



H3C 中低端 IPv6 以太网交换机

典型配置指导

杭州华三通信技术有限公司

<http://www.h3c.com.cn>

资料版本：20081203-C-1.01

声明

Copyright © 2008 杭州华三通信技术有限公司及其许可者 版权所有，保留一切权利。

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

H3C、**H3C**、Aolynk、、H³Care、、TOP G、、IRF、NetPilot、Neocean、NeoVTL、SecPro、SecPoint、SecEngine、SecPath、Comware、Secware、Storware、NQA、VVG、V²G、VⁿG、PSPT、XGbus、N-Bus、TiGem、InnoVision、HUASAN、华三均为杭州华三通信技术有限公司的商标。对于本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

由于产品版本升级或其他原因，本手册内容有可能变更。H3C 保留在没有任何通知或者提示的情况下对本手册的内容进行修改的权利。本手册仅作为使用指导，H3C 尽全力在本手册中提供准确的信息，但是 H3C 并不确保手册内容完全没有错误，本手册中的所有陈述、信息和建议也不构成任何明示或暗示的担保。

技术支持

用户支持邮箱：customer_service@h3c.com

技术支持热线电话：800-810-0504（固话拨打）

400-810-0504（手机、固话均可拨打）

网址：<http://www.h3c.com.cn>

前言

本书简介

本手册各章节内容如下：

模块	配置举例
01-登录交换机典型配置指导	● 通过 Console 口配置 Telnet 登录方式典型配置指导 ● 通过 Telnet 配置 Console 口登录方式典型配置指导 ● 通过 WEB 网管登录交换机典型配置指导 ● 对登录用户的控制典型配置指导
02-VLAN 典型配置指导	● 基于端口的 VLAN 典型配置指导 ● 基于 MAC 的 VLAN 典型配置指导 ● 基于协议的 VLAN 典型配置指导 ● 基于 IP 子网的 VLAN 典型配置指导 ● Isolate-user-vlan 典型配置指导 ● Super VLAN 典型配置指导
03-GVRP 典型配置指导	GVRP 典型配置指导
04-Voice VLAN 典型配置指导	Voice VLAN 典型配置
05-IP 地址-IP 性能典型配置指导	● IP 地址典型配置指导 ● IP 性能典型配置指导
06-QinQ 典型配置指导	● QinQ 典型配置指导 ● 基于流的灵活 QinQ 典型配置指导
07-BPDU Tunnel 典型配置指导	BPDU Tunnel 典型配置指导
08-VLAN 映射典型配置指导	● 1:1 VLAN 映射和 N:1 VLAN 映射典型配置指导 ● 1:2 VLAN 映射和 2:2 VLAN 映射典型配置指导
09-MAC 地址表管理典型配置指导	MAC 地址表管理典型配置指导
10-链路聚合典型配置指导	链路聚合典型配置指导
11-IP Source Guard 典型配置指导	● 静态绑定表项配置指导 ● 动态绑定表项配置指导
12-LLDP 典型配置指导	LLDP 配置指导
13-MSTP 典型配置指导	● MSTP 典型配置指导 ● RSTP 配置举例

模块	配置举例
14-IPv4 路由典型配置指导	● 静态路典型配置指导 ● RIP 版本典型配置指导 ● RIP 引入外部路由典型配置指导 ● 配置 RIP 接口附加度量值典型配置指导 ● 配置 RIP 发布聚合路由典型配置指导 ● OSPF 基本功能典型配置指导 ● OSPF 应用典型配置指导 ● OSPF 发布聚合路由典型配置指导 ● OSPF 的 Stub 区域典型配置指导 ● OSPF 的 NSSA 区域典型配置指导 ● OSPF 的 DR 选择典型配置指导 ● OSPF 虚连接典型配置指导 ● OSPF GR 典型配置指导 ● 路由过滤典型配置指导 ● IS-IS 基本配置典型指导 ● IS-IS 的 DIS 选择典型配置指导 ● IS-IS 引入外部路由典型配置指导 ● IS-IS GR 典型配置指导 ● IS-IS 验证典型配置指导 ● BGP 基本功能典型配置指导 ● BGP 与 IGP 交互典型配置指导 ● BGP 负载分担典型配置指导 ● BGP 团体典型配置指导 ● BGP 路由反射器典型配置指导 ● BGP 联盟典型配置指导 ● BGP 路径选择典型配置指导 ● 在 IPv4 路由引入中应用路由策略典型配置指导 ● 应用路由策略过滤接收的 BGP 路由典型配置指导
15-IPv6 典型配置指导	● IPv6 基础典型配置指导 ● IPv6 手动隧道典型配置指导 ● IPv4 兼容 IPv6 自动隧道典型配置指导 ● 6to4 隧道典型配置指导 ● ISATAP 隧道典型配置指导
16-IPv6 路由典型配置指导	● IPv6 静态路由典型配置指导 ● IPv6 RIPng 路由协议典型配置指导 ● 配置 RIPng 引入外部路由典型配置指导 ● IPv6 RIPng 跨越 IPv4 网络应用典型配置指导 ● 配置 OSPFv3 区域典型配置指导 ● OSPFv3 引入外部路由典型配置指导 ● OSPFv3 的 DR 选择典型配置指导 ● IPv6 IS-IS 路由协议典型配置指导 ● IPv6 BGP 路由协议基本配置指导 ● IPv6 BGP 路由反射典型配置指导 ● 在 IPv6 路由引入中应用路由策略典型配置指导

模块	配置举例
17-IPv4 组播典型配置指导	● IGMP 典型配置指导 ● IGMP Snooping 典型配置指导 ● 组播 VLAN 典型配置指导 ● PIM 典型配置指导 ● MSDP 典型配置指导 ● 组播路由与转发配置指导 ● MBGP 典型配置指导 ● 组播 VPN 典型配置指导
18-IPv6 组播典型配置指导	● MLD 典型配置指导 ● MLD Snooping 典型配置指导 ● IPv6 组播 VLAN 典型配置指导 ● IPv6 PIM 典型配置指导 ● IPv6 MBGP 典型配置指导
19-802.1x 典型配置指导	● 802.1x 简介 ● 802.1x 典型配置指导 ● Guest VLAN、动态下发 VLAN 典型配置举例 ● 下发 ACL 应用典型配置指导 ● EAD 快速部署典型配置指导
20-AAA 典型配置指导	● Telnet 用户通过 HWTACACS 服务器认证、授权、计费典型配置指导 ● Telnet 用户通过 local 认证、HWTACACS 授权、RADIUS 计费的应用配置 ● SSH 用户通过 RADIUS 服务器认证、授权、计费的应用配置 ● EAD 应用配置
21-MAC 地址认证典型配置指导	● MAC 地址本地认证典型配置指导 ● MAC 地址 RADIUS 认证典型配置指导 ● 下发 ACL 典型配置指导
22-Portal 典型配置指导	● Portal 直接认证方式典型配置指导 ● Portal 二次地址分配认证方式典型配置指导 ● 三层 Portal 认证方式典型配置指导 ● Portal 直接认证方式（支持 EAD）典型配置指导
23-ARP 典型配置指导	● ARP 基本功能典型配置指导 ● 代理 ARP 典型配置指导 ● 端口隔离时的本地代理 ARP 典型配置指导 ● ARP Detection 典型配置举例
24-DHCP 典型配置指导	● DHCP 服务器静态绑定地址典型配置指导 ● DHCP 服务器动态分配地址典型配置指导 ● DHCP 中继典型配置指导 ● DHCP Snooping 典型配置指导 ● DHCP Snooping 支持 Option 82 典型配置指导 ● DHCP 客户端典型配置指导 ● 自动配置功能典型配置指导

模块	配置举例
25-ACL 典型配置指导	● 基本 IPv4 ACL 典型配置指导 ● 高级 IPv4 ACL 典型配置指导 ● 二层 ACL 典型配置指导 ● 用户自定义 ACL 和流模板典型配置指导 ● 基本 IPv6 ACL 典型配置指导 ● 高级 IPv6 ACL 典型配置指导
26-QoS 典型配置指导	● 端口限速和流量监管典型配置指导 ● 优先级重标记和队列调度典型配置指导 ● 优先级映射和队列调度典型配置指导 ● 流镜像和重定向至端口典型配置指导 ● 重定向至下一跳典型配置指导
27-端口镜像典型配置指导	● 本地端口镜像典型配置指导 ● 远程端口镜像典型配置指导（方式一） ● 远程端口镜像典型配置指导（方式二）
28-Cluster 典型配置指导	Cluster 典型配置指导
29-SNMP-RMON 典型配置指导	● SNMPv2c 监控管理交换机典型配置指导 ● SNMPv3 监控管理交换机典型配置指导 ● SNMP 操作日志输出典型配置指导 ● RMON 简介 ● RMON 典型配置指导
30-NTP 典型配置指导	● NTP 服务器/客户端模式典型配置指导 ● 配置 NTP 对等体模式 ● NTP 广播模式典型配置指导 ● NTP 组播模式典型配置指导 ● 带身份验证的 NTP 广播模式典型配置指导
31-FTP-TFTP 典型配置指导	● FTP 客户端典型配置指导 ● FTP 服务器典型配置指导 ● TFTP 客户端典型配置指导
32-UDP Helper 典型配置指导	UDP Helper 典型配置指导
33-信息中心典型配置指导	● 日志信息发送到 Unix 日志主机典型配置指导 ● 日志信息发送到 Linux 日志主机典型配置指导 ● 日志发送到控制台典型配置指导
34-域名解析典型配置指导	● 静态域名解析典型配置指导 ● 动态域名解析典型配置指导 ● DNS proxy 典型配置举例指导
35-文件系统管理典型配置指导	● 文件系统管理典型配置指导 ● 配置文件管理典型配置指导
36-在线远程升级交换机典型配置指导	● 远程升级分布式交换机典型配置指导 ● 远程升级集中式交换机典型配置指导
37-NQA 典型配置指导	NQA 配置指导

模块	配置举例
38-VRRP 典型配置指导	● 基于 IPv4 的 VRRP 单备份组举例 ● 基于 IPv4 的 VRRP 监视接口举例 ● 基于 IPv4 的 VRRP 多备份组举例 ● 基于 IPv6 的 VRRP 单备份组举例 ● 基于 IPv6 的 VRRP 监视接口举例 ● 基于 IPv6 的 VRRP 多备份组举例
39-SSH 典型配置指导	● 设备作为 SSH 服务器并采用 password 认证时的配置指导 ● 设备作为 SSH 服务器并采用 publickey 认证（认证密钥算法为 RSA）时的配置指导 ● 设备作为 SSH 客户端并采用 password 认证时的配置指导 ● 设备作为 SSH 客户端并采用 publickey 认证（认证密钥算法为 DSA）时的配置指导 ● 设备作为 SFTP 客户端典型配置指导 ● 设备作为 SFTP 服务器典型配置指导
40-端口安全典型配置指导	● 端口安全 autolearn 模式典型配置指导 ● 端口安全 userLoginWithOUI 模式典型配置指导 ● 端口安全 macAddressWithRadius 模式典型配置指导 ● 端口安全 macAddressElseUserLoginSecure 模式典型配置指导
41-端口隔离典型配置指导	● 端口隔离概述 ● 端口隔离配置指导
42-LLDP 典型配置指导	● LLDP 简介 ● LLDP 典型配置指导 ● LLDP 兼容 CDP 功能典型配置举例
43-MCE 典型配置指导	● 使用 OSPF/RIP/IS-IS 引入 VPN 路由的 MCE 典型配置指导 ● 使用 BGP 引入 VPN 路由的 MCE 典型配置指导
44-PoE 典型配置指导	● PoE 简介 ● 集中式设备 PoE 典型配置指导 ● 分布式设备 PoE 典型配置指导
45-OAM 典型配置指导	OAM 典型配置指导
46-连通错误检测典型配置指导	连通错误检测典型配置指导
47-RRPP 典型配置指导	● RRPP 单环拓扑典型配置指导（不支持保护 VLAN） ● RRPP 单域相交环拓扑典型配置指导（不支持保护 VLAN） ● RRPP 多域相交环拓扑典型配置指导（不支持保护 VLAN） ● RRPP 单环拓扑典型配置指导（支持保护 VLAN） ● RRPP 相交环拓扑典型配置指导（支持保护 VLAN） ● RRPP 相交环负载分担拓扑典型配置指导（支持保护 VLAN）
48-sFlow 典型配置指导	sFlow 典型配置指导
49-SSL-HTTPS 典型配置指导	SSL-HTTPS 典型配置指导
50-PKI 典型配置指导	● PKI 实体向 CA 申请证书典型配置指导（方式一） ● PKI 实体向 CA 申请证书典型配置指导（方式二） ● 证书属性的访问控制策略应用典型配置指导
51-Track 典型配置指导	● VRRP、Track 与 NQA 联动典型配置指导 ● 静态路由、Track 与 NQA 联动配置指导

模块	配置举例
52-EPON-OLT 典型配置指导	• OLT 典型配置指导 • ONU 远程管理典型配置指导 • UNI 端口典型配置指导
53-Smart Link 典型配置指导	• Smart Link 简介 • Smart Link 典型配置指导 • 多 Smart Link 组负载分担配置举例
54-MPLS 典型配置指导	• MPLS 基本配置指导 • MPLS L2VPN 典型配置指导 • MPLS L3VPN 典型配置指导

本书约定

1. 图形界面格式约定

格 式	意 义
< >	带尖括号 “< >” 表示按钮名，如 “单击<确定>按钮”。
[]	带方括号 “[]” 表示窗口名、菜单名和数据表，如 “弹出[新建用户]窗口”。
/	多级菜单用 “/” 隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

2. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
 说明	对操作内容的描述进行必要的补充和说明。

目 录

1 登录交换机典型配置指导	1-1
1.1 通过Console口配置Telnet登录方式典型配置指导	1-1
1.1.1 组网图	1-1
1.1.2 应用要求	1-1
1.1.3 适用产品、版本	1-1
1.1.4 配置过程和解释	1-1
1.1.5 完整配置	1-3
1.1.6 配置注意事项	1-3
1.2 通过Telnet配置Console口登录方式典型配置指导	1-4
1.2.1 组网图	1-4
1.2.2 应用要求	1-4
1.2.3 适用产品、版本	1-4
1.2.4 配置过程和解释	1-4
1.2.5 完整配置	1-5
1.2.6 配置注意事项	1-6
1.3 通过WEB网管登录交换机典型配置指导	1-7
1.3.1 组网图	1-7
1.3.2 应用要求	1-7
1.3.3 适用产品、版本	1-7
1.3.4 配置过程和解释	1-7
1.3.5 完整配置	1-8
1.3.6 配置注意事项	1-8
1.4 对登录用户的控制典型配置指导	1-8
1.4.1 组网图	1-8
1.4.2 应用要求	1-8
1.4.3 适用产品、版本	1-9
1.4.4 配置过程和解释	1-9
1.4.5 完整配置	1-9
1.4.6 配置注意事项	1-10

1 登录交换机典型配置指导

1.1 通过 Console 口配置 Telnet 登录方式典型配置指导

通过交换机 Console 口进行本地登录是登录交换机的最基本的方式，也是配置通过其他方式登录交换机的基础。

1.1.1 组网图

图1-1 通过 Console 口配置 Telnet 登录方式的组网图



1.1.2 应用要求

如上组网中，建立本地配置环境，只需将 PC 机（或终端）的串口通过配置电缆与以太网交换机的 Console 口连接。当前用户通过 Console 口（AUX 用户界面）登录到交换机对 Telnet 登录方式进行配置，且用户级别为管理级（3 级）。

1.1.3 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5500-SI 系列以太网交换机	Release 1207 软件版本	全系列硬件版本 (除 S5500-20TP-SI)
	Release 1301 软件版本	S5500-20TP-SI
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6100, Release 6300 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.1.4 配置过程和解释

- 配置 Telnet 登录方式的公共属性

进入系统视图，启动 Telnet 服务

```
<Sysname> system-view
```

```
[Sysname] telnet server enable
```

配置从 VTY 用户界面登录后可以访问的命令级别为 2 级

```
[Sysname] user-interface vty 0
[Sysname-ui-vty0] user privilege level 2
# 设置 VTY0 用户界面支持 Telnet 协议
[Sysname-ui-vty0] protocol inbound telnet
# 设置 VTY0 用户的终端屏幕的一屏显示 30 行命令
[Sysname-ui-vty0] screen-length 30
# 设置 VTY0 用户历史命令缓冲区可存放 20 条命令
[Sysname-ui-vty0] history-command max-size 20
# 设置 VTY0 用户界面的超时时间为 6 分钟
[Sysname-ui-vty0] idle-timeout 6
```

- 通过 Telnet 登录用户的认证方式

Telnet 登录有以下几种认证方式：

认证方式为 None，认证方式为 Password，认证方式为 Scheme。下面我们分别描述这几种认证方式的配置：

- (1) 设置通过 VTY0 用户界面登录交换机的 Telnet 用户不需要进行认证

```
[Sysname] user-interface vty 0
[Sysname-ui-vty0] authentication-mode none
```

- (2) 设置通过 VTY0 口登录交换机的 Telnet 用户进行 Password 认证，并设置用户的认证口令为明文方式，口令为 123456

```
[Sysname] user-interface vty 0
[Sysname-ui-vty0] authentication-mode password
[Sysname-ui-vty0] set authentication password simple 123456
```

- (3) 设置登录用户的认证方式为 Scheme，采用本地认证的方式

创建本地用户 guest，并进入本地用户视图

```
[Sysname] local-user guest
# 设置本地用户的认证口令为明文方式，口令为 123456
```

```
[Sysname-luser-guest] password simple 123456
```

设置 VTY 用户的服务类型为 Telnet 且用户级别为 2

```
[Sysname-luser-guest] service-type telnet level 2
[Sysname-luser-guest] quit
```

进入 VTY 用户界面视图

```
[Sysname] user-interface vty 0
```

设置通过 VTY0 口登录交换机的 Telnet 用户进行 Scheme 认证

```
[Sysname-ui-vty0] authentication-mode scheme
[Sysname-ui-vty0] quit
```

指定 system 域为缺省域，并设置该域 Scheme 认证方式 local

```
[Sysname] domain default enable system
[Sysname] domain system
[Sysname-isp-system] authentication default local
```

1.1.5 完整配置

- 认证方式为 None 时 Telnet 登录方式的配置

```
#
telnet server enable
#
user-interface vty 0
 authentication-mode none
 user privilege level 2
 history-command max-size 20
 idle-timeout 6 0
 screen-length 30
 protocol inbound telnet
```

- 认证方式为 Password 时 Telnet 登录方式的配置

```
#
telnet server enable
#
user-interface vty 0
 authentication-mode password
 user privilege level 2
 set authentication password simple 123456
 history-command max-size 20
 idle-timeout 6 0
 screen-length 30
 protocol inbound telnet
```

- 认证方式为 Scheme 时 Telnet 登录方式的配置

```
#
domain system
 authentication default local
#
telnet server enable
#
local-user guest
 service-type telnet
 level 2
 password simple 123456
#
user-interface vty 0
 authentication-mode scheme
 user privilege level 2
 history-command max-size 20
 idle-timeout 6 0
 screen-length 30
 protocol inbound telnet
```

1.1.6 配置注意事项

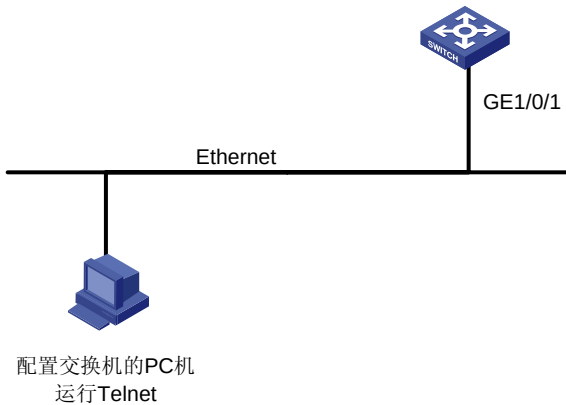
无

1.2 通过 Telnet 配置 Console 口登录方式典型配置指导

交换机支持 Telnet 功能，用户可以通过 Telnet 方式对交换机进行远程管理和维护。

1.2.1 组网图

图1-2 通过 Telnet 配置 Console 口登录方式的组网图



1.2.2 应用要求

如上组网中，当前用户通过 Telnet 方式登录到交换机对 Console 口登录方式进行配置，且用户级别为管理级（3 级）。

1.2.3 适用产品、版本

表1-2 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5500-SI 系列以太网交换机	Release 1207 软件版本	全系列硬件版本 (除 S5500-20TP-SI)
	Release 1301 软件版本	S5500-20TP-SI
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6100, Release 6300 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.2.4 配置过程和解释

- 配置 Console 口登录方式的公共属性

配置从 AUX 用户界面登录后可以访问的命令级别为 2 级。

```
[Sysname] user-interface aux 0
```

```
[Sysname-ui-aux0] user privilege level 2
```

配置 Console 口使用的波特率为 19200bit/s

```
[Sysname-ui-aux0] speed 19200
```

配置终端屏幕的一屏显示 30 行命令

```
[Sysname-ui-aux0] screen-length 30
```

配置历史命令缓冲区可存放 20 条命令

```
[Sysname-ui-aux0] history-command max-size 20
```

配置 AUX 用户界面的超时时间为 6 分钟

```
[Sysname-ui-aux0] idle-timeout 6
```

- 配置 Console 口登录用户的认证方式

Console 口登录有以下几种认证方式：

认证方式为 None，认证方式为 Password，认证方式为 Scheme。下面我们分别描述这几种认证方式的配置：

- (1) 设置登录用户的认证方式为 None

```
[Sysname] user-interface aux 0
```

```
[Sysname-ui-aux0] authentication-mode none
```

- (2) 设置登录用户的认证方式为 Password，并设置用户的认证口令为明文方式，口令为 123456

```
[Sysname] user-interface aux 0
```

```
[Sysname-ui-aux0] authentication-mode password
```

```
[Sysname-ui-aux0] set authentication password simple 123456
```

- (3) 设置登录用户的认证方式为 Scheme，采用本地认证的方式

创建本地用户 guest，并进入本地用户视图

```
[Sysname] local-user guest
```

设置本地用户的认证口令为明文方式，口令为 123456

```
[Sysname-luser-guest] password simple 123456
```

设置本地用户的服务类型为 Terminal 且用户级别为 2

```
[Sysname-luser-guest] service-type terminal level 2
```

```
[Sysname-luser-guest] quit
```

进入 AUX 用户界面视图

```
[Sysname] user-interface aux 0
```

设置通过 Console 口登录交换机的用户进行 Scheme 认证

```
[Sysname-ui-aux0] authentication-mode scheme
```

指定 system 域为缺省域，并设置该域 Scheme 认证方式 local

```
[Sysname] domain default enable system
```

```
[Sysname] domain system
```

```
[Sysname-isp-system] authentication default local
```

1.2.5 完整配置

- 认证方式为 None 时 Console 口登录方式的配置

```
#
```

```
user-interface aux 0
```

```
authentication-mode none
```

```
user privilege level 2
history-command max-size 20
idle-timeout 6 0
speed 19200
screen-length 30
```

- 认证方式为 Password 时 Console 口登录方式的配置

```
#
user-interface aux 0
authentication-mode password
user privilege level 2
set authentication password simple 123456
history-command max-size 20
idle-timeout 6 0
speed 19200
screen-length 30
```

- 认证方式为 Scheme 时 Console 口登录方式的配置

```
#
domain system
authentication default local
#
local-user guest
password simple 123456
service-type terminal
level 2
#
user-interface aux 0
authentication-mode scheme
user privilege level 2
history-command max-size 20
idle-timeout 6 0
speed 19200
screen-length 30
```

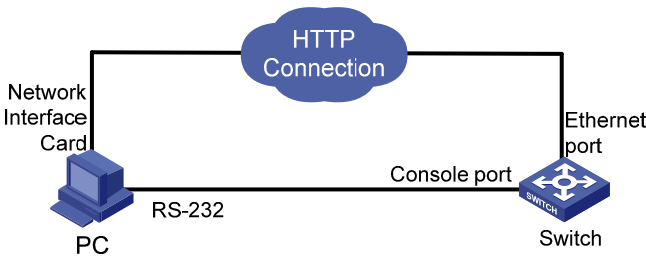
1.2.6 配置注意事项

无

1.3 通过 WEB 网管登录交换机典型配置指导

1.3.1 组网图

图1-3 通过 WEB 网管登录交换机示意图



1.3.2 应用要求

如上组网图所示，PC 通过 WEB 网管登录交换机，实现对交换机的远程管理。

1.3.3 适用产品、版本

表1-3 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5500-SI 系列以太网交换机	Release 1207 软件版本	全系列硬件版本 (除 S5500-20TP-SI)
	Release 1301 软件版本	S5500-20TP-SI
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.3.4 配置过程和解释

通过 Console 口正确配置以太网交换机 VLAN 1 接口的 IP 地址（VLAN 1 为交换机的缺省 VLAN）为 10.153.17.82，子网掩码为 255.255.255.0。

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-VLAN-interface1] ip address 10.153.17.82 255.255.255.0
[Sysname-VLAN-interface1] quit
```

配置 WEB 网管用户名为 admin，认证口令为 admin，用户级别为 3 级。

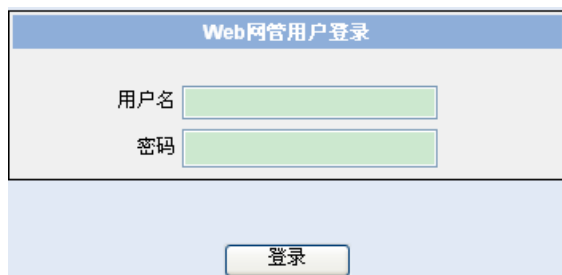
```
[Sysname] local-user admin
[Sysname-luser-admin] service-type telnet level 3
[Sysname-luser-admin] password simple admin
[Sysname-luser-admin] quit
```

开启交换机的 WEB Server 功能。

```
[Sysname] ip http enable
```

通过浏览器登录交换机：在WEB网管终端(PC)的浏览器地址栏内输入http://10.153.17.82（WEB网管终端和以太网交换机之间要路由可达），浏览器会显示WEB网管的登录页面，如图 1-4所示。

图1-4 WEB网管登录页面



Web网管用户登录

用户名

密码

登录

输入在交换机上添加的用户名和密码，点击<登录>按钮后即可登录，显示WEB网管初始页面。

1.3.5 完整配置

```
#
local-user admin
password simple admin
service-type telnet
level 3
#
interface Vlan-interface1
ip address 10.153.17.82 255.255.255.0
```

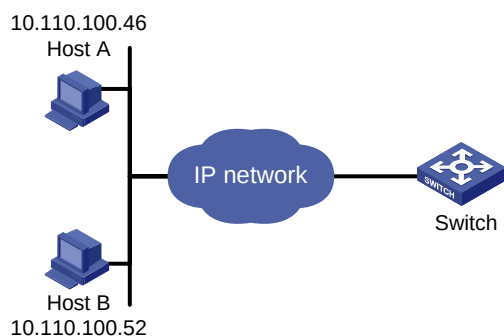
1.3.6 配置注意事项

缺省情况下，WEB网管功能处于开启状态。

1.4 对登录用户的控制典型配置指导

1.4.1 组网图

图1-5 对登录用户的控制典型配置示意图



1.4.2 应用要求

如上组网中，仅允许来自 10.110.100.52 和 10.110.100.46 的 Telnet/SNMP/WEB 用户访问交换机。

1.4.3 适用产品、版本

表1-4 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5500-SI 系列以太网交换机	Release 1207 软件版本	全系列硬件版本 (除 S5500-20TP-SI)
	Release 1301 软件版本	S5500-20TP-SI
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6100, Release 6300 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.4.4 配置过程和解释

创建并进入基本 ACL 视图 2000

```
[Sysname] acl number 2000 match-order config
```

```
[Sysname-acl-basic-2000]
```

定义子规则，仅允许来自 10.110.100.52 和 10.110.100.46 的 Telnet/SNMP/WEB 用户访问交换机

```
[Sysname-acl-basic-2000] rule 1 permit source 10.110.100.52 0
```

```
[Sysname-acl-basic-2000] rule 2 permit source 10.110.100.46 0
```

```
[Sysname-acl-basic-2000] rule 3 deny source any
```

```
[Sysname-acl-basic-2000] quit
```

引用访问控制列表 2000，通过源 IP 对 Telnet 用户进行控制

```
[Sysname] user-interface vty 0 4
```

```
[Sysname-ui-vty0-4] acl 2000 inbound
```

引用访问控制列表 2000，通过源 IP 对网管用户进行控制

```
[Sysname] snmp-agent community read aaa acl 2000
```

```
[Sysname] snmp-agent group v2c groupa acl 2000
```

```
[Sysname] snmp-agent usm-user v2c usera groupa acl 2000
```

引用访问控制列表 2000，通过源 IP 对 WEB 用户进行控制

```
[Sysname] ip http acl 2000
```

1.4.5 完整配置

- 对 Telnet 用户进行控制

```
#
```

```
acl number 2000
```

```
rule 1 permit source 10.110.100.52 0
```

```
rule 2 permit source 10.110.100.46 0
```

```
rule 3 deny
```

```
#
user-interface vty 0 4
acl 2000 inbound
• 通过源 IP 对网管用户进行控制
#
acl number 2000
rule 1 permit source 10.110.100.52 0
rule 2 permit source 10.110.100.46 0
rule 3 deny
#
snmp-agent community read aaa acl 2000
snmp-agent group v2c groupa acl 2000
snmp-agent usm-user v2c usera groupa acl 2000
• 通过源 IP 对 WEB 用户进行控制
#
ip http acl 2000
#
acl number 2000
rule 1 permit source 10.110.100.52 0
rule 2 permit source 10.110.100.46 0
rule 3 deny
```

1.4.6 配置注意事项

S7500E 系列以太网交换机不支持 WEB 用户登录，因此对 WEB 用户的控制，不适用于 S7500E 系列以太网交换机。

目 录

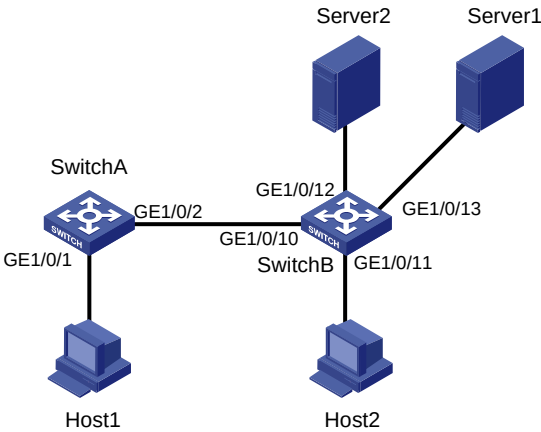
1 VLAN典型配置指导	1-1
1.1 基于端口的VLAN典型配置指导	1-1
1.1.1 组网图	1-1
1.1.2 应用要求	1-1
1.1.3 适用产品、版本	1-1
1.1.4 配置过程和解释	1-2
1.1.5 完整配置	1-3
1.1.6 配置注意事项	1-3
1.2 基于MAC的VLAN典型配置指导	1-4
1.2.1 组网图	1-4
1.2.2 应用要求	1-4
1.2.3 适用产品、版本	1-4
1.2.4 配置过程和解释	1-4
1.2.5 完整配置	1-6
1.2.6 配置注意事项	1-6
1.3 基于协议的VLAN典型配置指导	1-7
1.3.1 组网图	1-7
1.3.2 应用要求	1-7
1.3.3 适用产品、版本	1-7
1.3.4 配置过程和解释	1-7
1.3.5 完整配置	1-8
1.3.6 配置注意事项	1-9
1.4 基于IP子网的VLAN典型配置指导	1-9
1.4.1 组网图	1-9
1.4.2 应用要求	1-9
1.4.3 适用产品、版本	1-10
1.4.4 配置过程和解释	1-10
1.4.5 完整配置	1-10
1.4.6 配置注意事项	1-11
1.5 Isolate-user-vlan典型配置指导	1-11
1.5.1 组网图	1-11
1.5.2 应用要求	1-11
1.5.3 适用产品、版本	1-12
1.5.4 配置过程和解释	1-12
1.5.5 完整配置	1-13
1.5.6 配置注意事项	1-14
1.6 Super VLAN典型配置指导	1-15
1.6.1 组网图	1-15
1.6.2 应用要求	1-15
1.6.3 使用产品、版本	1-15
1.6.4 配置过程和解释	1-15
1.6.5 完整配置	1-17
1.6.6 配置注意事项	1-18

1 VLAN 典型配置指导

1.1 基于端口的 VLAN 典型配置指导

1.1.1 组网图

图1-1 基于端口的 VLAN 组网示意图



1.1.2 应用要求

- 如图 1-1 所示，Switch A 和 Switch B 分别连接了不同部门使用的 Host1/Host2 和 Server1/Server2。
- 为保证部门间数据的二层隔离，现要求将 Host1 和 Server1 划分到 VLAN100 中，Host2 和 Server2 划分到 VLAN200 中。并分别为两个 VLAN 设置描述字符为“Dept1”和“Dept2”。
- 在 SwitchA 上配置 VLAN 接口，对 Host1 发往 Server2 的数据进行三层转发。

1.1.3 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5500-SI 系列以太网交换机	Release 1207 软件版本	全系列硬件版本 (除 S5500-20TP-SI)
	Release 1301 软件版本	S5500-20TP-SI
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6100, Release 6300 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.1.4 配置过程和解释

- 配置 Switch A

创建 VLAN100，并配置 VLAN100 的描述字符串为“Dept1”，将端口 GigabitEthernet1/0/1 加入到 VLAN100。

```
<SwitchA> system-view
[SwitchA] vlan 100
[SwitchA-vlan100] description Dept1
[SwitchA-vlan100] port GigabitEthernet 1/0/1
[SwitchA-vlan100] quit
```

创建 VLAN200，并配置 VLAN200 的描述字符串为“Dept2”。

```
[SwitchA] vlan 200
[SwitchA-vlan200] description Dept2
[SwitchA-vlan200] quit
```

创建 VLAN100 和 VLAN200 的接口，IP 地址分别配置为 192.168.1.1 和 192.168.2.1，用来对 Host1 发往 Server2 的报文进行三层转发。

```
[SwitchA] interface Vlan-interface 100
[SwitchA-Vlan-interface100] ip address 192.168.1.1 24
[SwitchA-Vlan-interface100] quit
[SwitchA] interface Vlan-interface 200
[SwitchA-Vlan-interface200] ip address 192.168.2.1 24
```

- 配置 Switch B

创建 VLAN100，并配置 VLAN100 的描述字符串为“Dept1”，将端口 GigabitEthernet1/0/13 加入到 VLAN100。

```
<SwitchB> system-view
[SwitchB] vlan 100
[SwitchB-vlan100] description Dept1
[SwitchB-vlan100] port GigabitEthernet 1/0/13
[SwitchB-vlan100] quit
```

创建 VLAN200，并配置 VLAN200 的描述字符串为“Dept2”，将端口 GigabitEthernet1/0/11 和 GigabitEthernet1/0/12 加入到 VLAN200。

```
[SwitchB] vlan 200
[SwitchB-vlan200] description Dept2
[SwitchB-vlan200] port GigabitEthernet1/0/11 GigabitEthernet 1/0/12
[SwitchB-vlan200] quit
```

- 配置 Switch A 和 Switch B 之间的链路

由于 Switch A 和 Switch B 之间的链路需要同时传输 VLAN100 和 VLAN200 的数据，所以可以配置两端的端口为 Trunk 端口，且允许这两个 VLAN 的报文通过。

配置 Switch A 的 GigabitEthernet1/0/2 端口。

```
[SwitchA] interface GigabitEthernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-type trunk
[SwitchA-GigabitEthernet1/0/2] port trunk permit vlan 100 200
```

配置 Switch B 的 GigabitEthernet1/0/10 端口。

```
[SwitchB] interface GigabitEthernet 1/0/10
[SwitchB-GigabitEthernet1/0/10] port link-type trunk
[SwitchB-GigabitEthernet1/0/10] port trunk permit vlan 100 200
```

1.1.5 完整配置

- SwitchA 上的配置

```
#
vlan 100
description dept1
#
vlan 200
description dept2
#
interface Vlan-interface 100
ip address 192.168.1.1 255.255.255.0
#
interface Vlan-interface 200
ip address 192.168.2.1 255.255.255.0
#
interface GigabitEthernet1/0/1
port access vlan 100
#
interface GigabitEthernet1/0/2
port link-type trunk
port trunk permit vlan 1 100 200
```

- SwitchB 上的配置

```
#
vlan 100
description dept1
#
vlan 200
description dept2
#
interface GigabitEthernet1/0/10
port link-type trunk
port trunk permit vlan 1 100 200
#
interface GigabitEthernet1/0/11
port access vlan 200
#
interface GigabitEthernet1/0/12
port access vlan 200
#
interface GigabitEthernet1/0/13
port access vlan 100
```

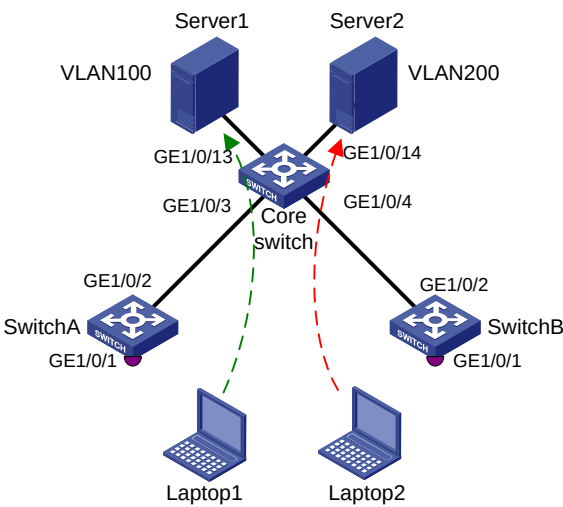
1.1.6 配置注意事项

无

1.2 基于 MAC 的 VLAN 典型配置指导

1.2.1 组网图

图1-2 基于 MAC 的 VLAN 组网示意图



1.2.2 应用要求

- 如 图 1-2所示，SwitchA和SwitchB的GigabitEthernet1/0/1 端口分别连接到两个会议室，Laptop1 和Laptop2 是会议用笔记本电脑，会在两个会议室间移动使用。
- Laptop1 和 Laptop2 分别属于两个部门，两个部门间使用 VLAN100 和 VLAN200 进行隔离。现要求这两台笔记本电脑无论在哪个会议室使用，均只能访问自己部门的服务器，即 Server1 和 Server2。
- Laptop1 和 Laptop2 的 MAC 地址分别为 000d-88f8-4e71、0014-222c-aa69。

1.2.3 适用产品、版本

表1-2 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S5500-SI 系列以太网交换机	Release 1207 软件版本	全系列硬件版本 (除 S5500-20TP-SI)
	Release 1301 软件版本	S5500-20TP-SI
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6100, Release 6300 软件版本	全系列硬件版本

1.2.4 配置过程和解释

- SwitchA 的配置
创建 VLAN100 和 VLAN200，并将 GigabitEthernet1/0/2 配置为 Trunk 端口，允许 VLAN100 和 VLAN200 的报文通过。

```
<SwitchA> system-view
```

```
[SwitchA] vlan 100
[SwitchA-vlan100] quit
[SwitchA] vlan 200
[SwitchA-vlan200] quit
[SwitchA] interface GigabitEthernet1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-type trunk
[SwitchA-GigabitEthernet1/0/2] port trunk permit vlan 100 200
[SwitchA-GigabitEthernet1/0/2] quit
```

将 GigabitEthernet1/0/1 配置为 Hybrid 端口, 并使其在发送 VLAN100 和 VLAN200 的报文时去掉 VLAN Tag。

```
[SwitchA] interface GigabitEthernet1/0/1
[SwitchA-GigabitEthernet1/0/1] port link-type hybrid
[SwitchA-GigabitEthernet1/0/1] port hybrid vlan 100 200 untagged
[SwitchA-GigabitEthernet1/0/1] quit
```

创建 Laptop1 的 MAC 地址与 VLAN100 的关联, 创建 Laptop2 的 MAC 地址与 VLAN200 的关联, 开启 GigabitEthernet1/0/1 端口的 MAC-VLAN 功能。

```
[SwitchA] mac-vlan mac-address 000d-88f8-4e71 vlan 100
[SwitchA] mac-vlan mac-address 0014-222c-aa69 vlan 200
[SwitchA] interface GigabitEthernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] mac-vlan enable
```

- SwitchB 的配置

SwitchB 的配置与 SwitchA 完全一致, 这里不再赘述。

- Core Switch 的配置

创建 VLAN100 和 VLAN200, 并将 GigabitEthernet1/0/13 和 GigabitEthernet 1/0/14 端口分别加入这两个 VLAN。

```
<CoreSwitch> system-view
[CoreSwitch] vlan 100
[CoreSwitch-vlan100] port gigabitethernet 1/0/13
[CoreSwitch-vlan100] quit
[CoreSwitch] vlan 200
[CoreSwitch-vlan200] port gigabitethernet 1/0/14
[CoreSwitch-vlan200] quit
```

配置 GigabitEthernet1/0/3 和 GigabitEthernet1/0/4 端口为 Trunk 端口, 均允许 VLAN100 和 VLAN200 的报文通过。

```
[CoreSwitch] interface GigabitEthernet1/0/3
[CoreSwitch-GigabitEthernet1/0/3] port link-type trunk
[CoreSwitch-GigabitEthernet1/0/3] port trunk permit vlan 100 200
[CoreSwitch-GigabitEthernet1/0/3] quit
[CoreSwitch] interface GigabitEthernet1/0/4
[CoreSwitch-GigabitEthernet1/0/4] port link-type trunk
[CoreSwitch-GigabitEthernet1/0/4] port trunk permit vlan 100 200
[CoreSwitch-GigabitEthernet1/0/4] quit
```

1.2.5 完整配置

- SwitchA 的配置

```
#
mac-vlan mac-address 000d-88f8-4e71 vlan 100 priority 0
mac-vlan mac-address 0014-222c-aa69 vlan 200 priority 0
#
vlan 100
#
vlan 200
#
#
interface GigabitEthernet1/0/1
port link-type hybrid
port hybrid vlan 1 100 200 untagged
mac-vlan enable
#
interface GigabitEthernet1/0/2
port link-type trunk
port trunk permit vlan 1 100 200
```

SwitchB 的配置与 SwitchA 完全一致，这里不再赘述。

- Core Switch 的配置

```
#
vlan 100
#
vlan 200
#
interface GigabitEthernet1/0/3
port link-type trunk
port trunk permit vlan 1 100 200
#
interface GigabitEthernet1/0/4
port link-type trunk
port trunk permit vlan 1 100 200
#
interface GigabitEthernet1/0/13
port access vlan 100
#
interface GigabitEthernet1/0/14
port access vlan 200
```

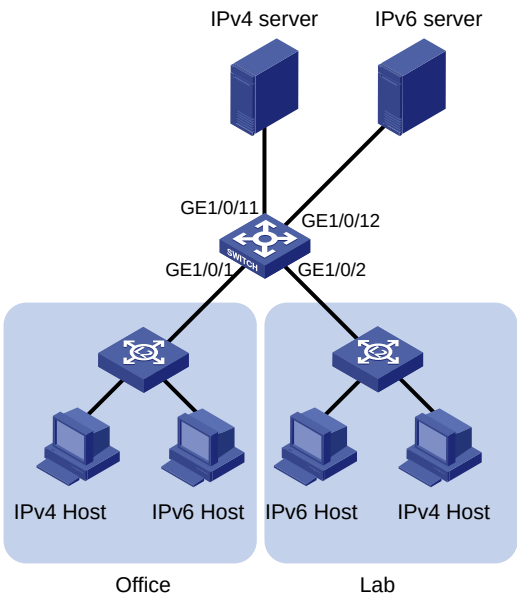
1.2.6 配置注意事项

基于 MAC 的 VLAN 只能在 Hybrid 端口上配置。

1.3 基于协议的 VLAN 典型配置指导

1.3.1 组网图

图1-3 基于协议的 VLAN 组网示意图



1.3.2 应用要求

如图 1-3所示，通过配置交换机的协议VLAN功能，使办公区和实验室中基于IPv4 网络和基于IPv6 网络的主机能分别与处在不同VLAN内的对应服务器进行通信，且两种网络协议的报文能够通过 VLAN进行隔离，其中IPv4 网络使用VLAN100，IPv6 网络使用VLAN200。

1.3.3 适用产品、版本

表1-3 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6100, Release 6300 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.3.4 配置过程和解释

- 上行端口的配置

创建 VLAN100，将端口 GigabitEthernet1/0/11 加入 VLAN100

```
<Sysname> system-view
```

```
[Sysname] vlan 100
```



```
[Sysname-vlan100] port GigabitEthernet 1/0/11
```

创建 VLAN200, 将端口 GigabitEthernet1/0/12 加入 VLAN200

```
[Sysname-vlan100] quit
```

```
[Sysname] vlan 200
```

```
[Sysname-vlan200] port GigabitEthernet 1/0/12
```

- 配置协议模板并与下行端口绑定

创建 VLAN200 和 VLAN100 的协议模板, 分别匹配 IPv4 和 IPv6 协议。

```
[Sysname-vlan200] protocol-vlan ipv6
```

```
[Sysname-vlan200] quit
```

```
[Sysname] vlan100
```

```
[Sysname-vlan100] protocol-vlan ipv4
```

```
[Sysname-vlan100] quit
```

配置端口 GigabitEthernet1/0/1 为 Hybrid 端口, 并在转发 VLAN100 和 VLAN200 的报文时去掉 VLAN Tag。

```
[Sysname] interface GigabitEthernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] port link-type hybrid
```

```
[Sysname-GigabitEthernet1/0/1] port hybrid vlan 100 200 untagged
```

配置端口 GigabitEthernet1/0/1 分别与 VLAN100 的协议模板 0, VLAN200 的协议模板 0 进行绑定。

```
[Sysname-GigabitEthernet1/0/1] port hybrid protocol-vlan vlan 100 0
```

```
[Sysname-GigabitEthernet1/0/1] port hybrid protocol-vlan vlan 200 0
```

同理配置端口 GigabitEthernet1/0/2 为 Hybrid 端口, 在转发 VLAN100 和 VLAN200 的报文时去掉 VLAN Tag, 并与 VLAN100 和 VLAN200 的协议模板 0 进行绑定

```
[Sysname] interface GigabitEthernet 1/0/2
```

```
[Sysname-GigabitEthernet1/0/2] port link-type hybrid
```

```
[Sysname-GigabitEthernet1/0/2] port hybrid vlan 100 200 untagged
```

```
[Sysname-GigabitEthernet1/0/2] port hybrid protocol-vlan vlan 100 0
```

```
[Sysname-GigabitEthernet1/0/2] port hybrid protocol-vlan vlan 200 0
```

1.3.5 完整配置

```
#
```

```
vlan 100
```

```
protocol-vlan 0 ipv4
```

```
#
```

```
vlan 200
```

```
protocol-vlan 0 ipv6
```

```
#
```

```
interface GigabitEthernet1/0/1
```

```
port link-type hybrid
```

```
port hybrid vlan 1 100 200 untagged
```

```
port hybrid protocol-vlan vlan 100 0
```

```
port hybrid protocol-vlan vlan 200 0
```

```
#
```

```
interface GigabitEthernet1/0/2
```

```
port link-type hybrid
```

```

port hybrid vlan 1 100 200 untagged
port hybrid protocol-vlan vlan 100 0
port hybrid protocol-vlan vlan 200 0
#
interface Ethernet1/0/11
port access vlan 100
#
interface Ethernet1/0/12
port access vlan 200

```

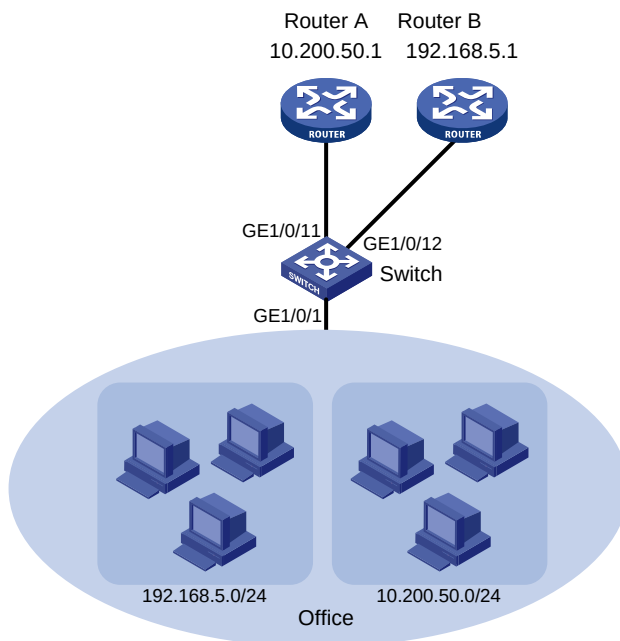
1.3.6 配置注意事项

无

1.4 基于 IP 子网的 VLAN 典型配置指导

1.4.1 组网图

图1-4 基于 IP 子网的 VLAN 组网示意图



1.4.2 应用要求

如图 1-4所示，办公区内的主机被配置到两个不同的网段（192.168.5.0/24 和 10.200.50.0/24）中，要求通过配置IP子网VLAN功能，使交换机能够将GigabitEthernet1/0/1 端口收到的报文根据源主机所属网段的不同，分别在不同的VLAN内传输，并到达指定的网关（RouterA和RouterB）。

其中 192.168.5.0/24 网段的报文分发到 VLAN100 中传输，10.200.50.0/24 网段的报文分发到 VLAN200 中传输。

1.4.3 适用产品、版本

表1-4 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6100, Release 6300 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.4.4 配置过程和解释

- 上行端口的配置

创建 VLAN100, 将端口 GigabitEthernet1/0/12 加入 VLAN100

```
[Sysname] vlan 100
```

```
[Sysname-vlan100] port GigabitEthernet 1/0/12
```

创建 VLAN200, 将端口 GigabitEthernet1/0/11 加入 VLAN200

```
[Sysname-vlan100] quit
```

```
[Sysname] vlan 200
```

```
[Sysname-vlan200] port GigabitEthernet 1/0/11
```

- 配置 IP 子网 VLAN 并与下行端口绑定

将 10.200.50.0/24 网段与 VLAN200 进行关联, 将 192.168.5.0/24 网段与 VLAN100 进行关联

```
[Sysname-vlan200] ip-subnet-vlan ip 10.200.50.0 255.255.255.0
```

```
[Sysname-vlan200] quit
```

```
[Sysname] vlan100
```

```
[Sysname-vlan100] ip-subnet-vlan ip 192.168.5.0 255.255.255.0
```

配置端口 GigabitEthernet1/0/1 为 Hybrid 端口, 并在转发 VLAN100 和 VLAN200 的报文时去掉 VLAN Tag。

```
[Sysname] interface GigabitEthernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] port link-type hybrid
```

```
[Sysname-GigabitEthernet1/0/1] port hybrid vlan 100 200 untagged
```

配置端口 GigabitEthernet1/0/1 分别与 VLAN100 和 VLAN200 的子网进行关联。

```
[Sysname-GigabitEthernet1/0/1] port hybrid ip-subnet-vlan vlan 100
```

```
[Sysname-GigabitEthernet1/0/1] port hybrid ip-subnet-vlan vlan 200
```

1.4.5 完整配置

```
#
vlan 100
ip-subnet-vlan 0 ip 192.168.5.0 255.255.255.0
#
vlan 200
```

```

ip-subnet-vlan 0 ip 10.200.50.0 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-type hybrid
port hybrid vlan 1 100 200 untagged
port hybrid ip-subnet-vlan vlan 100
port hybrid ip-subnet-vlan vlan 200
#
interface Ethernet1/0/11
port access vlan 200
#
interface Ethernet1/0/12
port access vlan 100

```

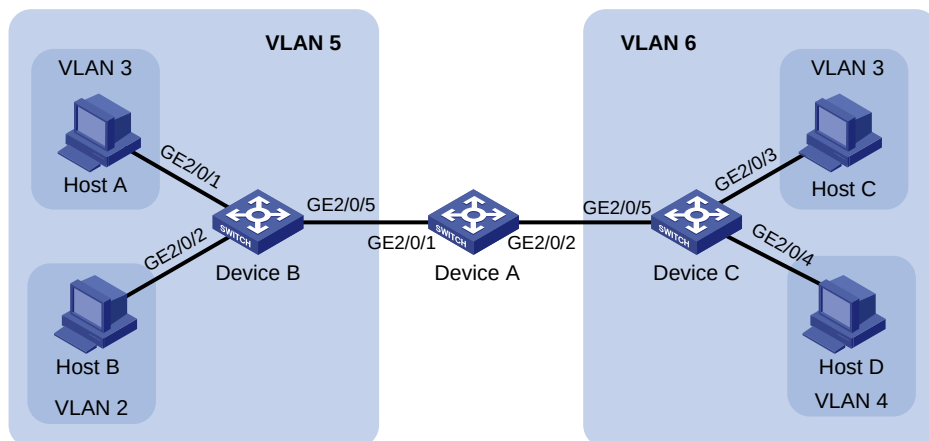
1.4.6 配置注意事项

无

1.5 Isolate-user-vlan 典型配置指导

1.5.1 组网图

图1-5 Isolate-user-vlan 组网示意图



1.5.2 应用要求

- DeviceB 和 DeviceC 在初始状态下分别位于两个独立的网络中，并根据自身情况创建了相应的 VLAN；由于网络规划的变更，现要求使用 DeviceA 将 DeviceB 和 DeviceC 连通。
- 出于安全性的考虑，要求DeviceB和DeviceC所连接的设备间不能直接通信，如 图 1-5所示，由于这两台设备本地创建的VLAN编号有重复，HostA和HostC处在同一个VLAN中，存在一定安全隐患。因此需要使用 Isolate-user-vlan 功能，使 DeviceB 和 DeviceC 上配置的 VLAN2/VLAN3 和VLAN3/VLAN4 仅在本地产有效，DeviceA使用VLAN5 和VLAN6 对这两个网络进行划分，而无需考虑这两个网络内部VLAN的配置。
- DeviceA 使用 VLAN 接口对两个网络间的报文进行三层转发。

1.5.3 适用产品、版本

表1-5 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S7500E 系列以太网交换机	Release 6100, Release 6300 软件版本	全系列硬件版本

1.5.4 配置过程和解释

- 配置 DeviceB

配置 Isolate-user-vlan。

```
<DeviceB> system-view
[DeviceB] vlan 5
[DeviceB-vlan5] isolate-user-vlan enable
[DeviceB-vlan5] port GigabitEthernet 2/0/5
[DeviceB-vlan5] quit
```

配置 Secondary VLAN。

```
[DeviceB] vlan 3
[DeviceB-vlan3] port GigabitEthernet 2/0/1
[DeviceB-vlan3] quit
[DeviceB] vlan 2
[DeviceB-vlan2] port GigabitEthernet 2/0/2
[DeviceB-vlan2] quit
```

配置 Isolate-user-vlan 和 Secondary VLAN 间的映射关系。

```
[DeviceB] isolate-user-vlan 5 secondary 2 to 3
```

- 配置 DeviceC

配置 Isolate-user-vlan。

```
<DeviceC> system-view
[DeviceC] vlan 6
[DeviceC-vlan6] isolate-user-vlan enable
[DeviceC-vlan6] port GigabitEthernet 2/0/5
[DeviceC-vlan6] quit
```

配置 Secondary VLAN。

```
[DeviceC] vlan 3
[DeviceC-vlan3] port GigabitEthernet 2/0/3
[DeviceC-vlan3] quit
[DeviceC] vlan 4
[DeviceC-vlan4] port GigabitEthernet 2/0/4
```

配置 Isolate-user-vlan 和 Secondary VLAN 间的映射关系。

```
[DeviceC-vlan4] quit
[DeviceC] isolate-user-vlan 6 secondary 3 to 4
```

- 配置 DeviceA

创建 VLAN5 和 VLAN6, 并将 GigabitEthernet2/0/1 和 GigabitEthernet2/0/2 端口分别加入 VLAN5 和 VLAN6, 本例中以这两个端口为 Access 端口为例进行配置。

```
[DeviceA] vlan 5
[DeviceA-vlan5] port GigabitEthernet 2/0/1
[DeviceA-vlan5] quit
[DeviceA] vlan 6
[DeviceA-vlan6] port GigabitEthernet 2/0/2
[DeviceA-vlan6] quit
```

创建 VLAN5 和 VLAN6 的接口, 使两个网络间的数据可以通过 Device A 进行三层转发, IP 地址分别为 192.168.0.1 和 192.168.1.1。

```
[DeviceA] interface Vlan-interface 5
[DeviceA-Vlan-interface5] ip address 192.168.0.1 24
[DeviceA-Vlan-interface5] quit
[DeviceA] interface Vlan-interface 6
[DeviceA-Vlan-interface6] ip address 192.168.1.1 24
```

用户也可以将 GigabitEthernet2/0/1 和 GigabitEthernet2/0/2 端口配置为 Trunk 端口或 Hybrid 端口, 只需要保证这两个端口分别在发送 VLAN5 和 VLAN6 的报文时去掉 VLAN Tag 即可。

1.5.5 完整配置

- DeviceB 的完整配置

```
#
vlan 2 to 3
#
vlan 5
  isolate-user-vlan enable
#
interface GigabitEthernet2/0/1
  port link-type hybrid
  undo port hybrid vlan 1
  port hybrid vlan 3 5 untagged
  port hybrid pvid vlan 3
#
interface GigabitEthernet2/0/2
  port link-type hybrid
  undo port hybrid vlan 1
  port hybrid vlan 2 5 untagged
  port hybrid pvid vlan 2
#
interface GigabitEthernet2/0/5
  port link-type hybrid
  undo port hybrid vlan 1
  port hybrid vlan 2 3 5 untagged
  port hybrid pvid vlan 5
#
isolate-user-vlan 5 secondary 2 3
```

- DeviceC 的完整配置

```
#
vlan 3 to 4
#
vlan 6
isolate-user-vlan enable
#
interface GigabitEthernet2/0/3
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 3 6 untagged
port hybrid pvid vlan 3

#
interface GigabitEthernet2/0/4
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 4 6 untagged
port hybrid pvid vlan 4

#
interface GigabitEthernet2/0/5
port link-type hybrid
undo port hybrid vlan 1
port hybrid vlan 3 4 6 untagged
port hybrid pvid vlan 6
#
isolate-user-vlan 50 secondary 2 3
```

- DeviceA 的完整配置

```
#
vlan 5 to 6
#
interface Vlan-interface 5
ip address 192.168.0.1 255.255.255.0
#
interface Vlan-interface 6
ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet2/0/1
port access vlan 5
#
interface GigabitEthernet2/0/2
port access vlan 6
```

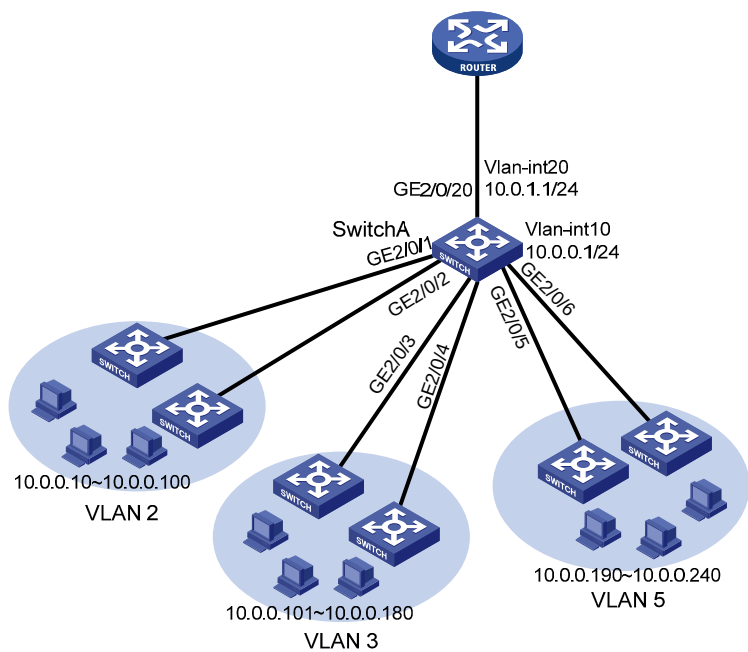
1.5.6 配置注意事项

无

1.6 Super VLAN 典型配置指导

1.6.1 组网图

图1-6 Super VLAN 组网示意图



1.6.2 应用要求

- SwitchA作为汇聚层交换机，下面通过接入层交换机连接了大量的客户端，这些客户端都使用了 10.0.0.0/24 网段的地址。现要求按 图 1-6所示，将主机划分到三个VLAN中进行管理，保证不同VLAN内的主机之间二层隔离。
- 为节约 IP 地址，不对三个 VLAN 分别划分子网，要求使用 SwitchA 的 Vlan-interface10 接口作为所有主机的网关，转发主机对外网的访问需求，同时通过 ARP 代理实现 VLAN 间主机的三层互通。
- SwitchA 通过 Vlan-interface20 接口连接到外部网络。

1.6.3 使用产品、版本

表1-6 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S7500E 系列以太网交换机	Release 6300 软件版本	全系列硬件版本

1.6.4 配置过程 and 解释

创建 VLAN20，将 GigabitEthernet 2/0/20 加入 VLAN20，并配置 Vlan-interface20 接口的地址为 10.0.1.1/24。

```
<Sysname> system-view
[Sysname] vlan 20
[Sysname-vlan20] port gigabitethernet 2/0/20
[Sysname-vlan20] quit
```



```
[Sysname] interface vlan-interface 20
```

```
[Sysname-Vlan-interface20] ip address 10.0.1.1 255.255.255.0
```

创建 VLAN10，并配置 VLAN10 接口的 IP 地址为 10.0.0.1/24。

```
<Sysname> system-view
```

```
[Sysname] vlan 10
```

```
[Sysname-vlan10] quit
```

```
[Sysname] interface vlan-interface 10
```

```
[Sysname-Vlan-interface10] ip address 10.0.0.1 255.255.255.0
```

开启 VLAN10 接口的本地 ARP 代理功能，使 VLAN2、3、5 之间能够通过 VLAN10 接口的处理完成 ARP 请求和答复过程。

```
[Sysname-Vlan-interface10] local-proxy-arp enable
```

```
[Sysname-Vlan-interface10] quit
```

创建 VLAN2，并添加端口 GigabitEthernet2/0/1 和端口 GigabitEthernet2/0/2。

```
[Sysname] vlan 2
```

```
[Sysname-vlan2] port GigabitEthernet 2/0/1 GigabitEthernet 2/0/2
```

创建 VLAN3，并添加端口 GigabitEthernet2/0/3 和端口 GigabitEthernet2/0/4。

```
[Sysname-vlan2] quit
```

```
[Sysname] vlan 3
```

```
[Sysname-vlan3] port GigabitEthernet 2/0/3 GigabitEthernet 2/0/4
```

创建 VLAN5，并添加端口 GigabitEthernet2/0/5 和端口 GigabitEthernet2/0/6。

```
[Sysname-vlan3] quit
```

```
[Sysname] vlan 5
```

```
[Sysname-vlan5] port GigabitEthernet 2/0/5 GigabitEthernet 2/0/6
```

指定 VLAN10 为 Super VLAN，VLAN2、VLAN3 和 VLAN5 为 Sub VLAN。

```
[Sysname-vlan5] quit
```

```
[Sysname] vlan 10
```

```
[Sysname-vlan10] supervlan
```

```
[Sysname-vlan10] subvlan 2 3 5
```

查看 VLAN 10 的相关信息，验证以上配置是否生效。

```
<Sysname> display supervlan
```

```
SuperVLAN ID : 10
```

```
SubVLAN ID : 2-3 5
```

```
VLAN ID: 10
```

```
VLAN Type: static
```

```
It is a Super VLAN.
```

```
Route Interface: configured
```

```
IP Address: 10.0.0.1
```

```
Subnet Mask: 255.255.255.0
```

```
Description: VLAN 0010
```

```
Tagged Ports: none
```

```
Untagged Ports: none
```

```
VLAN ID: 2
```

```
VLAN Type: static
It is a Sub VLAN.
Route Interface: configured
IP Address: 10.0.0.1
Subnet Mask: 255.255.255.0
Description: VLAN 0002
Tagged Ports: none
Untagged Ports:
    GigabitEthernet2/0/1    GigabitEthernet2/0/2
```

```
VLAN ID: 3
VLAN Type: static
It is a Sub VLAN.
Route Interface: configured
IP Address: 10.0.0.1
Subnet Mask: 255.255.255.0
Description: VLAN 0003
Tagged Ports: none
Untagged Ports:
    GigabitEthernet2/0/3    GigabitEthernet2/0/4
```

```
VLAN ID: 5
VLAN Type: static
It is a Sub VLAN.
Route Interface: configured
IP Address: 10.0.0.1
Subnet Mask: 255.255.255.0
Description: VLAN 0005
Tagged Ports: none
Untagged Ports:
    GigabitEthernet2/0/5    GigabitEthernet2/0/6
```

1.6.5 完整配置

```
#
vlan 2 to 3
#
vlan 5
#
vlan 10
    supervlan
    subvlan 2 to 3 5
#
vlan 20
#
interface Vlan-interface10
    ip address 10.0.0.1 255.255.255.0
    local-proxy-arp enable
#
```

```

interface Vlan-interface20
 ip address 10.0.1.1 255.255.255.0
#
interface GigabitEthernet2/0/1
 port access vlan 2
#
interface GigabitEthernet2/0/2
 port access vlan 2
#
interface GigabitEthernet2/0/3
 port access vlan 3
#
interface GigabitEthernet2/0/4
 port access vlan 3
#
interface GigabitEthernet2/0/5
 port access vlan 5
#
interface GigabitEthernet2/0/6
 port access vlan 5
#
interface GigabitEthernet2/0/20
 port access vlan 20

```

1.6.6 配置注意事项

- **local-proxy-arp enable** 命令以及本地代理 ARP 功能的相关内容，请参见“ARP 典型配置指导”中的介绍。
- 如果某个 VLAN 被指定为 Super VLAN，则该 VLAN 不能被指定为某个端口的 GuestVlan；同样，如果某个 VLAN 被指定为某个端口的 GuestVlan，则该 VLAN 不能被指定为 Super VLAN。GuestVlan 的相关内容请参见“802.1x 典型配置指导”。
- 在 Super VLAN 下可以配置二层组播功能，但是由于 Super VLAN 内不包含任何端口，因此该配置将不会生效。
- 在 Super VLAN 对应的 VLAN 接口下可以配置 DHCP、三层组播、动态路由等功能，但是只有 DHCP 的配置生效，其它配置将不会生效。
- 在 Super VLAN 对应的 VLAN 接口下配置 VRRP 功能后，会对网络性能造成影响，建议用户不要这样配置。

目 录

1 GVRP典型配置指导.....	1-1
1.1 GVRP典型配置指导	1-1
1.1.1 组网图.....	1-1
1.1.2 应用要求	1-1
1.1.3 适用产品、版本	1-1
1.1.4 配置过程和解释	1-2
1.1.5 完整配置	1-4
1.1.6 配置注意事项	1-6

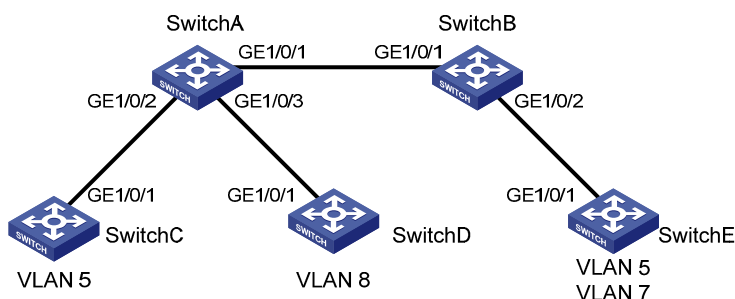
1 GVRP 典型配置指导

1.1 GVRP 典型配置指导

通过使用 GVRP，可以使同一局域网内的交换机接收来自其它交换机的 VLAN 注册信息，并动态更新本地的 VLAN 注册信息，包括当前的 VLAN 成员、这些 VLAN 成员可以通过哪个端口到达等。而且设备能够将本地的 VLAN 注册信息向其它设备传播，以使同一局域网内所有设备的 VLAN 信息达成一致，减少人工配置的工作量。

1.1.1 组网图

图1-1 GVRP 组网示意图



1.1.2 应用要求

组网情况如上图所示：

- 交换机上涉及的以太网端口均配置为 Trunk 端口，且允许所有 VLAN 通过；
- 所有交换机均开启全局 GVRP 和端口 GVRP 功能；
- SwitchC 配置静态 VLAN5，SwitchD 配置静态 VLAN8，SwitchE 配置静态 VLAN5 和 VLAN7，SwitchA 和 SwitchB 未进行静态 VLAN 的配置；
- 配置 SwitchE 的以太网端口 GigabitEthernet1/0/1 的注册模式为 fixed，显示 SwitchA、SwitchB 和 SwitchE 上动态注册的 VLAN 信息；
- 配置 SwitchE 的以太网端口 GigabitEthernet1/0/1 的注册模式为 forbidden，显示 SwitchA、SwitchB 和 SwitchE 上动态注册的 VLAN 信息。

1.1.3 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5500-SI 系列以太网交换机	Release 1207 软件版本	全系列硬件版本 (除 S5500-20TP-SI)

产品	软件版本	硬件版本
	Release 1301 软件版本	S5500-20TP-SI
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6100, Release 6300 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.1.4 配置过程和解释

- 配置 SwitchA

开启全局 GVRP。

```
<SwitchA> system-view
```

```
[SwitchA] gvrp
```

将以太网端口 GigabitEthernet1/0/1 配置为 Trunk 端口，并允许所有 VLAN 通过。

```
[SwitchA] interface GigabitEthernet 1/0/1
```

```
[SwitchA-GigabitEthernet1/0/1] port link-type trunk
```

```
[SwitchA-GigabitEthernet1/0/1] port trunk permit vlan all
```

在以太网端口 GigabitEthernet1/0/1 上开启 GVRP。

```
[SwitchA-GigabitEthernet1/0/1] gvrp
```

```
[SwitchA-GigabitEthernet1/0/1] quit
```

将以太网端口 GigabitEthernet1/0/2 配置为 Trunk 端口，并允许所有 VLAN 通过。

```
[SwitchA] interface GigabitEthernet 1/0/2
```

```
[SwitchA-GigabitEthernet1/0/2] port link-type trunk
```

```
[SwitchA-GigabitEthernet1/0/2] port trunk permit vlan all
```

在以太网端口 GigabitEthernet1/0/2 上开启 GVRP。

```
[SwitchA-GigabitEthernet1/0/2] gvrp
```

```
[SwitchA-GigabitEthernet1/0/2] quit
```

将以太网端口 GigabitEthernet1/0/3 配置为 Trunk 端口，并允许所有 VLAN 通过。

```
[SwitchA] interface GigabitEthernet 1/0/3
```

```
[SwitchA-GigabitEthernet1/0/3] port link-type trunk
```

```
[SwitchA-GigabitEthernet1/0/3] port trunk permit vlan all
```

在以太网端口 GigabitEthernet1/0/3 上开启 GVRP。

```
[SwitchA-GigabitEthernet1/0/3] gvrp
```

- 配置 SwitchB

配置 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 端口为 Trunk 端口，允许所有 VLAN 通过；并开启全局和以上两个端口的 GVRP 功能。配置过程可参见 SwitchA 的配置。

- 配置 SwitchC

创建 VLAN 5

```
<SwitchC> system-view
```

```
[SwitchC] vlan 5
```

[SwitchC-vlan5]

配置 GigabitEthernet1/0/1 端口为 Trunk 端口, 允许所有 VLAN 通过, 并开启全局和该端口的 GVRP 功能。配置过程可参见 SwitchA 的配置。



说明

为避免重复, 以下设备的配置只描述配置要点, 具体配置命令可参考上述设备的配置。

- 配置 SwitchD

配置 GigabitEthernet1/0/1 端口为 Trunk 端口, 允许所有 VLAN 通过; 同时开启全局和该端口的 GVRP 功能。

创建 VLAN8。

- 配置 SwitchE

配置 GigabitEthernet1/0/1 端口为 Trunk 端口, 允许所有 VLAN 通过; 同时开启全局和该端口的 GVRP 功能。

创建 VLAN5 和 VLAN7。

- 显示 SwitchA、SwitchB 和 SwitchE 上动态注册的 VLAN 信息。

显示 SwitchA 上的动态 VLAN 信息。

```
[SwitchA] display vlan dynamic
Total 3 dynamic VLAN exist(s).
The following dynamic VLANs exist:
5, 7, 8,
```

显示 SwitchB 上的动态 VLAN 信息。

```
[SwitchB] display vlan dynamic
Total 3 dynamic VLAN exist(s).
The following dynamic VLANs exist:
5, 7, 8,
```

显示 SwitchE 上的动态 VLAN 信息。

```
[SwitchE] display vlan dynamic
Total 1 dynamic VLAN exist(s).
The following dynamic VLANs exist:
8
```

- 配置 SwitchE 的以太网端口 GigabitEthernet1/0/1 的注册模式为 fixed, 显示 SwitchA、SwitchB 和 SwitchE 上动态注册的 VLAN 信息。

配置 SwitchE 的以太网端口 GigabitEthernet1/0/1 的注册模式为 fixed。

```
[SwitchE] interface GigabitEthernet 1/0/1
[SwitchE-GigabitEthernet1/0/1] gvrp registration fixed
```

显示 SwitchA 上的动态 VLAN 信息。

```
[SwitchA] display vlan dynamic
Total 3 dynamic VLAN exist(s).
The following dynamic VLANs exist:
```

```
5, 7, 8,
```

显示 SwitchB 上的动态 VLAN 信息。

```
[SwitchB] display vlan dynamic
Total 3 dynamic VLAN exist(s).
The following dynamic VLANs exist:
5, 7, 8,
```

显示 SwitchE 上的动态 VLAN 信息。

```
[SwitchE-GigabitEthernet1/0/1] display vlan dynamic
No dynamic vlans exist!
```

- 配置 SwitchE 的以太网端口 GigabitEthernet1/0/1 的注册模式为 forbidden，显示 SwitchA、SwitchB 和 SwitchE 上动态注册的 VLAN 信息。

配置 SwitchE 的以太网端口 GigabitEthernet1/0/1 的注册模式为 forbidden。

```
[SwitchE-GigabitEthernet1/0/1] gvrp registration forbidden
```

显示 SwitchA 上的动态 VLAN 信息。

```
[SwitchA] display vlan dynamic
Total 2 dynamic VLAN exist(s).
The following dynamic VLANs exist:
5, 8,
```

显示 SwitchB 上的动态 VLAN 信息。

```
[SwitchB] display vlan dynamic
Total 2 dynamic VLAN exist(s).
The following dynamic VLANs exist:
5, 8,
```

显示 SwitchE 上的动态 VLAN 信息。

```
[SwitchE] display vlan dynamic
No dynamic vlans exist!
```

1.1.5 完整配置

- SwitchA 上的配置

```
#
gvrp
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan all
gvrp
#
interface GigabitEthernet1/0/2
port link-type trunk
port trunk permit vlan all
gvrp
#
interface GigabitEthernet1/0/3
port link-type trunk
```



```

port trunk permit vlan all
gvrp

```

- SwitchB 上的配置

```

#
gvrp
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan all
gvrp
#
interface GigabitEthernet1/0/2
port link-type trunk
port trunk permit vlan all
gvrp

```

- SwitchC 上的配置

```

#
gvrp
#
vlan 5
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan all
gvrp

```

- SwitchD 上的配置

```

#
gvrp
#
vlan 8
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan all
gvrp

```

- SwitchE 上的配置

```

#
gvrp
#
vlan 5
#
vlan 7
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan all
gvrp registration forbidden

```

1.1.6 配置注意事项

- **port trunk permit vlan all** 命令只在 GVRP 功能配置过程中是必须执行的, 在没有配置 GVRP 的情况下, 建议用户不要使用该命令, 以防止未授权 VLAN 的用户通过该端口访问受限资源。
- 开启端口 GVRP 功能前, 必须先开启全局 GVRP 功能。
- 需要启动 GVRP 的端口必须为 Trunk 端口, 而且在该端口上开启 GVRP 后, 交换机不允许用户改变端口的 Trunk 类型为其他类型。
- GVRP 功能与业务环回功能互斥, 两者不可以同时应用。
- GVRP 功能只能运行在 MSTP 的 CIST 实例上, 并且 CIST 实例上被 MSTP 阻塞的端口不能收发 GVRP 报文。

目 录

1 Voice VLAN典型配置指导.....	1-1
1.1 Voice VLAN典型配置	1-1
1.1.1 组网图.....	1-1
1.1.2 应用要求	1-1
1.1.3 适用产品、版本	1-2
1.1.4 配置过程和解释	1-2
1.1.5 完整配置	1-3
1.1.6 配置注意事项	1-4

1 Voice VLAN 典型配置指导

1.1 Voice VLAN 典型配置

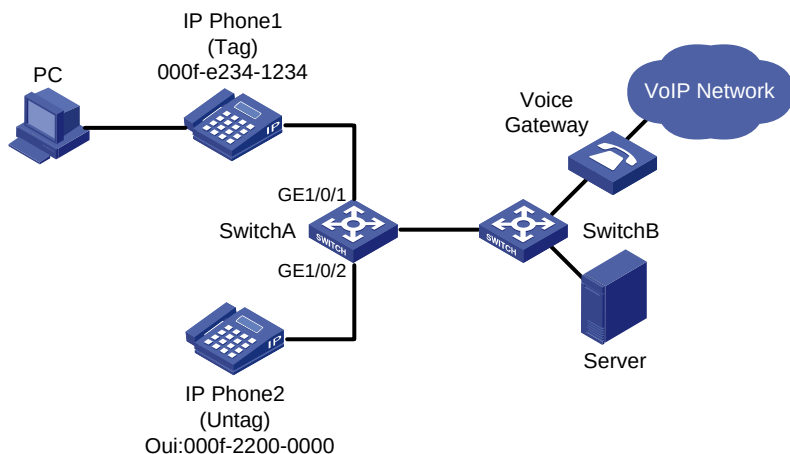
在自动模式下，Voice VLAN 功能将自动侦测进入端口报文的源 MAC 地址，如果能够与系统可识别的 OUI 地址相匹配，则将该报文识别为语音报文，在 Voice VLAN 中传输。

如果一段时间后，该端口没有再次收到源 MAC 地址符合 OUI 地址的报文，将自动退出 Voice VLAN，这段时间也称为 Voice VLAN 的老化时间。

在手动模式下，需要管理员通过手工配置命令将端口加入 Voice VLAN 或从 Voice VLAN 中删除。

1.1.1 组网图

图1-1 自动模式 Voice VLAN 组网示意图



1.1.2 应用要求

- 如图 1-1所示，PC机通过与IP Phone1 串连后接入SwitchA的GigabitEthernet1/0/1 端口，IP Phone2 单独接入GigabitEthernet1/0/2 端口。其中IP Phone1 发出的是Tag语音流（携带有Voice VLAN的VLAN Tag），IP Phone2 发出的是Untag语音流（未携带任何VLAN Tag）。现需要配置Voice VLAN功能，达到如下的要求：
- 配置 VLAN2 为 Voice VLAN，用来传输语音数据，老化时间是 100 分钟。传输用户业务数据的 VLAN 为 VLAN6。
- 要求使 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 端口能够自动识别语音流，并将语音数据与 PC 的业务数据划分到不同 VLAN，通过 SwitchB 分别发送至语音网关和服务器。
- IP Phone1 和 IP Phone2 的 OUI 地址不在交换机的缺省 OUI 范围内，需要增加 OUI 地址“000f-e200-0000”和“000f-2200-0000”，描述字符分别为“IP Phone1”和“IP Phone2”。

1.1.3 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301 软件版本, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301 软件版本, Release 5303 软件版本	全系列硬件版本
S5500-SI 系列以太网交换机	Release 1207 软件版本	全系列硬件版本 (除 S5500-20TP-SI)
	Release 1301 软件版本	S5500-20TP-SI
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6100 软件版本, Release 6300 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.1.4 配置过程和解释

创建 VLAN2、VLAN6。

```
<SwitchA> system-view
[SwitchA] vlan 2
[SwitchA-vlan2] quit
[SwitchA] vlan 6
[SwitchA-vlan6] quit
```

设置 Voice VLAN 的老化时间。

```
[SwitchA] voice vlan aging 100
```

设置 OUI 地址 000f-e200-0000，描述字符为“IP Phone1”。

```
[SwitchA] voice vlan mac-address 000f-e200-0000 mask ffff-ff00-0000 description IP Phone1
```

设置 OUI 地址 000f-2200-0000，描述字符为“IP Phone2”。

```
[SwitchA] voice vlan mac-address 000f-2200-0000 mask ffff-ff00-0000 description IP Phone2
```

全局开启 Voice VLAN 功能。

```
[SwitchA] voice vlan 2 enable
```

将端口 GigabitEthernet1/0/1 上 Voice VLAN 的工作模式设置为自动模式。（可选，缺省情况下，端口的 Voice VLAN 工作在自动模式。）

```
[SwitchA] interface GigabitEthernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] voice vlan mode auto
```

将端口 GigabitEthernet1/0/1 设定为 Trunk 端口。

```
[SwitchA-GigabitEthernet1/0/1] port link-type trunk
```

设置端口的缺省 VLAN 为 VLAN6，并允许 VLAN6 的报文通过，以供 PC 机的正常数据通信使用。

```
[SwitchA-GigabitEthernet1/0/1] port trunk pvid vlan 6
[SwitchA-GigabitEthernet1/0/1] port trunk permit vlan 6
```

开启端口 Voice VLAN 功能。

```
[SwitchA-GigabitEthernet1/0/1] voice vlan enable
```



说明

- 完成以上配置后，当 PC 报文通过时，数据自动在端口的缺省 VLAN、也就是业务 VLAN 中传输；当 IP Phone 的报文通过时，端口自动将 Voice VLAN 加入到端口允许通过的 VLAN 列表中，而且在发送时以带有 Tag 的形式发送，使 IP Phone 可以正常接收报文。
- 端口 GigabitEthernet1/0/1 也可以配置为 Hybrid 端口，配置过程与 Trunk 端口类似，只需要将业务 VLAN 配置为缺省 VLAN 即可，当 IP Phone 发出的报文通过时，端口自动将 Voice VLAN 加入到允许通过的 Tagged Port 列表中，保证 Voice VLAN 的报文带有 VLAN Tag 发送。

由于 IP Phone2 只能发出 Untag 的语音流，因此 GigabitEthernet1/0/2 端口只能配置为手工模式。

```
[SwitchA-GigabitEthernet1/0/1] quit
```

```
[SwitchA] interface GigabitEthernet 1/0/2
```

```
[SwitchA-GigabitEthernet1/0/2] undo voice vlan mode auto
```

配置 GigabitEthernet1/0/2 端口为 Access 端口，设置允许通过的 VLAN 为 Voice VLAN。

```
[SwitchA-GigabitEthernet1/0/2] port access vlan 2
```

开启端口 Voice VLAN 功能。

```
[SwitchA-GigabitEthernet1/0/2] voice vlan enable
```



说明

- 端口 GigabitEthernet1/0/2 也可以配置为 Trunk 或 Hybrid 端口，同样需要将 Voice VLAN 配置为缺省 VLAN，且必须配置在发送 Voice VLAN 的报文时去掉 VLAN Tag。
- 如果 IP Phone2 发出的是 Tag 语音流，则 GigabitEthernet1/0/2 端口只能配置为 Trunk 或 Hybrid 端口，并以保留 VLAN Tag 的方式发送 VLAN2 的报文。

1.1.5 完整配置

```
#
vlan 1 to 2
#
vlan 6
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 1 6
port trunk pvid vlan 6
voice vlan enable
#
interface GigabitEthernet1/0/2
port access vlan 2
undo voice vlan mode auto
voice vlan enable
#
voice vlan aging 100
voice vlan mac-address 000f-2200-0000 mask ffff-ff00-0000 description IP Phone2
```

```
voice vlan mac-address 000f-e200-0000 mask ffff-ff00-0000 description IP Phone1
voice vlan 2 enable
```

1.1.6 配置注意事项

- 缺省情况下，系统将以下地址预置为 Voice VLAN 的 OUI 地址，用户可以自行删除或修改这些预置地址。

表1-2 设备预置的 OUI 地址

序号	OUI 地址	生产厂商
1	0001-e300-0000	Siemens phone
2	0003-6b00-0000	Cisco phone
3	0004-0d00-0000	Avaya phone
4	00d0-1e00-0000	Pingtel phone
5	0060-b900-0000	Philips/NEC phone
6	00e0-7500-0000	Polycom phone
7	00e0-bb00-0000	3com phone

- 由于工作在自动模式下的端口不能通过命令配置加入 Voice VLAN，因此，如果用户将某个 VLAN 同时配置为 Voice VLAN 和协议 VLAN，则协议 VLAN 功能将不能与该端口进行绑定。关于协议 VLAN 的介绍请参见本手册“VLAN”部分。
- 工作在自动模式的端口，不能将缺省 VLAN 设置为 Voice VLAN，否则系统会输出信息，提示用户无法进行配置。
- 同一时刻只能有一个 VLAN 使能 Voice VLAN。
- Voice VLAN 功能只支持在静态 VLAN 上启动，不能配置动态 VLAN 作为 Voice VLAN。
- 当 Voice VLAN 工作在安全模式时，设备只允许源地址是可识别的语音 OUI 地址的数据通过，源地址不合法的报文将直接被丢弃（包括一些认证报文，如 802.1x 认证报文）。建议用户尽量不要在 Voice VLAN 中同时传输语音和业务数据。如确有此需要，请确认 Voice VLAN 的安全模式已关闭。

目 录

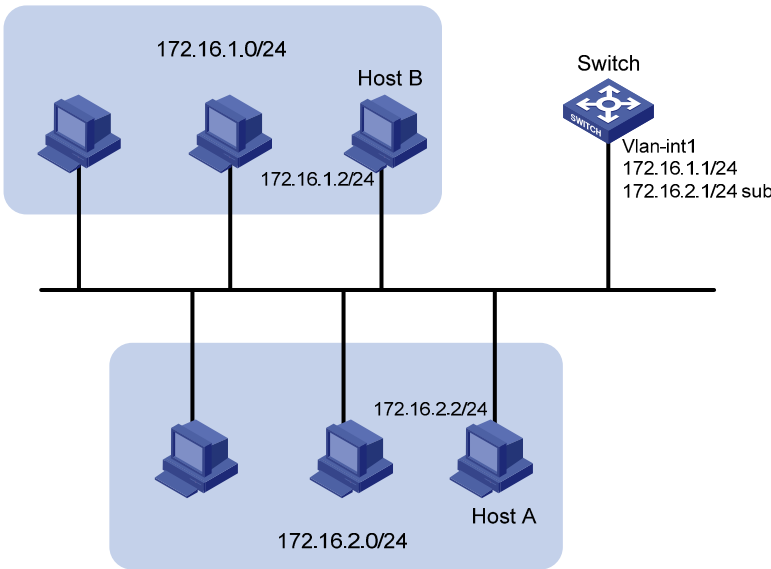
1 IP地址-IP性能典型配置指导.....	1-1
1.1 IP地址典型配置指导	1-1
1.1.1 组网图	1-1
1.1.2 应用要求	1-1
1.1.3 适用产品、版本	1-1
1.1.4 配置过程和解释	1-2
1.1.5 完整配置	1-3
1.1.6 配置注意事项	1-3
1.2 IP性能典型配置指导	1-3
1.2.1 组网图	1-3
1.2.2 应用要求	1-3
1.2.3 适用产品、版本	1-3
1.2.4 配置过程和解释	1-4
1.2.5 完整配置	1-4
1.2.6 配置注意事项	1-5

1 IP 地址-IP 性能典型配置指导

1.1 IP 地址典型配置指导

1.1.1 组网图

图1-1 IP 地址配置组网图



1.1.2 应用要求

Switch 的端口(属于 VLAN1)连接一个局域网,局域网中的计算机分别属于 2 个网段: 172.16.1.0/24 和 172.16.2.0/24。要求这两个网段的主机都可以通过 Switch 与外部网络通信, 且这两个网段中的主机能够互通。

1.1.3 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301 软件版本, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301 软件版本, Release 5303 软件版本	全系列硬件版本
S5500-SI 系列以太网交换机	Release 1207 软件版本	全系列硬件版本 (除 S5500-20TP-SI)
	Release 1301 软件版本	S5500-20TP-SI
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6100 软件版本, Release 6300 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.1.4 配置过程和解释

针对上述的需求，如果在 Switch 的 VLAN 接口 1 上只配置一个 IP 地址，则只有一部分主机能够通过 Switch 与外部网络通信。为了使局域网内的所有主机都能够通过 Switch 访问外部网络，需要配置 VLAN 接口 1 的从 IP 地址。为了使两个网段中的主机能够互通，两个网段中的主机都需要将 Switch 设置为网关。

配置 VLAN 接口 1 的主 IP 地址和从 IP 地址。

```
<Switch> system-view
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ip address 172.16.1.1 255.255.255.0
[Switch-Vlan-interface1] ip address 172.16.2.1 255.255.255.0 sub
[Switch-Vlan-interface1] return
```

在 172.16.1.0/24 网段中的主机上配置网关为 172.16.1.1；在 172.16.2.0/24 网段中的主机上配置网关为 172.16.2.1。

使用 **ping** 命令检测 Switch 与网络 172.16.1.0/24 内主机的连通性。

```
<Switch> ping 172.16.1.2
  PING 172.16.1.2: 56 data bytes, press CTRL_C to break
    Reply from 172.16.1.2: bytes=56 Sequence=1 ttl=255 time=25 ms
    Reply from 172.16.1.2: bytes=56 Sequence=2 ttl=255 time=27 ms
    Reply from 172.16.1.2: bytes=56 Sequence=3 ttl=255 time=26 ms
    Reply from 172.16.1.2: bytes=56 Sequence=4 ttl=255 time=26 ms
    Reply from 172.16.1.2: bytes=56 Sequence=5 ttl=255 time=26 ms

  --- 172.16.1.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
  round-trip min/avg/max = 25/26/27 ms
```

显示信息表示 Switch 与网络 172.16.1.0/24 内的主机可以互通。

使用 **ping** 命令检测 Switch 与网络 172.16.2.0/24 内主机的连通性。

```
<Switch> ping 172.16.2.2
  PING 172.16.2.2: 56 data bytes, press CTRL_C to break
    Reply from 172.16.2.2: bytes=56 Sequence=1 ttl=255 time=25 ms
    Reply from 172.16.2.2: bytes=56 Sequence=2 ttl=255 time=26 ms
    Reply from 172.16.2.2: bytes=56 Sequence=3 ttl=255 time=26 ms
    Reply from 172.16.2.2: bytes=56 Sequence=4 ttl=255 time=26 ms
    Reply from 172.16.2.2: bytes=56 Sequence=5 ttl=255 time=26 ms

  --- 172.16.2.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
  round-trip min/avg/max = 25/25/26 ms
```

显示信息表示 Switch 与网络 172.16.2.0/24 内的主机可以互通。

使用 **ping** 命令检测网络 172.16.1.0/24 和网络 172.16.2.0/24 内主机的连通性。在 Host A 上可以 ping 通 Host B。

1.1.5 完整配置

```
#
interface Vlan-interface1
 ip address 172.16.1.1 255.255.255.0
 ip address 172.16.2.1 255.255.255.0 sub
#
```

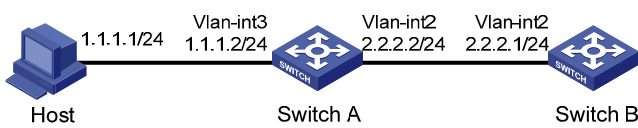
1.1.6 配置注意事项

- 一个接口只能有一个主 IP 地址。新配置的主 IP 地址将覆盖原有主 IP 地址。
- 当接口被配置为通过 BOOTP、DHCP 方式获取 IP 地址后，则不能再给该接口配置从 IP 地址。
- 同一接口的主、从 IP 地址可以在同一网段，但不同接口之间的 IP 地址不可以在同一网段。

1.2 IP 性能典型配置指导

1.2.1 组网图

图1-2 配置收发定向广播报文组网图



1.2.2 应用要求

如 图 1-2所示，Host的接口和Switch A的VLAN接口 3 处于同一个网段（1.1.1.0/24），Switch A的VLAN接口 2 和Switch B的VLAN接口 2 处于另外一个网段（2.2.2.0/24）。Host上配置默认网关为 Switch A的VLAN接口 3 的地址（1.1.1.2/24），Switch B上配置静态路由使得Host与Switch B之间路由可达。

1.2.3 适用产品、版本

表1-2 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301 软件版本， Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301 软件版本， Release 5303 软件版本	全系列硬件版本
S5500-SI 系列以太网交换机	Release 1207 软件版本	全系列硬件版本 (除 S5500-20TP-SI)
	Release 1301 软件版本	S5500-20TP-SI
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6100 软件版本， Release 6300 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.2.4 配置过程和解释

(1) 配置 Switch A

配置允许 Switch A 接收定向的广播报文。

```
<SwitchA> system-view
```

```
[SwitchA] ip forward-broadcast
```

创建 VLAN2 和 VLAN3。

```
[SwitchA] vlan 2
```

```
[SwitchA-Vlan2] quit
```

```
[SwitchA] vlan 3
```

```
[SwitchA-Vlan3] quit
```

配置 VLAN 接口 3 和 VLAN 接口 2 的 IP 地址。

```
[SwitchA] interface vlan-interface 3
```

```
[SwitchA-Vlan-interface3] ip address 1.1.1.2 24
```

```
[SwitchA-Vlan-interface3] quit
```

```
[SwitchA] interface vlan-interface 2
```

```
[SwitchA-Vlan-interface2] ip address 2.2.2.2 24
```

配置允许 VLAN 接口 2 转发定向广播报文。

```
[SwitchA-Vlan-interface2] ip forward-broadcast
```

(2) 配置 Switch B

配置允许 Switch B 接收定向的广播报文。

```
<SwitchB> system-view
```

```
[SwitchB] ip forward-broadcast
```

创建 VLAN2。

```
[SwitchB] vlan 2
```

```
[SwitchB-Vlan2] quit
```

配置 Switch B 到 Host 的静态路由。

```
[SwitchB] ip route-static 1.1.1.1 24 2.2.2.2
```

配置 VLAN 接口 2 的 IP 地址。

```
[SwitchB] interface vlan-interface 2
```

```
[SwitchB-Vlan-interface2] ip address 2.2.2.1 24
```

配置完成以后，在 Host 上 ping Switch A 的 VLAN 接口 2 所在子网网段的广播地址（2.2.2.255）时，Switch B 的 VLAN 接口 2 可以收到该报文。取消掉任何一个 **ip forward-broadcast** 的配置，Switch B 的 VLAN 接口 2 都不能收到该报文。

1.2.5 完整配置

- Switch A 上的配置

```
#
```

```
ip forward-broadcast
```

```
#
```

```
vlan 2
```

```
#
vlan 3
#
interface Vlan-interface2
 ip address 2.2.2.2 255.255.255.0
 ip forward-broadcast
#
interface Vlan-interface3
 ip address 1.1.1.2 255.255.255.0
```

- Switch B 上的配置

```
#
 ip forward-broadcast
#
vlan 2
#
interface Vlan-interface2
 ip address 2.2.2.1 255.255.255.0
#
 ip route-static 1.1.1.0 255.255.255.0 2.2.2.2
```

1.2.6 配置注意事项

无

目 录

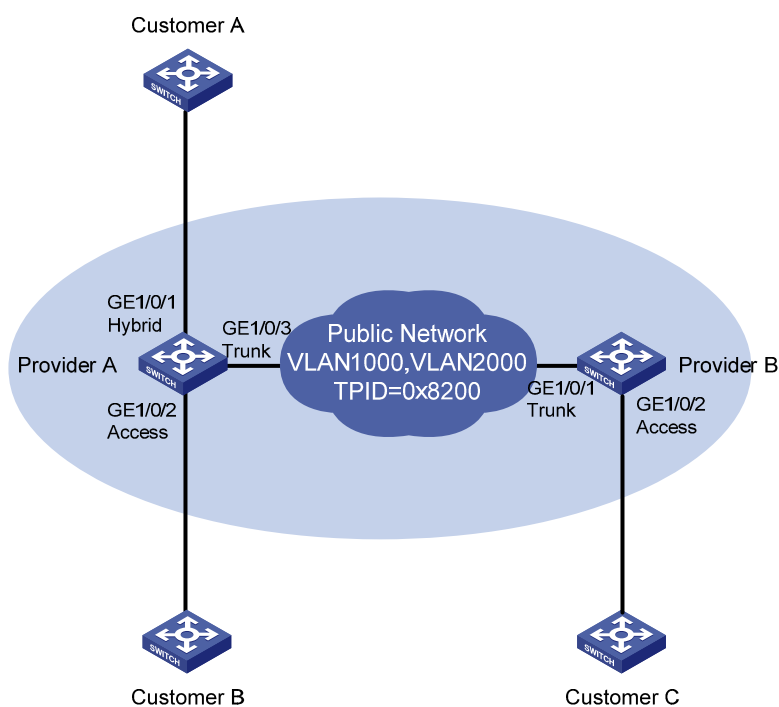
1 QinQ典型配置指导	1-1
1.1 QinQ典型配置指导	1-1
1.1.1 组网图	1-1
1.1.2 应用要求	1-1
1.1.3 适用产品、版本	1-2
1.1.4 配置过程和解释	1-2
1.1.5 完整配置	1-4
1.1.6 配置注意事项	1-5
1.2 基于流的灵活QinQ典型配置指导	1-5
1.2.1 组网图	1-5
1.2.2 应用要求	1-5
1.2.3 适用产品、版本	1-6
1.2.4 配置过程和解释	1-6
1.2.5 完整配置	1-8
1.2.6 配置注意事项	1-10

1 QinQ 典型配置指导

1.1 QinQ 典型配置指导

1.1.1 组网图

图1-1 QinQ 组网示意图



1.1.2 应用要求

Provider A、Provider B 作为运营商网络边缘设备，Customer A、Customer B、Customer C 为用户网络边缘设备。Provider A、Provider B 之间通过 Trunk 端口连接，Provider A 属于运营商网络的 VLAN1000，Provider B 属于运营商网络的 VLAN2000。Provider A 和 Provider B 之间，运营商采用其他厂商的设备，TPID 值为 0x8200。



说明

缺省情况下，H3C 系列交换机使用的 TPID 值为 0x8100。

希望配置完成后达到下列要求：

- Customer A 的 VLAN10 的报文可以和 Customer B 的 VLAN10 的报文经过运营商网络的 VLAN1000 转发后互通
- Customer A 的 VLAN20 的报文可以和 Customer C 的 VLAN20 的报文经过运营商网络的 VLAN2000 转发后互通

1.1.3 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5500-SI 系列以太网交换机	Release 1207 软件版本	全系列硬件版本 (除 S5500-20TP-SI)
	Release 1301 软件版本	S5500-20TP-SI
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.1.4 配置过程和解释



说明

这里只介绍运营商边缘设备上的配置，用户必须通过配置保证运营商网络内部的设备允许 QinQ 报文外层 Tag 对应的 VLAN 通过。

(1) Provider A 的配置

创建 VLAN1000 和 VLAN2000。

```
<ProviderA> system-view
[ProviderA] vlan 1000
[ProviderA-vlan1000] quit
[ProviderA] vlan 2000
[ProviderA-vlan2000] quit
```

• GigabitEthernet1/0/1 端口的配置

配置端口为 Hybrid 端口，允许 VLAN1000 和 VLAN2000 的报文通过，并且在发送时去掉外层 Tag。

```
[ProviderA] interface GigabitEthernet 1/0/1
[ProviderA-GigabitEthernet1/0/1] port link-type hybrid
[ProviderA-GigabitEthernet1/0/1] port hybrid vlan 1000 2000 untagged
```



说明

- 如果用户使用的是 S3610 或 S5510 系列交换机的 Release 5301 版本，则在 GigabitEthernet1/0/1 端口上，还必须允许用户 VLAN10 和 VLAN20 通过，即将配置命令修改为“port hybrid vlan 10 20 1000 2000 untagged”。
- 如果用户使用的是上述交换机的 Release 5303 版本，可以关闭 VLAN 检查功能（在端口视图下执行 **vlan-check disable** 命令），这样 GigabitEthernet1/0/1 端口即可以不必允许 VLAN10 和 VLAN20 通过。

将来自 VLAN10 的报文封装 VLAN ID 为 1000 的外层 Tag。


```
[ProviderA-GigabitEthernet1/0/1] qinq vid 1000
[ProviderA-GigabitEthernet1/0/1-vid-1000] raw-vlan-id inbound 10
[ProviderA-GigabitEthernet1/0/1-vid-1000] quit
```

将来自 VLAN20 的报文封装 VLAN ID 为 2000 的外层 Tag。

```
[ProviderA-GigabitEthernet1/0/1] qinq vid 2000
[ProviderA-GigabitEthernet1/0/1-vid-2000] raw-vlan-id inbound 20
[ProviderA-GigabitEthernet1/0/1-vid-2000] quit
[ProviderA-GigabitEthernet1/0/1] quit
```

- GigabitEthernet1/0/2 端口的配置

配置端口为 Access 端口，允许 VLAN1000 的报文通过。

```
[ProviderA] interface GigabitEthernet 1/0/2
[ProviderA-GigabitEthernet1/0/2] port access vlan 1000
```

配置该端口的基本 QinQ 功能，将来自 VLAN10 的报文封装 VLAN ID 为 1000 的外层 Tag。

```
[ProviderA-GigabitEthernet1/0/2] qinq enable
[ProviderA-GigabitEthernet1/0/2] quit
```

- GigabitEthernet1/0/3 端口的配置

配置端口为 Trunk 端口，且允许 VLAN1000 和 VLAN2000 的报文通过。

```
[ProviderA] interface GigabitEthernet 1/0/3
[ProviderA-GigabitEthernet1/0/3] port link-type trunk
[ProviderA-GigabitEthernet1/0/3] port trunk permit vlan 1000 2000
```

为与公共网络中的设备进行互通，配置交换机发送报文时携带运营商 VLAN Tag 的 TPID 值为 0x8200。

```
[ProviderA-GigabitEthernet1/0/3] quit
[ProviderA] qinq ethernet-type service-tag 8200
```



说明

- 在 S3610、S5510、S3500-EA 或 S5500-SI 交换机上配置 QinQ 报文的 TPID 值时，所使用的命令和所在视图与 S5500-EI 系列交换机不同，具体命令的说明请参见各产品的操作手册，下文中不再赘述。
 - 在同时配置了基本 QinQ 和灵活 QinQ 的情况下，交换机对于没有匹配灵活 QinQ 规则的报文将使用基本 QinQ 功能进行处理。
-

(2) Provider B 的配置

创建 VLAN1000 和 VLAN2000。

```
<ProviderB> system-view
[ProviderB] vlan 1000
[ProviderB-vlan1000] quit
[ProviderB] vlan 2000
[ProviderB-vlan2000] quit
```

- GigabitEthernet1/0/1 端口的配置

配置端口为 Trunk 端口，且允许 VLAN1000 和 VLAN2000 的报文通过。

```
<ProviderB> system-view
```

```
[ProviderB] interface GigabitEthernet 1/0/1
[ProviderB-GigabitEthernet1/0/1] port link-type trunk
[ProviderB-GigabitEthernet1/0/1] port trunk permit vlan 1000 2000
```

为与公共网络中的设备进行互通，配置交换机发送报文时携带运营商 VLAN Tag 的 TPID 值为 0x8200。

```
[ProviderB-GigabitEthernet1/0/1] quit
[ProviderB] qinq ethernet-type service-tag 8200
```

- GigabitEthernet1/0/2 端口的配置

配置端口为 Access 端口，允许 VLAN2000 的报文通过。

```
[ProviderB] interface GigabitEthernet 1/0/2
[ProviderB-GigabitEthernet1/0/2] port access vlan 2000
```

配置该端口的基本 QinQ 功能，将来自 VLAN20 的报文封装 VLAN ID 为 2000 的外层 Tag。

```
[ProviderB-GigabitEthernet1/0/2] qinq enable
```

(3) 公共网络设备的配置

由于 Provider A 和 Provider B 之间使用的公共网络设备可能来自于其他厂商，这里只介绍基本原理：配置公共网络中与 Provider A 的 GigabitEthernet1/0/3 端口和 Provider B 的 GigabitEthernet1/0/1 端口连接的设备，使其相应的端口允许 VLAN1000 和 VLAN2000 的报文携带 VLAN Tag 进行发送即可。

1.1.5 完整配置

- ProviderA 的配置

```
#
qinq ethernet-type service-tag 8200
#
vlan 1000
#
vlan 2000
#
interface GigabitEthernet1/0/1
port link-type hybrid
port hybrid vlan 1 1000 2000 untagged
qinq vid 1000
raw-vlan-id inbound 10
qinq vid 2000
raw-vlan-id inbound 20
#
interface GigabitEthernet1/0/2
port access vlan 1000
qinq enable
#
interface GigabitEthernet1/0/3
port link-type trunk
port trunk permit vlan 1 1000 2000
```

- DeviceB 的配置

```
#
```

```

qinq ethernet-type service-tag 8200
#
vlan 1000
#
vlan 2000
#
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 1 1000 2000
#
interface GigabitEthernet1/0/2
port access vlan 2000
qinq enable

```

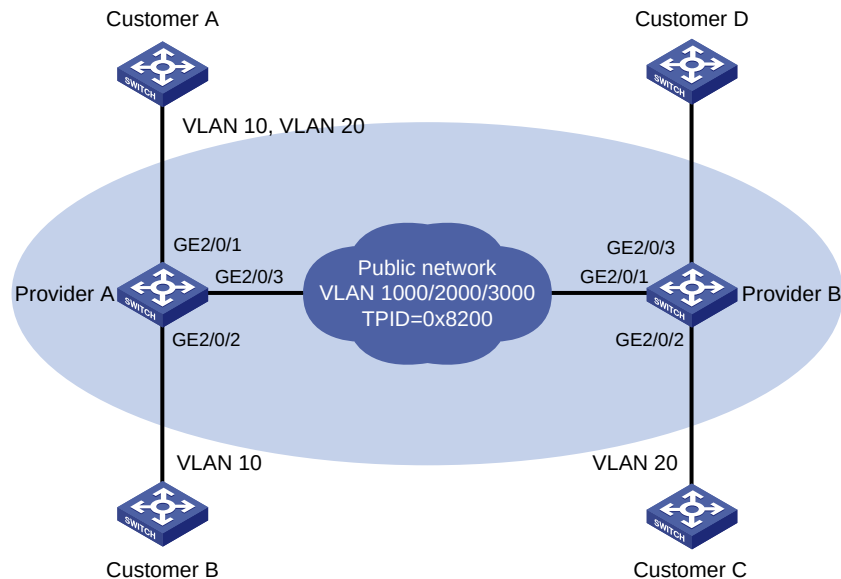
1.1.6 配置注意事项

一个内层 VLAN Tag 只能对应一个外层 VLAN Tag。如果用户想改变报文的外层 VLAN Tag，需要先删除旧的外层 VLAN Tag 配置，然后再配置新的外层 VLAN Tag。

1.2 基于流的灵活 QinQ 典型配置指导

1.2.1 组网图

图1-2 基于流的灵活 QinQ 组网示意图



1.2.2 应用要求

Provider A、Provider B 作为运营商网络边缘设备。Customer A、Customer B、Customer C、CustomerD 为用户网络边缘设备。Provider A、Provider B 之间通过 Trunk 端口连接，允许运营商网络的 VLAN1000、VLAN2000 和 VLAN3000 通过。Provider A 和 Provider B 之间，运营商采用其他厂商的设备，TPID 值为 0x8200。

希望配置完成后达到下列要求：

- Customer A 的 VLAN10 的报文可以和 Customer B 的 VLAN10 的报文经过运营商网络的 VLAN1000 转发后互通；
- Customer A 的 VLAN20 的报文可以和 Customer C 的 VLAN20 的报文经过运营商网络的 VLAN2000 转发后互通。
- Customer A 的其余 VLAN 的报文可以通过运营商网络的 VLAN3000 转发至 Customer D。

1.2.3 适用产品、版本

表1-2 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S7500E 系列以太网交换机	Release 6100, Release 6300 版本	全系列硬件版本

1.2.4 配置过程和解释

(1) Provider A 的配置

创建 VLAN1000、VLAN2000 和 VLAN3000。

```
<ProviderA> system-view
[ProviderA] vlan 1000
[ProviderA-vlan1000] quit
[ProviderA] vlan 2000
[ProviderA-vlan2000] quit
[ProviderA] vlan 3000
[ProviderA-vlan3000] quit
```

• GigabitEthernet2/0/1 端口的配置

配置端口为 Hybrid 端口，且允许 VLAN1000、VLAN2000 和 VLAN3000 的报文通过，并且在发送时去掉外层 Tag。

```
[ProviderA] interface gigabitethernet 2/0/1
[ProviderA-GigabitEthernet2/0/1] port link-type hybrid
[ProviderA-GigabitEthernet2/0/1] port hybrid vlan 1000 2000 3000 untagged
```

将 VLAN3000 配置为该端口的缺省 VLAN，并配置基本 QinQ 功能，为接收的报文封装 VLAN3000 的 Tag。

```
[ProviderA-GigabitEthernet2/0/1] port hybrid pvid vlan 3000
[ProviderA-GigabitEthernet2/0/1] qinq enable
[ProviderA-GigabitEthernet2/0/1] quit
```

创建流分类规则，将 Customer A 的 VLAN10 的报文定义为“A10”类。

```
[ProviderA] traffic classifier A10
[ProviderA-classifier-A10] if-match customer-vlan-id 10
[ProviderA-classifier-A10] quit
```

定义流行为，为报文封装 VLAN1000 的外层 VLAN Tag，流行为命名为“P1000”。

```
[ProviderA] traffic behavior P1000
[ProviderA-behavior-P1000] nest top-most vlan-id 1000
[ProviderA-behavior-P1000] quit
```

与以上配置类似，创建流分类“A20”匹配用户 VLAN ID 为 20 的报文，并创建流行为，为此类报文封装外层 VLAN2000 的 Tag。

```
[ProviderA] traffic classifier A20
[ProviderA-classifier-A20] if-match customer-vlan-id 20
[ProviderA-classifier-A20] quit
[ProviderA] traffic behavior P2000
[ProviderA-behavior-P2000] nest top-most vlan-id 2000
[ProviderA-behavior-P2000] quit
```

创建 QoS 策略，将流分类“A10”和流行为“P1000”进行关联，将流分类“A20”和流行为“P2000”关联，该策略命名为“qinq”。

```
[ProviderA] qos policy qinq
[ProviderA-qospolicy-qinq] classifier A10 behavior P1000
[ProviderA-qospolicy-qinq] classifier A20 behavior P2000
[ProviderA-qospolicy-qinq] quit
```

在 GigabitEthernet2/0/1 端口的接收方向应用“qinq”规则。

```
[ProviderA] interface gigabitethernet 2/0/1
[ProviderA-GigabitEthernet2/0/1] qos apply policy qinq inbound
```

- GigabitEthernet2/0/2 端口的配置

配置端口的缺省 VLAN 为 VLAN1000。

```
[ProviderA] interface gigabitethernet 2/0/2
[ProviderA-GigabitEthernet2/0/2] port access vlan 1000
```

配置端口的基本 QinQ 功能，将来自 VLAN10 的报文封装 VLAN ID 为 1000 的外层 Tag。

```
[ProviderA-GigabitEthernet2/0/2] qinq enable
[ProviderA-GigabitEthernet2/0/2] quit
```

- GigabitEthernet2/0/3 端口的配置

配置端口为 Trunk 端口，且允许 VLAN1000、VLAN2000 和 VLAN3000 的报文通过。

```
[ProviderA] interface gigabitethernet 2/0/3
[ProviderA-GigabitEthernet2/0/3] port link-type trunk
[ProviderA-GigabitEthernet2/0/3] port trunk permit vlan 1000 2000 3000
```

为与公共网络中的设备进行互通，配置运营商网络的 TPID 为 0x8200，即配置端口在添加外层 Tag 时使用的 TPID 值为 0x8200。

```
[ProviderA-GigabitEthernet2/0/3] qinq ethernet-type service-tag 8200
```

(2) Provider B 的配置

创建 VLAN1000、VLAN2000 和 VLAN3000。

```
<ProviderA> system-view
[ProviderA] vlan 1000
[ProviderA-vlan1000] quit
[ProviderA] vlan 2000
[ProviderA-vlan2000] quit
[ProviderA] vlan 3000
[ProviderA-vlan3000] quit
```

- GigabitEthernet2/0/1 端口的配置

配置端口为 Trunk 端口，且允许 VLAN1000、VLAN2000 和 VLAN3000 的报文通过。

```
<ProviderB> system-view
[ProviderB] interface gigabitethernet 2/0/1
[ProviderB-GigabitEthernet2/0/1] port link-type trunk
[ProviderB-GigabitEthernet2/0/1] port trunk permit vlan 1000 2000 3000
```

为与公共网络中的设备进行互通，配置运营商网络的 TPID 为 0x8200，即配置端口添加外层 Tag 时使用的 TPID 值为 0x8200。

```
[ProviderB-GigabitEthernet2/0/1] qinq ethernet-type service-tag 8200
[ProviderB-GigabitEthernet2/0/1] quit
```

- GigabitEthernet2/0/2 端口的配置

配置端口的缺省 VLAN 为 VLAN2000。

```
[ProviderB] interface gigabitethernet 2/0/2
[ProviderB-GigabitEthernet2/0/2] port access vlan 2000
```

配置端口的基本 QinQ 功能，将来自 VLAN20 的报文封装 VLAN ID 为 2000 的外层 Tag。

```
[ProviderB-GigabitEthernet2/0/2] qinq enable
[ProviderB-GigabitEthernet2/0/2] quit
```

- GigabitEthernet2/0/3 端口的配置

配置端口的缺省 VLAN 为 VLAN3000。

```
[ProviderB] interface gigabitethernet 2/0/3
[ProviderB-GigabitEthernet2/0/3] port access vlan 3000
```

配置端口的基本 QinQ 功能，为来自所有用户 VLAN 的报文封装 VLAN ID 为 3000 的外层 Tag。

```
[ProviderB-GigabitEthernet2/0/3] qinq enable
```

(3) 公共网络设备的配置

由于 Provider A 和 Provider B 之间使用的公共网络设备可能来自于其他厂商，这里只介绍基本原理：配置公共网络中与 Provider A 的 GigabitEthernet2/0/3 端口和 Provider B 的 GigabitEthernet2/0/1 端口连接的设备，使其相应的端口允许 VLAN1000、VLAN2000 和 VLAN3000 的报文携带 VLAN Tag 进行发送即可。

1.2.5 完整配置

- ProviderA 的配置

```
#
vlan 1000
#
vlan 2000
#
vlan 3000
#
#
traffic classifier A10 operator and
if-match customer-vlan-id 10
traffic classifier A20 operator and
if-match customer-vlan-id 20
#
```

```

traffic behavior P1000
  nest top-most vlan-id 1000
traffic behavior P2000
  nest top-most vlan-id 2000
#
qos policy qinq
  classifier A10 behavior P1000
  classifier A20 behavior P2000
#
interface GigabitEthernet2/0/1
  port link-type hybrid
  port hybrid vlan 1 100 1000 2000 3000 untagged
  port hybrid pvid vlan 3000
  qinq enable
  qos apply policy qinq inbound
#
interface GigabitEthernet2/0/2
  port access vlan 1000
  qinq enable
#
interface GigabitEthernet2/0/3
  port link-type trunk
  port trunk permit vlan 1 100 2000 3000
  qinq ethernet-type service-tag 8200

```

- ProviderB 的配置

```

#
vlan 1000
#
vlan 2000
#
vlan 3000
#
interface GigabitEthernet2/0/1
  port link-type trunk
  port trunk permit vlan 1 1000 2000 3000
  qinq ethernet-type service-tag 8200
#
interface GigabitEthernet2/0/2
  port access vlan 2000
  qinq enable
#
interface GigabitEthernet2/0/3
  port access vlan 3000
  qinq enable

```

1.2.6 配置注意事项

- 开启灵活 QinQ 前必须先配置端口的基本 QinQ 功能，灵活 QinQ 的优先级高于基本 QinQ，即当端口接收的报文不能匹配流分类规则的情况下，才根据基本 QinQ 的功能封装外层 VLAN Tag。
- S7500E 系列交换机的灵活 QinQ 的配置是基于 QoS 策略实现的，关于 QoS 策略的更多详细信息，请参见操作手册中“QoS”部分的介绍。

目 录

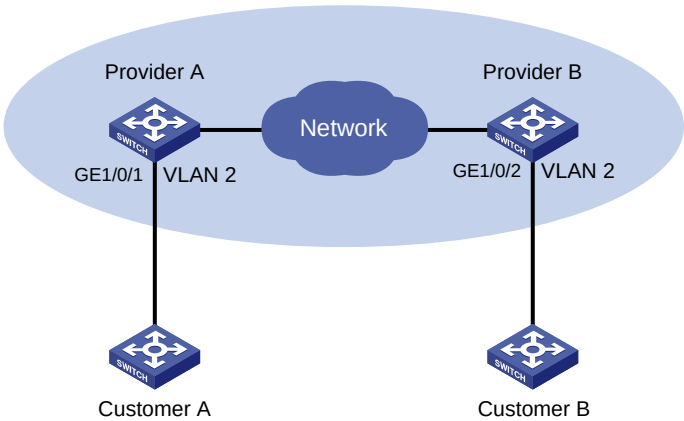
- 1 BPDU Tunnel典型配置指导 1-1
 - 1.1 BPDU Tunnel典型配置指导 1-1
 - 1.1.1 组网图 1-1
 - 1.1.2 应用要求 1-1
 - 1.1.3 适用产品、版本 1-1
 - 1.1.4 配置过程和解释 1-2
 - 1.1.5 完整配置 1-2
 - 1.1.6 配置注意事项 1-3

1 BPDU Tunnel 典型配置指导

1.1 BPDU Tunnel 典型配置指导

1.1.1 组网图

图1-1 BPDU Tunnel 组网示意图



1.1.2 应用要求

Customer A、Customer B 为用户网络接入设备，Provider A、Provider B 为运营商网络接入设备，运营商网络中的设备之间通过配置好的 Trunk 端口实现连接。

要求通过配置实现：

- 处于不同地域的用户 Customer A、Customer B 可以跨越运营商网络进行统一的生成树计算。
- BPDU Tunnel 报文采用的组播目的 MAC 地址为 0x0100-0CCD-CDD0。

1.1.3 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5500-SI 系列以太网交换机	Release 1207 软件版本	全系列硬件版本 (除 S5500-20TP-SI)
	Release 1301 软件版本	S5500-20TP-SI
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6100, Release 6300 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.1.4 配置过程和解释



说明

- BPDU TUNNEL 功能与 NTDP 功能不兼容，两者不可以同时应用。如果要开启端口的 BPDU TUNNEL 功能，必须先用 **undo ntdp enable** 命令关闭端口的 NTDP 功能。关于 NTDP 功能的介绍，请参见相应产品手册中的“集群管理配置”。
- S7500E 系列以太网交换机 Release 6100、Release 6300 软件版本均不支持 NTDP 功能，用户在做 S7500E 系列以太网交换机的配置时，无需在以太网端口视图下执行 **undo ntdp enable** 命令。
- S7500E 系列以太网交换机 Release 6300 软件版本不支持 **bpdu-tunnel dot1q enable** 命令，用户在做 Release 6300 软件版本的功能配置时无需执行 **bpdu-tunnel dot1q enable** 命令。

(1) Provider A 的配置

配置 BPDU Tunnel 报文采用的组播目的 MAC 地址为 0x0100-0CCD-CDD0。

```
<ProviderA> system-view
```

```
[ProviderA] bpdu-tunnel tunnel-dmac 0100-0ccd-cdd0
```

配置 GigabitEthernet1/0/1 端口使用 VLAN 2 对用户报文进行传输。

```
[ProviderA] interface GigabitEthernet 1/0/1
```

```
[ProviderA-GigabitEthernet1/0/1] port access vlan 2
```

配置 GigabitEthernet1/0/1 端口对 BPDU 报文进行透明传输。

```
[ProviderA-GigabitEthernet1/0/1] stp disable
```

```
[ProviderA-GigabitEthernet1/0/1] undo ntdp enable
```

```
[ProviderA-GigabitEthernet1/0/1] bpdu-tunnel dot1q enable
```

```
[ProviderA-GigabitEthernet1/0/1] bpdu-tunnel dot1q stp
```

(2) Provider B 的配置

配置 BPDU Tunnel 报文采用的组播目的 MAC 地址为 0x0100-0CCD-CDD0。

```
<ProviderB> system-view
```

```
[ProviderB] bpdu-tunnel tunnel-dmac 0100-0ccd-cdd0
```

配置 GigabitEthernet1/0/2 端口使用 VLAN 2 对用户报文进行传输。

```
[ProviderB] interface GigabitEthernet1/0/2
```

```
[ProviderB-GigabitEthernet1/0/2] port access vlan 2
```

配置 GigabitEthernet1/0/2 端口对 BPDU 报文进行透明传输。

```
[ProviderB-GigabitEthernet1/0/2] stp disable
```

```
[ProviderB-GigabitEthernet1/0/2] undo ntdp enable
```

```
[ProviderB-GigabitEthernet1/0/2] bpdu-tunnel dot1q enable
```

```
[ProviderB-GigabitEthernet1/0/2] bpdu-tunnel dot1q stp
```

1.1.5 完整配置

- ProviderA 的配置

```
#
```

```
bpdu-tunnel tunnel-dmac 0100-0ccd-cdd0
```

```
#
```

```
interface GigabitEthernet1/0/1
port access vlan 2
stp disable
undo ntdp enable
bpdu-tunnel dot1q enable
bpdu-tunnel dot1q stp
```

- DeviceB 的配置

```
#
bpdu-tunnel tunnel-dmac 0100-0ccd-cdd0
#
interface GigabitEthernet1/0/2
port access vlan 2
stp disable
undo ntdp enable
bpdu-tunnel dot1q enable
bpdu-tunnel dot1q stp
```

1.1.6 配置注意事项

- 只有全局 BPDU Tunnel 功能打开后，端口的 BPDU Tunnel 功能才能生效。缺省情况下，全局的 BPDU Tunnel 功能处于开启状态，用户无需手工开启；各端口的 BPDU Tunnel 功能处于关闭状态。如果全局的 BPDU Tunnel 被关闭，用户可以在系统视图下使用 **bpdu-tunnel dot1q enable** 命令将其开启。
- BPDU Tunnel 功能与 GVRP 功能不兼容，两者不可以同时应用。关于 GVRP 的介绍，请参见“GVRP 典型配置指导”。
- 在运营商网络两端的报文输入/输出设备上配置的 BPDU Tunnel 报文采用的组播目的 MAC 地址必须保持一致，否则，系统无法对 BPDU Tunnel 报文进行正确的识别。

目 录

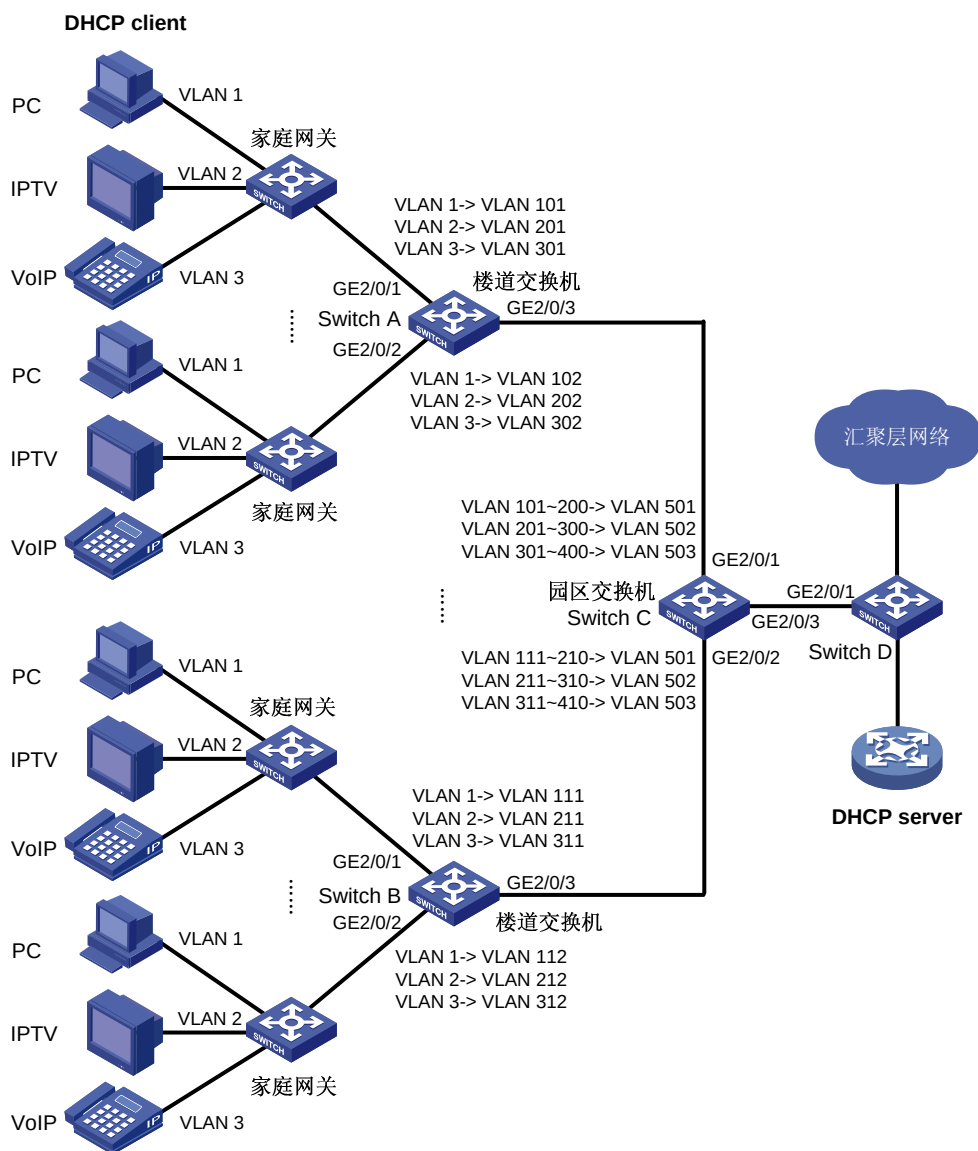
1 VLAN映射典型配置指导	1-1
1.1 1:1 VLAN映射和N:1 VLAN映射典型配置指导	1-1
1.1.1 组网图	1-1
1.1.2 应用要求	1-1
1.1.3 适用产品、版本	1-2
1.1.4 配置过程和解释	1-2
1.1.5 完整配置	1-9
1.1.6 配置注意事项	1-15
1.2 1:1 VLAN映射和 2:2 VLAN映射典型配置指导	1-16
1.2.1 组网图	1-16
1.2.2 应用要求	1-16
1.2.3 适用产品、版本	1-16
1.2.4 配置过程和解释	1-16
1.2.5 完整配置	1-19
1.2.6 配置注意事项	1-21

1 VLAN 映射典型配置指导

1.1 1:1 VLAN 映射和 N:1 VLAN 映射典型配置指导

1.1.1 组网图

图1-1 1:1 和 N:1 VLAN 映射组网示意图



1.1.2 应用要求

在多业务智能小区中，每户家庭都有 PC、IPTV 和 VoIP 三种网络业务应用，各个业务终端均使用汇聚层的 DHCP 服务器自动分配 IP 地址。

家庭网关将这些业务分别使用 VLAN1、VLAN2 和 VLAN3 发送至楼道交换机，再经由园区交换机发送至汇聚层网络。为实现对多个用户的多种业务进行精确划分，现要求使用 1:1 和 N:1 VLAN 映射功能完成以下使用需求：

- 在楼道交换机上使用 1:1 VLAN 映射功能，实现将不同家庭网关发出的相同 VLAN 的报文进行区分
- 在园区交换机上使用 N:1 VLAN 映射功能，根据业务类型将所有用户的报文分为三类上送至汇聚层交换机

1.1.3 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S7500E 系列以太网交换机	Release 6100, Release 6300 软件版本	全系列硬件版本



说明

S7500E 系列交换机的 Release 6100 软件版本仅支持 1:1 VLAN 映射。

1.1.4 配置过程和解释

(1) 配置 Switch A

- VLAN 和端口的配置

创建 CVLAN（Custom VLAN）和 SVLAN（Service VLAN）。

```
<SwitchA> system-view
[SwitchA] vlan 2 to 3
[SwitchA] vlan 101 to 102
[SwitchA] vlan 201 to 202
[SwitchA] vlan 301 to 302
```

配置端口 GigabitEthernet2/0/1 允许第一个家庭的 CVLAN 和对应 SVLAN 的报文通过。

```
[SwitchA] interface gigabitethernet 2/0/1
[SwitchA-GigabitEthernet2/0/1] port link-type trunk
[SwitchA-GigabitEthernet2/0/1] port trunk permit vlan 1 2 3 101 201 301
```

开启端口 GigabitEthernet2/0/1 的基本 QinQ 功能。

```
[SwitchA-GigabitEthernet2/0/1] qinq enable
[SwitchA] quit
```

配置端口 GigabitEthernet2/0/2 允许第二个家庭的 CVLAN 和对应 SVLAN 的报文通过。

```
[SwitchA] interface gigabitethernet 2/0/2
[SwitchA-GigabitEthernet2/0/2] port link-type trunk
[SwitchA-GigabitEthernet2/0/2] port trunk permit vlan 1 2 3 102 202 302
```

开启端口 GigabitEthernet2/0/2 的基本 QinQ 功能。

```
[SwitchA-GigabitEthernet2/0/2] qinq enable
[SwitchA] quit
```

- 配置上行报文映射策略

配置流分类 c1、c2 和 c3，分别匹配家庭网关发出的 CVLAN。

```
[SwitchA] traffic classifier c1
[SwitchA-classifier-c1] if-match customer-vlan-id 1
[SwitchA-classifier-c1] traffic classifier c2
[SwitchA-classifier-c2] if-match customer-vlan-id 2
[SwitchA-classifier-c2] traffic classifier c3
[SwitchA-classifier-c3] if-match customer-vlan-id 3
[SwitchA-classifier-c3] quit
```

配置流行为 b1、b2、b3、b4、b5、b6，分别定义替换不同的 SVLAN（101、201、301、102、202、302）的动作。

```
[SwitchA] traffic behavior b1
[SwitchA-behavior-b1] remark service-vlan-id 101
[SwitchA-behavior-b1] traffic behavior b2
[SwitchA-behavior-b2] remark service-vlan-id 201
[SwitchA-behavior-b2] traffic behavior b3
[SwitchA-behavior-b3] remark service-vlan-id 301
[SwitchA-behavior-b3] traffic behavior b4
[SwitchA-behavior-b4] remark service-vlan-id 102
[SwitchA-behavior-b4] traffic behavior b5
[SwitchA-behavior-b5] remark service-vlan-id 202
[SwitchA-behavior-b5] traffic behavior b6
[SwitchA-behavior-b6] remark service-vlan-id 302
[SwitchA-behavior-b6] quit
```

配置 QoS 策略 p1 和 p2，根据网络规划将流分类和流行为进行绑定。

```
[SwitchA] qos policy p1
[SwitchA-policy-p1] classifier c1 behavior b1
[SwitchA-policy-p1] classifier c2 behavior b2
[SwitchA-policy-p1] classifier c3 behavior b3
[SwitchA-policy-p1] quit
[SwitchA] qos policy p2
[SwitchA-policy-p2] classifier c1 behavior b4
[SwitchA-policy-p2] classifier c2 behavior b5
[SwitchA-policy-p2] classifier c3 behavior b6
[SwitchA-policy-p2] quit
```

- 配置下行报文映射策略

配置下行策略，将 SVLAN 映射回原来的 CVLAN，配置思路类似与配置上行策略，这里不再赘述。

```
[SwitchA] traffic classifier c11
[SwitchA-classifier-c11] if-match service-vlan-id 101
[SwitchA-classifier-c11] traffic classifier c22
[SwitchA-classifier-c22] if-match service-vlan-id 201
[SwitchA-classifier-c22] traffic classifier c33
[SwitchA-classifier-c33] if-match service-vlan-id 301
[SwitchA-classifier-c33] traffic classifier c44
[SwitchA-classifier-c44] if-match service-vlan-id 102
[SwitchA-classifier-c44] traffic classifier c55
[SwitchA-classifier-c55] if-match service-vlan-id 202
[SwitchA-classifier-c55] traffic classifier c66
```



```
[SwitchA-classifier-c66] if-match service-vlan-id 302
[SwitchA-classifier-c66] quit
[SwitchA] traffic behavior b11
[SwitchA-behavior-b11] remark customer-vlan-id 1
[SwitchA-behavior-b11] traffic behavior b22
[SwitchA-behavior-b22] remark customer-vlan-id 2
[SwitchA-behavior-b22] traffic behavior b33
[SwitchA-behavior-b33] remark customer-vlan-id 3
[SwitchA-behavior-b33] quit
[SwitchA] qos policy p11
[SwitchA-policy-p11] classifier c11 behavior b11
[SwitchA-policy-p11] classifier c22 behavior b22
[SwitchA-policy-p11] classifier c33 behavior b33
[SwitchA-policy-p11] quit
[SwitchA] qos policy p22
[SwitchA-policy-p22] classifier c44 behavior b11
[SwitchA-policy-p22] classifier c55 behavior b22
[SwitchA-policy-p22] classifier c66 behavior b33
[SwitchA-policy-p22] quit
```

- 在端口上应用 QoS 策略

在端口 GigabitEthernet2/0/1 的入方向应用上行策略 p1。

```
[SwitchA] interface GigabitEthernet 2/0/1
[SwitchA-GigabitEthernet2/0/1] qos apply policy p1 inbound
```

在端口 GigabitEthernet2/0/1 的出方向应用下行策略 p11。

```
[SwitchA-GigabitEthernet2/0/1] qos apply policy p11 outbound
[SwitchA-GigabitEthernet2/0/1] quit
```

在端口 GigabitEthernet2/0/2 的入方向应用上行策略 p2。

```
[SwitchA] interface GigabitEthernet 2/0/2
[SwitchA-GigabitEthernet2/0/2] qos apply policy p2 inbound
```

在端口 GigabitEthernet2/0/2 的出方向应用下行策略 p22。

```
[SwitchA-GigabitEthernet2/0/2] qos apply policy p22 outbound
[SwitchA-GigabitEthernet2/0/2] quit
```

- 配置上行端口

配置端口 GigabitEthernet2/0/3 允许 SVLAN 的报文通过。

```
[SwitchA] interface gigabitethernet 2/0/3
[SwitchA-GigabitEthernet2/0/3] port link-type trunk
[SwitchA-GigabitEthernet2/0/3] port trunk permit vlan 101 201 301 102 202 302
```

(2) 配置 Switch B

- VLAN 和端口的配置

创建 CVLAN 和 SVLAN。

```
<SwitchB> system-view
[SwitchB] vlan 2 to 3
[SwitchB] vlan 111 to 112
[SwitchB] vlan 211 to 212
```

```
[SwitchB] vlan 311 to 312
```

配置端口 GigabitEthernet2/0/1 允许 CVLAN 和 SVLAN 的报文通过。

```
[SwitchB] interface gigabitethernet 2/0/1
```

```
[SwitchB-GigabitEthernet2/0/1] port link-type trunk
```

```
[SwitchB-GigabitEthernet2/0/1] port trunk permit vlan 1 2 3 111 211 311
```

开启端口 GigabitEthernet2/0/1 的基本 QinQ 功能。

```
[SwitchB-GigabitEthernet2/0/1] qinq enable
```

```
[SwitchB] quit
```

配置端口 GigabitEthernet2/0/2 允许 CVLAN 和 SVLAN 的报文通过。

```
[SwitchB] interface gigabitethernet 2/0/2
```

```
[SwitchB-GigabitEthernet2/0/2] port link-type trunk
```

```
[SwitchB-GigabitEthernet2/0/2] port trunk permit vlan 1 2 3 112 212 312
```

开启端口 GigabitEthernet2/0/2 的基本 QinQ 功能。

```
[SwitchB-GigabitEthernet2/0/2] qinq enable
```

```
[SwitchB] quit
```

- 配置上行报文映射策略

配置上行策略，将不同用户的不同业务 CVLAN 映射到不同的 SVLAN。配置思路与 SwitchA 上的配置类似，这里不再赘述。

```
[SwitchB] traffic classifier c1
```

```
[SwitchB-classifier-c1] if-match customer-vlan-id 1
```

```
[SwitchB-classifier-c1] traffic classifier c2
```

```
[SwitchB-classifier-c2] if-match customer-vlan-id 2
```

```
[SwitchB-classifier-c2] traffic classifier c3
```

```
[SwitchB-classifier-c3] if-match customer-vlan-id 3
```

```
[SwitchB-classifier-c3] quit
```

```
[SwitchB] traffic behavior b1
```

```
[SwitchB-behavior-b1] remark service-vlan-id 111
```

```
[SwitchB-behavior-b1] traffic behavior b2
```

```
[SwitchB-behavior-b2] remark service-vlan-id 211
```

```
[SwitchB-behavior-b2] traffic behavior b3
```

```
[SwitchB-behavior-b3] remark service-vlan-id 311
```

```
[SwitchB-behavior-b3] traffic behavior b4
```

```
[SwitchB-behavior-b4] remark service-vlan-id 112
```

```
[SwitchB-behavior-b4] traffic behavior b5
```

```
[SwitchB-behavior-b5] remark service-vlan-id 212
```

```
[SwitchB-behavior-b5] traffic behavior b6
```

```
[SwitchB-behavior-b6] remark service-vlan-id 312
```

```
[SwitchB-behavior-b6] quit
```

```
[SwitchB] qos policy p1
```

```
[SwitchB-policy-p1] classifier c1 behavior b1
```

```
[SwitchB-policy-p1] classifier c2 behavior b2
```

```
[SwitchB-policy-p1] classifier c3 behavior b3
```

```
[SwitchB-policy-p1] quit
```

```
[SwitchB] qos policy p2
```

```
[SwitchB-policy-p2] classifier c1 behavior b4
```

```
[SwitchB-policy-p2] classifier c2 behavior b5
[SwitchB-policy-p2] classifier c3 behavior b6
[SwitchB-policy-p2] quit
```

- 配置下行报文映射策略

配置下行策略，将 SVLAN 映射回原来的 CVLAN。配置思路与 SwitchA 上的配置类似，这里不再赘述。

```
[SwitchB] traffic classifier c11
[SwitchB-classifier-c11] if-match service-vlan-id 111
[SwitchB-classifier-c11] traffic classifier c22
[SwitchB-classifier-c22] if-match service-vlan-id 211
[SwitchB-classifier-c22] traffic classifier c33
[SwitchB-classifier-c33] if-match service-vlan-id 311
[SwitchB-classifier-c33] traffic classifier c44
[SwitchB-classifier-c44] if-match service-vlan-id 112
[SwitchB-classifier-c44] traffic classifier c55
[SwitchB-classifier-c55] if-match service-vlan-id 212
[SwitchB-classifier-c55] traffic classifier c66
[SwitchB-classifier-c66] if-match service-vlan-id 312
[SwitchB-classifier-c66] quit
[SwitchB] traffic behavior b11
[SwitchB-behavior-b11] remark customer-vlan-id 1
[SwitchB-behavior-b11] traffic behavior b22
[SwitchB-behavior-b22] remark customer-vlan-id 2
[SwitchB-behavior-b22] traffic behavior b33
[SwitchB-behavior-b33] remark customer-vlan-id 3
[SwitchB-behavior-b33] quit
[SwitchB] qos policy p11
[SwitchB-policy-p11] classifier c11 behavior b11
[SwitchB-policy-p11] classifier c22 behavior b22
[SwitchB-policy-p11] classifier c33 behavior b33
[SwitchB-policy-p11] quit
[SwitchB] qos policy p22
[SwitchB-policy-p22] classifier c44 behavior b11
[SwitchB-policy-p22] classifier c55 behavior b22
[SwitchB-policy-p22] classifier c66 behavior b33
[SwitchB-policy-p22] quit
```

- 在端口上应用 QoS 策略

在端口 GigabitEthernet2/0/1 的入方向应用上行策略 p1。

```
[SwitchB] interface GigabitEthernet 2/0/1
[SwitchB-GigabitEthernet2/0/1] qos apply policy p1 inbound
```

在端口 GigabitEthernet2/0/1 的出方向应用下行策略 p11。

```
[SwitchB-GigabitEthernet2/0/1] qos apply policy p11 outbound
[SwitchB-GigabitEthernet2/0/1] quit
```

在端口 GigabitEthernet2/0/2 的入方向应用上行策略 p2。

```
[SwitchB-GigabitEthernet2/0/2] qos apply policy p2 inbound
```

在端口 GigabitEthernet2/0/2 的出方向应用下行策略 p22。

```
[SwitchB-GigabitEthernet2/0/2] qos apply policy p22 outbound
```

```
[SwitchB-GigabitEthernet2/0/2] quit
```

- 配置上行端口

配置端口 GigabitEthernet2/0/3 允许 SVLAN 的报文通过。

```
[SwitchB] interface gigabitethernet 2/0/3
```

```
[SwitchB-GigabitEthernet2/0/3] port link-type trunk
```

```
[SwitchB-GigabitEthernet2/0/3] port trunk permit vlan 111 211 311 112 212 312
```

(3) 配置 Switch C

- VLAN 和端口的配置

根据楼道交换机发送的报文创建所有对应的 CVLAN，以及根据业务分类映射后的 SVLAN501、502、503，配置过程这里省略。

配置端口 GigabitEthernet2/0/1 允许 CVLAN 和 SVLAN 的报文通过。

```
<SwitchC> system-view
```

```
[SwitchC] interface gigabitethernet 2/0/1
```

```
[SwitchC-GigabitEthernet2/0/1] port link-type trunk
```

```
[SwitchC-GigabitEthernet2/0/1] port trunk permit vlan 101 201 301 102 202 302 501 502 503
```

开启端口 GigabitEthernet2/0/1 的用户侧 QinQ 功能。

```
[SwitchC-GigabitEthernet2/0/1] qinq enable downlink
```

```
[SwitchC-GigabitEthernet2/0/1] quit
```

配置端口 GigabitEthernet2/0/2 允许 CVLAN 和 SVLAN 的报文通过。

```
[SwitchC] interface gigabitethernet 2/0/2
```

```
[SwitchC-GigabitEthernet2/0/2] port link-type trunk
```

```
[SwitchC-GigabitEthernet2/0/2] port trunk permit vlan 111 211 311 112 212 312 501 502 503
```

开启端口 GigabitEthernet2/0/2 的用户侧 QinQ 功能。

```
[SwitchC-GigabitEthernet2/0/2] qinq enable downlink
```

```
[SwitchC-GigabitEthernet2/0/2] quit
```

- DHCP Snooping 和 ARP Detection 的配置

开启 DHCP Snooping 功能。交换机在接收下行报文时，可以通过查找 SVLAN 对应的 DHCP Snooping 表项中的 DHCP 客户端 IP 地址、MAC 地址、以及 CVLAN 的绑定表项，将报文的 SVLAN 修改为原来的 CVLAN。

```
[SwitchC] dhcp-snooping
```

在每个进行映射的 VLAN 上都使能 ARP Detection 功能，以便对 ARP 报文进行 VLAN 映射处理。

```
[SwitchC] vlan 101
```

```
[SwitchC-vlan101] arp detection enable
```

```
[SwitchC-vlan101] vlan 201
```

```
[SwitchC-vlan201] arp detection enable
```

```
[SwitchC-vlan201] vlan 301
```

```
[SwitchC-vlan301] arp detection enable
```

```
[SwitchC-vlan301] vlan 102
```

```
[SwitchC-vlan102] arp detection enable
```

```
[SwitchC-vlan102] vlan 202
```

```
[SwitchC-vlan202] arp detection enable
[SwitchC-vlan202] vlan 302
[SwitchC-vlan302] arp detection enable
[SwitchC-vlan302] vlan 111
[SwitchC-vlan111] arp detection enable
[SwitchC-vlan111] vlan 211
[SwitchC-vlan211] arp detection enable
[SwitchC-vlan211] vlan 311
[SwitchC-vlan311] arp detection enable
[SwitchC-vlan311] vlan 112
[SwitchC-vlan112] arp detection enable
[SwitchC-vlan112] vlan 212
[SwitchC-vlan212] arp detection enable
[SwitchC-vlan212] vlan 312
[SwitchC-vlan312] arp detection enable
[SwitchC-vlan312] vlan 501
[SwitchC-vlan501] arp detection enable
[SwitchC-vlan501] vlan 502
[SwitchC-vlan502] arp detection enable
[SwitchC-vlan502] vlan 503
[SwitchC-vlan503] arp detection enable
[SwitchC-vlan503] quit
```

- 配置上行报文映射策略

配置上行策略，将不同用户的相同业务 VLAN（CVLAN）映射到同一个 VLAN（SVLAN）。

```
[SwitchC] traffic classifier c1
[SwitchC-classifier-c1] if-match customer-vlan-id 101 to 200
[SwitchC-classifier-c1] traffic classifier c2
[SwitchC-classifier-c2] if-match customer-vlan-id 201 to 300
[SwitchC-classifier-c2] traffic classifier c3
[SwitchC-classifier-c3] if-match customer-vlan-id 301 to 400
[SwitchC-classifier-c3] traffic classifier c4
[SwitchC-classifier-c4] if-match customer-vlan-id 111 to 210
[SwitchC-classifier-c4] traffic classifier c5
[SwitchC-classifier-c5] if-match customer-vlan-id 211 to 310
[SwitchC-classifier-c5] traffic classifier c6
[SwitchC-classifier-c6] if-match customer-vlan-id 311 to 410
[SwitchC-classifier-c6] quit
[SwitchC] traffic behavior b1
[SwitchC-behavior-b1] remark service-vlan-id 501
[SwitchC-behavior-b1] traffic behavior b2
[SwitchC-behavior-b2] remark service-vlan-id 502
[SwitchC-behavior-b2] traffic behavior b3
[SwitchC-behavior-b3] remark service-vlan-id 503
[SwitchC-behavior-b3] quit
[SwitchC] qos policy p1
[SwitchC-policy-p1] classifier c1 behavior b1 mode dot1q-tag-manipulation
[SwitchC-policy-p1] classifier c2 behavior b2 mode dot1q-tag-manipulation
```

```
[SwitchC-policy-p1] classifier c3 behavior b3 mode dot1q-tag-manipulation
[SwitchC-policy-p1] classifier c4 behavior b1 mode dot1q-tag-manipulation
[SwitchC-policy-p1] classifier c5 behavior b2 mode dot1q-tag-manipulation
[SwitchC-policy-p1] classifier c6 behavior b3 mode dot1q-tag-manipulation
[SwitchC-policy-p1] quit
```

- 在端口上应用 QoS 策略

在端口 GigabitEthernet2/0/1 的入方向应用上行策略 p1。

```
[SwitchC] interface GigabitEthernet 2/0/1
[SwitchC-GigabitEthernet2/0/1] qos apply policy p1 inbound
[SwitchC-GigabitEthernet2/0/1] quit
```

在端口 GigabitEthernet2/0/2 的入方向应用上行策略 p1。

```
[SwitchC] interface GigabitEthernet 2/0/2
[SwitchC-GigabitEthernet2/0/2] qos apply policy p1 inbound
[SwitchC-GigabitEthernet2/0/2] quit
```

- 配置上行端口

配置端口 GigabitEthernet2/0/3 允许 SVLAN 的报文通过。

```
[SwitchC] interface gigabitethernet 2/0/3
[SwitchC-GigabitEthernet2/0/3] port link-type trunk
[SwitchC-GigabitEthernet2/0/3] port trunk permit vlan 501 502 503
```

配置端口 GigabitEthernet2/0/3 为 DHCP Snooping 信任端口。

```
[SwitchC-GigabitEthernet2/0/3] dhcp-snooping trust
```

配置端口 GigabitEthernet2/0/3 为 ARP 信任端口。

```
[SwitchC-GigabitEthernet2/0/3] arp detection trust
```

开启端口 GigabitEthernet2/0/3 的网络侧 QinQ 功能。

```
[SwitchC-GigabitEthernet2/0/3] qinq enable uplink
```

(4) 配置 Switch D

创建 SVLAN 501、502、503，配置过程这里不再赘述。

使能 DHCP Snooping 功能。

```
<SwitchD> system-view
[SwitchD] dhcp-snooping
```

配置端口 GigabitEthernet2/0/1 允许 SVLAN 的报文通过。

```
[SwitchD] interface gigabitethernet 2/0/1
[SwitchD-GigabitEthernet2/0/1] port link-type trunk
[SwitchD-GigabitEthernet2/0/1] port trunk permit vlan 501 502 503
```

配置端口 GigabitEthernet2/0/1 为信任端口，但为了节省系统资源，不记录客户端 IP 地址和 MAC 地址的绑定关系。

```
[SwitchD-GigabitEthernet2/0/1] dhcp-snooping trust no-user-binding
```

1.1.5 完整配置

- SwitchA 的配置

```
#
```

```
vlan 2 to 3
#
vlan 101 to 102
#
vlan 201 to 202
#
vlan 301 to 302
#
traffic classifier c2 operator and
  if-match customer-vlan-id 2
traffic classifier c3 operator and
  if-match customer-vlan-id 3
traffic classifier c1 operator and
  if-match customer-vlan-id 1
traffic classifier c11 operator and
  if-match service-vlan-id 101
traffic classifier c22 operator and
  if-match service-vlan-id 201
traffic classifier c33 operator and
  if-match service-vlan-id 301
traffic classifier c44 operator and
  if-match service-vlan-id 102
traffic classifier c55 operator and
  if-match service-vlan-id 202
traffic classifier c66 operator and
  if-match service-vlan-id 302
#
traffic behavior b11
  remark customer-vlan-id 1
traffic behavior b22
  remark customer-vlan-id 2
traffic behavior b33
  remark customer-vlan-id 3
traffic behavior b6
  remark service-vlan-id 302
traffic behavior b4
  remark service-vlan-id 102
traffic behavior b2
  remark service-vlan-id 201
traffic behavior tet
traffic behavior b5
  remark service-vlan-id 202
traffic behavior b3
  remark service-vlan-id 301
traffic behavior b1
  remark service-vlan-id 101
#
qos policy p11
```

```

classifier c11 behavior b11
classifier c22 behavior b22
classifier c33 behavior b33
qos policy p22
classifier c44 behavior b11
classifier c55 behavior b22
classifier c66 behavior b33
qos policy p2
classifier c1 behavior b4
classifier c2 behavior b5
classifier c3 behavior b6
qos policy p1
classifier c1 behavior b1
classifier c2 behavior b2
classifier c3 behavior b3
#
interface GigabitEthernet2/0/1
port link-type trunk
port trunk permit vlan 1 to 3 101 201 301
qinq enable
qos apply policy p1 inbound
qos apply policy p11 outbound
#
interface GigabitEthernet2/0/2
port link-type trunk
port trunk permit vlan 1 to 3 102 202 302
qinq enable
qos apply policy p2 inbound
qos apply policy p22 outbound
#
interface GigabitEthernet2/0/3
port link-type trunk
port trunk permit vlan 1 101 to 102 201 to 202 301 to 302

```

- SwitchB 的配置

```

#
vlan 2 to 3
#
vlan 111 to 112
#
vlan 211 to 212
#
vlan 311 to 312
#
traffic classifier c1 operator and
if-match customer-vlan-id 1
traffic classifier c2 operator and
if-match customer-vlan-id 2
traffic classifier c3 operator and

```



```

if-match customer-vlan-id 3
traffic classifier c11 operator and
if-match service-vlan-id 111
traffic classifier c22 operator and
if-match service-vlan-id 211
traffic classifier c33 operator and
if-match service-vlan-id 311
traffic classifier c44 operator and
if-match service-vlan-id 112
traffic classifier c55 operator and
if-match service-vlan-id 212
traffic classifier c66 operator and
if-match service-vlan-id 312
#
traffic behavior b11
remark customer-vlan-id 1
traffic behavior b22
remark customer-vlan-id 2
traffic behavior b33
remark customer-vlan-id 3
traffic behavior b6
remark service-vlan-id 312
traffic behavior b4
remark service-vlan-id 112
traffic behavior b2
remark service-vlan-id 211
traffic behavior tet
traffic behavior b5
remark service-vlan-id 212
traffic behavior b3
remark service-vlan-id 311
traffic behavior b1
remark service-vlan-id 111
#
qos policy p11
classifier c11 behavior b11
classifier c22 behavior b22
classifier c33 behavior b33
qos policy p22
classifier c44 behavior b11
classifier c55 behavior b22
classifier c66 behavior b33
qos policy p2
classifier c1 behavior b4
classifier c2 behavior b5
classifier c3 behavior b6
qos policy p1
classifier c1 behavior b1

```

```

classifier c2 behavior b2
classifier c3 behavior b3
#
interface GigabitEthernet2/0/1
port link-type trunk
port trunk permit vlan 1 to 3 111 211 311
qinq enable
qos apply policy p1 inbound
qos apply policy p11 outbound
#
interface GigabitEthernet2/0/2
port link-type trunk
port trunk permit vlan 1 to 3 112 212 312
qinq enable
qos apply policy p2 inbound
qos apply policy p22 outbound
#
interface GigabitEthernet2/0/3
port link-type trunk
port trunk permit vlan 1 111 to 112 211 to 212 311 to 312

```

- SwitchC 的配置

```

#
dhcp-snooping
#
vlan 101
arp detection enable
#
vlan 102
arp detection enable
#
vlan 111
arp detection enable
#
vlan 112
arp detection enable
#
vlan 201
arp detection enable
#
vlan 202
arp detection enable
#
vlan 211
arp detection enable
#
vlan 212
arp detection enable
#

```

```

vlan 301
  arp detection enable
#
vlan 302
  arp detection enable
#
vlan 311
  arp detection enable
#
vlan 312
  arp detection enable
#
vlan 501
  arp detection enable
#
vlan 502
  arp detection enable
#
vlan 503
  arp detection enable
#
#
traffic classifier c6 operator and
  if-match customer-vlan-id 311 to 410
traffic classifier c4 operator and
  if-match customer-vlan-id 111 to 210
traffic classifier c2 operator and
  if-match customer-vlan-id 201 to 300
traffic classifier c5 operator and
  if-match customer-vlan-id 211 to 310
traffic classifier c3 operator and
  if-match customer-vlan-id 301 to 400
traffic classifier c1 operator and
  if-match customer-vlan-id 101 to 200
#
traffic behavior b2
  remark service-vlan-id 502
traffic behavior b3
  remark service-vlan-id 503
traffic behavior b1
  remark service-vlan-id 501
#
qos policy p1
  classifier c1 behavior b1 mode dot1q-tag-manipulation
  classifier c2 behavior b2 mode dot1q-tag-manipulation
  classifier c3 behavior b3 mode dot1q-tag-manipulation
  classifier c4 behavior b1 mode dot1q-tag-manipulation
  classifier c5 behavior b2 mode dot1q-tag-manipulation

```

```

classifier c6 behavior b3 mode dot1q-tag-manipulation
#
interface GigabitEthernet2/0/1
port link-type trunk
port trunk permit vlan 1 101 to 102 201 to 202 301 to 302 501 to 503
qinq enable downlink
qos apply policy p1 inbound
#
interface GigabitEthernet2/0/2
port link-type trunk
port trunk permit vlan 1 111 to 112 211 to 212 311 to 312 501 to 503
qinq enable downlink
qos apply policy p1 inbound
#
interface GigabitEthernet2/0/3
port link-type trunk
port trunk permit vlan 1 501 to 503
qinq enable uplink
dhcp-snooping trust
arp detection trust

```

- SwichD 的配置

```

#
dhcp-snooping
#
vlan 501 to 503
#
interface GigabitEthernet2/0/1
port link-type trunk
port trunk permit vlan 1 501 to 503
dhcp-snooping trust no-user-binding

```

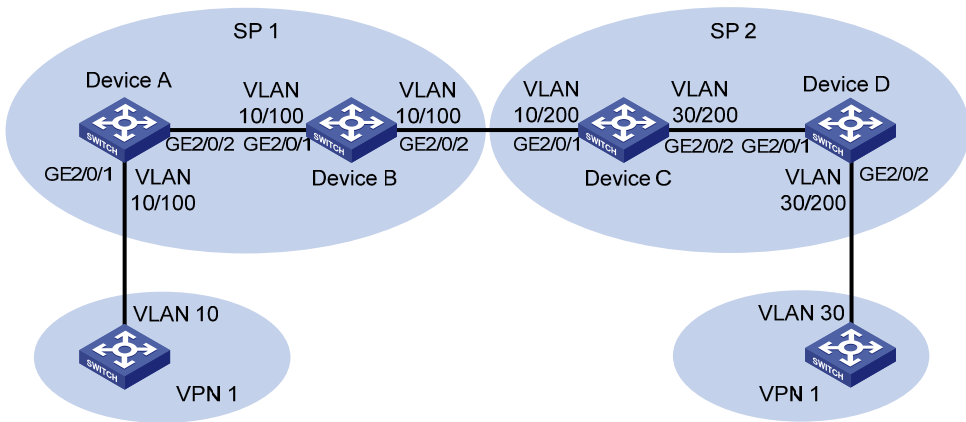
1.1.6 配置注意事项

- 在配置前，需要事先规划好 CVLAN 和 SVLAN 的映射关系。
- 在下行端口上应用策略前，需要先开启端口的用户侧 QinQ 功能；在下行端口上关闭用户侧 QinQ 功能之前，需要先解除 QoS 策略在该端口上的绑定。
- 在 N:1VLAN 映射中，如果用户想要改变 VLAN 映射关系，必须先用 **reset dhcp-snooping** 命令来清除 DHCP Snooping 表项，然后再修改 QoS 策略中的 VLAN 映射关系。
- 在配置 N:1VLAN 映射时，不能在交换机上为 SVLAN 和 CVLAN 创建 VLAN 接口。

1.2 1:2 VLAN 映射和 2:2 VLAN 映射典型配置指导

1.2.1 组网图

图1-2 基于流的灵活 QinQ 组网示意图



1.2.2 应用要求

用户在两地的办公区域之间创建了 VPN1 的连接，两地发送给运营商的报文分别使用 VLAN10 和 VLAN30 的标签。该 VPN 连接在公网中穿越两个 SP（Service Provider，网络服务提供商），现要求在 SP 网络的设备上使用 1:2 VLAN 映射和 2:2 VLAN 映射功能，完成以下的需求：

- 两个 SP 网络均使用两层标签传输用户数据，SP1 为用户分配的外层标签为 VLAN 100，SP2 为用户分配的外层标签为 VLAN200，且数据在穿越两个 SP 网络时标签可以自行修改以适应下一 SP 网络的规划。
- 要求处于不同地域的 VPN1 内的不同 VLAN 之间可以互通。

1.2.3 适用产品、版本

表1-2 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S7500E 系列以太网交换机	Release 6300 版本	全系列硬件版本

1.2.4 配置过程和解释

(1) 配置 Device A

创建 VLAN100。

```
<DeviceA> system-view
[DeviceA] vlan 100
[DeviceA-vlan100] quit
```

配置上行策略，为 VLAN 10 报文添加 VLAN ID 为 100 的外层 VLAN Tag。

```
[DeviceA] traffic classifier nest
[DeviceA-classifier-nest] if-match customer-vlan-id 10
[DeviceA-classifier-nest] quit
[DeviceA] traffic behavior nest
```

```
[DeviceA-behavior-nest] nest top-most vlan-id 100
```

```
[DeviceA-behavior-nest] quit
```

```
[DeviceA] qos policy nest
```

```
[DeviceA-qospolicy-nest] classifier nest behavior nest
```

```
[DeviceA-qospolicy-nest] quit
```

配置端口 GigabitEthernet2/0/1 为 Hybrid 端口，且在发送 VLAN 100 的报文时去掉 VLAN 标签。

```
[DeviceA] interface gigabitethernet 2/0/1
```

```
[DeviceA-GigabitEthernet2/0/1] port link-type hybrid
```

```
[DeviceA-GigabitEthernet2/0/1] port hybrid vlan 100 untagged
```

开启端口 GigabitEthernet2/0/1 的基本 QinQ 功能。

```
[DeviceA-GigabitEthernet2/0/1] qinq enable
```

在端口 GigabitEthernet2/0/1 的入方向应用上行策略 nest。

```
[DeviceA-GigabitEthernet2/0/1] qos apply policy nest inbound
```

```
[DeviceA-GigabitEthernet2/0/1] quit
```

配置上行端口 GigabitEthernet2/0/2 为 Trunk 端口，且允许 VLAN 100 的报文携带 VLAN 标签通过。

```
[DeviceA] interface gigabitethernet 2/0/2
```

```
[DeviceA-GigabitEthernet2/0/2] port link-type trunk
```

```
[DeviceA-GigabitEthernet2/0/2] port trunk permit vlan 100
```

(2) 配置 Device B

创建 VLAN100。

```
<DeviceB> system-view
```

```
[DeviceB] vlan 100
```

```
[DeviceB-vlan100] quit
```

配置端口 GigabitEthernet2/0/1 为 Trunk 端口，且允许 VLAN 100 的报文携带 VLAN 标签通过。

```
[DeviceB] interface gigabitethernet 2/0/1
```

```
[DeviceB-GigabitEthernet2/0/1] port link-type trunk
```

```
[DeviceB-GigabitEthernet2/0/1] port trunk permit vlan 100
```

```
[DeviceB-GigabitEthernet2/0/1] quit
```

配置端口 GigabitEthernet2/0/2 为 Trunk 端口，且允许 VLAN 100 的报文携带 VLAN 标签通过。

```
[DeviceB] interface gigabitethernet 2/0/2
```

```
[DeviceB-GigabitEthernet2/0/2] port link-type trunk
```

```
[DeviceB-GigabitEthernet2/0/2] port trunk permit vlan 100
```

(3) 配置 Device C

创建 VLAN200。

```
<DeviceC> system-view
```

```
[DeviceC] vlan 200
```

```
[DeviceC-vlan200] quit
```

配置端口 GigabitEthernet2/0/1 入方向对报文的分类规则 downlink_in，匹配内层 VLAN 为 10，外层 VLAN 为 100 的报文。

```
[DeviceC] traffic classifier downlink_in
```

```
[DeviceC-classifier-downlink_in] if-match customer-vlan-id 10
```

```
[DeviceC-classifier-downlink_in] if-match service-vlan-id 100
```

```
[DeviceC-classifier-downlink_in] quit
```

配置端口 GigabitEthernet2/0/1 入方向对报文的流行为 downlink_in，将报文的外层 VLAN 替换为 200。

```
[DeviceC] traffic behavior downlink_in
```

```
[DeviceC-behavior-downlink_in] remark service-vlan-id 200
```

```
[DeviceC-behavior-downlink_in] quit
```

配置端口 GigabitEthernet2/0/1 入方向的策略 downlink_in，将入方向的流分类和流行为进行绑定。

```
[DeviceC] qos policy downlink_in
```

```
[DeviceC-qospolicy-downlink_in] classifier downlink_in behavior downlink_in
```

```
[DeviceC-qospolicy-downlink_in] quit
```

配置端口 GigabitEthernet2/0/1 出方向对报文的分类规则 downlink_out，匹配内层 VLAN 为 30，外层 VLAN 为 200 的报文。

```
[DeviceC] traffic classifier downlink_out
```

```
[DeviceC-classifier-downlink_out] if-match customer-vlan-id 30
```

```
[DeviceC-classifier-downlink_out] if-match service-vlan-id 200
```

```
[DeviceC-classifier-downlink_out] quit
```

配置端口 GigabitEthernet2/0/1 出方向对报文的流行为 downlink_out，将报文的内层 VLAN 替换为 10，外层 VLAN 替换为 100。

```
[DeviceC] traffic behavior downlink_out
```

```
[DeviceC-behavior-downlink_out] remark customer-vlan-id 10
```

```
[DeviceC-behavior-downlink_out] remark service-vlan-id 100
```

```
[DeviceC-behavior-downlink_out] quit
```

配置端口 GigabitEthernet2/0/1 出方向的策略 downlink_out，将出方向的流分类和流行为进行绑定。

```
[DeviceC] qos policy downlink_out
```

```
[DeviceC-qospolicy-downlink_out] classifier downlink_out behavior downlink_out
```

```
[DeviceC-qospolicy-downlink_out] quit
```

配置端口 GigabitEthernet2/0/2 出方向对报文的分类规则 uplink_out，匹配内层 VLAN 为 10，外层 VLAN 为 200 的报文。

```
[DeviceC] traffic classifier uplink_out
```

```
[DeviceC-classifier-uplink_out] if-match customer-vlan-id 10
```

```
[DeviceC-classifier-uplink_out] if-match service-vlan-id 200
```

```
[DeviceC-classifier-uplink_out] quit
```

配置端口 GigabitEthernet2/0/2 出方向对报文的流行为 uplink_out，将报文的内层 VLAN 替换为 30。

```
[DeviceC] traffic behavior uplink_out
```

```
[DeviceC-behavior-uplink_out] remark customer-vlan-id 30
```

```
[DeviceC-behavior-uplink_out] quit
```

配置端口 GigabitEthernet2/0/2 出方向的策略 uplink_out，将出方向的流分类和流行为进行绑定。

```
[DeviceC] qos policy uplink_out
```

```
[DeviceC-qospolicy-uplink_out] classifier uplink_out behavior uplink_out
```

```
[DeviceC-qospolicy-uplink_out] quit
```

将策略应用到端口 GigabitEthernet2/0/1 和 GigabitEthernet2/0/2。

```
[DeviceC] interface gigabitethernet 2/0/1
[DeviceB-GigabitEthernet2/0/1] port link-type trunk
[DeviceB-GigabitEthernet2/0/1] port trunk permit vlan 200
[DeviceC-GigabitEthernet2/0/1] qos apply policy downlink_in inbound
[DeviceC-GigabitEthernet2/0/1] qos apply policy downlink_out outbound
[DeviceC-GigabitEthernet2/0/1] quit
[DeviceC] interface gigabitethernet 2/0/2
[DeviceB-GigabitEthernet2/0/2] port link-type trunk
[DeviceB-GigabitEthernet2/0/2] port trunk permit vlan 200
[DeviceC-GigabitEthernet2/0/2] qos apply policy uplink_out outbound
[DeviceC-GigabitEthernet2/0/2] quit
```

(4) 配置 Device D

创建 VLAN200。

```
<DeviceD> system-view
[DeviceD] vlan 200
[DeviceD-vlan200] quit
```

配置上行策略，为 VLAN 30 的报文添加 VLAN ID 为 200 的外层 VLAN Tag。

```
[DeviceD] traffic classifier nest
[DeviceD-classifier-nest] if-match customer-vlan-id 30
[DeviceD-classifier-nest] quit
[DeviceD] traffic behavior nest
[DeviceD-behavior-nest] nest top-most vlan-id 200
[DeviceD-behavior-nest] quit
[DeviceD] qos policy nest
[DeviceD-qospolicy-nest] classifier nest behavior nest
[DeviceD-qospolicy-nest] quit
```

配置端口 GigabitEthernet2/0/1 为 Trunk 端口，且允许 VLAN 200 的报文携带 VLAN 标签通过。

```
[DeviceD] interface gigabitethernet 2/0/1
[DeviceD-GigabitEthernet2/0/1] port link-type trunk
[DeviceD-GigabitEthernet2/0/1] port trunk permit vlan 200
```

配置端口 GigabitEthernet2/0/2 为 Hybrid 端口，且允许 VLAN 200 的报文不带 VLAN 标签通过。

```
[DeviceD] interface gigabitethernet 2/0/2
[DeviceD-GigabitEthernet2/0/2] port link-type hybrid
[DeviceD-GigabitEthernet2/0/2] port hybrid vlan 200 untagged
```

开启端口 GigabitEthernet2/0/2 的基本 QinQ 功能。

```
[DeviceD-GigabitEthernet2/0/2] qinq enable
```

在端口 GigabitEthernet2/0/2 的入方向应用上行策略 nest。

```
[DeviceD-GigabitEthernet2/0/2] qos apply policy nest inbound
[DeviceD-GigabitEthernet2/0/2] quit
```

1.2.5 完整配置

- DeviceA 的配置

#


```

vlan 100
#
traffic classifier nest operator and
if-match customer-vlan-id 10
#
traffic behavior nest
nest top-most vlan-id 100
#
qos policy nest
classifier nest behavior nest
#
interface GigabitEthernet2/0/1
port link-type hybrid
port hybrid vlan 1 100 untagged
qinq enable
qos apply policy nest inbound
#
interface GigabitEthernet2/0/2
port link-type trunk
port trunk permit vlan 1 100

```

- DeviceB 的配置

```

#
vlan 100
#
interface GigabitEthernet2/0/1
port link-type trunk
port trunk permit vlan 1 100
#
interface GigabitEthernet2/0/2
port link-type trunk
port trunk permit vlan 1 100

```

- DeviceC 的配置

```

#
vlan 200
#
traffic classifier uplink_out operator and
if-match customer-vlan-id 10
if-match service-vlan-id 200
traffic classifier downlink_in operator and
if-match customer-vlan-id 10
if-match service-vlan-id 100
traffic classifier downlink_out operator and
if-match customer-vlan-id 30
if-match service-vlan-id 200
#
traffic behavior uplink_out
remark customer-vlan-id 30
traffic behavior downlink_in

```

```

remark service-vlan-id 200
traffic behavior downlink_out
remark customer-vlan-id 10
remark service-vlan-id 100
#
qos policy uplink_out
classifier uplink_out behavior uplink_out
qos policy downlink_in
classifier downlink_in behavior downlink_in
qos policy downlink_out
classifier downlink_out behavior downlink_out
#
interface GigabitEthernet2/0/1
port link-type trunk
port trunk permit vlan 1 200
qos apply policy downlink_in inbound
qos apply policy downlink_out outbound
#
interface GigabitEthernet2/0/2
port link-type trunk
port trunk permit vlan 1 200
qos apply policy uplink_out outbound

```

- DeviceD 的配置

```

#
vlan 100
#
traffic classifier nest operator and
if-match customer-vlan-id 30
#
traffic behavior nest
nest top-most vlan-id 200
#
qos policy nest
classifier nest behavior nest
#
interface GigabitEthernet2/0/1
port link-type trunk
port trunk permit vlan 1 200
#
interface GigabitEthernet2/0/2
port link-type hybrid
port hybrid vlan 1 200 untagged
qinq enable
qos apply policy nest inbound

```

1.2.6 配置注意事项

关于 QoS 策略的更多详细信息，请参见 S7500E 系列以太网交换机操作手册 Release 6300 版本的“QoS 分册”中“QoS”部分的介绍。

目 录

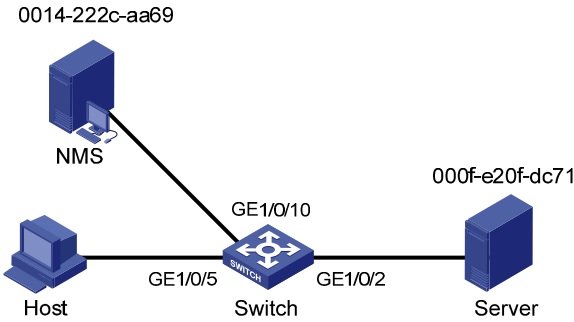
- 1 MAC地址表管理典型配置指导 1-1
 - 1.1 MAC地址表管理典型配置指导 1-1
 - 1.1.1 组网图 1-1
 - 1.1.2 应用要求 1-1
 - 1.1.3 适用产品、版本 1-1
 - 1.1.4 配置过程和解释 1-2
 - 1.1.5 完整配置 1-2
 - 1.1.6 配置注意事项 1-3

1 MAC 地址表管理典型配置指导

1.1 MAC 地址表管理典型配置指导

1.1.1 组网图

图1-1 MAC 地址表管理组网示意图



1.1.2 应用要求

服务器通过 GigabitEthernet1/0/2 端口连接到交换机。为避免交换机在转发目的地址为服务器地址的报文时进行广播，要求在交换机上设置静态的服务器 MAC 地址表项，使交换机始终通过 GigabitEthernet1/0/2 端口单播发送去往服务器的报文。端口 GigabitEthernet1/0/10 连接 NMS（Network Management Server，网管服务器），为增加网络管理的安全性，要求该端口仅允许这台 NMS 接入。

- 服务器的 MAC 地址为 000f-e20f-dc71
- 图中所有端口均属于 VLAN10
- NMS 的 MAC 地址为 0014-222c-aa69
- Switch 的 MAC 地址表项老化时间为 500 秒

1.1.3 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5500-SI 系列以太网交换机	Release 1207 软件版本	全系列硬件版本 (除 S5500-20TP-SI)
	Release 1301 软件版本	S5500-20TP-SI
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6100, Release 6300 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.1.4 配置过程和解释

创建 VLAN10，并将 GigabitEthernet1/0/2、GigabitEthernet1/0/5、GigabitEthernet1/0/10 端口加入 VLAN10。

```
<Sysname> system-view
```

```
[Sysname] vlan 10
```

```
[Sysname-vlan10] port GigabitEthernet1/0/2 GigabitEthernet1/0/5 GigabitEthernet1/0/10
```

添加静态 MAC 地址。

```
[Sysname] mac-address static 000f-e20f-dc71 interface GigabitEthernet 1/0/2 vlan 10
```

设置交换机上动态 MAC 地址表项的老化时间为 500 秒。

```
[Sysname] mac-address timer aging 500
```

在系统视图下查看 MAC 地址配置。

```
[Sysname] display mac-address interface GigabitEthernet 1/0/2
```

MAC ADDR	VLAN ID	STATE	PORT INDEX	AGING TIME(s)
000f-e20f-dc71	1	Config static	GigabitEthernet1/0/2	NOAGED
00e0-fc17-a7d6	1	Learned	GigabitEthernet1/0/2	AGING
00e0-fc5e-b1fb	1	Learned	GigabitEthernet1/0/2	AGING
00e0-fc55-f116	1	Learned	GigabitEthernet1/0/2	AGING

--- 4 mac address(es) found on port GigabitEthernet1/0/2 ---

#通过配置最大 MAC 学习数为 0 与手工添加静态 MAC 表项功能的配合，实现 GigabitEthernet1/0/10 端口只能转发源地址为 NMS 的报文，保证其他主机无法通过此端口通信。

```
[Sysname] interface GigabitEthernet 1/0/10
```

```
[Sysname-GigabitEthernet1/0/10] port access vlan 10
```

```
[Sysname-GigabitEthernet1/0/10] mac-address max-mac-count 0
```

```
[Sysname-GigabitEthernet1/0/10] mac-address static 0014-222c-aa69 vlan 10
```

#配置当端口学习的 MAC 地址数达到设置的最大 MAC 地址数后，禁止转发收到的源 MAC 地址不在 MAC 地址表里的数据帧（S3610、S5510、S3500-EA 三个系列以太网交换机支持此步骤）。

```
[Sysname-GigabitEthernet1/0/10] mac-address max-mac-count disable-forwarding
```

1.1.5 完整配置

```
#  
mac-address timer aging 500  
#  
vlan 10  
#  
interface GigabitEthernet1/0/2  
port access vlan 10  
mac-address static 000f-e20f-dc71 vlan 10  
#  
interface GigabitEthernet1/0/5  
port access vlan 10  
#  
interface GigabitEthernet1/0/10
```

```
port access vlan 10
mac-address max-mac-count 0
mac-address max-mac-count disable-forwarding
mac-address static 0014-222c-aa69 vlan 10
```

1.1.6 配置注意事项

- 除 S7500E 系列以太网交换机 Release 6300 软件版本以外，其它设备及其版本不能在聚合端口上配置静态和动态 MAC 地址表项。
- MAC 地址的老化时间作用于全部端口上，地址老化只对动态的（设备学习到的或者用户配置的动态的）MAC 地址表项起作用。
- S5500-SI、S5500-EI、S7500E 三个系列以太网交换机不支持 **mac-address max-mac-count** 命令中的 **disable-forwarding** 参数，当端口学习的 MAC 地址数达到配置的最大 MAC 地址数后，端口会禁止转发收到的源 MAC 地址不在 MAC 地址表里的数据帧。

目 录

- 1 链路聚合典型配置指导..... 1-1
 - 1.1 链路聚合典型配置指导 1-1
 - 1.1.1 组网图..... 1-1
 - 1.1.2 应用要求 1-1
 - 1.1.3 适用产品、版本 1-1
 - 1.1.4 配置过程和解释 1-2
 - 1.1.5 完整配置 1-3
 - 1.1.6 配置注意事项 1-4

1 链路聚合典型配置指导

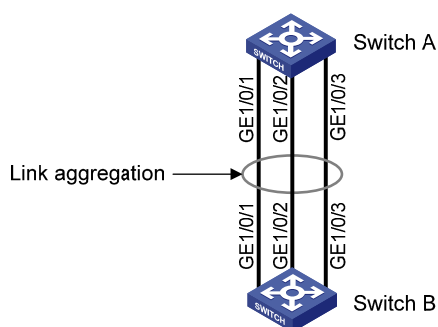
1.1 链路聚合典型配置指导

链路聚合是将多个物理以太网端口聚合在一起形成一个逻辑上的聚合组，使用链路聚合服务的上层实体把同一聚合组内的多条物理链路视为一条逻辑链路。

链路聚合可以实现出/入负荷在聚合组中各个成员端口之间分担，以增加带宽。同时，同一聚合组的各个成员端口之间彼此动态备份，提高了连接可靠性。

1.1.1 组网图

图1-1 链路聚合配置示例图



1.1.2 应用要求

- 设备 Switch A 用 3 个端口聚合接入设备 Switch B，从而实现出/入负荷在各成员端口中分担。
- Switch A 的接入端口为 GigabitEthernet1/0/1～GigabitEthernet1/0/3。

1.1.3 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5500-SI 系列以太网交换机	Release 1207 软件版本	全系列硬件版本 (除 S5500-20TP-SI)
	Release 1301 软件版本	S5500-20TP-SI
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6100, Release 6300 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.1.4 配置过程和解释



说明

以下只列出对 Switch A 的配置，对 Switch B 也需要作相同的配置，才能实现链路聚合。

(1) 配置聚合组，实现端口的负载分担（下面两种方式任选其一）

- 采用手工聚合方式

创建手工聚合组 1。

```
<SwitchA> system-view
```

```
[SwitchA] link-aggregation group 1 mode manual
```

将以太网端口 GigabitEthernet1/0/1 至 GigabitEthernet1/0/3 加入聚合组 1。

```
[SwitchA] interface GigabitEthernet 1/0/1
```

```
[SwitchA-GigabitEthernet1/0/1] port link-aggregation group 1
```

```
[SwitchA-GigabitEthernet1/0/1] interface GigabitEthernet 1/0/2
```

```
[SwitchA-GigabitEthernet1/0/2] port link-aggregation group 1
```

```
[SwitchA-GigabitEthernet1/0/2] interface GigabitEthernet 1/0/3
```

```
[SwitchA-GigabitEthernet1/0/3] port link-aggregation group 1
```

- 采用静态 LACP 聚合方式

创建静态 LACP 聚合组 1。

```
<SwitchA> system-view
```

```
[SwitchA] link-aggregation group 1 mode static
```

将以太网端口 GigabitEthernet1/0/1 至 GigabitEthernet1/0/3 加入聚合组 1。

```
[SwitchA] interface GigabitEthernet 1/0/1
```

```
[SwitchA-GigabitEthernet1/0/1] port link-aggregation group 1
```

```
[SwitchA-GigabitEthernet1/0/1] interface GigabitEthernet 1/0/2
```

```
[SwitchA-GigabitEthernet1/0/2] port link-aggregation group 1
```

```
[SwitchA-GigabitEthernet1/0/2] interface GigabitEthernet 1/0/3
```

```
[SwitchA-GigabitEthernet1/0/3] port link-aggregation group 1
```

S7500E 系列以太网交换机的 Release 6300 软件版本支持链路聚合的配置稍有不同，具体配置聚合组的方式如下：

- 采用静态聚合模式

创建二层聚合端口 1。

```
<SwitchA> system-view
```

```
[SwitchA] interface bridge-aggregation 1
```

```
[SwitchA-Bridge-Aggregation1] quit
```

将以太网端口 GigabitEthernet1/0/1 至 GigabitEthernet1/0/3 加入聚合组 1。

```
[SwitchA] interface GigabitEthernet 1/0/1
```

```
[SwitchA-GigabitEthernet1/0/1] port link-aggregation group 1
```

```
[SwitchA-GigabitEthernet1/0/1] interface GigabitEthernet 1/0/2
```

```
[SwitchA-GigabitEthernet1/0/2] port link-aggregation group 1
```

```
[SwitchA-GigabitEthernet1/0/2] interface GigabitEthernet 1/0/3
```

```
[SwitchA-GigabitEthernet1/0/3] port link-aggregation group 1
```

- 采用动态聚合模式

创建二层聚合端口 1，并配置成动态聚合模式。

```
<SwitchA> system-view
[SwitchA] interface bridge-aggregation 1
[SwitchA-Bridge-Aggregation1] link-aggregation mode dynamic
[SwitchA-Bridge-Aggregation1] quit

# 将以太网端口 GigabitEthernet1/0/1 至 GigabitEthernet1/0/3 加入聚合组 1。

[SwitchA] interface GigabitEthernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] port link-aggregation group 1
[SwitchA-GigabitEthernet1/0/1] interface GigabitEthernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-aggregation group 1
[SwitchA-GigabitEthernet1/0/2] interface GigabitEthernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] port link-aggregation group 1
```

1.1.5 完整配置

(1) 采用手工聚合方式：

```
#
link-aggregation group 1 mode manual

#
interface GigabitEthernet1/0/1
port link-aggregation group 1

#
interface GigabitEthernet1/0/2
port link-aggregation group 1

#
interface GigabitEthernet1/0/3
port link-aggregation group 1

#
```

(2) 采用静态 LACP 聚合方式：

```
#
link-aggregation group 1 mode static
interface GigabitEthernet1/0/1
port link-aggregation group 1

#
interface GigabitEthernet1/0/2
port link-aggregation group 1

#
interface GigabitEthernet1/0/3
port link-aggregation group 1

#
```

S7500E 系列以太网交换机的 Release 6300 软件版本支持链路聚合的配置过程稍有不同，具体配置聚合组的方式如下：

- 采用静态聚合模式

```
#
```

```

interface Bridge-Aggregation1
#
interface GigabitEthernet1/0/1
port link-aggregation group 1
#
interface GigabitEthernet1/0/2
port link-aggregation group 1
#
interface GigabitEthernet1/0/3
port link-aggregation group 1
#

```

- 采用动态聚合模式

```

#
interface Bridge-Aggregation1
link-aggregation mode dynamic
#
interface GigabitEthernet1/0/1
port link-aggregation group 1
#
interface GigabitEthernet1/0/2
port link-aggregation group 1
#
interface GigabitEthernet1/0/3
port link-aggregation group 1
#

```

1.1.6 配置注意事项

- 不同平台软件对静态聚合方式的实现不同，所以不同平台软件的产品采用静态聚合方式对接时，容易产生问题。有关平台软件的版本信息可以通过 **display version** 命令查看。
- 配置了 RRPP 的端口、配置了静态 MAC 地址或者黑洞 MAC 地址的端口、使能 Voice VLAN 的端口以及使能 802.1x 的端口不能加入聚合组。

目 录

1 IP Source Guard典型配置指导	1-1
1.1 IP Source Guard概述	1-1
1.2 静态绑定表项配置指导	1-1
1.2.1 组网图	1-1
1.2.2 应用要求	1-1
1.2.3 适用产品、版本	1-2
1.2.4 配置过程和解释	1-2
1.2.5 完整配置	1-3
1.2.6 配置注意事项	1-3
1.3 动态绑定表项配置指导	1-3
1.3.1 组网图	1-3
1.3.2 应用要求	1-3
1.3.3 适用产品、版本	1-4
1.3.4 配置过程和解释	1-4
1.3.5 完整配置	1-5
1.3.6 配置注意事项	1-5

1 IP Source Guard 典型配置指导

1.1 IP Source Guard 概述

通过 IP Source Guard 绑定功能，可以对端口转发的报文进行过滤控制，防止非法 IP 地址和 MAC 地址的报文通过端口，提高了端口的安全性。端口接收到报文后查找 IP Source Guard 绑定表项，如果报文中的特征项与绑定表项中记录的特征项匹配，则端口转发该报文，否则做丢弃处理。

IP Source Guard 支持的报文特征项包括：源 IP 地址、源 MAC 地址，可支持端口与如下特征项的组合（下文简称绑定表项）：

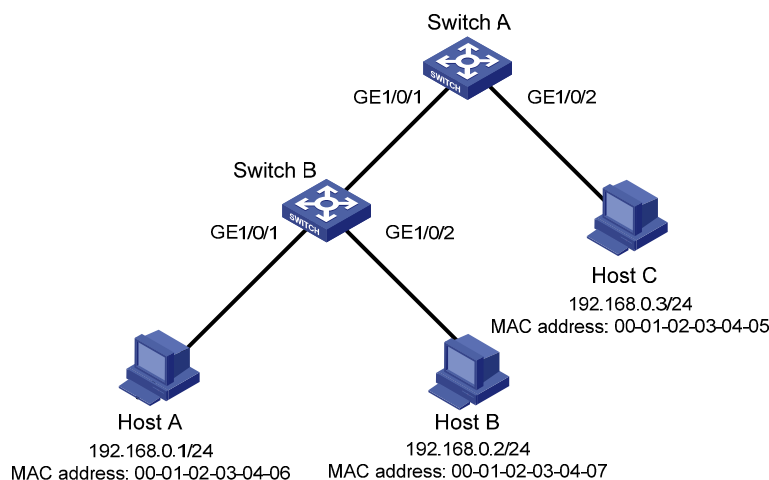
- 源 IP
- 源 MAC
- 源 IP+源 MAC

该特性提供两种绑定机制：一种是通过手工配置方式提供绑定表项，称为静态绑定；另外一种由 DHCP Snooping 提供绑定表项，称为动态绑定。而且，绑定是针对端口的，一个端口被绑定后，仅该端口被限制，其他端口不受该绑定影响。

1.2 静态绑定表项配置指导

1.2.1 组网图

图1-1 静态绑定表项典型配置组网图



1.2.2 应用要求

2 台交换机（Switch A、Switch B）、3 台数据终端（Host A、Host B、Host C）接入到以太网中互相通信。Host A 与 Host B 分别接到 Switch B 的端口 GigabitEthernet1/0/1、GigabitEthernet1/0/2 上；Host C 接到 Switch A 的端口 GigabitEthernet1/0/2 上。Switch B 接到 Switch A 的端口 GigabitEthernet1/0/1 上。

具体应用需求如下：

- 在 Switch A 的 GigabitEthernet1/0/2 上只允许 MAC 地址为 00-01-02-03-04-05 与 IP 地址为 192.168.0.3 的数据终端 Host C 发送的 IP 报文通过。
- Switch A 的 GigabitEthernet1/0/1 上只允许 MAC 地址为 00-01-02-03-04-06 与 IP 地址为 192.168.0.1 的数据终端 Host A 发送的 IP 报文通过。
- 在 Switch B 的 GigabitEthernet1/0/1 上只允许 MAC 地址为 00-01-02-03-04-06 与 IP 地址为 192.168.0.1 的数据终端 Host A 发送的 IP 报文通过。
- 在 Switch B 的 GigabitEthernet1/0/2 上只允许 MAC 地址为 00-01-02-03-04-07 与 IP 地址为 192.168.0.2 的数据终端 Host B 发送的 IP 报文通过。

1.2.3 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301 软件版本, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301 软件版本, Release 5303 软件版本	全系列硬件版本
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6100 软件版本, Release 6300 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.2.4 配置过程和解释

(1) 配置 Switch A

配置各接口的 IP 地址（略）。

配置在 Switch A 的 GigabitEthernet1/0/2 上只允许 MAC 地址为 00-01-02-03-04-05 与 IP 地址为 192.168.0.3 的数据终端 Host C 发送的 IP 报文通过。

```
<SwitchA> system-view
```

```
[SwitchA] interface gigabitethernet 1/0/2
```

```
[SwitchA-GigabitEthernet1/0/2] user-bind ip-address 192.168.0.3 mac-address 0001-0203-0405
```

```
[SwitchA-GigabitEthernet1/0/2] quit
```

配置在 Switch A 的 GigabitEthernet1/0/1 上只允许 MAC 地址为 00-01-02-03-04-06 与 IP 地址为 192.168.0.1 的数据终端 Host A 发送的 IP 报文通过。

```
[SwitchA] interface gigabitethernet 1/0/1
```

```
[SwitchA-GigabitEthernet1/0/1] user-bind ip-address 192.168.0.1 mac-address 0001-0203-0406
```

(2) 配置 Switch B

配置各接口的 IP 地址（略）。

配置在 Switch B 的 GigabitEthernet1/0/1 上只允许 MAC 地址为 00-01-02-03-04-06 与 IP 地址为 192.168.0.1 的数据终端 Host A 发送的 IP 报文通过。

```
<SwitchB> system-view
```

```
[SwitchB] interface gigabitethernet 1/0/1
```

```
[SwitchB-GigabitEthernet1/0/1] user-bind ip-address 192.168.0.1 mac-address 0001-0203-0406
```

```
[SwitchA-GigabitEthernet1/0/1] quit
```

配置在 Switch B 的 GigabitEthernet1/0/2 上只允许 MAC 地址为 00-01-02-03-04-07 与 IP 地址为 192.168.0.2 的数据终端 Host B 发送的 IP 报文通过。

```
[SwitchB] interface gigabitethernet 1/0/2
```

```
[SwitchB-GigabitEthernet1/0/2] user-bind ip-address 192.168.0.2 mac-address 0001-0203-0407
```

1.2.5 完整配置

- SwitchA

```
#
```

```
interface GigabitEthernet1/0/2
```

```
user-bind ip-address 192.168.0.3 mac-address 0001-0203-0405
```

```
#
```

```
interface GigabitEthernet1/0/1
```

```
user-bind ip-address 192.168.0.1 mac-address 0001-0203-0406
```

SwitchB

```
#
```

```
interface GigabitEthernet1/0/1
```

```
user-bind ip-address 192.168.0.1 mac-address 0001-0203-0406
```

```
#
```

```
interface GigabitEthernet1/0/2
```

```
user-bind ip-address 192.168.0.2 mac-address 0001-0203-0407
```

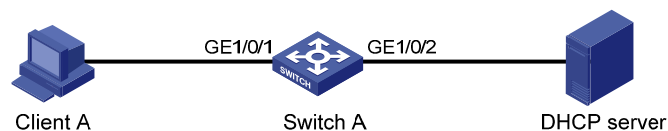
1.2.6 配置注意事项

无。

1.3 动态绑定表项配置指导

1.3.1 组网图

图1-2 动态绑定表项典型配置组网图



1.3.2 应用要求

Switch A 通过端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 分别与客户端 Client A 和 DHCP Server 相连。Switch A 上使能 DHCP Snooping 功能。

具体应用需求如下：

- Client A（MAC 地址为 00-01-02-03-04-06）通过 DHCP Server 获取 IP 地址。
- 在 Switch A 上生成 Client A 的 DHCP Snooping 表项。
- 在端口 GigabitEthernet1/0/1 上启用动态绑定功能，防止客户端使用伪造的不同源 IP 地址对服务器进行攻击。

1.3.3 适用产品、版本

表1-2 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301 软件版本, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301 软件版本, Release 5303 软件版本	全系列硬件版本
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6100 软件版本, Release 6300 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.3.4 配置过程和解释

(1) 配置 Switch A

配置端口 GigabitEthernet1/0/1 的动态绑定功能。

```
<SwitchA> system-view
[SwitchA] interface GigabitEthernet1/0/1
[SwitchA-GigabitEthernet1/0/1] ip check source ip-address mac-address
[SwitchA-GigabitEthernet1/0/1] quit
```

开启 DHCP Snooping 功能。

```
[SwitchA] dhcp-snooping
# 设置与 DHCP 服务器相连的端口 GigabitEthernet1/0/2 为信任端口。
[SwitchA] interface GigabitEthernet1/0/2
[SwitchA-GigabitEthernet1/0/2] dhcp-snooping trust
[SwitchA-GigabitEthernet1/0/2] return
```

(2) 验证配置结果

显示端口 GigabitEthernet1/0/1 从 DHCP Snooping 获取的动态表项。

```
<SwitchA> display ip check source
The following user address bindings have been configured:
MAC                IP                Vlan    Port                Status
0001-0203-0406    192.168.0.1      1       GigabitEthernet1/0/1  DHCP-SNP
-----1 binding entries queried, 1 listed-----
```

显示 DHCP Snooping 已有的动态表项，查看其是否和端口 GigabitEthernet1/0/1 获取的动态表项一致。

```
<SwitchA> display dhcp-snooping
DHCP Snooping is enabled.
The client binding table for all untrusted ports.
Type : D--Dynamic , S--Static
Type IP Address      MAC Address      Lease      VLAN Interface
==== =====
D    192.168.0.1      0001-0203-0406  86335      1    GigabitEthernet1/0/1
```

从以上显示信息可以看出，端口 `GigabitEthernet1/0/1` 在配置动态绑定功能之后获取了 DHCP Snooping 产生的动态表项。

1.3.5 完整配置

```
#
dhcp-snooping
#
interface GigabitEthernet1/0/1
 ip check source ip-address mac-address
#
interface GigabitEthernet1/0/2
 dhcp-snooping trust
```

1.3.6 配置注意事项

- (1) IP Source Guard 功能与端口加入聚合组互斥。
- (2) 当用户同时配置 QoS 策略和 IP Source Guard 功能时，系统只会应用 QoS 策略中定义的流行为。

目 录

1 DLDP典型配置指导	1-1
1.1 DLDP概述	1-1
1.1.1 DLDP简介	1-1
1.2 DLDP配置指导	1-2
1.2.1 组网图	1-2
1.2.2 应用要求	1-2
1.2.3 适用产品、版本	1-2
1.2.4 配置过程和解释	1-2
1.2.5 完整配置	1-4
1.2.6 配置注意事项	1-4

1 DLDP 典型配置指导

1.1 DLDP 概述

1.1.1 DLDP 简介

在实际组网中，有时会出现一种特殊的现象——单向链路（即单通）。所谓单向链路是指本端设备可以通过链路层收到对端设备发送的报文，但对端设备不能收到本端设备的报文。单向链路会引起一系列问题，比如生成树拓扑中存在环路等。

以光纤为例，单向链路分为两种类型：一种是光纤交叉相连，另一种是一条光纤未连接或一条光纤断路。图 1-1 中交叉的光纤表示光纤接反的情况，图 1-2 中空心线表示一条光纤未连接或一条光纤断路的情况。

图1-1 光纤交叉连接

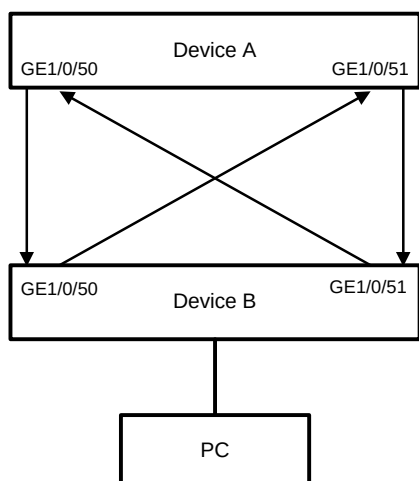
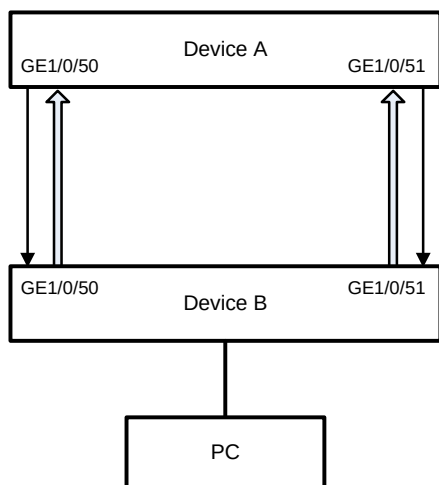


图1-2 一条光纤未连接或一条光纤断路

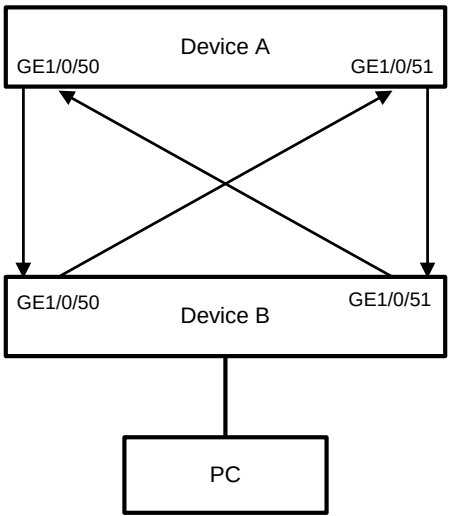


DLDP（Device Link Detection Protocol，设备连接检测协议）可以监控光纤或铜质双绞线的链路状态。如果发现单向链路存在，DLDP 会根据用户配置，自动关闭或通知用户手工关闭相关端口，以防止网络问题的发生。

1.2 DLDP 配置指导

1.2.1 组网图

图1-3 DLDP 典型配置组网图



1.2.2 应用要求

- Device A 和 Device B 通过两对光纤相连，但是出现了光纤接反的情况；
- 要求通过配置达到下列要求：当 DLDP 检测出单向链路后，自动断开单向链路；当网管人员正确连接光纤后，恢复被 DLDP Down 掉的端口。

1.2.3 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301 软件版本，Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301 软件版本，Release 5303 软件版本	全系列硬件版本
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6300 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.2.4 配置过程和解释

(1) 配置 Device A

在端口 GigabitEthernet1/0/50 及 GigabitEthernet1/0/51 使能 DLDP 功能。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/50
[DeviceA-GigabitEthernet1/0/50] dldp enable
[DeviceA-GigabitEthernet1/0/50] quit
[DeviceA] interface gigabitethernet 1/0/51
```

```
[DeviceA-GigabitEthernet1/0/51] dldp enable
```

```
[DeviceA-GigabitEthernet1/0/51] quit
```

配置发送 Advertisement 报文的时间间隔为 6 秒。

```
[DeviceA] dldp interval 6
```

配置 DelayDown 定时器的超时时间为 2 秒。

```
[DeviceA] dldp delaydown-timer 2
```

配置 DLDP 的工作模式为加强模式。

```
[DeviceA] dldp work-mode enhance
```

配置发现单向链路后端口的关闭模式为自动模式。

```
[DeviceA] dldp unidirectional-shutdown auto
```

全局使能 DLDP 功能。

```
[DeviceA] dldp enable
```

查看 DLDP 状态。

```
[DeviceA] display dldp
```

```
DLDP global status : enable
```

```
DLDP interval : 6s
```

```
DLDP work-mode : enhance
```

```
DLDP authentication-mode : none
```

```
DLDP unidirectional-shutdown : auto
```

```
DLDP delaydown-timer : 2s
```

```
The number of enabled ports is 2.
```

```
Interface GigabitEthernet1/0/50
```

```
DLDP port state : disable
```

```
DLDP link state : down
```

```
The neighbor number of the port is 0.
```

```
Interface GigabitEthernet1/0/51
```

```
DLDP port state : disable
```

```
DLDP link state : down
```

```
The neighbor number of the port is 0.
```

从上述显示信息可以看出，端口 GigabitEthernet1/0/50 和 GigabitEthernet1/0/51 均进入 Disable 状态且链路状态也均是 down，表明 DLDP 在这两个端口探测到了单向链路，并且已经将这两个端口关闭。

恢复设备上所有被 DLDP 协议 down 掉的端口。

```
[DeviceA] dldp reset
```

(2) 配置 Device B

Device B 上的配置与 Device A 上的配置完全一致，此处不再赘述。



说明

当光纤交叉连接时，两台设备上的四个端口均处于 Disable 状态。

1.2.5 完整配置

- Device A

```
#
dldp enable
dldp interval 6
dldp work-mode enhance
dldp delaydown-timer 2
#
interface GigabitEthernet1/0/50
dldp enable
#
interface GigabitEthernet1/0/51
dldp enable
```

- Device B

Device B 上的完整配置与 Device A 完全一致，此处不再赘述。

1.2.6 配置注意事项

- (1) 在链路未连通的情况下，DLDP 不起作用，只有当链路连通后，DLDP 才能检测出单向链路，因此在使能 DLDP 之前，请先连接好光纤或铜质双绞线。
- (2) 只有在全局和端口均使能 DLDP 的情况下，才能启动 DLDP 功能、正常地收发 DLDP 报文。
- (3) **dldp interval** 命令配置的时间间隔应该小于 STP 收敛时间的三分之一。如果设定的时间太长，DLDP 在没有关闭单向链路的情况下已出现 STP 环路，并且设备需要经过较长时间才能发现单向链路，可能造成较多的错误流量转发；如果设定的时间太短，会增加网络的流量。因此，此时间间隔建议采用缺省值。
- (4) 如果用户配置了 DLDP 的认证方式，要确保两个通过光纤/铜质双绞线连接的设备配置了相同的 DLDP 认证方式和认证口令，否则 DLDP 不能通过认证。只有通过认证后 DLDP 才能正常工作。
- (5) DLDP 报文使用的目的 MAC 地址分为 A 类和 B 类，这与产品使用的软件版本相关。为保证 DLDP 的正常工作，互连设备需要使用相同类别的目的 MAC 地址。以下表格描述了使用 A 类（使用新的地址）目的 MAC 地址的软件版本，其余软件版本均使用 B 类 MAC 地址。

表1-2 使用 A 类目的 MAC 地址的软件版本

产品系列	使用 A 类目的 MAC 地址的软件版本
S3600 系列以太网交换机	Release 1510P06 及其之后发布的软件版本
S5600 系列以太网交换机	Release 1510P06 及其之后发布的软件版本
S5100 系列以太网交换机	Release 2200 及其之后发布的软件版本
S3610 系列以太网交换机	所有软件版本
S5510 系列以太网交换机	所有软件版本
S5500-EI 系列以太网交换机	所有软件版本

目 录

1 MSTP典型配置指导.....	1-1
1.1 MSTP典型配置指导.....	1-1
1.1.1 组网图.....	1-1
1.1.2 应用要求	1-1
1.1.3 适用产品、版本	1-2
1.1.4 配置过程和解释	1-2
1.1.5 完整配置	1-3
1.1.6 注意事项	1-4
1.2 RSTP配置举例	1-4
1.2.1 组网图.....	1-5
1.2.2 应用要求	1-5
1.2.3 适用产品、版本	1-5
1.2.4 配置过程和解释	1-6
1.2.5 完整配置	1-8
1.2.6 注意事项	1-9

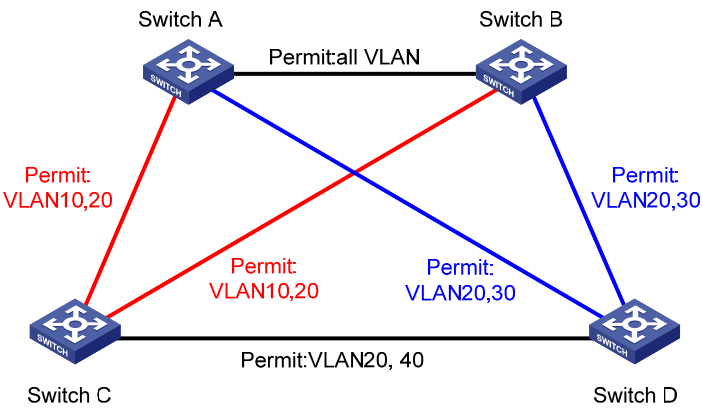
1 MSTP 典型配置指导

1.1 MSTP 典型配置指导

MSTP（Multiple Spanning Tree Protocol，多生成树协议）功能允许用户将一个或者多个 VLAN 映射到 MSTI（Multiple Spanning Tree Instance，多生成树实例）上，但每个 VLAN 只允许对应一个 MSTI。使指定 VLAN 的报文只在建立了映射关系的实例内发送，以节省通信开销和减少资源占用率。

1.1.1 组网图

图1-1 MSTP 配置组网图



VLAN	所属实例
VLAN 10	MSTI 1
VLAN 20	MSTI 0
VLAN 30	MSTI 3
VLAN 40	MSTI 4



说明
图 1-1中链路上的说明“permit:”表示该链路允许哪些VLAN的报文通过。

1.1.2 应用要求

配置MSTP使图 1-1中不同VLAN的报文按照不同的生成树实例转发。具体配置为：

- 网络中所有交换机属于同一个 MST 域；
- VLAN 10 的报文沿着实例 1 转发，VLAN 30 沿着实例 3 转发，VLAN 40 沿着实例 4 转发，VLAN 20 沿着实例 0 转发。

图 1-1中Switch A和Switch B为汇聚层设备，Switch C和Switch D为接入层设备。VLAN 10、VLAN30 在汇聚层设备终结，VLAN 40 在接入层设备终结，因此可以配置实例 1 和实例 3 的树根分别为Switch A和Switch B，实例 4 的树根为Switch C。

1.1.3 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5500-SI 系列以太网交换机	Release 1207 软件版本	全系列硬件版本 (除 S5500-20TP-SI)
	Release 1301 软件版本	S5500-20TP-SI
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6100, Release 6300 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.1.4 配置过程和解释

(1) 配置 Switch A

进入 MST 域视图。

```
<Sysname> system-view
```

```
[Sysname] stp region-configuration
```

配置 MST 域的域名、VLAN 映射关系和修订级别。

```
[Sysname-mst-region] region-name example
```

```
[Sysname-mst-region] instance 1 vlan 10
```

```
[Sysname-mst-region] instance 3 vlan 30
```

```
[Sysname-mst-region] instance 4 vlan 40
```

```
[Sysname-mst-region] revision-level 0
```

手工激活 MST 域的配置。

```
[Sysname-mst-region] active region-configuration
```

定义 Switch A 为实例 1 的树根。

```
[Sysname] stp instance 1 root primary
```

(2) 配置 Switch B

进入 MST 域视图。

```
<Sysname> system-view
```

```
[Sysname] stp region-configuration
```

配置 MST 域的域名、VLAN 映射关系和修订级别。

```
[Sysname-mst-region] region-name example
```

```
[Sysname-mst-region] instance 1 vlan 10
```

```
[Sysname-mst-region] instance 3 vlan 30
```

```
[Sysname-mst-region] instance 4 vlan 40
```

```
[Sysname-mst-region] revision-level 0
```

手工激活 MST 域的配置。

```
[Sysname-mst-region] active region-configuration
```

定义 Switch B 为实例 3 的树根。

```
[Sysname] stp instance 3 root primary
```

(3) 配置 Switch C

进入 MST 域视图，并配置 MST 域名、VLAN 映射关系和修订级别。

```
<Sysname> system-view
```

```
[Sysname] stp region-configuration
```

```
[Sysname-mst-region] region-name example
```

```
[Sysname-mst-region] instance 1 vlan 10
```

```
[Sysname-mst-region] instance 3 vlan 30
```

```
[Sysname-mst-region] instance 4 vlan 40
```

```
[Sysname-mst-region] revision-level 0
```

手工激活 MST 域的配置。

```
[Sysname-mst-region] active region-configuration
```

定义 Switch C 为实例 4 的树根。

```
[Sysname] stp instance 4 root primary
```

(4) 配置 Switch D

进入 MST 域视图。

```
<Sysname> system-view
```

```
[Sysname] stp region-configuration
```

配置 MST 域名、VLAN 映射关系和修订级别。

```
[Sysname-mst-region] region-name example
```

```
[Sysname-mst-region] instance 1 vlan 10
```

```
[Sysname-mst-region] instance 3 vlan 30
```

```
[Sysname-mst-region] instance 4 vlan 40
```

```
[Sysname-mst-region] revision-level 0
```

手工激活 MST 域的配置。

```
[Sysname-mst-region] active region-configuration
```

1.1.5 完整配置

- SwitchA 上的配置

```
#
```

```
stp instance 1 root primary
```

```
(stp enable)
```

```
stp region-configuration
```

```
region-name example
```

```
instance 1 vlan 10
```

```
instance 3 vlan 30
```

```
instance 4 vlan 40
```

```
active region-configuration
```

- SwitchB 上的配置

```
#
```

```

stp instance 3 root primary
(stp enable)
stp region-configuration
region-name example
instance 1 vlan 10
instance 3 vlan 30
instance 4 vlan 40
active region-configuration

```

- SwitchC 上的配置

```

#
stp instance 4 root primary
(stp enable)
stp region-configuration
region-name example
instance 1 vlan 10
instance 3 vlan 30
instance 4 vlan 40
active region-configuration

```

- SwitchD 上的配置

```

#
(stp enable)
stp region-configuration
instance 1 vlan 10
instance 3 vlan 30
instance 4 vlan 40
active region-configuration

```

1.1.6 注意事项

- 不能同时在端口上配置 MSTP 和以下功能：业务环回、RRPP、Smart Link 和 STP 协议的 BPDU Tunnel 功能。
- 只有当两台或者多台交换机的 Format Selector（802.1s 协议规定的协议选择因子，缺省值为 0，不可配置）、MST 域名、VLAN 映射表、MST 域的修订级别完全相同时，它们才能属于同一个 MST 域。
- 在完整配置显示时，部分设备缺省全局开启 STP 功能，这些设备的完整配置中没有 stp enable 项。

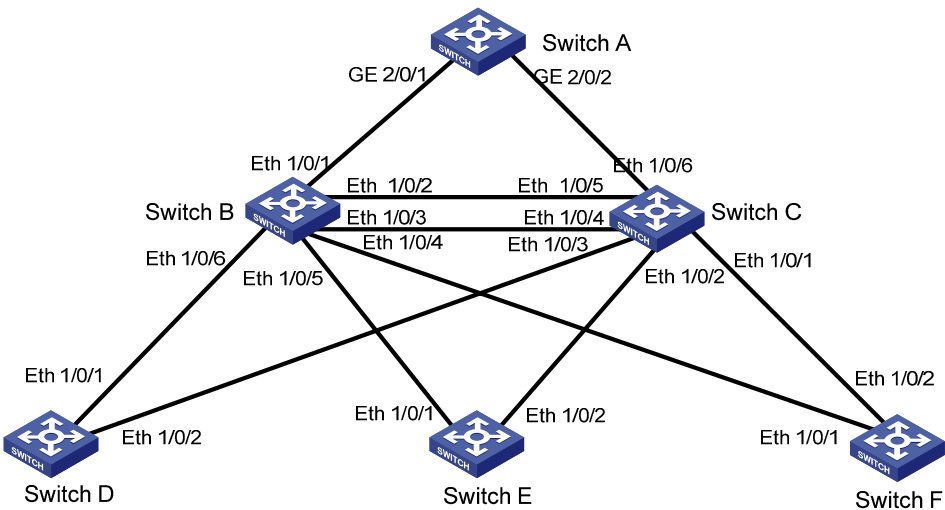
1.2 RSTP 配置举例

RSTP（Rapid Spanning Tree Protocol，快速生成树协议）是 STP 协议的优化版。其“快速”体现在，当一个端口被选为根端口和指定端口后，其进入转发状态的延时在某种条件下大大缩短，从而缩短了网络最终达到拓扑稳定所需要的时间。

RSTP 可以快速收敛，但是和 STP 一样存在以下缺陷：局域网内所有网桥共享一棵生成树，不能按 VLAN 阻塞冗余链路，所有 VLAN 的报文都沿着一棵生成树进行转发。

1.2.1 组网图

图1-2 RSTP 配置组网图



1.2.2 应用要求

- (1) SwitchA 为核心层交换机，作为树根
- (2) Switch B、Switch C 为汇聚层交换机
 - Switch C 为 Switch B 的备份交换机，当 Switch B 出现故障的时候，由 Switch C 转发数据
 - Switch C 和 Switch B 之间通过两条链路相连，保证在一条链路发生故障的时候，另一条可以正常工作
- (3) Switch D、Switch E、Switch F 为接入层交换机
 - Switch D、Switch E、Switch F 下面直接挂接用户的计算机
 - Switch D、Switch E、Switch F 分别通过一个端口与 Switch C、Switch B 相连

在后面的配置步骤中仅列出了 RSTP 相关的配置，由于 Switch D、Switch E 和 Switch F 的 RSTP 配置基本一致，本例只列出了 Switch D 上面的 RSTP 配置。



说明

- Switch A 一般是高中端交换机，如 S7500E 系列交换机。
- Switch B、Switch C 一般为低端交换机中的 S3610 系列、S5500 系列交换机。
- Switch D、Switch E、Switch F 一般为低端交换机中的 S3100 系列、S5100 系列等。

1.2.3 适用产品、版本

表1-2 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本

产品	软件版本	硬件版本
S5500-SI 系列以太网交换机	Release 1207 软件版本	全系列硬件版本 (除 S5500-20TP-SI)
	Release 1301 软件版本	S5500-20TP-SI
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6100, Release 6300 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.2.4 配置过程和解释

(1) Switch A 的配置

设备启动 RSTP。

```
<Sysname> system-view
[Sysname] stp enable
[Sysname] stp mode rstp
```

设备 MSTP 设备启动后, 各个端口的 RSTP 默认为启动状态, 在不参与 RSTP 计算的端口上关闭 MSTP, 注意不要将参与 RSTP 计算的端口 MSTP 关闭。(此处仅列举出 GigabitEthernet 2/0/4)

```
[Sysname] interface GigabitEthernet 2/0/4
[Sysname-GigabitEthernet2/0/4] stp disable
```

配置 Switch A 为树根, 有两种方法:

- 将 Switch A 的 Bridge 优先级配置为 0

```
[Sysname] stp priority 0
```

- 直接使用命令将 Switch A 指定为树根

```
[Sysname] stp root primary
```

在与 Switch B、Switch C 相连的指定端口上启动根保护功能

```
[Sysname] interface GigabitEthernet 2/0/1
[Sysname-GigabitEthernet2/0/1] stp root-protection
[Sysname-GigabitEthernet2/0/1] quit
[Sysname] interface GigabitEthernet 2/0/2
[Sysname-GigabitEthernet2/0/2] stp root-protection
[Sysname-GigabitEthernet2/0/2] quit
```

启动 Switch A 的 TC 防攻击功能。

```
[Sysname] stp tc-protection enable
```

(2) Switch B 的配置

设备启动 RSTP。

```
<Sysname> system-view
[Sysname] stp enable
[Sysname] stp mode rstp
```

MSTP 设备启动后, 各个端口的 RSTP 默认为启动状态, 在不参与 RSTP 计算的端口上关闭 MSTP, 注意不要将参与 RSTP 计算的端口 MSTP 关闭。(此处仅列举出 Ethernet 1/0/8)

```
[Sysname] interface Ethernet 1/0/8
[Sysname-Ethernet1/0/8] stp disable
[Sysname-Ethernet1/0/8] quit
```

配置 Switch B 的 Bridge 优先级配置为 4096。

```
[Sysname] stp priority 4096
```

在各个指定端口上启动根保护功能

```
[Sysname] interface Ethernet 1/0/4
[Sysname-Ethernet1/0/4] stp root-protection
[Sysname-Ethernet1/0/4] quit
[Sysname] interface Ethernet 1/0/5
[Sysname-Ethernet1/0/5] stp root-protection
[Sysname-Ethernet1/0/5] quit
[Sysname] interface Ethernet 1/0/6
[Sysname-Ethernet1/0/6] stp root-protection
[Sysname-Ethernet1/0/6] quit
```

MSTP 的工作模式、时间参数、端口上的参数都采用缺省值。

(3) Switch C 的配置

设备启动 RSTP。

```
<Sysname> system-view
[Sysname] stp enable
[Sysname] stp mode rstp
```

设备的 MSTP 启动后，各个端口的 RSTP 默认为启动状态，在不参与 RSTP 计算的端口上关闭 MSTP，注意不要将参与 RSTP 计算的端口 MSTP 关闭。(此处仅列举出 Ethernet 1/0/8)

```
[Sysname] interface Ethernet 1/0/8
[Sysname-Ethernet1/0/8] stp disable
[Sysname-Ethernet1/0/8] quit
```

配置 Switch C 的 Bridge 优先级配置为 8192，充当 Switch B 的备份交换机。

```
[Sysname] stp priority 8192
```

在各个指定端口上启动根保护功能

```
[Sysname] interface Ethernet 1/0/1
[Sysname-Ethernet1/0/1] stp root-protection
[Sysname-Ethernet1/0/1] quit
[Sysname] interface Ethernet 1/0/2
[Sysname-Ethernet1/0/2] stp root-protection
[Sysname-Ethernet1/0/2] quit
[Sysname] interface Ethernet 1/0/3
[Sysname-Ethernet1/0/3] stp root-protection
[Sysname-Ethernet1/0/3] quit
```

MSTP 的工作模式、时间参数、端口上的参数都采用缺省值。

(4) Switch D 的配置

设备启动 RSTP。

```
<Sysname> system-view
```

```
[Sysname] stp enable
```

```
[Sysname] stp mode rstp
```

设备的 MSTP 启动后，各个端口的 RSTP 默认为启动状态，在不参与 RSTP 计算的端口上关闭 MSTP，注意不要将参与 RSTP 计算的端口 MSTP 关闭。(此处仅列举出 Ethernet 1/0/3)

```
[Sysname] interface Ethernet 1/0/3
```

```
[Sysname-Ethernet1/0/3] stp disable
```

将直接与用户相连的端口配置为边缘端口，并使能 BPDU 保护功能。（此处仅以 Ethernet 1/0/3 为例）

```
[Sysname-Ethernet1/0/3] stp edged-port enable
```

```
[Sysname-Ethernet1/0/3] quit
```

```
[Sysname] stp bpdu-protection
```

MSTP 的工作模式、时间参数、端口的其他参数都采用缺省值。

Swicth E 和 F 的配置同 Swicth D。

1.2.5 完整配置

(1) SwitchA 上的配置

```
#
```

```
stp mode rstp
```

```
stp instance 0 priority 0
```

```
(stp instance 0 root primary)
```

```
stp TC-protection enable
```

```
stp enable
```

```
#
```

```
interface GigabitEthernet2/0/1
```

```
stp root-portection
```

```
#
```

```
interface GigabitEthernet2/0/2
```

```
stp root-portection
```

```
#
```

```
interface GigabitEthernet2/0/4
```

```
stp disable
```

(2) SwitchB 上的配置

```
#
```

```
stp mode rstp
```

```
stp instance 0 priority 4096
```

```
stp enable
```

```
#
```

```
interface Ethernet1/0/4
```

```
stp root-portection
```

```
#
```

```
interface Ethernet1/0/5
```

```
stp root-portection
```

```
#
```

```
interface Ethernet1/0/6
```

```
stp root-portection
```

```
#
```



```
interface Ethernet1/0/8
```

```
stp disable
```

(3) SwitchC 上的配置

```
#
```

```
stp mode rstp
```

```
stp instance 0 priority 8192
```

```
stp enable
```

```
#
```

```
interface Ethernet1/0/1
```

```
stp root-portection
```

```
#
```

```
interface Ethernet1/0/2
```

```
stp root-portection
```

```
#
```

```
interface Ethernet1/0/3
```

```
stp root-portection
```

```
#
```

```
interface Ethernet1/0/8
```

```
stp disable
```

(4) SwitchD 上的配置

```
#
```

```
stp mode rstp
```

```
stp enable
```

```
#
```

```
interface Ethernet1/0/3
```

```
stp disable
```

```
interface Ethernet3/0/5
```

```
stp edged-port enable
```

```
stp bpdu-portection
```

1.2.6 注意事项

stp mode 命令用于设置交换机的 STP 工作模式：STP、RSTP 或 MSTP。缺省工作于 MSTP 模式。

目 录

1 IPv4 路由典型配置指导	1-1
1.1 静态路由典型配置指导	1-1
1.1.1 组网图	1-1
1.1.2 应用要求	1-1
1.1.3 适用产品、版本	1-2
1.1.4 配置过程和解释	1-2
1.1.5 完整配置	1-2
1.1.6 配置注意事项	1-3
1.2 RIP版本典型配置指导	1-4
1.2.1 组网图	1-4
1.2.2 应用要求	1-4
1.2.3 适用产品、版本	1-4
1.2.4 配置过程和解释	1-5
1.2.5 完整配置	1-6
1.2.6 配置注意事项	1-7
1.3 RIP引入外部路由典型配置指导	1-7
1.3.1 组网图	1-7
1.3.2 应用要求	1-7
1.3.3 适用产品、版本	1-7
1.3.4 配置过程和解释	1-7
1.3.5 完整配置	1-9
1.3.6 配置注意事项	1-11
1.4 配置RIP接口附加度量值典型配置指导	1-11
1.4.1 组网图	1-11
1.4.2 应用要求	1-11
1.4.3 适用产品、版本	1-11
1.4.4 配置过程和解释	1-11
1.4.5 完整配置	1-13
1.4.6 配置注意事项	1-15
1.5 配置RIP发布聚合路由典型配置指导	1-15
1.5.1 组网图	1-15
1.5.2 应用要求	1-15
1.5.3 适用产品、版本	1-15
1.5.4 配置过程和解释	1-16
1.5.5 完整配置	1-17
1.5.6 配置注意事项	1-19
1.6 OSPF基本功能典型配置指导	1-19
1.6.1 组网图	1-20
1.6.2 应用要求	1-20
1.6.3 适用产品、版本	1-20
1.6.4 配置过程和解释	1-20
1.6.5 完整配置	1-23

1.6.6 配置注意事项	1-25
1.7 OSPF应用典型配置指导	1-25
1.7.1 组网图	1-25
1.7.2 应用要求	1-25
1.7.3 适用产品、版本	1-26
1.7.4 配置过程和解释	1-26
1.7.5 完整配置	1-28
1.7.6 配置注意事项	1-29
1.8 OSPF发布聚合路由典型配置指导	1-30
1.8.1 组网图	1-30
1.8.2 应用要求	1-30
1.8.3 适用产品、版本	1-30
1.8.4 配置过程和解释	1-30
1.8.5 完整配置	1-32
1.8.6 配置注意事项	1-34
1.9 OSPF的Stub区域典型配置指导	1-35
1.9.1 组网图	1-35
1.9.2 应用要求	1-35
1.9.3 适用产品、版本	1-35
1.9.4 配置过程和解释	1-35
1.9.5 完整配置	1-38
1.9.6 配置注意事项	1-39
1.10 OSPF的NSSA区域典型配置指导	1-40
1.10.1 组网图	1-40
1.10.2 应用要求	1-40
1.10.3 适用产品、版本	1-40
1.10.4 配置过程和解释	1-40
1.10.5 完整配置	1-42
1.10.6 配置注意事项	1-44
1.11 OSPF的DR选择典型配置指导	1-44
1.11.1 组网图	1-44
1.11.2 应用要求	1-44
1.11.3 适用产品、版本	1-45
1.11.4 配置过程和解释	1-45
1.11.5 完整配置	1-49
1.11.6 配置注意事项	1-50
1.12 OSPF虚连接典型配置指导	1-50
1.12.1 组网图	1-51
1.12.2 应用要求	1-51
1.12.3 适用产品、版本	1-51
1.12.4 配置过程和解释	1-51
1.12.5 完整配置	1-53
1.12.6 配置注意事项	1-54
1.13 OSPF GR典型配置指导	1-54
1.13.1 组网图	1-55
1.13.2 应用要求	1-55

1.13.3 适用产品、版本	1-55
1.13.4 配置过程和解释	1-55
1.13.5 完整配置	1-56
1.13.6 配置注意事项	1-57
1.14 路由过滤典型配置指导	1-58
1.14.1 组网图	1-58
1.14.2 应用要求	1-58
1.14.3 适用产品、版本	1-58
1.14.4 配置过程和解释	1-59
1.14.5 完整配置	1-61
1.14.6 配置注意事项	1-63
1.15 IS-IS基本配置典型指导	1-63
1.15.1 组网图	1-64
1.15.2 应用要求	1-64
1.15.3 适用产品、版本	1-64
1.15.4 配置过程和解释	1-64
1.15.5 完整配置	1-68
1.15.6 配置注意事项	1-70
1.16 IS-IS的DIS选择典型配置指导	1-70
1.16.1 组网图	1-70
1.16.2 应用要求	1-71
1.16.3 适用产品、版本	1-71
1.16.4 配置过程和解释	1-71
1.16.5 完整配置	1-75
1.16.6 配置注意事项	1-76
1.17 IS-IS引入外部路由典型配置指导	1-76
1.17.1 组网图	1-76
1.17.2 应用要求	1-76
1.17.3 适用产品、版本	1-77
1.17.4 配置过程和解释	1-77
1.17.5 完整配置	1-80
1.17.6 配置注意事项	1-82
1.18 IS-IS GR典型配置指导	1-82
1.18.1 组网图	1-83
1.18.2 应用要求	1-83
1.18.3 适用产品、版本	1-83
1.18.4 配置过程和解释	1-83
1.18.5 完整配置	1-84
1.18.6 配置注意事项	1-85
1.19 IS-IS验证典型配置指导	1-86
1.19.1 组网图	1-86
1.19.2 应用要求	1-86
1.19.3 适用产品、版本	1-86
1.19.4 配置过程和解释	1-86
1.19.5 完整配置	1-88
1.19.6 配置注意事项	1-90

1.20 BGP基本功能典型配置指导	1-90
1.20.1 组网图	1-91
1.20.2 应用要求	1-91
1.20.3 适用产品、版本	1-91
1.20.4 配置过程和解释	1-91
1.20.5 完整配置	1-94
1.20.6 配置注意事项	1-96
1.21 BGP与IGP交互典型配置指导	1-97
1.21.1 组网图	1-97
1.21.2 应用要求	1-97
1.21.3 适用产品、版本	1-97
1.21.4 配置过程和解释	1-98
1.21.5 完整配置	1-100
1.21.6 配置注意事项	1-101
1.22 BGP负载分担典型配置指导	1-101
1.22.1 组网图	1-102
1.22.2 应用要求	1-102
1.22.3 适用产品、版本	1-102
1.22.4 配置过程和解释	1-102
1.22.5 完整配置	1-104
1.22.6 配置注意事项	1-105
1.23 BGP团体典型配置指导	1-105
1.23.1 组网图	1-106
1.23.2 应用要求	1-106
1.23.3 适用产品、版本	1-106
1.23.4 配置过程和解释	1-106
1.23.5 完整配置	1-108
1.23.6 配置注意事项	1-109
1.24 BGP路由反射器典型配置指导	1-109
1.24.1 组网图	1-110
1.24.2 应用要求	1-110
1.24.3 适用产品、版本	1-110
1.24.4 配置过程和解释	1-110
1.24.5 完整配置	1-112
1.24.6 配置注意事项	1-113
1.25 BGP联盟典型配置指导	1-114
1.25.1 组网图	1-114
1.25.2 应用要求	1-114
1.25.3 适用产品、版本	1-114
1.25.4 配置过程和解释	1-115
1.25.5 完整配置	1-117
1.25.6 配置注意事项	1-120
1.26 BGP路径选择典型配置指导	1-120
1.26.1 组网图	1-121
1.26.2 应用要求	1-121
1.26.3 适用产品、版本	1-121

1.26.4 配置过程和解释	1-121
1.26.5 完整配置	1-124
1.26.6 配置注意事项	1-126
1.27 在IPv4路由引入中应用路由策略典型配置指导	1-126
1.27.1 组网图	1-127
1.27.2 应用要求	1-127
1.27.3 适用产品、版本	1-127
1.27.4 配置过程和解释	1-127
1.27.5 完整配置	1-130
1.27.6 配置注意事项	1-131
1.28 应用路由策略过滤接收的BGP路由典型配置指导	1-132
1.28.1 组网图	1-132
1.28.2 应用要求	1-132
1.28.3 适用产品、版本	1-132
1.28.4 配置过程和解释	1-133
1.28.5 完整配置	1-134
1.28.6 配置注意事项	1-136

1 IPv4 路由典型配置指导

1.1 静态路由典型配置指导

1. 静态路由

静态路由是一种特殊的路由，由管理员手工配置。在组网结构比较简单的网络中，只需配置静态路由就可以实现网络互通。恰当地设置和使用静态路由可以改善网络的性能，并可为重要的网络应用保证带宽。

静态路由的缺点在于：不能自动适应网络拓扑结构的变化，当网络发生故障或者拓扑发生变化后，可能会出现路由不可达，导致网络中断，此时必须由网络管理员手工修改静态路由的配置。

2. 缺省路由

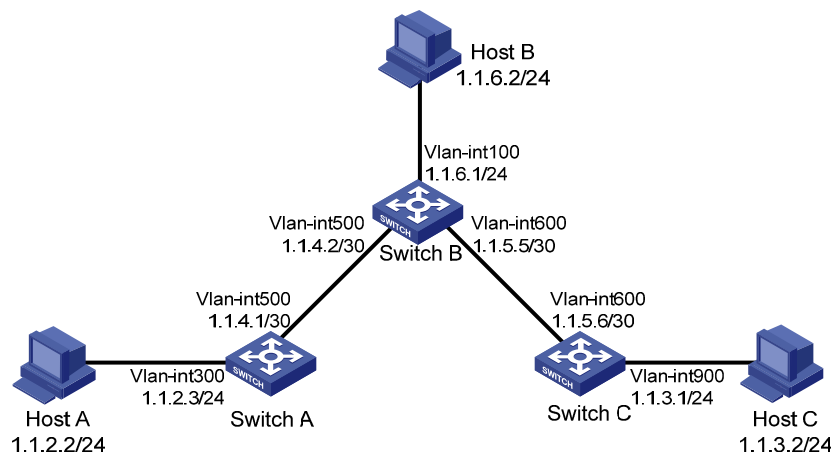
缺省路由是在路由器没有找到匹配的路由表入口项时才使用的路由：

- 如果报文的目的地址不能与路由表的任何入口项相匹配，那么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址不在路由表中，那么该报文将被丢弃，并向源端返回一个 ICMP 报文报告该目的地址或网络不可达。

缺省路由可以通过静态路由配置，以网络 0.0.0.0（掩码也为 0.0.0.0）的形式在路由表中出现，也可以由某些动态路由协议生成，如 OSPF、IS-IS 和 RIP。

1.1.1 组网图

图1-1 静态路由配置组网图



1.1.2 应用要求

路由器各接口及主机的 IP 地址和掩码如上图所示。要求采用静态路由，使图中任意两台主机之间都能互通。

1.1.3 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5500-SI 系列以太网交换机	Release 1207 软件版本	全系列硬件版本 (除 S5500-20TP-SI)
	Release 1301 软件版本	S5500-20TP-SI
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6100, Release 6300 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.1.4 配置过程和解释

- (1) 配置各接口的 IP 地址（略）
- (2) 配置静态路由

在 Switch A 上配置缺省路由。

```
<SwitchA> system-view
[SwitchA] ip route-static 0.0.0.0 0.0.0.0 1.1.4.2
```

在 Switch B 上配置两条静态路由。

```
<SwitchB> system-view
[SwitchB] ip route-static 1.1.2.0 255.255.255.0 1.1.4.1
[SwitchB] ip route-static 1.1.3.0 255.255.255.0 1.1.5.6
```

在 Switch C 上配置缺省路由。

```
<SwitchC> system-view
[SwitchC] ip route-static 0.0.0.0 0.0.0.0 1.1.5.5
```

- (3) 配置主机

配置 Host A 的缺省网关为 1.1.2.3，Host B 的缺省网关为 1.1.6.1，Host C 的缺省网关为 1.1.3.1，具体配置过程略。

1.1.5 完整配置

- 配置 Switch A

```
#
vlan 300
#
vlan 500
#
interface Vlan-interface300
ip address 1.1.2.3 255.255.255.0
```



```

#
interface Vlan-interface500
 ip address 1.1.4.1 255.255.255.252
#
ip route-static 0.0.0.0 0.0.0.0 1.1.4.2
#

```

- 配置 Switch B

```

#
vlan 100
#
vlan 500
#
vlan 600
#
interface Vlan-interface100
 ip address 1.1.6.1 255.255.255.0
#
interface Vlan-interface500
 ip address 1.1.4.2 255.255.255.252
#
interface Vlan-interface600
 ip address 1.1.5.5 255.255.255.252
#
ip route-static 1.1.2.0 255.255.255.0 1.1.4.1
ip route-static 1.1.3.0 255.255.255.0 1.1.5.6
#

```

- 配置 Switch C

```

#
vlan 600
#
vlan 900
#
interface Vlan-interface600
 ip address 1.1.5.6 255.255.255.252
#
interface Vlan-interface900
 ip address 1.1.3.1 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 1.1.5.5
#

```

1.1.6 配置注意事项

- 在配置静态路由时，建议不要直接指定广播类型接口作出接口（如 VLAN 接口等）。因为广播类型的接口，会导致出现多个下一跳，无法唯一确定下一跳。在某些特殊应用中，如果必须配置广播接口（如 VLAN 接口等）为出接口，则必须同时指定其对应的下一跳地址。

- 对于不同的静态路由，可以为它们配置不同的优先级，从而更灵活地应用路由管理策略。例如：配置到达相同目的地的多条路由，如果指定相同优先级，则可实现负载分担，如果指定不同优先级，则可实现路由备份。
- 在配置静态路由时，如果先指定下一跳地址，然后将该地址配置为本地接口（如 VLAN 接口等）的 IP 地址，静态路由不会生效。

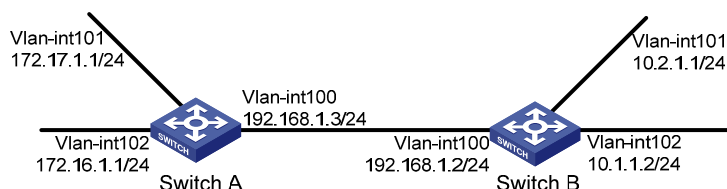
1.2 RIP 版本典型配置指导

RIP（Routing Information Protocol，路由信息协议）是一种较为简单的内部网关协议（Interior Gateway Protocol，IGP），主要用于规模较小的网络中，比如校园网以及结构较简单的地区性网络。对于更为复杂的环境和大型网络，一般不使用 RIP。

由于 RIP 的实现较为简单，在配置和维护管理方面也远比 OSPF 和 IS-IS 容易，因此在实际组网中仍有广泛地应用。

1.2.1 组网图

图1-2 配置 RIP 的版本



1.2.2 应用要求

如上图所示，要求在 Switch A 和 Switch B 的所有接口上使能 RIP，并使用 RIP-2 进行网络互连。

1.2.3 适用产品、版本

表1-2 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5500-SI 系列以太网交换机	Release 1207 软件版本	全系列硬件版本 (除 S5500-20TP-SI)
	Release 1301 软件版本	S5500-20TP-SI
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6100, Release 6300 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.2.4 配置过程和解释

(1) 配置各接口的 IP 地址（略）

(2) 配置 RIP 基本功能

配置 Switch A。

```
<SwitchA> system-view
[SwitchA] rip
[SwitchA-rip-1] network 192.168.1.0
[SwitchA-rip-1] network 172.16.0.0
[SwitchA-rip-1] network 172.17.0.0
[SwitchA-rip-1] quit
```

配置 Switch B。

```
<SwitchB> system-view
[SwitchB] rip
[SwitchB-rip-1] network 192.168.1.0
[SwitchB-rip-1] network 10.0.0.0
[SwitchB-rip-1] quit
```

查看 Switch A 的 RIP 路由表。

```
[SwitchA] display rip 1 route
Route Flags: R - RIP, T - TRIP
                P - Permanent, A - Aging, S - Suppressed, G - Garbage-collect
-----
Peer 192.168.1.2 on Vlan-interface100

```

Destination/Mask	Nexthop	Cost	Tag	Flags	Sec
10.0.0.0/8	192.168.1.2	1	0	RA	11

从路由表中可以看出，RIP-1 发布的路由信息使用的是自然掩码。

(3) 配置 RIP 的版本

在 Switch A 上配置 RIP-2。

```
[SwitchA] rip
[SwitchA-rip-1] version 2
[SwitchA-rip-1] undo summary
```

在 Switch B 上配置 RIP-2。

```
[SwitchB] rip
[SwitchB-rip-1] version 2
[SwitchB-rip-1] undo summary
```

查看 Switch A 的 RIP 路由表。

```
[SwitchA] display rip 1 route
Route Flags: R - RIP, T - TRIP
                P - Permanent, A - Aging, S - Suppressed, G - Garbage-collect
-----
Peer 192.168.1.2 on Vlan-interface100

```

Destination/Mask	Nexthop	Cost	Tag	Flags	Sec
10.2.1.0/24	192.168.1.2	1	0	RA	16
10.1.1.0/24	192.168.1.2	1	0	RA	16

从路由表中可以看出，RIP-2 发布的路由中带有更为精确的子网掩码信息。



说明

由于 RIP 路由信息的老化时间较长，所以在配置 RIP-2 版本后的一段时间里，路由表中可能还会存在 RIP-1 的路由信息。

1.2.5 完整配置

- 配置 Switch A

```
#
vlan 100 to 102
#
interface Vlan-interface100
 ip address 192.168.1.3 255.255.255.0
#
interface Vlan-interface101
 ip address 172.17.1.1 255.255.255.0
#
interface Vlan-interface102
 ip address 172.16.1.1 255.255.255.0
#
rip 1
 undo summary
 version 2
 network 192.168.1.0
 network 172.16.0.0
 network 172.17.0.0
#
```

- 配置 Switch B

```
#
vlan 100 to 102
#
interface Vlan-interface100
 ip address 192.168.1.2 255.255.255.0
#
interface Vlan-interface101
 ip address 10.2.1.1 255.255.255.0
#
interface Vlan-interface102
 ip address 10.1.1.2 255.255.255.0
#
rip 1
 undo summary
 version 2
 network 192.168.1.0
 network 10.0.0.0
#
```

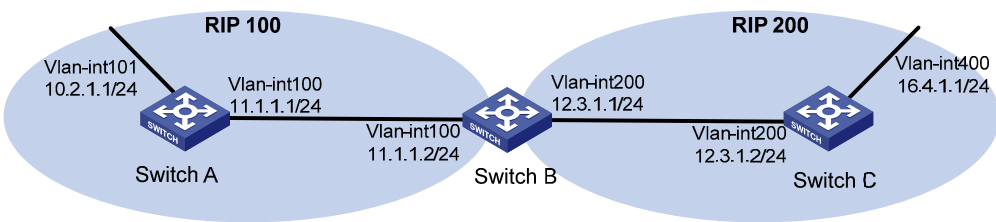
1.2.6 配置注意事项

- S5500-EI 系列交换机的 release 2102 软件版本仅支持 RIP 单进程。
- S5500-SI 系列交换机的 Release 1207 软件版本和 Release 1301 软件版本仅支持 RIP 单进程。
- RIP-2 有两种报文传送方式：广播方式和组播方式，缺省将采用组播方式发送报文，使用的组播地址为 224.0.0.9。当接口运行 RIP-2 广播方式时，也可接收 RIP-1 的报文。
- RIP 只在指定网段的接口上运行；对于不在指定网段上的接口，RIP 既不在它上面接收和发送路由，也不将它的接口路由转发出去。因此，RIP 启动后必须指定其工作网段。

1.3 RIP 引入外部路由典型配置指导

1.3.1 组网图

图1-3 配置 RIP 引入外部路由组网图



1.3.2 应用要求

- Switch B 上运行两个 RIP 进程：RIP100 和 RIP200。Switch B 通过 RIP100 和 Switch A 交换路由信息，通过 RIP200 和 Switch C 交换路由信息。
- 在 Switch B 上配置 RIP 进程 200 引入外部路由，引入直连路由和 RIP 进程 100 的路由，使得 Switch C 能够学习到达 10.2.1.0/24 和 11.1.1.0/24 的路由，但 Switch A 不能学习到达 12.3.1.0/24 和 16.4.1.0/24 的路由。
- 在 Switch B 配置过滤策略，对引入的 RIP100 的一条路由（10.2.1.1/24）进行过滤，使其不发布给 Switch C。

1.3.3 适用产品、版本

表1-3 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6100, Release 6300 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.3.4 配置过程和解释

- (1) 配置各接口的 IP 地址（略）

(2) 配置 RIP 基本功能

在 Switch A 上启动 RIP 进程 100，并配置 RIP 版本号为 2。

```
<SwitchA> system-view
[SwitchA] rip 100
[SwitchA-rip-100] network 10.0.0.0
[SwitchA-rip-100] network 11.0.0.0
[SwitchA-rip-100] version 2
[SwitchA-rip-100] undo summary
[SwitchA-rip-100] quit
```

在 Switch B 上启动两个 RIP 进程，进程号分别为 100 和 200，并配置 RIP 版本号为 2。

```
<SwitchB> system-view
[SwitchB] rip 100
[SwitchB-rip-100] network 11.0.0.0
[SwitchB-rip-100] version 2
[SwitchB-rip-100] undo summary
[SwitchB-rip-100] quit
[SwitchB] rip 200
[SwitchB-rip-200] network 12.0.0.0
[SwitchB-rip-200] version 2
[SwitchB-rip-200] undo summary
[SwitchB-rip-200] quit
```

在 Switch C 上启动 RIP 进程 200，并配置 RIP 版本号为 2。

```
<SwitchC> system-view
[SwitchC] rip 200
[SwitchC-rip-200] network 13.0.0.0
[SwitchC-rip-200] network 16.0.0.0
[SwitchC-rip-200] version 2
[SwitchC-rip-200] undo summary
```

查看 Switch C 的路由表信息。

```
[SwitchC] display ip routing-table
```

Routing Tables: Public

Destinations : 6		Routes : 6			
Destination/Mask	Proto	Pre	Cost	NextHop	Interface
12.3.1.0/24	Direct	0	0	12.3.1.2	Vlan200
12.3.1.2/32	Direct	0	0	127.0.0.1	InLoop0
16.4.1.0/24	Direct	0	0	16.4.1.1	Vlan400
16.4.1.1/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0

(3) 配置 RIP 引入外部路由

在 Switch B 配置 RIP 进程 200 引入外部路由，引入直连路由和 RIP 进程 100 的路由。

```
[SwitchB] rip 200
[SwitchB-rip-200] import-route rip 100
[SwitchB-rip-200] import-route direct
[SwitchB-rip-200] quit
```

查看路由引入后 Switch C 的路由表信息。

```
[SwitchC] display ip routing-table
```

Routing Tables: Public

Destinations : 8		Routes : 8				
Destination/Mask	Proto	Pre	Cost	NextHop	Interface	
10.2.1.0/24	RIP	100	1	12.3.1.1	Vlan200	
11.1.1.0/24	RIP	100	1	12.3.1.1	Vlan200	
12.3.1.0/24	Direct	0	0	12.3.1.2	Vlan200	
12.3.1.2/32	Direct	0	0	127.0.0.1	InLoop0	
16.4.1.0/24	Direct	0	0	16.4.1.1	Vlan400	
16.4.1.1/32	Direct	0	0	127.0.0.1	InLoop0	
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0	
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0	

(4) 配置 RIP 对引入的路由进行过滤

在 Switch B 上配置 ACL，并对引入的 RIP 进程 100 的路由进行过滤，使其不发布给 Switch C。

```
[SwitchB] acl number 2000
```

```
[SwitchB-acl-basic-2000] rule deny source 10.2.1.1 0.0.0.255
```

```
[SwitchB-acl-basic-2000] rule permit
```

```
[SwitchB-acl-basic-2000] quit
```

```
[SwitchB] rip 200
```

```
[SwitchB-rip-100] filter-policy 2000 export rip 100
```

查看过滤后 Switch C 的路由表。

```
[SwitchC] display ip routing-table
```

Routing Tables: Public

Destinations : 7		Routes : 7				
Destination/Mask	Proto	Pre	Cost	NextHop	Interface	
11.1.1.0/24	RIP	100	1	12.3.1.1	Vlan200	
12.3.1.0/24	Direct	0	0	12.3.1.2	Vlan200	
12.3.1.2/32	Direct	0	0	127.0.0.1	InLoop0	
16.4.1.0/24	Direct	0	0	16.4.1.1	Vlan400	
16.4.1.1/32	Direct	0	0	127.0.0.1	InLoop0	
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0	
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0	

1.3.5 完整配置

- 配置 Switch A

```
#
```

```
vlan 100 to 101
```

```
#
```

```
interface Vlan-interface100
```

```
ip address 11.1.1.1 255.255.255.0
```

```
#
```

```
interface Vlan-interface101
```

```
ip address 10.2.1.1 255.255.255.0
```

```

#
rip 100
undo summary
version 2
network 10.0.0.0
network 11.0.0.0
#
• 配置 Switch B
#
acl number 2000
rule 0 deny source 10.2.1.0 0.0.0.255
rule 5 permit
#
vlan 100
#
vlan 200
#
interface Vlan-interface100
ip address 11.1.1.2 255.255.255.0
#
interface Vlan-interface200
ip address 12.3.1.1 255.255.255.0
#
rip 100
undo summary
version 2
network 11.0.0.0
#
rip 200
undo summary
version 2
network 12.0.0.0
filter-policy 2000 export rip 100
import-route direct
import-route rip 100
#
• 配置 Switch C
#
vlan 200
#
vlan 400
#
interface Vlan-interface200
ip address 12.3.1.2 255.255.255.0
#
interface Vlan-interface400
ip address 16.4.1.1 255.255.255.0
#

```



```
rip 200
undo summary
version 2
network 13.0.0.0
network 16.0.0.0
#
```

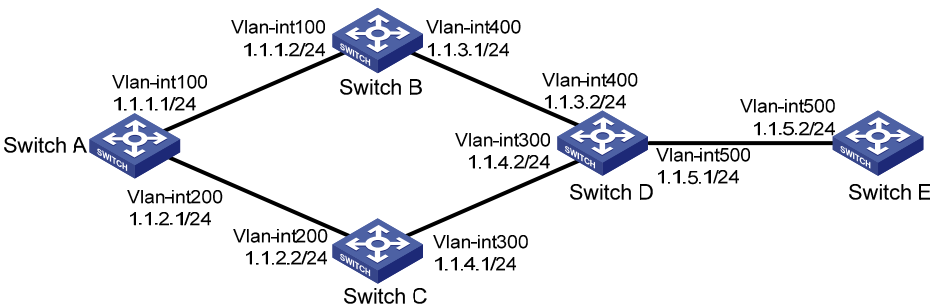
1.3.6 配置注意事项

无

1.4 配置 RIP 接口附加度量值典型配置指导

1.4.1 组网图

图1-4 配置 RIP 接口附加度量值



1.4.2 应用要求

- 在 Switch A、Switch B、Switch C、Switch D 和 Switch E 的所有接口上使能 RIP，并使用 RIP-2 进行网络互连。
- Switch A 有两条链路可以到达 Switch D，其中，通过 Switch B 到达 Switch D 的链路比通过 Switch C 到达 Switch D 的链路更加稳定。通过在 Switch A 的 Vlan-interface200 上配置接口接收 RIP 路由的附加度量值，使得 Switch A 优选从 Switch B 学到的 1.1.5.0/24 网段的路由。

1.4.3 适用产品、版本

表1-4 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6100, Release 6300 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.4.4 配置过程和解释

- (1) 配置各接口的地址（略）

(2) 配置 RIP 基本功能

配置 Switch A。

```
<SwitchA> system-view
[SwitchA] rip 1
[SwitchA-rip-1] network 1.0.0.0
[SwitchA-rip-1] version 2
[SwitchA-rip-1] undo summary
[SwitchA-rip-1] quit
```

配置 Switch B。

```
<SwitchB> system-view
[SwitchB] rip 1
[SwitchB-rip-1] network 1.0.0.0
[SwitchB-rip-1] version 2
[SwitchB-rip-1] undo summary
```

配置 Switch C。

```
<SwitchC> system-view
[SwitchB] rip 1
[SwitchC-rip-1] network 1.0.0.0
[SwitchC-rip-1] version 2
[SwitchC-rip-1] undo summary
```

配置 Switch D。

```
<SwitchD> system-view
[SwitchD] rip 1
[SwitchD-rip-1] network 1.0.0.0
[SwitchD-rip-1] version 2
[SwitchD-rip-1] undo summary
```

配置 Switch E。

```
<SwitchE> system-view
[SwitchE] rip 1
[SwitchE-rip-1] network 1.0.0.0
[SwitchE-rip-1] version 2
[SwitchE-rip-1] undo summary
```

查看 Switch A 的 IP 路由表。

```
[SwitchA] display rip 1 database
  1.0.0.0/8, cost 0, ClassfulSumm
    1.1.1.0/24, cost 0, nexthop 1.1.1.1, Rip-interface
    1.1.2.0/24, cost 0, nexthop 1.1.2.1, Rip-interface
    1.1.3.0/24, cost 1, nexthop 1.1.1.2
    1.1.4.0/24, cost 1, nexthop 1.1.2.2
    1.1.5.0/24, cost 2, nexthop 1.1.1.2
    1.1.5.0/24, cost 2, nexthop 1.1.2.2
```

可以看到，到达网段 1.1.5.0/24 有两条 RIP 路由，下一跳分别是 Switch B（IP 地址为 1.1.1.2）和 Switch C（IP 地址为 1.1.2.2），cost 值都是 2；到达网段 1.1.4.0/24 的下一跳是 Switch B，cost 为 1。

(3) 配置 RIP 接口附加度量值

在 Switch A 上配置接口 Vlan-interface200 的接口附加度量值为 3。

```
[SwitchA] interface vlan-interface 200
[SwitchA-Vlan-interface200] rip metricin 3
[SwitchA-Vlan-interface200] display rip 1 database
  1.0.0.0/8, cost 0, ClassfulSumm
  1.1.1.0/24, cost 0, nexthop 1.1.1.1, Rip-interface
  1.1.2.0/24, cost 0, nexthop 1.1.2.1, Rip-interface
  1.1.3.0/24, cost 1, nexthop 1.1.1.2
  1.1.4.0/24, cost 2, nexthop 1.1.1.2
  1.1.5.0/24, cost 2, nexthop 1.1.1.2
```

可以看到，到达网段 1.1.5.0/24 的 RIP 路由仅有一条，下一跳是 Switch B（IP 地址为 1.1.1.2），cost 值为 2。

1.4.5 完整配置

• 配置 Switch A

```
#
vlan 100
#
vlan 200
#
interface Vlan-interface100
 ip address 1.1.1.1 255.255.255.0
#
interface Vlan-interface200
 ip address 1.1.2.1 255.255.255.0
 rip metricin 3
#
rip 1
 undo summary
 version 2
 network 1.0.0.0
#
```

• 配置 Switch B

```
#
vlan 100
#
vlan 400
#
interface Vlan-interface100
 ip address 1.1.1.2 255.255.255.0
#
interface Vlan-interface400
 ip address 1.1.3.1 255.255.255.0
#
rip 1
```

```
undo summary
version 2
network 1.0.0.0
```

```
#
```

- 配置 Switch C

```
#
```

```
vlan 200
```

```
#
```

```
vlan 300
```

```
#
```

```
interface Vlan-interface200
```

```
ip address 1.1.2.2 255.255.255.0
```

```
#
```

```
interface Vlan-interface300
```

```
ip address 1.1.4.1 255.255.255.0
```

```
#
```

```
rip 1
```

```
undo summary
```

```
version 2
```

```
network 1.0.0.0
```

```
#
```

- 配置 Switch D

```
#
```

```
vlan 300
```

```
#
```

```
vlan 400
```

```
#
```

```
vlan 500
```

```
#
```

```
interface Vlan-interface300
```

```
ip address 1.1.4.2 255.255.255.0
```

```
#
```

```
interface Vlan-interface400
```

```
ip address 1.1.3.2 255.255.255.0
```

```
#
```

```
interface Vlan-interface500
```

```
ip address 1.1.5.1 255.255.255.0
```

```
#
```

```
rip 1
```

```
undo summary
```

```
version 2
```

```
network 1.0.0.0
```

```
#
```

- 配置 Switch E

```
#
```

```
vlan 500
```

```
#
```

```
interface Vlan-interface500
ip address 1.1.5.2 255.255.255.0
#
rip 1
undo summary
version 2
network 1.0.0.0
#
```

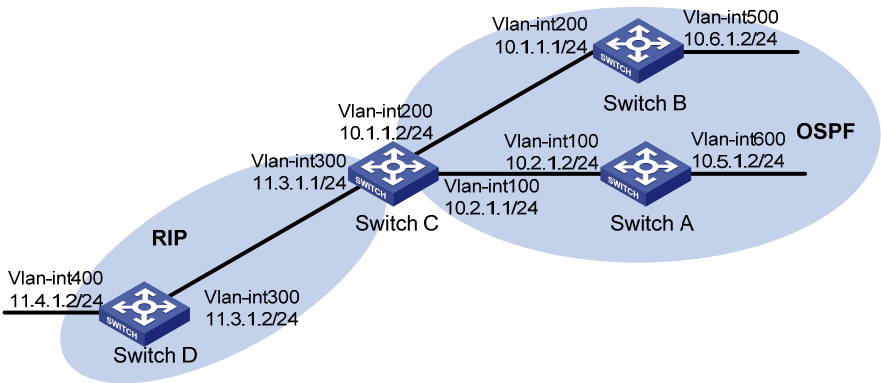
1.4.6 配置注意事项

无

1.5 配置 RIP 发布聚合路由典型配置指导

1.5.1 组网图

图1-5 配置 RIP 发布聚合路由



1.5.2 应用要求

- Switch A、Switch B 运行 OSPF，Switch D 运行 RIP，Switch C 同时运行 OSPF 和 RIP。
- 在 Switch C 上配置 RIP 进程引入 OSPF 路由，使 Switch D 有到达 10.1.1.0/24、10.2.1.0/24、10.5.1.0/24 和 10.6.1.0/24 网段的路由。
- 为了减小 Switch D 的路由表规模，在 Switch C 上配置路由聚合，只发布聚合后的路由 10.0.0.0/8。

1.5.3 适用产品、版本

表1-5 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6100, Release 6300 软件版本	全系列硬件版本

产品	软件版本	硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.5.4 配置过程和解释

(1) 配置各接口的地址（略）

(2) 配置 OSPF 基本功能

配置 Switch A。

```
<SwitchA> system-view
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 10.5.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] network 10.2.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
```

配置 Switch B。

```
<SwitchB> system-view
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] network 10.6.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
```

配置 Switch C。

```
<SwitchC> system-view
[SwitchC] ospf
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] network 10.2.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] quit
```

(3) 配置 RIP 基本功能

配置 Switch C。

```
<SwitchC> system-view
[SwitchC] rip 1
[SwitchC-rip-1] network 11.3.1.0
[SwitchC-rip-1] version 2
[SwitchC-rip-1] undo summary
```

配置 Switch D。

```
<SwitchD> system-view
[SwitchD] rip 1
[SwitchD-rip-1] network 11.0.0.0
[SwitchD-rip-1] version 2
[SwitchD-rip-1] undo summary
[SwitchD-rip-1] quit
```

在 Switch C 上配置 RIP 引入外部路由，引入 OSPF 进程 1 的路由和直连路由。

```
[SwitchC-rip-1] import-route direct
```

```
[SwitchC-rip-1] import-route ospf 1
```

查看 Switch D 的路由表信息。

```
[SwitchD] display ip routing-table
```

```
Routing Tables: Public
```

```
Destinations : 10      Routes : 10
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
10.1.1.0/24	RIP	100	1	11.3.1.1	Vlan300
10.2.1.0/24	RIP	100	1	11.3.1.1	Vlan300
10.5.1.0/24	RIP	100	1	11.3.1.1	Vlan300
10.6.1.0/24	RIP	100	1	11.3.1.1	Vlan300
11.3.1.0/24	Direct	0	0	11.3.1.2	Vlan300
11.3.1.2/32	Direct	0	0	127.0.0.1	InLoop0
11.4.1.0/24	Direct	0	0	11.4.1.2	Vlan400
11.4.1.2/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0

(4) 在 Switch C 上配置路由聚合，只发布聚合路由 10.0.0.0/8。

```
[SwitchC] interface vlan-interface 300
```

```
[SwitchC-Vlan-interface300] rip summary-address 10.0.0.0 8
```

查看 Switch D 的路由表信息。

```
[SwitchD] display ip routing-table
```

```
Routing Tables: Public
```

```
Destinations : 7      Routes : 7
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
10.0.0.0/8	RIP	100	1	11.3.1.1	Vlan300
11.3.1.0/24	Direct	0	0	11.3.1.2	Vlan300
11.3.1.2/32	Direct	0	0	127.0.0.1	InLoop0
11.4.1.0/24	Direct	0	0	11.4.1.2	Vlan400
11.4.1.2/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0

1.5.5 完整配置

- 配置 Switch A

```
#
```

```
vlan 100
```

```
#
```

```
vlan 600
```

```
#
```

```
interface Vlan-interface100
```

```
ip address 10.2.1.2 255.255.255.0
```

```

#
interface Vlan-interface600
 ip address 10.5.1.2 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.5.1.0 0.0.0.255
  network 10.2.1.0 0.0.0.255
#

```

- 配置 Switch B

```

#
vlan 200
#
vlan 500
#
interface Vlan-interface200
 ip address 10.1.1.1 255.255.255.0
#
interface Vlan-interface500
 ip address 10.6.1.2 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 10.6.1.0 0.0.0.255
#

```

- 配置 Switch C

```

#
vlan 100
#
vlan 200
#
vlan 300
#
interface Vlan-interface100
 ip address 10.2.1.1 255.255.255.0
#
interface Vlan-interface200
 ip address 10.1.1.2 255.255.255.0
#
interface Vlan-interface300
 ip address 11.3.1.1 255.255.255.0
 rip summary-address 10.0.0.0 255.0.0.0
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 10.2.1.0 0.0.0.255

```



```

#
rip 1
undo summary
version 2
network 11.0.0.0
import-route direct
import-route ospf 1
#
• 配置 Switch D
#
vlan 300
#
vlan 400
#
interface Vlan-interface300
ip address 11.3.1.2 255.255.255.0
#
interface Vlan-interface400
ip address 11.4.1.2 255.255.255.0
#
rip 1
undo summary
version 2
network 11.0.0.0
#

```

1.5.6 配置注意事项

无

1.6 OSPF 基本功能典型配置指导

OSPF（Open Shortest Path First，开放最短路径优先）是 IETF 组织开发的一个基于链路状态的内部网关协议。目前针对 IPv4 协议使用的是 OSPF Version 2（RFC 2328）。

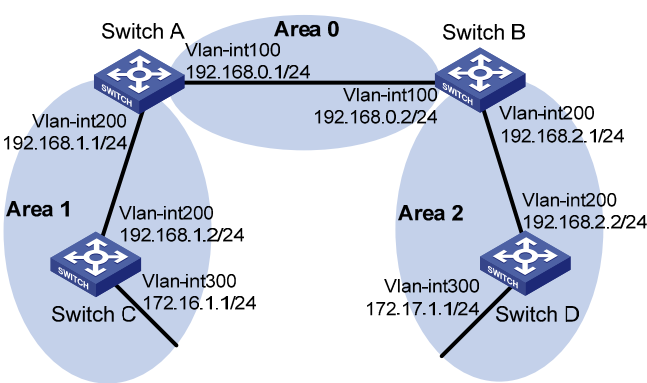
OSPF 具有如下特点：

- 适应范围广——支持各种规模的网络，最多可支持几百台路由器。
- 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，使这一变化在自治系统中同步。
- 无自环——由于 OSPF 根据收集到的链路状态用最短路径树算法计算路由，从算法本身保证了不会生成自环路由。
- 区域划分——允许自治系统的网络被划分成区域来管理，区域间传送的路由信息被进一步抽象，从而减少了占用的网络带宽。
- 等价路由——支持到同一目的地址的多条等价路由。
- 路由分级——使用 4 类不同的路由，按优先顺序来说分别是：区域内路由、区域间路由、第一类外部路由、第二类外部路由。

- 支持验证——支持基于接口的报文验证，以保证报文交互和路由计算的安全性。
- 组播发送——在某些类型的链路上以组播地址发送协议报文，减少对其他设备的干扰。

1.6.1 组网图

图1-6 OSPF 基本配置组网图



1.6.2 应用要求

- 所有的交换机都运行 OSPF，并将整个自治系统划分为 3 个区域。
- 其中 Switch A 和 Switch B 作为 ABR 来转发区域之间的路由。
- 配置完成后，每台交换机都应学到 AS 内的到所有网段的路由。

1.6.3 适用产品、版本

表1-6 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6100, Release 6300 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.6.4 配置过程 and 解释

- (1) 配置各接口的 IP 地址（略）
- (2) 配置 OSPF 基本配置

配置 Switch A。

```

<SwitchA> system-view
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] area 1

```

```
[SwitchA-ospf-1-area-0.0.0.1] network 192.168.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.1] quit
[SwitchA-ospf-1] quit
```

配置 Switch B。

```
<SwitchB> system-view
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] area 2
[SwitchB-ospf-1-area-0.0.0.2] network 192.168.2.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.2] quit
[SwitchB-ospf-1] quit
```

配置 Switch C。

```
<SwitchC> system-view
[SwitchC] ospf
[SwitchC-ospf-1] area 1
[SwitchC-ospf-1-area-0.0.0.1] network 192.168.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.1] network 172.16.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.1] quit
[SwitchC-ospf-1] quit
```

配置 Switch D。

```
<SwitchD> system-view
[SwitchD] ospf
[SwitchD-ospf-1] area 2
[SwitchD-ospf-1-area-0.0.0.2] network 192.168.2.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.2] network 172.17.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.2] quit
[SwitchD-ospf-1] quit
```

(3) 检验配置结果

查看 Switch A 的 OSPF 邻居。

```
[SwitchA] display ospf peer verbose
```

```
OSPF Process 1 with Router ID 192.168.0.1
```

```
Neighbors
```

```
Area 0.0.0.0 interface 192.168.0.1(Vlan-interface 100)'s neighbors
```

```
Router ID: 192.168.0.2      Address: 192.168.0.2      GR State: Normal
```

```
State: Full Mode:Nbr is Master Priority: 1
```

```
DR: 192.168.0.2 BDR: 192.168.0.1 MTU: 0
```

```
Dead timer due in 36 sec
```

```
Neighbor is up for 00:15:04
```

```
Authentication Sequence: [ 0 ]
```

```
Neighbor state change count: 3
```

```
Neighbors
```

```

Area 0.0.0.1 interface 192.168.1.1(Vlan-interface 200)'s neighbors
Router ID: 192.168.1.2      Address: 192.168.1.2      GR State: Normal
State: Full  Mode:Nbr is Slave  Priority: 1
DR: 192.168.1.2  BDR: 192.168.1.1  MTU: 0
Dead timer due in 39 sec
Neighbor is up for 00:07:32
Authentication Sequence: [ 0 ]
Neighbor state change count: 2

```

显示 Switch A 的 OSPF 路由信息。

```
[SwitchA] display ospf routing
```

```

OSPF Process 1 with Router ID 192.168.0.1
Routing Tables

Routing for Network

```

Destination	Cost	Type	NextHop	AdvRouter	Area
172.16.1.0/24	1563	Stub	192.168.1.2	172.16.1.1	0.0.0.1
172.17.1.0/24	3125	Inter-area	192.168.0.2	192.168.2.1	0.0.0.0
192.168.1.0/24	1562	Stub	192.168.1.1	192.168.0.1	0.0.0.1
192.168.2.0/24	3124	Inter-area	192.168.0.2	192.168.2.1	0.0.0.0
192.168.0.0/24	1562	Stub	192.168.0.1	192.168.0.1	0.0.0.0

```

Total Nets: 5
Intra Area: 3  Inter Area: 2  ASE: 0  NSSA: 0

```

显示 Switch A 的 LSDB。

```
[SwitchA] display ospf lsdb
```

```

OSPF Process 1 with Router ID 192.168.0.1
Link State Data Base

Area: 0.0.0.0

```

Type	LinkState ID	AdvRouter	Age	Len	Sequence	Metric
Router	192.168.2.1	192.168.2.1	874	48	80000006	1562
Router	192.168.0.1	192.168.0.1	976	48	80000005	1562
Sum-Net	192.168.1.0	192.168.0.1	630	28	80000001	1562
Sum-Net	172.17.1.0	192.168.2.1	411	28	80000001	1563
Sum-Net	192.168.2.0	192.168.2.1	429	28	80000001	1562
Sum-Net	172.16.1.0	192.168.0.1	565	28	80000001	1563

```

Area: 0.0.0.1

```

Type	LinkState ID	AdvRouter	Age	Len	Sequence	Metric
Router	192.168.1.2	192.168.1.2	964	48	80000003	1562
Router	192.168.0.1	192.168.0.1	590	48	80000002	1562
Router	172.16.1.1	172.16.1.1	526	60	80000005	1562
Sum-Net	172.17.1.0	192.168.0.1	410	28	80000001	3125
Sum-Net	192.168.2.0	192.168.0.1	428	28	80000001	3124

```
Sum-Net 192.168.0.0 192.168.0.1 630 28 80000001 1562
```

查看 Switch D 的路由表。

```
[SwitchD] display ospf routing
```

```
OSPF Process 1 with Router ID 192.168.2.2
```

```
Routing Tables
```

```
Routing for Network
```

Destination	Cost	Type	NextHop	AdvRouter	Area
172.16.1.0/24	4687	Inter-area	192.168.2.1	192.168.2.1	0.0.0.2
172.17.1.0/24	1	Stub	172.17.1.1	192.168.2.2	0.0.0.2
192.168.1.0/24	4686	Inter-area	192.168.2.1	192.168.2.1	0.0.0.2
192.168.2.0/24	1562	Stub	192.168.2.2	192.168.2.2	0.0.0.2
192.168.0.0/24	3124	Inter-area	192.168.2.1	192.168.2.1	0.0.0.2

```
Total Nets: 5
```

```
Intra Area: 2 Inter Area: 3 ASE: 0 NSSA: 0
```

使用 Ping 进行测试连通性。

```
[SwitchD] ping 172.16.1.1
```

```
PING 172.16.1.1: 56 data bytes, press CTRL_C to break
```

```
Reply from 172.16.1.1: bytes=56 Sequence=1 ttl=253 time=62 ms
```

```
Reply from 172.16.1.1: bytes=56 Sequence=2 ttl=253 time=16 ms
```

```
Reply from 172.16.1.1: bytes=56 Sequence=3 ttl=253 time=62 ms
```

```
Reply from 172.16.1.1: bytes=56 Sequence=4 ttl=253 time=94 ms
```

```
Reply from 172.16.1.1: bytes=56 Sequence=5 ttl=253 time=63 ms
```

```
--- 172.16.1.1 ping statistics ---
```

```
5 packet(s) transmitted
```

```
5 packet(s) received
```

```
0.00% packet loss
```

```
round-trip min/avg/max = 16/59/94 ms
```

1.6.5 完整配置

- 配置 Switch A

```
#
```

```
vlan 100
```

```
#
```

```
vlan 200
```

```
#
```

```
interface Vlan-interface100
```

```
ip address 192.168.0.1 255.255.255.0
```

```
#
```

```
interface Vlan-interface200
```

```
ip address 192.168.1.1 255.255.255.0
```

```
#
```

```
ospf 1
```

```
area 0.0.0.0
```

```
network 192.168.0.0 0.0.0.255
```

```

area 0.0.0.1
network 192.168.1.0 0.0.0.255
#
• 配置 Switch B
#
vlan 100
#
vlan 200
#
interface Vlan-interface100
ip address 192.168.0.2 255.255.255.0
#
interface Vlan-interface200
ip address 192.168.2.1 255.255.255.0
#
ospf 1
area 0.0.0.0
network 192.168.0.0 0.0.0.255
area 0.0.0.2
network 192.168.2.0 0.0.0.255
#
• 配置 Switch C
#
vlan 200
#
vlan 300
#
interface Vlan-interface200
ip address 192.168.1.2 255.255.255.0
#
interface Vlan-interface300
ip address 172.16.1.1 255.255.255.0
#
ospf 1
area 0.0.0.1
network 192.168.1.0 0.0.0.255
network 172.16.1.0 0.0.0.255
#
• 配置 Switch D
#
vlan 200
#
vlan 300
#
interface Vlan-interface200
ip address 192.168.2.2 255.255.255.0
#

```

```
interface Vlan-interface300
ip address 172.17.1.1 255.255.255.0
#
ospf 1
area 0.0.0.2
network 192.168.2.0 0.0.0.255
network 172.17.1.0 0.0.0.255
#
```

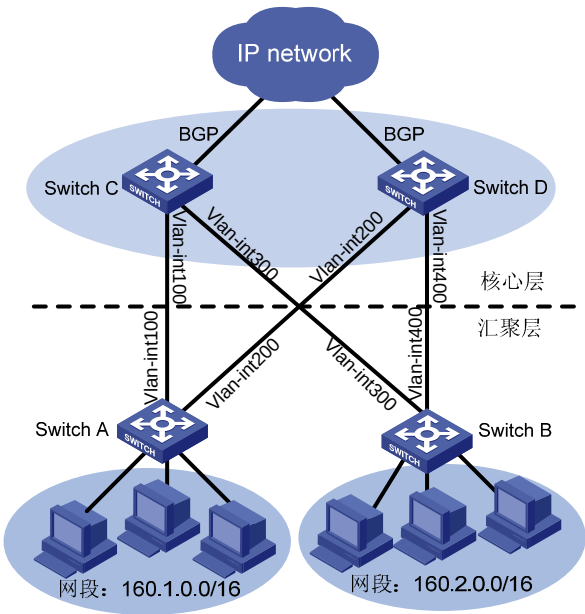
1.6.6 配置注意事项

- S5500-EI 系列交换机的 Release 2102 软件版本仅支持 OSPF 单进程。
- 在 OSPF 的各项配置任务中，必须先启动 OSPF、指定接口和区域号后，才能配置其它的功能特性。
- 一个网段只能属于一个区域，并且必须为每个运行 OSPF 协议的接口指明属于某一个特定的区域。

1.7 OSPF 应用典型配置指导

1.7.1 组网图

图1-7 OSPF 应用典型配置指导



设备	接口	IP 地址	设备	接口	IP 地址
Switch A	Vlan-int100	10.1.1.1/24	Switch C	Vlan-int100	10.1.1.2/24
	Vlan-int200	10.1.2.1/24		Vlan-int300	10.1.3.2/24
Switch B	Vlan-int300	10.1.3.1/24	Switch D	Vlan-int200	10.1.2.2/24
	Vlan-int400	10.1.4.1/24		Vlan-int400	10.1.4.2/24

1.7.2 应用要求

某企业存在多个分支机构，各分支网络通过企业的一级网与外部网络连接。该一级网由四台核心交换机组成，其中两台交换机作为汇聚层设备分别连接各分支网络。两台交换机均为双上行（提供冗余备份链路），上连两台核心交换机负责连接外部网络。实现以下访问需求：

- 汇聚层和核心层交换机之间均采用三层互联，使用 OSPF 路由协议，且均属于区域 0。
- 在汇聚层设备上将去往分支网络的聚合路由（与 Switch A 上下连分支网络均属于 160.1.0.0/16 网段，与 Switch B 上下连分支网络均属于 160.2.0.0/16 网段，）发布到 OSPF 网络，让两台核心层设备能够通过 OSPF 学习到去往分支网络的路由。
- 在核心层交换机上通过 BGP 学习路由，并将 BGP 学到的路由重新注入到 OSPF 网络，最终达到在两台汇聚层交换机上去往外网的路由形成两条等价路由。

1.7.3 适用产品、版本

表1-7 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6100, Release 6300 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.7.4 配置过程 and 解释

本配置举例仅列出与 OSPF 相关内容，有关 BGP 路由学习和引入的内容请参见 BGP 部分。

(1) 配置接口的 IP 地址（略）

(2) 配置 OSPF

配置 Switch A。

```
<SwitchA> system-view
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] network 10.1.2.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] quit
```

配置 Switch B。

```
<SwitchB> system-view
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 10.1.3.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] network 10.1.4.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
```

配置 Switch C。

```
<SwitchC> system-view
[SwitchC] ospf
[SwitchC-ospf-1] area 0
```



```
[SwitchC-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] network 10.1.3.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] quit
[SwitchC-ospf-1] quit
```

配置 Switch D。

```
<SwitchD> system-view
[SwitchD] ospf
[SwitchD-ospf-1] area 0
[SwitchD-ospf-1-area-0.0.0.0] network 10.1.2.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] network 10.1.4.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] quit
[SwitchC-ospf-1] quit
```

查看 Switch A 的路由表信息（假定 Switch A 下连三个分支网络）。

```
[SwitchA] display ip routing-table
Routing Tables: Public
Destinations : 14      Routes : 14
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
10.1.1.0/24	Direct	0	0	10.1.1.1	Vlan100
10.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
10.1.2.0/24	Direct	0	0	10.1.2.1	Vlan200
10.1.2.1/32	Direct	0	0	127.0.0.1	InLoop0
10.1.3.0/24	OSPF	10	2	10.1.1.2	Vlan100
10.1.4.0/24	OSPF	10	2	10.1.2.2	Vlan200
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
160.1.1.0/24	Direct	0	0	160.1.1.1	Vlan1
160.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
160.1.2.0/24	Direct	0	0	160.1.2.1	Vlan2
160.1.2.1/32	Direct	0	0	127.0.0.1	InLoop0
160.1.3.0/24	Direct	0	0	160.1.3.1	Vlan3
160.1.3.1/32	Direct	0	0	127.0.0.1	InLoop0

(3) 配置路由引入

在 Switch A 上配置 OSPF 引入直连路由（一部分分支网络与 Switch A 直连），只发布聚合路由 160.1.0.0/16。

```
[SwitchA] ospf
[SwitchA-ospf-1] import-route direct
[SwitchA-ospf-1] asbr-summary 160.1.0.0 16
```

在 Switch B 上配置 OSPF 引入直连路由（另一部分各分支网络与 Switch B 直连），只发布聚合路由 160.2.0.0/16。

```
[SwitchB] ospf
[SwitchB-ospf-1] import-route direct
[SwitchB-ospf-1] asbr-summary 160.2.0.0 16
```

在 Switch C 上配置 OSPF 引入 BGP 路由。

```
[SwitchC] ospf
[SwitchC-ospf-1] import-route bgp
# 在 Switch D 上配置 OSPF 引入 BGP 路由。
[SwitchD] ospf
[SwitchD-ospf-1] import-route bgp
```

1.7.5 完整配置

- 配置 Switch A

```
#
vlan 100
#
vlan 200
#
interface Vlan-interface100
 ip address 10.1.1.1 255.255.255.0
#
interface Vlan-interface200
 ip address 10.1.2.1 255.255.255.0
#
ospf 1
 asbr-summary 160.1.0.0 255.255.0.0
 import-route direct
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 10.1.2.0 0.0.0.255
#
```

- 配置 Switch B

```
#
vlan 300
#
vlan 400
#
interface Vlan-interface300
 ip address 10.1.3.1 255.255.255.0
#
interface Vlan-interface400
 ip address 10.1.4.1 255.255.255.0
#
ospf 1
 asbr-summary 160.2.0.0 255.255.0.0
 import-route direct
 area 0.0.0.0
  network 10.1.3.0 0.0.0.255
  network 10.1.4.0 0.0.0.255
#
```

- 配置 Switch C

```
#
```

```
vlan 100
#
vlan 300
#
interface Vlan-interface100
 ip address 10.1.1.2 255.255.255.0
#
interface Vlan-interface300
 ip address 10.1.3.2 255.255.255.0
#
ospf 1
 import-route bgp
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 10.1.3.0 0.0.0.255
#
```

- 配置 Switch D

```
#
vlan 200
#
vlan 400
#
interface Vlan-interface200
 ip address 10.1.2.2 255.255.255.0
#
interface Vlan-interface400
 ip address 10.1.4.2 255.255.255.0
#
ospf 1
 import-route bgp
 area 0.0.0.0
  network 10.1.2.0 0.0.0.255
  network 10.1.4.0 0.0.0.255
#
```

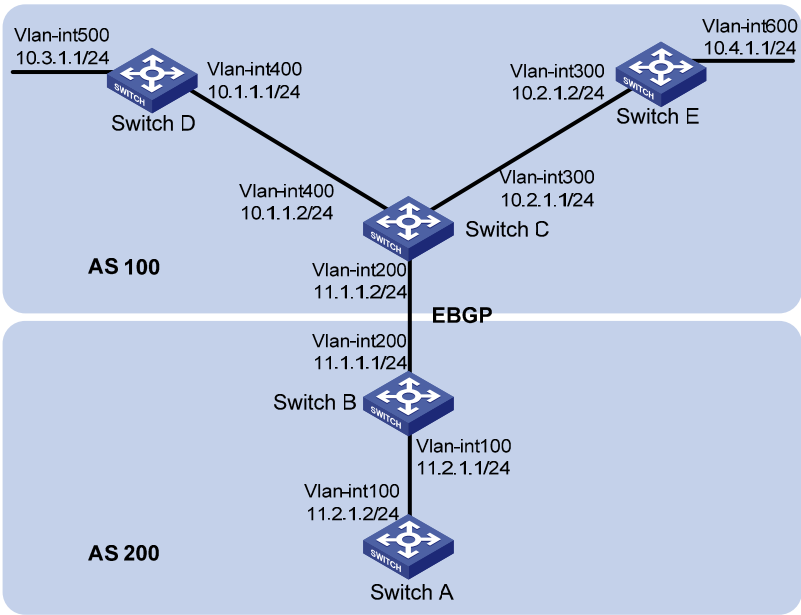
1.7.6 配置注意事项

无

1.8 OSPF 发布聚合路由典型配置指导

1.8.1 组网图

图1-8 配置 OSPF 发布聚合路由



1.8.2 应用要求

- Switch A 和 Switch B 位于 AS200 内，AS200 内使用 OSPF 做为 IGP 协议；
- Switch C、Switch D 和 Switch E 位于 AS100 内，AS100 内使用 OSPF 做为 IGP 协议；
- Switch B 和 Switch C 之间建立 EBGP 连接，在 Router C 上配置 BGP 引入 OSPF 路由；
- 在 Switch B 上配置 OSPF 进程引入 BGP 路由，为了减小 Switch A 的路由表规模，在 Switch B 上配置路由聚合，只发布聚合后的路由 10.0.0.0/8。

1.8.3 适用产品、版本

表1-8 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6100, Release 6300 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.8.4 配置过程和解释

- (1) 配置接口的 IP 地址（略）

(2) 配置 OSPF

配置 Switch A。

```
<SwitchA> system-view
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 11.2.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] quit
```

配置 Switch B。

```
<SwitchB> system-view
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 11.2.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
```

配置 Switch C。

```
<SwitchC> system-view
[SwitchC] ospf
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] network 10.2.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] quit
[SwitchC-ospf-1] quit
```

配置 Switch D。

```
<SwitchD> system-view
[SwitchD] ospf
[SwitchD-ospf-1] area 0
[SwitchD-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] network 10.3.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] quit
```

配置 Switch E。

```
<SwitchE> system-view
[SwitchE] ospf
[SwitchE-ospf-1] area 0
[SwitchE-ospf-1-area-0.0.0.0] network 10.2.1.0 0.0.0.255
[SwitchE-ospf-1-area-0.0.0.0] network 10.4.1.0 0.0.0.255
[SwitchE-ospf-1-area-0.0.0.0] quit
[SwitchE-ospf-1] quit
```

(3) 配置 BGP

配置 Switch B。

```
<SwitchB> system-view
[SwitchB] bgp 200
[SwitchB-bgp] peer 11.1.1.2 as-number 100
[SwitchB-bgp] quit
```

配置 Switch C。

```
<SwitchC> system-view
```

```
[SwitchC] bgp 100
```

```
[SwitchC-bgp] peer 11.1.1.1 as-number 200
```

```
[SwitchC-bgp] import-route ospf
```

(4) 在 Switch B 上配置路由引入

在 Switch B 上配置 OSPF 引入 BGP 路由

```
[SwitchB] ospf
```

```
[SwitchB-ospf-1] import-route bgp
```

查看 Switch A 的路由表信息。

```
[SwitchA] display ip routing-table
```

Routing Tables: Public

Destinations : 8 Routes : 8

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
10.1.1.0/24	O_ASE	150	1	11.2.1.1	Vlan100
10.2.1.0/24	O_ASE	150	1	11.2.1.1	Vlan100
10.3.1.0/24	O_ASE	150	1	11.2.1.1	Vlan100
10.4.1.0/24	O_ASE	150	1	11.2.1.1	Vlan100
11.2.1.0/24	Direct	0	0	11.2.1.2	Vlan100
11.2.1.2/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0

(5) 在 Switch B 上配置路由聚合，只发布聚合路由 10.0.0.0/8。

```
[SwitchB-ospf-1] asbr-summary 10.0.0.0 8
```

查看 Switch A 的路由表信息。

```
[SwitchA] display ip routing-table
```

Routing Tables: Public

Destinations : 5 Routes : 5

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
10.0.0.0/8	O_ASE	150	2	11.2.1.1	Vlan100
11.2.1.0/24	Direct	0	0	11.2.1.2	Vlan100
11.2.1.2/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0

1.8.5 完整配置

- 配置 Switch A

```
#
```

```
vlan 100
```

```
#
```

```
interface Vlan-interface100
```

```
ip address 11.2.1.2 255.255.255.0
```

```
#
```

```

ospf 1
 area 0.0.0.0
  network 11.2.1.0 0.0.0.255
#
• 配置 Switch B
#
vlan 100
#
vlan 200
#
interface Vlan-interface100
 ip address 11.2.1.1 255.255.255.0
#
interface Vlan-interface200
 ip address 11.1.1.1 255.255.255.0
#
bgp 200
 undo synchronization
 peer 11.1.1.2 as-number 100
#
ospf 1
 asbr-summary 10.0.0.0 255.0.0.0
 import-route bgp
 area 0.0.0.0
  network 11.2.1.0 0.0.0.255
#
• 配置 Switch C
#
vlan 200
#
vlan 300
#
vlan 400
#
interface Vlan-interface200
 ip address 11.1.1.2 255.255.255.0
#
interface Vlan-interface300
 ip address 10.2.1.1 255.255.255.0
#
interface Vlan-interface400
 ip address 10.1.1.2 255.255.255.0
#
bgp 100
 import-route ospf 1
 undo synchronization
 peer 11.1.1.1 as-number 200
#

```

```

ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 10.2.1.0 0.0.0.255
#
• 配置 Switch D
#
vlan 400
#
vlan 500
#
interface Vlan-interface400
 ip address 10.1.1.1 255.255.255.0
#
interface Vlan-interface500
 ip address 10.3.1.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 10.3.1.0 0.0.0.255
#
• 配置 Switch E
#
vlan 300
#
vlan 600
#
interface Vlan-interface300
 ip address 10.2.1.2 255.255.255.0
#
interface Vlan-interface600
 ip address 10.4.1.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.2.1.0 0.0.0.255
  network 10.4.1.0 0.0.0.255
#

```

1.8.6 配置注意事项

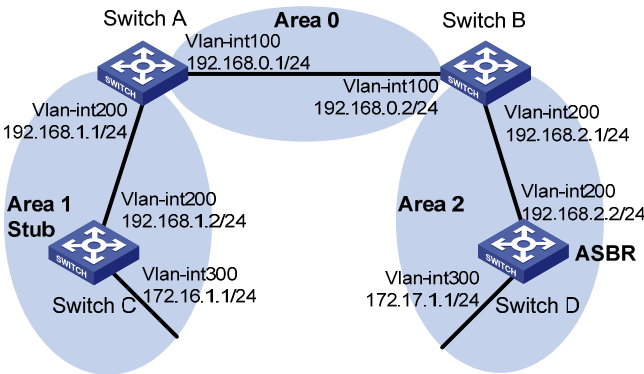
无

1.9 OSPF 的 Stub 区域典型配置指导

OSPF 划分区域后，可以减少网络中 LSA 的数量，OSPF 的扩展性也得以增强。对于位于 AS 边缘的一些非骨干区域，为了更多的缩减其路由表规模和降低 LSA 的数量，可以将它们配置为 Stub 区域。

1.9.1 组网图

图1-9 配置 OSPF Stub 区域组网图



1.9.2 应用要求

- 所有的交换机都运行 OSPF，整个自治系统划分为 3 个区域。
- 其中 Switch A 和 Switch B 作为 ABR 来转发区域之间的路由，Switch D 作为 ASBR 引入了外部路由（静态路由）。
- 要求将 Area1 配置为 Stub 区域，减少通告到此区域内的 LSA 数量，但不影响路由的可达性。

1.9.3 适用产品、版本

表1-9 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6100, Release 6300 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.9.4 配置过程和解释

- (1) 配置接口的 IP 地址（略）
- (2) 配置 OSPF（同前例 1.6 ）
- (3) 配置 Switch D 引入静态路由

```
[SwitchD] ip route-static 200.0.0.0 8 null 0
```

```
[SwitchD] ospf
```

```
[SwitchD-ospf-1] import-route static
```

```
[SwitchD-ospf-1] quit
```

查看 Switch C 的 ABR/ASBR 信息。

```
[SwitchC] display ospf abr-asbr
```

```
OSPF Process 1 with Router ID 172.16.1.1
```

```
Routing Table to ABR and ASBR
```

Type	Destination	Area	Cost	NextHop	RtType
Intra-area	192.168.0.1	0.0.0.1	1562	192.168.1.1	ABR
Inter-area	172.17.1.1	0.0.0.1	4686	192.168.1.1	ASBR

查看 Switch C 的 OSPF 路由表。

```
[SwitchC] display ospf routing
```

```
OSPF Process 1 with Router ID 172.16.1.1
```

```
Routing Tables
```

```
Routing for Network
```

Destination	Cost	Type	NextHop	AdvRouter	Area
172.16.1.0/24	1	Stub	172.16.1.1	172.16.1.1	0.0.0.1
172.17.1.0/24	4687	Inter-area	192.168.1.1	192.168.0.1	0.0.0.1
192.168.1.0/24	1562	Stub	192.168.1.2	172.16.1.1	0.0.0.1
192.168.2.0/24	4686	Inter-area	192.168.1.1	192.168.0.1	0.0.0.1
192.168.0.0/24	3124	Inter-area	192.168.1.1	192.168.0.1	0.0.0.1

```
Routing for ASEs
```

Destination	Cost	Type	Tag	NextHop	AdvRouter
200.0.0.0/8	10	Type2	1	192.168.1.1	172.17.1.1

```
Routing for NSSAs
```

Destination	Cost	Type	Tag	NextHop	AdvRouter

```
Total Nets: 6
```

```
Intra Area: 2 Inter Area: 3 ASE: 1 NSSA: 0
```



说明

当 Switch C 所在区域为普通区域时，可以看到路由表中存在 AS 外部的路由。

(4) 配置 Area1 为 Stub 区域

配置 Switch A。

```
[SwitchA] ospf
```

```
[SwitchA-ospf-1] area 1
```

```
[SwitchA-ospf-1-area-0.0.0.1] stub
```

```
[SwitchA-ospf-1-area-0.0.0.1] quit
```

```
[SwitchA-ospf-1] quit
```

配置 Switch C。

```
[SwitchC] ospf
[SwitchC-ospf-1] stub-router
[SwitchC-ospf-1] area 1
[SwitchC-ospf-1-area-0.0.0.1] stub
[SwitchC-ospf-1-area-0.0.0.1] quit
[SwitchC-ospf-1] quit
```

显示 Switch C 的 OSPF 路由表。

```
[SwitchC] display ospf routing
      OSPF Process 1 with Router ID 172.16.1.1
      Routing Tables
```

```
Routing for Network
Destination      Cost  Type      NextHop      AdvRouter      Area
0.0.0.0/0        65536 Inter-area 192.168.1.1   192.168.0.1    0.0.0.1
172.16.1.0/24    1      Stub      172.16.1.1   172.16.1.1     0.0.0.1
172.17.1.0/24    68660 Inter-area 192.168.1.1   192.168.0.1    0.0.0.1
192.168.1.0/24   1562   Stub      192.168.1.2   172.16.1.1     0.0.0.1
192.168.2.0/24   68659 Inter-area 192.168.1.1   192.168.0.1    0.0.0.1
192.168.0.0/24   67097 Inter-area 192.168.1.1   192.168.0.1    0.0.0.1

Total Nets: 6
Intra Area: 2  Inter Area: 4  ASE: 0  NSSA: 0
```



说明

当把 Switch C 所在区域配置为 Stub 区域时，已经看不到 AS 外部的路由，取而代之的是一条缺省路由。

配置禁止向 Stub 区域通告 Type3 LSA。

```
[SwitchA] ospf
[SwitchA-ospf-1] area 1
[SwitchA-ospf-1-area-0.0.0.1] stub no-summary
[SwitchA-ospf-1-area-0.0.0.1] quit
```

查看 Switch C 的 OSPF 路由表。

```
[SwitchC] display ospf routing
      OSPF Process 1 with Router ID 172.16.1.1
      Routing Tables
```

```
Routing for Network
Destination      Cost  Type      NextHop      AdvRouter      Area
0.0.0.0/0        1563   Inter-area 192.168.1.1   192.168.0.1    0.0.0.1
172.16.1.0/24    1      Stub      172.16.1.1   172.16.1.1     0.0.0.1
192.168.1.0/24   1562   Stub      192.168.1.2   172.16.1.1     0.0.0.1

Total Nets: 3
Intra Area: 2  Inter Area: 1  ASE: 0  NSSA: 0
```



说明

禁止向 Stub 区域通告 Summary LSA 后，Stub 路由器的路由表项进一步减少，只保留了一条通往区域外部的缺省路由。

1.9.5 完整配置

- 配置 Switch A

```
#
vlan 100
#
vlan 200
#
interface Vlan-interface100
 ip address 192.168.0.1 255.255.255.0
#
interface Vlan-interface200
 ip address 192.168.1.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 192.168.0.0 0.0.0.255
 area 0.0.0.1
  network 192.168.1.0 0.0.0.255
 stub no-summary
```

- 配置 Switch B

```
#
vlan 100
#
vlan 200
#
interface Vlan-interface100
 ip address 192.168.0.2 255.255.255.0
#
interface Vlan-interface200
 ip address 192.168.2.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 192.168.0.0 0.0.0.255
 area 0.0.0.2
  network 192.168.2.0 0.0.0.255
```

- 配置 Switch C

```
#
vlan 200
```

```

#
vlan 300
#
interface Vlan-interface200
ip address 192.168.1.2 255.255.255.0
#
interface Vlan-interface300
ip address 172.16.1.1 255.255.255.0
#
ospf 1
stub-router
area 0.0.0.1
network 192.168.1.0 0.0.0.255
network 172.16.1.0 0.0.0.255
stub
#

```

- 配置 Switch D

```

#
vlan 200
#
vlan 300
#
interface Vlan-interface200
ip address 192.168.2.2 255.255.255.0
#
interface Vlan-interface300
ip address 172.17.1.1 255.255.255.0
#
ospf 1
area 0.0.0.2
network 192.168.2.0 0.0.0.255
network 172.17.1.0 0.0.0.255
import-route static
#
ip route-static 200.0.0.0 255.0.0.0 NULL0
#

```

1.9.6 配置注意事项

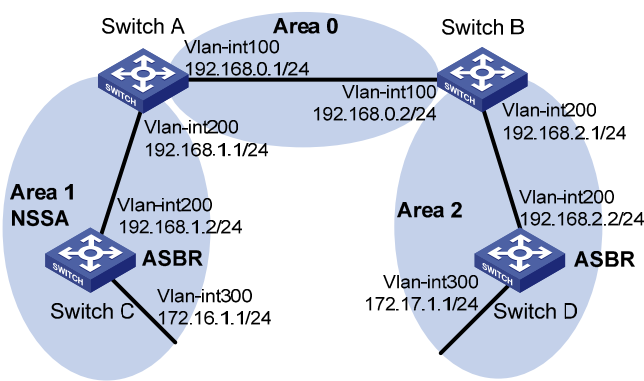
- 所有连接到 **Stub** 区域的路由器必须使用 **stub** 命令将该区域配置成 **Stub** 属性。
- 骨干区域不能配置成 **Stub** 区域。
- 如果要将一个区域配置成 **Stub** 区域，则该区域中的所有路由器必须都要配置 **stub [no-summary]** 命令。
- **Stub** 区域内不能存在 **ASBR**，即自治系统外部的路由不能在本区域内传播。
- 虚连接不能穿过 **Stub** 区域。

1.10 OSPF 的 NSSA 区域典型配置指导

Stub 区域不能引入外部路由，为此又产生了 NSSA 区域的概念。NSSA 区域中允许 Type7 LSA（NSSA External LSA）的传播。Type7 LSA 由 NSSA 区域的 ASBR 产生，当它到达 NSSA 区域的 ABR 时，就会转换成 Type5 LSA（AS External LSA），并通告到其他区域。

1.10.1 组网图

图1-10 配置 OSPF NSSA 区域组网图



1.10.2 应用要求

- 所有的交换机都运行 OSPF，整个自治系统划分为 3 个区域。
- 其中 Switch A 和 Switch B 作为 ABR 来转发区域之间的路由，Switch D 作为 ASBR 引入了外部路由（静态路由）。
- 要求将 Area1 配置为 NSSA 区域，同时将 Switch C 配置为 ASBR 引入外部路由（静态路由），且路由信息可正确的在 AS 内传播。

1.10.3 适用产品、版本

表1-10 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6100, Release 6300 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.10.4 配置过程和解释

- (1) 配置各接口的 IP 地址（略）
- (2) 配置 OSPF（同前例 1.6 ）
- (3) 配置 Switch D 引入静态路由（同前例 1.9 ）

(4) 配置 Area1 区域为 NSSA 区域

配置 Switch A。

```
[SwitchA] ospf
[SwitchA-ospf-1] area 1
[SwitchA-ospf-1-area-0.0.0.1] nssa default-route-advertise no-summary
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] quit
```

配置 Switch C。

```
[SwitchC] ospf
[SwitchC-ospf-1] area 1
[SwitchC-ospf-1-area-0.0.0.1] nssa
[SwitchC-ospf-1-area-0.0.0.1] quit
[SwitchC-ospf-1] quit
```



说明

建议在 ABR（这里的 Switch A）上配置 **default-route-advertise no-summary** 参数，这样可以减少 NSSA 路由器的路由表数量。其他 NSSA 路由器只需配置 **nssa** 命令就可以。

查看 Switch C 的 OSPF 路由表。

```
[SwitchC] display ospf routing

    OSPF Process 1 with Router ID 172.16.1.1

    Routing Tables

Routing for Network
Destination      Cost   Type      NextHop      AdvRouter      Area
0.0.0.0/0        1563   Inter-area 192.168.1.1   192.168.0.1     0.0.0.1
172.16.1.0/24    1      Stub      172.16.1.1   172.16.1.1     0.0.0.1
192.168.1.0/24   1562   Stub      192.168.1.2   172.16.1.1     0.0.0.1

Total Nets: 3
Intra Area: 2  Inter Area: 1  ASE: 0  NSSA: 0
```

(5) 配置 Switch C 引入静态路由

```
[SwitchC] ip route-static 100.0.0.0 8 null 0
[SwitchC] ospf
[SwitchC-ospf-1] import-route static
[SwitchC-ospf-1] quit
```

查看 Switch D 的 OSPF 路由表。

```
[SwitchD-ospf-1] display ospf routing

    OSPF Process 1 with Router ID 172.17.1.1

    Routing Tables

Routing for Network
Destination      Cost   Type      NextHop      AdvRouter      Area
172.16.1.0/24    4687   Inter-area 192.168.2.1   192.168.0.2     0.0.0.2
172.17.1.0/24    1      Stub      172.17.1.1   172.17.1.1     0.0.0.2
```

192.168.1.0/24	4686	Inter-area	192.168.2.1	192.168.0.2	0.0.0.2
192.168.2.0/24	1562	Stub	192.168.2.2	172.17.1.1	0.0.0.2
192.168.0.0/24	3124	Inter-area	192.168.2.1	192.168.0.2	0.0.0.2
Routing for ASEs					
Destination	Cost	Type	Tag	NextHop	AdvRouter
100.0.0.0/8	10	Type2	1	192.168.2.1	192.168.0.1
Routing for NSSAs					
Destination	Cost	Type	Tag	NextHop	AdvRouter
Total Nets: 6					
Intra Area: 2 Inter Area: 3 ASE: 1 NSSA: 0					



说明

在 Switch D 上可以看到 NSSA 区域引入的一条 AS 外部的路由。

1.10.5 完整配置

- 配置 Switch A

```
#
vlan 100
#
vlan 200
#
interface Vlan-interface100
 ip address 192.168.0.1 255.255.255.0
#
interface Vlan-interface200
 ip address 192.168.1.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 192.168.0.0 0.0.0.255
 area 0.0.0.1
  network 192.168.1.0 0.0.0.255
 nssa default-route-advertise no-summary
#
```

- 配置 Switch B

```
#
vlan 100
#
vlan 200
#
interface Vlan-interface100
 ip address 192.168.0.2 255.255.255.0
#
interface Vlan-interface200
```



```

ip address 192.168.2.1 255.255.255.0
#
ospf 1
area 0.0.0.0
network 192.168.0.0 0.0.0.255
area 0.0.0.2
network 192.168.2.0 0.0.0.255
#

```

- 配置 Switch C

```

#
vlan 200
#
vlan 300
#
interface Vlan-interface200
ip address 192.168.1.2 255.255.255.0
#
interface Vlan-interface300
ip address 172.16.1.1 255.255.255.0
#
ospf 1
area 0.0.0.1
network 192.168.1.0 0.0.0.255
network 172.16.1.0 0.0.0.255
nssa
import-route static
#
ip route-static 100.0.0.0 255.0.0.0 NULL0
#

```

- 配置 Switch D

```

#
vlan 200
#
vlan 300
#
interface Vlan-interface200
ip address 192.168.2.2 255.255.255.0
#
interface Vlan-interface300
ip address 172.17.1.1 255.255.255.0
#
ospf 1
area 0.0.0.2
network 192.168.2.0 0.0.0.255
network 172.17.1.0 0.0.0.255
import-route static
#
ip route-static 200.0.0.0 255.0.0.0 NULL0

```

1.10.6 配置注意事项

所有连接到 NSSA 区域的路由器必须使用 **nssa** 命令将该区域配置成 NSSA 属性。

1.11 OSPF 的 DR 选择典型配置指导

在广播网和 NBMA 网络中，任意两台路由器之间都要交换路由信息。如果网络中有 n 台路由器，则需要建立 $n(n-1)/2$ 个邻接关系。这使得任何一台路由器的路由变化都会导致多次传递，浪费了带宽资源。为解决这一问题，OSPF 协议定义了指定路由器 DR（Designated Router），所有路由器都只将信息发送给 DR，由 DR 将网络链路状态发送出去。

如果 DR 由于某种故障而失效，则网络中的路由器必须重新选举 DR，再与新的 DR 同步。这需要较长的时间，在这段时间内，路由的计算是不正确的。为了能够缩短这个过程，OSPF 提出了 BDR（Backup Designated Router，备份指定路由器）的概念。

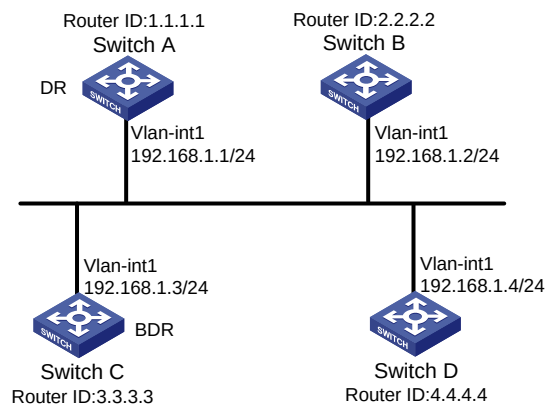
BDR 实际上是对 DR 的一个备份，在选举 DR 的同时也选举出 BDR，BDR 也和本网段内的所有路由器建立邻接关系并交换路由信息。当 DR 失效后，BDR 会立即成为 DR。由于不需要重新选举，并且邻接关系事先已建立，所以这个过程是非常短暂的。当然这时还需要再重新选举出一个新的 BDR，虽然一样需要较长的时间，但并不会影响路由的计算。

运行 OSPF 进程的网络中，既不是 DR 也不是 BDR 的路由器为 DR Other。DR Other

仅与 DR 和 BDR 之间建立邻接关系，DR Other 之间不交换任何路由信息。这样就减少了广播网和 NBMA 网络上各路由器之间邻接关系的数量，同时减少网络流量，节约了带宽资源。

1.11.1 组网图

图1-11 配置 OSPF 优先级的 DR 选择组网图



1.11.2 应用要求

- Switch A、Switch B、Switch C、Switch D 在同一网段，运行 OSPF 协议；
- 配置 Switch A 为 DR，Switch C 为 BDR。

1.11.3 适用产品、版本

表1-11 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6100, Release 6300 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.11.4 配置过程和解释

(1) 配置各接口的 IP 地址（略）

(2) 配置 OSPF 基本功能

配置 Switch A，启动 OSPF，并设置其 Router ID 为 1.1.1.1。

```
<SwitchA> system-view
[SwitchA] router id 1.1.1.1
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] quit
```

配置 Switch B，启动 OSPF，并设置其 Router ID 为 2.2.2.2。

```
<SwitchB> system-view
[SwitchB] router id 2.2.2.2
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] quit
```

配置 Switch C，启动 OSPF，并设置其 Router ID 为 3.3.3.3。

```
<SwitchC> system-view
[SwitchC] router id 3.3.3.3
[SwitchC] ospf
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] quit
[SwitchC-ospf-1] quit
```

配置 Switch D，启动 OSPF，并设置其 Router ID 为 4.4.4.4。

```
<SwitchD> system-view
[SwitchD] router id 4.4.4.4
```

```

[SwitchD] ospf
[SwitchD-ospf-1] area 0
[SwitchD-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] quit
[SwitchD-ospf-1] quit

# 查看 Switch A 的邻居信息。

[SwitchA] display ospf peer verbose

      OSPF Process 1 with Router ID 1.1.1.1
      Neighbors

Area 0.0.0.0 interface 192.168.1.1(Vlan-interface1)'s neighbors
Router ID: 2.2.2.2      Address: 192.168.1.2      GR State: Normal
State: 2-Way  Mode: None  Priority: 1
DR: 192.168.1.4  BDR: 192.168.1.3  MTU: 0
Dead timer due in 38 sec
Neighbor is up for 00:01:31
Authentication Sequence: [ 0 ]
Neighbor state change count: 2

Router ID: 3.3.3.3      Address: 192.168.1.3      GR State: Normal
State: Full  Mode: Nbr is Master  Priority: 1
DR: 192.168.1.4  BDR: 192.168.1.3  MTU: 0
Dead timer due in 31 sec
Neighbor is up for 00:01:28
Authentication Sequence: [ 0 ]
Neighbor state change count: 2

Router ID: 4.4.4.4      Address: 192.168.1.4      GR State: Normal
State: Full  Mode: Nbr is Master  Priority: 1
DR: 192.168.1.4  BDR: 192.168.1.3  MTU: 0
Dead timer due in 31 sec
Neighbor is up for 00:01:28
Authentication Sequence: [ 0 ]
Neighbor state change count: 2

```

可以看到 Switch D 为 DR，Switch C 为 BDR。

(3) 配置接口上的路由器优先级

配置 Switch A。

```

[SwitchA] interface vlan-interface 1
[RouterA-Vlan-interface1] ospf dr-priority 100
[RouterA-Vlan-interface1] quit

```

配置 Switch B。

```

[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ospf dr-priority 0
[SwitchB-Vlan-interface1] quit

```

配置 Switch C。

```
[SwitchC] interface vlan-interface 1
[SwitchC-Vlan-interface1] ospf dr-priority 2
[SwitchC-Vlan-interface] quit
```

查看 Switch D 的邻居信息。

```
[SwitchD] display ospf peer verbose
```

```
OSPF Process 1 with Router ID 4.4.4.4
```

```
Neighbors
```

```
Area 0.0.0.0 interface 192.168.1.4(Vlan-interface1)'s neighbors
```

```
Router ID: 1.1.1.1      Address: 192.168.1.1      GR State: Normal
```

```
State: Full Mode:Nbr is Slave Priority: 100
```

```
DR: 192.168.1.4 BDR: 192.168.1.3 MTU: 0
```

```
Dead timer due in 31 sec
```

```
Neighbor is up for 00:11:17
```

```
Authentication Sequence: [ 0 ]
```

```
Neighbor state change count: 3
```

```
Router ID: 2.2.2.2      Address: 192.168.1.2      GR State: Normal
```

```
State: Full Mode:Nbr is Slave Priority: 0
```

```
DR: 192.168.1.4 BDR: 192.168.1.3 MTU: 0
```

```
Dead timer due in 35 sec
```

```
Neighbor is up for 00:11:19
```

```
Authentication Sequence: [ 0 ]
```

```
Neighbor state change count: 3
```

```
Router ID: 3.3.3.3      Address: 192.168.1.3      GR State: Normal
```

```
State: Full Mode:Nbr is Slave Priority: 2
```

```
DR: 192.168.1.4 BDR: 192.168.1.3 MTU: 0
```

```
Dead timer due in 33 sec
```

```
Neighbor is up for 00:11:15
```

```
Authentication Sequence: [ 0 ]
```

```
Neighbor state change count: 3
```

可以看到，网络中 DR/BDR 并没有改变。



说明

网络中 DR/BDR 已经存在的情况下，接口上的路由器优先级的配置并不会立即生效。

(4) 重启 OSPF 进程（略）

查看 Switch D 的邻居信息。

```
[SwitchD] display ospf peer verbose
```

```
OSPF Process 1 with Router ID 4.4.4.4
```

```
Neighbors
```

```

Area 0.0.0.0 interface 192.168.1.4(Vlan-interface1)'s neighbors
Router ID: 1.1.1.1      Address: 192.168.1.1      GR State: Normal
  State: Full  Mode: Nbr is Slave  Priority: 100
  DR: 192.168.1.1  BDR: 192.168.1.3  MTU: 0
  Dead timer due in 39 sec
  Neighbor is up for 00:01:40
  Authentication Sequence: [ 0 ]
  Neighbor state change count: 2

Router ID: 2.2.2.2      Address: 192.168.1.2      GR State: Normal
  State: 2-Way  Mode: None  Priority: 0
  DR: 192.168.1.1  BDR: 192.168.1.3  MTU: 0
  Dead timer due in 35 sec
  Neighbor is up for 00:01:44
  Authentication Sequence: [ 0 ]
  Neighbor state change count: 2

Router ID: 3.3.3.3      Address: 192.168.1.3      GR State: Normal
  State: Full  Mode: Nbr is Slave  Priority: 2
  DR: 192.168.1.1  BDR: 192.168.1.3  MTU: 0
  Dead timer due in 39 sec
  Neighbor is up for 00:01:41
  Authentication Sequence: [ 0 ]
  Neighbor state change count: 2

```

可以看到 Switch A 成为 DR，Switch C 为 BDR。



说明

- 如果邻居的状态是 Full，这说明它和邻居之间形成了邻接关系；
- 如果邻居的状态是 2-Way，则说明它们都不是 DR 或 BDR，两者之间不需要交换 LSA。

查看 OSPF 接口的状态。

```
[SwitchA] display ospf interface
```

```

      OSPF Process 1 with Router ID 1.1.1.1
      Interfaces

Area: 0.0.0.0

```

IP Address	Type	State	Cost	Pri	DR	BDR
192.168.1.1	Broadcast	DR	1	100	192.168.1.1	192.168.1.3

```
[SwitchB] display ospf interface
```

```

      OSPF Process 1 with Router ID 2.2.2.2
      Interfaces

Area: 0.0.0.0

```

IP Address	Type	State	Cost	Pri	DR	BDR
192.168.1.2	Broadcast	DROther	1	0	192.168.1.1	192.168.1.3



说明

如果 OSPF 接口的状态是 DROther，则说明它既不是 DR，也不是 BDR。

1.11.5 完整配置

- 配置 Switch A

```
#
router id 1.1.1.1
#
interface Vlan-interface1
ip address 192.168.1.1 255.255.255.0
ospf dr-priority 100
#
ospf 1
area 0.0.0.0
network 192.168.1.0 0.0.0.255
#
```

- 配置 Switch B

```
#
router id 2.2.2.2
#
interface Vlan-interface1
ip address 192.168.1.2 255.255.255.0
ospf dr-priority 0
#
ospf 1
area 0.0.0.0
network 192.168.1.0 0.0.0.255
#
```

- 配置 Switch C

```
#
router id 3.3.3.3
#
interface Vlan-interface1
ip address 192.168.1.3 255.255.255.0
ospf dr-priority 2
#
ospf 1
area 0.0.0.0
network 192.168.1.0 0.0.0.255
#
```

- 配置 Switch D

```
#
```

```
router id 4.4.4.4
#
interface Vlan-interface1
ip address 192.168.1.4 255.255.255.0
#
ospf 1
area 0.0.0.0
network 192.168.1.0 0.0.0.255
#
```

1.11.6 配置注意事项

- 只有在广播或 NBMA 类型接口才会选举 DR，在点到点或点到多点类型的接口上不需要选举 DR。
- DR 是某个网段中的概念，是针对路由器的接口而言的。某台路由器在一个接口上可能是 DR，在另一个接口上有可能是 BDR，或者是 DR Other。
- 路由器的优先级可以影响 DR/BDR 的选举过程，但是当 DR/BDR 已经选举完毕，就算一台具有更高优先级的路由器变为有效，也不会替换该网段中已经存在的 DR/BDR 成为新的 DR/BDR。
- DR 并不一定就是路由器优先级最高的路由器接口；同理，BDR 也并不一定就是路由器优先级次高的路由器接口。

1.12 OSPF 虚连接典型配置指导

OSPF 划分区域之后，并非所有的区域都是平等的关系。其中有一个区域是与众不同的，它的区域号（Area ID）是 0，通常被称为骨干区域。骨干区域负责区域之间的路由，非骨干区域之间的路由信息必须通过骨干区域来转发。对此，OSPF 有两个规定：

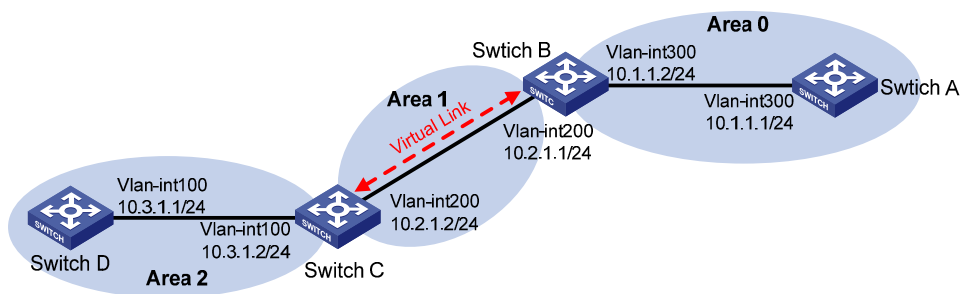
- 所有非骨干区域必须与骨干区域保持连通；
- 骨干区域自身也必须保持连通。

但在实际应用中，可能会因为各方面条件的限制，无法满足这个要求。这时可以通过配置 OSPF 虚连接（Virtual Link）予以解决。

虚连接是指在两台 ABR 之间通过一个非骨干区域而建立的一条逻辑上的连接通道。它的两端必须是 ABR，而且必须在两端同时配置方可生效。为虚连接两端提供一条非骨干区域内部路由的区域称为传输区（Transit Area）。

1.12.1 组网图

图1-12 配置 OSPF 虚链路组网图



1.12.2 应用要求

- Area2 与 Area0 没有直接相连。Area1 被用作传输区域(Transit Area)来连接 Area2 和 Area0。Switch B 和 Switch C 之间配置一条虚连接。
- 配置完成后，Switch B 能够学到 Area2 中的路由。

1.12.3 适用产品、版本

表1-12 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6100, Release 6300 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.12.4 配置过程和解释

```
(1) 配置各接口的 IP 地址（略）
(2) 配置 OSPF 基本功能
# 配置 Switch A，启动 OSPF，并设置其 Router ID 为 1.1.1.1。
<SwitchA> system-view
[SwitchA] ospf 1 router-id 1.1.1.1
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
# 配置 Switch B，启动 OSPF，并设置其 Router ID 为 2.2.2.2。
<SwitchB> system-view
[SwitchB] ospf 1 router-id 2.2.2.2
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
```

```
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] area 1
[SwitchB-ospf-1-area-0.0.0.1] network 10.2.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.1] quit
```

配置 Switch C，启动 OSPF，并设置其 Router ID 为 3.3.3.3。

```
<SwitchC> system-view
[SwitchC] ospf 1 router-id 3.3.3.3
[SwitchC-ospf-1] area 1
[SwitchC-ospf-1-area-0.0.0.1] network 10.2.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.1] quit
[SwitchC-ospf-1] area 2
[SwitchC-ospf-1-area-0.0.0.2] network 10.3.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.2] quit
```

配置 Switch D，启动 OSPF，并设置其 Router ID 为 4.4.4.4。

```
<SwitchD> system-view
[SwitchD] ospf 1 router-id 4.4.4.4
[SwitchD-ospf-1] area 2
[SwitchD-ospf-1-area-0.0.0.2] network 10.3.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.2] quit
```

查看 Switch B 的 OSPF 路由表。

```
[SwitchB] display ospf routing

    OSPF Process 1 with Router ID 2.2.2.2

    Routing Tables

    Routing for Network

    Destination      Cost      Type      NextHop      AdvRouter      Area
    10.2.1.0/24       2         Transit   10.2.1.1      3.3.3.3        0.0.0.1
    10.1.1.0/24       2         Transit   10.1.1.2      2.2.2.2        0.0.0.0
    Total Nets: 2
    Intra Area: 2  Inter Area: 0  ASE: 0  NSSA: 0
```



说明

由于 Area0 没有与 Area2 直接相连，所以 Switch B 的路由表中没有 Area 2 的路由。

(3) 配置虚连接

配置 Switch B。

```
[SwitchB] ospf
[SwitchB-ospf-1] area 1
[SwitchB-ospf-1-area-0.0.0.1] vlink-peer 3.3.3.3
[SwitchB-ospf-1-area-0.0.0.1] quit
[SwitchB-ospf-1] quit
```

配置 Switch C。

```
[SwitchC] ospf 1
[SwitchC-ospf-1] area 1
[SwitchC-ospf-1-area-0.0.0.1] vlink-peer 2.2.2.2
```

```
[SwitchC-ospf-1-area-0.0.0.1] quit
```

查看 Switch B 的 OSPF 路由表。

```
[SwitchB] display ospf routing
```

```
OSPF Process 1 with Router ID 2.2.2.2
```

```
Routing Tables
```

```
Routing for Network
```

Destination	Cost	Type	NextHop	AdvRouter	Area
10.2.1.0/24	2	Transit	10.2.1.1	3.3.3.3	0.0.0.1
10.3.1.0/24	5	Inter	10.2.1.2	3.3.3.3	0.0.0.0
10.1.1.0/24	2	Transit	10.1.1.2	2.2.2.2	0.0.0.0

```
Total Nets: 3
```

```
Intra Area: 2 Inter Area: 1 ASE: 0 NSSA: 0
```

可以看到，Switch B 已经学到了 Area2 的路由 10.3.1.0/24。

1.12.5 完整配置

- 配置 Switch A

```
#
```

```
vlan 300
```

```
#
```

```
interface Vlan-interface300
```

```
ip address 10.1.1.1 255.255.255.0
```

```
#
```

```
ospf 1 router-id 1.1.1.1
```

```
area 0.0.0.0
```

```
network 10.1.1.0 0.0.0.255
```

```
#
```

- 配置 Switch B

```
#
```

```
vlan 200
```

```
#
```

```
vlan 300
```

```
#
```

```
interface Vlan-interface200
```

```
ip address 10.2.1.1 255.255.255.0
```

```
#
```

```
interface Vlan-interface300
```

```
ip address 10.1.1.2 255.255.255.0
```

```
#
```

```
ospf 1 router-id 2.2.2.2
```

```
area 0.0.0.0
```

```
network 10.1.1.0 0.0.0.255
```

```
area 0.0.0.1
```

```
network 10.2.1.0 0.0.0.255
```

```
vlink-peer 3.3.3.3
```

```
#
```

- 配置 Switch C

```

#
vlan 100
#
vlan 200
#
interface Vlan-interface100
 ip address 10.3.1.2 255.255.255.0
#
interface Vlan-interface200
 ip address 10.2.1.2 255.255.255.0
#
ospf 1 router-id 3.3.3.3
 area 0.0.0.1
  network 10.2.1.0 0.0.0.255
 vlink-peer 2.2.2.2
 area 0.0.0.2
  network 10.3.1.0 0.0.0.255
#
• 配置 Switch D
#
vlan 100
#
interface Vlan-interface100
 ip address 10.3.1.1 255.255.255.0
#
ospf 1 router-id 4.4.4.4
 area 0.0.0.2
  network 10.3.1.0 0.0.0.255
#

```

1.12.6 配置注意事项

- 为使虚连接生效，在虚连接的两端都需配置 `vlink-peer` 命令，并且两端配置的 `hello`、`dead` 等参数必须一致。
- 虚连接不能穿过 Stub 区域。
- 虚连接也不能穿过 NSSA 区域。

1.13 OSPF GR 典型配置指导

基于 OSPF 的 GR Restarter 进行协议重启后，为了与其 OSPF 邻居重新同步链路状态数据库，它必须完成下列两项任务：

- 在不改变邻接关系的前提下，重新获取网络中的有效 OSPF 邻居信息；
- 重新获取网络链路状态数据库的内容。

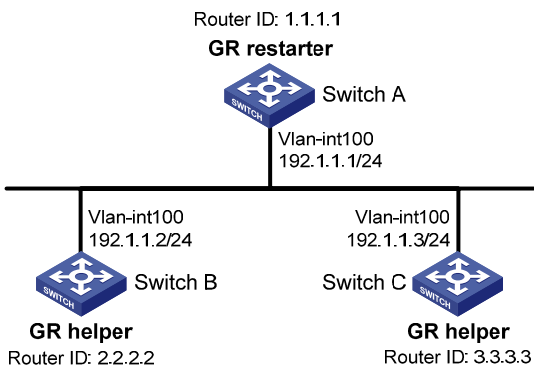
在 OSPF 协议重启前，GR Restarter 产生 Grace-LSA 协商 GR 能力。在重启过程中，GR Helper 继续宣告与 GR Restarter 的邻接状态不变。

OSPF 协议重启完毕后，GR Restarter 会立即向其邻接的 GR Helper 发送一个 OSPF GR 信号。这样，OSPF 邻居就不会复位与它的邻居关系。在收到其 OSPF 邻居的响应后，GR Restarter 会重新恢复与它的邻居关系列表。

邻居关系重新建立后，GR Restarter 与其所有具备 GR 感知能力的 OSPF 邻居之间同步数据库，并交换路由信息。交换完成后，GR Restarter 根据新的路由转发信息更新路由表和转发表，删除失效的路由，完成 OSPF 协议收敛。

1.13.1 组网图

图1-13 OSPF GR 配置组网图



1.13.2 应用要求

- Switch A、Switch B 和 Switch C 既属于同一自治系统，也属于同一 OSPF 域，通过 OSPF 协议实现网络互连，并提供 GR 机制。
- Switch A 作为非 IETF 标准 GR Restarter，Switch B 和 Switch C 作为非 IETF 标准 GR Helper 并且通过 GR 机制与 Switch A 保持带外同步。

1.13.3 适用产品、版本

表1-13 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.13.4 配置过程和解释

(1) 配置 Switch A，启动 OSPF，并设置其 Router ID 为 1.1.1.1。

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ip address 192.1.1.1 255.255.255.0
[SwitchA-Vlan-interface100] quit
[SwitchA] router id 1.1.1.1
```

```
[SwitchA] ospf 100
[SwitchA-ospf-100] enable link-local-signaling
[SwitchA-ospf-100] enable out-of-band-resynchronization
[RouterA-ospf-100] graceful-restart
[SwitchA-ospf-100] area 0
[SwitchA-ospf-100-area-0.0.0.0] network 192.1.1.0 0.0.0.255
[SwitchA-ospf-100-area-0.0.0.0] return
```

(2) 配置 Switch B，启动 OSPF，并设置其 Router ID 为 2.2.2.2。

```
<SwitchB> system-view
[SwitchB] acl number 2000
[SwitchB-acl-basic-2000] rule 10 permit source 192.1.1.1 0.0.0.0
[SwitchB-acl-basic-2000] quit
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ip address 192.1.1.2 255.255.255.0
[SwitchB-Vlan-interface100] quit
[SwitchB] router id 2.2.2.2
[SwitchB] ospf 100
[SwitchB-ospf-100] enable link-local-signaling
[SwitchB-ospf-100] enable out-of-band-resynchronization
[SwitchB-ospf-100] graceful-restart help 2000
[SwitchB-ospf-100] area 0
[SwitchB-ospf-100-area-0.0.0.0] network 192.1.1.0 0.0.0.255
[SwitchB-ospf-100-area-0.0.0.0] quit
```

(3) 配置 Switch C，启动 OSPF，并设置其 Router ID 为 3.3.3.3。

```
<SwitchC> system-view
[SwitchC] interface vlan-interface 100
[SwitchC-Vlan-interface100] ip address 192.1.1.3 255.255.255.0
[SwitchC-Vlan-interface100] quit
[SwitchC] router id 3.3.3.3
[SwitchC] ospf 100
[SwitchC-ospf-100] enable link-local-signaling
[SwitchC-ospf-100] enable out-of-band-resynchronization
[SwitchC-ospf-100] area 0
[SwitchC-ospf-100-area-0.0.0.0] network 192.1.1.0 0.0.0.255
[SwitchC-ospf-100-area-0.0.0.0] quit
```

(4) 检验配置效果

运行稳定后，在 Switch A 上重启 OSPF 协议的 GR 进程。

```
<SwitchA> reset ospf 100 process graceful-restart
```

1.13.5 完整配置

- 配置 Switch A

```
#
router id 1.1.1.1
#
vlan 100
#
interface Vlan-interface100
```

```

ip address 192.1.1.1 255.255.255.0
#
ospf 100
enable link-local-signaling
enable out-of-band-resynchronization
graceful-restart nonstandard
area 0.0.0.0
network 192.1.1.0 0.0.0.255
#
• 配置 Switch B
#
router id 2.2.2.2
#
vlan 100
#
acl number 2000
rule 10 permit source 192.1.1.1 0
#
interface Vlan-interface100
ip address 192.1.1.2 255.255.255.0
ospf dr-priority 0
#
ospf 100
enable link-local-signaling
enable out-of-band-resynchronization
graceful-restart help 2000
area 0.0.0.0
network 192.1.1.0 0.0.0.255
#
• 配置 Switch C
#
router id 3.3.3.3
#
vlan 100
#
interface Vlan-interface100
ip address 192.1.1.3 255.255.255.0
ospf dr-priority 2
#
ospf 100
enable link-local-signaling
enable out-of-band-resynchronization
area 0.0.0.0
network 192.1.1.0 0.0.0.255
#

```

1.13.6 配置注意事项

以 IETF 标准方式实现 GR 时，要求这些 GR 设备上必须预先使能以下两种能力：

- Opaque LSA 发布能力；
- IETF GR 能力。

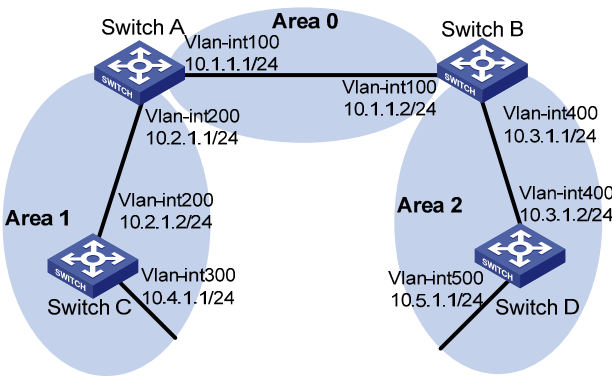
以非 IETF 标准方式实现 GR 时，要求这些 GR 设备上必须预先使能以下三种能力：

- 本地链路信令能力；
- 带外同步能力；
- 非标准 GR 能力。

1.14 路由过滤典型配置指导

1.14.1 组网图

图1-14 配置路由过滤



1.14.2 应用要求

- 所有的交换机都运行 OSPF，整个自治系统划分为 3 个区域。
- 其中 Switch A 和 Switch B 作为 ABR 来转发区域之间的路由。
- 在 Switch C 上配置为 ASBR 引入外部路由（静态路由），并在 Switch C 上配置过滤策略，对引入的一条路由（3.1.3.0/24）进行过滤。
- 在 Switch A 上配置路由策略，对路由（10.5.1.0/24）进行过滤。

1.14.3 适用产品、版本

表1-14 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6100, Release 6300 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.14.4 配置过程和解释

(1) 配置各接口的 IP 地址（略）

(2) 配置 OSPF

配置 Switch A。

```
<SwitchA> system-view
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] area 1
[SwitchA-ospf-1-area-0.0.0.1] network 10.2.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.1] quit
[SwitchA-ospf-1] quit
```

配置 Switch B。

```
<SwitchB> system-view
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] area 2
[SwitchB-ospf-1-area-0.0.0.2] network 10.3.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.2] quit
[SwitchB-ospf-1] quit
```

配置 Switch C。

```
<SwitchC> system-view
[SwitchC] ospf
[SwitchC-ospf-1] area 1
[SwitchC-ospf-1-area-0.0.0.1] network 10.2.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.1] network 10.4.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.1] quit
[SwitchC-ospf-1] quit
```

配置 Switch D。

```
<SwitchD> system-view
[SwitchD] ospf
[SwitchD-ospf-1] area 2
[SwitchD-ospf-1-area-0.0.0.2] network 10.3.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.2] network 10.5.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.2] quit
[SwitchD-ospf-1] quit
```

(3) 配置引入自治系统外部路由

在 Switch C 上配置一条到目的网段 3.1.1.0/24 的静态路由。

```
[SwitchC] ip route-static 3.1.1.0 24 10.4.1.2
```

在 Switch C 上配置一条到目的网段 3.1.2.0/24 的静态路由。

```
[SwitchC] ip route-static 3.1.2.0 24 10.4.1.2
```

在 Switch C 上配置一条到目的网段 3.1.3.0/24 的静态路由。

```
[SwitchC] ip route-static 3.1.3.0 24 10.4.1.2
```

在 Switch C 上配置 OSPF 引入静态路由。

```
[SwitchC] ospf 1
```

```
[SwitchC-ospf-1] import-route static
```

```
[SwitchC-ospf-1] quit
```

在 Switch A 上查看路由信息。

```
[SwitchA] display ip routing-table
```

Routing Tables: Public

Destinations : 12 Routes : 12

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
3.1.1.0/24	O_ASE	150	1	10.2.1.2	Vlan200
3.1.2.0/24	O_ASE	150	1	10.2.1.2	Vlan200
3.1.3.0/24	O_ASE	150	1	10.2.1.2	Vlan200
10.1.1.0/24	Direct	0	0	10.1.1.1	Vlan200
10.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
10.2.1.0/24	Direct	0	0	10.2.1.1	Vlan200
10.2.1.1/32	Direct	0	0	127.0.0.1	InLoop0
10.3.1.0/24	OSPF	10	4	10.1.1.2	Vlan100
10.4.1.0/24	OSPF	10	13	10.2.1.2	Vlan200
10.5.1.0/24	OSPF	10	14	10.1.1.2	Vlan100
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0

(4) 在 Switch C 配置对路由 3.1.3.0/24 进行过滤

配置 IPv4 地址前缀列表。

```
[SwitchC] ip ip-prefix prefix1 index 1 deny 3.1.3.0 24
```

```
[SwitchC] ip ip-prefix prefix1 index 2 permit 3.1.1.0 24
```

```
[SwitchC] ip ip-prefix prefix1 index 3 permit 3.1.2.0 24
```

配置对引入的静态路由信息进行过滤，过滤掉路由 3.1.3.0/24。

```
[SwitchC] ospf 1
```

```
[SwitchC-ospf-1] filter-policy ip-prefix prefix1 export static
```

在 Switch A 上查看路由信息。

```
[SwitchA] display ip routing-table
```

Routing Tables: Public

Destinations : 11 Routes : 11

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
3.1.1.0/24	O_ASE	150	1	10.2.1.2	Vlan200
3.1.2.0/24	O_ASE	150	1	10.2.1.2	Vlan200
10.1.1.0/24	Direct	0	0	10.1.1.1	Vlan100

10.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
10.2.1.0/24	Direct	0	0	10.2.1.1	Vlan200
10.2.1.1/32	Direct	0	0	127.0.0.1	InLoop0
10.3.1.0/24	OSPF	10	4	10.1.1.2	Vlan100
10.4.1.0/24	OSPF	10	13	10.2.1.2	Vlan200
10.5.1.0/24	OSPF	10	14	10.1.1.2	Vlan100
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0

可以看到，到目的网段 3.1.3.0/24 的路由被过滤掉了。

(5) 在 Switch A 上配置对路由 10.5.1.1/24 进行过滤

在 Switch A 上配置访问控制列表。

```
[SwitchA] acl number 2000
[SwitchA-acl-basic-2000] rule 0 deny source 10.5.1.0 0.0.0.255
[SwitchA-acl-basic-2000] rule 1 permit source any
[SwitchA-acl-basic-2000] quit
```

配置对通过 LSA 计算出来的路由信息 10.5.1.0/24 进行过滤。

```
[SwitchA] ospf 1
[SwitchA-ospf-1] filter-policy 2000 import
[SwitchA-ospf-1] quit
```

在 Switch A 上查看路由信息。

```
[SwitchA] display ip routing-table
Routing Tables: Public
          Destinations : 10          Routes : 10
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
3.1.1.0/24	O_ASE	150	1	10.2.1.2	Vlan200
3.1.2.0/24	O_ASE	150	1	10.2.1.2	Vlan200
10.1.1.0/24	Direct	0	0	10.1.1.1	Vlan100
10.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
10.2.1.0/24	Direct	0	0	10.2.1.1	Vlan200
10.2.1.1/32	Direct	0	0	127.0.0.1	InLoop0
10.3.1.0/24	OSPF	10	4	10.1.1.2	Vlan100
10.4.1.0/24	OSPF	10	13	10.2.1.2	Vlan200
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0

可以看到，到 10.5.1.1/24 的路由被过滤掉了。

1.14.5 完整配置

- 配置 Switch A

```
#
acl number 2000
 rule 0 deny source 10.5.1.0 0.0.0.255
 rule 1 permit
#
```

```

vlan 100
#
vlan 200
#
interface Vlan-interface100
 ip address 10.1.1.1 255.255.255.0
#
interface Vlan-interface200
 ip address 10.2.1.1 255.255.255.0
#
ospf 1
 filter-policy 2000 import
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
 area 0.0.0.1
  network 10.2.1.0 0.0.0.255
#

```

- 配置 Switch B

```

#
vlan 100
#
vlan 400
#
interface Vlan-interface100
 ip address 10.1.1.2 255.255.255.0
#
interface Vlan-interface400
 ip address 10.3.1.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
 area 0.0.0.2
  network 10.3.1.0 0.0.0.255
#

```

- 配置 Switch C

```

#
vlan 200
#
vlan 300
#
interface Vlan-interface200
 ip address 10.2.1.2 255.255.255.0
#
interface Vlan-interface300
 ip address 10.4.1.1 255.255.255.0
#
ospf 1

```

```

filter-policy ip-prefix prefix1 export static
import-route static
area 0.0.0.1
network 10.2.1.0 0.0.0.255
network 10.4.1.0 0.0.0.255
#
ip ip-prefix prefix1 index 1 deny 3.1.3.0 24
ip ip-prefix prefix1 index 2 permit 3.1.1.0 24
ip ip-prefix prefix1 index 3 permit 3.1.2.0 24
#
ip route-static 3.1.1.0 255.255.255.0 10.4.1.2
ip route-static 3.1.2.0 255.255.255.0 10.4.1.2
ip route-static 3.1.3.0 255.255.255.0 10.4.1.2
#
• 配置 Switch D
#
vlan 400
#
vlan 500
#
interface Vlan-interface400
ip address 10.3.1.2 255.255.255.0
#
interface Vlan-interface500
ip address 10.5.1.1 255.255.255.0
#
ospf 1
area 0.0.0.2
network 10.3.1.0 0.0.0.255
network 10.5.1.0 0.0.0.255
#

```

1.14.6 配置注意事项

无

1.15 IS-IS 基本配置典型指导

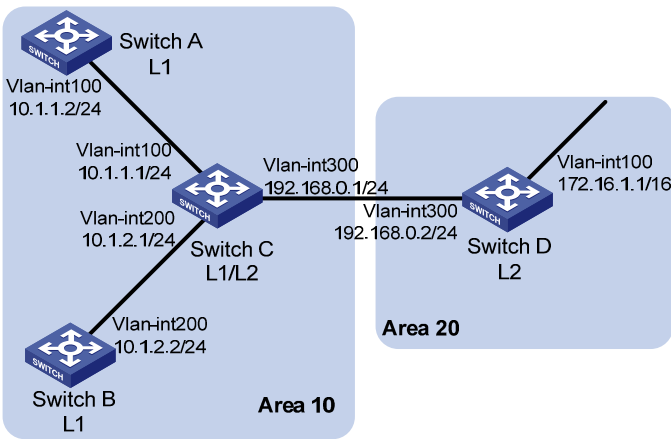
IS-IS（Intermediate System-to-Intermediate System intra-domain routing information exchange protocol，中间系统到中间系统的域内路由信息交换协议）最初是国际标准化组织（the International Organization for Standardization, ISO）为它的无连接网络协议（ConnectionLess Network Protocol, CLNP）设计的一种动态路由协议。

为了提供对 IP 的路由支持，IETF 在 RFC 1195 中对 IS-IS 进行了扩充和修改，使它能够同时应用在 TCP/IP 和 OSI 环境中，称为集成化 IS-IS（Integrated IS-IS 或 Dual IS-IS）。

IS-IS 属于内部网关协议（Interior Gateway Protocol, IGP），用于自治系统内部。IS-IS 是一种链路状态协议，使用最短路径优先（Shortest Path First, SPF）算法进行路由计算。

1.15.1 组网图

图1-15 IS-IS 基本配置组网图



1.15.2 应用要求

如上图所示，Switch A、Switch B、Switch C 和 Switch D 属于同一自治系统，要求他们之间通过 IS-IS 协议达到 IP 网络互连的目的。

其中，Switch A 和 Switch B 为 Level-1 交换机，Switch D 为 Level-2 交换机，Switch C 作为 Level-1-2 交换机将两个区域相连。Switch A、Switch B 和 Switch C 的区域号为 10，Switch D 的区域号为 20。

1.15.3 适用产品、版本

表1-15 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6100, Release 6300 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.15.4 配置过程和解释

- (1) 配置各接口的 IPv4 地址（略）
- (2) 配置 IS-IS

配置 Switch A。

```
<SwitchA> system-view
[SwitchA] isis 1
[SwitchA-isis-1] is-level level-1
[SwitchA-isis-1] network-entity 10.0000.0000.0001.00
[SwitchA-isis-1] quit
[SwitchA] interface vlan-interface 100
```

```
[SwitchA-Vlan-interface100] isis enable 1
[SwitchA-Vlan-interface100] quit
```

配置 Switch B。

```
<SwitchB> system-view
[SwitchB] isis 1
[SwitchB-isis-1] is-level level-1
[SwitchB-isis-1] network-entity 10.0000.0000.0002.00
[SwitchB-isis-1] quit
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] isis enable 1
[SwitchB-Vlan-interface200] quit
```

配置 Switch C。

```
<SwitchC> system-view
[SwitchC] isis 1
[SwitchC-isis-1] network-entity 10.0000.0000.0003.00
[SwitchC-isis-1] quit
[SwitchC] interface vlan-interface 100
[SwitchC-Vlan-interface100] isis enable 1
[SwitchC-Vlan-interface100] quit
[SwitchC] interface vlan-interface 200
[SwitchC-Vlan-interface200] isis enable 1
[SwitchC-Vlan-interface200] quit
[SwitchC] interface vlan-interface 300
[SwitchC-Vlan-interface300] isis enable 1
[SwitchC-Vlan-interface300] quit
```

配置 Switch D。

```
<SwitchD> system-view
[SwitchD] isis 1
[SwitchD-isis-1] is-level level-2
[SwitchD-isis-1] network-entity 20.0000.0000.0004.00
[SwitchD-isis-1] quit
[SwitchD] interface vlan-interface 100
[SwitchD-Vlan-interface100] isis enable 1
[SwitchD-Vlan-interface100] quit
[SwitchD] interface vlan-interface 300
[SwitchD-Vlan-interface300] isis enable 1
[SwitchD-Vlan-interface300] quit
```

(3) 验证配置结果

显示各交换机的 IS-IS LSDB 信息，查看 LSP 是否完整。

```
[SwitchA] display isis lsdb
```

```
Database information for ISIS(1)
```

```
-----
```

```
Level-1 Link State Database
```

LSPID	Seq Num	Checksum	Holdtime	Length	ATT/P/OL

0000.0000.0001.00-00*	0x00000004	0xdf5e	1096	68	0/0/0
0000.0000.0002.00-00	0x00000004	0xee4d	1102	68	0/0/0
0000.0000.0002.01-00	0x00000001	0xdaaf	1102	55	0/0/0
0000.0000.0003.00-00	0x00000009	0xcaa3	1161	111	1/0/0
0000.0000.0003.01-00	0x00000001	0xadda	1112	55	0/0/0

*-Self LSP, +-Self LSP(Extended), ATT-Attached, P-Partition, OL-Overload

[SwitchB] display isis lsdb

Database information for ISIS(1)

Level-1 Link State Database

LSPID	Seq Num	Checksum	Holdtime	Length	ATT/P/OL

0000.0000.0001.00-00	0x00000006	0xdb60	988	68	0/0/0
0000.0000.0002.00-00*	0x00000008	0xe651	1189	68	0/0/0
0000.0000.0002.01-00*	0x00000005	0xd2b3	1188	55	0/0/0
0000.0000.0003.00-00	0x00000014	0x194a	1190	111	1/0/0
0000.0000.0003.01-00	0x00000002	0xabdb	995	55	0/0/0

*-Self LSP, +-Self LSP(Extended), ATT-Attached, P-Partition, OL-Overload

[SwitchC] display isis lsdb

Database information for ISIS(1)

Level-1 Link State Database

LSPID	Seq Num	Checksum	Holdtime	Length	ATT/P/OL

0000.0000.0001.00-00	0x00000006	0xdb60	847	68	0/0/0
0000.0000.0002.00-00	0x00000008	0xe651	1053	68	0/0/0
0000.0000.0002.01-00	0x00000005	0xd2b3	1052	55	0/0/0
0000.0000.0003.00-00*	0x00000014	0x194a	1051	111	1/0/0
0000.0000.0003.01-00*	0x00000002	0xabdb	854	55	0/0/0

*-Self LSP, +-Self LSP(Extended), ATT-Attached, P-Partition, OL-Overload

Level-2 Link State Database

LSPID	Seq Num	Checksum	Holdtime	Length	ATT/P/OL

0000.0000.0003.00-00* 0x00000012 0xc93c 842 100 0/0/0
0000.0000.0004.00-00 0x00000026 0x331 1173 84 0/0/0
0000.0000.0004.01-00 0x00000001 0xee95 668 55 0/0/0

*-Self LSP, +-Self LSP(Extended), ATT-Attached, P-Partition, OL-Overload

[SwitchD] display isis lsdb

Database information for ISIS(1)

Level-2 Link State Database

LSPID	Seq Num	Checksum	Holdtime	Length	ATT/P/OL

0000.0000.0003.00-00	0x00000013	0xc73d	1003	100	0/0/0
0000.0000.0004.00-00*	0x0000003c	0xd647	1194	84	0/0/0
0000.0000.0004.01-00*	0x00000002	0xec96	1007	55	0/0/0

*-Self LSP, +-Self LSP(Extended), ATT-Attached, P-Partition, OL-Overload

显示各交换机的 IS-IS 路由信息。Level-1 交换机的路由表中应该有一条缺省路由，且下一跳为 Level-1-2 交换机，Level-2 交换机的路由表中应该有所有 Level-1 和 Level-2 的路由。

[SwitchA] display isis route

Route information for ISIS(1)

ISIS(1) IPv4 Level-1 Forwarding Table

IPv4 Destination	IntCost	ExtCost	ExitInterface	NextHop	Flags

10.1.1.0/24	10	NULL	Vlan100	Direct	D/L/-
10.1.2.0/24	20	NULL	Vlan100	10.1.1.1	R/-/-
192.168.0.0/24	20	NULL	Vlan100	10.1.1.1	R/-/-
0.0.0.0/0	10	NULL	Vlan100	10.1.1.1	R/-/-

Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set

[SwitchC] display isis route

Route information for ISIS(1)

ISIS(1) IPv4 Level-1 Forwarding Table

IPv4 Destination	IntCost	ExtCost	ExitInterface	NextHop	Flags

192.168.0.0/24	10	NULL	Vlan300	Direct	D/L/-
10.1.1.0/24	10	NULL	Vlan100	Direct	D/L/-
10.1.2.0/24	10	NULL	Vlan200	Direct	D/L/-

Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set

ISIS(1) IPv4 Level-2 Forwarding Table

IPv4 Destination	IntCost	ExtCost	ExitInterface	NextHop	Flags

192.168.0.0/24	10	NULL	Vlan300	Direct	D/L/-
10.1.1.0/24	10	NULL	Vlan100	Direct	D/L/-
10.1.2.0/24	10	NULL	Vlan200	Direct	D/L/-
172.16.0.0/16	20	NULL	Vlan300	192.168.0.2	R/-/-

Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set

[SwitchD] display isis route

Route information for ISIS(1)

ISIS(1) IPv4 Level-2 Forwarding Table

IPv4 Destination	IntCost	ExtCost	ExitInterface	NextHop	Flags

192.168.0.0/24	10	NULL	Vlan300	Direct	D/L/-
10.1.1.0/24	20	NULL	Vlan300	192.168.0.1	R/-/-
10.1.2.0/24	20	NULL	Vlan300	192.168.0.1	R/-/-
172.16.0.0/16	10	NULL	Vlan100	Direct	D/L/-

Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set

1.15.5 完整配置

- 配置 Switch A

```
#
vlan 100
#
isis 1
 is-level level-1
 network-entity 10.0000.0000.0001.00
#
```

```

interface NULL0
#
interface Vlan-interface100
ip address 10.1.1.2 255.255.255.0
isis enable 1
#
• 配置 Switch B
#
vlan 200
#
isis 1
is-level level-1
network-entity 10.0000.0000.0002.00
#
interface Vlan-interface200
ip address 10.1.2.2 255.255.255.0
isis enable 1
#
• 配置 Switch C
#
vlan 100
#
vlan 200
#
vlan 300
#
isis 1
network-entity 10.0000.0000.0003.00
#
interface Vlan-interface100
ip address 10.1.1.1 255.255.255.0
isis enable 1
#
interface Vlan-interface200
ip address 10.1.2.1 255.255.255.0
isis enable 1
#
interface Vlan-interface300
ip address 192.168.0.1 255.255.255.0
isis enable 1
#
• 配置 Switch D
#
vlan 100
#
vlan 300
#

```

```

isis 1
 is-level level-2
 network-entity 20.0000.0000.0004.00
#
interface Vlan-interface100
 ip address 172.16.1.1 255.255.255.0
 isis enable 1
#
interface Vlan-interface300
 ip address 192.168.0.2 255.255.255.0
 isis enable 1
#

```

1.15.6 配置注意事项

- 属于不同区域的 Level-1 路由器不能形成邻居关系。
- Level-2 路由器是否形成邻居关系则与区域无关。
- 当路由器是 Level-1 或者 Level-2 类型时，接口的路由层次类型只能由路由器的类型决定，不能通过 isis circuit-level 命令改变；当路由器是 Level-1-2 类型时，接口的路由层次类型可以通过 isis circuit-level 命令改变，以建立不同层次的邻接关系。

1.16 IS-IS 的 DIS 选择典型配置指导

在广播网络中，IS-IS 需要在所有的路由器中选举一个路由器作为 DIS（Designated Intermediate System）。

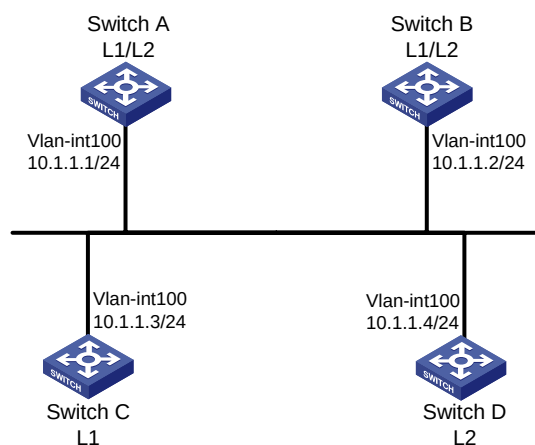
DIS 用来创建和更新伪节点（Pseudonodes），并负责生成伪节点的 LSP，用来描述这个网络上有哪些路由器。

伪节点是用来模拟广播网络的一个虚拟节点，并非真实的路由器。在 IS-IS 中，伪节点用 DIS 的 System ID 和一个字节的 Circuit ID（非 0 值）标识。

使用伪节点可以简化网络拓扑，使产生的 LSP 数量较少，减少 SPF 的资源消耗。

1.16.1 组网图

图1-16 配置 IS-IS 的 DIS 选择组网图



1.16.2 应用要求

如上图所示，Switch A、Switch B、Switch C 和 Switch D 都运行 IS-IS 路由协议以实现互连，它们属于同一区域 10，网络类型为广播网（以太网）。其中 Switch A 和 Switch B 是 Level-1-2 交换机，Switch C 为 Level-1 交换机，Switch D 为 Level-2 交换机。

要求通过改变接口的 DIS 优先级，将 Switch A 配置为 Level-1-2 的 DIS。

1.16.3 适用产品、版本

表1-16 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6100, Release 6300 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.16.4 配置过程和解释

(1) 配置各接口的 IPv4 地址（略）

(2) 配置 IS-IS

配置 Switch A。

```
<SwitchA> system-view
[SwitchA] isis 1
[SwitchA-isis-1] network-entity 10.0000.0000.0001.00
[SwitchA-isis-1] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] isis enable 1
[SwitchA-Vlan-interface100] quit
```

配置 Switch B。

```
<SwitchB> system-view
[SwitchB] isis 1
[SwitchB-isis-1] network-entity 10.0000.0000.0002.00
[SwitchB-isis-1] quit
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] isis enable 1
[SwitchB-Vlan-interface100] quit
```

配置 Switch C。

```
<SwitchC> system-view
[SwitchC] isis 1
[SwitchC-isis-1] network-entity 10.0000.0000.0003.00
[SwitchC-isis-1] is-level level-1
```

```
[SwitchC-isis-1] quit
[SwitchC] interface vlan-interface 100
[SwitchC-Vlan-interface100] isis enable 1
[SwitchC-Vlan-interface100] quit
```

配置 Switch D。

```
<SwitchD> system-view
[SwitchD] isis 1
[SwitchD-isis-1] network-entity 10.0000.0000.0004.00
[SwitchD-isis-1] is-level level-2
[SwitchD-isis-1] quit
[SwitchD] interface vlan-interface 100
[SwitchD-Vlan-interface100] isis enable 1
[SwitchD-Vlan-interface100] quit
```

查看 Switch A 的 IS-IS 邻居信息。

```
[SwitchA] display isis peer
```

```
Peer information for ISIS(1)
-----
System Id: 0000.0000.0002
Interface: Vlan-interface100      Circuit Id: 0000.0000.0003.01
State: Up      HoldTime: 21s      Type: L1(L1L2)      PRI: 64

System Id: 0000.0000.0003
Interface: Vlan-interface100      Circuit Id: 0000.0000.0003.01
State: Up      HoldTime: 27s      Type: L1            PRI: 64

System Id: 0000.0000.0002
Interface: Vlan-interface100      Circuit Id: 0000.0000.0004.01
State: Up      HoldTime: 28s      Type: L2(L1L2)      PRI: 64

System Id: 0000.0000.0004
Interface: Vlan-interface100      Circuit Id: 0000.0000.0004.01
State: Up      HoldTime: 30s      Type: L2            PRI: 64
```

显示 Switch A 的 IS-IS 接口信息。

```
[SwitchA] display isis interface
```

```
Interface information for ISIS(1)
-----
Interface: Vlan-interface100
Id      IPV4.State      IPV6.State      MTU      Type      DIS
001      Up              Down            1497     L1/L2     No/No
```

显示 Switch C 的 IS-IS 接口信息。

```
[SwitchC] display isis interface
```

```
Interface information for ISIS(1)
```

```

-----
Interface: Vlan-interface100
Id      IPV4.State    IPV6.State    MTU    Type    DIS
001      Up          Down        1497   L1/L2   Yes/No

```

显示 Switch D 的 IS-IS 接口信息。

```
[SwitchD] display isis interface
```

```

Interface information for ISIS(1)
-----
Interface: Vlan-interface100
Id      IPV4.State    IPV6.State    MTU    Type    DIS
001      Up          Down        1497   L1/L2   No/Yes

```



说明

从接口信息中可以看到，在使用缺省 DIS 优先级的情况下，Switch C 为 Level-1 的 DIS，Switch D 为 Level-2 的 DIS。Level-1 和 Level-2 的伪节点分别是 0000.0000.0003.01 和 0000.0000.0004.01。

(3) 配置 Switch A 的 DIS 优先级

```

[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] isis dis-priority 100
[SwitchA-Vlan-interface100] quit

```

查看 Switch A 的 IS-IS 邻居信息。

```
[SwitchA] display isis peer
```

```

Peer information for ISIS(1)
-----

System Id: 0000.0000.0002
Interface: Vlan-interface100    Circuit Id: 0000.0000.0001.01
State: Up    HoldTime: 21s    Type: L1(L1L2)    PRI: 64

System Id: 0000.0000.0003
Interface: Vlan-interface100    Circuit Id: 0000.0000.0001.01
State: Up    HoldTime: 27s    Type: L1    PRI: 64

System Id: 0000.0000.0002
Interface: Vlan-interface100    Circuit Id: 0000.0000.0001.01
State: Up    HoldTime: 28s    Type: L2(L1L2)    PRI: 64

System Id: 0000.0000.0004
Interface: Vlan-interface100    Circuit Id: 0000.0000.0001.01
State: Up    HoldTime: 30s    Type: L2    PRI: 64

```

查看 Switch A 的 IS-IS 接口信息。

```
[SwitchA] display isis interface
```

```
Interface information for ISIS(1)
-----
Interface: Vlan-interface100
Id      IPV4.State   IPV6.State   MTU    Type   DIS
001      Up           Down        1497   L1/L2  Yes/Yes
```



说明

从上述信息中可以看到，在改变 IS-IS 接口的 DIS 优先级后，Switch A 立即成为 Level-1-2 的 DR（DIS），且伪节点是 0000.0000.0001.01。

显示 Switch C 的 IS-IS 邻居和接口信息。

```
[SwitchC] display isis peer
```

```
Peer information for ISIS(1)
-----
System Id: 0000.0000.0002
Interface: Vlan-interface100    Circuit Id: 0000.0000.0001.01
State: Up    HoldTime: 25s    Type: L1    PRI: 64

System Id: 0000.0000.0001
Interface: Vlan-interface100    Circuit Id: 0000.0000.0001.01
State: Up    HoldTime: 7s    Type: L1    PRI: 100
```

```
[SwitchC] display isis interface
```

```
Interface information for ISIS(1)
-----
Interface: Vlan-interface100
Id      IPV4.State   IPV6.State   MTU    Type   DIS
001      Up           Down        1497   L1/L2  No/No
```

显示 Switch D 的 IS-IS 邻居和接口信息。

```
[SwitchD] display isis peer
```

```
Peer information for ISIS(1)
-----
System Id: 0000.0000.0001
Interface: Vlan-interface100    Circuit Id: 0000.0000.0001.01
State: Up    HoldTime: 9s    Type: L2    PRI: 100

System Id: 0000.0000.0002
Interface: Vlan-interface100    Circuit Id: 0000.0000.0001.01
State: Up    HoldTime: 28s    Type: L2    PRI: 64
```



```
[SwitchD] display isis interface
```

```
Interface information for ISIS(1)
```

```
-----
```

```
Interface: Vlan-interface100
```

Id	IPV4.State	IPV6.State	MTU	Type	DIS
001	Up	Down	1497	L1/L2	No/No

1.16.5 完整配置

- 配置 Switch A

```
#
vlan 100
#
isis 1
 network-entity 10.0000.0000.0001.00
#
interface Vlan-interface100
 ip address 10.1.1.1 255.255.255.0
 isis enable 1
 isis dis-priority 100
#
```

- 配置 Switch B

```
#
vlan 100
#
isis 1
 network-entity 10.0000.0000.0002.00
#
interface Vlan-interface100
 ip address 10.1.1.2 255.255.255.0
 isis enable 1
#
```

- 配置 Switch C

```
#
vlan 100
#
isis 1
 is-level level-1
 network-entity 10.0000.0000.0003.00
#
interface Vlan-interface100
 ip address 10.1.1.3 255.255.255.0
 isis enable 1
#
```

- 配置 Switch D

```
#
vlan 100
```

```
#
isis 1
is-level level-2
network-entity 10.0000.0000.0004.00
#
interface Vlan-interface100
ip address 10.1.1.4 255.255.255.0
isis enable 1
#
```

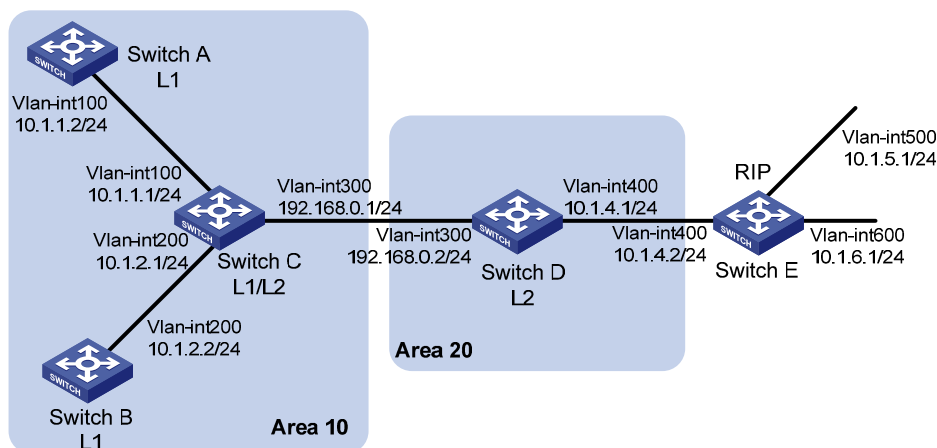
1.16.6 配置注意事项

- 对于 IS-IS，Level-1 和 Level-2 的 DIS 是分别选举的，可以为不同级别的 DIS 选举设置不同的优先级。优先级数值越高，被选中的可能性就越大。
- 当广播网络中优先级最高的路由器有多台时，则其中 MAC 地址最大的路由器会被选中。如果所有路由器的 DIS 优先级都是 0，仍然会选择其中 MAC 地址最大的路由器作为 DIS。

1.17 IS-IS 引入外部路由典型配置指导

1.17.1 组网图

图1-17 配置 IS-IS 引入外部路由组网图



1.17.2 应用要求

- Switch A、Switch B、Switch C 和 Switch D 属于同一自治系统，要求他们之间通过 IS-IS 协议达到 IP 网络互连的目的。
- Switch A 和 Switch B 为 Level-1 路由器，Switch D 为 Level-2 路由器，Switch C 作为 Level-1-2 路由器将两个区域相连。Switch A、Switch B 和 Switch C 的区域号为 10，Switch D 的区域号为 20。
- 在 Switch D 的 IS-IS 进程中引入 RIP 路由。

1.17.3 适用产品、版本

表1-17 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6100, Release 6300 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.17.4 配置过程和解释

(1) 配置各接口的 IP 地址（略）

(2) 配置 IS-IS 基本功能

配置 Switch A。

```
<SwitchA> system-view
[SwitchA] isis 1
[SwitchA-isis-1] is-level level-1
[SwitchA-isis-1] network-entity 10.0000.0000.0001.00
[SwitchA-isis-1] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] isis enable 1
[SwitchA-Vlan-interface100] quit
```

配置 Switch B。

```
<SwitchB> system-view
[SwitchB] isis 1
[SwitchB-isis-1] is-level level-1
[SwitchB-isis-1] network-entity 10.0000.0000.0002.00
[SwitchB-isis-1] quit
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] isis enable 1
[SwitchB-Vlan-interface200] quit
```

配置 Switch C。

```
<SwitchC> system-view
[SwitchC] isis 1
[SwitchC-isis-1] network-entity 10.0000.0000.0003.00
[SwitchC-isis-1] quit
[SwitchC] interface vlan-interface 200
[SwitchC-Vlan-interface200] isis enable 1
[SwitchC-Vlan-interface200] quit
[SwitchC] interface vlan-interface 100
[SwitchC-Vlan-interface100] isis enable 1
```

```
[SwitchC-Vlan-interface100] quit
[SwitchC] interface vlan-interface 300
[SwitchC-Vlan-interface300] isis enable 1
[SwitchC-Vlan-interface300] quit
```

配置 Switch D。

```
<SwitchD> system-view
[SwitchD] isis 1
[SwitchD-isis-1] is-level level-2
[SwitchD-isis-1] network-entity 20.0000.0000.0004.00
[SwitchD-isis-1] quit
[SwitchD] interface interface vlan-interface 300
[SwitchD-Vlan-interface300] isis enable 1
[SwitchD-Vlan-interface300] quit
```

显示各路由器的 IS-IS 路由信息。

```
[SwitchA] display isis route
```

```

Route information for ISIS(1)
-----

ISIS(1) IPv4 Level-1 Forwarding Table
-----

IPv4 Destination    IntCost  ExtCost  ExitInterface  NextHop    Flags
-----
10.1.1.0/24         10       NULL     VLAN100        Direct     D/L/-
10.1.2.0/24         20       NULL     VLAN100        10.1.1.1   R/-/-
192.168.0.0/24      20       NULL     VLAN100        10.1.1.1   R/-/-
0.0.0.0/0           10       NULL     VLAN100        10.1.1.1   R/-/-

Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set
```

```
[SwitchC] display isis route
```

```

Route information for ISIS(1)
-----

ISIS(1) IPv4 Level-1 Forwarding Table
-----

IPv4 Destination    IntCost  ExtCost  ExitInterface  NextHop    Flags
-----
10.1.1.0/24         10       NULL     VLAN100        Direct     D/L/-
10.1.2.0/24         10       NULL     VLAN200        Direct     D/L/-
192.168.0.0/24      10       NULL     VLAN300        Direct     D/L/-

Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set
```

ISIS(1) IPv4 Level-2 Forwarding Table

IPv4 Destination	IntCost	ExtCost	ExitInterface	NextHop	Flags

10.1.1.0/24	10	NULL	VLAN100	Direct	D/L/-
10.1.2.0/24	10	NULL	VLAN200	Direct	D/L/-
192.168.0.0/24	10	NULL	VLAN300	Direct	D/L/-

Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set

[SwitchD] display isis route

Route information for ISIS(1)

ISIS(1) IPv4 Level-2 Forwarding Table

IPv4 Destination	IntCost	ExtCost	ExitInterface	NextHop	Flags

192.168.0.0/24	10	NULL	VLAN300	Direct	D/L/-
10.1.1.0/24	20	NULL	VLAN300	192.168.0.1	R/-/-
10.1.2.0/24	20	NULL	VLAN300	192.168.0.1	R/-/-

Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set

(3) 在 Switch D 和 Switch E 之间运行 RIPv2, 在 Switch D 上配置 IS-IS 进程引入 RIP 路由。

在 Switch D 上配置 RIPv2。

[SwitchD] rip 1

[SwitchD-rip-1] network 10.0.0.0

[SwitchD-rip-1] version 2

[SwitchD-rip-1] undo summary

在 Switch E 上配置 RIPv2。

[SwitchE] rip 1

[SwitchE-rip-1] network 10.0.0.0

[SwitchE-rip-1] version 2

[SwitchE-rip-1] undo summary

在 Switch D 上配置 IS-IS 进程引入 RIP 进程的路由。

[Switch-rip-1] quit

[SwitchD] isis 1

[SwitchD-isis]import-route rip level-2

显示 Switch C 的 IS-IS 路由信息。

[SwitchC] display isis route

Route information for ISIS(1)

ISIS(1) IPv4 Level-1 Forwarding Table

IPv4 Destination	IntCost	ExtCost	ExitInterface	NextHop	Flags
10.1.1.0/24	10	NULL	VLAN100	Direct	D/L/-
10.1.2.0/24	10	NULL	VLAN200	Direct	D/L/-
192.168.0.0/24	10	NULL	VLAN300	Direct	D/L/-

Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set

ISIS(1) IPv4 Level-2 Forwarding Table

IPv4 Destination	IntCost	ExtCost	ExitInterface	NextHop	Flags
10.1.1.0/24	10	NULL	VLAN100	Direct	D/L/-
10.1.2.0/24	10	NULL	VLAN200	Direct	D/L/-
192.168.0.0/24	10	NULL	VLAN300	Direct	D/L/-
10.1.4.0/24	10	NULL	VLAN300	192.168.0.2	R/L/-
10.1.5.0/24	20	NULL	VLAN300	192.168.0.2	R/L/-
10.1.6.0/24	20	NULL	VLAN300	192.168.0.2	R/L/-

Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set

1.17.5 完整配置

- 配置 Switch A

```
#
vlan 100
#
isis 1
 is-level level-1
 network-entity 10.0000.0000.0001.00
#
interface Vlan-interface100
 ip address 10.1.1.2 255.255.255.0
 isis enable 1
#
```

- 配置 Switch B

```
#
vlan 200
#
isis 1
 is-level level-1
 network-entity 10.0000.0000.0002.00
```

```

#
interface Vlan-interface200
 ip address 10.1.2.2 255.255.255.0
 isis enable 1
#
• 配置 Switch C
#
vlan 100
#
vlan 200
#
vlan 300
#
isis 1
 is-level level-1
 network-entity 10.0000.0000.0003.00
#
interface Vlan-interface100
 ip address 10.1.1.1 255.255.255.0
 isis enable 1
#
interface Vlan-interface200
 ip address 10.1.2.2 255.255.255.0
 isis enable 1
#
interface Vlan-interface300
 ip address 192.168.0.1 255.255.255.0
 isis enable 1
#
• 配置 Switch D
#
vlan 300
#
vlan 400
#
isis 1
 is-level level-2
 network-entity 20.0000.0000.0004.00
 import-route rip 1
#
interface Vlan-interface300
 ip address 192.168.0.2 255.255.255.0
 isis enable 1
#
rip 1
 undo summary
version 2

```

```

network 10.0.0.0
#
•    配置 Switch E
#
vlan 400
#
vlan 500
#
vlan 600
#
interface Vlan-interface400
ip address 10.1.4.2 255.255.255.0
#
interface Vlan-interface500
ip address 10.1.5.1 255.255.255.0
#
interface Vlan-interface600
ip address 10.1.6.1 255.255.255.0
#
rip 1
undo summary
version 2
network 10.0.0.0
#

```

1.17.6 配置注意事项

无

1.18 IS-IS GR 典型配置指导

基于 IS-IS 的 GR Restarter 进行协议重启后，为了与其 IS-IS 邻居重新同步链路状态数据库，它必须完成下列两项任务：

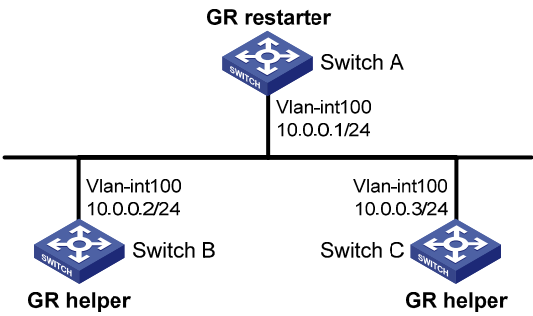
- 在不改变邻接关系的前提下，重新获取网络中的有效 IS-IS 邻居信息；
- 重新获取网络链路状态数据库的内容。

IS-IS 协议重启完毕后，GR Restarter 会立即向邻接的 GR Helper 发送一个 IS-IS GR 信号。这样，IS-IS 邻居就不会复位与其的邻居关系。在收到其 IS-IS 邻居的响应后，GR Restarter 会重新恢复与其的邻居关系列表。

邻居关系重新建立后，GR Restarter 与其所有具备 GR 感知能力的 IS-IS 邻居之间同步数据库，并交换路由信息。交换完成后，GR Restarter 根据新的路由转发信息更新路由表和转发表，删除失效的路由，完成 IS-IS 协议收敛。

1.18.1 组网图

图1-18 IS-IS GR 配置组网图



1.18.2 应用要求

如上图所示，Switch A、Switch B 和 Switch C 属于同一域。这三台交换机都运行 IS-IS 协议以实现路由互连。

1.18.3 适用产品、版本

表1-18 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.18.4 配置过程和解释

(1) 配置各交换机接口的 IP 地址和 IS-IS 协议

配置各接口的 IP 地址和子网掩码，具体配置过程略。

配置各交换机之间采用 IS-IS 协议进行互连，确保 Switch A、Switch B 和 Switch C 之间能够在网络层互通，并且各交换机之间能够借助 IS-IS 协议实现动态路由更新，具体配置过程略。

(2) 配置 IS-IS GR

使能 Switch A 的 IS-IS 协议的 GR 能力，并配置重启间隔时间。

```
<SwitchA> system-view
[SwitchA] isis 1
[SwitchA-isis-1] graceful-restart
[SwitchA-isis-1] graceful-restart interval 150
[SwitchA-isis-1] return
```

Switch B 和 Switch C 的配置与 Switch A 相似，配置过程略。

(3) 检验配置效果

Switch A 分别与 Switch B 和 Switch C 建立邻接关系后，三台交换机开始交换路由信息。Switch A 的 IS-IS 协议重启，进入重启模式后，通过 GR 机制向邻居重新发送连接请求，同步数据库。使用 **display isis graceful-restart status** 命令，可查看 Switch A 上 IS-IS 协议的 GR 状态。

重启 Switch A。

```
<SwitchA> reset isis all 1
```

```
Warning : Reset ISIS process? [Y/N]:y
```

查看 Switch A 上 IS-IS 协议的 GR 状态。

```
<SwitchA> display isis graceful-restart status
```

```
Restart information for ISIS(1)
```

```
-----
```

```
IS-IS(1) Level-1 Restart Status
```

```
Restart Interval: 150
```

```
SA Bit Supported
```

```
Total Number of Interfaces = 1
```

```
Restart Status: RESTARTING
```

```
T3 Timer Status:
```

```
Remaining Time: 65535
```

```
T2 Timer Status:
```

```
Remaining Time: 59
```

```
Interface Vlan1
```

```
T1 Timer Status:
```

```
Remaining Time: 1
```

```
RA Not Received
```

```
Complete CSNP Not Received
```

```
Number of T1 Pre Expiry: 0
```

```
IS-IS(1) Level-2 Restart Status
```

```
Restart Interval: 150
```

```
SA Bit Supported
```

```
Total Number of Interfaces = 1
```

```
Restart Status: RESTARTING
```

```
T3 Timer Status:
```

```
Remaining Time: 65535
```

```
T2 Timer Status:
```

```
Remaining Time: 59
```

```
Interface Vlan1
```

```
T1 Timer Status:
```

```
Remaining Time: 1
```

```
RA Not Received
```

```
Complete CSNP Not Received
```

```
Number of T1 Pre Expiry: 0
```

1.18.5 完整配置

- 配置 Switch A

```
#
```

```

vlan 100
#
isis 1
 graceful-restart
 graceful-restart interval 150
 network-entity 10.0000.0000.0003.00
#
interface Vlan-interface100
 ip address 10.0.0.1 255.255.255.0
 isis enable 1
#

```

- 配置 Switch B

```

#
vlan 100
#
isis 1
 graceful-restart
 graceful-restart interval 150
 is-level level-1
 network-entity 10.0000.0000.0001.00
#
interface Vlan-interface100
 ip address 10.0.0.2 255.255.255.0
 isis enable 1
#

```

- 配置 Switch C

```

#
vlan 100
#
isis 1
 graceful-restart
 graceful-restart interval 150
 is-level level-1
 network-entity 10.0000.0000.0002.00
#
interface Vlan-interface100
 ip address 10.0.0.3 255.255.255.0
 isis enable 1
#

```

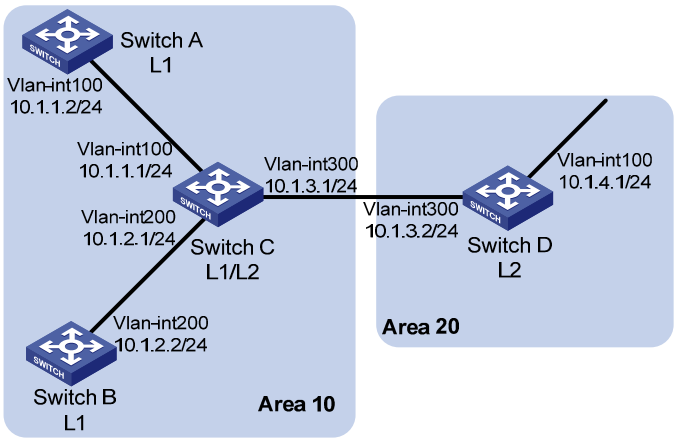
1.18.6 配置注意事项

无

1.19 IS-IS 验证典型配置指导

1.19.1 组网图

图1-19 IS-IS 验证配置举例图



1.19.2 应用要求

如图 1-19所示，Switch A、Switch B、Switch C和Switch D属于同一路由域，要求他们之间通过IS-IS协议达到IP网络互连的目的。

其中，Switch A、Switch B 和 Switch C 属于同一个区域，区域号为 10，Switch D 属于另外一个区域，区域号为 20。

在区域 10 内配置区域验证，防止不可信任的路由信息加入到区域 10 的 LSDB 中；在 Switch C 和 Switch D 上配置路由域验证，防止将不可信的路由信息注入当前路由域；分别在 Switch A、Switch B、Switch C 和 Switch D 上配置邻居关系验证。

1.19.3 适用产品、版本

表1-19 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6100, Release 6300 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.19.4 配置过程和解释

- (1) 配置各接口的 IP 地址（略）
- (2) 配置 IS-IS 基本功能

配置 Switch A。

```

<SwitchA> system-view
[SwitchA] isis 1
[SwitchA-isis-1] network-entity 10.0000.0000.0001.00
[SwitchA-isis-1] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] isis enable 1
[SwitchA-Vlan-interface100] quit

```

配置 Switch B。

```

<SwitchB> system-view
[SwitchB] isis 1
[SwitchB-isis-1] network-entity 10.0000.0000.0002.00
[SwitchB-isis-1] quit
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] isis enable 1
[RouterB--Vlan-interface200] quit

```

配置 Switch C。

```

<SwitchC> system-view
[SwitchC] isis 1
[SwitchC-isis-1] network-entity 10.0000.0000.0003.00
[SwitchC-isis-1] quit
[SwitchC] interface vlan-interface 100
[SwitchC-Vlan-interface200] isis enable 1
[SwitchC-Vlan-interface200] quit
[SwitchC] interface vlan-interface 200
[SwitchC-Vlan-interface300] isis enable 1
[SwitchC-Vlan-interface300] quit
[SwitchC] interface vlan-interface 300
[SwitchC-Vlan-interface300] isis enable 1
[SwitchC-Vlan-interface300] quit

```

配置 Switch D。

```

<SwitchD> system-view
[SwitchD] isis 1
[SwitchD-isis-1] network-entity 20.0000.0000.0001.00
[SwitchD-isis-1] quit
[SwitchD] interface vlan-interface 300
[SwitchD-Vlan-interface300] isis enable 1
[SwitchD-Vlan-interface300] quit

```

(3) 在 Switch A、Switch B、Switch C 和 Switch D 之间建立邻居关系验证

分别在 Switch A 的 Vlan-interface100、Switch C 的 Vlan-interface100 配置邻居关系验证，验证方式为 MD5 密文，验证密码为“eRg”。

```

[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] isis authentication-mode md5 eRg
[SwitchA-Vlan-interface100] quit
[SwitchC] interface vlan-interface 100
[SwitchC-Vlan-interface100] isis authentication-mode md5 eRg

```

```
[SwitchC-Vlan-interface100] quit
```

分别在 Switch B 的 Vlan-interface200、Switch C 的 Vlan-interface200 上配置邻居关系验证，验证方式为 MD5 密文，验证密码为“t5Hr”。

```
[SwitchB] interface vlan-interface 200
```

```
[SwitchB-Vlan-interface200] isis authentication-mode md5 t5Hr
```

```
[SwitchB-Vlan-interface200] quit
```

```
[SwitchC] interface vlan-interface 200
```

```
[SwitchC-Vlan-interface200] isis authentication-mode md5 t5Hr
```

```
[SwitchC-Vlan-interface200] quit
```

分别在 Switch C 的 Vlan-interface300、Switch D 的 Vlan-interface300 配置邻居关系验证，验证方式为 MD5 密文，验证密码为“hSec”。

```
[SwitchC] interface vlan-interface 300
```

```
[SwitchC-Vlan-interface300] isis authentication-mode md5 hSec
```

```
[SwitchC-Vlan-interface300] quit
```

```
[SwitchD] interface vlan-interface 300
```

```
[SwitchD-Vlan-interface300] isis authentication-mode md5 hSec
```

```
[SwitchD-Vlan-interface300] quit
```

(4) 在 Switch A、Switch B 和 Switch C 上配置区域验证，验证方式为 MD5 密文验证，验证密码为“10Sec”。

```
[SwitchA] isis 1
```

```
[SwitchA-isis-1] area-authentication-mode md5 10Sec
```

```
[SwitchA-isis-1] quit
```

```
[SwitchB] isis 1
```

```
[SwitchB-isis-1] area-authentication-mode md5 10Sec
```

```
[SwitchB-isis-1] quit
```

```
[SwitchC] isis 1
```

```
[SwitchC-isis-1] area-authentication-mode md5 10Sec
```

```
[SwitchC-isis-1] quit
```

(5) 在 Switch C 和 Switch D 上配置路由域验证，验证方式为 MD5 密文验证，验证密码为“1020Sec”。

```
[SwitchC] isis 1
```

```
[SwitchC-isis-1] domain-authentication-mode md5 1020Sec
```

```
[SwitchC-isis-1] quit
```

```
[SwitchD] isis 1
```

```
[SwitchD-isis-1] domain-authentication-mode md5 1020Sec
```

1.19.5 完整配置

配置 Switch A

```
#
```

```
vlan 100
```

```
#
```

```
isis 1
```

```
network-entity 10.0000.0000.0001.00
```

```
area-authentication-mode md5 4_"NF,<I(R/Q=^Q`MAF4<1!!
```

```
#
```

```

interface Vlan-interface100
ip address 10.1.1.2 255.255.255.0
isis enable 1
isis authentication-mode md5 #G&R_%_'^C[Q=^Q`MAF4<1!! level-1
isis authentication-mode md5 #G&R_%_'^C[Q=^Q`MAF4<1!! level-2
#

```

配置 Switch B

```

#
vlan 200
#
isis 1
network-entity 10.0000.0000.0002.00
area-authentication-mode md5 4_"NF,<I(R/Q=^Q`MAF4<1!!
#
interface Vlan-interface200
ip address 10.1.2.2 255.255.255.0
isis enable 1
isis authentication-mode md5 BG#5Z'a!THWQ=^Q`MAF4<1!! level-1
isis authentication-mode md5 BG#5Z'a!THWQ=^Q`MAF4<1!! level-2
#

```

配置 Switch C

```

#
vlan 100
#
vlan 200
#
vlan 300
#
isis 1
network-entity 10.0000.0000.0003.00
area-authentication-mode md5 4_"NF,<I(R/Q=^Q`MAF4<1!!
domain-authentication-mode md5 4@>KGW#KZ!_Q=^Q`MAF4<1!!
#
interface Vlan-interface100
ip address 10.1.1.1 255.255.255.0
isis enable 1
isis authentication-mode md5 #G&R_%_'^C[Q=^Q`MAF4<1!! level-1
isis authentication-mode md5 #G&R_%_'^C[Q=^Q`MAF4<1!! level-2
#
interface Vlan-interface200
ip address 10.1.2.1 255.255.255.0
isis enable 1
isis authentication-mode md5 BG#5Z'a!THWQ=^Q`MAF4<1!! level-1
isis authentication-mode md5 BG#5Z'a!THWQ=^Q`MAF4<1!! level-2
#
interface Vlan-interface300
ip address 10.1.3.1 255.255.255.0

```

```

isis enable 1
isis authentication-mode md5 WBG1G<<>#5[Q=^Q`MAF4<1!! level-1
isis authentication-mode md5 WBG1G<<>#5[Q=^Q`MAF4<1!! level-2
#
配置 Switch D
#
vlan 100
#
vlan 300
#
isis 1
network-entity 20.0000.0000.0001.00
domain-authentication-mode md5 4@>KGW#KZ!_Q=^Q`MAF4<1!!
#
interface Vlan-interface100
ip address 10.1.4.1 255.255.255.0
#
interface Vlan-interface300
ip address 10.1.3.2 255.255.255.0
isis enable 1
isis authentication-mode md5 WBG1G<<>#5[Q=^Q`MAF4<1!! level-1
isis authentication-mode md5 WBG1G<<>#5[Q=^Q`MAF4<1!! level-2
#

```

1.19.6 配置注意事项

无

1.20 BGP 基本功能典型配置指导

BGP（Border Gateway Protocol，边界网关协议）是一种用于 AS（Autonomous System，自治系统）之间的动态路由协议。AS 是拥有同一选路策略，在同一技术管理部门下运行的一组路由器。

早期发布的三个版本分别是 BGP-1（RFC 1105）、BGP-2（RFC 1163）和 BGP-3（RFC 1267），当前使用的版本是 BGP-4（RFC 1771）。BGP-4 做为事实上的 Internet 外部路由协议标准，被广泛应用于 ISP（Internet Service Provider，因特网服务提供商）之间。

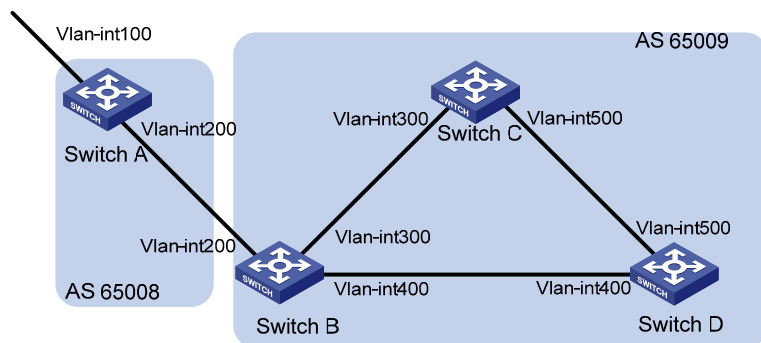
BGP 特性描述如下：

- BGP 是一种外部网关协议（Exterior Gateway Protocol，EGP），与 OSPF、RIP 等内部网关协议（Interior Gateway Protocol，IGP）不同，其着眼点不在于发现和计算路由，而在于控制路由的传播和选择最佳路由。
- BGP 使用 TCP 作为其传输层协议（端口号 179），提高了协议的可靠性。
- BGP 支持 CIDR（Classless Inter-Domain Routing，无类别域间路由）。
- 路由更新时，BGP 只发送更新的路由，大大减少了 BGP 传播路由所占用的带宽，适用于在 Internet 上传播大量的路由信息。
- BGP 路由通过携带 AS 路径信息彻底解决路由环路问题。
- BGP 提供了丰富的路由策略，能够对路由实现灵活的过滤和选择。

- BGP 易于扩展，能够适应网络新的发展。

1.20.1 组网图

图1-20 BGP 基本配置组网图



设备	接口	IP 地址	设备	接口	IP 地址
Switch A	Vlan-int100	8.1.1.1/8	Switch D	Vlan-int400	9.1.1.2/24
	Vlan-int200	200.1.1.2/24		Vlan-int500	9.1.2.2/24
Switch B	Vlan-int400	9.1.1.1/24	Switch C	Vlan-int500	9.1.2.1/24
	Vlan-int200	200.1.1.1/24		Vlan-int300	9.1.3.2/24
	Vlan-int300	9.1.3.1/24			

1.20.2 应用要求

如上图所示，所有交换机均运行 BGP 协议，Switch A 和 Switch B 之间建立 EBGP 连接，Switch B、Switch C 和 Switch D 之间建立 IBGP 全连接。

1.20.3 适用产品、版本

表1-20 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6100, Release 6300 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.20.4 配置过程和解释

- (1) 配置各接口的 IP 地址（略）
- (2) 配置 IBGP 连接

配置 Switch B，启动 BGP，并设置其 Router ID 为 2.2.2.2。

```

<SwitchB> system-view
[SwitchB] bgp 65009
[SwitchB-bgp] router-id 2.2.2.2
[SwitchB-bgp] peer 9.1.1.2 as-number 65009
[SwitchB-bgp] peer 9.1.3.2 as-number 65009

```

```
[SwitchB-bgp] quit
```

配置 Switch C，启动 BGP，并设置其 Router ID 为 3.3.3.3。

```
<SwitchC> system-view
```

```
[SwitchC] bgp 65009
```

```
[SwitchC-bgp] router-id 3.3.3.3
```

```
[SwitchC-bgp] peer 9.1.3.1 as-number 65009
```

```
[SwitchC-bgp] peer 9.1.2.2 as-number 65009
```

```
[SwitchC-bgp] quit
```

配置 Switch D，启动 BGP，并设置其 Router ID 为 4.4.4.4。

```
<SwitchD> system-view
```

```
[SwitchD] bgp 65009
```

```
[SwitchD-bgp] router-id 4.4.4.4
```

```
[SwitchD-bgp] peer 9.1.1.1 as-number 65009
```

```
[SwitchD-bgp] peer 9.1.2.1 as-number 65009
```

```
[SwitchD-bgp] quit
```

(3) 配置 EBGP 连接

配置 Switch A，启动 BGP，并设置其 Router ID 为 1.1.1.1。

```
<SwitchA> system-view
```

```
[SwitchA] bgp 65008
```

```
[SwitchA-bgp] router-id 1.1.1.1
```

```
[SwitchA-bgp] peer 200.1.1.1 as-number 65009
```

将 8.0.0.0/8 网段路由通告到 BGP 路由表中。

```
[SwitchA-bgp] network 8.0.0.0
```

```
[SwitchA-bgp] quit
```

配置 Switch B。

```
[SwitchB] bgp 65009
```

```
[SwitchB-bgp] peer 200.1.1.2 as-number 65008
```

```
[SwitchB-bgp] quit
```

查看 Switch B 的 BGP 对等体的连接状态。

```
[SwitchB] display bgp peer
```

```
BGP local router ID : 2.2.2.2
```

```
Local AS number : 65009
```

```
Total number of peers : 3                Peers in established state : 3
```

Peer	V	AS	MsgRcvd	MsgSent	OutQ	PrefRcv	Up/Down	State
9.1.1.2	4	65009	56	56	0	0	00:40:54	Established
9.1.3.2	4	65009	49	62	0	0	00:44:58	Established
200.1.1.2	4	65008	49	65	0	1	00:44:03	Established

可以看出，Switch B 到其他交换机的 BGP 连接均已建立。

查看 Switch A 路由表信息。

```
[SwitchA] display bgp routing-table
```

```
Total Number of Routes: 1

BGP Local router ID is 1.1.1.1
Status codes: * - valid, > - best, d - damped,
              h - history, i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete
Network      NextHop      MED      LocPrf    PrefVal Path/Ogn

*> 8.0.0.0      0.0.0.0      0          0          i
```

查看 Switch B 的路由表。

```
[SwitchB] display bgp routing-table
Total Number of Routes: 1

BGP Local router ID is 2.2.2.2
Status codes: * - valid, > - best, d - damped,
              h - history, i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete
Network      NextHop      MED      LocPrf    PrefVal Path/Ogn

*> 8.0.0.0      200.1.1.2    0          0          65008i
```

查看 Switch C 的路由表。

```
[SwitchC] display bgp routing-table
Total Number of Routes: 1

BGP Local router ID is 3.3.3.3
Status codes: * - valid, > - best, d - damped,
              h - history, i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete
Network      NextHop      MED      LocPrf    PrefVal Path/Ogn

i 8.0.0.0      200.1.1.2    0          100        0          65008i
```



说明

从路由表可以看出，Switch A 没有学到 AS 65009 内部的任何路由，Switch C 虽然学到了 AS 65008 中的 8.0.0.0 的路由，但因为下一跳 200.1.1.2 不可达，所以也不是有效路由。

(4) 配置 BGP 引入直连路由

配置 Switch B。

```
[SwitchB] bgp 65009
[SwitchB-bgp] import-route direct

# 显示 Switch A 的 BGP 路由表。

[SwitchA] display bgp routing-table
```

```
Total Number of Routes: 4
```

```
BGP Local router ID is 1.1.1.1
```

```
Status codes: * - valid, > - best, d - damped,
```

```
h - history, i - internal, s - suppressed, S - Stale
```

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

	Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
*>	8.0.0.0	0.0.0.0	0	0		i
*>	9.1.1.0/24	200.1.1.1	0	0	65009?	
*>	9.1.3.0/24	200.1.1.1	0	0	65009?	
*	200.1.1.0	200.1.1.1	0	0	65009?	

显示 Switch C 的路由表。

```
[SwitchC] display bgp routing-table
```

```
Total Number of Routes: 4
```

```
BGP Local router ID is 3.3.3.3
```

```
Status codes: * - valid, > - best, d - damped,
```

```
h - history, i - internal, s - suppressed, S - Stale
```

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

	Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
*>i	8.0.0.0	200.1.1.2	0	100	0	65008i
*>i	9.1.1.0/24	9.1.3.1	0	100	0	?
* i	9.1.3.0/24	9.1.3.1	0	100	0	?
*>i	200.1.1.0	9.1.3.1	0	100	0	?

可以看出，到 8.0.0.0 的路由变为有效路由，下一跳为 Switch A 的地址。

使用 Ping 进行验证。

```
[SwitchC] ping 8.1.1.1
```

```
PING 8.1.1.1: 56 data bytes, press CTRL_C to break
```

```
Reply from 8.1.1.1: bytes=56 Sequence=1 ttl=254 time=31 ms
```

```
Reply from 8.1.1.1: bytes=56 Sequence=2 ttl=254 time=47 ms
```

```
Reply from 8.1.1.1: bytes=56 Sequence=3 ttl=254 time=31 ms
```

```
Reply from 8.1.1.1: bytes=56 Sequence=4 ttl=254 time=16 ms
```

```
Reply from 8.1.1.1: bytes=56 Sequence=5 ttl=254 time=31 ms
```

```
--- 8.1.1.1 ping statistics ---
```

```
5 packet(s) transmitted
```

```
5 packet(s) received
```

```
0.00% packet loss
```

```
round-trip min/avg/max = 16/31/47 ms
```

1.20.5 完整配置

- 配置 Switch A

#

```

vlan 100
#
vlan 200
#
interface Vlan-interface100
 ip address 8.1.1.1 255.0.0.0
#
interface Vlan-interface200
 ip address 200.1.1.2 255.255.255.0
#
bgp 65008
 router-id 1.1.1.1
 network 8.0.0.0
 undo synchronization
 peer 200.1.1.1 as-number 65009
#

```

- 配置 Switch B

```

#
vlan 200
#
vlan 300
#
vlan 400
#
interface Vlan-interface200
 ip address 200.1.1.1 255.255.255.0
#
interface Vlan-interface300
 ip address 9.1.3.1 255.255.255.0
#
interface Vlan-interface400
 ip address 9.1.1.1 255.255.255.0
#
bgp 65009
 router-id 2.2.2.2
 import-route direct
 undo synchronization
 peer 9.1.1.2 as-number 65009
 peer 200.1.1.2 as-number 65008
 peer 9.1.3.2 as-number 65009
#

```

- 配置 Switch C

```

#
vlan 300
#
vlan 500
#
interface Vlan-interface300

```

```

ip address 9.1.3.2 255.255.255.0
#
interface Vlan-interface500
ip address 9.1.2.1 255.255.255.0
#
bgp 65009
router-id 3.3.3.3
undo synchronization
peer 9.1.2.2 as-number 65009
peer 9.1.3.1 as-number 65009
#

```

• 配置 Switch D

```

#
vlan 400
#
vlan 500
#
interface Vlan-interface400
ip address 9.1.1.2 255.255.255.0
#
interface Vlan-interface500
ip address 9.1.2.2 255.255.255.0
#
bgp 65009
router-id 4.4.4.4
undo synchronization
peer 9.1.1.1 as-number 65009
peer 9.1.2.1 as-number 65009
#

```

1.20.6 配置注意事项

- 一台路由器如果要运行 BGP 协议，则必须存在 Router ID。Router ID 是一个 32 比特无符号整数，是一台路由器在自治系统中的唯一标识。
- 如果对等体和对等体组都对某个选项做了配置，配置以最后一次的修改为准。
- 由于 BGP 使用 TCP 连接，所以在配置 BGP 时需要指定对等体的 IP 地址。BGP 对等体不一定就是相邻的路由器，利用逻辑链路也可以建立 BGP 对等体关系。有时为了增强 BGP 连接的稳定性，通常使用 Loopback 接口地址建立连接。
- 路由器的 Router ID 可以手工配置，如果没有通过命令指定 Router ID，系统会从当前接口的 IP 地址中自动选取一个作为路由器的 Router ID。其选择顺序是：优先从 Loopback 接口中选择最大的 IP 地址作为路由器的 Router ID，如果没有配置 Loopback 接口，则选取接口中最大的 IP 地址作为路由器的 Router ID。只有在路由器的 Router ID 所在接口被删除或去除手工配置的 Router ID 的情况下才会重新选择路由器的 Router ID。为了增加网络的可靠性，建议将 Router ID 手工配置为 Loopback 接口的 IP 地址。

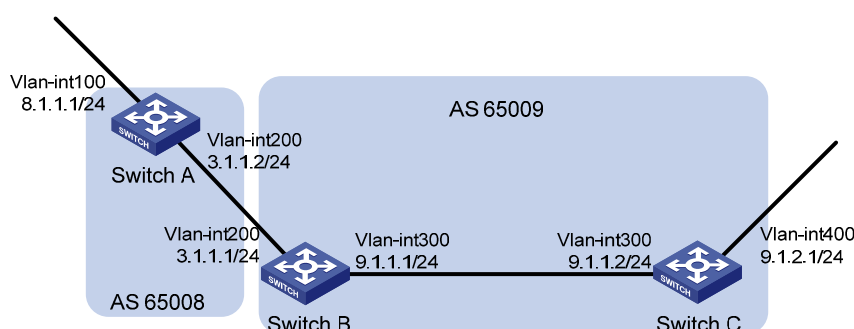
- 当两个设备之间建立多条 BGP 连接时，如果没有明确指定建立 TCP 连接的源接口，可能会由于无法根据到达 BGP 对等体的最优路由确定 TCP 连接源接口从而导致无法建立 TCP 连接，因此建议用户在此情况下配置 BGP 对等体时明确配置 BGP 会话建立 TCP 连接的源接口为指定接口。
- 通常情况下，EBGP 对等体之间必须具有直连的物理链路，如果不满足这一要求，则必须使用 peer ebgp-max-hop 命令允许它们之间经过多跳建立 TCP 连接。但是，对于直连 EBGP 使用 LoopBack 接口建立邻居关系，不需要 peer ebgp-max-hop 命令的配置。
- 创建 IBGP 对等体组不需要指定 AS 号。
- 如果对等体组中已经存在对等体，则不能改变该对等体组的 AS 号，也不能使用 undo 命令删除已指定的自治系统号。
- 在混合 EBGP 对等体组中，需要单独指定各对等体的 AS 号。

1.21 BGP 与 IGP 交互典型配置指导

BGP 可以向邻居 AS 发送本地 AS 内部网络的路由信息，但 BGP 不是自己去发现 AS 内部的路由信息，而是引入 IGP 的路由信息到 BGP 路由表中，并发布给对等体。在引入 IGP 路由时，还可以针对不同的路由协议来对路由信息进行过滤。

1.21.1 组网图

图1-21 BGP 与 IGP 交互配置组网图



1.21.2 应用要求

- 在 AS 65009 内使用 OSPF 作为 IGP 协议；
- Switch A 和 Switch B 建立 EBGP 连接，Switch C 为 AS 内部的一台非 BGP 交换机。

1.21.3 适用产品、版本

表1-21 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本

产品	软件版本	硬件版本
S7500E 系列以太网交换机	Release 6100, Release 6300 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.21.4 配置过程和解释

(1) 配置各接口的 IP 地址（略）

(2) 配置 OSPF（略）

(3) 配置 EBGP 连接

配置 Switch A，启动 BGP，并设置其 Router ID 为 1.1.1.1。

```
<SwitchA> system-view
[SwitchA] bgp 65008
[SwitchA-bgp] router-id 1.1.1.1
[SwitchA-bgp] peer 3.1.1.1 as-number 65009
```

将 8.1.1.0/24 网段通告到 BGP 路由表中。

```
[SwitchA-bgp] network 8.1.1.0 24
[SwitchA-bgp] quit
```

配置 Switch B，启动 BGP，并设置其 Router ID 为 2.2.2.2。

```
<SwitchB> system-view
[SwitchB] bgp 65009
[SwitchB-bgp] router-id 2.2.2.2
[SwitchB-bgp] peer 3.1.1.2 as-number 65008
[SwitchB-bgp] quit
```

(4) 配置 BGP 与 IGP 交互

在 Switch B 上配置 BGP 引入 OSPF 路由。

```
[SwitchB] bgp 65009
[SwitchB-bgp] import-route ospf 1
[SwitchB-bgp] quit
```

查看 Switch A 的路由表。

```
[SwitchA] display bgp routing-table
```

```
Total Number of Routes: 3

BGP Local router ID is 1.1.1.1
Status codes: * - valid, > - best, d - damped,
              h - history, i - internal, s - suppressed, S - Stale
Origin : i - IGP, e - EGP, ? - incomplete

   Network          NextHop      MED       LocPrf   PrefVal Path/Ogn
-----
*>  8.1.1.0/24       0.0.0.0        0           0         i
*>  9.1.1.0/24       3.1.1.1        0           0        65009?
*>  9.1.2.0/24       3.1.1.1        2           0        65009?
```


在 Switch B 上配置 OSPF 引入 BGP 路由。

```
[SwitchB] ospf
[SwitchB-ospf-1] import-route bgp
[SwitchB-ospf-1] quit
```

显示 Switch C 的路由表。

```
<SwitchC> display ip routing-table
Routing Tables: Public
    Destinations : 7          Routes : 7

Destination/Mask    Proto   Pre  Cost   NextHop         Interface
-----
8.1.1.0/24          0_ASE   150   1       9.1.1.1         Vlan300
9.1.1.0/24          Direct  0      0       9.1.1.2         Vlan300
9.1.1.2/32          Direct  0      0       127.0.0.1       InLoop0
9.1.2.0/24          Direct  0      0       9.1.2.1         Vlan400
9.1.2.1/32          Direct  0      0       127.0.0.1       InLoop0
127.0.0.0/8         Direct  0      0       127.0.0.1       InLoop0
127.0.0.1/32        Direct  0      0       127.0.0.1       InLoop0
```

(5) 配置路由自动聚合

配置 Switch B。

```
[SwitchB] bgp 65009
[SwitchB-bgp] summary automatic
```

显示 Switch A 的 BGP 路由表。

```
[SwitchA] display bgp routing-table

Total Number of Routes: 2

BGP Local router ID is 1.1.1.1
Status codes: * - valid, > - best, d - damped,
              h - history, i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete
   Network          NextHop         MED         LocPrf        PrefVal Path/Ogn
-----
*>  8.1.1.0/24      0.0.0.0          0           0             i
*>  9.0.0.0         3.1.1.1          0           0             65009?
```

使用 Ping 进行验证。

```
[SwitchA] ping -a 8.1.1.1 9.1.2.1
PING 9.1.2.1: 56 data bytes, press CTRL_C to break
  Reply from 9.1.2.1: bytes=56 Sequence=1 ttl=254 time=15 ms
  Reply from 9.1.2.1: bytes=56 Sequence=2 ttl=254 time=31 ms
  Reply from 9.1.2.1: bytes=56 Sequence=3 ttl=254 time=47 ms
  Reply from 9.1.2.1: bytes=56 Sequence=4 ttl=254 time=46 ms
  Reply from 9.1.2.1: bytes=56 Sequence=5 ttl=254 time=47 ms

--- 9.1.2.1 ping statistics ---
```

```
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 15/37/47 ms
```

1.21.5 完整配置

- 配置 Switch A

```
#
vlan 100
#
vlan 200
#
interface Vlan-interface100
 ip address 8.1.1.1 255.255.255.0
#
interface Vlan-interface200
 ip address 3.1.1.2 255.255.255.0
#
bgp 65008
 router-id 1.1.1.1
 network 8.1.1.0 255.255.255.0
 undo synchronization
 peer 3.1.1.1 as-number 65009
#
```

- 配置 Switch B

```
#
vlan 200
#
vlan 300
#
interface Vlan-interface200
 ip address 3.1.1.1 255.255.255.0
#
interface Vlan-interface300
 ip address 9.1.1.1 255.255.255.0
#
bgp 65009
 router-id 2.2.2.2
 summary automatic
 import-route ospf 1
 undo synchronization
 peer 3.1.1.2 as-number 65008
#
ospf 1
 import-route bgp
 area 0.0.0.0
 network 9.1.1.0 0.0.0.255
#
```

- 配置 Switch C

```
#
vlan 300
#
vlan 400
#
interface Vlan-interface300
 ip address 9.1.1.2 255.255.255.0
#
interface Vlan-interface400
 ip address 9.1.2.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
 network 9.1.1.0 0.0.0.255
 network 9.1.2.0 0.0.0.255
#
```

1.21.6 配置注意事项

- 通过 import-route 命令引入到 BGP 路由表中的路由的 ORIGIN 属性为 Incomplete。
- 使用 network 命令发布到 BGP 路由表中的网段路由的 ORIGIN 属性为 IGP。
- 要发布的网段路由必须存在于本地的 IP 路由表中，使用路由策略可以更为灵活的控制所发布的路由。

1.22 BGP 负载分担典型配置指导

基于迭代的 BGP 负载分担，即如果依赖路由本身是负载分担的（假设有三个下一跳地址），则 BGP 也会生成相同数量的下一跳地址来指导报文转发。需要说明的是，基于迭代的 BGP 负载分担并不需要命令配置，这一特性在交换机上始终启用。

在实现方法上，BGP 的负载分担与 IGP 的负载分担有所不同：

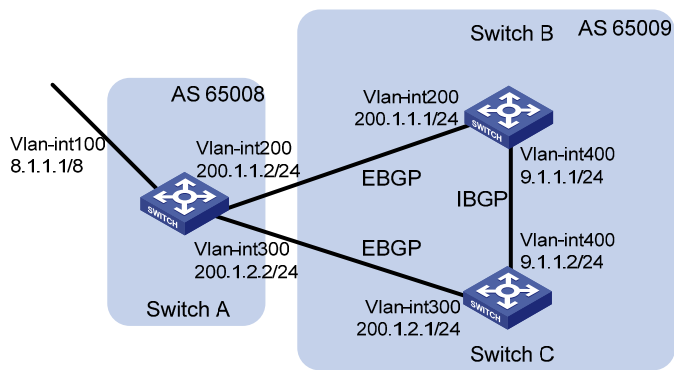
- IGP 是通过协议定义的路由算法，对到达同一目的地址的不同路由，根据计算结果，将度量值（metric）相等的（如 RIP、OSPF）路由进行负载分担，选择的标准很明确（按 metric）。
- BGP 本身并没有路由计算的算法，它只是一个选路的路由协议，因此，不能根据一个明确的度量值决定是否对路由进行负载分担，但 BGP 有丰富的选路规则，可以在对路由进行一定的选择后，有条件地进行负载分担，也就是将负载分担加入到 BGP 的选路规则中去。

MED 属性仅在相邻两个 AS 之间交换，收到此属性的 AS 一方不会再将其通告给任何其他第三方 AS。

MED 属性相当于 IGP 使用的度量值（metrics），它用于判断流量进入 AS 时的最佳路由。当一个运行 BGP 的路由器通过不同的 EBGP 对等体得到目的地址相同但下一跳不同的多条路由时，在其它条件相同的情况下，将优先选择 MED 值较小者作为最佳路由。

1.22.1 组网图

图1-22 配置 BGP 路径选择的组网图



1.22.2 应用要求

- 所有交换机都配置 BGP，Switch A 在 AS 65008 中，Switch B 和 Switch C 在 AS 65009 中。
- Switch A 与 Switch B、Switch C 之间运行 EBGP，Switch B 和 Switch C 之间运行 IBGP。
- 在 Switch A 上配置负载分担的路由条数为 2，以提高链路利用率。

1.22.3 适用产品、版本

表1-22 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6100, Release 6300 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.22.4 配置过程和解释

- (1) 配置各接口的 IP 地址（略）
- (2) 配置 BGP 连接

配置 Switch A，启动 BGP，并设置其 Router ID 为 1.1.1.1。

```
<SwitchA> system-view
[SwitchA] bgp 65008
[SwitchA-bgp] router-id 1.1.1.1
[SwitchA-bgp] peer 200.1.1.1 as-number 65009
[SwitchA-bgp] peer 200.1.2.1 as-number 65009

# 将 8.0.0.0/8 网段路由通告到 BGP 路由表中。

[SwitchA-bgp] network 8.0.0.0 255.0.0.0
[SwitchA-bgp] quit
```

配置 Switch B，启动 BGP，并设置其 Router ID 为 2.2.2.2。

```
<SwitchB> system-view
[SwitchB] bgp 65009
[SwitchB-bgp] router-id 2.2.2.2
[SwitchB-bgp] peer 200.1.1.2 as-number 65008
[SwitchB-bgp] peer 9.1.1.2 as-number 65009
[SwitchB-bgp] network 9.1.1.0 255.255.255.0
[SwitchB-bgp] quit
```

配置 Switch C，启动 BGP，并设置其 Router ID 为 3.3.3.3。

```
<SwitchC> system-view
[SwitchC] bgp 65009
[SwitchC-bgp] router-id 3.3.3.3
[SwitchC-bgp] peer 200.1.2.2 as-number 65008
[SwitchC-bgp] peer 9.1.1.1 as-number 65009
[SwitchC-bgp] network 9.1.1.0 255.255.255.0
[SwitchC-bgp] quit
```

查看 Switch A 的路由表。

```
[SwitchA] display bgp routing-table
```

```
Total Number of Routes: 3
```

```
BGP Local router ID is 1.1.1.1
```

```
Status codes: * - valid, > - best, d - damped,
```

```
h - history, i - internal, s - suppressed, S - Stale
```

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

	Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
*>	8.0.0.0	0.0.0.0	0	0		i
*>	9.1.1.0/24	200.1.1.1	0	0	65009i	
*		200.1.2.1	0	0	65009i	

从路由表中可以看出，到目的地址 9.1.1.0/24 有两条有效路由，其中下一跳为 200.1.1.1 的路由是最优路由（因为 Switch B 的路由器 ID 要小一些）。

(3) 配置负载分担

配置 Switch A。

```
[SwitchA] bgp 65008
[SwitchA-bgp] balance 2
[SwitchA-bgp] quit
```

查看 Switch A 的路由表。

```
[SwitchA] display bgp routing-table
```

```
Total Number of Routes: 3
```

```
BGP Local router ID is 1.1.1.1
```

```
Status codes: * - valid, > - best, d - damped,
```

h - history, i - internal, s - suppressed, S - Stale					
Origin : i - IGP, e - EGP, ? - incomplete					
Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
*> 8.0.0.0	0.0.0.0	0	0	i	
*> 9.1.1.0/24	200.1.1.1	0	0	65009i	
*>	200.1.2.1	0	0	65009i	

从路由表中可以看到，BGP 路由 9.1.1.0/24 存在两个下一跳，分别是 200.1.1.1 和 200.1.2.1，且都是最优路由。

1.22.5 完整配置

- 配置 Switch A

```
#
vlan 100
#
vlan 200
#
vlan 300
#
interface Vlan-interface100
 ip address 8.1.1.1 255.0.0.0
#
interface Vlan-interface200
 ip address 200.1.1.2 255.255.255.0
#
interface Vlan-interface300
 ip address 200.1.2.2 255.255.255.0
#
bgp 65008
 router-id 1.1.1.1
 network 8.0.0.0
 undo synchronization
 balance 2
 peer 200.1.1.1 as-number 65009
 peer 200.1.2.1 as-number 65009
#
```

- 配置 Switch B

```
#
vlan 200
#
vlan 400
#
interface Vlan-interface200
 ip address 200.1.1.1 255.255.255.0
#
interface Vlan-interface400
 ip address 9.1.1.1 255.255.255.0
```

```
#
bgp 65009
router-id 2.2.2.2
network 9.1.1.0 255.255.255.0
undo synchronization
peer 200.1.1.2 as-number 65008
peer 9.1.1.2 as-number 65009
#
```

- 配置 Switch C

```
#
vlan 300
#
vlan 400
#
interface Vlan-interface300
ip address 200.1.2.1 255.255.255.0
#
interface Vlan-interface400
ip address 9.1.1.2 255.255.255.0
#
bgp 65009
router-id 3.3.3.3
network 9.1.1.0 255.255.255.0
undo synchronization
peer 9.1.1.1 as-number 65009
peer 200.1.2.2 as-number 65008
#
```

1.22.6 配置注意事项

- BGP 只对 AS_PATH 属性、ORIGIN 属性、LOCAL_PREF 和 MED 值完全相同的路由进行负载分担。
- BGP 负载分担特性适用于 EBGP、IBGP 以及联盟之间。
- 如果有多条到达同一目的地的路由，则根据配置的路由条数选择多条路由进行负载分担。

1.23 BGP 团体典型配置指导

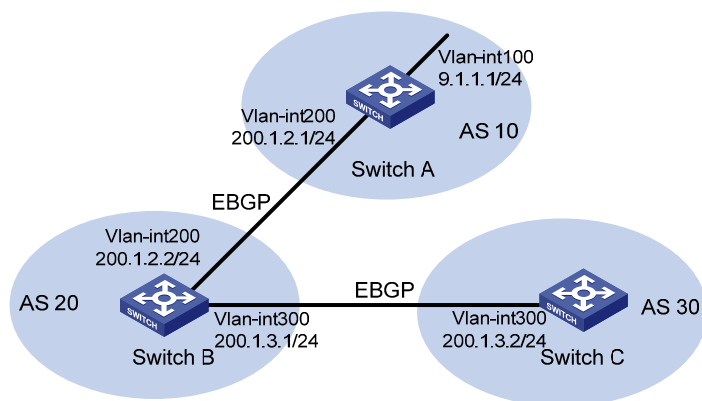
对等体组可以使一组对等体共享相同的策略，而利用团体可以使多个 AS 中的一组 BGP 路由器共享相同的策略。团体是一个路由属性，在 BGP 对等体之间传播，它并不受到 AS 范围的限制。

BGP 路由器在将带有团体属性的路由发布给其它对等体之前，可以改变此路由原有的团体属性。

除了使用公认的团体属性外，用户还可以使用团体属性列表自定义扩展团体属性，以便更为灵活地控制路由策略。

1.23.1 组网图

图1-23 BGP 团体组网图



1.23.2 应用要求

- Switch B 分别与 Switch A、Switch C 之间建立 EBGP 连接。
- 通过在 Switch A 上配置 NO_EXPORT 团体属性，使得 AS 10 发布到 AS 20 中的路由，不再被 AS 20 向其他 AS 发布。

1.23.3 适用产品、版本

表1-23 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6100, Release 6300 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.23.4 配置过程和解释

(1) 配置各接口的 IP 地址（略）

(2) 配置 EBGP

配置 Switch A，启动 BGP，并设置其 Router ID 为 1.1.1.1。

```
<SwitchA> system-view
[SwitchA] bgp 10
[SwitchA-bgp] router-id 1.1.1.1
[SwitchA-bgp] peer 200.1.2.2 as-number 20
[SwitchA-bgp] network 9.1.1.0 255.255.255.0
[SwitchA-bgp] quit
```

配置 Switch B，启动 BGP，并设置其 Router ID 为 2.2.2.2。


```
<SwitchB> system-view
```

```
[SwitchB] bgp 20
```

```
[SwitchB-bgp] router-id 2.2.2.2
```

```
[SwitchB-bgp] peer 200.1.2.1 as-number 10
```

```
[SwitchB-bgp] peer 200.1.3.2 as-number 30
```

```
[SwitchB-bgp] quit
```

配置 Switch C，启动 BGP，并设置其 Router ID 为 3.3.3.3。

```
<SwitchC> system-view
```

```
[SwitchC] bgp 30
```

```
[SwitchC-bgp] router-id 3.3.3.3
```

```
[SwitchC-bgp] peer 200.1.3.1 as-number 20
```

```
[SwitchC-bgp] quit
```

查看 Switch B 的路由表。

```
[SwitchB] display bgp routing-table 9.1.1.0
```

```
BGP local router ID : 2.2.2.2
```

```
Local AS number : 20
```

```
Paths: 1 available, 1 best
```

```
BGP routing table entry information of 9.1.1.0/24:
```

```
From : 200.1.2.1 (1.1.1.1)
```

```
Original nexthop: 200.1.2.1
```

```
AS-path : 10
```

```
Origin : igp
```

```
Attribute value : MED 0, pref-val 0, pre 255
```

```
State : valid, external, best,
```

```
Advertised to such 1 peers:
```

```
200.1.3.2
```

可以看出，Switch B 把收到的路由发布给了位于 AS 30 内的 Switch C。

查看 Switch C 的路由表。

```
[SwitchC] display bgp routing-table
```

```
Total Number of Routes: 1
```

```
BGP Local router ID is 3.3.3.3
```

```
Status codes: * - valid, > - best, d - damped,
```

```
h - history, i - internal, s - suppressed, S - Stale
```

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

Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn

*> 9.1.1.0/24	200.1.3.1		0	20	10i

从路由表可以确认，Switch C 从 Switch B 那里学到了目的地址为 9.1.1.0/24 的路由。

(3) 配置 BGP 团体属性

配置路由策略。

```
[SwitchA] route-policy comm_policy permit node 0
```

```
[SwitchA-route-policy] apply community no-export
[SwitchA-route-policy] quit
# 应用路由策略。

[SwitchA] bgp 10
[SwitchA-bgp] peer 200.1.2.2 route-policy comm_policy export
[SwitchA-bgp] peer 200.1.2.2 advertise-community
# 查看 Switch B 的路由表。

[SwitchB] display bgp routing-table 9.1.1.0
BGP local router ID : 2.2.2.2
Local AS number : 20
Paths: 1 available, 1 best

BGP routing table entry information of 9.1.1.0/24:
From : 200.1.2.1 (1.1.1.1)
Original nexthop: 200.1.2.1
Community : No-Export
AS-path : 10
Origin : igp
Attribute value : MED 0, pref-val 0, pre 255
State : valid, external, best,
Not advertised to any peers yet
```

在 Switch B 的 BGP 路由表中可以看到配置的团体属性。此时在 Switch C 的 BGP 路由表中已经没有到目的地址 9.1.1.0/24 的路由。

1.23.5 完整配置

- 配置 Switch A

```
#
vlan 100
#
vlan 200
#
interface Vlan-interface100
ip address 9.1.1.1 255.255.255.0
#
interface Vlan-interface200
ip address 200.1.2.1 255.255.255.0
#
bgp 10
router-id 1.1.1.1
network 9.1.1.0 255.255.255.0
undo synchronization
peer 200.1.2.2 as-number 20
peer 200.1.2.2 route-policy comm_policy export
peer 200.1.2.2 advertise-community
#
```

```

route-policy comm_policy permit node 0
  apply community no-export
#
• 配置 Switch B
#
vlan 200
#
vlan 300
#
interface Vlan-interface200
  ip address 200.1.2.2 255.255.255.0
#
interface Vlan-interface300
  ip address 200.1.3.1 255.255.255.0
#
bgp 20
  router-id 2.2.2.2
  undo synchronization
  peer 200.1.2.1 as-number 10
  peer 200.1.3.2 as-number 30
#
• 配置 Switch C
#
vlan 300
#
interface Vlan-interface300
  ip address 200.1.3.2 255.255.255.0
#
bgp 30
  router-id 3.3.3.3
  undo synchronization
  peer 200.1.3.1 as-number 20
#

```

1.23.6 配置注意事项

配置 BGP 团体时，必须使用路由策略来定义具体的团体属性，然后在发布路由信息时应用此路由策略。

1.24 BGP 路由反射器典型配置指导

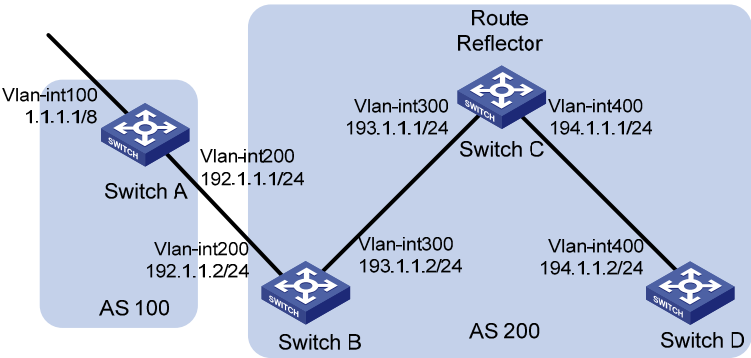
为保证 IBGP 对等体之间的连通性，需要在 IBGP 对等体之间建立全连接关系。假设在一个 AS 内部有 n 台路由器，那么应该建立的 IBGP 连接数就为 $n(n-1)/2$ 。当 IBGP 对等体数目很多时，对网络资源和 CPU 资源的消耗都很大。

利用路由反射可以解决这一问题。在一个 AS 内，其中一台路由器作为路由反射器 RR（Router Reflector），其它路由器做为客户机（Client）与路由反射器之间建立 IBGP 连接。路由反射器在客户机之间传递（反射）路由信息，而客户机之间不需要建立 BGP 连接。

既不是反射器也不是客户机的 BGP 路由器被称为非客户机（Non-Client）。非客户机与路由反射器之间，以及所有的非客户机之间仍然必须建立全连接关系。

1.24.1 组网图

图1-24 配置 BGP 路由反射器的组网图



1.24.2 应用要求

- 所有交换机运行 BGP 协议，Switch A 与 Switch B 建立 EBGP 连接，Switch C 与 Switch B 和 Switch D 之间建立 IBGP 连接。
- Switch C 作为路由反射器，Switch B 和 Switch D 为 Switch C 的客户机。
- Switch D 能够通过 Switch C 学到路由 1.0.0.0/8。

1.24.3 适用产品、版本

表1-24 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6100, Release 6300 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.24.4 配置过程和解释

- (1) 配置各接口的 IP 地址（略）
- (2) 配置 BGP 连接
- # 配置 Switch A，启动 BGP，并设置其 Router ID 为 1.1.1.1。
- ```
<SwitchA> system-view
[SwitchA] bgp 100
[SwitchA-bgp] router-id 1.1.1.1
[SwitchA-bgp] peer 192.1.1.2 as-number 200
```
- # 通告 1.0.0.0/8 网段路由到 BGP 路由表中。

```
[SwitchA-bgp] network 1.0.0.0
```

```
[SwitchA-bgp] quit
```

# 配置 Switch B，启动 BGP，并设置其 Router ID 为 2.2.2.2。

```
<SwitchB> system-view
```

```
[SwitchB] bgp 200
```

```
[SwitchB-bgp] router-id 2.2.2.2
```

```
[SwitchB-bgp] peer 192.1.1.1 as-number 100
```

```
[SwitchB-bgp] peer 193.1.1.1 as-number 200
```

```
[SwitchB-bgp] peer 193.1.1.1 next-hop-local
```

```
[SwitchB-bgp] quit
```

# 配置 Switch C，启动 BGP，并设置其 Router ID 为 3.3.3.3。

```
<SwitchC> system-view
```

```
[SwitchC] bgp 200
```

```
[SwitchC-bgp] router-id 3.3.3.3
```

```
[SwitchC-bgp] peer 193.1.1.2 as-number 200
```

```
[SwitchC-bgp] peer 194.1.1.2 as-number 200
```

```
[SwitchC-bgp] quit
```

# 配置 Switch D，启动 BGP，并设置其 Router ID 为 4.4.4.4。

```
<SwitchD> system-view
```

```
[SwitchD] bgp 200
```

```
[SwitchD-bgp] router-id 4.4.4.4
```

```
[SwitchD-bgp] peer 194.1.1.1 as-number 200
```

```
[SwitchD-bgp] quit
```

### (3) 配置路由反射器

# 配置 Switch C。

```
[SwitchC] bgp 200
```

```
[SwitchC-bgp] peer 193.1.1.2 reflect-client
```

```
[SwitchC-bgp] peer 194.1.1.2 reflect-client
```

```
[SwitchC-bgp] quit
```

### (4) 验证配置效果

# 查看 Switch B 的 BGP 路由表。

```
[SwitchB] display bgp routing-table
```

```
Total Number of Routes: 1
```

```
BGP Local router ID is 2.2.2.2
```

```
Status codes: * - valid, > - best, d - damped,
```

```
h - history, i - internal, s - suppressed, S - Stale
```

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

| Network | NextHop | MED | LocPrf | PrefVal | Path/Ogn |
|---------|---------|-----|--------|---------|----------|
|---------|---------|-----|--------|---------|----------|

|            |           |   |   |      |  |
|------------|-----------|---|---|------|--|
| *> 1.0.0.0 | 192.1.1.1 | 0 | 0 | 100i |  |
|------------|-----------|---|---|------|--|

# 查看 Switch D 的 BGP 路由表。

```
[SwitchD] display bgp routing-table
```

```

Total Number of Routes: 1

BGP Local router ID is 4.4.4.4
Status codes: * - valid, > - best, d - damped,
 h - history, i - internal, s - suppressed, S - Stale
 Origin : i - IGP, e - EGP, ? - incomplete

```

| Network   | NextHop   | MED | LocPrf | PrefVal | Path/Ogn |
|-----------|-----------|-----|--------|---------|----------|
| i 1.0.0.0 | 193.1.1.2 | 0   | 100    | 0       | 100i     |

可以看出，Switch D 从 Switch C 已经学到了 1.0.0.0/8 路由。

### 1.24.5 完整配置

- 配置 Switch A

```

#
vlan 100
#
vlan 200
#
interface Vlan-interface100
 ip address 1.1.1.1 255.0.0.0
#
interface Vlan-interface200
 ip address 192.1.1.1 255.255.255.0
#
bgp 100
 router-id 1.1.1.1
 network 1.0.0.0
 undo synchronization
 peer 192.1.1.2 as-number 200
#

```

- 配置 Switch B

```

#
vlan 200
#
vlan 300
#
interface Vlan-interface200
 ip address 192.1.1.2 255.255.255.0
#
interface Vlan-interface300
 ip address 193.1.1.2 255.255.255.0
#
bgp 200
 router-id 2.2.2.2
 undo synchronization
 peer 192.1.1.1 as-number 100

```

```

peer 193.1.1.1 as-number 200
peer 193.1.1.1 next-hop-local
#
• 配置 Switch C
#
vlan 300
#
vlan 400
#
interface Vlan-interface300
ip address 193.1.1.1 255.255.255.0
#
interface Vlan-interface400
ip address 194.1.1.1 255.255.255.0
#
bgp 200
router-id 3.3.3.3
undo synchronization
peer 193.1.1.2 as-number 200
peer 194.1.1.2 as-number 200
peer 193.1.1.2 reflect-client
peer 194.1.1.2 reflect-client
#
• 配置 Switch D
#
vlan 400
#
interface Vlan-interface400
ip address 194.1.1.2 255.255.255.0
#
bgp 200
router-id 4.4.4.4
undo synchronization
peer 194.1.1.1 as-number 200
#

```

#### 1.24.6 配置注意事项

- 通常情况下，路由反射器的客户之间不要求是全连接的，路由缺省通过反射器从一个客户反射到其它客户；如果客户之间是全连接的，可以禁止客户间的反射，以便减少开销。
- 禁止客户机之间的路由反射后，客户机到非客户机之间的路由仍然可以被反射。
- 通常，一个集群里只有一个路由反射器。此时是由反射器的路由器 ID 来识别该集群的。设置多个路由反射器可提高网络的稳定性。如果一个集群中配有多个路由反射器，请使用相关命令为所有的路由反射器配置同样的集群 ID，以避免路由环路。

# 1.25 BGP 联盟典型配置指导

联盟（Confederation）是处理 AS 内部的 IBGP 网络连接激增的另一种方法，它将一个自治系统划分为若干个子自治系统，每个子自治系统内部的 IBGP 对等体建立全连接关系，子自治系统之间建立 EBGP 连接关系。

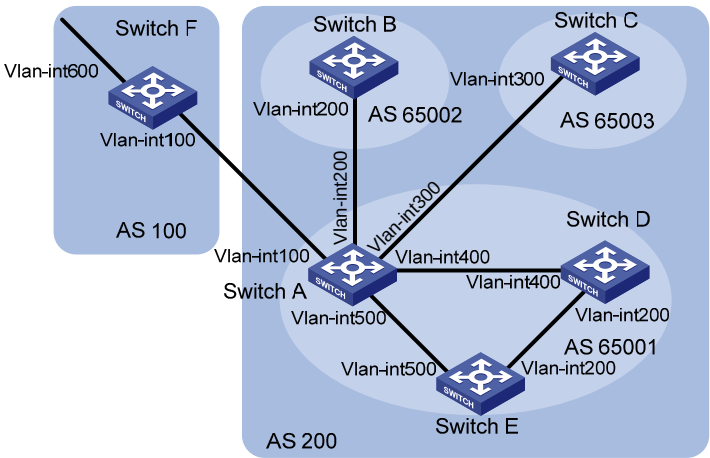
在不属于联盟的 BGP 发言者看来，属于同一个联盟的多个子自治系统是一个整体，外界不需要了解内部的子自治系统情况，联盟 ID 就是标识联盟这一整体的自治系统号。

联盟的缺陷是：从非联盟方案向联盟方案转变时，要求路由器重新进行配置，逻辑拓扑也要改变。

在大型 BGP 网络中，路由反射器和联盟可以被同时使用。

## 1.25.1 组网图

图1-25 配置联盟组网图



| 设备       | 接口          | IP 地址        | 设备       | 接口          | IP 地址        |
|----------|-------------|--------------|----------|-------------|--------------|
| Switch A | Vlan-int100 | 200.1.1.1/24 | Switch D | Vlan-int200 | 10.1.5.1/24  |
|          | Vlan-int200 | 10.1.1.1/24  |          | Vlan-int400 | 10.1.3.2/24  |
|          | Vlan-int300 | 10.1.2.1/24  | Switch E | Vlan-int200 | 10.1.5.2/24  |
|          | Vlan-int400 | 10.1.3.1/24  |          | Vlan-int500 | 10.1.4.2/24  |
|          | Vlan-int500 | 10.1.4.1/24  | Switch F | Vlan-int100 | 200.1.1.2/24 |
| Switch B | Vlan-int200 | 10.1.1.2/24  |          | Vlan-int600 | 9.1.1.1/24   |
| Switch C | Vlan-int300 | 10.1.2.2/24  |          |             |              |

## 1.25.2 应用要求

AS 200 中有多台 BGP 交换机，为了减少 IBGP 的连接数，现将他们划分为 3 个子自治系统：AS 65001、AS 65002 和 AS 65003。其中 AS 65001 内的三台交换机建立 IBGP 全连接。

## 1.25.3 适用产品、版本

表1-25 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本    |
|-------------------|---------------------------------|---------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本 |



| 产品                | 软件版本                            | 硬件版本    |
|-------------------|---------------------------------|---------|
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本 |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本 |

#### 1.25.4 配置过程和解释

(1) 配置各接口的 IP 地址（略）

(2) 配置 BGP 联盟

# 配置 Switch A，启动 BGP，并设置其 Router ID 为 1.1.1.1。

```
<SwitchA> system-view
[SwitchA] bgp 65001
[SwitchA-bgp] router-id 1.1.1.1
[SwitchA-bgp] confederation id 200
[SwitchA-bgp] confederation peer-as 65002 65003
[SwitchA-bgp] peer 10.1.1.2 as-number 65002
[SwitchA-bgp] peer 10.1.1.2 next-hop-local
[SwitchA-bgp] peer 10.1.2.2 as-number 65003
[SwitchA-bgp] peer 10.1.2.2 next-hop-local
[SwitchA-bgp] quit
```

# 配置 Switch B，启动 BGP，并设置其 Router ID 为 2.2.2.2。

```
<SwitchB> system-view
[SwitchB] bgp 65002
[SwitchB-bgp] router-id 2.2.2.2
[SwitchB-bgp] confederation id 200
[SwitchB-bgp] confederation peer-as 65001 65003
[SwitchB-bgp] peer 10.1.1.1 as-number 65001
[SwitchB-bgp] quit
```

# 配置 Switch C，启动 BGP，并设置其 Router ID 为 3.3.3.3。

```
<SwitchC> system-view
[SwitchC] bgp 65003
[SwitchC-bgp] router-id 3.3.3.3
[SwitchC-bgp] confederation id 200
[SwitchC-bgp] confederation peer-as 65001 65002
[SwitchC-bgp] peer 10.1.2.1 as-number 65001
[SwitchC-bgp] quit
```

(3) 配置 AS 65001 内的 IBGP 连接

# 配置 Switch A。

```
[SwitchA] bgp 65001
[SwitchA-bgp] peer 10.1.3.2 as-number 65001
[SwitchA-bgp] peer 10.1.3.2 next-hop-local
[SwitchA-bgp] peer 10.1.4.2 as-number 65001
[SwitchA-bgp] peer 10.1.4.2 next-hop-local
[SwitchA-bgp] quit
```

# 配置 Switch D，启动 BGP，并设置其 Router ID 为 4.4.4.4。

```
<SwitchD> system-view
[SwitchD] bgp 65001
[SwitchD-bgp] router-id 4.4.4.4
[SwitchD-bgp] confederation id 200
[SwitchD-bgp] peer 10.1.3.1 as-number 65001
[SwitchD-bgp] peer 10.1.5.2 as-number 65001
[SwitchD-bgp] quit
```

# 配置 Switch E，启动 BGP，并设置其 Router ID 为 5.5.5.5。

```
<SwitchE> system-view
[SwitchE] bgp 65001
[SwitchE-bgp] router-id 5.5.5.5
[SwitchE-bgp] confederation id 200
[SwitchE-bgp] peer 10.1.4.1 as-number 65001
[SwitchE-bgp] peer 10.1.5.1 as-number 65001
[SwitchE-bgp] quit
```

(4) 配置 AS 100 和 AS 200 之间的 EBGP 连接

# 配置 Switch A。

```
[SwitchA] bgp 65001
[SwitchA-bgp] peer 200.1.1.2 as-number 100
[SwitchA-bgp] quit
```

# 配置 Switch F。

```
<SwitchF> system-view
[SwitchF] bgp 100
[SwitchF-bgp] router-id 6.6.6.6
[SwitchF-bgp] peer 200.1.1.1 as-number 200
[SwitchF-bgp] network 9.1.1.0 255.255.255.0
[SwitchF-bgp] quit
```

(5) 验证配置结果

# 查看 Switch B 的 BGP 路由表。

```
[SwitchB] display bgp routing-table
```

```
Total Number of Routes: 1
```

```
BGP Local router ID is 2.2.2.2
```

```
Status codes: * - valid, > - best, d - damped,
```

```
h - history, i - internal, s - suppressed, S - Stale
```

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

| Network | NextHop | MED | LocPrf | PrefVal | Path/Ogn |
|---------|---------|-----|--------|---------|----------|
|---------|---------|-----|--------|---------|----------|

|                |          |   |     |   |              |
|----------------|----------|---|-----|---|--------------|
| *>i 9.1.1.0/24 | 10.1.1.1 | 0 | 100 | 0 | (65001) 100i |
|----------------|----------|---|-----|---|--------------|

```
[SwitchB] display bgp routing-table 9.1.1.0
```

```
BGP local router ID : 2.2.2.2
```

```
Local AS number : 65002
```

```
Paths: 1 available, 1 best
```

```
BGP routing table entry information of 9.1.1.0/24:
```

```
From : 10.1.1.1 (1.1.1.1)
```

```
Relay Nexthop : 0.0.0.0
```

```
Original nexthop: 10.1.1.1
```

```
AS-path : (65001) 100
```

```
Origin : igp
```

```
Attribute value : MED 0, localpref 100, pref-val 0, pre 255
```

```
State : valid, external-confed, best,
```

```
Not advertised to any peers yet
```

# 查看 Switch D 的 BGP 路由表。

```
[SwitchD] display bgp routing-table
```

```
Total Number of Routes: 1
```

```
BGP Local router ID is 4.4.4.4
```

```
Status codes: * - valid, > - best, d - damped,
```

```
h - history, i - internal, s - suppressed, S - Stale
```

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

| Network | NextHop | MED | LocPrf | PrefVal | Path/Ogn |
|---------|---------|-----|--------|---------|----------|
|---------|---------|-----|--------|---------|----------|

|                |          |   |     |   |      |
|----------------|----------|---|-----|---|------|
| *>i 9.1.1.0/24 | 10.1.3.1 | 0 | 100 | 0 | 100i |
|----------------|----------|---|-----|---|------|

```
[SwitchD] display bgp routing-table 9.1.1.0
```

```
BGP local router ID : 4.4.4.4
```

```
Local AS number : 65001
```

```
Paths: 1 available, 1 best
```

```
BGP routing table entry information of 9.1.1.0/24:
```

```
From : 10.1.3.1 (1.1.1.1)
```

```
Relay Nexthop : 0.0.0.0
```

```
Original nexthop: 10.1.3.1
```

```
AS-path : 100
```

```
Origin : igp
```

```
Attribute value : MED 0, localpref 100, pref-val 0, pre 255
```

```
State : valid, internal, best,
```

```
Not advertised to any peers yet
```

### 1.25.5 完整配置

- 配置 Switch A

```
#
```

```
vlan 100
```

```
#
```

```
vlan 200
```

```
#
```

```
vlan 300
```

```
#
vlan 400
#
vlan 500
#
interface Vlan-interface100
 ip address 200.1.1.1 255.255.255.0
#
interface Vlan-interface200
 ip address 10.1.1.1 255.255.255.0
#
interface Vlan-interface300
 ip address 10.1.2.1 255.255.255.0
#
interface Vlan-interface400
 ip address 10.1.3.1 255.255.255.0
#
interface Vlan-interface500
 ip address 10.1.4.1 255.255.255.0
#
bgp 65001
 router-id 1.1.1.1
 confederation id 200
 confederation peer-as 65002 65003
 undo synchronization
 peer 10.1.4.2 as-number 65001
 peer 10.1.1.2 as-number 65002
 peer 200.1.1.2 as-number 100
 peer 10.1.2.2 as-number 65003
 peer 10.1.3.2 as-number 65001
 peer 10.1.4.2 next-hop-local
 peer 10.1.1.2 next-hop-local
 peer 10.1.2.2 next-hop-local
 peer 10.1.3.2 next-hop-local
#
```

- 配置 Switch B

```
#
vlan 100
#
interface Vlan-interface100
 ip address 10.1.1.2 255.255.255.0
#
bgp 65002
 router-id 2.2.2.2
 confederation id 200
 confederation peer-as 65001 65003
 undo synchronization
 peer 10.1.1.1 as-number 65001
```

- 配置 Switch C

```
#
vlan 100
#
interface Vlan-interface100
 ip address 10.1.2.2 255.255.255.0
#
bgp 65003
 router-id 3.3.3.3
 confederation id 200
 confederation peer-as 65001 65002
 undo synchronization
 peer 10.1.2.1 as-number 65001
#
```

- 配置 Switch D

```
#
vlan 100
#
vlan 200
#
interface Vlan-interface100
 ip address 10.1.3.2 255.255.255.0
#
interface Vlan-interface200
 ip address 10.1.5.1 255.255.255.0
#
bgp 65001
 router-id 4.4.4.4
 confederation id 200
 undo synchronization
 peer 10.1.5.2 as-number 65001
 peer 10.1.3.1 as-number 65001
#
```

- 配置 Switch E

```
#
vlan 100
#
vlan 200
#
interface Vlan-interface100
 ip address 10.1.4.2 255.255.255.0
#
interface Vlan-interface200
 ip address 10.1.5.2 255.255.255.0
#
bgp 65001
 router-id 5.5.5.5
```

```

confederation id 200
undo synchronization
peer 10.1.4.1 as-number 65001
peer 10.1.5.1 as-number 65001
#
• 配置 Switch F
#
vlan 100
#
vlan 200
#
interface Vlan-interface100
ip address 9.1.1.1 255.255.255.0
#
interface Vlan-interface200
ip address 200.1.1.2 255.255.255.0
#
bgp 100
router-id 6.6.6.6
network 9.1.1.0 255.255.255.0
undo synchronization
peer 200.1.1.1 as-number 200
#

```

### 1.25.6 配置注意事项

如果其他路由器的联盟实现机制不同于 RFC 标准，可以使用 **confederation nonstandard** 命令，以便和非标准的设备兼容。

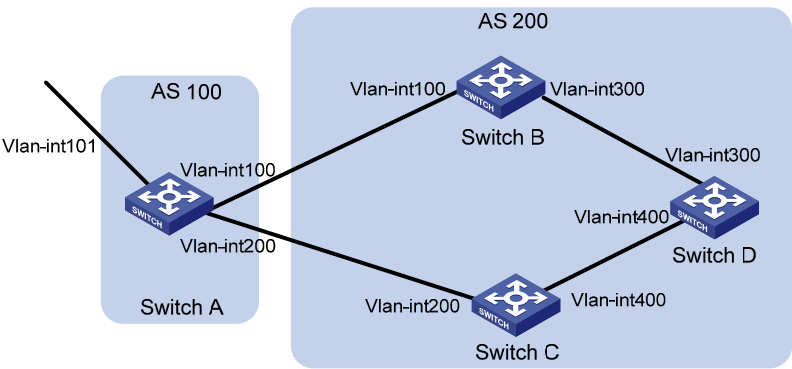
## 1.26 BGP 路径选择典型配置指导

BGP 选择路由时采取如下策略：

- 首先丢弃下一跳（NEXT\_HOP）不可达的路由；
- 优选 Preferred-value 值最大的路由；
- 优选本地优先级（LOCAL\_PREF）最高的路由；
- 优选本路由器始发的路由；
- 优选 AS 路径（AS\_PATH）最短的路由；
- 依次选择 ORIGIN 类型为 IGP、EGP、Incomplete 的路由；
- 优选 MED 值最低的路由；
- 依次选择从 EBGp、联盟、IBGP 学来的路由；
- 优选下一跳 Cost 值最低的路由；
- 优选 CLUSTER\_LIST 长度最短的路由；
- 优选 ORIGINATOR\_ID 最小的路由；
- 优选 Router ID 最小的路由器发布的路由；

1.26.1 组网图

图1-26 配置 BGP 路径选择的组网图



| 设备       | 接口          | IP 地址        | 设备       | 接口          | IP 地址        |
|----------|-------------|--------------|----------|-------------|--------------|
| Switch A | Vlan-int101 | 1.0.0.1/8    | Switch D | Vlan-int400 | 195.1.1.1/24 |
|          | Vlan-int100 | 192.1.1.1/24 |          | Vlan-int300 | 194.1.1.1/24 |
|          | Vlan-int200 | 193.1.1.1/24 | Switch C | Vlan-int400 | 195.1.1.2/24 |
| Switch B | Vlan-int100 | 192.1.1.2/24 |          | Vlan-int200 | 193.1.1.2/24 |
|          | Vlan-int300 | 194.1.1.2/24 |          |             |              |

1.26.2 应用要求

- 所有交换机都运行 BGP 协议。Switch A 与 Switch B 和 Switch C 之间运行 EBGP；Switch D 与 Switch B 和 Switch C 之间运行 IBGP。
- AS 200 中运行 OSPF 协议。
- 配置不同的路由策略，使得 Switch D 优选 Switch C 学到的 1.0.0.0/8 路由。

1.26.3 适用产品、版本

表1-26 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本    |
|-------------------|---------------------------------|---------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本 |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本 |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本 |

1.26.4 配置过程和解释

- 配置各接口的 IP 地址（略）
- 配置 Switch B、Switch C 和 Switch D 之间运行 OSPF 协议

# 配置 Switch B。

```
<SwitchB> system-view
[SwitchB] ospf
[SwitchB-ospf] area 0
```

```
[SwitchB-ospf-1-area-0.0.0.0] network 192.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] network 194.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] quit
```

# 配置 Switch C。

```
<SwitchC> system-view
[SwitchC] ospf
[SwitchC-ospf] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 193.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] network 195.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] quit
[SwitchC-ospf-1] quit
```

# 配置 Switch D。

```
<SwitchD> system-view
[SwitchD] ospf
[SwitchD-ospf] area 0
[SwitchD-ospf-1-area-0.0.0.0] network 194.1.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] network 195.1.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] quit
[SwitchD-ospf-1] quit
```

### (3) 配置 BGP 连接

# 配置 Switch A。

```
<SwitchA> system-view
[SwitchA] bgp 100
[SwitchA-bgp] peer 192.1.1.2 as-number 200
[SwitchA-bgp] peer 193.1.1.2 as-number 200
```

# 将 1.0.0.0/8 网段通告到 Switch A 的 BGP 路由表中。

```
[SwitchA-bgp] network 1.0.0.0 8
[SwitchA-bgp] quit
```

# 配置 Switch B。

```
[SwitchB] bgp 200
[SwitchB-bgp] peer 192.1.1.1 as-number 100
[SwitchB-bgp] peer 194.1.1.1 as-number 200
[SwitchB-bgp] quit
```

# 配置 Switch C。

```
[SwitchC] bgp 200
[SwitchC-bgp] peer 193.1.1.1 as-number 100
[SwitchC-bgp] peer 195.1.1.1 as-number 200
[SwitchC-bgp] quit
```

# 配置 Switch D。

```
[SwitchD] bgp 200
[SwitchD-bgp] peer 194.1.1.2 as-number 200
[SwitchD-bgp] peer 195.1.1.2 as-number 200
[SwitchD-bgp] quit
```



(4) 通过配置 1.0.0.0/8 路由的不同属性值，使得 Switch D 优选 Switch C 学到的路由。

- 在 Switch A 上对发布给对等体 192.1.1.2 的 1.0.0.0/8 路由配置较高的 MED 属性值，使得 Switch D 优选 Switch C 学到的路由。

# 定义编号为 2000 的 ACL，允许路由 1.0.0.0/8 通过。

```
[SwitchA] acl number 2000
[SwitchA-acl-basic-2000] rule permit source 1.0.0.0 0.255.255.255
[SwitchA-acl-basic-2000] quit
```

# 定义两个 Route-policy，一个名为 apply\_med\_50，为路由 1.0.0.0/8 设置 MED 属性值为 50；另一个名为 apply\_med\_100，为路由 1.0.0.0/8 设置 MED 属性值为 100。

```
[SwitchA] route-policy apply_med_50 permit node 10
[SwitchA-route-policy] if-match acl 2000
[SwitchA-route-policy] apply cost 50
[SwitchA-route-policy] quit
[SwitchA] route-policy apply_med_100 permit node 10
[SwitchA-route-policy] if-match acl 2000
[SwitchA-route-policy] apply cost 100
[SwitchA-route-policy] quit
```

# 对发布给对等体 193.1.1.2（SwitchC）的路由应用名为 apply\_med\_50 的 Route-policy，对发布给对等体 192.1.1.2（SwitchB）的路由应用名为 apply\_med\_100 的 Route-policy。

```
[SwitchA] bgp 100
[SwitchA-bgp] peer 193.1.1.2 route-policy apply_med_50 export
[SwitchA-bgp] peer 192.1.1.2 route-policy apply_med_100 export
[SwitchA-bgp] quit
```

# 查看 Switch D 的 BGP 路由表。

```
[SwitchD] display bgp routing-table
```

```
Total Number of Routes: 2

BGP Local router ID is 194.1.1.1
Status codes: * - valid, > - best, d - damped,
 h - history, i - internal, s - suppressed, S - Stale
 Origin : i - IGP, e - EGP, ? - incomplete

 Network NextHop MED LocPrf PrefVal Path/Ogn

*>i 1.0.0.0 193.1.1.1 50 100 0 100i
* i 192.1.1.1 100 100 0 100i
```

可以看到，Switch D 从 Switch C 学到 1.0.0.0/8 的路由是最优的。

- 在 Switch B 和 Switch C 上分别对 1.0.0.0/8 路由配置不同的本地优先级，使得 Switch D 优选 Switch C 学到的路由。

# 在 Switch C 上定义编号为 2000 的 ACL，允许 1.0.0.0/8 路由通过。

```
[SwitchC] acl number 2000
[SwitchC-acl-basic-2000] rule permit source 1.0.0.0 0.255.255.255
[SwitchC-acl-basic-2000] quit
```

# 在 Switch C 上定义名为 localpref 的 Route-policy，设置路由 1.0.0.0/8 的本地优先级为 200（缺省的本地优先级为 100）。

```
[SwitchC] route-policy localpref permit node 10
[SwitchC-route-policy] if-match acl 2000
[SwitchC-route-policy] apply local-preference 200
[SwitchC-route-policy] quit
```

# 为从 BGP 对等体 193.1.1.1 的路由应用名为 localpref 的 Router-policy。

```
[SwitchC] bgp 200
[SwitchC-bgp] peer 193.1.1.1 route-policy localpref import
[SwitchC-bgp] quit
```

# 查看 Switch D 的 BGP 路由表。

```
[SwitchD] display bgp routing-table
```

```
Total Number of Routes: 2

BGP Local router ID is 194.1.1.1
Status codes: * - valid, > - best, d - damped,
 h - history, i - internal, s - suppressed, S - Stale
 Origin : i - IGP, e - EGP, ? - incomplete
 Network NextHop MED LocPrf PrefVal Path/Ogn

*>i 1.0.0.0 193.1.1.1 0 200 0 100i
* i 192.1.1.1 0 100 0 100i
```

可以看到，Switch D 从 Switch C 学到 1.0.0.0/8 的路由是最优的。

### 1.26.5 完整配置

- 配置 Switch A

```
#
vlan 100 to 101
#
vlan 200
#
acl number 2000
 rule 0 permit source 1.0.0.0 0.255.255.255
#
interface Vlan-interface100
 ip address 192.1.1.1 255.255.255.0
#
interface Vlan-interface101
 ip address 1.0.0.1 255.0.0.0
#
interface Vlan-interface200
 ip address 193.1.1.1 255.255.255.0
#
bgp 100
 network 1.0.0.0
```

```

undo synchronization
peer 192.1.1.2 as-number 200
peer 193.1.1.2 as-number 200
peer 192.1.1.2 route-policy apply_med_100 export
peer 193.1.1.2 route-policy apply_med_50 export
#
route-policy apply_med_50 permit node 10
if-match acl 2000
apply cost 50
route-policy apply_med_100 permit node 10
if-match acl 2000
apply cost 100
#

```

- 配置 Switch B

```

#
vlan 100
#
vlan 300
#
interface Vlan-interface100
ip address 192.1.1.2 255.255.255.0
#
interface Vlan-interface300
ip address 194.1.1.2 255.255.255.0
#
bgp 200
undo synchronization
peer 192.1.1.1 as-number 100
peer 194.1.1.1 as-number 200
#
ospf 1
area 0.0.0.0
network 192.1.1.0 0.0.0.255
network 194.1.1.0 0.0.0.255
#

```

- 配置 Switch C

```

#
vlan 200
#
vlan 400
#
acl number 2000
rule 0 permit source 1.0.0.0 0.255.255.255
#
interface Vlan-interface200
ip address 193.1.1.2 255.255.255.0
#
interface Vlan-interface400

```

```

ip address 195.1.1.2 255.255.255.0
#
bgp 200
undo synchronization
peer 193.1.1.1 as-number 100
peer 195.1.1.1 as-number 200
peer 193.1.1.1 route-policy localpref import
#
ospf 1
area 0.0.0.0
network 193.1.1.0 0.0.0.255
network 195.1.1.0 0.0.0.255
#
route-policy localpref permit node 10
if-match acl 2000
apply local-preference 200
#

```

- 配置 Switch D

```

#
vlan 300
#
vlan 400
#
interface Vlan-interface300
ip address 194.1.1.1 255.255.255.0
#
interface Vlan-interface400
ip address 195.1.1.1 255.255.255.0
#
bgp 200
undo synchronization
peer 194.1.1.2 as-number 200
peer 195.1.1.2 as-number 200
#
ospf 1
area 0.0.0.0
network 194.1.1.0 0.0.0.255
network 195.1.1.0 0.0.0.255
#

```

### 1.26.6 配置注意事项

无

## 1.27 在 IPv4 路由引入中应用路由策略典型配置指导

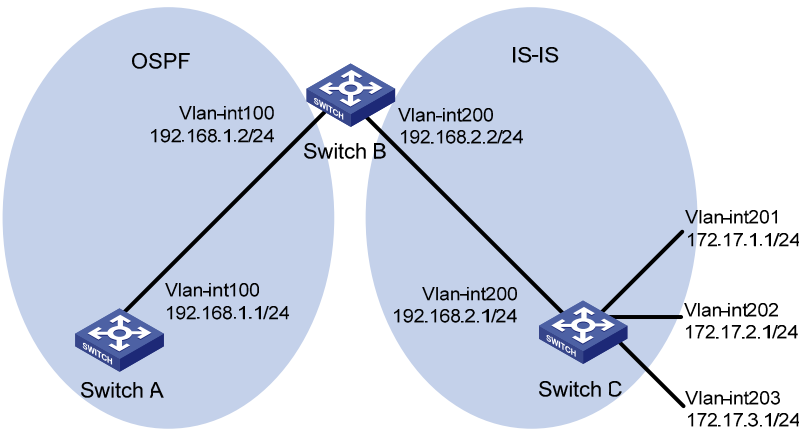
路由策略（Routing Policy）是为了改变网络流量所经过的途径而修改路由信息的技术，主要通过改变路由属性（包括可达性）来实现。

路由器在发布与接收路由信息时，可能需要实施一些策略，以便对路由信息进行过滤，例如只接收或发布满足一定条件的路由信息。一种路由协议可能需要引入其它的路由协议发现的路由信息，路由器在引入其它路由协议的路由信息时，可能只需要引入一部分满足条件的路由信息，并控制所引入的路由信息的某些属性，以使其满足本协议的要求。

为实现路由策略，首先要定义将要实施路由策略的路由信息的特征，即定义一组匹配规则。可以以路由信息中的不同属性作为匹配依据进行设置，如目的地址、发布路由信息的路由器地址等。匹配规则可以预先设置好，然后再将它们应用于路由的发布、接收和引入等过程的路由策略中。

1.27.1 组网图

图1-27 在 IPv4 路由引入中应用路由策略组网图



1.27.2 应用要求

如上图所示，Switch B 与 Switch A 之间通过 OSPF 协议交换路由信息，与 Switch C 之间通过 IS-IS 协议交换路由信息。

要求在 Switch B 上配置路由引入，将 IS-IS 路由引入到 OSPF 中去，并同时使用路由策略设置路由的属性。其中，设置 172.17.1.0/24 的路由的开销为 100，设置 172.17.2.0/24 的路由的 Tag 属性为 20。

1.27.3 适用产品、版本

表1-27 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本    |
|-------------------|---------------------------------|---------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本 |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本 |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本 |

1.27.4 配置过程和解释

- (1) 配置各接口的 IP 地址（略）

## (2) 配置 IS-IS 路由协议

# 配置 Switch C。

```
<SwitchC> system-view
[SwitchC] isis
[SwitchC-isis-1] is-level level-2
[SwitchC-isis-1] network-entity 10.0000.0000.0001.00
[SwitchC-isis-1] quit
[SwitchC] interface vlan-interface 200
[SwitchC-Vlan-interface200] isis enable
[SwitchC-Vlan-interface200] quit
[SwitchC] interface vlan-interface 201
[SwitchC-Vlan-interface201] isis enable
[SwitchC-Vlan-interface201] quit
[SwitchC] interface vlan-interface 202
[SwitchC-Vlan-interface202] isis enable
[SwitchC-Vlan-interface202] quit
[SwitchC] interface vlan-interface 203
[SwitchC-Vlan-interface203] isis enable
[SwitchC-Vlan-interface203] quit
```

# 配置 Switch B。

```
<SwitchB> system-view
[SwitchB] isis
[SwitchB-isis-1] is-level level-2
[SwitchB-isis-1] network-entity 10.0000.0000.0002.00
[SwitchB-isis-1] quit
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] isis enable
[SwitchB-Vlan-interface200] quit
```

## (3) 配置 OSPF 路由协议及路由引入

# 配置 Switch A，启动 OSPF。

```
<SwitchA> system-view
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] quit
```

# 配置 Switch B，启动 OSPF，并引入 IS-IS 路由。

```
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] import-route isis 1
[SwitchB-ospf-1] quit
```

# 查看 SwitchA 的 OSPF 路由表，可以看到引入的路由。

```
[SwitchA] display ospf routing
```

```
OSPF Process 1 with Router ID 192.168.1.1
```

#### Routing Tables

##### Routing for Network

| Destination    | Cost | Type | NextHop     | AdvRouter   | Area    |
|----------------|------|------|-------------|-------------|---------|
| 192.168.1.0/24 | 1562 | Stub | 192.168.1.1 | 192.168.1.1 | 0.0.0.0 |

##### Routing for ASEs

| Destination   | Cost | Type  | Tag | NextHop     | AdvRouter   |
|---------------|------|-------|-----|-------------|-------------|
| 172.17.1.0/24 | 1    | Type2 | 1   | 192.168.1.2 | 192.168.2.2 |
| 172.17.2.0/24 | 1    | Type2 | 1   | 192.168.1.2 | 192.168.2.2 |
| 172.17.3.0/24 | 1    | Type2 | 1   | 192.168.1.2 | 192.168.2.2 |

```
Total Nets: 4
```

```
Intra Area: 1 Inter Area: 0 ASE: 3 NSSA: 0
```

#### (4) 配置过滤列表

# 配置编号为 2002 的 ACL，允许 172.17.2.0/24 的路由通过。

```
[SwitchB] acl number 2002
```

```
[SwitchB-acl-basic-2002] rule permit source 172.17.2.0 0.0.0.255
```

```
[SwitchB-acl-basic-2002] quit
```

# 配置名为 prefix-a 的地址前缀列表，允许 172.17.1.0/24 的路由通过。

```
[SwitchB] ip ip-prefix prefix-a index 10 permit 172.17.1.0 24
```

#### (5) 配置路由策略

```
[SwitchB] route-policy isis2ospf permit node 10
```

```
[SwitchB-route-policy] if-match ip-prefix prefix-a
```

```
[SwitchB-route-policy] apply cost 100
```

```
[SwitchB-route-policy] quit
```

```
[SwitchB] route-policy isis2ospf permit node 20
```

```
[SwitchB-route-policy] if-match acl 2002
```

```
[SwitchB-route-policy] apply tag 20
```

```
[SwitchB-route-policy] quit
```

```
[SwitchB] route-policy isis2ospf permit node 30
```

```
[SwitchB-route-policy] quit
```

#### (6) 在路由引入时应用路由策略

# 配置 Switch B，设置在路由引入时应用路由策略。

```
[SwitchB] ospf
```

```
[SwitchB-ospf-1] import-route isis 1 route-policy isis2ospf
```

```
[SwitchB-ospf-1] quit
```

# 查看 Switch A 的 OSPF 路由表，可以看到目的地址为 172.17.1.0/24 的路由的开销为 100，目的地址为 172.17.2.0/24 的路由的标记域（Tag）为 20，而其他外部路由没有变化。

```
[SwitchA] display ospf routing
```

```
OSPF Process 1 with Router ID 192.168.1.1
```

#### Routing Tables

| Routing for Network |      |         |             |             |         |
|---------------------|------|---------|-------------|-------------|---------|
| Destination         | Cost | Type    | NextHop     | AdvRouter   | Area    |
| 192.168.1.0/24      | 1    | Transit | 192.168.1.1 | 192.168.1.1 | 0.0.0.0 |

| Routing for ASEs |      |       |     |             |             |
|------------------|------|-------|-----|-------------|-------------|
| Destination      | Cost | Type  | Tag | NextHop     | AdvRouter   |
| 172.17.1.0/24    | 100  | Type2 | 1   | 192.168.1.2 | 192.168.2.2 |
| 172.17.2.0/24    | 1    | Type2 | 20  | 192.168.1.2 | 192.168.2.2 |
| 172.17.3.0/24    | 1    | Type2 | 1   | 192.168.1.2 | 192.168.2.2 |
| 192.168.2.0/24   | 1    | Type2 | 1   | 192.168.1.2 | 192.168.2.2 |

| Total Nets: 5 |               |        |         |  |  |
|---------------|---------------|--------|---------|--|--|
| Intra Area: 1 | Inter Area: 0 | ASE: 4 | NSSA: 0 |  |  |

### 1.27.5 完整配置

- 配置 Switch A

```
#
vlan 100
#
interface Vlan-interface100
 ip address 192.168.1.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
 network 192.168.1.0 0.0.0.255
#
```

- 配置 Switch B

```
#
vlan 100
#
vlan 200
#
isis 1
 is-level level-2
 network-entity 10.0000.0000.0002.00
#
acl number 2002
 rule 0 permit source 172.17.2.0 0.0.0.255
#
interface Vlan-interface100
 ip address 192.168.1.2 255.255.255.0
#
interface Vlan-interface200
 ip address 192.168.2.2 255.255.255.0
 isis enable 1
#
ospf 1
```



```

import-route isis 1 route-policy isis2ospf
area 0.0.0.0
network 192.168.1.0 0.0.0.255
#
route-policy isis2ospf permit node 10
if-match ip-prefix prefix-a
apply cost 100
route-policy isis2ospf permit node 20
if-match acl 2002
apply tag 20
route-policy isis2ospf permit node 30
#
ip ip-prefix prefix-a index 10 permit 172.17.1.0 24
#

```

#### • 配置 Switch C

```

#
vlan 200 to 203
#
isis 1
is-level level-2
network-entity 10.0000.0000.0001.00
#
interface Vlan-interface200
ip address 192.168.2.1 255.255.255.0
isis enable 1
#
interface Vlan-interface201
ip address 172.17.1.1 255.255.255.0
isis enable 1
#
interface Vlan-interface202
ip address 172.17.2.1 255.255.255.0
isis enable 1
#
interface Vlan-interface203
ip address 172.17.3.1 255.255.255.0
isis enable 1
#

```

### 1.27.6 配置注意事项

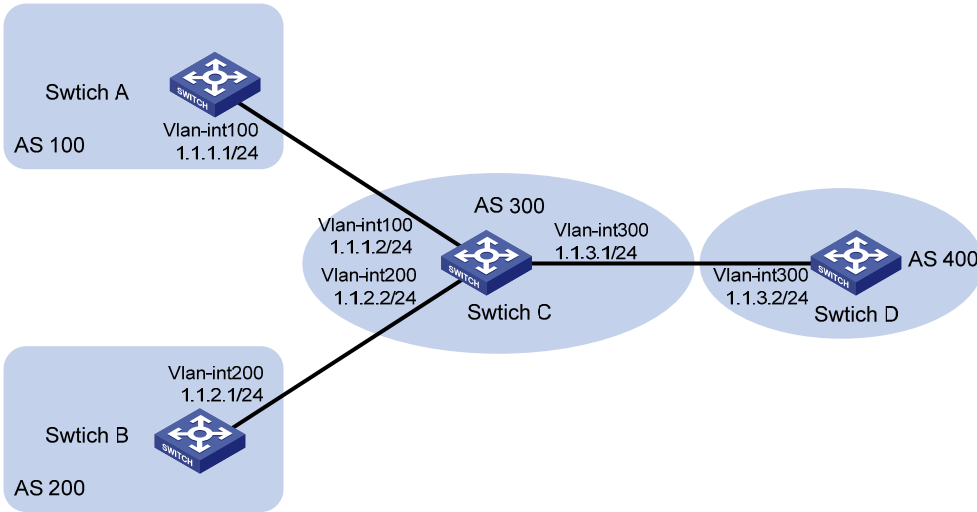
- **permit** 指定节点的匹配模式为允许模式。当路由信息通过该节点的过滤后，将执行该节点的 **apply** 子句，不进入下一个节点的测试；如果路由信息没有通过该节点过滤，将进入下一个节点继续测试。
- **deny** 指定节点的匹配模式为拒绝模式（此模式下 **apply** 子句不会被执行）。当路由项满足该节点的所有 **if-match** 子句时，将不执行 **apply** 子句，不进入下一个节点的测试；如果路由项不满足该节点的 **if-match** 子句，将进入下一个节点继续测试。

- 如果路由策略中定义了一个以上的节点，则各节点中至少应该有一个节点的匹配模式是 **permit**。当路由策略用于路由信息过滤时，如果某路由信息没有通过任一节点，则认为该路由信息没有通过该路由策略。如果路由策略的所有节点都是 **deny** 模式，则没有路由信息能通过该路由策略。
- 对于同一个 **Route-policy** 节点，在匹配的过程中，各个 **if-match** 子句间是“与”的关系，即路由信息必须同时满足所有匹配条件，才可以执行 **apply** 子句的动作。
- 在一个节点中，可以没有 **if-math** 子句，也可以有多个 **if-match** 子句。当不指定 **if-match** 子句时，如果该节点的匹配模式为允许模式，则所有路由信息都会通过该节点的过滤；如果该节点的匹配模式为拒绝模式，则所有路由信息都会被拒绝。

## 1.28 应用路由策略过滤接收的 BGP 路由典型配置指导

### 1.28.1 组网图

图1-28 配置应用路由策略过滤接收的 BGP 路由



### 1.28.2 应用要求

- 所有交换机均运行 **BGP** 协议，Switch A、Switch B 和 Switch C 之间建立 **EBGP** 连接，Switch C 和 Switch D 之间建立 **EBGP** 连接。
- 通过配置路由策略，使得 Switch D 拒绝接收来自 AS200 的路由。

### 1.28.3 适用产品、版本

表1-28 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本    |
|-------------------|---------------------------------|---------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本 |

| 产品                | 软件版本                            | 硬件版本    |
|-------------------|---------------------------------|---------|
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本 |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本 |

#### 1.28.4 配置过程和解释

(1) 配置接口 IP 地址（略）

(2) 配置 BGP 基本功能

# 配置 Switch A。

```
<SwitchA> system-view
[SwitchA] bgp 100
[SwitchA-bgp] router-id 1.1.1.1
[SwitchA-bgp] peer 1.1.1.2 as-number 300
```

# 配置 Switch B。

```
<SwitchB> system-view
[SwitchB] bgp 200
[SwitchB-bgp] router-id 2.2.2.2
[SwitchB-bgp] peer 1.1.2.2 as-number 300
```

# 配置 Switch C。

```
<SwitchC> system-view
[SwitchC] bgp 300
[SwitchC-bgp] router-id 3.3.3.3
[SwitchC-bgp] peer 1.1.1.1 as-number 100
[SwitchC-bgp] peer 1.1.2.1 as-number 200
[SwitchC-bgp] peer 1.1.3.2 as-number 400
```

# 配置 Switch D。

```
<SwitchD> system-view
[SwitchD] bgp 400
[SwitchD-bgp] router-id 4.4.4.4
[SwitchD-bgp] peer 1.1.3.1 as-number 300
[SwitchD-bgp] quit
```

# 配置 Switch A，将网段路由 4.4.4.4/24、5.5.5.5/24、6.6.6.6/24 发布到 BGP 路由表中。

```
[SwitchA-bgp] network 4.4.4.4 24
[SwitchA-bgp] network 5.5.5.5 24
[SwitchA-bgp] network 6.6.6.6 24
```

# 配置 Switch B，将网段路由 7.7.7.7/24、8.8.8.8/24、9.9.9.9/24 发布到 BGP 路由表中。

```
[SwitchB-bgp] network 7.7.7.7 24
[SwitchB-bgp] network 8.8.8.8 24
[SwitchB-bgp] network 9.9.9.9 24
```

# 查看 Switch D 的 BGP 路由表。

```
[SwitchD-bgp] display bgp routing-table
```

```
Total Number of Routes: 6
```

```
BGP Local router ID is 4.4.4.4
```

```
Status codes: * - valid, > - best, d - damped,
```

```
h - history, i - internal, s - suppressed, S - Stale
```

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

| Network       | NextHop | MED | LocPrf | PrefVal | Path/Ogn |
|---------------|---------|-----|--------|---------|----------|
| *> 4.4.4.0/24 | 1.1.3.1 |     |        | 0       | 300 100i |
| *> 5.5.5.0/24 | 1.1.3.1 |     |        | 0       | 300 100i |
| *> 6.6.6.0/24 | 1.1.3.1 |     |        | 0       | 300 100i |
| *> 7.7.7.0/24 | 1.1.3.1 |     |        | 0       | 300 200i |
| *> 8.8.8.0/24 | 1.1.3.1 |     |        | 0       | 300 200i |
| *> 9.9.9.0/24 | 1.1.3.1 |     |        | 0       | 300 200i |

从路由表可以看出，Switch D 同时学到了来自 AS 100 的路由 4.4.4.0/24、5.5.5.0/24、6.6.6.0/24 和来自 AS 200 的路由 7.7.7.0/24、8.8.8.0/24、9.9.9.0/24。

(3) 配置 Switch D 拒绝接收来自 AS200 的路由。

# 在 Switch D 上配置编号为 1 的 AS 路径过滤列表。

```
[SwitchD] ip as-path 1 permit .*200.*
```

# 在 Switch D 上配置名称为 “rt1” 的路由策略。

```
[SwitchD] route-policy rt1 deny node 1
```

```
[SwitchD] if-match as-path 1
```

```
[SwitchD] route-policy rt2 permit node 2
```

# 在 Switch D 上，配置对从对等体 1.1.3.1 接收的路由指定名称为 “rt1” 的路由策略。

```
[SwitchD] bgp 400
```

```
[SwitchD] peer 1.1.3.1 route-policy rt1 import
```

# 查看 Switch D 的 BGP 路由表。

```
[SwitchD] display bgp routing-table
```

```
Total Number of Routes: 3
```

```
BGP Local router ID is 4.4.4.4
```

```
Status codes: * - valid, > - best, d - damped,
```

```
h - history, i - internal, s - suppressed, S - Stale
```

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

| Network       | NextHop | MED | LocPrf | PrefVal | Path/Ogn |
|---------------|---------|-----|--------|---------|----------|
| *> 4.4.4.0/24 | 1.1.3.1 |     |        | 0       | 300 100i |
| *> 5.5.5.0/24 | 1.1.3.1 |     |        | 0       | 300 100i |
| *> 6.6.6.0/24 | 1.1.3.1 |     |        | 0       | 300 100i |

从路由表可以看出，Switch D 只学到了来自 AS 100 的路由 4.4.4.0/24、5.5.5.0/24、6.6.6.0/24。

## 1.28.5 完整配置

- 配置 Switch A

```
#
vlan 100
#
interface Vlan-interface100
 ip address 1.1.1.1 255.255.255.0
#
bgp 100
 router-id 1.1.1.1
 network 4.4.4.0 255.255.255.0
 network 5.5.5.0 255.255.255.0
 network 6.6.6.0 255.255.255.0
 undo synchronization
 peer 1.1.1.2 as-number 300
```

```
#
```

- 配置 Switch B

```
#
vlan 200
#
interface Vlan-interface200
 ip address 1.1.2.1 255.255.255.0
#
bgp 200
 router-id 2.2.2.2
 network 7.7.7.0 255.255.255.0
 network 8.8.8.0 255.255.255.0
 network 9.9.9.0 255.255.255.0
 undo synchronization
 peer 1.1.2.2 as-number 300
```

```
#
```

- 配置 Switch C

```
#
vlan 100
#
vlan 200
#
vlan 300
#
interface Vlan-interface100
 ip address 1.1.1.2 255.255.255.0
#
interface Vlan-interface200
 ip address 1.1.2.2 255.255.255.0
#
interface Vlan-interface300
 ip address 1.1.3.1 255.255.255.0
#
bgp 300
 router-id 3.3.3.3
```

```
undo synchronization
peer 1.1.1.1 as-number 100
peer 1.1.2.1 as-number 200
peer 1.1.3.2 as-number 400
#
```

- 配置 Switch D

```
#
vlan 300
#
bgp 400
router-id 4.4.4.4
undo synchronization
peer 1.1.3.1 as-number 300
peer 1.1.3.1 route-policy rt1 import
#
route-policy rt1 deny node 1
if-match as-path 1
route-policy rt2 permit node 2
#
ip as-path 1 permit .*200.*
#
```

## 1.28.6 配置注意事项

无

# 目 录

|                                  |      |
|----------------------------------|------|
| 1 IPv6 管理典型配置指导 .....            | 1-1  |
| 1.1 IPv6 基础典型配置指导 .....          | 1-1  |
| 1.1.1 组网图 .....                  | 1-1  |
| 1.1.2 应用要求 .....                 | 1-1  |
| 1.1.3 适用产品、版本 .....              | 1-1  |
| 1.1.4 配置过程和解释 .....              | 1-2  |
| 1.1.5 完整配置 .....                 | 1-3  |
| 1.1.6 配置注意事项 .....               | 1-4  |
| 1.2 IPv6 手动隧道典型配置指导 .....        | 1-4  |
| 1.2.1 组网图 .....                  | 1-5  |
| 1.2.2 应用要求 .....                 | 1-5  |
| 1.2.3 适用产品、版本 .....              | 1-5  |
| 1.2.4 配置过程和解释 .....              | 1-5  |
| 1.2.5 完整配置 .....                 | 1-8  |
| 1.2.6 配置注意事项 .....               | 1-11 |
| 1.3 IPv4 兼容IPv6 自动隧道典型配置指导 ..... | 1-11 |
| 1.3.1 组网图 .....                  | 1-11 |
| 1.3.2 应用要求 .....                 | 1-12 |
| 1.3.3 适用产品、版本 .....              | 1-12 |
| 1.3.4 配置过程和解释 .....              | 1-12 |
| 1.3.5 完整配置 .....                 | 1-14 |
| 1.3.6 配置注意事项 .....               | 1-15 |
| 1.4 6to4 隧道典型配置指导 .....          | 1-15 |
| 1.4.1 组网图 .....                  | 1-16 |
| 1.4.2 应用要求 .....                 | 1-16 |
| 1.4.3 适用产品、版本 .....              | 1-16 |
| 1.4.4 配置过程和解释 .....              | 1-17 |
| 1.4.5 完整配置 .....                 | 1-20 |
| 1.4.6 配置注意事项 .....               | 1-22 |
| 1.5 ISATAP隧道典型配置指导 .....         | 1-22 |
| 1.5.1 组网图 .....                  | 1-23 |
| 1.5.2 应用要求 .....                 | 1-23 |
| 1.5.3 适用产品、版本 .....              | 1-23 |
| 1.5.4 配置过程和解释 .....              | 1-23 |
| 1.5.5 完整配置 .....                 | 1-26 |
| 1.5.6 配置注意事项 .....               | 1-27 |

# 1 IPv6 管理典型配置指导

## 1.1 IPv6 基础典型配置指导

当用户需要访问 IPv6 网络时，交换机上必须要配置 IPv6 地址，并确保用户和交换机之间网络层互通。全球单播地址、站点本地地址、链路本地地址三者必选其一。

特别当用户需要访问使用 IPv6 的公网时，必须配置 IPv6 全球单播地址。

(1) IPv6 站点本地地址和全球单播地址可以通过下面方式配置：

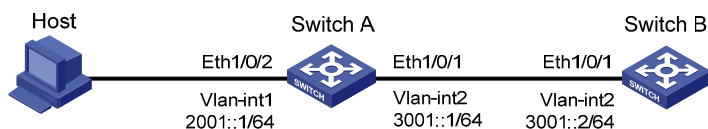
- 采用 EUI-64 格式形成：当配置采用 EUI-64 格式形成 IPv6 地址时，接口的 IPv6 地址的前缀是所配置的前缀，而接口标识符则由接口的链路层地址转化而来。
- 手工配置：用户手工配置 IPv6 站点本地地址或全球单播地址。

(2) IPv6 的链路本地地址可以通过两种方式获得：

- 自动生成：设备根据链路本地地址前缀（FE80::/64）及接口的链路层地址，自动为接口生成链路本地地址；
- 手动指定：用户手工配置 IPv6 链路本地地址。

### 1.1.1 组网图

图1-1 IPv6 基础配置组网示意图



### 1.1.2 应用要求

- Host、Switch A 和 Switch B 通过以太网端口直接相连，将以太网端口分别加入相应的 VLAN 中，并在 VLAN 接口上配置 IPv6 地址，验证设备之间的互通性。
- Switch A 的 VLAN 接口 2 的全球单播地址为 3001::1/64，VLAN 接口 1 的全球单播地址为 2001::1/64。
- Switch B 的 VLAN 接口 2 的全球单播地址为 3001::2/64，有可以到 Host 的路由。
- Host 上安装了 IPv6，根据 IPv6 邻居发现协议自动配置 IPv6 地址。

### 1.1.3 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

| 产品             | 软件版本                            | 硬件版本    |
|----------------|---------------------------------|---------|
| S3610 系列以太网交换机 | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5510 系列以太网交换机 | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |



| 产品                | 软件版本                            | 硬件版本                         |
|-------------------|---------------------------------|------------------------------|
| S5500-SI 系列以太网交换机 | Release 1207 软件版本               | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本               | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本                      |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本                      |

#### 1.1.4 配置过程和解释



说明

- 交换机上已经创建相应 VLAN 接口。
- 对于 S3610/S5510 系列以太网交换机，在使能 IPv6 功能之前，必须先将设备运行模式切换到 IPv4/IPv6 双协议栈模式，即执行 **switch-mode dual-ipv4-ipv6** 命令；否则，即使使能 IPv6，设备也不支持 IPv6 报文的转发。另外需要注意的是，执行 **switch-mode** 命令切换的协议栈只有在重启设备后才能生效。

##### (1) 配置 Switch A

# 使能交换机的 IPv6 转发功能。

```
<SwitchA> system-view
```

```
[SwitchA] ipv6
```

# 手工指定 VLAN 接口 2 的全球单播地址，同时会自动生成链路本地地址。

```
[SwitchA] interface vlan-interface 2
```

```
[SwitchA-Vlan-interface2] ipv6 address 3001::1/64
```

```
[SwitchA-Vlan-interface2] quit
```

# 手工指定 VLAN 接口 1 的全球单播地址，并允许其发布 RA 消息。（缺省情况下，所有的接口不会发布 RA 消息）

```
[SwitchA] interface vlan-interface 1
```

```
[SwitchA-Vlan-interface1] ipv6 address 2001::1/64
```

```
[SwitchA-Vlan-interface1] undo ipv6 nd ra halt
```

##### (2) 配置 Switch B

# 使能交换机的 IPv6 转发功能。

```
<SwitchB> system-view
```

```
[SwitchB] ipv6
```

# 配置 VLAN 接口 2 的全球单播地址。

```
[SwitchB] interface vlan-interface 2
```

```
[SwitchB-Vlan-interface2] ipv6 address 3001::2/64
```

```
[SwitchB-Vlan-interface2] quit
```

# 配置 IPv6 静态路由，该路由的目的地址为 2001::/64，下一跳地址为 3001::1。

```
[SwitchB] ipv6 route-static 2001:: 64 3001::1
```

### (3) 配置 Host

Host 上安装 IPv6，根据 IPv6 邻居发现协议自动配置 IPv6 地址。

```
[SwitchA] display ipv6 neighbors interface ethernet 1/0/2
```

| Type: S-Static      D-Dynamic |                |     |           |       |   |      |
|-------------------------------|----------------|-----|-----------|-------|---|------|
| IPv6 Address                  | Link-layer     | VID | Interface | State | T | Age  |
| FE80::215:E9FF:FEA6:7D14      | 0015-e9a6-7d14 | 1   | Eth1/0/2  | STALE | D | 1238 |
| 2001::15B:E0EA:3524:E791      | 0015-e9a6-7d14 | 1   | Eth1/0/2  | STALE | D | 1248 |

通过上面的信息可以知道 Host 上获得的 IPv6 全球单播地址为 2001::15B:E0EA:3524:E791。

### (4) 验证配置结果

# 使用 display ipv6 interface 命令显示 Switch 的接口信息。

```
[SwitchA] display ipv6 interface vlan-interface 2
```

```
[SwitchA] display ipv6 interface vlan-interface 1
```

```
[SwitchB] display ipv6 interface vlan-interface 2
```

# 在 Host 上使用 Ping 测试和 Switch A 及 Switch B 的互通性；在 Switch B 上使用 Ping 测试和 Switch A 及 Host 的互通性。



#### 注意

在 Ping 链路本地地址时，需要使用 **-i** 参数，来指定链路本地地址的接口。

---

```
[SwitchB] ping ipv6 -c 1 3001::1
```

```
PING 3001::1 : 56 data bytes, press CTRL_C to break
```

```
Reply from 3001::1
```

```
bytes=56 Sequence=1 hop limit=64 time = 2 ms
```

```
--- 3001::1 ping statistics ---
```

```
1 packet(s) transmitted
```

```
1 packet(s) received
```

```
0.00% packet loss
```

```
round-trip min/avg/max = 2/2/2 ms
```

```
[SwitchB-Vlan-interface2] ping ipv6 -c 1 2001::15B:E0EA:3524:E791
```

```
PING 2001::15B:E0EA:3524:E791 : 56 data bytes, press CTRL_C to break
```

```
Reply from 2001::15B:E0EA:3524:E791
```

```
bytes=56 Sequence=1 hop limit=63 time = 3 ms
```

```
--- 2001::15B:E0EA:3524:E791 ping statistics ---
```

```
1 packet(s) transmitted
```

```
1 packet(s) received
```

```
0.00% packet loss
```

```
round-trip min/avg/max = 3/3/3 ms
```

从 Host 上也可以 ping 通 Switch B 和 Switch A，证明它们是互通的。

## 1.1.5 完整配置

### (1) SwitchA 上的配置

```
#
ipv6
#
interface Vlan-interface1
ipv6 address 2001::1/64
undo ipv6 nd ra halt
#
interface Vlan-interface2
ipv6 address 3001::1/64
#
(2) SwitchB 上的配置
#
ipv6
#
interface Vlan-interface2
ipv6 address 3001::2/64
#
ipv6 route-static 2001:: 64 3001::1
#
```

### 1.1.6 配置注意事项

- 当接口配置了 IPv6 站点本地地址或全球单播地址后，同时会自动生成链路本地地址，且与采用 **ipv6 address auto link-local** 命令生成的链路本地地址相同。
- 配置链路本地地址时，手工指定方式的优先级高于自动生成方式。即如果先采用自动生成方式，之后手工指定，则手工指定的地址会覆盖自动生成的地址；如果先手工指定，之后采用自动生成的方式，则自动配置不生效，接口的链路本地地址仍是手工指定的。此时，如果删除手工指定的地址，则自动生成的链路本地地址会生效。

## 1.2 IPv6 手动隧道典型配置指导

IPv6 over IPv4 隧道机制是将 IPv6 数据报文前封装上 IPv4 的报文头，通过隧道（Tunnel）使 IPv6 报文穿越 IPv4 网络，实现隔离的 IPv6 网络的互通。

根据隧道终点的 IPv4 地址的获取方式不同，隧道分为“配置隧道”及“自动隧道”。

- 如果 IPv6 over IPv4 隧道的终点地址不能从 IPv6 报文的目的地址中自动获取，需要进行手工配置，这样的隧道即为“配置隧道”。
- 如果 IPv6 over IPv4 隧道的接口地址采用内嵌 IPv4 地址的特殊 IPv6 地址形式，即可以从 IPv6 报文的目的地址中自动获取隧道终点的 IPv4 地址，这样的隧道即为“自动隧道”。

根据对 IPv6 报文的封装方式的不同，IPv6 over IPv4 隧道分为以下几种模式：

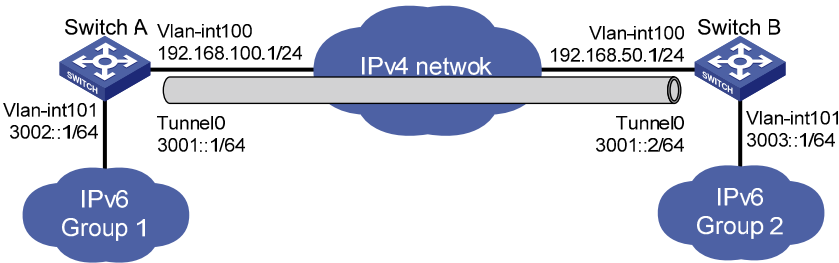
- IPv6 手动隧道
- IPv4 兼容 IPv6 自动隧道
- 6to4 隧道
- ISATAP（Intra-Site Automatic Tunnel Addressing Protocol，站点内自动隧道寻址协议）隧道

在上面列出的隧道模式中，IPv6 手动隧道为配置隧道；IPv4 兼容 IPv6 自动隧道、6to4 隧道及 ISATAP 隧道为自动隧道。

IPv6 手动隧道是点到点之间的链路，一条链路就是一个单独的隧道。主要用于边缘路由器-边缘路由器或主机-边缘路由器之间定期安全通信的稳定连接，可实现与远端 IPv6 网络的连接。

1.2.1 组网图

图1-2 IPv6 手动隧道组网图



1.2.2 应用要求

如 图 1-2所示，两个IPv6 网络分别通过Switch A和Switch B与IPv4 网络连接，要求在Switch A和Switch B之间建立IPv6 手动隧道，使两个IPv6 网络可以互通。

1.2.3 适用产品、版本

表1-2 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本    |
|-------------------|---------------------------------|---------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本 |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本 |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本 |

1.2.4 配置过程和解释

 说明

- 已经在 Switch A 和 Switch B 上创建相应的 VLAN 接口；
- 已经配置 Switch A 的 Vlan-interface100 和 Switch B 的 Vlan-interface100 可以正常通讯，IPv4 报文路由可达。
- 对于 S3610/S5510 系列以太网交换机，在使能 IPv6 功能之前，必须先将设备运行模式切换到 IPv4/IPv6 双协议栈模式，即执行 **switch-mode dual-ipv4-ipv6** 命令；否则，即使使能 IPv6，设备也不支持 IPv6 报文的转发。另外需要注意的是，执行 **switch-mode** 命令切换的协议栈只有在重启设备后才能生效。

(1) 配置 Switch A

# 使能交换机的 IPv6 转发功能。

```
<SwitchA> system-view
```

```
[SwitchA] ipv6
```

# 配置接口 Vlan-interface100 的地址。

```
[SwitchA] interface vlan-interface 100
```

```
[SwitchA-Vlan-interface100] ip address 192.168.100.1 255.255.255.0
```

```
[SwitchA-Vlan-interface100] quit
```

# 配置接口 Vlan-interface101 的 IPv6 地址。

```
[SwitchA] interface vlan-interface 101
```

```
[SwitchA-Vlan-interface101] ipv6 address 3002::1 64
```

```
[SwitchA-Vlan-interface101] quit
```

# 配置链路聚合组或业务环回组，请根据产品实际支持情况进行选择。



#### 注意

- S7500E Release 6300 软件版本的隧道接口必须引用业务环回组以实现报文的接收和发送，且隧道引用的业务环回组必须已创建，否则隧道接口状态不会 up，隧道无法通讯。
  - 表 1-2 所列除 S7500E Release 6300 软件版本外的其它产品，隧道接口必须引用链路聚合组以实现报文的接收和发送，且隧道引用的链路聚合组必须已创建，否则隧道接口状态不会 up，隧道无法通讯。
- 

- 配置链路聚合组。需要注意的是，将端口加入到链路聚合组时，需要在端口上关闭 STP 功能。

```
[SwitchA] link-aggregation group 1 mode manual
```

```
[SwitchA] link-aggregation group 1 service-type tunnel
```

```
[SwitchA] interface GigabitEthernet 1/0/2
```

```
[SwitchA-GigabitEthernet1/0/2] stp disable
```

```
[SwitchA-GigabitEthernet1/0/2] port link-aggregation group 1
```

```
[SwitchA-GigabitEthernet1/0/2] quit
```

- 配置业务环回组。需要注意的是，将端口加入到业务环回组时，需要在端口上关闭 STP 功能。

```
[SwitchA] service-loopback group 1 type tunnel
```

```
[SwitchA] interface GigabitEthernet 1/0/2
```

```
[SwitchA-GigabitEthernet1/0/2] stp disable
```

```
[SwitchA-GigabitEthernet1/0/2] port service-loopback group 1
```

```
[SwitchA-GigabitEthernet1/0/2] quit
```

# 配置手动隧道。

```
[SwitchA] interface tunnel 0
```

```
[SwitchA-Tunnel0] ipv6 address 3001::1/64
```

```
[SwitchA-Tunnel0] source vlan-interface 100
```

```
[SwitchA-Tunnel0] destination 192.168.50.1
```

```
[SwitchA-Tunnel0] tunnel-protocol ipv6-ipv4
```

# 在 Tunnel 接口视图下配置隧道引用链路聚合组 1 或业务环回组 1，请根据产品实际支持情况进行选择。

- 在 Tunnel 接口视图下配置隧道引用链路聚合组 1

```
[SwitchA-Tunnel0] aggregation-group 1
```

```
[SwitchA-Tunnel0] quit
```

- 在 Tunnel 接口视图下配置隧道引用业务环回组 1。

```
[SwitchA-Tunnel0] service-loopback-group 1
[SwitchA-Tunnel0] quit
```

# 配置从 Switch A 经过 Tunnel0 接口到 Group 2 的静态路由。

```
[SwitchA] ipv6 route-static 3003:: 64 tunnel 0
```

## (2) 配置 Switch B

# 使能交换机的 IPv6 转发功能。

```
<SwitchB> system-view
[SwitchB] ipv6
```

# 配置接口 Vlan-interface100 的地址。

```
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ip address 192.168.50.1 255.255.255.0
[SwitchB-Vlan-interface100] quit
```

# 配置接口 Vlan-interface101 的 IPv6 地址。

```
[SwitchB] interface vlan-interface 101
[SwitchB-Vlan-interface101] ipv6 address 3003::1 64
[SwitchB-Vlan-interface101] quit
```

# 配置链路聚合组或业务环回组，请根据产品实际支持情况进行选择。



### 注意

- S7500E Release 6300 软件版本的隧道接口必须引用业务环回组以实现报文的接收和发送，且隧道引用的业务环回组必须已创建，否则隧道接口状态不会 up，隧道无法通讯。
  - 表 1-2 所列除 S7500E Release 6300 软件版本外的其它产品，隧道接口必须引用链路聚合组以实现报文的接收和发送，且隧道引用的链路聚合组必须已创建，否则隧道接口状态不会 up，隧道无法通讯。
- 

- 配置链路聚合组。需要注意的是，将端口加入到链路聚合组时，需要在端口上关闭 STP 功能。

```
[SwitchB] link-aggregation group 1 mode manual
[SwitchB] link-aggregation group 1 service-type tunnel
[SwitchB] interface GigabitEthernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] stp disable
[SwitchB-GigabitEthernet1/0/2] port link-aggregation group 1
[SwitchB-GigabitEthernet1/0/2] quit
```

- 配置业务环回组。需要注意的是，将端口加入到业务环回组时，需要在端口上关闭 STP 功能。

```
[SwitchB] service-loopback group 1 type tunnel
[SwitchB] interface GigabitEthernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] stp disable
[SwitchB-GigabitEthernet1/0/2] port service-loopback group 1
[SwitchB-GigabitEthernet1/0/2] quit
```

# 配置手动隧道。

```
[SwitchB] interface tunnel 0
[SwitchB-Tunnel0] ipv6 address 3001::2/64
[SwitchB-Tunnel0] source vlan-interface 100
[SwitchB-Tunnel0] destination 192.168.100.1
[SwitchB-Tunnel0] tunnel-protocol ipv6-ipv4
```

# 在 Tunnel 接口视图下配置隧道引用链路聚合组 1 或业务环回组 1，请根据产品实际支持情况进行选择。

- 在 Tunnel 接口视图下配置隧道引用链路聚合组 1。

```
[SwitchB-Tunnel0] aggregation-group 1
[SwitchB-Tunnel0] quit
```

- 在 Tunnel 接口视图下配置隧道引用业务环回组 1。

```
[SwitchB-Tunnel0] service-loopback-group 1
[SwitchB-Tunnel0] quit
```

# 配置从 Switch B 经过 Tunnel0 接口到 Group 1 的静态路由。

```
[SwitchB] ipv6 route-static 3002:: 64 tunnel 0
```

### (3) 验证配置结果

完成以上配置之后，分别通过 **display** 命令查看 Switch A 和 Switch B 的 Tunnel 接口状态。

```
[SwitchA] display ipv6 interface tunnel 0
[SwitchB] display ipv6 interface tunnel 0
```

# 从 Switch A 上可以 Ping 通对端的 Vlan-int101 接口的 IPv6 地址：

```
[SwitchA] ping ipv6 3003::1
 PING 3003::1 : 56 data bytes, press CTRL_C to break
 Reply from 3003::1:
 bytes=56 Sequence=1 hop limit=64 time = 1 ms
 Reply from 3003::1:
 bytes=56 Sequence=2 hop limit=64 time = 1 ms
 Reply from 3003::1:
 bytes=56 Sequence=3 hop limit=64 time = 1 ms
 Reply from 3003::1:
 bytes=56 Sequence=4 hop limit=64 time = 1 ms
 Reply from 3003::1:
 bytes=56 Sequence=5 hop limit=64 time = 1 ms

 --- 3003::1 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 1/1/1 ms
```

## 1.2.5 完整配置

### (1) SwitchA 上的配置

- SwitchA 上的配置（隧道引用链路聚合组）

```
#
```

```

ipv6
#
link-aggregation group 1 mode manual
link-aggregation group 1 service-type tunnel
#
interface Vlan-interface100
ip address 192.168.100.1 255.255.255.0
#
interface Vlan-interface101
ipv6 address 3002::1/64
#
interface GigabitEthernet1/0/2
stp disable
port link-aggregation group 1
#
interface Tunnel0
ipv6 address 3001::1/64
source Vlan-interface100
destination 192.168.50.1
aggregation-group 1
#
ipv6 route-static 3003:: 64 tunnel 0
#

```

- SwitchA 上的配置（隧道引用业务环回组）

```

#
ipv6
#
service-loopback group 1 type tunnel
#
interface Vlan-interface100
ip address 192.168.100.1 255.255.255.0
#
interface Vlan-interface101
ipv6 address 3002::1/64
#
interface GigabitEthernet1/0/2
port service-loopback group 1
#
interface Tunnel0
ipv6 address 3001::1/64
source Vlan-interface100
destination 192.168.50.1
service-loopback-group 1
#
ipv6 route-static 3003:: 64 tunnel 0
#

```

- (2) SwitchB 上的配置



- SwitchB 上的配置（隧道引用链路聚合组）

```
#
ipv6
#
link-aggregation group 1 mode manual
link-aggregation group 1 service-type tunnel
#
vlan 100
#
interface Vlan-interface100
ip address 192.168.100.1 255.255.255.0
#
interface Vlan-interface101
ipv6 address 3003::1/64
#
interface GigabitEthernet1/0/2
stp disable
port link-aggregation group 1
#
interface Tunnel0
ipv6 address 3001::1/64
source Vlan-interface100
destination 192.168.50.1
aggregation-group 1
#
ipv6 route-static 3002:: 64 tunnel 0
#
```

- SwitchB 上的配置（隧道引用业务环回组）

```
#
ipv6
#
service-loopback group 1 type tunnel
#
vlan 100
#
interface Vlan-interface100
ip address 192.168.100.1 255.255.255.0
#
interface Vlan-interface101
ipv6 address 3003::1/64
#
interface GigabitEthernet1/0/2
stp disable
port service-loopback group 1
#
interface Tunnel0
ipv6 address 3001::1/64
source Vlan-interface100
```

```

destination 192.168.50.1
service-loopback-group 1
#
ipv6 route-static 3002:: 64 tunnel 0
#

```

### 1.2.6 配置注意事项

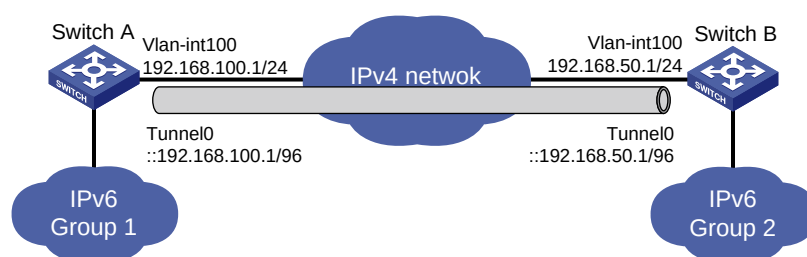
- 在隧道的两端应配置相同的隧道模式，否则可能造成报文传输失败。
- 分布式交换机（例如 S7500E 系列）的 Tunnel 接口号的形式为 A/B/C，A、B、C 分别代表单板槽位号、子卡槽位号、Tunnel 接口号。
- 当在分布式交换机（例如 S7500E 系列）上创建 Tunnel 接口时，建议 Tunnel 接口的槽号与所设置的源端端口所在槽位保持一致，即使用发出报文的实际端口的槽位号，这样可以提高转发效率。
- 在分布式交换机（例如 S7500E 系列）上，主备倒换或备板被拔出时，建立在主控板或备板上的隧道不会被真正删除，若再配置相同的隧道，系统会提示隧道已经存在。如果需要真正删除隧道接口，请使用 **undo interface tunnel** 命令来删除。
- 如果隧道两端 Tunnel 接口的地址不在同一个网段，则必须配置通过隧道到达对端的转发路由，以便需要进行封装的报文能正常转发。用户可以配置静态路由，也可以配置动态路由。在 Tunnel 的两端都要进行此项配置。
- 配置静态路由时，需要手动配置到达目的地址（不是隧道的终点 IPv4 地址，而是封装前报文的目的 IPv6 地址）的路由，并配置出接口为本端 Tunnel 接口或下一跳为对端的 Tunnel 接口地址。在隧道的两端都要进行此项配置。
- 配置动态路由时，需要在隧道两端的 Tunnel 接口使能动态路由协议。在隧道的两端都要进行此项配置。

## 1.3 IPv4 兼容 IPv6 自动隧道典型配置指导

IPv4 兼容 IPv6 自动隧道是点到多点的链路。隧道两端采用特殊的 IPv6 地址：IPv4 兼容 IPv6 地址，其格式为：0:0:0:0:0:0:a.b.c.d/96，其中 a.b.c.d 是 IPv4 地址。通过这个嵌入的 IPv4 地址可以自动确定隧道的终点，使 IPv6 隧道的建立非常方便。但由于它必须使用 IPv4 兼容 IPv6 地址，仍依赖于 IPv4 地址，在使用时有一定的局限性。

### 1.3.1 组网图

图1-3 IPv4 兼容 IPv6 自动隧道组网图



### 1.3.2 应用要求

如图 1-3所示，两个IPv6 网络分别通过Switch A和Switch B与IPv4 网络连接，要求在Switch A和Switch B之间建立IPv4 兼容IPv6 自动隧道，使两个IPv6 网络可以互通。

### 1.3.3 适用产品、版本

表1-3 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本    |
|-------------------|---------------------------------|---------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本 |

### 1.3.4 配置过程 and 解释



#### 说明

- 已经在 Switch A 和 Switch B 上创建相应的 VLAN 接口；
- Switch A 的 Vlan-interface100 和 Switch B 的 Vlan-interface100 可以正常通讯，IPv4 报文路由可达。
- 对于 S3610/S5510 系列以太网交换机，在使能 IPv6 功能之前，必须先将设备运行模式切换到 IPv4/IPv6 双协议栈模式，即执行 **switch-mode dual-ipv4-ipv6** 命令；否则，即使使能 IPv6，设备也不支持 IPv6 报文的转发。另外需要注意的是，执行 **switch-mode** 命令切换的协议栈只有在重启设备后才能生效。

#### (1) 配置 Switch A

# 使能交换机的 IPv6 转发功能。

```
<SwitchA> system-view
```

```
[SwitchA] ipv6
```

# 配置接口 Vlan-interface100 的地址。

```
[SwitchA] interface vlan-interface 100
```

```
[SwitchA-Vlan-interface100] ip address 192.168.100.1 255.255.255.0
```

```
[SwitchA-Vlan-interface100] quit
```



#### 注意

表 1-3所列产品的隧道接口必须引用链路聚合组以实现报文的接收和发送，且隧道引用的链路聚合组必须已创建，否则隧道接口状态不会up，隧道无法通讯。

# 配置链路聚合组。需要注意的是，将端口加入到链路聚合组时，需要在端口上关闭 STP 功能。

```
[SwitchA] link-aggregation group 1 mode manual
```

```
[SwitchA] link-aggregation group 1 service-type tunnel
```

```
[SwitchA] interface GigabitEthernet 1/0/2
```

```
[SwitchA-GigabitEthernet1/0/2] stp disable
```

```
[SwitchA-GigabitEthernet1/0/2] port link-aggregation group 1
```

```
[SwitchA-GigabitEthernet1/0/2] quit
```

# 配置自动隧道。

```
[SwitchA] interface tunnel 0
```

```
[SwitchA-Tunnel0] ipv6 address ::192.168.100.1/96
```

```
[SwitchA-Tunnel0] source vlan-interface 100
```

```
[SwitchA-Tunnel0] tunnel-protocol ipv6-ipv4 auto-tunnel
```

# 在 Tunnel 接口视图下配置隧道引用链路聚合组 1

```
[SwitchA-Tunnel0] aggregation-group 1
```

## (2) 配置 Switch B

# 使能交换机的 IPv6 转发功能。

```
<SwitchB> system-view
```

```
[SwitchB] ipv6
```

# 配置接口 Vlan-interface100 的地址。

```
[SwitchB] interface vlan-interface 100
```

```
[SwitchB-Vlan-interface100] ip address 192.168.50.1 255.255.255.0
```

```
[SwitchB-Vlan-interface100] quit
```



### 注意

表 1-3所列产品的隧道接口必须引用链路聚合组以实现报文的接收和发送，且隧道引用的链路聚合组必须已创建，否则隧道接口状态不会up，隧道无法通讯。

---

# 配置链路聚合组。需要注意的是，将端口加入到链路聚合组时，需要在端口上关闭 STP 功能。

```
[SwitchB] link-aggregation group 1 mode manual
```

```
[SwitchB] link-aggregation group 1 service-type tunnel
```

```
[SwitchB] interface GigabitEthernet 1/0/2
```

```
[SwitchB-GigabitEthernet1/0/2] stp disable
```

```
[SwitchB-GigabitEthernet1/0/2] port link-aggregation group 1
```

```
[SwitchB-GigabitEthernet1/0/2] quit
```

# 配置自动隧道

```
[SwitchB] interface tunnel 0
```

```
[SwitchB-Tunnel0] ipv6 address ::192.168.50.1/96
```

```
[SwitchB-Tunnel0] source vlan-interface 100
```

```
[SwitchB-Tunnel0] tunnel-protocol ipv6-ipv4 auto-tunnel
```

# 在 Tunnel 接口视图下配置隧道引用链路聚合组 1。

```
[SwitchB-Tunnel0] aggregation-group 1
```

## (3) 验证配置结果

完成以上配置之后，分别通过 **display** 命令查看 Switch A 和 Switch B 的 Tunnel 接口状态。

```
[SwitchA] display ipv6 interface tunnel 0
```

```
[SwitchB] display ipv6 interface tunnel 0
```

# 从 Switch A 上可以 Ping 通对端的 IPv4 兼容 IPv6 地址：

```
[SwitchA] ping ipv6 ::192.168.50.1
```

```

PING ::192.168.50.1 : 56 data bytes, press CTRL_C to break
 Reply from ::192.168.50.1
 bytes=56 Sequence=1 hop limit=64 time = 1 ms
 Reply from ::192.168.50.1
 bytes=56 Sequence=2 hop limit=64 time = 1 ms
 Reply from ::192.168.50.1
 bytes=56 Sequence=3 hop limit=64 time = 1 ms
 Reply from ::192.168.50.1
 bytes=56 Sequence=4 hop limit=64 time = 1 ms
 Reply from ::192.168.50.1
 bytes=56 Sequence=5 hop limit=64 time = 1 ms

--- ::192.168.50.1 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 1/1/1 ms

```

### 1.3.5 完整配置

#### (1) SwitchA 上的配置

```

#
ipv6
#
link-aggregation group 1 mode manual
link-aggregation group 1 service-type tunnel
#
vlan 100
#
interface Vlan-interface100
ip address 192.168.100.1 255.255.255.0
#
interface GigabitEthernet1/0/2
stp disable
port link-aggregation group 1
#
interface Tunnel0
ipv6 address ::192.168.100.1/96
tunnel-protocol ipv6-ipv4 auto-tunnel
source Vlan-interface100
aggregation-group 1
#

```

#### (2) SwitchB 上的配置

```

#
ipv6
#
link-aggregation group 1 mode manual
link-aggregation group 1 service-type tunnel
#

```

```

vlan 100
#
interface Vlan-interface100
 ip address 192.168.50.1 255.255.255.0
#
interface GigabitEthernet1/0/2
 stp disable
 port link-aggregation group 1
#
interface Tunnel0
 ipv6 address ::192.168.50.1/96
 tunnel-protocol ipv6-ipv4 auto-tunnel
 source Vlan-interface100
 aggregation-group 1
#

```

### 1.3.6 配置注意事项

- 在隧道的两端应配置相同的隧道模式，否则可能造成报文传输失败。
- 自动隧道不需要配置目的地址。
- 对于自动隧道，使用同种封装协议的 Tunnel 接口不能同时配置完全相同的源地址。
- 如果隧道两端 Tunnel 接口的地址不在同一个网段，则必须配置通过隧道到达对端的转发路由，以便需要进行封装的报文能正常转发。
- 配置静态路由时，需要手动配置到达目的地址（不是隧道的终点 IPv4 地址，而是封装前报文的目的 IPv6 地址）的路由，并配置出接口为本端 Tunnel 接口或下一跳为对端的 Tunnel 接口地址。在隧道的两端都要进行此项配置。
- 对于自动隧道，不支持动态路由。

## 1.4 6to4 隧道典型配置指导

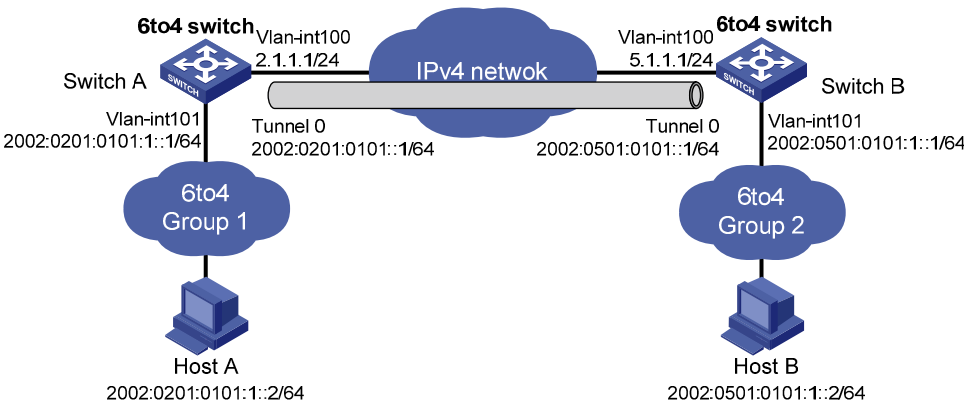
6to4 隧道是点到多点的自动隧道，主要用于将多个 IPv6 孤岛通过 IPv4 网络连接到 IPv6 网络。6to4 隧道通过 IPv6 报文的目的地址中嵌入的 IPv4 地址，可以自动获取隧道的终点。

6to4 隧道采用特殊的地址：6to4 地址，其格式为：2002:abcd:efgh:子网号::接口 ID/64，其中 2002 表示固定的 IPv6 地址前缀，abcd:efgh 表示该 6to4 隧道对应的 32 位 IPv4 源地址，用 16 进制表示（如 1.1.1.1 可以表示为 0101:0101）。通过这个嵌入的 IPv4 地址可以自动确定隧道的终点，使隧道的建立非常方便。

由于 6to4 地址的 64 位地址前缀中的 16 位子网号可以由用户自定义，前缀中的前 48 位已由固定数值、隧道起点或终点设备的 IPv4 地址确定，使 IPv6 报文通过隧道进行转发成为可能。

1.4.1 组网图

图1-4 6to4 隧道组网图



1.4.2 应用要求

如图 1-4所示，两个 6to4 网络通过网络边缘 6to4 switch（Switch A和Switch B）与IPv4 网络相连，为了实现 6to4 网络中的主机Host A和Host B之间的互通，需要配置 6to4 隧道。

6to4 网络之间的互通需要为 6to4 网络内的主机及 6to4 switch 配置 6to4 地址。

- Switch A 上接口 Vlan-int100 的 IPv4 地址为 2.1.1.1/24，转换成 IPv6 地址后使用 6to4 前缀 2002:0201:0101::/48。对此前缀进行子网划分，Tunnel0 使用 2002:0201:0101::/64 子网，Vlan-int101 使用 2002:0201:0101:1::/64 子网。
- Switch B 上接口 Vlan-int100 的 IPv4 地址为 5.1.1.1/24，转换成 IPv6 地址后使用 6to4 前缀 2002:0501:0101::/48。对此前缀进行子网划分，Tunnel0 使用 2002:0501:0101::/64 子网，Vlan-int101 使用 2002:0501:0101:1::/64 子网。

1.4.3 适用产品、版本

表1-4 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本    |
|-------------------|---------------------------------|---------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本 |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本 |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本 |

#### 1.4.4 配置过程和解释



##### 说明

- 已经在 Switch A 和 Switch B 上创建相应的 VLAN 接口；
- 对于 S3610/S5510 系列以太网交换机，在使能 IPv6 功能之前，必须先将设备运行模式切换到 IPv4/IPv6 双协议栈模式，即执行 **switch-mode dual-ipv4-ipv6** 命令；否则，即使使能 IPv6，设备也不支持 IPv6 报文的转发。另外需要注意的是，执行 **switch-mode** 命令切换的协议栈只有在重启设备后才能生效。

##### (1) 配置 Switch A

# 使能交换机的 IPv6 转发功能。

```
<SwitchA> system-view
```

```
[SwitchA] ipv6
```

# 配置接口 Vlan-interface100 的地址。

```
[SwitchA] interface vlan-interface 100
```

```
[SwitchA-Vlan-interface100] ip address 2.1.1.1 24
```

```
[SwitchA-Vlan-interface100] quit
```

# 配置接口 Vlan-interface101 的地址。

```
[SwitchA] interface vlan-interface 101
```

```
[SwitchA-Vlan-interface101] ipv6 address 2002:0201:0101:1::1/64
```

```
[SwitchA-Vlan-interface101] quit
```

# 配置链路聚合组或业务环回组，请根据产品实际支持情况进行选择。



##### 注意

- S7500E Release 6300 软件版本的隧道接口必须引用业务环回组以实现报文的接收和发送，且隧道引用的业务环回组必须已创建，否则隧道接口状态不会 up，隧道无法通讯。
- 表 1-4 所列除 S7500E Release 6300 软件版本外的其它产品，隧道接口必须引用链路聚合组以实现报文的接收和发送，且隧道引用的链路聚合组必须已创建，否则隧道接口状态不会 up，隧道无法通讯。

- 配置链路聚合组。需要注意的是，将端口加入到链路聚合组时，需要在端口上关闭 STP 功能。

```
[SwitchA] link-aggregation group 1 mode manual
```

```
[SwitchA] link-aggregation group 1 service-type tunnel
```

```
[SwitchA] interface GigabitEthernet 1/0/3
```

```
[SwitchA-GigabitEthernet1/0/3] stp disable
```

```
[SwitchA-GigabitEthernet1/0/3] port link-aggregation group 1
```

```
[SwitchA-GigabitEthernet1/0/3] quit
```

- 配置业务环回组。需要注意的是，将端口加入到业务环回组时，需要在端口上关闭 STP 功能。

```
[SwitchA] service-loopback group 1 type tunnel
```

```
[SwitchA] interface GigabitEthernet 1/0/3
```

```
[SwitchA-GigabitEthernet1/0/3] stp disable
```

```
[SwitchA-GigabitEthernet1/0/3] port service-loopback group 1
```

```
[SwitchA-GigabitEthernet1/0/3] quit
```



# 配置 6to4 隧道。

```
[SwitchA] interface tunnel 0
[SwitchA-Tunnel0] ipv6 address 2002:201:101::1/64
[SwitchA-Tunnel0] source vlan-interface 100
[SwitchA-Tunnel0] tunnel-protocol ipv6-ipv4 6to4
```

# 在 Tunnel 接口视图下配置隧道引用链路聚合组 1 或业务环回组 1，请根据产品实际支持情况进行选择。

- 在 Tunnel 接口视图下配置隧道引用链路聚合组 1。

```
[SwitchA-Tunnel0] aggregation-group 1
[SwitchA-Tunnel0] quit
```

- 在 Tunnel 接口视图下配置隧道引用业务环回组 1。

```
[SwitchA-Tunnel0] service-loopback-group 1
[SwitchA-Tunnel0] quit
```

# 配置到目的地址 2002::/16，下一跳为 Tunnel 接口的静态路由。

```
[SwitchA] ipv6 route-static 2002:: 16 tunnel 0
```

## (2) 配置 Switch B

# 使能交换机的 IPv6 转发功能。

```
<SwitchB> system-view
```

```
[SwitchB] ipv6
```

# 配置接口 Vlan-interface100 的地址。

```
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ip address 5.1.1.1 24
[SwitchB-Vlan-interface100] quit
```

# 配置接口 Vlan-interface101 的地址。

```
[SwitchB] interface vlan-interface 101
[SwitchB-Vlan-interface101] ipv6 address 2002:0501:0101:1::1/64
[SwitchB-Vlan-interface101] quit
```

# 配置链路聚合组或业务环回组，请根据产品实际支持情况进行选择。



### 注意

- S7500E Release 6300 软件版本的隧道接口必须引用业务环回组以实现报文的接收和发送，且隧道引用的业务环回组必须已创建，否则隧道接口状态不会 up，隧道无法通讯。
- 表 1-4 所列除 S7500E Release 6300 软件版本外的其它产品，隧道接口必须引用链路聚合组以实现报文的接收和发送，且隧道引用的链路聚合组必须已创建，否则隧道接口状态不会 up，隧道无法通讯。

- 
- 配置链路聚合组。需要注意的是，将端口加入到链路聚合组时，需要在端口上关闭 STP 功能。

```
[SwitchB] link-aggregation group 1 mode manual
[SwitchB] link-aggregation group 1 service-type tunnel
[SwitchB] interface GigabitEthernet 1/0/3
```

```
[SwitchB-GigabitEthernet1/0/3] stp disable
[SwitchB-GigabitEthernet1/0/3] port link-aggregation group 1
[SwitchB-GigabitEthernet1/0/3] quit
```

- 配置业务环回组。需要注意的是，将端口加入到业务环回组时，需要在端口上关闭 STP 功能。

```
[SwitchB] service-loopback group 1 type tunnel
[SwitchB] interface GigabitEthernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] stp disable
[SwitchB-GigabitEthernet1/0/3] port service-loopback group 1
[SwitchB-GigabitEthernet1/0/3] quit
```

# 配置 6to4 隧道。

```
[SwitchB] interface tunnel 0
[SwitchB-Tunnel0] ipv6 address 2002:0501:0101::1/64
[SwitchB-Tunnel0] source vlan-interface 100
[SwitchB-Tunnel0] tunnel-protocol ipv6-ipv4 6to4
```

# 在 Tunnel 接口视图下配置隧道引用链路聚合组 1 或业务环回组 1，请根据产品实际支持情况进行选择。

- 在 Tunnel 接口视图下配置隧道引用链路聚合组 1。

```
[SwitchB-Tunnel0] aggregation-group 1
[SwitchB-Tunnel0] quit
```

- 在 Tunnel 接口视图下配置隧道引用业务环回组 1。

```
[SwitchB-Tunnel0] service-loopback-group 1
[SwitchB-Tunnel0] quit
```

# 配置到目的地址 2002::/16，下一跳为 Tunnel 接口的静态路由。

```
[SwitchB] ipv6 route-static 2002:: 16 tunnel 0
```

### (3) 验证配置结果

完成以上配置之后，Host A 与 Host B 可以互相 Ping 通。

```
D:\>ping6 -s 2002:201:101:1::2 2002:501:101:1::2
```

```
Pinging 2002:501:101:1::2
```

```
from 2002:201:101:1::2 with 32 bytes of data:
```

```
Reply from 2002:501:101:1::2: bytes=32 time=13ms
```

```
Reply from 2002:501:101:1::2: bytes=32 time=1ms
```

```
Reply from 2002:501:101:1::2: bytes=32 time=1ms
```

```
Reply from 2002:501:101:1::2: bytes=32 time<1ms
```

```
Ping statistics for 2002:501:101:1::2:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 0ms, Maximum = 13ms, Average = 3ms
```

## 1.4.5 完整配置

### (1) SwitchA 上的配置

- SwitchA 上的配置（隧道引用链路聚合组）

```
#
ipv6
#
link-aggregation group 1 mode manual
link-aggregation group 1 service-type tunnel
#
interface Vlan-interface100
ip address 2.1.1.1 255.255.255.0
#
interface Vlan-interface101
ipv6 address 2002:201:101:1::1/64
#
interface GigabitEthernet1/0/3
stp disable
port link-aggregation group 1
#
interface Tunnel0
ipv6 address 2002:201:101::1/64
tunnel-protocol ipv6-ipv4 6to4
source Vlan-interface100
aggregation-group 1
#
ip route-static 5.1.1.1 255.255.255.0 [nexthop]
#
ipv6 route-static 2002::16 Tunnel0
#
```

- SwitchA 上的配置（隧道引用业务环回组）

```
#
ipv6
#
service-loopback group 1 type tunnel
#
interface Vlan-interface100
ip address 2.1.1.1 255.255.255.0
#
interface Vlan-interface101
ipv6 address 2002:201:101:1::1/64
#
interface GigabitEthernet1/0/3
stp disable
port service-loopback group 1
#
interface Tunnel0
ipv6 address 2002:201:101::1/64
```

```

tunnel-protocol ipv6-ipv4 6to4
source Vlan-interface100
service-loopback-group 1
#
ip route-static 5.1.1.1 255.255.255.0 [nexthop]
#
ipv6 route-static 2002:: 16 Tunnel0
#

```

## (2) SwitchB 上的配置

- SwitchB 上的配置（隧道引用链路聚合组）

```

#
ipv6
#
link-aggregation group 1 mode manual
link-aggregation group 1 service-type tunnel
#
interface Vlan-interface100
ip address 5.1.1.1 255.255.255.0
#
interface Vlan-interface101
ipv6 address 2002:501:101:1::1/64
#
interface GigabitEthernet1/0/3
stp disable
port link-aggregation group 1
#
interface Tunnel0
ipv6 address 2002:501:101:1::1/64
tunnel-protocol ipv6-ipv4 6to4
source Vlan-interface100
aggregation-group 1
#
ip route-static 2.1.1.1 255.255.255.0 [nexthop]
#
ipv6 route-static 2002:: 16 Tunnel0
#

```

- SwitchB 上的配置（隧道引用业务环回组）

```

#
ipv6
#
service-loopback group 1 type tunnel
#
interface Vlan-interface100
ip address 5.1.1.1 255.255.255.0
#
interface Vlan-interface101
ipv6 address 2002:501:101:1::1/64

```

```
#
interface GigabitEthernet1/0/3
 stp disable
 port service-loopback group 1
#
interface Tunnel0
 ipv6 address 2002:501:101::1/64
 tunnel-protocol ipv6-ipv4 6to4
 source Vlan-interface100
 service-loopback-group 1
#
ip route-static 2.1.1.1 255.255.255.0 [nexthop]
#
ipv6 route-static 2002:: 16 Tunnel0
#
```

#### 1.4.6 配置注意事项

- 在隧道的两端应配置相同的隧道模式，否则可能造成报文传输失败。
- 自动隧道不需要配置目的地址。
- 对于自动隧道，使用同种封装协议的 Tunnel 接口不能同时配置完全相同的源地址。
- 分布式交换机（例如 S7500E 系列）的 Tunnel 接口号的形式为 A/B/C，A、B、C 分别代表单板槽位号、子卡槽位号、Tunnel 接口号。
- 当在分布式交换机（例如 S7500E 系列）上创建 Tunnel 接口时，建议 Tunnel 接口的槽号与所设置的源端端口所在槽位保持一致，即使用发出报文的实际端口的槽位号，这样可以提高转发效率。
- 在分布式交换机（例如 S7500E 系列）上，主备倒换或备板被拔出时，建立在主控板或备板上的隧道不会被真正删除，若再配置相同的隧道，系统会提示隧道已经存在。如果需要真正删除隧道接口，请使用 **undo interface tunnel** 命令来删除。
- 如果隧道两端 Tunnel 接口的地址不在同一个网段，则必须配置通过隧道到达对端的转发路由，以便需要进行封装的报文能正常转发。
- 配置静态路由时，需要手动配置到达目的地址（不是隧道的终点 IPv4 地址，而是封装前报文的目的 IPv6 地址）的路由，并配置出接口为本端 Tunnel 接口或下一跳为对端的 Tunnel 接口地址。在隧道的两端都要进行此项配置。
- 对于自动隧道，不支持动态路由。

### 1.5 ISATAP 隧道典型配置指导

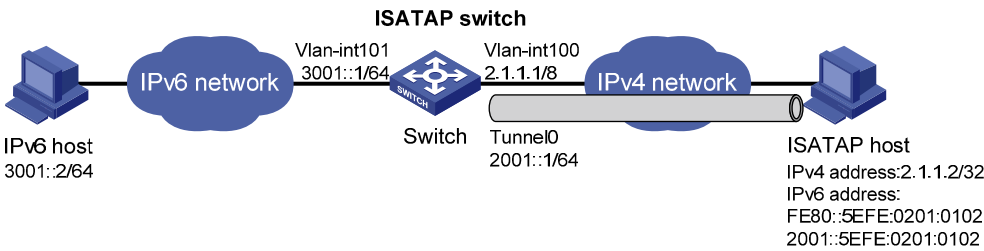
ISATAP 隧道是点到点的自动隧道技术，通过在 IPv6 报文的目的地址中嵌入的 IPv4 地址，可以自动获取隧道的终点。

使用 ISATAP 隧道时，IPv6 报文的目的地址和隧道接口的 IPv6 地址都要采用特殊的 ISATAP 地址。ISATAP 地址格式为：Prefix(64bit):0:5EFE:ip-address。其中，64 位的 Prefix 为任何合法的 IPv6 单播地址前缀，ip-address 为 32 位 IPv4 源地址，形式为 a.b.c.d 或者 abcd:efgh，且该 IPv4 地址不要求全球唯一。通过这个嵌入的 IPv4 地址就可以自动建立隧道，完成 IPv6 报文的传送。

ISATAP 隧道主要用于在 IPv4 网络中 IPv6 路由器-IPv6 路由器、IPv6 主机-IPv6 路由器的连接。

1.5.1 组网图

图1-5 ISATAP 隧道组网图



1.5.2 应用要求

如 图 1-5所示，IPv6 网络和IPv4 网络通过ISATAP交换机相连，要求将IPv4 网络中的IPv6 主机通过 ISATAP隧道接入到IPv6 网络。

1.5.3 适用产品、版本

表1-5 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本    |
|-------------------|---------------------------------|---------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本 |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本 |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本 |

1.5.4 配置过程和解释



说明

- 已经在 Switch 上创建相应的 VLAN 接口；
- 已经配置 Switch 的 Vlan-interface101 和 ISATAP host 之间 IPv4 报文路由可达。
- 对于 S3610/S5510 系列以太网交换机，在使能 IPv6 功能之前，必须先将设备运行模式切换到 IPv4/IPv6 双协议栈模式，即执行 **switch-mode dual-ipv4-ipv6** 命令；否则，即使使能 IPv6，设备也不支持 IPv6 报文的转发。另外需要注意的是，执行 **switch-mode** 命令切换的协议栈只有在重启设备后才能生效。

(1) 配置 Switch

# 使能 IPv6 转发功能。

```
<Switch> system-view
```

```
[Switch] ipv6
```

# 配置各接口地址。

```
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ipv6 address 3001::1/64
[Switch-Vlan-interface100] quit
[Switch] interface vlan-interface 101
[Switch-Vlan-interface101] ip address 2.1.1.1 255.0.0.0
[Switch-Vlan-interface101] quit
```

# 配置链路聚合组或业务环回组，请根据产品实际支持情况进行选择。



#### 注意

- S7500E Release 6300 软件版本的隧道接口必须引用业务环回组以实现报文的接收和发送，且隧道引用的业务环回组必须已创建，否则隧道接口状态不会 up，隧道无法通讯。
  - 表 1-5 所列除 S7500E Release 6300 软件版本外的其它产品，隧道接口必须引用链路聚合组以实现报文的接收和发送，且隧道引用的链路聚合组必须已创建，否则隧道接口状态不会 up，隧道无法通讯。
- 

- 配置链路聚合组。需要注意的是，将端口加入到链路聚合组时，需要在端口上关闭 STP 功能。

```
[Switch] link-aggregation group 1 mode manual
[Switch] link-aggregation group 1 service-type tunnel
[Switch] interface GigabitEthernet 1/0/3
[Switch-GigabitEthernet1/0/3] stp disable
[Switch-GigabitEthernet1/0/3] port link-aggregation group 1
[Switch-GigabitEthernet1/0/3] quit
```

- 配置业务环回组。需要注意的是，将端口加入到业务环回组时，需要在端口上关闭 STP 功能。

```
[Switch] service-loopback group 1 type tunnel
[Switch] interface GigabitEthernet 1/0/3
[Switch-GigabitEthernet1/0/3] stp disable
[Switch-GigabitEthernet1/0/3] port service-loopback group 1
[Switch-GigabitEthernet1/0/3] quit
```

# 配置 ISATAP 隧道。

```
[Switch] interface tunnel 0
[Switch-Tunnel0] ipv6 address 2001::1/64 eui-64
[Switch-Tunnel0] source vlan-interface 101
[Switch-Tunnel0] tunnel-protocol ipv6-ipv4 isatap
```

# 在 Tunnel 接口视图下配置隧道引用链路聚合组 1 或业务环回组 1，请根据产品实际支持情况进行选择。

- 在 Tunnel 接口视图下配置隧道引用链路聚合组 1。

```
[Switch-Tunnel0] aggregation-group 1
```

- 在 Tunnel 接口视图下配置隧道引用业务环回组 1。

```
[Switch-Tunnel0] service-loopback-group 1
```

# 取消对 RA 消息发布的抑制，使主机可以通过交换机发布的 RA 消息获取地址前缀等信息。

```
[Switch-Tunnel0] undo ipv6 nd ra halt
```

```
[Switch-Tunnel0] quit
```

# 配置到 ISATAP 主机的静态路由。

```
[Switch] ipv6 route-static 2001:: 16 tunnel 0
```

## (2) 配置主机

ISATAP 主机上的具体配置与主机的操作系统有关，下面仅以 Windows XP 操作系统为例进行说明。

# 在 Windows XP 上，ISATAP 接口通常为接口 2，只要在该接口上配置 ISATAP 交换机的 IPv4 地址即可完成主机侧的配置。先看看这个 ISATAP 接口的信息：

```
C:\>ipv6 if 2
```

```
Interface 2: Automatic Tunneling Pseudo-Interface
```

```
Guid {48FCE3FC-EC30-E50E-F1A7-71172AEEE3AE}
```

```
does not use Neighbor Discovery
```

```
does not use Router Discovery
```

```
routing preference 1
```

```
EUI-64 embedded IPv4 address: 0.0.0.0
```

```
router link-layer address: 0.0.0.0
```

```
preferred link-local fe80::5efe:2.1.1.2, life infinite
```

```
link MTU 1280 (true link MTU 65515)
```

```
current hop limit 128
```

```
reachable time 42500ms (base 30000ms)
```

```
retransmission interval 1000ms
```

```
DAD transmits 0
```

```
default site prefix length 48
```

# 它自动生成了一个 ISATAP 格式的 link-local 地址（fe80::5efe:2.1.1.2）。我们需要设置这个接口上的 ISATAP 交换机的 IPv4 地址：

```
C:\>ipv6 rlu 2 2.1.1.1
```

# 只需要这么一个命令，这就完成了主机的配置，我们再来看看这个 ISATAP 接口的信息：

```
C:\>ipv6 if 2
```

```
Interface 2: Automatic Tunneling Pseudo-Interface
```

```
Guid {48FCE3FC-EC30-E50E-F1A7-71172AEEE3AE}
```

```
does not use Neighbor Discovery
```

```
uses Router Discovery
```

```
routing preference 1
```

```
EUI-64 embedded IPv4 address: 2.1.1.2
```

```
router link-layer address: 2.1.1.1
```

```
preferred global 2001::5efe:2.1.1.2, life 29d23h59m46s/6d23h59m46s (public)
```

```
preferred link-local fe80::5efe:2.1.1.2, life infinite
```

```
link MTU 1500 (true link MTU 65515)
```

```
current hop limit 255
```

```
reachable time 42500ms (base 30000ms)
```

```
retransmission interval 1000ms
```

```
DAD transmits 0
```

```
default site prefix length 48
```



# 对比前后的区别，我们可以看到主机获取了 2001::/64 的前缀，自动生成地址 2001::5efe:2.1.1.2，同时还会发现这么一行“uses Router Discovery”表明主机启用了路由器发现，这时 ping 一下交换机上隧道接口的 IPv6 地址，可以 ping 通，这时候表明 ISATAP 隧道已经成功建立。

### 1.5.5 完整配置

- Switch 上的配置（隧道引用链路聚合组）

```
#
ipv6
#
link-aggregation group 1 mode manual
link-aggregation group 1 service-type tunnel
#
interface Vlan-interface100
ipv6 address 3001::1/64
#
interface Vlan-interface101
ip address 2.1.1.1 255.0.0.0
#
interface GigabitEthernet1/0/3
stp disable
port link-aggregation group 1
#
interface Tunnel0
ipv6 address 2001::1/64 eui-64
undo ipv6 nd ra halt
tunnel-protocol ipv6-ipv4 isatap
source Vlan-interface101
aggregation-group 1
#
ipv6 route-static 2001::16 tunnel 0
#
```

- Switch 上的配置（隧道引用业务环回组）

```
#
ipv6
#
service-loopback group 1 type tunnel
#
interface Vlan-interface100
ipv6 address 3001::1/64
#
interface Vlan-interface101
ip address 2.1.1.1 255.0.0.0
#
interface GigabitEthernet1/0/3
stp disable
port service-loopback group 1
#
```

```

interface Tunnel0
 ipv6 address 2001::1/64 eui-64
 undo ipv6 nd ra halt
 tunnel-protocol ipv6-ipv4 isatap
 source Vlan-interface101
 service-loopback-group 1
#
 ipv6 route-static 2001:: 16 tunnel 0
#

```

### 1.5.6 配置注意事项

- 对于自动隧道，使用同种封装协议的 Tunnel 接口不能同时配置完全相同的源地址。
- 分布式交换机（例如 S7500E 系列）的 Tunnel 接口号的形式为 A/B/C，A、B、C 分别代表单板槽位号、子卡槽位号、Tunnel 接口号。
- 当在分布式交换机（例如 S7500E 系列）上创建 Tunnel 接口时，建议 Tunnel 接口的槽号与所设置的源端端口所在槽位保持一致，即使用发出报文的实际端口的槽位号，这样可以提高转发效率。
- 在分布式交换机（例如 S7500E 系列）上，主备倒换或备板被拔出时，建立在主控板或备板上的隧道不会被真正删除，若再配置相同的隧道，系统会提示隧道已经存在。如果需要真正删除隧道接口，请使用 **undo interface tunnel** 命令来删除。
- 如果隧道两端 Tunnel 接口的地址不在同一个网段，则必须配置通过隧道到达对端的转发路由，以便需要进行封装的报文能正常转发。
- 配置静态路由时，需要手动配置到达目的地址（不是隧道的终点 IPv4 地址，而是封装前报文的目的 IPv6 地址）的路由，并配置出接口为本端 Tunnel 接口或下一跳为对端的 Tunnel 接口地址。在隧道的两端都要进行此项配置。
- 对于自动隧道，不支持动态路由。

# 目 录

|                                       |      |
|---------------------------------------|------|
| 1 IPv6 路由典型配置指导 .....                 | 1-1  |
| 1.1 IPv6 静态路由典型配置指导 .....             | 1-1  |
| 1.1.1 组网图 .....                       | 1-1  |
| 1.1.2 应用要求 .....                      | 1-1  |
| 1.1.3 适用产品、版本 .....                   | 1-1  |
| 1.1.4 配置过程和解释 .....                   | 1-2  |
| 1.1.5 完整配置 .....                      | 1-3  |
| 1.1.6 配置注意事项 .....                    | 1-4  |
| 1.2 IPv6 RIPng路由协议典型配置指导 .....        | 1-4  |
| 1.2.1 组网图 .....                       | 1-4  |
| 1.2.2 应用要求 .....                      | 1-4  |
| 1.2.3 适用产品、版本 .....                   | 1-4  |
| 1.2.4 配置过程和解释 .....                   | 1-5  |
| 1.2.5 完整配置 .....                      | 1-7  |
| 1.2.6 配置注意事项 .....                    | 1-8  |
| 1.3 配置RIPng引入外部路由典型配置指导 .....         | 1-9  |
| 1.3.1 组网图 .....                       | 1-9  |
| 1.3.2 应用要求 .....                      | 1-9  |
| 1.3.3 适用产品、版本 .....                   | 1-9  |
| 1.3.4 配置过程和解释 .....                   | 1-9  |
| 1.3.5 完整配置 .....                      | 1-11 |
| 1.3.6 配置注意事项 .....                    | 1-13 |
| 1.4 IPv6 RIPng跨越IPv4 网络应用典型配置指导 ..... | 1-13 |
| 1.4.1 组网图 .....                       | 1-13 |
| 1.4.2 应用要求 .....                      | 1-13 |
| 1.4.3 适用产品、版本 .....                   | 1-13 |
| 1.4.4 配置过程和解释 .....                   | 1-14 |
| 1.4.5 完整配置 .....                      | 1-15 |
| 1.4.6 配置注意事项 .....                    | 1-17 |
| 1.5 配置OSPFv3 区域典型配置指导 .....           | 1-17 |
| 1.5.1 组网图 .....                       | 1-18 |
| 1.5.2 应用要求 .....                      | 1-18 |
| 1.5.3 适用产品、版本 .....                   | 1-18 |
| 1.5.4 配置过程和解释 .....                   | 1-18 |
| 1.5.5 完整配置 .....                      | 1-22 |
| 1.5.6 配置注意事项 .....                    | 1-23 |
| 1.6 OSPFv3 引入外部路由典型配置指导 .....         | 1-24 |
| 1.6.1 组网图 .....                       | 1-24 |
| 1.6.2 应用要求 .....                      | 1-24 |
| 1.6.3 适用产品、版本 .....                   | 1-25 |
| 1.6.4 配置过程和解释 .....                   | 1-25 |
| 1.6.5 完整配置 .....                      | 1-27 |

|                                    |      |
|------------------------------------|------|
| 1.6.6 配置注意事项 .....                 | 1-29 |
| 1.7 OSPFv3 的DR选择典型配置指导 .....       | 1-29 |
| 1.7.1 组网图 .....                    | 1-29 |
| 1.7.2 应用要求 .....                   | 1-29 |
| 1.7.3 适用产品、版本 .....                | 1-29 |
| 1.7.4 配置过程和解释 .....                | 1-30 |
| 1.7.5 完整配置 .....                   | 1-32 |
| 1.7.6 配置注意事项 .....                 | 1-33 |
| 1.8 IPv6 IS-IS路由协议典型配置指导 .....     | 1-34 |
| 1.8.1 组网图 .....                    | 1-34 |
| 1.8.2 应用要求 .....                   | 1-34 |
| 1.8.3 适用的产品、版本 .....               | 1-35 |
| 1.8.4 配置过程和解释 .....                | 1-35 |
| 1.8.5 完整配置 .....                   | 1-36 |
| 1.8.6 配置注意事项 .....                 | 1-38 |
| 1.9 IPv6 BGP路由协议基本配置指导 .....       | 1-38 |
| 1.9.1 组网图 .....                    | 1-38 |
| 1.9.2 应用要求 .....                   | 1-38 |
| 1.9.3 适用产品、版本 .....                | 1-39 |
| 1.9.4 配置过程和解释 .....                | 1-39 |
| 1.9.5 完整配置 .....                   | 1-40 |
| 1.9.6 配置注意事项 .....                 | 1-42 |
| 1.10 IPv6 BGP路由反射典型配置指导 .....      | 1-43 |
| 1.10.1 组网图 .....                   | 1-43 |
| 1.10.2 应用要求 .....                  | 1-43 |
| 1.10.3 适用产品、版本 .....               | 1-43 |
| 1.10.4 配置过程和解释 .....               | 1-43 |
| 1.10.5 完整配置 .....                  | 1-44 |
| 1.10.6 配置注意事项 .....                | 1-46 |
| 1.11 在IPv6 路由引入中应用路由策略典型配置指导 ..... | 1-46 |
| 1.11.1 组网图 .....                   | 1-47 |
| 1.11.2 应用要求 .....                  | 1-47 |
| 1.11.3 适用产品、版本 .....               | 1-47 |
| 1.11.4 配置过程和解释 .....               | 1-47 |
| 1.11.5 完整配置 .....                  | 1-49 |
| 1.11.6 配置注意事项 .....                | 1-50 |

# 1 IPv6 路由典型配置指导

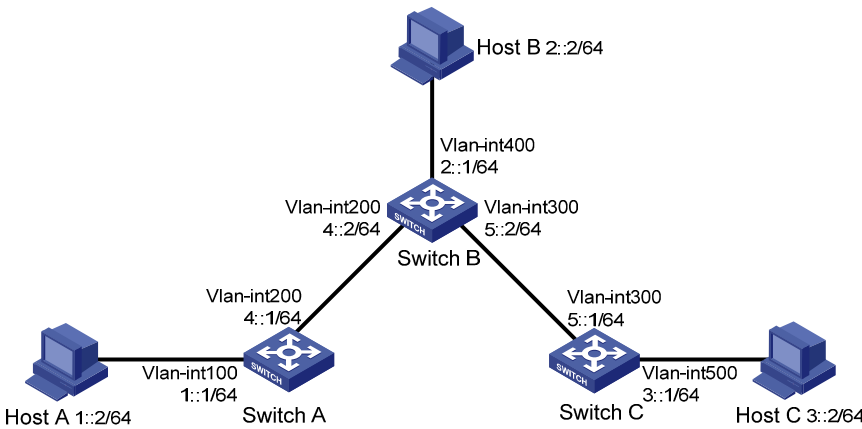
## 1.1 IPv6 静态路由典型配置指导

静态路由是一种特殊的路由，它由管理员手工配置。当网络结构比较简单时，只需配置静态路由就可以使网络正常工作。恰当地设置和使用静态路由可以改进网络的性能，并可为重要的应用保证带宽。

静态路由的缺点在于：当网络发生故障或者拓扑发生变化后，可能会出现路由不可达，导致网络中断，此时必须由网络管理员手工修改静态路由的配置。

### 1.1.1 组网图

图1-1 IPv6 静态路由配置示例图



### 1.1.2 应用要求

要求各交换机之间配置 IPv6 静态路由协议后，可以使所有主机和交换机之间互通。

### 1.1.3 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本                         |
|-------------------|---------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本               | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本               | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本                      |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本                      |

### 1.1.4 配置过程和解释

(1) 配置各 VLAN 虚接口的 IPv6 地址（略）

(2) 配置 IPv6 静态路由

# 在 Switch A 上配置 IPv6 缺省路由。

```
<SwitchA> system-view
[SwitchA] ipv6
[SwitchA] ipv6 route-static :: 0 4::2
```

# 在 Switch B 上配置两条 IPv6 静态路由。

```
<SwitchB> system-view
[SwitchB] ipv6
[SwitchB] ipv6 route-static 1:: 64 4::1
[SwitchB] ipv6 route-static 3:: 64 5::1
```

# 在 Switch C 上配置 IPv6 缺省路由。

```
<SwitchC> system-view
[SwitchC] ipv6
[SwitchC] ipv6 route-static :: 0 5::2
```

(3) 配置主机地址和网关

根据组网图配置好各主机的 IPv6 地址，并将 Host A 的缺省网关配置为 1::1，Host B 的缺省网关配置为 2::1，Host C 的缺省网关配置为 3::1。

(4) 查看配置结果

# 查看 Switch A 的 IPv6 路由表。

```
[SwitchA] display ipv6 routing-table
```

Routing Table :

```
Destinations : 7 Routes : 7
```

```
Destination: ::/0 Protocol : Static
NextHop : 4::2 Preference: 60
Interface : Vlan200 Cost : 0
```

```
Destination: ::1/128 Protocol : Direct
NextHop : ::1 Preference: 0
Interface : InLoop0 Cost : 0
```

```
Destination: 1::/64 Protocol : Direct
NextHop : 1::1 Preference: 0
Interface : Vlan100 Cost : 0
```

```
Destination: 1::1/128 Protocol : Direct
NextHop : ::1 Preference: 0
Interface : InLoop0 Cost : 0
```

```
Destination: 4::/64 Protocol : Direct
NextHop : 4::1 Preference: 0
Interface : Vlan200 Cost : 0
```

```
Destination: 4::1/128 Protocol : Direct
NextHop : ::1 Preference: 0
Interface : InLoop0 Cost : 0
```

```
Destination: FE80::/10 Protocol : Direct
NextHop : :: Preference: 0
Interface : NULL0 Cost : 0
```

# 使用 Ping 进行验证。

```
[SwitchA] ping ipv6 3::1
PING 3::1 : 56 data bytes, press CTRL_C to break
Reply from 3::1
bytes=56 Sequence=1 hop limit=254 time = 63 ms
Reply from 3::1
bytes=56 Sequence=2 hop limit=254 time = 62 ms
Reply from 3::1
bytes=56 Sequence=3 hop limit=254 time = 62 ms
Reply from 3::1
bytes=56 Sequence=4 hop limit=254 time = 63 ms
Reply from 3::1
bytes=56 Sequence=5 hop limit=254 time = 63 ms

--- 3::1 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 62/62/63 ms
```

### 1.1.5 完整配置

- 配置 Switch A

```
#
ipv6
#
ipv6 route-static :: 0 4::2
#
```

- 配置 Switch B

```
#
ipv6
#
ipv6 route-static 1:: 64 4::1
ipv6 route-static 3:: 64 5::1
#
```

- 配置 Switch C

```
#
ipv6
#
ipv6 route-static :: 0 5::2
```

### 1.1.6 配置注意事项

在配置静态路由时，可以指定出接口，如果出接口类型为 VLAN 接口，则必须指定下一跳地址。

## 1.2 IPv6 RIPng 路由协议典型配置指导

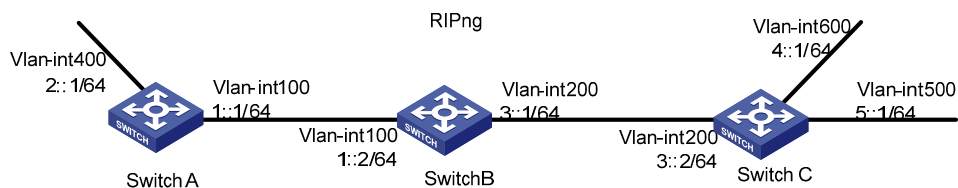
RIPng 又称为下一代 RIP 协议（RIP next generation），它是对原来的 IPv4 网络中 RIP-2 协议的扩展。大多数 RIP 的概念都可以用于 RIPng。

为了在 IPv6 网络中应用，RIPng 对原有的 RIP 协议进行了如下修改：

- UDP 端口号：使用 UDP 的 521 端口发送和接收路由信息。
- 组播地址：使用 FF02::9 作为链路本地范围内的 RIPng 路由器组播地址。
- 前缀长度：目的地址使用 128 比特的前缀长度。
- 下一跳地址：使用 128 比特的 IPv6 地址。
- 源地址：使用链路本地地址 FE80::/10 作为源地址发送 RIPng 路由信息更新报文。

### 1.2.1 组网图

图1-2 RIPng 配置组网图



### 1.2.2 应用要求

- Switch A、Switch B 和 Switch C 相连并通过 RIPng 来学习网络中的 IPv6 路由信息；
- 在 Switch B 上对接收的 Switch C 的路由（3::/64）进行过滤，使其不加入到 Switch B 的 RIPng 进程的路由表中，也不发布给 Switch A。

### 1.2.3 适用产品、版本

表1-2 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本                         |
|-------------------|---------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本               | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本               | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本                      |



| 产品                | 软件版本              | 硬件版本    |
|-------------------|-------------------|---------|
| S3500-EA 系列以太网交换机 | Release 5303 软件版本 | 全系列硬件版本 |

#### 1.2.4 配置过程和解释

(1) 配置各接口的 IPv6 地址（略）

(2) 配置 RIPng 的基本功能

# 配置 Switch A。

```
<SwitchA> system-view
[SwitchA] ipv6
[SwitchA] ripng 1
[SwitchA-ripng-1] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ripng 1 enable
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 400
[SwitchA-Vlan-interface400] ripng 1 enable
[SwitchA-Vlan-interface400] quit
```

# 配置 Switch B。

```
<SwitchB> system-view
[SwitchB] ipv6
[SwitchB] ripng 1
[SwitchB-ripng-1] quit
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] ripng 1 enable
[SwitchB-Vlan-interface200] quit
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ripng 1 enable
[SwitchB-Vlan-interface100] quit
```

# 配置 Switch C。

```
<SwitchC> system-view
[SwitchC] ipv6
[SwitchC] ripng 1
[SwitchC-ripng-1] quit
[SwitchC] interface vlan-interface 200
[SwitchC-Vlan-interface200] ripng 1 enable
[SwitchC-Vlan-interface200] quit
[SwitchC] interface vlan-interface 500
[SwitchC-Vlan-interface500] ripng 1 enable
[SwitchC-Vlan-interface500] quit
[SwitchC] interface vlan-interface 600
[SwitchC-Vlan-interface600] ripng 1 enable
[SwitchC-Vlan-interface600] quit
```

# 查看 Switch B 的 RIPng 路由表。

```
[SwitchB] display ripng 1 route
Route Flags: A - Aging, S - Suppressed, G - Garbage-collect

Peer FE80::20F:E2FF:FE23:82F5 on Vlan-interface100
Dest 1::/64,
 via FE80::20F:E2FF:FE23:82F5, cost 1, tag 0, A, 6 Sec
Dest 2::/64,
 via FE80::20F:E2FF:FE23:82F5, cost 1, tag 0, A, 6 Sec

Peer FE80::20F:E2FF:FE00:100 on Vlan-interface200
Dest 3::/64,
 via FE80::20F:E2FF:FE00:100, cost 1, tag 0, A, 11 Sec
Dest 4::/64,
 via FE80::20F:E2FF:FE00:100, cost 1, tag 0, A, 11 Sec
Dest 5::/64,
 via FE80::20F:E2FF:FE00:100, cost 1, tag 0, A, 11 Sec
```

# 查看 Switch A 的 RIPng 路由表。

```
[SwitchA] display ripng 1 route
Route Flags: A - Aging, S - Suppressed, G - Garbage-collect

Peer FE80::200:2FF:FE64:8904 on Vlan-interface100
Dest 1::/64,
 via FE80::200:2FF:FE64:8904, cost 1, tag 0, A, 31 Sec
Dest 4::/64,
 via FE80::200:2FF:FE64:8904, cost 2, tag 0, A, 31 Sec
Dest 5::/64,
 via FE80::200:2FF:FE64:8904, cost 2, tag 0, A, 31 Sec
Dest 3::/64,
 via FE80::200:2FF:FE64:8904, cost 1, tag 0, A, 31 Sec
```

(3) 配置 Switch B 对接收和发布的路由进行过滤

```
[SwitchB] acl ipv6 number 2000
[SwitchB-acl6-basic-2000] rule deny source 3::/64
[SwitchB-acl6-basic-2000] rule permit
[SwitchB-acl6-basic-2000] quit
[SwitchB] ripng 1
[SwitchB-ripng-1] filter-policy 2000 import
[SwitchB-ripng-1] filter-policy 2000 export
[SwitchB-ripng-1] quit
```

# 查看 Switch B 和 Switch A 的 RIPng 路由表。

```
[SwitchB] display ripng 1 route
Route Flags: A - Aging, S - Suppressed, G - Garbage-collect

Peer FE80::20F:E2FF:FE23:82F5 on Vlan-interface100
Dest 1::/64,
```

```

 via FE80::20F:E2FF:FE23:82F5, cost 1, tag 0, A, 2 Sec
Dest 2::/64,
 via FE80::20F:E2FF:FE23:82F5, cost 1, tag 0, A, 2 Sec

Peer FE80::20F:E2FF:FE00:100 on Vlan-interface200
Dest 4::/64,
 via FE80::20F:E2FF:FE00:100, cost 1, tag 0, A, 5 Sec
Dest 5::/64,
 via FE80::20F:E2FF:FE00:100, cost 1, tag 0, A, 5 Sec
[SwitchA] display ripng 1 route
Route Flags: A - Aging, S - Suppressed, G - Garbage-collect

Peer FE80::20F:E2FF:FE00:1235 on Vlan-interface100
Dest 1::/64,
 via FE80::20F:E2FF:FE00:1235, cost 1, tag 0, A, 2 Sec
Dest 4::/64,
 via FE80::20F:E2FF:FE00:1235, cost 2, tag 0, A, 2 Sec
Dest 5::/64,
 via FE80::20F:E2FF:FE00:1235, cost 2, tag 0, A, 2 Sec

```

### 1.2.5 完整配置

- 配置 Switch A

```

#
ipv6
#
vlan 100
#
vlan 400
#
interface Vlan-interface100
 ipv6 address 1::1/64
 ripng 1 enable
#
interface Vlan-interface400
 ipv6 address 2::1/64
 ripng 1 enable
#
ripng 1
#

```

- 配置 Switch B

```

#
ipv6
#
vlan 100
#
vlan 200
#

```

```

acl ipv6 number 2000
 rule 0 deny source 3::/64
 rule 5 permit
#
interface Vlan-interface100
 ipv6 address 1::2/64
 ripng 1 enable
#
interface Vlan-interface200
 ipv6 address 3::1/64
 ripng 1 enable
#
ripng 1
 filter-policy 2000 import
 filter-policy 2000 export
#

```

- 配置 Switch C

```

#
ipv6
#
vlan 200
#
vlan 500
#
vlan 600
#
interface Vlan-interface200
 ipv6 address 3::2/64
 ripng 1 enable
#
interface Vlan-interface500
 ipv6 address 5::1/64
 ripng 1 enable
#
interface Vlan-interface600
 ipv6 address 4::1/64
 ripng 1 enable
#
ripng 1
#

```

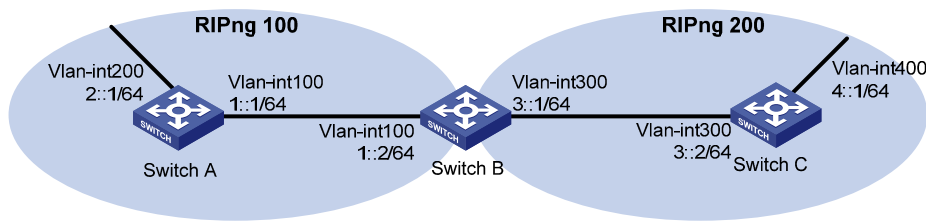
### 1.2.6 配置注意事项

如果接口没有使能 RIPng，那么 RIPng 进程在该接口上既不发送也不接收 RIPng 路由。

## 1.3 配置 RIPng 引入外部路由典型配置指导

### 1.3.1 组网图

图1-3 配置 RIPng 引入外部路由组网图



### 1.3.2 应用要求

如图 1-3所示，Switch B上运行两个RIPng进程：RIPng100 和RIPng200。Switch B通过RIPng100 和Switch A交换路由信息，通过RIPng200 和Switch C交换路由信息。

要求在 Switch B 上配置路由引入，将两个不同进程的 RIPng 路由相互引入到对方的 RIPng 进程中，将引入的 RIPng200 的路由缺省度量值设为 3。

### 1.3.3 适用产品、版本

表1-3 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本    |
|-------------------|---------------------------------|---------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本 |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本 |

### 1.3.4 配置过程和解释

(1) 配置各接口的 IPv6 地址（略）

# 在 Switch A 上启动 RIPng 进程 100。

```
<SwitchA> system-view
[SwitchA] ripng 100
[SwitchA-ripng-100] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ripng 100 enable
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 200
[SwitchA-Vlan-interface200] ripng 100 enable
```

# 在 Switch B 上启动两个 RIPng 进程，进程号分别为 100 和 200。

```
<SwitchB> system-view
[SwitchB] ripng 100
```

```
[SwitchB-ripng-100] quit
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ripng 100 enable
[SwitchB-Vlan-interface100] quit
[SwitchB] ripng 200
[SwitchB-ripng-200] quit
[SwitchB] interface vlan-interface 300
[SwitchA-Vlan-interface300] ripng 200 enable
```

# 在 Switch C 上启动 RIPng 进程 200。

```
<SwitchC> system-view
[SwitchC] ripng 200
[SwitchC] interface vlan-interface 300
[SwitchC-Vlan-interface300] ripng 200 enable
[SwitchC-Vlan-interface300] quit
[SwitchC] interface vlan-interface 400
[SwitchC-Vlan-interface400] ripng 200 enable
[SwitchC-Vlan-interface400] quit
```

# 查看 Switch A 的路由表信息。

```
[SwitchA] display ipv6 routing-table
```

Routing Table :

| Destinations : 6 | Routes : 6 |
|------------------|------------|
|------------------|------------|

|                      |                   |
|----------------------|-------------------|
| Destination: ::1/128 | Protocol : Direct |
| NextHop : ::1        | Preference: 0     |
| Interface : InLoop0  | Cost : 0          |

|                     |                   |
|---------------------|-------------------|
| Destination: 1::/64 | Protocol : Direct |
| NextHop : 1::1      | Preference: 0     |
| Interface : Vlan100 | Cost : 0          |

|                       |                   |
|-----------------------|-------------------|
| Destination: 1::1/128 | Protocol : Direct |
| NextHop : ::1         | Preference: 0     |
| Interface : InLoop0   | Cost : 0          |

|                     |                   |
|---------------------|-------------------|
| Destination: 2::/64 | Protocol : Direct |
| NextHop : 2::1      | Preference: 0     |
| Interface : Vlan200 | Cost : 0          |

|                       |                   |
|-----------------------|-------------------|
| Destination: 2::1/128 | Protocol : Direct |
| NextHop : ::1         | Preference: 0     |
| Interface : InLoop0   | Cost : 0          |

|                        |                   |
|------------------------|-------------------|
| Destination: FE80::/10 | Protocol : Direct |
| NextHop : ::           | Preference: 0     |
| Interface : NULL0      | Cost : 0          |

(2) 配置 RIPng 引入外部路由

# 在 Switch B 上将两个不同 RIPng 进程的路由相互引入到对方的路由表中。

```
[SwitchB] ripng 100
[SwitchB-ripng-100] default cost 3
[SwitchB-ripng-100] import-route ripng 200
[SwitchB-ripng-100] quit
[SwitchB] ripng 200
[SwitchB-ripng-200] import-route ripng 100
[SwitchB-ripng-200] quit
```

# 查看路由引入后 Switch A 的路由表信息。

```
[SwitchA] display ipv6 routing-table
```

Routing Table :

|                  |            |
|------------------|------------|
| Destinations : 7 | Routes : 7 |
|------------------|------------|

|                      |                   |
|----------------------|-------------------|
| Destination: ::1/128 | Protocol : Direct |
| NextHop : ::1        | Preference: 0     |
| Interface : InLoop0  | Cost : 0          |

|                     |                   |
|---------------------|-------------------|
| Destination: 1::/64 | Protocol : Direct |
| NextHop : 1::1      | Preference: 0     |
| Interface : Vlan100 | Cost : 0          |

|                       |                   |
|-----------------------|-------------------|
| Destination: 1::1/128 | Protocol : Direct |
| NextHop : ::1         | Preference: 0     |
| Interface : InLoop0   | Cost : 0          |

|                     |                   |
|---------------------|-------------------|
| Destination: 2::/64 | Protocol : Direct |
| NextHop : 2::1      | Preference: 0     |
| Interface : Vlan200 | Cost : 0          |

|                       |                   |
|-----------------------|-------------------|
| Destination: 2::1/128 | Protocol : Direct |
| NextHop : ::1         | Preference: 0     |
| Interface : InLoop0   | Cost : 0          |

|                                   |                  |
|-----------------------------------|------------------|
| Destination: 4::/64               | Protocol : RIPng |
| NextHop : FE80::200:BFF:FE01:1C02 | Preference: 100  |
| Interface : Vlan100               | Cost : 4         |

|                        |                   |
|------------------------|-------------------|
| Destination: FE80::/10 | Protocol : Direct |
| NextHop : ::           | Preference: 0     |
| Interface : NULL0      | Cost : 0          |

### 1.3.5 完整配置

- 配置 Switch A

```
#
```

```
ipv6
```

```
#
```

```
vlan 100
```

```
#
vlan 200
#
interface Vlan-interface100
ipv6 address 1::1/64
ripng 100 enable
#
interface Vlan-interface200
ipv6 address 2::1/64
ripng 100 enable
#
ripng 200
#
```

- 配置 Switch B

```
#
ipv6
#
vlan 100
#
vlan 300
#
interface Vlan-interface100
ipv6 address 1::2/64
ripng 100 enable
#
interface Vlan-interface300
ipv6 address 3::1/64
ripng 200 enable
#
ripng 100
default cost 3
import-route ripng 200
#
ripng 200
import-route ripng 100
#
```

- 配置 Switch C

```
#
ipv6
#
vlan 300
#
vlan 400
#
interface Vlan-interface300
ipv6 address 3::2/64
ripng 200 enable
```



```
#
interface Vlan-interface400
 ipv6 address 4::1/64
 ripng 200 enable
#
ripng 200
#
```

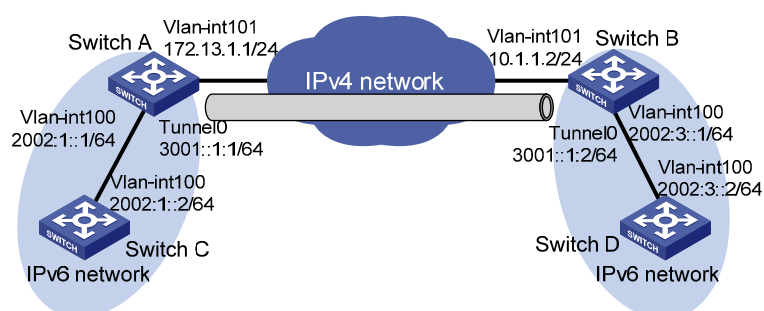
### 1.3.6 配置注意事项

- S5500-EI 系列交换机的 Release 2102 软件版本仅支持 RIPng 单进程。
- S5500-SI 系列交换机的 Release 1207 软件版本和 Release 1301 软件版本仅支持 RIPng 单进程。

## 1.4 IPv6 RIPng 跨越 IPv4 网络应用典型配置指导

### 1.4.1 组网图

图1-4 IPv6 RIPng 跨越 IPv4 网络应用典型配置指导



### 1.4.2 应用要求

如图 1-4所示，两个IPv6 网络分别通过Switch A和Switch B与IPv4 网络连接，Switch A与Switch B 之间路由可达，要求在Switch A和Switch B之间建立IPv6 手动隧道，使两个IPv6 网络可以使用RIPng 进行网络互连。

### 1.4.3 适用产品、版本

表1-4 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本    |
|-------------------|---------------------------------|---------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本 |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本 |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本 |

#### 1.4.4 配置过程和解释

(1) 配置各接口的 IPv6 地址和 IPv4 地址（略）

(2) 配置 Switch A

# 使能 IPv6 转发功能。

```
<SwitchA> system-view
```

```
[SwitchA] ipv6
```

# 配置手动隧道。

```
[SwitchA] interface tunnel 0
```

```
[SwitchA-Tunnel0] ipv6 address 3001::1:1 64
```

```
[SwitchA-Tunnel0] source vlan-interface 101
```

```
[SwitchA-Tunnel0] destination 10.1.1.2
```

```
[SwitchA-Tunnel0] tunnel-protocol ipv6-ipv4
```

```
[SwitchA-Tunnel0] quit
```

# 配置 RIPng 的基本功能

```
[SwitchA] ripng 1
```

```
[SwitchA-ripng-1] quit
```

```
[SwitchA] interface vlan-interface 100
```

```
[SwitchA-Vlan-interface100] ripng 1 enable
```

```
[SwitchA-Vlan-interface100] quit
```

```
[SwitchA] interface tunnel 0
```

```
[SwitchA-Tunnel0] ripng 1 enable
```

```
[SwitchA-Tunnel0] quit
```

(3) 配置 Switch B

# 使能 IPv6 转发功能。

```
<SwitchB> system-view
```

```
[SwitchB] ipv6
```

# 配置手动隧道。

```
[SwitchB] interface tunnel 0
```

```
[SwitchB-Tunnel0] ipv6 address 3001::1:2 64
```

```
[SwitchB-Tunnel0] source vlan-interface 101
```

```
[SwitchB-Tunnel0] destination 172.13.1.1
```

```
[SwitchB-Tunnel0] tunnel-protocol ipv6-ipv4
```

```
[SwitchB-Tunnel0] quit
```

# 配置 RIPng 的基本功能

```
[SwitchA] ripng 1
```

```
[SwitchA-ripng-1] quit
```

```
[SwitchA] interface vlan-interface 100
```

```
[SwitchA-Vlan-interface100] ripng 1 enable
```

```
[SwitchA-Vlan-interface100] quit
```

```
[SwitchA] interface tunnel 0
```

```
[SwitchA-Tunnel0] ripng 1 enable
```

```
[SwitchA-Tunnel0] quit
```

(4) 配置 Switch C

# 使能 IPv6 转发功能。

```
<SwitchB> system-view
```

```
[SwitchB] ipv6
```

# 配置 RIPng 的基本功能

```
[SwitchA] ripng 1
```

```
[SwitchA-ripng-1] quit
```

```
[SwitchA] interface vlan-interface 100
```

```
[SwitchA-Vlan-interface100] ripng 1 enable
```

```
[SwitchA-Vlan-interface100] quit
```

#### (5) 配置 Switch D

# 使能 IPv6 转发功能。

```
<SwitchB> system-view
```

```
[SwitchB] ipv6
```

# 配置 RIPng 的基本功能

```
[SwitchA] ripng 1
```

```
[SwitchA-ripng-1] quit
```

```
[SwitchA] interface vlan-interface 100
```

```
[SwitchA-Vlan-interface100] ripng 1 enable
```

```
[SwitchA-Vlan-interface100] quit
```

在 Switch C 上用命令 **display ipv6 routing-table**，可以看到 Switch C 已知道网络 2002:3::/64 的存在。

在 Switch D 上用命令 **display ipv6 routing-table**，可以看到 Switch D 也知道网络 2002:1::/64 的存在。

### 1.4.5 完整配置

- 配置 Switch A

```
#
```

```
ipv6
```

```
#
```

```
vlan 100 to 101
```

```
#
```

```
interface Vlan-interface100
```

```
ipv6 address 2002:1::1/64
```

```
ripng 1 enable
```

```
#
```

```
interface Vlan-interface101
```

```
ip address 172.13.1.1 255.255.255.0
```

```
#
```

```
interface Tunnel0
```

```
ipv6 address 3001::1:1/64
```

```
ripng 1 enable
```

```
tunnel-protocol ipv6-ipv4
```

```
source Vlan-interface101
```

```
destination 10.1.1.2
```

```
#
```

```

ripng 1
#
• 配置 Switch B
#
ipv6
#
vlan 100
#
vlan 101
#
interface Vlan-interface100
ipv6 address 2002:3::1/64
ripng 1 enable
#
interface Vlan-interface101
ip address 10.1.1.2 255.255.255.0
#
interface Tunnel0
ipv6 address 3001::1:2/64
ripng 1 enable
tunnel-protocol ipv6-ipv4
source Vlan-interface101
destination 172.13.1.1
#
ripng 1
#
• 配置 Switch C
#
ipv6
#
vlan 100
#
interface Vlan-interface100
ipv6 address 2002:1::2/64
ripng 1 enable
#
ripng 1
#
• 配置 Switch D
#
ipv6
#
vlan 100
#
interface Vlan-interface100
ipv6 address 2002:3::2/64
ripng 1 enable

```

```

ripng 1
#
```

#### 1.4.6 配置注意事项

- 如果隧道两端 Tunnel 接口的地址不在同一个网段,则必须配置通过隧道到达对端的转发路由,以便需要进行封装的报文能正常转发。用户可以配置静态路由,也可以配置动态路由。
- 配置动态路由时,需要在隧道两端的 Tunnel 接口使能动态路由协议。在隧道的两端都要进行此项配置。
- 分布式交换机(例如 S7500E 系列)的 Tunnel 接口号的形式为 A/B/C, A、B、C 分别代表单板槽位号、子卡槽位号、Tunnel 接口号。
- 当在分布式交换机(例如 S7500E 系列)上创建 Tunnel 接口时,建议 Tunnel 接口的槽号与所设置的源端口所在槽位保持一致,即使用发出报文的实际端口的槽位号,这样可以提高转发效率。

### 1.5 配置 OSPFv3 区域典型配置指导

OSPFv3 是 OSPF (Open Shortest Path First, 开放式最短路径优先) 版本 3 的简称, 主要提供对 IPv6 的支持, 遵循的标准为 RFC 2740 (OSPF for IPv6)。

OSPFv3 和 OSPFv2 在很多方面是相同的:

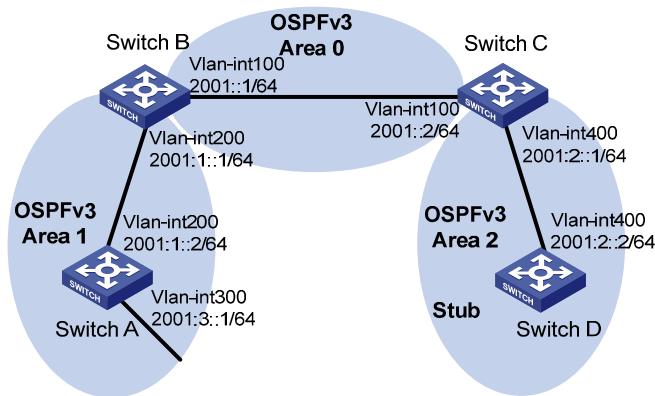
- Router ID, Area ID 仍然是 32 位的。
- 相同类型的报文: Hello 报文, DD (Database Description, 数据库描述) 报文, LSR (Link State Request, 链路状态请求) 报文, LSU (Link State Update, 链路状态更新) 报文和 LSAck (Link State Acknowledgment, 链路状态确认) 报文。
- 相同的邻居发现机制和邻接形成机制。
- 相同的 LSA 扩散机制和老化机制。

OSPFv3 和 OSPFv2 的不同主要有:

- OSPFv3 是基于链路 (Link) 运行, OSPFv2 是基于网段 (Network) 运行。
- OSPFv3 在同一条链路上可以运行多个实例。
- OSPFv3 是通过 Router ID 来标识邻接的邻居。OSPFv2 则是通过 IP 地址来标识邻接的邻居。

### 1.5.1 组网图

图1-5 配置 OSPFv3 区域组网图



### 1.5.2 应用要求

- 所有的交换机都运行 OSPFv3，整个自治系统划分为 3 个区域。其中 Switch B 和 Switch C 作为 ABR 来转发区域之间的路由。
- 要求将 Area2 配置为 Stub 区域，减少通告到此区域内的 LSA 数量，可进一步减少 Stub 区域路由表规模，将 Area 2 配置为 Totally Stub 区域，但不能影响路由的可达性。

### 1.5.3 适用产品、版本

表1-5 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本    |
|-------------------|---------------------------------|---------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本 |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本 |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本 |

### 1.5.4 配置过程和解释

- 配置各接口的 IPv6 地址（略）
- 配置 OSPFv3 基本功能

# 配置 Switch A，启动 OSPFv3，并设置其 Router ID 为 1.1.1.1。

```
<SwitchA> system-view
[SwitchA] ipv6
[SwitchA] ospfv3
[SwitchA-ospfv3-1] router-id 1.1.1.1
[SwitchA-ospfv3-1] quit
[SwitchA] interface vlan-interface 300
[SwitchA-Vlan-interface300] ospfv3 1 area 1
```

```
[SwitchA-Vlan-interface300] quit
[SwitchA] interface vlan-interface 200
[SwitchA-Vlan-interface200] ospfv3 1 area 1
[SwitchA-Vlan-interface200] quit
```

# 配置 Switch B，启动 OSPFv3，并设置其 Router ID 为 2.2.2.2。

```
<SwitchB> system-view
[SwitchB] ipv6
[SwitchB] ospfv3
[SwitchB-ospf-1] router-id 2.2.2.2
[SwitchB-ospf-1] quit
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ospfv3 1 area 0
[SwitchB-Vlan-interface100] quit
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] ospfv3 1 area 1
[SwitchB-Vlan-interface200] quit
```

# 配置 Switch C，启动 OSPFv3，并设置其 Router ID 为 3.3.3.3。

```
<SwitchC> system-view
[SwitchC] ipv6
[SwitchC] ospfv3
[SwitchC-ospfv3-1] router-id 3.3.3.3
[SwitchC-ospfv3-1] quit
[SwitchC] interface vlan-interface 100
[SwitchC-Vlan-interface100] ospfv3 1 area 0
[SwitchC-Vlan-interface100] quit
[SwitchC] interface vlan-interface 400
[SwitchC-Vlan-interface400] ospfv3 1 area 2
[SwitchC-Vlan-interface400] quit
```

# 配置 Switch D，启动 OSPFv3，并设置其 Router ID 为 4.4.4.4。

```
<SwitchD> system-view
[SwitchD] ipv6
[SwitchD] ospfv3
[SwitchD-ospfv3-1] router-id 4.4.4.4
[SwitchD-ospfv3-1] quit
[SwitchD] interface vlan-interface 400
[SwitchD-Vlan-interface400] ospfv3 1 area 2
[SwitchD-Vlan-interface400] quit
```

# 查看 Switch B 的 OSPFv3 邻居状态。

```
[SwitchB] display ospfv3 peer
```

```
OSPFv3 Area ID 0.0.0.0 (Process 1)
```

```

Neighbor ID Pri State Dead Time Interface Instance ID
3.3.3.3 1 Full/DR 00:00:39 Vlan100 0
```

```
OSPFv3 Area ID 0.0.0.1 (Process 1)
```

```

Neighbor ID Pri State Dead Time Interface Instance ID
1.1.1.1 1 Full/Backup 00:00:38 Vlan200 0
```

# 查看 Switch C 的 OSPFv3 邻居状态。

```
[SwitchC] display ospfv3 peer
```

```
OSPFv3 Area ID 0.0.0.0 (Process 1)
```

```

Neighbor ID Pri State Dead Time Interface Instance ID
2.2.2.2 1 Full/Backup 00:00:39 Vlan100 0
```

```
OSPFv3 Area ID 0.0.0.2 (Process 1)
```

```

Neighbor ID Pri State Dead Time Interface Instance ID
4.4.4.4 1 Full/DR 00:00:38 Vlan400 0
```

# 查看 Switch D 的 OSPFv3 路由表信息。

```
[SwitchD] display ospfv3 routing
```

```
E1 - Type 1 external route, IA - Inter area route, I - Intra area route
E2 - Type 2 external route, * - Selected route
```

```
OSPFv3 Router with ID (4.4.4.4) (Process 1)
```

```

*Destination: 2001::/64
```

```
 Type : IA Cost : 2
 NextHop : FE80::F40D:0:93D0:1 Interface: Vlan400
```

```
*Destination: 2001:1::/64
```

```
 Type : IA Cost : 3
 NextHop : FE80::F40D:0:93D0:1 Interface: Vlan400
```

```
*Destination: 2001:2::/64
```

```
 Type : I Cost : 1
 NextHop : directly-connected Interface: Vlan400
```

```
*Destination: 2001:3::/64
```

```
 Type : IA Cost : 4
 NextHop : FE80::F40D:0:93D0:1 Interface: Vlan400
```

(3) 配置 Stub 区域

# 配置 Switch D 的 Stub 区域。

```
[SwitchD] ospfv3
```



```
[SwitchD-ospfv3-1] area 2
```

```
[SwitchD-ospfv3-1-area-0.0.0.2] stub
```

# 配置 Switch C 的 Stub 区域，设置发送到 Stub 区域的缺省路由的开销为 10。

```
[SwitchC] ospfv3
```

```
[SwitchC-ospfv3-1] area 2
```

```
[SwitchC-ospfv3-1-area-0.0.0.2] stub
```

```
[SwitchC-ospfv3-1-area-0.0.0.2] default-cost 10
```

# 查看 Switch D 的 OSPFv3 路由表信息，可以看到路由表中多了一条缺省路由，它的开销值为直连路由的开销和所配置的开销值之和。

```
[SwitchD] display ospfv3 routing
```

```
E1 - Type 1 external route, IA - Inter area route, I - Intra area route
```

```
E2 - Type 2 external route, * - Seleted route
```

```
OSPFv3 Router with ID (4.4.4.4) (Process 1)
```

```

```

```
*Destination: ::/0
```

```
 Type : IA Cost : 11
```

```
 NextHop : FE80::F40D:0:93D0:1 Interface: Vlan400
```

```
*Destination: 2001::/64
```

```
 Type : IA Cost : 2
```

```
 NextHop : FE80::F40D:0:93D0:1 Interface: Vlan400
```

```
*Destination: 2001:1::/64
```

```
 Type : IA Cost : 3
```

```
 NextHop : FE80::F40D:0:93D0:1 Interface: Vlan400
```

```
*Destination: 2001:2::/64
```

```
 Type : I Cost : 1
```

```
 NextHop : directly-connected Interface: Vlan400
```

```
*Destination: 2001:3::/64
```

```
 Type : IA Cost : 4
```

```
 NextHop : FE80::F40D:0:93D0:1 Interface: Vlan400
```

(4) 进一步减少 Stub 区域路由表规模，将 Area 2 配置为 Totally Stub 区域。

# 配置 Switch C，设置 Area2 为 Totally Stub 区域。

```
[SwitchC-ospfv3-1-area-0.0.0.2] stub no-summary
```

# 查看 Switch D 的 OSPFv3 路由表，可以发现路由表项数目减少了，其他非直连路由都被抑制，只有缺省路由被保留。

```
[SwitchD] display ospfv3 routing
```

```
E1 - Type 1 external route, IA - Inter area route, I - Intra area route
```

```
E2 - Type 2 external route, * - Seleted route
```

```

*Destination: ::/0
Type : IA Cost : 11
NextHop : FE80::F40D:0:93D0:1 Interface: Vlan400

*Destination: 2001:2::/64
Type : I Cost : 1
NextHop : directly-connected Interface: Vlan400

```

### 1.5.5 完整配置

- 配置 Switch A

```

#
ipv6
#
vlan 200
#
vlan 300
#
interface Vlan-interface200
ipv6 address 2001:1::2/64
ospfv3 1 area 0.0.0.1
#
interface Vlan-interface300
ipv6 address 2001:3::1/64
ospfv3 1 area 0.0.0.1
#
ospfv3 1
router-id 1.1.1.1
#

```

- 配置 Switch B

```

#
ipv6
#
vlan 100
#
vlan 200
#
interface Vlan-interface100
ipv6 address 2001::1/64
ospfv3 1 area 0.0.0.0
#
interface Vlan-interface200
ipv6 address 2001:1::1/64
ospfv3 1 area 0.0.0.1
#

```

```

ospfv3 1
router-id 2.2.2.2
#
• 配置 Switch C
#
ipv6
#
vlan 100
#
vlan 400
#
interface Vlan-interface100
ipv6 address 2001::2/64
ospfv3 1 area 0.0.0.0
#
interface Vlan-interface400
ipv6 address 2001:2::1/64
ospfv3 1 area 0.0.0.2
#
ospfv3 1
router-id 3.3.3.3
area 0.0.0.2
stub no-summary
default-cost 10
#
• 配置 Switch D
#
ipv6
#
vlan 400
#
interface Vlan-interface400
ipv6 address 2001:2::2/64
ospfv3 1 area 0.0.0.2
#
ospfv3 1
router-id 4.4.4.4
area 0.0.0.2
stub
#

```

### 1.5.6 配置注意事项

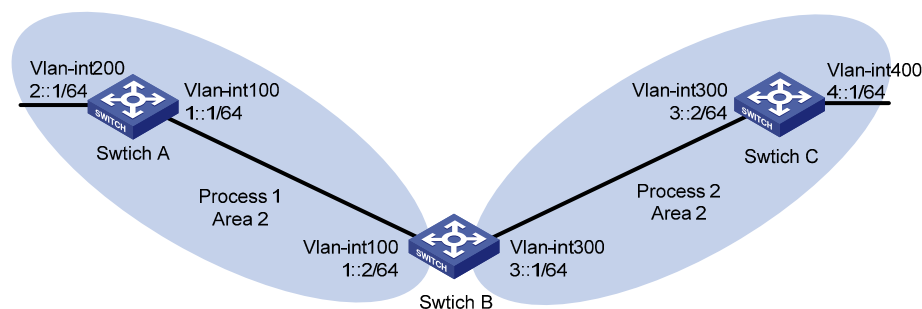
- OSPFv3 的区域不能直接删除，只有区域视图下的所有配置都删除后，且该区域中相关接口的状态都为 down，此区域才会自动删除。
- 对于位于 Stub 区域中的所有路由器都必须配置 stub 命令，参数 no-summary 只能在 ABR 上配置。

- 如果 ABR 使用了 **stub** 命令中的参数 **no-summary**，则此 ABR 只向区域内发布一条描述缺省路由的 Inter-Area-Prefix-LSA。这种既没有 AS-external-LSA，也没有 Inter-Area-Prefix-LSA、Inter-Area-Router-LSA 的 Stub 区域，又称为 Totally Stub 区域。
- 要在路由器上使能 OSPFv3 功能，必须先创建 OSPFv3 进程、指定该进程的 Router ID 以及在接口上使能 OSPFv3 功能。
- Router ID 用来在一个自治系统中唯一的标识一台路由器。在 OSPFv3 中，用户必须手工配置一个 Router ID，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。因此，为了保证 OSPFv3 运行的稳定性，在进行网络规划时，应确定路由器 ID 的划分并手工配置。需要注意的是，如果在同一台路由器上运行了多个 OSPFv3 进程，必须为不同的进程指定不同的 Router ID。

## 1.6 OSPFv3 引入外部路由典型配置指导

### 1.6.1 组网图

图1-6 配置 OSPFv3 引入外部路由组网图



### 1.6.2 应用要求

- Switch A、Switch B 和 Switch C 位于 Area 2 内；
- Switch B 上运行两个 OSPFv3 进程：OSPFv3 1 和 OSPFv3 2。Switch B 通过 OSPFv3 1 和 Switch A 交换路由信息，通过 OSPFv3 2 和 Switch C 交换路由信息；
- 在 Switch B 上配置 OSPFv3 进程 2 引入外部路由，引入直连路由和 OSPFv3 进程 1 的路由，并将引入的外部路由的缺省度量值设置为 3，使得 Switch C 能够学习到达 1::0/64 和 2::0/64 的路由，但 Switch A 不能学习到达 3::0/64 和 4::0/64 的路由。

### 1.6.3 适用产品、版本

表1-6 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本    |
|-------------------|---------------------------------|---------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本 |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本 |

### 1.6.4 配置过程和解释

(1) 配置各接口的 IPv6 地址（略）

# 在 Switch A 上启动 OSPFv3 进程 1。

```
<SwitchA> system-view
[SwitchA] ipv6
[SwitchA] ospfv3 1
[SwitchA-ospfv3-1] router-id 1.1.1.1
[SwitchA-ospfv3-1] quit
[SwitchA] interface Vlan-interface 100
[SwitchA-Vlan-interface100] ospfv3 1 area 2
[SwitchA-Vlan-interface100] quit
[SwitchA] interface Vlan-interface 200
[SwitchA-Vlan-interface200] ospfv3 1 area 2
[SwitchA-Vlan-interface200] quit
```

# 在 Switch B 上启动两个 OSPFv3 进程，进程号分别为 1 和 2。

```
<SwitchB> system-view
[SwitchB] ipv6
[SwitchB] ospfv3 1
[SwitchB-ospfv3-1] router-id 2.2.2.2
[SwitchB-ospfv3-1] quit
[SwitchB] interface Vlan-interface 100
[SwitchB-Vlan-interface100] ospfv3 1 area 2
[SwitchB-Vlan-interface100] quit
[SwitchB] ospfv3 2
[SwitchB-ospfv3-2] router-id 3.3.3.3
[SwitchB-ospfv3-2] quit
[SwitchB] interface Vlan-interface 300
[SwitchB-Vlan-interface300] ospfv3 2 area 2
[SwitchB-Vlan-interface300] quit
```

# 在 Switch C 上启动 OSPFv3 进程 2。

```
<SwitchC> system-view
[SwitchC] ipv6
[SwitchC] ospfv3 2
```

```
[SwitchC-ospfv3-2] router-id 4.4.4.4
[SwitchC-ospfv3-2] quit
[SwitchC] interface Vlan-interface 300
[SwitchC-Vlan-interface300] ospfv3 2 area 2
[SwitchC-Vlan-interface300] quit
[SwitchC] interface Vlan-interface 400
[SwitchC-Vlan-interface400] ospfv3 2 area 2
[SwitchC-Vlan-interface400] quit
```

# 查看 Switch C 的路由表信息。

```
[SwitchB] display ipv6 routing-table
```

Routing Table :

| Destinations : 6 | Routes : 6 |
|------------------|------------|
|------------------|------------|

|                      |                   |
|----------------------|-------------------|
| Destination: ::1/128 | Protocol : Direct |
| NextHop : ::1        | Preference: 0     |
| Interface : InLoop0  | Cost : 0          |

|                     |                   |
|---------------------|-------------------|
| Destination: 3::/64 | Protocol : Direct |
| NextHop : 3::2      | Preference: 0     |
| Interface : Vlan300 | Cost : 0          |

|                       |                   |
|-----------------------|-------------------|
| Destination: 3::2/128 | Protocol : Direct |
| NextHop : ::1         | Preference: 0     |
| Interface : InLoop0   | Cost : 0          |

|                     |                   |
|---------------------|-------------------|
| Destination: 4::/64 | Protocol : Direct |
| NextHop : 4::1      | Preference: 0     |
| Interface : Vlan400 | Cost : 0          |

|                       |                   |
|-----------------------|-------------------|
| Destination: 4::1/128 | Protocol : Direct |
| NextHop : ::1         | Preference: 0     |
| Interface : InLoop0   | Cost : 0          |

|                        |                   |
|------------------------|-------------------|
| Destination: FE80::/10 | Protocol : Direct |
| NextHop : ::           | Preference: 0     |
| Interface : NULL0      | Cost : 0          |

## (2) 配置 OSPFv3 引入外部路由

# 在 Switch B 上配置 OSPFv3 引入外部路由, 引入直连路由和 OSPFv3 1 的路由。

```
[SwitchB] ospfv3 2
[SwitchB-ospfv3-2] default cost 3
[SwitchB-ospfv3-2] import-route ospfv3 1
[SwitchB-ospfv3-2] import-route direct
[SwitchB-ospfv3-2] quit
```

# 查看路由引入后 Switch C 的路由表信息。

```
[SwitchC] display ipv6 routing-table
```

Routing Table :

Destinations : 8      Routes : 8

|                      |                   |
|----------------------|-------------------|
| Destination: ::1/128 | Protocol : Direct |
| NextHop : ::1        | Preference: 0     |
| Interface : InLoop0  | Cost : 0          |

|                                   |                   |
|-----------------------------------|-------------------|
| Destination: 1::/64               | Protocol : OSPFv3 |
| NextHop : FE80::200:CFF:FE01:1C03 | Preference: 150   |
| Interface : Vlan300               | Cost : 3          |

|                                   |                   |
|-----------------------------------|-------------------|
| Destination: 2::/64               | Protocol : OSPFv3 |
| NextHop : FE80::200:CFF:FE01:1C03 | Preference: 150   |
| Interface : Vlan300               | Cost : 3          |

|                     |                   |
|---------------------|-------------------|
| Destination: 3::/64 | Protocol : Direct |
| NextHop : 3::2      | Preference: 0     |
| Interface : Vlan300 | Cost : 0          |

|                       |                   |
|-----------------------|-------------------|
| Destination: 3::2/128 | Protocol : Direct |
| NextHop : ::1         | Preference: 0     |
| Interface : InLoop0   | Cost : 0          |

|                     |                   |
|---------------------|-------------------|
| Destination: 4::/64 | Protocol : Direct |
| NextHop : 4::1      | Preference: 0     |
| Interface : Vlan400 | Cost : 0          |

|                       |                   |
|-----------------------|-------------------|
| Destination: 4::1/128 | Protocol : Direct |
| NextHop : ::1         | Preference: 0     |
| Interface : InLoop0   | Cost : 0          |

|                        |                   |
|------------------------|-------------------|
| Destination: FE80::/10 | Protocol : Direct |
| NextHop : ::           | Preference: 0     |
| Interface : NULL0      | Cost : 0          |

### 1.6.5 完整配置

- 配置 Switch A

```
#
ipv6
#
vlan 100
#
vlan 200
#
interface Vlan-interface100
ipv6 address 1::1/64
ospfv3 1 area 0.0.0.2
#
interface Vlan-interface200
```

```

ipv6 address 2::1/64
ospfv3 1 area 0.0.0.2
#
ospfv3 1
router-id 1.1.1.1
#

```

- 配置 Switch B

```

#
ipv6
#
vlan 100
#
vlan 300
#
interface Vlan-interface100
ipv6 address 1::2/64
ospfv3 1 area 0.0.0.2
#
interface Vlan-interface300
ipv6 address 3::1/64
ospfv3 2 area 0.0.0.2
#
ospfv3 1
router-id 2.2.2.2
#
ospfv3 2
router-id 3.3.3.3
default cost 3
import-route direct
import-route ospfv3 1
#

```

- 配置 Switch C

```

#
ipv6
#
vlan 300
#
vlan 400
#
interface Vlan-interface300
ipv6 address 3::2/64
ospfv3 2 area 0.0.0.2
#
interface Vlan-interface400
ipv6 address 4::1/64
ospfv3 2 area 0.0.0.2
#
ospfv3 2

```



```
router-id 4.4.4.4
#
```

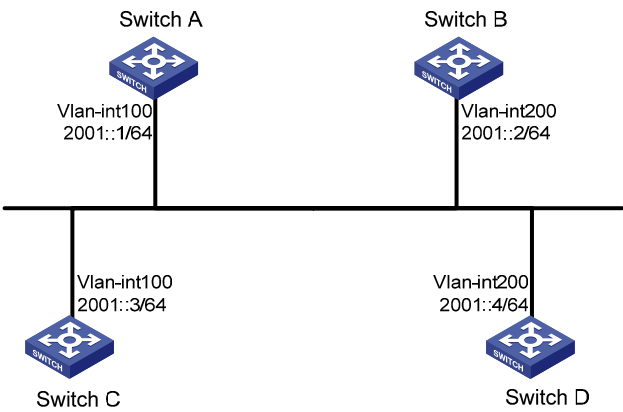
### 1.6.6 配置注意事项

- 要在路由器上使能 OSPFv3 功能，必须先创建 OSPFv3 进程、指定该进程的 Router ID 以及在接口上使能 OSPFv3 功能。
- Router ID 用来在一个自治系统中唯一的标识一台路由器。在 OSPFv3 中，用户必须手工配置一个 Router ID，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。因此，为了保证 OSPFv3 运行的稳定性，在进行网络规划时，应确定路由器 ID 的划分并手工配置。需要注意的是，如果在同一台路由器上运行了多个 OSPFv3 进程，必须为不同的进程指定不同的 Router ID。
- S5500-EI 系列交换机的 release2102 软件版本仅支持 OSPFv3 单进程。

## 1.7 OSPFv3 的 DR 选择典型配置指导

### 1.7.1 组网图

图1-7 配置 OSPFv3 的 DR 选择组网图



### 1.7.2 应用要求

- Switch A 的优先级为 100，它是网络上的最高优先级，所以 Switch A 被选为 DR；
- Switch C 的优先级为 2，它是优先级次高的，被选为 BDR；
- Switch B 的优先级为 0，这意味着它将无法成为 DR；
- Switch D 没有配置优先级，取缺省值 1。

### 1.7.3 适用产品、版本

表1-7 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本    |
|-------------------|---------------------------------|---------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本 |

| 产品                | 软件版本                            | 硬件版本    |
|-------------------|---------------------------------|---------|
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本 |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本 |

#### 1.7.4 配置过程和解释

(1) 配置各接口的 IPv6 地址（略）

(2) 配置 OSPFv3 基本功能

# 配置 Switch A，启动 OSPFv3，并设置其 Router ID 为 1.1.1.1。

```
<SwitchA> system-view
[SwitchA] ipv6
[SwitchA] ospfv3
[SwitchA-ospfv3-1] router-id 1.1.1.1
[SwitchA-ospfv3-1] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ospfv3 1 area 0
[SwitchA-Vlan-interface100] quit
```

# 配置 Switch B，启动 OSPFv3，并设置其 Router ID 为 2.2.2.2。

```
<SwitchB> system-view
[SwitchB] ipv6
[SwitchB] ospfv3
[SwitchB-ospfv3-1] router-id 2.2.2.2
[SwitchB-ospfv3-1] quit
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] ospfv3 1 area 0
[SwitchB-Vlan-interface200] quit
```

# 配置 Switch C，启动 OSPFv3，并设置其 Router ID 为 3.3.3.3。

```
<SwitchC> system-view
[SwitchC] ipv6
[SwitchC] ospfv3
[SwitchC-ospfv3-1] router-id 3.3.3.3
[SwitchC-ospfv3-1] quit
[SwitchC] interface vlan-interface 100
[SwitchC-Vlan-interface100] ospfv3 1 area 0
[SwitchC-Vlan-interface100] quit
```

# 配置 Switch D，启动 OSPFv3，并设置其 Router ID 为 4.4.4.4。

```
<SwitchD> system-view
[SwitchD] ipv6
[SwitchD] ospfv3
[SwitchD-ospfv3-1] router-id 4.4.4.4
[SwitchD-ospfv3-1] quit
[SwitchD] interface vlan-interface 200
[SwitchD-Vlan-interface200] ospfv3 1 area 0
```

```
[SwitchD-Vlan-interface200] quit
```

# 查看 Switch A 的邻居信息，可以看到 DR 优先级（缺省为 1）以及邻居状态，此时优先级相等，Router ID 大者被选为 DR，可以看到 Switch D 为 DR，Switch C 为 BDR。

```
[SwitchA] display ospfv3 peer
```

```
OSPFv3 Area ID 0.0.0.0 (Process 1)

Neighbor ID Pri State Dead Time Interface Instance ID
2.2.2.2 1 2-Way/DROther 00:00:36 Vlan200 0
3.3.3.3 1 Full/Backup 00:00:35 Vlan100 0
4.4.4.4 1 Full/DR 00:00:33 Vlan200 0
```

# 查看 Switch D 的邻居信息，可以看到 Switch D 和其他邻居之间的邻居状态都为 Full。

```
[SwitchD] display ospfv3 peer
```

```
OSPFv3 Area ID 0.0.0.0 (Process 1)

Neighbor ID Pri State Dead Time Interface Instance ID
1.1.1.1 1 Full/DROther 00:00:30 Vlan100 0
2.2.2.2 1 Full/DROther 00:00:37 Vlan200 0
3.3.3.3 1 Full/Backup 00:00:31 Vlan100 0
```

### (3) 配置接口的 DR 优先级

# 配置 Switch A 的接口 Vlan-interface100 的 DR 优先级为 100。

```
[SwitchA] interface vlan-interface 100
```

```
[SwitchA-Vlan-interface100] ospfv3 dr-priority 100
```

```
[SwitchA-Vlan-interface100] quit
```

# 配置 Switch B 的接口 Vlan-interface200 的 DR 优先级为 0。

```
[SwitchB] interface vlan-interface 200
```

```
[SwitchB-Vlan-interface200] ospfv3 dr-priority 0
```

```
[SwitchB-Vlan-interface200] quit
```

# 配置 Switch C 的接口 Vlan-interface100 的 DR 优先级为 2。

```
[SwitchC] interface vlan-interface 100
```

```
[SwitchC-Vlan-interface100] ospfv3 dr-priority 2
```

```
[SwitchC-Vlan-interface100] quit
```

# 显示 Switch A 的邻居信息，可以看到 DR 优先级已经更新，但 DR/BDR 并未改变。

```
[SwitchA] display ospfv3 peer
```

```
OSPFv3 Area ID 0.0.0.0 (Process 1)

Neighbor ID Pri State Dead Time Interface Instance ID
2.2.2.2 0 2-Way/DROther 00:00:38 Vlan200 0
3.3.3.3 2 Full/Backup 00:00:32 Vlan100 0
4.4.4.4 1 Full/DR 00:00:36 Vlan200 0
```

# 显示 Switch D 的邻居信息，可以看到 Switch D 仍然为 DR。

```
[SwitchD] display ospfv3 peer
```

```
OSPFv3 Area ID 0.0.0.0 (Process 1)
```

| Neighbor ID | Pri | State        | Dead Time | Interface | Instance ID |
|-------------|-----|--------------|-----------|-----------|-------------|
| 1.1.1.1     | 100 | Full/DROther | 00:00:33  | Vlan100   | 0           |
| 2.2.2.2     | 0   | Full/DROther | 00:00:36  | Vlan200   | 0           |
| 3.3.3.3     | 2   | Full/Backup  | 00:00:40  | Vlan100   | 0           |

#### (4) 重新进行 DR/BDR 选择

# 将所有接口一次 **shutdown** 和 **undo shutdown**，使 OSPFv3 进行 DR/BDR 的重新选举。

# 查看 Switch A 的邻居信息，可以看到 Switch C 为 BDR。

```
[SwitchA] display ospfv3 peer
```

```
OSPFv3 Area ID 0.0.0.0 (Process 1)
```

| Neighbor ID | Pri | State        | Dead Time | Interface | Instance ID |
|-------------|-----|--------------|-----------|-----------|-------------|
| 2.2.2.2     | 0   | Full/DROther | 00:00:31  | Vlan200   | 0           |
| 3.3.3.3     | 2   | Full/Backup  | 00:00:39  | Vlan100   | 0           |
| 4.4.4.4     | 1   | Full/DROther | 00:00:37  | Vlan200   | 0           |

# 查看 Switch D 的邻居信息，可以看到 Switch A 为 DR。

```
[SwitchD] display ospfv3 peer
```

```
OSPFv3 Area ID 0.0.0.0 (Process 1)
```

| Neighbor ID | Pri | State         | Dead Time | Interface | Instance ID |
|-------------|-----|---------------|-----------|-----------|-------------|
| 1.1.1.1     | 100 | Full/DR       | 00:00:34  | Vlan100   | 0           |
| 2.2.2.2     | 0   | 2-Way/DROther | 00:00:34  | Vlan200   | 0           |
| 3.3.3.3     | 2   | Full/Backup   | 00:00:32  | Vlan100   | 0           |

## 1.7.5 完整配置

- 配置 Switch A

```
#
ipv6
#
vlan 100
#
interface Vlan-interface100
ipv6 address 2001::1/64
ospfv3 1 area 0.0.0.0
ospfv3 dr-priority 100
#
ospfv3 1
router-id 1.1.1.1
#
```

- 配置 Switch B

```
#
ipv6
```

```

#
vlan 200
#
interface Vlan-interface200
 ipv6 address 2001::2/64
 ospfv3 1 area 0.0.0.0
 ospfv3 dr-priority 0
#
ospfv3 1
 router-id 2.2.2.2
#
• 配置 Switch C
#
ipv6
#
vlan 100
#
#
interface Vlan-interface100
 ipv6 address 2001::3/64
 ospfv3 1 area 0.0.0.0
 ospfv3 dr-priority 2
#
ospfv3 1
 router-id 3.3.3.3
#
• 配置 Switch D
#
ipv6
#
vlan 200
#
interface Vlan-interface200
 ipv6 address 2001::4/64
 ospfv3 1 area 0.0.0.0
#
ospfv3 1
 router-id 4.4.4.4
#

```

### 1.7.6 配置注意事项

- 要在路由器上使能 OSPFv3 功能，必须先创建 OSPFv3 进程、指定该进程的 Router ID 以及在接口上使能 OSPFv3 功能。
- Router ID 用来在一个自治系统中唯一的标识一台路由器。在 OSPFv3 中，用户必须手工配置一个 Router ID，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。因此，为了保证 OSPFv3 运行的稳定性，在进行网络规划时，应确定路由器 ID 的划分并手工配置。需

要注意的是，如果在同一台路由器上运行了多个 OSPFv3 进程，必须为不同的进程指定不同的 Router ID。

## 1.8 IPv6 IS-IS 路由协议典型配置指导

IS-IS（Intermediate System-to-Intermediate System intra-domain routing information exchange protocol，IS-IS 路由协议）支持多种网络层协议，其中包括 IPv6 协议，支持 IPv6 协议的 IS-IS 路由协议又称为 IPv6 IS-IS 动态路由协议。IETF 的 draft-ietf-isis-ipv6-05 中规定了 IS-IS 为支持 IPv6 所新增的内容，主要是新添加的支持 IPv6 协议的两个 TLVs（Type-Length-Values）和一个新的 NLPID（Network Layer Protocol Identifier，网络层协议标识符）。

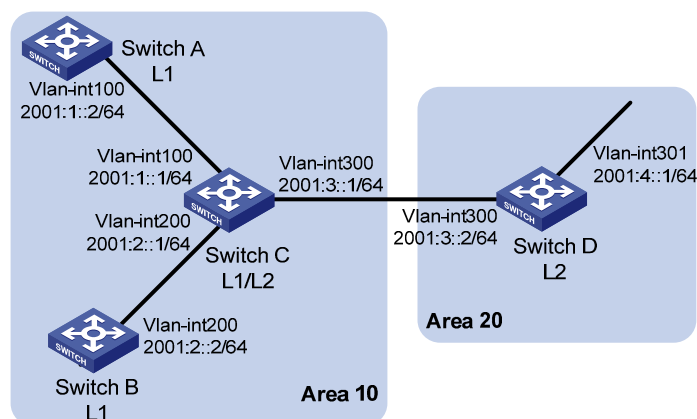
TLV 是 LSP（Link State PDU 或 Link State Packet）中的一个可变长字段值。新增的两个 TLV 分别是：

- IPv6 Reachability: 类型值为 236（0xEC），通过定义路由信息前缀、度量值等信息来说明网络的可达性。
- IPv6 Interface Address: 类型值为 232（0xE8），它对应于 IPv4 中的“IP Interface Address”TLV，只不过把原来的 32 比特的 IPv4 地址改为 128 比特的 IPv6 地址。

NLPID 是标识网络层协议报文的一个 8 比特字段，IPv6 的 NLPID 值为 142（0x8E）。如果 IS-IS 路由器支持 IPv6，那么它必须以这个 NLPID 值向外发布路由信息。

### 1.8.1 组网图

图1-8 IPv6 IS-IS 典型配置组网图



### 1.8.2 应用要求

Switch A、Switch B、Switch C 和 Switch D 属于同一自治系统，所有交换机已使能了 IPv6 能力，要求他们之间通过 IPv6 IS-IS 协议达到 IPv6 网络互连的目的。

其中 Switch A 和 Switch B 是 Level-1 交换机，Switch D 是 Level-2 交换机，Switch C 是 Level-1-2 交换机。Switch A、Switch B 和 Switch C 属于区域 10，而 Switch D 属于区域 20。

### 1.8.3 适用的产品、版本

表1-8 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本    |
|-------------------|---------------------------------|---------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本 |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本 |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本 |

### 1.8.4 配置过程和解释

(1) 配置各接口的 IPv6 地址（略）

(2) 配置 IPv6 IS-IS

# 配置 Switch A。

```
<SwitchA> system-view
[SwitchA] isis 1
[SwitchA-isis-1] is-level level-1
[SwitchA-isis-1] network-entity 10.0000.0000.0001.00
[SwitchA-isis-1] ipv6 enable
[SwitchA-isis-1] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] isis ipv6 enable 1
[SwitchA-Vlan-interface100] quit
```

# 配置 Switch B。

```
<SwitchB> system-view
[SwitchB] isis 1
[SwitchB-isis-1] is-level level-1
[SwitchB-isis-1] network-entity 10.0000.0000.0002.00
[SwitchB-isis-1] ipv6 enable
[SwitchB-isis-1] quit
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] isis ipv6 enable 1
[SwitchB-Vlan-interface200] quit
```

# 配置 Switch C。

```
<SwitchC> system-view
[SwitchC] isis 1
[SwitchC-isis-1] network-entity 10.0000.0000.0003.00
[SwitchC-isis-1] ipv6 enable
[SwitchC-isis-1] quit
[SwitchC] interface vlan-interface 100
[SwitchC-Vlan-interface100] isis ipv6 enable 1
```

```

[SwitchC-Vlan-interface100] quit
[SwitchC] interface vlan-interface 200
[SwitchC-Vlan-interface200] isis ipv6 enable 1
[SwitchC-Vlan-interface200] quit
[SwitchC] interface vlan-interface 300
[SwitchC-Vlan-interface300] isis ipv6 enable 1
[SwitchC-Vlan-interface300] quit
配置 Switch D。
<SwitchD> system-view
[SwitchD] isis 1
[SwitchD-isis-1] is-level level-2
[SwitchD-isis-1] network-entity 20.0000.0000.0004.00
[SwitchD-isis-1] ipv6 enable
[SwitchD-isis-1] quit
[SwitchD] interface vlan-interface 300
[SwitchD-Vlan-interface300] isis ipv6 enable 1
[SwitchD-Vlan-interface300] quit
[SwitchD] interface vlan-interface 301
[SwitchD-Vlan-interface301] isis ipv6 enable 1
[SwitchD-Vlan-interface301] quit

```

### 1.8.5 完整配置

- 配置 Switch A。

```

#
ipv6
#
vlan 100
#
isis 1
is-level level-1
network-entity 10.0000.0000.0001.00
#
ipv6 enable
#
#
interface Vlan-interface100
ipv6 address 2001:1::2/64
isis ipv6 enable 1
#

```

- 配置 Switch B。

```

#
ipv6
#
vlan 200
#
isis 1
is-level level-1

```



```

network-entity 10.0000.0000.0002.00
#
ipv6 enable
#
interface Vlan-interface200
ipv6 address 2001:2::2/64
isis ipv6 enable 1
#

```

- 配置 Switch C。

```

#
ipv6
#
vlan 100
#
vlan 200
#
vlan 300
#
isis 1
network-entity 10.0000.0000.0003.00
#
ipv6 enable
#
interface Vlan-interface100
ipv6 address 2001:1::1/64
isis ipv6 enable 1
#
interface Vlan-interface200
ipv6 address 2001:2::1/64
isis ipv6 enable 1
#
interface Vlan-interface300
ipv6 address 2001:3::1/64
isis ipv6 enable 1
#

```

- 配置 Switch D。

```

#
ipv6
#
vlan 300 to 301
#
isis 1
is-level level-2
network-entity 20.0000.0000.0004.00
#
ipv6 enable
#
interface Vlan-interface300

```

```

ipv6 address 2001:3::2/64
isis ipv6 enable 1
#
interface Vlan-interface301
ipv6 address 2001:4::1/64
isis ipv6 enable 1
#

```

### 1.8.6 配置注意事项

无

## 1.9 IPv6 BGP 路由协议基本配置指导

传统的 BGP-4 只能管理 IPv4 的路由信息，对于使用其它网络层协议（如 IPv6 等）的应用，在跨自治系统传播时就受到一定限制。

为了提供对多种网络层协议的支持，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）。

为了实现对 IPv6 协议的支持，IPv6 BGP 需要将 IPv6 网络层协议的信息反映到 NLRI（Network Layer Reachable 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：

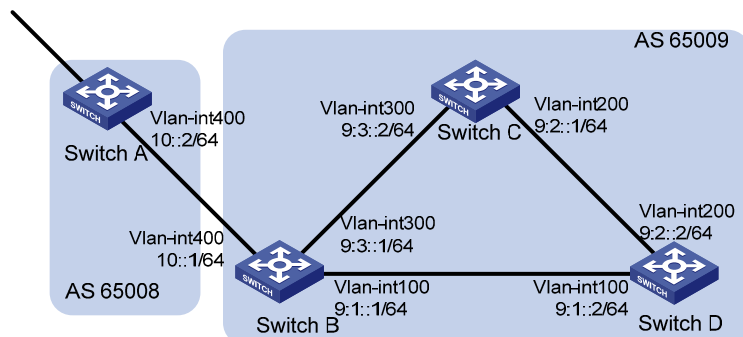
- MP\_REACH\_NLRI: Multiprotocol Reachable NLRI，多协议可达 NLRI。用于发布可达路由及下一跳信息。
- MP\_UNREACH\_NLRI: Multiprotocol Unreachable NLRI，多协议不可达 NLRI。用于撤销不可达路由。

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。

### 1.9.1 组网图

图1-9 IPv6 BGP 基本配置组网图



### 1.9.2 应用要求

如上图所示，所有交换机运行 IPv6 BGP 协议，Switch A 和 Switch B 之间建立 EBGP 连接，Switch B、Switch C 和 Switch D 之间建立 IBGP 全连接。

### 1.9.3 适用产品、版本

表1-9 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本    |
|-------------------|---------------------------------|---------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本 |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本 |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本 |

### 1.9.4 配置过程和解释

(1) 配置各 VLAN 接口的 IPv6 地址（略）

(2) 配置 IBGP 连接

# 配置 Switch B。

```
<SwitchB> system-view
[SwitchB] ipv6
[SwitchB] bgp 65009
[SwitchB-bgp] router-id 2.2.2.2
[SwitchB-bgp] ipv6-family
[SwitchB-bgp-af-ipv6] peer 9:1::2 as-number 65009
[SwitchB-bgp-af-ipv6] peer 9:3::2 as-number 65009
[SwitchB-bgp-af-ipv6] quit
[SwitchB-bgp] quit
```

# 配置 Switch C。

```
<SwitchC> system-view
[SwitchC] ipv6
[SwitchC] bgp 65009
[SwitchC-bgp] router-id 3.3.3.3
[SwitchC-bgp] ipv6-family
[SwitchC-bgp-af-ipv6] peer 9:3::1 as-number 65009
[SwitchC-bgp-af-ipv6] peer 9:2::2 as-number 65009
[SwitchC-bgp-af-ipv6] quit
[SwitchC-bgp] quit
```

# 配置 Switch D。

```
<SwitchD> system-view
[SwitchD] ipv6
[SwitchD] bgp 65009
[SwitchD-bgp] router-id 4.4.4.4
[SwitchD-bgp] ipv6-family
[SwitchD-bgp-af-ipv6] peer 9:1::1 as-number 65009
[SwitchD-bgp-af-ipv6] peer 9:2::1 as-number 65009
```

```
[SwitchD-bgp-af-ipv6] quit
```

```
[SwitchD-bgp] quit
```

### (3) 配置 EBGP 连接

# 配置 Switch A。

```
<SwitchA> system-view
```

```
[SwitchA] ipv6
```

```
[SwitchA] bgp 65008
```

```
[SwitchA-bgp] router-id 1.1.1.1
```

```
[SwitchA-bgp] ipv6-family
```

```
[SwitchA-bgp-af-ipv6] peer 10::1 as-number 65009
```

```
[SwitchA-bgp-af-ipv6] quit
```

```
[SwitchA-bgp] quit
```

# 配置 Switch B。

```
[SwitchB] bgp 65009
```

```
[SwitchB-bgp] ipv6-family
```

```
[SwitchB-bgp-af-ipv6] peer 10::2 as-number 65008
```

# 查看 Switch B 的对等体信息。

```
[SwitchB] display bgp ipv6 peer
```

```
BGP local router ID : 2.2.2.2
```

```
Local AS number : 65009
```

```
Total number of peers : 3 Peers in established state : 3
```

| Peer   | V | AS    | MsgRcvd | MsgSent | OutQ | PrefRcv | Up/Down  | State       |
|--------|---|-------|---------|---------|------|---------|----------|-------------|
| 10::2  | 4 | 65008 | 3       | 3       | 0    | 0       | 00:01:16 | Established |
| 9:3::2 | 4 | 65009 | 2       | 3       | 0    | 0       | 00:00:40 | Established |
| 9:1::2 | 4 | 65009 | 2       | 4       | 0    | 0       | 00:00:19 | Established |

# 查看 Switch C 的对等体信息。

```
[SwitchC] display bgp ipv6 peer
```

```
BGP local router ID : 3.3.3.3
```

```
Local AS number : 65009
```

```
Total number of peers : 2 Peers in established state : 2
```

| Peer   | V | AS    | MsgRcvd | MsgSent | OutQ | PrefRcv | Up/Down  | State       |
|--------|---|-------|---------|---------|------|---------|----------|-------------|
| 9:3::1 | 4 | 65009 | 4       | 4       | 0    | 0       | 00:02:18 | Established |
| 9:2::2 | 4 | 65009 | 4       | 5       | 0    | 0       | 00:01:52 | Established |

可以看出，Switch A 和 Switch B 之间建立的 EBGP 连接，Switch B、Switch C 和 Switch D 之间建立了 IBGP 连接。

## 1.9.5 完整配置

- 配置 Switch A

```
#
```

```

ipv6
#
vlan 400
#
interface Vlan-interface400
 ipv6 address 10::2/64
#
bgp 65008
 router-id 1.1.1.1
#
 ipv6-family
 peer 10::1 as-number 65009
#

```

- 配置 Switch B

```

#
ipv6
#
vlan 100
#
vlan 300
#
vlan 400
#
interface Vlan-interface100
 ipv6 address 9:1::1/64
#
interface Vlan-interface300
 ipv6 address 9:3::1/64
#
interface Vlan-interface400
 ipv6 address 10::1/64
#
bgp 65009
 router-id 2.2.2.2
#
 ipv6-family
 peer 10::2 as-number 65008
 peer 9:1::2 as-number 65009
 peer 9:3::2 as-number 65009
#

```

- 配置 Switch C

```

#
ipv6
#
vlan 200
#
vlan 300
#

```

```

interface Vlan-interface200
 ipv6 address 9:2::1/64
#
interface Vlan-interface300
 ipv6 address 9:3::2/64
#
bgp 65009
 router-id 3.3.3.3
#
 ipv6-family
 peer 9:3::1 as-number 65009
 peer 9:2::2 as-number 65009
#

```

#### • 配置 Switch D

```

#
ipv6
#
vlan 100
#
vlan 200
#
interface Vlan-interface100
 ipv6 address 9:1::2/64
#
interface Vlan-interface200
 ipv6 address 9:2::2/64
#
bgp 65009
 router-id 4.4.4.4
#
 ipv6-family
 peer 9:1::1 as-number 65009
 peer 9:2::1 as-number 65009
#

```

### 1.9.6 配置注意事项

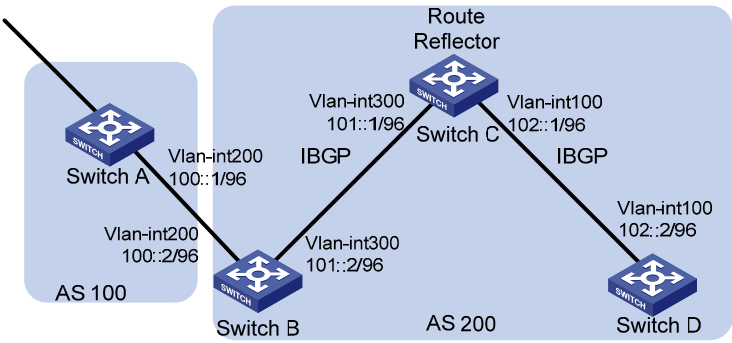
- 为了提高 IPv6 BGP 连接的可靠性和稳定性，可将 IPv6 BGP 连接所使用的本地接口配置成 Loopback 接口，这样当网络中存在冗余链路时，不会因为其中某个接口或链路的故障而使 IPv6 BGP 连接中断。
- 当 BGP 对等体之间同时建立多条 BGP 连接时，如果没有明确指定建立 TCP 连接的源接口，可能会由于无法根据到达 BGP 对等体的最优路由确定 TCP 连接源接口从而导致无法建立 TCP 连接，因此建议用户在此情况下配置 BGP 对等体时明确配置 BGP 会话建立 TCP 连接的源接口为指定接口。

- 通常情况下，EBGP 对等体之间必须具有直连的物理链路，如果不满足这一要求，则必须使用 **peer ebgp-max-hop** 命令允许它们之间经过多跳建立 TCP 连接。但是，对于直连 EBGP 使用 Loopback 接口建立邻居关系，不需要 **peer ebgp-max-hop** 命令的配置。

## 1.10 IPv6 BGP 路由反射典型配置指导

### 1.10.1 组网图

图1-10 IPv6 BGP 路由反射器配置组网图



### 1.10.2 应用要求

Switch B 接收了一个经过 EBGP 的更新报文并将之传给 Switch C。Switch C 被配置为路由反射器，它有两个客户机：Switch B 和 Switch D。

Switch B 和 Switch D 间不需要建立 IBGP 连接，当 Switch C 接收了来自 Switch B 的路由更新时，它将此信息反射给 Switch D；反之，接收到的 Switch D 的路由信息也会被反射给 Switch B。

### 1.10.3 适用产品、版本

表1-10 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本    |
|-------------------|---------------------------------|---------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本 |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本 |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本 |

### 1.10.4 配置过程和解释

(1) 配置各 VLAN 接口的 IPv6 地址（略）

(2) 配置 IPv6 BGP 基本功能

# 配置 Switch A。

```
<SwitchA> system-view
[SwitchA] ipv6
```

```
[SwitchA] bgp 100
[SwitchA-bgp] router-id 1.1.1.1
[SwitchA-bgp] ipv6-family
[SwitchA-bgp-af-ipv6] peer 100::2 as-number 200
[SwitchA-bgp-af-ipv6] network 1:: 64
```

# 配置 Switch B。

```
<SwitchB> system-view
[SwitchB] ipv6
[SwitchB] bgp 200
[SwitchB-bgp] router-id 2.2.2.2
[SwitchB-bgp] ipv6-family
[SwitchB-bgp-af-ipv6] peer 100::1 as-number 100
[SwitchB-bgp-af-ipv6] peer 101::1 as-number 200
[SwitchB-bgp-af-ipv6] peer 101::1 next-hop-local
```

# 配置 Switch C。

```
<SwitchC> system-view
[SwitchC] ipv6
[SwitchC] bgp 200
[SwitchC-bgp] router-id 3.3.3.3
[SwitchC-bgp] ipv6-family
[SwitchC-bgp-af-ipv6] peer 101::2 as-number 200
[SwitchC-bgp-af-ipv6] peer 102::2 as-number 200
```

# 配置 Switch D。

```
<SwitchD> system-view
[SwitchD] ipv6
[SwitchD] bgp 200
[SwitchD-bgp] router-id 4.4.4.4
[SwitchD-bgp] ipv6-family
[SwitchD-bgp-af-ipv6] peer 102::1 as-number 200
```

(3) 配置路由反射器

# 配置 Switch C 作为路由反射器，Switch B 和 Switch D 是它的两个客户机。

```
[SwitchC-bgp-af-ipv6] peer 101::2 reflect-client
[SwitchC-bgp-af-ipv6] peer 102::2 reflect-client
```

在 Switch B 上用命令 **display bgp ipv6 routing-table**，可以看到 Switch B 已知道网络 1::/64 的存在。

在 Switch D 上用命令 **display bgp ipv6 routing-table**，可以看到 Switch D 也知道网络 1::/64 的存在。

## 1.10.5 完整配置

- 配置 Switch A。

```
#
ipv6
#
vlan 200
```



```
#
interface Vlan-interface200
 ipv6 address 100::1/96
#
bgp 100
 router-id 1.1.1.1
#
 ipv6-family
 network 1:: 64
 peer 100::2 as-number 200
#
```

- 配置 Switch B。

```
#
ipv6
#
vlan 200
#
vlan 300
#
interface Vlan-interface200
 ipv6 address 100::2/96
#
interface Vlan-interface300
 ipv6 address 101::2/96
#
bgp 200
 router-id 2.2.2.2
#
 ipv6-family
 peer 100::1 as-number 100
 peer 101::1 as-number 200
 peer 101::1 next-hop-local
#
```

- 配置 Switch C。

```
#
ipv6
#
vlan 100
#
vlan 300
#
interface Vlan-interface100
 ipv6 address 102::1/96
#
interface Vlan-interface300
 ipv6 address 101::1/96
#
bgp 200
```

```

router-id 3.3.3.3
#
ipv6-family
peer 101::2 as-number 200
peer 102::2 as-number 200
peer 101::2 reflect-client
peer 102::2 reflect-client
#
• 配置 Switch D。
#
ipv6
#
vlan 100
#
interface Vlan-interface100
ipv6 address 102::2/96
#
bgp 200
router-id 4.4.4.4
#
ipv6-family
peer 102::1 as-number 200
#

```

#### 1.10.6 配置注意事项

- 通常情况下，路由反射器的客户之间不要求是全连接的，路由缺省通过反射器从一个客户反射到其它客户；如果客户之间是全连接的，可以禁止客户间的反射，以便减少开销。
- 当一个集群里有多个路由反射器时，需要给所有位于同一个集群内的路由反射器配置相同的 Cluster\_ID，以避免路由循环。

### 1.11 在 IPv6 路由引入中应用路由策略典型配置指导

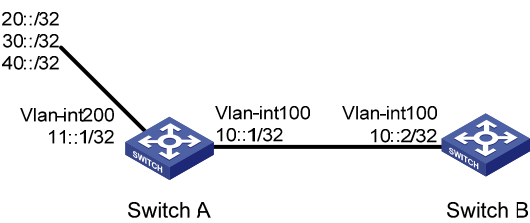
路由策略（Routing Policy）是为了改变网络流量所经过的途径而修改路由信息的技术，主要通过改变路由属性（包括可达性）来实现。

路由器在发布与接收路由信息时，可能需要实施一些策略，以便对路由信息进行过滤，例如只接收或发布满足一定条件的路由信息。一种路由协议可能需要引入其它的路由协议发现的路由信息，路由器在引入其它路由协议的路由信息时，可能只需要引入一部分满足条件的路由信息，并控制所引入的路由信息的某些属性，以使其满足本协议的要求。

为实现路由策略，首先要定义将要实施路由策略的路由信息的特征，即定义一组匹配规则。可以以路由信息中的不同属性作为匹配依据进行设置，如目的地址、发布路由信息的路由器地址等。匹配规则可以预先设置好，然后再将它们应用于路由的发布、接收和引入等过程的路由策略中。

1.11.1 组网图

图1-11 在 IPv6 路由引入中应用路由策略组网图



1.11.2 应用要求

- 在 Switch A 和 Switch B 上使能 RIPng 协议。
- 在 Switch A 上配置三条静态路由，并设置在引入静态路由时应用路由策略，使三条静态路由部分引入、部分被屏蔽掉——20::/32 和 40::/32 网段的路由是可见的，30::/32 网段的路由则被屏蔽。
- 通过在 Switch B 上查看 RIPng 路由表，验证路由策略是否生效。

1.11.3 适用产品、版本

表1-11 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本                         |
|-------------------|---------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本               | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本               | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本                      |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本                      |

1.11.4 配置过程和解释

(1) 配置 Switch A

# 配置接口 Vlan-interface100 和 Vlan-interface200 的 IPv6 地址。

```
<SwitchA> system-view
[SwitchA] ipv6
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ipv6 address 10::1 32
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 200
[SwitchA-Vlan-interface200] ipv6 address 11::1 32
```

```
[SwitchA-Vlan-interface200] quit
在接口下使能 RIPng。
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ripng 1 enable
[SwitchA-Vlan-interface100] quit
配置三条静态路由。
[SwitchA] ipv6 route-static 20:: 32 11::2
[SwitchA] ipv6 route-static 30:: 32 11::2
[SwitchA] ipv6 route-static 40:: 32 11::2
配置路由策略。
[SwitchA] ip ipv6-prefix a index 10 permit 30:: 32
[SwitchA] route-policy static2ripng deny node 0
[SwitchA-route-policy] if-match ipv6 address prefix-list a
[SwitchA-route-policy] quit
[SwitchA] route-policy static2ripng permit node 10
[SwitchA-route-policy] quit
启动 RIPng 协议并引入静态路由。
[SwitchA] ripng
[SwitchA-ripng-1] import-route static route-policy static2ripng
```

## (2) 配置 Switch B

```
配置接口 Vlan-interface100 的 IPv6 地址。
[SwitchB] ipv6
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ipv6 address 10::2 32
在接口下使能 RIPng。
[SwitchB-Vlan-interface100] ripng 1 enable
[SwitchB-Vlan-interface100] quit
启动 RIPng 协议。
[SwitchB] ripng
查看 RIPng 路由表。
[SwitchB-ripng-1] display ripng 1 route
Route Flags: A - Aging, S - Suppressed, G - Garbage-collect

Peer FE80::7D58:0:CA03:1 on Vlan-interface 100
Dest 10::/32,
 via FE80::7D58:0:CA03:1, cost 1, tag 0, A, 18 Sec
Dest 20::/32,
 via FE80::7D58:0:CA03:1, cost 1, tag 0, A, 8 Sec
Dest 40::/32,
 via FE80::7D58:0:CA03:1, cost 1, tag 0, A, 3 Sec
```

### 1.11.5 完整配置

- 配置 Switch A

```
#
ipv6
#
vlan 1
#
vlan 100
#
vlan 200
#
interface Vlan-interface100
 ipv6 address 10::1/32
 ripng 1 enable
#
interface Vlan-interface200
 ipv6 address 11::1/32
#
ripng 1
 import-route static route-policy static2ripng
#
route-policy static2ripng deny node 0
 if-match ipv6 address prefix-list a
route-policy static2ripng permit node 10
#
ip ipv6-prefix a index 10 permit 30:: 32
#
ipv6 route-static 20:: 32 11::2
ipv6 route-static 30:: 32 11::2
ipv6 route-static 40:: 32 11::2
#
```

- 配置 Switch B

```
#
ipv6
#
vlan 100
#
interface Vlan-interface100
 ipv6 address 10::2/32
 ripng 1 enable
#
ripng 1
#
```

#### 1.11.6 配置注意事项

- 如果所有表项都是 **deny** 模式，则任何路由都不能通过该过滤列表。这种情况下，需要在多条 **deny** 模式的表项后定义一条 **permit :: 0 less-equal 128** 的表项，以允许其它所有 IPv6 路由信息通过。
- **permit** 指定节点的匹配模式为允许模式。当路由信息通过该节点的过滤后，将执行该节点的 **apply** 子句，不进入下一个节点的测试；如果路由信息没有通过该节点过滤，将进入下一个节点继续测试。
- **deny** 指定节点的匹配模式为拒绝模式（此模式下 **apply** 子句不会被执行）。当路由项满足该节点的所有 **if-match** 子句时，将被拒绝通过该节点，不进入下一个节点的测试；如果路由项不满足该节点的 **if-match** 子句，将进入下一个节点继续测试。
- 如果路由策略中定义了一个以上的节点，则各节点中至少应该有一个节点的匹配模式是 **permit**。当路由策略用于路由信息过滤时，如果某路由信息没有通过任一节点，则认为该路由信息没有通过该路由策略。如果路由策略的所有节点都是 **deny** 模式，则没有路由信息能通过该路由策略。
- 对于同一个 **Route-policy** 节点，在匹配的过程中，各个 **if-match** 子句间是“与”的关系，即路由信息必须同时满足所有匹配条件，才可以执行 **apply** 子句的动作。
- 在一个节点中，可以没有 **if-match** 子句，也可以有多个 **if-match** 子句。当不指定 **if-match** 子句时，如果该节点的匹配模式为允许模式，则所有路由信息都会通过该节点的过滤；如果该节点的匹配模式为拒绝模式，则所有路由信息都会被拒绝。

# 目 录

|                                       |      |
|---------------------------------------|------|
| 1 组播典型配置指导.....                       | 1-1  |
| 1.1 IGMP典型配置指导 .....                  | 1-1  |
| 1.1.1 IGMP基本功能配置指导 .....              | 1-1  |
| 1.1.2 IGMP SSM Mapping典型配置指导 .....    | 1-4  |
| 1.2 IGMP Snooping典型配置指导 .....         | 1-9  |
| 1.2.1 组策略及模拟主机加入配置指导 .....            | 1-9  |
| 1.2.2 静态端口配置指导 .....                  | 1-12 |
| 1.2.3 IGMP Snooping查询器配置指导 .....      | 1-18 |
| 1.3 组播VLAN典型配置指导 .....                | 1-21 |
| 1.3.1 基于子VLAN的IPv4 组播VLAN典型配置指导 ..... | 1-22 |
| 1.3.2 基于端口的IPv4 组播VLAN典型配置指导 .....    | 1-25 |
| 1.4 PIM典型配置指导 .....                   | 1-29 |
| 1.4.1 PIM-DM典型配置指导 .....              | 1-29 |
| 1.4.2 PIM-SM非管理域配置指导 .....            | 1-34 |
| 1.4.3 PIM-SM管理域配置指导 .....             | 1-42 |
| 1.4.4 PIM-SSM典型配置指导 .....             | 1-48 |
| 1.5 MSDP典型配置指导 .....                  | 1-54 |
| 1.5.1 借助BGP路由的AS间组播配置指导 .....         | 1-54 |
| 1.5.2 借助静态RPF对等体的AS间组播配置指导 .....      | 1-63 |
| 1.5.3 Anycast RP应用配置指导 .....          | 1-70 |
| 1.6 组播路由与转发配置指导 .....                 | 1-77 |
| 1.6.1 改变RPF路由配置指导 .....               | 1-77 |
| 1.6.2 衔接RPF路由配置指导 .....               | 1-81 |
| 1.7 MBGP典型配置指导 .....                  | 1-84 |
| 1.7.1 MBGP典型配置指导 .....                | 1-84 |
| 1.8 组播VPN典型配置指导 .....                 | 1-90 |
| 1.8.1 单AS内的MD VPN典型配置指导 .....         | 1-90 |

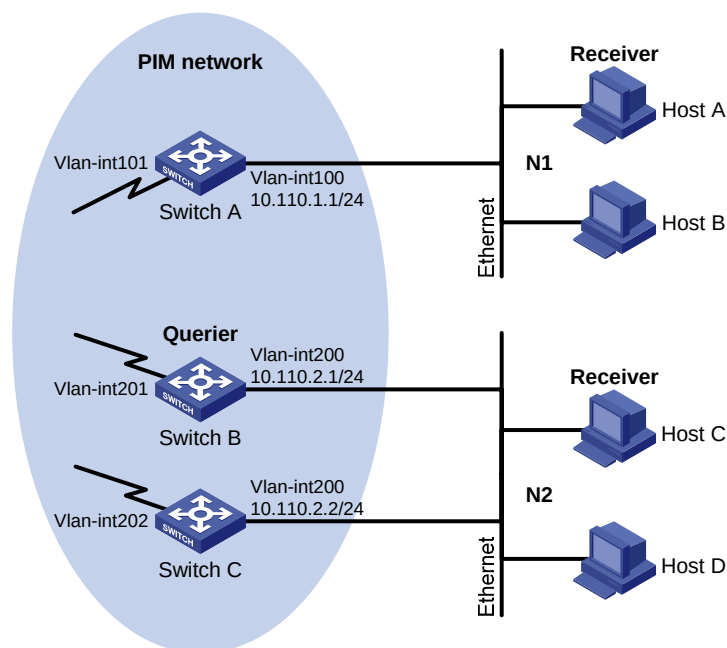
# 1 组播典型配置指导

## 1.1 IGMP 典型配置指导

### 1.1.1 IGMP 基本功能配置指导

#### 1. 组网图

图1-1 IGMP 典型配置指导组网图



#### 2. 组网需求

- 接收者（Receiver）通过组播方式接收视频点播信息，不同组织的接收者组成末梢网络 N1 和 N2，Host A 与 Host C 分别为 N1 和 N2 中的组播信息接收者。
- PIM 网络中的 Switch A 连接 N1，Switch B 与 Switch C 共同连接 N2。
- Switch A 通过 Vlan-interface100 连接 N1，通过 Vlan-interface101 连接 PIM 网络中的其它设备。
- Switch B 与 Switch C 分别通过各自的 Vlan-interface200 连接 N2，并分别通过 Vlan-interface201 和 Vlan-interface202 连接 PIM 网络中的其它设备。
- Switch A 与 N1 之间运行 IGMPv2；Switch B 和 Switch C 与 N2 之间也分别运行 IGMPv2。且由于 Switch B 的接口 IP 地址较小，因此在 N2 中通常由其来充当 IGMP 查询器。
- 配置 SwitchA 发送 IGMP 普遍组查询报文的时间间隔为 30 秒，最大响应时间为 5 秒，发送 IGMP 特定组查询报文的时间间隔为 2 秒。



### 3. 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本    |
|-------------------|---------------------------------|---------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本 |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本 |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本 |

### 4. 配置过程和解释

#### (1) 配置 IP 地址和单播路由协议

请按照 图 1-1配置各接口的IP地址和子网掩码，具体配置过程略。

配置 PIM 网络内各交换机之间采用 OSPF 协议进行互连，确保 PIM 网络内部在网络层互通，并且各交换机之间能够借助单播路由协议实现动态路由更新，具体配置过程略。

#### (2) 使能 IP 组播路由，并使能 PIM-DM 和 IGMP

# 在 Switch A 上使能 IP 组播路由，在各接口上使能 PIM-DM，并在主机侧接口 Vlan-interface100 上使能 IGMP。

```
<SwitchA> system-view
[SwitchA] multicast routing-enable
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] igmp enable
[SwitchA-Vlan-interface100] pim dm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim dm
[SwitchA-Vlan-interface101] quit
```

# 在 SwitchA 上配置发送 IGMP 通用组查询报文的时间间隔、最大响应时间，以及发送特定组查询报文的时间间隔。

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] igmp timer query 30
[SwitchA-Vlan-interface100] igmp max-response-time 5
[SwitchA-Vlan-interface100] igmp last-member-query-interval 2
```

# 在 Switch B 上使能 IP 组播路由，在各接口上使能 PIM-DM，并在主机侧接口 Vlan-interface200 上使能 IGMP。

```
<SwitchB> system-view
[SwitchB] multicast routing-enable
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] igmp enable
[SwitchB-Vlan-interface200] pim dm
```

```
[SwitchB-Vlan-interface200] quit
[SwitchB] interface vlan-interface 201
[SwitchB-Vlan-interface201] pim dm
[SwitchB-Vlan-interface201] quit
```

# 在 Switch C 上使能 IP 组播路由，在各接口上使能 PIM-DM，并在主机侧接口 Vlan-interface200 上使能 IGMP。

```
<SwitchC> system-view
[SwitchC] multicast routing-enable
[SwitchC] interface vlan-interface 200
[SwitchC-Vlan-interface200] igmp enable
[SwitchC-Vlan-interface200] pim dm
[SwitchC-Vlan-interface200] quit
[SwitchC] interface vlan-interface 202
[SwitchC-Vlan-interface202] pim dm
[SwitchC-Vlan-interface202] quit
```

### (3) 检验配置效果

通过使用 **display igmp interface** 命令可以查看各交换机接口上 IGMP 的配置和运行情况。例如：

# 查看 Switch B 在 Vlan-interface200 上的 IGMP 信息。

```
[SwitchB] display igmp interface vlan-interface 200
Vlan-interface200(10.110.2.1):
 IGMP is enabled
 Current IGMP version is 2
 Value of query interval for IGMP(in seconds): 60
 Value of other querier present interval for IGMP(in seconds): 125
 Value of maximum query response time for IGMP(in seconds): 10
 Querier for IGMP: 10.110.2.1 (this router)
 Total 1 IGMP Group reported
```

## 5. 完整配置

SwitchA、SwitchB 和 SwitchC 的完整配置类似，下面以 SwitchA 的完整配置为例：

```
#
multicast routing-enable
#
vlan 100 to 101
#
interface Vlan-interface100
 igmp enable
 igmp timer query 30
 igmp max-response-time 5
 igmp last-member-query-interval 2
 pim dm
#
interface Vlan-interface101
 pim dm
```

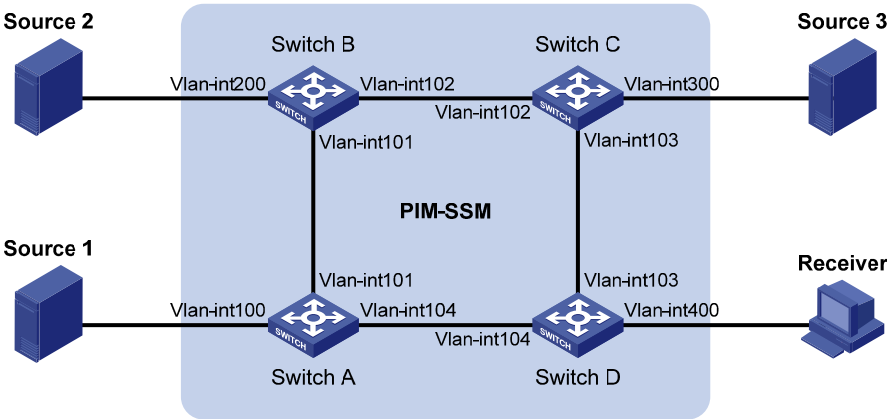
6. 配置注意事项

- 应确保发送 IGMP 普遍组查询报文的时间间隔大于 IGMP 普遍组查询的最大响应时间，否则有可能造成对组播组成员的误删除。
- 对 IGMP 普遍组查询的最大响应时间、发送 IGMP 特定组查询报文的时间间隔以及 IGMP 其它查询器的存在时间所做的配置，只有当设备运行在 IGMPv2 或 IGMPv3 时才有效。

1.1.2 IGMP SSM Mapping 典型配置指导

1. 组网图

图1-2 IGMP SSM Mapping 功能配置组网图



| 设备       | 接口          | IP 地址          | 设备       | 接口          | IP 地址          |
|----------|-------------|----------------|----------|-------------|----------------|
| Source 1 | -           | 133.133.1.1/24 | Source 3 | -           | 133.133.3.1/24 |
| Source 2 | -           | 133.133.2.1/24 | Receiver | -           | 133.133.4.1/24 |
| Switch A | Vlan-int100 | 133.133.1.2/24 | Switch C | Vlan-int300 | 133.133.3.2/24 |
|          | Vlan-int101 | 192.168.1.1/24 |          | Vlan-int103 | 192.168.3.1/24 |
|          | Vlan-int104 | 192.168.4.2/24 |          | Vlan-int102 | 192.168.2.2/24 |
| Switch B | Vlan-int200 | 133.133.2.2/24 | Switch D | Vlan-int400 | 133.133.4.2/24 |
|          | Vlan-int101 | 192.168.1.2/24 |          | Vlan-int103 | 192.168.3.2/24 |
|          | Vlan-int102 | 192.168.2.1/24 |          | Vlan-int104 | 192.168.4.1/24 |

2. 组网需求

- 在 PIM-SSM 网络中，接收者通过组播方式接收视频点播信息。接收者主机运行 IGMPv2，且不能升级至 IGMPv3，因此在加入组播组时无法指定组播源。
- 接收者主机加入的组播组范围为 232.1.1.0/24。
- 要求通过在 Switch D 上配置 IGMP SSM Mapping 功能，以使接收者主机只接收来自 Source 1 和 Source 3 的组播数据。

3. 适用产品、版本

表1-2 配置适用的产品与软硬件版本关系

| 产品              | 软件版本                            | 硬件版本    |
|-----------------|---------------------------------|---------|
| S7500E 系列以太网交换机 | Release 6100, Release 6300 软件版本 | 全系列硬件版本 |

## 4. 配置过程和解释

### (1) 配置 IP 地址和单播路由协议

请按照 图 1-2配置各接口的IP地址和子网掩码，具体配置过程略。

配置 PIM-SSM 网络内的各交换机之间采用 OSPF 协议进行互连，确保 PIM-SSM 网络内部在网络层互通，并且各交换机之间能够借助单播路由协议实现动态路由更新，具体配置过程略。

### (2) 使能 IP 组播路由，并使能 PIM-SM、IGMP 和 IGMP SSM Mapping 功能

# 在 Switch D 上使能 IP 组播路由，在各接口上使能 PIM-SM，并在主机侧接口 Vlan-interface400 上使能 IGMP 和 IGMP SSM Mapping 功能，配置 IGMP 版本为 3。

```
<SwitchD> system-view
[SwitchD] multicast routing-enable
[SwitchD] interface vlan-interface 400
[SwitchD-Vlan-interface400] igmp enable
[SwitchD-Vlan-interface400] igmp version 3
[SwitchD-Vlan-interface400] igmp ssm-mapping enable
[SwitchD-Vlan-interface400] pim sm
[SwitchD-Vlan-interface400] quit
[SwitchD] interface vlan-interface 103
[SwitchD-Vlan-interface103] pim sm
[SwitchD-Vlan-interface103] quit
[SwitchD] interface vlan-interface 104
[SwitchD-Vlan-interface104] pim sm
[SwitchD-Vlan-interface104] quit
```

# 在 Switch A 上使能 IP 组播路由，并在各接口上使能 PIM-SM。

```
<SwitchA> system-view
[SwitchA] multicast routing-enable
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] pim sm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim sm
[SwitchA-Vlan-interface101] quit
[SwitchA] interface vlan-interface 104
[SwitchA-Vlan-interface104] pim sm
[SwitchA-Vlan-interface104] quit
```

Switch B 和 Switch C 的配置与 Switch A 相似，配置过程略。

### (3) 配置 C-BSR 和 C-RP

# 在 Switch D 上配置 C-BSR 和 C-RP 的位置。

```
[SwitchD] pim
[SwitchD-pim] c-bsr vlan-interface 104
[SwitchD-pim] c-rp vlan-interface 104
[SwitchD-pim] quit
```

### (4) 配置 SSM 组播组的地址范围

# 在 Switch D 上配置 SSM 组播组地址范围为 232.1.1.0/24。

```
[SwitchD] acl number 2000
[SwitchD-acl-basic-2000] rule permit source 232.1.1.0 0.0.0.255
[SwitchD-acl-basic-2000] quit
[SwitchD] pim
[SwitchD-pim] ssm-policy 2000
[SwitchD-pim] quit
```

Switch A、Switch B 和 Switch C 的配置与 Switch D 相似，配置过程略。

#### (5) 配置 IGMP SSM Mapping 规则

# 在 Switch D 上配置 IGMP SSM Mapping 规则。

```
[SwitchD] igmp
[SwitchD-igmp] ssm-mapping 232.1.1.1 24 133.133.1.1
[SwitchD-igmp] ssm-mapping 232.1.1.1 24 133.133.3.1
[SwitchD-igmp] quit
```

#### (6) 检验配置效果

通过使用 **display igmp ssm-mapping** 命令可以查看交换机上的 IGMP SSM Mapping 规则。例如：

# 查看 Switch D 上组播组 232.1.1.1 的 IGMP SSM Mapping 规则。

```
[SwitchD] display igmp ssm-mapping 232.1.1.1
VPN-Instance: public net
Group: 232.1.1.1
Source list:
133.133.1.1
133.133.3.1
```

通过使用 **display igmp ssm-mapping group** 命令可以查看交换机上依据 IGMP SSM Mapping 规则创建的组播组信息。例如：

# 查看 Switch D 上依据 IGMP SSM Mapping 规则创建的组播组信息。

```
[SwitchD] display igmp ssm-mapping group
Total 1 IGMP SSM-mapping Group(s).
Interface group report information of VPN-Instance: public net
Vlan-interface400(133.133.4.2):
Total 1 IGMP SSM-mapping Group reported

Group Address	Last Reporter	Uptime	Expires
232.1.1.1	133.133.4.1	00:02:04	off


```

通过使用 **display pim routing-table** 命令可以查看交换机的 PIM 路由表信息。例如：

# 查看 Switch D 上的 PIM 路由表信息。

```
[SwitchD] display pim routing-table
VPN-Instance: public net
Total 0 (*, G) entry; 2 (S, G) entry

(133.133.1.1, 232.1.1.1)
RP: 192.168.4.1
Protocol: pim-ssm, Flag:
UpTime: 00:13:25
```

```

Upstream interface: Vlan-interface104
Upstream neighbor: 192.168.4.2
RPF prime neighbor: 192.168.4.2
Downstream interface(s) information:
Total number of downstreams: 1
1: Vlan-interface400
Protocol: igmp, UpTime: 00:13:25, Expires: -

(133.133.3.1, 232.1.1.1)
RP: 192.168.4.1
Protocol: pim-ssm, Flag:
UpTime: 00:13:25
Upstream interface: Vlan-interface103
Upstream neighbor: 192.168.3.1
RPF prime neighbor: 192.168.3.1
Downstream interface(s) information:
Total number of downstreams: 1
1: Vlan-interface400
Protocol: igmp, UpTime: 00:13:25, Expires: -

```

## 5. 完整配置

- DeviceD 的完整配置

```

#
multicast routing-enable
#
acl number 2000
rule 0 permit source 232.1.1.0 0.0.0.255
#
vlan 103 to 104
#
vlan 400
#
interface Vlan-interface103
pim sm
#
interface Vlan-interface104
pim sm
#
interface Vlan-interface400
igmp enable
igmp version 3
igmp ssm-mapping enable
#
igmp
ssm-mapping 232.1.1.0 24 133.133.1.1
ssm-mapping 232.1.1.0 24 133.133.3.1
#
pim

```

```

c-bsr Vlan-interface104
c-rp Vlan-interface104
ssm-policy 2000

```

- DeviceA 的配置

```

#
multicast routing-enable
#
acl number 2000
rule 0 permit source 232.1.1.0 0.0.0.255
#
vlan 100 to 101
#
vlan 104
#
interface Vlan-interface100
pim sm
#
interface Vlan-interface101
pim sm
#
interface Vlan-interface101
pim sm

```

DeviceB 和 DeviceC 的配置与 DeviceA 的基本一致, 仅 VLAN 接口编号存在差异, 这里不再赘述。

## 6. 配置注意事项

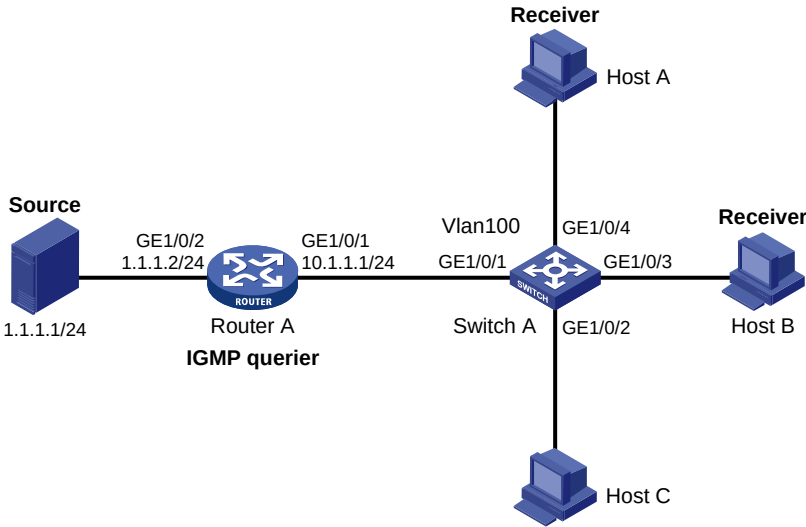
- IGMP SSM Mapping 不对 IGMPv3 的报告报文进行处理。
- 为保证本网段内运行任意版本 IGMP 的接收者主机都能得到 SSM 服务, 建议在处于该网段的接口上运行 IGMPv3。
- 对于同时支持 IGMP Snooping 和 IGMP 的交换机来说, 若 VLAN 接口上运行的是 IGMPv3, 则在使用 **igmp-snooping host-join** 命令配置模拟主机加入时即便不指定组播源, 模拟主机也仍将发送 IGMPv3 的报告报文, 这种情况下不会依据 IGMP SSM Mapping 规则创建相应的组播组。

# 1.2 IGMP Snooping 典型配置指导

## 1.2.1 组策略及模拟主机加入配置指导

### 1. 组网图

图1-3 模拟主机加入配置组网图



### 2. 应用要求

- 如图 1-3所示，Router A通过GigabitEthernet1/0/2 接口连接组播源（Source），通过GigabitEthernet1/0/1 接口连接Switch A；
- Router A 与 Switch A 之间运行 IGMPv2，Switch A 上运行版本 2 的 IGMP Snooping，并由 Router A 充当 IGMP 查询器；
- 通过配置，使连接在 Switch A 上的接收者（Receiver）Host A 和 Host B 只能接收发往组播组 224.1.1.1 的组播数据；
- 要求通过配置，使连接在 Switch A 上的接收者（Receiver）Host A 和 Host B 即使由于突然出现了某种意外而临时中断接收组播数据时，组播数据也能够不间断地通过 Switch A 的接口 GigabitEthernet1/0/3 和 GigabitEthernet1/0/4 转发出去。

### 3. 适用产品、版本

表1-3 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本                         |
|-------------------|---------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本               | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本               | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本                      |



| 产品                | 软件版本                            | 硬件版本    |
|-------------------|---------------------------------|---------|
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本 |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本 |

#### 4. 配置过程和解释

##### (1) 配置各设备接口的 IP 地址

请按照 图 1-3 配置各接口的 IP 地址和子网掩码，具体配置过程略。

##### (2) 配置 Router A

# 使能 IP 组播路由，在各接口上使能 PIM-DM，并在接口 GigabitEthernet1/0/1 上使能 IGMPv2。

```
<RouterA> system-view
[RouterA] multicast routing-enable
[RouterA] interface GigabitEthernet 1/0/1
[RouterA-GigabitEthernet1/0/1] igmp enable
[RouterA-GigabitEthernet1/0/1] pim dm
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface GigabitEthernet 1/0/2
[RouterA-GigabitEthernet1/0/2] pim dm
[RouterA-GigabitEthernet1/0/2] quit
```

##### (3) 配置 Switch A

# 全局使能 IGMP Snooping。

```
<SwitchA> system-view
[SwitchA] igmp-snooping
[SwitchA-igmp-snooping] quit
```

# 创建 VLAN 100，把端口 GigabitEthernet1/0/1 到 GigabitEthernet1/0/4 添加到该 VLAN 中，并在该 VLAN 内使能 IGMP Snooping，并开启丢弃未知组播数据报文功能。

```
[SwitchA] vlan 100
[SwitchA-vlan100] port GigabitEthernet 1/0/1 to GigabitEthernet 1/0/4
[SwitchA-vlan100] igmp-snooping enable
[SwitchA-vlan100] igmp-snooping drop-unknown
[SwitchA-vlan100] quit
```

# 配置组播组过滤器，使 VLAN 100 内的主机只能加入组播组 224.1.1.1。

```
[SwitchA] acl number 2001
[SwitchA-acl-basic-2001] rule permit source 224.1.1.1 0
[SwitchA-acl-basic-2001] quit
[SwitchA] igmp-snooping
[SwitchA-igmp-snooping] group-policy 2001 vlan 100
[SwitchA-igmp-snooping] quit
```

# 在 GigabitEthernet1/0/3 和 GigabitEthernet1/0/4 上分别使能模拟主机加入功能。

```
[SwitchA] interface GigabitEthernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] igmp-snooping host-join 224.1.1.1 vlan 100
[SwitchA-GigabitEthernet1/0/3] quit
```

```
[SwitchA] interface GigabitEthernet 1/0/4
[SwitchA-GigabitEthernet1/0/4] igmp-snooping host-join 224.1.1.1 vlan 100
[SwitchA-GigabitEthernet1/0/4] quit
```

#### (4) 检验配置效果

# 查看 Switch A 上 VLAN 100 内 IGMP Snooping 组播组的详细信息。

```
[SwitchA] display igmp-snooping group vlan 100 verbose
 Total 1 IP Group(s).
 Total 1 IP Source(s).
 Total 1 MAC Group(s).

Port flags: D-Dynamic port, S-Static port, A-Aggregation port, C-Copy port
Subvlan flags: R-Real VLAN, C-Copy VLAN
Vlan(id):100.
 Total 1 IP Group(s).
 Total 1 IP Source(s).
 Total 1 MAC Group(s).
 Router port(s):total 1 port.
 GE1/0/1 (D) (00:01:30)
 IP group(s):the following ip group(s) match to one mac group.
 IP group address:224.1.1.1
 (0.0.0.0, 224.1.1.1):
 Attribute: Host Port
 Host port(s):total 2 port.
 GE1/0/3 (D) (00:03:23)
 GE1/0/4 (D) (00:03:23)
 MAC group(s):
 MAC group address:0100-5e01-0101
 Host port(s):total 2 port.
 GE1/0/3
 GE1/0/4
```

由此可见，Switch A 上的端口 GigabitEthernet1/0/3 和 GigabitEthernet1/0/4 已经加入了组播组（0.0.0.0，224.1.1.1）。

## 5. 完整配置

```
#
acl number 2001
 rule 0 permit source 224.1.1.1 0
#
igmp-snooping
group-policy 2001 vlan 100
#
vlan 100
 igmp-snooping enable
 igmp-snooping drop-unknown
#
interface GigabitEthernet1/0/1
 port access vlan 100
```

```
#
interface GigabitEthernet1/0/2
port access vlan 100
#
interface GigabitEthernet1/0/3
port access vlan 100
igmp-snooping host-join 224.1.1.1 vlan 1
#
interface GigabitEthernet1/0/4
port access vlan 100
igmp-snooping host-join 224.1.1.1 vlan 1
#
```

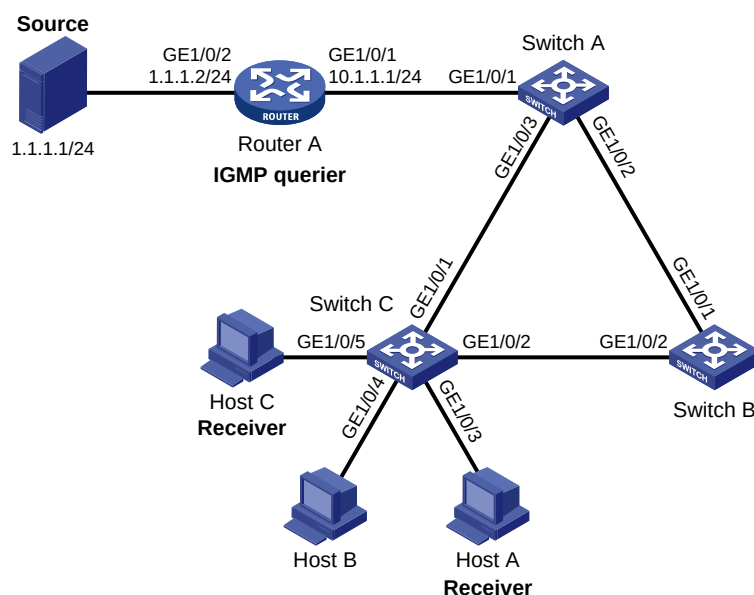
## 6. 配置注意事项

- 二、三层组播协议可以同时运行在交换机上，但是在同一个 VLAN 和该 VLAN 对应的虚接口上不能同时运行二层和三层组播协议。
- 在启动指定 VLAN 的 IGMP Snooping 前，应首先在系统视图下启动全局 IGMP Snooping 功能，否则将无法配置成功。
- 与静态成员端口不同，配置了模拟主机加入的端口会作为动态成员端口而参与动态成员端口的老化过程。
- 在使能了丢弃未知 IPv4 组播数据报文功能之后，未知 IPv6 组播数据报文也将被丢弃。

## 1.2.2 静态端口配置指导

### 1. 组网图

图1-4 静态路由器端口配置组网图



### 2. 应用要求

当某些组播接收者需要固定、稳定的接收到某个组播组的数据时，可以配置静态端口来增强组播数据在传输过程中的可靠性。

- 如图 1-4所示，Router A通过GigabitEthernet1/0/2 接口连接组播源（Source），通过GigabitEthernet1/0/1 接口连接Switch A；
- Router A 与 Switch A 之间运行 IGMP，Switch A、Switch B 和 Switch C 上都运行 IGMP Snooping，并由 Router A 充当 IGMP 查询器；
- 假设由于受 STP 等链路层协议的影响，为了避免出现环路，Switch A—Switch C 的转发路径在正常情况下是阻断的，组播数据只能通过 Switch A—Switch B—Switch C 的路径传递给连接在 Switch C 上的接收者（Receiver）Host A 和 Host C；
- 要求通过将 Switch A 上连接 Switch C 的端口 GigabitEthernet1/0/3 配置为静态路由器端口，从而保证当 Switch A—Switch B—Switch C 的路径出现阻断时，组播数据可以几乎不间断地通过 Switch A—Switch C 的新路径传递给接收者。
- 将 SwitchC 的端口 GigabitEthernet1/0/3 和 GigabitEthernet1/0/5 配置为静态成员端口，从而保证这两个端口下连接的主机能收到固定的接收组播组 225.1.1.1 的组播数据。



#### 说明

如果没有配置静态路由器端口，那么当 Switch A—Switch B—Switch C 的路径出现阻断时，至少需要等待一个 IGMP 查询和响应周期完成后，组播数据才能通过 Switch A—Switch C 的新路径传递给接收者，组播数据的传输在这个过程中将中断。

### 3. 适用产品、版本

表1-4 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本                         |
|-------------------|---------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本               | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本               | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本                      |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本                      |

### 4. 配置过程和解释

#### (1) 配置各设备接口的 IP 地址

请按照 图 1-4配置各接口的IP地址和子网掩码，具体配置过程略。

#### (2) 配置 Router A

# 使能 IP 组播路由，在各接口上使能 PIM-DM，并在接口 GigabitEthernet1/0/1 上使能 IGMP。

```
<RouterA> system-view
```

```
[RouterA] multicast routing-enable
[RouterA] interface GigabitEthernet 1/0/1
[RouterA-GigabitEthernet1/0/1] igmp enable
[RouterA-GigabitEthernet1/0/1] pim dm
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface GigabitEthernet 1/0/2
[RouterA-GigabitEthernet1/0/2] pim dm
[RouterA-GigabitEthernet1/0/2] quit
```

### (3) 配置 Switch A

# 全局使能 IGMP Snooping。

```
<SwitchA> system-view
[SwitchA] igmp-snooping
[SwitchA-igmp-snooping] quit
```

# 创建 VLAN 100，把端口 GigabitEthernet1/0/1 到 GigabitEthernet1/0/3 添加到该 VLAN 中，并在该 VLAN 内使能 IGMP Snooping。

```
[SwitchA] vlan 100
[SwitchA-vlan100] port GigabitEthernet 1/0/1 to GigabitEthernet 1/0/3
[SwitchA-vlan100] igmp-snooping enable
[SwitchA-vlan100] quit
```

# 把 GigabitEthernet1/0/3 配置为静态路由器端口。

```
[SwitchA] interface GigabitEthernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] igmp-snooping static-router-port vlan 100
[SwitchA-GigabitEthernet1/0/3] quit
```

### (4) 配置 Switch B

# 全局使能 IGMP Snooping。

```
<SwitchB> system-view
[SwitchB] igmp-snooping
[SwitchB-igmp-snooping] quit
```

# 创建 VLAN 100，把端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 添加到该 VLAN 中，并在该 VLAN 内使能 IGMP Snooping。

```
[SwitchB] vlan 100
[SwitchB-vlan100] port GigabitEthernet 1/0/1 GigabitEthernet 1/0/2
[SwitchB-vlan100] igmp-snooping enable
[SwitchB-vlan100] quit
```

### (5) 配置 Switch C

# 全局使能 IGMP Snooping。

```
<SwitchC> system-view
[SwitchC] igmp-snooping
[SwitchC-igmp-snooping] quit
```

# 创建 VLAN 100，把端口 GigabitEthernet1/0/1 到 GigabitEthernet1/0/5 添加到该 VLAN 中，并在该 VLAN 内使能 IGMP Snooping。

```
[SwitchC] vlan 100
[SwitchC-vlan100] port GigabitEthernet 1/0/1 to GigabitEthernet 1/0/5
```

```
[SwitchC-vlan100] igmp-snooping enable
```

```
[SwitchC-vlan100] quit
```

# 在 VLAN 100 内的端口 GigabitEthernet1/0/3 和 GigabitEthernet1/0/5 上配置静态加入组播组 225.1.1.1。

```
[SwitchC] interface GigabitEthernet 1/0/3
```

```
[SwitchC-GigabitEthernet1/0/3] igmp-snooping static-group 225.1.1.1 vlan 100
```

```
[SwitchC-GigabitEthernet1/0/3] quit
```

```
[SwitchC] interface GigabitEthernet 1/0/5
```

```
[SwitchC-GigabitEthernet1/0/5] igmp-snooping static-group 225.1.1.1 vlan 100
```

```
[SwitchC-GigabitEthernet1/0/5] quit
```

#### (6) 检验配置效果

# 查看 Switch A 上 VLAN 100 内 IGMP Snooping 组播组的详细信息。

```
[SwitchA] display igmp-snooping group vlan 100 verbose
```

```
Total 1 IP Group(s).
```

```
Total 1 IP Source(s).
```

```
Total 1 MAC Group(s).
```

```
Port flags: D-Dynamic port, S-Static port, A-Aggregation port, C-Copy port
```

```
Subvlan flags: R-Real VLAN, C-Copy VLAN
```

```
Vlan(id):100.
```

```
Total 1 IP Group(s).
```

```
Total 1 IP Source(s).
```

```
Total 1 MAC Group(s).
```

```
Router port(s):total 2 port.
```

```
GE1/0/1 (D) (00:01:30)
```

```
GE1/0/3 (S)
```

```
IP group(s):the following ip group(s) match to one mac group.
```

```
IP group address:225.1.1.1
```

```
(0.0.0.0, 225.1.1.1):
```

```
Attribute: Host Port
```

```
Host port(s):total 1 port.
```

```
GE1/0/2 (D) (00:03:23)
```

```
MAC group(s):
```

```
MAC group address:0100-5e01-0101
```

```
Host port(s):total 1 port.
```

```
GE1/0/2
```

由此可见，Switch A 上的端口 GigabitEthernet1/0/3 已经成为了静态路由器端口。

# 查看 Switch C 上 VLAN 100 内 IGMP Snooping 组播组的详细信息。

```
[SwitchC] display igmp-snooping group vlan 100 verbose
```

```
Total 1 IP Group(s).
```

```
Total 1 IP Source(s).
```

```
Total 1 MAC Group(s).
```

```
Port flags: D-Dynamic port, S-Static port, A-Aggregation port, C-Copy port
```

```
Subvlan flags: R-Real VLAN, C-Copy VLAN
```

```
Vlan(id):100.
```

```

Total 1 IP Group(s).
Total 1 IP Source(s).
Total 1 MAC Group(s).
Router port(s):total 1 port.
GE1/0/2 (D) (00:01:30)
IP group(s):the following ip group(s) match to one mac group.
IP group address:225.1.1.1
(0.0.0.0, 225.1.1.1):
Host port(s):total 1 port.
GE1/0/3 (S)
GE1/0/5 (S)
MAC group(s):
MAC group address:0100-5e01-0101
Host port(s):total 1 port.
GE1/0/3
GE1/0/5

```

由此可见，Switch C 上的端口 GigabitEthernet1/0/3 和 GigabitEthernet1/0/5 已经成为了静态成员端口。

## 5. 完整配置

### (1) SwitchA 配置信息

```

#
igmp-snooping
#
vlan 100
igmp-snooping enable
#
interface GigabitEthernet1/0/1
port access vlan 100
#
interface GigabitEthernet1/0/2
port access vlan 100
#
interface GigabitEthernet1/0/3
port access vlan 100
igmp-snooping static-router-port vlan 100
#

```

### (2) SwitchB 配置信息

```

#
igmp-snooping
#
vlan 100
igmp-snooping enable
#
interface GigabitEthernet1/0/1
port access vlan 100
#

```

```
interface GigabitEthernet1/0/2
port access vlan 100
#
```

### (3) SwitchC 配置信息

```
#
igmp-snooping
#
vlan 100
igmp-snooping enable
#
interface GigabitEthernet1/0/1
port access vlan 100
#
interface GigabitEthernet1/0/2
port access vlan 100
#
interface GigabitEthernet1/0/3
port access vlan 100
igmp-snooping static-group 225.1.1.1 vlan 100
#
interface GigabitEthernet1/0/4
port access vlan 100
#
interface GigabitEthernet1/0/5
port access vlan 100
igmp-snooping static-group 225.1.1.1 vlan 100
#
```

## 6. 配置注意事项

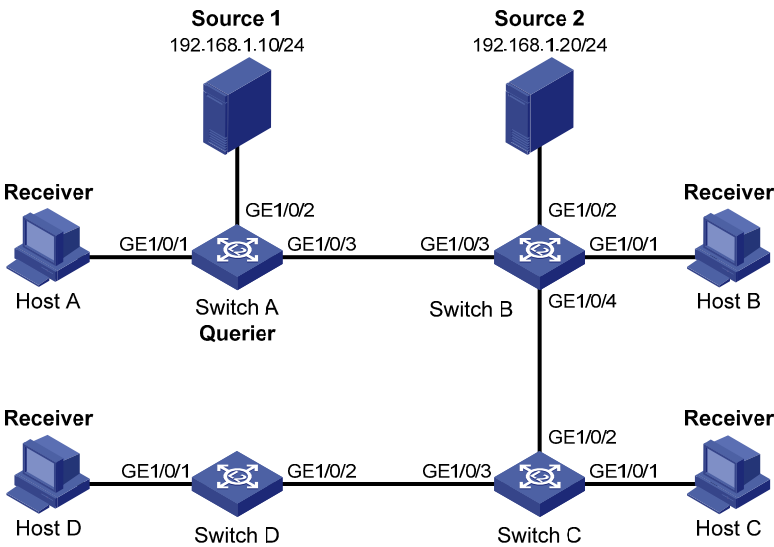
无



### 1.2.3 IGMP Snooping 查询器配置指导

#### 1. 组网图

图1-5 IGMP Snooping 查询器配置组网图



#### 2. 应用要求

- 如图 1-5所示，在一个没有三层设备的纯二层网络环境中，组播源Source 1 和Source 2 分别向组播组 224.1.1.1 和 225.1.1.1 发送组播数据，Host A和Host C是组播组 224.1.1.1 的接收者（Receiver），Host B和Host D则是组播组 225.1.1.1 的接收者；
- 所有接收者均使用 IGMPv2，所有交换机上都运行版本 2 的 IGMP Snooping，并选择距组播源较近的 Switch A 来充当 IGMP Snooping 查询器；
- 为了防止交换机在没有二层组播转发表项时将组播数据在 VLAN 内广播，要求在所有交换机上都使能丢弃未知组播数据报文的功能；
- 由于交换机不会将收到源 IP 地址为 0.0.0.0 的 IGMP 查询报文的端口设置为动态路由器端口，从而会影响二层组播转发表项的建立并导致组播数据无法正常转发，因此要求通过配置改变缺省的 IGMP 查询报文源 IP 地址（即 0.0.0.0）以避免上述问题的出现。

#### 3. 适用产品、版本

表1-5 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本                         |
|-------------------|---------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本               | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本               | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本                      |

| 产品                | 软件版本                            | 硬件版本    |
|-------------------|---------------------------------|---------|
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本 |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本 |

#### 4. 配置过程 and 解释

##### (1) 配置 Switch A

# 全局使能 IGMP Snooping。

```
<SwitchA> system-view
[SwitchA] igmp-snooping
[SwitchA-igmp-snooping] quit
```

# 创建 VLAN 100，并把端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/3 添加到该 VLAN 中。

```
[SwitchA] vlan 100
[SwitchA-vlan100] port GigabitEthernet 1/0/1 to GigabitEthernet 1/0/3
```

# 在 VLAN 100 内使能 IGMP Snooping，并使能丢弃未知组播数据报文功能。

```
[SwitchA-vlan100] igmp-snooping enable
[SwitchA-vlan100] igmp-snooping drop-unknown
```

# 在 VLAN 100 内使能 IGMP Snooping 查询器。

```
[SwitchA-vlan100] igmp-snooping querier
```

# 在 VLAN 100 内把 IGMP 普遍组查询和特定组查询报文的源 IP 地址均设置为 192.168.1.1。

```
[SwitchA-vlan100] igmp-snooping general-query source-ip 192.168.1.1
[SwitchA-vlan100] igmp-snooping special-query source-ip 192.168.1.1
```

##### (2) 配置 Switch B

# 全局使能 IGMP Snooping。

```
<SwitchB> system-view
[SwitchB] igmp-snooping
[SwitchB-igmp-snooping] quit
```

# 创建 VLAN 100，把端口 GigabitEthernet1/0/1 到 GigabitEthernet1/0/4 添加到该 VLAN 中。

```
[SwitchB] vlan 100
[SwitchB-vlan100] port GigabitEthernet 1/0/1 to GigabitEthernet 1/0/4
```

# 在 VLAN 100 内使能 IGMP Snooping，并使能丢弃未知组播数据报文功能。

```
[SwitchB-vlan100] igmp-snooping enable
[SwitchB-vlan100] igmp-snooping drop-unknown
[SwitchB-vlan100] quit
```

Switch C 和 Switch D 的配置与 Switch B 相似，配置过程略。

##### (3) 检验配置效果

当 IGMP Snooping 查询器开始工作之后，除查询器以外的所有交换机都能收到 IGMP 普遍组查询报文。通过使用 **display igmp-snooping statistics** 命令可以查看 IGMP 报文的统计信息，例如：

# 查看 Switch B 上收到的 IGMP 报文的统计信息。

```
[SwitchB-vlan100] display igmp-snooping statistics
Received IGMP general queries:3.
Received IGMPv1 reports:0.
Received IGMPv2 reports:12.
Received IGMP leaves:0.
Received IGMPv2 specific queries:0.
Sent IGMPv2 specific queries:0.
Received IGMPv3 reports:0.
Received IGMPv3 reports with right and wrong records:0.
Received IGMPv3 specific queries:0.
Received IGMPv3 specific sg queries:0.
Sent IGMPv3 specific queries:0.
Sent IGMPv3 specific sg queries:0.
Received error IGMP messages:0.
```

## 5. 完整配置

- SwitchA 配置信息

```
#
igmp-snooping
#
vlan 100
igmp-snooping enable
igmp-snooping drop-unknown
igmp-snooping querier
igmp-snooping general-query source-ip 192.168.1.1
igmp-snooping special-query source-ip 192.168.1.1
#
interface GigabitEthernet1/0/1
port access vlan 100
#
interface GigabitEthernet1/0/2
port access vlan 100
#
interface GigabitEthernet1/0/3
port access vlan 100
#
```

- SwitchB 配置信息

```
#
igmp-snooping
#
vlan 100
igmp-snooping enable
igmp-snooping drop-unknown
#
interface GigabitEthernet1/0/1
```

```
port access vlan 100
#
interface GigabitEthernet1/0/2
port access vlan 100
#
interface GigabitEthernet1/0/3
port access vlan 100
#
interface GigabitEthernet1/0/4
port access vlan 100
#
```

SwitchC 和 SwitchD 的配置过程和 SwitchB 配置过程类似。

## 6. 配置注意事项

- 尽管 IGMP Snooping 查询器并不参与 IGMP 查询器的选举，但在运行了 IGMP 的组播网络中，配置 IGMP Snooping 查询器不但没有实际的意义，反而可能会由于其发送的 IGMP 普遍组查询报文的源 IP 地址较小而影响 IGMP 查询器的选举。
- 应确保发送 IGMP 普遍组查询报文的时间间隔大于 IGMP 普遍组查询的最大响应时间，否则有可能造成对组播组成员的误删。

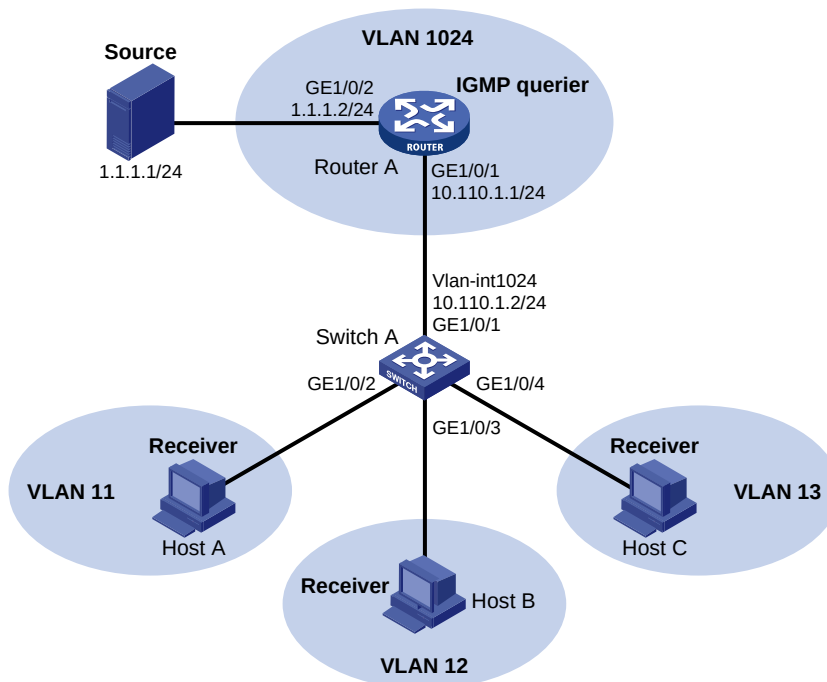
## 1.3 组播 VLAN 典型配置指导

在传统的组播点播方式下，当属于不同 VLAN 的主机 Host A、Host B 和 Host C 分别进行组播点播时，Router A 需要把组播数据在每个 VLAN 内都复制一份。这样既造成了带宽的浪费，也给三层设备增加了额外的负担。

### 1.3.1 基于子 VLAN 的 IPv4 组播 VLAN 典型配置指导

#### 1. 组网图

图1-6 基于子 VLAN 的 IPv4 组播 VLAN 典型配置组网图



#### 2. 应用要求

- 如图 1-6所示，Router A通过GigabitEthernet1/0/2 接口连接组播源（Source），通过 GigabitEthernet1/0/1 接口连接Switch A；
- Router A 与 Switch A 之间运行 IGMP，Switch A 上运行 IGMP Snooping，并由 Router A 充当 IGMP 查询器；
- Switch A 的端口 GigabitEthernet1/01 属于 VLAN 1024，端口 GigabitEthernet1/0/2 到 GigabitEthernet1/0/4 分别属于 VLAN 11 到 VLAN 13，Host A 到 Host C 分别连接到 Switch A 的端口 GigabitEthernet1/0/2 到 GigabitEthernet1/0/4 上；
- 通过配置组播 VLAN，使 Router A 向 Switch A 下的这三台主机传送组播数据时，只需要向 VLAN 1024 发送一份即可，而不必向每个 VLAN 都发送。

#### 3. 适用产品、版本

表1-6 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本                         |
|-------------------|---------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本               | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本               | S5500-20TP-SI                |

| 产品                | 软件版本                            | 硬件版本    |
|-------------------|---------------------------------|---------|
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本 |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本 |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本 |

#### 4. 配置过程 and 解释

##### (1) 配置各设备接口的 IP 地址

请按照 图 1-6 配置各接口的 IP 地址和子网掩码，具体配置过程略。

##### (2) 配置 Router A

# 使能 IP 组播路由，在各接口上使能 PIM-DM，并在接口 GigabitEthernet1/0/1 上使能 IGMP。

```
<RouterA> system-view
[RouterA] multicast routing-enable
[RouterA] interface GigabitEthernet 1/0/1
[RouterA-GigabitEthernet1/0/1] pim dm
[RouterA-GigabitEthernet1/0/1] igmp enable
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface GigabitEthernet 1/0/2
[RouterA-GigabitEthernet1/0/2] pim dm
[RouterA-GigabitEthernet1/0/2] quit
```

##### (3) 配置 Switch A

# 全局使能 IGMP Snooping。

```
<SwitchA> system-view
[SwitchA] igmp-snooping
[SwitchA-igmp-snooping] quit
```

# 创建 VLAN 11，并把端口 GigabitEthernet1/0/2 添加到该 VLAN 中。

```
[SwitchA] vlan 11
[SwitchA-vlan11] port GigabitEthernet 1/0/2
[SwitchA-vlan11] quit
```

VLAN 12 与 VLAN 13 的配置与 VLAN 11 相似，配置过程略。

# 创建 VLAN 1024，把端口 GigabitEthernet1/0/1 添加到该 VLAN 中，并在该 VLAN 内使能 IGMP Snooping。

```
[SwitchA] vlan 1024
[SwitchA-vlan1024] port GigabitEthernet 1/0/1
[SwitchA-vlan1024] igmp-snooping enable
[SwitchA-vlan1024] quit
```

# 使能 VLAN 1024 为组播 VLAN，并把 VLAN 11 到 VLAN 13 都配置为该组播 VLAN 的子 VLAN。

```
[SwitchA] multicast-vlan 1024 enable
[SwitchA] multicast-vlan 1024 subvlan 11 to 13
```

##### (4) 检验配置效果

# 查看 Switch A 上所有组播 VLAN 及其子 VLAN 的信息。

```
[SwitchA] display multicast-vlan
multicast vlan 1024's subvlan list:
vlan 11-13
```

## 5. 完整配置

此处仅列出 SwitchA 上的完整配置

```
#
igmp-snooping
#
vlan 11 to 13
#
interface GigabitEthernet1/0/2
port access vlan 11
#
interface GigabitEthernet1/0/3
port access vlan 12
#
interface GigabitEthernet1/0/4
port access vlan 13
#
interface GigabitEthernet1/0/1
port access vlan 1024
#
multicast-vlan 1024 enable
multicast-vlan 1024 subvlan 11 to 13
#
```

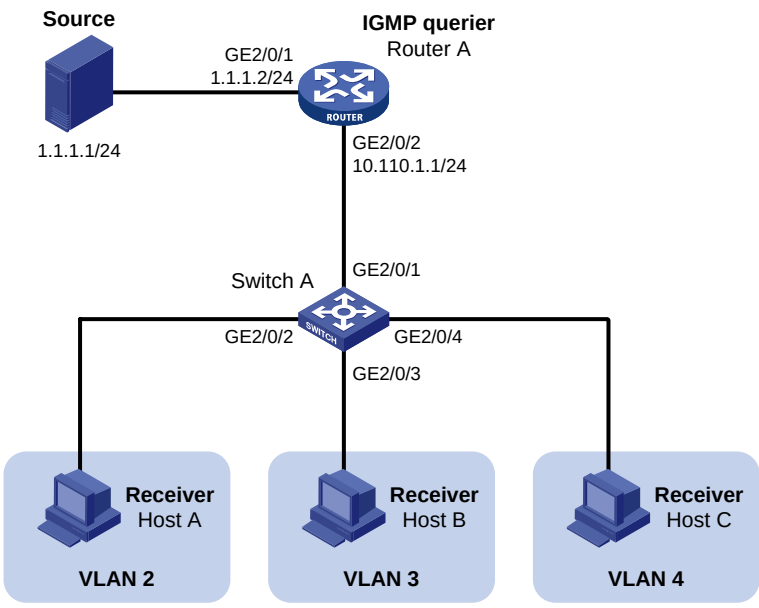
## 6. 配置注意事项

- 如果设备上已使能了 IP 组播路由，则不允许在该设备上配置组播 VLAN。
- 在配置成为组播 VLAN 的 VLAN 内必须使能 IGMP Snooping，才能实现组播 VLAN 功能；而在组播 VLAN 的子 VLAN 内不必使能 IGMP Snooping。

### 1.3.2 基于端口的 IPv4 组播 VLAN 典型配置指导

#### 1. 组网图

图1-7 基于端口的 IPv4 组播 VLAN 配置组网图



#### 2. 组网需求

- 如图 1-7所示，Router A通过接口GigabitEthernet2/0/1 连接组播源（Source），通过接口 GigabitEthernet2/0/2 连接Switch A；
- Router A 上运行 IGMPv2，Switch A 上运行版本 2 的 IGMP Snooping，并由 Router A 充当 IGMP 查询器；
- Switch A 的端口 GigabitEthernet2/0/1 属于 VLAN 10，端口 GigabitEthernet2/0/2 到 GigabitEthernet2/0/4 分别属于 VLAN 2 到 VLAN 4，Host A 到 Host C 分别连接到 Switch A 的端口 GigabitEthernet2/0/2 到 GigabitEthernet2/0/4 上；
- 组播源向组播组 224.1.1.1 发送组播数据，Host A、Host B 和 Host C 都是该组播组的接收者（Receiver）；
- 通过配置基于端口的组播 VLAN，使 Router A 通过组播 VLAN 向 Switch A 下分属不同用户 VLAN 的主机分发组播数据。

#### 3. 适用产品、版本

表1-7 配置适用的产品与软硬件版本关系

| 产品              | 软件版本              | 硬件版本    |
|-----------------|-------------------|---------|
| S7500E 系列以太网交换机 | Release 6300 软件版本 | 全系列硬件版本 |

#### 4. 配置步骤和解释

##### (1) 配置 IP 地址

请按照 图 1-7配置各接口的IP地址和子网掩码，具体配置过程略。



## (2) 配置 Router A

# 使能 IP 组播路由，在各接口上使能 PIM-DM，并在主机侧接口 Ethernet1/0/2 上使能 IGMP。

```
<RouterA> system-view
[RouterA] multicast routing-enable
[RouterA] interface gigabitethernet 2/0/1
[RouterA-GigabitEthernet2/0/1] pim dm
[RouterA-GigabitEthernet2/0/1] quit
[RouterA] interface gigabitethernet 2/0/2
[RouterA-GigabitEthernet2/0/2] pim dm
[RouterA-GigabitEthernet2/0/2] igmp enable
```

## (3) 配置 Switch A

# 全局使能 IGMP Snooping。

```
<SwitchA> system-view
[SwitchA] igmp-snooping
[SwitchA-igmp-snooping] quit
```

# 创建 VLAN 10，把端口 GigabitEthernet2/0/1 添加到该 VLAN 中，并在该 VLAN 内使能 IGMP Snooping。

```
[SwitchA] vlan 10
[SwitchA-vlan10] port gigabitethernet 2/0/1
[SwitchA-vlan10] igmp-snooping enable
[SwitchA-vlan10] quit
```

# 创建 VLAN 2，并在该 VLAN 内使能 IGMP Snooping。

```
[SwitchA] vlan 2
[SwitchA-vlan2] igmp-snooping enable
[SwitchA-vlan2] quit
```

VLAN 3 与 VLAN 4 的配置与 VLAN 2 相似，配置过程略。

# 配置端口 GigabitEthernet2/0/2 为 Hybrid 类型，缺省 VLAN 为 VLAN 2；允许 VLAN 2 和 VLAN 10 的报文通过，且均不携带 Tag。

```
[SwitchA] interface gigabitethernet 2/0/2
[SwitchA-GigabitEthernet2/0/2] port link-type hybrid
[SwitchA-GigabitEthernet2/0/2] port hybrid pvid vlan 2
[SwitchA-GigabitEthernet2/0/2] port hybrid vlan 2 untagged
[SwitchA-GigabitEthernet2/0/2] port hybrid vlan 10 untagged
[SwitchA-GigabitEthernet2/0/2] quit
```

GigabitEthernet2/0/3 与 GigabitEthernet2/0/4 的配置与 GigabitEthernet2/0/2 相似，不同的是 GigabitEthernet2/0/3 的缺省 VLAN 为 3，允许 VLAN3 和 VLAN10 的报文不带 Tag 通过；GigabitEthernet2/0/4 的缺省 VLAN 为 4，允许 VLAN4 和 VLAN10 的报文不带 Tag 通过，配置过程略。

# 配置 VLAN 10 为组播 VLAN。

```
[SwitchA] multicast-vlan 10
```

# 将端口 GigabitEthernet2/0/2 到 GigabitEthernet2/0/4 添加到组播 VLAN 10 内。

```
[SwitchA-mvlan-10] port gigabitethernet 2/0/2 to gigabitethernet 2/0/4
```

```
[SwitchA-mvlan-10] quit
```

#### (4) 检验配置效果

# 查看 Switch A 上所有组播 VLAN 的信息。

```
[SwitchA] display multicast-vlan
```

```
Total 1 multicast-vlan(s)
```

```
Multicast vlan 10
```

```
subvlan list:
```

```
no subvlan
```

```
port list:
```

```
GE2/0/2 GE2/0/3 GE2/0/4
```

# 查看 Switch A 上 IGMP Snooping 组播组的信息。

```
[SwitchA] display igmp-snooping group
```

```
Total 1 IP Group(s).
```

```
Total 1 IP Source(s).
```

```
Total 1 MAC Group(s).
```

```
Port flags: D-Dynamic port, S-Static port, C-Copy port
```

```
Subvlan flags: R-Real VLAN, C-Copy VLAN
```

```
Vlan(id):10.
```

```
Total 1 IP Group(s).
```

```
Total 1 IP Source(s).
```

```
Total 1 MAC Group(s).
```

```
Router port(s):total 1 port.
```

```
GE2/0/1 (D)
```

```
IP group(s):the following ip group(s) match to one mac group.
```

```
IP group address:224.1.1.1
```

```
(0.0.0.0, 224.1.1.1):
```

```
Host port(s):total 3 port.
```

```
GE2/0/2 (D)
```

```
GE2/0/3 (D)
```

```
GE2/0/4 (D)
```

```
MAC group(s):
```

```
MAC group address:0100-5e01-0101
```

```
Host port(s):total 3 port.
```

```
GE2/0/2
```

```
GE2/0/3
```

```
GE2/0/4
```

由此可见，IGMP Snooping 统一在组播 VLAN（VLAN 10）中维护路由器端口和成员端口。

## 5. 完整配置

此处仅列出 SwitchA 上的完整配置。

```
#
```

```
igmp-snooping
```

```
#
```

```
vlan 2
```

```

igmp-snooping enable
#
vlan 3
igmp-snooping enable
#
vlan 4
igmp-snooping enable
#
vlan 10
igmp-snooping enable
#
interface GigabitEthernet2/0/1
port access vlan 10
#
interface GigabitEthernet2/0/2
port link-type hybrid
port hybrid vlan 1 to 2 10 untagged
port hybrid pvid vlan 2
#
interface GigabitEthernet2/0/3
port link-type hybrid
port hybrid vlan 1 3 10 untagged
port hybrid pvid vlan 3
#
interface GigabitEthernet2/0/4
port link-type hybrid
port hybrid vlan 1 4 10 untagged
port hybrid pvid vlan 4
#
multicast-vlan 10
port GigabitEthernet2/0/2 to GigabitEthernet2/0/4

```

## 6. 配置注意事项

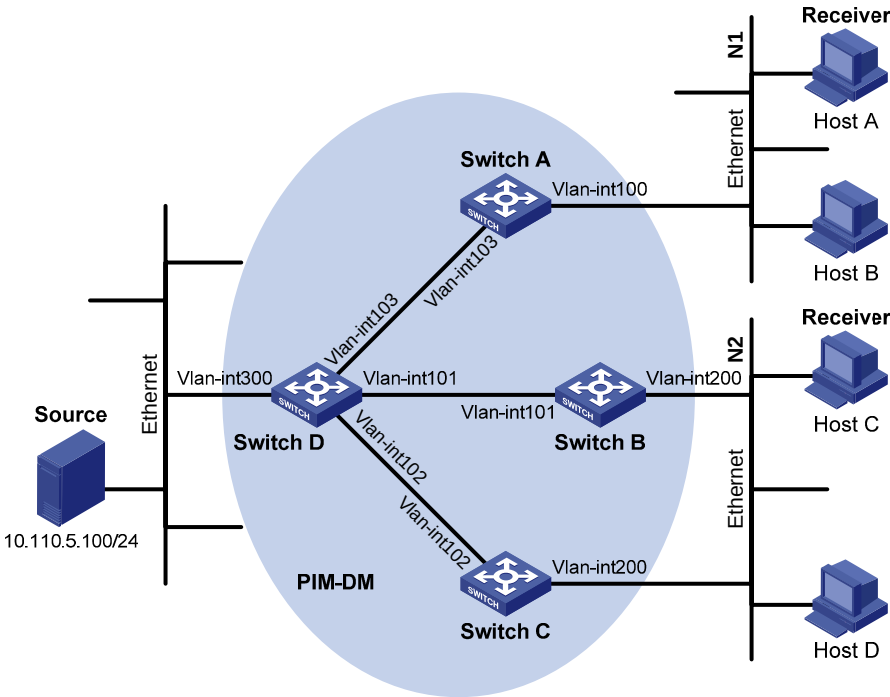
- 一个端口只能属于一个组播 VLAN。
- 在已使能了 IP 组播路由的设备上不允许再配置组播 VLAN。

# 1.4 PIM 典型配置指导

## 1.4.1 PIM-DM 典型配置指导

### 1. 组网图

图1-8 PIM-DM 典型配置组网图



| 设备       | 接口          | IP 地址          | 设备       | 接口          | IP 地址          |
|----------|-------------|----------------|----------|-------------|----------------|
| Switch A | Vlan-int100 | 10.110.1.1/24  | Switch D | Vlan-int300 | 10.110.5.1/24  |
|          | Vlan-int103 | 192.168.1.1/24 |          | Vlan-int103 | 192.168.1.2/24 |
| Switch B | Vlan-int200 | 10.110.2.1/24  |          | Vlan-int101 | 192.168.2.2/24 |
|          | Vlan-int101 | 192.168.2.1/24 |          | Vlan-int102 | 192.168.3.2/24 |
| Switch C | Vlan-int200 | 10.110.2.2/24  |          |             |                |
|          | Vlan-int102 | 192.168.3.1/24 |          |             |                |

### 2. 应用要求

- 接收者通过组播方式接收视频点播信息，不同组织的接收者群体组成末梢网络，每个末梢网络中都存在至少一个接收者，整个 PIM 域采用 DM 方式；
- Host A 和 Host C 为两个末梢网络中的组播信息接收者；Switch D 通过 Vlan-interface300 接口与组播源（Source）所在的网络连接；Switch A 通过 Vlan-interface100 接口连接末梢网络 N1，通过 Vlan-interface103 接口连接 Switch D；Switch B 和 Switch C 通过各自的 Vlan-interface200 接口连接末梢网络 N2，分别通过 Vlan-interface101 和 Vlan-interface102 接口连接 Switch D；
- Switch A 与末梢网络 N1 之间运行 IGMPv2；Switch B 和 Switch C 与末梢网络 N2 之间也运行 IGMPv2。

### 3. 适用产品、版本

表1-8 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本    |
|-------------------|---------------------------------|---------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本 |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本 |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本 |

### 4. 配置过程和解释

#### (1) 配置 IP 地址和单播路由协议

请按照 图 1-8配置各接口的IP地址和子网掩码，具体配置过程略。

配置 PIM-DM 域内的各交换机之间采用 OSPF 协议进行互连,确保 PIM-DM 域内部在网络层互通，并且各交换机之间能够借助单播路由协议实现动态路由更新，具体配置过程略。

#### (2) 使能 IP 组播路由，并在各接口上使能 PIM-DM 和 IGMP

# 在 Switch A 上使能 IP 组播路由，在各接口上使能 PIM-DM，并在 Switch A 连接末梢网络的接口 Vlan-interface100 上使能 IGMPv2。

```
<SwitchA> system-view
[SwitchA] multicast routing-enable
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] igmp enable
[SwitchA-Vlan-interface100] pim dm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 103
[SwitchA-Vlan-interface103] pim dm
[SwitchA-Vlan-interface103] quit
```

Switch B 和 Switch C 的配置与 Switch A 相似，配置过程略。

# 在 Switch D 上使能 IP 组播路由，并在其各接口上使能 PIM-DM。

```
<SwitchD> system-view
[SwitchD] multicast routing-enable
[SwitchD] interface vlan-interface 300
[SwitchD-Vlan-interface300] pim dm
[SwitchD-Vlan-interface300] quit
[SwitchD] interface vlan-interface 103
[SwitchD-Vlan-interface103] pim dm
[SwitchD-Vlan-interface103] quit
[SwitchD] interface vlan-interface 101
[SwitchD-Vlan-interface101] pim dm
[SwitchD-Vlan-interface101] quit
```

```
[SwitchD] interface vlan-interface 102
[SwitchD-Vlan-interface102] pim dm
[SwitchD-Vlan-interface102] quit
```

### (3) 检验配置效果

通过使用 **display pim interface** 命令可以查看交换机接口上 PIM 的配置和运行情况。例如：

# 查看 Switch D 上 PIM 的配置信息。

```
[SwitchD] display pim interface
```

| Interface | NbrCnt | HelloInt | DR-Pri | DR-Address          |
|-----------|--------|----------|--------|---------------------|
| Vlan300   | 0      | 30       | 1      | 10.110.5.1 (local)  |
| Vlan103   | 1      | 30       | 1      | 192.168.1.2 (local) |
| Vlan101   | 1      | 30       | 1      | 192.168.2.2 (local) |
| Vlan102   | 1      | 30       | 1      | 192.168.3.2 (local) |

通过使用 **display pim neighbor** 命令可以查看交换机之间的 PIM 邻居关系。例如：

# 查看 Switch D 上 PIM 的邻居关系信息。

```
[SwitchD] display pim neighbor
```

Total Number of Neighbors = 3

| Neighbor    | Interface | Uptime   | Expires  | Dr-Priority |
|-------------|-----------|----------|----------|-------------|
| 192.168.1.1 | Vlan103   | 00:02:22 | 00:01:27 | 1           |
| 192.168.2.1 | Vlan101   | 00:00:22 | 00:01:29 | 3           |
| 192.168.3.1 | Vlan102   | 00:00:23 | 00:01:31 | 5           |

假如 Host A 需要接收组播组 G（225.1.1.1）的信息，当组播源 S（10.110.5.100/24）向组播组 G 发送组播数据时，通过扩散生成 SPT，SPT 路径中各交换机（Switch A 和 Switch D）上都存在（S，G）表项，Host A 向 Switch A 注册，在 Switch A 上生成（\*，G）表项。通过使用 **display pim routing-table** 命令可以查看交换机的 PIM 路由表信息。例如：

# 查看 Switch A 上的 PIM 路由表信息。

```
[SwitchA] display pim routing-table
```

Total 1 (\*, G) entry; 1 (S, G) entry

```
(*, 225.1.1.1)
 Protocol: pim-dm, Flag: WC
 UpTime: 00:04:25
 Upstream interface: NULL
 Upstream neighbor: NULL
 RPF prime neighbor: NULL
 Downstream interface(s) information:
 Total number of downstreams: 1
 1: Vlan-interface100
 Protocol: igmp, UpTime: 00:04:25, Expires: never
(10.110.5.100, 225.1.1.1)
 Protocol: pim-dm, Flag: ACT
 UpTime: 00:06:14
 Upstream interface: Vlan-interface103,
 Upstream neighbor: 192.168.1.2
 RPF prime neighbor: 192.168.1.2
```

```

Downstream interface(s) information:
 Total number of downstreams: 1
 1: Vlan-interface100
 Protocol: pim-dm, UpTime: 00:04:25, Expires: never

```

Switch B 和 Switch C 上的显示信息与 Switch A 类似。

# 查看 Switch D 上的 PIM 路由表信息。

```

[SwitchD] display pim routing-table
Total 0 (*, G) entry; 1 (S, G) entry

(10.110.5.100, 225.1.1.1)
 Protocol: pim-dm, Flag: LOC ACT
 UpTime: 00:03:27
 Upstream interface: Vlan-interface300
 Upstream neighbor: NULL
 RPF prime neighbor: NULL
 Downstream interface(s) information:
 Total number of downstreams: 3
 1: Vlan-interface103
 Protocol: pim-dm, UpTime: 00:03:27, Expires: never
 2: Vlan-interface101
 Protocol: pim-dm, UpTime: 00:03:27, Expires: never
 3: Vlan-interface102
 Protocol: pim-dm, UpTime: 00:03:27, Expires: never

```

## 5. 完整配置

### (1) SwitchA 配置信息

```

#
multicast routing-enable
#
interface Vlan-interface100
 ip address 10.110.1.1 255.255.255.0
 igmp enable
 pim dm
#
interface Vlan-interface103
 ip address 192.168.1.1 255.255.255.0
 pim dm
#

```

### (2) SwitchB 配置信息

```

#
multicast routing-enable
#
interface Vlan-interface101
 ip address 192.168.2.1 255.255.255.0
 pim dm
#
interface Vlan-interface200

```

```
ip address 10.110.2.1 255.255.255.0
igmp enable
pim dm
#
```

### (3) SwitchC 配置信息

```
#
multicast routing-enable
#
interface Vlan-interface102
ip address 192.168.3.1 255.255.255.0.
pim dm
#
interface Vlan-interface200
ip address 10.110.2.2 255.255.255.0
igmp enable
pim dm
#
```

### (4) SwitchD 配置信息

```
#
multicast routing-enable
#
interface Vlan-interface101
ip address 192.168.2.2 255.255.255.0.
pim dm
#
interface Vlan-interface102
ip address 192.168.3.2 255.255.255.0
pim dm
#
interface Vlan-interface103
ip address 192.168.1.2 255.255.255.0
pim dm
#
interface Vlan-interface300
ip address 10.110.5.1 255.255.255.0
pim dm
#
```

## 6. 配置注意事项

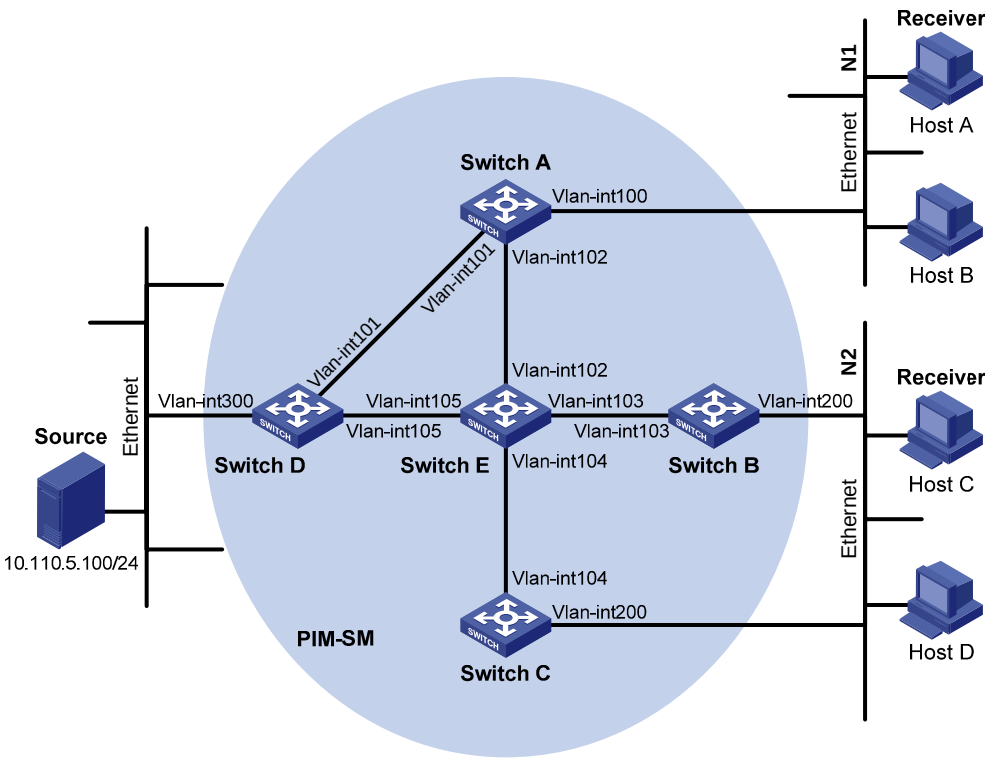
在部署 PIM-DM 域时，建议在非边界交换机的所有接口上启动 PIM-DM。



# 1.4.2 PIM-SM 非管理域配置指导

## 1. 组网图

图1-9 PIM-SM 典型配置组网图



| 设备       | 接口          | IP 地址          | 设备       | 接口          | IP 地址          |
|----------|-------------|----------------|----------|-------------|----------------|
| Switch A | Vlan-int100 | 10.110.1.1/24  | Switch D | Vlan-int300 | 10.110.5.1/24  |
|          | Vlan-int101 | 192.168.1.1/24 |          | Vlan-int101 | 192.168.1.2/24 |
|          | Vlan-int102 | 192.168.9.1/24 |          | Vlan-int105 | 192.168.4.2/24 |
| Switch B | Vlan-int200 | 10.110.2.1/24  | Switch E | Vlan-int104 | 192.168.3.2/24 |
|          | Vlan-int103 | 192.168.2.1/24 |          | Vlan-int103 | 192.168.2.2/24 |
| Switch C | Vlan-int200 | 10.110.2.2/24  |          | Vlan-int102 | 192.168.9.2/24 |
|          | Vlan-int104 | 192.168.3.1/24 |          | Vlan-int105 | 192.168.4.1/24 |

## 2. 应用要求

- 接收者通过组播方式接收视频点播信息，不同组织的接收者群体组成末梢网络，每个末梢网络中都存在至少一个接收者，整个 PIM 域采用 SM 非管理域方式。
- Host A 和 Host C 为两个末梢网络中的组播信息接收者；
- Switch D 通过 Vlan-interface300 接口与组播源（Source）所在网络连接；
- Switch A 通过 Vlan-interface100 接口连接末梢网络 N1，通过 Vlan-interface101 接口和 Vlan-interface102 接口分别连接 Switch D 和 Switch E；
- Switch B 和 Switch C 通过各自的 Vlan-interface200 接口连接末梢网络 N2，分别通过 Vlan-interface103 和 Vlan-interface104 接口连接 Switch E。
- 将 Switch D 的 Vlan-interface105 接口和 Switch E 的 Vlan-interface102 接口都配置为 C-BSR 和 C-RP，其中 Switch E 上 C-BSR 的优先级较高。C-RP 所服务的组播组范围为 225.1.1.0/24，通过改变哈希掩码长度使此范围内的组地址间隔映射到这两个 C-RP 上。
- Switch A 与末梢网络 N1 之间运行 IGMPv2；Switch B 和 Switch C 与末梢网络 N2 之间也运行 IGMPv2。

### 3. 适用产品、版本

表1-9 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本    |
|-------------------|---------------------------------|---------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本 |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本 |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本 |

### 4. 配置过程和解释

#### (1) 配置 IP 地址和单播路由协议

请按照 图 1-9配置各接口的IP地址和子网掩码，具体配置过程略。

配置 PIM-SM 域内的各交换机之间采用 OSPF 协议进行互连,确保 PIM-SM 域内部在网络层互通，并且各交换机之间能够借助单播路由协议实现动态路由更新，具体配置过程略。

#### (2) 使能 IP 组播路由，并在各接口上使能 PIM-SM 和 IGMP

# 在 Switch A 上使能 IP 组播路由，在各接口上使能 PIM-SM，并在 Switch A 连接末梢网络的接口 Vlan-interface100 上使能 IGMPv2。

```
<SwitchA> system-view
[SwitchA] multicast routing-enable
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] igmp enable
[SwitchA-Vlan-interface100] pim sm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim sm
[SwitchA-Vlan-interface101] quit
[SwitchA] interface vlan-interface 102
[SwitchA-Vlan-interface102] pim sm
[SwitchA-Vlan-interface102] quit
```

Switch B 和 Switch C 的配置与 Switch A 相似，Switch D 和 Switch E 除了不需要在相应接口上使能 IGMP 外，其它的配置也与 Switch A 相似，配置过程略。

#### (3) 配置 C-BSR 和 C-RP

# 在 Switch D 上配置 RP 通告的服务范围，以及 C-BSR 和 C-RP 的位置，并指定哈希掩码长度为 32，C-BSR 的优先级为 10。

```
<SwitchD> system-view
[SwitchD] acl number 2005
[SwitchD-acl-basic-2005] rule permit source 225.1.1.0 0.0.0.255
[SwitchD-acl-basic-2005] quit
```

```
[SwitchD] pim
[SwitchD-pim] c-bsr vlan-interface 105 32 10
[SwitchD-pim] c-rp vlan-interface 105 group-policy 2005
[SwitchD-pim] quit
```

# 在 Switch E 上配置 RP 通告的服务范围，以及 C-BSR 和 C-RP 的位置，并指定哈希掩码长度为 32，C-BSR 的优先级为 20。

```
<SwitchE> system-view
[SwitchE] acl number 2005
[SwitchE-acl-basic-2005] rule permit source 225.1.1.0 0.0.0.255
[SwitchE-acl-basic-2005] quit
[SwitchE] pim
[SwitchE-pim] c-bsr vlan-interface 102 32 20
[SwitchE-pim] c-rp vlan-interface 102 group-policy 2005
[SwitchE-pim] quit
```

#### (4) 检验配置效果

通过使用 **display pim interface** 命令可以查看交换机接口上 PIM 的配置和运行情况。例如：

# 查看 Switch A 上 PIM 的配置信息。

```
[SwitchA] display pim interface
```

| Interface | NbrCnt | HelloInt | DR-Pri | DR-Address         |
|-----------|--------|----------|--------|--------------------|
| Vlan100   | 0      | 30       | 1      | 10.110.1.1 (local) |
| Vlan101   | 1      | 30       | 1      | 192.168.1.2        |
| Vlan102   | 1      | 30       | 1      | 192.168.9.2        |

通过使用 **display pim bsr-info** 命令可以查看交换机上 BSR 选举的信息，以及本地配置并生效的 C-RP 信息。例如：

# 查看 Switch A 上的 BSR 信息，以及本地配置并生效的 C-RP 信息。

```
[SwitchA] display pim bsr-info
Elected BSR Address: 192.168.9.2
Priority: 20
Hash mask length: 32
State: Accept Preferred
Scope: Not scoped
Uptime: 01:40:40
Expires: 00:01:42
```

# 查看 Switch D 上的 BSR 信息，以及本地配置并生效的 C-RP 信息。

```
[SwitchD] display pim bsr-info
Elected BSR Address: 192.168.9.2
Priority: 20
Hash mask length: 32
State: Accept Preferred
Scope: Not scoped
Uptime: 00:05:26
Expires: 00:01:45
Candidate BSR Address: 192.168.4.2
Priority: 10
Hash mask length: 32
```

```
State: Candidate
Scope: Not scoped

Candidate RP: 192.168.4.2(Vlan-interface105)
Priority: 0
HoldTime: 150
Advertisement Interval: 60
Next advertisement scheduled at: 00:00:34
```

# 查看 Switch E 上的 BSR 信息，以及本地配置并生效的 C-RP 信息。

```
[SwitchE] display pim bsr-info
Elected BSR Address: 192.168.9.2
Priority: 20
Hash mask length: 32
State: Elected
Scope: Not scoped
Uptime: 00:00:18
Next BSR message scheduled at: 00:01:52
Candidate BSR Address: 192.168.9.2
Priority: 20
Hash mask length: 32
State: Elected
Scope: Not scoped
```

```
Candidate RP: 192.168.9.2(Vlan-interface102)
Priority: 0
HoldTime: 150
Advertisement Interval: 60
Next advertisement scheduled at: 00:00:48
```

通过使用 **display pim rp-info** 命令可以查看交换机上获取的 RP 信息。例如：

# 查看 Switch A 上的 RP 信息。

```
[SwitchA] display pim rp-info
PIM-SM BSR RP information:
Group/MaskLen: 225.1.1.0/24
RP: 192.168.4.2
Priority: 0
HoldTime: 150
Uptime: 00:51:45
Expires: 00:02:22

RP: 192.168.9.2
Priority: 0
HoldTime: 150
Uptime: 00:51:45
Expires: 00:02:22
```

假如 Host A 需要接收组播组 G(225.1.1.0)的信息，由于根据哈希算法得出 G 对应的 RP 为 Switch E，Switch A 和 Switch E 之间会生成 RPT。当组播源 S（10.110.5.100/24）向 RP 发起注册后，

Switch D 和 Switch E 之间会生成 SPT。当 Switch A 收到组播数据后立即执行从 RPT 到 SPT 的切换。RPT 路径中的交换机（Switch A 和 Switch E）上存在（\*, G）表项，而 SPT 路径中的交换机（Switch A 和 Switch D）上存在（S, G）表项，通过使用 **display pim routing-table** 命令可以查看交换机的 PIM 路由表信息。例如：

# 查看 Switch A 上的 PIM 路由表信息。

```
[SwitchA] display pim routing-table
Total 1 (*, G) entry; 1 (S, G) entry

(*, 225.1.1.0)
 RP: 192.168.9.2
 Protocol: pim-sm, Flag: WC
 UpTime: 00:13:46
 Upstream interface: Vlan-interface102,
 Upstream neighbor: 192.168.9.2
 RPF prime neighbor: 192.168.9.2
 Downstream interface(s) information:
 Total number of downstreams: 1
 1: : Vlan-interface100
 Protocol: igmp, UpTime: 00:13:46, Expires:00:03:06
(10.110.5.100, 225.1.1.0)
 RP: 192.168.9.2
 Protocol: pim-sm, Flag: SPT ACT
 UpTime: 00:00:42
 Upstream interface: Vlan-interface101,
 Upstream neighbor: 192.168.1.2
 RPF prime neighbor: 192.168.1.2
 Downstream interface(s) information:
 Total number of downstreams: 1
 1: : Vlan-interface100
 Protocol: pim-sm, UpTime: 00:00:42, Expires:00:03:06
```

Switch B 和 Switch C 上的显示信息与 Switch A 类似。

# 查看 Switch D 上的 PIM 路由表信息。

```
[SwitchD] display pim routing-table
Total 0 (*, G) entry; 1 (S, G) entry

(10.110.5.100, 225.1.1.0)
 RP: 192.168.9.2
 Protocol: pim-sm, Flag: SPT ACT
 UpTime: 00:00:42
 Upstream interface: Vlan-interface300
 Upstream neighbor: NULL
 RPF prime neighbor: NULL
 Downstream interface(s) information:
 Total number of downstreams: 1
 1: : Vlan-interface105
 Protocol: pim-sm, UpTime: 00:00:42, Expires:00:02:06
```

# 查看 Switch E 上的 PIM 路由表信息。

```
[SwitchE] display pim routing-table
Total 1 (*, G) entry; 0 (S, G) entry
```

```
(*, 225.1.1.0)
 RP: 192.168.9.2 (local)
 Protocol: pim-sm, Flag: WC
 UpTime: 00:13:16
 Upstream interface: Register
 Upstream neighbor: 192.168.4.2
 RPF prime neighbor: 192.168.4.2
 Downstream interface(s) information:
 Total number of downstreams: 1
 1: : Vlan-interface102
 Protocol: pim-sm, UpTime: 00:13:16, Expires: 00:03:22
```

## 5. 完整配置

### (1) SwitchA 配置信息

```
#
multicast routing-enable
#
interface Vlan-interface100
 ip address 10.110.1.1 255.255.255.0
 igmp enable
 pim sm
#
interface Vlan-interface101
 ip address 192.168.1.1 255.255.255.0
 pim sm
#
interface Vlan-interface102
 ip address 192.168.9.1 255.255.255.0
 pim sm
#
```

### (2) SwitchB 配置信息

```
#
multicast routing-enable
#
interface Vlan-interface103
 ip address 192.168.2.1 255.255.255.0
 pim sm
#
interface Vlan-interface200
 ip address 10.110.2.1 255.255.255.0
 igmp enable
 pim sm
#
```

### (3) SwitchC 配置信息

```
#
multicast routing-enable
#
interface Vlan-interface104
 ip address 192.168.3.1 255.255.255.0
 pim sm
#
interface Vlan-interface200
 ip address 10.110.2.2 255.255.255.0
 igmp enable
 pim sm
```

### (4) SwitchD 配置信息

```
#
acl number 2005
 rule 0 permit source 225.1.1.0 0.0.0.255
#
multicast routing-enable
#
interface Vlan-interface101
 ip address 192.168.1.2 255.255.255.0
 pim sm
#
interface Vlan-interface105
 ip address 192.168.4.2 255.255.255.0
 pim sm
#
interface Vlan-interface300
 ip address 10.110.5.1 255.255.255.0
 pim sm
#
pim
 c-bsr Vlan-interface105 32 10
 c-rp Vlan-interface105 group-policy 2005
#
```

### (5) SwitchE 配置信息

```
#
acl number 2005
 rule 0 permit source 225.1.1.0 0.0.0.255
#
multicast routing-enable
#
interface Vlan-interface102
 ip address 192.168.9.2 255.255.255.0
 pim sm
#
```

```

interface Vlan-interface103
 ip address 192.168.2.2 255.255.255.0
 pim sm
#
interface Vlan-interface104
 ip address 192.168.3.2 255.255.255.0
 pim sm
#
interface Vlan-interface105
 ip address 192.168.4.1 255.255.255.0
 pim sm
#
pim
c-bsr Vlan-interface102 32 20
c-rp Vlan-interface102 group-policy 2005
#

```

## 6. 配置注意事项

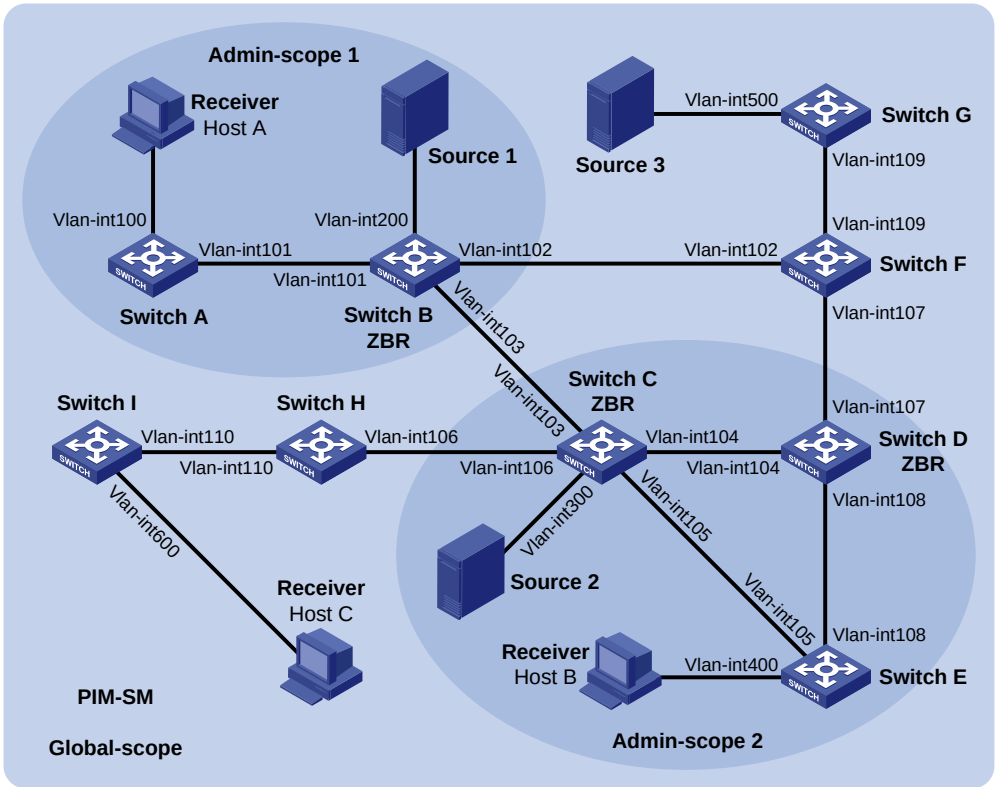
- 在同一台三层交换机上只能配置一个候选 BSR，在另外的接口上配置 BSR 会取代先前的配置。
- 建议候选 BSR 和候选 RP 应配置在骨干网的三层交换机上。
- 配置 RP 时，若没有指定所服务的组播组范围，该 RP 为所有组播组服务。否则，所服务组的范围限定为指定范围的组播组。
- 用户可以配置基本访问控制列表，对相关的组播 IP 地址进行过滤，从而控制静态 RP 所服务的组播组范围。
- 如果使用静态 RP，PIM 域内所有路由器必须采用相同的配置。
- 如果配置的静态 RP 地址是本机某个状态为 UP 的接口地址，本机就作为静态 RP。
- 在 BSR 机制选举产生的 RP 有效时，静态 RP 不起作用。
- 作为静态 RP 的接口不必启动 PIM 协议。
- 合法 BSR 的范围是为了防止网络中合法的 BSR 被恶意取代，除此范围以外的其他 BSR 信息不会被三层交换机接收，保护网络中 BSR 的安全性。
- 合法 C-RP 的范围是为了防止 C-RP 欺骗，可以限定合法 C-RP 的范围，并且限定每个 C-RP 所服务的组范围。



### 1.4.3 PIM-SM 管理域配置指导

#### 1. 组网图

图1-10 PIM-SM 管理域配置组网图



| 设备       | 接口          | IP 地址          | 设备       | 接口          | IP 地址           |
|----------|-------------|----------------|----------|-------------|-----------------|
| Switch A | Vlan-int100 | 192.168.1.1/24 | Switch D | Vlan-int104 | 10.110.4.2/24   |
|          | Vlan-int101 | 10.110.1.1/24  |          | Vlan-int108 | 10.110.7.1/24   |
| Switch B | Vlan-int200 | 192.168.2.1/24 |          | Vlan-int107 | 10.110.8.1/24   |
|          | Vlan-int101 | 10.110.1.2/24  | Switch E | Vlan-int400 | 192.168.4.1/24  |
|          | Vlan-int103 | 10.110.2.1/24  |          | Vlan-int105 | 10.110.5.2/24   |
|          | Vlan-int102 | 10.110.3.1/24  |          | Vlan-int108 | 10.110.7.2/24   |
| Switch C | Vlan-int300 | 192.168.3.1/24 | Switch F | Vlan-int109 | 10.110.9.1/24   |
|          | Vlan-int104 | 10.110.4.1/24  |          | Vlan-int107 | 10.110.8.2/24   |
|          | Vlan-int105 | 10.110.5.1/24  |          | Vlan-int102 | 10.110.3.2/24   |
|          | Vlan-int103 | 10.110.2.2/24  | Switch G | Vlan-int500 | 192.168.5.1/24  |
|          | Vlan-int106 | 10.110.6.1/24  |          | Vlan-int109 | 10.110.9.2/24   |
| Switch H | Vlan-int110 | 10.110.10.1/24 | Source 1 | -           | 192.168.2.10/24 |
|          | Vlan-int106 | 10.110.6.2/24  | Source 2 | -           | 192.168.3.10/24 |
| Switch I | Vlan-int600 | 192.168.6.1/24 | Source 3 | -           | 192.168.5.10/24 |
|          | Vlan-int110 | 10.110.10.2/24 |          |             |                 |

#### 2. 应用要求

- 接收者通过组播方式接收视频点播信息，整个 PIM 域采用 SM 管理域方式，划分为管理域 1、管理域 2 和 Global 域，Switch B、Switch C 和 Switch D 为各管理域的 ZBR。
- Source 1 和 Source 2 分别向组播组 239.1.1.1 发送内容不同的组播信息，Host A 和 Host B 则分别只接收来自 Source 1 和 Source 2 的组播信息；Source 3 向组播组 224.1.1.1 发送组播信息，Host C 为其接收者。
- Switch B 的 Vlan-interface101 接口为管理域 1 的 C-BSR 和 C-RP，服务于 239.0.0.0/8；Switch D 的 Vlan-interface104 接口为管理域 2 的 C-BSR 和 C-RP，服务于 239.0.0.0/8；

Switch F 的 Vlan-interface109 和 Switch H 的 Vlan-interface110 接口均为 Global 域的 C-BSR 和 C-RP，服务于 239.0.0.0/8 以外的所有组播组，但 Switch F 的优先级较高。

- Switch A、Switch E 和 Switch I 分别与各自所连接的接收者之间运行 IGMPv2。

### 3. 适用产品、版本

表1-10 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本    |
|-------------------|---------------------------------|---------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本 |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本 |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本 |

### 4. 配置过程和解释

#### (1) 配置 IP 地址和单播路由协议

请按照 图 1-10 配置各接口的 IP 地址和子网掩码，具体配置过程略。

配置 PIM-SM 域内的各交换机之间采用 OSPF 协议进行互连，确保 PIM-SM 域内部在网络层互通，并且各交换机之间能够借助单播路由协议实现动态路由更新，具体配置过程略。

#### (2) 使能 IP 组播路由和管理域机制，并使能 PIM-SM 和 IGMP

# 在 Switch A 上使能 IP 组播路由和管理域机制，在各接口上使能 PIM-SM，并在其连接有接收者的接口 Vlan-interface100 上使能 IGMP。

```
<SwitchA> system-view
[SwitchA] multicast routing-enable
[SwitchA] pim
[SwitchA-pim] c-bsr admin-scope
[SwitchA-pim] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] igmp enable
[SwitchA-Vlan-interface100] pim sm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim sm
[SwitchA-Vlan-interface101] quit
```

Switch E 和 Switch I 的配置与 Switch A 相似，配置过程略。

# 在 Switch B 上使能 IP 组播路由和管理域机制，并在各接口上使能 PIM-SM。

```
<SwitchB> system-view
[SwitchB] multicast routing-enable
[SwitchB] pim
[SwitchB-pim] c-bsr admin-scope
```

```
[SwitchB-pim] quit
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] pim sm
[SwitchB-Vlan-interface200] quit
[SwitchB] interface vlan-interface 101
[SwitchB-Vlan-interface101] pim sm
[SwitchB-Vlan-interface101] quit
[SwitchB] interface vlan-interface 102
[SwitchB-Vlan-interface102] pim sm
[SwitchB-Vlan-interface102] quit
[SwitchB] interface vlan-interface 103
[SwitchB-Vlan-interface103] pim sm
[SwitchB-Vlan-interface103] quit
```

Switch C、Switch D、Switch F、Switch G 和 Switch H 的配置与 Switch B 相似，配置过程略。

### (3) 配置管理域边界

# 在 Switch B 上将接口 Vlan-interface102 和 Vlan-interface103 配置为管理域 1 的边界。

```
[SwitchB] interface vlan-interface 102
[SwitchB-Vlan-interface102] multicast boundary 239.0.0.0 8
[SwitchB-Vlan-interface102] quit
[SwitchB] interface vlan-interface 103
[SwitchB-Vlan-interface103] multicast boundary 239.0.0.0 8
[SwitchB-Vlan-interface103] quit
```

# 在 Switch C 上将接口 Vlan-interface103 和 Vlan-interface106 配置为管理域 2 的边界。

```
<SwitchC> system-view
[SwitchC] interface vlan-interface 103
[SwitchC-Vlan-interface103] multicast boundary 239.0.0.0 8
[SwitchC-Vlan-interface103] quit
[SwitchC] interface vlan-interface 106
[SwitchC-Vlan-interface106] multicast boundary 239.0.0.0 8
[SwitchC-Vlan-interface106] quit
```

# 在 Switch D 上将接口 Vlan-interface107 配置为管理域 2 的边界。

```
<SwitchD> system-view
[SwitchD] interface vlan-interface 107
[SwitchD-Vlan-interface107] multicast boundary 239.0.0.0 8
[SwitchD-Vlan-interface107] quit
```

### (4) 配置 C-BSR 和 C-RP

# 在 Switch B 上配置 RP 通告的服务范围，并将接口 Vlan-interface101 配置为管理域 1 的 C-BSR 和 C-RP。

```
[SwitchB] acl number 2001
[SwitchB-acl-basic-2001] rule permit source 239.0.0.0 0.255.255.255
[SwitchB-acl-basic-2001] quit
[SwitchB] pim
[SwitchB-pim] c-bsr group 239.0.0.0 8
[SwitchB-pim] c-bsr vlan-interface 101
[SwitchB-pim] c-rp vlan-interface 101 group-policy 2001
```

```
[SwitchB-pim] quit
```

# 在 Switch D 上配置 RP 通告的服务范围,并将接口 Vlan-interface104 配置为管理域 2 的 C-BSR 和 C-RP。

```
[SwitchD] acl number 2001
```

```
[SwitchD-acl-basic-2001] rule permit source 239.0.0.0 0.255.255.255
```

```
[SwitchD-acl-basic-2001] quit
```

```
[SwitchD] pim
```

```
[SwitchD-pim] c-bsr group 239.0.0.0 8
```

```
[SwitchD-pim] c-bsr vlan-interface 104
```

```
[SwitchD-pim] c-rp vlan-interface 104 group-policy 2001
```

```
[SwitchD-pim] quit
```

# 在 Switch F 上将接口 Vlan-interface109 配置为 Global 域的 C-BSR 和 C-RP。

```
<SwitchF> system-view
```

```
[SwitchF] pim
```

```
[SwitchF-pim] c-bsr global
```

```
[SwitchF-pim] c-bsr vlan-interface 109
```

```
[SwitchF-pim] c-rp vlan-interface 109
```

```
[SwitchF-pim] quit
```

#### (5) 检验配置效果

通过使用 **display pim bsr-info** 命令可以查看交换机上 BSR 选举的信息,以及本地配置并生效的 C-RP 信息。例如:

# 查看 Switch B 上的 BSR 信息,以及本地配置并生效的 C-RP 信息。

```
[SwitchB] display pim bsr-info
```

```
Elected BSR Address: 10.110.9.1
```

```
Priority: 0
```

```
Hash mask length: 30
```

```
State: Accept Preferred
```

```
Scope: Global
```

```
Uptime: 00:01:45
```

```
Expires: 00:01:25
```

```
Elected BSR Address: 10.110.1.2
```

```
Priority: 0
```

```
Hash mask length: 30
```

```
State: Elected
```

```
Scope: 239.0.0.0/8
```

```
Uptime: 00:04:54
```

```
Next BSR message scheduled at: 00:00:06
```

```
Candidate BSR Address: 10.110.1.2
```

```
Priority: 0
```

```
Hash mask length: 30
```

```
State: Elected
```

```
Scope: 239.0.0.0/8
```

```
Candidate RP: 10.110.1.2(Vlan-interface101)
```

```
Priority: 0
```

```
HoldTime: 150
```

```
Advertisement Interval: 60
Next advertisement scheduled at: 00:00:15

查看 Switch D 上的 BSR 信息，以及本地配置并生效的 C-RP 信息。
```

```
[SwitchD] display pim bsr-info
Elected BSR Address: 10.110.9.1
Priority: 0
Hash mask length: 30
State: Accept Preferred
Scope: Global
Uptime: 00:01:45
Expires: 00:01:25
Elected BSR Address: 10.110.4.2
Priority: 0
Hash mask length: 30
State: Elected
Scope: 239.0.0.0/8
Uptime: 00:03:48
Next BSR message scheduled at: 00:01:12
Candidate BSR Address: 10.110.4.2
Priority: 0
Hash mask length: 30
State: Elected
Scope: 239.0.0.0/8

Candidate RP: 10.110.4.2(Vlan-interface104)
Priority: 0
HoldTime: 150
Advertisement Interval: 60
Next advertisement scheduled at: 00:00:10
```

# 查看 Switch F 上的 BSR 信息，以及本地配置并生效的 C-RP 信息。

```
[SwitchF] display pim bsr-info
Elected BSR Address: 10.110.9.1
Priority: 0
Hash mask length: 30
State: Elected
Scope: Global
Uptime: 00:11:11
Next BSR message scheduled at: 00:00:49
Candidate BSR Address: 10.110.9.1
Priority: 0
Hash mask length: 30
State: Elected
Scope: Global

Candidate RP: 10.110.9.1(Vlan-interface109)
Priority: 0
HoldTime: 150
```

```
Advertisement Interval: 60
```

```
Next advertisement scheduled at: 00:00:55
```

通过使用 **display pim rp-info** 命令可以查看交换机上获取的 RP 信息。例如：

# 查看 Switch B 上的 RP 信息。

```
[SwitchB] display pim rp-info
```

```
PIM-SM BSR RP information:
```

```
Group/MaskLen: 224.0.0.0/4
```

```
RP: 10.110.9.1
```

```
Priority: 0
```

```
HoldTime: 150
```

```
Uptime: 00:03:39
```

```
Expires: 00:01:51
```

```
Group/MaskLen: 239.0.0.0/8
```

```
RP: 10.110.1.2 (local)
```

```
Priority: 0
```

```
HoldTime: 150
```

```
Uptime: 00:07:44
```

```
Expires: 00:01:51
```

# 查看 Switch D 上的 RP 信息。

```
[SwitchD] display pim rp-info
```

```
PIM-SM BSR RP information:
```

```
Group/MaskLen: 224.0.0.0/4
```

```
RP: 10.110.9.1
```

```
Priority: 0
```

```
HoldTime: 150
```

```
Uptime: 00:03:42
```

```
Expires: 00:01:48
```

```
Group/MaskLen: 239.0.0.0/8
```

```
RP: 10.110.4.2 (local)
```

```
Priority: 0
```

```
HoldTime: 150
```

```
Uptime: 00:06:54
```

```
Expires: 00:02:41
```

# 查看 Switch F 上的 RP 信息。

```
[SwitchF] display pim rp-info
```

```
PIM-SM BSR RP information:
```

```
Group/MaskLen: 224.0.0.0/4
```

```
RP: 10.110.9.1 (local)
```

```
Priority: 0
```

```
HoldTime: 150
```

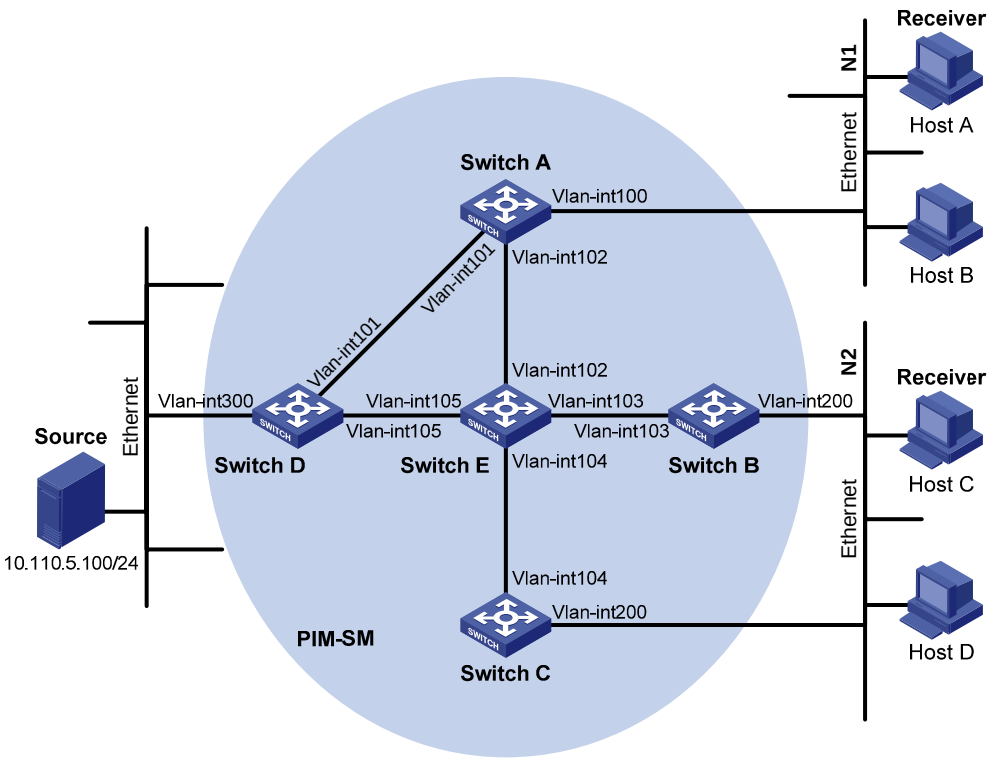
```
Uptime: 00:00:32
```

```
Expires: 00:01:58
```

## 1.4.4 PIM-SSM 典型配置指导

### 1. 组网图

图1-11 PIM-SSM 典型配置组网图



| 设备       | 接口          | IP 地址          | 设备       | 接口          | IP 地址          |
|----------|-------------|----------------|----------|-------------|----------------|
| Switch A | Vlan-int100 | 10.110.1.1/24  | Switch D | Vlan-int300 | 10.110.5.1/24  |
|          | Vlan-int101 | 192.168.1.1/24 |          | Vlan-int101 | 192.168.1.2/24 |
|          | Vlan-int102 | 192.168.9.1/24 |          | Vlan-int105 | 192.168.4.2/24 |
| Switch B | Vlan-int200 | 10.110.2.1/24  | Switch E | Vlan-int104 | 192.168.3.2/24 |
|          | Vlan-int103 | 192.168.2.1/24 |          | Vlan-int103 | 192.168.2.2/24 |
| Switch C | Vlan-int200 | 10.110.2.2/24  |          | Vlan-int102 | 192.168.9.2/24 |
|          | Vlan-int104 | 192.168.3.1/24 |          | Vlan-int105 | 192.168.4.1/24 |

### 2. 应用要求

- 接收者通过组播方式接收视频点播信息，不同组织的接收者群体组成末梢网络，每个末梢网络中都存在至少一个接收者，整个 PIM 域采用 SSM 方式；
- Host A 和 Host C 为两个末梢网络中的组播信息接收者；
- Switch D 通过 Vlan-interface300 接口与组播源（Source）所在网络连接；
- Switch A 通过 Vlan-interface100 接口连接末梢网络 N1，通过 Vlan-interface101 接口和 Vlan-interface102 接口分别连接 Switch D 和 Switch E；
- Switch B 和 Switch C 通过各自的 Vlan-interface200 接口连接末梢网络 N2，分别通过 Vlan-interface103 和 Vlan-interface104 接口连接 Switch E；
- SSM 组播组的范围是 232.1.1.0/24；
- Switch A 与末梢网络 N1 之间运行 IGMPv3；Switch B 和 Switch C 与末梢网络 N2 之间也运行 IGMPv3。

### 3. 适用产品、版本

表1-11 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本    |
|-------------------|---------------------------------|---------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本 |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本 |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本 |

### 4. 配置过程和解释

#### (1) 配置 IP 地址和单播路由协议

请按照 图 1-11 配置各接口的 IP 地址和子网掩码，具体配置过程略。

配置 PIM-SM 域内的各交换机之间采用 OSPF 协议进行互连，确保 PIM-SM 域内部网络层互通，并且各交换机之间能够借助单播路由协议实现动态路由更新，具体配置过程略。

#### (2) 使能 IP 组播路由，并在各接口上使能 PIM-SM 和 IGMP

# 在 Switch A 上使能 IP 组播路由，在各接口上使能 PIM-SM，并在 Switch A 连接末梢网络的接口 Vlan-interface100 上使能 IGMPv3。

```
<SwitchA> system-view
[SwitchA] multicast routing-enable
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] igmp enable
[SwitchA-Vlan-interface100] igmp version 3
[SwitchA-Vlan-interface100] pim sm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim sm
[SwitchA-Vlan-interface101] quit
[SwitchA] interface vlan-interface 102
[SwitchA-Vlan-interface102] pim sm
[SwitchA-Vlan-interface102] quit
```

Switch B 和 Switch C 的配置与 Switch A 相似，Switch D 和 Switch E 除了不需要在相应接口上使能 IGMP 外，其它的配置也与 Switch A 相似，配置过程略。

#### (3) 配置 SSM 组播组的地址范围

# 在 Switch A 上配置 SSM 组播组地址范围为 232.1.1.0/24。

```
[SwitchA] acl number 2000
[SwitchA-acl-basic-2000] rule permit source 232.1.1.0 0.0.0.255
[SwitchA-acl-basic-2000] quit
[SwitchA] pim
[SwitchA-pim] ssm-policy 2000
```



```
[SwitchA-pim] quit
```

Switch B、Switch C、Switch D 和 Switch E 的配置与 Switch A 相似，配置过程略。

#### (4) 检验配置效果

通过使用 **display pim interface** 命令可以查看交换机接口上 PIM 的配置和运行情况。例如：

# 查看 Switch A 上 PIM 的配置信息。

```
[SwitchA] display pim interface
```

| Interface | NbrCnt | HelloInt | DR-Pri | DR-Address         |
|-----------|--------|----------|--------|--------------------|
| Vlan100   | 0      | 30       | 1      | 10.110.1.1 (local) |
| Vlan101   | 1      | 30       | 1      | 192.168.1.2        |
| Vlan102   | 1      | 30       | 1      | 192.168.9.2        |

假如 Host A 需要接收指定组播源 S (10.110.5.100/24) 发往组播组 G (232.1.1.1) 的信息，Switch A 会向组播源方向构造 SPT，SPT 路径中的交换机 (Switch A 和 Switch D) 上生成 (S, G) 表项，而 SPT 路径之外的交换机 (Switch E) 上没有组播路由项，通过使用 **display pim routing-table** 命令可以查看交换机的 PIM 路由表信息。例如：

# 查看 Switch A 上的 PIM 路由表信息。

```
[SwitchA] display pim routing-table
```

```
Total 0 (*, G) entry; 1 (S, G) entry
```

```
(10.110.5.100, 232.1.1.1)
```

```
Protocol: pim-ssm, Flag:
```

```
UpTime: 00:13:25
```

```
Upstream interface: Vlan-interface101
```

```
Upstream neighbor: 192.168.1.2
```

```
RPF prime neighbor: 192.168.1.2
```

```
Downstream interface(s) information:
```

```
Total number of downstreams: 1
```

```
1: : Vlan-interface100
```

```
Protocol: igmp, UpTime: 00:13:25, Expires: -
```

Switch B 和 Switch C 上的显示信息与 Switch A 类似。

# 查看 Switch D 上的 PIM 路由表信息。

```
[SwitchD] display pim routing-table
```

```
Total 0 (*, G) entry; 1 (S, G) entry
```

```
(10.110.5.100, 232.1.1.1)
```

```
Protocol: pim-ssm, Flag:LOC
```

```
UpTime: 00:12:05
```

```
Upstream interface: Vlan-interface300
```

```
Upstream neighbor: NULL
```

```
RPF prime neighbor: NULL
```

```
Downstream interface(s) information:
```

```
Total number of downstreams: 1
```

```
1: : Vlan-interface105
```

```
Protocol: pim-ssm, UpTime: 00:12:05, Expires: 00:03:25
```

## 5. 完整配置

### (1) SwitchA 配置信息

```
#
multicast routing-enable
#
acl number 2000
 rule 0 permit source 232.1.1.0 0.0.0.255
#
interface Vlan-interface100
 ip address 10.110.1.1 255.255.255.0
 igmp enable
 igmp version 3
 pim sm
#
interface Vlan-interface101
 ip address 192.168.1.1 255.255.255.0
 pim sm
#
interface Vlan-interface102
 ip address 192.168.9.1 255.255.255.0
 pim sm
#
pim
 ssm-policy 2000
#
```

### (2) SwitchB 配置信息

```
#
multicast routing-enable
#
acl number 2000
 rule 0 permit source 232.1.1.0 0.0.0.255
#
interface Vlan-interface103
 ip address 192.168.2.1 255.255.255.0
 pim sm
#
interface Vlan-interface200
 ip address 10.110.2.1 255.255.255.0
 igmp enable
 igmp version 3
 pim sm
#
pim
 ssm-policy 2000
#
```

### (3) SwitchC 配置信息

```
#
```

```
multicast routing-enable
#
acl number 2000
 rule 0 permit source 232.1.1.0 0.0.0.255
#
interface Vlan-interface104
 ip address 192.168.3.1 255.255.255.0
 pim sm
#
interface Vlan-interface200
 ip address 10.110.2.2 255.255.255.0
 igmp enable
 igmp version 3
 pim sm
#
pim
 ssm-policy 2000
#
```

#### (4) SwitchD 配置信息

```
#
multicast routing-enable
#
acl number 2000
 rule 0 permit source 232.1.1.0 0.0.0.255
#
interface Vlan-interface101
 ip address 192.168.1.2 255.255.255.0
 pim sm
#
interface Vlan-interface105
 ip address 192.168.4.2 255.255.255.0
 pim sm
#
interface Vlan-interface300
 ip address 10.110.5.1 255.255.255.0
 pim sm
#
pim
 ssm-policy 2000
#
```

#### (5) SwitchE 配置信息

```
#
multicast routing-enable
#
acl number 2000
 rule 0 permit source 232.1.1.0 0.0.0.255
#
interface Vlan-interface102
```

```
ip address 192.168.9.2 255.255.255.0
pim sm
#
interface Vlan-interface103
ip address 192.168.2.2 255.255.255.0
pim sm
#
interface Vlan-interface104
ip address 192.168.3.2 255.255.255.0
pim sm
#
interface Vlan-interface105
ip address 192.168.4.1 255.255.255.0
pim sm
#
pim
ssm-policy 2000
#
```

## 6. 配置注意事项

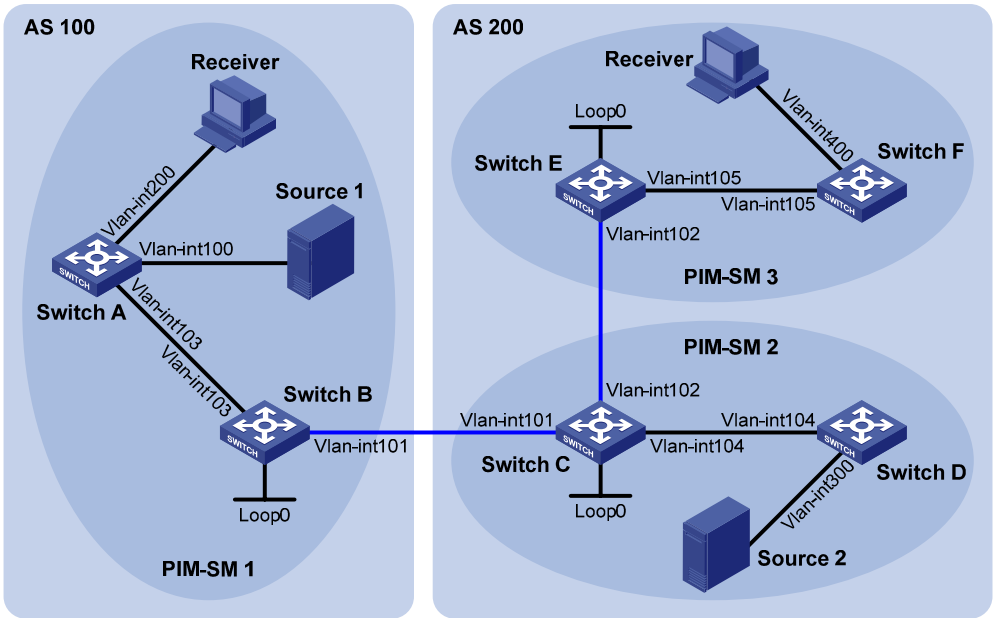
- PIM-SSM 模型需要 IGMPv3 的支持，因此应确保连接接收者的 PIM 路由器上使能了 IGMPv3。
- 应确保域内所有路由器上配置的 SSM 组播组地址范围都一致，否则组播信息将无法通过 SSM 模型进行传输。
- 如果某组播组属于 SSM 组播组范围，但该组成员使用 IGMPv1 或 IGMPv2 发送加入报文，则设备不会触发（\*, G）加入报文。

# 1.5 MSDP 典型配置指导

## 1.5.1 借助 BGP 路由的 AS 间组播配置指导

### 1. 组网图

图1-12 借助 BGP 路由的 AS 间组播配置组网图



| 设备       | 接口          | IP 地址          | 设备       | 接口          | IP 地址           |
|----------|-------------|----------------|----------|-------------|-----------------|
| Switch A | Vlan-int103 | 10.110.1.2/24  | Switch D | Vlan-int104 | 10.110.4.2/24   |
|          | Vlan-int100 | 10.110.2.1/24  |          | Vlan-int300 | 10.110.5.1/24   |
|          | Vlan-int200 | 10.110.3.1/24  | Switch E | Vlan-int105 | 10.110.6.1/24   |
| Switch B | Vlan-int103 | 10.110.1.1/24  |          | Vlan-int102 | 192.168.3.2/24  |
|          | Vlan-int101 | 192.168.1.1/24 |          | Loop0       | 3.3.3.3/32      |
|          | Loop0       | 1.1.1.1/32     | Switch F | Vlan-int105 | 10.110.6.2/24   |
| Switch C | Vlan-int104 | 10.110.4.1/24  |          | Vlan-int400 | 10.110.7.1/24   |
|          | Vlan-int102 | 192.168.3.1/24 | Source 1 | -           | 10.110.2.100/24 |
|          | Vlan-int101 | 192.168.1.2/24 | Source 2 | -           | 10.110.5.100/24 |
|          | Loop0       | 2.2.2.2/32     |          |             |                 |

### 2. 应用要求

- 网络中存在两个自治系统：PIM-SM 1 属于 AS 100，PIM-SM 2 和 PIM-SM 3 属于 AS 200。各 AS 内部采用 OSPF 进行互联，AS 之间采用 BGP 交换路由信息；
- 每个 PIM-SM 域分别拥有 0 或 1 个组播源和接收者，域内运行 OSPF 协议以提供单播路由；
- 将 Switch B、Switch C 和 Switch E 各自的 Loopback0 接口分别配置为各自 PIM-SM 域的 C-BSR 和 C-RP；
- 在 Switch B 与 Switch C 之间通过 EBGP 建立 MSDP 对等体关系，在 Switch C 与 Switch E 之间通过 IBGP 建立 MSDP 对等体关系。

### 3. 适用产品、版本

表1-12 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本    |
|-------------------|---------------------------------|---------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本 |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本 |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本 |

### 4. 配置过程和解释

#### (1) 配置各交换机接口的 IP 地址和单播路由协议

请按照 图 1-12 配置各接口的 IP 地址和子网掩码，具体配置过程略。

配置 AS 内的各交换机之间采用 OSPF 协议进行互连，确保各 AS 内部在网络层互通，并且各交换机之间能够借助单播路由协议实现动态路由更新，具体配置过程略。

#### (2) 使能 IP 组播路由，使能 PIM-SM 和 IGMP，并配置 BSR 的服务边界

# 在 Switch A 上使能 IP 组播路由，在各接口上使能 PIM-SM，并在主机侧接口 Vlan-interface200 上使能 IGMP。

```
<SwitchA> system-view
[SwitchA] multicast routing-enable
[SwitchA] interface vlan-interface 103
[SwitchA-Vlan-interface103] pim sm
[SwitchA-Vlan-interface103] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] pim sm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 200
[SwitchA-Vlan-interface200] igmp enable
[SwitchA-Vlan-interface200] pim sm
[SwitchA-Vlan-interface200] quit
```

Switch B、Switch C、Switch D、Switch E 和 Switch F 上的配置与 Switch A 相似，配置过程略。

# 在 Switch B 上配置 BSR 的服务边界。

```
[SwitchB] interface vlan-interface 101
[SwitchB-Vlan-interface101] pim bsr-boundary
[SwitchB-Vlan-interface101] quit
```

Switch C 和 Switch E 上的配置与 Switch B 相似，配置过程略。

#### (3) 配置 C-BSR 和 C-RP 的位置

# 在 Switch B 上将 Loopback0 接口配置为 C-BSR 和 C-RP。

```
[SwitchB] pim
```

```
[SwitchB-pim] c-bsr loopback 0
[SwitchB-pim] c-rp loopback 0
[SwitchB-pim] quit
```

Switch C 和 Switch E 上的配置与 Switch B 相似，配置过程略。

#### (4) 配置 BGP 协议，将 BGP 与 OSPF 互相引入

# 在 Switch B 上配置 EBGP，并引入 OSPF 路由。

```
[SwitchB] bgp 100
[SwitchB-bgp] router-id 1.1.1.1
[SwitchB-bgp] peer 192.168.1.2 as-number 200
[SwitchB-bgp] import-route ospf 1
[SwitchB-bgp] quit
```

# 在 Switch C 上配置 IBGP 和 EBGP，并引入 OSPF 路由。

```
[SwitchC] bgp 200
[SwitchC-bgp] router-id 2.2.2.2
[SwitchC-bgp] peer 192.168.1.1 as-number 100
[SwitchC-bgp] peer 192.168.3.2 as-number 200
[SwitchC-bgp] import-route ospf 1
[SwitchC-bgp] quit
```

# 在 Switch E 上配置 IBGP，并引入 OSPF 路由。

```
[SwitchE] bgp 200
[SwitchE-bgp] router-id 3.3.3.3
[SwitchE-bgp] peer 192.168.3.1 as-number 200
[SwitchE-bgp] import-route ospf 1
[SwitchE-bgp] quit
```

# 在 Switch B 的 OSPF 中引入 BGP。

```
[SwitchB] ospf 1
[SwitchB-ospf-1] import-route bgp
[SwitchB-ospf-1] quit
```

Switch C 和 Switch E 上的配置与 Switch B 相似，配置过程略。

#### (5) 配置 MSDP 对等体

# 在 Switch B 上配置 MSDP 对等体。

```
[SwitchB] msdp
[SwitchB-msdp] peer 192.168.1.2 connect-interface vlan-interface 101
[SwitchB-msdp] quit
```

# 在 Switch C 上配置 MSDP 对等体。

```
[SwitchC] msdp
[SwitchC-msdp] peer 192.168.1.1 connect-interface vlan-interface 101
[SwitchC-msdp] peer 192.168.3.2 connect-interface vlan-interface 102
[SwitchC-msdp] quit
```

# 在 Switch E 上配置 MSDP 对等体。

```
[SwitchE] msdp
[SwitchE-msdp] peer 192.168.3.1 connect-interface vlan-interface 102
```

```
[SwitchE-msdp] quit
```

## (6) 检验配置效果

通过使用 **display bgp peer** 命令可以查看交换机之间 BGP 对等体的关系。例如：

# 查看 Switch B 上 BGP 对等体关系的信息。

```
[SwitchB] display bgp peer
```

```
BGP local router ID : 1.1.1.1
Local AS number : 100
Total number of peers : 1 Peers in established state : 1

Peer V AS MsgRcvd MsgSent OutQ PrefRcv Up/Down State
192.168.1.2 4 200 24 21 0 6 00:13:09 Established
```

# 查看 Switch C 上 BGP 对等体关系的信息。

```
[SwitchC] display bgp peer
```

```
BGP local router ID : 2.2.2.2
Local AS number : 200
Total number of peers : 2 Peers in established state : 2

Peer V AS MsgRcvd MsgSent OutQ PrefRcv Up/Down State
192.168.1.1 4 100 18 16 0 1 00:12:04 Established
192.168.3.2 4 200 21 20 0 6 00:12:05 Established
```

# 查看 Switch E 上 BGP 对等体关系的信息。

```
[SwitchE] display bgp peer
```

```
BGP local router ID : 3.3.3.3
Local AS number : 200
Total number of peers : 1 Peers in established state : 1

Peer V AS MsgRcvd MsgSent OutQ PrefRcv Up/Down State
192.168.3.1 4 200 16 14 0 1 00:10:58 Established
```

通过使用 **display bgp routing-table** 命令可以查看交换机上的 BGP 路由表。例如：

# 查看 Switch C 上 BGP 路由表的信息。

```
[SwitchC] display bgp routing-table
```

```
Total Number of Routes: 13

BGP Local router ID is 2.2.2.2
Status codes: * - valid, > - best, d - damped,
 h - history, i - internal, s - suppressed, S - Stale
Origin : i - IGP, e - EGP, ? - incomplete

Network NextHop MED LocPrf PrefVal Path/Ogn
```



```
*> 1.1.1.1/32 192.168.1.1 0 0 100?
*>i 2.2.2.2/32 192.168.3.2 0 100 0 ?
*> 3.3.3.3/32 0.0.0.0 0 0 ?
*> 192.168.1.0 0.0.0.0 0 0 ?
* 192.168.1.1 0 0 100?
*> 192.168.1.1/32 0.0.0.0 0 0 ?
*> 192.168.1.2/32 0.0.0.0 0 0 ?
* 192.168.1.1 0 0 100?
*> 192.168.3.0 0.0.0.0 0 0 ?
* i 192.168.3.2 0 100 0 ?
*> 192.168.3.1/32 0.0.0.0 0 0 ?
*> 192.168.3.2/32 0.0.0.0 0 0 ?
* i 192.168.3.2 0 100 0 ?
```

当 PIM-SM 1 和 PIM-SM 2 域内的组播源 Source 1 和 Source 2 发送组播信息时，PIM-SM 1 和 PIM-SM 3 域内的接收者（Receiver）能收到该组播信息。通过使用 **display msdp brief** 命令可以查看交换机之间 MSDP 对等体建立情况。例如：

# 查看 Switch B 上 MSDP 对等体建立情况的简要信息。

```
[SwitchB] display msdp brief
```

```
MSDP Peer Brief Information
```

| Configured | Up | Listen | Connect | Shutdown | Down |
|------------|----|--------|---------|----------|------|
| 1          | 1  | 0      | 0       | 0        | 0    |

| Peer's Address | State | Up/Down time | AS  | SA Count | Reset Count |
|----------------|-------|--------------|-----|----------|-------------|
| 192.168.1.2    | Up    | 00:12:27     | 200 | 13       | 0           |

# 查看 Switch C 上 MSDP 对等体建立情况的简要信息。

```
[SwitchC] display msdp brief
```

```
MSDP Peer Brief Information
```

| Configured | Up | Listen | Connect | Shutdown | Down |
|------------|----|--------|---------|----------|------|
| 2          | 2  | 0      | 0       | 0        | 0    |

| Peer's Address | State | Up/Down time | AS  | SA Count | Reset Count |
|----------------|-------|--------------|-----|----------|-------------|
| 192.168.3.2    | Up    | 00:15:32     | 200 | 8        | 0           |
| 192.168.1.1    | Up    | 00:06:39     | 100 | 13       | 0           |

# 查看 Switch E 上 MSDP 对等体建立情况的简要信息。

```
[SwitchE] display msdp brief
```

```
MSDP Peer Brief Information
```

| Configured | Up | Listen | Connect | Shutdown | Down |
|------------|----|--------|---------|----------|------|
| 1          | 1  | 0      | 0       | 0        | 0    |

| Peer's Address | State | Up/Down time | AS  | SA Count | Reset Count |
|----------------|-------|--------------|-----|----------|-------------|
| 192.168.3.1    | Up    | 01:07:08     | 200 | 8        | 0           |

# 查看 Switch B 上 MSDP 对等体的详细信息。

```
[SwitchB] display msdp peer-status
```

```
MSDP Peer 192.168.1.2, AS 200
```

```

Description:
Information about connection status:
 State: Up
 Up/down time: 00:15:47
 Resets: 0
 Connection interface: Vlan-interface101 (192.168.1.1)
 Number of sent/received messages: 16/16
 Number of discarded output messages: 0
 Elapsed time since last connection or counters clear: 00:17:51
Information about (Source, Group)-based SA filtering policy:
 Import policy: none
 Export policy: none
Information about SA-Requests:
 Policy to accept SA-Request messages: none
 Sending SA-Requests status: disable
 Minimum TTL to forward SA with encapsulated data: 0
 SAs learned from this peer: 0, SA-cache maximum for the peer: none
 Input queue size: 0, Output queue size: 0
Counters for MSDP message:
 Count of RPF check failure: 0
 Incoming/outgoing SA messages: 0/0
 Incoming/outgoing SA requests: 0/0
 Incoming/outgoing SA responses: 0/0
 Incoming/outgoing data packets: 0/0

```

## 5. 完整配置

### (1) SwitchA 配置信息

```

#
multicast routing-enable
#
interface Vlan-interface100
 ip address 10.110.2.1 255.255.255.0
 pim sm
#
interface Vlan-interface103
 ip address 10.110.1.2 255.255.255.0
 pim sm
#
interface Vlan-interface200
 ip address 10.110.3.1 255.255.255.0
 igmp enable
 pim sm
#
ospf 1
 area 0.0.0.0
 network 10.110.1.0 0.0.0.255
 network 10.110.2.0 0.0.0.255
 network 10.110.3.0 0.0.0.255

```

```
#
```

## (2) SwitchB 配置信息

```
#
```

```
multicast routing-enable
```

```
#
```

```
interface LoopBack0
```

```
ip address 1.1.1.1 255.255.255.255
```

```
pim sm
```

```
#
```

```
interface Vlan-interface101
```

```
ip address 192.168.1.1 255.255.255.0
```

```
pim bsr-boundary
```

```
pim sm
```

```
#
```

```
interface Vlan-interface103
```

```
ip address 10.110.1.1 255.255.255.0
```

```
pim sm
```

```
#
```

```
bgp 100
```

```
router-id 1.1.1.1
```

```
import-route ospf 1
```

```
undo synchronization
```

```
peer 192.168.1.2 as-number 200
```

```
#
```

```
ospf 1
```

```
import-route bgp
```

```
area 0.0.0.0
```

```
network 192.168.1.0 0.0.0.255
```

```
network 10.110.1.0 0.0.0.255
```

```
network 1.1.1.1 0.0.0.0
```

```
#
```

```
pim
```

```
c-bsr LoopBack0
```

```
c-rp LoopBack0
```

```
#
```

```
msdp
```

```
peer 192.168.1.2 connect-interface vlan-interface 101
```

```
#
```

## (3) SwitchC 配置信息

```
#
```

```
multicast routing-enable
```

```
#
```

```
interface LoopBack0
```

```
ip address 2.2.2.2 255.255.255.255
```

```
pim sm
```

```
#
```

```
interface Vlan-interface101
```

```
ip address 192.168.1.2 255.255.255.0
```

```

pim bsr-boundary

pim sm
#
interface Vlan-interface102
ip address 192.168.3.1 255.255.255.0
pim sm
#
interface Vlan-interface104
ip address 10.110.4.1 255.255.255.0
pim sm
#
bgp 100
router-id 2.2.2.2
import-route ospf 1
undo synchronization
peer 192.168.1.1 as-number 100
peer 192.168.3.2 as-number 200
#
ospf 1
import-route bgp
area 0.0.0.0
network 192.168.1.0 0.0.0.255
network 192.168.3.0 0.0.0.255
network 10.110.4.1 0.0.0.255
network 2.2.2.2 0.0.0.0
#
pim
c-bsr LoopBack0
c-rp LoopBack0
#
msdp
peer 192.168.1.1 connect-interface vlan-interface 101
peer 192.168.3.2 connect-interface vlan-interface 102
#

```

#### (4) SwitchD 配置信息

```

#
multicast routing-enable
#
interface Vlan-interface104
ip address 10.110.4.2 255.255.255.0
pim sm
#
interface Vlan-interface300
ip address 10.110.5.1 255.255.255.0
pim sm
#

```

#### (5) SwitchE 配置信息

```

#
multicast routing-enable
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
 pim sm
#
interface Vlan-interface102
 ip address 192.168.3.2 255.255.255.0
 pim bsr-boundary
 pim sm
#
interface Vlan-interface105
 ip address 10.110.6.1 255.255.255.0
 pim sm
#
bgp 100
 router-id 3.3.3.3
 import-route ospf 1
 undo synchronization
 peer 192.168.3.1 as-number 200
#
ospf 1
 import-route bgp
 area 0.0.0.0
 network 192.168.3.0 0.0.0.255
 network 10.110.6.1 0.0.0.255
 network 3.3.3.3 0.0.0.0
#
pim
 c-bsr LoopBack0
 c-rp LoopBack0
#
msdp
 peer 192.168.3.1 connect-interface vlan-interface 102
#

```

#### (6) SwitchF 配置信息

```

#
multicast routing-enable
#
interface Vlan-interface105
 ip address 10.110.6.2 255.255.255.0
 pim sm
#
interface Vlan-interface400
 ip address 10.110.7.1 255.255.255.0
 pim sm
igmp enable

```

#

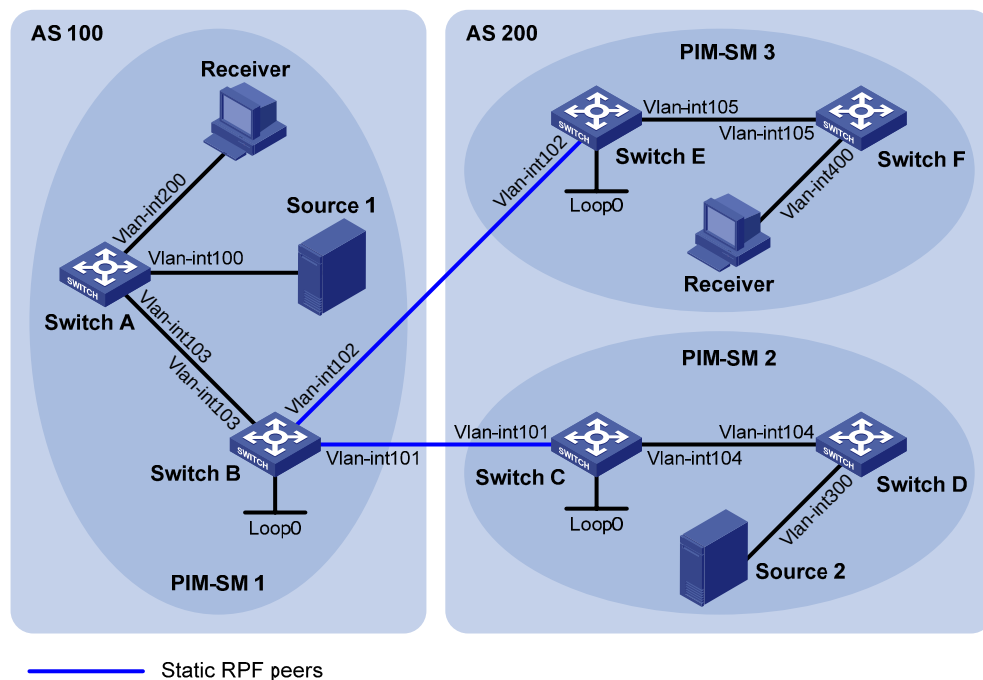
## 6. 配置注意事项

- MSDP 的适用前提：域内组播路由协议必须是 PIM-SM。
- MSDP 仅对 ASM（Any-Source Multicast，任意信源组播）模型有意义。

### 1.5.2 借助静态 RPF 对等体的 AS 间组播配置指导

#### 1. 组网图

图1-13 借助静态 RPF 对等体的 AS 间组播配置组网图



| 设备       | 接口          | IP 地址          | 设备       | 接口          | IP 地址           |
|----------|-------------|----------------|----------|-------------|-----------------|
| Switch A | Vlan-int103 | 10.110.1.2/24  | Switch D | Vlan-int104 | 10.110.4.2/24   |
|          | Vlan-int100 | 10.110.2.1/24  |          | Vlan-int300 | 10.110.5.1/24   |
|          | Vlan-int200 | 10.110.3.1/24  | Switch E | Vlan-int105 | 10.110.6.1/24   |
| Switch B | Vlan-int103 | 10.110.1.1/24  |          | Vlan-int102 | 192.168.3.2/24  |
|          | Vlan-int101 | 192.168.1.1/24 |          | Loop0       | 3.3.3.3/32      |
|          | Vlan-int102 | 192.168.3.1/24 | Switch F | Vlan-int105 | 10.110.6.2/24   |
| Switch C | Loop0       | 1.1.1.1/32     |          | Vlan-int400 | 10.110.7.1/24   |
|          | Vlan-int101 | 192.168.1.2/24 | Source 1 | -           | 10.110.2.100/24 |
|          | Vlan-int104 | 10.110.4.1/24  |          | -           | 10.110.5.100/24 |
| Switch C | Loop0       | 2.2.2.2/32     | Source 2 | -           | 10.110.5.100/24 |
|          |             |                |          |             |                 |

#### 2. 应用要求

- 网络中存在两个自治系统：PIM-SM 1 属于 AS 100，PIM-SM 2 和 PIM-SM 3 属于 AS 200。各 AS 内部采用 OSPF 进行互联，AS 之间采用 BGP 交换路由信息；
- 每个 PIM-SM 域分别拥有 0 或 1 个组播源和接收者，域内运行 OSPF 以提供单播路由；
- PIM-SM 2 和 PIM-SM 3 都是 STUB 区域，这两个区域与 PIM-SM 1 之间无需运行 BGP 或 MBGP，而是与之建立静态 RPF 对等体，从而避免对 SA 消息进行 RPF 检查；
- 将 Switch B、Switch C 和 Switch E 各自的 Loopback0 接口分别配置为各自 PIM-SM 域的 C-BSR 和 C-RP；

- Switch B 的静态 RPF 对等体为 Switch C 和 Switch E，Switch C 和 Switch E 也分别只有 Switch B 这一个静态 RPF 对等体，任何交换机都能够接收来自其静态 RPF 对等体的且被相应过滤策略允许的 SA 消息。

### 3. 适用产品、版本

表1-13 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本    |
|-------------------|---------------------------------|---------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本 |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本 |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本 |

### 4. 配置过程和解释

#### (1) 配置各交换机接口的 IP 地址和单播路由协议

请按照 图 1-13 配置各接口的 IP 地址和掩码，具体配置过程略。

配置 AS 内的各交换机之间采用 OSPF 协议进行互连，确保 AS 内部在网络层互通，并且各交换机之间能够借助单播路由协议实现动态路由更新，具体配置过程略。

#### (2) 使能 IP 组播路由，使能 PIM-SM 和 IGMP，并配置 BSR 的服务边界

# 在 Switch A 上使能 IP 组播路由，在各接口上使能 PIM-SM，并在主机侧接口 Vlan-interface200 上使能 IGMP。

```
<SwitchA> system-view
[SwitchA] multicast routing-enable
[SwitchA] interface vlan-interface 103
[SwitchA-Vlan-interface103] pim sm
[SwitchA-Vlan-interface103] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] pim sm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 200
[SwitchA-Vlan-interface200] igmp enable
[SwitchA-Vlan-interface200] pim sm
[SwitchA-Vlan-interface200] quit
```

Switch B、Switch C、Switch D、Switch E 和 Switch F 上的配置与 Switch A 相似，配置过程略。

# 在 Switch B 上配置 BSR 的服务边界。

```
[SwitchB] interface vlan-interface 102
[SwitchB-Vlan-interface102] pim bsr-boundary
[SwitchB-Vlan-interface102] quit
[SwitchB] interface vlan-interface 101
```

```
[SwitchB-Vlan-interface101] pim bsr-boundary
[SwitchB-Vlan-interface101] quit
```

Switch C 和 Switch E 上的配置与 Switch B 相似，配置过程略。

### (3) 配置 C-BSR 和 C-RP 的位置

# 在 Switch B 上将 Loopback0 接口配置为 C-BSR 和 C-RP。

```
[SwitchB] pim
[SwitchB-pim] c-bsr loopback 0
[SwitchB-pim] c-rp loopback 0
[SwitchB-pim] quit
```

Switch C 和 Switch E 上的配置与 Switch B 相似，配置过程略。

### (4) 配置静态 RPF 对等体

# 配置 Switch C 和 Switch E 作为 Switch B 的 MSDP 对等体及静态 RPF 对等体。

```
[SwitchB] ip ip-prefix list-df permit 192.168.0.0 16 greater-equal 16 less-equal 32
[SwitchB] msdp
[SwitchB-msdp] peer 192.168.3.2 connect-interface vlan-interface 102
[SwitchB-msdp] peer 192.168.1.2 connect-interface vlan-interface 101
[SwitchB-msdp] static-rpf-peer 192.168.3.2 rp-policy list-df
[SwitchB-msdp] static-rpf-peer 192.168.1.2 rp-policy list-df
[SwitchB-msdp] quit
```

# 配置 Switch B 作为 Switch C 的 MSDP 对等体及静态 RPF 对等体。

```
[SwitchC] ip ip-prefix list-c permit 192.168.0.0 16 greater-equal 16 less-equal 32
[SwitchC] msdp
[SwitchC-msdp] peer 192.168.1.1 connect-interface vlan-interface 101
[SwitchC-msdp] static-rpf-peer 192.168.1.1 rp-policy list-c
[SwitchC-msdp] quit
```

# 配置 Switch B 作为 Switch E 的 MSDP 对等体及静态 RPF 对等体。

```
[SwitchE] ip ip-prefix list-c permit 192.168.0.0 16 greater-equal 16 less-equal 32
[SwitchE] msdp
[SwitchE-msdp] peer 192.168.3.1 connect-interface vlan-interface 102
[SwitchE-msdp] static-rpf-peer 192.168.3.1 rp-policy list-c
[SwitchE-msdp] quit
```

### (5) 检验配置效果

通过使用 **display bgp peer** 命令可以查看交换机之间 BGP 对等体建立情况，如果无任何信息输出，说明交换机之间未建立 BGP 对等体关系。

当 PIM-SM 1 和 PIM-SM 2 域内的组播源 Source 1 和 Source 2 发送组播信息时，PIM-SM 1 和 PIM-SM 3 域内的接收者（Receiver）能收到该组播信息，通过使用 **display msdp brief** 命令可以查看交换机之间 MSDP 对等体的建立情况。例如：

# 查看 Switch B 上 MSDP 对等体的简要信息。

```
[SwitchB] display msdp brief
MSDP Peer Brief Information
```

| Configured | Up | Listen | Connect | Shutdown | Down |
|------------|----|--------|---------|----------|------|
| 2          | 2  | 0      | 0       | 0        | 0    |



| Peer's Address | State | Up/Down time | AS | SA Count | Reset Count |
|----------------|-------|--------------|----|----------|-------------|
| 192.168.3.2    | Up    | 01:07:08     | ?  | 8        | 0           |
| 192.168.1.2    | Up    | 00:16:39     | ?  | 13       | 0           |

# 查看 Switch C 上 MSDP 对等体的简要信息。

```
[SwitchC] display msdp brief
```

MSDP Peer Brief Information

| Configured | Up | Listen | Connect | Shutdown | Down |
|------------|----|--------|---------|----------|------|
| 1          | 1  | 0      | 0       | 0        | 0    |

| Peer's Address | State | Up/Down time | AS | SA Count | Reset Count |
|----------------|-------|--------------|----|----------|-------------|
| 192.168.1.1    | Up    | 01:07:09     | ?  | 8        | 0           |

# 查看 Switch E 上 MSDP 对等体的简要信息。

```
[SwitchE] display msdp brief
```

MSDP Peer Brief Information

| Configured | Up | Listen | Connect | Shutdown | Down |
|------------|----|--------|---------|----------|------|
| 1          | 1  | 0      | 0       | 0        | 0    |

| Peer's Address | State | Up/Down time | AS | SA Count | Reset Count |
|----------------|-------|--------------|----|----------|-------------|
| 192.168.3.1    | Up    | 00:16:40     | ?  | 13       | 0           |

## 5. 完整配置

### (1) SwitchA 配置信息

```
#
multicast routing-enable
#
interface Vlan-interface100
 ip address 10.110.2.1 255.255.255.0
 pim sm
#
interface Vlan-interface103
 ip address 10.110.1.2 255.255.255.0
 pim sm
#
interface Vlan-interface200
 ip address 10.110.3.1 255.255.255.0
 igmp enable
 pim sm
#
ospf 1
 area 0.0.0.0
 network 10.110.1.0 0.0.0.255
 network 10.110.2.0 0.0.0.255
 network 10.110.3.0 0.0.0.255
#
```

### (2) SwitchB 配置信息

```

#
multicast routing-enable
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
 pim sm
#
interface Vlan-interface101
 ip address 192.168.1.1 255.255.255.0
 pim bsr-boundary
 pim sm
#
interface Vlan-interface102
 ip address 192.168.3.1 255.255.255.0
 pim bsr-boundary
 pim sm
#
interface Vlan-interface103
 ip address 10.110.1.1 255.255.255.0
 pim sm
#
ospf 1
 area 0.0.0.0
 network 192.168.1.0 0.0.0.255
 network 10.110.1.0 0.0.0.255
 network 1.1.1.1 0.0.0.0
#
pim
 c-bsr LoopBack0
 c-rp LoopBack0
#
msdp
 peer 192.168.3.2 connect-interface vlan-interface 102
 peer 192.168.1.2 connect-interface vlan-interface 101
 static-rpf-peer 192.168.3.2 rp-policy list-df
 static-rpf-peer 192.168.1.2 rp-policy list-df
#
 ip ip-prefix list-df index 10 permit 192.168.0.0 16 greater-equal 16 less-equal
 32
#

```

### (3) SwitchC 配置信息

```

#
multicast routing-enable
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
 pim sm
#

```

```

interface Vlan-interface101
 ip address 192.168.1.2 255.255.255.0
 pim bsr-boundary
 pim sm
#
interface Vlan-interface104
 ip address 10.110.4.1 255.255.255.0
 pim sm
#
ospf 1
 area 0.0.0.0
 network 192.168.1.0 0.0.0.255
 network 10.110.4.1 0.0.0.255
 network 2.2.2.2 0.0.0.0
#
pim
 c-bsr LoopBack0
 c-rp LoopBack0
#
msdp
 peer 192.168.1.1 connect-interface vlan-interface 101
 static-rpf-peer 192.168.1.1 rp-policy list-c
#
ip ip-prefix list-c permit 192.168.0.0 16 greater-equal 16 less-equal 32
#

```

#### (4) SwitchD 配置信息

```

#
multicast routing-enable
#
interface Vlan-interface104
 ip address 10.110.4.2 255.255.255.0
 pim sm
#
interface Vlan-interface300
 ip address 10.110.5.1 255.255.255.0
 pim sm
#

```

#### (5) SwitchE 配置信息

```

#
multicast routing-enable
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
 pim sm
#
interface Vlan-interface102
 ip address 192.168.3.2 255.255.255.0
 pim bsr-boundary

```

```

pim sm
#
interface Vlan-interface105
 ip address 10.110.6.1 255.255.255.0
 pim sm
#
ospf 1
 area 0.0.0.0
 network 192.168.3.0 0.0.0.255
 network 10.110.6.1 0.0.0.255
 network 3.3.3.3 0.0.0.0
#
pim
 c-bsr LoopBack0
 c-rp LoopBack0
#
msdp
 peer 192.168.3.1 connect-interface vlan-interface 102
 static-rpf-peer 192.168.3.1 rp-policy list-c
#
ip ip-prefix list-c permit 192.168.0.0 16 greater-equal 16 less-equal 32
#

```

#### (6) SwitchF 配置信息

```

#
multicast routing-enable
#
interface Vlan-interface105
 ip address 10.110.6.2 255.255.255.0
 pim sm
#
interface Vlan-interface400
 ip address 10.110.7.1 255.255.255.0
 pim sm
 igmp enable
#

```

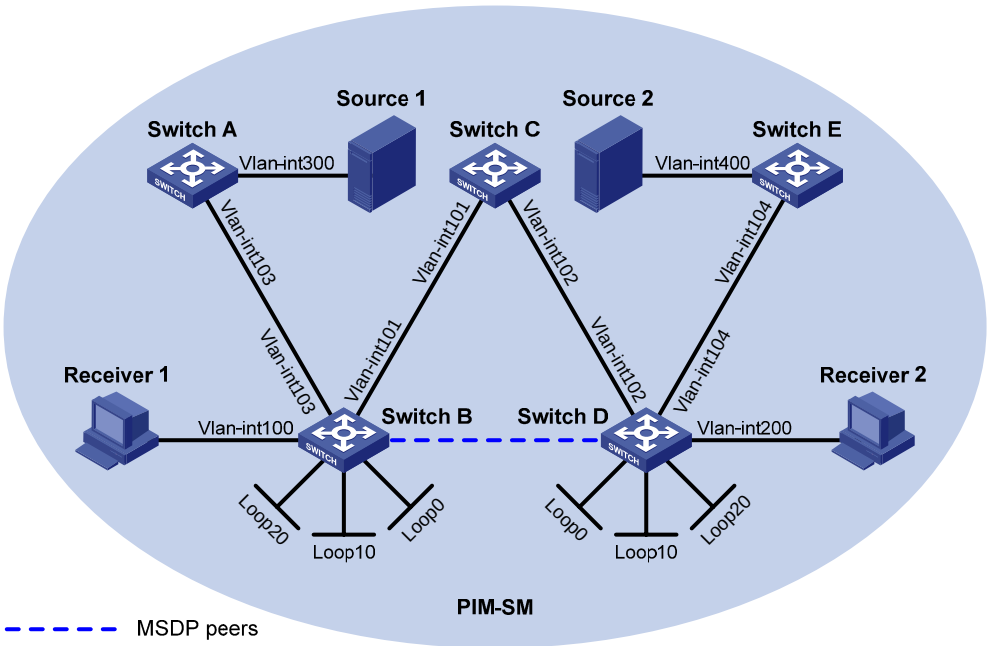
#### 6. 配置注意事项

无

1.5.3 Anycast RP 应用配置指导

1. 组网图

图1-14 Anycast RP 应用配置组网图



| 设备       | 接口          | IP 地址           | 设备       | 接口          | IP 地址          |
|----------|-------------|-----------------|----------|-------------|----------------|
| Source 1 | -           | 10.110.5.100/24 | Switch C | Vlan-int101 | 192.168.1.2/24 |
| Source 2 | -           | 10.110.6.100/24 |          | Vlan-int102 | 192.168.2.2/24 |
| Switch A | Vlan-int300 | 10.110.5.1/24   | Switch D | Vlan-int200 | 10.110.3.1/24  |
|          | Vlan-int103 | 10.110.2.2/24   |          | Vlan-int104 | 10.110.4.1/24  |
| Switch B | Vlan-int100 | 10.110.1.1/24   |          | Vlan-int102 | 192.168.2.1/24 |
|          | Vlan-int103 | 10.110.2.1/24   |          | Loop0       | 2.2.2.2/32     |
|          | Vlan-int101 | 192.168.1.1/24  |          | Loop10      | 4.4.4.4/32     |
|          | Loop0       | 1.1.1.1/32      |          | Loop20      | 10.1.1.1/32    |
|          | Loop10      | 3.3.3.3/32      | Switch E | Vlan-int400 | 10.110.6.1/24  |
|          | Loop20      | 10.1.1.1/32     |          | Vlan-int104 | 10.110.4.2/24  |

2. 应用要求

- PIM-SM 域内拥有多个组播源和接收者，并在域内运行 OSPF 协议以提供单播路由；
- 通过配置 Anycast RP，使接收者侧 DR 能够向拓扑距离最近的 RP 发起加入，组播源侧 DR 也向拓扑距离最近的 RP 发起注册；
- 将 Switch B 和 Switch D 各自的 Loopback10 接口配置为 C-BSR、Loopback20 接口配置为 C-RP；
- Switch B 的 Router ID 为 1.1.1.1，Switch D 的 Router ID 为 2.2.2.2，在 Switch B 和 Switch D 之间建立 MSDP 对等体关系。

3. 适用产品、版本

表1-14 配置适用的产品与软硬件版本关系

| 产品             | 软件版本                            | 硬件版本    |
|----------------|---------------------------------|---------|
| S3610 系列以太网交换机 | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |

| 产品                | 软件版本                            | 硬件版本    |
|-------------------|---------------------------------|---------|
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本 |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本 |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本 |

#### 4. 配置过程和解释

##### (1) 配置各交换机接口的 IP 地址和单播路由协议

请按照 图 1-14 配置各接口的 IP 地址和子网掩码，具体配置过程略。

配置 PIM-SM 域内的各交换机之间采用 OSPF 协议进行互连, 确保 PIM-SM 域内部在网络层互通, 并且各交换机之间能够借助单播路由协议实现动态路由更新，具体配置过程略。

##### (2) 使能 IP 组播路由，并使能 PIM-SM 和 IGMP

# 在 Switch B 上使能 IP 组播路由，在各接口上使能 PIM-SM，并在主机侧接口 Vlan-interface100 上使能 IGMP。

```
<SwitchB> system-view
[SwitchB] multicast routing-enable
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] igmp enable
[SwitchB-Vlan-interface100] pim sm
[SwitchB-Vlan-interface100] quit
[SwitchB] interface vlan-interface 103
[SwitchB-Vlan-interface103] pim sm
[SwitchB-Vlan-interface103] quit
[SwitchB] interface Vlan-interface 101
[SwitchB-Vlan-interface101] pim sm
[SwitchB-Vlan-interface101] quit
[SwitchB] interface loopback 0
[SwitchB-LoopBack0] pim sm
[SwitchB-LoopBack0] quit
[SwitchB] interface loopback 10
[SwitchB-LoopBack10] pim sm
[SwitchB-LoopBack10] quit
[SwitchB] interface loopback 20
[SwitchB-LoopBack20] pim sm
[SwitchB-LoopBack20] quit
```

Switch A、Switch C、Switch D 和 Switch E 上的配置与 Switch B 相似，配置过程略。

##### (3) 配置 C-BSR 和 C-RP 的位置

# 在 Switch B 上将 Loopback10 配置为 C-BSR，将 Loopback20 配置为 C-RP。

```
[SwitchB] pim
[SwitchB-pim] c-bsr loopback 10
```

```
[SwitchB-pim] c-rp loopback 20
```

```
[SwitchB-pim] quit
```

Switch D 上的配置与 Switch B 相似，配置过程略。

#### (4) 配置 MSDP 对等体

# 在 Switch B 的 Loopback0 接口上配置 MSDP 对等体。

```
[SwitchB] msdp
```

```
[SwitchB-msdp] originating-rp loopback 0
```

```
[SwitchB-msdp] peer 2.2.2.2 connect-interface loopback 0
```

```
[SwitchB-msdp] quit
```

# 在 Switch D 的 Loopback0 接口上配置 MSDP 对等体。

```
[SwitchD] msdp
```

```
[SwitchD-msdp] originating-rp loopback 0
```

```
[SwitchD-msdp] peer 1.1.1.1 connect-interface loopback 0
```

```
[SwitchD-msdp] quit
```

#### (5) 检验配置效果

通过使用 **display msdp brief** 命令可以查看交换机之间 MSDP 对等体建立情况。

# 查看 Switch B 上 MSDP 对等体的简要信息。

```
[SwitchB] display msdp brief
```

MSDP Peer Brief Information

| Configured | Up | Listen | Connect | Shutdown | Down |
|------------|----|--------|---------|----------|------|
| 1          | 1  | 0      | 0       | 0        | 0    |

| Peer's Address | State | Up/Down time | AS | SA Count | Reset Count |
|----------------|-------|--------------|----|----------|-------------|
| 2.2.2.2        | Up    | 00:10:17     | ?  | 0        | 0           |

# 查看 Switch D 上 MSDP 对等体的简要信息。

```
[SwitchD] display msdp brief
```

MSDP Peer Brief Information

| Configured | Up | Listen | Connect | Shutdown | Down |
|------------|----|--------|---------|----------|------|
| 1          | 1  | 0      | 0       | 0        | 0    |

| Peer's Address | State | Up/Down time | AS | SA Count | Reset Count |
|----------------|-------|--------------|----|----------|-------------|
| 1.1.1.1        | Up    | 00:10:18     | ?  | 0        | 0           |

通过使用 **display pim routing-table** 命令可以查看交换机上的 PIM 路由。

当 Source 1（10.110.5.100/24）开始向组播组 G（225.1.1.1）发送组播信息时，Receiver 1 加入组播组 G。通过比较 Switch B 与 Switch D 上 PIM 路由的显示信息，可知当前的有效 RP 为 Switch B：Source 1 向 Switch B 注册，Receiver 1 向 Switch B 加入。

# 查看 Switch B 上的 PIM 路由的信息。

```
[SwitchB] display pim routing-table
```

Total 1 (\*, G) entry; 1 (S, G) entry

```
(*, 225.1.1.1)
```

```
RP: 10.1.1.1 (local)
```

```
Protocol: pim-sm, Flag: WC
```

```

UpTime: 00:15:04
Upstream interface: Register
Upstream neighbor: NULL
RPF prime neighbor: NULL
Downstream interface(s) information:
Total number of downstreams: 1
1: Vlan-interface100
Protocol: igmp, UpTime: 00:15:04, Expires: -

```

```

(10.110.5.100, 225.1.1.1)
RP: 10.1.1.1 (local)
Protocol: pim-sm, Flag: SPT 2MSDP ACT
UpTime: 00:46:28
Upstream interface: Vlan-interface103
Upstream neighbor: 10.110.2.2
RPF prime neighbor: 10.110.2.2
Downstream interface(s) information:
Total number of downstreams: 1
1: Vlan-interface100
Protocol: pim-sm, UpTime: - , Expires: -

```

# 查看 Switch D 上的 PIM 路由的信息。

```
[SwitchD] display pim routing-table
```

Switch D 上没有信息输出。

Receiver 1 离开组播组 G，Source 1 也停止向组播组 G 发送组播数据。当 Source 2 (10.110.6.100/24) 开始向组播组 G 发送组播信息时，Receiver 2 加入组播组 G。通过比较 Switch B 与 Switch D 上 PIM 路由的显示信息，可知当前的有效 RP 为 Switch D：Source 2 向 Switch D 注册，Receiver 2 向 Switch D 加入。

# 查看 Switch B 上的 PIM 路由的信息。

```
[SwitchB] display pim routing-table
```

Switch B 上没有信息输出。

# 查看 Switch D 上的 PIM 路由的信息。

```
[SwitchD] display pim routing-table
Total 1 (*, G) entry; 1 (S, G) entry

```

```

(*, 225.1.1.1)
RP: 10.1.1.1 (local)
Protocol: pim-sm, Flag: WC
UpTime: 00:12:07
Upstream interface: Register
Upstream neighbor: NULL
RPF prime neighbor: NULL
Downstream interface(s) information:
Total number of downstreams: 1
1: Vlan-interface200
Protocol: igmp, UpTime: 00:12:07, Expires: -

```



```

(10.110.6.100, 225.1.1.1)
RP: 10.1.1.1 (local)
Protocol: pim-sm, Flag: SPT 2MSDP ACT
UpTime: 00:40:22
Upstream interface: Vlan-interface104
Upstream neighbor: 10.110.4.2
RPF prime neighbor: 10.110.4.2
Downstream interface(s) information:
Total number of downstreams: 1
1: Vlan-interface200
Protocol: pim-sm, UpTime: - , Expires: -

```

## 5. 完整配置

### (1) SwitchA 配置信息

```

#
multicast routing-enable
#
interface Vlan-interface103
ip address 10.110.2.2 255.255.255.0
pim sm
#
interface Vlan-interface200
ip address 10.110.5.1 255.255.255.0
igmp enable
pim sm
#
ospf 1
area 0.0.0.0
network 10.110.2.0 0.0.0.255
network 10.110.5.0 0.0.0.255
#

```

### (2) SwitchB 配置信息

```

#
multicast routing-enable
#
interface LoopBack0
ip address 1.1.1.1 255.255.255.255
pim sm
#
interface LoopBack10
ip address 3.3.3.3 255.255.255.255
pim sm
#
interface LoopBack20
ip address 10.1.1.1 255.255.255.255
pim sm
#

```

```

interface Vlan-interface100
 ip address 10.110.1.1 255.255.255.0
pim sm
#
interface Vlan-interface101
 ip address 192.168.1.1 255.255.255.0
pim sm
#
interface Vlan-interface103
 ip address 10.110.2.1 255.255.255.0
pim sm
#
ospf 1
 area 0.0.0.0
 network 192.168.1.0 0.0.0.255
 network 10.110.1.0 0.0.0.255
 network 10.110.2.0 0.0.0.255
 network 1.1.1.1 0.0.0.0
 network 3.3.3.3 0.0.0.0
 network 10.1.1.1 0.0.0.0
#
pim
 c-bsr LoopBack10
 c-rp LoopBack20
#
msdp
 originating-rp loopback 0
 peer 2.2.2.2 connect-interface loopback 0
#

```

### (3) SwitchC 配置信息

```

#
multicast routing-enable
#
interface Vlan-interface101
 ip address 192.168.1.2 255.255.255.0
pim sm
#
interface Vlan-interface102
 ip address 192.168.2.2 255.255.255.0
pim sm
#
ospf 1
 area 0.0.0.0
 network 192.168.1.0 0.0.0.255
 network 192.168.2.0 0.0.0.255
#

```

### (4) SwitchD 配置信息

```

#

```

```

multicast routing-enable
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
 pim sm
#
interface LoopBack10
 ip address 4.4.4.4 255.255.255.255
 pim sm
#
interface LoopBack20
 ip address 10.1.1.1 255.255.255.255
 pim sm
#
interface Vlan-interface102
 ip address 192.168.2.1 255.255.255.0
 pim sm
#
interface Vlan-interface104
 ip address 10.110.4.1 255.255.255.0
 pim sm
#
interface Vlan-interface200
 ip address 10.110.3.1 255.255.255.0
 pim sm
#
ospf 1
 area 0.0.0.0
 network 192.168.2.0 0.0.0.255
 network 10.110.4.0 0.0.0.255
 network 10.110.3.0 0.0.0.255
 network 2.2.2.2 0.0.0.0
 network 4.4.4.4 0.0.0.0
 network 10.1.1.1 0.0.0.0
#
pim
 c-bsr LoopBack10
 c-rp LoopBack20
#
msdp
 originating-rp loopback 0
 peer 1.1.1.1 connect-interface loopback 0
#

```

#### (5) SwitchE 配置信息

```

#
multicast routing-enable
#
interface Vlan-interface104

```

```

ip address 10.110.4.2 255.255.255.0
pim sm
#
interface Vlan-interface400
ip address 10.110.6.1 255.255.255.0
pim sm
igmp enable
#

```

## 6. 配置注意事项

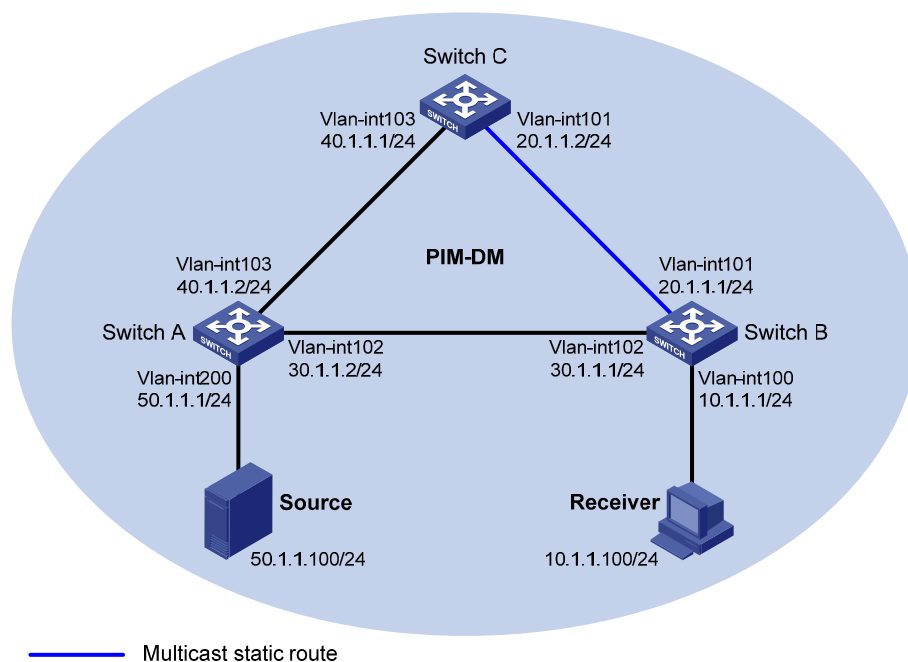
- 必须为 Anycast RP 地址配置 32 位的子网掩码（即 255.255.255.255），也即将其配置为一个主机地址。
- MSDP 对等体的地址不能与 Anycast RP 地址相同。

## 1.6 组播路由与转发配置指导

### 1.6.1 改变 RPF 路由配置指导

#### 1. 组网图

图1-15 改变 RPF 路由配置指导



#### 2. 应用要求

- 网络中运行 PIM-DM，所有交换机都支持组播功能；
- Switch A、Switch B 和 Switch C 之间运行 OSPF 协议；
- 通常情况下，Receiver 能通过 Switch A—Switch B 这条与单播路径相同的路径接收来自 Source 的组播信息；

- 要求通过配置，使 Receiver 能通过 Switch A—Switch C—Switch B 这条与单播路径不同的路径接收来自 Source 的组播信息。

### 3. 适用产品、版本

表1-15 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本    |
|-------------------|---------------------------------|---------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本 |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本 |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本 |

### 4. 配置过程 and 解释

#### (1) 配置各交换机接口的 IP 地址和单播路由协议

请按照 图 1-15 配置各接口的 IP 地址和掩码，具体配置过程略。

配置 PIM-DM 域内的各交换机之间采用 OSPF 协议进行互连，确保 PIM-DM 域内部在网络层互通，并且各交换机之间能够借助单播路由协议实现动态路由更新，具体配置过程略。

#### (2) 使能 IP 组播路由，并使能 PIM-DM 和 IGMP

# 在 Switch B 上使能 IP 组播路由，在各接口上使能 PIM-DM，并在主机侧接口 Vlan-interface100 上使能 IGMP。

```
<SwitchB> system-view
[SwitchB] multicast routing-enable
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] igmp enable
[SwitchB-Vlan-interface100] pim dm
[SwitchB-Vlan-interface100] quit
[SwitchB] interface vlan-interface 101
[SwitchB-Vlan-interface101] pim dm
[SwitchB-Vlan-interface101] quit
[SwitchB] interface vlan-interface 102
[SwitchB-Vlan-interface102] pim dm
[SwitchB-Vlan-interface102] quit
```

# 在 Switch A 上使能 IP 组播路由，并在各接口上使能 PIM-DM。

```
<SwitchA> system-view
[SwitchA] multicast routing-enable
[SwitchA] interface vlan-interface 200
[SwitchA-Vlan-interface200] pim dm
[SwitchA-Vlan-interface200] quit
[SwitchA] interface vlan-interface 102
[SwitchA-Vlan-interface102] pim dm
```

```
[SwitchA-Vlan-interface102] quit
[SwitchA] interface vlan-interface 103
[SwitchA-Vlan-interface103] pim dm
[SwitchA-Vlan-interface103] quit
```

Switch C 上的配置与 Switch A 相似，配置过程略。

# 在 Switch B 上使用 **display multicast rpf-info** 命令查看到 Source 的 RPF 信息。

```
[SwitchB] display multicast rpf-info 50.1.1.100
RPF information about source 50.1.1.100:
 RPF interface: Vlan-interface102, RPF neighbor: 30.1.1.2
 Referenced route/mask: 50.1.1.0/24
 Referenced route type: igp
 Route selection rule: preference-preferred
 Load splitting rule: disable
```

Switch B 上当前的 RPF 路由来源于单播路由，RPF 邻居是 Switch A。

### (3) 配置组播静态路由

# 在 Switch B 上配置组播静态路由，到 Source 的 RPF 邻居为 Switch C。

```
[SwitchB] ip rpf-route-static 50.1.1.100 24 20.1.1.2
```

### (4) 检验配置效果

# 在 Switch B 上使用 **display multicast rpf-info** 命令查看到 Source 的 RPF 信息。

```
[SwitchB] display multicast rpf-info 50.1.1.100
RPF information about source 50.1.1.100:
 RPF interface: Vlan-interface101, RPF neighbor: 20.1.1.2
 Referenced route/mask: 50.1.1.0/24
 Referenced route type: multicast static
 Route selection rule: preference-preferred
 Load splitting rule: disable
```

与配置组播静态路由前相比，Switch B 上的 RPF 路由已经产生了变化，其来源变为组播静态路由，RPF 邻居变为 Switch C。

## 5. 完整配置

### (1) SwitchA 配置信息

```
#
multicast routing-enable
#
interface Vlan-interface102
ip address 30.1.1.2 255.255.255.0
pim dm
#
interface Vlan-interface103
ip address 40.1.1.2 255.255.255.0
pim dm
#
interface Vlan-interface200
ip address 50.1.1.1 255.255.255.0
```

```
pim dm
```

```
#
```

## (2) SwitchB 配置信息

```
#
```

```
multicast routing-enable
```

```
#
```

```
interface Vlan-interface100
```

```
ip address 10.1.1.1 255.255.255.0.
```

```
igmp enable
```

```
pim dm
```

```
#
```

```
interface Vlan-interface101
```

```
ip address 20.1.1.1 255.255.255.0.
```

```
pim dm
```

```
#
```

```
interface Vlan-interface102
```

```
ip address 30.1.1.1 255.255.255.0
```

```
pim dm
```

```
#
```

```
ip rpf-route-static 50.1.1.0 24 20.1.1.2
```

```
#
```

## (3) SwitchC 配置信息

```
#
```

```
multicast routing-enable
```

```
#
```

```
interface Vlan-interface101
```

```
ip address 20.1.1.2 255.255.255.0.
```

```
pim dm
```

```
#
```

```
interface Vlan-interface103
```

```
ip address 40.1.1.1 255.255.255.0
```

```
pim dm
```

```
#
```

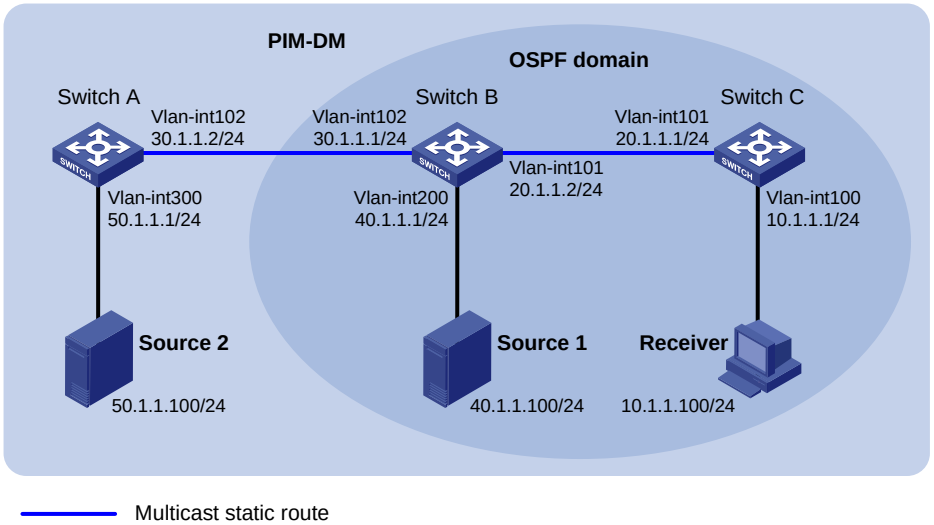
## 6. 配置注意事项

无

## 1.6.2 衔接 RPF 路由配置指导

### 1. 组网图

图1-16 衔接 RPF 路由配置组网图



### 2. 应用要求

- 网络中运行 PIM-DM，所有交换机都支持组播功能；
- Switch B 和 Switch C 之间运行 OSPF 协议，并与 Switch A 单播路由隔离；
- 通常情况下，Receiver 能接收来自 OSPF 域内 Source 1 的组播信息；
- 要求通过配置，使 Receiver 也可以接收来自 OSPF 域外 Source 2 的组播信息。

### 3. 适用产品、版本

表1-16 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本    |
|-------------------|---------------------------------|---------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本 |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本 |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本 |

### 4. 配置过程和解释

#### (1) 配置各交换机接口的 IP 地址和单播路由协议

请按照 图 1-16 配置各接口的 IP 地址和掩码，具体配置过程略。

配置 Switch B 和 Switch C 之间采用 OSPF 协议进行互连，确保 Switch B 和 Switch C 之间在网络层互通，并且能够借助单播路由协议实现动态路由更新，具体配置过程略。

#### (2) 使能 IP 组播路由，并使能 PIM-DM 和 IGMP



# 在 Switch C 上使能 IP 组播路由，在各接口上使能 PIM-DM，并在主机侧接口 Vlan-interface100 上使能 IGMP。

```
<SwitchC> system-view
[SwitchC] multicast routing-enable
[SwitchC] interface vlan-interface 100
[SwitchC-Vlan-interface100] igmp enable
[SwitchC-Vlan-interface100] pim dm
[SwitchC-Vlan-interface100] quit
[SwitchC] interface vlan-interface 101
[SwitchC-Vlan-interface101] pim dm
[SwitchC-Vlan-interface101] quit
```

# 在 Switch A 上使能 IP 组播路由，并在各接口上使能 PIM-DM。

```
<SwitchA> system-view
[SwitchA] multicast routing-enable
[SwitchC] interface vlan-interface 300
[SwitchC-Vlan-interface300] pim dm
[SwitchC-Vlan-interface300] quit
[SwitchC] interface vlan-interface 102
[SwitchC-Vlan-interface102] pim dm
[SwitchC-Vlan-interface102] quit
```

Switch B 上的配置与 Switch A 相似，配置过程略。

# 在 Switch B 和 Switch C 上分别使用 **display multicast rpf-info** 命令查看到 Source 2 的 RPF 信息。

```
[SwitchB] display multicast rpf-info 50.1.1.100
[SwitchC] display multicast rpf-info 50.1.1.100
```

没有显示信息输出，说明在 Switch B 和 Switch C 上都没有到 Source 2 的 RPF 路由。

### (3) 配置组播静态路由

# 在 Switch B 上配置组播静态路由，到 Source 2 的 RPF 邻居为 Switch A。

```
[SwitchB] ip rpf-route-static 50.1.1.100 24 30.1.1.2
```

# 在 Switch C 上配置组播静态路由，到 Source 2 的 RPF 邻居为 Switch B。

```
[SwitchC] ip rpf-route-static 50.1.1.100 24 20.1.1.2
```

### (4) 检验配置效果

# 在 Switch B 和 Switch C 上分别使用 **display multicast rpf-info** 命令查看到 Source 2 的 RPF 信息。

```
[SwitchB] display multicast rpf-info 50.1.1.100
RPF information about source 50.1.1.100:
 RPF interface: Vlan-interface102, RPF neighbor: 30.1.1.2
 Referenced route/mask: 50.1.1.0/24
 Referenced route type: multicast static
 Route selection rule: preference-preferred
 Load splitting rule: disable
[SwitchC] display multicast rpf-info 50.1.1.100
RPF information about source 50.1.1.100:
```

```
RPF interface: Vlan-interface101, RPF neighbor: 20.1.1.2
```

```
Referenced route/mask: 50.1.1.0/24
```

```
Referenced route type: multicast static
```

```
Route selection rule: preference-preferred
```

```
Load splitting rule: disable
```

与配置组播静态路由前相比，Switch B 和 Switch C 上都有了到 Source 2 的 RPF 路由，且其均来源于组播静态路由。

## 5. 完整配置

### (1) SwitchA 配置信息

```
#
multicast routing-enable
#
interface Vlan-interface102
ip address 30.1.1.2 255.255.255.0.
pim dm
#
interface Vlan-interface300
ip address 50.1.1.1 255.255.255.0
pim dm
#
```

### (2) SwitchB 配置信息

```
#
multicast routing-enable
#
interface Vlan-interface101
ip address 20.1.1.2 255.255.255.0.
pim dm
#
interface Vlan-interface102
ip address 30.1.1.1 255.255.255.0
pim dm
#
interface Vlan-interface200
ip address 40.1.1.1 255.255.255.0.
pim dm
#
ip rpf-route-static 50.1.1.100 24 20.1.1.2
#
```

### (3) SwitchC 配置信息

```
#
multicast routing-enable
#
interface Vlan-interface100
ip address 10.1.1.1 255.255.255.0.
igmp enable
pim dm
```

```
#
interface Vlan-interface101
ip address 20.1.1.1 255.255.255.0
pim dm
#
ip rpf-route-static 50.1.1.100 24 20.1.1.2
#
```

6. 配置注意事项

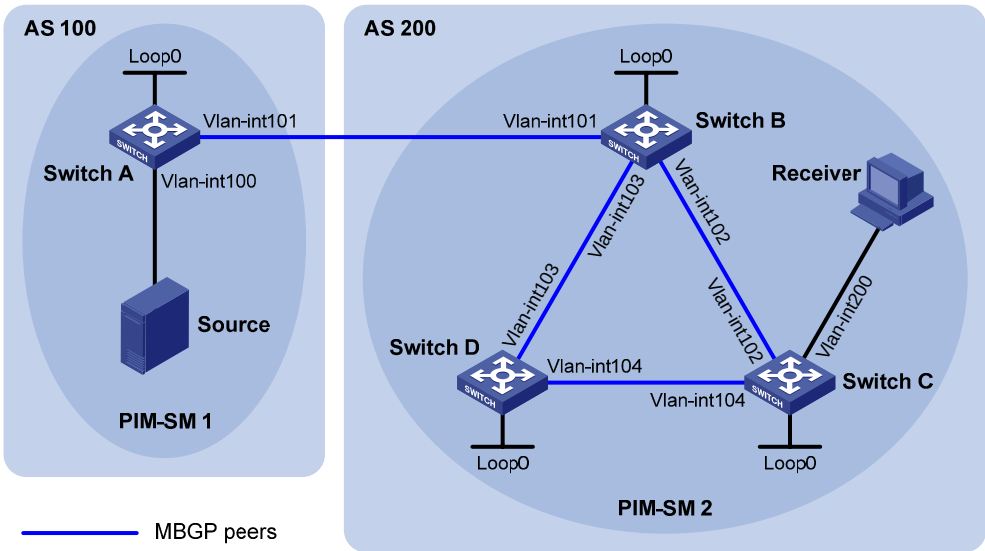
无

1.7 MBGP 典型配置指导

1.7.1 MBGP 典型配置指导

1. 组网图

图1-17 MBGP 典型配置组网图



| 设备       | 接口          | IP 地址           | 设备       | 接口          | IP 地址          |
|----------|-------------|-----------------|----------|-------------|----------------|
| Source   | -           | 10.110.1.100/24 | Switch C | Vlan-int200 | 10.110.2.1/24  |
| Switch A | Vlan-int100 | 10.110.1.1/24   |          | Vlan-int102 | 192.168.2.2/24 |
|          | Vlan-int101 | 192.168.1.1/24  |          | Vlan-int104 | 192.168.4.1/24 |
|          | Loop0       | 1.1.1.1/32      |          | Loop0       | 3.3.3.3/32     |
| Switch B | Vlan-int101 | 192.168.1.2/24  | Switch D | Vlan-int103 | 192.168.3.2/24 |
|          | Vlan-int102 | 192.168.2.1/24  |          | Vlan-int104 | 192.168.4.2/24 |
|          | Vlan-int103 | 192.168.3.1/24  |          | Loop0       | 4.4.4.4/32     |
|          | Loop0       | 2.2.2.2/32      |          |             |                |

2. 应用要求

- 网络中存在两个自治系统：PIM-SM 1 属于 AS 100，PIM-SM 2 属于 AS 200。各 AS 内部采用 OSPF 进行互联，AS 之间采用 MBGP 交换组播路由信息；
- 组播源属于 AS 100 内的 PIM-SM 1，接收者则属于 AS 200 内的 PIM-SM 2；
- 将 Switch A 和 Switch B 各自的 Loopback0 接口分别配置为各自 PIM-SM 域的 C-BSR 和 C-RP；
- 在 Switch A 与 Switch B 之间通过 MBGP 建立 MSDP 对等体关系。

### 3. 适用产品、版本

表1-17 配置适用的产品与软硬件版本关系

| 产品              | 软件版本              | 硬件版本    |
|-----------------|-------------------|---------|
| S7500E 系列以太网交换机 | Release 6300 软件版本 | 全系列硬件版本 |

### 4. 配置过程和解释

(1) 配置各交换机接口的 IP 地址和单播路由协议

- 请按照 图 1-17 配置各接口的 IP 地址和子网掩码，具体配置过程略。
- 配置 AS200 内的各交换机之间采用 OSPF 路由协议交换路由信息（AS 内各路由器创建的 OSPF 进程号为 1），确保各 AS 内部在网络层互通，能学到彼此 Loopback 接口的路由，配置方法请参见“IPv4 路由典型配置指导”。

(2) 使能 IP 组播路由，使能 PIM-SM 和 IGMP，并配置 BSR 的服务边界

# 在 Switch A 上使能 IP 组播路由，在各接口上使能 PIM-SM。

```
<SwitchA> system-view
[SwitchA] multicast routing-enable
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] pim sm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim sm
[SwitchA-Vlan-interface101] quit
```

Switch B 和 Switch D 上的配置与 Switch A 相似，配置过程略。

# 在 Switch C 上使能 IP 组播路由，在各接口上使能 PIM-SM，并在主机侧接口 Vlan-interface200 上使能 IGMP。

```
<SwitchC> system-view
[SwitchC] multicast routing-enable
[SwitchC] interface vlan-interface 102
[SwitchC-Vlan-interface102] pim sm
[SwitchC-Vlan-interface102] quit
[SwitchC] interface vlan-interface 104
[SwitchC-Vlan-interface104] pim sm
[SwitchC-Vlan-interface104] quit
[SwitchC] interface vlan-interface 200
[SwitchC-Vlan-interface200] pim sm
[SwitchC-Vlan-interface200] igmp enable
[SwitchC-Vlan-interface200] quit
```

# 在 Switch A 上配置 BSR 的服务边界。

```
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim bsr-boundary
[SwitchA-Vlan-interface101] quit
```

# 在 Switch B 上配置 BSR 的服务边界。

```
[SwitchB] interface vlan-interface 101
[SwitchB-Vlan-interface101] pim bsr-boundary
[SwitchB-Vlan-interface101] quit
```

### (3) 配置 Loopback0 接口和 C-BSR、C-RP 的位置

# 在 Switch A 上配置 Loopback0 接口和 C-BSR、C-RP 的位置。

```
[SwitchA] interface loopback 0
[SwitchA-LoopBack0] ip address 1.1.1.1 32
[SwitchA-LoopBack0] pim sm
[SwitchA-LoopBack0] quit
[SwitchA] pim
[SwitchA-pim] c-bsr hash-length 32
[SwitchA-pim] c-bsr priority 20
[SwitchA-pim] c-bsr loopback 0
[SwitchA-pim] c-rp loopback 0
[SwitchA-pim] quit
```

# 在 Switch B 上配置 Loopback0 接口和 C-BSR、C-RP 的位置。

```
[SwitchB] interface loopback 0
[SwitchB-LoopBack0] ip address 2.2.2.2 32
[SwitchB-LoopBack0] pim sm
[SwitchB-LoopBack0] quit
[SwitchB] pim
[SwitchB-pim] c-bsr hash-length 32
[SwitchB-pim] c-bsr priority 20
[SwitchB-pim] c-bsr loopback 0
[SwitchB-pim] c-rp loopback 0
[SwitchB-pim] quit
```

### (4) 配置 BGP 协议，配置 MBGP 对等体，并互相引入路由

# 在 Switch A 上配置 EBGP 邻接关系、配置 MBGP 对等体。

```
[SwitchA] bgp 100
[SwitchA-bgp] router-id 1.1.1.1
[SwitchA-bgp] peer 192.168.1.2 as-number 200
[SwitchA-bgp] import-route direct
[SwitchA-bgp] ipv4-family multicast
[SwitchA-bgp-af-mul] peer 192.168.1.2 enable
[SwitchA-bgp-af-mul] import-route direct
[SwitchA-bgp-af-mul] quit
[SwitchA-bgp] quit
```

# 在 Switch B 上配置 EBGP 邻接关系、配置 MBGP 对等体，并引入 OSPF 路由。

```
[SwitchB] bgp 200
[SwitchB-bgp] router-id 2.2.2.2
[SwitchB-bgp] peer 192.168.1.1 as-number 100
[SwitchB-bgp] import-route ospf 1
[SwitchB-bgp] ipv4-family multicast
[SwitchB-bgp-af-mul] peer 192.168.1.1 enable
[SwitchB-bgp-af-mul] import-route ospf 1
```

```
[SwitchB-bgp-af-mul] quit
```

```
[SwitchB-bgp] quit
```

#### (5) 配置 MSDP 对等体

# 在 Switch A 上配置 MSDP 对等体。

```
[SwitchA] msdp
```

```
[SwitchA-msdp] peer 192.168.1.2 connect-interface vlan-interface 101
```

```
[SwitchA-msdp] quit
```

# 在 Switch B 上配置 MSDP 对等体。

```
[SwitchB] msdp
```

```
[SwitchB-msdp] peer 192.168.1.1 connect-interface vlan-interface 101
```

```
[SwitchB-msdp] quit
```

#### (6) 检验配置效果

通过使用 **display bgp multicast peer** 命令可以查看交换机之间 MBGP 对等体的关系。例如：

# 查看 Switch B 上 MBGP 对等体关系的信息。

```
[SwitchB] display bgp multicast peer
```

```
BGP local router ID : 2.2.2.2
Local AS number : 200
Total number of peers : 3 Peers in established state : 3
```

| Peer        | V | AS  | MsgRcvd | MsgSent | OutQ | PrefRcv | Up/Down  | State       |
|-------------|---|-----|---------|---------|------|---------|----------|-------------|
| 192.168.1.1 | 4 | 100 | 56      | 56      | 0    | 0       | 00:40:54 | Established |

通过使用 **display msdp brief** 命令可以查看交换机之间 MSDP 对等体建立情况。例如：

# 查看 Switch B 上 MSDP 对等体建立情况的简要信息。

```
[SwitchB] display msdp brief
```

MSDP Peer Brief Information of VPN-Instance: public net

| Configured | Up | Listen | Connect | Shutdown | Down |
|------------|----|--------|---------|----------|------|
| 1          | 1  | 0      | 0       | 0        | 0    |

| Peer's Address | State | Up/Down time | AS  | SA Count | Reset Count |
|----------------|-------|--------------|-----|----------|-------------|
| 192.168.1.1    | Up    | 00:07:17     | 100 | 1        | 0           |

## 5. 完整配置

### • SwitchA 的完整配置

```
#
```

```
multicast routing-enable
```

```
#
```

```
vlan 100 to 101
```

```
#
```

```
interface Vlan-interface100
```

```
pim sm
```

```
#
```

```
interface Vlan-interface101
```

```
pim bsr-boundary
```

```

pim sm
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
 pim sm
#
bgp 100
 router-id 1.1.1.1
 import-route direct
 undo synchronization
 peer 192.168.1.2 as-number 200
#
 ipv4-family multicast
 import-route direct
 peer 192.168.1.2 enable
#
pim
 c-bsr hash-length 32
 c-bsr priority 20
 c-bsr LoopBack0
 c-rp LoopBack0
#
msdp
 peer 192.168.1.2 connect-interface Vlan-interface101

```

- SwitchB 的完整配置

```

#
 multicast routing-enable
#
vlan 101 to 103
#
interface Vlan-interface101
 pim bsr-boundary
 pim sm
#
interface Vlan-interface102
 pim sm
#
interface Vlan-interface103
 pim sm
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
 pim sm
#
bgp 200
 router-id 2.2.2.2
 import-route ospf 1
 undo synchronization

```

```

peer 192.168.1.1 as-number 100
#
ipv4-family multicast
import-route ospf 1
peer 192.168.1.1 enable
#
pim
c-bsr hash-length 32
c-bsr priority 20
c-bsr LoopBack0
c-rp LoopBack0
#
msdp
peer 192.168.1.1 connect-interface Vlan-interface101

```

- SwitchC 的完整配置

```

#
multicast routing-enable
#
vlan 102
#
vlan 104
#
vlan200
#
interface Vlan-interface102
pim sm
#
interface Vlan-interface104
pim sm
#
interface Vlan-interface200
igmp enable
pim sm

```

- SwitchD 的完整配置

```

#
multicast routing-enable
#
vlan 103 to 104
#
interface Vlan-interface103
pim sm
#
interface Vlan-interface104
pim sm

```

## 6. 配置注意事项

- 通过 **import-route** 命令引入到 MBGP 路由表中的路由的 ORIGIN 属性为 Incomplete。



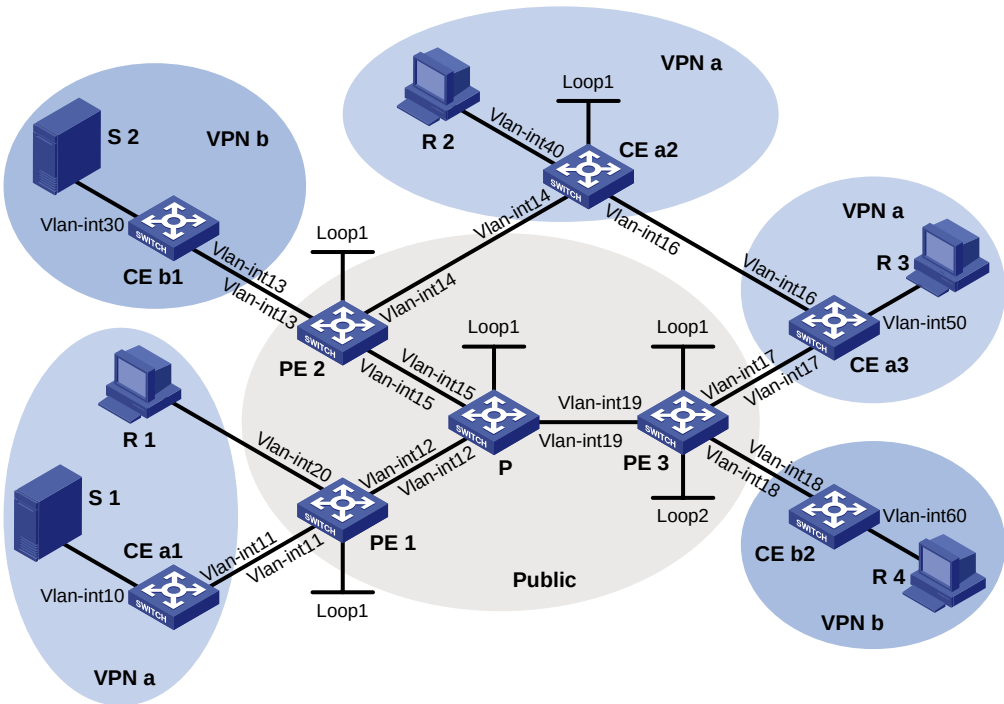
- 配置 IPv4 MBGP 对等体组的前提是，在 BGP-IPv4 组播地址族下存在已经使能的 IPv4 单播对等体组。

## 1.8 组播 VPN 典型配置指导

### 1.8.1 单 AS 内的 MD VPN 典型配置指导

#### 1. 组网图

图1-18 单 AS 内 MD VPN 配置组网图



| 设备   | 接口         | IP 地址          | 设备    | 接口         | IP 地址          |
|------|------------|----------------|-------|------------|----------------|
| S 1  | -          | 10.110.7.2/24  | PE 3  | Vlan-int19 | 192.168.8.1/24 |
| S 2  | -          | 10.110.8.2/24  |       | Vlan-int17 | 10.110.5.1/24  |
| R 1  | -          | 10.110.1.2/24  |       | Vlan-int18 | 10.110.6.1/24  |
| R 2  | -          | 10.110.9.2/24  |       | Loop1      | 1.1.1.3/32     |
| R 3  | -          | 10.110.10.2/24 |       | Loop2      | 33.33.33.33/32 |
| R 4  | -          | 10.110.11.2/24 | CE a1 | Vlan-int10 | 10.110.7.1/24  |
| P    | Vlan-int12 | 192.168.6.2/24 | CE a2 | Vlan-int11 | 10.110.2.2/24  |
|      | Vlan-int15 | 192.168.7.2/24 |       | Vlan-int14 | 10.110.4.2/24  |
|      | Vlan-int19 | 192.168.8.2/24 |       | Vlan-int16 | 10.110.12.1/24 |
|      | Loop1      | 2.2.2.2/32     |       | Loop1      | 22.22.22.22/32 |
| PE 1 | Vlan-int12 | 192.168.6.1/24 | CE a3 | Vlan-int50 | 10.110.10.1/24 |
|      | Vlan-int20 | 10.110.1.1/24  |       | Vlan-int17 | 10.110.5.2/24  |
|      | Vlan-int11 | 10.110.2.1/24  |       | Vlan-int16 | 10.110.12.2/24 |
|      | Loop1      | 1.1.1.1/32     | CE b1 | Vlan-int30 | 10.110.8.1/24  |
| PE 2 | Vlan-int15 | 192.168.7.1/24 |       | Vlan-int13 | 10.110.3.2/24  |
|      | Vlan-int13 | 10.110.3.1/24  | CE b2 | Vlan-int60 | 10.110.11.1/24 |
|      | Vlan-int14 | 10.110.4.1/24  |       | Vlan-int18 | 10.110.6.2/24  |
|      | Loop1      | 1.1.1.2/32     |       |            |                |

#### 2. 应用要求

应用要求如 表 1-18所示。

表1-18 单 AS 内的 MD VPN 配置组网需求

| 项目                | 组网需求                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 组播源和接收者           | <ul style="list-style-type: none"> <li>• VPN a 中的组播源为 S 1，接收者为 R 1、R 2 和 R 3</li> <li>• VPN b 中的组播源为 S 2，接收者为 R 4</li> <li>• VPN a 中的 Share-Group 地址为 239.1.1.1</li> <li>• VPN b 中的 Share-Group 地址为 239.2.2.2</li> </ul>                                                                                                                                                                  |
| PE 上各接口所属的 VPN 实例 | <ul style="list-style-type: none"> <li>• PE 1: Vlan-interface11 和 Vlan-interface20 属于 VPN 实例 a，Vlan-interface12 和 Loopback1 属于公网实例</li> <li>• PE 2: Vlan-interface13 属于 VPN 实例 b，Vlan-interface14 属于 VPN 实例 a，Vlan-interface15 和 Loopback1 属于公网实例</li> <li>• PE 3: Vlan-interface17 属于 VPN 实例 a，Vlan-interface18 和 Loopback2 属于 VPN 实例 b，Vlan-interface19 和 Loopback1 接口属于公网实例</li> </ul> |
| 单播路由协议和 MPLS      | <ul style="list-style-type: none"> <li>• 在公网中配置 OSPF，在各 PE 与 CE 之间配置 RIP</li> <li>• 在 PE 1、PE 2 和 PE 3 各自的 Loopback1 接口之间建立 BGP 对等体连接并传递所有私网路由</li> <li>• 在公网中配置 MPLS</li> </ul>                                                                                                                                                                                                          |
| IP 组播路由功能         | <ul style="list-style-type: none"> <li>• 在 P 上使能 IP 组播路由</li> <li>• 在 PE 1、PE 2 和 PE 3 的公网实例中均使能 IP 组播路由</li> <li>• 在 PE 1、PE 2 和 PE 3 的 VPN 实例 a 中均使能 IP 组播路由</li> <li>• 在 PE 2 和 PE 3 的 VPN 实例 b 中均使能 IP 组播路由</li> <li>• 在 CE a1、CE a2、CE a3、CE b1 和 CE b2 上均使能 IP 组播路由</li> </ul>                                                                                                      |
| IGMP 功能           | <ul style="list-style-type: none"> <li>• 在 PE 1 的 Vlan-interface20 接口上使能 IGMPv2</li> <li>• 在 CE a2 的 Vlan-interface40、CE a3 的 Vlan-interface50 和 CE b2 的 Vlan-interface60 接口上分别使能 IGMPv2</li> </ul>                                                                                                                                                                                       |
| PIM 功能            | <ul style="list-style-type: none"> <li>• 在 P 的所有接口上均使能 PIM-SM</li> <li>• 在 PE 1、PE 2 和 PE 3 的所有公网和私网接口上均使能 PIM-SM</li> <li>• 在 CE a1、CE a2、CE a3、CE b1 和 CE b2 的所有接口上均使能 PIM-SM</li> <li>• P 的 Loopback1 接口为公网的 C-BSR 和 C-RP（服务于所有组播组）</li> <li>• CE a2 的 Loopback1 接口为 VPN a 的 C-BSR 和 C-RP（服务于所有组播组）</li> <li>• PE 3 的 Loopback2 接口为 VPN b 的 C-BSR 和 C-RP（服务于所有组播组）</li> </ul>          |

# 目 录

|                                       |      |
|---------------------------------------|------|
| 1 IPv6 组播典型配置指导 .....                 | 1-1  |
| 1.1 MLD典型配置指导 .....                   | 1-1  |
| 1.1.1 MLD基本功能配置指导 .....               | 1-1  |
| 1.1.2 MLD SSM Mapping功能典型配置指导 .....   | 1-4  |
| 1.2 MLD Snooping典型配置指导 .....          | 1-8  |
| 1.2.1 IPv6 组策略模拟主机加入配置指导 .....        | 1-8  |
| 1.2.2 静态端口配置指导 .....                  | 1-12 |
| 1.2.3 MLD Snooping查询器配置指导 .....       | 1-17 |
| 1.3 IPv6 组播VLAN典型配置指导 .....           | 1-20 |
| 1.3.1 基于子VLAN的IPv6 组播VLAN典型配置指导 ..... | 1-20 |
| 1.3.2 基于端口的IPv6 组播VLAN典型配置指导 .....    | 1-23 |
| 1.4 IPv6 PIM典型配置指导 .....              | 1-27 |
| 1.4.1 IPv6 PIM-DM典型配置指导 .....         | 1-27 |
| 1.4.2 IPv6 PIM-SM典型配置指导 .....         | 1-31 |
| 1.4.3 IPv6 PIM-SSM典型配置指导 .....        | 1-38 |
| 1.5 IPv6 MBGP典型配置指导 .....             | 1-42 |
| 1.5.1 IPv6 MBGP典型配置指导 .....           | 1-42 |

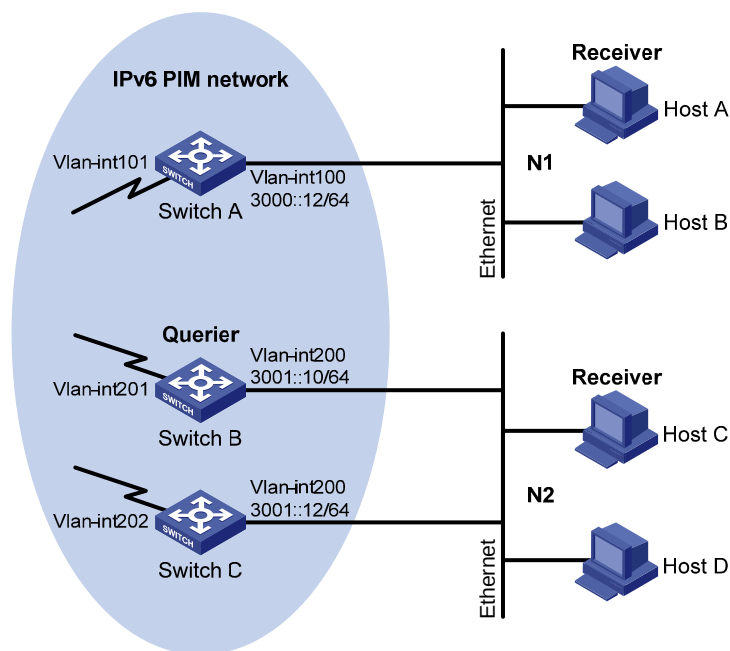
# 1 IPv6 组播典型配置指导

## 1.1 MLD 典型配置指导

### 1.1.1 MLD 基本功能配置指导

#### 1. 组网图

图1-1 MLD 基本功能配置组网图



#### 2. 组网需求

- 接收者通过组播方式接收视频点播信息，不同组织的接收者组成末梢网络 N1 和 N2，Host A 与 Host C 分别为 N1 和 N2 中的组播信息接收者。
- IPv6 PIM 网络中的 Switch A 连接 N1，Switch B 与 Switch C 共同连接 N2。
- Switch A 通过 Vlan-interface100 连接 N1，通过 Vlan-interface101 连接 IPv6 PIM 网络中的其它设备。
- Switch B 与 Switch C 分别通过各自的 Vlan-interface200 连接 N2，并分别通过 Vlan-interface201 和 Vlan-interface202 连接 IPv6 PIM 网络中的其它设备。
- Switch A 与 N1 之间运行 MLDv1；Switch B 和 Switch C 与 N2 之间也分别运行 MLDv1。且由于 Switch B 的接口 IP 地址较小，因此在 N2 中通常由其来充当 IGMP 查询器。
- 配置 SwitchA 发送 MLD 普遍组查询报文的时间间隔为 30 秒，最大响应时间为 5 秒，发送 MLD 特定组查询报文的时间间隔为 2 秒。

### 3. 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

| 产品              | 软件版本              | 硬件版本    |
|-----------------|-------------------|---------|
| S7500E 系列以太网交换机 | Release 6300 软件版本 | 全系列硬件版本 |

### 4. 配置过程 and 解释

(1) 使能 IPv6 转发功能，并配置 IPv6 地址和 IPv6 单播路由协议

使能各交换机的IPv6 转发功能，并按照 图 1-1配置各接口的IP地址和前缀长度，具体配置过程略。

配置 IPv6 PIM 网络内的各交换机之间采用 OSPFv3 协议进行互连，确保 IPv6 PIM 网络内部在网络层互通，并且各交换机之间能够借助单播路由协议实现动态路由更新，具体配置过程略。

(2) 使能 IPv6 组播路由，并使能 IPv6 PIM-DM 和 MLD

# 在 Switch A 上使能 IPv6 组播路由，在各接口上使能 IPv6 PIM-DM，并在主机侧接口 Vlan-interface100 上使能 MLD。

```
<SwitchA> system-view
[SwitchA] multicast ipv6 routing-enable
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] mld enable
[SwitchA-Vlan-interface100] pim ipv6 dm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim ipv6 dm
[SwitchA-Vlan-interface101] quit
```

# 在 SwitchA 上配置发送 MLD 通用组查询报文的时间间隔、最大响应时间，以及发送特定组查询报文的时间间隔。

```
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] mld timer query 30
[SwitchA-Vlan-interface100] mld max-response-time 5
[SwitchA-Vlan-interface100] mld last-listener-query-interval 2
```

# 在 Switch B 上使能 IPv6 组播路由，在各接口上使能 IPv6 PIM-DM，并在主机侧接口 Vlan-interface200 上使能 MLD。

```
<SwitchB> system-view
[SwitchB] multicast ipv6 routing-enable
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] mld enable
[SwitchB-Vlan-interface200] pim ipv6 dm
[SwitchB-Vlan-interface200] quit
[SwitchB] interface vlan-interface 201
[SwitchB-Vlan-interface201] pim ipv6 dm
[SwitchB-Vlan-interface201] quit
```

# 在 Switch C 上使能 IPv6 组播路由，在各接口上使能 IPv6 PIM-DM，并在主机侧接口 Vlan-interface200 上使能 MLD。

```

<SwitchC> system-view
[SwitchC] multicast ipv6 routing-enable
[SwitchC] interface vlan-interface 200
[SwitchC-Vlan-interface200] mld enable
[SwitchC-Vlan-interface200] pim ipv6 dm
[SwitchC-Vlan-interface200] quit
[SwitchC] interface vlan-interface 202
[SwitchC-Vlan-interface202] pim ipv6 dm
[SwitchC-Vlan-interface202] quit

```

### (3) 检查配置效果

通过使用 **display mld interface** 命令可以查看各交换机接口上 MLD 的配置和运行情况。例如：

# 查看 Switch B 在 Vlan-interface200 上的 MLD 信息。

```

[SwitchB] display mld interface vlan-interface 200
Vlan-interface200(FE80::200:5EFF:FE66:5100):
 MLD is enabled
 Current MLD version is 1
 Value of query interval for MLD(in seconds): 125
 Value of other querier present interval for MLD(in seconds): 255
 Value of maximum query response time for MLD(in seconds): 10
 Querier for MLD: FE80::200:5EFF:FE66:5100 (this router)
 Total 1 MLD Group reported

```

## 5. 完整配置

SwitchA、SwitchB 和 SwitchC 的完整配置类似，下面以 SwitchA 的完整配置为例：

```

#
multicast ipv6 routing-enable
#
vlan 100 to 101
#
interface Vlan-interface100
 mld enable
 mld timer query 30
 mld max-response-time 5
 mld last-listener-query-interval 2
 pim ipv6 dm
#
interface Vlan-interface101
 pim ipv6 dm

```

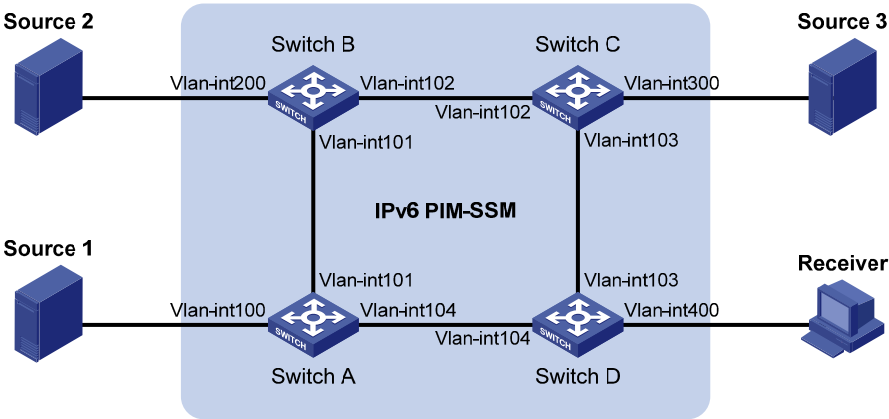
## 6. 配置注意事项

应确保发送 MLD 普遍组查询报文的时间间隔大于 MLD 普遍组查询的最大响应时间，否则有可能造成对 IPv6 组播组成员的误删除。

1.1.2 MLD SSM Mapping 功能典型配置指导

1. 组网图

图1-2 MLD SSM Mapping 功能配置组网图



| 设备       | 接口          | IP 地址      | 设备       | 接口          | IP 地址      |
|----------|-------------|------------|----------|-------------|------------|
| Source 1 | -           | 1001::1/64 | Source 3 | -           | 3001::1/64 |
| Source 2 | -           | 2001::1/64 | Receiver | -           | 4001::1/64 |
| Switch A | Vlan-int100 | 1001::2/64 | Switch C | Vlan-int300 | 3001::2/64 |
|          | Vlan-int101 | 1002::1/64 |          | Vlan-int103 | 3002::1/64 |
|          | Vlan-int104 | 1003::1/64 |          | Vlan-int102 | 2002::2/64 |
| Switch B | Vlan-int200 | 2001::2/64 | Switch D | Vlan-int400 | 4001::2/64 |
|          | Vlan-int101 | 1002::2/64 |          | Vlan-int103 | 3002::2/64 |
|          | Vlan-int102 | 2002::1/64 |          | Vlan-int104 | 1003::2/64 |

2. 组网需求

- 在 IPv6 PIM-SSM 网络中，接收者通过组播方式接收视频点播信息。接收者主机运行 MLDv1，且不能升级至 MLDv2，因此在加入 IPv6 组播组时无法指定 IPv6 组播源。
- 接收者主机加入的组播组范围为 FF3E::/64。
- 要求通过在 Switch D 上配置 MLD SSM Mapping 功能，以使接收者主机只接收来自 Source 1 和 Source 3 的 IPv6 组播数据。

3. 适用产品、版本

表1-2 配置适用的产品与软硬件版本关系

| 产品              | 软件版本              | 硬件版本    |
|-----------------|-------------------|---------|
| S7500E 系列以太网交换机 | Release 6300 软件版本 | 全系列硬件版本 |

4. 配置过程 and 解释

(1) 使能 IPv6 转发功能，并配置 IPv6 地址和 IPv6 单播路由协议

使能各交换机的IPv6 转发功能，并按照 图 1-2配置各接口的IPv6 地址和前缀长度，具体配置过程略。  
配置 PIM-SSM 网络内的各交换机之间采用 OSPFv3 协议进行互连，确保 IPv6 PIM-SSM 网络内部在网络层互通，并且各交换机之间能够借助单播路由协议实现动态路由更新，具体配置过程略。

(2) 使能 IPv6 组播路由，并使能 IPv6 PIM-SM、MLD 和 MLD SSM Mapping 功能

# 在 Switch D 上使能 IPv6 组播路由，在各接口上使能 IPv6 PIM-SM，并在主机侧接口 Vlan-interface400 上使能 MLD 和 MLD SSM Mapping 功能，配置 MLD 版本为 2。

```

<SwitchD> system-view
[SwitchD] multicast ipv6 routing-enable
[SwitchD] interface vlan-interface 400
[SwitchD-Vlan-interface400] mld enable
[SwitchD-Vlan-interface400] mld version 2
[SwitchD-Vlan-interface400] mld ssm-mapping enable
[SwitchD-Vlan-interface400] pim ipv6 sm
[SwitchD-Vlan-interface400] quit
[SwitchD] interface vlan-interface 103
[SwitchD-Vlan-interface103] pim ipv6 sm
[SwitchD-Vlan-interface103] quit
[SwitchD] interface vlan-interface 104
[SwitchD-Vlan-interface104] pim ipv6 sm
[SwitchD-Vlan-interface104] quit

```

# 在 Switch A 上使能 IPv6 组播路由，并在各接口上使能 IPv6 PIM-SM。

```

<SwitchA> system-view
[SwitchA] multicast ipv6 routing-enable
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] pim ipv6 sm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim ipv6 sm
[SwitchA-Vlan-interface101] quit
[SwitchA] interface vlan-interface 104
[SwitchA-Vlan-interface104] pim ipv6 sm
[SwitchA-Vlan-interface104] quit

```

Switch B 和 Switch C 的配置与 Switch A 相似，配置过程略。

### (3) 配置 C-BSR 和 C-RP

# 在 Switch D 上配置 C-BSR 和 C-RP 的位置。

```

[SwitchD] pim ipv6
[SwitchD-pim6] c-bsr 1003::2
[SwitchD-pim6] c-rp 1003::2
[SwitchD-pim6] quit

```

### (4) 配置 IPv6 SSM 组播组的地址范围

# 在 Switch D 上配置 IPv6 SSM 组播组的地址范围为 FF3E::/64。

```

[SwitchD] acl ipv6 number 2000
[SwitchD-acl6-basic-2000] rule permit source ff3e:: 64
[SwitchD-acl6-basic-2000] quit
[SwitchD] pim ipv6
[SwitchD-pim6] ssm-policy 2000
[SwitchD-pim6] quit

```

Switch A、Switch B 和 Switch C 的配置与 Switch D 相似，配置过程略。

### (5) 配置 MLD SSM Mapping 规则

# 在 Switch D 上配置 MLD SSM Mapping 规则。



```
[SwitchD] mld
[SwitchD-mld] ssm-mapping ff3e::101 64 1001::1
[SwitchD-mld] ssm-mapping ff3e::101 64 3001::1
[SwitchD-mld] quit
```

#### (6) 检验配置效果

通过使用 **display mld ssm-mapping** 命令可以查看交换机上的 MLD SSM Mapping 规则。例如：

# 查看 Switch D 上 IPv6 组播组 FF3E::101 的 MLD SSM Mapping 规则。

```
[SwitchD] display mld ssm-mapping ff3e::101
Group: FF3E::101
Source list:
 1001::1
 3001::1
```

通过使用 **display mld ssm-mapping group** 命令可以查看交换机上依据 MLD SSM Mapping 规则创建的 IPv6 组播组信息。例如：

# 查看 Switch D 上依据 MLD SSM Mapping 规则创建的 IPv6 组播组信息。

```
[SwitchD] display mld ssm-mapping group
Total 1 MLD SSM-mapping Group(s).
Interface group report information
Vlan-interface400 (4001::2):
 Total 1 MLD SSM-mapping Group reported
 Group Address: FF3E::101
 Last Reporter: 4001::1
 Uptime: 00:02:04
 Expires: off
```

通过使用 **display pim ipv6 routing-table** 命令可以查看交换机的 IPv6 PIM 路由表信息。例如：

# 查看 Switch D 上 IPv6 PIM 路由表信息。

```
[SwitchD] display pim ipv6 routing-table
Total 0 (*, G) entry; 2 (S, G) entry

(1001::1, FF3E::101)
 Protocol: pim-ssm, Flag:
 UpTime: 00:13:25
 Upstream interface: Vlan-interface104
 Upstream neighbor: 1003::1
 RPF prime neighbor: 1003::1
 Downstream interface(s) information:
 Total number of downstreams: 1
 1: Vlan-interface400
 Protocol: mld, UpTime: 00:13:25, Expires: -

(3001::1, FF3E::101)
 Protocol: pim-ssm, Flag:
 UpTime: 00:13:25
 Upstream interface: Vlan-interface103
 Upstream neighbor: 3002::1
```

```
RPF prime neighbor: 3002::1
Downstream interface(s) information:
Total number of downstreams: 1
1: Vlan-interface400
Protocol: mld, UpTime: 00:13:25, Expires: -
```

## 5. 完整配置

- DeviceD 的完整配置

```
#
multicast ipv6 routing-enable
#
acl ipv6 number 2000
rule permit source ff3e:: 64
#
vlan 103 to 104
#
vlan 400
#
interface Vlan-interface103
pim ipv6 sm
#
interface Vlan-interface104
pim ipv6 sm
#
interface Vlan-interface400
mld enable
mld version 2
mld ssm-mapping enable
#
mld
ssm-mapping ff3e::101 64 1001::1
ssm-mapping ff3e::101 64 3001::1
#
pim ipv6
c-bsr 1003::2
c-rp 1003::2
ssm-policy 2000
```

- DeviceA 的配置

```
#
multicast ipv6 routing-enable
#
acl ipv6 number 2000
rule permit source ff3e:: 64
#
vlan 100 to 101
#
vlan 104
#
```

```

interface Vlan-interface100
pim ipv6 sm
#
interface Vlan-interface101
pim ipv6 sm
#
interface Vlan-interface104
pim ipv6 sm

```

DeviceB 和 DeviceC 的配置与 DeviceA 的基本一致，仅 VLAN 接口编号存在差异，这里不再赘述。

## 6. 配置注意事项

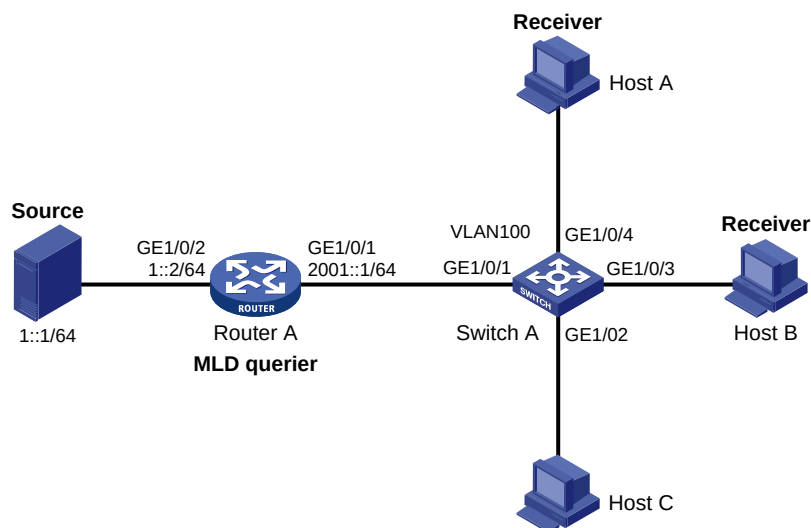
- 为保证本网段内运行任意版本 MLD 的接收者主机都能得到 SSM 服务，建议在处于该网段的接口上运行 MLDv2。
- 对于同时支持 MLD Snooping 和 MLD 的交换机来说，若 VLAN 接口上运行的是 MLDv2，则在使用 **mld-snooping host-join** 命令配置模拟主机加入时即便不指定 IPv6 组播源，模拟主机也仍将发送 MLDv2 的报告报文，这种情况下不会依据 MLD SSM Mapping 规则创建相应的 IPv6 组播组。

## 1.2 MLD Snooping 典型配置指导

### 1.2.1 IPv6 组策略模拟主机加入配置指导

#### 1. 组网图

图1-3 模拟主机加入配置组网图



#### 2. 应用要求

- 如图 1-3所示，Router A通过GigabitEthernet1/0/2 接口连接IPv6 组播源（Source），通过 GigabitEthernet1/0/1 接口连接Switch A；
- Router A 与 Switch A之间运行 MLDv1，Switch A上运行版本 1 的 MLD Snooping，并由 Router A 充当 MLD 查询器；

- 通过配置，使连接在 Switch A 上的接收者（Receiver）Host A 和 Host B 只能接收发往 IPv6 组播组 FF1E::101 的 IPv6 组播数据；
- 要求通过配置，使连接在 Switch A 上的接收者（Receiver）Host A 和 Host B 即使由于突然出现了某种意外而临时中断接收 IPv6 组播数据时，IPv6 组播数据也能够不间断地通过 Switch A 的接口 GigabitEthernet1/0/3 和 GigabitEthernet1/0/4 转发出去。

### 3. 适用产品、版本

表1-3 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本                         |
|-------------------|---------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本               | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本               | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6300 软件版本               | 全系列硬件版本                      |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本                      |

### 4. 配置过程和解释

#### (1) 配置各设备接口的 IPv6 地址

请按照 图 1-3 配置各接口的 IPv6 地址和前缀长度，具体配置过程略。

#### (2) 配置 Router A

# 使能 IPv6 组播路由，在各接口上使能 IPv6 PIM-DM，并在接口 GigabitEthernet1/0/1 上使能 MLDv1。

```
<RouterA> system-view
[RouterA] multicast ipv6 routing-enable
[RouterA] interface GigabitEthernet 1/0/1
[RouterA-GigabitEthernet1/0/1] mld enable
[RouterA-GigabitEthernet1/0/1] pim ipv6 dm
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface GigabitEthernet 1/0/2
[RouterA-GigabitEthernet1/0/2] pim ipv6 dm
[RouterA-GigabitEthernet1/0/2] quit
```

#### (3) 配置 Switch A

# 全局使能 MLD Snooping。

```
<SwitchA> system-view
[SwitchA] mld-snooping
[SwitchA-mld-snooping] quit
```

# 创建 VLAN 100，把端口 GigabitEthernet1/0/1 到 GigabitEthernet1/0/4 添加到该 VLAN 中，并在该 VLAN 内使能 MLD Snooping，并使能丢弃未知 IPv6 组播数据报文功能。。

```
[SwitchA] vlan 100
[SwitchA-vlan100] port GigabitEthernet 1/0/1 to GigabitEthernet 1/0/4
[SwitchA-vlan100] mld-snooping enable
[SwitchA-vlan100] mld-snooping drop-unknown
[SwitchA-vlan100] quit
```

# 配置 IPv6 组播组过滤器，使 VLAN 100 内的主机只能加入 IPv6 组播组 FF1E::101。

```
[SwitchA] acl ipv6 number 2001
[SwitchA-acl6-basic-2001] rule permit source ff1e::101 128
[SwitchA-acl6-basic-2001] quit
[SwitchA] mld-snooping
[SwitchA-mld-snooping] group-policy 2001 vlan 100
[SwitchA-mld-snooping] quit
```

# 在 GigabitEthernet1/0/3 和 GigabitEthernet1/0/4 上分别使能模拟主机加入功能。

```
[SwitchA] interface GigabitEthernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] mld-snooping host-join ff1e::101 vlan 100
[SwitchA-GigabitEthernet1/0/3] quit
[SwitchA] interface GigabitEthernet 1/0/4
[SwitchA-GigabitEthernet1/0/4] mld-snooping host-join ff1e::101 vlan 100
[SwitchA-GigabitEthernet1/0/4] quit
```

#### (4) 检验配置效果

# 查看 Switch A 上 VLAN 100 内 MLD Snooping 组播组的详细信息。

```
[SwitchA] display mld-snooping group vlan 100 verbose
 Total 1 IP Group(s).
 Total 1 IP Source(s).
 Total 1 MAC Group(s).

 Port flags: D-Dynamic port, S-Static port, A-Aggregation port, C-Copy port
 Subvlan flags: R-Real VLAN, C-Copy VLAN
 Vlan(id):100.
 Total 1 IP Group(s).
 Total 1 IP Source(s).
 Total 1 MAC Group(s).
 Router port(s):total 1 port.
 GE1/0/1 (D) (00:01:30)
 IP group(s):the following ip group(s) match to one mac group.
 IP group address:FF1E::101
 (:, FF1E::101):
 Attribute: Host Port
 Host port(s):total 2 port.
 GE1/0/3 (D) (00:03:23)
 GE1/0/4 (D) (00:03:23)
 MAC group(s):
 MAC group address:3333-0000-1001
 Host port(s):total 2 port.
```

```
GE1/0/3
```

```
GE1/0/4
```

由此可见，Switch A 上的端口 GigabitEthernet1/0/3 和 GigabitEthernet1/0/4 已经加入了 IPv6 组播组 (::, FF1E::101)。

## 5. 完整配置

### (1) SwitchA 配置信息

```
#
acl ipv6 number 2001
 rule permit source ff1e::101 128
#
mld-snooping
 group-policy 2001 vlan 100
#
vlan 100
 mld-snooping enable
 mld-snooping drop-unknown #
#
interface GigabitEthernet1/0/1
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port access vlan 100
#
interface GigabitEthernet1/0/3
 port access vlan 100
 mld-snooping host-join ff1e::101 vlan 100
#
interface GigabitEthernet1/0/4
 port access vlan 100
 mld-snooping host-join ff1e::101 vlan 100
#
```

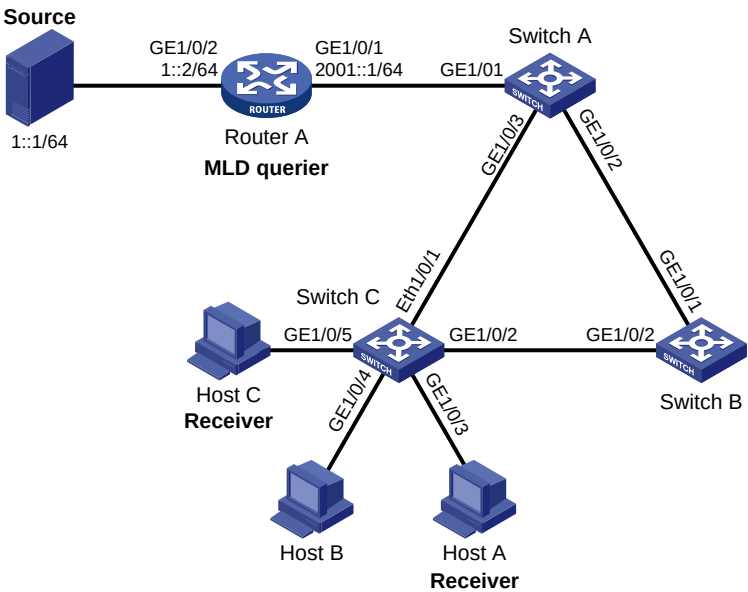
## 6. 配置注意事项

- 二、三层组播协议可以同时运行在交换机上，但是在同一个 VLAN 和该 VLAN 对应的虚接口上不能同时运行二层和三层组播协议。
- 在启动指定 VLAN 的 MLD Snooping 前，应首先在系统视图下启动全局 MLD Snooping 功能，否则将无法配置成功。
- 与静态成员端口不同，配置了模拟主机加入的端口会作为动态成员端口而参与动态成员端口的老化过程。

## 1.2.2 静态端口配置指导

### 1. 组网图

图1-4 静态路由器端口配置组网图



### 2. 应用要求

- 当某些组播接收者需要固定、稳定的接收到某个组播组的数据时，可以配置静态端口来增强组播数据在传输过程中的可靠性。
- 如图 1-4所示，Router A通过GigabitEthernet1/0/2 接口连接IPv6 组播源（Source），通过GigabitEthernet1/0/1 接口连接Switch A；
- Router A 与 Switch A 之间运行 MLD，Switch A、Switch B 和 Switch C 上运行 MLD Snooping，并由 Router A 充当 MLD 查询器；
- 假设由于受 STP 等链路层协议的影响，为了避免出现环路，Switch A—Switch C 的转发路径在正常情况下是阻断的，IPv6 组播数据只能通过 Switch A—Switch B—Switch C 的路径传递给连接在 Switch C 上的接收者（Receiver）Host A 和 Host C；
- 要求通过将 Switch A 上连接 Switch C 的端口 GigabitEthernet1/0/3 配置为静态路由器端口，从而保证当 Switch A—Switch B—Switch C 的路径出现阻断时，IPv6 组播数据可以几乎不间断地通过 Switch A—Switch C 的新路径传递给接收者。
- 将 SwitchC 的端口 GigabitEthernet1/0/3 和 GigabitEthernet1/0/5 配置为静态成员端口，从而保证这两个端口下连接的主机能固定接收组播组 FF1E::101 的组播数据。



#### 说明

如果没有配置静态路由器端口，那么当 Switch A—Switch B—Switch C 的路径出现阻断时，至少需要等待一个 MLD 查询和响应周期完成后，IPv6 组播数据才能通过 Switch A—Switch C 的新路径传递给接收者，IPv6 组播数据的传输在这个过程中将中断。

### 3. 适用产品、版本

表1-4 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本                         |
|-------------------|---------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本               | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本               | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6300 软件版本               | 全系列硬件版本                      |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本                      |

### 4. 配置过程和解释

#### (1) 配置各设备接口的 IPv6 地址

请按照 图 1-4配置各接口的IPv6 地址和前缀长度，具体配置过程略。

#### (2) 配置 Router A

# 使能 IPv6 组播路由, 在各接口上使能 IPv6 PIM-DM, 并在接口 GigabitEthernet1/0/1 上使能 MLD。

```
<RouterA> system-view
[RouterA] multicast ipv6 routing-enable
[RouterA] interface GigabitEthernet 1/0/1
[RouterA-GigabitEthernet1/0/1] mld enable
[RouterA-GigabitEthernet1/0/1] pim ipv6 dm
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface GigabitEthernet 1/0/2
[RouterA-GigabitEthernet1/0/2] pim ipv6 dm
[RouterA-GigabitEthernet1/0/2] quit
```

#### (3) 配置 Switch A

# 全局使能 MLD Snooping。

```
<SwitchA> system-view
[SwitchA] mld-snooping
[SwitchA-mld-snooping] quit
```

# 创建 VLAN 100, 把端口 GigabitEthernet1/0/1 到 GigabitEthernet1/0/3 添加到该 VLAN 中, 并在该 VLAN 内使能 MLD Snooping。

```
[SwitchA] vlan 100
[SwitchA-vlan100] port GigabitEthernet 1/0/1 to GigabitEthernet 1/0/3
[SwitchA-vlan100] mld-snooping enable
[SwitchA-vlan100] quit
```

# 把 GigabitEthernet1/0/3 配置为静态路由器端口。

```
[SwitchA] interface GigabitEthernet 1/0/3
```



```
[SwitchA-GigabitEthernet1/0/3] mld-snooping static-router-port vlan 100
```

```
[SwitchA-GigabitEthernet1/0/3] quit
```

#### (4) 配置 Switch B

# 全局使能 MLD Snooping。

```
<SwitchB> system-view
```

```
[SwitchB] mld-snooping
```

```
[SwitchB-mld-snooping] quit
```

# 创建 VLAN 100，把端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 添加到该 VLAN 中，并在该 VLAN 内使能 MLD Snooping。

```
[SwitchB] vlan 100
```

```
[SwitchB-vlan100] port GigabitEthernet 1/0/1 GigabitEthernet 1/0/2
```

```
[SwitchB-vlan100] mld-snooping enable
```

```
[SwitchB-vlan100] quit
```

#### (5) 配置 Switch C

# 全局使能 MLD Snooping。

```
<SwitchC> system-view
```

```
[SwitchC] mld-snooping
```

```
[SwitchC-mld-snooping] quit
```

# 创建 VLAN 100，把端口 GigabitEthernet1/0/1 到 GigabitEthernet1/0/5 添加到该 VLAN 中，并在该 VLAN 内使能 MLD Snooping。

```
[SwitchC] vlan 100
```

```
[SwitchC-vlan100] port GigabitEthernet 1/0/1 to GigabitEthernet 1/0/5
```

```
[SwitchC-vlan100] mld-snooping enable
```

```
[SwitchC-vlan100] quit
```

# 在 VLAN 100 内的端口 GigabitEthernet1/0/3 和 GigabitEthernet1/0/5 上配置静态加入组播组 FF1E::101。

```
[SwitchC] interface GigabitEthernet 1/0/3
```

```
[SwitchC-GigabitEthernet1/0/3] igmp-snooping static-group FF1E::101 vlan 100
```

```
[SwitchC-GigabitEthernet1/0/3] quit
```

```
[SwitchC] interface GigabitEthernet 1/0/5
```

```
[SwitchC-GigabitEthernet1/0/5] igmp-snooping static-group FF1E::101 vlan 100
```

```
[SwitchC-GigabitEthernet1/0/5] quit
```

#### (6) 检验配置效果

# 查看 Switch A 上 VLAN 100 内 MLD Snooping 组播组的详细信息。

```
[SwitchA] display mld-snooping group vlan 100 verbose
```

```
Total 1 IP Group(s).
```

```
Total 1 IP Source(s).
```

```
Total 1 MAC Group(s).
```

```
Port flags: D-Dynamic port, S-Static port, A-Aggregation port, C-Copy port
```

```
Subvlan flags: R-Real VLAN, C-Copy VLAN
```

```
Vlan(id):100.
```

```
Total 1 IP Group(s).
```

```
Total 1 IP Source(s).
```

```

Total 1 MAC Group(s).
Router port(s):total 2 port.
 GE1/0/1 (D) (00:01:30)
 GE1/0/3 (S)
IP group(s):the following ip group(s) match to one mac group.
 IP group address:FF1E::101
 (:, FF1E::101):
 Attribute: Host Port
 Host port(s):total 1 port.
 GE1/0/2 (D) (00:03:23)
MAC group(s):
 MAC group address:3333-0000-0101
 Host port(s):total 1 port.
 GE1/0/2

```

由此可见，Switch A 上的端口 GigabitEthernet1/0/3 已经成为了静态路由器端口。

# 查看 SwitchC 上 VLAN 100 内 MLD Snooping 组播组的详细信息。

```

[SwitchC] display mld-snooping group vlan 100 verbose
 Total 1 IP Group(s).
 Total 1 IP Source(s).
 Total 1 MAC Group(s).

Port flags: D-Dynamic port, S-Static port, A-Aggregation port, C-Copy port
Subvlan flags: R-Real VLAN, C-Copy VLAN
Vlan(id):100.
 Total 1 IP Group(s).
 Total 1 IP Source(s).
 Total 1 MAC Group(s).
 Router port(s):total 2 port.
 GE1/0/1 (D) (00:01:30)
 IP group(s):the following ip group(s) match to one mac group.
 IP group address:FF1E::101
 (:, FF1E::101):
 Attribute: Host Port
 Host port(s):total 1 port.
 GE1/0/3 (S)
 GE1/0/3 (S)
MAC group(s):
 MAC group address:3333-0000-0101
 Host port(s):total 1 port.
 GE1/0/3
 GE1/0/5

```

由此可见，Switch C 上的端口 GigabitEthernet1/0/3 和 GigabitEthernet1/0/5 已经成为了静态成员端口。

## 5. 完整配置

### (1) SwitchA 配置信息

```
#
```

```

mld-snooping
#
vlan 100
 mld-snooping enable
#
interface GigabitEthernet1/0/1
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port access vlan 100
#
interface GigabitEthernet1/0/3
 port access vlan 100
 mld-snooping static-router-port vlan 100
#

```

## (2) SwitchB 配置信息

```

#
mld-snooping
#
vlan 100
 mld-snooping enable
#
interface GigabitEthernet1/0/1
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port access vlan 100
#

```

## (3) SwitchC 配置信息

```

#
mld-snooping
#
vlan 100
 mld-snooping enable
#
interface GigabitEthernet1/0/1
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port access vlan 100
#
interface GigabitEthernet1/0/3
 port access vlan 100
 mld-snooping static-group FF1E::101 vlan 100
#
interface GigabitEthernet1/0/4
 port access vlan 100
#

```

```
interface GigabitEthernet1/0/5
port access vlan 100
mld-snooping static-group FF1E::101 vlan 100
#
```

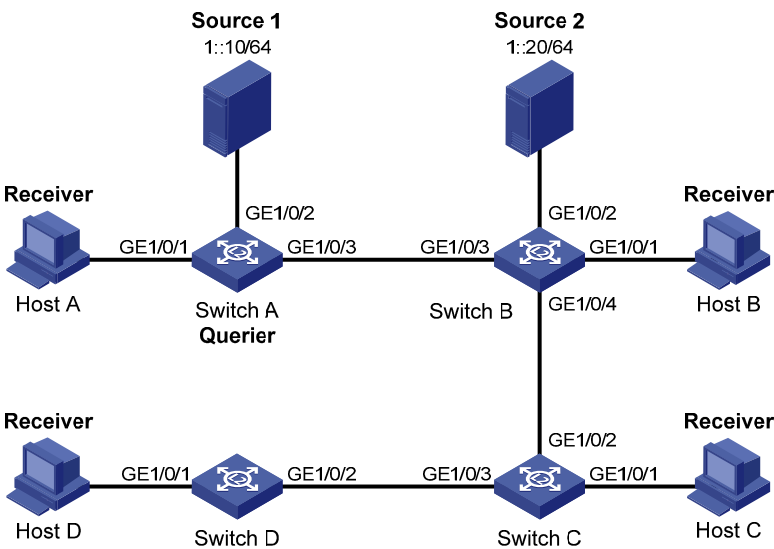
6. 配置注意事项

无

1.2.3 MLD Snooping 查询器配置指导

1. 组网图

图1-5 MLD Snooping 查询器配置组网图



2. 应用要求

- 如图 1-5所示，在一个没有三层设备的纯二层网络环境中，IPv6 组播源Source 1 和Source 2 分别向IPv6 组播组FF1E::101 和FF1E::102 发送IPv6 组播数据，Host A和Host C是IPv6 组播组FF1E::101 的接收者（Receiver），Host B和Host D则是IPv6 组播组FF1E::102 的接收者；
- 所有接收者均使用 MLDv1，所有交换机上都运行版本 1 的 MLD Snooping，并选择距 IPv6 组播源较近的 Switch A 来充当 MLD Snooping 查询器；
- 为了防止交换机在没有二层 IPv6 组播转发表项时将 IPv6 组播数据在 VLAN 内广播，要求在所有交换机上都使能丢弃未知 IPv6 组播数据报文的功能。

3. 适用产品、版本

表1-5 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本                         |
|-------------------|---------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本               | 全系列硬件版本<br>(除 S5500-20TP-SI) |

| 产品                | 软件版本              | 硬件版本          |
|-------------------|-------------------|---------------|
|                   | Release 1301 软件版本 | S5500-20TP-SI |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本 | 全系列硬件版本       |
| S7500E 系列以太网交换机   | Release 6300 软件版本 | 全系列硬件版本       |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本 | 全系列硬件版本       |

#### 4. 配置过程 and 解释

##### (1) 配置 Switch A

# 全局使能 MLD Snooping。

```
<SwitchA> system-view
[SwitchA] mld-snooping
[SwitchA-mld-snooping] quit
```

# 创建 VLAN 100，并把端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/3 添加到该 VLAN 中。

```
[SwitchA] vlan 100
[SwitchA-vlan100] port GigabitEthernet 1/0/1 GigabitEthernet 1/0/3
```

# 在 VLAN 100 内使能 MLD Snooping，并使能丢弃未知 IPv6 组播数据报文功能。

```
[SwitchA-vlan100] mld-snooping enable
[SwitchA-vlan100] mld-snooping drop-unknown
```

# 在 VLAN 100 内使能 MLD Snooping 查询器。

```
[SwitchA-vlan100] mld-snooping querier
[SwitchA-vlan100] quit
```

##### (2) 配置 Switch B

# 全局使能 MLD Snooping。

```
<SwitchB> system-view
[SwitchB] mld-snooping
[SwitchB-mld-snooping] quit
```

# 创建 VLAN 100，把端口 GigabitEthernet1/0/1 到 GigabitEthernet1/0/4 添加到该 VLAN 中。

```
[SwitchB] vlan 100
[SwitchB-vlan100] port GigabitEthernet 1/0/1 to GigabitEthernet 1/0/4
```

# 在 VLAN 100 内使能 MLD Snooping，并使能丢弃未知 IPv6 组播数据报文功能。

```
[SwitchB-vlan100] mld-snooping enable
[SwitchB-vlan100] mld-snooping drop-unknown
[SwitchB-vlan100] quit
```

Switch C 和 Switch D 的配置与 Switch B 相似，配置过程略。

##### (3) 检验配置效果

# 查看 Switch B 上收到的 MLD 报文的统计信息。

```
[SwitchB-vlan100] display mld-snooping statistics
Received MLD general queries:3.
Received MLDv1 specific queries:0.
```

```
Received MLDv1 reports:12.
Received MLD done:0.
Sent MLDv1 specific queries:0.
Received MLDv2 reports:0.
Received MLDv2 reports with right and wrong records:0.
Received MLDv2 specific queries:0.
Received MLDv2 specific sg queries:0.
Sent MLDv2 specific queries:0.
Sent MLDv2 specific sg queries:0.
Received error MLD messages:0.
```

Switch C 收到了 MLD 普遍组查询报文，由此可见，Switch A 上 MLD Snooping 查询器已经开始正常工作了。

## 5. 完整配置

### (1) SwitchA 配置信息

```
#
mld-snooping
#
vlan 100
mld-snooping enable
mld-snooping drop-unknown
mld-snooping querier
#
interface GigabitEthernet1/0/1
port access vlan 100
#
interface GigabitEthernet1/0/2
port access vlan 100
#
interface GigabitEthernet1/0/3
port access vlan 100
#
```

### (2) SwitchB 配置信息

```
#
mld-snooping
#
vlan 100
mld-snooping enable
mld-snooping drop-unknown
#
interface GigabitEthernet1/0/1
port access vlan 100
#
interface GigabitEthernet1/0/2
port access vlan 100
#
interface GigabitEthernet1/0/3
```

```

port access vlan 100
#
interface GigabitEthernet1/0/3
port access vlan 100
#

```

Switch C 和 Switch D 的配置与 Switch B 相似，配置过程略。

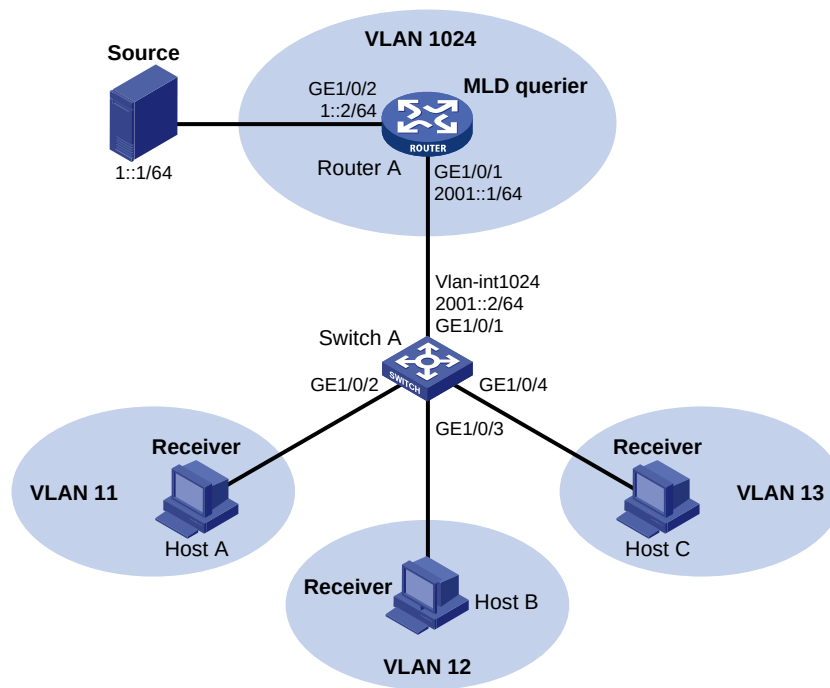
## 1.3 IPv6 组播 VLAN 典型配置指导

在传统的组播点播方式下，当属于不同 VLAN 的主机 Host A、Host B 和 Host C 分别进行组播点播时，Router A 需要把组播数据在每个 VLAN 内都复制一份。这样既造成了带宽的浪费，也给三层设备增加了额外的负担。

### 1.3.1 基于子 VLAN 的 IPv6 组播 VLAN 典型配置指导

#### 1. 组网图

图1-6 基于子 VLAN 的 IPv6 组播 VLAN 典型配置组网图



#### 2. 应用要求

- 如图 1-6所示，Router A通过GigabitEthernet1/0/2 接口连接IPv6 组播源（Source），通过 GigabitEthernet1/0/1 接口连接Switch A；
- Router A 与 Switch A之间运行 MLD，Switch A上运行 MLD Snooping，并由 Router A 充当 MLD 查询器；
- Switch A 的端口 GigabitEthernet1/0/1 属于 VLAN 1024，端口 GigabitEthernet1/0/2 到 GigabitEthernet1/0/4 分别属于 VLAN 11 到 VLAN 13，Host A 到 Host C 分别连接到 Switch A 的端口 GigabitEthernet1/0/2 到 GigabitEthernet1/0/4 上；

- 通过配置 IPv6 组播 VLAN，使 Router A 向 Switch A 下的这三台主机传送 IPv6 组播数据时，只需要向 VLAN 1024 发送一份即可，而不必向每个 VLAN 都发送。

### 3. 适用产品、版本

表1-6 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本                         |
|-------------------|---------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本               | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本               | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6300 软件版本               | 全系列硬件版本                      |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本                      |

### 4. 配置过程和解释

#### (1) 配置各设备接口的 IPv6 地址

请按照图 1-6 配置各接口的 IPv6 地址和前缀长度，具体配置过程略。

#### (2) 配置 Router A

# 使能 IPv6 组播路由，在各接口上使能 IPv6 PIM-DM，并在接口 GigabitEthernet1/0/1 上使能 MLD。

```
<RouterA> system-view
[RouterA] multicast ipv6 routing-enable
[RouterA] interface GigabitEthernet 1/0/1
[RouterA-GigabitEthernet1/0/1] pim ipv6 dm
[RouterA-GigabitEthernet1/0/1] mld enable
[RouterA-GigabitEthernet1/0/1] quit
[RouterA] interface GigabitEthernet1/0/2
[RouterA-GigabitEthernet1/0/2] pim ipv6 dm
[RouterA-GigabitEthernet1/0/2] quit
```

#### (3) 配置 Switch A

# 全局使能 MLD Snooping。

```
<SwitchA> system-view
[SwitchA] mld-snooping
[SwitchA-mld-snooping] quit
```

# 创建 VLAN 11，并把端口 GigabitEthernet1/0/2 添加到该 VLAN 中。

```
[SwitchA] vlan 11
[SwitchA-vlan11] port GigabitEthernet1/0/2
[SwitchA-vlan11] quit
```

VLAN 12 与 VLAN 13 的配置与 VLAN 11 相似，配置过程略。



# 创建 VLAN 1024，把端口 GigabitEthernet1/0/1 添加到该 VLAN 中，并在该 VLAN 内使能 MLD Snooping。

```
[SwitchA] vlan 1024
[SwitchA-vlan1024] port GigabitEthernet1/0/1
[SwitchA-vlan1024] mld-snooping enable
[SwitchA-vlan1024] quit
```

# 使能 VLAN 1024 为 IPv6 组播 VLAN，并把 VLAN 11 到 VLAN 13 都配置为该 IPv6 组播 VLAN 的子 VLAN。

```
[SwitchA] multicast-vlan ipv6 1024 enable
[SwitchA] multicast-vlan ipv6 1024 subvlan 11 to 13
```

#### (4) 检验配置效果

# 查看 Switch A 上所有 IPv6 组播 VLAN 及其子 VLAN 的信息。

```
[SwitchA] display multicast-vlan ipv6
IPv6 multicast vlan 1024's subvlan list:
 vlan 11-13
```

## 5. 完整配置

### (1) SwitchA 配置信息

```
#
mld-snooping
#
vlan 11 to 13
#
interface GigabitEthernet1/0/2
port access vlan 11
#
interface GigabitEthernet1/0/3
port access vlan 12
#
interface GigabitEthernet1/0/4
port access vlan 13
#
vlan 1024
port GigabitEthernet1/0/1
mld-snooping enable
#
multicast-vlan ipv6 1024 enable
multicast-vlan ipv6 1024 subvlan 11 to 13
#
```

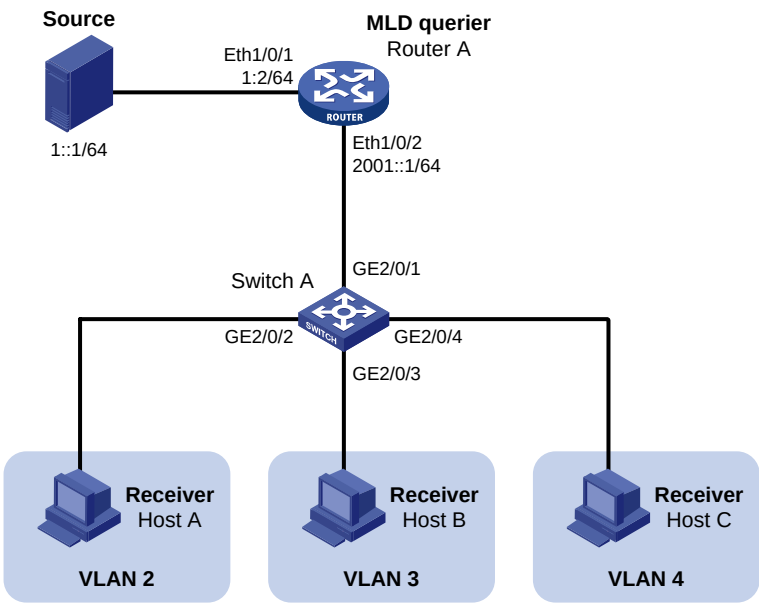
## 6. 配置注意事项

- 如果设备上已使能了 IPv6 组播路由，则不允许在该设备上配置 IPv6 组播 VLAN。
- 在配置成为 IPv6 组播 VLAN 的 VLAN 内必须使能 MLD Snooping，才能实现 IPv6 组播 VLAN 功能；而在 IPv6 组播 VLAN 的子 VLAN 内不必使能 MLD Snooping。

### 1.3.2 基于端口的 IPv6 组播 VLAN 典型配置指导

#### 1. 组网图

图1-7 基于端口的 IPv6 组播 VLAN 配置组网图



#### 2. 组网需求

- 如图 1-7所示，Router A通过接口Ethernet1/0/1 连接IPv6 组播源（Source），通过接口Ethernet1/0/2 连接Switch A；
- Router A 上运行 MLDv1，Switch A 上运行版本 1 的 MLD Snooping，并由 Router A 充当 MLD 查询器；
- Switch A 的端口 GigabitEthernet2/0/1 属于 VLAN 10，端口 GigabitEthernet2/0/2 到 GigabitEthernet2/0/4 分别属于 VLAN 2 到 VLAN 4，Host A 到 Host C 分别连接到 Switch A 的端口 GigabitEthernet2/0/2 到 GigabitEthernet2/0/4 上；
- IPv6 组播源向 IPv6 组播组 FF1E::101 发送 IPv6 组播数据，Host A、Host B 和 Host C 都是该 IPv6 组播组的接收者（Receiver）；
- 通过配置基于端口的 IPv6 组播 VLAN，使 Router A 通过 IPv6 组播 VLAN 向 Switch A 下分属不同用户 VLAN 的主机分发 IPv6 组播数据。

#### 3. 适用产品、版本

表1-7 配置适用的产品与软硬件版本关系

| 产品              | 软件版本              | 硬件版本    |
|-----------------|-------------------|---------|
| S7500E 系列以太网交换机 | Release 6300 软件版本 | 全系列硬件版本 |

#### 4. 配置过程和解释

##### (1) 使能 IPv6 转发功能，并配置 IPv6 地址

使能各设备的IPv6 转发功能，并按照 图 1-7配置各接口的IPv6 地址和前缀长度，具体配置过程略。

## (2) 配置 Router A

# 使能 IPv6 组播路由, 在各接口上使能 IPv6 PIM-DM, 并在主机侧接口 Ethernet1/0/2 上使能 MLD。

```
<RouterA> system-view
[RouterA] multicast ipv6 routing-enable
[RouterA] interface ethernet 1/0/1
[RouterA-Ethernet1/0/1] pim ipv6 dm
[RouterA-Ethernet1/0/1] quit
[RouterA] interface ethernet 1/0/2
[RouterA-Ethernet1/0/2] pim ipv6 dm
[RouterA-Ethernet1/0/2] mld enable
```

## (3) 配置 Switch A

# 全局使能 MLD Snooping。

```
<SwitchA> system-view
[SwitchA] mld-snooping
[SwitchA-mld-snooping] quit
```

# 创建 VLAN 10, 把端口 GigabitEthernet2/0/1 添加到该 VLAN 中, 并在该 VLAN 内使能 MLD Snooping。

```
[SwitchA] vlan 10
[SwitchA-vlan10] port gigabitethernet 2/0/1
[SwitchA-vlan10] mld-snooping enable
[SwitchA-vlan10] quit
```

# 创建 VLAN 2, 并在该 VLAN 内使能 MLD Snooping。

```
[SwitchA] vlan 2
[SwitchA-vlan2] mld-snooping enable
[SwitchA-vlan2] quit
```

VLAN 3 与 VLAN 4 的配置与 VLAN 2 相似, 配置过程略。

# 配置端口 GigabitEthernet2/0/2 为 Hybrid 类型, 缺省 VLAN 为 VLAN 2; 允许 VLAN 2 和 VLAN 10 的报文通过, 且均不携带 Tag。

```
[SwitchA] interface gigabitethernet 2/0/2
[SwitchA-GigabitEthernet2/0/2] port link-type hybrid
[SwitchA-GigabitEthernet2/0/2] port hybrid pvid vlan 2
[SwitchA-GigabitEthernet2/0/2] port hybrid vlan 2 untagged
[SwitchA-GigabitEthernet2/0/2] port hybrid vlan 10 untagged
[SwitchA-GigabitEthernet2/0/2] quit
```

GigabitEthernet2/0/3 与 GigabitEthernet2/0/4 的配置与 GigabitEthernet2/0/2 相似, 不同的是 GigabitEthernet2/0/3 的缺省 VLAN 为 3, 允许 VLAN3 和 VLAN10 的报文不带 Tag 通过; GigabitEthernet2/0/4 的缺省 VLAN 为 4, 允许 VLAN4 和 VLAN10 的报文不带 Tag 通过, 配置过程略。

# 配置 VLAN 10 为 IPv6 组播 VLAN。

```
[SwitchA] multicast-vlan ipv6 10
```

# 将端口 GigabitEthernet2/0/2 到 GigabitEthernet2/0/4 添加到 IPv6 组播 VLAN 10 内。

```
[SwitchA-ipv6-mvlan-10] port gigabitethernet 2/0/2 to gigabitethernet 2/0/4
```

```
[SwitchA-ipv6-mvlan-10] quit
```

#### (4) 检验配置效果

# 查看 Switch A 上所有 IPv6 组播 VLAN 的信息。

```
[SwitchA] display multicast-vlan ipv6
```

```
Total 1 IPv6 multicast-vlan(s)
```

```
IPv6 Multicast vlan 10
```

```
subvlan list:
```

```
no subvlan
```

```
port list:
```

```
GE1/0/2 GE1/0/3 GE1/0/4
```

# 查看 Switch A 上 MLD Snooping 组播组的信息。

```
[SwitchA] display mld-snooping group
```

```
Total 1 IP Group(s).
```

```
Total 1 IP Source(s).
```

```
Total 1 MAC Group(s).
```

```
Port flags: D-Dynamic port, S-Static port, C-Copy port
```

```
Subvlan flags: R-Real VLAN, C-Copy VLAN
```

```
Vlan(id):10.
```

```
Total 1 IP Group(s).
```

```
Total 1 IP Source(s).
```

```
Total 1 MAC Group(s).
```

```
Router port(s):total 1 port.
```

```
GE2/0/1 (D)
```

```
IP group(s):the following ip group(s) match to one mac group.
```

```
IP group address:FF1E::101
```

```
(::, FF1E::101):
```

```
Host port(s):total 3 port.
```

```
GE2/0/2 (D)
```

```
GE2/0/3 (D)
```

```
GE2/0/4 (D)
```

```
MAC group(s):
```

```
MAC group address:3333-0000-0101
```

```
Host port(s):total 3 port.
```

```
GE2/0/2
```

```
GE2/0/3
```

```
GE2/0/4
```

## 5. 完整配置

此处仅列出 SwitchA 上的完整配置。

```
#
```

```
mld-snooping
```

```
#
```

```
vlan 2
```

```
mld-snooping enable
```

```

#
vlan 3
 mld-snooping enable
#
vlan 4
 mld-snooping enable
#
vlan 10
 mld-snooping enable
#
interface GigabitEthernet2/0/1
 port access vlan 10
#
interface GigabitEthernet2/0/2
 port link-type hybrid
 port hybrid vlan 1 to 2 10 untagged
 port hybrid pvid vlan 2
#
interface GigabitEthernet2/0/3
 port link-type hybrid
 port hybrid vlan 1 3 10 untagged
 port hybrid pvid vlan 3
#
interface GigabitEthernet2/0/4
 port link-type hybrid
 port hybrid vlan 1 4 10 untagged
 port hybrid pvid vlan 4
#
multicast-vlan ipv6 10
 port GigabitEthernet2/0/2 to GigabitEthernet2/0/4

```

## 6. 配置注意事项

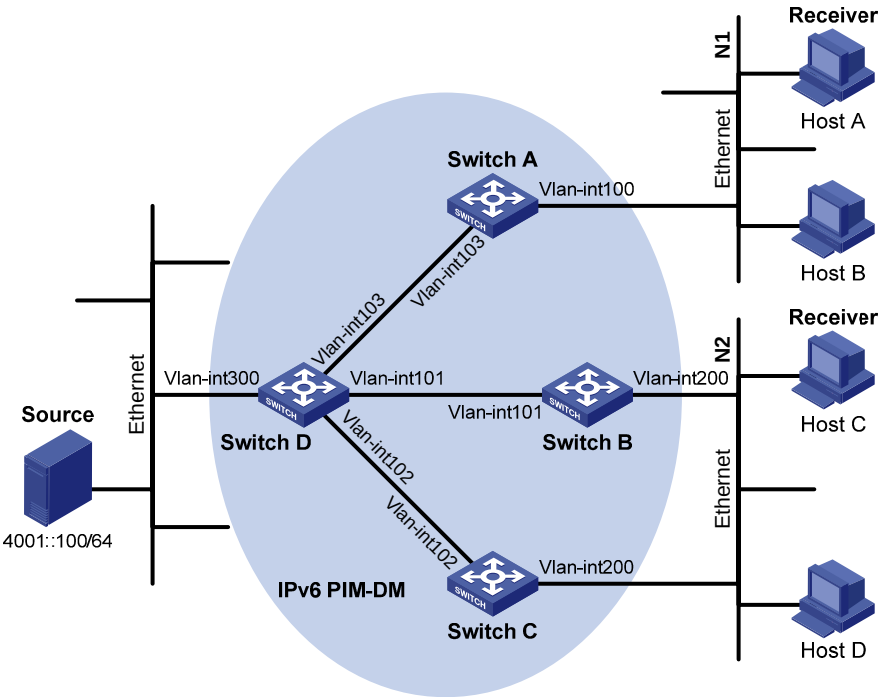
- 一个端口只能属于一个 IPv6 组播 VLAN。
- 在已使能了 IPv6 组播路由的设备上不允许再配置 IPv6 组播 VLAN。

# 1.4 IPv6 PIM 典型配置指导

## 1.4.1 IPv6 PIM-DM 典型配置指导

### 1. 组网图

图1-8 IPv6 PIM-DM 典型配置组网图



| 设备       | 接口          | IP 地址      | 设备       | 接口          | IP 地址      |
|----------|-------------|------------|----------|-------------|------------|
| Switch A | Vlan-int100 | 1001::1/64 | Switch D | Vlan-int300 | 4001::1/64 |
|          | Vlan-int103 | 1002::1/64 |          | Vlan-int103 | 1002::2/64 |
| Switch B | Vlan-int200 | 2001::1/64 |          | Vlan-int101 | 2002::2/64 |
|          | Vlan-int101 | 2002::1/64 |          | Vlan-int102 | 3001::2/64 |
| Switch C | Vlan-int200 | 2001::2/64 |          |             |            |
|          | Vlan-int102 | 3001::1/64 |          |             |            |

### 2. 应用要求

- 接收者通过组播方式接收视频点播信息，不同组织的接收者群体组成末梢网络，每个末梢网络中都存在至少一个接收者，整个 IPv6 PIM 域采用 DM 方式。
- Host A 和 Host C 为两个末梢网络中的 IPv6 组播信息接收者；Switch D 通过 Vlan-interface300 接口与 IPv6 组播源（Source）所在的网络连接；Switch A 通过 Vlan-interface100 接口连接末梢网络 N1，通过 Vlan-interface103 接口连接 Switch D；Switch B 和 Switch C 通过各自的 Vlan-interface200 接口连接末梢网络 N2，分别通过 Vlan-interface101 和 Vlan-interface102 接口连接 Switch D。
- Switch A 与末梢网络 N1 之间运行 MLDv1；Switch B 和 Switch C 与末梢网络 N2 之间也运行 MLDv1。

### 3. 适用产品、版本

表1-8 配置适用的产品与软硬件版本关系

| 产品              | 软件版本              | 硬件版本    |
|-----------------|-------------------|---------|
| S7500E 系列以太网交换机 | Release 6300 软件版本 | 全系列硬件版本 |

### 4. 配置过程 and 解释

#### (1) 使能 IPv6 转发功能，并配置 IPv6 地址和 IPv6 单播路由协议

使能各交换机的IPv6 转发功能，并按照 图 1-8配置各接口的IPv6 地址和前缀长度，配置方法请参见“IPv6 典型配置指导”。

配置 IPv6 PIM-DM 域内的各交换机之间采用 OSPFv3 协议进行互连，确保 IPv6 PIM-DM 域内部在网络层互通，并且各交换机之间能够借助 IPv6 单播路由协议实现动态路由更新，配置方法请参见“IPv6 路由典型配置指导”。

#### (2) 使能 IPv6 组播路由，并使能 IPv6 PIM-DM 和 MLD

# 在 Switch A 上使能 IPv6 组播路由，在各接口上使能 IPv6 PIM-DM，并在其连接末梢网络的接口 Vlan-interface100 上使能 MLD。

```
<SwitchA> system-view
[SwitchA] multicast ipv6 routing-enable
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] mld enable
[SwitchA-Vlan-interface100] pim ipv6 dm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 103
[SwitchA-Vlan-interface103] pim ipv6 dm
[SwitchA-Vlan-interface103] quit
```

Switch B 和 Switch C 的配置与 Switch A 相似，配置过程略。

# 在 Switch D 上使能 IPv6 组播路由，并在各接口上使能 IPv6 PIM-DM。

```
<SwitchD> system-view
[SwitchD] multicast ipv6 routing-enable
[SwitchD] interface vlan-interface 300
[SwitchD-Vlan-interface300] pim ipv6 dm
[SwitchD-Vlan-interface300] quit
[SwitchD] interface vlan-interface 103
[SwitchD-Vlan-interface103] pim ipv6 dm
[SwitchD-Vlan-interface103] quit
[SwitchD] interface vlan-interface 101
[SwitchD-Vlan-interface101] pim ipv6 dm
[SwitchD-Vlan-interface101] quit
[SwitchD] interface vlan-interface 102
[SwitchD-Vlan-interface102] pim ipv6 dm
[SwitchD-Vlan-interface102] quit
```

#### (3) 检验配置效果

通过使用 **display pim ipv6 interface** 命令可以查看交换机接口上 IPv6 PIM 的配置和运行情况。例如：

# 查看 Switch D 上 IPv6 PIM 的配置信息。

```
[SwitchD] display pim ipv6 interface
```

| Interface | NbrCnt | HelloInt | DR-Pri | DR-Address |
|-----------|--------|----------|--------|------------|
| Vlan300   | 0      | 30       | 1      | 4001::1    |
|           |        |          |        | (local)    |
| Vlan103   | 0      | 30       | 1      | 1002::2    |
|           |        |          |        | (local)    |
| Vlan101   | 1      | 30       | 1      | 2002::2    |
|           |        |          |        | (local)    |
| Vlan102   | 1      | 30       | 1      | 3001::2    |
|           |        |          |        | (local)    |

通过使用 **display pim ipv6 neighbor** 命令可以查看交换机之间的 IPv6 PIM 邻居关系。例如：

# 查看 Switch D 上 IPv6 PIM 的邻居关系信息。

```
[SwitchD] display pim ipv6 neighbor
```

Total Number of Neighbors = 3

| Neighbor | Interface | Uptime   | Expires  | Dr-Priority |
|----------|-----------|----------|----------|-------------|
| 1002::1  | Vlan103   | 00:04:00 | 00:01:29 | 1           |
| 2002::1  | Vlan101   | 00:04:16 | 00:01:29 | 3           |
| 3001::1  | Vlan102   | 00:03:54 | 00:01:17 | 5           |

假如 Host A 需要接收 IPv6 组播组 G (FF0E::101) 的信息，当 IPv6 组播源 S (4001::100/64) 向 IPv6 组播组 G 发送 IPv6 组播数据时，通过扩散生成 SPT，SPT 路径中各交换机 (Switch A 和 Switch D) 上都存在 (S, G) 表项，Host A 向 Switch A 发送 MLD 报告以加入 IPv6 组播组 G，在 Switch A 上生成 (\*, G) 表项。通过使用 **display pim ipv6 routing-table** 命令可以查看交换机的 IPv6 PIM 路由表信息。例如：

# 查看 Switch A 上的 IPv6 PIM 路由表信息。

```
[SwitchA] display pim ipv6 routing-table
```

Total 1 (\*, G) entry; 1 (S, G) entry

(\*, FF0E::101)

Protocol: pim-dm, Flag: WC

UpTime: 00:01:24

Upstream interface: NULL

Upstream neighbor: NULL

RPF prime neighbor: NULL

Downstream interface(s) information:

Total number of downstreams: 1

1: Vlan-interface100

Protocol: mld, UpTime: 00:01:20, Expires: never

(4001::100, FF0E::101)

Protocol: pim-dm, Flag: ACT

UpTime: 00:01:20



```

Upstream interface: Vlan-interface103
Upstream neighbor: 1002::2
RPF prime neighbor: 1002::2
Downstream interface(s) information:
Total number of downstreams: 1
1: Vlan-interface100
Protocol: pim-dm, UpTime: 00:01:20, Expires: never

```

Switch B 和 Switch C 上的显示信息与 Switch A 类似。

# 查看 Switch D 上的 IPv6 PIM 路由表信息。

```

[SwitchD] display pim ipv6 routing-table
Total 0 (*, G) entry; 1 (S, G) entry

(4001::100, FF0E::101)
Protocol: pim-dm, Flag: LOC ACT
UpTime: 00:02:19
Upstream interface: Vlan-interface300
Upstream neighbor: NULL
RPF prime neighbor: NULL
Downstream interface(s) information:
Total number of downstreams: 3
1: Vlan-interface103
Protocol: pim-dm, UpTime: 00:02:19, Expires: never
2: Vlan-interface101
Protocol: pim-dm, UpTime: 00:02:19, Expires: never
3: Vlan-interface102
Protocol: pim-dm, UpTime: 00:02:19, Expires: never

```

## 5. 完整配置

- SwitchA 的完整配置

```

#
multicast ipv6 routing-enable
#
vlan 100
#
vlan 103
#
interface Vlan-interface100
mld enable
pim ipv6 dm
#
interface Vlan-interface103
pim ipv6 dm

```

SwitchB 和 SwitchC 的完整配置与 SwitchA 类似，这里不再赘述。

- SwitchD 的完整配置

```

#
multicast ipv6 routing-enable

```

```
#
vlan 101 to vlan 103
#
vlan 300
#
interface Vlan-interface101
pim ipv6 dm
#
interface Vlan-interface102
pim ipv6 dm
#
interface Vlan-interface103
pim ipv6 dm
#
interface Vlan-interface300
pim ipv6 dm
```

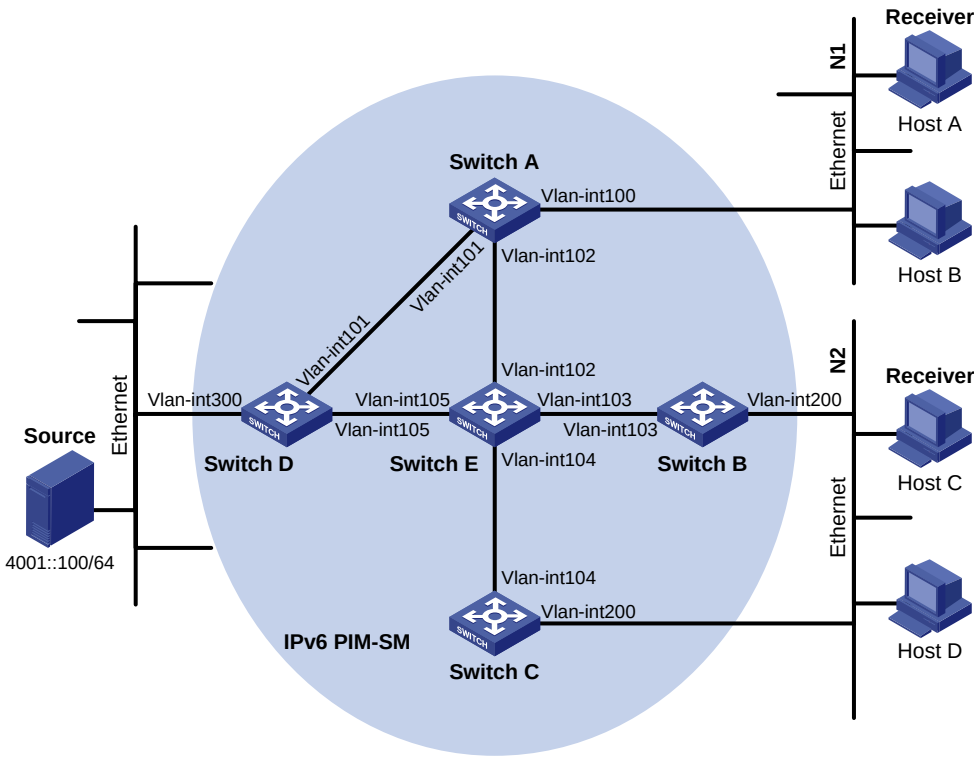
6. 配置注意事项

- 同一台设备所有接口上所启用的 IPv6 PIM 模式必须相同。
- IPv6 PIM-DM 不能与处于 IPv6 SSM 组地址范围内的 IPv6 组播组同时使用。

1.4.2 IPv6 PIM-SM 典型配置指导

1. 组网图

图1-9 IPv6 PIM-SM 典型配置组网图



| 设备       | 接口          | IP 地址      | 设备       | 接口          | IP 地址      |
|----------|-------------|------------|----------|-------------|------------|
| Switch A | Vlan-int100 | 1001::1/64 | Switch D | Vlan-int300 | 4001::1/64 |
|          | Vlan-int101 | 1002::1/64 |          | Vlan-int101 | 1002::2/64 |
|          | Vlan-int102 | 1003::1/64 |          | Vlan-int105 | 4002::1/64 |
| Switch B | Vlan-int200 | 2001::1/64 | Switch E | Vlan-int104 | 3001::2/64 |
|          | Vlan-int103 | 2002::1/64 |          | Vlan-int103 | 2002::2/64 |

|          |             |            |  |             |            |
|----------|-------------|------------|--|-------------|------------|
| Switch C | Vlan-int200 | 2001::2/64 |  | Vlan-int102 | 1003::2/64 |
|          | Vlan-int104 | 3001::1/64 |  | Vlan-int105 | 4002::2/64 |

## 2. 应用要求

- 接收者通过组播方式接收视频点播信息，不同组织的接收者群体组成末梢网络，每个末梢网络中都存在至少一个接收者，整个 IPv6 PIM 域采用 SM 方式。
- Host A 和 Host C 为两个末梢网络中的 IPv6 组播信息接收者；Switch D 通过 Vlan-interface300 接口与 IPv6 组播源（Source）所在网络连接；Switch A 通过 Vlan-interface100 接口连接末梢网络 N1，通过 Vlan-interface101 接口和 Vlan-interface102 接口分别连接 Switch D 和 Switch E；Switch B 和 Switch C 通过各自的 Vlan-interface200 接口连接末梢网络 N2，分别通过 Vlan-interface103 和 Vlan-interface104 接口连接 Switch E。
- 将 Switch D 的 Vlan-interface105 接口和 Switch E 的 Vlan-interface102 都配置为 C-BSR 和 C-RP，其中 Switch E 上 C-BSR 的优先级较高。C-RP 所服务的 IPv6 组播组范围为 FF0E::101/64，通过改变哈希掩码长度使此范围内的 IPv6 组地址间隔映射到这两个 C-RP 上。
- Switch A 与末梢网络 N1 之间运行 MLDv1；Switch B 和 Switch C 与末梢网络 N2 之间也运行 MLDv1。

## 3. 适用产品、版本

表1-9 配置适用的产品与软硬件版本关系

| 产品              | 软件版本              | 硬件版本    |
|-----------------|-------------------|---------|
| S7500E 系列以太网交换机 | Release 6300 软件版本 | 全系列硬件版本 |

## 4. 配置过程 and 解释

### (1) 使能 IPv6 转发功能，并配置 IPv6 地址和 IPv6 单播路由协议

使能各交换机的 IPv6 转发功能，并按照图 1-9 配置各接口的 IPv6 地址和前缀长度，配置方法请参见“IPv6 典型配置指导”。

配置 IPv6 PIM-SM 域内的各交换机之间采用 OSPFv3 协议进行互连，确保 IPv6 PIM-SM 域内部在网络层互通，并且各交换机之间能够借助 IPv6 单播路由协议实现动态路由更新，配置方法请参见“IPv6 路由典型配置指导”。

### (2) 使能 IPv6 组播路由，并使能 IPv6 PIM-SM 和 MLD

# 在 Switch A 上使能 IPv6 组播路由，在各接口上使能 IPv6 PIM-SM，并在其连接末梢网络的接口 Vlan-interface300 上使能 MLD。

```
<SwitchA> system-view
[SwitchA] multicast ipv6 routing-enable
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] mld enable
[SwitchA-Vlan-interface100] pim ipv6 sm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim ipv6 sm
```

```
[SwitchA-Vlan-interface101] quit
[SwitchA] interface vlan-interface 102
[SwitchA-Vlan-interface102] pim ipv6 sm
[SwitchA-Vlan-interface102] quit
```

Switch B 和 Switch C 的配置与 Switch A 相似，Switch D 和 Switch E 除了不需要在相应接口上使能 MLD 外，其它的配置也与 Switch A 相似，配置过程略。

### (3) 配置 C-BSR 和 C-RP

# 在 Switch D 上配置 RP 通告的服务范围，以及 C-BSR 和 C-RP 的位置，并指定哈希掩码长度为 128，C-BSR 的优先级为 10。

```
<SwitchD> system-view
[SwitchD] acl ipv6 number 2005
[SwitchD-acl6-basic-2005] rule permit source ff0e::101 64
[SwitchD-acl6-basic-2005] quit
[SwitchD] pim ipv6
[SwitchD-pim6] c-bsr 4002::1 128 10
[SwitchD-pim6] c-rp 4002::1 group-policy 2005
[SwitchD-pim6] quit
```

# 在 Switch E 上配置 RP 通告的服务范围，以及 C-BSR 和 C-RP 的位置，并指定哈希掩码长度为 128，C-BSR 的优先级为 20。

```
<SwitchE> system-view
[SwitchE] acl ipv6 number 2005
[SwitchE-acl6-basic-2005] rule permit source ff0e::101 64
[SwitchE-acl6-basic-2005] quit
[SwitchE] pim ipv6
[SwitchE-pim6] c-bsr 1003::2 128 20
[SwitchE-pim6] c-rp 1003::2 group-policy 2005
[SwitchE-pim6] quit
```

### (4) 检验配置效果

通过使用 **display pim ipv6 interface** 命令可以查看交换机接口上 IPv6 PIM 的配置和运行情况。例如：

# 查看 Switch A 上 IPv6 PIM 的配置信息。

```
[SwitchA] display pim ipv6 interface
```

| Interface | NbrCnt | HelloInt | DR-Pri | DR-Address |
|-----------|--------|----------|--------|------------|
| Vlan100   | 0      | 30       | 1      | 1001::1    |
|           |        |          |        | (local)    |
| Vlan101   | 1      | 30       | 1      | 1002::2    |
| Vlan102   | 1      | 30       | 1      | 1003::2    |

通过使用 **display pim ipv6 bsr-info** 命令可以查看交换机上 BSR 选举的信息，以及本地配置并生效的 C-RP 信息。例如：

# 查看 Switch A 上的 BSR 信息，以及本地配置并生效的 C-RP 信息。

```
[SwitchA] display pim ipv6 bsr-info
```

|                              |
|------------------------------|
| Elected BSR Address: 1003::2 |
| Priority: 20                 |
| Hash mask length: 128        |

```
State: Accept Preferred
```

```
Uptime: 00:04:22
```

```
Expires: 00:01:46
```

# 查看 Switch D 上的 BSR 信息，以及本地配置并生效的 C-RP 信息。

```
[SwitchD] display pim ipv6 bsr-info
```

```
Elected BSR Address: 1003::2
```

```
Priority: 20
```

```
Hash mask length: 128
```

```
State: Elected
```

```
Uptime: 00:05:26
```

```
Expires: 00:01:45
```

```
Candidate BSR Address: 4002::1
```

```
Priority: 10
```

```
Hash mask length: 128
```

```
State: Candidate
```

```
Candidate RP: 4002::1(Vlan-interface105)
```

```
Priority: 0
```

```
HoldTime: 130
```

```
Advertisement Interval: 60
```

```
Next advertisement scheduled at: 00:00:48
```

# 查看 Switch E 上的 BSR 信息，以及本地配置并生效的 C-RP 信息。

```
[SwitchE] display pim ipv6 bsr-info
```

```
Elected BSR Address: 1003::2
```

```
Priority: 20
```

```
Hash mask length: 128
```

```
State: Elected
```

```
Uptime: 00:01:10
```

```
Next BSR message scheduled at: 00:01:48
```

```
Candidate BSR Address: 1003::2
```

```
Priority: 20
```

```
Hash mask length: 128
```

```
State: Elected
```

```
Candidate RP: 1003::2(Vlan-interface102)
```

```
Priority: 0
```

```
HoldTime: 130
```

```
Advertisement Interval: 60
```

```
Next advertisement scheduled at: 00:00:48
```

通过使用 **display pim ipv6 rp-info** 命令可以查看交换机上获取的 RP 信息。例如：

# 查看 Switch A 上的 RP 信息。

```
[SwitchA] display pim ipv6 rp-info
```

```
PIM-SM BSR RP information:
```

```
prefix/prefix length: FF0E::101/64
```

```
RP: 4002::1
```

```
Priority: 0
```

```
HoldTime: 130
Uptime: 00:05:19
Expires: 00:02:11
```

```
RP: 1003::2
Priority: 0
HoldTime: 130
Uptime: 00:05:19
Expires: 00:02:11
```

假如 Host A 需要接收 IPv6 组播组 G（FF0E::100）的信息，由于根据哈希算法得出 G 对应的 RP 为 Router E，因此 Switch A 和 Switch E 之间会生成 RPT。当 IPv6 组播源 S（4001::100/64）向 RP 发起注册后，Switch D 和 Switch E 之间会生成 SPT。当 Switch A 收到 IPv6 组播数据后立即执行从 RPT 到 SPT 的切换。RPT 路径中的交换机（Switch A 和 Switch E）上存在（\*, G）表项，而 SPT 路径中的交换机（Switch A 和 Switch D）上存在（S, G）表项，通过使用 **display pim ipv6 routing-table** 命令可以查看交换机的 IPv6 PIM 路由表信息。例如：

# 查看 Switch A 上的 IPv6 PIM 路由表信息。

```
[SwitchA] display pim ipv6 routing-table
```

```
Total 1 (*, G) entry; 1 (S, G) entry
```

```
(*, FF0E::100)
```

```
RP: 1003::2
Protocol: pim-sm, Flag: WC
UpTime: 00:03:45
Upstream interface: Vlan-interface102
Upstream neighbor: 1003::2
RPF prime neighbor: 1003::2
Downstream interface(s) information:
Total number of downstreams: 1
1: Vlan-interface100
Protocol: mld, UpTime: 00:02:15, Expires: 00:03:06
```

```
(4001::100, FF0E::100)
```

```
RP: 1003::2
Protocol: pim-sm, Flag: SPT ACT
UpTime: 00:02:15
Upstream interface: Vlan-interface101
Upstream neighbor: 1002::2
RPF prime neighbor: 1002::2
Downstream interface(s) information:
Total number of downstreams: 1
1: Vlan-interface100
Protocol: pim-sm, UpTime: 00:02:15, Expires: 00:03:06
```

Switch B 和 Switch C 上的显示信息与 Switch A 类似。

# 查看 Switch D 上的 IPv6 PIM 路由表信息。

```
[SwitchD] display pim ipv6 routing-table
```

```
Total 0 (*, G) entry; 1 (S, G) entry
```

```
(4001::100, FF0E::100)
RP: 1003::2
Protocol: pim-sm, Flag: SPT LOC ACT
UpTime: 00:14:44
Upstream interface: Vlan-interface300
Upstream neighbor: NULL
RPF prime neighbor: NULL
Downstream interface(s) information:
Total number of downstreams: 1
1: Vlan-interface105
Protocol: mld, UpTime: 00:14:44, Expires: 00:02:26
```

# 查看 Switch E 上的 IPv6 PIM 路由表信息。

```
[SwitchE] display pim ipv6 routing-table
Total 1 (*, G) entry; 0 (S, G) entry
```

```
(*, FF0E::100)
RP: 1003::2 (local)
Protocol: pim-sm, Flag: WC
UpTime: 00:16:56
Upstream interface: Register
Upstream neighbor: 4002::1
RPF prime neighbor: 4002::1
Downstream interface(s) information:
Total number of downstreams: 1
1: Vlan-interface102
Protocol: pim-sm, UpTime: 00:16:56, Expires: 00:02:34
```

## 5. 完整配置

- SwitchA 的完整配置

```
#
multicast ipv6 routing-enable
#
vlan 100 to 102
#
interface Vlan-interface100
mld enable
pim ipv6 sm
#
interface Vlan-interface101
pim ipv6 sm
#
interface Vlan-interface102
pim ipv6 sm
```

SwitchB 和 SwitchC 的配置与 SwitchA 类似，这里不再赘述。

- SwitchD 的完整配置

```

#
multicast ipv6 routing-enable
#
acl ipv6 number 2005
 rule 0 permit source FF0E::101/64
#
vlan 101
#
vlan 105
#
vlan 300
#
interface Vlan-interface101
 pim ipv6 sm
#
interface Vlan-interface105
 pim ipv6 sm
#
interface Vlan-interface300
 pim ipv6 sm
#
pim ipv6
 c-bsr hash-length 128
 c-bsr priority 10
 c-bsr 4002::1
 c-rp 4002::1 group-policy 2005

```

- SwitchE 的完整配置

```

#
multicast ipv6 routing-enable
#
acl ipv6 number 2005
 rule 0 permit source FF0E::101/64
#
vlan 102 to 105
#
interface Vlan-interface102
 pim ipv6 sm
#
interface Vlan-interface103
 pim ipv6 sm
#
interface Vlan-interface104
 pim ipv6 sm
#
interface Vlan-interface105
 pim ipv6 sm
#
pim ipv6

```



```

c-bsr hash-length 128
c-bsr priority 20
c-bsr 1003::2
c-rp 1003::2 group-policy 2005

```

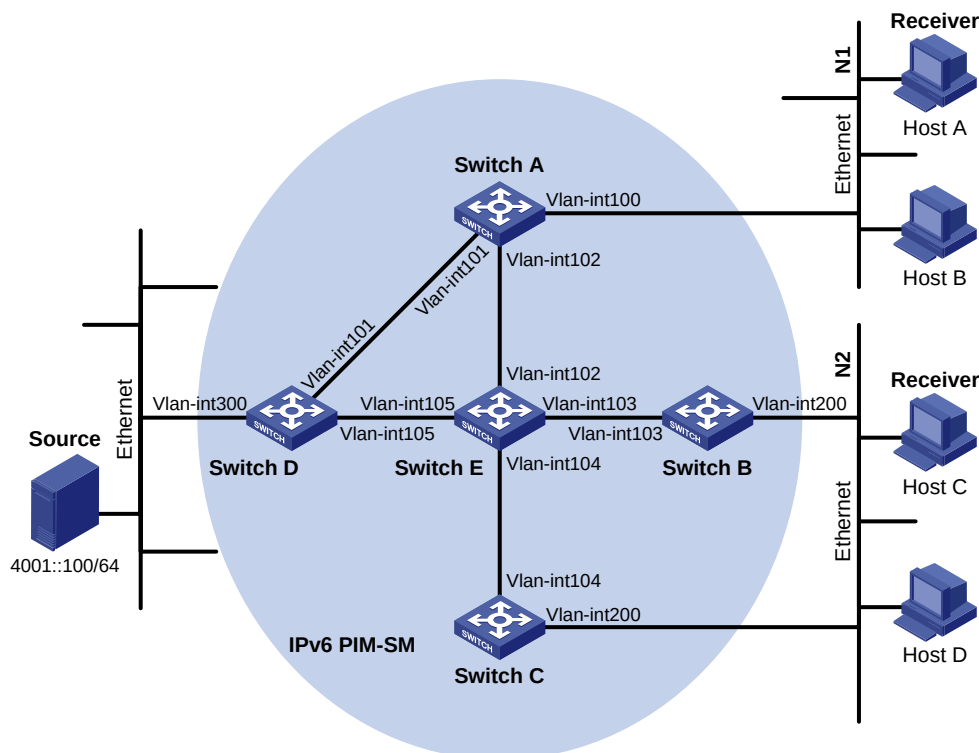
## 6. 配置注意事项

- 同一台设备所有接口上所启用的 IPv6 PIM 模式必须相同。
- 在配置 C-RP 时，应在 C-RP 与 IPv6 PIM-SM 域中的其它设备之间保留较大的通信带宽。
- 一个 RP 可以为多个 IPv6 组播组服务，也可以为所有 IPv6 组播组服务。每个 IPv6 组播组在任意时刻，只能由唯一的一个 RP 为其转发数据，而不能由多个 RP 转发数据。
- 由于 BSR 与 IPv6 PIM-SM 域中的其它设备需要交换大量信息，因此应在 C-BSR 与 IPv6 PIM-SM 域中的其它设备之间保留较大的通信带宽。

## 1.4.3 IPv6 PIM-SSM 典型配置指导

### 1. 组网图

图1-10 IPv6 PIM-SSM 典型配置组网图



| 设备       | 接口          | IP 地址      | 设备       | 接口          | IP 地址      |
|----------|-------------|------------|----------|-------------|------------|
| Switch A | Vlan-int100 | 1001::1/64 | Switch D | Vlan-int300 | 4001::1/64 |
|          | Vlan-int101 | 1002::1/64 |          | Vlan-int101 | 1002::2/64 |
|          | Vlan-int102 | 1003::1/64 |          | Vlan-int105 | 4002::1/64 |
| Switch B | Vlan-int200 | 2001::1/64 | Switch E | Vlan-int104 | 3001::2/64 |
|          | Vlan-int103 | 2002::1/64 |          | Vlan-int103 | 2002::2/64 |
| Switch C | Vlan-int200 | 2001::2/64 |          | Vlan-int102 | 1003::2/64 |
|          | Vlan-int104 | 3001::1/64 |          | Vlan-int105 | 4002::2/64 |

### 2. 应用要求

- 接收者通过组播方式接收视频点播信息，不同组织的接收者群体组成末梢网络，每个末梢网络中都存在至少一个接收者，整个 IPv6 PIM 域采用 SSM 方式。

- Host A 和 Host C 为两个末梢网络中的 IPv6 组播信息接收者；Switch D 通过 Vlan-interface300 接口与 IPv6 组播源（Source）所在网络连接；Switch A 通过 Vlan-interface100 接口连接末梢网络 N1，通过 Vlan-interface101 接口和 Vlan-interface102 接口分别连接 Switch D 和 Switch E；Switch B 和 Switch C 通过各自的 Vlan-interface200 接口连接末梢网络 N2，分别通过 Vlan-interface103 和 Vlan-interface104 接口连接 Switch E；Switch E 连接 Switch A、Switch B、Switch C 和 Switch D。
- SSM 组播组的范围是 FF3E::/64。
- Switch A 与末梢网络 N1 之间运行 MLDv2；Switch B 和 Switch C 与末梢网络 N2 之间也运行 MLDv2。

### 3. 适用产品、版本

表1-10 配置适用的产品与软硬件版本关系

| 产品              | 软件版本              | 硬件版本    |
|-----------------|-------------------|---------|
| S7500E 系列以太网交换机 | Release 6300 软件版本 | 全系列硬件版本 |

### 4. 配置过程和解释

#### (1) 使能 IPv6 转发功能，并配置 IPv6 地址和 IPv6 单播路由协议

使能各交换机的 IPv6 转发功能，并按照图 1-10 配置各接口的 IPv6 地址和前缀长度，配置方法请参见“IPv6 典型配置指导”。

配置 IPv6 PIM-SM 域内的各交换机之间采用 OSPFv3 协议进行互连，确保 IPv6 PIM-SM 域内部在网络层互通，并且各交换机之间能够借助 IPv6 单播路由协议实现动态路由更新，配置方法请参见“IPv6 路由典型配置指导”。

#### (2) 使能 IPv6 组播路由，并使能 IPv6 PIM-SM 和 MLD

# 在 Switch A 上使能 IPv6 组播路由，在各接口上使能 IPv6 PIM-SM，并在其连接末梢网络的接口 Vlan-interface100 上使能 MLD，且配置其版本为 2。

```
<SwitchA> system-view
[SwitchA] multicast ipv6 routing-enable
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] mld enable
[SwitchA-Vlan-interface100] mld version 2
[SwitchA-Vlan-interface100] pim ipv6 sm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim ipv6 sm
[SwitchA-Vlan-interface101] quit
[SwitchA] interface vlan-interface 102
[SwitchA-Vlan-interface102] pim ipv6 sm
[SwitchA-Vlan-interface102] quit
```

Switch B 和 Switch C 的配置与 Switch A 相似，Switch D 和 Switch E 除了不需要在相应接口上使能 MLD 外，其它的配置也与 Switch A 相似，配置过程略。

#### (3) 配置 IPv6 SSM 组播组的地址范围

# 在 Switch A 上配置 IPv6 SSM 组播组的地址范围为 FF3E::/64。

```
[SwitchA] acl ipv6 number 2000
[SwitchA-acl6-basic-2000] rule permit source ff3e:: 64
[SwitchA-acl6-basic-2000] quit
[SwitchA] pim ipv6
[SwitchA-pim6] ssm-policy 2000
[SwitchA-pim6] quit
```

Switch B、Switch C、Switch D 和 Switch E 的配置与 Switch A 相似，配置过程略。

#### (4) 检验配置效果

通过使用 **display pim ipv6 interface** 命令可以查看交换机接口上 IPv6 PIM 的配置和运行情况。例如：

# 查看 Switch A 上 IPv6 PIM 的配置信息。

```
[SwitchA] display pim ipv6 interface
```

| Interface | NbrCnt | HelloInt | DR-Pri | DR-Address |
|-----------|--------|----------|--------|------------|
| Vlan100   | 0      | 30       | 1      | 1001::1    |
|           |        |          |        | (local)    |
| Vlan101   | 1      | 30       | 1      | 1002::2    |
| Vlan102   | 1      | 30       | 1      | 1003::2    |

假如 Host A 需要接收指定 IPv6 组播源 S（4001::100/64）发往 IPv6 组播组 G（FF3E::101）的信息，Switch A 会向 IPv6 组播源方向构造 SPT，SPT 路径中的交换机（Switch A 和 Switch D）上生成（S，G）表项，而 SPT 路径之外的交换机（Switch E）上没有 IPv6 组播路由项，通过使用 **display pim ipv6 routing-table** 命令可以查看交换机的 IPv6 PIM 路由表信息。例如：

# 查看 Switch A 上的 IPv6 PIM 路由表信息。

```
[SwitchA] display pim ipv6 routing-table
Total 0 (*, G) entry; 1 (S, G) entry

(4001::100, FF3E::101)
 Protocol: pim-ssm, Flag:
 UpTime: 00:00:11
 Upstream interface: Vlan-interface101
 Upstream neighbor: 1002::2
 RPF prime neighbor: 1002::2
 Downstream interface(s) information:
 Total number of downstreams: 1
 1: Vlan-interface100
 Protocol: mld, UpTime: 00:00:11, Expires: 00:03:25
```

Switch B 和 Switch C 上的显示信息与 Switch A 类似。

# 查看 Switch D 上的 IPv6 PIM 路由表信息。

```
[SwitchD] display pim ipv6 routing-table
Total 0 (*, G) entry; 1 (S, G) entry

(4001::100, FF3E::101)
 Protocol: pim-ssm, Flag: LOC
 UpTime: 00:08:02
```

```

Upstream interface: Vlan-interface300
Upstream neighbor: NULL
RPF prime neighbor: NULL
Downstream interface(s) information:
Total number of downstreams: 1
1: Vlan-interface105
Protocol: pim-ssm, UpTime: 00:08:02, Expires: 00:03:25

```

## 5. 完整配置

- SwitchA 的完整配置

```

#
multicast ipv6 routing-enable
#
acl ipv6 number 2000
rule permit source ff3e:: 64
#
vlan 100 to 102
#
interface Vlan-interface100
mld enable
mld version 2
pim ipv6 sm
#
interface Vlan-interface101
pim ipv6 sm
#
interface Vlan-interface102
pim ipv6 sm
#
pim ipv6
ssm-policy 2000

```

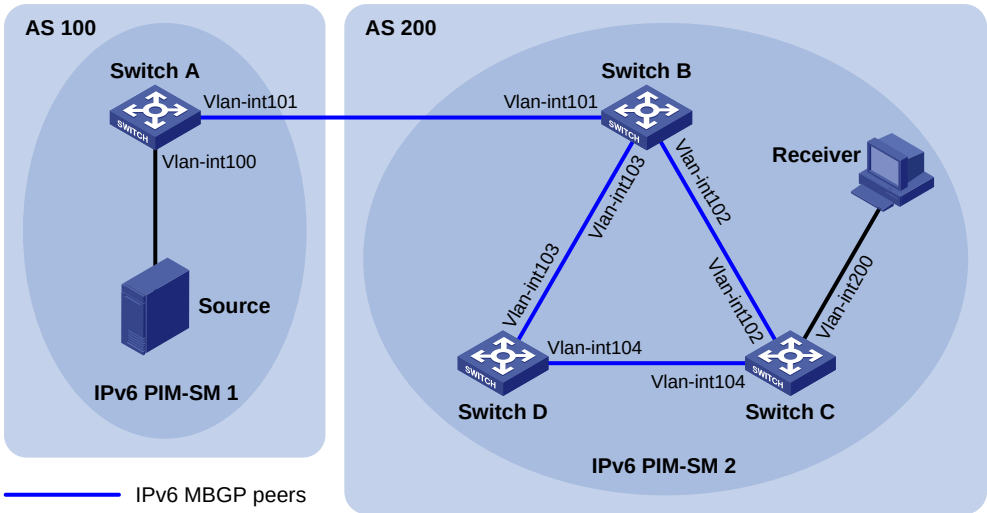
Switch B 和 Switch C 的配置与 Switch A 相似，Switch D 和 Switch E 除了不需要在相应接口上使能 MLD 外，其它的配置也与 Switch A 相似，完整配置这里不再赘述。

# 1.5 IPv6 MBGP 典型配置指导

## 1.5.1 IPv6 MBGP 典型配置指导

### 1. 组网图

图1-11 IPv6 MBGP 典型配置组网图



| 设备       | 接口          | IP 地址        | 设备       | 接口          | IP 地址      |
|----------|-------------|--------------|----------|-------------|------------|
| Source   | -           | 1002::100/64 | Switch C | Vlan-int200 | 3002::1/64 |
| Switch A | Vlan-int100 | 1002::1/64   |          | Vlan-int102 | 2001::2/64 |
|          | Vlan-int101 | 1001::1/64   |          | Vlan-int104 | 3001::1/64 |
| Switch B | Vlan-int101 | 1001::2/64   | Switch D | Vlan-int103 | 2002::2/64 |
|          | Vlan-int102 | 2001::1/64   |          | Vlan-int104 | 3001::2/64 |
|          | Vlan-int103 | 2002::1/64   |          |             |            |

### 2. 应用要求

- 网络中存在两个自治系统：IPv6 PIM-SM 1 属于 AS 100，IPv6 PIM-SM 2 属于 AS 200。各 AS 内部采用 OSPFv3 进行互联，AS 之间采用 IPv6 MBGP 交换 IPv6 组播路由信息；
- IPv6 组播源属于 AS 100 内的 IPv6 PIM-SM 1，接收者则属于 AS 200 内的 IPv6 PIM-SM 2；
- 将 Switch A 和 Switch B 各自的 Vlan-interface101 接口分别配置为各自 IPv6 PIM-SM 域的 C-BSR 和 C-RP。

### 3. 适用产品、版本

表1-11 配置适用的产品与软硬件版本关系

| 产品              | 软件版本              | 硬件版本    |
|-----------------|-------------------|---------|
| S7500E 系列以太网交换机 | Release 6300 软件版本 | 全系列硬件版本 |

### 4. 配置过程 and 解释

#### (1) 配置各交换机接口的 IPv6 地址和 IPv6 单播路由协议

- 请按照 图 1-11配置各接口的IPv6 地址和前缀长度，配置方法请参见“IPv6 典型配置指导”。

- 配置 AS200 内的各交换机之间采用 OSPFv3 路由协议交换路由信息（AS 内各路由器创建的 OSPFv3 进程号为 1），确保各 AS 内部在网络层互通，配置过程请参见“IPv6 路由典型配置指导”。

(2) 使能 IPv6 组播路由，使能 IPv6 PIM-SM 和 MLD，并配置 BSR 的服务边界

# 在 Switch A 上使能 IPv6 组播路由，在各接口上使能 IPv6 PIM-SM。

```
<SwitchA> system-view
[SwitchA] multicast ipv6 routing-enable
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] pim ipv6 sm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim ipv6 sm
[SwitchA-Vlan-interface101] quit
```

Switch B 和 Switch D 上的配置与 Switch A 相似，配置过程略。

# 在 Switch C 上使能 IPv6 组播路由，在各接口上使能 IPv6 PIM-SM，并在主机侧接口 Vlan-interface200 上使能 MLD。

```
<SwitchC> system-view
[SwitchC] multicast ipv6 routing-enable
[SwitchC] interface vlan-interface 102
[SwitchC-Vlan-interface102] pim ipv6 sm
[SwitchC-Vlan-interface102] quit
[SwitchC] interface vlan-interface 104
[SwitchC-Vlan-interface104] pim ipv6 sm
[SwitchC-Vlan-interface104] quit
[SwitchC] interface vlan-interface 200
[SwitchC-Vlan-interface200] pim ipv6 sm
[SwitchC-Vlan-interface200] mld enable
[SwitchC-Vlan-interface200] quit
```

# 在 Switch A 上配置 BSR 的服务边界。

```
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] pim ipv6 bsr-boundary
[SwitchA-Vlan-interface101] quit
```

# 在 Switch B 上配置 BSR 的服务边界。

```
[SwitchB] interface vlan-interface 101
[SwitchB-Vlan-interface101] pim ipv6 bsr-boundary
[SwitchB-Vlan-interface101] quit
```

(3) 配置 C-BSR 和 C-RP 的位置

# 在 Switch A 上配置 C-BSR 和 C-RP 的位置。

```
[SwitchA] pim ipv6
[SwitchA-pim6] c-bsr hash-length 32
[SwitchA-pim6] c-bsr priority 20
[SwitchA-pim6] c-bsr 1001::1
[SwitchA-pim6] c-rp 1001::1
```

```
[SwitchA-pim6] quit
```

# 在 Switch B 上配置 C-BSR 和 C-RP 的位置。

```
[SwitchB] pim ipv6
```

```
[SwitchB-pim6] c-bsr hash-length 32
```

```
[SwitchB-pim6] c-bsr priority 20
```

```
[SwitchB-pim6] c-bsr 1001::2
```

```
[SwitchB-pim6] c-rp 1001::2
```

```
[SwitchB-pim6] quit
```

(4) 配置 BGP 协议，并配置 IPv6 MBGP 对等体

# 在 Switch A 上配置 EBGP 邻接关系、并配置 IPv6 MBGP 对等体。

```
[SwitchA] ipv6
```

```
[SwitchA] bgp 100
```

```
[SwitchA-bgp] router-id 1.1.1.1
```

```
[SwitchA-bgp] ipv6-family
```

```
[SwitchA-bgp-af-ipv6] peer 1001::2 as-number 200
```

```
[SwitchA-bgp-af-ipv6] import-route direct
```

```
[SwitchA-bgp-af-ipv6] quit
```

```
[SwitchA-bgp] ipv6-family multicast
```

```
[SwitchA-bgp-af-ipv6-mul] peer 1001::2 enable
```

```
[SwitchA-bgp-af-ipv6-mul] import-route direct
```

```
[SwitchA-bgp-af-ipv6-mul] quit
```

```
[SwitchA-bgp] quit
```

# 在 Switch B 上配置 EBGP 邻接关系、配置 IPv6 MBGP 对等体，并引入 OSPFv3 路由。

```
[SwitchB] ipv6
```

```
[SwitchB] bgp 200
```

```
[SwitchB-bgp] router-id 2.2.2.2
```

```
[SwitchB-bgp] ipv6-family
```

```
[SwitchB-bgp-af-ipv6] peer 1001::1 as-number 100
```

```
[SwitchB-bgp-af-ipv6] import-route ospfv3 1
```

```
[SwitchB-bgp-af-ipv6] quit
```

```
[SwitchB-bgp] ipv6-family multicast
```

```
[SwitchB-bgp-af-ipv6-mul] peer 1001::1 enable
```

```
[SwitchB-bgp-af-ipv6-mul] import-route ospfv3 1
```

```
[SwitchB-bgp-af-ipv6-mul] quit
```

```
[SwitchB-bgp] quit
```

(5) 检验配置效果

通过使用 **display bgp ipv6 multicast peer** 命令可以查看交换机之间 IPv6 MBGP 对等体的关系。

例如：

# 查看 Switch B 上 IPv6 MBGP 对等体关系的信息。

```
[SwitchB] display bgp ipv6 multicast peer
```

```
BGP local router ID : 2.2.2.2
```

```
Local AS number : 200
```

```
Total number of peers : 3 Peers in established state : 3
```

| Peer    | V | AS  | MsgRcvd | MsgSent | OutQ | PrefRcv | Up/Down  | State       |
|---------|---|-----|---------|---------|------|---------|----------|-------------|
| 1001::1 | 4 | 100 | 56      | 56      | 0    | 0       | 00:40:54 | Established |

## 5. 完整配置

- SwitchA 的完整配置

```
#
multicast ipv6 routing-enable
#
vlan 100 to 101
#
interface Vlan-interface100
pim ipv6 sm
#
interface Vlan-interface101
pim ipv6 bsr-boundary
pim ipv6 sm
#
bgp 100
router-id 1.1.1.1
import-route direct
undo synchronization
peer 1001:2 as-number 200
#
ipv6-family
import-route direct
peer 1001::2 as-number 200
#
ipv6-family multicast
import-route direct
peer 1001:2 enable
#
pim ipv6
c-bsr hash-length 32
c-bsr priority 20
c-bsr 1001:1
c-rp 1001:1
```

- SwitchB 的完整配置

```
#
multicast ipv6 routing-enable
#
vlan 101 to 103
#
interface Vlan-interface101
pim ipv6 bsr-boundary
pim ipv6 sm
#
interface Vlan-interface102
```



```

pim ipv6 sm
#
interface Vlan-interface103
pim ipv6 sm
#
bgp 200
router-id 2.2.2.2
import-route ospfv3 1
undo synchronization
peer 1001:1 as-number 100
#
ipv6-family
import-route ospfv3 1
peer 1001::1 as-number 100
#
ipv6-family multicast
import-route ospfv3 1
peer 1001:1 enable
#
pim ipv6
c-bsr hash-length 32
c-bsr priority 20
c-bsr 1001:2
c-rp 1001:2

```

- SwitchC 的完整配置

```

#
multicast ipv6 routing-enable
#
vlan 102
#
vlan 104
#
vlan200
#
interface Vlan-interface102
pim ipv6 sm
#
interface Vlan-interface104
pim ipv6 sm
#
interface ipv6 Vlan-interface200
mld enable
pim sm

```

- SwitchD 的完整配置

```

#
multicast ipv6 routing-enable
#
vlan 103 to 104

```

```

interface Vlan-interface103
pim ipv6 sm

interface Vlan-interface104
pim ipv6 sm
```

## 6. 配置注意事项

配置 IPv6 MBGP 对等体组时，需要先在 IPv6 地址族视图下将对等体加入对等体组，然后在 BGP IPv6 组播地址族视图下使能 IPv6 MBGP 对等体组，并把 IPv6 MBGP 对等体加入 IPv6 MBGP 对等体组。

# 目 录

|                                     |      |
|-------------------------------------|------|
| 1 802.1x典型配置指导 .....                | 1-1  |
| 1.1 802.1x简介 .....                  | 1-1  |
| 1.2 802.1x典型配置指导 .....              | 1-1  |
| 1.2.1 组网图 .....                     | 1-1  |
| 1.2.2 应用要求 .....                    | 1-1  |
| 1.2.3 适用产品、版本 .....                 | 1-2  |
| 1.2.4 配置过程和解释 .....                 | 1-2  |
| 1.2.5 完整配置 .....                    | 1-3  |
| 1.2.6 配置注意事项 .....                  | 1-4  |
| 1.3 Guest VLAN、动态下发VLAN典型配置举例 ..... | 1-4  |
| 1.3.1 组网图 .....                     | 1-4  |
| 1.3.2 组网需求 .....                    | 1-5  |
| 1.3.3 适用产品、版本 .....                 | 1-5  |
| 1.3.4 配置过程和解释 .....                 | 1-5  |
| 1.3.5 完整配置 .....                    | 1-6  |
| 1.3.6 配置注意事项 .....                  | 1-7  |
| 1.4 下发ACL应用典型配置指导 .....             | 1-7  |
| 1.4.1 组网图 .....                     | 1-7  |
| 1.4.2 应用要求 .....                    | 1-7  |
| 1.4.3 适用产品、版本 .....                 | 1-8  |
| 1.4.4 配置过程和解释 .....                 | 1-8  |
| 1.4.5 完整配置 .....                    | 1-9  |
| 1.4.6 配置注意事项 .....                  | 1-9  |
| 1.5 EAD快速部署典型配置指导 .....             | 1-9  |
| 1.5.1 组网图 .....                     | 1-10 |
| 1.5.2 应用要求 .....                    | 1-10 |
| 1.5.3 适用产品、版本 .....                 | 1-10 |
| 1.5.4 配置过程和解释 .....                 | 1-10 |
| 1.5.5 完整配置 .....                    | 1-11 |
| 1.5.6 配置注意事项 .....                  | 1-11 |

# 1 802.1x 典型配置指导

## 1.1 802.1x 简介

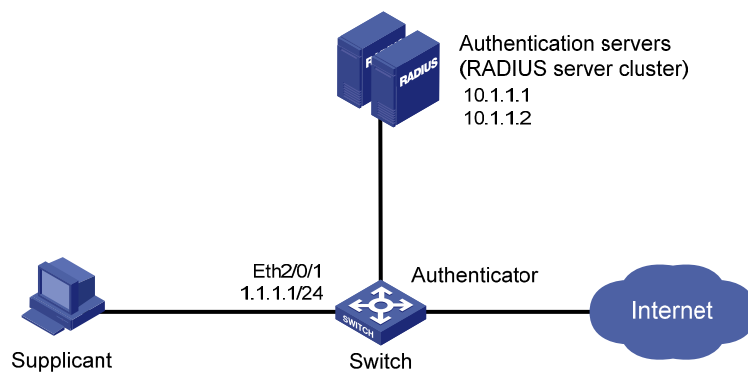
IEEE802 LAN/WAN 委员会为解决无线局域网网络安全问题，提出了 802.1x 协议。后来，802.1x 协议作为局域网端口的一个普通接入控制机制在以太网中被广泛应用，主要解决以太网内认证和安全方面的问题。

802.1x 协议是一种基于端口的网络接入控制协议（Port Based Network Access Control）。“基于端口的网络接入控制”是指在局域网接入设备的端口这一级对所接入的用户设备进行认证和控制。连接在端口上的用户设备如果能通过认证，就可以访问局域网中的资源；如果不能通过认证，则无法访问局域网中的资源。

## 1.2 802.1x 典型配置指导

### 1.2.1 组网图

图1-1 启动 802.1x 和 RADIUS 对接入用户进行 AAA 操作



### 1.2.2 应用要求

- 要求在各端口上对接入用户进行认证，以控制其访问 Internet；接入控制方式要求是基于 MAC 地址的接入控制。
- 所有接入用户都属于一个缺省的域：aabbcc.net，该域最多可容纳 30 个用户；认证时，先进行 RADIUS 认证，如果 RADIUS 服务器没有响应再转而进行本地认证；计费时，如果 RADIUS 计费失败则切断用户连接使其下线。
- 由两台 RADIUS 服务器组成的服务器组与交换机相连，其 IP 地址分别为 10.1.1.1 和 10.1.1.2，要求使用前者作为主认证/备份计费服务器，使用后者作为备份认证/主计费服务器。
- 设置系统与认证 RADIUS 服务器交互报文时的共享密钥为 name、与计费 RADIUS 服务器交互报文时的共享密钥为 money。
- 设置系统在向 RADIUS 服务器发送报文后 5 秒种内如果没有得到响应就向其重新发送报文，发送报文的次数总共为 5 次，设置系统每 15 分钟就向 RADIUS 服务器发送一次实时计费报文。
- 设置系统从用户名中去除用户域名后再将之传给 RADIUS 服务器。

- 本地 802.1x 接入用户的用户名为 localuser，密码为 localpass，使用明文输入；闲置切断功能处于打开状态，正常连接时用户空闲时间超过 20 分钟，则切断其连接。

### 1.2.3 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本                         |
|-------------------|---------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301 软件版本               | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301 软件版本               | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本               | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本               | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本                      |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本                      |

### 1.2.4 配置过程和解释

# 配置各接口的 IP 地址（略）。

# 添加本地接入用户，启动闲置切断功能并设置相关参数。

```
<Sysname> system-view
[Sysname] local-user localuser
[Sysname-luser-localuser] service-type lan-access
[Sysname-luser-localuser] password simple localpass
[Sysname-luser-localuser] attribute idle-cut 20
[Sysname-luser-localuser] quit
```

# 创建 RADIUS 方案 radius1 并进入其视图。

```
[Sysname] radius scheme radius1
```

# 设置主认证/计费 RADIUS 服务器的 IP 地址。

```
[Sysname-radius-radius1] primary authentication 10.1.1.1
[Sysname-radius-radius1] primary accounting 10.1.1.2
```

# 设置备份认证/计费 RADIUS 服务器的 IP 地址。

```
[Sysname-radius-radius1] secondary authentication 10.1.1.2
[Sysname-radius-radius1] secondary accounting 10.1.1.1
```

# 设置系统与认证 RADIUS 服务器交互报文时的共享密钥。

```
[Sysname-radius-radius1] key authentication name
```

# 设置系统与计费 RADIUS 服务器交互报文时的共享密钥。

```
[Sysname-radius-radius1] key accounting money
```

# 设置系统向 RADIUS 服务器重发报文的时间间隔与次数。

```
[Sysname-radius-radius1] timer response-timeout 5
[Sysname-radius-radius1] retry 5
```

# 设置系统向 RADIUS 服务器发送实时计费报文的时间间隔。

```
[Sysname-radius-radius1] timer realtime-accounting 15
```

# 指示系统从用户名中去除用户域名后再将之传给 RADIUS 服务器。

```
[Sysname-radius-radius1] user-name-format without-domain
```

```
[Sysname-radius-radius1] quit
```

# 创建域 aabbcc.net 并进入其视图。

```
[Sysname] domain aabbcc.net
```

# 指定 radius1 为该域用户的 RADIUS 方案，并采用 local 作为备选方案。

```
[Sysname-isp-aabbcc.net] authentication default radius-scheme radius1 local
```

```
[Sysname-isp-aabbcc.net] authorization default radius-scheme radius1 local
```

```
[Sysname-isp-aabbcc.net] accounting default radius-scheme radius1 local
```

# 设置该域最多可容纳 30 个用户。

```
[Sysname-isp-aabbcc.net] access-limit enable 30
```

# 启动闲置切断功能并设置相关参数。

```
[Sysname-isp-aabbcc.net] idle-cut enable 20
```

```
[Sysname-isp-aabbcc.net] quit
```

# 配置域 aabbcc.net 为缺省用户域。

```
[Sysname] domain default enable aabbcc.net
```

# 开启全局 802.1x 特性。

```
[Sysname] dot1x
```

# 开启指定端口 Ethernet2/0/1 的 802.1x 特性。

```
[Sysname] interface Ethernet 2/0/1
```

```
[Sysname-Ethernet2/0/1] dot1x
```

```
[Sysname-Ethernet2/0/1] quit
```

# 设置接入控制方式（该命令可以不配置，因为端口的接入控制在缺省情况下就是基于 MAC 地址的）。

```
[Sysname] dot1x port-method macbased interface Ethernet 2/0/1
```

### 1.2.5 完整配置

```

domain default enable aabbcc.net

dot1x

radius scheme radius1
primary authentication 10.1.1.1
primary accounting 10.1.1.2
secondary authentication 10.1.1.2
secondary accounting 10.1.1.1
key authentication name
key accounting money
timer realtime-accounting 15
```

```

timer response-timeout 5
user-name-format without-domain
retry 5
#
domain aabbcc.net
authentication default radius-scheme radius1 local
authorization default radius-scheme radius1 local
accounting default radius-scheme radius1 local
access-limit enable 30
#
local-user localuser
password simple localpass
service-type lan-access
attribute idle-cut 20
#
interface Ethernet2/0/1
dot1x
#

```

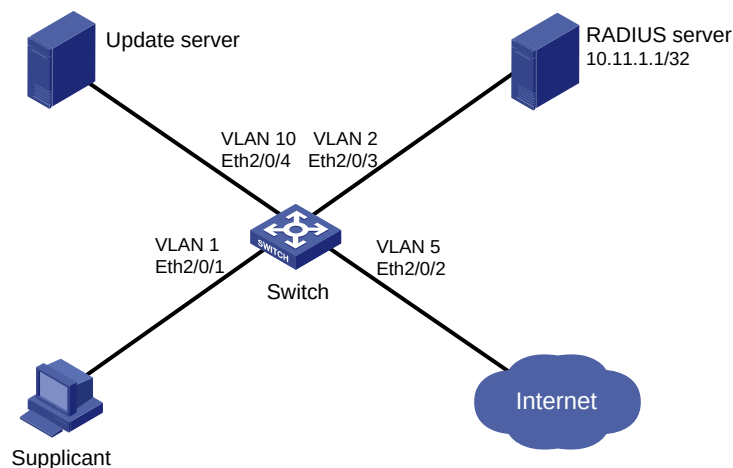
### 1.2.6 配置注意事项

- 只有同时开启全局和端口的 802.1x 特性后，802.1x 的配置才能在端口上生效。
- 一般情况下，用户无需使用 **dot1x timer** 命令改变部分定时器值，除非在一些特殊或恶劣的网络环境下，可以使用该命令调节交互进程。例如，用户网络状况比较差的情况下，可以适当地将客户端认证超时定时器值调大一些；网络处在风险位置，容易受攻击的情况下，可以适当地将静默定时器值调大一些，反之，可以将其调小一些来提高对用户认证请求的响应速度。另外，可以通过调节认证服务器超时定时器的值来适应认证服务器性能的不同情况。
- 对于 802.1x 用户，如果采用 EAP 中继认证方式，则设备会把客户端输入的内容直接封装后发给服务器，这种情况下 **user-name-format** 命令的设置无效。

## 1.3 Guest VLAN、动态下发 VLAN 典型配置举例

### 1.3.1 组网图

图1-2 GuestVlan、动态下发 VLAN 典型组网图



### 1.3.2 组网需求

- 主机通过 802.1x 认证接入网络，认证服务器为 RADIUS 服务器，RADIUS 服务器支持动态 VLAN 下发功能。
- 设置系统与 RADIUS 服务器交互报文时的共享密钥为 abc。
- Update Server 是用于客户端软件下载和升级的服务器，在 VLAN10 内。
- 交换机连接 Internet 网络的端口 Ethernet2/0/2 在 VLAN5 内。
- 当交换机从端口发送触发认证报文（EAP-Request/Identity）超过设定的最大次数而没有收到任何回应报文后，Ethernet2/0/1 被加入 Guest VLAN 中，此时 Supplicant 和 Update Server 都在 VLAN10 内，Supplicant 可以访问 Update Server 并下载 802.1x 客户端。
- 当用户认证成功上线，认证服务器下发 VLAN5。此时 Supplicant 和 Ethernet2/0/2 都在 VLAN5 内，Supplicant 可以访问 Internet。

### 1.3.3 适用产品、版本

表1-2 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本                         |
|-------------------|---------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301 软件版本               | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301 软件版本               | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本               | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本               | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本                      |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本                      |

### 1.3.4 配置过程和解释

# 配置 RADIUS 方案 2000。

```
<Sysname> system-view
[Sysname] radius scheme 2000
[Sysname-radius-2000] primary authentication 10.11.1.1 1812
[Sysname-radius-2000] primary accounting 10.11.1.1 1813
[Sysname-radius-2000] key authentication abc
[Sysname-radius-2000] key accounting abc
[Sysname-radius-2000] user-name-format without-domain
[Sysname-radius-2000] quit
```

# 配置 domain，该 domain 使用刚才配置好的 RADIUS 方案 2000。

```
[Sysname] domain system
[Sysname-isp-system] authentication default radius-scheme 2000
[Sysname-isp-system] authorization default radius-scheme 2000
[Sysname-isp-system] accounting default radius-scheme 2000
[Sysname-isp-system] quit
```



# 开启全局 802.1x 特性。

```
[Sysname] dot1x
```

# 开启指定端口的 802.1x 特性。

```
[Sysname] interface Ethernet 2/0/1
```

```
[Sysname-Ethernet2/0/1] dot1x
```

# 配置端口上进行接入控制的方式为 **portbased**。

```
[Sysname-Ethernet2/0/1] dot1x port-method portbased
```

# 配置端口上进行接入控制的模式为 **auto**。

```
[Sysname-Ethernet2/0/1] dot1x port-control auto
```

```
[Sysname-Ethernet2/0/1] quit
```

# 创建 VLAN10。

```
[Sysname] vlan 10
```

```
[Sysname-vlan10] quit
```

# 配置指定端口的 Guest VLAN。

```
[Sysname] dot1x guest-vlan 10 interface Ethernet 2/0/1
```

通过命令 **display current-configuration** 或者 **display interface Ethernet 2/0/1** 可以查看 Guest VLAN 配置情况。

在没有用户上线、用户认证失败或用户成功下线等情况下发送触发认证报文（EAP-Request/Identity）超过设定的最大次数时，通过命令 **display vlan 10** 可以查看端口配置的 Guest VLAN 是否生效。

在用户成功上线后，通过命令 **display vlan 5** 可以查看服务器下发的动态 VLAN 是否生效。

### 1.3.5 完整配置

```
#
radius scheme 2000
 primary authentication 10.11.1.1 1812
 primary accounting 10.11.1.1 1813
 key authentication abc
 key accounting abc
 user-name-format without-domain
#
domain system
 authentication default radius-scheme 2000
 authorization default radius-scheme 2000
 accounting default radius-scheme 2000
#
dot1x
dot1x guest-vlan 10 interface Ethernet 2/0/1
#
interface Ethernet 2/0/1
 dot1x
 dot1x port-method portbased
 dot1x port-control auto
```

```
quit
#
vlan 10
```

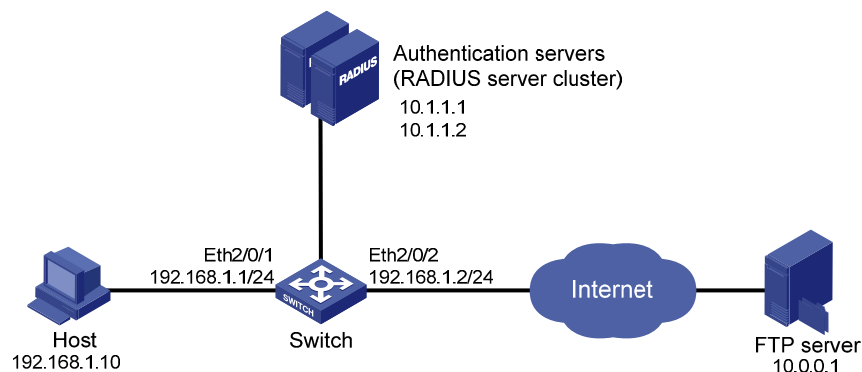
### 1.3.6 配置注意事项

- 当端口的接入控制方式为 **portbased** 时，Guest VLAN 才能生效；若端口的接入控制为 **macbased**，Guest VLAN 能够配置成功，但不生效。
- 802.1x 组播触发功能开启的情况下，Guest VLAN 才能生效。
- 如果某个 VLAN 被指定为 Super VLAN，则该 VLAN 不能被指定为某个端口的 Guest VLAN；同样，如果某个 VLAN 被指定为某个端口的 Guest VLAN，则该 VLAN 不能被指定为 Super VLAN。
- 可以指定携带 Tag 方式的 VLAN 为 Hybrid 端口的 Guest VLAN，但该 Guest VLAN 不会生效。同样当 Hybrid 端口的 Guest VLAN 生效后，则不能再配置该 Guest VLAN 为携带 Tag 方式的 VLAN。
- 不同的端口可以配置不同的 Guest VLAN，但一个端口只能配置一个 Guest VLAN。
- 如果用户端设备发出的是携带 Tag 的数据流，且接入端口上使能了 802.1x 认证和 Guest VLAN，为保证各种功能的正常使用，请为 Voice VLAN、端口的缺省 VLAN 和 802.1x 的 Guest VLAN 分配不同的 VLAN ID。

## 1.4 下发 ACL 应用典型配置指导

### 1.4.1 组网图

图1-3 下发 ACL 典型组网图



### 1.4.2 应用要求

如图 1-3 所示，主机 Host 通过 802.1x 认证接入网络，认证服务器为 RADIUS 服务器。Internet 网络中有一台 FTP 服务器，IP 地址为 10.0.0.1。

- 在认证服务器上配置授权下发 ACL 3000。
- 在 Switch 的 Ethernet2/0/1 上开启 802.1x 认证，并配置 ACL 3000。

当用户认证成功上线，认证服务器下发 ACL 3000。此时 ACL 3000 在 Ethernet2/0/1 上生效，Host 可以访问 Internet，但不能访问 FTP 服务器。

### 1.4.3 适用产品、版本

表1-3 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本                         |
|-------------------|---------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301 软件版本               | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301 软件版本               | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本               | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本               | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本                      |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本                      |

### 1.4.4 配置过程和解释

(1) 在 Switch 上配置 ACL 下发

# 配置各接口的 IP 地址（略）。

# 配置 RADIUS 方案。

```
<Sysname> system-view
[Sysname] radius scheme 2000
[Sysname-radius-2000] primary authentication 10.1.1.1 1812
[Sysname-radius-2000] primary accounting 10.1.1.2 1813
[Sysname-radius-2000] key authentication abc
[Sysname-radius-2000] key accounting abc
[Sysname-radius-2000] user-name-format without-domain
[Sysname-radius-2000] quit
```

# 配置 ISP 域的 AAA 方案。

```
[Sysname] domain 2000
[Sysname-isp-2000] authentication default radius-scheme 2000
[Sysname-isp-2000] authorization default radius-scheme 2000
[Sysname-isp-2000] accounting default radius-scheme 2000
[Sysname-isp-2000] quit
```

# 配置 ACL 3000，拒绝目的 IP 地址为 10.0.0.1 的报文通过。

```
[Sysname] acl number 3000
[Sysname-acl-adv-3000] rule 0 deny ip destination 10.0.0.1 0
```

# 开启全局 802.1x 特性。

```
[Sysname] dot1x
```

# 开启指定端口的 802.1x 特性。

```
[Sysname] interface Ethernet 2/0/1
[Sysname-Ethernet2/0/1] dot1x
```

### 1.4.5 完整配置

```
#
dot1x
#
radius scheme 2000
 primary authentication 10.1.1.1
 primary accounting 10.1.1.2
 key authentication abc
 key accounting abc
 user-name-format without-domain
#
domain 2000
 authentication default radius-scheme 2000
 authorization default radius-scheme 2000
 accounting default radius-scheme 2000
#
acl number 3000
 rule 0 deny ip destination 10.0.0.1 0
#
interface Ethernet2/0/1
 dot1x
#
```

### 1.4.6 配置注意事项

- 在服务器上配置授权 ACL 之前，需要在设备上配置相应的规则。
- 管理员可以通过改变服务器的授权 ACL 设置或设备上对应的 ACL 规则来改变用户的访问权限。

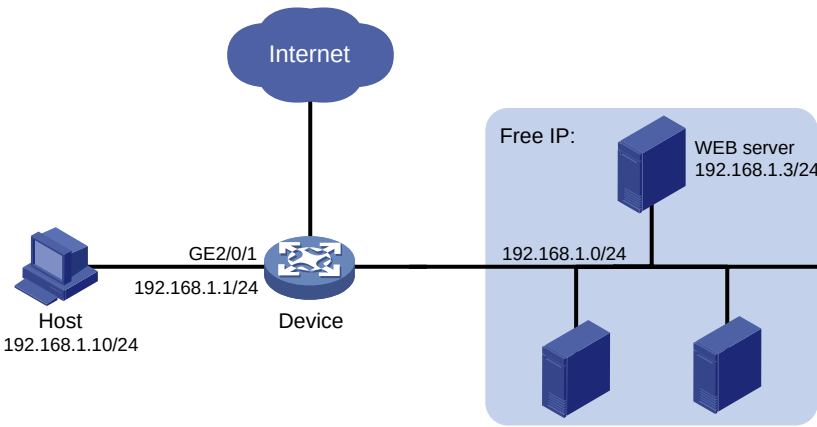
## 1.5 EAD 快速部署典型配置指导

EAD（Endpoint Admission Defense，端点准入防御）方案作为一个整合方案，提升了网络的整体防御能力。但是在实际的应用过程中 EAD 客户端的部署工作量很大，带来不便。

通过 802.1x 认证支持用户快速重定向到 EAD 客户端下载服务器，实现了 EAD 客户端的快速部署。

### 1.5.1 组网图

图1-4 EAD 快速部署典型配置组网图



### 1.5.2 应用要求

用户主机 Host 接入设备 Device，Device 与 Free IP 网段、外部网络相连。

- 认证成功之前，Host 通过浏览器访问外部网络会被重定向至 WEB 服务器，进行 802.1x 客户端的下载及安装。
- 认证成功之后，Host 可直接访问网络。

### 1.5.3 适用产品、版本

表1-4 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本                         |
|-------------------|---------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301 软件版本               | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301 软件版本               | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本               | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本               | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本                      |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本                      |

### 1.5.4 配置过程和解释

#### (1) 配置 WEB 服务器

用户在使用 EAD 快速部署功能之前首先必须配置好 WEB 服务器，即用户接入设备后用于下载 802.1x 客户端的重定向服务器。

#### (2) 配置 Device 支持 EAD 快速部署

# 配置各接口的 IP 地址（略）。

# 配置 Free IP。

```
<Device> system-view
```

```
[Device] dot1x free-ip 192.168.1.0 24
```

# 配置 IE 访问的重定向 URL。

```
[Device] dot1x url http://192.168.1.3
```

# 开启全局 802.1x 特性。

```
[Device] dot1x
```

# 开启指定端口的 802.1x 特性。

```
[Device] interface GigabitEthernet 2/0/1
```

```
[Device-GigabitEthernet2/0/1] dot1x
```

用户在 802.1x 认证成功之前，通过浏览器访问任何外部网站都会被重定向到 WEB server 页面，此页面提供客户端的下载服务。

### 1.5.5 完整配置

```
#
dot1x
dot1x url http://192.168.1.3
dot1x free-ip 192.168.1.0 255.255.255.0
#
interface GigabitEthernet2/0/1
dot1x
#
```

### 1.5.6 配置注意事项

- 目前，MAC 地址认证和端口安全特性不支持 EAD 的快速部署功能，全局使能 MAC 认证或端口安全功能将会使 EAD 快速部署功能失效。
- MAC 地址认证和 802.1x 特性的 Guest VLAN 功能与 Free IP 配置互斥。
- 未通过 802.1x 认证的用户在没有配置 Free IP 的情况下，不能通过 DHCP 服务器动态获得 IP 地址，但是若配置了 Free IP，并且与 DHCP 服务器在同一个网段时，用户便可以动态获得 IP 地址。
- 地址栏内输入的地址应该为 X.X.X.X（点分十进制格式）的非免费 IP 网段地址才会被重定向到 WEB server 页面。

# 目 录

|                                                     |      |
|-----------------------------------------------------|------|
| 1 AAA典型配置指导.....                                    | 1-1  |
| 1.1 AAA简介.....                                      | 1-1  |
| 1.2 Telnet用户通过HWTACACS服务器认证、授权、计费典型配置指导 .....       | 1-1  |
| 1.2.1 组网图.....                                      | 1-1  |
| 1.2.2 应用要求 .....                                    | 1-2  |
| 1.2.3 适用产品、版本 .....                                 | 1-2  |
| 1.2.4 配置过程和解释 .....                                 | 1-2  |
| 1.2.5 完整配置 .....                                    | 1-3  |
| 1.2.6 配置注意事项 .....                                  | 1-3  |
| 1.3 Telnet用户通过local认证、HWTACACS授权、RADIUS计费的应用配置..... | 1-4  |
| 1.3.1 组网图.....                                      | 1-4  |
| 1.3.2 应用要求 .....                                    | 1-4  |
| 1.3.3 适用产品、版本 .....                                 | 1-4  |
| 1.3.4 配置过程和解释 .....                                 | 1-5  |
| 1.3.5 完整配置 .....                                    | 1-5  |
| 1.3.6 配置注意事项 .....                                  | 1-6  |
| 1.4 SSH用户通过RADIUS服务器认证、授权、计费的应用配置.....              | 1-6  |
| 1.4.1 组网图.....                                      | 1-6  |
| 1.4.2 应用要求 .....                                    | 1-6  |
| 1.4.3 适用产品、版本 .....                                 | 1-7  |
| 1.4.4 配置过程和解释 .....                                 | 1-7  |
| 1.4.5 完整配置 .....                                    | 1-8  |
| 1.5 EAD应用配置 .....                                   | 1-9  |
| 1.5.1 组网图.....                                      | 1-9  |
| 1.5.2 应用要求 .....                                    | 1-9  |
| 1.5.3 适用产品、版本 .....                                 | 1-9  |
| 1.5.4 配置过程和解释 .....                                 | 1-10 |
| 1.5.5 完整配置 .....                                    | 1-11 |

# 1 AAA 典型配置指导

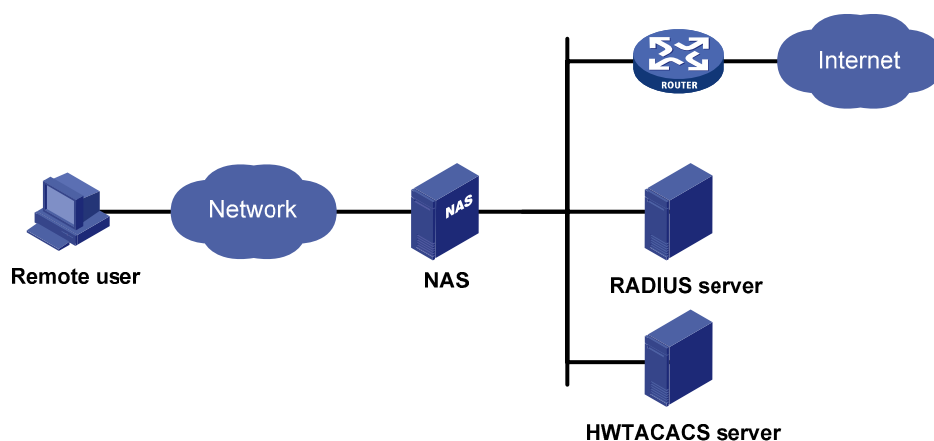
## 1.1 AAA 简介

AAA 是 Authentication、Authorization、Accounting（认证、授权、计费）的简称，是网络安全的一种管理机制，提供了认证、授权、计费三种安全功能。

AAA 是运行于 NAS（Network Access Server，网络接入服务器）上的客户端程序，它提供了一个对认证、授权和计费这三种安全功能进行统一配置的框架。

AAA 一般采用客户机/服务器结构，客户端运行于 NAS 上，服务器上则集中管理用户信息。NAS 对于用户来讲是服务器端，对于服务器来说是客户端。AAA 的基本组网结构如图 1-1。

图1-1 AAA 基本组网结构示意图

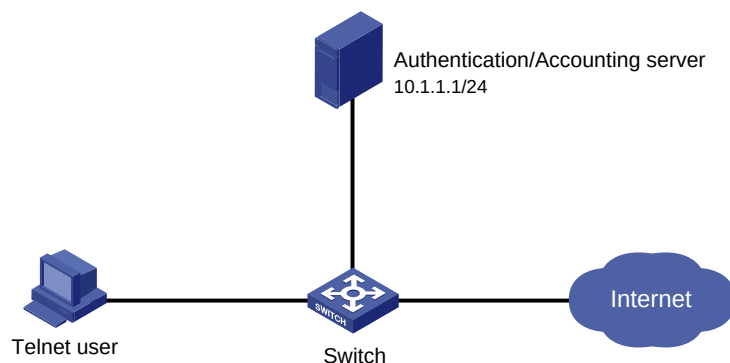


当用户想要通过某网络与 NAS 建立连接，从而获得访问其它网络的权利或取得某些网络资源权利时，NAS 起到了验证用户或对应连接的作用。NAS 负责把用户的认证、授权、计费信息透传给服务器（RADIUS 服务器或 HWTACACS 服务器），RADIUS 协议或 HWTACACS 协议规定了 NAS 与服务器之间如何传递用户信息。

## 1.2 Telnet 用户通过 HWTACACS 服务器认证、授权、计费典型配置指导

### 1.2.1 组网图

图1-2 配置 Telnet 用户的远端 HWTACACS 认证、授权和计费





### 1.2.2 应用要求

通过配置 Switch 实现 HWTACACS 服务器对登录 Switch 的用户进行认证、授权、计费，如果 HWTACACS 服务器无响应，则切换为备选 Local 认证。

- 一台 HWTACACS 服务器（担当认证、授权、计费服务器的职责）与 Switch 相连，服务器 IP 地址为 10.1.1.1。
- Switch 与认证、授权、计费 HWTACACS 服务器交互报文时的共享密钥均为 expert，发送给 HWTACACS 服务器的用户名中不带域名。
- 在 HWTACACS 服务器上设置与 Switch 交互报文时的共享密钥为 expert。

### 1.2.3 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本                         |
|-------------------|---------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本               | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本               | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本                      |

### 1.2.4 配置过程和解释

# 开启 Switch 的 Telnet 服务器功能。

```
<Switch> system-view
```

```
[Switch] telnet server enable
```

# 配置 Telnet 用户登录采用 AAA 认证方式。

```
[Switch] user-interface vty 0 4
```

```
[Switch-ui-vty0-4] authentication-mode scheme
```

```
[Switch-ui-vty0-4] quit
```

# 配置 HWTACACS 方案。

```
[Switch] hwtacacs scheme hwtac
```

```
[Switch-hwtacacs-hwtac] primary authentication 10.1.1.1 49
```

```
[Switch-hwtacacs-hwtac] primary authorization 10.1.1.1 49
```

```
[Switch-hwtacacs-hwtac] primary accounting 10.1.1.1 49
```

```
[Switch-hwtacacs-hwtac] key authentication expert
```

```
[Switch-hwtacacs-hwtac] key authorization expert
```

```
[Switch-hwtacacs-hwtac] key accounting expert
```

```
[Switch-hwtacacs-hwtac] user-name-format without-domain
```

```
[Switch-hwtacacs-hwtac] quit
```

# 配置 ISP 域的 AAA 方案。

```
[Switch] domain 1
[Switch-isp-1] authentication login hwtacacs-scheme hwtac local
[Switch-isp-1] authorization login hwtacacs-scheme hwtac local
[Switch-isp-1] accounting login hwtacacs-scheme hwtac local
[Switch-isp-1] quit
```

# 创建本地用户 telnet。

```
[Switch] local-user telnet
[Switch-luser-telnet] service-type telnet
[Switch-luser-telnet] password simple telnet
```

### 1.2.5 完整配置

```
#
telnet server enable
#
hwtacacs scheme hwtac
primary authentication 10.1.1.1
primary authorization 10.1.1.1
primary accounting 10.1.1.1
key authentication expert
key authorization expert
key accounting expert
user-name-format without-domain
#
domain 1
authentication login hwtacacs-scheme hwtac local
authorization login hwtacacs-scheme hwtac local
accounting login hwtacacs-scheme hwtac local
#
user-interface aux 0
user-interface vty 0 4
authentication-mode scheme
#
local-user telnet
service-type telnet
password simple telnet
```

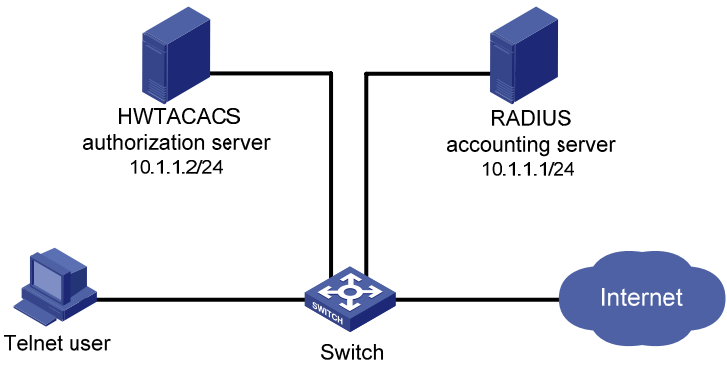
### 1.2.6 配置注意事项

使用 Telnet 登陆时输入用户名为 `userid@1`，以使用域 1 进行认证。

# 1.3 Telnet 用户通过 local 认证、HWTACACS 授权、RADIUS 计费的应用配置

## 1.3.1 组网图

图1-3 配置 Telnet 用户的 local 认证，HWTACACS 授权和 RADIUS 计费



## 1.3.2 应用要求

通过配置 Switch 实现 local 认证，HWTACACS 授权和 RADIUS 计费。Telnet 用户的用户名和密码为 telnet。

- 一台 HWTACACS 服务器(担当授权服务器的职责)与 Switch 相连,服务器 IP 地址为 10.1.1.2。Switch 与授权 HWTACACS 服务器交互报文时的共享密钥均为 expert，发送给 HWTACACS 服务器的用户名中不带域名。
- 一台 RADIUS 服务器（担当计费服务器的职责）与 Switch 相连，服务器 IP 地址为 10.1.1.1。Switch 与计费 RADIUS 服务器交互报文时的共享密钥为 expert。



说明

其他接入如果需要此类 AAA 应用，和 Telnet 在域的 AAA 配置上类似，只有接入的区分。

## 1.3.3 适用产品、版本

表1-2 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本                         |
|-------------------|---------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本               | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本               | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本                      |

### 1.3.4 配置过程和解释

# 配置各接口的 IP 地址（略）。

# 开启 Switch 的 Telnet 服务器功能。

```
<Switch> system-view
```

```
[Switch] telnet server enable
```

# 配置 Telnet 用户登录采用 AAA 认证方式。

```
[Switch] user-interface vty 0 4
```

```
[Switch-ui-vty0-4] authentication-mode scheme
```

```
[Switch-ui-vty0-4] quit
```

# 配置 HWTACACS 方案。

```
[Switch] hwtacacs scheme hwtac
```

```
[Switch-hwtacacs-hwtac] primary authorization 10.1.1.2 49
```

```
[Switch-hwtacacs-hwtac] key authorization expert
```

```
[Switch-hwtacacs-hwtac] user-name-format without-domain
```

```
[Switch-hwtacacs-hwtac] quit
```

# 配置 RADIUS 方案。

```
[Switch] radius scheme rd
```

```
[Switch-radius-rd] primary accounting 10.1.1.1 1813
```

```
[Switch-radius-rd] key accounting expert
```

```
[Switch-radius-rd] server-type extended
```

```
[Switch-radius-rd] user-name-format without-domain
```

```
[Switch-radius-rd] quit
```

# 创建本地用户 telnet。

```
[Switch] local-user telnet
```

```
[Switch-luser-telnet] service-type telnet
```

```
[Switch-luser-telnet] password simple telnet
```

# 配置 ISP 域的 AAA 方案。

```
[Switch] domain 1
```

```
[Switch-isp-1] authentication login local
```

```
[Switch-isp-1] authorization login hwtacacs-scheme hwtac
```

```
[Switch-isp-1] accounting login radius-scheme rd
```

```
[Switch-isp-1] quit
```

### 1.3.5 完整配置

```
#
```

```
telnet server enable
```

```
#
```

```
hwtacacs scheme hwtac
```

```
primary authorization 10.1.1.2
```

```
key authorization expert
```

```
user-name-format without-domain
```

```
#
```

```

radius scheme rd
primary accounting 10.1.1.1 1813
key accounting expert
server-type extended
user-name-format without-domain
#
domain 1
authentication login local
authorization login hwtacacs-scheme hwtac
accounting login radius-scheme rd
#
local-user telnet
password simple telnet
service-type telnet
#
user-interface aux 0
user-interface vty 0 4
authentication-mode scheme
#

```

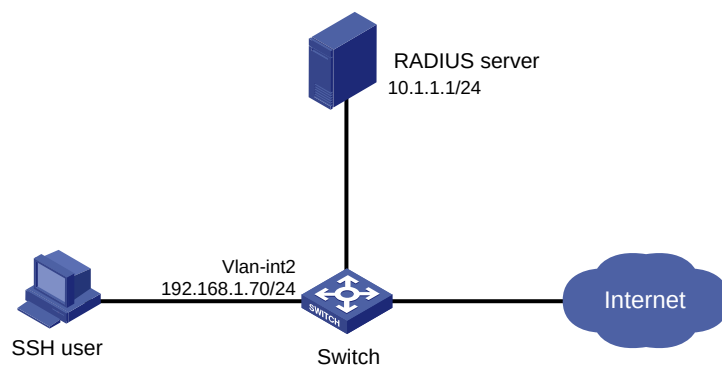
### 1.3.6 配置注意事项

使用 Telnet 登陆时输入用户名为 telnet@1，以使用域 1 进行认证。

## 1.4 SSH 用户通过 RADIUS 服务器认证、授权、计费的应用配置

### 1.4.1 组网图

图1-4 SSH 用户 RADIUS 认证、授权和计费配置组网图



### 1.4.2 应用要求

如 图 1-4所示，配置Switch实现RADIUS服务器对登录Switch的SSH用户进行认证、授权和计费。

- 一台 RADIUS 服务器（其担当认证 RADIUS 服务器和计费 RADIUS 服务器的职责）与 Switch 相连，服务器 IP 地址为 10.1.1.1。
- Switch 与认证、计费 RADIUS 服务器交互报文时的共享密钥均为 expert，发送给 RADIUS 服务器的用户名带域名。
- RADIUS 服务器使用 CAMS 服务器。

### 1.4.3 适用产品、版本

表1-3 配置适用的产品与软硬件版本关系

| 产品                | 软件版本              | 硬件版本                         |
|-------------------|-------------------|------------------------------|
| S5500-SI 系列以太网交换机 | Release 1207 软件版本 | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本 | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本 | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6300 软件版本 | 全系列硬件版本                      |

### 1.4.4 配置过程和解释

#### (1) 配置 RADIUS server



##### 说明

本文以 CAMS 服务器 V2.10 为例，说明该例中 RADIUS server 的基本配置。

# 增加接入设备。

登录进入 CAMS 管理平台，点击左侧菜单树中【系统管理】->【系统配置】的“接入设备配置”->“修改”->“增加”后，进入接入设备配置页面。

- 添加 Switch 的 IP 地址 192.168.1.70;
- 设置与 Switch 交互报文时的认证、计费共享密钥为 expert;
- 选择协议类型为 LAN 接入业务;
- 设置认证及计费的端口号分别为 1812 和 1813;
- 选择 RADIUS 协议类型为扩展协议;
- 选择 RADIUS 报文类型为标准报文。

# 增加设备管理用户。

点击左侧菜单树中【用户管理】->【设备管理用户】的“增加”后，进入设备管理用户配置页面。

- 添加用户名 hello@bbb 和密码;
- 选择服务类型为 SSH;
- 设置 EXEC 权限级别为 3;
- 添加所管理主机 IP 地址范围。

#### (2) 配置 Switch

# 配置 VLAN 接口 2 的 IP 地址，SSH 客户端将通过该地址连接 SSH 服务器。

```
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.1.70 255.255.255.0
[Switch-Vlan-interface2] quit
```

# 生成 RSA 及 DSA 密钥对，并启动 SSH 服务器。

```
[Switch] public-key local create rsa
```

```

[Switch] public-key local create dsa
[Switch] ssh server enable
配置 SSH 用户登录采用 AAA 认证方式。
[Switch] user-interface vty 0 4
[Switch-ui-vty0-4] authentication-mode scheme
配置用户远程登录 Switch 的协议为 SSH。
[Switch-ui-vty0-4] protocol inbound ssh
[Switch-ui-vty0-4] quit
配置 RADIUS 方案。
[Switch] radius scheme rad
[Switch-radius-rad] primary authentication 10.1.1.1 1812
[Switch-radius-rad] primary accounting 10.1.1.1 1813
[Switch-radius-rad] key authentication expert
[Switch-radius-rad] key accounting expert
[Switch-radius-rad] user-name-format with-domain
[Switch-radius-rad] quit
配置 ISP 域的 AAA 方案。
[Switch] domain bbb
[Switch-isp-bbb] authentication login radius-scheme rad
[Switch-isp-bbb] authorization login radius-scheme rad
[Switch-isp-bbb] accounting login radius-scheme rad
[Switch-isp-bbb] quit

```

使用 SSH 登陆时输入用户名为 *userid@bbb*，以使用域 *bbb* 进行认证。

### (3) SSH 用户建立与 Switch 的连接

在 SSH 客户端按照提示输入用户名 *hello@bbb* 及密码，即可进入 Switch 的用户界面。用户登录系统后所能访问的命令级别由 CAMS 服务器授权，可通过设备管理用户界面的 EXEC 权限级别来设置。

## 1.4.5 完整配置

```

#
radius scheme rad
 primary authentication 10.1.1.1 1812
 primary accounting 10.1.1.1 1813
 key authentication expert
 key accounting expert
 user-name-format with-domain
#
domain bbb
 authentication login radius-scheme rad
 authorization login radius-scheme rad
 accounting login radius-scheme rad
#
ssh server enable
#

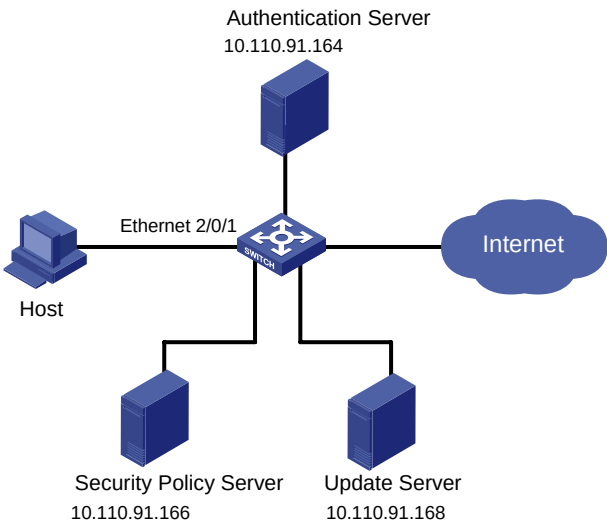
```

```
user-interface vty 0 4
authentication-mode scheme
protocol inbound ssh
```

1.5 EAD 应用配置

1.5.1 组网图

图1-5 EAD 典型配置组网图



1.5.2 应用要求

- Host 与以太网交换机的端口 Ethernet 2/0/1 相连接。
- 通过对交换机的配置，认证成功之前，Host 通过浏览器访问外部网络会被重定向至 Update 服务器，进行 802.1x 客户端的下载及安装。
- 通过对交换机、RADIUS 服务器、安全策略服务器的配置，实现 RADIUS 服务器对接入用户的远端认证和安全策略服务器对用户的 EAD 操作控制。

说明

本配置举例给出交换机上的相应配置，RADIUS 服务器、安全策略服务器的相关配置，请参见相应服务器的说明。

1.5.3 适用产品、版本

表1-4 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本                         |
|-------------------|---------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本               | 全系列硬件版本<br>(除 S5500-20TP-SI) |



| 产品                | 软件版本                            | 硬件版本          |
|-------------------|---------------------------------|---------------|
|                   | Release 1301 软件版本               | S5500-20TP-SI |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本       |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本       |

#### 1.5.4 配置过程和解释

##### (1) 配置 WEB 服务器

用户在使用 EAD 快速部署功能之前首先必须配置好 Update 服务器做为 WEB 服务器，即用于下载 802.1x 客户端的重定向服务器。

##### (2) 配置 EAD 快速部署

# 配置 Free IP。

```
<Switch> system-view
[Switch] dot1x free-ip 10.110.91.0 24
```

# 配置 IE 访问的重定向 URL。

```
[Switch] dot1x url http:// 10.110.91.168
```

# 开启全局 802.1x 特性。

```
[Switch] dot1x
```

# 开启指定端口的 802.1x 特性。

```
[Switch] interface ethernet 2/0/1
[Switch-Ethernet2/0/1] dot1x
```

##### (3) 配置 EAD 功能

# 配置 RADIUS 方案。

```
[Switch] radius scheme cams
[Switch-radius-cams] primary authentication 10.110.91.164 1812
[Switch-radius-cams] primary accounting 10.110.91.164 1813
[Switch-radius-cams] key authentication expert
[Switch-radius-cams] key accounting expert
[Switch-radius-cams] user-name-format with-domain
[Switch-radius-cams] server-type extended
```

# 配置安全策略服务器地址。

```
[Switch-radius-cams] security-policy-server 10.110.91.166
```

#配置缺省的 AAA 方案。

```
[Switch] domain aaa
[Switch-isp-aaa] authentication default radius-scheme cams
[Switch-isp-aaa] authorization default radius-scheme cams
[Switch-isp-aaa] accounting default radius-scheme cams
```

使用 Telnet 登陆时输入用户名为 *userid@aaa*，以使用域 *aaa* 进行认证。

##### (4) 用户连接

用户在 802.1x 认证成功之前，通过浏览器访问任何外部网站都会被重定向到 Update Server 页面，此页面提供客户端的下载服务。

下载客户端，并输入正确的用户名、密码，客户端通过认证服务器的身份验证以后，安全客户端对 Host 的安全状况进行检测，并与安全策略服务器交互，如果不符合安全认证的标准，安全策略服务器下发 ACL 控制报文到交换机，交换机只允许客户端访问 Update 服务器。

只有当客户端安装了补丁，并且客户端的安全标准满足了安全认证的标准以后，安全客户端将客户端的安全状态传递到安全策略服务器，安全策略服务器将再次下发 ACL，使交换机打开客户端的访问权限，使之能够访问更多的网络资源。

### 1.5.5 完整配置

```
#
radius scheme cams
 primary authentication 10.110.91.164 1812
 primary accounting 10.110.91.164 1813
 key authentication expert
 key accounting expert
 user-name-format with-domain
 server-type extended
 security-policy-server 10.110.91.166
#
domain aaa
 authentication default radius-scheme cams
 authorization default radius-scheme cams
 accounting default radius-scheme cams
#
dot1x
 dot1x free-ip 10.110.91.0 24
 dot1x url http:// 10.110.91.168
#
interface ethernet 2/0/1
 dot1x
#
```

# 目 录

|                               |     |
|-------------------------------|-----|
| 1 MAC地址认证典型配置指导.....          | 1-1 |
| 1.1 MAC地址认证简介.....            | 1-1 |
| 1.2 MAC地址本地认证典型配置指导.....      | 1-1 |
| 1.2.1 组网图.....                | 1-1 |
| 1.2.2 应用要求 .....              | 1-1 |
| 1.2.3 适用产品、版本 .....           | 1-2 |
| 1.2.4 配置过程和解释 .....           | 1-2 |
| 1.2.5 完整配置 .....              | 1-3 |
| 1.2.6 配置注意事项 .....            | 1-3 |
| 1.3 MAC地址RADIUS认证典型配置指导 ..... | 1-3 |
| 1.3.1 组网图.....                | 1-3 |
| 1.3.2 应用要求 .....              | 1-3 |
| 1.3.3 适用产品、版本 .....           | 1-4 |
| 1.3.4 配置过程和解释 .....           | 1-4 |
| 1.3.5 完整配置 .....              | 1-5 |
| 1.3.6 配置注意事项 .....            | 1-5 |
| 1.4 下发ACL典型配置指导 .....         | 1-6 |
| 1.4.1 组网图.....                | 1-6 |
| 1.4.2 应用要求 .....              | 1-6 |
| 1.4.3 适用产品、版本 .....           | 1-6 |
| 1.4.4 配置过程和解释 .....           | 1-6 |
| 1.4.5 完整配置 .....              | 1-7 |
| 1.4.6 配置注意事项 .....            | 1-8 |

# 1 MAC 地址认证典型配置指导

## 1.1 MAC 地址认证简介

MAC 地址认证是一种基于端口和 MAC 地址对用户的网络访问权限进行控制的认证方法，它不需要用户安装任何客户端软件。设备在首次检测到用户的 MAC 地址以后，即启动对该用户的认证操作。认证过程中，也不需要用户手动输入用户名或者密码。

目前设备支持两种方式的 MAC 地址认证：

- 通过 RADIUS（Remote Authentication Dial-In User Service，远程认证拨号用户服务）服务器认证。
- 本地认证。

有关远程 RADIUS 认证和本地认证的详细介绍请参见“AAA-RADIUS-HWTACACS 操作”。

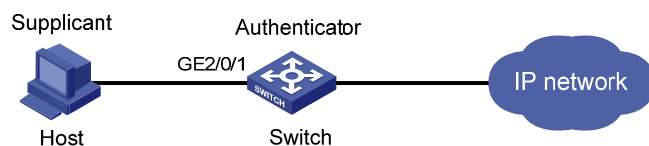
认证方式确定后，可根据需求选择 MAC 认证用户名的类型，包括以下两种方式：

- MAC 地址用户名：使用用户的 MAC 地址作为认证时的用户名和密码；
- 固定用户名：不论用户的 MAC 地址为何值，所有用户均使用在设备上预先配置的本地用户名和密码进行认证。

## 1.2 MAC 地址本地认证典型配置指导

### 1.2.1 组网图

图1-1 启动 MAC 地址认证对接入用户进行本地认证



### 1.2.2 应用要求

如图 1-1所示，某用户的工作站与以太网设备的端口GigabitEthernet2/0/1 相连接。

- 设备的管理者希望在各端口上对用户接入进行 MAC 地址认证，以控制其对 Internet 的访问。
- 要求设备每隔 180 秒就对用户是否下线进行检测；并且当用户认证失败时，需等待 3 分钟后才能对用户再次发起认证。
- 所有用户都属于域：aabbcc.net，认证时使用本地认证的方式。用户名为 aaa，密码为 123456。

### 1.2.3 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本                         |
|-------------------|---------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本               | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本               | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本                      |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本                      |

### 1.2.4 配置过程和解释

(1) 在交换机上配置 MAC 地址认证

# 添加本地接入用户。

```
<Switch> system-view
[Switch] local-user aaa
[Switch-luser-aaa] password simple 123456
[Switch-luser-aaa] service-type lan-access
[Switch-luser-aaa] quit
```

# 配置 ISP 域，使用本地认证方式。

```
[Switch] domain aabbcc.net
[Switch-isp-aabbcc.net] authentication lan-access local
[Switch-isp-aabbcc.net] quit
```

# 开启全局 MAC 地址认证特性。

```
[Switch] mac-authentication
```

# 开启端口 GigabitEthernet2/0/1 的 MAC 地址认证特性。

```
[Switch] mac-authentication interface GigabitEthernet 2/0/1
```

# 配置 MAC 地址认证用户所使用的 ISP 域。

```
[Switch] mac-authentication domain aabbcc.net
```

# 配置 MAC 地址认证的定时器。

```
[Switch] mac-authentication timer offline-detect 180
[Switch] mac-authentication timer quiet 180
```

# 配置 MAC 地址认证使用固定用户名、密码格式。

```
[Switch] mac-authentication user-name-format fixed account aaa password simple 123456
```

## 1.2.5 完整配置

```
#
system-view
local-user aaa
password simple 123456
service-type lan-access
#
domain aabbcc.net
authentication lan-access local
#
mac-authentication
mac-authentication timer offline-detect 180
mac-authentication timer quiet 180
mac-authentication domain aabbcc.net
mac-authentication user-name-format fixed account aaa password simple 123456
#
interface GigabitEthernet2/0/1
mac-authentication
#
```

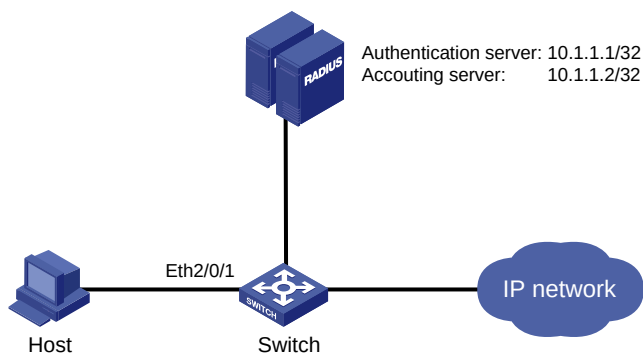
## 1.2.6 配置注意事项

本地用户的服务类型应设置为 **lan-access**。

# 1.3 MAC 地址 RADIUS 认证典型配置指导

## 1.3.1 组网图

图1-2 启动 MAC 地址认证对接入用户进行 RADIUS 认证



## 1.3.2 应用要求

如图 1-2所示，用户主机Host通过端口Ethernet2/0/1 连接到设备上，设备通过RADIUS服务器对用户进行身份认证。

- 设备的管理者希望在各端口上对用户接入进行 MAC 地址认证，以控制其对 Internet 的访问。
- 要求设备每隔 180 秒就对用户是否下线进行检测；并且当用户认证失败时，需等待 3 分钟后才能对用户再次发起认证。

### 1.3.3 适用产品、版本

表1-2 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本                         |
|-------------------|---------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本               | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本               | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本                      |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本                      |

### 1.3.4 配置过程和解释

(1) 在 Device 上配置 MAC 地址认证

# 配置各接口的 IP 地址（略）。

# 配置 RADIUS 方案。

```
[Switch> system-view
[Switch] radius scheme 2000
[Switch-radius-2000] primary authentication 10.1.1.1 1812
[Switch-radius-2000] primary accounting 10.1.1.2 1813
[Switch-radius-2000] key authentication abc
[Switch-radius-2000] key accounting abc
[Switch-radius-2000] user-name-format without-domain
[Switch-radius-2000] quit
```

# 配置 ISP 域的 AAA 方案。

```
[Switch] domain 2000
[Switch-isp-2000] authentication default radius-scheme 2000
[Switch-isp-2000] authorization default radius-scheme 2000
[Switch-isp-2000] accounting default radius-scheme 2000
[Switch-isp-2000] quit
```

# 开启全局 MAC 地址认证特性。

```
[Switch] mac-authentication
```

# 开启端口 GigabitEthernet2/0/1 的 MAC 地址认证特性。

```
[Switch] mac-authentication interface Ethernet 2/0/1
```

# 配置 MAC 地址认证用户所使用的 ISP 域。

```
[Switch] mac-authentication domain 2000
```

# 配置 MAC 地址认证的定时器。

```
[Switch] mac-authentication timer offline-detect 180
```

```
[Switch] mac-authentication timer quiet 180
```

# 配置 MAC 地址认证使用固定用户名、密码格式。

```
[Switch] mac-authentication user-name-format fixed account aaa password simple 123456
```

### 1.3.5 完整配置

```
#
radius scheme 2000
 primary authentication 10.1.1.1
 primary accounting 10.1.1.2
 key authentication abc
 key accounting abc
 user-name-format without-domain

#
domain 2000
 authentication default radius-scheme 2000
 authorization default radius-scheme 2000
 accounting default radius-scheme 2000

#
mac-authentication
 mac-authentication timer offline-detect 180
 mac-authentication timer quiet 180
 mac-authentication domain 2000
 mac-authentication user-name-format fixed account aaa password simple 123456

#
interface Ethernet2/0/1
 mac-authentication

#
```

### 1.3.6 配置注意事项

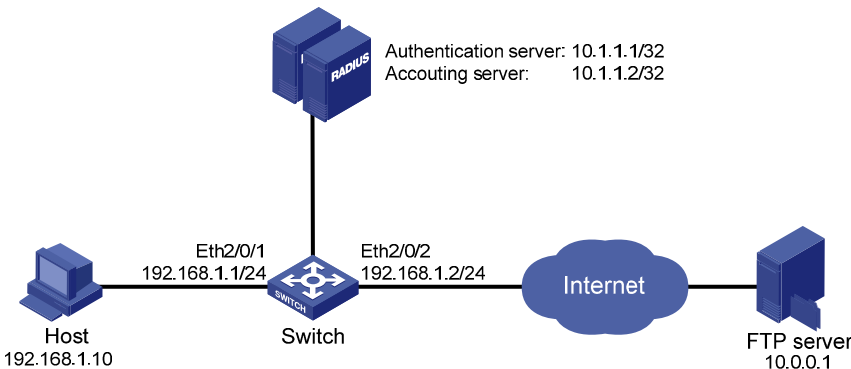
- RADIUS 服务器上配置的用户名和密码必须与设备上配置的 MAC 地址认证的用户名和密码保持一致。
- RADIUS 服务器上配置的认证、计费 Key 需要和交换机上配置保持一致，才能认证成功。



# 1.4 下发 ACL 典型配置指导

## 1.4.1 组网图

图1-3 下发 ACL 典型配置组网图



## 1.4.2 应用要求

如图 1-3所示，主机Host通过MAC认证接入网络，认证服务器为RADIUS服务器。Internet网络中有一台FTP服务器，IP地址为 10.0.0.1。

- 在认证服务器上配置授权下发 ACL 3000。
- 在 Switch 的 Ethernet2/0/1 上开启 MAC 认证，并配置 ACL 3000。
- 当用户认证成功上线，认证服务器下发 ACL 3000。此时 ACL 3000 在 Ethernet2/0/1 上生效，Host 可以访问 Internet，但不能访问 FTP 服务器。

## 1.4.3 适用产品、版本

表1-3 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本                         |
|-------------------|---------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本               | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本               | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本                      |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本                      |

## 1.4.4 配置过程和解释

(1) 在 Device 上配置 MAC 地址认证

# 配置各接口的 IP 地址（略）。

# 配置 RADIUS 方案。

```
[Switch> system-view
[Switch] radius scheme 2000
[Switch-radius-2000] primary authentication 10.1.1.1 1812
[Switch-radius-2000] primary accounting 10.1.1.2 1813
[Switch-radius-2000] key authentication abc
[Switch-radius-2000] key accounting abc
[Switch-radius-2000] user-name-format without-domain
[Switch-radius-2000] quit
```

# 配置 ISP 域的 AAA 方案。

```
[Switch] domain 2000
[Switch-isp-2000] authentication default radius-scheme 2000
[Switch-isp-2000] authorization default radius-scheme 2000
[Switch-isp-2000] accounting default radius-scheme 2000
[Switch-isp-2000] quit
```

# 配置 ACL 3000，拒绝目的 IP 地址为 10.0.0.1 的报文通过。

```
[Sysname] acl number 3000
[Sysname-acl-adv-3000] rule 0 deny ip destination 10.0.0.1 0
[Sysname-acl-adv-3000] quit
```

# 开启全局 MAC 地址认证特性。

```
[Switch] mac-authentication
```

# 开启端口 Ethernet2/0/1 的 MAC 地址认证特性。

```
[Switch] mac-authentication interface Ethernet 2/0/1
```

# 配置 MAC 地址认证用户所使用的 ISP 域。

```
[Switch] mac-authentication domain 2000
```

# 配置 MAC 地址认证的定时器。

```
[Switch] mac-authentication timer offline-detect 180
[Switch] mac-authentication timer quiet 180
```

# 配置 MAC 地址认证用户名格式。使用带连字符的 MAC 地址作为用户名与密码。

```
[Switch] mac-authentication user-name-format mac-address with-hyphen
```

### 1.4.5 完整配置

```
#
radius scheme 2000
primary authentication 10.1.1.1
primary accounting 10.1.1.2
key authentication abc
key accounting abc
user-name-format without-domain

#
domain 2000
authentication default radius-scheme 2000
authorization default radius-scheme 2000
accounting default radius-scheme 2000
```

```
#
acl number 3000
 rule 0 deny ip destination 10.0.0.1 0
#
mac-authentication
 mac-authentication timer offline-detect 180
 mac-authentication timer quiet 180
 mac-authentication domain 2000
 mac-authentication user-name-format mac-address with-hyphen
#
interface Ethernet2/0/1
 mac-authentication
#
```

#### 1.4.6 配置注意事项

- RADIUS 服务器上配置的认证、计费 Key 需要和交换机上配置保持一致，才能认证成功。
- RADIUS 服务器上配置的用户名和密码的类型必须与设备上配置的 MAC 地址认证的用户名和密码类型保持一致。
- 作为用户名和密码的 MAC 地址中的字母必须为小写字母。

# 目 录

|                                     |      |
|-------------------------------------|------|
| 1 Portal典型配置指导 .....                | 1-1  |
| 1.1 Portal简介 .....                  | 1-1  |
| 1.2 Portal直接认证方式典型配置指导 .....        | 1-1  |
| 1.2.1 组网图 .....                     | 1-1  |
| 1.2.2 应用要求 .....                    | 1-1  |
| 1.2.3 适用产品、版本 .....                 | 1-1  |
| 1.2.4 配置过程和解释 .....                 | 1-2  |
| 1.2.5 完整配置 .....                    | 1-3  |
| 1.2.6 配置注意事项 .....                  | 1-3  |
| 1.3 Portal二次地址分配认证方式典型配置指导 .....    | 1-4  |
| 1.3.1 组网图 .....                     | 1-4  |
| 1.3.2 应用要求 .....                    | 1-4  |
| 1.3.3 适用产品、版本 .....                 | 1-4  |
| 1.3.4 配置过程和解释 .....                 | 1-4  |
| 1.3.5 完整配置 .....                    | 1-5  |
| 1.3.6 配置注意事项 .....                  | 1-6  |
| 1.4 三层Portal认证方式典型配置指导 .....        | 1-6  |
| 1.4.1 组网图 .....                     | 1-6  |
| 1.4.2 应用要求 .....                    | 1-6  |
| 1.4.3 适用产品、版本 .....                 | 1-7  |
| 1.4.4 配置过程和解释 .....                 | 1-7  |
| 1.4.5 完整配置 .....                    | 1-7  |
| 1.4.6 配置注意事项 .....                  | 1-8  |
| 1.5 Portal直接认证方式（支持EAD）典型配置指导 ..... | 1-8  |
| 1.5.1 组网图 .....                     | 1-8  |
| 1.5.2 应用要求 .....                    | 1-8  |
| 1.5.3 适用产品、版本 .....                 | 1-9  |
| 1.5.4 配置过程和解释 .....                 | 1-9  |
| 1.5.5 完整配置 .....                    | 1-10 |
| 1.5.6 配置注意事项 .....                  | 1-11 |

# 1 Portal 典型配置指导

## 1.1 Portal 简介

Portal 在英语中是入口的意思。Portal 认证通常也称为 Web 认证，一般将 Portal 认证网站称为门户网站。

未认证用户上网时，设备强制用户登录到特定站点，用户可以免费访问其中的服务。当用户需要使用互联网中的其它信息时，必须在门户网站进行认证，只有认证通过后才可以使用互联网资源。

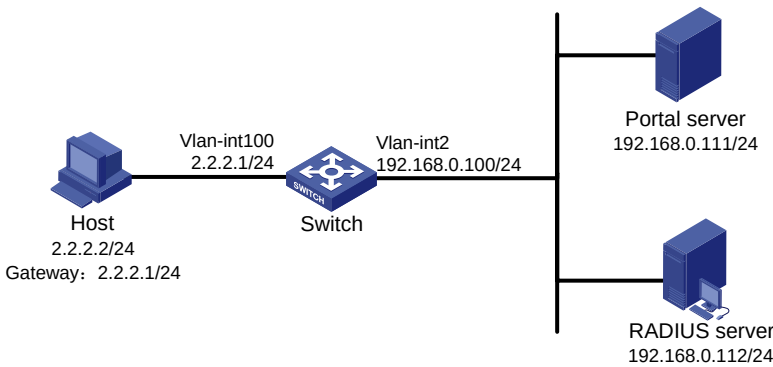
用户可以主动访问已知的 Portal 认证网站，输入用户名和密码进行认证，这种开始 Portal 认证的方式称作主动认证。反之，如果用户试图通过 HTTP 访问其他外网，将被强制访问 Portal 认证网站，从而开始 Portal 认证过程，这种方式称作强制认证。

Portal 业务可以为运营商提供方便的管理功能，门户网站可以开展广告、社区服务、个性化的业务等，使宽带运营商、设备提供商和内容服务提供商形成一个产业生态系统。

## 1.2 Portal 直接认证方式典型配置指导

### 1.2.1 组网图

图1-1 配置 Portal 直接认证组网图



### 1.2.2 应用要求

- 配置交换机采用直接方式的 Portal 认证。用户在未通过 Portal 认证前，只能访问 Portal 服务器；用户通过 Portal 认证后，可以访问外部网络。
- 采用 RADIUS 服务器作为认证/计费服务器。

### 1.2.3 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

| 产品              | 软件版本                            | 硬件版本    |
|-----------------|---------------------------------|---------|
| S7500E 系列以太网交换机 | Release 6100, Release 6300 软件版本 | 全系列硬件版本 |

## 1.2.4 配置过程和解释



### 说明

按照组网图配置设备各接口的 IP 地址，保证在不启动 Portal 的前提下各设备之间的路由可达。

在接入设备上进行以下配置。

#### (1) 配置 RADIUS 方案

# 创建名字为 rs1 的 RADIUS 方案并进入该方案视图。

```
<Switch> system-view
```

```
[Switch] radius scheme rs1
```

# 配置 RADIUS 方案的服务器类型为 extended。

```
[Switch-radius-rs1] server-type extended
```

# 配置 RADIUS 方案的主认证和主计费服务器及其通信密钥。

```
[Switch-radius-rs1] primary authentication 192.168.0.112
```

```
[Switch-radius-rs1] primary accounting 192.168.0.112
```

```
[Switch-radius-rs1] key authentication radius
```

```
[Switch-radius-rs1] key accounting radius
```

# 配置发送给 RADIUS 服务器的用户名不携带 ISP 域名。

```
[Switch-radius-rs1] user-name-format without-domain
```

```
[Switch-radius-rs1] quit
```

#### (2) 配置认证域

# 创建并进入名字为 dm1 的 ISP 域。

```
[Switch] domain dm1
```

# 配置 ISP 域的 RADIUS 方案 rs1。

```
[Switch-isp-dm1] authentication portal radius-scheme rs1
```

```
[Switch-isp-dm1] authorization portal radius-scheme rs1
```

```
[Switch-isp-dm1] accounting portal radius-scheme rs1
```

```
[Switch-isp-dm1] quit
```

# 配置系统缺省的 ISP 域 dm1，所有接入用户共用此缺省域的认证和计费方式。

```
[Switch] domain default enable dm1
```

#### (3) 配置 Portal 认证

# 配置 Portal 服务器：名称为 newpt，IP 地址为 192.168.0.111，密钥为 portal，端口为 50100，URL 为 http://192.168.0.111/portal。

```
[Switch] portal server newpt ip 192.168.0.111 key portal port 50100 url
http://192.168.0.111/portal
```

# 在与用户 Host 相连的接口上使能 Portal 认证。

```
[Switch] interface vlan-interface 100
```

```
[Switch-Vlan-interface100] ip address 2.2.2.1 255.255.255.0
```

```
[Switch-Vlan-interface100] portal server newpt method direct
```

```
[Switch] quit
```

# 配置与服务器通信的接口 IP 地址。

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.0.100 255.255.255.0
[Switch-Vlan-interface2] quit
```

### 1.2.5 完整配置

```
#
domain default enable dm1
#
#
portal server newpt ip 192.168.0.111 key portal url http://192.168.0.111/portal
#
radius scheme rs1
server-type extended
primary authentication 192.168.0.112
primary accounting 192.168.0.112
key authentication radius
key accounting radius
user-name-format without-domain
#
domain dm1
authentication portal radius-scheme rs1
authorization portal radius-scheme rs1
accounting portal radius-scheme rs1
#
interface Vlan-interface2
ip address 192.168.0.100 255.255.255.0
#
interface Vlan-interface100
ip address 2.2.2.1 255.255.255.0
portal server newpt method direct
#
```

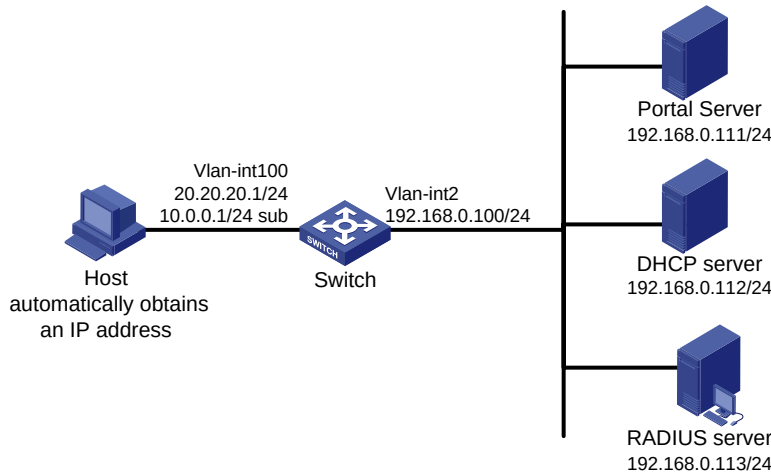
### 1.2.6 配置注意事项

- 设备向 Portal 服务器主动发送报文时使用的目的端口号必须与远程 Portal 服务器实际使用的端口号保持一致。
- 已配置的 Portal 服务器及其参数仅在该 Portal 服务器未被接口引用时才可以被删除或修改。
- 使能 Portal 的接口上所引用的 Portal 服务器必须已经存在。

# 1.3 Portal 二次地址分配认证方式典型配置指导

## 1.3.1 组网图

图1-2 配置 Portal 二次地址分配认证组网图



## 1.3.2 应用要求

- 配置交换机采用二次地址分配方式的 Portal 认证。用户通过 DHCP 服务器获取 IP 地址，Portal 认证前分配一个私网地址；通过 Portal 认证后，用户申请到一个公网地址，才可以访问外部网络。
- 采用 RADIUS 服务器作为认证/计费服务器。

## 1.3.3 适用产品、版本

表1-2 配置适用的产品与软硬件版本关系

| 产品              | 软件版本                            | 硬件版本    |
|-----------------|---------------------------------|---------|
| S7500E 系列以太网交换机 | Release 6100, Release 6300 软件版本 | 全系列硬件版本 |

## 1.3.4 配置过程和解释



### 说明

- Portal 二次地址分配认证方式应用中，DHCP 服务器上需创建公网地址池（20.20.20.0/24）及私网地址池（10.0.0.0/24），具体配置略。关于 DHCP 的详细配置请参见本手册“DHCP”模块的介绍。
- Portal 二次地址分配认证方式应用中，接入设备必须配置为 DHCP 中继（不能配置为 Server），且启动 Portal 的接口需要配置主 IP 地址（公网 IP）及从 IP 地址（私网 IP）。
- 按照组网图配置设备各接口的 IP 地址，保证在不启动 Portal 的前提下各设备之间的路由可达。
- 以下仅列出与 Portal 二次地址分配认证方式有关的配置，RADIUS 方案、ISP 域的配置请参见 1.2 Portal 直接认证方式典型配置指导。

在接入设备上以下配置。



# 配置 Portal 服务器：名称为 newpt，IP 地址为 192.168.0.111，密钥为 portal，端口为 50100，URL 为 http://192.168.0.111/portal。

```
<Switch> system-view
[Switch] portal server newpt ip 192.168.0.111 key portal port 50100 url
http://192.168.0.111/portal
```

# 配置 DHCP 中继，并启动 DHCP 中继的安全地址匹配检查功能。

```
[Switch] dhcp enable
[Switch] dhcp relay server-group 0 ip 192.168.0.112
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 20.20.20.1 255.255.255.0
[Switch-Vlan-interface100] ip address 10.0.0.1 255.255.255.0 sub
[Switch-Vlan-interface100] dhcp select relay
[Switch-Vlan-interface100] dhcp relay server-select 0
[Switch-Vlan-interface100] dhcp relay address-check enable
```

# 在与用户 Host 相连的接口上使能 Portal 认证。

```
[Switch-Vlan-interface100] portal server newpt method redhcp
[Switch-Vlan-interface100] quit
```

# 配置与服务器通信的接口 IP 地址。

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.0.100 255.255.255.0
[Switch-Vlan-interface2] quit
```

### 1.3.5 完整配置

```
#
domain default enable dm1
#
portal server newpt ip 192.168.0.111 key portal url http://192.168.0.111/portal
#
radius scheme rs1
server-type extended
primary authentication 192.168.0.112
primary accounting 192.168.0.112
key authentication radius
key accounting radius
user-name-format without-domain
#
domain dm1
authentication portal radius-scheme rs1
authorization portal radius-scheme rs1
accounting portal radius-scheme rs1
#
interface Vlan-interface2
ip address 192.168.0.100 255.255.255.0
#
interface Vlan-interface100
ip address 20.20.20.1 255.255.255.0
```

```

ip address 10.0.0.1 255.255.255.0 sub
dhcp select relay
dhcp relay server-select 0
dhcp relay address-check enable
portal server newpt method redhcp
#

```

### 1.3.6 配置注意事项

在二次地址分配认证方式下，允许用户在未通过 Portal 认证时以公网地址向外发送报文，但相应的回应报文则受限制。

## 1.4 三层 Portal 认证方式典型配置指导

三层认证方式和非三层认证方式的不同：

### 1. 组网方式不同

三层认证方式的认证客户端和接入设备之间可以跨接三层转发设备；非三层认证方式则要求认证客户端和接入设备之间没有三层转发。

### 2. 用户标识不同

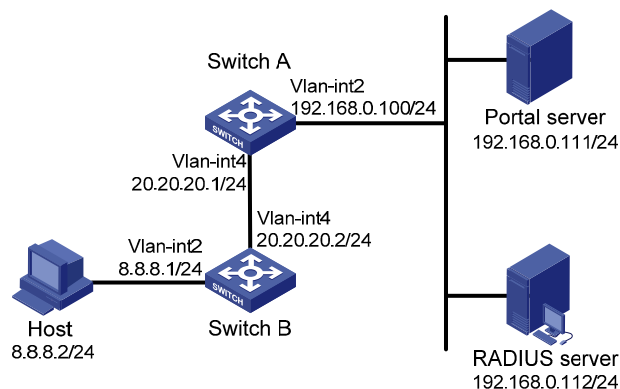
由于三层认证可以跨接三层设备，而接入设备不会学习认证客户端的 MAC 地址信息，所以是以 IP 地址唯一标识用户；而非三层认证方式中的接入设备则可以学习到认证客户端的 MAC 地址，所以是以 IP 和 MAC 地址的组合来唯一标识用户。

以上不同的组网方式和用户标识特点使得：

- 认证客户端的 MAC 地址不变、IP 地址改变时，在三层认证方式下会激发新的 Portal 认证；
- 而在非三层认证方式下不会激发新的 Portal 认证。只有认证客户端的 MAC 地址和 IP 地址同时改变时，非三层认证方式下才会激发新的 Portal 认证。

### 1.4.1 组网图

图1-3 配置三层 Portal 认证组网图



### 1.4.2 应用要求

Switch A 支持 Portal 认证功能。用户 Host 通过 Switch B 接入到 Switch A。

- 配置 Switch A 采用三层 Portal 认证。用户在未通过 Portal 认证前，只能访问 Portal 服务器；用户通过 Portal 认证后，可以访问外部网络。
- 采用 RADIUS 服务器作为认证/计费服务器。

### 1.4.3 适用产品、版本

表1-3 配置适用的产品与软硬件版本关系

| 产品              | 软件版本                            | 硬件版本    |
|-----------------|---------------------------------|---------|
| S7500E 系列以太网交换机 | Release 6100, Release 6300 软件版本 | 全系列硬件版本 |

### 1.4.4 配置过程和解释



说明

- 按照组网图配置设备各接口的 IP 地址，保证在不启动 Portal 的前提下各设备之间的路由可达。
- 以下仅列出跨三层设备支持 Portal 认证的主要配置，RADIUS 方案、ISP 域的配置请参见 1.2 Portal 直接认证方式典型配置指导。

在 Switch A 上进行以下配置。

# 配置 Portal 服务器：名称为 newpt，IP 地址为 192.168.0.111，密钥为 portal，端口为 50100，URL 为 http://192.168.0.111/portal。

```
<SwitchA> system-view
[SwitchA] portal server newpt ip 192.168.0.111 key portal port 50100 url
http://192.168.0.111/portal
```

# 在与 Switch B 相连的接口上使能 Portal 认证。

```
[SwitchA] interface vlan-interface 4
[SwitchA-Vlan-interface4] ip address 20.20.20.1 255.255.255.0
[SwitchA-Vlan-interface4] portal server newpt method layer3
[SwitchA-Vlan-interface4] quit
```

# 配置与服务器通信的接口 IP 地址。

```
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 192.168.0.100 255.255.255.0
[SwitchA-Vlan-interface2] quit
```

Switch B 上需要配置到 192.168.0.0/24 网段的缺省路由，下一跳为 20.20.20.1，具体配置略。

### 1.4.5 完整配置

```
#
domain default enable dm1
#
portal server newpt ip 192.168.0.111 key portal url http://192.168.0.111/portal
#
radius scheme rs1
server-type extended
primary authentication 192.168.0.112
```

```

primary accounting 192.168.0.112
key authentication radius
key accounting radius
user-name-format without-domain
security-policy-server 192.168.0.113
#
domain dm1
authentication portal radius-scheme rs1
authorization portal radius-scheme rs1
accounting portal radius-scheme rs1
#
interface Vlan-interface2
ip address 192.168.0.100 255.255.255.0
#
interface Vlan-interface4
ip address 20.20.20.1 255.255.255.0
portal server newpt method layer3
#

```

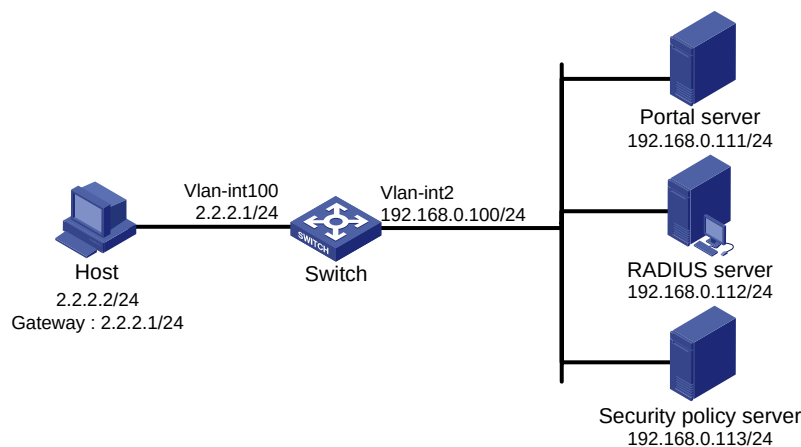
### 1.4.6 配置注意事项

对于跨三层设备支持 Portal 认证的应用只能配置 **layer3** 方式，但三层 Portal 认证方式不要求接入设备和 Portal 用户之间必需跨越三层设备。

## 1.5 Portal 直接认证方式（支持 EAD）典型配置指导

### 1.5.1 组网图

图1-4 配置 Portal 直接认证方式（支持 EAD）认证组网图



### 1.5.2 应用要求

- 配置交换机采用直接方式的 Portal 认证，开启 EAD 认证。用户在通过身份认证而没有通过安全认证时可以访问 192.168.0.0/24 网段；用户通过安全认证后，可以随意访问外部网络。
- 采用 RADIUS 服务器作为认证/计费服务器。
- 需要配置安全策略服务器。

### 1.5.3 适用产品、版本

表1-4 配置适用的产品与软硬件版本关系

| 产品              | 软件版本                            | 硬件版本    |
|-----------------|---------------------------------|---------|
| S7500E 系列以太网交换机 | Release 6100, Release 6300 软件版本 | 全系列硬件版本 |

### 1.5.4 配置过程和解释



#### 说明

按照组网图配置设备各接口的 IP 地址，保证在不启动 Portal 的前提下各设备之间的路由可达。

在接入设备上进行以下配置。

#### (1) 配置 RADIUS 方案

# 创建名字为 rs1 的 RADIUS 方案并进入该方案视图。

```
<Switch> system-view
```

```
[Switch] radius scheme rs1
```

# 配置 RADIUS 方案的服务器类型为 extended。

```
[Switch-radius-rs1] server-type extended
```

# 配置 RADIUS 方案的主认证和主计费服务器及其通信密钥。

```
[Switch-radius-rs1] primary authentication 192.168.0.112
```

```
[Switch-radius-rs1] primary accounting 192.168.0.112
```

```
[Switch-radius-rs1] key accounting radius
```

```
[Switch-radius-rs1] key authentication radius
```

```
[Switch-radius-rs1] user-name-format without-domain
```

# 配置 RADIUS 方案的安全策略服务器。

```
[Switch-radius-rs1] security-policy-server 192.168.0.113
```

```
[Switch-radius-rs1] quit
```

#### (2) 配置认证域

# 创建并进入名字为 dm1 的 ISP 域。

```
[Switch] domain dm1
```

# 配置 ISP 域的 RADIUS 方案 rs1。

```
[Switch-isp-dm1] authentication portal radius-scheme rs1
```

```
[Switch-isp-dm1] authorization portal radius-scheme rs1
```

```
[Switch-isp-dm1] accounting portal radius-scheme rs1
```

```
[Switch-isp-dm1] quit
```

# 配置系统缺省的 ISP 域 dm1，所有接入用户共用此缺省域的认证和计费方式。

```
[Switch] domain default enable dm1
```

#### (3) 配置受限资源对应的 ACL 为 3000，非受限资源对应的 ACL 为 3001

```
[Switch] acl number 3000
```

```
[Switch-acl-adv-3000] rule permit ip destination 192.168.0.0 0.0.0.255
```

```
[Switch-acl-adv-3000] quit
[Switch] acl number 3001
[Switch-acl-adv-3001] rule permit ip
[Switch-acl-adv-3001] quit
```

---



#### 说明

安全策略服务器上需要将 ACL 3000 和 ACL 3001 分别指定为隔离 ACL 和安全 ACL。

---

#### (4) 配置 Portal 认证

# 配置 Portal 服务器：名称为 newpt，IP 地址为 192.168.0.111，密钥为 portal，端口为 50100，URL 为 http://192.168.0.111/portal。

```
[Switch] portal server newpt ip 192.168.0.111 key portal port 50100 url
http://192.168.0.111/portal
```

# 在与用户 Host 相连的接口上使能 Portal 认证。

```
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 2.2.2.1 255.255.255.0
[Switch-Vlan-interface100] portal server newpt method direct
[Switch] quit
```

# 配置与服务器通信的接口 IP 地址。

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.0.100 255.255.255.0
```

### 1.5.5 完整配置

```
#
domain default enable dm1
#
#
portal server newpt ip 192.168.0.111 key portal url http://192.168.0.111/portal
#
radius scheme rs1
server-type extended
primary authentication 192.168.0.112
primary accounting 192.168.0.112
key authentication radius
key accounting radius
user-name-format without-domain
security-policy-server 192.168.0.113
#
domain dm1
authentication portal radius-scheme rs1
authorization portal radius-scheme rs1
accounting portal radius-scheme rs1
#
acl number 3000
rule permit ip destination 192.168.0.0 0.0.0.255
```

```
#
acl number 3001
 rule permit ip
#
interface Vlan-interface2
 ip address 192.168.0.100 255.255.255.0
#
interface Vlan-interface100
 ip address 2.2.2.1 255.255.255.0
 portal server newpt method direct
#
```

### 1.5.6 配置注意事项

安全策略服务器的相关配置请参考《CAMS 综合访问管理服务器 EAD 安全策略组件 用户手册》。

# 目 录

|                              |     |
|------------------------------|-----|
| 1 ARP典型配置指导 .....            | 1-1 |
| 1.1 ARP基本功能典型配置指导.....       | 1-1 |
| 1.1.1 组网图.....               | 1-1 |
| 1.1.2 应用要求 .....             | 1-1 |
| 1.1.3 适用产品、版本 .....          | 1-1 |
| 1.1.4 配置过程和解释 .....          | 1-1 |
| 1.1.5 完整配置 .....             | 1-2 |
| 1.1.6 配置注意事项 .....           | 1-2 |
| 1.2 代理ARP典型配置指导.....         | 1-2 |
| 1.2.1 组网图.....               | 1-2 |
| 1.2.2 应用要求 .....             | 1-3 |
| 1.2.3 适用产品、版本 .....          | 1-3 |
| 1.2.4 配置过程和解释 .....          | 1-3 |
| 1.2.5 完整配置 .....             | 1-3 |
| 1.2.6 配置注意事项 .....           | 1-4 |
| 1.3 端口隔离时的本地代理ARP典型配置指导..... | 1-4 |
| 1.3.1 组网图.....               | 1-4 |
| 1.3.2 应用要求 .....             | 1-4 |
| 1.3.3 适用产品、版本 .....          | 1-4 |
| 1.3.4 配置过程和解释 .....          | 1-5 |
| 1.3.5 完整配置 .....             | 1-5 |
| 1.3.6 配置注意事项 .....           | 1-6 |
| 1.4 ARP Detection典型配置举例..... | 1-6 |
| 1.4.1 组网图.....               | 1-6 |
| 1.4.2 应用要求 .....             | 1-6 |
| 1.4.3 适用产品、版本 .....          | 1-7 |
| 1.4.4 配置过程和解释 .....          | 1-7 |
| 1.4.5 完整配置 .....             | 1-7 |
| 1.4.6 配置注意事项 .....           | 1-8 |



# 1 ARP 典型配置指导

## 1.1 ARP 基本功能典型配置指导

### 1.1.1 组网图

无

### 1.1.2 应用要求

- 设置交换机的动态 ARP 表项的老化时间为 10 分钟。
- 设置接口 Vlan-interface10 上可以学习动态 ARP 表项的最大个数为 1000。
- 增加一条长静态 ARP 表项, IP 地址为 192.168.1.1/24, 对应的 MAC 地址为 000f-e201-0000, 表项对应的出端口为属于 VLAN 10 的端口 GigabitEthernet1/0/10。
- 增加一条短静态 ARP 表项, IP 地址为 192.168.1.2/24, 对应的 MAC 地址为 000f-e201-0001。

### 1.1.3 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                                    | 硬件版本                         |
|-------------------|-----------------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301 软件版本, Release 5303 软件版本    | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301 软件版本, Release 5303 软件版本    | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本                       | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本                       | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本                       | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100 软件版本,<br>Release 6300 软件版本 | 全系列硬件版本                      |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本                       | 全系列硬件版本                      |

### 1.1.4 配置过程和解释

# 设置交换机的动态 ARP 表项的老化时间为 10 分钟。

```
[Switch] arp timer aging 10
```

# 设置接口 Vlan-interface10 上可以学习动态 ARP 表项的最大个数为 1000。

```
[Switch] vlan 10
```

```
[Switch-vlan10] quit
```

```
[Switch-GigabitEthernet1/0/10] port access vlan 10
```

```
[Switch-GigabitEthernet1/0/10] quit
```

```
[Switch] interface vlan-interface 10
```

```
[Switch-vlan-interface10] arp max-learning-num 1000
```

```
[Switch-vlan-interface10] quit
```

# 增加一条长静态 ARP 表项。

```
[Switch] arp static 192.168.1.1 000f-e201-0000 10 gigabitethernet1/0/10
```

# 增加一条短静态 ARP 表项。

```
[Switch] arp static 192.168.1.2 000f-e201-0001
```

### 1.1.5 完整配置

```
#
vlan 10
#
interface Vlan-interface10
 arp max-learning-num 1000
#
interface GigabitEthernet1/0/10
 port access vlan 10
#
 arp timer aging 10
 arp static 192.168.1.1 000f-e201-0000 10 GigabitEthernet1/0/10
 arp static 192.168.1.2 000f-e201-0001
#
```

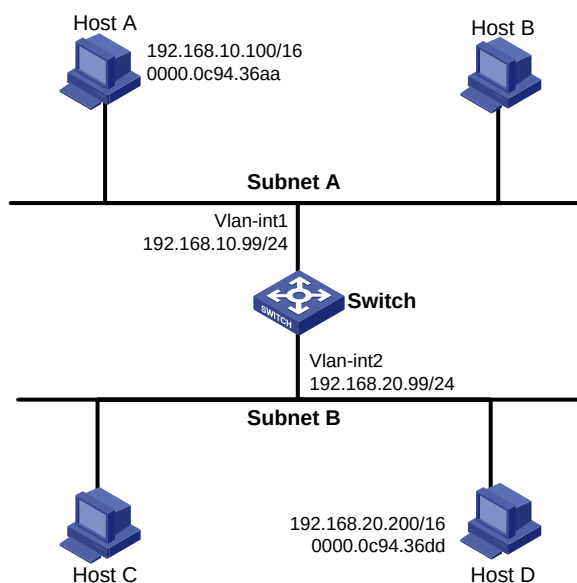
### 1.1.6 配置注意事项

无

## 1.2 代理 ARP 典型配置指导

### 1.2.1 组网图

图1-1 配置代理 ARP 组网图



### 1.2.2 应用要求

- Host A 属于 VLAN 1，IP 地址为 192.168.10.100/16，Host D 属于 VLAN 2，IP 地址为 192.168.20.200/16。
- 在交换机上启用代理 ARP 功能，实现 Host A 和 Host D 的通信。

### 1.2.3 适用产品、版本

表1-2 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                                | 硬件版本                         |
|-------------------|-------------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301 软件版本，Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301 软件版本，Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本                   | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本                   | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本                   | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100 软件版本，Release 6300 软件版本 | 全系列硬件版本                      |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本                   | 全系列硬件版本                      |

### 1.2.4 配置过程和解释

# 配置 VLAN1 接口的 IP 地址，并开启代理 ARP 功能。

```
<Switch> system-view
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ip address 192.168.10.99 255.255.255.0
[Switch-Vlan-interface1] proxy-arp enable
[Switch-Vlan-interface1] quit
```

# 配置 VLAN2 接口的 IP 地址，并开启代理 ARP 功能。

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.20.99 255.255.255.0
[Switch-Vlan-interface2] proxy-arp enable
[Switch-Vlan-interface2] quit
```

### 1.2.5 完整配置

```
#
interface Vlan-interface1
 ip address 192.168.10.99 255.255.255.0
 proxy-arp enable
#
interface Vlan-interface2
 ip address 192.168.20.99 255.255.255.0
 proxy-arp enable
#
```

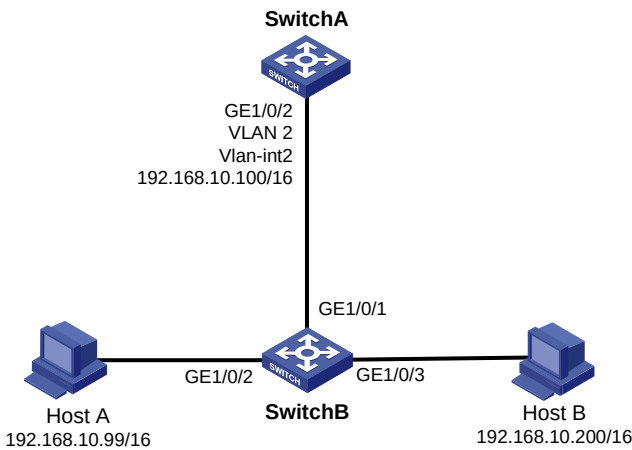
1.2.6 配置注意事项

无

1.3 端口隔离时的本地代理 ARP 典型配置指导

1.3.1 组网图

图1-2 配置端口隔离时的本地代理 ARP 组网图



1.3.2 应用要求

- Host A 和 Host B 属于同一个 VLAN，分别与 SwitchB 的端口 GigabitEthernet1/0/2 和 GigabitEthernet1/0/3 相连；
- SwitchB 通过端口 GigabitEthernet1/0/1 与 SwitchA 相连；
- 实现被隔离的端口 GigabitEthernet1/0/2 和 GigabitEthernet1/0/3 能够三层互通。

1.3.3 适用产品、版本

表1-3 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                                | 硬件版本                         |
|-------------------|-------------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301 软件版本，Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301 软件版本，Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本                   | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本                   | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本                   | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100 软件版本，Release 6300 软件版本 | 全系列硬件版本                      |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本                   | 全系列硬件版本                      |

### 1.3.4 配置过程和解释

# 配置 SwitchB 的端口 GigabitEthernet1/0/1、GigabitEthernet1/0/2、GigabitEthernet1/0/3 属于 VLAN2。

```
<SwitchB> system-view
[SwitchB] vlan 2
[SwitchB-vlan2] port gigabitethernet 1/0/1
[SwitchB-vlan2] port gigabitethernet 1/0/2
[SwitchB-vlan2] port gigabitethernet 1/0/3
[SwitchB-vlan2] quit
```

# 配置 SwitchB 的端口 GigabitEthernet1/0/2 和 GigabitEthernet1/0/3 隔离。

```
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] port-isolate enable
[SwitchB-GigabitEthernet1/0/2] quit
[SwitchB] interface gigabitethernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] port-isolate enable
[SwitchB-GigabitEthernet1/0/3] quit
```

# 配置 SwitchA 的 VLAN 接口 2 的 IP 地址。

```
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/2
[SwitchA-vlan2] quit
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 192.168.10.100 255.255.0.0
```

# 配置本地代理 ARP，实现 Host A 和 Host B 之间的三层互通。

```
[SwitchA-Vlan-interface2] local-proxy-arp enable
[SwitchA-Vlan-interface2] quit
```

### 1.3.5 完整配置

- SwitchB 上的配置

```
#
vlan 2
#
interface GigabitEthernet1/0/1
port access vlan 2
#
interface GigabitEthernet1/0/2
port access vlan 2
port-isolate enable
#
interface GigabitEthernet1/0/3
port access vlan 2
port-isolate enable
#
```

- SwitchA 上的配置

```
#
vlan 2
```

```
#
interface GigabitEthernet1/0/2
port access vlan 2
#
interface Vlan-interface2
ip address 192.168.10.100 255.255.0.0
local-proxy-arp enable
#
```

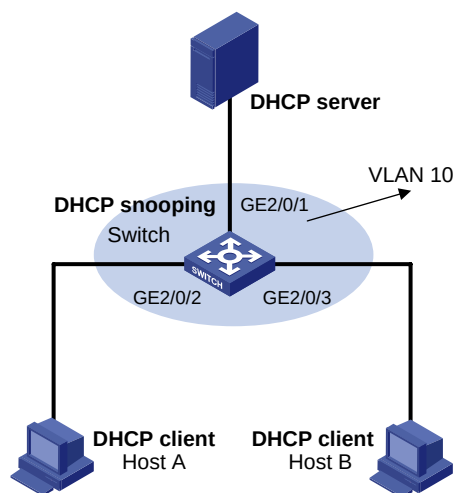
### 1.3.6 配置注意事项

- 关于端口隔离的具体配置请参考“端口隔离典型配置指导”部分。
- 当开启端口隔离的交换机上进行的是二、三层流量同时隔离时，可以通过在其上层交换机相应VLAN接口上开启本地代理ARP功能，实现Host A和Host B的互通，如 [图 1-2](#)。
- 当开启端口隔离的交换机（如 S3610&S5510 系列以太网交换机）上只进行二层流量隔离时，可以同时在此交换机的相应 VLAN 接口上启用本地代理 ARP 功能，实现 Host A 和 Host B 的互通。

## 1.4 ARP Detection 典型配置举例

### 1.4.1 组网图

图1-3 ARP Detection 典型配置组网图



### 1.4.2 应用要求

- Switch 是 DHCP Snooping 设备，在 VLAN 10 内启用 ARP Detection 功能，对 DHCP 客户端进行保护，保证合法用户可以正常转发报文，否则丢弃。
- Host A 和 Host B 是 DHCP 客户端。

### 1.4.3 适用产品、版本

表1-4 配置适用的产品与软硬件版本关系

| 产品              | 软件版本                                 | 硬件版本    |
|-----------------|--------------------------------------|---------|
| S7500E 系列以太网交换机 | Release 6100 软件版本, Release 6300 软件版本 | 全系列硬件版本 |

### 1.4.4 配置过程和解释

- (1) 配置 DHCP 服务器（略）
- (2) 配置 Host A 和 Host B 通过 DHCP 自动获取 IP 地址（略）
- (3) 配置 Switch 为 DHCP Snooping 设备

# 配置 Switch 所有端口属于 VLAN 10（略）。

# 配置 DHCP Snooping 功能。

```
<Switch> system-view
[Switch] dhcp-snooping
[Switch] interface gigabitethernet 2/0/1
[Switch-GigabitEthernet2/0/1] dhcp-snooping trust
[Switch-GigabitEthernet2/0/1] quit
```

# 配置 ARP Detection 特性，端口状态缺省为非信任状态，上行端口配置为信任状态，下行端口按缺省配置。

```
[Switch] vlan 10
[Switch-vlan10] arp detection enable
[Switch-vlan10] quit
[Switch] interface gigabitethernet 2/0/1
[Switch-GigabitEthernet2/0/1] arp detection trust
[Switch-GigabitEthernet2/0/1] quit
```

# 配置报文有效性检查。

```
[Switch] arp detection validate dst-mac ip src-mac
```

# 配置 ARP 报文上送限速，速率为 150pps。

```
[Switch] interface gigabitethernet 2/0/2
[Switch-GigabitEthernet2/0/2] arp rate-limit rate 150 drop
[Switch-GigabitEthernet2/0/2] quit
[Switch] interface gigabitethernet 2/0/3
[Switch-GigabitEthernet2/0/3] arp rate-limit rate 150 drop
[Switch-GigabitEthernet2/0/3] quit
```

### 1.4.5 完整配置

```
#
dhcp-snooping
#
interface GigabitEthernet2/0/1
dhcp-snooping trust
arp detection trust
#
```

```
vlan 10
 arp detection enable
#
interface GigabitEthernet2/0/2
 arp rate-limit rate 150 drop
#
interface GigabitEthernet2/0/3
 arp rate-limit rate 150 drop
#
 arp detection validate dst-mac ip src-mac
#
```

#### 1.4.6 配置注意事项

无



# 目 录

|                                           |      |
|-------------------------------------------|------|
| 1 DHCP典型配置指导.....                         | 1-1  |
| 1.1 DHCP服务器静态绑定地址典型配置指导.....              | 1-1  |
| 1.1.1 组网图.....                            | 1-1  |
| 1.1.2 应用要求 .....                          | 1-1  |
| 1.1.3 适用产品、版本 .....                       | 1-1  |
| 1.1.4 配置过程和解释 .....                       | 1-1  |
| 1.1.5 完整配置 .....                          | 1-2  |
| 1.1.6 配置注意事项 .....                        | 1-2  |
| 1.2 DHCP服务器动态分配地址典型配置指导.....              | 1-3  |
| 1.2.1 组网图.....                            | 1-3  |
| 1.2.2 应用要求 .....                          | 1-3  |
| 1.2.3 适用产品、版本 .....                       | 1-3  |
| 1.2.4 配置过程和解释 .....                       | 1-4  |
| 1.2.5 完整配置 .....                          | 1-4  |
| 1.2.6 配置注意事项 .....                        | 1-5  |
| 1.3 DHCP中继典型配置指导 .....                    | 1-5  |
| 1.3.1 组网图.....                            | 1-6  |
| 1.3.2 应用要求 .....                          | 1-6  |
| 1.3.3 适用产品、版本 .....                       | 1-6  |
| 1.3.4 配置过程和解释 .....                       | 1-7  |
| 1.3.5 完整配置 .....                          | 1-7  |
| 1.3.6 配置注意事项 .....                        | 1-7  |
| 1.4 DHCP Snooping典型配置指导 .....             | 1-8  |
| 1.4.1 组网图.....                            | 1-8  |
| 1.4.2 应用要求 .....                          | 1-8  |
| 1.4.3 适用产品、版本 .....                       | 1-8  |
| 1.4.4 配置过程和解释 .....                       | 1-9  |
| 1.4.5 完整配置 .....                          | 1-9  |
| 1.4.6 配置注意事项 .....                        | 1-10 |
| 1.5 DHCP Snooping支持Option 82 典型配置指导 ..... | 1-10 |
| 1.5.1 组网图.....                            | 1-11 |
| 1.5.2 应用要求 .....                          | 1-11 |
| 1.5.3 适用产品、版本 .....                       | 1-11 |
| 1.5.4 配置过程和解释 .....                       | 1-12 |
| 1.5.5 完整配置 .....                          | 1-13 |
| 1.5.6 配置注意事项 .....                        | 1-14 |
| 1.6 DHCP客户端典型配置指导 .....                   | 1-14 |
| 1.6.1 组网图.....                            | 1-14 |
| 1.6.2 应用要求 .....                          | 1-14 |
| 1.6.3 适用产品、版本 .....                       | 1-14 |
| 1.6.4 配置过程和解释 .....                       | 1-15 |
| 1.6.5 完整配置 .....                          | 1-15 |

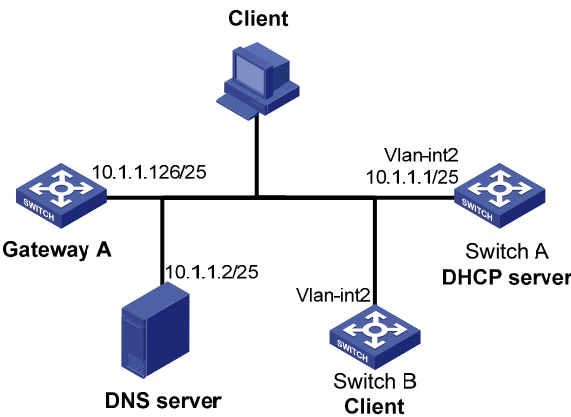
|                        |      |
|------------------------|------|
| 1.6.6 配置注意事项 .....     | 1-15 |
| 1.7 自动配置功能典型配置指导 ..... | 1-15 |
| 1.7.1 组网图 .....        | 1-16 |
| 1.7.2 应用需求 .....       | 1-16 |
| 1.7.3 适用产品、版本 .....    | 1-17 |
| 1.7.4 配置过程和解释 .....    | 1-17 |
| 1.7.5 完整配置 .....       | 1-21 |
| 1.7.6 注意事项 .....       | 1-23 |

# 1 DHCP 典型配置指导

## 1.1 DHCP 服务器静态绑定地址典型配置指导

### 1.1.1 组网图

图1-1 DHCP 服务器静态绑定地址组网图



### 1.1.2 应用要求

Switch B 作为 DHCP 客户端，从 DHCP 服务器 Switch A 获取静态绑定的 IP 地址、域名服务器、网关地址等信息。

### 1.1.3 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                                | 硬件版本    |
|-------------------|-------------------------------------|---------|
| S3610 系列以太网交换机    | Release 5301 软件版本，Release 5303 软件版本 | 全系列硬件版本 |
| S5510 系列以太网交换机    | Release 5301 软件版本，Release 5303 软件版本 | 全系列硬件版本 |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本                   | 全系列硬件版本 |
| S7500E 系列以太网交换机   | Release 6100 软件版本，Release 6300 软件版本 | 全系列硬件版本 |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本                   | 全系列硬件版本 |

### 1.1.4 配置过程和解释

# 配置接口的 IP 地址。

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 10.1.1.1 25
[SwitchA-Vlan-interface2] quit
```

# 使能 DHCP 服务。

```
[SwitchA] dhcp enable
```

# 配置 DHCP 地址池 0，采用静态绑定方式分配 IP 地址。

```
[SwitchA] dhcp server ip-pool 0
```

```
[SwitchA-dhcp-pool-0] static-bind ip-address 10.1.1.5
```

```
[SwitchA-dhcp-pool-0] static-bind mac-address 000f-e200-0002
```

```
[SwitchA-dhcp-pool-0] dns-list 10.1.1.2
```

```
[SwitchA-dhcp-pool-0] gateway-list 10.1.1.126
```

```
[SwitchA-dhcp-pool-0] quit
```

### 1.1.5 完整配置

```

dhcp server ip-pool 0
static-bind ip-address 10.1.1.5 mask 255.0.0.0
static-bind mac-address 000f-e200-0002
gateway-list 10.1.1.126
dns-list 10.1.1.2
expired unlimited

interface Vlan-interface2
ip address 10.1.1.1 255.255.255.128

dhcp enable
#
```

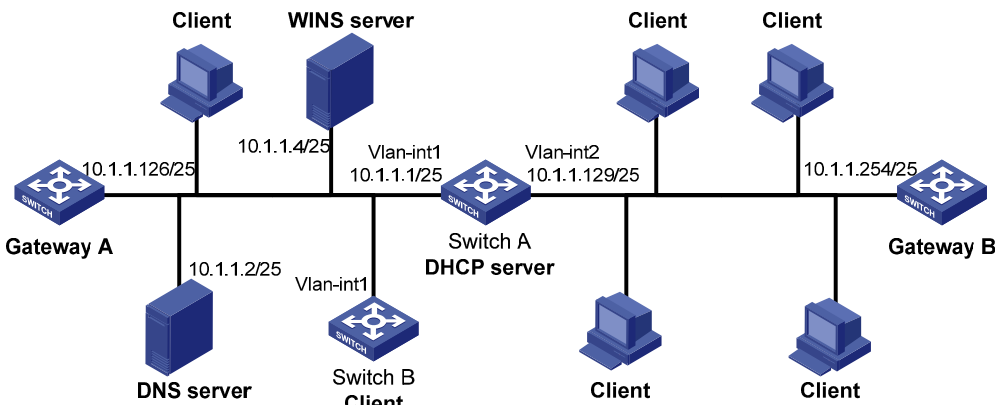
### 1.1.6 配置注意事项

- 静态绑定的 IP 地址不能是 DHCP 服务器的接口 IP 地址，否则会导致 IP 地址冲突，被绑定的客户端将无法获取到 IP 地址。
- 目前一个 DHCP 地址池中只能配置一个静态绑定，可以是 IP 地址与 MAC 地址的绑定，也可以是 IP 地址与客户端 ID（用于唯一标识一个客户端的，4~160 个字符的字符串）的绑定。
- 静态绑定的客户端 ID，要与在待绑定客户端通过 **display dhcp client verbose** 命令显示的客户端 ID 一致。否则，客户端无法成功获取 IP 地址。

## 1.2 DHCP 服务器动态分配地址典型配置指导

### 1.2.1 组网图

图1-2 DHCP 服务器动态分配地址组网图



### 1.2.2 应用要求

- 作为 DHCP 服务器的 Switch A 为网段 10.1.1.0/24 中的客户端动态分配 IP 地址，该地址池网段分为两个子网网段：10.1.1.0/25 和 10.1.1.128/25；
- Switch A 的两个 VLAN 接口，VLAN 接口 1 和 VLAN 接口 2 的地址分别为 10.1.1.1/25 和 10.1.1.129/25；
- 10.1.1.0/25 网段内的地址租用期限为 10 天 12 小时，域名后缀为 aabbcc.com，DNS 服务器地址为 10.1.1.2/25，WINS 服务器地址为 10.1.1.4/25，网关的地址为 10.1.1.126/25；
- 10.1.1.128/25 网段内的地址租用期限为 5 天，域名后缀为 aabbcc.com，DNS 服务器地址为 10.1.1.2/25，无 WINS 服务器地址，网关的地址为 10.1.1.254/25。
- 10.1.1.0/25 网段与 10.1.1.128/25 网段的域名后缀、DNS 服务器地址相同，可以只配置 10.1.1.0/24 网段的域名后缀和 DNS 服务器地址，10.1.1.0/25 网段与 10.1.1.128/25 网段继承 10.1.1.0/24 网段的配置。
- 开启 Switch A 的伪服务器检测功能，方便管理员从系统日志中查找伪服务器信息。

### 1.2.3 适用产品、版本

表1-2 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                                | 硬件版本    |
|-------------------|-------------------------------------|---------|
| S3610 系列以太网交换机    | Release 5301 软件版本，Release 5303 软件版本 | 全系列硬件版本 |
| S5510 系列以太网交换机    | Release 5301 软件版本，Release 5303 软件版本 | 全系列硬件版本 |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本                   | 全系列硬件版本 |
| S7500E 系列以太网交换机   | Release 6100 软件版本，Release 6300 软件版本 | 全系列硬件版本 |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本                   | 全系列硬件版本 |

## 1.2.4 配置过程和解释

# 使能 DHCP 服务。

```
[SwitchA] dhcp enable
```

# 配置不参与自动分配的 IP 地址（DNS 服务器、WINS 服务器和网关地址）。

```
[SwitchA] dhcp server forbidden-ip 10.1.1.2
```

```
[SwitchA] dhcp server forbidden-ip 10.1.1.4
```

```
[SwitchA] dhcp server forbidden-ip 10.1.1.126
```

```
[SwitchA] dhcp server forbidden-ip 10.1.1.254
```

# 配置伪服务器检测功能。

```
[SwitchA] dhcp server detect
```

# 配置 DHCP 地址池 0 的共有属性（地址池范围、DNS 服务器地址）。

```
[SwitchA] dhcp server ip-pool 0
```

```
[SwitchA-dhcp-pool-0] network 10.1.1.0 mask 255.255.255.0
```

```
[SwitchA-dhcp-pool-0] domain-name aabbcc.com
```

```
[SwitchA-dhcp-pool-0] dns-list 10.1.1.2
```

```
[SwitchA-dhcp-pool-0] quit
```

# 配置 DHCP 地址池 1 的属性（地址池范围、网关、WINS 服务器地址、地址租用期限）。

```
[SwitchA] dhcp server ip-pool 1
```

```
[SwitchA-dhcp-pool-1] network 10.1.1.0 mask 255.255.255.128
```

```
[SwitchA-dhcp-pool-1] gateway-list 10.1.1.126
```

```
[SwitchA-dhcp-pool-1] expired day 10 hour 12
```

```
[SwitchA-dhcp-pool-1] nbns-list 10.1.1.4
```

```
[SwitchA-dhcp-pool-1] quit
```

# 配置 DHCP 地址池 2 的属性（地址池范围、地址租用期限、网关）。

```
[SwitchA] dhcp server ip-pool 2
```

```
[SwitchA-dhcp-pool-2] network 10.1.1.128 mask 255.255.255.128
```

```
[SwitchA-dhcp-pool-2] expired day 5
```

```
[SwitchA-dhcp-pool-2] gateway-list 10.1.1.254
```

```
[SwitchA-dhcp-pool-2] quit
```

开启伪服务器检测功能后，Switch A 记录所有 DHCP 服务器的信息，包括合法的 DHCP 服务器。管理员需要从系统日志中查找伪 DHCP 服务器。当 Switch A 发现网络中的其它 DHCP 服务器时，会记录如下所示的日志信息。

```
<SwitchA>
```

```
%Apr 30 08:07:51:896 2000 H3C DHCP/4/DHCP_LOCAL_SERVER:
```

```
Local DHCP server information: Server IP (detected by DHCP server) =
```

```
10.1.1.5, DHCP server interface = Vlan-interface1
```

```
Source client information: DHCP message type = DHCPREQUEST, DHCP
```

```
client hardware address = 000f-e200-000b
```

## 1.2.5 完整配置

```
#
```

```
dhcp server ip-pool 0
```

```
network 10.1.1.0 mask 255.255.255.0
```

```

dns-list 10.1.1.2
domain-name aabbcc.com
#
dhcp server ip-pool 1
network 10.1.1.0 mask 255.255.255.128
gateway-list 10.1.1.126
nbns-list 10.1.1.4
expired day 10 hour 12
#
dhcp server ip-pool 2
network 10.1.1.128 mask 255.255.255.128
gateway-list 10.1.1.254
expired day 5
#
dhcp server forbidden-ip 10.1.1.2
dhcp server forbidden-ip 10.1.1.4
dhcp server forbidden-ip 10.1.1.126
dhcp server forbidden-ip 10.1.1.254
dhcp server detect
#
dhcp enable
#

```

### 1.2.6 配置注意事项

- 如果 DHCP 服务器的地址池中没有足够的可供分配的 IP 地址，则服务器无法为客户端分配地址，服务器不会将父地址池中的 IP 地址分配给客户端。故在本例中，建议从 VLAN 接口 1 申请 IP 地址的客户端数目不要超过 122 个；从 VLAN 接口 2 申请 IP 地址的客户端不要超过 124 个。
- DHCP 服务器与客户端在同一网段的情况下，如果服务器的接口视图下配置了 **dhcp select server global-pool subaddress** 命令，则当 DHCP 服务器为客户端分配 IP 地址时，从与服务器接口（与客户端相连的接口）的从 IP 地址在同一网段的地址池中选择地址分配给客户端。如果接口有多个从 IP 地址，则从第一个从 IP 地址开始依次匹配。否则，服务器从与接口主 IP 地址在同一网段的地址池中选择地址分配给客户端。

## 1.3 DHCP 中继典型配置指导

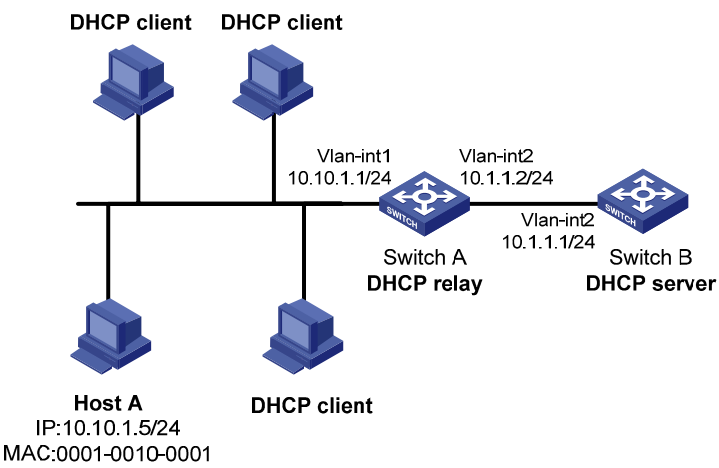
由于在 IP 地址动态获取过程中采用广播方式发送报文，因此 DHCP 只适用于 DHCP 客户端和服务

器处于同一个子网内的情况。为进行动态主机配置，需要在所有网段上都设置一个 DHCP 服务器，这显然是很不经济的。

DHCP 中继功能的引入解决了这一难题：子网内的客户端可以通过 DHCP 中继与其他子网的 DHCP 服务器通信，最终获取到 IP 地址。这样，多个网络上的 DHCP 客户端可以使用同一个 DHCP 服务器，既节省了成本，又便于进行集中管理。

1.3.1 组网图

图1-3 DHCP 中继配置示例图



1.3.2 应用要求

- 具有 DHCP 中继功能的 Switch A 通过端口（属于 VLAN1）连接到 DHCP 客户端所在的网络，交换机 VLAN 接口 1 的 IP 地址为 10.10.1.1/24，VLAN 接口 2 的 IP 地址为 10.1.1.2/24；
- DHCP 服务器的 IP 地址为 10.1.1.1/24。
- Switch A 作为 DHCP 中继，负责转发 DHCP 报文，使 DHCP 客户端可以从 DHCP 服务器上申请到 10.10.1.0/24 网段的 IP 地址及相关配置信息；
- 客户端主机除 Host A 使用固定 IP 地址 10.10.1.5/24 外，其余主机通过 DHCP 方式动态获取 IP 地址。
- 开启 Switch A 上的 DHCP 中继地址表项检查功能，使合法固定 IP 地址用户和通过 DHCP 服务器获取 IP 地址的用户访问网络，防止客户端私自修改 IP 地址访问网络。

1.3.3 适用产品、版本

表1-3 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                                | 硬件版本                         |
|-------------------|-------------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301 软件版本，Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301 软件版本，Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本                   | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本                   | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本                   | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100 软件版本，Release 6300 软件版本 | 全系列硬件版本                      |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本                   | 全系列硬件版本                      |



### 1.3.4 配置过程和解释

# 使能 DHCP 服务。

```
<SwitchA> system-view
[SwitchA] dhcp enable
```

# 配置 VLAN 接口 1 工作在 DHCP 中继模式。

```
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ip address 10.10.1.1 24
[SwitchA-Vlan-interface1] dhcp select relay
[SwitchA-Vlan-interface1] quit
```

# 配置 DHCP 服务器的地址，并配置 VLAN 接口 1 对应 DHCP 服务器组 1。

```
[SwitchA] dhcp relay server-group 1 ip 10.1.1.1
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] dhcp relay server-select 1
[SwitchA-Vlan-interface1] quit
```

# 在 DHCP 中继上为 Host A 配置一条静态用户地址表项，IP 地址为 10.10.1.5/24，MAC 地址为 0001-0010-0001。

```
[SwitchA] dhcp relay security static 10.10.1.5 0001-0010-0001
```

# 开启 DHCP 中继地址匹配检查功能。

```
[SwitchA] interface Vlan-interface 1
[SwitchA-Vlan-interface1] dhcp relay address-check enable
[SwitchA-Vlan-interface1] quit
```

### 1.3.5 完整配置

```
#
dhcp relay server-group 1 ip 10.1.1.1
#
interface Vlan-interface1
ip address 10.10.1.1 255.255.255.0
dhcp select relay
dhcp relay server-select 1
dhcp relay address-check enable
#
dhcp enable
#
dhcp relay security static 10.10.1.5 0001-0010-0001
#
```

### 1.3.6 配置注意事项

- 为了使DHCP客户端能从DHCP服务器获得IP地址，还需要在DHCP服务器上进行一些配置。关于DHCP服务器配置，可以参考 1.2 DHCP服务器动态分配地址典型配置指导。
- DHCP 中继与 DHCP 服务器之间必须有路由可达。

- DHCP 中继的地址匹配检查功能与 DHCP 中继的其他配置无直接关系。即只要执行了 **dhcp relay address-check enable** 命令，地址匹配检查功能就可以生效，不需要配置 DHCP 中继的其他功能，如使能 DHCP、配置接口工作在 DHCP 中继模式等。

## 1.4 DHCP Snooping 典型配置指导

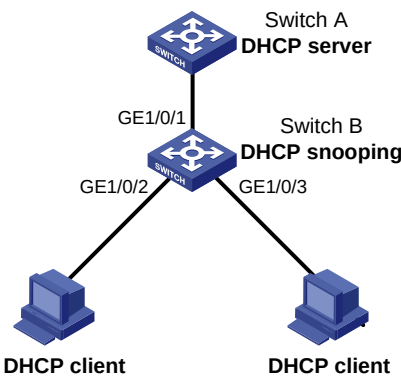
出于安全性的考虑，网络管理员可能需要记录用户上网时所用的 IP 地址，确认用户从 DHCP Server 获取的 IP 地址和用户主机的 MAC 地址的对应关系。

DHCP Snooping 通过以下两种方法来获得用户从 DHCP Server 获取的 IP 地址和用户 MAC 地址信息：

- 监听 DHCP-ACK 报文
- 监听 DHCP-REQUEST 报文

### 1.4.1 组网图

图1-4 DHCP Snooping 组网配置示意图



### 1.4.2 应用要求

Switch B 通过以太网端口 GigabitEthernet1/0/1 连接到 DHCP 服务器，通过以太网端口 GigabitEthernet1/0/2、GigabitEthernet1/0/3 连接到 DHCP 客户端。要求：

- 与 DHCP 服务器相连的端口可以转发 DHCP 服务器的响应报文，而其他端口不转发 DHCP 服务器的响应报文。
- 记录 DHCP-REQUEST 和信任端口收到的 DHCP-ACK 广播报文中 DHCP 客户端 IP 地址及 MAC 地址的绑定关系。
- 支持 Option 82 功能。接收到客户端发送的 DHCP 请求报文后，将以 verbose 格式填充的 Option 82 添加到 DHCP 请求报文中，并转发该报文。

### 1.4.3 适用产品、版本

表1-4 配置适用的产品与软硬件版本关系

| 产品             | 软件版本                                | 硬件版本    |
|----------------|-------------------------------------|---------|
| S3610 系列以太网交换机 | Release 5301 软件版本，Release 5303 软件版本 | 全系列硬件版本 |
| S5510 系列以太网交换机 | Release 5301 软件版本，Release 5303 软件版本 | 全系列硬件版本 |

| 产品                | 软件版本                                 | 硬件版本                         |
|-------------------|--------------------------------------|------------------------------|
| S5500-SI 系列以太网交换机 | Release 1207 软件版本                    | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本                    | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本                    | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100 软件版本, Release 6300 软件版本 | 全系列硬件版本                      |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本                    | 全系列硬件版本                      |

需要注意的是：S5500-SI 系列以太网交换机仅支持开启 DHCP Snooping，及配置信任端口功能，不支持在 DHCP Snooping 设备上应用 Option 82 功能。

#### 1.4.4 配置过程和解释

# 使能 DHCP Snooping 功能。

```
<SwitchB> system-view
[SwitchB] dhcp-snooping
```

# 配置 GigabitEthernet1/0/1 端口为信任端口。

```
[SwitchB] interface gigabitethernet1/0/1
[SwitchB-GigabitEthernet1/0/1] dhcp-snooping trust
[SwitchB-GigabitEthernet1/0/1] quit
```

# 在端口 GigabitEthernet1/0/2 上配置 DHCP Snooping 支持 Option 82 功能。

```
[SwitchB] interface gigabitethernet1/0/2
[SwitchB-GigabitEthernet1/0/2] dhcp-snooping information enable
```

# 在端口 GigabitEthernet1/0/2 上配置 Option 82 以 verbose 格式进行填充。

```
[SwitchB-GigabitEthernet1/0/2] dhcp-snooping information format verbose node-identifier
sysname
[SwitchB-GigabitEthernet1/0/2] quit
```

# 在端口 GigabitEthernet1/0/3 上配置 DHCP Snooping 支持 Option 82 功能。

```
[SwitchB] interface gigabitethernet1/0/3
[SwitchB-GigabitEthernet1/0/3] dhcp-snooping information enable
```

# 在端口 GigabitEthernet1/0/3 上配置 Option 82 以 verbose 格式进行填充。

```
[SwitchB-GigabitEthernet1/0/3] dhcp-snooping information format verbose node-identifier
sysname
```

#### 1.4.5 完整配置

```
#
dhcp-snooping
#
interface GigabitEthernet1/0/1
dhcp-snooping trust
#
interface GigabitEthernet1/0/2
dhcp-snooping information enable
```

```
dhcp-snooping information format verbose node-identifier sysname
#
interface GigabitEthernet1/0/3
dhcp-snooping information enable
dhcp-snooping information format verbose node-identifier sysname
#
```

#### 1.4.6 配置注意事项

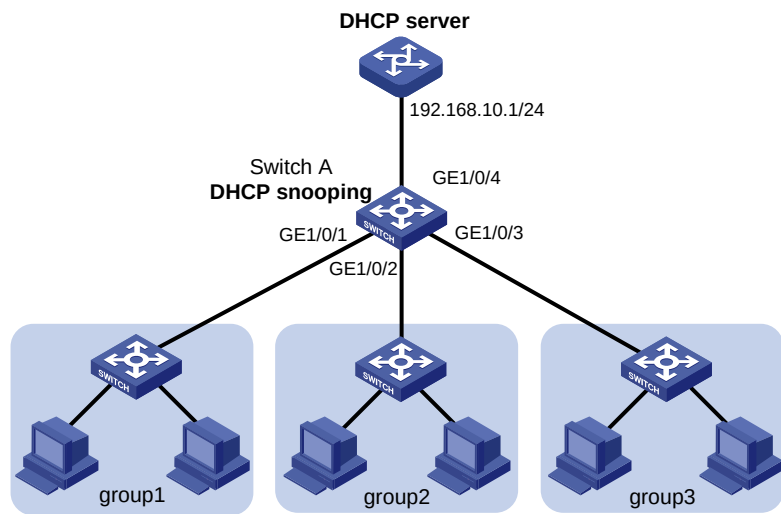
- 设备只有位于 DHCP 客户端与 DHCP 服务器之间，或 DHCP 客户端与 DHCP 中继之间时，DHCP Snooping 功能配置后才能正常工作；设备位于 DHCP 服务器与 DHCP 中继之间时，DHCP Snooping 功能配置后不能正常工作。
- 使能 DHCP Snooping 功能的设备，不能作为 DHCP 服务器和 DHCP 中继。
- 建议不要在同一台设备上同时配置 DHCP 客户端/BOOTP 客户端和 DHCP Snooping 功能，否则可能无法生成 DHCP Snooping 表项，DHCP 客户端/BOOTP 客户端也可能申请不到 IP 地址。
- 为了使 DHCP 客户端能从合法的 DHCP 服务器获取 IP 地址，必须将与合法 DHCP 服务器相连的端口设置为信任端口，设置的信任端口和与 DHCP 客户端相连的端口必须在同一个 VLAN 内。
- 建议不要在设备上同时配置 DHCP Snooping 功能和灵活 QinQ 功能，否则可能导致 DHCP Snooping 功能无法正常使用。
- DHCP Snooping 不支持链路聚合。若以太网端口加入聚合组，则该端口上进行的 DHCP Snooping 配置不会生效；该端口退出聚合组后，之前的 DHCP Snooping 配置才会生效。

### 1.5 DHCP Snooping 支持 Option 82 典型配置指导

DHCP snooping 设备通过在 DHCP 请求报文中添加 Option 82，将 DHCP 客户端的位置信息告诉给 DHCP 服务器，从而使得 DHCP 服务器能够为主机分配合适的 IP 地址和其他配置信息，并实现对客户端的安全和计费等控制。

### 1.5.1 组网图

图1-5 DHCP Snooping 组网配置示意图



### 1.5.2 应用要求

某公司的办公区域包括三个小组 group1、group2 和 group3，独立地分布在三个房间中。该公司通过 DHCP server 统一管理 IP 地址，为不同的小组分配不同范围的地址。具体需求如下：

- DHCP 服务器为办公室设备分配 192.168.10.0/24 网段的地址，有效期为 12 小时，并指定 DNS 和 WINS 服务器地址分别为 192.168.100.2 和 192.168.100.3。
- Switch A 上开启 DHCP snooping 功能，并配置与 DHCP 服务器相连的端口 GigabitEthernet1/0/4 为信任端口。
- 三个小组 group1、group2 和 group3 分别通过端口 GigabitEthernet1/0/1、GigabitEthernet1/0/2 和 GigabitEthernet1/0/3 接入 DHCP snooping 设备。
- 配置 DHCP snooping 支持 Option 82，将用户与 DHCP snooping 设备相连的端口信息添加到 DHCP 报文的 Option 82 字段。
- 配置 DHCP 服务器支持 Option 82，根据 Option 82 中携带的小组信息，为 group1 的用户分配 192.168.10.2~192.168.10.25 之间的地址；为 group2 的用户分配 192.168.10.100~192.168.10.150 之间的地址；为 group3 的用户分配 192.168.10.151~192.168.10.200 之间的地址。

### 1.5.3 适用产品、版本

表1-5 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                                | 硬件版本                         |
|-------------------|-------------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301 软件版本，Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301 软件版本，Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本                   | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本                   | S5500-20TP-SI                |

| 产品                | 软件版本                                | 硬件版本    |
|-------------------|-------------------------------------|---------|
| S5500-EI 系列以太网交换机 | Release 2102 软件版本                   | 全系列硬件版本 |
| S7500E 系列以太网交换机   | Release 6100 软件版本，Release 6300 软件版本 | 全系列硬件版本 |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本                   | 全系列硬件版本 |

## 1.5.4 配置过程 and 解释

### 1. Switch A 上的配置

# 使能 DHCP Snooping 功能。

```
<SwitchA> system-view
[SwitchA] dhcp-snooping
```

# 配置 GigabitEthernet1/0/4 端口为信任端口。

```
[SwitchA] interface gigabitethernet1/0/4
[SwitchA-GigabitEthernet1/0/4] dhcp-snooping trust
[SwitchA-GigabitEthernet1/0/4] quit
```

# 在端口 GigabitEthernet1/0/1 上配置 DHCP Snooping 支持 Option 82 功能，并配置 Option 82 的填充方式为 Normal。

```
[SwitchA] interface gigabitethernet1/0/1
[SwitchA-GigabitEthernet1/0/1] dhcp-snooping information enable
[SwitchA-GigabitEthernet1/0/1] dhcp-snooping information format normal
[SwitchA-GigabitEthernet1/0/1] quit
```

# 在端口 GigabitEthernet1/0/2 上配置 DHCP Snooping 支持 Option 82 功能，并配置 Option 82 的填充方式为 Normal。

```
[SwitchA] interface gigabitethernet1/0/2
[SwitchA-GigabitEthernet1/0/2] dhcp-snooping information enable
[SwitchA-GigabitEthernet1/0/2] dhcp-snooping informationformat normal
[SwitchA-GigabitEthernet1/0/2] quit
```

# 在端口 GigabitEthernet1/0/3 上配置 DHCP Snooping 支持 Option 82 功能，并配置 Option 82 的填充方式为 Normal。

```
[SwitchA] interface gigabitethernet1/0/3
[SwitchA-GigabitEthernet1/0/3] dhcp-snooping information enable
[SwitchA-GigabitEthernet1/0/3] dhcp-snooping information format normal
[SwitchA-GigabitEthernet1/0/3] quit
```

### 2. DHCP 服务器的配置



说明

DHCP server 使用的是 Cisco Catalyst 3745 设备上的配置，对应的软件版本为 IOS 12.3(11)T2 版本，如果使用其他型号或其他版本的设备，请参考随机资料中的用户手册进行操作。

# 配置接口的 IP 地址为 192.168.10.1/24。

```
Server> enable
Server# configure terminal
Server(config)# interface fastethernet 0/0
Server(config-if)# ip address 192.168.10.1 255.255.255.0
Server(config-if)# exit

配置 DHCP Server 功能，并配置使用 Option 82 信息进行地址分配。
```

```
Server(config)# service dhcp
Server(config)# ip dhcp use class

为从 DHCP snooping 设备 GigabitEthernet1/0/1 端口接入的 group1 用户建立 DHCP 分类，并配置匹配的 Option 82 信息为 Circuit ID 子选项中的 VLAN 编号与端口编号，无需匹配的内容可以使用通配符 “*” 代替。
```

```
Server(config)# ip dhcp class group1
Server(dhcp-class)# relay agent information
Server(dhcp-class-relayinfo)# relay-information hex 0106000400010001*
Server(dhcp-class-relayinfo)# exit
```

# 为从 DHCP snooping 设备 GigabitEthernet1/0/2 端口接入的 group2 用户配置分类和匹配信息，方法与上面命令相似，只是将 Option 82 信息中的端口编号由 1 改为 2。

```
Server(config)# ip dhcp class group2
Server(dhcp-class)# relay agent information
Server(dhcp-class-relayinfo)# relay-information hex 0106000400010002*
Server(dhcp-class-relayinfo)# exit
```

# 为从 DHCP snooping 设备 GigabitEthernet1/0/3 端口接入的 group3 用户配置分类和匹配信息，方法与上面命令相似。

```
Server(config)# ip dhcp class group3
Server(dhcp-class)# relay agent information
Server(dhcp-class-relayinfo)# relay-information hex 0106000400010003*
Server(dhcp-class-relayinfo)# exit
```

# 创建 DHCP 地址池 office，为 DHCP 地址池配置租约期限、网关、DNS 和 WINS 服务器地址。

```
Server(config)# ip dhcp pool office
Server(dhcp-config)# network 192.168.10.0
Server(dhcp-config)# lease 0 12
Server(dhcp-config)# default-router 192.168.10.1
Server(dhcp-config)# dns-server 192.168.100.2
Server(dhcp-config)# netbios-name-server 192.168.100.3
```

# 为三个 DHCP 分类分别指定地址范围。

```
Server(dhcp-config)# class group1
Server(dhcp-pool-class)# address range 192.168.10.2 192.168.10.25
Server(dhcp-pool-class)# class group2
Server(dhcp-pool-class)# address range 192.168.10.100 192.168.10.150
Server(dhcp-pool-class)# class group3
Server(dhcp-pool-class)# address range 192.168.10.151 192.168.10.200
```

## 1.5.5 完整配置

#

```

dhcp-snooping
#
interface GigabitEthernet1/0/4
dhcp-snooping trust
#
interface GigabitEthernet1/0/1
dhcp-snooping information enable
dhcp-snooping information format normal
#
interface GigabitEthernet1/0/2
dhcp-snooping information enable
dhcp-snooping information format normal
#
interface GigabitEthernet1/0/3
dhcp-snooping information enable
dhcp-snooping information format normal
#

```

### 1.5.6 配置注意事项

- 只有使能 DHCP snooping 功能之后，DHCP Option 82 功能才能生效。
- DHCP snooping option 82 功能建议在最靠近 DHCP client 的 snooping 设备上使用，以达到精确定位用户位置的目的。

## 1.6 DHCP 客户端典型配置指导

指定设备的接口作为 DHCP 客户端后，可以使用 DHCP 协议从 DHCP 服务器动态获得 IP 地址等参数，方便用户配置，也便于集中管理。

### 1.6.1 组网图

如图 1-2

### 1.6.2 应用要求

在交换机上配置 VLAN 接口 1 通过 DHCP 方式来获取 IP 地址。

### 1.6.3 适用产品、版本

表1-6 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                                | 硬件版本                         |
|-------------------|-------------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301 软件版本，Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301 软件版本，Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本                   | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本                   | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本                   | 全系列硬件版本                      |



| 产品                | 软件版本                                 | 硬件版本    |
|-------------------|--------------------------------------|---------|
| S7500E 系列以太网交换机   | Release 6100 软件版本, Release 6300 软件版本 | 全系列硬件版本 |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本                    | 全系列硬件版本 |

#### 1.6.4 配置过程和解释

# 创建交换机 VLAN1 接口并进入 Vlan-interface1 接口视图

```
[SwitchB] interface Vlan-interface 1
```

# 配置 Vlan-interface1 通过 DHCP 方式来获取 IP 地址

```
[SwitchB-Vlan-interface1] ip address dhcp-alloc
```

```
[SwitchB-Vlan-interface1] quit
```

#### 1.6.5 完整配置

```
#
interface Vlan-interface1
 ip address dhcp-alloc
#
```

#### 1.6.6 配置注意事项

建议不要在同一台设备上同时配置 DHCP 客户端和 DHCP Snooping 功能，否则可能无法生成 DHCP Snooping 表项，DHCP 客户端也可能申请不到 IP 地址。

### 1.7 自动配置功能典型配置指导

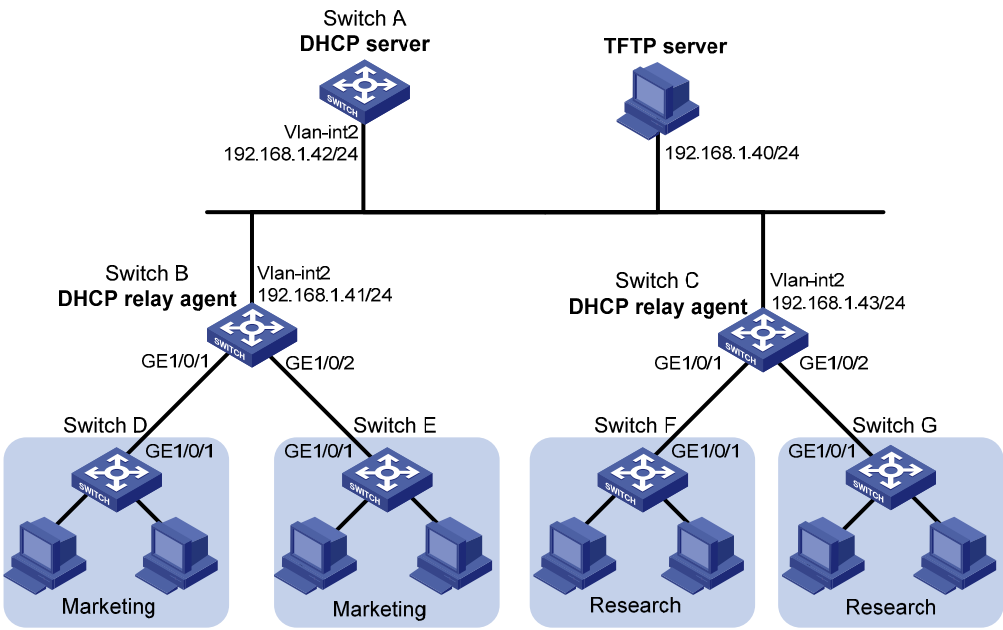
自动配置功能是指在设备空配置启动时自动获取并执行配置文件的功能。自动配置功能简化了网络配置，便于实现对设备的集中管理。

自动配置的基本工作过程为：

- (1) 交换机在空配置启动时，系统会自动将处于 up 状态的接口（如缺省 VLAN 对应的接口）配置为通过 DHCP 方式获得 IP 地址及后续获取配置文件所需要的信息（例如：配置文件名、TFTP 服务器的域名、TFTP 服务器的 IP 地址、DNS 服务器 IP 地址等信息）。
- (2) 如果交换机成功地从 DHCP 服务器获取到 IP 地址及配置文件名等相关信息，则发起 TFTP 请求，从指定的 TFTP 服务器获取配置文件。如果设备没有获取到相关信息，则在空配置文件的情况下正常启动。

### 1.7.1 组网图

图1-6 自动配置组网图



### 1.7.2 应用需求

某公司下属两个部门：市场部门和研发部门，连接终端主机的交换机分别通过不同的网关设备（同时作为DHCP中继）连入网络，如图 1-6所示。

- Switch A 作为 DHCP server，分别为市场部 and 研发部的主机分配 IP 地址和其他网络配置参数；
- 主机上运行 TFTP32 软件，作为 TFTP server；
- 市场部的网关设备为 Switch B，Switch B 同时作为 DHCP 中继，通过 VLAN 接口 2 与 DHCP server、TFTP server 相连，通过 VLAN 接口 3 与连接终端主机的 Switch D 和 Switch E 相连。VLAN 接口 3 的 IP 地址为 192.168.2.1/24。
- Switch D 和 Switch E 分别通过 VLAN 接口 3 与 DHCP 中继 Switch B 连接。
- 研发部的网关设备为 Switch C，Switch C 同时作为 DHCP 中继，通过 VLAN 接口 2 与 DHCP server、TFTP server 相连，通过 VLAN 接口 3 与连接终端主机的 Switch F 和 Switch G 相连。VLAN 接口 3 的 IP 地址为 192.168.3.1/24。
- Switch F 和 Switch G 分别通过 VLAN 接口 3 与 DHCP 中继 Switch C 连接。

为了简化对网络中设备的管理，使网络管理员能够通过 Telnet 方式登录、控制设备，并提供一定的安全保证，连接终端主机的交换机运行自动配置功能，使得交换机启动后自动获取配置文件。配置文件包括如下内容：

- 接口通过 DHCP 获取 IP 地址；
- 启动 Telnet 服务器功能；
- 创建本地用户；
- 配置通过 Telnet 方式登录设备时，需要进行认证。

### 1.7.3 适用产品、版本

表1-7 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                                 | 硬件版本    |
|-------------------|--------------------------------------|---------|
| S3610 系列以太网交换机    | Release 5301 软件版本, Release 5303 软件版本 | 全系列硬件版本 |
| S5510 系列以太网交换机    | Release 5301 软件版本, Release 5303 软件版本 | 全系列硬件版本 |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本                    | 全系列硬件版本 |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本                    | 全系列硬件版本 |

### 1.7.4 配置过程和解释



#### 说明

以下配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下配置不冲突。

#### 1. DHCP server 设备 Switch A 的配置

# 配置 VLAN 接口 2 的 IP 地址

```
<SwitchA> system-view
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/1
[SwitchA-vlan2] quit
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 192.168.1.42
[SwitchA-Vlan-interface2] quit
```

# 使能 DHCP 服务。

```
[SwitchA] dhcp enable
```

# 配置 DHCP 地址池 market，为市场部动态分配 192.168.2.0/24 网段的地址，并指定 TFTP 服务器、网关地址和配置文件名。

```
[SwitchA] dhcp server ip-pool market
[SwitchA-dhcp-pool-market] network 192.168.2.0 24
[SwitchA-dhcp-pool-market] tftp ip-address 192.168.1.40
[SwitchA-dhcp-pool-market] gateway-list 192.168.2.1
[SwitchA-dhcp-pool-market] bootfile-name market.cfg
[SwitchA-dhcp-pool-market] quit
```

# 配置 DHCP 地址池 research，为研发部动态分配 192.168.3.0/24 网段的地址，并指定 TFTP 服务器、网关地址和配置文件名。

```
[SwitchA] dhcp server ip-pool research
[SwitchA-dhcp-pool-research] network 192.168.3.0 24
[SwitchA-dhcp-pool-research] tftp ip-address 192.168.1.40
[SwitchA-dhcp-pool-research] gateway-list 192.168.3.1
[SwitchA-dhcp-pool-research] bootfile-name research.cfg
```

```
[SwitchA-dhcp-pool-research] quit
```

# 配置到达 DHCP 中继的静态路由。

```
[SwitchA] ip route-static 192.168.2.0 24 192.168.1.41
```

```
[SwitchA] ip route-static 192.168.3.0 24 192.168.1.43
```

```
[SwitchA] quit
```

## 2. DHCP 中继设备 Switch B 的配置

# 配置 VLAN 接口 2 和 VLAN 接口 3 的 IP 地址

```
<SwitchB> system-view
```

```
[SwitchB] vlan 2
```

```
[SwitchB-vlan2] port gigabitethernet 1/0/3
```

```
[SwitchB-vlan2] quit
```

```
[SwitchB] interface vlan-interface 2
```

```
[SwitchB-Vlan-interface2] ip address 192.168.1.41
```

```
[SwitchB-Vlan-interface2] quit
```

```
[SwitchB] vlan 3
```

```
[SwitchB-vlan3] port gigabitethernet 1/0/1
```

```
[SwitchB-vlan3] port gigabitethernet 1/0/2
```

```
[SwitchB-vlan3] quit
```

```
[SwitchB] interface vlan-interface 3
```

```
[SwitchB-Vlan-interface3] ip address 192.168.2.1
```

```
[SwitchB-Vlan-interface3] quit
```

# 使能 DHCP 服务。

```
[SwitchB] dhcp enable
```

# 配置 DHCP 服务器的地址

```
[SwitchB] dhcp relay server-group 1 ip 192.168.1.42
```

# 配置 VLAN 接口 3 工作在 DHCP 中继模式。

```
[SwitchB] interface vlan-interface 3
```

```
[SwitchB-Vlan-interface3] dhcp select relay
```

# 配置 VLAN 接口 3 对应 DHCP 服务器组 1。

```
[SwitchB-Vlan-interface3] dhcp relay server-select 1
```

## 3. DHCP 中继设备 Switch C 的配置

# 配置接口的 IP 地址

```
<SwitchC> system-view
```

```
[SwitchC] vlan 2
```

```
[SwitchC-vlan2] port gigabitethernet 1/0/3
```

```
[SwitchC-vlan2] quit
```

```
[SwitchC] interface vlan-interface 2
```

```
[SwitchC-Vlan-interface2] ip address 192.168.1.43
```

```
[SwitchC-Vlan-interface2] quit
```

```
[SwitchC] vlan 3
```

```
[SwitchC-vlan3] port gigabitethernet 1/0/1
```

```
[SwitchC-vlan3] port gigabitethernet 1/0/2
```

```
[SwitchC-vlan3] quit
[SwitchC] interface vlan-interface 3
[SwitchC-Vlan-interface3] ip address 192.168.3.1
[SwitchC-Vlan-interface3] quit

使能 DHCP 服务。

[SwitchC] dhcp enable

配置 DHCP 服务器的地址

[SwitchC] dhcp relay server-group 1 ip 192.168.1.42

配置 VLAN 接口 3 工作在 DHCP 中继模式。

[SwitchC] interface vlan-interface 3
[SwitchC-Vlan-interface3] dhcp select relay

配置 VLAN 接口 3 对应 DHCP 服务器组 1。

[SwitchC-Vlan-interface3] dhcp relay server-select 1
```

#### 4. 配置主机作为 TFTP server

# 在主机的“D:/TFTP server”目录下创建配置文件 market.cfg，文件内容如下。

```
#
sysname Market
#
telnet server enable
#
vlan 3
#
local-user market
password simple market
service-type telnet
level 3
#
interface Vlan-interface3
ip address dhcp-alloc
#
interface GigabitEthernet1/0/1
port access vlan 3
#
user-interface vty 0 4
authentication-mode scheme
user privilege level 3
#
return
```

# 在主机的“D:/TFTP server”目录下创建配置文件 research.cfg，文件内容如下。

```
#
sysname Research
#
telnet server enable
#
```

```

vlan 3
#
local-user research
password simple research
service-type telnet
level 3
#
interface Vlan-interface3
ip address dhcp-alloc
#
interface GigabitEthernet1/0/1
port access vlan 3
#
user-interface vty 0 4
authentication-mode scheme
user privilege level 3
#
return

```

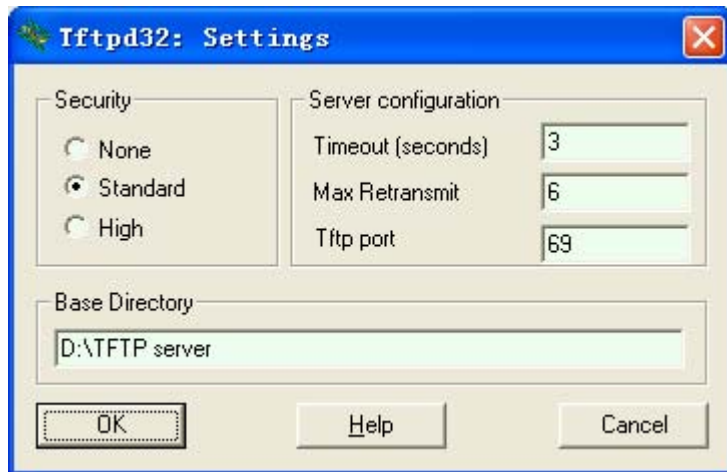
# 运行TFTP32 软件，点击<Settings>，如图 1-7所示。

图1-7 TFTP server 配置界面



# 将配置文件保存的路径设置为“Base Directory”，单击<OK>，如图 1-8所示。

图1-8 设置文件保存的路径



# 配置主机到达 192.168.2.0/24 和 192.168.3.0/24 网段的路由，即在主机上执行如下命令：

```
route add 192.168.2.0 mask 255.255.255.0 192.168.1.41
route add 192.168.3.0 mask 255.255.255.0 192.168.1.43
```

### 1.7.5 完整配置

- Switch A 上的完整配置

```
#
vlan 1
#
vlan 2
#
dhcp server ip-pool market
network 192.168.2.0 mask 255.255.255.0
gateway-list 192.168.2.1
bootfile-name market.cfg
tftp-server ip-address 192.168.1.17
#
dhcp server ip-pool research
network 192.168.3.0 mask 255.255.255.0
gateway-list 192.168.3.1
bootfile-name research.cfg
tftp-server ip-address 192.168.1.17
#
interface Vlan-interface2
ip address 192.168.1.42 255.255.255.0
#
interface GigabitEthernet1/0/1
port access vlan 2
#
ip route-static 192.168.2.0 255.255.255.0 192.168.1.41
ip route-static 192.168.3.0 255.255.255.0 192.168.1.43
#
dhcp enable
```

```
#
```

- Switch B 上的完整配置

```
#
```

```
dhcp relay server-group 1 ip 192.168.1.42
```

```
#
```

```
vlan 1
```

```
#
```

```
vlan 2
```

```
#
```

```
vlan 3
```

```
#
```

```
interface Vlan-interface2
```

```
ip address 192.168.1.41 255.255.255.0
```

```
#
```

```
interface Vlan-interface3
```

```
ip address 192.168.2.1 255.255.255.0
```

```
dhcp select relay
```

```
dhcp relay server-select 1
```

```
#
```

```
interface GigabitEthernet1/0/1
```

```
port access vlan 3
```

```
#
```

```
interface GigabitEthernet1/0/2
```

```
port access vlan 3
```

```
#
```

```
interface GigabitEthernet1/0/3
```

```
port access vlan 2
```

```
#
```

```
dhcp enable
```

```
#
```

- Switch C 上的完整配置

```
#
```

```
dhcp relay server-group 1 ip 192.168.1.42
```

```
#
```

```
vlan 1
```

```
#
```

```
vlan 2
```

```
#
```

```
vlan 3
```

```
#
```

```
interface Vlan-interface2
```

```
ip address 192.168.1.43 255.255.255.0
```

```
#
```

```
interface Vlan-interface3
```

```
ip address 192.168.3.1 255.255.255.0
```

```
dhcp select relay
```

```
dhcp relay server-select 1
```

```
#
```



```
interface GigabitEthernet1/0/1
port access vlan 3
#
interface GigabitEthernet1/0/2
port access vlan 3
#
interface GigabitEthernet1/0/3
port access vlan 2
#
dhcp enable
#
```

### 1.7.6 注意事项

- 设备应用自动配置功能之前，需要完成 DHCP server、DHCP 中继、TFTP server 和 DNS server（可选）的配置，并将设备的配置文件保存到 TFTP 服务器。
- DHCP server 需要为客户端分配网关地址，设备才能够跨网段请求 TFTP 和 DNS 服务。
- 为了保证自动配置功能正常使用，建议设备启动前，只将设备的一个接口连入网络。
- 设备通过自动配置功能获取配置文件后，只是执行配置文件，不会将配置文件保存到本地。设备再次启动时，需要重新获取配置文件。

# 目 录

|                              |      |
|------------------------------|------|
| 1 IPv4 ACL典型配置指导 .....       | 1-1  |
| 1.1 基本IPv4 ACL典型配置指导 .....   | 1-1  |
| 1.1.1 组网图 .....              | 1-1  |
| 1.1.2 应用要求 .....             | 1-1  |
| 1.1.3 适用产品、版本 .....          | 1-1  |
| 1.1.4 配置过程和解释 .....          | 1-1  |
| 1.1.5 完整配置 .....             | 1-2  |
| 1.1.6 配置注意事项 .....           | 1-3  |
| 1.2 高级IPv4 ACL典型配置指导 .....   | 1-4  |
| 1.2.1 组网图 .....              | 1-4  |
| 1.2.2 应用要求 .....             | 1-4  |
| 1.2.3 适用产品、版本 .....          | 1-4  |
| 1.2.4 配置过程和解释 .....          | 1-5  |
| 1.2.5 完整配置 .....             | 1-6  |
| 1.2.6 配置注意事项 .....           | 1-7  |
| 1.3 二层ACL典型配置指导 .....        | 1-7  |
| 1.3.1 组网图 .....              | 1-8  |
| 1.3.2 应用要求 .....             | 1-8  |
| 1.3.3 适用产品、版本 .....          | 1-8  |
| 1.3.4 配置过程和解释 .....          | 1-8  |
| 1.3.5 完整配置 .....             | 1-9  |
| 1.3.6 配置注意事项 .....           | 1-9  |
| 1.4 用户自定义ACL和流模板典型配置指导 ..... | 1-10 |
| 1.4.1 组网图 .....              | 1-10 |
| 1.4.2 应用要求 .....             | 1-10 |
| 1.4.3 适用产品、版本 .....          | 1-11 |
| 1.4.4 配置过程和解释 .....          | 1-11 |
| 1.4.5 完整配置 .....             | 1-11 |
| 1.4.6 配置注意事项 .....           | 1-12 |
| 2 IPv6 ACL典型配置指导 .....       | 2-1  |
| 2.1 基本IPv6 ACL典型配置指导 .....   | 2-1  |
| 2.1.1 组网图 .....              | 2-1  |
| 2.1.2 应用要求 .....             | 2-1  |
| 2.1.3 适用产品、版本 .....          | 2-1  |
| 2.1.4 配置过程和解释 .....          | 2-1  |
| 2.1.5 完整配置 .....             | 2-2  |
| 2.1.6 配置注意事项 .....           | 2-2  |
| 2.2 高级IPv6 ACL典型配置指导 .....   | 2-3  |
| 2.2.1 组网图 .....              | 2-3  |
| 2.2.2 应用要求 .....             | 2-3  |
| 2.2.3 适用产品、版本 .....          | 2-4  |

2.2.4 配置过程和解释 .....2-4

2.2.5 完整配置 .....2-4

2.2.6 配置注意事项 .....2-5

# 1 IPv4 ACL 典型配置指导

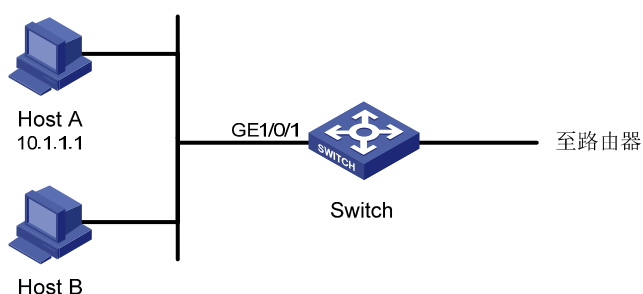
## 1.1 基本 IPv4 ACL 典型配置指导

基本 IPv4 ACL 只根据源 IP 地址信息制定匹配规则，对报文进行相应的分析处理。

基本 IPv4 ACL 的序号取值范围为 2000～2999。

### 1.1.1 组网图

图1-1 配置基本 IPv4 ACL 组网图



### 1.1.2 应用要求

Host A 和 Host B 通过端口 GigabitEthernet 1/0/1 接入交换机（以 S5500-EI 为例），Host A 的 IP 地址为 10.1.1.1。要求配置基本 IPv4 ACL，实现在每天 8:00～18:00 的时间段内，只允许 Host A 发出的 IP 报文通过，拒绝其它的 IP 报文通过。

### 1.1.3 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本                         |
|-------------------|---------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本               | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本               | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本                      |

### 1.1.4 配置过程和解释

# 定义周期时间段 trname，时间范围为每天的 8:00～18:00。

```
<Switch> system-view
```

```
[Switch] time-range trname 8:00 to 18:00 daily
```

# 定义基本 IPv4 ACL 2000，配置源 IP 地址为 10.1.1.1 的访问规则。

```
[Switch] acl number 2000
[Switch-acl-basic-2000] rule permit source 10.1.1.1 0 time-range trname
[Switch-acl-basic-2000] quit
```

# 定义基本 IPv4 ACL 2001，配置源 IP 地址为任意地址的访问规则。

```
[Switch] acl number 2001
[Switch-acl-basic-2001] rule deny time-range trname
[Switch-acl-basic-2001] quit
```

# 定义类 classifier\_hostA，对匹配基本 IPv4 ACL 2000 的报文进行分类。

```
[Switch] traffic classifier classifier_hostA
[Switch-classifier-classifier_hostA] if-match acl 2000
[Switch-classifier-classifier_hostA] quit
```

# 定义流行为 behavior\_hostA，动作为允许报文通过。

```
[Switch] traffic behavior behavior_hostA
[Switch-behavior-behavior_hostA] filter permit
[Switch-behavior-behavior_hostA] quit
```

# 定义类 classifier\_hostB，对匹配基本 IPv4 ACL 2001 的报文进行分类。

```
[Switch] traffic classifier classifier_hostB
[Switch-classifier-classifier_hostB] if-match acl 2001
[Switch-classifier-classifier_hostB] quit
```

# 定义流行为 behavior\_hostB，动作为拒绝报文通过。

```
[Switch] traffic behavior behavior_hostB
[Switch-behavior-behavior_hostB] filter deny
[Switch-behavior-behavior_hostB] quit
```

# 定义策略 policy\_host，为类 classifier\_hostA 指定流行为 behavior\_hostA，为类 classifier\_hostB 指定流行为 behavior\_hostB。其中 **filter permit** 和 **filter deny** 动作必须配置到不同的 **classifier-behavior** 中，并且在配置过程中需要注意两者的先后顺序，以保证应用策略后实际的运行结果与用户的配置意图一致。

```
[Switch] qos policy policy_host
[Switch-qospolicy-policy_host] classifier classifier_hostA behavior behavior_hostA
[Switch-qospolicy-policy_host] classifier classifier_hostB behavior behavior_hostB
[Switch-qospolicy-policy_host] quit
```

# 将策略 policy\_host 应用到端口 GigabitEthernet 1/0/1。

```
[Switch] interface GigabitEthernet 1/0/1
[Switch-GigabitEthernet1/0/1] qos apply policy policy_host inbound
```

### 1.1.5 完整配置

```
#
traffic classifier classifier_hostB operator and
if-match acl 2001
traffic classifier classifier_hostA operator and
if-match acl 2000
#
```

```

traffic behavior behavior_hostB
 filter deny
traffic behavior behavior_hostA
 filter permit
#
qos policy policy_host
 classifier classifier_hostA behavior behavior_hostA
 classifier classifier_hostB behavior behavior_hostB
##
time-range trname 08:00 to 18:00 daily
#
acl number 2000
 rule 0 permit source 10.1.1.1 0 time-range trname
acl number 2001
 rule 0 deny time-range trname
#
interface GigabitEthernet1/0/1
 qos apply policy policy_host inbound
#

```

### 1.1.6 配置注意事项

需要注意的是：

- 当基本 IPv4 ACL 的匹配顺序为 **config** 时，用户可以修改该 ACL 中的任何一条已经存在的规则，在修改 ACL 中的某条规则时，该规则中没有修改到的部分仍旧保持原来的状态；当 ACL 的匹配顺序为 **auto** 时，用户不能修改该 ACL 中的任何一条已经存在的规则，否则系统会提示错误信息。
- 新建或修改后的规则不能和已经存在的规则相同，否则会导致创建或修改不成功，系统会提示该规则已经存在。
- 当基本 IPv4 ACL 的匹配顺序为 **auto** 时，新建的规则将按照“深度优先”的原则插入到已有的规则中，但是所有规则对应的编号不会改变。
- 当基本 IPv4 ACL 被 QoS 策略引用对报文进行流分类时，ACL 规则中定义的动作（**deny** 或 **permit**）不起作用，交换机对匹配此 ACL 的报文采取的动作由 QoS 策略中流行为定义的动作决定。
- 当基本 IPv4 ACL 被 QoS 策略引用对报文进行流分类时，各产品的限制情况如下表所示。

表1-2 各产品的限制情况

| 产品                | 说明                                            |
|-------------------|-----------------------------------------------|
| S3610 系列以太网交换机    | 不支持配置 <b>logging</b> 参数                       |
| S5510 系列以太网交换机    | 不支持配置 <b>logging</b> 参数                       |
| S5500-SI 系列以太网交换机 | 不支持配置 <b>logging</b> 参数                       |
| S5500-EI 系列以太网交换机 | 不支持配置 <b>logging</b> 参数                       |
| S7500E 系列以太网交换机   | 不支持配置 <b>logging</b> 和 <b>vpn-instance</b> 参数 |

## 1.2 高级 IPv4 ACL 典型配置指导

高级 IPv4 ACL 可以使用报文的源 IP 地址信息、目的 IP 地址信息、IP 承载的协议类型、协议的特性（例如 TCP 或 UDP 的源端口、目的端口，ICMP 协议的消息类型、消息码等）等信息来制定匹配规则。

高级 IPv4 ACL 支持对三种报文优先级的分析处理：

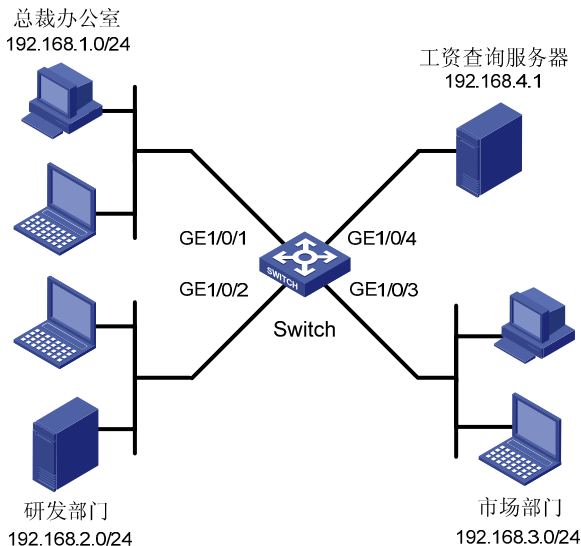
- ToS（Type of Service，服务类型）优先级
- IP 优先级
- DSCP（Differentiated Services CodePoint，差分服务编码点）优先级

用户可以利用高级 IPv4 ACL 定义比基本 IPv4 ACL 更准确、更丰富、更灵活的匹配规则。

高级 IPv4 ACL 的序号取值范围为 3000～3999。

### 1.2.1 组网图

图1-2 配置高级 IPv4 ACL 组网图



### 1.2.2 应用要求

公司企业网通过交换机（以 S5500-EI 为例）实现各部门之间的互连。要求配置高级 IPv4 ACL，禁止研发部门和市场部门在上班时间（8:00 至 18:00）访问工资查询服务器（IP 地址为 192.168.4.1），而总裁办公室不受限制，可以随时访问。

### 1.2.3 适用产品、版本

表1-3 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本                         |
|-------------------|---------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本               | 全系列硬件版本<br>(除 S5500-20TP-SI) |

| 产品                | 软件版本                            | 硬件版本          |
|-------------------|---------------------------------|---------------|
|                   | Release 1301 软件版本               | S5500-20TP-SI |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本       |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本       |

#### 1.2.4 配置过程和解释

##### (1) 定义工作时间段

# 定义 8:00 至 18:00 的周期时间段。

```
<Switch> system-view
[Switch] time-range trname 8:00 to 18:00 working-day
```

##### (2) 定义到工资查询服务器的访问规则

# 定义研发部门到工资查询服务器的访问规则。

```
[Switch] acl number 3000
[Switch-acl-adv-3000] rule deny ip source 192.168.2.0 0.0.0.255 destination 192.168.4.1 0
time-range trname
[Switch-acl-adv-3000] quit
```

# 定义市场部门到工资查询服务器的访问规则。

```
[Switch] acl number 3001
[Switch-acl-adv-3001] rule deny ip source 192.168.3.0 0.0.0.255 destination 192.168.4.1 0
time-range trname
[Switch-acl-adv-3001] quit
```

##### (3) 应用访问规则

# 定义类 classifier\_rd，对匹配高级 IPv4 ACL 3000 的报文进行分类。

```
[Switch] traffic classifier classifier_rd
[Switch-classifier-classifier_rd] if-match acl 3000
[Switch-classifier-classifier_rd] quit
```

# 定义流行为 behavior\_rd，动作为拒绝报文通过。

```
[Switch] traffic behavior behavior_rd
[Switch-behavior-behavior_rd] filter deny
[Switch-behavior-behavior_rd] quit
```

# 定义类 classifier\_market，对匹配高级 IPv4 ACL 3001 的报文进行分类。

```
[Switch] traffic classifier classifier_market
[Switch-classifier-classifier_market] if-match acl 3001
[Switch-classifier-classifier_market] quit
```

# 定义流行为 behavior\_market，动作为拒绝报文通过。

```
[Switch] traffic behavior behavior_market
[Switch-behavior-behavior_market] filter deny
[Switch-behavior-behavior_market] quit
```

# 定义策略 policy\_rd，为类 classifier\_rd 指定流行为 behavior\_rd。



```
[Switch] qos policy policy_rd
[Switch-qospolicy-policy_rd] classifier classifier_rd behavior behavior_rd
[Switch-qospolicy-policy_rd] quit

定义策略 policy_market，为类 classifier_market 指定流行为 behavior_market。

[Switch] qos policy policy_market
[Switch-qospolicy-policy_market] classifier classifier_market behavior behavior_market
[Switch-qospolicy-policy_market] quit

将策略 policy_rd 应用到端口 GigabitEthernet 1/0/2。

[Switch] interface GigabitEthernet 1/0/2
[Switch-GigabitEthernet1/0/2] qos apply policy policy_rd inbound
[Switch-GigabitEthernet1/0/2] quit

将策略 policy_market 应用到端口 GigabitEthernet 1/0/3。

[Switch] interface GigabitEthernet 1/0/3
[Switch-GigabitEthernet1/0/3] qos apply policy policy_market inbound
```

### 1.2.5 完整配置

```
#
traffic classifier classifier_market operator and
if-match acl 3001
traffic classifier classifier_rd operator and
if-match acl 3000
#
traffic behavior behavior_market
filter deny
traffic behavior behavior_rd
filter deny
#
qos policy policy_market
classifier classifier_market behavior behavior_market
qos policy policy_rd
classifier classifier_rd behavior behavior_rd
#
time-range trname 08:00 to 18:00 working-day
#
acl number 3000
rule 0 deny ip source 192.168.2.0 0.0.0.255 destination 192.168.4.1 0 time-range trname
acl number 3001
rule 0 deny ip source 192.168.3.0 0.0.0.255 destination 192.168.4.1 0 time-range trname
#
interface GigabitEthernet1/0/2
qos apply policy policy_rd inbound
#
interface GigabitEthernet1/0/3
qos apply policy policy_market inbound
#
```

### 1.2.6 配置注意事项

需要注意的是：

- 当 ACL 的匹配顺序为 **config** 时，用户可以修改该 ACL 中的任何一条已经存在的规则，在修改 ACL 中的某条规则时，该规则中没有修改到的部分仍旧保持原来的状态；当 ACL 的匹配顺序为 **auto** 时，用户不能修改该 ACL 中的任何一条已经存在的规则，否则系统会提示错误信息。
- 新创建或修改后的规则不能和已经存在的规则相同，否则会导致创建或修改不成功，系统会提示该规则已经存在。
- 当 ACL 的匹配顺序为 **auto** 时，新创建的规则将按照“深度优先”的原则插入到已有的规则中，但是所有规则对应的编号不会改变。
- 当高级 IPv4 ACL 被 QoS 策略引用对报文进行流分类时，ACL 规则中定义的动作（**deny** 或 **permit**）不起作用，交换机对匹配此 ACL 的报文采取的动作由 QoS 策略中流行为定义的动作决定。
- 当高级 IPv4 ACL 被 QoS 策略引用对报文进行流分类时，各产品的限制情况如下表所示。

表1-4 各产品的限制情况

| 产品                | 说明                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| S3610 系列以太网交换机    | 不支持配置 <b>logging</b> 、 <b>reflective</b> 和 <b>established</b> 参数                                                                                                                                                                                                                                                                                                                |
| S5510 系列以太网交换机    | 不支持配置 <b>logging</b> 、 <b>reflective</b> 和 <b>established</b> 参数                                                                                                                                                                                                                                                                                                                |
| S5500-SI 系列以太网交换机 | <ul style="list-style-type: none"><li>• 不支持配置 <b>logging</b>、<b>reflective</b> 和 <b>established</b> 参数</li><li>• 不支持配置操作符 <b>operator</b> 取值为 <b>neq</b></li></ul>                                                                                                                                                                                                              |
| S5500-EI 系列以太网交换机 | <ul style="list-style-type: none"><li>• 当 QoS 策略应用于入方向（<b>inbound</b>）时，不支持配置 <b>logging</b> 和 <b>reflective</b> 参数；不支持配置操作符 <b>operator</b> 取值为 <b>neq</b></li><li>• 当 QoS 策略应用于出方向（<b>outbound</b>）时，不支持配置 <b>logging</b> 和 <b>reflective</b> 参数；不支持配置操作符 <b>operator</b> 取值为 <b>gt</b>、<b>lt</b>、<b>neq</b> 和 <b>range</b></li></ul>                                         |
| S7500E 系列以太网交换机   | <ul style="list-style-type: none"><li>• 当 QoS 策略应用于入方向（<b>inbound</b>）时，不支持配置 <b>logging</b>、<b>reflective</b> 和 <b>vpn-instance</b> 参数；不支持配置操作符 <b>operator</b> 取值为 <b>neq</b></li><li>• 当 QoS 策略应用于出方向（<b>outbound</b>）时，不支持配置 <b>logging</b>、<b>reflective</b> 和 <b>vpn-instance</b> 参数；不支持配置操作符 <b>operator</b> 取值为 <b>gt</b>、<b>lt</b>、<b>neq</b> 和 <b>range</b></li></ul> |

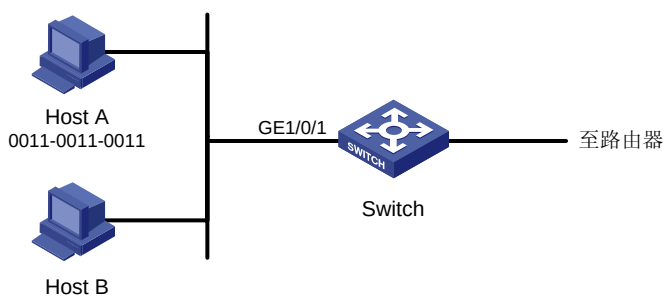
## 1.3 二层 ACL 典型配置指导

二层 ACL 根据报文的源 MAC 地址、目的 MAC 地址、802.1p 优先级、二层协议类型等二层信息制定匹配规则，对报文进行相应的分析处理。

二层 ACL 的序号取值范围为 4000～4999。

### 1.3.1 组网图

图1-3 配置二层 ACL 组网图



### 1.3.2 应用要求

Host A 和 Host B 通过端口 GigabitEthernet 1/0/1 接入交换机（以 S5500-EI 为例），Host A 的 MAC 地址为 0011-0011-0011。要求配置二层 ACL，实现在每天 8:00~18:00 的时间段内，对 Host A 发出的目的 MAC 为 0011-0011-0012 的报文进行过滤。

### 1.3.3 适用产品、版本

表1-5 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本                         |
|-------------------|---------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本               | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本               | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本                      |

### 1.3.4 配置过程和解释

# 定义周期时间段 trname，时间范围为每天的 8:00~18:00。

```
<Switch> system-view
```

```
[Switch] time-range trname 8:00 to 18:00 daily
```

# 定义二层 ACL 4000，配置源 MAC 地址为 0011-0011-0011，目的 MAC 地址为 0011-0011-0012 的报文的访问规则。

```
[Switch] acl number 4000
```

```
[Switch-acl-basic-4000] rule deny source-mac 0011-0011-0011 ffff-ffff-ffff dest-mac 0011-0011-0012 ffff-ffff-ffff time-range trname
```

```
[Switch-acl-basic-4000] quit
```

# 定义类 classifier\_hostA，对匹配二层 ACL 4000 的报文进行分类。

```
[Switch] traffic classifier classifier_hostA
```

```
[Switch-classifier-classifier_hostA] if-match acl 4000
```

```
[Switch-classifier-classifier_hostA] quit
```

# 定义流行为 behavior\_hostA，动作为拒绝报文通过。

```
[Switch] traffic behavior behavior_hostA
[Switch-behavior-behavior_hostA] filter deny
[Switch-behavior-behavior_hostA] quit
```

# 定义策略 policy\_hostA，为类 classifier\_hostA 指定流行为 behavior\_hostA。

```
[Switch] qos policy policy_hostA
[Switch-qospolicy-policy_hostA] classifier classifier_hostA behavior behavior_hostA
[Switch-qospolicy-policy_hostA] quit
```

# 将策略 policy\_hostA 应用到端口 GigabitEthernet 1/0/1。

```
[Switch] interface GigabitEthernet 1/0/1
[Switch-GigabitEthernet1/0/1] qos apply policy policy_hostA inbound
```

### 1.3.5 完整配置

```
#
traffic classifier classifier_hostA operator and
if-match acl 4000
#
traffic behavior behavior_hostA
filter deny
#
qos policy policy_hostA
classifier classifier_hostA behavior behavior_hostA
#
time-range trname 08:00 to 18:00 daily
#
acl number 4000
rule 0 deny source-mac 0011-0011-0011 ffff-ffff-ffff dest-mac 0011-0011-0012 ffff-ffff-ffff
time-range trname
#
interface GigabitEthernet1/0/1
qos apply policy policy_hostA inbound
#
```

### 1.3.6 配置注意事项

需要注意的是：

- 当 ACL 的匹配顺序为 **config** 时，用户可以修改该 ACL 中的任何一条已经存在的规则，在修改 ACL 中的某条规则时，该规则中没有修改到的部分仍旧保持原来的状态；当 ACL 的匹配顺序为 **auto** 时，用户不能修改该 ACL 中的任何一条已经存在的规则，否则系统会提示错误信息。
- 新创建或修改后的规则不能和已经存在的规则相同，否则会导致创建或修改不成功，系统会提示该规则已经存在。
- 当 ACL 的匹配顺序为 **auto** 时，新创建的规则将按照“深度优先”的原则插入到已有的规则中，但是所有规则对应的编号不会改变。

- 当二层 ACL 被 QoS 策略引用对报文进行流分类时, ACL 规则中定义的动作(**deny** 或 **permit**)不起作用, 交换机对匹配此 ACL 的报文采取的动作由 QoS 策略中流行为定义的动作决定。
- 当二层 ACL 被 QoS 策略引用对报文进行流分类时, 各产品的限制情况如下表所示。

表1-6 各产品的限制情况

| 产品                | 说明                   |
|-------------------|----------------------|
| S3610 系列以太网交换机    | 不支持配置 <b>lsap</b> 参数 |
| S5510 系列以太网交换机    | 不支持配置 <b>lsap</b> 参数 |
| S5500-SI 系列以太网交换机 | 不支持配置 <b>lsap</b> 参数 |
| S5500-EI 系列以太网交换机 | 不支持配置 <b>lsap</b> 参数 |
| S7500E 系列以太网交换机   | 不支持配置 <b>lsap</b> 参数 |

## 1.4 用户自定义 ACL 和流模板典型配置指导

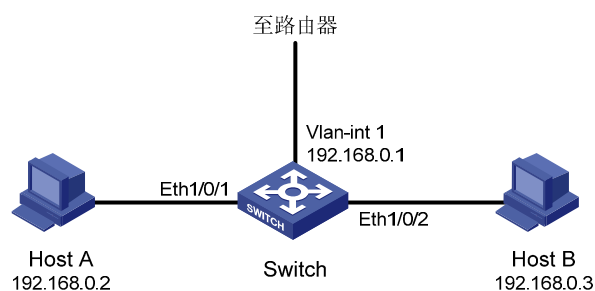
用户自定义 ACL 可以以报文的二层报文头、IP 报文头等为基准, 指定从第几个字节开始与掩码进行“与”操作, 将从报文提取出来的字符串和用户定义的字符串进行比较, 找到匹配的报文, 然后进行相应的处理。

用户自定义 ACL 的序号取值范围为 5000~5999。

流模板的主要功能是对硬件下发的 ACL 规则中所能包含的信息进行限制。在以太网端口下发的 ACL 规则中包含的信息必须是该端口下发流模板中定义信息的子集。比如, 流模板定义了源 IP 地址、目的 IP 地址、源 TCP 端口、目的 TCP 端口等限制, 只有在上述范围内的 ACL 规则可以正确下发到硬件中, 用于 QoS 等功能; 否则 ACL 规则将不能下发到硬件中, 导致 QoS 功能不能引用此 ACL 规则。

### 1.4.1 组网图

图1-4 配置用户自定义 ACL 和流模板组网图



### 1.4.2 应用要求

公司企业网通过交换机（以 S3610 为例）实现互连, 网络环境描述如下:

- Host A 的 IP 地址为 192.168.0.2, 通过端口 Ethernet 1/0/1 接入交换机; Host B 的 IP 地址为 192.168.0.3, 通过端口 Ethernet 1/0/2 接入交换机。
- Host A 和 Host B 属于 VLAN 1, 二者的网关都设置为 192.168.0.1 (交换机 VLAN 1 接口的 IP 地址), 通过交换机访问 Internet。

要求配置用户自定义 ACL，对 Host A 发出的仿冒网关 IP 地址的 ARP 报文进行过滤。

### 1.4.3 适用产品、版本

表1-7 配置适用的产品与软硬件版本关系

| 产品             | 软件版本                            | 硬件版本    |
|----------------|---------------------------------|---------|
| S3610 系列以太网交换机 | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5510 系列以太网交换机 | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |

### 1.4.4 配置过程和解释

# 定义用户自定义 ACL 5000，配置源 IP 地址为 192.168.0.1 的 ARP 报文的访问规则。其中 L2 表示从报文的二层头开始计算，0806 为 ARP 协议号，ffff 为掩码，12 为以太网报文中协议类型字段的偏移量，start 表示从报文的报文头开始计算，c0a80001 为 192.168.0.1 的十六进制形式，28 为 ARP 报文中源 IP 地址字段的偏移量。

```
<Switch> system-view
```

```
[Switch] acl number 5000
```

```
[Switch-acl-user-5000] rule deny L2 0806 ffff 12 start c0a80001 ffffffff 28
```

# 定义扩展型流模板 ftemplate\_hostA。

```
[Switch] flow-template ftemplate_hostA extend L2 12 2 start 28 4
```

# 在端口 Ethernet 1/0/1 上应用流模板 ftemplate\_hostA。

```
[Switch] interface Ethernet 1/0/1
```

```
[Switch-Ethernet1/0/1] flow-template ftemplate_hostA
```

```
[Switch-Ethernet1/0/1] quit
```

# 定义类 classifier\_hostA，对匹配用户自定义 ACL 5000 的报文进行分类。

```
[Switch] traffic classifier classifier_hostA
```

```
[Switch-classifier-classifier_hostA] if-match acl 5000
```

```
[Switch-classifier-classifier_hostA] quit
```

# 定义流行为 behavior\_hostA，动作为拒绝报文通过。

```
[Switch] traffic behavior behavior_hostA
```

```
[Switch-behavior-behavior_hostA] filter deny
```

```
[Switch-behavior-behavior_hostA] quit
```

# 定义策略 policy\_hostA，为类 classifier\_hostA 指定流行为 behavior\_hostA。

```
[Switch] qos policy policy_hostA
```

```
[Switch-qospolicy-policy_hostA] classifier classifier_hostA behavior behavior_hostA
```

```
[Switch-qospolicy-policy_hostA] quit
```

# 将策略 policy\_hostA 应用到端口 Ethernet 1/0/1。

```
[Switch] interface Ethernet 1/0/1
```

```
[Switch-Ethernet1/0/1] qos apply policy policy_hostA inbound
```

### 1.4.5 完整配置

```
#
```

```
flow-template ftemplate_hostA extend start 28 4 l2 12 2
```

```
#
```

```

traffic classifier classifier_hostA operator and
if-match acl 5000
#
traffic behavior behavior_hostA
filter deny
#
qos policy policy_hostA
classifier classifier_hostA behavior behavior_hostA
#
acl number 5000
rule 0 deny start c0a80001 ffffffff 28 l2 0806 ffff 12
#
interface Ethernet1/0/1
flow-template ftemplate_hostA
qos apply policy policy_hostA inbound
#

```

#### 1.4.6 配置注意事项

在配置用户自定义 ACL 时需要注意：

- 和其他类型的 IPv4 ACL 不同，用户自定义 ACL 中包含的规则不支持修改，只能进行覆盖性配置。
- 新创建的规则不能和已经存在的规则相同，否则会导致创建不成功。
- 用户自定义 ACL 的匹配顺序为配置顺序。
- 用户自定义 ACL 需要和扩展型用户自定义流模板配合使用，用户自定义 ACL 中设置的偏移范围必须包含在扩展型用户自定义流模板中设置的偏移范围之内，否则用户自定义 ACL 不能成功应用。
- 当用户自定义 ACL 被 QoS 策略引用对报文进行流分类时，ACL 规则中定义的动作（deny 或 permit）不起作用，交换机对匹配此 ACL 的报文采取的动作由 QoS 策略中流行为定义的动作决定。

在配置流模板时需要注意：

- S3610&S5510 系列以太网交换机支持的流模板包括缺省流模板和用户自定义流模板。其中，用户自定义流模板又可分为标准型和扩展型。
- 标准型用户自定义流模板包含了若干元素，与报文的各个字段相对应；扩展型用户自定义流模板必须和用户自定义 ACL 配合使用，用户可以使用扩展型用户自定义流模板和用户自定义 ACL 对报文的指定字段进行匹配。
- 流模板只对基于硬件处理的 ACL 有效，对基于软件处理的 ACL 不生效。
- 在端口上应用用户自定义流模板之前，必须先配置一个用户自定义流模板；一个端口上只能应用一个流模板。
- 在端口上应用流模板时，请关闭如下功能：802.1x 功能、集群功能（NDP、NTDP、HABP、Cluster）、DHCP Snooping、端口隔离、MAC+IP+端口绑定、灵活 QinQ、Voice VLAN，否则流模板将不能成功应用。同时建议用户不要在端口上应用流模板后开启这些功能。

- 当用户在某一端口应用了扩展型流模板后，不能在此端口上应用包含基本或高级 ACL 的 QoS 策略。
- S3610&S5510 系列以太网交换机最多支持配置两个用户自定义流模板。在配置标准型用户自定义流模板时，每个模板中所有的元素所占字节之和必须小于等于 16 个字节。各个元素所占的字节数如下表所示。

表1-8 各个元素所占字节数

| 名称                | 描述                    | 流模板中占用的字节数 |
|-------------------|-----------------------|------------|
| customer-cos      | 用户网络 802.1p 优先级域      | 1 字节       |
| customer-vlan-id  | 用户网络 VLAN ID 域        | 6 字节       |
| dip               | IP 报文头部的目的 IP 地址域     | 不占用字节      |
| dipv6             | IPv6 报文头部的目的 IPv6 地址域 | 10 字节      |
| dmac              | 以太网报文头部的目的 MAC 地址域    | 6 字节       |
| dport             | 目的端口域                 | 2 字节       |
| ethernet-protocol | 以太网报文头部的协议类型域         | 4 字节       |
| dscp              | IP 报文头部的 DSCP 域       | 1 字节       |
| ip-precedence     | IP 报文头部的 IP 优先级域      |            |
| tos               | IP 报文头部的 ToS 域        |            |
| fragments         | IP 报文的分片标志位域          | 不占用字节      |
| icmp-code         | ICMP 代码域              | 2 字节       |
| icmp-type         | ICMP 类型域              | 2 字节       |
| icmpv6-code       | ICMPv6 代码域            | 2 字节       |
| icmpv6-type       | ICMPv6 类型域            | 2 字节       |
| ip-protocol       | IP 报文头部的协议类型域         | 不占用字节      |
| ipv6-dscp         | IPv6 报文头部的 DSCP 域     | 1 字节       |
| ipv6-fragment     | IPv6 分片标志域            | 不占用字节      |
| ipv6-protocol     | IPv6 报文头部的协议类型域       | 不占用字节      |
| service-cos       | 运营商网络 802.1p 优先级域     | 不占用字节      |
| service-vlan-id   | 运营商网络 VLAN ID 域       | 不占用字节      |
| sip               | IP 报文头部的源 IP 地址域      | 不占用字节      |
| sipv6             | IPv6 报文头部的源 IPv6 地址域  | 不占用字节      |
| smac              | 以太网报文头部的源 MAC 地址域     | 6 字节       |
| sport             | 源端口域                  | 2 字节       |
| tcp-flag          | TCP 报文头部的标志域          | 1 字节       |





#### 说明

- **dscp**、**ip-precedence**、**tos** 三个元素占用同一个字节。同时配置这三个元素，或者同时配置这三个元素中的任意两个，它们在流模板中都只占用 1 个字节。
  - 同时配置 **icmp-code** 和 **icmp-type** 元素，两者所占字节数仍然为 2 个字节。
  - 同时配置 **icmpv6-code** 和 **icmpv6-type** 元素，两者所占字节数仍然为 2 个字节。
  - 同时配置 **icmp-code** 或 **icmp-type** 与 **sport** 元素，只占用 2 个字节；同时配置 **icmpv6-code** 或 **icmpv6-type** 与 **sport** 元素，只占用 2 个字节。
-

## 2 IPv6 ACL 典型配置指导

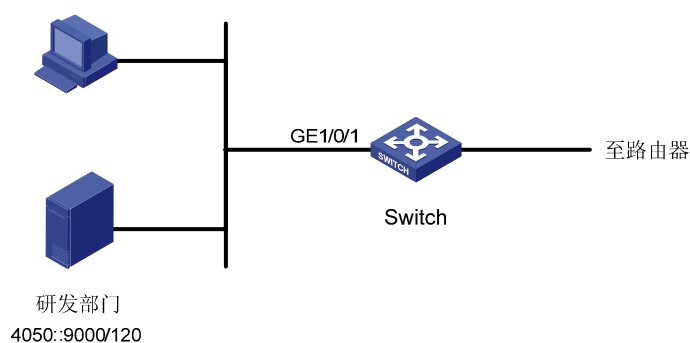
### 2.1 基本 IPv6 ACL 典型配置指导

基本 IPv6 ACL 只根据源 IPv6 地址信息制定匹配规则，对报文进行相应的分析处理。

基本 IPv6 ACL 的序号取值范围为 2000~2999。

#### 2.1.1 组网图

图2-1 配置基本 IPv6 ACL 组网图



#### 2.1.2 应用要求

公司企业网通过交换机（以 S5500-EI 为例）实现各部门之间的互连。

要求配置基本 IPv6 ACL，禁止研发部门（IPv6 地址为 4050::9000/120）访问网络。

#### 2.1.3 适用产品、版本

表2-1 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本                         |
|-------------------|---------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本               | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本               | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本                      |

#### 2.1.4 配置过程和解释

# 定义基本 IPv6 ACL 2000，配置研发部门的访问规则。

```
<Switch> system-view
[Switch] acl ipv6 number 2000
[Switch-acl6-basic-2000] rule deny source 4050::9000/120
[Switch-acl6-basic-2000] quit
```

# 定义类 classifier\_rd，对匹配 IPv6 ACL 2000 的报文进行分类。

```
[Switch] traffic classifier classifier_rd
[Switch-classifier-classifier_rd] if-match acl ipv6 2000
[Switch-classifier-classifier_rd] quit
```

# 定义流行为 behavior\_rd，动作为拒绝报文通过。

```
[Switch] traffic behavior behavior_rd
[Switch-behavior-behavior_rd] filter deny
[Switch-behavior-behavior_rd] quit
```

# 定义策略 policy\_rd，为类 classifier\_rd 指定流行为 behavior\_rd。

```
[Switch] qos policy policy_rd
[Switch-qospolicy-policy_rd] classifier classifier_rd behavior behavior_rd
[Switch-qospolicy-policy_rd] quit
```

# 将策略 policy\_rd 应用到端口 GigabitEthernet 1/0/1。

```
[Switch] interface GigabitEthernet 1/0/1
[Switch-GigabitEthernet1/0/1] qos apply policy policy_rd inbound
```

### 2.1.5 完整配置

```
#
traffic classifier classifier_rd operator and
if-match acl ipv6 2000
#
traffic behavior behavior_rd
filter deny
#
qos policy policy_rd
classifier classifier_rd behavior behavior_rd
#
acl ipv6 number 2000
rule 0 deny source 4050::9000/120
#
interface GigabitEthernet1/0/1
qos apply policy policy_rd inbound
#
```

### 2.1.6 配置注意事项

需要注意的是：

- 当 ACL 的匹配顺序为 **config** 时，用户可以修改该 ACL 中的任何一条已经存在的规则，在修改 ACL 中的某条规则时，该规则中没有修改到的部分仍旧保持原来的状态；当 ACL 的匹配顺序为 **auto** 时，用户不能修改该 ACL 中的任何一条已经存在的规则，否则系统会提示错误信息。
- 新建或修改后的规则不能和已经存在的规则相同，否则会导致创建或修改不成功，系统会提示该规则已经存在。
- 当 ACL 的匹配顺序为 **auto** 时，新建的规则将按照“深度优先”的原则插入到已有的规则中，但是所有规则对应的编号不会改变。

- 当基本 IPv6 ACL 被 QoS 策略引用对报文进行流分类时，ACL 规则中定义的动作（**deny** 或 **permit**）不起作用，交换机对匹配此 ACL 的报文采取的动作由 QoS 策略中流行为定义的动作决定。
- 当基本 IPv6 ACL 被 QoS 策略引用对报文进行流分类时，各产品的限制情况如下表所示。

表2-2 各产品的限制情况

| 产品                | 说明                                        |
|-------------------|-------------------------------------------|
| S3610 系列以太网交换机    | 不支持配置 <b>logging</b> 参数                   |
| S5510 系列以太网交换机    | 不支持配置 <b>logging</b> 参数                   |
| S5500-SI 系列以太网交换机 | 不支持配置 <b>logging</b> 和 <b>fragment</b> 参数 |
| S5500-EI 系列以太网交换机 | 不支持配置 <b>logging</b> 和 <b>fragment</b> 参数 |
| S7500E 系列以太网交换机   | 不支持配置 <b>logging</b> 和 <b>fragment</b> 参数 |

## 2.2 高级 IPv6 ACL 典型配置指导

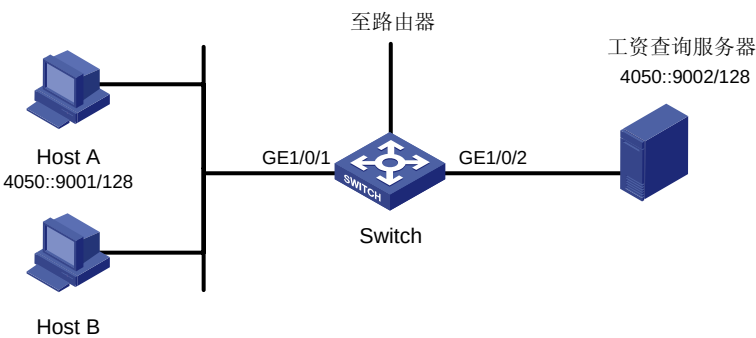
高级 IPv6 ACL 可以使用报文的源 IPv6 地址信息、目的 IPv6 地址信息、IPv6 承载的协议类型、协议的特性（例如 TCP 或 UDP 的源端口、目的端口，ICMP 协议的消息类型、消息码等）等信息来制定匹配规则。

用户可以利用高级 IPv6 ACL 定义比基本 IPv6 ACL 更准确、更丰富、更灵活的规则。

高级 IPv6 ACL 的序号取值范围 3000～3999。

### 2.2.1 组网图

图2-2 配置高级 IPv6 ACL 组网图



### 2.2.2 应用要求

公司企业网通过交换机（以 S5500-EI 为例）实现各部门之间的互连。Host A 和 Host B 通过端口 GigabitEthernet 1/0/1 接入交换机，Host A 的 IPv6 地址为 4050::9001，工资查询服务器的 IPv6 地址为 4050::9002。

要求配置高级 IPv6 ACL，禁止 Host A 访问工资查询服务器。

## 2.2.3 适用产品、版本

表2-3 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本                         |
|-------------------|---------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本               | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本               | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本                      |

## 2.2.4 配置过程和解释

# 定义高级 IPv6 ACL 3000，配置 Host A 的访问规则。

```
<Switch> system-view
[Switch] acl ipv6 number 3000
[Switch-acl6-adv-3000] rule deny ipv6 source 4050::9001 128 destination 4050::9002 128
[Switch-acl6-adv-3000] quit
```

# 定义类 classifier\_hostA，对匹配 IPv6 ACL 3000 的报文进行分类。

```
[Switch] traffic classifier classifier_hostA
[Switch-classifier-classifier_hostA] if-match acl ipv6 3000
[Switch-classifier-classifier_hostA] quit
```

# 定义流行为 behavior\_hostA，动作为拒绝报文通过。

```
[Switch] traffic behavior behavior_hostA
[Switch-behavior-behavior_hostA] filter deny
[Switch-behavior-behavior_hostA] quit
```

# 定义策略 policy\_hostA，为类 classifier\_hostA 指定流行为 behavior\_hostA。

```
[Switch] qos policy policy_hostA
[Switch-qospolicy-policy_hostA] classifier classifier_hostA behavior behavior_hostA
[Switch-qospolicy-policy_hostA] quit
```

# 将策略 policy\_hostA 应用到端口 GigabitEthernet 1/0/1。

```
[Switch] interface GigabitEthernet 1/0/1
[Switch-GigabitEthernet1/0/1] qos apply policy policy_hostA inbound
```

## 2.2.5 完整配置

```
#
traffic classifier classifier_hostA operator and
if-match acl ipv6 3000
#
traffic behavior behavior_hostA
filter deny
#
qos policy policy_hostA
```

```

classifier classifier_hostA behavior behavior_hostA
#
acl ipv6 number 3000
rule 0 deny ipv6 source 4050::9001/128 destination 4050::9002/128
#
interface GigabitEthernet1/0/1
qos apply policy policy_hostA inbound
#

```

## 2.2.6 配置注意事项

需要注意的是：

- 当 ACL 的匹配顺序为 **config** 时，用户可以修改该 ACL 中的任何一条已经存在的规则，在修改 ACL 中的某条规则时，该规则中没有修改到的部分仍旧保持原来的状态；当 ACL 的匹配顺序为 **auto** 时，用户不能修改该 ACL 中的任何一条已经存在的规则，否则系统会提示错误信息。
- 新创建或修改后的规则不能和已经存在的规则相同，否则会导致创建或修改不成功，系统会提示该规则已经存在。
- 当 ACL 的匹配顺序为 **auto** 时，新创建的规则将按照“深度优先”的原则插入到已有的规则中，但是所有规则对应的编号不会改变。
- 当高级 IPv6 ACL 被 QoS 策略引用对报文进行流分类时，ACL 规则中定义的动作（**deny** 或 **permit**）不起作用，交换机对匹配此 ACL 的报文采取的动作由 QoS 策略中流行为定义的动作决定。
- 当高级 IPv6 ACL 被 QoS 策略引用对报文进行流分类时，各产品的限制情况如下表所示。

表2-4 各产品的限制情况

| 产品                | 说明                                                                                                                                                                                                                                                                                                                                     |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| S3610 系列以太网交换机    | <ul style="list-style-type: none"> <li>不支持配置 <b>logging</b> 参数</li> <li>当 <b>protocol</b> 为除 <b>ipv6</b> 之外的其他协议类型时，不支持配置 <b>fragment</b> 参数</li> </ul>                                                                                                                                                                                |
| S5510 系列以太网交换机    | <ul style="list-style-type: none"> <li>不支持配置 <b>logging</b> 参数</li> <li>当 <b>protocol</b> 为除 <b>ipv6</b> 之外的其他协议类型时，不支持配置 <b>fragment</b> 参数</li> </ul>                                                                                                                                                                                |
| S5500-SI 系列以太网交换机 | <ul style="list-style-type: none"> <li>不支持配置 <b>dscp</b>、<b>fragment</b> 和 <b>logging</b> 参数</li> <li>不支持配置操作符 <b>operator</b> 取值为 <b>gt</b>、<b>lt</b>、<b>neq</b> 和 <b>range</b></li> </ul>                                                                                                                                            |
| S5500-EI 系列以太网交换机 | <ul style="list-style-type: none"> <li>当 QoS 策略应用于入方向（<b>inbound</b>）时，不支持配置 <b>logging</b> 和 <b>reflective</b> 参数；不支持配置操作符 <b>operator</b> 取值为 <b>neq</b></li> <li>当 QoS 策略应用于出方向（<b>outbound</b>）时，不支持配置 <b>logging</b> 和 <b>reflective</b> 参数；不支持配置操作符 <b>operator</b> 取值为 <b>gt</b>、<b>lt</b>、<b>neq</b> 和 <b>range</b></li> </ul> |
| S7500E 系列以太网交换机   | <ul style="list-style-type: none"> <li>当 QoS 策略应用于入方向（<b>inbound</b>）时，不支持配置 <b>logging</b> 和 <b>reflective</b> 参数；不支持配置操作符 <b>operator</b> 取值为 <b>neq</b></li> <li>当 QoS 策略应用于出方向（<b>outbound</b>）时，不支持配置 <b>logging</b> 和 <b>reflective</b> 参数；不支持配置操作符 <b>operator</b> 取值为 <b>gt</b>、<b>lt</b>、<b>neq</b> 和 <b>range</b></li> </ul> |

# 目 录

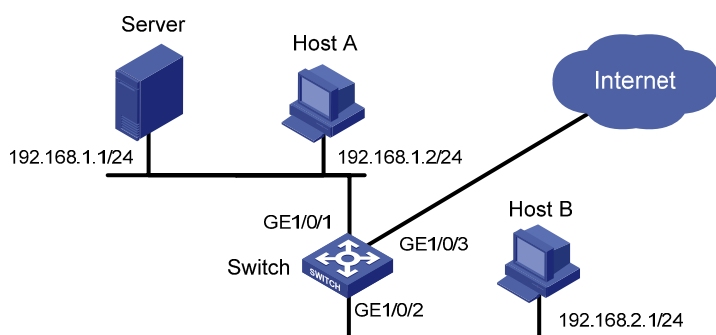
|                            |      |
|----------------------------|------|
| 1 QoS典型配置指导.....           | 1-1  |
| 1.1 端口限速和流量监管典型配置指导 .....  | 1-1  |
| 1.1.1 组网图.....             | 1-1  |
| 1.1.2 应用要求 .....           | 1-1  |
| 1.1.3 适用产品、版本 .....        | 1-1  |
| 1.1.4 配置过程和解释 .....        | 1-2  |
| 1.1.5 完整配置 .....           | 1-3  |
| 1.1.6 配置注意事项 .....         | 1-4  |
| 1.2 优先级重标记和队列调度典型配置指导..... | 1-6  |
| 1.2.1 组网图.....             | 1-6  |
| 1.2.2 应用要求 .....           | 1-6  |
| 1.2.3 适用产品、版本 .....        | 1-7  |
| 1.2.4 配置过程和解释 .....        | 1-7  |
| 1.2.5 完整配置 .....           | 1-9  |
| 1.2.6 配置注意事项 .....         | 1-9  |
| 1.3 优先级映射和队列调度典型配置指导 ..... | 1-11 |
| 1.3.1 组网图.....             | 1-11 |
| 1.3.2 应用要求 .....           | 1-11 |
| 1.3.3 适用产品、版本 .....        | 1-12 |
| 1.3.4 配置过程和解释 .....        | 1-12 |
| 1.3.5 完整配置 .....           | 1-13 |
| 1.3.6 配置注意事项 .....         | 1-13 |
| 1.4 流镜像和重定向至端口典型配置指导 ..... | 1-16 |
| 1.4.1 组网图.....             | 1-16 |
| 1.4.2 应用要求 .....           | 1-16 |
| 1.4.3 适用产品、版本 .....        | 1-17 |
| 1.4.4 配置过程和解释 .....        | 1-17 |
| 1.4.5 完整配置 .....           | 1-18 |
| 1.4.6 配置注意事项 .....         | 1-19 |
| 1.5 重定向至下一跳典型配置指导 .....    | 1-20 |
| 1.5.1 组网图.....             | 1-20 |
| 1.5.2 应用要求 .....           | 1-20 |
| 1.5.3 适用产品、版本 .....        | 1-20 |
| 1.5.4 配置过程和解释 .....        | 1-21 |
| 1.5.5 完整配置 .....           | 1-22 |
| 1.5.6 配置注意事项 .....         | 1-22 |

# 1 QoS 典型配置指导

## 1.1 端口限速和流量监管典型配置指导

### 1.1.1 组网图

图1-1 配置端口限速和流量监管组网图



### 1.1.2 应用要求

公司企业网通过交换机（以 S5500-EI 为例）实现互连。网络环境描述如下：

- Host A 的 IP 地址为 192.168.1.2，Server 的 IP 地址为 192.168.1.1，两者通过端口 GigabitEthernet 1/0/1 接入交换机；
- Host B 的 IP 地址为 192.168.2.1，通过端口 GigabitEthernet 1/0/2 接入交换机。

配置端口限速和流量监管，实现如下需求：

- 限制 Switch 向 Internet 发送的流量为 640kbps，丢弃超出限制的报文；
- 限制 Host A 向外发出的流量为 320kbps，丢弃超出限制的报文；
- 限制 Host B 与 Server 之间的流量为 64kbps，丢弃超出限制的报文。

### 1.1.3 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本                         |
|-------------------|---------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本               | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本               | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本                      |



#### 1.1.4 配置过程和解释

##### (1) 针对 Switch 配置端口限速

# 在端口 GigabitEthernet 1/0/3 上配置端口限速，限制端口发送报文的速率为 640kbps。

```
<Switch> system-view
[Switch] interface GigabitEthernet 1/0/3
[Switch-GigabitEthernet1/0/3] qos lr outbound cir 640
[Switch-GigabitEthernet1/0/3] quit
```

##### (2) 针对 Host A 配置流量监管

# 定义基本 ACL 2000，对源 IP 地址为 192.168.1.2 的报文进行分类。

```
[Switch] acl number 2000
[Switch-acl-basic-2000] rule permit source 192.168.1.2 0
[Switch-acl-basic-2000] quit
```

# 定义类 classifier\_hostA，匹配基本 ACL 2000。

```
[Switch] traffic classifier classifier_hostA
[Switch-classifier-classifier_hostA] if-match acl 2000
[Switch-classifier-classifier_hostA] quit
```

# 定义流行为 behavior\_hostA，动作为限制报文的流量为 320kbps。

```
[Switch] traffic behavior behavior_hostA
[Switch-behavior-behavior_hostA] car cir 320
[Switch-behavior-behavior_hostA] quit
```

# 定义策略 policy\_hostA，为类 classifier\_hostA 指定流行为 behavior\_hostA。

```
[Switch] qos policy policy_hostA
[Switch-qospolicy-policy_hostA] classifier classifier_hostA behavior behavior_hostA
[Switch-qospolicy-policy_hostA] quit
```

# 将策略 policy\_hostA 应用到端口 GigabitEthernet 1/0/1 上。

```
[Switch] interface GigabitEthernet 1/0/1
[Switch-GigabitEthernet1/0/1] qos apply policy policy_hostA inbound
[Switch-GigabitEthernet1/0/1] quit
```

##### (3) 针对 Host B 和 Server 配置流量监管

# 定义基本 ACL 3001，对源 IP 地址为 192.168.2.1，目的地址为 192.168.1.1 的报文进行分类。

```
[Switch] acl number 3001
[Switch-acl-adv-3001] rule permit ip source 192.168.2.1 0 destination 192.168.1.1 0
[Switch-acl-adv-3001] quit
```

# 定义基本 ACL 3002，对源 IP 地址为 192.168.1.1，目的地址为 192.168.2.1 的报文进行分类。

```
[Switch] acl number 3002
[Switch-acl-adv-3002] rule permit ip source 192.168.1.1 0 destination 192.168.2.1 0
[Switch-acl-adv-3002] quit
```

# 定义类 classifier\_hostB，匹配基本 ACL 3001。

```
[Switch] traffic classifier classifier_hostB
[Switch-classifier-classifier_hostB] if-match acl 3001
[Switch-classifier-classifier_hostB] quit
```

# 定义类 classifier\_Server，匹配基本 ACL 3002。

```
[Switch] traffic classifier classifier_Server
[Switch-classifier-classifier_Server] if-match acl 3002
[Switch-classifier-classifier_Server] quit
```

# 定义流行为 behavior\_hostB，动作为限制报文的流量为 64kbps。

```
[Switch] traffic behavior behavior_hostB
[Switch-behavior-behavior_hostB] car cir 64
[Switch-behavior-behavior_hostB] quit
```

# 定义流行为 behavior\_Server，动作为限制报文的流量为 64kbps。

```
[Switch] traffic behavior behavior_Server
[Switch-behavior-behavior_Server] car cir 64
[Switch-behavior-behavior_Server] quit
```

# 定义策略 policy\_hostB，为类 classifier\_hostB 指定流行为 behavior\_hostB。

```
[Switch] qos policy policy_hostB
[Switch-qospolicy-policy_hostB] classifier classifier_hostB behavior behavior_hostB
[Switch-qospolicy-policy_hostB] quit
```

# 定义策略 policy\_Server，为类 classifier\_Server 指定流行为 behavior\_Server。

```
[Switch] qos policy policy_Server
[Switch-qospolicy-policy_Server] classifier classifier_Server behavior behavior_Server
[Switch-qospolicy-policy_Server] quit
```

# 将策略 policy\_hostB 和 policy\_Server 分别应用到端口 GigabitEthernet 1/0/2 的入方向和出方向上。

```
[Switch] interface GigabitEthernet 1/0/2
[Switch-GigabitEthernet1/0/2] qos apply policy policy_hostB inbound
[Switch-GigabitEthernet1/0/2] qos apply policy policy_Server outbound
```

### 1.1.5 完整配置

```
#
traffic classifier classifier_hostA operator and
if-match acl 2000
traffic classifier classifier_hostB operator and
if-match acl 3001
traffic classifier classifier_Server operator and
if-match acl 3002
#
traffic behavior behavior_Server
car cir 64 cbs 4000 ebs 4000 green pass red discard yellow pass
traffic behavior behavior_hostA
car cir 320 cbs 4000 ebs 4000 green pass red discard yellow pass
traffic behavior behavior_hostB
car cir 64 cbs 4000 ebs 4000 green pass red discard yellow pass
#
qos policy policy_hostA
classifier classifier_hostA behavior behavior_hostA
qos policy policy_hostB
```

```

classifier classifier_hostB behavior behavior_hostB
qos policy policy_Server
classifier classifier_Server behavior behavior_Server
#
acl number 2000
rule 0 permit source 192.168.1.2 0
#
acl number 3001
rule 0 permit ip source 192.168.2.1 0 destination 192.168.1.1 0
acl number 3002
rule 0 permit ip source 192.168.1.1 0 destination 192.168.2.1 0
#
interface GigabitEthernet1/0/1
qos apply policy policy_hostA inbound
#
interface GigabitEthernet1/0/2
qos apply policy policy_hostB inbound
qos apply policy policy_Server outbound
#
interface GigabitEthernet1/0/3
qos lr outbound cir 640 cbs 40000
#

```

### 1.1.6 配置注意事项

需要注意的是：

- 一个策略可以应用到多个端口上，端口的每个方向（**inbound/outbound**）只能应用一个策略。
- S3610&S5510 系列以太网交换机不支持配置端口限速，用户可以使用 **qos gts** 命令配置流量整形，达到相同的效果。
- S3610&S5510 系列以太网交换机支持在端口或端口组上直接配置流量监管，用户可以使用 **qos car** 命令实现上述功能。
- 在 S5500-EI 系列以太网交换机上应用策略时，**inbound** 和 **outbound** 方向的支持情况和流行为中定义的动作有关，详细情况如下表所示。

表1-2 inbound 和 outbound 方向的支持情况

| 动作                | inbound 方向 | outbound 方向 |
|-------------------|------------|-------------|
| 流量统计              | 支持         | 支持          |
| 流量监管              | 支持         | 支持          |
| 流量过滤              | 支持         | 支持          |
| 流镜像               | 支持         | 支持          |
| 外层 VLAN 标签        | 支持         | 不支持         |
| 重定向               | 支持         | 不支持         |
| 标记报文的用户网络 VLAN ID | 不支持        | 支持          |
| 标记报文的 802.1p 优先级  | 支持         | 支持          |

| 动作                 | inbound 方向 | outbound 方向 |
|--------------------|------------|-------------|
| 标记报文的丢弃优先级         | 支持         | 不支持         |
| 标记报文的 DSCP 优先级     | 支持         | 支持          |
| 标记报文的 IP 优先级       | 支持         | 支持          |
| 标记报文的本地优先级         | 支持         | 不支持         |
| 标记报文的运营商网络 VLAN ID | 支持         | 支持          |



#### 注意

在 S5500-EI 系列以太网交换机上定义流行为时请遵循如下约束，否则策略将不能成功应用：

- **nest** 动作与除 **filter**、**remark dot1p** 以外的其他动作不能同时配置，并且将 **nest** 动作应用到端口/端口组之前必须在端口/端口组上开启基本 QinQ 功能。
- **remark service-vlan-id** 动作应用于入方向（**inbound**）时，与除 **filter**、**remark dot1p** 以外的其他动作不能同时配置。
- **mirror-to** 动作应用于出方向（**outbound**）时，不能与其他动作同时配置。

- 在 S7500E 系列以太网交换机支持将策略应用于端口/端口组、VLAN 和全局。应用策略时，**inbound** 和 **outbound** 方向的支持情况和流行为中定义的动作以及单板的类型有关，详细情况如下表所示。关于单板类型的详细介绍请参见安装手册。

表1-3 inbound 和 outbound 方向的支持情况

| 单板类型              | SC 单板      |             | SA 单板      |             | EA 单板      |             |
|-------------------|------------|-------------|------------|-------------|------------|-------------|
|                   | inbound 方向 | outbound 方向 | inbound 方向 | outbound 方向 | inbound 方向 | outbound 方向 |
| 流量统计              | 支持         | 支持          | 支持         | 不支持         | 支持         | 不支持         |
| 流量监管              | 支持         | 支持          | 支持         | 不支持         | 支持         | 不支持         |
| 流量过滤              | 支持         | 支持          | 支持         | 不支持         | 支持         | 不支持         |
| 流镜像               | 支持         | 支持          | 支持         | 不支持         | 支持         | 不支持         |
| 外层 VLAN 标签        | 支持         | 不支持         | 支持         | 不支持         | 支持         | 不支持         |
| 重定向               | 支持         | 不支持         | 支持         | 不支持         | 支持         | 不支持         |
| 标记报文的用户网络 VLAN ID | 不支持        | 支持          | 不支持        | 不支持         | 不支持        | 不支持         |
| 标记报文的 802.1p 优先级  | 支持         | 支持          | 支持         | 不支持         | 支持         | 不支持         |
| 标记报文的丢弃优先级        | 支持         | 不支持         | 支持         | 不支持         | 支持         | 不支持         |
| 标记报文的 DSCP 优先级    | 支持         | 支持          | 支持         | 不支持         | 支持         | 不支持         |
| 标记报文的 IP 优先级      | 支持         | 支持          | 支持         | 不支持         | 支持         | 不支持         |

| 单板类型               | SC 单板      |             | SA 单板      |             | EA 单板      |             |
|--------------------|------------|-------------|------------|-------------|------------|-------------|
| 动作                 | inbound 方向 | outbound 方向 | inbound 方向 | outbound 方向 | inbound 方向 | outbound 方向 |
| 标记报文的本地优先级         | 支持         | 不支持         | 支持         | 不支持         | 支持         | 不支持         |
| 标记报文的运营商网络 VLAN ID | 支持         | 支持          | 支持         | 不支持         | 支持         | 不支持         |



### 注意

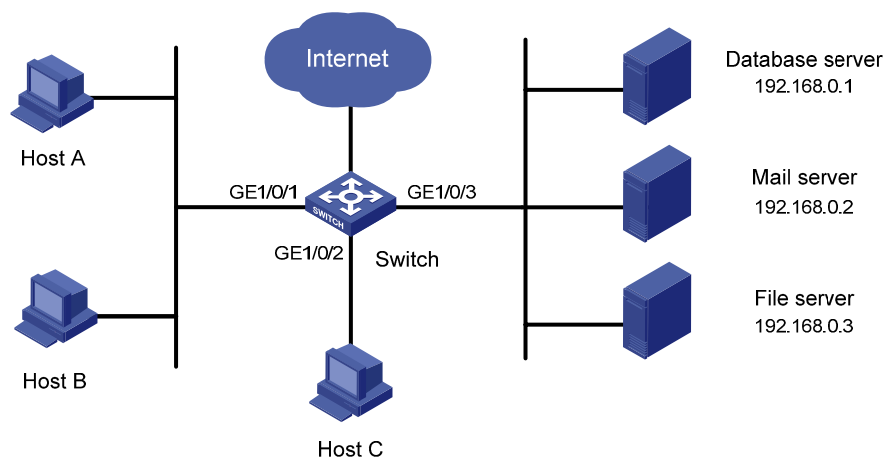
在 S7500E 系列以太网交换机上应用策略时需要注意：

- 包含 **nest**、**remark customer-vlan-id** 和 **remark service-vlan-id** 动作的策略不能应用于 VLAN 或全局。
- **nest** 动作与除 **filter**、**remark dot1p** 以外的其他动作不能同时配置，并且将 **nest** 动作应用到端口/端口组上时必须是在端口/端口组上开启基本 QinQ 功能，否则策略将不能成功应用。
- **remark service-vlan-id** 动作应用于入方向（**inbound**）时，与除 **filter**、**remark dot1p** 以外的其他动作不能同时配置，否则策略将不能成功应用。
- **mirror-to** 动作应用于出方向（**outbound**）时，不能与其他动作同时配置，否则策略将不能成功应用。
- 当某个策略包含的类中定义的分类规则只有 **if-match service-vlan-id** 时，并且流行为中定义的动作只有 **remark customer-vlan-id**（或只有 **remark customer-vlan-id** 和 **remark dot1p**）时，用户可以在 SA 单板和 EA 单板上开启了基本 QinQ 功能的端口的出方向（**outbound**）应用此策略，用来实现 1:1 VLAN Mapping 功能。

## 1.2 优先级重标记和队列调度典型配置指导

### 1.2.1 组网图

图1-2 配置优先级重标记和队列调度组网图



### 1.2.2 应用要求

公司企业网通过交换机（以 S5500-EI 为例）实现互连。网络环境描述如下：

- Host A 和 Host B 通过端口 GigabitEthernet 1/0/1 接入交换机；
- Host C 通过端口 GigabitEthernet 1/0/2 接入交换机；
- 数据库服务器、邮件服务器和文件服务器通过端口 GigabitEthernet 1/0/3 接入交换机。

配置优先级重标记和队列调度，实现如下需求：

- 当 Host A 和 Host B 访问服务器时，交换机优先处理 Host A 和 Host B 访问数据库服务器的报文，其次处理 Host A 和 Host B 访问邮件服务器的报文，最后处理 Host A 和 Host B 访问文件服务器的报文；
- 无论 Host C 访问 Internet 或访问服务器，交换机都优先处理 Host C 发出的报文。

### 1.2.3 适用产品、版本

表1-4 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本                         |
|-------------------|---------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本               | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本               | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本                      |

### 1.2.4 配置过程和解释

(1) 针对 Host A 和 Host B 的配置

# 定义高级 ACL 3000，对目的 IP 地址为 192.168.0.1 的报文进行分类。

```
<Switch> system-view
[Switch] acl number 3000
[Switch-acl-adv-3000] rule permit ip destination 192.168.0.1 0
[Switch-acl-adv-3000] quit
```

# 定义高级 ACL 3001，对目的 IP 地址为 192.168.0.2 的报文进行分类。

```
<Switch> system-view
[Switch] acl number 3001
[Switch-acl-adv-3001] rule permit ip destination 192.168.0.2 0
[Switch-acl-adv-3001] quit
```

# 定义高级 ACL 3002，对目的 IP 地址为 192.168.0.3 的报文进行分类。

```
<Switch> system-view
[Switch] acl number 3002
[Switch-acl-adv-3002] rule permit ip destination 192.168.0.3 0
[Switch-acl-adv-3002] quit
```

# 定义类 classifier\_dbserver，匹配高级 ACL 3000。

```
[Switch] traffic classifier classifier_dbserver
```

```
[Switch-classifier-classifier_dbserver] if-match acl 3000
```

```
[Switch-classifier-classifier_dbserver] quit
```

# 定义类 classifier\_mserver，匹配高级 ACL 3001。

```
[Switch] traffic classifier classifier_mserver
```

```
[Switch-classifier-classifier_mserver] if-match acl 3001
```

```
[Switch-classifier-classifier_mserver] quit
```

# 定义类 classifier\_fserver，匹配高级 ACL 3002。

```
[Switch] traffic classifier classifier_fserver
```

```
[Switch-classifier-classifier_fserver] if-match acl 3002
```

```
[Switch-classifier-classifier_fserver] quit
```

# 定义流行为 behavior\_dbserver，动作为重标记报文的本地优先级为 4。

```
[Switch] traffic behavior behavior_dbserver
```

```
[Switch-behavior-behavior_dbserver] remark local-precedence 4
```

```
[Switch-behavior-behavior_dbserver] quit
```

# 定义流行为 behavior\_mserver，动作为重标记报文的本地优先级为 3。

```
[Switch] traffic behavior behavior_mserver
```

```
[Switch-behavior-behavior_mserver] remark local-precedence 3
```

```
[Switch-behavior-behavior_mserver] quit
```

# 定义流行为 behavior\_fserver，动作为重标记报文的本地优先级为 2。

```
[Switch] traffic behavior behavior_fserver
```

```
[Switch-behavior-behavior_fserver] remark local-precedence 2
```

```
[Switch-behavior-behavior_fserver] quit
```

# 定义策略 policy\_server，为类指定流行为。

```
[Switch] qos policy policy_server
```

```
[Switch-qospolicy-policy_server] classifier classifier_dbserver behavior behavior_dbserver
```

```
[Switch-qospolicy-policy_server] classifier classifier_mserver behavior behavior_mserver
```

```
[Switch-qospolicy-policy_server] classifier classifier_fserver behavior behavior_fserver
```

```
[Switch-qospolicy-policy_server] quit
```

# 将策略 policy\_server 应用到端口 GigabitEthernet 1/0/1 上。

```
[Switch] interface GigabitEthernet 1/0/1
```

```
[Switch-GigabitEthernet1/0/1] qos apply policy policy_server inbound
```

```
[Switch-GigabitEthernet1/0/1] quit
```

# 配置端口 GigabitEthernet 1/0/3 的队列调度方式为 SP（Strict-Priority，严格优先级）。

```
[Switch] interface GigabitEthernet 1/0/3
```

```
[Switch-GigabitEthernet1/0/3] qos sp
```

```
[Switch-GigabitEthernet1/0/3] quit
```

## (2) 针对 Host C 的配置

# 配置端口 GigabitEthernet 1/0/2 的优先级信任模式为信任端口的优先级（缺省情况下即为信任端口的优先级，用户无需配置），并且设置端口的优先级为 5。

```
[Switch] interface GigabitEthernet 1/0/2
```

```
[Switch-GigabitEthernet1/0/2] qos priority 5
```

### 1.2.5 完整配置

```
#
traffic classifier classifier_fserver operator and
if-match acl 3002
traffic classifier classifier_dbserver operator and
if-match acl 3000
traffic classifier classifier_mserver operator and
if-match acl 3001
#
traffic behavior behavior_fserver
remark local-precedence 2
traffic behavior behavior_dbserver
remark local-precedence 4
traffic behavior behavior_mserver
remark local-precedence 3
#
qos policy policy_server
classifier classifier_dbserver behavior behavior_dbserver
classifier classifier_mserver behavior behavior_mserver
classifier classifier_fserver behavior behavior_fserver
#
acl number 3000
rule 0 permit ip destination 192.168.0.1 0
acl number 3001
rule 0 permit ip destination 192.168.0.2 0
acl number 3002
rule 0 permit ip destination 192.168.0.3 0
#
interface GigabitEthernet1/0/1
qos apply policy policy_server inbound
#
interface GigabitEthernet1/0/2
qos priority 5
#
interface GigabitEthernet1/0/3
qos sp
#
```

### 1.2.6 配置注意事项

需要注意的是：

- 在S5500-EI系列以太网交换机上应用策略时，**inbound**和**outbound**方向的支持情况请参见 表 1-2。
- 在S7500E系列以太网交换机上应用策略时，**inbound**和**outbound**方向的支持情况请参见 表 1-3。
- 在 S5500-EI/7500E 系列以太网交换机上应用策略后，如果报文同时匹配了 **inbound** 和 **outbound** 方向上的策略，当动作冲突时，**outbound** 方向上执行的动作会覆盖 **inbound** 方



向上执行的动作，结果将会以 **outbound** 方向上执行的动作为准。例如，报文在进入交换机时匹配到 **inbound** 方向上的策略，动作为 **remark dscp 10**，在离开交换机时匹配到 **outbound** 方向上的策略，动作为 **remark dscp 40**，最终报文的 DSCP 优先级为 40。

- S5500-SI/S5500-EI/S7500E 系列以太网交换机的端口支持 8 个输出队列，用户可以根据需要配置端口上的部分队列使用 SP（Strict-Priority，严格优先级）调度算法，部分队列使用 WRR（Weighted Round Robin，加权轮询）调度算法。通过将端口上的队列分别加入 SP 调度组和 WRR 调度组（即 group 1），实现 SP+WRR 的调度功能。在队列调度时，系统会优先保证 SP 调度组内的队列调度，当 SP 调度组内的队列中没有报文发送时，才会调度 WRR 调度组内的队列。SP 调度组内各个队列执行严格优先级调度方式，WRR 调度组内各个队列执行加权轮询调度方式。
- S3610&S5510 系列以太网交换机的端口支持 8 个输出队列，用户可以根据需要配置端口上的部分队列使用 SP 调度算法，部分队列使用 WRR 调度算法。通过将端口上的队列分别加入 SP 调度组和 WRR 调度组，实现 SP+WRR 的调度功能。进行队列调度时，各个组之间的调度方式为 SP，即比较各组中包含的最大队列编号，优先调度最大队列编号所在的组。例如，将队列 5、6、7 划分到 SP 调度组，将队列 2、3、4 划分到 WRR 调度组 1，将队列 0、1 划分到 WRR 调度组 2。经过比较，SP 调度组包含的最大队列编号为 7，WRR 调度组 1 包含的最大队列编号为 4，WRR 调度组 2 包含的最大队列编号为 1，因此交换机首先对 SP 组进行严格优先级调度；SP 组中的队列没有报文发送时，才在 WRR 组 1 中进行轮询调度；最后才会在 WRR 组 2 中进行轮询调度。
- 在 S3610&S5510 系列以太网交换机上配置使用 WRR 或 SP+WRR 队列调度算法时，必须将连续的队列划分到同一个调度组内。
- 缺省情况下，S5500-SI/S5500-EI 系列以太网交换机的所有端口采用 WRR 调度算法，队列 0～7 的权重分别为 1、2、3、4、5、9、13、15。
- 缺省情况下，S3610&S5510/S7500E 系列以太网交换机的所有端口采用 SP 调度算法。
- S3610&S5510 系列以太网交换机支持在端口或端口组上配置拥塞避免（WRED）功能，用户可以使用 **qos wred enable** 命令实现上述功能。
- 配置 **remark** 动作时，各产品支持的可重标记的优先级类型有所不同，具体情况如下表所示。

表1-5 各产品对 remark 动作的支持情况

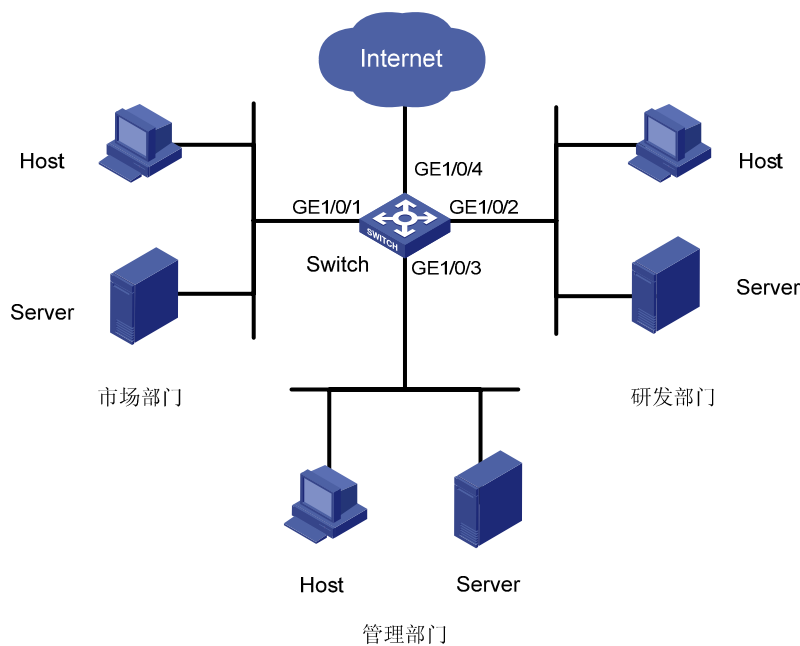
| 产品                | 说明                                                                                                                                                                                                                                         |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| S3610 系列以太网交换机    | 支持重标记报文的 802.1p 优先级（ <b>dot1p</b> ）、丢弃优先级（ <b>drop-precedence</b> ）、DSCP 优先级（ <b>dscp</b> ）、IP 优先级（ <b>ip-precedence</b> ）、本地优先级（ <b>local-precedence</b> ）和运营商网络 VLAN ID（ <b>service-vlan-id</b> ）                                        |
| S5510 系列以太网交换机    | 支持重标记报文的 802.1p 优先级（ <b>dot1p</b> ）、丢弃优先级（ <b>drop-precedence</b> ）、DSCP 优先级（ <b>dscp</b> ）、IP 优先级（ <b>ip-precedence</b> ）、本地优先级（ <b>local-precedence</b> ）和运营商网络 VLAN ID（ <b>service-vlan-id</b> ）                                        |
| S5500-SI 系列以太网交换机 | 支持重标记报文的 802.1p 优先级（ <b>dot1p</b> ）、DSCP 优先级（ <b>dscp</b> ）、IP 优先级（ <b>ip-precedence</b> ）和本地优先级（ <b>local-precedence</b> ）                                                                                                                |
| S5500-EI 系列以太网交换机 | 支持重标记报文的用户网络 VLAN ID（ <b>customer-vlan-id</b> ）、802.1p 优先级（ <b>dot1p</b> ）、丢弃优先级（ <b>drop-precedence</b> ）、DSCP 优先级（ <b>dscp</b> ）、IP 优先级（ <b>ip-precedence</b> ）、本地优先级（ <b>local-precedence</b> ）和运营商网络 VLAN ID（ <b>service-vlan-id</b> ） |

| 产品              | 说明                                                                                                                                                                                                                                         |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| S7500E 系列以太网交换机 | 支持重标记报文的用户网络 VLAN ID（ <b>customer-vlan-id</b> ）、802.1p 优先级（ <b>dot1p</b> ）、丢弃优先级（ <b>drop-precedence</b> ）、DSCP 优先级（ <b>dscp</b> ）、IP 优先级（ <b>ip-precedence</b> ）、本地优先级（ <b>local-precedence</b> ）和运营商网络 VLAN ID（ <b>service-vlan-id</b> ） |

## 1.3 优先级映射和队列调度典型配置指导

### 1.3.1 组网图

图1-3 配置优先级映射和队列调度组网图



### 1.3.2 应用要求

公司企业网通过交换机（以 S5500-EI 为例）实现各部门之间的互连。网络环境描述如下：

- 市场部门通过端口 GigabitEthernet 1/0/1 接入交换机；
- 研发部门通过端口 GigabitEthernet 1/0/2 接入交换机；
- 管理部门通过端口 GigabitEthernet 1/0/3 接入交换机；
- 市场部门、研发部门和管理部门内的设备发出的报文都不带有 802.1Q 标签头（VLAN Tag）。

要求配置优先级映射和队列调度，实现如下需求：

- 标记市场部门发出的报文的 802.1p 优先级为 3，通过优先级映射，将此类报文放入队列 4 中；
- 标记研发部门发出的报文的 802.1p 优先级为 4，通过优先级映射，将此类报文放入队列 3 中；
- 标记管理部门发出的报文的 802.1p 优先级为 5，通过优先级映射，将此类报文放入队列 6 中；
- 在端口 GigabitEthernet 1/0/4 上配置调度算法为 WRR，队列 3、4 和 6 所占的权重分别为 5、10 和 15。

### 1.3.3 适用产品、版本

表1-6 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本                         |
|-------------------|---------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本               | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本               | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本                      |

### 1.3.4 配置过程和解释

(1) 配置端口的端口优先级

# 配置端口 GigabitEthernet 1/0/1 的端口优先级为 3。

```
<Switch> system-view
[Switch] interface GigabitEthernet 1/0/1
[Switch-GigabitEthernet1/0/1] qos priority 3
[Switch-GigabitEthernet1/0/1] quit
```

# 配置端口 GigabitEthernet 1/0/2 的端口优先级为 4。

```
[Switch] interface GigabitEthernet 1/0/2
[Switch-GigabitEthernet1/0/2] qos priority 4
[Switch-GigabitEthernet1/0/2] quit
```

# 配置端口 GigabitEthernet 1/0/3 的端口优先级为 5。

```
[Switch] interface GigabitEthernet 1/0/3
[Switch-GigabitEthernet1/0/3] qos priority 5
[Switch-GigabitEthernet1/0/3] quit
```

(2) 配置优先级映射表

# 配置 802.1p 优先级到本地优先级映射表, 将 802.1p 优先级 3、4、5 对应的本地优先级配置为 4、3、6。

```
[Switch] qos map-table dot1p-lp
[Switch-maptbl-dot1p-lp] import 3 export 4
[Switch-maptbl-dot1p-lp] import 4 export 3
[Switch-maptbl-dot1p-lp] import 5 export 6
[Switch-maptbl-dot1p-lp] quit
```

(3) 配置队列调度

# 配置端口 GigabitEthernet 1/0/4 的队列调度算法为 WRR, 队列 3、4 和 6 所占的权重分别为 5、10 和 15。

```
[Switch] interface GigabitEthernet 1/0/4
```

```
[Switch-GigabitEthernet1/0/4] qos wrr 3 group 1 weight 5
[Switch-GigabitEthernet1/0/4] qos wrr 4 group 1 weight 10
[Switch-GigabitEthernet1/0/4] qos wrr 6 group 1 weight 15
```

### 1.3.5 完整配置

```
#
qos map-table dot1p-lp
import 3 export 4
import 4 export 3
import 5 export 6
#
interface GigabitEthernet1/0/1
qos priority 3
#
interface GigabitEthernet1/0/2
qos priority 4
#
interface GigabitEthernet1/0/3
qos priority 5
#
interface GigabitEthernet1/0/4
qos wrr 3 group 1 weight 5
qos wrr 4 group 1 weight 10
qos wrr 6 group 1 weight 15
#
```

### 1.3.6 配置注意事项

关于各产品支持的队列调度算法的具体情况，请参见 1.2.6 中的说明。

在 S3610/S5510 系列以太网交换机上配置优先级映射时需要注意：

- 对于不带有 802.1Q 标签头的报文，交换机将使用端口的优先级作为该端口接收的报文的本地优先级。
- 对于带有 802.1Q 标签头的报文，交换机提供两种优先级信任模式：信任报文的优先级（根据报文的 802.1p 优先级，查找 802.1p 优先级到本地优先级/丢弃优先级映射表，然后为报文标记本地优先级和丢弃优先级）和信任端口的优先级（使用接收端口的端口优先级作为本地优先级）。
- S3610/S5510 系列以太网交换机提供的 802.1p 优先级到本地优先级/丢弃优先级的映射关系缺省取值如下表所示。

表1-7 dot1p-lp, dot1p-dp 缺省映射关系

| 映射输入索引            | dot1p-lp 映射 | dot1p-dp 映射 |
|-------------------|-------------|-------------|
| 802.1p 优先级(dot1p) | 本地优先级 (lp)  | 丢弃优先级(dp)   |
| 0                 | 2           | 0           |
| 1                 | 0           | 0           |
| 2                 | 1           | 0           |

| 映射输入索引 | dot1p-lp 映射 | dot1p-dp 映射 |
|--------|-------------|-------------|
| 3      | 3           | 0           |
| 4      | 4           | 0           |
| 5      | 5           | 0           |
| 6      | 6           | 0           |
| 7      | 7           | 0           |

- S3610/S5510 系列以太网交换机还提供了 DSCP 优先级到本地优先级/丢弃优先级/802.1p 优先级/DSCP 优先级的映射表，分别对应相应的优先级映射关系，各个映射表的缺省关系取值如下表所示。

表1-8 dscp-lp, dscp-dp, dscp-dot1p, dscp-dscp 缺省映射关系

| 映射输入索引   | dscp-lp 映射 | dscp-dp 映射 | dscp-dot1p 映射     | dscp-dscp 映射 |
|----------|------------|------------|-------------------|--------------|
| DSCP 优先级 | 本地优先级(lp)  | 丢弃优先级(dp)  | 802.1p 优先级(dot1p) | DSCP 优先级     |
| 0~7      | 0          | 0          | 0                 | 0            |
| 8~15     | 1          | 0          | 1                 | 8            |
| 16~23    | 2          | 0          | 2                 | 16           |
| 24~31    | 3          | 0          | 3                 | 24           |
| 32~39    | 4          | 0          | 4                 | 32           |
| 40~47    | 5          | 0          | 5                 | 40           |
| 48~55    | 6          | 0          | 6                 | 48           |
| 56~63    | 7          | 0          | 7                 | 56           |



#### 注意

- 802.1p 优先级到本地优先级/丢弃优先级映射表和端口上的优先级信任模式相关联。配置了端口上的信任模式为信任报文的 802.1p 优先级后，这些映射表才能起作用。
- DSCP 优先级映到本地优先级/丢弃优先级/802.1p 优先级/DSCP 优先级映射表和流行为中 **primap** 动作相关联。在流行为中配置了 **primap** 动作后，这些映射表才能起作用。

在 S5500-SI 系列以太网交换机上配置优先级映射时需要注意：

- 对于不带有 802.1Q 标签头的报文，交换机将使用端口的优先级作为该端口接收的报文的 802.1p 优先级，然后根据此优先级查找 802.1p 优先级到本地优先级映射表，然后为报文标记本地优先级。
- 对于带有 802.1Q 标签头的报文，交换机将根据报文的 802.1p 优先级，查找 802.1p 优先级到本地优先级映射表，然后为报文标记本地优先级。
- S5500-SI 系列以太网交换机提供的 802.1p 优先级到本地优先级的映射关系缺省取值如下表所示。

表1-9 dot1p-lp 缺省映射关系

| 802.1p 优先级(dot1p) | 本地优先级 (lp) |
|-------------------|------------|
| 0                 | 2          |
| 1                 | 0          |
| 2                 | 1          |
| 3                 | 3          |
| 4                 | 4          |
| 5                 | 5          |
| 6                 | 6          |
| 7                 | 7          |



注意

S5500-SI 系列以太网交换机不支持编辑 802.1p 优先级到本地优先级（dot1p-lp）映射表。

在 S5500-EI/S7500E 系列以太网交换机上配置优先级映射时需要注意：

- S5500-EI/S7500E 系列以太网交换机提供两种优先级信任模式：信任报文的 DSCP 优先级和信任报文的 802.1p 优先级。
- 信任报文的 DSCP 优先级：根据报文的 DSCP 优先级，查找 DSCP 优先级到 802.1p 优先级/丢弃优先级/DSCP 优先级映射表，为报文标记 802.1p 优先级、丢弃优先级和新的 DSCP 优先级。然后再根据 802.1p 优先级查找 802.1p 优先级到本地优先级映射表，为报文标记本地优先级。
- 信任报文的 802.1p 优先级：对于不带有 802.1Q 标签头的报文，交换机将使用端口的优先级作为该端口接收的报文的 802.1p 优先级，然后根据此优先级查找 802.1p 优先级到本地优先级/丢弃优先级映射表，然后为报文标记本地优先级和丢弃优先级；对于带有 802.1Q 标签头的报文，根据报文的 802.1p 优先级，查找 802.1p 优先级到本地优先级/丢弃优先级映射表，然后为报文标记本地优先级和丢弃优先级。
- S5500-EI/S7500E 系列以太网交换机提供的 802.1p 优先级到本地优先级/丢弃优先级、DSCP 优先级到 802.1p 优先级/丢弃优先级/DSCP 优先级的映射关系缺省取值如下表所示。

表1-10 dot1p-lp,dot1p-dp 缺省映射关系

| 映射输入索引            | dot1p-lp 映射 | dot1p-dp 映射 |
|-------------------|-------------|-------------|
| 802.1p 优先级(dot1p) | 本地优先级 (lp)  | 丢弃优先级(dp)   |
| 0                 | 2           | 0           |
| 1                 | 0           | 0           |
| 2                 | 1           | 0           |
| 3                 | 3           | 0           |
| 4                 | 4           | 0           |
| 5                 | 5           | 0           |
| 6                 | 6           | 0           |

| 映射输入索引 | dot1p-ip 映射 | dot1p-dp 映射 |
|--------|-------------|-------------|
| 7      | 7           | 0           |

表1-11 dscp-dp, dscp-dot1p, dscp-dscp 缺省映射关系

| 映射输入索引   | dscp-dp 映射 | dscp-dot1p 映射     | dscp-dscp 映射 |
|----------|------------|-------------------|--------------|
| DSCP 优先级 | 丢弃优先级(dp)  | 802.1p 优先级(dot1p) | DSCP 优先级     |
| 0~7      | 0          | 0                 | 0            |
| 8~15     | 0          | 1                 | 8            |
| 16~23    | 0          | 2                 | 16           |
| 24~31    | 0          | 3                 | 24           |
| 32~39    | 0          | 4                 | 32           |
| 40~47    | 0          | 5                 | 40           |
| 48~55    | 0          | 6                 | 48           |
| 56~63    | 0          | 7                 | 56           |

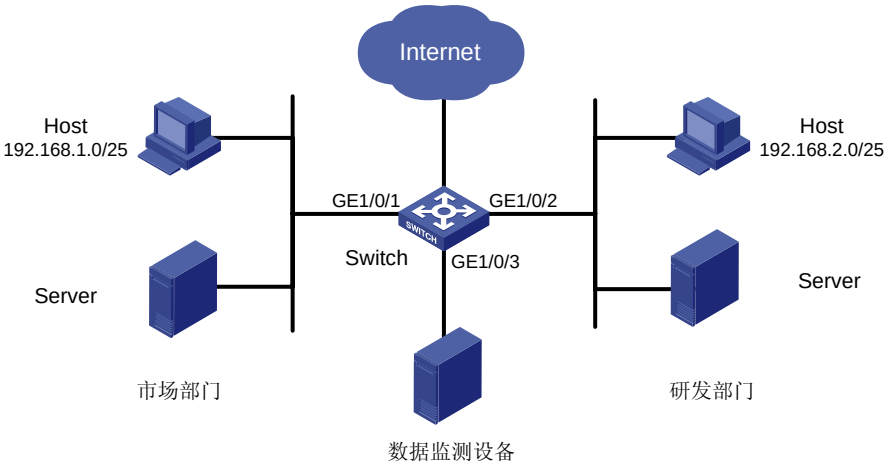
 注意

在 S5500-EI/S7500E 系列以太网交换机上配置 DSCP 优先级与丢弃优先级的映射关系时，不支持将 DSCP 优先级映射为丢弃优先级 1。

1.4 流镜像和重定向至端口典型配置指导

1.4.1 组网图

图1-4 配置流镜像和重定向至端口组网图



1.4.2 应用要求

公司企业网通过交换机（以 S5500-EI 为例）实现各部门之间的互连。网络环境描述如下：

- 市场部门通过端口 GigabitEthernet 1/0/1 接入交换机,其中 Host 的 IP 地址为 192.168.1.0/25,通过交换机访问 Internet;
- 研发部门通过端口 GigabitEthernet 1/0/2 接入交换机,其中 Host 的 IP 地址为 192.168.2.0/25,通过交换机访问 Internet;
- 数据监测设备通过端口 GigabitEthernet 1/0/3 接入交换机。

配置流镜像和重定向,实现如下需求:

- 在工作时间段(8:00 至 18:00)内,将市场部门内 Host 访问 Internet 的流量镜像到数据监测设备;
- 在工作时间段(8:00 至 18:00)内,将研发部门内 Host 访问 Internet 的流量重定向到数据监测设备。

网络管理员可以使用数据监测设备对各部门访问 Internet 的流量进行分析。

### 1.4.3 适用产品、版本

表1-12 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本                         |
|-------------------|---------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本               | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本               | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本                      |

### 1.4.4 配置过程和解释

#### (1) 定义工作时间段

# 定义 8:00 至 18:00 的周期时间段。

```
<Switch> system-view
[Switch] time-range trname 8:00 to 18:00 working-day
```

#### (2) 定义针对市场部门的策略

# 定义基本 ACL 2000, 对市场部门内的 Host 进行分类。

```
[Switch] acl number 2000
[Switch-acl-basic-2000] rule permit source 192.168.1.0 0.0.0.127 time-range trname
[Switch-acl-basic-2000] quit
```

# 定义类 classifier\_market, 匹配基本 ACL 2000。

```
[Switch] traffic classifier classifier_market
[Switch-classifier-classifier_market] if-match acl 2000
[Switch-classifier-classifier_market] quit
```



# 定义流行为 behavior\_market，动作为流镜像至端口 GigabitEthernet 1/0/3。

```
[Switch] traffic behavior behavior_market
[Switch-behavior-behavior_market] mirror-to interface GigabitEthernet 1/0/3
[Switch-behavior-behavior_market] quit
```

# 定义策略 policy\_market，为类 classifier\_market 指定流行为 behavior\_market。

```
[Switch] qos policy policy_market
[Switch-qospolicy-policy_market] classifier classifier_market behavior behavior_market
[Switch-qospolicy-policy_market] quit
```

### (3) 定义针对研发部门的策略

# 定义基本 ACL 2001，对研发部门内的 Host 进行分类。

```
[Switch] acl number 2001
[Switch-acl-basic-2001] rule permit source 192.168.2.0 0.0.0.127 time-range trname
[Switch-acl-basic-2001] quit
```

# 定义类 classifier\_rd，匹配基本 ACL 2001。

```
[Switch] traffic classifier classifier_rd
[Switch-classifier-classifier_rd] if-match acl 2001
[Switch-classifier-classifier_rd] quit
```

# 定义流行为 behavior\_rd，动作为重定向至端口 GigabitEthernet 1/0/3。

```
[Switch] traffic behavior behavior_rd
[Switch-behavior-behavior_rd] redirect interface GigabitEthernet 1/0/3
[Switch-behavior-behavior_rd] quit
```

# 定义策略 policy\_rd，为类 classifier\_rd 指定流行为 behavior\_rd。

```
[Switch] qos policy policy_rd
[Switch-qospolicy-policy_rd] classifier classifier_rd behavior behavior_rd
[Switch-qospolicy-policy_rd] quit
```

### (4) 应用策略

# 将策略 policy\_market 应用到端口 GigabitEthernet 1/0/1 上。

```
[Switch] interface GigabitEthernet 1/0/1
[Switch-GigabitEthernet1/0/1] qos apply policy policy_market inbound
[Switch-GigabitEthernet1/0/1] quit
```

# 将策略 policy\_rd 应用到端口 GigabitEthernet 1/0/2 上。

```
[Switch] interface GigabitEthernet 1/0/2
[Switch-GigabitEthernet1/0/2] qos a policy policy_rd inbound
```

## 1.4.5 完整配置

```
#
traffic classifier classifier_market operator and
if-match acl 2000
traffic classifier classifier_rd operator and
if-match acl 2001
#
traffic behavior behavior_market
mirror-to interface GigabitEthernet1/0/3
```

```

traffic behavior behavior_rd
 redirect interface GigabitEthernet1/0/3
#
qos policy policy_market
 classifier classifier_market behavior behavior_market
qos policy policy_rd
 classifier classifier_rd behavior behavior_rd
#
time-range trname 08:00 to 18:00 working-day
#
acl number 2000
 rule 0 permit source 192.168.1.0 0.0.0.127 time-range trname
acl number 2001
 rule 0 permit source 192.168.2.0 0.0.0.127 time-range trname
#
interface GigabitEthernet1/0/1
 qos apply policy policy_market inbound
#
interface GigabitEthernet1/0/2
 qos apply policy policy_rd inbound
#

```

#### 1.4.6 配置注意事项

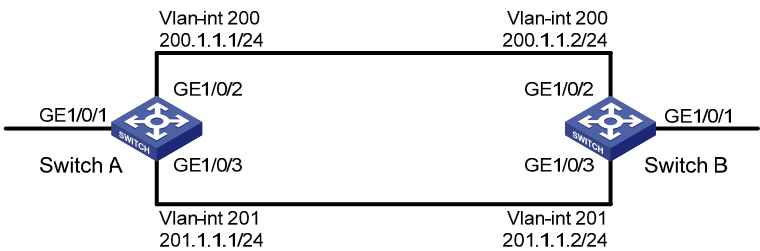
需要注意的是：

- 在S5500-EI系列以太网交换机上应用策略时，**inbound**和**outbound**方向的支持情况请参见 表 1-2。
- 在S7500E系列以太网交换机上应用策略时，**inbound**和**outbound**方向的支持情况请参见 表 1-3。
- 在 S5500-EI/S7500E 系列以太网交换机上配置 **mirror-to** 动作应用于出方向(**outbound**)时，不能与其他动作同时配置，否则策略将不能成功应用。
- 在 S3610&S5510 系列以太网交换机上，流镜像的目的端口不能为聚合组成员端口。
- 在 S3610&S5510 系列以太网交换机上同时配置本地端口镜像和流镜像时，本地端口镜像的目的端口和流镜像的目的端口必须为同一个端口。
- S3610&S5510 系列以太网交换机只支持配置一个流镜像目的端口，S5500-SI/S5500-EI/S7500E 系列以太网交换机支持配置多个流镜像目的端口。

# 1.5 重定向至下一跳典型配置指导

## 1.5.1 组网图

图1-5 配置重定向至下一跳组网图



## 1.5.2 应用要求

某网络环境描述如下：

- 交换机 Switch A 通过两条链路与 Switch B 连接，同时 Switch A 和 Switch B 各自连接其他的设备；
- Switch A 上的端口 GigabitEthernet 1/0/2 和 Switch B 上的端口 GigabitEthernet 1/0/2 属于 VLAN 200；
- Switch A 上的端口 GigabitEthernet 1/0/3 和 Switch B 上的端口 GigabitEthernet 1/0/3 属于 VLAN 201；
- Switch A 上 VLAN 200 虚接口的 IP 地址为 200.1.1.1，VLAN 201 虚接口的 IP 地址为 201.1.1.1；Switch B 上 VLAN 200 虚接口的 IP 地址为 200.1.1.2，VLAN 201 虚接口的 IP 地址为 201.1.1.2。

配置重定向至下一跳，实现策略路由功能，满足如下需求：

- 将 Switch A 的端口 GigabitEthernet 1/0/1 接收到的源 IP 地址为 2.1.1.1 的报文转发至 200.1.1.2；
- 将 Switch A 的端口 GigabitEthernet 1/0/1 接收到的源 IP 地址为 2.1.1.2 的报文转发至 201.1.1.2；
- 对于 Switch A 的端口 GigabitEthernet 1/0/1 接收到的其它报文，按照查找路由表的方式进行转发。

## 1.5.3 适用产品、版本

表1-13 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本                         |
|-------------------|---------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本               | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本               | S5500-20TP-SI                |

| 产品                | 软件版本                            | 硬件版本    |
|-------------------|---------------------------------|---------|
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本 |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本 |

#### 1.5.4 配置过程和解释

配置 Switch A

# 定义基本 ACL 2000，对源 IP 地址为 2.1.1.1 的报文进行分类。

```
<Switch> system-view
[Switch] acl number 2000
[Switch-acl-basic-2000] rule permit source 2.1.1.1 0
[Switch-acl-basic-2000] quit
```

# 定义基本 ACL 2001，对源 IP 地址为 2.1.1.2 的报文进行分类。

```
[Switch] acl number 2001
[Switch-acl-basic-2001] rule permit source 2.1.1.2 0
[Switch-acl-basic-2001] quit
```

# 定义类 classifier\_1，匹配基本 ACL 2000。

```
[Switch] traffic classifier classifier_1
[Switch-classifier-classifier_1] if-match acl 2000
[Switch-classifier-classifier_1] quit
```

# 定义流行为 behavior\_1，动作为重定向至 200.1.1.2。

```
[Switch] traffic behavior behavior_1
[Switch-behavior-behavior_1] redirect next-hop 200.1.1.2
[Switch-behavior-behavior_1] quit
```

# 定义类 classifier\_2，匹配基本 ACL 2001。

```
[Switch] traffic classifier classifier_2
[Switch-classifier-classifier_2] if-match acl 2001
[Switch-classifier-classifier_2] quit
```

# 定义流行为 behavior\_2，动作为重定向至 201.1.1.2。

```
[Switch] traffic behavior behavior_2
[Switch-behavior-behavior_2] redirect next-hop 201.1.1.2
[Switch-behavior-behavior_2] quit
```

# 定义策略 policy，为类 classifier\_1 指定流行为 behavior\_1，为类 classifier\_2 指定流行为 behavior\_2。

```
[Switch] qos policy policy
[Switch-qospolicy-policy] classifier classifier_1 behavior behavior_1
[Switch-qospolicy-policy] classifier classifier_2 behavior behavior_2
[Switch-qospolicy-policy] quit
```

# 将策略 policy 应用到端口 GigabitEthernet 1/0/1 的入方向上。

```
[Switch] interface GigabitEthernet 1/0/1
[Switch-GigabitEthernet1/0/1] qos apply policy policy inbound
```

### 1.5.5 完整配置

```
#
traffic classifier classifier_1 operator and
if-match acl 2000
traffic classifier classifier_2 operator and
if-match acl 2001
#
traffic behavior behavior_1
redirect next-hop 200.1.1.2
traffic behavior behavior_2
redirect next-hop 201.1.1.2
#
qos policy policy
classifier classifier_1 behavior behavior_1
classifier classifier_2 behavior behavior_2
#
acl number 2000
rule 0 permit source 2.1.1.1 0
acl number 2001
rule 0 permit source 2.1.1.2 0
#
interface GigabitEthernet1/0/1
qos apply policy policy inbound
#
```

### 1.5.6 配置注意事项

需要注意的是：

- 在S5500-EI系列以太网交换机上应用策略时，**inbound**和**outbound**方向的支持情况请参见 表 1-2。
- 在S7500E系列以太网交换机上应用策略时，**inbound**和**outbound**方向的支持情况请参见 表 1-3。
- 用户可以根据实际情况需要配置策略路由。与单纯依照 IP 报文的目的地址查找路由表进行转发不同，策略路由基于到达报文的源地址等信息灵活地进行路由选择。
- 策略路由的优先级要高于普通路由，即报文首先按照策略路由进行转发。如果无法匹配所有的策略路由条件，再按照普通路由进行转发。

# 目 录

|                             |      |
|-----------------------------|------|
| 1 端口镜像典型配置指导.....           | 1-1  |
| 1.1 本地端口镜像典型配置指导 .....      | 1-1  |
| 1.1.1 组网图 .....             | 1-1  |
| 1.1.2 应用要求 .....            | 1-1  |
| 1.1.3 适用产品、版本 .....         | 1-1  |
| 1.1.4 配置过程和解释 .....         | 1-2  |
| 1.1.5 完整配置 .....            | 1-2  |
| 1.1.6 配置注意事项 .....          | 1-2  |
| 1.2 远程端口镜像典型配置指导（方式一） ..... | 1-3  |
| 1.2.1 组网图 .....             | 1-3  |
| 1.2.2 应用要求 .....            | 1-4  |
| 1.2.3 适用产品、版本 .....         | 1-4  |
| 1.2.4 配置过程和解释 .....         | 1-4  |
| 1.2.5 完整配置 .....            | 1-5  |
| 1.2.6 配置注意事项 .....          | 1-6  |
| 1.3 远程端口镜像典型配置指导（方式二） ..... | 1-7  |
| 1.3.1 组网图 .....             | 1-8  |
| 1.3.2 应用要求 .....            | 1-8  |
| 1.3.3 适用产品、版本 .....         | 1-8  |
| 1.3.4 配置过程和解释 .....         | 1-9  |
| 1.3.5 完整配置 .....            | 1-10 |
| 1.3.6 配置注意事项 .....          | 1-11 |

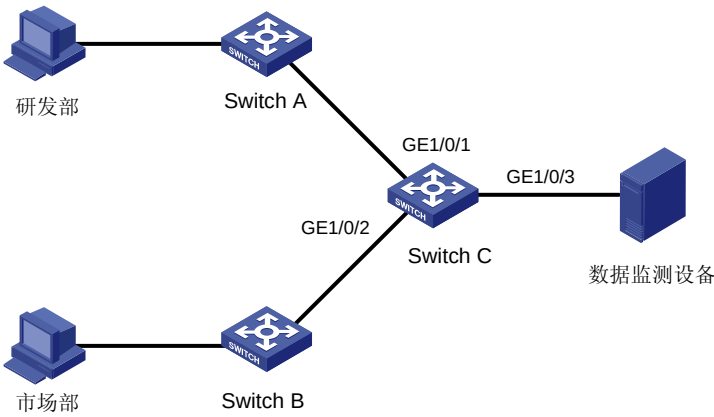
# 1 端口镜像典型配置指导

## 1.1 本地端口镜像典型配置指导

本地端口镜像是指将设备的一个或多个端口（源端口）的报文复制到本设备的一个监视端口（目的端口），用于报文的监视和分析。其中，源端口和目的端口必须在同一台设备上。

### 1.1.1 组网图

图1-1 配置本地端口镜像组网图



### 1.1.2 应用要求

某公司内部通过交换机（以S5500-EI系列以太网交换机为例，如图1-1中Switch C）实现各部门之间的互连，网络环境描述如下：

- 研发部通过端口 GigabitEthernet 1/0/1 接入 Switch C；
- 市场部通过端口 GigabitEthernet 1/0/2 接入 Switch C；
- 数据监测设备连接在 Switch C 的 GigabitEthernet 1/0/3 端口上。

网络管理员希望通过数据监测设备对研发部和市场部收发的报文进行监控。

使用本地端口镜像功能实现该需求，在 Switch C 上进行如下配置：

- 端口 GigabitEthernet 1/0/1 和 GigabitEthernet 1/0/2 为镜像源端口；
- 连接数据监测设备的端口 GigabitEthernet 1/0/3 为镜像目的端口。

### 1.1.3 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本                         |
|-------------------|---------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本               | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本               | S5500-20TP-SI                |

| 产品                | 软件版本                            | 硬件版本    |
|-------------------|---------------------------------|---------|
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本 |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本 |

#### 1.1.4 配置过程和解释

# 创建本地镜像组。

```
<SwitchC> system-view
```

```
[SwitchC] mirroring-group 1 local
```

# 为本地镜像组配置源端口和目的端口。

```
[SwitchC] mirroring-group 1 mirroring-port GigabitEthernet 1/0/1 GigabitEthernet 1/0/2 both
```

```
[SwitchC] mirroring-group 1 monitor-port GigabitEthernet 1/0/3
```

# 显示所有镜像组的配置信息。

```
[SwitchC] display mirroring-group all
```

```
mirroring-group 1:
```

```
type: local
```

```
status: active
```

```
mirroring port:
```

```
GigabitEthernet1/0/1 both
```

```
GigabitEthernet1/0/2 both
```

```
monitor port: GigabitEthernet1/0/3
```

#### 1.1.5 完整配置

```
#
```

```
mirroring-group 1 local
```

```
#
```

```
interface GigabitEthernet1/0/1
```

```
mirroring-group 1 mirroring-port both
```

```
#
```

```
interface GigabitEthernet1/0/2
```

```
mirroring-group 1 mirroring-port both
```

```
#
```

```
interface GigabitEthernet1/0/3
```

```
mirroring-group 1 monitor-port
```

```
#
```

#### 1.1.6 配置注意事项

需要注意的是：

- 镜像后的报文是否带有 VLAN Tag，不同的产品有所不同，请以各产品的实际情况为准。
- 配置本地端口镜像时，必须预先创建本地镜像组。
- 本地镜像组需要配置源端口、目的端口才能生效。其中源端口和目的端口不能是现有镜像组的成员端口，并且一个镜像组只能配置一个目的端口。
- 请用户不要在目的端口上开启 STP、RSTP 或 MSTP，否则可能会影响镜像功能的正常使用。
- 目的端口不用做其他用途，仅用于端口镜像。



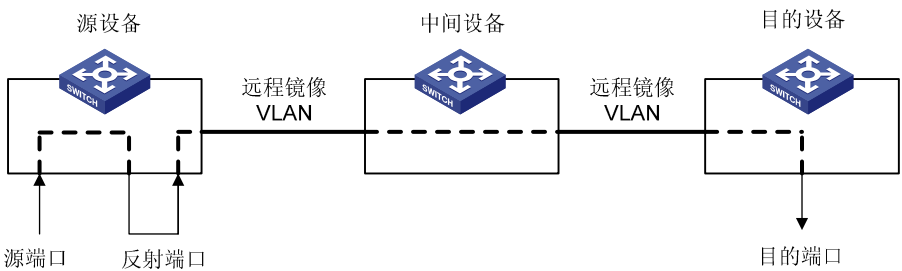
- S3610&S5510 系列以太网交换机只支持配置 1 个本地镜像组，S5500-SI/S5500-EI/S7500E 系列以太网交换机均支持 4 个本地镜像组。
- 在 S3610&S5510 系列以太网交换机上配置本地端口镜像时，目的端口不能为聚合组成员端口。

## 1.2 远程端口镜像典型配置指导（方式一）

远程端口镜像（方式一）通过远程源镜像组和远程目的镜像组互相配合的方式实现。

远程端口镜像（方式一）的应用如图 1-2 所示。

图1-2 远程端口镜像（方式一）应用示意图

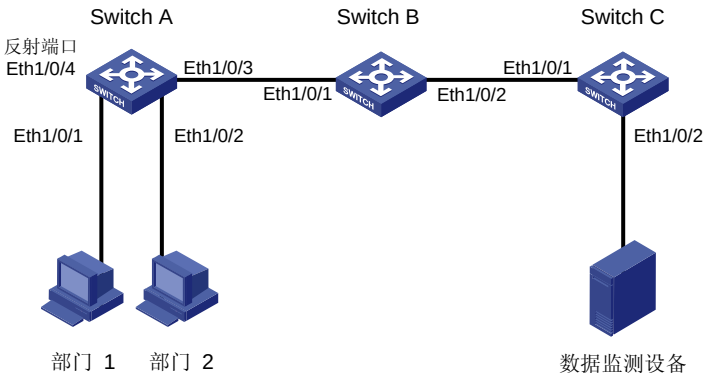


图中各设备的作用如下：

- 源设备：源端口所在的设备，用户需要在源设备上创建远程源镜像组。本设备负责将源端口的报文复制一份，然后通过反射端口将报文在远程镜像 VLAN 中进行广播，传输给中间设备或目的设备。
- 中间设备：网络中处于源设备和目的设备之间的设备。本设备负责将镜像报文传输给下一个中间设备或目的设备。如果源设备与目的设备直接相连，则不存在中间设备。用户需要确保远程镜像 VLAN 内源设备到目的设备的二层互通性。
- 目的设备：远程镜像目的端口所在的设备，用户需要在目的设备上创建远程目的镜像组。目的设备收到报文后，比较报文的 VLAN ID 和远程目的镜像组的远程镜像 VLAN 是否相同，如果相同，则将该报文通过镜像目的端口转发给监控设备。

### 1.2.1 组网图

图1-3 配置远程端口镜像（方式一）组网图



### 1.2.2 应用要求

某公司内部通过交换机（以S3610系列以太网交换机为例，如图1-3中Switch A、Switch B和Switch C）实现各部门之间的互连，网络环境描述如下：

- 部门1通过端口 Ethernet 1/0/1 接入 Switch A；
- 部门2通过端口 Ethernet 1/0/2 接入 Switch A；
- Switch A 的端口 Ethernet 1/0/3 和 Switch B 的端口 Ethernet 1/0/1 相连；
- Switch B 的端口 Ethernet 1/0/2 和 Switch C 的端口 Ethernet 1/0/1 相连；
- 数据监测设备连接在 Switch C 的 Ethernet 1/0/2 端口上。

网络管理员希望通过数据监测设备对部门1和部门2发送的报文进行监控。

使用远程端口镜像功能实现该需求，进行如下配置：

- Switch A 充当源设备，Switch B 充当中间设备，Switch C 充当目的设备；
- 在 Switch A 上配置远程源镜像组，定义 VLAN 2 为远程镜像 VLAN，端口 Ethernet 1/0/1 和 Ethernet 1/0/2 为镜像源端口，端口 Ethernet 1/0/4 为反射端口；
- 配置 Switch A 的端口 Ethernet 1/0/3、Switch B 的端口 Ethernet 1/0/1 和 Ethernet 1/0/2、Switch C 的端口 Ethernet 1/0/1 的端口类型为 Trunk 端口，并且都允许 VLAN 2 的报文通过；
- 在 Switch C 上配置远程目的镜像组，定义 VLAN 2 为远程镜像 VLAN，连接数据监测设备的端口 Ethernet 1/0/2 为镜像目的端口。

### 1.2.3 适用产品、版本

表1-2 配置适用的产品与软硬件版本关系

| 产品             | 软件版本                            | 硬件版本    |
|----------------|---------------------------------|---------|
| S3610 系列以太网交换机 | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5510 系列以太网交换机 | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |

### 1.2.4 配置过程 and 解释

(1) 配置 Switch A（源设备）

# 创建远程源镜像组。

```
<SwitchA> system-view
```

```
[SwitchA] mirroring-group 1 remote-source
```

# 创建 VLAN 2。

```
[SwitchA] vlan 2
```

```
[SwitchA-vlan2] quit
```

# 为远程源镜像组配置远程镜像 VLAN、源端口和反射端口。

```
[SwitchA] mirroring-group 1 remote-probe vlan 2
```

```
[SwitchA] mirroring-group 1 mirroring-port Ethernet 1/0/1 Ethernet 1/0/2 inbound
```

```
[SwitchA] mirroring-group 1 reflector-port Ethernet 1/0/4
```

# 配置端口 Ethernet 1/0/3 的端口类型为 Trunk 端口，允许 VLAN 2 的报文通过。

```
[SwitchA] interface Ethernet 1/0/3
```

```
[SwitchA-Ethernet1/0/3] port link-type trunk
[SwitchA-Ethernet1/0/3] port trunk permit vlan 2
```

## (2) 配置 Switch B（中间设备）

# 配置端口 Ethernet 1/0/1 的端口类型为 Trunk 端口，允许 VLAN 2 的报文通过。

```
<SwitchB> system-view
[SwitchB] interface Ethernet 1/0/1
[SwitchB-Ethernet1/0/1] port link-type trunk
[SwitchB-Ethernet1/0/1] port trunk permit vlan 2
[SwitchB-Ethernet1/0/1] quit
```

# 配置端口 Ethernet 1/0/2 的端口类型为 Trunk 端口，允许 VLAN 2 的报文通过。

```
[SwitchB] interface Ethernet 1/0/2
[SwitchB-Ethernet1/0/2] port link-type trunk
[SwitchB-Ethernet1/0/2] port trunk permit vlan 2
```

## (3) 配置 Switch C（目的设备）

# 配置端口 Ethernet 1/0/1 的端口类型为 Trunk 端口，允许 VLAN 2 的报文通过。

```
<SwitchC> system-view
[SwitchC] interface Ethernet 1/0/1
[SwitchC-Ethernet1/0/1] port link-type trunk
[SwitchC-Ethernet1/0/1] port trunk permit vlan 2
[SwitchC-Ethernet1/0/1] quit
```

# 创建远程目的镜像组。

```
[SwitchC] mirroring-group 1 remote-destination
```

# 创建 VLAN 2。

```
[SwitchC] vlan 2
[SwitchC-vlan2] quit
```

# 为远程目的镜像组配置远程镜像 VLAN 和目的端口。

```
[SwitchC] mirroring-group 1 remote-probe vlan 2
[SwitchC] mirroring-group 1 monitor-port Ethernet 1/0/2
[SwitchC] interface Ethernet 1/0/2
[SwitchC-Ethernet1/0/2] port access vlan 2
```

## 1.2.5 完整配置

Switch A 上的完整配置：

```
#
mirroring-group 1 remote-source
mirroring-group 1 remote-probe vlan 2
#
vlan 2
#
interface Ethernet1/0/1
mirroring-group 1 mirroring-port inbound
#
interface Ethernet1/0/2
mirroring-group 1 mirroring-port inbound
```

```
#
interface Ethernet1/0/3
port link-type trunk
port trunk permit vlan 1 to 2
#
interface Ethernet1/0/4
mirroring-group 1 reflector-port
#
```

Switch B 上的完整配置：

```
#
interface Ethernet1/0/1
port link-type trunk
port trunk permit vlan 1 to 2
#
interface Ethernet1/0/2
port link-type trunk
port trunk permit vlan 1 to 2
#
```

Switch C 上的完整配置：

```
#
mirroring-group 1 remote-destination
mirroring-group 1 remote-probe vlan 2
#
vlan 2
#
interface Ethernet1/0/1
port link-type trunk
port trunk permit vlan 1 to 2
#
interface Ethernet1/0/2
port access vlan 2
mirroring-group 1 monitor-port
#
```

### 1.2.6 配置注意事项

配置远程端口镜像（方式一）的源设备时需要注意：

- 在源设备上通过配置远程源镜像组实现远程镜像功能，S3610&S5510 系列以太网交换机只支持配置 1 个远程源镜像组。
- 远程源镜像组的所有端口都属于同一台设备，一个远程源镜像组只能配置一个反射端口。
- 反射端口不能是现有镜像组的成员端口、聚合组成员端口，不能配置 QinQ 功能。反射口必须为 Access 端口且属于缺省 VLAN。
- 端口的双工模式、端口速率、MDI 属性取值均为缺省值时，才能将端口配置为反射端口；将某个端口配置为反射端口后，不能再修改此端口双工模式、端口速率、MDI 属性的取值，即这些属性只能为缺省值。

- 请用户不要在反射端口连接网线，不要在反射端口上配置下列功能：STP、RSTP、MSTP、802.1x、IGMP Snooping、静态 ARP 和 MAC 地址学习功能，否则可能会影响镜像功能的正常使用。
- 配置远程镜像 VLAN 时，要求该 VLAN 为静态 VLAN 并预先创建。被配置成远程镜像 VLAN 后，该 VLAN 不能直接删除，必须先删除远程镜像 VLAN 的配置才能够删除这个 VLAN。如果镜像组生效后，远程镜像 VLAN 被取消，那么该镜像组将失效。
- 远程镜像 VLAN 不用做其他用途，仅用于远程镜像。
- 一个远程镜像 VLAN 只能被一个远程源镜像组使用。

配置远程端口镜像（方式一）的目的设备时需要注意：

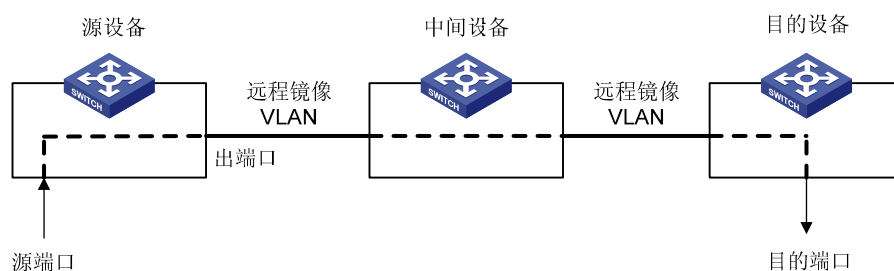
- 在目的设备上通过配置远程目的镜像组实现远程镜像功能。
- 目的端口不能是现有镜像组的成员端口。
- 请用户不要在目的端口上开启 STP、RSTP 或 MSTP，否则可能会影响镜像功能的正常使用。
- 目的端口不用做其他用途，仅用于端口镜像。
- 配置远程镜像 VLAN 时，要求该 VLAN 为静态 VLAN 并预先创建。被配置成远程镜像 VLAN 后，该 VLAN 不能直接删除，必须先删除远程镜像 VLAN 的配置才能够删除这个 VLAN。如果镜像组生效后，远程镜像 VLAN 被取消，那么该镜像组将失效。
- 一个远程镜像 VLAN 只能被一个远程目的镜像组使用。
- 远程镜像 VLAN 不用做其他用途，仅用于远程镜像。

### 1.3 远程端口镜像典型配置指导（方式二）

远程端口镜像（方式二）通过远程源镜像组和远程目的镜像组互相配合的方式实现。

远程端口镜像（方式二）的应用如图 1-4所示。

图1-4 远程端口镜像（方式二）应用示意图



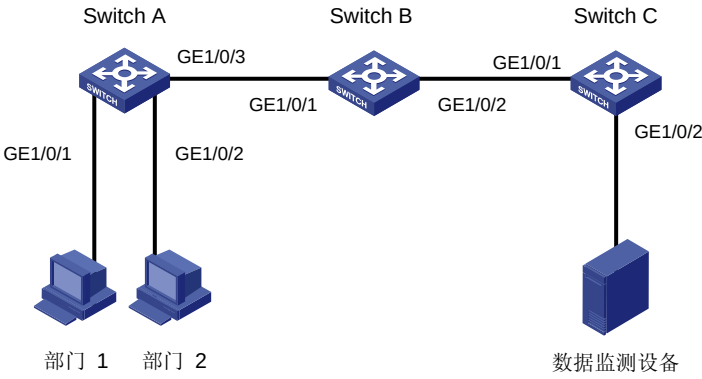
图中各设备的作用如下：

- 源设备：源端口所在的设备，用户需要在源设备上创建远程源镜像组。本设备负责将源端口的报文复制一份，然后通过出端口将报文在远程镜像 VLAN 中进行广播，传输给中间设备或目的设备。
- 中间设备：网络中处于源设备和目的设备之间的设备。本设备负责将镜像报文传输给下一个中间设备或目的设备。如果源设备与目的设备直接相连，则不存在中间设备。用户需要确保远程镜像 VLAN 内源设备到目的设备的二层互通性。

- 目的设备：远程镜像目的端口所在的设备，用户需要在目的设备上创建远程目的镜像组。目的设备收到报文后，比较报文的 VLAN ID 和远程目的镜像组的远程镜像 VLAN 是否相同，如果相同，则将该报文通过镜像目的端口转发给监控设备。

### 1.3.1 组网图

图1-5 配置远程端口镜像（方式二）组网图



### 1.3.2 应用要求

某公司内部通过交换机（以S5500-EI系列以太网交换机为例，如图 1-5中Switch A、Switch B和Switch C）实现各部门之间的互连，网络环境描述如下：

- 部门 1 通过端口 GigabitEthernet 1/0/1 接入 Switch A；
- 部门 2 通过端口 GigabitEthernet 1/0/2 接入 Switch A；
- Switch A 的端口 GigabitEthernet 1/0/3 和 Switch B 的端口 GigabitEthernet 1/0/1 相连；
- Switch B 的端口 GigabitEthernet 1/0/2 和 Switch C 的端口 GigabitEthernet 1/0/1 相连；
- 数据监测设备连接在 Switch C 的端口 GigabitEthernet 1/0/2 上。

网络管理员希望通过数据监测设备对部门 1 和部门 2 发送的报文进行监控。

使用远程端口镜像功能实现该需求，进行如下配置：

- Switch A 充当源设备，Switch B 充当中间设备，Switch C 充当目的设备；
- 在 Switch A 上配置远程源镜像组，定义 VLAN 2 为远程镜像 VLAN，端口 GigabitEthernet 1/0/1 和 GigabitEthernet 1/0/2 为镜像源端口，端口 GigabitEthernet 1/0/3 为出端口；
- 配置 Switch A 的端口 GigabitEthernet 1/0/3、Switch B 的端口 GigabitEthernet 1/0/1 和 GigabitEthernet 1/0/2、Switch C 的端口 GigabitEthernet 1/0/1 的端口类型为 Trunk 端口，并且都允许 VLAN 2 的报文通过；
- 在 Switch C 上配置远程目的镜像组，定义 VLAN 2 为远程镜像 VLAN，连接数据监测设备的端口 GigabitEthernet 1/0/2 为镜像目的端口。

### 1.3.3 适用产品、版本

表1-3 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本    |
|-------------------|---------------------------------|---------|
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本 |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本 |

### 1.3.4 配置过程和解释

#### (1) 配置 Switch A（源设备）

# 创建远程源镜像组。

```
<SwitchA> system-view
```

```
[SwitchA] mirroring-group 1 remote-source
```

# 创建 VLAN 2。

```
[SwitchA] vlan 2
```

```
[SwitchA-vlan2] quit
```

# 为远程源镜像组配置远程镜像 VLAN、源端口和出端口。

```
[SwitchA] mirroring-group 1 remote-probe vlan 2
```

```
[SwitchA] mirroring-group 1 mirroring-port GigabitEthernet 1/0/1 GigabitEthernet 1/0/2
inbound
```

```
[SwitchA] mirroring-group 1 monitor-egress GigabitEthernet 1/0/3
```

# 配置端口 GigabitEthernet 1/0/3 的端口类型为 Trunk 端口，允许 VLAN 2 的报文通过。

```
[SwitchA] interface GigabitEthernet 1/0/3
```

```
[SwitchA-GigabitEthernet1/0/3] port link-type trunk
```

```
[SwitchA-GigabitEthernet1/0/3] port trunk permit vlan 2
```

#### (2) 配置 Switch B（中间设备）

# 配置端口 GigabitEthernet 1/0/1 的端口类型为 Trunk 端口，允许 VLAN 2 的报文通过。

```
<SwitchB> system-view
```

```
[SwitchB] interface GigabitEthernet 1/0/1
```

```
[SwitchB-GigabitEthernet1/0/1] port link-type trunk
```

```
[SwitchB-GigabitEthernet1/0/1] port trunk permit vlan 2
```

```
[SwitchB-GigabitEthernet1/0/1] quit
```

# 配置端口 GigabitEthernet 1/0/2 的端口类型为 Trunk 端口，允许 VLAN 2 的报文通过。

```
[SwitchB] interface GigabitEthernet 1/0/2
```

```
[SwitchB-GigabitEthernet1/0/2] port link-type trunk
```

```
[SwitchB-GigabitEthernet1/0/2] port trunk permit vlan 2
```

#### (3) 配置 Switch C（目的设备）

# 配置端口 GigabitEthernet 1/0/1 的端口类型为 Trunk 端口，允许 VLAN 2 的报文通过。

```
<SwitchC> system-view
```

```
[SwitchC] interface GigabitEthernet 1/0/1
```

```
[SwitchC-GigabitEthernet1/0/1] port link-type trunk
```

```
[SwitchC-GigabitEthernet1/0/1] port trunk permit vlan 2
```

```
[SwitchC-GigabitEthernet1/0/1] quit
```

# 创建远程目的镜像组。

```
[SwitchC] mirroring-group 1 remote-destination
```

# 创建 VLAN 2。

```
[SwitchC] vlan 2
```

```
[SwitchC-vlan2] quit
```

# 为远程目的镜像组配置远程镜像 VLAN 和目的端口。

```
[SwitchC] mirroring-group 1 remote-probe vlan 2
[SwitchC] mirroring-group 1 monitor-port GigabitEthernet 1/0/2
[SwitchC] interface GigabitEthernet 1/0/2
[SwitchC-GigabitEthernet1/0/2] port access vlan 2
```

### 1.3.5 完整配置

Switch A 上的完整配置：

```
#
mirroring-group 1 remote-source
mirroring-group 1 remote-probe vlan 2
#
vlan 2
#
interface GigabitEthernet1/0/1
mirroring-group 1 mirroring-port inbound
#
interface GigabitEthernet1/0/2
mirroring-group 1 mirroring-port inbound
#
interface GigabitEthernet1/0/3
port link-type trunk
port trunk permit vlan 1 to 2
mirroring-group 1 monitor-egress
#
```

Switch B 上的完整配置：

```
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 1 to 2
#
interface GigabitEthernet1/0/2
port link-type trunk
port trunk permit vlan 1 to 2
#
```

Switch C 上的完整配置：

```
#
mirroring-group 1 remote-destination
mirroring-group 1 remote-probe vlan 2
#
vlan 2
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 1 to 2
#
```



```
interface GigabitEthernet1/0/2
port access vlan 2
mirroring-group 1 monitor-port
#
```

### 1.3.6 配置注意事项

配置远程端口镜像（方式二）的源设备时需要注意：

- 在源设备上通过配置远程源镜像组实现远程镜像功能。
- 远程源镜像组的所有端口都属于同一台设备，一个远程源镜像组只能配置一个出端口。
- 出端口不能为现有镜像组的成员端口。
- 请用户不要在出端口上配置下列功能：STP、RSTP、MSTP、802.1x、IGMP Snooping、QinQ、静态 ARP 和 MAC 地址学习功能，否则可能会影响镜像功能的正常使用。
- 配置远程镜像 VLAN 时，要求该 VLAN 为静态 VLAN 并预先创建。被配置成远程镜像 VLAN 后，该 VLAN 不能直接删除，必须先删除远程镜像 VLAN 的配置才能够删除这个 VLAN。如果镜像组生效后，远程镜像 VLAN 被取消，那么该镜像组将失效。
- 远程镜像 VLAN 不用做其他用途，仅用于远程镜像功能。
- 一个远程镜像 VLAN 只能被一个远程源镜像组使用。

配置远程端口镜像（方式二）的目的设备时需要注意：

- 在目的设备上通过配置远程目的镜像组实现远程镜像功能。
- 目的端口不能是现有镜像组的成员端口。
- 请用户不要在目的端口上使能 STP、RSTP 或 MSTP，否则可能会影响镜像功能的正常使用。
- 目的端口不用做其他用途，仅用于端口镜像。
- 配置远程镜像 VLAN 时，要求该 VLAN 为静态 VLAN 并预先创建。被配置成远程镜像 VLAN 后，该 VLAN 不能直接删除，必须先删除远程镜像 VLAN 的配置才能够删除这个 VLAN。如果镜像组生效后，远程镜像 VLAN 被取消，那么该镜像组将失效。
- 远程镜像 VLAN 不用做其他用途，仅用于远程镜像功能。
- 一个远程镜像 VLAN 只能被一个远程目的镜像组使用。

# 目 录

- 1 Cluster典型配置指导..... 1-1
  - 1.1 Cluster典型配置指导 ..... 1-1
    - 1.1.1 组网图..... 1-1
    - 1.1.2 应用要求 ..... 1-1
    - 1.1.3 适用产品、版本 ..... 1-2
    - 1.1.4 配置过程和解释 ..... 1-2
    - 1.1.5 完整配置 ..... 1-5
    - 1.1.6 配置注意事项 ..... 1-5

# 1 Cluster 典型配置指导

## 1.1 Cluster 典型配置指导

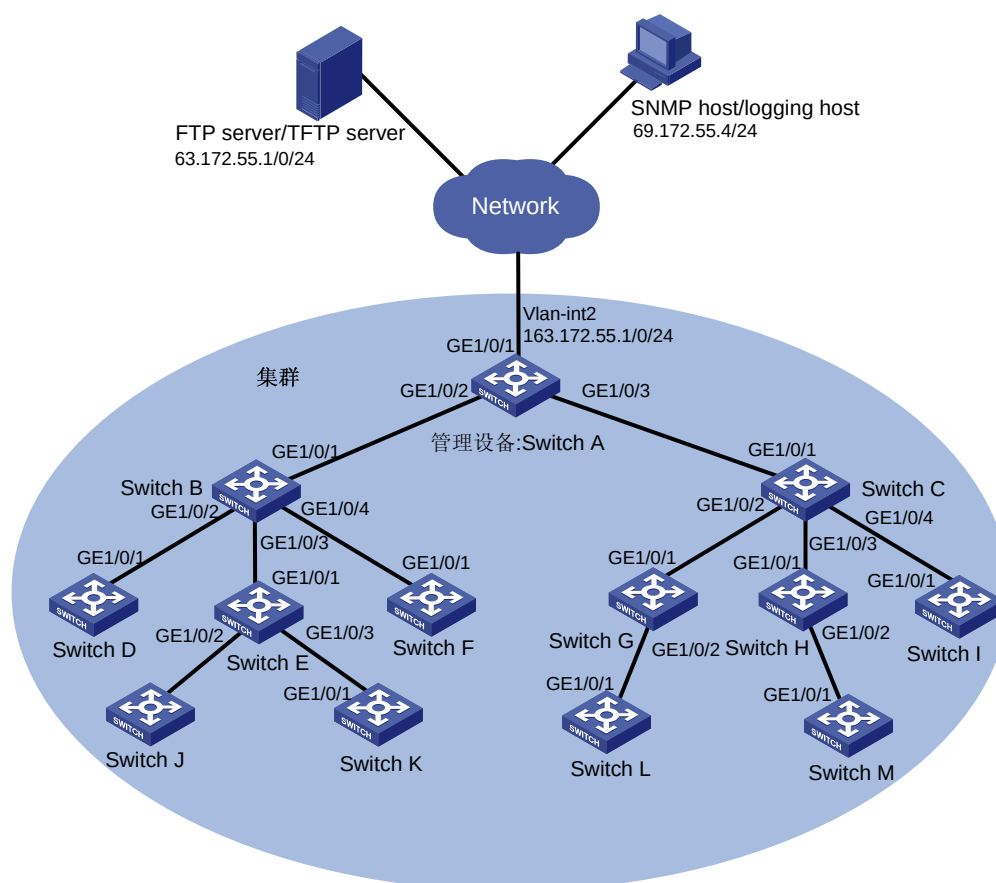
集群功能通过 HGMP V2（Huawei Group Management Protocol，华为组管理协议）实现。使用 HGMP V2 功能，网络管理员可以通过一个主交换机的公网 IP 地址，实现对多个交换机的管理。主交换机称为管理设备，其它被管理的交换机称为成员设备。成员设备一般不设置公网 IP 地址，通过管理设备重定向来实现对成员设备的管理和维护。管理设备和成员设备组成了一个“集群”。

在复杂的网络结构中，网络管理员可以通过 HGMP 功能，对网络内的交换机进行远程管理。这样可以节省大量的重复配置时间，降低配置复杂程度。

网络管理员只需要在管理交换机上建立集群，并打开成员交换机的 NDP 和 NTDP 功能，使能 HGMP 功能后就可以通过管理交换机管理集群成员了。

### 1.1.1 组网图

图1-1 HGMP 典型组网图



### 1.1.2 应用要求

- 13 台交换机构成一个集群
- Switch A 为管理设备，其它为成员设备
- 配置集群的管理 VLAN 为 VLAN 10

- 管理交换机的 IP 地址为 163.172.55.1
- 配置集群的 TFTP Server 的 IP 地址为 63.172.55.1
- 配置集群的 SNMP 网管站的 IP 地址为 69.172.55.4
- 整个集群使用相同的 TFTP server、SNMP 网管站

管理交换机：

- GigabitEthernet1/0/1 属于 VLAN2，VLAN2 的接口 IP 地址为 163.172.55.1
- 管理设备通过 GigabitEthernet1/0/2 和端口 GigabitEthernet1/0/3 下挂两台成员设备

成员交换机：

- 成员交换机 Switch B 通过 GigabitEthernet1/0/2、GigabitEthernet1/0/3、GigabitEthernet1/0/4 和下挂交换机 Switch D、Switch E、Switch F 相连
- 成员交换机 Switch C 通过 GigabitEthernet1/0/2、GigabitEthernet1/0/3、GigabitEthernet1/0/4 和下挂交换机 Switch G、Switch H、Switch I 相连
- 成员交换机 Switch E 通过 GigabitEthernet1/0/2、GigabitEthernet1/0/3 和下挂交换机 Switch J、Switch K 相连



说明

- Switch A、Switch B、Switch C 一般为低端交换机中的 S5500-SI 系列、S5500-EI 系列交换机。
- Switch D、Switch E、Switch F 可以为低端交换机中的 S3610 系列、S5510 系列。

### 1.1.3 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本                         |
|-------------------|---------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本               | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本               | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本                      |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本                      |

### 1.1.4 配置过程和解释

(1) 配置成员设备（以 Switch B 设备为例）

# 启动设备上的 NDP 和 NTPD。

```
<Sysname> system-view
[Sysname] ndp enable
[Sysname] ntpd enable
```

# 启动端口 GigabitEthernet1/0/1、GigabitEthernet1/0/2、GigabitEthernet1/0/3、GigabitEthernet1/0/4 上的 NDP 和 NTDP。

```
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ndp enable
[Sysname-GigabitEthernet1/0/1] ntdp enable
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] interface GigabitEthernet 1/0/2
[Sysname-GigabitEthernet1/0/2] ndp enable
[Sysname-GigabitEthernet1/0/2] ntdp enable
[Sysname-GigabitEthernet1/0/2] quit
[Sysname] interface GigabitEthernet 1/0/3
[Sysname-GigabitEthernet1/0/3] ndp enable
[Sysname-GigabitEthernet1/0/3] ntdp enable
[Sysname-GigabitEthernet1/0/3] quit
[Sysname] interface GigabitEthernet 1/0/4
[Sysname-GigabitEthernet1/0/4] ndp enable
[Sysname-GigabitEthernet1/0/4] ntdp enable
[Sysname-GigabitEthernet1/0/4] quit
```



#### 说明

- 成员交换机上与设备相连的端口都要启动 NDP、NTDP 功能。
  - 为了避免管理设备在拓扑收集时收集到不需要加入集群的设备的拓扑信息并把它加入到集群中，建议在与不需要加入集群设备相连的端口上关闭 NDP 功能。
  - 为了避免管理设备在拓扑收集时收集到不需要加入集群的设备的拓扑信息并把它加入到集群中，建议在与不需要加入集群设备相连的端口上关闭 NTDP 功能。
- 

## (2) 配置管理设备

# 启动集群功能。

```
<Sysname> system-view
[Sysname] cluster enable
```

# 关闭上行端口 GigabitEthernet 1/0/1 的 NDP 功能。

```
[Sysname] ndp enable
[Sysname] undo ndp enable interface GigabitEthernet 1/0/1
```

# 启动 GigabitEthernet 1/0/2、GigabitEthernet 1/0/3 上的 NDP。

```
[Sysname] interface GigabitEthernet 1/0/2
[Sysname-GigabitEthernet1/0/2] ndp enable
[Sysname-GigabitEthernet1/0/2] quit
[Sysname] interface GigabitEthernet 1/0/3
[Sysname-GigabitEthernet1/0/3] ndp enable
[Sysname-GigabitEthernet1/0/3] quit
```

# 配置 NDP 信息的有效保留时间为 120 秒。

```
[Sysname] ndp timer aging 120
```

# 配置 NDP 报文发送的时间间隔为 100 秒。

```
[Sysname] ndp timer hello 100
```

# 启动设备上的 NTDP 和端口 GigabitEthernet 1/0/2、GigabitEthernet 1/0/3 上的 NTDP。

```
[Sysname] ntdp enable
[Sysname] interface GigabitEthernet 1/0/2
[Sysname-GigabitEthernet1/0/2] ntdp enable
[Sysname-GigabitEthernet1/0/2] quit
[Sysname] interface GigabitEthernet 1/0/3
[Sysname-GigabitEthernet1/0/3] ntdp enable
[Sysname-GigabitEthernet1/0/3] quit
```

# 配置拓扑收集范围为 2 跳

```
[Sysname] ntdp hop 2
```

# 配置被收集设备转发拓扑收集请求的延迟时间为 180ms。

```
[Sysname] ntdp timer hop-delay 180
```

# 配置被收集设备的端口转发拓扑收集请求的延迟时间为 20ms。

```
[Sysname] ntdp timer port-delay 20
```

# 配置定时拓扑收集的时间间隔为 3 分钟。

```
[Sysname] ntdp timer 3
```

# 配置集群的管理 VLAN 为 VLAN10。

```
[Sysname] vlan 10
[Sysname-vlan10] quit
[Sysname] management-vlan 10
```

# 将管理设备与候选设备相连的端口配置为 Trunk 口，并且允许管理 VLAN 通过。

```
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type trunk
[Sysname-GigabitEthernet1/0/1] port trunk permit vlan 10
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] interface GigabitEthernet 1/0/3
[Sysname-GigabitEthernet1/0/3] port link-type trunk
[Sysname-GigabitEthernet1/0/3] port trunk permit vlan 10
[Sysname-GigabitEthernet1/0/3] quit
```

# 启动集群功能。

```
[Sysname] cluster enable
```

# 进入集群视图。

```
[Sysname] cluster
[Sysname-cluster]
```

# 配置集群内部使用的 IP 地址池，起始地址为 172.16.0.1，有 14 个地址。

```
[Sysname-cluster] ip-pool 172.16.0.1 255.255.255.240
```

# 配置集群名字，建立集群。

```
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster]
```

# 配置成员设备信息的保留时间为 100 秒。

```
[aaa_0.Sysname-cluster] holdtime 100
```

# 配置握手报文定时发送的时间间隔为 10 秒。

```
[aaa_0.Sysname-cluster] timer 10
```

# 配置集群内部公用的 TFTP Server 及 SNMP 网管站。

```
[aaa_0.Sysname-cluster] tftp-server 63.172.55.1
```

```
[aaa_0.Sysname-cluster] snmp-host 69.172.55.4
```

### (3) 集群成员上的操作

在管理设备将下挂的设备加入到集群以后，在成员设备上作下列操作。

# 成员设备从集群内部公用的 TFTP 服务器下载文件 **aaa.txt** 到本地。

```
<aaa_1.Sysname> tftp cluster get aaa.txt
```

# 成员设备上载文件 **bbb.txt** 到集群内部公用的 TFTP 服务器。

```
<aaa_1.Sysname> tftp cluster put bbb.txt
```

## 1.1.5 完整配置

Switch A 配置

```
#
ntdp hop 2
ntdp timer port-delay 20
ntdp timer hop-delay 180
ntdp timer 3
#
ndp timer hello 100
ndp timer aging 120
#
cluster
ip-pool 172.16.0.1 255.255.255.248
build aaa
holdtime 100
tftp-server 63.172.55.1
snmp-host 69.172.55.4 community-string read public write private
#
```

## 1.1.6 配置注意事项

- 在进行了上述配置之后，用户只要在管理设备上通过命令 **cluster switch-to { member-number | mac-address H-H-H }** 切换到成员设备配置视图就可以对成员设备进行维护管理，通过命令 **cluster switch-to administrator** 切换回管理设备配置视图。
- 在管理设备上用户还可以通过命令 **reboot member { member-number | mac-address H-H-H } [ eraseflash ]** 对成员设备进行重启操作。
- 在进行了上述配置之后，用户可以在网管站接受集群所有成员的日志和 SNMP trap。
- 交换机不支持作为 TFTP 服务器端。
- 集群的管理 VLAN 缺省为 1，为了提高安全性，将集群的管理报文与其它报文隔离，建议将集群的管理 VLAN 配置为其它 VLAN。

- 如果接入网管设备（包括 FTP/TFTP 服务器、网管主机和日志主机）的端口不允许管理 VLAN 通过，网管设备将无法通过管理设备对集群内部的设备进行管理，这时，需要在管理设备上将接入网管设备（包括 FTP/TFTP 服务器、网管主机和日志主机）的 VLAN 接口配置为网管接口。
- 建议各类定时器的配置采用缺省值。
- 集群中被配置为黑名单中的设备下挂的其他设备不能使用 **display cluster current-topology** 命令显示。



# 目 录

|                                |     |
|--------------------------------|-----|
| 1 SNMP典型配置指导.....              | 1-1 |
| 1.1 SNMP简介.....                | 1-1 |
| 1.2 SNMPv2c监控管理交换机典型配置指导 ..... | 1-1 |
| 1.2.1 组网图.....                 | 1-1 |
| 1.2.2 应用要求 .....               | 1-1 |
| 1.2.3 适用产品、版本 .....            | 1-1 |
| 1.2.4 配置过程和解释 .....            | 1-2 |
| 1.2.5 完整配置 .....               | 1-3 |
| 1.2.6 配置注意事项 .....             | 1-3 |
| 1.3 SNMPv3 监控管理交换机典型配置指导 ..... | 1-3 |
| 1.3.1 组网图.....                 | 1-3 |
| 1.3.2 应用要求 .....               | 1-3 |
| 1.3.3 适用产品、版本 .....            | 1-4 |
| 1.3.4 配置过程和解释 .....            | 1-4 |
| 1.3.5 完整配置 .....               | 1-5 |
| 1.3.6 配置注意事项 .....             | 1-5 |
| 1.4 SNMP操作日志输出典型配置指导 .....     | 1-5 |
| 1.4.1 组网图.....                 | 1-5 |
| 1.4.2 应用要求 .....               | 1-5 |
| 1.4.3 适用产品、版本 .....            | 1-6 |
| 1.4.4 配置过程和解释 .....            | 1-6 |
| 1.4.5 完整配置 .....               | 1-7 |
| 1.4.6 配置注意事项 .....             | 1-7 |
| 2 RMON典型配置指导.....              | 2-1 |
| 2.1 RMON简介.....                | 2-1 |
| 2.2 RMON典型配置指导.....            | 2-1 |
| 2.2.1 组网图.....                 | 2-1 |
| 2.2.2 应用要求 .....               | 2-1 |
| 2.2.3 适用产品、版本 .....            | 2-1 |
| 2.2.4 配置过程和解释 .....            | 2-2 |
| 2.2.5 完整配置 .....               | 2-2 |
| 2.2.6 配置注意事项 .....             | 2-2 |

# 1 SNMP 典型配置指导

## 1.1 SNMP 简介

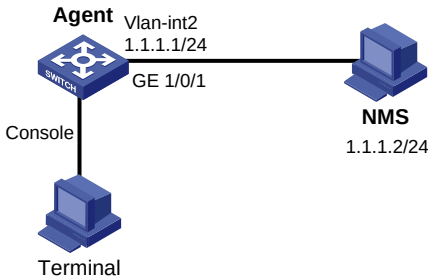
SNMP（Simple Network Management Protocol，简单网络管理协议）是使用 TCP/IP 协议族对互联网上的设备进行管理的一个框架，它提供一组基本的操作来监视和维护互联网。SNMP 具有以下优势：

- 自动化网络管理。网络管理员可以利用 SNMP 平台在网络上的节点检索信息、修改信息、发现故障、完成故障诊断、进行容量规划和生成报告。
- 屏蔽不同设备的物理差异，实现对不同厂商产品的自动化管理。SNMP 只提供最基本的功能集，使得管理任务分别与设备物理特性和下层的联网技术相对独立，从而实现对不同厂商设备的管理，特别适合在小型、快速和低成本的环境中使用。

## 1.2 SNMPv2c 监控管理交换机典型配置指导

### 1.2.1 组网图

图1-1 SNMPv2c 监控管理交换机组网图



### 1.2.2 应用要求

- 网管工作站（NMS）与以太网交换机（Agent）通过以太网相连
- 网管工作站 IP 地址为 1.1.1.2/24
- 以太网交换机的 VLAN 接口 IP 地址为 1.1.1.1/24
- NMS 通过 SNMP v2c 对 Agent 进行监控管理，Agent 在故障或者出错的时候能够主动向 NMS 报告情况

### 1.2.3 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

| 产品             | 软件版本                            | 硬件版本    |
|----------------|---------------------------------|---------|
| S3610 系列以太网交换机 | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5510 系列以太网交换机 | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |

| 产品                | 软件版本                            | 硬件版本                         |
|-------------------|---------------------------------|------------------------------|
| S5500-SI 系列以太网交换机 | Release 1207 软件版本               | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本               | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本                      |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本                      |

#### 1.2.4 配置过程和解释

- 配置 Agent

# 设置 SNMP 基本信息，包括版本、团体名。

```
<Sysname> system-view
[Sysname] snmp-agent sys-info version v2c
[Sysname] snmp-agent community read public
[Sysname] snmp-agent community write private
```

# 设置网管使用的 Vlan-interface2 (IP 地址为 1.1.1.1/24)，将用于网管的端口 GigabitEthernet1/0/1 加入到 VLAN2 中。

```
[Sysname] vlan 2
[Sysname-vlan2] port GigabitEthernet 1/0/1
[Sysname-vlan2] quit
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ip address 1.1.1.1 255.255.255.0
[Sysname-Vlan-interface2] quit
```

# 设置交换机的联系人和位置信息，以方便维护。

```
[Sysname] snmp-agent sys-info version all
[Sysname] snmp-agent sys-info contact Mr.Chen-Tel:5651
[Sysname] snmp-agent sys-info location telephone-closet,3rd-floor
```

# 允许向网管工作站 (NMS) 1.1.1.2/24 发送 Trap 报文，使用的团体名为 public。

```
[Sysname] snmp-agent trap enable
[Sysname] snmp-agent target-host trap address udp-domain 1.1.1.2 udp-port 5000 params securityname public
```

- 配置 NMS (具体设置请参考 NMS 配套手册)

# 选择 SNMP 版本号为 SNMPv2c，设置“只读团体名”为 public，“读写团体名”为 private，SNMP 端口号选择 161。

# 为了能够接收 Agent 发来的 trap 报文，需在 NMS 端设置监听 trap 报文的 udp 端口号为 5000 (和 Agent 端命令行配置端口一致)。

# 配置完成后，即可实现 NMS 对交换机的远程监控和管理，当交换机有告警事件发生时会自动向 NMS 发送 trap 报文。

## 1.2.5 完整配置

```
#
interface Vlan-interface2
 ip address 1.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port access vlan 2
#
snmp-agent
snmp-agent local-engineid 800063A20300E0FC123456
snmp-agent community read public
snmp-agent community write private
snmp-agent sys-info contact Mr.Chen-Tel:5651
snmp-agent sys-info location telephone-closet,2rd-floor
snmp-agent sys-info version all
snmp-agent target-host trap address udp-domain 1.1.1.2 udp-port 5000 params securityname
public
#
```

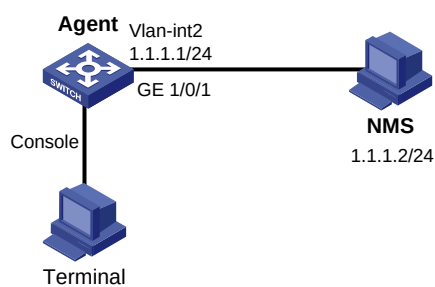
## 1.2.6 配置注意事项

- (1) 用户可利用网管系统（如 Quidview）完成对交换机的查询和配置操作，具体设置请参考 NMS 配套手册。
- (2) 网管侧的配置必须和交换机侧保持一致，否则无法进行相应操作。

## 1.3 SNMPv3 监控管理交换机典型配置指导

### 1.3.1 组网图

图1-2 SNMPv3 监控管理交换机组网图



### 1.3.2 应用要求

- 网管工作站（NMS）与以太网交换机（Agent）通过以太网相连
- 网管工作站 IP 地址为 1.1.1.2/24
- 以太网交换机的 VLAN 接口 IP 地址为 1.1.1.1/24
- NMS 通过 SNMP v3 对 Agent 的接口状态进行监控管理，Agent 在故障或者出错的时候能够主动向 NMS 报告情况，NMS 接收 Trap 的端口号为 5000

### 1.3.3 适用产品、版本

表1-2 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本                         |
|-------------------|---------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本               | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本               | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本                      |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本                      |

### 1.3.4 配置过程和解释

- 配置 Agent

# 设置访问权限。

```
<Sysname> system-view
```

```
[Sysname] undo snmp-agent mib-view ViewDefault
```

```
[Sysname] snmp-agent mib-view included test interfaces
```

```
[Sysname] snmp-agent group v3 managev3group read-view test write-view test
```

```
[Sysname] snmp-agent usm-user v3 managev3user managev3group
```

# 设置交换机的联系人和位置信息，以方便维护。

```
[Sysname] snmp-agent sys-info contact Mr.Chen-Tel:5651
```

```
[Sysname] snmp-agent sys-info location telephone-closet,2rd-floor
```

# 设置网管使用的 Vlan-interface2 (IP 地址为 1.1.1.1/24)，将用于网管的端口 GigabitEthernet1/0/1 加入到 VLAN2 中。

```
[Sysname] vlan 2
```

```
[Sysname-vlan2] port GigabitEthernet 1/0/1
```

```
[Sysname-vlan2] quit
```

```
[Sysname] interface vlan-interface 2
```

```
[Sysname-Vlan-interface2] ip address 1.1.1.1 255.255.255.0
```

```
[Sysname-Vlan-interface2] quit
```

# 将 Vlan-interface2 的 IP 地址作为 Trap 报文的源地址。

```
[Sysname] snmp-agent trap source Vlan-interface 2
```

# 允许向网管工作站 (NMS) 1.1.1.2/24 发送 Trap 报文，使用的团体名为 public。

```
[Sysname] snmp-agent trap enable
```

```
[Sysname] snmp-agent target-host trap address udp-domain 1.1.1.2 udp-port 5000 params securityname public
```

- 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，需要分别设置认证方式、认证密码、加密方式、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，具体情况请参考 NMS 的配套手册。

### 1.3.5 完整配置

```
#
interface Vlan-interface2
 ip address 1.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port access vlan 2
#
snmp-agent
snmp-agent local-engineid 800063A20300E0FC123456
snmp-agent sys-info contact Mr.Chen-Tel:5651
snmp-agent sys-info location telephone-closet,2rd-floor
snmp-agent sys-info version v3
snmp-agent group v3 managev3group read-view test write-view test
snmp-agent target-host trap address udp-domain 1.1.1.2 udp-port 5000 params securityname
public
snmp-agent mib-view included test interfaces
snmp-agent usm-user v3 managev3user managev3group
snmp-agent trap source Vlan-interface2
```

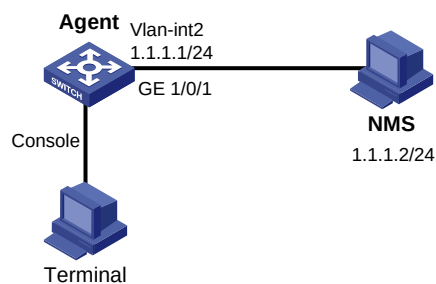
### 1.3.6 配置注意事项

- (1) 用户可利用网管系统完成对交换机的查询和配置操作，具体设置请参考 NMS 配套手册。
- (2) 网管侧的配置必须和交换机侧保持一致，否则无法进行相应操作。

## 1.4 SNMP 操作日志输出典型配置指导

### 1.4.1 组网图

图1-3 SNMP 操作日志信息输出组网图



### 1.4.2 应用要求

- 网管工作站（NMS）与以太网交换机（Agent）通过以太网相连

- 网管工作站 IP 地址为 1.1.1.2/2
- 以太网交换机的 VLAN 接口 IP 地址为 1.1.1.1/24
- NMS 对 Agent 执行的 get/set 操作日志通过 Console 通道输出到控制台。

### 1.4.3 适用产品、版本

表1-3 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本                         |
|-------------------|---------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本               | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本               | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本                      |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本                      |

### 1.4.4 配置过程和解释

- 配置 Agent

# 设置 SNMP 基本信息，包括版本、团体名。

```
<Sysname> system-view
[Sysname] snmp-agent sys-info version all
[Sysname] snmp-agent community read public
[Sysname] snmp-agent community write private
```

# 设置网管使用的 Vlan-interface2 (IP 地址为 1.1.1.1/24)，将用于网管的端口 GigabitEthernet1/0/1 加入到 VLAN2 中。

```
[Sysname] vlan 2
[Sysname-vlan2] port GigabitEthernet 1/0/1
[Sysname-vlan2] quit
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ip address 1.1.1.1 255.255.255.0
[Sysname-Vlan-interface2] quit
```

# 打开控制台对日志信息的显示功能（可选，缺省情况下，该功能是打开的）。

```
<Sysname> terminal monitor
<Sysname> terminal logging
```

# 配置信息中心允许输出级别为 informational 及 informational 之上级别的 SNMP 系统信息到 Console 口。

```
<Sysname> system-view
[Sysname] info-center source snmp channel console log level informational
```

# 打开 Agent 的 SNMP 日志开关，对 NMS 的 GET 和 SET 操作进行记录。

```
[Sysname] snmp-agent log get-operation
```

```
[Sysname] snmp-agent log set-operation
```

- NMS 对 Agent 进行 GET 操作时，可以在控制台上看到如下日志信息。

```
%Sep 9 02:49:40:566 2007 Sysname SNMP/6/GET:
```

```
seqNO = <10> srcIP = <1.1.1.2> op = <get> node = <sysName(1.3.6.1.2.1.1.5.0)> value=<>
```

- NMS 对 Agent 进行 SET 操作，可以在控制台上看到如下日志信息。

```
%Sep 9 02:59:42:576 2007 Sysname SNMP/6/SET:
```

```
seqNO = <11> srcIP = <1.1.1.2> op = <set> errorIndex = <0> errorStatus =<noError> node =
<sysName(1.3.6.1.2.1.1.5.0)> value = <Sysname>
```

### 1.4.5 完整配置

```

info-center source SNMP channel 0

interface Vlan-interface2
ip address 1.1.1.1 255.255.255.0

interface GigabitEthernet1/0/1
port access vlan 2

snmp-agent
snmp-agent local-engineid 800063A20300E0FC123456
snmp-agent community read public
snmp-agent community write private
snmp-agent log all
snmp-agent sys-info version all
```

### 1.4.6 配置注意事项

- (1) 信息中心的系统信息可以输出到控制台或日志缓冲区等方向。本举例是将 SNMP 日志信息输出到控制台，如果要配置别的输出方向，请参见各产品操作手册的“信息中心”部分；
- (2) 本例配置的前提是 NMS 已经能够对 Agent 进行 get/set 操作。
- (3) 大量的日志记录会占用设备的存储空间，影响设备的性能。正常情况下，建议关闭 SNMP 日志功能。



# 2 RMON 典型配置指导

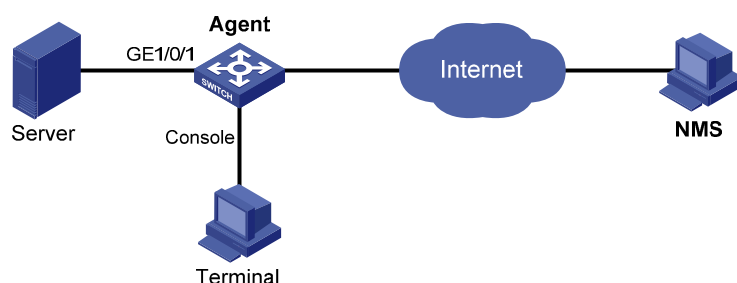
## 2.1 RMON 简介

RMON (Remote Monitoring, 远程网络监视) 的实现完全基于 SNMP 体系结构, 它与现存的 SNMP 框架相兼容, 不需对该协议进行任何修改。RMON 使 SNMP 更有效、更积极主动地监测远程网络设备, 为监控子网的运行提供了一种高效的手段。RMON 能够减少网管站同代理间的通讯流量, 达到简便而有力地管理大型互连网络的目的。

## 2.2 RMON 典型配置指导

### 2.2.1 组网图

图2-1 配置 RMON 组网图



### 2.2.2 应用要求

Agent 通过 console 口连接配置终端, 通过 Internet 连接远端 NMS。在 RMON 以太网统计表中设定一个表项, 对以太网端口 GigabitEthernet1/0/1 进行性能统计, 当端口在一段时间内收到的字节数超过设置的门限后, 记录日志。

### 2.2.3 适用产品、版本

表2-1 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本                         |
|-------------------|---------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本               | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本               | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本                      |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本                      |

## 2.2.4 配置过程和解释

# 配置 RMON 对接口 GigabitEthernet1/0/1 进行流量统计。

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] rmon statistics 1 owner user1-rmon
[Sysname-GigabitEthernet1/0/1] return
```

# 配置一个事件，在该事件被触发的时候，会记录日志。

```
<Sysname> system-view
[Sysname] rmon event 1 log owner 1-rmon
```

# 配置一个告警组，对接口 GigabitEthernet1/0/1 收到的字节数进行抽样，当超过上下限值的时候，都会记录日志。

```
[Sysname] rmon alarm 1 1.3.6.1.2.1.16.1.1.1.4.1 10 delta rising-threshold 1000 1
falling-threshold 100 1 owner 1-rmon
```



说明

节点 1.3.6.1.2.1.16.1.1.1.4.1 表示 RMON 统计组 1 接收到的字节数，即 GigabitEthernet1/0/1 接收到的字节数。

---

## 2.2.5 完整配置

```
#
interface GigabitEthernet1/0/1
 rmon statistics 1 owner user1-rmon
#
 rmon event 1 description null log owner 1-rmon
 rmon alarm 1 1.3.6.1.2.1.16.1.1.1.4.1 10 delta rising-threshold 1000 1 falling-threshold
100 1 owner 1-rmon
```

## 2.2.6 配置注意事项

无

# 目 录

|                               |      |
|-------------------------------|------|
| 1 NTP典型配置指导.....              | 1-1  |
| 1.1 NTP简介.....                | 1-1  |
| 1.2 NTP服务器/客户端模式典型配置指导 .....  | 1-1  |
| 1.2.1 组网图.....                | 1-1  |
| 1.2.2 应用要求 .....              | 1-1  |
| 1.2.3 适用产品、版本 .....           | 1-1  |
| 1.2.4 配置过程和解释 .....           | 1-2  |
| 1.2.5 完整配置 .....              | 1-2  |
| 1.2.6 配置注意事项 .....            | 1-2  |
| 1.3 配置NTP对等体模式.....           | 1-2  |
| 1.3.1 组网图.....                | 1-2  |
| 1.3.2 应用要求 .....              | 1-2  |
| 1.3.3 适用产品、版本 .....           | 1-3  |
| 1.3.4 配置过程和解释 .....           | 1-3  |
| 1.3.5 完整配置 .....              | 1-3  |
| 1.3.6 配置注意事项 .....            | 1-4  |
| 1.4 NTP广播模式典型配置指导 .....       | 1-4  |
| 1.4.1 组网图.....                | 1-4  |
| 1.4.2 应用要求 .....              | 1-4  |
| 1.4.3 适用产品、版本 .....           | 1-4  |
| 1.4.4 配置过程和解释 .....           | 1-5  |
| 1.4.5 完整配置 .....              | 1-5  |
| 1.4.6 配置注意事项 .....            | 1-5  |
| 1.5 NTP组播模式典型配置指导 .....       | 1-6  |
| 1.5.1 组网图.....                | 1-6  |
| 1.5.2 应用要求 .....              | 1-6  |
| 1.5.3 适用产品、版本 .....           | 1-6  |
| 1.5.4 配置过程和解释 .....           | 1-6  |
| 1.5.5 完整配置 .....              | 1-7  |
| 1.5.6 配置注意事项 .....            | 1-8  |
| 1.6 带身份验证的NTP广播模式典型配置指导 ..... | 1-8  |
| 1.6.1 组网图.....                | 1-8  |
| 1.6.2 应用要求 .....              | 1-8  |
| 1.6.3 适用产品、版本 .....           | 1-9  |
| 1.6.4 配置过程和解释 .....           | 1-9  |
| 1.6.5 完整配置 .....              | 1-10 |
| 1.6.6 配置注意事项 .....            | 1-10 |

# 1 NTP 典型配置指导

## 1.1 NTP 简介

NTP（Network Time Protocol，网络时间协议）是由 RFC 1305 定义的时间同步协议，用来在分布式时间服务器和客户端之间进行时间同步。NTP 基于 UDP 报文进行传输，使用的 UDP 端口号为 123。

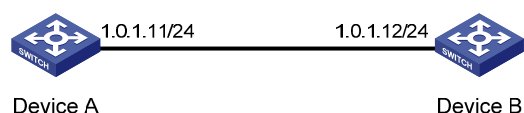
使用 NTP 的目的是对网络内所有具有时钟的设备进行时钟同步，使网络内所有设备的时钟保持一致，从而使设备能够提供基于统一时间的多种应用。

对于运行 NTP 的本地系统，既可以接受来自其他时钟源的同步，又可以作为时钟源同步其他的时钟，并且可以和其他设备互相同步。

## 1.2 NTP 服务器/客户端模式典型配置指导

### 1.2.1 组网图

图1-1 配置 NTP 服务器/客户端模式组网图



### 1.2.2 应用要求

- Device A 设置本地时钟作为参考时钟，层数为 2；
- Device B 工作在客户端模式，指定 Device A 为 NTP 服务器。

### 1.2.3 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                                 | 硬件版本                         |
|-------------------|--------------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301 软件版本, Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301 软件版本, Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本                    | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本                    | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本                    | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100 软件版本, Release 6300 软件版本 | 全系列硬件版本                      |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本                    | 全系列硬件版本                      |

## 1.2.4 配置过程和解释

- 配置 Device A

# 设置本地时钟作为参考时钟，层数为 2。

```
<DeviceA> system-view
[DeviceA] ntp-service refclock-master 2
```

- 配置 Device B

# 设置 Device A 为 Device B 的 NTP 服务器。

```
<DeviceB> system-view
[DeviceB] ntp-service unicast-server 1.0.1.11
```

## 1.2.5 完整配置

- Device A 上的配置

```

ntp-service refclock-master 2
```

- Device B 上的配置

```

ntp-service unicast-server 1.0.1.11
```

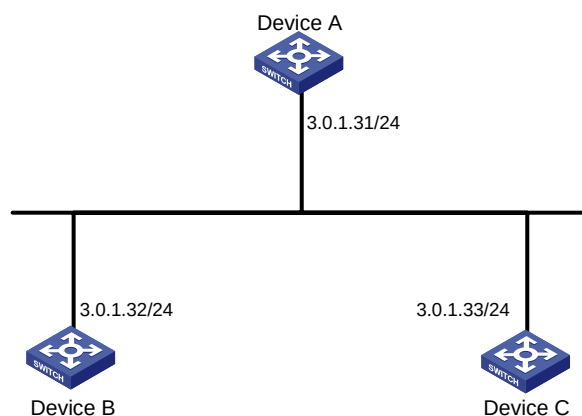
## 1.2.6 配置注意事项

- (1) S7500E 系列以太网交换机支持设置本身时钟作为参考时钟；
- (2) S3610/S5510/S5500-SI/S5500-EI 系列以太网交换机均不支持设置本身时钟为参考时钟，只有当其时钟被同步后，才能作为时钟源去同步其他设备。

## 1.3 配置 NTP 对等体模式

### 1.3.1 组网图

图1-2 配置 NTP 对等体模式组网图



### 1.3.2 应用要求

- Device A 设置本地时钟作为参考时钟，层数为 2；
- Device B 工作在客户端模式，指定 Device A 为 NTP 服务器；

- Device C 工作在对等体模式，将 Device B 设为对等体。Device C 为主动对等体，Device B 为被动对等体。

### 1.3.3 适用产品、版本

表1-2 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                                 | 硬件版本                         |
|-------------------|--------------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301 软件版本, Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301 软件版本, Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本                    | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本                    | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本                    | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100 软件版本, Release 6300 软件版本 | 全系列硬件版本                      |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本                    | 全系列硬件版本                      |

### 1.3.4 配置过程和解释

#### (1) 配置 Device A

# 设置本地时钟作为参考时钟，层数为 2。

```
<DeviceA> system-view
[DeviceA] ntp-service refclock-master 2
```

#### (2) 配置 Device B

# 设置 Device A 为 Device B 的 NTP 服务器。

```
<DeviceB> system-view
[DeviceB] ntp-service unicast-server 3.0.1.31
```

#### (3) 配置 Device C (Device B 向 Device A 同步后)

# 设置 Device B 为对等体。

```
<DeviceC> system-view
[DeviceC] ntp-service unicast-peer 3.0.1.32
```

### 1.3.5 完整配置

- Device A 上的配置

```
#
ntp-service refclock-master 2
```

- Device B 上的配置

```
#
ntp-service unicast-server 3.0.1.31
```

- Device C 上的配置

```
#
```

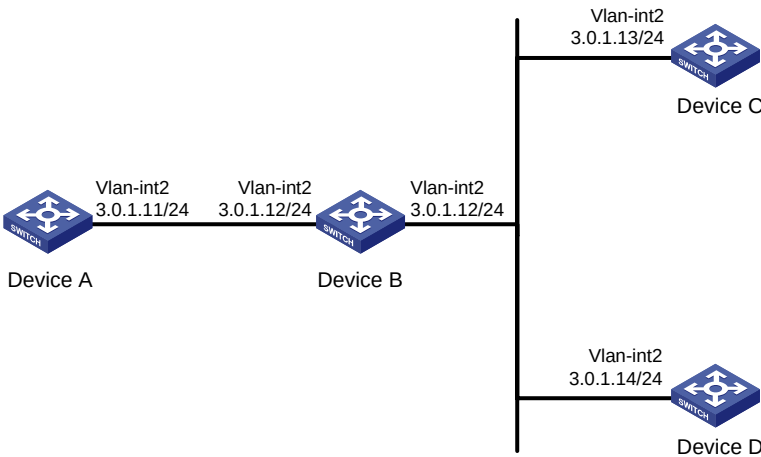
1.3.6 配置注意事项

- (1) S7500E 系列以太网交换机支持设置本身时钟作为参考时钟；
- (2) S3610/S5510/S5500-SI/S5500-EI 系列以太网交换机均不支持设置本身时钟为参考时钟，只有当其时钟被同步后，才能作为时钟源去同步其他设备。

1.4 NTP 广播模式典型配置指导

1.4.1 组网图

图1-3 NTP 广播模式配置组网图



1.4.2 应用要求

- Device C 是支持本地时钟作为主时钟的交换机（如 S7500E），并设置本地时钟作为 NTP 主时钟，层数为 2。
- Device A和Device D是 表 1-3所列任意型号的以太网交换机。设置Device A和Device D工作于广播客户端模式，分别从各自的Vlan-interface2 监听广播消息。

1.4.3 适用产品、版本

表1-3 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                                 | 硬件版本                         |
|-------------------|--------------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301 软件版本, Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301 软件版本, Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本                    | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本                    | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本                    | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100 软件版本, Release 6300 软件版本 | 全系列硬件版本                      |

| 产品                | 软件版本              | 硬件版本    |
|-------------------|-------------------|---------|
| S3500-EA 系列以太网交换机 | Release 5303 软件版本 | 全系列硬件版本 |

#### 1.4.4 配置过程和解释

##### (1) 配置 Device C

# 设置为广播服务器，从 Vlan-interface2 发送广播消息包

```
<DeviceC> system-view
[DeviceC] interface Vlan-interface 2
[DeviceC-Vlan-interface2] ntp-service broadcast-server
```

##### (2) 配置 Device A

# 设置为广播客户端，从 Vlan-interface2 监听广播消息

```
<DeviceA> system-view
[DeviceA] interface Vlan-interface 2
[DeviceA-Vlan-interface2] ntp-service broadcast-client
```

##### (3) 配置 Device D

# 设置为广播客户端，从 Vlan-interface2 监听广播消息

```
<DeviceD> system-view
[DeviceD] interface Vlan-interface 2
[DeviceD-Vlan-interface2] ntp-service broadcast-client
```

#### 1.4.5 完整配置

- Device C 上的配置

```
#
interface Vlan-interface2
ip address 3.0.1.13 255.255.255.0
ntp-service broadcast-server
```

- Device A 上的配置

```
#
interface Vlan-interface2
ip address 3.0.1.11 255.255.255.0
ntp-service broadcast-client
```

- Device D 上的配置

```
#
interface Vlan-interface2
ip address 3.0.1.14 255.255.255.0
ntp-service broadcast-client
```

#### 1.4.6 配置注意事项

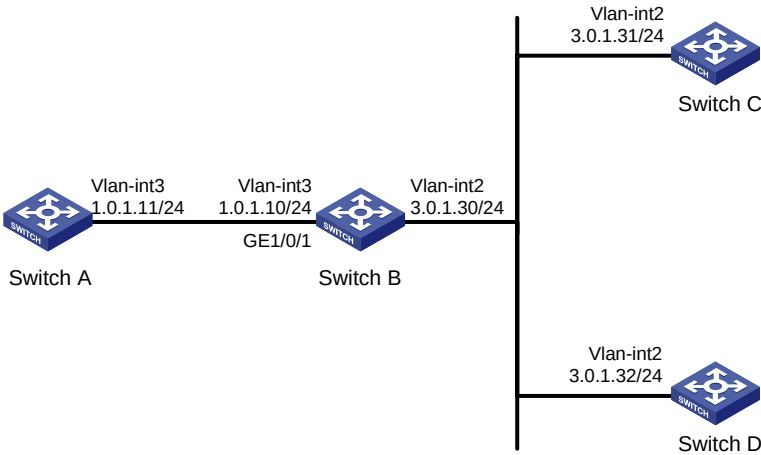
- (1) S7500E 系列以太网交换机支持设置本身时钟作为参考时钟；
- (2) S3610/S5510/S5500-SI/S5500-EI 系列以太网交换机均不支持设置本身时钟为参考时钟，只有当其时钟被同步后，才能作为时钟源去同步其他设备。



# 1.5 NTP 组播模式典型配置指导

## 1.5.1 组网图

图1-4 配置 NTP 组播模式组网图



## 1.5.2 应用要求

- Switch C 设置本地时钟作为参考时钟，层数为 2；
- Switch C 工作在组播服务器模式，从 VLAN 接口 2 向外发送组播报文；
- Switch A 和 Switch D 工作在组播客户端模式，Switch A 从 VLAN 接口 3 监听组播报文，Switch D 从 VLAN 接口 2 监听组播报文。

## 1.5.3 适用产品、版本

表1-4 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                                 | 硬件版本                         |
|-------------------|--------------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301 软件版本, Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301 软件版本, Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本                    | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本                    | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本                    | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100 软件版本, Release 6300 软件版本 | 全系列硬件版本                      |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本                    | 全系列硬件版本                      |

## 1.5.4 配置过程和解释

### (1) 配置 Switch C

# 设置本地时钟作为参考时钟，层数为 2。

```
<SwitchC> system-view
```

```
[SwitchC] ntp-service refclock-master 2
```

# 设置 Switch C 为组播服务器，从 VLAN 接口 2 发送组播报文。

```
[SwitchC] interface vlan-interface 2
```

```
[SwitchC-Vlan-interface2] ntp-service multicast-server
```

## (2) 配置 Switch D

# 设置 Switch D 为组播客户端，从 VLAN 接口 2 监听组播报文。

```
<SwitchD> system-view
```

```
[SwitchD] interface vlan-interface 2
```

```
[SwitchD-Vlan-interface2] ntp-service multicast-client
```

## (3) 配置 Switch B

由于 Switch A 与 Switch C 不在同一网段，所以 Switch B 上需要配置组播功能，否则 Switch A 收不到 Switch C 发出的组播报文。

# 配置组播功能。

```
<SwitchB> system-view
```

```
[SwitchB] multicast routing-enable
```

```
[SwitchB] interface vlan-interface 2
```

```
[SwitchB-Vlan-interface2] pim dm
```

```
[SwitchB-Vlan-interface2] quit
```

```
[SwitchB] vlan 3
```

```
[SwitchB-vlan3] port GigabitEthernet 1/0/1
```

```
[SwitchB-vlan3] quit
```

```
[SwitchB] interface vlan-interface 3
```

```
[SwitchB-Vlan-interface3] igmp enable
```

```
[SwitchB-Vlan-interface3] quit
```

```
[SwitchB] interface GigabitEthernet 1/0/1
```

```
[SwitchB-GigabitEthernet1/0/1] igmp-snooping static-group 224.0.1.1 vlan 3
```

## (4) 配置 Switch A

```
<SwitchA> system-view
```

```
[SwitchA] interface vlan-interface 3
```

# 设置 Switch A 为组播客户端，从 VLAN 接口 3 监听组播报文。

```
[SwitchA-Vlan-interface3] ntp-service multicast-client
```

## 1.5.5 完整配置

- Switch A 上的配置

```
#
```

```
interface Vlan-interface3
```

```
ntp-service multicast-client
```

- Switch B 上的配置

```
#
```

```
multicast routing-enable
```

```
#
```

```
interface Vlan-interface2
```

```
pim dm
```

```
#
interface Vlan-interface3
 igmp enable
#
interface GigabitEthernet1/0/1
 port access vlan 3
 igmp-snooping static-group 224.0.1.1 vlan 3
```

- Switch C 上的配置

```
#
ntp-service refclock-master 2
#
interface Vlan-interface2
 ntp-service multicast-server
```

- Switch D 上的配置

```
#
interface Vlan-interface2
 ntp-service multicast-client
```

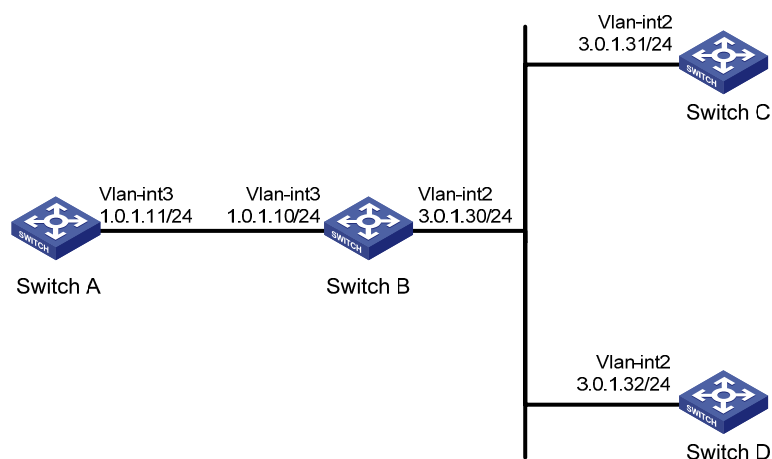
### 1.5.6 配置注意事项

- (1) S7500E 系列以太网交换机支持设置本身时钟作为参考时钟；
- (2) S3610/S5510/S5500-SI/S5500-EI 系列以太网交换机均不支持设置本身时钟为参考时钟，只有当其时钟被同步后，才能作为时钟源去同步其他设备；
- (3) S5500-SI 系列以太网交换机由于不支持三层组播功能，所以在本举例中不能充当 Switch B。

## 1.6 带身份验证的 NTP 广播模式典型配置指导

### 1.6.1 组网图

图1-5 配置带身份验证的 NTP 广播模式组网图



### 1.6.2 应用要求

- Switch C 设置本地时钟作为参考时钟，层数为 3；
- Switch C 工作在广播服务器模式，从 VLAN 接口 2 向外发送广播报文；

- Switch D 工作在广播客户端模式，从 VLAN 接口 2 监听广播报文；
- 同时在 Switch C 和 Switch D 上配置 NTP 验证。

### 1.6.3 适用产品、版本

表1-5 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                                 | 硬件版本                         |
|-------------------|--------------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301 软件版本, Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301 软件版本, Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本                    | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本                    | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本                    | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100 软件版本, Release 6300 软件版本 | 全系列硬件版本                      |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本                    | 全系列硬件版本                      |

### 1.6.4 配置过程和解释

#### (1) 配置 Switch C

# 设置本地时钟作为参考时钟，层数为 3。

```
<SwitchC> system-view
```

```
[SwitchC] ntp-service refclock-master 3
```

# 配置 NTP 验证。

```
[SwitchC] ntp-service authentication enable
```

```
[SwitchC] ntp-service authentication-keyid 88 authentication-mode md5 123456
```

```
[SwitchC] ntp-service reliable authentication-keyid 88
```

# 设置 Switch C 为 NTP 广播服务器并指定密钥编号。

```
[SwitchC] interface vlan-interface 2
```

```
[SwitchC-Vlan-interface2] ntp-service broadcast-server authentication-keyid 88
```

#### (2) 配置 Switch D

# 配置 NTP 验证。

```
<SwitchD> system-view
```

```
[SwitchD] ntp-service authentication enable
```

```
[SwitchD] ntp-service authentication-keyid 88 authentication-mode md5 123456
```

```
[SwitchD] ntp-service reliable authentication-keyid 88
```

# 设置 Switch D 为 NTP 广播客户端。

```
[SwitchD] interface vlan-interface 2
```

```
[SwitchD-Vlan-interface2] ntp-service broadcast-client
```

## 1.6.5 完整配置

- Switch C 上的配置

```
#
interface Vlan-interface2
 ntp-service broadcast-server authentication-keyid 88
#
ntp-service authentication enable
ntp-service authentication-keyid 88 authentication-mode md5 OUM!K%F<+${Q=^Q`MAF4<1!!
ntp-service reliable authentication-keyid 88
ntp-service refclock-master 3
#
```

- Switch D 上的配置

```
#
interface Vlan-interface2
 ntp-service broadcast-client
#
ntp-service authentication enable
ntp-service authentication-keyid 88 authentication-mode md5 OUM!K%F<+${Q=^Q`MAF4<1!!
ntp-service reliable authentication-keyid 88
#
```

## 1.6.6 配置注意事项

- (1) S7500E 系列以太网交换机支持设置本身时钟作为参考时钟；
- (2) S3610/S5510/S5500-SI/S5500-EI 系列以太网交换机均不支持设置本身时钟为参考时钟，只有当其时钟被同步后，才能作为时钟源去同步其他设备。

# 目 录

|                         |     |
|-------------------------|-----|
| 1 FTP-TFTP典型配置指导 .....  | 1-1 |
| 1.1 FTP客户端典型配置指导 .....  | 1-1 |
| 1.1.1 组网图 .....         | 1-1 |
| 1.1.2 应用要求 .....        | 1-1 |
| 1.1.3 适用产品、版本 .....     | 1-1 |
| 1.1.4 配置过程和解释 .....     | 1-2 |
| 1.1.5 完整配置 .....        | 1-3 |
| 1.1.6 配置注意事项 .....      | 1-3 |
| 1.2 FTP服务器典型配置指导 .....  | 1-3 |
| 1.2.1 组网图 .....         | 1-3 |
| 1.2.2 应用要求 .....        | 1-3 |
| 1.2.3 适用产品、版本 .....     | 1-3 |
| 1.2.4 配置过程和解释 .....     | 1-4 |
| 1.2.5 完整配置 .....        | 1-5 |
| 1.2.6 配置注意事项 .....      | 1-5 |
| 1.3 TFTP客户端典型配置指导 ..... | 1-6 |
| 1.3.1 组网图 .....         | 1-6 |
| 1.3.2 应用要求 .....        | 1-6 |
| 1.3.3 适用产品、版本 .....     | 1-6 |
| 1.3.4 配置过程和解释 .....     | 1-6 |
| 1.3.5 完整配置 .....        | 1-7 |
| 1.3.6 配置注意事项 .....      | 1-7 |

# 1 FTP-TFTP 典型配置指导



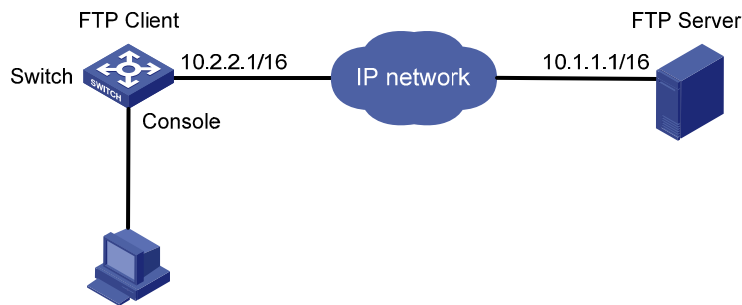
## 说明

本节中的所有配置均基于 FTP/TFTP 客户端和服务端路由可达的条件下进行，相关的 IP 地址和路由协议的配置请用户参考本手册相关章节的介绍，本节中不再赘述。

## 1.1 FTP 客户端典型配置指导

### 1.1.1 组网图

图1-1 FTP 客户端组网示意图



### 1.1.2 应用要求

如图 1-1所示：

- 设备作为 FTP 客户端，从 FTP 服务器上下载新的启动文件。
- FTP 服务器的 IP 地址为 10.1.1.1/16。
- 服务器上已设置设备登录 FTP 服务器的用户名为 abc，密码为 pwd。设备以用户名 abc、密码 pwd 登录 FTP 服务器。

### 1.1.3 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本                         |
|-------------------|---------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本               | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本               | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本                      |

| 产品                | 软件版本              | 硬件版本    |
|-------------------|-------------------|---------|
| S3500-EA 系列以太网交换机 | Release 5303 软件版本 | 全系列硬件版本 |

#### 1.1.4 配置过程和解释

# 删除设备中的多余文件，以保证剩余足够的空间，用于存储新的启动文件。

```
<Sysname> dir
```

```
Directory of flash:/
```

```

 0 drw- - Dec 07 2005 10:00:57 filename
 1 drw- - Jan 02 2006 14:27:51 logfile
 2 -rw- 1216 Jan 02 2006 14:28:59 config.cfg
 3 -rw- 1216 Jan 02 2006 16:27:26 backup.cfg
```

```
31496 KB total (12133 KB free)
```

```
<Sysname> delete /unreserved flash:/backup.cfg
```

# 以 FTP 方式登录服务器，获取系统启动文件。

```
<Sysname> ftp 10.1.1.1
```

```
Trying 10.1.1.1 ...
```

```
Press CTRL+K to abort
```

```
Connected to 10.1.1.1.
```

```
220 FTP service ready.
```

```
User(10.1.1.1:(none)):abc
```

```
331 Password required for abc.
```

```
Password:
```

```
230 User logged in.
```

```
[ftp] binary
```

```
200 Type set to I.
```

```
[ftp] get aaa.bin bbb.bin
```

```
227 Entering Passive Mode (10.1.1.1,4,1).
```

```
125 BINARY mode data connection already open, transfer starting for aaa.bin.
```

```
.....226 Transfer complete.
```

```
FTP: 5805100 byte(s) received in 19.898 second(s) 291.74 byte(s)/sec.
```

```
[ftp] bye
```

# 用户可以通过 **boot-loader** 命令来指定获取的文件为下次启动时的主用启动文件，重启设备后，实现设备启动文件的升级。

```
<Sysname> boot-loader file bbb.bin main
```

```
<Sysname> reboot
```





#### 注意

- **boot-loader** 命令指定的下次启动时的启动文件必须存放在设备的根目录下。可使用文件的拷贝或移动操作来调整文件的路径为根目录。该命令的详细介绍请参见各产品命令手册的“系统维护与调试”部分。
- 对于 S7500E 系列交换机，启动文件的扩展名为“.app”。
- 为 S7500E 系列交换机指定主用启动文件时，**boot-loader** 命令中需要指定槽位编号，例如“**boot-loader file bbb.app slot 1 main**”。

### 1.1.5 完整配置

本配置指导中使用的均为一次性生效的命令，不会保存到配置文件中，不涉及完整配置。

### 1.1.6 配置注意事项

- FTP 传输文件有两种模式：一种是二进制（binary）模式，用于传输程序文件；另一种是 ASCII 码模式，用于传输文本文件。
- S3610&S5510 系列交换机不支持指定启动文件的主用/备用属性。

## 1.2 FTP 服务器典型配置指导

### 1.2.1 组网图

图1-2 FTP 服务器组网示意图



### 1.2.2 应用要求

如图 1-2所示：

- 应用要求设备作为 FTP 服务器，客户端上传新的启动文件。
- 设备以太网接口的 IP 地址为 1.1.1.1/16。
- 客户端登录 FTP 服务器的用户名为 abc，密码为 pwd。
- PC 作为 FTP 客户端。

### 1.2.3 适用产品、版本

表1-2 配置适用的产品与软硬件版本关系

| 产品             | 软件版本                            | 硬件版本    |
|----------------|---------------------------------|---------|
| S3610 系列以太网交换机 | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5510 系列以太网交换机 | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |

| 产品                | 软件版本                            | 硬件版本                         |
|-------------------|---------------------------------|------------------------------|
| S5500-SI 系列以太网交换机 | Release 1207 软件版本               | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本               | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本                      |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本                      |

#### 1.2.4 配置过程和解释

- 配置 Device (FTP Server)

# 在设备上添加一个本地用户 abc，并设置其认证密码为 pwd。

```
<Sysname> system-view
```

```
[Sysname] local-user abc
```

```
[Sysname-luser-abc] password simple pwd
```

# 指定 abc 可以使用的服务类型为 FTP，并设置其授权访问目录。

```
[Sysname-luser-abc] service-type ftp
```

```
[Sysname-luser-abc] work-directory flash:/
```

# 配置 abc 的用户级别为 3 级，使其可以向访问目录中上传文件。

```
[Sysname-luser-abc] level 3
```

```
[Sysname-luser-abc] quit
```

# 启动设备的 FTP 服务。

```
[Sysname] ftp server enable
```

```
[Sysname] quit
```

# 删除设备中的多余文件，以保证剩余足够的空间，用于存储新的启动文件。

```
<Sysname> dir
```

```
Directory of flash:/
```

```
 0 drw- - Dec 07 2005 10:00:57 filename
 1 drw- - Jan 02 2006 14:27:51 logfile
 2 -rw- 1216 Jan 02 2006 14:28:59 config.cfg
 3 -rw- 1216 Jan 02 2006 16:27:26 back.cfg
 4 drw- - Jan 02 2006 15:20:21 ftp
```

```
31496 KB total (12133 KB free)
```

```
<Sysname> delete /unreserved flash:/back.cfg
```

- 配置 PC (FTP Client)

# 以 FTP 方式登录 FTP 服务器，上传启动文件，并存放于 FTP 服务器的根目录下。

```
c:\> ftp 1.1.1.1
```

```
Connected to 1.1.1.1.
```

```
220 FTP service ready.
```

```
User(1.1.1.1:(none)):abc
```

```
331 Password required for abc.
```

```
Password:
230 User logged in.
ftp> put aaa.bin bbb.bin
200 Port command okay.
150 Opening BINARY mode data connection for bbb.bin.
226 Transfer complete.
ftp: 发送 2737556 字节, 用时 7.02Seconds 390.24Kbytes/sec.
ftp>
```

# 用户可以通过 **boot-loader** 命令来指定上传的程序为下次启动时的主用启动文件（假设本例中的设备支持启动文件的主备用属性），重启设备后，实现设备启动文件的升级。

```
<Sysname> boot-loader file bbb.bin
<Sysname> reboot
```



#### 注意

- **boot-loader** 命令指定的下次启动时的启动文件必须存放在设备的根目录下。可使用文件的拷贝或移动操作来调整文件的路径为根目录。该命令的详细介绍请参见本手册“系统维护与调试操作”。
  - 对于 S7500E 系列交换机，启动文件的扩展名为“.app”。
  - 为 S7500E 系列交换机指定主用启动文件时，**boot-loader** 命令中需要指定槽位编号，例如“**boot-loader file bbb.app slot 1 main**”。
- 



#### 说明

- 利用 FTP 功能升级配置文件时，操作步骤与上述介绍完全一致，需要注意的是获取后的配置文件同样要放在设备的根目录下。
  - 利用 FTP 远程升级 Bootrom 程序，文件传送完成后再执行 **bootrom update** 命令来更新系统配置。
- 

### 1.2.5 完整配置

```
#
ftp server enable
#
local-user ftp
password simple ftp
work-directory flash:/
level 3
service-type ftp
#
```

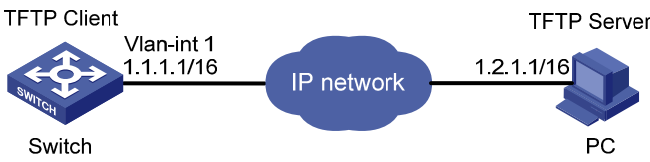
### 1.2.6 配置注意事项

设备作为 FTP 服务器时，对客户端的访问操作有级别限制：如果要对设备的文件系统执行写操作（比如上传、删除、创建/删除文件夹），则必须将 FTP 登录用户的级别设置为 3；如果执行其它操作（比如普通的查看操作），则 FTP 登录用户的级别不受限制，可以为 0~3 中的任意级别。

# 1.3 TFTP 客户端典型配置指导

## 1.3.1 组网图

图1-3 TFTP 客户端组网示意图



## 1.3.2 应用要求

如图 1-3所示：

- 设备作为 TFTP 客户端，PC 作为 TFTP 服务器
- PC 的 IP 地址为 1.2.1.1/16，在 PC 上已经配置了 TFTP 的工作路径。
- 设备上 VLAN 接口 1 的 IP 地址为 1.1.1.1/16，设备和 PC 相连的端口属于该 VLAN。
- 设备通过 TFTP 协议从 TFTP 服务器上下载启动文件，同时将设备的配置文件 config.cfg 上传到 TFTP 服务器的工作目录实现配置文件的备份。

## 1.3.3 适用产品、版本

表1-3 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本                         |
|-------------------|---------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本               | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本               | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本                      |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本                      |

## 1.3.4 配置过程和解释

- 配置 PC（TFTP 服务器），包括启动 TFTP 服务器并设置工作目录，具体配置步骤略
- 配置交换机（TFTP 客户端）



注意

如果设备的内存空间不够大，请删除内存中原有的应用程序然后再下载新的应用程序到设备的内存中。

# 将应用程序 **aaa.bin** 从 TFTP 服务器上下载到设备。

```
<Sysname> tftp 1.2.1.1 get aaa.bin bbb.bin
```

# 将设备的配置文件 **config.cfg** 上传到 TFTP 服务器。

```
<Sysname> tftp 1.2.1.1 put config.bin configback.bin
```

# 用户可以通过 **boot-loader** 命令来指定下载的程序为下次启动时的主用启动文件（假设本例中的设备支持启动文件的主备用属性），然后重启设备，实现设备启动文件的升级。

```
<Sysname> boot-loader file bbb.bin main
```

```
<Sysname> reboot
```

---



注意

- **boot-loader** 命令指定的下次启动时的启动文件必须存放在设备的根目录下。可使用文件的拷贝或移动操作来调整文件的路径为根目录。该命令的详细介绍请参见本手册“系统维护与调试操作”。
  - 对于 S7500E 系列交换机，启动文件的扩展名为“.app”。
  - 为 S7500E 系列交换机指定主用启动文件时，**boot-loader** 命令中需要指定槽位编号，例如“**boot-loader file bbb.app slot 1 main**”。
- 

### 1.3.5 完整配置

本配置指导中使用的均为一次性生效的命令，不会保存到配置文件中，不涉及完整配置。

### 1.3.6 配置注意事项

无

# 目 录

- 1 UDP Helper典型配置指导 ..... 1-1
  - 1.1 UDP Helper典型配置指导 ..... 1-1
    - 1.1.1 组网图 ..... 1-1
    - 1.1.2 应用要求 ..... 1-1
    - 1.1.3 适用产品、版本 ..... 1-1
    - 1.1.4 配置过程和解释 ..... 1-2
    - 1.1.5 完整配置 ..... 1-2
    - 1.1.6 配置注意事项 ..... 1-2

# 1 UDP Helper 典型配置指导

## 1.1 UDP Helper 典型配置指导

网络中的主机有时需要通过发送广播报文，来获得网络配置或查询网络中其他设备的名称。但是，当主机与服务器或待查询的设备不在同一个广播域时，主机就无法获得所需要的信息。

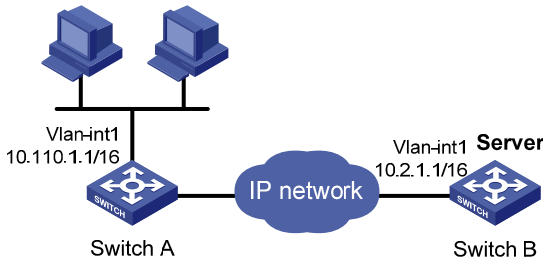
为解决上述问题，以太网交换机提供了 UDP Helper 功能。通过该功能可以实现对指定 UDP 端口的 IP 广播报文进行中继转发，即将指定 UDP 端口的广播报文转换为单播报文发送给指定的目的服务器，起到中继的作用。

使能 UDP Helper 功能后，如果设备接收到广播报文，将根据报文的 UDP 目的端口号来判断是否要对其中继转发，并进行相应的处理：

- 如果报文的 UDP 目的端口号与配置的需要中继转发的 UDP 端口号匹配，则修改 IP 报文头的目的 IP 地址，将报文发给指定的目的服务器；
- 否则，直接将报文送给上层协议处理。

### 1.1.1 组网图

图1-1 UDP Helper 组网示意图



### 1.1.2 应用要求

Switch A 的 VLAN 接口 1 的 IP 地址为 10.110.1.1/16，连接到网段 10.110.0.0/16。配置将目的 UDP 端口号为 55 的广播报文中继转发到指定的目的服务器 10.2.1.1/16。

### 1.1.3 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                                | 硬件版本                         |
|-------------------|-------------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301 软件版本，Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301 软件版本，Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本                   | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本                   | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本                   | 全系列硬件版本                      |

| 产品                | 软件版本              | 硬件版本    |
|-------------------|-------------------|---------|
| S7500E 系列以太网交换机   | Release 6300 软件版本 | 全系列硬件版本 |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本 | 全系列硬件版本 |

#### 1.1.4 配置过程和解释

在开始下面的配置之前，需确保 Switch A 到 10.2.0.0 网段路由可达。

# 在 Switch A 上使能 UDP Helper 功能。

```
<SwitchA> system-view
```

```
[SwitchA] udp-helper enable
```

# 配置将目的 UDP 端口号为 55 的广播报文进行中继转发。

```
[SwitchA] udp-helper port 55
```

# 配置中继转发的目的服务器为 10.2.1.1。

```
[SwitchA] interface vlan-interface 1
```

```
[SwitchA-Vlan-interface1] ip address 10.110.1.1 16
```

```
[SwitchA-Vlan-interface1] udp-helper server 10.2.1.1
```

#### 1.1.5 完整配置

```
#
```

```
udp-helper enable
```

```
udp-helper port 55
```

```
#
```

```
interface Vlan-interface1
```

```
ip address 10.110.1.1 255.255.0.0
```

```
udp-helper server 10.2.1.1
```

```
#
```

#### 1.1.6 配置注意事项

- UDP Helper 功能不能中继转发 DHCP 广播报文，即中继转发的 UDP 端口不能配置为 67 和 68。
- S3610 和 S5510 系列以太网交换机缺省情况下禁止接收直连网段广播报文。如果要保证 UDP Helper 功能可用，须先在系统视图下配置 **ip forward-broadcast** 命令。如果 S3610 和 S5510 系列以太网交换机已配置 DHCP 功能或 NTP 广播模式，设备都会自动允许接收定向广播报文，此时不配置 **ip forward-broadcast** 命令也可以使 UDP Helper 功能生效。关于 **ip forward-broadcast** 命令详细介绍可参见相关产品手册的“IP 地址-IP 性能”中的详细介绍。
- 只有开启 UDP Helper 功能后，才能配置需要中继转发的 UDP 端口。否则，将会有错误提示信息。当关闭 UDP Helper 功能后，所有已配置的指定 UDP 端口都被取消。



# 目 录

|                                  |     |
|----------------------------------|-----|
| 1 信息中心典型配置指导.....                | 1-1 |
| 1.1 信息中心简介.....                  | 1-1 |
| 1.2 日志信息发送到Unix日志主机典型配置指导 .....  | 1-1 |
| 1.2.1 组网图.....                   | 1-1 |
| 1.2.2 应用要求 .....                 | 1-1 |
| 1.2.3 适用产品、版本 .....              | 1-1 |
| 1.2.4 配置过程和解释 .....              | 1-1 |
| 1.2.5 完整配置 .....                 | 1-2 |
| 1.2.6 配置注意事项 .....               | 1-3 |
| 1.3 日志信息发送到Linux日志主机典型配置指导 ..... | 1-3 |
| 1.3.1 组网图.....                   | 1-3 |
| 1.3.2 应用要求 .....                 | 1-3 |
| 1.3.3 适用产品、版本 .....              | 1-3 |
| 1.3.4 配置过程和解释 .....              | 1-3 |
| 1.3.5 完整配置 .....                 | 1-4 |
| 1.3.6 配置注意事项 .....               | 1-4 |
| 1.4 日志发送到控制台典型配置指导.....          | 1-5 |
| 1.4.1 组网图.....                   | 1-5 |
| 1.4.2 应用要求 .....                 | 1-5 |
| 1.4.3 适用产品、版本 .....              | 1-5 |
| 1.4.4 配置过程和解释 .....              | 1-5 |
| 1.4.5 完整配置 .....                 | 1-6 |
| 1.4.6 配置注意事项 .....               | 1-6 |

# 1 信息中心典型配置指导

## 1.1 信息中心简介

信息中心是系统的信息枢纽，它能够对所有的系统信息进行分类、管理。通过与 `debugging` 程序的结合，信息中心为网络管理员和开发人员监控网络运行情况和诊断网络故障提供了强有力的支持。

## 1.2 日志信息发送到 Unix 日志主机典型配置指导

### 1.2.1 组网图

图1-1 日志信息发送到 Unix 日志主机组网图



### 1.2.2 应用要求

交换机的日志信息发送到 Unix 日志主机上，日志主机的 IP 地址为 202.38.1.10，只允许严重性高于 `informational` 的日志信息发送到日志主机上，允许输出信息的模块为 `ARP` 和 `IP`。

### 1.2.3 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                                 | 硬件版本                         |
|-------------------|--------------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301 软件版本, Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301 软件版本, Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本                    | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本                    | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本                    | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100 软件版本, Release 6300 软件版本 | 全系列硬件版本                      |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本                    | 全系列硬件版本                      |

### 1.2.4 配置过程和解释

- 交换机上的配置

# 开启信息中心。

```
<Sysname> system-view
```

```
[Sysname] info-center enable
```

# 缺省情况下，系统向 loghost 通道输出所有模块的系统信息。为了得到 ARP 和 IP 模块的系统信息，需首先关闭所有模块向日志主机通道输出信息的功能。

```
[Sysname] undo info-center source default channel loghost
```

# 将 IP 地址为 202.38.1.10 的主机用作日志主机，只允许严重等级高于或等于 informational 的日志信息输出至日志主机，允许输出信息的模块为 ARP 和 IP。

```
[Sysname] info-center loghost 202.38.1.10 facility local4
```

```
[Sysname] info-center source arp channel loghost log level informational debug state off trap state off
```

```
[Sysname] info-center source ip channel loghost log level informational debug state off trap state off
```

- 日志主机上的配置

下面的配置示例是在 SunOS 4.0 上完成的，在其它厂商的 Unix 操作系统上的配置操作基本与之相似。

# 以超级用户（root）的身份执行以下命令。

```
mkdir /var/log/Sysname
```

```
touch /var/log/Sysname/information
```

# 以超级用户（root）的身份编辑文件/etc/syslog.conf，加入以下选择/动作组合（selector/action pairs）。

```
Sysname configuration messages
```

```
local4.info /var/log/Sysname/information
```

# 当日志文件 information 建立且/etc/syslog.conf 文件被修改了之后，应通过执行以下命令给系统守护进程 syslogd 一个 HUP 信号来使 syslogd 重新读取它的配置文件/etc/syslog.conf。

```
ps -ae | grep syslogd
```

```
147
```

```
kill -HUP 147
```

## 1.2.5 完整配置

- 交换机上的配置

```
#
```

```
info-center source ARP channel 2 trap state off
```

```
info-center source IP channel 2 trap state off
```

```
undo info-center source default channel 2
```

```
info-center loghost 202.38.1.10 facility local4
```

- 日志主机上的配置

```
#
```

```
mkdir /var/log/Sysname
```

```
touch /var/log/Sysname/information
```

```
Sysname configuration messages
```

```
local4.info /var/log/Sysname/information
```

```
#
```

```
ps -ae | grep syslogd
```

```
147
```

```
kill -HUP 147
```

1.2.6 配置注意事项

在编辑/etc/syslog.conf时应注意以下问题：

- 注释只允许独立成行，并以字符# 开头。
- 选择/动作组合之间必须以一个制表符分隔，而不能输入空格。
- 在文件名之后不得有多余的空格。
- /etc/syslog.conf 中指定的设备名及接受的日志信息级别与交换机上配置的 **info-center loghost** 和 **info-center source** 命令中的相应参数应保持一致，否则日志信息可能无法正确输出到日志主机上。

1.3 日志信息发送到 Linux 日志主机典型配置指导

1.3.1 组网图

图1-2 日志信息发送到 Linux 日志主机组网图



1.3.2 应用要求

交换机的日志信息发送到 Linux 日志主机上，日志主机的 IP 地址为 202.38.1.10，只允许严重性高于 errors 的日志信息发送到日志主机上，允许输出信息的模块为所有模块。

1.3.3 适用产品、版本

表1-2 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                                 | 硬件版本                         |
|-------------------|--------------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301 软件版本, Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301 软件版本, Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本                    | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本                    | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本                    | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100 软件版本, Release 6300 软件版本 | 全系列硬件版本                      |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本                    | 全系列硬件版本                      |

1.3.4 配置过程和解释

- 交换机上的配置

# 开启信息中心。

<Sysname> system-view

```
[Sysname] info-center enable
```

# 将 IP 地址为 202.38.1.10 的主机用作日志主机，只允许严重等级高于或等于 errors 的日志信息输出至日志主机，允许输出信息的模块为所有模块。

```
[Sysname] info-center loghost 202.38.1.10 facility local7
```

```
[Sysname] info-center source default channel loghost log level errors debug state off trap state off
```

- 日志主机上的配置

# 以超级用户（root）的身份执行以下命令。

```
mkdir /var/log/Sysname
```

```
touch /var/log/Sysname/information
```

# 以超级用户（root）的身份编辑文件/etc/syslog.conf，加入以下选择/动作组合（selector/action pairs）。

```
Sysname configuration messages
```

```
local7.info /var/log/Sysname/information
```

# 当日志文件 information 建立且/etc/syslog.conf 文件被修改了之后，应通过执行以下命令查看系统守护进程 syslogd 的进程号，杀死 syslogd 进程，并重新用-r 选项在后台启动 syslogd。

```
ps -ae | grep syslogd
```

```
147
```

```
kill -9 147
```

```
syslogd -r &
```

### 1.3.5 完整配置

- 交换机上的配置

```
#
```

```
info-center source default channel 2 log level error trap state off
```

```
info-center loghost 202.38.1.10
```

- 日志主机上的配置

```
#
```

```
mkdir /var/log/Sysname
```

```
touch /var/log/Sysname/information
```

```
Sysname configuration messages
```

```
local7.info /var/log/Sysname/information
```

```
#
```

```
ps -ae | grep syslogd
```

```
147
```

```
kill -9 147
```

```
syslogd -r &
```

### 1.3.6 配置注意事项

对 Linux 日志主机，必须保证 syslogd 进程是以-r 选项启动。

在编辑/etc/syslog.conf 时应注意以下问题：

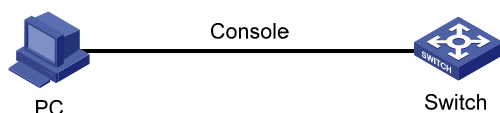
- 注释只允许独立成行，并以字符# 开头。
- 选择/动作组合之间必须以一个制表符分隔，而不能输入空格。

- 在文件名之后不得有多余的空格。
- /etc/syslog.conf 中指定的设备名及接受的日志信息级别与交换机上配置的 **info-center loghost** 和 **info-center source** 命令中的相应参数应保持一致，否则日志信息可能无法正确输出到日志主机上。

## 1.4 日志发送到控制台典型配置指导

### 1.4.1 组网图

图1-3 日志信息发送到控制台组网示意图



### 1.4.2 应用要求

交换机的严重性高于 **informational** 的日志信息将会发送到控制台上，允许输出信息的模块为 **ARP** 和 **IP**。

### 1.4.3 适用产品、版本

表1-3 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                                 | 硬件版本                         |
|-------------------|--------------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301 软件版本, Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301 软件版本, Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本                    | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本                    | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本                    | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100 软件版本, Release 6300 软件版本 | 全系列硬件版本                      |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本                    | 全系列硬件版本                      |

### 1.4.4 配置过程和解释

# 开启信息中心。

```
<Sysname> system-view
```

```
[Sysname] info-center enable
```

# 系统缺省向 **console** 通道输出所有模块的系统信息，为了得到 **ARP** 和 **IP** 模块的系统信息，需首先关闭所有模块向 **console** 通道输出信息的功能。

```
[Sysname] undo info-center source default channel console
```

# 配置控制台日志输出，只允许严重等级高于或等于 **informational** 的日志信息输出至控制台，允许输出信息的模块为 **ARP** 和 **IP**。

```
[Sysname] info-center console channel console
```

```
[Sysname] info-center source arp channel console log level informational debug state off trap
state off
```

```
[Sysname] info-center source ip channel console log level informational debug state off trap
state off
```

# 打开终端显示功能。

```
<Sysname> terminal monitor
```

```
<Sysname> terminal logging
```

#### 1.4.5 完整配置

```
#
```

```
info-center source ARP channel 0 trap state off
```

```
info-center source IP channel 0 trap state off
```

```
undo info-center source default channel 0
```

#### 1.4.6 配置注意事项

无

# 目 录

|                            |     |
|----------------------------|-----|
| 1 域名解析典型配置指导.....          | 1-1 |
| 1.1 静态域名解析典型配置指导.....      | 1-1 |
| 1.1.1 组网图.....             | 1-1 |
| 1.1.2 应用要求.....            | 1-1 |
| 1.1.3 适用产品、版本.....         | 1-1 |
| 1.1.4 配置过程和解释.....         | 1-1 |
| 1.1.5 完整配置.....            | 1-2 |
| 1.2 动态域名解析典型配置指导.....      | 1-2 |
| 1.2.1 组网图.....             | 1-2 |
| 1.2.2 应用要求.....            | 1-2 |
| 1.2.3 适用产品、版本.....         | 1-3 |
| 1.2.4 配置过程和解释.....         | 1-3 |
| 1.2.5 完整配置.....            | 1-3 |
| 1.2.6 配置注意事项.....          | 1-4 |
| 1.3 DNS proxy典型配置举例指导..... | 1-4 |
| 1.3.1 组网图.....             | 1-4 |
| 1.3.2 应用要求.....            | 1-4 |
| 1.3.3 适用产品、版本.....         | 1-5 |
| 1.3.4 配置过程和解释.....         | 1-5 |
| 1.3.5 完整配置.....            | 1-6 |
| 1.3.6 配置注意事项.....          | 1-6 |



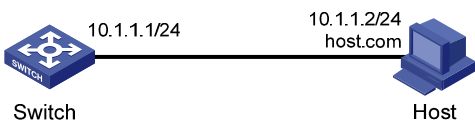
# 1 域名解析典型配置指导

## 1.1 静态域名解析典型配置指导

静态域名解析就是手工建立域名和 IP 地址之间的对应关系。当用户使用域名进行某些应用(如 telnet 应用)时，系统查找静态域名解析表，从中获取指定域名对应的 IP 地址。

### 1.1.1 组网图

图1-1 静态域名解析配置组网图



### 1.1.2 应用要求

交换机利用静态域名解析功能，实现通过主机名 host.com 访问 IP 地址为 10.1.1.2 的主机 Host。

### 1.1.3 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                                    | 硬件版本                         |
|-------------------|-----------------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301 软件版本,<br>Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301 软件版本,<br>Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本                       | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本                       | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本                       | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100 软件版本,<br>Release 6300 软件版本 | 全系列硬件版本                      |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本                       | 全系列硬件版本                      |

### 1.1.4 配置过程和解释

# 配置主机名 host.com 对应的 IP 地址为 10.1.1.2。

```
<Sysname> system-view
```

```
[Sysname] ip host host.com 10.1.1.2
```

# 执行 ping host.com 命令，Switch 通过静态域名解析可以解析到 host.com 对应的 IP 地址为 10.1.1.2。

```
[Sysname] ping host.com
```

```
 PING host.com (10.1.1.2):
```

```

56 data bytes, press CTRL_C to break
Reply from 10.1.1.2: bytes=56 Sequence=1 ttl=128 time=2 ms
Reply from 10.1.1.2: bytes=56 Sequence=2 ttl=128 time=2 ms
Reply from 10.1.1.2: bytes=56 Sequence=3 ttl=128 time=2 ms
Reply from 10.1.1.2: bytes=56 Sequence=4 ttl=128 time=2 ms
Reply from 10.1.1.2: bytes=56 Sequence=5 ttl=128 time=2 ms

--- host.com ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 2/2/2 ms

```

### 1.1.5 完整配置

```

#
ip host host.com 10.1.1.2
#

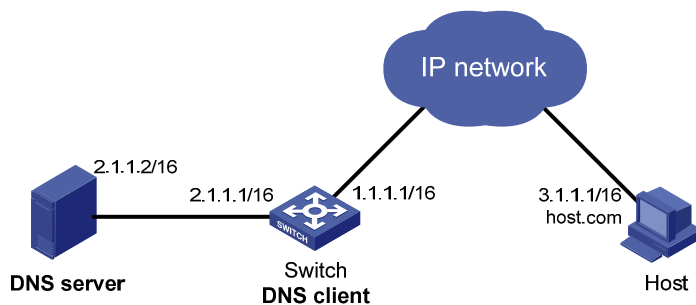
```

## 1.2 动态域名解析典型配置指导

域名系统（DNS，Domain Name System）是一种用于 TCP/IP 应用程序的分布式数据库，提供域名与 IP 地址之间的转换。通过域名系统，用户进行某些应用时，可以直接使用便于记忆的、有意义的域名，由网络中的域名解析服务器解析为正确的 IP 地址。

### 1.2.1 组网图

图1-2 动态域名解析组网图



### 1.2.2 应用要求

- 域名服务器的 IP 地址是 2.1.1.2/16，配置域名后缀为 com。
- 交换机作为 DNS 客户端，使用动态域名解析和域名后缀列表功能，实现通过输入 host 来访问域名为 host.com、IP 地址为 3.1.1.1/16 的主机 Host。

### 1.2.3 适用产品、版本

表1-2 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                                    | 硬件版本                         |
|-------------------|-----------------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301 软件版本,<br>Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301 软件版本,<br>Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本                       | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本                       | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本                       | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100 软件版本,<br>Release 6300 软件版本 | 全系列硬件版本                      |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本                       | 全系列硬件版本                      |

### 1.2.4 配置过程和解释

# 使能动态域名解析功能。

```
<Sysname> system-view
[Sysname] dns resolve
```

# 配置域名服务器的 IP 地址为 2.1.1.2。

```
[Sysname] dns server 2.1.1.2
```

# 配置域名后缀 com。

```
[Sysname] dns domain com
```

在设备上执行 **ping host** 的命令，可以 ping 通主机，且对应的目的地址为 3.1.1.1。

```
[Sysname] ping host
 Trying DNS resolve, press CTRL_C to break
Trying DNS server (2.1.1.2)
 PING host.com (3.1.1.1):
 56 data bytes, press CTRL_C to break
 Reply from 3.1.1.1: bytes=56 Sequence=1 ttl=126 time=3 ms
 Reply from 3.1.1.1: bytes=56 Sequence=2 ttl=126 time=1 ms
 Reply from 3.1.1.1: bytes=56 Sequence=3 ttl=126 time=1 ms
 Reply from 3.1.1.1: bytes=56 Sequence=4 ttl=126 time=1 ms
 Reply from 3.1.1.1: bytes=56 Sequence=5 ttl=126 time=1 ms

--- host.com ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 1/1/3 ms
```

### 1.2.5 完整配置

#

```
dns resolve
dns server 2.1.1.2
dns domain com
#
```

### 1.2.6 配置注意事项

- 在开始上面的配置之前，确保设备与主机之间的路由可达，设备和主机都已经配置完毕。
- DNS 客户端需要和域名服务器配合使用，才能根据域名解析到正确的 IP 地址。

## 1.3 DNS proxy 典型配置举例指导

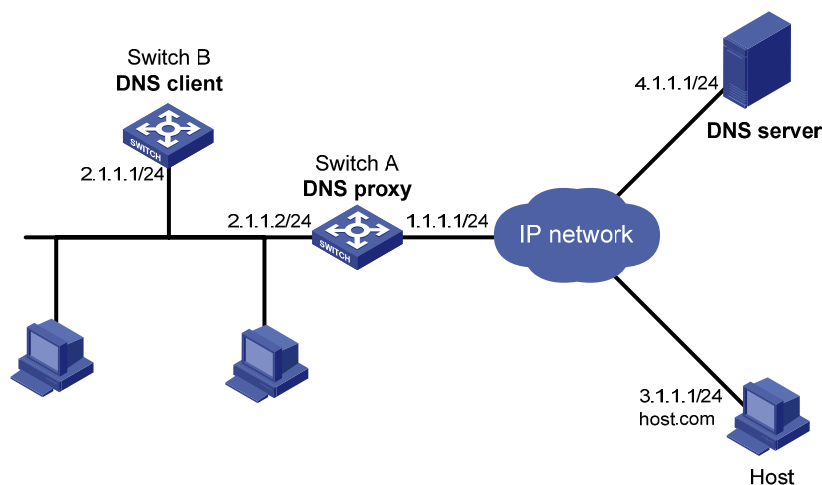
DNS 代理（DNS proxy）用来在 DNS client 和 DNS server 之间转发 DNS 请求和应答报文，代替 DNS client 进行域名解析。

局域网内的 DNS client 把 DNS proxy 当作 DNS server，将 DNS 请求报文发送给 DNS proxy。DNS proxy 将该请求报文转发到真正的 DNS server，并将 DNS server 的应答报文返回给 DNS client，从而实现域名解析。

使用 DNS proxy 功能后，当 DNS server 的地址发生变化时，只需改变 DNS proxy 上的配置，无需改变局域网内每个 DNS client 的配置，从而简化了网络管理。

### 1.3.1 组网图

图1-3 DNS proxy 组网图



### 1.3.2 应用要求

- Switch B 作为 DNS 客户端，指定域名服务器为 Switch A。
- Switch A 作为 DNS 代理。实际域名服务器的 IP 地址为 4.1.1.1。
- Switch B 通过 DNS 代理 Switch A 实现域名解析。

### 1.3.3 适用产品、版本

表1-3 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                                    | 硬件版本                         |
|-------------------|-----------------------------------------|------------------------------|
| S5500-SI 系列以太网交换机 | Release 1207 软件版本                       | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本                       | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本                       | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100 软件版本,<br>Release 6300 软件版本 | 全系列硬件版本                      |

### 1.3.4 配置过程和解释

#### (1) 配置 DNS 代理 Switch A

# 配置域名服务器的 IP 地址为 4.1.1.1。

```
<SwitchA> system-view
[SwitchA] dns server 4.1.1.1
```

# 使能 DNS proxy 功能。

```
[SwitchA] dns proxy enable
```

#### (2) 配置 DNS 客户端 Switch B

# 使能动态域名解析功能。

```
<SwitchB> system-view
[SwitchB] dns resolve
```

# 配置域名服务器的 IP 地址为 2.1.1.2。

```
[SwitchB] dns server 2.1.1.2
```

#### (3) 验证配置结果

# 在 Switch B 上执行 ping host.com 命令，可以 ping 通主机，且对应的目的地址为 3.1.1.1。

```
[SwitchB] ping host.com
Trying DNS resolve, press CTRL_C to break
Trying DNS server (2.1.1.2)
PING host.com (3.1.1.1):
 56 data bytes, press CTRL_C to break
 Reply from 3.1.1.1: bytes=56 Sequence=1 ttl=126 time=3 ms
 Reply from 3.1.1.1: bytes=56 Sequence=2 ttl=126 time=1 ms
 Reply from 3.1.1.1: bytes=56 Sequence=3 ttl=126 time=1 ms
 Reply from 3.1.1.1: bytes=56 Sequence=4 ttl=126 time=1 ms
 Reply from 3.1.1.1: bytes=56 Sequence=5 ttl=126 time=1 ms

--- host.com ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 1/1/3 ms
```

### 1.3.5 完整配置

- 配置 DNS 代理 Switch A

```
#
```

```
dns proxy enable
```

```
dns server 4.1.1.1
```

```
#
```

- 配置 DNS 客户端 Switch B

```
#
```

```
dns resolve
```

```
dns server 2.1.1.2
```

```
#
```

### 1.3.6 配置注意事项

- 在开始上面的配置之前，确保设备与主机之间的路由可达，设备和主机都已经配置完毕。
- DNS 客户端需要和域名服务器配合使用，才能根据域名解析到正确的 IP 地址。

# 目 录

- 1 文件系统管理典型配置指导 ..... 1-1
  - 1.1 文件系统管理典型配置指导 ..... 1-1
    - 1.1.1 组网图 ..... 1-1
    - 1.1.2 应用要求 ..... 1-1
    - 1.1.3 适用产品、版本 ..... 1-1
    - 1.1.4 配置过程和解释 ..... 1-1
    - 1.1.5 完整配置 ..... 1-3
    - 1.1.6 配置注意事项 ..... 1-3
  - 1.2 配置文件管理典型配置指导 ..... 1-3
    - 1.2.1 组网图 ..... 1-3
    - 1.2.2 应用要求 ..... 1-3
    - 1.2.3 适用产品、版本 ..... 1-3
    - 1.2.4 配置过程和解释 ..... 1-4
    - 1.2.5 完整配置 ..... 1-5
    - 1.2.6 配置注意事项 ..... 1-5

# 1 文件系统管理典型配置指导

## 1.1 文件系统管理典型配置指导

### 1.1.1 组网图

本节内容主要用于指导用户如何对 H3C 系列交换机的文件系统进行操作，包括拷贝/删除文件，创建/删除文件夹以及其他一些常用的配置，不涉及具体的组网需求。

### 1.1.2 应用要求

在下面的例子中，将指导用户如何利用文件系统将现有配置文件备份到其他文件夹，并在故障出现时将该配置文件进行恢复。

### 1.1.3 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本                         |
|-------------------|---------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本               | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本               | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本                      |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本                      |

### 1.1.4 配置过程和解释

#### 1. 将现有配置文件备份到其他文件夹中

# 查看当前目录下的文件及子目录。

```
<Sysname> dir
```

```
Directory of flash:/
```

```
 0 drw- - Feb 16 2006 11:45:36 logfile
 1 -rw- 1691 Feb 16 2006 11:46:19 config.cfg
 2 drw- - Feb 16 2006 15:20:27 test
 3 -rw- 184108 Feb 16 2006 15:30:20 aaa.bin
```

```
31496 KB total (10588 KB free)
```

# 创建名为 `cfg_bak` 的目录，用于备份配置文件。



```
<Sysname> mkdir cfg_bak
```

```
.
```

```
%Created dir flash:/cfg_bak.
```

# 将 Flash 目录下的 config.cfg 文件拷贝到 cfg\_bak 文件夹中。

```
<Sysname> copy config.cfg flash:/cfg_bak
```

```
Copy flash:/config.cfg to flash:/cfg_bak/config.cfg?[Y/N]:y
```

```
..
```

```
%Copy file flash:/config.cfg to flash:/cfg_bak/config.cfg...Done.
```

```
<Sysname>
```

# 进入 cfg\_bak 目录，并查看当前工作目录。

```
<Sysname> cd cfg_bak
```

```
<Sysname> pwd
```

```
flash:/cfg_bak
```

# 查看当前目录下的文件及子目录。

```
<Sysname> dir
```

```
Directory of flash:/cfg_bak/
```

```
0 -rw- 1691 Apr 26 2007 18:32:23 config.cfg
```

```
31496 KB total (10588 KB free)
```

# 将该文件重命名为 cfg\_20080210.cfg，用于标识备份时间，并使用 **dir** 命令进行确认。

```
<Sysname> rename config.cfg cfg_20080210.cfg
```

```
Rename flash:/cfg_bak/config.cfg to flash:/cfg_bak/cfg_20080210.cfg?[Y/N]:y
```

```
.
```

```
%Renamed file flash:/cfg_bak/config.cfg to flash:/cfg_bak/cfg_20080210.cfg.
```

```
<Sysname> dir
```

```
Directory of flash:/cfg_bak/
```

```
0 -rw- 1691 Apr 26 2000 18:52:03 cfg_20080210.cfg
```

```
31496 KB total (10588 KB free)
```

2. 在配置出现错误时，将备份的配置文件进行恢复，以便迅速恢复网络畅通。

# 返回上一级目录。

```
<Sysname> cd ..
```

# 显示当前的工作路径。

```
<Sysname> pwd
```

```
flash:/
```

# 将现有配置文件另存为 cfg\_temp，保存到 cfg\_bak 文件夹中。

```
<Sysname> copy config.cfg flash:/cfg_bak/cfg_temp.cfg
```

```
Copy flash:/config.cfg to flash:/cfg_bak/cfg_temp.cfg?[Y/N]:y
```

```
...
```

```
%Copy file flash:/config.cfg to flash:/cfg_bak/cfg_temp.cfg...Done.
```

# 将 Flash 目录下的 config.cfg 文件彻底删除。

```
<Sysname> delete /unreserved config.cfg
```

```
The contents cannot be restored!!! Delete flash:/config.cfg?[Y/N]:y
```

```
Deleting a file permanently will take a long time. Please wait...
```

```
..
```

```
%Delete file flash:/config.cfg...Done.

将 cfg_bak 目录中备份的 cfg_20080210.cfg 文件恢复到 Flash 根目录中，并重命名为 config.cfg。

<Sysname> copy flash:/cfg_bak/cfg_20080210.cfg flash:/config.cfg
Copy flash:/cfg_bak/cfg_20080210.cfg to flash:/config.cfg?[Y/N]:y
...
%Copy file flash:/cfg_bak/cfg_20080210.cfg to flash:/config.cfg...Done.

使用 dir 命令确认配置文件已恢复成功。

<Sysname> dir
Directory of flash:/
 0 drw- - Feb 16 2006 11:45:36 logfile
 1 -rw- 1691 Feb 16 2006 12:15:19 config.cfg
 2 drw- - Feb 16 2006 15:20:27 test
 3 -rw- 184108 Feb 16 2006 15:30:20 aaa.bin
31496 KB total (10588 KB free)
```



#### 说明

用户也可以在不删除错误的 config.cfg 文件的情况下，直接使用 **copy** 命令将备份的配置文件进行恢复，系统会在拷贝时提示用户是否进行覆盖，选择覆盖即可。

### 1.1.5 完整配置

本配置指导中使用的均为一次性生效的命令，不会保存到配置文件中，不涉及完整配置。

### 1.1.6 配置注意事项

无

## 1.2 配置文件管理典型配置指导

### 1.2.1 组网图

本节内容主要用于指导用户如何对 H3C 系列交换机的配置进行保存，以及对配置文件的清除、远程备份等相关操作，不涉及具体的组网需求。

### 1.2.2 应用要求

在下面的例子中，将指导用户如何进行配置文件的保存、远程备份，以及指定下次启动时使用的配置文件等相关操作。

### 1.2.3 适用产品、版本

表1-2 配置适用的产品与软硬件版本关系

| 产品             | 软件版本                            | 硬件版本    |
|----------------|---------------------------------|---------|
| S3610 系列以太网交换机 | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5510 系列以太网交换机 | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |

| 产品                | 软件版本                            | 硬件版本                         |
|-------------------|---------------------------------|------------------------------|
| S5500-SI 系列以太网交换机 | Release 1207 软件版本               | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本               | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本                      |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本                      |

## 1.2.4 配置过程和解释

### 1. 将现有配置保存并进行远程备份

# 将现有配置进行保存，使用缺省文件名 **config.cfg** 并覆盖现有配置文件。

```
<Sysname> save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/config.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/config.cfg exists, overwrite? [Y/N]:y

Validating file. Please wait...
Now saving current configuration to the device.
Saving configuration flash:/config.cfg. Please wait...
.....
Configuration is saved to flash successfully.

将该配置文件备份到 TFTP 服务器（IP 地址为 192.168.0.4）上。

<Sysname> backup startup-configuration to 192.168.0.4
Backup next startup-configuration file to 192.168.0.4, please wait...
finished!
```



#### 说明

- 关于 TFTP 服务器的目录和相关权限设置，请参见 TFTP 服务器软件的使用说明。
- 在备份前，请确认交换机与 TFTP 服务器路由可达，以确保备份正常进行。
- 建议用户在备份完成后，到 TFTP 服务器的工作目录下查找备份的配置文件，确认备份效果。

### 2. 在设备上保存多个配置文件并指定下次启动时使用的配置文件

# 在进行一系列配置后，将配置另存为 **config\_new.cfg** 进行保存，并指定该配置文件的 **backup** 属性。

```
<Sysname> save backup
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/config.cfg]
(To leave the existing filename unchanged, press the enter key):config_new.cfg

Validating file. Please wait...
```

```
Now saving current configuration to the device.
Saving configuration flash:/config_new.cfg. Please wait...
.....
Configuration is saved to flash successfully.
指定 config.cfg 作为下次启动时使用的配置文件。
<Sysname> startup saved-configuration config.cfg main
```

---



#### 说明

S7500E 系列交换机不支持配置文件的主用或备用属性，即在配置下次启动使用的配置文件时不能输入 **main** 或 **backup** 参数。

---

# 如果当前启动的配置文件（config.cfg）出现问题，用户可以从 TFTP 服务器上将备份的配置文件进行恢复。

```
<Sysname> restore startup-configuration from 192.168.0.4 config.cfg
Configuration file config.cfg already exists. Overwrite? [Y/N]:y
Restore next startup-configuration file from 192.168.0.4. Please wait.....
finished!
```

### 1.2.5 完整配置

本配置指导中使用的均为一次性生效的命令，不会保存到配置文件中，不涉及完整配置。

### 1.2.6 配置注意事项

无

# 目 录

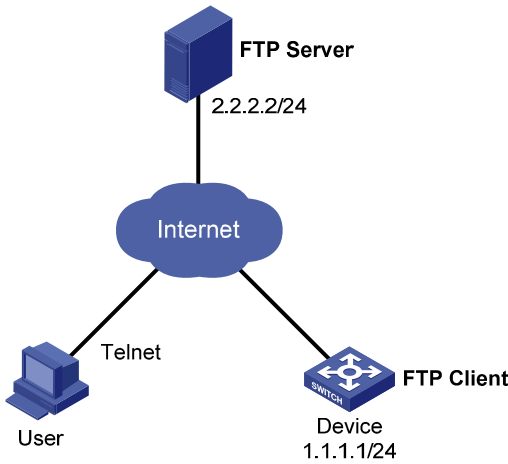
|                            |     |
|----------------------------|-----|
| 1 在线远程升级交换机典型配置指导.....     | 1-1 |
| 1.1 远程升级分布式交换机典型配置指导 ..... | 1-1 |
| 1.1.1 组网图.....             | 1-1 |
| 1.1.2 应用要求 .....           | 1-1 |
| 1.1.3 适用产品、版本 .....        | 1-1 |
| 1.1.4 配置过程和解释 .....        | 1-1 |
| 1.1.5 完整配置 .....           | 1-2 |
| 1.1.6 配置注意事项 .....         | 1-3 |
| 1.2 远程升级集中式交换机典型配置指导 ..... | 1-3 |
| 1.2.1 组网图.....             | 1-3 |
| 1.2.2 应用要求 .....           | 1-3 |
| 1.2.3 适用产品、版本 .....        | 1-3 |
| 1.2.4 配置过程和解释 .....        | 1-4 |
| 1.2.5 完整配置 .....           | 1-5 |
| 1.2.6 配置注意事项 .....         | 1-5 |

# 1 在线远程升级交换机典型配置指导

## 1.1 远程升级分布式交换机典型配置指导

### 1.1.1 组网图

图1-1 配置远程升级组网图



### 1.1.2 应用要求

- Device 作为 FTP Client，设备的应用程序 `aaa.app`（其中同时包含有主机软件升级文件和 BootROM 升级文件）都保存在 FTP Server 的 `aaa` 目录下；
- Device 上的一个 VLAN 接口的 IP 地址为 `1.1.1.1/24`，FTP Server 的 IP 地址为 `2.2.2.2/24`，Device 与 FTP Server 之间路由可达；
- User 通过 Telnet 远程登录到 Device，对 Device 进行操作（从 FTP Server 上下载应用程序，通过命令行实现 Device 的远程升级），请确定 User 与 Device 之间路由可达。

### 1.1.3 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

| 产品              | 软件版本                                 | 硬件版本    |
|-----------------|--------------------------------------|---------|
| S7500E 系列以太网交换机 | Release 6100 软件版本, Release 6300 软件版本 | 全系列硬件版本 |

### 1.1.4 配置过程和解释

(1) 在 FTP Server 上的配置（注意：不同的服务器类型配置可能不同）

# 启动 FTP Server 功能。

```
<FTP-Server> system-view
```

```
[FTP-Server] ftp server enable
```

# 配置一个 FTP 用户名为 `aaa`，密码为 `hello`。

```
[FTP-Server] local-user aaa
```

```
[FTP-Server-luser-aaa] password cipher hello
```

# 配置该用户对 aaa 目录具有读写权限。

```
[FTP-Server-luser-aaa] service-type ftp
```

```
[FTP-Server-luser-aaa] work-directory flash:/aaa
```

(2) 在 Device 上的配置

# 在用户视图下输入命令，登录到 FTP Server。

```
<Device> ftp 2.2.2.2
```

```
Trying 2.2.2.2 ...
```

```
Press CTRL+K to abort
```

```
Connected to 2.2.2.2.
```

```
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
```

```
User(2.2.2.2:(none)):aaa
```

```
331 Give me your password, please
```

```
Password:
```

```
230 Logged in successfully
```

```
[ftp]
```

# 将 FTP Server 上的文件 aaa.app 下载到 Device 的 Flash。

```
[ftp] get aaa.app
```

# 中断 FTP 连接，并退回到用户视图下。

```
[ftp] bye
```

```
<Device>
```

# 升级业务板 BootROM(假设业务板的槽位号为 2)。

```
<Device> bootrom update file aaa.app slot 2
```

# 升级主控板的 Bootrom。

```
<Device> bootrom update file aaa.app slot 0
```

# 指定主控板 0 下次启动时的应用程序文件。

```
<Device> boot-loader file aaa.app slot 0 main
```

# 当本设备的主控板为主备模式时，需要同时升级备用板的程序，并指定其为下次启动时的应用程序，并升级 BootROM。若备用板的槽位号为 1，则命令如下：

```
<Device> copy aaa.app slot1#flash:/
```

```
<Device> boot-loader file slot1#flash:/aaa.app slot 1 main
```

```
<Device> bootrom update file slot1#flash:/aaa.app slot 1
```

# 重启设备，实现应用程序的升级。

```
<Device> reboot
```

### 1.1.5 完整配置

- FTP Server 上的配置

```
#
```

```
ftp server enable
```

```
#
```

```
local-user aaa
```

```
password cipher 3MQ*TZ,03KCQ=^Q`MAF4<1!!
work-directory flash:/aaa
service-type ftp
```

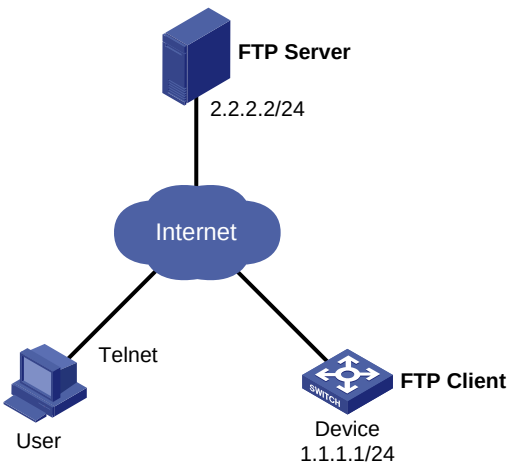
### 1.1.6 配置注意事项

- 在线升级时，上传文件操作也可以通过 TFTP 实现；
- 除在线升级外，用户还可以在 BOOTROM 菜单下实现软件和 BOOTROM 升级。
- 使用不同的 FTP Server，客户端登录时显示信息会有差异，请以实际情况为准。

## 1.2 远程升级集中式交换机典型配置指导

### 1.2.1 组网图

图1-2 配置远程升级组网图



### 1.2.2 应用要求

- Device 作为 FTP Client，设备的应用程序 aaa.bin 和 Bootrom 程序 boot.btm 都保存在 FTP Server 的 aaa 目录下；
- Device 上的一个 VLAN 接口的 IP 地址为 1.1.1.1/24，FTP Server 的 IP 地址为 2.2.2.2/24，Device 与 FTP Server 之间路由可达；
- User 通过 Telnet 远程登录到 Device，对 Device 进行操作（从 FTP Server 上下载应用程序，通过命令行实现 Device 的远程升级），请确定 User 与 Device 之间路由可达。

### 1.2.3 适用产品、版本

表1-2 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                                    | 硬件版本                         |
|-------------------|-----------------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301 软件版本，<br>Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301 软件版本，<br>Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本                       | 全系列硬件版本<br>(除 S5500-20TP-SI) |



| 产品                | 软件版本              | 硬件版本          |
|-------------------|-------------------|---------------|
|                   | Release 1301 软件版本 | S5500-20TP-SI |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本 | 全系列硬件版本       |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本 | 全系列硬件版本       |

#### 1.2.4 配置过程和解释

(1) 在 FTP Server 上的配置（注意：不同的服务器类型配置可能不同）

# 启动 FTP Server 功能。

```
<FTP-Server> system-view
```

```
[FTP-Server] ftp server enable
```

# 配置一个 FTP 用户名为 aaa，密码为 hello。

```
[FTP-Server] local-user aaa
```

```
[FTP-Server-luser-aaa] password cipher hello
```

# 配置该用户对 aaa 目录具有读写权限。

```
[FTP-Server-luser-aaa] service-type ftp
```

```
[FTP-Server-luser-aaa] work-directory flash:/aaa
```

(2) 在 Device 上的配置

# 在用户视图下输入命令，登录到 FTP Server。

```
<Device> ftp 2.2.2.2
```

```
Trying 2.2.2.2 ...
```

```
Press CTRL+K to abort
```

```
Connected to 2.2.2.2.
```

```
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
```

```
User(2.2.2.2:(none)):aaa
```

```
331 Give me your password, please
```

```
Password:
```

```
230 Logged in successfully
```

```
[ftp]
```

# 将 FTP Server 上的文件 aaa.bin 和 boot.btm 下载到 Device 的 Flash。

```
[ftp] get aaa.bin
```

```
[ftp] get boot.btm
```

# 中断 FTP 连接，并退回到用户视图下。

```
[ftp] bye
```

```
<Device>
```

# 升级设备的 Bootrom。

```
<Device> bootrom update file boot.btm
```

# 指定设备下次启动时的应用程序。

```
<Device> boot-loader file aaa.bin main
```

# 重启设备，实现应用程序的升级。

```
<Device> reboot
```

### 1.2.5 完整配置

- FTP Server 上的配置

```

ftp server enable

local-user aaa
password cipher 3MQ*TZ,03KCQ=^Q`MAF4<1!!
work-directory flash:/aaa
service-type ftp
```

### 1.2.6 配置注意事项

- 在线升级时，上传文件操作也可以通过 TFTP 实现；
- 除在线升级外，用户还可以在 **BOOTROM** 菜单下实现软件和 **BOOTROM** 升级。
- 使用不同的 **FTP Server**，客户端登录时显示信息会有差异，请以实际情况为准。

# 目 录

|                              |      |
|------------------------------|------|
| 1 NQA典型配置指导 .....            | 1-1  |
| 1.1 NQA概述 .....              | 1-1  |
| 1.2 NQA配置指导 .....            | 1-1  |
| 1.2.1 ICMP-echo测试配置举例 .....  | 1-1  |
| 1.2.2 DHCP测试配置举例 .....       | 1-3  |
| 1.2.3 FTP测试配置举例 .....        | 1-5  |
| 1.2.4 HTTP测试配置举例 .....       | 1-7  |
| 1.2.5 UDP-jitter测试配置举例 ..... | 1-8  |
| 1.2.6 SNMP测试配置举例 .....       | 1-11 |
| 1.2.7 TCP测试配置举例 .....        | 1-13 |
| 1.2.8 UDP-echo测试配置举例 .....   | 1-15 |

# 1 NQA 典型配置指导

## 1.1 NQA 概述

NQA 是 Network Quality Analyzer（网络质量分析）的简称。NQA 通过发送测试报文，对网络性能、网络提供的服务及服务质量进行分析，并为用户提供网络性能和服务质量的参数，如时延抖动、TCP 连接时延、FTP 连接时延和文件传输速率等。

利用 NQA 的测试结果，用户可以：

- (1) 及时了解网络的性能状况，针对不同的网络性能，进行相应处理。
- (2) 对网络故障进行诊断和定位。

## 1.2 NQA 配置指导

### 1.2.1 ICMP-echo 测试配置举例

#### 1. 组网图

图1-1 ICMP-echo 测试组网图



#### 2. 应用要求

使用 NQA 进行 ICMP-echo 测试，测试本端（Switch A）发送的报文是否可以到达指定的目的端（Switch B），以及报文的往返时间。

#### 3. 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本                         |
|-------------------|---------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本               | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本               | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本                      |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本                      |

#### 4. 配置过程和解释

# 创建 ICMP-echo 类型的 NQA 测试组并配置相关测试参数。

```
<SwitchA> system-view
[SwitchA] nqa entry admin test
[SwitchA-nqa-admin-test] type icmp-echo
[SwitchA-nqa-admin-test-icmp-echo] destination ip 10.2.2.2
```

# 配置可选参数。

```
[SwitchA-nqa-admin-test-icmp-echo] probe count 10
[SwitchA-nqa-admin-test-icmp-echo] probe timeout 500
[SwitchA-nqa-admin-test-icmp-echo] frequency 5000
[SwitchA-nqa-admin-test-icmp-echo] history-records 10
[SwitchA-nqa-admin-test-icmp-echo] quit
```

# 启动 ICMP-echo 测试操作。

```
[SwitchA] nqa schedule admin test start-time now lifetime forever
```

# 测试执行一段时间后，停止 ICMP-echo 测试操作。

```
[SwitchA] undo nqa schedule admin test
```

# 显示 ICMP-echo 测试中最后一次测试的结果。

```
[SwitchA] display nqa result admin test
NQA entry(admin admin, tag test) test results:
 Destination IP address: 10.2.2.2
 Send operation times: 10 Receive response times: 10
 Min/Max/Average round trip time: 0/16/1
 Square-Sum of round trip time: 256
 Last succeeded probe time: 2007-08-23 15:00:01.2
 Extend results:
 Packet lost in test: 0%
 Failures due to timeout: 0
 Failures due to disconnect: 0
 Failures due to no connection: 0
 Failures due to sequence error: 0
 Failures due to internal error: 0
 Failures due to other errors: 0
```

# 显示 ICMP-echo 测试的历史记录。

```
[SwitchA] display nqa history admin test
NQA entry(admin admin, tag test) history record(s):
```

| Index | Response | Status    | Time                  |
|-------|----------|-----------|-----------------------|
| 370   | 3        | Succeeded | 2007-08-23 15:00:01.2 |
| 369   | 3        | Succeeded | 2007-08-23 15:00:01.2 |
| 368   | 3        | Succeeded | 2007-08-23 15:00:01.2 |
| 367   | 5        | Succeeded | 2007-08-23 15:00:01.2 |
| 366   | 3        | Succeeded | 2007-08-23 15:00:01.2 |
| 365   | 3        | Succeeded | 2007-08-23 15:00:01.2 |
| 364   | 3        | Succeeded | 2007-08-23 15:00:01.1 |
| 363   | 2        | Succeeded | 2007-08-23 15:00:01.1 |

|     |   |           |                       |
|-----|---|-----------|-----------------------|
| 362 | 3 | Succeeded | 2007-08-23 15:00:01.1 |
| 361 | 2 | Succeeded | 2007-08-23 15:00:01.1 |

5. 完整配置

```
• 在 SwitchA 上启动 NQA 的 ICMP-echo 测试
#
nqa entry admin test
 type icmp-echo
 destination ip 10.2.2.2
 probe count 10
 probe timeout 500
 frequency 5000
 history-records 10
#
nqa schedule admin test start-time now lifetime forever
```

6. 配置注意事项

当前设备暂不支持配置 NQA 测试的结束时间，需要通过执行 **undo nqa schedule** 命令停止测试。

1.2.2 DHCP 测试配置举例

1. 组网图

图1-2 DHCP 测试组网图



2. 应用要求

使用 NQA 的 DHCP 测试功能,测试 Switch A 从 DHCP 服务器 Switch B 申请到 IP 地址所需的时间。

3. 适用产品、版本

表1-2 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本                         |
|-------------------|---------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本               | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本               | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本                      |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本                      |

#### 4. 配置过程和解释

# 创建 DHCP 类型的 NQA 测试组并配置相关测试参数。

```
<SwitchA> system-view
[SwitchA] nqa entry admin test
[SwitchA-nqa-admin-test] type dhcp
[SwitchA-nqa-admin-test-dhcp] operation interface vlan-interface 2
[SwitchA-nqa-admin-test-dhcp] quit
```

# 启动 DHCP 测试操作。

```
[SwitchA] nqa schedule admin test start-time now lifetime forever
```

# 测试执行一段时间后，停止 DHCP 测试操作。

```
[SwitchA] undo nqa schedule admin test
```

# 显示 DHCP 测试中最后一次测试的结果。

```
[SwitchA] display nqa result admin test
NQA entry(admin admin, tag test) test results:
 Send operation times: 1 Receive response times: 1
 Min/Max/Average round trip time: 624/624/624
 Square-Sum of round trip time: 389376
 Last succeeded probe time: 2007-11-22 09:56:03.2
 Extend results:
 Packet lost in test: 0%
 Failures due to timeout: 0
 Failures due to disconnect: 0
 Failures due to no connection: 0
 Failures due to sequence error: 0
 Failures due to internal error: 0
 Failures due to other errors: 0
```

# 显示 DHCP 测试的历史记录。

```
[SwitchA] display nqa history admin test
NQA entry(admin admin, tag test) history record(s):

Index	Response	Status	Time
1	624	Succeeded	2007-11-22 09:56:03.2


```

#### 5. 完整配置

- 在 SwitchA 上启动 NQA 的 DHCP 测试

```
#
nqa entry admin test
type dhcp
operation interface Vlan-interface2
#
nqa schedule admin test start-time now lifetime forever
```

#### 6. 配置注意事项

当前设备暂不支持配置 NQA 测试的结束时间，需要通过执行 **undo nqa schedule** 命令停止测试。

### 1.2.3 FTP 测试配置举例

#### 1. 组网图

图1-3 FTP 测试组网图



#### 2. 应用要求

使用 NQA 的 FTP 测试功能，测试 Switch A 是否可以和指定的 FTP 服务器 Switch B 建立连接，以及往 FTP 服务器上传一个文件的时间。登录 FTP 服务器的用户名为 admin，密码为 systemtest，要传送到服务器的文件名为 config.txt。

#### 3. 适用产品、版本

表1-3 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本                         |
|-------------------|---------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本               | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本               | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本                      |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本                      |

#### 4. 配置过程 and 解释

# 创建 FTP 类型的 NQA 测试组并配置相关测试参数。

```
<SwitchA> system-view
[SwitchA] nqa entry admin test
[SwitchA-nqa-admin-test] type ftp
[SwitchA-nqa-admin-test-ftp] destination ip 10.2.2.2
[SwitchA-nqa-admin-test-ftp] source ip 10.1.1.1
[SwitchA-nqa-admin-test-ftp] operation put
[SwitchA-nqa-admin-test-ftp] username admin
[SwitchA-nqa-admin-test-ftp] password systemtest
[SwitchA-nqa-admin-test-ftp] filename config.txt
[SwitchA-nqa-admin-test-ftp] quit
```

# 启动 FTP 测试操作。

```
[SwitchA] nqa schedule admin test start-time now lifetime forever
```



# 测试执行一段时间后，停止 FTP 测试操作。

```
[SwitchA] undo nqa schedule admin test
```

# 显示 FTP 测试中最后一次测试的结果。

```
[SwitchA] display nqa result admin test
```

```
NQA entry(admin admin, tag test) test results:
```

```
Destination IP address: 10.2.2.2
```

```
Send operation times: 1 Receive response times: 1
```

```
Min/Max/Average round trip time: 173/173/173
```

```
Square-Sum of round trip time: 29929
```

```
Last succeeded probe time: 2007-11-22 10:07:28.6
```

```
Extend results:
```

```
Packet lost in test: 0%
```

```
Failures due to timeout: 0
```

```
Failures due to disconnect: 0
```

```
Failures due to no connection: 0
```

```
Failures due to sequence error: 0
```

```
Failures due to internal error: 0
```

```
Failures due to other errors: 0
```

# 显示 FTP 测试的历史记录。

```
[SwitchA] display nqa history admin test
```

```
NQA entry(admin admin, tag test) history record(s):
```

| Index | Response | Status    | Time                  |
|-------|----------|-----------|-----------------------|
| 1     | 173      | Succeeded | 2007-11-22 10:07:28.6 |

## 5. 完整配置

- 在 SwitchA 上启动 NQA 的 FTP 测试

```
#
```

```
nqa entry admin test
```

```
type ftp
```

```
destination ip 10.2.2.2
```

```
filename config.txt
```

```
operation put
```

```
password systemtest
```

```
source ip 10.1.1.1
```

```
username admin
```

```
#
```

```
nqa schedule admin test start-time now lifetime forever
```

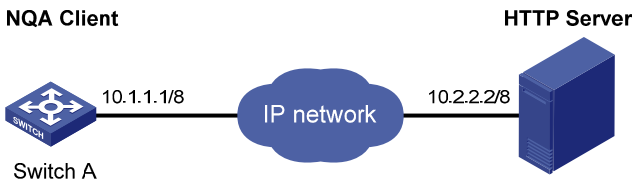
## 6. 配置注意事项

当前设备暂不支持配置 NQA 测试的结束时间，需要通过执行 **undo nqa schedule** 命令停止测试。

## 1.2.4 HTTP 测试配置举例

### 1. 组网图

图1-4 HTTP 测试组网图



### 2. 应用要求

使用 NQA 的 HTTP 测试功能，测试是否可以和指定的 HTTP 服务器之间建立连接，以及从 HTTP 服务器获取数据的时间。

### 3. 适用产品、版本

表1-4 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本                         |
|-------------------|---------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本               | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本               | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本                      |

### 4. 配置过程 and 解释

# 创建 HTTP 类型的 NQA 测试组并配置相关测试参数。

```
<SwitchA> system-view
[SwitchA] nqa entry admin test
[SwitchA-nqa-admin-test] type http
[SwitchA-nqa-admin-test-http] destination ip 10.2.2.2
[SwitchA-nqa-admin-test-http] operation get
[SwitchA-nqa-admin-test-http] url /index.htm
[SwitchA-nqa-admin-test-http] http-version v1.0
[SwitchA-nqa-admin-test-http] quit
```

# 启动 HTTP 测试操作。

```
[SwitchA] nqa schedule admin test start-time now lifetime forever
```

# 测试执行一段时间后，停止 HTTP 测试操作。

```
[SwitchA] undo nqa schedule admin test
```

# 显示 HTTP 测试中一次测试的结果。

```
[SwitchA] display nqa result admin test
NQA entry(admin admin, tag test) test results:
 Destination IP address: 10.2.2.2
 Send operation times: 1 Receive response times: 1
 Min/Max/Average round trip time: 64/64/64
 Square-Sum of round trip time: 4096
 Last succeeded probe time: 2007-11-22 10:12:47.9
 Extend results:
 Packet lost in test: 0%
 Failures due to timeout: 0
 Failures due to disconnect: 0
 Failures due to no connection: 0
 Failures due to sequence error: 0
 Failures due to internal error: 0
 Failures due to other errors: 0
```

# 显示 HTTP 测试的历史记录。

```
[SwitchA] display nqa history admin test
NQA entry(admin admin, tag test) history record(s):
 Index Response Status Time

 1 64 Succeeded 2007-11-22 10:12:47.9
```

## 5. 完整配置

- 在 SwitchA 上启动 NQA 的 HTTP 测试

```
#
nqa entry admin test
 type http
 destination ip 10.2.2.2
 url /index.htm
#
nqa schedule admin test start-time now lifetime forever
```

## 6. 配置注意事项

当前设备暂不支持配置 NQA 测试的结束时间，需要通过执行 **undo nqa schedule** 命令停止测试。

## 1.2.5 UDP-jitter 测试配置举例

### 1. 组网图

图1-5 UDP-jitter 测试组网图



## 2. 应用要求

使用 NQA 的 UDP-jitter 测试功能，测试本端（Switch A）和指定的目的端（Switch B）之间传送报文的时延抖动，使用的端口号为 9000。

## 3. 适用产品、版本

表1-5 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本                         |
|-------------------|---------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本               | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本               | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本                      |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本                      |

## 4. 配置过程 and 解释

### (1) 配置 Switch B

# 使能 NQA 服务器，配置监听的 IP 地址为 10.2.2.2 和端口号为 9000。

```
<SwitchB> system-view
[SwitchB] nqa server enable
[SwitchB] nqa server udp-echo 10.2.2.2 9000
```

### (2) 配置 Switch A

# 创建 UDP-jitter 类型的 NQA 测试组并配置相关测试参数。

```
<SwitchA> system-view
[SwitchA] nqa entry admin test
[SwitchA-nqa-admin-test] type udp-jitter
[SwitchA-nqa-admin-test-udp-jitter] destination ip 10.2.2.2
[SwitchA-nqa-admin-test-udp-jitter] destination port 9000
[SwitchA-nqa-admin-test-udp-jitter] quit
```

# 启动 UDP-jitter 测试操作。

```
[SwitchA] nqa schedule admin test start-time now lifetime forever
```

# 测试执行一段时间后，停止 UDP-jitter 测试操作。

```
[SwitchA] undo nqa schedule admin test
```

# 显示 UDP-jitter 测试中最后一次测试的结果。

```
[SwitchA] display nqa result admin test
NQA entry(admin admin, tag test) test results:
Destination IP address: 10.2.2.2
```

```

Send operation times: 10 Receive response times: 10
Min/Max/Average round trip time: 7/10/8
Square-Sum of round trip time: 646
Last succeeded probe time: 2007-11-22 10:16:49.0
Extend results:
Packet lost in test: 0%
Failures due to timeout: 0
Failures due to disconnect: 0
Failures due to no connection: 0
Failures due to sequence error: 0
Failures due to internal error: 0
Failures due to other errors: 0
UDP-jitter results:
RTT number: 10
SD max delay: 5 DS max delay: 5
Min positive SD: 1 Min positive DS: 0
Max positive SD: 1 Max positive DS: 0
Positive SD number: 2 Positive DS number: 0
Positive SD sum: 2 Positive DS sum: 0
Positive SD average: 1 Positive DS average: 0
Positive SD square sum: 2 Positive DS square sum: 0
Min negative SD: 1 Min negative DS: 0
Max negative SD: 2 Max negative DS: 0
Negative SD number: 3 Negative DS number: 0
Negative SD sum: 4 Negative DS sum: 0
Negative SD average: 1 Negative DS average: 0
Negative SD square sum: 6 Negative DS square sum: 0
SD lost packet(s): 0 DS lost packet(s): 0
Lost packet(s) for unknown reason: 0

```

---



#### 说明

UDP-jitter 测试中每次探测发送一组报文, 这组报文对应一条历史记录。因此, 如果了解 UDP-jitter 测试的结果, 建议通过 **display nqa result** 命令来查看探测结果, 不要通过 **display nqa history** 命令查看历史记录。

---

## 5. 完整配置

- SwitchB

```

#
nqa server enable
nqa server udp-echo 10.2.2.2 9000

```

- 在 SwitchA 上启动 NQA 的 UDP-jitter 测试

```

#
nqa entry admin test
type udp-jitter
destination ip 10.2.2.2
destination port 9000

```

```
#
```

```
nqa schedule admin test start-time now lifetime forever
```

## 6. 配置注意事项

当前设备暂不支持配置 NQA 测试的结束时间，需要通过执行 **undo nqa schedule** 命令停止测试。

## 1.2.6 SNMP 测试配置举例

### 1. 组网图

图1-6 SNMP 配置测试组网图



### 2. 应用要求

使用 NQA 的 SNMP 查询功能,测试从 Switch A 发出一个 SNMP 协议查询报文到收到 SNMP Agent (Switch B) 响应报文所用的时间。

### 3. 适用产品、版本

表1-6 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本                         |
|-------------------|---------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本               | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本               | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本                      |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本                      |

### 4. 配置过程和解释

(1) 在 SNMP Agent 上进行配置

# 启动 SNMP Agent 服务，设置 SNMP 版本为 all、只读团体名为 public、读写团体名为 private。

```
<SwitchB> system-view
```

```
[SwitchB] snmp-agent sys-info version all
```

```
[SwitchB] snmp-agent community read public
```

```
[SwitchB] snmp-agent community write private
```

(2) 在 Switch A 上进行配置

# 创建 SNMP 查询类型的测试组并配置相关测试参数。

```
<SwitchA> system-view
[SwitchA] nqa entry admin test
[SwitchA-nqa-admin-test] type snmp
[SwitchA-nqa-admin-test-snmp] destination ip 10.2.2.2
[SwitchA-nqa-admin-test-snmp] quit
```

# 启动测试操作。

```
[SwitchA] nqa schedule admin test start-time now lifetime forever
```

# 测试执行一段时间后，停止 SNMP 测试操作。

```
[SwitchA] undo nqa schedule admin test
```

# 显示 SNMP 测试中最后一次测试的结果。

```
[SwitchA] display nqa result admin test
NQA entry(admin admin, tag test) test results:
 Destination IP address: 10.2.2.2
 Send operation times: 1 Receive response times: 1
 Min/Max/Average round trip time: 50/50/50
 Square-Sum of round trip time: 2500
 Last succeeded probe time: 2007-11-22 10:24:41.1
 Extend results:
 Packet lost in test: 0%
 Failures due to timeout: 0
 Failures due to disconnect: 0
 Failures due to no connection: 0
 Failures due to sequence error: 0
 Failures due to internal error: 0
 Failures due to other errors: 0
```

# 显示 SNMP 测试的历史记录。

```
[SwitchA] display nqa history admin test
NQA entry(admin admin, tag test) history record(s):
 Index Response Status Time

 1 50 Timeout 2007-11-22 10:24:41.1
```

## 5. 完整配置

- 在 SwitchA 上启动 NQA 的 SNMP 测试

```
#
nqa entry admin test
 type snmp
 destination ip 10.2.2.2
#
nqa schedule admin test start-time now lifetime forever
```

- SwitchB

```
#
snmp-agent
snmp-agent local-engineid 800063A20300E0FC123456
snmp-agent community read public
```

```
snmp-agent community write private
snmp-agent sys-info version all
```

## 6. 配置注意事项

当前设备暂不支持配置 NQA 测试的结束时间，需要通过执行 **undo nqa schedule** 命令停止测试。

### 1.2.7 TCP 测试配置举例

#### 1. 组网图

图1-7 TCP 测试组网图



#### 2. 应用要求

使用 NQA 的 TCP 测试功能，测试本端（Switch A）和指定目的端（Switch B）之间建立 TCP 连接所需的时间，使用的端口号为 9000。

#### 3. 适用产品、版本

表1-7 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本                         |
|-------------------|---------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本               | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本               | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本                      |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本                      |

#### 4. 配置过程和解释

##### (1) 配置 Switch B

# 使能 NQA 服务器，配置监听 IP 地址 10.2.2.2 和端口号 9000。

```
<SwitchB> system-view
[SwitchB] nqa server enable
[SwitchB] nqa server tcp-connect 10.2.2.2 9000
```

##### (2) 配置 Switch A

# 创建 TCP 类型的测试组并配置相关测试参数。



```

<SwitchA> system-view
[SwitchA] nqa entry admin test
[SwitchA-nqa-admin-test] type tcp
[SwitchA-nqa-admin-test-tcp] destination ip 10.2.2.2
[SwitchA-nqa-admin-test-tcp] destination port 9000
[SwitchA-nqa-admin-test-tcp] quit

启动测试操作。

[SwitchA] nqa schedule admin test start-time now lifetime forever

测试执行一段时间后，停止 TCP 测试操作。

[SwitchA] undo nqa schedule admin test

显示 TCP 测试中最后一次测试的结果。

[SwitchA] display nqa result admin test
 NQA entry(admin admin, tag test) test results:
 Destination IP address: 10.2.2.2
 Send operation times: 1 Receive response times: 1
 Min/Max/Average round trip time: 13/13/13
 Square-Sum of round trip time: 169
 Last succeeded probe time: 2007-11-22 10:27:25.1
 Extend results:
 Packet lost in test: 0%
 Failures due to timeout: 0
 Failures due to disconnect: 0
 Failures due to no connection: 0
 Failures due to sequence error: 0
 Failures due to internal error: 0
 Failures due to other errors: 0

显示 TCP 测试的历史记录。

[SwitchA] display nqa history admin test
 NQA entry(admin admin, tag test) history record(s):

```

| Index | Response | Status    | Time                  |
|-------|----------|-----------|-----------------------|
| 1     | 13       | Succeeded | 2007-11-22 10:27:25.1 |

## 5. 完整配置

- SwitchB

```
#
```

```
nqa server enable
nqa server tcp-connect 10.2.2.2 9000
```

- 在 SwitchA 上启动 NQA 的 TCP 测试

```
#
```

```
nqa entry admin test
 type tcp
 destination ip 10.2.2.2
 destination port 9000
```

```
#
```

```
nqa schedule admin test start-time now lifetime forever
```

6. 配置注意事项

当前设备暂不支持配置 NQA 测试的结束时间，需要通过执行 **undo nqa schedule** 命令停止测试。

1.2.8 UDP-echo 测试配置举例

1. 组网图

图1-8 UDP-echo 测试组网图



2. 应用要求

使用 NQA 的 UDP-echo 测试功能，测试本端（Switch A）和指定目的端（Switch B）之间 UDP 协议报文的往返时间，使用的端口号设置为 8000。

3. 适用产品、版本

表1-8 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本                         |
|-------------------|---------------------------------|------------------------------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本                      |
| S5500-SI 系列以太网交换机 | Release 1207 软件版本               | 全系列硬件版本<br>(除 S5500-20TP-SI) |
|                   | Release 1301 软件版本               | S5500-20TP-SI                |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本                      |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本                      |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本                      |

4. 配置过程 and 解释

(1) 配置 Switch B

# 使能 NQA 服务器，配置监听的 IP 地址为 10.2.2.2 和端口号为 8000。

```
<SwitchB> system-view
[SwitchB] nqa server enable
[SwitchB] nqa server udp-echo 10.2.2.2 8000
```

(2) 配置 Switch A

# 创建 UDP-echo 类型的测试组并配置相关测试参数。

```
<SwitchA> system-view
[SwitchA] nqa entry admin test
[SwitchA-nqa-admin-test] type udp-echo
```

```
[SwitchA-nqa-admin-test-udp-echo] destination ip 10.2.2.2
```

```
[SwitchA-nqa-admin-test-udp-echo] destination port 8000
```

```
[SwitchA-nqa-admin-test-udp-echo] quit
```

# 启动测试操作。

```
[SwitchA] nqa schedule admin test start-time now lifetime forever
```

# 测试执行一段时间后，停止 UDP-echo 测试操作。

```
[SwitchA] undo nqa schedule admin test
```

# 显示 UDP-echo 测试中一次测试的结果。

```
[SwitchA] display nqa result admin test
```

```
NQA entry(admin admin, tag test) test results:
```

```
Destination IP address: 10.2.2.2
```

```
Send operation times: 1 Receive response times: 1
```

```
Min/Max/Average round trip time: 25/25/25
```

```
Square-Sum of round trip time: 625
```

```
Last succeeded probe time: 2007-11-22 10:36:17.9
```

```
Extend results:
```

```
Packet lost in test: 0%
```

```
Failures due to timeout: 0
```

```
Failures due to disconnect: 0
```

```
Failures due to no connection: 0
```

```
Failures due to sequence error: 0
```

```
Failures due to internal error: 0
```

```
Failures due to other errors: 0
```

# 显示 UDP-echo 测试的历史记录。

```
[SwitchA] display nqa history admin test
```

```
NQA entry(admin admin, tag test) history record(s):
```

| Index | Response | Status    | Time                  |
|-------|----------|-----------|-----------------------|
| 1     | 25       | Succeeded | 2007-11-22 10:36:17.9 |

## 5. 完整配置

- SwitchB

```
#
```

```
nqa server enable
```

```
nqa server udp-echo 10.2.2.2 8000
```

- 在 SwitchA 上启动 NQA 的 UDP-echo 测试

```
#
```

```
nqa entry admin test
```

```
type udp-echo
```

```
destination ip 10.2.2.2
```

```
destination port 8000
```

```
#
```

```
nqa schedule admin test start-time now lifetime forever
```

## 6. 配置注意事项

当前设备暂不支持配置 NQA 测试的结束时间，需要通过执行 **undo nqa schedule** 命令停止测试。

# 目 录

|                            |     |
|----------------------------|-----|
| 1 基于IPv4的VRRP典型配置指导 .....  | 1-1 |
| 1.1 基于IPv4的VRRP单备份组举例..... | 1-1 |
| 1.1.1 组网图 .....            | 1-1 |
| 1.1.2 应用要求 .....           | 1-1 |
| 1.1.3 适用产品、版本 .....        | 1-2 |
| 1.1.4 配置过程和解释 .....        | 1-2 |
| 1.1.5 完整配置 .....           | 1-3 |
| 1.1.6 配置注意事项 .....         | 1-3 |
| 1.2 基于IPv4的VRRP监视接口举例..... | 1-4 |
| 1.2.1 组网图 .....            | 1-4 |
| 1.2.2 应用要求 .....           | 1-4 |
| 1.2.3 适用产品、版本 .....        | 1-4 |
| 1.2.4 配置过程和解释 .....        | 1-5 |
| 1.2.5 完整配置 .....           | 1-5 |
| 1.2.6 配置注意事项 .....         | 1-6 |
| 1.3 基于IPv4的VRRP多备份组举例..... | 1-6 |
| 1.3.1 组网图 .....            | 1-7 |
| 1.3.2 应用要求 .....           | 1-7 |
| 1.3.3 适用产品、版本 .....        | 1-7 |
| 1.3.4 配置过程和解释 .....        | 1-7 |
| 1.3.5 完整配置 .....           | 1-9 |
| 1.3.6 配置注意事项 .....         | 1-9 |
| 2 基于IPv6的VRRP典型配置指导 .....  | 2-1 |
| 2.1 基于IPv6的VRRP单备份组举例..... | 2-1 |
| 2.1.1 组网图 .....            | 2-1 |
| 2.1.2 应用要求 .....           | 2-1 |
| 2.1.3 适用产品、版本 .....        | 2-1 |
| 2.1.4 配置过程和解释 .....        | 2-2 |
| 2.1.5 完整配置 .....           | 2-3 |
| 2.1.6 配置注意事项 .....         | 2-3 |
| 2.2 基于IPv6的VRRP监视接口举例..... | 2-4 |
| 2.2.1 组网图 .....            | 2-4 |
| 2.2.2 应用要求 .....           | 2-4 |
| 2.2.3 适用产品、版本 .....        | 2-4 |
| 2.2.4 配置过程和解释 .....        | 2-5 |
| 2.2.5 完整配置 .....           | 2-6 |
| 2.2.6 配置注意事项 .....         | 2-6 |
| 2.3 基于IPv6的VRRP多备份组举例..... | 2-7 |
| 2.3.1 组网图 .....            | 2-7 |
| 2.3.2 应用要求 .....           | 2-7 |
| 2.3.3 适用产品、版本 .....        | 2-8 |

2.3.4 配置过程和解释 ..... 2-8

2.3.5 完整配置 ..... 2-9

2.3.6 配置注意事项 ..... 2-10

# 1 基于 IPv4 的 VRRP 典型配置指导

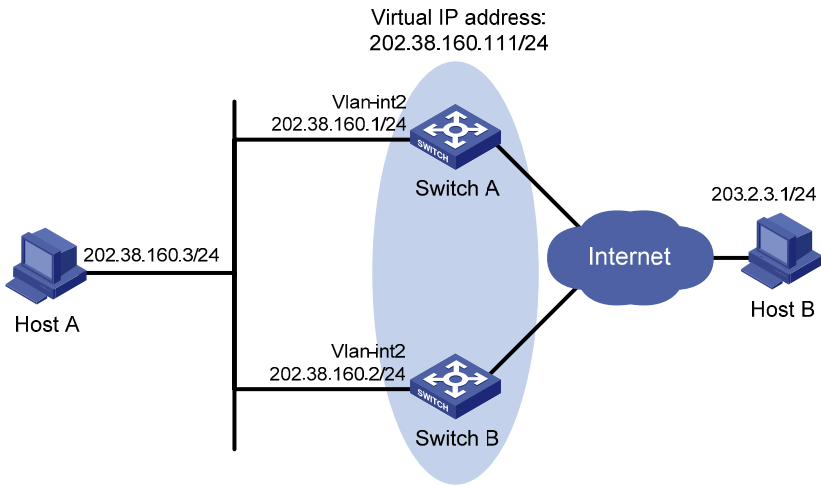
## 1.1 基于 IPv4 的 VRRP 单备份组举例

VRRP（Virtual Router Redundancy Protocol，虚拟路由器冗余协议）是一种容错协议。在具有多播或广播能力的局域网（如以太网）中，借助 VRRP 能在某设备故障时提供高利用度的缺省链路，而无需修改动态路由协议、路由发现协议的配置信息。通过 VRRP 建立备份链路，提高了网络的安全性、能有效避免单一链路发生故障后网络中断问题出现。

借助 VRRP 单备份组组网，使用两台或多台交换机组成一个虚拟备份组，负责提供两条或多条通往外部网络的稳定的链路，避免备份组内的单台或多台交换机发生故障而引起的通信中断。

### 1.1.1 组网图

图1-1 VRRP 单备份组配置组网图



### 1.1.2 应用要求

- Host A 需要访问 Internet 上的 Host B，Host A 的缺省网关为 202.38.160.111/24；
- 当 Switch A 正常工作时，Host A 发送给 Host B 的报文通过 Switch A 转发；当 Switch A 出现故障时，Host A 发送给 Host B 的报文通过 Switch B 转发。

VRRP 备份组构成：

- 备份组号为 1
- 备份组虚拟路由器的 IP 地址为 202.38.160.111
- Switch A 做 Master
- Switch B 做备份交换机，允许抢占

表1-1 组网说明

| 交换机      | 与 Host A 相连的以太网端口 | VLAN 接口 IP 地址   | 交换机在备份组中的优先级 | 抢占方式 |
|----------|-------------------|-----------------|--------------|------|
| Switch A | Ethernet 1/0/6    | 202.38.160.1/24 | 110          | 允许抢占 |

| 交换机      | 与 Host A 相连的以太网端口 | VLAN 接口 IP 地址   | 交换机在备份组中的优先级 | 抢占方式 |
|----------|-------------------|-----------------|--------------|------|
| Switch B | Ethernet 1/0/5    | 202.38.160.2/24 | 100（缺省值）     | 允许抢占 |

### 1.1.3 适用产品、版本

表1-2 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本    |
|-------------------|---------------------------------|---------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本 |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本 |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本 |

### 1.1.4 配置过程和解释

- 配置交换机 A

# 配置 VLAN2。

```
<Switch A> system-view
[Switch A] vlan 2
[Switch A-vlan2] port Ethernet1/0/6
[Switch A-vlan2] quit
[Switch A] interface Vlan-interface 2
[Switch A-Vlan-interface2] ip address 202.38.160.1 255.255.255.0
```

# 创建一个备份组。

```
[Switch A-Vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.111
```

# 设置交换机 A 在备份组中的优先级。

```
[Switch A-Vlan-interface2] vrrp vrid 1 priority 110
```

# 设置 Switch A 工作在抢占方式，抢占延迟时间为 5 秒。

```
[Switch A-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
```



说明

缺省情况下，备份组工作在抢占方式，抢占延迟时间为 0 秒。

- 配置交换机 B

# 配置 VLAN2。

```
<Switch B> system-view
[Switch B] vlan 2
[Switch B-Vlan2] port Ethernet1/0/5
```

```
[Switch B-Vlan2] quit
```

```
[Switch B] interface Vlan-interface 2
```

```
[Switch B-Vlan-interface2] ip address 202.38.160.2 255.255.255.0
```

# 创建一个备份组。

```
[Switch B-Vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.111
```

# 设置 Switch B 工作在抢占方式，抢占延迟时间为 5 秒。

```
[Switch B-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
```

配置完成后，可以通过 **display vrrp** 命令查看配置后的结果。

正常情况下，Switch A 行使网关的职能，当 Switch A 关机或出现故障，Switch B 将接替行使网关的职能。

设置抢占方式的目的是当 Switch A 恢复工作后，能够继续成为 Master 行使网关的职能。

### 1.1.5 完整配置

- Switch A 上的配置

```
#
```

```
interface Vlan-interface2
```

```
ip address 202.38.160.1 255.255.255.0
```

```
vrrp vrid 1 virtual-ip 202.38.160.111
```

```
vrrp vrid 1 priority 110
```

```
vrrp vrid 1 preempt-mode timer delay 5
```

```
#
```

```
interface Ethernet1/0/6
```

```
port access vlan 2
```

```
#
```

- SwitchB 上的配置

```
#
```

```
interface Vlan-interface2
```

```
ip address 202.38.160.2 255.255.255.0
```

```
vrrp vrid 1 virtual-ip 202.38.160.111
```

```
vrrp vrid 1 preempt-mode timer delay 5
```

```
#
```

```
interface Ethernet1/0/5
```

```
port access vlan 2
```

```
#
```

### 1.1.6 配置注意事项

- 虚拟 IP 地址和接口 IP 地址必须在同一网段，且为合法的主机地址，不能为全零地址(0.0.0.0)、广播地址(255.255.255.255)、环回地址、非 A/B/C 类地址和其它非法 IP 地址(如 0.0.0.1)，否则备份组无法正常工作。
- 对于同一个 VRRP 备份组的配置，必须保证备份组虚拟路由器的 IP 地址个数、每个备份组虚拟路由器的 IP 地址、定时器间隔时间和认证方式完全一样。



- 如果网络流量过大或者不同的交换机上的定时器差异等因素，会导致 Backup 路由器的定时器异常超时而发生状态转换。对于这种情况，可以通过将 VRRP 通告报文的发送时间间隔延长和设置抢占延迟时间的办法来解决。

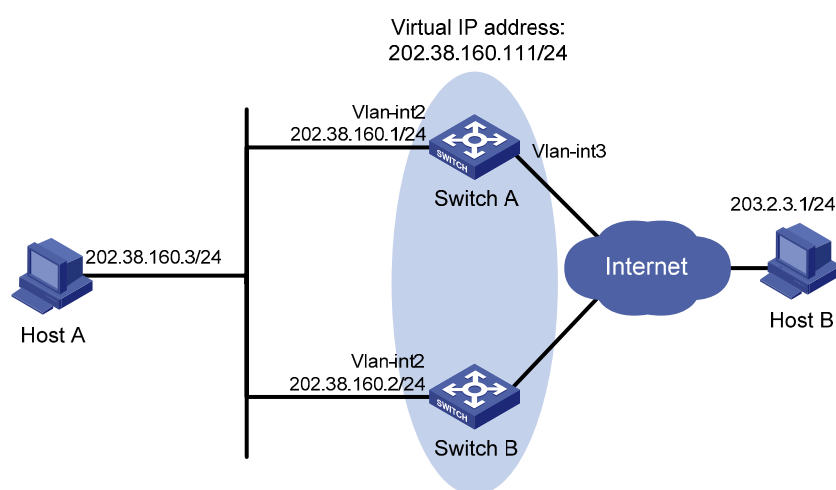
## 1.2 基于 IPv4 的 VRRP 监视接口举例

VRRP 的监视接口功能更好地扩充了 Backup 交换机的备份功能，即不仅能在备份组所在的接口出现故障时提供备份功能，而且在交换机的其它接口不可用时，也可以使用备份功能。具体做法是通过设置监视某个接口的命令来实现。

当被监视的接口 DOWN 掉时，拥有这个接口的交换机的优先级会自动降低一个数值（*value-reduced*），可能导致备份组内其它交换机的优先级高于这个交换机的优先级，从而使得其它优先级高的交换机转变为 Master。

### 1.2.1 组网图

图1-2 VRRP 监视接口配置组网图



### 1.2.2 应用要求

通过配置监视接口来实现：即使交换机 A 仍然工作，但当其连接 Internet 的接口不可用时，由 Switch B（具备另外一条链路和外界相连）来行使网关的职能。

为了便于说明，设备备份组号为 1。

- Host A 需要访问 Internet 上的 Host B，Host A 的缺省网关为 202.38.160.111/24；
- Switch A 和 Switch B 属于虚拟 IP 地址为 202.38.160.111 的备份组 1；
- 当 Switch A 正常工作时，Host A 发送给 Host B 的报文通过 Switch A 转发；当 Switch A 连接 Internet 的 VLAN 接口 3 不可用时，Host A 发送给 Host B 的报文通过 Switch B 转发。

### 1.2.3 适用产品、版本

表1-3 配置适用的产品与软硬件版本关系

| 产品             | 软件版本                            | 硬件版本    |
|----------------|---------------------------------|---------|
| S3610 系列以太网交换机 | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |

| 产品                | 软件版本                            | 硬件版本    |
|-------------------|---------------------------------|---------|
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本 |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本 |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本 |

#### 1.2.4 配置过程和解释

- 配置 Switch A

# 配置 VLAN2。

```
<Switch A> system-view
[Switch A] vlan 2
[Switch A-vlan2] port Ethernet1/0/6
[Switch A-vlan2] quit
[Switch A] interface Vlan-interface 2
[Switch A-Vlan-interface2] ip address 202.38.160.1 255.255.255.0
```

# 创建一个备份组。

```
[Switch A-Vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.111
```

# 设置备份组的优先级。

```
[Switch A-Vlan-interface2] vrrp vrid 1 priority 110
```

# 设置监视接口。

```
[Switch A-Vlan-interface2] vrrp vrid 1 track interface Vlan-interface 3 reduced 30
```

- 配置 Switch B

# 配置 VLAN2。

```
<Switch B> system-view
[Switch B] vlan 2
[Switch B-vlan2] port Ethernet1/0/5
[Switch B-vlan2] quit
[Switch B] interface Vlan-interface 2
[Switch B-Vlan-interface2] ip address 202.38.160.2 255.255.255.0
```

# 创建一个备份组。

```
[Switch B-Vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.111
```

配置完成后，可以通过 **display vrrp** 命令查看配置后的结果。

正常情况下，Switch A 行使网关的职能，当 Switch A 的接口 Vlan-interface 3 不可用时，Switch A 的优先级降低 30，低于 Switch B 优先级，Switch B 将抢占成为 Master 行使网关的职能。

当 Switch A 的接口 Vlan-interface3 恢复工作后，Switch A 能够继续成为 Master 行使网关的职能。

#### 1.2.5 完整配置

- SwitchA 上的配置

```
#
interface Vlan-interface2
ip address 202.38.160.1 255.255.255.0
vrrp vrid 1 virtual-ip 202.38.160.111
vrrp vrid 1 priority 110
vrrp vrid 1 track interface Vlan-interface3 reduced 30
#
interface Ethernet1/0/6
port access vlan 2
#
• SwitchB 上的配置
#
interface Vlan-interface2
ip address 202.38.160.2 255.255.255.0
vrrp vrid 1 virtual-ip 202.38.160.111
#
interface Ethernet1/0/5
port access vlan 2
#
```

### 1.2.6 配置注意事项

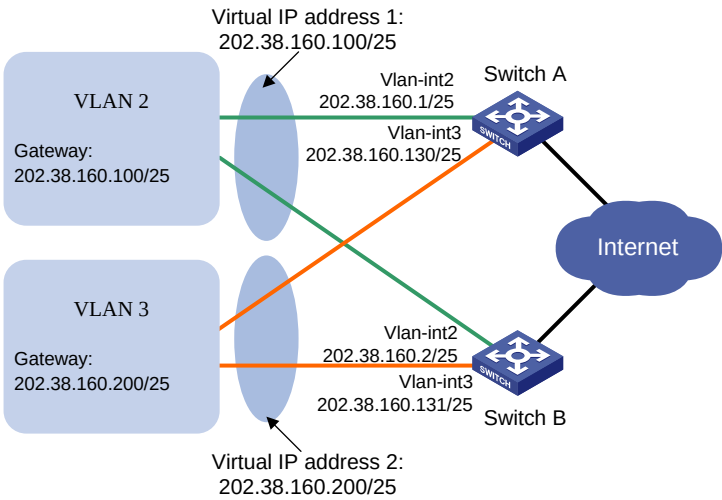
- 虚拟 IP 地址和接口 IP 地址必须在同一网段，且为合法的主机地址，不能为全零地址(0.0.0.0)、广播地址(255.255.255.255)、环回地址、非 A/B/C 类地址和其它非法 IP 地址(如 0.0.0.1)，否则备份组无法正常工作。
- 不允许对 IP 地址所有者进行监视指定接口的配置。
- 建议用户在配置监视接口功能时，在上行 Trunk 端口禁止 VRRP 备份组监视接口所对应的 VLAN 通过。
- 被监视接口的状态由 down 变为 up 后，对应设备的优先级数会自动恢复。
- 用户在配置降低优先级幅度时，需要确保降低后的优先级，比备份组内其他交换机的优先级要低，确保备份组内有其他交换机被选为 Master 交换机。
- 对于同一个 VRRP 备份组的配置，必须保证备份组虚拟路由器的 IP 地址个数、每个备份组虚拟路由器的 IP 地址、定时器间隔时间和认证方式完全一样。
- 如果网络流量过大或者不同的交换机上的定时器差异等因素，会导致 Backup 路由器的定时器异常超时而发生状态转换。对于这种情况，可以通过将 VRRP 通告报文的发送时间间隔延长和设置抢占延迟时间的办法来解决。

## 1.3 基于 IPv4 的 VRRP 多备份组举例

通过 VRRP 多备份组的组网，实现了链路备份功能和负载分担功能。保证用户在交换机发生故障，或者当链路流量较大的时候，不会因为故障导致与外部网络中止联系。

1.3.1 组网图

图1-3 VRRP 多备份组配置组网图



1.3.2 应用要求

- VLAN 2 内主机的缺省网关为 202.38.160.100/25；VLAN 3 内主机的缺省网关为 202.38.160.200/25；
- Switch A 和 Switch B 同时属于虚拟 IP 地址为 202.38.160.100/25 的备份组 1 和虚拟 IP 地址为 202.38.160.200/25 的备份组 2；
- 在备份组 1 中 Switch A 的优先级高于 Switch B，在备份组 2 中 Switch B 的优先级高于 Switch A，从而保证 VLAN 2 和 VLAN 3 内的主机分别通过 Switch A 和 Switch B 通信，当 Switch A 或 Switch B 出现故障时，主机可以通过另一台设备继续通信，避免通信中断。

1.3.3 适用产品、版本

表1-4 配置适用的产品与软硬件版本关系

| 产品                | 软件版本                            | 硬件版本    |
|-------------------|---------------------------------|---------|
| S3610 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5510 系列以太网交换机    | Release 5301, Release 5303 软件版本 | 全系列硬件版本 |
| S5500-EI 系列以太网交换机 | Release 2102 软件版本               | 全系列硬件版本 |
| S7500E 系列以太网交换机   | Release 6100, Release 6300 软件版本 | 全系列硬件版本 |
| S3500-EA 系列以太网交换机 | Release 5303 软件版本               | 全系列硬件版本 |

1.3.4 配置过程和解释

- 配置 Switch A
- # 配置 VLAN2。
- ```
<Switch A> system-view
[Switch A] vlan 2
```

```
[Switch A-vlan2] port Ethernet1/0/5
[Switch A-vlan2] quit
[Switch A] interface Vlan-interface 2
[Switch A-Vlan-interface2] ip address 202.38.160.1 255.255.255.128
# 创建一个备份组 1，并配置备份组 1 的虚拟 IP 地址为 202.38.160.100。
[Switch A-Vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.100
# 设置备份组的优先级。
[Switch A-Vlan-interface2] vrrp vrid 1 priority 110
[Switch A-Vlan-interface2] quit
```

配置 VLAN 3。

```
[Switch A] vlan 3
[Switch A-vlan3] port Ethernet 1/0/6
[Switch A-vlan3] quit
[Switch A] interface vlan-interface 3
[Switch A-Vlan-interface3] ip address 202.38.160.130 255.255.255.128
# 创建一个备份组 2，并配置备份组 2 的虚拟 IP 地址为 202.38.160.200。
[Switch A-Vlan-interface3] vrrp vrid 2 virtual-ip 202.38.160.200
```

• 配置 Switch B

配置 VLAN2。

```
<Switch B> system-view
[Switch B] vlan 2
[Switch B-vlan2] port Ethernet1/0/5
[Switch B-vlan2] quit
[Switch B] interface Vlan-interface 2
[Switch B-Vlan-interface2] ip address 202.38.160.2 255.255.255.128
# 创建一个备份组 1，并配置备份组 1 的虚拟 IP 地址为 202.38.160.100。
[Switch B-Vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.100
[Switch B-Vlan-interface2] quit
```

配置 VLAN 3。

```
[Switch B] vlan 3
[Switch B-vlan3] port Ethernet 1/0/6
[Switch B-vlan3] quit
[Switch B] interface vlan-interface 3
[Switch B-Vlan-interface3] ip address 202.38.160.131 255.255.255.128
# 创建一个备份组 2，并配置备份组 2 的虚拟 IP 地址为 202.38.160.200。
[Switch B-Vlan-interface3] vrrp vrid 2 virtual-ip 202.38.160.200
```

设置备份组的优先级。

```
[Switch B-Vlan-interface3] vrrp vrid 2 priority 110
```

配置完成后，可以通过 **display vrrp** 命令查看配置后的结果。

在备份组 1 中 Switch A 为 Master 交换机，Switch B 为 Backup 交换机，缺省网关为 202.38.160.100/25 的主机通过 Switch A 访问 Internet；备份组 2 中 Switch A 为 Backup 交换机，Switch B 为 Master 交换机，缺省网关为 202.38.160.200/25 的主机通过 Switch B 访问 Internet。

1.3.5 完整配置

- Switch A 上的配置

```
#
interface Vlan-interface2
 ip address 202.38.160.1 255.255.255.128
 vrrp vrid 1 virtual-ip 202.38.160.100
 vrrp vrid 1 priority 110
#
interface Vlan-interface3
 ip address 202.38.160.130 255.255.255.128
 vrrp vrid 2 virtual-ip 202.38.160.200
#
interface Ethernet1/0/5
 port access vlan 2
#
interface Ethernet1/0/6
 port access vlan 3
#
```

- Switch B 上的配置

```
#
interface Vlan-interface2
 ip address 202.38.160.2 255.255.255.128
 vrrp vrid 1 virtual-ip 202.38.160.100
#
interface Vlan-interface3
 ip address 202.38.160.131 255.255.255.128
 vrrp vrid 2 virtual-ip 202.38.160.200
 vrrp vrid 2 priority 110
#
interface Ethernet1/0/5
 port access vlan 2
#
interface Ethernet1/0/6
 port access vlan 3
#
```

1.3.6 配置注意事项

- 虚拟 IP 地址和接口 IP 地址必须在同一网段，且为合法的主机地址，不能为全零地址(0.0.0.0)、广播地址(255.255.255.255)、环回地址、非 A/B/C 类地址和其它非法 IP 地址(如 0.0.0.1)，否则备份组无法正常工作。
- 对于同一个 VRRP 备份组的配置，必须保证备份组虚拟路由器的 IP 地址个数、每个备份组虚拟路由器的 IP 地址、定时器间隔时间和认证方式完全一样。
- 如果网络流量过大或者不同的交换机上的定时器差异等因素，会导致 Backup 路由器的定时器异常超时而发生状态转换。对于这种情况，可以通过将 VRRP 通告报文的发送时间间隔延长和设置抢占延迟时间的办法来解决。

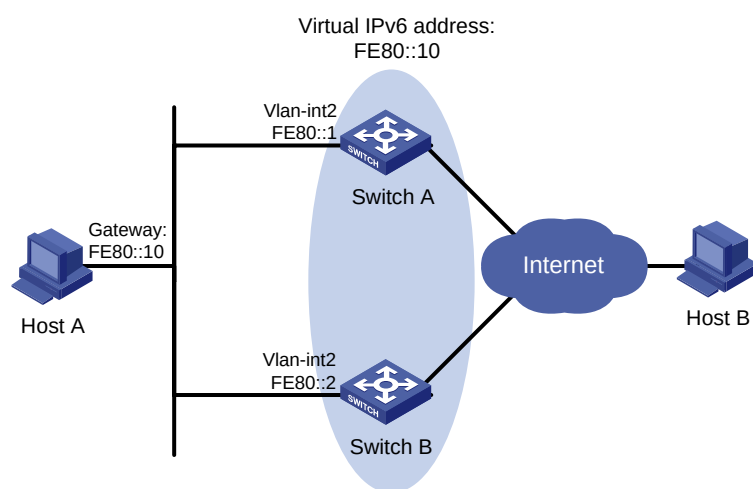
2 基于 IPv6 的 VRRP 典型配置指导

2.1 基于 IPv6 的 VRRP 单备份组举例

VRRP 协议的实现有 VRRPv2 和 VRRPv3 两个版本。其中,VRRPv2 基于 IPv4,VRRPv3 基于 IPv6。两个版本的 VRRP 在功能实现上并没有区别,只是在 IPv4 设备上和 IPv6 设备上使用的命令不同。借助 VRRP 单备份组组网,使用两台或多台交换机组成一个虚拟备份组,负责提供两条或多条通往外部网络的稳定的链路,避免备份组内的单台或多台交换机发生故障而引起的通信中断。

2.1.1 组网图

图2-1 VRRP 单备份组配置组网图



2.1.2 应用要求

- Host A 需要访问 Internet 上的 Host B, Host A 的缺省网关为 FE80::10;
- Switch A 和 Switch B 属于虚拟 IPv6 地址为 FE80::10 的备份组 1;
- 当 Switch A 正常工作时, Host A 发送给 Host B 的报文通过 Switch A 转发; 当 Switch A 出现故障时, Host A 发送给 Host B 的报文通过 Switch B 转发。

2.1.3 适用产品、版本

表2-1 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6100, Release 6300 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

2.1.4 配置过程和解释



说明

对于 S3610/S5510 系列以太网交换机，在使能 IPv6 功能之前，必须先将设备运行模式切换到 IPv4/IPv6 双协议栈模式，即执行 **switch-mode dual-ipv4-ipv6** 命令；否则，即使使能 IPv6，设备也不支持 IPv6 报文的转发。另外需要注意的是，执行 **switch-mode** 命令切换的协议栈只有在重启设备后才能生效。

- 配置交换机 A

配置 VLAN2。

```
<Switch A> system-view
[Switch A] ipv6
[Switch A] vlan 2
[Switch A-vlan2] port Ethernet1/0/6
[Switch A-vlan2] quit
[Switch A] interface Vlan-interface 2
[Switch A-Vlan-interface2] ipv6 address fe80::1 link-local
[Switch A-Vlan-interface2] ipv6 address 1::1 64
```

创建一个备份组。

```
[Switch A-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
```

设置交换机 A 在备份组中的优先级。

```
[Switch A-Vlan-interface2] vrrp ipv6 vrid 1 priority 110
```

设置 Switch A 工作在抢占方式。

```
[Switch A-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode
```



说明

缺省情况下，备份组工作在抢占方式，抢占延迟时间为 0 秒。

配置允许发布 RA 消息。

```
[Switch A-Vlan-interface2] undo ipv6 nd ra halt
```

- 配置交换机 B

配置 VLAN2。

```
<Switch B> system-view
[Switch B] ipv6
[Switch B] vlan 2
[Switch B-Vlan2] port Ethernet1/0/5
[Switch B-Vlan2] quit
[Switch B] interface Vlan-interface 2
[Switch B-Vlan-interface2] ipv6 address fe80::2 link-local
[Switch B-Vlan-interface2] ipv6 address 1::2 64
```


创建一个备份组。

```
[Switch B-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
```

配置允许发布 RA 消息。

```
[Switch B-Vlan-interface2] undo ipv6 nd ra halt
```

配置完成后，在 Host A 上可以 ping 通 Host B。通过 **display vrrp ipv6** 命令可以查看配置后的结果。

正常情况下，Switch A 行使网关的职能，当 Switch A 关机或出现故障，Switch B 将接替行使网关的职能。

设置抢占方式的目的是当 Switch A 恢复工作后，能够继续成为 Master 行使网关的职能。

2.1.5 完整配置

- Switch A 上的配置

```
#
ipv6
#
interface Vlan-interface2
  ipv6 address fe80::1 link-local
  ipv6 address 1::1 64
  vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
  vrrp ipv6 vrid 1 priority 110
  undo ipv6 nd ra halt
#
interface Ethernet1/0/6
  port access vlan 2
#
```

- SwitchB 上的配置

```
#
ipv6
#
interface Vlan-interface2
  ipv6 address fe80::2 link-local
  ipv6 address 1::2 64
  vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
  undo ipv6 nd ra halt
#
interface Ethernet1/0/5
  port access vlan 2
#
```

2.1.6 配置注意事项

- 对于同一个 VRRP 备份组的配置，必须保证备份组虚拟路由器的 IP 地址个数、每个备份组虚拟路由器的 IP 地址、定时器间隔时间和认证方式完全一样。

- 如果网络流量过大或者不同的交换机上的定时器差异等因素，会导致 Backup 路由器的定时器异常超时而发生状态转换。对于这种情况，可以通过将 VRRP 通告报文的发送时间间隔延长和设置抢占延迟时间的办法来解决。

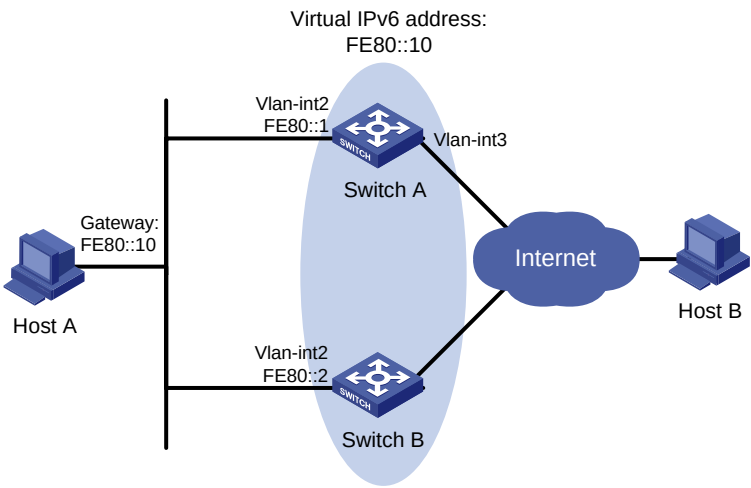
2.2 基于 IPv6 的 VRRP 监视接口举例

VRRP 的监视接口功能更好地扩充了 Backup 交换机的备份功能，即不仅能在备份组所在的接口出现故障时提供备份功能，而且在交换机的其它接口不可用时，也可以使用备份功能。具体做法是通过设置监视某个接口的命令来实现。

当被监视的接口 DOWN 掉时，拥有这个接口的交换机的优先级会自动降低一个数值（*value-reduced*），可能导致备份组内其它交换机的优先级高于这个交换机的优先级，从而使得其它优先级高的交换机转变为 Master。

2.2.1 组网图

图2-2 VRRP 监视接口配置组网图



2.2.2 应用要求

通过配置监视接口来实现：即使交换机 A 仍然工作，但当其连接 Internet 的接口不可用时，由 Switch B（具备另外一条链路和外界相连）来行使网关的职能。

为了便于说明，设备备份组号为 1。

- Host A 需要访问 Internet 上的 Host B，Host A 的缺省网关为 FE80::10；
- Switch A 和 Switch B 属于虚拟 IPv6 地址为 FE80::10 的备份组 1；
- 当 Switch A 正常工作时，Host A 发送给 Host B 的报文通过 Switch A 转发；当 Switch A 连接 Internet 的 VLAN 接口 3 不可用时，Host A 发送给 Host B 的报文通过 Switch B 转发。

2.2.3 适用产品、版本

表2-2 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本

产品	软件版本	硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6100, Release 6300 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

2.2.4 配置过程和解释



说明

对于 S3610/S5510 系列以太网交换机，在使能 IPv6 功能之前，必须先将设备运行模式切换到 IPv4/IPv6 双协议栈模式，即执行 **switch-mode dual-ipv4-ipv6** 命令；否则，即使使能 IPv6，设备也不支持 IPv6 报文的转发。另外需要注意的是，执行 **switch-mode** 命令切换的协议栈只有在重启设备后才能生效。

• 配置 Switch A

配置 VLAN2。

```
<Switch A> system-view
[Switch A] ipv6
[Switch A] vlan 2
[Switch A-vlan2] port Ethernet1/0/6
[Switch A-vlan2] quit
[Switch A] interface Vlan-interface 2
[Switch A-Vlan-interface2] ipv6 address fe80::1 link-local
[Switch A-Vlan-interface2] ipv6 address 1::1 64
```

创建一个备份组。

```
[Switch A-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
```

设置备份组的优先级。

```
[Switch A-Vlan-interface2] vrrp ipv6 vrid 1 priority 110
```

配置 Switch A 工作在抢占方式，抢占延迟时间为 5 秒。

```
[Switch A-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode timer delay 5
```

设置监视接口。

```
[Switch A-Vlan-interface2] vrrp ipv6 vrid 1 track interface Vlan-interface 3 reduced 30
```

• 配置 Switch B

配置 VLAN2。

```
<Switch B> system-view
[Switch B] ipv6
[Switch B] vlan 2
[Switch B-vlan2] port Ethernet1/0/5
[Switch B-vlan2] quit
```

```
[Switch B] interface Vlan-interface 2
[Switch B-Vlan-interface2] ipv6 address fe80::2 link-local
[Switch B-Vlan-interface2] ipv6 address 1::2 64
```

创建一个备份组。

```
[Switch B-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
```

配置 Switch B 工作在抢占方式，抢占延迟时间为 5 秒。

```
[SwitchB-Vlan-interface2] vrrp ipv6 vrid 1 preempt-mode timer delay 5
```

配置完成后，可以通过 **display vrrp ipv6** 命令查看配置后的结果。

正常情况下，Switch A 行使网关的职能，当 Switch A 的接口 Vlan-interface 3 不可用时，Switch A 的优先级降低 30，低于 Switch B 优先级，Switch B 将抢占成为 Master 行使网关的职能。

当 Switch A 的接口 Vlan-interface3 恢复工作后，Switch A 能够继续成为 Master 行使网关的职能。

2.2.5 完整配置

- Switch A 上的配置

```
#
ipv6
#
interface Vlan-interface2
ipv6 address fe80::1 link-local
ipv6 address 1::1 64
vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
vrrp ipv6 vrid 1 priority 110
vrrp ipv6 vrid 1 preempt-mode timer delay 5
vrrp ipv6 vrid 1 track interface Vlan-interface3 reduced 30
#
interface Ethernet1/0/6
port access vlan 2
#
```

- SwitchB 上的配置

```
#
ipv6
#
interface Vlan-interface2
ipv6 address fe80::2 link-local
ipv6 address 1::2 64
vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
vrrp ipv6 vrid 1 preempt-mode timer delay 5
#
interface Ethernet1/0/5
port access vlan 2
#
```

2.2.6 配置注意事项

- 不允许对 IP 地址所有者进行监视指定接口的配置。

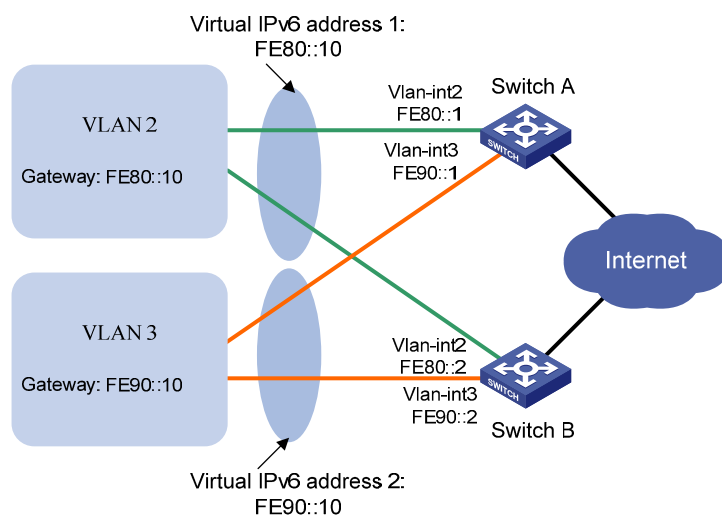
- 建议用户在配置监视接口功能时，在上行 Trunk 端口禁止 VRRP 备份组监视接口所对应的 VLAN 通过。
- 被监视接口的状态由 down 变为 up 后，对应设备的优先级数会自动恢复。
- 用户在配置降低优先级幅度时，需要确保降低后的优先级，比备份组内其他交换机的优先级要低，确保备份组内有其他交换机被选为 Master 交换机。
- 对于同一个 VRRP 备份组的配置，必须保证备份组虚拟路由器的 IP 地址个数、每个备份组虚拟路由器的 IP 地址、定时器间隔时间和认证方式完全一样。
- 如果网络流量过大或者不同的交换机上的定时器差异等因素，会导致 Backup 路由器的定时器异常超时而发生状态转换。对于这种情况，可以通过将 VRRP 通告报文的发送时间间隔延长和设置抢占延迟时间的办法来解决。

2.3 基于 IPv6 的 VRRP 多备份组举例

通过 VRRP 多备份组的组网，实现了链路备份功能和负载分担功能。保证用户在交换机发生故障，或者当链路流量较大的时候，不会因为故障导致与外部网络中止联系。

2.3.1 组网图

图2-3 VRRP 多备份组配置组网图



2.3.2 应用要求

- VLAN 2 内主机的缺省网关为 FE80::10；VLAN 3 内主机的缺省网关为 FE90::10；
- Switch A 和 Switch B 同时属于虚拟 IPv6 地址为 FE80::10 的备份组 1 和虚拟 IPv6 地址为 FE90::10 的备份组 2；
- 在备份组 1 中 Switch A 的优先级高于 Switch B，在备份组 2 中 Switch B 的优先级高于 Switch A，从而保证 VLAN 2 和 VLAN 3 内的主机分别通过 Switch A 和 Switch B 通信，当 Switch A 或 Switch B 出现故障时，主机可以通过另一台设备继续通信，避免通信中断。

2.3.3 适用产品、版本

表2-3 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6100, Release 6300 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

2.3.4 配置过程和解释



说明

对于 S3610/S5510 系列以太网交换机，在使能 IPv6 功能之前，必须先将设备运行模式切换到 IPv4/IPv6 双协议栈模式，即执行 **switch-mode dual-ipv4-ipv6** 命令；否则，即使使能 IPv6，设备也不支持 IPv6 报文的转发。另外需要注意的是，执行 **switch-mode** 命令切换的协议栈只有在重启设备后才能生效。

• 配置 Switch A

配置 VLAN2。

```
<Switch A> system-view
[Switch A] ipv6
[Switch A] vlan 2
[Switch A-vlan2] port Ethernet1/0/5
[Switch A-vlan2] quit
[Switch A] interface Vlan-interface 2
[Switch A-Vlan-interface2] ipv6 address fe80::1 link-local
[Switch A-Vlan-interface2] ipv6 address 1::1 64
```

创建一个备份组 1，并配置备份组 1 的虚拟 IPv6 地址为 FE80::10。

```
[Switch A-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
```

设置备份组的优先级。

```
[Switch A-Vlan-interface2] vrrp ipv6 vrid 1 priority 110
[Switch A-Vlan-interface2] quit
```

配置 VLAN 3。

```
[Switch A] vlan 3
[Switch A-vlan3] port Ethernet 1/0/6
[Switch A-vlan3] quit
[Switch A] interface vlan-interface 3
[Switch A-Vlan-interface3] ipv6 address fe90::1 link-local
[Switch A-Vlan-interface3] ipv6 address 2::1 64
```

创建一个备份组 2，并配置备份组 2 的虚拟 IPv6 地址为 FE90::10。

```
[Switch A-Vlan-interface3] vrrp ipv6 vrid 2 virtual-ip fe90::10 link-local
```

- 配置 Switch B

配置 VLAN2。

```
<Switch B> system-view
```

```
[Switch A] ipv6
```

```
[Switch B] vlan 2
```

```
[Switch B-vlan2] port Ethernet1/0/5
```

```
[Switch B-vlan2] quit
```

```
[Switch B] interface Vlan-interface 2
```

```
[Switch B-Vlan-interface2] ipv6 address fe80::2 link-local
```

```
[Switch B-Vlan-interface2] ipv6 address 1::2 64
```

创建一个备份组 1。

```
[Switch B-Vlan-interface2] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
```

```
[Switch B-Vlan-interface2] quit
```

配置 VLAN 3。

```
[Switch B] vlan 3
```

```
[Switch B-vlan3] port Ethernet 1/0/6
```

```
[Switch B-vlan3] quit
```

```
[Switch B] interface vlan-interface 3
```

```
[Switch B-Vlan-interface3] ipv6 address fe90::2 link-local
```

```
[Switch B-Vlan-interface3] ipv6 address 2::2 64
```

创建一个备份组 2，并配置备份组 2 的虚拟 IPv6 地址为 FE90::10。

```
[Switch B-Vlan-interface3] vrrp ipv6 vrid 2 virtual-ip fe90::10 link-local
```

设置备份组的优先级。

```
[Switch B-Vlan-interface3] vrrp ipv6 vrid 2 priority 110
```

配置完成后，可以通过 **display vrrp** 命令查看配置后的结果。

在备份组 1 中 Switch A 为 Master 交换机，Switch B 为 Backup 交换机，缺省网关为 FE80::10 的主机通过 Switch A 访问 Internet；备份组 2 中 Switch A 为 Backup 交换机，Switch B 为 Master 交换机，缺省网关为 FE90::10 的主机通过 Switch B 访问 Internet。

2.3.5 完整配置

- Switch A 上的配置

```
#
```

```
ipv6
```

```
#
```

```
interface Vlan-interface2
```

```
ipv6 address fe80::1 link-local
```

```
ipv6 address 1::1 64
```

```
vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
```

```
vrrp ipv6 vrid 1 priority 110
```

```
#
```

```
interface Vlan-interface3
```

```

ipv6 address fe90::1 link-local
ipv6 address 2::1 64
vrrp ipv6 vrid 2 virtual-ip fe90::10 link-local
#
interface Ethernet1/0/5
port access vlan 2
#
interface Ethernet1/0/6
port access vlan 3
#

```

• SwitchB 上的配置

```

#
ipv6
#
interface Vlan-interface2
ipv6 address fe80::2 link-local
ipv6 address 1::2 64
vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
#
interface Vlan-interface3
ipv6 address fe90::2 link-local
ipv6 address 2::2 64
vrrp ipv6 vrid 2 virtual-ip fe80::20 link-local
vrrp ipv6 vrid 2 priority 110
#
interface Ethernet1/0/5
port access vlan 2
#
interface Ethernet1/0/6
port access vlan 3
#

```

2.3.6 配置注意事项

- IPv6 网络中，主机需要手动配置默认网关才能实现 VRRP 备份组负载分担的功能。
- 对于同一个 VRRP 备份组的配置，必须保证备份组虚拟路由器的 IP 地址个数、每个备份组虚拟路由器的 IP 地址、定时器间隔时间和认证方式完全一样。
- 如果网络流量过大或者不同的交换机上的定时器差异等因素，会导致 Backup 路由器的定时器异常超时而发生状态转换。对于这种情况，可以通过将 VRRP 通告报文的发送时间间隔延长和设置抢占延迟时间的办法来解决。

目 录

1 SSH典型配置指导	1-1
1.1 设备作为SSH服务器并采用password认证时的配置指导	1-1
1.1.1 组网图	1-1
1.1.2 应用要求	1-1
1.1.3 适用产品、版本	1-1
1.1.4 配置过程和解释	1-1
1.1.5 完整配置	1-3
1.1.6 配置注意事项	1-4
1.2 设备作为SSH服务器并采用publickey认证（认证密钥算法为RSA）时的配置指导	1-4
1.2.1 组网图	1-4
1.2.2 应用要求	1-4
1.2.3 适用产品、版本	1-4
1.2.4 配置过程和解释	1-5
1.2.5 完整配置	1-9
1.2.6 配置注意事项	1-10
1.3 设备作为SSH客户端并采用password认证时的配置指导	1-10
1.3.1 组网图	1-10
1.3.2 应用要求	1-10
1.3.3 适用产品、版本	1-10
1.3.4 配置过程和解释	1-11
1.3.5 完整配置	1-13
1.3.6 配置注意事项	1-14
1.4 设备作为SSH客户端并采用publickey认证（认证密钥算法为DSA）时的配置指导	1-14
1.4.1 组网图	1-14
1.4.2 应用要求	1-14
1.4.3 适用产品、版本	1-14
1.4.4 配置过程和解释	1-15
1.4.5 完整配置	1-16
1.4.6 配置注意事项	1-17
1.5 设备作为SFTP客户端典型配置指导	1-17
1.5.1 组网图	1-17
1.5.2 应用要求	1-18
1.5.3 适用产品、版本	1-18
1.5.4 配置过程和解释	1-18
1.5.5 完整配置	1-21
1.5.6 配置注意事项	1-22
1.6 设备作为SFTP服务器典型配置指导	1-22
1.6.1 组网图	1-22
1.6.2 应用要求	1-22
1.6.3 适用产品、版本	1-22
1.6.4 配置过程和解释	1-23
1.6.5 完整配置	1-24

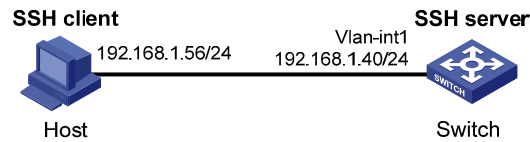
1.6.6 配置注意事项 1-25

1 SSH 典型配置指导

1.1 设备作为 SSH 服务器并采用 password 认证时的配置指导

1.1.1 组网图

图1-1 设备作为 SSH 服务器并采用 password 认证时的配置组网图



1.1.2 应用要求

如图 1-1，配置Host（SSH客户端）与Switch建立本地连接。Host采用SSH协议登录到Switch上，以保证数据信息交换的安全。SSH用户采用的认证方式为password认证。

1.1.3 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5500-SI 系列以太网交换机	Release 1207 软件版本	全系列硬件版本 (除 S5500-20TP-SI)
	Release 1301 软件版本	S5500-20TP-SI
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6100, Release 6300 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.1.4 配置过程和解释

(1) 配置 SSH 服务器 Switch

生成 RSA 及 DSA 密钥对，并启动 SSH 服务器。

```
<Switch> system-view
[Switch] public-key local create rsa
[Switch] public-key local create dsa
[Switch] ssh server enable
```



注意

- 生成服务器端的 RSA 和 DSA 密钥对是完成 SSH 登录的必要操作。
 - 因为 S7500E 以太网交换机、S3610 以太网交换机、S5510 以太网交换机和 S3500-EA 以太网交换机只支持 RSA 密钥对，所以当 S7500E、S3610、S5510 或 S3500-EA 作为服务器时只用生成 RSA 密钥对。
-

配置 VLAN 接口 1 的 IP 地址，客户端将通过该地址连接 SSH 服务器。

```
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ip address 192.168.1.40 255.255.255.0
[Switch-Vlan-interface1] quit
```

设置 SSH 客户端登录用户界面的认证方式为 AAA 认证。

```
[Switch] user-interface vty 0 4
[Switch-ui-vty0-4] authentication-mode scheme
```

设置 Switch 上远程用户登录协议为 SSH。

```
[Switch-ui-vty0-4] protocol inbound ssh
[Switch-ui-vty0-4] quit
```

创建本地用户 client001，并设置用户访问的命令级别为 3。

```
[Switch] local-user client001
[Switch-luser-client001] password simple aabbcc
[Switch-luser-client001] service-type ssh level 3
[Switch-luser-client001] quit
```

配置 SSH 用户 client001 的服务类型为 Stelnet，认证方式为 password 认证。

```
[Switch] ssh user client001 service-type stelnet authentication-type
password
```

(2) 配置 SSH 客户端 Host



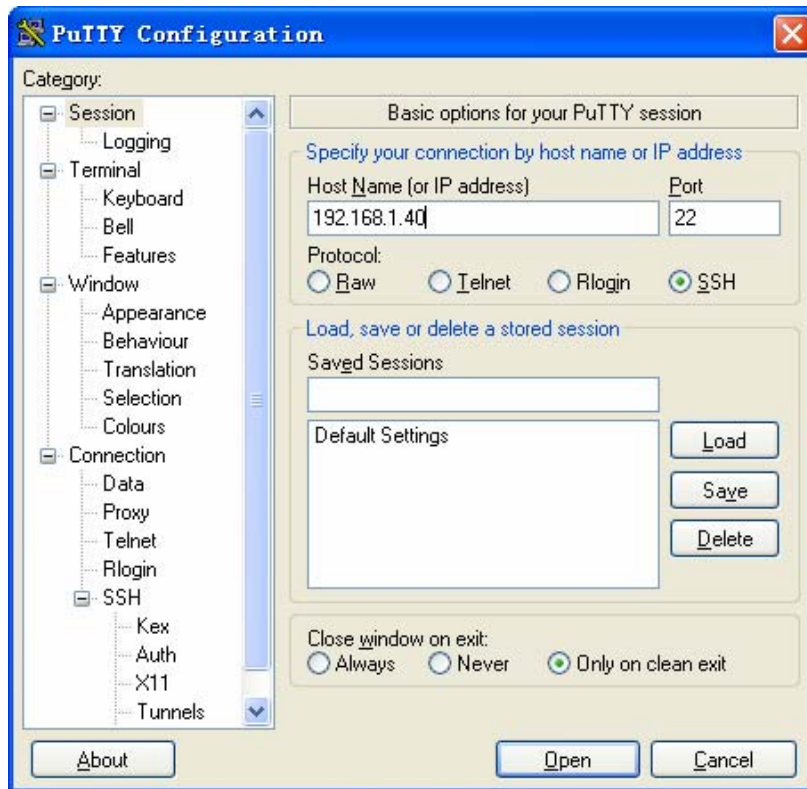
说明

SSH 客户端软件有很多，例如 PuTTY、OpenSSH 等。本文中仅以客户端软件 PuTTY0.58 为例，说明 SSH 客户端的配置方法。

建立与 SSH 服务器端的连接。

打开 PuTTY.exe 程序，出现如图 1-2 所示的客户端配置界面。在“Host Name (or IP address)”文本框中输入 SSH 服务器的 IP 地址为 192.168.1.40。

图1-2 SSH 客户端配置界面



在图 1-2 中，单击<Open>按钮，按提示输入用户名client001 及密码aabbcc，即可进入Switch的配置界面。

1.1.5 完整配置

- SSH 服务器端配置

```
#
vlan 1
#
local-user client001
password simple aabbcc
service-type ssh
level 3
#
interface Vlan-interface1
ip address 192.168.1.40 255.255.255.0
#
ssh server enable
ssh user client001 service-type stelnet authentication-type password
#
user-interface vty 0 4
authentication-mode scheme
user privilege level 3
protocol inbound ssh
#
```

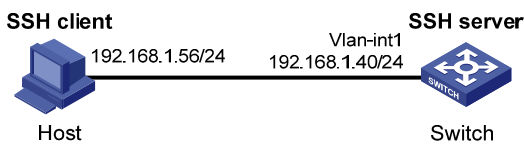
1.1.6 配置注意事项

- SSH 客户端通过 `publickey` 和 `password` 两种方式进行认证尝试的次数总和，不能超过 `ssh server authentication-retries` 命令配置的 SSH 连接认证尝试次数，否则，客户端认证失败，无法登录 SSH 服务器。
- 目前，设备作为 SSH 服务器时，支持 SSH2 和 SSH1 两个版本；设备作为 SSH 客户端时，只支持 SSH2 版本。
- S7500E 以太网交换机、S3610 以太网交换机、S5510 以太网交换机和 S3500-EA 以太网交换机只支持 RSA 密钥对。

1.2 设备作为 SSH 服务器并采用 publickey 认证（认证密钥算法为 RSA）时的配置指导

1.2.1 组网图

图1-3 设备作为 SSH 服务器并采用 publickey 认证时的配置组网图



1.2.2 应用要求

如图 1-3，配置 Host（SSH 客户端）与 Switch 建立本地连接。Host 采用 SSH 协议登录到 Switch 上，以保证数据信息交换的安全。SSH 用户采用的认证方式为 `publickey` 认证，认证时采用的公共密钥算法为 RSA。

1.2.3 适用产品、版本

表1-2 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5500-SI 系列以太网交换机	Release 1207 软件版本	全系列硬件版本 (除 S5500-20TP-SI)
	Release 1301 软件版本	S5500-20TP-SI
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6100, Release 6300 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.2.4 配置过程和解释

(1) 配置 SSH 服务器 Switch

生成 RSA 及 DSA 密钥对，并启动 SSH 服务器。

```
<Switch> system-view
[Switch] public-key local create rsa
[Switch] public-key local create dsa
[Switch] ssh server enable
```



注意

- 生成服务器端的 RSA 和 DSA 密钥对是完成 SSH 登录的必要操作。
 - 因为 S7500E 以太网交换机、S3610 以太网交换机、S5510 以太网交换机和 S3500-EA 以太网交换机只支持 RSA 密钥对，所以当 S7500E、S3610、S5510 或 S3500-EA 作为服务器时只用生成 RSA 密钥对。
-

配置 VLAN 接口 1 的 IP 地址，客户端将通过该地址连接 SSH 服务器。

```
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ip address 192.168.1.40 255.255.255.0
[Switch-Vlan-interface1] quit
```

设置用户接口上认证模式为 AAA 认证。

```
[Switch] user-interface vty 0 4
[Switch-ui-vty0-4] authentication-mode scheme
```

设置 Switch 上远程用户登录协议为 SSH。

```
[Switch-ui-vty0-4] protocol inbound ssh
```

设置用户能访问的命令级别为 3。

```
[Switch-ui-vty0-4] user privilege level 3
[Switch-ui-vty0-4] quit
```



说明

这里需要先在 SSH 客户端使用 SSH 客户端软件生成 RSA 密钥对，将生成的 RSA 公钥保存到指定文件中，并将此公钥文件通过 FTP/TFTP 方式上传到服务器端，文件名为 key.pub。相关配置请参见客户端的配置。

从文件 key.pub 中导入远端的公钥。

```
[Switch] public-key peer Switch001 import sshkey key.pub
```

设置 SSH 用户 client002 的认证方式为 publickey，并指定公钥为 Switch001。

```
[Switch] ssh user client002 service-type stelnet authentication-type
publickey assign publickey Switch001
```

(2) 配置 SSH 客户端 Host



说明

SSH 客户端软件有很多，例如 PuTTY、OpenSSH 等。本文中仅以客户端软件 PuTTY0.58 为例，说明 SSH 客户端的配置方法。

生成 RSA 密钥对。

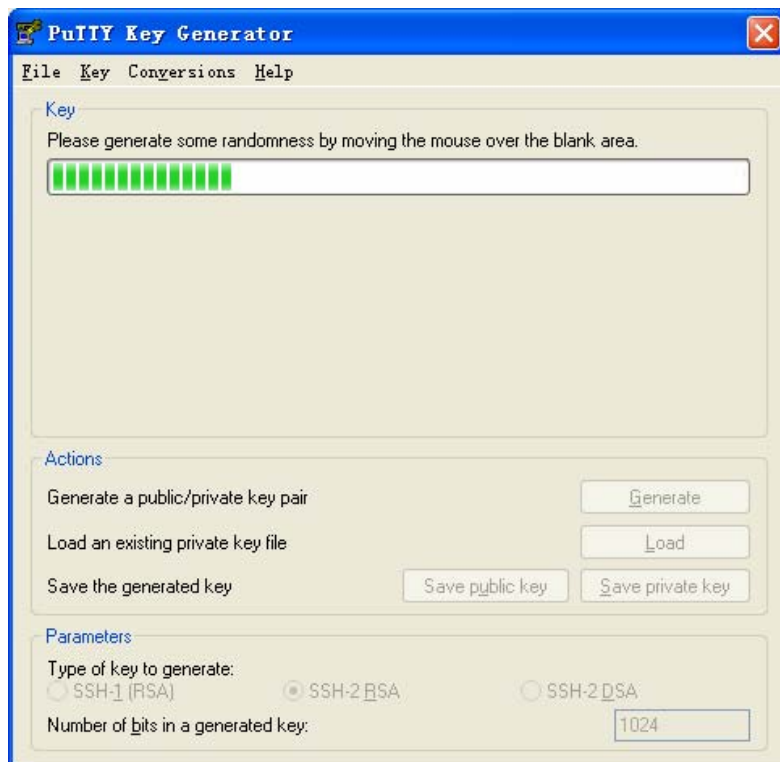
在客户端运行 PuTTYGen.exe，在参数栏中选择“SSH-2 RSA”，点击<Generate>，产生客户端密钥对。

图1-4 生成客户端密钥（1）



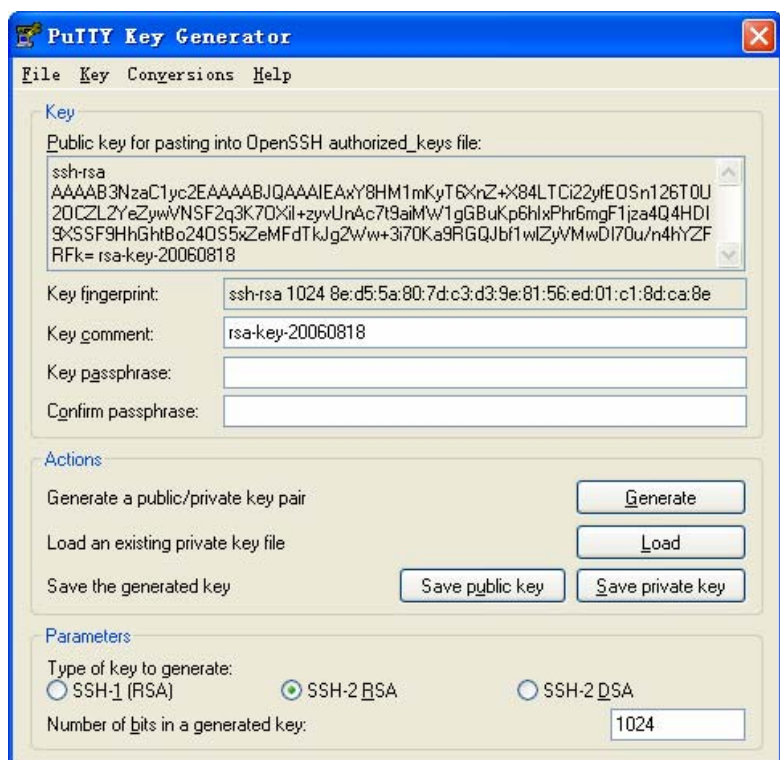
在产生密钥对的过程中需不停的移动鼠标，鼠标移动仅限于下图蓝色框中除绿色标记进程条外的地方，否则进程条的显示会不动，密钥对将停止产生，见 图 1-5。

图1-5 生成客户端密钥（2）



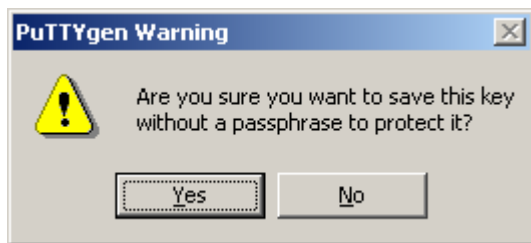
密钥对产生后，点击<Save public key>，输入存储公钥的文件名 key.pub，点击保存。

图1-6 生成客户端密钥（3）



点击<Save private key>存储私钥，弹出警告框，提醒是否保存没做任何保护措施私钥，点击<Yes>，输入私钥文件名为 private，点击保存。

图1-7 生成客户端密钥（4）



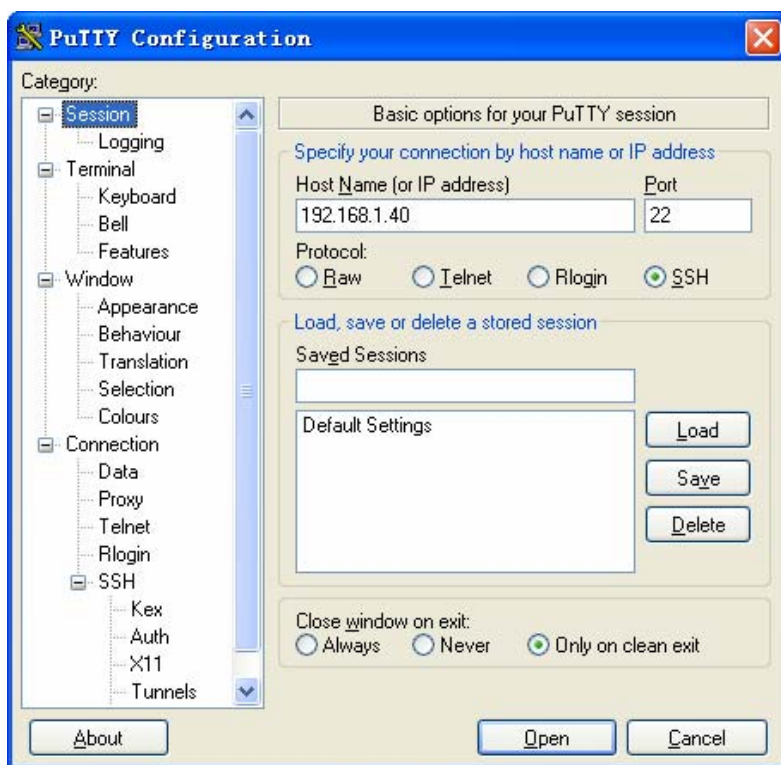
说明

客户端生成密钥对后，需要将保存的公钥文件通过 FTP/TFTP 方式上传到服务器，并完成服务器的配置后，才可继续客户端的配置。

指定私钥文件，并建立与 SSH 服务器的连接。

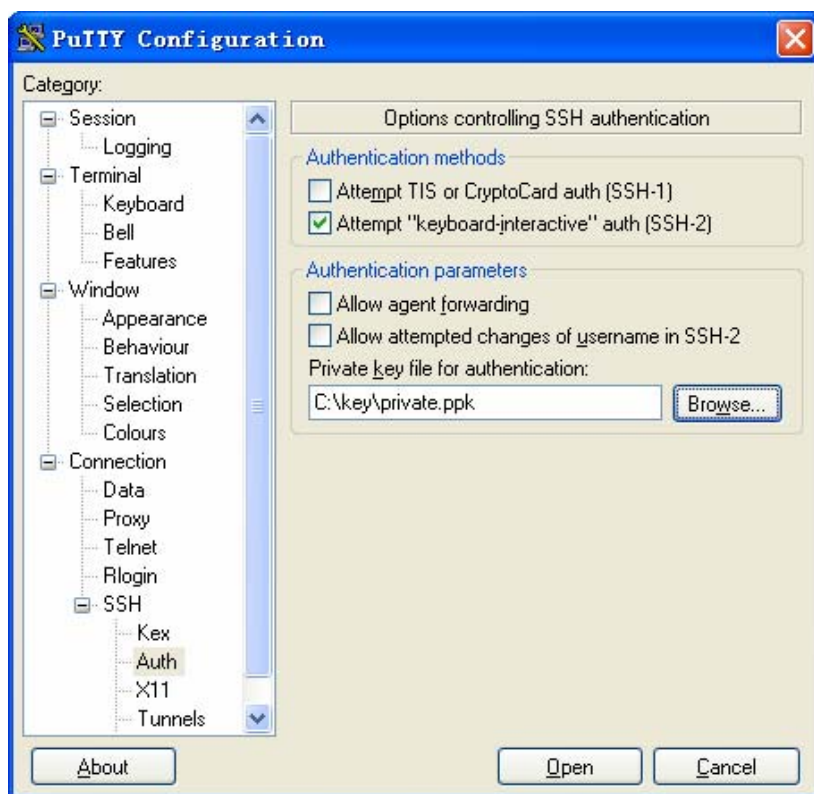
打开PuTTY.exe程序，出现如图 1-8所示的客户端配置界面。在“Host Name（or IP address）”文本框中输入SSH服务器的IP地址为 192.168.1.40。

图1-8 SSH 客户端配置界面（1）



单击“SSH”下面的“Auth”（认证），出现如图 1-9的界面。单击<Browse...>按钮，弹出文件选择窗口。选择与配置到服务器端的公钥对应的私钥文件private。

图1-9 SSH 客户端配置界面（2）



(3) 如图 1-9，单击<Open>按钮，按提示输入用户名client002，即可进入Switch的配置界面。

1.2.5 完整配置

- SSH 服务器端配置

```
#
vlan 1
#
public-key peer Switch001
public-key-code begin
30819D300D06092A864886F70D010101050003818B0030818702818100A2DBC1FD76A837B
EF5D322598442D6753B2E8F7ADD6D6209C80843B206B309078AFE2416CB4FAD496A662724
3EAD766D57AEA70B901B4B4566D9A651B133BAE34E9B9F04E542D64D0E9814D7E3CBCDBCA
F28FF21EE4EADAE6DF52001944A40414DFF280FF043B14838288BE7F9438DC71ABBC2C28B
F78F34ADF3D1C912579A19020125
public-key-code end
peer-public-key end
#
interface Vlan-interface1
ip address 192.168.1.40 255.255.255.0
#
ssh server enable
ssh user client002 service-type stelnet authentication-type publickey
assign publickey Switch001
#
user-interface vty 0 4
authentication-mode scheme
```

```

user privilege level 3
protocol inbound ssh
#

```

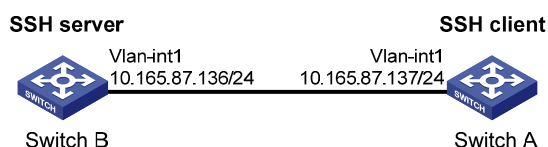
1.2.6 配置注意事项

- SSH 客户端通过 `publickey` 和 `password` 两种方式进行认证尝试的次数总和，不能超过 `ssh server authentication-retries` 命令配置的 SSH 连接认证尝试次数，否则，客户端认证失败，无法登录 SSH 服务器。
- 目前，设备作为 SSH 服务器时，支持 SSH2 和 SSH1 两个版本；设备作为 SSH 客户端时，只支持 SSH2 版本。
- S7500E 系列以太网交换机、S3610 系列以太网交换机、S5510 系列以太网交换机和 S3500-EA 系列以太网交换机只支持 RSA 密钥对。

1.3 设备作为 SSH 客户端并采用 password 认证时的配置指导

1.3.1 组网图

图1-10 设备作为 SSH 客户端并采用 password 认证时的配置组网图



1.3.2 应用要求

如图 1-10，配置 Switch A 作为客户端，采用 SSH 协议登录到 Switch B 上。SSH 用户采用的认证方式为 password 认证，用户名为 `client001`，密码为 `aabbcc`。

1.3.3 适用产品、版本

表1-3 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5500-SI 系列以太网交换机	Release 1207 软件版本	全系列硬件版本 (除 S5500-20TP-SI)
	Release 1301 软件版本	S5500-20TP-SI
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6100, Release 6300 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.3.4 配置过程和解释

(1) 配置 SSH 服务器 Switch B

生成 RSA 及 DSA 密钥对，并启动 SSH 服务器。

```
<SwitchB> system-view
[SwitchB] public-key local create rsa
[SwitchB] public-key local create dsa
[SwitchB] ssh server enable
```



注意

- 生成服务器端的 RSA 和 DSA 密钥对是完成 SSH 登录的必要操作。
 - 因为 S7500E 系列以太网交换机、S3610 系列以太网交换机、S5510 系列以太网交换机和 S3500-EA 系列以太网交换机只支持 RSA 密钥对，所以当 S7500E、S3610、S5510 或 S3500-EA 作为服务器时只用生成 RSA 密钥对。
-

配置 VLAN 接口 1 的 IP 地址，客户端将通过该地址连接 SSH 服务器。

```
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ip address 10.165.87.136 255.255.255.0
[SwitchB-Vlan-interface1] quit
```

设置 SSH 客户端登录用户界面的认证方式为 AAA 认证。

```
[SwitchB] user-interface vty 0 4
[SwitchB-ui-vty0-4] authentication-mode scheme
```

设置 Switch B 上远程用户登录协议为 SSH。

```
[SwitchB-ui-vty0-4] protocol inbound ssh
[SwitchB-ui-vty0-4] quit
```

创建本地用户 client001。

```
[SwitchB] local-user client001
[SwitchB-luser-client001] password simple aabbcc
[SwitchB-luser-client001] service-type ssh level 3
[SwitchB-luser-client001] quit
```

配置 SSH 用户 client001 的服务类型为 Stelnet，认证方式为 password 认证。

```
[SwitchB] ssh user client001 service-type stelnet authentication-type
password
```

(2) 配置 SSH 客户端 Switch A

配置 VLAN 接口 1 的 IP 地址。

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ip address 10.165.87.137 255.255.255.0
[SwitchA-Vlan-interface1] quit
```

配置客户端对服务器不进行首次认证。

```
[SwitchA] undo ssh client first-time
```

在客户端配置 SSH 服务器端的 DSA 主机公钥。在公共密钥编辑视图输入服务器端的主机公钥。



注意

因为 S7500E 系列以太网交换机、S3610 系列以太网交换机、S5510 系列以太网交换机和 S3500-EA 系列以太网交换机只支持 RSA 密钥对，所以当 S7500E、S3610、S5510 或 S3500-EA 作为服务器时配置到客户端的主机公钥为 RSA 密钥对。

```
[SwitchA] public-key peer key1
[SwitchA-pkey-public-key] public-key-code begin
[SwitchA-pkey-key-code] 308201B73082012C06072A8648CE3804013082011F02818100
D757262C4584C44C211F18BD96E5F0
[SwitchA-pkey-key-code] 61C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE6
5BE6C265854889DC1EDBD13EC8B274
[SwitchA-pkey-key-code] DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B06
FD60FE01941DDD77FE6B12893DA76E
[SwitchA-pkey-key-code] EBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B36
8950387811C7DA33021500C773218C
[SwitchA-pkey-key-code] 737EC8EE993B4F2DED30F48EDACE915F0281810082269009E1
4EC474BAF2932E69D3B1F18517AD95
[SwitchA-pkey-key-code] 94184CCDFCEAE96EC4D5EF93133E84B47093C52B20CD35D024
92B3959EC6499625BC4FA5082E22C5
[SwitchA-pkey-key-code] B374E16DD00132CE71B020217091AC717B612391C76C1FB2E8
8317C1BD8171D41ECB83E210C03CC9
[SwitchA-pkey-key-code] B32E810561C21621C73D6DAAC028F4B1585DA7F42519718CC9
B09EEF0381840002818000AF995917
[SwitchA-pkey-key-code] E1E570A3F6B1C2411948B3B4FFA256699B3BF871221CC9C5DF
257523777D033BEE77FC378145F2AD
[SwitchA-pkey-key-code] D716D7DB9FCABB4ADB6FB4FDB0CA25C761B308EF53009F710
1F7C62621216D5A572C379A32AC290
[SwitchA-pkey-key-code] E55B394A217DA38B65B77F0185C8DB8095522D1EF044B465E8
716261214A5A3B493E866991113B2D
[SwitchA-pkey-key-code] 485348
[SwitchA-pkey-key-code] public-key-code end
[SwitchA-pkey-public-key] peer-public-key end
```

指定服务器 10.165.87.136 对应的主机公钥名称为 key1。

```
[SwitchA] ssh client authentication server 10.165.87.136 assign publickey
key1
[SwitchA] quit
```

建立到服务器 10.165.87.136 的 SSH 连接。

```
<SwitchA> ssh2 10.165.87.136
Username: client001
Trying 10.165.87.136
Press CTRL+K to abort
Connected to 10.165.87.136...
Enter password:
```

* Copyright (c) 2004-2007 Hangzhou H3C Tech. Co., Ltd. All rights reserved.*

```
* Without the owner's prior written consent,
* no decompiling or reverse-engineering shall be allowed.
*****
```

<SwitchB>

1.3.5 完整配置

- 配置 Switch B

```
#
vlan 1
#
local-user client001
password simple aabbcc
service-type ssh
level 3
#
interface Vlan-interface1
ip address 10.165.87.136 255.255.255.0
#
ssh server enable
ssh user client001 service-type stelnet authentication-type password
#
user-interface vty 0 4
authentication-mode scheme
user privilege level 3
protocol inbound ssh
#
```

- 配置 Switch A

```
#
vlan 1
#
public-key peer key1
public-key-code begin
308201B73082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18B
D96E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC
1EDBD13EC8B274DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B06FD60FE019
41DDD77FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B3689
50387811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F0281810082269
009E14EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C5
2B20CD35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC7
17B612391C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAA
C028F4B1585DA7F42519718CC9B09EEF0381840002818000AF995917E1E570A3F6B1C2411
948B3B4FFA256699B3BF871221CC9C5DF257523777D033BEE77FC378145F2ADD716D7DB9F
CABB4ADBF6FB4FDB0CA25C761B308EF53009F7101F7C62621216D5A572C379A32AC290E55
B394A217DA38B65B77F0185C8DB8095522D1EF044B465E8716261214A5A3B493E86699111
3B2D485348
public-key-code end
peer-public-key end
```



```
#
interface Vlan-interface1
ip address 10.165.87.137 255.255.255.0
#
undo ssh client first-time
ssh client authentication server 10.165.87.136 assign publickey key1
#
```

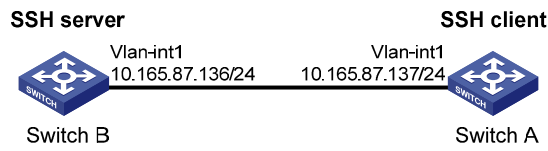
1.3.6 配置注意事项

- SSH 客户端通过 publickey 和 password 两种方式进行认证尝试的次数总和，不能超过 **ssh server authentication-retries** 命令配置的 SSH 连接认证尝试次数，否则，客户端认证失败，无法登录 SSH 服务器。
- 目前，设备作为 SSH 服务器时，支持 SSH2 和 SSH1 两个版本；设备作为 SSH 客户端时，只支持 SSH2 版本。
- S7500E 系列以太网交换机、S3610 系列以太网交换机、S5510 系列以太网交换机和 S3500-EA 系列以太网交换机只支持 RSA 密钥对。

1.4 设备作为 SSH 客户端并采用 publickey 认证（认证密钥算法为 DSA）时的配置指导

1.4.1 组网图

图1-11 设备作为 SSH 客户端并采用 publickey 认证时的配置组网图



1.4.2 应用要求

如 图 1-11，配置Switch A作为客户端，采用SSH协议登录到Switch B上。SSH用户采用的认证方式为publickey认证，认证时采用的公共密钥算法为DSA。

1.4.3 适用产品、版本

表1-4 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S5500-SI 系列以太网交换机	Release 1207 软件版本	全系列硬件版本 (除 S5500-20TP-SI)
	Release 1301 软件版本	S5500-20TP-SI
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本

1.4.4 配置过程和解释

(1) 配置 SSH 服务器 Switch B

生成 RSA 及 DSA 密钥对，并启动 SSH 服务器。

```
<SwitchB> system-view
[SwitchB] public-key local create rsa
[SwitchB] public-key local create dsa
[SwitchB] ssh server enable
```



注意

生成服务器端的 RSA 和 DSA 密钥对是完成 SSH 登录的必要操作。

配置 VLAN 接口 1 的 IP 地址，客户端将通过该地址连接 SSH 服务器。

```
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ip address 10.165.87.136 255.255.255.0
[SwitchB-Vlan-interface1] quit
```

设置 SSH 客户端登录用户界面的认证方式为 AAA 认证。

```
[SwitchB] user-interface vty 0 4
[SwitchB-ui-vty0-4] authentication-mode scheme
```

设置 Switch B 上远程用户登录协议为 SSH。

```
[SwitchB-ui-vty0-4] protocol inbound ssh
```

设置用户能访问的命令级别为 3。

```
[SwitchB-ui-vty0-4] user privilege level 3
[SwitchB-ui-vty0-4] quit
```



说明

这时需要先在 SSH 客户端生成 DSA 密钥对，将生成的 DSA 公钥保存到指定文件中，并将此公钥文件通过 FTP/TFTP 方式上传到服务器端，文件名为 key.pub。有关配置请参见客户端的配置。

从文件 key.pub 中导入远端的公钥。

```
[SwitchB] public-key peer Switch001 import sshkey key.pub
```

设置 SSH 用户 client002 的认证方式为 publickey，并指定公钥为 Switch001。

```
[SwitchB] ssh user client002 service-type stelnet authentication-type
publickey assign publickey Switch001
```

(2) 配置 SSH 客户端 Switch A

配置 VLAN 接口 1 的 IP 地址。

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ip address 10.165.87.137 255.255.255.0
[SwitchA-Vlan-interface1] quit
```

生成 DSA 密钥对。

```
[SwitchA] public-key local create dsa
# 将生成的 DSA 主机公钥导出到指定文件 key.pub 中。
[SwitchA] public-key local export dsa ssh2 key.pub
[SwitchA] quit
```



说明

客户端生成密钥对后，需要将保存的公钥文件通过 FTP/TFTP 方式上传到服务器，并完成服务器的配置后，才可继续客户端的配置。

建立到服务器 10.165.87.136 的 SSH 连接。

```
<SwitchA> ssh2 10.165.87.136
Username: client002
Trying 10.165.87.136 ...
Press CTRL+K to abort
Connected to 10.165.87.136 ...

The Server is not authenticated. Continue? [Y/N]:y
Do you want to save the server public key? [Y/N]:n

*****
* Copyright (c) 2004-2007 Hangzhou H3C Tech. Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,
* no decompiling or reverse-engineering shall be allowed.
*****

<SwitchB>
```

1.4.5 完整配置

- 配置 SwitchB

```
#
vlan 1
#
public-key peer Switch001
public-key-code begin
308201B73082012C06072A8648CE3804013082011F02818100D757262C4584C44C211F18B
D96E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C265854889DC
1EDBD13EC8B274DA9F75BA26CCB987723602787E922BA84421F22C3C89CB9B06FD60FE019
41DDD77FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F358214B16A2FAC4B3689
50387811C7DA33021500C773218C737EC8EE993B4F2DED30F48EDACE915F0281810082269
009E14EC474BAF2932E69D3B1F18517AD9594184CCDFCEAE96EC4D5EF93133E84B47093C5
2B20CD35D02492B3959EC6499625BC4FA5082E22C5B374E16DD00132CE71B020217091AC7
17B612391C76C1FB2E88317C1BD8171D41ECB83E210C03CC9B32E810561C21621C73D6DAA
C028F4B1585DA7F42519718CC9B09EEF038184000281803BF8D3EA929534652503080E493
17BFAC598C730EC8AD95C71354CAC413A67339072779F8264AD5209EFDD4A45A5929235A0
6F937DB49015F386FF4F8BD8FB0A6C26C8F6BDD15EA10A43EFB5AFF391CED1AC849647A8B
```

```

AA0AD5EFF7E1B28B549C681EC828BD855A2814B04D92DCD62AD667E486B99F2B4F4641F3C
968BA24D3C
public-key-code end
peer-public-key end
#
interface Vlan-interface1
ip address 10.165.87.136 255.255.255.0
#
ssh server enable
ssh user client002 service-type stelnet authentication-type publickey
assign publickey Switch001
#
user-interface vty 0 4
authentication-mode scheme
user privilege level 3
protocol inbound ssh
#
• 配置 Switch A
#
vlan 1
#
interface Vlan-interface1
ip address 10.165.87.137 255.255.255.0
#

```

1.4.6 配置注意事项

- SSH 客户端通过 **publickey** 和 **password** 两种方式进行认证尝试的次数总和，不能超过 **ssh server authentication-retries** 命令配置的 SSH 连接认证尝试次数，否则，客户端认证失败，无法登录 SSH 服务器。
- 目前，设备作为 SSH 服务器时，支持 SSH2 和 SSH1 两个版本；设备作为 SSH 客户端时，只支持 SSH2 版本。

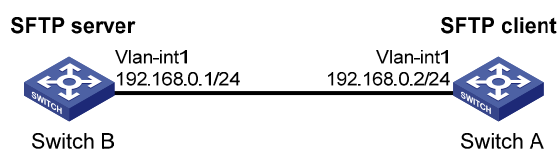
1.5 设备作为 SFTP 客户端典型配置指导

SFTP 是 Secure FTP 的简称，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。同时，由于设备支持作为客户端的功能，用户可以从本地设备安全登录到远程设备上，进行文件的安全传输。

1.5.1 组网图

图1-12 设备作为 SFTP 客户端组网图



1.5.2 应用要求

如图 1-12，Switch A和Switch B之间建立SSH连接，Switch A作为SFTP客户端登录到Switch B，进行文件管理和文件传送等操作。SSH用户采用的认证方式为publickey认证，认证时采用的公共密钥算法为RSA。

1.5.3 适用产品、版本

表1-5 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5500-SI 系列以太网交换机	Release 1207 软件版本	全系列硬件版本 (除 S5500-20TP-SI)
	Release 1301 软件版本	S5500-20TP-SI
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6100, Release 6300 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.5.4 配置过程和解释

(1) 配置服务器端 Switch B

生成 RSA 及 DSA 密钥对，并启动 SSH 服务器。

```
<SwitchB> system-view
[SwitchB] public-key local create rsa
[SwitchB] public-key local create dsa
[SwitchB] ssh server enable
```



注意

- 生成服务器端的 RSA 和 DSA 密钥对是完成 SFTP 登录的必要操作。
- 因为 S7500E 系列以太网交换机、S3610 系列以太网交换机、S5510 系列以太网交换机和 S3500-EA 系列以太网交换机只支持 RSA 密钥对，所以当 S7500E、S3610、5510 或 S3500-EA 作为 SFTP 服务器时只用生成 RSA 密钥对。

启动 SFTP 服务器。

```
[SwitchB] sftp server enable
```

配置 VLAN 接口 1 的 IP 地址，客户端将通过该地址连接 SSH 服务器。

```
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ip address 192.168.0.1 255.255.255.0
[SwitchB-Vlan-interface1] quit
```

设置 SSH 客户端登录用户界面的认证方式为 AAA 认证。

```
[SwitchB] user-interface vty 0 4
[SwitchB-ui-vty0-4] authentication-mode scheme

# 设置 Switch B 上远程用户登录协议为 SSH。

[SwitchB-ui-vty0-4] protocol inbound ssh
[SwitchB-ui-vty0-4] quit
```



说明

这时需要先在 SFTP 客户端生成 RSA 密钥对，将生成的 RSA 公钥保存到指定文件中，并将此公钥文件通过 FTP/TFTP 方式上传到服务器端，文件名为 **pubkey**。有关配置请参见客户端的配置。

从文件 **pubkey** 中导入远端的公钥。

```
[SwitchB] public-key peer Switch001 import sshkey pubkey
```

设置 SSH 用户 **client001** 的服务类型为 SFTP，认证方式为 **publickey**，并指定公钥为 **Switch001**，工作目录为 **cf:/**。

```
[SwitchB] ssh user client001 service-type sftp authentication-type publickey
assign publickey Switch001 work-directory cf:/
```

(2) 配置客户端 Switch A

配置 VLAN 接口 1 的 IP 地址。

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ip address 192.168.0.2 255.255.255.0
[SwitchA-Vlan-interface1] quit
```

生成 RSA 密钥对。

```
[SwitchA] public-key local create rsa
```

将生成的 RSA 主机公钥导出到指定文件 **pubkey** 中。

```
[SwitchA] public-key local export rsa ssh2 pubkey
[SwitchA] quit
```



说明

客户端生成密钥对后，需要将保存的公钥文件通过 FTP/TFTP 方式上传到服务器，并完成服务器的配置后，才可继续客户端的配置。

与远程 SFTP 服务器建立连接，进入 SFTP Client 视图。

```
<SwitchA> sftp 192.168.0.1
```

```
Input Username: client001
```

```
Trying 192.168.0.1 ...
```

```
Press CTRL+K to abort
```

```
Connected to 192.168.0.1 ...
```

```
The Server is not authenticated. Continue? [Y/N]:y
```

```
Do you want to save the server public key? [Y/N]:n
```

```
sftp-client>
```

显示服务器的当前目录，删除文件 z，并检查此目录是否删除成功。

```
sftp-client> dir
```

```
-rwxrwxrwx  1 noone  nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx  1 noone  nogroup        225 Aug 24 08:01 pubkey2
-rwxrwxrwx  1 noone  nogroup        283 Aug 24 07:39 pubkey1
drwxrwxrwx  1 noone  nogroup         0 Sep 01 06:22 new
-rwxrwxrwx  1 noone  nogroup        225 Sep 01 06:55 pub
-rwxrwxrwx  1 noone  nogroup         0 Sep 01 08:00 z
```

```
sftp-client> delete z
```

The following files will be deleted:

/z

Are you sure to delete it? [Y/N]:y

This operation may take a long time.Please wait...

File successfully Removed

```
sftp-client> dir
```

```
-rwxrwxrwx  1 noone  nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx  1 noone  nogroup        225 Aug 24 08:01 pubkey2
-rwxrwxrwx  1 noone  nogroup        283 Aug 24 07:39 pubkey1
drwxrwxrwx  1 noone  nogroup         0 Sep 01 06:22 new
-rwxrwxrwx  1 noone  nogroup        225 Sep 01 06:55 pub
```

新增目录 new1，并检查新目录是否创建成功。

```
sftp-client> mkdir new1
```

Success

New directory created

```
sftp-client> dir
```

```
-rwxrwxrwx  1 noone  nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx  1 noone  nogroup        225 Aug 24 08:01 pubkey2
-rwxrwxrwx  1 noone  nogroup        283 Aug 24 07:39 pubkey1
drwxrwxrwx  1 noone  nogroup         0 Sep 01 06:22 new
-rwxrwxrwx  1 noone  nogroup        225 Sep 01 06:55 pub
drwxrwxrwx  1 noone  nogroup         0 Sep 02 06:30 new1
```

将目录名 new1 更名为 new2，并查看是否更名成功。

```
sftp-client> rename new1 new2
```

Success

File successfully renamed

```
sftp-client> dir
```

```
-rwxrwxrwx  1 noone  nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx  1 noone  nogroup        225 Aug 24 08:01 pubkey2
-rwxrwxrwx  1 noone  nogroup        283 Aug 24 07:39 pubkey1
drwxrwxrwx  1 noone  nogroup         0 Sep 01 06:22 new
-rwxrwxrwx  1 noone  nogroup        225 Sep 01 06:55 pub
drwxrwxrwx  1 noone  nogroup         0 Sep 02 06:33 new2
```

从服务器上下载文件 pubkey2 到本地，并更名为 public。

```
sftp-client> get pubkey2 public
```

```

Remote file:/pubkey2 ---> Local file: public
Downloading file successfully ended
# 将本地文件 pu 上传到服务器上，更名为 puk，并查看上传是否成功。
sftp-client> put pu puk
Local file:pu ---> Remote file: /puk
Uploading file successfully ended
sftp-client> dir
-rwxrwxrwx  1 noone  nogroup  1759 Aug 23 06:52 config.cfg
-rwxrwxrwx  1 noone  nogroup   225 Aug 24 08:01 pubkey2
-rwxrwxrwx  1 noone  nogroup   283 Aug 24 07:39 pubkey1
drwxrwxrwx  1 noone  nogroup    0 Sep 01 06:22 new
drwxrwxrwx  1 noone  nogroup    0 Sep 02 06:33 new2
-rwxrwxrwx  1 noone  nogroup   283 Sep 02 06:35 pub
-rwxrwxrwx  1 noone  nogroup   283 Sep 02 06:36 puk
sftp-client>
# 退出 SFTP。
sftp-client> quit
Bye
Connection closed.
<SwitchA>

```

1.5.5 完整配置

- 配置 SwitchB

```

#
vlan 1
#
public-key peer Switch001
public-key-code begin
330819F300D06092A864886F70D010101050003818D0030818902818100AA71FC45D099C0
456ACFD73E9D903A41721B440CF5D5E1DBAC642A7C8BD46C69AC84718CAE40D297E51FAC
FCF9BD75B09D76FD863E0539635EB803F2459A8BB2D32D2EA5A77C86753D4FBC20022CDB4
24B44900EE752C1E3BEA519DF0709CEDC1B3D3557662D1F703269C67B26E5B53B75EA586D
DE615429AC5EC292FFCA1290203010001
public-key-code end
peer-public-key end
#
interface Vlan-interface1
ip address 192.168.0.1 255.255.255.0
#
ssh server enable
sftp server enable
ssh user client001 service-type sftp authentication-type publickey assign
publi
ckey Switch001 work-directory cf:/
#
user-interface vty 0 4
authentication-mode scheme

```

```

protocol inbound ssh
#
• 配置 SwitchA
#
vlan 1
#
interface Vlan-interface1
ip address 192.168.0.2 255.255.255.0
#

```

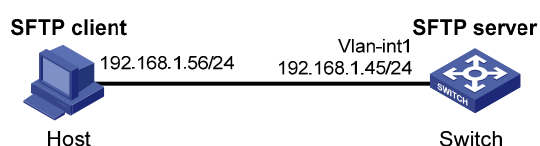
1.5.6 配置注意事项

- SSH 用户的服务类型设置为 **sftp** 或者 **all**。
- S7500E 系列以太网交换机、S3610 系列以太网交换机、S5510 系列以太网交换机和 S3500-EA 系列以太网交换机只支持 RSA 密钥对。

1.6 设备作为 SFTP 服务器典型配置指导

1.6.1 组网图

图1-13 设备作为 SFTP 服务器组网图



1.6.2 应用要求

如图 1-13，Host 和 Switch 之间建立 SSH 连接，Host 作为 SFTP 客户端登录到 Switch，进行文件管理和文件传送等操作，用户名为 client002，密码为 aabbcc。

1.6.3 适用产品、版本

表1-6 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5500-SI 系列以太网交换机	Release 1207 软件版本	全系列硬件版本 (除 S5500-20TP-SI)
	Release 1301 软件版本	S5500-20TP-SI
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6100, Release 6300 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.6.4 配置过程和解释

(1) 配置 SFTP 服务器 Switch

生成 RSA 及 DSA 密钥对，并启动 SSH 服务器。

```
<Switch> system-view
[Switch] public-key local create rsa
[Switch] public-key local create dsa
[Switch] ssh server enable
```



注意

- 生成服务器端的 RSA 和 DSA 密钥对是完成 SFTP 登录的必要操作。
 - 因为 S7500E 系列以太网交换机、S3610 系列以太网交换机、S5510 系列以太网交换机和 S3500-EA 系列以太网交换机只支持 RSA 密钥对，所以当 S7500E、S3500-EA、S3610 或 5510 作为 SFTP 服务器时只用生成 RSA 密钥对。
-

启动 SFTP 服务器。

```
[Switch] sftp server enable
```

配置 VLAN 接口 1 的 IP 地址，客户端将通过该地址连接 SSH 服务器。

```
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ip address 192.168.1.45 255.255.255.0
[Switch-Vlan-interface1] quit
```

设置 SSH 客户端登录用户界面的认证方式为 AAA 认证。

```
[Switch] user-interface vty 0 4
[Switch-ui-vty0-4] authentication-mode scheme
```

设置 Switch 上远程用户登录协议为 SSH。

```
[Switch-ui-vty0-4] protocol inbound ssh
[Switch-ui-vty0-4] quit
```

创建本地用户 client002。

```
[Switch] local-user client002
[Switch-luser-client002] password simple aabbcc
[Switch-luser-client002] service-type ssh
[Switch-luser-client002] quit
```

配置 SSH 用户认证方式为 password，服务类型为 SFTP。

```
[Switch] ssh user client002 service-type sftp authentication-type password
```

(2) 配置 SFTP 客户端 Host



说明

- SFTP 客户端软件有很多，本文中仅以客户端软件 PuTTY0.58 中的 PSFTP 为例，说明 SFTP 客户端的配置方法。
 - PSFTP 只支持 password 认证，不支持 publickey 认证
-

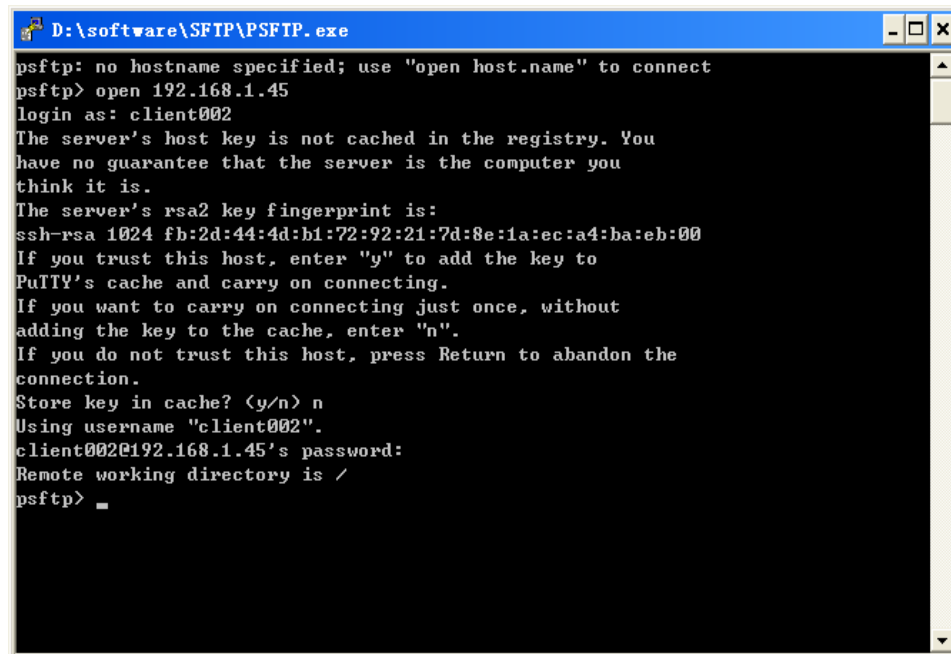
建立与 SFTP 服务器的连接。

打开psftp.exe程序，出现如图 1-14所示的客户端配置界面。输入如下命令：

```
open 192.168.1.45
```

根据提示输入用户名 client002，密码 aabbcc，即可登录 SFTP 服务器。

图1-14 SFTP 客户端登录界面



1.6.5 完整配置

- 配置 Switch

```
#
vlan 1
#
local-user client002
password simple aabbcc
service-type ssh
#
interface Vlan-interface1
ip address 192.168.1.45 255.255.255.0
#
ssh server enable
sftp server enable
ssh user client002 service-type sftp authentication-type password
#
user-interface vty 0 4
authentication-mode scheme
protocol inbound ssh
#
return
```

1.6.6 配置注意事项

- 设备作为 **SFTP** 服务器时,同时只能有一个用户访问 **SFTP** 服务器。如果以 WinSCP 作为 **SFTP** 客户端,则无法直接编辑服务器上的文件,需要采用将服务器上的文件下载到本地,在本地修改后上传到服务器的方式实现对文件的编辑。
- **SSH** 用户的服务类型设置为 **sftp** 或者 **all**。
- **S7500E** 系列以太网交换机、**S3610** 系列以太网交换机、**S5510** 系列以太网交换机和 **S3500-EA** 系列以太网交换机只支持 **RSA** 密钥对。

目 录

1 端口安全典型配置指导.....	1-1
1.1 端口安全autolearn模式典型配置指导.....	1-1
1.1.1 组网图.....	1-1
1.1.2 应用要求.....	1-1
1.1.3 适用产品、版本.....	1-1
1.1.4 配置过程和解释.....	1-1
1.1.5 完整配置.....	1-3
1.1.6 配置注意事项.....	1-3
1.2 端口安全userLoginWithOUI模式典型配置指导.....	1-3
1.2.1 组网图.....	1-4
1.2.2 组网需求.....	1-4
1.2.3 适用产品、版本.....	1-4
1.2.4 配置过程和解释.....	1-4
1.2.5 完整配置.....	1-8
1.2.6 配置注意事项.....	1-8
1.3 端口安全macAddressWithRadius模式典型配置指导.....	1-8
1.3.1 组网图.....	1-9
1.3.2 组网需求.....	1-9
1.3.3 适用产品、版本.....	1-9
1.3.4 配置过程和解释.....	1-9
1.3.5 完整配置.....	1-11
1.3.6 配置注意事项.....	1-12
1.4 端口安全macAddressElseUserLoginSecure模式典型配置指导.....	1-12
1.4.1 组网图.....	1-12
1.4.2 组网需求.....	1-13
1.4.3 适用产品、版本.....	1-13
1.4.4 配置过程和解释.....	1-13
1.4.5 完整配置.....	1-16
1.4.6 配置注意事项.....	1-17

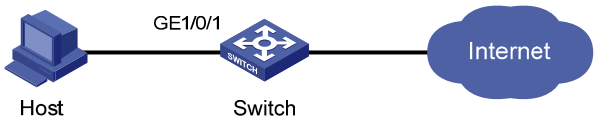
1 端口安全典型配置指导

1.1 端口安全 autolearn 模式典型配置指导

在端口安全 autolearn 模式下，端口学习到的 MAC 地址被保存在安全 MAC 地址表项中。当端口下的安全 MAC 地址数超过端口允许学习的最大安全 MAC 地址数后，端口模式会自动转变为 secure 模式。之后，该端口不会再添加新的安全 MAC，只有源 MAC 地址为安全 MAC 地址、已配置的静态 MAC 地址的报文，才能通过该端口。

1.1.1 组网图

图1-1 端口安全 autolearn 模式配置组网图



1.1.2 应用要求

在交换机的端口 GigabitEthernet1/0/1 上对接入用户做如下的限制：

- 允许 64 个用户自由接入，不进行认证，将学习到的用户 MAC 地址添加为安全 MAC 地址；
- 当安全 MAC 地址数量达到 64 后，停止学习；当再有新的 MAC 地址接入时，触发入侵检测，并将此端口关闭 30 秒；

1.1.3 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S5500-SI 系列以太网交换机	Release 1207 软件版本	全系列硬件版本 (除 S5500-20TP-SI)
	Release 1301 软件版本	S5500-20TP-SI
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6300 软件版本	全系列硬件版本

1.1.4 配置过程和解释

使能端口安全功能。

```
<Switch> system-view
[Switch] port-security enable
```

打开入侵检测 Trap 开关。

```
[Switch] port-security trap intrusion
```

设置端口允许的最大安全 MAC 地址数为 64。

```
[Switch] interface GigabitEthernet 1/0/1
```

```
[Switch-GigabitEthernet1/0/1] port-security max-mac-count 64
```

设置端口安全模式为 autoLearn。

```
[Switch-GigabitEthernet1/0/1] port-security port-mode autolearn
```

设置触发入侵检测特性后的保护动作为暂时关闭端口，关闭时间为 30 秒。

```
[Switch-GigabitEthernet1/0/1] port-security intrusion-mode disableport-temporarily
```

```
[Switch-GigabitEthernet1/0/1] quit
```

```
[Switch] port-security timer disableport 30
```

(1) 验证配置结果

上述配置完成后，可以用 **display** 命令显示端口安全配置情况，如下：

```
<Switch> display port-security interface gigabitethernet 1/0/1
```

```
Equipment port-security is enabled
```

```
Intrusion trap is enabled
```

```
Disableport Timeout: 30s
```

```
OUI value:
```

```
GigabitEthernet1/0/1 is link-up
```

```
Port mode is autoLearn
```

```
NeedToKnow mode is disabled
```

```
Intrusion Protection mode is DisablePortTemporarily
```

```
Max MAC address number is 64
```

```
Stored MAC address number is 0
```

```
Authorization is permitted
```

可以看到端口的最大安全 MAC 数为 64，端口模式为 autoLearn，入侵检测 Trap 开关打开，入侵保护动作为 DisablePortTemporarily，入侵发生后端口禁用时间为 30 秒。

配置完成后，允许地址学习，学习到的 MAC 地址数可以用上述命令显示，如学习到 5 个，那么存储的安全 MAC 地址数就为 5，可以在端口视图下用 **display this** 命令查看学习到的 MAC 地址，如：

```
<Switch> system-view
```

```
[Switch] interface gigabitethernet 1/0/1
```

```
[Switch-GigabitEthernet1/0/1] display this
```

```
#
```

```
interface GigabitEthernet1/0/1
```

```
port-security max-mac-count 64
```

```
port-security port-mode autolearn
```

```
port-security mac-address security 0002-0000-0015 vlan 1
```

```
port-security mac-address security 0002-0000-0014 vlan 1
```

```
port-security mac-address security 0002-0000-0013 vlan 1
```

```
port-security mac-address security 0002-0000-0012 vlan 1
```

```
port-security mac-address security 0002-0000-0011 vlan 1
```

```
#
```

当学习到的 MAC 地址数达到 64 后，用命令 **display port-security interface** 可以看到端口模式变为 secure，再有新的 MAC 地址到达将触发入侵保护，Trap 信息如下：

```
#May 2 03:15:55:871 2000 Switch PORTSEC/1/VIOLATION:Traph3cSecureViolation
```

```
A intrusion occurs!
```

```
IfIndex: 9437207
```

```
Port: 9437207
```

```
MAC Addr: 0.2.0.0.0.21
VLAN ID: 1
IfAdminStatus: 1
```

并且可以通过下述命令看到端口安全将此端口关闭：

```
<Switch-GigabitEthernet1/0/1> display interface gigabitethernet 1/0/1
GigabitEthernet1/0/1 current state: Port Security Disabled
IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 000f-cb00-5558
Description: GigabitEthernet1/0/1 Interface
.....
```

30 秒后，端口状态恢复：

```
[Switch-GigabitEthernet1/0/1] display interface gigabitethernet 1/0/1
GigabitEthernet1/0/1 current state: UP
IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 000f-cb00-5558
Description: GigabitEthernet1/0/1 Interface
.....
```

此时，如手动删除几条安全 MAC 地址后，端口安全的状态重新恢复为 autoLearn，可以继续学习 MAC 地址。

1.1.5 完整配置

```
#
port-security enable
port-security trap intrusion
port-security timer disableport 30
#
interface GigabitEthernet1/0/1
port-security max-mac-count 64
port-security port-mode autolearn
port-security intrusion-mode disableport-temporarily
#
```

1.1.6 配置注意事项

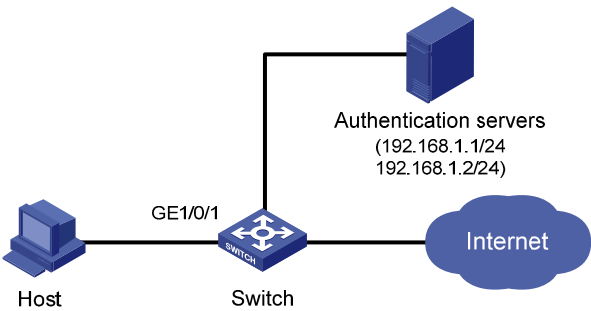
- 在使能端口安全功能之前，需要关闭全局的 802.1x 和 MAC 地址认证功能。
- 端口安全模式的配置与端口加入聚合组互斥。
- 当多个用户通过认证时，端口下所允许的最大用户数根据不同的端口安全模式，取最大安全 MAC 地址数与相应模式下允许认证用户数的最小值。
- 端口上有用户在线的情况下，端口安全功能无法关闭。

1.2 端口安全 userLoginWithOUI 模式典型配置指导

在端口安全 userLoginWithOUI 模式下，端口必须通过 802.1x 认证才能开启，且只允许认证成功用户报文通过。除此之外，端口还允许一个指定 OUI 的源 MAC 地址的报文认证通过。

1.2.1 组网图

图1-2 端口安全 userLoginWithOUI 模式组网图



1.2.2 组网需求

客户端通过端口 GigabitEthernet1/0/1 连接到交换机上，交换机通过 RADIUS 服务器对客户端进行身份认证，如果认证成功，客户端被授权允许访问 Internet 资源。

交换机的管理者希望对接入用户的端口 GigabitEthernet1/0/1 做如下限制：

- 允许一个 802.1x 用户上线；
- 最多可以配置 16 个 OUI 值，还允许端口上有一个与 OUI 值匹配的 MAC 地址用户通过。

1.2.3 适用产品、版本

表1-2 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S5500-SI 系列以太网交换机	Release 1207 软件版本	全系列硬件版本 (除 S5500-20TP-SI)
	Release 1301 软件版本	S5500-20TP-SI
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6300 软件版本	全系列硬件版本

1.2.4 配置过程和解释



说明

- 下述配置步骤包含了部分 AAA/RADIUS 协议配置命令，具体介绍请参见“AAA-RADIUS-HWTACACS 配置”。
- 接入用户和 RADIUS 服务器上的配置略。

(1) 具体的配置步骤

- 配置 RADIUS 协议

创建名为 radsun 的 RADIUS 方案。

```
<Switch> system-view
[Switch] radius scheme radsun
```


设置主认证 RADIUS 服务器的 IP 地址为 192.168.1.1，主计费 RADIUS 服务器的 IP 地址为 192.168.1.2。

```
[Switch-radius-radsun] primary authentication 192.168.1.1
```

```
[Switch-radius-radsun] primary accounting 192.168.1.2
```

设置从认证 RADIUS 服务器的 IP 地址为 192.168.1.2，从计费 RADIUS 服务器的 IP 地址为 192.168.1.1。

```
[Switch-radius-radsun] secondary authentication 192.168.1.2
```

```
[Switch-radius-radsun] secondary accounting 192.168.1.1
```

设置与认证 RADIUS 服务器交互报文时的加密密码为 name。

```
[Switch-radius-radsun] key authentication name
```

设置与计费 RADIUS 服务器交互报文时的加密密码为 money。

```
[Switch-radius-radsun] key accounting money
```

设置 RADIUS 服务器应答超时时间为 5 秒，RADIUS 报文的超时重传次数的最大值为 5。

```
[Switch-radius-radsun] timer response-timeout 5
```

```
[Switch-radius-radsun] retry 5
```

设置向 RADIUS 服务器发送实时计费报文的时间间隔为 15 分钟。

```
[Switch-radius-radsun] timer realtime-accounting 15
```

设置将去除域名的用户名发送给 RADIUS 服务器。

```
[Switch-radius-radsun] user-name-format without-domain
```

```
[Switch-radius-radsun] quit
```

创建名为 sun 的 ISP 域，并进入其视图。

```
[Switch] domain sun
```

指定名为 radsun 的 RADIUS 方案为该域用户的缺省 RADIUS 方案。

```
[Switch-isp-sun] authentication default radius-scheme radsun
```

设置该 ISP 域最多可容纳 30 个用户。

```
[Switch-isp-sun] access-limit enable 30
```

```
[Switch-isp-sun] quit
```

- 配置端口安全特性

使能端口安全功能。

```
[Switch] port-security enable
```

添加 5 个 OUI 值。

```
[Switch] port-security oui 1234-0100-1111 index 1
```

```
[Switch] port-security oui 1234-0200-1111 index 2
```

```
[Switch] port-security oui 1234-0300-1111 index 3
```

```
[Switch] port-security oui 1234-0400-1111 index 4
```

```
[Switch] port-security oui 1234-0500-1111 index 5
```

```
[Switch] interface GigabitEthernet 1/0/1
```

设置端口安全模式为 userLoginWithOUI。

```
[Switch-GigabitEthernet1/0/1] port-security port-mode userlogin-withoui
```

(2) 验证配置结果

查看名为 radsun 的 RADIUS 方案的配置信息:

```
<Switch> display radius scheme radsun
SchemeName = radsun
Index = 0 Type = standard
Primary Auth IP = 192.168.1.1 Port = 1812 State = active
Primary Acct IP = 192.168.1.2 Port = 1813 State = active
Second Auth IP = 192.168.1.2 Port = 1812 State = active
Second Acct IP = 192.168.1.1 Port = 1813 State = active
Auth Server Encryption Key = name
Acct Server Encryption Key = money
Accounting-On packet disable, send times = 5 , interval = 3s
Interval for timeout(second) = 5
Retransmission times for timeout = 5
Interval for realtime accounting(minute) = 15
Retransmission times of realtime-accounting packet = 5
Retransmission times of stop-accounting packet = 500
Quiet-interval(min) = 5
Username format = without-domain
Data flow unit = Byte
Packet unit = one
```

查看名为 sun 的 ISP 域的配置信息:

```
<Switch> display domain sun
Domain = sun
State = Active
Access-limit = 30
Accounting method = Required
Default authentication scheme : radius=radsun
Default authorization scheme : local
Default accounting scheme : local
Domain User Template:
Idle-cut = Disable
Self-service = Disable
```

查看端口安全的配置信息:

```
<Switch> display port-security interface gigabitethernet 1/0/1
Equipment port-security is enabled
Trap is disabled
Disableport Timeout: 20s
OUI value:
Index is 1, OUI value is 123401
Index is 2, OUI value is 123402
Index is 3, OUI value is 123403
Index is 4, OUI value is 123404
Index is 5, OUI value is 123405

GigabitEthernet1/0/1 is link-up
Port mode is userLoginWithOUI
NeedToKnow mode is disabled
```

```
Intrusion Protection mode is NoAction
Max MAC address number is not configured
Stored MAC address number is 0
Authorization is permitted
```

配置完成后，如果有 802.1x 用户上线，则可以看到存储的安全 MAC 地址数为 1。还可以通过下述命令查看 802.1x 用户的情况：

```
<Switch> display dot1x interface gigabitethernet 1/0/1
Equipment 802.1X protocol is enabled
CHAP authentication is enabled

Configuration: Transmit Period    30 s, Handshake Period    15 s
                  Quiet Period    60 s, Quiet Period Timer is disabled
                  Supp Timeout    30 s, Server Timeout    100 s
                  The maximal retransmitting times    2

Total maximum 802.1X user resource number is 1024 per slot
Total current used 802.1X resource number is 1
```

```
GigabitEthernet1/0/1 is link-up
802.1X protocol is enabled
Handshake is enabled
The port is an authenticator
Authentication Mode is Auto
Port Control Type is Mac-based
Guest VLAN: 0
Max number of on-line users is 256

EAPOL Packet: Tx 16331, Rx 102
Sent EAP Request/Identity Packets : 16316
EAP Request/Challenge Packets: 6
EAP Success Packets: 4, Fail Packets: 5
Received EAPOL Start Packets : 6
EAPOL LogOff Packets: 2
EAP Response/Identity Packets : 80
EAP Response/Challenge Packets: 6
Error Packets: 0
1. Authenticated user : MAC address: 0002-0000-0011
```

```
Controlled User(s) amount to 1
```

此外，端口还允许一个与 OUI 值匹配的 MAC 地址的用户通过，可以通过下述命令查看：

```
<Switch> display mac-address interface gigabitethernet 1/0/1
MAC ADDR          VLAN ID   STATE          PORT INDEX          AGING TIME(s)
1234-0300-0011    1         Learned        GigabitEthernet1/0/1  AGING

--- 1 mac address(es) found ---
```

1.2.5 完整配置

```
#
port-security enable
port-security oui 1234-0100-0000 index 1
port-security oui 1234-0200-0000 index 2
port-security oui 1234-0300-0000 index 3
port-security oui 1234-0400-0000 index 4
port-security oui 1234-0500-0000 index 5
#
radius scheme radsun
primary authentication 192.168.1.1
primary accounting 192.168.1.2
secondary authentication 192.168.1.2
secondary accounting 192.168.1.1
key authentication name
key accounting money
timer realtime-accounting 15
timer response-timeout 5
user-name-format without-domain
retry 5
#
domain sun
authentication default radius-scheme radsun
access-limit enable 30
#
interface GigabitEthernet1/0/1
port-security port-mode userlogin-withoutui
#
```

1.2.6 配置注意事项

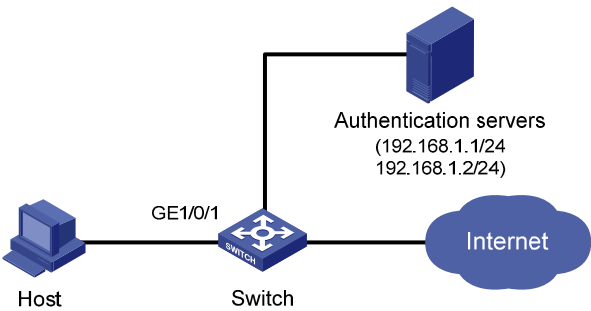
- 在使能端口安全功能之前，需要关闭全局的 802.1x 和 MAC 地址认证功能。
- 端口安全模式的配置与端口加入聚合组互斥。
- 当多个用户通过认证时，端口下所允许的最大用户数根据不同的端口安全模式，取最大安全 MAC 地址数与相应模式下允许认证用户数的最小值。
- 允许通过认证的用户 OUI 值可以配置多条。
- 端口上有用户在线的情况下，端口安全功能无法关闭。

1.3 端口安全 macAddressWithRadius 模式典型配置指导

在 macAddressWithRadius 安全模式下，交换机将在启动端口安全的端口上对接入用户采用 MAC 地址认证。

1.3.1 组网图

图1-3 端口安全 macAddressWithRadius 模式组网图



1.3.2 组网需求

客户端通过端口 GigabitEthernet1/0/1 连接到交换机上，交换机通过 RADIUS 服务器对客户端进行身份认证。如果认证成功，客户端被授权允许访问 Internet 资源。

交换机的管理者希望对接入用户的端口 GigabitEthernet1/0/1 做如下限制：

- 对接入用户进行 MAC 地址认证；
- 所有接入用户都属于一个缺省的域 sun，MAC 地址认证时使用用户 host 的 MAC 地址作为用户名和密码。
- 对未通过 MAC 认证的报文，触发入侵检测特性，丢弃源地址是此 MAC 地址的报文，保证该端口的安全性。

1.3.3 适用产品、版本

表1-3 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S5500-SI 系列以太网交换机	Release 1207 软件版本	全系列硬件版本 (除 S5500-20TP-SI)
	Release 1301 软件版本	S5500-20TP-SI
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6300 软件版本	全系列硬件版本

1.3.4 配置过程和解释



说明

- 下述配置步骤包含了部分 AAA/RADIUS 协议配置命令，具体介绍请参见“AAA-RADIUS-HWTACACS 配置”。
- 接入用户和 RADIUS 服务器上的配置略。

(1) 具体的配置步骤

- 配置 RADIUS 协议

创建名为 radsun 的 RADIUS 方案。

```
<Switch> system-view
```

```
[Switch] radius scheme radsun
```

设置主认证 RADIUS 服务器的 IP 地址为 192.168.1.1，主计费 RADIUS 服务器的 IP 地址为 192.168.1.2。

```
[Switch-radius-radsun] primary authentication 192.168.1.1
```

```
[Switch-radius-radsun] primary accounting 192.168.1.2
```

设置从认证 RADIUS 服务器的 IP 地址为 192.168.1.2，从计费 RADIUS 服务器的 IP 地址为 192.168.1.1。

```
[Switch-radius-radsun] secondary authentication 192.168.1.2
```

```
[Switch-radius-radsun] secondary accounting 192.168.1.1
```

设置与认证 RADIUS 服务器交互报文时的加密密码为 name。

```
[Switch-radius-radsun] key authentication name
```

设置与计费 RADIUS 服务器交互报文时的加密密码为 money。

```
[Switch-radius-radsun] key accounting money
```

设置 RADIUS 服务器应答超时时间为 5 秒，RADIUS 报文的超时重传次数的最大值为 5。

```
[Switch-radius-radsun] timer response-timeout 5
```

```
[Switch-radius-radsun] retry 5
```

设置向 RADIUS 服务器发送实时计费报文的时间间隔为 15 分钟。

```
[Switch-radius-radsun] timer realtime-accounting 15
```

设置将去除域名的用户名发送给 RADIUS 服务器。

```
[Switch-radius-radsun] user-name-format without-domain
```

```
[Switch-radius-radsun] quit
```

创建名为 sun 的 ISP 域，并进入其视图。

```
[Switch] domain sun
```

指定名为 radsun 的 RADIUS 方案为该域用户的缺省 RADIUS 方案。

```
[Switch-isp-sun] authentication default radius-scheme radsun
```

```
[Switch-isp-sun] quit
```

- 配置端口安全特性

使能端口安全功能。

```
[Switch] port-security enable
```

配置 MAC 地址认证用户所使用的 ISP 域。

```
[Switch] mac-authentication domain sun
```

设置端口允许的最大安全 MAC 地址数为 64。

```
[Switch-GigabitEthernet1/0/1] port-security max-mac-count 64
```

设置端口安全模式为 macAddressWithRadius。

```
[Switch-GigabitEthernet1/0/1] port-security port-mode mac-authentication
```

配置入侵检测特性为 blockmac。

```
[Switch-GigabitEthernet1/0/1] port-security intrusion-mode blockmac
```

(2) 验证配置结果

查看端口安全的配置信息：

```
<Switch> display port-security interface gigabitethernet 1/0/1
Equipment port-security is enabled
Trap is disabled
Disableport Timeout: 20s
OUI value:
```

```
GigabitEthernet1/0/1 is link-up
Port mode is macAddressWithRadius
NeedToKnow mode is disabled
Intrusion Protection mode is BlockMacAddress
Max MAC address number is 64
Stored MAC address number is 1
Authorization is permitted
```

查看 MAC 地址认证情况：

```
<Switch> display mac-authentication interface gigabitethernet 1/0/1
MAC address authentication is enabled.
User name format is MAC address, like xxxxxxxxxxxx
Fixed username:mac
Fixed password:not configured
Offline detect period is 300s
Quiet period is 60s
Server response timeout value is 100s
The max allowed user number is 1024 per slot
Current user number amounts to 1
Current domain is sun
```

Silent MAC User info:

MAC Addr	From Port	Port Index

```
GigabitEthernet1/0/1 is link-up
MAC address authentication is enabled
Authenticate success: 1, failed: 0
Current online user number is 1
```

MAC Addr	Authenticate State	Auth Index
000f-3d80-2b38	MAC_AUTHENTICATOR_SUCCESS	11

此外，因为配置了入侵检测特性为 **blockmac**，对未通过 MAC 认证的报文，触发入侵检测特性，丢弃源地址是此 MAC 地址的报文，保证该端口的安全性。

1.3.5 完整配置

```
#
port-security enable
#
mac-authentication domain sun
#
radius scheme radsun
primary authentication 192.168.1.1
```

```

primary accounting 192.168.1.2
secondary authentication 192.168.1.2
secondary accounting 192.168.1.1
key authentication name
key accounting money
timer realtime-accounting 15
timer response-timeout 5
user-name-format without-domain
retry 5
#
domain sun
authentication default radius-scheme radsun
#
interface GigabitEthernet1/0/1
port-security max-mac-count 64
port-security port-mode mac-authentication
port-security intrusion-mode blockmac
#
return

```

1.3.6 配置注意事项

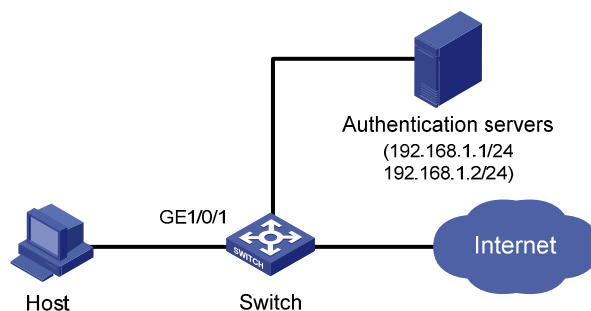
- 在使能端口安全功能之前，需要关闭全局的 802.1x 和 MAC 地址认证功能。
- 端口安全模式的配置与端口加入聚合组互斥。
- 当多个用户通过认证时，端口下所允许的最大用户数根据不同的端口安全模式，取最大安全 MAC 地址数与相应模式下允许认证用户数的最小值。
- 端口上有用户在线的情况下，端口安全功能无法关闭。

1.4 端口安全 macAddressElseUserLoginSecure 模式典型配置指导

在端口安全 macAddressElseUserLoginSecure 模式下，端口同时处于 macAddressWithRadius 模式和 userLoginSecure 模式，但 MAC 地址认证优先级大于 802.1x 认证。对于非 802.1x 报文直接进行 MAC 地址认证，对于 802.1x 报文先进行 MAC 地址认证，如果 MAC 地址认证失败再进行 802.1x 认证。

1.4.1 组网图

图1-4 端口安全 macAddressElseUserLoginSecure 模式组网图



1.4.2 组网需求

客户端通过端口 GigabitEthernet1/0/1 连接到交换机上，交换机通过 RADIUS 服务器对客户端进行身份认证。如果认证成功，客户端被授权允许访问 Internet 资源。

交换机的管理者希望对接入用户的端口 GigabitEthernet1/0/1 做如下的限制：

- 可以有多个 MAC 认证用户上线；
- 如果是 802.1x 用户请求认证，先进行 MAC 地址认证，MAC 地址认证失败，再进行 802.1x 认证。802.1x 用户限制为 1 个；
- MAC 地址认证设置用户名格式为自定义用户名和密码的形式，上线的 MAC 地址认证用户和 802.1x 认证用户总和不能超过 64 个；
- 为防止报文发往未知目的 MAC 地址，启动 NeedToKnow 特性。

1.4.3 适用产品、版本

表1-4 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S5500-SI 系列以太网交换机	Release 1207 软件版本	全系列硬件版本 (除 S5500-20TP-SI)
	Release 1301 软件版本	S5500-20TP-SI
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6300 软件版本	全系列硬件版本

1.4.4 配置过程和解释



说明

- 下述配置步骤包含了部分 AAA/RADIUS 协议配置命令，具体介绍请参见“AAA-RADIUS-HWTACACS 配置”。
- 接入用户和 RADIUS 服务器上的配置略。

(1) 具体的配置步骤

- 配置 RADIUS 协议

创建名为 radsun 的 RADIUS 方案。

```
<Switch> system-view
```

```
[Switch] radius scheme radsun
```

设置主认证 RADIUS 服务器的 IP 地址为 192.168.1.1，主计费 RADIUS 服务器的 IP 地址为 192.168.1.2。

```
[Switch-radius-radsun] primary authentication 192.168.1.1
```

```
[Switch-radius-radsun] primary accounting 192.168.1.2
```

设置从认证 RADIUS 服务器的 IP 地址为 192.168.1.2，从计费 RADIUS 服务器的 IP 地址为 192.168.1.1。

```
[Switch-radius-radsun] secondary authentication 192.168.1.2
```

```
[Switch-radius-radsun] secondary accounting 192.168.1.1
```

设置与认证 RADIUS 服务器交互报文时的加密密码为 name。

```
[Switch-radius-radsun] key authentication name
```

设置与计费 RADIUS 服务器交互报文时的加密密码为 money。

```
[Switch-radius-radsun] key accounting money
```

设置 RADIUS 服务器应答超时时间为 5 秒，RADIUS 报文的超时重传次数的最大值为 5。

```
[Switch-radius-radsun] timer response-timeout 5
```

```
[Switch-radius-radsun] retry 5
```

设置向 RADIUS 服务器发送实时计费报文的时间间隔为 15 分钟。

```
[Switch-radius-radsun] timer realtime-accounting 15
```

设置将去除域名的用户名发送给 RADIUS 服务器。

```
[Switch-radius-radsun] user-name-format without-domain
```

```
[Switch-radius-radsun] quit
```

创建名为 sun 的 ISP 域，并进入其视图。

```
[Switch] domain sun
```

指定名为 radsun 的 RADIUS 方案为该域用户的缺省 RADIUS 方案。

```
[Switch-isp-sun] authentication default radius-scheme radsun
```

```
[Switch-isp-sun] quit
```

- 配置端口安全特性

使能端口安全功能。

```
[Switch] port-security enable
```

配置 MAC 地址认证用户所使用的 ISP 域。

```
[Switch] mac-authentication domain sun
```

配置 MAC 认证的用户名为 aaa，密码为 123456。

```
[Switch] mac-authentication user-name-format fixed account aaa password simple 123456
```

```
[Switch] interface gigabitethernet 1/0/1
```

设置端口允许的最大安全 MAC 地址数为 64。

```
[Switch-GigabitEthernet1/0/1] port-security max-mac-count 64
```

设置端口安全模式为 macAddressElseUserLoginSecure。

```
[Switch-GigabitEthernet1/0/1] port-security port-mode mac-else-userlogin-secure
```

设置端口 NeedToKnow 模式为 ntkonly。

```
[Switch-GigabitEthernet1/0/1] port-security ntk-mode ntkonly
```

(2) 验证配置结果

查看端口安全的配置信息：

```
<Switch> display port-security interface gigabitethernet 1/0/1
```

```
Equipment port-security is enabled
```

```
Trap is disabled
```

```
Disableport Timeout: 20s
```

```
OUI value:
```

```
GigabitEthernet1/0/1 is link-up
Port mode is macAddressElseUserLoginSecure
NeedToKnow mode is NeedToKnowOnly
Intrusion Protection mode is NoAction
Max MAC address number is 64
Stored MAC address number is 0
Authorization is permitted
```

查看 MAC 地址认证情况:

```
<Switch> display mac-authentication interface gigabitethernet 1/0/1
MAC address authentication is enabled.
User name format is fixed account
Fixed username:aaa
Fixed password:123456
Offline detect period is 300s
Quiet period is 60s
Server response timeout value is 100s
The max allowed user number is 1024 per slot
Current user number amounts to 3
Current domain is sun
```

Silent MAC User info:

MAC Addr	From Port	Port Index

```
GigabitEthernet1/0/1 is link-up
MAC address authentication is enabled
Authenticate success: 3, failed: 1
Current online user number is 3
```

MAC Addr	Authenticate State	Auth Index
1234-0300-0011	MAC_AUTHENTICATOR_SUCCESS	13
1234-0300-0012	MAC_AUTHENTICATOR_SUCCESS	14
1234-0300-0013	MAC_AUTHENTICATOR_SUCCESS	15

查看 802.1x 认证情况:

```
<Switch> display dot1x interface gigabitethernet 1/0/1
Equipment 802.1X protocol is enabled
CHAP authentication is enabled
Configuration: Transmit Period 30 s, Handshake Period 15 s
Quiet Period 60 s, Quiet Period Timer is disabled
Supp Timeout 30 s, Server Timeout 100 s
The maximal retransmitting times 2
EAD quick deploy configuration:
EAD timeout: 30 m
The maximum 802.1X user resource number is 1024 per slot
Total current used 802.1X resource number is 1
GigabitEthernet1/0/1 is link-up
802.1X protocol is enabled
Handshake is enabled
```

```

The port is an authenticator
Authentication Mode is Auto
Port Control Type is Mac-based
802.1X Multicast-trigger is enabled
Guest VLAN: 0
Max number of on-line users is 256
EAPOL Packet: Tx 16331, Rx 102
Sent EAP Request/Identity Packets : 16316
EAP Request/Challenge Packets: 6
EAP Success Packets: 4, Fail Packets: 5
Received EAPOL Start Packets : 6
EAPOL LogOff Packets: 2
EAP Response/Identity Packets : 80
EAP Response/Challenge Packets: 6
Error Packets: 0
1. Authenticated user : MAC address: 0002-0000-0011
Controlled User(s) amount to 1

```

此外，因为设置了 NeedToKnow 特性，目的 MAC 地址未知、广播和多播报文都被丢弃。

1.4.5 完整配置

```

#
port-security enable
#
mac-authentication domain sun
mac-authentication user-name-format fixed account aaa password simple 123456
#
radius scheme radsun
primary authentication 192.168.1.1
primary accounting 192.168.1.2
secondary authentication 192.168.1.2
secondary accounting 192.168.1.1
key authentication name
key accounting money
timer realtime-accounting 15
timer response-timeout 5
user-name-format without-domain
retry 5
#
domain sun
authentication default radius-scheme radsun
#
interface GigabitEthernet1/0/1
port-security max-mac-count 64
port-security port-mode mac-else-userlogin-secure
port-security ntk-mode ntkonly
#

```

1.4.6 配置注意事项

- 在使能端口安全功能之前，需要关闭全局的 802.1x 和 MAC 地址认证功能。
- 端口安全模式的配置与端口加入聚合组互斥。
- 当多个用户通过认证时，端口下所允许的最大用户数根据不同的端口安全模式，取最大安全 MAC 地址数与相应模式下允许认证用户数的最小值。
- `macAddressElseUserLoginSecure` 或 `macAddressElseUserLoginSecureExt` 安全模式下工作的端口，对于同一个报文，只有 MAC 地址认证和 802.1x 认证均失败后，才会触发入侵检测特性。

目 录

- 1 端口隔离典型配置指导..... 1-1
 - 1.1 端口隔离概述..... 1-1
 - 1.2 端口隔离配置指导 1-1
 - 1.2.1 组网图..... 1-1
 - 1.2.2 适用产品、版本 1-1
 - 1.2.3 配置过程和解释 1-2
 - 1.2.4 完整配置 1-2
 - 1.2.5 配置注意事项 1-2

1 端口隔离典型配置指导

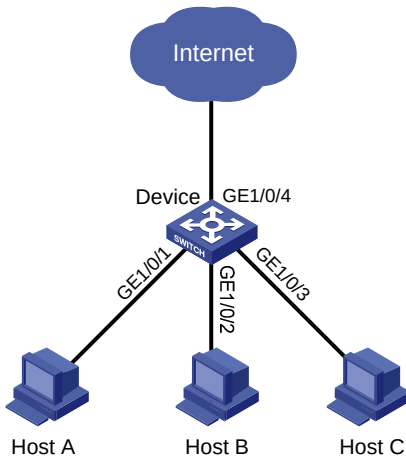
1.1 端口隔离概述

为了实现报文之间的隔离，可以将不同的端口加入不同的 VLAN，但会浪费有限的 VLAN 资源。采用端口隔离特性，可以实现同一 VLAN 内端口之间的隔离。用户只需要将端口加入到隔离组中，就可以实现隔离组内端口之间数据的隔离。端口隔离功能为用户提供了更安全、更灵活的组网方案。

1.2 端口隔离配置指导

1.2.1 组网图

图1-1 端口隔离典型配置组网图



- 应用要求小区用户 Host A、Host B、Host C 分别与 Device 的端口 GigabitEthernet1/0/1、GigabitEthernet1/0/2、GigabitEthernet1/0/3 相连；
- 设备通过 GigabitEthernet1/0/4 端口与外部网络相连；
- 端口 GigabitEthernet1/0/1、GigabitEthernet1/0/2、GigabitEthernet1/0/3 和 GigabitEthernet1/0/4 属于同一 VLAN；请实现小区用户 Host A、Host B 和 Host C 彼此之间不能互通，但可以和外部网络通信。

1.2.2 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5500-SI 系列以太网交换机	Release 1207 软件版本	全系列硬件版本 (除 S5500-20TP-SI)
	Release 1301 软件版本	S5500-20TP-SI

产品	软件版本	硬件版本
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6100, Release 6300 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.2.3 配置过程和解释

将端口 GigabitEthernet1/0/1、GigabitEthernet1/0/2、GigabitEthernet1/0/3 加入隔离组。

```
<Device> system-view
[Device] interface GigabitEthernet1/0/1
[Device-GigabitEthernet1/0/1] port-isolate enable
[Device-GigabitEthernet1/0/1] quit
[Device] interface GigabitEthernet1/0/2
[Device-GigabitEthernet1/0/2] port-isolate enable
[Device-GigabitEthernet1/0/2] quit
[Device] interface GigabitEthernet1/0/3
[Device-GigabitEthernet1/0/3] port-isolate enable
```

显示隔离组中的信息。

```
<Device> display port-isolate group
Port-isolate group information:
Uplink port support: NO
Group ID: 1
    GigabitEthernet1/0/1    GigabitEthernet1/0/2    GigabitEthernet1/0/3
```

1.2.4 完整配置

```
#
interface GigabitEthernet1/0/1
port-isolate enable
#
interface GigabitEthernet1/0/2
port-isolate enable
#
interface GigabitEthernet1/0/3
port-isolate enable
```

1.2.5 配置注意事项

- (1) 目前，设备只支持一个隔离组，即由系统自动创建的隔离组 1，用户不可删除该隔离组或创建其它的隔离组。
- (2) 隔离组内可以加入的端口数量没有限制。
- (3) 隔离组内的端口和隔离组外相同 VLAN 端口数据流量双向互通，隔离组内端口之间不可互通。
- (4) 其中 S5500-SI、S5500-EI 系列以太网交换机的端口隔离特性对二、三层数据报文均隔离，而表 1-1 中其它各系列交换机仅对二层数据报文进行隔离。

目 录

1 LLDP典型配置指导	1-1
1.1 LLDP简介	1-1
1.2 LLDP典型配置指导	1-1
1.2.1 组网图	1-1
1.2.2 应用要求	1-1
1.2.3 适用产品、版本	1-1
1.2.4 配置过程和解释	1-2
1.2.5 完整配置	1-4
1.2.6 配置注意事项	1-4
1.3 LLDP兼容CDP功能典型配置举例	1-5
1.3.1 组网图	1-5
1.3.2 应用需求	1-5
1.3.3 适用产品、版本	1-5
1.3.4 配置过程和解释	1-5
1.3.5 完整配置	1-6
1.3.6 配置注意事项	1-7

1 LLDP 典型配置指导

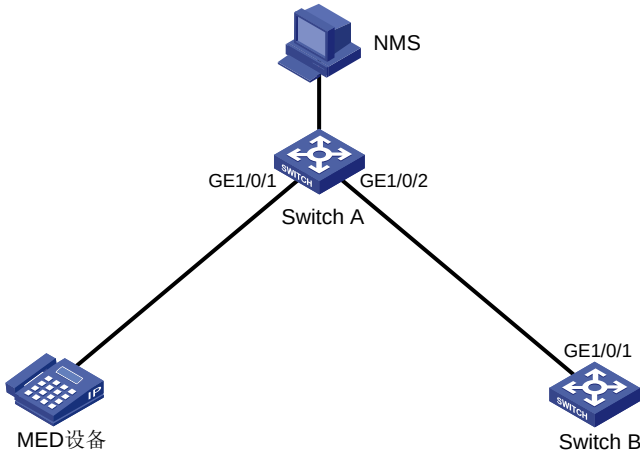
1.1 LLDP 简介

LLDP（Link Layer Discovery Protocol，链路层发现协议）是链路层协议，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，同时也把从邻居接收的 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。

1.2 LLDP 典型配置指导

1.2.1 组网图

图1-1 LLDP 典型配置举例图



1.2.2 应用要求

- NMS 通过以太网与 Switch A 相连，Switch A 分别通过 GigabitEthernet1/0/1、GigabitEthernet1/0/2 与 MED 设备、Switch B 相连。
- 在 Switch A 和 Switch B 的相应接口配置 LLDP 功能，使得 NMS 可以对 Switch A 链路的通信情况进行判断。

1.2.3 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S5500-EI 系列以太网交换机	Release 2102 软件版本	S5500-EI 全系列硬件版本
S7500E 系列以太网交换机	Release 6300 软件版本	全系列硬件版本

1.2.4 配置过程和解释

(1) 配置 Switch A

进入系统视图。

```
<SwitchA> system-view
```

全局使能 LLDP 功能。

```
[SwitchA] lldp enable
```

分别在 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 接口使能 LLDP 功能并配置其工作模式为 rx。

```
[SwitchA] interface GigabitEthernet1/0/1
```

```
[SwitchA-GigabitEthernet1/0/1] lldp enable
```

```
[SwitchA-GigabitEthernet1/0/1] lldp admin-status rx
```

```
[SwitchA-GigabitEthernet1/0/1] quit
```

```
[SwitchA] interface GigabitEthernet1/0/2
```

```
[SwitchA-GigabitEthernet1/0/2] lldp enable
```

```
[SwitchA-GigabitEthernet1/0/2] lldp admin-status rx
```

```
[SwitchA-GigabitEthernet1/0/2] quit
```

(2) 配置 Switch B

进入系统视图。

```
<SwitchB> system-view
```

全局使能 LLDP 功能。

```
[SwitchB] lldp enable
```

在 GigabitEthernet1/0/1 使能 LLDP 功能并配置其工作模式为 tx。

```
[SwitchB] interface GigabitEthernet1/0/1
```

```
[SwitchB-GigabitEthernet1/0/1] lldp enable
```

```
[SwitchB-GigabitEthernet1/0/1] lldp admin-status tx
```

(3) 验证配置结果

在 Switch A 上显示全局和接口的状态信息。

```
<SwitchA> display lldp status
```

```
Global status of LLDP : Enable
```

```
The current number of neighbors : 2
```

```
Neighbor information last changed time : 0 days, 0 hours, 4 minutes, 40 seconds
```

```
Transmit interval : 30s
```

```
Hold multiplier : 4
```

```
Reinit delay : 2s
```

```
Transmit delay : 2s
```

```
Trap interval : 5s
```

```
Fast start times : 3
```

```
Port 0 [GigabitEthernet1/0/1] :
```

```
Port status of LLDP : Enable
```

```
Admin status : Rx_Only
```

```
Trap flag : No
```

```
Roll time : 0s
```

```
Number of neighbors : 1
```

```
Number of MED neighbors : 1
```

```
Number of sent optional TLV : 0
```

```
Number of received unknown TLV : 0
```

```
Port 1 [GigabitEthernet1/0/2] :
```

```
Port status of LLDP : Enable
```

```
Admin status : Rx_Only
```

```
Trap flag : No
```

```
Roll time : 0s
```

```
Number of neighbors : 1
```

```
Number of MED neighbors : 0
```

```
Number of sent optional TLV : 0
```

```
Number of received unknown TLV : 3
```

```
……（其他端口的显示信息略）
```

缺省情况下，Telnet 终端信息中心屏幕开关处于关闭状态。欲在 NMS 端看到 LLDP 状态变化产生的日志信息，需打开屏幕开关。

```
<SwitchA> terminal monitor
```

将 Switch A 和 Switch B 上的链路断掉，Switch A 上会相继输出如下日志信息，Switch B 与此类似（此信息只有在终端屏幕开关打开的情况下才能看到）。

```
%Nov 21 11:38:42:86 2007 H3C IFNET/4/LINK UPDOWN: GigabitEthernet1/0/2: link status is DOWN
```

```
%Nov 21 11:40:26:846 2007 H3C LLDP/2/AGEOUTREM:Port GigabitEthernet1/0/2 (IfIndex 9437201):Neighbor aged out, chassis ID: 000f-e272-8351, port ID: GigabitEthernet1/0/1.
```

在 Switch A 上显示全局和接口的状态信息。

```
<SwitchA> display lldp status
```

```
Global status of LLDP : Enable
```

```
The current number of neighbors : 1
```

```
Neighbor information last changed time : 0 days, 0 hours, 5 minutes, 20 seconds
```

```
Transmit interval : 30s
```

```
Hold multiplier : 4
```

```
Reinit delay : 2s
```

```
Transmit delay : 2s
```

```
Trap interval : 5s
```

```
Fast start times : 3
```

```
Port 0 [GigabitEthernet1/0/1] :
```

```
Port status of LLDP : Enable
```

```
Admin status : Rx_Only
```

```
Trap flag : No
```

```
Roll time : 0s
```

```
Number of neighbors : 1
```

```
Number of MED neighbors : 1
```

```

Number of sent optional TLV      : 0
Number of received unknown TLV  : 5

Port 1 [GigabitEthernet1/0/2] :
Port status of LLDP             : Enable
Admin status                    : Rx_Only
Trap flag                      : No
Roll time                      : 0s

Number of neighbors             : 0
Number of MED neighbors         : 0
Number of sent optional TLV     : 0
Number of received unknown TLV : 0
..... (其他端口的显示信息略)

```

1.2.5 完整配置

- Switch A 上的配置

```

#
interface GigabitEthernet1/0/1
 lldp admin-status rx
#
interface GigabitEthernet1/0/2
 lldp admin-status rx

```

- Switch B 上的配置

```

#
interface GigabitEthernet1/0/1
 lldp admin-status tx

```

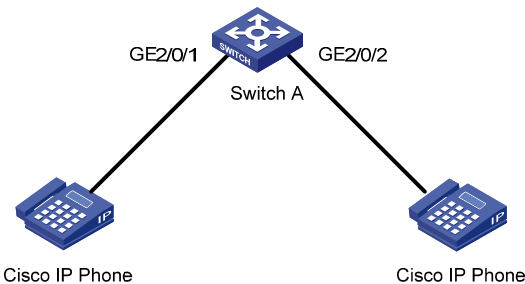
1.2.6 配置注意事项

欲在终端屏幕上查看邻居变化产生的日志信息，需保证终端屏幕开关（通过命令 `terminal monitor` 打开）、日志信息开关（通过命令 `terminal logging` 打开）以及信息中心（通过命令 `info-center enable` 打开）处于打开状态。缺省情况下，S5500-EI 系列以太网交换机 `telnet` 终端屏幕开关处于关闭状态，日志信息开关和信息中心都处于开启状态，所以举例中仅对屏幕开关进行了配置，其他保持缺省情况即可。详情请参考产品操作手册“信息中心”部分。

1.3 LLDP 兼容 CDP 功能典型配置举例

1.3.1 组网图

图1-2 LLDP 兼容 CDP 功能典型配置举例图



1.3.2 应用需求

- Switch A 通过 GigabitEthernet2/0/1 和 GigabitEthernet2/0/2 分别与 Cisco 的 IP 电话相连；
- 在 Switch A 上配置语音 VLAN，VLAN ID 为 2，在 Switch A 上通过配置 LLDP 兼容 CDP 功能使得 IP 电话完成语音 VLAN 自动配置，语音数据流将被限制在配置的语音 VLAN 内，与其它数据流区分开来。

1.3.3 适用产品、版本

表1-2 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S7500E 系列以太网交换机	Release 6300 软件版本	全系列硬件版本

1.3.4 配置过程和解释

(1) 在 Switch A 上配置语音 VLAN

创建 VLAN 2。

```
<SwitchA> system-view
[SwitchA] vlan 2
[SwitchA-vlan2] quit
```

使能全局 Voice VLAN 功能。

```
[SwitchA] voice vlan 2 enable
```

在端口 GigabitEthernet2/0/1 和 GigabitEthernet2/0/2 上使能 Voice VLAN 功能。

```
[SwitchA] interface GigabitEthernet 2/0/1
[SwitchA-GigabitEthernet2/0/1] undo voice vlan mode auto
[SwitchA-GigabitEthernet2/0/1] voice vlan enable
[SwitchA-GigabitEthernet2/0/1] port access vlan 2
[SwitchA-GigabitEthernet2/0/1] quit
[SwitchA] interface GigabitEthernet 2/0/2
[SwitchA-GigabitEthernet2/0/2] undo voice vlan mode auto
[SwitchA-GigabitEthernet2/0/2] voice vlan enable
[SwitchA-GigabitEthernet2/0/2] port access vlan 2
```

```
[SwitchA-GigabitEthernet2/0/2] quit
```

(2) 在 Switch A 上配置 LLDP 兼容 CDP 功能

全局使能 LLDP 功能。

```
[SwitchA] lldp enable
```

全局使能 LLDP 兼容 CDP 功能。

```
[SwitchA] lldp compliance cdp
```

分别在端口 GigabitEthernet2/0/1 和 GigabitEthernet2/0/2 下使能 LLDP 功能配置其工作模式为 TxRx，配置 LLDP 兼容 CDP 模式为 TxRx。

```
[SwitchA] interface GigabitEthernet 2/0/1
```

```
[SwitchA-GigabitEthernet2/0/1] lldp enable
```

```
[SwitchA-GigabitEthernet2/0/1] lldp admin-status txrx
```

```
[SwitchA-GigabitEthernet2/0/1] lldp compliance admin-status cdp txrx
```

```
[SwitchA-GigabitEthernet2/0/1] quit
```

```
[SwitchA] interface GigabitEthernet 2/0/2
```

```
[SwitchA-GigabitEthernet2/0/2] lldp enable
```

```
[SwitchA-GigabitEthernet2/0/2] lldp admin-status txrx
```

```
[SwitchA-GigabitEthernet2/0/2] lldp compliance admin-status cdp txrx
```

```
[SwitchA-GigabitEthernet2/0/2] quit
```

(3) 验证配置结果

在 Switch A 上显示邻居信息。

```
[SwitchA] display lldp neighbor-information
```

```
CDP neighbor-information of port 97[GigabitEthernet2/0/1]:
```

```
  CDP neighbor index : 1
```

```
  Chassis ID          : SEP00141CBCDBFE
```

```
  Port ID             : Port 1
```

```
  Software version    : P0030301MFG2
```

```
  Platform            : Cisco IP Phone 7960
```

```
  Duplex              : Full
```

```
CDP neighbor-information of port 98[GigabitEthernet2/0/2]:
```

```
  CDP neighbor index : 2
```

```
  Chassis ID          : SEP00141CBCDBFF
```

```
  Port ID             : Port 1
```

```
  Software version    : P0030301MFG2
```

```
  Platform            : Cisco IP Phone 7960
```

```
  Duplex              : Full
```

1.3.5 完整配置

```
#
```

```
voice vlan 2 enable
```

```
#
```

```
lldp compliance cdp
```

```
#
```

```
vlan 2
```

```
#
```

```
interface GigabitEthernet2/0/1
port access vlan 2
undo voice vlan mode auto
voice vlan enable
lldp compliance admin-status cdp txrx
#
interface GigabitEthernet2/0/2
port access vlan 2
undo voice vlan mode auto
voice vlan enable
lldp compliance admin-status cdp txrx
#
```

1.3.6 配置注意事项

- 关于 Voice VLAN 的详细介绍，请参考“Voice VLAN 典型配置指导”。
- 欲使 LLDP 兼容 CDP 功能生效，必须先在全局使能 LLDP 兼容 CDP 功能，同时将端口下 LLDP 兼容 CDP 功能的工作模式配置为 TxRx。
- CDP 报文中 TTL 的最大值为 255，CDP 报文中的 TTL 值等于 LLDP 的发送周期与 TTL 乘数的乘积，为了保证 LLDP 兼容 CDP 功能的正常运行，用户在配置 LLDP 的发送周期和 TTL 乘数时需要注意，LLDP 的发送周期与 TTL 乘数的乘积应该小于或等于 255。

目 录

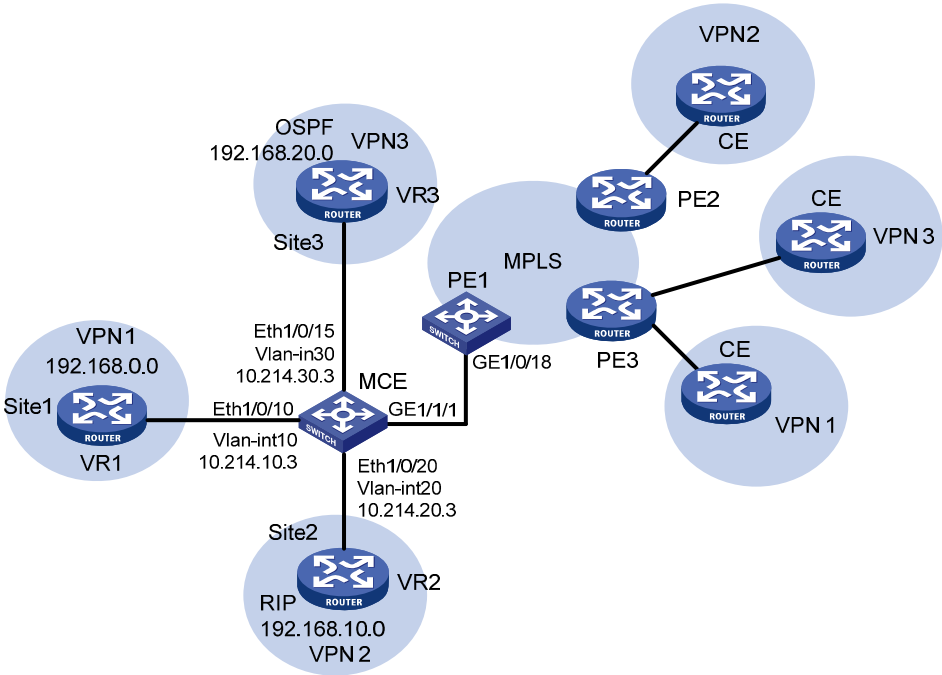
1 MCE典型配置指导	1-1
1.1 使用OSPF/RIP/IS-IS引入VPN路由的MCE典型配置指导	1-1
1.1.1 组网图	1-1
1.1.2 应用要求	1-1
1.1.3 适用产品、版本	1-1
1.1.4 配置过程和解释	1-2
1.1.5 完整配置	1-10
1.1.6 配置注意事项	1-14
1.2 使用BGP引入VPN路由的MCE典型配置指导	1-15
1.2.1 组网图	1-15
1.2.2 应用要求	1-15
1.2.3 适用产品、版本	1-15
1.2.4 配置过程和解释	1-16
1.2.5 完整配置	1-19
1.2.6 配置注意事项	1-21

1 MCE 典型配置指导

1.1 使用 OSPF/RIP/IS-IS 引入 VPN 路由的 MCE 典型配置指导

1.1.1 组网图

图1-1 MCE 组网示意图一



1.1.2 应用要求

- MCE 设备通过 Vlan-interface10 接口（IP 地址 10.214.10.3）连接到 VPN1，地址范围为 192.168.0.0/16，通过 Vlan-interface20（IP 地址 10.214.20.3）接口连接到 VPN2，通过 Vlan-interface30（IP 地址 10.214.30.3）接口连接到 VPN3。
- 其中 Site1 内未使用路由协议；Site2 内运行 RIP 路由协议，地址范围为 192.168.10.0/24；Site3 内运行 OSPF 路由协议，地址范围为 192.168.20.0/24。
- 要求 MCE 设备能够将 VPN 之间的路由隔离，并通过 OSPF 将各 VPN 的路由发布到 PE 设备。
- 对于使用RIP、IS-IS协议把VPN的路由发布到PE设备，其具体配置只在 1.1.4 (5)MCE与PE1 间的路由配置处与使用OSPF作为MCE到PE 之间路由协议时配置不同，所以只在“（5）MCE 与PE1 间的路由配置”中添加了相应RIP和IS-IS配置过程。

1.1.3 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本

产品	软件版本	硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6100 软件版本	配置 LSQ1SRP1CB 引擎或者全部采用 EA 系列业务板
	Release 6300 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.1.4 配置过程和解释



说明

- 为在配置过程中区分设备，现假设 MCE 系统名为“MCE”，VPN1、VPN2 和 VPN3 的出口路由器分别名为“VR1”、“VR2”和“VR3”，PE1 设备系统名为“PE1”。
- 下面对 VPN 的出口路由器和 PE 设备的配置均在假设其为 H3C 设备的基础上进行，如这些设备使用的是非 H3C 设备，配置步骤请参考该产品的用户手册。

(1) 配置 MCE 上的 VPN 实例并与接口进行绑定

切换 MCE 设备的工作模式为 MCE 模式，并重新启动设备。

```
<MCE> system-view
[MCE] switch-mode mce
[MCE] quit
<MCE> reboot
```



说明

在配置 S7500E 系列交换机的 MCE 功能时，不需要配置 **switch-mode mce** 命令和重启设备。

在 MCE 设备上配置 VPN 实例，名称分别为 VPN1、VPN2 和 VPN3，RD 分别取值为 10:1、20:1 和 30:1。

```
<MCE> system-view
[MCE] ip vpn-instance vpn1
[MCE-vpn-instance-vpn1] route-distinguisher 10:1
[MCE-vpn-instance-vpn1] quit
[MCE] ip vpn-instance vpn2
[MCE-vpn-instance-vpn2] route-distinguisher 20:1
[MCE-vpn-instance-vpn2] quit
[MCE] ip vpn-instance vpn3
[MCE-vpn-instance-vpn3] route-distinguisher 30:1
```

创建 VLAN10，将端口 Eth1/0/10 加入 VLAN10，并创建 Vlan-interface10 接口。

```
[MCE-vpn-instance-vpn3] quit
[MCE] vlan 10
[MCE-vlan10] port Ethernet 1/0/10
[MCE-vlan10] quit
```

```
[MCE] interface Vlan-interface 10
```

配置 Vlan-interface10 接口与 VPN1 实例进行绑定, 并配置 IP 地址为 10.214.10.3, 掩码为 24 位。

```
[MCE-Vlan-interface10] ip binding vpn-instance vpn1
```

```
[MCE-Vlan-interface10] ip address 10.214.10.3 24
```

```
[MCE-Vlan-interface10] quit
```

使用类似步骤配置 VLAN20, 将端口 Eth1/0/20 加入 VLAN20, 配置接口与 VPN2 实例绑定并配置 IP 地址。

```
[MCE] vlan 20
```

```
[MCE-vlan20] port Ethernet 1/0/20
```

```
[MCE-vlan20] quit
```

```
[MCE] interface Vlan-interface 20
```

```
[MCE-Vlan-interface20] ip binding vpn-instance vpn2
```

```
[MCE-Vlan-interface20] ip address 10.214.20.3 24
```

```
[MCE-Vlan-interface20] quit
```

使用类似步骤配置 VLAN30, 将端口 Eth1/0/15 加入 VLAN30, 配置接口与 VPN3 实例绑定并配置 IP 地址。

```
[MCE] vlan 30
```

```
[MCE-vlan30] port Ethernet 1/0/15
```

```
[MCE-vlan30] quit
```

```
[MCE] interface Vlan-interface 30
```

```
[MCE-Vlan-interface30] ip binding vpn-instance vpn3
```

```
[MCE-Vlan-interface30] ip address 10.214.30.3 24
```

```
[MCE-Vlan-interface30] quit
```

(2) MCE 与 Site1 之间的路由配置



说明

MCE 与 Site1 直接相连, 且 Site1 内未使用路由协议, 因此可以使用静态路由进行配置。

- 在 VR1 上的配置

配置与 MCE 连接的接口地址为 10.214.10.2/24, 连接 Site1 接口的地址为 192.168.0.1/24。向 VLAN 中增加端口和配置接口 IP 地址的配置这里省略。

在 VR1 上配置缺省路由, 指定出方向报文的下一跳地址为 10.214.10.3。

```
<VR1> system-view
```

```
[VR1] ip route-static 0.0.0.0 0.0.0.0 10.214.10.3
```

- 在 MCE 上的配置

在 MCE 上指定静态路由, 去往 192.168.0.0 网段的报文, 下一跳地址为 10.214.10.2, 并将此路由与 VPN1 实例绑定。

```
[MCE-Vlan-interface20] quit
```

```
[MCE] ip route-static vpn-instance vpn1 192.168.0.0 16 10.214.10.2
```

显示 MCE 上为 VPN1 实例维护的路由信息。

```
[MCE] display ip routing-table vpn-instance vpn1
```

```
Routing Tables: vpn1
```

Destinations : 5 Routes : 5

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
10.214.10.0/24	Direct	0	0	10.214.10.3	Vlan10
10.214.10.3/32	Direct	0	0	127.0.0.1	InLoop0
192.168.0.0/16	Static	60	0	10.214.10.2	Vlan10

可以看到，已经在 MCE 上为 Site1 指定了静态路由。

(3) MCE 与 Site2 之间的路由配置

- 在 VR2 上的配置

在 VR2 上，配置与 MCE 连接的接口地址为 10.214.20.2/24（配置过程略），配置 RIP，将网段 192.168.10.0 和 10.214.20.0 发布。

```
<VR2> system-view
[VR2] rip 20
[VR2-rip-20] network 192.168.10.0
[VR2-rip-20] network 10.0.0.0
```

- 在 MCE 上的配置



说明

Site2 内已经运行了 RIP，因此可以在 MCE 上配置 RIP 路由协议，加入到 Site2 的路由运算中，自动更新路由信息。

配置 RIP 协议，进程为 20，并与 VPN2 实例进行绑定。

```
[MCE] rip 20 vpn-instance vpn2
```

将网段 10.214.10.0 发布，关闭路由自动聚合功能，引入 OSPF（进程号 20）的路由信息。

需要注意的是，当 MCE 与 PE 间路由为 RIP 或 IS-IS 时，import-route 命令中参数 ospf 也对应改为 rip 或 isis。

```
[MCE-rip-20] network 10.0.0.0
[MCE-rip-20] undo summary
[MCE-rip-20] import-route ospf
```

在 MCE 上查看 VPN2 实例的路由信息。

```
[MCE-rip-20] display ip routing-table vpn-instance vpn2
```

Routing Tables: vpn2

Destinations : 5 Routes : 5

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
10.214.20.0/24	Direct	0	0	10.214.20.3	Vlan20
10.214.20.3/32	Direct	0	0	127.0.0.1	InLoop0

```
192.168.10.0/24    RIP    100    1    10.214.20.2    Vlan20
```

可以看到，MCE 已经通过 RIP 学习到了 Site2 内的私网路由，并与 Site1 内的 192.168.0.0 路由信息分别维护在两个路由表内，有效进行了隔离。

(4) MCE 与 Site3 之间的路由配置

- 在 VR3 上的配置

将 VR3 与 MCE 设备连接的接口 IP 地址设置为 10.214.30.2/24，配置过程省略。在 VR3 上配置 OSPF 协议，进程为 30，将 192.168.20.0 和 10.214.30.0 网段发布。

```
<VR3> system-view
[VR3] ospf 30
[VR3-ospf-30] area 0
[VR3-ospf-30-area-0.0.0.0] network 192.168.20.0 0.0.0.255
[VR3-ospf-30-area-0.0.0.0] network 10.214.30.0 0.0.0.255
```

- 在 MCE 上的配置



说明

Site3 内已经运行了 OSPF，因此可以在 MCE 上配置 OSPF 路由协议，加入到 Site3 的路由运算中，自动更新路由信息。

配置 MCE 的 Loopback0 接口，用于指定 MCE 的 Router ID，地址为 101.101.10.1。配置步骤这里省略。

在 MCE 设备上配置 OSPF30 进程，与 VPN3 实例绑定，开启 OSPF 多实例功能（当 MCE 上只有一个 OSPF 进程时不需要配制此功能），发布 10.214.30.0 网段。

需要注意的是，当 MCE 与 PE 间路由为 RIP 或 IS-IS 时，此处 OSPF 配置中不需要开启 OSPF 多实例功能。

```
<MCE> system-view
[MCE] ospf 30 router id 101.101.10.1 vpn-instance vpn3
[MCE-ospf-30] vpn-instance-capability simple
[MCE-ospf-30] area 0
[MCE-ospf-30-area-0.0.0.0] network 10.214.30.0 0.0.0.255
```

在 MCE 设备上查看 VPN3 实例中的路由信息。

```
[MCE-ospf-30-area-0.0.0.0] display ip routing-table vpn-instance vpn3
Routing Tables: vpn3
Destinations : 5          Routes : 5
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
10.214.30.0/24	Direct	0	0	10.214.30.3	Vlan30
10.214.30.3/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.20.0/24	OSPF	10	2	10.214.30.2	Vlan30

可以看到，MCE 已经通过 OSPF 学习到了 Site3 内的私网路由。

(5) MCE 与 PE1 间的路由配置

- 在 MCE 上的配置

MCE 使用 GigabitEthernet1/1/1 端口连接到 PE1 的 GigabitEthernet1/0/18 端口，需要配置这个端口为 Trunk 端口，并允许 VLAN10、VLAN20 和 VLAN30 的报文携带 Tag 通过。

```
[MCE] interface GigabitEthernet 1/1/1
[MCE-GigabitEthernet1/1/1] port link-type trunk
[MCE-GigabitEthernet1/1/1] port trunk permit vlan 10 20 30
```

配置 MCE 启动 OSPF 进程 10，绑定到 VPN1 实例，域 ID 设置为 10，在 Area0 区域发布 10.214.10.0 网段，并引入 VPN1 的静态路由。

```
[MCE-GigabitEthernet1/1/1] quit
[MCE] ospf 10 router-id 101.101.10.1 vpn-instance vpn1
[MCE-ospf-10] domain-id 10
[MCE-ospf-10] area 0
[MCE-ospf-10-area-0.0.0.0] network 10.214.10.0 0.0.0.255
[MCE-ospf-10-area-0.0.0.0] quit
[MCE-ospf-10] import-route static
[MCE-ospf-10] quit
```

配置 MCE 启动 OSPF 进程 20，绑定到 VPN2 实例，域 ID 设置为 20，在 Area0 区域发布 10.214.20.0 网段，并引入 VPN2 的 RIP 路由。

```
[MCE] ospf 20 router-id 101.101.10.1 vpn-instance vpn2
[MCE-ospf-20] domain-id 20
[MCE-ospf-20] area 0
[MCE-ospf-20-area-0.0.0.0] network 10.214.20.0 0.0.0.255
[MCE-ospf-20-area-0.0.0.0] quit
[MCE-ospf-20] import-route rip
```

配置 MCE 的 OSPF 进程 30，域 ID 设置为 30，在 Area0 区域发布 10.214.30.0 网段。

```
[MCE] ospf 30 router-id 101.101.10.1 vpn-instance vpn3
[MCE-ospf-30] domain-id 30
[MCE-ospf-30] area 0
[MCE-ospf-30-area-0.0.0.0] network 10.214.30.0 0.0.0.255
[MCE-ospf-30-area-0.0.0.0] quit
```

- 在 PE1 上的配置

配置 PE1 的 GigabitEthernet1/0/18 端口允许 VLAN10、VLAN20 和 VLAN30 的报文通过。

```
<PE1> system-view
[PE1] interface GigabitEthernet 1/0/18
[PE1-GigabitEthernet1/0/18] port link-type trunk
[PE1-GigabitEthernet1/0/18] port trunk permit vlan 10 20 30
```

配置 PE1 的 Vlan-interface10、Vlan-interface20 和 Vlan-interface30 的接口分别为 10.214.10.4、10.214.20.4 和 10.214.30.4，并分别与 VPN1、VPN2 和 VPN3 实例进行绑定，配置步骤这里省略。

配置 PE1 的 Loopback0 接口，用于指定 PE1 的 Router ID，地址为 100.100.10.1。配置过程这里省略。

配置 PE1 启动 OSPF 进程 10，绑定到 VPN1 实例，域 ID 为 10，在 Area0 区域发布 10.214.10.0 网段。

```
[PE1-GigabitEthernet1/0/18] quit
[PE1] ospf 10 router-id 100.100.10.1 vpn-instance vpn1
[PE1-ospf-10] domain-id 10
[PE1-ospf-10] area 0
[PE1-ospf-10-area-0.0.0.0] network 10.214.10.0 0.0.0.255
```

配置 PE1 启动 OSPF 进程 20 和进程 30，绑定到 VPN2 和 VPN3 实例，域 ID 分别为 20 和 30，并分别在 Area0 区域发布 10.214.20.0 和 10.214.30.0 网段。配置过程与上文类似，这里不再赘述。

显示 PE 上的 VPN1 路由信息。

```
[PE-ospf-10-area-0.0.0.0] display ip routing-table vpn-instance vpn1
```

```
Routing Tables: vpn1
```

```
Destinations : 6          Routes : 6
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
10.214.10.0/24	Direct	0	0	10.214.10.4	Vlan10
10.214.10.4/32	Direct	0	0	127.0.0.1	InLoop0
100.100.10.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.0.0/16	O_ASE	150	1	10.214.10.2	Vlan10

可以看到，Site1 内的静态路由已经引入到 MCE 与 PE 间的 OSPF 路由表中。

显示 PE 上的 VPN2 路由信息。

```
<PE> display ip routing-table vpn-instance vpn2
```

```
Routing Tables: vpn2
```

```
Destinations : 6          Routes : 6
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
10.214.20.0/24	Direct	0	0	10.214.20.4	Vlan20
10.214.20.4/32	Direct	0	0	127.0.0.1	InLoop0
200.200.20.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.10.0/24	O_ASE	150	1	10.214.20.2	Vlan20

显示 PE 上的 VPN3 路由信息。

```
<PE> display ip routing-table vpn-instance vpn3
```

```
Routing Tables: vpn3
```

```
Destinations : 6          Routes : 6
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
10.214.30.0/24	Direct	0	0	10.214.30.4	Vlan30
10.214.30.4/32	Direct	0	0	127.0.0.1	InLoop0
200.200.30.3/32	Direct	0	0	127.0.0.1	InLoop0


```
192.168.20.0/24    OSPF    10    1    10.214.30.2    Vlan30
```

至此，通过配置，已经将三个 VPN 站点内的路由信息完整地传播到 PE 中，配置完成。

当使用 RIP 作为 MCE 到 PE 间路由协议时，配置如下

- 在 MCE 上的配置

MCE 使用 GigabitEthernet1/1/1 端口连接到 PE1 的 GigabitEthernet1/0/18 端口，需要配置这个端口为 Trunk 端口，并允许 VLAN10、VLAN20 和 VLAN30 的报文携带 Tag 通过。

```
[MCE] interface GigabitEthernet 1/1/1
[MCE-GigabitEthernet1/1/1] port link-type trunk
[MCE-GigabitEthernet1/1/1] port trunk permit vlan 10 20 30
```

配置 MCE 启动 RIP 进程 10，绑定到 VPN1 实例，发布 10.214.10.0 网段，并引入 VPN1 的静态路由。

```
[MCE-GigabitEthernet1/1/1] quit
[MCE] rip 10 vpn-instance vpn1
[MCE-rip-10] network 10.0.0.0
[MCE-rip-10] import-route static
[MCE-rip-10] quit
```

配置 MCE 启动 RIP 进程 20，发布 10.214.20.0 网段。

```
[MCE] rip 20 vpn-instance vpn2
[MCE-rip-20] network 10.0.0.0
[MCE-rip-20] quit
```

#配置 MCE 启动 RIP 进程 30，绑定到 VPN3 实例，发布 10.214.30.0 网段，并引入 VPN2 的 OSPF 路由。

```
[MCE] rip 30 vpn-instance vpn3
[MCE-rip-30] network 10.0.0.0
[MCE-rip-30] import-route ospf
[MCE-rip-30] quit
```

- 在 PE1 上的配置

配置 PE1 的 GigabitEthernet1/0/18 端口允许 VLAN10、VLAN20 和 VLAN30 的报文通过。

```
<PE1> system-view
[PE1] interface GigabitEthernet 1/0/18
[PE1-GigabitEthernet1/0/18] port link-type trunk
[PE1-GigabitEthernet1/0/18] port trunk permit vlan 10 20 30
[PE1-GigabitEthernet1/0/18] quit
```

配置 PE1 的 Vlan-interface10、Vlan-interface20 和 Vlan-interface30 的接口分别为 10.214.10.4、10.214.20.4 和 10.214.30.4，并分别与 VPN1、VPN2 和 VPN3 实例进行绑定，配置步骤这里省略。

配置 PE1 启动 RIP 进程 10，绑定到 VPN1 实例，域 ID 为 10，发布 10.214.10.0 网段。

```
[PE1] rip 10 vpn-instance vpn1
[PE1-rip-10] network 10.0.0.0
```

配置 PE1 启动 RIP 进程 20 和进程 30，绑定到 VPN2 和 VPN3 实例，并分别发布 10.214.20.0 和 10.214.30.0 网段。配置过程与上文类似，这里不再赘述。

当使用 IS-IS 作为 MCE 到 PE 间路由协议时，配置如下

- 在 MCE 上的配置

MCE 使用 GigabitEthernet1/1/1 端口连接到 PE1 的 GigabitEthernet1/0/18 端口，需要配置这个端口为 Trunk 端口，并允许 VLAN10、VLAN20 和 VLAN30 的报文携带 Tag 通过。

```
[MCE] interface GigabitEthernet 1/1/1
[MCE-GigabitEthernet1/1/1] port link-type trunk
[MCE-GigabitEthernet1/1/1] port trunk permit vlan 10 20 30
[MCE-GigabitEthernet1/1/1] quit
```

配置 MCE 启动 IS-IS 进程 10，绑定到 VPN1 实例；网络实体名称为 10.0000.0000.0001.00；路由类型为 level-1-2。同时在 Vlan-interface10 接口上使能 IS-IS 进程 10，并引入 VPN1 的静态路由。

```
[MCE] isis 10 vpn-instance vpn1
[MCE-isis-10] network-entity 10.0000.0000.0001.00
[MCE-isis-10] is-level level-1-2
[MCE-isis-10] import-route static level-1-2
[MCE-isis-10] quit
[MCE] interface Vlan-interface 10
[MCE-vpn-instance-vpn10] isis enable 10
[MCE-vpn-instance-vpn10] quit
```

配置 MCE 启动 IS-IS 进程 20，绑定到 VPN2 实例；网络实体名称为 10.0000.0000.0002.00；路由类型为 level-1-2，同时在 Vlan-interface20 接口上使能 IS-IS 进程 20，并引入 VPN2 的 RIP 路由。

```
[MCE] isis 20 vpn-instance vpn2
[MCE-isis-20] network-entity 10.0000.0000.0002.00
[MCE-isis-20] is-level level-1-2
[MCE-isis-20] import-route rip level-1-2
[MCE-isis-20] quit
[MCE] interface Vlan-interface 20
[MCE-vpn-instance-vpn20] isis enable 20
[MCE-vpn-instance-vpn20] quit
```

#配置 MCE 启动 IS-IS 进程 30，绑定到 VPN3 实例；网络实体名称为 10.0000.0000.0003.00；路由类型为 level-1-2，同时在 Vlan-interface30 接口上使能 IS-IS 进程 30，并引入 VPN3 的 OSPF 路由。

```
[MCE] isis 30 vpn-instance vpn3
[MCE-isis-30] network-entity 10.0000.0000.0003.00
[MCE-isis-30] is-level level-1-2
[MCE-isis-30] import-route ospf level-1-2
[MCE-isis-30] quit
[MCE] interface Vlan-interface 30
[MCE-vpn-instance-vpn30] isis enable 30
[MCE-vpn-instance-vpn30] quit
```

- 在 PE1 上的配置

配置 PE1 的 GigabitEthernet1/0/18 端口允许 VLAN10、VLAN20 和 VLAN30 的报文通过。

```
<PE1> system-view
[PE1] interface GigabitEthernet 1/0/18
[PE1-GigabitEthernet1/0/18] port link-type trunk
[PE1-GigabitEthernet1/0/18] port trunk permit vlan 10 20 30
```

```
[PE1-GigabitEthernet1/0/18] quit
```

配置 PE1 的 Vlan-interface10、Vlan-interface20 和 Vlan-interface30 的接口分别为 10.214.10.4、10.214.20.4 和 10.214.30.4，并分别与 VPN1、VPN2 和 VPN3 实例进行绑定，配置步骤这里省略。

配置 PE1 启动 IS-IS 进程 10，绑定到 VPN1 实例，网络实体名称为 10.0000.0000.0004.00；路由类型为 level-1-2，同时在 Vlan-interface10 接口上使能 IS-IS 进程 10。

```
[PE1] isis 10 vpn-instance vpn1
```

```
[PE1-isis-30] network-entity 10.0000.0000.0004.00
```

```
[PE1-isis-30] is-level level-1-2
```

```
[PE1-isis-30] quit
```

```
[PE1] interface Vlan-interface 10
```

```
[PE1-Vlan-interface10] isis enable 10
```

```
[PE1-Vlan-interface10] quit
```

配置 PE1 启动 IS-IS 进程 20 和进程 30，绑定到 VPN2 和 VPN3 实例，网络实体名称分别为 10.0000.0000.0005.00 和 10.0000.0000.0006.00，并分别在 Vlan-interface20 和 Vlan-interface30 使能 IS-IS 进程 20 和 IS-IS 进程 30。配置过程与上文类似，这里不再赘述。

1.1.5 完整配置



说明

此处仅列出 MCE 设备上的完整配置，组网中其他设备的配置请参见该产品的用户手册。

使用 OSPF 作为 MCE 到 PE 之间路由协议的完整配置

```
#
```

```
ip vpn-instance vpn1
```

```
route-distinguisher 10:1
```

```
#
```

```
ip vpn-instance vpn2
```

```
route-distinguisher 20:1
```

```
#
```

```
ip vpn-instance vpn3
```

```
route-distinguisher 30:1
```

```
#
```

```
vlan 1
```

```
#
```

```
vlan 10
```

```
#
```

```
vlan 20
```

```
#
```

```
vlan 30
```

```
#
```

```
interface LoopBack0
```

```
ip address 101.101.10.1 255.255.255.255
```

```
#
```

```
interface Vlan-interface10
```

```
ip binding vpn-instance vpn1
```

```

ip address 10.214.10.3 255.255.255.0
#
interface Vlan-interface20
ip binding vpn-instance vpn2
ip address 10.214.20.3 255.255.255.0
#
interface Vlan-interface30
ip binding vpn-instance vpn3
ip address 10.214.30.3 255.255.255.0
#
interface Ethernet1/0/10
port access vlan 10
#
interface Ethernet1/0/15
port access vlan 30
#
interface Ethernet1/0/20
port access vlan 20
#
interface GigabitEthernet1/1/1
port link-type trunk
port trunk permit vlan 1 10 20 30
#
ospf 10 router-id 101.101.10.1 vpn-instance vpn1
vpn-instance-capability simple
import-route static
domain-id 0.0.0.10
area 0.0.0.0
network 10.214.10.0 0.0.0.255
#
ospf 20 router-id 101.101.10.1 vpn-instance vpn2
vpn-instance-capability simple
import-route rip 20
domain-id 0.0.0.20
area 0.0.0.0
network 10.214.20.0 0.0.0.255
#
ospf 30 router-id 101.101.10.1 vpn-instance vpn3
vpn-instance-capability simple
domain-id 0.0.0.30
area 0.0.0.0
network 10.214.30.0 0.0.0.255
#
rip 20 vpn-instance vpn2
network 10.0.0.0
import-route ospf 20
#
ip route-static vpn-instance vpn1 192.168.0.0 255.255.0.0 10.214.10.2

```

使用 RIP 作为 MCE 到 PE 之间路由协议的完整配置

```
#
ip vpn-instance vpn1
  route-distinguisher 10:1
#
ip vpn-instance vpn2
  route-distinguisher 20:1
#
ip vpn-instance vpn3
  route-distinguisher 30:1
#
vlan 1
#
vlan 10
#
vlan 20
#
vlan 30
#
interface Vlan-interface10
  ip binding vpn-instance vpn1
  ip address 10.214.10.3 255.255.255.0
#
interface Vlan-interface20
  ip binding vpn-instance vpn2
  ip address 10.214.20.3 255.255.255.0
#
interface Vlan-interface30
  ip binding vpn-instance vpn3
  ip address 10.214.30.3 255.255.255.0
#
interface Ethernet1/0/10
  port access vlan 10
#
interface Ethernet1/0/15
  port access vlan 30
#
interface Ethernet1/0/20
  port access vlan 20
#
interface GigabitEthernet1/1/1
  port link-type trunk
  port trunk permit vlan 1 10 20 30
#
rip 10 vpn-instance vpn1
  import-route static
  network 10.0.0.0
#
```

```

rip 20 vpn-instance vpn2
 network 10.0.0.0
#
rip 30 vpn-instance vpn3
 import-route ospf 30
 network 10.214.30.0 0.0.0.255
#
ospf 30 router-id 101.101.10.1 vpn-instance vpn3
 area 0.0.0.0
 network 10.214.30.0 0.0.0.255
 import-route rip 30
#
 ip route-static vpn-instance vpn1 192.168.0.0 255.255.0.0 10.214.10.2

```

使用 IS-IS 作为 MCE 到 PE 之间路由协议的完整配置

```

#
ip vpn-instance vpn1
 route-distinguisher 10:1
#
ip vpn-instance vpn2
 route-distinguisher 20:1
#
ip vpn-instance vpn3
 route-distinguisher 30:1
#
vlan 1
#
vlan 10
#
vlan 20
#
vlan 30
#
interface Vlan-interface10
 ip binding vpn-instance vpn1
 ip address 10.214.10.3 255.255.255.0
 isis enable 10
#
interface Vlan-interface20
 ip binding vpn-instance vpn2
 ip address 10.214.20.3 255.255.255.0
 isis enable 20
#
interface Vlan-interface30
 ip binding vpn-instance vpn3
 ip address 10.214.30.3 255.255.255.0
 isis enable 30
#
interface Ethernet1/0/10

```

```

port access vlan 10
#
interface Ethernet1/0/15
port access vlan 30
#
interface Ethernet1/0/20
port access vlan 20
#
interface GigabitEthernet1/1/1
port link-type trunk
port trunk permit vlan 1 10 20 30
#
isis 10 vpn-instance vpn1
is-level level-1-2
network-entity 10.0000.0000.0001.00
import-route static level-1-2
#
isis 20 vpn-instance vpn2
is-level level-1-2
network-entity 10.0000.0000.0002.00
import-route rip 20 level-1-2
#
isis 30 vpn-instance vpn3
is-level level-1-2
network-entity 10.0000.0000.0003.00
import-route ospf 30 level-1-2
#
ospf 30 router-id 101.101.10.1 vpn-instance vpn3
area 0.0.0.0
network 10.214.30.0 0.0.0.255
import-route isis 30
#
rip 20 vpn-instance vpn2
network 10.0.0.0
import-route isis 20
#
ip route-static vpn-instance vpn1 192.168.0.0 255.255.0.0 10.214.10.2

```

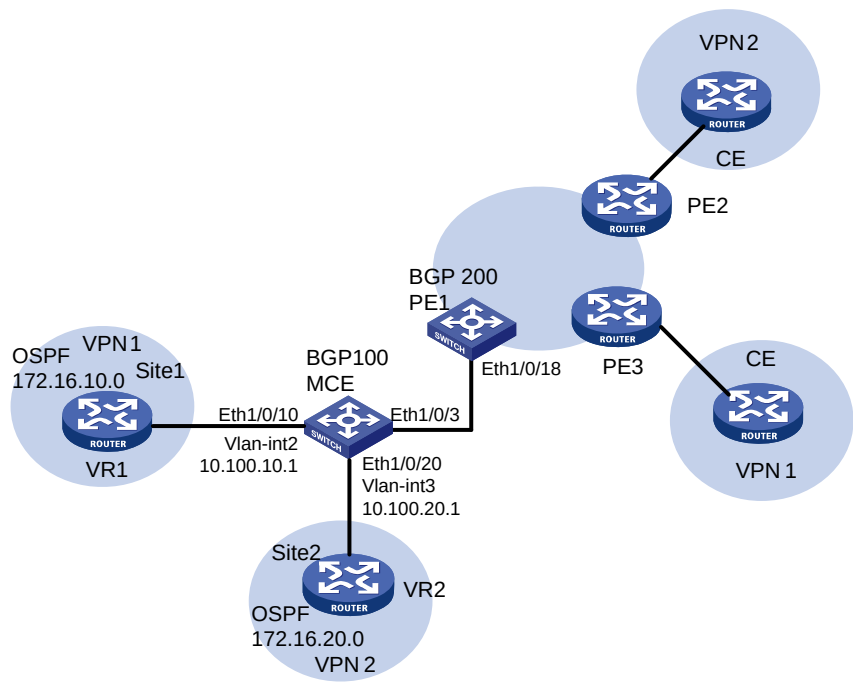
1.1.6 配置注意事项

无

1.2 使用 BGP 引入 VPN 路由的 MCE 典型配置指导

1.2.1 组网图

图1-2 MCE 组网示意图二



1.2.2 应用要求

- 使用 H3C 设备作为 MCE 设备,将 Site1 和 Site2 内的 VPN 路由发布到 PE 设备,使穿过 MPLS 骨干网络的同一 VPN 内的设备间能够正常通信。
- Site1 和 Site2 内部均使用 OSPF 协议, MCE 与 PE 间使用 EBGP 协议。

1.2.3 适用产品、版本

表1-2 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6100 软件版本	配置 LSQ1SRP1CB 引擎或者全部采用 EA 系列业务板
	Release 6300 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.2.4 配置过程和解释



说明

- 为在配置过程中区分设备，现假设 MCE 系统名为“MCE”，VPN1 和 VPN2 的出口路由器分别名为“VR1”和“VR2”，PE1 设备系统名为“PE1”。
- 下面对 VPN 的出口路由器和 PE 设备的配置均在假设其为 H3C 设备的基础上进行，如这些设备使用的是非 H3C 设备，配置步骤请参考该产品的用户手册。

(1) 配置 MCE 上的 VPN 实例并与接口进行绑定

切换 MCE 设备的工作模式为 MCE 模式，并重新启动设备。

```
<MCE> system-view
[MCE] switch-mode mce
[MCE] quit
<MCE> reboot
```



说明

在配置 S7500E 系列交换机的 MCE 功能时，不需要配置 **switch-mode mce** 命令和重启设备。

在 MCE 设备上配置 VPN 实例，名称分别为 VPN1 和 VPN2，RD 分别取值为 10:1、20:1，VPN Target 取值与 RD 取相同数值，Export 和 Import 均取此值。

```
<MCE> system-view
[MCE] ip vpn-instance vpn1
[MCE-vpn-instance-vpn1] route-distinguisher 10:1
[MCE-vpn-instance-vpn1] vpn-target 10:1 both
[MCE-vpn-instance-vpn1] quit
[MCE] ip vpn-instance vpn2
[MCE-vpn-instance-vpn2] route-distinguisher 20:1
[MCE-vpn-instance-vpn2] vpn-target 20:1 both
[MCE-vpn-instance-vpn2] quit
```

创建 VLAN2，将端口 Eth1/0/10 加入 VLAN2，并创建 Vlan-interface2 接口。

```
[MCE] vlan 2
[MCE-vlan2] port Ethernet 1/0/10
[MCE-vlan2] quit
[MCE] interface Vlan-interface 2
```

配置 Vlan-interface2 接口与 VPN1 实例进行绑定，并配置 IP 地址为 10.100.10.1，掩码为 24 位。

```
[MCE-Vlan-interface2] ip binding vpn-instance vpn1
[MCE-Vlan-interface2] ip address 10.100.10.1 24
[MCE-Vlan-interface2] quit
```

使用类似步骤配置 VLAN3，将端口 Eth1/0/20 加入 VLAN3，配置接口与 VPN2 实例绑定并配置 IP 地址。

```
[MCE] vlan 3
[MCE-vlan3] port Ethernet 1/0/20
[MCE-vlan3] quit
[MCE] interface Vlan-interface 3
```

```
[MCE-Vlan-interface3] ip binding vpn-instance vpn2
[MCE-Vlan-interface3] ip address 10.100.20.1 24
[MCE-Vlan-interface3] quit
```

(2) MCE 与 Site1 之间的路由配置

- 在 VR1 上的配置

启动 OSPF 进程 10，将网段 172.16.10.0 和 10.100.10.0 发布。

```
<VR1> system-view
[VR1] ospf 10
[VR1-ospf-10] area 0
[VR1-ospf-10-area-0.0.0.0] network 10.100.10.0 0.0.0.255
[VR1-ospf-10-area-0.0.0.0] network 172.16.10.0 0.0.0.255
```

- 在 MCE 上的配置

配置 MCE 的 OSPF 协议，进程 10 与 VPN1 实例绑定，Router ID 为 10.10.10.1，引入 VPN1 中的 BGP 路由信息，开启 OSPF 多实例功能，并将网段 10.100.10.0 发布。

```
<MCE> system-view
[MCE] ospf 10 router-id 10.10.10.1 vpn-instance vpn1
[MCE-ospf-10] vpn-instance capability simple
[MCE-ospf-10] import-route bgp
[MCE-ospf-10] area 0
[MCE-ospf-10-area-0.0.0.0] network 10.100.10.0 0.0.0.255
```

显示 VPN1 实例的路由信息。

```
[MCE-ospf-10-area-0.0.0.0] display ip routing-table vpn-instance vpn1
Routing Tables: vpn1
Destinations : 5 Routes : 5
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
10.100.10.0/24	Direct	0	0	10.100.10.1	Vlan2
10.100.10.1/32	Direct	0	0	127.0.0.1	InLoop0
172.16.10.0/24	OSPF	10	1	10.100.10.2	Vlan2

可以看到，MCE 已经通过 OSPF 进程 10 学习到了 Site1 内的路由。

(3) MCE 与 Site2 之间的路由配置

- 在 VR2 上的配置

启动 OSPF 进程 20，将网段 172.16.20.0 和 10.100.20.0 发布。

```
<VR2> system-view
[VR2] ospf 20
[VR2-ospf-20] area 0
[VR2-ospf-20-area-0.0.0.0] network 10.100.20.0 0.0.0.255
[VR2-ospf-20-area-0.0.0.0] network 172.16.20.0 0.0.0.255
```

- 在 MCE 上的配置

配置 MCE 的 OSPF 协议，进程 20 与 VPN2 实例绑定，Router ID 为 10.10.10.1，引入 VPN2 中的 BGP 路由信息，开启 OSPF 多实例功能，并将网段 10.100.20.0 发布。

```
<MCE> system-view
[MCE] ospf 20 router-id 10.10.10.1 vpn-instance vpn2
[MCE-ospf-20] vpn-instance capability simple
[MCE-ospf-20] import-route bgp
[MCE-ospf-20] area 0
[MCE-ospf-20-area-0.0.0.0] network 10.100.20.0 0.0.0.255
```

显示 VPN2 实例的路由信息。

```
[MCE] display ip routing-table vpn-instance vpn2
```

Routing Tables: vpn2

```
Destinations : 5          Routes : 5
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
10.100.20.0/24	Direct	0	0	10.100.20.1	Vlan3
10.100.20.1/32	Direct	0	0	127.0.0.1	InLoop0
172.16.20.0/24	OSPF	10	1	10.100.20.2	Vlan3

(4) MCE 与 PE1 之间的路由配置

- 在 MCE 上的配置

MCE 使用 Ethernet1/0/3 端口连接到 PE1 的 Ethernet1/0/18 端口，需要配置这个端口为 Trunk 端口，并允许 VLAN2 和 VLAN3 的报文携带 Tag 通过。

```
[MCE] interface Ethernet 1/0/3
[MCE-Ethernet1/0/3] port link-type trunk
[MCE-Ethernet1/0/3] port trunk permit vlan 2 3
```

配置 MCE 启动 BGP 进程 100。

```
[MCE] bgp 100
[MCE-bgp]
```

进入 VPN1 实例的 IPv4 地址族视图。

```
[MCE-bgp] ipv4-family vpn-instance vpn1
[MCE-bgp-vpn1]
```

指定 PE1（假设与 VPN1 绑定的接口地址为 10.100.10.3，BGP 进程为 200）为 EBGP 对等体，并引入 OSPF 进程 10 的路由信息。

```
[MCE-bgp-vpn1] peer 10.100.10.3 as-number 200
[MCE-bgp-vpn1] import-route ospf 10
[MCE-bgp-vpn1] quit
```

进入 VPN2 实例的 IPv4 地址族视图，指定 PE1（假设与 VPN2 绑定的接口地址为 10.100.20.3，BGP 进程为 200）为 EBGP 对等体，并引入 OSPF 进程 20 的路由信息。

```
[MCE-bgp] ipv4-family vpn-instance vpn2
[MCE-bgp-vpn2] peer 10.100.20.3 as-number 200
[MCE-bgp-vpn2] import-route ospf 20
```

- 在 PE1 上的配置

配置 PE1 的 Ethernet1/0/18 端口允许 VLAN2 和 VLAN3 的报文通过。

```
<PE1> system-view
[PE1] interface Ethernet1/0/18
[PE1-Ethernet1/0/18] port link-type trunk
[PE1-Ethernet1/0/18] port trunk permit vlan 2 3
```

配置 PE1 的 Vlan-interface2 和 Vlan-interface3 接口的 IP 地址分别为 10.100.10.3 和 10.100.20.3，并分别与 VPN1 和 VPN2 实例进行绑定，配置步骤这里省略。

在 PE1 上配置 BGP200，并在两个 VPN 实例的 IPv4 地址族视图中分别指定 MCE 为 EBGP 对等体。

```
[PE1] bgp 200
[PE1-bgp] ipv4-family vpn-instance vpn1
[PE1-bgp-vpn1] peer 10.100.10.1 as-number 100
[PE1-bgp-vpn1] quit
[PE1-bgp] ipv4-family vpn-instance vpn2
[PE1-bgp-vpn2] peer 10.100.20.1 as-number 100
[PE1-bgp-vpn2] return
```

显示 PE1 上 VPN1 实例的路由信息。

```
<PE1> display ip routing-table vpn-instance vpn1
```

```
Routing Tables: vpn1
```

```
Destinations : 5          Routes : 5
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
10.100.10.0/24	Direct	0	0	10.100.10.3	Vlan2
10.100.10.3/32	Direct	0	0	127.0.0.1	InLoop0
172.16.10.0/24	BGP	255	2	10.100.10.2	Vlan2

显示 PE1 上 VPN2 实例的路由信息。

```
<PE1> display ip routing-table vpn-instance vpn2
```

```
Routing Tables: vpn2
```

```
Destinations : 5          Routes : 5
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
10.100.20.0/24	Direct	0	0	10.100.20.3	Vlan3
10.100.20.3/32	Direct	0	0	127.0.0.1	InLoop0
172.16.20.0/24	BGP	255	2	10.100.20.2	Vlan3

至此，MCE 设备已经将两个 VPN 实例内的 OSPF 路由全部引入 PE 的 EBGP 路由表中，配置完成。

1.2.5 完整配置

```
#
```

```

ip vpn-instance vpn1
 route-distinguisher 10:1
 vpn-target 10:1 export-extcommunity
 vpn-target 10:1 import-extcommunity
#
ip vpn-instance vpn2
 route-distinguisher 20:1
 vpn-target 20:1 export-extcommunity
 vpn-target 20:1 import-extcommunity
#
vlan 1
#
vlan 10
#
vlan 20
#
interface LoopBack0
 ip address 101.10.10.1 255.255.255.255
#
interface Vlan-interface10
 ip binding vpn-instance vpn1
 ip address 10.100.10.1 255.255.255.0
#
interface Vlan-interface20
 ip binding vpn-instance vpn2
 ip address 10.100.20.1 255.255.255.0
#
interface Ethernet1/0/10
 port access vlan 10
#
interface Ethernet1/0/20
 port access vlan 20
#
interface GigabitEthernet1/1/1
 port link-type trunk
 port trunk permit vlan 1 10 20
#
bgp 100
 undo synchronization
 ipv4-family vpn-instance vpn1
 peer 10.100.10.3 as-number 200
 import-route ospf 10
#
 ipv4-family vpn-instance vpn2
 peer 10.100.10.3 as-number 200
 import-route ospf 20
#
ospf 10 router-id 10.10.10.1 vpn-instance vpn1

```

```
vpn-instance-capability simple
area 0.0.0.0
network 10.100.10.0 0.0.0.255
import-route bgp
#
ospf 10 router-id 10.10.20.1 vpn-instance vpn2
vpn-instance-capability simple
area 0.0.0.0
network 10.100.20.0 0.0.0.255
import-route bgp
```

1.2.6 配置注意事项

在 MCE 上为指定 VPN 实例配置的 VPN Target 必须与 PE 上为该 VPN 实例配置的 VPN Target 值一致。

目 录

1 PoE典型配置指导	1-1
1.1 PoE简介	1-1
1.2 集中式设备PoE典型配置指导.....	1-1
1.2.1 组网图	1-1
1.2.2 应用要求	1-1
1.2.3 适用产品、版本	1-1
1.2.4 配置过程和解释	1-2
1.2.5 完整配置	1-2
1.2.6 配置注意事项	1-3
1.3 分布式设备PoE典型配置指导.....	1-3
1.3.1 组网图	1-3
1.3.2 应用要求	1-3
1.3.3 适用产品、版本	1-3
1.3.4 配置过程和解释	1-3
1.3.5 完整配置	1-4
1.3.6 配置注意事项	1-4

1 PoE 典型配置指导

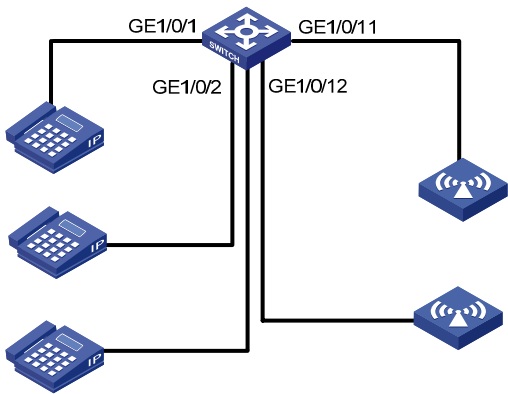
1.1 PoE 简介

PoE（Power over Ethernet，以太网供电，又称远程供电）是指设备通过以太网接口，利用双绞线对外接 PD（Powered Device，受电设备）设备（如 IP 电话、无线 AP、网络摄像头等）进行远程供电。

1.2 集中式设备 PoE 典型配置指导

1.2.1 组网图

图1-1 PoE 组网图



1.2.2 应用要求

交换机通过 PoE 接口为 PD 设备供电。

- GigabitEthernet1/0/1 与 GigabitEthernet1/0/2 接入 IP 电话。
- GigabitEthernet1/0/11 与 GigabitEthernet1/0/12 接入 AP 设备。
- GigabitEthernet1/0/2 的供电优先级为 critical，要求在新接入 PD 导致 PSE 功率过载时，停止对新接 PD 入供电（即采用 PD 功率管理的缺省策略）。
- GigabitEthernet1/0/11 下接的 AP 设备的功率不能超过 9000 毫瓦。

1.2.3 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S5500-SI 系列以太网交换机	Release 1207 软件版本	S5500-SI 系列 PoE 机型
S5500-EI 系列以太网交换机	Release 2102 软件版本	S5500-EI 系列 PoE 机型

1.2.4 配置过程和解释

使能 PoE 接口 GigabitEthernet1/0/1、GigabitEthernet1/0/2、GigabitEthernet1/0/11 和 GigabitEthernet1/0/12 远程供电功能。

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] poe enable
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] interface GigabitEthernet 1/0/2
[Sysname-GigabitEthernet1/0/2] poe enable
[Sysname-GigabitEthernet1/0/2] quit
[Sysname] interface GigabitEthernet 1/0/11
[Sysname-GigabitEthernet1/0/11] poe enable
[Sysname-GigabitEthernet1/0/11] quit
[Sysname] interface GigabitEthernet 1/0/12
[Sysname-GigabitEthernet1/0/12] poe enable
[Sysname-GigabitEthernet1/0/12] return
```

配置 GigabitEthernet1/0/2 对外供电的优先级为 critical。

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/2
[Sysname-GigabitEthernet1/0/2] poe priority critical
[Sysname-GigabitEthernet1/0/2] quit
```

配置 PoE 接口 GigabitEthernet1/0/11 的最大供电功率为 9000 毫瓦。

```
[Sysname] interface GigabitEthernet 1/0/11
[Sysname-GigabitEthernet1/0/11] poe max-power 9000
[Sysname-GigabitEthernet1/0/11] quit
```

配置完成后，IP 电话和 AP 设备被供电，能够正常工作。

1.2.5 完整配置

```
#
interface GigabitEthernet1/0/1
  poe enable
#
interface GigabitEthernet1/0/2
  poe enable
  poe priority critical
#
interface GigabitEthernet1/0/11
  poe enable
  poe max-power 9000
#
interface GigabitEthernet1/0/12
  poe enable
#
```

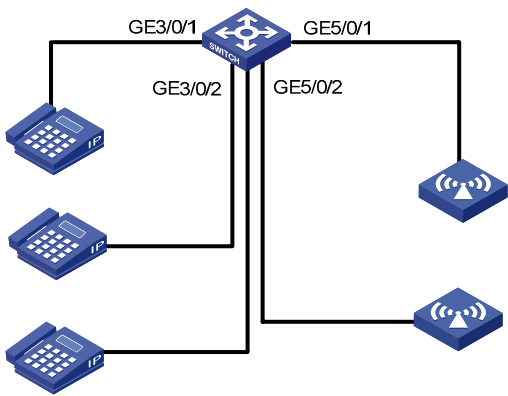
1.2.6 配置注意事项

无

1.3 分布式设备 PoE 典型配置指导

1.3.1 组网图

图1-2 PoE 组网图



1.3.2 应用要求

交换机通过 PoE 接口为 PD 设备供电。

- 设备有两块支持 PoE 远程供电的单板，分别插在第 3 和第 5 号槽位，PSE ID 分别为 10 和 16。
- 给 PSE 10 分配 400 瓦功率，假设 PSE 16 的 PSE 最大功率的缺省值可以满足需求。
- GigabitEthernet3/0/1 与 GigabitEthernet3/0/2 接入 IP 电话。
- GigabitEthernet5/0/1 与 GigabitEthernet5/0/2 接入 AP 设备。
- GigabitEthernet3/0/2 的供电优先级为 critical，要求在新接入 PD 导致 PSE 功率过载时，停止对新接 PD 入供电（即采用 PD 功率管理的缺省策略）。
- GigabitEthernet5/0/1 下接的 AP 设备的功率不能超过 9000 毫瓦。

1.3.3 适用产品、版本

表1-2 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S7500E 系列以太网交换机	Release 6100, Release 6300 软件版本	S7500E 系列硬件版本（配置支持 PoE 功能业务板）

1.3.4 配置过程和解释

使能 PSE 的远程供电功能。

```
<Sysname> system-view
```

```
[Sysname] poe enable pse 10
```

```
[Sysname] poe enable pse 16
```

配置 PSE 10 最大功率为 400 瓦。

```
[Sysname] poe max-power 400 pse 10
```

使能 PoE 接口 GigabitEthernet3/0/1、GigabitEthernet3/0/2、GigabitEthernet5/0/1 和 GigabitEthernet5/0/2 远程供电功能。

```
[Sysname] interface gigabitethernet 3/0/1
[Sysname-GigabitEthernet3/0/1] poe enable
[Sysname-GigabitEthernet3/0/1] quit
[Sysname] interface gigabitethernet 3/0/2
[Sysname-GigabitEthernet3/0/2] poe enable
[Sysname-GigabitEthernet3/0/2] quit
[Sysname] interface gigabitethernet 5/0/1
[Sysname-GigabitEthernet5/0/1] poe enable
[Sysname-GigabitEthernet5/0/1] quit
[Sysname] interface gigabitethernet 5/0/2
[Sysname-GigabitEthernet5/0/2] poe enable
[Sysname-GigabitEthernet5/0/2] quit
```

配置 GigabitEthernet3/0/2 对外供电的优先级为 critical。

```
[Sysname] interface gigabitethernet 3/0/2
[Sysname-GigabitEthernet3/0/2] poe priority critical
[Sysname-GigabitEthernet3/0/2] quit
```

配置 PoE 接口 GigabitEthernet5/0/1 的最大供电功率为 9000 毫瓦。

```
[Sysname] interface gigabitethernet 5/0/1
[Sysname-GigabitEthernet5/0/1] poe max-power 9000
```

配置完成后，IP 电话和 AP 设备被供电，能够正常工作。

1.3.5 完整配置

```
#
poe max-power 400 pse 10
poe enable pse 10
poe enable pse 16
#
interface GigabitEthernet3/0/1
poe enable
#
interface GigabitEthernet3/0/2
poe enable
poe priority critical
#
interface GigabitEthernet5/0/1
poe enable
poe max-power 9000
#
interface GigabitEthernet5/0/2
poe enable
```

1.3.6 配置注意事项

S7500E 系列交换机都具有 PoE 供电功能，其中 S7502E 是通过机箱背面的 PoE 电源输入端与外置 PoE 供电设备相连实现 PoE 电源输入；而除 S7502E 以外的交换机是通过具有 PoE 功能的电源

模块（如 PSR1400-D 和 PSR2800-ACV）提供 PoE 电源输入的，不需要连接外置 PoE 供电设备，详细介绍可参考《H3C S7500E 系列以太网交换机 安装手册》。

目 录

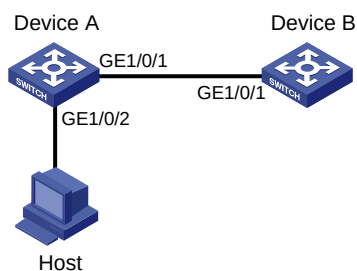
- 1 OAM典型配置指导..... 1-1
 - 1.1 OAM典型配置指导 1-1
 - 1.1.1 组网图..... 1-1
 - 1.1.2 应用要求 1-1
 - 1.1.3 适用产品、版本 1-1
 - 1.1.4 配置过程和解释 1-1
 - 1.1.5 完整配置 1-2
 - 1.1.6 配置注意事项 1-3

1 OAM 典型配置指导

1.1 OAM 典型配置指导

1.1.1 组网图

图1-1 OAM 组网示意图



1.1.2 应用要求

- 在设备 Device A 和 Device B 上配置以太网 OAM 协议，对二层数据链路层进行管理；
- 验证链路的性能，测试用户 Host 接入的设备 Device A 收到错误帧的情况。

1.1.3 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6300 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.1.4 配置过程和解释

- 配置 Device A

配置端口 GigabitEthernet1/0/1 的以太网 OAM 工作模式为 passive 模式，并使能以太网 OAM 功能。

```
<DeviceA> system-view
[DeviceA] interface GigabitEthernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] oam mode passive
[DeviceA-GigabitEthernet1/0/1] oam enable
[DeviceA-GigabitEthernet1/0/1] quit
```

配置错误帧事件周期为 20 秒。

```
[DeviceA] oam errored-frame period 20
```

配置错误帧事件阈值为 10。

```
[DeviceA] oam errored-frame threshold 10
```

显示以太网 OAM 全局配置信息。

```
[DeviceA] display oam configuration
```

Configuration of the errored symbol/frame event window/threshold :

```
-----
Errored-symbol Event period      : 1
Errored-symbol Event threshold   : 1
Errored-frame Event period       : 20
Errored-frame Event threshold    : 10
Errored-frame-period Event period : 1000
Errored-frame-period Event threshold : 1
Errored-frame-seconds Event period : 60
Errored-frame-seconds Event threshold : 1
```

- 配置 Device B

配置端口 GigabitEthernet1/0/1 的以太网 OAM 工作模式为缺省模式 active，并使能以太网 OAM 功能。

```
<DeviceB> system-view
```

```
[DeviceB] interface GigabitEthernet 1/0/1
```

```
[DeviceB-GigabitEthernet1/0/1] oam enable
```

```
[DeviceB-GigabitEthernet1/0/1] quit
```

显示一般链路事件统计信息。

```
[DeviceB] display oam link-event remote
```

```
Port :GigabitEthernet1/0/1
```

```
Link Status :Up
```

```
OAMRemoteErrFrameEvent : (ms = milliseconds)
```

```
-----
Event Time Stamp      : 5789      Errored FrameWindow : 10(100ms)
Errored Frame Threshold : 1      Errored Frame       : 3
Error Running Total   : 35      Event Running Total : 17
```

上面的显示信息表明从 Device A 连接建立后，总共发生了 35 次错误，其中错误帧事件有 17 次，链路的性能不稳定。

1.1.5 完整配置

- DeviceA 的配置

```
#
```

```
oam errored-frame period 20
```

```
oam errored-frame threshold 10
```

```
#
```

```
interface GigabitEthernet1/0/1
```

```
oam mode passive
```

```
oam enable
```

- DeviceB 的配置

```
#
```

```
interface GigabitEthernet1/0/1
```

1.1.6 配置注意事项

- 以太网 OAM 连接只能由 **active** 模式的以太网 OAM 实体发起,而 **passive** 模式的以太网 OAM 实体只能等待对端以太网 OAM 实体的连接请求;两个 **passive** 模式的以太网 OAM 实体之间是无法建立以太网 OAM 连接的。
- 当以太网 OAM 功能使能后,不能更改以太网 OAM 的工作模式。如果需要更改工作模式,需先将以太网 OAM 功能关闭,再更改工作模式。

目 录

1 连通错误检测典型配置指导 1-1

 1.1 连通错误检测典型配置指导 1-1

 1.1.1 组网图 1-1

 1.1.2 应用要求 1-1

 1.1.3 适用产品、版本 1-1

 1.1.4 配置过程和解释 1-1

 1.1.5 完整配置 1-4

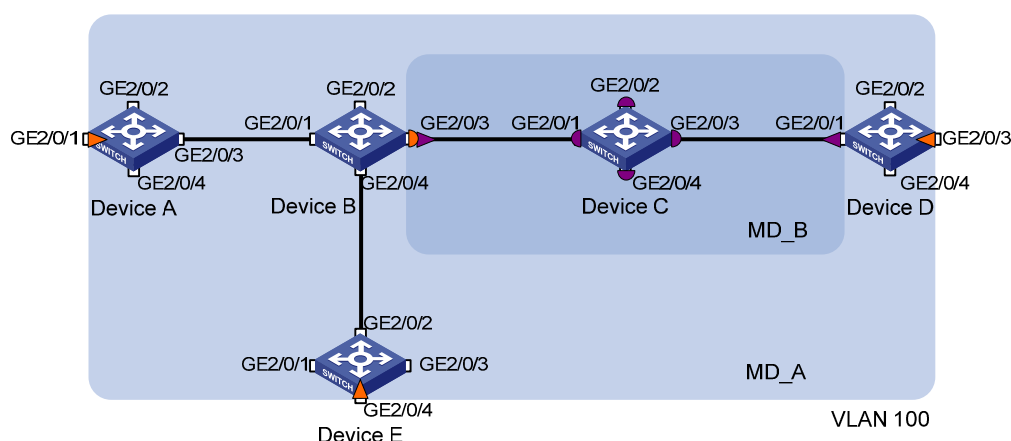
 1.1.6 配置注意事项 1-6

1 连通错误检测典型配置指导

1.1 连通错误检测典型配置指导

1.1.1 组网图

图1-1 连通错误检测组网示意图



1.1.2 应用要求

- 在该网络中规划两个域：MD_A（浅蓝色域）和 MD_B（深蓝色域），级别分别为 5 和 3。确定每个域的边界端口，确定每个端口所属的域。每个维护域中维护集的 VLAN ID 均为 100。
- 对每一个维护域，查找所有的边界端口；对每一个边界端口，根据维护域的位置确定配置在它上面的维护端点的方向；为每一个维护端点确定一个维护集内唯一的 ID；确定每个维护端点所要检测的远端维护端点，并使能这些维护端点。
- 确认需要配置维护中间点的设备。选择合适的维护中间点规则。
- 通过 CC（Continuity Check，连续性检测功能）功能检测到链路出现故障后，可以使用 LB（Loopback，环回功能）功能进行故障定位。
- 通过 CC 功能获取整个组网的状态后，使用 LT（Linktrace，链路跟踪功能）功能进行路径查找或故障定位。

1.1.3 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S7500E 系列以太网交换机	Release 6300 软件版本	全系列硬件版本

1.1.4 配置过程和解释

1. 配置服务实例

根据组网图中每台设备上的端点所属的域，共需要完成以下配置：

- 在 Device A 和 Device E 上配置维护域 MD_A，级别为 5
- 在 Device C 上配置维护域 MD_B，级别为 3
- 在 Device B 和 Device D 上配置维护域 MD_A 和 MD_B 及相应级别
- 在每个维护域内配置一个维护集
- 为每个维护集创建一个服务实例

(1) Device A 的配置（Device E 的配置和 Device A 相同）

```
<DeviceA> system-view
[DeviceA] cfd enable
[DeviceA] cfd md MD_A level 5
[DeviceA] cfd ma MA_MD_A md MD_A vlan 100
[DeviceA] cfd service-instance 1 md MD_A ma MA_MD_A
```

(2) Device C 的配置

```
<DeviceC> system-view
[DeviceC] cfd enable
[DeviceC] cfd md MD_B level 3
[DeviceC] cfd ma MA_MD_B md MD_B vlan 100
[DeviceC] cfd service-instance 2 md MD_B ma MA_MD_B
```

(3) Device B 的配置（Device D 的配置和 Device B 相同）

```
<DeviceB> system-view
[DeviceB] cfd enable
[DeviceB] cfd md MD_A level 5
[DeviceB] cfd ma MA_MD_A md MD_A vlan 100
[DeviceB] cfd service-instance 1 md MD_A ma MA_MD_A
[DeviceB] cfd md MD_B level 3
[DeviceB] cfd ma MA_MD_B md MD_B vlan 100
[DeviceB] cfd service-instance 2 md MD_B ma MA_MD_B
```

2. 配置维护端点并启用维护端点的 CC 功能

- 在维护域 MD_A 中，边界端口有三个：Device A 上的 GigabitEthernet2/0/1，Device D 上的 GigabitEthernet2/0/3 和 Device E 上的 GigabitEthernet2/0/4，分别在这三个端口上配置内向的维护端点。
- 在维护域 MD_B 中，有两个边界端口：Device B 上的 GigabitEthernet2/0/3 和 Device D 上的 GigabitEthernet2/0/1，分别在这两个端口上配置外向的维护端点。
- 在维护域 MD_A 和 MD_B 中，每个维护端点都检测其他维护端点的报文。维护端点的 ID 分配如表 1-2 所示。

表1-2 维护端口 ID 分配表

设备	端口	ID
DeviceA	GigabitEthernet2/0/1	1001
DeviceB	GigabitEthernet2/0/3	2001
DeviceD	GigabitEthernet2/0/1	4001
	GigabitEthernet2/0/3	4002
DeviceE	GigabitEthernet2/0/4	5001

(2) Device A 的配置

配置 GigabitEthernet2/0/1 端口的 ID, 并配置其检测 Device D 上的 GigabitEthernet2/0/3 和 Device E 上的 GigabitEthernet2/0/4 端口的报文。

```
<DeviceA> system-view
[DeviceA] interface GigabitEthernet 2/0/1
[DeviceA-GigabitEthernet2/0/1] cfd mep 1001 service-instance 1 inbound
[DeviceA-GigabitEthernet2/0/1] cfd remote-mep 5001 service-instance 1 mep 1001
[DeviceA-GigabitEthernet2/0/1] cfd remote-mep 4002 service-instance 1 mep 1001
[DeviceA-GigabitEthernet2/0/1] cfd mep service-instance 1 mep 1001 enable
[DeviceA-GigabitEthernet2/0/1] cfd cc service-instance 1 mep 1001 enable
```

(3) Device B 的配置

配置 GigabitEthernet2/0/3 端口的 ID, 并配置其检测 Device D 上的 GigabitEthernet2/0/1 端口的报文。

```
<DeviceB> system-view
[DeviceB] interface GigabitEthernet 2/0/3
[DeviceB-GigabitEthernet2/0/3] cfd mep 2001 service-instance 2 outbound
[DeviceB-GigabitEthernet2/0/3] cfd remote-mep 4001 service-instance 2 mep 2001
[DeviceB-GigabitEthernet2/0/3] cfd mep service-instance 2 mep 2001 enable
[DeviceB-GigabitEthernet2/0/3] cfd cc service-instance 2 mep 2001 enable
```

(4) Device D 的配置

配置 GigabitEthernet2/0/1 端口的 ID, 并配置其检测 Device B 上的 GigabitEthernet2/0/3 端口的报文。

```
<DeviceD> system-view
[DeviceD] interface GigabitEthernet 2/0/1
[DeviceD-GigabitEthernet2/0/1] cfd mep 4001 service-instance 2 outbound
[DeviceD-GigabitEthernet2/0/1] cfd remote-mep 2001 service-instance 2 mep 4001
[DeviceD-GigabitEthernet2/0/1] cfd mep service-instance 2 mep 4001 enable
[DeviceD-GigabitEthernet2/0/1] cfd cc service-instance 2 mep 4001 enable
```

配置 GigabitEthernet2/0/3 端口的 ID, 并配置其检测 Device A 上的 GigabitEthernet2/0/1 和 Device E 上的 GigabitEthernet2/0/4 端口的报文。

```
[DeviceD-GigabitEthernet2/0/1] interface GigabitEthernet 2/0/3
[DeviceD-GigabitEthernet2/0/3] cfd mep 4002 service-instance 1 inbound
[DeviceD-GigabitEthernet2/0/3] cfd remote-mep 1001 service-instance 1 mep 4002
[DeviceD-GigabitEthernet2/0/3] cfd remote-mep 5001 service-instance 1 mep 4002
[DeviceD-GigabitEthernet2/0/3] cfd mep service-instance 1 mep 4002 enable
[DeviceD-GigabitEthernet2/0/3] cfd cc service-instance 1 mep 4002 enable
```

(5) Device E 的配置

配置 GigabitEthernet2/0/4 端口的 ID, 并配置其检测 Device A 上的 GigabitEthernet2/0/1 和 Device D 上的 GigabitEthernet2/0/3 端口的报文。

```
<DeviceE> system-view
[DeviceE] interface GigabitEthernet 2/0/4
[DeviceE-GigabitEthernet2/0/4] cfd mep 5001 service-instance 1 inbound
```

```
[DeviceE-GigabitEthernet2/0/4] cfd remote-mep 1001 service-instance 1 mep 5001
[DeviceE-GigabitEthernet2/0/4] cfd remote-mep 4002 service-instance 1 mep 5001
[DeviceE-GigabitEthernet2/0/4] cfd mep service-instance 1 mep 5001 enable
[DeviceE-GigabitEthernet2/0/4] cfd cc service-instance 1 mep 5001 enable
```

3. 配置维护中间点生成规则

缺省情况下，设备上不配置维护中间点。如果在该维护域内的所有端口上都规划有维护中间点，则应选择 **default** 规则。如果仅在低层维护域有维护端点时规划维护中间点，则应选择 **explicit** 规则。

- 将维护域 MD_A 的维护中间点规划在 Device B 上，并且只在端口上有低层次维护端点时配置。即，在端口 GigabitEthernet2/0/3 上配置有 MD_B 域的维护端点，维护域 MD_A 中的维护中间点配置在此端口即可。根据上述规划，在设备 Device B 上配置维护域 MD_A 的维护中间点生成规则为 **explicit**。
- 将维护域 MD_B 的维护中间点规划在 Device C 上，并且在所有端口上均进行配置。根据上述规划确定，在设备 Device C 上配置维护域 MD_B 的维护中间点生成规则为 **default**。

(1) Device B 的配置

```
<DeviceB> system-view
[DeviceB] cfd mip-rule explicit service-instance 1
```

(2) Device C 的配置

```
<DeviceC> system-view
[DeviceC] cfd mip-rule default service-instance 2
```

4. 配置维护端点的 LB 功能

如图 1-1 所示，根据已配置的维护端点，在设备 Device A 上使用 LB 功能。由设备 Device A 发送 LBM 报文给设备 Device D 上的维护端点。

Device A 的配置。

```
<DeviceA> system-view
[DeviceA] cfd loopback service-instance 1 mep 1001 target-mep 4002
```

5. 配置维护端点的 LT 功能

如图 1-1 所示，根据已配置的维护端点，在设备 Device A 上使用 LT 功能。由设备 Device A 发送 LTM 报文给设备 Device D 上的维护端点。

Device A 的配置。

```
<DeviceA> system-view
[DeviceA] cfd linktrace service-instance 1 mep 1001 target-mep 4002
```

1.1.5 完整配置

- Device A 的完整配置

```
#
cfd enable
cfd md MD_A level 5
cfd ma MA_MD_A md MD_A vlan 100
cfd service-instance 1 md MD_A ma MA_MD_A
cfd linktrace service-instance 1 mep 1001 target-mep 4002
cfd loopback service-instance 1 mep 1001 target-mep 4002
```

```
#
interface GigabitEthernet2/0/1
 cfd mep 1001 service-instance 1 inbound
 cfd mep service-instance 1 mep 1001 enable
 cfd cc service-instance 1 mep 1001 enable
 cfd remote-mep 4002 service-instance 1 mep 1001
 cfd remote-mep 5001 service-instance 1 mep 1001
```

- Device B 的完整配置

```
#
 cfd enable
 cfd md MD_B level 3
 cfd ma MA_MD_B md MD_B vlan 100
 cfd service-instance 2 md MD_B ma MA_MD_B
 cfd md MD_A level 5
 cfd ma MA_MD_A md MD_A vlan 100
 cfd service-instance 1 md MD_A ma MA_MD_A
 cfd mip-rule explicit service-instance 1
```

```
#
interface GigabitEthernet2/0/3
 cfd mep 2001 service-instance 2 inbound
 cfd mep service-instance 2 mep 2001 enable
 cfd cc service-instance 2 mep 2001 enable
 cfd remote-mep 4001 service-instance 2 mep 2001
```

- Device C 的完整配置

```
#
 cfd enable
 cfd md MD_B level 3
 cfd ma MA_MD_B md MD_B vlan 100
 cfd service-instance 2 md MD_B ma MA_MD_B
 cfd mip-rule default service-instance 2
```

- Device D 的完整配置

```
#
 cfd enable
 cfd md MD_B level 3
 cfd ma MA_MD_B md MD_B vlan 100
 cfd service-instance 2 md MD_B ma MA_MD_B
 cfd md MD_A level 5
 cfd ma MA_MD_A md MD_A vlan 100
 cfd service-instance 1 md MD_A ma MA_MD_A

#
interface GigabitEthernet2/0/1
 cfd mep 4001 service-instance 2 outbound
 cfd mep service-instance 2 mep 4001 enable
 cfd cc service-instance 2 mep 4001 enable
 cfd remote-mep 2001 service-instance 2 mep 4001
```

```
#
```

```
#
```

```
interface GigabitEthernet2/0/3
 cfd mep 4002 service-instance 1 inbound
 cfd mep service-instance 1 mep 4002 enable
 cfd cc service-instance 1 mep 4002 enable
 cfd remote-mep 1001 service-instance 1 mep 4002
 cfd remote-mep 5001 service-instance 1 mep 4002
```

- Device E 的完整配置

```
#
 cfd enable
 cfd md MD_A level 5
 cfd ma MA_MD_A md MD_A vlan 100
 cfd service-instance 1 md MD_A ma MA_MD_A
#
interface GigabitEthernet2/0/4
 cfd mep 5001 service-instance 1 outbound
 cfd mep service-instance 1 mep 5001 enable
 cfd cc service-instance 1 mep 5001 enable
 cfd remote-mep 1001 service-instance 1 mep 5001
 cfd remote-mep 4002 service-instance 1 mep 5001
```

1.1.6 配置注意事项

创建维护域、创建维护集、创建服务实例这三个操作必须依次进行配置，顺序不可变更。

目 录

1 RRPP典型配置指导（不支持保护VLAN）	1-1
1.1 RRPP单环拓扑典型配置指导	1-1
1.1.1 组网图	1-1
1.1.2 应用要求	1-1
1.1.3 适用产品、版本	1-1
1.1.4 配置过程和解释	1-2
1.1.5 完整配置	1-3
1.1.6 配置注意事项	1-3
1.2 RRPP单域相交环拓扑典型配置指导	1-4
1.2.1 组网图	1-4
1.2.2 应用要求	1-4
1.2.3 适用产品、版本	1-5
1.2.4 配置过程和解释	1-5
1.2.5 完整配置	1-7
1.2.6 配置注意事项	1-9
1.3 RRPP多域相交环拓扑典型配置指导	1-9
1.3.1 组网图	1-9
1.3.2 应用要求	1-9
1.3.3 适用产品、版本	1-10
1.3.4 配置过程和解释	1-10
1.3.5 完整配置	1-13
1.3.6 配置注意事项	1-15
2 RRPP典型配置指导（支持保护VLAN）	2-1
2.1 RRPP单环拓扑典型配置指导	2-1
2.1.1 组网图	2-1
2.1.2 应用要求	2-1
2.1.3 适用产品、版本	2-2
2.1.4 配置过程和解释	2-2
2.1.5 完整配置	2-3
2.1.6 配置注意事项	2-3
2.2 RRPP相交环拓扑典型配置指导	2-5
2.2.1 组网图	2-5
2.2.2 应用要求	2-5
2.2.3 适用产品、版本	2-5
2.2.4 配置过程和解释	2-6
2.2.5 完整配置	2-8
2.2.6 配置注意事项	2-9
2.3 RRPP相交环负载分担拓扑典型配置指导	2-10
2.3.1 组网图	2-10
2.3.2 应用要求	2-11
2.3.3 适用产品、版本	2-11

2.3.4 配置过程和解释 2-11

2.3.5 完整配置 2-18

2.3.6 配置注意事项 2-23

1 RRPP 典型配置指导（不支持保护 VLAN）

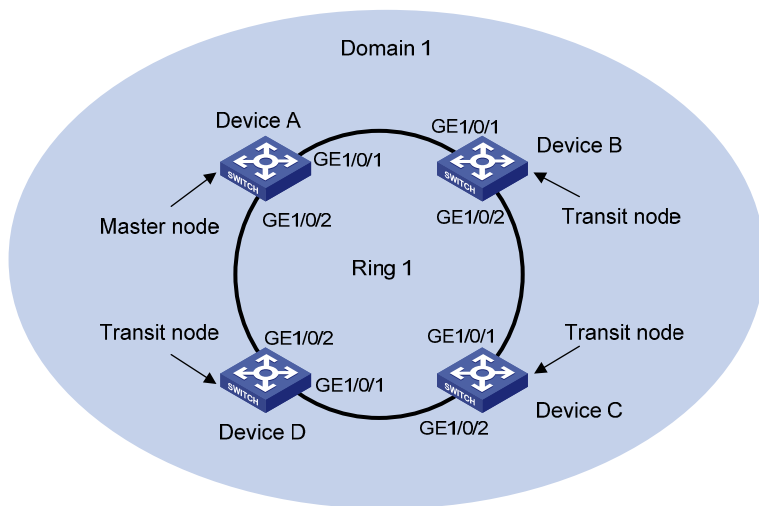
1.1 RRPP 单环拓扑典型配置指导

RRPP（Rapid Ring Protection Protocol，快速环网保护协议）是一个专门应用于以太网环的链路层协议。它在以太网环完整时能够防止数据环路引起的广播风暴，而当以太网环上一条链路断开时能迅速恢复环网上各个节点之间的通信通路。和 STP 协议相比，RRPP 协议有如下特点：

- 拓扑收敛速度快
- 拓扑收敛时间与环网上的节点数无关

1.1.1 组网图

图1-1 RRPP 单环拓扑组网示意图



1.1.2 应用要求

- Device A、Device B、Device C、Device D 构成 RRPP 域 1；
- RRPP 域 1 的控制 VLAN 为 VLAN 4092；
- Device A、Device B、Device C 和 Device D 构成主环 1；
- Device A 为主环的主节点，GigabitEthernet1/0/1 为主端口，GigabitEthernet1/0/2 为副端口；
- Device B、Device C 和 Device D 为主环的传输节点，各自的 GigabitEthernet1/0/1 为主端口，GigabitEthernet1/0/2 为副端口；
- 主环的定时器取缺省值。

1.1.3 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本

产品	软件版本	硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6100 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.1.4 配置过程和解释



说明

- 以下只列出了主节点 Device A 和传输节点 Device B 上的配置，Device C 和 Device D 上的配置与 Device B 相同。
- 接入 RRPP 环的端口已经配置为 Trunk 端口，并允许数据 VLAN 的报文通过。具体配置请参见本手册“以太网端口基本配置指导”部分的介绍。
- 接入 RRPP 环的端口已经关闭 STP 协议。

(1) Device A 上的配置

在 Device A 上创建 RRPP 域，并指定控制 VLAN。

```
<DeviceA> system-view
[DeviceA] rrpp domain 1
[DeviceA-rrpp-domain1] control-vlan 4092
```

指定 Device A 为 RRPP 主环主节点，同时指定 Device A 接入 RRPP 主环的主端口和副端口分别为 GigabitEthernet1/0/1、GigabitEthernet1/0/2。

```
[DeviceA-rrpp-domain1] ring 1 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
```

使能 RRPP 环。

```
[DeviceA-rrpp-domain1] ring 1 enable
[DeviceA-rrpp-domain1] quit
```

使能 RRPP 协议

```
[DeviceA] rrpp enable
```

(2) Device B 上的配置

在 Device B 上创建 RRPP 域，并指定控制 VLAN。注意与域内其它节点使用相同域 ID、相同控制 VLAN。

```
<DeviceB> system-view
[DeviceB] rrpp domain 1
[DeviceB-rrpp-domain1] control-vlan 4092
```

指定 Device B 为 RRPP 主环传输节点，同时指定 Device B 接入 RRPP 主环的主端口和副端口分别为 GigabitEthernet1/0/1、GigabitEthernet1/0/2。

```
[DeviceB-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
```

使能 RRPP 环。

```
[DeviceB-rrpp-domain1] ring 1 enable
```

```
[DeviceB-rrpp-domain1] quit
```

使能 RRPP 协议。

```
[DeviceB] rrpp enable
```

1.1.5 完整配置

- Device A 上的配置

```
#
```

```
rrpp domain 1
```

```
control-vlan 4092
```

```
ring 1 node-mode master primary-port GigabitEthernet1/0/1 secondary-port  
GigabitEthernet1/0/2 level 0
```

```
ring 1 enable
```

```
#
```

```
rrpp enable
```

```
#
```

- Device B 上的配置

```
#
```

```
rrpp domain 1
```

```
control-vlan 4092
```

```
ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port  
GigabitEthernet1/0/2 level 0
```

```
ring 1 enable
```

```
#
```

```
rrpp enable
```

```
#
```

1.1.6 配置注意事项

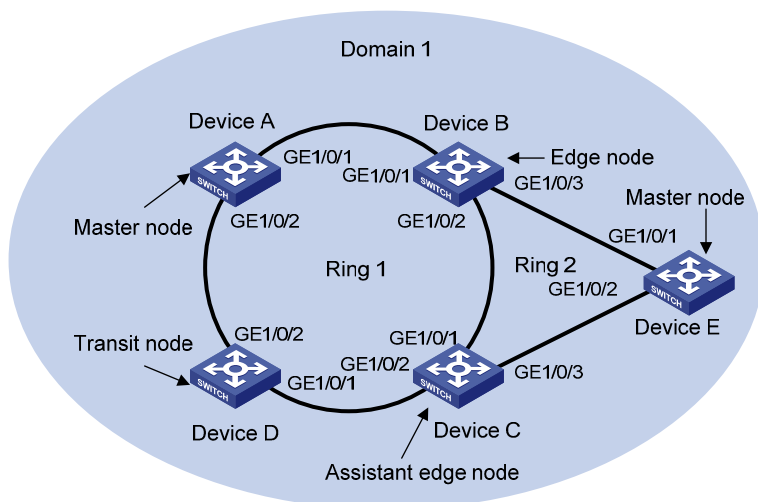
- RRPP 没有自动选举机制，因此只有为环网上的每个节点进行正确配置，才能让协议真正实现环网的检测和保护。请注意保证配置的正确性。
- 在配置 RRPP 功能之前，需要在物理上搭建以太网环形拓扑的组网环境。
- 在配置 RRPP 环之前必须先配置控制 VLAN。
- 为 RRPP 域配置的控制 VLAN 必须是设备上没有创建过的 VLAN。
- 用户可以配置主环的控制 VLAN，而子环的控制 VLAN 由系统自动分配，其 VLAN ID 为主环的控制 VLAN ID 加 1。因此，用户在配置控制 VLAN 时一定要选取两个连续的没有创建过的 VLAN。如果当前设备上没有两个连续的没有创建过的 VLAN，则配置失败。
- 每一个 RRPP 域都有唯一的控制 VLAN 和它绑定，控制 VLAN 的删除是在删除 RRPP 域的同时完成的，控制 VLAN 不能用 **undo vlan all** 命令删除。
- 控制 VLAN 不能被指定为远程镜像 VLAN 或 isolate-user-vlan。
- 控制 VLAN 上不能运行 QinQ 和 VLAN 映射功能，否则 RRPP 协议报文不能进行正常转发。
- 不要将接入 RRPP 环的端口的缺省 VLAN ID 设置为 RRPP 控制 VLAN ID，以免影响协议报文正常收发。

- RRPP 环的节点角色、端口角色和环的级别一经配置不能直接修改，如果用户想改变上述配置，必须先删除现有的配置。
- 使用 `undo rrpp domain` 命令删除 RRPP 域时，必须保证 RRPP 域内没有配置 RRPP 环，否则删除操作不能成功。
- 接入 RRPP 环的端口必须配置为 Trunk 端口，并允许数据 VLAN 的报文通过。
- 接入 RRPP 环的端口不能是聚合端口、业务环回口。
- 接入 RRPP 环的端口不能使能 STP、802.1x、MAC 地址认证、Voice VLAN、Smart Link 功能。
- 不建议在 RRPP 端口上启用 OAM 远端环回功能，否则可能引起短时间的广播风暴。
- 建议接入 RRPP 环的端口使能链路状态快速上报功能（端口的 `link-delay` 设置为 0），以提高 RRPP 的拓扑变化收敛速度。
- 如果用户想在一个没有配置 RRPP 功能的设备上透传 RRPP 协议报文，需保证该设备上只有接入 RRPP 环的两个端口允许所在 RRPP 环对应的控制 VLAN 的报文通过，而其他端口不允许控制 VLAN 的报文通过。否则，其他 VLAN 的报文可能通过透传进入控制 VLAN，对 RRPP 环产生冲击。

1.2 RRPP 单域相交环拓扑典型配置指导

1.2.1 组网图

图1-2 RRPP 单域相交环拓扑组网示意图



1.2.2 应用要求

- Device A、Device B、Device C、Device D 和 Device E 构成 RRPP 域 1；
- RRPP 域 1 的控制 VLAN 为 VLAN 4092；
- Device A、Device B、Device C 和 Device D 构成主环 Ring 1；
- Device B、Device C 和 Device E 构成子环 Ring 2；
- Device A 为主环的主节点，GigabitEthernet1/0/1 为主端口，GigabitEthernet1/0/2 为副端口；
- Device E 为子环的主节点，GigabitEthernet1/0/1 为主端口，GigabitEthernet1/0/2 为副端口；

- Device B 为主环的传输节点和子环的边缘节点，GigabitEthernet1/0/2 为公共端口，GigabitEthernet1/0/3 为边缘端口；
- Device C 为主环的传输节点和子环的辅助边缘节点，GigabitEthernet1/0/1 为公共端口，GigabitEthernet1/0/3 为边缘端口；
- Device D 为主环的传输节点，GigabitEthernet1/0/1 为主端口，GigabitEthernet1/0/2 为副端口；
- 主环和子环的定时器都取缺省值。

1.2.3 适用产品、版本

表1-2 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6100 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.2.4 配置过程和解释



说明

- 接入 RRPP 环的端口已经配置为 Trunk 端口，并允许数据 VLAN 的报文通过。具体配置请参见本手册“以太网端口基本配置指导”部分的介绍。
- 接入 RRPP 环的端口已经关闭 STP 协议。

(1) Device A 上的配置

在 Device A 上创建 RRPP 域，并指定控制 VLAN。

```
<DeviceA> system-view
```

```
[DeviceA] rrpp domain 1
```

```
[DeviceA-rrpp-domain1] control-vlan 4092
```

指定 Device A 为 RRPP 主环主节点，同时指定 Device A 接入 RRPP 主环的主端口和副端口分别为 GigabitEthernet1/0/1、GigabitEthernet1/0/2。

```
[DeviceA-rrpp-domain1] ring 1 node-mode master primary-port gigabitethernet 1/0/1  
secondary-port gigabitethernet 1/0/2 level 0
```

使能 RRPP 环。

```
[DeviceA-rrpp-domain1] ring 1 enable
```

```
[DeviceA-rrpp-domain1] quit
```

使能 RRPP 协议

```
[DeviceA] rrpp enable
```

(2) Device B 上的配置

在 Device B 上创建 RRPP 域，并指定控制 VLAN。注意与域内其它节点使用相同域 ID、相同控制 VLAN。

```
<DeviceB> system-view
```

```
[DeviceB] rrpp domain 1
```

```
[DeviceB-rrpp-domain1] control-vlan 4092
```

指定 Device B 为 RRPP 主环传输节点，同时指定 Device B 接入 RRPP 主环的主端口和副端口分别为 GigabitEthernet1/0/1、GigabitEthernet1/0/2。

```
[DeviceB-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1  
secondary-port gigabitethernet 1/0/2 level 0
```

指定 Device B 为 RRPP 子环边缘节点，同时指定 Device B 接入 RRPP 子环的公共端口和边缘端口分别为 GigabitEthernet1/0/2、GigabitEthernet1/0/3。注意使用 **ring** 命令对边缘节点进行配置的时候，不需要配置 level 参数。

```
[DeviceB-rrpp-domain1] ring 2 node-mode edge common-port gigabitethernet 1/0/2 edge-port  
gigabitethernet 1/0/3
```

使能 RRPP 主环和 RRPP 子环。

```
[DeviceB-rrpp-domain1] ring 1 enable
```

```
[DeviceB-rrpp-domain1] ring 2 enable
```

```
[DeviceB-rrpp-domain1] quit
```

使能 RRPP 协议。

```
[DeviceB] rrpp enable
```

(3) Device C 上的配置

在 Device C 上创建 RRPP 域，并指定控制 VLAN。注意与域内其它节点使用相同域 ID、相同控制 VLAN。

```
<DeviceC> system-view
```

```
[DeviceC] rrpp domain 1
```

```
[DeviceC-rrpp-domain1] control-vlan 4092
```

指定 Device C 为 RRPP 主环传输节点，同时指定 Device C 接入 RRPP 主环的主端口和副端口分别为 GigabitEthernet1/0/1、GigabitEthernet1/0/2。

```
[DeviceC-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1  
secondary-port gigabitethernet 1/0/2 level 0
```

指定 Device C 为 RRPP 子环辅助边缘节点，同时指定 Device C 接入 RRPP 子环的公共端口和边缘端口分别为 GigabitEthernet1/0/1、GigabitEthernet1/0/3。注意使用 **ring** 命令对辅助边缘节点进行配置的时候，不需要配置 level 参数。

```
[DeviceC-rrpp-domain1] ring 2 node-mode assistant-edge common-port gigabitethernet 1/0/1  
edge-port gigabitethernet 1/0/3
```

使能 RRPP 主环和 RRPP 子环。

```
[DeviceC-rrpp-domain1] ring 1 enable
```

```
[DeviceC-rrpp-domain1] ring 2 enable
```

```
[DeviceC-rrpp-domain1] quit
```

使能 RRPP 协议。

```
[DeviceC] rrpp enable
```

(4) Device D 上的配置

在 Device D 上创建 RRPP 域，并指定控制 VLAN。注意与域内其它节点使用相同域 ID、相同控制 VLAN。

```
<DeviceD> system-view
```

```
[DeviceD] rrpp domain 1
```

```
[DeviceD-rrpp-domain1] control-vlan 4092
```

指定 Device D 为 RRPP 主环传输节点，同时指定 Device D 接入 RRPP 主环的主端口和副端口分别为 GigabitEthernet1/0/1、GigabitEthernet1/0/2。

```
[DeviceD-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1  
secondary-port gigabitethernet 1/0/2 level 0
```

使能 RRPP 环。

```
[DeviceD-rrpp-domain1] ring 1 enable
```

```
[DeviceD-rrpp-domain1] quit
```

使能 RRPP 协议。

```
[DeviceD] rrpp enable
```

(5) Device E 上的配置

在 Device E 上创建 RRPP 域，并指定控制 VLAN。注意与域内其它节点使用相同域 ID、相同控制 VLAN。

```
<DeviceE> system-view
```

```
[DeviceE] rrpp domain 1
```

```
[DeviceE-rrpp-domain1] control-vlan 4092
```

指定 Device E 为 RRPP 子环主节点，同时指定 Device E 接入 RRPP 子环的主端口和副端口分别为 GigabitEthernet1/0/1、GigabitEthernet1/0/2。

```
[DeviceE-rrpp-domain1] ring 2 node-mode master primary-port gigabitethernet 1/0/1  
secondary-port gigabitethernet 1/0/2 level 1
```

使能 RRPP 子环。

```
[DeviceE-rrpp-domain1] ring 2 enable
```

```
[DeviceE-rrpp-domain1] quit
```

使能 RRPP 协议。

```
[DeviceE] rrpp enable
```

1.2.5 完整配置

• Device A 上的配置

```
#
```

```
rrpp domain 1
```

```
control-vlan 4092
```

```
ring 1 node-mode master primary-port GigabitEthernet1/0/1 secondary-port  
GigabitEthernet1/0/2 level 0
```

```
ring 1 enable
```

```
#
```

```
rrpp enable
```


#

- Device B 上的配置

#

```
rrpp domain 1
```

```
control-vlan 4092
```

```
ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port  
GigabitEthernet1/0/2 level 0
```

```
ring 2 node-mode edge common-port GigabitEthernet1/0/2 edge-port GigabitEthernet1/0/3
```

```
ring 1 enable
```

```
ring 2 enable
```

#

```
rrpp enable
```

#

- Device C 上的配置

#

```
rrpp domain 1
```

```
control-vlan 4092
```

```
ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port  
GigabitEthernet1/0/2 level 0
```

```
ring 2 node-mode assistant-edge common-port GigabitEthernet1/0/1 edge-port  
GigabitEthernet1/0/3
```

```
ring 1 enable
```

```
ring 2 enable
```

#

```
rrpp enable
```

#

- Device D 上的配置

#

```
rrpp domain 1
```

```
control-vlan 4092
```

```
ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port  
GigabitEthernet1/0/2 level 0
```

```
ring 1 enable
```

#

```
rrpp enable
```

#

- Device E 上的配置

#

```
rrpp domain 1
```

```
control-vlan 4092
```

```
ring 2 node-mode master primary-port GigabitEthernet1/0/1 secondary-port  
GigabitEthernet1/0/2 level 1
```

```
ring 2 enable
```

#

```
rrpp enable
```

#

1.2.6 配置注意事项

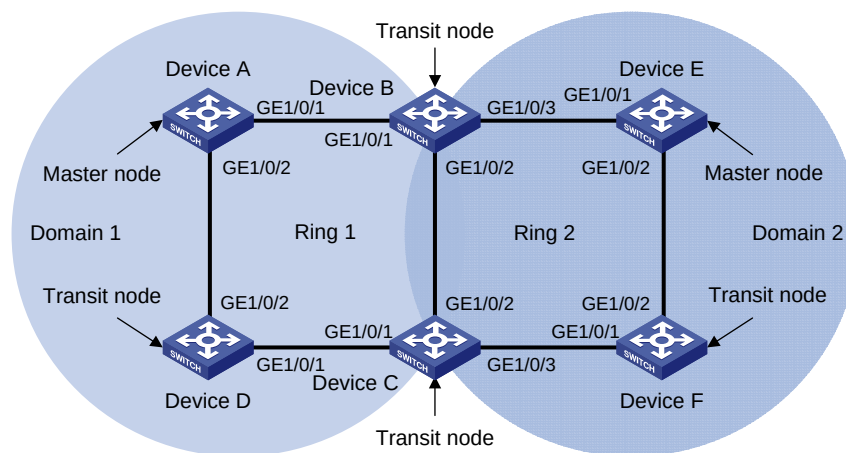
除 RRPP 单环拓扑典型配置举例中所列注意事项外，还需注意：

- 配置 RRPP 域时，最好先配置主环，再配置子环，并且在同一个 RRPP 域中，不同的 RRPP 环不能使用相同的 Ring ID。
- 如果一台设备在同一个 RRPP 域中的多个 RRPP 环上，则只能有一个主环，而且在其他子环上的节点角色只能是边缘节点或者辅助边缘节点。
- 使用 **ring** 命令对边缘节点或辅助边缘节点进行配置的时候，不需要配置 **level** 参数。
- 一台设备在所有 RRPP 域中配置的环的总数不能大于 16。
- 不要将接入 RRPP 环的端口的缺省 VLAN ID 设置为 RRPP 控制 VLAN ID 或者子控制 VLAN ID（子控制 VLAN ID 为主控制 VLAN ID 加 1），以免影响协议报文正常收发。
- 配置边缘节点和辅助边缘节点时，必须先进行主环配置，然后再进行子环配置。并且，在删除边缘节点的主环配置前，必须先删除所有的子环配置。但是，处于使能状态的 RRPP 环不能被删除。

1.3 RRPP 多域相交环拓扑典型配置指导

1.3.1 组网图

图1-3 RRPP 多域相交环拓扑组网示意图



1.3.2 应用要求

- Device A、Device B、Device C 和 Device D 构成 RRPP 域 1；Device E、Device F、Device C 和 Device B 构成 RRPP 域 2；
- RRPP 域 1 的控制 VLAN 为 VLAN 4090，RRPP 域 2 的控制 VLAN 为 VLAN 4092；
- Device A、Device B、Device C 和 Device D 构成主环 1；
- Device E、Device F、Device C 和 Device B 构成主环 2；
- 在 RRPP 域 1 的主环 1 上，Device A 为主环的主节点，GigabitEthernet1/0/1 为主端口，GigabitEthernet1/0/2 为副端口；
- 在 RRPP 域 2 的主环 2 上 Device E 为主环的主节点，GigabitEthernet1/0/1 为主端口，GigabitEthernet1/0/2 为副端口；

- Device B 为 RRPP 域 1 的主环 1 上的传输节点和 RRPP 域 2 的主环 2 上的传输节点，GigabitEthernet1/0/2 为多域相交公共端口；
- Device C 为 RRPP 域 1 的主环 1 上的传输节点和 RRPP 域 2 的主环 2 上的传输节点，GigabitEthernet1/0/2 为多域相交公共端口；
- Device D 为 RRPP 域 1 的主环 1 上的传输节点，GigabitEthernet1/0/1 为主端口，GigabitEthernet1/0/2 为副端口；
- Device F 为 RRPP 域 2 的主环 2 上的传输节点，GigabitEthernet1/0/1 为主端口，GigabitEthernet1/0/2 为副端口；
- 各域主环的定时器都取缺省值。

1.3.3 适用产品、版本

表1-3 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.3.4 配置过程和解释



说明

- 对于多域相交环，各域内环的配置是相互独立的，不同域内的数据 VLAN 必须相互隔离。
- 各域内接入 RRPP 环的端口已经配置为 Trunk 端口，并允许所在域数据 VLAN 的报文通过。具体配置请参见本手册“以太网端口基本配置指导”部分的介绍。
- 接入 RRPP 环的端口已经关闭 STP 协议。

(1) Device A 上的配置

在 Device A 上创建 RRPP 域 1，并指定控制 VLAN。

```
<DeviceA> system-view
```

```
[DeviceA] rrpp domain 1
```

```
[DeviceA-rrpp-domain1] control-vlan 4090
```

指定 Device A 为 RRPP 主环主节点，同时指定 Device A 接入 RRPP 主环的主端口和副端口分别为 GigabitEthernet1/0/1、GigabitEthernet1/0/2。

```
[DeviceA-rrpp-domain1] ring 1 node-mode master primary-port gigabitethernet 1/0/1  
secondary-port gigabitethernet 1/0/2 level 0
```

使能 RRPP 环。

```
[DeviceA-rrpp-domain1] ring 1 enable
```

```
[DeviceA-rrpp-domain1] quit
```

使能 RRPP 协议

```
[DeviceA] rrpp enable
```

(2) Device B 上的配置

在 Device B 上创建 RRPP 域 1，并指定控制 VLAN。注意与 Domain1 内其它节点使用相同域 ID、相同控制 VLAN。

```
<DeviceB> system-view
```

```
[DeviceB] rrpp domain 1
```

```
[DeviceB-rrpp-domain1] control-vlan 4090
```

指定 Device B 为 Domain1 RRPP 主环传输节点，同时指定 Device B 接入 RRPP 主环的主端口和副端口分别为 GigabitEthernet1/0/1、GigabitEthernet1/0/2。

```
[DeviceB-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1  
secondary-port gigabitethernet 1/0/2 level 0
```

使能 RRPP 环 1。

```
[DeviceB-rrpp-domain1] ring 1 enable
```

```
[DeviceB-rrpp-domain1] quit
```

在 Device B 上创建 RRPP 域 2，并指定控制 VLAN。注意与 Domain2 内其它节点使用相同域 ID、相同控制 VLAN。

```
[DeviceB] rrpp domain 2
```

```
[DeviceB-rrpp-domain2] control-vlan 4092
```

指定 Device B 为 Domain2 RRPP 主环传输节点，同时指定 Device B 接入 RRPP 主环的主端口和副端口分别为 GigabitEthernet1/0/2、GigabitEthernet1/0/3。

```
[DeviceB-rrpp-domain2] ring 2 node-mode transit primary-port gigabitethernet 1/0/2  
secondary-port gigabitethernet 1/0/3 level 0
```

使能 RRPP 环 2。

```
[DeviceB-rrpp-domain2] ring 2 enable
```

```
[DeviceB-rrpp-domain2] quit
```

使能 RRPP 协议。

```
[DeviceB] rrpp enable
```

(3) Device C 上的配置

在 Device C 上创建 RRPP 域 1，并指定控制 VLAN。注意与 Domain1 内其它节点使用相同域 ID、相同控制 VLAN。

```
<DeviceC> system-view
```

```
[DeviceC] rrpp domain 1
```

```
[DeviceC-rrpp-domain1] control-vlan 4090
```

指定 Device C 为 Domain1 RRPP 主环传输节点，同时指定 Device C 接入 RRPP 主环的主端口和副端口分别为 GigabitEthernet1/0/1、GigabitEthernet1/0/2。

```
[DeviceC-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1  
secondary-port gigabitethernet 1/0/2 level 0
```

使能 RRPP 环 1。

```
[DeviceC-rrpp-domain1] ring 1 enable
```

```
[DeviceC-rrpp-domain1] quit
```

在 Device C 上创建 RRPP 域 2，并指定控制 VLAN。注意与 Domain2 内其它节点使用相同域 ID、相同控制 VLAN。

```
[DeviceC] rrpp domain 2
```

```
[DeviceC-rrpp-domain2] control-vlan 4092
```

指定 Device C 为 Domain2 RRPP 主环传输节点，同时指定 Device C 接入 RRPP 主环的主端口和副端口分别为 GigabitEthernet1/0/3、GigabitEthernet1/0/2。

```
[DeviceC-rrpp-domain2] ring 2 node-mode transit primary-port gigabitethernet 1/0/3  
secondary-port gigabitethernet 1/0/2 level 0
```

使能 RRPP 环 2。

```
[DeviceC-rrpp-domain2] ring 2 enable
```

```
[DeviceC-rrpp-domain2] quit
```

使能 RRPP 协议。

```
[DeviceC] rrpp enable
```

(4) Device D 上的配置

在 Device D 上创建 RRPP 域 1，并指定控制 VLAN。注意与 Domain1 内其它节点使用相同域 ID、相同控制 VLAN。

```
<DeviceD> system-view
```

```
[DeviceD] rrpp domain 1
```

```
[DeviceD-rrpp-domain1] control-vlan 4090
```

指定 Device D 为 Domain1 RRPP 主环传输节点，同时指定 Device D 接入 RRPP 主环的主端口和副端口分别为 GigabitEthernet1/0/1、GigabitEthernet1/0/2。

```
[DeviceD-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1  
secondary-port gigabitethernet 1/0/2 level 0
```

使能 RRPP 环 1。

```
[DeviceD-rrpp-domain1] ring 1 enable
```

```
[DeviceD-rrpp-domain1] quit
```

使能 RRPP 协议。

```
[DeviceD] rrpp enable
```

(5) Device E 上的配置

在 Device E 上创建 RRPP 域 2，并指定控制 VLAN。注意与 Domain2 内其它节点使用相同域 ID、相同控制 VLAN。

```
<DeviceE> system-view
```

```
[DeviceE] rrpp domain 2
```

```
[DeviceE-rrpp-domain2] control-vlan 4092
```

指定 Device E 为 Domain2 RRPP 主环主节点，同时指定 Device E 接入 RRPP 主环的主端口和副端口分别为 GigabitEthernet1/0/1、GigabitEthernet1/0/2。

```
[DeviceE-rrpp-domain2] ring 2 node-mode master primary-port gigabitethernet 1/0/1  
secondary-port gigabitethernet 1/0/2 level 0
```

使能 RRPP 环 2。

```
[DeviceE-rrpp-domain2] ring 2 enable
```

```
[DeviceE-rrpp-domain2] quit
```

使能 RRPP 协议。

```
[DeviceE] rrpp enable
```

(6) Device F 上的配置

在 Device F 上创建 RRPP 域 2，并指定控制 VLAN。注意与 Domain2 内其它节点使用相同域 ID、相同控制 VLAN。

```
<DeviceF> system-view
```

```
[DeviceF] rrpp domain 2
```

```
[DeviceF-rrpp-domain2] control-vlan 4092
```

指定 Device F 为 Domain2 RRPP 主环传输节点，同时指定 Device F 接入 RRPP 主环的主端口和副端口分别为 GigabitEthernet1/0/1、GigabitEthernet1/0/2。

```
[DeviceF-rrpp-domain2] ring 2 node-mode transit primary-port gigabitethernet 1/0/1  
secondary-port gigabitethernet 1/0/2 level 0
```

使能 RRPP 环 2。

```
[DeviceF-rrpp-domain2] ring 2 enable
```

```
[DeviceF-rrpp-domain2] quit
```

使能 RRPP 协议。

```
[DeviceF] rrpp enable
```

1.3.5 完整配置

- Device A 上的配置

```
#
```

```
rrpp domain 1
```

```
control-vlan 4090
```

```
ring 1 node-mode master primary-port GigabitEthernet1/0/1 secondary-port  
GigabitEthernet1/0/2 level 0
```

```
ring 1 enable
```

```
#
```

```
rrpp enable
```

```
#
```

- Device B 上的配置

```
#
```

```
rrpp domain 1
```

```
control-vlan 4090
```

```
ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port  
GigabitEthernet1/0/2 level 0
```

```
ring 1 enable
```

```
#
```

```
rrpp domain 2
```

```
control-vlan 4092
```

```
ring 2 node-mode transit primary-port GigabitEthernet1/0/2 secondary-port  
GigabitEthernet1/0/3 level 0
```

```
ring 2 enable
```

```
#
```

```
rrpp enable
```

#

- Device C 上的配置

#

```
rrpp domain 1
```

```
control-vlan 4090
```

```
ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port  
GigabitEthernet1/0/2 level 0
```

```
ring 1 enable
```

#

```
rrpp domain 2
```

```
control-vlan 4092
```

```
ring 2 node-mode transit primary-port GigabitEthernet1/0/3 secondary-port  
GigabitEthernet1/0/2 level 0
```

```
ring 2 enable
```

#

```
rrpp enable
```

#

- Device D 上的配置

#

```
rrpp domain 1
```

```
control-vlan 4090
```

```
ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port  
GigabitEthernet1/0/2 level 0
```

```
ring 1 enable
```

#

```
rrpp enable
```

#

- Device E 上的配置

#

```
rrpp domain 2
```

```
control-vlan 4092
```

```
ring 2 node-mode master primary-port GigabitEthernet1/0/1 secondary-port  
GigabitEthernet1/0/2 level 0
```

```
ring 2 enable
```

#

```
rrpp enable
```

#

- Device F 上的配置

#

```
rrpp domain 2
```

```
control-vlan 4092
```

```
ring 2 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port  
GigabitEthernet1/0/2 level 0
```

```
ring 2 enable
```

#

```
rrpp enable
```

#

1.3.6 配置注意事项

除 RRPP 单域拓扑典型配置举例中所列注意事项外，还需注意：

- 多域相交环必须是主环相交，即不可以把子环节点上的端口配置为多域相交公共端口。
- 主节点副端口处于阻塞状态，不能配置为多域相交公共端口。
- 不可以把同一节点接入同一 RRPP 环的两个端口同时配置为多域相交公共端口。
- 在配置多域相交环时，不可以在 RRPP 协议全局使能的情况下使能或关闭多域相交公共端口所在的 RRPP 环。
- 在配置多域相交环时，各域内环的配置是相互独立的，不同域内的数据 VLAN 必须相互隔离。

2 RRPP 典型配置指导（支持保护 VLAN）



说明

为了兼容不支持保护 VLAN 配置的 RRPP 版本，在使用旧版本配置文件启动设备后，RRPP 域保护所有的 VLAN。

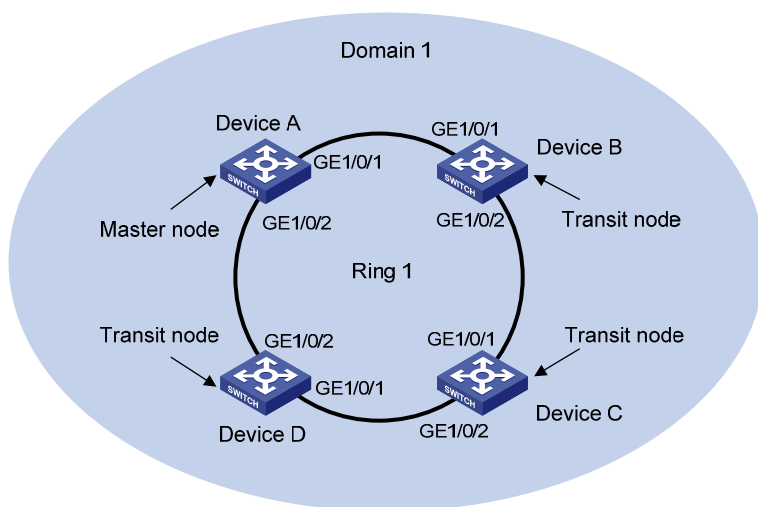
2.1 RRPP 单环拓扑典型配置指导

RRPP（Rapid Ring Protection Protocol，快速环网保护协议）是一个专门应用于以太网环的链路层协议。它在以太网环完整时能够防止数据环路引起的广播风暴，而当以太网环上一条链路断开时能迅速恢复环网上各个节点之间的通信通路。和 STP 协议相比，RRPP 协议有如下特点：

- 拓扑收敛速度快
- 拓扑收敛时间与环网上的节点数无关

2.1.1 组网图

图2-1 RRPP 单环拓扑组网示意图



2.1.2 应用要求

- Device A、Device B、Device C、Device D 构成 RRPP 域 1；
- RRPP 域 1 的控制 VLAN 为 VLAN 4092；
- RRPP 域 1 保护所有 VLAN；
- Device A、Device B、Device C 和 Device D 构成主环 1；
- Device A 为主环的主节点，GigabitEthernet1/0/1 为主端口，GigabitEthernet1/0/2 为副端口；
- Device B、Device C 和 Device D 为主环的传输节点，各自的 GigabitEthernet1/0/1 为主端口，GigabitEthernet1/0/2 为副端口；
- 主环的定时器取缺省值。

2.1.3 适用产品、版本

表2-1 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S7500E 系列以太网交换机	Release 6300 软件版本	全系列硬件版本

2.1.4 配置过程和解释



说明

- 以下只列出了主节点 Device A 和传输节点 Device B 上的配置，Device C 和 Device D 上的配置与 Device B 相同。
- 接入 RRPP 环的端口已经配置为 Trunk 端口，并允许数据 VLAN 的报文通过。具体配置请参见本手册“以太网端口基本配置指导”部分的介绍。
- 接入 RRPP 环的端口已经关闭 STP 协议。

(1) Device A 上的配置

在 Device A 上创建 RRPP 域，并指定控制 VLAN。

```
<DeviceA> system-view
[DeviceA] rrpp domain 1
[DeviceA-rrpp-domain1] control-vlan 4092
```

配置保护 VLAN 引用所有 MSTP 实例，实例 ID 范围以具体设备为准，下面以实例 ID 范围为 0～31 举例。

```
[DeviceA-rrpp-domain1] protected-vlan reference-instance 0 to 31
```

指定 Device A 为 RRPP 主环主节点，同时指定 Device A 接入 RRPP 主环的主端口和副端口分别为 GigabitEthernet1/0/1、GigabitEthernet1/0/2。

```
[DeviceA-rrpp-domain1] ring 1 node-mode master primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
```

使能 RRPP 环。

```
[DeviceA-rrpp-domain1] ring 1 enable
[DeviceA-rrpp-domain1] quit
```

使能 RRPP 协议

```
[DeviceA] rrpp enable
```

(2) Device B 上的配置

在 Device B 上创建 RRPP 域，并指定控制 VLAN。注意与域内其它节点使用相同域 ID、相同控制 VLAN。

```
<DeviceB> system-view
[DeviceB] rrpp domain 1
[DeviceB-rrpp-domain1] control-vlan 4092
```

配置保护 VLAN 引用所有 MSTP 实例，实例 ID 范围以具体设备为准，下面以实例 ID 范围为 0～31 举例。

```
[DeviceB-rrpp-domain1] protected-vlan reference-instance 0 to 31
```

指定 Device B 为 RRPP 主环传输节点，同时指定 Device B 接入 RRPP 主环的主端口和副端口分别为 GigabitEthernet1/0/1、GigabitEthernet1/0/2。

```
[DeviceB-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1  
secondary-port gigabitethernet 1/0/2 level 0
```

使能 RRPP 环。

```
[DeviceB-rrpp-domain1] ring 1 enable  
[DeviceB-rrpp-domain1] quit
```

使能 RRPP 协议。

```
[DeviceB] rrpp enable
```

配置完成后，用户可以使用 **display** 命令查看 RRPP 的配置情况。

2.1.5 完整配置

- Device A 上的配置

```
#  
rrpp domain 1  
control-vlan 4092  
protected-vlan reference-instance 0 to 31  
ring 1 node-mode master primary-port GigabitEthernet1/0/1 secondary-port  
GigabitEthernet1/0/2 level 0  
ring 1 enable  
#  
rrpp enable  
#
```

- Device B 上的配置

```
#  
rrpp domain 1  
control-vlan 4092  
protected-vlan reference-instance 0 to 31  
ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port  
GigabitEthernet1/0/2 level 0  
ring 1 enable  
#  
rrpp enable  
#
```

2.1.6 配置注意事项

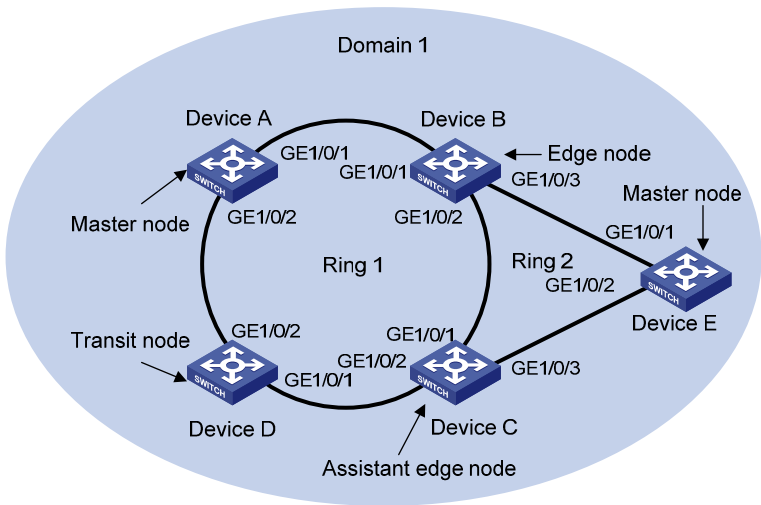
- RRPP 没有自动选举机制，因此只有为环网上的每个节点进行正确配置，才能让协议真正实现环网的检测和保护。请注意保证配置的正确性。
- 在配置 RRPP 功能之前，需要在物理上搭建以太网环形拓扑的组网环境。
- 在配置 RRPP 环之前必须先配置控制 VLAN。
- 为 RRPP 域配置的控制 VLAN 必须是设备上没有创建过的 VLAN。
- 用户可以配置主环的控制 VLAN，而子环的控制 VLAN 由系统自动分配，其 VLAN ID 为主环的控制 VLAN ID 加 1。因此，用户在配置控制 VLAN 时一定要选取两个连续的没有创建过的 VLAN。如果当前设备上没有两个连续的没有创建过的 VLAN，则配置失败。

- 每一个 RRPP 域都有唯一的控制 VLAN 和它绑定，控制 VLAN 的删除是在删除 RRPP 域的同时完成的，控制 VLAN 不能用 **undo vlan all** 命令删除。
- 控制 VLAN 不能被指定为远程镜像 VLAN 或 isolate-user-vlan。
- 控制 VLAN 上不能运行 QinQ 和 VLAN 映射功能，否则 RRPP 协议报文不能进行正常转发。
- 不要将接入 RRPP 环的端口的缺省 VLAN ID 设置为 RRPP 控制 VLAN ID，以免影响协议报文正常收发。
- 配置 RRPP 环之前，必须配置保护 VLAN。且在配置 RRPP 域的环之前可以删除、修改已经配置的保护 VLAN，在配置环之后允许删除、修改已经配置的保护 VLAN，但不允许删除该域所有的保护 VLAN。在删除 RRPP 域时也会同时删除其保护 VLAN。
- **protected-vlan** 命令通过引用 MSTP 实例的间接方式来配置 RRPP 域所保护的 VLAN 列表。MSTP 的实例和 VLAN 映射关系发生变化时，RRPP 域实际所保护的 VLAN 也会根据 RRPP 域的保护 VLAN 所引用的实例变化。
- RRPP 端口允许通过的 VLAN 都应该被 RRPP 域保护。
- 必须同时使能 RRPP 协议和 RRPP 环，当前设备的 RRPP 域才能激活。
- RRPP 环的节点角色、端口角色和环的级别一经配置不能直接修改，如果用户想改变上述配置，必须先删除现有的配置。
- 使用 **undo rrpp domain** 命令删除 RRPP 域时，必须保证 RRPP 域内没有配置 RRPP 环，否则删除操作不能成功。
- 接入 RRPP 环的端口必须配置为 Trunk 端口，并允许数据 VLAN 的报文通过。
- 接入 RRPP 环的端口不能是聚合端口、业务环回组成员端口、Smart Link 组成员端口。
- 接入 RRPP 环的端口不能使能 STP、802.1x、MAC 地址认证、Voice VLAN、Smart Link 功能。
- 不建议在 RRPP 端口上启用 OAM 远端环回功能，否则可能引起短时间的广播风暴。
- 建议接入 RRPP 环的端口使能链路状态快速上报功能（端口的 link-delay 设置为 0），以提高 RRPP 的拓扑变化收敛速度。
- 如果用户想在一个没有配置 RRPP 功能的设备上透传 RRPP 协议报文，需保证该设备上只有接入 RRPP 环的两个端口允许所在 RRPP 环对应的控制 VLAN 的报文通过，而其他端口不允许控制 VLAN 的报文通过。否则，其他 VLAN 的报文可能通过透传进入控制 VLAN，对 RRPP 环产生冲击。

2.2 RRPP 相交环拓扑典型配置指导

2.2.1 组网图

图2-2 RRPP 相交环拓扑组网示意图



2.2.2 应用要求

- Device A、Device B、Device C、Device D 和 Device E 构成 RRPP 域 1；
- RRPP 域 1 的控制 VLAN 为 VLAN 4092；
- RRPP 域 1 保护所有 VLAN；
- Device A、Device B、Device C 和 Device D 构成主环 Ring 1；
- Device B、Device C 和 Device E 构成子环 Ring 2；
- Device A 为主环的主节点，GigabitEthernet1/0/1 为主端口，GigabitEthernet1/0/2 为副端口；
- Device E 为子环的主节点，GigabitEthernet1/0/1 为主端口，GigabitEthernet1/0/2 为副端口；
- Device B 为主环的传输节点和子环的边缘节点，GigabitEthernet1/0/2 为公共端口，GigabitEthernet1/0/3 为边缘端口；
- Device C 为主环的传输节点和子环的辅助边缘节点，GigabitEthernet1/0/1 为公共端口，GigabitEthernet1/0/3 为边缘端口；
- Device D 为主环的传输节点，GigabitEthernet1/0/1 为主端口，GigabitEthernet1/0/2 为副端口；
- 主环和子环的定时器都取缺省值。

2.2.3 适用产品、版本

表2-2 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S7500E 系列以太网交换机	Release 6300 软件版本	全系列硬件版本

2.2.4 配置过程和解释



说明

- 接入 RRPP 环的端口已经配置为 Trunk 端口，并允许数据 VLAN 的报文通过。具体配置请参见本手册“以太网端口基本配置指导”部分的介绍。
- 接入 RRPP 环的端口已经关闭 STP 协议。

(1) Device A 上的配置

在 Device A 上创建 RRPP 域，并指定控制 VLAN。

```
<DeviceA> system-view
```

```
[DeviceA] rrpp domain 1
```

```
[DeviceA-rrpp-domain1] control-vlan 4092
```

配置保护 VLAN 引用所有 MSTP 实例，实例 ID 范围以具体设备为准，下面以实例 ID 范围为 0～31 举例。

```
[DeviceA-rrpp-domain1] protected-vlan reference-instance 0 to 31
```

指定 Device A 为 RRPP 主环主节点，同时指定 Device A 接入 RRPP 主环的主端口和副端口分别为 GigabitEthernet1/0/1、GigabitEthernet1/0/2。

```
[DeviceA-rrpp-domain1] ring 1 node-mode master primary-port gigabitethernet 1/0/1  
secondary-port gigabitethernet 1/0/2 level 0
```

使能 RRPP 环。

```
[DeviceA-rrpp-domain1] ring 1 enable
```

```
[DeviceA-rrpp-domain1] quit
```

使能 RRPP 协议

```
[DeviceA] rrpp enable
```

(2) Device B 上的配置

在 Device B 上创建 RRPP 域，并指定控制 VLAN。注意与域内其它节点使用相同域 ID、相同控制 VLAN。

```
<DeviceB> system-view
```

```
[DeviceB] rrpp domain 1
```

```
[DeviceB-rrpp-domain1] control-vlan 4092
```

配置保护 VLAN 引用所有 MSTP 实例，实例 ID 范围以具体设备为准，下面以实例 ID 范围为 0～31 举例。

```
[DeviceB-rrpp-domain1] protected-vlan reference-instance 0 to 31
```

指定 Device B 为 RRPP 主环传输节点，同时指定 Device B 接入 RRPP 主环的主端口和副端口分别为 GigabitEthernet1/0/1、GigabitEthernet1/0/2。

```
[DeviceB-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1  
secondary-port gigabitethernet 1/0/2 level 0
```

指定 Device B 为 RRPP 子环边缘节点，同时指定 Device B 接入 RRPP 子环的边缘端口为 GigabitEthernet1/0/3。注意使用 **ring** 命令对边缘节点进行配置的时候，不需要配置 level 参数。

```
[DeviceB-rrpp-domain1] ring 2 node-mode edge edge-port gigabitethernet 1/0/3
```

使能 RRPP 主环和 RRPP 子环。

```
[DeviceB-rrpp-domain1] ring 1 enable
[DeviceB-rrpp-domain1] ring 2 enable
[DeviceB-rrpp-domain1] quit
```

使能 RRPP 协议。

```
[DeviceB] rrpp enable
```

(3) Device C 上的配置

在 Device C 上创建 RRPP 域，并指定控制 VLAN。注意与域内其它节点使用相同域 ID、相同控制 VLAN。

```
<DeviceC> system-view
[DeviceC] rrpp domain 1
[DeviceC-rrpp-domain1] control-vlan 4092
```

配置保护 VLAN 引用所有 MSTP 实例，实例 ID 范围以具体设备为准，下面以实例 ID 范围为 0~31 举例。

```
[DeviceC-rrpp-domain1] protected-vlan reference-instance 0 to 31
```

指定 Device C 为 RRPP 主环传输节点，同时指定 Device C 接入 RRPP 主环的主端口和副端口分别为 GigabitEthernet1/0/1、GigabitEthernet1/0/2。

```
[DeviceC-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
```

指定 Device C 为 RRPP 子环辅助边缘节点，同时指定 Device C 接入 RRPP 子环的边缘端口为 GigabitEthernet1/0/3。注意使用 **ring** 命令对辅助边缘节点进行配置的时候，不需要配置 level 参数。

```
[DeviceC-rrpp-domain1] ring 2 node-mode assistant-edge edge-port gigabitethernet 1/0/3
```

使能 RRPP 主环和 RRPP 子环。

```
[DeviceC-rrpp-domain1] ring 1 enable
[DeviceC-rrpp-domain1] ring 2 enable
[DeviceC-rrpp-domain1] quit
```

使能 RRPP 协议。

```
[DeviceC] rrpp enable
```

(4) Device D 上的配置

在 Device D 上创建 RRPP 域，并指定控制 VLAN。注意与域内其它节点使用相同域 ID、相同控制 VLAN。

```
<DeviceD> system-view
[DeviceD] rrpp domain 1
[DeviceD-rrpp-domain1] control-vlan 4092
```

配置保护 VLAN 引用所有 MSTP 实例，实例 ID 范围以具体设备为准，下面以实例 ID 范围为 0~31 举例。

```
[DeviceD-rrpp-domain1] protected-vlan reference-instance 0 to 31
```

指定 Device D 为 RRPP 主环传输节点，同时指定 Device D 接入 RRPP 主环的主端口和副端口分别为 GigabitEthernet1/0/1、GigabitEthernet1/0/2。

```
[DeviceD-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 1/0/1
secondary-port gigabitethernet 1/0/2 level 0
```

使能 RRPP 环。

```
[DeviceD-rrpp-domain1] ring 1 enable  
[DeviceD-rrpp-domain1] quit
```

使能 RRPP 协议。

```
[DeviceD] rrpp enable
```

(5) Device E 上的配置

在 Device E 上创建 RRPP 域，并指定控制 VLAN。注意与域内其它节点使用相同域 ID、相同控制 VLAN。

```
<DeviceE> system-view  
[DeviceE] rrpp domain 1  
[DeviceE-rrpp-domain1] control-vlan 4092
```

配置保护 VLAN 引用所有 MSTP 实例，实例 ID 范围以具体设备为准，下面以实例 ID 范围为 0~31 举例。

```
[DeviceE-rrpp-domain1] protected-vlan reference-instance 0 to 31
```

指定 Device E 为 RRPP 子环主节点，同时指定 Device E 接入 RRPP 子环的主端口和副端口分别为 GigabitEthernet1/0/1、GigabitEthernet1/0/2。

```
[DeviceE-rrpp-domain1] ring 2 node-mode master primary-port gigabitethernet 1/0/1  
secondary-port gigabitethernet 1/0/2 level 1
```

使能 RRPP 子环。

```
[DeviceE-rrpp-domain1] ring 2 enable  
[DeviceE-rrpp-domain1] quit
```

使能 RRPP 协议。

```
[DeviceE] rrpp enable
```

配置完成后，用户可以使用 **display** 命令查看 RRPP 的配置情况。

2.2.5 完整配置

- Device A 上的配置

```
#  
rrpp domain 1  
control-vlan 4092  
protected-vlan reference-instance 0 to 31  
ring 1 node-mode master primary-port GigabitEthernet1/0/1 secondary-port  
GigabitEthernet1/0/2 level 0  
ring 1 enable  
#  
rrpp enable  
#
```

- Device B 上的配置

```
#  
rrpp domain 1  
control-vlan 4092  
protected-vlan reference-instance 0 to 31  
ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port
```



```
GigabitEthernet1/0/2 level 0
```

```
ring 2 node-mode edge edge-port GigabitEthernet1/0/3
```

```
ring 1 enable
```

```
ring 2 enable
```

```
#
```

```
rrpp enable
```

```
#
```

- Device C 上的配置

```
#
```

```
rrpp domain 1
```

```
control-vlan 4092
```

```
protected-vlan reference-instance 0 to 31
```

```
ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port
```

```
GigabitEthernet1/0/2 level 0
```

```
ring 2 node-mode assistant-edge edge-port GigabitEthernet1/0/3
```

```
ring 1 enable
```

```
ring 2 enable
```

```
#
```

```
rrpp enable
```

```
#
```

- Device D 上的配置

```
#
```

```
rrpp domain 1
```

```
control-vlan 4092
```

```
protected-vlan reference-instance 0 to 31
```

```
ring 1 node-mode transit primary-port GigabitEthernet1/0/1 secondary-port
```

```
GigabitEthernet1/0/2 level 0
```

```
ring 1 enable
```

```
#
```

```
rrpp enable
```

```
#
```

- Device E 上的配置

```
#
```

```
rrpp domain 1
```

```
control-vlan 4092
```

```
protected-vlan reference-instance 0 to 31
```

```
ring 2 node-mode master primary-port GigabitEthernet1/0/1 secondary-port
```

```
GigabitEthernet1/0/2 level 1
```

```
ring 2 enable
```

```
#
```

```
rrpp enable
```

```
#
```

2.2.6 配置注意事项

除 RRPP 单环拓扑典型配置举例中所列注意事项外，还需注意：

- 配置 RRPP 域时，最好先配置主环，再配置子环，并且在同一个 RRPP 域中，不同的 RRPP 环不能使用相同的 Ring ID。

- 如果一台设备在同一个 RRPP 域中的多个 RRPP 环上，则只能有一个主环，而且在其他子环上的节点角色只能是边缘节点或者辅助边缘节点。
- 使用 **ring** 命令对边缘节点或辅助边缘节点进行配置的时候，不需要配置 **level** 参数。
- 使能子环之前必须先使能主环。关闭主环前必须先关闭该主环所在的 RRPP 域内的所有子环。
- 一台设备在所有 RRPP 域中配置的环的总数不能大于 16。
- 不要将接入 RRPP 环的端口的缺省 VLAN ID 设置为 RRPP 控制 VLAN ID 或者子控制 VLAN ID（子控制 VLAN ID 为主控制 VLAN ID 加 1），以免影响协议报文正常收发。
- 配置边缘节点和辅助边缘节点时，必须先进行主环配置，然后再进行子环配置。并且，在删除边缘节点的主环配置前，必须先删除所有的子环配置。但是，处于使能状态的 RRPP 环不能被删除。

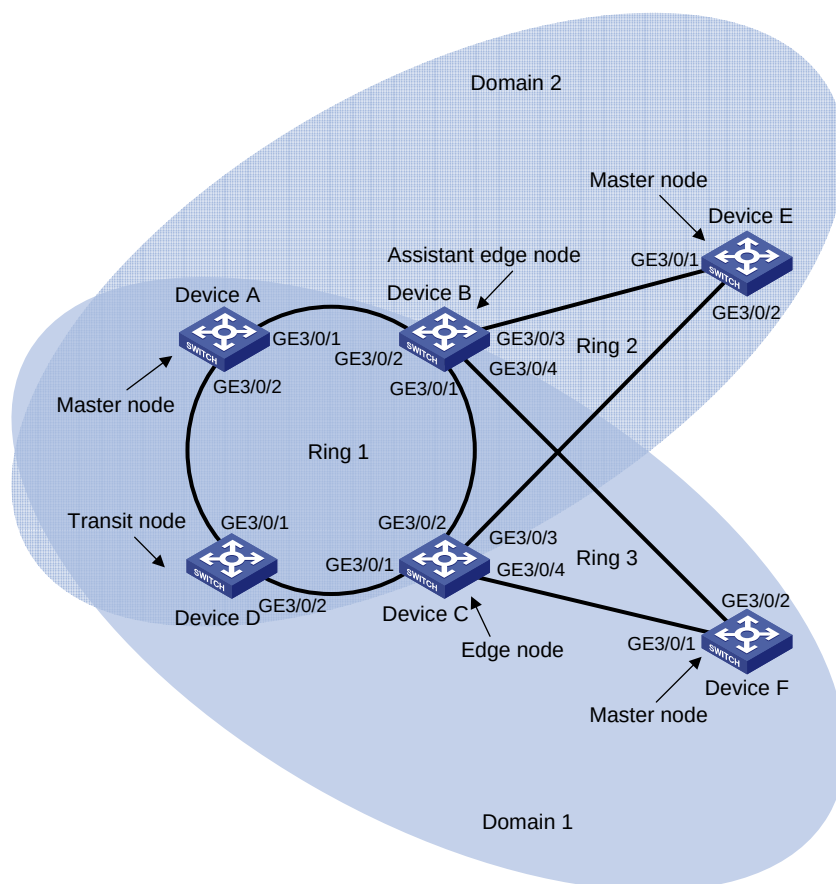
2.3 RRPP 相交环负载分担拓扑典型配置指导

在同一个环网中，可能同时存在多个 VLAN 的数据流量，RRPP 可以实现流量的负载分担，即不同 VLAN 的流量沿不同的路径进行转发。

通过在同一个环网上配置多个 RRPP 域，不同 RRPP 域发送不同 VLAN（称之为保护 VLAN）的流量，实现不同 VLAN 的数据流量在该环网中的拓扑不同，从而达到负载分担的目的。

2.3.1 组网图

图2-3 RRPP 相交环负载分担拓拓扑组网示意图



2.3.2 应用要求

- Device A、Device B、Device C、Device D 和 Device F 构成 RRPP 域 1，RRPP 域 1 的控制 VLAN 为 VLAN 100。Device A 为主环 1 的主节点，Device D 为主环 1 的传输节点，Device F 为子环 3 的主节点，Device C 为子环 3 的边缘节点，Device B 为子环 3 的辅助边缘节点。
- Device A、Device B、Device C、Device D 和 Device E 构成 RRPP 域 2，RRPP 域 2 的控制 VLAN 为 VLAN 105。Device A 为主环 1 的主节点，Device D 为主环 1 的传输节点，Device E 为子环 2 的主节点，Device C 为子环 2 的边缘节点，Device B 为子环 2 的辅助边缘节点。
- RRPP 域 1 保护 VLAN 10，RRPP 域 2 保护 VLAN 20。由此可以按照 VLAN 在主环上实现负载分担。
- 由于子环 2 和子环 3 的边缘节点和辅助边缘节点的配置一样，并且对应的主环链路也相同，因此可以将子环 2 和子环 3 加入环组，从而减少 Edge-Hello 报文的收发数量。

2.3.3 适用产品、版本

表2-3 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S7500E 系列以太网交换机	Release 6300 软件版本	全系列硬件版本

2.3.4 配置过程和解释

配置思路：

- 创建数据 VLAN，将各 RRPP 域需要保护的 VLAN 映射到不同的 MSTP 实例；
- 各设备上 RRPP 环的接入端口关闭 STP，并配置允许通过的 VLAN；
- 创建 RRPP 域；
- 为 RRPP 域指定控制 VLAN；
- 配置各域的保护 VLAN，引用需要保护的 VLAN 所映射到的 MSTP 实例；
- 指定设备在 RRPP 环上的节点角色和设备接入 RRPP 环的端口；
- 使能 RRPP 环；
- 使能 RRPP 协议；
- 在边缘节点和辅助边缘节点上配置环组。

(1) Device A 上的配置

配置 Device A 为主环主节点。

配置 MSTP 实例。

```
<DeviceA> system-view
[DeviceA] vlan 10
[DeviceA-vlan10] vlan 20
[DeviceA-vlan20] quit
[DeviceA] stp region-configuration
[DeviceA-mst-region] instance 1 vlan 10
[DeviceA-mst-region] instance 2 vlan 20
[DeviceA-mst-region] active region-configuration
```

```
[DeviceA-mst-region] quit
```

配置接入 RRPP 环的端口。

```
[DeviceA] interface gigabitethernet 3/0/1
[DeviceA-GigabitEthernet3/0/1] link-delay 0
[DeviceA-GigabitEthernet3/0/1] stp disable
[DeviceA-GigabitEthernet3/0/1] port link-type trunk
[DeviceA-GigabitEthernet3/0/1] undo port trunk permit vlan 1
[DeviceA-GigabitEthernet3/0/1] port trunk permit vlan 10 20
[DeviceA-GigabitEthernet3/0/1] interface gigabitethernet 3/0/2
[DeviceA-GigabitEthernet3/0/2] link-delay 0
[DeviceA-GigabitEthernet3/0/2] stp disable
[DeviceA-GigabitEthernet3/0/2] port link-type trunk
[DeviceA-GigabitEthernet3/0/2] undo port trunk permit vlan 1
[DeviceA-GigabitEthernet3/0/2] port trunk permit vlan 10 20
[DeviceA-GigabitEthernet3/0/2] quit
```

配置 RRPP 域 1，指定控制 VLAN、保护 VLAN，配置并使能 RRPP 环。

```
[DeviceA] rrpp domain 1
[DeviceA-rrpp-domain1] control-vlan 100
[DeviceA-rrpp-domain1] protected-vlan reference-instance 1
[DeviceA-rrpp-domain1] ring 1 node-mode master primary-port gigabitethernet 3/0/1
secondary-port gigabitethernet 3/0/2 level 0
[DeviceA-rrpp-domain1] ring 1 enable
[DeviceA-rrpp-domain1] quit
```

配置 RRPP 域 2，指定控制 VLAN、保护 VLAN，配置并使能 RRPP 环。

```
[DeviceA] rrpp domain 2
[DeviceA-rrpp-domain2] control-vlan 105
[DeviceA-rrpp-domain2] protected-vlan reference-instance 2
[DeviceA-rrpp-domain2] ring 1 node-mode master primary-port gigabitethernet 3/0/2
secondary-port gigabitethernet 3/0/1 level 0
[DeviceA-rrpp-domain2] ring 1 enable
[DeviceA-rrpp-domain2] quit
```

使能 RRPP 协议。

```
[DeviceA] rrpp enable
```

(2) Device B 上的配置

配置 Device B 为子环 2、子环 3 的辅助边缘节点。

配置 MSTP 实例。

```
<DeviceB> system-view
[DeviceB] vlan 10
[DeviceB-vlan10] vlan 20
[DeviceB-vlan20] quit
[DeviceB] stp region-configuration
[DeviceB-mst-region] instance 1 vlan 10
[DeviceB-mst-region] instance 2 vlan 20
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit
```

配置接入 RRPP 环的端口。

```
[DeviceB] interface gigabitethernet 3/0/1
[DeviceB-GigabitEthernet3/0/1] link-delay 0
[DeviceB-GigabitEthernet3/0/1] stp disable
[DeviceB-GigabitEthernet3/0/1] port link-type trunk
[DeviceB-GigabitEthernet3/0/1] undo port trunk permit vlan 1
[DeviceB-GigabitEthernet3/0/1] port trunk permit vlan 10 20
[DeviceB-GigabitEthernet3/0/1] interface gigabitethernet 3/0/2
[DeviceB-GigabitEthernet3/0/2] link-delay 0
[DeviceB-GigabitEthernet3/0/2] stp disable
[DeviceB-GigabitEthernet3/0/2] port link-type trunk
[DeviceB-GigabitEthernet3/0/2] undo port trunk permit vlan 1
[DeviceB-GigabitEthernet3/0/2] port trunk permit vlan 10 20
[DeviceB-GigabitEthernet3/0/2] interface gigabitethernet 3/0/3
[DeviceB-GigabitEthernet3/0/3] link-delay 0
[DeviceB-GigabitEthernet3/0/3] stp disable
[DeviceB-GigabitEthernet3/0/3] port link-type trunk
[DeviceB-GigabitEthernet3/0/3] undo port trunk permit vlan 1
[DeviceB-GigabitEthernet3/0/3] port trunk permit vlan 20
[DeviceB-GigabitEthernet3/0/3] interface gigabitethernet 3/0/4
[DeviceB-GigabitEthernet3/0/4] link-delay 0
[DeviceB-GigabitEthernet3/0/4] stp disable
[DeviceB-GigabitEthernet3/0/4] port link-type trunk
[DeviceB-GigabitEthernet3/0/4] undo port trunk permit vlan 1
[DeviceB-GigabitEthernet3/0/4] port trunk permit vlan 10
[DeviceB-GigabitEthernet3/0/4] quit
```

配置 RRPP 域 1，指定控制 VLAN、保护 VLAN，配置并使能 RRPP 环。

```
[DeviceB] rrpp domain 1
[DeviceB-rrpp-domain1] control-vlan 100
[DeviceB-rrpp-domain1] protected-vlan reference-instance 1
[DeviceB-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 3/0/1
secondary-port gigabitethernet 3/0/2 level 0
[DeviceB-rrpp-domain1] ring 3 node-mode assistant-edge edge-port gigabitethernet 3/0/4
[DeviceB-rrpp-domain1] ring 1 enable
[DeviceB-rrpp-domain1] ring 3 enable
[DeviceB-rrpp-domain1] quit
```

配置 RRPP 域 2，指定控制 VLAN、保护 VLAN，配置并使能 RRPP 环。

```
[DeviceB] rrpp domain 2
[DeviceB-rrpp-domain2] control-vlan 105
[DeviceB-rrpp-domain2] protected-vlan reference-instance 2
[DeviceB-rrpp-domain2] ring 1 node-mode transit primary-port gigabitethernet 3/0/1
secondary-port gigabitethernet 3/0/2 level 0
[DeviceB-rrpp-domain2] ring 2 node-mode assistant-edge edge-port gigabitethernet 3/0/3
[DeviceB-rrpp-domain2] ring 1 enable
[DeviceB-rrpp-domain2] ring 2 enable
[DeviceB-rrpp-domain2] quit
```

使能 RRPP 协议。

```
[DeviceB] rrpp enable
```

(3) Device C 上的配置

配置 Device C 为子环 2、子环 3 的边缘节点。

配置 MSTP 实例。

```
<DeviceC> system-view
```

```
[DeviceC] vlan 10
```

```
[DeviceC-vlan10] vlan 20
```

```
[DeviceC-vlan20] quit
```

```
[DeviceC] stp region-configuration
```

```
[DeviceC-mst-region] instance 1 vlan 10
```

```
[DeviceC-mst-region] instance 2 vlan 20
```

```
[DeviceC-mst-region] active region-configuration
```

```
[DeviceC-mst-region] quit
```

配置接入 RRPP 环的端口。

```
[DeviceC] interface gigabitethernet 3/0/1
```

```
[DeviceC-GigabitEthernet3/0/1] link-delay 0
```

```
[DeviceC-GigabitEthernet3/0/1] stp disable
```

```
[DeviceC-GigabitEthernet3/0/1] port link-type trunk
```

```
[DeviceC-GigabitEthernet3/0/1] undo port trunk permit vlan 1
```

```
[DeviceC-GigabitEthernet3/0/1] port trunk permit vlan 10 20
```

```
[DeviceC-GigabitEthernet3/0/1] interface gigabitethernet 3/0/2
```

```
[DeviceC-GigabitEthernet3/0/2] link-delay 0
```

```
[DeviceC-GigabitEthernet3/0/2] stp disable
```

```
[DeviceC-GigabitEthernet3/0/2] port link-type trunk
```

```
[DeviceC-GigabitEthernet3/0/2] undo port trunk permit vlan 1
```

```
[DeviceC-GigabitEthernet3/0/2] port trunk permit vlan 10 20
```

```
[DeviceC-GigabitEthernet3/0/2] interface gigabitethernet 3/0/3
```

```
[DeviceC-GigabitEthernet3/0/3] link-delay 0
```

```
[DeviceC-GigabitEthernet3/0/3] stp disable
```

```
[DeviceC-GigabitEthernet3/0/3] port link-type trunk
```

```
[DeviceC-GigabitEthernet3/0/3] undo port trunk permit vlan 1
```

```
[DeviceC-GigabitEthernet3/0/3] port trunk permit vlan 20
```

```
[DeviceC-GigabitEthernet3/0/3] interface gigabitethernet 3/0/4
```

```
[DeviceC-GigabitEthernet3/0/4] link-delay 0
```

```
[DeviceC-GigabitEthernet3/0/4] stp disable
```

```
[DeviceC-GigabitEthernet3/0/4] port link-type trunk
```

```
[DeviceC-GigabitEthernet3/0/4] undo port trunk permit vlan 1
```

```
[DeviceC-GigabitEthernet3/0/4] port trunk permit vlan 10
```

```
[DeviceC-GigabitEthernet3/0/4] quit
```

配置 RRPP 域 1，指定控制 VLAN、保护 VLAN，配置并使能 RRPP 环。

```
[DeviceC] rrpp domain 1
```

```
[DeviceC-rrpp-domain1] control-vlan 100
```

```
[DeviceC-rrpp-domain1] protected-vlan reference-instance 1
```

```
[DeviceC-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 3/0/1
```

```
secondary-port gigabitethernet 3/0/2 level 0
```

```
[DeviceC-rrpp-domain1] ring 3 node-mode edge edge-port gigabitethernet 3/0/4
```

```
[DeviceC-rrpp-domain1] ring 1 enable
```

```
[DeviceC-rrpp-domain1] ring 3 enable
```

```
[DeviceC-rrpp-domain1] quit
```

配置 RRPP 域 2，指定控制 VLAN、保护 VLAN，配置并使能 RRPP 环。

```
[DeviceC] rrpp domain 2
```

```
[DeviceC-rrpp-domain2] control-vlan 105
```

```
[DeviceC-rrpp-domain2] protected-vlan reference-instance 2
```

```
[DeviceC-rrpp-domain2] ring 1 node-mode transit primary-port gigabitethernet 3/0/1
```

```
secondary-port gigabitethernet 3/0/2 level 0
```

```
[DeviceC-rrpp-domain2] ring 2 node-mode edge edge-port gigabitethernet 3/0/3
```

```
[DeviceC-rrpp-domain2] ring 1 enable
```

```
[DeviceC-rrpp-domain2] ring 2 enable
```

```
[DeviceC-rrpp-domain2] quit
```

使能 RRPP 协议。

```
[DeviceC] rrpp enable
```

(4) Device D 上的配置

配置 Device D 为主环传输节点。

配置 MSTP 实例。

```
<DeviceD> system-view
```

```
[DeviceD] vlan 10
```

```
[DeviceD-vlan10] vlan 20
```

```
[DeviceD-vlan20] quit
```

```
[DeviceD] stp region-configuration
```

```
[DeviceD-mst-region] instance 1 vlan 10
```

```
[DeviceD-mst-region] instance 2 vlan 20
```

```
[DeviceD-mst-region] active region-configuration
```

```
[DeviceD-mst-region] quit
```

配置接入 RRPP 环的端口。

```
[DeviceD] interface gigabitethernet 3/0/1
```

```
[DeviceD-GigabitEthernet3/0/1] link-delay 0
```

```
[DeviceD-GigabitEthernet3/0/1] stp disable
```

```
[DeviceD-GigabitEthernet3/0/1] port link-type trunk
```

```
[DeviceD-GigabitEthernet3/0/1] undo port trunk permit vlan 1
```

```
[DeviceD-GigabitEthernet3/0/1] port trunk permit vlan 10 20
```

```
[DeviceD-GigabitEthernet3/0/1] interface gigabitethernet 3/0/2
```

```
[DeviceD-GigabitEthernet3/0/2] link-delay 0
```

```
[DeviceD-GigabitEthernet3/0/2] stp disable
```

```
[DeviceD-GigabitEthernet3/0/2] port link-type trunk
```

```
[DeviceD-GigabitEthernet3/0/2] undo port trunk permit vlan 1
```

```
[DeviceD-GigabitEthernet3/0/2] port trunk permit vlan 10 20
```

```
[DeviceD-GigabitEthernet3/0/2] quit
```

配置 RRPP 域 1，指定控制 VLAN、保护 VLAN，配置并使能 RRPP 环。

```
[DeviceD] rrpp domain 1
```

```
[DeviceD-rrpp-domain1] control-vlan 100
[DeviceD-rrpp-domain1] protected-vlan reference-instance 1
[DeviceD-rrpp-domain1] ring 1 node-mode transit primary-port gigabitethernet 3/0/1
secondary-port gigabitethernet 3/0/2 level 0
[DeviceD-rrpp-domain1] ring 1 enable
[DeviceD-rrpp-domain1] quit
```

配置 RRPP 域 2，指定控制 VLAN、保护 VLAN，配置并使能 RRPP 环。

```
[DeviceD] rrpp domain 2
[DeviceD-rrpp-domain2] control-vlan 105
[DeviceD-rrpp-domain2] protected-vlan reference-instance 2
[DeviceD-rrpp-domain2] ring 1 node-mode transit primary-port gigabitethernet 3/0/1
secondary-port gigabitethernet 3/0/2 level 0
[DeviceD-rrpp-domain2] ring 1 enable
[DeviceD-rrpp-domain2] quit
```

使能 RRPP 协议。

```
[DeviceD] rrpp enable
```

(5) Device E 上的配置

配置 Device E 为域 2 子环 2 的主节点。

配置 MSTP 实例。

```
<DeviceE> system-view
[DeviceE] vlan 20
[DeviceE-vlan20] quit
[DeviceE] stp region-configuration
[DeviceE-mst-region] instance 2 vlan 20
[DeviceE-mst-region] active region-configuration
[DeviceE-mst-region] quit
```

配置接入 RRPP 环的端口。

```
[DeviceE] interface gigabitethernet 3/0/1
[DeviceE-GigabitEthernet3/0/1] link-delay 0
[DeviceE-GigabitEthernet3/0/1] stp disable
[DeviceE-GigabitEthernet3/0/1] port link-type trunk
[DeviceE-GigabitEthernet3/0/1] undo port trunk permit vlan 1
[DeviceE-GigabitEthernet3/0/1] port trunk permit vlan 20
[DeviceE-GigabitEthernet3/0/1] interface gigabitethernet 3/0/2
[DeviceE-GigabitEthernet3/0/2] link-delay 0
[DeviceE-GigabitEthernet3/0/2] stp disable
[DeviceE-GigabitEthernet3/0/2] port link-type trunk
[DeviceE-GigabitEthernet3/0/2] undo port trunk permit vlan 1
[DeviceE-GigabitEthernet3/0/2] port trunk permit vlan 20
[DeviceE-GigabitEthernet3/0/2] quit
```

配置 RRPP 域 2，指定控制 VLAN、保护 VLAN，配置并使能 RRPP 环。

```
[DeviceE] rrpp domain 2
[DeviceE-rrpp-domain2] control-vlan 105
[DeviceE-rrpp-domain2] protected-vlan reference-instance 2
[DeviceE-rrpp-domain2] ring 2 node-mode master primary-port gigabitethernet 3/0/2
```



```
secondary-port gigabitethernet 3/0/1 level 1
[DeviceE-rrpp-domain2] ring 2 enable
[DeviceE-rrpp-domain2] quit
```

使能 RRPP 协议。

```
[DeviceE] rrpp enable
```

(6) Device F 上的配置

配置 Device F 为域 1 子环 3 的主节点。

配置 MSTP 实例。

```
<DeviceF> system-view
[DeviceF] vlan 10
[DeviceF-vlan10] quit
[DeviceF] stp region-configuration
[DeviceF-mst-region] instance 1 vlan 10
[DeviceF-mst-region] active region-configuration
[DeviceF-mst-region] quit
```

配置接入 RRPP 环的端口。

```
[DeviceF] interface gigabitethernet 3/0/1
[DeviceF-GigabitEthernet3/0/1] link-delay 0
[DeviceF-GigabitEthernet3/0/1] stp disable
[DeviceF-GigabitEthernet3/0/1] port link-type trunk
[DeviceF-GigabitEthernet3/0/1] undo port trunk permit vlan 1
[DeviceF-GigabitEthernet3/0/1] port trunk permit vlan 10
[DeviceF-GigabitEthernet3/0/1] interface gigabitethernet 3/0/2
[DeviceF-GigabitEthernet3/0/2] link-delay 0
[DeviceF-GigabitEthernet3/0/2] stp disable
[DeviceF-GigabitEthernet3/0/2] port link-type trunk
[DeviceF-GigabitEthernet3/0/2] undo port trunk permit vlan 1
[DeviceF-GigabitEthernet3/0/2] port trunk permit vlan 10
[DeviceF-GigabitEthernet3/0/2] quit
```

配置 RRPP 域 1，指定控制 VLAN、保护 VLAN，配置并使能 RRPP 环。

```
[DeviceF] rrpp domain 1
[DeviceF-rrpp-domain1] control-vlan 100
[DeviceF-rrpp-domain1] protected-vlan reference-instance 1
[DeviceF-rrpp-domain1] ring 3 node-mode master primary-port gigabitethernet 3/0/1
secondary-port gigabitethernet 3/0/2 level 1
[DeviceF-rrpp-domain1] ring 3 enable
[DeviceF-rrpp-domain1] quit
```

使能 RRPP 协议。

```
[DeviceF] rrpp enable
```

(7) 完成以上配置后，在 Device B 和 Device C 上进行环组配置

```
<DeviceB> system-view
[DeviceB] rrpp ring-group 1
[DeviceB-rrpp-ring-group1] domain 2 ring 2
[DeviceB-rrpp-ring-group1] domain 1 ring 3
```

```

<DeviceC> system-view
[DeviceC] rrpp ring-group 1
[DeviceC-rrpp-ring-group1] domain 2 ring 2
[DeviceC-rrpp-ring-group1] domain 1 ring 3

```

2.3.5 完整配置

- Device A 上的配置

```

#
vlan 10
#
vlan 20
#
stp region-configuration
instance 1 vlan 10
instance 2 vlan 20
active region-configuration
#
interface GigabitEthernet3/0/1
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 20
stp disable
#
interface GigabitEthernet3/0/2
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 20
stp disable
#
rrpp domain 1
control-vlan 100
protected-vlan reference-instance 1
ring 1 node-mode master primary-port GigabitEthernet3/0/1 secondary-port
GigabitEthernet3/0/2 level 0
ring 1 enable
#
rrpp domain 2
control-vlan 105
protected-vlan reference-instance 1
ring 1 node-mode master primary-port GigabitEthernet3/0/2 secondary-port
GigabitEthernet3/0/1 level 0
ring 1 enable
#
rrpp enable
#

```

- Device B 上的配置

```

#
vlan 10

```

```

#
vlan 20
#
stp region-configuration
instance 1 vlan 10
instance 2 vlan 20
active region-configuration
#
interface GigabitEthernet3/0/1
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 20
stp disable
#
interface GigabitEthernet3/0/2
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 20
stp disable
#
interface GigabitEthernet3/0/3
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 20
stp disable
#
interface GigabitEthernet3/0/4
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10
stp disable
#
rrpp domain 1
control-vlan 100
protected-vlan reference-instance 1
ring 1 node-mode transit primary-port GigabitEthernet3/0/1 secondary-port
GigabitEthernet3/0/2 level 0
ring 3 node-mode assistant-edge edge-port GigabitEthernet3/0/4
ring 1 enable
ring 3 enable
#
rrpp domain 2
control-vlan 105
protected-vlan reference-instance 2
ring 1 node-mode transit primary-port GigabitEthernet3/0/1 secondary-port
GigabitEthernet3/0/2 level 0
ring 2 node-mode assistant-edge edge-port GigabitEthernet3/0/3
ring 1 enable

```

```
ring 2 enable
```

```
#
```

```
rrpp ring-group 1
```

```
domain 2 ring 2
```

```
domain 1 ring 3
```

```
#
```

```
rrpp enable
```

```
#
```

- Device C 上的配置

```
#
```

```
vlan 10
```

```
#
```

```
vlan 20
```

```
#
```

```
stp region-configuration
```

```
instance 1 vlan 10
```

```
instance 2 vlan 20
```

```
active region-configuration
```

```
#
```

```
interface GigabitEthernet3/0/1
```

```
port link-type trunk
```

```
undo port trunk permit vlan 1
```

```
port trunk permit vlan 10 20
```

```
stp disable
```

```
#
```

```
interface GigabitEthernet3/0/2
```

```
port link-type trunk
```

```
undo port trunk permit vlan 1
```

```
port trunk permit vlan 10 20
```

```
stp disable
```

```
#
```

```
interface GigabitEthernet3/0/3
```

```
port link-type trunk
```

```
undo port trunk permit vlan 1
```

```
port trunk permit vlan 20
```

```
stp disable
```

```
#
```

```
interface GigabitEthernet3/0/4
```

```
port link-type trunk
```

```
undo port trunk permit vlan 1
```

```
port trunk permit vlan 10
```

```
stp disable
```

```
#
```

```
rrpp domain 1
```

```
control-vlan 100
```

```
protected-vlan reference-instance 1
```

```
ring 1 node-mode transit primary-port GigabitEthernet3/0/1 secondary-port  
GigabitEthernet3/0/2 level 0
```

```

ring 3 node-mode edge edge-port GigabitEthernet3/0/4
ring 1 enable
ring 3 enable
#
rrpp domain 2
control-vlan 105
protected-vlan reference-instance 1
ring 1 node-mode transit primary-port GigabitEthernet3/0/1 secondary-port
GigabitEthernet3/0/2 level 0
ring 2 node-mode edge edge-port GigabitEthernet3/0/3
ring 1 enable
ring 2 enable
#
rrpp ring-group 1
domain 2 ring 2
domain 1 ring 3
#
rrpp enable
#
• Device D 上的配置
#
vlan 10
#
vlan 20
#
stp region-configuration
instance 1 vlan 10
instance 2 vlan 20
active region-configuration
#
interface GigabitEthernet3/0/1
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 20
stp disable
#
interface GigabitEthernet3/0/2
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10 20
stp disable
#
rrpp domain 1
control-vlan 100
protected-vlan reference-instance 1
ring 1 node-mode transit primary-port GigabitEthernet3/0/1 secondary-port
GigabitEthernet3/0/2 level 0
ring 1 enable

```

```
#
rrpp domain 2
control-vlan 105
protected-vlan reference-instance 1
ring 1 node-mode transit primary-port GigabitEthernet3/0/1 secondary-port
GigabitEthernet3/0/2 level 0
ring 1 enable
```

```
#
rrpp enable
```

```
#
```

- Device E 上的配置

```
#
vlan 20
#
stp region-configuration
instance 2 vlan 20
active region-configuration
#
interface GigabitEthernet3/0/1
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 20
stp disable
```

```
#
interface GigabitEthernet3/0/2
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 20
stp disable
```

```
#
rrpp domain 2
control-vlan 105
protected-vlan reference-instance 2
ring 2 node-mode master primary-port GigabitEthernet3/0/2 secondary-port
GigabitEthernet3/0/1 level 1
ring 2 enable
```

```
#
rrpp enable
```

```
#
```

- Device F 上的配置

```
#
vlan 10
#
stp region-configuration
instance 1 vlan 10
active region-configuration
#
interface GigabitEthernet3/0/1
```

```

port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10
stp disable
#
interface GigabitEthernet3/0/2
port link-type trunk
undo port trunk permit vlan 1
port trunk permit vlan 10
stp disable
#
rrpp domain 1
control-vlan 100
protected-vlan reference-instance 1
ring 3 node-mode master primary-port GigabitEthernet3/0/1 secondary-port
GigabitEthernet3/0/2 level 1
ring 3 enable
#
rrpp enable
#

```

2.3.6 配置注意事项

除 RRPP 单环拓扑和相交环拓扑典型配置举例中所列注意事项外，还需注意：

- 为了减少 Edge-Hello 报文的收发数量，用户可以采用环组机制，即将具有相同边缘节点 / 辅助边缘节点配置的一组子环加入环组。在配置了环组的情况下，与不支持环组配置的 RRPP 版本不能互通。
- 只能在边缘节点设备或辅助边缘节点设备上才能进行环组配置，而且两个设备上配置的环组中包含的子环必须相同，否则环组不能正常工作。
- 一个子环只能属于一个环组。
- 设备在一个环组内的所有子环上应该具有相同的类型，要么都是边缘节点，要么都是辅助边缘节点。
- 如果需要将激活的环加入环组，需要按照下述顺序进行操作：先在辅助边缘节点将环加入环组，再在边缘节点将环加入环组。
- 如果需要将激活的环从环组中删除，需要按照下述顺序进行操作：先在边缘节点将环从环组中删除，再在辅助边缘节点将环从环组中删除。
- 在同一环组中，子环所对应主环的链路必须相同，如果主环链路本身的配置就不相同，或者由于修改配置以后不相同，环组功能都不能正常运行。
- 边缘节点环组和对应的辅助边缘节点环组的配置和激活状态必须相同。

目 录

- 1 sFlow典型配置指导 1-1
 - 1.1 sFlow典型配置指导 1-1
 - 1.1.1 组网图 1-1
 - 1.1.2 应用要求 1-1
 - 1.1.3 适用产品、版本 1-2
 - 1.1.4 配置过程和解释 1-2
 - 1.1.5 完整配置 1-2
 - 1.1.6 配置注意事项 1-2

1 sFlow 典型配置指导

1.1 sFlow 典型配置指导

sFlow（Sampled Flow，采样流）是一种基于报文采样的网络流量监控技术，主要用于对网络流量进行统计分析。

sFlow 有以下两种采样机制：

- 基于数据包的流采样：对通过设备端口的报文进行数据包采样，获取数据流的相关信息。
- 基于时间的端口统计信息采样：定期查询开启 sFlow 功能的端口，获取各端口的统计信息。

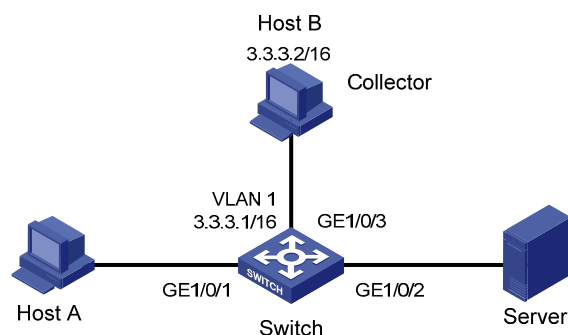
sFlow 系统包含一个嵌入在设备中的 sFlow Agent 和一个远端的 sFlow Collector。其中，sFlow Agent 用于获取端口统计信息和端口的数据流信息，将信息组装成 sFlow 报文，发送到 sFlow Collector。sFlow Collector 用于分析 sFlow 报文，并显示分析结果。

作为一种网络流量监控技术，sFlow 具有如下优点：

- 支持在千兆或更高速的网络上精确地监控网络流量。
- 一个 sFlow Collector 能够监控多个 sFlow Agent，具有良好的扩展性。
- 以极低的代价实现了 sFlow Agent。

1.1.1 组网图

图1-1 配置 sFlow 组网图



1.1.2 应用要求

网络环境描述如下：

- Host A 与远端服务器 Server 分别通过端口 GigabitEthernet 1/0/1 和端口 GigabitEthernet 1/0/2 接入 Switch；
- Host B 为运行 sFlow Collector 的设备，IP 地址为 3.3.3.2，通过端口 GigabitEthernet 1/0/3 接入 Switch，sFlow Collector 的端口为 6343；
- 端口 GigabitEthernet 1/0/3 属于 VLAN 1，VLAN 1 的 IP 地址为 3.3.3.1。

要求在 Switch 上运行 sFlow Agent，并在端口 GigabitEthernet 1/0/1 上开启 sFlow 功能，使 Agent 能够对进入该端口的网络流量进行监控。Switch 将 sFlow 报文通过 GigabitEthernet 1/0/3 发送给 Host B，Host B 再对 sFlow 报文进行分析并显示。

1.1.3 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件产品
S7500E 系列以太网交换机	Release 6300 软件版本	全系列硬件产品

1.1.4 配置过程和解释

配置 sFlow Agent 的 IP 地址。

```
<Switch> system-view
```

```
[Switch] sflow agent ip 3.3.3.1
```

配置 sFlow Collector 的 IP 地址和端口号。如果没有指定具体的端口号，则缺省值为 6343。

```
[Switch] sflow collector ip 3.3.3.2
```

配置轮询时间间隔为 30 秒。

```
[Switch] sflow interval 30
```

在端口 GigabitEthernet 1/0/1 上开启 sFlow 功能，对入方向的数据包采样。

```
[Switch] interface GigabitEthernet 1/0/1
```

```
[Switch-GigabitEthernet1/0/1] sflow enable inbound
```

配置采样频率为 100000，即 100000 个报文中采样 1 个报文。

```
[Switch-GigabitEthernet1/0/1] sflow sampling-rate 100000
```

显示 sFlow 的配置信息。

```
[Switch-GigabitEthernet1/0/1] display sflow
```

```
sFlow Global Information:
```

```
Agent IP:3.3.3.1
```

```
Collector IP:3.3.3.2 Port: 6343
```

```
Interval(s): 30
```

```
sFlow Port Information:
```

Interface	Direction	Rate	Mode	Status

GE1/0/1	Inbound	100000	Random	Active

1.1.5 完整配置

```
#
```

```
sflow agent ip 3.3.3.1
```

```
sflow collector ip 3.3.3.2
```

```
sflow interval 30
```

```
#
```

```
interface GigabitEthernet1/0/1
```

```
sflow enable inbound
```

```
sflow sampling-rate 100000
```

```
#
```

1.1.6 配置注意事项

需要注意的是：

- 目前设备不支持配置 **sflow sampling-mode determine** 命令，即不支持配置 sFlow 的采样模式为 **determine**。
- 目前设备只支持 sFlow Agent 功能，并且仅支持配置一个 sFlow Agent IP 地址。
- 目前设备支持配置两个 sFlow Collector，并且两个 sFlow Collector 不允许配置相同的地址；配置两个 Collector 目的是启用一个 sFlow Collector 作为冗余备份，交换机发送 sFlow 报文时同时向两个 sFlow Collector 发送。
- sFlow Agent 和 sFlow Collector 不能配置相同的 IP 地址。
- sFlow Agent 的 IP 地址可以配置为本设备上 LoopBack 接口的 IP 地址。
- 如果用户需要对聚合端口开启 sFlow 功能，则必须在聚合组内各端口下分别配置。

目 录

- 1 SSL-HTTPS典型配置指导 1-1
 - 1.1 SSL-HTTPS典型配置指导..... 1-1
 - 1.1.1 组网图 1-1
 - 1.1.2 应用要求 1-1
 - 1.1.3 适用产品、版本 1-2
 - 1.1.4 配置过程和解释 1-2
 - 1.1.5 完整配置 1-3
 - 1.1.6 配置注意事项 1-3

1 SSL-HTTPS 典型配置指导

1.1 SSL-HTTPS 典型配置指导

SSL（Secure Sockets Layer，安全套接层）是一个安全协议，为基于 TCP 的应用层协议提供安全连接，如 SSL 可以为 HTTP 协议提供安全连接，即 HTTPS（HTTP Security，HTTP 安全）。

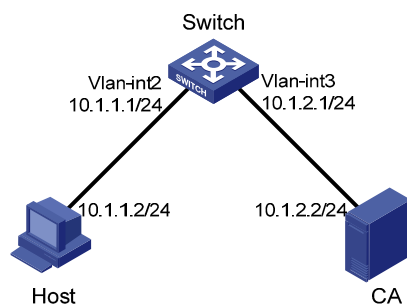
对于支持 Web 网管功能的交换机，开启 HTTP 服务后，交换机可以作为 Web 服务器，允许用户通过 HTTP 协议登录，并利用 Web 页面实现对交换机的访问和控制。但是 HTTP 协议本身不能对 Web 服务器的身份进行验证，也不能保证数据传输的私密性，无法提供安全性保证。为此，将 HTTP 和 SSL 结合，通过 SSL 对客户端身份和服务器进行验证，对传输的数据进行加密，从而实现对设备的安全管理。

HTTPS 通过 SSL 协议，从以下几方面提高了设备的安全性：

- 通过 SSL 协议保证合法客户端可以安全地访问设备，禁止非法的客户端访问设备；
- 客户端与设备之间交互的数据需要经过加密，保证了数据传输的安全性和完整性，从而实现了设备的安全管理；
- 为设备制定基于证书属性的访问控制策略，对客户端的访问权限进行控制，进一步避免了非法客户对设备进行攻击。

1.1.1 组网图

图1-1 SSL-HTTPS 典型配置网图



1.1.2 应用要求

- Switch 作为 HTTPS 服务器；
- Host 作为 HTTPS 客户端，通过基于 SSL 的 HTTP 协议访问 HTTPS 服务器；
- CA（Certification Authority，认证机构）为 Switch 颁发证书。



注意

本配置举例中，采用 Windows Server 作为 CA，在 CA 上需要安装 SCEP（Simple Certificate Enrollment Protocol，简单证书注册协议）插件。

1.1.3 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5500-SI 系列以太网交换机	Release 1207 软件版本	全系列硬件版本 (除 S5500-20TP-SI)
	Release 1301 软件版本	S5500-20TP-SI
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.1.4 配置过程和解释

(1) 为 Switch 申请证书

配置 PKI 实体。

```
<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en] common-name http-server1
[Sysname-pki-entity-en] fqdn ssl.security.com
[Sysname-pki-entity-en] quit
```

配置 PKI 域。

```
[Sysname] pki domain 1
[Sysname-pki-domain-1] ca identifier ca1
[Sysname-pki-domain-1] certificate request url http://10.1.2.2/certsrv/mscep/mscep.dll
[Sysname-pki-domain-1] certificate request from ra
[Sysname-pki-domain-1] certificate request entity en
[Sysname-pki-domain-1] quit
```

用 RSA 算法生成本地的密钥对。

```
[Sysname] public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits of the modulus[default = 1024]:
Generating Keys...
.....++++++
.....++++++
.....++++++
....++++++
.....
```

从 CA 获取服务器证书。

```
[Sysname] pki retrieval-certificate ca domain 1
```

本地证书申请。

```
[Sysname] pki request-certificate domain 1
```

(2) 配置 HTTPS 服务使用的 SSL 服务器端策略

创建一个名为 myssl 的 SSL 服务器端策略。

```
[Sysname] ssl server-policy myssl
```

配置 SSL 服务器端策略使用的 PKI 域名为 1。

```
[Sysname-ssl-server-policy-mysl] pki-domain 1
```

配置服务器端需要认证客户端。

```
[Sysname-ssl-server-policy-mysl] client-verify enable
```

```
[Sysname-ssl-server-policy-mysl] quit
```

(3) 配置 HTTPS 服务与 SSL 服务器端策略关联，并使能 HTTPS 服务

配置 HTTPS 服务使用的 SSL 策略为 myssl。

```
[Sysname] ip https ssl-server-policy myssl
```

使能 HTTPS 服务。

```
[Sysname] ip https enable
```

(4) 验证配置结果

在 Host 上打开 IE 浏览器，输入网址 https://10.1.1.1，可以登录 Switch，并实现对 Switch 的控制。

1.1.5 完整配置

```
#
pki entity en
    common-name http-server1
    fqdn ssl.security.com
#
pki domain 1
    ca identifier ca1
    certificate request url http://10.1.2.2/certsrv/mscep/mscep.dll
    certificate request from ra
    certificate request entity en
#
ssl server-policy myssl
    pki-domain 1
    client-verify enable
#
ip https ssl-server-policy myssl
#
```

1.1.6 配置注意事项

- 在进行 SSL 服务器端策略配置之前，需要先配置 PKI（Public Key Infrastructure，公钥基础设施）域。

- 如果服务器端需要对客户端进行基于证书的身份验证，即配置了 **client-verify enable** 命令，而 SSL 客户端的证书不存在或不能被信任，则必须先为 SSL 客户端申请并安装证书。
- 如果服务器端证书不能被信任，请在 SSL 客户端安装为 SSL 服务器颁发证书的 CA 服务器根证书，或服务器向 SSL 客户端信任的 CA 服务器重新申请证书。
- 使用 **display ssl server-policy** 命令查看 SSL 服务器端策略支持的加密套件。如果 SSL 服务器端和客户端支持的加密套件不匹配，请用 **ciphersuite** 命令修改 SSL 服务器支持的加密套件。
- 关闭 HTTPS 服务后，将自动取消 HTTPS 服务与 SSL 服务器端策略的关联。再次使能 HTTPS 服务之前，需要重新配置 HTTPS 服务与 SSL 服务器端策略关联。
- 使能 HTTPS 服务，会触发 SSL 的握手协商过程。在 SSL 握手协商过程中，如果设备的本地证书已经存在，则 SSL 协商可以成功，HTTPS 服务可以正常启动；如果设备的本地证书不存在，则 SSL 协商过程会触发证书申请流程。由于证书申请需要较长的时间，会导致 SSL 协商不成功，从而无法正常启动 HTTPS 服务。因此，在这种情况下，需要多次执行 **ip https enable** 命令，这样 HTTPS 服务才能正常启动。

目 录

1 PKI典型配置指导	1-1
1.1 PKI实体向CA申请证书典型配置指导（方式一）	1-1
1.1.1 组网图	1-1
1.1.2 应用要求	1-1
1.1.3 适用产品、版本	1-1
1.1.4 配置过程和解释	1-2
1.1.5 完整配置	1-4
1.1.6 配置注意事项	1-5
1.2 PKI实体向CA申请证书典型配置指导（方式二）	1-5
1.2.1 组网图	1-5
1.2.2 应用要求	1-5
1.2.3 适用产品、版本	1-6
1.2.4 配置过程和解释	1-6
1.2.5 完整配置	1-9
1.2.6 配置注意事项	1-9
1.3 证书属性的访问控制策略应用典型配置指导	1-9
1.3.1 组网图	1-10
1.3.2 应用要求	1-10
1.3.3 适用产品、版本	1-10
1.3.4 配置过程和解释	1-10
1.3.5 完整配置	1-12
1.3.6 配置注意事项	1-12

1 PKI 典型配置指导

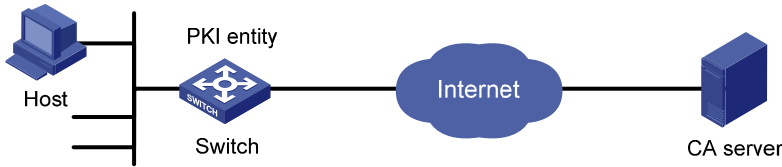
1.1 PKI 实体向 CA 申请证书典型配置指导（方式一）

PKI（Public Key Infrastructure，公钥基础设施）是通过使用公开密钥技术和数字证书来确保系统信息安全，并负责验证数字证书持有者身份的一种体系。

PKI 的功能是通过签发数字证书来绑定证书持有者的身份和相关的公开密钥，为用户获取证书、访问证书和宣告证书作废提供了方便的途径。同时利用数字证书及相关的各种服务（证书发布、黑名单发布等）实现通信过程中各实体的身份认证，保证了通信数据的机密性、完整性和不可否认性。

1.1.1 组网图

图1-1 PKI 实体向 CA 申请证书组网图（方式一）



1.1.2 应用要求



说明

本配置举例中，CA 服务器上采用 RSA Keon 软件。

在作为 PKI 实体的设备 Switch 上进行相关配置，实现以下需求：

- 设备向 CA 服务器申请本地证书
- 获取 CRL 为证书验证做准备

1.1.3 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5500-SI 系列以太网交换机	Release 1207 软件版本	全系列硬件版本 (除 S5500-20TP-SI)
	Release 1301 软件版本	S5500-20TP-SI
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.1.4 配置过程和解释

- CA 服务器端的配置

(1) 创建 CA 服务器 myca

在本例中，CA 服务器上首先需要进行基本属性 Nickname 和 Subject DN 的配置。其它属性选择默认值。其中，Nickname 为可信任的 CA 名称，Subject DN 为 CA 的 DN 属性，包括 CN、OU、O 和 C。

(2) 配置扩展属性

基本属性配置完毕之后，还需要在生成的 CA 服务器管理页面上对“Jurisdiction Configuration”进行配置，主要内容包括：根据需要选择合适的扩展选项；启动自动颁发证书功能；添加可以自动颁发证书的地址范围。

(3) 配置 CRL 发布

CA 服务器的基本配置完成之后，需要进行 CRL 的相关配置。

本例中选择 CRL 的发布方式为 HTTP，自动生成 CRL 发布点的 URL 为 `http://4.4.4.133:447/myca.crl`。

以上配置完成之后，还需要保证设备的系统时钟与 CA 的时钟同步才可以正常使用设备来申请证书和获取 CRL。

- 设备 Switch 上的配置

(4) 配置实体命名空间

配置实体名称为 aaa，通用名为 Switch。

```
<Switch> system-view
[Switch] pki entity aaa
[Switch-pki-entity-aaa] common-name Switch
[Switch-pki-entity-aaa] quit
```

(5) 配置 PKI 域参数

创建并进入 PKI 域 torsa。

```
[Switch] pki domain torsa
```

配置可信任的 CA 名称为 myca。

```
[Switch-pki-domain-torsa] ca identifier myca
```

配置注册服务器 URL，格式为 `http://host:port/Issuing Jurisdiction ID`。其中的 Issuing Jurisdiction ID 为 CA 服务器上生成的 16 进制字符串。

```
[Switch-pki-domain-torsa] certificate request url
http://4.4.4.133:446/c95e970f632d27be5e8cbf80e971d9c4a9a93337
```

配置证书申请的注册受理机构为 CA。

```
[Switch-pki-domain-torsa] certificate request from ca
```

指定实体名称为 aaa。

```
[Switch-pki-domain-torsa] certificate request entity aaa
```

配置 CRL 发布点位置。

```
[Switch-pki-domain-torsa] crl url http://4.4.4.133:447/myca.crl
[Switch-pki-domain-torsa] quit
```

(6) 用 RSA 算法生成本地密钥对

```
[Switch] public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
       It may take a few minutes.
Press CTRL+C to abort.
Input the bits in the modulus [default = 1024]:
Generating keys...
.....+++++
.....+++++
.....+++++
.....+++++
.
```

(7) 证书申请

获取 CA 证书并下载至本地。

```
[Switch] pki retrieval-certificate ca domain torsa
Retrieving CA/RA certificates. Please wait a while.....
The trusted CA's finger print is:
    MD5  fingerprint:EDE9 0394 A273 B61A F1B3 0072 A0B1 F9AB
    SHA1 fingerprint: 77F9 A077 2FB8 088C 550B A33C 2410 D354 23B2 73A8
```

Is the finger print correct?(Y/N):y

```
Saving CA/RA certificates chain, please wait a moment.....
CA certificates retrieval success.
```

获取 CRL 并下载至本地。

```
[Switch] pki retrieval-crl domain torsa
Connecting to server for retrieving CRL. Please wait a while....
CRL retrieval success!
```

手工申请本地证书。

```
[Switch] pki request-certificate domain torsa challenge-word
Certificate is being requested, please wait.....
Enrolling the local certificate, please wait a while.....
Certificate request Successfully!
Saving the local certificate to device.....
Done!
```

(8) 验证配置结果

通过以下显示命令可以查看获取的本地证书信息。

```
<Switch> display pki certificate local domain torsa
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            9A96A48F 9A509FD7 05FFF4DF 104AD094
        Signature Algorithm: sha1WithRSAEncryption
```

```

Issuer:
  C=cn
  O=org
  OU=test
  CN=myca
Validity
  Not Before: Jan  8 09:26:53 2007 GMT
  Not After : Jan  8 09:26:53 2008 GMT
Subject:
  CN=Switch
Subject Public Key Info:
  Public Key Algorithm: rsaEncryption
  RSA Public Key: (1024 bit)
    Modulus (1024 bit):
      00D67D50 41046F6A 43610335 CA6C4B11
      F8F89138 E4E905BD 43953BA2 623A54C0
      EA3CB6E0 B04649CE C9CDDD38 34015970
      981E96D9 FF4F7B73 A5155649 E583AC61
      D3A5C849 CBDE350D 2A1926B7 0AE5EF5E
      D1D8B08A DBF16205 7C2A4011 05F11094
      73EB0549 A65D9E74 0F2953F2 D4F0042F
      19103439 3D4F9359 88FB59F3 8D4B2F6C
      2B
    Exponent: 65537 (0x10001)
  X509v3 extensions:
    X509v3 CRL Distribution Points:
      URI:http://4.4.4.133:447/myca.crl

  Signature Algorithm: sha1WithRSAEncryption
      836213A4 F2F74C1A 50F4100D B764D6CE
      B30C0133 C4363F2F 73454D51 E9F95962
      EDE9E590 E7458FA6 765A0D3F C4047BC2
      9C391FF0 7383C4DF 9A0CCFA9 231428AF
      987B029C C857AD96 E4C92441 9382E798
      8FCC1E4A 3E598D81 96476875 E2F86C33
      75B51661 B6556C5E 8F546E97 5197734B
      C8C29AC7 E427C8E4 B9AAF5AA 80A75B3C

```

关于获取的 CA 证书及 CRL 文件的详细信息可以通过相应的显示命令来查看，此处略。具体内容请参考命令 **display pki certificate ca domain** 和 **display pki crl domain**。

1.1.5 完整配置

```

#
pki entity aaa
  common-name Switch
#
pki domain torsa
  ca identifier myca
  certificate request url http://4.4.4.133:446/c95e970f632d27be5e8cbf80e971d9c4a9a93337

```

```
certificate request from ca
certificate request entity aaa
crl url http://4.4.4.133:447/myca.crl
#
```

1.1.6 配置注意事项

- 当采用 RSA Keon 软件时，不需要安装 SCEP 插件。此时，配置 PKI domain 时，需要使用 **certificate request from ca** 命令指定实体从 CA 注册申请证书。
- 若本地证书已存在，为保证密钥对与现存证书的一致性，不应执行创建密钥对命令，必须在删除本地证书后再执行 **public-key local create rsa** 命令生成新的密钥对。
- 如果本地证书已存在，则不允许再执行证书申请操作，以避免因相关配置的修改使得证书与注册信息不匹配。若想重新申请，请先使用 **pki delete-certificate** 命令删除存储于本地的 CA 证书与本地证书，然后再执行 **pki request-certificate domain** 命令。
- 当无法通过 SCEP 协议向 CA 在线申请证书时，可以使用可选参数 **pkcs10** 打印出本地的证书申请信息。用户保存证书申请信息，并将其通过带外方式发送给 CA 进行证书申请。
- 证书申请之前必须保证实体时钟与 CA 的时钟同步，否则申请证书的有效期会出现异常。

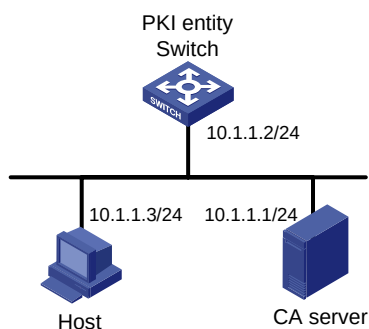
1.2 PKI 实体向 CA 申请证书典型配置指导（方式二）

PKI（Public Key Infrastructure，公钥基础设施）是通过使用公开密钥技术和数字证书来确保系统信息安全，并负责验证数字证书持有者身份的一种体系。

PKI 的功能是通过签发数字证书来绑定证书持有者的身份和相关的公开密钥，为用户获取证书、访问证书和宣告证书作废提供了方便的途径。同时利用数字证书及相关的各种服务（证书发布、黑名单发布等）实现通信过程中各实体的身份认证，保证了通信数据的机密性、完整性和不可否认性。

1.2.1 组网图

图1-2 PKI 实体向 CA 申请证书组网图（方式二）



1.2.2 应用要求



说明

本配置举例中，采用 Windows 2003 server 做 CA 服务器。

配置 PKI 实体 Switch 向 CA 服务器申请本地证书。

1.2.3 适用产品、版本

表1-2 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5500-SI 系列以太网交换机	Release 1207 软件版本	全系列硬件版本 (除 S5500-20TP-SI)
	Release 1301 软件版本	S5500-20TP-SI
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.2.4 配置过程和解释

- CA 服务器端的配置

- (1) 安装证书服务器组件

打开[控制面板]/[添加/删除程序]，选择[添加/删除 Windows 组件]中的“证书服务”进行安装。

- (2) 安装 SCEP 插件

由于 Windows 2003 server 作为 CA 服务器时，缺省情况下不支持 SCEP，所以需要安装 SCEP 插件，才能使设备具备证书自动注册、获取等功能。插件安装完毕后，弹出提示框，提示框中的 URL 地址即为设备上配置的注册服务器地址。

- (3) 修改证书服务的属性

完成上述配置后，打开[控制面板/管理工具]中的[证书颁发机构]，如果安装成功，在[颁发的证书]中将存在两个 CA 颁发给 RA 的证书。选择[CA server 属性]中的“策略模块”的属性为“如果可以的话，按照证书模板中的设置。否则，将自动颁发证书(F)。”

- (4) 修改 IIS 服务的属性

打开[控制面板/管理工具]中的[Internet 信息服务(IIS)管理器]，将[默认网站 属性]中“主目录”的本地路径修改为证书服务保存的路径。另外，为了避免与已有的服务冲突，建议修改默认网站的 TCP 端口号为未使用的端口号。

以上配置完成之后，还需要保证设备的系统时钟与 CA 的时钟同步才可以正常使用设备来申请证书。

- 设备 Switch 上的配置

- (1) 配置实体命名空间

配置实体名称为 aaa，通用名为 Switch。

```
<Switch> system-view
[Switch] pki entity aaa
[Switch-pki-entity-aaa] common-name Switch
[Switch-pki-entity-aaa] quit
```

- (2) 配置 PKI 域参数

创建并进入 PKI 域 torsa。

```
[Switch] pki domain torsa
```

配置可信任的 CA 名称为 myca。

```
[Switch-pki-domain-torsa] ca identifier myca
```

配置注册服务器 URL，格式为 http://host:port/ certsrv/mscep/mscep.dll。其中，host:port 为 CA 服务器的主机地址和端口号。

```
[Switch-pki-domain-torsa] certificate request url
http://10.1.1.1:8080/certsrv/mscep/mscep.dll
```

配置证书申请的注册受理机构为 RA。

```
[Switch-pki-domain-torsa] certificate request from ra
```

指定实体名称为 aaa。

```
[Switch-pki-domain-torsa] certificate request entity aaa
```

(3) 用 RSA 算法生成本地密钥对

```
[Switch] public-key local create rsa
```

The range of public key size is (512 ~ 2048).

NOTES: If the key modulus is greater than 512,

It may take a few minutes.

Press CTRL+C to abort.

Input the bits in the modulus [default = 1024]:

Generating keys...

.....+++++

.....+++++

.....+++++

.....+++++

.

(4) 证书申请

获取 CA 证书并下载至本地。

```
[Switch] pki retrieval-certificate ca domain torsa
```

Retrieving CA/RA certificates. Please wait a while.....

The trusted CA's finger print is:

MD5 fingerprint:766C D2C8 9E46 845B 4DCE 439C 1C1F 83AB

SHA1 fingerprint:97E5 DDED AB39 3141 75FB DB5C E7F8 D7D7 7C9B 97B4

Is the finger print correct?(Y/N):y

Saving CA/RA certificates chain, please wait a moment.....

CA certificates retrieval success.

手工申请本地证书。

```
[Switch] pki request-certificate domain torsa challenge-word
```

Certificate is being requested, please wait.....

Enrolling the local certificate, please wait a while.....

Certificate request Successfully!

Saving the local certificate to device.....

Done!

1. 验证配置结果

通过以下显示命令可以查看获取的本地证书信息。

```
<Switch> display pki certificate local domain torsa
```

Certificate:

Data:

Version: 3 (0x2)

Serial Number:

48FA0FD9 00000000 000C

Signature Algorithm: sha1WithRSAEncryption

Issuer:

C=US

CN=CA server

Validity

Not Before: Nov 21 12:32:16 2007 GMT

Not After : Nov 21 12:42:16 2008 GMT

Subject:

CN=Switch

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)

Modulus (1024 bit):

00A6637A 8CDEA1AC B2E04A59 F7F6A9FE

5AEE52AE 14A392E4 E0E5D458 0D341113

0BF91E57 FA8C67AC 6CE8FEBB 5570178B

10242FDD D3947F5E 2DA70BD9 1FAF07E5

1D167CE1 FC20394F 476F5C08 C5067DF9

CB4D05E6 55DC11B6 9F4C014D EA600306

81D403CF 2D93BC5A 8AF3224D 1125E439

78ECEFE1 7FA9AE7B 877B50B8 3280509F

6B

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Subject Key Identifier:

B68E4107 91D7C44C 7ABCE3BA 9BF385F8 A448F4E1

X509v3 Authority Key Identifier:

keyid:9D823258 EADFEFA2 4A663E75 F416B6F6 D41EE4FE

DirName:CN=CA server,C=US

serial:3E02B7AA C80BBE8C 49899FD7 E5854B31

X509v3 CRL Distribution Points:

URI:http://l00192b/CertEnroll/CA%20server.crl

URI:file://\l00192b\CertEnroll\CA server.crl

Authority Information Access:

CA Issuers - URI:http://l00192b/CertEnroll/l00192b_CA%20server.crt

CA Issuers - URI:file://\l00192b\CertEnroll\l00192b_CA server.crt

```
1.3.6.1.4.1.311.20.2:  
 .0.I.P.S.E.C.I.n.t.e.r.m.e.d.i.a.t.e.0.f.f.l.i.n.e  
Signature Algorithm: sha1WithRSAEncryption  
81029589 7BFA1CBD 20023136 B068840B  
..... (略)
```

关于获取的 CA 证书的详细信息可以通过相应的显示命令来查看，此处略。具体内容请参考命令 **display pki certificate ca domain**。

1.2.5 完整配置

```
#  
pki entity aaa  
common-name Switch  
#  
pki domain torsa  
ca identifier myca  
certificate request url http://10.1.1.1:8080/certsrv/mscep/mscep.dll  
certificate request from ra  
certificate request entity aaa  
#
```

1.2.6 配置注意事项

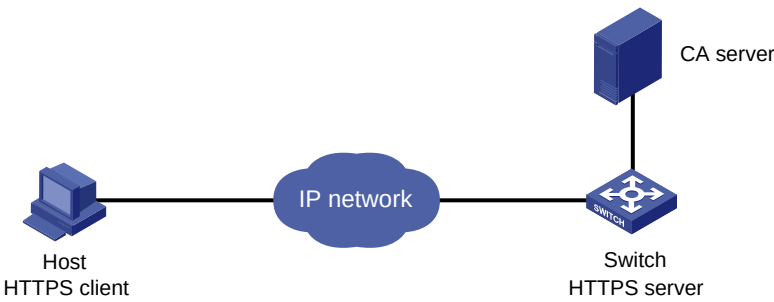
- 当采用 Windows Server 作为 CA 时，需要安装 SCEP 插件。此时，配置 PKI domain 时，需要使用 **certificate request from ra** 命令指定实体从 RA 注册申请证书。
- Windows 2000 CA 服务器对证书申请的数据长度有一定的限制。实体 DN 配置项超过一定数据长度时，申请证书没有回应。
- 若本地证书已存在，为保证密钥对与现存证书的一致性，不应执行创建密钥对命令，必须在删除本地证书后再执行 **public-key local create rsa** 命令生成新的密钥对。
- 如果本地证书已存在，则不允许再执行证书申请操作，以避免因相关配置的修改使得证书与注册信息不匹配。若想重新申请，请先使用 **pki delete-certificate** 命令删除存储于本地的 CA 证书与本地证书，然后再执行 **pki request-certificate domain** 命令。
- 当无法通过 SCEP 协议向 CA 在线申请证书时，可以使用可选参数 **pkcs10** 打印出本地的证书申请信息。用户保存证书申请信息，并将其通过带外方式发送给 CA 进行证书申请。
- 证书申请之前必须保证实体时钟与 CA 的时钟同步，否则申请证书的有效期会出现异常。

1.3 证书属性的访问控制策略应用典型配置指导

通过配置证书属性的访问控制策略，可以对用户的访问权限进行进一步的控制，保证了与之通信的服务器的安全性。

1.3.1 组网图

图1-3 证书属性的访问控制策略应用组网图



1.3.2 应用要求



说明

本配置举例中，CA 服务器上采用 RSA Keon 软件。

- 客户端通过 HTTPS（HTTP Security，HTTP 安全）协议远程访问设备（HTTPS 服务器）。
- 通过 SSL 协议保证合法客户端安全登录 HTTPS 服务器。
- 为 HTTPS 服务器制定证书属性的访问控制策略，对客户端的访问权限进行控制。

1.3.3 适用产品、版本

表1-3 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S3610 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5510 系列以太网交换机	Release 5301, Release 5303 软件版本	全系列硬件版本
S5500-SI 系列以太网交换机	Release 1207 软件版本	全系列硬件版本 (除 S5500-20TP-SI)
	Release 1301 软件版本	S5500-20TP-SI
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S3500-EA 系列以太网交换机	Release 5303 软件版本	全系列硬件版本

1.3.4 配置过程和解释



说明

SSL 策略所引用的 PKI 域必须首先创建。

(1) 配置 PKI 域参数

创建并进入 PKI 域 `torsa`。

```
[Switch] pki domain torsa
```

配置可信任的 CA 名称为 myca。

```
[Switch-pki-domain-torsa] ca identifier myca
```

配置注册服务器 URL，格式为 http://host:port/Issuing Jurisdiction ID。其中的 Issuing Jurisdiction ID 为 CA 服务器上生成的 16 进制字符串。

```
[Switch-pki-domain-torsa] certificate request url
http://4.4.4.133:446/c95e970f632d27be5e8cbf80e971d9c4a9a93337
```

配置证书申请的注册受理机构为 CA。

```
[Switch-pki-domain-torsa] certificate request from ca
```

指定实体名称为 aaa。

```
[Switch-pki-domain-torsa] certificate request entity aaa
```

配置 CRL 发布点位置。

```
[Switch-pki-domain-torsa] crl url http://4.4.4.133:447/myca.crl
```

```
[Switch-pki-domain-torsa] quit
```

(2) 配置 HTTPS 服务器

配置 HTTPS 服务器使用的 SSL 策略。

```
<Switch> system-view
```

```
[Switch] ssl server-policy myssl
```

```
[Switch-ssl-server-policy-myssl] pki-domain torsa
```

```
[Switch-ssl-server-policy-myssl] client-verify enable
```

```
[Switch-ssl-server-policy-myssl] quit
```

(3) 配置证书属性组

配置证书属性组 mygroup1，并创建两个属性规则。规则 1 定义证书主题名的 DN 包含字符串 aabbcc；规则 2 定义证书颁发者名中的 IP 地址等于 10.0.0.1。

```
[Switch] pki certificate attribute-group mygroup1
```

```
[Switch-pki-cert-attribute-group-mygroup1] attribute 1 subject-name dn ctn aabbcc
```

```
[Switch-pki-cert-attribute-group-mygroup1] attribute 2 issuer-name ip equ 10.0.0.1
```

```
[Switch-pki-cert-attribute-group-mygroup1] quit
```

配置证书属性组 mygroup2，并创建两个属性规则。规则 1 定义证书备用主题名中的 FQDN 不包含字符串 apple；规则 2 定义证书颁发者名的 DN 包含字符串 aabbcc。

```
[Switch] pki certificate attribute-group mygroup2
```

```
[Switch-pki-cert-attribute-group-mygroup2] attribute 1 alt-subject-name fqdn nctn apple
```

```
[Switch-pki-cert-attribute-group-mygroup2] attribute 2 issuer-name dn ctn aabbcc
```

```
[Switch-pki-cert-attribute-group-mygroup2] quit
```

(4) 配置证书访问控制策略

配置访问控制策略 myacp，并建立两个控制规则。

```
[Switch] pki certificate access-control-policy myacp
```

```
[Switch-pki-cert-acp-myacp] rule 1 deny mygroup1
```

```
[Switch-pki-cert-acp-myacp] rule 2 permit mygroup2
```

```
[Switch-pki-cert-acp-myacp] quit
```

(5) 配置 HTTPS 服务器与相关策略进行关联，并启动 HTTPS 服务器

配置指定 HTTPS 服务器的 SSL 策略为 myssl。

```
[Switch] ip https ssl-server-policy myssl
# 配置指定 HTTPS 服务器的证书访问控制策略为 myacp。
[Switch] ip https certificate access-control-policy myacp
# 启动 HTTPS 服务器。
[Switch] ip https enable
```

1.3.5 完整配置

```
#
pki domain torsa
  ca identifier myca
  certificate request url http://4.4.4.133:446/c95e970f632d27be5e8cbf80e971d9c4a9a93337
  certificate request from ca
  certificate request entity aaa
  crl url http://4.4.4.133:447/myca.crl
#
pki certificate attribute-group mygroup1
  attribute 1 subject-name dn ctn aabbcc
  attribute 2 issuer-name ip equ 10.0.0.1
pki certificate attribute-group mygroup2
  attribute 1 alt-subject-name fqdn nctn apple
  attribute 2 issuer-name dn ctn aabbcc
#
pki certificate access-control-policy myacp
  rule 1 deny mygroup1
  rule 2 permit mygroup2
#
ssl server-policy myssl
  pki-domain torsa
  client-verify enable
#
ip https ssl-server-policy myssl
#
ip https certificate access-control-policy myacp
#
```

1.3.6 配置注意事项

配置证书属性控制规则时，*group-name* 必须是已存在的证书属性组的名称。

目 录

1 Track典型配置指导	1-1
1.1 VRRP、Track与NQA联动典型配置指导	1-1
1.1.1 组网图	1-1
1.1.2 应用要求	1-1
1.1.3 适用产品、版本	1-1
1.1.4 配置过程和解释	1-2
1.1.5 完整配置	1-4
1.1.6 配置注意事项	1-5
1.1.7 组网图	1-5
1.1.8 应用要求	1-6
1.1.9 适用产品、版本	1-6
1.1.10 配置过程和解释	1-6
1.1.11 完整配置	1-8
1.1.12 配置注意事项	1-8

1 Track 典型配置指导

1.1 VRRP、Track 与 NQA 联动典型配置指导

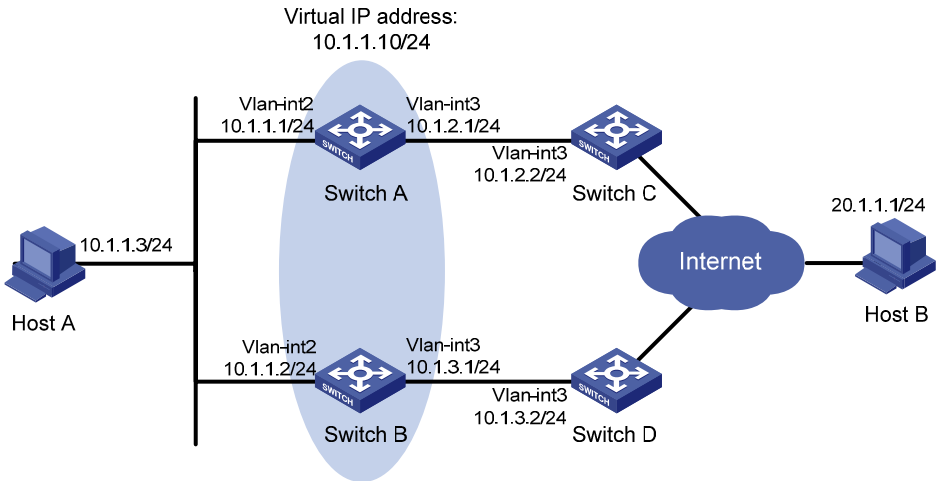
Track 的用途是实现联动功能。

联动功能由应用模块、Track 模块和监测模块三部分组成。联动功能是指通过建立联动项，实现不同模块之间的联动，即由监测模块通过 Track 模块触发应用模块执行某种操作。监测模块负责对链路状态、网络性能等进行探测，并通过 Track 模块将探测结果通知给应用模块。应用模块感知到网络状态的变化后，及时进行相应的处理，从而避免通信的中断或服务质量的降低。

Track 模块位于应用模块和监测模块之间，主要功能是屏蔽不同监测模块的差异，为应用模块提供统一的接口。

1.1.1 组网图

图1-1 VRRP、Track 与 NQA 联动配置组网图



1.1.2 应用要求

- Host A 需要访问 Internet 上的 Host B，Host A 的缺省网关为 10.1.1.10/24；
- Switch A 和 Switch B 属于虚拟 IP 地址为 10.1.1.10 的备份组 1；
- 当 Switch A 正常工作时，Host A 发送给 Host B 的报文通过 Switch A 转发；当通过 NQA 监测到 Switch A 上行链路不通时，Host A 发送给 Host B 的报文通过 Switch B 转发。

1.1.3 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S5500-SI 系列以太网交换机	Release 1207 软件版本	全系列硬件版本 (除 S5500-20TP-SI)
	Release 1301 软件版本	S5500-20TP-SI
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本

产品	软件版本	硬件版本
S7500E 系列以太网交换机	Release 6300 软件版本	全系列硬件版本

1.1.4 配置过程 and 解释

(1) 按照 图 1-1配置各接口的IP地址，具体配置过程略。

(2) 在 Switch A 上配置 NQA 测试组

```
<SwitchA> system-view
```

创建管理员名为 admin、操作标签为 test 的 NQA 测试组。

```
[SwitchA] nqa entry admin test
```

配置测试类型为 ICMP-echo。

```
[SwitchA-nqa-admin-test] type icmp-echo
```

配置目的地址为 10.1.2.2。

```
[SwitchA-nqa-admin-test-icmp-echo] destination ip 10.1.2.2
```

测试频率为 100ms。

```
[SwitchA-nqa-admin-test-icmp-echo] frequency 100
```

配置联动项 1（连续失败 5 次触发联动）。

```
[SwitchA-nqa-admin-test-icmp-echo] reaction 1 checked-element probe-fail threshold-type  
consecutive 5 action-type trigger-only
```

```
[SwitchA-nqa-admin-test-icmp-echo] quit
```

启动探测。

```
[SwitchA] nqa schedule admin test start-time now lifetime forever
```

(3) 在 Switch A 上配置 Track 项

配置 Track 项 1，关联 NQA 测试组（管理员为 admin，操作标签为 test）的联动项 1。

```
[SwitchA] track 1 nqa entry admin test reaction 1
```

(4) 在 Switch A 上配置 VRRP

创建备份组 1，并配置备份组 1 的虚拟 IP 地址为 10.1.1.10。

```
[SwitchA] interface vlan-interface 2
```

```
[SwitchA-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.10
```

设置 Switch A 在备份组 1 中的优先级为 110。

```
[SwitchA-Vlan-interface2] vrrp vrid 1 priority 110
```

设置备份组的认证方式为 SIMPLE，认证字为 hello。

```
[SwitchA-Vlan-interface2] vrrp vrid 1 authentication-mode simple hello
```

设置 Master 交换机发送 VRRP 报文的间隔时间为 5 秒。

```
[SwitchA-Vlan-interface2] vrrp vrid 1 timer advertise 5
```

设置 Switch A 工作在抢占方式，抢占延迟时间为 5 秒。

```
[SwitchA-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
```

设置监视 Track 项。


```
[SwitchA-Vlan-interface2] vrrp vrid 1 track 1 reduced 30
```

(5) 在 Switch B 上配置 VRRP

```
<SwitchB> system-view
```

```
[SwitchB] interface vlan-interface 2
```

创建备份组 1，并配置备份组 1 的虚拟 IP 地址为 10.1.1.10。

```
[SwitchB-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.10
```

设置备份组的认证方式为 SIMPLE，认证字为 hello。

```
[SwitchB-Vlan-interface2] vrrp vrid 1 authentication-mode simple hello
```

设置 Master 交换机发送 VRRP 报文的间隔时间为 5 秒。

```
[SwitchB-Vlan-interface2] vrrp vrid 1 timer advertise 5
```

设置 Switch B 工作在抢占方式，抢占延迟时间为 5 秒。

```
[SwitchB-Vlan-interface2] vrrp vrid 1 preempt-mode timer delay 5
```

(6) 验证配置结果

配置完成后，在 Host A 上可以 ping 通 Host B。通过 **display vrrp** 命令查看配置后的结果。

显示 Switch A 上备份组 1 的详细信息。

```
[SwitchA-Vlan-interface2] display vrrp verbose
```

```
IPv4 Standby Information:
Run Method      : VIRTUAL-MAC
Virtual IP Ping : Enable
Interface       : Vlan-interface2
VRID            : 1                Adver. Timer   : 5
Admin Status    : UP              State          : Master
Config Pri      : 110             Run Pri        : 110
Preempt Mode    : YES             Delay Time     : 5
Auth Type       : SIMPLE TEXT     Key            : hello
Track Object    : 1              Pri Reduced    : 0
Virtual IP      : 10.1.1.10
Virtual MAC     : 0000-5e00-0101
Master IP       : 10.1.1.1
```

显示 Switch B 上备份组 1 的详细信息。

```
[SwitchB-Vlan-interface2] display vrrp verbose
```

```
IPv4 Standby Information:
Run Method      : VIRTUAL-MAC
Virtual IP Ping : Enable
Interface       : Vlan-interface2
VRID            : 1                Adver. Timer   : 5
Admin Status    : UP              State          : Backup
Config Pri      : 100             Run Pri        : 100
Preempt Mode    : YES             Delay Time     : 5
Auth Type       : SIMPLE TEXT     Key            : hello
Virtual IP      : 10.1.1.10
Master IP       : 10.1.1.1
```

以上显示信息表示在备份组 1 中 Switch A 为 Master 交换机，Switch B 为 Backup 交换机，Host A 发送给 Host B 的报文通过 Switch A 转发。

Switch A 与 Switch C 不通时，在 Host A 上仍然可以 ping 通 Host B。通过 **display vrrp** 命令查看备份组的信息。

Switch A 与 Switch C 不通时，显示 Switch A 上备份组 1 的详细信息。

```
[SwitchA-Vlan-interface2] display vrrp verbose
IPv4 Standby Information:
Run Method      : VIRTUAL-MAC
Virtual IP Ping : Enable
Interface       : Vlan-interface2
VRID            : 1                      Adver. Timer   : 5
Admin Status    : UP                      State          : Backup
Config Pri      : 110                     Run Pri        : 80
Preempt Mode    : YES                     Delay Time     : 5
Auth Type       : SIMPLE TEXT             Key            : hello
Track Object    : 1                      Pri Reduced    : 30
Virtual IP      : 10.1.1.10
Master IP       : 10.1.1.2
```

Switch A 与 Switch C 不通时，显示 Switch B 上备份组 1 的详细信息。

```
[SwitchB-Vlan-interface2] display vrrp verbose
IPv4 Standby Information:
Run Method      : VIRTUAL-MAC
Virtual IP Ping : Enable
Interface       : Vlan-interface2
VRID            : 1                      Adver. Timer   : 5
Admin Status    : UP                      State          : Master
Config Pri      : 100                     Run Pri        : 100
Preempt Mode    : YES                     Delay Time     : 5
Auth Type       : SIMPLE TEXT             Key            : hello
Virtual IP      : 10.1.1.10
Virtual MAC     : 0000-5e00-0101
Master IP       : 10.1.1.2
```

以上显示信息表示 Switch A 与 Switch C 不通时，Switch A 的优先级降低为 80，成为 Backup 交换机，Switch B 成为 Master 交换机，Host A 发送给 Host B 的报文通过 Switch B 转发。

1.1.5 完整配置

- 配置 Switch A

```
#
vlan 2 to 3
#
interface Vlan-interface2
 ip address 10.1.1.1 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.10
 vrrp vrid 1 priority 110
 vrrp vrid 1 preempt-mode timer delay 5
 vrrp vrid 1 timer advertise 5
```

```

vrp vrid 1 track 1 reduced 30
vrp vrid 1 authentication-mode simple hello
#
interface Vlan-interface3
ip address 10.1.2.1 255.255.255.0
#
nqa entry admin test
type icmp-echo
destination ip 10.1.2.2
frequency 100
reaction 1 checked-element probe-fail threshold-type consecutive 5 action-type
trigger-only
#
track 1 nqa entry admin test reaction 1
#
nqa schedule admin test start-time now lifetime forever
#
• 配置 Switch B
#
vlan 2
#
interface Vlan-interface2
vrp vrid 1 virtual-ip 10.1.1.10
vrp vrid 1 preempt-mode timer delay 5
vrp vrid 1 timer advertise 5
vrp vrid 1 authentication-mode simple hello
#

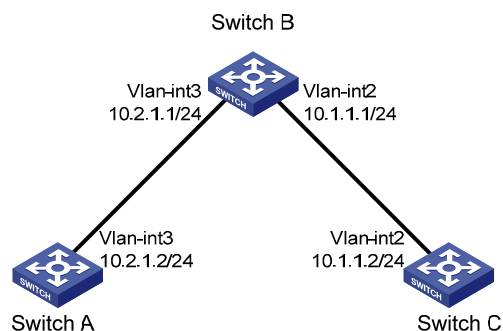
```

1.1.6 配置注意事项

- 不允许对 IP 地址拥有者进行监视指定 Track 项的配置。
- 被监视 Track 项的状态由 Negative 变为 Positive 后，对应的交换机优先级会自动恢复。
- 被监视的 Track 项可以是未创建的 Track 项。可以通过 **vrp vrid track** 命令指定监视的 Track 项后，再通过 **track** 命令创建该 Track 项。

图1-2 静态路由、Track 与 NQA 联动配置组网图静态路由、Track 与 NQA 联动配置指导

1.1.7 组网图



1.1.8 应用要求

- Switch A 到达 Switch C 的静态路由下一跳为 Switch B。
- 在 Switch A 上通过静态路由、Track 与 NQA 联动，对到达 Switch C 的静态路由有效性进行实时判断。

1.1.9 适用产品、版本

表1-2 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S5500-SI 系列以太网交换机	Release 1207 软件版本	全系列硬件版本 (除 S5500-20TP-SI)
	Release 1301 软件版本	S5500-20TP-SI
S5500-EI 系列以太网交换机	Release 2102 软件版本	全系列硬件版本
S7500E 系列以太网交换机	Release 6300 软件版本	全系列硬件版本

1.1.10 配置过程和解释

(1) 按照 图 1-2配置各接口的IP地址，具体配置过程略。

(2) 在 Switch A 上配置静态路由，并与 Track 项关联

配置到达 Switch C 的静态路由下一跳地址为 10.2.1.1，并配置静态路由与 Track 项 1 关联。

```
<SwitchA> system-view
```

```
[SwitchA] ip route-static 10.1.1.2 24 10.2.1.1 track 1
```

(3) 在 Switch A 上配置 NQA 测试组

创建管理员名为 admin、操作标签为 test 的 NQA 测试组。

```
[SwitchA] nqa entry admin test
```

配置测试类型为 ICMP-echo。

```
[SwitchA-nqa-admin-test] type icmp-echo
```

配置目的地址为 10.2.1.1。

```
[SwitchA-nqa-admin-test-icmp-echo] destination ip 10.2.1.1
```

测试频率为 100ms。

```
[SwitchA-nqa-admin-test-icmp-echo] frequency 100
```

配置联动项 1（连续失败 5 次触发联动）。

```
[SwitchA-nqa-admin-test-icmp-echo] reaction 1 checked-element probe-fail threshold-type  
consecutive 5 action-type trigger-only
```

```
[SwitchA-nqa-admin-test-icmp-echo] quit
```

启动探测。

```
[SwitchA] nqa schedule admin test start-time now lifetime forever
```

(4) 在 Switch A 上配置 Track 项

配置 Track 项 1，关联 NQA 测试组（管理员为 admin，操作标签为 test）的联动项 1。

```
[SwitchA] track 1 nqa entry admin test reaction 1
```

(5) 验证配置结果

显示 Switch A 上 Track 项的信息。

```
[SwitchA] display track all
```

```
Track ID: 1
```

```
Status: Positive
```

```
Reference object:
```

```
NQA entry: admin test
```

```
Reaction: 1
```

显示 Switch A 的路由表。

```
[SwitchA] display ip routing-table
```

```
Routing Tables: Public
```

```
Destinations : 5 Routes : 5
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
10.1.1.0/24	Static	60	0	10.2.1.1	Vlan3
10.2.1.0/24	Direct	0	0	10.2.1.2	Vlan3
10.2.1.2/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0

以上显示信息表示，NQA 测试的结果为下一跳地址 10.2.1.1 可达（Track 项状态为 Positive），配置的静态路由生效。

在 Switch B 上删除 VLAN 接口 3 的 IP 地址。

```
<SwitchB> system-view
```

```
[SwitchB] interface vlan-interface 3
```

```
[SwitchB-Vlan-interface3] undo ip address
```

显示 Switch A 上 Track 项的信息。

```
[SwitchA] display track all
```

```
Track ID: 1
```

```
Status: Negative
```

```
Reference object:
```

```
NQA entry: admin test
```

```
Reaction: 1
```

显示 Switch A 的路由表。

```
[SwitchA] display ip routing-table
```

```
Routing Tables: Public
```

```
Destinations : 4 Routes : 4
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
10.2.1.0/24	Direct	0	0	10.2.1.2	Vlan3
10.2.1.2/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0

以上显示信息表示，NQA 测试的结果为下一跳地址 10.2.1.1 不可达（Track 项状态为 Negative），配置的静态路由无效。

1.1.11 完整配置

- 配置 Switch A

```
#
vlan 3
#
interface Vlan-interface3
 ip address 10.2.1.2 255.255.255.0
#
nqa entry admin test
 type icmp-echo
 destination ip 10.2.1.1
 frequency 100
 reaction 1 checked-element probe-fail threshold-type consecutive 5 action-type
 trigger-only
#
ip route-static 10.1.1.0 255.255.255.0 10.2.1.1 track 1
#
track 1 nqa entry admin test reaction 1
#
nqa schedule admin test start-time now lifetime forever
#
```

1.1.12 配置注意事项

无

目 录

1 EPON-OLT典型配置指导.....	1-1
1.1 OLT典型配置指导.....	1-1
1.1.1 OLT端口隔离典型配置指导	1-1
1.1.2 光纤备份典型配置指导	1-2
1.1.3 IP Source Guard绑定典型配置指导	1-6
1.2 ONU远程管理典型配置指导	1-8
1.2.1 ONU和ONU端口的绑定典型配置指导	1-8
1.2.2 配置ONU的RSTP典型配置指导	1-10
1.2.3 IGMP Snooping模式下的组播典型配置指导	1-11
1.2.4 可控组播模式下的组播典型配置指导	1-13
1.2.5 升级ONU典型配置指导	1-16
1.3 UNI端口典型配置指导	1-19
1.3.1 UNI端口优先级重标记配置举例	1-19

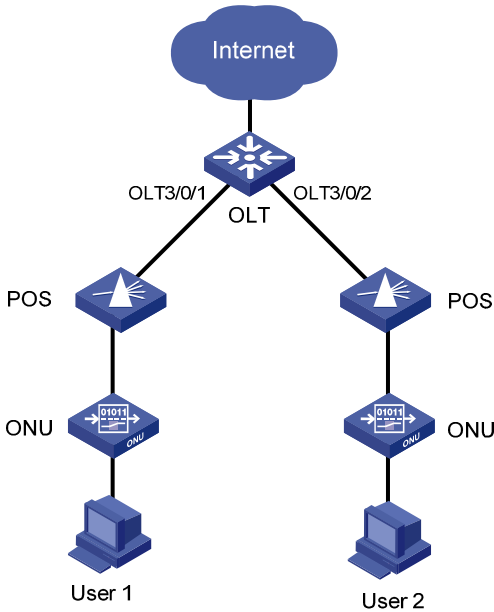
1 EPON-OLT 典型配置指导

1.1 OLT 典型配置指导

1.1.1 OLT 端口隔离典型配置指导

1. 组网图

图1-1 端口隔离组网示意图



2. 应用要求

- OLT 设备通过上行口与外部网络相连;
- 将端口 OLT3/0/1 和 OLT3/0/2 进行端口隔离,使其中两 OLT 端口下的用户彼此之间二层报文不能互通,但可以和外部网络通信。

3. 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S7500E 系列以太网交换机	Release 6300 软件版本	全系列硬件版本

4. 配置过程 and 解释

将端口 OLT3/0/1 和 OLT3/0/2 加入隔离组。

```
<Sysname> system-view
[Sysname] interface olt3/0/1
[Sysname-Olt3/0/1] port-isolate enable
[Sysname-Olt3/0/1] quit
[Sysname] interface olt3/0/2
```



```
[Sysname-Olt3/0/2] port-isolate enable
```

```
[Sysname-Olt3/0/2] quit
```

显示隔离组中的信息。

```
<Sysname> display port-isolate group
```

```
Port-isolate group information:
```

```
Uplink port support: NO
```

```
Group ID: 1
```

```
olt3/0/1 olt3/0/2
```

5. 完整配置

```
#
```

```
interface Olt3/0/1
```

```
port-isolate enable
```

```
#
```

```
interface Olt3/0/2
```

```
port-isolate enable
```

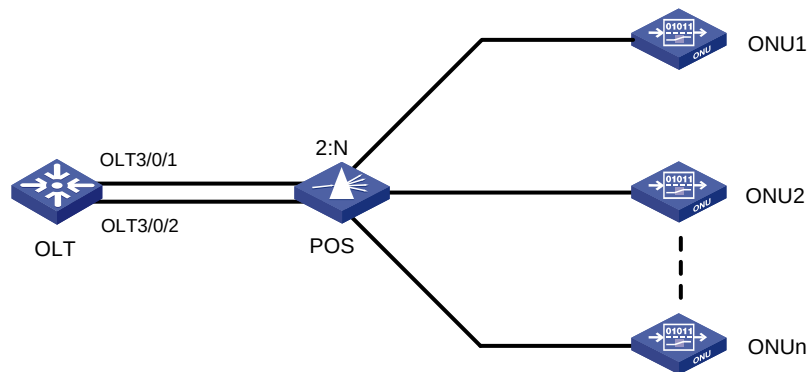
6. 配置注意事项

无

1.1.2 光纤备份典型配置指导

1. 组网图

图1-2 光纤备份配置网示意图



2. 应用要求

- S7500E 交换机作为 OLT 设备，通过两条光纤连接到一个 POS（Passive Optical Splitter，无源光纤分支器）设备，POS 连接下面多个 ONU 设备。
- 为提高服务可靠性，需要在 S7500E 上配置光纤备份功能，将两个接有光纤的 OLT 端口配置为一个光纤备份组，在某一条光纤出现故障时，交换机可以自动将业务切换至备份光纤上；在日常维护中，用户可以将业务手工切换到备份光纤，以便进行主用光纤的维护和检修。

3. 适用产品、版本

表1-2 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S7500E 系列以太网交换机	Release 6300 软件版本	全系列硬件版本

4. 配置过程 and 解释

- 光纤备份组的配置

在进行光纤备份配置前，请首先完成 EPON OLT 和 ONU 连接的基本配置，保证 ONU 设备的正常注册和所有光纤的正常工作，具体配置请参见 S7500E 交换机的操作手册。

创建光纤备份组 1。

```
<Sysname> system-view
[Sysname] ftth
[Sysname-ftth] fiber-backup group 1
Create group 1 successfully.
```

将 OLT3/0/1 端口和 OLT3/0/2 端口加入该光纤备份组，使 OLT3/0/1 端口为主用端口，OLT3/0/2 端口为备用端口。



说明

先加入的端口为主用端口，后加入的端口为备用端口。

```
[Sysname-fiber-group1] group member olt3/0/1
[Sysname-fiber-group1] group member olt3/0/2
[Sysname-fiber-group1]
%Nov 23 12:53:02:491 2007 H3C IFNET/4/LINK UPDOWN:
  Olt3/0/2: link status is DOWN
%Nov 23 12:53:02:882 2007 H3C IFNET/4/LINK UPDOWN:
  Olt3/0/1: link status is UP
```

查看光纤备份组端口状态。

```
[Sysname-fiber-group1] display fiber-backup group 1
fiber backup group 1 information:
Member      Role      State
-----
Olt3/0/1    MASTER    ACTIVE
Olt3/0/2    SLAVE     READY
```

- 光纤备份组自动切换

当 OLT3/0/1 端口出现故障或其所连接的光纤无法正常通信时，设备可以自动将 OLT3/0/2 端口切换为主用端口，同时将流量切换到该端口进行传输。

```
[Sysname-fiber-group1]
#Nov 23 12:57:23:907 2007 H3C EPON/1/TRAP_EPON_OLTSWITCH:
Trap 1.3.6.1.4.1.25506.2.42.1.8.0.28<hh3cEponOltSwitchoverTrap>: An OLT switchover trap
has been detected,
Master interface index is 29556737,
```

```

Master interface description is 0lt3/0/2 Interface
Slave interface index is 29556738,
Slave interface description is 0lt3/0/1 Interface
Reason is "olt shutdown"
%Nov 23 12:57:24:61 2007 H3C IFNET/4/LINK UPDOWN:
  0lt3/0/1: link status is DOWN
%Nov 23 12:57:24:452 2007 H3C IFNET/4/LINK UPDOWN:
  0lt3/0/2: link status is UP

```

显示切换后的主备端口状态。

```

[Sysname-fiber-group1] display fiber-backup group 1
fiber backup group 1 information:
Member          Role          State
-----
0lt3/0/2        MASTER        ACTIVE
0lt3/0/1        SLAVE         DOWN

```

可以看到 OLT3/0/2 端口已经成为主用端口，并处于 ACTIVE 状态；OLT3/0/1 端口成为备用端口，处于 DOWN 状态。

- 光纤备份组手工切换

在两条光纤均正常工作的情况下（即 OLT3/0/1 端口为主用端口，处于 ACTIVE 状态；OLT3/0/2 为备用端口，处于 READY 状态），用户如果需要对 OLT3/0/1 端口所连接的光纤进行维护和检修，可以手工将 OLT3/0/1 端口和 OLT3/0/2 端口进行主备切换，使业务流量通过 OLT3/0/2 端口进行传输。

```

[Sysname-fiber-group1] port switch-over
[Sysname-fiber-group1]
#Nov 23 12:54:53:307 2007 H3C EPON/1/TRAP_EPON_OLTSWITCH:
  Trap 1.3.6.1.4.1.25506.2.42.1.8.0.28<hh3cEponOltSwitchoverTrap>: An OLT switchover trap
has been detected,
  Master interface index is 29556738,
  Master interface description is 0lt3/0/2 Interface
  Slave interface index is 29556737,
  Slave interface description is 0lt3/0/1 Interface
  Reason is "manual switch"
%Nov 23 12:54:53:537 2007 H3C IFNET/4/LINK UPDOWN:
  0lt3/0/1: link status is DOWN
%Nov 23 12:54:53:927 2007 H3C IFNET/4/LINK UPDOWN:
  0lt3/0/2: link status is UP

```

切换完成后，查看备份组的端口状态。

```

[Sysname-fiber-group1] display fiber-backup group 1
fiber backup group 1 information:
Member          Role          State
-----
0lt3/0/2        MASTER        ACTIVE
0lt3/0/1        SLAVE         READY

```

可以看到 OLT3/0/2 端口已经成为主用端口，并处于 ACTIVE 状态；OLT3/0/1 端口成为备用端口，处于 READY 状态。

如果关闭 OLT3/0/2 端口，则 OLT3/0/1 端口将再次成为主用端口。

```
[Sysname-fiber-group1] quit
[Sysname] interface olt3/0/2
[Sysname-Olt3/0/2] shutdown
[Sysname-Olt3/0/2]
#Nov 23 12:57:23:907 2007 H3C EPON/1/TRAP_EPON_OLTSWITCH:
  Trap 1.3.6.1.4.1.25506.2.42.1.8.0.28<hh3cEponOltSwitchoverTrap>: An OLT switcho
ver trap has been detected,
  Master interface index is 29556737,
  Master interface description is Olt3/0/1 Interface
  Slave interface index is 29556738,
  Slave interface description is Olt3/0/2 Interface
  Reason is "olt shutdown"
%Nov 23 12:57:24:61 2007 H3C IFNET/4/LINK UPDOWN:
  Olt3/0/2: link status is DOWN
%Nov 23 12:57:24:452 2007 H3C IFNET/4/LINK UPDOWN:
  Olt3/0/1: link status is UP
[Sysname-Olt3/0/2] display fiber-backup group 1
  fiber backup group 1 information:
  Member      Role      State
  -----
  Olt3/0/1     MASTER   ACTIVE
  Olt3/0/2     SLAVE    DOWN
```

5. 完整配置

```
#
ftth
  fiber-backup group 1
#
interface Olt3/0/1
  port fiber-backup group 1
#
interface Olt3/0/2
  port fiber-backup group 1
```

6. 配置注意事项

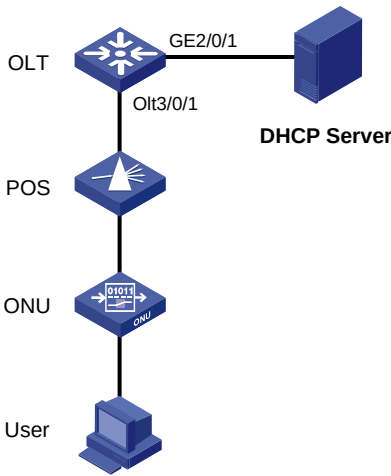
- 本组网需要使用 2:N 型的 POS 配合 OLT 实现光纤备份，对于 ONU 设备无特殊要求。
- 光纤备份组中端口的主备角色根据端口加入备份组的先后顺序确定，当端口所在的单板重启时，该端口将重新加入备份组，备份组的角色分配可能会产生变化。
- 在主备切换过程中，ONU 设备需要重新注册，因此完成切换的时间需要 2~3 秒。
- 可以触发光纤备份组自动进行主备切换的条件包括：FER（Frame Error Rate，帧错误率）告警、光纤断路、OLT 单板或端口自检失败、OLT 端口被关闭。以上故障信息用户均可以通过查看系统日志进行查看。
- 光纤备份组中的主备端口可以存在于不同的单板上，这样可以避免 OLT 单板故障造成的线路中断。

- 备份组的编号范围为 1~80。如果需要删除备份组，必须先从备份组内删除所有成员端口。
- 每个备份组最多只允许加入两个 OLT 端口，一个 OLT 端口不允许加入两个不同的备份组。
- 当备份组中加入第二个 OLT 端口后，需要用户手工同步第一个 OLT 端口及其下所有 ONU 的配置到第二个 OLT 端口，以确保主备切换后业务能正常运行。如果两个端口配置不一致，在 Master 端口切换后，有可能因配置变化导致业务失效。
- 光纤主备切换可以由用户手动进行，也可以在设备检测到链路故障后自动切换，切换后端口状态和角色会有变化。
- 如果备份组中的备份端口在切换前不是 READY 状态，则不能完成切换。

1.1.3 IP Source Guard 绑定典型配置指导

1. 组网图

图1-3 IP Source Guard 绑定组网示意图



2. 应用要求

- OLT 通过端口 GigabitEthernet2/0/1 与 DHCP Server 相连, 通过端口 OLT3/0/1 和分光器下接一个 ONU，最后，ONU 的 UNI1 下接一台用户；
- 在 OLT 上开启 DHCP Snooping 功能；
- 将 ONU（MAC 地址为 000f-e200-0001）与 ONU 端口 ONU3/0/1:1 进行绑定；
- 用户（MAC 地址为 00-01-02-03-04-06）通过 DHCP Server 获取 IP 地址，则在 OLT 上生成 User 的 DHCP Snooping 表项；
- 在端口 OLT3/0/1 上启用 IP 过滤功能，防止客户端使用伪造的不同源 IP 地址对服务器进行攻击。

3. 适用产品、版本

表1-3 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S7500E 系列以太网交换机	Release 6300 软件版本	全系列硬件版本

4. 配置过程 and 解释



说明

本例中只介绍 OLT 上的配置，DHCP Server 的配置请参考“DHCP 典型配置指导”。

(1) 配置 OLT

开启 DHCP Snooping 功能。

```
<Sysname> system-view
```

```
[Sysname] dhcp-snooping
```

配置与 DHCP 服务器相连的端口 GigabitEthernet2/0/1 为信任端口。

```
[Sysname] interface GigabitEthernet2/0/1
```

```
[Sysname-GigabitEthernet2/0/1] dhcp-snooping trust
```

```
[Sysname-GigabitEthernet2/0/1] quit
```

配置端口 OLT3/0/1 的端口过滤功能。

```
[Sysname] interface Olt 3/0/1
```

```
[Sysname-Olt3/0/1] ip check source ip-address mac-address
```

创建 ONU 端口 ONU3/0/1:1，并将 ONU 与端口 ONU3/0/1:1 进行绑定。

```
[Sysname-Olt3/0/1] using onu 1
```

```
[Sysname-Olt3/0/1] quit
```

```
[Sysname] interface onu3/0/1:1
```

```
[Sysname-Onu3/0/1:1] bind onuid 000f-e200-0001
```

(2) 验证结果

当用户从 DHCP 服务器成功获取 IP 地址后，可以在 OLT 设备上显示端口 OLT3/0/1 从 DHCP Snooping 获取的动态表项。

```
<Sysname> display ip check source interface olt 3/0/1
```

```
The Following User address bind have been configured:
```

Mac	IP	Vlan	Port	Status
0001-0203-0406	192.168.0.1	1	Olt3/0/1	DHCP-SNP

显示 DHCP Snooping 已有的动态表项，查看其是否和端口 OLT3/0/1 获取的动态表项一致。

```
<Sysname> display dhcp-snooping
```

```
DHCP Snooping is enabled.
```

```
The client binding table for all untrusted ports.
```

```
Type : D--Dynamic , S--Static
```

Type	IP Address	MAC Address	Lease	VLAN	Interface

====	=====	=====	=====	====	=====

D	192.168.0.1	0001-0203-0406	86335	1	Onu3/0/1:1

从以上显示信息可以看出，端口 OLT3/0/1 在配置 IP Source Guard 功能之后获取了 DHCP Snooping 产生的动态表项。

5. 完整配置

```
#
```

```
dhcp-snooping
```

```
#
interface GigabitEthernet2/0/1
  dhcp-snooping trust
#
interface Olt3/0/1
  using onu 1
  ip check source ip-address mac-address
#
interface Onu3/0/1:1
  bind onuid 000f-e200-0001
```

6. 配置注意事项

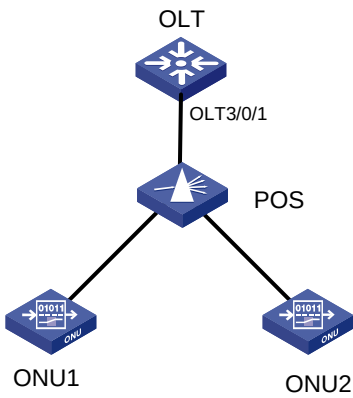
无

1.2 ONU 远程管理典型配置指导

1.2.1 ONU 和 ONU 端口的绑定典型配置指导

1. 组网图

图1-4 将 ONU 和 ONU 端口绑定的示意图



2. 应用要求

将 ONU1（MAC 地址为 000f-e200-0031）和 ONU2（MAC 地址为 000f-e200-3749）分别与 ONU3/0/1:1 端口和 ONU3/0/1:2 端口进行绑定。两台 ONU 的扩展 OAM 版本号均为 2。

3. 适用产品、版本

表1-4 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S7500E 系列以太网交换机	Release 6300 软件版本	全系列硬件版本

4. 配置过程和解释

配置 OUI 及扩展 OAM 版本号列表。

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
```

```
[Sysname] ftth
[Sysname-ftth] epon-parameter ouilist oui 000fe2 oam-version 2 slot 3
[Sysname-ftth] quit
```

创建 ONU 端口 ONU3/0/1:1 和 ONU3/0/1:2，并将 ONU1 与端口 ONU3/0/1:1 进行绑定，ONU2 与端口 ONU3/0/1:2 进行绑定。

```
[Sysname] interface olt 3/0/1
[Sysname-Olt3/0/1] using onu 1 to 2
[Sysname-Olt3/0/1] quit
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] bind onuid 000f-e200-0031
[Sysname-Onu3/0/1:1] quit
[Sysname] interface onu 3/0/1:2
[Sysname-Onu3/0/1:2] bind onuid 000f-e200-3749
```

当该两 ONU 上电后，显示其绑定结果及状态信息。

```
<Sysname> display onuinfo interface Olt 4/0/1
```

ONU Mac Address	LLID	Dist(M)	Port	Board/Ver	Sft/Epm	State	Aging
000f-e200-0031	1	<50	Onu4/0/1:1	ET704-A-L/B	110/100	Up	N/A
000f-e200-3749	2	<50	Onu4/0/1:2	ET704-A-L/B	110/100	Up	N/A

```

--- 2 entries found ---

```

5. 完整配置

```
#
ftth
epon-parameter ouilist oui 000fe2 oam-version 2 slot 3
#
interface Olt3/0/1
using onu 1 to 2
#
interface Onu3/0/1:1
bind onuid 000f-e200-0031
#
interface Onu3/0/1:2
bind onuid 000f-e200-3749
```

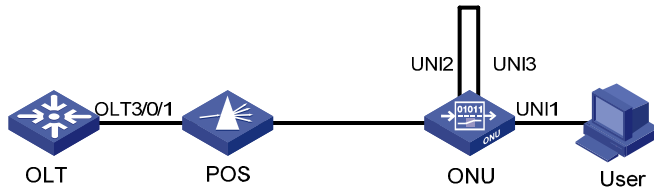
6. 配置注意事项

- 一个 ONU 端口上只能绑定一台 ONU，且一台 ONU 也只能绑定到一个 OLT 下的一个 ONU 端口，即：在一个 OLT 端口下，ONU 端口和 ONU 设备是一一对应的关系。
- 在光纤备份情况下，一台 ONU 可以绑定到互为备份的两个 OLT 端口下的两个 ONU 端口。

1.2.2 配置 ONU 的 RSTP 典型配置指导

1. 组网图

图1-5 ONU 的 RSTP 配置组网示意图



2. 应用要求

- UNI 端口 1 连接一个用户，如果误将 UNI 端口 2 和 UNI 端口 3 互连，且 ONU 的 RSTP 功能处于关闭状态，那么当用户 ping 一个自己 PC 的 ARP 表项中不存在的 IP 地址时，UNI 端口 2 和 UNI 端口 3 之间会产生广播风暴；
- 开启 ONU 的 RSTP 功能后，则可以抑制该现象的产生。

3. 适用产品、版本

表1-5 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S7500E 系列以太网交换机	Release 6300 软件版本	全系列硬件版本

4. 配置过程和解释

开启 ONU 的 RSTP 功能后，可抑制 UNI 端口 2 和 UNI 端口 3 之间广播风暴的产生。

```
<Sysname> system-view
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] onu-protocol stp enable
```

5. 完整配置

```
#
interface Onu3/0/1:1
onu-protocol stp enable
```

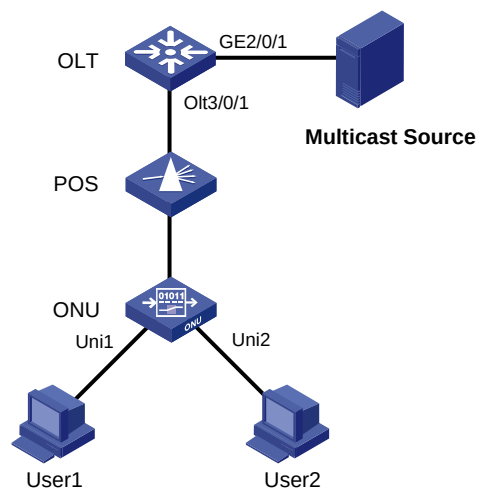
6. 配置注意事项

在 S7500E 交换机全局开启 STP 功能的情况下，所有 ONU 都必须开启 STP 功能，且 ONU 不能作为 STP 根桥，以免网络出现异常。

1.2.3 IGMP Snooping 模式下的组播典型配置指导

1. 组网图

图1-6 IGMP Snooping 模式下的组播配置组网示意图



2. 应用要求

- 交换机的 GigabitEthernet2/0/1 与组播源相连,通过端口 OLT3/0/1 和分光器下接一台 ONU(该 ONU 已与 ONU3/0/1:1 端口绑定), UNI 端口 1 和 UNI 端口 2 下分别接有 User1 和 User2;
- 现要求 User1 可点播 225.1.2.1~225.1.2.255 之间的频道, User2 可点播 225.1.3.1~225.1.3.255 之间的频道。

3. 适用产品、版本

表1-6 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S7500E 系列以太网交换机	Release 6300 软件版本	全系列硬件版本

4. 配置过程和解释

配置组播 IP 地址与组播 VLAN 的对应关系。

```
<Sysname> system-view
[Sysname] ftth
[Sysname-ftth] multicast vlan-id 1002 dest-ip 225.1.2.1 to 225.1.2.255
[Sysname-ftth] multicast vlan-id 1003 dest-ip 225.1.3.1 to 225.1.3.255
[Sysname-ftth] quit
```

全局开启 IGMP Snooping 功能。

```
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
```

在 VLAN 1002 和 VLAN 1003 内启动 IGMP Snooping 功能。

```
[Sysname] vlan 1002
[Sysname-vlan1002] igmp-snooping enable
[Sysname-vlan1002] quit
```

```
[Sysname] vlan 1003
```

```
[Sysname-vlan1003] igmp-snooping enable
```

```
[Sysname-vlan1003] quit
```

配置 ONU 的组播模式为 IGMP Snooping 模式。

```
[Sysname] interface Onu 3/0/1:1
```

```
[Sysname-Onu3/0/1:1] multicast-mode igmp-snooping
```

将 ONU 的 UNI 1 端口和 UNI 2 端口各加入组播 VLAN 1002 和 VLAN 1003, 并配置 ONU 为 Trunk 类型（配置成 Trunk 类型后将允许所有 VLAN 的报文通过）。

```
[Sysname-Onu3/0/1:1] uni 1 multicast vlan 1002
```

```
[Sysname-Onu3/0/1:1] uni 2 multicast vlan 1003
```

```
[Sysname-Onu3/0/1:1] port link-type trunk
```

开启 UNI 1 和 UNI 2 端口删除下行组播流 VLAN Tag 功能。

```
[Sysname-Onu3/0/1:1] uni 1 multicast-strip-tag enable
```

```
[Sysname-Onu3/0/1:1] uni 2 multicast-strip-tag enable
```

```
[Sysname-Onu3/0/1:1] quit
```

配置端口 OLT3/0/1 为 Hybrid 类型，允许 VLAN 1002 和 VLAN 1003 的报文通过，且发送 VLAN 1002 和 VLAN 1003 的报文时携带 Tag。

```
[Sysname] interface olt 3/0/1
```

```
[Sysname-Olt3/0/1] port link-type hybrid
```

```
[Sysname-Olt3/0/1] port hybrid vlan 1002 1003 tagged
```

配置端口 GigabitEthernet2/0/1 为 Trunk 类型，并允许 VLAN 1002 和 VLAN 1003 的报文通过。

```
[Sysname] interface GigabitEthernet2/0/1
```

```
[Sysname-GigabitEthernet2/0/1] port link-type trunk
```

```
[Sysname-GigabitEthernet2/0/1] port trunk permit vlan 1002 1003
```

5. 完整配置

```
#
```

```
igmp-snooping
```

```
#
```

```
vlan 1002
```

```
igmp-snooping enable
```

```
#
```

```
vlan 1003
```

```
igmp-snooping enable
```

```
#
```

```
ftth
```

```
multicast vlan-id 1002 dest-ip 225.1.2.1 to 225.1.2.255
```

```
multicast vlan-id 1003 dest-ip 225.1.3.1 to 225.1.3.255
```

```
#
```

```
interface GigabitEthernet2/0/1
```

```
port link-type trunk
```

```
port trunk permit vlan 1 1002 to 1003
```

```
#
```

```
interface Olt3/0/1
```

```
using onu 1
```

```
port link-type hybrid
port hybrid vlan 1 1002 to 1003 tagged
#
interface Onu3/0/1:1
uni 1 multicast vlan 1002
uni 1 multicast-strip-tag enable
uni 2 multicast vlan 1003
uni 2 multicast-strip-tag enable
port link-type trunk
```

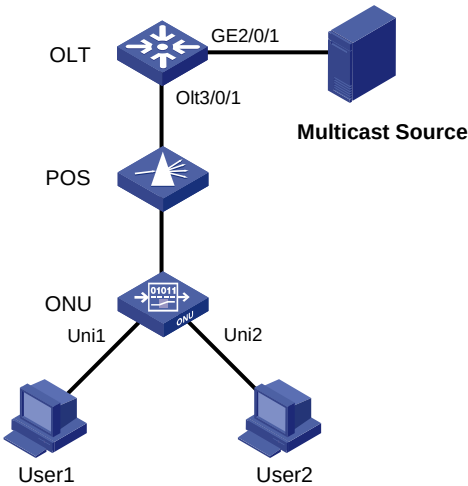
6. 配置注意事项

一个组播 IP 地址只能属于一个组播 VLAN。

1.2.4 可控组播模式下的组播典型配置指导

1. 组网图

图1-7 可控组播模式组网示意图



2. 应用要求

交换机的 GigabitEthernet2/0/1 与组播源相连，并通过端口 OLT3/0/1 和分光器下接一台 ONU（该 ONU 已与 ONU3/0/1:1 端口绑定），最后，UNI 端口 1 和 UNI 端口 2 下分别接有 User1 和 User2。通过配置组播控制，使得 User1 和 User2 对频道 1（225.1.1.1）和频道 2（225.1.2.1）拥有不同的访问权限。

- User1: 允许观看频道 1，且仅对频道 2 拥有 60 秒的预览；
- User2: 不允许观看频道 1，但可以观看频道 2。

3. 适用产品、版本

表1-7 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S7500E 系列以太网交换机	Release 6300 软件版本	全系列硬件版本

4. 配置过程和解释

配置组播 IP 与组播 VLAN 的对应关系。

```
<Sysname> system-view
[Sysname] ftth
[Sysname-ftth] multicast vlan-id 1002 dest-ip 225.1.1.1
[Sysname-ftth] multicast vlan-id 1003 dest-ip 225.1.2.1
[Sysname-ftth] quit
```

全局开启 IGMP Snooping 功能。

```
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
```

在 VLAN 1002 和 VLAN 1003 内启动 IGMP Snooping 功能。

```
[Sysname] vlan 1002
[Sysname-vlan1002] igmp-snooping enable
[Sysname-vlan1002] vlan 1003
[Sysname-vlan1003] igmp-snooping enable
[Sysname-vlan1003] quit
```

配置 ONU 的组播模式为可控组播模式。

```
[Sysname-Onu3/0/1:1] multicast-mode multicast-control
```

配置 ONU UNI 端口 1 下的用户可观看频道 1，且仅对频道 2 拥有 60 秒的预览，并开启该端口删除下行组播流 VLAN Tag 功能。

```
[Sysname-Onu3/0/1:1] uni 1 multicast-control multicast-address 225.1.1.1 rule permit
[Sysname-Onu3/0/1:1] uni 1 multicast-control multicast-address 225.1.2.1 rule preview
time-slice 1
[Sysname-Onu3/0/1:1] uni 1 multicast-strip-tag enable
```

配置 ONU UNI 端口 2 下的用户不允许观看频道 1，但可观看频道 2，并开启该端口删除下行组播流 VLAN Tag 功能。

```
[Sysname-Onu3/0/1:1] uni 2 multicast-control multicast-address 225.1.1.1 rule deny
[Sysname-Onu3/0/1:1] uni 2 multicast-control multicast-address 225.1.2.1 rule permit
[Sysname-Onu3/0/1:1] uni 2 multicast-strip-tag enable
```

配置 ONU 为 Trunk 类型（配置成 Trunk 类型后将允许所有 VLAN 的报文通过）。

```
[Sysname-Onu3/0/1:1] port link-type trunk
```

配置端口 OLT3/0/1 为 Hybrid 类型，允许 VLAN 1002 和 VLAN 1003 的报文通过，且发送 VLAN 1002 和 VLAN 1003 的报文时携带 Tag。

```
[Sysname] interface olt 3/0/1
[Sysname-olt3/0/1] port link-type hybrid
[Sysname-olt3/0/1] port hybrid vlan 1002 1003 tagged
```

配置端口 GigabitEthernet2/0/1 为 Trunk 类型，并允许 VLAN 1002 和 VLAN 1003 的报文通过。

```
[Sysname] interface GigabitEthernet2/0/1
[Sysname-GigabitEthernet2/0/1] port link-type trunk
[Sysname-GigabitEthernet2/0/1] port trunk permit vlan 1002 1003
```

5. 完整配置

```
#
igmp-snooping
#
vlan 1002
    igmp-snooping enable
#
vlan 1003
    igmp-snooping enable
#
ftth
    multicast vlan-id 1002 dest-ip 225.1.1.1
    multicast vlan-id 1003 dest-ip 225.1.2.1
#
interface GigabitEthernet2/0/1
    port link-type trunk
    port trunk permit vlan 1 1002 to 1003
#
interface Olt3/0/1
    using onu 1
    port link-type hybrid
    port hybrid vlan 1 1002 to 1003 tagged
#
interface Onu3/0/1:1
    multicast-mode multicast-control
    uni 1 multicast-strip-tag enable
    uni 2 multicast-strip-tag enable
    uni 1 multicast-control multicast-address 225.1.1.1 rule permit
    uni 1 multicast-control multicast-address 225.1.2.1 rule preview time-slice 1
    uni 2 multicast-control multicast-address 225.1.1.1 rule deny
    uni 2 multicast-control multicast-address 225.1.2.1 rule permit
    port link-type trunk
```

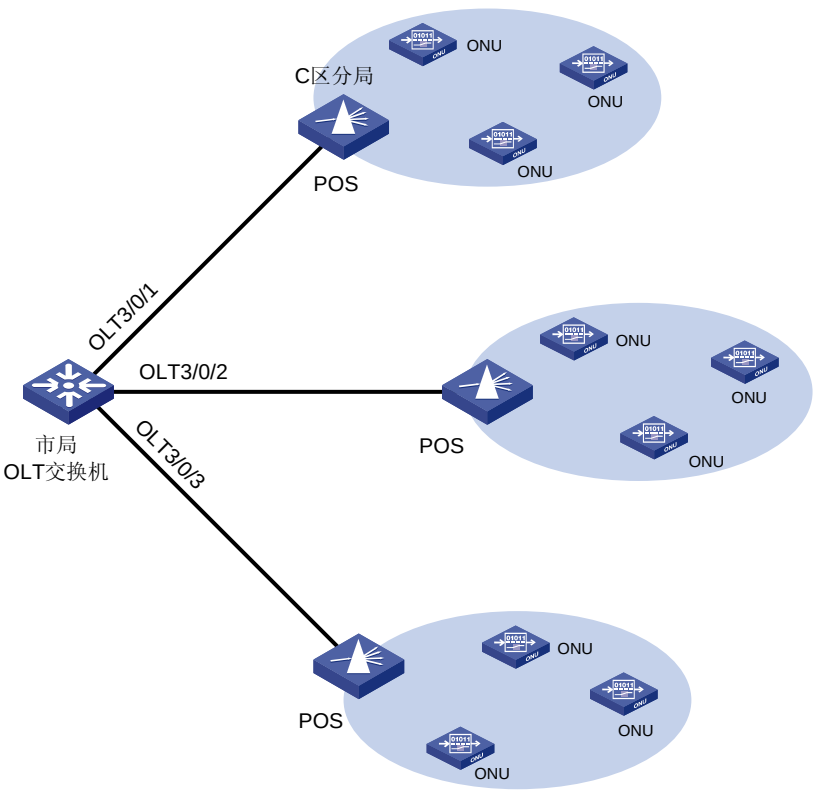
6. 配置注意事项

一个组播 IP 地址只能属于一个组播 VLAN。

1.2.5 升级 ONU 典型配置指导

1. 组网图

图1-8 ONU 升级组网图



说明

为了简化组网图，本图仅以三个 OLT 端口为例进行说明，其余 OLT 端口略。

2. 应用要求

- 某市广电局端 S7500E 交换机有 12 个 OLT 端口下挂了 150 台 A 类型的 ONU;
- A 型 ONU 的厂家近期发布了 A 型 ONU 的增强软件版本 110，解决了上一版本 109 的一些软件 bug，还增加了一些新功能。
- 市局决定对这些 ONU 全部进行升级。其中对于 C 区分局（连接 OLT3/0/1 端口）下挂的 5 台 A 型 ONU，网络管理者认为 109 版本能够满足当前需求，且使用中未发现问题，所以仍然使用 109 版本。但为了以后可能会升级到 110 版本的需要，要求先在分局大楼（大楼通过 ONU3/0/1:1 端口绑定的 A 型 ONU 实现 FTTB 接入）试用 110 版本。

3. 适用产品、版本

表1-8 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S7500E 系列以太网交换机	Release 6300 软件版本	全系列硬件版本

4. 配置过程 and 解释

上传升级文件 **a110.app** 和 **a109.app** 到交换机主用主控板和备用主控板，详细过程请参见《H3C S7500E 系列以太网交换机 安装手册》交换机的软件维护部分。

用户可以在端口视图（包括 OLT 端口视图、ONU 端口视图）和 FTTH 视图下配置升级 ONU 设备的软件版本，其中在两种端口视图下的配置优先级高于 FTTH 视图下的配置，而两种端口视图下的配置优先级相等，即后进行的配置会覆盖前面的配置。因此，根据组网需求，升级 ONU 软件版本的配置过程如下：

- 在 OLT3/0/1 端口视图下配置，将其下挂的 A 类型 ONU 全部升级到 109 版本。
- 在 ONU3/0/1:1 端口视图下配置，使该端口下挂的 A 类型 ONU 升级到 110 版本。
- 在 FTTH 视图下配置，把 S7500E 交换机的 12 个 OLT 下挂的 ONU 全部升级到 110 版本。由于 OLT 端口视图下的升级配置优先级高于 FTTH 视图，故此操作不会影响到 OLT3/0/1 端口下挂的 ONU 设备。

在 OLT3/0/1 端口视图下配置升级所有下挂 A 类型的 ONU 到 109 版本。

```
[Sysname] interface olt 3/0/1
[Sysname-Olt3/0/1] update onu filename a109.app
Update flash:/ a109.app?[Y/N]:y
Info: Download file to onu may take a long time, please wait...
Please wait while the firmware is being burnt, and check the software version after
re-registration!
[Sysname-Olt3/0/1] quit
```

升级 C 区分局大楼 ONU3/0/1:1 对应的 A 型 ONU 到 110 版本。

```
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] update onu filename a110.app
Update flash:/ a110.app?[Y/N]:y
Info: Download file to onu may take a long time, please wait...
Please wait while the firmware is being burnt, and check the software version after
re-registration!
[Sysname-Onu3/0/1:1] quit
```

配置 S7500E 交换机对所有下挂 A 类型的 ONU 升级到 110 版本。

```
<Sysname> system-view
[Sysname] ftth
[Sysname-ftth] update onu onu-type a filename a110.app
```

5. 完整配置

```
#
interface Onu3/0/1:1
 bind onuid 000f-e200-0001
update onu filename flash:/a110.app
#
interface Onu3/0/1:2
 bind onuid 000f-e200-0002
update onu filename flash:/a109.app
#
interface Onu3/0/1:3
```



```

bind onuid 000f-e200-0003
update onu filename flash:/a109.app
#
interface Onu3/0/1:4
bind onuid 000f-e200-0004
update onu filename flash:/a109.app
#
interface Onu3/0/1:5
bind onuid 000f-e200-0005
update onu filename flash:/a109.app
#
ftth
update onu onu-type A filename flash:/a110.app

```

6. 配置注意事项

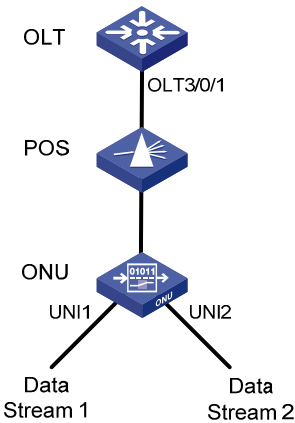
- 在进行升级之前，须确保 ONU 升级文件已经上传到 S7500E 主用主控板上（不能使用备用主控板上的升级文件完成加载），具体上传过程请参见《H3C S7500E 系列以太网交换机 安装手册》中交换机的软件维护章节。
- 如果需要新上线的 ONU 能够自动升级，则需要把升级文件同时上传到主用主控板和备用主控板，以防止交换机主备倒换后原备用主控板没有升级文件可用所致使的升级失败。
- 不同类型的 ONU 升级所需升级文件不同，如果 ONU 和升级文件不匹配，升级将不会成功。如：在 OLT 端口视图下指定了升级 ET704-A 类型 ONU 的升级文件，则该 OLT 端口下挂的其它类型 ONU 将不能成功升级。
- 为了实现批量升级，节省系统资源，升级命令配置后，OLT 会延迟 15~20s 时间后再执行升级命令。
- 在 ONU 软件更新过程中，建议用户不要对 ONU 断电，以免更新失败。
- 升级文件传送到 ONU 后，ONU 将自动重启完成升级过程。
- 配置升级 OLT 端口下所有已创建 ONU 端口对应的 ONU 后，如果新上线的 ONU 所对应的端口在升级命令配置之前已创建，则直接升级（当然，和升级文件不匹配的 ONU 是不能升级成功的）。反之（即：对应 ONU 端口在升级命令配置之后创建），则不升级。
- 配置升级交换机下指定类型的 ONU 后，如果新创建的 ONU 端口对应的 ONU 符合指定类型且上线后，交换机会自动对其进行升级。
- 端口下配置的升级命令优先级高于 FTTH 视图下的升级命令。即：假如 ONU 端口 ONU3/0/1:1 对应的 ONU 为 A 类型，在 FTTH 视图下配置了升级 A 类型 ONU 的升级文件为 1.app，同时在 ONU3/0/1:1 端口视图下配置了升级文件为 2.app，则该 ONU 会选择 2.app 文件进行升级。
- OLT 最多可同时对 64 种类型的 ONU 进行升级，即可通过按类型升级 ONU 的命令行为 64 种不同类型的 ONU 指定升级文件。

1.3 UNI 端口典型配置指导

1.3.1 UNI 端口优先级重标记配置举例

1. 组网图

图1-9 UNI 端口优先级重标记配置组网示意图



2. 应用要求

- 配置 ONU 上行带宽为 50Mbps;
- 配置 UNI 端口 1 和 UNI 端口 2 的 VLAN 操作模式均为透传模式;
- 配置 UNI 端口 1 优先级重标记: 对源 MAC 地址为 000A-EB7F-AAAB 的带 Tag 报文重新打上 CoS 3 的优先级;
- 配置 UNI 端口 2 优先级重标记: 对源 MAC 为 001B-EB7F-21AC 的带 Tag 报文重新打上 CoS 1 的优先级。

3. 适用产品、版本

表1-9 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S7500E 系列以太网交换机	Release 6300 软件版本	全系列硬件版本

4. 配置过程 and 解释

创建 ONU 端口 ONU3/0/1:1, 并将 ONU 绑定到此 ONU 端口。

```
<Sysname> system-view
[Sysname] interface olt 3/0/1
[Sysname-Olt3/0/1] using onu 1
[Sysname-Olt3/0/1] quit
[Sysname] interface onu 3/0/1:1
[Sysname-Onu3/0/1:1] bind onuid 000f-e200-0104
```

配置 ONU 上行带宽为 50Mbps (64Kbps*800)。

```
[Sysname-Onu3/0/1:1] upstream-sla minimum-bandwidth 800 maximum-bandwidth 800
```

配置 UNI 端口 1 和 UNI 端口 2 的 VLAN 操作模式为透传模式。

```
[Sysname-Onu3/0/1:1] uni 1 vlan-mode transparent
```

```
[Sysname-Onu3/0/1:1] uni 2 vlan-mode transparent
```

配置 UNI 端口 1 和 UNI 端口 2 优先级重标记。

```
[Sysname-Onu3/0/1:1] uni 1 classification-marking index 1 queue 3 priority 3 src-mac equal  
000A-EB7F-AAAB
```

```
[Sysname-Onu3/0/1:1] uni 2 classification-marking index 1 queue 1 priority 1 src-mac equal  
001B-EB7F-21AC
```

配置完成后，当从 ONU 的两个 UNI 端口进来的两条数据流（流量各为 50Mbps）往 OLT 侧转发时，由于 ONU 端口产生拥塞，则丢弃了源 MAC 地址为 001B-EB7F-21AC 的报文，因为该报文的队列优先级比源 MAC 地址为 000A-EB7F-AAAB 的报文低。

5. 完整配置

```
#
```

```
interface Olt3/0/1
```

```
using onu 1
```

```
#
```

```
interface Onu3/0/1:1
```

```
bind onuid 000f-e200-0104
```

```
upstream-sla minimum-bandwidth 800 maximum-bandwidth 800
```

```
uni 1 classification-marking index 1 queue 3 priority 3 src-mac equal 000a-eb7f-aaab
```

```
uni 2 classification-marking index 1 queue 1 priority 1 src-mac equal 001b-eb7f-21ac
```

6. 配置注意事项

H3C 的 ONU 的每个 UNI 端口最多只支持配置 8 条匹配规则。

目 录

1 Smart Link典型配置指导	1-1
1.1 Smart Link简介	1-1
1.2 Smart Link典型配置指导	1-1
1.2.1 组网图	1-1
1.2.2 应用要求	1-1
1.2.3 适用产品、版本	1-1
1.2.4 配置过程和解释	1-2
1.2.5 完整配置	1-3
1.2.6 配置注意事项	1-4
1.3 多Smart Link组负载分担配置举例	1-5
1.3.1 组网图	1-5
1.3.2 应用需求	1-5
1.3.3 适用产品、版本	1-5
1.3.4 配置过程和解释	1-5
1.3.5 完整配置	1-7
1.3.6 配置注意事项	1-9

1 Smart Link 典型配置指导

1.1 Smart Link 简介

如图 1-1所示，双上行组网是目前常用组网之一。一般情况下，通过开启STP（Spanning Tree Protocol，生成树协议）来实现网络中的链路冗余备份，但STP不适用于对收敛时间有很高要求的用户。

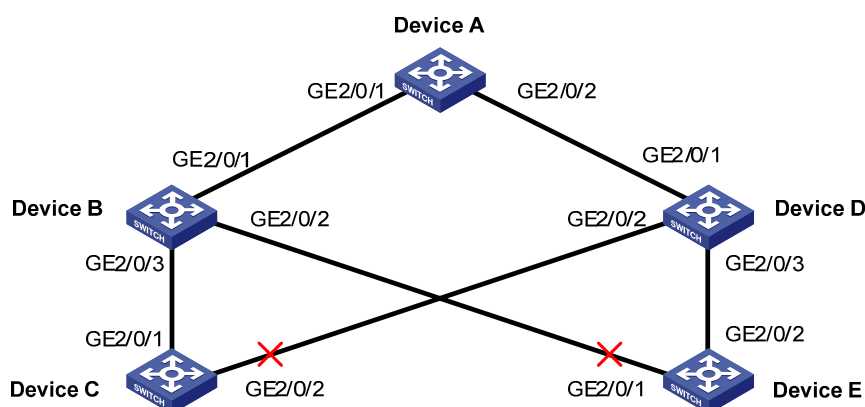
Smart Link 功能可以满足用户对链路快速收敛的需求，可以实现主备链路的冗余备份及其快速迁移。在双上行组网环境下，当主用链路出现故障时，设备自动将流量切换到备用链路，这样就起到了冗余阻塞和链路备份的作用。

Smart Link 的主要特点是：专用于双上行组网；收敛速度快（达到亚秒级）；配置简单，便于用户操作。

1.2 Smart Link 典型配置指导

1.2.1 组网图

图1-1 配置 Smart Link 组网图



1.2.2 应用要求

- 设备 Device C、设备 Device E 双上行到设备 Device A;
- 双上行链路进行灵活备份;
- 在 VLAN 1 内发送和接收 Flush 报文。

1.2.3 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S7500E 系列以太网交换机	Release 6300 软件版本	全系列硬件版本

1.2.4 配置过程和解释

(1) 设备 Device C 上的配置

创建 Smart Link 组。

```
<DeviceC> system-view
[DeviceC] interface GigabitEthernet 2/0/1
[DeviceC-GigabitEthernet2/0/1] undo stp enable
[DeviceC-GigabitEthernet2/0/1] quit
[DeviceC] interface GigabitEthernet 2/0/2
[DeviceC-GigabitEthernet2/0/2] undo stp enable
[DeviceC-GigabitEthernet2/0/2] quit
[DeviceC] smart-link group 1
```

配置保护所有引用实例所绑定的 VLAN（当前设备支持的实例范围为 0~31）。

```
[DeviceC-smlk-group1] protected-vlan reference-instance 0 to 31
```

配置端口 GigabitEthernet 2/0/1 为主端口，端口 GigabitEthernet 2/0/2 为副端口。

```
[DeviceC-smlk-group1] port GigabitEthernet 2/0/1 master
[DeviceC-smlk-group1] port GigabitEthernet 2/0/2 slave
```

开启发送 Flush 报文的功能。

```
[DeviceC-smlk-group1] flush enable
```

(2) 设备 Device E 上的配置

创建 Smart Link 组。

```
<DeviceE> system-view
[DeviceE] interface GigabitEthernet 2/0/1
[DeviceE-GigabitEthernet2/0/1] undo stp enable
[DeviceE-GigabitEthernet2/0/1] quit
[DeviceE] interface GigabitEthernet 2/0/2
[DeviceE-GigabitEthernet2/0/2] undo stp enable
[DeviceE-GigabitEthernet2/0/2] quit
[DeviceE] smart-link group 1
```

配置保护所有引用实例所绑定的 VLAN（当前设备支持的实例范围为 0~31）。

```
[DeviceE-smlk-group1] protected-vlan reference-instance 0 to 31
```

配置端口 GigabitEthernet 2/0/2 为主端口，端口 GigabitEthernet 2/0/1 为副端口。

```
[DeviceE-smlk-group1] port GigabitEthernet 2/0/2 master
[DeviceE-smlk-group1] port GigabitEthernet 2/0/1 slave
```

开启发送 Flush 报文的功能。

```
[DeviceE-smlk-group1] flush enable
```

(3) 设备 Device B 上的配置

开启接收 Flush 报文的功能。

```
<DeviceB> system-view
[DeviceB] interface GigabitEthernet 2/0/1
[DeviceB-GigabitEthernet2/0/1] smart-link flush enable
```

```
[DeviceB-GigabitEthernet2/0/1] quit
[DeviceB] interface GigabitEthernet 2/0/2
[DeviceB-GigabitEthernet2/0/2] smart-link flush enable
[DeviceB-GigabitEthernet2/0/2] quit
[DeviceB] interface GigabitEthernet 2/0/3
[DeviceB-GigabitEthernet2/0/3] smart-link flush enable
```

(4) 设备 Device D 上的配置

开启接收 Flush 报文的功能。

```
<DeviceD> system-view
[DeviceD] interface GigabitEthernet 2/0/1
[DeviceD-GigabitEthernet2/0/1] smart-link flush enable
[DeviceD-GigabitEthernet2/0/1] quit
[DeviceD] interface GigabitEthernet 2/0/2
[DeviceD-GigabitEthernet2/0/2] smart-link flush enable
[DeviceD-GigabitEthernet2/0/2] quit
[DeviceD] interface GigabitEthernet 2/0/3
[DeviceD-GigabitEthernet2/0/3] smart-link flush enable
```

(5) 设备 Device A 上的配置

开启接收 Flush 报文的功能。

```
<DeviceA> system-view
[DeviceA] interface GigabitEthernet 2/0/1
[DeviceA-GigabitEthernet2/0/1] smart-link flush enable
[DeviceA-GigabitEthernet2/0/1] quit
[DeviceA] interface GigabitEthernet 2/0/2
[DeviceA-GigabitEthernet2/0/2] smart-link flush enable
```

配置完毕后，用户可以使用 **display** 命令查看 Smart Link 的配置和报文统计情况。

1.2.5 完整配置

- Device A 上的配置

```
#
interface GigabitEthernet2/0/1
 smart-link flush enable control-vlan 1
#
interface GigabitEthernet2/0/2
 smart-link flush enable control-vlan 1
#
```

- Device B 上的配置

```
#
interface GigabitEthernet2/0/1
 smart-link flush enable control-vlan 1
#
interface GigabitEthernet2/0/2
 smart-link flush enable control-vlan 1
#
interface GigabitEthernet2/0/3
 smart-link flush enable control-vlan 1
```

##

- Device C 上的配置

##

```
smart-link group 1
protected-vlan reference-instance 0 to 31
```

##

```
interface GigabitEthernet2/0/1
undo stp enable
port smart-link group 1 master
```

##

```
interface GigabitEthernet2/0/2
undo stp enable
port smart-link group 1 slave
```

##

- Device D 上的配置

##

```
interface GigabitEthernet2/0/1
smart-link flush enable control-vlan 1
```

##

```
interface GigabitEthernet2/0/2
smart-link flush enable control-vlan 1
```

##

```
interface GigabitEthernet2/0/3
smart-link flush enable control-vlan 1
```

##

- Device E 上的配置

##

```
smart-link group 1
protected-vlan reference-instance 0 to 31
```

##

```
interface GigabitEthernet2/0/1
undo stp enable
port smart-link group 1 slave
```

##

```
interface GigabitEthernet2/0/2
undo stp enable
port smart-link group 1 master
```

##

1.2.6 配置注意事项

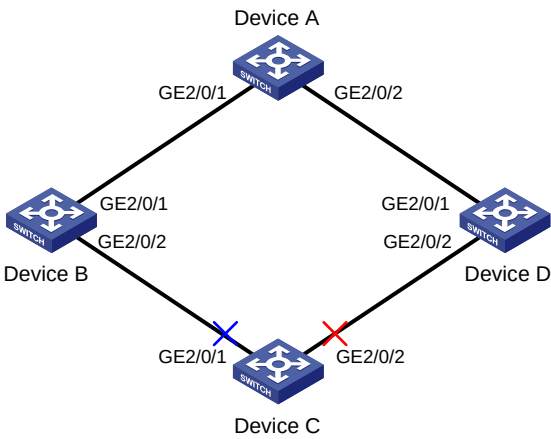
- 如果打算配置某端口为 Smart Link 组成员端口（即主端口和副端口），则需先手工关闭该端口，待 Smart Link 组配置完成后，再开启该端口，以避免形成环路，导致广播风暴。
- 如果打算配置某端口为 Smart Link 组成员端口，则需关闭该端口的 STP 功能和 RRPP 功能，并确保该端口不是聚合成员端口和业务环回组成员端口。
- 不同的 Smart Link 组需要配置不同的控制 VLAN。
- 用户需要配置保证控制 VLAN 存在，并且 Smart Link 组成员端口允许控制 VLAN 的报文通过。

- 不要删除已经配置成控制 VLAN 的 VLAN，否则会影响 Flush 报文的发送。
- 在相关设备上配置的接收处理 Flush 报文的控制 VLAN 和在 Smart Link 设备上配置的发送控制 VLAN 要相同，如果二者不相同，相关设备将对接收到的 Flush 报文不做处理直接转发。

1.3 多 Smart Link 组负载分担配置举例

1.3.1 组网图

图1-2 配置 Smart Link 多实例负载分担组网图



1.3.2 应用需求

- 设备 Device C 上 VLAN 1~200 的流量通过设备 Device B、Device D 双上行到设备 Device A。要求进行负载分担，VLAN 1~100 和 VLAN 101~200 的两组流量分别通过不同的链路上行到设备 Device A；
- 设备 Device C 上进行双上行链路灵活备份，Smart Link 组 1 的引用实例 0（绑定 VLAN 1~100）的流量从经过 Device B 的链路通向设备 Device A；而 Smart Link 组 2 的引用实例 2（绑定 VLAN 101~200）的流量从经过 Device D 链路通向设备 Device A；
- Smart Link 组 1 和组 2 分别在 VLAN 10 和 VLAN 101 内发送和接收 Flush 报文。

1.3.3 适用产品、版本

表1-2 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S7500E 系列以太网交换机	Release 6300 软件版本	全系列硬件版本

1.3.4 配置过程和解释

(1) 设备 Device C 上的配置

创建 VLAN 并配置 VLAN 与 MSTP 实例的映射关系。

```
<DeviceC> system-view
[DeviceC] vlan 1 to 200
[DeviceC] stp region-configuration
[DeviceC-mst-region] instance 0 vlan 1 to 100
```

```
[DeviceC-mst-region] instance 2 vlan 101 to 200
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
```

关闭端口的 STP 功能，并将端口配置为 Trunk 端口且允许 VLAN 1~200 通过。

```
[DeviceC] interface GigabitEthernet 2/0/1
[DeviceC-GigabitEthernet2/0/1] undo stp enable
[DeviceC-GigabitEthernet2/0/1] port link-type trunk
[DeviceC-GigabitEthernet2/0/1] port trunk permit vlan 1 to 200
[DeviceC-GigabitEthernet2/0/1] quit
[DeviceC-GigabitEthernet2/0/1] interface GigabitEthernet 2/0/2
[DeviceC-GigabitEthernet2/0/2] undo stp enable
[DeviceC-GigabitEthernet2/0/2] port link-type trunk
[DeviceC-GigabitEthernet2/0/2] port trunk permit vlan 1 to 200
[DeviceC-GigabitEthernet2/0/2] quit
```

创建 Smart Link 组 1。

```
[DeviceC] smart-link group 1
```

配置 Smart Link 组 1 的保护 VLAN。

```
[DeviceC-smlk-group1] protected-vlan reference-instance 0
```

配置端口 GigabitEthernet 2/0/1 为主端口，端口 GigabitEthernet 2/0/2 为副端口。

```
[DeviceC-smlk-group1] port GigabitEthernet 2/0/1 master
[DeviceC-smlk-group1] port GigabitEthernet 2/0/2 slave
```

配置角色抢占模式。

```
[DeviceC-smlk-group1] preemption mode role
```

开启发送 Flush 报文的功能。

```
[DeviceC-smlk-group-1] flush enable control-vlan 10
[DeviceC-smlk-group-1] quit
```

创建 Smart Link 组 2。

```
[DeviceC] smart-link group 2
```

配置 Smart Link 组 2 的保护 VLAN。

```
[DeviceC-smlk-group2] protected-vlan reference-instance 2
```

配置端口 GigabitEthernet 2/0/1 为副端口，端口 GigabitEthernet 2/0/2 为主端口。

```
[DeviceC-smlk-group2] port GigabitEthernet 2/0/1 slave
[DeviceC-smlk-group2] port GigabitEthernet 2/0/2 master
```

配置角色抢占模式。

```
[DeviceC-smlk-group2] preemption mode role
```

开启发送 Flush 报文的功能。

```
[DeviceC-smlk-group2] flush enable control-vlan 101
```

(2) 设备 Device B 上的配置

开启接收 Flush 报文的功能。

```
<DeviceB> system-view
[DeviceB] vlan 1 to 200
```

```
[DeviceB] interface GigabitEthernet 2/0/1
[DeviceB-GigabitEthernet2/0/1] port link-type trunk
[DeviceB-GigabitEthernet2/0/1] port trunk permit vlan 1 to 200
[DeviceB-GigabitEthernet2/0/1] smart-link flush enable control-vlan 10 101
[DeviceB-GigabitEthernet2/0/1] quit
[DeviceB] interface GigabitEthernet 2/0/2
[DeviceB-GigabitEthernet2/0/2] port link-type trunk
[DeviceB-GigabitEthernet2/0/2] port trunk permit vlan 1 to 200
[DeviceB-GigabitEthernet2/0/2] smart-link flush enable control-vlan 10 101
```

(3) 设备 Device D 上的配置

开启接收 Flush 报文的功能。

```
<DeviceD> system-view
[DeviceD] vlan 1 to 200
[DeviceD] interface GigabitEthernet 2/0/1
[DeviceD-GigabitEthernet2/0/1] port link-type trunk
[DeviceD-GigabitEthernet2/0/1] port trunk permit vlan 1 to 200
[DeviceD-GigabitEthernet2/0/1] smart-link flush enable control-vlan 10 101
[DeviceD-GigabitEthernet2/0/1] quit
[DeviceD] interface GigabitEthernet 2/0/2
[DeviceD-GigabitEthernet2/0/2] port link-type trunk
[DeviceD-GigabitEthernet2/0/2] port trunk permit vlan 1 to 200
[DeviceD-GigabitEthernet2/0/2] smart-link flush enable control-vlan 10 101
```

(4) 设备 Device A 上的配置

开启接收 Flush 报文的功能。

```
<DeviceA> system-view
[DeviceA] vlan 1 to 200
[DeviceA] interface GigabitEthernet 2/0/1
[DeviceA-GigabitEthernet2/0/1] port link-type trunk
[DeviceA-GigabitEthernet2/0/1] port trunk permit vlan 1 to 200
[DeviceA-GigabitEthernet2/0/1] smart-link flush enable control-vlan 10 101
[DeviceA-GigabitEthernet2/0/1] quit
[DeviceA] interface GigabitEthernet 2/0/2
[DeviceA-GigabitEthernet2/0/2] port link-type trunk
[DeviceA-GigabitEthernet2/0/2] port trunk permit vlan 1 to 200
[DeviceA-GigabitEthernet2/0/2] smart-link flush enable control-vlan 10 101
```

配置完毕后，用户可以使用 **display** 命令查看 Smart Link 的配置和报文统计情况。

1.3.5 完整配置

- Device A 上的配置

```
#
vlan 1
#
vlan 2 to 200
#
interface GigabitEthernet2/0/1
port link-type trunk
```

```

port trunk permit vlan 1 to 200
smart-link flush enable control-vlan 10 101
#
interface GigabitEthernet2/0/2
port link-type trunk
port trunk permit vlan 1 to 200
smart-link flush enable control-vlan 10 101
#

```

- Device B 上的配置

```

#
vlan 1
#
vlan 2 to 200
#
interface GigabitEthernet2/0/1
port link-type trunk
port trunk permit vlan 1 to 200
smart-link flush enable control-vlan 10 101
#
interface GigabitEthernet2/0/2
port link-type trunk
port trunk permit vlan 1 to 200
smart-link flush enable control-vlan 10 101
#

```

- Device C 上的配置

```

#
vlan 1
#
vlan 2 to 200
#
stp region-configuration
instance 2 vlan 101 to 200
active region-configuration
#
smart-link group 1
preemption mode role
protected-vlan reference-instance 0
flush enable control-vlan 10
smart-link group 2
preemption mode role
protected-vlan reference-instance 2
flush enable control-vlan 101
#
interface GigabitEthernet2/0/1
port link-type trunk
port trunk permit vlan 1 to 200
undo stp enable
port smart-link group 1 master

```

```

port smart-link group 2 slave
#
interface GigabitEthernet2/0/2
port link-type trunk
port trunk permit vlan 1 to 200
undo stp enable
port smart-link group 1 slave
port smart-link group 2 master
#

```

- Device D 上的配置

```

#
vlan 1
#
vlan 2 to 200
#
interface GigabitEthernet2/0/1
port link-type trunk
port trunk permit vlan 1 to 200
smart-link flush enable control-vlan 10 101
#
interface GigabitEthernet2/0/2
port link-type trunk
port trunk permit vlan 1 to 200
smart-link flush enable control-vlan 10 101
#

```

1.3.6 配置注意事项

请参考 1.2.6 配置注意事项。

目 录

1 MPLS典型配置指导	1-1
1.1 MPLS基本配置指导.....	1-1
1.1.1 配置LDP会话典型配置指导	1-1
1.2 MPLS L2VPN典型配置指导	1-7
1.2.1 CCC远程连接方式的MPLS L2VPN典型配置指导	1-7
1.2.2 SVC方式的MPLS L2VPN典型配置指导	1-12
1.2.3 Martini方式的MPLS L2VPN典型配置指导	1-18
1.2.4 Kompella方式的MPLS L2VPN典型配置指导	1-24
1.3 MPLS L3VPN典型配置指导	1-29
1.3.1 MPLS L3VPN基本配置典型配置指导	1-29
1.3.2 跨域VPN-OptionA方式典型配置指导	1-40
1.3.3 跨域VPN-OptionB方式典型配置指导	1-50
1.3.4 跨域VPN-OptionC方式典型配置指导	1-59
1.3.5 运营商的运营商典型配置指导	1-69
1.3.6 嵌套VPN典型配置指导	1-81
1.3.7 OSPF伪连接典型配置指导	1-95
1.3.8 BGP的AS号替换配置指导	1-103

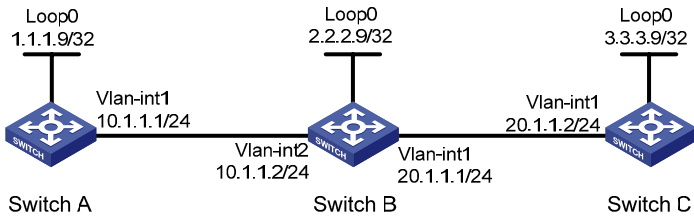
1 MPLS 典型配置指导

1.1 MPLS 基本配置指导

1.1.1 配置 LDP 会话典型配置指导

1. 组网图

图1-1 配置 LDP 会话组网图



2. 应用要求

- Switch A、Switch B 和 Switch C 均支持 MPLS，运行 OSPF 作为 MPLS 骨干网上的 IGP。
- 在 Switch A 和 Switch B、Switch B 和 Switch C 之间建立本地 LDP 会话。
- 在 Switch A 和 Switch C 之间建立远端 LDP 会话。
- 三台设备间使用本地 LDP 会话建立一条 LSP 通道。

3. 适用产品、版本

表1-1 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S7500E 系列以太网交换机	Release 6300 软件版本	LSQ1SRP1CB 引擎或者全部采用 EA 系列业务板

4. 配置过程 and 解释

(1) 配置各接口的 IP 地址

按照 图 1-1配置各接口IP地址和掩码，包括VLAN接口和Loopback接口，配置方法请参见“IP地址-IP性能典型配置指导”。

(2) 配置 OSPF 协议发布的路由信息

配置 Switch A。

```
<SwitchA> system-view
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 1.1.1.9 0.0.0.0
[SwitchA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] quit
```

配置 Switch B。

```
<SwitchB> system-view
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 2.2.2.9 0.0.0.0
[SwitchB-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] quit
```

配置 Switch C。

```
<SwitchC> system-view
[SwitchC] ospf
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 3.3.3.9 0.0.0.0
[SwitchC-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] quit
[SwitchC-ospf-1] quit
```

配置完成后，在各设备上执行 **display ip routing-table** 命令，可以看到相互之间都学到了对方的主机路由。以 Switch A 为例：

```
[SwitchA] display ip routing-table
Routing Tables: Public
          Destinations : 9          Routes : 9
Destination/Mask  Proto  Pre  Cost    NextHop    Interface
-----
1.1.1.9/32       Direct  0     0      127.0.0.1   InLoop0
2.2.2.9/32       OSPF   10    1563     10.1.1.2   Vlan1
3.3.3.9/32       OSPF   10    3125     10.1.1.2   Vlan1
10.1.1.0/24      Direct  0     0      10.1.1.1   Vlan1
10.1.1.1/32      Direct  0     0      127.0.0.1   InLoop0
10.1.1.2/32      Direct  0     0      10.1.1.2   Vlan1
20.1.1.0/24      OSPF   10    3124     10.1.1.2   Vlan1
127.0.0.0/8      Direct  0     0      127.0.0.1   InLoop0
127.0.0.1/32     Direct  0     0      127.0.0.1   InLoop0
```

Switch A 和 Switch B, Switch B 和 Switch C 之间应建立起 OSPF 邻居关系，执行 **display ospf peer verbose** 命令可以看到邻居达到 FULL 状态。以 Switch A 为例：

```
[SwitchA] display ospf peer verbose
          OSPF Process 1 with Switch ID 1.1.1.9
          Neighbors
Area 0.0.0.0 interface 10.1.1.1(Vlan-interface1)'s neighbors
Router ID: 2.2.2.9      Address: 10.1.1.2      GR State: Normal
State: Full  Mode:Nbr is Master  Priority: 1
DR: None  BDR: None  MTU: 1500
Dead timer due in 39 sec
Neighbor is up for 00:02:13
Authentication Sequence: [ 0 ]
```

(3) 配置 MPLS 基本能力，并使能 LDP

配置 Switch A。

```
[SwitchA] mpls lsr-id 1.1.1.9
[SwitchA] mpls
[SwitchA-mpls] quit
[SwitchA] mpls ldp
[SwitchA-mpls-ldp] quit
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] mpls
[SwitchA-Vlan-interface1] mpls ldp
[SwitchA-Vlan-interface1] quit
```

配置 Switch B。

```
[SwitchB] mpls lsr-id 2.2.2.9
[SwitchB] mpls
[SwitchB-mpls] quit
[SwitchB] mpls ldp
[SwitchB-mpls-ldp] quit
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] mpls
[SwitchB-Vlan-interface1] mpls ldp
[SwitchB-Vlan-interface1] quit
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] mpls
[SwitchB-Vlan-interface2] mpls ldp
[SwitchB-Vlan-interface2] quit
```

配置 Switch C。

```
[SwitchC] mpls lsr-id 1.1.1.9
[SwitchC] mpls
[SwitchC-mpls] quit
[SwitchC] mpls ldp
[SwitchC-mpls-ldp] quit
[SwitchC] interface vlan-interface 1
[SwitchC-Vlan-interface1] mpls
[SwitchC-Vlan-interface1] mpls ldp
[SwitchC-Vlan-interface1] quit
```

完成上述配置后，Switch A 和 Switch B、Switch B 和 Switch C 之间的本地 LDP 会话建立成功。

在各设备上执行 **display mpls ldp session** 命令，可以看到 LDP 会话的建立情况；执行 **display mpls ldp peer** 命令，可以看到 LDP 的对等体情况。以 Switch A 为例：

```
[SwitchA] display mpls ldp session

LDP Session(s) in Public Network

Total number of sessions: 1

-----
Peer-ID      Status      LAM  SsnRole  FT   MD5   KA-Sent/Rcv
-----
2.2.2.9:0    Operational  DU   Passive  Off  Off   5/5
-----

LAM : Label Advertisement Mode      FT : Fault Tolerance
```

```
[SwitchA] display mpls ldp peer
LDP Peer Information in Public network
Total number of peers: 1
```

Peer-ID	Transport-Address	Discovery-Source
2.2.2.9:0	2.2.2.9	Vlan-interface1

(4) 配置远端 LDP 会话

配置 Switch A。

```
[SwitchA] mpls ldp remote-peer peerc
[SwitchA-mpls-ldp-remote-peerc] remote-ip 3.3.3.9
[SwitchA-mpls-ldp-remote-peerc] quit
```

配置 Switch C。

```
[SwitchC] mpls ldp remote-peer peera
[SwitchC-mpls-ldp-remote-peera] remote-ip 1.1.1.9
[SwitchC-mpls-ldp-remote-peera] quit
```

完成上述配置后，在 Switch A 上查看 LDP 会话的建立情况和 LDP 的对等体情况，可以看到增加了与 Switch C 的远端 LDP 会话。

```
[SwitchA] display mpls ldp session
LDP Session(s) in Public Network
Total number of sessions: 2
```

Peer-ID	Status	LAM	SsnRole	FT	MD5	KA-Sent/Rcv
2.2.2.9:0	Operational	DU	Passive	Off	Off	35/35
3.3.3.9:0	Operational	DU	Passive	Off	Off	8/8

```

LAM : Label Advertisement Mode      FT : Fault Tolerance
[SwitchA] display mpls ldp peer
```

```
LDP Peer Information in Public network
Total number of peers: 2
```

Peer-ID	Transport-Address	Discovery-Source
2.2.2.9:0	2.2.2.9	Vlan-interface1
3.3.3.9:0	3.3.3.9	Remote Peer : peerc

配置 LSP 的触发策略为 **all**，即所有静态路由和 IGP 路由项都会触发 LDP 建立 LSP。

- 配置 Switch A。

```
[SwitchA] mpls
[SwitchA-mpls] lsp-trigger all
[SwitchA-mpls] return
```

- 配置 Switch B。

```
[SwitchB] mpls
```

```
[SwitchB-mpls] lsp-trigger all
```

```
[SwitchB-mpls] quit
```

- 配置 Switch C。

```
[SwitchC] mpls
```

```
[SwitchC-mpls] lsp-trigger all
```

```
[SwitchC-mpls] quit
```

5. 完整配置

- Switch A 的完整配置

```
#
```

```
mpls lsr-id 1.1.1.9
```

```
#
```

```
mpls
```

```
lsp-trigger all
```

```
#
```

```
mpls ldp
```

```
#
```

```
mpls ldp remote-peer peerc
```

```
remote-ip 3.3.3.9
```

```
#
```

```
interface Vlan-interface1
```

```
mpls
```

```
mpls ldp
```

```
#
```

```
ospf 1
```

```
area 0.0.0.0
```

```
network 1.1.1.9 0.0.0.0
```

```
network 10.1.1.0 0.0.0.255
```

- Switch B 的完整配置

```
#
```

```
mpls lsr-id 2.2.2.9
```

```
#
```

```
mpls
```

```
lsp-trigger all
```

```
#
```

```
mpls ldp
```

```
#
```

```
interface Vlan-interface1
```

```
mpls
```

```
mpls ldp
```

```
#
```

```
interface Vlan-interface2
```

```
mpls
```

```
mpls ldp
```

```
#
```

```
ospf 1
```

```
area 0.0.0.0
```

```
network 2.2.2.9 0.0.0.0
network 10.1.1.0 0.0.0.255
network 20.1.1.0 0.0.0.255
```

- Switch C 的完整配置

```
#
mpls lsr-id 3.3.3.9
#
mpls
lsp-trigger all
#
mpls ldp
#
mpls ldp remote-peer peera
remote-ip 1.1.1.9
#
interface Vlan-interface1
mpls
mpls ldp
#
ospf 1
area 0.0.0.0
network 3.3.3.9 0.0.0.0
network 20.1.1.0 0.0.0.255
```

6. 配置注意事项

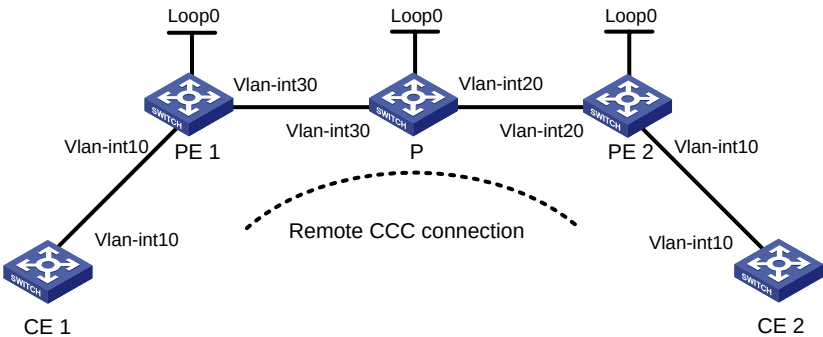
- 由于 MPLS 功能会在原有报文上封装一层或多层标签，因此建议用户在使能某 VLAN 接口的 MPLS 功能后，将该 VLAN 内端口的 jumboframe 功能开启，并根据实际应用和标签嵌套层数配置相应的帧长，避免某些报文因超长而被丢弃。例如：如果需要对 FTP 报文封装两层 MPLS 标签，请配置端口的 jumboframe 帧长为 1544 字节（FTP 报文 1518 字节 + MPLS 标签 4 字节 × 2 + VLAN 标签 4 字节 + 以太网帧头长度 14 字节）。关于 jumboframe 功能请参见接入分册的“以太网端口配置”。
- 如果取消接口的 LDP 能力将会导致接口下的所有 LDP 会话中断，基于这些会话的所有 LSP 也将被删除。
- 如果对等体与指定的远端对等体之间已经存在本地邻接关系，则远程邻接关系将不能建立。
- 如果已经存在远程邻接关系，又为远端对等体创建了本地邻接关系，则在本地对等体和远端对等体的 LDP 传输地址、Keepalive 保持时间配置一致时，将建立本地邻接关系，远端对等体将被删除；本地对等体和远端对等体的 LDP 传输地址或 Keepalive 保持时间配置不一致时，将无法建立本地邻接关系，继续保持远程邻接关系。即两个 LSR 之间只能存在一个远程会话或一个本地会话，并且，本地会话的优先级高于远程会话。
- 即将配置的远端对等体的 IP 地址不能与已经存在的远端对等体 IP 地址重复；否则配置不成功，将返回出错消息。

1.2 MPLS L2VPN 典型配置指导

1.2.1 CCC 远程连接方式的 MPLS L2VPN 典型配置指导

1. 组网图

图1-2 CCC 远程连接方式的 MPLS L2VPN 组网图



设备	接口	IP 地址	设备	接口	IP 地址
CE 1	Vlan-int10	100.1.1.1/24	P	Loop0	10.0.0.2/32
PE 1	Loop0	10.0.0.1/32		Vlan-int20	10.2.2.2/24
	Vlan-int30	10.1.1.1/24		Vlan-int30	10.1.1.2/24
CE 2	Vlan-int10	100.1.1.2/24	PE 2	Loop0	10.0.0.3/32
				Vlan-int20	10.2.2.1/24

2. 应用要求

在 PE1 和 PE2 之间建立 CCC 远程连接，为 CE1 和 CE2 之间提供 MPLS L2VPN 服务。

3. 适用产品、版本

表1-2 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S7500E 系列以太网交换机	Release 6300 软件版本	LSQ1SRP1CB 引擎或者全部采用 EA 系列业务板

4. 配置过程 and 解释

配置 CCC 远程连接的关键步骤包括：

- 在 PE 上创建 CCC 远程连接（不需要配置静态 LSP）。
- 在 P 上配置两条静态 LSP，用于双向传递报文。

(1) 配置 CE 1

配置 VLAN10 接口的 IP 地址。

```
<CE1> system-view
[CE1] interface vlan-interface 10
[CE1-Vlan-interface10] ip address 100.1.1.1 24
```

(2) 配置 PE 1

配置 Loopback0 接口的 IP 地址，并作为 LSR ID，开启全局 MPLS 功能。

```
<PE1> system-view
[PE1] interface loopback 0
```

```
[PE1-LoopBack0] ip address 10.0.0.1 32
```

```
[PE1-LoopBack0] quit
```

```
[PE1] mpls lsr-id 10.0.0.1
```

```
[PE1] mpls
```

```
[PE1-mpls] quit
```

开启全局 MPLS L2VPN 功能。

```
[PE1] mpls l2vpn
```

创建 Vlan-interface10 接口。

```
[PE1] interface Vlan-interface 10
```

```
[PE1-Vlan-interface10] quit
```

配置接口 Vlan-interface30 的 IP 地址，并在该接口下开启 MPLS 功能。

```
[PE1] interface vlan-interface 30
```

```
[PE1-Vlan-interface30] ip address 10.1.1.1 24
```

```
[PE1-Vlan-interface30] mpls
```

```
[PE1-Vlan-interface30] quit
```

创建 CE 1 到 CE 2 的远程连接：入接口为连接 CE 1 的接口 Vlan-interface 10，入标签为 100；下一跳地址为 P 的 Vlan-interface30 地址，出标签为 200。

```
[PE1] ccc ce1-ce2 interface vlan-interface 10 in-label 100 out-label 200 next-hop 10.1.1.2
```

(3) 配置 P

配置 Loopback0 接口的 IP 地址，并作为 LSR ID，开启全局 MPLS 功能。

```
<P> system-view
```

```
[P] interface loopback 0
```

```
[P-LoopBack0] ip address 10.0.0.2 32
```

```
[P-LoopBack0] quit
```

```
[P] mpls lsr-id 10.0.0.2
```

```
[P] mpls
```

```
[P-mpls] quit
```

配置接口 Vlan-interface30 的 IP 地址，并在该接口下开启 MPLS 功能。

```
[P] interface vlan-interface 30
```

```
[P-Vlan-interface30] ip address 10.1.1.2 24
```

```
[P-Vlan-interface30] mpls
```

```
[P-Vlan-interface30] quit
```

配置接口 Vlan-interface20 的 IP 地址，并在该接口下开启 MPLS 功能。

```
[P] interface vlan-interface 20
```

```
[P-Vlan-interface20] ip address 10.2.2.2 24
```

```
[P-Vlan-interface20] mpls
```

```
[P-Vlan-interface20] quit
```

配置一条静态 LSP 用于转发由 PE 1 去往 PE 2 的报文：入接口为 Vlan-interface 30，入标签为 200，下一跳地址为 PE 2 的 Vlan-interface 20 的接口地址，出标签为 201。

```
[P] static-lsp transit pe1_pe2 incoming-interface vlan-interface 30 in-label 200 next-hop 10.2.2.1 out-label 201
```

配置另一条静态 LSP 用于转发由 PE 2 去往 PE 1 的报文：入接口为 Vlan-interface 20，入标签为 101，下一跳地址为 PE 1 的 Vlan-interface 30 的接口地址，出标签为 100。

```
[P] static-lsp transit pe2_pe1 incoming-interface vlan-interface 20 in-label 101 next-hop 10.1.1.1 out-label 100
```

(4) 配置 PE 2

配置 Loopback0 接口的 IP 地址，并作为 LSR ID，开启全局 MPLS 功能。

```
<PE2> system-view
[PE2] interface loopback 0
[PE2-LoopBack0] ip address 10.0.0.3 32
[PE2-LoopBack0] quit
[PE2] mpls lsr-id 10.0.0.3
[PE2] mpls
[PE2-mpls] quit
```

开启全局 MPLS L2VPN 功能。

```
[PE2] mpls l2vpn
```

配置接口 Vlan-interface10。

```
[PE2] interface vlan-interface 10
[PE2-Vlan-interface10] quit
```

配置接口 Vlan-interface20 的 IP 地址，并在该接口下开启 MPLS 功能。

```
[PE2] interface vlan-interface 20
[PE2-Vlan-interface20] ip address 10.2.2.1 24
[PE2-Vlan-interface20] mpls
[PE2-Vlan-interface20] quit
```

创建 CE 2 到 CE 1 的远程连接：入接口为连接 CE 2 的接口 Vlan-interface 10，入标签为 201；下一跳地址为 P 设备 Vlan-interface20 接口地址，出标签为 101。

```
[PE2] ccc ce2-ce1 interface vlan-interface 10 in-label 201 out-label 101 next-hop 10.2.2.2
```

(5) 配置 CE 2

```
<CE2> system-view
[CE2] interface vlan-interface 10
[CE2-Vlan-interface10] ip address 100.1.1.2 24
```

(6) 配置完成后的检验

配置完成后，在 PE 1 上查看 CCC 连接信息，可以看到建立了一条 CCC 本地连接。

```
[PE1] display ccc
Total ccc vc      : 1
Local ccc vc      : 0, 0 up
Remote ccc vc     : 1, 1 up
***Name           : ce1-ce2
Type              : remote
State             : up
Intf              : Vlan-interface10 (up)
In-label          : 100
Out-label         : 200
Nexthop           : 10.1.1.2
```

CE 1 与 CE 2 之间能够 ping 通。

```
[CE1] ping 100.1.1.2
PING 100.1.1.2: 56 data bytes, press CTRL_C to break
  Reply from 100.1.1.2: bytes=56 Sequence=1 ttl=255 time=180 ms
  Reply from 100.1.1.2: bytes=56 Sequence=2 ttl=255 time=60 ms
  Reply from 100.1.1.2: bytes=56 Sequence=3 ttl=255 time=10 ms
  Reply from 100.1.1.2: bytes=56 Sequence=4 ttl=255 time=70 ms
  Reply from 100.1.1.2: bytes=56 Sequence=5 ttl=255 time=60 ms
--- 100.1.1.2 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 10/76/180 ms
```

5. 完整配置

- CE 1 的完整配置

```
#
interface Vlan-interface10
 ip address 100.1.1.1 255.255.255.0
```

- PE 1 的完整配置

```
#
mpls lsr-id 10.0.0.1
#
mpls
#
mpls l2vpn
#
interface LoopBack0
 ip address 10.0.0.1 255.255.255.255
#
interface Vlan-interface10
#
interface Vlan-interface30
 ip address 10.1.1.1 255.255.255.0
mpls
#
ccc ce1-ce2 interface Vlan-interface10 in-label 100 out-label 200 nexthop 10.1.1.2
```

- P 的完整配置

```
#
mpls lsr-id 10.0.0.2
#
mpls
#
interface Vlan-interface20
 ip address 10.2.2.2 255.255.255.0
mpls
#
```



```

interface Vlan-interface30
 ip address 10.1.1.2 255.255.255.0
 mpls
#
 static-lsp transit pe1_pe2 incoming-interface Vlan-interface30 in-label 200 nexthop
10.2.2.1 out-label 201
 static-lsp transit pe2_pe1 incoming-interface Vlan-interface20 in-label 101 nexthop
10.1.1.1 out-label 100

```

- PE 2 的完整配置

```

#
 mpls lsr-id 10.0.0.3
#
 mpls
#
 mpls l2vpn
#
 interface LoopBack0
 ip address 10.0.0.3 255.255.255.255
#
 interface Vlan-interface10
#
 interface Vlan-interface20
 ip address 10.2.2.1 255.255.255.0
 mpls
#
 ccc ce2-ce1 interface vlan-interface 10 in-label 201 out-label 101 next-hop 10.2.2.2

```

- CE 2 的完整配置

```

#
 interface Vlan-interface10
 ip address 100.1.1.2 255.255.255.0

```

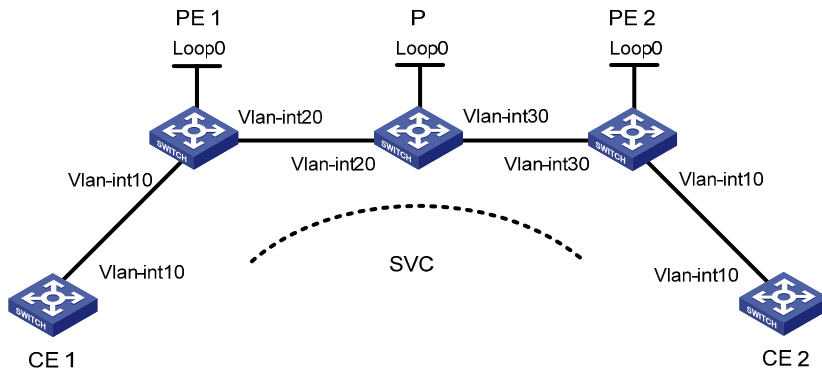
6. 配置注意事项

- 在 PE 上不必为 CCC 远程连接配置静态 LSP，仅需要在创建 CCC 远程连接时为它配置入标签和出标签即可，一个入标签对应一个 CCC 连接，相当于配置了静态 LSP。
- PE 之间的所有 P 路由器上需要配置两条方向相反静态 LSP，用于专门传输 CCC 连接的数据。

1.2.2 SVC 方式的 MPLS L2VPN 典型配置指导

1. 组网图

图1-3 SVC 方式的 MPLS L2VPN 组网图



设备	接口	IP 地址	设备	接口	IP 地址
CE 1	Vlan-int10	100.1.1.1/24	P	Loop0	192.4.4.4/32
PE 1	Loop0	192.2.2.2/32		Vlan-int30	10.2.2.2/24
	Vlan-int20	10.1.1.1/24		Vlan-int20	10.1.1.2/24
CE 2	Vlan-int10	100.1.1.2/24	PE 2	Loop0	192.3.3.3/32
				Vlan-int30	10.2.2.1/24

2. 应用要求

在 PE1 和 PE2 之间建立 SVC 方式的 MPLS L2VPN，为 CE1 和 CE2 之间的数据通信提供隧道服务。

3. 适用产品、版本

表1-3 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S7500E 系列以太网交换机	Release 6300 软件版本	LSQ1SRP1CB 引擎或者全部采用 EA 系列业务板

4. 配置过程 and 解释

主要的配置步骤可分为两部分：

- 在 PE 和 P 上配置 MPLS 基本转发能力：包括配置 LSR ID、使能 MPLS 和 LDP、在 PE 1—P—PE 2 之间运行 IGP（本配置例中使用 OSPF）以建立 LSP。
- 建立 SVC 方式的 MPLS L2VPN 连接：包括在 PE 1 和 PE 2 上使能 MPLS L2VPN、创建 SVC 连接并指定 VC 标签。

(1) 配置 CE 1

```
<CE1> system-view
[CE1] interface vlan-interface 10
[CE1-Vlan-interface10] ip address 100.1.1.1 24
```

(2) 配置 PE 1

配置 LSR ID，全局使能 MPLS。

```
<PE1> system-view
[PE1] interface loopback 0
```

```
[PE1-LoopBack0] ip address 192.2.2.2 32
```

```
[PE1-LoopBack0] quit
```

```
[PE1] mpls lsr-id 192.2.2.2
```

```
[PE1] mpls
```

配置触发 LSP 的建立。

```
[PE1-mpls] lsp-trigger all
```

```
[PE1-mpls] quit
```

全局使能 MPLS L2VPN 和 LDP。

```
[PE1] mpls l2vpn
```

```
[PE1] mpls ldp
```

```
[PE1-mpls-ldp] quit
```

配置连接 P 的接口 Vlan-interface20，在此接口上使能 LDP。

```
[PE1] interface vlan-interface 20
```

```
[PE1-Vlan-interface20] ip address 10.1.1.1 24
```

```
[PE1-Vlan-interface20] mpls
```

```
[PE1-Vlan-interface20] mpls ldp
```

```
[PE1-Vlan-interface20] quit
```

在 PE 1 上运行 OSPF，用于建立 LSP。

```
[PE1] ospf
```

```
[PE1-ospf-1] area 0
```

```
[PE1-ospf-1-area-0.0.0.0] network 10.1.1.1 0.0.0.255
```

```
[PE1-ospf-1-area-0.0.0.0] network 192.2.2.2 0.0.0.0
```

```
[PE1-ospf-1-area-0.0.0.0] quit
```

```
[PE1-ospf-1] quit
```

在接入 CE 1 的接口 Vlan-interface10 上创建一条 SVC 方式 MPLS L2VPN 连接。此接口不需配置 IP 地址。

```
[PE1] interface vlan-interface 10
```

```
[PE1-Vlan-interface10] mpls static-l2vc destination 192.3.3.3 transmit-vpn-label 100  
receive-vpn-label 200
```

```
[PE1-Vlan-interface10] quit
```

(3) 配置 P

配置 LSR ID，全局使能 MPLS。

```
<P> system-view
```

```
[P] interface loopback 0
```

```
[P-LoopBack0] ip address 192.4.4.4 32
```

```
[P-LoopBack0] quit
```

```
[P] mpls lsr-id 192.4.4.4
```

```
[P] mpls
```

配置触发 LSP 的建立。

```
[P-mpls] lsp-trigger all
```

```
[P-mpls] quit
```

全局使能 LDP。

```
[P] mpls ldp
```

```
[P-mps-ldp] quit
```

配置连接 PE 1 的接口 Vlan-interface20，在此接口上使能 LDP。

```
[P] interface vlan-interface 20
```

```
[P-Vlan-interface20] ip address 10.1.1.2 24
```

```
[P-Vlan-interface20] mpls
```

```
[P-Vlan-interface20] mpls ldp
```

```
[P-Vlan-interface20] quit
```

配置连接 PE 2 的接口 Vlan-interface30，在此接口上使能 LDP。

```
[P] interface vlan-interface 30
```

```
[P-Vlan-interface30] link-protocol ppp
```

```
[P-Vlan-interface30] ip address 10.2.2.2 24
```

```
[P-Vlan-interface30] mpls
```

```
[P-Vlan-interface30] mpls ldp
```

```
[P-Vlan-interface30] quit
```

在 P 上运行 OSPF，用于建立 LSP。

```
[P] ospf
```

```
[P-ospf-1] area 0
```

```
[P-ospf-1-area-0.0.0.0] network 10.1.1.2 0.0.0.255
```

```
[P-ospf-1-area-0.0.0.0] network 10.2.2.2 0.0.0.255
```

```
[P-ospf-1-area-0.0.0.0] network 192.4.4.4 0.0.0.0
```

```
[P-ospf-1-area-0.0.0.0] quit
```

```
[P-ospf-1] quit
```

(4) 配置 PE 2

配置 LSR ID，全局使能 MPLS。

```
<PE2> system-view
```

```
[PE2] interface loopback 0
```

```
[PE2-LoopBack0] ip address 192.3.3.3 32
```

```
[PE2-LoopBack0] quit
```

```
[PE2] mpls lsr-id 192.3.3.3
```

```
[PE2] mpls
```

配置触发 LSP 的建立。

```
[PE2-mpls] lsp-trigger all
```

```
[PE2-mpls] quit
```

全局使能 MPLS L2VPN 和 LDP。

```
[PE2] mpls l2vpn
```

```
[PE2] mpls ldp
```

```
[PE2-mpls-ldp] quit
```

配置连接 P 的接口 Vlan-interface30，在此接口上使能 LDP。

```
[PE2] interface vlan-interface 30
```

```
[PE2-Vlan-interface30] ip address 10.2.2.1 24
```

```
[PE2-Vlan-interface30] mpls
```

```
[PE2-Vlan-interface30] mpls ldp
```

```
[PE2-Vlan-interface30] quit
```

在 PE 2 上运行 OSPF，用于建立 LSP。

```
[PE2] ospf
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 10.2.2.1 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] network 192.3.3.3 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

在接入 CE 2 的接口 Vlan-interface10 上创建一条 SVC 方式 MPLS L2VPN 连接。此接口不需配置 IP 地址。

```
[PE2] interface vlan-interface 10
[PE2-Vlan-interface10] mpls static-l2vc destination 192.2.2.2 transmit-vpn-label 200
receive-vpn-label 100
[PE2-Vlan-interface10] quit
```

(5) 配置 CE 2

```
<CE2> system-view
[CE2] interface vlan-interface 10
[CE2-Vlan-interface10] ip address 100.1.1.2 24
```

- 配置完成后的检验

在 PE 1 上查看 SVC 的 L2VPN 连接信息，可以看到建立了一条 L2VPN 连接。

```
[PE1] display mpls static-l2vc
total connections: 1, 1 up, 0 down


| ce-intf | state | destination | tr-label | rcv-label | tnl-policy |
|---------|-------|-------------|----------|-----------|------------|
| Vlan10  | up    | 192.3.3.3   | 100      | 200       | default    |


```

在 PE 2 上也可以看到 SVC 的 L2VPN 连接。

```
[PE2] display mpls static-l2vc
total connections: 1, 1 up, 0 down


| ce-intf | state | destination | tr-label | rcv-label | tnl-policy |
|---------|-------|-------------|----------|-----------|------------|
| Vlan20  | up    | 192.2.2.2   | 200      | 100       | default    |


```

CE 1 与 CE 2 之间能够 ping 通。

```
[CE1] ping 100.1.1.2
PING 100.1.1.2: 56 data bytes, press CTRL_C to break
  Reply from 100.1.1.2: bytes=56 Sequence=1 ttl=255 time=150 ms
  Reply from 100.1.1.2: bytes=56 Sequence=2 ttl=255 time=130 ms
  Reply from 100.1.1.2: bytes=56 Sequence=3 ttl=255 time=130 ms
  Reply from 100.1.1.2: bytes=56 Sequence=4 ttl=255 time=140 ms
  Reply from 100.1.1.2: bytes=56 Sequence=5 ttl=255 time=80 ms
--- 100.1.1.2 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 80/126/150 ms
```

5. 完整配置

- CE 1 的完整配置

#

```

interface Vlan-interface10
 ip address 100.1.1.1 255.255.255.0

```

- PE 1 的完整配置

```

#
mpls lsr-id 192.2.2.2
#
mpls
 lsp-trigger all
#
mpls l2vpn
#
mpls ldp
#
interface LoopBack0
 ip address 192.2.2.2 255.255.255.255
#
interface Vlan-interface10
 mpls static-l2vc destination 192.3.3.3 transmit-vpn-label 100 receive-vpn-label 200
#
interface Vlan-interface20
 ip address 10.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
ospf 1
 area 0
  network 10.1.1.1 0.0.0.255
  network 192.2.2.2 0.0.0.0

```

- P 的完整配置

```

#
mpls lsr-id 192.4.4.4
#
mpls
 lsp-trigger all
#
mpls ldp
#
interface LoopBack0
 ip address 192.4.4.4 255.255.255.255
#
interface Vlan-interface20
 ip address 10.1.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface Vlan-interface30
 ip address 10.2.2.2 255.255.255.0
 mpls

```

```

mpls ldp
#
ospf 1
area 0
network 10.1.1.2 0.0.0.255
network 10.2.2.2 0.0.0.255
network 192.4.4.4 0.0.0.0

```

- PE 2 的完整配置

```

#
mpls lsr-id 192.3.3.3
#
mpls
lsp-trigger all
#
mpls l2vpn
#
mpls ldp
#
interface LoopBack0
ip address 192.3.3.3 255.255.255.255
#
interface Vlan-interface10
mpls static-l2vc destination 192.2.2.2 transmit-vpn-label 200 receive-vpn-label 100
#
interface Vlan-interface30
ip address 10.2.2.1 255.255.255.0
mpls
mpls ldp
#
ospf 1
area 0
network 10.2.2.1 0.0.0.255
network 192.3.3.3 0.0.0.0

```

- CE 2 的完整配置

```

#
interface Vlan-interface10
ip address 100.1.1.2 255.255.255.0

```

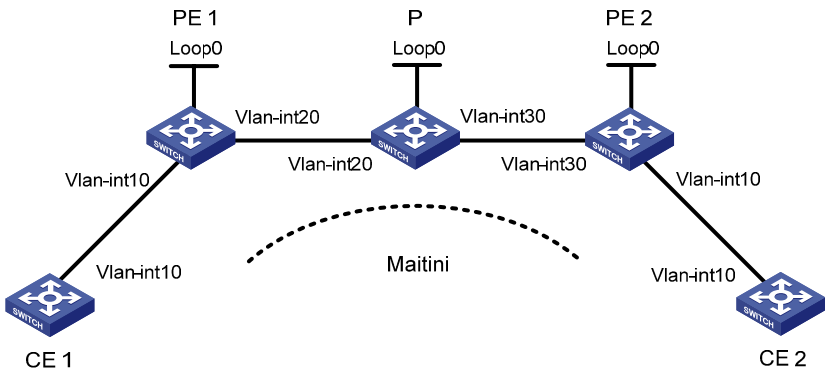
6. 配置注意事项

无

1.2.3 Martini 方式的 MPLS L2VPN 典型配置指导

1. 组网图

图1-4 Martini 方式的 MPLS L2VPN 组网图



设备	接口	IP 地址	设备	接口	IP 地址
CE 1	Vlan-int10	100.1.1.1/24	P	Loop0	192.4.4.4/32
PE 1	Loop0	192.2.2.2/32		Vlan-int20	10.1.1.2/24
	Vlan-int20	10.1.1.1/24		Vlan-int30	10.2.2.2/24
CE 2	Vlan-int10	100.1.1.2/24	PE 2	Loop0	192.3.3.3/32
				Vlan-int30	10.2.2.1/24

2. 应用要求

在 PE1 和 PE2 之间建立 Martini 方式的 MPLS L2VPN，为 CE1 和 CE2 之间的数据通信提供隧道服务。

3. 适用产品、版本

表1-4 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S7500E 系列以太网交换机	Release 6300 软件版本	LSQ1SRP1CB 引擎或者全部采用 EA 系列业务板

4. 配置过程 and 解释

(1) 配置 CE 1

```
<CE1> system-view
[CE1] interface vlan-interface 10
[CE1-Vlan-interface10] ip address 100.1.1.1 24
```

(2) 配置 PE 1

配置 LSR ID，全局使能 MPLS。

```
<PE1> system-view
[PE1] interface loopback 0
[PE1-LoopBack0] ip address 192.2.2.2 32
[PE1-LoopBack0] quit
[PE1] mpls lsr-id 192.2.2.2
[PE1] mpls
```

配置触发 LSP 的建立。


```
[PE1-mpls] lsp-trigger all
```

```
[PE1-mpls] quit
```

全局使能 MPLS L2VPN 和 LDP。

```
[PE1] mpls l2vpn
```

```
[PE1] mpls ldp
```

```
[PE1-mpls-ldp] quit
```

配置 PE 1 与 PE 2 建立 LDP 远程会话。

```
[PE1] mpls ldp remote-peer 1
```

```
[PE1-mpls-ldp-remote-1] remote-ip 192.3.3.3
```

```
[PE1-mpls-ldp-remote-1] quit
```

配置连接 P 的接口 Vlan-interface20，在此接口上使能 LDP。

```
[PE1] interface vlan-interface 20
```

```
[PE1-Vlan-interface20] ip address 10.1.1.1 24
```

```
[PE1-Vlan-interface20] mpls
```

```
[PE1-Vlan-interface20] mpls ldp
```

```
[PE1-Vlan-interface20] quit
```

在 PE 1 上运行 OSPF，用于建立 LSP。

```
[PE1] ospf
```

```
[PE1-ospf-1] area 0
```

```
[PE1-ospf-1-area-0.0.0.0] network 10.1.1.1 0.0.0.255
```

```
[PE1-ospf-1-area-0.0.0.0] network 192.2.2.2 0.0.0.0
```

```
[PE1-ospf-1-area-0.0.0.0] quit
```

```
[PE1-ospf-1] quit
```

在接入 CE 1 的接口 Vlan-interface10 上创建 L2VPN 连接。此接口不需配置 IP 地址。

```
[PE1] interface vlan-interface 10
```

```
[PE1-Vlan-interface10] mpls l2vc 192.3.3.3 101
```

```
[PE1-Vlan-interface10] quit
```

(3) 配置 P

配置 LSR ID，全局使能 MPLS。

```
<P> system-view
```

```
[P] interface loopback 0
```

```
[P-LoopBack0] ip address 192.4.4.4 32
```

```
[P-LoopBack0] quit
```

```
[P] mpls lsr-id 192.4.4.4
```

```
[P] mpls
```

配置触发 LSP 的建立。

```
[P-mpls] lsp-trigger all
```

```
[P-mpls] quit
```

全局使能 LDP。

```
[P] mpls ldp
```

```
[P-mpls-ldp] quit
```

配置连接 PE 1 的接口 Vlan-interface20，在此接口上使能 LDP。

```
[P] interface vlan-interface 20
[P-Vlan-interface20] ip address 10.1.1.2 24
[P-Vlan-interface20] mpls
[P-Vlan-interface20] mpls ldp
[P-Vlan-interface20] quit
```

配置连接 PE 2 的接口 Vlan-interface30，在此接口上使能 LDP。

```
[P] interface vlan-interface 30
[P-Vlan-interface30] ip address 10.2.2.2 24
[P-Vlan-interface30] mpls
[P-Vlan-interface30] mpls ldp
[P-Vlan-interface30] quit
```

在 P 上运行 OSPF，用于建立 LSP。

```
[P] ospf
[P-ospf-1] area 0
[P-ospf-1-area-0.0.0.0] network 10.1.1.2 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 10.2.2.2 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 192.4.4.4 0.0.0.0
[P-ospf-1-area-0.0.0.0] quit
[P-ospf-1] quit
```

(4) 配置 PE 2

配置 LSR ID，全局使能 MPLS。

```
<PE2> system-view
[PE2] interface loopback 0
[PE2-LoopBack0] ip address 192.3.3.3 32
[PE2-LoopBack0] quit
[PE2] mpls lsr-id 192.3.3.3
[PE2] mpls
```

配置触发 LSP 的建立。

```
[PE2-mpls] lsp-trigger all
[PE2-mpls] quit
```

全局使能 MPLS L2VPN 和 LDP。

```
[PE2] mpls l2vpn
[PE2] mpls ldp
[PE2-mpls-ldp] quit
```

配置 PE 2 与 PE 1 建立 LDP 远程会话。

```
[PE2] mpls ldp remote-peer 2
[PE2-mpls-ldp-remote-2] remote-ip 192.2.2.2
[PE2-mpls-ldp-remote-2] quit
```

配置连接 P 的接口 Vlan-interface30，在此接口上使能 LDP。

```
[PE2] interface vlan-interface 30
[PE2-Vlan-interface30] ip address 10.2.2.1 24
[PE2-Vlan-interface30] mpls
[PE2-Vlan-interface30] mpls ldp
[PE2-Vlan-interface30] quit
```

在 PE 2 上运行 OSPF，用于建立 LSP。

```
[PE2] ospf
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 192.3.3.3 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] network 10.2.2.1 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

在接入 CE 2 的接口 Vlan-interface10 上创建 L2VPN 连接。此接口不需配置 IP 地址。

```
[PE2] interface vlan-interface 10
[PE2-Vlan-interface10] mpls l2vc 192.2.2.2 101
[PE2-Vlan-interface10] quit
```

(5) 配置 CE 2

```
<CE2> system-view
[CE2] interface vlan-interface 10
[CE2-Vlan-interface10] ip address 100.1.1.2 24
```

(6) 配置完成后的检验

在 PE 1 上查看 L2VPN 连接信息，可以看到建立了一条 L2VC。

```
[PE1] display mpls l2vc
total ldp vc : 1      1 up      0 down
```

Transport	Client	VC	Local	Remote	Tunnel
VC ID	Intf	State	VC Label	VC Label	Policy
101	Vlan10	up	8193	8192	default

在 PE 2 上也可以看到 L2VC 连接。

```
[PE2] display mpls l2vc
total ldp vc : 1      1 up      0 down
```

Transport	Client	VC	Local	Remote	Tunnel
VC ID	Intf	State	VC Label	VC Label	Policy
101	Vlan10	up	8192	8193	default

CE 1 与 CE 2 之间能够 ping 通。

```
[CE1] ping 100.1.1.2
  PING 100.1.1.2: 56 data bytes, press CTRL_C to break
    Reply from 100.1.1.2: bytes=56 Sequence=1 ttl=255 time=30 ms
    Reply from 100.1.1.2: bytes=56 Sequence=2 ttl=255 time=60 ms
    Reply from 100.1.1.2: bytes=56 Sequence=3 ttl=255 time=50 ms
    Reply from 100.1.1.2: bytes=56 Sequence=4 ttl=255 time=40 ms
    Reply from 100.1.1.2: bytes=56 Sequence=5 ttl=255 time=70 ms
  --- 100.1.1.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 30/50/70 ms
```

5. 完整配置

- CE 1 的完整配置

```
#  
interface Vlan-interface10  
ip address 100.1.1.1 255.255.255.0
```

- PE 1 的完整配置

```
#  
mpls lsr-id 192.2.2.2  
#  
mpls  
lsp-trigger all  
#  
mpls l2vpn  
#  
mpls ldp  
#  
mpls ldp remote-peer 1  
remote-ip 192.3.3.3  
#  
interface LoopBack0  
ip address 192.2.2.2 255.255.255.255  
#  
interface Vlan-interface10  
mpls l2vc 192.3.3.3 101  
#  
interface Vlan-interface20  
ip address 10.1.1.1 255.255.255.0  
mpls  
mpls ldp  
#  
ospf 1  
area 0  
network 10.1.1.1 0.0.0.255  
network 192.2.2.2 0.0.0.0
```

- P 的完整配置

```
#  
mpls lsr-id 192.4.4.4  
#  
mpls  
lsp-trigger all  
#  
mpls ldp  
#  
interface LoopBack0  
ip address 192.4.4.4 255.255.255.255  
#  
interface Vlan-interface20
```

```

ip address 10.1.1.2 255.255.255.0
mpls
mpls ldp
#
interface Vlan-interface30
ip address 10.2.2.2 255.255.255.0
mpls
mpls ldp
#
ospf 1
area 0
network 10.1.1.2 0.0.0.255
network 10.2.2.2 0.0.0.255
network 192.4.4.4 0.0.0.0

```

- PE 2 的完整配置

```

#
mpls lsr-id 192.3.3.3
#
mpls
lsp-trigger all
#
mpls l2vpn
#
mpls ldp
#
mpls ldp remote-peer 2
remote-ip 192.2.2.2
#
interface LoopBack0
ip address 192.3.3.3 255.255.255.255
#
interface Vlan-interface10
mpls l2vc 192.2.2.2 101
#
interface Vlan-interface30
ip address 10.2.2.1 255.255.255.0
mpls
mpls ldp
#
ospf 1
area 0
network 10.2.2.1 0.0.0.255
network 192.3.3.3 0.0.0.0

```

- CE 2 的完整配置

```

#
interface Vlan-interface10
ip address 100.1.1.2 255.255.255.0

```

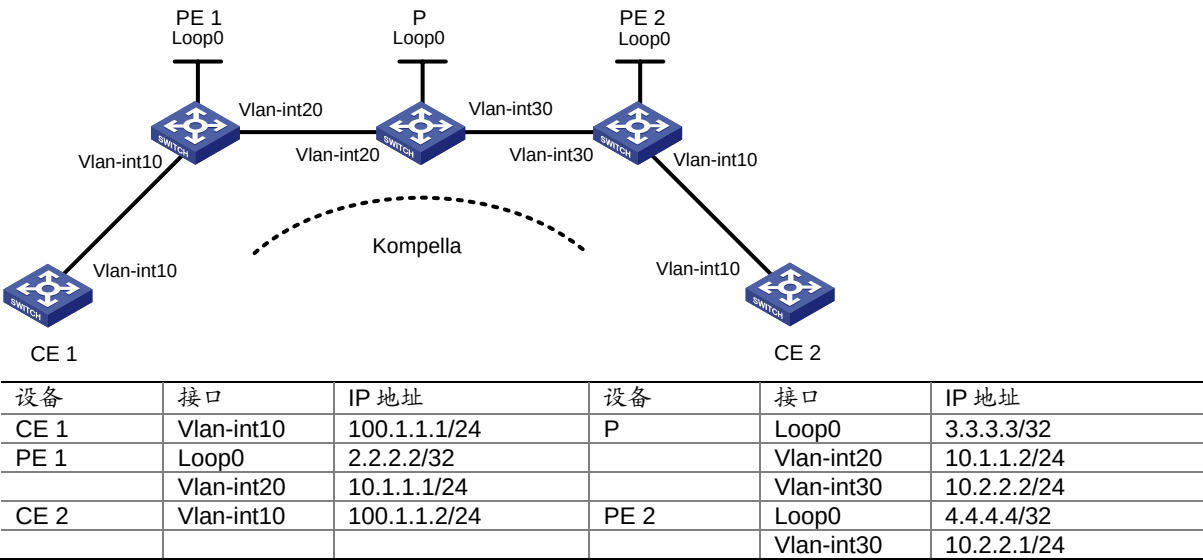
6. 配置注意事项

无

1.2.4 Kompella 方式的 MPLS L2VPN 典型配置指导

1. 组网图

图1-5 Kompella 方式的 MPLS L2VPN 组网图



2. 应用要求

在 PE1 和 PE2 之间建立 Kompella 方式的 MPLS L2VPN，为 CE1 和 CE2 之间的数据通信提供隧道服务。

3. 适用产品、版本

表1-5 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S7500E 系列以太网交换机	Release 6300 软件版本	LSQ1SRP1CB 引擎或者全部采用 EA 系列业务板

4. 配置过程 and 解释

(1) 在 MPLS 骨干网上配置 IGP

本例中使用 OSPF，具体配置步骤请参考以上几个 MPLS L2VPN 配置举例。
配置完成后，在各 LSR 上执行 **display ip routing-table** 命令可以看到都已学到彼此 LSR ID 的路由；执行 **display ospf peer** 命令可以建立了 OSPF 邻居关系，状态为 FULL。

(2) 配置 MPLS 基本能力和 LDP，建立 LDP LSP

具体配置步骤请参考以上几个 MPLS L2VPN 配置举例。
配置完成后，在各 LSR 上执行 **display mpls ldp session** 和 **display mpls ldp peer** 命令可以看到 LDP 会话和对等体的建立情况，执行 **display mpls lsp** 命令可以看到 LSP 的建立情况。

(3) 配置 BGP 的 L2VPN 能力

配置 PE 1。

```
<PE1> system-view
[PE1] mpls l2vpn
[PE1] bgp 100
[PE1-bgp] peer 4.4.4.4 as-number 100
[PE1-bgp] peer 4.4.4.4 connect-interface loopback 0
[PE1-bgp] l2vpn-family
[PE1-bgp-af-l2vpn] policy vpn-target
[PE1-bgp-af-l2vpn] peer 4.4.4.4 enable
[PE1-bgp-af-l2vpn] quit
[PE1-bgp] quit
```

配置 PE 2。

```
<PE2> system-view
[PE2] mpls l2vpn
[PE2] bgp 100
[PE2-bgp] peer 2.2.2.2 as-number 100
[PE2-bgp] peer 2.2.2.2 connect-interface loopback 0
[PE2-bgp] l2vpn-family
[PE2-bgp-af-l2vpn] policy vpn-target
[PE2-bgp-af-l2vpn] peer 2.2.2.2 enable
[PE2-bgp-af-l2vpn] quit
[PE2-bgp] quit
```

配置完成后，在 PE 1 和 PE 2 上执行 **display bgp l2vpn peer** 命令可以看到 PE 之间建立了对等体关系，状态为 Established。

以 PE 1 为例：

```
[PE1] display bgp l2vpn peer
BGP local router ID : 2.2.2.2
Local AS number : 100
Total number of peers : 1          Peers in established state : 1
Peer      V   AS   MsgRcvd   MsgSent   OutQ   PrefRcv   Up/Down   State
4.4.4.4   4   100      2         5         0         0   00:01:07 Established
```

(4) 配置 L2VPN 和 CE 连接

配置 PE 1。

```
[PE1] mpls l2vpn vpn1 encapsulation vlan
[PE1-mpls-l2vpn-vpn1] route-distinguisher 100:1
[PE1-mpls-l2vpn-vpn1] vpn-target 1:1
[PE1-mpls-l2vpn-vpn1] ce ce1 id 1 range 10
[PE1-mpls-l2vpn-ce-vpn1-ce1] connection ce-offset 2 interface Vlan-interface10
[PE1-mpls-l2vpn-ce-vpn1-ce1] quit
[PE1-mpls-l2vpn-vpn1] quit
```

配置 PE 2。

```
[PE2] mpls l2vpn vpn1 encapsulation vlan
[PE2-mpls-l2vpn-vpn1] route-distinguisher 100:1
[PE2-mpls-l2vpn-vpn1] vpn-target 1:1
[PE2-mpls-l2vpn-vpn1] ce ce2 id 2 range 10
```

```
[PE2-mppls-l2vpn-ce-vpn1-ce2] connection ce-offset 1 interface vlan-interface 10
[PE2-mppls-l2vpn-ce-vpn1-ce2] quit
[PE2-mppls-l2vpn-vpn1] quit
```

(5) 配置完成后的检验

完成上述配置后，在 PE 上执行 **display mpls l2vpn connection** 命令，可以看到建立了一条 L2VPN 连接，状态为 up。

以 PE 1 为例：

```
[PE1] display mpls l2vpn connection
1 total connections,
connections: 1 up, 0 down, 0 local, 1 remote, 0 unknown
VPN name: vpn1,
1 total connections,
connections: 1 up, 0 down, 0 local, 1 remote, 0 unknown
CE name: ce1, id: 1,
Rid type status peer-id route-distinguisher intf
2 rmt up 4.4.4.4 100:1 Vlan10
```

CE 1 与 CE 2 之间能够 ping 通。

```
[CE1] ping 100.1.1.2
PING 100.1.1.2: 56 data bytes, press CTRL_C to break
Reply from 100.1.1.2: bytes=56 Sequence=1 ttl=255 time=90 ms
Reply from 100.1.1.2: bytes=56 Sequence=2 ttl=255 time=77 ms
Reply from 100.1.1.2: bytes=56 Sequence=3 ttl=255 time=34 ms
Reply from 100.1.1.2: bytes=56 Sequence=4 ttl=255 time=46 ms
Reply from 100.1.1.2: bytes=56 Sequence=5 ttl=255 time=94 ms
--- 100.1.1.2 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 34/68/94 ms
```

5. 完整配置

- CE1 的完整配置

```
#
interface Vlan-interface10
ip address 100.1.1.1 255.255.255.0
```

- PE1 的完整配置

```
#
mpls lsr-id 2.2.2.2
#
mpls
lsp-trigger all
#
mpls l2vpn
#
mpls ldp
#
```



```

interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
interface Vlan-interface10
#
interface Vlan-interface20
 ip address 10.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
ospf 1
 area 0
  network 10.1.1.1 0.0.0.255
  network 2.2.2.2 0.0.0.0
#
bgp 100
 undo synchronization
 peer 4.4.4.4 as-number 100
 peer 4.4.4.4 connect-interface LoopBack0
#
 l2vpn-family
  peer 4.4.4.4 enable
#
 mpls l2vpn vpn1 encapsulation vlan
  route-distinguisher 100:1
  vpn-target 1:1 import-extcommunity
  vpn-target 1:1 export-extcommunity
  ce ce1 id 1 range 10 default-offset 0
  connection ce-offset 2 interface Vlan-interface10

```

- P 的完整配置

```

#
 mpls lsr-id 3.3.3.3
#
 mpls
  lsp-trigger all
#
 mpls ldp
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
#
interface Vlan-interface20
 ip address 10.1.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface Vlan-interface30
 ip address 10.2.2.2 255.255.255.0

```

```

mpls
mpls ldp
#
ospf 1
area 0
network 10.1.1.2 0.0.0.255
network 10.2.2.2 0.0.0.255
network 3.3.3.3 0.0.0.0

```

- PE2 的完整配置

```

#
mpls lsr-id 4.4.4.4
#
mpls
lsp-trigger all
#
mpls l2vpn
#
mpls ldp
#
interface LoopBack0
ip address 4.4.4.4 255.255.255.255
#
interface Vlan-interface10
#
interface Vlan-interface30
ip address 10.2.2.1 255.255.255.0
mpls
mpls ldp
#
ospf 1
area 0
network 10.2.2.1 0.0.0.255
network 4.4.4.4 0.0.0.0
#
bgp 100
undo synchronization
peer 2.2.2.2 as-number 100
peer 2.2.2.2 connect-interface LoopBack0
#
l2vpn-family
peer 2.2.2.2 enable
#
mpls l2vpn vpn1 encapsulation vlan
route-distinguisher 100:1
vpn-target 1:1 import-extcommunity
vpn-target 1:1 export-extcommunity
ce ce2 id 2 range 10 default-offset 0
connection ce-offset 1 interface Vlan-interface10

```

- CE2 的完整配置

```
#
interface Vlan-interface10
ip address 100.1.1.2 255.255.255.0
```

6. 配置注意事项

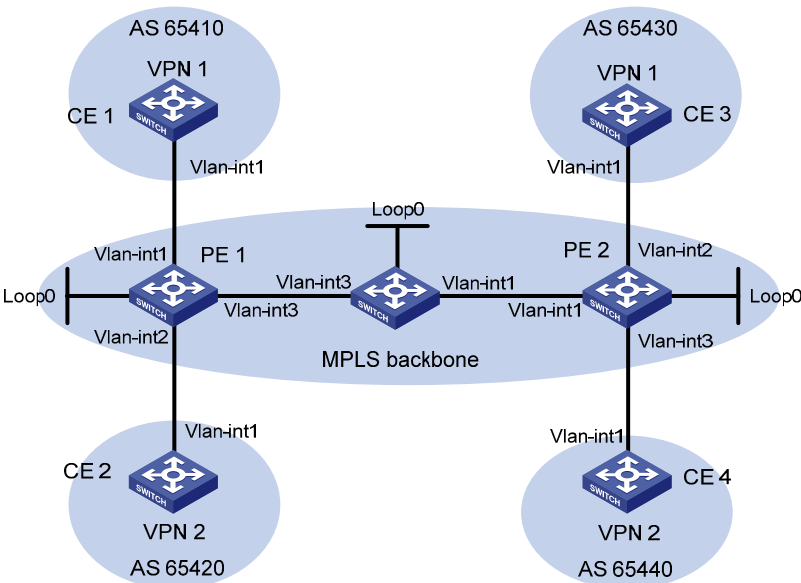
- Kompella 方式 MPLS L2VPN 必须在 PE 上为每个直接相连的 CE 所在的 VPN 创建 L2VPN 实例。创建 L2VPN 时指定的封装类型应与 CE 侧接口的封装类型对应。
- 上述配置中在 MPLS-L2VPN 视图下配置的 VPN-Target 和 RD（Route Distinguisher，路由标识）与配置 MPLS L3VPN 时在 VPN 实例视图下配置的 VPN-Target 和 RD（Route Distinguisher，路由标识）作用相同。对于 Kompella L2VPN，必须配置 RD。RD 配置后不能修改，除非先删除创建的 VPN，然后重新创建。

1.3 MPLS L3VPN 典型配置指导

1.3.1 MPLS L3VPN 基本配置典型配置指导

1. 组网图

图1-6 MPLS L3VPN 基本配置组网图



设备	接口	IP 地址	设备	接口	IP 地址
CE 1	Vlan-int1	10.1.1.1/24	P	Loop0	2.2.2.9/32
PE 1	Loop0	1.1.1.9/32		Vlan-int1	172.2.1.1/24
	Vlan-int1	10.1.1.2/24		Vlan-int3	172.1.1.2/24
	Vlan-int3	172.1.1.1/24	PE 2	Loop0	3.3.3.9/32
	Vlan-int2	10.2.1.2/24		Vlan-int1	172.2.1.2/24
CE 2	Vlan-int1	10.2.1.1/24		Vlan-int2	10.3.1.2/24
CE 3	Vlan-int1	10.3.1.1/24		Vlan-int3	10.4.1.2/24
CE 4	Vlan-int1	10.4.1.1/24			

2. 应用要求

- CE 1、CE 3 属于 VPN 1，CE 2、CE 4 属于 VPN 2；

- VPN 1 使用的 VPN Target 属性为 111:1, VPN 2 使用的 VPN Target 属性为 222:2。不同 VPN 用户之间不能互相访问;
- PE、P 为支持 MPLS 的设备, 在 PE1 和 PE2 之间建立 MPLS L3VPN。

3. 适用产品、版本

表1-6 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S7500E 系列以太网交换机	Release 6300 软件版本	LSQ1SRP1CB 引擎或者全部采用 EA 系列业务板

4. 配置过程和解释

(1) 在 MPLS 骨干网上配置 IGP 协议, 实现骨干网 PE 和 P 的互通

配置 PE 1。

```
<PE1> system-view
[PE1] interface loopback 0
[PE1-LoopBack0] ip address 1.1.1.9 32
[PE1-LoopBack0] quit
[PE1] interface vlan-interface 3
[PE1-Vlan-interface3] ip address 172.1.1.1 24
[PE1-Vlan-interface3] quit
[PE1] ospf
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 172.1.1.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] network 1.1.1.9 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

配置 P。

```
<P> system-view
[P] interface loopback 0
[P-LoopBack0] ip address 2.2.2.9 32
[P-LoopBack0] quit
[P] interface vlan-interface 3
[P-Vlan-interface3] ip address 172.1.1.2 24
[P-Vlan-interface3] quit
[P] interface vlan-interface 1
[P-Vlan-interface1] ip address 172.2.1.1 24
[P-Vlan-interface1] quit
[P] ospf
[P-ospf-1] area 0
[P-ospf-1-area-0.0.0.0] network 172.1.1.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 172.2.1.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 2.2.2.9 0.0.0.0
[P-ospf-1-area-0.0.0.0] quit
[P-ospf-1] quit
```

配置 PE 2。

```
<PE2> system-view
[PE2] interface loopback 0
[PE2-LoopBack0] ip address 3.3.3.9 32
[PE2-LoopBack0] quit
[PE2] interface vlan-interface 1
[PE2-Vlan-interface1] ip address 172.2.1.2 24
[PE2-Vlan-interface1] quit
[PE2] ospf
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 172.2.1.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] network 3.3.3.9 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

配置完成后，PE 1、P、PE 2 之间应能建立 OSPF 邻居，执行 **display ospf peer** 命令可以看到邻居达到 FULL 状态。执行 **display ip routing-table** 命令可以看到 PE 之间学习到对方的 Loopback 路由。

以 PE 1 为例：

```
[PE1] display ip routing-table
Routing Tables: Public
          Destinations : 9          Routes : 9

Destination/Mask    Proto    Pre  Cost   NextHop         Interface
1.1.1.9/32          Direct   0     0    127.0.0.1       InLoop0
2.2.2.9/32          OSPF     10    1    172.1.1.2       Vlan3
3.3.3.9/32          OSPF     10    2    172.1.1.2       Vlan3
127.0.0.0/8         Direct   0     0    127.0.0.1       InLoop0
127.0.0.1/32        Direct   0     0    127.0.0.1       InLoop0
172.1.1.0/24        Direct   0     0    172.1.1.1       Vlan3
172.1.1.1/32        Direct   0     0    127.0.0.1       InLoop0
172.1.1.2/32        Direct   0     0    172.1.1.2       Vlan3
172.2.1.0/24        OSPF     10    1    172.1.1.2       Vlan3

[PE1] display ospf peer verbose

          OSPF Process 1 with Router ID 1.1.1.9

          Neighbors

Area 0.0.0.0 interface 172.1.1.1(Vlan-interface3)'s neighbors
Router ID: 172.1.1.2      Address: 172.1.1.2      GR State: Normal

  State: Full  Mode:Nbr is Master  Priority: 1
  DR: None    BDR: None    MTU: 1500
  Dead timer due in 38 sec
  Neighbor is up for 00:02:44
  Authentication Sequence: [ 0 ]
  Neighbor state change count: 5
```

(2) 在 MPLS 骨干网上配置 MPLS 基本能力和 MPLS LDP，建立 LDP LSP

配置 PE 1。

```
[PE1] mpls lsr-id 1.1.1.9
[PE1] mpls
```

```
[PE1-mpls] lsp-trigger all
[PE1-mpls] quit
[PE1] mpls ldp
[PE1-mpls-ldp] quit
[PE1] interface vlan-interface 3
[PE1-Vlan-interface3] mpls
[PE1-Vlan-interface3] mpls ldp
[PE1-Vlan-interface3] quit
```

配置 P。

```
[P] mpls lsr-id 2.2.2.9
[P] mpls
[P-mpls] lsp-trigger all
[P-mpls] quit
[P] mpls ldp
[P-mpls-ldp] quit
[P] interface vlan-interface 3
[P-Vlan-interface3] mpls
[P-Vlan-interface3] mpls ldp
[P-Vlan-interface3] quit
[P] interface vlan-interface 1
[P-Vlan-interface1] mpls
[P-Vlan-interface1] mpls ldp
[P-Vlan-interface1] quit
```

配置 PE 2。

```
[PE2] mpls lsr-id 3.3.3.9
[PE2] mpls
[PE2-mpls] lsp-trigger all
[PE2-mpls] quit
[PE2] mpls ldp
[PE2-mpls-ldp] quit
[PE2] interface vlan-interface 1
[PE2-Vlan-interface1] mpls
[PE2-Vlan-interface1] mpls ldp
[PE2-Vlan-interface1] quit
```

上述配置完成后，PE 1、P、PE 2 之间应能建立 LDP 会话，执行 **display mpls ldp session** 命令可以看到显示结果中 Session State 项为 Operational。执行 **display mpls ldp lsp** 命令，可以看到 LDP LSP 的建立情况。

以 PE 1 为例：

```
[PE1] display mpls ldp session
```

LDP Session(s) in Public Network						
Peer-ID	Status	LAM	SsnRole	FT	MD5	KA-Sent/Rcv
2.2.2.9:0	Operational	DU	Passive	Off	Off	5/5

```

LAM : Label Advertisement Mode      FT : Fault Tolerance

```

```
[PE1] display mpls ldp lsp
```

```

LDP LSP Information
-----
SN  DestAddress/Mask  In/OutLabel  Next-Hop  In/Out-Interface
-----
1   1.1.1.9/32        3/NULL      127.0.0.1  Vlan-interface3/InLoop0
2   2.2.2.9/32        NULL/3      172.1.1.2  -----/Vlan-interface3
3   3.3.3.9/32        NULL/1024   172.1.1.2  -----/Vlan-interface3
-----
A '*' before an LSP means the LSP is not established
A '*' before a Label means the USCB or DSCB is stale
```

(3) 在 PE 设备上配置 VPN 实例，将 CE 接入 PE

配置 PE 1。

```
[PE1] ip vpn-instance vpn1
[PE1-vpn-instance-vpn1] route-distinguisher 100:1
[PE1-vpn-instance-vpn1] vpn-target 111:1
[PE1-vpn-instance-vpn1] quit
[PE1] ip vpn-instance vpn2
[PE1-vpn-instance-vpn2] route-distinguisher 100:2
[PE1-vpn-instance-vpn2] vpn-target 222:2
[PE1-vpn-instance-vpn2] quit
[PE1] interface vlan-interface 1
[PE1-Vlan-interface1] ip binding vpn-instance vpn1
[PE1-Vlan-interface1] ip address 10.1.1.2 24
[PE1-Vlan-interface1] quit
[PE1] interface vlan-interface 2
[PE1-Vlan-interface2] ip binding vpn-instance vpn2
[PE1-Vlan-interface2] ip address 10.2.1.2 24
[PE1-Vlan-interface2] quit
```

配置 PE 2。

```
[PE2] ip vpn-instance vpn1
[PE2-vpn-instance-vpn1] route-distinguisher 200:1
[PE2-vpn-instance-vpn1] vpn-target 111:1
[PE2-vpn-instance-vpn1] quit
[PE2] ip vpn-instance vpn2
[PE2-vpn-instance-vpn2] route-distinguisher 200:2
[PE2-vpn-instance-vpn2] vpn-target 222:2
[PE2-vpn-instance-vpn2] quit
[PE2] interface vlan-interface 2
[PE2-Vlan-interface2] ip binding vpn-instance vpn1
[PE2-Vlan-interface2] ip address 10.3.1.2 24
[PE2-Vlan-interface2] quit
[PE2] interface vlan-interface 3
[PE2-Vlan-interface3] ip binding vpn-instance vpn2
[PE2-Vlan-interface3] ip address 10.4.1.2 24
[PE2-Vlan-interface3] quit
```

按图 1-6配置各CE的接口IP地址，配置过程略。

配置完成后，在 PE 设备上执行 **display ip vpn-instance** 命令可以看到 VPN 实例的配置情况。各 PE 能 ping 通自己接入的 CE。

以 PE 1 和 CE 1 为例：

```
[PE1] display ip vpn-instance
Total VPN-Instances configured : 2
VPN-Instance Name      RD          Create Time
vpn1                    100:1       2006/08/13 09:32:45
vpn2                    100:2       2006/08/13 09:42:59
[PE1] ping -vpn-instance vpn1 10.1.1.1
PING 10.1.1.1: 56 data bytes, press CTRL_C to break
  Reply from 10.1.1.1: bytes=56 Sequence=1 ttl=255 time=56 ms
  Reply from 10.1.1.1: bytes=56 Sequence=2 ttl=255 time=4 ms
  Reply from 10.1.1.1: bytes=56 Sequence=3 ttl=255 time=4 ms
  Reply from 10.1.1.1: bytes=56 Sequence=4 ttl=255 time=52 ms
  Reply from 10.1.1.1: bytes=56 Sequence=5 ttl=255 time=3 ms
--- 10.1.1.1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 3/23/56 ms
```

(4) 在 PE 与 CE 之间建立 EBGP 对等体，引入 VPN 路由

配置 CE 1。

```
<CE1> system-view
[CE1] bgp 65410
[CE1-bgp] peer 10.1.1.2 as-number 100
[CE1-bgp] import-route direct
[CE1-bgp] quit
```



说明

另外 3 个 CE 设备（CE 2 ~ CE 4）配置与 CE 1 设备配置类似，配置过程省略。

配置 PE 1。

```
[PE1] bgp 100
[PE1-bgp] ipv4-family vpn-instance vpn1
[PE1-bgp-vpn1] peer 10.1.1.1 as-number 65410
[PE1-bgp-vpn1] import-route direct
[PE1-bgp-vpn1] quit
[PE1-bgp] ipv4-family vpn-instance vpn2
[PE1-bgp-vpn2] peer 10.2.1.1 as-number 65420
[PE1-bgp-vpn2] import-route direct
[PE1-bgp-vpn2] quit
[PE1-bgp] quit
```




说明

PE 2 的配置与 PE 1 类似，配置过程省略。

配置完成后，在 PE 设备上执行 **display bgp vpnv4 vpn-instance peer** 命令，可以看到 PE 与 CE 之间的 BGP 对等体关系已建立，并达到 Established 状态。

以 PE 1 与 CE 1 的对等体关系为例：

```
[PE1] display bgp vpnv4 vpn-instance vpn1 peer
BGP local router ID : 1.1.1.9
Local AS number : 100
Total number of peers : 1          Peers in established state : 1
```

Peer	V	AS	MsgRcvd	MsgSent	OutQ	PrefRcv	Up/Down	State
10.1.1.1	4	65410	11	9	0	1	00:06:37	Established

(5) 在 PE 之间建立 MP-IBGP 对等体

配置 PE 1。

```
[PE1] bgp 100
[PE1-bgp] peer 3.3.3.9 as-number 100
[PE1-bgp] peer 3.3.3.9 connect-interface loopback 0
[PE1-bgp] ipv4-family vpnv4
[PE1-bgp-af-vpnv4] peer 3.3.3.9 enable
[PE1-bgp-af-vpnv4] quit
[PE1-bgp] quit
```

配置 PE 2。

```
[PE2] bgp 100
[PE2-bgp] peer 1.1.1.9 as-number 100
[PE2-bgp] peer 1.1.1.9 connect-interface loopback 0
[PE2-bgp] ipv4-family vpnv4
[PE2-bgp-af-vpnv4] peer 1.1.1.9 enable
[PE2-bgp-af-vpnv4] quit
[PE2-bgp] quit
```

配置完成后，在 PE 设备上执行 **display bgp peer** 或 **display bgp vpnv4 all peer** 命令，可以看到 PE 之间的 BGP 对等体关系已建立，并达到 Established 状态。

```
[PE1] display bgp peer
BGP local router ID : 1.1.1.9
Local AS number : 100
Total number of peers : 1          Peers in established state : 1
```

Peer	V	AS	MsgRcvd	MsgSent	OutQ	PrefRcv	Up/Down	State
3.3.3.9	4	100	2	6	0	0	00:00:12	Established

(6) 配置完成后的检验

在 PE 设备上执行 **display ip routing-table vpn-instance** 命令，可以看到去往对端 CE 的路由。

以 PE 1 为例：

```
[PE1] display ip routing-table vpn-instance vpn1
```

Routing Tables: vpn1

Destinations : 3			Routes : 3		
Destination/Mask	Proto	Pre	Cost	NextHop	Interface
10.1.1.0/24	Direct	0	0	10.1.1.2	Vlan1
10.1.1.2/32	Direct	0	0	127.0.0.1	InLoop0
10.3.1.0/24	BGP	255	0	3.3.3.9	NULL0

[PE1] display ip routing-table vpn-instance vpn2

Routing Tables: vpn2

Destinations : 3			Routes : 3		
Destination/Mask	Proto	Pre	Cost	NextHop	Interface
10.2.1.0/24	Direct	0	0	10.2.1.2	Vlan2
10.2.1.2/32	Direct	0	0	127.0.0.1	InLoop0
10.4.1.0/24	BGP	255	0	3.3.3.9	NULL0

同一 VPN 的 CE 能够相互 Ping 通，不同 VPN 的 CE 不能相互 Ping 通。

例如：CE 1 能够 Ping 通 CE 3（10.3.1.1），但不能 Ping 通 CE 4（10.4.1.1）。

[CE1] ping 10.3.1.1

```
PING 10.3.1.1: 56 data bytes, press CTRL_C to break
  Reply from 10.3.1.1: bytes=56 Sequence=1 ttl=253 time=72 ms
  Reply from 10.3.1.1: bytes=56 Sequence=2 ttl=253 time=34 ms
  Reply from 10.3.1.1: bytes=56 Sequence=3 ttl=253 time=50 ms
  Reply from 10.3.1.1: bytes=56 Sequence=4 ttl=253 time=50 ms
  Reply from 10.3.1.1: bytes=56 Sequence=5 ttl=253 time=34 ms
--- 10.3.1.1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 34/48/72 ms
```

[CE1] ping 10.4.1.1

```
PING 10.4.1.1: 56 data bytes, press CTRL_C to break
  Request time out
  Request time out
  Request time out
  Request time out
  Request time out
--- 10.4.1.1 ping statistics ---
  5 packet(s) transmitted
  0 packet(s) received
  100.00% packet loss
```

5. 完整配置

- CE1 的完整配置

```
#
interface Vlan-interface1
 ip address 10.1.1.1 255.255.255.0
#
bgp 65410
 peer 10.1.1.2 as-number 100
```

```

import-route direct
• CE2 的完整配置
#
interface Vlan-interface1
 ip address 10.2.1.1 255.255.255.0
#
bgp 65420
 peer 10.2.1.2 as-number 100
import-route direct
• PE1 的完整配置
#
mpls lsr-id 1.1.1.9
#
ip vpn-instance vpn1
 route-distinguisher 100:1
 vpn-target 111:1 export-extcommunity
 vpn-target 111:1 import-extcommunity
#
ip vpn-instance vpn2
 route-distinguisher 100:2
 vpn-target 222:1 export-extcommunity
 vpn-target 222:1 import-extcommunity
#
mpls
 lsp-trigger all
#
mpls ldp
#
interface LoopBack0
 ip address 1.1.1.9 255.255.255.255
#
interface Vlan-interface1
 ip binding vpn-instance vpn1
 ip address 10.1.1.2 255.255.255.0
#
interface Vlan-interface2
 ip binding vpn-instance vpn2
 ip address 10.2.1.2 255.255.255.0
#
interface Vlan-interface3
 ip address 172.1.1.1 255.255.255.0
mpls
mpls ldp
#
ospf 1
 area 0
  network 172.1.1.0 0.0.0.255
  network 1.1.1.9 0.0.0.0

```

```
#
bgp 100
undo synchronization
peer 3.3.3.9 as-number 100
peer 3.3.3.9 connect-interface LoopBack0
#
ipv4-family vpn-instance vpn1
peer 10.1.1.1 as-number 65410
import-route direct
#
ipv4-family vpn-instance vpn2
peer 10.2.1.1 as-number 65420
import-route direct
#
ipv4-family vpnv4
peer 3.3.3.9 enable
```

- P 的完整配置

```
#
mpls lsr-id 2.2.2.9
#
mpls
lsp-trigger all
#
mpls ldp
#
interface LoopBack0
ip address 2.2.2.9 255.255.255.255
#
interface Vlan-interface1
ip address 172.2.1.1 255.255.255.0
mpls
mpls ldp
#
interface Vlan-interface30
ip address 172.1.1.2 255.255.255.0
mpls
mpls ldp
#
ospf 1
area 0
network 172.1.1.0 0.0.0.255
network 172.2.1.0 0.0.0.255
network 2.2.2.9 0.0.0.0
```

- PE2 的完整配置

```
#
mpls lsr-id 3.3.3.9
#
ip vpn-instance vpn1
```

```

route-distinguisher 200:1
vpn-target 111:1 export-extcommunity
vpn-target 111:1 import-extcommunity
#
ip vpn-instance vpn2
route-distinguisher 200:2
vpn-target 222:1 export-extcommunity
vpn-target 222:1 import-extcommunity
#
mpls
lsp-trigger all
#
mpls ldp
#
interface LoopBack0
ip address 3.3.3.9 255.255.255.255
#
interface Vlan-interface1
ip address 172.2.1.2 255.255.255.0
#
interface Vlan-interface2
ip binding vpn-instance vpn1
ip address 10.3.1.2 255.255.255.0
#
interface Vlan-interface3
ip binding vpn-instance vpn2
ip address 10.4.1.2 255.255.255.0
#
ospf 1
area 0
network 172.1.1.0 0.0.0.255
network 3.3.3.9 0.0.0.0
#
bgp 100
undo synchronization
peer 1.1.1.9 as-number 100
peer 1.1.1.9 connect-interface LoopBack0
#
ipv4-family vpn-instance vpn1
peer 10.1.1.1 as-number 65430
import-route direct
#
ipv4-family vpn-instance vpn2
peer 10.2.1.1 as-number 65440
import-route direct
#
ipv4-family vpnv4
peer 1.1.1.9 enable

```

• CE3 的完整配置

```
#
interface Vlan-interface1
ip address 10.3.1.1 255.255.255.0
#
bgp 65430
peer 10.3.1.2 as-number 100
import-route direct
```

• CE4 的完整配置

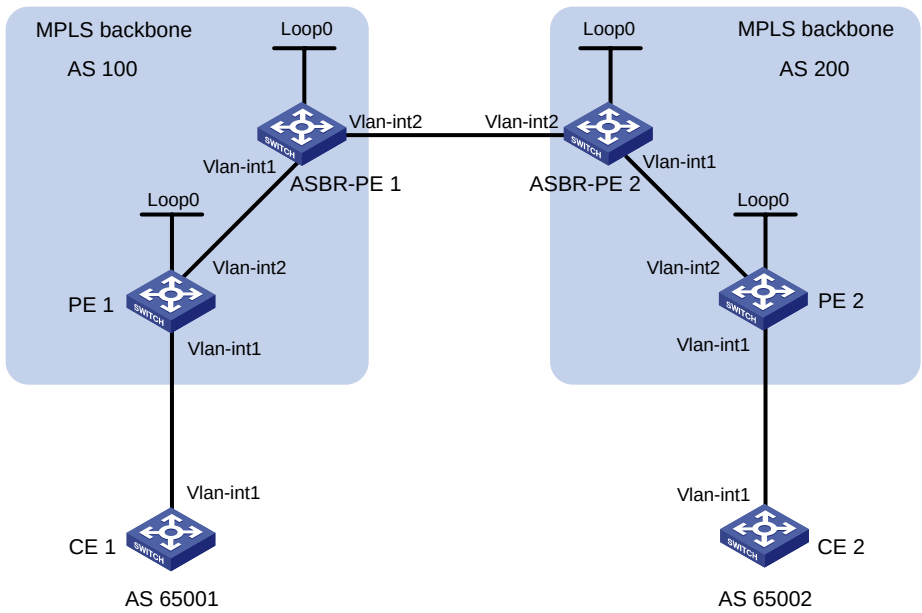
```
#
interface Vlan-interface1
ip address 10.4.1.1 255.255.255.0
#
bgp 65440
peer 10.4.1.2 as-number 100
import-route direct
```

6. 配置注意事项

执行 **ip binding vpn-instance** 命令将删除接口上已经配置的 IP 地址，因此需要重新配置接口的 IP 地址。

1.3.2 跨域 VPN-OptionA 方式典型配置指导

1. 组网图



设备	接口	IP 地址	设备	接口	IP 地址
CE 1	Vlan-int1	10.1.1.1/24	CE 2	Vlan-int1	10.2.1.1/24
PE 1	Loop0	1.1.1.9/32	PE 2	Loop0	4.4.4.9/32
	Vlan-int1	10.1.1.2/24		Vlan-int1	10.2.1.2/24
	Vlan-int2	172.1.1.2/24		Vlan-int2	162.1.1.2/24
ASBR-PE 1	Loop0	2.2.2.9/32	ASBR-PE 2	Loop0	3.3.3.9/32
	Vlan-int1	172.1.1.1/24		Vlan-int1	162.1.1.1/24
	Vlan-int2	192.1.1.1/24		Vlan-int2	192.1.1.2/24

图1-7 跨域 VPN-OptionA 方式组网图

2. 应用要求

- CE 1 和 CE 2 属于同一个 VPN。
- CE 1 通过 AS100 的 PE 1 接入，CE 2 通过 AS200 的 PE 2 接入。
- 采用 OptionA 方式实现跨域的 MPLS L3VPN，即，采用 VRF-to-VRF 方式管理 VPN 路由。
- 同一个 AS 内部的 MPLS 骨干网使用 OSPF 作为 IGP。

3. 适用产品、版本

表1-7 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S7500E 系列以太网交换机	Release 6300 软件版本	LSQ1SRP1CB 引擎或者全部采用 EA 系列业务板

4. 配置过程 and 解释

(1) 在 MPLS 骨干网上配置 IGP 协议，实现骨干网内互通

本例中采用 OSPF，具体配置步骤请参考 MPLS L3VPN 基本配置典型配置指导。



说明
需要将作为 LSR ID 的 LoopBack 接口的 32 位地址通过 OSPF 发布出去。

配置完成后，ASBR-PE 与本 AS 的 PE 之间应能建立 OSPF 邻居，执行 **display ospf peer** 命令可以看到邻居达到 FULL 状态，PE 之间能学习到对方的 Loopback 地址。

ASBR-PE 与本 AS 的 PE 之间能够互相 ping 通。

(2) 在 MPLS 骨干网上配置 MPLS 基本能力和 MPLS LDP，建立 LDP LSP

配置 PE 1 的 MPLS 基本能力，并在与 ASBR-PE 1 相连的接口上使能 LDP。

```
<PE1> system-view
[PE1] mpls lsr-id 1.1.1.9
[PE1] mpls
[PE1-mpls] quit
[PE1] mpls ldp
[PE1-mpls-ldp] quit
[PE1] interface vlan-interface 1
[PE1-Vlan-interface1] mpls
[PE1-Vlan-interface1] mpls ldp
[PE1-Vlan-interface1] quit
```

配置 ASBR-PE 1 的 MPLS 基本能力，并在与 PE 1 相连的接口上使能 LDP。

```
<ASBR-PE1> system-view
[ASBR-PE1] mpls lsr-id 2.2.2.9
[ASBR-PE1] mpls
[ASBR-PE1-mpls] quit
[ASBR-PE1] mpls ldp
```

```
[ASBR-PE1-mpls-ldp] quit
[ASBR-PE1] interface vlan-interface 1
[ASBR-PE1-Vlan-interface1] mpls
[ASBR-PE1-Vlan-interface1] mpls ldp
[ASBR-PE1-Vlan-interface1] quit
```

配置 ASBR-PE 2 的 MPLS 基本能力，并在与 PE 2 相连的接口上使能 LDP。

```
<ASBR-PE2> system-view
[ASBR-PE2] mpls lsr-id 3.3.3.9
[ASBR-PE2] mpls
[ASBR-PE2-mpls] quit
[ASBR-PE2] mpls ldp
[ASBR-PE2-mpls-ldp] quit
[ASBR-PE2] interface vlan-interface 1
[ASBR-PE2-Vlan-interface1] mpls
[ASBR-PE2-Vlan-interface1] mpls ldp
[ASBR-PE2-Vlan-interface1] quit
```

配置 PE 2 的 MPLS 基本能力，并在与 ASBR-PE 2 相连的接口上使能 LDP。

```
<PE2> system-view
[PE2] mpls lsr-id 4.4.4.9
[PE2] mpls
[PE2-mpls] quit
[PE2] mpls ldp
[PE2-mpls-ldp] quit
[PE2] interface vlan-interface 2
[PE2-Vlan-interface2] mpls
[PE2-Vlan-interface2] mpls ldp
[PE2-Vlan-interface2] quit
```

上述配置完成后，同一 AS 的 PE 和 ASBR-PE 之间应该建立起 LDP 邻居，在各设备上执行 **display mpls ldp session** 命令可以看到显示结果中 Session State 项为“Operational”。

(3) 在 PE 设备上配置 VPN 实例，将 CE 接入 PE

 说明

同一 AS 内的 ASBR-PE 与 PE 的 VPN 实例的 VPN Target 应能匹配，不同 AS 的 PE 的 VPN 实例的 VPN Target 则不需要匹配。

配置 CE 1。

```
<CE1> system-view
[CE1] interface vlan-interface 1
[CE1-Vlan-interface1] ip address 10.1.1.1 24
[CE1-Vlan-interface1] quit
```

配置 PE 1。

```
[PE1] ip vpn-instance vpn1
[PE1-vpn-instance-vpn1] route-distinguisher 100:1
[PE1-vpn-instance-vpn1] vpn-target 100:1 both
```



```
[PE1-vpn-instance-vpn1] quit
[PE1] interface vlan-interface 1
[PE1-Vlan-interface1] ip binding vpn-instance vpn1
[PE1-Vlan-interface1] ip address 10.1.1.2 24
[PE1-Vlan-interface1] quit
```

配置 CE 2。

```
<CE2> system-view
[CE2] interface vlan-interface 1
[CE2-Vlan-interface1] ip address 10.2.1.1 24
[CE2-Vlan-interface1] quit
```

配置 PE 2。

```
[PE2] ip vpn-instance vpn1
[PE2-vpn-instance] route-distinguisher 200:2
[PE2-vpn-instance] vpn-target 100:1 both
[PE2-vpn-instance] quit
[PE2] interface vlan-interface 1
[PE2-Vlan-interface1] ip binding vpn-instance vpn1
[PE2-Vlan-interface1] ip address 10.2.1.2 24
[PE2-Vlan-interface1] quit
```

配置 ASBR-PE 1: 创建 VPN 实例，并将此实例绑定到连接 ASBR-PE 2 的接口（ASBR-PE 1 认为 ASBR-PE 2 是自己的 CE）。

```
[ASBR-PE1] ip vpn-instance vpn1
[ASBR-PE1-vpn-instance-vpn1] route-distinguisher 100:1
[ASBR-PE1-vpn-instance-vpn1] vpn-target 100:1 both
[ASBR-PE1-vpn-instance-vpn1] quit
[ASBR-PE1] interface vlan-interface 2
[ASBR-PE1-Vlan-interface2] ip binding vpn-instance vpn1
[ASBR-PE1-Vlan-interface2] ip address 192.1.1.1 24
[ASBR-PE1-Vlan-interface2] quit
```

配置 ASBR-PE 2: 创建 VPN 实例，并将此实例绑定到连接 ASBR-PE 1 的接口（ASBR-PE 2 认为 ASBR-PE 1 是自己的 CE）。

```
[ASBR-PE2] ip vpn-instance vpn1
[ASBR-PE2-vpn-vpn-vpn1] route-distinguisher 200:1
[ASBR-PE2-vpn-vpn-vpn1] vpn-target 100:1 both
[ASBR-PE2-vpn-vpn-vpn1] quit
[ASBR-PE2] interface vlan-interface 2
[ASBR-PE2-Vlan-interface2] ip binding vpn-instance vpn1
[ASBR-PE2-Vlan-interface2] ip address 192.1.1.2 24
[ASBR-PE2-Vlan-interface2] quit
```

上述配置完成后，在各 PE 设备上执行 **display ip vpn-instance** 命令能正确显示 VPN 实例配置。

各 PE 能 ping 通 CE。ASBR-PE 之间也能互相 ping 通。

(4) 在 PE 与 CE 之间建立 EBGP 对等体，引入 VPN 路由

配置 CE 1。

```
[CE1] bgp 65001
```

```
[CE1-bgp] peer 10.1.1.2 as-number 100
[CE1-bgp] import-route direct
[CE1-bgp] quit
```

配置 PE 1。

```
[PE1] bgp 100
[PE1-bgp] ipv4-family vpn-instance vpn1
[PE1-bgp-vpn1] peer 10.1.1.1 as-number 65001
[PE1-bgp-vpn1] import-route direct
[PE1-bgp-vpn1] quit
[PE1-bgp] quit
```

配置 CE 2。

```
[CE2] bgp 65002
[CE2-bgp] peer 10.2.1.2 as-number 200
[CE2-bgp] import-route direct
[CE2-bgp] quit
```

配置 PE 2。

```
[PE2] bgp 200
[PE2-bgp] ipv4-family vpn-instance vpn1
[PE2-bgp-vpn1] peer 10.2.1.1 as-number 65002
[PE2-bgp-vpn1] import-route direct
[PE2-bgp-vpn1] quit
[PE2-bgp] quit
```

(5) PE 与本 AS 的 ASBR-PE 之间建立 IBGP 对等体, ASBR-PE 之间建立 EBGP 对等体

配置 PE 1。

```
[PE1] bgp 100
[PE1-bgp] peer 2.2.2.9 as-number 100
[PE1-bgp] peer 2.2.2.9 connect-interface loopback 0
[PE1-bgp] ipv4-family vpv4
[PE1-bgp-af-vpv4] peer 2.2.2.9 enable
[PE1-bgp-af-vpv4] peer 2.2.2.9 next-hop-local
[PE1-bgp-af-vpv4] quit
[PE1-bgp] quit
```

配置 ASBR-PE 1。

```
[ASBR-PE1] bgp 100
[ASBR-PE1-bgp] ipv4-family vpn-instance vpn1
[ASBR-PE1-bgp-vpn1] peer 192.1.1.2 as-number 200
[ASBR-PE1-bgp-vpn1] quit
[ASBR-PE1-bgp] peer 1.1.1.9 as-number 100
[ASBR-PE1-bgp] peer 1.1.1.9 connect-interface loopback 0
[ASBR-PE1-bgp] ipv4-family vpv4
[ASBR-PE1-bgp-af-vpv4] peer 1.1.1.9 enable
[ASBR-PE1-bgp-af-vpv4] peer 1.1.1.9 next-hop-local
[ASBR-PE1-bgp-af-vpv4] quit
[ASBR-PE1-bgp] quit
```

配置 ASBR-PE 2。

```
[ASBR-PE2] bgp 200
[ASBR-PE2-bgp] ipv4-family vpn-instance vpn1
[ASBR-PE2-bgp-vpn1] peer 192.1.1.1 as-number 100
[ASBR-PE2-bgp-vpn1] quit
[ASBR-PE2-bgp] peer 4.4.4.9 as-number 200
[ASBR-PE2-bgp] peer 4.4.4.9 connect-interface loopback 0
[ASBR-PE2-bgp] ipv4-family vpnv4
[ASBR-PE2-bgp-af-vpnv4] peer 4.4.4.9 enable
[ASBR-PE2-bgp-af-vpnv4] peer 4.4.4.9 next-hop-local
[ASBR-PE2-bgp-af-vpnv4] quit
[ASBR-PE2-bgp] quit
```

配置 PE 2。

```
[PE2] bgp 200
[PE2-bgp] peer 3.3.3.9 as-number 200
[PE2-bgp] peer 3.3.3.9 connect-interface loopback 0
[PE2-bgp] ipv4-family vpnv4
[PE2-bgp-af-vpnv4] peer 3.3.3.9 enable
[PE2-bgp-af-vpnv4] peer 3.3.3.9 next-hop-local
[PE2-bgp-af-vpnv4] quit
[PE2-bgp] quit
```

(6) 配置完成后的检验

上述配置完成后，CE 之间能学习到对方的接口路由，CE 1 和 CE 2 能够相互 ping 通。

5. 完整配置

- CE1 的完整配置

```
#
interface Vlan-interface1
 ip address 10.1.1.1 255.255.255.0
#
bgp 65001
 peer 10.1.1.2 as-number 100
 import-route direct
```

- PE1 的完整配置

```
#
mpls lsr-id 1.1.1.9
#
ip vpn-instance vpn1
 route-distinguisher 100:1
 vpn-target 100:1 export-extcommunity
 vpn-target 100:1 import-extcommunity
#
mpls
 lsp-trigger all
#
mpls ldp
#
```

```

interface LoopBack0
 ip address 1.1.1.9 255.255.255.255
#
interface Vlan-interface1
 ip binding vpn-instance vpn1
 ip address 10.1.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface Vlan-interface2
 ip address 172.1.1.2 255.255.255.0
 mpls
 mpls ldp
#
ospf 1
 area 0
  network 10.1.1.0 0.0.0.255
  network 172.1.1.0 0.0.0.255
  network 1.1.1.9 0.0.0.0
#
bgp 100
 undo synchronization
 peer 2.2.2.9 as-number 100
 peer 2.2.2.9 connect-interface LoopBack0
#
 ipv4-family vpn-instance vpn1
  peer 10.1.1.1 as-number 65001
  import-route direct
#
 ipv4-family vpnv4
  peer 2.2.2.9 enable
  peer 2.2.2.9 next-hop-local

```

- ASBR-PE1 的完整配置

```

#
 mpls lsr-id 2.2.2.9
#
 ip vpn-instance vpn1
  route-distinguisher 100:1
  vpn-target 100:1 export-extcommunity
  vpn-target 100:1 import-extcommunity
#
 mpls
 lsp-trigger all
#
 mpls ldp
#
 interface LoopBack0
  ip address 2.2.2.9 255.255.255.255

```

```

#
interface Vlan-interface1
 ip address 172.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface Vlan-interface2
 ip binding vpn-instance vpn1
 ip address 192.1.1.1 255.255.255.0
 mpls
 mpls ldp
#
ospf 1
 area 0
  network 172.1.1.0 0.0.0.255
  network 192.1.1.0 0.0.0.255
  network 2.2.2.9 0.0.0.0
#
bgp 100
 undo synchronization
 peer 1.1.1.9 as-number 100
 peer 1.1.1.9 connect-interface LoopBack0
#
ipv4-family vpn-instance vpn1
 peer 192.1.1.2 as-number 200
 import-route direct
#
ipv4-family vpnv4
 peer 1.1.1.9 enable
 peer 1.1.1.9 next-hop-local

```

- ASBR-PE2 的完整配置

```

#
mpls lsr-id 3.3.3.9
#
ip vpn-instance vpn1
 route-distinguisher 200:1
 vpn-target 100:1 export-extcommunity
 vpn-target 100:1 import-extcommunity
#
mpls
 lsp-trigger all
#
mpls ldp
#
interface LoopBack0
 ip address 3.3.3.9 255.255.255.255
#
interface Vlan-interface1

```

```

ip address 162.1.1.1 255.255.255.0
mpls
mpls ldp
#
interface Vlan-interface2
ip binding vpn-instance vpn1
ip address 192.1.1.2 255.255.255.0
mpls
mpls ldp
#
ospf 1
area 0
network 162.1.1.0 0.0.0.255
network 192.1.1.0 0.0.0.255
network 3.3.3.9 0.0.0.0
#
bgp 200
undo synchronization
peer 4.4.4.9 as-number 200
peer 4.4.4.9 connect-interface LoopBack0
#
ipv4-family vpn-instance vpn1
peer 192.1.1.1 as-number 100
import-route direct
#
ipv4-family vpnv4
peer 4.4.4.9 enable
peer 4.4.4.9 next-hop-local

```

- PE2 的完整配置

```

#
mpls lsr-id 4.4.4.9
#
ip vpn-instance vpn1
route-distinguisher 200:2
vpn-target 100:1 export-extcommunity
vpn-target 100:1 import-extcommunity
#
mpls
lsp-trigger all
#
mpls ldp
#
interface LoopBack0
ip address 4.4.4.9 255.255.255.255
#
interface Vlan-interface1
ip binding vpn-instance vpn1
ip address 10.2.1.2 255.255.255.0

```

```

mpls
mpls ldp
#
interface Vlan-interface2
ip address 162.1.1.2 255.255.255.0
mpls
mpls ldp
#
ospf 1
area 0
network 10.2.1.0 0.0.0.255
network 162.1.1.0 0.0.0.255
network 4.4.4.9 0.0.0.0
#
bgp 200
undo synchronization
peer 3.3.3.9 as-number 200
peer 3.3.3.9 connect-interface LoopBack0
#
ipv4-family vpn-instance vpn1
peer 10.2.1.1 as-number 65002
import-route direct
#
ipv4-family vpnv4
peer 3.3.3.9 enable
peer 3.3.3.9 next-hop-local

```

- CE2 的完整配置

```

#
interface Vlan-interface1
ip address 10.2.1.1 255.255.255.0
#
bgp 65002
peer 10.2.1.2 as-number 200
import-route direct

```

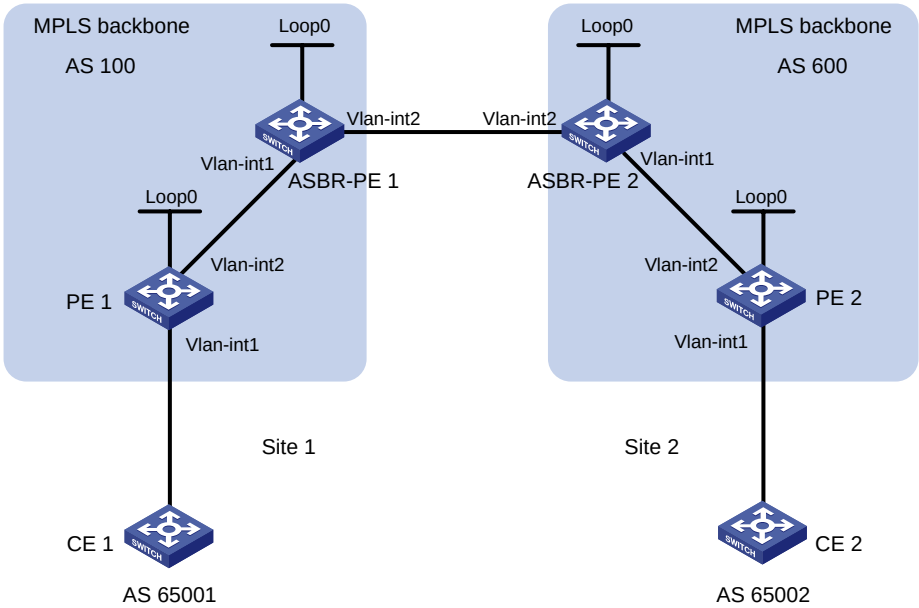
6. 配置注意事项

在跨域 VPN-OptionA 方式中,对于同一个 VPN,同一 AS 内的 ASBR-PE 与 PE 的 VPN 实例的 VPN Target 应能匹配; 不同 AS 的 PE 之间的 VPN 实例的 VPN Target 则不需要匹配。

1.3.3 跨域 VPN-OptionB 方式典型配置指导

1. 组网图

图1-8 跨域 VPN-OptionB 方式组网图



设备	接口	IP 地址	设备	接口	IP 地址
PE 1	Loop0	2.2.2.9/32	PE 2	Loop0	5.5.5.9/32
	Vlan-int1	30.0.0.1/8		Vlan-int1	20.0.0.1/8
	Vlan-int2	1.1.1.2/8		Vlan-int2	9.1.1.2/8
ASBR-PE 1	Loop0	3.3.3.9/32	ASBR-PE 2	Loop0	4.4.4.9/32
	Vlan-int1	1.1.1.1/8		Vlan-int1	9.1.1.1/8
	Vlan-int2	11.0.0.2/8		Vlan-int2	11.0.0.1/8

2. 应用要求

- Site 1 和 Site 2 属于同一个 VPN，Site 1 的 CE 1 通过 AS 100 的 PE 1 接入，Site 2 的 CE 2 通过 AS 600 的 PE 2 接入；
- 同一自治系统内的 PE 设备之间运行 IS-IS 作为 IGP；
- PE 1 与 ASBR-PE 1 间通过 MP-IBGP 交换标签 IPv4 路由；
- PE 2 与 ASBR-PE 2 间通过 MP-IBGP 交换标签 IPv4 路由；
- ASBR-PE 1 与 ASBR-PE 2 间通过 MP-EBGP 交换标签 IPv4 路由；
- ASBR 上不对接收的 VPN-IPv4 路由进行 VPN Target 过滤。

3. 适用产品、版本

表1-8 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S7500E 系列以太网交换机	Release 6300 软件版本	LSQ1SRP1CB 引擎或者全部采用 EA 系列业务板

4. 配置过程 and 解释

在跨域 VPN-OptionB 方式的配置中，CE 设备上的配置与跨域 VPN-OptionA 方式基本一致，这里不再赘述。

(1) 配置 PE 1

在 PE 1 上运行 IS-IS。

```
<PE1> system-view
[PE1] isis 1
[PE1-isis-1] network-entity 10.111.111.111.111.00
[PE1-isis-1] quit
```

配置 LSR ID，使能 MPLS 和 LDP。

```
[PE1] mpls lsr-id 2.2.2.9
[PE1] mpls
[PE1-mpls] label advertise non-null
[PE1-mpls] quit
[PE1] mpls ldp
[PE1-mpls-ldp] quit
```

配置 Vlan-interface2，在接口上运行 IS-IS，并使能 MPLS 和 LDP。

```
[PE1] interface vlan-interface 2
[PE1-Vlan-interface2] ip address 1.1.1.2 255.0.0.0
[PE1-Vlan-interface2] isis enable 1
[PE1-Vlan-interface2] mpls
[PE1-Vlan-interface2] mpls ldp
[PE1-Vlan-interface2] quit
```

创建 Loopback0 接口，在接口上运行 IS-IS。

```
[PE1] interface loopback 0
[PE1-LoopBack0] ip address 2.2.2.9 32
[PE1-LoopBack0] isis enable 1
[PE1-LoopBack0] quit
```

创建一个 VPN 实例，名为 vpn1，配置 RD 和 VPN Target 属性。

```
[PE1] ip vpn-instance vpn1
[PE1-vpn-instance-vpn1] route-distinguisher 11:11
[PE1-vpn-instance-vpn1] vpn-target 1:1 2:2 3:3 import-extcommunity
[PE1-vpn-instance-vpn1] vpn-target 3:3 export-extcommunity
[PE1-vpn-instance-vpn1] quit
```

将连接 CE 1 的接口绑定到创建的 VPN 实例。

```
[PE1] interface vlan-interface 1
[PE1-Vlan-interface1] ip binding vpn-instance vpn1
[PE1-Vlan-interface1] ip address 30.0.0.1 8
[PE1-Vlan-interface1] quit
```

在 PE 1 上运行 BGP。

```
[PE1] bgp 100
```

配置 IBGP 对等体 3.3.3.9 为 VPNv4 对等体。

```
[PE1-bgp] peer 3.3.3.9 as-number 100
[PE1-bgp] peer 3.3.3.9 connect-interface loopback 0
[PE1-bgp] ipv4-family vpnv4
[PE1-bgp-af-vpnv4] peer 3.3.3.9 enable
```

```
[PE1-bgp-af-vpnv4] quit
```

将直连路由引入 VPN1 的 VPN 路由表。

```
[PE1-bgp] ipv4-family vpn-instance vpn1
```

```
[PE1-bgp-vpn1] import-route direct
```

```
[PE1-bgp-vpn1] quit
```

```
[PE1-bgp] quit
```

(2) 配置 ASBR-PE 1

在 ASBR-PE 1 上运行 IS-IS。

```
<ASBR-PE1> system-view
```

```
[ASBR-PE1] isis 1
```

```
[ASBR-PE1-isis-1] network-entity 10.222.222.222.00
```

```
[ASBR-PE1-isis-1] quit
```

配置 LSR ID，使能 MPLS 和 LDP。

```
[ASBR-PE1] mpls lsr-id 3.3.3.9
```

```
[ASBR-PE1] mpls
```

```
[ASBR-PE1-mpls] label advertise non-null
```

```
[ASBR-PE1-mpls] quit
```

```
[ASBR-PE1] mpls ldp
```

```
[ASBR-PE1-mpls-ldp] quit
```

配置接口 Vlan-interface1，在接口上运行 IS-IS，并使能 MPLS 和 LDP。

```
[ASBR-PE1] interface vlan-interface1
```

```
[ASBR-PE1-Vlan-interface1] ip address 1.1.1.1 255.0.0.0
```

```
[ASBR-PE1-Vlan-interface1] isis enable 1
```

```
[ASBR-PE1-Vlan-interface1] mpls
```

```
[ASBR-PE1-Vlan-interface1] mpls ldp
```

```
[ASBR-PE1-Vlan-interface1] quit
```

配置接口 Vlan-interface2，使能 MPLS。

```
[ASBR-PE1] interface vlan-interface 2
```

```
[ASBR-PE1-Vlan-interface2] ip address 11.0.0.2 255.0.0.0
```

```
[ASBR-PE1-Vlan-interface2] mpls
```

```
[ASBR-PE1-Vlan-interface2] quit
```

创建 Loopback0 接口，并运行 IS-IS。

```
[ASBR-PE1] interface loopback 0
```

```
[ASBR-PE1-LoopBack0] ip address 3.3.3.9 32
```

```
[ASBR-PE1-LoopBack0] isis enable 1
```

```
[ASBR-PE1-LoopBack0] quit
```

在 ASBR-PE 1 上运行 BGP

```
[ASBR-PE1] bgp 100
```

```
[ASBR-PE1-bgp] peer 2.2.2.9 as-number 100
```

```
[ASBR-PE1-bgp] peer 2.2.2.9 connect-interface loopback 0
```

```
[ASBR-PE1-bgp] peer 11.0.0.1 as-number 600
```

```
[ASBR-PE1-bgp] peer 11.0.0.1 connect-interface vlan-interface 2
```

不对接收的 VPNv4 路由进行 Import VPN-target 过滤。

```
[ASBR-PE1-bgp] ipv4-family vpnv4
```

```
[ASBR-PE1-bgp-af-vpnv4] undo policy vpn-target
```

将 IBGP 对等体 2.2.2.9 和 EBGP 对等体 11.0.0.1 都配置为 VPNv4 对等体。

```
[ASBR-PE1-bgp-af-vpnv4] peer 11.0.0.1 enable
```

```
[ASBR-PE1-bgp-af-vpnv4] peer 2.2.2.9 enable
```

```
[ASBR-PE1-bgp-af-vpnv4] quit
```

(3) 配置 ASBR-PE 2

在 ASBR-PE 2 上运行 IS-IS。

```
<ASBR-PE2> system-view
```

```
[ASBR-PE2] isis 1
```

```
[ASBR-PE2-isis-1] network-entity 10.222.222.222.00
```

```
[ASBR-PE2-isis-1] quit
```

配置 LSR ID，使能 MPLS 和 LDP。

```
[ASBR-PE2] mpls lsr-id 4.4.4.9
```

```
[ASBR-PE2] mpls
```

```
[ASBR-PE2-mpls] label advertise non-null
```

```
[ASBR-PE2-mpls] quit
```

```
[ASBR-PE2] mpls ldp
```

```
[ASBR-PE2-mpls-ldp] quit
```

配置接口 Vlan-interface1，在接口上运行 IS-IS，并使能 MPLS 和 LDP。

```
[ASBR-PE2] interface vlan-interface 1
```

```
[ASBR-PE2-Vlan-interface1] ip address 9.1.1.1 255.0.0.0
```

```
[ASBR-PE2-Vlan-interface1] isis enable 1
```

```
[ASBR-PE2-Vlan-interface1] mpls
```

```
[ASBR-PE2-Vlan-interface1] mpls ldp
```

```
[ASBR-PE2-Vlan-interface1] quit
```

配置接口 Vlan-interface2，使能 MPLS。

```
[ASBR-PE2] interface vlan-interface 2
```

```
[ASBR-PE2-Vlan-interface2] ip address 11.0.0.1 255.0.0.0
```

```
[ASBR-PE2-Vlan-interface2] mpls
```

```
[ASBR-PE2-Vlan-interface2] quit
```

创建 Loopback0 接口，并运行 IS-IS。

```
[ASBR-PE2] interface loopback 0
```

```
[ASBR-PE2-LoopBack0] ip address 4.4.4.9 32
```

```
[ASBR-PE2-LoopBack0] isis enable 1
```

```
[ASBR-PE2-LoopBack0] quit
```

在 ASBR-PE 2 上运行 BGP。

```
[ASBR-PE2] bgp 600
```

```
[ASBR-PE2-bgp] peer 11.0.0.2 as-number 100
```

```
[ASBR-PE2-bgp] peer 11.0.0.2 connect-interface vlan-interface 2
```

```
[ASBR-PE2-bgp] peer 5.5.5.9 as-number 600
```

```
[ASBR-PE2-bgp] peer 5.5.5.9 connect-interface loopback 0
```

不对接收的 VPNv4 路由进行 Import VPN-target 过滤。

```
[ASBR-PE2-bgp] ipv4-family vpnv4
```

```
[ASBR-PE2-bgp-af-vpnv4] undo policy vpn-target
```

将 IBGP 对等体 5.5.5.9 和 EBGP 对等体 11.0.0.2 都配置为 VPNv4 对等体。

```
[ASBR-PE2-bgp-af-vpnv4] peer 11.0.0.2 enable
```

```
[ASBR-PE2-bgp-af-vpnv4] peer 5.5.5.9 enable
```

```
[ASBR-PE2-bgp-af-vpnv4] quit
```

```
[ASBR-PE2-bgp] quit
```

(4) 配置 PE 2

在 PE 2 上运行 IS-IS。

```
<PE2> system-view
```

```
[PE2] isis 1
```

```
[PE2-isis-1] network-entity 10.111.111.111.111.00
```

```
[PE2-isis-1] quit
```

配置 LSR ID，使能 MPLS 和 LDP。

```
[PE2] mpls lsr-id 5.5.5.9
```

```
[PE2] mpls
```

```
[PE2-mpls] label advertise non-null
```

```
[PE2-mpls] quit
```

```
[PE2] mpls ldp
```

```
[PE2-mpls-ldp] quit
```

配置接口 Vlan-interface2，在接口上运行 IS-IS，并使能 MPLS 和 LDP。

```
[PE2] interface vlan-interface 2
```

```
[PE2-Vlan-interface2] ip address 9.1.1.2 255.0.0.0
```

```
[PE2-Vlan-interface2] isis enable 1
```

```
[PE2-Vlan-interface2] mpls
```

```
[PE2-Vlan-interface2] mpls ldp
```

```
[PE2-Vlan-interface2] quit
```

创建 Loopback0 接口，在接口上运行 IS-IS。

```
[PE2] interface loopback 0
```

```
[PE2-LoopBack0] ip address 5.5.5.9 32
```

```
[PE2-LoopBack0] isis enable 1
```

```
[PE2-LoopBack0] quit
```

创建一个 VPN 实例，名为 vpn1，配置 RD 和 VPN Target 属性。

```
[PE2] ip vpn-instance vpn1
```

```
[PE2-vpn-instance-vpn1] route-distinguisher 12:12
```

```
[PE2-vpn-instance-vpn1] vpn-target 1:1 2:2 3:3 import-extcommunity
```

```
[PE2-vpn-instance-vpn1] vpn-target 3:3 export-extcommunity
```

```
[PE2-vpn-instance-vpn1] quit
```

将连接 CE 2 的接口绑定到创建的 VPN 实例。

```
[PE2] interface Vlan-interface1
```

```
[PE2-Vlan-interface1] ip binding vpn-instance vpn1
```

```
[PE2-Vlan-interface1] ip address 20.0.0.1 8
```

```
[PE2-Vlan-interface1] quit
```

在 PE 2 上运行 BGP。

```
[PE2] bgp 600
```

配置 IBGP 对等体 4.4.4.9 为 VPNv4 对等体。

```
[PE2-bgp] peer 4.4.4.9 as-number 600
```

```
[PE2-bgp] peer 4.4.4.9 connect-interface loopback 0
```

```
[PE2-bgp] ipv4-family vpnv4
```

```
[PE2-bgp-af-vpnv4] peer 4.4.4.9 enable
```

```
[PE2-bgp-af-vpnv4] quit
```

将直连路由引入 VPN1 的 VPN 路由表。

```
[PE2-bgp] ipv4-family vpn-instance vpn1
```

```
[PE2-bgp-vpn1] import-route direct
```

```
[PE2-bgp-vpn1] quit
```

```
[PE2-bgp] quit
```

(5) 配置完成后的检验

配置完成后，在 PE 2 上对 PE 1 进行 Ping 操作，可以 Ping 通。

在 PE 1 上对 PE 2 进行 Ping 操作，也可以 Ping 通。

5. 完整配置

- PE1 的完整配置

```
#
```

```
mpls lsr-id 2.2.2.9
```

```
#
```

```
ip vpn-instance vpn1
```

```
route-distinguisher 11:11
```

```
vpn-target 3:3 export-extcommunity
```

```
vpn-target 1:1 2:2 3:3 import-extcommunity
```

```
#
```

```
mpls
```

```
label advertise non-null
```

```
lsp-trigger all
```

```
#
```

```
mpls ldp
```

```
#
```

```
isis 1
```

```
network-entity 10.1111.1111.1111.00
```

```
#
```

```
interface LoopBack0
```

```
ip address 2.2.2.9 255.255.255.255
```

```
isis enable 1
```

```
#
```

```
interface Vlan-interface1
```

```
ip binding vpn-instance vpn1
```

```
ip address 30.0.0.1 255.0.0.0
```

```
#
```

```
interface Vlan-interface2
```

```

ip address 1.1.1.2 255.0.0.0
isis enable 1
mpls
mpls ldp
#
bgp 100
undo synchronization
peer 3.3.3.9 as-number 100
peer 3.3.3.9 connect-interface LoopBack0
#
ipv4-family vpn-instance vpn1
import-route direct
#
ipv4-family vpv4
peer 3.3.3.9 enable

```

- ASBR-PE1 的完整配置

```

#
mpls lsr-id 3.3.3.9
#
mpls
label advertise non-null
lsp-trigger all
#
mpls ldp
#
isis 1
network-entity 10.2222.2222.2222.00
#
interface LoopBack0
ip address 3.3.3.9 255.255.255.255
isis enable 1
#
interface Vlan-interface1
ip address 1.1.1.1 255.0.0.0
isis enable 1
mpls
mpls ldp
#
interface Vlan-interface2
ip address 11.0.0.2 255.0.0.0
mpls
#
bgp 100
undo synchronization
peer 2.2.2.9 as-number 100
peer 2.2.2.9 connect-interface LoopBack0
peer 11.0.0.1 as-number 600
peer 11.0.0.1 connect-interface Vlan-interface 2

```

```

#
ipv4-family vpnv4
    peer 2.2.2.9 enable
    peer 11.0.0.1 enable
    undo policy vpn-target

```

- ASBR-PE2 的完整配置

```

#
mpls lsr-id 4.4.4.9
#
mpls
    label advertise non-null
    lsp-trigger all
#
mpls ldp
#
isis 1
    network-entity 10.2222.2222.2222.00
#
interface LoopBack0
    ip address 4.4.4.9 255.255.255.255
    isis enable 1
#
interface Vlan-interface1
    ip address 9.1.1.1 255.0.0.0
    isis enable 1
    mpls
    mpls ldp
#
interface Vlan-interface2
    ip address 11.0.0.1 255.0.0.0
    mpls
#
bgp 600
    undo synchronization
    peer 5.5.5.9 as-number 600
    peer 5.5.5.9 connect-interface LoopBack0
    peer 11.0.0.2 as-number 100
    peer 11.0.0.2 connect-interface Vlan-interface 2
#
ipv4-family vpnv4
    peer 5.5.5.9 enable
    peer 11.0.0.2 enable
    undo policy vpn-target

```

- PE2 的完整配置

```

#
mpls lsr-id 5.5.5.9
#
ip vpn-instance vpn1

```

```

route-distinguisher 12:12
vpn-target 3:3 export-extcommunity
vpn-target 1:1 2:2 3:3 import-extcommunity
#
mpls
  label advertise non-null
  lsp-trigger all
#
mpls ldp
#
isis 1
  network-entity 10.1111.1111.1111.00
#
interface LoopBack0
  ip address 5.5.5.9 255.255.255.255
  isis enable 1
#
interface Vlan-interface1
  ip binding vpn-instance vpn1
  ip address 20.0.0.1 255.0.0.0
#
interface Vlan-interface2
  ip address 9.1.1.2 255.0.0.0
  isis enable 1
mpls
mpls ldp
#
bgp 600
  undo synchronization
  peer 4.4.4.9 as-number 600
  peer 4.4.4.9 connect-interface LoopBack0
#
  ipv4-family vpn-instance vpn1
    import-route direct
#
  ipv4-family vpnv4
    peer 4.4.4.9 enable

```

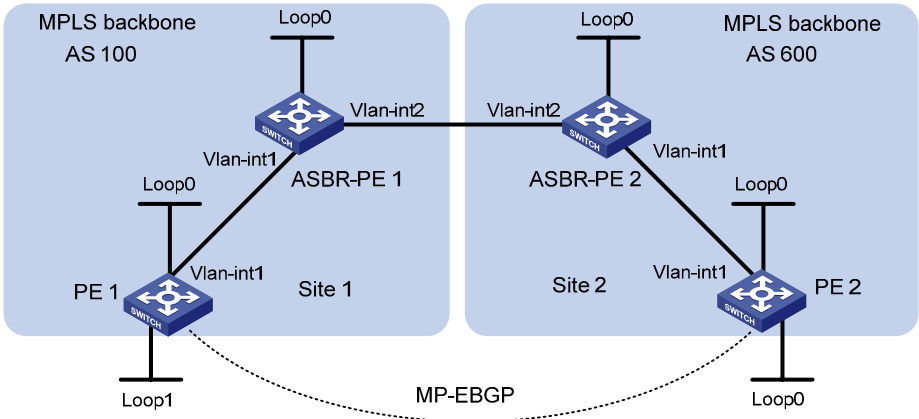
6. 配置注意事项

在跨域 VPN-OptionB 方式中,对于同一个 VPN,同一 AS 内的 ASBR-PE 与 PE 的 VPN 实例的 VPN Target 应能匹配; 不同 AS 的 PE 之间的 VPN 实例的 VPN Target 也需要匹配。

1.3.4 跨域 VPN-OptionC 方式典型配置指导

1. 组网图

图1-9 跨域 VPN-OptionC 方式组网图



设备	接口	IP 地址	设备	接口	IP 地址
PE 1	Loop0	2.2.2.9/32	PE 2	Loop0	5.5.5.9/32
	Loop1	30.0.0.1/32		Loop1	20.0.0.1/32
	Vlan-int1	1.1.1.2/8		Vlan-int1	9.1.1.2/8
ASBR-PE 1	Loop0	3.3.3.9/32	ASBR-PE 2	Loop0	4.4.4.9/32
	Vlan-int1	1.1.1.1/8		Vlan-int1	9.1.1.1/8
	Vlan-int2	11.0.0.2/8		Vlan-int2	11.0.0.1/8

2. 应用要求

- Site 1 和 Site 2 属于同一个 VPN，Site 1 通过 AS 100 的 PE 1 接入，Site 2 通过 AS 600 的 PE 2 接入；
- 同一自治系统内的 PE 设备之间运行 IS-IS 作为 IGP；
- PE 1 与 ASBR-PE 1 间通过 MP-IBGP 交换标签 IPv4 路由；
- PE 2 与 ASBR-PE 2 间通过 MP-IBGP 交换标签 IPv4 路由；
- PE 1 与 PE 2 建立 MP-EBGP 对等体；
- ASBR-PE 1 和 ASBR-PE 2 上分别配置路由策略，对从对方接收的路由压入标签；
- ASBR-PE 1 与 ASBR-PE 2 间通过 MP-EBGP 交换标签 IPv4 路由。

3. 适用产品、版本

表1-9 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S7500E 系列以太网交换机	Release 6300 软件版本	LSQ1SRP1CB 引擎或者全部采用 EA 系列业务板

4. 配置过程 and 解释

(1) 配置 PE 1

在 PE 1 上运行 IS-IS。

```
<PE1> system-view
```

```
[PE1] isis 1
```

```
[PE1-isis-1] network-entity 10.111.111.111.111.00
```

```
[PE1-isis-1] quit
```

配置 LSR ID，使能 MPLS 和 LDP。

```
[PE1] mpls lsr-id 2.2.2.9
```

```
[PE1] mpls
```

```
[PE1-mpls] quit
```

```
[PE1] mpls ldp
```

```
[PE1-mpls-ldp] quit
```

配置接口 Vlan-interface1，在接口上运行 IS-IS，并使能 MPLS 和 LDP。

```
[PE1] interface vlan-interface 1
```

```
[PE1-Vlan-interface1] ip address 1.1.1.2 255.0.0.0
```

```
[PE1-Vlan-interface1] isis enable 1
```

```
[PE1-Vlan-interface1] mpls
```

```
[PE1-Vlan-interface1] mpls ldp
```

```
[PE1-Vlan-interface1] quit
```

创建 Loopback0 接口，在接口上运行 IS-IS。

```
[PE1] interface loopback 0
```

```
[PE1-LoopBack0] ip address 2.2.2.9 32
```

```
[PE1-LoopBack0] isis enable 1
```

```
[PE1-LoopBack0] quit
```

创建 VPN 实例，名称为 vpn1，为其配置 RD 和 VPN Target 属性。

```
[PE1] ip vpn-instance vpn1
```

```
[PE1-vpn-instance-vpn1] route-distinguisher 11:11
```

```
[PE1-vpn-instance-vpn1] vpn-target 1:1 2:2 3:3 import-extcommunity
```

```
[PE1-vpn-instance-vpn1] vpn-target 3:3 export-extcommunity
```

```
[PE1-vpn-instance-vpn1] quit
```

创建 Loopback1 接口，并将此接口绑定到 vpn1。

```
[PE1] interface loopback 1
```

```
[PE1-LoopBack1] ip binding vpn-instance vpn1
```

```
[PE1-LoopBack1] ip address 30.0.0.1 32
```

```
[PE1-LoopBack1] quit
```

在 PE 1 上运行 BGP。

```
[PE1] bgp 100
```

配置 PE 1 向 IBGP 对等体 3.3.3.9 发布标签路由及从 3.3.3.9 接收标签路由的能力。

```
[PE1-bgp] peer 3.3.3.9 as-number 100
```

```
[PE1-bgp] peer 3.3.3.9 connect-interface loopback 0
```

```
[PE1-bgp] peer 3.3.3.9 label-route-capability
```

配置 PE 1 到 EBGP 对等体 5.5.5.9 的最大跳数为 10。

```
[PE1-bgp] peer 5.5.5.9 as-number 600
```

```
[PE1-bgp] peer 5.5.5.9 connect-interface loopback 0
```

```
[PE1-bgp] peer 5.5.5.9 ebgp-max-hop 10
```

配置对等体 5.5.5.9 作为 VPNv4 对等体。

```
[PE1-bgp] ipv4-family vpnv4
```

```
[PE1-bgp-af-ipv4] peer 5.5.5.9 enable
```

```
[PE1-bgp-af-ipv4] quit
```

将直连路由引入 vpn1 的路由表。

```
[PE1-bgp] ipv4-family vpn-instance vpn1
```

```
[PE1-bgp-vpn1] import-route direct
```

```
[PE1-bgp-vpn1] quit
```

```
[PE1-bgp] quit
```

(2) 配置 ASBR-PE1

在 ASBR-PE 1 上运行 IS-IS。

```
<ASBR-PE1> system-view
```

```
[ASBR-PE1] isis 1
```

```
[ASBR-PE1-isis-1] network-entity 10.222.222.222.00
```

```
[ASBR-PE1-isis-1] quit
```

配置 LSR ID，使能 MPLS 和 LDP。

```
[ASBR-PE1] mpls lsr-id 3.3.3.9
```

```
[ASBR-PE1] mpls
```

```
[ASBR-PE1-mpls] quit
```

```
[ASBR-PE1] mpls ldp
```

```
[ASBR-PE1-mpls-ldp] quit
```

配置接口 Vlan-interface1，在接口上运行 IS-IS，并使能 MPLS 和 LDP。

```
[ASBR-PE1] interface vlan-interface 1
```

```
[ASBR-PE1-Vlan-interface1] ip address 1.1.1.1 255.0.0.0
```

```
[ASBR-PE1-Vlan-interface1] isis enable 1
```

```
[ASBR-PE1-Vlan-interface1] mpls
```

```
[ASBR-PE1-Vlan-interface1] mpls ldp
```

```
[ASBR-PE1-Vlan-interface1] quit
```

配置接口 Vlan-interface2，并在接口上使能 MPLS。

```
[ASBR-PE1] interface vlan-interface 2
```

```
[ASBR-PE1-Vlan-interface2] ip address 11.0.0.2 255.0.0.0
```

```
[ASBR-PE1-Vlan-interface2] mpls
```

```
[ASBR-PE1-Vlan-interface2] quit
```

创建 Loopback0 接口，在接口上运行 IS-IS。

```
[ASBR-PE1] interface loopback 0
```

```
[ASBR-PE1-LoopBack0] ip address 3.3.3.9 32
```

```
[ASBR-PE1-LoopBack0] isis enable 1
```

```
[ASBR-PE1-LoopBack0] quit
```

创建路由策略。

```
[ASBR-PE1] route-policy policy1 permit node 1
```

```
[ASBR-PE1-route-policy] apply mpls-label
```

```
[ASBR-PE1-route-policy] quit
```

```
[ASBR-PE1] route-policy policy2 permit node 1
```

```
[ASBR-PE1-route-policy] if-match mpls-label
```

```
[ASBR-PE1-route-policy] apply mpls-label
```

```
[ASBR-PE1-route-policy] quit
```

在 ASBR-PE 1 上运行 BGP，引入 IS-IS 进程 1 的路由。

```
[ASBR-PE1] bgp 100
[ASBR-PE1-bgp] import-route isis 1
```

对 IBGP 对等体 2.2.2.9 发布来的路由应用已配置的路由策略 policy2。

```
[ASBR-PE1-bgp] peer 2.2.2.9 as-number 100
[ASBR-PE1-bgp] peer 2.2.2.9 route-policy policy2 export
```

向 IBGP 对等体 2.2.2.9 发布标签路由及从 2.2.2.9 接收标签路由的能力。

```
[ASBR-PE1-bgp] peer 2.2.2.9 connect-interface loopback 0
[ASBR-PE1-bgp] peer 2.2.2.9 label-route-capability
```

对 EBGP 对等体 11.0.0.1 发布来的路由应用已配置的路由策略 policy1。

```
[ASBR-PE1-bgp] peer 11.0.0.1 as-number 600
[ASBR-PE1-bgp] peer 11.0.0.1 route-policy policy1 export
```

向 EBGP 对等体 11.0.0.1 发布标签路由及从 11.0.0.1 接收标签路由的能力。

```
[ASBR-PE1-bgp] peer 11.0.0.1 label-route-capability
[ASBR-PE1-bgp] quit
```

(3) 配置 ASBR-PE 2

在 ASBR-PE 2 上运行 IS-IS。

```
<ASBR-PE2> system-view
[ASBR-PE2] isis 1
[ASBR-PE2-isis-1] network-entity 10.222.222.222.00
[ASBR-PE2-isis-1] quit
```

配置 LSR ID，使能 MPLS 和 LDP。

```
[ASBR-PE2] mpls lsr-id 4.4.4.9
[ASBR-PE2] mpls
[ASBR-PE2-mpls] quit
[ASBR-PE2] mpls ldp
[ASBR-PE2-mpls-ldp] quit
```

配置接口 Vlan-interface1，在接口上运行 IS-IS，并在接口上使能 MPLS 和 LDP。

```
[ASBR-PE2] interface vlan-interface 1
[ASBR-PE2-Vlan-interface1] ip address 9.1.1.1 255.0.0.0
[ASBR-PE2-Vlan-interface1] isis enable 1
[ASBR-PE2-Vlan-interface1] mpls
[ASBR-PE2-Vlan-interface1] mpls ldp
[ASBR-PE2-Vlan-interface1] quit
```

创建 Loopback0 接口，在接口上运行 IS-IS。

```
[ASBR-PE2] interface loopback 0
[ASBR-PE2-LoopBack0] ip address 4.4.4.9 32
[ASBR-PE2-LoopBack0] isis enable 1
[ASBR-PE2-LoopBack0] quit
```

配置接口 Vlan-interface2，在接口上使能 MPLS。

```
[ASBR-PE2] interface vlan-interface 2
[ASBR-PE2-Vlan-interface2] ip address 11.0.0.1 255.0.0.0
```

```
[ASBR-PE2-Vlan-interface2] mpls
```

```
[ASBR-PE2-Vlan-interface2] quit
```

创建路由策略。

```
[ASBR-PE2] route-policy policy1 permit node 1
```

```
New Sequence of this List
```

```
[ASBR-PE2-route-policy] apply mpls-label
```

```
[ASBR-PE2-route-policy] quit
```

```
[ASBR-PE2] route-policy policy2 permit node 1
```

```
[ASBR-PE2-route-policy] if-match mpls-label
```

```
[ASBR-PE2-route-policy] apply mpls-label
```

```
[ASBR-PE2-route-policy] quit
```

在 ASBR-PE 2 上运行 BGP，引入 IS-IS 进程 1 的路由。

```
[ASBR-PE2] bgp 600
```

```
[ASBR-PE2-bgp] import-route isis 1
```

向 IBGP 对等体 5.5.5.9 发布标签路由及从 5.5.5.9 接收标签路由的能力。

```
[ASBR-PE2-bgp] peer 5.5.5.9 as-number 600
```

```
[ASBR-PE2-bgp] peer 5.5.5.9 connect-interface loopback 1
```

```
[ASBR-PE2-bgp] peer 5.5.5.9 label-route-capability
```

对 IBGP 对等体 5.5.5.9 发布来的路由应用已配置的路由策略 policy2。

```
[ASBR-PE2-bgp] peer 5.5.5.9 route-policy policy2 export
```

对 EBGP 对等体 11.0.0.2 发布来的路由应用已配置的路由策略 policy1。

```
[ASBR-PE2-bgp] peer 11.0.0.2 as-number 100
```

```
[ASBR-PE2-bgp] peer 11.0.0.2 route-policy policy1 export
```

向 EBGP 对等体 11.0.0.2 发布标签路由及从 11.0.0.2 接收标签路由的能力。

```
[ASBR-PE2-bgp] peer 11.0.0.2 label-route-capability
```

```
[ASBR-PE2-bgp] quit
```

(4) 配置 PE 2

在 PE 2 上运行 IS-IS。

```
<PE2> system-view
```

```
[PE2] isis 1
```

```
[PE2-isis-1] network-entity 10.111.111.111.111.00
```

```
[PE2-isis-1] quit
```

配置 LSR ID，使能 MPLS 和 LDP。

```
[PE2] mpls lsr-id 5.5.5.9
```

```
[PE2] mpls
```

```
[PE2-mpls] quit
```

```
[PE2] mpls ldp
```

```
[PE2-mpls-ldp] quit
```

配置接口 Vlan-interface1，在接口上运行 IS-IS，并使能 MPLS 和 LDP。

```
[PE2] interface vlan-interface 1
```

```
[PE2-Vlan-interface1] ip address 9.1.1.2 255.0.0.0
```

```
[PE2-Vlan-interface1] isis enable 1
```

```
[PE2-Vlan-interface1] mpls
[PE2-Vlan-interface1] mpls ldp
[PE2-Vlan-interface1] quit
```

创建 Loopback0 接口，在接口上运行 IS-IS。

```
[PE2] interface loopback 0
[PE2-LoopBack0] ip address 5.5.5.9 32
[PE2-LoopBack0] isis enable 1
[PE2-LoopBack0] quit
```

创建 VPN 实例，名称为 vpn1，为其配置 RD 和 VPN Target 属性。

```
[PE2] ip vpn-instance vpn1
[PE2-vpn-instance-vpn1] route-distinguisher 11:11
[PE2-vpn-instance-vpn1] vpn-target 1:1 2:2 3:3 import-extcommunity
[PE2-vpn-instance-vpn1] vpn-target 3:3 export-extcommunity
[PE2-vpn-instance-vpn1] quit
```

创建 Loopback1 接口，并将此接口绑定到 vpn1。

```
[PE2] interface loopback 1
[PE2-LoopBack1] ip binding vpn-instance vpn1
[PE2-LoopBack1] ip address 20.0.0.1 32
[PE2-LoopBack1] quit
```

在 PE 2 上运行 BGP。

```
[PE2] bgp 600
```

配置 PE 2 向 IBGP 对等体 4.4.4.9 发布标签路由及从 4.4.4.9 接收标签路由的能力。

```
[PE2-bgp] peer 4.4.4.9 as-number 600
[PE2-bgp] peer 4.4.4.9 connect-interface loopback 1
[PE2-bgp] peer 4.4.4.9 label-route-capability
```

配置 PE 2 到 EBGP 对等体 2.2.2.9 的最大跳数为 10。

```
[PE2-bgp] peer 2.2.2.9 as-number 100
[PE2-bgp] peer 2.2.2.9 connect-interface loopback 1
[PE2-bgp] peer 2.2.2.9 ebgp-max-hop 10
```

配置对等体 2.2.2.9 作为 VPNv4 对等体。

```
[PE2-bgp] ipv4-family vpnv4
[PE2-bgp-af-vpnv4] peer 2.2.2.9 enable
[PE2-bgp-af-vpnv4] quit
```

将直连路由引入 vpn1 的路由表。

```
[PE2-bgp] ipv4-family vpn-instance vpn1
[PE2-bgp-vpn1] import-route direct
[PE2-bgp-vpn1] quit
[PE2-bgp] quit
```

配置完成后，在 PE2 上对 PE1 进行 Ping 操作，可以 Ping 通：

```
[PE2] ping -vpn-instance vpn1 30.0.0.1
```

在 PE1 上对 PE2 进行 Ping 操作，也可以 Ping 通：

```
[PE1] ping -vpn-instance vpn1 20.0.0.1
```

5. 完整配置

- PE1 的完整配置

```
#
mpls lsr-id 2.2.2.9
#
ip vpn-instance vpn1
  route-distinguisher 11:11
  vpn-target 3:3 export-extcommunity
  vpn-target 1:1 2:2 3:3 import-extcommunity
#
mpls
  lsp-trigger all
#
mpls ldp
#
isis 1
  network-entity 10.1111.1111.1111.00
#
interface LoopBack0
  ip address 2.2.2.9 255.255.255.255
  isis enable 1
#
interface LoopBack1
  ip binding vpn-instance vpn1
  ip address 30.0.0.1 255.255.255.255
#
interface Vlan-interface1
  ip address 1.1.1.2 255.0.0.0
  isis enable 1
  mpls
  mpls ldp
#
bgp 100
  undo synchronization
  peer 5.5.5.9 as-number 600
  peer 3.3.3.9 as-number 100
  peer 5.5.5.9 ebgp-max-hop 10
  peer 5.5.5.9 connect-interface LoopBack0
  peer 3.3.3.9 label-route-capability
  peer 3.3.3.9 connect-interface LoopBack0
#
ipv4-family vpn-instance vpn1
  import-route direct
#
ipv4-family vpv4
  peer 5.5.5.9 enable
```

- ASBR-PE1 的完整配置

```

#
mpls lsr-id 3.3.3.9
#
mpls
  lsp-trigger all
#
mpls ldp
#
isis 1
  network-entity 10.2222.2222.2222.00
#
interface LoopBack0
  ip address 3.3.3.9 255.255.255.255
  isis enable 1
#
interface Vlan-interface1
  ip address 1.1.1.1 255.0.0.0
  isis enable 1
mpls
mpls ldp
#
interface Vlan-interface2
  ip address 11.0.0.2 255.0.0.0
mpls
#
bgp 100
  import-route isis 1
  undo synchronization
  peer 11.0.0.1 as-number 600
  peer 2.2.2.9 as-number 100
  peer 11.0.0.1 route-policy policy1 export
  peer 2.2.2.9 route-policy policy2 export
  peer 11.0.0.1 label-route-capability
  peer 2.2.2.9 label-route-capability
  peer 2.2.2.9 connect-interface LoopBack0
#
route-policy policy1 permit node 1
  apply mpls-label
route-policy policy2 permit node 1
  if-match mpls-label
  apply mpls-label

```

- ASBR-PE2 的完整配置

```

#
mpls lsr-id 4.4.4.9
#
mpls
  lsp-trigger all
#

```



```

mpls ldp
#
isis 1
 network-entity 10.2222.2222.2222.00
#
interface LoopBack0
 ip address 4.4.4.9 255.255.255.255
 isis enable 1
#
interface Vlan-interface1
 ip address 9.1.1.1 255.0.0.0
 isis enable 1
mpls
mpls ldp
#
interface Vlan-interface2
 ip address 11.0.0.1 255.0.0.0
mpls
#
bgp 600
 import-route isis 1
 undo synchronization
 peer 11.0.0.2 as-number 100
 peer 5.5.5.9 as-number 600
 peer 11.0.0.2 route-policy policy1 export
 peer 5.5.5.9 route-policy policy2 export
 peer 11.0.0.2 label-route-capability
 peer 5.5.5.9 label-route-capability
 peer 5.5.5.9 connect-interface LoopBack1
#
route-policy policy1 permit node 1
 apply mpls-label
route-policy policy2 permit node 1
 if-match mpls-label
 apply mpls-label

```

- PE2 的完整配置

```

#
mpls lsr-id 5.5.5.9
#
ip vpn-instance vpn1
 route-distinguisher 11:11
 vpn-target 3:3 export-extcommunity
 vpn-target 1:1 2:2 3:3 import-extcommunity
#
mpls
 lsp-trigger all
#
mpls ldp

```

```

#
isis 1
 network-entity 10.1111.1111.1111.00
#
interface LoopBack0
 ip address 5.5.5.9 255.255.255.255
 isis enable 1
#
interface LoopBack1
 ip binding vpn-instance vpn1
 ip address 20.0.0.1 255.255.255.255
#
interface Vlan-interface1
 ip address 9.1.1.2 255.0.0.0
 isis enable 1
mpls
mpls ldp
#
bgp 600
 undo synchronization
 peer 4.4.4.9 as-number 600
 peer 2.2.2.9 as-number 100
 peer 2.2.2.9 ebgp-max-hop 10
 peer 4.4.4.9 connect-interface LoopBack1
 peer 4.4.4.9 label-route-capability
 peer 2.2.2.9 connect-interface LoopBack1
#
 ipv4-family vpn-instance vpn1
  import-route direct
#
 ipv4-family vpnv4
  peer 2.2.2.9 enable

```

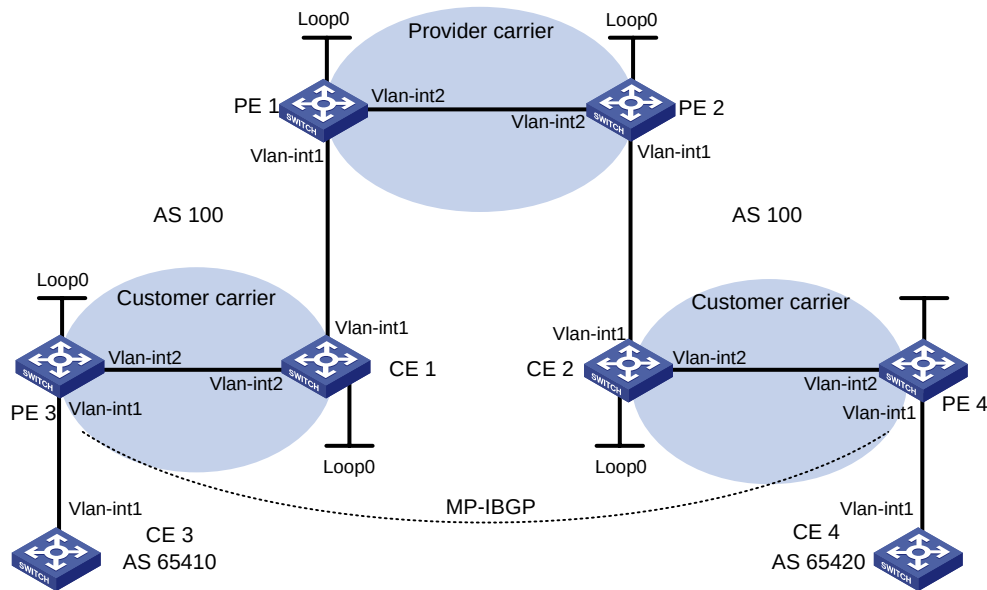
6. 配置注意事项

无

1.3.5 运营商的运营商典型配置指导

1. 组网图

图1-10 运营商的运营商组网图



设备	接口	IP 地址	设备	接口	IP 地址
CE 3	Vlan-int1	100.1.1.1/24	CE 4	Vlan-int1	120.1.1.1/24
PE 3	Loop0	1.1.1.9/32	PE 4	Loop0	6.6.6.9/32
	Vlan-int1	100.1.1.2/24		Vlan-int1	120.1.1.2/24
	Vlan-int2	10.1.1.1/24		Vlan-int2	20.1.1.2/24
CE 1	Loop0	2.2.2.9/32	CE 2	Loop0	5.5.5.9/32
	Vlan-int2	10.1.1.2/24		Vlan-int1	21.1.1.2/24
	Vlan-int1	11.1.1.1/24		Vlan-int2	20.1.1.1/24
PE 1	Loop0	3.3.3.9/32	PE 2	Loop0	4.4.4.9/32
	Vlan-int1	11.1.1.2/24		Vlan-int2	30.1.1.2/24
	Vlan-int2	30.1.1.1/24		Vlan-int1	21.1.1.1/24

2. 应用要求

二级运营商向自己的客户提供 MPLS L3VPN 服务。

在图 1-10中：

- PE 1 和 PE 2 是一级运营商骨干网的 PE 设备；
- CE 1 和 CE 2 是二级运营商的设备，作为 CE 接入一级运营商的骨干网；
- PE 3 和 PE 4 是二级运营商的设备，为二级运营商的客户提供接入；
- CE 3 和 CE 4 是二级运营商的客户。

3. 适用产品、版本

表1-10 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S7500E 系列以太网交换机	Release 6300 软件版本	LSQ1SRP1CB 引擎或者全部采用 EA 系列业务板

4. 配置过程和解释

运营商的运营商的配置关键在于理解两类路由的交换过程，即：

- 二级运营商 VPN 内部路由在一级运营商骨干网上的交换：一级运营商将二级运营商作为自己的 CE 接入；
 - 二级运营商本身客户的 VPN 路由在二级运营商 PE 设备间的交换：需要在二级运营商 PE 设备（PE 3 和 PE 4）间建立 MP-IBGP 对等体关系。
- (1) 配置一级运营商骨干网的 MPLS L3VPN，使用 IS-IS 作为骨干网的 IGP 协议，PE 1 和 PE 2 之间使能 LDP，并建立 MP-IBGP 对等体关系

配置 PE 1。

```
<PE1> system-view
[PE1] interface loopback 0
[PE1-LoopBack0] ip address 3.3.3.9 32
[PE1-LoopBack0] quit
[PE1] mpls lsr-id 3.3.3.9
[PE1] mpls
[PE1-mpls] quit
[PE1] mpls ldp
[PE1-mpls-ldp] quit
[PE1] isis 1
[PE1-isis-1] network-entity 10.0000.0000.0000.0004.00
[PE1-isis-1] quit
[PE1] interface loopback 0
[PE1-LoopBack0] isis enable 1
[PE1-LoopBack0] quit
[PE1] interface vlan-interface 2
[PE1-Vlan-interface2] ip address 30.1.1.1 24
[PE1-Vlan-interface2] isis enable 1
[PE1-Vlan-interface2] mpls
[PE1-Vlan-interface2] mpls ldp
[PE1-Vlan-interface2] mpls ldp transport-address interface
[PE1-Vlan-interface2] quit
[PE1] bgp 100
[PE1-bgp] peer 4.4.4.9 as-number 100
[PE1-bgp] peer 4.4.4.9 connect-interface loopback 0
[PE1-bgp] ipv4-family vpnv4
[PE1-bgp-af-vpnv4] peer 4.4.4.9 enable
[PE1-bgp-af-vpnv4] quit
[PE1-bgp] quit
```



说明

PE 2 的配置与 PE 1 类似，配置过程省略。

配置完成后，在 PE 1 或 PE 2 上执行 **display mpls ldp session** 命令可以看到 LDP 会话建立成功；执行 **display bgp peer** 命令可以看到 BGP 对等体关系已建立，并达到 Established 状态；执行 **display isis peer** 命令可以看到 IS-IS 邻居关系已建立，状态为 up。

以 PE1 为例：

```
[PE1] display mpls ldp session
```

```

      LDP Session(s) in Public Network
-----
Peer-ID      Status      LAM  SsnRole  FT   MD5   KA-Sent/Rcv
-----
4.4.4.9:0    Operational  DU   Active   Off  Off   378/378
-----
LAM : Label Advertisement Mode      FT : Fault Tolerance
[PE1] display bgp peer
BGP local router ID : 3.3.3.9
Local AS number : 100
Total number of peers : 1      Peers in established state : 1
Peer      V  AS  MsgRcvd  MsgSent  OutQ  PrefRcv  Up/Down  State
4.4.4.9   4 100   162     145     0       0   02:12:47 Established
[PE1] display isis peer
      Peer information for ISIS(1)
-----
System Id   Interface      Circuit Id  State HoldTime  Type  PRI
0000.0000.0005 Vlan-interface2 001      Up    29s     L1L2  --

```

(2) 配置二级运营商网络：使用 IS-IS 作为 IGP 协议，PE 3 和 CE 1、PE 4 和 CE 2 之间分别使能 LDP

配置 PE 3。

```

<PE3> system-view
[PE3] interface loopback 0
[PE3-LoopBack0] ip address 1.1.1.9 32
[PE3-LoopBack0] quit
[PE3] mpls lsr-id 1.1.1.9
[PE3] mpls
[PE3-mpls] quit
[PE3] mpls ldp
[PE3-mpls-ldp] quit
[PE3] isis 2
[PE3-isis-2] network-entity 10.0000.0000.0000.0001.00
[PE3-isis-2] quit
[PE3] interface loopback 0
[PE3-LoopBack0] isis enable 2
[PE3-LoopBack0] quit
[PE3] interface vlan-interface 2
[PE3-Vlan-interface2] ip address 10.1.1.1 24
[PE3-Vlan-interface2] isis enable 2
[PE3-Vlan-interface2] mpls
[PE3-Vlan-interface2] mpls ldp
[PE3-Vlan-interface2] mpls ldp transport-address interface
[PE3-Vlan-interface2] quit

```

配置 CE 1。

```
<CE1> system-view
```

```

[CE1] interface loopback 0
[CE1-LoopBack0] ip address 2.2.2.9 32
[CE1-LoopBack0] quit
[CE1] mpls lsr-id 2.2.2.9
[CE1] mpls
[CE1-mpls] quit
[CE1] mpls ldp
[CE1-mpls-ldp] quit
[CE1] isis 2
[CE1-isis-2] network-entity 10.0000.0000.0000.0002.00
[CE1-isis-2] quit
[CE1] interface loopback 0
[CE1-LoopBack0] isis enable 2
[CE1-LoopBack0] quit
[CE1] interface vlan-interface 2
[CE1-Vlan-interface2] ip address 10.1.1.2 24
[CE1-Vlan-interface2] isis enable 2
[CE1-Vlan-interface2] mpls
[CE1-Vlan-interface2] mpls ldp
[CE1-Vlan-interface2] mpls ldp transport-address interface
[CE1-Vlan-interface2] quit

```

配置完成后，PE 3 和 CE 1 之间应能建立 LDP 和 IS-IS 邻居关系。



说明

PE 4 和 CE 2 之间的配置与 PE 3 和 CE 1 之间的配置类似，配置过程省略。

(3) 配置二级运营商 CE 接入到一级运营商的 PE

配置 PE 1，并引入 IS-IS 路由。

```

[PE1] ip vpn-instance vpn1
[PE1-vpn-instance-vpn1] route-distinguisher 200:1
[PE1-vpn-instance-vpn1] vpn-target 1:1
[PE1-vpn-instance-vpn1] quit
[PE1] mpls ldp vpn-instance vpn1
[PE1-mpls-ldp-vpn-instance-vpn1] quit
[PE1] isis 2 vpn-instance vpn1
[PE1-isis-2] network-entity 10.0000.0000.0000.0003.00
[PE1-isis-2] import-route bgp
[PE1-isis-2] quit
[PE1] interface vlan-interface1
[PE1-Vlan-interface1] ip binding vpn-instance vpn1
[PE1-Vlan-interface1] ip address 11.1.1.2 24
[PE1-Vlan-interface1] isis enable 2
[PE1-Vlan-interface1] mpls
[PE1-Vlan-interface1] mpls ldp
[PE1-Vlan-interface1] mpls ldp transport-address interface
[PE1-Vlan-interface1] quit

```

```

[PE1] bgp 100
[PE1-bgp] ipv4-family vpn-instance vpn1
[PE1-bgp-vpn1] import isis 2
[PE1-bgp-vpn1] quit
[PE1-bgp] quit

# 配置 CE 1。

[CE1] interface vlan-interface1
[CE1-Vlan-interface1] ip address 11.1.1.1 24
[CE1-Vlan-interface1] isis enable 2
[CE1-Vlan-interface1] mpls
[CE1-Vlan-interface1] mpls ldp
[CE1-Vlan-interface1] mpls ldp transport-address interface
[CE1-Vlan-interface1] quit

```

配置完成后，PE 1 和 CE 1 之间应能建立 LDP 和 IS-IS 邻居关系。



说明

PE 2 和 CE 2 之间的配置与 PE 1 和 CE 1 之间的配置类似，配置过程省略。

(4) 配置二级运营商的客户接入 PE

配置 CE 3。

```

<CE3> system-view
[CE3] interface vlan-interface1
[CE3-Vlan-interface1] ip address 100.1.1.1 24
[CE3-Vlan-interface1] quit
[CE3] bgp 65410
[CE3-bgp] peer 100.1.1.2 as-number 100
[CE3-bgp] import-route direct
[CE3-bgp] quit

```

配置 PE 3。

```

[PE3] ip vpn-instance vpn1
[PE3-vpn-instance-vpn1] route-distinguisher 100:1
[PE3-vpn-instance-vpn1] vpn-target 1:1
[PE3-vpn-instance-vpn1] quit
[PE3] interface Vlan-interface1
[PE3-Vlan-interface1] ip binding vpn-instance vpn1
[PE3-Vlan-interface1] ip address 100.1.1.2 24
[PE3-Vlan-interface1] quit
[PE3] bgp 100
[PE3-bgp] ipv4-family vpn-instance vpn1
[PE3-bgp-vpn1] peer 100.1.1.1 as-number 65410
[PE3-bgp-vpn1] import-route direct
[PE3-bgp-vpn1] quit
[PE3-bgp] quit

```



说明

PE 4 和 CE 4 之间的配置与 PE 3 和 CE 3 之间的配置类似，配置过程省略。

(5) 在二级运营商的 PE 之间建立 MP-IBGP 对等体关系，交换二级运营商的客户的 VPN 路由
配置 PE 3。

```
[PE3] bgp 100
[PE3-bgp] peer 6.6.6.9 as-number 100
[PE3-bgp] peer 6.6.6.9 connect-interface loopback 0
[PE3-bgp] ipv4-family vpnv4
[PE3-bgp-af-vpnv4] peer 6.6.6.9 enable
[PE3-bgp-af-vpnv4] quit
[PE3-bgp] quit
```



说明

PE 4 的配置与 PE 3 类似，配置过程省略。

(6) 配置完成后的检验

所有配置完成后，在 PE 1 和 PE 2 上执行 **display ip routing-table** 命令，可以看到 PE 1 和 PE 2 的公网路由表中只有一级运营商网络的路由。以 PE 1 为例：

```
[PE1] display ip routing-table
Routing Tables: Public
          Destinations : 7          Routes : 7

Destination/Mask    Proto   Pre  Cost   NextHop         Interface
3.3.3.9/32          Direct  0     0    127.0.0.1       InLoop0
4.4.4.9/32          ISIS    15   10     30.1.1.2        Vlan2
30.1.1.0/24          Direct  0     0     30.1.1.1        Vlan2
30.1.1.1/32          Direct  0     0    127.0.0.1       InLoop0
30.1.1.2/32          Direct  0     0     30.1.1.2        Vlan2
127.0.0.0/8          Direct  0     0    127.0.0.1       InLoop0
127.0.0.1/32         Direct  0     0    127.0.0.1       InLoop0
```

在 PE 1 和 PE 2 上执行 **display ip routing-table vpn-instance** 命令，可以看到 VPN 路由表中有二级运营商网络的内部路由，但没有二级运营商维护的 VPN 路由。以 PE 1 为例：

```
[PE1] display ip routing-table vpn-instance vpn1
Routing Tables: vpn1
          Destinations : 11         Routes : 11

Destination/Mask    Proto   Pre  Cost   NextHop         Interface
1.1.1.9/32          ISIS    15   20     11.1.1.1        Vlan1
2.2.2.9/32          ISIS    15   10     11.1.1.1        Vlan1
5.5.5.9/32          BGP     255   0      4.4.4.9         NULL0
6.6.6.9/32          BGP     255   0      4.4.4.9         NULL0
10.1.1.0/24          ISIS    15   20     11.1.1.1        Vlan1
11.1.1.0/24          Direct  0     0     11.1.1.1        Vlan1
11.1.1.1/32          Direct  0     0    127.0.0.1       InLoop0
```


11.1.1.2/32	Direct	0	0	11.1.1.2	Vlan1
20.1.1.0/24	BGP	255	0	4.4.4.9	NULL0
21.1.1.0/24	BGP	255	0	4.4.4.9	NULL0
21.1.1.2/32	BGP	255	0	4.4.4.9	NULL0

在 CE 1 和 CE 2 上执行 **display ip routing-table** 命令，可以看到公网路由表中有二级运营商网络的内部路由，但没有二级运营商维护的 VPN 路由。以 CE 1 为例：

```
[CE1] display ip routing-table
```

Routing Tables: Public

Destinations : 16			Routes : 16		
Destination/Mask	Proto	Pre	Cost	NextHop	Interface
1.1.1.9/32	ISIS	15	10	10.1.1.2	Vlan2
2.2.2.9/32	Direct	0	0	127.0.0.1	InLoop0
5.5.5.9/32	ISIS	15	74	11.1.1.2	Vlan1
6.6.6.9/32	ISIS	15	74	11.1.1.2	Vlan1
10.1.1.0/24	Direct	0	0	10.1.1.2	Vlan2
10.1.1.1/32	Direct	0	0	10.1.1.1	Vlan2
10.1.1.2/32	Direct	0	0	127.0.0.1	InLoop0
11.1.1.0/24	Direct	0	0	11.1.1.1	Vlan1
11.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
11.1.1.2/32	Direct	0	0	11.1.1.2	Vlan1
20.1.1.0/24	ISIS	15	74	11.1.1.2	Vlan1
21.1.1.0/24	ISIS	15	74	11.1.1.2	Vlan1
21.1.1.2/32	ISIS	15	74	11.1.1.2	Vlan1
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0

在 PE 3 和 PE 4 上执行 **display ip routing-table** 命令，可以看到公网路由表中有二级运营商网络的内部路由。以 PE 3 为例：

```
[PE3] display ip routing-table
```

Routing Tables: Public

Destinations : 11			Routes : 11		
Destination/Mask	Proto	Pre	Cost	NextHop	Interface
1.1.1.9/32	Direct	0	0	127.0.0.1	InLoop0
2.2.2.9/32	ISIS	15	10	10.1.1.2	Vlan2
5.5.5.9/32	ISIS	15	84	10.1.1.2	Vlan2
6.6.6.9/32	ISIS	15	84	10.1.1.2	Vlan2
10.1.1.0/24	Direct	0	0	10.1.1.1	Vlan2
10.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
10.1.1.2/32	Direct	0	0	10.1.1.2	Vlan2
11.1.1.0/24	ISIS	15	20	10.1.1.2	Vlan2
20.1.1.0/24	ISIS	15	84	10.1.1.2	Vlan2
21.1.1.0/24	ISIS	15	84	10.1.1.2	Vlan2
21.1.1.2/32	ISIS	15	84	10.1.1.2	Vlan2
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0

在 PE 3 和 PE 4 上执行 **display ip routing-table vpn-instance** 命令，可以看到 VPN 路由表中有远端 VPN 客户的路由。以 PE 3 为例：

```
[PE3] display ip routing-table vpn-instance vpn1
```

```
Routing Tables: vpn1
```

Destinations : 3			Routes : 3		
Destination/Mask	Proto	Pre	Cost	NextHop	Interface
100.1.1.0/24	Direct	0	0	100.1.1.2	Vlan1
100.1.1.2/32	Direct	0	0	127.0.0.1	InLoop0
120.1.1.0/24	BGP	255	0	6.6.6.9	NULL0

PE 3 和 PE 4 可以相互 Ping 通:

```
[PE3] ping 20.1.1.2
```

```
PING 20.1.1.2: 56 data bytes, press CTRL_C to break
```

```
Reply from 20.1.1.2: bytes=56 Sequence=1 ttl=252 time=127 ms
```

```
Reply from 20.1.1.2: bytes=56 Sequence=2 ttl=252 time=97 ms
```

```
Reply from 20.1.1.2: bytes=56 Sequence=3 ttl=252 time=83 ms
```

```
Reply from 20.1.1.2: bytes=56 Sequence=4 ttl=252 time=70 ms
```

```
Reply from 20.1.1.2: bytes=56 Sequence=5 ttl=252 time=60 ms
```

```
--- 20.1.1.2 ping statistics ---
```

```
5 packet(s) transmitted
```

```
5 packet(s) received
```

```
0.00% packet loss
```

```
round-trip min/avg/max = 60/87/127 ms
```

CE 3 和 CE 4 可以互相 Ping 通。

```
[CE3] ping 120.1.1.1
```

```
PING 120.1.1.1: 56 data bytes, press CTRL_C to break
```

```
Reply from 120.1.1.1: bytes=56 Sequence=1 ttl=252 time=102 ms
```

```
Reply from 120.1.1.1: bytes=56 Sequence=2 ttl=252 time=69 ms
```

```
Reply from 120.1.1.1: bytes=56 Sequence=3 ttl=252 time=105 ms
```

```
Reply from 120.1.1.1: bytes=56 Sequence=4 ttl=252 time=88 ms
```

```
Reply from 120.1.1.1: bytes=56 Sequence=5 ttl=252 time=87 ms
```

```
--- 120.1.1.1 ping statistics ---
```

```
5 packet(s) transmitted
```

```
5 packet(s) received
```

```
0.00% packet loss
```

```
round-trip min/avg/max = 69/90/105 ms
```

5. 完整配置

- PE1 的完整配置

```
#
```

```
mpls lsr-id 3.3.3.9
```

```
#
```

```
ip vpn-instance vpn1
```

```
route-distinguisher 200:1
```

```
vpn-target 1:1 export-extcommunity
```

```
vpn-target 1:1 import-extcommunity
```

```
#
```

```
mpls
```

```

lsp-trigger all
#
mpls ldp
#
mpls ldp vpn-instance vpn1
#
isis 1
network-entity 10.0000.0000.0000.0004.00
#
isis 2 vpn-instance vpn1
network-entity 10.0000.0000.0000.0003.00
import-route bgp
#
interface LoopBack0
ip address 3.3.3.9 255.255.255.255
isis enable 1
#
interface Vlan-interface1
ip binding vpn-instance vpn1
ip address 11.1.1.2 255.255.255.0
isis enable 2
mpls
mpls ldp
mpls ldp transport-address interface
#
interface Vlan-interface2
ip address 30.1.1.1 255.255.255.0
isis enable 1
mpls
mpls ldp
mpls ldp transport-address interface
#
bgp 100
undo synchronization
peer 4.4.4.9 as-number 100
peer 4.4.4.9 connect-interface LoopBack0
#
ipv4-family vpn-instance vpn1
import-route isis 2
#
ipv4-family vpnv4
peer 4.4.4.9 enable
• PE2 的完整配置
#
mpls lsr-id 4.4.4.9
#
ip vpn-instance vpn1
route-distinguisher 200:1

```

```

vpn-target 1:1 export-extcommunity
vpn-target 1:1 import-extcommunity
#
mpls
lsp-trigger all
#
mpls ldp
#
mpls ldp vpn-instance vpn1
#
isis 1
network-entity 10.0000.0000.0000.0004.00
#
isis 2 vpn-instance vpn1
network-entity 10.0000.0000.0000.0003.00
import-route bgp
#
interface LoopBack0
ip address 4.4.4.9 255.255.255.255
isis enable 1
#
interface Vlan-interface1
ip binding vpn-instance vpn1
ip address 21.1.1.1 255.255.255.0
isis enable 2
mpls
mpls ldp
mpls ldp transport-address interface
#
interface Vlan-interface2
ip address 30.1.1.2 255.255.255.0
isis enable 1
mpls
mpls ldp
mpls ldp transport-address interface
#
bgp 100
undo synchronization
peer 3.3.3.9 as-number 100
peer 3.3.3.9 connect-interface LoopBack0
#
ipv4-family vpn-instance vpn1
import-route isis 2
#
ipv4-family vpnv4
peer 3.3.3.9 enable
• CE1 的完整配置
#

```

```

mpls lsr-id 2.2.2.9
#
mpls
  lsp-trigger all
#
mpls ldp
#
isis 2
  network-entity 10.0000.0000.0000.0002.00
#
interface LoopBack0
  ip address 2.2.2.9 255.255.255.255
  isis enable 2
#
interface Vlan-interface1
  ip binding vpn-instance vpn1
  ip address 11.1.1.1 255.255.255.0
  isis enable 2
mpls
mpls ldp
mpls ldp transport-address interface
#
interface Vlan-interface2
  ip address 10.1.1.2 255.255.255.0
  isis enable 2
mpls
mpls ldp
mpls ldp transport-address interface

```

- CE2 的完整配置

CE2 的完整配置除接口 IP 地址和路由发布网段与 CE1 不同外，其他配置基本一致，这里不再赘述。

- PE3 的完整配置

```

#
mpls lsr-id 1.1.1.9
#
ip vpn-instance vpn1
  route-distinguisher 100:1
  vpn-target 1:1 export-extcommunity
  vpn-target 1:1 import-extcommunity
#
mpls
  lsp-trigger all
#
mpls ldp
#
mpls ldp vpn-instance vpn1
#
isis 2

```

```

network-entity 10.0000.0000.0000.0001.00
#
interface LoopBack0
 ip address 1.1.1.9 255.255.255.255
 isis enable 2
#
interface Vlan-interface1
 ip binding vpn-instance vpn1
 ip address 100.1.1.2 255.255.255.0
#
interface Vlan-interface2
 ip address 10.1.1.1 255.255.255.0
 isis enable 2
mpls
mpls ldp
mpls ldp transport-address interface
#
bgp 100
 undo synchronization
 peer 6.6.6.9 as-number 100
 peer 6.6.6.9 connect-interface LoopBack0
#
ipv4-family vpn-instance vpn1
 peer 100.1.1.1 as-number 65410
 import-route direct
#
ipv4-family vpnv4
 peer 6.6.6.9 enable

```

- PE4 的完整配置

PE4 的完整配置除接口 IP 地址和路由发布网段与 PE3 不同外，其他配置基本一致，这里不再赘述。

- CE3 的完整配置

```

#
interface Vlan-interface1
 ip address 100.1.1.1 255.255.255.0
#
bgp 65410
 peer 100.1.1.2 as-number 100
 import-route direct

```

- CE4 的完整配置

```

#
interface Vlan-interface1
 ip address 120.1.1.1 255.255.255.0
#
bgp 65420
 peer 120.1.1.2 as-number 100
 import-route direct

```

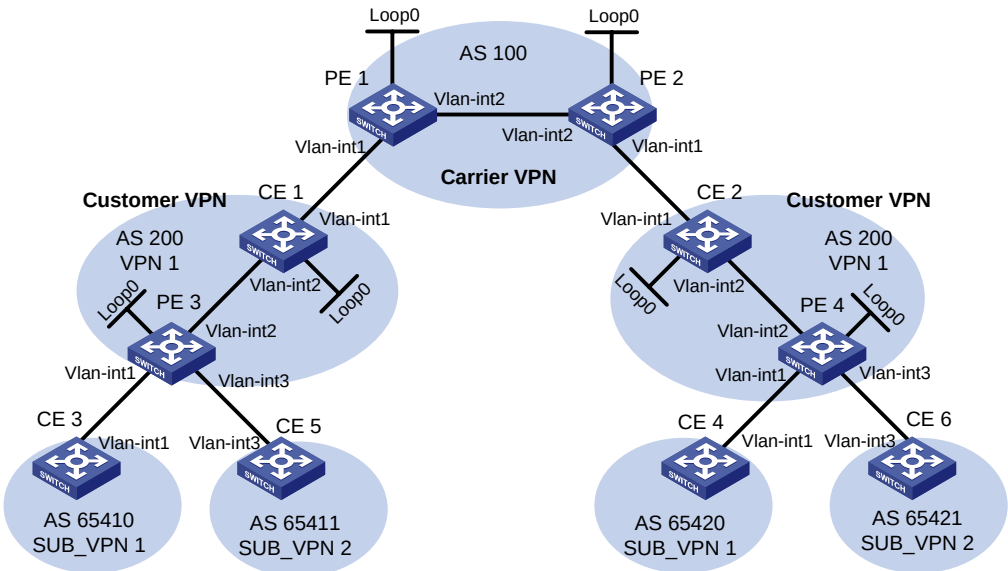
6. 配置注意事项

无

1.3.6 嵌套 VPN 典型配置指导

1. 组网图

图1-11 嵌套 VPN 组网示意图



设备	接口	IP 地址	设备	接口	IP 地址
CE 1	Loop0	2.2.2.9/32	CE 2	Loop0	5.5.5.9/32
	Vlan-int2	10.1.1.2/24		Vlan-int1	21.1.1.2/24
	Vlan-int1	11.1.1.1/24		Vlan-int2	20.1.1.1/24
CE 3	Vlan-int1	100.1.1.1/24	CE 4	Vlan-int1	120.1.1.1/24
CE 5	Vlan-int3	110.1.1.1/24	CE 6	Vlan-int3	130.1.1.1/24
PE 1	Loop0	3.3.3.9/32	PE 2	Loop0	4.4.4.9/32
	Vlan-int1	11.1.1.2/24		Vlan-int1	21.1.1.1/24
	Vlan-int2	30.1.1.1/24		Vlan-int2	30.1.1.2/24
PE 3	Loop0	1.1.1.9/32	PE 4	Loop0	6.6.6.9/32
	Vlan-int1	100.1.1.2/24		Vlan-int1	120.1.1.2/24
	Vlan-int2	10.1.1.1/24		Vlan-int2	20.1.1.2/24
	Vlan-int3	110.1.1.2/24		Vlan-int3	130.1.1.2/24

2. 应用要求

运营商向客户提供嵌套VPN服务。如图 1-11所示：

- PE 1 和 PE 2 是运营商骨干网的 PE 设备，支持嵌套 VPN 功能；
- CE 1 和 CE 2 是 VPN 用户的 CE 设备，接入运营商的骨干网，该 CE 设备支持发送 VPNv4 路由；
- PE 3 和 PE 4 是用户网络内部的 PE 设备，支持 MPLS L3VPN；
- CE 3、CE 4、CE 5 和 CE 6 是用户网络内部的子 VPN 的 CE 设备；

配置嵌套 VPN 的关键在于理解子 VPN 路由在运营商 PE 设备上的处理过程：

- 运营商 PE（PE 1 和 PE 2）收到用户 CE（CE 1 和 CE 2）发送来的 VPNv4 路由时，需要将该 VPNv4 路由的 RD 更换为用户 CE 所处 VPN 的 RD，同时将用户 CE 所处 VPN 的 ERT 添加到路由的扩展团体属性列表中，然后再按照一般的 VPNv4 路由发送出去；

- 为了实现用户网络内部子 VPN 的路由在用户 PE 和运营商 PE 间交换，需要在运营商 PE 和用户 CE 间建立 MP-EBGP 对等体关系。

3. 适用产品、版本

表1-11 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S7500E 系列以太网交换机	Release 6300 软件版本	LSQ1SRP1CB 引擎或者全部采用 EA 系列业务板

4. 配置过程 and 解释

- (1) 配置运营商骨干网的 MPLS L3VPN，使用 IS-IS 作为骨干网的 IGP 协议，PE 1 和 PE 2 之间使能 LDP，并建立 MP-IBGP 对等体关系

配置 PE 1。

```
<PE1> system-view
[PE1] interface loopback 0
[PE1-LoopBack0] ip address 3.3.3.9 32
[PE1-LoopBack0] quit
[PE1] mpls lsr-id 3.3.3.9
[PE1] mpls
[PE1-mpls] quit
[PE1] mpls ldp
[PE1-mpls-ldp] quit
[PE1] isis 1
[PE1-isis-1] network-entity 10.0000.0000.0000.0004.00
[PE1-isis-1] quit
[PE1] interface loopback 0
[PE1-LoopBack0] isis enable 1
[PE1-LoopBack0] quit
[PE1] interface vlan-interface 2
[PE1-Vlan-interface2] ip address 30.1.1.1 24
[PE1-Vlan-interface2] isis enable 1
[PE1-Vlan-interface2] mpls
[PE1-Vlan-interface2] mpls ldp
[PE1-Vlan-interface2] quit
[PE1] bgp 100
[PE1-bgp] peer 4.4.4.9 as-number 100
[PE1-bgp] peer 4.4.4.9 connect-interface loopback 0
[PE1-bgp] ipv4-family vpnv4
[PE1-bgp-af-vpnv4] peer 4.4.4.9 enable
[PE1-bgp-af-vpnv4] quit
[PE1-bgp] quit
```



说明

PE 2 的配置与 PE 1 类似，配置过程省略。

配置完成后, 在 PE 1 或 PE 2 上执行 **display mpls ldp session** 命令可以看到 LDP 会话建立成功; 执行 **display bgp peer** 命令可以看到 BGP 对等体关系已建立, 并达到 **Established** 状态; 执行 **display isis peer** 命令可以看到 IS-IS 邻居关系已建立, 状态为 **up**。

以 PE 1 为例:

```
[PE1] display mpls ldp session
```

```

      LDP Session(s) in Public Network
-----
Peer-ID      Status      LAM  SsnRole  FT   MD5   KA-Sent/Rcv
-----
4.4.4.9:0    Operational  DU   Active   Off  Off   378/378
-----
LAM : Label Advertisement Mode      FT : Fault Tolerance
[PE1] display bgp peer
BGP local router ID : 3.3.3.9
Local AS number : 100
Total number of peers : 1      Peers in established state : 1
Peer      V  AS  MsgRcvd  MsgSent  OutQ  PrefRcv  Up/Down  State
4.4.4.9   4 100   162     145     0       0   02:12:47 Established
[PE1] display isis peer
      Peer information for ISIS(1)
-----
System Id   Interface      Circuit Id  State HoldTime  Type  PRI
0000.0000.0005 Vlan-interface2 001      Up    29s     L1L2  --

```

(2) 配置用户网络: 使用 IS-IS 作为 IGP 协议, PE 3 和 CE 1、PE 4 和 CE 2 之间分别使能 LDP
配置 PE 3。

```

<PE3> system-view
[PE3] interface loopback 0
[PE3-LoopBack0] ip address 1.1.1.9 32
[PE3-LoopBack0] quit
[PE3] mpls lsr-id 1.1.1.9
[PE3] mpls
[PE3-mpls] quit
[PE3] mpls ldp
[PE3-mpls-ldp] quit
[PE3] isis 2
[PE3-isis-2] network-entity 10.0000.0000.0000.0001.00
[PE3-isis-2] quit
[PE3] interface loopback 0
[PE3-LoopBack0] isis enable 2
[PE3-LoopBack0] quit
[PE3-Vlan-interface2] ip address 10.1.1.1 24
[PE3-Vlan-interface2] isis enable 2
[PE3-Vlan-interface2] mpls
[PE3-Vlan-interface2] mpls ldp
[PE3-Vlan-interface2] quit

```

配置 CE 1。

```
<CE1> system-view
[CE1] interface loopback 0
[CE1-LoopBack0] ip address 2.2.2.9 32
[CE1-LoopBack0] quit
[CE1] mpls lsr-id 2.2.2.9
[CE1] mpls
[CE1-mpls] quit
[CE1] mpls ldp
[CE1-mpls-ldp] quit
[CE1] isis 2
[CE1-isis-2] network-entity 10.0000.0000.0000.0002.00
[CE1-isis-2] quit
[CE1] interface loopback 0
[CE1-LoopBack0] isis enable 2
[CE1-LoopBack0] quit
[CE1] interface vlan-interface 2
[CE1-Vlan-interface2] ip address 10.1.1.2 24
[CE1-Vlan-interface2] isis enable 2
[CE1-Vlan-interface2] mpls
[CE1-Vlan-interface2] mpls ldp
[CE1-Vlan-interface2] quit
```

配置完成后，PE 3 和 CE 1 之间可以建立 LDP 和 IS-IS 邻居关系。



说明

PE 4 和 CE 2 之间的配置与 PE 3 和 CE 1 之间的配置类似，配置过程省略。

(3) 配置用户 CE 接入到运营商的 PE

配置 PE 1

```
[PE1] ip vpn-instance vpn1
[PE1-vpn-instance-vpn1] route-distinguisher 200:1
[PE1-vpn-instance-vpn1] vpn-target 1:1
[PE1-vpn-instance-vpn1] quit
[PE1] interface vlan-interface1
[PE1-Vlan-interface1] ip binding vpn-instance vpn1
[PE1-Vlan-interface1] ip address 11.1.1.2 24
[PE1-Vlan-interface1] mpls
[PE1-Vlan-interface1] quit
[PE1] bgp 100
[PE1-bgp] ipv4-family vpn-instance vpn1
[PE1-bgp-vpn1] peer 11.1.1.1 as-number 200
[PE1-bgp-vpn1] quit
[PE1-bgp] quit
```

配置 CE 1。

```
[CE1] interface vlan-interface 1
```

```
[CE1-Vlan-interface1] ip address 11.1.1.1 24
[CE1-Vlan-interface1] mpls
[CE1-Vlan-interface1] quit
[CE1] bgp 200
[CE1-bgp] peer 11.1.1.2 as-number 100
[CE1-bgp] import isis 2
[CE1-bgp] quit
```



说明

PE 2 和 CE 2 之间的配置与 PE 1 和 CE 1 之间的配置类似，配置过程省略。

(4) 配置子 VPN 的 CE 接入用户网络的 PE

配置 CE 3。

```
<CE3> system-view
[CE3] interface vlan-interface1
[CE3-Vlan-interface1] ip address 100.1.1.1 24
[CE3-Vlan-interface1] quit
[CE3] bgp 65410
[CE3-bgp] peer 100.1.1.2 as-number 200
[CE3-bgp] import-route direct
[CE3-bgp] quit
```

配置 CE 5。

```
<CE5> system-view
[CE5] interface vlan-interface 3
[CE5-Vlan-interface3] ip address 110.1.1.1 24
[CE5-Vlan-interface3] quit
[CE5] bgp 65411
[CE5-bgp] peer 110.1.1.2 as-number 200
[CE5-bgp] import-route direct
[CE5-bgp] quit
```

配置 PE 3。

```
[PE3] ip vpn-instance SUB_VPN1
[PE3-vpn-instance-SUB_VPN1] route-distinguisher 100:1
[PE3-vpn-instance-SUB_VPN1] vpn-target 2:1
[PE3-vpn-instance-SUB_VPN1] quit
[PE3] interface vlan-interface 1
[PE3-Vlan-interface1] ip binding vpn-instance SUB_VPN1
[PE3-Vlan-interface1] ip address 100.1.1.2 24
[PE3-Vlan-interface1] quit
[PE3] ip vpn-instance SUB_VPN2
[PE3-vpn-instance-SUB_VPN2] route-distinguisher 101:1
[PE3-vpn-instance-SUB_VPN2] vpn-target 2:2
[PE3-vpn-instance-SUB_VPN2] quit
[PE3] interface vlan-interface 3
[PE3-Vlan-interface3] ip binding vpn-instance SUB_VPN2
```

```
[PE3-Vlan-interface3] ip address 110.1.1.2 24
[PE3-Vlan-interface3] quit
[PE3] bgp 200
[PE3-bgp] ipv4-family vpn-instance SUB_VPN1
[PE3-bgp-SUB_VPN1] peer 100.1.1.1 as-number 65410
[PE3-bgp-SUB_VPN1] import-route direct
[PE3-bgp-SUB_VPN1] quit
[PE3-bgp] ipv4-family vpn-instance SUB_VPN2
[PE3-bgp-SUB_VPN2] peer 100.1.1.1 as-number 65411
[PE3-bgp-SUB_VPN2] import-route direct
[PE3-bgp-SUB_VPN2] quit
[PE3-bgp] quit
```



说明

PE 4 和 CE 4, CE 6 之间的配置与 PE 3 和 CE 3, CE 5 之间的配置类似, 配置过程省略。

(5) 在运营商的 PE 和用户的 CE 之间建立 MP-EBGP 对等体关系, 交换用户的 VPNv4 路由

配置 PE 1, 使能嵌套 VPN 特性。

```
[PE1] bgp 100
[PE1-bgp] ipv4-family vpnv4
[PE1-bgp-af-vpnv4] nesting-vpn
[PE1-bgp-af-vpnv4] peer 11.1.1.1 vpn-instance vpn1 enable
[PE1-bgp-af-vpnv4] quit
[PE1-bgp] quit
```

配置 CE 1, 使能 VPNv4 能力, 使之与 PE 1 建立 VPNv4 邻居关系。

```
[CE1] bgp 200
[CE1-bgp] ipv4-family vpnv4
[CE1-bgp-af-vpnv4] peer 11.1.1.2 enable

# 配置允许本地 AS 号在所接收的路由的 AS_PATH 属性中出现。
[CE1-bgp-af-vpnv4] peer 11.1.1.2 allow-as-loop 2
```

配置接收所有 VPNv4 路由。

```
[CE1-bgp-af-vpnv4] undo policy vpn-target
[CE1-bgp-af-vpnv4] quit
[CE1-bgp] quit
```



说明

PE 2 和 CE 2 之间的配置与 PE 1 和 CE 1 之间的配置类似, 配置过程省略。

(6) 在用户网络内部的 PE 和 CE 之间建立 MP-IBGP 对等体关系, 交换用户内部子 VPN 的 VPNv4 路由

配置 PE 3。

```
[PE3] bgp 200
```

```
[PE3-bgp] peer 2.2.2.9 as-number 200
[PE3-bgp] peer 2.2.2.9 connect-interface loopback 0
[PE3-bgp] ipv4-family vpnv4
[PE3-bgp-af-vpnv4] peer 2.2.2.9 enable
```

配置允许本地 AS 号在所接收的路由的 AS_PATH 属性中出现。

```
[PE3-bgp-af-vpnv4] peer 2.2.2.9 allow-as-loop 2
[PE3-bgp-af-vpnv4] quit
[PE3-bgp] quit
```

配置 CE 1。

```
[CE1] bgp 200
[CE1-bgp] peer 1.1.1.9 as-number 200
[CE1-bgp] peer 1.1.1.9 connect-interface loopback 0
[CE1-bgp] ipv4-family vpnv4
[CE1-bgp-af-vpnv4] peer 1.1.1.9 enable
[CE1-bgp-af-vpnv4] undo policy vpn-target
[CE1-bgp-af-vpnv4] quit
[CE1-bgp] quit
```



说明

PE 4 和 CE 2 之间的配置与 PE 3 和 CE 1 之间的配置类似，配置过程省略。

(7) 配置完成后的检验

所有配置完成后，在 PE 1 和 PE 2 上执行 **display ip routing-table** 命令，可以看到 PE 1 和 PE 2 的公网路由表中只有运营商网络的路由。以 PE 1 为例：

```
[PE1] display ip routing-table
```

```
Routing Tables: Public
```

```
Destinations : 7      Routes : 7
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
3.3.3.9/32	Direct	0	0	127.0.0.1	InLoop0
4.4.4.9/32	ISIS	15	10	30.1.1.2	Vlan2
30.1.1.0/24	Direct	0	0	30.1.1.1	Vlan2
30.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
30.1.1.2/32	Direct	0	0	30.1.1.2	Vlan2
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0

在 PE 1 和 PE 2 上执行 **display ip routing-table vpn-instance** 命令，可以看到 VPN 路由表中有用户子 VPN 网络的路由。以 PE 1 为例：

```
[PE1] display ip routing-table vpn-instance vpn1
```

```
Routing Tables: vpn1
```

```
Destinations : 9      Routes : 9
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
11.1.1.0/24	Direct	0	0	11.1.1.1	Vlan1
11.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
11.1.1.2/32	Direct	0	0	11.1.1.2	Vlan1
100.1.1.0/24	BGP	255	0	11.1.1.1	NULL0
110.1.1.0/24	BGP	255	0	11.1.1.1	NULL0
120.1.1.0/24	BGP	255	0	4.4.4.9	NULL0
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
130.1.1.0/24	BGP	255	0	4.4.4.9	NULL0

在 CE 1 和 CE 2 上执行 **display bgp vpnv4 all routing-table** 命令，可以看到用户网络中 VPNv4 路由表中有子 VPN 网络的内部路由。以 CE 1 为例：

```
[CE1] display bgp vpnv4 all routing-table
```

```
BGP Local router ID is 11.11.11.11
```

```
Status codes: * - valid, > - best, d - damped,
```

```
h - history, i - internal, s - suppressed, S - Stale
```

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

```
Total number of routes from all PE: 4
```

```
Route Distinguisher: 100:1
```

Network	NextHop	In/Out Label	MED	LocPrf
*> 100.1.1.0/24	1.1.1.9	1024/1024		

```
Route Distinguisher: 101:1
```

Network	NextHop	In/Out Label	MED	LocPrf
*> 110.1.1.0/24	1.1.1.9	1025/1025		

```
Route Distinguisher: 200:1
```

Network	NextHop	In/Out Label	MED	LocPrf
*> 120.1.1.0/24	11.1.1.2	1026/1027		

```
Route Distinguisher: 201:1
```

Network	NextHop	In/Out Label	MED	LocPrf
*> 130.1.1.0/24	11.1.1.2	1027/1028		

在 PE 3 和 PE 4 上执行 **display ip routing-table vpn-instance SUB_VPN1** 命令，可以看到私网路由表中有从运营商 PE 发布到用户网络子 VPN 内部的路由。以 PE 3 为例：

```
[PE3] display ip routing-table vpn-instance SUB_VPN1
```

```
Routing Tables: SUB_VPN1
```

```
Destinations : 5 Routes : 5
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
100.1.1.0/24	Direct	0	0	100.1.1.2	Vlan1
100.1.1.2/32	Direct	0	0	127.0.0.1	InLoop0
120.1.1.0/24	BGP	255	0	2.2.2.9	NULL0
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0

在 CE 3 和 CE 4 上执行 **display ip routing-table** 命令，可以看到路由表中有远端子 VPN 的路由。以 CE 3 为例：

```
[CE3] display ip routing-table
```

```
Routing Tables: Public
```

```
Destinations : 5 Routes : 5
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
100.1.1.0/24	Direct	0	0	100.1.1.1	Vlan1
100.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
120.1.1.0/24	BGP	255	0	100.1.1.2	Vlan1
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0

在 CE 5 和 CE 6 上执行 **display ip routing-table** 命令，可以看到路由表中有远端子 VPN 的路由。以 CE 5 为例：

```
[CE5] display ip routing-table
```

```
Routing Tables: Public
```

```
Destinations : 5 Routes : 5
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
110.1.1.0/24	Direct	0	0	110.1.1.1	Vlan1
110.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
130.1.1.0/24	BGP	255	0	110.1.1.2	Vlan1

CE 3 和 CE 4 可以互相 Ping 通。

```
[CE3] ping 120.1.1.1
```

```
PING 120.1.1.1: 56 data bytes, press CTRL_C to break
```

```

Reply from 120.1.1.1: bytes=56 Sequence=1 ttl=252 time=102 ms
Reply from 120.1.1.1: bytes=56 Sequence=2 ttl=252 time=69 ms
Reply from 120.1.1.1: bytes=56 Sequence=3 ttl=252 time=105 ms
Reply from 120.1.1.1: bytes=56 Sequence=4 ttl=252 time=88 ms
Reply from 120.1.1.1: bytes=56 Sequence=5 ttl=252 time=87 ms

--- 120.1.1.1 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
round-trip min/avg/max = 69/90/105 ms

```

CE 5 和 CE 6 可以互相 Ping 通。

```

[CE5] ping 130.1.1.1
PING 130.1.1.1: 56 data bytes, press CTRL_C to break
Reply from 130.1.1.1: bytes=56 Sequence=1 ttl=252 time=102 ms
Reply from 130.1.1.1: bytes=56 Sequence=2 ttl=252 time=69 ms
Reply from 130.1.1.1: bytes=56 Sequence=3 ttl=252 time=105 ms
Reply from 130.1.1.1: bytes=56 Sequence=4 ttl=252 time=88 ms
Reply from 130.1.1.1: bytes=56 Sequence=5 ttl=252 time=87 ms

--- 130.1.1.1 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
round-trip min/avg/max = 69/90/105 ms

```

CE 3 和 CE 6 不能互相 Ping 通。

```

[CE3] ping 130.1.1.1
PING 130.1.1.1: 56 data bytes, press CTRL_C to break
Request time out
Request time out
Request time out
Request time out
Request time out

--- 130.1.1.1 ping statistics ---
 5 packet(s) transmitted
 0 packet(s) received
100.00% packet loss

```

5. 完整配置

- PE1 的完整配置

```

#
mpls lsr-id 3.3.3.9
#

```



```

ip vpn-instance vpn1
  route-distinguisher 200:1
  vpn-target 1:1 export-extcommunity
  vpn-target 1:1 import-extcommunity
#
mpls
  lsp-trigger all
#
mpls ldp
#
isis 1
  network-entity 10.0000.0000.0000.0004.00
#
interface LoopBack0
  ip address 3.3.3.9 255.255.255.255
  isis enable 1
#
interface Vlan-interface1
  ip binding vpn-instance vpn1
  ip address 11.1.1.2 255.255.255.0
  mpls
#
interface Vlan-interface2
  ip address 30.1.1.1 255.255.255.0
  isis enable 1
  mpls
  mpls ldp
#
bgp 100
  undo synchronization
  peer 4.4.4.9 as-number 100
  peer 4.4.4.9 connect-interface LoopBack0
#
  ipv4-family vpn-instance vpn1
    peer 11.1.1.1 as-number 200
  #
  ipv4-family vpnv4
    peer 4.4.4.9 enable
    nesting-vpn
    peer 11.1.1.1 vpn-instance vpn1 enable

```

- CE1 的基本配置

```

#
mpls lsr-id 2.2.2.9
#
mpls
  lsp-trigger all
#
mpls ldp

```

```

#
isis 2
 network-entity 10.0000.0000.0000.0002.00
#
interface LoopBack0
 ip address 2.2.2.9 255.255.255.255
 isis enable 2
#
interface Vlan-interface1
 ip address 11.1.1.1 255.255.255.0
 mpls
#
interface Vlan-interface2
 ip address 10.1.1.2 255.255.255.0
 isis enable 2
 mpls
 mpls ldp
#
bgp 200
 import-route isis 2
 undo synchronization
 peer 11.1.1.2 as-number 100
 peer 1.1.1.9 as-number 200
 peer 1.1.1.9 connect-interface LoopBack0
#
 ipv4-family vpnv4
  undo policy vpn-target
 peer 11.1.1.2 enable
 peer 11.1.1.2 allow-as-loop 2
 peer 1.1.1.9 enable

```

- PE3 的完整配置

```

#
mpls lsr-id 1.1.1.9
#
ip vpn-instance SUB_VPN1
 route-distinguisher 100:1
 vpn-target 2:1 export-extcommunity
 vpn-target 2:1 import-extcommunity
#
ip vpn-instance SUB_VPN2
 route-distinguisher 101:1
 vpn-target 2:2 export-extcommunity
 vpn-target 2:2 import-extcommunity
#
mpls
 lsp-trigger all
#
mpls ldp

```

```

#
isis 2
 network-entity 10.0000.0000.0000.0001.00
#
interface LoopBack0
 ip address 1.1.1.9 255.255.255.255
 isis enable 2
#
interface Vlan-interface1
 ip binding vpn-instance SUB_VPN1
 ip address 100.1.1.2 255.255.255.0
#
interface Vlan-interface2
 ip address 10.1.1.1 255.255.255.0
 isis enable 2
mpls
mpls ldp
#
interface Vlan-interface3
 ip binding vpn-instance SUB_VPN2
 ip address 110.1.1.2 255.255.255.0
#
bgp 200
 undo synchronization
 peer 2.2.2.9 as-number 200
 peer 2.2.2.9 connect-interface LoopBack0
#
ipv4-family vpn-instance SUB_VPN1
 peer 100.1.1.1 as-number 65410
 import-route direct
#
ipv4-family vpn-instance SUB_VPN2
 peer 100.1.1.1 as-number 65411
 import-route direct
#
ipv4-family vpnv4
 peer 2.2.2.9 enable
 peer 2.2.2.9 allow-as-loop 2

```

- CE3 的完整配置

```

#
interface Vlan-interface1
 ip address 100.1.1.1 255.255.255.0
#
bgp 65410
 peer 100.1.1.2 as-number 200
 import-route direct

```

- CE5 的完整配置

```

#

```

```

interface Vlan-interface3
 ip address 110.1.1.1 255.255.255.0
#
bgp 65411
 peer 110.1.1.2 as-number 200
 import-route direct

```

- PE2 的完整配置

```

#
mpls lsr-id 4.4.4.9
#
ip vpn-instance vpn1
 route-distinguisher 200:1
 vpn-target 1:1 export-extcommunity
 vpn-target 1:1 import-extcommunity
#
mpls
 lsp-trigger all
#
mpls ldp
#
isis 1
 network-entity 10.0000.0000.0000.0005.00
#
interface LoopBack0
 ip address 4.4.4.9 255.255.255.255
 isis enable 1
#
interface Vlan-interface1
 ip binding vpn-instance vpn1
 ip address 21.1.1.2 255.255.255.0
 mpls
#
interface Vlan-interface2
 ip address 30.1.1.2 255.255.255.0
 isis enable 1
 mpls
 mpls ldp
#
bgp 100
 undo synchronization
 peer 3.3.3.9 as-number 100
 peer 3.3.3.9 connect-interface LoopBack0
#
ipv4-family vpn-instance vpn1
 peer 11.1.1.2 as-number 200
#
ipv4-family vpnv4
 peer 3.3.3.9 enable

```

```
nesting-vpn
peer 11.1.1.2 vpn-instance vpn1 enable
```

说明：

CE2、PE4、CE4、CE6 在网络中的位置与 CE1、PE3、CE3、CE5 所处位置一一对应，因此在配置上，只有接口地址以及路由发布网段的不同，配置思路基本一致，这些设备的完整配置这里不再赘述。

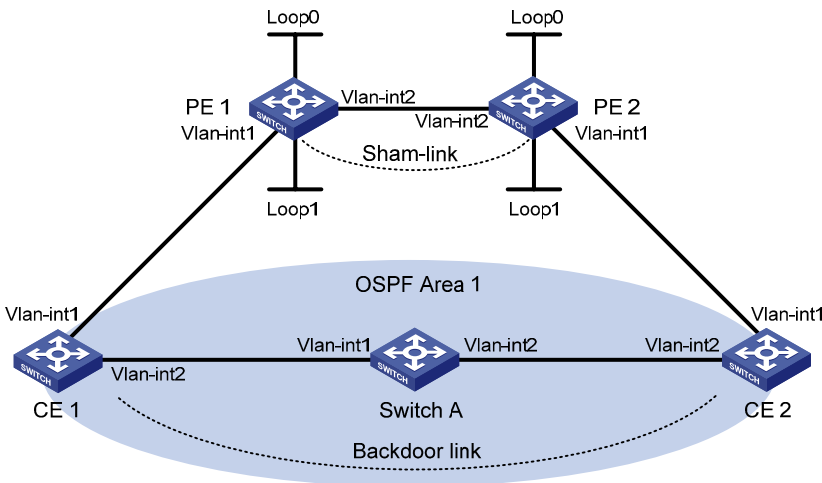
6. 配置注意事项

- 同一用户 VPN 的不同子 VPN 之间地址空间不能重叠。
- 建议嵌套 VPN 对等体的地址不要与公网中对等体的地址重叠。
- 配置嵌套 VPN 对等体或对等体组之前，需要先配置 BGP-VPN 实例视图下的 CE 对等体或对等体组。
- 目前嵌套 VPN 不支持多跳 EBGp 组网方式，因此运营商 PE 和 CE 之间必须使用直连接口地址建立邻居关系。
- 如果子 VPN 的 CE 设备直接连接运营商 PE 设备，则需要在该 PE 设备上配置策略路由，使得主 VPN 和子 VPN 可以互访。

1.3.7 OSPF 伪连接典型配置指导

1. 组网图

图1-12 OSPF 伪连接组网示意图



设备	接口	IP 地址	设备	接口	IP 地址
CE 1	Vlan-int1	100.1.1.1/24	CE 2	Vlan-int1	120.1.1.1/24
	Vlan-int2	20.1.1.1/24		Vlan-int2	30.1.1.2/24
PE 1	Loop0	1.1.1.9/32	PE 2	Loop0	2.2.2.9/32
	Loop1	3.3.3.3/32		Loop1	5.5.5.5/32
	Vlan-int1	100.1.1.2/24		Vlan-int1	120.1.1.2/24
	Vlan-int2	10.1.1.1/24		Vlan-int2	10.1.1.2/24
Switch A	Vlan-int1	20.1.1.2/24			
	Vlan-int2	30.1.1.1/24			

2. 应用要求

- CE 1 和 CE 2 都属于 VPN 1，它们分别接入 PE 1 和 PE 2；

- CE 1 和 CE 2 在同一个 OSPF 区域中；
- CE 1 与 CE 2 之间的 VPN 流量通过 MPLS 骨干网转发，不使用 OSPF 的区域内部路由。

3. 适用产品、版本

表1-12 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S7500E 系列以太网交换机	Release 6300 软件版本	LSQ1SRP1CB 引擎或者全部采用 EA 系列业务板

4. 配置过程 and 解释

(1) 配置用户网络上的 OSPF

在 CE 1、Switch A、CE 2 上配置普通 OSPF，发布图 1-12 中所示各接口的网段地址。具体配置过程略。

配置完成后，CE 1 和 CE 2 应学习到对端 Vlan-interface1 接口的 OSPF 路由。

以 CE 1 为例：

```
<CE1> display ip routing-table
Routing Tables: Public
  Destinations : 9          Routes : 9
Destination/Mask    Proto   Pre  Cost   NextHop         Interface
20.1.1.0/24         Direct  0     0       20.1.1.1         Vlan2
20.1.1.1/32         Direct  0     0       127.0.0.1        InLoop0
20.1.1.2/32         Direct  0     0       20.1.1.2         Vlan2
30.1.1.0/24         OSPF    10    3124    20.1.1.2         Vlan2
100.1.1.0/24        Direct  0     0       100.1.1.1        Vlan1
100.1.1.1/32        Direct  0     0       127.0.0.1        InLoop0
120.1.1.0/24        OSPF    10    3125    20.1.1.2         Vlan2
127.0.0.0/8         Direct  0     0       127.0.0.1        InLoop0
127.0.0.1/32        Direct  0     0       127.0.0.1        InLoop0
```

(2) 在骨干网上配置 MPLS L3VPN

配置 PE 1。

配置 PE 1 的 MPLS 基本能力和 MPLS LDP 能力，建立 LDP LSP。

```
<PE1> system-view
[PE1] interface loopback 0
[PE1-LoopBack0] ip address 1.1.1.9 32
[PE1-LoopBack0] quit
[PE1] mpls lsr-id 1.1.1.9
[PE1] mpls
[PE1-mpls] quit
[PE1] mpls ldp
[PE1-mpls-ldp] quit
[PE1] interface vlan-interface 2
[PE1-Vlan-interface2] ip address 10.1.1.1 24
[PE1-Vlan-interface2] mpls
```

```
[PE1-Vlan-interface2] mpls ldp
```

```
[PE1-Vlan-interface2] quit
```

配置 PE 1 的 MP-IBGP 对等体为 PE2。

```
[PE1] bgp 100
```

```
[PE1-bgp] peer 2.2.2.9 as-number 100
```

```
[PE1-bgp] peer 2.2.2.9 connect-interface loopback 0
```

```
[PE1-bgp] ipv4-family vpnv4
```

```
[PE1-bgp-af-vpnv4] peer 2.2.2.9 enable
```

```
[PE1-bgp-af-vpnv4] quit
```

```
[PE1-bgp] quit
```

配置 PE 1 的 OSPF。

```
[PE1]ospf 1
```

```
[PE1-ospf-1]area 0
```

```
[PE1-ospf-1-area-0.0.0.0]network 1.1.1.9 0.0.0.0
```

```
[PE1-ospf-1-area-0.0.0.0]network 10.1.1.0 0.0.0.255
```

```
[PE1-ospf-1-area-0.0.0.0]quit
```

```
[PE1-ospf-1]quit
```

配置 PE 2 的 MPLS 基本能力和 MPLS LDP 能力，建立 LDP LSP。

```
<PE2> system-view
```

```
[PE2] interface loopback 0
```

```
[PE2-LoopBack0] ip address 2.2.2.9 32
```

```
[PE2-LoopBack0] quit
```

```
[PE2] mpls lsr-id 2.2.2.9
```

```
[PE2] mpls
```

```
[PE2-mpls] quit
```

```
[PE2] mpls ldp
```

```
[PE2-mpls-ldp] quit
```

```
[PE2] interface vlan-interface 2
```

```
[PE2-Vlan-interface2] ip address 10.1.1.2 24
```

```
[PE2-Vlan-interface2] mpls
```

```
[PE2-Vlan-interface2] mpls ldp
```

```
[PE2-Vlan-interface2] quit
```

配置 PE 2 的 MP-IBGP 对等体为 PE1。

```
[PE2] bgp 100
```

```
[PE2-bgp] peer 1.1.1.9 as-number 100
```

```
[PE2-bgp] peer 1.1.1.9 connect-interface loopback 0
```

```
[PE2-bgp] ipv4-family vpnv4
```

```
[PE2-bgp-af-vpnv4] peer 1.1.1.9 enable
```

```
[PE2-bgp-af-vpnv4] quit
```

```
[PE2-bgp] quit
```

配置 PE 2 的 OSPF。

```
[PE2]ospf 1
```

```
[PE2-ospf-1]area 0
```

```
[PE2-ospf-1-area-0.0.0.0]network 2.2.2.9 0.0.0.0
```

```
[PE2-ospf-1-area-0.0.0.0]network 10.1.1.0 0.0.0.255
```

```
[PE2-ospf-1-area-0.0.0.0]quit
```

```
[PE2-ospf-1]quit
```

(3) 配置 PE 接入 CE

配置 PE 1 接入 CE 1。

```
[PE1] ip vpn-instance vpn1
```

```
[PE1-vpn-instance-vpn1] route-distinguisher 100:1
```

```
[PE1-vpn-instance-vpn1] vpn-target 1:1
```

```
[PE1-vpn-instance-vpn1] quit
```

```
[PE1] interface vlan-interface 1
```

```
[PE1-Vlan-interface1] ip binding vpn-instance vpn1
```

```
[PE1-Vlan-interface1] ip address 100.1.1.2 24
```

```
[PE1-Vlan-interface1] quit
```

```
[PE1] ospf 100 vpn-instance vpn1
```

```
[PE1-ospf-100] domain-id 10
```

```
[PE1-ospf-100] area 1
```

```
[PE1-ospf-100-area-0.0.0.1] network 100.1.1.0 0.0.0.255
```

```
[PE1-ospf-100-area-0.0.0.1] quit
```

```
[PE1-ospf-100] quit
```

```
[PE2] bgp 100
```

```
[PE1-bgp] ipv4-family vpn-instance vpn1
```

```
[PE1-bgp-vpn1] import-route ospf 100
```

```
[PE1-bgp-vpn1] quit
```

```
[PE1-bgp] quit
```

配置 PE 2 接入 CE 2。

```
[PE2] ip vpn-instance vpn1
```

```
[PE2-vpn-instance-vpn1] route-distinguisher 100:2
```

```
[PE2-vpn-instance-vpn1] vpn-target 1:1
```

```
[PE2-vpn-instance-vpn1] quit
```

```
[PE2] interface vlan-interface 1
```

```
[PE2-Vlan-interface1] ip binding vpn-instance vpn1
```

```
[PE2-Vlan-interface1] ip address 120.1.1.2 24
```

```
[PE2-Vlan-interface1] quit
```

```
[PE2] ospf 100 vpn-instance vpn1
```

```
[PE2-ospf-100] domain-id 10
```

```
[PE2-ospf-100] area 1
```

```
[PE2-ospf-100-area-0.0.0.1] network 120.1.1.0 0.0.0.255
```

```
[PE2-ospf-100-area-0.0.0.1] quit
```

```
[PE2-ospf-100] quit
```

```
[PE2] bgp 100
```

```
[PE2-bgp] ipv4-family vpn-instance vpn1
```

```
[PE2-bgp-vpn1] import-route ospf 100
```

```
[PE2-bgp-vpn1] quit
```

```
[PE2-bgp] quit
```

完成上述配置后，在 PE 设备上执行 **display ip routing-table vpn-instance** 命令，可以看到去往对端 CE 的路由是通过用户网络的 OSPF 路由，不是通过骨干网的 BGP 路由。

以 PE 1 为例：


```
[PE1] display ip routing-table vpn-instance vpn1
```

```
Routing Tables: vpn1
```

Destinations : 5			Routes : 5			
Destination/Mask	Proto	Pre	Cost	NextHop	Interface	
20.1.1.0/24	OSPF	10	1563	100.1.1.1	Vlan1	
30.1.1.0/24	OSPF	10	3125	100.1.1.1	Vlan1	
100.1.1.0/24	Direct	0	0	100.1.1.2	Vlan1	
100.1.1.2/32	Direct	0	0	127.0.0.1	InLoop0	
120.1.1.0/24	OSPF	10	3126	100.1.1.1	Vlan1	

(4) 配置 Sham-link

配置 PE 1。

```
[PE1] interface loopback 1
```

```
[PE1-LoopBack1] ip binding vpn-instance vpn1
```

```
[PE1-LoopBack1] ip address 3.3.3.3 32
```

```
[PE1-LoopBack1] quit
```

```
[PE1] ospf 100
```

```
[PE1-ospf-100] area 1
```

```
[PE1-ospf-100-area-0.0.0.1] sham-link 3.3.3.3 5.5.5.5 cost 10
```

```
[PE1-ospf-100-area-0.0.0.1] quit
```

```
[PE1-ospf-100] quit
```

配置 PE 2。

```
[PE2] interface loopback 1
```

```
[PE2-LoopBack1] ip binding vpn-instance vpn1
```

```
[PE2-LoopBack1] ip address 5.5.5.5 32
```

```
[PE2-LoopBack1] quit
```

```
[PE2] ospf 100
```

```
[PE2-ospf-100] area 1
```

```
[PE2-ospf-100-area-0.0.0.1] sham-link 5.5.5.5 3.3.3.3 cost 10
```

```
[PE2-ospf-100-area-0.0.0.1] quit
```

```
[PE2-ospf-100] quit
```

完成上述配置后，在 PE 设备上再次执行 **display ip routing-table vpn-instance** 命令，可以看到去往对端 CE 的路由变成了通过骨干网的 BGP 路由，并且有去往 Sham-link 目的地址的路由。

以 PE 1 为例：

```
[PE1] display ip routing-table vpn-instance vpn1
```

```
Routing Tables: vpn1
```

Destinations : 6			Routes : 6			
Destination/Mask	Proto	Pre	Cost	NextHop	Interface	
3.3.3.3/32	Direct	0	0	127.0.0.1	InLoop0	
5.5.5.5/32	BGP	255	0	2.2.2.9	NULL0	
20.1.1.0/24	OSPF	10	1563	100.1.1.1	Vlan1	
100.1.1.0/24	Direct	0	0	100.1.1.2	Vlan1	
100.1.1.2/32	Direct	0	0	127.0.0.1	InLoop0	
120.1.1.0/24	BGP	255	0	2.2.2.9	NULL0	

在 CE 设备上执行 **display ip routing-table** 命令，可以看到去往对端 CE 的 OSPF 路由开销变为 10（为 Sham-link 配置的开销），下一跳变为接入 PE 的 Vlan-interface1 接口，即去往对端的 VPN 流量将通过骨干网转发。

以 CE 1 为例：

```
[CE1] display ip routing-table
```

```
Routing Tables: Public
```

Destinations : 9			Routes : 9		
Destination/Mask	Proto	Pre	Cost	NextHop	Interface
20.1.1.0/24	Direct	0	0	20.1.1.1	Vlan2
20.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
20.1.1.2/32	Direct	0	0	20.1.1.2	Vlan2
30.1.1.0/24	OSPF	10	1574	100.1.1.2	Vlan1
100.1.1.0/24	Direct	0	0	100.1.1.1	Vlan1
100.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
120.1.1.0/24	OSPF	10	12	100.1.1.2	Vlan1
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0

在 PE 上执行 **display ospf sham-link** 命令可以看到 Sham-link 的建立情况。

以 PE 1 为例：

```
[PE1] display ospf sham-link
```

```
OSPF Process 100 with Router ID 100.1.1.2
```

```
Sham Link:
```

Area	RouterId	Source-IP	Destination-IP	State	Cost
0.0.0.1	100.1.1.2	3.3.3.3	5.5.5.5	P-2-P	10

执行 **display ospf sham-link area** 命令可以看到对端状态为 Full。

```
[PE1] display ospf sham-link area 1
```

```
OSPF Process 100 with Router ID 100.1.1.2
```

```
Sham-Link: 3.3.3.3 --> 5.5.5.5
```

```
Neighbour State: Full
```

```
Area: 0.0.0.1
```

```
Cost: 10 State: P-2-P, Type: Sham
```

```
Timers: Hello 10 , Dead 40 , Retransmit 5 , Transmit Delay 1
```

5. 完整配置

• PE1 的完整配置

```
#
mpls lsr-id 1.1.1.9
#
ip vpn-instance vpn1
 route-distinguisher 100:1
 vpn-target 1:1 export-extcommunity
 vpn-target 1:1 import-extcommunity
#
mpls
 lsp-trigger all
```

```

#
mpls ldp
#
interface LoopBack0
 ip address 1.1.1.9 255.255.255.255
#
interface LoopBack1
 ip binding vpn-instance vpn1
 ip address 3.3.3.3 255.255.255.255
#
interface Vlan-interface1
 ip binding vpn-instance vpn1
 ip address 100.1.1.2 255.255.255.0
#
interface Vlan-interface2
 ip address 10.1.1.1 255.255.255.0
mpls
mpls ldp
#
bgp 100
 undo synchronization
 peer 2.2.2.9 as-number 100
 peer 2.2.2.9 connect-interface LoopBack0
#
 ipv4-family vpn-instance vpn1
  import-route ospf 100
#
 ipv4-family vpnv4
  peer 2.2.2.9 enable
#
ospf 1
 area 0.0.0.0
  network 1.1.1.9 0.0.0.0
  network 10.1.1.0 0.0.0.255
#
ospf 100 vpn-instance vpn1
 domain-id 0.0.0.10
 area 0.0.0.1
  network 100.1.1.0 0.0.0.255
  sham-link 3.3.3.3 5.5.5.5 cost 10

```

- PE2 的完整配置

```

#
mpls lsr-id 2.2.2.9
#
ip vpn-instance vpn1
 route-distinguisher 100:2
 vpn-target 1:1 export-extcommunity
 vpn-target 1:1 import-extcommunity

```

```

#
mpls
  lsp-trigger all
#
mpls ldp
#
interface LoopBack0
  ip address 2.2.2.9 255.255.255.255
#
interface LoopBack1
  ip binding vpn-instance vpn1
  ip address 5.5.5.5 255.255.255.255
#
interface Vlan-interface1
  ip binding vpn-instance vpn1
  ip address 120.1.1.2 255.255.255.0
#
interface Vlan-interface2
  ip address 10.1.1.2 255.255.255.0
mpls
mpls ldp
#
bgp 100
  undo synchronization
  peer 1.1.1.9 as-number 100
  peer 1.1.1.9 connect-interface LoopBack0
#
  ipv4-family vpn-instance vpn1
    import-route ospf 100
#
  ipv4-family vpnv4
    peer 1.1.1.9 enable
#
ospf 1
  area 0.0.0.0
    network 2.2.2.9 0.0.0.0
    network 10.1.1.0 0.0.0.255
#
ospf 100 vpn-instance vpn1
  domain-id 0.0.0.10
  area 0.0.0.1
    network 100.1.1.0 0.0.0.255
    sham-link 5.5.5.5 3.3.3.3 cost 10

```



说明

在CE 1、Switch A、CE 2上只需要配置普通OSPF，发布图 1-12中所示各接口的网段地址。完整配置这里省略。

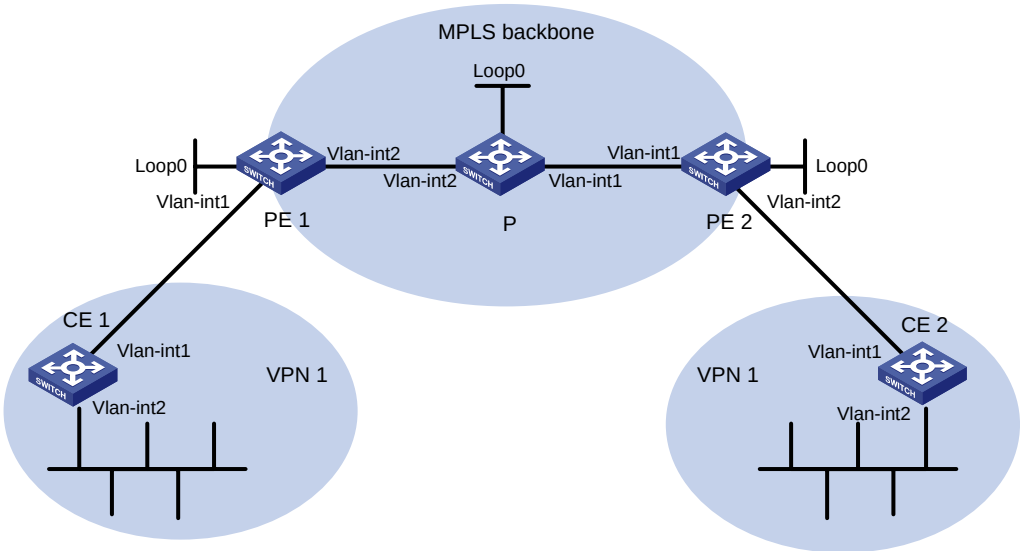
6. 配置注意事项

无

1.3.8 BGP 的 AS 号替换配置指导

1. 组网图

图1-13 BGP 的 AS 号替换组网图



设备	接口	IP 地址	设备	接口	IP 地址
CE 1	Vlan-int1	10.1.1.1/24	P	Loop0	2.2.2.9/32
	Vlan-int2	100.1.1.1/24		Vlan-int1	30.1.1.1/24
PE 1	Loop0	1.1.1.9/32		Vlan-int2	20.1.1.2/24
	Vlan-int1	10.1.1.2/24	PE 2	Loop0	3.3.3.9/32
	Vlan-int2	20.1.1.1/24		Vlan-int1	30.1.1.2/24
CE 2	Vlan-int1	10.2.1.1/24		Vlan-int2	10.2.1.2/24
	Vlan-int2	200.1.1.1/24			

2. 应用要求

如图所示，CE 1 和 CE 2 同属于 VPN 1，分别接入 PE 1 和 PE 2，并且 CE 1 和 CE 2 复用 AS 号 600。

3. 适用产品、版本

表1-13 配置适用的产品与软硬件版本关系

产品	软件版本	硬件版本
S7500E 系列以太网交换机	Release 6300 软件版本	LSQ1SRP1CB 引擎或者全部采用 EA 系列业务板

4. 配置过程和解释

(1) 配置基本 MPLS L3VPN

- 在 MPLS 骨干网上配置 OSPF，PE 和 P 之间能够学到对方 Loopback 接口的路由；
- 在 MPLS 骨干网上配置 MPLS 基本能力和 MPLS LDP，建立 LDP LSP；
- PE 之间建立 MP-IBGP 对等体关系，发布 VPN-IPv4 路由；

- 在 PE 2 上配置 VPN 1 的 VPN 实例，接入 CE 2；
- 在 PE 1 上配置 VPN 1 的 VPN 实例，接入 CE 1；
- PE 1 和 CE 1、PE 2 和 CE 2 之间配置 BGP，将 CE 的路由引入 PE。

完成上述配置后，在 CE 2 上执行 **display ip routing-table** 命令，可以看到 CE 2 能够学到 CE 1 接入 PE 1 的接口所在网段（10.1.1.0/24）的路由，但没有到达 CE 1 内部 VPN（100.1.1.0/24）的路由。CE 1 上也存在同样的现象。

```
<CE2> display ip routing-table
```

```
Routing Tables: Public
```

Destinations : 8		Routes : 8			
Destination/Mask	Proto	Pre	Cost	NextHop	Interface
10.1.1.0/24	BGP	255	0	10.2.1.2	Vlan1
10.1.1.1/32	BGP	255	0	10.2.1.2	Vlan1
10.2.1.0/24	Direct	0	0	10.2.1.1	Vlan1
10.2.1.1/32	Direct	0	0	127.0.0.1	InLoop0
10.2.1.2/32	Direct	0	0	10.2.1.2	Vlan1
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
200.1.1.0/24	Direct	0	0	200.1.1.1	InLoop0
200.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0

在 PE 上执行 **display ip routing-table vpn-instance** 命令，可以看到 PE 的 VPN 实例中有到达对端 CE 内部 VPN 的路由。

以 PE 2 为例：

```
<PE2> display ip routing-table vpn-instance vpn1
```

```
Routing Tables: vpn1
```

Destinations : 7		Routes : 7			
Destination/Mask	Proto	Pre	Cost	NextHop	Interface
10.1.1.0/24	BGP	255	0	1.1.1.9	NULL0
10.1.1.1/32	BGP	255	0	1.1.1.9	NULL0
10.2.1.0/24	Direct	0	0	10.2.1.2	Vlan1
10.2.1.1/32	Direct	0	0	10.2.1.1	Vlan1
10.2.1.2/32	Direct	0	0	127.0.0.1	InLoop0
100.1.1.1/32	BGP	255	0	1.1.1.9	NULL0
200.1.1.1/32	BGP	255	0	10.2.1.1	Vlan1

在 PE 2 上打开 BGP 的 Update 报文调试信息开关，可以看到 PE 2 发布了去往 100.1.1.1/32 的路由，AS 路径信息为“100 600”。

```
<PE2> terminal monitor
```

```
<PE2> terminal debugging
```

```
<PE2> debugging bgp update vpn-instance vpn1 verbose
```

```
<PE2> refresh bgp vpn-instance vpn1 all export
```

```
*0.4402392 PE2 RM/7/RMDEBUG:
```

```
BGP.vpn1: Send UPDATE to 10.2.1.1 for following destinations :
```

```
Origin : Incomplete
```

```
AS Path : 100 600
```

```
Next Hop : 10.2.1.2
```

```
100.1.1.1/32,
```

在 CE 2 上执行 **display bgp routing-table peer received-routes** 命令，可以看到 CE 2 没有接收 100.1.1.1/32 的路由。

```
<CE2> display bgp routing-table peer 10.2.1.2 received-routes
Total Number of Routes: 4
BGP Local router ID is 10.2.1.1
Status codes: * - valid, > - best, d - damped,
               h - history, i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

```

	Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
*>	10.1.1.0/24	10.2.1.2			0	100?
*>	10.1.1.1/32	10.2.1.2			0	100?
*	10.2.1.0/24	10.2.1.2	0		0	100?
*	10.2.1.1/32	10.2.1.2	0		0	100?

(2) 配置 BGP 的 AS 号替换功能

在 PE 2 上配置 BGP 的 AS 号替换功能。

```
<PE2> system-view
[PE2] bgp 100
[PE2-bgp] ipv4-family vpn-instance vpn1
[PE2-bgp-vpn1] peer 10.2.1.1 substitute-as
[PE2-bgp-vpn1] quit
[PE2-bgp] quit
```

可以看到 PE 2 向 CE2 发布的路由中，100.1.1.1/32 的 AS 路径信息由“100 600”变为“100 100”：

```
*0.13498737 PE2 RM/7/RMDEBUG:
      BGP.vpn1: Send UPDATE to 10.2.1.1 for following destinations :
      Origin   : Incomplete
      AS Path   : 100 100
      Next Hop  : 10.2.1.2
      100.1.1.1/32
```

再次查看 CE 2 接收的路由信息和路由表：

```
<CE2> display bgp routing-table peer 10.2.1.2 received-routes
Total Number of Routes: 5
BGP Local router ID is 10.2.1.1
Status codes: * - valid, > - best, d - damped,
               h - history, i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

```

	Network	NextHop	MED	LocPrf	PrefVal	Path/Ogn
*>	10.1.1.0/24	10.2.1.2			0	100?
*>	10.1.1.1/32	10.2.1.2			0	100?
*	10.2.1.0/24	10.2.1.2	0		0	100?
*	10.2.1.1/32	10.2.1.2	0		0	100?
*>	100.1.1.1/32	10.2.1.2			0	100 100?

```
<CE2> display ip routing-table
Routing Tables: Public
      Destinations : 9          Routes : 9

```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
10.1.1.0/24	BGP	255	0	10.2.1.2	Vlan1

10.1.1.1/32	BGP	255	0	10.2.1.2	Vlan1
10.2.1.0/24	Direct	0	0	10.2.1.1	Vlan1
10.2.1.1/32	Direct	0	0	127.0.0.1	InLoop0
10.2.1.2/32	Direct	0	0	10.2.1.2	Vlan1
100.1.1.1/32	BGP	255	0	10.2.1.2	Vlan1
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
200.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0

在 PE 1 上也配置 BGP 的 AS 号替换功能后, CE 1 和 CE 2 的 VLAN 接口能够相互 Ping 通。

```
<CE1> ping -a 100.1.1.1 200.1.1.1
PING 200.1.1.1: 56 data bytes, press CTRL_C to break
  Reply from 200.1.1.1: bytes=56 Sequence=1 ttl=253 time=109 ms
  Reply from 200.1.1.1: bytes=56 Sequence=2 ttl=253 time=67 ms
  Reply from 200.1.1.1: bytes=56 Sequence=3 ttl=253 time=66 ms
  Reply from 200.1.1.1: bytes=56 Sequence=4 ttl=253 time=85 ms
  Reply from 200.1.1.1: bytes=56 Sequence=5 ttl=253 time=70 ms
--- 200.1.1.1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 66/79/109 ms
```

5. 完整配置

- PE1 的完整配置

```
#
mpls lsr-id 1.1.1.9
#
ip vpn-instance vpn1
  route-distinguisher 100:1
  vpn-target 1:1 export-extcommunity
  vpn-target 1:1 import-extcommunity
#
mpls
  lsp-trigger all
#
mpls ldp
#
interface LoopBack0
  ip address 1.1.1.9 255.255.255.255
#
interface Vlan-interface1
  ip binding vpn-instance vpn1
  ip address 10.1.1.2 255.255.255.0
#
interface Vlan-interface2
  ip address 20.1.1.1 255.255.255.0
mpls
```



```

mpls ldp
#
bgp 100
undo synchronization
peer 3.3.3.9 as-number 100
peer 3.3.3.9 connect-interface LoopBack0
    peer 10.1.1.1 substitute-as
#
ipv4-family vpn-instance vpn1
    import-route bgp 600
#
ipv4-family vpv4
    peer 3.3.3.9 enable
#

```

- PE2 的完整配置

```

#
mpls lsr-id 3.3.3.9
#
ip vpn-instance vpn1
    route-distinguisher 100:1
    vpn-target 1:1 export-extcommunity
    vpn-target 1:1 import-extcommunity
#
mpls
    lsp-trigger all
#
mpls ldp
#
interface LoopBack0
    ip address 3.3.3.9 255.255.255.255
#
interface Vlan-interface1
    ip address 30.1.1.2 255.255.255.0
    mpls
        mpls ldp
#
interface Vlan-interface2
    ip binding vpn-instance vpn1
    ip address 10.2.1.2 255.255.255.0
#
bgp 100
undo synchronization
peer 1.1.1.9 as-number 100
peer 1.1.1.9 connect-interface LoopBack0
    peer 10.2.1.1 substitute-as
#
ipv4-family vpn-instance vpn1
    import-route bgp 600

```

```
#  
ipv4-family vpnv4  
    peer 1.1.1.9 enable  
#
```

6. 配置注意事项

无