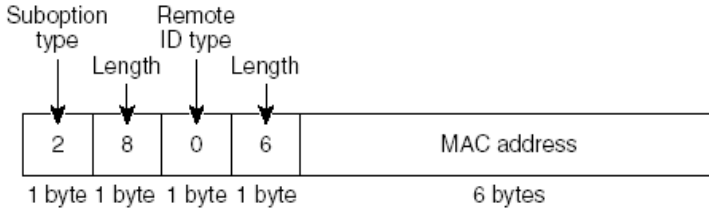


图 4-2 Remote ID 默认内容填充格式

非默认内容分为自定义字符串和设备名称两种，需在填充格式配置为用户配置格式下生效。Remote ID 的非默认内容填充格式如下图所示：

Remote ID Suboption Frame Format (for user-configured string):

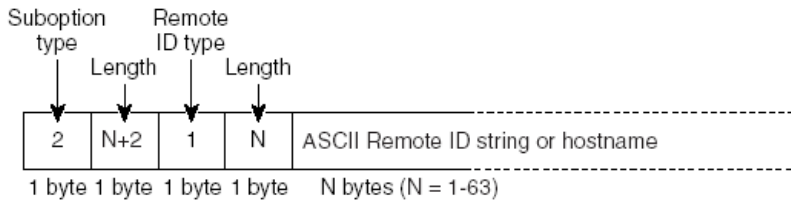


图 4-3 Remote ID 非默认内容填充格式

表 4-6 配置 Remote ID 内容

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 Remote ID 内容	dhcp-snooping information format remote-id { <i>string</i> default <i>hostname</i> }	必选 缺省情况，Remote ID 内容为默认内容，即设备端口的 MAC 地址

配置 Circuit ID 内容

Circuit ID 的内容分为默认内容和非默认内容两种。Circuit ID 的默认内容填充格式如下图所示：

Circuit ID Suboption Frame Format

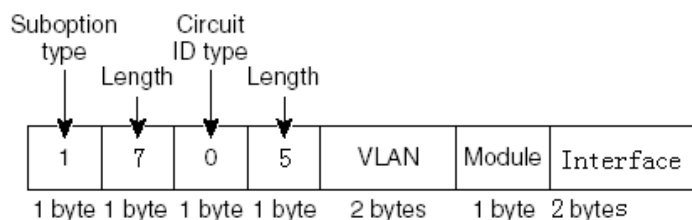


图 4-4 Circuit ID 默认内容填充格式

非默认内容，需在填充格式配置为用户配置格式下生效。Circuit ID 的非默认内容填充格式如下图所示：

Circuit ID Suboption Frame Format (for user-configured string):

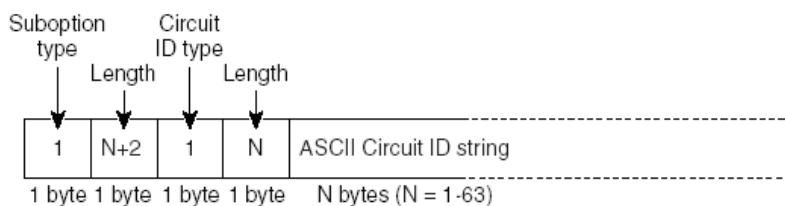


图 4-5 Circuit ID 非默认内容填充格式

表 4-7 配置 Circuit ID 内容

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface interface-name	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配
进入汇聚组配置模式	link-aggregation link-aggregation-id	

步骤	命令	说明
		置模式后, 后续配置只在 汇聚组生效
配置 Circuit ID 内容	dhcp-snooping information format circuit-id { <i>string</i> default }	必选 缺省情况, Circuit ID 内 容为默认内容

配置 Option82 选项填充格式

Option82 选项填充格式分为默认格式和用户配置格式。

当填充格式为默认格式时, Remote ID 和 Circuit ID 的内容均为默认内容; 只有当填充格式配置成用户配置格式后, Remote ID 和 Circuit ID 的非默认内容才会生效。

表 4-8 配置 Option82 选项填充格式

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 Option82 选项填充格式	dhcp-snooping information format { default user-config }	必选 缺省情况, 填充格式为默 认格式

配置 Option82 选项报文处理策略

配置 Option82 选项报文处理策略, 可以对包含 Option82 选项的 DHCP 请求报文采取不同的转发策略。

表 4-9 配置 Option82 选项报文处理策略

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 Option82 选项报文处理策略	dhcp-snooping information policy { drop keep replace }	必选 缺省情况，处理策略为 replace

52.2.3 配置 DHCP snooping 绑定表项存储

-B -S -E -A

DHCP snooping 功能支持绑定表项自动或手动存储到指定路径中，如果设备重启，可恢复已存储的绑定表项，避免因绑定表项丢失而影响通信。

指定路径可以是设备 FLASH、FTP 服务器或 TFTP 服务器。

配置条件

在配置绑定表项存储路径为 FTP/TFTP 服务器之前，首先完成以下任务：

- FTP/TFTP 服务器端，正常启用了 FTP/TFTP 服务器功能；
- 设备可以 ping 通 FTP/TFTP 服务器端的 IP 地址。

配置 DHCP snooping 绑定表项自动存储

DHCP snooping 绑定表项可配置为自动存储模式，即系统自行定时对绑定表项进行存储。

系统会周期性地对绑定表项进行刷新，检测绑定表项是否存在更新，如存在更新，需在存储时延到后，才将更新后的表项存储到指定路径中。存储时延可防止和控制因表项不断更新而导致系统频繁进行存储。

表 4-10 配置 DHCP snooping 绑定表项自动存储

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
配置 DHCP snooping 绑定表项自动存储	dhcp-snooping database savetype auto { flash <i>file-name</i> ftp <i>dest-ip-address ftp-username ftp-password file-name</i> tftp <i>dest-ip-address file-name</i> }	必选 缺省情况，绑定表项存储模式为自动模式，存储路径为 flash，存储文件名为“dhcsp_binding.db”
配置绑定表项存储时延	dhcp-snooping database savedelay <i>seconds</i>	可选 缺省情况，绑定表项存储时延为 1800 秒
配置绑定表项刷新时间间隔	dhcp-snooping database savepool <i>seconds</i>	可选 缺省情况，绑定表项刷新时间间隔为 30 秒

配置 DHCP snooping 绑定表项手动存储

DHCP snooping 绑定表项可配置为手动存储模式，即须通过执行存储命令完成绑定表项的存储。

表 4-11 配置 DHCP snooping 绑定表项手动存储

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 DHCP snooping 绑定表项手动存储	dhcp-snooping database savetype manual { flash <i>file-name</i>	必选 缺省情况，绑定表项存储模式为自动模式，存储路

步骤	命令	说明
	ftp <i>dest-ip-address</i> <i>ftp-username</i> <i>ftp-password</i> <i>file-name</i> tftp <i>dest-ip-address</i> <i>file-name</i> }	径为 flash, 存储文件名为 "dhcsp_binding.db"
配置存储绑定文件	dhcp-snooping database save	必选 将绑定表项存储到指定路径中 缺省情况, 绑定表项未存储到指定路径中

52.2.4 DHCP snooping 监控与维护

-B -S -E -A

表 4-12 DHCP snooping 监控与维护

命令	说明
clear dhcp-snooping database { interface <i>interface-list</i> link-aggregation <i>link-aggregation-id</i> ip-address <i>ip-address</i> / mac-address <i>mac-address</i> vlan <i>vlan-id</i> all }	清除绑定表项
clear dhcp-snooping packet statistics [interface <i>interface-name</i> link-aggregation <i>link-aggregation-id</i>]	清除收发 DHCP 报文统计信息

命令	说明
show dhcp-snooping [interface <i>interface-name</i> link-aggregation <i>link-aggregation-id</i> save detail]	显示 DHCP snooping 的配置信息
show dhcp-snooping database [{ begin exclude include } <i>expression</i> redirect { file <i>file-name</i> ftp [vrf <i>vrf-name</i>] { <i>hostname</i> <i>dest-ip-address</i> } <i>ftp-username</i> <i>ftp-password</i> <i>file-name</i> } }] [interface <i>interface-name</i> ip-address <i>ip-address</i> vlan <i>vlan-id</i> mac-address <i>mac-address</i> link-aggregation <i>link-aggregation-id</i> [{ begin exclude include } <i>expression</i> redirect { file <i>file-name</i> ftp [vrf <i>vrf-name</i>] { <i>hostname</i> <i>dest-ip-address</i> } <i>ftp-username</i> <i>ftp-password</i> <i>file-name</i> } }] detail]	显示 DHCP snooping 绑定表项信息
show dhcp-snooping packet statistics [interface <i>interface-name</i> link-aggregation <i>link-aggregation-id</i>]	显示收发 DHCP 报文的统计信息

52.3 DHCP snooping 典型配置举例

52.3.1 配置 DHCP snooping 的基本功能

-B -S -E -A

网络需求

- DHCP Server1 为合法的 DHCP 服务器，DHCP Server2 为非法的 DHCP 服务器。
- 配置 DHCP snooping 功能后，PC1 和 PC2 均只能从 DHCP Server1 获取地址。

网络拓扑

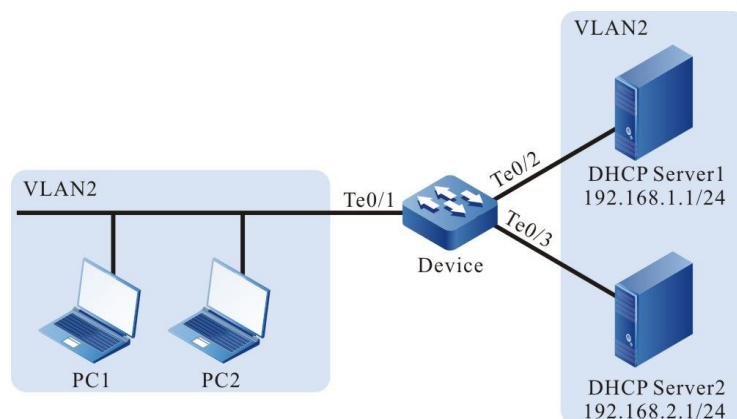


图 4-6 配置 DHCP snooping 基本功能组网图

配置步骤

步骤 1： 在 Device 上配置 VLAN 和端口的链路类型。

#创建 VLAN2。

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#配置端口 tengigabitethernet0/1~tengigabitethernet0/3 的链路类型为 Access，允许 VLAN2 的业务通过。

```
Device(config)#interface tengigabitethernet 0/1-0/3
Device(config-if-range)#switchport mode access
Device(config-if-range)#switchport access vlan 2
Device(config-if-range)#exit
```

步骤 2： 配置 DHCP Server1 的地址池为 192.168.1.100~192.168.1.199 和 DHCP Server2 的地址池为 192.168.2.100~192.168.2.199。（略）

步骤 3： 在 Device 上配置 DHCP snooping 功能。

#使能 DHCP snooping 功能。

配置手册

发布 1.1 04/2020

```
Device(config)#dhcp-snooping
```

#配置端口 tengigabitethernet0/2 为信任端口。

```
Device(config)#interface tengigabitethernet 0/2
Device(config-if-tengigabitethernet0/2)#dhcp-snooping trust
Device(config-if-tengigabitethernet0/2)#exit
```

步骤 4: 检验结果。

#PC1 和 PC2 成功获取地址后, 在 Device 上查看 DHCP snooping 表项。

```
Device#show dhcp-snooping database
dhcp-snooping database:
database entries count:2
database entries delete time :300
-----
 macAddr      ipAddr      transtion-id  vlan  interface  leaseTime(s)  status
-----
0013.0100.0002 192.168.1.101  1      2    te0/1      107990        active
-----
0013.0100.0001 192.168.1.100  0      2    te0/1      107989        active
-----
Total valid DHCP Client binding table for this criterion: 2
```

PC1、PC2 均只能从 DHCP Server1 获取地址。

53 Dynamic ARP Inspection

53.1 Dynamic ARP Inspection 简介

Dynamic ARP Inspection (动态 ARP 检测) 功能, 简称 DAI 功能。通过检测 ARP (Address Resolution Protocol, 地址解析协议) 报文的合法性, 发现并防止 ARP 欺骗攻击, 增强网络安全性。DAI 功能主要分为以下两类:

- 端口 DAI 功能: 对指定端口接收到的 ARP 报文进行合法性检测, 便于发现并防止 ARP 欺骗攻击;

ARP 报文合法性检测的依据为端口 IP Source Guard 绑定表项, 具体检测原理如下:

接收到的 ARP 报文中, 发送端 IP 地址、源 MAC 地址及 VLAN ID 与端口 IP Source Guard 绑定表项完全匹配, 则该 ARP 报文为合法报文, 对其进行转发; 否则, 该 ARP 报文为非法报文, 将其丢弃, 并记录日志信息。

- 全局 DAI 功能: 对所有端口接收到的 ARP 报文进行合法性检测, 防止伪装用户发送伪造的 ARP 报文, 导致设备建立错误的 ARP 表项。

ARP 报文合法性检测的依据为全局 IP Source Guard 绑定表项, 具体检测原理如下:

接收到的 ARP 报文中, 发送端 IP 地址与全局 IP Source Guard 绑定表项中的 IP 地址相同, 但源 MAC 地址不同时, 该 ARP 报文为伪造报文, 将其丢弃, 不记录日志信息。

端口 DAI、全局 DAI 功能还会对 ARP 报文进行有效性检测, 具体检测原理如下:

接收到的 ARP 报文中的源 MAC 地址与发送端 MAC 地址不同, 则该报文为无效报文, 将其丢弃, 不记录日志信息。

- 端口 ARP 攻击检测: 对指定端口接收到的 ARP 报文不进行合法性检测, 只记录日志信息, 用于发现 ARP 攻击。

53.2 Dynamic ARP Inspection 功能配置

表 5-1 Dynamic ARP Inspection 功能配置列表

配置任务	
配置端口 Dynamic ARP Inspection 功能	配置端口 Dynamic ARP Inspection 功能
配置全局 Dynamic ARP Inspection 功能	配置全局 Dynamic ARP Inspection 功能

53.2.1 配置端口 Dynamic ARP Inspection 功能

-B -S -E -A

配置条件

在配置端口 Dynamic ARP Inspection 功能前，首先完成以下任务：

- 配置端口 IP Source Guard 绑定表项。

配置端口 Dynamic ARP Inspection 功能

使能端口 DAI 功能后，系统会依据端口 IP Source Guard 绑定表项，对该端口接收到的 ARP 报文进行合法性检测，非法报文会被丢弃，且被记录到日志中。

日志中记录的内容包括：VLAN ID、接收端口、发送端 IP 地址、目的 IP 地址、发送端 MAC 地址、目的 MAC 地址、相同非法 ARP 报文数。用户可以根据记录的日志信息来作进一步分析，比如定位发起 ARP 攻击的主机。

缺省情况下，日志信息周期性输出，可通过配置日志输出间隔时间来控制报文的记录、输出及老化。日志输出间隔时间作为以下日志相关参数的基础值：

- 日志刷新周期：用于判断日志是否需输出及老化。如果配置的日志输出间隔时间小于 5 秒，则日志刷新周期等于 1 秒；否则，日志刷新周期等于五分之一的日志输出间隔时间；
- 日志老化时间：老化时间超时后，日志会被删除。日志老化时间为一倍的日志输出间隔时间；
- 日志令牌：日志刷新周期内，允许记录的最大日志数目。日志令牌数为十五倍的日志刷新周期值。

使能端口 DAI 功能后，还可以配置端口 ARP 限速功能，即对每秒处理的 ARP 报文数目进行限制，避免系统由于长期处理大量 ARP 报文，导致其他协议报文无法及时得到处理。

说明：

- 端口 ARP 限速功能，即对每秒处理的 ARP 报文数目进行限制，避免系统由于长期处理大量 ARP 报文，导致其他协议报文无法及时得到处理。一秒内接收到的 ARP 报文数目超过速率上限值后，这一秒内后续接收到的 ARP 报文会被丢弃。如果端口连续 20 秒接收到的 ARP 报文都超速，则会将相应端口关闭，来隔离报文冲击源。

表 5-2 配置端口 Dynamic ARP Inspection 功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface <i>interface-name</i>	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	
使能端口 DAI 功能	ip arp inspection	必选 缺省情况下，端口 DAI 功能处于禁用状态
配置端口处理 ARP 报文的 上限值	ip arp inspection rate-limit <i>limit-value</i>	可选 缺省情况下，端口处理 ARP 报文的上限值为 15pps

步骤	命令	说明
回退到全局配置模式	exit	-
配置缓存日志数目	ip arp inspection log-buffer <i>buffer-size</i>	可选 缺省情况下，系统可以缓存的日志数为 32 配置为 0，表示日志不进行缓存，即检测到非法 ARP 报文后，日志直接输出到终端
配置日志输出间隔时间	ip arp inspection log-interval <i>seconds</i>	可选 缺省情况下，日志输出间隔时间为 20 秒 配置为 0，表示日志的输出不需等待，即检测到非法 ARP 报文后，日志直接输出到终端
配置日志输出级别	ip arp inspection log-level <i>log-level</i>	可选 缺省情况下，日志输出级别为 6

说明：

- 端口 DAI 功能使能后，对应端口收到的所有 ARP 报文（广播 ARP 及单播 ARP）都重定向到 CPU 进行检测、软件转发、日志记录等，当 ARP 报文量较大时会严重消耗 CPU 资源，因此，在设备通信正常的情况下，不建议使能端口 DAI 功能，当怀疑网络中存在 ARP 欺骗攻击时，才需要使能端口 DAI 功能来进行检测和定位。

- 同一端口下，端口 DAI 功能不能与端口安全功能同时使能。
- 在汇聚组配置模式下配置端口处理 ARP 报文速率上限值后，该汇聚组的每个成员端口的 ARP 报文速率上限值均为该值。
- 如果端口连续 20 秒收到的 ARP 报文都超过上限值，但端口未自动关闭，需参见配置手册 Error-Disable 相关章节。

53.2.2 配置全局 Dynamic ARP Inspection 功能

-B -S -E -A

配置条件

在配置全局 Dynamic ARP Inspection 功能前，首先完成以下任务：

- 配置全局 IP Source Guard 绑定表项。

配置全局 Dynamic ARP Inspection 功能

使能全局 DAI 功能后，系统会依据全局 IP Source Guard 绑定表项，对接收到的 ARP 报文进行合法性检查，非法报文直接丢弃，不会记录日志。

表 5-3 配置全局 Dynamic ARP Inspection 功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
使能全局 DAI 功能	arp-security	必选 缺省情况下，全局 DAI 功能处于禁用状态

53.2.3 配置 Dynamic ARP Inspection ARP 攻击检测

-B -S -E -A

配置条件

配置手册

发布 1.1 04/2020

无

配置 Dynamic ARP Inspection ARP 攻击检测

使能 ARP 攻击检测后，系统会对接收到的 ARP 报文不进行合法性检查，只记录日志。

表 5-4 配置 Dynamic ARP Inspection ARP 攻击检测

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface <i>interface-name</i>	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	
使能端口 ARP 攻击检测	ip arp inspection attack	必选 缺省情况下，端口未使能 ARP 攻击检测

53.2.4 Dynamic ARP Inspection 监控与维护 -B -S -E -A

表 5-5 Dynamic ARP Inspection 监控与维护

命令	说明
clear ip arp inspection { log-information log-statistics pkt-statistics [interface <i>interface-name</i> 	删除 DAI 功能记录的统计相关信息

命令	说明
link-aggregation <i>link-aggregation-id</i> }	
show arp-security	显示全局 DAI 功能状态
show ip arp inspection [interface <i>interface-name</i> link-aggregation <i>link-aggregation-id</i>]	显示端口 DAI 功能的配置信息
show ip arp inspection log-information	显示端口 DAI 功能记录的日志信息
show ip arp inspection log-statistics	显示日志数目相关的统计信息
show ip arp inspection pkt-statistics [interface <i>interface-name</i> link-aggregation <i>link-aggregation-id</i>]	显示 ARP 报文相关的统计信息

53.3 DAI 典型配置举例

53.3.1 配置 DAI 基本功能 **-B -S -E -A**

网络需求

- PC1、PC2 通过 Device 接入 IP Network。
- 在 Device 上配置端口 DAI 功能，防止 ARP 攻击和欺骗。

网络拓扑

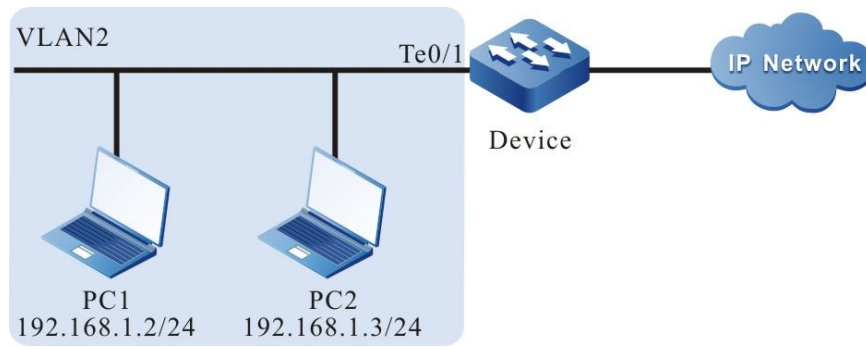


图 5-1 配置 DAI 基本功能组网图

配置步骤

步骤 1： 在 Device 上配置 VLAN 和端口的链路类型。

#创建 VLAN2。

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#配置端口 tengigabitethernet0/1 的链路类型为 Access，允许 VLAN2 的业务通过。

```
Device(config)#interface tengigabitethernet 0/1
Device(config-if-tengigabitethernet0/1)#switchport mode access
Device(config-if-tengigabitethernet0/1)#switchport access vlan 2
Device(config-if-tengigabitethernet0/1)#exit
```

步骤 2： 在 Device 上配置端口 DAI 功能。

#在端口 tengigabitethernet0/1 上使能端口 DAI 功能，并配置端口 tengigabitethernet0/1 处理 ARP 报文的上限值为 30pps。

```
Device(config)#interface tengigabitethernet 0/1
Device(config-if-tengigabitethernet0/1)#ip arp inspection
Device(config-if-tengigabitethernet0/1)#ip arp inspection rate-limit 30
Device(config-if-tengigabitethernet0/1)#exit
```

步骤 3： 在 Device 上配置绑定表项。

#在端口 tengigabitethernet0/1 上配置 MAC 地址为 0012.0100.0001，IP 地址为 192.168.1.2，VLAN 为 2 的端口 IP Source Guard 绑定表项。

```
Device(config)#interface tengigabitethernet 0/1
Device(config-if-tengigabitethernet0/1)#ip source binding 0012.0100.0001 vlan 2 192.168.1.2
Device(config-if-tengigabitethernet0/1)#exit
```

步骤 4: 检验结果。

#查看 DAI 相关配置信息。

```
Device#show ip arp inspection
Dynamic ARP Inspection information:
Dynamic ARP Inspection log buffer size: 30
Dynamic ARP Inspection log Interval: 20
Dynamic ARP Inspection log Level: 6
Dynamic ARP Inspection interface information :
-----
interface      status  rate-limit(pps)  attack
te0/1          enable  30                OFF
te0/2          disable 15                OFF
.....
```

#当端口 tengigabitethernet0/1 接收 ARP 报文的速率超过 30pps 时, Device 会将超过速率的报文丢弃, 并输出以下提示信息。

```
Jan 1 02:21:06: The rate on interface tengigabitethernet0/1 too fast ,the arp packet drop!
```

#当端口 tengigabitethernet0/1 接收 ARP 报文的速率超过 30pps 且持续 20 秒时, Device 将关闭端口 tengigabitethernet0/1, 并输出以下提示信息。

```
Jan 1 02:21:26: %LINK-INTERFACE_DOWN-4: interface tengigabitethernet0/1, changed state to down
Jan 1 02:21:26: The rate of arp packet is too fast,dynamic arp inspection shut down the tengigabitethernet0/1 !
```

#当端口 tengigabitethernet0/1 接收到的 ARP 报文与绑定表项不一致时, Device 记录以下格式的非非法信息到 DAI 日志中, 并定时输出。

```
Jan 1 07:19:49: SEC-7-DARPLLOG: sender IP address: 192.168.1.3 sender MAC address:0011.0100.0001 target IP address: 0.0.0.0 target MAC address:0000.0000.0000 vlan ID:2 interface ID: tengigabitethernet0/1 record packet :32 packet(s)
```

#查看 DAI 日志。

```
Device#show ip arp inspection log-information
LogCountInBuffer:1
```

```
SEC-7-DARPLLOG: sender IP address: 192.168.1.3 sender MAC address:0011.0100.0001 target IP address: 0.0.0.0 target MAC address:0000.0000.0000 vlan ID:2 interface ID: tengigabitethernet0/1 record packet :0 packet(s)
```

53.3.2 DAI 与 DHCP Snooping 联用

-B -S -E -A

网络需求

- PC1、PC2 通过 Device1 接入 IP Network，PC2 为 DHCP 客户端，Device2 为 DHCP 中继。
- Device1 配置 DHCP Snooping 及端口 DAI 功能，实现 PC2 能正常访问 IP Network，PC1 不能访问 IP Network。

网络拓扑

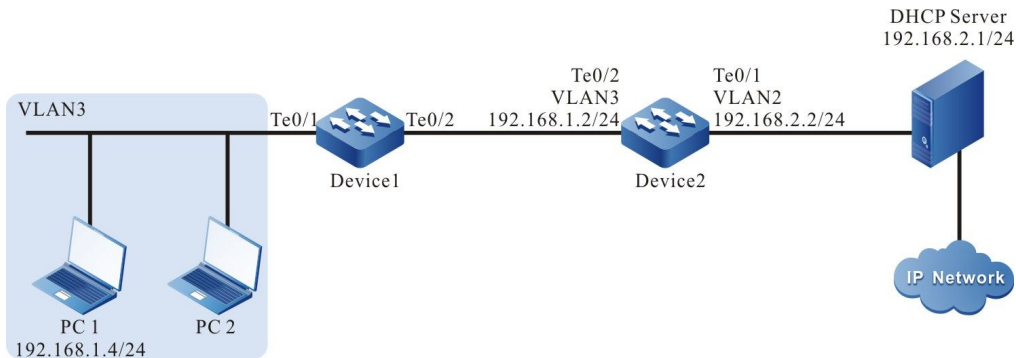


图 5-2 DAI 与 DHCP Snooping 联用组网图

配置步骤

步骤 1： 在 Device1 上配置 VLAN 和端口的链路类型。

#创建 VLAN3。

```
Device1#configure terminal
Device1(config)#vlan 3
Device1(config-vlan3)#exit
```

#配置端口 tengigabitethernet0/1 和端口 tengigabitethernet0/2 的链路类型为 Access，都允许 VLAN3 的业务通过。

```
Device1(config)#interface tengigabitethernet 0/1-0/2
Device1(config-if-range)#switchport access vlan 3
Device1(config-if-range)#exit
```

步骤 2： 在 Device2 上配置 VLAN 和端口的链路类型。

#创建 VLAN2 和 VLAN3。

```
Device2#configure terminal
Device2(config)#vlan 2-3
```

#配置端口 tengigabitethernet0/1 和端口 tengigabitethernet0/2 的链路类型为 Access，端口 tengigabitethernet0/1 允许 VLAN2 的业务通过，端口 tengigabitethernet0/2 允许 VLAN3 的业务通过。

```
Device2(config)#interface tengigabitethernet 0/1
Device2(config-if-tengigabitethernet0/1)#switchport mode access
Device2(config-if-tengigabitethernet0/1)#switchport access vlan 2
Device2(config-if-tengigabitethernet0/1)#exit
Device2(config)#interface tengigabitethernet 0/2
Device2(config-if-tengigabitethernet0/2)#switchport mode access
Device2(config-if-tengigabitethernet0/2)#switchport access vlan 3
Device2(config-if-tengigabitethernet0/2)#exit
```

步骤 3： 在 Device1 和 Device2 上配置对应 VLAN 接口及 IP 地址。（略）

步骤 4： 在 Device1 上配置 DHCP Snooping 功能。

#使能 DHCP Snooping 功能，配置端口 gigabitethernet0/2 为信任端口。

```
Device1(config)#dhcp-snooping
Device1(config)#interface tengigabitethernet 0/2
Device1(config-if-tengigabitethernet0/2)#dhcp-snooping trust
Device1(config-if-tengigabitethernet0/2)#exit
```

步骤 5： 在 Device1 上配置端口 DAI 功能。

#端口 tengigabitethernet0/1 上使能端口 DAI 功能。

```
Device1(config)#interface tengigabitethernet 0/1
Device1(config-if-tengigabitethernet0/1)#ip arp inspection
Device1(config-if-tengigabitethernet0/1)#exit
```

步骤 6： 在 Device2 上配置 DHCP 中继服务器 IP 地址。

#配置 DHCP 中继服务器 IP 地址为 198.168.2.1。

```
Device2(config)#ip dhcp-server 192.168.2.1
```

步骤 7： 检验结果。

#PC2 成功获取到地址后，在 Device1 上查看 DHCP Snooping 动态表项。

```
Device1#show dhcp-snooping database
dhcp-snooping database:
database entries count:1
database entries delete time :300
-----
macAddr    ipAddr    transtion-id  vlan  interface  leaseTime(s)  status
0013.0100.0001 192.168.1.100  2      2    te0/1      107990        active
-----
```

#PC2 能正常访问 IP Network，PC1 不能访问 IP Network。

54 Host Guard

54.1 Host Guard 简介

Host Guard（主机保护）功能主要用于接入层设备，防止攻击者伪造的 ARP（Address Resolution Protocol，地址解析协议）报文破坏终端设备上的 ARP 表。Host Guard 保护的主机 IP 地址通常对应于网络中的网关设备、重要服务器的 IP 地址。

Host Guard 功能中存在以下两个概念：

- 主机保护组：由一系列的主机保护组规则组成，即被保护的主机 IP 地址的集合；
- 主机保护组规则：一条被保护的主机 IP 地址。

Host Guard 功能的工作原理如下：

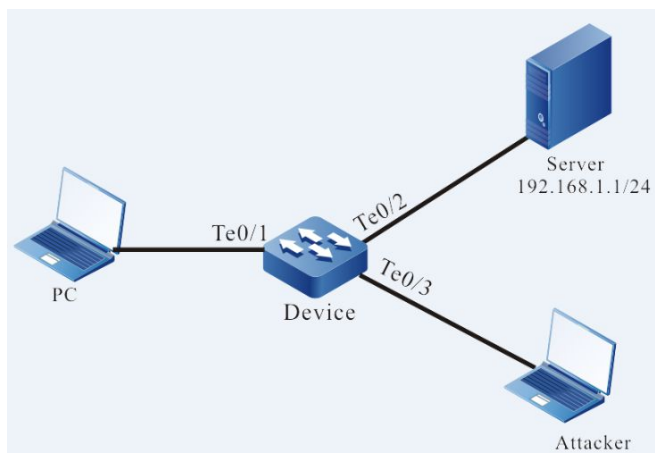


图 6-1 Host Guard 功能简介图

如上图所示，Attacker 可以利用 Server 的 IP 地址 192.168.1.1 伪造 ARP 报文，经过 Device 转发到 PC，将 PC 上的 ARP 表破坏，导致 PC 不能够正常访问 Server。

在 Device 上，把 Server 的 IP 地址 192.168.1.1 作为一条主机保护组规则应用到端口 te0/2 后，当 Device 接收到的 ARP 报文中，发送端 IP 地址与 Server 的 IP 地址相同，如果接收端口是 te0/2，该报文可被正常处理；如果接收端口不是 te0/2，该报文被丢弃。即 Server 发送的 ARP 报文只能通过端口 te0/2 转发，Attacker 伪造的 ARP 报文会被丢弃。

54.2 Host Guard 功能配置

表 6-1 Host Guard 功能配置列表

配置任务	
配置 Host Guard 功能	配置主机保护组
	配置主机保护组的应用

54.2.1 配置 Host Guard 功能

-B -S -E -A

配置条件

配置手册

发布 1.1 04/2020

无

配置主机保护组

主机保护组由一系列的主机保护组规则组成，可将网络中的网关、重要服务器的 IP 地址配置为主机保护组中的规则。

表 6-2 配置主机保护组

步骤	命令	说明
进入全局配置模式	configure terminal	-
创建主机保护组	host-guard group <i>group-name</i>	必选 缺省情况下，没有创建任何主机保护组
配置主机保护组规则	permit host <i>ip-address</i>	必选 缺省情况下，未配置主机保护组规则

说明：

- 每个主机保护组中最多支持 128 条主机保护组规则。

配置主机保护组的应用

将主机保护组应用到端口上，可对接收到的 ARP 报文进行监控，实现对 ARP 表的保护。

表 6-3 配置主机保护组的应用

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface <i>interface-name</i>	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	
配置主机保护组的应用	host-guard binding <i>group-name</i>	必选 缺省情况下，端口或汇聚组上不存在应用的主机保护组

54.2.2 Host Guard 监控与维护

-B -S -E -A

表 6-4 Host Guard 监控与维护

命令	说明
show host-guard binding [interface <i>interface-id</i> link-aggregation <i>link-aggregation-id</i>]	显示主机保护组的应用信息
show host-guard group [<i>group-name</i>]	显示主机保护组及规则的配置信息

55 AAA

55.1 AAA 简介

AAA 指的是 Authentication (认证), Authorization (授权), Accounting (统计)。自网络诞生以来, 认证、授权以及统计体制就成为其运营的基础。网络中各类资源的使用, 需要由认证、授权和统计进行管理。AAA 一般采用客户机/服务器结构, 客户端运行于 NAS (Network Access Server, 网络接入服务器) 上, 服务器上集中管理用户信息。NAS 对于用户来讲是服务器端, 对于服务器来说是客户端。

其中, 认证 (Authentication) 指用户在使用网络系统中的资源时对用户身份的确认。这一过程, 通过与用户的交互获得身份信息, 然后提交给认证服务器; 后者对身份信息与存储在数据库里的用户信息进行核对处理, 然后根据处理结果确认用户身份是否正确。授权 (Authorization) 指网络系统授权用户以特定的方式使用其资源, 这一过程指定了被认证的用户在接入网络后能够使用的业务和拥有的权限, 如授予的 IP 地址等。统计 (Accounting) 指网络系统收集、记录用户对网络资源的使用, 以便向用户收取资源使用费用, 或者用于审计等目的。

RADIUS (远程身份认证拨入用户服务) 是一种 C/S 结构的协议, 它的客户端最初就是 NAS 服务器。RADIUS 协议认证机制灵活, 可以采用 PAP、CHAP 或者 Unix 登录认证等多种方式。RADIUS 是一种可扩展的协议, 它进行的全部工作都是基于 Attribute-Length-Value 的向量进行的。RADIUS 的基本工作原理是: 用户接入 NAS, NAS 向 RADIUS 服务器使用 Access-Require 数据包提交用户信息, 包括用户名、密码等相关信息, 其中用户密码是经过 MD5 加密的, 双方使用共享密钥, 这个密钥不经过网络传播; RADIUS 服务器对用户名和密码的合法性进行检验, 必要时可以提出一个 Challenge, 要求进一步对用户认证, 也可以对 NAS 进行类似的认证; 如果合法, 给 NAS 返回 Access-Accept 数据包, 允许用户进行下一步工作, 否则返回 Access-Reject 数据包, 拒绝用户访问; 如果允许访问, NAS 向 RADIUS 服务器提出统计请求 Account-Require, RADIUS 服务器响应 Account-Accept, 对用户的统计开始, 同时用户可以进行自己的相关操作。

TACACS（终端访问控制器访问控制系统）对于 Unix 网络来说是一个比较老的认证协议，它允许远程访问服务器传送用户登录密码给认证服务器，认证服务器决定该用户是否可以登录系统。TACACS 是一个加密协议，但它的安全性不及之后的 TACACS+ 和 RADIUS。TACACS+ 其实是一个全新的协议。TACACS+ 和 RADIUS 在现有网络里已经取代了早期的协议。TACACS+ 使用传输控制协议（TCP），而 RADIUS 使用用户数据报协议（UDP）。RADIUS 从用户角度结合了认证和授权，而 TACACS+ 分离了这两个操作。

55.2 AAA 功能配置

表 55-1 AAA 功能配置列表

配置任务	
配置 AAA 域	配置 ISP 域
配置 AAA 域下认证功能	配置 ISP 域下 default、login、ppp、xauth 认证方法
配置 AAA 域下授权功能	配置 ISP 域下 default、login、ppp、xauth 授权方法
配置 AAA 域下统计功能	配置 ISP 域下 default、login、ppp、xauth 统计方法
配置进入特权模式的认证方法	配置进入特权模式的认证方法
配置开启命令行授权	配置启用命令行授权
	配置启用 Console 授权
配置系统统计功能	配置系统事件统计方法
配置统计相关属性	配置关闭空用户名统计

配置任务	
	配置发送统计更新报文
	配置发送统计失败处理方式
配置 RADIUS 方案	配置 RADIUS 服务器
	配置 RADIUS 相关属性
	配置发送 RADIUS 报文的源地址
配置 TACACS 方案	配置 TACACS 服务器
	配置发送 TACACS 报文的源地址

55.2.1 配置 AAA 域

-B -S -E -A

域：（domain）NAS对用户的管理是基于ISP（Internet Service Provider，互联网服务提供者）域的，每个用户都属于一个ISP域，一般情况下，用户所属的ISP域是由用户登录时提供的用户名决定的。系统默认存在一个system域。在域下面可以配置每种接入用户的认证、授权、计费方法。

基于域进行用户和AAA管理的解决方案完整阐述如下：

NAS 设备对用户的管理是基于ISP 域的。一般情况下，用户所属的 ISP 域是由用户登录时提供的用户名决定的。

“用户输入的用户名” = “设备理解的用户名” + “域名”

用户认证时，设备按照如下先后顺序判定其所属的域，然后执行域中的AAA策略：

- 1) 【可选】登录/接入模块配置指定的认证域；
- 2) 用户名中指定的ISP 域；
- 3) 系统缺省的 ISP 域。

配置条件

无

配置 ISP 域

表 55-2 配置 AAA 域

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 ISP 域视图	domain <i>isp-name</i>	可选。 缺省情况下，系统存在一个名称为 system 的 ISP 域。
退出到全局配置模式	exit	-
配置缺省的 ISP 域	domain default enable <i>isp-name</i>	可选。 缺省情况下，系统缺省 ISP 域为 system 域。

55.2.2 配置 AAA 域下认证功能 -B -S -E -A

AAA 提供了一系列的认证方式保证设备及网络服务的安全性。比如，通过对用户登录进行认证，禁止非法用户操作设备；对用户进入特权模式进行认证，限制用户对设备的使用权限；对 PPP 会话连接进行认证，限制非法连接的建立。

配置条件

无

配置 ISP 域下认证方法

用户在尝试登录某个特定 ISP 域的时候，AAA 可以对该用户进行认证，禁止认证不通过的用户登录到指定的 ISP 域上。

表 55-3 配置 ISP 域下认证方法列表

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 ISP 域视图	domain <i>isp-name</i>	必选。 缺省情况下，系统存在一个名称为 system 的 ISP 域。
配置 ISP 域下缺省认证方法	aaa authentication default { none / local / radius-group <i>group-name</i> / tacacs-group <i>group-name</i> }	可选。 缺省情况下，ISP 域下的 default 认证方法为 local。
配置 ISP 域下用户登录认证方法	aaa authentication login { none / enable / local / radius-group <i>group-name</i> / tacacs-group <i>group-name</i> }	可选。 缺省情况下，未配置登录认证方法，采用域下缺省认证方法。
配置 ISP 域下 dot1x 认证方法	aaa authentication dot1x { none / local / radius-group <i>group-name</i> / tacacs-group <i>group-name</i> }	可选。 缺省情况下，未配置 dot1x 认证方法，采用域下缺省认证方法。

55.2.3 配置 AAA 域下授权功能 **-B -S -E -A**

在认证成功后，AAA 的授权功能可以控制管理员用户对设备资源的权限，以及控制接入用户对网络资源的访问，限制管理员执行未被授权的命令，限制接入用户访问未被授权的网络资源。

配置条件

在配置域下的命令行授权，请先配置开启命令行授权，域下配置的命令行授权才能生效。

配置 ISP 域下授权方法

用户在执行某个特定 ISP 域下的授权项时，AAA 可以对该用户进行授权，赋予用户一定的权限，并禁止授权不通过的用户执行域下的授权项。

表 55-4 配置 ISP 域下授权方法列表

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 ISP 域视图	domain <i>isp-name</i>	必选。 缺省情况下，系统存在一个名称为 system 的 ISP 域。
配置 ISP 域下缺省授权方法	aaa authorization default { if-authenticated / local / none / radius-group <i>group-name</i> / tacacs-group <i>group-name</i> }	可选。 缺省情况下，ISP 域下授权方法为 none
配置 ISP 域下 commands 授权方法	aaa authorization commands <i>cmd- /</i> { if-authenticated / none / radius-	可选。 缺省情况下，未配置 ISP 域下

步骤	命令	说明
	group <i>group-name</i> / tacacs-group <i>group-name</i> }	commands 授权方法。域下的授权方法为 none。 必须开启命令授权功能该配置才能生效。
配置 ISP 域下用户登录设备授权方法	aaa authorization login { if-authenticated / local / none / radius-group <i>group-name</i> / tacacs-group <i>group-name</i> }	可选。 缺省情况下, 未配置 ISP 域下登录授权方法, 使用域下缺省授权方法。

说明:

- **aaa authorization commands** 命令和 **aaa authorization config-commands** 命令配置无先后顺序。

55.2.4 配置 AAA 域下统计功能

-B -S -E -A

用户在设备上的使用命令情况、登录会话情况、网络服务状况以及系统事件等都可以采用用户定义的方法进行统计, 统计的结果可以作为对用户计费的依据。

配置条件

无

配置 ISP 域下统计方法

用户在成功登录到某个 ISP 域上时，AAA 可以对该用户进行统计，包括统计登录起始时间、登录结束时间、输入过的命令等。

表 55-5 配置 ISP 域下统计方法

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 ISP 域视图	domain <i>isp-name</i>	必选。 缺省情况下，系统存在一个名称为 system 的 ISP 域。
配置 ISP 域下命令行统计方法	aaa accounting commands <i>cmd-lvl</i> { [broadcast] tacacs-group <i>group-name</i> }	可选。 缺省情况下，未配置命令统计方法，不进行命令统计。
配置 ISP 域下缺省统计方法	aaa accounting default { none { start-stop stop-only wait-start [broadcast] { radius-group <i>group-name</i> / tacacs-group <i>group-name</i> } } }	可选。 缺省情况下，ISP 域下统计方法为 none。
配置 ISP 域下用户登录设备统计方法	aaa accounting login { none { start-stop stop-only wait-start [broadcast] { radius-group <i>group-name</i> / tacacs-group <i>group-name</i> } } }	可选。 缺省情况下，未配置 ISP 域下用户登录设备统计方法，使用 ISP 域下缺省统计方法。

步骤	命令	说明
配置 ISP 域下 dot1x 统计方法	aaa accounting dot1x { none { start-stop stop-only wait-start [broadcast] { radius-group <i>group-name</i> / tacacs-group <i>group-name</i> } } }	可选。 缺省情况下，未配置 ISP 域下 dot1x 统计方法，使用 ISP 域下缺省统计方法。

55.2.5 配置进入特权模式认证方法

-B -S -E -A

用户成功登录设备后，AAA 可以对用户输入 enable 命令进入特权模式进行认证，禁止认证不通过的用户进入特权模式。

配置条件

无

配置特权模式认证方法

表 55-6 配置特权模式认证方法

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置特权模式认证方法	aaa authentication enable-method { none / enable / radius-group <i>group-name</i> / tacacs-group <i>group-name</i> }	可选。 缺省情况下，配置特权模式认证方法为 enable。

说明:

- 使用 **RADIUS** 认证方法时以 **\$enableLEVEL\$** 格式的用户名的密码作为验证密码，其中 **LEVEL** 表示当前用户进入的用户级别，取值范围是 **0-15**，**15** 级为最高级别。

55.2.6 配置开启命令行授权

-B -S -E -A

配置条件

无

配置启用命令授权

设备有 0~15 级命令，命令授权就是通过授权方法确定用户使用的命令级别，限制用户使用高于当前级别的命令。

表 55-7 全局模式下启用命令授权

步骤	命令	说明
进入全局配置模式	configure terminal	-
启用命令授权	aaa authorization config-commands	必选。 缺省情况下，关闭命令授权功能。

配置启用 CONSOLE 授权

如果需要对 CONSOLE 口进行访问限制，可以启用 CONSOLE 口授权，并且需要启动命令授权功能，打开后设备会对 CONSOLE 口执行的命令进行授权。

表 55-8 配置启用 Console 授权

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置启用 Console 授权	aaa authorization console	必选。 缺省情况下，未启用 Console 授权。

55.2.7 配置系统事件统计功能

-B -S -E -A

用户可以通过配置系统事件统计方法将系统启动和重启等事件发往服务器进行统计。

配置条件

无

配置系统事件统计方法

表 55-9 配置系统事件统计方法列表

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置系统事件统计方法	aaa accounting system { none { start-stop [broadcast] { tacacs-group group-name } } }	必选 缺省情况下，未对系统事件进行统计。

说明：

- 系统事件统计仅支持 TACACS 协议，不支持 RADIUS 协议。

55.2.8 配置统计相关属性 **-B -S -E -A**

配置条件

无

配置关闭空用户名统计

用户可以通过配置 **aaa accounting suppress null-username** 命令关闭 AAA 的空用户名统计。缺省情况下开启 AAA 对空用户名统计。

表 55-10 配置关闭空用户名统计

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置关闭空用户名统计	aaa accounting suppress null-username	必选。 缺省情况下，开启对空用户名统计。

配置发送统计更新报文

用户可以配置发送统计更新报文方式，主要包括实时发送和周期发送两种。

表 55-11 配置发送统计更新报文

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置发送统计更新报文	aaa accounting update periodic interval	必选。 缺省情况下，不发送统计更新报文

配置发送统计失败处理方式

表 55-12 配置发送统计失败处理方式

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置发送统计失败的处理方式	aaa accounting start-fail {online offline}	可选。 缺省情况下，统计开始失败用户不能上线。

55.2.9 配置 RADIUS 方案

-B -S -E -A

配置 RADIUS 方案需要完成服务器的关键参数配置。

配置条件

无

配置 RADIUS 服务器

若 AAA 需要使用 RADIUS 方法进行认证、授权以及统计时，需要配置 RADIUS 服务器相关参数，包括服务器 IP 地址、认证/授权端口、统计端口以及共享密钥等信息。

而在进入 RADIUS 服务器之前需要配置 RADIUS 服务器组，在配置方法列表时引用该服务器组名，即可使用 RADIUS 服务器组对用户进行认证、授权以及统计。

表 55-13 配置 RADIUS 服务器

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 RADIUS 服务器组名 (此命令也可以进入 RADIUS 服务器组配置模式)	aaa server group radius <i>group-name</i>	必选。 缺省情况下，未配置 RADIUS 服务器组名。
配置 RADIUS 服务器	server {<i>ip-address</i>/<i>ipv6 ip-address</i>} [acc-port <i>acc-port-num</i>] [auth-port <i>auth-port-num</i>] [priority <i>priority</i>] { key [0 7] <i>key</i> }	必选。 缺省情况下，未配置 RADIUS 服务器
配置 RADIUS 静默时间	dead-time <i>dead-time</i>	可选。 缺省情况下，RADIUS 服务器静默时间为 0，表示不静默。
配置 RADIUS 最大重传次数	retransmit <i>retries</i>	可选。 缺省情况下，向 RADIUS 服务器

步骤	命令	说明
		重传最大次数为 3 次。
配置 RADIUS 服务器应答超时时间	timeout <i>timeout</i>	可选。 缺省情况下，等待 RADIUS 服务器应答超时时间为 5 秒。
配置解析 RADIUS 服务器下发的 tunnel 属性时不检查 TAG 标识	tunnel without-tag	可选。 缺省情况下，解析 RADIUS 服务器下发的 tunnel 属性方式时需要 TAG 标识
配置 RADIUS 服务器组所属的 VRF	ip vrf forwarding <i>vrf-name</i>	可选。 缺省情况下，RADIUS 服务器组属于全局 VRF。

说明：

- 设备根据配置的 **priority** 值选择使用 **RADIUS** 服务器的顺序。
- 静默时间是指：设备把那些对认证请求不作出响应的 **RADIUS** 服务器标记为不可用，在 **dead-time** 这段时间内不再向这些服务器发送请求。
- 在设备和 **RADIUS** 服务器上配置的共享密钥必须一致。

配置 RADIUS 相关属性

表 55-14 配置 RADIUS 相关属性

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置登录认证的 RADIUS 报文中属性 service-type 的值	radius login service-type attr-value	可选 缺省情况下, RADIUS 报文中 service-type 值为 7
配置 NAS 设备与 RADIUS 服务器最大的并发数	radius control-speed pck-num	可选 缺省情况下, NAS 设备与 RADIUS 服务器最大的并发报文数为 100
配置客户端与服务器端会话的标识字段为 state	radius session state	可选 缺省情况下, 客户端与服务器端会话的标识字段为 session-id
配置 NAS 设备与 RADIUS 服务器通信使用固定的源端口	radius source-port fixed	可选 缺省情况下, NAS 设备与 RADIUS 服务器通信使用随机端口

配置发送 RADIUS 报文的源地址

表 55-15 配置发送 RADIUS 报文的源地址

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 RADIUS 源地址选择的接口	ip radius source-interface <i>interface-name</i> [vrf <i>vrf-name</i>]	可选 缺省情况下, 设备自动选择源接口

配置发送 RADIUS 的 accounting-on 功能

account-on 功能主要用于 AAA 进程第一次被拉起时将指定 RADIUS 服务器上的在线用户全部下线。缺省情况下, accounting-on 功能关闭; 当开启 account-on 功能, 缺省的重传间隔为 6 秒, 最大重传次数为 50 次; 由于高端设备业务板卡启动时间较慢, 建议用户在配置时, 设置重传次数和间隔时间尽量不要低于缺省值。

表 55-16 配置 RADIUS 的 accounting-on 功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 RADIUS 服务器组模式	aaa server group radius <i>group-name</i>	-
配置 RADIUS 的 account on 功能	accounting-on enable [interval <i>seconds</i> send <i>send-times</i>]	可选。 缺省情况下, accounting-on 功能关闭。

55.2.10配置 TACACS 方案

-B -S -E -A

配置 TACACS 方案需要配置服务器的关键参数。

配置条件

无

配置 TACACS 服务器

配置 TACACS 服务器后，若 AAA 需要使用 TACACS 方法进行认证、授权以及统计时，需要配置 TACACS 服务器相关参数，包括服务器 IP 地址、共享密钥、服务器端口号等配置信息。

在配置方法时引用该服务器组名，即可使用 TACACS 服务器组对用户进行认证、授权以及统计。

表 55-17 配置 TACACS 服务器

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 TACACS 服务器组名 (该命令也可以进入 TACACS 服务器组配置模式)	aaa server group tacacs group-name	必选。 缺省情况下，未配置 TACACS 服务器组名。
配置 TACACS 服务器	server {ip-address ipv6 ip-address} [port port-num] [priority priority] { key [0 7] key}	必选。 缺省情况下，未配置 TACACS 服务器组的成员服务器
配置 TACACS 服务器应答超时时间	timeout timeout	可选。 缺省情况下，等待 TACACS 服务

步骤	命令	说明
		器应答超时时间为 5 秒
配置 TACACS 服务器组的 VRF 属性	ip vrf forwarding <i>vrf-name</i>	可选。 缺省情况下，TACACS 服务器组属于全局 VRF

说明：

可以多次执行 **server** {*ip-address*|**ipv6** *ip-address*} [**port** *port-num*] [**priority** *priority*] {**key** [0 | 7] *key*}配置 TACACS 服务器组下的多个 TACACS 服务器，设备将根据配置的先后顺序选择服务器进行认证，当一个服务器失效后，设备会自动选择下一个服务器。

- 在设备和 TACACS 服务器上配置的共享密钥必须一致。

配置发送 TACACS 报文的源地址

表 55-18 配置发送 TACACS 报文的源地址

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 TACACS 源地址选择的接口	ip tacacs source-interface <i>interface-name</i> [vrf <i>vrf-name</i>]	可选。 缺省情况下，设备自动选择源接口

55.2.11 AAA 监控与维护

-B -S -E -A

表 55-19 AAA 监控与维护

命令	说明
debug aaa { authentication authorization accounting event error all }	打开 AAA 调试信息开关
debug radius [details]	打开 RADIUS 调试信息开关
debug tacacs [details]	打开 TACACS 调试信息开关
show aaa configuration	显示 AAA 配置信息
show aaa module [module-name]	用于显示 AAA 的功能模块，以及该模块最后一次操作 AAA 得到的结果
show aaa server [radius tacacs]	显示 AAA 的 RADIUS/TACACS 服务器配置和状态
show aaa session [module-name]	显示 AAA 统计会话
show aaa source-address	显示 AAA 使用的源地址

55.3 AAA 典型配置举例

55.3.1 配置 Telnet 用户登录使用本地认证

-B -S -E -A

网络需求

- 配置 Device 对 Telnet 用户登录进行本地认证。

网络拓扑

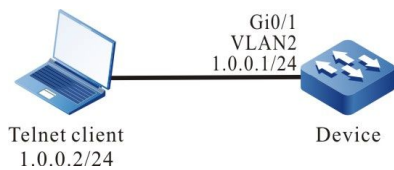


图 55-1 配置 Telnet 用户登录使用本地认证组网图

配置步骤

- 步骤 1： 配置 VLAN，并将端口加入对应的 VLAN。（略）
- 步骤 2： 配置各接口的 IP 地址。（略）
- 步骤 3： 配置 Device。

#配置用户名为 admin，密码为 admin。

```
Device#configure terminal
Device(config)#user admin password 0 admin
```

#配置 AAA 认证方式为本地认证。

```
Device(config)#aaa new-model
Device(config)#aaa authentication login default local
```

#配置 Telnet 会话并开启 AAA 本地认证。

```
Device(config)#line vty 0 15
Device(config-line)#login authentication default
Device(config-line)#exit
```

- 步骤 4： 检验结果。

客户端通过 telnet 登陆 Device 时，按提示输入用户名 admin 和密码 admin，能成功进入到 Device 的 Shell 用户界面。

55.3.2 配置 Telnet 用户登录使用 RADIUS 认证、授权与统计

-B -S -E -A

网络需求

- Device 连接 Telnet 客户端和 RADIUS 服务器端，且 IP 路由可达。
- RADIUS 服务器的 IP 地址为 2.0.0.2/24，认证、授权端口为 1812，统计端口为 1813，共享密钥为 admin。
- Telnet 用户登录 Device 时，要求通过 RADIUS 服务器进行认证、授权和统计。
- RADIUS 服务器故障时使用本地认证和授权。

网络拓扑

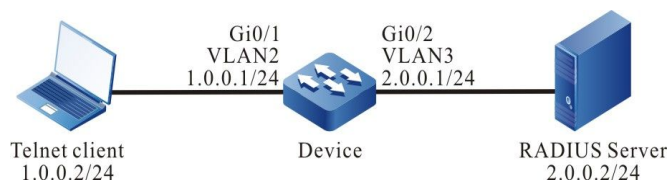


图 55-2 配置 Telnet 用户登录使用 RADIUS 认证、授权与统计组网图

配置步骤

步骤 1： 配置 VLAN，并将端口加入对应的 VLAN。（略）

步骤 2： 配置各接口的 IP 地址。（略）

步骤 3： 配置 Device。

#配置 AAA，使用 RADIUS 认证/授权和统计。

说明：

- 认证和授权首先使用方法列表中第一种方法，在服务器故障时才使用第二种方法进行认证和授权。
-

```
Device#configure terminal
Device(config)#aaa new-model
Device(config)#aaa authentication login authen-list radius local
Device(config)#aaa authorization exec author-list radius local
Device(config)#aaa accounting exec account-list start-stop radius
```

#配置 RADIUS 服务器，认证端口为 1812，统计端口为 1813，共享密钥为 admin。

```
Device(config)#radius-server host 2.0.0.2 auth-port 1812 acct-port 1813 key admin
```

#配置 Telnet 会话，并开启 RADIUS 认证、授权和统计。

```
Device(config)#line vty 0 15
Device(config-line)#login authentication authen-list
Device(config-line)#authorization exec author-list
Device(config-line)#accounting exec account-list
Device(config-line)#exit
```

步骤 4： 配置 RADIUS 服务器。

RADIUS 服务器的界面设置请参考服务器帮助文档，下面列出大致步骤。

#在 RADIUS 服务器上增加用户 admin，设置密码为 admin，并为该用户配置用户级别为 15。

#设置服务器的 IP 地址为 2.0.0.2，共享密钥为 admin，认证端口为 1812，统计端口为 1813。

#设置客户端的 IP 地址为 2.0.0.1，共享密钥为 admin。

步骤 5： 检验结果，验证认证/授权和统计。

#Telnet 用户登录 Device 后授权成功，show privilege 查看用户优先级为 15。

#能在 RADIUS 服务器上查看到登录和断开的统计信息。

55.3.3 配置 Telnet 用户级别切换使用 RADIUS 认证 **-B -S -E -A**

网络需求

- Device 连接 Telnet 客户端和 RADIUS 服务器端，且 IP 路由可达。

- RADIUS 服务器的 IP 地址为 2.0.0.2/24，认证/授权端口为 1812，共享密钥为 admin。
- Telnet 用户登录 Device 后用户级别从 1 切换为 3 时，要求通过 RADIUS 服务器进行认证。

网络拓扑

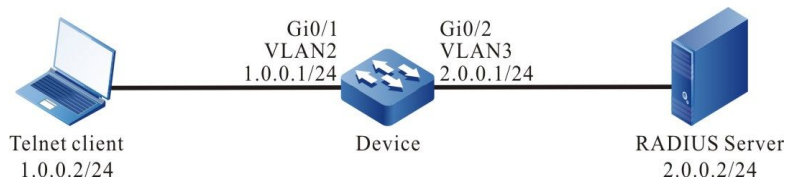


图 55-3 配置 Telnet 用户级别切换使用 RADIUS 认证组网图

配置步骤

步骤 1： 配置 VLAN，并将端口加入对应的 VLAN。（略）

步骤 2： 配置各接口的 IP 地址。（略）

步骤 3： 配置 Device。

#配置用户级别切换使用 RADIUS 认证。

```
Device#configure terminal
Device(config)#aaa new-model
Device(config)#aaa authentication enable default radius
```

#配置 RADIUS 服务器，认证端口为 1812，共享密钥为 admin。

```
Device(config)#radius-server host 2.0.0.2 auth-port 1812 acct-port 1813 key admin
```

步骤 4： 配置 RADIUS 服务器。

RADIUS 服务器的界面设置请参考服务器帮助文档，下面列出大致步骤。

#增加用户级别为 3 的用户名 \$enab3\$，设置密码为 admin。

说明：

- 用户级别切换固定使用\$enabLEVEL\$格式的用户名认证，其中大写的 LEVEL 为用户希望切换到的级别。
- 用户级别降低时无需认证。

步骤 5： 检验结果。

Telnet 用户按照提示输入用户名和密码登录后用户级别默认为 1，执行 enable 3 命令后输入密码 admin，经 RADIUS 服务器认证成功后用户级别切换为 3。

55.3.4 配置 SHELL 命令的 TACACS 授权与统计

-B -S -E -A

网络需求

- Device 与 TACACS 服务器互联，且 IP 路由可达。
- TACACS 服务器 IP 地址为 2.0.0.2/24，服务端口为 49，共享密钥为 admin。
- Telnet 客户端登录 Device 后，操作的用户级别为 15 的 SHELL 命令要求通过 TACACS 服务器授权，并将这些 SHELL 命令记录到 TACACS 服务器上。

网络拓扑

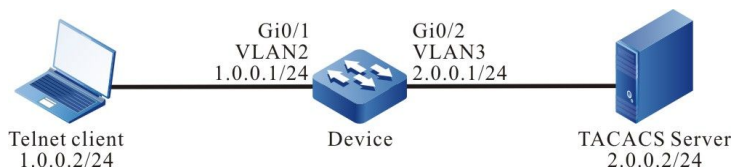


图 55-4 配置 SHELL 命令的 TACACS 授权与统计组网图

配置步骤

步骤 1： 配置 VLAN，并将端口加入对应的 VLAN。（略）

步骤 2： 配置各接口的 IP 地址。（略）

步骤 3: 配置 Device。

#配置 TACACS 命令授权和统计。

说明:

- 授权和统计前必须认证成功。
-

```
Device#configure terminal
Device(config)#aaa new-model
Device(config)#aaa authentication login shell tacacs
Device(config)#aaa authorization commands 15 cmd-author tacacs
Device(config)#aaa authorization config-commands
Device(config)#aaa accounting commands 15 cmd-accounting start-stop tacacs
```

#配置 TACACS 服务器，服务端口为 49，共享密钥为 admin。

```
Device(config)#tacacs-server host 2.0.0.2 port 49 key admin
```

#配置 Telnet 会话并开启 TACACS 授权与统计。

```
Device(config)#line vty 0 15
Device(config-line)#login authentication shell
Device(config-line)#authorization commands 15 cmd-author
Device(config-line)#accounting commands 15 cmd-accounting
Device(config-line)#exit
```

步骤 4: 配置 TACACS 服务器。

TACACS 服务器的界面设置请参考服务器帮助文档，下面列出大致步骤。

#在服务器上增加客户端 2.0.0.1，共享密钥为 admin，选择 “TACACS+(Cisco IOS)” 认证。

#为 Telnet 用户 admin 设置 SHELL 命令授权。允许 configure terminal、router ospf、router rip 命令，拒绝其它命令。

步骤 5: 检验结果。

#Telnet 用户登录到 Device 后，执行相应 SHELL 命令，授权成功的命令能成功执行，授权失败的命令执行失败。

```
Device#configure terminal
% Enter configuration commands, one per line. End with CNTL+Z.
Device(config)#router ospf 100
```

```
Device(config-ospf)#exit
Device(config)#router rip
Device(config-rip)#exit
Device(config)#interface gigabitethernet 0/1
Command authorization failed
Device(config)#router bgp 100
Command authorization failed
```

#查看命 SHELL 命令统计信息。

在 TACACS 服务器上能够查看到 SHELL 命令的统计信息。

56 802.1X

56.1 802.1X 简介

56.1.1 802.1X *-B -S -E -A*

802.1X 是 IEEE 在 2001 年 6 月提出的宽带接入认证方案，它定义了基于物理端口的网络接入控制协议（Port-Based Network Access Control）。802.1X 利用 IEEE 802 架构局域网的物理访问特性，提供了一套对以点对点方式（point-to-point）连接到局域网端口上的设备进行认证、计费、授权的方法。

802.1X 系统为典型的客户端/服务器结构，如下图所示，包括三个实体分别为：Supplicant system（客户端）、Authentication system（认证设备）以及 Authentication server system（认证服务器）。

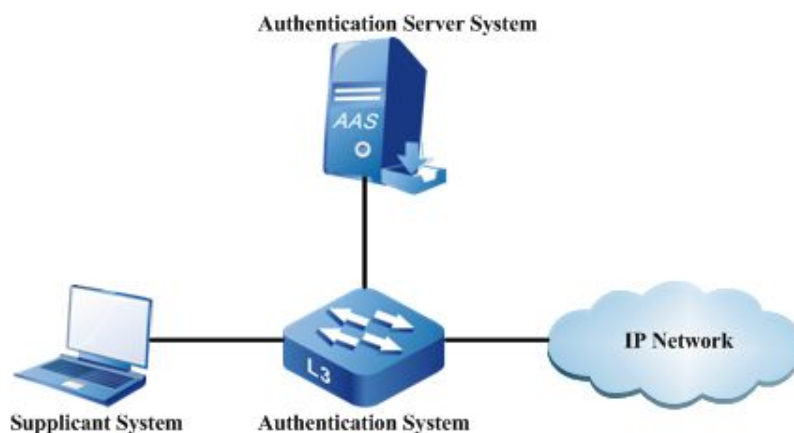


图 8-1 802.1X 体系结构

- 客户端安装支持 802.1X 认证的客户端软件，向认证设备发送认证请求，认证成功则正常接入网络。
- 认证设备位于客户端和认证服务器之间，通过与服务器交互来控制客户端的网络接入。
- 认证服务器通常为 RADIUS (Remote Authentication Dial-In User Service, 远程认证拨号用户服务) 服务器，用来验证客户端的合法性，并将认证结果通知给认证设备，由认证设备根据认证结果控制客户端的网络接入。

802.1X 认证使用的 EAP (Extensible Authentication Protocol, 可扩展认证协议) 是 PPP 认证的一个通用协议，用于实现客户端、认证设备、认证服务器之间认证信息的交互。802.1X 协议使用 EAPOL (EAP Over LAN) 帧封装格式对 EAP 报文进行封装，实现客户端与认证设备的交互。根据应用场景不同，802.1X 协议会将 EAP 报文封装在不同的帧格式中，来实现认证设备与认证服务器的交互，在中继认证方式中 EAP 报文会被封装在 EAPOR (EAP Over RADIUS) 帧格式中；在终结认证方式中 EAP 报文会被封装在标准的 RADIUS 帧格式。

802.1X 认证方式分为中继认证方式和终结认证方式。

中继认证方式流程如下图所示：

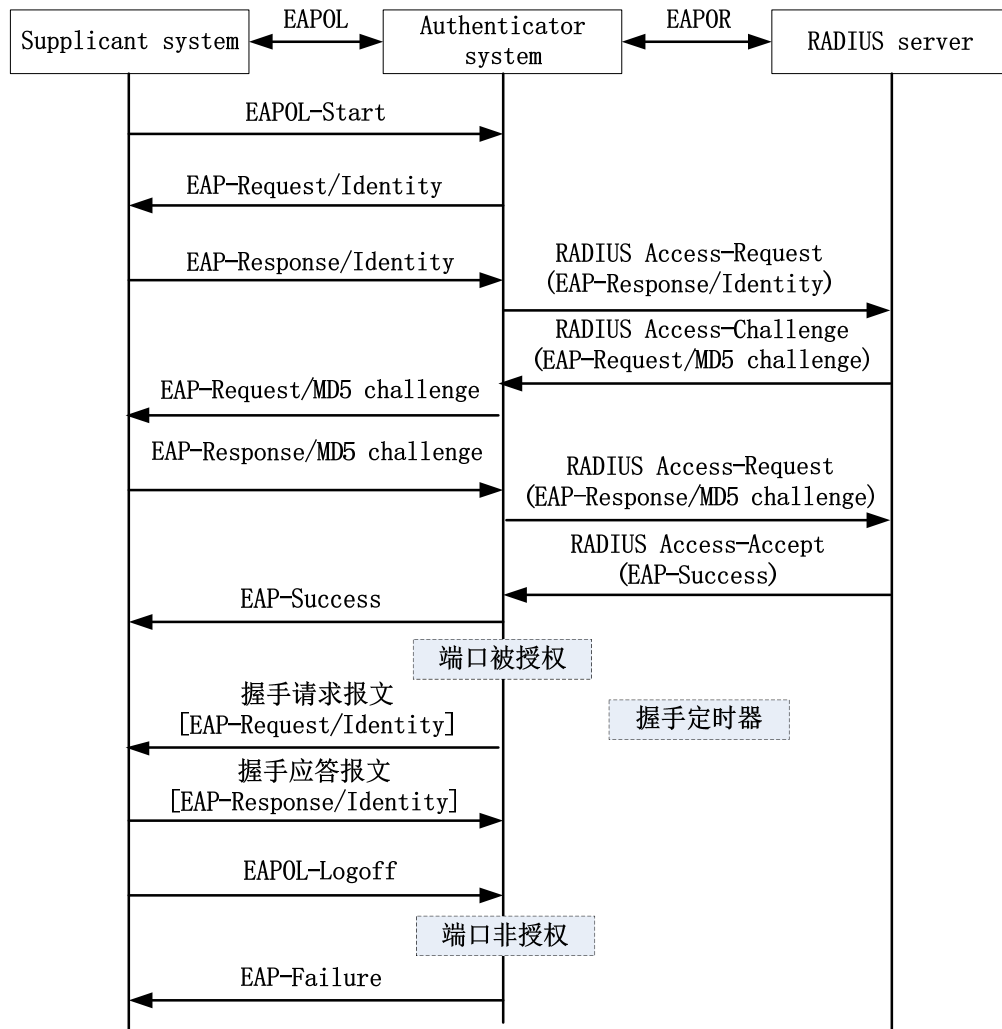


图 8-2 802.1X 中继认证流程

中继认证流程如下：

- 当用户有访问网络需求时打开 802.1X 客户端程序，输入已在认证服务器上注册的合法用户名和密码，发起认证请求（EAPOL-Start 报文）。此时，客户端程序将发出请求认证的报文给认证设备，开始启动一次认证过程；
- 认证设备收到请求认证的数据帧后，将发出一个请求帧（EAP-Request/Identity 报文）要求用户的客户端程序发送输入的用户名；
- 客户端程序响应认证设备发出的请求，将用户名信息通过数据帧（EAP-Response/Identity 报文）发送给认证设备。认证设备将客户端发送的数据帧封装到报文中（RADIUS Access-Request 报文）送给认证服务器进行处理；
- RADIUS 服务器收到认证设备转发的用户名信息后，将该信息与数据库中的用户名

表对比，找到该用户名对应的密码信息，用随机生成的一个加密字对它进行加密处理，同时也将此加密字通过 RADIUS Access-Challenge 报文发送给认证设备，由认证设备转发给客户端程序；

- 客户端程序收到由认证设备传来的加密字（EAP-Request/MD5 Challenge 报文）后，用该加密字对密码部分进行加密处理（此种加密算法通常是不可逆的，生成 EAP-Response/MD5 Challenge 报文），并通过认证设备传给认证服务器；
- RADIUS 认证服务器将收到的已加密的密码信息（RADIUS Access-Request 报文）和本地经过加密运算后的密码信息进行对比，如果相同，则认为该用户为合法用户，反馈认证通过的消息（RADIUS Access-Accept 报文和 EAP-Success 报文）；
- 认证设备收到认证通过消息后将端口改为授权状态，允许用户通过端口访问网络；
- 客户端也可以发送 EAPOL-Logoff 报文给认证设备，主动要求下线，认证设备把端口状态从授权状态改变成未授权状态，并向客户端发送 EAP-Failure 报文。

此认证方需要认证设备和认证服务器都支持 EAP 协议。

终结认证方式流程如下图所示：

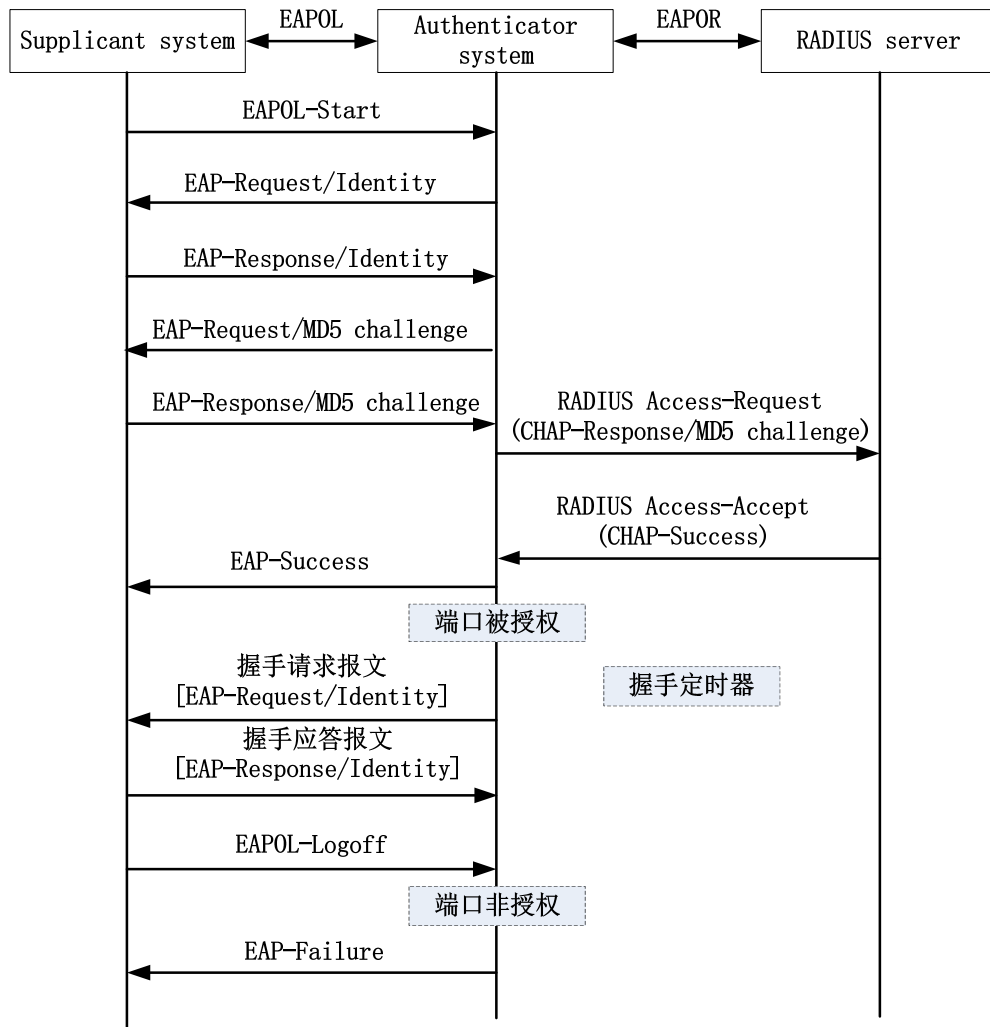


图 8-3 802.1X 终结认证流程

- 终结认证方式与中继认证方式的认证流程相比，不同之处在于，对用户口令信息进行加密处理的随机加密字由认证设备生成，之后认证设备会把用户名、随机加密字和客户端加密后的口令信息一起送给 RADIUS 服务器，进行相关的认证处理。

终结认证方式用于较早部署的不支持 EAP 协议的认证服务器。

认证设备支持两种接入控制方式：

- 基于端口接入控制方式 (Portbased)，端口下的第一个用户认证成功后，其它接入用户无须认证就可以接入网络，但是当第一个用户下线后，其它用户也会被拒绝接入网络；
- 基于用户接入控制方式 (Macbased)，端口下的所有接入用户均需要单独认证，某个用户下线后，也只有此用户无法接入网络，不影响其他用户接入网络。

Auto VLAN 有时又叫 Assigned VLAN，客户端通过服务器认证时，服务器会把授权的 VLAN 信息下发到认证设备，如果下发的 VLAN 在认证设备存在且合法，认证端口加入到下发的 VLAN 中。客户端下线之后，端口恢复为未认证状态，端口从这个 Auto VLAN 中删除，端口缺省 VLAN 恢复为以前配置的 VLAN。

当启用了 Guest VLAN 功能后，用户无需认证也可以且仅可以访问该 VLAN 内的资源；当用户认证成功后，端口离开 Guest VLAN，用户可以访问其他的网络资源。通常用户在 Guest VLAN 中可以获取 802.1X 客户端软件以升级客户端，或执行其他一些应用程序（例如防病毒软件、操作系统补丁等）升级等，使能 802.1X 认证并正确配置 Guest VLAN 后，端口将以 Untagged 方式加入到 Guest VLAN 内。此时 Guest VLAN 中端口下的用户发起认证，如果认证失败，端口仍然处在 Guest VLAN 内；如果认证成功，分为以下两种情况：

- 如果认证服务器下发一个 VLAN，这时端口离开 Guest VLAN，加入下发的 VLAN 中。用户下线后，端口会回到 Guest VLAN 中；
- 如果认证服务器不下发 VLAN，这时端口离开 Guest VLAN，加入认证设备中已配置好的 Config VLAN 中，用户下线后，端口会回到 Guest VLAN 中。

56.1.2 安全通道认证 **-B -S -E -A**

安全通道认证功能基于 802.1X 认证功能，不但可以实现 802.1X 认证，还可以为特定的终端用户开辟一条安全通道，使终端用户在未认证的情况下能访问指定网络中的资源，或者指定特定的终端用户免认证访问网络资源。

56.1.3 MAC 地址认证 **-B -S -E -A**

实际网络中，除了大量的终端用户外，可能还有一部分网络终端（如网络打印机等），这部分终端没有自带或无法安装 802.1X 认证客户端软件，可以使用免客户端认证方式接入网络。这种认证方法不需要用户安装任何 802.1X 认证客户端软件，认证设备在首次检测到用户的 MAC 地址后，认证设备使用已经配置好的用户名和密码或者用户的 MAC 地址作为用户名和密码发送给认证服务器进行认证。

MAC 地址认证使用的用户名密码格式通常有以下两种：

MAC 地址作为用户名和密码格式：使用认证用户的 MAC 地址作为用户名和密码；

固定用户名和密码格式：使用认证设备上已配置的用户名和密码。

56.2 802.1X 功能配置

表 8-1 802.1X 功能配置列表

配置任务	
配置 802.1X 认证	使能 802.1X 认证
配置安全通道认证	使能安全通道认证功能
	配置及应用安全通道
配置 802.1X 认证及安全通道认证属性	配置端口认证方式
	配置组播触发功能
	配置重认证功能
	配置端口最大认证失败次数
	配置省去用户名中 IP 字段功能
	配置报文透传功能
	配置保活功能
	配置不等待服务器回应功能
配置 MAC 地址认证	使能 MAC 地址认证功能
	配置 MAC 地址认证用户名格式
配置公共属性	配置受控方向

配置任务	
	配置可认证主机列表
	配置 IP 授权功能
	配置认证请求报文最大发送次数
	配置认证报文最大发送次数
	配置认证失败记录日志功能
	配置 ARP 保活功能
	配置端口最大用户数
	配置 IP ACL 前缀名称
	配置默认生效 VLAN
	配置允许未认证用户在 PVID 所属 VLAN 内通信功能
	配置端口接入控制方式
	配置 Guest VLAN
	配置 Guest ACL
	配置 Critical VLAN
	配置用户认证迁移功能
	配置定时器参数
	恢复端口缺省配置

配置任务	
	配置日志记录步长

56.2.1 配置 802.1X 认证功能 **-B -S -E -A**

在同一个端口下允许同时配置 802.1X 认证与 MAC 地址认证。

- 终端用户先进行 MAC 地址认证时，如认证通过，不处理该终端用户发起的 802.1X 认证。否则，正常处理该终端用户发起的 802.1X 认证。
- 终端用户先进行 802.1X 认证，则不再进行 MAC 地址认证。

配置条件

无

使能 802.1X 认证

使能 802.1X 认证功能，终端用户需要安装带有 802.1X 认证功能的客户端软件。

表 8-2 使能 802.1X

步骤	命令	说明
进入全局配置模式	configure terminal	-
使能全局 802.1X 认证	dot1x { enable disable }	可选 缺省情况下，全局 802.1X 认证功能处于使能状态
进入二层以太网接口配置模式	interface interface-name	必选其一

步骤	命令	说明
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
使能 802.1X 认证	dot1x port-control { enable disable }	必选 缺省情况下，端口下 802.1X 认证功能处于禁用状态

说明：

- 不能在同一端口同时使能 802.1X 认证功能和安全通道认证功能。
- 同一端口下支持同时使能 802.1X 认证功能和端口安全功能，但存在如下限制，不允许配置端口安全 IP 规则及 MAX 规则。
- 802.1X 认证功能与端口安全功能共用时，如果端口安全配置了相关的 MAC 规则，则 802.1X 不处理该终端的发送报文及认证请求，由端口安全处理。

配置 ARP/IP 报文触发生成 802.1X 用户功能

端口下使能 802.1X 认证功能后，在终端用户未发起认证时希望在认证设备上查看终端用户的信息，则需要配置 ARP/IP 报文触发生成 802.1X 用户功能。

同一端口下同时使能 802.1X 认证功能和 ARP/IP 报文触发生成 802.1X 用户功能，当认证设备收到端口下的终端用户的 ARP 或者 IP 报文就可以生成 802.1X 用户。

表 8-3 使能 ARP/IP 报文触发生成 802.1X 用户功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface <i>interface-name</i>	必选其一 进入二层以太接口配置模式后, 后续配置只在当前端口生效; 进入汇聚组配置模式后, 后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	
配置 ARP/IP 报文触发生成 802.1X 用户功能	dot1x arp-ip-auth { enable disable }	必选 缺省情况下, 端口下 ARP/IP 报文触发生成 802.1X 用户功能处于禁用状态
配置 ARP/IP 报文触发生成的 802.1X 用户超时时间	dot1x arp-ip-auth timeout <i>timeout-value</i>	可选 缺省情况下, 端口下 ARP/IP 报文触发生成的 802.1X 用户超时时间为 5 分钟

56.2.2 配置安全通道认证

-B -S -E -A

配置条件

无

使能安全通道认证

安全通道认证功能基于 802.1X 认证功能，不但可以实现 802.1X 认证，还可以为特定的终端用户开辟一条安全通道，使终端用户在未认证的情况下能访问指定网络中的资源，或者指定特定的终端用户免认证访问网络资源。

表 8-4 使能安全通道认证

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface <i>interface-name</i>	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	
使能安全通道认证	dot1x free-ip	必选 缺省情况下，端口下的安全通道认证功能处于禁用状态

说明：

不能在同一端口同时使能安全通道认证功能和端口安全功能。

不能在同一端口同时使能 802.1X 认证功能和安全通道认证功能。

不能在同一端口同时使能 MAC 地址认证功能和安全通道认证功能。

端口下使能安全通道认证功能，但设备上未应用安全通道或未配置安全通道规则时，安全通道认证功能与 802.1X 认证功能相同。

安全通道认证时，用户认证通过后，会占用芯片资源，如果芯片资源不足，会导致用户认证不通过。

配置及应用安全通道

端口下使能安全通道认证功能后，希望允许终端用户在未认证的情况下能访问指定网络中的资源，或者指定特定的终端用户免认证访问网络资源，则需要配置及应用安全通道。

配置安全通道规则可分为以下类型。

- 配置终端用户允许访问指定网络资源。
 - 配置指定终端用户允许访问网络资源。

表 8-5 应用安全通道

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置安全通道	hybrid access-list advanced { <i>access-list-number</i> <i>access-list-name</i> }	必选 缺省情况下，设备中未配置安全通道
配置安全通道规则	[<i>sequence</i>] permit protocol { any <i>source-ip-addr source-wildcard</i> / host <i>source-ip-addr</i> } { any <i>source-mac-addr source-wildcard</i> / host <i>source-mac-addr</i> } { any / <i>destination-ip-addr destination-wildcard</i> / host <i>destination-ip-</i>	必选 缺省情况下，安全通道下没有安全通道规则

步骤	命令	说明
	<i>addr</i> { any / <i>destination-mac-addr</i> <i>destination-wildcard</i> / host <i>destination-mac-addr</i> }	
应用安全通道	global security access-group { <i>access-group-number</i> <i>access-group-name</i> }	必选 缺省情况下，系统中未应用任何安全通道

说明：

设备可以配置多个安全通道，一个安全通道可以配置多条安全通道规则。

安全通道类型只允许为混合高级 ACL，设备中只允许应用一个安全通道。

56.2.3 配置 802.1X 认证及安全通道认证属性 **-B -S -E -A**

如果端口下没有使能 802.1X 认证功能或安全通道认证功能，则配置的相关属性不生效。

配置条件

无

配置端口认证方式

802.1X 认证方式可以分为两类：中继认证方式和终结认证方式。

802.1X 认证系统由三部分组成：客户端、认证设备和认证服务器。标准 802.1X 协议规定客户端和认证服务器之间通过 EAP 报文进行交互，认证设备在交互中充当着“中继”的角色，认证设备将客户端

发送来的 EAP 数据封装在其他协议中，例如 RADIUS 协议，发送给认证服务器，同样地，认证设备也将认证服务器发送过来的 EAP 数据封装在 EAPOL 报文中转发给客户端，这种交互方式称之为中继认证方式，中继认证方式要求认证服务器支持 EAP 协议，配置 EAP 中继认证方式具体支持的认证机制取决于客户端和认证服务器。

部署较早的认证服务器可能不支持 EAP 协议，需要配置成终结认证方式，客户端的 EAP 报文不会被直接发送到认证服务器，而是由认证设备完成与客户端的 EAP 报文交互，认证设备获取足够的用户认证信息后，将认证信息发送到认证服务器进行认证。

EAP 终结认证方式支持 PAP（Password Authentication Protocol 即密码验证协议）认证和 CHAP（Challenge Handshake Authentication Protocol,质询握手验证协议）认证。

表 8-6 配置端口认证方式

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太网接口配置模式	interface <i>interface-name</i>	必选其一
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	进入二层以太网接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
配置端口认证模式	dot1x eap-relay { enable disable }	必选 缺省情况下，端口下认证方式为终结认证方式

说明：

配置终结认证方式，目前仅支持基于 MD5（Message Digest Algorithm，消息摘要算法第五版）的 EAP 认证。802.1x 认证功能和安全通道认证功能支持中继及终结认证方式。

客户端采用证书认证时，认证端口需要配置为中继认证方式。

MAC 地址认证只支持终结认证方式。

配置组播触发功能

某些终端安装了 802.1X 认证客户端，但客户端不会主动发起认证，认证过程只能依靠认证设备来触发。认证设备会向配置了组播触发的端口周期性发送请求用户名的组播报文，客户端收到此类报文后响应认证设备的认证请求，开始认证处理流程。

表 8-7 配置组播触发功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface <i>interface-name</i>	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	
使能组播触发	dot1x multicast-trigger	必选 缺省情况下，端口下组播触发功能处于禁用状态
配置组播触发周期	dot1x multicast-period <i>multicast-period-value</i>	可选

步骤	命令	说明
		缺省情况下，端口下组播触发时间为 15 秒

说明：

如果客户端不支持组播触发功能，客户端的网卡显示可能会不正常，同时会造成重认证失败。

配置重认证功能

为了检测客户端是否在线，避免客户端异常死机等原因影响对用户计费的准确性，以及防止客户端被他人冒用，认证设备会向客户端周期性发起重认证请求，此过程中用户无需再次输入用户名和密码。

表 8-8 配置重认证功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太网接口配置模式	interface <i>interface-name</i>	必选其一 进入二层以太网接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	
配置重认证功能	dot1x reauthentication	必选 缺省情况下，端口下使能重认证功能

配置最大认证失败次数

客户端认证失败次数达到上限值后，客户端进入静默状态，在静默时间内认证设备不再响应此客户端发起的认证请求。

表 8-9 配置最大认证失败次数

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface interface-name	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation link-aggregation-id	
配置端口认证失败次数上限	dot1x max-authfail max-authfail-value	必选 缺省情况下，端口下最大认证失败次数为 1

配置报文透传功能

实际应用环境中，待认证终端与认证设备之间可能跨越中间设备，如果这些中间设备不能透传 EAPOL 报文，认证过程将不能正常进行。为使认证正常进行，需要在中间设备接收 EAPOL 报文的端口使能 EAPOL 报文透传功能，并为这个端口配置一个上联端口。如果使能 EAPOL 报文透传功能的端口接收到 EAPOL 报文，会将报文从配置的上联端口发送出去，如果与上联端口直连的设备为认证设备，则认证设备接收到 EAPOL 报文后做相应处理。

表 8-10 配置报文透传功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface <i>interface-name</i>	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	
配置报文透传功能	dot1x eapol-relay { enable disble }	必选 缺省情况下，端口下报文透传功能处于禁用状态
配置报文透传上联端口	dot1x eapol-relay uplink { interface <i>interface-name</i> link-aggregation <i>link-aggregation-id</i> }	必选 缺省情况下，端口下没有配置上联端口

配置保活功能

为了检测客户端是否在线，认证设备会向客户端周期性地发送 EAP-Request/Identity 报文，如果接收到客户端回应的 EAP-Response/Identity 报文后，会向客户端发送 EAP-Request/MD5 Challenge 报文，如果认证系统接收到 EAP-Response/MD5 Challenge 报文则确认客户端正常在线，并发送 EAP-Success 报文通知客户端保活成功。

表 8-11 配置保活功能

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
进入二层以太接口配置模式	interface <i>interface-name</i>	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	
配置保活功能	dot1x keepalive { enable disable }	必选 缺省情况下，端口下保活功能处于禁用状态
配置保活时间	dot1x keepalive period <i>period-value</i>	可选 缺省情况下，端口下保活周期为 60 秒
配置保活报文重传次数	dot1x keepalive retries <i>retries-value</i>	可选 缺省情况下，端口下最大保活次数为 3
配置保活类型	dot1x keepalive type { request-identity request-md5 }	可选 缺省情况下，端口下保活类型为标准保活。

说明：

保活功能需要 802.1X 认证客户端软件（如我司的 TC 客户端）支持，如果客户端不支持，会造成保活失败导致用户下线。

配置不等待服务器回应功能

在中继认证方式下，客户端可能发出一些服务器不会回应的报文，这些报文会使认证设备与认证服务器的会话通道被占用，导致后续客户端认证失败，可在端口下使能不等待服务器回应功能来避免出现此类问题。

表 8-12 配置不等待服务器回应功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface <i>interface-name</i>	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	
配置不等待服务器回应功能	dot1x nowait-result	必选 缺省情况下，端口不等待服务器回应处于禁用状态

56.2.4 配置 MAC 地址认证

-B -S -E -A

在同一个端口下允许同时配置 802.1X 认证与 MAC 地址认证。

- 终端用户先进行 MAC 地址认证时，如认证通过，不处理该终端用户发起的 802.1X 认证。否则，正常处理该终端用户发起的 802.1X 认证。
- 终端用户先进行 802.1X 认证，则不再进行 MAC 地址认证。

配置条件

无

使能 MAC 地址认证功能

MAC 地址认证也称为免客户端认证，这种认证方式既适用于无法安装客户端软件的终端进行认证，又适用于没有安装客户端软件、不用输入用户名密码就能进行认证的终端用户。

在认证设备端口下配置 MAC 地址认证相关参数时，如果端口没有使能 MAC 地址认证功能，则配置的相关功能不生效。

表 8-13 使能 MAC 地址认证功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface <i>interface-name</i>	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	
使能 MAC 地址认证功能	dot1x mac-authentication { enable disable }	必选 缺省情况下，端口下的 MAC 地址认证功能处于禁用状态

说明：

同一端口下支持同时使能 MAC 地址认证功能和端口安全功能，但存在如下限制，不允许配置端口安全 IP 规则及 MAX 规则。

不能在同一端口同时使能 MAC 地址认证功能和安全通道认证功能。

配置 MAC 地址认证用户名格式

MAC 地址认证使用的用户名密码格式分为两种：固定的用户名密码格式、MAC 地址用户名密码格式。

固定的用户名密码格式：认证设备接收到终端用户的数据报文时，会将配置好的用户名和密码发送给认证服务器进行认证。

MAC 地址用户名密码格式：认证设备会将终端用户的 MAC 地址作为用户名和密码。作为用户名和密码的 MAC 地址格式可分为两种，一种为带连字号的，如 00-01-7a-00-00-01。另一种为不带连字号的如 00017a000001。

表 8-14 配置 MAC 地址认证用户名格式

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface <i>interface-name</i>	必选其一
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
配置 MAC 地址认证用户名格式	dot1x mac-authentication username-format { fixed account <i>account-value</i> password <i>password-value</i> mac-address [with-hyphen without-hyphen] }	必选 缺省情况下，MAC 地址认证使用带连字号的 MAC 地址作为用户名和密码

配置域名分隔符

认证设备可以基于域管理用户，若认证用户名中携带域名，则设备使用对应的 AAA 服务器组中的服务器对用户进行认证、授权和计费，若认证用户名中未携带域名，则使用系统中的缺省配置的认证服务器进行认证；所以认证设备需要能够准确解析用户名中的用户名和域名，对于为用户提供认证服务起到决定性作用。由于不同的客户端所支持的用户名域名分隔符不同，为了更好地管理和控制不同用户名格式的用户接入，需要在认证设备上指定可支持的域名分隔符。

目前，支持的域名分隔符包括@、\和/，

域名分隔符为 '@' 时，认证用户名格式为 `username@domain`

域名分隔符为 '/' 时，认证用户名格式为 `username/domain`

域名分隔符为 '\' 时，认证用户名格式为 `domain\username`

其中 `username` 为纯用户名、`domain` 为域名，如果用户名中包含有多个域名分隔符字符，则认证设备仅将第一个出现的域名分隔符识别为实际使用的域名分隔符，其它字符都被认为是域名中的一部分。

表 8-15 配置域名分隔符

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太网接口配置模式	interface <i>interface-name</i>	必选其一
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	进入二层以太网接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
配置域名分隔符	dot1x domain-delimiter <i>domain-delimiter-type</i>	必选

步骤	命令	说明
		缺省情况下，端口下域名分隔符为 '@'

说明：

使用携带域名的用户名进行认证时，认证设备上需要配置相应的认证服务器组。

配置认证用户名格式

认证用户以 'username@domain' 的格式命名，域名分隔符 '@' 后面的为域名，认证设备通过解析域名决定使用哪个认证服务器组对该用户进行认证。由于有些较早期的服务器不能接受携带有域名的用户名，因此认证设备需要将用户名中携带的域名去除，仅将认证用户名发送给服务器。通过配置认证用户名格式，可以选择向认证设备发送的认证用户名中是否携带域名。

目前，支持的域名分隔符包括@、\和/。

表 8-16 配置认证用户名格式

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface <i>interface-name</i>	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	

步骤	命令	说明
配置认证用户名格式	dot1x user-name-format { with-domain without-domain }	必选 缺省情况下，向认证服务器发送携带域名的认证用户名

说明：

配置向认证服务器发送不携带域名的认证用户名功能的端口，不支持进行证书认证。

配置认证报文交互模式

在实际的应用场景中，大部分客户端发起认证后，认证设备与客户端之间支持单播/组播认证交互模式。但仍然存在小部分认证客户端只识别组播认证报文，即目的 MAC 地址为 0180.C200.0003 的认证报文，此时端口下可以配置组播认证交互模式。

大部分认证客户端，认证设备第一次接收到服务器回应的 EAP 报文后，后续与客户端及认证服务器交互时，均以服务器报文中携带的 identifier 标识为准。极少部分认证客户端认证时需要以认证设备生成的 identifier 标识为准，遇到此类情况，需要在端口下配置关心 EAP 认证报文中 identifier 标识功能。

表 8-17 配置认证报文交互模式

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface <i>interface-name</i>	必选其一

步骤	命令	说明
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	进入二层以太网接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
配置认证交互模式	dot1x auth-mac { multicast unicast }	必选 缺省情况下，端口下采用单播认证报文交互模式
关心 EAP 认证报文中 identifier 标识功能	dot1x identifier { match ignore }	可选 缺省情况下，不关心 EAP 认证报文中 identifier 标识

说明：

只有极少的客户端需要关心认证交互报文的 identifier 标识功能，除非有明确需求，否则应尽量避免配置该功能。

56.2.5 配置公共属性

-B -S -E -A

配置公共属性参数时，如果端口下没有使能 802.1X 认证功能、安全通道认证通过或 MAC 地址认证功能，则配置的相关功能不生效。

配置条件

端口下配置 IP 授权功能时，同时需要配置 ARP 保活功能。

配置受控方向

端口受控方向分为：双向受控和单向受控。

- 双向受控指，端口禁止接收和转发报文。
- 单向受控指，禁止接收客户端报文，但允许向客户端转发报文。

此功能用于与 WOL (Wake On Lan, 局域网唤醒) 功能配合使用。某些终端处于休眠状态，但其网卡仍然能处理一些特殊报文，例如 WOL 报文。当网卡接收到 WOL 报文后，会启动终端设备，进入工作状态。

当休眠终端接入端口开启认证功能时，此时可以配置端口为单向受控，保证能正常向终端转发 WOL 报文。终端启动后能发起认证活动，认证通过后能正常访问网络资源。

跨网段发送 WOL 报文时，需要在认证设备上配置 ARP 转发表项。

表 8-18 配置受控方向

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface interface-name	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
配置受控方向	dot1x control-direction { both in }	必选 缺省情况下，端口下双向受控。

配置可认证主机列表

使能可认证主机列表功能后，只允许 MAC 地址处于可认证主机列表中的用户进行认证活动，其他用户发起的认证会被拒绝。

表 8-19 配置可认证主机列表

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface <i>interface-name</i>	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	
配置可认证主机列表	dot1x auth-address { enable disable <i>mac-address</i> }	必选 缺省情况下，端口下可认证主机列表处于禁用状态

配置 IP 授权功能

端口下开启 IP 授权功能，如果检测到认证用户的 IP 地址发生了变化，则会强制用户下线，可分为以下几种模式：

disable：禁用模式，此模式下不检测用户的 IP 地址。

dhcp-server：DHCP Server 模式，配置此模式时，需要在设备上配置 DHCP Snooping 功能，认证用户从 DHCP 服务器上获取 IP 地址后，设备上记录认证用户与 IP 地址绑定关系，如果检测到用户 IP 地址发生变化，会强制用户下线。

radius-server: RADIUS Server 模式, RADIUS Server 在 RADIUS 报文中封装 Frame-IP-Address 字段中封装认证用户应使用的 IP 地址, 认证设备上记录用户与该 IP 地址绑定关系, 如果检测到用户 IP 地发生变化, 会强制用户下线。

Supplicant: 客户端模式, 用户第一次认证通过后, 设备上记录认证用户与 IP 地址绑定关系, 如果检测到用户 IP 地址发生化, 会强制用户下线。

表 8-20 配置 IP 授权功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface interface-name	必选其一 进入二层以太接口配置模式后, 后续配置只在当前端口生效; 进入汇聚组配置模式后, 后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation link-aggregation-id	
配置 IP 授权功能	dot1x authorization ip-auth-mode { disable dhcp-server radius-server supplicant }	必选 缺省情况下, 端口下 IP 授权功能处于禁用状态

配置认证请求报文最大发送次数

认证设备接收到客户端发送的 EAPOL-Start 报文后, 会向客户端发送认证请求 EAP-Request/Identity 报文, 若认证设备未接收到回应报文则会对该报文进行重传, 此功能用于配置 EAP-Request/Identity 报文的最大发送次数, 如果发送次数超过了配置的最大上限值, 则认证设备会判定此客户端已经失去连接, 结束认证活动。

重传 EAP-Request/Identity 报文过程请参下图:

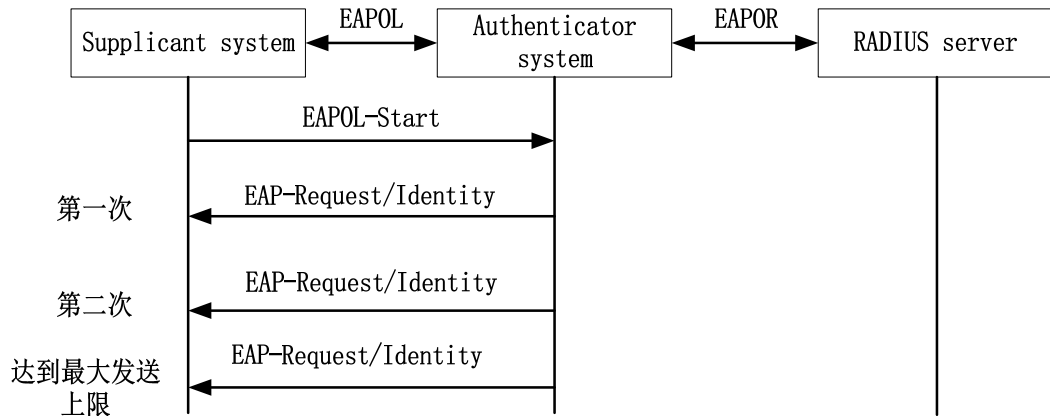


图 8-4 重传 EAP-Request/identity 报文

表 8-21 配置认证请求报文最大发送次数

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太网接口配置模式	interface <i>interface-name</i>	必选其一 进入二层以太网接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	
配置认证请求报文最大发送次数	dot1x max-reauth <i>count</i>	必选 缺省情况下，端口下认证请求报文最大发送次数为 3

配置认证报文最大发送次数

认证过程中，认证设备会向客户端发送除 EAP-Request/Identity 报文以外的其他 EAP-Request 报文，例如 EAP-Request/MD5 challenge 报文，若认证设备未接收到回应报文则会对该报文进行重传，此功能用于配置此类报文的最大发送次数，如果发送次数超过了配置的最大上限值，则认证设备会判定此客户端认证失败。

重传 EAP-Request 报文过程请参看下图：

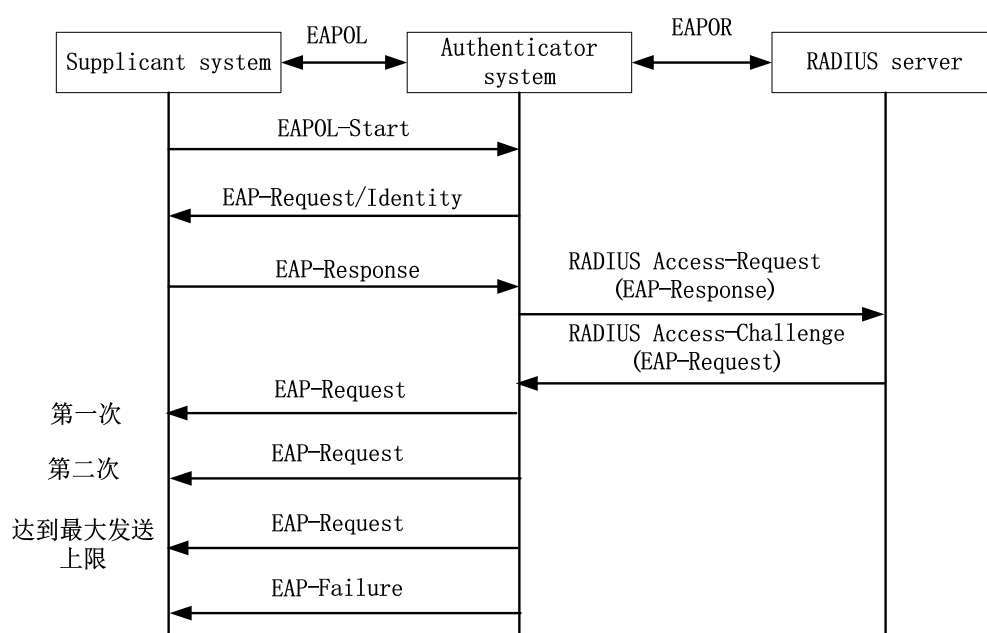


图 8-4 重传 EAP-Request 报文过程

表 8-22 配置认证报文最大发送次数

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太网接口配置模式	interface interface-name	必选其一 进入二层以太网接口配置模式后，后续配置只在当前

步骤	命令	说明
		端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	
配置认证报文最大发送次数	dot1x max-req <i>count</i>	必选 缺省情况下，端口下认证报文最大发送次数为 2

配置认证失败记录日志功能

使能认证失败记录日志功能后，认证设备会记录认证失败的相关信息，便于排查故障原因。

表 11-23 配置认证失败记录日志功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface <i>interface-name</i>	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	

步骤	命令	说明
配置记录认证失败日志功能	dot1x syslog { enable disable }	必选 缺省情况下，端口下认证失败记录日志能处于禁用状态

配置 ARP 保活功能

终端用户认证通过后，为了检测用户是否在线，认证设备向已认证用户发送 ARP 请求报文，认证设备通过能否接收到用户的 ARP 响应报文来确认用户是否在线。

表 8-24 配置 ARP 保活功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface <i>interface-name</i>	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	
配置 ARP 保活功能	dot1x client-probe { enable disable }	必选 缺省情况下，端口下的 ARP 保活功能处于禁用状态

说明：

认证设备需要获取到已认证通过的用户的 IP 地址，才能正常触发 ARP 保活功能，在保护期间未接收到认证设备的 ARP 回应报文，会执行强制用户下线操作。

配置端口最大用户数

如果端口下认证的用户数目达到配置的上限后，认证系统不再响应新用户发起的认证请求。

表 8-25 配置端口最大用户数

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface <i>interface-name</i>	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	
配置端口最大用户数	authentication max-user-num <i>max-uer-num-value</i>	必选 缺省情况下，端口下最大允许接入的用户数目为 256

说明：

端口下需要配置成基于用户接入控制方式（Macbased），否则配置允许接入的用户数目不生效。

配置 IP ACL 前缀名称

终端用户认证通过后，服务器下发 IP ACL 编号大于 2000 时，设备中需要配置名为“IP ACL 前缀名称” + “ACL 编号”的 IP ACL。例如，服务器下发编号为 2001 的 ACL，则设备上应配置名为“assignacl-2001”的 IP ACL。

表 8-26 配置 IP ACL 前缀名称

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 IP ACL 前缀名称	dot1x number-acl-prefix <i>number-acl-prefix-name</i>	必选 缺省情况下，IP ACL 前缀名称为“assignacl-”

说明：

接入控制方式配置为基于端口的多主机模式(portbased host-mode multi-hosts)时，下发 ACL 功能不生效。

配置默认生效 VLAN

当服务器未配置下发 VLAN（Auto VLAN）时，希望认证通过用户在指定的 VLAN 内通信，可通过此配置来指定 VLAN

表 8-27 配置默认生效 VLAN

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置默认生效 VLAN	dot1x default-active-vlan default-active-vlan-id	必选 缺省情况下，端口下未配置默认生效 VLAN

说明：

用户认证通过后与 VLAN 绑定的优先级顺序依次为，服务器下发 VLAN、默认生效 VLAN、端口的 PVID 所属 VLAN。

端口下配置基于用户接入控制方式时（Macbased）时，端口满足 VLAN 模式为 hybrid 模式且启用了 MAC VLAN 条件时配置的默认生效 VLAN 才会生效。

配置允许未认证用户在 PVID 所属 VLAN 内通信功能

端口接入多个终端，每个终端均需进行接入控制，有些不能发起 802.1X 认证终端也希望访问的网络资源，可开启此命令。使能该功能后，未认证终端用户能在 PVID 所属 VLAN 中正常通信。

此功能需满足以下条件，才能正常运行

- 端口使能 802.1X 认证或 MAC 地址认证。
- 端口接入控制方式为基于用户的接入控制方式（Macbased）。
- 端口 VLAN 模式为 Hybrid 模式。
- 端口下需使能只接收 Untag 报文功能。

表 8-28 配置允许未认证用户在 PVID 所属 VLAN 内通信功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置允许未认证用户在 PVID 所属 VLAN 内通信功能	dot1x native-vlan-free	必选 缺省情况下，端口下允许未认证用户在 PVID 所属 VLAN 内通信功能处于禁用状态

说明：

端口使能该功能后，端口下还需使能只接收 Untag 报文功能(端口下配置命令：
switchport accept frame-type untag)，保证未认证通过的用户发送的报文只在 PVID 所属 VLAN 内转发。

该功能建议与服务器下发 VLAN 或配置默认生效 VLAN 一起使用。

该功能不支持安全通道认证。

配置端口接入控制方式

端口的接入控制方式有两类：基于端口的接入控制方式和基于用户的接入控制认证方式。

基于端口的接入控制方式 (Portbased)：端口下只允许一个用户认证通过。

基于用户的接入控制方式 (Macbased)：端口下允许多个用户认证通过，端口下用户需要各自通过认证，才能访问网络。

基于端口接入控制方式又分为两类：多主机模式和单主机模式。

多主机模式 (Multi-hosts)：端口下有一个用户认证通过后，端口下的其他用户无需认证即可访问网络。

单主机模式 (Single-host)：端口下只允许一个用户通过认证并且访问网络，其他用户无法访问网络，也无法再认证通过。

表 8-29 配置端口接入控制方式

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface <i>interface-name</i>	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	
配置接入控制方式	authentication port-method { macbased portbased }	必选 缺省情况下，端口下开启用户认证方式
基于端口接入控制方式	authentication port-method portbased host-mode { multi-hosts single-host }	可选 缺省情况下，端口下开启多主机认证方式

说明：

配置基于端口接入控制方式下的主机模式时，需要保证接入控制方式已经配置成基于端口接入控制方式 (Portbased)。

配置 Guest VLAN

用户在 Guest VLAN 中可以获取 802.1X 客户端软件以升级客户端，或执行其他些应用程序（例如防病毒软件、操作系统补丁等）升级等。

表 8-30 配置 Guest VLAN

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface interface-name	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation link-aggregation-id	
配置 Guest VLAN	authentication guest-vlan guest-vlan-id	必选 缺省情况下，端口下没有配置 Guest VLAN，取值范围为 1~4094

说明：

端口的 Guest VLAN 不能应用到动态 VLAN 上，如 Guest VLAN 所指定的 VLAN ID 是由 GVRP 自动创建的 VLAN，那 Guest VLAN 可以配置成功，但不会生效。

为保证各种功能可以正常使用，请为 Voice VLAN、Private VLAN 以及 Guest VLAN 等分配不同的 VLAN ID。

配置 Guest ACL

如果用户未认证通过，可以在端口下配置 Guest ACL 来限制用户在 Guest VLAN 中访问的资源。

表 8-31 配置 Guest ACL

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太网接口配置模式	interface <i>interface-name</i>	必选其一 进入二层以太网接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	
配置 Guest ACL	authentication guest-acl <i>guest-acl-name</i>	必选 缺省情况下，端口下没有配置 Guest ACL 规则

说明：

端口下未配置 Guest VLAN，则配置 Guest ACL 不生效。

Guest ACL 只在基于用户的接入控制方式（Macbased）下才会生效。

认证设备中已经配置了相应的 ACL 规则。

配置 Critical VLAN

用户采用 RADIUS 认证时，由于认证服务器不可达而导致的认证失败，允许该用户访问指定 VLAN 内的资源，此 VLAN 被称为 Critical VLAN。

端口配置为基于端口接入控制方式时，当端口上有用户进行认证，但所有认证服务器均不可达，端口会被加入到 Critical VLAN，端口下所有用户均可以访问 Critical VLAN 内的资源。

端口配置为基于用户接入控制方式时，当端口上有用户进行认证，但所有认证服务器均不可达，该用户将被仅允许访问 Critical VLAN 内的资源。

端口配置为基于用户接入控制方式需满足以下条件，才能正常运行：

- 端口 VLAN 模式为 Hybrid 模式。
- 端口使能 MAC VLAN 功能。已经处于 Critical VLAN 内的用户发起认证活动，如果认证服务器仍不可达，此用户仍处于 Critical VLAN 内，如果认证服务器可达，则该用户随着认证结果退出 Critical VLAN。

端口加入 Critical VLAN 后，认证设备如果配置了 AAA 探测功能，检测到认证服务器可达后，如果配置了 critical-vlan recovery reinitialize 功能，则：

- 如果端口是 mac-based 接入控制方式，加入 Critical VLAN 的端口会向所有处于 Critical VLAN 的用户主动发送单播报文，触发用户重新进行认证
- 如果端口是 port-based 接入控制方式，加入 Critical VLAN 的端口会主动发送组播报文，触发用户重新进行认证

表 8-32 配置 Critical VLAN

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface interface-name	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation link-aggregation-id	
配置 Critical VLAN	authentication critical-vlan critical-vlan-id	必选 缺省情况下，端口下没有配置 Critical VLAN，取值范围为 1~4094

步骤	命令	说明
配置端口恢复及触发认证	authentication critical-vlan recovery-action reinitialize	可选 缺省情况下，检测到认证服务器可达后，端口仅离开 Critical VLAN

说明：

- 此功能只支持 RADIUS 认证。
- 如果设备上配置了 radius 和逃生功能，即配置了 `aaa authentication dot1x radius none` 和 `critical vlan`，当用户进行认证时，认证服务器不可达，用户不会进入 Critical VLAN，直接逃生；如果只配置了逃生功能，即配置了 `aaa authentication dot1x none`，且配置了 `critical vlan`，当用户进行认证时，逃生功能生效。
- 端口下仅配置 Guest VLAN 功能时，认证失败的用户均处于 Guest VLAN 内。端口下同时配置 Guest VLAN 和 Critical VLAN 功能时，用户由于认证服务器不可达而导致认证失败时，会进入 Critical VLAN，其他原因导致认证失败会进入 Guest VLAN。
- AAA 探测功能请参看 AAA 小节配置。

配置用户认证迁移功能

用户认证迁移功能适用于同一个用户（基于终端 MAC 地址区分）从相同设备的一个认证端口迁移到另外一个认证端口的场景。当禁用用户认证迁移功能时，用户在设备的一个端口上被认证后，该用户不允许在该设备的另外一个认证端口上发起认证；当使能用户认证迁移功能时，用户在一个端口上被认证后，设备在检测到该用户迁移到另外一个认证端口后，设备先删除原先端口上的认证信息后允许用户在新的认证端口上发起认证。

无论是否使能用户认证迁移功能，设备在检测到用户在认证端口间迁移时都会记录日志。

表 8-33 配置用户认证迁移功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface interface-name	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation link-aggregation-id	
配置用户认证迁移功能	authentication station-move { enable disable }	必选 缺省情况下，用户认证迁移功能处于禁用状态。

配置定时器参数

端口下定时器参数包含：重认证定时器、静默定时器、服务器超时定时器、客户端超时定时器、MAC地址认证用户下线检查定时器。

重认证定时器 (re-authperiod)：端口下配置重认证功能后，认证设备定期向客户端发起重认证请求，适用于 802.1X 认证。

静默定时器 (quiet-period)：客户端到达最大认证失败次数，需要等待静默时间超时时，认证设备才会再次响应客户端认证请求，适用于 802.1X 认证和 MAC 地址认证。

服务器超时定时器 (server-timeout)：认证设备在指定的时间内没有接收到服务器回应报文，则认为与服务器失去连接，适用于 802.1X 认证和 MAC 地址认证。

客户端超时定时器 (supp-timeout)：认证设备在指定的时间内没有接收到 802.1X 客户端回应报文，则认为与用户失去连接，适用于 802.1X 认证。

MAC 地址认证用户下线检查定时器 (offline-detect)：使能 MAC 地址认证后，端口下周期检测用户是否在线，适用于 MAC 地址认证。

表 8-34 配置定时器参数

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface <i>interface-name</i>	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	
配置定时器参数	dot1x timeout { re-authperiod <i>re-authperiod-value</i> quiet-period <i>quiet-period-value</i> server-timeout <i>server-timeout-value</i> supp-timeout <i>supp-timeout-value</i> offline-detect <i>offline-detect-value</i> }	必选 缺省情况下， 端口下重认证时间为 3600 秒，取值范围为 5~65535 静默时间 60 秒，取值范围为 1~65535 服务器的超时时间 30 秒，取值范围为 5~3600 客户端的超时时间 30 秒，取值范围为 5~3600 客户端下线检查时间 300 秒，取值范围为 5~3600

配置 MAB 功能

当终端通过 MAC 地址认证通过后，还需要通过客户端认证来使用更高访问权限的时候，可以开启该功能。

表 8-35 使能 MAB 功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface interface-name	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation link-aggregation-id	
使能 802.1X 认证	dot1x port-control { enable disable }	必选 缺省情况下，端口下 802.1X 认证功能处于禁用状态
使能 MAC 地址认证功能	dot1x mac-authentication { enable disable }	必选 缺省情况下，端口下的 MAC 地址认证功能处于禁用状态
使能 MAB 功能	dot1x after-mac-auth { enable disable }	必选 缺省情况下，端口下的 MAB 功能处于禁用状态

恢复端口缺省配置

恢复端口下的 802.1X 认证和 MAC 地址认证的缺省配置。

表 8-36 恢复端口缺省配置

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface <i>interface-name</i>	必选其一 进入二层以太接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	
恢复端口缺省配置	dot1x default	必选 端口下关闭 802.1X 认证和 MAC 地址认证功能，相关的配置参数恢复成缺省值，且缺省配置参数不生效

说明：

命令 show dot1x 用于查看详细的认证缺省配置参数。

56.2.6 802.1X 监控与维护

-B -S -E -A

表 8-37 802.1X 监控与维护

命令	说明
clear dot1x statistic [interface <i>interface-name</i> link-aggregation <i>link-aggregation-id</i> mac { <i>mac-address</i> all }]	清除认证统计信息
clear dot1x auth-fail-user history [mac <i>mac-address</i>]	清除认证失败记录信息
show authentication user [interface <i>interface-name</i> link-aggregation <i>link-aggregation-id</i> mac <i>mac-address</i> summary]	显示认证管理用户信息
show authentication intf-status [interface <i>interface-name</i> link-aggregation <i>link-aggregation-id</i>]	显示认证状态信息
show dot1x	显示认证的缺省配置信息
show dot1x auth-fail-user history [recent mac <i>mac-address</i>]	显示认证失败信息
show dot1x auth-address [<i>mac-address</i> / interface <i>interface-name</i> / link-aggregation <i>link-aggregation-id</i>]	显示可认证主机列表信息
show dot1x config [interface <i>interface-name</i> link-aggregation <i>link-aggregation-id</i>]	显示认证的配置信息
show dot1x free-ip	显示安全通道配置信息。

命令	说明
show dot1x global config	显示全局配置信息
show dot1x statistic [interface <i>interface-name</i> link-aggregation <i>link-aggregation-id</i> mac { <i>mac-address</i> all }]	显示认证统计信息
show dot1x user [interface <i>interface-name</i> link-aggregation <i>link-aggregation-id</i> summary]	显示用户信息

56.3 802.1X 典型配置举例

56.3.1 配置 802.1X 的 Portbased 认证 **-B -S -E -A**

网络需求

- 同一 LAN 上的用户 PC1 和 PC2 通过 Device 接入 IP Network, Device 上使能 802.1X 接入控制;
- 认证方式采用 RADIUS 认证;
- 用户未认证通过时仅允许访问 Update Server, 用户认证通过后允许访问 IP Network;
- LAN 上有一个用户认证通过后, 该 LAN 上的其他用户不需要认证即可访问 IP Network。

网络拓扑

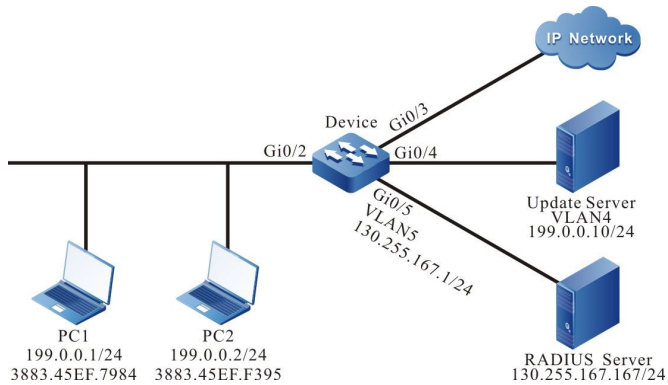


图 8-6 配置 802.1X 的 Portbased 认证组网图

配置步骤

步骤 1： 在 Device 上配置 VLAN 和端口的链路类型。

#在 Device 上创建 VLAN2~VLAN5。

```
Device#configure terminal
Device(config)# vlan 2-5
Device(config)#exit
```

#配置端口 gigabitethernet0/2 的链路类型为 Access，允许 VLAN2 的业务通过。

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode access
Device(config-if-gigabitethernet0/2)#switchport access vlan 2
Device(config-if-gigabitethernet0/2)#exit
```

#在 Device 的 gigabitethernet 0/3~gigabitethernet 0/5 上配置端口链路类型为 Access，分别允许 VLAN3~VLAN5 的业务通过。（略）

步骤 2： 配置 Device 的接口 IP 地址。

#配置 VLAN5 的 IP 地址为 130.255.167.1/24。

```
Device(config)#interface vlan 5
Device(config-if-vlan5)#ip address 130.255.167.1 255.255.255.0
Device(config-if-vlan5)#exit
```

步骤 3： 配置 AAA 认证。

#在 Device 上使能 AAA 认证，采用 RADIUS 认证方式。服务器密钥为 admin，优先级为 1，RADIUS 服务器地址为 130.255.167.167/24。

```
Device(config)#domain system
```

配置手册

```
Device(config-isp-system)# aaa authentication dot1x radius-group radius
Device(config-isp-system)#exit
Device(config)#aaa server group radius radius
Device(config-sg-radius-radius)#server 130.255.167.167 priority 1 key admin
```

步骤 4: 配置 AAA 服务器。

#在 AAA 服务器上配置用户名、密码及密钥值为 admin。 (略)

#在 AAA 服务器上配置 RADIUS 下发 Auto VLAN 的三个属性: 64 为 VLAN, 65 为 802, 81 为 VLAN3。 (略)

步骤 5: 配置端口 802.1X 认证。

#端口上使能 802.1X 认证, 认证模式为 Portbased。

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#dot1x port-control enable
Device(config-if-gigabitethernet0/2)#authentication port-method portbased
Device(config-if-gigabitethernet0/2)#exit
```

#配置端口的 Guest VLAN 为 VLAN4。

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#authentication guest-vlan 4
Device(config-if-gigabitethernet0/2)#exit
```

步骤 6: 检验结果。

#认证通过前, gigabitethernet0/2 被加入 Guest VLAN 中, 此时 PC1、PC2 用户在 VLAN4 内, 并且允许访问 Update Server。

```
Device#show vlan 4
```

```
-----
NO.  VID  VLAN-Name          Owner  Mode   Interface
-----
1   4   VLAN0004                  static Untagged gi0/2 gi0/4
-----
```

#验证 PC1 能够认证通过, 认证服务器下发 VLAN3, 此时 PC1、PC2 用户都在 VLAN3 内, 都可以访问 IP Network。

```
Device#show dot1x user
```

```
-----
NO 1  : MAC_ADDRESS= 3883.45ef.7984 STATUS=   Authorized   USER_NAME=  admin
      VLAN=      3      INTERFACE=  gi0/2      USER_TYPE=  DOT1X
-----
```


AUTH_STATE= AUTHENTICATED BACK_STATE= IDLE IP_ADDRESS= Unknown
IPV6_ADDRESS= Unknown

Online time: 0 week 0 day 0 hours 0 minute 51 seconds

Total: 1 Authorized: 1 Unauthorized/guest/critical: 0/0/0 Unknown: 0

56.3.2 配置 802.1X 的 Macbased 认证 **-B -S -E -A**

网络需求

- PC1 和 PC2 通过 Device 接入 IP Network, Device 采用 802.1X 接入控制;
- 认证方式采用 RADIUS 认证;
- PC 未认证通过时仅允许访问 Update Server,认证通过后允许访问 IP Network;
- LAN 上的一个用户认证通过后, 该 LAN 上的其他用户仍然需要认证通过才允许访问 IP Network。

网络拓扑

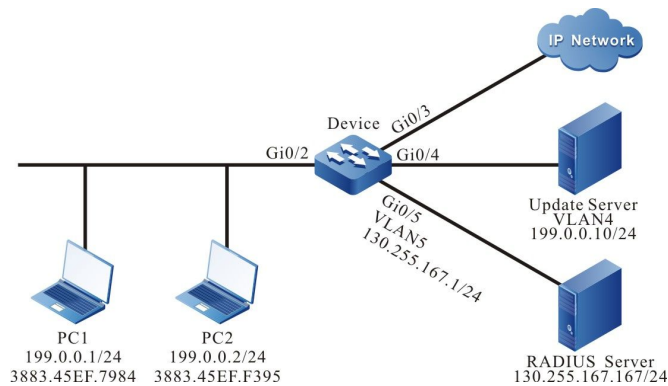


图 8-7 配置 802.1X 的 Macbased 认证组网图

配置步骤

步骤 1: 在 Device 上配置 VLAN 和端口的链路类型。

#在 Device 上创建 VLAN2~VLAN5。

```
Device#configure terminal
Device(config)#vlan 2-5
Device(config)#exit
```

#配置端口 gigabitethernet 0/2 的链路类型为 Hybrid，允许 VLAN2 的业务通过并且 PVID 配置为 2。

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport hybrid untagged vlan 2
Device(config-if-gigabitethernet0/2)#switchport hybrid pvid vlan 2
```

```
Device(config-if-gigabitethernet0/2)#exit
```

#在 Device 的 gigabitethernet 0/3~gigabitethernet 0/5 上配置端口链路类型为 Access，分别允许 VLAN3~VLAN5 的业务通过。（略）

步骤 2： 配置 Device 的接口 IP 地址。

#配置 VLAN5 的 IP 地址为 130.255.167.1/24。

```
Device(config)#interface vlan 5
Device(config-if-vlan5)#ip address 130.255.167.1 255.255.255.0
Device(config-if-vlan5)#exit
```

步骤 3： 配置 AAA 认证。

#在 Device 上开启 AAA 认证，采用 RADIUS 认证方式，服务器密钥为 admin，优先级为 1，RADIUS 服务器地址为 130.255.167.167/24。

```
Device(config)#domain system
Device(config-isp-system)# aaa authentication dot1x radius-group radius
Device(config-isp-system)#exit
Device(config)#aaa server group radius radius
Device(config-sg-radius-radius)#server 130.255.167.167 priority 1 key admin
```

步骤 4： 配置 AAA 服务器。

#在 AAA 服务器上配置用户名和密码以及密钥值为 admin。（略）

#在 AAA 服务器上配置 RADIUS 下发 Auto VLAN 的三个属性：64 为 VLAN，65 为 802，81 为 VLAN3。（略）

步骤 5： 配置 802.1X 认证。

#端口使能 802.1X 认证，配置认证模式为 Macbased。

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#dot1x port-control enable
Device(config-if-gigabitethernet0/2)#authentication port-method macbased
Device(config-if-gigabitethernet0/2)#exit
```

#使能 gigabitethernet0/2 的 MAC VLAN。

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#mac-vlan enable
Device(config-if-gigabitethernet0/2)#exit
```

#配置端口的 Guest VLAN 为 VLAN4。

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#authentication guest-vlan 4
Device(config-if-gigabitethernet0/2)#exit
```

步骤 6: 检验结果。

#认证通过前，gigabitethernet0/2 被加入 Guest VLAN 中，此时 PC1、PC2 用户在 VLAN4 内，PC1 和 PC2 能够访问 Update Server。

```
Device#show vlan 4
-----
NO. VID VLAN-Name          Owner Mode  Interface
-----
1  4  VLAN0004                static Untagged gi0/2 gi0/4
-----
```

#PC1 用户发起认证并成功认证后，PC1 用户在 Auto VLAN3 内，可以访问 IP Network，此时 PC2 仍需要认证通过才能访问 IP Network。

```
Device#show dot1x user
-----
NO 1 : MAC_ADDRESS= 3883.45ef.7984 STATUS=   Authorized   USER_NAME=  admin
      VLAN=       3      INTERFACE=   gi0/2      USER_TYPE=  DOT1X
      AUTH_STATE= AUTHENTICATED BACK_STATE= IDLE      IP_ADDRESS=  Unknown
      IPV6_ADDRESS= Unknown

      Online time: 0 week 0 day 0 hours 0 minute 51 seconds
```

```
Total: 1  Authorized: 1  Unauthorized/guest/critical: 0/0/0  Unknown: 0
```

#PC2 用户输入错误的用户名或密码认证失败后，PC2 用户在 Guest VLAN4 内，可以访问 Update Server。

```
Device#show dot1x user
-----
NO 1 : MAC_ADDRESS= 3883.45ef.f395 STATUS=   Unauth(guest)  USER_NAME=  admin
      VLAN=       4      INTERFACE=   gi0/2      USER_TYPE=  DOT1X
      AUTH_STATE= GUEST_HELD  BACK_STATE= IDLE      IP_ADDRESS=  Unknown
      IPV6_ADDRESS= Unknown
```

```
Total:1  Authorized: 0  Unauthorized/guest/critical: 0/1/0  Unknown: 0
```

56.3.3 配置 802.1X 透传模式

-B -S -E -A

网络需求

- PC 通过 Device1 与开启 802.1X 接入控制的 Device2 相连，接入 IP Network。
- Device1 开启透传功能，Device2 使用 RADIUS 认证方式。
- PC 认证通过后允许访问 IP Network。

网络拓扑

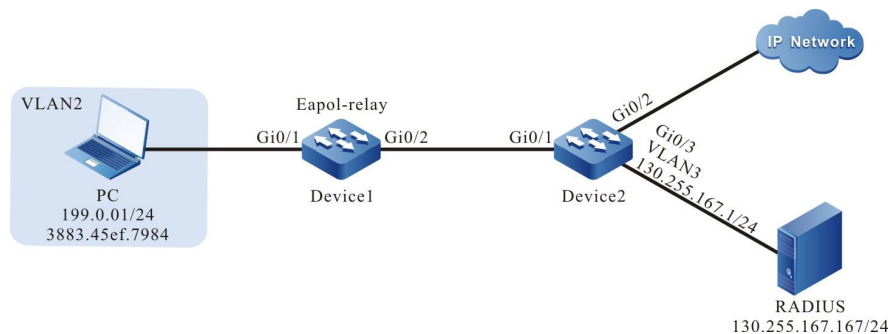


图 8-8 配置 802.1X 透传模式组网图

配置步骤

步骤 1： 在 Device2 上配置 VLAN 和端口的链路类型。

#在 Device2 上创建 VLAN2~VLAN3。

```
Device2#configure terminal
Device2(config)#vlan 2-3
Device2(config)#exit
```

#配置 gigabitethernet 0/1 的链路类型为 Access，允许 VLAN2 的业务通过。

```
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#switchport mode access
Device2(config-if-gigabitethernet0/1)#switchport access vlan 2
Device2(config-if-gigabitethernet0/1)#exit
```

#在 Device2 的 gigabitethernet 0/2~ gigabitethernet 0/3 上配置端口链路类型为 Access，允许 VLAN2~VLAN3 的业务通过。（略）

步骤 2： 配置 Device2 的接口 IP 地址。

#配置 VLAN3 的 IP 地址为 130.255.167.1/24。

```
Device2(config)#interface vlan 3
Device2(config-if-vlan3)#ip address 130.255.167.1 255.255.255.0
Device2(config-if-vlan3)#exit
```

步骤 3： 配置 AAA 认证。

#在 Device2 上开启 AAA 认证，采用 RADIUS 认证方式，服务器密钥为 admin，优先级为 1，RADIUS 服务器地址为 130.255.167.167/24。

```
Device(config)#domain system
Device(config-isp-system)# aaa authentication dot1x radius-group radius
Device(config-isp-system)#exit
Device(config)#aaa server group radius radius
Device(config-sg-radius-radius)#server 130.255.167.167 priority 1 key admin
```

步骤 4： 配置 AAA 服务器。

#在 AAA 服务器上配置用户名和密码以及密钥值为 admin（略）。

步骤 5： 配置 Device1 端口 VLAN。

#在 Device1 的 gigabitethernet0/1~gigabitethernet0/2 上配置端口链路类型为 Access,允许 VLAN2 的业务通过。（略）

步骤 6： 在 Device1 上使能 802.1X 透传功能。

#在 Device1 的 gigabitethernet0/1 上配置 802.1X 透传模式，上联端口为 gigabitethernet0/2。

```
Device1(config)#interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#dot1x eapol-relay enable
Device1(config-if-gigabitethernet0/1)#dot1x eapol-relay uplink interface gigabitethernet 0/2
Device1(config-if-gigabitethernet0/1)#exit
```

步骤 7： 在 Device2 上配置 802.1X 认证模式。

#开启 gigabitethernet0/1 的 802.1X 认证，端口认证模式为 Portbased。

```
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#dot1x port-control enable
Device2(config-if-gigabitethernet0/1)#authentication port-method portbased
Device2(config-if-gigabitethernet0/1)#exit
```

步骤 8: 检验结果。

#PC 用户能够认证成功，可以访问 IP Network。

```
Device2#show dot1x user
```

```
-----
NO 1 : MAC_ADDRESS= 3883.45ef.7984 STATUS=   Authorized   USER NAME=  admin
      VLAN=         2      INTERFACE=  gi0/1      USER_TYPE=  DOT1X
      AUTH_STATE=  AUTHENTICATED  BACK_STATE=  IDLE      IP_ADDRESS=  Unknown
      IPV6_ADDRESS= Unknown

      Online time: 0 week 0 day 0 hours 0 minute 51 seconds

Total: 1  Authorized: 1  Unauthorized/guest/critical: 0/0/0  Unknown: 0
```

56.3.4 配置 802.1X 免客户端认证 **-B -S -E -A**

网络需求

- 网络打印机通过 Device 接入 IP Network，Device 采用 802.1X 接入控制。
- Device 定时对网络打印机进行下线检测。
- 认证时使用 RADIUS 认证方式。
- 网络打印机认证通过后可以执行来自 IP Network 的打印任务。

网络拓扑

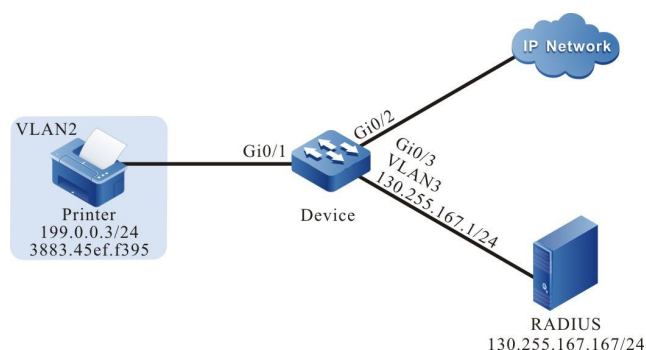


图 8-9 配置 802.1X 免客户端认证组网图

配置步骤

步骤 1： 在 Device 上配置 VLAN 和端口的链路类型。

#在 Device 上创建 VLAN2~VLAN3。

```
Device#configure terminal
Device(config)#vlan 2-3
Device(config)#exit
```

#在 gigabitethernet 0/1 上配置端口链路类型为 Access，允许 VLAN2 的业务通过。

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
Device(config-if-gigabitethernet0/1)#exit
```

#在 Device 的 gigabitethernet 0/2~gigabitethernet 0/3 上配置端口链路类型为 Access，允许 VLAN2~VLAN3 的业务通过。（略）

步骤 2： 配置 Device 的接口 IP 地址。

#配置 VLAN3 的 IP 地址为 130.255.167.1/24。

```
Device(config)#interface vlan 3
Device(config-if-vlan3)#ip address 130.255.167.1 255.255.255.0
Device(config-if-vlan3)#exit
```

步骤 3： 配置 AAA 认证。

#在 Device 上开启 AAA 认证，采用 RADIUS 认证方式，服务器密钥为 admin，优先级为 1，RADIUS 服务器地址为 130.255.167.167/24。

```
Device(config)#domain system
Device(config-isp-system)# aaa authentication dot1x radius-group radius
Device(config-isp-system)#exit
Device(config)#aaa server group radius radius
Device(config-sg-radius-radius)#server 130.255.167.167 priority 1 key admin
```

步骤 4： 配置 AAA 服务器。

#在 AAA 服务器上配置用户名和密码以及密钥为 admin。（略）

步骤 5: 配置 802.1X 认证。

#配置 802.1X 免客户端认证模式，使用网络打印机的 MAC 地址作为用户名和密码。

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#dot1x mac-authentication enable
Device(config-if-gigabitethernet0/1)#exit
```

#配置 Device 每隔 120 秒对打印机进行下线检测。

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#dot1x timeout offline-detect 120
Device(config-if-gigabitethernet0/1)#exit
```

步骤 6: 检验结果。

#网络打印机能够认证通过，可以执行来自 IP Network 的打印任务。

```
Device#show dot1x user
-----
NO 1 : MAC_ADDRESS= 3883.45ef.f395 STATUS= Authorized USER_NAME= 38-83-45-ef-f3-95
      VLAN= 2 INTERFACE= gi0/1 USER_TYPE= DOT1X
      AUTH_STATE= AUTHENTICATED BACK_STATE= IDLE IP_ADDRESS= 199.0.0.3
      IPV6_ADDRESS= Unknown

      Online time: 0 week 0 day 0 hours 1 minutes 6 seconds
Total: 1 Authorized: 1 Unauthorized/guest/critical: 0/0/0 Unknown: 0
```

56.3.5 配置安全通道

-B -S -E -A

网络需求

- 同一 LAN 上的用户 PC1 和 PC2 通过 Device 接入 IP Network，Device 上使能安全通道接入控制；
- 认证方式采用 RADIUS 认证；
- PC1 认证通过前允许访问 Update Server，认证通过后允许访问 Update Server 及 IP Network；

- PC2 不需进行认证即可允许访问 Update Server 及 IP Network。

网络拓扑

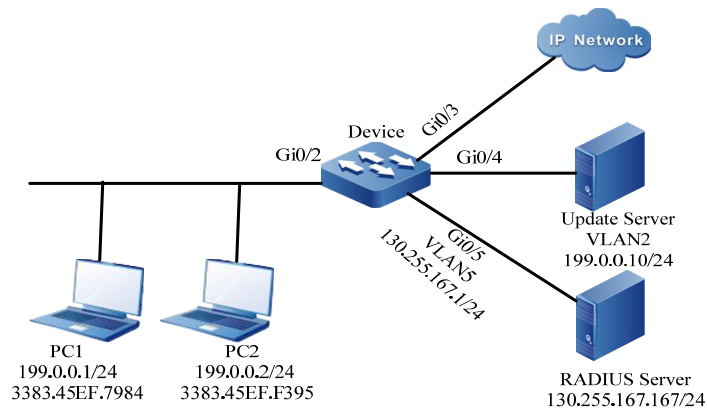


图 8-10 配置安全通道组网图

配置步骤

步骤 1： 在端口上配置 VLAN 和端口的链路类型。

#在 Device 上创建 VLAN2, VLAN5。

```
Device#configure terminal
Device(config)#vlan 2,5
Device(config)#exit
```

#配置 gigabitethernet0/2 的口链路类型为 Access, 允许 VLAN2 的业务通过。

```
Device#configure terminal
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)# switchport mode access
Device(config-if-gigabitethernet0/2)# switchport access vlan 2
Device(config-if-gigabitethernet0/2)#end
```

#在 Device 的 gigabitethernet 0/3~gigabitethernet 0/4 上配置端口链路类型为 Access, 允许 VLAN2 的业务通过。gigabitethernet 0/5 上配置端口链路类型为 Access, 允许 VLAN5 的业务通过。(略)

步骤 2: 配置 Device 的接口 IP 地址。

#配置 VLAN5 的 IP 地址为 130.255.167.1/24。

```
Device#configure terminal
Device(config)#interface vlan 5
Device(config-if-vlan5)#ip address 130.255.167.1 255.255.255.0
Device(config-if-vlan5)#end
```

步骤 3: 配置 AAA 认证。

#在 Device 上开启 AAA 认证，采用 RADIUS 认证方式，服务器密钥为 admin，优先级为 1，RADIUS 服务器地址为 130.255.167.167/24。

```
Device(config)#domain system
Device(config-isp-system)# aaa authentication dot1x radius-group radius
Device(config-isp-system)#exit
Device(config)#aaa server group radius radius
Device(config-sg-radius-radius)#server 130.255.167.167 priority 1 key admin
```

步骤 4: 配置 AAA 服务器。

#在 AAA 服务器上配置用户名和密码以及密钥值为 admin。（略）

步骤 5: 配置安全通道。

#端口 gigabitethernet 0/2 使能安全通道接入控制。

```
Device#configure terminal
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#dot1x free-ip
Device(config-if-gigabitethernet0/2)#exit
```

#配置一条名称为 channel 的安全通道，并配置允许 PC1 访问 Update Server，PC2 允许访问 Update Server 及 IP Network。

```
Device#configure terminal
Device(config)#hybrid access-list advanced channel
Device (config-adv-hybrid-nacl)#permit ip any any host 199.0.0.10 any
Device(config-adv-hybrid-nacl)#permit ip host 199.0.0.2 any any
```

#应用名为 channel 的安全通道。

```
Device#configure terminal
Device(config)#global security access-group channel
```

Device(config)#exit

步骤 6: 检验结果。

#查看安全通道配置信息

```
Device#show dot1x free-ip
802.1X free-ip Enable Interface (num:1): gi0/2
global security access-group channel
Total free-ip user number : 0
```

```
Device#show hybrid access-list channel
hybrid access-list advanced channel
10 permit ip any any host 199.0.0.10 any
20 permit ip host 199.0.0.2 any any any
可以看到 gigabitethernet 0/2 上开启了安全通道,并绑定了 channel 安全通道规则。
```

#PC1 认证通过前, 可以访问 Update Server, 不能访问其他网络资源。

#PC1 用户发起认证并成功认证后, 查看用户认证信息

Device#show dot1x user

```
-----
NO 1 : MAC_ADDRESS= 3883.45ef.7984 STATUS= Authorized USER_NAME= admin
      VLAN= 2 INTERFACE= gi0/2 USER_TYPE= DOT1X
      AUTH_STATE= AUTHENTICATED BACK_STATE= IDLE IP_ADDRESS= 199.0.0.1
      IPV6_ADDRESS= Unknown
```

Online time: 0 week 0 day 0 hours 0 minute 51 seconds

Total: 1 Authorized: 1 Unauthorized/guest/critical: 0/0/0 Unknown: 0
可以看到 PC1 的用户已经认证通过, 此时可以访问 Update Server 及 IP Network。

#PC2 不需进行认证即可访问 Update Server 及 IP Network。

56.3.6 配置 IP 授权 DHCP Server 模式 **-B -S -E -A**

网络需求

- PC 通过 Device 接入 IP Network, Device 使能 802.1X 接入控制;
- 认证方式采用 RADIUS 认证;
- PC1 通过指定的 DHCP Server 获取 IP 地址后可以访问 IP Network;
- PC2 配置携带静态 IP 地址认证后无法访问 IP Network。

网络拓扑

配置手册

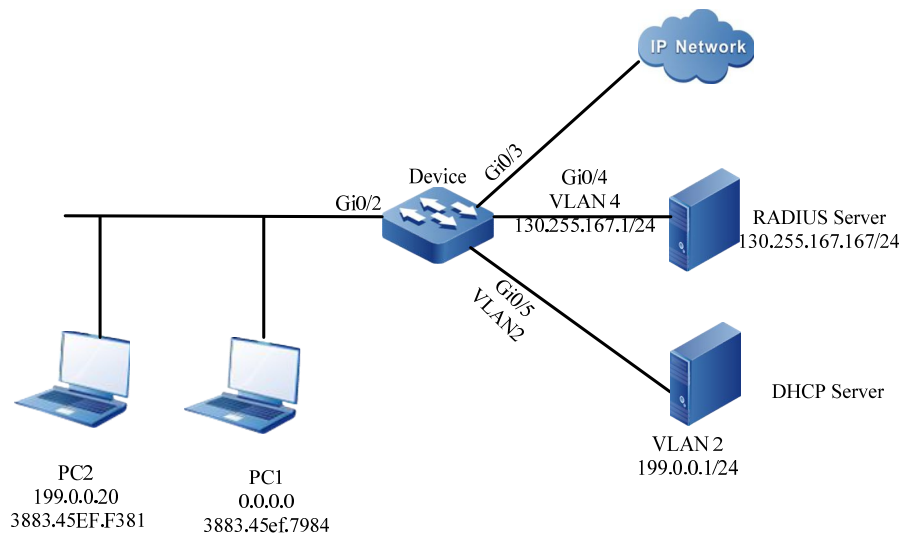


图 8-11 配置 802.1X IP 授权 DHCP Server 模式组网图

配置步骤

步骤 1: 在 Device 上配置 VLAN 和端口的链路类型。

#在 Device 上创建 VLAN2, VLAN4, 在 gigabitethernet0/2 配置端口链路类型为 Hybrid, 允许 VLAN2 的业务通过并且 PVID 配置为 2。

```
Device#configure terminal
Device(config)#vlan 2,4
Device(config)#intergice gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode hybrid
Device(config-if-gigabitethernet0/2)#switchport hybrid untagged vlan 2
Device(config-if-gigabitethernet0/2)#switchport hybrid pvid vlan 2
Device(config-if-gigabitethernet0/2)#exit
```

#在 Device 的 gigabitethernet0/5 上配置端口链路类型为 Access, 允许 VLAN2 的业务通过。(略)

#在 Device 的 gigabitethernet0/4 上配置端口链路类型为 Access, 允许 VLAN4 的业务通过。(略)

步骤 2: 配置 Device 的接口 IP 地址。

#配置 VLAN4 的 IP 地址为 130.255.167.1/24。

```
Device(config)#intergice vlan 4
Device(config-if-vlan4)#ip address 130.255.167.1 255.255.255.0
Device(config-if-vlan4)#exit
```

步骤 3: 配置 AAA 认证。

#在 Device 上开启 AAA 认证, 采用 RADIUS 认证方式, 服务器密钥为 admin, 优先级为 1, RADIUS 服务器地址为 130.255.167.167/24。

```
Device(config)#domain system
Device(config-isp-system)# aaa authentication dot1x radius-group radius
Device(config-isp-system)#exit
Device(config)#aaa server group radius radius
Device(config-sg-radius-radius)#server 130.255.167.167 priority 1 key admin
```

步骤 4: 配置 AAA 服务器。

#在 AAA 服务器上配置用户名和密码以及密钥值为 admin。 (略)

步骤 5: 配置 DHCP 服务器。

#在 DHCP 服务器上配置分配 IP 地址段为 199.0.0.2-199.0.0.10, 子网掩码为 255.255.255.0。
(略)

步骤 6: 在 Device 上使能 DHCP Snooping 功能, 配置 Device 端口 gigabitethernet0/5 为信任端口。

```
Device(config)#dhcp-snooping
Device(config)#intergice gigabitethernet 0/5
Device(config-if-gigabitethernet0/5)#dhcp-snooping trust
Device(config-if-gigabitethernet0/5)#exit
```

步骤 7: 在 Device 上配置 802.1X 认证。

#开启 gigabitethernet0/2 的 802.1X 认证。

```
Device(config)#intergice gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#dot1x port-control enable
Device(config-if-gigabitethernet0/2)#exit
```

#配置 gigabitethernet0/2 的 IP 授权为 DHCP Server 模式。

```
Device(config)#intergice gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#dot1x authorization ip-auth-mode dhcp-server
Device(config-if-gigabitethernet0/2)#exit
```

#使能 gigabitethernet0/2 的 ARP 保活。

```
Device(config)#int gige gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#dot1x client-probe enable
Device(config-if-gigabitethernet0/2)#exit
```

步骤 8: 检验结果。

#PC1 用户能够认证成功, 可以从 DHCP 服务器获取 IP 地址并访问 IP Network。

```
Device#show dot1x user
```

```
-----
NO 1 : MAC_ADDRESS= 3883.45ef.7984 STATUS=   Authorized   USER_NAME=  admin
      VLAN=         2      INTERFACE=  gi0/2      USER_TYPE=  DOT1X
      AUTH_STATE=  AUTHENTICATED  BACK_STATE=  IDLE      IP_ADDRESS=  199.0.0.3
      IPV6_ADDRESS= Unknown
```

Online time: 0 week 0 day 0 hours 0 minutes 36 seconds

Total: 1 Authorized: 1 Unauthorized/guest/critical: 0/0/0 Unknown: 0

#PC2 用户认证后处于 GET-IP 状态无法获取 IP 地址。

```
NO 1 : MAC_ADDRESS= 3883.45ef.f381 STATUS=   Unauthorized  USER_NAME=  admin
      VLAN=         2      INTERFACE=  gi0/2      USER_TYPE=  DOT1X
      AUTH_STATE=  GET_IP    BACK_STATE=  IDLE      IP_ADDRESS=  Unknown
      IPV6_ADDRESS= Unknown
```

Online time: 0 week 0 day 0 hour 0 minute 34 seconds

Total: 1 Authorized: 0 Unauthorized/guest/critical: 1/0/0 Unknown: 0

#通过验证, PC2 无法访问 IP Network。

56.3.7 配置 802.1X Critical VLAN

-B -S -E -A

网络需求

- PC 通过 Device 接入 IP Network, Device 使能 802.1X 接入控制;
- 认证方式采用 RADIUS 认证;
- PC 由于服务器不可达导致认证失败时仅允许访问 Update Server。

网络拓扑

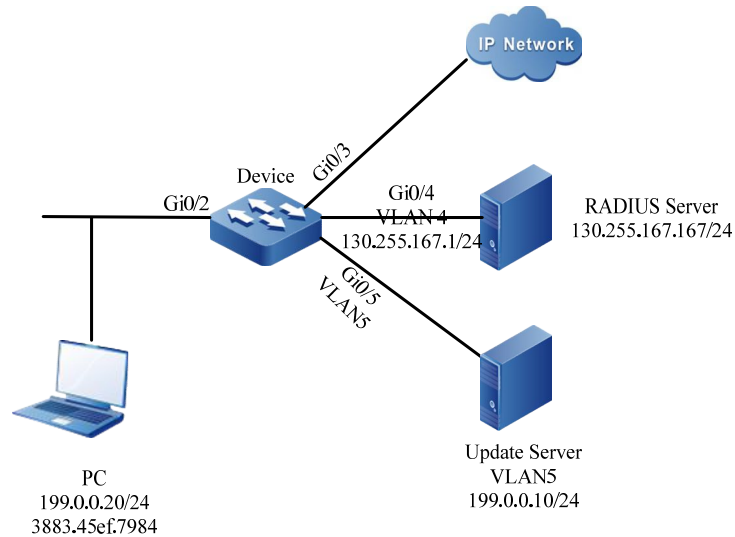


图 8-12 配置 802.1X Critical VLAN 组网图

配置步骤

步骤 1: 在 Device 上配置 VLAN 和端口的链路类型。

#在 Device 上创建 VLAN2, VLAN4, VLAN5, 在 gigabitEthernet0/2 配置端口链路类型为 Hybrid, 允许 VLAN2 的业务通过并且 PVID 配置为 2。

```
Device#configure terminal
Device(config)#vlan 2,4,5
Device(config)#intgigabitEthernet 0/2
Device(config-if-gigabitEthernet0/2)#switchport mode hybrid
Device(config-if-gigabitEthernet0/2)#switchport hybrid untagged vlan 2
Device(config-if-gigabitEthernet0/2)#switchport hybrid pvid vlan 2
Device(config-if-gigabitEthernet0/2)#exit
```

#在 Device 的 gigabitEthernet0/5 上配置端口链路类型为 Access, 允许 VLAN5 的业务通过。(略)

#在 Device 的 gigabitEthernet0/4 上配置端口链路类型为 Access, 允许 VLAN4 的业务通过。(略)

步骤 2: 配置 Device 的接口 IP 地址。

#配置 VLAN4 的 IP 地址为 130.255.167.1/24。

安全

```
Device(config)#intergice vlan 4
Device(config-if-vlan4)#ip address 130.255.167.1 255.255.255.0
Device(config-if-vlan4)#exit
```

步骤 3: 配置 AAA 认证。

#在 Device 上开启 AAA 认证，采用 RADIUS 认证方式，服务器密钥为 admin，优先级为 1，RADIUS 服务器地址为 130.255.167.167/24。

```
Device(config)#domain system
Device(config-isp-system)# aaa authentication dot1x radius-group radius
Device(config-isp-system)#exit
Device(config)#aaa server group radius radius
Device(config-sg-radius-radius)#server 130.255.167.167 priority 1 key admin
```

步骤 4: 配置 AAA 服务器。

#在 AAA 服务器上配置用户名和密码以及密钥值为 admin。（略）

步骤 5: 在 Device 上配置 802.1X 认证。

#开启 gigabitethernet 0/2 的 802.1X 认证。

```
Device(config)#intergice gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#dot1x port-control enable
Device(config-if-gigabitethernet0/2)#exit
```

#使能 gigabitethernet0/2 的 MAC VLAN。

```
Device(config)#intergice gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#mac-vlan enable
Device(config-if-gigabitethernet0/2)#exit
```

#配置端口的 Critical VLAN 为 VLAN5。

```
Device(config)#intergice gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#authentication critical-vlan 5
Device(config-if-gigabitethernet0/2)#exit
```

步骤 6: 检验结果。

#由于服务器异常，Device 无法 ping 通服务器，导致用户由于服务器不可达认证失败，PC 用户在 Critical VLAN 内，能够访问 Update Server。

```
Device#show dot1x user
```

```
-----
NO 1 : MAC_ADDRESS= 3883.45ef.7984 STATUS= Unauth(critical) USER_NAME= admin
1200
```



```
VLAN= 5      INTERFACE= gi0/2      USER_TYPE= DOT1X
AUTH_STATE= CRITICAL_HELD  BACK_STATE= IDLE      IP_ADDRESS= Unknown
IPV6_ADDRESS= Unknown
```

Total: 1 Authorized: 0 Unauthorized/guest/critical: 0/0/1 Unknown: 0

#此时端口 gigabitethernet0/2 被加入到 Critical VLAN 中。

Device#show vlan 5

```
-----
NO. VID VLAN-Name      Owner Mode   Intergice
-----
1  5 VLAN5              static Untagged gi0/2 gi0/5
-----
```

56.3.8 配置 802.1x 与端口安全共用

-B -S -E -A

网络需求

- PC 通过 Device 接入 IP Network，Device 使能 802.1X 接入控制和端口安全；
- 认证方式采用 RADIUS 认证；
- 配置没有匹配 PC1 的 MAC 地址的端口安全规则，PC1 可以认证通过访问 IP Network；
- 配置匹配 PC2 的 MAC 地址的端口安全 deny 规则，PC2 无法认证通过。

网络拓扑

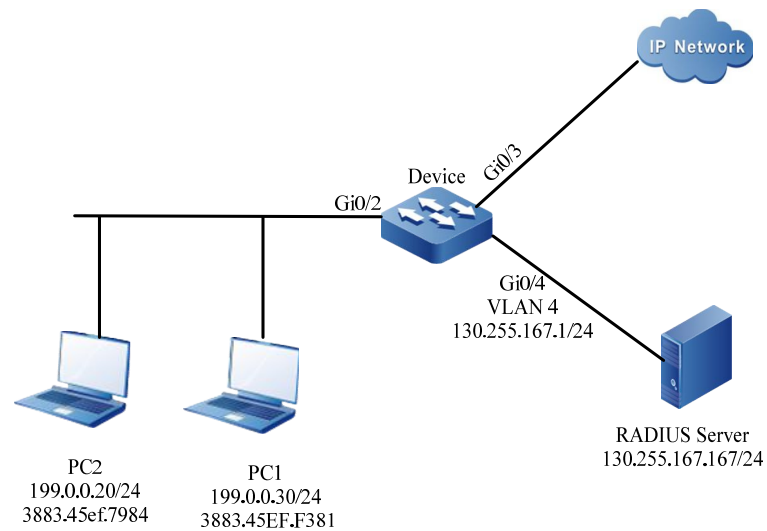


图 8-13 配置 802.1X 与端口安全共用组网图

配置步骤

步骤 1: 在 Device 上配置 VLAN 和端口的链路类型。

#在 Device 上创建 VLAN2, VLAN4, 在 gigabitethernet0/2 配置端口链路类型为 Hybrid, 允许 VLAN2 的业务通过并且 PVID 配置为 2。

```
Device#configure terminal
Device(config)#vlan 2,4
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode hybrid
Device(config-if-gigabitethernet0/2)#switchport hybrid untagged vlan 2
Device(config-if-gigabitethernet0/2)#switchport hybrid pvid vlan 2
Device(config-if-gigabitethernet0/2)#exit
```

#在 Device 的 gigabitethernet0/4 上配置端口链路类型为 Access, 允许 VLAN4 的业务通过。(略)

步骤 2: 配置 Device 的接口 IP 地址。

#配置 VLAN4 的 IP 地址为 130.255.167.1/24。

```
Device(config)#interface vlan 4
Device(config-if-vlan4)#ip address 130.255.167.1 255.255.255.0
Device(config-if-vlan4)#exit
```

步骤 3: 配置 AAA 认证。

#在 Device 上开启 AAA 认证，采用 RADIUS 认证方式，服务器密钥为 admin，优先级为 1，RADIUS 服务器地址为 130.255.167.167/24。

```
Device(config)#domain system
Device(config-isp-system)# aaa authentication dot1x radius-group radius
Device(config-isp-system)#exit
Device(config)#aaa server group radius radius
Device(config-sg-radius-radius)#server 130.255.167.167 priority 1 key admin
```

步骤 4： 配置 AAA 服务器。

#在 AAA 服务器上配置用户名和密码以及密钥值为 admin。（略）

步骤 5： 在 Device 上配置 802.1X 认证。

#开启 gigabitethernet0/2 的 802.1X 认证。

```
Device(config)#intergice gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#dot1x port-control enable
Device(config-if-gigabitethernet0/2)#exit
```

步骤 6： 在 Device 上配置端口安全。

#在端口 gigabitethernet0/2 上使能端口安全。

```
Device(config)#intergice gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#port-security enable
Device(config-if-gigabitethernet0/2)exit
```

#在端口 gigabitethernet0/2 上配置端口安全规则。

```
Device(config)#intergice gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#port-security deny mac-address
3883.45EF.7984
Device(config-if-gigabitethernet0/2)exit
```

步骤 7： 检验结果。

#PC1 用户可以认证成功，认证通过可以访问 IP Network。

```
Device#show dot1x user
```

```
NO 1 : MAC_ADDRESS= 3883.45ef.f381 STATUS= Authorized USER_NAME= admin
      VLAN= 2 INTERFACE= gi0/2 USER_TYPE= DOT1X
      AUTH_STATE= AUTHENTICATED BACK_STATE= IDLE IP_ADDRESS= Unknown
      IPV6_ADDRESS= Unknown
```

Online time: 0 week 0 day 0 hour 0 minute 1 second

Total: 1 Authorized: 1 Unauthorized/guest/critical: 0/0/0 Unknown: 0

#PC2 用户无法认证成功，无法访问网络。

57 ACL 配置

57.1 ACL 简介

57.1.1 ACL 简介

ACL (Access Control List, 访问控制列表)，一个 ACL 由一系列的规则组成，每条规则都是一个允许、拒绝或注释的语句，声明了相应的匹配条件及行为。ACL 规则通过匹配报文中某些字段实现对报文过滤。

ACL 可以由多条规则组成，每一条规则指定的匹配内容都不完全相同，不同规则中的匹配内容可能存在重叠或矛盾。ACL 规则匹配严格按照序号由小到大的顺序进行，序号小的规则优先生效。序号 (Sequence) 指的是规则在整个 ACL 中的顺序编号。

在 ACL 最后一条规则之后，隐含了一条内容为拒绝所有报文的规则，其序号比 ACL 中所有规则的序号都要大，且这条隐含的规则是不可见的，它将丢弃与前面所有规则都不能匹配的报文。即当报文与前面所有的规则都不匹配时，便会匹配该缺省的规则，将报文丢弃。

按照 ACL 的用途，可将 ACL 分为七种类型，IP 标准 ACL、IP 扩展 ACL、MAC 标准 ACL、MAC 扩展 ACL、Hybrid 扩展 ACL、IPv6 标准 ACL、IPv6 扩展 ACL。ACL 名称既可以使用数字，也可以使用用户自定义字符串。ACL 的名称使用数字时，对应的 ACL 类别和数字取值范围如下：

- IP 标准 ACL: 1 ~ 1000;
- IP 扩展 ACL: 1001 ~ 2000;
- MAC 标准 ACL: 2001 ~ 3000;
- MAC 扩展 ACL: 3001 ~ 4000;
- Hybrid 扩展 ACL: 5001 ~ 6000;
- IPv6 标准 ACL: 6001 ~ 7000;
- IPv6 扩展 ACL: 7001 ~ 8000;

ACL 的名称使用用户自定义字符串时，所有 ACL 共享同一个名称空间，也就是说，如果 IP 标准 ACL 使用了某个名称，那么其他 ACL 类型就不能再使用这个名称。

ACL 还可以根据匹配执行相应动作组，详情请参见“QOS 配置手册”。

57.1.2 时间域简介

时间域是时间段的集合，一个时间域可包含零到多个时间段，时间域的时间范围是各个时间段的并集。

时间段有以下两种：

- 周期性时间段，周期性时间段是选择星期一到星期日中某一天或某几天，以及开始时间点和结束时间点作为时间段，每周重复生效；
- 绝对时间段，绝对时间段是以指定的日期和时间范围内生效。

用户常常有一些这样的需求：

某个网段的 PC 只有在工作日的上班时间段内（排除所有的节假日）可以访问服务器；周六的下午允许所有 PC 与外部互联网通信等等；

这些基于时间的通信控制需求，可以通过在 ACL 或 ACL 规则中绑定时间域来满足。

57.2 ACL 功能配置

表 11-1 ACL 功能配置列表

配置任务	
配置 IP 标准 ACL	配置 IP 标准 ACL
	配置以数字命名的 IP 标准 ACL
配置 IP 扩展 ACL	配置 IP 扩展 ACL
	配置以数字命名的 IP 扩展 ACL
配置 MAC 标准 ACL	配置 MAC 标准 ACL
	配置以数字命名的 MAC 标准 ACL
配置 MAC 扩展 ACL	配置 MAC 扩展 ACL
	配置以数字命名的 MAC 扩展 ACL
配置 Hybrid 扩展 ACL	配置 Hybrid 扩展 ACL
	配置以数字命名的 Hybrid 扩展 ACL
配置 IPv6 标准 ACL	配置 IPv6 标准 ACL
	配置以数字命名的 IPv6 标准 ACL
配置 IPv6 扩展 ACL	配置 IPv6 扩展 ACL
	配置以数字命名的 IPv6 扩展 ACL
配置 ACL 规则条目数限制	配置 ACL 规则条目数限制
配置时间域	配置时间域
	配置周期性时间段

配置任务	
	配置绝对时间段
	配置刷新周期
	配置最大时间偏差
	配置时间域与 ACL 规则绑定
	配置时间域与 ACL 绑定
配置 ACL 的应用	配置 IP ACL 应用到端口
	配置 MAC ACL 应用到端口
	配置 IP ACL 应用到 VLAN
	配置 IP ACL 应用到全局
	配置 Hybrid ACL 应用到全局
	配置 IP ACL 应用到接口
	配置 MAC ACL 应用到接口
	配置 IPv6 ACL 应用到端口
配置 IPv6 ACL 应用到接口	

57.2.1 配置 IP 标准 ACL **-B -S -E -A**

IP 标准 ACL 只根据源 IP 地址制定规则，对报文进行过滤处理。

配置条件

无

配置 IP 标准 ACL

IP 标准 ACL 名称可以使用数字，也可以使用用户自定义字符串。IP 标准 ACL 名称如果使用数字时，可配置 ACL 的最大数目有限制；如果采用用户自定义的字符串时，可配置 ACL 的最大数目无限制。用户可以根据实际情况，选择合适的 ACL 名称。

表 57-2 配置 IP 标准 ACL

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 IP 标准 ACL	ip access-list standard { <i>access-list-number</i> <i>access-list-name</i> }	必选 缺省情况下，未配置 IP 标准 ACL IP 标准 ACL 的编号范围为 1 ~ 1000
配置 ACL 允许规则	[<i>sequence</i>] permit { any <i>source-addr</i> <i>source-wildcard</i> / host <i>source-addr</i> } [time-range <i>time-range-name</i>] [log] [pbr-action-group <i>pbr-action-group-name</i>] [l3-action-group <i>l3-action-group-name</i>] [egr-action-group	可选 缺省情况下，未配置 ACL 允许规则

步骤	命令	说明
	<i>egr-action-group-name</i>] [vfp-action-group <i>vfp-action-group-name</i>]	
配置 ACL 拒绝规则	[<i>sequence</i>] deny { any <i>source-addr source-wildcard</i> / host <i>source-addr</i> } [time-range <i>time-range-name</i>] [log] [pbr-action-group <i>pbr-action-group-name</i>] [I3-action-group <i>I3-action-group-name</i>] [egr-action-group <i>egr-action-group-name</i>] [vfp-action-group <i>vfp-action-group-name</i>]	可选 缺省情况下，未配置 ACL 拒绝规则
配置 ACL 注释	[<i>sequence</i>] remark <i>comment</i>	可选 缺省情况下，未配置 ACL 规则的注释

说明：

- 使用命令 **ip access-list standard** 创建 IP 标准访问控制列表时，只有在 IP 标准访问

控制列表配置模式下配置规则后，才能创建访问控制列表。

- 序号 (sequence) 指的是规则在整条 ACL 中的顺序编号。ACL 对报文进行匹配过滤时，严格按照从小序号到大序号的顺序进行，序号小的规则首先生效。当所有的规则都不匹配时，会执行默认的丢弃动作，即一切没有被允许通过的报文都会被丢弃。

配置以数字命名的 IP 标准 ACL

以数字命名 IP 标准 ACL 规则可以让用户快速识别规则访问控制列表的类型。不过以数字命名的 IP 标准 ACL 存在一定局限性，如：访问列表个数有限、用户识别 ACL 规则繁琐。

表 57-3 配置以数字命名的 IP 标准 ACL

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置以数字命名的 IP 标准 ACL	access-list <i>access-list-number</i> { permit deny } { any <i>source-addr source-wildcard</i> host <i>source-addr</i> } [time-range <i>time-range-name</i>] [log] [pbr-action-group <i>pbr-action-group-name</i>] [l3-action-group <i>l3-action-group-name</i>] [egr-action-group <i>egr-action-group-name</i>] [vfp-action-	必选 缺省情况下，未配置以数字命名的 IP 标准 ACL IP 标准 ACL 的编号范围为 1 ~ 1000

步骤	命令	说明
	group <i>vfp-action-group-name</i>]	
配置以数字命名的 IP 标准 ACL 注释	access-list <i>access-list-number</i> remark <i>comment</i>	可选 缺省情况下，未配置以数字命名的 IP 标准 ACL 规则的注释

说明：

- 如果指定编号的 ACL 不存在，则创建一个新的 ACL，同时添加新的规则。如果指定编号的 ACL 存在，则仅添加新的规则。

57.2.2 配置 IP 扩展 ACL **-B -S -E -A**

IP 扩展 ACL 可以根据 IP 协议号、源 IP 地址、目的 IP 地址、源 TCP/UDP 端口号、目的 TCP/UDP 端口号、报文优先级、TCP 标志、分片标志等字段制定分类规则，对报文进行过滤处理。

配置条件

无

配置 IP 扩展 ACL

IP 扩展 ACL 名称可以使用数字，也可以使用用户自定义字符串。IP 扩展 ACL 名称如果使用数字时，可配置 ACL 的最大数目有限制；如果采用用户自定义的字符串时，可配置 ACL 的最大数目无限制。用户可以根据实际情况，选择合适的 ACL 名称。IP 扩展 ACL 比 IP 标准 ACL 所定义的内容更加丰富、准确、灵活。

表 57-4 配置 IP 扩展 ACL

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 IP 扩展 ACL	ip access-list extended { <i>access-list-number</i> <i>access-list-name</i> }	必选 缺省情况下，未配置 IP 扩展 ACL IP 扩展 ACL 的编号范围为 1001 ~ 2000
配置 ACL 允许规则	[<i>sequence</i>] permit <i>protocol</i> { any <i>source-addr</i> <i>source-wildcard</i> / host <i>source-addr</i> } [<i>operator</i> <i>source-port</i>] { any <i>destination-addr</i> <i>destination-wildcard</i> / host <i>destination-addr</i> } [<i>operator</i> <i>destination-port</i>] [ack fin psh rst syn urg] [precedence <i>precedence</i>] [tos <i>tos</i>] [dscp <i>dscp</i>] [fragments] [log] [time-range <i>time-range-name</i>] [pbr-action-group <i>pbr-action-group-name</i>]	可选 缺省情况下，未配置 ACL 允许规则

步骤	命令	说明
	<p>[l3-action-group <i>l3-action-group-name</i>]</p> <p>[egr-action-group <i>egr-action-group-name</i>] [vfp-action-group <i>vfp-action-group-name</i>]</p>	
配置 ACL 拒绝规则	<p>[<i>sequence</i>] deny</p> <p><i>protocol</i> { any <i>source-addr source-wildcard</i> / host <i>source-addr</i> }</p> <p>[<i>operator source-port</i>]</p> <p>{ any <i>destination-addr destination-wildcard</i> / host <i>destination-addr</i> }</p> <p>[<i>operator destination-port</i>] [ack fin psh rst syn urg]</p> <p>[precedence <i>precedence</i>] [tos <i>tos</i>]</p> <p>[dscp <i>dscp</i>]</p> <p>[fragments] [log]</p> <p>[time-range <i>time-range-name</i>]</p> <p>[pbr-action-group <i>pbr-action-group-name</i>]</p> <p>[l3-action-group <i>l3-action-group-name</i>]</p>	<p>可选</p> <p>缺省情况下，未配置 ACL 拒绝规则</p>

步骤	命令	说明
	[egr-action-group <i>egr-action-group-name</i>] [vfp-action-group <i>vfp-action-group-name</i>]	
配置 ACL 注释	[<i>sequence</i>] remark <i>comment</i>	可选 缺省情况下，未配置 ACL 规则的注释

说明：

- 使用命令 **ip access-list extended** 创建 IP 扩展访问控制列表时，只有在 IP 扩展访问控制列表配置模式下配置规则后，才能创建访问控制列表。
- 序号 (sequence) 指的是规则在整条 ACL 中的顺序编号。ACL 对报文进行匹配过滤时，严格按照从小序号到大序号的顺序进行，序号小的规则首先生效。当所有的规则都不匹配时，会执行默认的丢弃动作，即一切没有被允许通过的报文都会被拒绝。

配置以数字命名的 IP 扩展 ACL

以数字命名 IP 扩展 ACL 规则可以让用户快速识别规则访问控制列表的类型。不过以数字命名的 IP 扩展 ACL 存在一定局限性，如：访问列表个数有限、用户识别 ACL 规则繁琐。IP 扩展 ACL 比 IP 标准 ACL 所定义的内容更加丰富、准确、灵活。

表 57-5 配置以数字命名的 IP 扩展 ACL

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
配置以数字命名的 IP 扩展 ACL	<pre> access-list <i>access-list-number</i> { permit deny } <i>protocol</i> { any <i>source-addr source-wildcard</i> / host <i>source-addr</i> } [<i>operator source-port</i>] { any / <i>destination-addr destination-wildcard</i> / host <i>destination-addr</i> } [<i>operator destination-port</i>] [ack fin psh rst syn urg] [precedence <i>precedence</i>] [tos <i>tos</i>] [dscp <i>dscp</i>] [fragments] [log] [time-range <i>time-range-name</i>] [pbr-action-group <i>pbr-action-group-name</i>] [l3-action-group <i>l3-action-group-name</i>] [egr-action-group <i>egr-action-group-name</i>] [vfp-action-group <i>vfp-action-group-name</i>] </pre>	<p>必选</p> <p>缺省情况下，未配置以数字命名的 IP 扩展 ACL</p> <p>IP 扩展 ACL 的编号范围为 1001 ~ 2000</p>

步骤	命令	说明
配置以数字命名的 IP 扩展 ACL 注释	access-list <i>access-list-number</i> remark <i>comment</i>	可选 缺省情况下，未配置以数字命名的 IP 扩展 ACL 规则的注释

说明：

- 如果指定编号的 ACL 不存在，则创建一个新的 ACL，同时添加新的规则。如果指定编号的 ACL 存在，则仅添加新的规则。

57.2.3 配置 MAC 标准 ACL

-B -S -E -A

MAC 标准 ACL 只根据源 MAC 地址制定规则，对报文进行过滤处理。

配置条件

无

配置 MAC 标准 ACL

MAC 标准 ACL 名称可以使用数字，也可以使用用户自定义字符串。MAC 标准 ACL 名称如果使用数字时，可配置的 ACL 数有限制；如果采用用户自定义的字符串时，可配置的 ACL 数无限制。用户可以根据实际情况，选择合适的 ACL 名称。

表 57-6 配置 MAC 标准 ACL

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
配置 MAC 标准 ACL	mac access-list standard { <i>access-list-number</i> <i>access-list-name</i> }	必选 缺省情况下, 未配置 MAC 标准 ACL MAC 标准 ACL 的编号范围为 2001 ~ 3000
配置 ACL 允许规则	[<i>sequence</i>] permit { any <i>source-addr source-wildcard</i> host source-addr } [time-range <i>time-range-name</i>] [log] [I2-action-group <i>I2-action-group-name</i>] [egr-action-group <i>egr-action-group-name</i>] [vfp-action-group <i>vfp-action-group-name</i>]	可选 缺省情况下, 未配置 ACL 允许规则
配置 ACL 拒绝规则	[<i>sequence</i>] deny { any <i>source-addr source-wildcard</i> host source-addr } [time-range <i>time-range-name</i>] [log] [I2-action-group <i>I2-action-group-name</i>] [egr-action-group <i>egr-action-group-name</i>] [vfp-action-	可选 缺省情况下, 未 ACL 拒绝规则

步骤	命令	说明
	group <i>vfp-action-group-name</i>]	
配置 ACL 注释	[<i>sequence</i>] remark <i>comment</i>	可选 缺省情况下，未配置 ACL 规则的注释

说明：

- 使用命令 **mac access-list standard** 创建 MAC 标准访问控制列表时，只有在 MAC 标准访问控制列表配置模式下配置规则后，才能创建访问控制列表。
- 序号 (sequence) 指的是规则在整条 ACL 中的顺序编号。ACL 对报文进行匹配过滤时，严格按照从小序号到大序号的顺序进行，序号小的规则首先生效。当所有的规则都不匹配时，会执行默认的丢弃动作，即一切没有被允许通过的报文都会被丢弃。

配置以数字命名的 MAC 标准 ACL

以数字命名 MAC 标准 ACL 规则可以让用户快速识别规则访问控制列表的类型。不过以数字命名的 MAC 标准 ACL 存在一定局限性，如：访问列表个数有限、用户识别 ACL 规则繁琐。

表 11-7 配置以数字命名的 MAC 标准 ACL

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置以数字命名的 MAC 标准 ACL	access-list <i>access-list-number</i> { permit deny } { any <i>source-addr source-wildcard</i>	必选 缺省情况下，未配置以数字命名的 MAC 标准 ACL

步骤	命令	说明
	host <i>source-addr</i> } [time-range <i>time-range-name</i>] [log] [I2-action-group <i>I2-action-group-name</i>] [egr-action-group <i>egr-action-group-name</i>] [vfp-action-group <i>vfp-action-group-name</i>]	MAC 标准 ACL 的编号范围为 2001 ~ 3000
配置以数字命名的 MAC 标准 ACL 注释	access-list <i>access-list-number</i> remark <i>comment</i>	可选 缺省情况下，未配置以数字命名的 MAC 标准 ACL 规则的注释

说明：

- 如果指定编号的 ACL 不存在，则创建一个新的 ACL，同时添加新的规则。如果指定编号的 ACL 存在，则仅添加新的规则。

57.2.4 配置 MAC 扩展 ACL

-B -S -E -A

MAC 扩展 ACL 可以根据以太协议类型、源 MAC 地址、目的 MAC 地址、VLAN ID、802.1p 优先级等属性制定分类规则，对报文进行过滤处理。

配置条件

无

配置 MAC 扩展 ACL

MAC 扩展 ACL 名称可以使用数字，也可以使用用户自定义字符串。MAC 扩展 ACL 名称如果使用数字时，可配置 ACL 最大数目有限制；如果采用用户自定义的字符串时，可配置 ACL 最大数目无限制。用户可以根据实际情况，选择合适的 ACL 名称。MAC 扩展 ACL 比 MAC 标准 ACL 所定义的内容更丰富，更准确，也更灵活。

表 11-8 配置 MAC 扩展 ACL

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 MAC 扩展 ACL	mac access-list extended { <i>access-list-number</i> <i>access-list-name</i> }	必选 缺省情况下，未配置 MAC 扩展 ACL MAC 扩展 ACL 的编号范围为 3001 ~ 4000
配置 ACL 允许规则	[<i>sequence</i>] permit { any <i>source-addr source-wildcard</i> / host source-addr } { any / <i>destination-addr destination-wildcard</i> / host destination-addr } [ether-type type] [cos cos] [vlan-id vlan] [time-range time-range-name] [log] [I2-action-group I2-action-group-name] [egr-action-group egr-action-group-name]	可选 缺省情况下，未配置 ACL 允许规则

步骤	命令	说明
	[vfp-action-group <i>vfp-action-group-name</i>]	
配置 ACL 拒绝规则	[<i>sequence</i>] deny { any <i>source-addr source-wildcard</i> / host <i>source-addr</i> } { any / <i>destination-addr destination-wildcard</i> / host <i>destination-addr</i> } [ether-type <i>type</i>] [cos <i>cos</i>] [vlan-id <i>vlan</i>] [time-range <i>time-range-name</i>] [log] [l2-action-group <i>l2-action-group-name</i>] [egr-action-group <i>egr-action-group-name</i>] [vfp-action-group <i>vfp-action-group-name</i>]	可选 缺省情况下，未配置 ACL 拒绝规则
配置 ACL 注释	[<i>sequence</i>] remark <i>comment</i>	可选 缺省情况下，未配置 ACL 规则的注释

说明：

- 使用命令 **mac access-list extended** 创建 MAC 扩展访问控制列表时，只有在 MAC 扩展访问控制列表配置模式下配置规则后，才能创建访问控制列表。
- 序号 (sequence) 指的是规则在整条 ACL 中的顺序编号。ACL 对报文进行匹配过滤

时，严格按照从小序号到大序号的顺序进行，序号小的规则首先生效。当所有的规则都不匹配时，会执行默认的丢弃动作，即一切没有被允许通过的报文都会被丢弃。

配置以数字命名的 MAC 扩展 ACL

以数字命名 MAC 扩展 ACL 规则可以让用户快速识别规则访问控制列表的类型。不过以数字命名的 MAC 扩展 ACL 存在一定局限性，如：访问列表个数有限、用户识别 ACL 规则繁琐。MAC 扩展 ACL 比 MAC 标准 ACL 所定义的内容更丰富，更准确，也更灵活。

表 57-9 配置以数字命名的 MAC 扩展 ACL

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置以数字命名的 MAC 扩展 ACL	access-list <i>access-list-number</i> { permit deny } { any <i>source-addr source-wildcard</i> / host <i>source-addr</i> } { any <i>destination-addr destination-wildcard</i> / host <i>destination-addr</i> } [ether-type <i>type</i>] [cos <i>cos</i>] [vlan-id <i>vlan</i>] [time-range <i>time-range-name</i>] [log] [I2-action-group <i>I2-action-group-name</i>] [egr-action-group <i>egr-action-group-name</i>] [vfp-action-group <i>vfp-action-group-name</i>]	必选 缺省情况下，未配置以数字命名的 MAC 扩展 ACL MAC 扩展 ACL 的编号范围为 3001 ~ 4000

步骤	命令	说明
配置以数字命名的 MAC 扩展 ACL 注释	access-list <i>access-list-number</i> remark <i>comment</i>	可选 缺省情况下，未配置以数字命名的 MAC 扩展 ACL 规则的注释

说明：

- 如果指定编号的 ACL 不存在，则创建一个新的 ACL，同时添加新的规则。如果指定编号的 ACL 存在，则仅添加新的规则。

57.2.5 配置 Hybrid 扩展 ACL **-B -S -E -A**

Hybrid 扩展 ACL 可以根据 IP 协议号、源 IP 地址、源 MAC 地址、报文优先级、VLAN ID、802.1p 优先级等属性制定分类规则，对报文进行过滤处理。

配置条件

无

配置 Hybrid 扩展 ACL

Hybrid 扩展 ACL 名称可以使用数字，也可以使用用户自定义字符串。Hybrid 扩展 ACL 名称如果使用数字时，可配置 ACL 最大数目有限制；如果采用用户自定义的字符串时，可配置 ACL 最大数目无限制。用户可以根据实际情况，选择合适的 ACL 名称。Hybrid 扩展 ACL 比单独使用 IP ACL 和 MAC ACL 所定义的内容更丰富，更准确，也更灵活，但 Hybrid 扩展 ACL 只能应用在全局上，且只能过滤接收的报文。

表 57-10 配置 Hybrid 扩展 ACL

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 Hybrid 扩展 ACL	hybrid access-list extended { <i>access-list-number</i> <i>access-list-name</i> }	必选 缺省情况下，未配置 Hybrid 扩展 ACL Hybrid 扩展 ACL 的编号范围为 5001 ~ 6000
配置 ACL 允许规则	[<i>sequence</i>] permit <i>protocol</i> { any <i>source-ip-addr source-wildcard</i> / host <i>source-ip-addr</i> } { any <i>source-mac-addr source-wildcard</i> / host <i>source-mac-addr</i> } [precedence <i>precedence</i>] [tos tos] [dscp dscp] [cos cos] [vlan-id vlan] [time-range <i>time-range-name</i>]	可选 缺省情况下，未配置 ACL 允许规则
配置 ACL 拒绝规则	[<i>sequence</i>] deny <i>protocol</i> { any <i>source-ip-addr source-wildcard</i> / host <i>source-ip-addr</i> } { any <i>source-mac-addr source-wildcard</i> / host <i>source-mac-addr</i> } [precedence	可选 缺省情况下，未配置 ACL 拒绝规则

步骤	命令	说明
	<i>precedence</i> [tos <i>tos</i>] [dscp <i>dscp</i>] [cos <i>cos</i>] [vlan-id <i>vlan</i>] [time-range <i>time-range-name</i>]	
配置 ACL 注释	[<i>sequence</i>] remark <i>comment</i>	可选 缺省情况下，未配置 ACL 规则的注释

说明：

- 使用命令 **hybrid access-list extended** 创建 Hybrid 扩展访问控制列表时，只有在 Hybrid 扩展访问控制列表配置模式下配置规则后，才能创建访问控制列表。
- 序号 (sequence) 指的是规则在整条 ACL 中的顺序编号。ACL 对报文进行匹配过滤时，严格按照从小序号到大序号的顺序进行，序号小的规则首先生效。当所有的规则都不匹配时，会执行默认的丢弃动作，即一切没有被允许通过的报文都会被丢弃。

配置以数字命名的 Hybrid 扩展 ACL

以数字命名 Hybrid 扩展 ACL 规则可以让用户快速识别规则访问控制列表的类型。不过以数字命名的 Hybrid 扩展 ACL 存在一定局限性，如：访问列表个数有限、用户识别 ACL 规则繁琐。

表 57-11 配置以数字命名的 Hybrid 扩展 ACL

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
配置以数字命名的 Hybrid 扩展 ACL	<pre>access-list access-list-number { permit deny } protocol { any source-ip-addr source-wildcard / host source-ip-addr } { any source-mac-addr source-wildcard / host source-mac-addr } [precedence precedence] [tos tos] [dscp dscp] [cos cos] [vlan-id vlan] [time-range time-range-name]</pre>	<p>必选</p> <p>缺省情况下，未配置以数字命名的 Hybrid 扩展 ACL</p> <p>Hybrid 扩展 ACL 的编号范围为 5001 ~ 6000</p>
配置以数字命名的 Hybrid 扩展 ACL 注释	<pre>access-list access-list-number remark comment</pre>	<p>可选</p> <p>缺省情况下，未配置以数字命名的 Hybrid 扩展 ACL 规则的注释</p>

说明：

- 如果指定编号的 ACL 不存在，则创建一个新的 ACL，同时添加新的规则。如果指定编号的 ACL 存在，则仅添加新的规则。

57.2.6 配置 IPv6 标准 ACL

-B -S -E -A

IPv6 标准 ACL 可以根据源 IPv6 地址字段制定分类规则，对报文进行过滤处理。

配置条件

无

配置 IPv6 标准 ACL

IPv6 标准 ACL 名称可以使用数字，也可以使用用户自定义字符串。IPv6 标准 ACL 名称如果使用数字时，可配置 ACL 的最大数目有限制；如果采用用户自定义的字符串时，可配置 ACL 的最大数目无限制。用户可以根据实际情况，选择合适的 ACL 名称。

表 11-12 配置 IPv6 标准 ACL

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 IPv6 标准 ACL	ipv6 access-list standard { <i>access-list-number</i> <i>access-list-name</i> }	必选 缺省情况下，未配置 IPv6 标准 ACL
配置 ACL 允许规则	[<i>sequence</i>] permit { any <i>source-addr/source-wildcard</i> / host source-addr } [time-range <i>time-range-name</i>] [pbr-action-group <i>pbr-action-group-name</i>] [I3-action-group <i>I3-action-group-name</i>] [egr-action-group	可选 缺省情况下，未配置 ACL 允许规则

步骤	命令	说明
	<i>egr-action-group-name</i>]	
配置 ACL 拒绝规则	[<i>sequence</i>] deny { any <i>source-addr/source-wildcard</i> / host <i>source-addr</i> } [time-range <i>time-range-name</i>] [I3-action-group <i>I3-action-group-name</i>] [egr-action-group <i>egr-action-group-name</i>] [pbr-action-group <i>pbr-action-group-name</i>]	可选 缺省情况下，未配置 ACL 拒绝规则
配置 ACL 注释	[<i>sequence</i>] remark <i>comment</i>	可选 缺省情况下，未配置 ACL 规则的注释

说明：

- 使用命令 **ipv6 access-list standard** 创建 IPv6 标准访问控制列表时，只有在 IPv6 标准访问控制列表配置模式下配置规则后，才能创建访问控制列表。
- 序号 (sequence) 指的是规则在整条 ACL 中的顺序编号。ACL 对报文进行匹配过滤时，严格按照从小序号到大序号的顺序进行，序号小的规则首先生效。当所有的规则都不匹配时，会执行默认的丢弃动作，即一切没有被允许通过的报文都会被拒绝。

配置以数字命名的 IPv6 标准 ACL

以数字命名 IPv6 标准 ACL 规则可以让用户快速识别规则访问控制列表的类型。不过以数字命名的 IPv6 标准 ACL 存在一定局限性，如：访问列表个数有限、用户识别 ACL 规则繁琐。

表 57-13 配置以数字命名的 IPv6 标准 ACL

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置以数字命名的 IPv6 标准 ACL	access-list <i>access-list-number</i> { permit deny } { any <i>source-addr/source-wildcard</i> / host <i>source-addr</i> } [time-range <i>time-range-name</i>] [I3-action-group <i>I3-action-group-name</i>] [egr-action-group <i>egr-action-group-name</i>] [pbr-action-group <i>pbr-action-group-name</i>]	必选 缺省情况下，未配置以数字命名的 IPv6 标准 ACL IPv6 标准 ACL 的编号范围为 6001 ~ 7000
配置以数字命名的 IPv6 标准 ACL 注释	access-list <i>access-list-number</i> remark <i>comment</i>	可选 缺省情况下，未配置以数字命名的 IPv6 标准 ACL 规则的注释

说明：

- 如果指定编号的 ACL 不存在，则创建一个新的 ACL，同时添加新的规则。如果指定编号的 ACL 存在，则仅添加新的规则。

57.2.7 配置 IPv6 扩展 ACL

-B -S -E -A

IPv6 扩展 ACL 可以根据 IPv6 协议号、源 IPv6 地址、目的 IPv6 地址、源 TCP/UDP 端口号、目的 TCP/UDP 端口号、报文优先级、TCP 标志等字段制定分类规则，对报文进行过滤处理。

配置条件

无

配置 IPv6 扩展 ACL

IPv6 扩展 ACL 名称可以使用数字，也可以使用用户自定义字符串。IPv6 扩展 ACL 名称如果使用数字时，可配置 ACL 的最大数目有限制；如果采用用户自定义的字符串时，可配置 ACL 的最大数目无限制。用户可以根据实际情况，选择合适的 ACL 名称。

表 57-14 配置 IPv6 扩展 ACL

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 IPv6 扩展 ACL	ipv6 access-list extended { <i>access-list-number</i> <i>access-list-name</i> }	必选 缺省情况下，未配置 IPv6 扩展 ACL
配置 ACL 允许规则	[<i>sequence</i>] permit protocol { any <i>source-addr/source-</i>	可选

步骤	命令	说明
	<pre>wildcard / host source-addr } [operator source-port] { any / destination- addr/destination-wildcard / host destination-addr } [operator destination-port] [ack / fin / psh / rst / syn / urg] [precedence precedence] [tos tos] [dscp dscp] [fragments] [time- range time-range-name] [pbr-action-group pbr- action-group-name] [l3-action-group l3-action- group-name] [egr-action- group egr-action-group- name]</pre>	缺省情况下，未配置 ACL 允许规则
配置 ACL 拒绝规则	<pre>[sequence] deny protocol { any source-addr/source- wildcard / host source-addr } [operator source-port] { any / destination- addr/destination-wildcard / host destination-addr } [operator destination-port] [ack / fin / psh / rst / syn / urg] [precedence precedence] [tos tos] [dscp dscp] [fragments] [time- range time-range-name]</pre>	可选 缺省情况下，未配置 ACL 拒绝规则

步骤	命令	说明
	<pre>[pbr-action-group pbr- action-group-name] [l3-action-group l3-action- group-name] [egr-action- group egr-action-group- name]</pre>	
配置 ACL 注释	<pre>[sequence] remark comment</pre>	可选 缺省情况下，未配置 ACL 规则的注释

说明：

- 使用命令 **ipv6 access-list extended** 创建 IPv6 扩展访问控制列表时，只有在 IPv6 扩展访问控制列表配置模式下配置规则后，才能创建访问控制列表。
- 序号 (sequence) 指的是规则在整条 ACL 中的顺序编号。ACL 对报文进行匹配过滤时，严格按照从小序号到大序号的顺序进行，序号小的规则首先生效。当所有的规则都不匹配时，会执行默认的丢弃动作，即一切没有被允许通过的报文都会被拒绝。

配置以数字命名的 IPv6 扩展 ACL

以数字命名 IPv6 扩展 ACL 规则可以让用户快速识别规则访问控制列表的类型。不过以数字命名的 IPv6 扩展 ACL 存在一定局限性，如：访问列表个数有限、用户识别 ACL 规则繁琐。

表 57-15 配置以数字命名的 IPv6 扩展 ACL

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
配置以数字命名的 IPv6 扩展 ACL	<pre> access-list <i>access-list-number</i> { permit deny } <i>protocol</i> { any <i>source-addr/source-wildcard</i> / host <i>source-addr</i> } [<i>operator source-port</i>] { any / <i>destination-addr/destination-wildcard</i> / host <i>destination-addr</i> } [<i>operator destination-port</i>] [ack / fin / psh / rst / syn / urg] [precedence <i>precedence</i>] [tos <i>tos</i>] [dscp <i>dscp</i>] [fragments] [time-range <i>time-range-name</i>] [pbr-action-group <i>pbr-action-group-name</i>] [l3-action-group <i>l3-action-group-name</i>] [egr-action-group <i>egr-action-group-name</i>] </pre>	<p>必选</p> <p>缺省情况下, 未配置以数字命名的 IPv6 扩展 ACL</p> <p>IPv6 扩展 ACL 的编号范围为 7001 ~ 8000</p>
配置以数字命名的 IPv6 扩展 ACL 注释	<pre> access-list <i>access-list-number</i> remark <i>comment</i> </pre>	<p>可选</p> <p>缺省情况下, 未配置以数字命名的 IPv6 扩展 ACL 规则的注释</p>

说明:

- 如果指定编号的 ACL 不存在，则创建一个新的 ACL，同时添加新的规则。如果指定编号的 ACL 存在，则仅添加新的规则。

57.2.8 配置 ACL 规则条目数限制 **-B -S -E -A**

配置条件

无

配置 ACL 规则条目数限制

使能后，单个 ACL 中可配置的规则条目数最大为 1024。

表 57-16 配置 ACL 规则条目数限制

步骤	命令	说明
进入全局配置模式	configure terminal	-
禁用/使能 ACL 规则条目数限制	access-list rule-limit { enable disable }	必选 缺省为使能，即每个 ACL 中可配置的规则条目数最大为 1024

57.2.9 配置时间域 **-B -S -E -A**

时间域是时间段的集合，一个时间域可包含零到多个时间段，时间域的时间范围是各个时间段的并集。时间域可与 ACL 或 ACL 规则进行绑定，作为 ACL 或 ACL 规则是否生效的条件。

配置条件

在配置时间域功能之前，首先完成以下任务：

- 配置 ACL。

配置时间域

配置时间域应用对象是否受时间域的限制。当处于使能状态时，各应用对象受时间域的限制。反之，则不受时间域的限制。

表 57-17 配置时间域

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置使能/禁用时间域	set time-range { disable enable }	必选 缺省为使能

配置周期性时间段

周期性时间段，周期性时间段是选择星期一到星期日中某一天或某几天，以及开始时间点和结束时间点作为时间段，每周重复生效。

表 11-18 配置周期性时间段

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置时间域	time-range <i>time-range-name</i>	必选 缺省情况下，未配置时间域
配置周期性时间段	[<i>sequence</i>] periodic [<i>day-of-the-week</i>] [<i>hh: mm[: ss]</i>] to	必选其一

步骤	命令	说明
	[<i>day-of-the-week</i>] [<i>hh: mm[: ss]</i>]	缺省情况下, 未配置周期性时间段
	[<i>sequence</i>] periodic { weekdays weekend daily } [<i>hh: mm[: ss]</i>] to [<i>hh: mm[: ss]</i>]	前一命令可以指定时间范围为单一的天 (如: Monday) 或者某几天 (如: Monday, Friday) 后一命令可以指定时间范围为每天、周末或工作日

配置绝对时间段

绝对时间段, 绝对时间段是以指定的日期和时间范围内生效。

表 11-19 配置绝对时间段

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置时间域	time-range <i>time-range-name</i>	必选 缺省情况下, 未配置时间域
配置时间域绝对时间段	[<i>sequence</i>] absolute start <i>hh: mm[: ss]</i> [<i>day</i> [<i>month</i> [<i>year</i>]]] end <i>hh: mm[: ss]</i> [<i>day</i> [<i>month</i> [<i>year</i>]]]	必选 缺省情况下, 未配置时间域绝对时间段

配置刷新周期

时间域的状态为生效和不生效两种，时间域的状态刷新周期默认为 1 分钟，根据当前系统时间自动刷新。因此，状态刷新时，与系统时间比较可能会存在 0-60 秒的时延。

表 11-20 配置刷新周期

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置时间域刷新周期	set time-range frequency { frequency-min / seconds frequency-sec}	必选 缺省值为 1 分钟 刷新周期为两次刷新之间的时间间隔，单位为分钟或秒

配置最大时间偏差

最大偏差时间指的是计数器累加时间与系统时间的最大偏差。时间统计一旦超出该偏差值，下次刷新时重新判断各时间域的状态并更新，以便时间统计更为精确。

表 11-21 配置最大时间偏差

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置时间域最大时间偏差	set time-range max-offset max-offset-number	必选 缺省值为 100 时间偏差单位为秒，取值范围为 1 ~ 300

配置时间域与 ACL 规则绑定

当需要控制某个用户在指定的时间段才能进行网络资源访问时，可以设置基于时间域的 ACL 规则对报文过滤。时间域的生效与否将直接影响与之关联的 ACL 规则。

表 11-22 配置时间域与 ACL 规则绑定

步骤	命令	说明
配置与 IP 标准 ACL 规则绑定	请参见“配置 IP 标准 ACL”	-
配置与 IP 扩展 ACL 规则绑定	请参见“配置 IP 扩展 ACL”	-
配置与 MAC 标准 ACL 规则绑定	请参见“配置 MAC 标准 ACL”	-
配置与 MAC 扩展 ACL 规则绑定	请参见“配置 MAC 扩展 ACL”	-
配置与 Hybrid 扩展 ACL 规则绑定	请参见“配置 Hybrid 扩展 ACL”	-
配置与 IPv6 标准 ACL 规则绑定	请参见“配置 IPv6 标准 ACL”	-
配置与 IPv6 扩展 ACL 规则绑定	请参见“配置 IPv6 扩展 ACL”	-

说明：

- 当 ACL 规则所绑定的时间域不存在时，ACL 规则处于生效状态。

配置时间域与 ACL 绑定

当需要控制某些用户在同一时间段才能进行网络资源访问时，可以设置基于时间域的 ACL 对报文过滤。时间域的生效与否将直接影响整个 ACL 包含的规则。

表 11-23 配置时间域与 ACL 绑定

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置时间域与 IP ACL 绑定	ip time-range <i>time-range-name</i> access-list { <i>access-list-number</i> <i>access-list-name</i> }	必选 缺省情况下，未配置时间域与 IP ACL 绑定
配置时间域与 MAC ACL 绑定	mac time-range <i>time-range-name</i> access-list { <i>access-list-number</i> <i>access-list-name</i> }	必选 缺省情况下，未配置时间域与 MAC ACL 绑定
配置时间域与 Hybrid ACL 绑定	hybrid time-range <i>time-range-name</i> access-list { <i>access-list-number</i> <i>access-list-name</i> }	必选 缺省情况下，未配置时间域与 Hybrid ACL 绑定
配置时间域与 IPv6 ACL 绑定	ipv6 time-range <i>time-range-name</i> access-list { <i>access-list-number</i> <i>access-list-name</i> }	必选 缺省情况下，未配置时间域与 IPv6 ACL 绑定

说明：

- 当 ACL 所绑定的时间域不存在时，ACL 处于生效状态。

57.2.10 配置 ACL 的应用 **-B -S -E -A**

ACL 可应用于全局、VLAN、端口和接口。IP ACL 可以应用到全局、VLAN、端口和接口入方向和出方向；Hybrid ACL 只能应用到全局入方向；MAC ACL 可以应用到端口和接口入方向和出方向；IPv6 ACL 可以应用到端口和接口。

ACL 应用于全局，则会对设备端口入方向的所有报文进行过滤；ACL 应用于 VLAN，则对 VLAN 内端口入方向的所有报文和出方向的转发报文进行过滤；ACL 应用于端口，则对端口入方向的所有报文和出方向的转发报文进行过滤；ACL 应用于接口，则对三层的转发报文进行过滤。

ACL 匹配有优先顺序，优先级从高到低顺序为应用到端口、应用到 VLAN、应用到全局。

如果报文同时匹配了应用到端口、VLAN 和全局的 ACL 规则，对于在高优先级过滤结果为 permit 的报文，将送到下一优先级的 ACL 过滤。对于在高优先级过滤结果为 deny 掉的报文，将直接进行丢弃，不再送到下一优先级的 ACL 处理。

配置条件

在配置 ACL 应用功能之前，首先完成以下任务：

- 配置 ACL。

配置 IP ACL 应用到端口

将 IP ACL 应用到端口上，对该端口通过的报文按照 IP ACL 进行相应分析、处理。

表 11-24 配置 IP ACL 应用到端口

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二/三层以太网接口配置模式	interface interface-name	必选其一

步骤	命令	说明
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	进入二/三层以太网接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
配置将 IP ACL 应用在端口上	ip access-group { <i>access-list-number</i> <i>access-list-name</i> } { in out vfp }	必选 缺省情况下，端口未应用 IP ACL

说明：

- 如果应用到端口的 ACL 不存在，通过该端口的所有报文都被允许。

配置 MAC ACL 应用到端口

将 MAC ACL 应用到端口上，对该端口通过的报文按照 MAC ACL 进行相应分析、处理。

表 11-25 配置 MAC ACL 应用到端口

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二/三层以太网接口配置模式	interface <i>interface-name</i>	必选其一 进入二/三层以太网接口配置模式后，后续配置只在当前端口生效；进入汇聚组
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	

步骤	命令	说明
		配置模式后, 后续配置只在汇聚组生效
配置将 MAC ACL 应用在端口上	mac access-group { <i>access-list-number</i> <i>access-list-name</i> } { in out vfp }	必选 缺省情况下, 端口未应用 MAC ACL

说明:

- 如果应用到端口的 ACL 不存在, 通过该端口的所有报文都被允许。

配置 IP ACL 应用到 VLAN

将 IP ACL 应用到 VLAN 上, 对该 VLAN 通过的报文按照 IP ACL 进行相应分析、处理。

表 11-26 配置 IP ACL 应用到 VLAN

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 VLAN 配置模式	vlan <i>vlan-id</i>	-
配置将 IP ACL 应用在 VLAN 上	ip access-group { <i>access-list-number</i> <i>access-list-name</i> } { in out vfp }	必选 缺省情况下, VLAN 未应用 IP ACL

说明：

- 如果应用到 VLAN 的 ACL 不存在，通过该 VLAN 的所有报文都被允许。

配置 IP ACL 应用到全局

将 IP ACL 应用到全局上，对所有端口通过的报文按照 IP ACL 进行相应分析、处理。

表 11-27 配置 IP ACL 应用到全局

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置将 IP ACL 应用在全局上	global ip access-group { <i>access-list-number</i> <i>access-list-name</i> } in	必选 缺省情况下，全局上未应用 IP ACL

说明：

- 如果应用到全局的 ACL 不存在，且所有端口上没有配置 ACL，则通过端口的所有报文都被允许。

配置 Hybrid ACL 应用到全局

将 Hybrid ACL 应用到全局上，对所有端口通过的报文按照 Hybrid ACL 进行相应分析、处理。

表 11-28 配置 Hybrid ACL 应用到全局

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
配置将 Hybrid ACL 应用在全局上	global hybrid access-group { <i>access-list-number</i> <i>access-list-name</i> } in	必选 缺省情况下，全局未应用 Hybrid ACL

说明：

- 如果应用到全局的 ACL 不存在，且所有端口上没有配置 ACL，则通过所有端口的所有报文都被允许。
- 配置 Hybrid ACL 应用到全局时，需要全局 IP Source Guard 功能处于关闭状态。

配置 IP ACL 应用到接口

将 IP ACL 应用到接口上，对该接口通过的报文按照 IP ACL 进行相应分析、处理。

表 11-29 配置 IP ACL 应用到接口

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置将 IP ACL 应用在接口上	ip access-group { <i>access-list-number</i> <i>access-list-name</i> } { in out self }	必选 缺省情况下，接口未应用 IP ACL

说明：

- 如果应用到接口的 ACL 不存在，通过该接口的所有报文都被允许。
-

配置 MAC ACL 应用到接口

将 MAC ACL 应用到接口上，对该接口通过的报文按照 MAC ACL 进行相应分析、处理。

表 11-30 配置 MAC ACL 应用到接口

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置将 MAC ACL 应用在接口上	mac access-group { <i>access-list-number</i> <i>access-list-name</i> } { in out }	必选 缺省情况下，接口上未应用 MAC ACL

说明：

- 如果应用到接口的 ACL 不存在，通过该接口的所有报文都被允许。
-

配置 IPv6 ACL 应用到端口

将 IPv6 ACL 应用到端口上，对该端口通过的报文按照 IPv6 ACL 进行相应分析、处理。

表 11-31 配置 IPv6 ACL 应用到端口

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二/三层以太网接口配置模式	interface <i>interface-name</i>	必选其一 进入二/三层以太网接口配置模式后, 后续配置只在当前端口生效; 进入汇聚组配置模式后, 后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	
配置将 IPv6 ACL 应用在端口上	ipv6 access-group { <i>access-list-number</i> <i>access-list-name</i> } { in out }	必选 缺省情况下, 端口未应用 IPv6 ACL

说明:

- 如果应用到端口的 ACL 不存在, 通过该端口的所有报文都被允许。

配置 IPv6 ACL 应用到接口

将 IPv6 ACL 应用到接口上, 对该接口通过的报文按照 IPv6 ACL 进行相应分析、处理。

表 11-32 配置 Ipv6 ACL 应用到接口

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-

步骤	命令	说明
配置将 IPv6 ACL 应用在接口上	ipv6 access-group { <i>access-list-number</i> <i>access-list-name</i> } { in out }	必选 缺省情况下, 接口未应用 IPv6 ACL

说明:

- 如果应用到接口的 ACL 不存在, 通过该接口的所有报文都被允许。

57.2.11 ACL 监控与维护

-B -S -E -A

表 11-33 ACL 监控与维护

命令	说明
show access-list [<i>access-list-number</i> <i>access-list-name</i>]	显示 ACL 的配置信息
show acl-object [global interface [vlan [in out] switchport [in out vfp]] vlan [in out]]	显示 VLAN、端口、全局应用 ACL 和 interface VLAN 的信息
show hybrid access-list [<i>access-list-number</i> <i>access-list-name</i>]	显示 Hybrid 扩展、高级 ACL 的配置信息
show ip access-list [<i>access-list-number</i> <i>access-list-name</i>]	显示 IP ACL 的配置信息

命令	说明
show ip interface list	显示接口应用的 IP ACL 信息
show ipv6 access-list [<i>access-list-number</i> <i>access-list-name</i>]	显示 IPv6 ACL 的配置信息
show mac access-list [<i>access-list-number</i> <i>access-list-name</i>]	显示 MAC ACL 的配置信息
show mac interface list	显示接口应用的 MAC ACL 信息
show time-range [<i>time-range-name</i>]	显示时间域的配置和状态信息
show time-range-state [<i>time-range-name</i>]	显示时间域的状态信息

57.3 ACL 典型配置举例

57.3.1 配置 IP 标准 ACL **-B -S -E -A**

网络需求

- PC1、PC2 和 PC3 通过 Device 接入 IP Network。
- 配置 IP 标准 ACL 规则，实现 PC1 能访问 IP Network，PC2 和 PC3 不能访问 IP Network。

网络拓扑

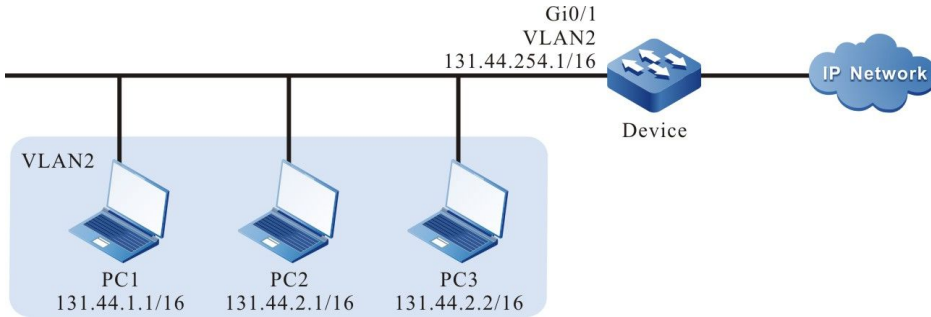


图 11-1 配置 IP 标准 ACL 组网图

配置步骤

步骤 1： 在 Device 上配置 VLAN 和端口的链路类型。

#创建 VLAN2。

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#配置端口 gigabitethernet0/1 的链路类型为 Access，允许 VLAN2 的业务通过。

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
Device(config-if-gigabitethernet0/1)#exit
```

步骤 2： 在 Device 上配置对应 VLAN 接口及 IP 地址。（略）

步骤 3： 配置 IP 标准 ACL。

#在 Device 上配置编号为 1 的 IP 标准 ACL。

```
Device(config)#ip access-list standard 1
```

#配置规则，允许 PC1 访问 IP Network。

```
Device(config-std-nacl)#permit host 131.44.1.1
```

#配置规则，阻止 131.44.2.0/24 网段访问 IP Network。

```
Device(config-std-nacl)#deny 131.44.2.0 0.0.0.255
Device(config-std-nacl)#exit
```

#在 Device 上查看编号为 1 的 ACL 的信息。

```
Device#show ip access-list 1
```

```
ip access-list standard 1
 10 permit host 131.44.1.1
 20 deny 131.44.2.0 0.0.0.255
```

步骤 4: 配置应用 IP 标准 ACL。

#将编号为 1 的 IP 标准 ACL 应用于 Device 端口 gigabitethernet0/1 入方向。

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#ip access-group 1 in
Device(config-if-gigabitethernet0/1)#exit
```

#在 Device 上查看 ACL 应用于端口的信息。

```
Device#show acl-object interface
-----Interface----Bind----Instance-----
Interface-----Direction----AcIType----AcIName
gi0/1           IN      IP      1
-----Interface----Bind----Instance-----
Interface VlanId-----Direction----AcIType----AcIName
Device#
```

步骤 5: 检验结果。

#PC1 能访问 IP Network; PC2 和 PC3 不能访问 IP Network。

57.3.2 配置带时间域的 IP 扩展 ACL **-B -S -E -A**

网络需求

- PC1、PC2 和 PC3 通过 Device 接入 IP Network。
- 配置 IP 扩展 ACL 规则，实现 PC1 指定时间内能访问 IP Network，PC2 能访问 IP Network 中 FTP 服务，PC3 不能访问 IP Network。

网络拓扑

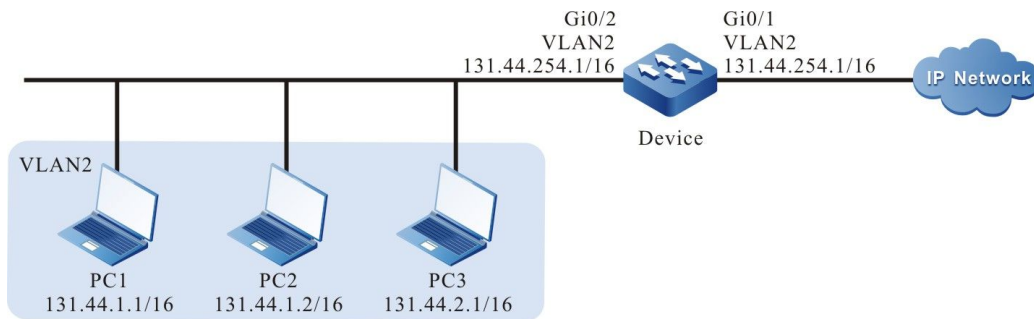


图 57-2 配置带时间域的 IP 扩展 ACL 组网图

配置步骤

步骤 1： 在 Device 上配置 VLAN 和端口的链路类型。

#创建 VLAN2。

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#配置端口 gigabitethernet0/1、gigabitethernet0/2 的链路类型为 Access，允许 VLAN2 的业务通过。

```
Device(config)#interface gigabitethernet 0/1,0/2
Device(config-if-range)#switchport mode access
Device(config-if-range)#switchport access vlan 2
Device(config-if-range)#exit
```

步骤 2： 在 Device 上配置对应 VLAN 接口及 IP 地址。（略）

步骤 3： 配置时间域。

在 Device 上配置时间域 “time-range-work”，范围为每天 08:00:00 到 18:00:00。

```
Device(config)#time-range time-range-work
Device(config-time-range)#periodic daily 08:00:00 to 18:00:00
Device(config-time-range)#exit
```

#在 Device 上查看当前系统时间。

```
Device#show clock
UTC FRI APR 05 15:26:31 2013
```

#在 Device 上查看定义的时间域 “time-range-work” 信息。

```
Device#show time-range time-range-work
```

```
Timerange name:time-range-work (STATE:active)
10 periodic daily 08:00:00 to 18:00:00 (active)
```

步骤 4： 配置 IP 扩展 ACL。

#在 Device 上配置编号为 1001 的 IP 扩展 ACL。

```
Device(config)#ip access-list extended 1001
```

#配置规则，阻止网段 131.44.2.0/24 访问 IP Network。

```
Device(config-ext-nacl)#deny ip 131.44.2.0 0.0.0.255 any
```

#配置规则，允许 PC2 访问 IP Network 的 FTP 服务。

```
Device(config-ext-nacl)#permit tcp host 131.44.1.2 any eq ftp
Device(config-ext-nacl)#permit tcp host 131.44.1.2 any eq ftp-data
```

#配置规则，允许 PC1 在定义的时间域 “time-range-work” 范围内访问 IP Network。

```
Device(config-ext-nacl)#permit ip host 131.44.1.1 any time-range time-range-work
Device(config-ext-nacl)#exit
```

#在 Device 上查看编号为 1001 的 ACL 的信息。

```
Device#show ip access-list 1001
ip access-list extended 1001
10 deny ip 131.44.2.0 0.0.0.255 any
20 permit tcp host 131.44.1.2 any eq ftp
30 permit tcp host 131.44.1.2 any eq ftp-data
40 permit ip host 131.44.1.1 any time-range time-range-work (active)
```

步骤 5： 配置应用 IP 扩展 ACL。

#将编号为 1001 的 IP 扩展 ACL 应用于 Device 端口 gigabitethernet0/1 出方向。

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#ip access-group 1001 out
Device(config-if-gigabitethernet0/1)#exit
```

#在 Device 上查看 ACL 应用于端口的信息。

```
Device#show acl-object interface
-----Interface----Bind----Instance-----
Interface-----Direction---AclType---AclName
gi0/1             OUT      IP      1001
-----Interface----Bind----Instance-----
Interface VlanId-----Direction---AclType---AclName
```

步骤 6: 检验结果。

#PC1 在每天的 08:00 到 18:00 能访问 IP Network; PC2 能访问 IP Network 中任意 FTP 服务器; PC3 不能访问 IP Network。

57.3.3 配置 MAC 标准 ACL **-B -S -E -A**

网络需求

- PC1、PC2 和 PC3 通过 Device 接入 IP Network。
- 配置 MAC 标准 ACL 规则，实现 PC1 能访问 IP Network，PC2、PC3 不能访问 IP Network。

网络拓扑

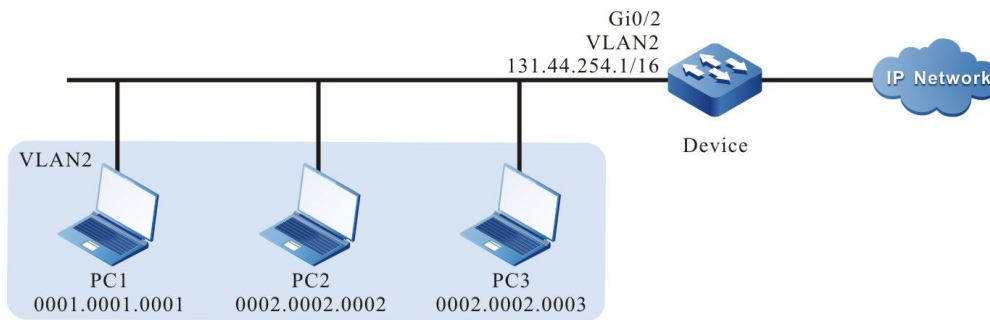


图 57-3 配置 MAC 标准 ACL 组网图

配置步骤

步骤 1: 在 Device 上配置 VLAN 和端口的链路类型。

#创建 VLAN2。

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#配置端口 gigabitethernet0/2 的链路类型为 Access，允许 VLAN2 的业务通过。

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#switchport mode access
Device(config-if-gigabitethernet0/2)#switchport access vlan 2
Device(config-if-gigabitethernet0/2)#exit
```

步骤 2: 在 Device 上配置对应 VLAN 接口及 IP 地址。(略)

步骤 3: 配置 MAC 标准 ACL。

#在 Device 上配置编号为 2001 的 MAC 标准 ACL。

```
Device(config)#mac access-list standard 2001
```

#配置规则, 允许 PC1 访问 IP Network。

```
Device(config-std-mac-nacl)#permit host 0001.0001.0001
```

#配置规则, 阻止 MAC 地址为 0002.0002.0000 掩码为 ffff.ffff.0000 网段访问 IP Network。

```
Device(config-std-mac-nacl)#deny 0002.0002.0000 0000.0000.ffff
```

#在 Device 上查看编号为 2001 的 ACL 的信息。

```
Device#show mac access-list 2001
mac access-list standard 2001
 10 permit host 0001.0001.0001
 20 deny 0002.0002.0000 0000.0000.ffff
```

步骤 4: 配置应用 MAC 标准 ACL。

#将编号为 2001 的 MAC 标准 ACL 应用于 Device 端口 gigabitethernet0/1 入方向。

```
Device(config)#interface gigabitethernet 0/2
Device(config-if-gigabitethernet0/2)#mac access-group 2001 in
Device(config-if-gigabitethernet0/2)#exit
```

#在 Device 上查看 ACL 应用于端口的信息。

```
Device#show acl-object interface
-----Interface----Bind----Instance-----
Interface-----Direction----AcIType----AcIName
gi0/2             IN      MAC     2001
-----Interface----Bind----Instance-----
Interface VlanId-----Direction----AcIType----AcIName
```

步骤 5: 检验结果。

#PC1 能访问 IP Network; PC2、PC3 不能访问 IP Network。

57.3.4 配置 MAC 扩展 ACL

-B -S -E -A

网络需求

- PC1、PC2 和 IP Phone 通过 Device1 接入 IP Network。
- 在 Device2 上配置 MAC 扩展 ACL 规则，实现 VLAN2 的用户不能访问 IP Network，VLAN3 除语音用户外其他用户均能访问 IP Network。

网络拓扑

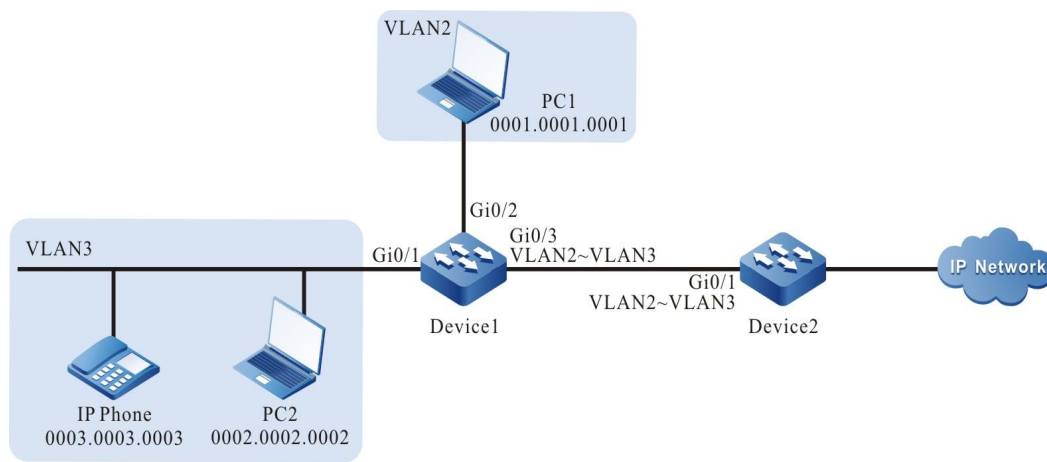


图 57-4 配置 MAC 扩展 ACL 组网图

配置步骤

步骤 1： 在 Device2 上配置 VLAN 和端口的链路类型。

#创建 VLAN2、VLAN3。

```
Device2#configure terminal
Device2(config)#vlan 2
Device2(config-vlan2)#exit
```

```
Device2#configure terminal
Device2(config)#vlan 3
Device2(config-vlan3)#exit
```

#配置端口 gigabitethernet0/1 的链路类型为 Trunk，允许 VLAN2、VLAN3 的业务通过。

```
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#switchport mode trunk
Device2(config-if-gigabitethernet0/1)#switchport trunk vlan 2-3
Device2(config-if-gigabitethernet0/1)#exit
```

步骤 2: 在 Device1 和 Device2 上配置对应 VLAN 接口及 IP 地址。(略)

步骤 3: 在 Device1 上配置 Voice-VLAN 将来自 IP Phone 报文的 cos 值设置为 7。(略)

步骤 4: 配置 MAC 扩展 ACL。

#在 Device2 上配置编号为 3001 的 MAC 扩展 ACL。

```
Device2(config)#mac access-list extended 3001
```

#配置规则, 阻止 VLAN2 内的用户访问 IP Network。

```
Device2(config-ext-mac-nacl)#deny any any vlan-id 2
```

#配置规则, 阻止 VLAN3 内的语音用户访问 IP Network。

```
Device2(config-ext-mac-nacl)#deny any any cos 7 vlan-id 3
```

#配置规则, 允许 VLAN3 内的其它用户访问 IP Network。

```
Device2(config-ext-mac-nacl)#permit any any vlan-id 3
```

#在 Device2 上查看编号为 3001 的 ACL 的信息。

```
Device2#show access-list 3001
mac access-list extended 3001
 10 deny any any vlan-id 2
 20 deny any any cos 7 vlan-id 3
 30 permit any any vlan-id 3
```

步骤 5: 配置应用 MAC 扩展 ACL。

#将编号为 3001 的 MAC 扩展 ACL 应用于 Device2 端口 gigabitethernet0/1 入方向。

```
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#mac access-group 3001 in
Device2(config-if-gigabitethernet0/1)#exit
```

#在 Device2 上查看 ACL 应用于端口的信息。

```
Device#show acl-object interface
-----Interface-----Bind-----Instance-----
Interface-----Direction----AclType----AclName
gi0/1             IN          MAC      3001
-----Interface-----Bind-----Instance-----
Interface VlanId-----Direction----AclType----AclName
```


步骤 6: 检验结果。

#PC2 能访问 IP Network; PC1、IP Phone 不能访问 IP Network。

说明:

- Voice-VLAN 相关配置请参见配置手册 Voice-VLAN 相关章节。

57.3.5 配置 Hybrid 扩展 ACL **-B -S -E -A**

网络需求

- PC1、PC2 和 PC3 通过 Device 接入 IP Network。
- 配置 Hybrid 扩展 ACL 规则，实现 PC1 指定时间范围内能访问 IP Network，PC2 和 PC3 不能访问 IP Network。

网络拓扑

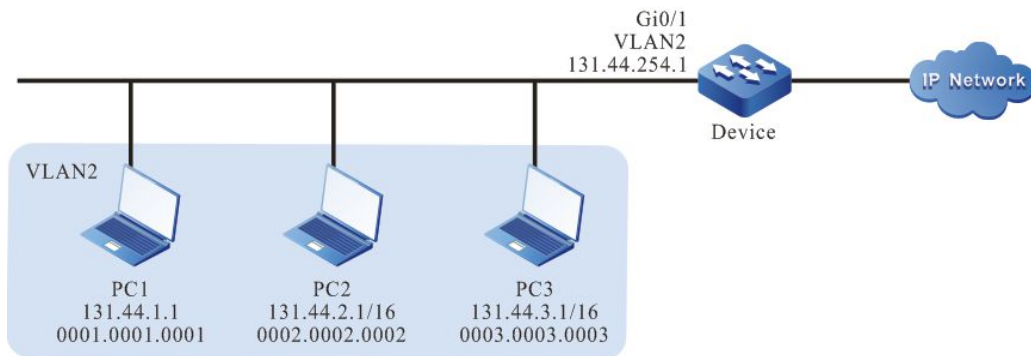


图 57-5 配置 Hybrid 扩展 ACL 组网图

配置步骤

步骤 1: 在 Device 上配置 VLAN 和端口的链路类型。

#创建 VLAN2。

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#配置端口 gigabitethernet0/1 的链路类型为 Access，允许 VLAN2 的业务通过。

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#switchport mode access
Device(config-if-gigabitethernet0/1)#switchport access vlan 2
Device(config-if-gigabitethernet0/1)#exit
```

步骤 2： 在 Device 上配置对应 VLAN 接口及 IP 地址。（略）

步骤 3： 配置时间域。

#在 Device 上配置时间域 “time-range-work”，范围为每天 08:00 到 18:00。

```
Device(config)#time-range time-range-work
Device(config-time-range)#periodic daily 08:00 to 18:00
Device(config-time-range)#exit
```

#在 Device 上查看当前系统时间。

```
Device#show clock

UTC FRI APR 05 15:26:31 2013
```

#在 Device 上查看定义的时间域 “time-range-work” 信息。

```
Device#show time-range time-range-work
Timerange name:time-range-work (STATE:active)
10 periodic daily 08:00 to 18:00 (active)
```

步骤 4： 配置 Hybrid 扩展 ACL 列表。

#在 Device 上配置编号为 5001 的 Hybrid 扩展 ACL。

```
Device(config)#hybrid access-list extended 5001
```

#配置规则，允许 PC1 在定义的时间域 “time-range-work” 范围内访问 IP Network。

```
Device(config-hybrid-nacl)#permit ip any host 0001.0001.0001 time-range time-range-work
```

#配置规则，阻止网段 131.44.0.0/16 访问 IP Network。

```
Device(config-hybrid-nacl)#deny ip 131.44.0.0 0.0.255.255 any
```

#配置规则，允许来自 IP Network 的所有报文通过 Device。

```
Device(config-hybrid-nacl)#permit ip any any
Device(config-hybrid-nacl)#exit
```

#在 Device 上查看编号为 5001 的 ACL 的信息。

```
Device#show hybrid access-list 5001
hybrid access-list extended 5001

10 permit ip any host 0001.0001.0001 time-range time-range-work (active)
20 deny ip 131.44.0.0 0.0.255.255 any
30 permit ip any any
```

步骤 5: 配置应用 Hybrid 扩展 ACL。

#将编号为 5001 的 Hybrid 扩展 ACL 应用于全局的入方向。

```
Device(config)#global hybrid access-group 5001 in
```

#在 Device 上查看 ACL 应用于全局的信息。

```
Device#show acl-object global

-----Global----Bind----Instance-----
Global-----Direction----AclType----AclName
global          IN      HYBRID   5001
```

步骤 6: 检验结果。

#PC1 在每天的 08:00 到 18:00 能访问 IP Network; PC2 和 PC3 不能访问 IP Network。

58 URPF

58.1 URPF 简介

在目前的 Internet 网上，很多网络攻击是利用伪造的源 IP 地址攻击报文进行攻击，这样做的目的是另一方面可以避免自己的 IP 地址被追踪；另一方面像 Land、Smurf 这类攻击，其报文源 IP 地址是被攻击对象 IP 地址。为了限制伪源地址攻击造成的危害，同时能对攻击源进行追踪，在 rfc2827、rfc3704 中提出在 ISP 或边缘网络接入设备上对入网伪造源 IP 地址流量进行过滤，在攻击报文产生源头抑制攻击。

URPF (Unicast Reverse Path Forwarding, 单播反向路径转发) 的主要功能是用于防止基于伪源地址欺骗的网络攻击行为，在报文转发流程中对报文的源地址进行反向路由表查找，根据路由表查找的结果判断是否允许该报文通过。从而起到预防 IP 地址欺骗的作用，特别是针对伪造源 IP 地址的 DoS (Denial of Service, 拒绝服务) 攻击非常有效。URPF 检查有严格 (strict) 和松散 (loose) 两种模式。

网络攻击已经对网络安全构成了严重威胁，URPF 通过在 ISP 或边缘接入设备上过滤伪造源 IP 地址的网络攻击报文，能尽早地抑制网络攻击报文带来的危害，是防范网络攻击的一种有效方法。

58.2 URPF 功能配置

表 58-1 URPF 功能配置列表

配置任务	
配置 URPF 功能	配置 URPF 检查

58.2.1 配置 URPF 功能 *-E -A*

配置条件

无。

配置 URPF 检查

配置 URPF 检查是为了在接收接口过滤基于伪源 IP 地址的攻击报文。URPF 支持严格 (strict) 和松散 (loose) 两种模式，在松散模式下，URPF 会对接收报文的源 IP 地址进行路由表查找，如果找到路由，则允许报文通过。而在严格模式下，不仅要找到路由，且其出接口和报文接收接口相同，才允许报文通过。

表 58-2 配置 URPF 检查

步骤	命令	说明
进入全局配置模式	configure terminal	-
开启全局 URPF 检查	ip urpf [allow-default-route]	必选
进入接口配置模式	interface interface-name	-
开启端口 URPF 检查	ip urpf { loose strict }	必选 缺省情况下，接口未开启 URPF 检查。需开启全局 URPF 检查后，接口 URPF 检查才能生效

58.2.2 URPF 监控与维护

-E -A

表 58-3 URPF 监控与维护

命令	说明
show ip urpf brief	显示接口 URPF 配置信息
show ip urpf config	显示全局以及接口 URPF 配置信息

58.3 URPF 典型配置举例

58.3.1 配置 URPF 严格模式 -E -A

网络需求

- PC 通过 Device 接入 IP Network，在 Device 上配置 URPF 严格模式。
- PC 模拟攻击者发送伪源地址的非法报文访问 IP Network，Device 的 URPF 功能将此报文丢弃。

网络拓扑

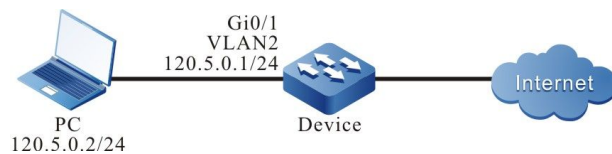


图 14-58-1 配置 URPF 严格模式组网图

配置步骤

- 步骤 1：配置 VLAN，并将端口加入对应的 VLAN。（略）
- 步骤 2：配置各接口的 IP 地址和路由，要求 PC 通过 Device 能访问 IP Network。（略）
- 步骤 3：配置 URPF 严格模式。

#在 Device 上使能 URPF 功能，并在接口 vlan2 上配置 URPF 严格模式。

```
Device#configure terminal
Device(config)#ip urpf
Device(config)#interface vlan2
Device(config-if- vlan2)#ip urpf strict
Device(config-if- vlan2)#exit
```

- 步骤 4：检验结果。

#PC 通过 Device 访问 IP Network，源地址为 120.5.0.2。

Device 上有到 120.5.0.2 的路由，路由出接口为 VLAN2。到源地址的路由出接口和报文接收的接口为同一接口 VLAN2，通过 URPF 严格模式检查，报文被 Device 转发，PC 能访问 IP Network。

#PC 模拟攻击者发送伪源地址的非法报文，通过 Device 访问 IP Network，源地址为 120.10.0.2。

Device 上没有到 120.10.0.2 的路由，URPF 将报文丢弃，PC 不能访问 IP Network。

58.3.2 配置 URPF 松散模式 **-E -A**

网络需求

- 网络环境中 PC1 经过 Device1、Device2、Device3 访问 PC2，PC2 的回应报文经过 Device3、Device1 到达 PC1。
- Device3 上配置 URPF 松散模式。
- PC1 模拟攻击者发送伪源地址的非法报文访问 PC2，Device3 的 URPF 功能将此报文丢弃。

网络拓扑

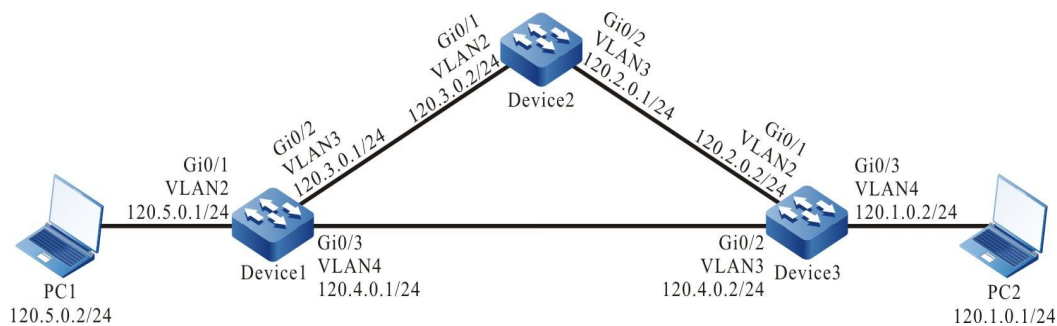


图 14-58-2 配置 URPF 松散模式组网图

配置步骤

步骤 1：配置 VLAN，并将端口加入对应的 VLAN。（略）

步骤 2：配置各接口的 IP 地址。（略）

步骤 3: 在网络中配置静态路由, 使 PC1 经过 Device1、Device2、Device3 访问 PC2, PC2 的回应报文经过 Device3、Device1 到达 PC1。

#配置 Device1、Device2、Device3 的静态路由, 构建网络需求中的网络环境。

```
Device1#configure terminal
Device1(config)#ip route 120.1.0.0 255.255.255.0 120.3.0.2
Device1(config)#ip route 120.2.0.0 255.255.255.0 120.3.0.2
```

```
Device2#configure terminal
Device2(config)#ip route 120.1.0.0 255.255.255.0 120.2.0.2
```

```
Device3#configure terminal
Device3(config)#ip route 120.5.0.0 255.255.255.0 120.4.0.1
```

#查看 Device1、Device2、Device3 的路由表。

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS
```

Gateway of last resort is not set

```
S 120.1.0.0/24 [1/10] via 120.3.0.2, 00:10:49, vlan3
S 120.2.0.0/24 [1/10] via 120.3.0.2, 00:11:19, vlan3
C 120.3.0.0/24 is directly connected, 00:19:15, vlan3
C 120.4.0.0/24 is directly connected, 00:15:00, vlan4
C 120.5.0.0/24 is directly connected, 00:07:36, vlan2
C 127.0.0.0/8 is directly connected, 357:23:02, lo0
```

```
Device2#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS
```

Gateway of last resort is not set

```
S 120.1.0.0/24 [1/10] via 120.2.0.2, 00:15:37, vlan3
C 120.2.0.0/24 is directly connected, 00:17:17, vlan3
C 120.3.0.0/24 is directly connected, 00:25:21, vlan2
C 127.0.0.0/8 is directly connected, 00:38:29, lo0
```

```
Device3#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS
```

Gateway of last resort is not set

```
C 120.1.0.0/24 is directly connected, 00:17:01, vlan4
C 120.2.0.0/24 is directly connected, 00:19:13, vlan2
C 120.4.0.0/24 is directly connected, 00:18:50, vlan3
S 120.5.0.0/24 [1/10] via 120.4.0.1, 00:17:19, vlan3
C 127.0.0.0/8 is directly connected, 00:26:16, lo0
```

步骤 4: 在 Device3 上配置 URPF 松散模式。

#在 Device3 上使能 URPF 功能, 并在 vlan 接口 2 上配置 URPF 松散模式。


```
Device3#configure terminal
Device3(config)#ip urpf
Device3(config)#interface vlan 2
Device3(config-if-vlan2)#ip urpf loose
Device3(config-if-vlan2)#exit
```

步骤 5: 检验结果。

#PC1 ping PC2

PC1 的 ping 请求报文经过 Device1、Device2、Device3 到达 PC2；PC2 的 ping 回应报文经过 Device3、Device1 到达 PC1。

#PC1 访问 PC2，源地址为 120.5.0.2。

Device3 上有到 120.5.0.2 的路由，路由出接口为 VLAN3。虽然到源地址的路由出接口 VLAN 3 和报文接收的接口 VLAN 2 不是同一接口，但通过 URPF 松散模式功能检查，报文被 Device3 转发,PC1 能访问 PC2，并且 PC2 的回应报文经 Device3、Device1 到达 PC1。

#PC1 模拟攻击者发送伪源地址的非法报文访问 PC2，源地址为 120.10.0.2。

Devic3 上没有到 120.10.0.2 的路由，URPF 将报文丢弃，PC1 不能访问 PC2。

说明：

- 由于此检测而产生的报文丢弃不会产生日志和统计信息。
 - URPF 的严格和松散模式的区别为：在松散模式下，URPF 会对接收报文的源 IP 地址进行路由表查找，如果找到路由，则允许该报文通过；而在严格模式下，不仅要找到路由，且其出接口和报文接收接口相同，才允许该报文通过。
 - 一般应用严格模式，松散模式应用于类似案例中“来回路径不一致”的网络环境。
-

59 攻击检测

59.1 攻击检测简介

攻击检测是维护网络安全的一个重要功能，它通过对经过设备处理的报文内容进行分析，判断报文是否具有攻击特征，并根据配置对具有攻击特征的报文执行一定的防范措施，如拦截攻击报文，记录攻击报文日志。通过在设备上配置攻击检测功能，一方面可以避免设备因遭受网络攻击而出现异常，提高设备防攻击能力；另一方面可以拦截经过设备转发的攻击流量，避免网络上其它设备因遭受攻击而不能正常工作。

59.2 攻击检测功能配置

表 59-1 攻击检测功能配置列表

配置任务	
配置软件攻击检测功能	配置拦截 IP 长度太小的报文
	配置拦截不合理分片报文
	配置拦截 Land 攻击报文
	配置拦截 Fraggle 攻击报文
	配置拦截 ICMP 洪水攻击报文
	配置拦截 TCP SYN 洪水攻击报文

配置任务	
	配置拦截地址、端口扫描攻击报文
	配置软件攻击检测日志记录
配置硬件攻击检测功能	配置拦截 IPv4&6 协议的 ICMP 分片报文
	配置拦截超大 ICMP v4 报文的攻击阈值 512 字节
	配置拦截超大 ICMP v6 报文的攻击阈值 512 字节
	配置拦截 IPv4 的 ping-of- death 类型的报文攻击
	配置拦截 smurf 攻击 IPv4 报文攻击
	配置拦截源、目的 MAC 相同的报文
	配置拦截源、目的 IP 相同的报文
	配置拦截源、目的端口相同的 TCP 报文
	配置拦截源、目的端口相同的 UDP 报文
	配置拦截 TCP 的控制字段(flags)和 seq 序列号为 0 的 IPv4&6 报文
	配置拦截 IPv4&6 报文不完整 TCP 协议头小于 20 字节攻击
	配置拦截 TCP 的 FIN、URG、PSH 都为 1 但 suquence 为 0 的 IPv4&6 攻击。

配置任务	
	配置拦截 TCP 中 SYN 和 FIN 标志位被同时置位的 IPv4&6 报文

说明：

- 软件攻击检测功能只对到本机的报文有效，硬件攻击检测功能则对所有交换端口接收的报文有效。
- 软件攻击检测支持对丢弃的报文进行统计和日志记录；硬件攻击检测由交换芯片实现，不支持对丢弃的报文进行统计和日志记录。

59.2.1 配置软件攻击检测功能

-B -S -E -A

软件攻击检测功能是指采用软件方式实现，只对目的地址为设备自身的报文进行攻击检测，从而防止设备自身遭受网络攻击。

配置条件

在配置拦截 ICMP 洪水、TCP SYN 洪水攻击检测功能之前，首先完成以下任务：

- 配置访问控制列表。

配置拦截 IP 长度太小的报文

当设备接收到 IP 长度（包括 IP 头和载荷）小于配置长度的 IP 报文时，将该报文丢弃。

表 59-2 配置拦截 IP 长度太小的报文

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
配置拦截 IP 长度太小的报文	anti-attack drop small-packet [length]	必选 缺省情况下，没有配置拦截 IP 长度太小的报文功能。配置该功能后，如果没有指定长度，则默认拦截 IP 长度小于 64 字节的报文

说明：

- 配置该命令后可能导致 BFD 报文被丢弃。

配置拦截不合理分片报文

当设备接收到 IP 分片报文，且该分片的片偏移加上自身载荷长度超过配置长度时，将该报文丢弃。

表 59-3 配置拦截不合理分片报文

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置拦截不合理分片报文	anti-attack drop fragment [max-off length]	必选 缺省情况下，没有配置拦截不合理分片报文功能。配置该功能后，如果没有指定长度，则默认拦截片偏移加上自身载荷长度超过 65535 的分片报文

配置拦截 ICMP 指定报文

当设备接收到指定过滤的 ICMP 报文进行丢弃。

表 59-4 配置指定的 ICMP 报文

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置拦截到本机的指定类型的 ICMPv4 报文	anti-attack drop icmp type{ ECHOREPLY UNREACH SOURCEQUENCH REDIRECT ECHO ROUTERADVERT ROUTERSOLICIT TIMXCEED PARAMPROB TSTAMP TSTAMPREPLY IREQ IREQREPLY MASKREQ MASKREPLY}	必选 缺省情况下，未配置拦截到本机的指定类型的 ICMPv4 报文

配置拦截 ICMP code 非零报文

当设备接收到 ICMP_ECHO、ICMP_MASKREQ、ICMP_TSTAMP 报文进行丢弃。

表 59-5 配置拦截 ICMP code 非零报文

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
拦截到本机的 code 字段为非零值的 ICMP 请求报文	anti-attack drop icmp code none-zero	必选 缺省情况下，未配置拦截到本机的 code 字段为非零值的 ICMP 请求报文

配置拦截 Land 攻击报文

Land 攻击是一种使用相同的源和目的 IP 和端口发送 TCP SYN 数据包到目标机上，使存在漏洞的目标系统创建一个与自身的 TCP 空连接，甚至导致目标系统崩溃。

当设备接收到源、目的 IP 相同，且源、目的端口相同的 TCP SYN 报文时，将该报文丢弃。

表 59-6 配置拦截 Land 攻击报文

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置拦截 Land 攻击报文	anti-attack detect tcp-land	必选 缺省情况下，没有配置拦截 Land 攻击报文功能

配置拦截 Fraggle 攻击报文

Fraggle 攻击只是其利用的是 UDP 报文目的端口 19 或者 7 进行攻击。

当设备接收到 UDP 报文时，目的端口是 19 或者 7，则认为该报文为 Fraggle 攻击报文，将该报文丢弃。

表 59-7 配置拦截 Fraggle 攻击报文

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置拦截 fraggle 攻击报文	anti-attack detect fraggle	必选 缺省情况下，没有配置拦截 Fraggle 攻击报文功能。

配置拦截 ICMP 洪水攻击报文

ICMP 洪水攻击通过向目标主机发送大量 ICMP 回显请求，使目标主机所在网络拥塞，目标主机消耗大量资源来进行响应，无法提供正常服务。

当设备一秒内接收到同一目的 IP 的 ICMP 报文个数超过允许通过的阈值时，则将超过阈值的报文丢弃。

表 59-8 配置拦截 ICMP 洪水攻击报文

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置拦截 ICMP 洪水攻击报文	anti-attack flood icmp list { access-list-number access-list-name } [maxcount number]	必选 缺省情况下，没有配置拦截 ICMP 洪水攻击报文功能。配置该功能后，如果没有指定阈值，则默认值为 500

说明：

- 配置拦截 ICMP 洪水攻击报文时，需先创建访问控制列表，用于指定保护的数据流，只有访问控制列表允许的数据流，才会检查是否为 ICMP 洪水攻击报文；否则，允许该报文通过。

配置拦截 TCP SYN 洪水攻击报文

TCP SYN Flood 攻击通过向目标主机发送大量 TCP SYN 请求，而不响应 ACK 消息，导致目标主机存在大量处于等待接收请求方 ACK 消息的半连接，占用目标主机可用资源，使其无法提供正常的网络服务。

当设备一秒内接收到同一目的 IP 的 TCP SYN 报文个数超过允许通过的阈值时，则将超过阈值的报文丢弃。

表 59-9 配置拦截 TCP SYN 洪水攻击报文

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置拦截 TCP SYN 洪水攻击报文	anti-attack flood tcp list { <i>access-list-number</i> <i>access-list-name</i> } [maxcount <i>number</i>]	必选 缺省情况下，没有配置拦截 TCP SYN 洪水攻击报文功能。配置该功能后，如果没有指定阈值，则默认值为 1000

说明：

- 配置拦截 TCP SYN 洪水攻击报文时，需先创建访问控制列表，用于指定保护的数据流，只有访问控制列表允许的数据流，才会检查是否为 TCP SYN 洪水攻击报文；否则，允许该报文通过。

配置拦截地址、端口扫描攻击报文

地址扫描攻击是指攻击者通过向网络上发送 ICMP 报文来探测网络上活动的主机，而端口扫描则是攻击者通过向网络上发送 TCP 或 UDP 报文来探测网络上活动主机开启的端口。通过地址、端口扫描，攻击者可以获取网络上活动主机信息。通常情况下，地址、端口扫描是攻击者发动网络攻击的前兆。

当设备一秒内接收到同一源 IP 发送到不同目的 IP 的 ICMP 报文超过阈值时，则认为是地址扫描攻击，将超过阈值的报文丢弃；当设备一秒内接收到同一源 IP 发送的不同目的端口 TCP 或 UDP 报文超过阈值时，则认为是端口扫描攻击，将超过阈值的报文丢弃。

表 59-10 配置拦截地址、端口扫描攻击报文

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置拦截地址、端口扫描攻击报文	anti-attack scanprotect { default interval { default / interval-value } addr-limit { default / max-addr-value } port-limit { default / max-port-value } ban-timeout { default / max-ban-timeout } }	必选 缺省情况下，没有配置拦截地址、端口扫描攻击报文功能。配置该功能后，默认时间间隔为 1s，默认地址扫描阈值为 10 个不同目的 IP，默认端口扫描阈值为 10 个不同目的端口

配置软件攻击检测日志记录

当设备软件攻击检测拦截到攻击报文时，记录日志信息。

表 59-11 配置软件攻击检测日志记录

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置软件攻击检测日志记录	anti-attack log	必选 缺省情况下，没有配置软件攻击检测日志功能

59.2.2 配置硬件攻击检测功能

-B -S -E -A

硬件攻击检测功能是指采用硬件方式实现。

配置条件

无

配置拦截 IPv4&6 协议的 ICMP 分片报文

当设备收到 IPv4&6 协议的 ICMP 分片报文时，将该报文丢弃。

表 59-12 配置拦截 IPv4&6 协议的 ICMP 分片报文

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置拦截 ICMP 分片报文的报文	anti-attack detect frag-icmp	必选 缺省情况下，没有拦截 IPv4&6 协议的 ICMP 分片报文

配置拦截超大 ICMP v4 报文

当设备收到超大 ICMP v4 报文时，将该报文丢弃。

表 59-13 配置拦截超大 ICMP v4 报文

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置拦截超大 ICMP v4 报文	anti-attack detect icmpv4-large	必选 缺省情况下，没有配置拦截超大 ICMP v4 报文，攻击阈值 512 字节

配置拦截超大 ICMP v6 报文

当设备收到超大 ICMP v6 报文时，将该报文丢弃。

表 59-14 配置拦截超大 ICMP v6 报文

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置拦截超大 ICMP v6 报文	anti-attack detect icmpv6-large	必选 缺省情况下，没有配置拦截超大 ICMP v6 报文，攻击阈值 512 字节

配置拦截 IPv4 的 ping-of- death 类型的报文

当设备收到 IPv4 的 ping-of- death 类型的报文时，将该报文丢弃。

表 59-15 配置拦截 IPv4 的 ping-of- death 类型的报文

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置拦截 IPv4 的 ping-of-death 类型的报文	anti-attack detect ping-of-death	必选 缺省情况下，没有配置拦截 IPv4 的 ping-of-death 类型的报文攻击

配置拦截 smurf 类型的报文

当设备收到 smurf 攻击的 IPv4 报文时，将该报文丢弃。

表 59-16 配置拦截 smurf 报文

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置拦截 smurf 类型的报文	anti-attack detect smurf	必选 缺省情况下，没有拦截 smurf 攻击 IPv4 报文

配置拦截源、目的 MAC 相同的报文

当设备交换端口接收到源、目的 MAC 相同的报文时，将该报文丢弃。

表 59-17 配置拦截源、目的 MAC 相同的报文

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
配置拦截源、目的 MAC 相同的报文	anti-attack detect src-dst-mac-equal	必选 缺省情况下，没有配置拦截源、目的 MAC 相同的报文功能

配置拦截源、目的 IP 相同的报文

当设备交换端口接收到源、目的 IP 相同的报文时，将该报文丢弃。

表 59-18 配置拦截源、目的 IP 相同的报文

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置拦截源、目的 IP 相同的报文	anti-attack detect src-dst-ip-equal	必选 缺省情况下，没有配置拦截源、目的 IP 相同的报文功能

配置拦截源、目的端口相同的 TCP/UDP 报文

当设备交换端口接收到 TCP/UDP 源、目的端口相同的报文时，将该报文丢弃。

表 59-19 配置拦截源、目的端口相同的 TCP/UDP 报文

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
配置拦截 TCP/UDP 源、目的端口相同的报文	anti-attack detect src-dst-port-equal	必选 缺省情况下，没有配置拦截源、目的端口相同的 TCP/UDP 报文功能

配置拦截 TCP 的控制字段(flags)和 seq 序列号为 0 的 IPv4&6 报文

当设备交换端口接收 TCP 的控制字段(flags)和 seq 序列号为 0 的 IPv4&6 报文时，将该报文丢弃。

表 59-20 配置拦截 TCP 的控制字段(flags)和 seq 序列号为 0 的 IPv4&6 报文

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置拦截拦截 TCP 的控制字段(flags)和 seq 序列号为 0 的 IPv4&6 报文	anti-attack detect tcp-flag-seq-zero	必选 缺省情况下，没有配置拦截 TCP 的控制字段(flags)和 seq 序列号为 0 的 IPv4&6 报文

配置拦截 IPv4&6 报文不完整 TCP 协议头小于 20 字节攻击

当设备交换端口接收 IPv4&6 报文不完整 TCP 协议头小于 20 字节攻击报文时，将该报文丢弃。

表 59-21 配置拦截 IPv4&6 报文不完整 TCP 协议头小于 20 字节攻击报文

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
配置拦截 IPv4&6 报文不完整 TCP 协议头小于 20 字节攻击	anti-attack detect tcp-hdr-incomplete	必选 缺省情况下，没有配置拦截 IPv4&6 报文不完整 TCP 协议头小于 20 字节攻击

配置拦截 TCP 的 FIN、URG、PSH 都为 1 但 sequence 为 0 的 IPv4&6 攻击

当设备交换端口接收 TCP 的 FIN、URG、PSH 都为 1 但 sequence 为 0 的 IPv4&6 攻击报文时，将该报文丢弃。

表 59-22 配置拦截 TCP 的 FIN、URG、PSH 都为 1 但 sequence 为 0 的 IPv4&6 攻击

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置拦截 TCP 的 FIN、URG、PSH 都为 1 但 sequence 为 0 的 IPv4&6 攻击报文	anti-attack detect tcp-invalid-flag	必选 缺省情况下，没有配置拦截 TCP 的 FIN、URG、PSH 都为 1 但 sequence 为 0 的 IPv4&6 攻击报文

配置拦截 TCP 中 SYN 和 FIN 标志位被同时置位的 IPv4&6 报文

当设备交换端口接收 TCP 中 SYN 和 FIN 标志位被同时置位的 IPv4&6 报文时，将该报文丢弃。

表 59-23 配置拦截 TCP 中 SYN 和 FIN 标志位被同时置位的 IPv4&6 报文攻击

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
配置拦截 TCP 中 SYN 和 FIN 标志位被同时置位的 IPv4&6 报文	anti-attack detect tcp-syn-fin	必选 缺省情况下，没有配置拦截 TCP 中 SYN 和 FIN 标志位被同时置位的 IPv4&6 报文

59.2.3 攻击检测监控与维护

-B -S -E -A

表 59-24 攻击检测监控与维护

命令	说明
clear anti-attack statistic	清除软件攻击检测统计信息
show anti-attack config	显示攻击检测软件和硬件配置信息
show anti-attack statistic	显示软件攻击检测统计信息
show anti-attack scanprotect config	显示扫描攻击检测配置信息
show anti-attack scanprotect monitor	显示扫描攻击检测统计信息
clear anti-attack scanprotect	清除扫描攻击检查统计信息

59.3 攻击检测典型配置举例

59.3.1 配置防 DDOS 攻击检测

-B -S -E -A

网络需求

- Device 通过端口 gigabitethernet0/1 接入 IP Network。
- Device 配置防 DDOS 攻击检测功能，检测到攻击报文时告警，并将攻击报文丢弃，以常见的 SYN Flood 攻击、Ping Flood 攻击、Land 攻击为例。

网络拓扑

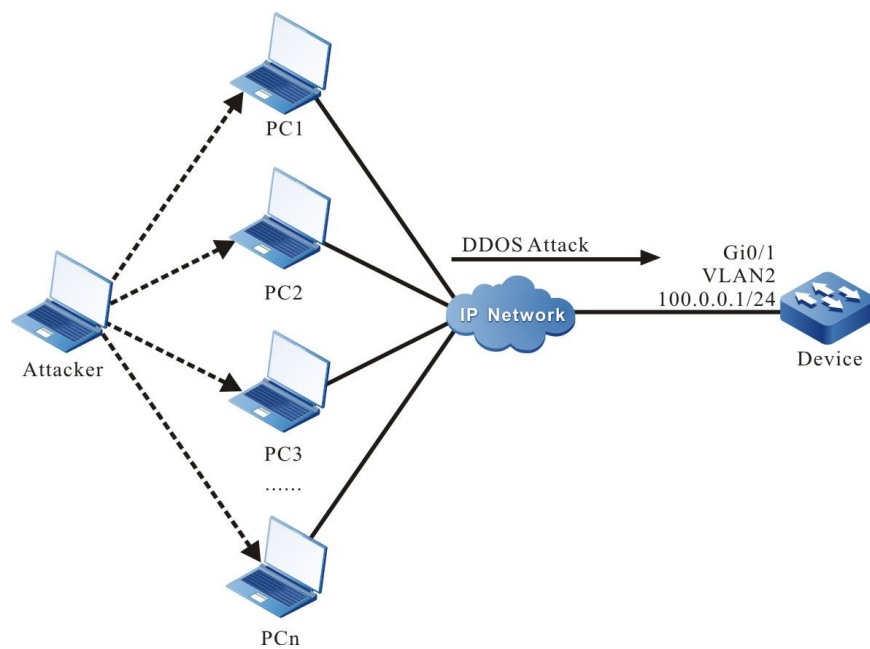


图 15-59-1 配置防 DDOS 攻击检测组网图

配置步骤

- 步骤 1: 配置 VLAN，并将端口加入对应的 VLAN。（略）
- 步骤 2: 配置各接口 IP 地址。（略）
- 步骤 3: 配置 ACL 规则。

#配置标准 ACL 规则，匹配需保护的 Device 地址。

```
Device#configure terminal
Device(config)#ip access-list standard 1
Device(config-std-nacl)#permit host 100.0.0.1
Device(config-std-nacl)#exit
```

步骤 4: 配置攻击检测功能，使能日志记录功能。

#在 Device 上配置 SYN Flood、Ping Flood、Land 攻击检测功能。

```
Device(config)# anti-attack detect tcp-land
Device(config)# anti-attack flood icmp list 1 maxcount 100
Device(config)# anti-attack flood tcp list 1 maxcount 100
```

#在 Device 上使能防 DDOS 攻击检测的日志记录功能。

```
Device(config)# anti-attack log
```

步骤 5: 检验结果。

#Device 受到 SYN Flood 攻击时，输出如下日志信息：

```
%FW_FLOOD_WARN-4: vlan2 gigabitethernet0/1 SYN flood attack detected, destination IP 100.0.0.1, 1000
packets/second.
```

#Device 受到 Ping flood 攻击时，输出如下日志信息：

```
%FW-FLOOD_WARN-4: vlan2 gigabitethernet0/1 ICMP flood attack detected, destination IP
104.1.1.1, overflow 20packets/second..
```

#Device 受到 Land 攻击时，输出如下日志信息：

```
%FW-LAND_WARN-4: LAND attack detected at vlan2 gigabitethernet0/1, source IP equal destination IP is
100.0.0.1, source port equal destination port is 1024.
```

#在 Device 上查看攻击检测报文统计信息。

```
IP attack      Drops
-----
Small IP      0
Fragment      0
Tcp-land      6256
Fraggle       0
SYN Flood     6200
ICMP Flood    4893
```

说明：

- DDOS 攻击检测功能仅对 CPU 处理的报文有效。

59.3.2 配置拦截源、目的 IP 地址相同的攻击检测

-B -S -E -A

网络需求

- Device 配置拦截源、目的 IP 地址相同的攻击检测功能，检测到攻击报文将其丢弃。

网络拓扑

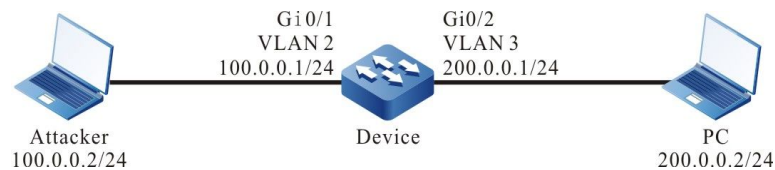


图 15-59-2 配置拦截源、目的 IP 地址相同的攻击检测组网图

配置步骤

- 步骤 1: 配置 VLAN，并将端口加入对应的 VLAN。（略）
- 步骤 2: 配置各接口 IP 地址。（略）
- 步骤 3: 配置攻击检测功能。

#配置拦截源、目的 IP 地址相同的攻击检测功能。

```
Device#configure terminal
Device(config)# anti-attack detect src-dst-ip-equal
```

- 步骤 4: 检验结果。

#当 Attacker 向 PC 发起源、目的 IP 地址相同的报文攻击时，在 PC 上捕获不到攻击报文。

说明:

- 拦截源、目的 IP 地址相同的攻击检测功能对 CPU 处理的报文和业务报文均有效。
 - 拦截源、目的 IP 地址相同的攻击检测功能进行报文丢弃时，不会生成日志和统计信息。
-

可靠性

60 HA

60.1 HA 简介

HA (High Availability, 高可用性)是设备上的一种高可用性管理平台，对一些系统级别故障进行定期检测，保证业务的持续不中断进行。

60.2 HA 功能配置

60.2.1 HA 监控与维护 *-B -S -E -A*

表 60-1 HA 监控与维护

命令	说明
<code>show ham job</code>	显示当前本地设备的 HA 任务处理节点表

61 ULFD

61.1 ULFD 简介

在传统的以太网中，通常使用光纤等物理介质进行设备间的连接。在实际的组网中，由于光纤交叉连接(图 2-1)，或者其中一条光纤未连接及断路(图 2-2)都会导致单向通信，这类故障链路称为单向链路。单向链路会引起一系列问题，比如生成树检测失效导致拓扑计算错误等。

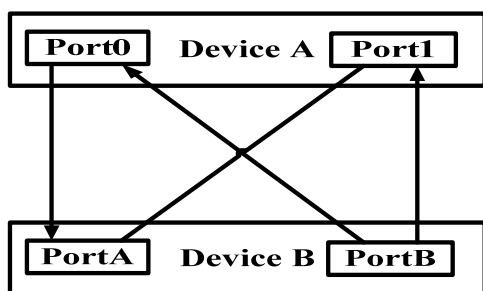


图 61-1 光纤交叉连接

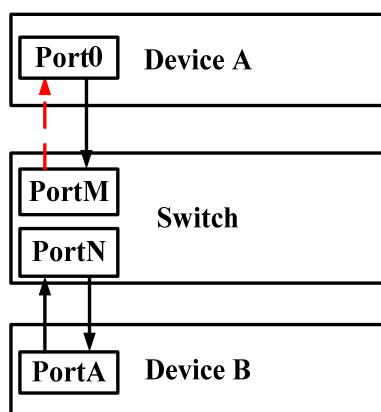


图 61-2 一条光纤未连接或者断路

ULFD (Unidirectional Link Fault Detection) 单向链路故障检测可以监控光纤或者双绞线是否存在单通链路。当 ULFD 检测到单通链路时，它负责关闭物理的和逻辑的单向连接，向用户发送告警信息，阻止其他协议的失效。

61.2 ULFD 功能配置

表 61-1 ULFD 功能配置列表

配置任务	
配置 ULFD 基本功能	使能全局 ULFD 功能
	使能以太接口 ULFD 功能
配置 ULFD 参数	配置 ULFD 检测报文发送周期
	重置被 ULFD 关闭的以太接口

61.2.1 配置 ULFD 基本功能

-B -S -E -A

配置条件

在配置 ULFD 基本功能前，首先完成以下任务：

- 保证 ULFD 检测端口物理连接正常。

使能全局 ULFD 功能

ULFD 具有两种工作模式，即普通 (normal) 模式和加强 (aggressive) 模式。这两种模式判断链路单通的依据有所不同。普通模式常被用于检查由于交叉连接引起的单通。加强模式用于检查交叉连接或者断路造成的单通连接。

表 61-2 使能全局 ULFD 功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
使能全局 ULFD 功能	ulfd { aggressive enable }	必选 缺省情况下，未使能全局 ULFD 功能

使能以太网接口 ULFD 功能

ULFD 检测需要同时使能全局 ULFD 检测功能和以太网接口 ULFD 检测功能。如果全局未使能 ULFD 功能，仅在以太网接口使能 ULFD 功能，ULFD 功能不生效。

如果全局使能的 ULFD 检测模式和以太网接口使能的 ULFD 检测模式不一致，则以以太网接口 ULFD 检测模式优先。

表 61-3 使能以太网接口 ULFD 功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层/三层以太网接口配置模式	interface interface-name	-
使能以太网接口 ULFD 功能	ulfd port [aggressive]	必选 缺省情况下，未使能以太网接口 ULFD 功能

说明:

- 如果在以太网接口上进行 ULFD 工作模式的切换，必须先取消原来的工作模式，再进行新模式的配置。

- 在以太网接口使能 ULFD 功能的时候，应确保邻居以太网接口也配置了 ULFD 功能，且工作在相同的检测模式下。

61.2.2 配置 ULFD 参数 -B -S -E -A

配置条件

在配置 ULFD 参数前，首先完成以下任务：

- 使能 ULFD 功能。

配置 ULFD 检测报文发送周期

ULFD 会周期性地发送检测报文，来探测网络是否存在单向链路，可以根据网络的实际情况来修改检测报文的发送周期。检测报文的发送周期取值范围 7~90 秒，缺省情况下为 15 秒。

表 61-4 配置 ULFD 检测报文发送周期

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 ULFD 报文发送周期	ulfd message time <i>time-value</i>	可选 缺省情况下，单通检测报文的发送周期为 15 秒

重置被 ULFD 关闭的以太网接口

若 ULFD 检测到单通并将该以太网接口关闭，如果要重新使能以太网接口的 ULFD 检测功能，则需要用户手工执行重置操作，该操作会将以太网接口置为 UP 状态，并重新开启 ULFD 检测。

表 61-5 重置被 ULFD 关闭的以太网接口

步骤	命令	说明
重置被 ULFD 关闭的以太网接口	ulfd reset [interface <i>interface-name</i>]	可选 缺省情况下，以太网接口被关闭后不会自动执行重置操作

61.2.3 ULFD 监控与维护 **-B -S -E -A**

表 61-6 ULFD 监控与维护

命令	说明
show ulfd [all interface <i>interface-name</i> [detail]]	显示 ULFD 全局配置信息和全部/指定以太网接口 ULFD 配置信息

61.3 ULFD 典型配置举例

61.3.1 配置 ULFD 基本功能 **-B -S -E -A**

网络需求

- Device1 和 Device2 之间通过光纤连接。
- 配置 ULFD 加强模式以实现检测到单向链路时关闭该端口。

网络拓扑



图 61-3 配置 ULFD 基本功能组网图

配置步骤

步骤 1: 配置 ULFD 功能。

#在 Device1 上使能 ULFD 功能, 并在端口 gigabitethernet0/1 配置 ULFD 工作模式为加强模式。

```
Device1#configure terminal
Device1(config)#ulfd aggressive
Device1(config)#interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#ulfd port aggressive
Device1(config-if-gigabitethernet0/1)#exit
```

#在 Device2 上使能 ULFD 功能, 并在端口 gigabitethernet0/1 配置 ULFD 工作模式为加强模式。

```
Device2#configure terminal
Device2(config)#ulfd aggressive
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#ulfd port aggressive
Device2(config-if-gigabitethernet0/1)#exit
```

#查看 Device1 端口 gigabitethernet0/1 的 ULFD 信息。

```
Device1#show ulfd interface gigabitethernet 0/1
Interface name   : gigabitethernet0/1
ULFD config mode : Aggressive
ULFD running mode : Aggressive
Link status      : Link Up
Link direction   : Bidirectional
ULFD fsm status  : Advertisement

Neighbors number : 1
-----
Device ID        : 00017a787878
Interface name   : gigabitethernet0/1
Device Name      : Device2
Message Interval : 15
Timeout Interval : 5
Link Direction   : Bidirectional
Aging Time       : 40
Time to Die      : 36
-----
```

说明:

- Device2 上查看端口 ULFD 信息的方法与 Device1 的一样。(略)
-

步骤 2: 检验结果。

#在实际的组网环境中, 参照图 2-1 和图 2-2 的所示, 当光纤交叉连接或者其中一条光纤未连接、断路都会导致单向通信, 配置 ULFD 功能后, 在 Device1 上检测到单通时端口 gigabitethernet0/1 将被关闭, 并输出如下日志信息:

```
%ULFD LOG WARN: gigabitethernet0/1: detected Unidirectional neighbor: device
ID[00017a787878], device name[Device2], interface name[gigabitethernet0/1]!
%LINK-INTERFACE_DOWN-3: interface gigabitethernet0/1, changed state to down
%ULFD-UNDIR_LINK_ERR_V3-4: ULFD shutdown interface gigabitethernet0/1 successful
```

#查看端口 gigabitethernet0/1 的状态, 可以看到该端口处于关闭状态。

```
Device1#show interface gigabitethernet 0/1
```

```
gigabitethernet0/1 configuration information
```

```
Description   :
Status        : Enabled
Link          : Down (Err-disabled)
Set Speed     : Auto
Act Speed     : Unknown
Set Duplex    : Auto
Act Duplex    : Unknown
Set Flow Control : Off
Act Flow Control : Off
Mdix          : Normal
Mtu           : 1824
Port mode     : LAN
Port ability  : 100M FD,1000M FD
Link Delay    : No Delay
Storm Control : Unicast Disabled
Storm Control : Broadcast Disabled
Storm Control : Multicast Disabled
Storm Action  : None
Port Type     : Nni
```

Pvid : 1
Set Medium : Fiber
Act Medium : Fiber
Mac Address : 0000.1111.2224

说明：

- 在配置 ULFD 功能的时候，应确保链路两端配置的 ULFD 工作在相同的检测模式下。
 - ULFD 普通工作模式为普通模式时，请参照此配置方法，普通模式只支持检测光纤交叉连接导致单通的情况。
-

62 VRRP

62.1 VRRP 简介

VRRP 全称 Virtual Router Redundancy Protocol（虚拟路由器冗余协议）。简单来说，VRRP 是一种容错协议，它保证当主机的下一跳设备发生故障时，可以及时的由另一台设备来代替，从而保持通讯的连续性和可靠性。为了使 VRRP 工作，首先要创建一个虚拟 IP 地址和 MAC 地址，这样在这个网络中就加入了一个虚拟设备。而这个网络上的主机与虚拟设备通信，无需了解这个网络上物理设备的任何信息。一个虚拟设备由一个主设备（Master）和若干个备份设备（Backup）组成，主设备实现真正的转发功能。当主设备出现故障时，备份设备成为新的主设备，接替它的工作。

下文中所提及的主设备皆以“Master”代替，备份设备皆以“Backup”代替。

62.2 VRRP 功能配置

表 62-1 VRRP 功能配置列表

配置任务	
配置 VRRP 基本功能	使能 VRRP 协议
	配置 VRRP 优先级
	配置 VRRP 抢占模式
	配置 VRRP 实 MAC 地址
配置 VRRP 联动组	配置 VRRP 联动组
配置 VRRP 网络认证	配置 VRRP 简单文本认证

配置任务	
配置 VRRP 与 Track 关联	配置 VRRP 联动 Track 监控 Master 上行线路
	配置 VRRP 联动 Track 监控 Master 和 Backup 互连线路

62.2.1 配置 VRRP 基本功能

-S -E -A

在 VRRP 的各项配置任务中，必须先使能 VRRP 协议，并且 VRRP 组虚拟 IP 地址需要和接口的 IP 地址处于同一网段，配置的其它功能特性才能生效。

配置条件

在配置 VRRP 基本功能之前，首先完成以下任务：

- 配置接口的 IP 地址。

使能 VRRP 协议

启用 VRRP 功能，需要在接口下创建 VRRP 组并配置虚拟 IP 地址。

表 62-2 使能 VRRP 协议

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface interface-name	必选
配置 VRRP 组	vrrp vrid ip ip-address	必选 使能 VRRP 协议。其中 vrid 为 VRRP 组号，ip-address 为虚拟 IP 地址

配置 VRRP 优先级

配置 VRRP 后，如果不设定优先级，其缺省优先级是 100；优先级高的设备会选举成为负责转发报文的 Master，其他的成为 Backup；如果所有设备的优先级相等，则根据各设备的接口 IP 地址大小进行选举，接口 IP 地址大的成为 Master；可以根据需要自行设置 VRRP 的优先级，其数值越大优先级越高。

表 62-3 配置 VRRP 优先级

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	必选
配置 VRRP 组的优先级	vrrp vrid priority <i>priority</i>	必选 配置 VRRP 的优先级，缺省优先级为 100

说明：

- 在虚 MAC 模式下，当接口 IP 地址与虚拟 IP 地址相同时，立即成为 Init 状态，优先级保持不变。如果用户确实需要配置虚 IP 地址和接口 IP 地址相同，则需将虚 MAC 模式改变成实 MAC 模式。

配置 VRRP 抢占模式

配置 VRRP 后。在抢占模式下，VRRP 组内其他设备一旦发现自己的优先级比当前 Master 的优先级高，就会成为 Master；在非抢占模式下，只要 Master 没有出现故障，其它设备即使配置更高的优先级，也不会成为 Master。

表 62-4 配置 VRRP 抢占模式

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	必选
配置 VRRP 组为抢占模式	vrrp vrid preempt	必选 缺省启动抢占模式

配置 VRRP 实 MAC 地址

一个 VRRP 组中的虚拟设备拥有一个虚拟 MAC 地址，根据 RFC2338 的规定，虚拟 MAC 地址的格式为：00-00-5E-00-01-{vrid}。当虚拟设备回应 ARP 请求时，回应的是虚拟 MAC 地址，而不是接口的真实 MAC 地址。值得说明的是，在缺省情况下使用的是接口虚拟 MAC 地址。

表 62-5 配置 VRRP 实 MAC 地址

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	必选
配置 VRRP 使用真实 MAC 地址	vrrp vrid use-bia	必选 缺省使用虚拟 MAC 地址

说明：

- 在缺省情况下，VRRP 配置后使用的是虚拟 MAC 地址，当配置本节命令后，则使用实 MAC，即主机发送报文时以实 MAC 地址进行转发；删除本节命令后，则使用虚拟

MAC 地址，即主机发送报文时以虚拟 MAC 地址进行转发

62.2.2 配置 VRRP 联动组 **-S -E -A**

VRRP 联动组可以减少 VRRP 协议报文的交互，减轻网络负荷，并达到毫秒级切换。通过将多个普通 VRRP 组加入到 1 个 VRRP 联动组中，不同 VRRP 组在联动组中担任不同的角色，如 Active 或非 Active，由联动组中的 Active 组发送协议报文，而非 Active 组不发送，非 Active 组状态和 Active 组状态保持一致，即 Active 组状态切换，非 Active 组状态同时也会切换，从而达到减少协议报文交互的目的。并且联动组可以配置 VRRP 报文的发送周期到毫秒级，从而达到快速切换的目的。

配置条件

在配置 VRRP 联动组之前，首先完成以下任务：

- 配置多个 VRRP 组。

配置 VRRP 联动组

配置 VRRP 联动组，首先需要创建 VRRP 联动组，然后再将配置的普通 VRRP 组加入到创建的联动组中，普通 VRRP 组在加入联动组时，可以以 Active 组的形式加入，也可以非 Active 组形式加入，但需要注意，一个联动组必须有一个 Active 组，同时也只能有一个 Active 组。

表 62-6 配置 VRRP 联动组

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置联动组	vrrp linkgroup <i>lgid</i> [interval <i>Interval-time</i>]	必选 Interval-time 缺省值为 1000ms
进入接口模式	interface <i>interface-name</i>	必选

步骤	命令	说明
将 VRRP 普通组以 Active 的方式加入到联动组中	vrrp vrid linkgroup lgid [active]	必选 如果不选择[active]则是以非 Active 的方式加入

说明：

- 除使用联动组实现负载均衡外，使用多个 VRRP 组也可以实现负载均衡，详细情况参见“VRRP 典型配置举例”中的“配置 VRRP 负载均衡”章节。
- 在联动组中，当 VRRP 普通组加入后，其普通组定时器会失效，即普通组 VRRP 报文发送周期会以联动组的定时器为准。

62.2.3 配置 VRRP 网络认证

-S -E -A

VRRP 支持简单文本认证，文本认证设置长度不超过 8 位的认证字。

配置条件

在配置 VRRP 网络认证前，首先完成以下任务：

- 配置一个 VRRP 组。

配置 VRRP 简单文本认证

表 62-7 配置 VRRP 简单文本认证

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface interface-name	必选

步骤	命令	说明
配置 VRRP 简单文本认证	vrrp vrid authentication text string	必选 缺省情况下，不启动简单文本认证功能 认证密码最长 8 个字符

62.2.4 配置 VRRP 与 Track 联动 -S -E -A

VRRP 可以对上行线路和 Master、Backup 互联线路进行线路状态的监控，以提高 VRRP 的可靠性。

配置条件

在配置 VRRP 与 Track 联动之前，首先完成以下任务：

- 配置了一个 VRRP 组。

配置 VRRP 联动 Track 监控 Master 上行线路

在 Master 上配置和 Track 联动，可以通过 Track 关联接口，或关联 BFD、RTR 等使之关注上行接口的状态，如果上行接口 down 后，VRRP 可以通过配置的消费值降低 Master 的优先级，此时，当 Backup 收到后会自动切换为 Master（值得注意的是，此时 Master 的优先级比 Backup 的优先级低），如果需要进行 Backup 的快速切换，可以在 Backup 上配置收低优先级快速切换命令。具体见下图。

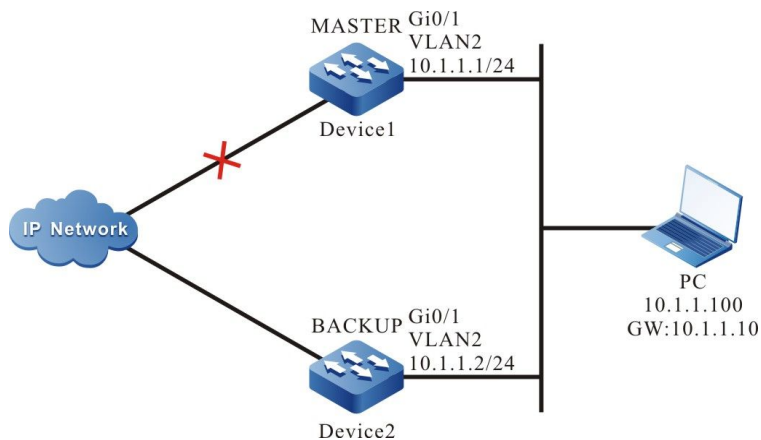


图 62-1 配置 VRRP 联动 Track 监控 Master 上行线路

配置 VRRP 联动 Track 关联上行接口

将 VRRP 和所要关心的上行接口通过 Track 关联，当上行接口 down 时，Master 会自动降低自身优先级，此时 Backup 会收到低优先级的 VRRP 报文而切换为 Master；如果用户配置了“收到低优先级报文快速切换”即 low-pri-master 功能时，backup 会快速切换为 Master。

表 62-8 配置 VRRP 联动 Track 关联上行接口（Master 上配置）

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口模式	interface <i>interface-name</i>	必选
配置 VRRP 关联上联接口	vrrp vrid track <i>interface-name</i> [<i>decrement</i>]	必选 缺省优先级消耗值为 10
配置 VRRP 收到低优先级报文快速切换功能	vrrp vrid switchover low-pri-master	可选 该命令在 backup 上进行配置，以实现当 master 降低优先级时进行快速切换

配置 VRRP 联动 Track (Track 关联 BFD、RTR 等)

如果 Track 关联 BFD、RTR 等，Master 可以直接关联该 Track，以达到监控线路的目的。当线路出现故障时，Master 则降低自身优先级，此时 Backup 收到低优先级的 VRRP 报文后切换为 Master。如果用户配置了“接收低优先级报文快速切换”即 low-pri-master 功能时，backup 会快速切换为 Master。

表 62-9 配置 Master 与 Track 联动（Track 关联 BFD、RTR 等）

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口模式	interface <i>interface-name</i>	必选
配置 VRRP 关联上联接口	vrrp vrid track track-id [<i>decrement</i>]	必选 缺省优先级消耗值为 10
配置 VRRP 收到低优先级报文快速切换功能	vrrp vrid switchover low-pri-master	可选 该命令在 backup 上进行配置，以实现当 Master 降低优先级时进行快速切换

说明：

- 关于 Track 创建、Track 关联 BFD 或 RTR 等配置方法见 Track 配置手册。
- low-pri-master 功能能使 Backup 在收到低优先级报文时，即使为不抢占模式，也会进行快速切换，如果没有配置该功能，则在收到低优先级报文时，Backup 会在下一个超时时间后进行切换。在对切换时间要求不严格的情况下，不需要配置 low-pri-master 功能，但在对切换时间要求严格的情况下，该功能能使切换时间达到毫秒级。

配置 VRRP 联动 Track 监控 Master、Backup 互连线路

通过配置 VRRP 联动 Track 监控 Master、Backup 互连线路，如果 Master、Backup 间线路 down 时，Backup 快速切换为 Master。具体见下图。

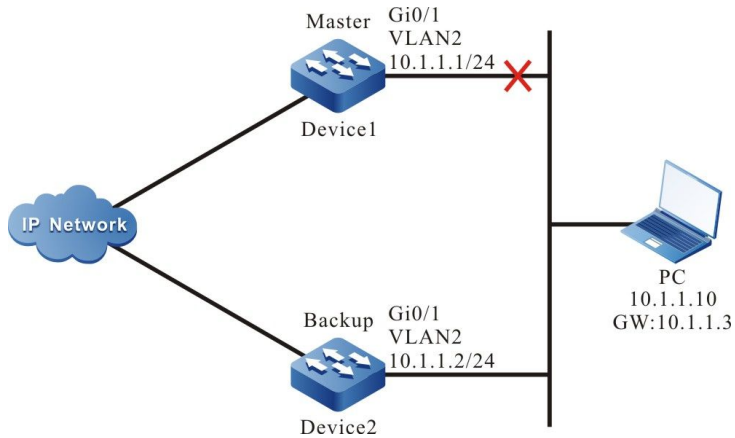


图 62-2 配置 VRRP 联动 Track 监控 Master、Backup 互连线路

表 62-10 配置 VRRP 联动 Track 监控 Master、Backup 互连线路

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口模式	interface interface-name	必选
配置 Backup VRRP 设备检测 Master、Backup 间线路 down 时快速切换功能	vrrp vrid track track-id switchover	必选

说明：

- 相关 Track 关联 BFD、RTR 配置参见 Track 配置手册。
- Track 可关联 BFD，以达到监控 Master、Backup 互联线路状态的目的。

62.2.5 VRRP 监控与维护

-S -E -A

表 62-11 VRRP 监控与维护

命令	说明
<code>show vrrp [brief] [interface interface-name] [group [linkgroup-number]]</code>	显示 VRRP 配置信息，其中包括虚拟 IP 地址信息、虚拟 MAC 地址信息、设备状态、设备优先级、依赖的设备接口地址、联动组信息等

62.3 VRRP 典型配置举例

62.3.1 配置 VRRP 单备份组

-S -E -A

网络需求

- Device1 和 Device2 上创建单 VRRP 备份组，使 Device1 和 Device2 共用一个虚拟 IP 地址，实现对用户主机缺省网关的备份，以此减少网络中断的时间。

网络拓扑

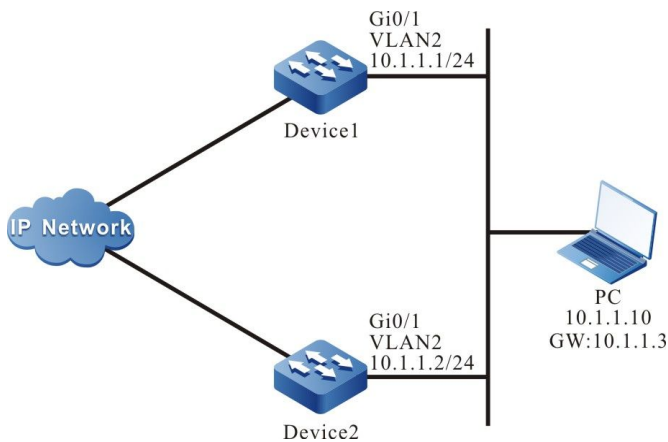


图 62-3 配置 VRRP 单备份组组网图

配置步骤

步骤 1： 配置 VLAN，并将端口加入对应的 VLAN。（略）

步骤 2: 配置各接口的 IP 地址。(略)

步骤 3: 创建 VRRP 组。

#Device1 上配置 VRRP 组 1, 虚拟 IP 地址为 10.1.1.3, 并配置优先级为 110。

```
Device1#configure terminal
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#vrrp 1 ip 10.1.1.3
Device1(config-if-vlan2)#vrrp 1 priority 110
Device1(config-if-vlan2)#exit
```

#Device2 上配置 VRRP 组 1, 虚拟 IP 地址为 10.1.1.3。

```
Device2#configure terminal
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#vrrp 1 ip 10.1.1.3
Device2(config-if-vlan2)#exit
```

步骤 4: 检验结果。

#查看 Device1 的 VRRP 状态。

```
Device1#show vrrp
Interface vlan2 (Flags 0x1)
Pri-addr : 10.1.1.1
Vrf : 0
Virtual router : 1
Virtual IP address : 10.1.1.3
Virtual MAC address : 00-00-5e-00-01-01 , installed into HW
Depend prefix:10.1.1.1/24
State : Master
Normal priority : 110
Currnet priority : 110
Priority reduced : 0
Preempt-mode : YES
Advertise-interval : 1
Authentication Mode : None
```

#查看 Device2 的 VRRP 状态。

```
Device2#show vrrp
Interface vlan2 (Flags 0x1)
Pri-addr : 10.1.1.2
Vrf : 0
Virtual router : 1
Virtual IP address : 10.1.1.3
Virtual MAC address : 00-00-5e-00-01-01
Depend prefix:10.1.1.2/24
State : Backup
Master addr : 10.1.1.1
Normal priority : 100
Currnet priority : 100
Priority reduced : 0
Preempt-mode : YES
Advertise-interval : 1
Authentication Mode : None
```

可以看到，Device1 的 VRRP 状态为 Master，Device2 的 VRRP 状态为 Backup。Device1 和 Device2 共用一个虚拟 IP 地址，主机通过该地址来与网络进行通信。当 Device1 故障后，Device2 立刻切换为 Master，进行数据转发。

说明：

- VRRP 状态的选取原则是先根据优先级，优先级大的为 Master，优先级相同的情况下，则根据接口的 IP 地址进行比较，IP 地址大的为 Master。
- VRRP 缺省工作在抢占模式，缺省优先级为 100。

62.3.2 配置 VRRP 联动组 *-S -E -A*

网络需求

- 在 Device1 和 Device2 接口上启用 VRRP，并加入联动组，仅由联动组中的 Active 组交互协议报文。
- 非 Active 组的 VRRP 状态与 Active 组的 VRRP 状态保持一致，Active 组状态发生切换时，非 Active 组一并切换。

网络拓扑

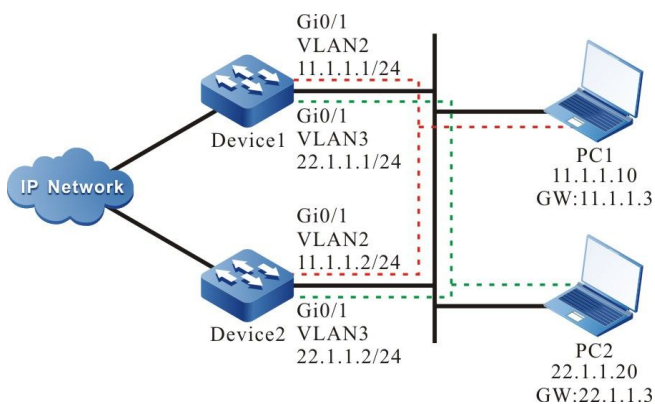


图 62-4 VRRP 多备份组组网图

配置步骤

步骤 1: 配置 VLAN, 并将端口加入对应的 VLAN。 (略)

步骤 2: 配置各接口的 IP 地址。 (略)

步骤 3: 创建 VRRP 联动组。

#Device1 上配置 VRRP 联动组 1。

```
Device1#configure terminal
Device1(config)#vrrp linkgroup 1
```

#Device2 上配置 VRRP 联动组 1。

```
Device2#configure terminal
Device2(config)#vrrp linkgroup 1
```

步骤 4: 创建 VRRP 组。

#Device1 接口上配置 VRRP 组 1 的虚拟 IP 地址为 11.1.1.3。

```
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#vrrp 1 ip 11.1.1.3
Device1(config-if-vlan2)#exit
```

#Device1 接口上配置 VRRP 组 2 的虚拟 IP 地址为 22.1.1.3。

```
Device1(config)#interface vlan 3
Device1(config-if-vlan3)#vrrp 2 ip 22.1.1.3
Device1(config-if-vlan3)#exit
```

#Device2 接口上配置 VRRP 组 1 的虚拟 IP 地址为 11.1.1.3。

```
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#vrrp 1 ip 11.1.1.3
Device2(config-if-vlan2)#exit
```

#Device2 接口上配置 VRRP 组 2 的虚拟 IP 地址为 22.1.1.3。

```
Device2(config)#interface vlan 3
Device2(config-if-vlan3)#vrrp 2 ip 22.1.1.3
Device2(config-if-vlan3)#exit
```

步骤 5: 配置 VRRP 加入联动组。

#Device1 上 VRRP 组 1 以 Active 方式加入联动组。

```
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#vrrp 1 linkgroup 1 active
```

```
Device1(config-if-vlan2)#exit
```

#Device1 上 VRRP 组 2 以非 Active 方式加入联动组。

```
Device1(config)#interface vlan 3
Device1(config-if-vlan3)#vrrp 2 linkgroup 1
Device1(config-if-vlan3)#exit
```

#Device2 上 VRRP 组 1 以 Active 方式加入联动组。

```
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#vrrp 1 linkgroup 1 active
Device2(config-if-vlan2)#exit
```

#Device2 上 VRRP 组 2 以非 Active 方式加入联动组。

```
Device2(config)#interface vlan 3
Device2(config-if-vlan3)#vrrp 2 linkgroup 1
Device2(config-if-vlan3)#exit
```

步骤 6: 检验结果。

#在 Device1 上查看 VRRP 状态。

```
Device1#show vrrp
Interface vlan2 (Flags 0x1)
  Pri-addr : 11.1.1.1
  Vrf : 0
  Virtual router : 1
  Linkgroup : 1
  Active : TRUE
  Virtual IP address : 11.1.1.3
  Virtual MAC address : 00-00-5e-00-01-01
  Depend prefix:11.1.1.1/24
  State : Backup
  Master addr : 11.1.1.2
  Normal priority : 100
  Currnet priority : 100
  Priority reduced : 0
  Preempt-mode : YES
  Advertise-interval : 1
  Authentication Mode : None

Interface vlan3 (Flags 0x1)
  Pri-addr : 22.1.1.1
  Vrf : 0
  Virtual router : 2
  Linkgroup : 1
  Active : FALSE
  Virtual IP address : 22.1.1.3
  Virtual MAC address : 00-00-5e-00-01-02
  Depend prefix:22.1.1.1/24
  State : Backup
  Master addr : 0.0.0.0
  Normal priority : 100
  Currnet priority : 100
  Priority reduced : 0
  Preempt-mode : YES
  Advertise-interval : 1
  Authentication Mode : None
```

#在 Device2 上查看 VRRP 状态。

```
Device2#show vrrp
Interface vlan2 (Flags 0x1)
  Pri-addr : 11.1.1.2
  Vrf : 0
  Virtual router : 1
  Linkgroup : 1
  Active : TRUE
  Virtual IP address : 11.1.1.3
  Virtual MAC address : 00-00-5e-00-01-01 , installed into HW
  Depend prefix:11.1.1.2/24
  State : Master
  Normal priority : 100
  Currnet priority : 100
  Priority reduced : 0
  Preempt-mode : YES
  Advertise-interval : 1
  Authentication Mode : None

Interface vlan3 (Flags 0x1)
  Pri-addr : 22.1.1.2
  Vrf : 0
  Virtual router : 2
  Linkgroup : 1
  Active : FALSE
  Virtual IP address : 22.1.1.3
  Virtual MAC address : 00-00-5e-00-01-02 , installed into HW
  Depend prefix:22.1.1.2/24
  State : Master
  Normal priority : 100
  Currnet priority : 100
  Priority reduced : 0
  Preempt-mode : YES
  Advertise-interval : 1
  Authentication Mode : None
```

可以看到，非 Active 组与 Active 组的 VRRP 状态是保持一致的。

步骤 7： 配置 Device1 中 VLAN2 接口的优先级为 110，使状态发生切换。

```
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#vrrp 1 priority 110
Device1(config-if-vlan2)#exit
```

#在 Device1 上查看 VRRP 状态。

```
Device1#show vrrp
Interface vlan2 (Flags 0x1)
  Pri-addr : 11.1.1.1
  Vrf : 0
  Virtual router : 1
  Linkgroup : 1
  Active : TRUE
  Virtual IP address : 11.1.1.3
  Virtual MAC address : 00-00-5e-00-01-01 , installed into HW
  Depend prefix:11.1.1.1/24
  State : Master
  Normal priority : 110
  Currnet priority : 110
  Priority reduced : 0
  Preempt-mode : YES
  Advertise-interval : 1
  Authentication Mode : None
```

```
Interface vlan3 (Flags 0x1)
Pri-addr : 22.1.1.1
Vrf : 0
Virtual router : 2
Linkgroup : 1
Active : FALSE
Virtual IP address : 22.1.1.3
Virtual MAC address : 00-00-5e-00-01-02 , installed into HW
Depend prefix:22.1.1/24
State : Master
Normal priority : 100
Currnet priority : 100
Priority reduced : 0
Preempt-mode : YES
Advertise-interval : 1
Authentication Mode : None
```

#在 Device2 上查看 VRRP 状态。

```
Device2#show vrrp
Interface vlan2 (Flags 0x1)
Pri-addr : 11.1.1.2
Vrf : 0
Virtual router : 1
Linkgroup : 1
Active : TRUE
Virtual IP address : 11.1.1.3
Virtual MAC address : 00-00-5e-00-01-01
Depend prefix:11.1.1.2/24
State : Backup
Master addr : 11.1.1.1
Normal priority : 100
Currnet priority : 100
Priority reduced : 0
Preempt-mode : YES
Advertise-interval : 1
Authentication Mode : None

Interface vlan3 (Flags 0x1)
Pri-addr : 22.1.1.2
Vrf : 0
Virtual router : 2
Linkgroup : 1
Active : FALSE
Virtual IP address : 22.1.1.3
Virtual MAC address : 00-00-5e-00-01-02
Depend prefix:22.1.1.2/24
State : Backup
Master addr : 0.0.0.0
Normal priority : 100
Currnet priority : 100
Priority reduced : 0
Preempt-mode : YES
Advertise-interval : 1
Authentication Mode : None
```

可以看到，当 Active 组状态切换时，非 Active 组一并切换，仍与 Active 组保持一致。并由联动组中的 Active 组负责发送协议报文，非 Active 组不发送报文。这样可以大大减少协议报文的交互，以减轻网络的负荷。

说明:

- 联动组的发送间隔粒度可以更小，最小可配置为毫秒级，以达到快速切换。

62.3.3 配置 VRRP 与 Track 联动 -S -E -A

网络需求

- Device1 和 Device2 之间启用 VRRP，Device1 和 Device2 共用一个虚拟 IP 地址，实现对用户主机缺省网关的备份。
- Device1 通过 Track 监控接口 VLAN3 状态。当 Device1 的上联口 VLAN3 为 down 时，VRRP 能感知到并发生状态切换，使得 Backup 将成为新的 Master，进行数据转发。

网络拓扑

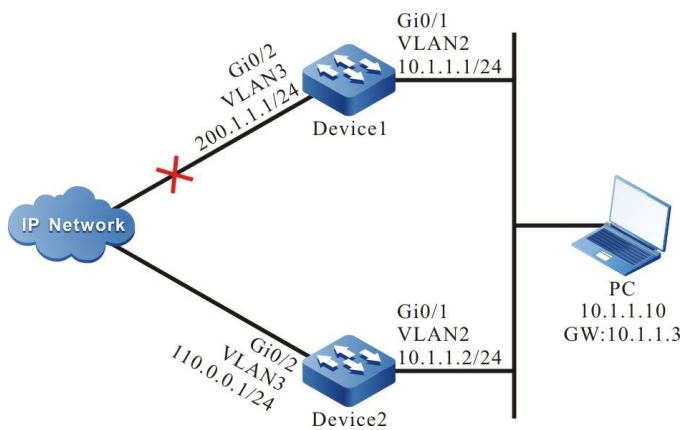


图 62-5 VRRP 与 Track 联动组网图

配置步骤

- 步骤 1: 配置 VLAN，并将端口加入对应的 VLAN。（略）
- 步骤 2: 配置各接口的 IP 地址。（略）
- 步骤 3: 创建 VRRP 组。

可靠性

#Device1 上配置 VRRP 组 1，虚拟 IP 地址为 10.1.1.3，并优先级为 110。

```
Device1#configure terminal
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#vrrp 1 ip 10.1.1.3
Device1(config-if-vlan2)#vrrp 1 priority 110
Device1(config-if-vlan2)#exit
```

#Device2 上配置 VRRP 组 1，虚拟 IP 地址为 10.1.1.3。

```
Device2#configure terminal
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#vrrp 1 ip 10.1.1.3
Device2(config-if-vlan2)#exit
```

#查看 Device1 的 VRRP 状态。

```
Device1#show vrrp
Interface vlan2 (Flags 0x1)
Pri-addr : 10.1.1.1
Vrf : 0
Virtual router : 1
Virtual IP address : 10.1.1.3
Virtual MAC address : 00-00-5e-00-01-01 , installed into HW
Depend prefix:10.1.1.1/24
State : Master
Normal priority : 110
Currnet priority : 110
Priority reduced : 0
Preempt-mode : YES
Advertise-interval : 1
Authentication Mode : None
```

#查看 Device2 的 VRRP 状态。

```
Device2#show vrrp
Interface vlan2 (Flags 0x1)
Pri-addr : 10.1.1.2
Vrf : 0
Virtual router : 1
Virtual IP address : 10.1.1.3
Virtual MAC address : 00-00-5e-00-01-01
Depend prefix:10.1.1.2/24
State : Backup
Master addr : 10.1.1.1
Normal priority : 100
Currnet priority : 100
Priority reduced : 0
Preempt-mode : YES
Advertise-interval : 1
Authentication Mode : None
```

步骤 4： 配置 VRRP 与 Track 联动。

#在 Device1 上配置 VRRP 与 Track 联动，监控上联接口 VLAN3，并配置优先级降低数额为 20。

```
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#vrrp 1 track vlan3 20
Device1(config-if-vlan2)#exit
```

#查看 Device1 的 VRRP 的状态。

```
Device1#show vrrp
Interface vlan2 (Flags 0x1)
Pri-addr : 10.1.1.1
Vrf : 0
Virtual router : 1
Virtual IP address : 10.1.1.3
Virtual MAC address : 00-00-5e-00-01-01 , installed into HW
Depend prefix:10.1.1.1/24
State : Master
Normal priority : 110
Currnet priority : 110
Priority reduced : 0
Preempt-mode : YES
Advertise-interval : 1
Authentication Mode : None
Track interface : vlan3
Reduce : 20
Reduce state : NO
```

当 Device1 的上联口 VLAN3 为 down 时，其 VRRP 优先级降低 20。此时 Device2 的优先级较高，因此要发生状态切换。

#查看 Device1 的 VRRP 状态。

```
Device1#show vrrp
Interface vlan2 (Flags 0x1)
Pri-addr : 10.1.1.1
Vrf : 0
Virtual router : 1
Virtual IP address : 10.1.1.3
Virtual MAC address : 00-00-5e-00-01-01
Depend prefix:10.1.1.1/24
State : Backup
Master addr : 10.1.1.2
Normal priority : 110
Currnet priority : 90
Priority reduced : 20
Preempt-mode : YES
Advertise-interval : 1
Authentication Mode : None
Track interface : vlan3
Reduce : 20
Reduce state : YES
```

#查看 Device2 的 VRRP 状态。

```
Device2#show vrrp
Interface vlan2 (Flags 0x1)
Pri-addr : 10.1.1.2
Vrf : 0
Virtual router : 1
Virtual IP address : 10.1.1.3
Virtual MAC address : 00-00-5e-00-01-01 , installed into HW
Depend prefix:10.1.1.2/24
State : Master
Normal priority : 100
Currnet priority : 100
Priority reduced : 0
Preempt-mode : YES
Advertise-interval : 1
Authentication Mode : None
```

说明:

- VRRP 与 Track 联动如需达到快速切换的目的, 可在 Backup 上配置 switchover low-pri-master。

62.3.4 配置 VRRP 与 BFD 联动

-S -E -A

网络需求

- Device1 和 Device2 间启用 VRRP。
- Device1 与 Device2 的 VRRP 状态切换时间至少需要 3s, 业务中断时间较长。
- 需要在 Device1 与 Device2 上配置 VRRP 与 BFD 联动, 以实现毫秒级的切换。

网络拓扑

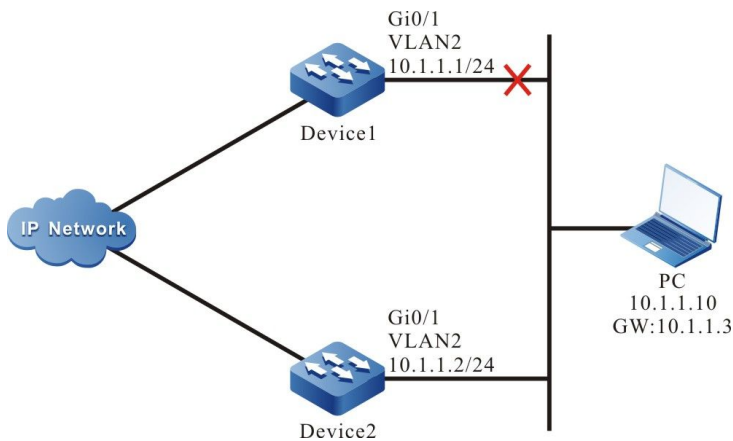


图 62-6 VRRP 与 BFD 联动组网图

配置步骤

- 步骤 1: 配置 VLAN, 并将端口加入对应的 VLAN。 (略)
- 步骤 2: 配置各接口的 IP 地址。 (略)
- 步骤 3: 创建 VRRP 组。

可靠性

#Device1 上配置 VRRP 组 1，虚拟 IP 地址为 10.1.1.3，并配置优先级为 105。

```
Device1#configure terminal
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#vrrp 1 ip 10.1.1.3
Device1(config-if-vlan2)#vrrp 1 priority 105
Device1(config-if-vlan2)#exit
```

#Device2 上配置 VRRP 组 1，虚拟 IP 地址为 10.1.1.3。

```
Device2#configure terminal
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#vrrp 1 ip 10.1.1.3
Device2(config-if-vlan2)#exit
```

#查看 Device1 的 VRRP 状态。

```
Device1#show vrrp
Interface vlan2 (Flags 0x1)
Pri-addr : 10.1.1.2
Vrf : 0
Virtual router : 1
Virtual IP address : 10.1.1.3
Virtual MAC address : 00-00-5e-00-01-01 , installed into HW
Depend prefix:10.1.1.2/24
State : Master
Normal priority : 105
Currnet priority : 105
Priority reduced : 0
Preempt-mode : YES
Advertise-interval : 1
Authentication Mode : None
```

#查看 Device2 的 VRRP 状态。

```
Device2#show vrrp
Interface vlan2 (Flags 0x1)
Pri-addr : 10.1.1.2
Vrf : 0
Virtual router : 1
Virtual IP address : 10.1.1.3
Virtual MAC address : 00-00-5e-00-01-01
Depend prefix:10.1.1.2/24
State : Backup
Master addr : 10.1.1.1
Normal priority : 100
Currnet priority : 100
Priority reduced : 0
Preempt-mode : YES
Advertise-interval : 1
Authentication Mode : None
```

步骤 4： 配置 Track 与 BFD 联动。

#Device1 上配置 Track 与 BFD 联动。

```
Device1(config)#track 1
Device1(config-track)#bfd interface vlan2 remote-ip 10.1.1.2 local-ip 10.1.1.1
Device1(config-track)#exit
```

#Device2 上配置 Track 与 BFD 联动。

```
Device2#configure terminal
Device2(config)#track 1
Device2(config-track)#bfd interface vlan2 remote-ip 10.1.1.1 local-ip 10.1.1.2
Device2(config-track)#exit
```

#在 Device1 上查看 BFD 的状态。

```
Device1#show bfd session
OurAddr      NeighAddr      LD/RD      State      Holddown      interface
10.1.1.1      10.1.1.2      6/7        UP         5000          vlan2
```

#在 Device2 上查看 BFD 的状态。

```
Device2#show bfd session
OurAddr      NeighAddr      LD/RD      State      Holddown      interface
10.1.1.2      10.1.1.1      7/6        UP         5000          vlan2
```

步骤 5: 配置 VRRP 与 Track 联动。

#在 Device2 上配置 VRRP 与 Track 联动, 并配置 switchover。

```
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#vrrp 1 track 1 switchover
Device2(config-track)#exit
```

步骤 6: 检验结果。

#在 Device2 上查看 VRRP 状态。

```
Device2#show vrrp
Interface vlan2 (Flags 0x1)
Pri-addr : 10.1.1.1
Vrf : 0
Virtual router : 1
Virtual IP address : 10.1.1.3
Virtual MAC address : 00-00-5e-00-01-01
Depend prefix:10.1.1.1/24
State : Backup
Master addr : 10.1.1.2
Normal priority : 100
Currnet priority : 100
Priority reduced : 0
Preempt-mode : YES
Advertise-interval : 1
Authentication Mode : None
Track object : 1
Switchover state : NO
```

当 Device1 线路故障时, BFD 会话 down 掉, Track 也会随之 down, Device2 能立即感知并切换为 Master, 进行数据转发。

#在 Device2 上查看 BFD 和 VRRP 状态。

```
Device2#show bfd session
OurAddr      NeighAddr      LD/RD      State      Holddown      interface
10.1.1.2     10.1.1.1       7/0        DOWN       5000          vlan2
Device2#show vrrp
Interface vlan2 (Flags 0x1)
Pri-addr : 10.1.1.2
Vrf : 0
Virtual router : 1
Virtual IP address : 10.1.1.3
Virtual MAC address : 00-00-5e-00-01-01 , installed into HW
Depend prefix:10.1.1.2/24
State : Master
Normal priority : 100
Currnet priority : 100
Priority reduced : 0
Preempt-mode : YES
Advertise-interval : 1
Authentication Mode : None
Track object : 1
Switchover state : YES
```

说明：

- VRRP 与 Track 联动时，Switchover 需配置在 Backup 上，一旦检测到 Track down，就立即切为 Master。
-

62.3.5 配置 VRRP 负载均衡

-S -E -A

网络需求

- Device1 与 Device2 同时属于两个 VRRP 组，Device1 在组 1 中为 Master，在组 2 中为 Backup，Device2 在组 1 的为 Backup，在组 2 中为 Master。
- PC1 通过 Device1 进行数据转发，PC2 通过 Device2 进行数据转发，以实现负载均衡。

网络拓扑

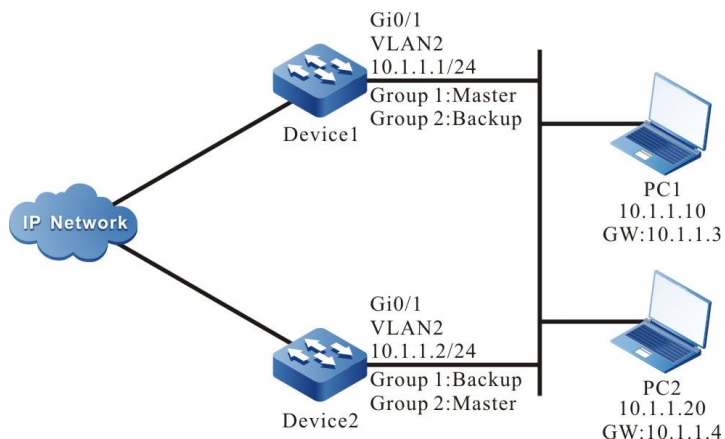


图 62-7 VRRP 负载均衡组网图

配置步骤

步骤 1: 配置 VLAN, 并将端口加入对应的 VLAN。 (略)

步骤 2: 配置各接口的 IP 地址。 (略)

步骤 3: 创建 VRRP 组 1。

#Device1 上配置 VRRP 组 1, 虚拟 IP 地址为 10.1.1.3, 并配置优先级为 110。

```
Device1#configure terminal
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#vrrp 1 ip 10.1.1.3
Device1(config-if-vlan2)#vrrp 1 priority 110
Device1(config-if-vlan2)#exit
```

#Device2 上配置 VRRP 组 1, 虚拟 IP 地址为 10.1.1.3。

```
Device2#configure terminal
Device2(config)#interface vlan 2
Device2(config-if-vlan2)#vrrp 1 ip 10.1.1.3
Device2(config-if-vlan2)#exit
```

步骤 4: 创建 VRRP 组 2。

#Device1 上配置 VRRP 组 2 的虚拟 IP 地址为 10.1.1.4。

```
Device1(config)#interface vlan 2
Device1(config-if-vlan2)#vrrp 2 ip 10.1.1.4
Device1(config-if-vlan2)#exit
```

#Device2 上配置 VRRP 组 2 的虚拟 IP 地址为 10.1.1.4, 并配置优先级为 110。

```
Device2(config)#interface vlan 2
```

```
Device2(config-if-vlan2)#vrrp 2 ip 10.1.1.4
Device2(config-if-vlan2)#vrrp 2 priority 110
Device2(config-if-vlan2)#exit
```

步骤 5: 检验结果。

#在 Device1 上查看 VRRP 的在组 1 和组 2 中的状态。

```
Device1#show vrrp
Interface vlan2 (Flags 0x1)
Pri-addr : 10.1.1.1
Vrf : 0
Virtual router : 1
Virtual IP address : 10.1.1.3
Virtual MAC address : 00-00-5e-00-01-01 , installed into HW
Depend prefix:10.1.1.1/24
State : Master
Normal priority : 110
Currnet priority : 110
Priority reduced : 0
Preempt-mode : YES
Advertise-interval : 1
Authentication Mode : None

Virtual router : 2
Virtual IP address : 10.1.1.4
Virtual MAC address : 00-00-5e-00-01-02
Depend prefix:10.1.1.1/24
State : Backup
Master addr : 10.1.1.2
Normal priority : 100
Currnet priority : 100
Priority reduced : 0
Preempt-mode : YES
Advertise-interval : 1
Authentication Mode : None
```

#在 Device2 上查看 VRRP 在组 1 和组 2 中的状态。

```
Device2#show vrrp
Interface vlan2 (Flags 0x1)
Pri-addr : 10.1.1.2
Vrf : 0
Virtual router : 1
Virtual IP address : 10.1.1.3
Virtual MAC address : 00-00-5e-00-01-01
Depend prefix:10.1.1.2/24
State : Backup
Master addr : 10.1.1.1
Normal priority : 100
Currnet priority : 100
Priority reduced : 0
Preempt-mode : YES
Advertise-interval : 1
Authentication Mode : None

Virtual router : 2
Virtual IP address : 10.1.1.4
Virtual MAC address : 00-00-5e-00-01-02 , installed into HW
Depend prefix:10.1.1.2/24
State : Master
Normal priority : 110
```



```
Currnet priority : 110  
Priority reduced : 0  
Preempt-mode : YES  
Advertise-interval : 1  
Authentication Mode : None
```

可以看到，Device1 作为 VRRP 组 1 的 Master，同时兼职为 VRRP 组 2 的 Backup。与 Device1 相反，Device2 作为 VRRP 组 2 的 Master，作为 VRRP 组 1 的 Backup。当某台设备故障时，两台 PC 均通过另一台设备进行数据转发。这样，不但起到了负载均衡的作用，同时也达到了相互备份的目的。

63 VRRPv3

63.1 VRRPv3 简介

VRRPv3 全称 Virtual Router Redundancy Protocol Version 3（虚拟路由器冗余协议版本 3）。简单来说，VRRPv3 是一种容错协议，它保证当主机的下一跳设备发生故障时，可以及时的由另一台设备来代替，从而保持通讯的连续性和可靠性。为了使 VRRPv3 工作，首先要创建一个虚拟 IP 地址和 MAC 地址，这样在这个网络中就加入了一个虚拟设备。而这个网络上的主机与虚拟设备通信，无需了解这个网络上物理设备的任何信息。一个虚拟设备由一个主设备（Master）和若干个备份设备（Backup）组成，主设备实现真正的转发功能。当主设备出现故障时，备份设备成为新的主设备，接替它的工作。

下文中所提及的主设备皆以“Master”代替，备份设备皆以“Backup”代替。

63.2 VRRPv3 功能配置

表 63-1 VRRPv3 功能配置列表

配置任务	
配置 VRRPv3 基本功能	使能 VRRPv3 协议
	配置 VRRPv3 优先级
	配置 VRRPv3 抢占模式
	配置 VRRPv3 虚拟 MAC 地址
配置 VRRPv3 与 Track 关联	配置 VRRPv3 联动 Track 监控 Master 上行线路

配置任务

配置 VRRPv3 联动 Track 监控 Master 和 Backup 互连线路

63.2.1 配置 VRRPv3 基本功能

-E -A

在 VRRPv3 的各项配置任务中，必须先使能 VRRPv3 协议，并且 VRRPv3 组虚拟 IPv6 link-local 地址需要在接口的 IPv6 link-local 地址使能后，配置的其它功能特性才能生效。

配置条件

在配置 VRRPv3 基本功能之前，首先完成以下任务：

- 使能接口的 IPv6 link-local 地址。

使能 VRRPv3 协议

启用 VRRPv3 功能，需要在接口下创建 VRRPv3 组并配置 IPv6 link-local 虚地址。如果需要配置全球虚地址，则该虚地址的网段必须和接口上的全球实地址的网段相同。

表 63-2 使能 VRRPv3 协议

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface interface-name	必选
配置 VRRPv3 组的 link-local 虚地址	ipv6 vrrp vrid ip ip-address link-local	必选 缺省情况下，不启用 VRRPv3
配置 VRRPv3 组的全球虚地址	ipv6 vrrp vrid ip ip-address	可选

步骤	命令	说明
		所配置的全局虚地址必须和接口上全球实地址在同一网段 缺省情况下，不启用全球虚地址

配置 VRRPv3 优先级

配置 VRRPv3 后，如果不设定优先级，其缺省优先级是 100；优先级高的设备会选举成为负责转发报文的 Master，其他的成为 Backup；如果所有设备的优先级相等，则根据各设备的接口 IPv6 link-local 地址大小进行选举，接口 IPv6 link-local 地址大的成为 Master；可以根据需要自行设置 VRRPv3 的优先级，其数值越大优先级越高。

表 63-3 配置 VRRPv3 优先级

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	必选
配置 VRRPv3 组的优先级	ipv6 vrrp vrid priority <i>priority</i>	必选 缺省情况下，VRRPv3 缺省优先级为 100

配置 VRRPv3 抢占模式

配置 VRRPv3 后。在抢占模式下，VRRPv3 组内其他设备一旦发现自己的优先级比当前 Master 的优先级高，就会成为 Master；在非抢占模式下，只要 Master 没有出现故障，其它设备即使配置更高的优先级，也不会成为 Master。

表 63-4 配置 VRRPv3 抢占模式

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface interface-name	必选
配置 VRRPv3 组为抢占模式	ipv6 vrrp vrid preempt	必选 缺省情况下，启用抢占功能

配置 VRRPv3 实 MAC 地址

一个 VRRPv3 组中的虚拟路由器拥有一个虚拟 MAC 地址，根据 RFC5798 的规定，虚拟 MAC 地址的格式为：00-00-5E-00-02-{vrid}。值得说明的是，在缺省情况下使用的是虚 MAC 地址。

表 63-5 配置 VRRPv3 实 MAC 地址

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface interface-name	必选
配置 VRRPv3 使用虚 MAC 地址	ipv6 vrrp vrid use-bia	必选 缺省情况下，VRRPv3 将使用虚 MAC 地址

说明：

- 在缺省情况下，VRRPv3 配置后使用的是虚 MAC 地址，当配置本节命令后，则使用实 MAC，即主机发送报文时以实 MAC 地址进行转发；删除本节命令后，则使用虚 MAC 地址，即主机发送报文时以虚 MAC 地址进行转发。

63.2.2 配置 VRRPv3 与 Track 联动

-E -A

VRRPv3 可以对上行线路和 Master、Backup 互联线路进行线路状态的监控，以提高 VRRPv3 的可靠性。

配置条件

在配置 VRRPv3 与 Track 联动之前，首先完成以下任务：

- 配置了一个 VRRPv3 组。

配置 VRRPv3 联动 Track 监控 Master 上行线路

在 Master 上配置和 Track 联动，可以通过 Track 关联接口，或关联 BFD、RTR 等使之关注上行接口的状态，如果上行接口 down 后，VRRPv3 可以通过配置的消费值降低 Master 的优先级，此时，当 Backup 收到后会自动切换为 Master（值得注意的是，此时 Master 的优先级比 Backup 的优先级低），如果需要进行 Backup 的快速切换，可以在 Backup 上配置收低优先级快速切换命令。具体见下图。

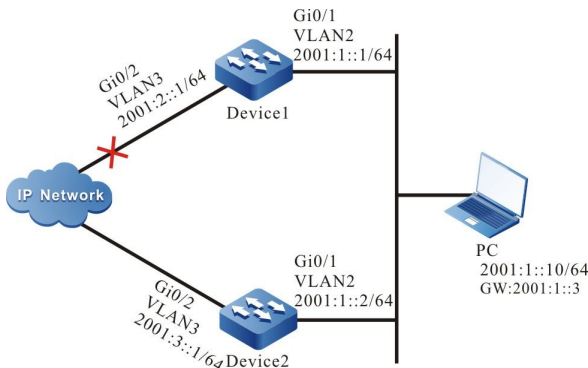


图 63-1 配置 VRRPv3 联动 Track 监控 Master 上行线路

配置 VRRPv3 联动 Track 关联上行接口

将 VRRPv3 和所要关心的上行接口通过 Track 关联，当上行接口 down 时，Master 会自动降低自身优先级，此时 Backup 会收到低优先级的 VRRPv3 报文而切换为 Master；如果用户配置了“收到低优先级报文快速切换”即 low-pri-master 功能时，backup 会快速切换为 Master。

表 63-6 配置 VRRPv3 联动 Track 关联上行接口（Master 上配置）

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口模式	interface <i>interface-name</i>	必选
配置 VRRPv3 关联上联接口	ipv6 vrrp vrid track <i>interface-name</i> [<i>decrement</i>]	必选 缺省情况下，VRRPv3 未与 Track 联动
配置 VRRPv3 收到低优先级报文快速切换功能	ipv6 vrrp vrid switchover low-pri-master	可选 缺省情况下，没有启用 low-pri-master 功能 该命令在 backup 上进行配置，以实现当 master 降低优先级时进行快速切换

配置 VRRPv3 联动 Track (Track 关联 BFD、RTR 等)

如果 Track 关联 BFD、RTR 等，Master 可以直接关联该 Track，以达到监控线路的目的。当线路出现故障时，Master 则降低自身优先级，此时 Backup 收到低优先级的 VRRPv3 报文后切换为 Master。如果用户配置了“接收低优先级报文快速切换”即 low-pri-master 功能时，backup 会快速切换为 Master。

表 63-7 配置 Master 与 Track 联动 (Track 关联 BFD、RTR 等)

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口模式	interface <i>interface-name</i>	必选
配置 VRRPv3 关联上联接口	ipv6 vrrp vrid track track-id [<i>decrement</i>]	必选 缺省情况下, VRRPv3 未与 Track 联动
配置 VRRPv3 收到低优先级报文快速切换功能	ipv6 vrrp vrid switchover low-pri-master	可选 缺省情况下, 没有启用 low-pri-master 功能 该命令在 backup 上进行配置, 以实现当 Master 降低优先级时进行快速切换

说明:

- 关于 Track 创建、Track 关联 BFD 或 RTR 等配置方法见 Track 配置手册。
- low-pri-master 功能能使 Backup 在收到低优先级报文时, 即使为不抢占模式, 也会进行快速切换, 如果没有配置该功能, 则在收到低优先级报文时, Backup 会在下一个超时时间后进行切换。在对切换时间要求不严格的情况下, 不需要配置 low-pri-master 功能, 但在对切换时间要求严格的情况下, 该功能能使切换时间达到毫秒级。

配置 VRRPv3 联动 Track 监控 Master、Backup 互连线路

通过配置 VRRPv3 联动 Track 监控 Master、Backup 互连线路, 如果 Master、Backup 间线路 down 时, Backup 快速切换为 Master。具体见下图。

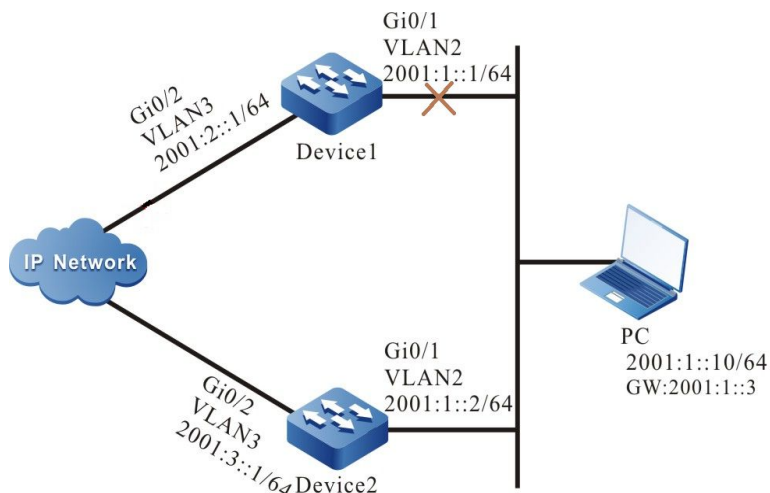


图 63-2 配置 VRRPv3 联动 Track 监控 Master、Backup 互连线路

表 63-8 配置 VRRPv3 联动 Track 监控 Master、Backup 互连线路

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口模式	interface interface-name	必选
配置 Backup VRRPv3 设备检测 Master、Backup 间线路 down 时快速切换功能	ipv6 vrrp vrid track track-id switchover	必选 缺省情况下，VRRPv3 未与 Track 联动

说明：

- 相关 Track 关联 BFD、RTR 配置参见 Track 配置手册。
- Track 可关联 BFD，以达到监控 Master、Backup 互连线路状态的目的。

63.2.3 VRRPv3 监控与维护

-E -A

表 63-9 VRRPv3 监控与维护

命令	说明
<code>show ipv6 vrrp [interface interface-name] [brief]</code>	显示 VRRPv3 配置信息，其中包括虚拟 IP 地址信息、虚拟 MAC 地址信息、设备状态、设备优先级、依赖的设备接口地址等

63.3 VRRPv3 典型配置举例

63.3.1 配置基于 IPv6 的 VRRP 单备份组 -E -A

网络需求

- Device1 和 Device2 上创建基于 IPv6 的 VRRP 单备份组，使 Device1 和 Device2 共用相同的虚拟 IPv6 link-local 地址和 global 地址，实现对用户主机缺省网关的备份，以此减少网络中断的时间。

网络拓扑

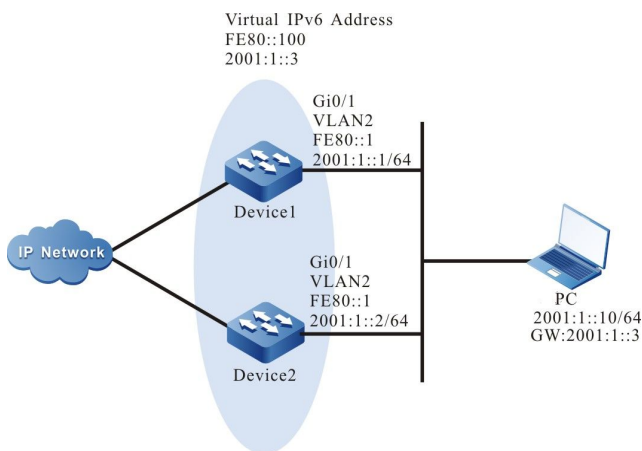


图 63-3 配置基于 IPv6 的 VRRP 单备份组组网图

配置步骤

- 步骤 1: 配置 VLAN，并将端口加入对应的 VLAN。（略）
- 步骤 2: 配置各接口的 IPv6 地址，同时开启 RA 响应和 RA 周期发送的开关。

```
Device1#configure terminal
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 address fe80::1 link-local
Device1(config-if-vlan2)#ipv6 address 2001:1::1/64
Device1(config-if-vlan2)#no ipv6 nd suppress-ra period
Device1(config-if-vlan2)#no ipv6 nd suppress-ra response
Device1(config-if-vlan2)#exit
Device2#configure terminal
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ipv6 address fe80::2 link-local
Device2(config-if-vlan2)#ipv6 address 2001:1::2/64
Device2(config-if-vlan2)#no ipv6 nd suppress-ra period
Device2(config-if-vlan2)#no ipv6 nd suppress-ra response
Device2(config-if-vlan2)#exit
```

步骤 3: 创建基于 IPv6 的 VRRP 组。

#Device1 上配置 VRRP 组 1, 虚拟 IP 地址为 2001:1::3 和 fe80::100, 并配置优先级为 110。

```
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 vrrp 1 ip fe80::100 link-local
Device1(config-if-vlan2)#ipv6 vrrp 1 ip 2001:1::3
Device1(config-if-vlan2)#ipv6 vrrp 1 priority 110
Device1(config-if-vlan2)#exit
```

#Device2 上配置 VRRP 组 1, 虚拟 IP 地址为 2001:1::3 和 fe80::100。

```
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ipv6 vrrp 1 ip fe80::100 link-local
Device2(config-if-vlan2)#ipv6 vrrp 1 ip 2001:1::3
Device2(config-if-vlan2)#exit
```

步骤 4: 检验结果。

#查看 Device1 的 IPv6 VRRP 状态。

```
Device1#show ipv6 vrrp
Interface vlan2 (Flags 0x9)
  Pri-addr : fe80::1
  Vrf : 0
  Pri-matchaddr : fe80::1
  Virtual router : 1
  Mac mode: real mac mode
  Virtual IP address : fe80::100
  Global address count:1
    Global Match address : 2001:1::1
    Global Virtual IP address : 2001:1::3
  Virtual MAC address : 00-00-5e-00-02-01
  State : Master
  Normal priority : 110
  Current priority : 110
  Priority reduced : 0
  Preempt-mode : YES
  Advertise-interval : 100
  Authentication Mode : None
```

#查看 Device2 的 IPv6 VRRP 状态。

```
Device2#show ipv6 vrrp
```

```
Interface vlan2 (Flags 0x9)
Pri-addr : fe80::2
Vrf : 0
Pri-matchaddr : fe80::2
Virtual router : 1
Mac mode: real mac mode
Virtual IP address : fe80::100
Global address count:1
  Global Match address : 2001:1::2
  Global Virtual IP address : 2001:1::3
Virtual MAC address : 00-00-5e-00-02-01
State : Backup
Master addr : fe80::1
Normal priority : 100
Currnet priority : 100
Priority reduced : 0
Preempt-mode : YES
Advertise-interval : 100
Authentication Mode : None
```

可以看到，Device1 的 VRRP 状态为 Master，Device2 的 VRRP 状态为 Backup。Device1 和 Device2 共用一个虚拟 IP 地址，主机通过该地址来与网络进行通信。当 Device1 故障后，Device2 立刻切换为 Master，进行数据转发。

说明：

- VRRPV3 缺省工作在抢占模式，缺省优先级为 100。
- VRRPV3 状态的选取原则是先根据优先级，优先级大的抢占成为 Master，优先级相同的情况下，则根据接口的 IP link-local 地址进行比较，IP 地址大的抢占成为 Master。

63.3.2 配置基于 IPv6 的 VRRP 与 Track 联动 **-E -A**

网络需求

- Device1 和 Device2 上创建基于 IPv6 的 VRRP 单备份组，使 Device1 和 Device2 共用相同的虚拟 IPv6 link-local 地址和 global 地址，实现对用户主机缺省网关的备份，以此减少网络中断的时间。
- Device1 通过 Track 监控接口 VLAN3 状态。当 Device1 的上联口 VLAN3 为 down 时，VRRP 能感知到监控接口 down 事件并降低自身优先级，使得 Backup 抢占成为新的 Master，继续进行数据转发。

网络拓扑

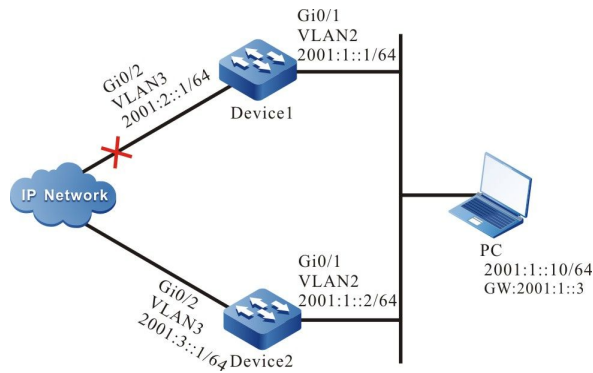


图 63-4 配置基于 IPv6 的 VRRP 与 Track 联动组网图

配置步骤

步骤 1： 配置 VLAN，并将端口加入对应的 VLAN。（略）

步骤 2： 配置各接口的 IPv6 地址，同时开启 RA 响应和 RA 周期发送的开关。

```
Device1#configure terminal
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 address fe80::1 link-local
Device1(config-if-vlan2)#ipv6 address 2001:1::1/64
Device1(config-if-vlan2)#no ipv6 nd suppress-ra period
Device1(config-if-vlan2)#no ipv6 nd suppress-ra response
Device1(config-if-vlan2)#exit
Device2#configure terminal
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ipv6 address fe80::2 link-local
Device2(config-if-vlan2)#ipv6 address 2001:1::2/64
Device2(config-if-vlan2)#no ipv6 nd suppress-ra period
Device2(config-if-vlan2)#no ipv6 nd suppress-ra response
Device2(config-if-vlan2)#exit
```

步骤 3： 创建基于 IPv6 的 VRRP 组。

#Device1 上配置 VRRP 组 1，虚拟 IP 地址为 2001:1::3 和 fe80::100，并配置优先级为 110。

```
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 vrrp 1 ip fe80::100 link-local
Device1(config-if-vlan2)#ipv6 vrrp 1 ip 2001:1::3
Device1(config-if-vlan2)#ipv6 vrrp 1 priority 110
Device1(config-if-vlan2)#exit
```

#Device2 上配置 VRRP 组 1，虚拟 IP 地址为 2001:1::3 和 fe80::100。

```
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ipv6 vrrp 1 ip fe80::100 link-local
Device2(config-if-vlan2)#ipv6 vrrp 1 ip 2001:1::3
Device2(config-if-vlan2)#exit
```

#查看 Device1 的 IPv6 VRRP 状态。

```
Device1# show ipv6 vrrp
Interface vlan2 (Flags 0x9)
Pri-addr : fe80::1
Vrf : 0
Pri-matchaddr : fe80::1
Virtual router : 1
Mac mode: real mac mode
Virtual IP address : fe80::100
Global address count:1
  Global Match address : 2001:1::1
  Global Virtual IP address : 2001:1::3
Virtual MAC address : 00-00-5e-00-02-01
State : Master
Normal priority : 110
Currnet priority : 110
Priority reduced : 0
Preempt-mode : YES
Advertise-interval : 100
Authentication Mode : None
```

#查看 Device2 的 IPv6 VRRP 状态。

```
Device2#show ipv6 vrrp
Interface vlan2 (Flags 0x9)
Pri-addr : fe80::2
Vrf : 0
Pri-matchaddr : fe80::2
Virtual router : 1
Mac mode: real mac mode
Virtual IP address : fe80::100
Global address count:1
  Global Match address : 2001:1::2
  Global Virtual IP address : 2001:1::3
Virtual MAC address : 00-00-5e-00-02-01
State : Backup
Master addr : fe80::1
Normal priority : 100
Currnet priority : 100
Priority reduced : 0
Preempt-mode : YES
Advertise-interval : 100
Authentication Mode : None
```

步骤 4: 配置 VRRP 与 Track 联动。

#在 Device1 上配置 VRRPV3 与 Track 联动, 监控上联接口 VLAN3, 并配置优先级降低值为 20。

```
Device1#configure terminal
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 vrrp 1 track vlan3 20
Device1(config-if-vlan2)#exit
```

#查看 Device1 的 IPv6 VRRP 状态。

```
Device1#show ipv6 vrrp
Interface vlan2 (Flags 0x9)
Pri-addr : fe80::1
Vrf : 0
Pri-matchaddr : fe80::1
Virtual router : 1
Mac mode: real mac mode
Virtual IP address : fe80::100
Global address count:1
  Global Match address : 2001:1::1
  Global Virtual IP address : 2001:1::3
```

```
Virtual MAC address : 00-00-5e-00-02-01
State : Master
Normal priority : 110
Currnet priority : 110
Priority reduced : 0
Preempt-mode : YES
Advertise-interval : 100
Authentication Mode : None
Track interface : vlan3
Reduce : 20
Reduce state : NO
```

步骤 5: 检验结果。

当 Device1 的监控接口 VLAN3 变为 down 时，其 VRRP 优先级降低 20。此时 Device2 的优先级较高，抢占成为 Master，状态发生切换。

#查看 Device1 的 IPv6 VRRP 的状态。

```
Device1#show ipv6 vrrp
Interface vlan2 (Flags 0x9)
Pri-addr : fe80::1
Vrf : 0
Pri-matchaddr : fe80::1
Virtual router : 1
Mac mode: real mac mode
Virtual IP address : fe80::100
Global address count:1
  Global Match address : 2001:1::1
  Global Virtual IP address : 2001:1::3
Virtual MAC address : 00-00-5e-00-02-01
State : Backup
Master addr : fe80::2
Normal priority : 110
Currnet priority : 90
Priority reduced : 20
Preempt-mode : YES
Advertise-interval : 100
Authentication Mode : None
Track interface : vlan3
Reduce : 20
Reduce state : YES
```

#查看 Device2 的 IPv6 VRRP 的状态。

```
Device2#show ipv6 vrrp
Interface vlan2 (Flags 0x9)
Pri-addr : fe80::2
Vrf : 0
Pri-matchaddr : fe80::2
Virtual router : 1
Mac mode: real mac mode
Virtual IP address : fe80::100
Global address count:1
  Global Match address : 2001:1::2
  Global Virtual IP address : 2001:1::3
Virtual MAC address : 00-00-5e-00-02-01
State : Master
Normal priority : 100
Currnet priority : 100
Priority reduced : 0
Preempt-mode : YES
Advertise-interval : 100
Authentication Mode : None
```

63.3.3 配置基于 IPv6 的 VRRP 负载均衡 -E -A

网络需求

- Device1 和 Device2 上创建基于 IPv6 的 VRRP 两个备份组，Device1 与 Device2 同时属于两个 VRRP 组，Device1 在组 1 中为 Master，在组 2 中为 Backup，Device2 在组 1 的为 Backup，在组 2 中为 Master。
- PC1 通过 Device1 进行数据转发，PC2 通过 Device2 进行数据转发，以实现负载均衡。

网络拓扑

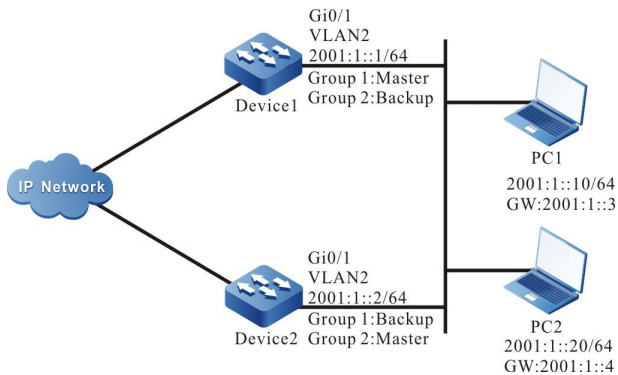


图 63-5 配置基于 IPv6 的 VRRP 负载均衡组网图

配置步骤

- 步骤 1: 配置 VLAN，并将端口加入对应的 VLAN。（略）
- 步骤 2: 配置各接口的 IPv6 地址，同时开启 RA 响应和 RA 周期发送的开关。

```

Device1#configure terminal
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 address fe80::1 link-local
Device1(config-if-vlan2)#ipv6 address 2001:1::1/64
Device1(config-if-vlan2)#no ipv6 nd suppress-ra period
Device1(config-if-vlan2)#no ipv6 nd suppress-ra response
Device1(config-if-vlan2)#exit
Device2#configure terminal
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ipv6 address fe80::2 link-local
Device2(config-if-vlan2)#ipv6 address 2001:1::2/64
Device2(config-if-vlan2)#no ipv6 nd suppress-ra period
Device2(config-if-vlan2)#no ipv6 nd suppress-ra respons
Device2(config-if-vlan2)#exit

```


步骤 3: 创建基于 IPv6 的 VRRP 组 1。

#Device1 上配置 VRRP 组 1, 虚拟 IP 地址为 2001:1::3 和 fe80::100, 并配置优先级为 110。

```
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 vrrp 1 ip fe80::100 link-local
Device1(config-if-vlan2)#ipv6 vrrp 1 ip 2001:1::3
Device1(config-if-vlan2)#ipv6 vrrp 1 priority 110
Device1(config-if-vlan2)#exit
```

#Device2 上配置 VRRP 组 1, 虚拟 IP 地址为 2001:1::3 和 fe80::100。

```
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ipv6 vrrp 1 ip fe80::100 link-local
Device2(config-if-vlan2)#ipv6 vrrp 1 ip 2001:1::3
Device2(config-if-vlan2)#exit
```

步骤 4: 创建基于 IPv6 的 VRRP 组 2。

#Device1 上配置 VRRP 组 2, 虚拟 IP 地址为 2001:1::4 和 fe80::200。

```
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ipv6 vrrp 2 ip fe80::200 link-local
Device1(config-if-vlan2)#ipv6 vrrp 2 ip 2001:1::4
Device1(config-if-vlan2)#exit
```

#Device2 上配置 VRRP 组 2, 虚拟 IP 地址为 2001:1::4 和 fe80::200, 并配置优先级为 110。

```
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ipv6 vrrp 2 ip fe80::200 link-local
Device2(config-if-vlan2)#ipv6 vrrp 2 ip 2001:1::4
Device2(config-if-vlan2)#ipv6 vrrp 2 priority 110
Device2(config-if-vlan2)#exit
```

步骤 5: 检验结果。

#在 Device1 上分别查看 IPv6 VRRP 在组 1 和组 2 状态。

```
Device1#show ipv6 vrrp
Interface vlan2 (Flags 0x9)
  Pri-addr : fe80::1
  Vrf : 0
  Pri-matchaddr : fe80::1
  Virtual router : 1
  Mac mode: real mac mode
  Virtual IP address : fe80::100
  Global address count:1
    Global Match address : 2001:1::1
    Global Virtual IP address : 2001:1::3
  Virtual MAC address : 00-00-5e-00-02-01
  State : Master
  Normal priority : 110
  Currnet priority : 110
  Priority reduced : 0
  Preempt-mode : YES
  Advertise-interval : 100
  Authentication Mode : None

  Pri-matchaddr : fe80::1
  Virtual router : 2
```

```
Mac mode: real mac mode
Virtual IP address : fe80::200
Global address count:1
  Global Match address : 2001:1::1
  Global Virtual IP address : 2001:1::4
Virtual MAC address : 00-00-5e-00-02-02
State : Backup
Master addr : fe80::2
Normal priority : 100
Currnet priority : 100
Priority reduced : 0
Preempt-mode : YES
Advertise-interval : 100
Authentication Mode : None
```

#在 Device2 上分别查看 IPv6 VRRP 在组 1 和组 2 状态。

```
Device2#show ipv6 vrrp
Interface vlan2 (Flags 0x9)
Pri-addr : fe80::2
Vrf : 0
Pri-matchaddr : fe80::2
Virtual router : 1
  Mac mode: real mac mode
  Virtual IP address : fe80::100
  Global address count:1
    Global Match address : 2001:1::2
    Global Virtual IP address : 2001:1::3
  Virtual MAC address : 00-00-5e-00-02-01
  State : Backup
  Master addr : fe80::1
  Normal priority : 100
  Currnet priority : 100
  Priority reduced : 0
  Preempt-mode : YES
  Advertise-interval : 100
  Authentication Mode : None

Pri-matchaddr : fe80::2
Virtual router : 2
  Mac mode: real mac mode
  Virtual IP address : fe80::200
  Global address count:1
    Global Match address : 2001:1::2
    Global Virtual IP address : 2001:1::4
  Virtual MAC address : 00-00-5e-00-02-02
  State : Master
  Normal priority : 110
  Currnet priority : 110
  Priority reduced : 0
  Preempt-mode : YES
  Advertise-interval : 100
  Authentication Mode : None
```

可以看到，Device1 作为 VRRP 组 1 的 Master，同时成为 VRRP 组 2 的 Backup，而 Device2 作为 VRRP 组 2 的 Master，作为 VRRP 组 1 的 Backup。当某台设备故障时，两台 PC 均通过另一台设备进行数据转发。这样，不但起到了负载均衡的作用，同时也达到了相互备份的目的。

64 Track

64.1 Track 简介

Track 可用于监控系统运行过程中的一些信息，其它业务模块可通过与 Track 相关联，从而使得业务模块能监控系统运行过程中的变化。业务模块关联 Track 后，当 Track 监控的信息发生变化时，Track 会通知业务模块，业务模块则可根据通知进行相应处理。例如，在实际应用中，VRRP、VBRP 常通过关联 Track 来监控上行接口状态、网络可达性等信息，并根据这些信息调整自己的优先级，达到主备切换的目的。

64.2 Track 功能配置

表 64-1 Track 功能配置列表

配置任务	
配置 Track 组	配置 Track 组
配置监控对象	配置监控接口状态
	配置监控二层以太网接口状态
	配置监控接口直连路由
	配置监控路由可达

配置任务	
	配置监控 RTR 组
	配置监控汇聚组状态
	配置监控 BFD 会话

64.2.1 配置 Track 组 -B -S -E -A

配置条件

无

配置 Track 组

系统可以配置多个 Track 组，每个 Track 组相互独立，一个 Track 组中可以包括多个监控对象。

Track 组具有“与”、“或”两种逻辑：

- 当 Track 组逻辑为“与”时，需 Track 组中所有监控对象都为 up 状态，Track 组状态才为 up 状态；反之，则为 down 状态；
- 当 Track 组逻辑为“或”时，只需 Track 对象中一个监控对象为 up 状态，则 Track 对象状态为 up；反之，则为 down 状态。

表 64-2 配置 Track 组

步骤	命令	说明
进入全局配置模式	configure terminal	-
创建 Track 组	track group-id	必选
配置 Track 组逻辑	logic operator { AND OR }	可选 AND : 逻辑“与” OR : 逻辑“或”

步骤	命令	说明
		缺省情况下, Track 组逻辑为“与”

说明:

- 当业务模块需通过 Track 来监控一些信息时, 除在 Track 组中配置监控对象外, 还需参考各业务模块配置手册, 配置业务模块关联 Track 组命令。

64.2.2 配置监控对象

-B -S -E -A

配置条件

在配置监控对象之前, 首先完成以下任务:

- 配置 Track 组。

配置监控接口状态

Track 组中可配置监控对象为接口状态。当接口网络层协议 up 时, 该监控对象状态为 up; 当接口网络层协议 down 时, 该监控对象状态为 down。

表 64-3 配置监控接口状态

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 Track 配置模式	track group-id	必选
配置监控接口状态	interface interface-name line-protocol	必选

步骤	命令	说明
	interface <i>interface-name</i> line-ipv6-protocol	

配置监控二层以太接口状态

Track 组中可配置监控对象为二层以太接口状态。当二层以太接口 up 时，该监控对象状态为 up；当二层以太接口 down 时，该监控对象状态为 down。

表 64-4 配置监控二层以太接口状态

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 Track 配置模式	track <i>group-id</i>	必选
配置监控二层以太接口状态	switchport <i>interface-name</i>	必选

配置监控接口直连路由

Track 组中可配置监控对象为接口直连路由。当接口存在 IP 地址且状态为 up 时，监控对象状态为 up；当接口不存在 IP 地址或状态为 down 时，监控对象状态为 down。

表 64-5 配置监控接口直连路由

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 Track 配置模式	track <i>group-id</i>	必选

步骤	命令	说明
配置监控接口直连路由	interface <i>interface-name</i> ip-routing interface <i>interface-name</i> ipv6-routing	必选

配置监控路由可达

Track 组中可配置监控对象为路由可达。当存在到所配置网络的路由时，监控对象状态为 up；当不存在到所配置网络的路由时，监控对象状态为 down。

表 64-6 配置监控路由可达

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 Track 配置模式	track <i>group-id</i>	必选
配置监控路由可达	ip-route <i>network mask</i> [vrf <i>vrf-name</i>] [metric <i>metric-value</i>] ipv6-route <i>network mask</i> [vrf <i>vrf-name</i>] [metric <i>metric-value</i>]	必选 当带有 metric 选项时，到网络的路由度量值需小于配置值，监控对象状态才为 up

配置监控 RTR 组

Track 组中可配置监控对象为 RTR 组。当 RTR 组状态为可达时，监控对象状态为 up；当 RTR 组状态不可达时，监控对象状态为 down。RTR(Response Time Reporter，响应时间报告者)是一种网络检测监控工具。Track 通过监控 RTR 组，可以达到间接监控网络通信情况的目的。

表 64-7 配置监控 RTR 组

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 Track 配置模式	track group-id	必选
配置监控 RTR 组	rtr rtr-group-id	必选

说明：

- RTR 组相关配置请参见 SLA 配置手册。

配置监控汇聚组状态

Track 组中可配置监控对象为汇聚组状态。当汇聚组状态为 up 时，监控对象状态为 up；当汇聚组状态为 down 时，监控对象状态为 down。

表 64-8 配置监控汇聚组状态

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 Track 配置模式	track group-id	必选
配置监控 BFD 会话	link-aggregation link-aggregation-id	必选

配置监控 BFD 会话

Track 组中可配置监控对象为 BFD 会话。当 BFD 会话状态 up 时，监控对象状态为 up；当 BFD 会话状态 down 时，监控对象状态为 down。BFD 协议是一套标准化的全网统一的检测机制，用于快速检测、监控网络中路径或者 IP 路由转发的连通状况。通过 Track 监控 BFD 会话，可以达到间接监控网络连通状况的目的。

表 64-9 配置监控 BFD 会话

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 Track 配置模式	track group-id	必选
配置监控 BFD 会话	bfd interface interface-name remote-ip ip-address local-ip ip-address bfd interface interface-name remote-ipv6 ipv6-address local-ipv6 ipv6-address	必选 在配置监控 BFD 会话时，需在 BFD 会话两端都进行配置，否则 BFD 会话不能成功建立

64.2.3 Track 监控与维护

-B -S -E -A

表 64-10 Track 监控与维护

命令	说明
show track object group-id	显示 Track 组信息
show track bfd-session	显示 Track 监控的 BFD 会话信息

65 BFD

65.1 BFD 简介

BFD (Bidirectional Forwarding Detection, 双向转发检测) 协议是一套标准化的全网统一的检测机制, 用于快速检测、监控网络中路径或者 IP 路由转发的连通状况。它提供的是一种通用的、标准化的、介质无关、协议无关的快速故障检测机制, 可以为各上层应用 (如路由协议等) 快速检测两台设备之间的线路故障。

BFD 可以在系统之间任何类型的路径上提供故障检测, BFD 会话基于上层应用的需要而建立。如果多个应用协议对应相同的路径, 则可以使用一个 BFD 会话进行检测。

BFD 协议与上层应用协议的处理流程包括:

- (1) 上层应用协议将邻居信息 (包括对端 IP 地址、本端 IP 地址、接口等) 发送给 BFD 协议。
- (2) BFD 协议查询是否存在对应的会话, 如果不存在就根据接收到的邻居信息创建相应的会话, 接着 BFD 会话发送 BFD 控制报文驱动 BFD 状态机的运行, BFD 控制报文是通过三次握手机制完成相应的会话, 历经 Down (启动) 状态到 Init (初始化) 状态的迁移, Init 状态到 Up (完成) 状态的迁移, 会话建立的过程会进行会话的参数协商, 包括报文发送间隔, 检测间隔等。
- (3) 当会话建立完成后, 通过周期性的发送检测报文进行路径状况的检测, 如果在检测间隔内没有接收到对端设备发送的 BFD 控制报文, BFD 协议就会认为此路径存在故障, 将故障信息通告给上层应用协议。
- (4) 上层应用协议接收到故障报告后, 去使能邻居、删除邻居时通知 BFD 协议删除会话, 如果没有其他上层协议需要检测该会话链路, 则删除对应的会话。

从检测路径的类型来看，分为本端与对端相邻的单跳 IP 路径检测，本端与对端不相邻的多跳 IP 路径检测。目前，OSPF、RIP、EBGP、ISIS、LDP、RSVP-TE、TRACK、静态路由这些协议与 BFD 联动属于单跳 IP 路径检测，IBGP 与 BFD 联动属于多跳 IP 路径检测。

65.2 BFD 功能配置

表 65-1 BFD 功能配置列表

配置任务	
配置 BFD 基本功能	配置 BFD 控制报文的最小发送时间间隔
	配置 BFD 控制报文的最小接收时间间隔
	配置 BFD 会话的检测超时倍数

65.2.1 配置 BFD 基本功能 *-E -A*

配置条件

在配置 BFD 基本功能之前，首先完成以下任务：

- 配置接口的 IP 地址，使各相邻节点网络层可达。
- 配置与 BFD 联动的上层应用。

配置 BFD 控制报文的最小发送时间间隔

表 65-2 配置 BFD 控制报文的最小发送时间间隔

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
进入接口配置模式	interface <i>interface-name</i>	-
配置 BFD 控制报文的最小发送时间间隔	bfd min-transmit-interval <i>value</i>	可选 缺省情况下, BFD 控制报文的最小发送时间间隔是 1000 毫秒

说明:

- 本端 BFD 报文的实际发送时间间隔 = MAX (本端 BFD 控制报文的最小发送时间间隔, 对端 BFD 控制报文的最小接收时间间隔)。
- 接口模式下配置 BFD 控制报文的最小发送时间间隔仅对单跳 IP 会话生效。

配置 BFD 控制报文的最小接收时间间隔

表 65-3 配置 BFD 控制报文的最小接收时间间隔

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置 BFD 控制报文的最小接收时间间隔	bfd min-receive-interval <i>value</i>	可选 缺省情况下, 配置 BFD 控制报文的最小接收时间间隔是 1000 毫秒

说明:

- 对端 BFD 控制报文的实际发送时间间隔 = MAX (对端 BFD 控制报文的的最小发送时间间隔, 本端 BFD 控制报文的的最小接收时间间隔) 。
- 接口模式下配置 BFD 控制报文的的最小接收时间间隔仅对单跳 IP 会话生效。

配置 BFD 会话的检测超时倍数

表 65-4 配置 BFD 会话的检测超时倍数

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface interface-name	-
配置 BFD 会话的检测超时倍数	bfd multiplier value	可选 缺省情况下, BFD 会话的超时检测倍数是 5

说明:

- 为了保证 BFD 会话检测的有效性, 请谨慎配置 BFD 检测超时倍数的最小值。
- 本端 BFD 实际检测时间 = 对端 BFD 会话的检测超时倍数×对端 BFD 报文的实际发送时间间隔。
- 接口模式下配置 BFD 控制报文的检测超时倍数仅对单跳 IP 会话生效。

配置 BFD 会话的快速检测功能

表 65-5 配置 BFD 会话的快速检测功能

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
配置 BFD 会话的快速检测功能	bfd fast-detect	可选 缺省情况下, BFD 会话的快速检测功能是关闭的

65.2.2 BFD 监控与维护

-E -A

表 65-6 BFD 监控与维护

命令	说明
clear bfd drop statistics	清除 BFD 错误报文统计信息
clear bfd error-statistics	清除 BFD 错误统计信息
show bfd	显示设备所支持的 BFD 参数
show bfd client [<i>client-name</i>]	显示 BFD 客户端信息
show bfd discriminator	显示 BFD 鉴别值信息
show bfd drop statistics	显示 BFD 错误报文统计信息
show bfd error-statistics	显示 BFD 错误统计信息
show bfd session [<i>neighbor-ipv4-address</i>] [detail]	显示 BFD IPv4 会话信息
show bfd session ipv6 [<i>neighbor-ipv6-address</i> [<i>interface-name</i>]] [detail]	显示 BFD IPv6 会话信息

65.3 BFD 典型配置举例

65.3.1 配置 BFD 基本功能

-E -A

网络需求

- Device 4 为连接设备，只对数据进行透明传输。
- Device1、Device2、Device3 运行 OSPF 协议，Device1 和 Device3 配置 BFD 检测功能。
- 修改 BFD 参数，当 Device4 与 Device3 之间的线路出现故障时，Device1 和 Device3 之间的业务数据能够实现毫秒级切换。

网络拓扑

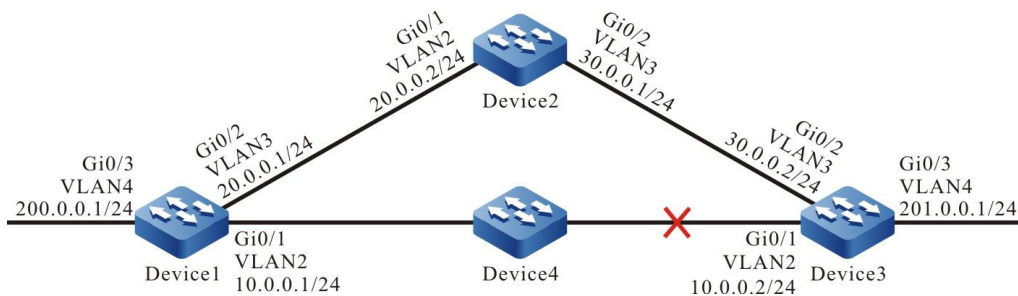


图 65-1 配置 BFD 基本功能组网图

配置步骤

步骤 1：配置 VLAN，并将端口加入对应的 VLAN。（略）

步骤 2：配置各接口 IP 地址。（略）

步骤 3：配置 OSPF。

#配置 Device1。

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#router-id 1.1.1.1
Device1(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
```

```
Device1(config-ospf)#network 20.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 200.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#配置 Device2。

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#router-id 2.2.2.2
Device2(config-ospf)#network 20.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 30.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#配置 Device3。

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#router-id 3.3.3.3
Device3(config-ospf)#network 10.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 30.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 201.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#exit
```

步骤 4： 配置 OSPF 与 BFD 联动。

#配置 Device1。

```
Device1(config)#bfd fast-detect
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ip ospf bfd
Device1(config-if-vlan2)#exit
```

#配置 Device3。

```
Device3(config)#bfd fast-detect
Device3(config)#interface vlan2
Device3(config-if-vlan2)#ip ospf bfd
Device3(config-if-vlan2)#exit
```

#查看 Device1 的 BFD 会话。

```
Device1#show bfd session detail
Total session number: 1
OurAddr          NeighAddr        LD/RD           State           Holddown        interface
```



```
10.0.0.1      10.0.0.2      12/19      UP      5000      vlan2
Type:direct
Local State:UP Remote State:UP Up for: 0h:10m:57s Number of times UP:1
Send Interval:1000ms Detection time:5000ms(1000ms*5)
Local Diag:0 Demand mode:0 Poll bit:0
MinTxInt:1000 MinRxInt:1000 Multiplier:5
Remote MinTxInt:1000 Remote MinRxInt:1000 Remote Multiplier:5
Registered protocols:OSPF
```

可以看到 OSPF 与 BFD 联动成功，会话正常建立，检测超时时间为 5 秒。

#查看 Device1 的路由表。

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS
Gateway of last resort is not set
C 10.0.0.0/24 is directly connected, 00:20:01, vlan2
C 20.0.0.0/24 is directly connected, 00:25:22, vlan3
O 30.0.0.0/24 [110/2] via 20.0.0.2, 00:12:31, vlan3
   [110/2] via 10.0.0.2, 00:11:20, vlan2
C 127.0.0.0/8 is directly connected, 00:31:09, lo0
C 200.0.0.0/24 is directly connected, 00:20:10, vlan4
O 201.0.0.0/24 [110/2] via 10.0.0.2, 00:11:30, vlan2
```

从路由表中可以看到，路由 201.0.0.0/24 优选 Device1 和 Device3 之间的线路进行通信。

步骤 5： 配置 BFD 参数。

#配置 Device1，修改 BFD 控制报文的最小发送时间间隔和最小接收时间间隔为 100 毫秒，检测超时倍数为 3。

```
Device1(config)#interface vlan2
Device1(config-if-vlan2)#bfd min-transmit-interval 100
Device1(config-if-vlan2)#bfd min-receive-interval 100
Device1(config-if-vlan2)#bfd multiplier 3
Device1(config-if-vlan2)#exit
```

#配置 Device3，修改 BFD 控制报文的最小发送时间间隔和最小接收时间间隔为 100 毫秒，检测超时倍数为 3。

```
Device3(config)#interface vlan2
Device3(config-if-vlan2)#bfd min-transmit-interval 100
```

```
Device3(config-if-vlan2)#bfd min-receive-interval 100
Device3(config-if-vlan2)#bfd multiplier 3
```

```
Device3(config-if-vlan2)#exit
```

步骤 6: 检验结果。

#查看 Device1 的 BFD 会话。

```
Device1#show bfd session detail
Total session number: 1
OurAddr      NeighAddr      LD/RD      State      Holddown      interface
10.0.0.1     10.0.0.2      12/19      UP         300           vlan2
Type:direct
Local State:UP Remote State:UP Up for: 0h:11m:27s Number of times UP:1
Send Interval:100ms Detection time:300ms(100ms*3)
Local Diag:0 Demand mode:0 Poll bit:0
MinTxInt:100 MinRxInt:100 Multiplier:3
Remote MinTxInt:100 Remote MinRxInt:100 Remote Multiplier:3
Registered protocols:OSPF
```

修改 BFD 参数后，BFD 检测超时时间从之前的 5 秒协商成了 300 毫秒。

#当 Device1 和 Device3 之间的线路出现故障后，BFD 会快速检测到故障并通知 OSPF，OSPF 将路由切换到 Device2 上进行通信，查看 Device1 的路由表。

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS
Gateway of last resort is not set
C 10.0.0.0/24 is directly connected, 00:25:00, vlan2
C 20.0.0.0/24 is directly connected, 00:30:33, vlan3
O 30.0.0.0/24 [110/2] via 20.0.0.2, 00:17:32, vlan3
C 127.0.0.0/8 is directly connected, 00:36:10, lo0
C 200.0.0.0/24 is directly connected, 00:25:11, vlan4
O 201.0.0.0/24 [110/3] via 20.0.0.2, 00:00:10, vlan3
```

对比步骤 3 的路由表可以看到，路由 201.0.0.0/24 已经切换到 Device2 进行通信。

Device3 上 BFD 处理方式与 Device1 类似。

66 ERPS

66.1 ERPS 简介

在以太二层网络中，对于网络可靠性一般采用 STP 协议（Spanning Tree Protocol，生成树协议），但 STP（Spanning Tree Protocol，生成树协议）一般收敛时间为秒级，网络直径较大时收敛时间更长。为了缩短收敛时间，消除网络尺寸的影响，ERPS（Ethernet Ring Protection Switching，以太环网保护倒换）技术应运而生。ERPS（Ethernet Ring Protection Switching，以太环网保护倒换）是 ITU-T 定义的一种二层破环协议标准，协议标准号为 ITU-T G.8032/Y1344，又称为 G.8032。G.8032 是具备高可靠性和稳定性的以太环网链路层技术。它在以太环网完整时能够防止数据环路硬气的广播风波，而当以太环网链路故障时能迅速恢复环网上各个节点之间的通信道路，具备较高的收敛速度。同时，如果环网内制造商的设备都支持该协议则可以实现互通。

ERPS 相关概念定义：

- ERPS（Ethernet Ring Protection Switching，以太环网保护倒换）环：ERPS 环是 ERPS 协议的基本单位，由一组配置了相同的控制 VLAN（Virtual Local Area Network，虚拟局域网）且互连的网络设备构成。ERPS 环分为主环和子环，主环是封闭的环，子环是非封闭的环。主环和子环的属性由用户确定。
- 端口角色：ERPS 协议中规定的端口角色有 RPL owner 端口、RPL neighbour 端口和普通端口三种类型；其中 RPL neighbor 端口类型只有 ERPSv2 版本支持。
- RPL owner 端口：一个 ERPS 环只有一个 RPL owner 端口，由用户配置指定。ERPS 协议通过阻塞 RPL owner 端口的转发状态来防止链路产生环路。RPL owner 端口所在链路即为环保护链路 RPL（Ring Protection Link，环保护链路）。
- RPL neighbour 端口：RPL neighbor 端口指的是与 RPL owner 端口直接相连的节点端口。正常情况下 RPL owner 端口和 RPL neighbor 端口都会被阻塞，以防止环路产生。当 ERPS 环网出现故障时，RPL owner 端口和 RPL neighbor 端口都会被放开。
- 普通端口：在 ERPS 环中，除 RPL owner 端口和 RPL neighbor 端口以外的端口都

是普通端口。普通端口负责监测自己的直连链路状态，并把链路状态变化及时通知其他节点端口。

- ERPS 控制 VLAN：用来传递 ERPS 协议报文。控制 VLAN 由用户指定，用作 ERPS 控制 VLAN 的 VLAN（Virtual Local Area Network，虚拟局域网）不能给其他业务使用。每个 ERPS 环的控制 VLAN 不同。
- ERPS 数据实例：需要 ERPS 环保护的数据 VLAN 映射的数据实例。

66.2 ERPS 功能配置

表 66-1 ERPS 功能配置列表

配置任务	
配置 ERPS 环	配置 ERPS 环
	使能 ERPS 协议
配置 ERPS 环定时器	配置 ERPS 环定时器
配置 ERPS 网络优化	配置 ERPS 端口阻塞切换方式
	清除 ERPS 配置的阻塞点
	配置 ERPS 拓扑变化通告
	配置 ERPS TC 限制功能
配置 ERPS 与 CFM 联动	配置 ERPS 联动 CFM

66.2.1 配置 ERPS 环

-B -S -E -A

配置 ERPS 环时，需要对各节点上接入 ERPS 环的端口和环上的各节点进行必要的配置。

配置条件

在配置 ERPS 环之前，首先完成以下任务：

- 需要创建控制 VLAN；
- 需要将环端口的环网协议关闭；
- 需要将环端口配置为 trunk 模式；
- 需要将环端口加入环所属的控制 VLAN；
- 需要配置好 MSTP 实例与所要包含 VLAN 之间的映射关系。

配置 ERPS 环

配置 ERPS 环的基本功能

表 66-2 配置 ERPS 环

步骤	命令	说明
进入全局配置模式	configure terminal	-
创建 ERPS 环	erps ring <i>ring-id</i>	必选 缺省情况下，没有创建 ERPS 环，环的取值范围为 1~64
配置 ERPS 环控制 VLAN	control vlan <i>vlan-id</i>	必选 缺省情况下，没有配置 ERPS 环控制 VLAN
配置 ERPS 环数据实例	instance <i>instance-list</i>	必选 缺省情况下，没有配置 ERPS 数据实例

配置 ERPS 环端口 PORT0	port0 { interface <i>interface-name</i> link-aggregation <i>link-aggregation-id</i> } [rpl { owner neighbour }]	必选 缺省情况下, 没有配置 ERPS port0 端口 rpl owner : 表示端口为 RPL 的 owner 端口 rpl neighbour : 表示端口为 RPL 的 neighbour 端口 不配置 rpl 表示端口为普通端口
配置 ERPS 环端口 PORT1	port1 { interface <i>interface-name</i> link-aggregation <i>link-aggregation-id</i> } [rpl { owner neighbour }]	必选 缺省情况下, 没有配置 ERPS port1 端口 rpl owner : 表示端口为 RPL 的 owner 端口 rpl neighbour : 表示端口为 RPL 的 neighbour 端口 不配置 rpl 表示端口为普通端口
配置 ERPS 环版本信息	version { <i>v1</i> / <i>v2</i> }	可选 缺省情况下, 版本为 version v2
配置 ERPS 环报文 mel 值	mel <i>level-id</i>	可选

		缺省情况下，mel 的值为 7，取值范围为 0~7
配置 ERPS 环为子环	sub-ring	可选 缺省情况下，ERPS 环为主环
配置 ERPS 环非回切模式	revertive disable	可选 缺省情况下，ERPS 为回切模式
配置 ERPS 子环虚通道	virtual-channel enable	可选 缺省情况下，ERPS 为非虚通道

说明：

- ERPS 控制 VLAN 只可用于 ERPS 协议报文传输，不可用于其他业务。同一个 ERPS 环中的所有节点需要配置相同的 mel 值
- 相交环组网环境下不推荐使用子环虚通道方式进行组网。

使能 ERPS 协议

在上述配置完成以后，使用本命令启动 ERPS 协议。

表 66-3 ERPS 环上使能协议

步骤	命令	说明
进入全局配置模式	configure terminal	-

进入 ERPS 配置模式	erps ring <i>ring-id</i>	-
使能 ERPS 协议	erps enable	必选 缺省情况下，环没有使能 ERPS 协议

66.2.2 配置 ERPS 环定时器

-B -S -E -A**配置条件**

在配置 ERPS 定时器之前，首先完成以下任务：

- 配置 ERPS 环。

配置 ERPS 环定时器

ERPS 环中节点设备或链路故障恢复后，为了防止出现网络震荡，会启用到 ERPS 环定时器，从而减少业务流量的中断时间。

表 66-4 配置 ERPS 环定时器

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 ERPS 配置模式	erps ring <i>ring-id</i>	-
配置 ERPS 环 Guard 定时器	guard-timer <i>time-value</i>	必选 缺省情况下，Guard 定时器的超时时间为 500 毫秒，Guard 定时器范围为 10 ~ 2000 毫秒

配置 ERPS 环 Hold-off 定时器	holdoff-timer <i>time-value</i>	必选 缺省情况下, hold-off 定时器的超时时间为 0 毫秒, hold-off 定时器范围为 0 ~ 10000 毫秒
配置 ERPS 环 WTR 定时器	wtr-timer <i>time-value</i>	必选 缺省情况下, WTR 定时器的超时时间为 5 分钟, WTR 定时器范围为 1 ~ 12 分钟

66.2.3 配置 ERPS 网络优化

-B -S -E -A

配置条件

在配置 ERPS 网络优化前, 首先完成以下任务:

- 配置 ERPS 环。

配置 ERPS 端口阻塞切换方式

由于 RPL owner 端口所在链路的带宽或许可以承载更多的用户流量, 此时可以考虑将带宽低的链路进行阻塞, 让用户流量回到 RPL 上进行传输。

表 66-5 配置 ERPS 端口阻塞切换方式

步骤	命令	说明
配置 ERPS 端口阻塞切换方式	erps ring <i>ring-id</i> { interface <i>interface-name</i> link-aggregation <i>link-aggregation-id</i> }	必选 缺省情况下, 没有配置 ERPS 环端口的阻塞点切换方式

	switch { force manual }	
--	----------------------------------	--

清除 ERPS 配置的阻塞点

清除 ERPS 环配置的阻塞点切换操作。

表 66-6 清除 ERPS 配置的阻塞点

步骤	命令	说明
清除 ERPS 配置的阻塞点	clear erps ring <i>ring-id</i>	必选

配置 ERPS 拓扑变化通告

当本 ERPS 环的拓扑发生变化，而没有及时通知到上级二层网络，那么上级二层网络的 MAC 地址表中仍然保留下游网络拓扑变化前的 MAC 地址表项，这样会导致用户流量中断。为了保证用户流量正常通信，因此需要根据用户实际网络选择本 ERPS 环的拓扑变化通知对象。

表 66-7 配置 ERPS 环拓扑变化通告

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 ERPS 配置模式	erps ring <i>ring-id</i>	-
配置 ERPS 环拓扑变化通告	tc-notify erps ring <i>ring-list</i>	必选 缺省没有通知 erps 拓扑变化

配置 ERPS TC 限制功能

频繁的拓扑变化通告会导致 CPU 处理能力下降，且 ERPS 环上被频繁刷新 Flush-FDB 报文占用网络带宽，为避免此类情况，需要对拓扑变化通告报文进行抑制。通过配置 ERPS 拓扑变化保护时间间隔和在拓扑变化保护时间间隔内处理拓扑变化报文的最大阈值来抑制拓扑变化通告并避免频繁的删除 MAC 地址表项和 ARP 表项，从而达到保护设备的目的。

表 66-8 配置 ERPS TC 限制功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 ERPS 配置模式	erps ring <i>ring-id</i>	-
配置 ERPS 拓扑变化 TC 限制使能	tc-limit enable	必选 缺省没有使能 TC 限制功能
配置 ERPS 拓扑变化 TC 限制的时间间隔	tc-limit interval <i>interval-value</i>	可选 缺省时间间隔为 2 秒，取值范围为 1~500 秒
配置 ERPS 拓扑变化 TC 限制的阈值	tc-limit threshold <i>threshold-value</i>	可选 缺省值为 3，取值范围为 1~64

66.2.4 配置 ERPS 与 CFM 联动

-B -S -E -A**配置条件**

在配置 ERPS 与 CFM（Connectivity Fault Management, 连通性故障管理）联动前，首先完成以下任务：

- 配置 ERPS 基本功能。
- 配置 CFM 功能

配置 ERPS 与 CFM 联动

在加入 ERPS 环的环端口上配置以太网 CFM 联动功能后，可以加速故障检测，实现拓扑的快速收敛和减少流量的中断时间。

表 66-9 配置 ERPS 与 CFM 联动

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface <i>interface-name</i>	必选其一
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	进入二层以太接口配置模式后，后续配置只在当前端口生效； 进入汇聚组配置模式后，后续配置只在汇聚组生效
配置 ERPS 与 CFM 联动	erps ring <i>ring-id</i> track cfm md <i>md-name</i> ma <i>ma-name</i> mep <i>mep-id</i>	必选 缺省情况下，端口没有和 CFM 联动

	remote-mep <i>rmep-id</i>	
--	----------------------------------	--

66.2.5 ERPS 监控与维护

-B -S -E -A

表 66-10 ERPS 监控与维护

命令	说明
clear erps [ring <i>ring-id</i>] statistics	清除 ERPS 相关统计信息
show erps [ring <i>ring-id</i>] config	显示 ERPS 的配置信息
show erps [ring <i>ring-id</i>] detail	显示 ERPS 的详细信息
show erps [ring <i>ring-id</i>] statistics	显示 ERPS 的统计信息

66.3 ERPS 典型配置举例

66.3.1 配置 ERPS 基本功能

-B -S -E -A

网络需求

- 所有 device 在同一个二层网络内。
- 所有 device 开启 ERPS，通过 ERPS 对网络中链路环路进行断环。

网络拓扑

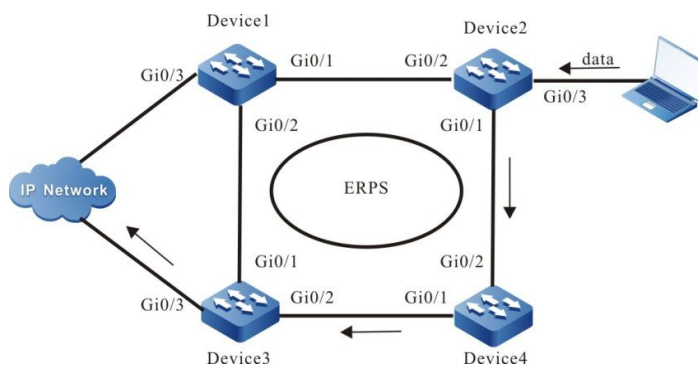


图 66-1 配置 ERPS 基本功能

配置步骤

步骤 1: 配置 vlan 及端口链路类型。

#Device1 创建 VLAN2, VLAN100~VLAN200, 配置端口 gigabitethernet0/1 和 gigabitethernet0/2 的链路类型为 Trunk, 允许 VLAN2, vlan100~VLAN200 业务通过。

```
Device1#configure terminal
Device1(config)#vlan 2,100-200
Device1(config)# interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#shutdown
Device1(config-if-gigabitethernet0/1)# switchport mode trunk
Device1(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device1(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device1(config-if-gigabitethernet0/1)#exit
Device1(config)# interface gigabitethernet 0/2
Device1(config-if-gigabitethernet0/1)# switchport mode trunk
Device1(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device1(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device1(config-if-gigabitethernet0/1)#end
```

#Device2 创建 VLAN2, VLAN100~VLAN200, 配置端口 gigabitethernet0/1 和 gigabitethernet0/2 的链路类型为 Trunk, 允许 VLAN2, vlan100~VLAN200 业务通过。

```
Device1#configure terminal
Device1(config)#vlan 2,100-200
Device1(config)# interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#shutdown
Device1(config-if-gigabitethernet0/1)# switchport mode trunk
```

```
Device1(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device1(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device1(config-if-gigabitethernet0/1)#exit
Device1(config)# interface gigabitethernet 0/2
Device1(config-if-gigabitethernet0/1)# switchport mode trunk
Device1(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device1(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device1(config-if-gigabitethernet0/1)#end
```

#Device3 创建 VLAN2, VLAN100~VLAN200, 配置端口 gigabitethernet0/1 和 gigabitethernet0/2 的链路类型为 Trunk, 允许 VLAN2, vlan100~VLAN200 业务通过。

```
Device1#configure terminal
Device1(config)#vlan 2,100-200
Device1(config)# interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#shutdown
Device1(config-if-gigabitethernet0/1)# switchport mode trunk
Device1(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device1(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device1(config-if-gigabitethernet0/1)#exit
Device1(config)# interface gigabitethernet 0/2
Device1(config-if-gigabitethernet0/1)# switchport mode trunk
Device1(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device1(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device1(config-if-gigabitethernet0/1)#end
```

#Device4 创建 VLAN2, VLAN100~VLAN200, 配置端口 gigabitethernet0/1 和 gigabitethernet0/2 的链路类型为 Trunk, 允许 VLAN2, vlan100~VLAN200 业务通过。

```
Device1#configure terminal
Device1(config)#vlan 2,100-200
Device1(config)# interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#shutdown
Device1(config-if-gigabitethernet0/1)# switchport mode trunk
Device1(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device1(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device1(config-if-gigabitethernet0/1)#exit
Device1(config)# interface gigabitethernet 0/2
Device1(config-if-gigabitethernet0/1)# switchport mode trunk
Device1(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device1(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
```

```
Device1(config-if-gigabitethernet0/1)#end
```

步骤 2: 配置 MST 实例。

#Device1 配置 MST 实例 1 映射 vlan100-200, 并激活实例。

```
Device1#configure terminal
Device1(config)# spanning-tree mst configuration
Device1(config-mst)# instance 1 vlan 100-200
Device1(config-mst)# active configuration pending
Device1(config-mst)#end
```

#Device2 配置 MST 实例 1 映射 vlan100-200, 并激活实例。

```
Device1#configure terminal
Device1(config)# spanning-tree mst configuration
Device1(config-mst)# instance 1 vlan 100-200
Device1(config-mst)# active configuration pending
Device1(config-mst)#end
```

#Device3 配置 MST 实例 1 映射 vlan100-200, 并激活实例。

```
Device1#configure terminal
Device1(config)# spanning-tree mst configuration
Device1(config-mst)# instance 1 vlan 100-200
Device1(config-mst)# active configuration pending
Device1(config-mst)#end
```

#Device4 配置 MST 实例 1 映射 vlan100-200, 并激活实例。

```
Device1#configure terminal
Device1(config)# spanning-tree mst configuration
Device1(config-mst)# instance 1 vlan 100-200
Device1(config-mst)# active configuration pending
Device1(config-mst)#end
```

步骤 3: 配置 ERPS。

#Device1 配置 ERPS ring1, 配置 vlan2 为 ring1 的控制 vlan, 配置 gigabitethernet0/1 为 ring1 的 normal 端口, 配置 gigabitethernet0/2 为 ring1 的 owner 端口, 配置实例 1 为 ring1 的数据 vlan, 并使能 ring1 的 ERPS 功能。

```
Device1# configure terminal
Device1(config)#erps ring 1
```



```
Device1(config-erps1)# control vlan 2
Device1(config-erps1)# port0 interface g0/1
Device1(config-erps1)# port1 interface g0/2 rpl owner
Device1(config-erps1)# instance 1
Device1(config-erps1)# erps enable
Device1(config-erps1)# exit
Device1(config)# interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#no shutdown
Device1(config-if-gigabitethernet0/1)# end
```

Device2 配置 ERPS ring1, 配置 vlan2 为 ring1 的控制 vlan, 配置 gigabitethernet0/1 为 ring1 的 normal 端口, 配置 gigabitethernet0/2 为 ring1 的 normal 端口, 配置实例 1 为 ring1 的数据 vlan, 并使能 ring1 的 ERPS 功能。

```
Device2# configure terminal
Device2(config)#erps ring 1
Device2(config-erps1)# control vlan 2
Device2(config-erps1)# port0 interface g0/1
Device2(config-erps1)# port1 interface g0/2
Device2(config-erps1)# instance 1
Device2(config-erps1)# erps enable
Device2(config-erps1)# exit
Device2(config)# interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#no shutdown
Device2(config-if-gigabitethernet0/1)# end
```

Device3 配置 ERPS ring1, 配置 vlan2 为 ring1 的控制 vlan, 配置 gigabitethernet0/1 为 ring1 的 neighbour 端口, 配置 gigabitethernet0/2 为 ring1 的 normal 端口, 配置实例 1 为 ring1 的数据 vlan, 并使能 ring1 的 ERPS 功能。

```
Device3# configure terminal
Device3(config)#erps ring 1
Device3(config-erps1)# control vlan 2
Device3(config-erps1)# port0 interface g0/1 rpl neighbor
Device3(config-erps1)# port1 interface g0/2
Device3(config-erps1)# instance 1
Device3(config-erps1)# erps enable
Device3(config-erps1)# exit
Device3(config)# interface gigabitethernet 0/1
Device3(config-if-gigabitethernet0/1)#no shutdown
Device3(config-if-gigabitethernet0/1)# end
```

Device4 配置 ERPS ring1, 配置 vlan2 为 ring1 的控制 vlan, 配置 gigabitethernet0/1 为 ring1 的 normal 端口, 配置 gigabitethernet0/2 为 ring1 的 normal 端口, 配置实例 1 为 ring1 的数据 vlan, 并使能 ring1 的 ERPS 功能。

```
Device4# configure terminal
Device4(config)#erps ring 1
Device4(config-erps1)# control vlan 2
Device4(config-erps1)# port0 interface g0/1
Device4(config-erps1)# port1 interface g0/2
Device4(config-erps1)# instance 1
Device4(config-erps1)# erps enable
Device4(config-erps1)# exit
Device4(config)# interface gigabitethernet 0/1
Device4(config-if-gigabitethernet0/1)#no shutdown
Device4(config-if-gigabitethernet0/1)# end
```

步骤 4: 检验结果。

#待网络拓扑稳定后, 查看各 Device 的 ERPS 信息, 以 device1 为例。

#查看 Device1 的 ERPS 信息。

```
Device1# show erps ring 1 detail
Ring ID      : 1
Version      : v2
R-APS mel    : 7
Instance     : 1 vlans mapped : 100-200
Control VLAN : 2
Node role    : Owner
Node state   : idle
Guard timer  : 500 ms      Running : 0 ms
Holdoff timer : 0 ms      Running : 0 ms
WTR timer    : 5 min      Running : 0 s
WTB timer    : 7 s        Running : 0 s
Subring      : No
Tc-limit enable : No
Tc-limit Interval : 2
Tc-limit Threshold : 3
Revertive operation : Revertive
```

R-APS channel : Non-Virtual channel

Enable status : Enable

Gigabitethernet0/1 Flush Logic

Remote Node ID : 0000-0000-0000

Remote BPR : 0

Gigabitethernet0/1 track CFM

MD Name :

MA Name :

MEP ID : 0

RMEP ID : 0

CFM State : 0

Gigabitethernet0/2 Flush Logic

Remote Node ID : 0000-0000-0000

Remote BPR : 0

Gigabitethernet0/2 track CFM

MD Name :

MA Name :

MEP ID : 0

RMEP ID : 0

CFM State : 0

Port	Name	PortRole	SwitchType	PortStatus	SignalStatus
Port0	gigabitethernet0/1	Normal	--	Forwarding	Non-failed
Port1	gigabitethernet0/2	Owner	--	Blocking	Non-failed

说明:

- 配置 ERPS 前, 确保环网中至少一个点的链路状态为 down, 否则会造成环路。
-

66.3.2 配置 ERPS 负载

-B -S -E -A

网络需求

- 所有 device 在同一个二层网络内。
- Data1 的数据流量经过 device2-device1 传输, Data2 的数据流量经过 device4-

device3 传输，实现负载分担并提供链路备份。

网络拓扑

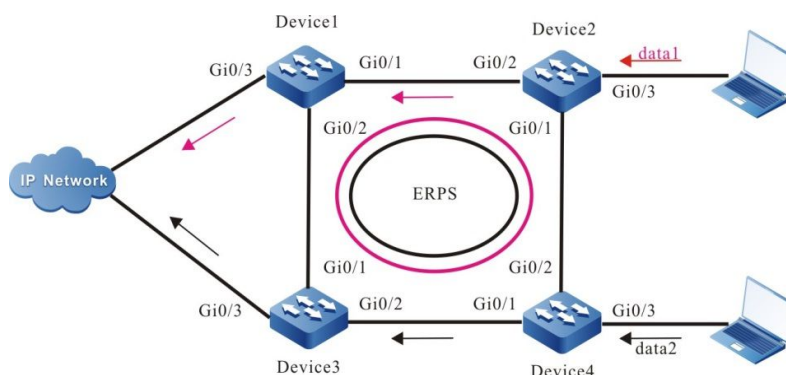


图 66-2 配置 ERPS 负载

配置步骤

步骤 1: 配置 vlan 及端口链路类型。

#Device1 创建 VLAN2~VLAN3, VLAN100~VLAN200, VLAN300~VLAN400, 配置端口 gigabitethernet0/1 和 gigabitethernet0/2 的链路类型为 Trunk, 允许 VLAN2~VLAN3, vlan100~VLAN200, VLAN300~VLAN400 的业务通过。

```
Device1#configure terminal
Device1(config)#vlan 2,100-200
Device1(config)# interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#shutdown
Device1(config-if-gigabitethernet0/1)# switchport mode trunk
Device1(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device1(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device1(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 3,300-400
Device1(config-if-gigabitethernet0/1)#exit
Device1(config)# interface gigabitethernet 0/2
Device1(config-if-gigabitethernet0/1)# switchport mode trunk
Device1(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device1(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device1(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 3,300-400
Device1(config-if-gigabitethernet0/1)#end
```

#Device2 创建 VLAN2~VLAN3, VLAN100~VLAN200, VLAN300~VLAN400, 配置端口 gigabitethernet0/1 和 gigabitethernet0/2 的链路类型为 Trunk, 允许 VLAN2~VLAN3, vlan100~VLAN200, VLAN300~VLAN400 的业务通过。

```
Device2#configure terminal
Device2(config)#vlan 2,100-200
Device2(config)# interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#shutdown
Device2(config-if-gigabitethernet0/1)# switchport mode trunk
Device2(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device2(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device2(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 3,300-400
Device2(config-if-gigabitethernet0/1)#exit
Device2(config)# interface gigabitethernet 0/2
Device2(config-if-gigabitethernet0/1)# switchport mode trunk
Device2(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device2(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device2(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 3,300-400
Device2(config-if-gigabitethernet0/1)#end
```

Device3 创建 VLAN2~VLAN3, VLAN100~VLAN200, VLAN300~VLAN400, 配置端口 gigabitethernet0/1 和 gigabitethernet0/2 的链路类型为 Trunk, 允许 VLAN2~VLAN3, vlan100~VLAN200, VLAN300~VLAN400 的业务通过。

```
Device3#configure terminal
Device3(config)#vlan 2,100-200
Device3(config)# interface gigabitethernet 0/1
Device3(config-if-gigabitethernet0/1)#shutdown
Device3(config-if-gigabitethernet0/1)# switchport mode trunk
Device3(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device3(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device3(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 3,300-400
Device3(config-if-gigabitethernet0/1)#exit
Device3(config)# interface gigabitethernet 0/2
Device3(config-if-gigabitethernet0/1)# switchport mode trunk
Device3(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device3(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device3(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 3,300-400
Device3(config-if-gigabitethernet0/1)#end
```

#Device4 创建 VLAN2~VLAN3, VLAN100~VLAN200, VLAN300~VLAN400, 配置端口 gigabitethernet0/1 和 gigabitethernet0/2 的链路类型为 Trunk, 允许 VLAN2~VLAN3, vlan100~VLAN200, VLAN300~VLAN400 的业务通过。

```
Device4#configure terminal
Device4(config)#vlan 2,100-200
Device4(config)# interface gigabitethernet 0/1
Device4(config-if-gigabitethernet0/1)#shutdown
Device4(config-if-gigabitethernet0/1)# switchport mode trunk
Device4(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device4(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device4(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 3,300-400
Device4(config-if-gigabitethernet0/1)#exit
Device4(config)# interface gigabitethernet 0/2
Device4(config-if-gigabitethernet0/1)# switchport mode trunk
Device4(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device4(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device4(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 3,300-400
Device4(config-if-gigabitethernet0/1)#end
```

步骤 2: 配置 MST 实例。

#Device1 配置 MST 实例 1 映射 vlan100-200, 配置 MST 实例 2 映射 vlan300-400, 并激活实例。

```
Device1#configure terminal
Device1(config)# spanning-tree mst configuration
Device1(config-mst)# instance 1 vlan 100-200
Device1(config-mst)# instance 2 vlan 300-400
Device1(config-mst)# active configuration pending
Device1(config-mst)#end
```

#Device2 配置 MST 实例 1 映射 vlan100-200, 配置 MST 实例 2 映射 vlan300-400, 并激活实例。

```
Device2#configure terminal
Device2(config)# spanning-tree mst configuration
Device2(config-mst)# instance 1 vlan 100-200
Device2(config-mst)# instance 2 vlan 300-400
Device2(config-mst)# active configuration pending
Device2(config-mst)#end
```

#Device3 配置 MST 实例 1 映射 vlan100-200, 配置 MST 实例 2 映射 vlan300-400, 并激活实例。

```
Device3#configure terminal
Device3(config)# spanning-tree mst configuration
Device3(config-mst)# instance 1 vlan 100-200
Device3(config-mst)# instance 2 vlan 300-400
Device3(config-mst)# active configuration pending
Device3(config-mst)#end
```

#Device4 配置 MST 实例 1 映射 vlan100-200，配置 MST 实例 2 映射 vlan300-400，并激活实例。

```
Device4#configure terminal
Device4(config)# spanning-tree mst configuration
Device4(config-mst)# instance 1 vlan 100-200
Device4(config-mst)# instance 2 vlan 300-400
Device4(config-mst)# active configuration pending
Device4(config-mst)#end
```

步骤 3： 配置 ERPS。

#Device1 配置 ERPS ring1，配置 vlan2 为 ring1 的控制 vlan，配置 gigabitethernet0/1 为 ring1 的 normal 端口，配置 gigabitethernet0/2 为 ring1 的 normal 端口，配置实例 1 为 ring1 的数据 vlan，并使能 ring1 的 ERPS 功能。

```
Device1# configure terminal
Device1(config)#erps ring 1
Device1(config-erps1)# control vlan 2
Device1(config-erps1)# port0 interface g0/1
Device1(config-erps1)# port1 interface g0/2
Device1(config-erps1)# instance 1
Device1(config-erps1)# erps enable
Device1(config-erps1)# end
```

#Device1 配置 ERPS ring2，配置 vlan3 为 ring2 的控制 vlan，配置 gigabitethernet0/1 为 ring2 的 normal 端口，配置 gigabitethernet0/2 为 ring2 的 normal 端口，配置实例 2 为 ring2 的数据 vlan，并使能 ring2 的 ERPS 功能。

```
Device1# configure terminal
Device1(config)#erps ring 2
Device1(config-erps1)# control vlan 3
Device1(config-erps1)# port0 interface g0/1
Device1(config-erps1)# port1 interface g0/2
Device1(config-erps1)# instance 2
Device1(config-erps1)# erps enable
```

```
Device1(config-erps1)# exit
Device1(config)# interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#no shutdown
Device1(config-if-gigabitethernet0/1)# end
```

Device2 配置 ERPS ring1, 配置 vlan2 为 ring1 的控制 vlan, 配置 gigabitethernet0/1 为 ring1 的 owner 端口, 配置 gigabitethernet0/2 为 ring1 的 normal 端口, 配置实例 1 为 ring1 的数据 vlan, 并使能 ring1 的 ERPS 功能。

```
Device2# configure terminal
Device2(config)#erps ring 1
Device2(config-erps1)# control vlan 2
Device2(config-erps1)# port0 interface g0/1 rpl owner
Device2(config-erps1)# port1 interface g0/2
Device2(config-erps1)# instance 1
Device2(config-erps1)# erps enable
Device2(config-erps1)# exit
```

Device2 配置 ERPS ring2, 配置 vlan3 为 ring1 的控制 vlan, 配置 gigabitethernet0/1 为 ring2 的 neighbour 端口, 配置 gigabitethernet0/2 为 ring2 的 normal 端口, 配置实例 2 为 ring2 的数据 vlan, 并使能 ring2 的 ERPS 功能。

```
Device2# configure terminal
Device2(config)#erps ring 1
Device2(config-erps1)# control vlan 3
Device2(config-erps1)# port0 interface g0/1 rpl neighbor
Device2(config-erps1)# port1 interface g0/2
Device2(config-erps1)# instance 2
Device2(config-erps1)# erps enable
Device2(config-erps1)# exit
Device2(config)# interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#no shutdown
Device2(config-if-gigabitethernet0/1)# end
```

Device3 配置 ERPS ring1, 配置 vlan2 为 ring1 的控制 vlan, 配置 gigabitethernet0/1 为 ring1 的 normal 端口, 配置 gigabitethernet0/2 为 ring1 的 normal 端口, 配置实例 1 为 ring1 的数据 vlan, 并使能 ring1 的 ERPS 功能。

```
Device3# configure terminal
Device3(config)#erps ring 1
Device3(config-erps1)# control vlan 2
Device3(config-erps1)# port0 interface g0/1 rpl neighbor
```



```
Device3(config-erps1)# port1 interface g0/2
Device3(config-erps1)# instance 1
Device3(config-erps1)# erps enable
Device3(config-erps1)# exit
```

Device3 配置 ERPS ring2，配置 vlan3 为 ring2 的控制 vlan，配置 gigabitethernet0/1 为 ring2 的 normal 端口，配置 gigabitethernet0/2 为 ring2 的 normal 端口，配置实例 2 为 ring2 的数据 vlan，并使能 ring2 的 ERPS 功能。

```
Device3# configure terminal
Device3(config)#erps ring 2
Device3(config-erps1)# control vlan 3
Device3(config-erps1)# port0 interface g0/1
Device3(config-erps1)# port1 interface g0/2
Device3(config-erps1)# instance 2
Device3(config-erps1)# erps enable
Device3(config-erps1)# exit
Device3(config)# interface gigabitethernet 0/1
Device3(config-if-gigabitethernet0/1)#no shutdown
Device3(config-if-gigabitethernet0/1)# end
```

Device4 配置 ERPS ring1，配置 vlan2 为 ring1 的控制 vlan，配置 gigabitethernet0/1 为 ring1 的 normal 端口，配置 gigabitethernet0/2 为 ring1 的 neighbour 端口，配置实例 1 为 ring1 的数据 vlan，并使能 ring1 的 ERPS 功能。

```
Device4# configure terminal
Device4(config)#erps ring 1
Device4(config-erps1)# control vlan 2
Device4(config-erps1)# port0 interface g0/1
Device4(config-erps1)# port1 interface g0/2 rpl neighbour
Device4(config-erps1)# instance 1
Device4(config-erps1)# erps enable
Device4(config-erps1)# exit
```

Device4 配置 ERPS ring2，配置 vlan3 为 ring2 的控制 vlan，配置 gigabitethernet0/1 为 ring2 的 normal 端口，配置 gigabitethernet0/2 为 ring2 的 owner 端口，配置实例 2 为 ring2 的数据 vlan，并使能 ring2 的 ERPS 功能。

```
Device4# configure terminal
Device4(config)#erps ring 2
Device4(config-erps1)# control vlan 3
Device4(config-erps1)# port0 interface g0/1
```

```
Device4(config-erps1)# port1 interface g0/2 rpl owner
Device4(config-erps1)# instance 2
Device4(config-erps1)# erps enable
Device4(config-erps1)# exit
Device4(config)# interface gigabitethernet 0/1
Device4(config-if-gigabitethernet0/1)#no shutdown
Device4(config-if-gigabitethernet0/1)# end
```

步骤 4: 检验结果。

#待网络拓扑稳定后, 查看各 Device 的 ERPS 信息, 以 device2 为例。

#查看 Device2 的 ERPS 信息。

```
Device2# show erps ring 1 detail
Ring ID      : 1
Version      : v2
R-APS mel    : 7
Instance     : 1 vlans mapped : 100-200
Control VLAN : 2
Node role    : Owner
Node state   : idle
Guard timer  : 500 ms      Running : 0 ms
Holdoff timer : 0 ms      Running : 0 ms
WTR timer    : 5 min      Running : 0 s
WTB timer    : 7 s        Running : 0 s
Subring      : No
Tc-limit enable : No
Tc-limit Interval : 2
Tc-limit Threshold : 3
Revertive operation : Revertive
R-APS channel : Non-Virtual channel
Enable status : Enable
Gigabitethernet0/1 Flush Logic
  Remote Node ID : 0000-0000-0000
  Remote BPR     : 0
Gigabitethernet0/1 track CFM
  MD Name       :
  MA Name       :
  MEP ID        : 0
```

```

RMEP ID : 0
CFM State : 0
Gigabitethernet0/2 Flush Logic
Remote Node ID : 0000-0000-0000
Remote BPR : 0
    
```

```

Gigabitethernet0/2 track CFM
MD Name :
MA Name :
MEP ID : 0
RMEP ID : 0
CFM State : 0
    
```

Port	Name	PortRole	SwitchType	PortStatus	SignalStatus
Port0	gigabitethernet0/1	Owner	--	Blocking	Non-failed
Port1	gigabitethernet0/2	Normal	--	Forwarding	Non-failed

```

Device2# show erps ring 2 detail
Ring ID : 2
Version : v2
R-APS mel : 7
Instance : 1 vlans mapped : 100-200
Control VLAN : 3
Node role : Neighbour
Node state : idle
Guard timer : 500 ms Running : 0 ms
Holdoff timer : 0 ms Running : 0 ms
WTR timer : 5 min Running : 0 s
WTB timer : 7 s Running : 0 s
Subring : No
Tc-limit enable : No
Tc-limit Interval : 2
Tc-limit Threshold : 3
Revertive operation : Revertive
R-APS channel : Non-Virtual channel
Enable status : Enable
Gigabitethernet0/1 Flush Logic
Remote Node ID : 0000-0000-0000
Remote BPR : 0
Gigabitethernet0/1 track CFM
    
```

```
MD Name :
MA Name :
MEP ID : 0
RMEP ID : 0
CFM State : 0
Gigabitethernet0/2 Flush Logic
Remote Node ID : 0000-0000-0000
Remote BPR : 0
Gigabitethernet0/2 track CFM
MD Name :
MA Name :
MEP ID : 0
RMEP ID : 0
CFM State : 0
```

Port	Name	PortRole	SwitchType	PortStatus	SignalStatus
Port0	gigabitethernet0/1	Neighbour	--	Blocking	Non-failed
Port1	gigabitethernet0/2	Normal	--	Forwarding	Non-failed

说明:

- 负载时，同一物理环上的多个逻辑环，不能配置相同的数据实例。
-

66.3.3 配置 ERPS 相交环 **-B -S -E -A**

网络需求

- 所有 device 在同一个二层网络内。
- Device1-device2-device4-device3 和 device3-device5-device6-device4 分别形成两个物理环路，所有 device 开启 ERPS，对链路环路进行断环。

网络拓扑

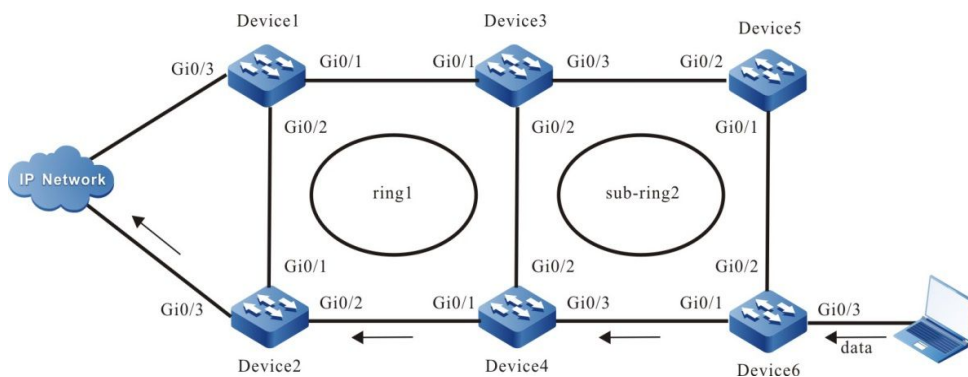


图 66-3 配置 ERPS 相交环

配置步骤

步骤 1: 配置 vlan 及端口链路类型。

#Device1 创建 VLAN2, VLAN100~VLAN200, 配置端口 gigabitethernet0/1 和 gigabitethernet0/2 的链路类型为 Trunk, 允许 VLAN2, vlan100~VLAN200 的业务通过。

```
Device1#configure terminal
Device1(config)#vlan 2,100-200
Device1(config)# interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#shutdown
Device1(config-if-gigabitethernet0/1)# switchport mode trunk
Device1(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device1(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device1(config-if-gigabitethernet0/1)#exit
Device1(config)# interface gigabitethernet 0/2
Device1(config-if-gigabitethernet0/1)# switchport mode trunk
Device1(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device1(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device1(config-if-gigabitethernet0/1)#end
```

#Device2 创建 VLAN2, VLAN100~VLAN200, 配置端口 gigabitethernet0/1 和 gigabitethernet0/2 的链路类型为 Trunk, 允许 VLAN2, vlan100~VLAN200 的业务通过。

```
Device2#configure terminal
Device2(config)#vlan 2,100-200
Device2(config)# interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#shutdown
```

```
Device2(config-if-gigabitethernet0/1)# switchport mode trunk
Device2(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device2(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device2(config-if-gigabitethernet0/1)#exit
Device2(config)# interface gigabitethernet 0/2
Device2(config-if-gigabitethernet0/1)# switchport mode trunk
Device2(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device2(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device2(config-if-gigabitethernet0/1)#end
```

Device3 创建 VLAN2~VLAN3, VLAN100~VLAN200, 配置端口 gigabitethernet0/1 和 gigabitethernet0/2 的链路类型为 Trunk, 允许 VLAN2, vlan100~VLAN200 的业务通过; 配置端口 gigabitethernet0/3 的链路类型为 Trunk, 允许 VLAN3, vlan100~VLAN200 的业务通过。

```
Device3#configure terminal
Device3(config)#vlan 2,100-200
Device3(config)# interface gigabitethernet 0/1
Device3(config-if-gigabitethernet0/1)#shutdown
Device3(config-if-gigabitethernet0/1)# switchport mode trunk
Device3(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device3(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device3(config-if-gigabitethernet0/1)#exit
Device3(config)# interface gigabitethernet 0/2
Device3(config-if-gigabitethernet0/1)# switchport mode trunk
Device3(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device3(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device3(config-if-gigabitethernet0/1)#end
Device3(config)# interface gigabitethernet 0/3
Device3(config-if-gigabitethernet0/1)#shutdown
Device3(config-if-gigabitethernet0/1)# switchport mode trunk
Device3(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device3(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 3,100-200
Device3(config-if-gigabitethernet0/1)#exit
```

Device4 创建 VLAN2~VLAN3, VLAN100~VLAN200, 配置端口 gigabitethernet0/1 和 gigabitethernet0/2 的链路类型为 Trunk, 允许 VLAN2, vlan100~VLAN200 的业务通过; 配置端口 gigabitethernet0/3 的链路类型为 Trunk, 允许 VLAN3, vlan100~VLAN200 的业务通过。

```
Device4#configure terminal
Device4(config)#vlan 2,100-200
```

```
Device4(config)# interface gigabitethernet 0/1
Device4(config-if-gigabitethernet0/1)#shutdown
Device4(config-if-gigabitethernet0/1)# switchport mode trunk
Device4(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device4(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device4(config-if-gigabitethernet0/1)#exit
Device4(config)# interface gigabitethernet 0/2
Device4(config-if-gigabitethernet0/1)# switchport mode trunk
Device4(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device4(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 2,100-200
Device4(config-if-gigabitethernet0/1)#end
Device4(config)# interface gigabitethernet 0/3
Device4(config-if-gigabitethernet0/1)#shutdown
Device4(config-if-gigabitethernet0/1)# switchport mode trunk
Device4(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device4(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 3,100-200
Device4(config-if-gigabitethernet0/1)#exit
```

#Device5 创建 VLAN3, VLAN100~VLAN200, 配置端口 gigabitethernet0/1 和 gigabitethernet0/2 的链路类型为 Trunk, 允许 VLAN3, vlan100~VLAN200 的业务通过。

```
Device5#configure terminal
Device5(config)#vlan 2,100-200
Device5(config)# interface gigabitethernet 0/1
Device5(config-if-gigabitethernet0/1)#shutdown
Device5(config-if-gigabitethernet0/1)# switchport mode trunk
Device5(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device5(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 3,100-200
Device5(config-if-gigabitethernet0/1)#exit
Device5(config)# interface gigabitethernet 0/2
Device5(config-if-gigabitethernet0/1)# switchport mode trunk
Device5(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device5(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 3,100-200
Device5(config-if-gigabitethernet0/1)#end
```

#Device6 创建 VLAN3, VLAN100~VLAN200, 配置端口 gigabitethernet0/1 和 gigabitethernet0/2 的链路类型为 Trunk, 允许 VLAN3, vlan100~VLAN200 的业务通过。

```
Device3#configure terminal
Device3(config)#vlan 3,100-200
Device3(config)# interface gigabitethernet 0/1
```

```
Device3(config-if-gigabitethernet0/1)#shutdown
Device3(config-if-gigabitethernet0/1)# switchport mode trunk
Device3(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device3(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 3,100-200
Device3(config-if-gigabitethernet0/1)#exit
Device3(config)# interface gigabitethernet 0/2
Device3(config-if-gigabitethernet0/1)# switchport mode trunk
Device3(config-if-gigabitethernet0/1)# no switchport trunk allowed vlan all
Device3(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 3,100-200
Device3(config-if-gigabitethernet0/1)#end
```

步骤 2: 配置 MST 实例。

#Device1 配置 MST 实例 1 映射 vlan100-200, 并激活实例。

```
Device1#configure terminal
Device1(config)# spanning-tree mst configuration
Device1(config-mst)# instance 1 vlan 100-200
Device1(config-mst)# active configuration pending
Device1(config-mst)#end
```

#Device2 配置 MST 实例 1 映射 vlan100-200, 并激活实例。

```
Device2#configure terminal
Device2(config)# spanning-tree mst configuration
Device2(config-mst)# instance 1 vlan 100-200
Device2(config-mst)# active configuration pending
Device2(config-mst)#end
```

#Device3 配置 MST 实例 1 映射 vlan100-200, 并激活实例。

```
Device3#configure terminal
Device3(config)# spanning-tree mst configuration
Device3(config-mst)# instance 1 vlan 100-200
Device3(config-mst)# active configuration pending
Device3(config-mst)#end
```

#Device4 配置 MST 实例 1 映射 vlan100-200, 并激活实例。

```
Device4#configure terminal
Device4(config)# spanning-tree mst configuration
Device4(config-mst)# instance 1 vlan 100-200
Device4(config-mst)# active configuration pending
Device4(config-mst)#end
```


#Device5 配置 MST 实例 1 映射 vlan100-200，并激活实例。

```
Device5#configure terminal
Device5(config)# spanning-tree mst configuration
Device5(config-mst)# instance 1 vlan 100-200
Device5(config-mst)# active configuration pending
Device5(config-mst)#end
```

#Device6 配置 MST 实例 1 映射 vlan100-200，并激活实例。

```
Device6#configure terminal
Device6(config)# spanning-tree mst configuration
Device6(config-mst)# instance 1 vlan 100-200
Device6(config-mst)# active configuration pending
Device6(config-mst)#end
```

步骤 3： 配置 ERPS。

#Device1 配置 ERPS ring1，配置 vlan2 为 ring1 的控制 vlan，配置 gigabitethernet0/1 为 ring1 的 normal 端口，配置 gigabitethernet0/2 为 ring1 的 owner 端口，配置实例 1 为 ring1 的数据 vlan，并使能 ring1 的 ERPS 功能。

```
Device1# configure terminal
Device1(config)#erps ring 1
Device1(config-erps1)# control vlan 2
Device1(config-erps1)# port0 interface g0/1
Device1(config-erps1)# port1 interface g0/2 rpl owner
Device1(config-erps1)# instance 1
Device1(config-erps1)# erps enable
Device1(config-erps1)# end
Device1(config)# interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#no shutdown
Device1(config-if-gigabitethernet0/1)# end
```

Device2 配置 ERPS ring1，配置 vlan2 为 ring1 的控制 vlan，配置 gigabitethernet0/1 为 ring1 的 neighbour 端口，配置 gigabitethernet0/2 为 ring1 的 normal 端口，配置实例 1 为 ring1 的数据 vlan，并使能 ring1 的 ERPS 功能。

```
Device2# configure terminal
Device2(config)#erps ring 1
Device2(config-erps1)# control vlan 2
Device2(config-erps1)# port0 interface g0/1 rpl neighbour
```

```
Device2(config-erps1)# port1 interface g0/2
Device2(config-erps1)# instance 1
Device2(config-erps1)# erps enable
Device2(config-erps1)# exit
Device2(config)# interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#no shutdown
Device2(config-if-gigabitethernet0/1)# end
```

Device3 配置 ERPS ring1，配置 vlan2 为 ring1 的控制 vlan，配置 gigabitethernet0/1 为 ring1 的 normal 端口，配置 gigabitethernet0/2 为 ring1 的 normal 端口，配置实例 1 为 ring1 的数据 vlan，并使能 ring1 的 ERPS 功能。

```
Device3# configure terminal
Device3(config)#erps ring 1
Device3(config-erps1)# control vlan 2
Device3(config-erps1)# port0 interface g0/1
Device3(config-erps1)# port1 interface g0/2
Device3(config-erps1)# instance 1
Device3(config-erps1)# erps enable
Device3(config-erps1)# exit
Device2(config)# interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#no shutdown
Device2(config-if-gigabitethernet0/1)# end
```

Device3 配置 ERPS ring2，配置 vlan3 为 ring2 的控制 vlan，配置 gigabitethernet0/3 为 ring2 的 normal 端口，配置实例 1 为 ring2 的数据 vlan，配置 ring2 为 sub-ring 并使能 ring2 的 ERPS 功能。

```
Device3# configure terminal
Device3(config)#erps ring 2
Device3(config-erps1)# control vlan 3
Device3(config-erps1)# port0 interface g0/3
Device3(config-erps1)# instance 1
Device3(config-erps1)# sub-ring
Device3(config-erps1)# erps enable
Device3(config-erps1)# exit
Device3(config)# interface gigabitethernet 0/3
Device3(config-if-gigabitethernet0/1)#no shutdown
Device3(config-if-gigabitethernet0/1)# end
```

Device4 配置 ERPS ring1，配置 vlan2 为 ring1 的控制 vlan，配置 gigabitethernet0/1 为 ring1 的 normal 端口，配置 gigabitethernet0/2 为 ring1 的 normal 端口，配置实例 1 为 ring1 的数据 vlan，并使能 ring1 的 ERPS 功能。

```
Device4# configure terminal
Device4(config)#erps ring 1
Device4(config-erps1)# control vlan 2
Device4(config-erps1)# port0 interface g0/1
Device4(config-erps1)# port1 interface g0/2
Device4(config-erps1)# instance 1
Device4(config-erps1)# erps enable
Device4(config-erps1)# exit
Device4(config)# interface gigabitethernet 0/1
Device4(config-if-gigabitethernet0/1)#no shutdown
Device4(config-if-gigabitethernet0/1)# end
```

Device4 配置 ERPS ring2，配置 vlan3 为 ring2 的控制 vlan，配置 gigabitethernet0/3 为 ring2 的 normal 端口，配置实例 1 为 ring2 的数据 vlan，配置 ring2 为 sub-ring 并使能 ring2 的 ERPS 功能。

```
Device4# configure terminal
Device4(config)#erps ring 2
Device4(config-erps1)# control vlan 3
Device4(config-erps1)# port0 interface g0/3
Device4(config-erps1)# instance 1
Device4(config-erps1)# sub-ring
Device4(config-erps1)# erps enable
Device4(config-erps1)# exit
Device4(config)# interface gigabitethernet 0/3
Device4(config-if-gigabitethernet0/1)#no shutdown
Device4(config-if-gigabitethernet0/1)# end
```

Device5 配置 ERPS ring2，配置 vlan3 为 ring2 的控制 vlan，配置 gigabitethernet0/2 为 ring2 的 normal 端口，配置 gigabitethernet0/1 为 ring2 的 owner 端口，配置实例 1 为 ring2 的数据 vlan，配置 ring2 为 sub-ring 并使能 ring2 的 ERPS 功能。

```
Device4# configure terminal
Device4(config)#erps ring 2
Device4(config-erps1)# control vlan 3
Device4(config-erps1)# port0 interface g0/1 rpl owner
Device4(config-erps1)# port0 interface g0/2
```

```
Device4(config-erps1)# instance 1
Device4(config-erps1)# sub-ring
Device4(config-erps1)# erps enable
Device4(config-erps1)# exit
Device4(config)# interface gigabitethernet 0/1
Device4(config-if-gigabitethernet0/1)#no shutdown
Device4(config-if-gigabitethernet0/1)# end
```

Device6 配置 ERPS ring2, 配置 vlan3 为 ring2 的控制 vlan, 配置 gigabitethernet0/2 为 ring2 的 neighbour 端口, 配置 gigabitethernet0/1 为 ring2 的 normal 端口, 配置实例 1 为 ring2 的数据 vlan, 配置 ring2 为 sub-ring 并使能 ring2 的 ERPS 功能。

```
Device4# configure terminal
Device4(config)#erps ring 2
Device4(config-erps1)# control vlan 3
Device4(config-erps1)# port0 interface g0/1
Device4(config-erps1)# port0 interface g0/2 rpl neighbour
Device4(config-erps1)# instance 1
Device4(config-erps1)# sub-ring
Device4(config-erps1)# erps enable
Device4(config-erps1)# exit
Device4(config)# interface gigabitethernet 0/1
Device4(config-if-gigabitethernet0/1)#no shutdown
Device4(config-if-gigabitethernet0/1)# end
```

步骤 4: 检验结果。

#待网络拓扑稳定后, 查看各 Device 的 ERPS 信息, 以 device3 为例。

#查看 Device2 的 ERPS 信息。

```
Device3# show erps ring 1 detail
Ring ID      : 1
Version      : v2
R-APS mel    : 7
Instance     : 1 vlans mapped : 100-200
Control VLAN : 2
Node role    : Normal
Node state   : idle
Guard timer  : 500 ms      Running : 0 ms
Holdoff timer: 0 ms       Running : 0 ms
```

WTR timer : 5 min Running : 0 s

WTB timer : 7 s Running : 0 s

Subring : No

Tc-limit enable : No

Tc-limit Interval : 2

Tc-limit Threshold : 3

Revertive operation : Revertive

R-APS channel : Non-Virtual channel

Enable status : Enable

Gigabitethernet0/1 Flush Logic

Remote Node ID : 0000-0000-0000

Remote BPR : 0

Gigabitethernet0/1 track CFM

MD Name :

MA Name :

MEP ID : 0

RMEP ID : 0

CFM State : 0

Gigabitethernet0/2 Flush Logic

Remote Node ID : 0000-0000-0000

Remote BPR : 0

Gigabitethernet0/2 track CFM

MD Name :

MA Name :

MEP ID : 0

RMEP ID : 0

CFM State : 0

Port	Name	PortRole	SwitchType	PortStatus	SignalStatus
------	------	----------	------------	------------	--------------

Port0	gigabitethernet0/1	Normal	--	Forwarding	Non-failed
-------	--------------------	--------	----	------------	------------

Port1	gigabitethernet0/2	Normal	--	Forwarding	Non-failed
-------	--------------------	--------	----	------------	------------

Device2# show erps ring 2 detail

Ring ID : 2

Version : v2

R-APS mel : 7

Instance : 1 vlans mapped : 100-200

Control VLAN : 3

Node role : Normal

Node state : idle
Guard timer : 500 ms Running : 0 ms
Holdoff timer : 0 ms Running : 0 ms
WTR timer : 5 min Running : 0 s
WTB timer : 7 s Running : 0 s
Subring : No
Tc-limit enable : No
Tc-limit Interval : 2
Tc-limit Threshold : 3
Revertive operation : Revertive
R-APS channel : Non-Virtual channel
Enable status : Enable

Gigabitethernet0/3 Flush Logic
Remote Node ID : 0000-0000-0000
Remote BPR : 0

Gigabitethernet0/1 track CFM
MD Name :
MA Name :
MEP ID : 0
RMEP ID : 0
CFM State : 0

Port	Name	PortRole	SwitchType	PortStatus	SignalStatus
Port0	gigabitethernet0/3	Normal	--	Forwarding	Non-failed

网络管理及监控

67 网络测试和故障诊断

67.1 网络测试和故障诊断简介

使用网络测试和故障诊断工具，可以检查网络连接状况，诊断系统故障。日常维护中，当需要检查网络连接情况时，可以使用 ping 功能和 traceroute 功能。当需要诊断系统故障时，可以打开系统调试信息，诊断系统故障。

67.2 网络测试和故障诊断应用

表 67-1 网络测试和故障诊断应用列表

应用功能	
ping 功能	ping
	ping ip
	交互模式 ping
	grouping
traceroute 功能	traceroute

应用功能	
	交互模式 traceroute
系统调试功能	系统调试

67.2.1 ping 功能 **-B -S -E -A**

ping 功能用于检查网络连接状况及主机是否可达。ping 功能发送 ICMP 回显请求报文给主机，并等待返回 ICMP 回显应答，用于判断目的端是否可达。ping 还能测出源端到目的端的往返时间。

配置条件

无

ping

表 67-2 ping

步骤	命令	说明
检测指定的目的地址是否可达	ping [vrf <i>vrf-name</i>] { [ip <i>host-name</i> <i>ip-address</i>] / [ipv6 <i>host-name</i> <i>ipv6-address</i>] <i>host-name</i> <i>ip-address</i> <i>ipv6-address</i> } [-l <i>packet-length</i>] [-w <i>wait-time</i>] [-n <i>packet-number</i> -t]	必选

交互模式 ping

如果需要使用到宽松的源路由选项、严格的源路由选项、记录路由、记录时间戳等选项，或者需要知道对端设备支持的最大 ICMP 报文的大小，可以通过交互模式 ping 来实现。

表 67-3 交互模式 ping

步骤	命令	说明
进入 ping 交互模式	ping [vrf vrf-name]	必选 在特权用户模式下执行该命令，进入 ping 交互模式
配置网络协议类型	Protocol [ip]: [ip ipv6]	可选 缺省情况下，使用 IPv4 协议
配置目的 IP 地址或主机名	Target IP address or hostname: { ip-address / host-name }	必选
配置发送 ICMP 请求报文的次数	Repeat count [5]: [repeat-count]	可选 缺省情况下，发送 5 次
配置 ICMP 请求报文的长度	Datagram size [76]: [datagram-size]	可选 报文长度是整个 IP 报文的大小 缺省情况下，报文长度为 76 字节
配置等待 ICMP 响应的超时时间	Timeout in seconds [2]: [timeout]	可选 缺省情况下，2 秒超时

步骤	命令	说明
开启扩展选项	Extended commands [no]: [yes / no]	可选 开启扩展选项后, 扩展选项的配置命令才可见 缺省情况下, 没有开启扩展选项
配置扩展选项, ICMP 请求报文的源 IP 地址或者出接口	Source address or interface: { <i>ip-address / interfacename</i> }	可选 开启扩展选项后才能配置该命令 缺省情况下, 未指定请求报文的源地址和出接口
配置扩展选择, ICMP 请求报文的服务类型	Type of service [0]: [<i>tos</i>]	可选.仅 IPv4 协议支持该命令。 开启扩展选项后, 才能配置该命令 缺省情况下, TOS 值为 0
配置扩展选项, 设置不允许分片	Set DF bit in IP header? [no]: [yes / no]	可选.仅 IPv4 协议支持该命令。 开启扩展选项后, 才能配置该命令 缺省情况下, 未设置 DF 标志, 允许分片
配置扩展选项, 校验回应报文的数据内容	Validate reply data? [no]: [yes / no]	可选.仅 IPv4 协议支持该命令。

步骤	命令	说明
		<p>开启扩展选项后，才能配置该命令</p> <p>缺省情况下，不校验数据内容</p>
配置扩展选项，ICMP 请求报文的数据内容	Data pattern [abcd]: [<i>data-pattern</i>]	<p>可选</p> <p>开启扩展选项后，才能配置该命令</p> <p>缺省情况下，数据内容模板为“abcd”</p>
配置扩展选项，宽松的源路由选项、严格的源路由选项、记录路由、记录时间戳、显示详细信息	Loose, Strict, Record, Timestamp, Verbose[none]: [l s] [r / t / v]	<p>可选.仅 IPv4 协议支持该命令。</p> <p>开启扩展选项后，才能配置该命令</p> <p>缺省情况下，未配置该扩展选项</p>
开启扫描发送 ICMP 请求报文	Sweep range of sizes [no]: [yes / no]	<p>可选.仅 IPv4 协议支持该命令。</p> <p>缺省情况下，扫描发送是关闭的</p>
配置扫描起始值	Sweep min size [36]: [<i>min-size</i>]	<p>可选.仅 IPv4 协议支持该命令。</p> <p>开启扫描发送后，才能配置该命令</p>

步骤	命令	说明
		缺省情况下，扫描起始值为 36
配置扫描结束值	Sweep max size [18024]: [<i>max-size</i>]	可选.仅 IPv4 协议支持该命令。 开启扫描发送后，才能配置该命令 缺省情况下，扫描结束值为 18024
配置扫描增量值	Sweep interval [1]: [<i>interval</i>]	可选.仅 IPv4 协议支持该命令。 开启扫描发送后，才能配置该命令 缺省情况下，扫描增量值为 1

grouping

设备支持一次性发送多个 ICMP 回显请求，根据目的主机返回的 ICMP 应答报文数得到更精确的网络连接状态。

表 67-4 grouping

步骤	命令	说明
发送多组 ICMP 请求报文，检测指定的目的地址是否可达	grouping [vrf vrf-name] { <i>hostname / ip-address</i> } [[-l <i>packet-length</i>] [-g <i>packet-</i>	必选

步骤	命令	说明
	<code>group] [-w wait-time] [-n packet-number] [-t]</code>	

说明：

- ping 目的主机名时，需要先配置 DNS 功能，否则 ping 会失败。DNS 配置参见“IP 网络协议配置”中的“域名解析服务配置”。

67.2.2 traceroute 功能 **-B -S -E -A**

traceroute 功能用于查看数据包从源站到目的站所经过的网关，它主要用于检测目的是否可达，以及分析出故障的网络节点。traceroute 的执行过程是：首先发送一份 TTL 为 1 的 IP 数据报给目的主机，第一跳网关丢弃该数据报，并发回一份 ICMP 超时差错报文，这样 traceroute 就得到了路径中的第一个网关的地址。然后 traceroute 发送一份 TTL 值为 2 的数据报，这样就可以得到第二跳网关的地址。继续这个过程直到到达目的主机，traceroute 报文的 UDP 端口号是目的端的任何一个应用程序都不可能使用的端口号，目的端收到该数据报后，发回一份端口不可达差错报文，这样就可以得到该路径上所有网关的地址了。

配置条件

无

traceroute

表 67-5 traceroute

步骤	命令	说明
查看数据报从源站到目的站经过的网关	<code>traceroute [vrf vrf-name] {{ip host-name / ip-address} / {ipv6 host-</code>	必选

步骤	命令	说明
	<i>name / ipv6-address</i> <i>host-name / ip-address</i> <i>/ ipv6-address</i> [-f start-ttl] [-w wait-time] [-m max-ttl]	

交互模式 traceroute

表 67-6 交互模式 traceroute

步骤	命令	说明
进入 traceroute 交互模式	traceroute [vrf <i>vrf-name</i>]	必选 在特权用户模式下执行该命令，进入 traceroute 交互模式
配置网络协议类型	Protocol [ip]: [ip ipv6]	可选 缺省情况下，使用 IPv4 协议
配置目的 IP 地址或主机名	Target IP address or hostname: { <i>ip-address</i> / <i>host-name</i> }	必选
配置 traceroute 报文的源 IP 地址或出接口	Source address or interface: { <i>ip-address</i> / <i>interface-name</i> }	可选 缺省情况下，未指定报文的源 IP 地址或出接口

步骤	命令	说明
配置等待每个探测报文响应的超时时间	Timeout in seconds [3]: <i>timeout</i>	可选 缺省情况下, 3 秒超时
配置发送具有同一 TTL 值的探测报文的次数	Probe count [3]: <i>probe-count</i>	可选 缺省情况下, 发送 3 次
配置探测报文的的最小 TTL 值	Minimum Time to Live [1]: <i>min-ttl</i>	可选 缺省情况下, 最小 TTL 值为 1
配置探测报文的的最大 TTL 值	Maximum Time to Live [30]: <i>max-ttl</i>	可选 缺省情况下, 最大 TTL 值为 30
配置探测报文的的目的 UDP 端口号	Port Number [33434]: <i>port-number</i>	可选 缺省情况下, 目的端口号为 33434
配置宽松的源路由选项、严格的源路由选项、记录路由、记录时间戳、显示详细信息	Loose, Strict, Record, Timestamp, Verbose[none]: [l s] [r / t / v]	可选, 仅 IPv4 协议支持该命令 缺省情况下, 未配置该选项

67.2.3 系统调试功能

-B -S -E -A

为了帮助用户诊断问题，设备的绝大多数功能模块，都提供了调试功能。

调试功能由两个开关控制：

- 模块的调试开关，控制是否生成模块的调试信息
- 屏幕输出开关，控制是否将调试信息输出到终端

配置条件

无

系统调试

表 67-7 系统调试

步骤	命令	说明
打开远程登录的系统调试屏幕输出开关	terminal monitor	可选 远程登录包括 telnet、ssh 等方式。 缺省情况下，开关是关闭的
进入全局配置模式	configure terminal	-
打开 console 控制台的系统调试屏幕输出开关	logging console	可选 缺省情况下，开关是开启的
退出全局配置模式	exit	-
打开系统功能模块的调试开关	debug { all module-name [option] }	可选

步骤	命令	说明
		缺省情况下，系统所有功能模块的调试开关都是关闭的

说明：

- 只有同时配置 **debug module-name option**、**terminal monitor** 或 **logging console** 命令后，才能在终端显示调试信息。
- 调试信息生成和输出会影响系统性能，所以，在需要的时候最好使用 **debug module-name option** 命令打开特定的调试开关，**debug all** 命令会打开全部调试开关，最好不要使用。调试结束后，要及时关闭相应的调试开关或者使用 **no debug all** 命令关闭所有的调试开关。

67.2.4 网络测试和故障诊断监控与维护

-B -S -E -A

表 67-8 系统测试和故障诊断监控与维护

命令	说明
show debugging	显示系统中已经打开调试开关的功能模块信息

67.3 网络测试和故障诊断典型配置举例

67.3.1 ping 的应用 **-B -S -E -A**

网络需求

- Device1 使用 telnet IP 地址登录 Device3 失败，现需要确认 Device1 与 Device3 之间 IP 路由是否可达。
- Device1 使用 telnet IPv6 地址登录 Device3 失败，现需要确认 Device1 与 Device3 之间 IPv6 路由是否可达。

网络拓扑

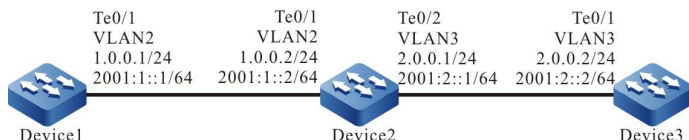


图 67-1 ping 的应用组网图

配置步骤

步骤 1： 配置各接口的 IP 地址和 IPv6 全球单播地址。（略）

步骤 2： 使用 ping 命令查看 Device1 和 Device3 之间是否可达。

#查看 Device1 ping Device3 的 IP 地址 2.0.0.2 能否 ping 通。

```
Device1#ping 2.0.0.2
Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 2.0.0.2 , timeout is 2 seconds:
.....
Success rate is 0% (0/5).
```

#查看 Device1 ping Device3 的 IPv6 地址 2001:2::2 能否 ping 通。

```
Device1#ping 2001:2::2
Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 2001:2::2 , timeout is 2 seconds:
.....
Success rate is 0% (0/5).
```

步骤 3： 使用 ping 命令查看 Device1 和 Device2 之间是否可达。

#查看 Device1 ping Device2 的 IP 地址 1.0.0.2 能否 ping 通。

```
Device1#ping 1.0.0.2
```

```
Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 1.0.0.2 , timeout is 2 seconds:
!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.
```

#查看 Device1 ping Device2 的 IPv6 地址 2001:1::2 能否 ping 通。

```
Device1#ping 2001:1::2
```

```
Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 2001:1::2 , timeout is 2 seconds:
!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.
```

步骤 4: 使用 ping 命令查看 Device2 和 Device3 之间是否可达。

#查看 Device2 ping Device3 的 IP 地址 2.0.0.2 能否 ping 通。

```
Device2#ping 2.0.0.2
```

```
Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 2.0.0.2 , timeout is 2 seconds:
!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/0/0 ms.
```

#查看 Device2 ping Device3 的 IPv6 地址 2001:2::2 能否 ping 通。

```
Device2#ping 2001:2::2
```

```
Press key (ctrl + shift + 6) interrupt it.
Sending 5, 76-byte ICMP Echos to 2001:2::2 , timeout is 2 seconds:
!!!!
Success rate is 100% (5/5). Round-trip min/avg/max = 0/176/883 ms.
```

从以上的排查结果可以看到 Device1 与 Device2 能互通，Device2 和 Device3 能互通，问题出现在 Device1 与 Device3 之间，后续可以对路由等配置进行检查，或使用 **debug ip icmp** 命令和 **debug ipv6 icmp** 命令分别查看 ICMP 报文和 ICMPv6 报文内容是否正确，也可以使用下面一节中介绍的 traceroute 来确认故障的网络节点。

67.3.2 traceroute 的应用 **-B -S -E -A**

网络需求

- Device1 使用 telnet IP 地址登录 Device3 失败，现需要确认 Device1 与 Device3 之间是否 IP 路由可达，如果路由不可达，需要确定出故障的网络节点。

- Device1 使用 telnet IPv6 地址登录 Device3 失败，现需要确认 Device1 与 Device3 之间是否 IPv6 路由可达，如果路由不可达，需要确定出故障的网络节点。

网络拓扑

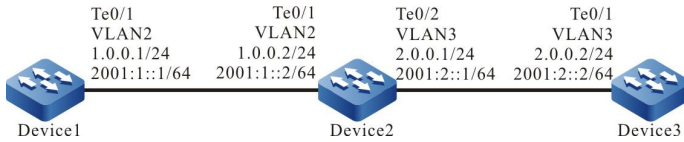


图 67-2 Traceroute 的应用组网图

配置步骤

步骤 1： 配置各接口的 IP 地址和 IPv6 全球单播地址。（略）

步骤 2： 使用 traceroute 命令确定 Device1 和 Device3 之间的故障节点。

#使用 traceroute 命令确定 Device1 和 Device3 之间的 IPv4 故障节点。

```
Device1#traceroute 2.0.0.2
Type escape sequence to abort.
Tracing the route to 2.0.0.2, min ttl = 1, max ttl = 30.

 0 1.0.0.2  0 ms  0 ms  0 ms
 1 * * *
 2 * * *
 3 * * *
 4 * * *
 5 * * *
 6
```

#使用 traceroute 命令确定 Device1 和 Device3 之间的 IPv6 故障节点。

```
Device1#traceroute 2001:2::2
Type escape sequence to abort.
Tracing the route to 2001:2::2, min ttl = 1, max ttl = 30.

 0 2001:1::2  0 ms  0 ms  0 ms
 1 * * *
 2 * * *
 3 * * *
 4 * * *
 5 * * *
 6
```

从以上的排查结果看 Device1 发出的 traceroute 报文能够到达 Device2，traceroute 报文从 Device2 不能够到达 Device3，后续需要对 Device2 和 Device3 的路由等配置及线路进行检查，或使用 **debug ip icmp** 命令和 **debug ipv6 icmp** 命令查看 ICMP 报文和 ICMPv6 报文内容是否正确，可以结合使用上一节中的 ping 来检测 Device2 与 Device3 之间的连通。

68 网关保活

68.1 网关保活简介

网关保活 (keepalive gateway) , 设置以太网接口向特定的网关地址发送保活报文, 用于监测目的网关的可达性, 网关不可达时, 关闭接口 IP 协议层。

接口上配置网关保活后, 该接口向配置的网关地址定时发送 ARP 请求报文, 当接口连续 N (N 为用户配置的重试次数) 次收不到 ARP 响应报文时关闭接口 IP 协议层, 直到再次收到 ARP 响应报文后启用接口 IP 协议层。

68.2 网关保活功能配置

表 68-1 网关保活功能配置列表

配置任务	
配置网关保活功能	配置网关保活基本功能
	配置保活报文发送参数

68.2.1 配置网关保活功能

-S -E -A**配置条件**

在配置网关保活功能之前，首先完成以下任务：

- 配置接口的 IP 地址。

配置网关保活基本功能

表 68-2 配置网关保活基本功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
配置网关保活	keepalive gateway <i>ip-address</i> [<i>interval</i> msec <i>interval</i>] [<i>retry-count</i>]	必选 缺省情况下，接口上未启用网关保活功能

配置保活报文发送参数

配置保活报文发送参数，可以控制网关保活报文的发送速率，保活报文的发送速率达到配置值时，暂停配置的时间后再继续发送保活报文。

表 68-3 配置保活报文发送参数

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置保活报文的发送速率	keepalive gateway disperse pkt-rate <i>packet-rate</i>	可选

步骤	命令	说明
		缺省情况下，保活报文的最大发送速率为100pps
配置暂停发送保活报文的时间	keepalive gateway disperse pause-time <i>pause-time</i>	可选 缺省情况下，暂停发送保活报文的时间为100 毫秒

68.2.2 网关保活监控与维护

-S -E -A

表 68-4 网关保活监控与维护

命令	说明
clear keepalive gateway statistics [<i>interface-name</i>]	清除网关保活的收发统计信息
show keepalive gateway [<i>interface-name</i>]	查看启用了网关保活的接口及其配置
show keepalive gateway disperse	查看网关保活报文的发送参数配置
show keepalive gateway statistics [<i>interface-name</i>]	查看网关保活的统计信息

68.3 网关保活典型配置举例

68.3.1 配置网关保活

-S -E -A**网络需求**

- Device 4 为连接设备，只对数据进行透明传输。
- Device1、Device2、Device3 上运行 OSPF 协议进行路由交互。
- Device1 到 201.0.0.0/24 网段的数据流优选 Device3。
- Device1 和 Device3 间的线路使用网关保活功能，当 Device1 和 Device3 间的线路出现故障后，网关保活会快速检测到故障并将相关接口的状态修改为 down，OSPF 感知到接口的状态变化后，将路由切换到 Device2 进行通信。

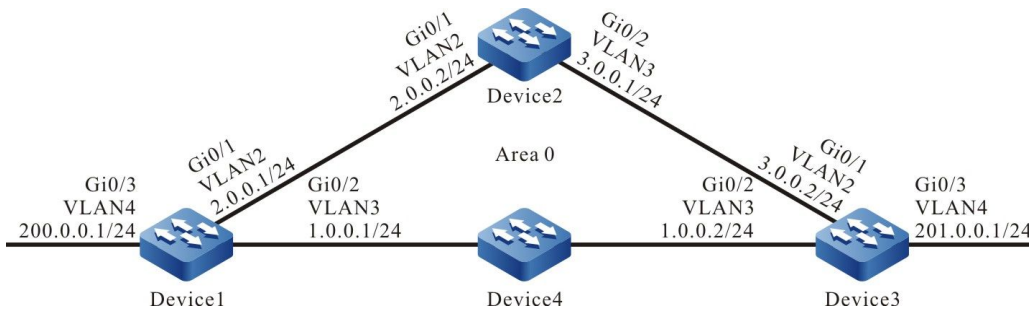
网络拓扑

图 68-1 配置网关保活组网图

配置步骤

步骤 1：配置 VLAN，并将端口加入对应的 VLAN。（略）

步骤 2：配置各接口 IP 地址。（略）

步骤 3：配置 OSPF 进程。

#配置 Device1。

```
Device1#configure terminal
Device1(config)#router ospf 100
Device1(config-ospf)#network 1.0.0.0 0.0.0.255 area 0
```

```
Device1(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#network 200.0.0.0 0.0.0.255 area 0
Device1(config-ospf)#exit
```

#配置 Device2。

```
Device2#configure terminal
Device2(config)#router ospf 100
Device2(config-ospf)#network 2.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
Device2(config-ospf)#exit
```

#配置 Device3。

```
Device3#configure terminal
Device3(config)#router ospf 100
Device3(config-ospf)#network 1.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 3.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#network 201.0.0.0 0.0.0.255 area 0
Device3(config-ospf)#exit
```

#查看 Device1 的路由表。

```
Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, Ex - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C 1.0.0.0/24 is directly connected, 00:20:17, vlan3
C 2.0.0.0/24 is directly connected, 13:01:32, vlan2
O 3.0.0.0/24 [110/2] via 2.0.0.2, 01:11:40, vlan2
   [110/2] via 1.0.0.2, 00:02:00, vlan3
C 200.0.0.0/24 is directly connected, 01:31:58, vlan4
O 201.0.0.0/24 [110/2] via 1.0.0.2, 00:02:00, vlan3
```

Device1 到 201.0.0.0/24 网段的数据流优选 Device3。

说明：

- Device2、Device3 的查看方法与 Device1 的一样，查看过程省略。
-

步骤 4： 配置网关保活。

#配置 Device1。

```
Device1(config)#interface vlan 3
Device1(config-if-vlan3)#keepalive gateway 1.0.0.2
Device1(config-if-vlan3)#exit
```

#配置 Device3。

```
Device3(config)#interface vlan 3
Device3(config-if-vlan3)#keepalive gateway 1.0.0.1
Device3(config-if-vlan3)#exit
```

#查看 Device1 的网关保活信息。

```
Device1#show keepalive gateway
interface vlan3 gateway 1.0.0.2 time 10s retry 3 remain 3 now UP
```

#查看 Device3 的网关保活信息。

```
Device3#show keepalive gateway
interface vlan3 gateway 1.0.0.1 time 10s retry 3 remain 3 now UP
```

步骤 5: 检验结果。

#当 Device1 和 Device3 间的线路出现故障后，网关保活会快速检测到故障，并将接口 VLAN3 的状态修改为 down。

```
Device1#show keepalive gateway
interface vlan3 gateway 1.0.0.2 time 10s retry 3 remain 0 now DOWN
```

#OSPF 感知到接口 VLAN3 的状态变化后，将路由切换到 Device2 进行通信。

```
Device1# show ip ospf interface vlan3
VLAN3 is down, line protocol is down
OSPF is enabled, but not running on this interface

Device1#show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, Ex - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

C 2.0.0.0/24 is directly connected, 13:16:40, vlan2
O 3.0.0.0/24 [110/2] via 2.0.0.2, 00:01:25, vlan2
C 200.0.0.0/24 is directly connected, 00:10:53, vlan4
O 201.0.0.0/24 [110/3] via 2.0.0.2, 00:00:18, vlan2
```

#可以看到 Device1 到 201.0.0.1/24 网段的数据流优选 Device2。

69 SLA

69.1 SLA 简介

SLA (Service Level Agreements: 服务等级协议), 它根据报文传输情况计算相关参数, 最终输出报告。SLA 又称为 RTR(Response Time Reporter, 响应时间报告者)。是一种网络检测监控工具。SLA 通过定期发送指定协议的报文来检测和监控网络通信情况。通过配置不同类型的 RTR 实体并进行调度, SLA 可以对不同的网络应用进行诊断并最终输出测试结果。

SLA 基本概念:

- RTR Entity (RTR 实体) : RTR 实体为一个通用的概念, 和具体类型的 RTR 实体无关。系统目前的 RTR 实体类型有: 用来检测网络基本通信情况的 ICMP-echo 实体、ICMP-path-echo 实体、ICMP-path-jitter 实体、UDP-echo 实体; 用来检测网络传输 VoIP 语音报文情况的 VoIP-jitter 实体; 用来检测接口流量的 FLOW-statistics 实体。
- RTR Group (RTR 实体组) : 一个 RTR 实体组是一个或多个 RTR 实体组成的集合。
- RTR responder (RTR 应答器) : RTR 应答器在目的端配置, 主要用来和源端建立连接, 并对源端发出的检测报文进行回应, 大部分实体不需要配置应答器, 但在使用 UDP-echo 实体、VoIP-jitter 实体时必须配置应答器。
- RTR Schedule (RTR 调度器) : 只配置 RTR 实体或 RTR 实体组无法进行对应的检测, 必须发起调度才能最终完成检测。

69.2 SLA 功能配置

表 69-1 SLA 功能配置列表

配置任务	
使能 RTR	使能 RTR
配置 RTR 实体	创建 RTR 实体
	配置 ICMP-echo 实体
	配置 ICMP-path-echo 实体
	配置 ICMP-path-jitter 实体
	配置 VoIP-jitter 实体
	配置 UDP-echo 实体
	配置 FLOW-statistics 实体
	配置实体共有配置
配置 RTR 实体组	配置 RTR 实体组
配置 RTR 应答器	配置 RTR 应答器
配置 RTR 调度器	配置 RTR 调度器
配置暂停调度实体	配置暂停调度实体
配置恢复调度实体	配置恢复调度实体

69.2.1 使能 RTR **-S -E -A**

在 RTR 的各项配置任务中，必须先使能 RTR，其它功能特性的配置才能生效。

配置条件

无

使能 RTR

表 69-2 使能 RTR

步骤	命令	说明
进入全局配置模式	configure terminal	-
使能 RTR	rtr enable	必选 缺省情况下，未使能 RTR

69.2.2 配置 RTR 实体 **-S -E -A**

配置条件

在配置 RTR 实体前，首先完成以下任务：

使能 RTR。

创建 RTR 实体

一种实体对应一种类型的检测，创建 RTR 实体并进入该实体配置模式后，可以配置实体的具体参数。

表 69-3 创建 RTR 实体

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
创建 RTR 实体	rtr entity-id entity-type	必选

配置 ICMP-echo 实体

ICMP-echo 实体的作用是对网络基本通信情况进行检测。其定期对网络中的某个目的地址发送 ICMP 回显请求报文，从而得到检测端到目的端报文传输的时延和丢包情况等。在一个检测周期内，ICMP-echo 实体只要收到一个 ICMP 回显请求回应报文，实体的状态就是可达的。

由于一般的网络设备都支持 ping，因此，这种实体在检测网络基本通信情况方面可以发挥作用。通过丰富的调度策略以及日志记录功能，可以让网络管理员及时了解网络通信情况以及历史信息，同时还减少了普通 ping 命令输入的繁琐。

表 69-4 配置 ICMP-echo 实体

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 ICMP-echo 实体配置模式	rtr entity-id [icmpecho]	-
配置检测属性	set [vrf vrf-name] target-ip-address [npacket] [data-size] [timeout] [frequency-value] [extend source-ip-address [tos] [set-DF] [verify-data]]	必选 缺省情况下，未配置实体的检测属性
配置将 rtt 值作为检测实体是否可达的判断依据	status-care rtt	可选 缺省情况下，未使用 rtt 值判断是否可达
配置实体共有配置	见配置实体共有配置	可选

说明：

- ICMP-echo 实体的调度间隔（frequency-value）需要满足如下要求：调度间隔 > npacket * timeout。
- 如果为该实体配置调度器，调度器的老化时间必须大于该实体的调度间隔。

配置 ICMP-path-echo 实体

ICMP-path-echo 实体的作用是对网络基本通信情况进行检测。其定期对网络中的某个目的地址发送 ICMP 回显请求报文，从而得到检测端到目的端报文传输的时延和丢包情况、且得到检测端与检测端到目的端的中间各设备之间的时延和丢包情况。在一个检测周期内，ICMP-path-echo 实体只要收到一个 ICMP 回显请求回应报文，实体的状态就是可达的。

由于一般的网络设备都支持 ping，因此，这种实体在检测网络基本通信情况方面可以发挥作用。通过丰富的调度策略以及历史记录功能，可以让网络管理员及时了解网络通信情况（比如路径上哪个网络设备处的时延比较严重）以及历史信息。

表 69-5 配置 ICMP-path-echo 实体

步骤	命令	说明
进入系统配置模式	configure terminal	-
进入 ICMP-path-echo 实体配置模式	rtr entity-id [icmp-path-echo]	-
配置检测属性	set dest-ipaddr target-ip-address [source-ipaddr source-ip-address]	必选
配置宽松的源站选路	lsr-path [hop-ip-address-list none]	可选 缺省情况下，未配置宽松的源站选路

步骤	命令	说明
配置只检测源端到目的端的网络情况	targetOnly [true false]	可选 缺省情况下，targetOnly 为 true 只检测源端到目的端的网络情况 targetOnly 配置为 false，会逐跳检测源端到目的端的网络情况
配置是否校验回应报文的数据内容	verify-data [true false]	可选 缺省情况下，不校验数据内容
配置实体共有配置	见配置实体共有配置	可选

配置 ICMP-path-jitter 实体

ICMP-path-jitter 实体的作用是对网络基本通信情况进行检测。其定期对网络中的某个目的地址发送 ICMP 回显请求报文，从而得到检测端到目的端报文传输的时延、抖动、丢包情况、且得到检测端与检测端到目的端的中间各设备之间的时延、抖动、丢包情况。在一个检测周期内，ICMP-path-jitter 实体只要收到一个 ICMP 回显请求回应报文，实体的状态就是可达的。

由于一般的网络设备都支持 ping，因此，这种实体在检测网络基本通信情况方面可以发挥作用。通过丰富的调度策略以及历史记录功能，可以让网络管理员及时了解网络通信情况（比如路径上哪个网络设备处的时延比较严重）以及历史信息。

表 69-6 配置 ICMP-path-jitter 实体

步骤	命令	说明
进入系统配置模式	configure terminal	-

步骤	命令	说明
进入 ICMP-path-jitter 实体配置模式	rtr <i>entity-id</i> [icmp-path-jitter]	-
配置检测属性	set dest-ipaddr <i>target-ip-address</i> [<i>pkt-number</i>] [<i>pkt-interval</i>] [source-ipaddr <i>source-ip-address</i>]	必选
配置宽松的源站选路的 IP 地址	lsr-path [<i>hop-ip-address-list</i> none]	可选 缺省情况下，未配置源站选路
配置只检测源端到目的端的网络情况	targetOnly [true false]	可选 缺省情况下，targetOnly 为 true 只检测源端到目的端的网络情况 targetOnly 配置为 false，会逐跳检测源端到目的端的网络情况
配置抖动阈值和超限规则	threshold-jitter <i>jitter</i> direction { be se }	可选 缺省情况下，抖动阈值为 6000 毫秒，超限规则为 be
配置是否校验回应报文的数据内容	verify-data [true false]	可选 缺省情况下，不校验数据内容
配置实体共有配置	见配置实体共有配置	可选

说明：

- 超限规则为 be 时，实际值大于等于阈值时判定为超限；超限规则为 se 时，实际值小于等于阈值时判定为超限。

配置 VoIP-jitter 实体

VoIP-jitter 实体是用来测量 VoIP 语音报文在普通 IP 网络中传输质量的 RTR 实体。

VoIP-jitter 实体可以模拟 G.711 A Law、G.711 mu Law、G.729A 这三种编码解码器或自定义的编码解码器从源设备向目的设备发送对应速率、报文间隔、对应大小的 UDP 数据报，并对报文的往返时间、单向报文丢失以及单向时延等进行统计，在这些统计信息的基础上计算出 ICPIF 值，最后根据 ICPIF 值估算出 MOS 值。在一个检测周期内，VoIP-jitter 实体只要收到一个检测回应报文，实体的状态就是可达的。

表 69-7 配置 VoIP-jitter 实体

步骤	命令	说明
进入系统配置模式	configure terminal	-
进入 VoIP-jitter 实体配置模式	rtr entity-id [jitter]	必选 如果实体已经存在，直接进入实体配置模式
配置检测属性	set dest-ipaddr target-ip-address dest-port target-port { g711alaw g711ulaw g729a user_defined packet-size packet-number packet-interval schedule-interval } [source-ipaddr source-ip-address] [source-port source-port]	必选

步骤	命令	说明
配置源到目的端的单向延时阈值和超限规则	threshold-sd-delay <i>sd-delay</i> direction { be se }	可选 缺省情况下，sd 延时阈值为 5000 毫秒，超限规则为 be
配置源到目的端的单向抖动阈值和超限规则	threshold-sd-jitter <i>sd-jitter</i> direction { be se }	可选 缺省情况下，sd 单向抖动阈值为 6000 毫秒，超限规则为 be
配置源到目的端的丢包阈值和超限规则	threshold-sd-pktloss <i>sd-packet</i> direction { be se }	可选 缺省情况下，sd 丢包阈值为 60000，超限规则为 be
配置目的到源端的单向延时阈值和超限规则	threshold-ds-delay <i>ds-delay</i> direction { be se }	可选 缺省情况下，ds 延时阈值为 5000 毫秒，超限规则为 be
配置目的到源端的单向抖动阈值和超限规则	threshold-ds-jitter <i>ds-jitter</i> direction { be se }	可选 缺省情况下，ds 单向抖动阈值为 6000 毫秒，超限规则为 be
配置目的到源端的丢包阈值和超限规则	threshold-ds-pktloss <i>ds-packet</i> direction { be se }	可选 缺省情况下，ds 丢包阈值为 60000，超限规则为 be
配置 icpif 值的阈值和超限规则	threshold-icpif <i>icpif-value</i> direction { be se }	可选

步骤	命令	说明
		缺省情况下, icpif 阈值为 100000000, 超限规则为 be
配置 mos 值的阈值和超限规则	threshold-mos <i>mos-value</i> direction { be se }	可选 缺省情况下, mos 阈值为 100000000, 超限规则 be
配置实体共有配置	见配置实体共有配置	可选

说明:

- 使用 VoIP-jitter 实体检测时, 除了配置 VoIP-jitter 实体外, 还需要在目的端配置 RTR 应答器。
- VoIP-jitter 实体默认发送报文个数比较多, 会占用网络带宽, 因此当配置这类实体超过 1 个时, shell 会进行提示。
- VoIP-jitter 实体检测网络传输语音报文的情况, 需要源端和目的端的时钟一致, 所以调度 VoIP-jitter 实体前, 还需要在目的端配置 NTP 服务端, 在源端配置 NTP 客户端, 待时钟同步后再配置 RTR 应答器, 最后配置调度器。NTP 的详细配置, 请参见 NTP 配置手册。
- 超限规则为 be 时, 实际值大于等于阈值时判定为超限; 超限规则为 se 时, 实际值小于等于阈值时判定为超限。

配置 UDP-echo 实体

UDP-echo 实体主要是对 IP 网络中的传输的 UDP 报文进行检测, 实体中需要指定发送的目的地址和端口。通过对该实体的调度, 可以有效监控 UDP 报文在 IP 网络中的传输情况。在一个检测周期内, UDP-echo 实体只要收到一个检测回应报文, 实体的状态就是可达的。

UDP-echo 实体通过有效监控, 可以记录 UDP 报文在 IP 网络中的往返延时、丢包 (数据报文) 等信息, 甚至可以以日志的方式记录监控的历史信息, 以供网络管理员了解网络通信情况以及排除故障等。

表 69-8 配置 UDP-echo 实体

步骤	命令	说明
进入系统配置模式	configure terminal	-
进入 UDP-echo 实体配置模式	rtr entity-id [udpecho]	必选 如果实体已经存在，直接进入实体配置模式
配置检测属性	set dest-ipaddr target-ip-address dest-port target-port [source-ipaddr source-ip-address] [source-port source-port]	必选 缺省情况下，未配置 UDP-echo 实体的检测属性
配置报文填充内容	data-pattern pad	可选 缺省情况下，填充内容为“ABCD”
配置实体共有配置	见配置实体共有配置	可选

说明：

- 使用 UDP-echo 实体检测时，除了配置 UDP-echo 实体外，还需要在目的端配置 RTR 应答器。

配置 FLOW-statistics 实体

FLOW-statistics 实体主要是对接口的流量进行检测，一个实体对应一个接口。通过对该实体的调度，可以有效监控该接口上的流量。在一个检测周期内，FLOW-statistics 实体监控的接口上有报文通过，实体的状态就是可达的。

FLOW-statistics 实体监控接口流量的间隔在 10s~10min 之间。通过有效监控，可以记录该接口上的流量峰值信息，甚至可以以日志方式记录每次监控时流量统计的历史信息，以供网络管理员了解网络通信情况以及排除故障等。

表 69-9 配置 FLOW-statistics 实体

步骤	命令	说明
进入系统配置模式	configure terminal	-
进入 FLOW-statistics 实体配置模式	rtr <i>entity-id</i> [flow-statistics]	必选 如果实体已经存在，直接进入实体配置模式
配置检测属性	flow-statistics interface <i>interface-name</i> interval <i>interval</i>	必选
配置接口接收的流量阈值和超限规则	threshold-inflow <i>flow-value</i> direction { be se }	可选 缺省情况下，接口接收的流量阈值为 200000000bps（比特/秒），超限规则为 be
配置接口接收报文的个数阈值和超限规则	threshold-inpacket <i>packet-value</i> direction { be se }	可选 缺省情况下，接口接收报文的个数阈值为 200000000，超限规则为 be
配置接口发送的流量阈值和超限规则	threshold-outflow <i>flow-value</i> direction { be se }	可选 缺省情况下，接口发送的流量阈值为 200000000 bps

步骤	命令	说明
		(比特/秒)，超限规则为 be
配置接口发送报文的个数阈值和超限规则	threshold-outpacket <i>packet-value</i> direction { be se }	可选 缺省情况下，接口发送报文的个数阈值为 200000000，超限规则为 be
配置实体共有配置	见配置实体共有配置	可选

说明：

- 超限规则为 be 时，实际值大于等于阈值时判定为超限；超限规则为 se 时，实际值小于等于阈值时判定为超限。

配置实体共有配置

表 69-10 配置实体共有配置

步骤	命令	说明
配置告警类型	alarm-type [log log-and-trap trap none]	可选 缺省情况下，告警方式为 none，不告警
配置保存历史记录 的条数	number-of-history-kept <i>history-number</i>	可选 缺省情况下，保存 1 条历史记录

步骤	命令	说明
配置保存历史记录的周期	periods <i>periods</i>	可选 缺省情况下，每次调度结束后保存一次历史记录
配置超时时间	timeout <i>timeout</i>	可选 缺省情况下，超时时间为： ICMP-path-echo 实体 5000 毫秒 ICMP-path-jitter 实体 5000 毫秒 VoIP-jitter 实体 50000 毫秒 UDP-echo 实体 5000 毫秒 不支持该共有命令的实体： ICMP-echo 实体 FLOW-statistics 实体
配置报文的 TOS 值	tos <i>tos-value</i>	可选 缺省情况下，TOS 值为 0 不支持该共有命令的实体： ICMP-echo 实体 FLOW-statistics 实体
配置实体的 VRF 属性	vrf <i>vrf-name</i>	可选 缺省情况下，未配置实体的 VRF 属性 不支持该共有命令的实体：

步骤	命令	说明
		ICMP-echo 实体 FLOW-statistics 实体
配置实体的调度间隔	frequency <i>seconds</i>	可选 缺省情况下，调度间隔为： ICMP-path-echo 实体 60 秒 ICMP-path-jitter 实体 60 秒 UDP-echo 实体 60 秒 不支持该共有命令的实体： ICMP-echo 实体 VoIP-jitter 实体 FLOW-statistics 实体
配置检测报文的长度	request-data-size <i>data-size</i>	可选 缺省情况下，检测报文长度为： ICMP-path-echo 实体 70 字节 ICMP-path-jitter 实体 70 字节 UDP-echo 实体 16 字节 不支持该共有命令的实体： ICMP-echo 实体 VoIP-jitter 实体

步骤	命令	说明
		FLOW-statistics 实体
配置丢包阈值和超限规则	threshold-pktloss <i>pktloss</i> direction { be se }	<p>可选</p> <p>缺省情况下, 丢包阈值为:</p> <p>ICMP-echo 实体 150</p> <p>ICMP-path-echo 实体 1</p> <p>ICMP-path-jitter 实体 100</p> <p>UDP-echo 实体 1</p> <p>超限规则为 be</p> <p>不支持该共有命令的实体:</p> <p>VoIP-jitter 实体</p> <p>FLOW-statistics 实体</p>
配置双向延时阈值和超限规则	threshold-rtt <i>rtt</i> direction { be se }	<p>可选</p> <p>缺省情况下, 双向延时阈值为:</p> <p>ICMP-echo 实体 9000 毫秒</p> <p>ICMP-path-echo 实体 9000 毫秒</p> <p>ICMP-path-jitter 实体 9000 毫秒</p> <p>VoIP-jitter 实体 9000 毫秒</p> <p>UDP-echo 实体 9000 毫秒</p> <p>超限规则为 be</p> <p>不支持该共有命令的实体:</p>

步骤	命令	说明
		FLOW-statistics 实体

说明:

- 如果 RTR 实体已经存在并且实体处于未调度状态, 执行 **rtr entity-id** 命令可以直接进入实体配置模式。
- 超限规则为 be 时, 实际值大于等于阈值时判定为超限; 超限规则为 se 时, 实际值小于等于阈值时判定为超限。
- ICMP-path-echo 实体的调度间隔需要满足以下要求: 调度间隔 > timeout。
- ICMP-path-jitter 实体的调度间隔需要满足以下要求: 调度间隔 > timeout; timeout 需要满足以下要求: timeout > pkt-number * pkt-interval; pkt-number 参数和 pkt-interval 参数见 ICMP-path-echo 实体的 **set** 命令。
- VoIP-jitter 实体的调度间隔在选择模拟 G.711ALaw、G.711muLaw、G.729A 这三种编解码器时需要满足以下要求: 调度间隔 > timeout + 5。选择用户自定义编解码器时需要满足以下要求: 调度间隔 > schedule-interval + 5; schedule-interval 又需要满足如下需求: schedule-interval > packet-number * packet-interval; schedule-interval、packet-number 和 packet-interval 参数见 VoIP-jitter 实体的 **set** 命令。
- UDP-echo 实体的调度间隔需要满足以下要求: 调度间隔 > timeout + 5。

69.2.3 配置 RTR 实体组 **-S -E -A**

一个 RTR 实体组是一个或多个 RTR 实体组成的集合。一个 RTR 实体可以属于多个 RTR 实体组, 组不能再成为组的成员, 一个组内只能包含一个成员一次。RTR 实体组以组 ID 来唯一标识, 组名由系统自动生成。

RTR 实体组的主要目的是为了更方便调度一个 RTR 集合。对 RTR 实体组的调度相当于对该 RTR 实体组内的所有存在的 RTR 实体进行调度, 检测结果存放在对应的 RTR 实体历史记录中。

配置条件

在配置 RTR 实体组前，首先完成以下任务：

使能 RTR。

配置 RTR 实体组

表 69-10 配置 RTR 实体组

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 RTR 实体组的配置模式	rtr group <i>group-id</i>	必选 如果对应的 RTR 实体组不存在，会自动创建这个实体组
添加 RTR 实体组内的成员	member <i>entity-list</i>	可选 缺省情况下，RTR 实体组不包含任何成员
配置 RTR 实体组的选项	option {or and }	可选 缺省情况下，RTR 实体组状态选项为 and（组内所有实体可达时，组状态才可达）
配置 RTR 实体组内成员间的调度间隔	interval <i>interval</i>	可选 缺省情况下，组内成员调度间隔为 0 秒
配置 RTR 实体组自动生成调度器	group probe	可选 缺省情况下，没有配置 RTR 实体组自动生成调度器

说明：

- 同一个 VoIP-jitter 实体或 UDP-echo 实体不能添加到多个组里面进行调度，否则调度结果可能不正确。
- RTR 实体组的调度间隔计算方法如下：调度间隔 = 所有成员调度间隔的最大值 + (成员数 - 1) * 成员间的调度间隔。

69.2.4 配置 RTR 应答器 *-S -E -A*

RTR 应答器主要用来和源端建立连接，并对源端发出的检测报文进行回应，从而保证检测结果的正确。VoIP-jitter 实体、UDP-echo 实体需要和目的端建立连接，因此必须在目的端配置 RTR 应答器。

配置条件

在配置 RTR 应答器前，首先完成以下任务：

使能 RTR。

配置 RTR 应答器

表 69-11 配置 RTR 应答器

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 RTR 应答器	rtr responder	必选 缺省情况下，未配置 RTR 应答器

69.2.5 配置 RTR 调度器

-S -E -A

RTR 调度器就是对 RTR 实体或组进行调度检测的策略。RTR 调度器可以以单个实体成员为对象，也可以以一个 RTR 实体组为对象，但不能同时以组和实体一起为对象。RTR 调度器以调度 ID 为唯一标识，和具体的 RTR 实体类型无关，但调度间隔必须考虑要调度的 RTR 实体或 RTR 实体组内成员的相关属性。RTR 调度器提供了丰富的调度策略，可以选择马上开始调度或隔一段时间后开始调度，甚至可以设定调度开始的绝对时间。另外，调度器可以在调度设定次数后自动消亡，也可以一直存在。

配置条件

在配置 RTR 调度器前，首先完成以下任务：

配置好需要调度的 RTR 实体或 RTR 实体组。

配置 RTR 调度器

表 69-12 配置 RTR 调度器

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 RTR 调度器， 调度某个实体或组	rtr schedule <i>schedule-id</i> { entity <i>entity-id</i> group <i>group-id</i> } start { <i>hh:mm</i> [<i>:ss</i>] <i>date month year</i> after <i>hh:mm</i> [<i>:ss</i>] now } ageout <i>ageout-time</i> life { forever <i>life-time</i> } repeat <i>repeat-times</i> }	必选 缺省情况下，未配置 RTR 调度器

说明：

- rtr 调度器的老化时间必需大于其调度对象的调度间隔，否则调度完一次以后，调度器会因为老化超时被删除。

69.2.6 配置暂停调度实体 **-S -E -A**

对处于正在调度的实体，可以配置暂停调度该实体。

配置条件

在配置暂停实体调度前，首先完成以下任务：

实体处于调度状态。

配置暂停调度实体

表 69-13 配置暂停实体调度

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置暂停调度实体	rtr <i>entity-id</i> halt	可选 缺省情况下，不暂停处于调度状态的停实体

说明：

- 只有单个实体才能配置 **rtr halt**，如果实体是 RTR 实体组的成员将不能配置 **rtr halt**
- 配置 **rtr halt** 后，如果在调度周期结束前仍然没有配置 **rtr resume**，调度该实体的调度器会因为老化超时而删除

69.2.7 配置恢复调度实体 **-S -E -A**

对处于暂停调度状态的实体，可以配置恢复调度实体。

配置条件

在配置恢复调度实体前，首先完成以下任务：

- 实体处于暂停调度状态。

配置暂停调度实体

表 69-14 配置暂停实体调度

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置恢复调度实体	rtr <i>entity-id</i> resume	可选

69.2.8 SLA 监控与维护

-S -E -A

表 69-15 SLA 监控与维护

命令	说明
show rtr entity [<i>entity-id</i>]	显示 RTR 实体的信息
show rtr group [<i>group-id</i>]	显示 RTR 实体组的信息
show rtr history <i>entity-id</i>	显示指定 RTR 实体的历史记录信息
show rtr schedule [<i>schedule-id</i>]	显示 RTR 调度器的信息

69.3 SLA 典型配置举例

69.3.1 配置 ICMP-echo 实体检测网络基本通信情况

-S -E -A

网络需求

- Device1 上使用 ICMP-echo 实体，检测 Device1 到 Device3 的网络基本通信情况。

网络拓扑



图 69-1 配置 ICMP-echo 实体组网图

配置步骤

- 步骤 1：配置 VLAN，并将端口加入对应的 VLAN。（略）
- 步骤 2：配置各接口的 IP 地址、路由，使 Device1 和 Device3 互通。（略）
- 步骤 3：配置 ICMP-echo 类型的实体，并添加属性参数。

#配置 Device1。

```

Device1#config terminal
Device1(config)#rtr enable
Device1(config)#rtr 1 icmpecho
Device1(config-rtr-icmpecho)#set 132.1.1.1 5 70 2 12 extend 131.1.1.1 0 TRUE FALSE
Device1(config-rtr-icmpecho)#alarm-type log
Device1(config-rtr-icmpecho)#number-of-history-kept 255
Device1(config-rtr-icmpecho)#threshold-pktLoss 10 direction be
Device1(config-rtr-icmpecho)#threshold-rtt 1000 direction be
Device1(config-rtr-icmpecho)#exit
  
```

#查看 ICMP-echo 实体参数。

```

Device1#show rtr entity 1
-----
ID:1      name:IcmpEcho1      Created:TRUE
*****type:ICMPECHO*****
CreatedTime:WED OCT 31 14:49:31 2012
LatestModifiedTime:WED OCT 31 14:53:53 2012
Times-of-schedule:0
TargetIp:132.1.1.1
Transmit-packets:5
Totally-send-packets:0
Packet-size:70
Timeout:2(s)
Alarm-type:log
Threshold-of-rtt:1000(ms) direction:be
Threshold-of-packet-loss:10 direction:be
Number-of-history-kept:255
Periods:1
Extend parameters:
sourceIp:131.1.1.1  tos:0  DF(DON'T FRAG):TRUE  Verify-data:FALSE
In-scheduling:FALSE
  
```

Schedule frequency:12(s)
Status:DEFAULT

结果显示实体参数与配置一致。

In-scheduling:FALSE 说明实体未进行调度。

Status:DEFAULT 说明实体状态为 DEFAULT。

说明：

- 实体在未调度时，状态为 DEFAULT；实体调度时，若实体可达，状态为 REACHABLE，不可达状态则为 UNREACHABLE。
-

步骤 4： 调度已定义的 ICMP-echo 实体，定义调度的各属性参数。

#配置 Device1

```
Device1(config)#rtr schedule 1 entity 1 start now ageout 100 life forever
```

步骤 5： 检验结果。

1) 当 Device1 到 Device3 的网络连通性正常时。

#查看实体状态。

```
Device1#show rtr entity 1
-----
ID:1      name:IcmpEcho1      Created:TRUE
*****type:ICMPECHO*****
CreatedTime:WED OCT 31 14:49:31 2012
LatestModifiedTime:WED OCT 31 14:53:53 2012
Times-of-schedule:1
Time-of-last-schedule:WED OCT 31 14:54:07 2012
TargetIp:132.1.1.1
Transmit-packets:5
Totally-send-packets:5
Packet-size:70
Timeout:2(s)
Alarm-type:log
Threshold-of-rtt:1000(ms) direction:be
Threshold-of-packet-loss:10 direction:be
Number-of-history-kept:255
Periods:1
Extend parameters:
sourceIp:131.1.1.1  tos:0  DF(DON'T FRAG):TRUE  Verify-data:FALSE
In-scheduling:TRUE
```

```
Schedule frequency:12(s)
Status:REACHABLE
```

In-scheduling:TRUE 说明实体处于调度中;

Status:REACHABLE 说明实体状态为可达,即 Device1 到 Device3 的网络连通正常。

2) 当 Device1 到 Device3 的网络连通性出现故障时。

因实体参数配置了告警模式为 log, 故网络不通时设备上打印告警信息, 如下:

```
Oct 31 14:54:46: [tRtrIcmpRcv]Rtr 1 (ICMPECHO) rtt [9000ms] was exceeded(>=) threshold [1000ms].
```

#查看实体状态。

```
Device1#show rtr entity 1
-----
ID:1      name:IcmpEcho1      Created:TRUE
*****type:ICMPECHO*****
CreatedTime:WED OCT 31 14:49:31 2012
LatestModifiedTime:WED OCT 31 14:53:53 2012
Times-of-schedule:4
Time-of-last-schedule:WED OCT 31 14:54:43 2012
TargetIp:132.1.1.1
Transmit-packets:5
Totally-send-packets:20
Packet-size:70
Timeout:2(s)
Alarm-type:log
Threshold-of-rtt:1000(ms) direction:be
Threshold-of-packet-loss:10 direction:be
Number-of-history-kept:255
Periods:1
Extend parameters:
sourceIp:131.1.1.1  tos:0  DF(DON'T FRAG):TRUE  Verify-data:FALSE
In-scheduling:TRUE
Schedule frequency:12(s)
Status:UNREACHABLE
```

In-scheduling:TRUE 说明实体处于调度中。

Status:UNREACHABLE 说明实体状态为不可达,即 Device1 到 Device3 的网络连通性不可达。

#查看历史记录内容。

```
Device1#show rtr history 1
-----
ID:1 Name:IcmpEcho1 CurHistorySize:4 MaxHistorysize:255
History recorded as following:
WED OCT 31 14:54:46 2012
  PktLoss:5 ,Rtt:invalid
WED OCT 31 14:54:32 2012
  PktLoss:0 ,Rtt:11 (ms)
WED OCT 31 14:54:20 2012
  PktLoss:0 ,Rtt:2 (ms)
WED OCT 31 14:54:07 2012
  PktLoss:0 ,Rtt:2 (ms)
```

历史记录中详细记录了每次调度的丢包和时延情况；Rtt 为 invalid 表明网络中出现了故障导致网络不可达。

69.3.2 配置 ICMP-path-echo 实体检测网络通信情况

-S -E -A

网络需求

- Device1 上使用 ICMP-path-echo 实体，检测 Device1 到 Device3 的路径网络通信情况。

网络拓扑



图 69-2 配置 ICMP-path-echo 实体组网图

配置步骤

- 步骤 1： 配置 VLAN，并将端口加入对应的 VLAN。（略）
- 步骤 2： 配置各接口的 IP 地址、路由，使 Device1、Device2、Device3 互通。（略）
- 步骤 3： 配置 ICMP-path-echo 类型的实体，并添加属性参数。

#配置 Device1。

```

Device1#config terminal
Device1(config)#rtr enable
Device1(config)#rtr 1 icmp-path-echo
Device1(config-rtr-icmppathecho)#set dest-ipaddr 192.0.0.2 source-ipaddr 110.1.0.1
Device1(config-rtr-icmppathecho)#number-of-history-kept 255
Device1(config-rtr-icmppathecho)#targetOnly false
Device1(config-rtr-icmppathecho)#exit
  
```

查看 ICMP-path-echo 实体参数。

```

Device1#show rtr entity 1
-----
ID:1      name:IcmpPathEcho1      Created:TRUE
*****type:ICMPPATHECHO*****
CreatedTime:WED OCT 24 10:18:02 2012
LatestModifiedTime:WED OCT 24 10:19:09 2012
Times-of-schedule:0
TargetIp:192.0.0.2
SourceIp:110.1.0.1
Transmit-packets:1 (each hop)
Request-data-size:70
  
```

```

Timeout:5000(ms)
Frequency:60(s)
TargetOnly:FALSE
Verify-data:FALSE
Alarm-type:none
Threshold-of-rtt:9000(ms) direction:be
Threshold-of-pktloss:1 direction:be
Number-of-history-kept:255
Periods:1
In-scheduling:FALSE
Status:DEFAULT
-----

```

结果显示实体参数与配置一致。

In-scheduling:FALSE 说明实体未进行调度。

Status:DEFAULT 说明实体状态为 DEFAULT。

步骤 4: 调度已定义的 ICMP-path-echo 实体, 定义调度的各属性参数。

#配置 Device1。

```
Device1(config)#rtr schedule 1 entity 1 start now ageout 100 life 600 repeat 10
```

步骤 5: 检验结果。

#查看实体状态。

```

Device1#show rtr entity 1
-----
ID:1      name:IcmpPathEcho1      Created:TRUE
*****type:ICMPPATHECHO*****
CreatedTime:WED OCT 24 10:18:02 2012
LatestModifiedTime:WED OCT 24 10:19:09 2012
Times-of-schedule:1
Time-of-last-schedule:WED OCT 24 10:20:01 2012
TargetIp:192.0.0.2
SourceIp:110.1.0.1
Transmit-packets:1 (each hop)
Request-data-size:70
Timeout:5000(ms)
Frequency:60(s)
TargetOnly:FALSE
Verify-data:FALSE
Alarm-type:none
Threshold-of-rtt:9000(ms) direction:be
Threshold-of-pktloss:1 direction:be
Number-of-history-kept:255
Periods:1
In-scheduling:TRUE
Status:REACHABLE

```

In-scheduling:TRUE 说明实体处于调度中。

Status:REACHABLE 说明实体状态为可达，即 Device1 到 Device3 的网络路径连通正常。

#查看历史记录内容。

```
Device1#show rtr history 1
-----
ID:1 Name:IcmpPathEcho1
History of hop-by-hop:
110.1.0.2 PktLoss:0 ,Rtt:2 (ms)
192.0.0.2 PktLoss:0 ,Rtt:1 (ms)
History of record from source to dest:
CurHistorySize:1 MaxHistorysize:255
WED OCT 24 10:20:01 2012
PktLoss:0 ,Rtt:1 (ms)
```

历史记录中详细记录了每次调度的丢包和时延情况。

#等待一段时间，进行 10 次调度后查看实体状态。

```
Device1#show rtr entity 1
-----
ID:1 name:IcmpPathEcho1 Created:TRUE
*****type:ICMPPATHECHO*****
CreatedTime:WED OCT 24 10:18:02 2012
LatestModifiedTime:WED OCT 24 10:19:09 2012
Times-of-schedule:10
Time-of-last-schedule:WED OCT 24 10:29:01 2012
TargetIp:192.0.0.2
SourceIp:110.1.0.1
Transmit-packets:1 (each hop)
Request-data-size:70
Timeout:5000(ms)
Frequency:60(s)
TargetOnly:FALSE
Verify-data:FALSE
Alarm-type:none
Threshold-of-rtt:9000(ms) direction:be
Threshold-of-pktloss:1 direction:be
Number-of-history-kept:255
Periods:1
In-scheduling:FALSE
Status:DEFAULT
```

等待 10 次调度后，调度停止，实体状态为 DEFAULT。

69.3.3 配置 ICMP-path-jitter 实体检测网络通信情况 **-S -E -A**

网络需求

- Device1 上使用 ICMP-path-jitter 实体，检测 Device1 到 Device3 的路径网络通信情况。

网络拓扑

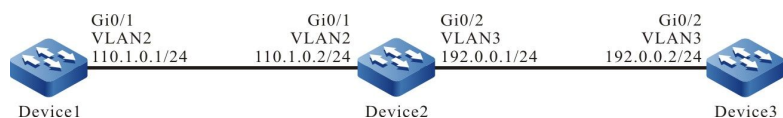


图 69-3 配置 ICMP-path-jitter 实体组网图

配置步骤

- 步骤 1: 配置 VLAN，并将端口加入对应的 VLAN。（略）
- 步骤 2: 配置各接口的 IP 地址、路由，使 Device1、Device2、Device3 互通。（略）
- 步骤 3: 配置 ICMP-path-jitter 类型的实体，并添加属性参数。

#配置 Device1。

```

Device1#config terminal
Device1(config)#rtr enable
Device1(config)#rtr 1 icmp-path-jitter
Device1(config-rtr-icmppathjitter)#set dest-ipaddr 192.0.0.2 10 20 source-ipaddr 110.1.0.1
Device1(config-rtr-icmppathjitter)#number-of-history-kept 255
Device1(config-rtr-icmppathjitter)#targetOnly false
Device1(config-rtr-icmppathjitter)#exit
  
```

#查看 ICMP-path-jitter 实体参数。

```

Device1#show rtr entity 1
-----
ID:1      name:IcmpPathJitter1      Created:TRUE
*****type:ICMPATHJITTER*****
CreatedTime:WED OCT 24 10:54:31 2012
LatestModifiedTime:WED OCT 24 10:56:12 2012
Times-of-schedule:0
TargetIp:192.0.0.2
SourceIp:110.1.0.1
Transmit-packets:10 (each hop)
Packets-interval:20(ms)
Request-data-size:70
Timeout:5000(ms)
Frequency:60(s)
TargetOnly:FALSE
Verify-data:FALSE
Alarm-type:none
Threshold-of-rtt:9000(ms) direction:be
Threshold-of-pktLoss: 200000000 direction:be
Threshold-of-jitter:6000(ms) direction:be
Number-of-history-kept:255
Periods:1
In-scheduling:FALSE
Status:DEFAULT
-----
  
```

结果显示实体参数与配置一致。

In-scheduling:FALSE 说明实体未进行调度。

Status:DEFAULT 说明实体状态为 DEFAULT。

步骤 4: 调度已定义的 ICMP-path-jitter 实体, 定义调度的各属性参数。

#配置 Device1。

```
Device1(config)#rtr schedule 1 entity 1 start now ageout 100 life foreve
```

步骤 5: 检验结果。

#查看实体状态。

```
Device1#show rtr entity 1
-----
ID:1      name:IcmpPathJitter1      Created:TRUE
*****type:ICMPATHJITTER*****
CreatedTime:WED OCT 24 10:54:31 2012
LatestModifiedTime:WED OCT 24 10:56:12 2012
Times-of-schedule:4
Time-of-last-schedule:WED OCT 24 11:00:25 2012
TargetIp:192.0.0.2
SourceIp:110.1.0.1
Transmit-packets:10 (each hop)
Packets-interval:20(ms)
Request-data-size:70
Timeout:5000(ms)
Frequency:60(s)
TargetOnly:FALSE
Verify-data:FALSE
Alarm-type:none
Threshold-of-rtt:9000(ms) direction:be
Threshold-of-pktLoss: 200000000 direction:be
Threshold-of-jitter:6000(ms) direction:be
Number-of-history-kept:255
Periods:1
In-scheduling:TRUE
Status:REACHABLE
-----
```

In-scheduling:TRUE 说明实体处于调度中。

Status:REACHABLE 说明实体状态可达, 即 Device1 到 Device2 的网络连通正常。

#查看历史记录内容。

```
Device1#show rtr history 1
-----
ID:1 Name:IcmpPathJitter1
History of hop-by-hop:
110.1.0.2 PktLoss:0 Rtt:1 (ms),Jitter:0 (ms)
192.0.0.2 PktLoss:0 Rtt:0 (ms),Jitter:0 (ms)
History of record from source to dest:
CurHistorySize:4 MaxHistorysize:255
WED OCT 24 11:00:25 2012
PktLoss:0 ,Rtt:1 (ms),Jitter:0 (ms)
WED OCT 24 10:59:25 2012
PktLoss:0 ,Rtt:0 (ms),Jitter:0 (ms)
```



```

WED OCT 24 10:58:25 2012
  PktLoss:0      ,Rtt:0      (ms),Jitter:0      (ms)
WED OCT 24 10:57:25 2012
  PktLoss:0      ,Rtt:0      (ms),Jitter:0      (ms)
-----

```

历史记录中详细记录了每次调度的丢包、时延和抖动情况。

69.3.4 配置 VoIP-jitter 实体检测网络传输语音报文的情况 -S -E -A

网络需求

- Device1 上使用 VoIP-jitter 实体，检测 Device1 到 Device3 网络传输语音报文的情况。

网络拓扑



图 69-4 配置 VoIP-jitter 实体组网图

配置步骤

步骤 1： 配置 VLAN，并将端口加入对应的 VLAN。（略）

步骤 2： 配置各接口的 IP 地址、路由，使 Device1 和 Device3 互通。（略）

步骤 3： 配置 ntp，进行时钟同步。

#配置 Device3。

```

Device3#config terminal
Device3(config)#ntp master

```

#配置 Device1。

```

Device1(config)#ntp server 192.0.0.2

```

#查看 Device3 成功作为时钟服务器端，提示时钟已被同步。

```

Device3#show ntp status
Current NTP status information
Clock is synchronized, stratum 8, reference is 127.127.8.10
reference time is D4321EF4.7BBBBB68 (08:01:56.483 Wed Oct 24 2012)

```

#查看 Device1 成功作为时钟客户端，提示时钟已被同步，并显示服务器端地址。

```
Device1#show ntp status
Current NTP status information
Clock is synchronized, stratum 9, reference is 192.0.0.2
reference time is D43222C1.91110F31 (08:18:09.566 Wed Oct 24 2012)
```

步骤 4: 在 Device3 上配置 responder，作为 responder 端。

#配置 Device3

```
Device3(config)#rtr enable
Device3(config)#rtr responder
```

步骤 5: 在 Device1 上配置 VoIP-jitter 实体，并添加属性参数。

#配置 Device1。

```
Device1#config terminal
Device1(config)#rtr enable
Device1(config)#rtr 1 jitter
Device1(config-rtr-jitter)#set dest-ipaddr 192.0.0.2 dest-port 1234 g711alaw source-ipaddr 110.1.0.1 source-
port 1234
Device1(config-rtr-jitter)#number-of-history-kept 255
Device1(config-rtr-jitter)#exit
```

#查看实体参数。

```
Device1#show rtr entity 1
-----
ID:1      name:Jitter1      Created:TRUE
*****type:JITTER*****
CreatedTime:WED OCT 24 16:02:32 2012
LatestModifiedTime:WED OCT 24 16:02:58 2012
Times-of-schedule:0
Entry-state:Pend
TargetIp:192.0.0.2  targetPort:1234
Codec:G.711 A-Law  Packet-size:172 Packet-number:1000
Packet-transmit-interval:20(ms)
frequency:60(s)
SourceIp:110.1.0.1  Soure-port:1234
TimeOut:50000(ms)
Alarm-type:none
Threshold-of-dsDelay:5000(ms) direction:be
Threshold-of-dsJitter:6000(ms) direction:be
Threshold-of-dsPktLoss:200000000 direction:be
Threshold-of-sdDelay:5000(ms) direction:be
Threshold-of-sdJitter:6000(ms) direction:be
Threshold-of-sdPktLoss:200000000 direction:be
Threshold-of-rtt:9000(ms) direction:be
Threshold-of-mos:10000000 direction:be
Threshold-of-icpif:100000000 direction:be
Number-of-history-kept:255
Periods:1
Status:DEFAULT
-----
```

结果显示实体参数与配置一致。

Status:DEFAULT 说明实体状态为 DEFAULT。

步骤 6: 调用已定义的 VoIP-jitter 实体, 定义调度的各属性参数。

#配置 Device1。

```
Device1(config)#rtr schedule 1 entity 1 start now ageout 100 life 600 repeat 10
```

步骤 7: 检验结果。

#查看实体状态。

```
Device1#show rtr entity 1
-----
ID:1      name:Jitter1      Created:TRUE
*****type:JITTER*****
CreatedTime:WED OCT 24 16:02:32 2012
LatestModifiedTime:WED OCT 24 16:06:02 2012
Times-of-schedule:3
Time-of-last-schedule:WED OCT 24 16:08:29 2012
Entry-state:Transmit
TargetIp:192.0.0.2  targetPort:1234
Codec:G.711 A-Law  Packet-size:172 Packet-number:1000
Packet-transmit-interval:20(ms)
frequency:60(s)
SourceIp:110.1.0.1  Soure-port:1234
TimeOut:50000(ms)
Alarm-type:none
Threshold-of-dsDelay:5000(ms) direction:be
Threshold-of-dsJitter:6000(ms) direction:be
Threshold-of-dsPktLoss:200000000 direction:be
Threshold-of-sdDelay:5000(ms) direction:be
Threshold-of-sdJitter:6000(ms) direction:be
Threshold-of-sdPktLoss:200000000 direction:be
Threshold-of-rtt:9000(ms) direction:be
Threshold-of-mos:10000000 direction:be
Threshold-of-icpif:100000000 direction:be
Number-of-history-kept:255
Periods:1
Status:REACHABLE
-----
```

Entry-state:Transmit 表明实体处于调度中。

Status:REACHABLE 表明实体状态为可达,说明 Device1 到 Device3 的网络正常传输语音报文。

#查看历史记录内容。

```
Device1#show rtr history 1
-----
ID:1 Name:Jitter1 CurHistorySize:3 MaxHistorysize:255
History recorded as following:
```

```

WED OCT 24 16:08:46 2012
  SdPktLoss:0      ,DsPktLoss:0      ,Rtt:185      (ms),
  SdDelay:14      (ms),DsDelay:178    (ms),SdJitter:8      (ms),DsJitter:183    (ms),
  Mos:5.000000    ,icpif:0.000000
WED OCT 24 16:07:45 2012
  SdPktLoss:0      ,DsPktLoss:0      ,Rtt:14      (ms),
  SdDelay:16      (ms),DsDelay:7      (ms),SdJitter:10     (ms),DsJitter:13     (ms),
  Mos:5.000000    ,icpif:0.000000
WED OCT 24 16:06:46 2012
  SdPktLoss:0      ,DsPktLoss:0      ,Rtt:17      (ms),
  SdDelay:16      (ms),DsDelay:9      (ms),SdJitter:11     (ms),DsJitter:13     (ms),
  Mos:5.000000    ,icpif:0.000000
-----
    
```

历史记录中详细记录了每次调度的单向丢包、往返时延、单向时延、单向抖动情况。

说明：

- VoIP-jitter 实体在配置之前，需要配置 NTP 服务实现网络时钟同步，并且需要在目的端配置 rtr responder 命令，作为响应端。注意，若未进行时钟同步或未配置 responder 端，调度结果会不正确。

69.3.5 配置 UDP-echo 实体检测网络传输 UDP 报文的情况 -S -E -A

网络需求

- Device1 上使用 UDP-echo 实体，检测 Device1 到 Device3 网络传输 UDP 报文的情况。

网络拓扑

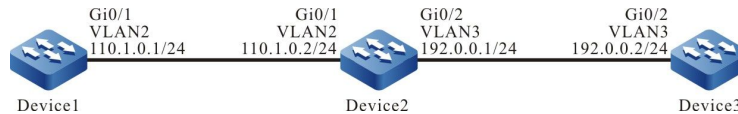


图 69-5 配置 UDP-echo 实体组网图

配置步骤

- 步骤 1：配置 VLAN，并将端口加入对应的 VLAN。（略）
- 步骤 2：配置各接口的 IP 地址、路由，使 Device1 和 Device3 互通。（略）

步骤 3： 在 Device3 上配置 responder，作为 responder 端。

#配置 Device3

```
Device3#config terminal
Device3(config)#rtr enable
Device3(config)#rtr responder
```

步骤 4： 在 Device1 上配置 UDP-echo 实体，并添加属性参数。

#配置 Device1。

```
Device1#config terminal
Device1(config)#rtr enable
Device1(config)#rtr 1 udpecho
Device1(config-rtr-udpecho)#set dest-ipaddr 192.0.0.2 dest-port 1001 source-ipaddr 110.1.0.1 source-port
1001
Device1(config-rtr-udpecho)#number-of-history-kept 255
Device1(config-rtr-udpecho)#frequency 10
Device1(config-rtr-udpecho)#exit
```

#查看实体参数。

```
Device1#show rtr entity 1
-----
ID:1      name:UdpEcho1      Created:TRUE
*****type:UDPECHO*****
CreatedTime:WED OCT 24 16:36:45 2012
LatestModifiedTime:WED OCT 24 16:37:44 2012
Times-of-schedule:0
Entry-state:Pend
TargetIp:192.0.0.2  TargetPort:1001
SourceIp:110.1.0.1  SourePort:1001
TimeOut:5000(ms)
request-data-size:16
Frequency:10(s)
Alarm-type:none
Threshold-of-rtt:9000(ms) direction:be
Threshold-of-pktloss:1 direction:be
Number-of-history-kept:255
Periods:1
Status:DEFAULT
-----
```

结果显示实体参数与配置一致。

Status:DEFAULT 说明实体状态为 DEFAULT。

步骤 5： 调用已定义的 UDP-echo 实体，定义调度的各属性参数。

#配置 Device1。

```
Device1(config)#rtr schedule 1 entity 1 start now ageout 100 life forever
```

配置手册

发布 1.1 04/2020

步骤 6: 检验结果。

#查看实体状态。

```
Device1#show rtr entity 1
-----
ID:1      name:UdpEcho1      Created:TRUE
*****type:UDPECHO*****
CreatedTime:WED OCT 24 16:36:45 2012
LatestModifiedTime:WED OCT 24 16:37:44 2012
Times-of-schedule:5
Time-of-last-schedule:WED OCT 24 16:39:50 2012
Entry-state:Pend
TargetIp:192.0.0.2   TargetPort:1001
SourceIp:110.1.0.1   SourePort:1001
TimeOut:5000(ms)
request-data-size:16
Frequcy:10(s)
Alarm-type:none
Threshold-of-rtt:9000(ms) direction:be
Threshold-of-pktloss:1 direction:be
Data-pattern:ABCD
Number-of-history-kept:255
Periods:1
Status:REACHABLE
-----
```

Status:REACHABLE 表明实体状态为可达,即 Device1 到 Device3 的网络正常传输 UDP 报文。

#查看历史记录内容。

```
Device1#show rtr history 1
-----
ID:1 Name:UdpEcho1 CurHistorySize:5   MaxHistorysize:255
History recorded as following:
WED OCT 24 16:39:54 2012
    PktLoss:0 ,Rtt:1 (ms)
WED OCT 24 16:39:44 2012
    PktLoss:0 ,Rtt:1 (ms)
WED OCT 24 16:39:33 2012
    PktLoss:0 ,Rtt:2 (ms)
WED OCT 24 16:39:23 2012
    PktLoss:0 ,Rtt:2 (ms)
WED OCT 24 16:39:13 2012
    PktLoss:0 ,Rtt:2 (ms)
-----
```

历史记录中详细记录了每次调度的丢包、时延情况。

说明:

- UDP-echo 实体在配置之前,需要在目的端配置 rtr responder 命令,作为响应端。
注意:若未配置 responder 端,调度结果会不正确。

69.3.6 配置 FLOW-statistics 实体检测接口流量

-S -E -A

网络需求

- Device1 上使用 FLOW-statistics 实体，检测接口 vlan2 流量。

网络拓扑

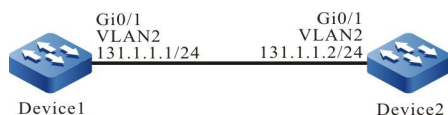


图 69-6 配置 FLOW-statistics 实体组网图

配置步骤

步骤 1： 配置各接口的 IP 地址。（略）

步骤 2： 在 Device1 上配置 FLOW-statistics 实体，并添加属性参数。

#配置 Device1。

```

Device1#config terminal
Device1(config)#rtr enable
Device1(config)#rtr 1 flow-statistics
Device1(config-rtr-flowsta)#flow-statistics interface vlan 2 interval 60
Device1(config-rtr-flowsta)#number-of-history-kept 255
Device1(config-rtr-flowsta)#exit
  
```

#查看实体参数。

```

Device1#show rtr entity 1
-----
ID:1      name:flow-statistics1      Created:TRUE
*****type:FLOWSTATISTICS*****
CreatedTime:THU OCT 25 09:57:43 2012
LatestModifiedTime:THU OCT 25 09:58:03 2012
Times-of-schedule:0
Alarm-type:none
Threshold-of-inputPkt:200000000 direction:be
Threshold-of-inputFlow:200000000 direction:be
Threshold-of-outputPkt:200000000 direction:be
Threshold-of-outputFlow:200000000 direction:be
Interface: vlan2
Statistics-interval:60(s)
Number-of-history-kept:255
Periods:1
  
```

```
Status:DEFAULT
-----
```

结果显示实体参数与配置一致。

Status: DEFAULT 说明实体状态为 DEFAULT。

步骤 3: 调用已定义的 FLOW-statistics 实体, 定义调度的各属性参数。

#配置 Device1。

```
Device1(config)#rtr schedule 1 entity 1 start now ageout 100 life 600 repeat 10
```

步骤 4: 检验结果。

1) 当接口 vlan2 上有接收的数据流量时。

#查看实体状态。

```
Device1#show rtr entity 1
-----
ID:1      name:flow-statistics1      Created:TRUE
*****type:FLOWSTATISTICS*****
CreatedTime:THU OCT 25 09:57:43 2012
LatestModifiedTime:THU OCT 25 09:58:03 2012
Times-of-schedule:2
Time-of-last-schedule:THU OCT 25 10:02:11 2012
Alarm-type:none
Threshold-of-inputPkt:200000000 direction:be
Threshold-of-inputFlow:200000000 direction:be
Threshold-of-outputPkt:200000000 direction:be
Threshold-of-outputFlow:200000000 direction:be
Interface: vlan 2
Statistics-interval:60(s)
Number-of-history-kept:255
Periods:1
Status:REACHABLE
-----
```

Status: REACHABLE 表明实体状态为可达, 即有数据报文进/出 vlan2 接口。

2) 当接口 vlan2 上没有进/出接口的数据流量时。

#查看实体状态。

```
Device1#show rtr entity 1
-----
ID:1      name:flow-statistics1      Created:TRUE
*****type:FLOWSTATISTICS*****
CreatedTime:THU OCT 25 09:57:43 2012
LatestModifiedTime:THU OCT 25 09:58:03 2012
Times-of-schedule:5
Time-of-last-schedule:THU OCT 25 10:05:11 2012
Alarm-type:none
Threshold-of-inputPkt:200000000 direction:be
Threshold-of-inputFlow:200000000 direction:be
Threshold-of-outputPkt:200000000 direction:be
```



```

Threshold-of-outputFlow:200000000 direction:be
Interface: vlan 2
Statistics-interval:60(s)
Number-of-history-kept:255
Periods:1
Status:UNREACHABLE
-----

```

Status: UNREACHABLE 表明无流量进/出接口 vlan2 时，实体状态为不可达。

#查看历史记录内容。

```

Device1#show rtr history 1
-----
ID:1      Name:flow-statistics1 CurHistorySize:5 MaxHistorysize:255
History recorded as following:
THU OCT 25 10:05:11 2012
  Input pkt:0      (packets/s),Input flow:0      (bits/s),
  Output pkt:0     (packets/s),Output flow:0     (bits/s)
THU OCT 25 10:04:11 2012
  Input pkt:209    (packets/s),Input flow:214000 (bits/s),
  Output pkt:0     (packets/s),Output flow:0     (bits/s)
THU OCT 25 10:03:11 2012
  Input pkt:8460   (packets/s),Input flow:8663000 (bits/s),
  Output pkt:0     (packets/s),Output flow:0     (bits/s)
THU OCT 25 10:02:11 2012
  Input pkt:8460   (packets/s),Input flow:8663000 (bits/s),
  Output pkt:0     (packets/s),Output flow:0     (bits/s)
THU OCT 25 10:01:12 2012
  Input pkt:6456   (packets/s),Input flow:6610000 (bits/s),
  Output pkt:0     (packets/s),Output flow:0     (bits/s)
-----

```

历史记录中详细记录了每次调度进、出接口 vlan2 的速率（基于个数和基于 bit）情况。

说明：

- FLOW-statistics 实体的可达性定义为：实体处于调度中，只要接口 IN 或 OUT 方向有流量，则实体状态为 REACHEABLE，无流量则为 UNREACHABLE。

69.3.7 配置 TRACK 与 SLA 联动 **-S -E -A**

网络需求

- TRACK 与 SLA 联动，通过实体状态对 Device1 上静态路由的有效性做判断。

网络拓扑

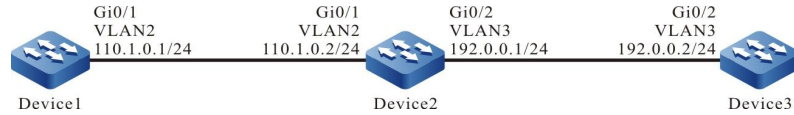


图 69-7 配置 TRACK 与 SLA 联动组网图

配置步骤

- 步骤 1: 配置 VLAN, 并将端口加入对应的 VLAN。 (略)
- 步骤 2: 配置各接口的 IP 地址。 (略)
- 步骤 3: 在 Device1 上配置 ICMP-echo 实体检测 Device1 到 Device2 的网络连通性, 并将实体加入实体组。

#配置 Device1。

```
Device1#config terminal
Device1(config)#rtr enable
Device1(config)#rtr 1 icmpecho
Device1(config-rtr-icmpecho)#set 110.1.0.2 5 70 2 12 extend 110.1.0.1 0 true false
Device1(config-rtr-icmpecho)#number-of-history-kept 255
Device1(config-rtr-icmpecho)#exit
Device1(config)#rtr group 1
Device1(config-rtr-group)#member 1
Device1(config-rtr-group)#exit
```

- 步骤 4: 定义 TRACK, 关联 SLA。

#配置 Device1。

```
Device1(config)#track 1
Device1(config-track)#rtr 1
```

- 步骤 5: 添加静态路由, 关联 TRACK。

#配置 Device1。

```
Device1(config)#ip route 192.0.0.0 255.255.255.0 110.1.0.2 track 1
```

- 步骤 6: 调度实体, 并检查静态路由的有效性。

#配置 Device1。

```
Device1(config)#rtr schedule 1 group 1 start now ageout 100 life forever
```

步骤 7: 检验结果。**1) 当 Device1 到 Device2 的网络连通性正常时。****#查看实体组状态。**

```
Device1#show rtr group 1
-----
ID:1      name:rtrGroup1    Members schedule interval:0
Option: AND  Status:REACHABLE
*****
type:SINGLE  Entity Id :1
```

实体组状态为 REACHEABLE.。

#在 Device1 的路由表中查看网段 192.0.0.0/24 的路由。

```
Device1#show ip route 192.0.0.0
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set

S   192.0.0.0/24 [1/10] via 110.1.0.2, 00:00:09, vlan2
```

结果显示有到网段 192.0.0.0/24 的路由，说明当实体组状态为 RECHABLE 时，判定静态路由有效。

2) 当 Device1 到 Device2 的网络连通性出现故障时。**#查看实体组状态。**

```
Device1#show rtr group 1
-----
ID:1      name:rtrGroup1    Members schedule interval:0
Option: AND  Status:UNREACHABLE
*****
type:SINGLE  Entity Id :1
```

实体组状态为 UNREACHEABLE.。

#在 Device1 的路由表中查看网段 192.0.0.0/24 的路由。

```
Device1#show ip route 192.0.0.2
Codes: C - connected, S - static, R - RIP, O - OSPF, OE-OSPF External, M - Management
       D - Redirect, E - IRMP, EX - IRMP external, o - SNSP, B - BGP, i-ISIS

Gateway of last resort is not set
```

结果显示没有到网段 192.0.0.0/24 的路由，说明当实体状态为 UNREACHABLE 时，判定静态路由无效。

70 NTP

70.1 NTP 简介

网络时间协议 NTP (Network Time Protocol) 是用于互联网中时间同步的标准互联网协议。NTP 的用途是把设备的时间同步到标准时间。目前采用的时间标准是世界标准时间 UTC (Universal Time Coordinated) 。

NTP 的设计充分考虑了互联网上时间同步的复杂性。NTP 提供的机制严格、实用、有效，适应于在各种规模、速度的互联网环境。NTP 不仅校正现行时间，而且持续跟踪时间的变化，能够自动进行调节，即使网络发生故障，也能维持时间的稳定。NTP 产生的网络开销较小，并具有保证网络安全的措施。这些措施的采用使 NTP 可以在互联网上获取可靠和精确的时间同步。

在实际应用中，应根据网络部署情况选择适当的 NTP 工作模式，以满足不同情况下的网络时钟同步需求。NTP 支持以下三种工作模式：

- 客户端/服务器模式

在客户端/服务器模式中，客户端向服务器发送 Mode 字段为 3 (客户模式) 的时钟同步报文，服务器收到报文后会自动工作在服务器模式，并发送 Mode 字段为 4 (服务器模式) 的应答报文，客户端收到应答报文后对系统时钟进行同步。在该模式下，客户端能从服务器同步时钟，而服务器无法从客户端同步时钟。

- 对等体模式

在对等体模式中，主动对等体和被动对等体之间首先交互 Mode 字段为 3（客户端模式）和 4（服务器模式）的 NTP 报文。之后，主动对等体向被动对等体发送 Mode 字段为 1（主动对等体模式）的时钟同步报文，被动对等体收到报文后自动工作在被动对等体模式，并发送 Mode 字段为 2（被动对等体模式）的时钟同步报文。经过报文的交互，对等体模式建立起来。在该模式下，主动对等体和被动对等体之间可以互相同步时钟。如果双方的时钟都已经同步，则以层数小的时钟为准。

- 广播模式

在广播模式中，广播服务器周期性地向广播地址 255.255.255.255 发送 Mode 字段为 5（广播服务器模式）的时钟同步报文，广播客户端侦听来自广播服务器的广播报文。当广播客户端接收到第一个广播报文后，广播客户端与广播服务器交互 Mode 字段为 3（客户端模式）和 4（服务器模式）的 NTP 报文，以获得广播客户端与广播服务器之间的网络延迟。之后，广播客户端继续侦听广播报文并根据接收的广播报文对系统时钟进行同步。

70.2 NTP 功能配置

表 70-1 NTP 功能配置列表

配置任务	
配置 NTP 基本功能	配置 NTP 客户端/服务器模式
	配置 NTP 对等体模式
	配置 NTP 广播模式
配置 NTP 可选参数	配置 NTP 参考时钟
	配置 NTP 报文的源接口
	配置 NTP 报文收发控制
	配置 NTP 动态会话的数目

配置任务	
配置 NTP 认证功能	配置 NTP 客户端/服务器模式认证
	配置 NTP 对等体模式认证
	配置 NTP 广播模式认证
配置 NTP 访问控制	配置 NTP 访问控制

70.2.1 配置 NTP 基本功能

-B -S -E -A

配置条件

配置 NTP 基本功能，首先完成以下任务：

- 配置接口的网络层地址，使 NTP 时钟服务请求端和时钟服务提供端之间网络层可达。
- NTP 时钟服务提供端使能了 NTP。

配置 NTP 客户端/服务器模式

当使用 NTP 客户端/服务器模式时，在服务器上不需要专门配置，但需要保证服务器的时钟为同步状态且时钟层数小于客户端的时钟层数。

在 NTP 客户端上需要进行如下配置。

表 70-2 配置 NTP 客户端

步骤	命令	说明
进入全局配置模式	configure terminal	-
指定 NTP 服务器	ntp server [vrf vrf-name] { ip-address domain-name } [version version key key-number source interface-name]	必选 缺省情况下，没有指定 NTP 服务器

说明：

- *ip-address* 参数是一个单播地址，不能为广播地址、组播地址或本设备 IP 地址。
- 通过 **source interface-name** 指定客户端报文发送源接口后，该接口的主 IP 地址将被设置为客户端发送报文的源 IP 地址。
- 如果在服务器上指定了发送报文的源接口，则客户端配置的服务器 IP 地址必须与这个源接口的 IP 地址相同，否则，客户端将无法正确处理服务器回应的报文，导致不能同步时钟。
- 可以通过多次配置 **ntp server** 命令指定多个服务器，最多可指定 64 个服务器。

配置 NTP 对等体模式

当使用 NTP 对等体模式时，在被动对等体上不需要专门配置，但需要保证被动对等体能够收发 NTP 报文，这可以通过在被动对等体上配置 **ntp master** 命令或“4.2.1 配置 NTP 基本功能”中的任何一条 NTP 命令来使能 NTP。

在 NTP 主动对等体上需要进行如下配置。

表 70-3 配置 NTP 主动对等体

步骤	命令	说明
进入全局配置模式	configure terminal	-
指定 NTP 被动对等体	ntp peer [vrf vrf-name] { ip-address domain-name } [version version key key-number source interface-name]	必选 缺省情况下，没有指定 NTP 被动对等体

说明：

- *ip-address* 参数是一个单播地址，不能为广播地址、组播地址或本设备 IP 地址。
- 通过 **source interface-name** 指定主动对等体报文发送源接口后，该接口的主 IP 地址将被设置为主动对等体发送报文的源 IP 地址。
- 如果在被动对等体上指定了发送报文的源接口，则主动对等体配置的服务器 IP 地址必须与这个源接口的 IP 地址相同，否则，主动对等体将无法正确处理被动对等体发送的报文，导致不能同步时钟。
- 可以通过多次配置 **ntp peer** 命令指定多个被动对等体，最多可指定 64 个被动对等体。

配置 NTP 广播模式

当使用 NTP 广播模式时，在广播服务器和广播客户端都需要进行配置，且需要保证广播服务器的时钟为同步状态且时钟层数小于广播客户端的时钟层数。由于广播服务器上需要指定一个发送 NTP 广播报文的接口，广播客户端上也需要指定一个接收 NTP 广播报文的接口，所以广播模式的配置只能在具体的接口模式下进行。

在 NTP 广播客户端上需要进行如下配置。

表 70-4 配置 NTP 广播客户端

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface interface-name	-
接口启用 NTP 广播客户端	ntp broadcast client	必选 缺省情况下，接口未启用 NTP 广播客户端

在 NTP 广播服务器上需要进行如下配置。

表 70-5 配置 NTP 广播服务器

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入接口配置模式	interface <i>interface-name</i>	-
接口启用 NTP 广播服务器	ntp broadcast [key <i>key-number</i> version <i>version-number</i>]	必选 缺省情况下，接口未启用 NTP 广播服务器

说明：

- 可以通过多次配置 **ntp broadcast client** 命令启用多个接口的广播客户端，最多可启用 32 个接口的广播客户端。
- 可以通过多次配置 **ntp broadcast** 命令启用多个接口的广播服务器，最多可启用 32 个接口的广播服务器。

70.2.2 配置 NTP 可选参数

-B -S -E -A

配置条件

无

配置 NTP 参考时钟

NTP 可以通过下面两种方式进行系统时间同步：

- 与本地时钟进行同步：即采用本地时钟作为 NTP 参考时钟。
- 与网络中的其他时钟源进行同步：即使用前述三种 NTP 工作模式中的任何一种。

表 70-6 配置本地时钟为 NTP 参考时钟

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置本地时钟为 NTP 参考时钟	ntp master [stratum-number]	必选 缺省情况下，未配置本地时钟为 NTP 参考时钟

说明：

- 配置本地时钟为 NTP 参考时钟后，NTP 不能从网络中的其他时钟源同步时钟。
- 配置本地时钟为 NTP 参考时钟后，本地设备可以作为时钟源同步网络中的其他设备。请谨慎使用本配置，以免导致网络中其他设备的时钟错误。

配置 NTP 报文的源接口

如果配置了 NTP 报文的源接口，当设备主动发送 NTP 报文时，将选择该指定源接口的主 IP 地址作为报文的源 IP 地址。

表 70-7 配置 NTP 报文的源接口

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 NTP 报文的源接口	ntp source interface-name	必选 缺省情况下，未配置 NTP 报文的源接口

说明：

- 如果使用命令 `ntp server` 或 `ntp peer` 指定了源接口，那么优先使用命令 `ntp server` 或 `ntp peer` 指定的源接口。
- 如果在接口模式下配置了 `ntp broadcast`，则 NTP 广播报文的源接口为配置了上述命令的接口。
- 如果指定的 NTP 报文的源接口处于 `down` 状态，则不发送 NTP 报文。
- 如果指定的 NTP 报文的源接口没有配置地址且处于 `up` 状态，则发送的 NTP 报文源 IP 地址为该报文出接口的主 IP 地址。

配置 NTP 报文收发控制

缺省情况下设备会接收和发送所有 NTP 报文。可以通过配置 NTP 报文收发控制，禁止接收和发送 NTP 报文。

表 70-8 配置 NTP 报文收发控制

步骤	命令	说明
进入全局配置模式	configure terminal	-
禁止接收和发送 NTP 报文	no ntp enable	必选 缺省情况下，未禁止接收和发送 NTP 报文

配置 NTP 动态会话的数目

通过配置 NTP 动态会话的数目，设置本地允许建立的最大 NTP 动态连接数目。

表 70-9 配置 NTP 动态会话的数目

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
设置本地允许建立的最大 NTP 动态连接数目	ntp max-dynamic-sessions <i>number</i>	必选 缺省情况下，允许建立的动态 NTP 会话的数目为 100

70.2.3 配置 NTP 认证功能 **-B -S -E -A**

在一些安全性要求较高的网络中，运行 NTP 协议时需要启用认证功能。通过对 NTP 时钟服务请求端和时钟服务提供端的交互报文进行认证，保证时钟服务请求端同步到合法的时间，提高了网络安全性。

配置条件

配置 NTP 认证功能，首先完成以下任务：

- 配置接口的网络层地址，使 NTP 时钟服务请求端和时钟服务提供端之间网络层可达。
- NTP 时钟服务提供端使能了 NTP。

配置 NTP 客户端/服务器模式认证

配置 NTP 客户端/服务器模式认证时，需要在客户端和服务器上都启用认证功能、配置认证密钥、将认证密钥设为受信密钥，并在客户端上指定与服务器关联的密钥。

在 NTP 客户端上需要进行如下配置。

表 70-10 配置 NTP 客户端认证

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
启用 NTP 认证功能	ntp authenticate	必选 缺省情况下, 未启用 NTP 认证功能
配置认证密钥	ntp authentication-key <i>key-number</i> md5 <i>key</i>	必选 缺省情况下, 未配置认证密钥
配置指定密钥为受信密钥	ntp trusted-key <i>key-number</i>	必选 缺省情况下, 未指定受信密钥
指定与服务器关联的密钥	ntp server [vrf <i>vrf-name</i>] { <i>ip-address</i> <i>domain-name</i> } [version <i>version</i> source <i>interface-name</i>] key <i>key-number</i>	必选

在 NTP 服务器上需要进行如下配置。

表 70-11 配置 NTP 服务器认证

步骤	命令	说明
进入全局配置模式	configure terminal	-
启用 NTP 认证功能	ntp authenticate	必选 缺省情况下, 未启用 NTP 认证功能
配置认证密钥	ntp authentication-key <i>key-number</i> md5 <i>key</i>	必选

步骤	命令	说明
		缺省情况下，未配置认证密钥
配置指定密钥为受信密钥	ntp trusted-key <i>key-number</i>	必选 缺省情况下，未指定受信密钥

说明：

- 服务器和客户端需要配置相同的认证密钥。
- 客户端可以将不存在的密钥与服务器关联。但是若想成功启用认证功能，则必须在关联密钥后，配置该密钥，并将其指定为受信密钥。

配置 NTP 对等体模式认证

配置 NTP 对等体模式认证时，需要在主动对等体和被动对等体上都启用认证功能、配置认证密钥、将认证密钥设为受信密钥，并在主动对等体上指定与被动对等体关联的密钥。

在 NTP 主动对等体上需要进行如下配置。

表 70-12 配置 NTP 主动对等体认证

步骤	命令	说明
进入全局配置模式	configure terminal	-
启用 NTP 认证功能	ntp authenticate	必选 缺省情况下，未启用 NTP 认证功能
配置认证密钥	ntp authentication-key <i>key-number</i> md5 <i>key</i>	必选

步骤	命令	说明
		缺省情况下，未配置认证密钥
配置指定密钥为受信密钥	ntp trusted-key <i>key-number</i>	必选 缺省情况下，未指定受信密钥
指定与被动对等体关联的密钥	ntp peer [<i>vrf vrf-name</i>] <i>ip-address</i> <i>domain-name</i> [version <i>version</i>] source <i>interface-name</i>] key <i>key-number</i>	必选

在 NTP 被动对等体上需要进行如下配置。

表 70-13 配置 NTP 被动对等体认证

步骤	命令	说明
进入全局配置模式	configure terminal	-
启用 NTP 认证功能	ntp authenticate	必选 缺省情况下，未启用 NTP 认证功能
配置认证密钥	ntp authentication-key <i>key-number</i> md5 <i>key</i>	必选 缺省情况下，未配置认证密钥
配置指定密钥为受信密钥	ntp trusted-key <i>key-number</i>	必选 缺省情况下，未指定受信密钥

说明：

- 主动对等体和被动对等体需要配置相同的认证密钥。
- 主动对等体可以将不存在的密钥与被动对等体关联。但是若想成功启用认证功能，则必须在关联密钥后，配置该密钥，并将其指定为受信密钥。

配置 NTP 广播模式认证

配置 NTP 广播模式认证时，需要在广播客户端和广播服务器上都启用认证功能、配置认证密钥、将认证密钥设为受信密钥，并在广播服务器上指定与该广播服务器关联的密钥。

在 NTP 广播客户端上需要进行如下配置。

表 70-14 配置 NTP 广播客户端认证

步骤	命令	说明
进入全局配置模式	configure terminal	-
启用 NTP 认证功能	ntp authenticate	必选 缺省情况下，未启用 NTP 认证功能
配置认证密钥	ntp authentication-key key-number md5 key	必选 缺省情况下，未配置认证密钥
配置指定密钥为受信密钥	ntp trusted-key key-number	必选 缺省情况下，未指定受信密钥

在 NTP 广播服务器上需要进行如下配置。

表 70-15 配置 NTP 广播服务器认证

步骤	命令	说明
进入全局配置模式	configure terminal	-
启用 NTP 认证功能	ntp authenticate	必选 缺省情况下，未启用 NTP 认证功能
配置认证密钥	ntp authentication-key <i>key-number</i> md5 <i>key</i>	必选 缺省情况下，未配置认证密钥
配置指定密钥为受信密钥	ntp trusted-key <i>key-number</i>	必选 缺省情况下，未指定受信密钥
进入接口配置模式	interface <i>interface-name</i>	-
指定与广播服务器关联的密钥	ntp broadcast [version <i>version-number</i>] key <i>key-number</i>	必选

说明：

- 广播服务器和广播客户端需要配置相同的认证密钥。
- 广播服务器可以将不存在的密钥与该广播服务器关联。但是若想成功启用认证功能，则必须在关联密钥后，配置该密钥，并将其指定为受信密钥。

70.2.4 配置 NTP 访问控制

-B -S -E -A

配置条件

配置手册

发布 1.1 04/2020

1465

配置 NTP 访问控制，首先完成以下任务：

- 配置与访问控制关联的 ACL。

配置 NTP 访问控制

NTP 可以通过与 ACL 进行关联的方式，来限制对本地 NTP 服务的访问。

表 70-16 配置 NTP 访问控制

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 NTP 访问控制	ntp access-group peer <i>access-list-number</i>	必选 缺省情况下，未配置 NTP 访问控制

70.2.5 NTP 监控与维护

-B -S -E -A

表 70-17 NTP 监控与维护

命令	说明
show ntp associations	显示 NTP 会话信息
show ntp status	显示 NTP 状态信息

70.3 NTP 典型配置举例

70.3.1 配置 NTP 服务器端与客户端

-B -S -E -A

网络需求

- Device1 为 NTP 服务器端，Device2 为 NTP 客户端。
- Device1 与 Device2 通过各自的接口互联，路由可达。
- NTP 服务器端为时钟源，客户端从服务器端获取时钟。

网络拓扑

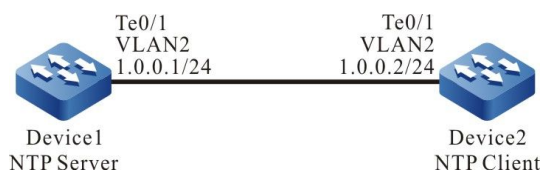


图 70-1 配置 NTP 服务器端与客户端组网图

配置步骤

步骤 1：配置 VLAN，并将端口加入对应的 VLAN。（略）

步骤 2：配置各接口的 IP 地址。（略）

步骤 3：配置 NTP 服务器端 Device1。

#配置设备本地时钟为参考时钟，时钟层数为 3。

```
Device1#configure terminal
Device1(config)#ntp master 3
Device1(config)#exit
```

步骤 4：配置 NTP 客户端 Device2。

#配置 Device2 为北京时区。

```
Device2#configure terminal
Device2(config)#clock timezone BEIJING +8
```

#指定 NTP 服务器 Device1，IP 地址为 1.0.0.1。

```
Device2(config)#ntp server 1.0.0.1
Device2(config)#exit
```

步骤 5：检验结果。

#在客户端 Device2 上执行 **show ntp status** 命令，查看时钟同步状态等信息，表明客户端与 NTP 服务器端 Device1 已经同步，时钟层数比 Device1 的大 1，为 4。

```
Device2#show ntp status
Current NTP status information
Clock is synchronized, stratum 4, reference is 1.0.0.1
reference time is D442EB0E.432F29BD (01:49:02.262 Tue Nov 06 2012)
```

#在客户端 Device2 上执行 **show clock** 命令查看设备时钟。

```
Device2#show clock
BEIJING(UTC+08:00) TUE NOV 06 09:49:30 2012
```

70.3.2 配置 NTP 服务器端与多级客户端 -B -S -E -A

网络需求

- Device1 为 NTP 服务器端，Device2、Device3 为 NTP 客户端。
- Device2 分别与 Device1、Device3 互联，且路由可达。
- Device1 为 Device2 提供时钟，Device2 为 Device3 提供时钟。

网络拓扑



图 70-2 配置 NTP 服务器端与多级客户端组网图

配置步骤

- 步骤 1：配置 VLAN，并将端口加入对应的 VLAN。（略）
- 步骤 2：配置各接口的 IP 地址。（略）
- 步骤 3：配置 NTP 服务器端 Device1。

#配置设备本地时钟为参考时钟，时钟层数为 3。

```
Device1#configure terminal
Device1(config)#ntp master 3
```

步骤 4: 配置 NTP 客户端 Device2。

#配置 Device2 为北京时区。

```
Device2#configure terminal
Device2(config)#clock timezone BEIJING +8
```

#指定 NTP 服务器端 Device1, IP 地址为 1.0.0.1。

```
Device2(config)#ntp server 1.0.0.1
```

步骤 5: 配置 NTP 客户端 Device3。

#配置 Device3 为北京时区。

```
Device3#configure terminal
Device3(config)#clock timezone BEIJING +8
```

#指定 NTP 服务器端 Device2, IP 地址为 2.0.0.1。

```
Device3(config)#ntp server 1.0.0.1
```

步骤 6: 检验结果, 分别在 Device2、Device3 上查看时钟同步信息。

#在客户端 Device2 上执行 **show ntp status** 命令, 查看时钟同步状态等信息, 表明 Device2 与 NTP 服务器端 Device1 已经同步, 时钟层数比 Device1 的大 1, 为 4。

```
Device2#show ntp status
Current NTP status information
Clock is synchronized, stratum 4, reference is 1.0.0.1
reference time is D44CC35E.BAA6A190 (13:02:22.729 Tue Nov 13 2012)
```

#在客户端 Device2 上执行 **show clock** 命令查看设备时钟。

```
Device2#show clock
BEIJING(UTC+08:00) TUE NOV 13 21:02:24 2012
```

#在客户端 Device3 上执行 **show ntp status** 命令, 查看时钟同步状态等信息, 表明 Device3 与 Device2 已经同步, 时钟层数比 Device2 的大 1, 为 5。

```
Device3#show ntp status
Current NTP status information
Clock is synchronized, stratum 5, reference is 2.0.0.1
reference time is D44CC365.5CC8C4C8 (13:02:29.362 Tue Nov 13 2012)
```

#在客户端 Device3 上执行 **show clock** 命令查看设备时钟。

```
Device3#show clock  
  
BEIJING(UTC+08:00) TUE NOV 13 21:02:36 2012
```

70.3.3 配置带 MD5 认证的 NTP 服务器端与客户端

-B -S -E -A

网络需求

- Device1 为 NTP 服务器端，Device2 为 NTP 客户端，双方用 MD5 算法认证。
- Device1 与 Device2 通过各自的接口互联，路由可达。
- NTP 服务器端为时钟源，客户端从服务器端获取时钟。

网络拓扑

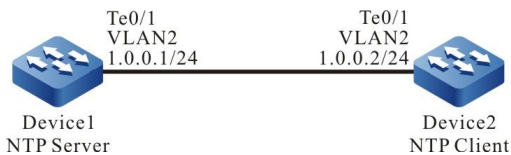


图 70-3 配置带 MD5 认证的 NTP 服务器端与客户端组网图

配置步骤

步骤 1： 配置 VLAN，并将端口加入对应的 VLAN。（略）

步骤 2： 配置各接口的 IP 地址。（略）

步骤 3： 配置 NTP 服务器端。

#配置设备本地时钟为参考时钟，时钟层数为 3。

```
Device1#configure terminal  
Device1(config)#ntp master 3
```

#启用认证。

```
Device1(config)#ntp authenticate
```

#配置认证密钥序号为 1，算法为 MD5，密钥为 admin。

```
Device1(config)#ntp authentication-key 1 md5 admin
```

#配置序号为 1 的密钥受信任。

```
Device1(config)#ntp trusted-key 1
```

步骤 4: 配置 NTP 客户端。

#配置 Device2 为北京时区。

```
Device2#configure terminal
Device2(config)#clock timezone BEIJING +8
```

#为客户端指定 NTP 服务器, IP 地址为 1.0.0.1。

```
Device2(config)#ntp server 1.0.0.1 key 1
```

#启用认证。

```
Device2(config)#ntp authenticate
```

#配置认证密钥序号为 1, 算法为 MD5, 密钥为 admin。

```
Device2(config)#ntp authentication-key 1 md5 admin
```

#配置序号为 1 的密钥受信任。

```
Device2(config)#ntp trusted-key 1
```

步骤 5: 检验结果。

#在客户端 Device2 上执行 **show ntp status** 命令, 查看时钟同步状态等信息, 表明客户端与 NTP 服务器端 Device1 已经同步, 时钟层数比 Device1 的大 1, 为 4。

```
Device2#show ntp status
Current NTP status information
Clock is synchronized, stratum 4, reference is 1.0.0.1
reference time is D442ECE1.8BB7B219 (01:56:49.545 Tue Nov 06 2012)
```

#在 Device2 上执行 **show clock** 命令查看设备时钟。

```
Device2#show clock
BEIJING(UTC+08:00) TUE NOV 06 09:56:52 2012
```

注意:

- NTP 客户端与服务器的认证序号必须相同, 密钥必须相同。
-

70.3.4 配置 NTP 对等体模式

-B -S -E -A

网络需求

- Device1 、 Device2、 Device3 通过各自的接口互联，路由可达。
- Device1 设置本地时钟作为参考时钟，层数为 3。
- Device2 为 NTP 客户端， 设置 Device1 为 NTP 服务器。
- Device3 设置 Device2 为对等体， Device3 为主动对等体， Device2 为被动对等体。

网络拓扑

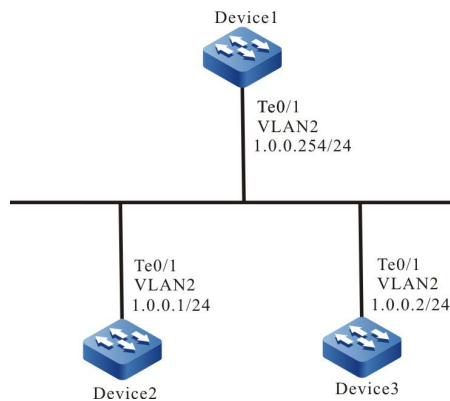


图 70-4 配置 NTP 对等体模式组网图

配置步骤

步骤 1: 配置各接口的 IP 地址。（略）

步骤 2: Device1 设置本地时钟为参考时钟，层数为 3。

```
Device1#configure terminal
Device1(config)#ntp master 3
```

步骤 3: Device2 指定 Device1 为 NTP 服务器。

#配置 Device2 为北京时区。

```
Device2#configure terminal
Device2(config)#clock timezone BEIJING
```

#指定 NTP 服务器 IP 地址为 1.0.0.254。

```
Device2(config)#ntp server 1.0.0.254
```

步骤 4: Device3 将 Device2 设置为对等体。

#配置 Device3 为北京时区。

```
Device3#configure terminal
Device3(config)#clock timezone BEIJING
```

#指定 NTP 对等体 IP 地址为 1.0.0.1。

```
Device3(config)#ntp peer 1.0.0.1
```

步骤 5: 检验结果。

#在客户端 Device2 上执行 **show ntp status** 命令，查看时钟同步状态等信息。

```
Device2#show ntp status
```

```
Current NTP status information
```

```
Clock is synchronized, stratum 4, reference is 1.0.0.254
```

```
reference time is D8E9785D.221F1F5 (03:09:17.8 Tue Apr 28 2015)
```

Device2 时钟层数比 Device1 的大 1，为 4，参考的时钟服务器地址为 1.0.0.254；表明客户端 Device2 与服务器端 Device1 已经同步。

#在客户端 Device2 上执行 **show clock** 命令查看设备时钟。

```
Device2#show clock
```

```
BEIJING(UTC+08:00) TUE APR 28 11:10:36 2015
```

#在主动对等体 Device3 上执行 **show ntp status** 命令，查看时钟同步状态等信息。

```
Device3#show ntp status
```

Current NTP status information

Clock is synchronized, stratum 5, reference is 1.0.0.1

reference time is D8E9795C.29835CC9 (03:13:32.162 Tue Apr 28 2015)

Device3 时钟层数比 Device2 的大 1，为 5，参考的时钟服务器地址为 1.0.0.1；表明主动对等体 Device3 与被动对等体 Device2 已经同步。

#在客户端 Device3 上执行 **show clock** 命令查看设备时钟。

Device3#show clock

BEIJING(UTC+08:00) TUE APR 28 11:16:19 2015

70.3.5 配置 NTP 广播模式

-B -S -E -A

网络需求

- Device1、Device2、Device3 通过各自的接口互联，路由可达。
- Device1 设置本地时钟作为参考时钟，层数为 3。
- Device1 为 NTP 广播服务器，从 VLAN2 接口发送 NTP 广播报文。
- Device2、Device3 为 NTP 广播客户端，分别在各自的接口 VLAN2 上监听 NTP 广播报文。

网络拓扑

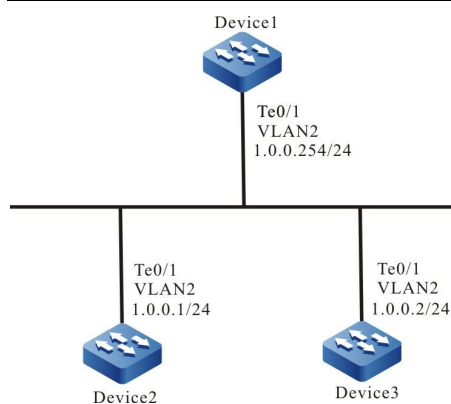


图 70-5 配置 NTP 广播模式组网图

配置步骤

步骤 1: 配置各接口的 IP 地址。（略）

步骤 2: Device1 设置本地时钟为参考时钟，层数为 3，配置 Device1 为 NTP 广播服务器，在接口 VLAN2 上发送 NTP 广播报文。

#配置本地时钟为参考时钟，时钟层数为 3。

```
Device1#configure terminal
Device1(config)#ntp master 3
```

#配置 Device1 为 NTP 广播服务器，在接口 VLAN2 上发送 NTP 广播报文。

```
Device1(config)#interface vlan2
Device1(config-if-vlan2)#ntp broadcast
```

步骤 3: 配置 Device2 为 NTP 广播客户端，在接口 VLAN2 监听 NTP 广播报文。

```
Device2#configure terminal
Device2(config)#interface vlan2
Device2(config-if-vlan2)#ntp broadcast client
```

步骤 4: 配置 Device3 为 NTP 广播客户端，在接口 VLAN2 上监听 NTP 广播报文。

```
Device3#configure terminal
Device3(config)#interface vlan2
Device3(config-if-vlan2)#ntp broadcast client
```

步骤 5: 检验结果。

#在客户端 Device2 上执行 **show ntp status** 命令, 查看时钟同步状态等信息。

```
Device2#show ntp status
```

```
Current NTP status information
```

```
Clock is synchronized, stratum 4, reference is 1.0.0.254
```

```
reference time is D8E97C99.5110D9FE (03:27:21.316 Tue Apr 28 2015)
```

Device2 时钟层数比 Device1 的大 1, 为 4, 参考的时钟服务器地址为 1.0.0.254;
表明客户端 Device2 与服务器端 Device1 已经同步。

#在客户端 Device2 上执行 **show clock** 命令查看设备时钟。

```
Device2#show clock
```

```
BEIJING(UTC+08:00) TUE APR 28 11:27:22 2015
```

#在客户端 Device3 上执行 **show ntp status** 命令, 查看时钟同步状态等信息。

```
Device3#show ntp status
```

```
Current NTP status information
```

```
Clock is synchronized, stratum 4, reference is 1.0.0.254
```

```
reference time is D8E97CAC.78F42CA6 (03:27:40.472 Tue Apr 28 2015)
```

Device3 时钟层数比 Device1 的大 1, 为 4, 参考的时钟服务器地址为 1.0.0.254;
表明客户端 Device3 与服务器端 Device1 已经同步。

#在客户端 Device3 上执行 **show clock** 命令查看设备时钟。

```
Device3#show clock
```

```
BEIJING(UTC+08:00) TUE APR 28 11:27:41 2015
```

70.3.6 配置 NTP 广播模式认证功能

-B -S -E -A**网络需求**

- Device1 、 Device2、 Device3 通过各自的接口互联，路由可达。
- Device1 设置本地时钟作为参考时钟，层数为 3。
- Device1 为 NTP 广播服务器，启用 NTP 认证，从 VLAN2 接口发送 NTP 广播报文。
- Device2、 Device3 为 NTP 广播客户端，启用 NTP 认证，分别在各自的接口 VLAN2 上监听 NTP 广播报文。

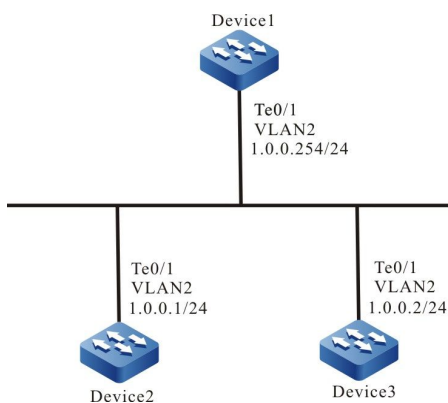
网络拓扑

图 70-6 配置 NTP 广播模式认证功能组网图

配置步骤

步骤 1： 配置各接口的 IP 地址。（略）

步骤 2： Device1 设置本地时钟为参考时钟，层数为 3，配置 Device1 为 NTP 广播服务器并配置 MD5 认证，在接口 VLAN2 上发送 NTP 广播报文。

#配置设备本地时钟为参考时钟，时钟层数为 3。

```
Device1#configure terminal
Device1(config)#ntp master 3
```

#启用认证。

配置手册

发布 1.1 04/2020

```
Device1(config)#ntp authenticate
```

#配置认证密钥序号为 1，算法为 MD5，密钥为 admin。

```
Device1(config)#ntp authentication-key 1 md5 admin
```

#配置序号为 1 的密钥受信任。

```
Device1(config)#ntp trusted-key 1
```

说明：

- NTP 客户端与服务器的认证序号必须相同，密钥必须相同。
-

#启用接口的 NTP 广播服务器，并指定与该广播服务器关联的密钥序号为 1。

```
Device1(config)#interface vlan2
```

```
Device1(config-if-vlan2)#ntp broadcast key 1
```

步骤 3： 配置 Device2 为 NTP 广播客户端并配置 MD5 认证，在接口 VLAN2 监听 NTP 广播报文。

#配置 Device2 为北京时区。

```
Device2#configure terminal
```

```
Device2(config)#clock timezone BEIJING
```

#启用认证。

```
Device2(config)#ntp authenticate
```

#配置认证密钥序号为 1，算法为 MD5，密钥为 admin。

```
Device2(config)#ntp authentication-key 1 md5 admin
```

#配置序号为 1 的密钥受信任。

```
Device2(config)#ntp trusted-key 1
```

#接口下配置 NTP 广播客户端。

```
Device2(config)#interface vlan2
```

```
Device2(config-if-vlan2)#ntp broadcast client
```

说明：

- 配置 NTP 广播模式认证功能时，需要在广播服务器上指定与该服务器关联的密钥序
-

号，在各个广播客户端上不需要指定。

步骤 4： 配置 Device3 为 NTP 广播客户端并配置 MD5 认证，在接口 VLAN2 监听 NTP 广播报文。

#配置 Device3 为北京时区。

```
Device3#configure terminal
Device3(config)#clock timezone BEIJING
```

#启用认证。

```
Device3(config)#ntp authenticate
```

#配置认证密钥序号为 1，算法为 MD5，密钥为 admin。

```
Device3(config)#ntp authentication-key 1 md5 admin
```

#配置序号为 1 的密钥受信任。

```
Device3(config)#ntp trusted-key 1
```

#接口下配置 NTP 广播客户端。

```
Device3(config)#interface vlan2
Device3(config-if-vlan2)#ntp broadcast client
```

说明：

- 配置 NTP 广播模式认证功能时，需要在广播服务器上指定与该服务器关联的密钥序号，在各个广播客户端上不需要指定。
-

步骤 5： 检验结果。

#在客户端 Device2 上执行 **show ntp status** 命令，查看时钟同步状态等信息。

```
Device2#show ntp status
Current NTP status information
Clock is synchronized, stratum 4, reference is 1.0.0.254
reference time is D90954DB.4DE52C7F (07:17:44.972 Fri May 22 2015)
```

Device2 的时钟层数比 Device1 的大 1，为 4；表明广播客户端与 NTP 广播服务器端 Device1 已经同步。

#在 Device2 上执行 **show clock** 命令查看设备时钟。

```
Device2#show clock
Beijing(UTC+08:00) FRI MAY 22 15:18:20 2015
```

#在客户端 Device3 上执行 **show ntp status** 命令，查看时钟同步状态等信息。

```
Device3#show ntp status

Current NTP status information

Clock is synchronized, stratum 4, reference is 1.0.0.254
reference time is D90957A2.1B393E2D (07:22:10.106 Fri May 22 2015)
```

Device3 的时钟层数比 Device1 的大 1，为 4；表明广播客户端与 NTP 广播服务器端 Device1 已经同步。

#在 Device3 上执行 **show clock** 命令查看设备时钟。

```
Device3#show clock
Beijing(UTC+08:00) FRI MAY 22 15:22:15 2015
```

71 端口镜像

71.1 端口镜像简介

71.1.1 端口镜像简介

端口镜像，又称为 SPAN (Switched Port Analyzer, 交换端口分析)，是用来监控设备端口数据流的一种管理方式。SPAN 包括本地 SPAN、远程 SPAN、封装的远程 SPAN、VLAN SPAN 四种。

71.1.2 基本概念 **-B -S -E -A**

SPAN 会话

SPAN 会话 (SPAN Session) 是指将设备一个或多个监控端口数据流镜像一份发送给目的端口。被镜像的数据流可以是输入数据流，也可以是输出数据流或者是同时镜像输入输出流。可以对处于关闭状态的端口配置 SPAN，此时的 SPAN 会话不生效，但只要相关的端口被打开，SPAN 即可生效。

本地 SPAN

本地 SPAN (Local SPAN) 支持在一台设备上的端口镜像，所有的监控端口和目的端口在同一台设备上。

远程 SPAN

远程 SPAN，又称为 RSPAN (Remote Switched Port Analyzer, 远程交换端口分析)，支持监控端口和目的端口不在同一台设备上，跨越二层网络实现远程监控。每个 RSPAN Session 在指定的 RSPAN VLAN，使镜像报文能够在二层网络中转发。RSPAN 包括 RSPAN Source Session(源会话)、RSPAN VLAN 和 RSPAN Destination Session(目的会话)，需要在不同的设备配置 RSPAN 源会话和 RSPAN 目的会话。配置 RSPAN 源会话时，需要指定一个或多个监控端口和一个或多个 RSPAN VLAN。监控端口镜像的数据发送到 RSPAN VLAN 中。在另一台设备配置 RSPAN 目的会话，需要指定目的端口和一个 RSPAN VLAN。RSPAN 目的会话将 RSPAN VLAN 数据发送到目的端口。

VLAN SPAN

VLAN SPAN 支持在一台设备上的 VLAN 镜像。将一个或多个监控 VLAN 数据流镜像一份发送给目的端口。被镜像的数据流可以是输入数据流，也可以是输出数据流或者是同时镜像输入输出流。

流量类型

流量类型 (Traffic Types) 分为三种, Receive (Rx) 监控端口的接收流量, Transmit (Tx)监控端口的转发流量, Both 监控端口的接收和转发流量。

SPAN 源端口

SPAN 源端口 (Source Port) , 也称为监控端口 (monitored port) , 它的数据被监控作为网络分析使用, 被监控的数据流既可以是输入方向、也可以是输出方向, 或者是双向。可以作用在不同的 VLAN 中。源端口可以是普通端口或汇聚组。一个源端口只能属于一个 SPAN 会话。

SPAN 目的端口

SPAN 目的端口 (Destination Port) 只能是单独的一个实际物理端口或汇聚组, 一个目的端口同时只能在一个 SPAN 会话中使用。目的端口可以是普通端口或汇聚组。

设备支持将目的端口作为普通转发端口, 但为了通用性, 并为了使监控的数据不被别的数据流干扰, 建议将目的端口从所有 VLAN 中删除。

说明:

- 目的端口不应连接到其他设备, 否则可能导致网络环路。
 - 目的端口不能再承载其他的业务。
 - 目的端口应大于等于监控端口的带宽, 否则可能会出现丢包的情况。
 - 目的端口不能启用 LACP(Link Aggregation Control Protocol, 链路汇聚控制协议) 或 802.1X 功能, 以避免镜像数据受到影响。
 - 单个会话目的端口数目最多能够支持 4 个, 根据芯片的不同, 不同板卡支持的目的端口数量可能不同。
-

RSPAN VLAN

RSPAN VLAN 应该是一个专门给 RSPAN 使用的空闲 VLAN。可在配置时选定一个空闲的 VLAN 即可, 但需要保证镜像端口到目的端口路径上的其他设备均配置了此 VLAN, 并将该路径上其他设备相应的端口加入此 VLAN。

71.2 SPAN 功能配置

表 71-1 SPAN 功能配置列表

配置任务	
配置 Local SPAN	配置 Local SPAN 会话
配置 RSPAN	配置 RSPAN VLAN
	配置 RSPAN 源会话
	配置 RSPAN 目的会话
配置 VLAN SPAN	配置 VLAN SPAN 会话

71.2.1 配置 Local SPAN *-B -S -E -A*

Local SPAN 用于分析本地设备端口的数据流。

配置条件

无

配置 Local SPAN 会话

Local SPAN 会话实现了复制一个或多个源端口收到或转发的报文，并从目的端口转发出去，同时不影响源端口的正常业务转发。

表 71-2 配置 Local SPAN 会话

步骤	命令	说明
进入全局配置模式	config terminal	-

步骤	命令	说明
配置 Local SPAN 会话源端	monitor session <i>session-number</i> source { interface <i>interface-list</i> link-aggregation <i>link-aggregation-id</i> } [both tx rx]	必选 缺省情况下，没有配置 Local SPAN 会话源端
配置 Local SPAN 会话目的端	monitor session <i>session-number</i> destination { interface <i>interface-name</i> link-aggregation <i>link-aggregation-id</i> }	必选 缺省情况下，没有配置 Local SPAN 会话目的端

说明：

- 在配置会话源端且指定开启镜像的端口为汇聚组时，所指定的汇聚组应该已经创建。若汇聚组没有创建，则配置失败。同理，在配置会话目的端且指定镜像报文转发端口为汇聚组时，所指定的汇聚组也必须已经创建。若汇聚组没有创建，则配置失败。
- 同一端口不能同时为同一会话的源端口和目的端口。
- 同一端口不能同时出现在多个会话中。

71.2.2 配置 RSPAN

-B -S -E -A

RSPAN 会话用于分析二层网络可达的远程设备的源端口的数据流。RSPAN 会话包括 RSPAN 源会话和 RSPAN 目的会话。

配置条件

无

配置 RSPAN VLAN

RSPAN 会话通过在镜像报文打上 RSPAN VLAN 标记，使镜像报文能够穿越二层网络。

表 71-3 配置 RSPAN VLAN

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入 VLAN 配置模式	vlan <i>vlan-id</i>	-
配置 VLAN 为 RSPAN VLAN	remote-span	必选 缺省情况下，没有配置 RSPAN VLAN

说明：

- RSPAN VLAN 不应承载其他业务，只能承载 RSPAN 流量。
- RSPAN VLAN 禁止开启 MAC 地址学习功能。
- 除了那些用于承载 RSPAN 流量的端口之外，不要将任何端口配置到 RSPAN VLAN 中。

配置 RSPAN 源会话

配置 RSPAN 源会话后，将镜像报文打上 RSPAN VLAN 标记，然后从 RSPAN 源会话的目的端口转发出去。

表 71-4 配置 RSPAN 源会话

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 RSPAN 源会话源端	monitor session <i>session-number</i> source { interface <i>interface-list</i> link-aggregation <i>link-aggregation-id</i> } [both tx rx]	必选 缺省情况下，没有配置 RSPAN 源会话源端
配置 RSPAN 源会话目的端	monitor session <i>session-number</i> destination remote vlan <i>vlan-id</i> interface <i>interface-name</i>	必选 缺省情况下，没有配置 RSPAN 源会话目的端

说明：

- 在配置会话源端且指定开启镜像的端口为汇聚组时，所指定的汇聚组应该已经创建。若汇聚组没有创建，则配置失败。
- 指定 VLAN 在 RSPAN 源会话之前必须设置为 RSPAN VLAN。
- 同一端口不能同时出现同一会话的源端和目的端。
- 同一端口不能同时出现在多个会话中。
- RSPAN 源会话目的端口只能是普通端口，不能是汇聚组。
- RSPAN 源会话只支持一个目的端口。

配置 RSPAN 目的会话

RSPAN 目的会话接收到报文时根据 RSPAN VLAN 标记识别镜像报文，将镜像报文转发到分析设备。

表 71-5 配置 RSPAN 目的会话

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 RSPAN 目的会话源端	monitor session <i>session-number</i> source remote vlan <i>vlan-id</i>	必选 缺省情况下, 没有配置 RSPAN 目的会话源端
配置 RSPAN 目的会话目的端	monitor session <i>session-number</i> destination { interface <i>interface-name</i> link-aggregation <i>link-aggregation-id</i> }	必选 缺省情况下, 没有配置 RSPAN 目的会话目的端

说明:

- 指定 VLAN 在 RSPAN 目的会话之前必须设置为 RSPAN VLAN。
- 同一端口不能同时出现在多个会话中。
- RSPAN 目的会话的目的端口的端口类型应为 Hybrid。

71.2.3 配置 VLAN SPAN **-B -S -E -A**

VLAN SPAN 会话用于分析指定 VLAN 的数据流。

配置条件

无

配置 VLAN SPAN 会话

VLAN SPAN 类似于 Local SPAN。VLAN SPAN 会话实现了复制一个或多个源 VLAN 收到或转发的报文，并从目的端口转发出去，同时不影响源 VLAN 的正常业务转发。

表 71-6 配置 VLAN SPAN 会话

步骤	命令	说明
进入全局配置模式	config terminal	-
配置 VLAN SPAN 会话源 VLAN	monitor session <i>session-number</i> source vlan [both tx rx]	必选 缺省情况下，没有配置 VLAN SPAN 会话源 VLAN
配置 VLAN SPAN 会话目的端	monitor session <i>session-number</i> destination interface <i>interface-name</i>	必选 缺省情况下，没有配置 VLAN SPAN 会话目的端

配置 VLAN SPAN 反射端口

VLAN SPAN 反射端口用于过滤流量，避免将不相关 VLAN 的流量镜像到目的端口。

表 71-7 配置 VLAN SPAN 反射端口

步骤	命令	说明
进入全局配置模式	config terminal	-
配置 VLAN SPAN 反射端口	monitor session <i>session-number</i> reflector-port interface <i>interface-name</i>	可选 缺省情况下，没有配置 VLAN SPAN 反射端口

说明：

- VLAN SPAN 会话的反射端口和目的端口不能是 VLAN SPAN 会话源 VLAN 的成员端口。
- VLAN SPAN 会话的目的端口只能是普通端口，不能是汇聚组。
- 同一端口不能同时为同一会话的反射端口和目的端口。
- VLAN SPAN 会话源 VLAN 成员端口不能同时出现在多个会话中。
- VLAN SPAN 会话的反射端口不能承载其他业务，只能被 VLAN SPAN 会话使用。
- 配置 VLAN SPAN 会话的源 VLAN 时，如果源 VLAN 的成员端口已经属于其他会话，则这些会话将主动删除这些端口。
- 系统只支持一个 VLAN SPAN 会话。

71.2.4 SPAN 监控与维护

-B -S -E -A

表 71-8 SPAN 监控与维护

命令	说明
show monitor rspan-vlan	显示 RSPAN VLAN
show monitor session { <i>session-number</i> all local remote }	显示 SPAN 会话配置信息

71.3 端口镜像典型配置举例

71.3.1 配置 Local SPAN *-B -S -E -A*

网络需求

- PC1、PC2 和 PC3 与 Device 相连，PC1 和 PC2 在 VLAN2 内通信。
- 在 Device 上配置 Local SPAN，源端口为 gigabitethernet0/1，目的端口为 gigabitethernet0/3，实现 PC3 对 Device 端口 gigabitethernet0/1 发送和接收到的报文进行监控。

网络拓扑

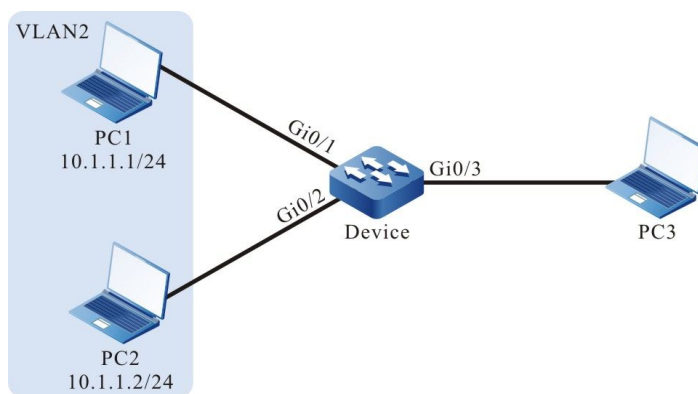


图 71-1 配置 Local SPAN 组网图

配置步骤

步骤 1： 配置 VLAN 及端口的链路类型。

#在 Device 上创建 VLAN2。

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#在 Device 上配置端口 gigabitethernet0/1 和端口 gigabitethernet0/2 的链路类型为 Access，允许 VLAN2 的业务通过。

```
Device(config)#interface gigabitethernet 0/1-0/2
Device(config-if-range)#switchport mode access
Device(config-if-range)#switchport access vlan 2
```

```
Device(config-if-range)#exit
```

步骤 2: 配置 Local SPAN。

#在 Device 上配置 Local SPAN，镜像源会话为端口 gigabitethernet0/1，目的会话为端口 gigabitethernet0/3。

```
Device(config)#monitor session 1 source interface gigabitethernet 0/1 both
Device(config)#monitor session 1 destination interface gigabitethernet 0/3
```

#在 Device 上查看 Local SPAN 的会话信息。

```
Device#show monitor session all
-----
Session 1
Type      : SPAN Local Session
Destination Interface : gigabitethernet0/3
Source Interface(both): gi0/1
```

步骤 3: 检验结果。

#PC1 与 PC2 之间相互通信时，在 PC3 上能捕获到端口 gigabitethernet0/1 发送和接收到的报文。

71.3.2 配置 RSPAN **-B -S -E -A**

网络需求

- PC1、PC2 与 Device1 相连，且在 VLAN2 内进行通信，PC3 与 Device2 相连。
- 在 Device1 和 Device2 上配置 RSPAN，实现 PC3 通过 RSPAN VLAN3 对 Device1 端口 gigabitethernet0/1 发送和接收到的报文进行监控。

网络拓扑

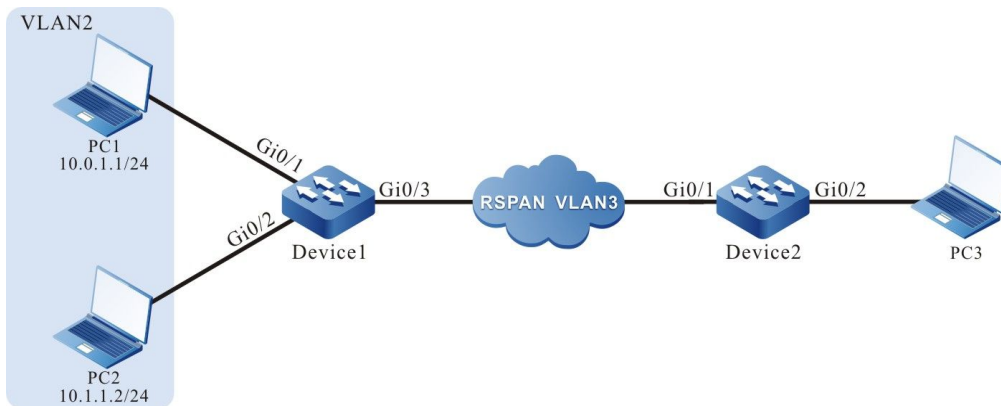


图 71-2 配置 RSPAN 组网图

配置步骤

步骤 1: 配置 VLAN 及端口的链路类型。

#在 Device1 上创建 VLAN2。

```
Device1#configure terminal
Device1(config)#vlan 2
Device1(config-vlan2)#exit
```

#在 Device1 上配置端口 gigabitethernet0/1 和端口 gigabitethernet0/2 的链路类型为 Access，允许 VLAN2 的业务通过。

```
Device1(config)#interface gigabitethernet 0/1-0/2
Device1(config-if-range)#switchport mode access
Device1(config-if-range)#switchport access vlan 2
Device1(config-if-range)#exit
```

#在 Device1 上配置端口 gigabitethernet0/3 的链路类型为 Trunk。

```
Device1(config)#interface gigabitethernet 0/3
Device1(config-if-gigabitethernet0/3)#switchport mode trunk
Device1(config-if-gigabitethernet0/3)#exit
```

#在 Device2 上配置端口 gigabitethernet0/1 的链路类型为 Trunk。

```
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#switchport mode trunk
Device2(config-if-gigabitethernet0/1)#exit
```

#在 Device2 上配置端口 gigabitethernet0/2 的链路类型为 Hybrid。

```
Device2(config)#interface gigabitethernet 0/2
Device2(config-if-gigabitethernet0/2)#switchport mode hybrid
Device2(config-if-gigabitethernet0/2)#exit
```

步骤 2: 在 Device1 和 Device2 上配置 RSPAN。

#在 Device1 上配置 VLAN3 为 RSPAN VLAN，并配置端口 gigabitethernet0/3 允许 VLAN3 的业务通过。

```
Device1(config)#vlan 3
Device1(config-vlan3)#remote-span
Device1(config-vlan3)#exit
Device1(config)#interface gigabitethernet 0/3
Device1(config-if-gigabitethernet0/3)#switchport trunk allowed vlan add 3
Device1(config-if-gigabitethernet0/3)#exit
```

#在 Device1 配置 RSPAN，镜像源会话为端口 gigabitethernet0/1，目的会话为端口 gigabitethernet0/3。

```
Device1(config)#monitor session 1 source interface gigabitethernet 0/1 both
Device1(config)#monitor session 1 destination remote vlan 3 interface gigabitethernet 0/3
```

#在 Device1 上查看 RSPAN 的会话信息。

```
Device1#show monitor session all
-----
Session 1
Type      : RSPAN Source Session
RSPAN VLAN : 3
Destination Interface : gigabitethernet0/3
Source Interface(both): gi0/1
```

#在 Device2 上配置 VLAN3 为 RSPAN VLAN，并配置端口 gigabitethernet0/1 允许 VLAN3 业务通过。

```
Device2(config)#vlan 3
Device2(config-vlan3)#remote-span
Device2(config-vlan3)#exit
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)# switchport trunk allowed vlan add 3
Device2(config-if-gigabitethernet0/1)#exit
```

#在 Device2 配置 RSPAN，镜像源会话为 RSPAN VLAN3，目的会话为端口 gigabitethernet0/2。

```
Device2(config)#monitor session 1 source remote vlan 3
Device2(config)#monitor session 1 destination interface gigabitethernet 0/2
```

#在 Device2 上查看 RSPAN 的会话信息。

```
Device2#show monitor session all
-----
Session 1
Type      : RSPAN Destination Session
RSPAN VLAN : 3
Destination Interface : gigabitethernet0/2
```

步骤 3: 检验结果。

#PC1 与 PC2 之间相互通信时, 在 PC3 上能捕获到 Device1 端口 gigabitethernet0/1 发送和接收到的报文。

71.3.3 配置 VLAN SPAN *-B -S -E -A*

网络需求

- PC1、PC2 和 PC3 与 Device 相连, PC1 和 PC2 在 VLAN2 内通信。
- 在 Device 上配置 VLAN SPAN, 源 vlan 为 vlan2, 反射端口为 gigabitethernet0/4, 目的端口为 gigabitethernet0/3, 实现 PC3 对 Device 的 vlan2 的发送和接收到的报文进行监控。

网络拓扑

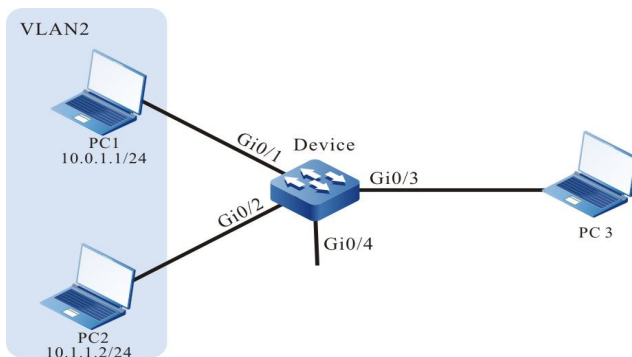


图 71-3 配置 VLAN SPAN 组网图

配置步骤

步骤 1: 配置 VLAN 及端口的链路类型。

#在 Device 上创建 VLAN2。

```
Device#configure terminal
Device(config)#vlan 2
Device(config-vlan2)#exit
```

#在 Device 上配置端口 gigabitethernet0/1 和端口 gigabitethernet0/2 的链路类型为 Trunk，允许 VLAN2 的业务通过。

```
Device(config)#interface gigabitethernet 0/1-0/2
Device(config-if-range)#switchport mode trunk
Device(config-if-range)# switchport trunk allowed vlan add 2
Device(config-if-range)#exit
```

步骤 2： 配置 VLAN SPAN。

#在 Device 上配置 VLAN SPAN，镜像源会话为 VLAN 2，反射端口为 gigabitethernet0/4，目的会话为端口 gigabitethernet0/3。

```
Device(config)#monitor session 1 source vlan 2 both
Device(config)#monitor session 1 reflector-port interface gigabitethernet0/4
Device(config)# monitor session 1 destination interface gigabitethernet0/3
Device#show monitor session all
-----
Session 1
Type      : SPAN Local VLAN Session
Reflector Interface : gi0/4
Destination Interface : gi0/3
Source VLAN(both): 2
```

步骤 3： 检验结果。

#PC1 与 PC2 之间相互通信时，在 PC3 上能捕获到 VLAN 2 发送和接收到的报文。

72 sFlow

72.1 sFlow 简介

sFlow，是一种用于网络流量采样和监控的技术，遵循 RFC3176 标准。sFlow 根据不同的配置进行不同方式的采样，采样的大致过程为，首先从采样报文中分析报文头部，然后按照标准定义封装成 sFlow 报文，发送到第三方接收者，便于用户通过第三方接收者分析与监控进入设备的流量。

sFlow 分为以下两种采样方式：

- sampler 采样方式：是由交换芯片提供的一种采样方式，对进入端口的流量进行随机采样；
- poller 采样方式：是一种软件采样方式，用于定期收集端口的报文和流量统计信息。

sFlow 中定义有以下两种角色：

- agent 角色：是设备上的 sFlow 代理，用于管理 sFlow 的两种采样方式，执行采样任务；
- receiver 角色：是支持 sFlow 协议的第三方接收者在本设备上的映射，用于保存第三方接收者的信息（例如 IP 地址和 UDP 端口号），并定期将设备上缓存的 sFlow 报文发送到第三方接收者。

72.2 sFlow 功能配置

表 72-1 sFlow 功能配置列表

配置任务	
配置 sFlow 基本功能	创建 agent 角色
	创建 receiver 角色
配置 sFlow 采样方式	配置 sampler 采样方式
	配置 poller 采样方式

72.2.1 配置 sFlow 基本功能

-B -S -E -A

配置条件

- 无。

创建 agent 角色

agent 角色用于配置和管理采样，目前，agent 角色支持的网络地址类型只能为 IPv4。

表 72-2 创建 agent 角色

步骤	命令	说明
进入全局配置模式	configure terminal	-
创建 agent 角色	sflow agent ip <i>ip-address</i>	必选 缺省情况下，没有创建 agent 角色

创建 receiver 角色

receiver 角色用于保存第三方接收者的信息，将设备上缓存的 sFlow 报文通过 UDP 方式发送到第三方接收者，报文发送的触发条件分为以下两种：

- 当指定的缓存区域已满，无法填入新增的 sFlow 采样信息时，首先将已经缓存的部分封装成 sFlow 报文，发送给第三方接收者，然后将新增的部分填入缓存区域，这种方式可以显著减少设备向第三方接收者发送 sFlow 报文的个数；
- 周期性地将缓存的 sFlow 采样信息封装成 sFlow 报文，发送给第三方接收者，这种方式可以避免由于在较长时间内没有收到新增的 sFlow 采样信息，不能将已经缓存的部分封装成 sFlow 报文发送给第三方接收者。

表 72-3 创建 receiver 角色

步骤	命令	说明
进入全局配置模式	configure terminal	-
创建 receiver 角色	sflow receiver <i>receiver-index</i> owner <i>owner-name</i> ip <i>ip-address</i> [packet-size <i>packet-size-value</i> timeout <i>timeout-value</i> udp-port <i>udp-port-number</i>]	必选 缺省情况下，没有创建 receiver 角色

72.2.2 配置 sFlow 采样方式

-B -S -E -A

配置条件

在配置 sFlow 采样方式之前，首先完成以下任务：

- 创建 agent 角色；
- 创建 receiver 角色。

配置 sampler 采样方式

sampler 采样方式，即接口流采样，是由交换芯片对接口收到的流量进行随机采样。得到样例报文后，首先拷贝报文首部信息，然后解析拷贝内容，并且从中抽取需要的采样信息缓存在设备上，最后将采样信息封装发送到 receiver 角色对应的第三方接收者。

表 72-4 配置接口 sampler 采样方式

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
进入二层以太接口配置模式	interface <i>interface-name</i>	-
配置 sampler 采样方式	sflow sampler receiver <i>receiver-index</i> [header-size <i>header-size-value</i> sample-rate <i>sample-rate-value</i> direction <i>direction-value</i> type <i>type-value</i>]	必选 缺省情况下，没有配置 sampler 采样方式

配置 poller 采样方式

poller 采样方式，即接口定时轮询采样，是指定时地将周期内接口上的报文和流量统计信息封装发送到 receiver 角色对应的第三方接收者。

表 72-5 配置 poller 采样方式

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface <i>interface-name</i>	-
配置 poller 采样方式	sflow poller <i>poller-index</i> receiver <i>receiver-index</i> [interval <i>interval-value</i> type <i>type-value</i>]	必选 缺省情况下，没有配置 poller 采样方式

72.2.3 sFlow 监控与维护

-B -S -E -A

表 72-6 sFlow 监控与维护

命令	说明
clear sflow receiver <i>receiver-index</i> statistics	清除与指定 receiver 角色相关的 sFlow 采样统计信息
show sflow	显示 sFlow 的配置和运行信息
show sflow agent	显示 agent 角色的配置和运行信息
show sflow poller [interface <i>interface-name</i> local]	显示接口上 poller 采样方式的配置和运行信息
show sflow receiver [<i>receiver-index</i> [statistics]]	显示与 receiver 角色相关的 sFlow 采样统计信息、配置和运行信息
show sflow sampler [interface <i>interface-name</i> local]	显示接口上 sampler 采样方式的配置和运行信息

72.3 sFlow 典型配置举例

72.3.1 配置 sFlow 基本功能

-B -S -E -A**网络需求**

- Device 为 sFlow 代理设备，与 NMS 服务器路由可达。
- NMS 服务器通过 sFlow 对 Device 的接口数据流量进行监控。

网络拓扑

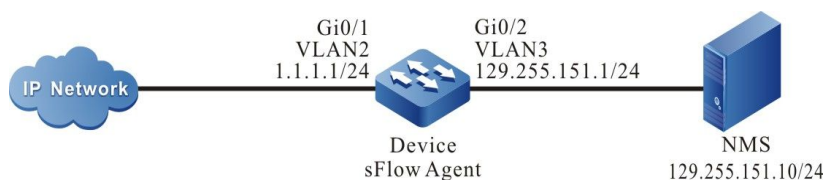


图 72-1 配置 sFlow 基本功能组网图

配置步骤

步骤 1： 配置 VLAN，并将接口加入对应的 VLAN。（略）

步骤 2： 配置各接口 IP 地址。（略）

步骤 3： 配置 sFlow 功能。

#启动 sFlow 代理。

```
Device#configure terminal
Device(config)#sflow agent ip 1.1.1.1
```

#配置 sFlow 统计输出报文的目的 IP 地址和目的 UDP 接口号，发送报文的间隔时间为 5 秒，缓存区域大小为 1400 字节。

```
Device(config)#sflow receiver 1 owner 1 ip 129.255.151.10 timeout 5 udp-port 6343 packet-size 1400
```

#对接口 gigabitethernet0/1 的入方向的流进行 sampler 采样，采样频率为 10。

```
Device(config)#interface gigabitethernet 0/1
Device(config-if-gigabitethernet0/1)#sflow sampler receiver 1 sample-rate 10 direction rx
```

#对接口 gigabitethernet0/1 的入方向的流进行 poller 采样，轮询周期为 20 秒。

```
Device(config-if-gigabitethernet0/1)#sflow poller 1 receiver 1 interval 20
Device(config-if-gigabitethernet0/1)#exit
```

步骤 4： 检验结果。

#查看 Device 上的 sFlow 的信息。

```
Device#show sflow

sFlow Agent Configuration: (Interval = 120, Current Tick = 0x002a6476)

  Address          Receivers Samplers  Pollers
  Version Id Type   Net Address Socket Number Number Number Boot Time / Exec Time
-----
  1.3      1 IPv4  1.1.1.1   0x1c  1/78   1/156  1/156  0x00000ab2/0x002a644c
```

sFlow Receivers Configuration: (Reset Delta = 18000, Current Tick = 0x002a6476)

Index	Owner	Datagram Maximum			Datagram Timeout	Reset Time /Expire Time
		Net Address	Port	Version		
1	1	129.255.151.10	6343	5	1400	5 0x002a644c/0x002a6578

sFlow Samplers Configuration:

Sampling Types: H - raw packet header E - ethernet packet
F - IPv4 packet S - IPv6 packet

Interface	Receiver Sampling		Sampling Direction	Maximum Header	Sampling Types	Pkts Number (Curr/Last)
	Index	Rate				
gi0/1	1	10 rx	128	H	0x0000/0x0001	

sFlow Pollers Configuration: (Current Tick = 0x002a6476)

Sampling Types: G - generic counter
E - ethernet counter

Interface	Receiver Sampling			Interval	Countdown
	Instance	Index	Types		
gi0/1	1	1	G	10	0x002a65b4

#NMS 上可以查看到 Device 上, 接口 gigabitethernet0/1 的入方向的流信息。

73 LLDP

73.1 LLDP 简介

73.1.1 LLDP 协议概述

-B -S -E -A

LLDP (Link Layer Discovery Protocol, 链路层发现协议) 是 IEEE 802.1ab 标准中定义的链路层协议, 它将本地设备的信息组织成 TLV (Type/Length/Value, 类型/长度/值), 封装在 LLDPDU (Link Layer Discovery Protocol Data Unit, 链路层发现协议数据单元) 中发送给直连的邻居设备, 同时也把从邻居设备接收的 LLDPDU 以标准 MIB (Management Information Base, 管理信息库) 的形式保存起来。通过 LLDP, 设备可以保存和管理自己以及直连邻居设备的信息, 供网络管理系统查询和判断链路的通信状况。

73.1.2 TLV 类型信息

-B -S -E -A

LLDP 可以封装的 TLV 包括基本 TLV、组织定义 TLV 以及 MED (Media Endpoint Discovery, 媒体终端发现) TLV。基本 TLV 是被视为网络设备管理基础的一组 TLV, 组织定义 TLV 和 MED TLV 是由标准组织以及其他机构定义的 TLV, 用于增强对网络设备的管理, 可根据实际需要配置是否在 LLDPDU 中发布。

基本 TLV

在基本 TLV 中, 有几种类型的 TLV 对于实现 LLDP 功能来说是必选的, 即必须在 LLDPDU 中发布, 如下表所示。

表 73-1 基本 TLV 说明

TLV 类型	说明	是否必须发布
End of LLDPDU TLV	标志 LLDPDU 结束	是
Chassis ID TLV	发送设备的 MAC 地址	是
Port ID TLV	用来标识 LLDPDU 发送端的端口。当设备不发送	是

TLV 类型	说明	是否必须发布
	MED TLV时, 内容为端口名称, 当选择发送MED TLV时, 内容为端口的MAC地址	
Time To Live TLV	本地设备信息在邻居设备上的存活时间	是
Port Description TLV	端口的描述字符串	否
System Name TLV	设备的名称	否
System Description TLV	系统描述	否
System Capabilities TLV	系统的主要功能以及有哪些主要功能被使能	否
Management Address TLV	管理地址, 以及对应的接口号和OID(Object Identifier, 对象标识)。管理地址可以是手动配置的IP地址; 若没有配置, 则选取设备的管理口的主IP地址; 若管理口没有配置, 则选取接口允许通过VLAN的主IP地址; 若任意VLAN未配置主IP地址, 管理地址值则为空。缺省会发送该TLV	是

组织定义 TLV

组织定义 TLV 包括 802.1 组织定义 TLV 和 802.3 组织定义 TLV，具体如下表所示。

表 73-2 802.1 组织定义 TLV 说明

TLV 类型	说明	是否必须发布
Port VLAN ID TLV	端口 VLAN ID	否
Port And Protocol VLAN ID TLV	端口的协议 VLAN ID	否
VLAN Name TLV	端口 VLAN 名称	否
Protocol Identity TLV	端口支持的协议类型，本地设备不支持发送 Protocol Identity TLV，但可以接收该类型的 TLV	否

表 73-3 802.3 组织定义 TLV 说明

TLV 类型	说明	是否必须发布
MAC/PHY Configuration/Status TLV	端口的速率和双工状态、是否支持端口速率自动协商、是否使能自动协商功能以及当前的速率和双工状态	否
Power Via MDI TLV	端口的供电能力	否
Link Aggregation TLV	端口是否支持链路聚合以及是否使能链路聚合	否

TLV 类型	说明	是否必须发布
Maximum Frame Size TLV	支持的最大帧长度，取端口配置的 MTU (Max Transmission Unit, 最大传输单元)	否

MED TLV

MED TLV 具体信息如下表。

表 73-4 MED TLV 说明

TLV 类型	说明	是否必须发布
LLDP-MED Capabilities TLV	设备的 MED 设备类型以及在 LLDPDU 中可以封装的 LLDP MED TLV 类型	否
Network Policy TLV	端口的 VLAN ID、支持的应用（如语音和视频）、应用的优先级以及使用的策略等信息	否
Extended Power-via-MDI TLV	设备的供电能力	否
Hardware Revision TLV	设备的硬件版本	否
Firmware Revision TLV	设备的固件版本	否
Software Revision TLV	设备的软件版本	否
Serial Number TLV	设备的序列号	否

TLV 类型	说明	是否必须发布
Manufacturer Name TLV	设备的制造厂商	否
Model Name TLV	设备的模块名	否
Asset ID TLV	设备的断言标识符，以便目录管理和断言跟踪	否
Location Identification TLV	连接设备的位置标识信息，供其它设备在基于位置的应用中使用	否

73.1.3 LLDP 工作机制

-B -S -E -A

LLDP 工作模式

端口分为以下四种 LLDP 工作模式：

- RxTx：既发送也接收 LLDPDU；
- Tx：只发送不接收 LLDPDU；
- Rx：只接收不发送 LLDPDU；
- Disable：既不发送也不接收 LLDPDU。

LLDP 发送机制

LLDP 发送机制如下：

- 当端口工作在 RxTx 或 Tx 模式时，将按照 LLDP 报文发送周期，定期向邻居设备发送 LLDPDU；
- 端口开启轮询功能后，会定期轮询本地设备中 LLDP 关心的配置是否发生变化，如果检查到配置变化，会立即发送 LLDPDU。为了防止本地信息频繁变化引起大量发

送 LLDPDU，每发送一个 LLDPDU 都需要延迟等待一段时间，才会继续发送下一个 LLDPDU；

- 当本地设备 LLDP 相关的某些配置发生变化（如：选择发布的 TLV 种类），或者开启轮询功能后，检查到配置变化，将启用快速发送机制，即立即连续发送指定数量的 LLDPDU，之后恢复为正常的 LLDP 报文发送周期；
- 当全局 LLDP 功能禁用或使能 LLDP 的端口执行 shutdown、加入汇聚组、禁用 LLDP 功能操作，以及执行设备重启操作时，会发送一个携带 CLOSE TLV 的 LLDPDU 通知邻居设备。

LLDP 接收机制

当端口工作在 RxTx 或 Rx 模式时，将对收到的 LLDPDU 及其携带的 TLV 进行有效性检查。通过有效性检查后，将邻居信息保存到本地设备，并根据 LLDPDU 中携带的 TTL（Time To Live，生存时间）值设置邻居信息在本地设备的老化时间，如果接收到的 LLDPDU 中的 TTL 值等于零，将立刻老化该邻居信息。LLDP 协议对邻居存储的能力是有限制的，目前设备单端口最多支持 20 个邻居信息，设备最大支持 2000 个邻居的存放，如果邻居达到上限，还有更多的邻居通告报文到达就会被丢弃，不予保存。

73.2 LLDP 功能配置

表 73-5 LLDP 功能配置列表

配置任务	
配置 LLDP 基本功能	使能全局 LLDP 功能
	使能端口 LLDP 功能
配置 LLDP 工作模式	配置 LLDP 工作模式
配置 LLDP 允许发布的 TLV	配置允许发布的基本 TLV
	配置允许发布的组织定义 TLV
	配置允许发布的 MED TLV

配置任务	
配置 LLDP 参数	配置邻居存活时间
	配置报文发送延迟时间
	配置报文发送周期
	配置快速发包数目
	配置重新初始化延迟
	配置 LLDP 配置检查周期

73.2.1 配置 LLDP 基本功能

-B -S -E -A

必须同时使能全局 LLDP 功能和端口 LLDP 功能，LLDP 才能正常工作。本地设备通过与其他设备交互 LLDPDU，得到邻居设备信息。

配置条件

无

使能全局 LLDP 功能

表 73-6 使能全局 LLDP 功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
使能全局 LLDP 功能	lldp run	必选 缺省情况下，全局未使能 LLDP 功能

使能端口 LLDP 功能

表 73-7 使能端口 LLDP 功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二/三层以太网接口配置模式	interface <i>interface-name</i>	必选其一 进入二/三层以太网接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	
使能端口 LLDP 功能	lldp enable	必选 缺省情况下，端口未使能 LLDP 功能

73.2.2 配置 LLDP 工作模式

-B -S -E -A

配置条件

无

配置 LLDP 工作模式

用户可以根据设备在网络中的角色设置不同的工作模式。如果是种子设备（网络拓扑收集的中心设备）建议将 LLDP 工作模式配置为 Rx，否则建议将 LLDP 工作模式配置为 Tx。

表 73-8 配置 LLDP 工作模式

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二/三层以太网接口配置模式	interface <i>interface-name</i>	必选其一 进入二/三层以太网接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	
配置 LLDP 工作模式为 Rx	lldp receive	可选
配置 LLDP 工作模式为 Tx	lldp transmit	缺省情况下，LLDP 工作模式为 RxTx LLDP 的工作模式最终由命令 lldp receive 和 lldp transmit 共同决定

73.2.3 配置 LLDP 允许发布的 TLV

-B -S -E -A

通过发布 TLV，可以让邻居设备了解本地设备的详细信息。

配置条件

无

配置 LLDP 允许发布的基本 TLV

用户可以根据实际应用的需要，发布不同的基本 TLV。

表 73-9 配置 LLDP 允许发布的基本 TLV

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二/三层以太网接口配置模式	interface <i>interface-name</i>	必选其一 进入二/三层以太网接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	
配置 LLDP 允许发布的基本 TLV	lldp tlv-select { basic-tlv { all port-description system-capability system-description system-name } }	可选 缺省情况下，允许发布所有基本 TLV

配置 LLDP 允许发布的组织定义 TLV

用户可以根据实际应用的需要，发布不同的组织定义 TLV。

表 73-10 配置 LLDP 允许发布的组织定义 TLV

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二/三层以太网接口配置模式	interface <i>interface-name</i>	必选其一 进入二/三层以太网接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	

步骤	命令	说明
		配置模式后, 后续配置只在汇聚组生效
配置 LLDP 允许发布的组织定义 TLV	lldp tlv-select { dot1-tlv { all port-vlan-id protocol-vlan-id vlan-name } dot3-tlv { all link-aggregation mac-physic max-frame-size power } }	可选 缺省情况下, 允许发布所有组织定义 TLV

配置 LLDP 允许发布的 MED TLV

用户可以根据实际应用的需要, 发布不同的 MED TLV。

表 73-11 配置 LLDP 允许发布的 MED TLV

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二/三层以太网接口配置模式	interface <i>interface-name</i>	必选其一 进入二/三层以太网接口配置模式后, 后续配置只在当前端口生效; 进入汇聚组配置模式后, 后续配置只在汇聚组生效
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	
配置 LLDP 允许发布的 MED TLV	lldp med-tlv-select { all capability location-id elin-address	可选

步骤	命令	说明
	<i>phonenum</i> network-policy power-via-mdi inventory }	缺省情况下，不允许发布所有 MED TLV

73.2.4 配置 LLDP 参数

-B -S -E -A

配置条件

无

配置邻居存活时间

通过配置邻居存活时间即 TTL，指定本地设备信息在邻居设备上存活的时间，使得邻居设备能够在本地设备存活时间到期后删除本地设备的信息。

表 73-12 配置邻居存活时间

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置本地设备在邻居设备上的存活时间	lldp holdtime <i>holdtime-value</i>	可选 缺省情况下，本地设备在邻居设备上的存活时间为 120 秒

配置报文发送延迟时间

通过配置报文发送延迟时间，可以防止本地信息频繁变化引起大量发送 LLDPDU。

表 73-13 配置报文发送延迟时间

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 LLDP 报文发送延迟时间	lldp transmit-delay <i>transmit-delay-value</i>	可选 缺省情况下, LLDP 报文发送延迟时间为 2 秒

配置报文发送周期

通过配置报文发送周期, 本地设备将定期向邻居设备发送 LLDP 报文, 使得本地设备在邻居设备上的信息不会被老化。

表 73-14 配置报文发送周期

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置 LLDP 报文发送周期	lldp transmit-interval <i>transmit-interval-value</i>	可选 缺省情况下, LLDP 报文发送周期为 30 秒

配置快速发包数目

当本地设备的 LLDP 相关的某些配置 (如: 选择发布的 TLV 种类) 发生变化, 或者使能轮询功能后轮询机制检查到本地设备中 LLDP 关心配置信息变化时, 为了让其它设备尽快发现本地设备的变化, 将启用快速发送机制, 即立即连续发送指定数量 (缺省为 3 个) 的 LLDPDU 后再恢复为正常的发送周期。

表 73-15 配置快速发包数目

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置快速发包数目	lldp fast-count <i>fast-count-value</i>	可选 缺省情况下，快速发包数目为 3 个

配置重新初始化延迟

当端口工作模式发生变化时，将对端口协议状态机进行重新初始化操作，为防止端口的工作模式频繁变化不断对端口协议状态机进行重新初始化，可以配置端口的重新初始化延迟时间。

表 73-16 配置重新初始化延迟

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置重新初始化延迟	lldp reinit <i>reinit-value</i>	可选 缺省情况下，重新初始化延迟时间为 2 秒

配置 LLDP 配置检查周期

为使 LLDP 配置变化后能够及时通知邻居设备，可以配置 LLDP 配置检查周期。

表 73-17 配置 LLDP 配置检查周期

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
进入二/三层以太网接口配置模式	interface <i>interface-name</i>	必选其一
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	进入二/三层以太网接口配置模式后，后续配置只在当前端口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效
使能轮询功能并配置轮询周期	lldp check-change-interval <i>check-change-interval-value</i>	可选 缺省情况下，轮询功能处于禁用状态

73.2.5 LLDP 监控与维护

-B -S -E -A

表 73-18 LLDP 监控与维护

命令	说明
clear lldp neighbors [interface <i>interface-name</i> link-aggregation <i>link-aggregation-id</i>]	清除邻居信息
show lldp neighbors [detail interface <i>interface-name</i> [detail] link-aggregation <i>link-aggregation-id</i> [detail]]	显示邻居信息
show lldp neighbors oui [interface <i>interface-name</i> link-aggregation <i>link-aggregation-id</i>]	显示邻居 OUI 地址信息及写入 Voice-VLAN OUI 表项状态

命令	说明
clear lldp statistics	清除 LLDP 报文统计信息
show lldp statistics { interface <i>interface-name</i> /link-aggregation <i>link-aggregation-id</i> }	显示指定端口的 LLDP 报文收发统计信息
show lldp	显示 LLDP 全局配置信息
show lldp interface <i>interface-name</i>	显示指定端口的 LLDP 工作模式和检查 LLDP 配置变化的轮询周期
show lldp link-aggregation <i>link-aggregation-id</i>	显示指定汇聚组的 LLDP 工作模式和检查 LLDP 配置变化的轮询周期
show lldp tlv-select [interface <i>interface-name</i> /link-aggregation <i>link-aggregation-id</i>]	用于显示基本 TLV 和组织定义 TLV 配置信息
show lldp voice neighbors [detail interface <i>interface-name</i> [detail] link-aggregation <i>link-aggregation-id</i> [detail]]	显示语音邻居信息

73.3 LLDP 典型配置举例

73.3.1 配置 LLDP 的基本功能

-B -S -E -A

网络需求

- 在 Device1、Device2、Device3 上分别配置 LLDP 功能，实现链路层邻居发现。

网络拓扑



图 73-1 配置 LLDP 基本功能组网图

配置步骤

步骤 1： 在 Device 上使能 LLDP 功能。

#在 Device1 上使能 LLDP 功能。

```
Device1#configure terminal
Device1(config)#lldp run
```

#在 Device2 上使能 LLDP 功能。

```
Device2#configure terminal
Device2(config)#lldp run
```

#在 Device3 上使能 LLDP 功能。

```
Device3#configure terminal
Device3(config)#lldp run
```

步骤 2： 在端口上配置 LLDP 功能。

#在 Device1 的端口 gigabitethernet0/1 上使能 LLDP 功能。

```
Device1(config)#interface gigabitethernet 0/1
Device1(config-if-gigabitethernet0/1)#lldp enable
Device1(config-if-gigabitethernet0/1)#exit
```

#在 Device2 的端口 gigabitethernet0/1 和 gigabitethernet0/2 上使能 LLDP 功能。

```
Device2(config)#interface gigabitethernet 0/1
Device2(config-if-gigabitethernet0/1)#lldp enable
Device2(config-if-gigabitethernet0/1)#exit
Device2(config)#interface gigabitethernet 0/2
Device2(config-if-gigabitethernet0/2)#lldp enable
Device2(config-if-gigabitethernet0/2)#exit
```

#在 Device3 的端口 gigabitethernet0/1 上使能 LLDP 功能。

```
Device3(config)#interface gigabitethernet 0/1
Device3(config-if-gigabitethernet0/1)#lldp enable
Device3(config-if-gigabitethernet0/1)#exit
```

步骤 3: 检验结果。

#查看 Device1 上的邻居信息。

```
Device1#show lldp neighbors
Capability codes:
(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Index   Local Intf      Hold-time  Capability  Peer Intf      Device ID
1       gi0/1           120        P,R,        gi0/1          Device2
```

Device1 发现邻居 Device2。

#查看 Device1 邻居的详细信息。

```
Device1#show lldp neighbors detail
Basic information
Chassis ID       : 0001.7a54.5d0b
Interface ID     : gi0/1
Interface Description : gigabitethernet0/1
System Name      : Device2
System Description : Hirschmann IT (R) Operating System Software
Time Remaining   : 111 seconds
System Capabilities : P,R,
Enabled Capabilities : P,R,
Management Addresses : IP;10.0.0.1

802.1 organizationally information
Port VLAN ID     : 1
Port And Protocol VLAN ID : 0
VLAN Name Of VLAN 1 : DEFAULT

802.3 organizationally information
Auto Negotiation : Supported, Enabled
PMD Auto Negotiation Advertised : 10BASE-T,10BASE-TFD,100BASE-TX,100BASE-TXFD,FDX-PAUSE,1000BASE-TFD,
Media Attachment Unit Type : 1000BaseTFD,
Port Class       : PSE
PSE Power        : Supported, Enabled
PSE Pairs Control Ability : No
Power Pairs      : 1
Power Class      : 1
Link Aggregation : Supported, Disabled
Link Aggregation ID : 0
Max Translate Unit : 1824

MED organizationally information
Capabilities      : Not Supported
Class Type       : Not Supported
Application Type  : Not Supported
Policy           : Not Supported
VLAN Tagged      : Not Supported
VLAN ID          : Not Supported
L2 Priority       : Not Supported
DSCP Value       : Not Supported
Location ID      : Not Supported
Power Type       : Not Supported
Power Source     : Not Supported
Power Priority    : Not Supported
Power Value      : Not Supported
```

HardwareRev	: Not Supported
FirmwareRev	: Not Supported
SoftwareRev	: Not Supported
SerialNum	: Not Supported
Manufacturer Name	: Not Supported
Model Name	: Not Supported
Asset Tracking Identifier	: Not Supported

Total entries displayed: 1

说明:

- 查看 Device2、Device3 的邻居信息请参照 Device1。
-

74 SNMP

74.1 SNMP 简介

SNMP (Simple Network Management Protocol, 简单网络管理协议)是管理互连网络设备的一个标准协议。其目的是保证管理信息能够在网管工作站 (Network Management Station) 和被管设备 SNMP 代理之间传送, 便于系统管理员完成网络系统的管理。

SNMP 是一个应用层协议, 为客户机/服务器模式, 主要包括三个部分:

- NMS (Network Management Station) ;
- SNMP 代理;

- MIB (Management Information Base) 。

设备所维护的全部被管理对象的结构集合称为管理信息库 (MIB) ， 被管理对象按照层次式树形结构组织， MIB 定义了一个设备获得的网络管理信息， 每个设备为了和标准的网络管理协议一致， 必须使用 MIB 中定义的格式显示信息。 ISO ASN.1 的一个子集为 MIB 定义了语法， 每个 MIB 都使用定义在 ASN.1 中的树形结构组织所有可用信息， 其中的每片信息是一个有标点的节点， 每一个节点包含一个对象标识符和一个简短的文本描述。

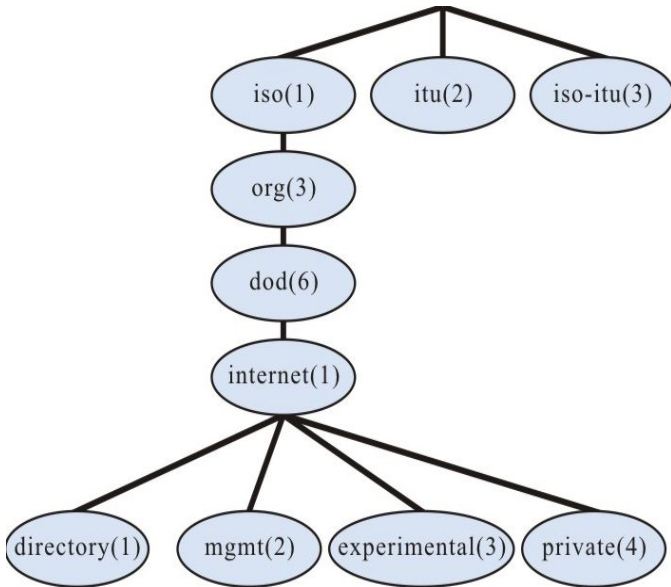


图 74-1 网络管理的 ASN.1 树示意图

SNMP 的协议版本分别有三个版本：SNMPv1、SNMPv2 和 SNMPv3

- SNMPv1：SNMP 协议的第一个版本，其缺点：安全问题、带宽浪费、管理者与管理者之间不具备通信能力、协议只提供了有限的操作。
- SNMPv2：在基于 SNMPv1 上做了一些改进，使得功能更强、安全性更好。
- SNMPv3：原始身份，信息的完整性和再传输保护的一些方面，内容机密，授权和进程控制，以上三项能力所需的远程配置和管理能力。

因此，SNMPv3 的发展集中在双重目标上，在增强体系结构提供可工作的安全平台的同时，还要维护网络管理体系结构的一致性。

SNMP 协议主要包括以下几种操作：

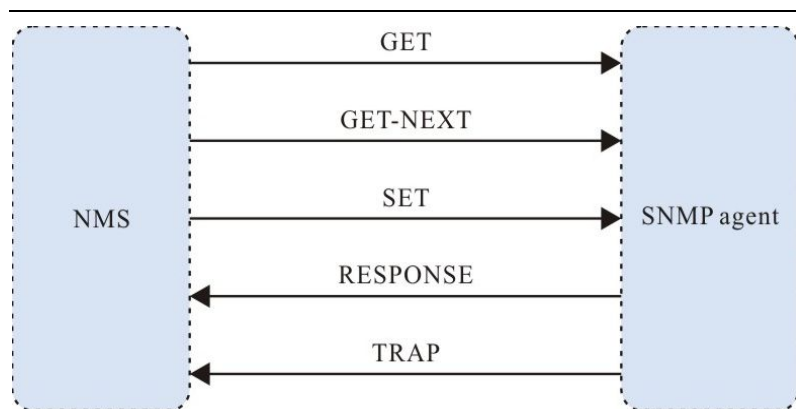


图 74-2 SNMP 管理操作图

- Get-request 操作：SNMP 网络工作站从 SNMP 代理提取一个或多个参数值。
- Get-next-request 操作：SNMP 网络工作站从 SNMP 代理提取一个或多个参数的下一个参数值。
- Get-bulk 操作：SNMP 网络工作站从 SNMP 代理提取批量的参数值。
- Set-request 操作：SNMP 网络工作站设置 SNMP 代理的一个或多个参数值。
- Get-response 操作：SNMP 代理返回一个或多个参数值，是 SNMP 代理对以上三种操作的响应操作。
- Trap 操作：SNMP 代理主动发出的报文，通知 SNMP 网络工作站某些事情发生。

SNMPv1 和 SNMPv2 版本使用认证名来鉴别是否有权使用 MIB 对象，所以只有网络工作站的认证名和设备中定义的某个认证名一致才能对设备进行管理。

认证名可以有以下两种属性：

- 只读（Read-only）：授权网络工作站对设备所有的 MIB 对象的读权限。
- 读写（Read-write）：授权网络工作站对设备所有的 MIB 对象读写权限。

SNMPv3 是通过安全模型以及安全级别来确定对数据采用哪种安全机制进行处理，安全模型的三种类型分别为：SNMPv1、SNMPv2c、SNMPv3

表 74-1 支持的安全模型和安全级别

安全模型	安全级别	认证	加密	说明
SNMPv1	NoAuthNoPriv	认证名	无	通过认证名确认数据的合法性
SNMPv2c	NoAuthNoPriv	认证名	无	通过认证名确认数据的合法性
SNMPv3	NoAuthNoPriv	用户名	无	通过用户名确认数据的合法性
SNMPv3	AuthNoPriv	MD5/SHA	无	使用 HMAC-MD5/HMAC-SHA 的数据认证方式
SNMPv3	AuthPriv	MD5/SHA	DES	使用 HMAC-MD5/HMAC-SHA 的数据认证方式和 CBC-DES 的数据加密方式

74.2 SNMP 功能配置

表 74-2 SNMP 功能配置列表

配置任务	
配置 SNMP 基本功能	使能 SNMP 服务
	配置 MIB 视图
	配置管理者联系信息
	配置设备物理位置信息
配置 SNMPv1/v2	配置 SNMP 团体名

配置任务	
	配置 SNMP Trap 功能
配置 SNMPv3	配置 SNMP 用户组
	配置 SNMP 用户
	配置 SNMP 通告
	配置 SNMP 代理转发

74.2.1 配置 SNMP 基本功能

-B -S -E -A

配置条件

无

使能 SNMP 服务

如果设备使能了 SNMP 服务，那么设备可以通过 SNMP 网管软件进行配置和管理。

表 74-3 使能 SNMP 服务

步骤	命令	说明
进入全局配置模式	config terminal	-
使能 SNMP 服务	snmp-server start [rfc]	必选 缺省情况下 SNMP 服务处于关闭状态

配置 MIB 视图

通过使用基于视图的访问控制模型，来判定一个操作关联的管理对象是否在视图允许之内，只有在视图允许之内的管理对象才被允许访问。

表 74-4 配置 MIB 视图

步骤	命令	说明
进入全局配置模式	config terminal	-
配置 MIB 视图	snmp-server view <i>view-name oid-string</i> { include exclude }	必选 缺省情况下 SNMP 的视图名为 Default
配置 MIB 中获取的系统启动时间类型	snmp-server mib2 sysuptime { snmp-agent-uptime system-uptime }	必选 缺省情况下为 system-uptime

配置管理者联系信息

管理者联系信息是在 SNMP 协议中的一个信息节点，网管软件可以通过 SNMP 获取这个信息。

表 74-5 配置管理者联系方式

步骤	命令	说明
进入全局配置模式	config terminal	-
配置管理者联系信息	snmp-server contact <i>contact-line</i>	必选

配置设备物理位置信息

设备物理位置信息是在 SNMP 协议中的一个信息节点，网管软件可以通过 SNMP 获取这个信息。

表 74-6 配置设备物理位置信息

步骤	命令	说明
进入全局配置模式	config terminal	-
配置设备物理位置信息	snmp-server location <i>location</i>	必选

74.2.2 配置 SNMPv1/v2 **-B -S -E -A**

配置条件

在配置 SNMPv1/v2 之前，首先完成以下任务：

- 配置链路层协议，保证链路层通信正常。
- 配置接口的 IP 地址，使各相邻节点网络层可达。

创建 SNMP 团体名

SNMPv1/SNMPv2c 采用的是基于团体名的安全方案，SNMP 团体名可以看作是 NMS 和 SNMP 代理之间的密码，也就是说 SNMP 代理只接受相同团体名的管理操作，对于来自不同团体名的 SNMP 将不会被响应，直接丢弃。

表 74-7 配置团体名

步骤	命令	说明
进入全局配置模式	config terminal	-
配置 SNMP 代理团体名	snmp-server community <i>community-name</i>	必选

步骤	命令	说明
	[view <i>view-name</i>] { ro rw } [<i>access-list-number</i> / <i>access-list-name</i>]	缺省情况下团体名为 public

74.2.3 配置 SNMPv3

-B -S -E -A

配置条件

在配置 SNMPv3 之前，首先完成以下任务：

- 配置链路层协议，保证链路层通信正常。
- 配置接口的 IP 地址，使各相邻节点网络层可达。

创建 SNMP 用户组

在进行控制的时候，可以将某些用户和一个组关联。同一个组的用户都具有相同的访问权限。

- 可以配置一个组与视图进行关联，这种视图有三类，分别是：只读视图、可写视图和通告视图。
- 可以配置组的安全级别，配置是否需要认证和加密。

表 74-8 创建 SNMP 用户组

步骤	命令	说明
进入全局配置模式	config terminal	-
创建 SNMP 用户组	snmp-server group <i>group-name v3</i>	必选

步骤	命令	说明
	{ authnopriv authpriv noauth } [notify <i>notify-view</i> read <i>read-view</i> write <i>write-view</i>]	authnopriv 认证但不加密 authpriv 既认证又加密 noauth 不认证不加密

创建 SNMP 用户

通过基于用户的安全模型来进行安全管理，网络工作站只有使用了合法的用户才能通 SNMP 代理进行通信，当然这个合法的用户需要进行配置。

针对 SNMPv3 来说，还可以指定安全级别、认证算法（MD5 或 SHA）、认证密码、加密算法（DES）和加密密码。

表 74-9 配置用户

步骤	命令	说明
进入全局配置模式	config terminal	-
创建 SNMP 用户	snmp-server user <i>user-name</i> <i>group-name</i> [remote <i>ip-address</i> <i>port-num</i>] v3 [auth { md5 sha } <i>password</i> [encrypt { des aes } <i>password</i>]] [access <i>access-list-number</i> <i>access-list-name</i> ipv6 <i>access-list-number</i>]	必选

说明：

- 配置基于用户安全模型（USM）的 SNMPv3 用户，保存每个用户的鉴别和加密信息。注意只有在配置了认证协议后才能配置加密协议。
- 对于远程用户（所谓的远程是相对于本地 SNMPv3 实体来说的，如果这个本地 SNMPv3 实体要与其他 SNMPv3 实体打交道，那么其他 SNMPv3 实体就称为远程 SNMPv3 实体，这在 noify 以及 proxy 中有涉及）来说，还需指定远程用户的 IP 地址和 UDP 端口号，在配置远程用户时还需注意，必须首先配置该用户对应的远程 SNMP 实体的 engineID。此外，每个用户必须与一个组对应，这样才能通过基于视图的访问控制将一个安全模型和安全名称映射为一个组名称。
- 在配置自动代理转发的时候，由于可能不知道被代理设备的 ip 地址，这个时候，只要在 ip-address 处输入 0.0.0.0 即可，另外，自动代理转发必须与保活机制结合在一起才行。

配置 SNMP 通告

SNMPv3 通告配置包含以下几种：

- SNMPv3 通告配置：对 SNMPv3 的通告进行配置，指定通告消息的类型为 inform；
- SNMPv3 通告过滤配置：通告过滤表示用于确定一个通告消息是否应该发送到一个目的地址的过滤；
- SNMPv3 通告地址映射表配置：将通告地址与一个过滤表关联。

表 74-10 配置通告

步骤	命令	说明
进入全局配置模式	config terminal	-
配置 SNMP 通告	snmp-server notify notify <i>notify-name</i> taglist inform	必选
配置 SNMP 通告过滤	snmp-server notify filter <i>filter-name</i> oid-	必选

步骤	命令	说明
	<i>subtree</i> { exclude include }	exclude: 表示过滤掉该 MIB 子树下所有对象的通告 include: 表示通告该 MIB 子树下所有对象
配置 SNMP 地址参数	snmp-server AddressParam { <i>address-name</i> paramIn } v3 <i>user-name</i> { noauth authpriv authnopriv }	必选
配置 SNMP 通告过滤映射表	snmp-server notify profile <i>filter-name</i> <i>address-param</i>	必选 <i>filter-name</i> : 指定需要映射的通告过滤名 <i>address-param</i> : 指定需要映射的地址参数名

配置 SNMP 代理转发

如果网络工作站无法直接访问被管理的 SNMP 代理，那么就需要中间的设备支持代理转发。目前只有 SNMPv3 支持代理转发。

表 74-11 配置代理转发

步骤	命令	说明
进入全局配置模式	config terminal	-

步骤	命令	说明
配置 SNMP 远程引擎标识	snmp-server engineID remote <i>ip-address port-num</i> [vrf <i>vrf-name</i>] <i>engine-id</i> [<i>group-name</i>]	必选 配置需要被代理转发的 SNMP 实体的引擎标识
配置 SNMP 地址参数	snmp-server AddressParam [<i>address-name</i> paramIn] v3 <i>user-name</i> { noauth authpriv authnopriv }	必选
配置 SNMP 通告地址	snmp-server TargetAddress <i>target-name ip-address port-num address-param taglist time-out retry-num</i>	必选
配置 SNMP 代理转发	snmp-server proxy <i>proxy-name</i> { inform trap read write } { <i>engineId</i> auto } <i>engineId address-param target-addr</i> [<i>context-name</i>]	必选

74.2.4 配置 SNMP Trap **-B -S -E -A**

Trap 是 SNMP 代理主动向网络工作站发送的信息，用于报告一些特定的事件。Trap 报文分为：通用 Trap 和自定义 Trap。通用 Trap 包含以下几种：Authentication、Linkdown、Linkup、Coldstart、Warmstart，自定义 Trap 是按照各个模块的需求输出的。

表 74-12 配置 Trap

步骤	命令	说明
进入全局配置模式	configure terminal	-
使能链路接口 down 或 up 的 traps	snmp-server enable traps snmp [linkup linkdown]	必选 缺省情况下 SNMP Trap 未使能
进入接口配置模式	interface <i>interface-type</i> <i>interface-num</i>	可选
配置接口状态变化的 Trap	snmp trap link-status	可选
配置 Trap 目标主机	snmp-server host { <i>ip-address</i> / <i>host-name</i> } traps { community <i>community-name</i> version { 1 2 } user <i>username</i> authnopriv authpriv noauth version 3 } [port <i>port-num</i> vrf <i>vrf-name</i>]	必选 需要将 ip-address 指定为网络工作站的 IP 地址
配置 Trap 报文的源地址	snmp-server trap-source <i>ip-address</i>	可选

说明：

- 由于 Trap 信息通常情况下比较多，所以会占用设备资源，从而影响设备性能，所以建议根据需要开启指定模块的 Trap 功能，不要所有模块的 Trap 都开启。

74.2.5 SNMP 监控与维护

-B -S -E -A

表 74-13 SNMP 监控与维护

命令	说明
show snmp-server	查看 SNMP 协议报文统计信息
show snmp-server AddressParams	查看 SNMP 代理地址参数信息
show snmp-server community	查看 SNMP 代理团体信息
show snmp-server contact	查看设备管理者联系方式
show snmp-server context	查看 SNMPv3 的上下文环境
show snmp-server engineGroup	显示 SNMP 代理引擎组的信息
show snmp-server engineID	显示 SNMP 代理引擎 ID 的信息
show snmp-server group	查看 SNMP 代理用户组信息
show snmp-server Host	显示 SNMP 代理 trap 主机的信息
show snmp-server location	查看设备放置的位置信息
show snmp-server notify filter	显示 SNMP 代理通告过滤的信息
show snmp-server notify notify	显示 SNMP 代理通告的信息
show snmp-server notify profile	显示 SNMP 代理通告关联的信息
show snmp-server port	查看 SNMP 协议配置的端口号

命令	说明
show snmp-server proxy	查看 SNMP 代理转发信息
show snmp-server reg-list	查看 SNMP 已经注册 MIB 的模块信息
show snmp-server TargetAddress	查看 SNMP 代理地址表项信息
show snmp-server user	查看 SNMP 用户信息
show snmp-server view	查看 SNMP 视图信息

74.3 SNMP 典型配置举例

74.3.1 配置 SNMP v1/v2c 代理服务器

-B -S -E -A

网络需求

- Device 为 SNMP Agent 设备，与 NMS 服务器路由可达。
- NMS 通过 SNMP v1 或 SNMP v2c 对 Device 进行监控以及管理，Device 在发生故障或者出错的时候会主动向 NMS 报告相应情况。

网络拓扑

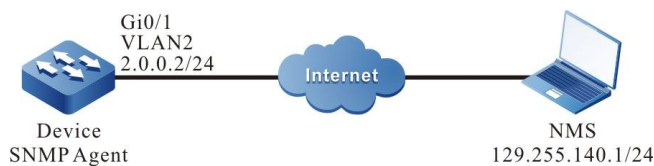


图 74-3 配置 SNMP v1/v2c 代理服务器组网图

配置步骤

步骤 1： 配置 VLAN，并将端口加入对应的 VLAN。（略）

步骤 2: 配置各接口的 IP 地址。(略)

步骤 3: 在设备 Device 上启动 SNMP 代理, 并配置 SNMP 的团体名。

#配置 Device。

启动 SNMP 代理, 配置节点视图名为 default、只读团体名为 public、读写团体名为 public。

```
Device#configure terminal
Device(config)#snmp-server start
Device(config)#snmp-server view default 1.3.6.1 include
Device(config)#snmp-server community public view default ro
Device(config)#snmp-server community public view default rw
```

步骤 4: 配置让 Device 主动向网络工作站 (NMS) 发送 Trap 报文, 且使用团体名 public。

#配置 Device。

```
Device(config)#snmp-server enable traps
Device(config)#snmp-server host 129.255.140.1 traps community public version 2
```

说明:

- **snmp-server host** 命令中指定的 SNMP 版本必须和 NMS 上运行的 SNMP 版本一致。
-

步骤 5: 配置 NMS。

#在使用 SNMP v1/v2c 版本的 NMS 上需要设置“只读团体名”和“读写团体名”。另外, 还要设置“超时”时间和“重试次数”。用户通过网管系统对设备进行查询和配置操作。

说明:

- 使用只读团体名时, 用户通过网管系统只能对设备进行查询操作。
 - 使用读写团体名时, 用户通过网管系统可对设备进行查询和配置操作。
-

步骤 6: 检验结果。

#NMS 通过 MIB 节点可以查询、设置设备 Device 某些参数的值。NMS 能收到来自设备 Device 的各种 Trap 信息，比如设备 Device 的接口 up、down，网络动荡引起的路由变化等，Device 会产生相应的 Trap 信息并发送给 NMS。

74.3.2 配置 SNMP v3 代理服务器

-B -S -E -A

网络需求

- Device 为 SNMP Agent 设备，与 NMS 服务器路由可达。
- NMS 通过 SNMP v3 对 Device 进行管理。

网络拓扑

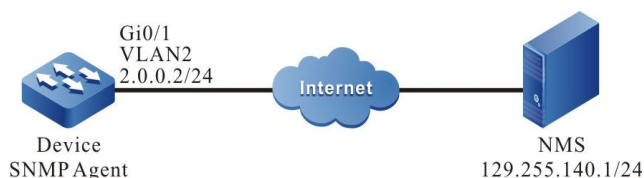


图 74-4 配置 SNMP v3 代理服务器组网图

配置步骤

步骤 1: 配置 VLAN，并将端口加入对应的 VLAN。（略）

步骤 2: 配置各接口的 IP 地址（略）。

步骤 3: 在 Device 上启动 SNMP 代理，并配置 SNMP v3 基本信息。

#配置 Device。

启动 SNMP 代理；配置节点视图名为 default，且可以访问节点 1.3.6.1 下的所有对象。

```
Device#configure terminal
Device(config)#snmp-server start
Device(config)#snmp-server view default1.3.6.1 include
```

配置用户组为 public，安全级别为 authpriv，读写视图、notify 视图均使用 default；配置用户名为 public，属于用户组 public，认证算法为 MD5，认证密码为 admin，加密算法为 DES，加密密码是 admin。

```
Device(config)#snmp-server group public v3 authpriv read default write default notify default
Device(config)#snmp-server user public public v3 auth md5 admin encrypt des admin
```

配置上下文环境名为 public。

```
Device(config)#snmp-server context public
```

步骤 4： 配置 NMS。

#在使用 SNMP v3 版本的 NMS 上需要设置用户名，选择安全级别。根据不同的安全级别，需要分别设置认证算法、认证密码、加密算法、加密密码等。另外，还要设置“超时”时间和“重试次数”。用户通过网管系统对设备进行查询和配置操作。

步骤 5： 检验结果。

NMS 上能通过 MIB 节点查询、设置 Device 某些参数的值。

74.3.3 配置 SNMP v3 trap 通告 **-B -S -E -A**

网络需求

- Device 为 SNMP Agent 设备，与 NMS 服务器路由可达。
- NMS 通过 SNMP v3 对 Device 进行监控。Device 在发生故障或者出错的时候会主动向 NMS 报告相应情况。

网络拓扑



图 74-5 配置 SNMPv3 trap 通告组网图

配置步骤

步骤 1: 配置各接口的 IP 地址 (略)。

步骤 2: 在 Device 上启动 SNMP 代理, 并配置 SNMP v3 基本信息。

#配置 Device。

启动 SNMP 代理; 配置节点视图名为 default, 且可以访问节点 1.3.6.1 下的所有对象。

```
Device#configure terminal
Device(config)#snmp-server start
Device(config)#snmp-server view default 1.3.6.1 include
```

配置用户组为 public, 安全级别为 authpriv, 读写视图、notify 视图均使用 default; 配置用户名为 public, 属于用户组 public, 认证算法为 MD5, 认证密码为 Admin, 加密算法为 DES, 加密密码是 Admin。

```
Device(config)#snmp-server group public v3 authpriv read default write default notify default
Device(config)#snmp-server user public public v3 auth md5 Admin encrypt des Admin
```

配置让 Device 发送所有 Trap 信息。

```
Device(config)#snmp-server enable traps
```

步骤 3: 配置 Device 向 NMS 发送 SNMP v3 trap 报文。

#配置 Device。

配置 NSM 上 SNMP v3 trap 用户名为 public, 安全级别为 authpriv。

```
Device(config)#snmp-server host 129.255.140.1 version 3 user public authpriv
```

步骤 4: 配置 NMS。

#NMS 上需要配置与 SNMP 代理一致的用户名和密码, 运行网管软件并监听 UDP 162 端口号。

步骤 5: 检验结果。

NMS 能收到来自设备 Device 的各种 Trap 信息, 比如设备 Device 的接口 up、down, 网络动荡引起的路由变化等, Device 会产生相应的 Trap 信息并发送给 NMS。

网络需求

- Device 为 SNMP Agent 设备，与 NMS 服务器路由可达。
- NMS 通过 SNMP v3 对 Device 进行监控。Device 在发生故障或者出错的时候会主动向 NMS 报告相应情况。

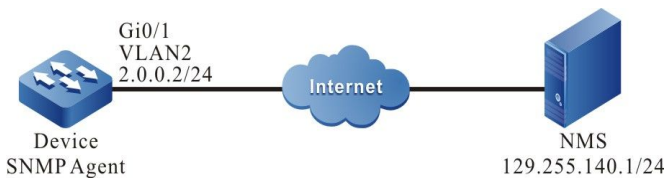
网络拓扑

图 74-6 配置 SNMPv3 通告组网图

配置步骤

- 步骤 1：配置 VLAN，并将端口加入对应的 VLAN。（略）
- 步骤 2：配置各接口的 IP 地址（略）。
- 步骤 3：在 Device 上启动 SNMP 代理，并配置 SNMP v3 基本信息。

#配置 Device。

启动 SNMP 代理；配置节点视图名为 default，且可以访问节点 1.3.6.1 下的所有对象。

```
Device#configure terminal
Device(config)#snmp-server start
Device(config)#snmp-server view default 1.3.6.1 include
```

配置用户组为 group1，安全级别为 authpriv，读写视图、notify 视图均使用 default。

```
Device(config)#snmp-server group group1 v3 authpriv read default write default notify default
```

配置用户名为 user2，属于用户组 group1，认证算法为 MD5，认证密码为 admin，加密算法为 DES，加密密码是 admin。

```
Device(config)#snmp-server user user2 group1 public v3 auth md5 admin encrypt des admin
```

配置上下文环境名为 public。

```
Device(config)#snmp-server context public
```

步骤 4: 配置 Device 向 NMS 发送通告消息。

#配置 Device。

配置远程用户即 NMS 的 IP 地址和 engineID。

```
Device(config)#snmp-server engineID remote 129.255.140.1 162 bb87654321
```

配置远程用户名为 user1, 属于用户组 group1, 认证算法为 MD5, 认证密码为 admin, 加密算法为 DES, 加密密码是 admin。

```
Device(config)#snmp-server user user1 group1 remote 129.255.140.1 162 v3 auth md5 admin encrypt des admin
```

配置本地地址参数名为 param-user1; 配置目标地址名为 target-user1, 使用地址参数 param-user1, 目标地址列表名为 target-user1。

```
Device(config)#snmp-server AddressParam param-user1 v3 user1 authpriv  
Device(config)#snmp-server TargetAddress target-user1 129.255.140.1 162 param-user1 tag-user1 10 3
```

配置 notify 的通告实体为 notify-user1; 配置 notify 的过滤实体为 filter-user1, 包含 1.3.6.1 节点下的所有对象的通告; 配置通告配置表, 让过滤实体 filter-user1 关联地址参数 param-user1。

```
Device(config)#snmp-server notify notify notify-user1 tag-user1 inform  
Device(config)#snmp-server notify filter filter-user1 1.3.6.1 include  
Device(config)#snmp-server notify profile filter-user1 param-user1
```

步骤 5: 配置 NMS。

#在使用 SNMP v3 版本的 NMS 上需要设置用户名, 选择安全级别。根据不同的安全级别, 需要分别设置认证算法、认证密码、加密算法、加密密码等, 并监听 UDP 端口号 162 即可。

步骤 6: 检验结果。

NMS 能收到来自设备 Device 的各种 Trap 信息, 比如设备 Device 的接口 up、down, 网络动荡引起的路由变化等, Device 会产生相应的 Trap 信息并发送给 NMS。

网络需求

- Device2 与 NMS 服务器路由可达。
- Device2 为代理设备 Agent，Device1 为被代理设备。
- Device1、Device2 上都运行 SNMP v3。
- NMS 上运行 SNMP v3。NMS 通过 SNMP v3 对 Device1、Device2 进行管理。

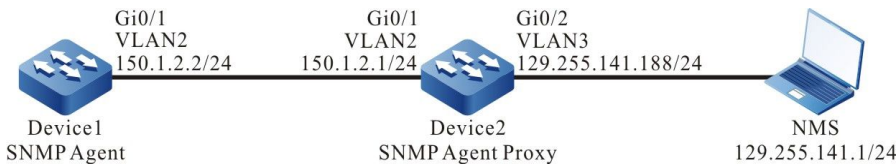
网络拓扑

图 74-7 配置 SNMP v3 代理转发组网图

配置步骤

- 步骤 1： 配置 VLAN，并将端口加入对应的 VLAN。（略）
- 步骤 2： 配置各接口的 IP 地址（略）。
- 步骤 3： 在代理设备 Device2 上启动 SNMP 代理，并配置 SNMPv3 基本信息。

#配置 Device2。

启动 SNMP 代理，配置节点视图名为 default，且可以访问节点 1.3.6.1 下的所有对象。

```
Device2#configure terminal
Device2(config)#snmp-server start
Device1(config)#snmp-server view default 1.3.6.1 include
```

配置用户组为 group-local，安全级别为 authpriv，读写视图、notify 视图均使用 default；配置用户名为 user1，属于用户组 group-local，认证算法为 MD5，认证密码为 proxy，加密算法为 DES，加密密码为 proxy。

```
Device1(config)#snmp-server group group-local v3 authpriv read default write default notify default
Device1(config)#snmp-server user user1 group-local v3 auth md5 admin encrypt des admin
```

步骤 4: 在被代理设备 Device1 上启动 SNMP 代理, 并配置 SNMP 视图。

#配置 Device1。

```
Device1#configure terminal
Device1(config)#snmp-server start
Device1(config)#snmp-server view default 1.3.6.1 include
```

步骤 5: 在代理设备 Device2 上配置被代理设备的相关信息。

#配置 Device2。

配置被代理设备的 IP 地址以及 engineID。

```
Device2(config)#snmp-server engineID remote 150.1.2.2 161 800016130300017a000137
```

配置被代理设备的用户组为 group-user, 安全级别为 authpriv, 读写视图、notify 视图均使用 default。

```
Device2(config)#snmp-server group group-user v3 authpriv read default write default notify default
```

配置用户名为 re-user, 属于用户组 group-user, 认证算法为 MD5, 认证密码为 admin, 加密算法为 DES, 加密密码为 admin。

```
Device2(config)#snmp-server user re-user group-user remote 150.1.2.2 161 v3 auth md5 admin encrypt des
admin
```

配置本地地址参数名为 plocal, 远程地址参数名为 puser; 配置目标地址名为 tuser, 使用地址参数 puser。

```
Device2(config)#snmp-server AddressParam plocal v3 user1 authpriv
Device2(config)#snmp-server AddressParam puser v3 re-user authpriv
Device2(config)#snmp-server TargetAddress tuser 150.1.2.2 161 puser taguser 10 2
```

配置代理转发名称为 proxy-re-user, 操作权限为 write, 被代理设备的 engineID 为 800016130300017a000137, 使用的地址参数 plocal, 使用目标地址 tuser; 配置上下文环境名 proxyuser。

```
Device2(config)#snmp-server proxy proxy-re-user write 800016130300017a000137 plocal tuser proxyuser
Device2(config)#snmp-server context proxyuser
```

#查看 Device2 的 engineID 信息。

```
Device2#show snmp-server engineID
Local engine ID: 8000161303000000052fd
```

IPAddress: 150.1.2.2 remote port: 161 remote engine ID: 800016130300017a000137

说明：

- 远端设备的 `enginID` 必须和被代理设备的一致，设备的 `enginID` 可以通过命令 `show snmp-server engineID` 查看。
 - 被代理设备监听协议为 UDP，端口为 161。
-

步骤 6： 在被代理设备 Device1 上进行 SNMPV3 的相关配置。

#配置 Device1。

配置用户组为 `g1`，安全级别为 `authpriv`，读写视图、`notify` 视图均使用 `default`；用户名为 `re-user`，认证算法为 `MD5`，认证密码为 `admin`，加密算法为 `DES`，加密密码为 `admin`。

```
Device1(config)#snmp-server group g1 v3 authpriv read default write default notify default
Device1(config)#snmp-server user re-user g1 v3 auth md5 admin encrypt des admin
Device1(config)#snmp-server context proxyuser
```

步骤 7： 配置 NMS。

#SNMP v3 采用认证和加密的安全机制，在 NMS 上需要设置用户名，选择安全级别。根据不同的安全级别，需要分别设置认证算法、认证密码、加密算法、加密密码等。另外，还要设置“超时”时间和“重试次数”。用户可利用网管系统完成对设备的查询和配置操作。当要查询或配置被代理设备时，NMS 上还需要设置代理转发的 `enginID` 为被代理设备的 `enginID`。

步骤 8： 检验结果。

#NMS 上能通过 MIB 节点查询、设置设备 Device2 和 Device1 某些参数的值。

75 RMON

75.1 RMON 简介

网络管理的一个重要作用在于对网络各个元素性能方面的监控，在传统的 SNMP 网络管理模式，管理的主动权更多地掌握在网管工作站侧，一般是通过网管工作站定时轮询各个设备的数据，然后在网管系统中进行统计分析，进而得出管理员所需的信息，这种方式下需要网管工作站向网络设备发送和接收大量的报文，当网络中的设备数量较多时，会给网络造成额外的负荷，同时会因为网络阻塞等因素给网管系统的运行带来各种意外。针对这种情况，提出了 RMON (Remote Network Monitoring, 远程网络监视) 的概念。

RMON 的实现仍然需要 SNMP 协议支持，它实际上是一组 MIB，分配在 MIB-2 下面，对象标识符为 1.3.6.1.2.1.16。和其它普通 MIB 相比，RMON 的差别在于其实现过程中加入了在 Agent 侧的计算，即把诸如性能统计等处理放到了设备中，这样在整个网络中实现了分布式处理，减少了前面所述的单纯网管工作站轮询所带来的不足。

由于 RMON 需要实现大量计算功能，所以以前的 RMON 代理 (又称为 Probe) 一般由专门的设备充当，分布在网络中对相应的目标进行监控。随着网络设备处理能力的提高，现在 RMON 逐渐融合到了网络设备本身里面，从而更高效地实现了 RMON 的要求。但是与此同时，这也对网络设备提出了更高的性能要求，毕竟 RMON 进行的计算往往会占用大量的系统资源，降低系统整体性能，这也是管理所带来的额外开销，因此 RMON 更多是在具备网络处理能力的硬件中实现，比如交换芯片。

RMON MIB 共分为 10 组：

- statistics: 对设备所有以太网接口进行的统计，如广播、冲突等的数据；
- history: 记录从 statistics 组取出来的周期性的统计信息采样；
- alarm: 允许管理控制台用户设置取样时间间隔并告警由 RMON 代理记录的任何

计数器或整数超出阈值；

- host: 包含依附于该子网的各种类型主机的进出流量；
- hostTopN: 包含存储的主机统计信息，这些主机的主机表中某些参数最高；
- matrix: 以矩阵的形式表示错误和利用信息，以便操作员能用任何一对地址对来检

索信息；

- filter: 允许监视器对和过滤器匹配的数据包进行观测；
- capture: 分组捕获组建立一组缓冲区，用于存储从通道中捕获的分组。
- event: 给出由 RMON 代理产生的所有事件的表；
- tokenRing: 维护子网为令牌环网的统计和配置信息。

75.2 RMON 功能配置

表 75-1 RMON 功能配置列表

配置任务	
使能 RMON 功能	使能 RMON 功能
配置 RMON 告警组	配置 RMON 告警实例
配置 RMON 事件组	配置 RMON 触发事情
配置 RMON 历史组	配置 RMON 历史组实例
配置 RMON 统计组	配置 RMON 统计管理功能

75.2.1 使能 RMON 功能 **-B -S -E -A**

配置条件

无

使能 RMON 功能

RMON 使能是为 RMON 的监控功能提供相关资源，只有配置了 RMON 的监控组功能后，资源才会生效。

表 75-2 使能 RMON 功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
使能 RMON 功能	rmon	必选

75.2.2 配置 RMON 告警组***-B -S -E -A***

RMON 告警组功能是指配置多个告警，每个告警监控一个告警实例，在取样时间间隔内当告警实例数据值变化超过上升门限值或者下降门限值时就会触发告警事件，按照告警事件组定义的处理方式进行告警处理。数据值连续超过门限值时，只对第一次超越进行告警。

配置条件

在配置 RMON 告警组之前，首先完成以下任务：

- 使能 SNMP 代理功能；
- 使能 SNMP 中 RMON 的 TRAP 功能。

配置 RMON 告警实例

表 75-3 配置 RMON 告警实例

步骤	命令	说明
进入全局配置模式	configure terminal	-
使能 RMON 功能	rmon	可选

步骤	命令	说明
配置 RMON 告警组	rmon alarm <i>alarm-num</i> <i>OID interval</i> { absolute delta } risingthreshold <i>rising-threshold</i> [<i>rising-event</i>] fallingthreshold <i>falling-threshold</i> [<i>falling-event</i>] [owner <i>owner</i>]	必选 缺省情况下为告警触发事件组为 1 缺省情况下为告警组的拥有者为 config

75.2.3 配置 RMON 扩展告警组

-B -S -E -A

RMON 扩展告警组可以对告警变量进行运算，然后将运算结果和设置的阈值比较，实现更为丰富的告警功能。

配置条件

在配置 RMON 告警组之前，首先完成以下任务：

- 使能 SNMP 代理功能；
- 使能 SNMP 中 RMON 的 TRAP 功能。
- 配置一个统计组

配置 RMON 告警实例

表 75-4 配置 RMON 告警实例

步骤	命令	说明
进入全局配置模式	configure terminal	-
使能 RMON 功能	rmon	可选

步骤	命令	说明
配置统计组	rmon statistics ethernet <i>statistics-num</i> <i>OID</i> [owner <i>owner</i>]	必选 缺省情况下为统计组的拥有者为 config
配置 RMON 告警组	rmon prialarm <i>alarm-num</i> <i>WORD interval</i> { absolute delta } risingthreshold <i>rising-threshold</i> <i>rising-</i> <i>event</i> fallingthreshold <i>falling-threshold</i> <i>falling-</i> <i>event</i> entrytype forever [owner <i>owner</i>]	必选 缺省情况下为告警组的拥有者为 config

75.2.4 配置 RMON 事件组

-B -S -E -A

配置 RMON 事件组功能是指配置多个事件，定义每个事件的事件编号以及处理方式，事件有如下几种处理方式：事件记录在日志，事件发送 TRAP 消息到网管，将事件记录在日志并发送 TRAP 消息到网管，不做处理。

配置条件

在配置 RMON 事件组之前，首先完成以下任务：

- 使能 SNMP 代理功能；
- 使能 SNMP 中 RMON 的 TRAP 功能。

配置 RMON 触发事件

RMON 触发事件主要用于 RMON 告警发生时的事件处理。

表 75-5 配置 RMON 触发事件

步骤	命令	说明
进入全局配置模式	configure terminal	-
使能 RMON 功能	rmon	可选
配置 RMON 事件组	rmon event event-num [description event- description /log max- num /owner owner / trap communit]	必选 缺省情况下事件组的拥有者为 config

75.2.5 配置 RMON 历史组

-B -S -E -A

配置 RMON 历史组功能是指配置多个历史组，RMON 历史组存储的是以固定间隔取样所获得的子网数据。该组由历史控制表和历史数据组成，控制表定义被取样的子网接口编号，取样间隔大小，以及每次取样数据的多少，而数据表则用于存储取样期间获得的各种数据。

配置条件

在配置 RMON 历史组之前，首先完成以下任务：

- 使能 SNMP 代理功能。

配置 RMON 历史组实例

RMON 历史组主要配置历史控制表的监控对象，取样间隔大小，以及取样数据多少等信息。

表 75-6 配置 RMON 历史组实例

步骤	命令	说明
进入全局配置模式	configure terminal	-

步骤	命令	说明
使能 RMON 功能	rmon	可选
配置 RMON 历史组	rmon history control <i>history-num</i> <i>OID</i> <i>buckets-num</i> [interval <i>interval</i>] [owner <i>owner</i>]	必选 缺省情况下取样的时间间隔为 1800 秒 缺省情况下历史组的拥有者为 config

75.2.6 配置 RMON 统计组

-B -S -E -A

配置 RMON 统计组功能是配置监控对象为以太网接口的统计信息。统计组提供一个表，该表每一行表示一个子网的统计信息，网络管理员可以从表中获取一个网段的各种统计信息（一个网段的流量，各种类型包的分布，各种类型错误包数、碰撞次数等）。

配置条件

在配置 RMON 统计组之前，首先完成以下任务：

- 使能 RMON 功能；
- 使能 SNMP 代理功能。

配置统计管理功能

表 75-7 配置 RMON 统计管理功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
使能 RMON 功能	rmon	必选

步骤	命令	说明
配置 RMON 统计组	rmon statistics ethernet statistics-num <i>OID</i> [owner owner]	必选 缺省情况下统计组的拥有者为 config

75.2.7 RMON 监控与维护 **-B -S -E -A**

表 75-8 RMON 监控与维护

命令	说明
show rmon alarm	显示设备中已经配置的 RMON 告警
show rmon alarm supportVariable	显示设备中 RMON 支持的监控对象
show rmon event	显示设备中已经配置的 RMON 事件
show rmon history { control ethernet control-num }	显示设备中已经配置的 RMON 历史组
show rmon prialarm	显示设备中已经配置的 RMON 扩展告警
show rmon statistics ethernet	显示设备中已经配置的 RMON 统计组

75.3 RMON 典型配置举例

75.3.1 配置 RMON 基本功能 **-B -S -E -A**

网络需求

- Device 为 RMON 代理设备，与 NMS 服务器路由可达。
- 通过 NMS 对 RMON 的事件组、告警组、历史组、统计组进行监控和管理。

网络拓扑



图 75-1 配置 RMON 基本功能组网图

配置步骤

步骤 1： 配置 VLAN，并将端口加入对应的 VLAN。（略）

步骤 2： 配置各接口的 IP 地址。（略）

步骤 3： 配置 SNMP 代理。

#启动 SNMP 代理，并配置节点视图名为 default、只读团体名为 public。

```
Device#configure terminal
Device(config)#snmp-server start
Device(config)#snmp-server view default 1.3.6.1 include
Device(config)#snmp-server community public view default ro
```

#使能 SNMP Trap 功能，并配置 Trap 报文的目的地址以及使用的团体名。

```
Device(config)#snmp-server enable traps
Device(config)#snmp-server host 129.255.151.1 traps community public
```

步骤 4： 配置 Device 的 RMON 事件组、告警组、历史组、统计组。

#启动 RMON 代理。

```
Device(config)#rmon
```

#配置 Event 事件组的序号为 1，对端口 gigabitethernet0/1 的入方向的报文进行记录。

```
Device(config)#rmon event 1 description gigabitethernet0/1_in_octets log 100 trap public
```

#配置 Alarm 告警事件组，监控对象为 ifInOctets.1，配置相对值采样，采样间隔为 10 秒。配置上升和下降门限值为 100，配置到了门限值触发的事件是 event 1。

```
Device(config)#rmon alarm 1 ifInOctets.1 10 delta risingthreshold 100 1 fallingthreshold 100 1 owner 1
```

#配置 RMON 的统计组。

```
Device(config)#rmon statistics ethernet 1 ifIndex.1
```

#配置 RMON 的历史组。

```
Device(config)#rmon history control 1 ifIndex.1 10
```

说明：

- 实例索引号 ifInOctets.1 对应的端口是设备上的 gigabitethernet0/1。可以通过 show interface switchport snmp ifindex 显示所有 2 层口 snmp index 值，show interface snmp ifindex 显示所有 3 层口 snmp index 值，show interface switchport XXXX snmp ifindex 显示指定 2 层口 snmp index 值，show interface XXXX snmp ifindex 显示指定 3 层口 snmp index 值
 - 远程监控的对象实例索引号，需要从 MIB-2 中的接口表 ifEntry 中进行读取。
-

步骤 5： 配置 NMS。

#在使用 SNMP v1/v2c 版本的 NMS 上需要设置“只读团体名”、“超时”时间和“重试次数”。

步骤 6： 检验结果。

#查看 Device 的 RMON 事件组表项配置。

```
Device#sh rmon event
Event 1 is active, owned by config
Description : gigabitethernet_0/1_in_octes
Event firing causes: log and trap, last fired at 11:38:07

Current log entries:
-----
logIndex      logTime      Description
-----
1             11:38:07    gigabitethernet_0/1_in_octes
```

#查看 Device 的 RMON 告警表项配置。

```
Device#show rmon alarm
Alarm 1 is active, owned by 1
Monitoring variable: ifInOctets.1, Sample interval: 10 second(s)
Taking samples type: delta, last value was 4225
Rising threshold : 100, assigned to event: 1
Falling threshold : 100, assigned to event: 1
```

#查看 Device 的 RMON 统计组表项配置。

```
Device#sh rmon statistics ethernet
-----
Ethernet statistics table information:
  Index: 1
  Data Source: ifIndex.1
  Owner: config
  Status: Valid
-----
ifIndex.1 statistics information:
-----
DropEvents:0
Octets: 26962295
Pkts:252941
BroadcastPkts:156943
MulticastPkts:62331
CRCAlignErrors:51
UndersizePkts:0
OversizePkts:0
Fragments:0
Jabbers:0
Collisions:0
Pkts64Octets:167737
Pkts65to127Octets:47962
Pkts128to255Octets:22497
Pkts256to511Octets:9967
Pkts512to1023Octets:4032
Pkts1024to1518Octets:745
```

#查看 Device 的 RMON 历史组表项配置。

```
Device#show rmon history control
-----
RMON history control entry index: 1
  Data source: IfIndex.1
  Buckets request: 10
  Buckets granted: 2
  Interval: 1800
  Owner: config
  Entry status: Valid
-----
```

#NMS 通过 MIB 节点可以查询设备 Device 中的 History、Event 和 Statistics 的信息。

NMS 能够收到来自设备 Device 的 Alarm 告警事件的 Trap 信息。例如当监控接口的入方向流量变化率大于上升门限或者小于下降门限，Device 会产生相应的 Trap 信息并发送给 NMS。

虚拟化

76 VST

76.1 VST 简介

随着用户降低成本和提高设备可靠性的要求不断高涨，我司提出了一种将多台物理交换机组合成一台虚拟交换机的技术，即 Virtual Switching Technology（虚拟交换技术），简称 VST。

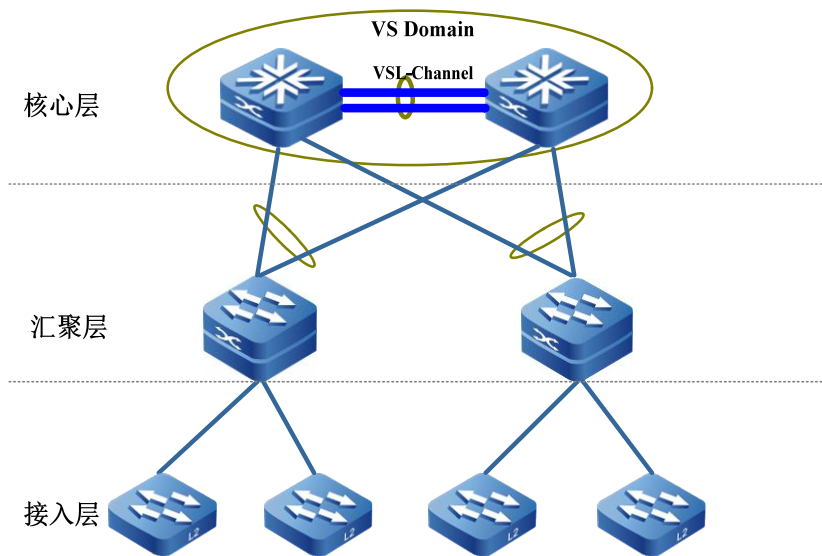


图 76-1 VST 物理网络视图

如图 1-1 所示，在核心层的两台设备之间通过虚拟交换链路接口连接，形成一个 VS Domain（虚拟交换域，也称堆叠系统），汇聚层设备通过链路汇聚上联到 VS Domain，核心层的 VS Domain 对其他网络设备来说就是一台虚拟设备。

该技术相对传统二层生成树和三层 VRRP/VBRP 技术，具有下列优势：

- 带宽成倍增加并被有效利用

传统的技术方案，由于运行 STP/RSTP/MSTP，原有两条上联链路会有一条处于转发状态，另一条链路处于备份状态；使用虚拟交换技术后，多个设备成为了一个单一的逻辑设备，因此不再需要把一些链路阻塞，两条链路形成一个汇聚组，都可以用来转发数据，从而有效利用这些链路的带宽，不会造成带宽资源浪费。另外，通过跨设备和跨板卡的聚合链路既可以提供冗余链路，又可以实现动态负载均衡，有效利用所有带宽。

- 高可靠性

虚拟交换系统由多台成员设备组成。主控设备负责整个虚拟交换系统的运行、管理和维护，其他成员设备处于备份状态。一旦主控设备发生故障，不再依赖 STP/RSTP/MSTP、VRRP/VBRP 等协议的收敛，系统会迅速从其他处于备份状态的成员设备中选举出新的主控设备，保证虚拟交换系统的业务不中断，在成员出现故障时提高了可靠性。

- 简化网络拓扑

通过虚拟交换技术形成的虚拟设备在网络中相当于一台设备。通过聚合链路与周边设备相连，因为不存在二层环路，所以没有必要配置 STP/RSTP/MSTP 协议。各种控制层协议运行在一台虚拟设备上，减少了设备间大量协议报文的交互，缩短了路由收敛时间。

- 统一管理

两台或多台设备形成堆叠系统之后，虚拟交换系统中的成员设备控制平面处于备份状态，但其数据平面是活动的，用户通过任意成员设备的端口均可登录虚拟交换系统，对整个虚拟设备进行统一管理，而不需要连接到每台成员设备上分别进行管理。

76.1.1 基本概念

虚拟交换域

虚拟交换域由一台或者多台成员设备组成。同一个虚拟交换域中的成员设备，其域编号配置必须相同。域编号唯一决定一个虚拟交换域。由于虚拟交换域 MAC 地址使用虚拟 MAC 地址模式获取时，虚拟交换域编号唯一决定该 MAC 地址，因此在同一个局域网中，多个堆叠系统之间的域编号不能相同。

虚拟交换成员设备

虚拟交换域中的每台物理设备亦称为虚拟交换成员设备。同一个堆叠域中，成员编号唯一决定一台成员设备。

虚拟交换链路接口及其成员端口

将多个具有堆叠能力的物理端口捆绑在一起形成一个虚拟交换链路接口（VSL-Channel）。虚拟交换链路接口是堆叠系统中各成员设备之间进行内部协议报文交互以及业务数据转发的逻辑链路通道，其中的物理端口都称为虚拟交换链路成员端口。

各成员设备加入同一个虚拟交换域，相互之间通过虚拟交换链路接口进行互联，最后形成一台虚拟设备。

LMP

LMP（Link Manage Protocol，链路管理协议）用于进行虚拟交换链路接口及其成员端口的管理。

RRP

RRP（Role Resolution Protocol，角色选举协议）用于进行堆叠系统中成员设备角色选举。

TDP

TDP（Topology Discovery Protocol，拓扑发现协议）用于通告堆叠系统内的成员设备信息，确保堆叠系统内所有成员设备信息的一致性。

76.2 VST 功能配置

表 76-1 VST 功能配置列表

配置任务	
配置虚拟交换成员设备	配置虚拟交换成员设备域编号
	配置虚拟交换成员设备编号

配置任务	
	配置虚拟交换成员设备优先级
配置虚拟交换链路接口	创建虚拟交换链路接口
	配置端口加入虚拟交换链路接口
配置设备运行模式	配置设备运行模式

76.2.1 配置虚拟交换成员设备 -B -S -E -A

在设备加入虚拟交换堆叠域前或者已经加入虚拟交换堆叠域后，都可以对设备进行相应的配置，包括修改其成员编号，域编号，优先级。

说明：

- 在堆叠模式下，修改虚拟交换成员设备的成员编号或域编号后，新配置的成员编号或域编号并不会立即生效，只有等到对应的虚拟交换成员设备保存配置并重启后，相应的配置才会生效。

配置条件

无

配置虚拟交换成员设备域编号

表 76-2 配置虚拟交换成员设备域编号

步骤	命令	说明
进入虚拟交换成员配置模式	switch virtual member member-id	-

步骤	命令	说明
配置虚拟交换成员设备域编号	domain <i>domain-id</i>	必选 缺省情况下，虚拟交换成员设备域编号为100

注意：

- 在堆叠模式下，将虚拟交换成员设备加入虚拟交换域中时，必须确保各虚拟交换成员设备域编号是相同的，否则虚拟交换成员设备将不能加入同一个虚拟交换域中。
- 在堆叠模式下，修改域编号后，新的域编号并不会立即生效，只有该虚拟交换成员设备保存配置并重启后，新的域编号才会生效。

配置虚拟交换成员设备编号

配置虚拟交换成员设备编号，对应两种情况：第一种情况，设备从未配置过虚拟交换成员设备编号，需要配置一个虚拟交换成员设备编号；第二种情况，设备已经配置了虚拟交换成员设备编号，需要修改为新的虚拟交换成员设备编号。所以配置虚拟交换成员设备编号，有两条命令，一条是配置虚拟交换成员设备编号，一条是修改虚拟交换成员设备编号，如表 1-3 所示。

表 76-3 配置 VST 成员设备编号

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置虚拟交换成员设备编号	switch virtual member <i>member-id</i>	必选 缺省情况下，设备无虚拟交换成员设备编号

步骤	命令	说明
修改虚拟交换成员设备编号	switch virtual member <i>member-id</i> rename <i>member-id-new</i>	可选

注意：

- 在堆叠模式下，修改虚拟交换成员设备编号后，必须保存配置并重启系统，新的虚拟交换成员设备编号才会生效。
- 在一个虚拟交换域中，每台虚拟交换成员设备的成员编号是独一无二的，不能出现两个虚拟交换成员设备的成员编号相同的情况，否则虚拟交换成员设备不能进行正常堆叠。

配置虚拟交换成员设备优先级

当多个虚拟交换成员设备加入同一个虚拟交换域时，可以通过配置各虚拟交换成员设备的优先级来提高虚拟交换成员设备当选为主控设备的可能性，优先级数值越大的越优先。

表 76-4 配置虚拟交换成员设备优先级

步骤	命令	说明
进入虚拟交换成员配置模式	switch virtual member <i>member-id</i>	-
配置虚拟交换成员设备优先级	priority <i>priority-num</i>	必选 缺省情况下，虚拟交换成员设备的优先级为 100

说明：

- 虚拟交换域中虚拟交换主控设备的选举规则：
 1. 虚拟交换主控设备优先；存在多个虚拟交换主控设备情况下，进行第二步比较，无虚拟交换主控设备进行第三步比较，否则结束比较；
 2. 作为虚拟交换主控设备运行时间长的优先；主控设备运行时间相同情况下，进行第三步比较，否则结束比较；
 3. 优先级大的优先；优先级相同情况下，进行第四步比较，否则结束比较；
 4. 成员编号小的优先。

76.2.2 配置虚拟交换链路接口 -B -S -E -A

虚拟交换链路接口 (VSL-Channel) 是一个逻辑接口。其通过将多个支持堆叠的物理端口捆绑在一起，从而实现对这些物理端口的统一管理。任何对虚拟交换链路接口的操作都将同时作用到每个物理成员端口。

配置条件

无

创建虚拟交换链路接口

表 76-5 创建虚拟交换链路接口

步骤	命令	说明
进入全局配置模式	configure terminal	-
创建虚拟交换链路接口	vsl-channel <i>vsl-channel-id</i>	必选 在单机模式下 <i>vsl-channel-id</i> 为一维值表示虚拟交换链路接口编号；堆叠模式下为二维值，第一维为虚拟交换成员编

步骤	命令	说明
		号，第二维为虚拟交换链路接口编号

注意：

- 删除虚拟交换链路接口时，虚拟交换链路接口内所有成员端口将全部退出该虚拟交换链路接口，成员端口的所有配置恢复为缺省情况。在删除虚拟交换链路接口前，请确认删除后网络中不会出现环路。

配置端口加入虚拟交换链路接口

表 76-6 配置端口加入虚拟交换链路接口

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二层以太接口配置模式	interface <i>interface-name</i>	-
配置端口加入虚拟交换链路接口	vsl-channel <i>vsl-channel-id</i> mode on [type extern]	必选

说明：

- 虚拟交换链路接口中的所有成员端口，端口能力级必须相同。

76.2.3 配置设备运行模式 **-B -S -E -A**

当前设备支持两种运行模式，单机模式及堆叠模式。设备只有以堆叠模式运行才能与其他虚拟交换成员设备形成一个虚拟交换域。

配置条件

无

配置设备运行模式

表 76-7 配置设备运行模式

步骤	命令	说明
进入特权用户模式	enable	-
配置设备运行模式	switch mode { stand-alone virtual }	必选 缺省情况下，设备以单机模式运行

说明：

- 当设备的运行模式发生改变后，设备将会进行重启，并在重启后以新的配置模式运行。
- 设备的不同运行模式，都对应各自独立的启动配置文件。
- 将设备切换到堆叠模式运行前，必须确保已经配置了虚拟交换成员设备编号，否则将不能进行切换。

表 76-8 VST 监控与维护

命令	说明
show switch virtual	显示虚拟交换域的基础信息
show switch virtual local config	显示本地虚拟交换成员设备的基础配置信息
show switch virtual local current	显示本地虚拟交换成员设备的基础运行信息
show switch virtual member member-id [config current]	显示虚拟交换成员设备的基础信息
show switch virtual topo	显示本地虚拟交换成员设备到虚拟交换域中其他虚拟交换成员设备的转发路径信息
show switch vsl-channel [vsl-channel-id]	显示虚拟交换域中虚拟交换链路接口的信息

76.3 VST 典型配置举例

76.3.1 配置设备形成链形堆叠系统

-B -S -E -A

网络需求

- 实现 Device0、Device1 形成链形堆叠系统，其中 Device0 成为主控设备。

网络拓扑

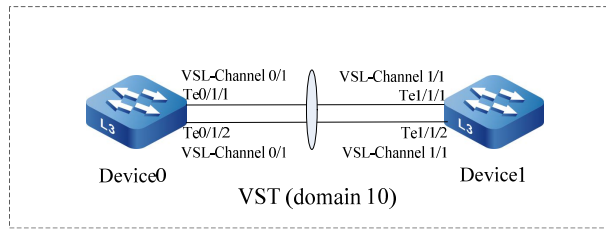


图 76-2 配置设备形成链形堆叠系统

配置步骤

步骤 1: 配置 Device0。

#在 Device0 上配置虚拟交换成员设备编号为 0，并配置域编号为 10，优先级为 255。

```
Device0#configure terminal
Device0(config)#switch virtual member 0
Do you want to modify member id(Yes|No)?y
% Member ID 0 config will take effect only after the exec command 'switch mode virtual' is issued
Device0(config-vst-member-0)#domain 10
% Domain ID 10 config will take effect only after the exec command 'switch mode virtual' is issued
Device0(config-vst-member-0)#priority 255
Device0(config-vst-member-0)#exit
```

#在 Device0 上创建虚拟交换链路接口 1，并将端口 tengigabitethernet1/1 和 tengigabitethernet1/2 加入虚拟交换链路接口 1。

```
Device0(config)#vsl-channel 1
Device0(config-vsl-channel-1)#exit
Device0(config)#interface tengigabitethernet 1/1-1/2
Device0(config-if-range)#vsl-channel 1 mode on
Device0(config-if-range)#exit
```

#在 Device0 上保存配置。

```
Device0#write
Are you sure to overwrite /flash/startup (Yes|No)?y
Building Configuration...done
Write to startup file ... OK
Write to mode file... OK
```

步骤 2: 配置 Device1。

#在 Device1 上配置虚拟交换成员设备编号为 1，并配置域编号为 10，优先级为 200。

```
Device1#configure terminal
Device1(config)#switch virtual member 1
```

```
Do you want to modify member id(Yes|No)?y
% Member ID 1 config will take effect only after the exec command 'switch mode virtual' is issued
Device1(config-vst-member-1)#domain 10
% Domain ID 10 config will take effect only after the exec command 'switch mode virtual' is issued
Device1(config-vst-member-1)#priority 200
Device1(config-vst-member-1)#exit
```

#在 Device1 上创建虚拟交换链路接口 1，并将端口 tengigabitethernet1/1 和 tengigabitethernet1/2 加入虚拟交换链路接口 1。

```
Device1(config)#vsl-channel 1
Device1(config-vsl-channel-1)#exit
Device1(config)#interface tengigabitethernet 1/1-1/2
Device1(config-if-range)#vsl-channel 1 mode on
Device1(config-if-range)#exit
```

#在 Device1 上保存配置。

```
Device1#write
Are you sure to overwrite /flash/startup (Yes|No)?y
Building Configuration...done
Write to startup file ... OK
Write to mode file... OK
```

步骤 3: 配置 Device0、Device1 运行模式为堆叠模式。

#配置 Device0 运行模式为堆叠模式。

```
Device0#switch mode virtual
This command will convert all interface names to naming convention "interface-type member-
number/slot/interface" ,
Please make sure to save current configuration.Do you want to proceed? (yes|no)?y
Converting interface names Building configuration...
Copying the startup configuration to backup file named "startup-backupalone"...
Please wait...system reloading is in progress!
ok
Reset system!
Jul 30 2014 17:36:14: %SYS-5-RELOAD: Reload requested
```

#配置 Device1 运行模式为堆叠模式。

```
Device1#switch mode virtual
This command will convert all interface names to naming convention "interface-type member-
number/slot/interface" ,
Please make sure to save current configuration.Do you want to proceed? (yes|no)?y
Converting interface names Building configuration...
Copying the startup configuration to backup file named "startup-backupalone"...
Please wait...system reloading is in progress!
ok
Reset system!
Jul 30 2014 17:36:20: %SYS-5-RELOAD: Reload requested
```

步骤 4: 检验结果。

#在 Device0 上查看，已经形成链形堆叠系统，且 Device0 为主控设备。

```
Device0#show switch virtual
Codes: L - local-device,I - isolate-device

Virtual Switch Mode      : VIRTUAL
Virtual Switch DomainId  : 10
Virtual Switch mac-address : 0001.7a6a.001b
```

```
----- VST MEMBER INFORMATION -----
CODE MemberID Role Pri LocalVsl RemoteVsl
-----
L 0 Master 255 vsl-channel 0/1 vsl-channel 1/1
  1 Member 200 vsl-channel 1/1 vsl-channel 0/1
```

77 MAD

77.1 MAD 简介

当堆叠系统中虚拟交换链路接口发生故障，堆叠系统分裂为多个虚拟交换域，出现多台全局配置完全相同的虚拟交换主控设备（以下简称为主控设备），这种情况称之为多激活。由于分裂出去的逻辑设备与原逻辑设备的全局配置完全相同，会出现网络配置冲突，导致流量异常。为避免这种情况对业务的影响，MAD（Multi-Active Detection，多激活检测）应运而生。

当前堆叠系统支持两种 MAD 方式：MAD LACP、MAD Fast-Hello，可以满足不同的组网需求。

MAD 状态分为两种：Active 状态、Recovery 状态。Active 状态表示正常工作状态，Recovery 状态表示禁用状态。禁用状态下，除虚拟交换链路成员端口、保留口以外的所有二/三层以太网接口、VLAN 接口都会被 MAD 关闭。

设备收到 MAD 检测报文时，会把报文中的数据与本逻辑设备的数据进行比较。若报文中的 VS Domain ID（发送端的虚拟交换域编号）与本逻辑设备的相同，且报文中的 Master ID（发送端所在虚拟交换域中，主控设备的成员编号）与本逻辑设备不同，则认为发生了多激活，开始多激活竞选。按照一定的竞选规则，同一虚拟交换域中，只会保留一台逻辑设备仍然保持 Active 状态，其他逻辑设备会进入 Recovery 状态。

MAD LACP 组网时必须使用中间设备，MAD Fast-Hello 组网时可以使用中间设备，也可以直连。若采用直连方式，需要保证任意两台虚拟交换成员设备间都有直连的线路用于多激活检测，即需要保证全连接。

77.2 MAD 功能配置

表 77-1 MAD 功能配置列表

配置任务	
配置 MAD LACP 功能	配置 MAD LACP 功能
配置 MAD Fast-Hello 功能	配置 MAD Fast-Hello 功能
配置保留口	配置保留口
配置恢复 MAD 状态为 Active 状态	配置恢复 MAD 状态为 Active 状态

77.2.1 配置 MAD LACP 功能

-B -S -E -A

MAD LACP 多激活检测通过扩展 LACP 协议报文字段，实现多激活检测及竞选。

配置条件

无

配置 MAD LACP 功能

表 77-2 配置 MAD LACP 功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
创建动态汇聚组	link-aggregation <i>link-aggregation-id</i> mode lacp	必选 缺省情况下，未创建指定汇聚组
进入汇聚组配置模式	link-aggregation <i>link-aggregation-id</i>	-
使能 MAD LACP 功能	mad enable	必选 缺省情况下，未使能 MAD LACP 功能

说明：

- 动态汇聚组才支持使能 MAD LACP 功能。
- 组网时使用的中间设备必须是支持 LACP 报文透传功能的我司设备。

77.2.2 配置 MAD Fast-Hello 功能

-B -S -E -A

MAD Fast-Hello 多激活检测的协议报文为我司自定义，直接携带多激活检测及竞选所需的数据。

配置条件

无

配置 MAD Fast-Hello 功能

表 77-3 配置 MAD Fast-Hello 功能

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置普通模式下的 MAD Fast-Hello 报文发送周期	mad fast-hello normal interval <i>interval-time</i>	可选 缺省情况下，普通模式下的 MAD Fast-Hello 报文发送周期为 2000 毫秒
配置激进模式下的 MAD Fast-Hello 报文发送周期	mad fast-hello aggressive interval <i>interval-time</i>	可选 缺省情况下，激进模式下的 MAD Fast-Hello 报文发送周期为 500 毫秒
配置激进模式持续时间	mad fast-hello aggressive duration <i>duration-time</i>	可选 缺省情况下，激进模式持续时间为 120 秒
进入 VLAN 配置模式	vlan <i>vlan-id</i>	-
配置控制 VLAN	mad fast-hello control-vlan	必选 缺省情况下，没有配置控制 VLAN
进入全局配置模式	exit	-
进入二层以太网接口配置模式	interface <i>interface-name</i>	-
配置端口的链路类型为 Trunk 类型	switchport mode trunk	必选

步骤	命令	说明
		缺省情况下，端口链路类型为 Access 类型
关闭端口的生成树功能	no spanning-tree enable	必选 缺省情况下，端口已使能生成树功能
配置控制端口	mad fast-hello vlan <i>vlan-id</i>	必选 缺省情况下，没有配置控制端口

说明：

- MAD Fast-Hello 的控制 VLAN、控制端口都只能专用于 MAD Fast-Hello 多激活检测，不能再配置其他业务。
- MAD Fast-Hello 的控制端口上，要关闭端口的生成树功能。

77.2.3 配置保留口

-B -S -E -A

当 MAD 状态变为 Recovery 状态时，保留口不会被 MAD 关闭，可以把有特殊用途需要保持 UP 状态的端口、接口（比如管理口），配置为保留口。

配置条件

无

配置保留口

表 77-4 配置保留口

步骤	命令	说明
进入全局配置模式	configure terminal	-
进入二/三层以太接口配置模式	interface interface-name	必选其一 进入二/三层以太接口配置模式后，后续配置只在当前接口生效；进入汇聚组配置模式后，后续配置只在汇聚组生效；进入接口配置模式后，后续配置只在当前接口生效
进入汇聚组配置模式	link-aggregation link-aggregation-id	
进入接口配置模式	interface vlan vlan-id	
配置保留口	mad exclude recovery	必选 缺省情况下，没有配置保留口

说明：

- 已使能 MAD LACP 功能的汇聚组不能配置为保留口。

77.2.4 配置恢复 MAD 状态为 Active 状态

-B -S -E -A

配置条件

无

配置恢复 MAD 状态为 Active 状态

表 77-5 配置恢复 MAD 状态为 Active 状态

步骤	命令	说明
进入全局配置模式	configure terminal	-
配置恢复 MAD 状态为 Active 状态	mad restore	必选 缺省情况下, MAD 状态为 Active 状态

说明:

- MAD 状态变为 Recovery 状态时, 对于已处于关闭状态的端口、接口, MAD 不会处理, 恢复 MAD 状态为 Active 状态时, 只会开启被 MAD 关闭的端口、接口。

77.2.5 MAD 监控与维护

-B -S -E -A

表 77-6 MAD 监控与维护

命令	说明
show mad exclude recovery interface [switchport vlan]	显示已配置的保留口
show mad fast-hello	显示 MAD Fast-Hello 信息
show mad lacp	显示 MAD LACP 信息
show mad status	显示 MAD 状态

77.3 MAD 典型配置举例

77.3.1 配置 MAD LACP 功能

-B -S -E -A

网络需求

- Device0、Device1 形成以 Device0 为主控设备的堆叠系统，PC1 通过堆叠系统访问 IP Network；
- 配置 MAD LACP 功能，使 Device1 设备因虚拟交换链路接口故障从堆叠系统分裂出去后，PC1 能正常访问 IP Network，不会出现因网络配置冲突导致业务异常的情况。

网络拓扑

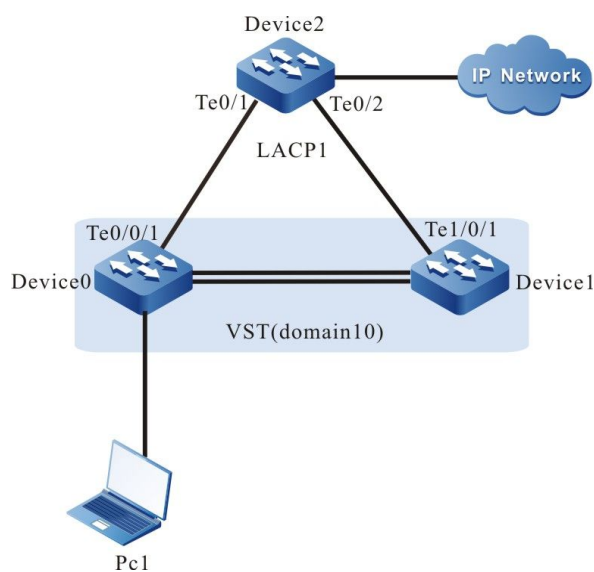


图 77-1 配置 MAD LACP 功能组网图

配置步骤

步骤 1： 使 Device0、Device1 形成以 Device0 为主控设备的堆叠系统。

略

步骤 2： 在 Device0 上配置 MAD LACP 功能。

#在 Device0 上创建 VLAN2，并创建动态汇聚组 1，配置汇聚组 1 链路类型为 Trunk，允许 VLAN 2 的业务通过。

```
Device0#configure terminal
Device0(config)#vlan 2
Device0(config-vlan2)#exit
Device0(config)#link-aggregation 1 mode lacp
Device0(config)#link-aggregation 1
Device0(config-link-aggregation1)#switchport mode trunk
Device0(config-link-aggregation1)#switchport trunk allowed vlan add 2
Device0(config-link-aggregation1)#exit
```

#在 Device0 上将端口 tengigabitethernet0/0/1,tengigabitethernet1/0/1 加入汇聚组 1。

```
Device0(config)#interface tengigabitethernet 0/0/1,1/0/1
Device0(config-if-range)#link-aggregation 1 active
Device0(config-if-range)#exit
```

#在 Device0 的汇聚组 1 上使能 MAD LACP 功能。

```
Device0(config)#link-aggregation 1
Device0(config-link-aggregation1)#mad enable
Device0(config-link-aggregation1)#exit
```

步骤 3： 配置 Device2。

#在 Device2 创建 VLAN2，并创建动态汇聚组 1，配置汇聚组 1 链路类型为 Trunk，允许 VLAN2 的业务通过。

```
Device2#configure terminal
Device2(config)#vlan 2
Device2(config-vlan2)#exit
Device2(config)#link-aggregation 1 mode lacp
Device2(config)#link-aggregation 1
Device2(config-link-aggregation1)#switchport mode trunk
Device2(config-link-aggregation1)#switchport trunk allowed vlan add 2
Device2(config-link-aggregation1)#exit
```

#在 Device2 上将端口 tengigabitethernet0/1,tengigabitethernet0/2 加入汇聚组 1。

```
Device2(config)#interface tengigabitethernet 0/1,0/2
Device2(config-if-range)#link-aggregation 1 active
Device2(config-if-range)#exit
```

步骤 4： 检验结果。

#查看 Device0 上的 MAD LACP 信息。

```
Device0#show mad lacp
-----MAD-LACP INFORMATION-----
Link-aggregation   Mad state
-----
1                   enable
```


#当 Device1 因虚拟交换链路接口故障从堆叠系统分裂出去后，以 Device0 为主控设备的堆叠系统的 MAD 状态为 Active 状态，以 Device1 为主控设备的堆叠系统的 MAD 状态为 Recovery 状态。

```
Device0#show mad status
MAD status: active
```

```
Device1#show mad status
MAD status: recovery
```

#PC1 能访问 IP Network。

77.3.2 配置 MAD Fast-Hello 功能

-B -S -E -A

网络需求

- Device0、Device1 形成以 Device0 为主控设备的堆叠系统；
- 配置 MAD Fast-Hello 功能，使 Device1 设备因虚拟交换链路接口故障从堆叠系统分裂出去后，不会出现因网络配置冲突导致业务异常的情况。

网络拓扑

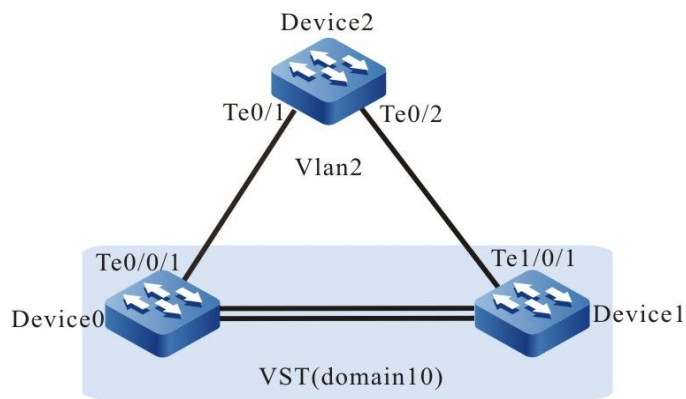


图 77-2 配置 MAD Fast-Hello 组网图

配置步骤

步骤 1： 使 Device0、Device1 形成以 Device0 为主控设备的堆叠系统。

略

步骤 2： 在 Device0 上配置 MAD Fast-Hello 功能。

#在 Device0 上创建 VLAN2，并配置为 MAD Fast-Hello 的控制 VLAN。

```
Device0#configure terminal
Device0(config)#vlan 2
Device0(config-vlan2)#mad fast-hello control-vlan
Device0(config-vlan2)#exit
```

#在 Device0 上配置端口 tengigabitethernet0/0/1,tengigabitethernet1/0/1 的链路类型为 Trunk，并加入 MAD Fast-Hello 的控制 VLAN。

```
Device0(config)#interface tengigabitethernet 0/0/1,1/0/1
Device0(config-if-range)#switchport mode trunk
Device0(config-if-range)#mad fast-hello vlan 2
Device0(config-if-range)#exit
```

#在 Device0 上将端口 tengigabitethernet0/0/1,tengigabitethernet1/0/1 的生成树功能关闭。

```
Device0(config)#interface tengigabitethernet 0/0/1,1/0/1
Device0(config-if-range)#no spanning-tree enable
Device0(config-if-range)#exit
```

步骤 3： 配置 Device2。

#Device2 上创建 VLAN2，并配置端口 tengigabitethernet0/1, tengigabitethernet0/2 的链路类型为 Trunk，允许 VLAN 2 的业务通过。

```
Device2#configure terminal
Device2(config)#vlan 2
Device2(config-vlan2)#exit
Device2(config)#interface tengigabitethernet 0/1,0/2
Device2(config-if-range)#switchport mode trunk
Device2(config-if-range)#switchport trunk allowed vlan add 2
Device2(config-if-range)#exit
```

#在 Device2 上将端口 tengigabitethernet0/1,tengigabitethernet0/2 的生成树功能关闭。

```
Device2(config)#interface tengigabitethernet 0/1,0/2
Device2(config-if-range)#no spanning-tree enable
Device2(config-if-range)#exit
```

步骤 4： 检验结果。

#在 Device0 上查看 MAD Fast-Hello 使能情况。

```
Device0#show mad fast-hello
MAD Fast-Hello Information:
Normal interval   : 2000 ms(default: 2000)
Aggressive interval : 500 ms(default: 500)
Aggressive duration : 120 s (default: 120)
Control vlan      : 2
-----
Interface   Control vlan
-----
te0/0/1     2
te1/0/1     2
```

#当 Device1 因虚拟交换链路接口故障从堆叠系统分裂出去后，以 Device0 为主控设备的堆叠系统的 MAD 状态为 Active 状态，以 Device1 为主控设备的堆叠系统的 MAD 状态为 Recovery 状态。

```
Device0#show mad status  
MAD status: active
```

```
Device1# show mad status  
MAD status: recovery
```