



SC9600 系列 高端路由交换机  
操作手册  
(V2.2)



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

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

公司网址：<http://www.inspur.com/>

技术支持热线：400-691-1766

技术支持邮箱：[inspur\\_network@inspur.com](mailto:inspur_network@inspur.com)

技术文档邮箱：[inspur\\_network@inspur.com](mailto:inspur_network@inspur.com)

客户投诉热线：400-691-1766

公司总部地址：北京市海淀区西北旺东路 10 号院（中关村软件园）东区 20 号

邮政编码：100094

---


## 声 明

### Copyright ©2019

浪潮思科网络科技有限公司

版权所有，保留一切权利。

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

 是浪潮思科网络科技有限公司的注册商标。

对于本手册中出现的其它商标，由各自的所有人拥有。

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

# 前 言

## 概述

本手册介绍 SC9600 系列高端交换机各种功能特性的配置方法，从命令功能、命令形式、参数说明、命令视图、命令指导、使用实例、相关命令七个方面进行介绍，旨在帮助用户快速搜索并获取产品各功能特性的配置命令的相关信息。

本操作手册适用于以下高端交换机产品型号：

- SC9603
- SC9608
- SC9612

## 读者范围

本手册适用于以下人员：

- 工程技术人员
- 工程开通人员
- 设备维护人员
- 网络管理人员
- 对该产品有兴趣的其他人员

## 内容介绍

章名	概要
第 1 章 基础配置	本章介绍了 SC9600 高端交换机的基本配置，包括：登陆交换机、配置接口、配置系统文件以及基本用户配置。

章名	概要
第 2 章 二层以太网功能配置	本章介绍了 SC9600 二层以太基本功能配置，包括：链路聚合、VLAN 和 VLAN 转换。
第 3 章 IP 业务配置	本章针对 SC9600 高端交换机的 IP 业务，包括：IPv4 和 IPv6 地址配置。
第 4 章 三层 IP 路由功能配置	本章介绍了 SC9600 中路由由相关的基本内容、配置过程和配置举例，包括：OSPF，BGP 和路由策略。
第 5 章 QoS 配置	本章介绍了 SC9600 中 QoS 的基本内容、配置过程和配置举例，包括：队列调度和拥塞控制。
第 6 章 组播配置	本章介绍了 SC9600 高端交换机的组播相关配置，包括：IGMP Snooping 配置以及 MLD Snooping 配置。
第 7 章 安全配置	本章介绍了 SC9600 中安全性相关的基本内容、配置过程和配置举例，包括：IPv4 ACL 及 IPv6 ACL 两个方面的内容。
第 8 章 可靠性配置	本章介绍了 SC9600 中可靠性管理的基本内容、配置过程和配置举例，包括：MSTP、RLINK、BFD 和 VRRP。
第 9 章 设备管理配置	本章介绍了 SC9600 高端交换机的设备管理相关配置，包括：设备线卡及硬件配置，以及设备镜像配置。
第 10 章 运维管理配置	本章介绍了 SC9600 高端交换机的运维管理配置，包括：SNMP、LLDP 以及 RMON 配置。
第 11 章 VPN 配置	本章介绍了 SC9600 中 VPN 隧道管理的基本内容、配置过程和配置举例，包括：6RD 隧道配置。

## 版本更新说明

手册版本	手册编号	更新说明
V1.0	SC9600_ V300R001_V1.0	手册第一次发行
V2.0	SC9600_ V300R001_V2.0	手册第二次发行
V2.1	SC9600_ V300R001_V2.1	手册更新，新增模块： 端口隔离配置、VTP 配置、ARP 代理配置、静态路由配置、WRED 配置、IGMP 配置、MLD 配置、Time-range 配置、IP 地址前缀过滤表配置、URPF 配置、DHCP Snooping 配置、AAA/Radius 配置、802.1X 配置、MFF 配置、ESR 配置、VRRPv3 配置、EFM 配置、CFM 配置、Y.1731 配置、Flush 配置、系统补丁配置、日志管理配置、DDM 配置、MMU 管理配置、NTP 配置、SMTP 配置、Netflow 配置、CPU 调试配置、ISS 模块 BUG 修订。
V2.2	SC9600_ V300R001_V2.2	手册更新，新增 ISS 模块模块：BUG 修订。

## 约定

介绍通用格式、符号的约定、键盘操作约定、鼠标操作约定以及三类标志。

### 1、通用格式

格式	意义
宋体	正文中文采用宋体字体，英文和数字采用 Arial 字体
黑体	全文标题使用黑体字

### 2、符号约定

格式	意义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用加粗字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用斜体表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x   y   ... }	表示从多个选项中仅选取一个。
[ x   y   ... ]	表示从多个选项中选择一个或者不选。
{ x   y   ... }*	表示从多个选项中至少选取一个。
[ x   y   ... ]*	表示从多个选项中选择一个、多个或者不选。
#	由“#”号开始的行表示为注释行。

### 3、键盘操作约定

格式	意义
加尖括号的字符	表示键名、按钮名。如 <Enter>、<Tab>、<Backspace>、<a> 等分别表示回车、制表、退格、小写字母 a
<键 1+键 2>	表示在键盘上同时按下几个键。如 <Ctrl+Alt+A> 表示同时按下“Ctrl”、“Alt”、“A”这三个键
<键 1, 键 2>	表示先按第一键，释放，再按第二键。如 <Alt, F> 表示先按 <Alt> 键，释放后，紧接着再按 <F> 键

### 4、鼠标操作约定

格式	意义
单击	快速按下并释放鼠标的左键
双击	连续两次快速按下并释放鼠标的左键
右击	快速按下并释放鼠标的右键
拖动	按住鼠标的左键不放，移动鼠标

## 5、标志

本书采用三个醒目标志来表示在操作过程中应该特别注意的地方。



说明、



注意、



警告：提醒操作中应注意的事项。

---

# 目 录

---

第 1 章 基础配置.....	1-1
1.1 概述.....	1-1
1.2 登陆交换机.....	1-1
1.2.1 Console 口登录交换机.....	1-1
1.2.2 Telnet 方式登录交换机.....	1-4
1.3 配置接口.....	1-5
1.3.1 管理接口.....	1-5
1.3.2 物理接口.....	1-6
1.4 基本配置.....	1-6
1.4.1 设备管理配置.....	1-6
1.4.2 系统基本环境配置.....	1-10
1.4.3 显示系统基本信息.....	1-13
1.4.4 密码恢复.....	1-16
1.4.5 密码管理配置.....	1-17
1.4.6 配置用户界面.....	1-19
1.4.7 配置用户权限.....	1-24
1.4.8 带内带外网管配置.....	1-29
1.5 配置文件系统.....	1-30
1.5.1 目录操作.....	1-30
1.5.2 文件操作.....	1-31
1.5.3 系统配置文件.....	1-32
1.5.4 FTP 配置.....	1-33
1.5.5 TFTP 配置.....	1-37

<b>第 2 章 二层以太网配置</b> .....	<b>2-1</b>
2.1 概述 .....	2-1
2.2 以太网接口配置.....	2-1
2.2.1 以太网接口配置概述.....	2-1
2.2.2 以太网接口基本属性配置.....	2-2
2.2.3 以太网接口高级属性配置.....	2-8
2.3 MAC 表配置 .....	2-10
2.3.1 配置 MAC 地址表管理.....	2-11
2.3.2 设置 MAC 地址表项 .....	2-11
2.3.3 设置系统 MAC 地址老化时间 .....	2-12
2.3.4 显示二层 MAC 地址表项.....	2-12
2.4 ARP 配置 .....	2-13
2.4.1 手工添加/删除静态 ARP 映射项 .....	2-13
2.4.2 清除动态 ARP 表项 .....	2-14
2.4.3 查看 ARP 的信息 .....	2-14
2.4.4 配置动态 ARP 映射表项老化时间 .....	2-14
2.4.5 设置 ARP 调试使能开关.....	2-15
2.5 防攻击配置.....	2-15
2.5.1 Anti-attack 简介.....	2-15
2.5.2 Anti-attack 配置.....	2-18
2.5.3 Anti-attack 配置举例 .....	2-21
2.6 链路聚合配置.....	2-24
2.6.1 端口汇聚简介 .....	2-24
2.6.2 配置汇聚组功能 .....	2-25
2.6.3 维护及调试.....	2-27
2.6.4 汇聚端口典型举例 .....	2-28
2.7 VLAN 配置 .....	2-30
2.7.1 VLAN 概述 .....	2-30
2.7.2 创建 VLAN .....	2-30
2.7.3 配置基于接口的 VLAN .....	2-31
2.7.4 配置基于 MAC 地址的 VLAN .....	2-32



2.7.5 配置基于 IP 子网的 VLAN .....	2-33
2.7.6 配置基于协议的 VLAN .....	2-34
2.7.7 配置 VLAN 其他参数 .....	2-35
2.7.8 维护及调试 .....	2-38
2.7.9 配置举例 .....	2-39
2.8 VLAN 转换配置 .....	2-42
2.8.1 绑定 VLAN 转换条目到接口 .....	2-42
2.8.2 配置或删除 VLAN 转换条目 .....	2-43
2.8.3 查看 VLAN 转换条目相关信息 .....	2-44
2.8.4 配置举例 .....	2-45
2.9 QinQ 配置 .....	2-48
2.9.1 配置接口的双标签工作状态 .....	2-48
2.9.2 配置当前接口 TPID .....	2-48
2.10 PVLAN 配置 .....	2-49
2.10.1 PVLAN 简介 .....	2-49
2.10.2 PVLAN 配置 .....	2-51
2.10.3 配置举例 .....	2-56
2.11 Voice VLAN 配置 .....	2-58
2.11.1 Voice VLAN 概述 .....	2-58
2.11.2 配置 Voice VLAN 功能 .....	2-60
2.11.3 维护及调试 .....	2-62
2.11.4 配置举例 .....	2-63
2.12 环回检测配置 .....	2-65
2.12.1 环回检测概述 .....	2-65
2.12.2 配置环回检测功能 .....	2-66
2.12.3 维护及调试 .....	2-68
2.12.4 配置举例 .....	2-69
<b>第 3 章 IP 业务配置 .....</b>	<b>3-1</b>
3.1 概述 .....	3-1
3.2 IPv4 配置 .....	3-1
3.2.1 配置 IP 收发包调试功能 .....	3-1

3.2.2	配置带内/带外/环回 IP 地址.....	3-2
3.2.3	配置 VLANIF 接口的 IP 地址.....	3-2
3.2.4	配置 TCP 连接数目.....	3-3
3.2.5	查看 VLAN 接口配置信息.....	3-4
3.2.6	查看 TCP/UDP 的连接状态.....	3-4
3.2.7	查看 IP 相关的统计信息.....	3-4
3.2.8	查看系统 IP 接口的信息.....	3-5
3.2.9	配置举例.....	3-5
3.3	IPv6 配置.....	3-7
3.3.1	配置 IPv6 基本功能.....	3-7
3.3.2	配置 IPv6 其他功能.....	3-9
3.3.3	配置 IPv6 邻居发现功能.....	3-10
3.3.4	配置 IPv6 调试功能.....	3-15
3.3.5	查看 IPv6 配置信息.....	3-16
3.3.6	配置举例.....	3-16
3.4	DHCP 配置.....	3-17
3.4.1	DHCP 简介.....	3-17
3.4.2	DHCP 配置.....	3-24
3.4.3	配置举例.....	3-36
<b>第 4 章</b>	<b>三层 IP 路由配置.....</b>	<b>4-1</b>
4.1	概述.....	4-1
4.2	RIP 配置.....	4-1
4.2.1	RIP 简介.....	4-1
4.2.2	RIP 配置.....	4-6
4.2.3	配置举例.....	4-14
4.3	RIPng 配置.....	4-20
4.3.1	RIPng 概述.....	4-20
4.3.2	支持的 RIPng 特性.....	4-26
4.3.3	配置 RIPng 基本功能.....	4-26
4.3.4	配置 RIPng 路由信息的发布与接收.....	4-29
4.3.5	配置 RIPng 相关参数.....	4-31

4.3.6 维护及调试.....	4-32
4.3.7 配置举例.....	4-34
4.4 OSPF 配置.....	4-38
4.4.1 OSPF 简介.....	4-38
4.4.2 OSPF 配置.....	4-58
4.4.3 OSPF 配置举例.....	4-86
4.5 IPv6 OSPFv3 配置.....	4-101
4.5.1 OSPFv3 简介.....	4-101
4.5.2 OSPFv3 配置.....	4-113
4.5.3 OSPFv3 配置举例.....	4-133
4.6 BGP 配置.....	4-145
4.6.1 BGP 简介.....	4-145
4.6.2 BGP 配置.....	4-153
4.6.3 BGP 配置举例.....	4-168
4.7 ISIS 配置.....	4-186
4.7.1 ISIS 简介.....	4-186
4.7.2 ISIS 配置.....	4-193
4.7.3 ISIS 配置举例.....	4-207
4.8 路由策略配置.....	4-215
4.8.1 路由策略概述.....	4-215
4.8.2 配置地址前缀列表.....	4-216
4.8.3 配置 Route-Policy.....	4-218
4.8.4 对 OSPF 路由协议应用路由策略.....	4-220
4.8.5 对 BGP 路由协议应用路由策略.....	4-221
4.8.6 维护及调试.....	4-223
4.8.7 配置举例.....	4-224
<b>第 5 章 QoS 配置.....</b>	<b>5-1</b>
5.1 概述.....	5-1
5.2 Diffserv 配置.....	5-1
5.2.1 Diffserv 简介.....	5-1
5.2.2 Diffserv 配置.....	5-2

5.2.3 配置举例.....	5-8
5.3 流量监管和流量整形配置.....	5-12
5.4 队列调度和拥塞控制配置.....	5-14
5.4.1 队列调度和拥塞控制概述.....	5-14
5.4.2 配置队列调度及拥塞控制.....	5-16
5.4.3 维护及调试.....	5-18
5.4.4 配置举例.....	5-19
<b>第 6 章 组播配置.....</b>	<b>6-1</b>
6.1 概述.....	6-1
6.2 IGMP Snooping 配置.....	6-1
6.2.1 IGMP Snooping 简介.....	6-1
6.2.2 配置静态二层组播.....	6-3
6.2.3 配置组播 VLAN 复制.....	6-4
6.2.4 配置 IGMP Snooping.....	6-5
6.2.5 维护及调试.....	6-8
6.2.6 配置举例.....	6-10
6.3 MLD Snooping 配置.....	6-20
6.3.1 MLD Snooping 简介.....	6-20
6.3.2 MLD Snooping 配置.....	6-21
6.3.3 MLD Snooping 配置举例.....	6-27
<b>第 7 章 安全配置.....</b>	<b>7-1</b>
7.1 概述.....	7-1
7.2 ACL 配置.....	7-1
7.2.1 ACL 概述.....	7-1
7.2.2 配置二层 ACL.....	7-2
7.2.3 配置三层 ACL.....	7-5
7.2.4 配置混合 ACL.....	7-10
7.2.5 配置三层 ACL6.....	7-12
7.2.6 配置 ACL 可选功能项.....	7-15
7.2.7 维护及调试.....	7-19

7.2.8 配置举例.....	7-21
7.3 IP Source Guard 配置.....	7-27
7.3.1 IP Source Guard 简介.....	7-27
7.3.2 IP Source Guard 配置.....	7-30
7.3.3 IP Source Guard 配置举例.....	7-32
<b>第 8 章 可靠性配置.....</b>	<b>8-1</b>
8.1 概述.....	8-1
8.2 MSTP 配置.....	8-1
8.2.1 STP 简介.....	8-1
8.2.2 RSTP 简介.....	8-2
8.2.3 MSTP 简介.....	8-3
8.2.4 配置设备加入指定的 MST 域.....	8-9
8.2.5 配置 MSTP 参数.....	8-11
8.2.6 配置 MSTP 保护功能.....	8-14
8.2.7 维护及调试.....	8-17
8.2.8 配置举例.....	8-18
8.3 RLINK 配置.....	8-23
8.3.1 RLINK 概述.....	8-23
8.3.2 配置 Resilient Link 组功能.....	8-24
8.3.3 配置 Monitor Link 组功能.....	8-26
8.3.4 配置 RLINK 其他功能参数.....	8-27
8.3.5 维护及调试.....	8-29
8.3.6 配置举例.....	8-31
8.4 BFD 配置.....	8-38
8.4.1 BFD 概述.....	8-38
8.4.2 配置 BFD 检测功能.....	8-39
8.4.3 配置 BFD 检测参数.....	8-41
8.4.4 维护及调试.....	8-43
8.4.5 配置举例.....	8-44
8.5 VRRP.....	8-48
8.5.1 VRRP 概述.....	8-48

8.5.2	配置 VRRP 备份组 .....	8-50
8.5.3	配置 VRRP 认证方式 .....	8-51
8.5.4	配置 VRRP 参数 .....	8-52
8.5.5	配置 VRRP 监视 BFD 会话状态 .....	8-54
8.5.6	维护及调试 .....	8-55
8.5.7	配置举例 .....	8-56
8.6	G.8032 配置 .....	8-60
8.6.1	G.8032 概述 .....	8-60
8.6.2	G.8032 故障检测机制 .....	8-62
8.6.3	G.8032 单环保护倒换机制 .....	8-63
8.6.4	G.8032 多环单点故障保护倒换机制 .....	8-68
8.6.5	G.8032 相交环多点故障保护倒换机制 .....	8-70
8.6.6	配置 G.8032 基本功能 .....	8-72
8.6.7	配置 G.8032 定时器参数 .....	8-74
8.6.8	配置 G.8032 可选功能 .....	8-75
8.6.9	维护及调试 .....	8-77
8.6.10	配置举例 .....	8-78
8.7	ESR 配置 .....	8-83
8.7.1	ESR 概述 .....	8-83
8.7.2	配置 ESR 基本功能 .....	8-84
8.7.3	配置 ESR 定时器参数 .....	8-86
8.7.4	配置 ESR 其他参数 .....	8-88
8.7.5	维护及调试 .....	8-89
8.7.6	配置举例 .....	8-91
8.8	EFM 配置 .....	8-101
8.8.1	EFM 概述 .....	8-101
8.8.2	SC9600 支持的 EFM 特性 .....	8-102
8.8.3	配置 EFM 链路发现 .....	8-104
8.8.4	配置 EFM 远端环回 .....	8-106
8.8.5	配置 EFM 链路监控 .....	8-107
8.8.6	配置 EFM 链路故障通告 .....	8-110

8.8.7 维护及调试.....	8-111
8.8.8 配置举例.....	8-113
8.9 CFM 配置.....	8-114
8.9.1 CFM 基本概念.....	8-115
8.9.2 SC9600 支持的 CFM 特性.....	8-117
8.9.3 配置 CFM 基本功能.....	8-118
8.9.4 配置 CFM 相关参数.....	8-123
8.9.5 配置 CFM 故障确认.....	8-125
8.9.6 配置 CFM 故障定位.....	8-127
8.9.7 维护及调试.....	8-129
8.9.8 配置举例.....	8-133
8.10 Y.1731 配置.....	8-138
8.10.1 Y.1731 概述.....	8-138
8.10.2 Y.1731 故障管理实例基本概念.....	8-139
8.10.3 SC9600 支持的 Y.1731 特性.....	8-142
8.10.4 配置 Y.1731 基本功能.....	8-146
8.10.5 配置 Y.1731 相关参数.....	8-150
8.10.6 配置 Y.1731 故障确认.....	8-154
8.10.7 配置 Y.1731 故障定位.....	8-155
8.10.8 配置单向丢包率测试.....	8-157
8.10.9 配置双向时延/抖动测试.....	8-158
8.10.10 配置双向吞吐量测试.....	8-160
8.10.11 维护及调试.....	8-161
8.10.12 配置举例.....	8-164
<b>第 9 章 设备管理配置.....</b>	<b>9-1</b>
9.1 概述.....	9-1
9.2 设备线卡及硬件配置.....	9-1
9.2.1 硬件配置概述.....	9-1
9.2.2 配置接口板外扩 TCAM 的资源模式.....	9-1
9.2.3 配置设备 CPU.....	9-3
9.2.4 配置设备风扇.....	9-4

9.2.5	配置设备内存 .....	9-5
9.2.6	配置设备温度 .....	9-5
9.2.7	配置其他硬件参数 .....	9-6
9.2.8	配置线卡 MAC 地址学习的 Hash 算法 .....	9-7
9.2.9	配置线卡 IP 地址学习的 Hash 算法 .....	9-9
9.2.10	配置线卡复位 .....	9-10
9.2.11	配置主备倒换 .....	9-11
9.2.12	维护及调试 .....	9-11
9.3	镜像配置 .....	9-12
9.3.1	镜像概述 .....	9-12
9.3.2	镜像分类 .....	9-13
9.3.3	配置本地端口镜像 .....	9-13
9.3.4	配置远程端口镜像 .....	9-15
9.3.5	配置流镜像 .....	9-17
9.3.6	维护及调试 .....	9-20
9.3.7	配置举例 .....	9-21
9.4	系统补丁配置 .....	9-27
9.4.1	系统补丁概述 .....	9-27
9.4.2	加载单板补丁 .....	9-27
9.4.3	配置是否激活补丁 .....	9-28
9.4.4	配置运行补丁 .....	9-29
9.4.5	删除系统补丁 .....	9-30
9.4.6	配置恢复补丁 .....	9-30
9.5	日志管理配置 .....	9-31
9.5.1	日志管理简介 .....	9-31
9.5.2	配置日志管理 .....	9-31
9.6	DDM 配置 .....	9-34
9.6.1	DDM 概述 .....	9-34
9.6.2	配置 DDM 基本功能 .....	9-34
9.6.3	维护及调试 .....	9-37
9.7	MMU 管理配置 .....	9-38



9.7.1 设置 CPU 口的内存管理单元寄存器的值.....	9-38
9.7.2 显示内存管理单元寄存器值.....	9-38
<b>第 10 章 运维管理配置.....</b>	<b>10-1</b>
10.1 概述.....	10-1
10.2 SNMP 配置.....	10-1
10.2.1 SNMP 概述.....	10-1
10.2.2 配置 SNMP 维护信息.....	10-3
10.2.3 配置 SNMP 基本功能.....	10-3
10.2.4 配置发送 Trap 功能.....	10-6
10.2.5 维护及调试.....	10-8
10.2.6 配置举例.....	10-10
10.3 LLDP 配置.....	10-11
10.3.1 LLDP 概述.....	10-11
10.3.2 LLDP 工作机制.....	10-11
10.3.3 配置 LLDP 基本功能.....	10-14
10.3.4 配置 LLDP 参数.....	10-15
10.3.5 维护及调试.....	10-20
10.3.6 配置举例.....	10-22
10.4 RMON 配置.....	10-24
10.4.1 RMON 概述.....	10-24
10.4.2 配置统计表.....	10-26
10.4.3 配置历史控制表.....	10-27
10.4.4 配置告警表.....	10-28
10.4.5 配置事件表.....	10-29
10.4.6 维护及调试.....	10-29
10.4.7 配置举例.....	10-31
10.5 NTP 配置.....	10-32
10.5.1 NTP 概述.....	10-32
10.5.2 配置 NTP 基本功能.....	10-33
10.5.3 配置 NTP 安全机制.....	10-36
10.5.4 维护及调试.....	10-39

---

10.5.5 配置举例.....	10-40
10.6 SMTP 配置.....	10-41
10.6.1 SMTP 简介.....	10-41
10.6.2 配置 SMTP.....	10-41
10.7 CPU 调试配置.....	10-42
10.7.1 CPU 调试概述.....	10-42
10.7.2 维护及调试.....	10-42
10.8 ISS 堆叠配置.....	10-44
10.8.1 堆叠简介.....	10-44
10.8.2 配置堆叠.....	10-45
10.8.3 维护及调试.....	10-47
10.8.4 堆叠配置举例.....	10-49
<b>第 11 章 VPN 配置.....</b>	<b>11-1</b>
11.1 概述.....	11-1
11.2 L3VPN 配置.....	11-1
11.2.1 L3VPN 简介.....	11-1
11.2.2 L3VPN 配置.....	11-4
11.2.3 维护及调试.....	11-10
11.2.4 配置举例.....	11-12
11.3 VPN 隧道管理配置.....	11-14
11.3.1 IPv6 隧道管理配置.....	11-14

# 第1章 基础配置

## 1.1 概述

本章介绍了 SC9600 系列高端交换机基础配置操作。

本章包括如下主题：

内容	页码
1.1 概述	1-1
1.2 登陆交换机	1-1
1.3 配置接口	1-5
1.4 基本配置	1-6
1.5 配置文件系统	1-30

## 1.2 登陆交换机

### 1.2.1 Console 口登录交换机

#### 目的

本节介绍使用本地 PC 机使用 Console 串口登录 SC9600 高端交换机上的操作步骤。

#### 前提

用户在使用超级终端方式登录 SC9600 高端交换机之前，需要确认：

- 已经对 SC9600 高端交换机上传了 OS 和 FPGA 版本。

#### 组网环境

用户使用 Console 口登陆管理 SC9600 高端交换机时，需要使用一根串口线连接线卡上的[Console]口，如图 1-1所示。

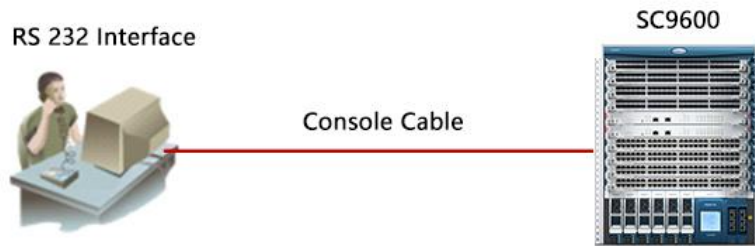


图 1-1 通过 Console 口登陆到 SC9600 高端交换机

## 过程

通过 Console 口登陆 SC9600 高端交换机的步骤如下。

1. 如图 1-1所示，使用一根串口线连接 PC 主机和 SC9600 高端交换机。
2. 在 PC 机上启动超级终端。选择菜单 [开始→程序→附件→通讯→超级终端]，弹出[连接描述]窗口。
3. 新建连接。

在[名称]输入框中输入需要创建连接的名称 SC9600 高端交换机。如图 1-2所示。



图 1-2 新建连接 SC9600 高端交换机

4. 设置连接端口。根据串口电缆的连接情况选择 COM1 或者 COM2 口。单击<确定>按钮，如图 1-3所示。

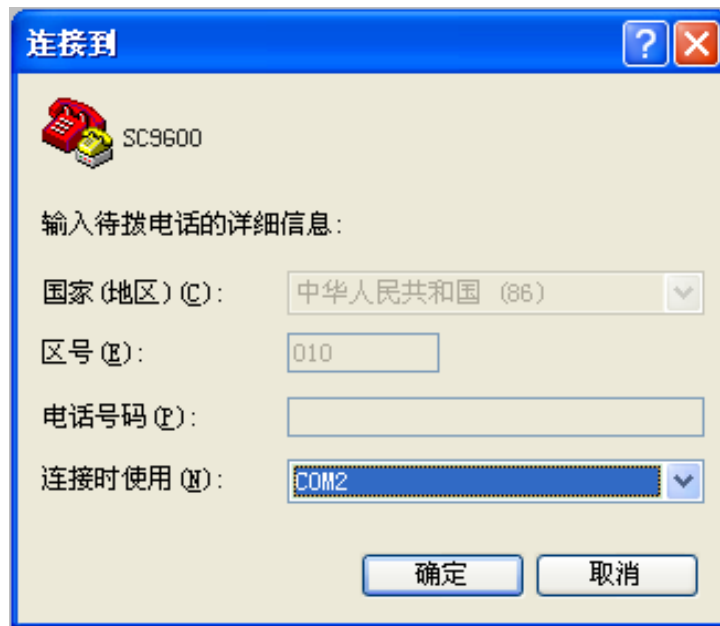


图 1-3 设置 SC9600 高端交换机连接端口

5. 设置串口属性。如图 1-4所示。

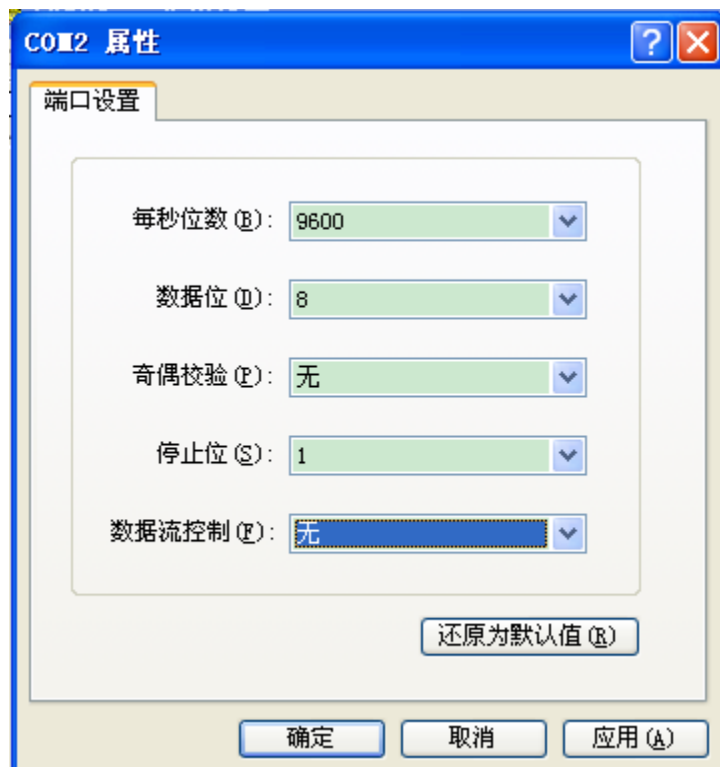


图 1-4 设置 SC9600 高端交换机串口属性

请按如表 1-1所示的参数进行设置。

表 1-1 串口登录 SC9600 高端交换机属性参数说明

参数	取值
每秒位数	9600
数据位	8
奇偶校验	无
停止位	1
数据流控制	无

6. 单击<确定>按钮。

#### 结果

按照以上步骤结束设置后，如果线卡运行正常，超级登陆终端会显示开机界面，表示登录到 SC9600 高端交换机。

## 1.2.2 Telnet 方式登录交换机

#### 目的

除了超级终端之外，登陆 SC9600 高端交换机也可以利用 Telnet 方式登录。SC9600 高端交换机本身提供的串口仅供日常版本上传、升级和维护使用。

本节介绍使用本地 PC 机使用 Telnet 方式登录 SC9600 高端交换机上的操作步骤。

Telnet 支持本地和远程用户登录，易于维护。

#### 前提

用户在使用 Telnet 方式登录 SC9600 高端交换机之前，需要确认：

- 本地 PC 机能 ping 通 SC9600 高端交换机。

#### 组网环境

用户使用 telnet 方式登录交叉汇聚网管线卡时，需要使用网线直连或通过 Hub 连接，如图 1-5所示。

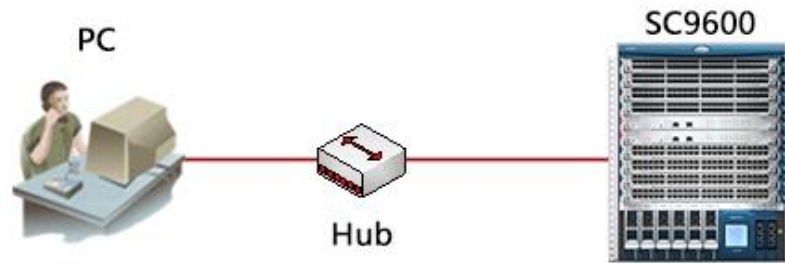


图 1-5 Telnet 方式登陆到 SC9600 高端交换机

使用 Telnet 登陆方式后，需要配置 SC9600 高端交换机 Telnet 用户，设置用户名和密码。

### 过程

通过 Telnet 方式登陆交叉汇聚网管线卡的步骤如下。

1. 输入用户名和密码（DMU 交叉汇聚网管线卡的初始用户名为 **admin**，密码为 **12345**），登录 SC9600 高端交换机。
2. 配置本线卡的 IP 地址。以供 Telnet 用户访问。
3. 在 Windows 环境下，选择[开始→运行]。

在[运行]列表框中输入命令 **Telnet x.x.x.x**。其中[x.x.x.x]为高端交换机的 IP 地址。

4. 单击<确定>按钮，启动 Telnet 客户端。如果网络连接正常，会弹出登陆界面。
5. 输入用户名和密码（DMU 交叉汇聚网管线卡的初始用户名为 **admin**，密码为 **12345**）后，系统进入配置模式。

## 1.3 配置接口

接口是 SC9600 高端交换机提供给用户操作或配置的单元，主要用于接收和发送数据。

接口从功能上可以划分为管理接口和业务接口，从物理形态上可以划分为物理接口和逻辑接口。

### 1.3.1 管理接口

#### 背景知识

管理接口，是一种人为的划分，主要是相对于业务接口而言的。管理接口主要为用户提供配置管理支持，也就是用户通过此类接口可以登录到 SC9600 高端交换机，并进行配置和管理操作。管理接口不承担业务传输。

### 操作步骤

SC9600 高端交换机提供 Console、ETH 两种管理接口。

接口名称	接口描述	接口用途
Console 口	遵循 EIA/TIA-232 标准，接口类型是 DCE。	该接口和配置终端的 COM 串口连接，用于搭建现场配置环境。
ETH 口	遵循 10/100BASE-TX 标准。	该接口和配置终端或网管站的网口连接，用于搭建现场或远程配置环境。

## 1.3.2 物理接口

### 背景知识

物理接口是实际存在的接口。物理接口分布在 SC9600 高端交换机的交换主控板和线路板上。

物理接口包括各管理接口和各业务接口。

### 操作步骤

SC9600 高端交换机目前支持物理接口包括：

- Console 口
- ETH 口
- 百兆以太网 FE (Fast Ethernet) 接口
- 千兆以太网 GE (Gigabit Ethernet) 接口
- 万兆以太网 10GE 接口

## 1.4 基本配置

### 1.4.1 设备管理配置

设备管理的配置任务主要是对交换机的单板状态、CPU、内存使用状态进行显示。

设备管理的配置任务包括：

- 复位交换机



- 升级系统或配置文件
- 设备管理的显示和调试
- 日志配置命令

#### 1.4.1.1 配置用户管理调试开关

##### 目的

本节介绍用户如何配置管理调试开关。

##### 过程

- 打开用户管理的调试开关的步骤：在特权用户模式下执行命令 `debug user`。
- 关闭用户管理的调试开关的步骤：在特权用户模式下执行命令 `no debug user`。

#### 1.4.1.2 复位交换机

##### 目的

当交换机出现故障需要重启的时候可以通过以下命令来复位—`reboot`。该命令的功能与冷启动的效果相同，但在设备的远程维护时，不需要用户到设备所在地重启，而直接在远地就可以重启设备。在一般情况下，禁止使用该命令，因为它导致网络工作在短时间内瘫痪，另外在重启设备时，要确认配置文件是否需要保存请在用户视图下进行下列配置。

##### 过程

复位交换机的步骤如下。

1. 在特权用户模式下执行命令 `Reboot`。
2. 执行命令 `y`。交换机进行复位操作。

#### 1.4.1.3 更新系统或配置文件

##### 目的

`upgrade (os|config)`: 升级系统文件或配置文件。在使用该命令之前要先用 `ftp` 命令把所要升级的文件 `download` 到设备中。该命令应在技术人员的指导下进行。

##### 过程

更新系统或配置文件的步骤如下：

1. 执行命令 `configure`，进入全局配置视图。

2. 执行命令 `upgrade {config|os}`。

#### 1.4.1.4 日志配置命令

##### 目的

如果用户想让系统记录日志则可以利用该命令，想取消记录系统日志功能则可以利用其 `no` 形式。为了跟踪系统的运行状况及当前系统的状态可以打开系统日志记录功能，使之自动记录系统的状态，从而可以掌握系统的运行状况进行相应的操作。该日志文件可以连续记录 2000 条记录，当记录超出 2000 条时，自动删除日期最久的记录。所以为了使系统不丢失记录，用户需要定期的把日志文件导出。

##### 操作步骤

日志配置命令如表 1-2 所示。

表 1-2 日志配置命令

目的	操作步骤	说明
打开系统日志功能	<code>Logging on</code>	
清除系统日志	<code>Clear logging history</code>	
打开记录功能	<code>Logging history[ etransmi&lt;0-7&gt;]</code>	
查看系统日志文件	<code>Show logging history[parameter substring]</code>	SUBSTRING : (可选项) 用于查找日志的关键词
打开告警记录功能	<code>Logging terminal[parameter&lt;0-7&gt;]</code>	
查看系统日志配置情况	<code>Show logging</code>	
配置历史日志记录的动作	<code>command-history action</code>	-
将系统产生的日志以自命名的文件形式存储在设备 Flash 上	<code>logging buf2file</code>	-
配置系统日志信息能以邮件形式发送到邮件服务器	<code>logging smtp</code>	-
配置系统日志信息能输出到 syslog 服务器	<code>logging syslog</code>	-
显示 syslog 服务器配置文件信息	<code>show syslog config</code>	-
配置 syslog 服务器	<code>syslog server</code>	-

目的	操作步骤	说明
手动添加日志内容	<b>write log log-buffer [ level ]</b>	-

### 1.4.1.5 配置访问控制列表

#### 目的

本节介绍如何配置访问控制列表。

#### 过程

如何配置访问控制列表的过程如下：

1. 执行命令 `configure`，进入全局配置视图。
2. 执行如下命令：
  - `management acl { enable | disable }`
  - `management acl ipv4-address [ipv4-address]`
  - `management acl ipv4-address/M { telnet| web | snmp | ssh | ftp | all }`
  - `management acl6 ipv6-address/M`
  - `management acl6 ipv6-address/M { telnet| web | snmp | ssh | ftp | all }`
  - `no management acl ipv4-address/M`
  - `no management acl6 ipv6-address/M`

#### 参数说明

参数	说明	取值
enable	使能 ACL 用户访问控制开关	-
disable	去使能 ACL 用户访问控制开关	-
ipv4-address	用户主机访问 ipv4 地址 或者一个网段地址	点分十进制,如 IPv4:A.B.C.D IPv6: X:X::X:X
ipv6-address	用户主机访问 ipv6 地址 或者一个网段地址	点分十进制,如 IPv4:A.B.C.D IPv6: X:X::X:X
M	掩码位数	整数形式,对于 IPv4,取值范围是 1-32; 对于 IPv6,取值范围为 1~128。
telnet web snmp ssh ftp all	配置关于 telnet、web、snmp、ssh、ftp 或者以上所有的访问列表	-

## 1.4.2 系统基本环境配置

系统基本配置和管理包括：

- 设置交换机的名称
- 设置系统时钟

### 1.4.2.1 配置交换机的系统名

#### 目的

本节介绍如何设置交换机的系统名。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	过程	参数说明
设置交换机的系统名	1. 执行命令 <code>configure</code> ，进入全局配置视图。 2. 执行命令 <code>hostname sys-name</code> 。	-
恢复交换机系统名的缺省值	1. 执行命令 <code>configure</code> ，进入全局配置视图。 2. 执行命令 <code>no hostname</code> 。	-

### 1.4.2.2 配置系统时钟

#### 目的

本节介绍如何设置系统时钟。

#### 过程

设置系统时钟的步骤如下：

在特权用户模式视图下执行命令 `clock set HH:MM:SS YY/MM/DD`。

### 1.4.2.3 夏令时设置

#### 目的

本节介绍如何设置和取消夏令时的名称和生效起始、终止时间。

#### 过程

设置夏令时的步骤如下：

- `clock summer-time summer-time-name date start-hour start-minutes start-day start-month start-year end-hour end-minutes end-day end-month end-year`

- **clock summer-time** *summer-time-name* **date** *start-hour start-minutes start-year/start-month/start-day end-hour end-minutes end-year/end-month / end-day*
- **clock summer-time** *summer-time-name* **recurring** { **first** | **second** | **third** | **fourth** | **fifth** | **last** } { **monday** | **tuesday** | **wednesday** | **thursday** | **friday** | **saturday** | **sunday** } { **january** | **february** | **march** | **april** | **may** | **june** | **july** | **august** | **september** | **october** | **november** | **december** } *start-hour start-minutes* { **first** | **second** | **third** | **fourth** | **fifth** | **last** } { **monday** | **tuesday** | **wednesday** | **thursday** | **friday** | **saturday** | **sunday** } { **january** | **february** | **march** | **april** | **may** | **june** | **july** | **august** | **september** | **october** | **november** | **december** } *end-hour end-minutes*

取消夏令时设置的步骤如下：

- **no clock summer-time**

参数说明如下：

参数	说明	取值
<i>summer-time-name</i>	指定夏令时区名称	字符串形式，取值范围是 1~32 个字符
<i>Date</i>	指定绝对夏令时	-
<i>Recurring</i>	指定周期夏令时	-
<i>start-hour</i>	指定起始小时	整数形式，取值范围是 0~23
<i>start-minutes</i>	指定起始分钟	整数形式，取值范围是 0~59
<i>start-day</i>	指定起始日期	整数形式，取值范围是 1~31
<i>start-month</i>	指定起始月份	整数形式，取值范围是 1~12
<i>start-year</i>	指定起始年份	整数形式，取值范围是 2001~2099
<i>end-hour</i>	指定结束小时	整数形式，取值范围是 0~23
<i>end-minutes</i>	指定结束分钟	整数形式，取值范围是 0~59
<i>end-day</i>	指定结束日期	整数形式，取值范围是 1~31
<i>end-month</i>	指定结束月份	整数形式，取值范围是 1~12
<i>end-year</i>	指定结束年份	整数形式，取值范围是 2001~2099
{ <b>first</b>   <b>second</b>   <b>third</b>   <b>fourth</b>   <b>fifth</b>   <b>last</b> }	指定月份中起始或结束的第一个工作日/第二个工作日/第三个工作日/第四个工作日/第五个工作日/最后一个工作日	-

#### 1.4.2.4 设置本地时区信息

##### 目的

本节介绍如何设置本地时区信息。

### 过程

设置本地时区信息的步骤：在特权用户模式视图下执行命令 `clock timezone time-zone-name { add | minus } offset`。

参数说明如下：

参数	说明	取值
time-zone-name	指定时区名称	字符串形式，取值范围是 1~10 个字符
Add	与通用协调时间 UTC 相比， <i>time-zone-name</i> 增加的时间偏移量。即，在系统默认的 UTC 时区的基础上，加上 <i>offset</i> ，就可以得到 <i>time-zone-name</i> 所标识的时区时间	-
Minus	与 UTC 时间相比， <i>time-zone-name</i> 减少的时间偏移量。即，在系统默认的 UTC 时区的基础上，减去 <i>offset</i> ，就可以得到 <i>time-zone-name</i> 所标识的时区时间	-
Offset	指定与 UTC 的时间差	形如 HH:MM，其中 H 表示小时，取值范围是 0~12，M 表示分钟，取值范围是 0~59

#### 1.4.2.5 配置 ping 请求包最大个数

### 目的

本节介绍如何配置 ping 请求包最大个。

### 过程

配置 ping 请求包最大个的步骤如下。

在全局配置视图下，执行命令 `ping max-request max-number`。

### 参数说明

参数	说明	取值
max-number	指定 traceroute 最大请求个数	整数形式，取值范围是 0~1000

### 1.4.3 显示系统基本信息

#### 1.4.3.1 显示和调试设备管理运行信息

##### 目的

在任意视图下执行 `show` 命令可以查看配置后设备管理的运行情况，通过查看显示信息验证配置的效果。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
显示当前 CPU 利用率	执行命令 <code>show cpu statistic</code>	-
显示当前内存利用率	执行命令 <code>show memory statistic</code>	-
显示当前的配置	执行命令 <code>show running-config</code>	-

#### 1.4.3.2 显示当前配置视图下的所有可用命令

##### 目的

本节介绍如何查看当前配置视图下的所有可用命令。

##### 过程

查看当前配置视图下的所有可用命令步骤如下。

在所有配置视图下，执行命令 `list`。

#### 1.4.3.3 显示设备硬件时钟

##### 目的

本节介绍如何显示设备硬件时钟。

##### 过程

显示设备硬件时钟的步骤如下。

在普通用户视图、特权用户视图或者全局配置视图下，执行命令 `show hwclock`。

#### 1.4.3.4 显示系统当前 CPU 的利用率

##### 目的

本节介绍如何显示系统当前 CPU 的利用率。

##### 过程

系统当前 CPU 的利用率的步骤如下。

在特权用户视图下，执行命令 `show cpu statistic`。

#### 1.4.3.5 显示用户所用过的历史命令

##### 目的

本节介绍用户如何显示用户所用过的历史命令。

##### 过程

显示用户所用过的历史命令步骤如下。

在普通用户视图、特权用户视图或者全局配置视图下，执行命令 `show history`。

#### 1.4.3.6 显示系统当前的软硬件信息

##### 目的

本节介绍用户如何显示系统当前的软硬件版本号、编译时间等信息。

##### 过程

显示系统当前的软硬件版本号、编译时间等信息的步骤如下。

在普通用户视图、特权用户视图或者全局配置视图下，执行命令 `show version`。

#### 1.4.3.7 显示 traceroute 最大请求包个数

##### 目的

本节介绍用户如何显示 traceroute 最大请求包个数。

##### 过程

显示 traceroute 最大请求包个数的步骤如下。

在特权用户视图和全局配置视图下，执行命令 `show traceroute max-request`。

#### 1.4.3.8 查看当前 telnet 用户的个数

##### 目的

本节介绍用户如何查看当前 telnet 用户的个数。

##### 过程

查看当前 telnet 用户的个数的步骤如下。

在特权用户视图下，执行命令 `show login-type count`。



### 1.4.3.9 显示系统中所有的 ping 信息

#### 目的

本节介绍用户如何显示系统中所有的 ping 信息。

#### 过程

显示系统中所有的 ping 信息的步骤如下。

在特权用户视图下, 执行命令 **show ping information slot slot-id destIP-address vlan vlan-id**。

#### 参数说明

参数	说明	取值
slot-id	指定槽位号	SC9600 系列交换机支持以下 3 种型号的槽位配置范围： SC9603: 取值范围是<1-3> SC9608: 取值范围是<1-8> SC9612: 取值范围是<1-12>
destIP-address	指定目的设备的 IP 地址	点分十进制
vlan-id	VLAN	整数形式, 取值范围 1~4094

### 1.4.3.10 显示系统支持的最大 ping 请求个数

#### 目的

本节介绍用户如何显示系统支持的最大 ping 请求个数。

#### 过程

显示系统支持的最大 ping 条数的步骤如下。

在特权用户视图或者全局配置视图下, 执行命令 **show ping max-request**。

### 1.4.3.11 查看 SC9600 的电源状态

#### 目的

本节介绍用户如何查看 SC9600 的电源状态。

#### 过程

查看 SC9600 的电源状态的步骤如下。

在特权用户视图、全局配置视图或者普通用户视图下, 执行命令 **show power**。

#### 1.4.3.12 查看 MAC 地址信息

##### 目的

本节介绍用户如何查看 SC9600 的默认 MAC 地址信息和正在使用的 MAC 地址信息。

##### 过程

SC9600 的默认 MAC 地址信息和正在使用的 MAC 地址信息的步骤如下。

在特权用户视图、全局配置视图或者普通用户视图下，执行命令 `show system`。

#### 1.4.3.13 查看访问控制列表的配置信息

##### 目的

本节介绍用户如何查看访问控制列表的配置信息。

##### 过程

查看访问控制列表的配置信息的步骤如下。

在全局配置视图下，执行命令 `show management acl`。

#### 1.4.4 密码恢复

##### 目的

当用户忘记密码时，可以通过本节介绍步骤完成密码恢复。

##### 过程

密码恢复的步骤如下：

1. 通过串口进入命令行操作界面，在输入用户名时输入小键盘的↑键或者 `ctrl+p`，进入 `key` 节点。
2. 执行命令 `get temporary-serial` 系统会自动生成一串随机码，按照提示的途径将随机码发送给交换机本系统。系统将根据随机码生成一个临时密码给用户。

用户得到临时密码后按照前面的步骤进入 `key` 节点，执行命令 `check temporary-password PWD`（PWD 为用户得到的临时密码）进入系统，然后对用户名和密码进行修改。

### 1.4.5 密码管理配置

SC9600 系列高端交换机能够向用户提供密码管理功能。在登录 SC9600 系列高端交换机之前需要先配置系统的登录密码，配置密码之后每次登录交换机都要先输入密码，系统认证通过后才允许用户登录交换机进行后续操作。对于密码验证失败的用户则无法登录成功。用户可以使用缺省的密码配置，也可以自行进行密码管理配置，自行进行密码管理的时候遵循以下步骤：

- 首先用户可用缺省的用户名，密码以管理员的权限登陆系统，登陆系统成功后可增加用户名，权限和密码。系统会将配置好的用户名，权限和密码自动加入到用户表里面
- 当用户进入系统需要输入密码验证身份时，系统对密码加以保护。命令行将不会显示输入的密码。在系统的配置文件或者终端上，均不能显示该密码的明文，必须以加密方式存储。当用户输入密码时，终端上采用显示\*\*\*\*\*的方式，没有用户密码的明文显示。密码配置时，命令行显示为\*\*\*\*\*，配置文件中显示为密文。

#### 1.4.5.1 分配用户权限

##### 目的

本节介绍了登陆 SC9600 后，增加用户名及其权限和密码。

SC9600 对登录用户划分为 4 种类等级，如表 1-3 所示。隶属于 Administrator 组中的用户才有权限新增用户。

表 1-3 SC9600 支持的用户类型

用户类型	描述
Administrators	级别最高，可执行任何命令。其中一些对设备影响很大的关键命令、重要操作强制要求具有此权限，如用户管理、ftp 操作、清除历史记录、减少终端个数、升级镜像和配置文件、启动/停止 ftp/telnet 功能等等。
operators	operators 级别比 administrators 稍低，拥有除 administrators 关键操作和重要强制命令外的所有命令权限。
Users	users 级别比 operator 稍低，拥有除 upgrade, tftp, snmp, sgm 等命令以外的所有命令权限。
guests	guests 级别最低，除了查看及少量配置功能外：如 ping、debug 系列命令等，没有任何执行和配置权限。需要注意的是 guests 无法查询到有一些比较重要的显示信息，如 show logging 系列命令、show running-config、show snmp config、show startup-config、show user config 等。

不同级别的用户登录后，只能使用等于或低于自己级别的命令。为了保密，用户在屏幕上看不到所键入的口令，如果三次以内输入正确的口令，则切换到高级别用户，否则保持原用户级别不变。

### 操作

根据不同目的，执行相应步骤，具体参见下表。

目的	过程	参数说明
增加用户名及其权限和密码	1. 执行命令 <code>configure</code> 进入全局配置视图。 2. 执行命令 <code>username username group { administrators   operators   users   guests } password password</code>	WORD 表示用户名，PASSWORD 表示配置的密码，[ ] 的内容表示可缺省，当缺省时用户权限为 users。
删除用户名及其权限和密码	1. 执行命令 <code>configure</code> 进入全局配置视图。 2. 执行命令 <code>no username username</code>	
修改当前登陆用户的密码	1. 执行命令 <code>configure</code> 进入全局配置视图。 2. 执行命令 <code>password password</code>	

#### 1.4.5.2 用户权限配置举例

### 组网需求

一台 PC 同一台 SC9600 交换机相连。用户可采用缺省配置，也可以根据各自实际要求自行配置密码参数。

### 组网图

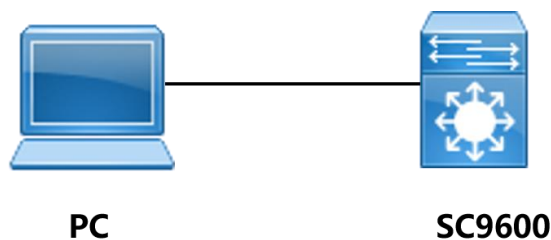


图 1-7 用户连接示意图

### 配置步骤

用缺省的用户名和密码登录系统，进入全局配置视图，增加一个用户名为 123，权限为 administrator，密码为 123 的缺省用户。

配置步骤如下。

```
SC9600#config
SC9600(config)#username 123 group administrator password 123
```

```
#退出登录
SC9600(config)#quit
SC9600#quit
#用前面配置的用户名 123，密码 123 可以登录成功
Uername: 123
Password: 123
SC9600#
```

### 1.4.6 配置用户界面

用户界面的配置主要包括：

- 用户进入或取消终端配置
- 配置终端显示的行的数目
- 配置终端显示的颜色
- 配置终端显示的语言
- 设置虚拟终端是否接收 debug 信息
- 设置虚拟终端的的登录方式
- 设置虚拟终端的超时时间

#### 1.4.6.1 设置终端接收调试信息的功能开关

##### 目的

本节介绍用户如何打开或者关闭命令行终端接收调试信息的功能。

##### 过程

配置命令行终端是否区分大小写的步骤如下。

在 line 配置视图下，执行命令 `monitor` 或者 `no monitor`。

#### 1.4.6.2 用户进入或取消终端配置

##### 目的

本节介绍用户如何进入或取消终端配置。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	过程	参数说明
----	----	------

目的	过程	参数说明
进入终端配置模式	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code>，进入全局配置视图。</li> <li>2. 执行命令 <code>line vty &lt;1-32&gt; [&lt;1-32&gt;]</code></li> </ol>	<1-32>: 要配置的起始终端号 <1-32>: 要配置的结束终端号，配置值需大于（或等于）起始终端号如果省略就只配置起始终端号
取消终端配置	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code>，进入全局配置视图。</li> <li>2. 执行命令 <code>no line vty &lt;1-32&gt; [&lt;1-32&gt;]</code></li> </ol>	

### 1.4.6.3 进入串口终端配置视图

#### 目的

本节介绍用户如何进入串口终端配置视图。

#### 过程

配置如何进入串口终端配置视图的步骤如下。

在全局配置视图或者 `line` 配置视图下，执行命令 `line console number`。

#### 参数说明

参数	说明	取值
<code>number</code>	指定要配置的串口终端号	整数形式，取值范围是 1~1

### 1.4.6.4 关闭一个虚终端

#### 目的

本节介绍用户如何关闭一个虚终端（即 `telnet` 和 `ssh` 连接终端）连接并重设该终端。

`vtty` 终端号包括 `telnet` 和 `ssh` 连接终端。

设备默认存在 5 个虚拟终端，即同一时刻允许 5 个用户同时 `Telnet` 登陆设备。

#### 过程

配置如何关闭一个虚终端的步骤如下。

在全局配置视图或者 `line` 配置视图下，执行命令 `kill vty vty-number`。

#### 参数说明

参数	说明	取值
<code>vty number</code>	配置单个虚终端的终端号	整数取值，取值范围是 1~32

### 1.4.6.5 配置命令行终端是否区分大小写

#### 目的

本节介绍用户如何配置命令行终端是否区分大小写。

#### 过程

配置命令行终端是否区分大小写的步骤如下。

在全局配置视图下，执行命令 `case-sensitive { enable | disable }`。

### 1.4.6.6 配置终端显示命令行的行数

#### 目的

本节介绍用户如何配置终端显示行的数目。

当用户使用终端显示命令行的行数时，用户可以根据自己的需要来配置当前终端显示的具体行数。当配置为 0 时则取消分屏显示功能

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	过程	参数说明
配置终端显示行的数目	在普通视图或者特权视图下执行命令 <code>terminal length terminal-length</code>	<code>terminal-length</code> 屏幕分屏显示的行数 整数形式，
恢复缺省值	在普通视图或者特权视图下执行命令 <code>no terminal length</code>	取值范围是 0~512 缺省的配置是 25 行

### 1.4.6.7 配置终端显示的颜色

#### 目的

本节介绍用户如设置虚拟终端的背景显示颜色，包括灰色、红色、绿色、黄色、蓝色、紫色、水色和白色。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	过程	参数说明
配置终端显示的颜色	在特权配置视图下执行命令 <code>terminal color { gray   red   green   yellow   blue   purple   water   white }</code>	-

### 1.4.6.8 配置终端显示的语言

#### 目的

本节介绍用户如何配置终端显示的语言。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	过程	参数说明
配置终端显示的语言	1. 执行命令 <code>configure</code> ，进入全局配置视图。 2. 执行命令 <code>line concole/ vty</code> 。 3. 执行命令 <code>language &lt;Chinese/English&gt;</code>	-

#### 1.4.6.9 配置虚拟终端是否接收 debug 信息

目的

本节介绍用户如何配置设置调试信息是否在屏幕上打印出来。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	过程	参数说明
设置虚拟终端是否接收 debug 信息	在特权配置视图下执行命令 <code>terminal monitor</code>	串口缺省为接收，telnet 为不接收
恢复缺省值	在特权配置视图下执行命令 <code>no terminal monitor</code>	当使用 <code>debug</code> 命令进行调试时要把 <code>debug</code> 信息输出到终端上可以利用此命令。利用此命令时先要利用 <code>logging history</code> 命令把优先级设为 <code>debug</code>

#### 1.4.6.10 配置虚拟终端的登录方式

目的

本节介绍用户如何配置虚拟终端的登录方式。

过程

在全局配置视图、line 配置视图下执行命令 `line vty vty-number` 或者 `line vty vty-number1 vty-number2`。

参数说明

参数	说明	取值
<code>vty number</code>	配置单个虚终端的终端号	整数取值，取值范围是 1~32
<code>vty-number1</code>	配置多个虚终端，要配置的起始终端号	整数取值，取值范围是 1~32
<code>vty-number2</code>	配置多个虚终端，要配置的结束终端号	整数取值，取值范围是 1~32

#### 1.4.6.11 设置虚拟终端的超时时间

目的



本节介绍用户如何设置虚拟终端的超时时间。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	过程	参数说明
设置虚拟终端的超时时间	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code> 进入全局配置视图。</li> <li>2. 执行命令 <code>line concole/ vty</code>。</li> <li>3. 执行命令 <code>timeout &lt;0-35791&gt;[&lt;0-59&gt;]</code></li> </ol>	<0-35791>:超时时间，单位：分 <0-59>超时时间，单位：秒
恢复缺省值	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code> 进入全局配置视图。</li> <li>2. 执行命令 <code>line concole/ vty</code>。</li> <li>3. 执行命令 <code>no timeout</code></li> </ol>	

#### 1.4.6.12 设置虚拟终端的无输入的超时时间

### 目的

本节介绍用户如何设置虚拟终端的无输入的超时时间。

### 过程

设置虚拟终端的无输入的超时时间的步骤如下。

在特权用户视图、全局配置视图、普通用户视图下，执行命令 **terminal timeout time**。

恢复虚拟终端无输入超时时间为缺省值为 600 秒的步骤如下。

在特权用户视图、全局配置视图、普通用户视图下，执行命令 **no terminal timeout**。

### 参数说明

参数	说明	取值
time	超时时间（单位为分钟）	整数，取值范围是 0-35791。
缺省值	缺省情况下，虚拟终端无输入超时时间为 600 秒。	600 秒

#### 1.4.6.13 显示当前设备登录用户信息

### 目的

本节介绍用户如何显示当前设备允许多少用户登录以及已登录用户的相关信息。

### 过程

显示当前设备登录用户信息的步骤如下。

在特权用户视图、全局配置视图、普通用户视图下，执行命令 **show lines**。

## 1.4.7 配置用户权限

本节介绍了登陆 SC9600 后，如何管理和分配用户权限。

### 1.4.7.1 新增用户

#### 目的

本节介绍了登陆 SC9600 后，如何新增用户。

SC9600 对登录用户划分为 4 种类等级，如表 1-4 所示。隶属于 Administrator 组中的用户才有权新增用户。

表 1-4 SC9600 支持的用户类型

用户类型	描述
Administrators	管理级：关系到系统基本运行的所有命令。还包括系统支撑模块的命令，这些命令对业务提供支撑作用，包括文件系统、FTP、TFTP、下载、用户管理命令、级别设置命令等。
operators	系统级：业务配置命令，包括路由、各个网络层次的命令，这些用于向用户提供直接网络服务。
users	监控级：用于系统维护、业务故障诊断等，包括 debug 命令。
guests	访问级：该级别包含的命令有网络诊断工具命令(如：ping 等)、用户界面的语言模式切换命令 (language-mode) 以及 telnet 命令，该级别命令不允许进行配置文件保存的目的。

不同级别的用户登录后，只能使用等于或低于自己级别的命令。为了保密，用户在屏幕上看不到所键入的口令，如果三次以内输入正确的口令，则切换到高级别用户，否则保持原用户级别不变。

#### 过程

增加用户的步骤如下。

在全局配置视图下执行命令 `username username group { administrators | operators | users | guests }`。

#### 参数说明

参数	说明	取值
username	指定待修改权限的用户名	字符串形式
administrators	指定优先级为管理级别	-
operators	指定优先级为操作级别	-
users	指定优先级为用户级别	-
guests	指定优先级为访问级别	-

#### 1.4.7.2 删除用户

##### 目的

本节介绍了在 SC9600 新增用户后，如果需要删除用户的操作。

隶属于 Administrator 组中的用户才有权限删除用户信息。

##### 过程

删除用户的步骤如下。

在全局配置视图下执行命令 `no username username`

#### 1.4.7.3 查看已创建的本地用户的属性

##### 目的

本节介绍了如何查看已创建的本地用户的属性。

##### 过程

查看已创建的本地用户的属性的步骤如下。

在特权用户视图下，执行命令 `show user config` 或者 `show user config name`。

##### 参数说明

参数	说明	取值
name	本地用户名	字符串形式，不支持空格，不区分大小写

#### 1.4.7.4 查看当前在线用户的个数

##### 目的

本节介绍了如何查看当前在线用户的个数。

##### 过程

查看当前在线用户的个数的步骤如下。

在特权用户视图下，执行命令 `show login-user count`。

#### 1.4.7.5 配置不同的域实现管理用户的登陆权限

##### 目的

本节介绍了如何配置不同的域实现管理用户的登陆权限。

##### 过程

配置不同的域实现管理用户的登陆权限的步骤如下。

在全局配置视图下，执行命令 **username username domain { telnet | ftp | ssh | http | console }**

**参数说明**

参数	说明	取值
username	指定待操作的用户名	字符串形式
telnet	支持 telnet 登陆	-
ftp	支持 ftp	-
ssh	支持 SSH 登陆	-
console	支持串口登陆	-

**1.4.7.6 提升用户权限**

**目的**

本节介绍了如何提升用户权限。

**过程**

根据不同目的，执行相应步骤，具体参见下表。

目的	过程	参数说明
提升用户的权限	1. 执行命令 <code>configure</code> ，进入全局配置视图。 2. 执行命令 <code>user privilege level { administrators   operators   users   guests } password PASSWORD</code>	
还原提升权限的密码为默认值	执行命令 <code>no user privilege level { administrators   operators   users   guests } password PASSWORD</code>	

**参数说明**

参数	说明	取值
administrators	指定优先级为管理级别	-
operators	指定优先级为操作级别	-
users	指定优先级为用户级别	-
guests	指定优先级为访问级别	-
PASSWORD	密码	-

**1.4.7.7 设置用户密码复杂度**

**目的**

本节介绍了如何设置用户密码复杂度。

**过程**

设置用户密码复杂度的步骤如下。

在全局配置视图下，执行命令 `username WORD pwd-complex pwd-complex` 或者 `user pwd-complex pwd-complex`。

**参数说明**

参数	说明	取值
WORD	指定用户名	-
pwd-complex	密码复杂度	整数，范围是 1-4

**1.4.7.8 设置指定用户或者全局用户的密码长度**

**目的**

本节介绍了如何设置指定用户或者全局用户的密码长度。

**过程**

设置指定用户或者全局用户的密码长度的步骤如下。

在全局配置视图下，执行命令 `username WORD pwd-length pwd-length` 或者 `user pwd-length pwd-length`。

**参数说明**

参数	说明	取值
WORD	指定用户名	字符串形式
pwd-length	用户密码长度	整数形式，长度范围是 1-64

**1.4.7.9 设置指定用户的密码生存周期**

**目的**

本节介绍了如何设置指定用户的密码生存周期。

**过程**

设置指定用户的密码生存周期的步骤如下。

在全局配置视图下，执行命令 `user pwd-live pwd-live-time` 或者 `username WORD pwd-live pwd-live-time`。

**参数说明**

参数	说明	取值
WORD	指定用户名，需提前创建	字符串形式
pwd-live-time	密码生存周期时间	整数范围，取值范围是 0-9999999，

参数	说明	取值
		单位为分钟

#### 1.4.7.10 设置指定用户登陆系统失败的最多次数

##### 目的

本节介绍了如何设置指定用户登陆系统失败的最多次数。

##### 过程

设置指定用户登陆系统失败的最多次数的步骤如下。

在全局配置视图下，执行命令 `user fail-count fail-count-time` 或者 `username WORD fail-count fail-count-time`。

##### 参数说明

参数	说明	取值
WORD	指定用户名，需提前创建	字符串形式
fail-count-time	登陆系统的失败最多次数	整数取值，取值范围是 1-10，单位为次

#### 1.4.7.11 设定在线用户的最大个数

##### 目的

本节介绍了如何设定在线用户的最大个数。

##### 过程

设定在线用户的最大个数的步骤如下。

在全局配置视图下，执行命令 `username WORD online-count online-count-num`。

##### 参数说明

参数	说明	取值
WORD	指定用户名，需提前创建	字符串形式
online-count-num	在线用户的最大个数	整数范围，取值范围是 1-64

#### 1.4.7.12 设置用户重认证时间间隔

##### 目的

本节介绍了如何设置用户重认证时间间隔。

##### 过程

设置用户重认证时间间隔的步骤如下。

在全局配置视图下，执行命令 `user reauth-interval reauth-interval-time` 或者 `username WORD reauth-interval reauth-interval-time`。

参数说明

参数	说明	取值
WORD	指定用户名，需提前创建	
reauth-interval-time	用户重认证时间间隔	整数范围，取值范围是 0-65535，单位为分钟

### 1.4.7.13 设置 telnet、ssh 和 ftp 用户登陆系统的最大次数

目的

本节介绍了如何设置 telnet、ssh 和 ftp 用户登陆系统的最大次数。

过程

设置 telnet、ssh 和 ftp 用户登陆系统的最大次数的步骤如下。

在全局配置视图下，执行命令 `user { telnet | ssh | ftp } max-count max-count-time`。

参数说明

参数	说明	取值
telnet	telnet 方式登陆的用户	-
Ssh	ssh 方式登陆的用户	-
Ftpd	ftp 方式登陆的用户	-
max-count-time	用户登陆系统的最大次数	整数范围，取值范围是 1-64

## 1.4.8 带内带外网管配置

### 1.4.8.1 带内网管配置

目的

本节介绍如何配置带内网管。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	过程	参数说明
配置带内网管	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code>，进入全局配置视图。</li> <li>2. 执行命令 <code>interface vlan vlan-id</code> 进入 VLANIF 配置视图。</li> <li>3. 执行命令 <code>ip address</code></li> </ol>	<code>ip-address/mask-length</code> ：指定 IP 地址及掩码地址，点分十进制； <code>mask-length</code> ：掩码地址位

目的	过程	参数说明
	<i>ip-address/mask-length</i> 或 <b>ip address ip-address mask-address</b> 配置带内 IP 地址。	数，取值为整数，范围从 1~32

### 1.4.8.2 带外网管配置

#### 目的

本节介绍如何配置带内网管。注意带外IP地址不能与带内IP为同网段IP。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	过程	参数说明
配置带外网管	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b>，进入全局配置视图。</li> <li>2. 执行命令 <b>interface ethernet 0/0/0</b> 进入带外口配置视图。</li> <li>3. 执行命令 <b>ip address ip-address/mask-length</b> 或 <b>ip address ip-address mask-address</b> 配置带外 IP 地址。</li> </ol>	<b>ip-address/mas k-length</b> ：指定 IP 地址及掩码地址，点 分 十 进 制 ； <b>mask-length</b> ：掩码地址位数，取值为整数，范围从 1~32

## 1.5 配置文件系统

为了方便用户对 Flash 等存储设备进行有效的管理，交换机提供了文件系统模块。文件系统为用户提供了文件和目录的访问管理功能，主要包括文件和目录的创建、删除、修改、更名，以及显示文件的内容等。缺省情况下，对于有可能给用户带来损失的命令（比如删除文件、覆盖文件等），文件系统将提示用户进行确认。

根据操作对象的不同，可以把文件系统操作分为以下几类：

- 目录操作；
- 文件操作；

### 1.5.1 目录操作

#### 目的

文件系统可以创建或删除目录、显示当前的工作目录以及指定目录下的文件或目录的信息。可以使用下面的命令来进行相应的目录操作。

#### 过程

目录操作的步骤如下。



目的	步骤
创建目录	在特权用户视图或全局配置视图下执行命令 <code>mkdir directory</code>
删除目录	在特权用户视图或全局配置视图下执行命令 <code>rmdir directory</code>
显示当前的工作目录	在特权用户视图下执行命令 <code>pwd</code>
显示目录下文件	在特权用户视图或全局配置视图下执行命令 <code>dir directory</code>
改变当前目录	执行命令 <code>cd directory</code>
更新系统或配置文件	在特权用户视图下执行命令 <code>upgrade {config os}</code>
列出一个目录或其子目录内容	在特权用户视图或全局配置视图下执行命令 <code>ls tree director</code> 在特权用户视图或全局配置视图下或者执行 <code>ls tree directory subtree</code>

## 1.5.2 文件操作

### 目的

文件系统可以删除文件、显示文件的内容、重新命名、拷贝文件、显示指定的文件的信息。可以使用下面的命令来进行相应的文件操作。

### 过程

文件操作的步骤如下。

目的	过程	参数说明
删除文件	在特权用户视图或者全局配置视图下执行命令 <code>del filename</code>	单个目录名或文件名的字符数不能超过 127 包含了设备名、单个目录名、文件名后的目录名长度不能超过 127
永久删除文件	在特权用户视图或者全局配置视图下执行命令 <code>remove filename</code>	<b>Filename:</b> 字符串形式。目录或文件的路径及名称中使用的字符不可以是空格、“~”、“*”、“/”、“\”、“:”、“”等字符，不区分大小写。
重新命名文件	在特权用户视图下执行命令 <code>rename src-filename new-filename</code>	<b>Filename:</b> 字符串形式。目录或文件的路径及名称中使用的字符不可以是空格、“~”、“*”、“/”、“\”、“:”、“”等字符，不区分大小写。
拷贝文件夹	在特权用户视图下执行命令 <code>xcopy srcfile destfile</code>	字符串形式
拷贝文件	在特权用户视图下执行命令 <code>copy srcfile destfile</code>	字符串形式
显示目录或文件信息	在特权用户视图或者全局配置视图	字符串形式

目的	过程	参数说明
	下执行命令 <code>dir directory</code>	
设置文件的属性	在特权用户视图或者全局配置视图下执行命令 <code>attrib NAME {+r +s +h -r -s -h} [ subtree ]</code>	字符串形式
显示指定二进制text文件的内容	在特权用户视图或者全局配置视图下执行命令 <code>type file { binary   text }</code>	字符串形式。目录或文件的路径及名称中使用的字符不可以是空格、、“~”、“*”、“/”、“\”、“:”、“”等字符，不区分大小写
清空指定文件的内容	在特权用户视图或者全局配置视图下执行命令 <code>zero filename</code>	<b>Filename:</b> 字符串形式。目录或文件的路径及名称中使用的字符不可以是空格、、“~”、“*”、“/”、“\”、“:”、“”等字符，不区分大小写。

### 1.5.3 系统配置文件

本节主要介绍设备的系统配置文件的相关操作。

#### 1.5.3.1 切换本地认证模式

##### 目的

本节介绍如何配置由其他的认证模式切换到本地认证模式。

##### 过程

切换本地认证模式的步骤如下。

1. 进入到全局模式。
2. 执行命令 **auth-degenerate**

#### 1.5.3.2 保存配置文件

##### 目的

本节介绍如何把当前系统的配置写到启动配置文件中。

##### 过程

保存配置文件的步骤如下。

- 1、进入到特权模式。
- 2、执行命令 **write file**。

## 1.5.4 FTP 配置

FTP（File Transfer Protocol，文件传输协议）是 Internet 和 IP 网络上传输文件的通用方法。由 FTP 提供的文件传输是将一个完整的文件从一个系统复制到另一个系统。FTP 支持有限数量的文件类型（ASCII，二进制等等）和文件结构（面向字节流或记录）。虽然目前大多数用户在通常情况下选择使用 Email 和 Web 传输文件，但是 FTP 仍然有着比较广泛的用途。FTP 协议在 TCP/IP 协议族中属于应用层协议，用于在远端服务器和本地主机之间传输文件。交换机提供的 FTP 服务包括：

**FTP Server 服务**，用户可以运行 FTP 客户端程序登录到服务器上（接受用户登录前，网络管理员需要事先配置好 FTP Server 的 IP 地址），访问服务器上的文件。

**FTP Client 服务**，用户在微机上通过终端仿真程序或 Telnet 程序建立与交换机（FTP Client）的连接后，输入 ftp X.X.X.X（X.X.X.X 代表远程 FTP Server 的 IP 地址）命令，建立交换机与远程 FTP Server 的连接，访问远程 FTP Server 上的文件。

本设备支持 IPv4 和 IPv6 两种网络地址下的 FTP 功能。

### 1.5.4.1 启动/关闭 FTP 服务器

#### 目的

本节介绍如何启动和关闭 FTP 服务器。

#### 过程

启动/关闭 FTP 服务器的步骤如下。

目的	过程
启动服务器	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code>，进入全局配置视图。</li> <li>2. 执行命令 <code>ftpd</code></li> </ol>
关闭服务器	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code>，进入全局配置视图。</li> <li>2. 执行命令 <code>no ftpd</code></li> </ol>

### 1.5.4.2 FTP 客户端介绍

FTP 客户端是交换机提供给用户的一个附加功能，它是一个应用模块，不用做任何功能配置。此时，交换机作为 FTP 客户端与远程服务器连接，并键入 FTP 客户端的命令来进行相应的操作（如建立、删除目录等）。

### 1.5.4.3 FTP Server 配置举例

#### 目的

交换机作为 FTP Server 实现配置文件的备份和软件升级配置举例。

交换机作为 FTP Client 时的配置。

设备	配置
Switch	启动 FTP Server，并作了用户名、密码、等相关的配置
PC	使用 FTP 客户端程序登录交换机

### 组网需求

交换机作为 FTP Server，远端的 PC 作为 FTP Client。在 FTP Server 上作了如下配置：配置了一个 FTP 用户名为 switch，密码为 hello，对该用户授权了交换机上 Flash 根目录的读写权限。交换机上带内或带外的 IP 地址为 1.1.1.1，PC 的 IP 地址为 1.1.1.2，交换机和 PC 之间路由可达。交换机的应用程序 switch.z 保存在 PC 上。PC 通过 FTP 向远端的交换机上传 switch.z，同时将交换机的配置文件 config 下载到 PC 实现配置文件的备份。

### 组网图

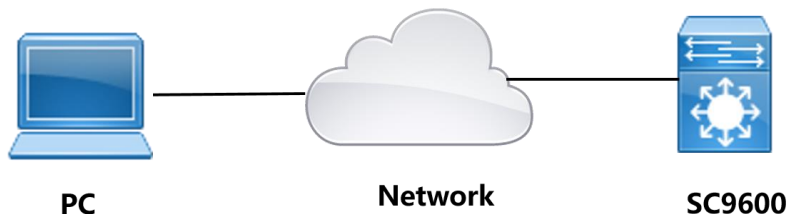


图 1-8 FTP 配置示意图

### 配置步骤

交换机上的配置

- 1) 用户登录到交换机上（用户可以在本地通过 Console 口登录到交换机上，也可以通过 telnet 远程登录到交换机上），并且在交换机上开启 FTP 服务。

```
SC9600#config
SC9600(config)#ftpd
```

- 2) 在 PC 上运行 FTP Client 程序，同交换机建立 FTP 连接，同时通过上载操作把交换机的应用程序 switch.z 上载到交换机的 Flash 根目录下，同时从交换机上下载配置文件 config。FTP Client 应用程序由用户自己购买、安装。

```
C:\ftp 1.1.1.1
220 FHN(1.0)FTP Server ready
User (1.1.1.1@none): admin
```

```

331 Password required
Password:
230 User logged in
ftp>bin
200 Type set to I, binary mode
ftp> put switch.z
200 Port set okay
150 Opening BINARY mode data connection
226 Transfer complete
ftp: 发送 3069212 字节, 用时 1.42Seconds 2158.38Kbytes/sec.
    
```

#获取交换机配置文件

```

ftp>ascii
200 Type is ASCII
ftp>get startcfg
150 Opening ASCII mode data connection
226 Transfer complete
ftp: 收到 14251 字节, 用时 0.22Seconds 65.07Kbytes/sec.
    
```



注意：

如果交换机的 Flash Memory 空间不够大, 请删除 Flash 中原有的应用程序然后再上载新的应用程序到交换机 Flash 中。

PC 作为 FTP server 时, 传送镜像文件使用 bin 模式, 传送配置文件时使用 ASCII 模式。

3) 在上载完毕后, 用户在交换机上进行升级操作。

用户可以通过命令 `upgrade os` 来作为下次启动时的应用程序, 然后重启交换机, 实现交换机应用程序的升级。

```

SC9600#config
SC9600(config)#upgrade os
SC9600(config)#quit
SC9600#reboot
    
```

#### 1.5.4.4 FTP Client 配置举例

##### 目的

交换机作为 FTP Client 实现配置文件的备份和软件升级配置举例。

设备	配置	配置说明	参数说明
Switch	可以直接使用 ftp 命令登录远端的 FTP Server	用户首先获取 FTP 用户命令和密码，然后登录远端的 FTP Server，这样才能取得相应目录和文件。	<b>put:</b> 将客户端的文件上传到服务器端。 <b>get:</b> 将服务器端文件下载到客户端中。
PC	启动 FTP Server，并作了用户名、密码、用户的权限等相关的配置	<b>ftp get ipv4-address user password remotefile [ port-id]</b> 或 <b>ftp get ipv4-address user password remotefile localfile filename [ port-id]</b> 或 <b>ftp put ipv4-address user password remotefile localfile filename [ port-id]</b>	<b>ipv4-address</b> 参数代表 FTP 服务器的 IP 地址； <b>remotefile:</b> 主机上要下载的文件名 <b>filename:</b> 指定本地文件名

### 组网要求

交换机作为 FTP Client，远端的 PC 作为 FTP Server，在 FTP Server 上作了如下配置：配置了一个 FTP 用户名为 123，密码为 123。配置 PC 的 IP 地址为 10.18.1.2。用户可以通过 telnet 远程登录到 SC9600 交换机上，从 FTP Server 上下载交换机的应用程序到交换机的 Flash，通过命令行实现交换机的远程升级。

### 组网图

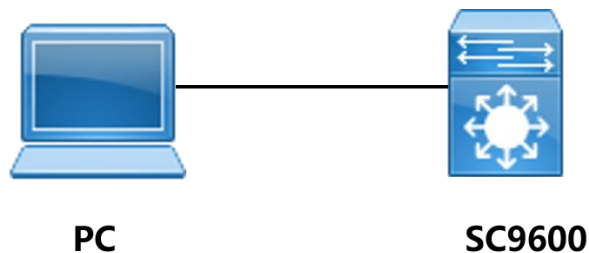


图 1-6 交换机作为 FTP client 配置组网图

### 配置步骤

# 进入全局配置视图，输入命令进行 FTP 连接，输入正确用户名和密码登录到 FTP Server。

```

SC9600#config
SC9600(config)#ftp get 10.18.1.2 123 123 d:\upgrade.z
Local path is "Ram:/flash/download".
Getting data...
3069212 bytes downloaded
    
```

# 升级程序下载到交换机 Download 目录下，通过升级命令进行升级。重新启动后，新的镜像文件才能生效。

```
SC9600(config)#upgrade os

WARNING: System will upgrade! Continue?[y/n]
System now is upgrading, please wait.
%Local path is "Ram:/flash/download".

SC9600(config)#reboot
```

## 1.5.5 TFTP 配置

TFTP (Trivial File Transfer Protocol, 简单文件传输协议)，最初打算引导无盘系统（通常是工作站或 X 终端），相对于另一种文件传输协议 FTP，TFTP 不具有复杂的交互存取接口和认证控制，适用于客户端和服务端之间不需要复杂交互的环境。TFTP 协议一般在 UDP 的基础上实现。

TFTP 协议传输是由客户端发起的。当需要下载文件时，由客户端向 TFTP 服务器发送读请求包，然后从服务器接收数据，并向服务器发送确认；当需要上传文件时，由客户端向 TFTP 服务器发送写请求包，然后向服务器发送数据，并接收服务器的确认。TFTP 传输文件的模式只为二进制模式。

配置 TFTP 之前，网络管理员需要首先配置好 TFTP 客户端和服务器的 IP 地址，并确保客户端和服务端之间可达。

本设备支持 IPv4 和 IPv6 两种网络地址下的 TFTP 功能。

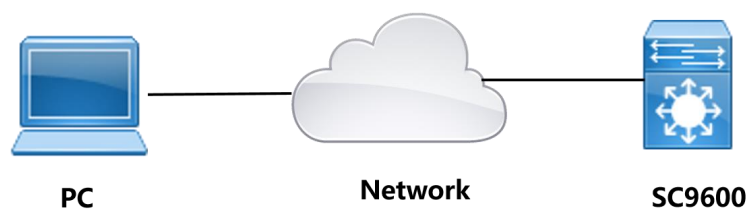


图 1-7 TFTP 配置示意图

### 1.5.5.1 配置 TFTP Server 开关

#### 目的

本节介绍了如何打开或者关闭设备的 TFTP Server 开关功能。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	过程
启动设备的 TFTP Server 功能	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code> 进入全局配置视图。</li> <li>2. 执行命令 <code>tftpd</code> 启动设备的 TFTP Server 功能。</li> </ol>
启动设备的 TFTP6 Server 功能	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code> 进入全局配置视图。</li> <li>2. 执行命令 <code>tftpd6</code> 启动设备的 TFTP6 Server 功能。</li> </ol>
关闭设备的 TFTP Server 功能	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code> 进入全局配置视图。</li> <li>2. 执行命令 <code>no tftpd</code> 关闭设备的 TFTP Server 功能。</li> </ol>
关闭设备的 TFTP6 Server 功能	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code> 进入全局配置视图。</li> <li>2. 执行命令 <code>no tftpd6</code> 关闭设备的 TFTP6 Server 功能。</li> </ol>

### 1.5.5.2 用 TFTP 下载文件



注意：

建议用户在技术人员的指导下进行该命令的操作。

#### 目的

当需要下载文件时，客户端向 TFTP 服务器发送读请求包，然后从服务器接收数据，并向服务器发送确认。在设备的实际运行维护中，往往需要从主机上将配置文件或操作系统文件下载到设备上，用于更改配置或者升级系统操作系统。该命令便是用于将文件下载到设备上。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	过程
通过 <code>tftp</code> 下载远程文件并存储在本地。（适用于 IPv4）	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code>，进入全局配置视图。</li> <li>2. 执行命令 <code>tftp get tftp-server dest-file</code> 或者 <code>tftp get ipv4-address remotefile localfile filename [ port-id ]</code></li> </ol>
通过 <code>tftp</code> 下载远程文件并存储在本地。（适用于 IPv6）	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code>，进入全局配置视图。</li> <li>2. 执行命令 <code>tftp6 get ipv6-address remotefile [ port-id ]</code> 或者 <code>tftp6 get ipv6-address remotefile localfile filename [ port-id ]</code></li> </ol>

#### 参数说明

参数	说明	取值
<code>ipv4-address</code>	主机的 IPv4 地址	点分十进制形式
<code>ipv6-address</code>	主机的 IPv6 地址	纯 2 进制表示：128 个 0 和 1 组成，



参数	说明	取值
		每 16 位为一段，共八段
remotefile	主机上要下载的文件名	字符串形式，长度范围是 1~63
filename	指定本地文件名	字符串形式，长度范围是 1~63
[ port-id ]	端口号，可选配置	整数形式，取值范围是 1~65535

### 1.5.5.3 用 TFTP 上传文件



注意：

建议用户在技术人员的指导下进行该命令的操作。

#### 目的

当交换机需要向 TFTP 服务器上传文件时，交换机作为客户端向 TFTP 服务器发送写请求包，然后向服务器发送数据，并接收服务器的确认。可以使用下面的命令上传文件。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
将本地文件上传到远程 TFTP Server。 (适用于 IPv4)	1. 执行命令 <code>configure</code> ，进入全局配置视图。 2. 执行命令 <code>tftp put ipv4-address remotefile config</code> 或者 <code>tftp put ipv4-address remotefile localfile filename [ port-id ]</code>
将本地文件上传到远程 TFTP Server。 (适用于 IPv6)	1. 执行命令 <code>configure</code> ，进入全局配置视图。 2. 执行命令 <code>tftp6 put ipv6-address remotefile config</code> 或者 <code>tftp6 put ipv6-address remotefile localfile filename [ port-id ]</code>

#### 参数说明

参数	说明	取值
ipv6-address	主机的 IPv4 地址	纯 2 进制表示：128 个 0 和 1 组成，每 16 位为一段，共八段
ipv4-address	主机的 IPv4 地址	点分十进制形式
remotefile	主机上要上传到服务器存放的文件名	字符串形式，长度范围是 1~63
filename	指定要上传的本地文件的文件名	字符串形式，长度范围是 1~63
[ port-id ]	端口号，可选配置	整数形式，取值范围是 1~65535

参数	说明	取值
config	指定上传设备的配置文件	-

### 1.5.5.4 TFTP Client 配置实例

#### 目的

交换机作为 TFTP Client 实现配置文件的备份和软件升级配置举例。

设备	配置	缺省值	配置说明
Switch	可以直接使用 TFTP 命令登录远端的 TFTP Server 上传或者下载文件	-	TFTP 适用于客户端和服务端之间不需要复杂交互的环境，请保证交换机和 TFTP Server 之间可达。
PC	启动 TFTP Server，并作了 TFTP 工作目录的配置	-	-

#### 组网需求

交换机作为 TFTP Client，PC 作为 TFTP Server，在 TFTP Server 上配置了 TFTP 的工作路径。交换机带内的 IP 地址为 1.1.1.1，交换机和 PC 相连的端口属于该 VLAN，PC 的 IP 地址为 1.1.1.2。交换机的应用程序 switch.z 保存在 PC 上。交换机通过 TFTP 从 TFTP Server 上下载 switch.z，同时将交换机的配置文件上传到 TFTP Server 的工作目录 vrpcfg.txt，实现配置文件的备份。

#### 组网图

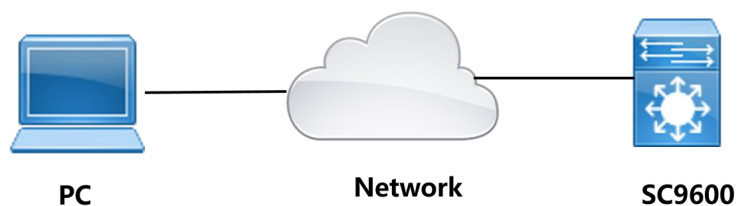


图 1-8 TFTP 配置示意图

#### 配置步骤

- 1) 在 PC 上启动了 TFTP Server，配置 TFTP Server 的工作目录。
- 2) 交换机上的配置

#用户登录到交换机上（用户可以在本地通过 Console 口登录到交换机上，也可以通过 telnet 远程登录到交换机上），并且进入全局配置视图。

```
SC9600#config
SC9600(config)#ftp get 1.1.1.2 switch.z
SC9600(config)#ftp put 1.1.1.2 vrpcfg.txt config
```

## 第2章 二层以太网配置

### 2.1 概述

本章介绍了 SC9600 系列高端交换机二层以太基本功能配置。

本章包括如下主题：

内容	页码
2.1 概述	2-1
2.2 以太网接口配置	2-1
2.3 MAC 表配置	2-10
2.4 ARP 配置	2-13
2.5 防攻击配置	2-15
2.6 链路聚合配置	2-24
2.7 VLAN 配置	2-30
2.8 VLAN 转换配置	2-42
2.9 QinQ 配置	2-48
2.10 PVLAN 配置	2-49
2.11 Voice VLAN 配置	2-58
2.12 环回检测配置	2-65

### 2.2 以太网接口配置

#### 2.2.1 以太网接口配置概述

以太网端口配置包括：

- 进入以太网端口视图
- 打开/关闭以太网端口
- 设置以太网端口双工状态
- 设置以太网端口速率

- 设置以太网端口流量控制
- 设置以太网端口的广播/组播报文的抑制功能
- 设置以太网端口速率抑制功能
- 设置端口优先级大小
- 设置以太网端口的最大传输单元
- 描述以太网端口
- 使能以太网设备带内网管地址
- 显示以太网端口状态

## 2.2.2 以太网接口基本属性配置

### 2.2.2.1 进入以太网端口视图

#### 背景信息

要对以太网端口进行配置，首先要进入以太网端口视图。

请在全局配置视图下进行下列配置。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
进入以太网端口视图	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code>，进入全局视图。</li> <li>2. 执行命令 <code>interface interface-type interface-number</code> 进入指定某一接口的配置视图。</li> </ol>	<p>interface-number: SC9600 系列交换机支持以下 3 种型号的接口配置范围：</p> <ul style="list-style-type: none"> <li>● SC9603 : 取值范围是 &lt;1-3&gt;/&lt;0-4&gt;/&lt;1-48&gt;</li> <li>● SC9608 : 取值范围是 &lt;1-8&gt;/&lt;0-4&gt;/&lt;1-48&gt;</li> <li>● SC9612 : 取值范围是 &lt;1-12&gt;/&lt;0-4&gt;/&lt;1-48&gt;</li> </ul>
退出以太网端口视图	执行命令 <code>quit</code>	-

### 2.2.2.2 打开/关闭以太网端口

#### 背景信息

当端口的相关参数及协议配置好之后，可以使用 **no shutdown** 命令打开端口；如果想使某端口不再转发数据，可以使用 **shutdown** 命令关闭端口。缺省情况下，端口为关闭状态。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
关闭以太网端口 当接口闲置时，即没有连接线缆进行工作时，请使用 <b>shutdow n</b> 命令关闭该接口，以防止由于干扰导致接口异常情况的发生。	1. 执行命令 <b>configure</b> ，进入全局视图。 2. 执行命令 <b>interface interface-type interface-number</b> 进入指定某一接口的配置视图。 3. 执行命令 <b>shutdown n</b> 关闭当前以太网。
打开以太网端口 当修改了接口的属性参数，而新配置未能立即生效，可使用 <b>shutdown</b> 和 <b>no shutdown n</b> 命令关闭和重启接口，使新配置生效	1. 执行命令 <b>configure</b> ，进入全局视图。 2. 执行命令 <b>interface interface-type interface-number</b> 进入指定某一接口的配置视图。 3. 执行命令 <b>no shutdown n</b> 开启当前以太网。

### 2.2.2.3 设置以太网端口双工状态

#### 背景信息

当希望端口在发送数据包的同时可以接收数据包，可以将端口设置为全双工属性；当希望端口同一时刻只能发送数据包或接收数据包时，可以将端口设置为半双工属性；当设置端口为自协商状态时，端口的双工状态由本端口和对端端口自动协商而定。

#### 配置前提

使用本命令之前，必须使用 **negotiation auto** 命令配置快速以太网电接口工作在非自协商模式时，才能配置接口的双工模式。否则，设备会提示 **%Info: Please configure negotiation auto disable first**。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
设置以太网端口工作于全双工状态	1. 执行命令 <b>configure</b> ，进入全局视图。 2. 执行命令 <b>interface interface-type interface-number</b> 进入指定某一接口的配置视图。 3. 执行命令 <b>duplex full</b> 指定该接口工作	缺省情况下，当以太网接口工作于非自动协商模式时，它的工作模式为全双工模式。

目的	步骤	参数说明
	于全双功模式	
设置以太网端口工作于半双功状态	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code>，进入全局视图。</li> <li>2. 执行命令 <code>interface interface-type interface-number</code> 进入指定某一接口的配置视图。</li> <li>3. 执行命令 <code>duplex half</code> 指定该接口工作于半双功模式</li> </ol>	

### 2.2.2.4 设置以太网端口速率

#### 背景信息

可以使用以下命令对以太网端口的速率进行设置，当设置端口速率为自协商状态时，端口的速率由本端口和对端端口双方自动协商而定。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	缺省值
配置以太网接口速率	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code>，进入全局视图。</li> <li>2. 执行命令 <code>interface interface-type interface-number</code> 进入指定某一接口的配置视图。</li> <li>3. 执行命令 <code>speed 10/100/1000</code> 设置接口的不同速率。分别为 10Mbit/s, 100Mbit/s 和 1000Mbit/s。</li> </ol>	缺省情况下，接口工作于非自协商模式时，其速率为接口支持的最大速率。

### 2.2.2.5 设置以太网端口流量控制

#### 背景信息

当本端和对端交换机都开启了流量控制功能后，如果本端交换机发生拥塞，它将向对端交换机发送消息，通知对端交换机暂时停止发送报文；对端交换机在接收到该消息后将暂时停止向本端发送报文；反之亦然。从而避免了报文丢失现象的发生。可以使用以下命令对本端以太网端口是否开启流量控制功能进行设置，关闭则不发送流控帧。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	缺省值
开启以太网端口流量控制	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code>，进入全局视图。</li> <li>2. 执行命令 <code>interface interface-type</code></li> </ol>	缺省情况下，以太网接口的流量控制为关闭

目的	步骤	缺省值
	interface-number 进入指定某一接口的配置视图。 3. 执行命令 flow -control enable	状态。
关闭以太网端口流量控制	1. 执行命令 configure, 进入全局视图。 2. 执行命令 interface interface-type interface-number 进入指定某一接口的配置视图。 3. 执行命令 flow -control disable	

### 2.2.2.6 设置以太网端口的广播/组播报文的抑制功能

#### 目的

为了防止由于广播组播报文泛滥造成端口阻塞，交换机提供对广播/组播报文的抑制功能。用户通过设置带宽值来抑制广播报文/组播/dlf 报文。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置以太网接口对广播、组播或未知单播报文进行风暴控制	1. 执行命令 configure, 进入全局视图。 2. 执行命令 interface interface-type interface-number 进入指定某一接口的配置视图。 3. 执行命令 storm-control { multicast   broadcast   dlf } 64kbps times 或 storm-control { multicast   broadcast   dlf } percent percent-value	缺省情况下，接口不对广播包、组播报或未知单播包进行速率限制。 broadcast: 指定对广播报文进行风暴控制 multicast: 指定对组播报文进行风暴控制 dlf: 指定对未知单播包进行风暴控制
取消风暴控制功能	1. 执行命令 configure, 进入全局视图。 2. 执行命令 interface interface-type interface-number 进入指定某一接口的配置视图。 3. 执行命令 no storm-control { multicast   broadcast   dlf }	64kbps: 表示通过的数据包带宽粒度为 64kbps times: 表示通过的数据包所占带宽为带宽粒度的倍数 percent: 表示通过的数据包所占带宽的百分比 percent-value: 表示通过的数据包所占带宽的百分比

### 2.2.2.7 设置以太网端口速率抑制功能

#### 背景信息



要在某些场合可能需要对端口的速率来进行控制，以便针对不同的用户提供不同带宽。具体的输入/输出带宽控制粒度可能会由于接口类型的不同而不同。

### 步骤

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置以太网端口速率抑制功能	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code>，进入全局视图。</li> <li>2. 执行命令 <code>interface interface-type interface-number</code> 进入指定某一接口的配置视图。</li> <li>3. 执行命令 <code>rate-limit {in/out} [ratio]</code></li> </ol>	缺省情况下，接口没有配置带宽限制。 <b>in:</b> 端口入方向带宽控制 <b>out:</b> 端口出方向带宽控制
取消以太网端口速率抑制功能	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code>，进入全局视图。</li> <li>2. 执行命令 <code>interface interface-type interface-number</code> 进入指定某一接口的配置视图。</li> <li>3. 执行命令 <code>no rate-limit {in/out}</code></li> </ol>	<b>rate-limit:</b> 带宽控制粒度，为 64kbps 的倍数。整数形式，取值范围是 1~16000

#### 2.2.2.8 设置端口优先级大小

##### 背景信息

通过对不同端口优先级的配置，保证重要业务量不受延迟或丢弃，同时保障网络的高效运行。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置以太网端口的优先级	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code>，进入全局视图。</li> <li>2. 执行命令 <code>interface interface-type interface-number</code> 进入指定某一接口的配置视图。</li> <li>3. 执行命令 <code>priority [level]</code></li> </ol>	缺省情况下，接口的优先级为 0。

#### 2.2.2.9 设置以太网端口的最大传输单元

##### 背景信息

在进行文件传输等大吞吐量数据交换的时候，可能会遇到大于标准以太网帧长的长帧。可以通过以下的命令设置允许帧通过的大小。

以太网接口的最大传输单元只影响 IP 在以太网口的组包和拆包,采用以太网 Ethernet\_II 格式时的最大传输单元为 1500,采用以太网 Ethernet\_SNAP 帧格式的最大传输单元为 1492。

### 过程

根据不同目的,执行相应步骤,具体参见下表。

目的	步骤	参数说明
设置以太网端口的最大传输单元	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code>, 进入全局视图。</li> <li>2. 执行命令 <code>interface interface-type interface-number</code> 进入指定某一接口的配置视图。</li> <li>3. 执行命令 <code>mtu mtu</code></li> </ol>	接口的最大传输单元值。整数形式,取值范围是 64-12228,单位:字节
恢复最大传输单元默认值	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code>, 进入全局视图。</li> <li>2. 执行命令 <code>interface interface-type interface-number</code> 进入指定某一接口的配置视图。</li> <li>3. 执行命令 <code>mtu default</code></li> </ol>	缺省情况下,接口默认的最大传输单元为 9216。

#### 2.2.2.10 配置连接网线类型适应方式

### 目的

当需要接口所能连接的网线类型与实际使用的网线相匹配时,配置连接网线类型适应方式。缺省情况下,接口不支持交叉网线类型。

### 步骤

根据不同目的,执行相应步骤,具体参见下表。

目的	步骤
配置接口适应交叉网线类型	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code>, 进入全局视图。</li> <li>2. 执行命令 <code>interface interface-type interface-number</code> 进入指定某一接口的配置视图。</li> <li>3. 执行命令 <code>mdi across</code>。</li> </ol>
配置接口仅适应直连网线	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code>, 进入全局视图。</li> <li>2. 执行命令 <code>interface interface-type interface-number</code> 进入指定某一接口的配置视图。</li> <li>3. 执行命令 <code>mdi normal</code>。</li> </ol>

#### 2.2.2.11 清除当前接口的统计信息

### 目的

本操作适用于当一个接口配置视图下存在大量信息需要清除时。

### 步骤

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置接口适应交叉网线类型	1. 执行命令 <code>configure</code> ，进入全局视图。 2. 执行命令 <code>interface interface-type interface-number</code> 进入指定某一接口的配置视图。 3. 执行命令 <code>reset counter</code>

### 2.2.2.12 描述以太网端口

#### 目的

使用以下命令设置端口的描述字符串，以区分各个端口。

#### 步骤

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
设置以太网端口描述字符串	1. 执行命令 <code>configure</code> ，进入全局视图。 2. 执行命令 <code>interface interface-type interface-number</code> 进入指定某一接口的配置视图。 3. 执行命令 <code>alias description</code> 。	缺省情况下，接口无描述信息。 <b>description</b> : 接口的描述信息，字符串形式，不支持空格，区分大小写。
删除以太网端口描述字符串	1. 执行命令 <code>configure</code> ，进入全局视图。 2. 执行命令 <code>interface interface-type interface-number</code> 进入指定某一接口的配置视图。 3. 执行命令 <code>no alias</code> 。	

## 2.2.3 以太网接口高级属性配置

### 2.2.3.1 配置端口环回检测

#### 目的

使用以下的配置任务可以开启端口环回监测功能并设置定时监测端口外部环回情况的时间间隔，以便定时监测各个端口是否被外部环回。如果发现某端口被环回，交换机会将该端口处于受控工作状态。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	命令	参数说明
全局关闭或者自动恢复	<code>loop-check action (port-block vlan-block)</code>	<code>port-block</code> 为当环回发生时只封闭环回发生所在的端口； <code>vlan-block</code> 为当环回发生

目的	命令	参数说明
环回检测	该命令配置的是发现环之后对成环端口的处理方式。	时封闭环回端口所在的 VLAN。
全局打开/关闭端口环回检测 trap 告警	loop-check trap (enable disable)	-
指定交换机的某端口在哪个 VLAN 上进行环回检测	loop-check vlan <1-4094>	-
使能、禁用端口环回检测	loop-check enable disable	-
重新使能端口的环回检测	loop-check reset	-
调试端口环回检测显示	show loop-check	显示端口环回检测的全局信息
	show loop-check interface	显示各个端口环回检测信息

### 2.2.3.2 显示以太网端口状态

#### 背景信息

在用户视图下执行 **show** 命令可以显示配置后以太网端口的运行情况，通过查看显示信息验证配置的效果。在以太网端口视图下，执行 **reset count** 命令可以清除以太网端口的统计信息。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
显示以太网端口状态	<ol style="list-style-type: none"> <li>1. 进入普通用户视图、特权用户视图、全局配置视图或者接口配置视图。</li> <li>2. 执行命令 <code>show interface { fastethernet   gigasethernet   xgigasethernet } interface-number config</code></li> </ol>
显示当前设备所有以太网接口及 trunk 接口（若已配置 trunk）的基本信息。	<ol style="list-style-type: none"> <li>1. 进入普通用户视图、特权用户视图、全局配置视图或者接口配置视图。</li> <li>2. 执行命令 <code>show interface verbose</code></li> </ol>

### 2.2.3.3 切换不同以太网接口配置视图

#### 目的

当配置完当前接口属性后需要配置其他接口属性可以使用本功能。

#### 步骤

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
切换当前以太网接口配置视图到新的以太网接口视图	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code>，进入全局视图。</li> <li>2. 执行命令 <code>interface interface-type interface-number</code> 进入指定某一接口的配置视图。</li> <li>3. 执行命令 <code>switch { fastethernet   gigaethernet   xgigaethernet } interface-number</code></li> </ol>

## 2.3 MAC 表配置

为了快速转发报文，交换机需要维护 MAC 地址表。MAC 地址表的表项包含了与交换机相连的设备的 MAC 地址及与此设备相连的交换机的端口号。MAC 地址表中的动态表项（非手工配置）是由交换机学习得来的。交换机学习 MAC 地址的方法如下：如果从某端口（假设为端口 A）收到一个数据帧，交换机就会分析该数据帧的源 MAC 地址（假设为 MAC-SOURCE），并认为目的 MAC 地址为 MAC-SOURCE 的报文可以由端口 A 转发；如果 MAC 地址表中已经包含 MAC-SOURCE，交换机将对应表项进行更新，如果 MAC 地址表中尚未包含 MAC-SOURCE，交换机则将这个新 MAC 地址（以及该 MAC 地址对应的转发端口）作为一个新的表项加入到 MAC 地址表中。

对于目的 MAC 地址能够在 MAC 地址表中找到的报文，系统会直接使用硬件转发；对于目的 MAC 地址不能在地址表中查到的报文，系统对报文采用广播方式进行转发。如果广播后，报文到达了目的 MAC 地址对应的网络设备，目的网络设备将应答此广播报文，应答报文中包含了此设备的 MAC 地址，交换机通过地址学习将新的 MAC 地址加入到 MAC 地址转发表中。去往同一目的 MAC 地址的后续报文，就可以利用该新增的 MAC 地址表项直接进行转发了。

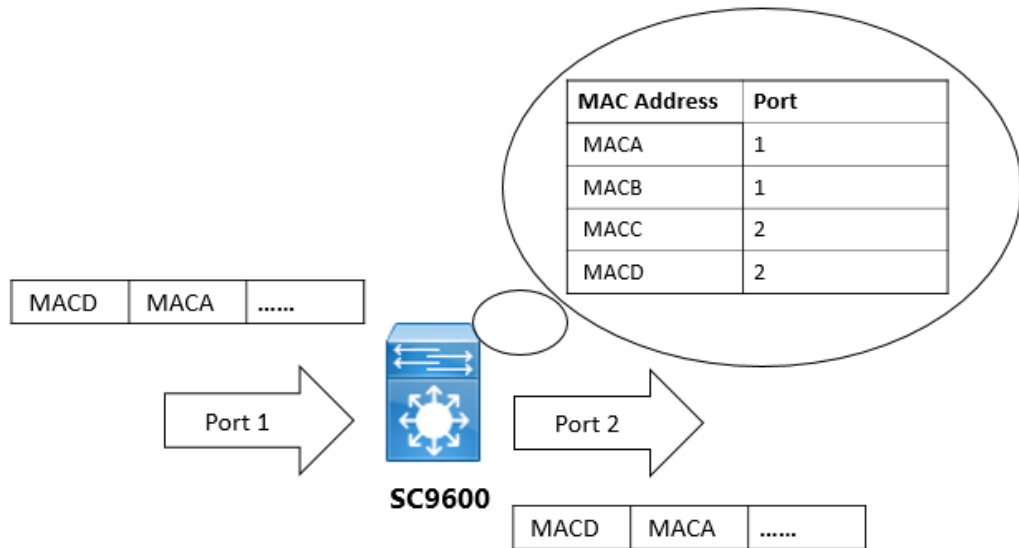


图 2-1 交换机利用转发表转发报文

### 2.3.1 配置 MAC 地址表管理

### 2.3.2 设置 MAC 地址表项

#### 目的

管理员根据实际情况可以手动添加、修改或删除 MAC 地址表中的表项。

使用静态 MAC 地址将用户设备与接口绑定，可以防止假冒身份的非法用户骗取数据，提高了设备的安全性。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
添加 / 修改地址表项	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code>，进入全局视图。</li> <li>2. 执行以下命令：  <code>mac-static</code>                    <code>vlan-id</code>  <code>mac-address { fastethernet  </code>  <code>gigaethernet   xgigaethernet }</code>  <code>interface-number</code> </li> </ol>	<p><code>vlan-id</code> VLAN: 接口编号，整数形式，取值范围是 1~4094</p> <p><code>mac-address</code> : 静态 MAC 地址，形如 AA:BB:CC:DD:EE:FF，其中 A~F 为一位十六进制数</p> <p><code>interface-number</code> : SC9600 系列交换机支持以下 3 种型号的接口配置范围：                      SC9603: 取值范围是&lt;1-3&gt;/&lt;0-4&gt;/&lt;1-48&gt;                      SC9608: 取值范围是&lt;1-8&gt;/&lt;0-4&gt;/&lt;1-48&gt;                      SC9612: 取值范围是&lt;1-12&gt;/&lt;0-4&gt;/&lt;1-48&gt;</p>

### 2.3.3 设置系统 MAC 地址老化时间

#### 背景信息

设置合适的老化时间可以有效的实现 MAC 地址老化的功能。用户设置的老化时间 过长或者过短，都可能导致交换机广播大量找不到目的 MAC 地址的数据报文，影响交换机的运行性能。如果用户设置的老化时间过长，交换机可能会保存许多过时的 MAC 地址表项，从而耗尽 MAC 地址表资源，导致交换机无法根据网络的变化更新 MAC 地址表。如果用户设置的老化时间太短，交换机可能会删除有效的 MAC 地址表项。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。



说明：

系统复位后，动态表项会丢失，而保存的静态表项和黑洞表项不会老化丢失。

目的	步骤	参数说明
设置 MAC 地址动态表项的老化时间	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code>，进入全局视图。</li> <li>2. 执行命令 <code>mac aging-time aging-time</code>。</li> </ol>	<p>缺省情况下，系统动态 MAC 地址表项老化时间为 300 秒。</p> <p><code>aging-time</code>: 指定动态 MAC 地址表项老化时间整数形式，取值范围是 60-1000000，单位：秒</p>

### 2.3.4 显示二层 MAC 地址表项

#### 目的

本节目的在于帮助用户快速定位到指定 MAC 地址的表项的相关信息，便于用户查询特定信息。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
显示二层静态转发表	<ol style="list-style-type: none"> <li>1. 进入普通用户视图、特权用户视图或者全局配置视图。</li> <li>2. 执行以下命令（任一）： <code>show mac-address MAC</code> <code>show mac-address MAC vlan VID</code></li> </ol>	<p><code>VID</code>: 指定 VLAN，可选参数 整数形式，取值范围是 1-4094</p> <p><code>MAC</code>: 指定静态 MAC 地址，形如 AA:BB:CC:DD:EE:FF，其中 A~F 为一位十六进制数</p> <p><code>config</code> 表示显示 MAC 地址配置信息；</p>

目的	步骤	参数说明
	<pre>show mac-address config show mac-address verbose</pre>	verbose 表示显示 MAC 地址除配置信息外所有详细信息

## 2.4 ARP 配置

ARP 映射表既可以动态维护，也可以手工维护。通常将用户手工配置的 IP 地址到 MAC 地址的映射，称之为静态 ARP。通过相关的手工维护命令，用户可以显示、添加、删除 ARP 映射表中的映射项。

### 2.4.1 手工添加/删除静态 ARP 映射项

#### 目的

本节介绍如何手工添加/删除静态 ARP 映射项。

静态 ARP 映射表项只能通过手动删除，不会受 ARP 映射表项老化时间的影响，同时设备也不能动态刷新此映射关系。静态 ARP 映射表项在设备正常工作期间一直有效。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
添加静态 ARP 映射表项	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code>，进入全局视图。</li> <li>2. 执行命令 <code>ip arp ip-address mac-address { gigaethernet   xgigaethernet } interface-number</code>。</li> </ol>	<p>缺省情况下，系统 ARP 映射表项为空，由动态 ARP 获取地址映射。</p> <p><b>ip-address:</b> 静态 ARP 映射项的 IP 地址，点分十进制形式</p> <p><b>mac-address:</b> 静态 ARP 映射项的 MAC 地址，形式是 AA:BB:CC:DD:EE:FF，其中 A~F 为 1 位十六进制数</p> <p><b>interface-number:</b> 静态 ARP 映射项的以太网接口编号 <b>interface-number:</b> SC9600 系列交换机支持以下 5 种型号的接口配置范围：</p> <p>SC9603: 取值范围是&lt;1-3&gt;/&lt;0-4&gt;/&lt;1-48&gt;</p> <p>SC9608: 取值范围是&lt;1-8&gt;/&lt;0-4&gt;/&lt;1-48&gt;</p> <p>SC9612: 取值范围是&lt;1-12&gt;/&lt;0-4&gt;/&lt;1-48&gt;</p> <p>SC9600-06E: 取值范围是&lt;1-6&gt;/&lt;0-4&gt;/&lt;1-48&gt;</p> <p>SC9600-10E : 取值范围是&lt;1-10&gt;/&lt;0-4&gt;/&lt;1-48&gt;</p>
删除静态 ARP 映射表项	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code>，进入全局视图。</li> <li>2. 执行命令 <code>no ip arp ip-address</code></li> </ol>	



## 2.4.2 清除动态 ARP 表项

### 目的

本节介绍如何清除动态 ARP 映射表项。

本节帮助用户可以在需要的时候手动删除设备的所有动态 ARP 映射表项。

执行此命令将取消 IP 地址和 MAC 地址的映射关系,可能导致暂时性无法访问某些节点,用户需谨慎使用。

### 过程

根据不同目的,执行相应步骤,具体参见下表。

目的	步骤
清除动态 ARP 映射表项	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code>, 进入全局视图。</li> <li>2. 执行命令 <code>flush arp dynamic</code>。</li> </ol>

## 2.4.3 查看 ARP 的信息

### 目的

本节介绍如何查看 ARP 相关信息。本节帮助用户通过查看局域网的 ARP 映射表后,来进行局域网的故障检测。ARP 在网络地址和本地网硬件地址之间建立了对应关系。每一个对应项记录在缓存中保持一段时间,然后放弃。

### 过程

根据不同目的,执行相应步骤,具体参见下表。

目的	步骤
查看 ARP 的信息	<ol style="list-style-type: none"> <li>1. 进入普通用户视图、特权用户视图或者全局配置视图。</li> <li>2. 执行命令 <code>show ip arp</code>。</li> </ol>

## 2.4.4 配置动态 ARP 映射表项老化时间

### 目的

本节介绍如何配置动态 ARP 映射表项的老化时间。

配置动态 ARP 映射表项的老化时间,可以减少因没有及时刷新动态 ARP 表项带来的地址解析错误问题。

### 过程

根据不同目的,执行相应步骤,具体参见下表。

目的	步骤	参数说明
添加静态 ARP 映射表项	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code>，进入全局视图。</li> <li>2. 执行命令 <code>ip arp aging-time { aging-time   default }</code>。</li> </ol>	<p>缺省情况下，系统动态 ARP 映射表项的老化时间为 1200 秒。</p> <p><b>aging-time:</b> 指定 ARP 映射表项的老化时间，整数形式，取值范围是 60~1200，单位：秒</p> <p><b>default:</b> 指定为缺省值，1200s</p>

## 2.4.5 设置 ARP 调试使能开关

### 目的

本节介绍如何设置 ARP 调试开关。

配置 arp 老化时间，可以减少因没有及时刷新动态 ARP 表项带来的地址解析错误问题。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
打开 ARP 调试开关	<p>执行命令 <code>debug arp { in   out   error   all }</code></p> <p><code>debug arp { dst-addr   src-addr } ip-address</code></p>	<p>{ in   out   error   all  dst-addr   src-addr }：表示收到的包、发出的包、错误包以及所有包。</p> <p>{ in   out   error   all  dst-addr   src-addr }：表示带有目的地址的包以及带有源地址的包。</p> <p><b>ip-address:</b> 表示目的地址或源地址的 IP 地址，点分十进制，如 IPv4: A.B.C.D</p>
关闭 ARP 调试开关	<p>执行命令 <code>no debug arp { in   out   error   all }</code></p> <p>或</p> <p><code>no debug arp { dst-addr   src-addr } ip-address</code></p>	

## 2.5 防攻击配置

### 2.5.1 Anti-attack 简介

#### 2.5.1.1 技术背景

所谓的网络安全威胁，即是通过特定技术或工具，对在网络、服务器和桌面上存储和传输的数据未经授权进行访问，甚至破坏或者修改这些数据，是当今网络安全中面临的基本威胁。

IP 网络的安全威胁分为两个方面：一是主机（包括用户主机和应用服务器等）的安全，二是网络自身（主要是网络设备，包括路由器、交换机等）的安全。用户主机所感知的

安全威胁主要是针对特定操作系统（主要是 Windows 系统）的攻击，诸如病毒、木马。网络设备主要面对的是基于 TCP/IP 协议的攻击。本软件主要针对网络自身，即网络设备的安全问题。

### 2.5.1.2 ARP 防攻击模块

#### 源 IP 地址冲突检测

所谓地址冲突，是指网络设备下挂的主机或者对接的其他网络设备设置的 IP 地址和该网络设备的接口 IP 地址冲突，网络设备如果无法检测到地址冲突，该网络设备下挂的其他主机的网关 ARP 地址有可能会被更新，导致下挂主机无法正常上网。

防攻击措施：当交换机收到 ARP 报文时，会判断该报文的源 IP 地址和交换机 ARP 缓存中 IP 地址是否相同。如果没有发现相应表项，则是正确报文；若发现 IP 地址相同，但 MAC 地址不同，交换机会立即发送一个地址冲突报文和免费 ARP 广播报文。地址冲突报文是通知对端主机或者设备，该地址已经被占用；免费 ARP 广播报文，是通知本网段内其他主机和网络设备，纠正本网段内其他主机或者网络设备的 ARP 表项，防止 ARP 表项指向错误的 MAC 地址。同时，交换机会上报地址冲突的告警信息并同时记录日志，以便维护人员能够及时了解设备遭受的攻击。

#### 源 MAC 地址冲突检测

这个功能也是为了防止网管的 ARP 缓存中多个 IP 的映射对应到同一个 MAC，而这个 MAC 通常就是攻击源。

防攻击措施：当交换机收到 ARP 报文时，会判断该报文的源 MAC 地址和交换机 ARP 缓存中 MAC 地址是否相同。如果没有发现表项，则是正确报文；如果发现 IP 地址相同，但 IP 地址不同，则交换机会立即发送一个地址冲突报文和免费 ARP 广播报文。地址冲突报文是通知对端主机或者设备，该地址已经被占用；免费 ARP 广播报文，是通知本网段内其他主机和网络设备，纠正本网段内其他主机或者网络设备的 ARP 表项，防止 ARP 表项指向错误的 MAC 地址。同时，交换机会上报地址冲突的告警信息并同时记录日志，以便维护人员能够及时了解设备遭受的攻击。

#### ARP 欺骗攻击防护

防止攻击源冒充网管非法监听通信，也被成为中间人攻击。ARP 攻击的核心思路就是利用 ARP 漏洞以伪造的 IP 不断发送请求，让所有主机的 ARP 缓存的 MAC 都指向自己，从而达到非法获取通信数据的目的。

防攻击措施：当交换机收到 ARP 请求报文时，会判断该报文的源 IP 地址和交换机本地接口的 IP 地址相同。如果发现 IP 地址相同，但对应的 MAC 不是设备的 MAC，则交换

机会立即发送一个地址冲突报文和免费 ARP 广播报文；如果该请求报文的目的是设备本地接口的 IP，但目的 MAC 不是设备的 MAC，如果该报文是 ARP 应答报文，则放行，如果不是，则立即发送一个地址冲突报文和免费 ARP 广播报文。地址冲突报文是通知对端主机或者设备，该地址已经被占用。免费 ARP 广播报文，是通知本网段内其他主机和网络设备，纠正本网段内其他主机或者网络设备的 ARP 表项，防止 ARP 表项指向错误的 MAC 地址。同时，交换机会上报地址冲突的告警信息并同时记录日志，以便维护人员能够及时了解设备遭受的攻击。

#### 动态 ARP 检测功能

动态 ARP 检测功能，可以配置对接口或 VLAN 下收到的 ARP 报文和 DHCP 绑定表进行匹配检查，当报文的检查项和绑定表中的特征项一致时，转发该报文，否则丢弃报文。同时可以配置告警功能，当丢弃的报文个数超过配置的阈值时，发送告警信息。

#### 2.5.1.3 Dos 防攻击模块

DoS 攻击，即拒绝服务攻击（DoS, Denial of Service），是指向设备发送大量的连接请求，占用设备本身的资源，严重的情况会造成设备瘫痪，一般情况下也会使设备的功能无法正常运行。因为主要是针对服务器的，目的是使服务器拒绝合法用户的请求，所以叫拒绝服务攻击。

随着攻击技术的发展，Dos 攻击也出现了升级，攻击者控制多台主机同时发起 DoS 攻击，也就是所谓的分布式拒绝服务攻击（DDoS, Distributed Denial of Service）攻击，它的规模更大，破坏性更强。

防攻击措施：确保某种协议遭受攻击时不会影响到其他协议的正常运行和业务的正常转发。同时，当攻击源对下挂在网络设备的服务器进行 DoS 攻击时，可以利用交换机的 ACL 功能，下发特定的 ACL 规则对攻击报文进行过滤，保障下挂的主机和服务器正常运行。

本模块用于端口的动态检测，通过硬件的计数功能，当某端口收到某种协议包的速率超过限速门限时，多余的包丢弃，但是丢弃的包依然被计数；当单位时间的某种协议包数超过屏蔽门限时，该端口将彻底屏蔽这种协议包一段时间，期满后恢复为限速规则。

#### 2.5.1.4 CPU 收包限速模块

通过全局配置，通过软件的方式对 CPU 收到的某种类型协议包计数，当超过所配置的速率时，多余的包全部丢弃。除了做速率限制外，还会检测最近两次收到的包在最短允许时间内是否内容重复，重复则丢弃。

## 2.5.2 Anti-attack 配置

### 2.5.2.1 Anti-attack 全局配置

#### 目的

本节介绍 anti-attack 全局配置，包括全局下设置 ARP 防攻击配置使能、设置 DOS 防攻击使能、设置 dos 防攻击锁定时间使能、设置 cpu 收包限速使能、设置 CPU 收包限速速率等。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
设置 ARP 防攻击配置使能	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>arp-antiattack (src-ip src-mac arp-cheat) (enable disable)</b>	src-ip src-mac arp-cheat : 源 ip 冲突检测、源 mac 冲突检测、arp 欺骗攻击防护
设置 DoS 防攻击使能	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>antiattack dos-limit (enable disable)</b>	-
设置 DoS 防攻击锁定时间使能	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>antiattack dos-limit lock-time (enable disable)</b>	-
设置 CPU 收包限速使能	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>antiattack pkt-limit (enable disable)</b>	-
设置 CPU 收包限速速率	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>antiattack pkt-limit (arp-request   arp-reply   stp   icmp   igmp   dhcp   udp   tcp   sgm   other   ip-to-self   ip-forward   ospf   bgp   rip ) rate</b>	rate: 门限速率，整数形式，取值范围是<0-500>。

### 2.5.2.2 Anti-attack 端口配置

#### 目的

本节介绍 Anti-attack 在端口下的配置。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
设置 dos 防攻击参数/去使能 dos 防攻击参数	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b> 或 <b>interface trunk trunk-number</b> 进入接口配置视图； 3. 执行命令 <b>antiattack dos-limit (arp ip icmp igmp udp tcp all) burst-normal { burst-normal-size   default } burst-max { burst-max-size   default } lock-time { lockup-time   default }</b> 或 <b>no antiattack dos-limit (arp ip icmp igmp udp tcp all)</b>	<b>interface-number</b> : SC9600 系列交换机支持以下 3 种型号的接口配置范围： SC9603 : 取值范围是 <1-3>/<0-4>/<1-48> SC9608 : 取值范围是 <1-8>/<0-4>/<1-48> SC9612 : 取值范围是 <1-12>/<0-4>/<1-48> <b>trunk-number</b> : 表示指定 trunk 接口号，整数形式，取值范围是 <1~128>。 <b>burst-normal-size</b> : 限速门限，整数形式，取值范围是 <1~16000>。 <b>burst-max-size</b> : 最大容许门限，整数形式，取值范围是 <1~2000000>。 <b>lockup-time</b> : 隔离时间，整数形式，取值范围是 <1-10000>。

2.5.2.3 Anti-attack 其他配置

目的

本节介绍 Anti-attack 其他基本配置。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
全局开启或关闭 ARP 报文限制功能	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>antiattack pkt-limit { enable   disable }</b> 。	<b>enable</b> 开启报文限制功能 <b>disable</b> 关闭报文限制功能
配置指定包类型的限制值	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>antiattack pkt-limit</b>	<b>packet-type</b> 指定的报文类型 arp-request arp-replay stp icmp igmp dhcp udp tcp sgm other  p-to-self  p-forw ard ospf bgp rip

目的	步骤	参数说明
	<i>packet-type maxnum.</i>	<b>maxnum</b> 指定报文的速率限速值 整数形式，取值范围是 0~500，单位：包/每秒 0 表示一个包都不允许通过

### 2.5.2.4 配置 Anti-attack 调试信息

#### 目的

本节介绍 Anti-attack 的调试功能配置。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
显示防攻击模块的调试信息	1. 进入特权用户视图； 2. 执行命令 <b>debug antiattack</b>	-
关闭防攻击模块的调试信息	1. 进入特权用户视图； 2. 执行命令 <b>no debug antiattack</b>	-
显示 ARP 防攻击模块的调试信息	1. 进入特权用户视图； 2. 执行命令 <b>debug dos-antiattack</b>	-
关闭 ARP 防攻击模块的调试信息	1. 进入特权用户视图； 2. 执行命令 <b>no debug dos-antiattack</b>	-
显示 ARP 防攻击模块的调试信息	1. 进入特权用户视图； 2. 执行命令 <b>debug arp-antiattack</b>	-
关闭 ARP 防攻击模块的调试信息	1. 进入特权用户视图； 2. 执行命令 <b>no debug arp-antiattack</b>	-

### 2.5.2.5 查看 Anti-attack 配置信息

#### 目的

本节介绍 Anti-attack 配置信息的查看，包括显示使能动态 ARP 检测功能的接口信息、查看 CPU 限速配置、DOS 防攻击全局以及端口配置、ARP 防攻击配置等。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
查看 DOS 防攻击全局配置信息	1. 进入普通用户视图或特权用户视图; 2. 执行命令 <b>show antiattack dos-limit interface</b>	-
查看 DOS 防攻击端口配置信息	1. 进入普通用户视图或特权用户视图; 2. 执行命令 <b>show antiattack dos-limit interface</b> { <b>fastethernet</b>   <b>gigaehternet</b>   <b>xgigaehternet</b> } <i>interface-number</i> 或 <b>show antiattack dos-limit interface</b> <b>trunk trunk-number</b>	interface-number: SC9600 系列交换机支持以下 3 种型号的接口配置范围: SC9603: 取值范围是 <1-3>/<0-4>/<1-48> SC9608: 取值范围是 <1-8>/<0-4>/<1-48> SC9612: 取值范围是 <1-12>/<0-4>/<1-48> trunk-number: 表示指定 trunk 接口号, 整数形式, 取值范围是 <1~128>。
查看全局 ARP 防攻击配置信息	1. 进入普通用户视图或特权用户视图; 2. 执行命令 <b>show arp-antiattack config</b>	-
查看 ARP 防攻击主机列表信息	1. 进入普通用户视图或特权用户视图; 2. 执行命令 <b>show arp-antiattack</b> { <b>trust-host</b>   <b>untrust-host</b> }	-

## 2.5.3 Anti-attack 配置举例

### 2.5.3.1 ARP 防攻击典型应用及配置

#### 组网要求

ARP 防攻击典型应用示意图如图 2-2 所示, 网络中存在的 ARP 威胁是: 用户 A 中病毒后, 会发出大量 ARP 攻击报文, 部分 ARP 报文的源 IP 地址在本网段内不停变化, 部分 ARP 报文的源 IP 地址和网关 IP 地址相同。

要求在 Switch 配置 ARP 的安全功能, 能够防止以上的攻击。

#### 组网图



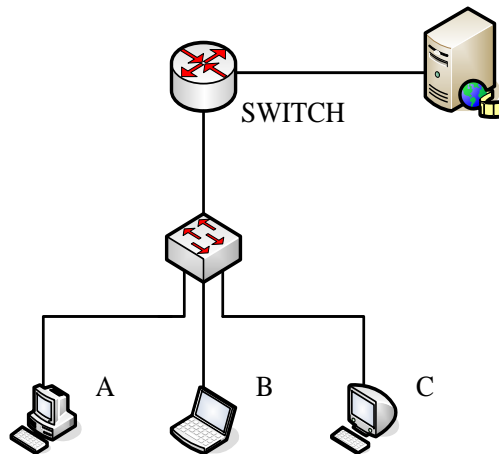


图 2-2 ARP 防攻击典型应用

#### 配置步骤

```
SC9600#show arp-antiattack config
arp-antiattack src-ip enable
```

#### 验证配置结果

使用 show arp-antiattack config 以及 show arp-antiattack statistic 命令可查看相关信息。

### 2.5.3.2 DOS 防攻击典型应用及配置

#### 组网要求

DOS 防攻击典型应用组网图如图 2-3所示,配置 DOS 防攻击相关功能--端口 ARP 限速及丢弃规则。

#### 组网图

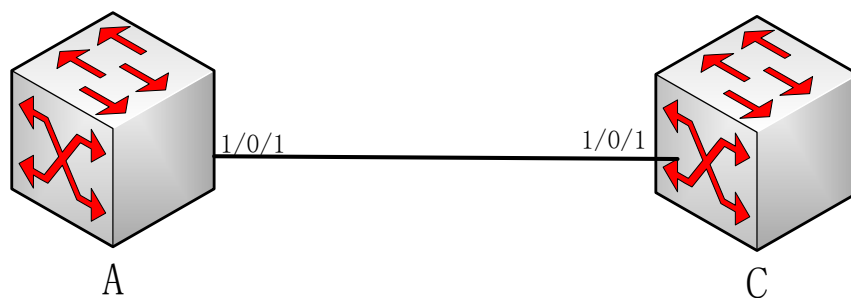


图 2-3 DOS 防攻击典型应用组网图

配置步骤

A 端

```
SC9600(config)#
SC9600(config)#antiattack dos-limit enable
SC9600(config)#antiattack dos-limit lock-time enable
SC9600(config)#interface gigaethernet 1/0/1
SC9600(config-ge1/0/1)#antiattack dos-limit arp burst-normal 1000 burst-max 1000
lock-time 10
```

验证配置结果

使用 show antiattack dos-limit interface 命令可查看相关信息如下：

```
SC9600#show antiattack dos-limit interface
```

```
antiattack dos-limit enable
```

Interface HWFlag	Type	ExpireTime	BurstNormal	BurstMax	LockTime	Count
ge-1/0/1	arp	0	1000	10000	10	<1 on

SC9600#

2.5.3.3 CPU 包限速典型应用级配置

组网要求

CPU 包限速典型应用示意图如图 2-4所示，配置端口 CPU 包限速规则—限制 arp 包为 500。

组网图

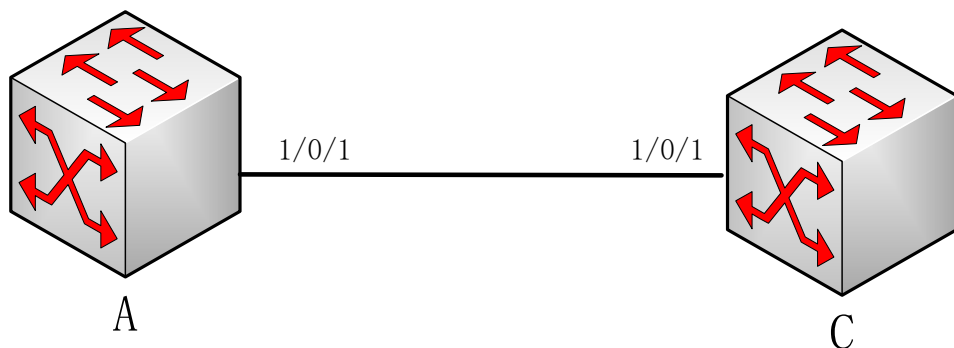


图 2-4 CPU 包限速典型应用

配置步骤

A 端

```
SC9600(config)#  
SC9600(config)#antiattack pkt-limit enable  
SC9600(config)#antiattack pkt-limit arp-request 500
```

#### 验证配置结果

使用 show antiattack config 命令可查看相关信息如下：

```
SC9600#show antiattack config  
antiattack pkt-limit enable  
antiattack pkt-limit arp-request 500  
antiattack pkt-limit arp-reply 112  
antiattack pkt-limit stp 112  
antiattack pkt-limit icmp 112  
antiattack pkt-limit igmp 112  
antiattack pkt-limit dhcp 112  
antiattack pkt-limit udp 112  
antiattack pkt-limit tcp 112  
antiattack pkt-limit sgm 112  
antiattack pkt-limit other 112  
antiattack pkt-limit ip-to-self 112  
antiattack pkt-limit ip-forward 112  
antiattack pkt-limit ospf 112  
antiattack pkt-limit bgp 112  
antiattack pkt-limit rip 112
```

## 2.6 链路聚合配置

### 2.6.1 端口汇聚简介

端口汇聚是将多个端口聚合在一起形成 1 个汇聚组，以实现出负荷在各成员端口中的分担，同时也提供了更高的连接可靠性。端口汇聚可以分为手工汇聚、动态 LACP 汇聚和静态 LACP 汇聚。同一个汇聚组中端口的类型应该保持一致，即如果某端口为电/光口，则其他端口也应为电/光口。

目前 SC9600 只支持手工汇聚和静态 LACP 汇聚功能。

## 2.6.2 配置汇聚组功能

### 背景信息



注意：

改变 Trunk 工作模式前请首先确保该 Trunk 中没有加入任何成员接口，否则无法修改 Trunk 的工作模式。删除已存在的成员接口请在相应接口视图下执行命令 `no join trunk trunk-id`

或在 Trunk 视图下执行命令 `no { gigaethernet | xgigaethernet } interface-number`。

### 目的

使用本节操作配置汇聚组及其基本功能，并加入多个成员接口增加设备间的带宽及可靠性。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
创建 Trunk 并进入其配置视图	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface eth-trunk trunk-id</b> 创建汇聚组并进入其配置视图，若待创建的组已存在，则直接进入其配置视图；</li> <li>3. 结束。</li> </ol>
配置 Trunk 的工作模式为静态 LACP 模式	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface eth-trunk trunk-id</b>，进入 trunk 接口视图；</li> <li>3. 执行命令 <b>mode lacp-static</b>，配置 trunk 的工作模式为静态 LACP 模式；</li> <li>4. 结束。</li> </ol>
向 Trunk 中加入成员接口	<p>方法一：</p> <ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface eth-trunk trunk-id</b>，进入 Trunk 接口视图。</li> <li>3. 执行命令 <b>add interface-type { interface-number1 [ to interface-number2 ]}</b>，增加成员接口。</li> <li>4. 结束。</li> </ol> <p>方法二：</p> <ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface interface-type interface-number</b>，进入接口视图。</li> <li>3. 执行命令 <b>join trunk trunk-id</b>，将当前接口加入 Trunk。</li> <li>4. 结束。</li> </ol>
(可选)配置	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> </ol>

目的	步骤
负载分担方式	<ol style="list-style-type: none"> <li>2. 执行命令 <b>interface eth-trunk trunk-id</b>, 进 trunk 接口视图;</li> <li>3. 执行命令 <b>load-balance { dst-ip   dst-mac   src-ip   src-mac   src-dst-ip   src-dst-mac }</b>, 配置 Trunk 的负载分担模式;</li> <li>4. 结束。</li> </ol>
(可选)配置活动接口数阈值	<p>配置活动接口数上限阈值</p> <ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>interface eth-trunk trunk-id</b>, 进 trunk 接口视图;</li> <li>3. 执行命令 <b>active-linknumber max link-number</b>, 配置链路聚合活动接口数上限阈值。</li> <li>4. 结束。</li> </ol> <p>配置活动接口数下限阈值</p> <ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>interface eth-trunk trunk-id</b>, 进 trunk 接口视图;</li> <li>3. 执行命令 <b>active-linknumber min link-number</b>, 配置链路聚合活动接口数上限阈值。</li> <li>4. 结束。</li> </ol>
(可选)配置系统 LACP 优先级	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>lACP system-priority { priority   default }</b>, 配置当前设备的系统 LACP 优先级。;</li> <li>3. 结束。</li> </ol>

附表:

参数	说明	取值
interface-number	指定作为观察端口以太网接口号	整数形式, SC9600 系列交换机支持以下 3 种型号的接口配置范围: SC9603 : 取值范围是 <1-3>/<0-4>/<1-48> SC9608 : 取值范围是 <1-8>/<0-4>/<1-48> SC9612 : 取值范围是 <1-12>/<0-4>/<1-48>
trunk-id	聚合组 ID	整数形式, 取值范围是 1~128
link-number	指定链路聚合活动接口数上限或阈值	整数形式, 取值范围是 1~8, 缺省情况下, 活动接口数上限阈值为 8, 活动接口数下限阈值为 1。
system-priority	指定系统 LACP 优先级	整数形式, 取值范围是 0~65535, 缺省情况下, 系统 LACP 优先级为 32768
port-priority	指定接口 LACP 优先级	整数形式, 取值范围是 0~65535,

参数	说明	取值
		缺省情况下，系统 LACP 优先级为 32768

### 2.6.3 维护及调试

#### 目的

当 LACP 功能不正常，需要进行查看、调试或定位问题时，可以使用本小节操作。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
打开 LACP 调试功能	<ol style="list-style-type: none"> <li>保持当前特权用户视图；</li> <li>执行命令 <b>debug lacp { timer   event   churn   mux   rx   tx   logic   sync   all }</b>打开调试开关；</li> <li>结束。</li> </ol>
关闭 LACP 调试功能	<ol style="list-style-type: none"> <li>保持当前特权用户视图；</li> <li>执行命令 <b>no debug lacp { timer   event   churn   mux   rx   tx   logic   sync   all }</b>打开调试开关；</li> <li>结束。</li> </ol>
查看 LACP 配置文件信息	<ol style="list-style-type: none"> <li>执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface eth-trunk trunk-number</b> 进入接口配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>执行命令 <b>show lacp config</b> 显示 LACP 汇聚配置文件的信息；</li> <li>结束。</li> </ol>
查看 LACP 全部或指定组信息	<ol style="list-style-type: none"> <li>执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或 <b>interface eth-trunk trunk-number</b> 进入接口配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>执行命令 <b>show lacp eth-trunk [ trunk-id ]</b> 显示指定的 LACP 汇聚组或全部 LACP 汇聚组的状态信息；</li> <li>结束。</li> </ol>
查看 LACP 协议相关配置信息	<ol style="list-style-type: none"> <li>执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或 <b>interface eth-trunk trunk-number</b> 进入接口配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>执行命令 <b>show lacp system</b> 显示 LACP 协议相关配置信息；</li> <li>结束。</li> </ol>

附表：

参数	说明	取值
timer	调试 lacp 定时器功能	-

参数	说明	取值
event	调试 lacp 功能	-
churn	调试 lacp churn 功能	-
mux	调试 lacp 聚合器功能	-
rx	接收 lcap 域报文可能产生的错误	-
tx	发送 lcap 域报文可能产生的错误	-
logic	调试 lacp logic 功能	-
sync	调试 lacp sync 功能	-
all	与 lacp 相关的所有功能	-

### 2.6.4 汇聚端口典型举例

#### 组网要求

在两台直接相连 Switch 设备上配置链路聚合组，提高两设备之间的带宽与可靠性，具体

要求如下：

- 两设备间的链路具有冗余备份的能力，当部分链路故障时使用备份链路替代故障链路，保持数据传输的不中断。
- 活动链路具有负载分担的能力。

#### 组网图

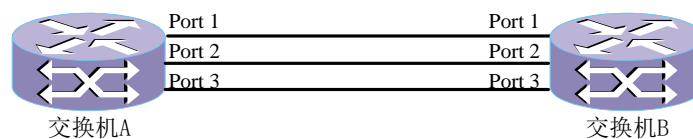


图 2-5 LACP 配置拓扑图

#### 配置步骤

注：两端配置一致，这里仅列出一端配置。

1. 创建 LACP 汇聚组  

```
SC9600(config)#interface eth-trunk 1
SC9600(config-eth-trunk-1)#no shutdown n
```
2. 接口 1-3 加入汇聚组  

```
SC9600(config)#interface gigabitEthernet 1/0/1 to gigabitEthernet 1/0/3
SC9600(config-ge1/0/1->ge1/0/3)#no shutdown n
SC9600(config-ge1/0/1->ge1/0/3)#join vlan 1 untagged
```

```

SC9600(config-ge1/0/1->ge1/0/3)#join eth-trunk 1/0/1
3. 配置结束，查看汇聚组的信息:
SC9600#show lacp eth-trunk 1
eth-trunk 1:
    LACP Status: master      Port number: 3

gigaetherenet-1/0/1
Port Status: Up and bind
Flag: S – Device is sending Slow LACPDUs
    F – Device is sending fast LACPDUs
Local information:
    Mode      Flags  Priority  AdminKey  OperKey  PortId  State
    active    F      32768    0x19      0x19     0x1     0xa9d7f8
Partner's information:
    Port              Flags  SysPri  PortPri  AdminKey  OperKey  OperPort
OperState DevID
    1                  F      32768    32768    0x0       0x19     0x1
0x9dfb6c 0x00046798185d

gigaetherenet-1/0/2
Port Status: Up and bind
Flag: S – Device is sending Slow LACPDUs
    F – Device is sending fast LACPDUs
Local information:
    Mode      Flags  Priority  AdminKey  OperKey  PortId  State
    active    F      32768    0x19      0x19     0x2     0xa9d7f8
Partner's information:
    Port              Flags  SysPri  PortPri  AdminKey  OperKey  OperPort
OperState DevID
    2                  F      32768    32768    0x0       0x19     0x2
0x9dfb6c 0x00046798185d

gigaetherenet-1/0/3
Port Status: Up and bind
Flag: S – Device is sending Slow LACPDUs
    F – Device is sending fast LACPDUs
Local information:
    Mode      Flags  Priority  AdminKey  OperKey  PortId  State
    active    F      32768    0x19      0x19     0x3     0xa9d7f8
Partner's information:
    Port              Flags  SysPri  PortPri  AdminKey  OperKey  OperPort

```



OperState	DevID							
	3	F	32768	32768	0x0	0x19	0x3	
0x9dfb6c	0x00046798185d							

## 2.7 VLAN 配置

### 2.7.1 VLAN 概述

#### VLAN 的含义

在逻辑上将一个局域网 LAN (Local Area Network) 划分成多个子集，每个子集形成各自的广播域，即虚拟局域网 VLAN (Virtual Local Area Network)。

简而言之，VLAN 是将 LAN 内的设备逻辑地而不是物理地划分为一个个网段，从而实现在一个 LAN 内隔离广播域的技术。

#### VLAN 的功能

- 隔离广播域，减少广播风暴，增强了安全性。
- 在大规模的组网环境中，VLAN 可以将网络故障限制在 VLAN 范围内，增强了网络的健壮性。

### 2.7.2 创建 VLAN

#### 目的

使用本节操作创建 VLAN，创建 VLAN 是配置其他 VLAN 功能的基本前提。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
创建并进入 VLANIF 接口配置视图	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface vlan vlan-id</b> 创建并进入 VLANIF 接口配置视图；</li> <li>3. 结束。</li> </ol>
删除已创建的 VLANIF	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>no vlan vlan-id</b> 删除指定 VLANIF 接口配置视图；</li> <li>3. 结束。</li> </ol>
创建 VLAN 并进入 VLAN 视图	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>vlan vlan-id1 [vlan-id2]</b> 创建一个或多个 VLAN 并进入 VLAN 视图；</li> <li>3. 结束。</li> </ol>

目的	步骤
删除一个或者批量删除多个 VLAN	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>no vlan vlan-id1 [vlan-id2]</b>用来删除一个或者批量删除多个 VLAN;</li> <li>3. 结束。</li> </ol>
切换 VLAN 配置视图	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>vlan vlan-id1 [vlan-id2]</b> 创建一个或多个 VLAN 并进入 VLAN 视图;</li> <li>3. 执行命令 <b>switch vlan vlan-id</b> 在 VLAN 配置视图下创建其他 VLAN, 并进入所创建的 VLAN 配置视图;</li> <li>4. 结束。</li> </ol>

附表:

参数	说明	取值
vlan-id	指定 VLAN 编号	整数形式, 取值范围是 1~4094

### 2.7.3 配置基于接口的 VLAN

#### 目的

使用本节操作配置基于接口的 VLAN。

#### 过程

根据不同目的, 执行相应步骤, 具体参见下表。

目的	步骤
配置接口的缺省 VLAN 并同时加入此 VLAN	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>interface { fastethernet   gigabernet   xgigabernet } interface-number</b> 或 <b>interface eth-trunk trunk-number</b> 进入接口配置视图;</li> <li>3. 执行命令 <b>port default vlan vlan-id</b> 配置接口的缺省 VLAN 并同时加入此 VLAN;</li> <li>4. 结束。</li> </ol>
配置 Hybrid 类型接口所属 VLAN	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>interface { fastethernet   gigabernet   xgigabernet } interface-number</b> 或 <b>interface eth-trunk trunk-number</b> 进入接口配置视图;</li> <li>3. 执行命令 <b>port hybrid vlan vlan-list { tagged   untagged }</b>配置 Hybrid 类型接口所属 VLAN;</li> <li>4. 结束。</li> </ol>
配置 Hybrid 类型接口的缺省 VLAN	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>interface { fastethernet   gigabernet   xgigabernet } interface-number</b> 或 <b>interface eth-trunk trunk-number</b> 进入接口配置视图;</li> <li>3. 执行命令 <b>port hybrid pvid { vlan-id   default }</b>配置 Hybrid 类型接口的缺省 VLAN;</li> <li>4. 结束。</li> </ol>

目的	步骤
配置接口的链路类型，也即接口类型	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b> 或 <b>interface eth-trunk trunk-number</b> 进入接口配置视图；</li> <li>3. 执行命令 <b>port link-type { access   trunk   hybrid   default }</b>配置接口的链路类型；</li> <li>4. 结束。</li> </ol>
配置 Trunk 类型接口加入 VLAN	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b> 或 <b>interface eth-trunk trunk-number</b> 进入接口配置视图；</li> <li>3. 执行命令 <b>port trunk allow-pass vlan vlan-list</b> 配置 Trunk 类型接口加入 VLAN；</li> <li>4. 结束。</li> </ol>
配置 Trunk 类型接口的缺省 VLAN	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b> 或 <b>interface eth-trunk trunk-number</b> 进入接口配置视图；</li> <li>3. 执行命令 <b>port trunk pvid { vlan-id   default }</b>配置 Trunk 类型接口的缺省 VLAN；</li> <li>4. 结束。</li> </ol>

附表：

参数	说明	取值
vlan-id	指定 VLAN 编号	整数形式，取值范围是 1~4094
vlan-list	指定 Trunk 类型接口所属的 VLAN 列表	形如：1,3,5~8，整数形式，取值范围是 1~4094
default	恢复 Trunk 类型接口的缺省 VLAN ID 为默认值	default: 1，默认缺省值为 VLAN1

## 2.7.4 配置基于 MAC 地址的 VLAN

### 目的

使用本节操作配置基于 MAC 地址划分 VLAN。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
使能或去使能接口基于 MAC 地址划分 VLAN 的功能	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b> 或 <b>interface eth-trunk trunk-number</b> 进入接口配置视图；</li> <li>3. 执行命令 <b>mac-vlan { enable   disable }</b>使能或去使能接口基于 MAC 地址</li> </ol>

目的	步骤
	划分 VLAN 的功能； 4. 结束。
配置接口允许基于 MAC 地址的 VLAN 通过	1. 执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b> 或 <b>interface eth-trunk trunk-number</b> 进入接口配置视图； 3. 执行命令 <b>port link-type hybrid</b> 配置接口链路类型为 hybrid； 4. 执行命令 <b>port hybrid vlan vlan-list untagged</b> 配置 Hybrid 类型接口加入基于 MAC 地址的 VLAN； 结束。
配置 MAC 地址与 VLAN 关联，同时可以配置 MAC 地址对应 VLAN 的 802.1p 优先级	1. 执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>mac-vlan mac-address vlan-id priority priority</b> 或执行命令 <b>mac-vlan mac-address vlan-id</b> 配置 MAC 地址与 VLAN 关联，同时可以配置 MAC 地址对应 VLAN 的 802.1p 优先级； 3. 结束。

附表：

参数	说明	取值
mac-address	指定与 VLAN 关联的 MAC 地址	形如 AA:BB:CC:DD:EE:FF，其中 A~F 取值为一位十六进制数
mac-mask	指定 MAC 地址掩码	形如 FF:FF:FF:FF:FF:FF
vlan-id	指定与 MAC 地址关联的 VLAN ID	整数形式，取值范围是 1~4094
priority	指定 MAC 地址对应 VLAN 的 802.1p 优先级	整数形式，取值范围是 0~7，值愈大优先级越高，缺省为 0

## 2.7.5 配置基于 IP 子网的 VLAN

### 目的

使用本节操作配置基于 IP 子网划分 VLAN。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
使能或去使能接口基于 IP 子网划分 VLAN 的功能	1. 执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b> 或 <b>interface eth-trunk trunk-number</b> 进入接口配置视图； 3. 执行命令 <b>ip-subnet-vlan { enable   disable }</b> 使能或去使能接口基于 IP 子网划分 VLAN 的功能； 4. 结束。
配置接口允许基于	1. 执行命令 <b>configure</b> 进入全局配置视图；

目的	步骤
IP 子网的 VLAN 通过	2. 执行命令 <code>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</code> 或 <code>interface eth-trunk trunk-number</code> 进入接口配置视图； 3. 执行命令 <b>port link-type hybrid</b> 配置接口链路类型为 hybrid； 4. 执行命令 <b>port hybrid vlan vlan-list untagged</b> 配置 Hybrid 类型接口加入基于 IP 子网的 VLAN； 结束。
配置基于 IP 子网划分 VLAN，同时可以配置 IP 子网对应 VLAN 的 802.1p 优先级	1. 执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>ip-subnet-vlan ip-address mask-address vlan-id priority priority</b> 或执行命令 <b>ip-subnet-vlan ip-address/mask-length vlan-id priority priority</b> 或执行命令 <b>ip-subnet-vlan ip-address mask-address vlan-id</b> 或执行命令 <b>ip-subnet-vlan ip-address/mask-length vlan-id</b> 配置基于 IP 子网划分 VLAN，同时可以配置 IP 子网对应 VLAN 的 802.1p 优先级； 3. 结束。

附表：

参数	说明	取值
ip-address	指定基于 IP 子网划分 VLAN 依据的源 IP 地址或网络地址	点分十进制格式
mask-address	指定子网掩码	点分十进制格式
vlan-id	指定基于 IP 子网划分的 VLAN ID	整数形式，取值范围是 1~4094
priority	可选项。 指定 IP 地址或网段对应 VLAN 的 802.1p 优先级	整数形式，取值范围是 0~7，值越大优先级越高，缺省值是 0

## 2.7.6 配置基于协议的 VLAN

### 目的

使用本节操作配置基于协议划分 VLAN。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置基于协议划分 VLAN，并指定关联的协议	1. 执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>protocol-vlan protocol-index { ethernet2   snap } ethernet-typevalue</b> 或执行命令 <b>protocol-vlan protocol-index llc dsap dsap-value ssap ssap-value</b> 配置基于协议划分 VLAN，并指定关联的协议； 3. 结束。
配置接口允许基于协议的 VLAN 通过	1. 执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <code>interface { fastethernet   gigaehternet   xgigaehternet }</code>

目的	步骤
	<code>interface-number</code> 或 <code>interface eth-trunk trunk-number</code> 进入接口配置视图； 3. 执行命令 <b>port link-type hybrid</b> 配置接口链路类型为 hybrid； 4. 执行命令 <b>port hybrid vlan <i>vlan-list</i> untagged }</b> 配置 Hybrid 类型接口加入基于协议的 VLAN； 结束。
配置接口关联协议 VLAN	1. 执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <code>interface { fastethernet   gigabitEthernet   xgigabitEthernet } <i>interface-number</i></code> 或 <code>interface eth-trunk <i>trunk-number</i></code> 进入接口配置视图； 3. 执行命令 <b>protocol-vlan <i>protocol-index</i> vid <i>vlan-id</i></b> 或执行命令 <b>protocol-vlan <i>protocol-index</i> vid <i>vlan-id</i> priority <i>priority</i></b> 配置接口关联协议 VLAN； 4. 结束。

附表：

参数	说明	取值
<code>protocol-index</code>	指定协议的索引值	整数形式，取值范围是 1~16
<code>ethernet-typevalue</code>	指定基于其他协议类型划分 VLAN，协议类型由对应十六进制数表示	十六进制数，取值范围是 0x600~0xffff
<code>ethernet2</code>	指定以太网报文的封装格式为 Ethernet 2	-
<code>snap</code>	指定以太网报文的封装格式为 snap	-
<code>llc</code>	指定以太网报文的封装格式为 llc	-
<code>ssap</code>	源服务接入点	-
<code>dsap</code>	目的服务接入点	-
<code>any</code>	任意服务接入点	-
<code>ssap-value</code>	指定源服务接入点取值	十六进制数，取值范围是 0x0~0xff
<code>dsap-value</code>	指定目的服务接入点取值	十六进制数，取值范围是 0x0~0xff
<code>protocol-index</code>	指定协议的索引值	整数形式，取值范围是 1~16
<code>vlan-id</code>	指定关联的协议 VLAN ID	整数形式，取值范围是 1~4094
<code>priority</code>	可选。 指定关联的协议 VLAN ID 优先级	整数形式，取值范围是 0~7

### 2.7.7 配置 VLAN 其他参数

#### 目的

使用本节操作配置 VLAN 相关的其他参数，用户根据实际情况选配。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置 VLANIF 接口的描述信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface vlan <i>vlan-id</i></b> 创建并进入 VLANIF 接口配置视图；</li> <li>3. 执行命令 <b>alias <i>description</i></b> 配置 VLANIF 接口的描述信息；</li> <li>4. 结束。</li> </ol>
配置 VLAN 的描述信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>vlan <i>vlan-id1</i> [<i>vlan-id2</i>]</b> 创建一个或多个 VLAN 并进入 VLAN 视图；</li> <li>3. 执行命令 <b>alias <i>description</i></b> 配置 VLAN 的描述信息；</li> <li>4. 结束。</li> </ol>
修改单个或者批量 VLAN 状态	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>static-vlan <i>vlan-id</i></b> 修改单个或者批量 VLAN 状态；</li> <li>3. 结束。</li> </ol>
配置当前接口的外层 Tag 的标签协议标识	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } <i>interface-number</i></b> 或 <b>interface eth-trunk <i>trunk-number</i></b> 进入接口配置视图；</li> <li>3. 执行命令 <b>tpid { <i>protocol-id</i>   standard }</b> 配置当前接口的外层 Tag 的标签协议标识；</li> <li>4. 结束。</li> </ol>
配置在 VLAN 转发过程中对未知单播包的处理	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>vlan <i>vlan-id1</i> [<i>vlan-id2</i>]</b> 创建一个或多个 VLAN 并进入 VLAN 视图；</li> <li>3. 执行命令 <b>unknown-unicast { forward   drop }</b> 用来配置在 VLAN 转发过程中对未知单播包的处理；</li> <li>4. 结束。</li> </ol>
配置在 VLAN 转发过程中对未知单播包的处理	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>unknown-unicast vlan <i>vlan-list</i> { forward   drop }</b> 或执行命令 <b>vlan <i>vlan-list</i> unknown-unicast { forward   drop }</b> 或执行命令 <b>vlan <i>vlan-id</i> unknown-unicast { forward   drop }</b> 配置在 VLAN 转发过程中对未知单播包的处理；</li> <li>3. 结束。</li> </ol>
配置在汇聚端口 VLAN 转发过程中对未知单播包在 trunk 接口上负载分担模式的处理	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>unknown-unicast load-balance { <i>dst-mac</i> <i>src-mac</i> <i>srcdst-mac</i> <i>schedule-profile name</i>  default }</b> 配置在汇聚端口 VLAN 转发过程中对未知单播包在 trunk 接口上负载分担模式的处理；</li> <li>3. 结束。</li> </ol>
配置在 VLAN 转发过程中对未知多播包的处理	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>vlan <i>vlan-id1</i> [<i>vlan-id2</i>]</b> 创建一个或多个 VLAN 并进入 VLAN 视图；</li> <li>3. 执行命令 <b>unknown-multicast { forward   drop }</b> 配置在 VLAN 转发过程中对未知多播包的处理；</li> <li>4. 结束。</li> </ol>
配置在 VLAN 转	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> </ol>

目的	步骤
发过程中对未知单播包的处理	2. 执行命令 <code>unknown-multicast vlan vlan-list { forward   drop }</code> 或执行命令 <code>vlan vlan-list unknown-multicast { forward   drop }</code> 或执行命令 <code>vlan vlan-id unknown-multicast { forward   drop }</code> 配置在 VLAN 转发过程中对未知单播包的处理; 3. 结束。
配置接口上 VLAN 匹配的优先级	1. 执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <code>interface { fastethernet   gigasethernet   xgigasethernet } interface-number</code> 或 <code>interface eth-trunk trunk-number</code> 进入接口配置视图; 3. 执行命令 <code>vlan precedence { mac-vlan   ip-subnet-vlan }</code> 配置接口上 VLAN 匹配的优先级; 4. 结束。
配置 VLAN 的类型为普通 VLAN	1. 执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <code>interface vlan vlan-id</code> 创建并进入 VLANIF 接口配置视图或执行命令 <code>vlan vlan-id1 [vlan-id2]</code> 创建一个或多个 VLAN 并进入 VLAN 视图; 3. 执行命令 <code>vlan normal</code> 配置 VLAN 的类型为普通 VLAN; 4. 结束。

附表:

参数	说明	取值
description	指定 VLANIF 接口的描述信息	字符串形式, 不支持空格, 区分大小写, 字符串长度范围是 1~32
vlan-id	指定关联的协议 VLAN ID	整数形式, 取值范围是 1~4094
protocol-id	当前接口的外层 Tag 的标签协议标识	十六进制数形式, 取值范围是 <0x600-0xffff>
standard	标准值	0x8100
schedule-profile	已创建的增强负载分担模板模式	-
Name	具体模版名称	-
src-mac	指定 trunk 基于源 MAC 地址进行负载分担	-
dst-mac	指定 trunk 基于目的 MAC 地址进行负载分担	-
srcdst-mac	指定 trunk 基于源 MAC 与目的 MAC 地址的异或进行负载分担	-
default	默认模式	默认负载分担模式为 srcdst-mac 模式
mac-vlan	指定优先根据基于 MAC 划分 VLAN 来匹配 VLAN	-
ip-subnet-vlan	指定优先根据基于 IP 子网划分 VLAN 来匹配 VLAN	-



## 2.7.8 维护及调试

### 目的

当 VLAN 功能不正常，需要进行查看、调试或定位问题时，可以使用本小节操作。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
打开或关闭 VLAN 或 VLANIF 接口的流量统计开关	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface vlan <i>vlan-id</i></b> 创建并进入 VLANIF 接口配置视图或执行命令 <b>vlan <i>vlan-id1</i> [<i>vlan-id2</i>]</b> 创建一个或多个 VLAN 并进入 VLAN 视图；</li> <li>3. 执行命令 <b>statistic { enable   disable }</b> 打开或关闭 VLAN 或 VLANIF 接口的流量统计开关；</li> <li>4. 结束。</li> </ol>
清除指定 VLAN 的统计信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>reset vlan <i>vlan-id</i> statistic</b> 清除指定 VLAN 的统计信息；</li> <li>3. 结束。</li> </ol>
查看基于 MAC 地址划分 VLAN 的配置信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，执行命令 <b>interface { fastethernet   gigasethernet   xgigasethernet } <i>interface-number</i></b> 或 <b>interface eth-trunk <i>trunk-number</i></b> 进入接口配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show mac-vlan</b> 或执行命令 <b>show mac-vlan <i>vlan-id</i></b> 或执行命令 <b>show mac-vlan interface</b> 查看基于 MAC 地址划分 VLAN 的配置信息；</li> <li>3. 结束。</li> </ol>
查看基于 IP 子网划分 VLAN 的配置信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，执行命令 <b>interface { fastethernet   gigasethernet   xgigasethernet } <i>interface-number</i></b> 或 <b>interface eth-trunk <i>trunk-number</i></b> 进入接口配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show ip-subnet-vlan</b> 或执行命令 <b>show ip-subnet-vlan <i>vlan-id</i></b> 或执行命令 <b>show ip-subnet-vlan interface</b> 查看基于 IP 子网划分 VLAN 的配置信息；</li> <li>3. 结束。</li> </ol>
查看基于协议划分 VLAN 的配置信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，执行命令 <b>interface { fastethernet   gigasethernet   xgigasethernet } <i>interface-number</i></b> 或 <b>interface eth-trunk <i>trunk-number</i></b> 进入接口配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show protocol-vlan</b> 或执行命令 <b>show protocol-vlan <i>protocol-index</i></b> 或执行命令 <b>show protocol-vlan interface</b> 查看基于协议划分 VLAN 的配置信息；</li> <li>3. 结束。</li> </ol>

目的	步骤
查看 VLAN 接口配置信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface vlan <i>vlan-id</i></b> 进入 VLANIF 接口配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show interface vlan <i>vlan-id</i> config</b> 或执行命令 <b>show interface vlan config</b> 查看 VLAN 接口配置信息；</li> <li>3. 结束。</li> </ol>
查看 VLAN 的相关信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>vlan <i>vlan-id</i></b> 进入 VLAN 配置视图，或执行命令 <b>interface vlan <i>vlan-id</i></b> 进入 VLANIF 接口配置视图，执行命令 <b>interface { fastethernet   gigasethernet   xgigasethernet } <i>interface-number</i></b> 或 <b>interface eth-trunk <i>trunk-number</i></b> 进入接口配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show vlan</b> 或执行命令 <b>show vlan all</b> 或执行命令 <b>show vlan all <i>vlan-list</i></b> 或执行命令 <b>show vlan property</b> 或执行命令 <b>show vlan property <i>vlan-list</i></b> 或执行命令 <b>show vlan verbose</b> 或执行命令 <b>show vlan <i>vlan-id</i> verbose</b> 查看 VLAN 的相关信息；</li> <li>3. 结束。</li> </ol>
查看 VLAN 统计信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，执行命令 <b>interface { fastethernet   gigasethernet   xgigasethernet } <i>interface-number</i></b> 或 <b>interface eth-trunk <i>trunk-number</i></b> 进入接口配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show vlan <i>vlan-id</i> statistic</b> 或执行命令 <b>show vlan <i>vlan-id</i> statistic slot <i>slot-id</i></b> 查看 VLAN 统计信息；</li> <li>3. 结束。</li> </ol>

附表：

参数	说明	取值
vlan-id	指定 VLAN ID	整数形式，取值范围是 1~4094
vlan-list	指定 VLAN 列表	整数形式，形如：1,2,3-5
slot-id	指定槽位号	SC9600 系列交换机支持以下 3 种型号的槽位配置范围： SC9603：取值范围是<1-3> SC9608：取值范围是<1-8> SC9612：取值范围是<1-12>

## 2.7.9 配置举例

### 组网要求

某企业用户，研发部和市场的员工电脑和部门服务器分别使用交换机 SC9600A 和 SC9600B 互连。现要求研发部的员工电脑能访问部门服务器 Server1，市场部的员工电脑能访问部门服务器 Server2，两个部门间不允许相互通信。

- 根据需求，需划分 2 个 VLAN，分别为 VLAN 100、VLAN 200，并分别设置 VLAN 描述符为“Development100”、“Market200”；
- 将研发部员工电脑和 Server1 划分到 VLAN 100 中；
- 将市场部员工电脑和 Server2 划分到 VLAN 200 中。

组网图

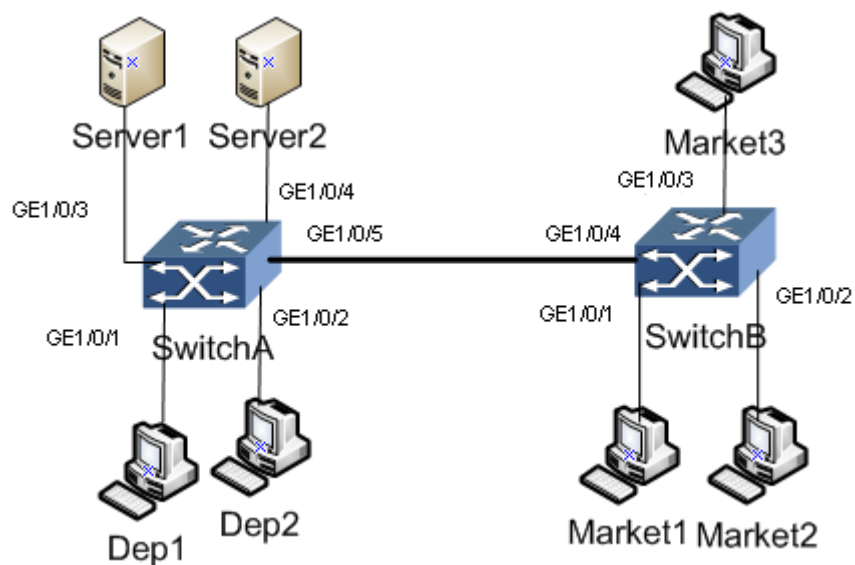


图 2-6 VLAN 配置拓扑图

配置步骤

1、配置 SC9600A。

```
SC9600A#configure
```

```
%Enter configuration commands.End with Ctrl+Z or command "quit" & "end"
```

```
//创建 VLAN100 并进入其配置视图。
```

```
SC9600A(config)#interface vlan 100
```

```
SC9600A(config-vlan-100)#
```

```
//配置 VLAN100 描述信息为 Development100。
```

```
SC9600A(config-vlan-100)#description Development100
```

//向 VLAN100 中加入端口 Ge1/0/1、Ge1/0/2 和 Ge1/0/3，并设置 VLAN100 为端口 Ge1/0/1、Ge1/0/2 和 Ge1/0/3 的 PVID 值。

```
SC9600A(config-vlan-100)#quit
```

```
SC9600A(config)#
```

```
SC9600A(config)#interface gigabitEthernet 1/0/1
```

```
SC9600A(config-gigabitEthernet 1/0/1)#port hybrid vlan 100 untagged
```

```
SC9600A(config-gigabitEthernet 1/0/1)#port hybrid pvid 100
```

```
SC9600A(config-gigabitEthernet 1/0/1)#quit
```

```
SC9600A(config)#interface gigabitEthernet 1/0/2
```

```
SC9600A(config-gigabitEthernet 1/0/2)#port hybrid vlan 100 untagged
```

```
SC9600A(config-gigabitEthernet 1/0/2)#port hybrid pvid 100
```

```
SC9600A(config-gigabitEthernet 1/0/2)#quit
```

```
SC9600A(config)#interface gigabitEthernet 1/0/3
```

```
SC9600A(config-gigabitEthernet 1/0/3)#port hybrid vlan 100 untagged
```

```
SC9600A(config-gigabitEthernet 1/0/3)#port hybrid pvid 100
```

```
SC9600A(config-gigabitEthernet 1/0/3)#quit
```

```
SC9600A(config)#
```

//创建 VLAN200 并进入其视图。

```
SC9600A(config)#interface vlan 200
```

```
SC9600A(config-vlan-200)#
```

//配置 VLAN200 描述信息为 Market200。

```
SC9600A(config-vlan-200)#description Market200
```

//向 VLAN200 中加入端口 Ge1/0/4、Ge1/0/5，并设置 VLAN200 为端口 Ge1/0/4、Ge1/0/5 的 PVID 值。

```
SC9600A(config-vlan-100)#quit
```

```
SC9600A(config)#
```

```
SC9600A(config)#interface gigabitEthernet 1/0/4
```

```
SC9600A(config-gigabitEthernet 1/0/4)#port hybrid vlan 200 untagged
```

```
SC9600A(config-gigabitEthernet 1/0/4)#port hybrid pvid 200
```

```
SC9600A(config-gigabitEthernet 1/0/4)#quit
```

```
SC9600A(config)#interface gigabitEthernet 1/0/5
```

```
SC9600A(config-gigabitEthernet 1/0/5)#port hybrid vlan 200 tagged
```

```
SC9600A(config-gigabitEthernet 1/0/5)#port hybrid pvid 200
```

```
SC9600A(config-gigabitEthernet 1/0/5)#quit
```

2、配置 SC9600B。

//创建 VLAN200 并进入其配置视图。

```
SC9600B#configure
```

```
    %Enter configuration commands.End with Ctrl+Z or command "quit" & "end"
```

```
SC9600B(config)#interface vlan 200
```

//配置 VLAN200 描述信息为 Market200。

```
SC9600B(config-vlan-200)#description Market200
```

//向 VLAN100 中加入端口 Ge1/0/1、Ge1/0/2、Ge1/0/3 和 Ge1/0/4，并设置 VLAN100 为端口 Ge1/0/1、Ge1/0/2 和 Ge1/0/3 的 PVID 值。

```
SC9600B(config-vlan-100)#quit
```

```
SC9600B(config)#
```

```
SC9600B(config)#interface gigabitEthernet 1/0/1
```

```
SC9600B(config-gigabitEthernet-1/0/1)#port hybrid vlan 200 untagged
```

```
SC9600B(config-gigabitEthernet-1/0/1)#port hybrid pvid 200
```

```
SC9600B(config-gigabitEthernet-1/0/1)#quit
```

```
SC9600B(config)#interface gigabitEthernet 1/0/2
```

```
SC9600B(config-gigabitEthernet-1/0/2)#port hybrid vlan 200 untagged
```

```
SC9600B(config-gigabitEthernet-1/0/2)#port hybrid pvid 200
```

```
SC9600B(config-gigabitEthernet-1/0/2)#quit
```

```
SC9600B(config)#interface gigabitEthernet 1/0/3
```

```
SC9600B(config-gigabitEthernet-1/0/3)#port hybrid vlan 200 untagged
```

```
SC9600B(config-gigabitEthernet-1/0/3)#port hybrid pvid 200
```

```
SC9600B(config-gigabitEthernet-1/0/3)#quit
```

```
SC9600B(config)#interface gigabitEthernet 1/0/4
```

```
SC9600B(config-gigabitEthernet-1/0/4)#port hybrid vlan 200 tagged
```

```
SC9600B(config-gigabitEthernet-1/0/4)#quit
```

```
SC9600B(config)#
```

## 2.8 VLAN 转换配置

### 2.8.1 绑定 VLAN 转换条目到接口

#### 目的

本节介绍如何绑定 VLAN 转换条目到接口。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
将 VLAN 转换条目绑定到接口	1. 执行命令 <code>configure</code> ，进入全局视图。 2. 执行命令 <code>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</code> ，进入接口配置视图。 3. 执行以下命令（任一）： <code>join translation-vlan map-index { in   out }</code> <code>join translation-vlan map-indexlist { in   out }</code>	参数说明参见下表
解除绑定到接口的 VLAN 转换条目	1. 执行命令 <code>configure</code> ，进入全局视图。 2. 执行以下命令（任一）： <code>no join translation-vlan map-index { in   out }</code> <code>no join translation-vlan map-indexlist { in   out }</code>	

附表：

参数	说明	取值
map-index	指定 VLAN 转换条目索引号	整数形式，取值范围是 1~8192
map-indexlist	指定多个 VLAN 转换条目索引号	整数形式，形如 1,2,5-10，取值范围是 1~8192
in	表示 VLAN 转换条目在接口入方向起作用	-
out	表示 VLAN 转换条目在接口出方向起作用	-

## 2.8.2 配置或删除 VLAN 转换条目

目的

本节介绍如何配置或删除 VLAN 转换条目。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
----	----	------

目的	步骤	参数说明
配置 VLAN 转换条目	1. 执行命令 <code>configure</code> ，进入全局视图。 2. 执行以下命令（任一）： <code>translation-vlan map-index inner-vlan vlan-id delete { inner   outer }</code> <code>translation-vlan map-index inner-vlan vlan-id delete { inner   outer } nto1</code> <code>translation-vlan map-index outer-vlan { vlan-id   vlan-id1/vlan-id2 } delete { inner   outer } [nto1]</code>	参数说明见下表
删除 VLAN 转换条目	1. 执行命令 <code>configure</code> ，进入全局视图。 2. 执行以下命令 <code>no translation-vlan map-index</code> <code>no translation-vlan all</code>	

附表：

参数	说明	取值
map-index	指定 VLAN 转换条目索引号	整数形式，取值范围是 1~8192
inner-vlan	表示匹配内层 VLAN	-
vlan-id	配置待匹配的指定 VLAN ID	整数形式，取值范围是 1~4094
inner	表示删除内层 VLAN Tag	-
outer	表示删除外层 VLAN Tag	-
nto1	配置该条目为 n:1 的条目	-
delete { inner   outer }	表示删除内层或外层 VLAN Tag	-

### 2.8.3 查看 VLAN 转换条目相关信息

#### 目的

本节介绍如何查看 VLAN 转换条目相关信息。

本操作帮助用户用户可以查看设备上的接口是否绑定有 VLAN 转换条目，包括 VLAN 转换条目的 index 信息、接口是入方向绑定还是出方向绑定或是双向绑定转换条目。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
----	----	------

目的	步骤	参数说明
查看 VLAN 转换条目相关信息	1. 执行命令进入普通用户视图或者特权用户视图。 2. 执行以下命令（任一）： show translation-vlan interface show translation-vlan interface vlan-list show translation-vlan interface all show translation-vlan mapped show translation-vlan mapped vlan-list	vlan-list: 指定 VLAN 列表，可选参数。支持输入多个 VLAN ID。支持形如：1,3,5-10 的输入，各 VLAN ID 之间以','及 '-' 分隔，其中 '-' 表示输入的是一个范围；

### 2.8.4 配置举例

#### 组网要求

接入网中，家庭用户通过家庭网关连接交换机 SC9600A，最后接入运营商网络。

User1 使用的语音业务数据通过家庭网关带有 VLAN10、Internet 上网业务数据带有 VLAN11；User2 使用的 Internet 上网业务数据通过家庭网关带有 VLAN12。

通过交换机 SC9600A 后，User1 的语音业务数据带有的 VLAN10 被转换成运营商网络的 VLAN100，Internet 上网业务数据带有的 VLAN11 被转换成运营商网络的 VLAN101；User2 的 Internet 上网业务数据带有的 VLAN12 被转换成运营商网络的 VLAN101。

#### 组网图

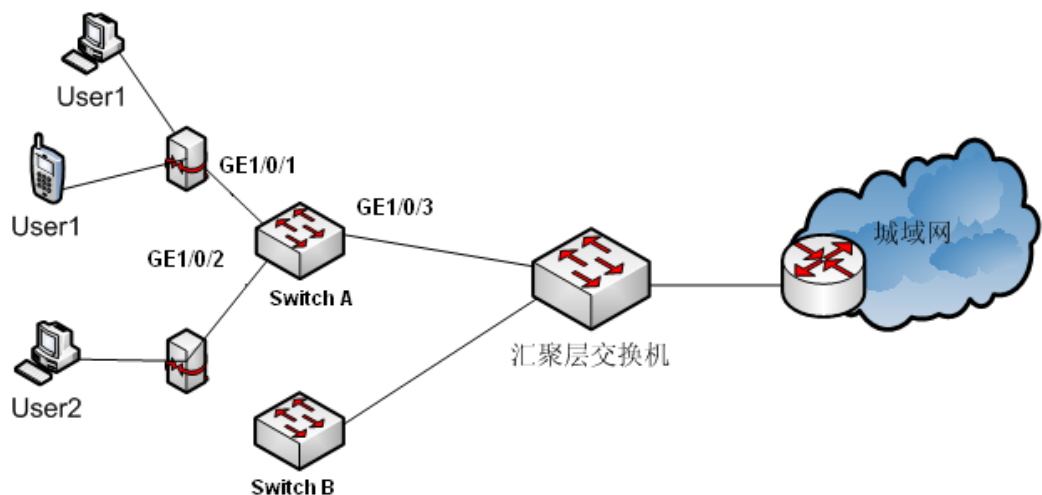


图 2-7 VLAN 转换配置拓扑图

#### 配置步骤



1. 创建接入网用户侧 VLAN;
2. 创建网络运营商 VLAN;
3. 创建 VLAN 转换规则表;
4. 将连接用户侧的端口加入用户侧 VLAN 和运营商 VLAN;
5. 在端口上添加转换规则表;
6. 将上联端口加入网络运营商 VLAN。

配置 SC9600A。

```
SC9600A#configure
%Enter configuration commands.End with Ctrl+Z or command "quit" & "end"
//创建接入网用户侧 VLAN10、VLAN11、VLAN12。
SC9600A(config)#interface vlan 10
SC9600A(config-vlan-10)#quit
SC9600A(config)#interface vlan 11
SC9600A(config-vlan-11)#quit
SC9600A(config)#interface vlan 12
SC9600A(config-vlan-12)#quit
SC9600A(config)#
//创建运营商网络 VLAN100、VLAN101。
SC9600A(config)#interface vlan 100
SC9600A(config-vlan-100)#quit
SC9600A(config)#interface vlan 101
SC9600A(config-vlan-101)#quit
SC9600A(config)#
//创建 VLAN 转换规则表 VLAN10->VLAN100，VLAN11->VLAN101，
VLAN12->VLAN101。
SC9600A(config)#
SC9600A(config)# translation-vlan 1 outer-vlan 10 replace outer 100
SC9600A(config)# translation-vlan 2 outer-vlan 11 replace outer 101
SC9600A(config)# translation-vlan 3 outer-vlan 12 replace outer 101
//进入端口 GE1/0/1，将端口加入 VLAN10、VLAN 11、VLAN100、VLAN101。
SC9600A(config)#interface gigabitEthernet 1/0/1
```

```
SC9600A(config-ge1/0/1)#port hybrid vlan 10 tagged
SC9600A(config-ge1/0/1)#port hybrid vlan 11 tagged
SC9600A(config-ge1/0/1)#port hybrid vlan 100 untagged
SC9600A(config-ge1/0/1)#port hybrid vlan 101 untagged
//将 VLAN 转换条目绑定到接口。
SC9600A(config-ge1/0/1)#join translation-vlan 1 in
SC9600A(config-ge1/0/1)#join translation-vlan 2 in
SC9600A(config-ge1/0/1)#quit
//进入端口 GE1/0/2，将端口加入 VLAN12、VLAN101。
SC9600A(config)#interface gigabitEthernet 1/0/2
SC9600A(config-ge1/0/2)#port hybrid vlan 12 tagged
SC9600A(config-ge1/0/2)#port hybrid vlan 101 untagged
SC9600A(config-ge1/0/2)# join translation-vlan 3 in
SC9600A(config-ge1/0/2)#quit
SC9600A(config)#
// 创建 VLAN 转换规则表 VLAN101->VLAN10，VLAN101->VLAN11，
VLAN101->VLAN12。
SC9600A(config)#
SC9600A(config)# translation-vlan 1 outer-vlan 100 replace outer 10
SC9600A(config)# translation-vlan 2 outer-vlan 101 replace outer 11
SC9600A(config)#translation-vlan 3 outer-vlan 101 replace outer 12
//进入端口 GE1/0/3，将端口加入 VLAN10、VLAN 11、VLAN12、VLAN100、VLAN101。
SC9600A(config)#interface gigabitEthernet 1/0/3
SC9600A(config-ge1/0/3)#port trunk allow-pass vlan 10 untagged
SC9600A(config-ge1/0/3)#port trunk allow-pass vlan 11 untagged
SC9600A(config-ge1/0/3)#port trunk allow-pass vlan 12 untagged
SC9600A(config-ge1/0/3)#port trunk allow-pass vlan 100 tagged
SC9600A(config-ge1/0/3)#port trunk allow-pass vlan 101 tagged
//将 VLAN 转换条目绑定到接口。
SC9600A(config-ge1/0/3)#join translation-vlan 1 in
SC9600A(config-ge1/0/3)#join translation-vlan 2 in
SC9600A(config-ge1/0/3)#join translation-vlan 3 in
SC9600A(config-ge1/0/3)#
SC9600A(config-ge1/0/3)#quit
```

## 2.9 QinQ 配置

QinQ 是指将用户私网 VLAN Tag 封装在公网 VLAN Tag 中,使报文带着两层 VLAN Tag 穿越运营商的骨干网络(公网)。在公网中报文只根据外层 VLAN Tag(即公网 VLAN Tag 传播,用户的私网 VLAN Tag 被屏蔽。

QinQ 主要可以解决如下几个问题:

- 缓解日益紧缺的公网 VLAN ID 资源问题。
- 用户可以规划自己的私网 VLAN ID, 不会导致和公网 VLAN ID 冲突。
- 为小型城域网或企业网提供一种较为简单的二层 VPN 解决方案。

### 2.9.1 配置接口的双标签工作状态

#### 目的

本节介绍配置接口的双标签工作状态。

#### 过程

根据不同目的, 执行相应步骤, 具体参见下表。

目的	步骤	参数说明
配置接口的双标签工作状态, 在实际的配置过程中要将 access 接口置为 tagged 模式。	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code>, 进入全局视图。</li> <li>2. 执行命令 <code>interface interface-type interface-number</code> 进入指定某一接口的配置视图。</li> <li>3. 执行命令 <code>dot1q-tunnel (enable disable)</code>。</li> </ol>	无

### 2.9.2 配置当前接口 TPID

#### 目的

本节介绍如何配置当前接口的外层 Tag 的标签协议标识。

由于不同的厂商在实现 QinQ 功能时, 对外层 Tag 采用了不同的协议类型, 因此当需要实现 SC9600 和其它厂商设备对接时, 使用 `tpid` 命令配置当前接口的外层 Tag 的标签协议标识。

#### 过程

根据不同目的, 执行相应步骤, 具体参见下表。

目的	步骤	参数说明
----	----	------

目的	步骤	参数说明
配置当前接口 TPID	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code>, 进入全局视图。</li> <li>2. 执行命令 <code>interface interface-type interface-number</code> 进入指定某一接口的配置视图。</li> <li>3. 执行命令 <code>tpid { standard   protocol-id }</code></li> </ol>	缺省情况下, 接口的 <code>tpid</code> 值为 <code>0x8100</code> 。 <code>protocol-id</code> : 当前接口的外层 Tag 的标签协议标识, 十六进制数形式, 取值范围是 <code>&lt;0x600-0xffff&gt;</code> <code>standard</code> : 标准值, <code>0x8100</code>

## 2.10 PVLAN 配置

### 2.10.1 PVLAN 简介

#### 产生背景

随着网络的迅速发展, 用户对于网络数据通信的安全性提出了更高的要求, 诸如防范黑客攻击、控制病毒传播等, 都要求保证网络用户通信的相对安全性; 传统的解决方法是给每个客户分配一个 VLAN 和相关的 IP 子网, 通过使用 VLAN, 每个客户被从第 2 层隔离开, 可以防止任何恶意的行为和 Ethernet 的信息探听。然而, 这种分配每个客户单一 VLAN 和 IP 子网的模型造成了巨大的可扩展方面的局限。这些局限主要有下述几方面:

1. VLAN 的限制: 交换机固有的 VLAN 数目的限制;
2. 复杂的 STP: 对于每个 VLAN, 每个相关的 Spanning Tree 的拓扑都需要管理;
3. IP 地址的紧缺: IP 子网的划分势必造成一些 IP 地址的浪费;
4. 路由的限制: 每个子网都需要相应的默认网关的配置。

而 pVlan 的产生, 不仅满足了用户通信安全的需要, 也很好的解决了上述问题。

#### 概念

PVLAN 即私有 VLAN (Private VLAN), PVLAN 采用两层 VLAN 隔离技术, 只有上层 VLAN 全局可见, 下层 VLAN 相互隔离。每个 pVLAN 包含 2 种 VLAN : 主 VLAN (primary VLAN) 和辅助 VLAN (Secondary VLAN), 其中主 VLAN 又称为上层 vlan, 全局可见; 辅助 VLAN (Secondary VLAN) 即下层 VLAN, 又包含两种类型: 隔离 VLAN (isolated VLAN) 和团体 VLAN (community VLAN), 其通信范围各不相同。

#### 目的

通过将端口划分到 pvlan 的各个子 vlan 的方法,不仅可以有效的限制各端口的通信范围,同时节省了有限的 vlan 资源和 IP 资源,为网络安全提供了保障。

### VLAN 类型

**Primary VLAN:** 每个 PVLAN 仅有一个 Primary VLAN, PVLAN 中的所有端口都从属于该 Primary VLAN。上行设备只能识别该 VLAN,而不能识别其下层的 VLAN。该 VLAN 可以和所有它所关联的 isolated VLAN, community VLAN 通信。

**Isolated VLAN:** 每个 PVLAN 仅有一个 Isolated VLAN, 其中的端口在 2 层不能互相通信。

**Community VLAN:** 同一个 community VLAN 中的各端口可以互相通信,也可以与 pVLAN 中的 promiscuous 端口通信,但不能和 pVlan 中其它 community VLAN 中的端口通信(每个 pVLAN 可以有多个 community VLAN)。

### 端口类型

处在 PVLAN 中的交换机物理端口,有两种接口类型。

- 1) 混杂端口 (Promiscuous Port)
- 2) 主机端口 (Host Port)

其中“混杂端口”是隶属于“Primary VLAN”的;“主机端口”是隶属于“Secondary VLAN”的。因为“Secondary VLAN”是具有两种属性的,那么,处于“Secondary VLAN”当中的“主机端口”依“Secondary VLAN”属性的不同而不同,也就是说“主机端口”会继承“Secondary VLAN”的属性。那么由此可知,“主机端口”也分为两类——“isolated 端口”和“community 端口”。

处于 pVLAN 中交换机上的一个物理端口要么是“混杂端口”要么是“isolated”端口,要么就是“community”端口。

### 相关特性

- 一个 promiscuous 端口仅能关联一个 primary VLAN。
- 一个 isolated 端口仅能关联一个二级 VLAN。
- 一个 community 端口仅能关联一个二级 VLAN。
- 一个二级 VLAN 仅能关联一个 primary VLAN。
- 每个 PVLAN 仅包含一个 primary VLAN。
- 多个 PVLAN 可以共存于同一台交换机或同一个交换网上。

- 一个 PVLAN 可以跨多台交换机工作，这些交换机通过交换机间的连接端口相连，在多设备间进行 PVLAN 数据传输。
- PVLAN 与普通的 VLAN 间不提供交互功能。

实现原理

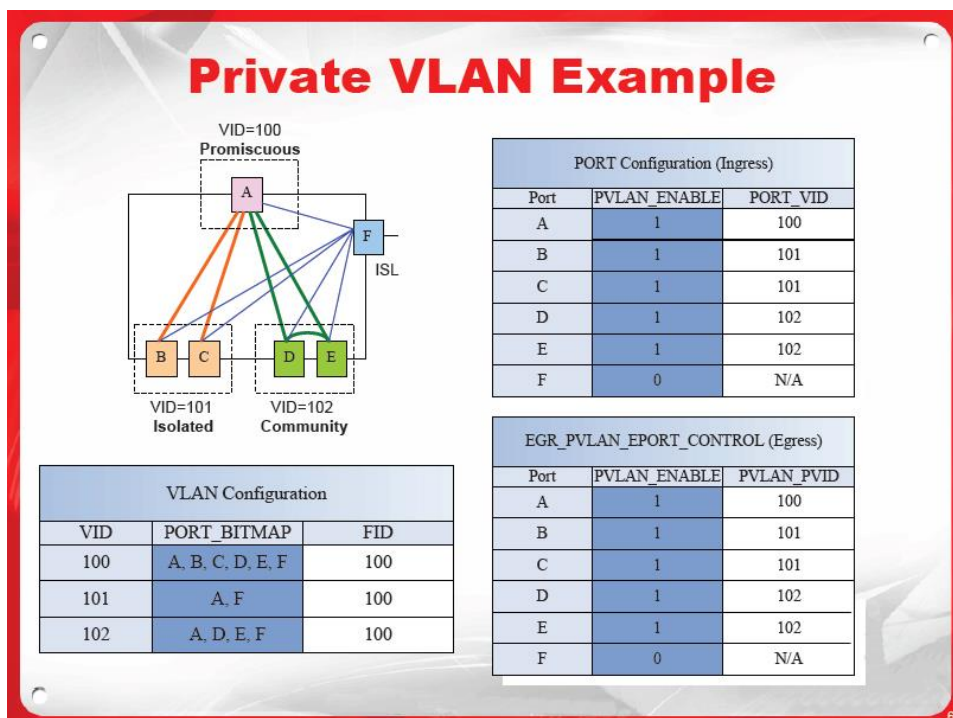


图 2-8 PVLAN 实现原理图

其中，从 B 或 C 出去的 untagged 报文被打上 PVID 为 101 的标签，只能被 A 接收。接收后将旧的 tag 值换为 A 的 PVID 即 100，转发出去。D 和 E 加入 VLAN102，从 D 或 E 出去的 untagged 报文被打上 PVID 为 102 的标签后，可在该 VLAN 内传输。而由于每个 VLAN 中都包含端口 A，故从 A 下发的报文可以到达下属的任何一个端口。

## 2.10.2 PVLAN 配置

### 2.10.2.1 PVLAN 关联配置

#### 2.10.2.1.1 主 VLAN 与辅助 VLAN 建立关联

目的

本节介绍如何将主 VLAN 与辅助 VLAN 建立关联。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
主 VLAN 与辅助 VLAN 建立关联	<ol style="list-style-type: none"> <li>在特权用户视图下执行命令 <code>vlan vlan-number</code>，进入 VLAN 配置视图；</li> <li>执行命令 <code>private-vlan association { add   remove } vlan-list</code></li> </ol>	<p><code>vlan-number</code>: VLAN ID，整数形式，取值范围是 1~4094；</p> <p><code>add</code>: 配置辅助 VLAN 列表与主 VLAN 相关联；</p> <p><code>remove</code>: 解除指定辅助 VLAN 列表与主 VLAN 的关联关系；</p> <p><code>vlan-list</code>: 辅 VLAN 列表，多个连续 VLAN 可以-连接起始和结束 VLAN，不连续 VLAN 之间以“，”分隔；整数形式，取值范围为 1-4094；</p>

2.10.2.1.2 建立混杂端口与主辅 vlan 之间的关联关系

目的

本节介绍如何建立混杂端口与主辅 vlan 之间的关联关系。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
建立混杂端口与主辅 vlan 之间的关联关系	<ol style="list-style-type: none"> <li>在特权用户视图下执行命令 <code>config</code>，进入全局配置视图；</li> <li>执行命令 <code>interface interface-type interface-number</code>，进入以太网或 trunk 接口配置视图；</li> <li>执行命令 <code>private-vlan mapping vlan-number { add   remove } vlan-list</code></li> </ol>	<p><code>interface-type</code>: 包括 3 种端口类型：  <code>fastethernet</code>  <code>gigaethernet</code>  <code>xgigaethernet</code></p> <p><code>interface-number</code>: SC9600 系列交换机支持以下 3 种型号的接口配置范围：  <code>SC9603</code> : 取值范围是 &lt;1-3&gt;/&lt;0-4&gt;/&lt;1-48&gt;  <code>SC9608</code> : 取值范围是 &lt;1-8&gt;/&lt;0-4&gt;/&lt;1-48&gt;  <code>SC9612</code> : 取值范围是 &lt;1-12&gt;/&lt;0-4&gt;/&lt;1-48&gt;</p> <p><code>vlan-number</code>: VLAN ID，整数形式，取值范围是 1~4094；</p> <p><code>add</code>: 配置辅助 VLAN 列表与主 VLAN 相关联；</p>

目的	步骤	参数说明
		<p><b>remove:</b> 解除指定辅助 VLAN 列表与主 VLAN 的关联关系;</p> <p><b>vlan-list:</b> 辅 VLAN 列表, 多个连续 VLAN 可以-连接起始和结束 VLAN, 不连续 VLAN 之间以“,”分隔; 整数形式, 取值范围为 1-4094;</p>

### 2.10.2.1.3 配置将主机端口关联到主 VLAN 和辅助 VLAN

#### 目的

本节介绍如何配置将主机端口关联到主 VLAN 和辅助 VLAN。

#### 过程

根据不同目的, 执行相应步骤, 具体参见下表。

目的	步骤	参数说明
配置将主机端口关联到主 VLAN 和辅助 VLAN	<ol style="list-style-type: none"> <li>在特权用户视图下执行命令 <b>config</b>, 进入全局配置视图;</li> <li>执行命令 <b>interface interface-type interface-number</b>, 进入以太网或 trunk 接口配置视图;</li> <li>执行命令 <b>private-vlan host-association vlan-number1 vlan-number2</b></li> </ol>	<p><b>interface-type:</b> 包括 3 种端口类型:                      fastethernet                      gigaehternet                      xgigaehternet</p> <p><b>interface-number:</b> SC9600 系列交换机支持以下 3 种型号的接口配置范围:                      SC9603 : 取值范围是 &lt;1-3&gt;/&lt;0-4&gt;/&lt;1-48&gt;                      SC9608 : 取值范围是 &lt;1-8&gt;/&lt;0-4&gt;/&lt;1-48&gt;                      SC9612 : 取值范围是 &lt;1-12&gt;/&lt;0-4&gt;/&lt;1-48&gt;</p> <p><b>vlan-number1:</b> 指定主 VLAN ID, 整数形式, 取值范围是 1~4094;</p> <p><b>vlan-number2:</b> 指定辅助 VLAN ID, 整数形式, 取值范围是 1~4094;</p>
解除主机端口与主 VLAN 和辅助 VLAN 的关联	<ol style="list-style-type: none"> <li>在特权用户视图下执行命令 <b>config</b>, 进入全局配置视图;</li> <li>执行命令 <b>interface interface-type interface-number</b>, 进入以太网或 trunk 接口配置视图;</li> <li>执行命令 <b>no private-vlan host-association vlan-number1 vlan-number2</b></li> </ol>	-



#### 2.10.2.1.4 配置在辅助 VLAN 配置节点下关联到主 VLAN

##### 目的

本节介绍如何配置在辅助 VLAN 配置节点下关联到主 VLAN。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置在辅助 VLAN 配置节点下关联到主 VLAN	1. 在特权用户视图下执行命令 <code>vlan vlan-number</code> ，进入 VLAN 配置视图； 2. 执行命令 <code>private-vlan primary-vid vlan-number</code>	<code>vlan-number</code> ：指定待关联的主 VLAN ID，整数形式，取值范围是 1~4094；

#### 2.10.2.1.5 配置主 VLAN 以及与其关联的辅助 VLAN

##### 目的

本节介绍如何配置配置主 VLAN 以及与其关联的辅助 VLAN。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置主 VLAN 以及与其关联的辅助 VLAN	1. 在特权用户视图下执行命令 <code>vlan vlan-number</code> ，进入 VLAN 配置视图； 2. 执行命令 <code>private-vlan association vlan-list</code>	<code>vlan-number</code> ：VLAN ID，整数形式，取值范围是 1~4094； <code>vlan-list</code> ：指定辅 VLAN ID 列表，形如 10,20,30-32，取值范围是 1~4094；
取消主 VLAN 与其关联的辅助 VLAN	1. 在特权用户视图下执行命令 <code>vlan vlan-number</code> ，进入 VLAN 配置视图； 2. 执行命令 <code>no private-vlan association</code>	-

#### 2.10.2.2 PVLAN 模式配置

##### 2.10.2.2.1 配置所属私有 VLAN 接口的模式

##### 目的

本节介绍如何配置配置所属私有 VLAN 接口的模式。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置所属私有 VLAN 接口的模式	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>config</code>，进入全局配置视图；</li> <li>2. 执行命令 <code>interface interface-type interface-number</code>，进入以太网或 trunk 接口配置视图；</li> <li>3. 执行命令 <code>private-vlan mode { native   host   promiscuous }</code></li> </ol>	<p><code>interface-number</code>：SC9600 系列交换机支持以下 3 种型号的接口配置范围：</p> <p>SC9603：取值范围是 &lt;1-3&gt;/&lt;0-4&gt;/&lt;1-48&gt;</p> <p>SC9608：取值范围是 &lt;1-8&gt;/&lt;0-4&gt;/&lt;1-48&gt;</p> <p>SC9612：取值范围是 &lt;1-12&gt;/&lt;0-4&gt;/&lt;1-48&gt;</p> <p><code>native</code>：指定非私有 VLAN 模式；</p> <p><code>host</code>：指定主机模式</p> <p><code>promiscuous</code>：指定混杂模式</p>

### 2.10.2.2.2 配置私有 VLAN 的模式

#### 目的

本节介绍如何配置私有 VLAN 的模式。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置私有 VLAN 的模式	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>vlan vlan-number</code>，进入 VLAN 配置视图；</li> <li>2. 执行命令 <code>private-vlan { primary   isolated   community }</code></li> </ol>	<p><code>vlan-number</code>：VLAN ID，整数形式，取值范围是 1~4094；</p> <p><code>primary</code>：指定为主 VLAN；</p> <p><code>isolated</code>：指定为隔离 VLAN</p> <p><code>community</code>：指定为通讯 VLAN</p>

### 2.10.2.2.3 恢复私有 VLAN 为普通 VLAN

#### 目的

本节介绍如何恢复私有 VLAN 为普通 VLAN。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
恢复私有 VLAN 为普通 VLAN	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>vlan vlan-number</code>，进入 VLAN 配置视图；</li> <li>2. 执行命令 <code>no private-vlan</code></li> </ol>	<p><code>vlan-number</code>：VLAN ID，整数形式，取值范围是 1~4094；</p>

### 2.10.2.3 查看 PVLAN 相关信息

#### 2.10.2.3.1 查看 PVLAN 接口信息

##### 目的

本节介绍如何查看 PVLAN 接口信息。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
查看 PVLAN 接口信息	<ol style="list-style-type: none"> <li>1. 执行命令进入普通用户视图或者特权用户视图。</li> <li>2. 执行命令 <code>show private-vlan interface</code></li> </ol>	-

#### 2.10.2.3.2 查看 PVLAN 关联映射信息

##### 目的

本节介绍如何查看 PVLAN 关联映射信息。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
查看 PVLAN 关联映射信息	<ol style="list-style-type: none"> <li>1. 执行命令进入普通用户视图或者特权用户视图。</li> <li>2. 执行命令 <code>show private-vlan mapping</code></li> </ol>	-

### 2.10.3 配置举例

#### 组网要求

如图所示，交换机的端口 9 为 promiscuous 端口，端口 1、2 属于隔离 vlan 2，其端口之间互相隔离，但都可以与端口 9 互通；端口 7、8 属于通讯 vlan 3，两端口可互通，也可与端口 9 互通；端口 11、12 属于通讯 vlan5，两端口可互通，也可与端口 9 互通。vlan 2，vlan3 与 vlan5 均为 secondary vlan，之间不能互通，但这些 vlan 中所有的端口以及端口 9 均属于 vlan100，即 primary vlan。

#### 组网图

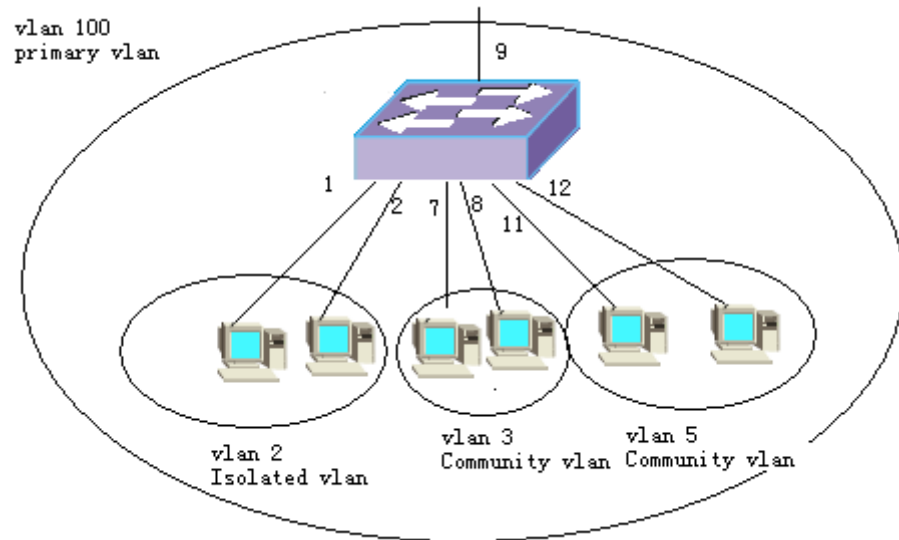


图 2-9 PVLAN 配置组网图

### 配置流程

- 1) 增加预先规划的 VLAN: 增加 vlan2、3、5、100;
- 2) 设置各个 VLAN 的模式: 设置 vlan100 模式为 primary, 即主 vlan, vlan2 为 isolated, 即隔离 vlan, vlan3、5 为 community, 即通讯 vlan;
- 3) 建立 VLAN 之间的关联: 将 vlan100 与 vlan2、3、5 关联;
- 4) 设置各个端口的模式: 设置端口 9 模式为 promiscuous, 即混杂模式, 端口 1、2、7、8、11、12 模式为 host, 即主机模式;
- 5) 将端口关联到各个 VLAN: 将端口 9 与 vlan100、2、3、5 关联, 端口 1、2 与 vlan100、vlan2 关联, 端口 7、8 与 vlan100、vlan3 关联, 端口 11、12 与 vlan100、vlan5 关联;
- 6) 配置完毕;

### 配置步骤

上述配置过程命令行如下:

```
SC9600A(config)#Vlan 2
SC9600A(config-vlan-2)#primary-vlan isolated
SC9600A(config-vlan-2)#q
SC9600A(config)#Vlan 3
SC9600A(config-vlan-3)#primary-vlan community
```

```
SC9600A(config-vlan-3)#q
SC9600A(config)#Vlan 5
SC9600A(config-vlan-5)#primary-vlan community
SC9600A(config-vlan-5)#q
SC9600A(config)#Vlan 100
SC9600A(config-vlan-100)#primary-vlan primary
SC9600A(config-vlan-100)#primary-vlan association 2,3,5
SC9600A(config-vlan-100)#q
SC9600A(config)#interface gigabitEthernet 1/0/9
SC9600A(config-gigabitEthernet 1/0/1)#private-vlan mode promiscuous
SC9600A(config-gigabitEthernet 1/0/1)#private-vlan mapping 100 add 2,3,5
SC9600A(config)#q
SC9600A(config)#interface gigabitEthernet 1/0/1 to gigabitEthernet 1/0/2
SC9600A(config-gigabitEthernet 1/0/1->1/0/2)#private-vlan mode host
SC9600A(config-gigabitEthernet 1/0/1->1/0/2)#private-vlan host-association 100 2
SC9600A(config)#q
SC9600A(config)#interface gigabitEthernet 1/0/7 to gigabitEthernet 1/0/8
SC9600A(config-gigabitEthernet 1/0/7->1/0/8)#private-vlan mode host
SC9600A(config-gigabitEthernet 1/0/7->1/0/8)#private-vlan host-association 100 3
SC9600A(config)#q
SC9600A(config)#interface gigabitEthernet 1/0/11 to gigabitEthernet 1/0/12
SC9600A(config-gigabitEthernet 1/0/11->1/0/12)#private-vlan mode host
SC9600A(config-gigabitEthernet 1/0/11->1/0/12)# private-vlan host-association 100 5
SC9600A(config)#q
```

配置完毕后，用如下命令显示配置结果。

```
show private-vlan
```

## 2.11 Voice VLAN 配置

### 2.11.1 Voice VLAN 概述

#### 简介

Voice VLAN 是为用户的语音数据流划分的 VLAN。用户通过创建 Voice VLAN 并将连接语音设备的接口加入到 Voice VLAN 中，使语音数据流集中在 Voice VLAN 中进行传

输。采用 Voice VLAN 的方式，便于对语音数据流进行有针对性的 QoS（Quality of Service）配置，提高语音数据流量的传输优先级，保证通话质量。

### Voice VLAN 实现方式

Voice VLAN 是通过如下方式实现对语音数据流的自动识别及接口的自动维护的：

#### (1) 配置 OUI 地址

首先为该 Voice VLAN 设置若干 OUI 地址，称为可识别的其它 OUI 地址，该地址包括一个 48 位的 MAC 地址和一个掩码。

#### (2) 配置接口工作模式

- 接口的工作模式设为自动工作模式

将 IP 语音设备上电时发出的报文的源 MAC 地址与掩码进行与运算，得到的值若等于相应的 OUI，则 Voice VLAN 认为该设备为语音设备，该接口自动加入 Voice VLAN，该接口下连接的语音设备所发出的带有 Voice VLAN 标签的语音流便能够通过该接口进行传输。当 Voice VLAN 内的某接口到达老化时间时还没有新的语音数据包通过，则自动将其从 Voice VLAN 中删除。

- 接口的工作模式设为手动模式

若接口的工作模式被设为手动模式，则 Voice VLAN 接口的增加和删除都必须手工进行。

### Voice VLAN 报文处理模式

Voice VLAN 对报文的处理方式可分为两种模式：安全模式和普通模式。

在普通模式下，Voice VLAN 相当于一个普通的 VLAN。两种模式对报文的处理方式如表 2-1。

表 2-1 Voice VLAN 报文处理方式

Voice VLAN 模式	报文类型	处理方式
安全模式	Untagged 报文	判断该报文源 MAC 地址是否为 OUI 地址： 是，则修改报文优先级并进行转发。 否，则不修改优先级并禁止在 Voice VLAN 内转发。
	带有 Voice VLAN Tag 的报文	
	带有其他 VLAN Tag 的报文	根据指定接口是否允许该 VLAN 通过来对报文进行转发和丢弃的处理，不受 Voice VLAN 的模式影响。

Voice VLAN 模式	报文类型	处理方式
普通模式	Untagged 报文	判断该报文源 MAC 地址是否为 OUI 地址： 是，则修改报文优先级并进行转发。 否，则不修改优先级并允许在 Voice VLAN 内转发。
	带有 Voice VLAN Tag 的报文	
	带有其他 VLAN Tag 的报文	根据指定接口是否允许该 VLAN 通过来对报文进行转发和丢弃的处理，不受 Voice VLAN 的模式影响。

### 2.11.2 配置 Voice VLAN 功能

#### 目的

使用本节操作配置 Voice VLAN，以满足对语音流的集中控制。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置 Voice VLAN 可识别的其他 OUI 地址	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>voice-vlan oui oui-mac-address [ name ]</b>设置 Voice VLAN 可识别的其他 OUI 地址；</li> <li>3. 结束。</li> </ol>
配置指定 VLAN 为 Voice VLAN，同时使能接口的 Voice VLAN 功能	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b> 或 <b>interface eth-trunk trunk-number</b> 进入接口配置视图；</li> <li>3. 执行命令 <b>voice-vlan voice-vlan enable</b> 使能接口的 Voice VLAN 功能；</li> <li>4. 结束。</li> </ol>
使能或去使能接口 Voice VLAN 的安全模式	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b> 或 <b>interface eth-trunk trunk-number</b> 进入接口配置视图；</li> <li>3. 执行命令 <b>voice-vlan security { enable   disable }</b>使能或去使能接口 Voice VLAN 的安全模式；</li> <li>4. 结束。</li> </ol>
配置接口的 Voice VLAN 操作模式	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b> 或 <b>interface eth-trunk trunk-number</b> 进入接口配置视图；</li> <li>3. 执行命令 <b>voice-vlan mode { auto   manual }</b>配置接口的 Voice VLAN 操作模式；</li> <li>4. 结束。</li> </ol>
(可选)配置	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> </ol>

目的	步骤
Voice VLAN 的老化时间	2. 执行命令 <b>voice-vlan aging-time { aging-time   default }</b> 设置 Voice VLAN 的老化时间； 3. 结束。
(可选)配置端口的 voice vlan 老化剩余时间	1. 执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b> 或 <b>interface eth-trunk trunk-number</b> 进入接口配置视图； 3. 执行命令 <b>voice-vlan aging remain-time { remain-time   default }</b> 配置端口的 voice vlan 老化剩余时间； 4. 结束。

附表：

参数	说明	取值
oui-mac-address	指定语音报文的 OUI 地址及其掩码	形如 AA:BB:CC:DD:EE:FF/M，其中 A~F 为一位十六进制数，M 为子网掩码，具体 OUI 地址参见下方： OUI 地址 0001-e300-0000 0003-6b00-0000 0004-0d00-0000 0060-b900-0000 00d0-1e00-0000 00e0-7500-0000 00e0-bb00-0000
[ name ]	可选参数，指定 OUI 地址的描述信息	字符串形式
voice-vlan	指定 VOICE VLAN 的 ID	整数形式，取值范围是 1~4094
enable	使能接口的 Voice VLAN 功能	-
disable	去使能接口的 Voice VLAN 功能	-
interface-number	指定以太网接口号	SC9600 系列交换机支持以下 3 种型号的接口配置范围： SC9603：取值范围是 <1-3>/<0-4>/<1-48> SC9608：取值范围是 <1-8>/<0-4>/<1-48> SC9612：取值范围是 <1-12>/<0-4>/<1-48>
trunk-number	指定 trunk 接口号	整数形式，取值范围是 1-128
auto	指定为自动模式	-
manual	指定为手动模式	-
enable	使能接口 Voice VLAN 的安全模式	-



参数	说明	取值
disable	去使能接口 Voice VLAN 的安全模式	-
aging-time	指定 Voice VLAN 的老化时间	整数形式，取值范围是 5~43200，单位：分钟
default	缺省 Voice VLAN 老化时间	5 分钟
Remain-time	指定 Voice VLAN 的老化时间	整数形式，取值范围是 1~43200，单位：分钟
default	缺省 Voice VLAN 老化时间	5 分钟

### 2.11.3 维护及调试

#### 目的

当 Voice VLAN 功能不正常，需要进行查看、调试或定位问题时，可以使用本小节操作。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
打开 Voice VLAN 调试同能	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>debug voice-vlan</b> 打开 Voice VLAN 调试同能；</li> <li>3. 结束。</li> </ol>
关闭 Voice VLAN 调试同能	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>no debug voice-vlan</b> 打开 Voice VLAN 调试同能；</li> <li>3. 结束。</li> </ol>
查看 Voice VLAN 配置信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gigasethernet   xgigasethernet } interface-number</b> 或 <b>interface eth-trunk trunk-number</b> 进入接口配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show voice-vlan config</b> 显示 Voice VLAN 配置信息；</li> <li>3. 结束。</li> </ol>
查看配置了 Voice VLAN 的接口信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gigasethernet   xgigasethernet } interface-number</b> 或 <b>interface eth-trunk trunk-number</b> 进入接口配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show voice-vlan interface</b> 显示配置了 Voice VLAN 的接口信息；</li> <li>3. 结束。</li> </ol>
查看 Voice	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配</li> </ol>

目的	步骤
VLAN 的 OUI 地址和相关属性信息	置视图，或执行命令 <b>interface { fastethernet   gigaehternet   xgigaethernet } interface-number</b> 或 <b>interface eth-trunk trunk-number</b> 进入接口配置视图，或不执行任何命令保持当前特权用户视图； 2. 执行命令 <b>show voice-vlan oui</b> 显示 Voice VLAN 的 OUI 地址和相关属性信息； 3. 结束。

附表：

参数	说明	取值
interface-number	指定以太网接口号	SC9600 系列交换机支持以下 3 种型号的接口配置范围： SC9603: 取值范围是<1-3>/<0-4>/<1-48> SC9608: 取值范围是<1-8>/<0-4>/<1-48> SC9612: 取值范围是<1-12>/<0-4>/<1-48>
trunk-number	指定 trunk 接口号	整数形式，取值范围是 1-128

### 2.11.4 配置举例

#### 组网要求

IP 电话 1 一端与 PC 连接，另一端与交换机 A 连接，IP 电话 2 仅与交换机 A 相连。希望 IP 电话 1 能在有语音数据的时候自动加入 Voice VLAN，优先传输语音数据，没有语音数据时自动退出 Voice VLAN；IP 电话 2 总在 Voice VLAN 中。

#### 组网图

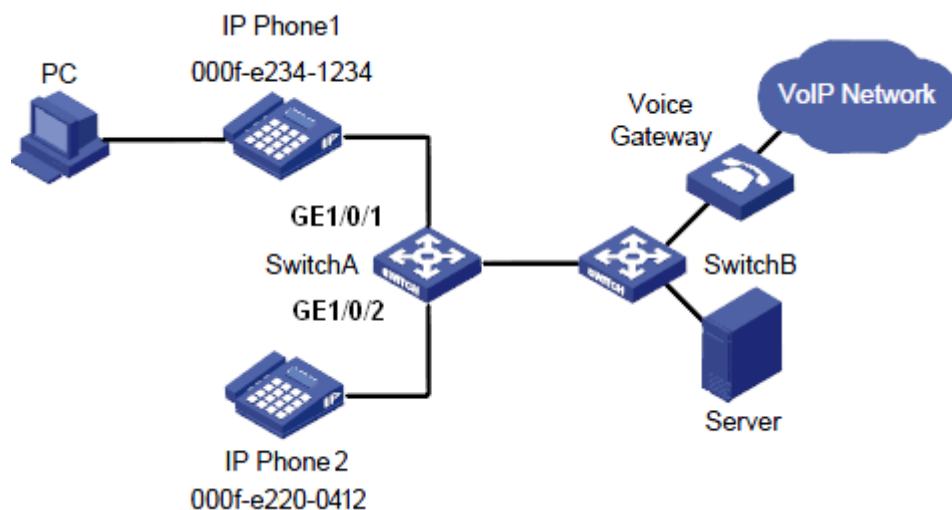


图 2-10 Voice VLAN 配置示意图

### 配置思路

根据上述要求,需要将 IP 电话 1 所连接的交换机端口 1/0/1 设为 Voice VLAN 自动模式, IP 电话 2 所连接的交换机端口 1/0/2 设为 Voice VLAN 手动模式。配置 OUI 为 00:0f:e2:00:00:00/24, 使能的 Voice VLAN 为 200。

当 IP 电话 1 发送源 MAC 与 OUI 匹配的语音流时, 端口 1/0/1 自动加入 VLAN 200, 将该数据流提高优先级传输。由于安全模式使能, 此时若 PC 发送源 MAC 与 OUI 不匹配的数据, 将不能通过。当源 MAC 与 OUI 匹配的流停止后, 该端口将自动退出 VLAN 200。若希望 PC 数据也能通过, 需要去使能安全模式: `voice-vlan security disable`。

### 配置步骤

1、配置 Voice VLAN 可识别的其他 OUI 地址。

```
SC9600#configure
SC9600(config)#voice-vlan oui 00:0f:e2:00:00:00/24
SC9600(config)#
```

2、创建 VLAN200, 并将端口加入。

```
SC9600(config)#Vlan 200
SC9600(config-vlan-200)#quit
SC9600(config)#interface gigabitEthernet 1/0/1
SC9600(config-gigabitEthernet1/0/1)#port hybrid pvid 100
SC9600(config-gigabitEthernet1/0/1)#port hybrid vlan 100 tagged
SC9600(config-gigabitEthernet1/0/1)#quit
SC9600(config)#interface gigabitEthernet 1/0/2
SC9600(config-gigabitEthernet1/0/2)#port hybrid pvid 200
SC9600(config-gigabitEthernet1/0/2)#port hybrid vlan 200 tagged
SC9600(config-gigabitEthernet1/0/2)#quit
```

3、配置端口 1/0/1 Voice 功能。

```
SC9600(config)#interface gigabitEthernet 1/0/1
SC9600(config-gigabitEthernet1/0/1)#voice-vlan 200 enable  \\指定 VLAN 为 Voice VLAN, 同时使能接口的 Voice VLAN 功能。
SC9600(config-gigabitEthernet1/0/1)#voice-vlan security enable  \\使能接口 Voice VLAN 的安全模式。
SC9600(config-gigabitEthernet1/0/1)#voice-vlan mode auto  \\配置接口的 Voice VLAN 操作模式为自动模式。
SC9600(config-gigabitEthernet1/0/1)#quit
```

4、配置端口 1/0/2 Voice VLAN 功能。

```
SC9600(config)#interface gigabitEthernet 1/0/2
```

```
SC9600(config-gigabitEthernet1/0/2)#voice-vlan 200 enable
```

```
SC9600(config-gigabitEthernet1/0/2)#voice-vlan security enable
```

```
SC9600(config-gigabitEthernet1/0/2)#voice-vlan mode manual
```

\\配置接口的 Voice VLAN 操作模式为手动模式。

5、结束。

## 2.12 环回检测配置

### 2.12.1 环回检测概述

#### 简介

ALB (Anti-loop Back) 是浪潮网络科技有限公司自主开发的端口环路检测协议。为了避免以太网中的环路导致网络崩溃，IEEE 制定了生成树协议 (STP)，但是生成树协议在收敛时间上比较长，而且需要网络中所有的设备都使能生成树协议才能有效的避免成环。而该协议能够简单、快速的查找到网络中的环，并对环进行处理，消除环或者消除环对本设备的影响。当在浪潮网络科技有限公司交换机的接口上使能了环路检测功能后，交换机就将周期性的从这个接口上发送环路检测数据，该数据是广播包，因此如果交换机的这个接口下联的网络存在环路，交换机就会接收到自己发出的这个数据，从而检测到这个接口下面的网络存在环路，此时交换机将把该端口与其他端口隔离开（默认处理），并且指示这个接口存在环路。

#### 支持的功能特性

- 支持快速检测并定位网络中的环路
- 支持基于端口的环回检测

通过端口发送 Untag 的 ALB 协议包检测，收包端口收到 ALB 协议包，判断比较源 MAC 与本机端口 MAC。若非本机端口 MAC 则转发出去；若为本机端口 MAC 则比较源端口号和收包端口的端口号，若一致则为远端成环 (remote-loop)，或不一致则为本地成环 (local-loop)，然后堵塞端口。

- 支持基于 VLAN 的环回检测

通过端口发送所要检测 VLAN (Tag) 的 ALB 协议包检测，收包端口收到 ALB 协议包，判断比较源 MAC 与本机端口 MAC。若非本机端口 MAC 则转发出去；若为

本机端口 MAC 则接着查询是否包的 VLAN 是否为本端口所要检测的 VLAN，若本端口所要检测的 VLAN 则比较源端口号和收包端口的端口号，若一致则为远端成环（remote-loop），或不一致则为本地成环（local-loop），然后堵塞（shut/nol-earning/port-trap）端口。若非本端口所要检测的 VLAN，则不予处理。



注意：

ALB 协议与其它环网检测，环网保护协议最好不要同时使用。在网络拓扑较为复杂的情况下会有很大的随机性，因此推荐用于用户端底层交换机，避免用户无意造成的环网对整个网络的影响。

### 2.12.2 配置环回检测功能

#### 目的

使用本节操作配置环回检测功能，以减小接入环路对整网的影响。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
使能/去使能接口环回检测功能	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b> 或 <b>interface eth-trunk trunk-number</b> 进入接口配置视图；</li> <li>3. 执行命令 <b>loop-check { enable   disable }</b>使能/去使能接口环回检测功能；</li> <li>4. 结束。</li> </ol>
配置设备对指定 VLAN 进行环回检测	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b> 或 <b>interface eth-trunk trunk-number</b> 进入接口配置视图；</li> <li>3. 执行命令 <b>loop-check vlan vlan-list</b> 设置设备对指定 VLAN 进行环回检测；</li> <li>4. 结束。</li> </ol>
（可选）配置链路发生环路时系统采取的处理动作	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>loop-check action { port-block   vlan-block }</b>设置链路发生环路时系统采取的处理动作；</li> <li>3. 结束。</li> </ol>
（可选）配置设备发送环回检测包的时间间隔	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>loop-check interval { interval-time   default }</b>设置设备发送环回检测包的时间间隔；</li> <li>4. 结束。</li> </ol>
（可选）配置	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> </ol>

目的	步骤
等待时间和发包间隔之间的倍数	<ol style="list-style-type: none"> <li>2. 执行命令 <b>loop-check recover-time</b> { <i>recover-time</i>   <b>default</b> } 设置等待时间和发包间隔之间的倍数；</li> <li>3. 结束。</li> </ol>
(可选)清除环回检测接口的状态	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface</b> { <b>fastethernet</b>   <b>gigaethernet</b>   <b>xgigaethernet</b> } <i>interface-number</i> 或 <b>interface eth-trunk</b> <i>trunk-number</i> 进入接口配置视图；</li> <li>3. 执行命令 <b>loop-check reset</b> 清除环回检测接口的状态；</li> <li>4. 结束。</li> </ol>
(可选)使能或去使能环回检测告警功能	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>loop-check trap</b> { <b>enable</b>   <b>disable</b> } 使能或去使能环回检测告警功能；</li> <li>3. 结束。</li> </ol>

附表：

参数	说明	取值
enable	使能接口环回检测功能	-
disable	去使能接口环回检测功能	-
vlan-list	指定 VLAN 列表, 表示在该 VLAN 上进行环回检测	整数形式, 取值范围是 1~4094
port-block	表示只要检测到该接口下任意一个 vlan 成环, 就将该接口加入的 vlan 都设置成阻塞	-
vlan-block	表示只对接口上检测到环路的 vlan 设置阻塞, 没有检测到环路的 vlan 任然可以正常工作	-
interface-number	指定以太网接口号	SC9600 系列交换机支持以下 3 种型号的接口配置范围: SC9603 : 取值范围是 <1-3>/<0-4>/<1-48> SC9608 : 取值范围是 <1-8>/<0-4>/<1-48> SC9612 : 取值范围是 <1-12>/<0-4>/<1-48>
trunk-number	指定 trunk 接口号	整数形式, 取值范围是 1-128
interval-time	指定接口发送环回检测包的时间间隔取值	整数形式, 取值范围是 <3-60>, 单位: 秒
default	恢复接口发送环回检测包的时间间隔为默认值	default: 5 秒
recover-time	指定阻塞接口恢复时间	整数形式, 取值范围是 <3-20>
default	默认恢复时间	default: 5 倍

参数	说明	取值
enable	使能环回检测告警功能	-
disable	去使能环回检测告警功能	-

### 2.12.3 维护及调试

#### 目的

当环回检测功能不正常，需要进行查看、调试或定位问题时，可以使用本小节操作。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
打开环回检测收发包调试功能	<ol style="list-style-type: none"> <li>1. 不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>debug loop-check { in   in-detail   out   out-detail   port-status   event   timer   all }</b>打开环回检测收发包调试功能；</li> <li>3. 结束。</li> </ol>
关闭环回检测收发包调试功能	<ol style="list-style-type: none"> <li>1. 不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>no debug loop-check { in   in-detail   out   out-detail   port-status   event   timer   all }</b>关闭环回检测收发包调试功能；</li> <li>3. 结束。</li> </ol>
查看环回检测功能的各项属性参数配置信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gigasethernet   xgigasethernet } interface-number</b> 或 <b>interface eth-trunk trunk-number</b> 进入接口配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show loop-check</b> 显示环回检测功能的各项属性参数配置信息；</li> <li>3. 结束。</li> </ol>
查看所有接口的环回检测状态或者指定显示某接口的环回检测功能配置情况	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gigasethernet   xgigasethernet } interface-number</b> 或 <b>interface eth-trunk trunk-number</b> 进入接口配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show loop-check interface</b> 或 <b>show loop-check interface { fastethernet   gigasethernet   xgigasethernet } interface-number</b> 或 <b>show port-uniisolate interface eth-trunk trunk-number</b> 或 <b>show loop-check interface eth-trunk trunk-number</b>；</li> <li>3. 结束。</li> </ol>

附表：

参数	说明	取值
interface-number	指定以太网接口号	SC9600 系列交换机支持以下 3 种型号的接口配置范围：

参数	说明	取值
		SC9603 : 取值范围是 <1-3>/<0-4>/<1-48> SC9608 : 取值范围是 <1-8>/<0-4>/<1-48> SC9612 : 取值范围是 <1-12>/<0-4>/<1-48>
trunk-number	指定 trunk 接口号	整数形式, 取值范围是 1-128
in	调试环回检测接收包信息	-
in-detail	调试环回检测详细接收包信息	-
out	调试环回检测发送包信息	-
out-detai	调试环回检测详细发送包信息	-
port-status	调试环回检测端口状态	-
event	调试环回检测功能	-
timer	调试环回检测定时器功能	-
all	显示所有环回检测的调试信息	-

### 2.12.4 配置举例

#### 组网要求

端口发生环路是指端口发出去的报文通过其它端口又回到该设备, 环路的存在可能导致广播风暴。环回检测就是监测设备的端口是否有环路存在。

配置 ALB 功能, 交换机 A, 分别为接口 1/0/1, 接口 1/0/2, 设交换机 B 没有任何去除环回的机制。

#### 组网图

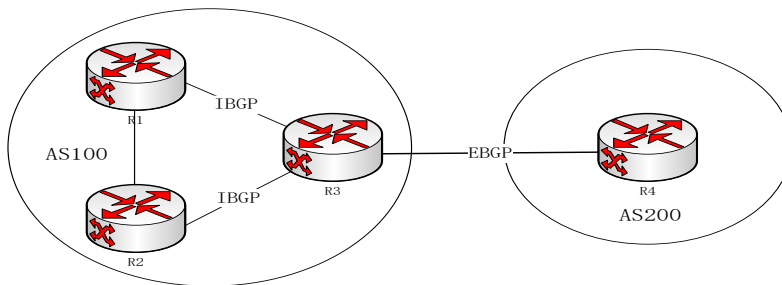


图 2-11 环回检测配置示意图

#### 配置步骤



1、在交换机 A 上配置使能接口 1 和接口 2 的环回检测功能且将接口 1 和接口 2 的环回检测 VLAN 配置成相同的且有效的 VLAN。

```
SC9600#configure
SC9600(config)#interface gigabitEthernet 1/0/1
SC9600(config-gigabitEthernet1/0/1)#loop-check enable
SC9600(config-gigabitEthernet1/0/1)#loop-check vlan 1
SC9600(config-gigabitEthernet1/0/1)#quit
SC9600(config)#interface gigabitEthernet 1/0/2
SC9600(config-gigabitEthernet1/0/2)#loop-check enable
SC9600(config-gigabitEthernet1/0/2)#loop-check vlan 1
SC9600(config-gigabitEthernet1/0/2)#quit
SC9600(config)#
```

2、（可选配）配置设备发送环回检测包的时间间隔。

```
SC9600(config)#loop-check interval 50
SC9600(config)#
```

3、（可选配）配置等待时间和发包间隔之间的倍数。

```
SC9600(config)#loop-check recover-time 20
SC9600(config)#
```

4、结束。

```
SC9600#show loop-check interface
```

Interface	Enable	State	Distance(rx/tx)	RemainTime(sec)
1/0/1	Yes	local-loop	0/0	59
1/0/2	Yes	ok	0/0	0
1/0/3	Yes	linkdown	0/0	0
1/0/4	Yes	linkdown	0/0	0
1/0/5	Yes	linkdown	0/0	0
1/0/6	Yes	linkdown	0/0	0
.....				



说明：

如上所示，交换机检测出了接口 1 与接口 2 成环，并对接口 1 进行了处理，消除这个环回。

## 第3章 IP 业务配置

### 3.1 概述

本章介绍了 SC9600 系列高端交换机的 IP 业务。

本章包括如下主题：

内容	页码
3.1 概述	3-1
3.2 IPv4 配置	3-1
3.3 IPv6 配置	3-7
3.4 DHCP 配置	3-17

### 3.2 IPv4 配置

#### 3.2.1 配置 IP 收发包调试功能

##### 目的

本节介绍打开 IP 收发包调试功能。本操作用于维护及调试设备 IP 功能。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
打开 IP 收发包调试功能	执行如下命令（根据需求）： <code>debug ip</code> <code>debug ip { in   out   all } [ level ]</code>	缺省情况下，IP 调试功能是关闭的。 in 显示收包的报文 - out 显示发包的报文 - all 显示所有 IP 包的调试信息 - [ level ] 指定调试级别 整数形式， 取值范围是 1~7
关闭 IP 收发包调试功能	执行命令 <code>no debug ip</code>	

### 3.2.2 配置带内/带外/环回 IP 地址

#### 目的

本节介绍如何配置设备的带内/带外/环回 IP 地址。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置设备的带内/带外/环回 IP 地址。	<p>配置带内 IP 地址：</p> <ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code>，进入全局配置视图。</li> <li>2. 执行命令 <code>interface vlan <i>vlan-id</i></code> 进入 VLANIF 配置视图。</li> <li>3. 执行命令 <code>ip address <i>ip-address</i>/<i>mask-length</i></code> 或 <code>ip address <i>ip-address</i> <i>mask-address</i></code> 配置带内 IP 地址。</li> </ol> <p>配置带外 IP 地址：</p> <ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code>，进入全局配置视图。</li> <li>2. 执行命令 <code>interface ethernet 0/0/0</code> 进入带外口配置视图。</li> <li>3. 执行命令 <code>ip address <i>ip-address</i>/<i>mask-length</i></code> 或 <code>ip address <i>ip-address</i> <i>mask-address</i></code> 配置带外 IP 地址。</li> </ol> <p>配置环回 IP 地址：</p> <ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code>，进入全局配置视图。</li> <li>2. 执行命令 <code>interface loopback <i>loopback-interface</i></code> 进入环回接口配置视图。</li> <li>3. 执行命令 <code>ip address <i>ip-address</i>/<i>mask-length</i></code> 或 <code>ip address <i>ip-address</i> <i>mask-address</i></code> 配置环回 IP 地址。</li> </ol>	<p><code>ip-address</code>：指定 IP 地址，点分十进制</p> <p><code>mask-address</code>：指定掩码地址，点分十进制</p> <p><code>ip-address/mask-length</code> 指定 IP 地址及掩码地址点分十进制；</p> <p><code>mask-length</code>：掩码地址位数，取值为整数，范围从 1~32</p>
删除设备的带内/带外/环回 IP 地址	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code>，进入全局配置视图。</li> <li>2. 执行命令 <code>interface vlan <i>vlan-id</i></code> 进入 VLANIF 配置视图或执行命令 <code>interface ethernet 0/0/0</code> 进入带外口配置视图或执行命令 <code>interface loopback <i>loopback-interface</i></code> 进入环回接口配置视图。</li> <li>3. 执行如下命令 <code>no ip address <i>ip-address</i></code>。</li> </ol>	

### 3.2.3 配置 VLANIF 接口的 IP 地址

#### 目的

本节介绍如何配置当前接口的外层 Tag 的标签协议标识。

本操作为设备上的接口配置 IP 地址和掩码地址，实现网络的互连互通。有时为了使设备的一个接口能够与多个子网相连，可以在一个接口上配置多个 IP 地址，其中一个为主 IP 地址，其余为从 IP 地址。当配置主 IP 地址时，如果接口上已经有主 IP 地址，则原主 IP 地址被删除，新配置的 IP 地址成为主 IP 地址。删除主 IP 地址前，必须先删除完所有的从 IP 地址。

设备上各接口配置的所有 IP 地址不能位于相同的子网。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置 VLANIF 接口的 IP 地址	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code>，进入全局配置视图。</li> <li>2. 执行命令 <code>interface vlan N1</code> 进入 VLAN N1 配置模式。</li> <li>3. 执行如下命令（根据需求）：  <code>ip address ip-address/mask-length</code>  <code>ip address ip-address mask-address</code> </li> </ol>	缺省情况下，系统最大 TCP 连接数目为 100。  Maxnum：指定 TCP 最大连接数，整数形式，取值范围是 1~100。
删除 VLANIF 接口的所有 IP 地址或指定 IP 地址	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code>，进入全局配置视图。</li> <li>2. 执行命令 <code>interface vlan N1</code> 进入 VLAN N1 配置模式。</li> <li>3. 执行如下命令（根据需求）：  <code>no ip address ip-address</code>  <code>no ip address</code> </li> </ol>	

## 3.2.4 配置 TCP 连接数目

### 目的

本节介绍如何配置当前接口的外层 Tag 的标签协议标识。

本操作帮助用户限制系统最大可接入的 TCP 连接数目。例如，当在设备上起一个 telnet 服务，则建议用户配置设备允许的最大客户连接数。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置 TCP 连接数目	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code>，进入全局配置视图。</li> <li>2. 执行命令 <code>ip tcp max-connnect maxnum</code></li> </ol>	缺省情况下，系统最大 TCP 连接数目为 100。  Maxnum: 指定 TCP 最大连接数，整数形式，取值范围是 1~200。

### 3.2.5 查看 VLAN 接口配置信息

#### 目的

本节介绍如何如何查看某一指定 VLAN 接口配置或查看所有 VLAN 接口配置信息。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
查看某一指定 VLAN 接口配置或查看所有 VLAN 接口配置信息	<ol style="list-style-type: none"> <li>1. 进入普通用户视图、特权用户视图或者 VLAN 配置视图。</li> <li>2. 执行命令以下命令（任一）： <code>show interface vlan vlan-id config</code> <code>show interface vlan config</code></li> </ol>	vlan-id 指定 VLAN ID，数形式，取值范围是 1~4094

### 3.2.6 查看 TCP/UDP 的连接状态

#### 目的

本节介绍如何查看当前 TCP/UDP 的连接状态表项。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
查看当前 TCP/UDP 的连接状态表项	<ol style="list-style-type: none"> <li>1. 进入普通用户视图或者特权用户视图。</li> <li>2. 执行命令 <code>show ip connect-table</code>。</li> </ol>	-

### 3.2.7 查看 IP 相关的统计信息

#### 目的

本节介绍如何查看 IP 相关的统计信息，包括包括现实 IP 统计信息、TCP 统计信息、UDP 统计信息、ICMP 统计信息、IGMP 统计信息以及 TCP/UDP 连接表信息。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
查看 IP 相关的统计信息	1.进入普通用户视图或者特权用户视图。 2. 执行如下命令（根据需求）： show ip statistics show ip tcp statistics show ip udp statistics show ip icmp statistics	-

### 3.2.8 查看系统 IP 接口的信息

#### 目的

本节介绍如何查看系统 IP 接口的信息。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
查看系统 IP 接口的信息	1.进入普通用户视图或者特权用户视图。 2. 执行命令 show ip interface	dc0 为带外地址，sw 0 为带内地址，lo0 为环回地址

### 3.2.9 配置举例

#### 组网要求

交换机 SC9600 通过以太网接口 gigaethernet1/0/1 连接到局域网，该局域网中的计算机分别属于两个不同网段，分别是 10.18.11.0/24 和 10.18.12.0/24，现要求通过交换机 SC9600 能分别访问这两个网络，但这两个网段内的计算机不能互通。

#### 组网图

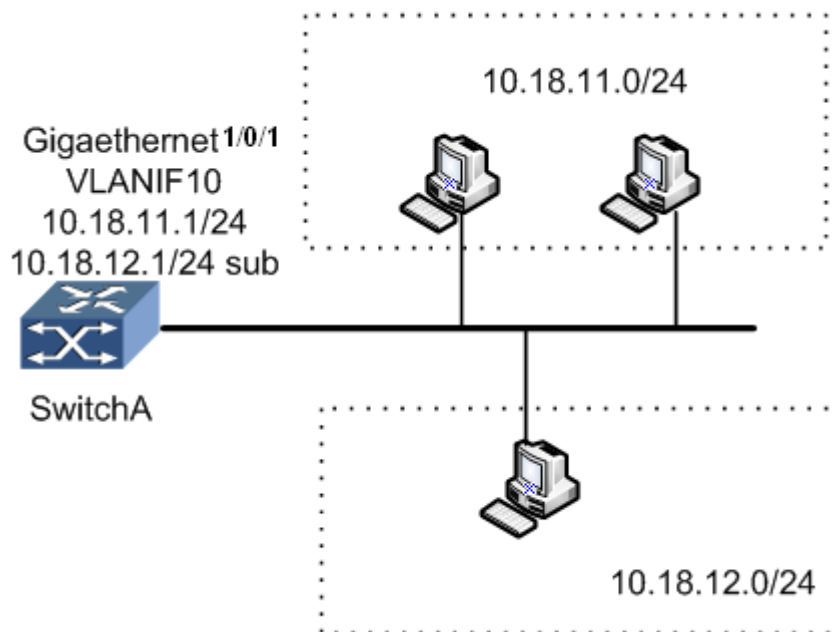


图 3-1 IPv4 地址配置拓扑图

### 配置步骤

- 1、配置 SC9600 的 VLAN10 接口的 IP 地址。

```
SC9600A#configure
```

```
SC9600A(config)#interface vlan 10
```

```
SC9600A(config-Man-10)#ip address 10.18.11.1/24
```

```
SC9600A(config-Man-10)#ip address 10.18.12.1/24 sub
```

```
SC9600A(config-Man-10)#quit
```

```
SC9600A(config)#
```

```
SC9600A(config)#interface gigaethernet 1/0/1
```

```
SC9600A(config-ge1/0/1)#port hybrid vlan 10 untagged
```

```
SC9600A(config-ge1/0/1)#port hybrid pvid 10
```

```
SC9600A(config-ge1/0/1)#quit
```

## 3.3 IPv6 配置

### 3.3.1 配置 IPv6 基本功能

#### 3.3.1.1 配置 IPv6 地址

##### 目的

本节介绍如何手动配置接口上 IPv6 单播地址、任播地址、组播地址以及链路本地地址。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
手工设置接口的 IPv6 地址和掩码长度	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 在全局配置视图下执行命令 <code>interface vlan vlan-id</code> 进入 VLAN IF 配置视图；</li> <li>3. 执行命令 <code>ipv6 address ipv6-address/mask-length</code>。</li> </ol>	<p><code>ipv6-address</code>: 指定 IPv6 地址 纯二进制表示: 128 个 0 或 1 组成, 每 16 位为一段, 共八段, 形如: X::X:X</p>
删除接口手工设置的 IPv6 地址	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 在全局配置视图下执行命令 <code>interface vlan vlan-id</code> 进入 VLAN IF 配置视图；</li> <li>3. 执行命令 <code>no ipv6 address</code> 删除接口上所有的地址或执行命令 <code>no ipv6 address ipv6-address</code> 删除指定地址。</li> </ol>	<p><code>mask-length</code>: 指定 IPv6 前缀的长度, 即掩码中连续“1”的个数。“1”必须是连续的。取值范围是 0~128。</p>
手工设置接口链路本地地址	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 在全局配置视图下执行命令 <code>interface vlan vlan-id</code> 进入 VLAN IF 配置视图；</li> <li>3. 执行命令 <code>ipv6 address ipv6-address link-local</code>。</li> </ol>	

#### 3.3.1.2 配置 IPv6 静态路由条目

##### 目的

本节介绍如何添加或删除一条静态 IPv6 路由条目。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。



目的	步骤	参数说明
添加一条静态 IPv6 路由条目	<ol style="list-style-type: none"> <li>在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>执行命令 <code>ipv6 route-static (X:X::X:X) &lt;0-128&gt; (X:X::X:X)</code>  <code>ipv6 route-static (X:X::X:X) &lt;0-128&gt; (X:X::X:X) vpn-instance NAME</code>  <code>ipv6 route-static (X:X::X:X) &lt;0-128&gt; interface tunnel &lt;1-1024&gt;</code>  <code>ipv6 route-static (X:X::X:X) &lt;0-128&gt; interface vlan &lt;1-4094&gt; link-local (X:X::X:X)。</code></li> </ol>	-
删除一条静态 IPv6 路由条目	<ol style="list-style-type: none"> <li>在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>执行命令 <code>no ipv6 route-static (X:X::X:X) &lt;0-128&gt;</code>  <code>no ipv6 route-static (X:X::X:X) &lt;0-128&gt; vpn-instance NAME</code>  <code>no ipv6 route-static all。</code></li> </ol>	-

### 3.3.1.3 配置 IPv6 单播路由转发功能

#### 目的

本节介绍如何使能或去使能 IPv6 单播路由转发功能。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
使能 IPv6 单播路由转发功能	<ol style="list-style-type: none"> <li>在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>执行命令 <code>ipv6 unicast-forwarding enable。</code></li> </ol>	-
去使能 IPv6 单播路由转发功能	<ol style="list-style-type: none"> <li>在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>执行命令 <code>no ipv6 unicast-forwarding disable。</code></li> </ol>	-

### 3.3.1.4 配置接口上发送 IPv6 报文的 MTU 值

#### 目的

本节介绍如何配置接口 MTU。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
设置接口 MTU	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 在全局配置视图下执行命令 <code>interface vlan vlan-id</code> 进入 VLAN IF 配置视图；</li> <li>3. 执行命令 <code>ipv6 mtu mtu-value</code>。</li> </ol>	<b>mtu-value</b> : 指定接口发送 IPv6 报文 MTU 值，取值范围是 1280~1500，单位：字节 整
恢复接口 MTU 为默认值	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 在全局配置视图下执行命令 <code>interface vlan vlan-id</code> 进入 VLAN IF 配置视图；</li> <li>3. 执行命令 <code>ipv6 mtu default</code>。</li> </ol>	<b>default</b> : 表示默认值为 1500 字节

### 3.3.2 配置 IPv6 其他功能

#### 3.3.2.1 测试 IPv6 网络连通性及主机可达性

##### 目的

本节介绍如何检测 IPv6 网络连接是否出现故障或者监察网络线路质量。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
测试 IPv6 网络连通性及主机可达性	<ol style="list-style-type: none"> <li>1. 进入特权用户视图；</li> <li>2. 执行命令               <pre>ping6 ipv6-address ping6 ipv6-address vpn-instance NAME ping6 ipv6-address -t ping6 ipv6-address -t vpn-instance NAME ping6 ipv6-address { -n -l -w } VALUE ping6 ipv6-address { -n -l -w } VALUE vpn-instance NAME ping6 ipv6-address { -n -l -w } VALUE { -n -l -w } VALUE ping6 ipv6-address { -n -l -w } VALUE { -n -l -w } VALUE vpn-instance NAME ping6 ipv6-address { -n -l -w } VALUE { -n -l -w } VALUE { -n -l -w } VALUE ping6 ipv6-address { -n -l -w } VALUE { -n -l -w } VALUE { -n -l -w } VALUE vpn-instance NAME</pre> </li> </ol>	<b>ipv6-address</b> : 指定 IPv6 地址，纯二进制表示：128 个 0 或 1 组成，每 16 位为一段，共八段，形如：X:X::X:X <b>-t</b> 表示不断执行该 ping 命令直到手动停止 <b>-n</b> 表示发送的回应请求数目 <b>-l</b> 表示发送的 ICMP 包长 <b>-w</b> 表示在等待回应过程中毫秒级超时值 <b>VALUE</b> 对应以上指标的数值 整数形式，取值范围是 1~65500 <b>Name</b> VPN 实例名 字符串，最大长度为 30

目的	步骤	参数说明
	<pre>ping6 ipv6-address { -n -l -w } VALUE { -n -l -w } VALUE -t ping6 ipv6-address { -n -l -w } VALUE { -n -l -w } VALUE -t vpn-instance NAME ping6 ipv6-address { -n -l -w } VALUE -t ping6 ipv6-address { -n -l -w } VALUE -t vpn-instance NAME。</pre>	

### 3.3.3 配置 IPv6 邻居发现功能

#### 3.3.3.1 配置 IPv6 静态邻居条目

##### 目的

本节介绍如何配置 IPv6 静态邻居条目。

##### 背景信息

目前设备最多可以支持 128 条静态邻居条目。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
添加一条 IPv6 静态邻居条目	<ol style="list-style-type: none"> <li>在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>执行命令 <code>interface vlan vlan-id</code> 进入 VLANIF 配置视图；</li> <li>执行命令 <code>ipv6 neighbor ipv6-address mac-address { gigasetherne   xgigasetherne } interface-number。</code></li> </ol>	<p><b>ipv6-address:</b> 指定邻居 IPv6 地址 纯二进制表示：128 个 0 或 1 组成，每 16 位为一段，共八段，形如：X:X:X:X</p> <p><b>vlan-id:</b> 指定 VLAN ID，取值范围是 1~4094</p> <p><b>mac-address:</b> 指定邻居 MAC 地址 形如：AA:BB:CC:DD:EE:FF，其中 A~F 分别为一位十六进制数</p>
删除一条 IPv6 静态邻居条目	<ol style="list-style-type: none"> <li>在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>执行命令 <code>no ipv6 neighbor ipv6-address。</code></li> </ol>	<p><b>interface-number:</b> SC9600 系列交换机支持以下 3 种型号的接口配置范围：</p> <p>SC9603 : 取值范围是 &lt;1-3&gt;/&lt;0-4&gt;/&lt;1-48&gt;</p> <p>SC9608 : 取值范围是 &lt;1-8&gt;/&lt;0-4&gt;/&lt;1-48&gt;</p> <p>SC9612 : 取值范围是 &lt;1-12&gt;/&lt;0-4&gt;/&lt;1-48&gt;</p>

### 3.3.3.2 配置 IPv6 路由通告报文中管理地址标志位

#### 目的

本节介绍如何配置路由通告报文中管理地址标志位。

#### 背景信息

使用本命令设置了路由通告报文中管理地址标志位后，收到该路由通告报文的主机将使用全状态自动配置来获取地址。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
使能路由通告报文中管理地址标志位	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 在全局配置视图下执行命令 <code>interface vlan vlan-id</code> 进入 VLAN IF 配置视图；</li> <li>3. 执行命令 <code>ipv6 nd autoconfig managed-address-flag enable</code>。</li> </ol>	-
去使能路由通告报文中管理地址标志位	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 在全局配置视图下执行命令 <code>interface vlan vlan-id</code> 进入 VLAN IF 配置视图；</li> <li>3. 执行命令 <code>ipv6 nd autoconfig managed-address-flag disable</code>。</li> </ol>	-

### 3.3.3.3 配置 IPv6 路由通告报文中 other stateful configuration 标志位

#### 目的

本节介绍如何配置路由通告报文中 other stateful configuration 标志位。

#### 背景信息

使用本命令设置了路由通告报文中 other stateful configuration 标志位，则收到该路由通告的主机会使用全状态自动配置来获取地址之外的信息。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
使能路由通告报文中 other stateful configuration 标志位	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 在全局配置视图下执行命令 <code>interface vlan vlan-id</code> 进入 VLAN IF 配置视图；</li> <li>3. 执行命令 <code>ipv6 nd autoconfig other-flag enable</code>。</li> </ol>	-
去使能路由通告报文中 other stateful configuration 标志位	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 在全局配置视图下执行命令 <code>interface vlan vlan-id</code> 进入 VLAN IF 配置视图；</li> <li>3. 执行命令 <code>ipv6 nd autoconfig other-flag disable</code>。</li> </ol>	-

### 3.3.3.4 配置 IPv6 路由通告报文中当前跳数限制字段值

#### 目的

本节介绍如何配置路由通告报文中当前跳数限制字段值。

#### 背景信息

使用本命令若设置该值为 0，则表示路由没有说明跳数限制的配置。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
设置路由通告报文中当前跳数限制字段值	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 在全局配置视图下执行命令 <code>interface vlan vlan-id</code> 进入 VLAN IF 配置视图；</li> <li>3. 执行命令 <code>ipv6 nd hop-limit hoplimit-value</code>。</li> </ol>	<b>hoplimit-value:</b> 指定路由通告报文中跳数字段值，取值范围是 1~255

### 3.3.3.5 配置接口 IPv6 路由通告功能

#### 目的

本节介绍如何配置路由通告功能。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
使能接口路由通告功能	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 在全局配置视图下执行命令 <code>interface vlan vlan-id</code> 进入 VLAN IF 配置视图；</li> <li>3. 执行命令 <code>ipv6 nd ra enable</code>。</li> </ol>	-
去使能接口路由通告功能	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 在全局配置视图下执行命令 <code>interface vlan vlan-id</code> 进入 VLAN IF 配置视图；</li> <li>3. 执行命令 <code>no ipv6 nd ra disable</code>。</li> </ol>	-

### 3.3.3.6 配置发送 IPv6 路由通告的最小和最大时间间隔

#### 目的

本节介绍如何配置路由通告的最小和最大时间间隔。

#### 背景信息

若设备作为缺省路由器时，则此间隔时间不能大于路由器通告报文生存有效时间。且使用本命令设置的发送路由通告最小时间间隔必须大于或等于最大时间间隔的 3/4。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
设置路由通告的最小和最大时间间隔	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 在全局配置视图下执行命令 <code>interface vlan vlan-id</code> 进入 VLAN IF 配置视图；</li> <li>3. 执行命令 <code>ipv6 nd ra min-interval min-value</code> 或 <code>ipv6 nd ra max-interval max-value</code>。</li> </ol>	<p><b>min-value:</b> 指定路由通告发送的最小间隔时间，取值范围是 3~1350，单位：秒</p> <p><b>max-value:</b> 指定路由通告发送的最大间隔时间，取值范围是 4~1800，单位：秒</p>
恢复默认路由通告的最小和最大时间间隔	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 在全局配置视图下执行命令 <code>interface vlan vlan-id</code> 进入 VLAN IF 配置视图；</li> <li>3. 执行命令 <code>ipv6 nd ra min-interval default</code> 或 <code>ipv6 nd ra max-interval default</code>。</li> </ol>	<p>最小间隔时间的默认值为 200 秒；最大间隔时间的默认值为 600 秒</p>

### 3.3.3.7 配置接口上发送 IPv6 路由通告报文所携带路由器生存期字段值

#### 目的

本节介绍如何配置路由通告报文所携带路由器生存期字段值。

#### 背景信息

每个路由通告（RA）报文中都携带有“路由器生存期”字段，该字段表明了该接口所在的链路上主机可以将该设备作为缺省设备的时间。若设置为 0，则表示本设备不再被当做缺省设备。若设置为非 0，则必须注意该值大于等于设备发送路由通告（RA）报文的间隔时间。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
设置接口上发送的路由通告报文中所携带的路由器生存期字段的值	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 在全局配置视图下执行命令 <code>interface vlan vlan-id</code> 进入 VLAN IF 配置视图；</li> <li>3. 执行命令 <code>ipv6 nd ra route-lifetime lifetime-value</code>。</li> </ol>	<b>lifetime-value</b> ：指定路由器通告报文生存期有效时间，取值范围是 0~9000，单位：秒
恢复接口上发送的路由通告报文中所携带的路由器生存期字段的值为默认值	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 在全局配置视图下执行命令 <code>interface vlan vlan-id</code> 进入 VLAN IF 配置视图；</li> <li>3. 执行命令 <code>ipv6 nd ra route-lifetime default</code>。</li> </ol>	<b>default</b> ：表示默认值 1800 秒

### 3.3.3.8 配置接口上通过 NDP 动态学习到的邻居处于可达状态时间

#### 目的

本节介绍如何配置接口上通过 NDP 动态学到的邻居处于可达状态的时间。

#### 背景信息

使用本命令后，设备可以通过配置的时间来检测不可用的邻居。若设置的时间越短则表示可以更快检测到邻居失败，但会浪费更多网络带宽。不建议该值配置过小。

根据 RFC4861 规定，邻居的实际可达时间要在配置的时间基础上进行一定浮动，范围在配置事件的 0.5 倍到 1.5 倍之间。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
设置接口上通过 NDP 动态学到的邻居处于可达状态的时间	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 在全局配置视图下执行命令 <code>interface vlan vlan-id</code> 进入 VLAN IF 配置视图；</li> <li>3. 执行命令 <code>ipv6 nd reachable-time reachable-value</code>。</li> </ol>	<code>reachable-value</code> ：指定接口上通过 NDP 动态学到的邻居处于可达状态的时间，取值范围是 30~3600，单位：秒
恢复接口上通过 NDP 动态学到的邻居处于可达状态的时间为默认值	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 在全局配置视图下执行命令 <code>interface vlan vlan-id</code> 进入 VLAN IF 配置视图；</li> <li>3. 执行命令 <code>ipv6 nd reachable-time default</code>。</li> </ol>	<code>default</code> ：表示默认值 300 秒

### 3.3.4 配置 IPv6 调试功能

#### 目的

本节介绍 IPv6 收发包、邻居发现、路由等调试功能。本操作用于维护及调试设备 IPv6 协议栈。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
打开 IPv6 ICMP 调试功能	<ol style="list-style-type: none"> <li>1. 进入特权用户视图；</li> <li>2. 执行命令 <code>debug icmp6 all</code> 打开该调试功能。</li> </ol>	缺省情况下，该调试功能是关闭的。
关闭 IPv6 ICMP 调试功能	<ol style="list-style-type: none"> <li>1. 进入特权用户视图；</li> <li>2. 执行命令 <code>no debug icmp6 all</code> 关闭该调试功能。</li> </ol>	
打开 IPv6 TCP 调试功能	<ol style="list-style-type: none"> <li>1. 进入特权用户视图；</li> <li>2. 执行命令 <code>debug tcp6 { in   out   error   event   all }</code> 打开该调试功能。</li> </ol>	缺省情况下，该调试功能是关闭的。
关闭 IPv6 TCP 调试功能	<ol style="list-style-type: none"> <li>1. 进入特权用户视图；</li> <li>2. 执行命令 <code>no debug tcp6 { in   out   error   event   all }</code> 关闭该调试功能。</li> </ol>	
打开 IPv6 UDP 调试功能	<ol style="list-style-type: none"> <li>1. 进入特权用户视图；</li> <li>2. 执行命令 <code>debug udp6 { in   out   error   all }</code> 打开该调试功能。</li> </ol>	缺省情况下，该调试功能是关闭的。



目的	步骤	参数说明
关闭 IPv6 UDP 调试功能	<ol style="list-style-type: none"> <li>1. 进入特权用户视图；</li> <li>2. 执行命令 <code>no debug udp6 { in   out   error   all }</code> 关闭该调试功能。</li> </ol>	

### 3.3.5 查看 IPv6 配置信息

#### 目的

本节介绍如何查询 IPv6 配置信息。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
查看接口 IPv6 基本信息	<ol style="list-style-type: none"> <li>1. 进入普通用户视图或特权用户视图；</li> <li>2. 执行命令 <code>show ipv6 interface</code> 或 <code>show ipv6 interface vlan-id</code>。</li> </ol>	vlan-id: 指定 VLAN ID, 整数形式, 取值范围是 1~4094
查看设备上所有 IPv6 邻居节点信息	<ol style="list-style-type: none"> <li>1. 进入普通用户视图或特权用户视图；</li> <li>2. 执行命令 <code>show ipv6 neighbor</code>。</li> </ol>	-
查看设备 IPv6 路由条目信息	<ol style="list-style-type: none"> <li>1. 进入普通用户视图或特权用户视图；</li> <li>2. 执行命令 <code>show ipv6 route</code>。</li> </ol>	-

### 3.3.6 配置举例

#### 组网要求

两台 SC9600 通过 `gigaethernet1/0/1` 相连，该接口分别加入 `VLANIF10`，现在为 `VLANIF10` 配置 IPv6 全球单播地址，使其互通。

#### 组网图

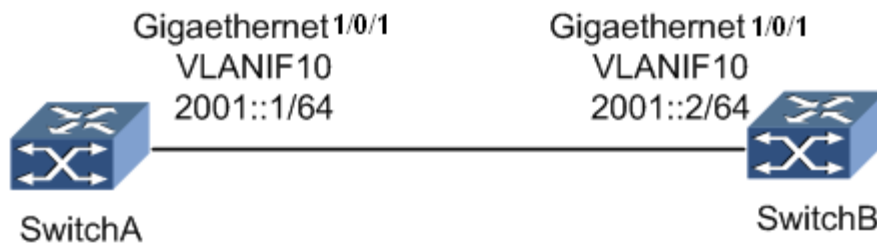


图 3-2 IPv6 地址配置拓扑图

### 配置步骤

1、配置 SC9600A 的 VLAN10 接口的 IP 地址。

```
SC9600A#configure
SC9600A(config)#interface vlan 10
//使能接口 IPv6 功能。
SC9600A(config-vlan-10)#ipv6 enable
SC9600A(config-vlan-10)#ipv6 address 2001::1/64
SC9600A(config-vlan-10)#quit
SC9600A(config)#
SC9600A(config)#interface gigabitEthernet 1/0/1
SC9600A(config-gigabitEthernet-1/0/1)#port hybrid vlan 10 untagged
SC9600A(config-gigabitEthernet-1/0/1)#port hybrid pvid 10
SC9600A(config-gigabitEthernet-1/0/1)#quit
```

2、配置 SC9600B 的 VLAN10 接口的 IP 地址。

```
SC9600B#configure
SC9600B(config)#interface vlan 10
//使能接口 IPv6 功能。
SC9600B(config-vlan-10)#ipv6 enable
SC9600B(config-vlan-10)#ipv6 address 2001::2/64
SC9600B(config-vlan-10)#quit
SC9600B(config)#
SC9600B(config)#interface gigabitEthernet 1/0/1
SC9600B(config-gigabitEthernet-1/0/1)#port hybrid vlan 10 untagged
SC9600B(config-gigabitEthernet-1/0/1)#port hybrid pvid 10
SC9600B(config-gigabitEthernet-1/0/1)#quit
```

## 3.4 DHCP 配置

### 3.4.1 DHCP 简介

#### 技术背景

连接到 Internet 的计算机需要在发送或接收数据报前知道其 IP 地址和其他信息，如网关地址、使用的子网掩码和域名服务器的地址。计算机可以通过 BOOTP 协议获取这些

信息。BOOTP 协议 (Bootstrap Protocol) 是一种较早出现的远程启动的协议, 通过与远程服务器通信以获取通信所需的必要信息, 主要用于无磁盘的客户端从服务器得到自己的 IP 地址、服务器的 IP 地址、启动映像文件名、网关 IP 地址等等。

BOOTP 设计用于相对静态的环境, 每台主机都有一个永久的网络连接。管理人员创建一个 BOOTP 配置文件, 该文件定义了每台主机的一组 BOOTP 参数。由于配置通常保持不变, 该文件不会经常改变。典型情况下, 配置将保持数星期不变。

随着网络规模的不断扩大和网络复杂度的提高, 经常出现计算机的数量超过可供分配的 IP 地址的情况。同时随着便携机及无线网络的广泛使用, 计算机的位置也经常变化, 相应的 IP 地址也必须经常更新, 从而导致网络配置越来越复杂。DHCP (Dynamic Host Configuration Protocol, 动态主机配置协议) 就是为满足这些需求而发展起来的。DHCP 采用客户端/服务器通信模式, 由客户端向服务器提出配置申请, 服务器返回 IP 地址等相应的配置信息, 以实现 IP 地址等信息的动态配置。

### 技术优点

DHCP 采用客户端/服务器的通信模式。所有的 IP 网络配置参数都由 DHCP 服务器集中管理, 并负责处理客户端的 DHCP 请求; 而客户端则会使用服务器分配的 IP 网络参数进行通信。

针对客户端的不同需求, DHCP 提供三种 IP 地址分配策略:

- 手工分配地址: 由管理员为少数特定客户端 (如 WWW 服务器等) 静态绑定固定的 IP 地址, 通过 DHCP 将配置的固定 IP 地址发给客户端;
- 自动分配地址: DHCP 为客户端分配租期为无限长的 IP 地址;
- 动态分配地址: DHCP 为客户端分配有有效期限的 IP 地址, 到达使用期限后, 客户端需要重新申请地址。

管理员可以选择 DHCP 采用哪种策略响应每个网络或每台主机。

DHCP 从两个方面扩充了 BOOTP:

- DHCP 允许计算机快速、动态的获取 IP 地址。为使用 DHCP 的动态地址分配机制, 管理员必须配置 DHCP 服务器, 使其能提供一组 IP 地址, 称之为地址池。任何时候一旦有新的计算机连接到网络上, 该计算机就与服务器联系, 并申请一个 IP 地址。服务器从配置的地址池选择一个地址, 并将它分配给该计算机。
- 与 BOOTP 相比, DHCP 可以为客户端提供更加丰富的网络配置信息。

### DHCP server 应用环境

在以下场合通常利用 DHCP 服务器来完成 IP 地址分配：

1. 网络规模较大，手工配置需要很大的工作量，并难以对整个网络进行集中管理。
2. 网络中主机数目大于该网络支持的 IP 地址数量，无法给每个主机分配一个固定的 IP 地址，且对同时接入网络的用户数目也有限制（比如，Internet 接入服务提供商即属于这种情况），大量用户必须通过 DHCP 服务动态获取 IP 地址。
3. 网络中只有少数主机需要固定的 IP 地址，大多数主机没有固定 IP 地址的需求。

DHCP Server 从地址池中为客户端选择并分配 IP 地址及其他相关参数。当作为 DHCP 服务器的设备收到 Client 发来的 DHCP 请求时，将根据配置选择合适的地址池，并从中挑选一个空闲的 IP 地址，与其他相关参数（如 DNS 服务器地址、地址租用期限等）一起发送给客户端。

Dhcp client 通过 DHCP server 获取 IP 地址的同时，如果 Server 支持 option43 功能，则发送的回应包中包含配置的 option 43 选项。

Option43 的内容可以通过命令行配置，默认情况下，设备没有使能该功能。

如果 DHCP 服务器支持 option 82 功能，当 DHCP 服务器收到 DHCP 中继转发来的带有 option 82 选项的报文后，会正常处理，为客户端分配 IP 地址等信息。发送的回应包中将包含请求包中的 option82 选项内容。

如果 DHCP 服务器不支持 option 82 功能，则当 DHCP 服务器收到 DHCP 中继转发来的带有 option 82 选项的报文，不会进行处理。

### DHCP server 安全功能

#### 1. 伪服务器检测功能

在网络中，如果有私自架设的 DHCP 服务器，当其他用户申请 IP 地址时，这台 DHCP 服务器就会与 DHCP 客户端进行交互，导致用户获得错误的 IP 地址，无法正常上网，这种私设的 DHCP 服务器称为伪 DHCP 服务器。

在 DHCP 服务器上使能伪 DHCP 服务器检测功能后，当 DHCP 客户端发送 DHCP-REQUEST 报文时，DHCP 服务器会从报文中获取给客户端分配 IP 地址的服务器的 IP 地址，并记录此 IP 地址及接收到报文的接口信息，以便管理员及时发现并处理伪 DHCP 服务器。

#### 2. IP 地址重复检测功能

为防止 IP 地址重复分配导致地址冲突，DHCP 服务器为客户端分配地址前，需要先对该地址进行探测。

地址探测是通过 ping 功能实现的，通过检测是否能在指定时间内得到 ping 响应来判断是否有地址冲突。DHCP 服务器发送目的地址为待分配地址的 ICMP 报文，如果在指定时间内没有得到响应，则继续发送 ICMP 报文，直到 ping 操作的次数达到最大值，如果仍然没有得到响应，则将地址分配给客户端，从而确保分配给客户端的 IP 地址是唯一的。

### 3. 地址匹配检测功能（防静态 IP 用户功能）

DHCP Server 给用户分配 IP 地址时，会记录 IP 地址和 MAC 的绑定关系，用户也可以手工配置用户地址表项，即 IP 地址与 MAC 地址的静态绑定。为了防止非法用户静态配置一个 IP 地址，并访问其他网络，当设备上使能了该功能后，如果用户配置的 IP 地址与用户的 MAC 地址的对应关系没有在 DHCP Server 的用户地址表中（包括 DHCP 动态记录的表项以及手工配置的用户地址表项），则 DHCP Server 将不允许该用户访问外部网络。该功能只对 DHCP Client 和 Server 在同一网段的情况。

#### DHCP relay 应用环境

原始的 DHCP 协议要求客户端和服务端只能在同一个子网内，不可以跨网段工作。因此，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，这显然是不经济的。DHCP 中继（DHCP Relay）的引入解决了这一问题，它在处于不同网段间的 DHCP 客户端和服务端之间承担中继服务，将 DHCP 协议报文跨网段中继到目的 DHCP 服务器，于是不同网络上的 DHCP 客户端可以共同使用一个 DHCP 服务器，既节省了成本，又便于进行集中管理。

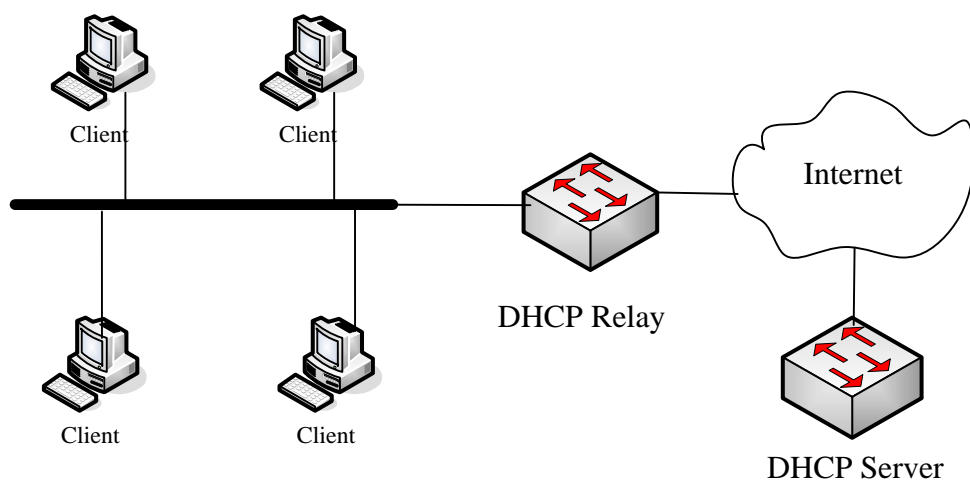


图 3-3 DHCP Relay 应用环境

DHCP Relay 处于不同网段间的 DHCP 客户端和服务端之间,为 DHCP client 和 Server 提供中继服务。

### DHCP relay 原理

DHCP 中继的工作过程如图所示。

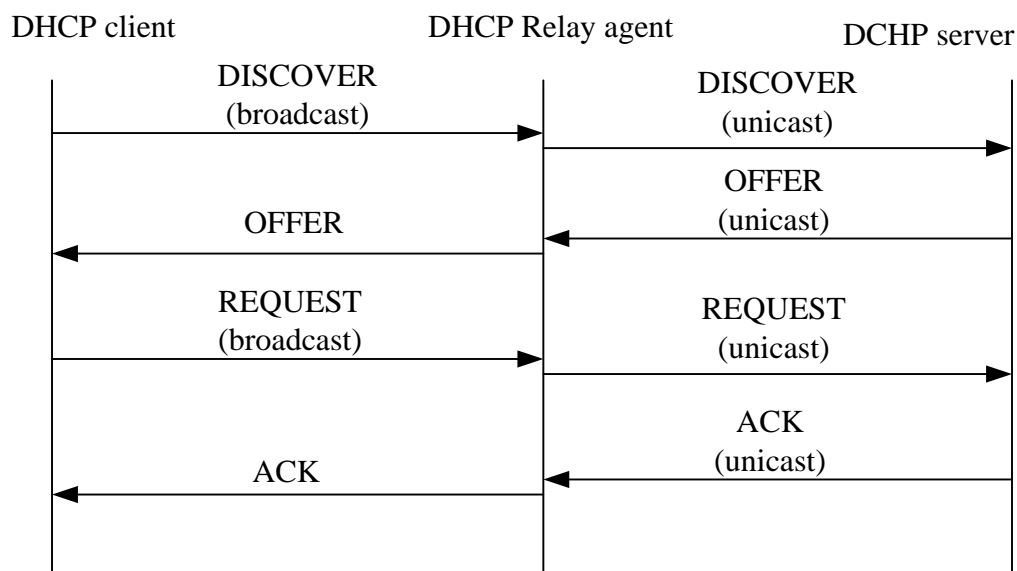


图 3-4 DHCP Relay 工作示意图

1. DHCP 中继接收到 DISCOVER 或 REQUEST 报文后,将进行如下处理:
  - 为防止 DHCP 报文形成环路,抛弃报文头中 hops 字段的值大于限定跳数的 DHCP 请求报文。否则,继续进行下面的操作。
  - 检查 giaddr 字段。如果是 0,需要将 giaddr 字段设置为接收请求报文的接口 IP 地址。如果接口有多个 IP 地址,可选择其一。以后从该接口接收的所有请求报文都使用该 IP 地址。如果 giaddr 字段不是 0,则不修改该字段。
  - 将 hops 字段增加 1,表明又经过一次 DHCP 中继。
  - 将请求报文的 TTL 设置为 DHCP 中继设备的 TTL 缺省值,而不是原来请求报文的 TTL 减 1。对中继报文的环路问题和跳数限制问题都可以通过 hops 字段来解决。

- DHCP 请求报文的地址修改为 DHCP 服务器或下一个 DHCP 中继的 IP 地址。从而，将 DHCP 请求报文中继转发给 DHCP 服务器或下一个 DHCP 中继。
- 2. DHCP 服务器根据 giaddr 字段为客户端分配 IP 地址等参数，并将 DHCP 应答报文发送给 giaddr 字段标识的 DHCP 中继。DHCP 中继接收到 DHCP 应答报文后，会进行如下处理：
  - DHCP 中继假设所有的应答报文都是发给直连的 DHCP 客户端。giaddr 字段用来识别与客户端直连的接口。如果 giaddr 不是本地接口的地址，DHCP 中继将丢弃应答报文。
  - DHCP 中继检查报文的广播标志位。如果广播标志位为 1，则将 DHCP 应答报文广播发送给 DHCP 客户端；否则将 DHCP 应答报单播发送给 DHCP 客户端，其目的地址为 yiaddr，链路层地址为 chaddr。

当 DHCP 服务器和客户端不在同一个子网内时，客户端要想从 DHCP 服务器上分配到 IP 地址，就必须由 DHCP 中继代理 (DHCP Relay Agent) 来转发 DHCP 请求包。DHCP 中继代理将客户端的 DHCP 报文转发到 DHCP 服务器之前，可以插入一些选项信息，以便 DHCP 服务器能更精确的得知客户端的信息，从而能更灵活的按相应的策略分配 IP 地址和其他参数。这个选项被称为：DHCP relay agent information option (中继代理信息选项)，选项号为 82，故又称为 option 82，相关标准文档为 RFC3046。

Option 82 是对 DHCP 选项的扩展应用。选项 82 只是一种应用扩展，是否携带选项 82 并不会影响 DHCP 原有的应用。另外还要看 DHCP 服务器是否支持选项 82。不支持选项 82 的 DHCP 服务器接收到插入了选项 82 的报文，或者支持选项 82 的 DHCP 服务器接收到了没有插入选项 82 的报文，这两种情况都不会对原有的基本的 DHCP 服务造成影响。要想支持选项 82 带来的扩展应用，则 DHCP 服务器本身必须支持选项 82 以及收到的 DHCP 报文必须被插入选项 82 信息。

Option 82 能够标识不同的用户，服务器可以根据 Option 82 为不同的用户分配不同的 IP 地址，从而实现 QoS、安全和计费的管理。

### DHCP Relay 安全功能

#### 1. 地址匹配检测功能

当客户端通过 DHCP 中继从 DHCP 服务器获取到 IP 地址时，DHCP 中继会记录 IP 地址与 MAC 地址的绑定关系。用户也可以手工配置用户地址表项，即 IP 地址与 MAC 地址的静态绑定。为了防止非法用户静态配置一个 IP 地址，并访问其他网络，设备支持 DHCP 中继的地址匹配检查功能。当设备上使能了该功能后，如果用户

配置的 IP 地址与用户的 MAC 地址的对应关系没有在 DHCP 中继的用户地址表中（包括 DHCP 中继动态记录的表项以及手工配置的用户地址表项），则 DHCP 中继将不允许该用户访问外部网络。

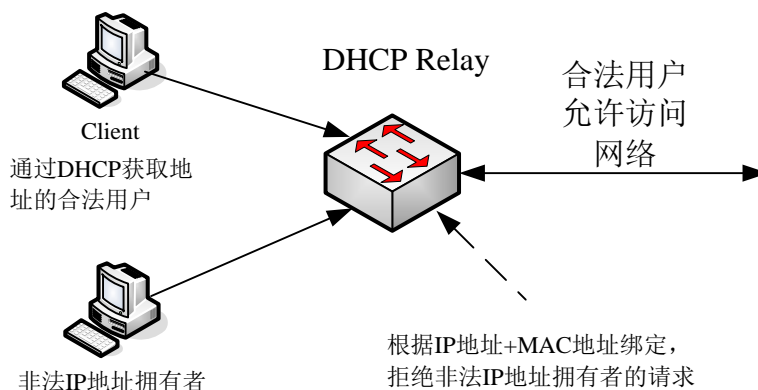


图 3-5 DHCP 安全示意图

如图所示，DHCP 安全实现的基本功能如下：

#### 1) 合法用户 IP 地址表的管理

维护一张用户地址表，所有合法用户都记录在表项中。

当客户端通过 DHCP 中继从 DHCP 服务器获取到 IP 地址时，DHCP 中继可以自动记录客户端 IP 地址与 MAC 地址的绑定关系，生成 DHCP 中继的动态用户地址表项。同时，为满足用户采用合法固定 IP 地址访问外部网络的需求，DHCP 中继也支持静态用户地址表项配置，即在 DHCP 中继上手工配置 IP 地址与 MAC 地址的绑定关系。

#### 2) 禁止非正常获取 IP 地址的用户上网的功能。

该功能需要硬件支持，对于和用户地址表中 MAC 地址与 IP 地址不匹配的数据，DHCP 中继将会丢弃。

#### 2. 用户表项定时刷新功能

当 DHCP 客户端通过 DHCP 中继从 DHCP 服务器获取到 IP 地址时，DHCP 中继会记录 IP 地址与 MAC 地址的绑定关系。由于 DHCP 客户端释放该 IP 地址时，会发送单播 DHCP-RELEASE 报文给 DHCP 服务器，而 DHCP 中继不会处理该报文，造成 DHCP 中继的用户地址项不能被实时刷新。用户可以通过配置 DHCP 中继动态用户地址表项的定时刷新功能，来解决上述问题。



每隔指定时间, DHCP 中继以客户端分配到的 IP 地址和自己的 MAC 地址向 DHCP 服务器发送 DHCP-REQUEST 报文:

- 如果 DHCP 服务器响应 DHCP-ACK 报文, 则表明这个 IP 地址已经可以进行分配, DHCP 中继会将动态用户地址表中对应的表项老化掉;
- 如果 DHCP 服务器响应 DHCP-NAK 报文, 则表示该 IP 地址的租约仍然存在, DHCP 中继不会老化该 IP 地址对应的表项。

### 3. 伪服务器检测功能

如果网络中有私自架设的 DHCP 服务器, 当客户端申请 IP 地址时, 这台 DHCP 服务器就会与 DHCP 客户端进行交互, 导致客户端获得错误的 IP 地址, 这种私设的 DHCP 服务器称为伪 DHCP 服务器。

在 DHCP Relay 上使能伪 DHCP 服务器检测功能后, 当 DHCP 客户端发送 DHCP-REQUEST 报文时, DHCP Relay 会从报文中获取给客户端分配 IP 地址的服务器的 IP 地址, 并记录此 IP 地址及接收到报文的接口信息, 以便管理员及时发现并处理伪 DHCP 服务器。

## 3.4.2 DHCP 配置

### 3.4.2.1 DHCP Server 配置

#### 3.4.2.1.1 开启/关闭交换机 DHCP 功能

##### 目的

本节介绍如何开启/关闭交换机 DHCP 功能。缺省情况下, 以太网交换机的 DHCP 功能处于关闭状态。

##### 过程

根据不同目的, 执行相应步骤, 具体参见下表。

目的	步骤	参数说明
开启/关闭交换机 DHCP 功能	1. 在特权用户视图下执行命令 <code>config</code> , 进入全局配置视图; 2. 执行命令 <code>dhcp { start   stop }</code>	-

#### 3.4.2.1.2 开启/关闭交换机 DHCP Server 功能

##### 目的

本节介绍如何开启/关闭交换机 DHCP Server 功能。缺省情况下，以太网交换机接口上 DHCP Server 功能处于关闭状态。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
开启/关闭交换机 DHCP Server 功能	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>config</code>，进入全局配置视图；</li> <li>2. 执行命令 <code>interface vlan-number</code>，进入 VLANIF 配置视图；</li> <li>3. 执行命令 <code>ip dhcp server</code> 或 <code>no ip dhcp</code></li> </ol>	<p><code>vlan-number</code>: VLAN ID, 整数形式, 取值范围是 1~4094;</p>

### 3.4.2.1.3 创建 DHCP 地址池

#### 目的

本节介绍如何创建 DHCP 地址池并进入 DHCP pool 配置视图。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
创建 DHCP 地址池	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>config</code>，进入全局配置视图；</li> <li>2. 执行命令 <code>dhcp pool pool-number</code></li> </ol>	<p><code>pool-number</code>: 指定地址池序号, 整数形式, 取值范围是 1~64;</p>
删除 DHCP 地址池	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>config</code>，进入全局配置视图；</li> <li>2. 执行命令 <code>no dhcp pool pool-number</code></li> </ol>	<p><code>pool-number</code>: 指定地址池序号, 整数形式, 取值范围是 1~64;</p>

### 3.4.2.1.4 配置 DHCP 地址池范围

#### 目的

本节介绍如何配置 DHCP 地址池范围。缺省情况下，没有配置动态分配的范围，即地址池中没有可供分配的地址。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
----	----	------

目的	步骤	参数说明
配置 DHCP 地址池范围	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>config</code>, 进入全局配置视图;</li> <li>2. 执行命令 <code>dhcp pool pool-number</code>, 进入 DHCP pool 配置视图;</li> <li>3. 执行命令 <code>network range start-ip-address end-ip-address mask mask-address</code></li> </ol>	<p><code>pool-number</code>: 指定地址池序号, 整数形式, 取值范围是 1~64;</p> <p><code>start-ip-address</code>: 指定可分配的起始 IP 地址, 点分十进制;</p> <p><code>end-ip-address</code>: 指定可分配的终结 IP 地址, 点分十进制;</p> <p><code>mask-address</code>: 指定掩码地址, 点分十进制;</p> <p><code>ip-address</code>: 指定网络地址, 点分十进制;</p>

### 3.4.2.1.5 配置 DHCP 地址池租用时间

#### 目的

本节介绍如何配置 DHCP 地址池租用时间。

#### 过程

根据不同目的, 执行相应步骤, 具体参见下表。

目的	步骤	参数说明
配置 DHCP 地址池租用时间	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>config</code>, 进入全局配置视图;</li> <li>2. 执行命令 <code>dhcp pool pool-number</code>, 进入 DHCP pool 配置视图;</li> <li>3. 执行命令 <code>lease-time { time   default }</code></li> </ol>	<p><code>pool-number</code>: 指定地址池序号, 整数形式, 取值范围是 1~64;</p> <p><code>time</code>: 指定租赁期有效时间, 整数形式, 取值范围是 1~120, 单位: 小时;</p> <p><code>default</code>: 默认租赁有效时间, 24 小时;</p>

### 3.4.2.1.6 配置 DHCP 地址池网关

#### 目的

本节介绍如何配置 DHCP 地址池网关。缺省情况下, 没有配置地址池的网关。

#### 过程

根据不同目的, 执行相应步骤, 具体参见下表。

目的	步骤	参数说明
配置 DHCP 地址池网关	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>config</code>, 进入全局配置视图;</li> <li>2. 执行命令 <code>dhcp pool pool-number</code>, 进入 DHCP pool 配置视图;</li> </ol>	<p><code>pool-number</code>: 指定地址池序号, 整数形式, 取值范围是 1~64;</p> <p><code>ip-address</code>: 指定网关 IP 地址, 点分十进制;</p>

目的	步骤	参数说明
	3. 执行命令 <b>gateway ip-address</b>	

### 3.4.2.1.7 配置 DHCP 地址池的 DNS 服务器地址

#### 目的

本节介绍如何配置 DHCP 地址池的 DNS 服务器地址。缺省情况下，没有配置地址池的 DNS 服务器地址，在配置了 dns 服务器后，才能配合 dns backup 服务器。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置 DHCP 地址池的 DNS 服务器地址	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>config</b>，进入全局配置视图；</li> <li>2. 执行命令 <b>dhcp pool pool-number</b>，进入 DHCP pool 配置视图；</li> <li>3. 执行命令 <b>dns ip-address</b> 或 <b>dns ip-address backup</b></li> </ol>	<p><b>pool-number</b>: 指定地址池序号，整数形式，取值范围是 1~64；</p> <p><b>ip-address</b>: 指定 dns 或备用 dns 的 IP 地址，点分十进制；</p>

### 3.4.2.1.8 配置 DHCP 地址池中排除的地址

#### 目的

本节介绍如何配置 DHCP 地址池中排除的地址。缺省情况下，地址池中的所有地址都参与自动分配。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置 DHCP 地址池中排除的地址	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>config</b>，进入全局配置视图；</li> <li>2. 执行命令 <b>dhcp pool pool-number</b>，进入 DHCP pool 配置视图；</li> <li>3. 执行命令 <b>dhcp server forbidden-ip ip-address1 [ ip-address2 ]</b></li> </ol>	<p><b>pool-number</b>: 指定地址池序号，整数形式，取值范围是 1~64；</p> <p><b>ip-address1</b>: 指定不参与自动分配的最小 IP 地址，点分十进制；</p> <p>[ <b>ip-address2</b> ]: 指定不参与自动分配的最大 IP 地址，不能小于 ip-address1。如果不指定该参数，则表示只有一个 IP 地址。点分十进制；</p> <p><b>ip-address</b>: 指定 dns 或备用 dns</p>

目的	步骤	参数说明
		的 IP 地址，点分十进制；
取消 DHCP 地址池中不参与自动分配的 IP 地址	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>config</code>，进入全局配置视图；</li> <li>2. 执行命令 <code>dhcp pool pool-number</code>，进入 DHCP pool 配置视图；</li> <li>3. 执行命令 <code>no dhcp server forbidden-ip ip-address1 [ ip-address2 ]</code></li> </ol>	<p><code>pool-number</code>: 指定地址池序号，整数形式，取值范围是 1~64；</p> <p><code>ip-address1</code>: 指定不参与自动分配的最小 IP 地址，点分十进制；</p> <p>[ <code>ip-address2</code> ]: 指定不参与自动分配的最大 IP 地址，不能小于 <code>ip-address1</code>。如果不指定该参数，则表示只有一个 IP 地址。点分十进制；</p> <p><code>ip-address</code>: 指定 dns 或备用 dns 的 IP 地址，点分十进制；</p>

### 3.4.2.1.9 配置 DHCP option82 功能

#### 目的

本节介绍如何配置使能或去使能 DHCP 服务器支持 Option82 功能。缺省情况下，以太网交换机的 DHCP Server option82 功能处于开启状态。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
使能或去使能 DHCP 服务器支持 Option82 功能	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>config</code>，进入全局配置视图；</li> <li>2. 执行命令 <code>dhcp server option82 (enable disable)</code></li> </ol>	<code>ip-address</code> : 指定 dns 或备用 dns 的 IP 地址，点分十进制；

### 3.4.2.1.10 静态绑定方式分配地址

#### 目的

本节介绍如何配置静态绑定方式分配地址。某些客户端（如 WWW 服务器等）需要固定的 IP 地址，可以通过将客户端的 MAC 地址与 IP 地址绑定的方式实现。当具有此 MAC 地址的客户端申请 IP 地址时，DHCP 服务器将根据客户端的 MAC 地址查找到对应的 IP 地址，并分配给客户端。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置静态绑定方式分配地址	<ol style="list-style-type: none"> <li>在特权用户视图下执行命令 <code>config</code>, 进入全局配置视图;</li> <li>执行命令 <code>dhcp server static-bind ip-address mac-address</code></li> </ol>	<p><code>ip-address</code>: 指定绑定的 IP 地址, 必须是地址池中合法的 IP 地址, 点分十进制;</p> <p><code>mac-address</code>: 指定用户的 MAC 地址, 形如 AA:BB:CC:DD:EE:FF, 其中 A~F 为一位十六进制数;</p>

### 3.4.2.1.11 配置 DHCP 地址重复检测功能

#### 目的

本节介绍如何配置 DHCP 地址重复检测功能。缺省情况下, 地址重复检测间隔为 500ms, 如果配置为 0, 则表明不进行检测。

#### 过程

根据不同目的, 执行相应步骤, 具体参见下表。

目的	步骤	参数说明
配置 DHCP 地址重复检测功能	<ol style="list-style-type: none"> <li>在特权用户视图下执行命令 <code>config</code>, 进入全局配置视图;</li> <li>执行命令 <code>dhcp address-check-time { checktime   default }</code></li> </ol>	<p><code>checktime</code>: 指定地址检测冲突的最大时间值, 整数形式, 取值范围是 0~10000, 单位: 毫秒;</p> <p><code>default</code>: 500, 单位: 毫秒;</p>

### 3.4.2.1.12 配置 DHCP 伪服务器检测功能

#### 目的

本节介绍如何配置 DHCP 伪服务器检测功能, 即使能或去使能对伪 DHCP 服务器的检测功能。缺省情况下, DHCP 伪服务器检测功能处于开启状态。

#### 过程

根据不同目的, 执行相应步骤, 具体参见下表。

目的	步骤	参数说明
配置 DHCP 伪服务器检测功能	<ol style="list-style-type: none"> <li>在特权用户视图下执行命令 <code>config</code>, 进入全局配置视图;</li> <li>执行命令 <code>dhcp server detect { enable   disable }</code></li> </ol>	-

### 3.4.2.1.13 查看 DHCP Server 统计信息

#### 目的

本节介绍如何查看 DHCP Server 统计信息

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
查看 DHCP Server 统计信息	1. 在特权用户视图下执行命令 <code>show dhcp server statistics</code>	-
清除 DHCP Server 统计信息	1. 在特权用户视图下执行命令 <code>reset dhcp server statistics</code>	-

3.4.2.1.14 DHCP-Server 显示和调试

目的

本节介绍如何配置 DHCP-Server 显示和调试信息

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
显示 DHCP 的配置信息	1. 进入普通用户视图或特权用户视图； 2. 执行命令 <code>show dhcp</code>	-
显示 DHCP Server 的地址池配置信息	1. 进入普通用户视图或特权用户视图； 2. 执行命令 <code>show dhcp pool</code>	-
显示 DHCP Server 配置信息	1. 进入普通用户视图或特权用户视图； 2. 执行命令 <code>show dhcp server</code>	-
显示 DHCP Server 中发生冲突的地址	1. 进入普通用户视图或特权用户视图； 2. 执行命令 <code>show dhcp server conflict</code>	-
显示分配的地址	1. 进入普通用户视图或特权用户视图； 2. 执行命令 <code>show dhcp bind-entry</code>	-
显示可用的地址信息	1. 进入普通用户视图或特权用户视图； 2. 执行命令 <code>show dhcp lease-entry</code>	-
调试 DHCP	1. 进入普通用户视图或特权用户视图； 2. 执行命令 <code>debug dhcp server</code> 或 <code>no debug dhcp server</code>	-

### 3.4.2.2 DHCP Relay 配置

#### 3.4.2.2.1 开启/关闭 DHCP Relay 功能

##### 目的

本节介绍如何开启/关闭 DHCP Relay 功能。缺省情况下，以太网交换机接口上的 DHCP-Relay 功能处于关闭状态。在接口上配置 DHCP Relay 功能时，需要在全局下打开 DHCP 开关。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
开启 / 关闭 DHCP Relay 功能	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>config</code>，进入全局配置视图；</li> <li>2. 执行命令 <code>interface vlan-number</code>，进入 VLANIF 配置视图；</li> <li>3. 执行命令 <code>ip dhcp relay</code> 或 <code>no ip dhcp</code></li> </ol>	<p><code>vlan-number</code>: VLAN ID, 整数形式, 取值范围是 1~4094;</p>

#### 3.4.2.2.2 配置 Relay 的 Server-ip

##### 目的

本节介绍如何配置 Relay 的 Server-ip。缺省情况下，接口上没有配置任何 server-ip，多次重复这个命令，可以配置多个 IP 地址，最多可以配置 3 个。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置 Relay 的 Server-ip	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>config</code>，进入全局配置视图；</li> <li>2. 执行命令 <code>interface vlan-number</code>，进入 VLANIF 配置视图；</li> <li>3. 执行命令 <code>dhcp relay server-ip ip-address</code></li> </ol>	<p><code>vlan-number</code>: VLAN ID, 整数形式, 取值范围是 1~4094;</p> <p><code>ip-address</code>: 指定 DHCP 中继所代理的 DHCP 服务器的 IP 地址, 点分十进制;</p>
删除配置的 Relay Server-ip	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>config</code>，进入全局配置视图；</li> <li>2. 执行命令 <code>interface vlan-number</code>，进入 VLANIF 配置视图；</li> <li>3. 执行命令 <code>no dhcp relay server-ip ip-address</code></li> </ol>	<p><code>vlan-number</code>: VLAN ID, 整数形式, 取值范围是 1~4094;</p> <p><code>ip-address</code>: 指定 DHCP 中继所代理的 DHCP 服务器的 IP 地址, 点分十进制;</p>



### 3.4.2.2.3 开启/关闭 option82 功能

#### 目的

本节介绍如何开启/关闭 option82 功能，即使能或去使能 DHCP 中继支持 Option82 功能。缺省情况下，以太网交换机的 DHCP-Relay option82 功能处于关闭状态。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
使能或去使能 DHCP 中继支持 Option82 功能	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>config</code>，进入全局配置视图；</li> <li>2. 执行命令 <code>interface vlan-number</code>，进入 VLANIF 配置视图；</li> <li>3. 执行命令 <code>dhcp option82 { enable   disable }</code></li> </ol>	<p><code>vlan-number</code>: VLAN ID，整数形式，取值范围是 1~4094；</p>

### 3.4.2.2.4 配置 option82 处理策略

#### 目的

本节介绍如何配置 option82 处理策略。缺省情况下，Relay option82 选项的处理策略为 keep。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置 option82 处理策略	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>config</code>，进入全局配置视图；</li> <li>2. 执行命令 <code>interface vlan-number</code>，进入 VLANIF 配置视图；</li> <li>3. 执行命令 <code>dhcp option82 { drop   keep   replace }</code></li> </ol>	<p><code>vlan-number</code>: VLAN ID，整数形式，取值范围是 1~4094；</p> <p><code>drop</code>: 若报文中携带 Option82 选项，则丢弃该报文；</p> <p><code>keep</code>: 若报文中携带 Option82 选项，则保持该报文中的 Option82 选项不变并进行转发；</p> <p><code>replace</code>: 若报文中携带 Option82 选项，则按照配置的填充内容填充 Option82 选项，替换报文中原有的 Option82 选项并进行转发；</p>

### 3.4.2.2.5 配置 circuit-id 子选项

#### 目的

本节介绍如何配置 circuit-id 子选项。缺省情况下，没有配置该选项。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置 circuit-id 子选项	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>config</code>，进入全局配置视图；</li> <li>2. 执行命令 <code>interface vlan-number</code>，进入 VLANIF 配置视图；</li> <li>3. 执行命令 <code>dhcp option82 circuit-id circuitid</code></li> </ol>	<p><b>vlan-number</b>: VLAN ID，整数形式，取值范围是 1~4094；</p> <p><b>circuit-id</b>: DHCP 中继代理信息选项的一个子选项：电路 ID，字符串形式；</p>
删除配置的 circuit-id 子选项	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>config</code>，进入全局配置视图；</li> <li>2. 执行命令 <code>interface vlan-number</code>，进入 VLANIF 配置视图；</li> <li>3. 执行命令 <code>no dhcp option82 circuit-id</code></li> </ol>	<p><b>vlan-number</b>: VLAN ID，整数形式，取值范围是 1~4094；</p>

### 3.4.2.2.6 配置 remote-id 子选项

#### 目的

本节介绍如何配置 remote-id 子选项。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置 remote-id 子选项	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>config</code>，进入全局配置视图；</li> <li>2. 执行命令 <code>interface vlan-number</code>，进入 VLANIF 配置视图；</li> <li>3. 执行命令 <code>dhcp option82 remote-id remoteid</code></li> </ol>	<p><b>vlan-number</b>: VLAN ID，整数形式，取值范围是 1~4094；</p> <p><b>remoteid</b>: 指定用户自定义的代理远程 ID 子选项内容</p> <p>默认情况下 Remote ID 包含的内容为设备的 mac 地址，如果用命令行配置该子选项的内容，则 option82 中 Remote ID 选项为配置的内容。字符串形式，区分大小写；</p>

目的	步骤	参数说明
删除配置的 remote-id 子选项	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>config</code>, 进入全局配置视图;</li> <li>2. 执行命令 <code>interface vlan-number</code>, 进入 VLANIF 配置视图;</li> <li>3. 执行命令 <code>no dhcp option82 remote-id</code></li> </ol>	<p>vlan-number: VLAN ID, 整数形式, 取值范围是 1~4094;</p>

#### 3.4.2.2.7 配置 Relay 的静态绑定条目

##### 目的

本节介绍如何配置 Relay 的静态绑定条目。

##### 过程

根据不同目的, 执行相应步骤, 具体参见下表。

目的	步骤	参数说明
配置 Relay 的静态绑定条目	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>config</code>, 进入全局配置视图;</li> <li>2. 执行命令 <code>dhcp relay static-bind ip-address mac-address</code></li> </ol>	<p>ip-address: 指定 DHCP 客户端的 IP 地址, 点分十进制;</p> <p>mac-address: 指定 DHCP 客户端的 MAC 地址, 形如 AA:BB:CC:DD:EE:FF, 其中 A~F 为一位十六进制数;</p>
删除配置的 Relay 静态绑定条目	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>config</code>, 进入全局配置视图;</li> <li>2. 执行命令 <code>no dhcp relay bind ip-address</code></li> </ol>	<p>ip-address: 指定 DHCP 客户端的 IP 地址, 点分十进制;</p>

#### 3.4.2.2.8 配置 DHCP 伪服务器检测功能

##### 目的

本节介绍如何配置 DHCP 伪服务器检测功能。缺省情况下, DHCP 伪服务器检测功能处于开启状态。

##### 过程

根据不同目的, 执行相应步骤, 具体参见下表。

目的	步骤	参数说明
配置 DHCP 伪服务器检测功能	1. 在特权用户视图下执行命令 <code>config</code> , 进入全局配置视图; 2. 执行命令 <code>dhcp server detect { enable   disable }</code>	-
查看记录的伪服务器信息	1. 在特权用户视图下执行命令 <code>debug dhcp fake-server</code>	-

### 3.4.2.2.9 查看 DHCP Relay 统计信息

#### 目的

本节介绍如何查看 DHCP Relay 统计信息。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
查看 DHCP Relay 统计信息	1. 在特权用户视图下执行命令 <code>show dhcprelay statistics</code>	-
清除 DHCP Relay 统计信息	1. 在特权用户视图下执行命令 <code>reset dhcp relay statistics</code>	-

### 3.4.2.2.10 DHCP Relay 显示和调试

#### 目的

本节介绍如何进行 DHCP Relay 显示和调试。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
显示 DHCP-Relay 的配置信息	1. 进入普通用户视图或特权用户视图; 2. 执行命令 <code>show dhcp relay</code>	-
显示 DHCP-Relay 的用户信息	1. 进入普通用户视图或特权用户视图; 2. 执行命令 <code>show dhcp relay user</code>	-
显示 DHCP 的全局配置信息	1. 进入普通用户视图或特权用户视图; 2. 执行命令 <code>show dhcp</code>	-
打开 / 关闭 DHCP-Relay 的	1. 进入普通用户视图或特权用户视图; 2. 执行命令 <code>(no) debug dhcp relay</code>	-

目的	步骤	参数说明
调试开关		

### 3.4.3 配置举例

#### 组网要求

常见的 DHCP 组网方式可分为两类：

1. DHCP 服务器和客户端都在一个子网内，直接进行 DHCP 协议的交互；
2. DHCP 服务器和客户端分别处于不同的子网中，必须通过 DHCP 中继实现 IP 地址的分配。无论哪种情况下，DHCP 服务器的配置都是差不多的。

DHCP 服务器为处于不同网段中的客户端动态分配 IP 地址，用户所在的网段分别为 10.1.1.0/24 和 10.1.2.0/24。

具体需求如下：

- 10.1.1.0/24 网段内的地址租用期限为 12 小时，DNS 服务器地址为 10.1.1.200，出口网关的地址为 10.1.1.1。
- 10.1.2.0/24 网段内的地址租用期限为 24 小时，DNS 服务器地址为 10.1.2.200，出口网关的地址为 10.1.2.1。

#### 组网图

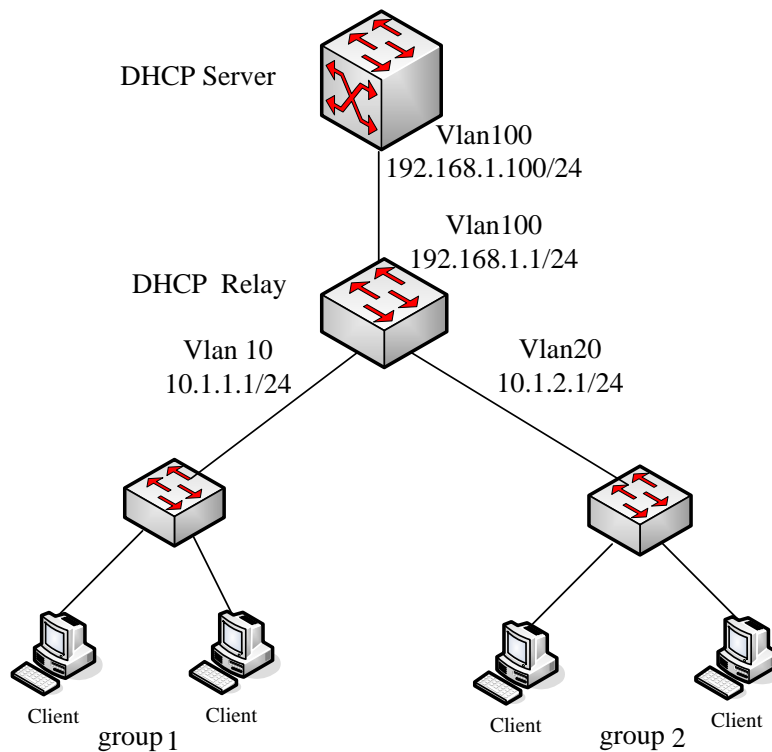


图 3-6 DHCP 组网图

### 配置步骤

#### 1、DHCP server 配置:

# 配置 DHCP Server 的 Vlan-interface10 接口的 IP 地址。

```
SC9600#configure
```

```
SC9600 (config)#dhcp enable
```

```
SC9600 (config)#interface vlan 100
```

```
SC9600 (config-vlan-100)#ip address 192.168.1.100/24
```

```
SC9600 (config-vlan-100)#ip dhcp server
```

# 配置地址池 1: 地址池范围、有效期, 并配置指定的 DNS 服务器。

```
SC9600 (config)#dhcp pool 1
```

```
SC9600 (config-dhcp-pool-1)#network range 10.1.1.2 10.1.1.100 mask 255.255.255.0
```

```
SC9600 (config-dhcp-pool-1)#gateway 10.1.1.1
```

```
SC9600 (config-dhcp-pool-1)#lease-time 12
```

```
SC9600 (config-dhcp-pool-1)# dns 10.1.1.200
```

# 配置地址池 2: 地址池范围、有效期, 并配置指定的 DNS 服务器。

```
SC9600 (config)#dhcp pool 2
```

```
SC9600 (config-dhcp-pool-2)#network range 10.1.2.2 10.1.2.100 mask 255.255.255.0
```

```
SC9600 (config-dhcp-pool-2)#gateway 10.1.2.1
```

```
SC9600 (config-dhcp-pool-2)#lease-time 24
```

```
SC9600 (config-dhcp-pool-2)# dns 10.1.2.200
```

2、DHCP Relay 配置:

# 配置 DHCP Relay 的 Vlan-interface20 接口的 IP 地址, 并配置为 Relay 模式。

```
SC9600 #configure
```

```
SC9600 (config)#dhcp enable
```

```
SC9600 (config)#interface vlan 10
```

```
SC9600 (config-vlan-10)#ip address 10.1.1.1/24
```

```
SC9600 (config-vlan-10)#ip dhcp relay
```

```
SC9600 (config-vlan-10)#dhcp relay server-ip 192.168.1.100
```

# 配置 DHCP Relay 的 Vlan-interface20 接口的 IP 地址, 并配置为 Relay 模式。

```
SC9600 #configure
```

```
SC9600 (config)#interface vlan 20
```

```
SC9600 (config-vlan-20)#ip address 10.1.2.1/24
```

```
SC9600 (config-vlan-20)#ip dhcp relay
```

```
SC9600 (config-vlan-20)#dhcp relay server-ip 192.168.1.100
```

# 配置 DHCP Relay 的 Vlan-interface100 接口的 IP 地址, 并配置 relay 模式。

```
SC9600 #configure
```

```
SC9600 (config)#interface vlan 100
```

```
SC9600 (config-vlan-100)#ip address 1.1.1.1/24
```

```
SC9600 (config-vlan-100)#ip dhcp relay
```

#### 注意事项

- 只有使能 DHCP Relay 功能之后, DHCP Option 82 功能才能生效。
- DHCP option 82 功能建议在最靠近 DHCP client 的设备上使用, 以达到精确定位用户位置的目的。

## 第4章 三层 IP 路由配置

### 4.1 概述

本章介绍了 SC9600 系列高端交换机路由相关的基本内容、配置过程和配置举例。

本章包括如下主题：

内容	页码
4.1 概述	4-1
4.2 RIP 配置	4-1
4.3 RIPng 配置	4-20
4.4 OSPF 配置	4-38
4.5 IPv6 OSPFv3 配置	4-101
4.6 BGP 配置	4-145
4.7 ISIS 配置	4-186
4.8 路由策略配置	4-215

### 4.2 RIP 配置

#### 4.2.1 RIP 简介

##### 4.2.1.1 RIP 操作

RIP 是使用最广泛的一种 IGP 路由信息协议。它把路由选择的参与者分为主动（**active**）机器和被动（**passive**）机器。被动机器即为静默（**silent**）机器。主动路由器向其他路由器通告其路由，而被动路由器接收通告并在此基础上更新其路由，但它们自己并不通告路由。RIP 中存在着许多细微的规则，它们决定了传播哪些路由，以及何时传播这些路由。这些规则帮助我们避免了形成路由环路，并且使路由传播更快，更可靠。

##### 4.2.1.2 RIP 工作机制

###### RIP 的基本概念



RIP 是一种基于距离矢量（Distance-Vector, D-V）算法的协议，它通过 UDP 报文进行路由信息的交换，默认使用端口号为 520。

RIP 使用跳数来衡量到达目的地址的距离，跳数称为度量值。在 RIP 中，路由器到与它直接相连网络的跳数为 0，通过一个路由器可达的网络的跳数为 1，其余依此类推。为限制收敛时间，RIP 规定度量值取 0~15 之间的整数，大于或等于 16 的跳数被定义为无穷大，即目的网络或主机不可达。由于这个限制，使得 RIP 不适合应用于大型网络。

为提高性能，防止产生路由环路，RIP 支持水平分割（Split Horizon）和毒性逆转（Poison Reverse）功能。

### RIP 的路由数据库

每个运行 RIP 的路由器管理一个路由数据库，该路由数据库包含了到所有可达目的地的路由项，这些路由项包含下列信息：

- 目的地址：主机或网络的地址。
- 下一跳地址：为到达目的地，需要经过的相邻路由器的接口 IP 地址。
- 出接口：本路由器转发报文的出接口。
- 度量值：本路由器到达目的地的开销。
- 路由时间：从路由项最后一次被更新到现在所经过的时间，路由项每次被更新时，路由时间重置为 0。
- 路由标记（Route Tag）：用于标识外部路由，在路由策略中可根据路由标记对路由信息进行灵活的控制。关于路由策略的详细信息，请参见“路由策略配置”。

### RIP 定时器

RIP 受四个定时器的控制，分别是 Update、Timeout、Suppress 和 Garbage-Collect。

- Update 定时器，定义了发送路由更新的时间间隔。
- Timeout 定时器，定义了路由老化时间。如果在老化时间内没有收到关于某条路由的更新报文，则该条路由在路由表中的度量值将会被设置为 16。
- Suppress 定时器，定义了 RIP 路由处于抑制状态的时长。当一条路由的度量值变为 16 时，该路由将进入抑制状态。在被抑制状态，只有来自同一邻居且度量值小于 16 的路由更新才会被路由器接收，取代不可达路由。

- **Garbage-Collect** 定时器，定义了一条路由从度量值变为 16 开始，直到它从路由表里被删除所经过的时间。在 **Garbage-Collect** 时间内，RIP 以 16 作为度量值向外发送这条路由的更新，如果 **Garbage-Collect** 超时，该路由仍没有得到更新，则该路由将从路由表中被彻底删除。

### 防止路由环路

RIP 是一种基于 D-V 算法的路由协议，由于它向邻居通告的是自己的路由表，存在发生路由环路的可能性。

RIP 通过以下机制来避免路由环路的产生：

- **计数到无穷(Counting to infinity)**: 将度量值等于 16 的路由定义为不可达(infinity)。在路由环路发生时，某条路由的度量值将会增加到 16，该路由被认为不可达。
- **水平分割(Split Horizon)**: RIP 从某个接口学到的路由，不会从该接口再发回给邻居路由器。这样不但减少了带宽消耗，还可以防止路由环路。
- **毒性逆转(Poison Reverse)**: 当一条路径信息变为无效之后，路由器并不立即将它从路由表中删除，而是用 16，即不可达的度量值将它广播出去。这样虽然增加了路由表的大小，但对消除路由循环很有帮助，它可以立即清除相邻路由器之间的任何环路。
- **触发更新(Triggered Updates)**: RIP 通过触发更新来避免在多个路由器之间形成路由环路的可能，而且可以加速网络的收敛速度。一旦某条路由的度量值发生了变化，就立刻向邻居路由器发布更新报文，而不是等到更新周期的到来。

#### 4.2.1.3 RIP 的启动和运行过程

RIP 启动和运行的整个过程可描述如下：

1. 路由器启动 RIP 后，便会向相邻的路由器发送请求报文 (Request message)，相邻的 RIP 路由器收到请求报文后，响应该请求，回送包含本地路由表信息的响应报 (Response message)。
2. 路由器收到响应报文后，更新本地路由表，同时向相邻路由器发送触发更新报文，通告路由更新信息。相邻路由器收到触发更新报文后，又向其各自的相邻路由器发送触发更新报文。在一连串的触发更新广播后，各路由器都能得到并保持最新的路由信息。
3. RIP 在缺省情况下每隔 30 秒向相邻路由器发送本地路由表，运行 RIP 协议的相邻路由器在收到报文后，对本地路由进行维护，选择一条最佳路由，再向其各自相

邻网络发送更新信息，使更新的路由最终能达到全局有效。同时，RIP 采用老化机制对超时的路由进行老化处理，以保证路由的实时性和有效性。

#### 4.2.1.4 RIP 的版本

RIP 有两个版本：RIP-1 和 RIP-2。

RIP-1 是有类别路由协议（Classful Routing Protocol），它只支持以广播方式发布协议报文。RIP-1 的协议报文无法携带掩码信息，它只能识别 A、B、C 类这样的自然网段的路由，因此 RIP-1 不支持不连续子网（Discontiguous Subnet）。

RIP-2 是一种无类别路由协议（Classless Routing Protocol），与 RIP-1 相比，它有以下优势：

- 支持路由标记，在路由策略中可根据路由标记对路由进行灵活的控制。
- 报文中携带掩码信息，支持路由聚合和 CIDR（Classless Inter-Domain Routing，无类域间路由）。
- 支持指定下一跳，在广播网上可以选择到最优下一跳地址。
- 支持组播路由发送更新报文，减少资源消耗。
- 支持对协议报文进行验证，并提供明文验证和 MD5 验证两种方式，增强安全性。

#### 4.2.1.5 RIP 的报文格式

##### RIP-1 的报文格式

RIP 报文由头部（Header）和多个路由表项（Route Entries）部分组成。在一个 RIP 报文中，最多可以有 25 个路由表项。

RIP-1 的报文格式如图 4-1 所示。

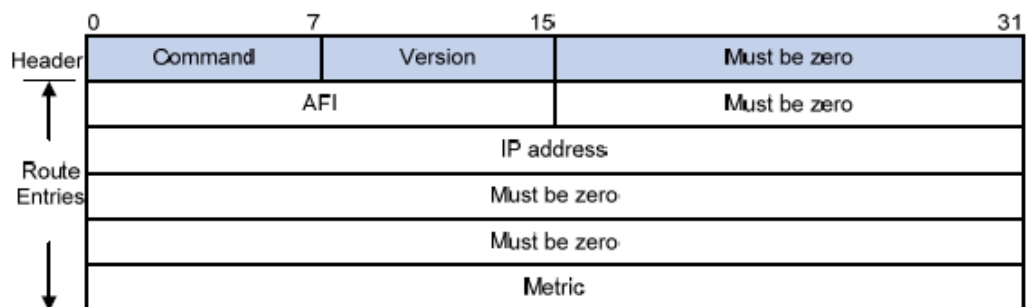


图 4-1 RIP-1 的报文格式

各字段的解释如下：

- **Command:** 标识报文的类型。值为 1 时表示 Request 报文, 值为 2 表示 Response 报文。
- **Version:** RIP 的版本号。对于 RIP-1 来说其值为 0x01。
- **AFI (Address Family Identifier):** 地址族标识, 其值为 2 时表示 IP 协议。
- **IP Address:** 该路由的目的 IP 地址, 可以是自然网段地址、子网地址或主机地址。
- **Metric:** 路由的度量值。

### RIP-2 的报文格式

RIP-2 的报文格式与 RIP-1 类似, 如图图 4-2所示。

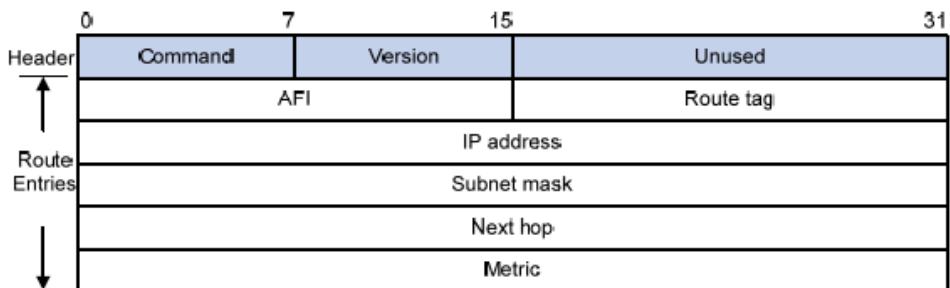


图 4-2 RIP-2 报文格式

其中, 与 RIP-1 不同的字段有：

- **Version:** RIP 的版本号。对于 RIP-2 来说其值为 0x02。
- **Route Tag:** 路由标记。
- **IP Address:** 该路由的目的 IP 地址, 可以是自然网段地址、子网地址或主机地址。
- **Subnet Mask:** 目的地址的掩码。
- **Next Hop:** 如果为 0.0.0.0, 则表示发布此条路由信息的路由器地址就是最优下一跳地址, 否则表示提供了一个比发布此条路由信息的路由器更优的下一条地址。

### RIP-2 的验证

RIP-2 为了支持报文验证, 使用第一个路由表项 (Route Entry) 作为验证项, 并将 AFI 字段的值设为 0xFFFF 标识报文携带认证信息, 如图图 4-3所示。

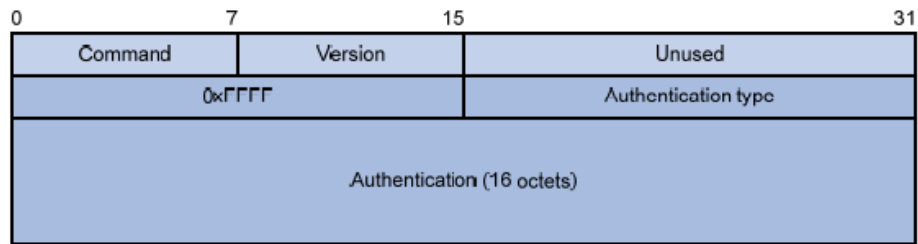


图 4-3 RIP-2 的验证报文格式

各字段的解释如下：

- **Authentication Type:** 验证类型。值为 2 时表示明文验证，值为 3 时表示 MD5 验证。
- **Authentication:** 验证字，当使用明文验证时包含了密码信息；当使用 MD5 验证时包含了 Key ID、MD5 验证数据长度和序列号的信息。

#### 4.2.1.6 支持的 RIP 特性

目前设备支持以下 RIP 特性：

- 支持 RIP-1 和 RIP-2
- 支持水平分割和毒性逆转
- 支持基于接口的简单认证和 MD5 认证方式
- 基于接口的对发送报文或接收报文版本的控制
- 支持对路由定时器时间的配置
- 支持对静态，直连，BGP，OSPF 路由的直连重分配

## 4.2.2 RIP 配置

### 4.2.2.1 基本配置

#### 4.2.2.1.1 使能与禁用 RIP 协议

##### 目的

本节介绍如何使能与禁用 RIP 协议。必须先启动 RIP，才能进入 RIP 协议配置模式，配置 RIP 协议的各种全局性的参数，需要注意的是关闭 RIP 后，原先配置的 RIP 参数也同时失效。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
使能 RIP 协议	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图； 2. 执行命令 <code>router rip</code>	-
去使能 RIP 协议	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图； 2. 执行命令 <code>no router rip</code>	-

4.2.2.1.2 添加或删除 RIP 接口

目的

本节介绍如何添加或删除 RIP 接口。可利用该命令将某个指定的网络接口上使能 rip 路由协议，在该网段上可以进行 RIP 路由表的相互转发,用 no 模式可以取消该配置，恢复缺省的配置，即不把接口配置到网段。

在一个路由器上的不同接口应该属于不同的网段，否则会出错。配置 RIP 接口的 network 命令中的参数所代表的网络必须是路由器上的有效网络，即路由器必须存在一个接口地址位于此网络中，如果不是，则此配置无效。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
添加指定的 RIP 接口	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图； 2. 执行命令 <code>router rip</code> ，进入 ROUTER RIP 配置视图 3. 执行命令 <code>network (A.B.C.D)</code>	(A.B.C.D)：使能 RIP 的网络地址，点分十进制；该地址必须与某一个 interface valn 下配置的 ip 地址完全匹配；
删除指定的 RIP 接口	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图； 2. 执行命令 <code>router rip</code> ，进入 ROUTER RIP 配置视图 3. 执行命令 <code>no network (A.B.C.D)</code>	(A.B.C.D)：使能 RIP 的网络地址，点分十进制；该地址必须与某一个 interface valn 下配置的 ip 地址完全匹配；

4.2.2.1.3 使能水平分割或毒性逆转

目的

本节介绍如何使能水平分割或毒性逆转。当前 RIP 协议启动时默认使能水平分割。当使能了水平分割时，毒性逆转功能就是关闭的。同样当使能了毒性逆转时，水平分割就是关闭的。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
使能水平分割 逆转	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图； 2. 执行命令 <code>router rip</code> ，进入 ROUTER RIP 配置视图。 3. 执行命令 <code>ip rip splithorizon enable</code> 。	-
使能毒性逆转	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图； 2. 执行命令 <code>router rip</code> ，进入 ROUTER RIP 配置视图。 3. 执行命令 <code>ip rip splithorizon disable</code> 。	-

#### 4.2.2.1.4 路由重分配配置

#### 目的

本节介绍如何路由重分配配置。在默认情况下，RIP 路由协议不发送非 RIP 类型的路由信息；如果能让 RIP 发送这些信息，就必须对 RIP 执行路由重分配。当前支持的路由重分配包括：直连路由重分配，静态路由重分配，OSPF 路由重分配，BGP 路由重分配。RIP 启动时默认重分配都是关闭的。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
直连重分配使 能或禁用	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图； 2. 执行命令 <code>router rip</code> ，进入 ROUTER RIP 配置视图 3. 执行命令 <code>redistribute connect</code> 或 <code>no redistribute connect</code>	-
静态重分配使 能或禁用	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图； 2. 执行命令 <code>router rip</code> ，进入 ROUTER RIP 配置视图 3. 执行命令 <code>redistribute static</code> 或 <code>no redistribute static</code>	-
OSPF 重分配 使能或禁用	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；	-

目的	步骤	参数说明
	2. 执行命令 <code>router rip</code> , 进入 ROUTER RIP 配置视图 3. 执行命令 <code>redistribute ospf</code> 或 <code>no redistribute ospf</code>	
BGP 重分配使能或禁用	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图; 2. 执行命令 <code>router rip</code> , 进入 ROUTER RIP 配置视图 3. 执行命令 <code>redistribute bgp</code> 或 <code>no redistribute bgp</code>	-

#### 4.2.2.1.5 定时器时间配置

##### 目的

本节介绍如何配置定时器时间。该命令配置 rip 路由的更新周期 `update`, 老化时间 `invalid`, 和垃圾回收时间 `garbage`。

注意: `invalid` 时间必须至少是 `update` 时间的 4 倍, `garbage` 必须至少是 `update` 时间的 8 倍, 并且 `garbage` 必须大于 `invalid`。`update` 的取值范围为 10~3600, 由于过小的 `update` 会增加网络负荷, 因此推荐 `update` 值不要小于 30。

##### 过程

根据不同目的, 执行相应步骤, 具体参见下表。

目的	步骤	参数说明
配置 rip 路由的更新, 老化和垃圾回收定时器	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图; 2. 执行命令 <code>router rip</code> , 进入 ROUTER RIP 配置视图 3. 执行命令 <code>ip rip timer basic (update) (invalid) (garbage)</code>	<code>update</code> : 路由更新时间。该参数定义了设备发送路由更新报文的周期。整数形式, 取值范围是 10~3600 秒 <code>invalid</code> : 路由超时时间。整数形式, 取值范围是 40~14400 秒 <code>garbage</code> : 从路由表中删除无效路由时间。整数形式, 取值范围是 80~28800 秒

#### 4.2.2.1.6 默认路由使能配置

##### 目的

本节介绍如何配置默认路由使能。该命令使能或禁用默认路由。缺省情况下是不支持默认路由的。



过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
使能默认路由	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>router rip</code>，进入 ROUTER RIP 配置视图</li> <li>3. 执行命令 <code>ip rip default-route enable</code></li> </ol>	-
禁用默认路由	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>router rip</code>，进入 ROUTER RIP 配置视图</li> <li>3. 执行命令 <code>ip rip default-route disable</code></li> </ol>	-

#### 4.2.2.2 RIP 接口配置

##### 4.2.2.2.1 RIP 收发包版本配置

目的

本节介绍如何配置 RIP 收发包版本。当前 RIP 接口可以配置 4 种发送 RIP 协议报文的方式，分别是不发送报文 `no-send`，报文以广播方式发送 `v1-compatible`，`v1` 和 `v2` 版本都可以发送 `v1v2`，报文以多播方式发送 `v2`。该命令行在 `vlan` 接口下进行配置，用来配置接口上 RIP 发送包的版本。当前 RIP 接口可以配置 4 种接收 RIP 协议报文的方式，分别是不接收报文 `no-receive`，只接收 `v1` 版本报文，`v1` 和 `v2` 版本都可以接收 `v1v2`，只接收 `v2` 版本报文。该命令行在 `vlan` 接口下进行配置，用来配置接口上 RIP 接收包的版本。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置发送报文的版本	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>interface vlan vlan-number</code>，进入 VLANIF 配置视图</li> <li>3. 执行命令 <code>ip rip send-version (no-send v1 v1-compatible  v2)</code></li> </ol>	<p><code>vlan-number</code>: VLAN ID，整数形式，取值范围是 1~4094；</p> <p><code>no-send</code>: 不发送 RIP 报文；</p> <p><code>v1-compatible</code>: 以广播的方式发送 RIPv2 版本报文；</p> <p><code>v1</code>: 发送 RIP-1 报文；</p> <p><code>v2</code>: 以组播的方式发送 RIPv2 版本的报文；</p>

目的	步骤	参数说明
配置接收报文的版本	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图;</li> <li>2. 执行命令 <code>interface vlan vlan-number</code>, 进入 VLANIF 配置视图</li> <li>3. 执行命令 <code>ip rip receive-version (no-receive v1 v1v2 v2)</code></li> </ol>	<p><code>vlan-number</code>: VLAN ID, 整数形式, 取值范围是 1~4094;</p> <p><code>no-receive</code>: 不接收 RIP 报文;</p> <p><code>v1</code>: 接收 RIP-1 报文;</p> <p><code>v2</code>: 接收 RIP-2 报文;</p> <p><code>v1v2</code>: 接收 RIP-1 和 RIP-2 报文</p>

#### 4.2.2.2.2 RIP 认证模式配置

##### 目的

本节介绍如何配置 RIP 认证模式。当前 RIP 接口可以配置 3 种认证模式, 分别是无认证, 简单认证, 和 MD5 认证。接口默认是无认证方式的。命令行在 `vlan` 接口下进行配置, 用来配置接口上 RIP 的认证方式。

注: RIPv1 版本不支持认证方式, 默认使能无认证。

##### 过程

根据不同目的, 执行相应步骤, 具体参见下表。

目的	步骤	参数说明
配置无认证方式	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图;</li> <li>2. 执行命令 <code>interface vlan vlan-number</code>, 进入 VLANIF 配置视图</li> <li>3. 执行命令 <code>no ip rip authentication</code></li> </ol>	<p><code>vlan-number</code>: VLAN ID, 整数形式, 取值范围是 1~4094;</p>
配置简单认证方式	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图;</li> <li>2. 执行命令 <code>interface vlan vlan-number</code>, 进入 VLANIF 配置视图</li> <li>3. 执行命令 <code>ip rip authentication text passw ord</code></li> </ol>	<p><code>vlan-number</code>: VLAN ID, 整数形式, 取值范围是 1~4094;</p> <p><code>passw ord</code>: 明文验证关键字, 字符串形式, 不支持空格, 区分大小写, 长度范围是: 1-16 个字符长度;</p>
使能 MD5 认证模式	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图;</li> <li>2. 执行命令 <code>interface vlan vlan-number</code>, 进入 VLANIF 配置视图</li> <li>3. 执行命令 <code>ip rip authentication md5 &lt;1-255&gt; KEY</code></li> </ol>	<p><code>&lt;1-255&gt;</code>: MD5 密文验证标识符, 整数形式, 取值范围是 1~255;</p> <p><code>KEY</code>: 密文验证关键字, 字符串形式, 不支持空格, 区分大小写, 长度范围是 1-16 个字符长度;</p>

#### 4.2.2.2.3 RIP 缺省路由开销配置

##### 目的

本节介绍如何配置 RIP 缺省路由开销。该命令用来配置 RIP 缺省的路由开销，有效值为 0~15；用 no 形式来恢复到缺省的配置。其初始默认值为 0。该命令行在 vlan 接口下进行配置。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置缺省的路由开销	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>interface vlan vlan-number</code>，进入 VLANIF 配置视图</li> <li>3. 执行命令 <code>ip rip default-metric (&lt;0-15&gt; default)</code></li> </ol>	<p><b>vlan-number:</b> VLAN ID，整数形式，取值范围是 1~4094；</p> <p><b>&lt;0-15&gt;:</b> 配置的缺省路由费用，整数形式，取值范围是 0~15，当配置为 0 时表示接口不发送默认路由；</p> <p><b>default:</b> RIP 接口默认路由度量值，为 0，表示接口不发送默认路由；</p>

#### 4.2.2.2.4 RIP 使能与禁用静默接口

### 目的

本节介绍如何配置 RIP 使能与禁用静默接口。该命令用来使能与禁用 RIP 接口的静默功能，使能接口的静默功能时该接口只接收 RIP 报文，不发送 RIP 报文。默认是禁用 RIP 接口的静默方式。该命令行在 vlan 接口下进行配置。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
使能和去使能接口的静默方式	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>interface vlan vlan-number</code>，进入 VLANIF 配置视图</li> <li>3. 执行命令 <code>ip rip passive-interface</code> 或 <code>no ip rip passive-interface</code></li> </ol>	<p><b>vlan-number:</b> VLAN ID，整数形式，取值范围是 1~4094；</p>

#### 4.2.2.3 查看 RIP 信息

##### 4.2.2.3.1 查看 RIP 配置

### 目的

该命令在全局模式下，可以查看到与 RIP 配置相关的所有信息。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
查看 RIP 的配置信息	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图； 2. 执行命令 <code>show ip rip configuration</code>	-

#### 4.2.2.3.2 查看 RIP 接口配置

##### 目的

该命令在全局模式下，可以查看到所有 RIP 接口配置相关的信息。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
查看 RIP 接口的配置信息	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图； 2. 执行命令 <code>show ip rip interface</code>	-

#### 4.2.2.3.3 查看 RIP 路由表

##### 目的

该命令在全局模式下，可以查看到 RIP 路由表的路由条目信息。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
查看 RIP 路由表信息	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图； 2. 执行命令 <code>show ip rip database</code>	-

#### 4.2.2.3.4 查看 RIP 全局参数

##### 目的

该命令在全局模式下，可以查看到 RIP 模块支持的最大路由数目，已分配路由数目，支持的最大接口数目，已分配的接口数目，支持的最大对等体数目，已分配的对等体数目，重分配标志，水平分割与毒性逆转标志，定时器时间。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
查看 RIP 相关全局参数	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>show ip rip resource</code></li> </ol>	-

#### 4.2.2.3.5 RIP 调试信息

### 目的

本节介绍如何显示 RIP 协议的调试信息。该命令在全局模式下，可以查看到 RIP 模块支持的最大路由数目，已分配路由数目，支持的最大接口数目，已分配的接口数目，支持的最大对等体数目，已分配的对等体数目，重分配标志，水平分割与毒性逆转标志，定时器时间。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
使能 RIP 调试信息开关	<ol style="list-style-type: none"> <li>1. 保持特权用户视图；</li> <li>2. 执行命令 <code>debug rip { pkt-in   pkt-out   rx   tx   config   sync-rx   sync-tx   sync-detail   socket-msg   socket-msg-detail   rt-trace   all }</code></li> </ol>	-
禁用 RIP 调试信息开关	<ol style="list-style-type: none"> <li>1. 保持在特权用户视图；</li> <li>2. 执行命令 <code>no debug rip { pkt-in   pkt-out   rx   tx   config   sync-rx   sync-tx   sync-detail   socket-msg   socket-msg-detail   rt-trace   all }</code></li> </ol>	

#### 4.2.3 配置举例

### 组网图 1

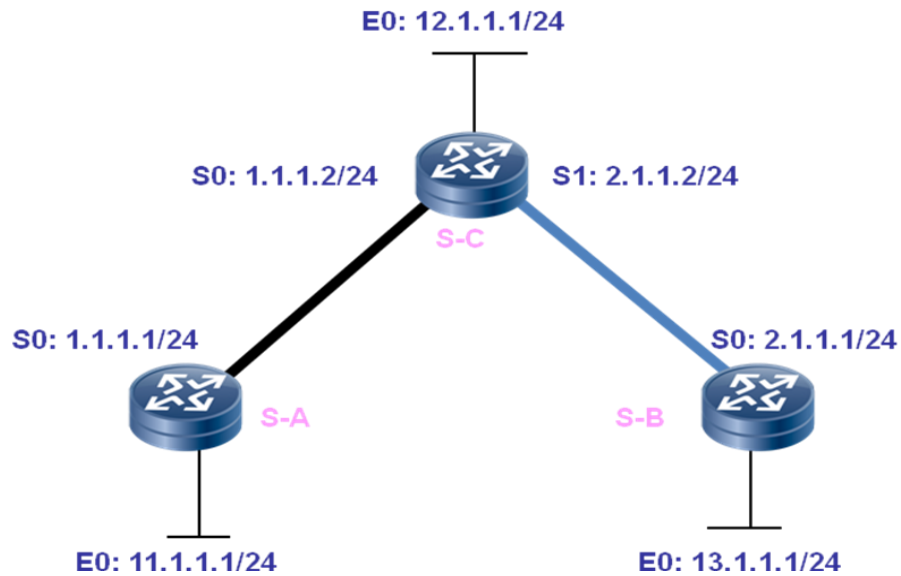


图 4-4 配置 RIP 拓扑结构

### 配置步骤 1

#### 1、S-A 配置:

```
SC9600#configure
SC9600(config)#route rip
SC9600(config-route-rip)#network 1.1.1.1
SC9600(config-route-rip)#network 11.1.1.1
```

#### 2、S-B 配置:

```
SC9600#configure
SC9600(config)#route rip
SC9600(config-route-rip)#network 13.1.1.1
SC9600(config-route-rip)#network 2.1.1.1
```

#### 3、S-C 配置:

```
SC9600#configure
SC9600(config)#route rip
SC9600(config-route-rip)#network 1.1.1.2
SC9600(config-route-rip)#network 12.1.1.1
SC9600(config-route-rip)#network 2.1.1.2
```

4、查看 RIP 配置信息

```
SC9600#show ip rip configuration
```

```
ip rip splithorizen disable
```

```
no redistribute static
```

```
no redistribute ospf
```

```
no redistribute connect
```

```
no redistribute bgp
```

```
network 1.1.1.2
```

```
network 3.3.3.4
```

```
interface vlan 1
```

```
ip rip send-version v1
```

```
ip rip receive-version v1
```

```
interface vlan 2
```

```
ip rip send-version v1-compatible
```

5、查看 RIP 接口信息

```
SC9600#show ip rip interface
```

```
Interface          :vlan 1
```

```
Interface status   :Down
```

```
Interface passive mode :False
```

```
Interface adress    :1.1.1.2
```

```
Interface netmask    :255.255.255.0
```

```
Authctication Type  :no authctication
```

```
Send Version        :rip version 1
```

```
Receive Version     :rip version 2
```

```
Interface defaulte metric :0
```

```

Interface          :vlan 2
Interface status   :Down
Interface passive mode :False
Interface adress    :3.3.3.4
Interface netmask   :255.255.255.0
Authctication Type :no authctication
Send Version        :rip version 2
Receive Version     :rip version 2
Interface defaulte metric :0
    
```

#### 6、查看 RIP 路由表

```
SC9600#show ip rip database
```

```
entry count = 2
```

destination	netmask	gateway	metric	age	state	proto
1.1.1.0	255.255.255.0	1.1.1.2	0	0	DOWN	rip
3.3.3.0	255.255.255.0	3.3.3.4	0	0	DOWN	rip

**组网图 2**



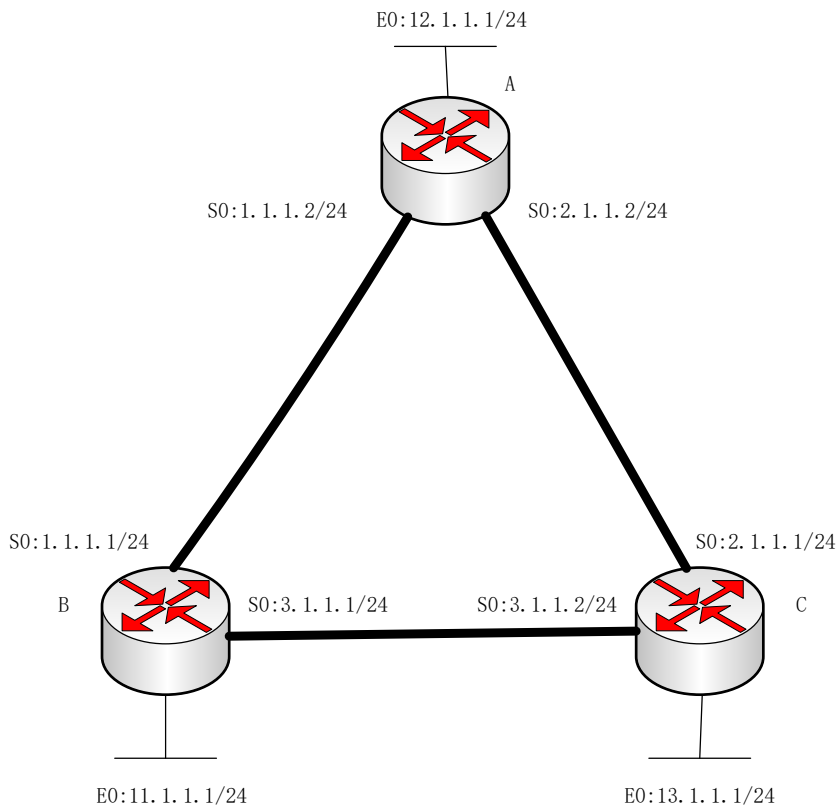


图 4-5 带有环状配置的 RIP 拓扑结构

### 配置步骤 2

在 A 中配置静态路由 192.168.2.1，掩码为 255.255.255.0，下一跳为 12.1.1.2，将其重分配到 rip 路由表中。

在 B 中配置静态路由 192.168.1.1，掩码为 255.255.255.0，下一跳为 11.1.1.2，将其重分配到 rip 路由表中。

在 C 中配置静态路由 192.168.3.1，掩码为 255.255.255.0，下一跳为 13.1.1.2，将其重分配到 rip 路由表中。

此时 C 路由器的路由表为：

destination	netmask	gateway	metric	age	state	proto
192.168.1.0	255.255.255.0	3.1.1.1	2	4	ACTIVE	rip
192.168.2.0	255.255.255.0	2.1.1.2	2	29	ACTIVE	rip
2.1.1.0	255.255.255.0	2.1.1.1	1	0	ACTIVE	rip

```
192.168.3.0      255.255.255.0    13.1.1.2        1      0      ACTIVE
netmgmt
```

```
3.1.1.0        255.255.255.0    3.1.1.2         1      0      ACTIVE rip
```

打开调试开关，首先观察路由器 C 的发出报文，在水平分割被打开的情况下发出报文：

```
2100/11/13 17:08:17 RIP:send packet to 224.0.0.9,port 520,length 44,source 3.1.1.2
```

Packet Parse:

```
Version: 2,Command:2
```

```
Route#0: Afi 2,Tag 0000
```

```
Dest:192.168.2.0,Mask:255.255.255.0 Nhop:3.1.1.2,Metric:2
```

```
Route#1: Afi 2,Tag 0000
```

```
Dest:192.168.3.0,Mask:255.255.255.0 Nhop:3.1.1.2,Metric:1
```

```
2100/11/13 17:08:47 RIP:send packet to 224.0.0.9,port 520,length 44,source 2.1.1.1
```

Packet Parse:

```
Version: 2,Command:2
```

```
Route#0: Afi 2,Tag 0000
```

```
Dest:192.168.1.0,Mask:255.255.255.0 Nhop:2.1.1.1,Metric:2
```

```
Route#1: Afi 2,Tag 0000
```

```
Dest:192.168.3.0,Mask:255.255.255.0 Nhop:2.1.1.1,Metric:1
```

然后打开毒性逆转开关，观察 C 路由器发出的报文

```
2100/11/13 17:14:47 RIP:send packet to 224.0.0.9,port 520,length 64,source 3.1.1.2
```

Packet Parse:

```
Version: 2,Command:2
```

```
Route#0: Afi 2,Tag 0000
```

```
Dest:192.168.1.0,Mask:255.255.255.0 Nhop:3.1.1.1,Metric:16
```

```
Route#1: Afi 2,Tag 0000
```

```
Dest:192.168.2.0,Mask:255.255.255.0 Nhop:3.1.1.2,Metric:2

Route#2: Afi 2,Tag 0000

Dest:192.168.3.0,Mask:255.255.255.0 Nhop:3.1.1.2,Metric:1

2100/11/13 17:14:47 RIP:send packet to 224.0.0.9,port 520,length 64,source 2.1.1.1

Packet Parse:

Version: 2,Command:2

Route#0: Afi 2,Tag 0000

Dest:192.168.1.0,Mask:255.255.255.0 Nhop:2.1.1.1,Metric:2

Route#1: Afi 2,Tag 0000

Dest:192.168.2.0,Mask:255.255.255.0 Nhop:2.1.1.2,Metric:16

Route#2: Afi 2,Tag 0000

Dest:192.168.3.0,Mask:255.255.255.0 Nhop:2.1.1.1,Metric:1
```

通过对比可以观察到,在水平分割的情况下,路由器 C 不将从某个接口学习到路由条目,再从这个接口发送回去。而在毒性逆转的情况下,路由器 C 将把从这个接口学习到的路由条目发送回去,但是将度量字段置为 16,用来表示不可达。

## 4.3 RIPng 配置

### 4.3.1 RIPng 概述

#### RIPng 简介

RIPng 是在 IPv6 网络中应用的 RIP 协议,并在原 RIP 协议基础上进行了一些扩展,用于自治域内少量路由的学习和发布。虽然支持 IPv6 的 RIPng 协议是基于 RIPv2 协议的,但是它并不是 RIPv2 的简单扩展,它实际上是一个完全独立的协议。



说明:

RIPng 协议不支持 IPv4,如果用户需要同时在 IPv4 和 IPv6 环境里使用 RIP 作为路由选择协议,就必须运行支持 IPv4 的 RIPv1 或 RIPv2,以及支持 IPv6 的 RIPng。

RIPng 当前只有一个版本是 RIPngv1。

### RIPng 与 RIPv1 和 RIPv2 的比较

RIPng 是对 RIP 进行必要的改造以使其适应 IPv6 下的选路要求，因此 RIPng 的基本工作原理同 RIP 是一样的，其主要的变化在地址和报文格式方面。下面列举了一些 RIPv1、RIPv2 与 RIPng 之间的主要区别：

- 地址版本。

RIPv1、RIPv2 是基于 IPv4 的，地址域只有 32bit，而 RIPng 基于 IPv6，使用的所有地址均为 128bit。RIPng 使用的 IPv6 多播地址是 FF02::9。

- 子网掩码和前缀长度。

RIPv1 被设计成用于无子网的网络，因此没有子网掩码的概念，这就决定了 RIPv1 不能用于传播变长的子网地址或用于 CIDR 的无类型地址。RIPv2 增加了对子网选路的支持，因此使用子网掩码区分网络路由和子网路由。IPv6 的地址前缀有明确的含义，因此 RIPng 中不再有子网掩码的概念，取而代之的是前缀长度。同样也是由于使用了 IPv6 地址，RIPng 中也没有必要再区分网络路由、子网路由和主机路由。

- 协议的使用范围。

RIPv1、RIPv2 的使用范围被设计成不只局限于 TCP/IP 协议簇，还能适应其他网络协议簇的规定，因此报文的的路由表项中包含有网络协议簇字段，但实际的实现程序很少被用于其他非 IP 的网络，因此 RIPng 中去掉了对这一功能的支持。

- 对下一跳的表示。

RIPv1 中没有下一跳的信息，接收端路由器把报文的源 IP 地址作为到目的网络路由的下一跳。RIPv2 中明确包含了下一跳信息，便于选择最优路由和防止出现选路环路及慢收敛。与 RIPv2 不同，为防止 RTE 过长，同时也是为了提高路由信息的传输效率，RIPng 中的下一跳字段是作为一个单独的路由信息存在的。

- 报文长度。

RIPv1、RIPv2 中对报文的长度均有限制，规定每个报文最多只能携带 25 个 RTE。而 RIPng 对报文长度、RTE 的数目都不作规定，报文的长度是由传输介质的 MTU 决定的。RIPng 对报文长度的处理，提高了网络对路由信息的传输效率。

- 安全性考虑。

RIPv1 报文中并不包含验证信息，因此也是不安全的，任何通过 UDP 的 520 端口发送分组的主机，都会被邻机当作一个路由器，从而很容易造成路由器欺骗。RIPv2 设计了验证报文来增强安全性，进行路由交换的路由器之间必须通过验证才能接收彼此的路由信息，但是 RIPv2 的安全性还是很不充分的。IPv6 包含有很好的安全性策略，因此 RIPng 中不再单独设计安全性验证报文，而是使用 IPv6 的安全性策略。

- 报文的发送方式。

RIPv1 使用广播来发送路由信息，不仅路由器会接收到分组，同一局域网内的所有主机也会接收到分组，这样做是不必要的，也是不安全的。因此 RIPv2 和 RIPng 既可以使用广播也可以使用多播发送报文，这样在支持多播的网络中就可以使用多播来发送报文，大大降低了网络中传播的路由信息的数量。

#### 4.3.1.1 RIPng 工作机制

##### RIPng 的基本概念

RIPng 是一种基于距离矢量（Distance-Vector, D-V）算法的协议，它通过 UDP 报文进行路由信息的交换，默认使用端口号为 521。与 RIPv1 和 RIPv2 不同之处是它没有设定消息的大小。在这里，消息的大小仅仅依赖于发送它的链路的 MTU 值。

RIPng 使用跳数来衡量到达目的地址的距离。在 RIPng 中，路由器到与它直接相连网络的跳数为 0，通过一个路由器可达的网络的跳数为 1，其余依此类推。为限制收敛时间，规定度量值取 0~15 之间的整数，大于或等于 16 的跳数被定义为无穷大，即目的网络或主机不可达。由于这个限制，使得 RIPng 不适合应用于大型网络。

为提高性能，防止产生路由环路，RIPng 支持水平分割（Split Horizon）和毒性逆转（Poison Reverse）功能。

##### RIPng 的路由数据库

每个运行 RIPng 的路由器管理一个路由数据库，该路由数据库包含了到所有可达目的地的路由项，这些路由项包含下列信息：

- 目的地址：主机或网络的地址。
- 下一跳地址：为到达目的地，需要经过的相邻路由器的接口 IP 地址。
- 出接口：本路由器转发报文的出接口。
- 度量值：本路由器到达目的地的开销。

- **路由时间**：从路由项最后一次被更新到现在所经过的时间，路由项每次被更新时，路由时间重置为 0。
- **路由标记 (Route Tag)**：用于标识外部路由，在路由策略中可根据路由标记对路由信息进行灵活的控制。

### RIPng 定时器

RIPng 受四个定时器的控制，分别是 Update、Timeout、Suppress 和 Garbage-Collect。

- **Update 定时器**，定义了发送路由更新的时间间隔。
- **Timeout 定时器**，定义了路由老化时间。如果在老化时间内没有收到关于某条路由的更新报文，则该条路由在路由表中的度量值将会被设置为 16。
- **Suppress 定时器**，定义了 RIP 路由处于抑制状态的时长。当一条路由的度量值变为 16 时，该路由将进入抑制状态。在被抑制状态，只有来自同一邻居且度量值小于 16 的路由更新才会被路由器接收，取代不可达路由。
- **Garbage-Collect 定时器**，定义了一条路由从度量值变为 16 开始，直到它从路由表里被删除所经过的时间。在 Garbage-Collect 时间内，RIPng 以 16 作为度量值向外发送这条路由的更新，如果 Garbage-Collect 超时，该路由仍没有得到更新，则该路由将从路由表中被彻底删除。

### 防止路由环路

由于 RIPng 也是一种基于距离向量算法的路由协议，它向邻居通告的是自己的路由表，存在发生路由环路的可能性。

它通过以下机制来避免路由环路的产生：

- **计数到无穷 (Counting to infinity)**：将度量值等于 16 的路由定义为不可达 (infinity)。在路由环路发生时，某条路由的度量值将会增加到 16，该路由被认为不可达。
- **水平分割 (Split Horizon)**：RIPng 从某个接口学到的路由，不会从该接口再发回给邻居路由器。这样不但减少了带宽消耗，还可以防止路由环路。
- **毒性逆转 (Poison Reverse)**：RIPng 从某个接口学到路由后，将该路由的度量值设置为 16 (不可达)，并从原接口发回邻居路由器。利用这种方式，可以清除对方路由表中的无用信息。
- **触发更新 (Triggered Updates)**：RIPng 通过触发更新来避免在多个路由器之间形成路由环路的可能，而且可以加速网络的收敛速度。一旦某条路由的度量值发生了变化，就立刻向邻居路由器发布更新报文，而不是等到更新周期的到来。

### 4.3.1.2 RIPng 的启动和运行过程

RIPng 启动和运行的整个过程可描述如下：

- 路由器启动 RIPng 后，便会向相邻的路由器发送请求报文（Request message），相邻的路由器收到请求报文后，响应该请求，回送包含本地路由表信息的响应报（Response message）。
- 路由器收到响应报文后，更新本地路由表，同时向相邻路由器发送触发更新报文，通告路由更新信息。相邻路由器收到触发更新报文后，又向其各自的相邻路由器发送触发更新报文。在一连串触发更新广播后，各路由器都能得到并保持最新的路由信息。
- RIPng 在缺省情况下每隔 30 秒向相邻路由器发送本地路由表，运行 RIPng 协议的相邻路由器在收到报文后，对本地路由进行维护，选择一条最佳路由，再向其各自相邻网络发送更新信息，使更新的路由最终能达到全局有效。同时，RIPng 采用老化机制对超时的路由进行老化处理，以保证路由的实时性和有效性。

### 4.3.1.3 RIPng 的报文格式

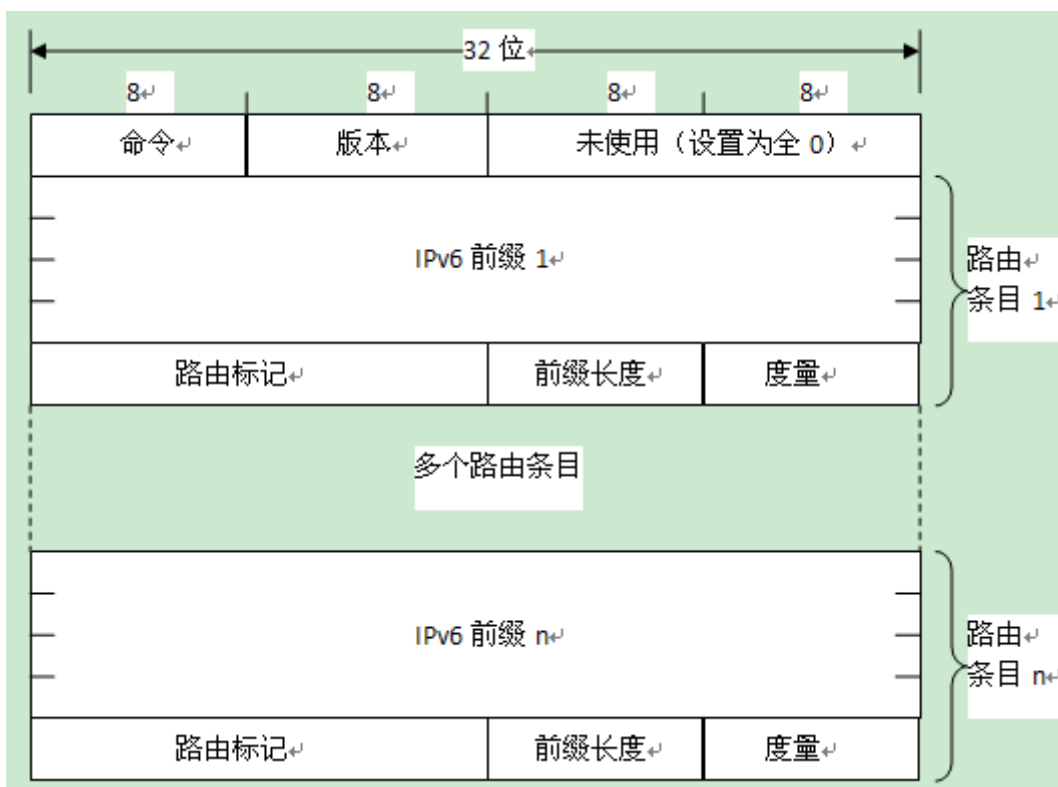


图 4-6 RIPng 报文格式

RIPng 是基于 UDP 的协议，并且使用端口号 521 发送和接收数据报。RIPng 报文大致可分为两类：选路信息报文和用于请求信息的报文。它们都使用相同的格式，由固定的首部和路由表项 RTE（Route Table Entry）组成，其中路由表项可以有多个。

- 首部包括命令字段和版本号字段。

同 RIP 一样，命令字段用来区分报文要实现的各种操作。其中命令号 1 表示请求部分或全部选路信息，命令号 2 表示响应，其中包含一个或多个 RTE。路由器可以通过发送请求命令向另一个路由器请求选路信息。路由器使用响应命令回答。版本号字段包含了协议的版本号（目前的版本号值为 1），接收方会检测该字段，以确定对方运行的 RIPng 协议本地是否能进行正确的解释。

- 报文的剩余部分是一个 RTE 序列，其中每一个 RTE 由目的 IPv6 前缀、路由标记、前缀的有效长度以及到目的网络的花费等 4 部分组成。IPv6 的地址为 128bit，因此在 RTE 中占用 16 字节。
- 路由标记字段是从 RIP 中保留下来的，其最主要的用途是用来对外部路由做标志，以区分内部路由和外部路由，供外部网关路由协议（如 EGP 或 BGP）使用。该字段也可用于其他目的，只要网络内所有运行 RIPng 的路由器对其解释是一致的。
- 前缀长度字段指明了前缀中有效位的长度，IPv6 中使用了前缀长度的概念代替了 IPv4 中的子网掩码。由于 IPv6 地址的意义很明确，因此 RIPng 中不再区分网络路由、子网路由或主机路由。
- 路由花费字段指明到目的网络的花费，由于 RIPng 的最大工作直径为 15 跳，因此该字段可以为 1 和 15 之间的任意值，16 即意味着目的地不可达。RIPng 中仍然使用固定的度量方式，即该字段的含义只能是跳数，路由器不能对其进行其他的解释。
- RIPng 的下一跳字段。

与 RIPv2 不同的是，RIPng 的下一跳字段是由一个单独的路由表项 RTE 指定的。RIPng 使用单独的路由表项 RTE 表示下一跳的原因是 IPv6 的地址多达 128bit，若将下一跳字段与目的网络地址放在同一个 RTE 中，则 RTE 的大小几乎将会增加一倍，因此 RIPng 中采取目的网络地址和下一跳分开的方法来减小 RTE 的长度。在表示下一跳的 RTE 中，路由标记和前缀长度字段必须为零，而度量字段为 0xFF。

RIPng 并没有限制报文的大小，RIPng 报文所能携带的最大 RTE 的数目是由物理介质的 MTU 所决定的。





说明：

计算公式：报文长度 = RTE 数目 × 20 + 4。其中，RTE 数目 = INT[(MTU - IPv6 首部长度 - UDP 首部长度 - RIPng 首部长度) / RTE 长度]

### 4.3.2 支持的 RIPng 特性

目前设备支持以下 RIPng 特性：

- 支持水平分割和毒性逆转
- 支持对路由定时器时间的配置
- 支持对静态、直连、BGP 和 OSPF 路由的直连重分配
- 支持对主机路由的学习
- 支持默认路由的使能

### 4.3.3 配置 RIPng 基本功能

#### 目的

用户可以执行本节操作配置 RIPng 基本功能，主要包括创建 RIPng 进程和在接口下使能 RIPng，是能够使用 RIP 特性的前提。

#### 前提配置

在配置 RIPng 基本功能之前，需完成以下任务：

- 保证接口的链路状态为 Up。
- 使能交换机的 IPv6 能力。
- 配置接口的网络层地址，使相邻节点的网络层可达。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
进入 RIPNG 或者 RIPNG VPN 配置节点	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>router ripng</b> 或 <b>router ripng rip-process</b> 或 <b>router ripng vpn-instance NAME</b> 或 <b>router ripng rip-process vpn-instance NAME</b> 从全局配置视图进入 RIPNG 或者 RIPNG VPN 配置节点；</li> <li>3. 结束。</li> </ol>

目的	步骤
删除 RIPNG 实例	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>no router ripng [rip-process]</b> 删除 RIPNG 实例;</li> <li>3. 结束。</li> </ol>
使能或去使能端口的 RIPng 功能	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>interface vlan vlan-id</b> 进入 VLANIF 配置视图;</li> <li>3. 执行命令 <b>ipv6 ripng rip-process { enable   disable }</b> 使能或去使能端口的 RIPng 功能;</li> <li>4. 结束。</li> </ol>
(可选) 配置重分配路由	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>router ripng</b> 进入 RIPNG 配置视图;</li> <li>3. 执行命令 <b>redistribute { static   ospf   connect   bgp   isis }</b> 或 <b>no redistribute { static   ospf   connect   bgp   isis }</b>;</li> <li>4. 结束。</li> </ol>
(可选) 配置引入路由默认开销值	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>router ripng</b> 进入 RIPNG 配置视图;</li> <li>3. 执行命令 <b>redistribute { static   ospf   connect   bgp   isis } cost cost-value;</b></li> <li>4. 结束。</li> </ol>
(可选) 配置重分配满足路由策略的路由	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>router ripng</b> 进入 RIPNG 配置视图;</li> <li>3. 执行命令 <b>redistribute { static   ospf   connect   bgp   isis } route-policy policy-name</b> 或 <b>no redistribute { static   ospf   connect   bgp   isis } route-policy;</b></li> <li>4. 结束。</li> </ol>
(可选) 配置使能支持默认路由	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>router ripng</b> 进入 RIPNG 配置视图;</li> <li>3. 执行命令 <b>default-route { enable   disable };</b></li> <li>4. 结束。</li> </ol>
(可选) 配置使能或者去使能 VLAN 所在接口 RIPng 接口为静默模式	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>interface vlan vlan-id</b> 进入 VLANIF 配置视图;</li> <li>3. 执行命令 <b>ipv6 ripng rip-process passive-interface { enable   disable };</b></li> <li>4. 结束。</li> </ol>
(可选) 配置发送或接收的路由信息报文度量偏移值	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>interface vlan vlan-id</b> 进入 VLANIF 配置视图;</li> <li>3. 执行命令 <b>ipv6 ripng rip-process metric-in { metric-in-number   default }</b> 或 <b>ipv6 ripng metric-out { metric-in-number   default }</b> 或 <b>ipv6 ripng rip-process metric-out { metric-in-number   default };</b></li> <li>4. 结束。</li> </ol>

目的	步骤
(可选) 配置接口 RIPng 使能或者去使能 bfd 功能	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>interface vlan vlan-id</b> 进入 VLANIF 配置视图;</li> <li>3. 执行命令 <b>ipv6 ripng rip-process bfd { enable   disable }</b>;</li> <li>4. 结束。</li> </ol>

附表:

参数	说明	取值
static	静态路由重分配	<b>redistribute static</b> 表示使能静态路由重分配 <b>no redistribute static</b> 表示禁止将静态路由条目导入到 RIP 路由数据库中, 已经导入的静态路由则必须老化进入垃圾回收定时器时间
ospf	OSPF 路由重分配	<b>redistribute ospf</b> 表示使能 ospf 路由重分配 <b>no redistribute ospf</b> 表示禁止 ospf 路由条目导入到 RIP 路由数据库中, 已经导入的静态路由则必须老化进入垃圾回收定时器时间
connect	直连路由重分配	<b>redistribute connect</b> 表示使能将直连路由条目导入到 RIP 路由数据库中 <b>no redistribute connect</b> 表示禁止将直连的路由条目导入到 RIP 路由数据库中, 已经导入的直连路由则必须老化进入垃圾回收定时器时间。
bgp	BGP 路由重分配	<b>redistribute bgp</b> 表示使能将 BGP 学习到的路由条目导入到 RIP 路由数据库中 <b>no redistribute bgp</b> 表示禁止将 BGP 的路由条目导入到 RIP 路由数据库中, 已经导入的 BGP 路由则必须老化进入垃圾回收定时器时间
isis	ISIS 路由重分配	<b>redistribute isis</b> 表示使能将 ISIS 学习到的路由条目导入到 RIP 路由数据库中 <b>no redistribute isis</b> 表示禁止将 ISIS 的路由条目导入到 RIP 路由数据库中, 已经导入的 BGP 路由则必须老化进入垃圾回收定时器时间
policy-name	路由策略的名字, 必须事先配置	字符串, 必须唯一, 不超过 20 个字节
cost-value	路由开销	整数取值, 取值范围是 1-15
enable	使能接口静默模式	-
disable	去使能接口静默模式	-
rip-process	RIPNG 进程号	整数取值, 取值范围是 1-2047
metric-in-number	对接收报文中路由条目度量值的偏移	整数形式, 取值范围是 0-15
metric-out-number	对发送报文中路由条目度量值的偏移	整数形式, 取值范围是 0-15

### 4.3.4 配置 RIPng 路由信息的发布与接收

#### 目的

用户可以执行本节操作配置 RIPng 基本功能，主要包括创建 RIPng 进程和在接口下使能 RIPng，是能够使用 RIP 特性的前提。

#### 前提配置

在配置 RIPng 基本功能之前，需完成以下任务：

- 保证接口的链路状态为 Up。
- 使能交换机的 IPv6 能力。
- 配置接口的网络层地址，使相邻节点的网络层可达。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置生成一条缺省路由到 RIPng 路由域中	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface vlan <i>vlan-id</i></b> 进入 VLANIF 配置视图；</li> <li>3. 执行命令 <b>ipv6 ripng <i>rip-process</i> default-route { only   originate } 或 <b>ipv6 ripng <i>rip-process</i> default-route { only   originate } cost <i>cost-value</i>;</b></b></li> <li>4. 结束。</li> </ol>
引入的路由设置 RIPng 权值	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>router ripng</b> 或 <b>router ripng <i>rip-process</i></b> 或 <b>router ripng vpn-instance <i>NAME</i></b> 或 <b>router ripng <i>rip-process</i> vpn-instance <i>NAME</i></b> 从全局配置视图进入 RIPNG 或者 RIPNG VPN 配置节点；</li> <li>3. 执行命令 <b>default-cost { <i>cost-value</i>   default }</b></li> <li>4. 结束。</li> </ol>
配置路由协议的出口过滤策略，只有通过过滤的路由才能被加入更新报文中发布出去	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>router ripng</b> 或 <b>router ripng <i>rip-process</i></b> 或 <b>router ripng vpn-instance <i>NAME</i></b> 或 <b>router ripng <i>rip-process</i> vpn-instance <i>NAME</i></b> 从全局配置视图进入 RIPNG 或者 RIPNG VPN 配置节点；</li> <li>3. 执行命令 <b>filter-policy export { static   ospf   connect   bgp   isis } route-policy <i>name</i></b> 或 <b>no filter-policy export { static   ospf   connect   bgp   isis } route-policy;</b></li> <li>4. 结束。</li> </ol>
配置实例接收或者发送路由过滤策略	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>router ripng</b> 或 <b>router ripng <i>rip-process</i></b> 或 <b>router ripng vpn-instance <i>NAME</i></b> 或 <b>router ripng <i>rip-process</i> vpn-instance <i>NAME</i></b> 从全局配置视图进入 RIPNG 或者 RIPNG VPN 配置节点；</li> </ol>

目的	步骤
	3. 执行命令 <b>filter-policy { export   import } route-policy name</b> 或 <b>no filter-policy { export   import } route-policy;</b> 4. 结束。
配置接口接收和发送路由的过滤策略	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>interface vlan vlan-id</b> 进入 VLANIF 配置视图; 3. 执行命令 <b>ipv6 ripng rip-process filter-policy { export   import } route-policy name</b> 或 <b>no ipv6 ripng rip-process filter-policy { export   import } route-policy;</b> 4. 结束。

附表:

参数	说明	取值
only	使能支持默认路由	-
originate	去使能支持默认路由	-
cost-value	缺省路由的开销	不配置 cost, 默认值为 1
cost-value	引入路由的缺省权值	整数取值, 取值范围是 0-15
Name	VPN 实例名, 输入的 VPN 名必须是真实存在的	字符串, 最大长度为 30
rip-process	RIP 多实例号	整数形式, 取值范围是 1-2047
vlan-id	vlan 接口号	整数取值, 取值范围是 1-4094
static	配置静态路由出口过滤策略	对 RIP 中引入的静态路由在被加入到更新报文中发布出去前, 可以使用该命令进行过滤。通过 NAME 指定的路由策略名称, 对静态路由进行过滤, 只有通过过滤条件的静态路由才能被加入到更新报文中发布出去。 基于协议对路由进行过滤, 则可以配置多个路由策略, 不会覆盖前面配置的路由策略。
ospf	配置引入 ospf 路由的路由策略	对 RIP 中引入的 OSPF 路由在被加入到更新报文中发布出去前, 可以使用该命令进行过滤。通过 NAME 指定的路由策略名称, 对 OSPF 路由进行过滤, 只有通过过滤条件的 OSPF 路由才能被加入到更新报文中发布出去。 基于协议对路由进行过滤, 则可以配置多个路由策略, 不会覆盖前面配置的路由策略。
connect	配置引入直连路由的路由策略	对 RIP 中引入的直连路由在被加入到更新报文中发布出去前, 可以使用该

参数	说明	取值
		命令进行过滤。通过 NAME 指定的路由策略名称，对直连路由进行过滤，只有通过过滤条件的直连路由才能被加入更新报文中发布出去。 基于协议对路由进行过滤，则可以配置多个路由策略，不会覆盖前面配置的路由策略
bgp	配置引入 BGP 路由的路由策略	对 RIP 中引入的 BGP 路由在被加入到更新报文中发布出去前，可以使用该命令进行过滤。通过 NAME 指定的路由策略名称，对 BGP 路由进行过滤，只有通过过滤条件的 BGP 路由才能被加入更新报文中发布出去。 基于协议对路由进行过滤，则可以配置多个路由策略，不会覆盖前面配置的路由策略
isis	配置引入 ISIS 路由的路由策略	对 RIP 中引入的 ISIS 路由在被加入到更新报文中发布出去前，可以使用该命令进行过滤。通过 NAME 指定的路由策略名称，对 ISIS 路由进行过滤，只有通过过滤条件的 ISIS 路由才能被加入更新报文中发布出去。 基于协议对路由进行过滤，则可以配置多个路由策略，不会覆盖前面配置的路由策略
name	路由策略的名字，必须事先配置	字符串，不超过 20 个字节。
export	发送路由策略	-
import	接收路由策略	-

### 4.3.5 配置 RIPng 相关参数

#### 目的

用户可以执行本节操作配置 RIPng 定时器、水平分割/毒性逆转、零域检查，对 RIPng 网络的性能进行调整和优化。

#### 前提配置

在调整和优化 RIPng 网络之前，需要完成以下任务：

- 配置接口的网络层地址，使相邻节点网络层可达。
- 执行 4.3.3 配置 RIPng 基本功能小节配置操作。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置 update timer，expire timer 和 garbage timer 的定时器	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>router ripng</b> 或 <b>router ripng rip-process</b> 或 <b>router ripng vpn-instance NAME</b> 或 <b>router ripng rip-process vpn-instance NAME</b> 从全局配置视图进入 RIPNG 或者 RIPNG VPN 配置节点；</li> <li>3. <b>timers update { update-value   default } expire { expire-value   default } garbage { garbage-value   default }</b></li> <li>4. 结束。</li> </ol>
对 RIPng 报文中的零域进行检查	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>router ripng rip-process</b> 进入 RIPNG 配置视图；</li> <li>3. 执行命令 <b>check-zero { enable   disable }</b>；</li> <li>4. 结束。</li> </ol>
使能或去使能 RIPNG 水平分割功能	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface vlan vlan-id</b> 进入 VLANIF 配置视图；</li> <li>3. 执行命令 <b>ipv6 ripng rip-process split-horizen { enable   disable }</b>；</li> <li>4. 结束。</li> </ol>

附表：

参数	说明	取值
distance	OSPF 路由协议距离	整数形式，取值范围是 1-254
Name	VPN 实例名，输入的 VPN 名必须是真实存在的	字符串，最大长度为 30
rip-process	RIP 多实例号	整数形式，取值范围是 1-2047
vlan-id	vlan 接口号	整数取值，取值范围是 1-4094

## 4.3.6 维护及调试

### 目的

当 RIPng 功能不正常，需要进行查看、调试或定位问题时，可以使用本小节操作。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
----	----

目的	步骤
打开 RIPng 协议调试功能	<ol style="list-style-type: none"> <li>保持当前特权用户视图；</li> <li>执行命令 <b>debug ripng { pkt-in   pkt-out   rx   tx   config   sync-rx   sync-tx   sync-detail   socket-msg   socket-msg-detail   rt-trace   all }</b> 打开 RIPng 协议调试功能；</li> <li>结束。</li> </ol>
关闭 RIPng 协议调试功能	<ol style="list-style-type: none"> <li>保持当前特权用户视图；</li> <li>执行命令 <b>no debug ripng { pkt-in   pkt-out   rx   tx   config   sync-rx   sync-tx   sync-detail   socket-msg   socket-msg-detail   rt-trace   all }</b>；</li> <li>结束。</li> </ol>
查看 RIPng 或者 RIPng 实例的配置信息	<ol style="list-style-type: none"> <li>执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface vlan <i>vlan-id</i></b> 进入 VLANIF 配置视图，或执行命令 <b>router ripng</b> 从全局配置视图进入 RIPNG 配置节点或不执行任何命令保持当前特权用户视图；</li> <li>执行命令 <b>show ipv6 ripng</b> 或 <b>show ipv6 ripng rip-process</b> 显示 RIPng 或者 RIPng 实例的配置信息；</li> <li>结束。</li> </ol>
查看 RIPng 实例或某个实例的接口信息	<ol style="list-style-type: none"> <li>执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface vlan <i>vlan-id</i></b>，或执行命令 <b>router ripng</b> 从全局配置视图进入 RIPNG 配置节点或不执行任何命令保持当前特权用户视图；</li> <li>执行命令 <b>show ipv6 ripng interface</b> 或 <b>show ipv6 ripng rip-process interface</b> 显示 RIPng 实例或某个实例的接口信息；</li> <li>结束。</li> </ol>
查看 RIPng 的详细接口信息	<ol style="list-style-type: none"> <li>执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface vlan <i>vlan-id</i></b>，或执行命令 <b>router ripng</b> 从全局配置视图进入 RIPNG 配置节点或不执行任何命令保持当前特权用户视图；</li> <li>执行命令 <b>show ipv6 ripng interface vlan</b> 或 <b>show ipv6 ripng rip-process interface vlan <i>vlan-id</i></b> 显示 RIPng 的详细接口信息；</li> <li>结束。</li> </ol>
查看 RIPng 实例或某个实例能够发送的路由表信息	<ol style="list-style-type: none"> <li>执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface vlan <i>vlan-id</i></b>，或执行命令 <b>router ripng</b> 从全局配置视图进入 RIPNG 配置节点或不执行任何命令保持当前特权用户视图；</li> <li>执行命令 <b>show ipv6 ripng database</b> 或 <b>show ipv6 ripng rip-process database</b> 或 <b>show ipv6 ripng rip-process database <i>ipv6-address Dst-Mask/ M</i></b> 显示 RIPng 实例或某个实例能够发送的路由表信息；</li> <li>结束。</li> </ol>
查看 RIPng 接口所有资源配置信息	<ol style="list-style-type: none"> <li>执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface vlan <i>vlan-id</i></b>，或执行命令 <b>router ripng</b> 从全局配置视图进入 RIPNG 配置节点或不执行任何命令保持当前特权用户视图；</li> <li>执行命令 <b>show ipv6 ripng resource</b> 显示 RIPng 接口所有资源配置信息；</li> <li>结束。</li> </ol>



目的	步骤
查看 RIPng 邻居信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图, 或执行命令 <b>configure</b> 进入全局配置视图, 或执行命令 <b>interface vlan <i>vlan-id</i></b>, 或执行命令 <b>router ripng</b> 从全局配置视图进入 RIPNG 配置节点或不执行任何命令保持当前特权用户视图;</li> <li>2. 执行命令 <b>show ipv6 ripng neighbor</b> 或 <b>show ipv6 ripng rip-process neighbor</b> 显示 RIPng 邻居信息;</li> <li>3. 结束。</li> </ol>
查看 RIPNG 的当前配置信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图, 或执行命令 <b>configure</b> 进入全局配置视图, 或执行命令 <b>interface vlan <i>vlan-id</i></b>, 或执行命令 <b>router ripng</b> 从全局配置视图进入 RIPNG 配置节点或不执行任何命令保持当前特权用户视图;</li> <li>2. 执行命令 <b>show ipv6 ripng config</b> 显示 RIPNG 的当前配置信息;</li> <li>3. 结束。</li> </ol>

附表:

参数	说明	取值
rip-process	RIPNG 进程号	整数取值, 取值范围是 1-2047, 不配置为 0
vlan-id	vlan 接口号	整数取值, 取值范围是 1-4094
ipv6-address	链路本地 ipv6 地址	在这种形式中, 128 位的 IP 地址被分为 8 组, 每组的 16 位用 4 个十六进制字符 (0~9, A~F) 来表示, 组和组之间用冒号 (:) 隔开。其中每个“X”代表一组十六进制数值
Dst-Maskk/ M	目的 IPV6 地址的路由前缀和掩码长度	整数形式, 取值范围是 0~128

### 4.3.7 配置举例

#### 组网要求

以交换机 A 为例, 要使其支持运行 RIPng 协议, 并且在指定的接口上可以接收和发送 RIPng 报文。

#### 组网图

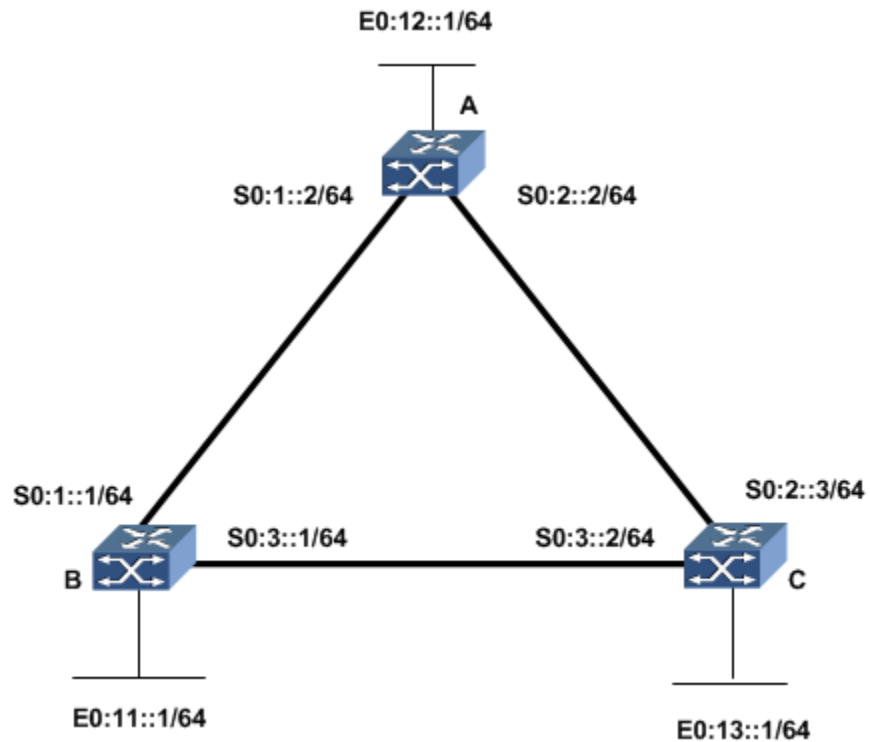


图 4-7 RIPng 配置示意图

### 配置前提

已配置好各链路接口 IPv6 地址，保证链路互通。

### 配置步骤

配置站点 SA。

```

SC9600#config
SC9600(config)#router ripng
SC9600(config-ripng-1)#
SC9600(config-ripng-1)#quit
SC9600(config)#interface vlan 2
//指定接口可以接收和发送 RIPng 报文
SC9600(config-Man-2)#ipv6 address 2::2/64
SC9600(config-Man-2)#ipv6 ripng enable
//查看 RIPng 路由表
SC9600#show ipv6 ripng database
route number:6
    
```

Prefix/Prefixlen	Nexthop	Metric	Age	State	Protocol
1::/64	::	0	0	Active	ripng
2::/64	::	0	0	Active	ripng
3::/64	fe80:3::204:67ff:398:101b	1	17	Active	ripng
11::/64	fe80:3::204:67ff:398:101b	2	17	Active	ripng
12::/64	::	1	0	Active	local
13::/64	fe80:4::204:67ff:398:100a	2	27	Active	ripng

//RIPng 接口在默认情况下是支持简单水平分割的，因此打开调试开关，观察接口发送的报文。

SC9600#

2013/05/04 11:40:26 RIPNG:src=fe80:4::

dst=ff02::9

sport=521, dport=521

2013/05/04 11:40:26 RIPNG:SEND[4]: RESPONSE version=1, packet size=84

prefix=1::/64 metric=1 tag=0

prefix=3::/64 metric=2 tag=0

prefix=11::/64 metric=3 tag=0

prefix=12::/64 metric=2 tag=0

2013/05/04 11:40:26 RIPNG:src=fe80:3::

dst=ff02::9

sport=521, dport=521

2013/05/04 11:40:26 RIPNG:SEND[3]: RESPONSE version=1, packet size=64

prefix=2::/64 metric=1 tag=0

prefix=12::/64 metric=2 tag=0

prefix=13::/64 metric=3 tag=0

//从上面的报文中可以看出，在 RIPng 接口简单水平分割开启的情况下，路由器 A 的 2::/64 接口没有将从 C 路由器那里学习到的 13::/64 路由条目发送回去。如下所示。

2100/05/04 11:40:26 RIPNG:src=fe80:4::

dst=ff02::9

sport=521, dport=521

```
2013/05/04 11:40:26 RIPNG:SEND[4]: RESPONSE version=1, packet size=84
prefix=1::/64 metric=1 tag=0
prefix=3::/64 metric=2 tag=0
prefix=11::/64 metric=3 tag=0
prefix=12::/64 metric=2 tag=0
```

//同样的路由器 A 的 1::2/64 接口没有将从 B 路由器那里学习到的 11::1/64 路由条目发送回去。如下所示。

```
2013/05/04 11:40:26 RIPNG:src=fe80:3::
dst=ff02::9
sport=521, dport=521
```

```
2013/05/04 11:40:26 RIPNG:SEND[3]: RESPONSE version=1, packet size=64
prefix=2::/64 metric=1 tag=0
prefix=12::/64 metric=2 tag=0
prefix=13::/64 metric=3 tag=0
```

在 Man 接口下面通过可以 ipv6 ripng splithorizen disable 命令,关闭简单水平分割功能,同时打开毒性逆转功能。如下报文为 A 路由上接口都打开了毒性逆转功能。

```
2013/05/04 12:00:26 RIPNG:src=fe80:4::
dst=ff02::9
sport=521, dport=521
```

```
2013/05/04 12:00:26 RIPNG:SEND[4]: RESPONSE version=1, packet size=124
prefix=1::/64 metric=1 tag=0
prefix=3::/64 metric=2 tag=0
prefix=11::/64 metric=3 tag=0
prefix=12::/64 metric=2 tag=0
nexthop=::/0
prefix=13::/64 metric=16 tag=0
```

```
2013/05/04 12:00:26 RIPNG:src=fe80:3::
dst=ff02::9
sport=521, dport=521
```

```
2013/05/04 12:00:26 RIPNG:SEND[3]: RESPONSE version=1, packet size=144
prefix=2::/64 metric=1 tag=0
nexthop=::/0
prefix=3::/64 metric=16 tag=0
prefix=11::/64 metric=16 tag=0
prefix=::/0 metric=0 tag=0
prefix=12::/64 metric=2 tag=0
prefix=13::/64 metric=3 tag=0
```

从报文中可以看出，RIPng 接口将从直接相连的对端学习到的路由条目，仍然发送回去，只是这些被发送回去的路由条目度量值字段被设置为了 16。

## 4.4 OSPF 配置

### 4.4.1 OSPF 简介

#### 4.4.1.1 产生背景

OSPF 协议是由 Internet Engineering Task Force 的 OSPF 工作组所开发的，特别为 TCP/IP 网络而设计，包括明确的支持 CIDR 和标记来源于外部的路由信息。OSPF 也提供了对路由更新的验证，并在发送/接收更新时使用 IP 多播。此外，还作了很多的工作使得协议仅用很少的路由流量就可以快速地响应拓扑改变。

OSPF 仅通过在 IP 包头中的目标地址来转发 IP 包。IP 包在 AS 中被转发，而没有被其他协议再次封装。OSPF 是一种动态路由协议，它可以快速地探知 AS 中拓扑的改变（例如路由器接口的失效），并在一段时间的收敛后计算出无环路的新路径。收敛的时间很短且只使用很小的路由流量。

在连接状态路由协议中，每台路由器都维持着一个数据库以描述 AS 的拓扑结构。这个数据库被称为连接状态数据库，所有参与的路由器都有着同样的数据库。数据库中的各项说明了特定路由器自身的状态（如该路由器的可用接口和可以到达的邻居）。该路由器通过洪泛/flooding 将其自身的状态传送到整个 AS 中。

所有的路由器同步地运行完全相同的算法。根据连接状态数据库，每台路由器构建出一棵以其自身为树根的最短路径树。最短路径树给出了到达 AS 中各个目标的路径，路由信息的起源在树中表现为树叶。当有多条等值的路径到达同一目标时，数据流量将在这些路径上平均分摊。路径的距离值表现为一个无量纲数。

OSPF 允许将一些网络组合到一起。这样的组被称为区域/area。区域对 AS 中的其他部分隐藏其内部的拓扑结构，信息的隐藏极大地减少了路由流量。同时，区域内的路由仅由区域自身的拓扑来决定，这可使区域抵御错误的路由信息。区域通常是一个子网化了的 IP 网络。OSPF 允许灵活的配置 IP 子网。由 OSPF 发布的每条路径都包含目标和掩码。同一个 IP 网络的两个子网可以有不同的大小（即不同的掩码），这常被称为变长子网/variable length subnetting。数据包按照最佳匹配（最长匹配）来转发。主机路径被看作掩码为“全 1”（0xffffffff）的子网来处理。

OSPF 协议中所有的信息交换都经过验证。这意味着，在 AS 中只有被信任的路由器才能参与路由。有多种验证方法可以被选择。事实上，可以为每个 IP 子网选用不同的验证方法。来源于外部的路由信息（如路由器从诸如 BGP [引用 23] 的外部网关协议中得到的路径）向整个 AS 内部宣告。外部数据与 OSPF 协议的连接状态数据相对独立。每条外部路径可以由所宣告的路由器作出标记，在自制系统边界路由器（ASBR）之间传递额外的信息。

#### 4.4.1.2 协议特点

- 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，使得自治系统中的其他节点能够快速同步这一变化。
- 无环路：OSPF 根据收集到的链路状态，用最短路径树算法计算路由，该算法保证了 OSPF 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，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，保证报文交互的安全性。
- 组播发送：在能够发送组播的链路上，以组播地址发送协议报文，减少对其他设备的干扰。

#### 4.4.1.3 基本概念

##### OSPF 路由的计算过程

OSPF 路由的计算过程可简单描述如下：

1. 每台 OSPF 路由器根据自己周围的网络拓扑结构生成链路状态通告 LSA (Link State Advertisement)，并通过更新报文将 LSA 发送给网络中的其它 OSPF 路由器。
2. 每台 OSPF 路由器都会收集其它路由器发来的 LSA，所有的 LSA 形成链路状态数据库 LSDB (Link State Database)，LSDB 是对整个自治系统的网络拓扑结构的描述。
3. OSPF 路由器将 LSDB 转换成一张带权的有向图，这张图是对整个网络拓扑结构的真实反映。各 OSPF 路由器得到的有向图是完全相同的。
4. 每台 OSPF 路由器根据有向图，使用 SPF 算法计算出一棵以自己为根的最短路径树，这棵树给出了到自治系统中各节点的路由。

### 路由器 ID 号

一台路由器如果要运行 OSPF 协议，必须存在路由器 ID。路由器 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。

路由器的 ID 可以手工配置，也可以由系统自动产生。如果是自动产生如果协议获取不到 routerID，则遵循如下规则：

1. 最小的静态环回地址；
2. 最小的静态主地址；
3. 最小的静态次地址；
4. 最小的静态 linklocal 地址；
5. 最小的 dhcp 分配的地址；

如果协议获取不到 routerID，则 routerID 为 0，对于多实例此时不能进行 network 的配置。

同时可以使用这个命令来手工配置 ID，输入的 ID 必须是本地 IP 地址，如果不是本地 IP 地址，则命令无效。为增强网络的稳定性，OSPF 的 ID 不随 IP 地址变化而变化，即使 ID 对应的 IP 地址被删除，也不会自动改变 OSPF 的 ID，此时需要人工修改 OSPF 的 ID。修改 OSPF 的 ID 后，OSPF 的邻居，数据库等信息会全部重新刷新，一段时间内会产生大量的协议流量，对网络造成冲击，因此不建议频繁使用本命令。

### OSPF 的协议报文

OSPF 有以下五种类型的协议报文：

1. Hello 报文：周期性发送，用于发现和维持 OSPF 邻居关系。
2. DD (Database Description Packet) 报文：描述本地 LSDB 的摘要信息，用于两台路由器开始建立邻接时进行数据库同步。
3. LSR 报文 (Link State Request Packet)：向对方请求所需的 LSA。
4. LSU 报文 (Link State Update Packet)：向对方发送其所需要的 LSA。
5. LSAck 报文 (Link State Acknowledgment Packet)：用来对收到的 LSA 进行确认。

### LSA 的类型

OSPF 中对路由信息的描述都是封装在 LSA 中发布出去，常用的 LSA 有以下类型：

1. Router LSA (Type1)：每个路由器都会产生，描述了路由器的链路状态和开销，在所属的区域内传播。
2. Network LSA (Type2)：由 DR 产生，描述本网段的链路状态，在所属的区域内传播。
3. Network Summary LSA (Type3)：由 ABR (Area Border Router) 产生，描述区域内某个网段的路由，并通告给其他区域。
4. ASBR Summary LSA (Type4)：由 ABR 产生，描述到 ASBR (Autonomous System Boundary Router) 的路由，通告给相关区域。
5. AS External LSA (Type5)：由 ASBR 产生，描述到 AS 外部的路由，通告到所有的区域 (除了 Stub 区域和 NSSA (Not-So-Stubby Area) 区域)。
6. NSSA LSA (Type7)：由 ASBR 产生，描述到 AS 外部的路由，仅在 NSSA 区域内传播。

### 邻居和邻接

在 OSPF 中，邻居 (Neighbors) 和邻接 (Adjacencies) 是两个不同的概念。

1. 邻居关系：SPF 路由器启动后，会通过 OSPF 接口向外发送 Hello 报文。收到 Hello 报文的 OSPF 路由器会检查报文中所定义的一些参数，如果双方一致就会形成邻居关系。
2. 邻接关系：形成邻居关系的双方不一定都能形成邻接关系，这要根据网络类型而定。只有当双方成功交换 DD 报文，并能交换 LSA 之后，才形成真正意义上的邻接关系。



#### 4.4.1.4 OSPF 区域与路由聚合

##### 划分区域

由于网络规模增大，运行 OSPF 路由协议的路由器数量增多，网络和路由器会产生以下的变化。

##### 1. 网络方面的变化

拓扑结构发生变化的概率增大，网络会经常处于“动荡”之中，造成网络中大量的 OSPF 协议报文传递，降低了网络的带宽利用率。每一次拓扑结构发生变化都会导致网络中所有的路由器重新进行路由计算。

##### 2. 路由器方面的变化

- (1) LSDB 增大
- (2) 占用存储空间增加
- (3) SPF 算法变复杂
- (4) CPU 负担变重

##### 3. 划分区域

为了解决上述问题，OSPF 协议将自治系统划分成不同的区域（Area）。区域是从逻辑上将路由器划分为不同的组，每个组用区域号（Area ID）来标识。区域的边界是路由器，而不是链路。一个网段（链路）只能属于一个区域，或者说每个运行 OSPF 的接口必须指明属于哪一个区域，如图 4-8所示。

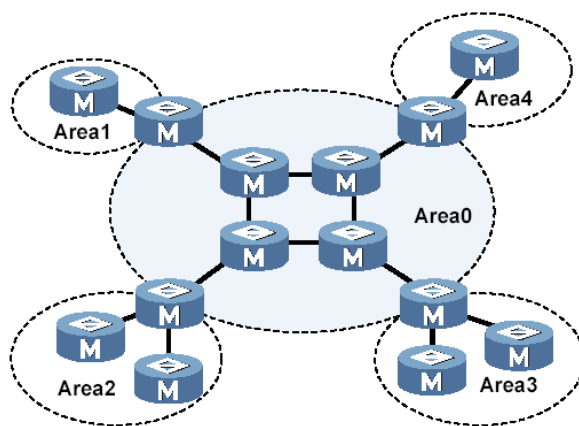


图 4-8 区域划分

划分区域后，可以在区域边界路由器上进行路由聚合，减少通告到其他区域的 LSA 数量。另外，划分区域还可以使网络拓扑变化造成的影响最小化。

### 路由器的类型

如图 4-9所示，OSPF 路由器根据在 AS 中的不同位置，可以分为以下四种类型：

#### 1. 区域内路由器（Internal Routers）

路由器的所有接口都属于同一个 OSPF 区域。

#### 2. 区域边界路由器 ABR（Area Border Routers）

路由器可以同时属于两个以上的区域，但其中一个必须是骨干区域。ABR 用来连接骨干区域和非骨干区域，它与骨干区域之间既可以是物理连接，也可以是逻辑上的连接。

#### 3. 骨干路由器（Backbone Routers）

路由器至少有一个接口属于骨干区域，因此，所有的 ABR 和位于 Area0 的内部路由器都是骨干路由器。

#### 4. 自治系统边界路由器 ASBR（AS boundary Routers）

与其他 AS 交换路由信息的路由器称为 ASBR。ASBR 并不一定位于 AS 的边界，它有可能是区域内路由器，也有可能是 ABR。只要一台 OSPF 路由器引入了外部路由的信息，它就成为 ASBR。

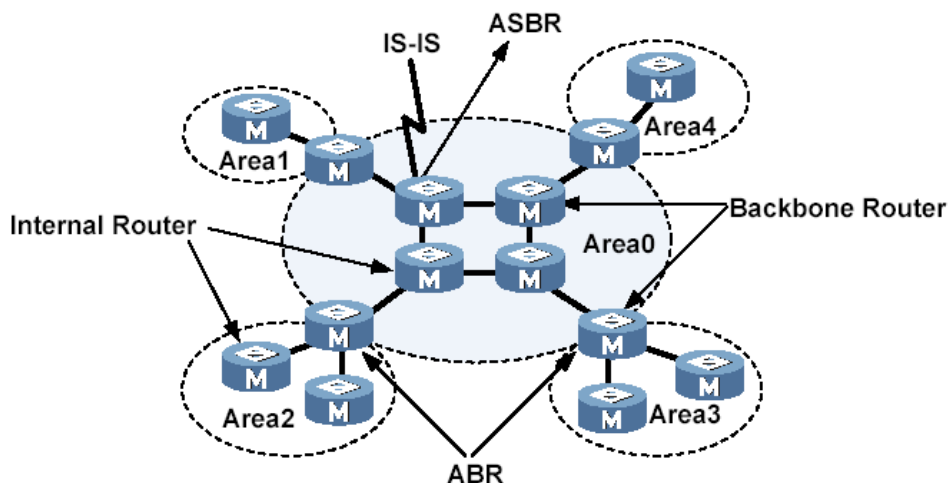


图 4-9 OSPF 路由器的类型

### 骨干区域

OSPF 划分区域之后，并非所有的区域都是平等的关系。其中有一个区域与众不同，通常被称为骨干区域，它的区域号（Area ID）是 0。

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 有以下规定：

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，可能会因为网络拓扑等限制，无法满足以上要求；这时可以通过配置 OSPF 虚连接满足要求。

### 虚连接

虚连接指在两台 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。虚连接相当于在两个 ABR 之间形成了一个点到点的连接。为虚连接两端提供一条非骨干区域内部路由的区域称为中转区域（Transit Area）。

虚连接有如下特点：

1. 虚连接的两端必须是 ABR。
2. 必须在两端同时配置虚连接，虚连接方能生效。
3. 虚连接和物理接口一样可以配置接口参数，如发送 HELLO 报文间隔等。
4. 两台 ABR 之间直接传递 OSPF 报文信息时，他们之间的 OSPF 路由器只起到转发报文的作用。由于协议报文的目的地不是这些路由器，所以这些报文对于他们而言是透明的，只是当作普通的 IP 报文来转发。

### Stub 区域

#### 1. Stub 区域的特点

Stub 区域的 ABR 不传播它们接收到的自治系统外部路由，在这些区域中路由器的路由表规模以及路由信息传递的数量会大大减少。

Stub 区域是一种可选的配置属性，并不是每个区域都符合配置的条件。通常来说，Stub 区域是位于自治系统边界，只有一个 ABR 的非骨干区域。

为保证到自治系统外的路由依旧可达，Stub 区域的 ABR 将生成一条缺省路由，并发布给 Stub 区域中的其他非 ABR 路由器。

#### 2. 配置 Stub 区域的注意事项

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 区域。

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。

### NSSA 区域

在 RFC1587 NSSA Option 中增加一类新的区域：NSSA 区域；同时增加一类新的 LSA：NSSA LSA（或称为 Type7 LSA）。

NSSA 区域其实是 Stub 区域的一个变形，它和 Stub 区域有许多相似的地方。

#### 1. NSSA 区域的特点

与 Stub 区域类似，NSSA 区域也不能配置虚连接。

与 Stub 区域类似，NSSA 区域也不允许 AS-External-LSA（即 Type5 LSA 注入，但可以允许 Type7 LSA 注入。

Type7 LSA 由 NSSA 区域的 ASBR 产生，在 NSSA 区域内传播。

当 Type7 LSA 到达 NSSA 的 ABR 时，由 ABR 将 Type7 LSA 转换成 AS-External LSA，传播到其他区域

#### 2. NSSA 区域举例

如图 4-10所示，运行 OSPF 协议的自治系统包括 3 个区域：区域 1、区域 2 和区域 0，区域 1 被定义为 NSSA 区域。与区域 1、区域 2 相连的非 OSPF 网络运行 RIP 协议。

区域 1 从 RIP 网络接收的 RIP 路由传播到 NSSA ASBR 后，由 NSSA ASB 产生 Type7 LSA 在区域 1 内传播；当 Type7 LSA 到达 NSSA ABR 后，转换成 Type5 LSA 传播到区域 0 和区域 2。

另一方面，区域 2 从 RIP 网络中接收的 RIP 路由通过区域 2 的 ASBR 产生 Type-5LSA 在 OSPF 自治系统中传播。但由于区域 1 是 NSSA 区域，所以 Type-5 LSA 不会到达区域 1。

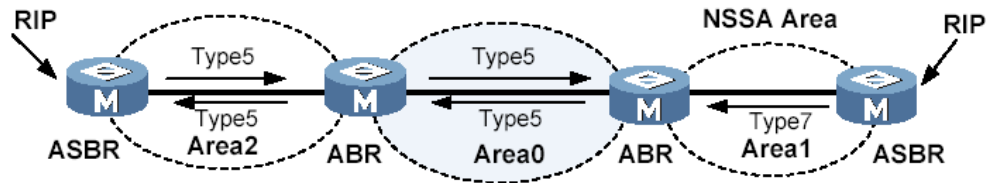


图 4-10 NSSA 区域

### 路由聚合

路由聚合是指：**ABR** 将具有相同前缀的路由信息聚合在一起后，形成一条路由发布到其它区域。

**AS** 被划分成不同的区域后，区域间可以通过路由聚合来减少路由信息，减小路由表的规模，提高路由器的运算速度。

例如，区域 1 内有三条区域内路由 19.1.1.0/24，19.1.2.0/24，19.1.3.0/24，如果此时在 **ABR** 上配置了路由聚合，将三条路由聚合成一条 19.1.0.0/16，则 **ABR** 就只生成一条聚合后的 **LSA**，并发布给其他区域的路由器。

### 路由类型

OSPF 将路由分为 4 级，按优先顺序分别是：

- 区域内路由 (Intra Area)；
- 区域间路由 (Inter Area)；
- 第一类外部路由 (Type1 External)；
- 第二类外部路由 (Type2 External)。

#### 1. AS 内部路由

**AS** 区域内和区域间路由描述的是 **AS** 内部的网络结构。缺省情况下，这两种路由的协议优先级为 10。

#### 2. AS 外部路由

外部路由则描述了应该如何选择到 **AS** 以外目的地址的路由。OSPF 将引入的 **AS** 外部路由分为两类：**Type1** 和 **Type2**。缺省情况下，这两种路由的协议优先级为 150。

第一类外部路由：指接收的是 **IGP** 路由（例如静态路由和 **RIP** 路由）。由于这类路由的可信程度比较高，所以计算出的外部路由的开销与自治系统内部的路由开销是相

同的，并且和 OSPF 自身路由的开销具有可比性；即到第一类外部路由的开销等于本路由器到相应的 ASBR 的开销+ASBR 到该路由目的地址的开销。

第二类外部路由：指接收的是 EGP 路由。由于这类路由的可信度比较低，所以 OSPF 协议认为从 ASBR 到自治系统之外的开销远远大于在自治系统之内到达 ASBR 的开销；所以计算路由开销时将主要考虑前者，即到第二类外部路由的开销=ASBR 到该路由目的地址的开销。如果两条路由由计算出的开销值相等，再考虑本路由器到相应的 ASBR 的开销。

#### 4.4.1.5 OSPF 网络

##### OSPF 网络类型

根据链路层协议类型将网络分为下列四种类型：

##### 1. 广播（Broadcast）类型

当链路层协议是 Ethernet、FDDI（Fiber Distributed Digital Interface）时，OSPF 缺省认为网络类型是 Broadcast。在该类型的网络中，通常以组播形式（224.0.0.5 和 224.0.0.6）发送协议报文。

##### 2. NBMA（Non-Broadcast Multi-Access）类型

当链路层协议是帧中继、ATM 或 X.25 时，OSPF 缺省认为网络类型是 NBMA。在该类型的网络中，以单播形式发送协议报文。

##### 3. 点到多点 P2MP（point-to-multipoint）类型

没有一种链路层协议会被缺省的认为是 Point-to-Multipoint 类型。点到多点必须是由其他的网络类型强制更改的。常用做法是将非全连通的 NBMA 改为点到多点的网络。在该类型的网络中，以组播形式（224.0.0.5）发送协议报文。

##### 4. 点到点 P2P（point-to-point）类型

当链路层协议是 PPP、HDLC 和 LAPB 时，OSPF 缺省认为网络类型是 P2P。在该类型的网络中，以组播形式（224.0.0.5）发送协议报文。

##### DR 和 BDR

在广播网和 NBMA 网络中，任意两台路由器之间都要传递路由信息。如果网络中有 n 台路由器，则需要建立  $nx(n-1)/2$  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 DR（Designated Router）、BDR（Backup Designated Router）和除 DR 和 BDR 之外的路由器（DR Other）。

### 1. DR

所有路由器都只将信息发送给 DR，由 DR 将网络链路状态广播出去。

### 2. BDR

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，并与新的 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）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。

### 3. DR Other

除 DR 和 BDR 之外的路由器（DR Other）之间将不再建立邻接关系，也不再交换任何路由信息。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。

## DR/BDR 选举

### 1. DR/BDR 选举过程

DR 和 BDR 不是人为指定的，而是由本网段中所有的路由器共同选举出来的。路由器接口的 DR 优先级决定了该接口在选举 DR、BDR 时所具有的资格。本网段内 DR 优先级大于 0 的路由器都可作为“候选人”。选举中使用的“选票”就是 Hello 报文。选举过程如下：

每台路由器将自己选出的 DR 写入 Hello 报文中，发给网段上的每台路由器。

如果处于同一网段的两台路由器同时宣布自己是 DR，DR 优先级高者胜出。如果优先级相等，则 Router ID 大者胜出。如果一台路由器的优先级为 0，则它不会被选举为 DR 或 BDR。

### 2. DR/BDR 选举特点

只有在广播或 NBMA 类型接口时才会选举 DR，在点到点或点到多点类型的接口上不需要选举 DR。

DR 是指某个网段中概念，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。

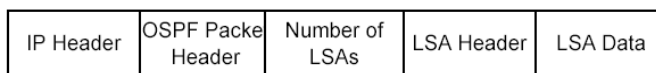
若 DR、BDR 已经选择完毕，当一台新路由器加入后，即使它的 DR 优先级值最大，也不会立即成为该网段中的 DR。

DR 不一定是 DR 优先级最大的路由器；同理，BDR 也不一定是 DR 优先级第二大的路由器。

#### 4.4.1.6 OSPF 报文格式

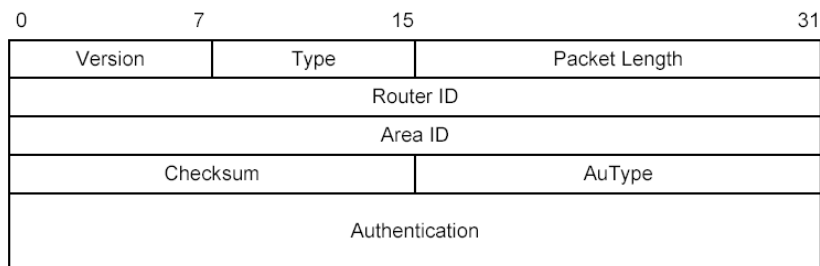
##### OSPF 报文结构

OSPF 用 IP 报文直接封装协议报文，协议号为 89。一个比较完整的 OSPF 报文（以 LSU 报文为例）结构如下图所示。



##### OSPF 报文头

OSPF 有五种报文类型，他们有相同的报文头。如下图所示：



主要字段的解释如下：

##### Version:

OSPF 的版本号，对于 OSPFv2，其值为 2。

##### Type:

OSPF 报文的类型，数值从 1 到 5，分别对应 Hello 报文、DD 报文、LSR 报文、LSU 报文和 LSAck 报文。

##### Packet length:

OSPF 报文的总长度，包括报文头在内，单位为字节。

##### AuType:



验证类型。可分为不验证、简单验证和 MD5 验证，其值分别为 0、1、2。

**Authentication:**

其数值根据验证类型而定。当验证类型为 0 时未作定义，为 1 时此字段为密码信息，类型为 2 时此字段包括 Key ID、MD5 验证数据长度和序列号的信息。

MD5 验证数据添加在 OSPF 报文后面，不包含在 Authenticaiton 字段中。

**Hello 报文**

最常用的一种报文，周期性的发送给本路由器的邻居。内容包括一些定时器的数值、DR、BDR 以及自己已知的邻居。Hello 报文格式如下图所示。

0	7	15	31
Version		Type=1	
Packet Length			
Router ID			
Area ID			
Checksum		AuType	
Authentication			
Network Mask			
HelloInterval		Options	Rtr Pri
RouterDeadInterval			
Designated Router			
Backup Designated Router			
Neighbor			
...			

主要字段解释如下：

**Network Mask:**

发送 Hello 报文的接口所在网络的掩码。

**HelloInterval:**

发送 Hello 报文的时间间隔。如果相邻两台路由器的 Hello 间隔时间不同，则不能建立邻居关系。

**Rtr Pri:**

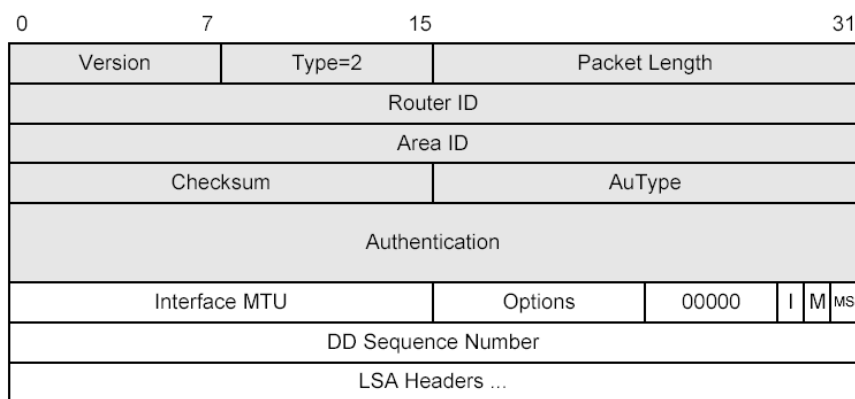
DR 优先级。如果设置为 0，则路由器不能成为 DR/BDR。

**RouterDeadInterval:**

失效时间。如果在此时间内未收到邻居发来的 Hello 报文，则认为邻居失效。如果相邻两台路由器的失效时间不同，则不能建立邻居关系。

### DD 报文

两台路由器进行数据库同步时，用 DD 报文来描述自己的 LSDB，内容包括 LSDB 中每一条 LSA 的 Header（LSA 的 Header 可以唯一标识一条 LSA）。LSA Header 只占一条 LSA 的整个数据量的一小部分，这样可以减少路由器之间的协议报文流量，对端路由器根据 LSA Header 就可以判断出是否已有这条 LSA。DD 报文格式如下图所示。



主要字段的解释如下：

#### Interface MTU:

在不分片的情况下，此接口最大可发出的 IP 报文长度。

#### I (Initial):

当发送连续多个 DD 报文时，如果这是第一个 DD 报文，则置为 1，否则置为 0。

#### M (More):

当发送连续多个 DD 报文时，如果这是最后一个 DD 报文，则置为 0，否则置为 1；表示后面还有其他的 DD 报文。

#### MS (Master/Slave):

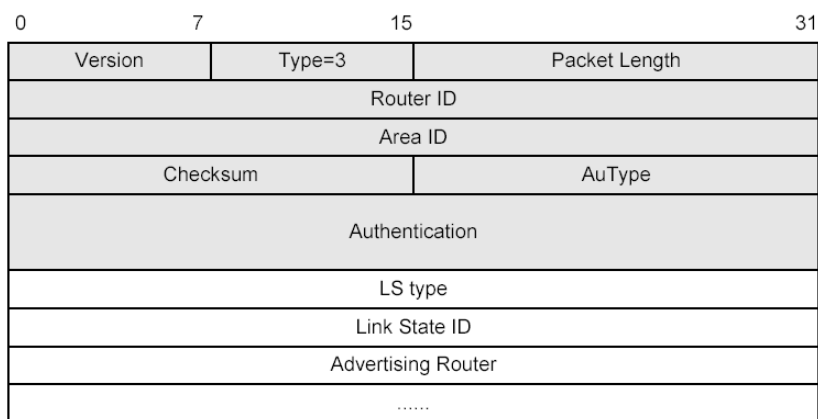
当两台 OSPF 路由器交换 DD 报文时，首先需要确定双方的主从关系，Router ID 大的一方会成为 Master。当值为 1 时表示发送方为 Master。

#### DD Sequence Number:

DD 报文序列号,由 Master 方规定起始序列号,每发送一个 DD 报文序列号加 1,Slave 方使用 Master 的序列号作为确认。主从双方利用序列号来保证 DD 报文传输的可靠性和完整性。

### LSR 报文

两台路由器互相交换过 DD 报文之后,知道对端的路由器有哪些 LSA 是本地的 LSDB 所缺少的,这时需要发送 LSR 报文向对方请求所需的 LSA。内容包括所需要的 LSA 的摘要。LSR 报文格式如下图所示。



主要字段解释如下:

**LS type:**

LSA 的类型号。例如 Type1 表示 Router LSA。

**Link State ID:**

即 LSA 头格式中的字段,根据 LSA 的类型而定。

**Advertising Router:**

产生此 LSA 的路由器的 Router ID。

### LSU 报文

用来向对端路由器发送所需要的 LSA, 内容是多条 LSA (全部内容) 的集合。LSU 报文格式如图所示。

0	7	15	31
Version	Type=4	Packet Length	
Router ID			
Area ID			
Checksum		AuType	
Authentication			
Number of LSAs			
LSAs...			

### LSAck 报文

用来对接收到的 LSU 报文进行确认。内容是需要确认的 LSA 的 Header（一个 LSAck 报文可对多个 LSA 进行确认）。报文格式如图所示。

0	7	15	31
Version	Type=5	Packet Length	
Router ID			
Area ID			
Checksum		AuType	
Authentication			
LSA Headers...			

### LSA 头格式

所有的 LSA 都有相同的报文头，其格式如图所示。

0	7	15	31
LS Age		Options	LS Type
Link State ID			
Advertising Router			
LS Sequence Number			
LS Checksum		Length	

主要字段的解释如下：

#### LS age:

LSA 产生后所经过的时间，以秒为单位。无论 LSA 是在链路上传送，还是保存在 LSDB 中，其值都会在不停的增长。

#### LS type:

LSA 的类型。

**Link State ID:**

具体数值根据 LSA 的类型而定。

**LS sequence number:**

LSA 的序列号，其他路由器根据这个值可以判断哪个 LSA 是最新的。

**length:**

LSA 的总长度，包括 LSA Header，以字节为单位。

**Router LSA**

Router LSA 格式如图所示。

0	7	15	31
LS Age		Options	LS Type=1
Link State ID			
Advertising Router			
LS Sequence Number			
LS Checksum		Length	
0	V   E   B	0	# Links
Link ID			
Link Data			
Type	# TOS	Metric	
.....			
TOS	0	TOS Metric	
Link ID			
Link Data			
.....			

主要字段的解释如下：

**Link State ID:**

最初产生此 LSA 的路由器的 Router ID。

**V (Virtual Link):**

如果产生此 LSA 的路由器是虚连接的端点，则置为 1。

**E (External):**

如果产生此 LSA 的路由器是 ASBR，则置为 1。

**B (Border):**

如果产生此 LSA 的路由器是 ABR，则置为 1。

**# links:**

LSA 中所描述的链路信息的数量，包括路由器上处于某区域中的所有链路和接口。

**Network LSA**

Network LSA 由广播网或 NBMA 网络中的 DR 发出，LSA 中记录了这一网络上所有路由器的 Router ID。如下图所示。

0	7	15	31
LS Age		Options	LS Type=2
Link State ID			
Advertising Router			
LS Sequence Number			
LS Checksum		Length	
Network Mask			
Attached Router			
.....			

主要字段的解释如下：

**Link State ID:**

DR 路由器的接口地址。

**Network Mask:**

广播网或 NBMA 网络地址的掩码。

**Attached Router:**

连接在同一个网络上的所有路由器的 Router ID，也包括 DR 的 Router ID。

**Summary LSA**

Type3 和 Type4 的 LSA 有相同的格式，它们都是由 ABR 产生。如图所示。

0	7	15	31
LS Age		Options	LS Type=3 or 4
Link State ID			
Advertising Router			
LS Sequence Number			
LS Checksum		Length	
Network Mask			
0	Metric		
TOS	TOS Metric		
.....			

主要字段的解释如下：

**Link State ID:**

对于 Type3 LSA 来说,它是所通告的网络地址;对于 Type4 来说,它是 ASBR 的 Router ID。

**Network Mask:**

Type3 LSA 的网络地址掩码。对于 Type4 LSA 来说没有意义, 设置为 0.0.0.0。

**metric:**

到目的地址的路由开销。

**AS-External LSA**

由 ASBR 产生, 描述到 AS 外部去的路由信息。如图所示。

0	7	15	31
LS Age		Options	LS Type=5
Link State ID			
Advertising Router			
LS Sequence Number			
LS Checksum		Length	
Network Mask			
E	0	Metric	
Forwarding Address			
External Route Tag			
E	TOS	TOS Metric	
Forwarding Address			
External Route Tag			
.....			

主要字段的解释如下：

**Link State ID:**

所要通告的其他外部 AS 的目的地址。

**Network Mask:**

所通告的目的地址的掩码。

**E (External Metric):**

外部度量值的类型。如果是第 2 类外部路由就设置为 1，如果是第 1 类外部路由则设置为 0。

**metirc:**

路由开销。

**Forwarding Address:**

到所通告的目的地址的报文将被转发到这个地址。通常为 0，表明以通告路由器为下一跳。

**External Route Tag:**

添加到外部路由上的标记。OSPF 本身并不使用这个字段，它可以用来对外部路由进行管理。

**NSSA External LSA**



由 ASBR 产生，且只能在 NSSA 区域内传播。其格式与 AS-External LSA 相同。

## 4.4.2 OSPF 配置

### 4.4.2.1 配置全局 OSPF

#### 4.4.2.1.1 使能 OSPF 进程

##### 目的

本节介绍如何启动和关闭（使能/去使能）OSPF 进程。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
启动默认 OSPF 进程	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图； 2. 执行命令 <code>router ospf</code>	-
启动指定 OSPF 进程	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图； 2. 执行命令 <code>router ospf process id</code>	Process id: SC9600 支持的 OSPF 进程 ID，取值范围为：1-2047
关闭默认 OSPF 进程	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图； 2. 执行命令 <code>no router ospf</code>	-
关闭指定 OSPF 进程	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图； 2. 执行命令 <code>no router ospf process id</code>	Process id: SC9600 支持的 OSPF 进程 ID，取值范围为：1-2047
关闭所有 OSPF 进程	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图； 2. 执行命令 <code>no router ospf all</code>	-

#### 4.4.2.1.2 使能 OSPF 进程指定 VPN 实例

##### 目的

本节介绍如何启动（使能）OSPF 进程指定的 VPN 实例。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
启动指定 OSPF 进程指定 VPN 实例	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>router ospf process id vpn-instance NAME</code></li> </ol>	Process id: SC9600 支持的 OSPF 进程 ID, 取值范围为: 1-2047; NAME: VPN 实例名, 命名规则为少于 31 字符
启动默认 OSPF 进程指定 VPN 实例	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>router ospf vpn-instance NAME</code></li> </ol>	NAME: VPN 实例名, 命名规则为少于 31 字符

#### 4.4.2.1.3 复位 OSPF 进程

##### 目的

本节介绍如何复位 OSPF 进程。

##### 过程

根据不同目的, 执行相应步骤, 具体参见下表。

目的	步骤	参数说明
复位 OSPF 进程	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>reset ospf</code></li> </ol>	-
复位指定 OSPF 进程	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>reset ospf process id</code></li> </ol>	Process id: SC9600 支持的 OSPF 进程 ID, 取值范围为: 1-2047

#### 4.4.2.1.4 清除 OSPF 统计信息

##### 目的

本节介绍如何清除 OSPF 统计信息。

##### 过程

根据不同目的, 执行相应步骤, 具体参见下表。

目的	步骤	参数说明
清除 OSPF 统计信息	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>reset ospf counters</code></li> </ol>	-

#### 4.4.2.2 配置 OSPF 节点

##### 4.4.2.2.1 配置路由器 ID

###### 目的

本节介绍如何配置路由器 ID。

###### 背景信息

配置的路由器 ID 必须为本地 IP 地址之一。

###### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置路由器 ID	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>router ospf</code>，进入 OSPF 配置视图；</li> <li>3. 执行命令 <code>router-id router-id</code></li> </ol>	<b>router-id</b> : 路由器 ID，点分十进制形式，形如： (A.B.C.D)，其中 A~D 为整数形式，取值范围为 1-255

##### 4.4.2.2.2 配置 OSPF 接口

###### 目的

本节介绍如何配置 OSPF 接口。

###### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置 OSPF 接口和区域	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>router ospf</code>，进入 OSPF 配置视图；</li> <li>3. 执行命令 <code>network network-address ospf-network-mask area area-id</code></li> </ol>	<b>Network-address</b> : 网络 IP 地址，点分十进制形式，形如：(A.B.C.D)，其中 A~D 为整数形式，取值范围为 1-255； <b>Ospf-network-mask</b> : OSPF 网络掩码，点分十进制形式，形如：(A.B.C.D)，其中 A~D 为整数形式，取值范围为 1-255； <b>area-id</b> : OSPF 区域 ID，点分十进制形式，形如：(A.B.C.D)，其中 A~D 为整数形式，取值范围为 1-255(大于 65535 的区域) 或者整数形式，取值范围为 0-4294967295(小于 65535 的区

目的	步骤	参数说明
		域)
删除 OSPF 接口	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图;</li> <li>2. 执行命令 <code>router ospf</code>, 进入 OSPF 配置视图;</li> <li>3. 执行命令 <code>no network network-address ospf-network-mask area area-id</code></li> </ol>	<p><b>Network-address:</b> 网络 IP 地址, 点分十进制形式, 形如: (A.B.C.D), 其中 A~D 为整数形式, 取值范围为 1-255;</p> <p><b>Ospf-network-mask:</b> OSPF 网络掩码, 点分十进制形式, 形如: (A.B.C.D), 其中 A~D 为整数形式, 取值范围为 1-255;</p> <p><b>area-id:</b> OSPF 区域 ID, 点分十进制形式, 形如: (A.B.C.D), 其中 A~D 为整数形式, 取值范围为 1-255(大于 65535 的区域) 或者整数形式, 取值范围为 0-4294967295(小于 65535 的区域)</p>

#### 4.4.2.2.3 配置 Stub 区域

##### 目的

本节介绍如何配置 Stub 区域。

##### 过程

根据不同目的, 执行相应步骤, 具体参见下表。

目的	步骤	参数说明
配置普通 Stub 区域	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图;</li> <li>2. 执行命令 <code>router ospf</code>, 进入 OSPF 配置视图;</li> <li>3. 执行命令 <code>area area-id stub</code></li> </ol>	<p><b>area-id:</b> OSPF 区域 ID, 点分十进制形式, 形如: (A.B.C.D), 其中 A~D 为整数形式, 取值范围为 1-255(大于 65535 的区域) 或者整数形式, 取值范围为 0-4294967295(小于 65535 的区域)</p>
配置 totalStub 区域	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图;</li> <li>2. 执行命令 <code>router ospf</code>, 进入 OSPF 配置视图;</li> <li>3. 执行命令 <code>area area-id stub no-summary</code></li> </ol>	<p><b>area-id:</b> OSPF 区域 ID, 点分十进制形式, 形如: (A.B.C.D), 其中 A~D 为整数形式, 取值范围为 1-255(大于 65535 的区域) 或者整数形式, 取值范围为 0-4294967295(小于 65535 的区域)</p>

目的	步骤	参数说明
		域)
配置默认 Summary LSA 开销	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图; 2. 执行命令 <code>router ospf</code> , 进入 OSPF 配置视图; 3. 执行命令 <code>area area-id default-cost cost</code>	Cost: 默认 summary LSA 开销, 整数形式, 取值范围为 1-65535
删除 Stub 区域	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图; 2. 执行命令 <code>router ospf</code> , 进入 OSPF 配置视图; 3. 执行命令 <code>no area area-id stub</code>	area-id: OSPF 区域 ID, 点分十进制形式, 形如: (A.B.C.D), 其中 A~D 为整数形式, 取值范围为 1-255(大于 65535 的区域) 或者整数形式, 取值范围为 0-4294967295(小于 65535 的区域)

#### 4.4.2.2.4 配置 NSSA 区域

##### 目的

本节介绍如何配置 NSSA 区域。

##### 过程

根据不同目的, 执行相应步骤, 具体参见下表。

目的	步骤	参数说明
配置 NSSA 区域	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图; 2. 执行命令 <code>router ospf</code> , 进入 OSPF 配置视图; 3. 执行命令 <code>area area-id nssa</code>	area-id: OSPF 区域 ID, 点分十进制形式, 形如: (A.B.C.D), 其中 A~D 为整数形式, 取值范围为 1-255(大于 65535 的区域) 或者整数形式, 取值范围为 0-4294967295(小于 65535 的区域)
配置 NSSA 默认 LSA 开销	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图; 2. 执行命令 <code>router ospf</code> , 进入 OSPF 配置视图; 3. 执行命令 <code>area area-id nssa default-cost cost</code> 或 <code>area area-id nssa default-cost default</code>	area-id: OSPF 区域 ID, 点分十进制形式, 形如: (A.B.C.D), 其中 A~D 为整数形式, 取值范围为 1-255(大于 65535 的区域) 或者整数形式, 取值范围为 0-4294967295(小于 65535 的区域); Cost: 默认 NSSA 的 LSA 开销,

目的	步骤	参数说明
		整数形式，取值范围为 1-65535
配置 no summary NSSA 区域	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>router ospf</code>，进入 OSPF 配置视图；</li> <li>3. 执行命令 <code>area area-id nssa no-summary</code></li> </ol>	<p><b>area-id:</b> OSPF 区域 ID，点分十进制形式，形如：(A.B.C.D)，其中 A~D 为整数形式，取值范围为 1-255(大于 65535 的区域) 或者整数形式，取值范围为 0-4294967295(小于 65535 的区域)</p>
配置 NSSA 区域聚合通告/不通告	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>router ospf</code>，进入 OSPF 配置视图；</li> <li>3. 执行命令 <code>area area-id nssa range dst-address dst-mask { advertise   no-advertise }</code></li> </ol>	<p><b>area-id:</b> OSPF 区域 ID，点分十进制形式，形如：(A.B.C.D)，其中 A~D 为整数形式，取值范围为 1-255(大于 65535 的区域) 或者整数形式，取值范围为 0-4294967295(小于 65535 的区域)；</p> <p><b>Dst-address:</b> 目的地址，点分十进制形式，形如：(A.B.C.D)，其中 A~D 为整数形式，取值范围为 1-255；</p> <p><b>Dst-mask:</b> 目的地址掩码，点分十进制形式，形如：(A.B.C.D)，其中 A~D 为整数形式，取值范围为 1-255；</p> <p><b>Advertise:</b> 将匹配到该网段的且非自己生成的 NSSA LSA 转换聚合合成一条 5 类 LSA；</p> <p><b>No-advertise:</b> 将匹配到该网段的且非自己生成的 NSSA LSA 不转换为 5 类 LSA</p>
配置 NSSA 指定转换路由器或者候选转换路由器	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>router ospf</code>，进入 OSPF 配置视图；</li> <li>3. 执行命令 <code>area area-id nssa translator { always   candidate }</code></li> </ol>	<p><b>area-id:</b> OSPF 区域 ID，点分十进制形式，形如：(A.B.C.D)，其中 A~D 为整数形式，取值范围为 1-255(大于 65535 的区域) 或者整数形式，取值范围为 0-4294967295(小于 65535 的区域)；</p> <p><b>Always:</b> 在 NSSA 区域的 ABR 中，指定转换路由器。允许将 NSSA 区域中的多个 ABR 配置成</p>

目的	步骤	参数说明
		转换路由器； <b>Candidate:</b> 在 NSSA 区域的 ABR 中，为候选转换路由器。如果在当前区域中，都没有指定转换路由器，则由所有的候选路由器进行选举产生转换路由器
删除 NSSA 区域	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图； 2. 执行命令 <code>router ospf</code> ，进入 OSPF 配置视图； 3. 执行命令 <code>no area area-id nssa</code>	<b>area-id:</b> OSPF 区域 ID，点分十进制形式，形如：(A.B.C.D)，其中 A~D 为整数形式，取值范围为 1-255(大于 65535 的区域) 或者整数形式，取值范围为 0-4294967295(小于 65535 的区域)
删除 NSSA 区域聚合	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图； 2. 执行命令 <code>router ospf</code> ，进入 OSPF 配置视图； 3. 执行命令 <code>no area area-id nssa range dst-address dst-mask</code>	<b>area-id:</b> OSPF 区域 ID，点分十进制形式，形如：(A.B.C.D)，其中 A~D 为整数形式，取值范围为 1-255(大于 65535 的区域) 或者整数形式，取值范围为 0-4294967295(小于 65535 的区域)； <b>Dst-address:</b> 目的地址，点分十进制形式，形如：(A.B.C.D)，其中 A~D 为整数形式，取值范围为 1-255； <b>Dst-mask:</b> 目的地址掩码，点分十进制形式，形如：(A.B.C.D)，其中 A~D 为整数形式，取值范围为 1-255；

#### 4.4.2.2.5 创建及配置 OSPF 虚接口

##### 目的

本节介绍如何配置 OSPF 虚接口。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
创建 OSPF 虚接口	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图； 2. 执行命令 <code>router ospf</code> ，进入 OSPF 配	<b>area-id:</b> OSPF 区域 ID，点分十进制形式，形如：(A.B.C.D)，其中 A~D 为整数形式，取值范围为

目的	步骤	参数说明
	置视图; 3. 执行命令 <code>area area-id virtual-link neighbor-address</code>	1-255(大于 65535 的区域) 或者整数形式, 取值范围为 0-4294967295(小于 65535 的区域); neighbor-address: 虚邻居的 Router ID, 点分十进制形式, 形如: (A.B.C.D), 其中 A~D 为整数形式, 取值范围为 1-255
删除 OSPF 虚接口	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图; 2. 执行命令 <code>router ospf</code> , 进入 OSPF 配置视图; 3. 执行命令 <code>no area area-id virtual-link neighbor-address</code>	area-id: OSPF 区域 ID, 点分十进制形式, 形如: (A.B.C.D), 其中 A~D 为整数形式, 取值范围为 1-255(大于 65535 的区域) 或者整数形式, 取值范围为 0-4294967295(小于 65535 的区域); neighbor-address: 虚邻居的 Router ID, 点分十进制形式, 形如: (A.B.C.D), 其中 A~D 为整数形式, 取值范围为 1-255
配置 OSPF 虚接口邻居超时时间	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图; 2. 执行命令 <code>router ospf</code> , 进入 OSPF 配置视图; 3. 执行命令 <code>area area-id virtual-link neighbor-address dead-interval dead-interval</code> 或 <code>area area-id virtual-link neighbor-address dead-interval default</code>	area-id: OSPF 区域 ID, 点分十进制形式, 形如: (A.B.C.D), 其中 A~D 为整数形式, 取值范围为 1-255(大于 65535 的区域) 或者整数形式, 取值范围为 0-4294967295(小于 65535 的区域); neighbor-address: 虚邻居的 Router ID, 点分十进制形式, 形如: (A.B.C.D), 其中 A~D 为整数形式, 取值范围为 1-255; dead-interval: 虚邻居的死亡时间, 整数形式, 取值范围是 0-2147483647, 单位: 秒
配置 OSPF 虚接口 Hello 间隔时间	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图; 2. 执行命令 <code>router ospf</code> , 进入 OSPF 配置视图; 3. 执行命令 <code>area area-id virtual-link neighbor-address hello-interval hello-interval</code>	area-id: OSPF 区域 ID, 点分十进制形式, 形如: (A.B.C.D), 其中 A~D 为整数形式, 取值范围为 1-255(大于 65535 的区域) 或者整数形式, 取值范围为 0-4294967295(小于 65535 的区域);



目的	步骤	参数说明
	或 area <i>area-id</i> virtual-link neighbor-address hello-interval default	neighbor-address: 虚邻居的 Router ID, 点分十进制形式, 形如: (A.B.C.D), 其中 A~D 为整数形式, 取值范围为 1-255; hello-interval: 呼叫虚邻居的时间间隔, 整数形式, 取值范围是 1~65535, 单位: 秒
配置 OSPF 虚接口重传间隔时间	1. 在特权用户视图下执行命令 configure 进入全局配置视图; 2. 执行命令 router ospf, 进入 OSPF 配置视图; 3. 执行命令 area <i>area-id</i> virtual-link neighbor-address retransmit-interval retransmit-interval 或 area <i>area-id</i> virtual-link neighbor-address retransmit-interval default	area-id: OSPF 区域 ID, 点分十进制形式, 形如: (A.B.C.D), 其中 A~D 为整数形式, 取值范围为 1-255(大于 65535 的区域) 或者整数形式, 取值范围为 0-4294967295(小于 65535 的区域); neighbor-address: 虚邻居的 Router ID, 点分十进制形式, 形如: (A.B.C.D), 其中 A~D 为整数形式, 取值范围为 1-255; retransmit-interval: 链路状态通告的重传时间间隔, 整数形式, 取值范围是 0-3600, 单位: 秒
配置 OSPF 虚接口传输时延	1. 在特权用户视图下执行命令 configure 进入全局配置视图; 2. 执行命令 router ospf, 进入 OSPF 配置视图; 3. 执行命令 area <i>area-id</i> virtual-link neighbor-address transmit-delay transmit-delay 或 area <i>area-id</i> virtual-link neighbor-address transmit-delay default	area-id: OSPF 区域 ID, 点分十进制形式, 形如: (A.B.C.D), 其中 A~D 为整数形式, 取值范围为 1-255(大于 65535 的区域) 或者整数形式, 取值范围为 0-4294967295(小于 65535 的区域); neighbor-address: 虚邻居的 Router ID, 点分十进制形式, 形如: (A.B.C.D), 其中 A~D 为整数形式, 取值范围为 1-255; transmit-delay: 链路状态通告的传输时延, 整数形式, 取值范围是 0-3600, 单位: 秒
配置 OSPF 虚接口简单密码认证	1. 在特权用户视图下执行命令 configure 进入全局配置视图; 2. 执行命令 router ospf, 进入 OSPF 配置视图; 3. 执行命令 area <i>area-id</i> virtual-link	area-id: OSPF 区域 ID, 点分十进制形式, 形如: (A.B.C.D), 其中 A~D 为整数形式, 取值范围为 1-255(大于 65535 的区域) 或者整数形式, 取值范围为

目的	步骤	参数说明
	<code>neighbor-address authentication</code> <code>simple-passw ord key</code>	0-4294967295(小于 65535 的区域); neighbor-address: 虚邻居的 Router ID,点分十进制形式,形如:(A.B.C.D),其中 A~D 为整数形式,取值范围为 1-255; key: 验证关键字,字符串形式,KEY 的长度不超过 8 字节
配置 OSPF 虚接口 MD5 认证	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图; 2. 执行命令 <code>router ospf</code> , 进入 OSPF 配置视图; 3. 执行命令 <code>area area-id virtual-link neighbor-address authentication md5 key-id key</code>	area-id: OSPF 区域 ID, 点分十进制形式, 形如: (A.B.C.D), 其中 A~D 为整数形式, 取值范围为 1-255(大于 65535 的区域) 或者整数形式, 取值范围为 0-4294967295(小于 65535 的区域); neighbor-address: 虚邻居的 Router ID,点分十进制形式,形如:(A.B.C.D),其中 A~D 为整数形式,取值范围为 1-255; md5 key-id: MD5 密文验证标识符, 整数形式, 取值范围是 1~255; key: 验证关键字, 字符串形式, KEY 的长度不超过 8 字节
配置删除 OSPF 虚接口认证	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图; 2. 执行命令 <code>router ospf</code> , 进入 OSPF 配置视图; 3. 执行命令 <code>area area-id virtual-link neighbor-address authentication</code>	area-id: OSPF 区域 ID, 点分十进制形式, 形如: (A.B.C.D), 其中 A~D 为整数形式, 取值范围为 1-255(大于 65535 的区域) 或者整数形式, 取值范围为 0-4294967295(小于 65535 的区域); neighbor-address: 虚邻居的 Router ID,点分十进制形式,形如:(A.B.C.D),其中 A~D 为整数形式,取值范围为 1-255
配置区域简单密码认证	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图; 2. 执行命令 <code>router ospf</code> , 进入 OSPF 配置视图; 3. 执行命令 <code>area area-id authentication simple-passw ord key</code>	area-id: OSPF 区域 ID, 点分十进制形式, 形如: (A.B.C.D), 其中 A~D 为整数形式, 取值范围为 1-255(大于 65535 的区域) 或者整数形式, 取值范围为 0-4294967295(小于 65535 的区

目的	步骤	参数说明
		域); key: 验证关键字, 字符串形式, KEY 的长度不超过 8 字节
配置区域 MD5 认证	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图;</li> <li>2. 执行命令 <code>router ospf</code>, 进入 OSPF 配置视图;</li> <li>3. 执行命令 <code>area area-id authentication md5 key-id key</code></li> </ol>	area-id: OSPF 区域 ID, 点分十进制形式, 形如: (A.B.C.D), 其中 A~D 为整数形式, 取值范围为 1-255(大于 65535 的区域) 或者整数形式, 取值范围为 0-4294967295(小于 65535 的区域); md5 key-id: MD5 密文验证标识符, 整数形式, 取值范围是 1~255; key: 验证关键字, 字符串形式, KEY 的长度不超过 8 字节
删除区域认证	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图;</li> <li>2. 执行命令 <code>router ospf</code>, 进入 OSPF 配置视图;</li> <li>3. 执行命令 <code>no area area-id authentication</code></li> </ol>	area-id: OSPF 区域 ID, 点分十进制形式, 形如: (A.B.C.D), 其中 A~D 为整数形式, 取值范围为 1-255(大于 65535 的区域) 或者整数形式, 取值范围为 0-4294967295(小于 65535 的区域)

#### 4.4.2.2.6 配置区域聚合

##### 目的

本节介绍如何配置区域聚合。

##### 过程

根据不同目的, 执行相应步骤, 具体参见下表。

目的	步骤	参数说明
区域聚合	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图;</li> <li>2. 执行命令 <code>router ospf</code>, 进入 OSPF 配置视图;</li> <li>3. 执行命令 <code>area area-id range dst-address dst-mask { advertise   no-advertise }</code></li> </ol>	area-id: OSPF 区域 ID, 点分十进制形式, 形如: (A.B.C.D), 其中 A~D 为整数形式, 取值范围为 1-255(大于 65535 的区域) 或者整数形式, 取值范围为 0-4294967295(小于 65535 的区域); Dst-address: 目的地址, 点分十进制形式, 形如: (A.B.C.D), 其中 A~D 为整数形式, 取值范围为

目的	步骤	参数说明
		1-255; Dst-mask: 目的地址掩码, 点分十进制形式, 形如: (A.B.C.D), 其中 A~D 为整数形式, 取值范围为 1-255; Advertise: 为聚合条目生成 Summary LSA; No-advertise: 不生成聚合条目对应的 Summary LSA
删除区域聚合	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图; 2. 执行命令 <code>router ospf</code> , 进入 OSPF 配置视图; 3. 执行命令 <code>no area area-id range dst-address dst-mask</code>	area-id: OSPF 区域 ID, 点分十进制形式, 形如: (A.B.C.D), 其中 A~D 为整数形式, 取值范围为 1-255(大于 65535 的区域) 或者整数形式, 取值范围为 0-4294967295(小于 65535 的区域); Dst-address: 目的地址, 点分十进制形式, 形如: (A.B.C.D), 其中 A~D 为整数形式, 取值范围为 1-255; Dst-mask: 目的地址掩码, 点分十进制形式, 形如: (A.B.C.D), 其中 A~D 为整数形式, 取值范围为 1-255

#### 4.4.2.2.7 配置路由协议过滤策略

##### 目的

本节介绍如何配置路由协议过滤策略。

##### 过程

根据不同目的, 执行相应步骤, 具体参见下表。

目的	步骤	参数说明
配置路由协议的过滤策略	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图; 2. 执行命令 <code>router ospf</code> , 进入 OSPF 配置视图; 3. 执行命令 <code>filter route-policy route-policy-name</code>	Route-policy-name: 指定的路由策略名, 必须是路由策略里面已经配置的, 字符串形式

目的	步骤	参数说明
取消路由协议的过滤策略	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>router ospf</code>，进入 OSPF 配置视图；</li> <li>3. 执行命令 <code>no filter route-policy route-policy-name</code></li> </ol>	Route-policy-name：指定的路由策略名，必须是路由策略里面已经配置的，字符串形式

#### 4.4.2.2.8 使能路由快速重分配功能

##### 目的

本节介绍如何使能路由快速重分配功能。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
使能 FRR	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>router ospf</code>，进入 OSPF 配置视图；</li> <li>3. 执行命令 <code>frr (enable   disable)</code></li> </ol>	Frr：快速路由重分配，Fast Router Re-distribution

#### 4.4.2.2.9 配置 GR 重启

##### 目的

本节介绍如何配置 GR(Graceful Restart)重启。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
使能 GR	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>router ospf</code>，进入 OSPF 配置视图；</li> <li>3. 执行命令 <code>graceful-restart</code></li> </ol>	-
配置 GR 周期	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>router ospf</code>，进入 OSPF 配置视图；</li> <li>3. 执行命令 <code>graceful-restart period</code></li> </ol>	Restart-time：重启过程时间，整数形式，取值范围是 40~1800，单位为秒

目的	步骤	参数说明
	<i>restart-time</i>	
使能 GR helper	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>router ospf</code>，进入 OSPF 配置视图；</li> <li>3. 执行命令 <code>graceful-restart helper</code></li> </ol>	-
去使能 GR 重启	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>router ospf</code>，进入 OSPF 配置视图；</li> <li>3. 执行命令 <code>no graceful-restart</code></li> </ol>	-
去使能 GR helper	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>router ospf</code>，进入 OSPF 配置视图；</li> <li>3. 执行命令 <code>no graceful-restart helper</code></li> </ol>	-
执行 GR 重启	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>router ospf</code>，进入 OSPF 配置视图；</li> <li>3. 执行命令 <code>graceful-restart begin</code></li> </ol>	-

#### 4.4.2.2.10 使能 opaque 功能

##### 目的

本节介绍如何使能 opaque 功能。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置 opaque 功能	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>router ospf</code>，进入 OSPF 配置视图；</li> <li>3. 执行命令 <code>opaque (enable   disable)</code></li> </ol>	-

#### 4.4.2.2.11 配置 OSPF 接口邻居

##### 目的

本节介绍如何配置 OSPF 接口邻居。

#### 背景信息

如果要通过此命令设置对端路由器的优先级，必须与对端交换机现在的优先级一致才有效。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置 OSPF 接口的邻居及其优先级	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>router ospf</code>，进入 OSPF 配置视图；</li> <li>3. 执行命令 <code>peer ipv4-address priority priority</code></li> </ol>	<p><b>ipv4-address</b>: 点分十进制形式，形如: (A.B.C.D)，其中 A~D 为整数形式，取值范围为 1-255；</p> <p><b>Priority</b>: 表示网络邻居的优先级的相应数值，整数形式，取值范围是 0-255</p>
删除手工配置邻居（接口 NBMA/P2MP 类型）	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>router ospf</code>，进入 OSPF 配置视图；</li> <li>3. 执行命令 <code>no peer ipv4-address</code></li> </ol>	<p><b>ipv4-address</b>: 点分十进制形式，形如: (A.B.C.D)，其中 A~D 为整数形式，取值范围为 1-255</p>

#### 4.4.2.2.12 配置路由计算间隔

##### 目的

本节介绍如何配置路由计算间隔。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置路由计算间隔	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>router ospf</code>，进入 OSPF 配置视图；</li> <li>3. 执行命令 <code>spf-running-interval interval</code> 或 <code>spf-running-interval default</code></li> </ol>	<p><b>Interval</b>: 指定路由计算间隔时间，整数形式，取值范围是 1~60，单位为 ms</p>

#### 4.4.2.2.13 配置 OSPF TTL

##### 目的

本节介绍如何配置 OSPF TTL。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
设置 ospf 有效 ttl 的值	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>router ospf</code>，进入 OSPF 配置视图；</li> <li>3. 执行命令 <code>valid-ttl-hops hop-number</code> 或 <code>valid-ttl-hops default</code></li> </ol>	<b>Hop-number:</b> 设置的跳数，整数形式，取值范围是 1~255

#### 4.4.2.2.14 配置 OSPF 重分配

### 目的

本节介绍如何配置 OSPF 重分配。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置 OSPF 重分配	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>router ospf</code>，进入 OSPF 配置视图；</li> <li>3. 执行命令 <code>redistribute { static   connect   rip   bgp   isis }</code></li> </ol>	参数分别代表配置引入静态路由的路由策略、配置引入直连路由的路由策略、配置引入 rip 协议的路由测量以及配置引入 BGP 路由的路由策略
删除 OSPF 重分配	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>router ospf</code>，进入 OSPF 配置视图；</li> <li>3. 执行命令 <code>no redistribute { static   connect   rip   bgp   isis }</code></li> </ol>	参数分别代表配置引入静态路由的路由策略、配置引入直连路由的路由策略、配置引入 rip 协议的路由测量以及配置引入 BGP 路由的路由策略
删除指定网络的重分配	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>router ospf</code>，进入 OSPF 配置视图；</li> <li>3. 执行命令 <code>no redistribute { static   connect   rip   bgp   isis } dst-address dst-mask</code></li> </ol>	<p><b>Dst-address:</b> 目的地址，点分十进制形式，形如：(A.B.C.D)，其中 A~D 为整数形式，取值范围为 1-255；</p> <p><b>Dst-mask:</b> 目的地址掩码，点分十进制形式，形如：(A.B.C.D)，其中 A~D 为整数形式，取值范围为 1-255</p>



目的	步骤	参数说明
配置重分配路由策略	<ol style="list-style-type: none"> <li>在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>执行命令 <code>router ospf</code>，进入 OSPF 配置视图；</li> <li>执行命令 <code>redistribute { static   connect   rip   bgp   isis } route-policy policy-name</code></li> </ol>	<p><b>Policy-name:</b> 路由策略的名字，字符串，不超过 20 个字节</p>
删除重分配路由策略	<ol style="list-style-type: none"> <li>在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>执行命令 <code>router ospf</code>，进入 OSPF 配置视图；</li> <li>执行命令 <code>no redistribute { static   connect   rip   bgp   isis } route-policy policy-name</code></li> </ol>	<p><b>Policy-name:</b> 路由策略的名字，字符串，不超过 20 个字节</p>
配置重分配开销	<ol style="list-style-type: none"> <li>在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>执行命令 <code>router ospf</code>，进入 OSPF 配置视图；</li> <li>执行命令 <code>redistribute { static   connect   rip   bgp   isis } metric metric type type</code></li> </ol>	<p><b>Metric:</b> 指定路由开销值，整数形式，取值范围是 0~65535；</p> <p><b>Type:</b> 整数形式，取值范围是 1~2</p>
配置重分配指定网络的开销	<ol style="list-style-type: none"> <li>在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>执行命令 <code>router ospf</code>，进入 OSPF 配置视图；</li> <li>执行命令 <code>redistribute { static   connect   rip   bgp   isis } dst-address dst-mask metric metric type type</code></li> </ol>	<p><b>Dst-address:</b> 目的地址，点分十进制形式，形如：(A.B.C.D)，其中 A~D 为整数形式，取值范围为 1-255；</p> <p><b>Dst-mask:</b> 目的地址掩码，点分十进制形式，形如：(A.B.C.D)，其中 A~D 为整数形式，取值范围为 1-255；</p> <p><b>Metric:</b> 指定路由开销值，整数形式，取值范围是 0~65535；</p> <p><b>Type:</b> 整数形式，取值范围是 1~2</p>
配置重分配的 translate 位	<ol style="list-style-type: none"> <li>在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>执行命令 <code>router ospf</code>，进入 OSPF 配置视图；</li> <li>执行命令 <code>redistribute { static   connect   rip   bgp   isis } dst-address dst-mask (translate   no-translate)</code></li> </ol>	<p><b>Dst-address:</b> 目的地址，点分十进制形式，形如：(A.B.C.D)，其中 A~D 为整数形式，取值范围为 1-255；</p> <p><b>Dst-mask:</b> 目的地址掩码，点分十进制形式，形如：(A.B.C.D)，其中 A~D 为整数形式，取值范围为 1-255；</p> <p><b>Translate:</b> 代表生成 NSSA LSA 时，设置 translate bit 位；</p> <p><b>No-translate:</b> 代表生成 NSSA LSA 时，不设置 translate bit 位</p>

目的	步骤	参数说明
配置拒绝特定的外部路由	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图； 2. 执行命令 <code>router ospf</code> ，进入 OSPF 配置视图； 3. 执行命令 <code>redistribute { static   connect   rip   bgp   isis } dst-address dst-mask not-advertise</code>	<code>Not-advertise</code> ：代表拒绝特定的外部路由

#### 4.4.2.2.15 使能 OSPF 上报 trap

##### 目的

本节介绍如何使能 OSPF 上报 trap。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
使能/去使能 OSPF 上报 trap 功能	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图； 2. 执行命令 <code>router ospf</code> ，进入 OSPF 配置视图； 3. 执行命令 <code>snmp-trap (enable   disable)</code>	-
使能/去使能 OSPF 上报 trap 具体功能	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图； 2. 执行命令 <code>router ospf</code> ，进入 OSPF 配置视图； 3. 执行命令 <code>snmp-trap (enable   disable) trap-name (ospffauthfailure   ospfifconfigerror   ospfifrxbadpacket   ospfifstatechange   ospflsdbapproachingoverflow   ospflsdboverflow   ospfmaxagelsa   ospfnbrrestarthelperstatuschange   ospfnbrstatechange   ospfnssatranslatorstatuschange   ospforiginatelsa   ospfrestartstatuschange   ospftxretransmit   ospfvirtifauthfailure   ospfvirtifconfigerror   ospfvirtifrxbadpacket   ospfvirtifstatechange   ospfvirtiftxretransmit   ospfvirtnbrrestarthelperstatuschange   ospfvirtnbrstatechange)</code>	-

#### 4.4.2.2.16 配置 OSPF 开销参考带宽

##### 目的

本节介绍如何配置 OSPF 开销参考带宽。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置 OSPF 开销参考带宽	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>router ospf</code>, 进入 OSPF 配置视图；</li> <li>3. 执行命令 <code>ospf cost-reference-rate bandwidth</code> 或 <code>ospf cost-reference-rate default</code></li> </ol>	Bandwidth: 指定参考速率可选范围，整数形式，取值范围是 1~100000

4.4.2.2.17 配置兼容 RFC1583

目的

本节介绍如何配置兼容 RFC1583。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置兼容 RFC1583	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>router ospf</code>, 进入 OSPF 配置视图；</li> <li>3. 执行命令 <code>rfc1583 compatible (enable   disable)</code></li> </ol>	Enable 表示兼容 RFC1583, disable 表示不兼容 RFC1583

4.4.2.2.18 配置缺省路由通告

目的

本节介绍如何配置缺省路由通告。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置缺省路由通告	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>router ospf</code>, 进入 OSPF 配置视图；</li> <li>3. 执行命令 <code>default-route-advertise always</code></li> </ol>	-
取消缺省路由通告配置	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>router ospf</code>, 进入 OSPF 配置视图；</li> <li>3. 执行命令 <code>no default-route-advertise always</code></li> </ol>	-

#### 4.4.2.2.19 配置区域 TE 使能

##### 目的

本节介绍如何配置区域 TE 使能。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
使能区域 TE	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>router ospf</code>，进入 OSPF 配置视图；</li> <li>3. 执行命令 <code>area area-id te (enable   disable)</code></li> </ol>	<b>area-id:</b> OSPF 区域 ID，点分十进制形式，形如：(A.B.C.D)，其中 A~D 为整数形式，取值范围为 1-255(大于 65535 的区域) 或者整数形式，取值范围为 0-4294967295(小于 65535 的区域)

#### 4.4.2.3 配置 OSPF 端口

##### 4.4.2.3.1 配置 OSPF 接口参数

##### 目的

本节介绍如何配置 OSPF 接口参数。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置 OSPF 接口类型	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>interface vlan vlan-id</code>，进入 VLANIF 配置视图；</li> <li>3. 执行命令 <code>ip ospf if-type&lt;broadcast   nbma   p2p   p2multip &gt;</code></li> </ol>	参数分别表示将接口的网络类型更改为广播、将接口的网络类型更改为 NBMA、将接口的网络类型更改为点到点以及将接口的网络类型更改为点到多点
配置 OSPF 接口优先级	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>interface vlan vlan-id</code>，进入 VLANIF 配置视图；</li> <li>3. 执行命令 <code>ip ospf priority priority</code> 或 <code>ip ospf priority default</code></li> </ol>	<b>Priority:</b> ospf 的接口优先级，整数形式，取值范围是 0~255，单位为每秒字节数

目的	步骤	参数说明
配置 OSPF 接口开销	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>interface vlan <i>vlan-id</i></code>, 进入 VLANIF 配置视图；</li> <li>3. 执行命令 <code>ip ospf cost <i>cost</i></code> 或 <code>ip ospf cost default</code></li> </ol>	<p><b>Cost:</b> 运行 OSPF 协议所需的开销, 整数形式, 取值范围是 0-65535</p>
配置 OSPF 接口 Hello 间隔时间	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>interface vlan <i>vlan-id</i></code>, 进入 VLANIF 配置视图；</li> <li>3. 执行命令 <code>ip ospf hello-interval <i>hello-interval</i></code> 或 <code>ip ospf hello-interval default</code></li> </ol>	<p><b>hello-interval :</b> 配置 OSPF 接口 Hello 间隔时间, 整数形式, 取值范围是 1-65535</p>
配置 OSPF 接口邻居超时时间	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>interface vlan <i>vlan-id</i></code>, 进入 VLANIF 配置视图；</li> <li>3. 执行命令 <code>ip ospf dead-interval <i>dead-interval</i></code> 或 <code>ip ospf dead-interval default</code></li> </ol>	<p><b>dead-interval :</b> 指定 OSPF 接口邻居超时时间, 整数形式, 取值范围是 0-2147483647</p>
配置 OSPF 接口重传间隔	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>interface vlan <i>vlan-id</i></code>, 进入 VLANIF 配置视图；</li> <li>3. 执行命令 <code>ip ospf retransmit-interval <i>retransmit-interval</i></code> 或 <code>ip ospf retransmit-interval default</code></li> </ol>	<p><b>retransmit-interval :</b> 接口重传间隔, 整数形式, 取值范围是 0-3600, 单位为秒</p>
配置 OSPF 接口传输时延	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>interface vlan <i>vlan-id</i></code>, 进入 VLANIF 配置视图；</li> <li>3. 执行命令 <code>ip ospf transmit-delay <i>transmit-delay</i></code> 或 <code>ip ospf transmit-delay default</code></li> </ol>	<p><b>transmit-delay :</b> 接口传输时延, 整数形式, 取值范围是 0~3600, 单位为秒</p>
配置发送轮询报文的时间间隔	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>interface vlan <i>vlan-id</i></code>, 进入 VLANIF 配置视图；</li> <li>3. 执行命令 <code>ip ospf poll-interval <i>poll-interval</i></code> 或 <code>ip ospf poll-interval default</code></li> </ol>	<p><b>poll-interval :</b> 指定 NBMA 网络上邻居路由器发送轮询 Hello 报文的时间间隔, 整数形式, 取值范围是 0-2147483647, 单位为秒</p>
配置接口简单密码认证	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>interface vlan <i>vlan-id</i></code>, 进入 VLANIF</li> </ol>	<p><b>Key:</b> 简单口令认证字, 字符串形式</p>

目的	步骤	参数说明
	配置视图； 3. 执行命令 ip ospf authentication simple-passw ord key	
配置接口 MD5 认证	1. 在特权用户视图下执行命令 configure 进入全局配置视图； 2. 执行命令 interface vlan <i>vlan-id</i> , 进入 VLANIF 配置视图； 3. 执行命令 ip ospf authentication md5 <i>key-id</i> <i>key</i>	Key-id: MD5 密文验证标识符，整数形式，取值范围是 1~255； Key: 简单口令认证字，字符串形式
清除接口认证	1. 在特权用户视图下执行命令 configure 进入全局配置视图； 2. 执行命令 interface vlan <i>vlan-id</i> , 进入 VLANIF 配置视图； 3. 执行命令 no ip ospf authentication	-

#### 4.4.2.3.2 配置 BFD

##### 目的

本节介绍如何配置 BFD。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置 BFD	1. 在特权用户视图下执行命令 configure 进入全局配置视图； 2. 执行命令 interface vlan <i>vlan-id</i> , 进入 VLANIF 配置视图； 3. 执行命令 ip ospf bfd (enable   disable)	Enable 表示在 vlan 接口下使能 BGP 特性，disable 表示在 vlan 接口下去使能 BGP 特性

#### 4.4.2.3.3 配置 fast-change

##### 目的

本节介绍如何配置 fast-change。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置 fast-change	1. 在特权用户视图下执行命令 configure 进入全局配置视图；	Enable 表示配置 ospf 协议快速建立邻居，

目的	步骤	参数说明
	2. 执行命令 <code>interface vlan <i>vlan-id</i></code> , 进入 VLANIF 配置视图; 3. 执行命令 <code>ip ospf fast-change (enable   disable)</code>	<code>disable</code> 表示不配置 ospf 协议快速建立邻居

#### 4.4.2.3.4 配置 OSPF 洪泛组

##### 目的

本节介绍如何配置 OSPF 洪泛组。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置 OSPF 洪泛组	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图; 2. 执行命令 <code>interface vlan <i>vlan-id</i></code> , 进入 VLANIF 配置视图; 3. 执行命令 <code>ip ospf flooding-group <i>flooding-group-name</i></code> 或 <code>ip ospf flooding-group default</code>	<code>flooding-group-name</code> : OSPF 洪泛组名，整数形式，取值范围是 0-64; 非 0 表示 处于同一个 <code>flooding-group</code> 的接口之间不进行 LSA 的扩散; 0 表示恢复正常模式。

#### 4.4.2.3.5 配置 OSPF 接口 MTU

##### 目的

本节介绍如何配置 OSPF 接口 MTU。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置 OSPF 接口 MTU	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图; 2. 执行命令 <code>interface vlan <i>vlan-id</i></code> , 进入 VLANIF 配置视图; 3. 执行命令 <code>ip ospf mtu <i>mtu</i></code> 或 <code>ip ospf mtu default</code>	<code>Mtu: ospf</code> 的接口 MTU 值，整数形式，取值范围是 572-1500
配置 MTU 检测	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图; 2. 执行命令 <code>interface vlan <i>vlan-id</i></code> , 进入 VLANIF 配置视图; 3. 执行命令 <code>ip ospf mtu-ignore (enable  </code>	<code>Enable</code> 表示忽略 MTU 检测, <code>disable</code> 表示不忽略 MTU 检测

目的	步骤	参数说明
	disable)	

#### 4.4.2.3.6 配置 passive 接口

##### 目的

本节介绍如何配置 passive 接口。

##### 背景信息

被动接口是指不收发协议消息的 OSPF 接口，在此接口上不建立任何邻居，但是接口路由将包含在 RouterLSA 中作为内部路由传播。可用于 Stub 路由。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置 passive 接口	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>interface vlan <i>vlan-id</i></code>，进入 VLANIF 配置视图；</li> <li>3. 执行命令 <code>ip ospf passive-interface</code></li> </ol>	-

#### 4.4.2.3.7 配置 OSPF 的 TE

##### 目的

本节介绍如何配置 OSPF 的 TE。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
使能/去使能 TE	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>interface vlan <i>vlan-id</i></code>，进入 VLANIF 配置视图；</li> <li>3. 执行命令 <code>ip ospf te (enable   disable)</code></li> </ol>	-
配置接口的管理组	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>interface vlan <i>vlan-id</i></code>，进入 VLANIF 配置视图；</li> </ol>	Group-name: TE 管理组号，整数形式，取值范围是 0-31



目的	步骤	参数说明
	3. 执行命令 <code>ip ospf te admin-group group-name</code>	
配置 TE 开销	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图; 2. 执行命令 <code>interface vlan vlan-id</code> , 进入 VLANIF 配置视图; 3. 执行命令 <code>ip ospf te cost cost</code>	<b>Cost:</b> 开销范围, 整数取值, 取值范围是 0-65535, 0 代表无开销
配置 OSPF 的 TE 最大带宽	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图; 2. 执行命令 <code>interface vlan vlan-id</code> , 进入 VLANIF 配置视图; 3. 执行命令 <code>ip ospf te max-bandw idth max-bandwidth</code> 或 <code>ip ospf te max-bandw idth default</code>	<b>max-bandw idth:</b> 最大带宽值, 整数形式, 取值范围是 0~4294967295, 单位为每秒字节数
配置 OSPF 的 TE 最大预留带宽	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图; 2. 执行命令 <code>interface vlan vlan-id</code> , 进入 VLANIF 配置视图; 3. 执行命令 <code>ip ospf te max-reserve-bandw idth max-reserve-bandwidth</code> 或 <code>ip ospf te max-reserve-bandw idth default</code>	<b>max-reserve-bandw idth:</b> 最大预留带宽, 整数形式, 取值范围是 0~4294967295, 单位为每秒字节数

#### 4.4.2.4 配置 OSPF 调试功能

##### 目的

本节介绍如何配置 OSPF 调试功能。

##### 过程

根据不同目的, 执行相应步骤, 具体参见下表。

目的	步骤	参数说明
开启全局 debug 信息	1. 进入特权用户视图; 2. 执行命令 <code>debug ospf (global all lsa hello packet neighbor interface ip-route rtm spf syn graceful-restart frr nbrchange)</code>	缺省情况下, 该调试功能是关闭的。
开启具体实例 debug 信息	1. 进入特权用户视图; 2. 执行命令 <code>debug ospf (global all lsa hello packet neighbor interface ip-route rtm spf syn graceful-restart frr nbrchange) process process-id</code>	<b>Process id:</b> SC9600 支持的 OSPF 进程 ID, 取值范围为: 1-2047 缺省情况下, 该调

目的	步骤	参数说明
		试功能是关闭的。
开启所有实例 debug 信息	1. 进入特权用户视图； 2. 执行命令 <code>debug ospf (global all lsa hello packet neighbor interface ip-route rtm spf syn graceful-restart frr nbrchange) process all</code>	缺省情况下，该调试功能是关闭的。
关闭全局 debug 信息	1. 进入特权用户视图； 2. 执行命令 <code>no debug ospf (global all lsa hello packet neighbor interface ip-route rtm spf syn graceful-restart frr nbrchange)</code>	缺省情况下，该调试功能是关闭的。
关闭具体实例 debug 信息	1. 进入特权用户视图； 2. 执行命令 <code>no debug ospf (global all lsa hello packet neighbor interface ip-route rtm spf syn graceful-restart frr nbrchange) process process-id</code>	Process id : SC9600 支持的 OSPF 进程 ID，取值范围为：1-2047 缺省情况下，该调试功能是关闭的。
关闭所有实例 debug 信息	1. 进入特权用户视图； 2. 执行命令 <code>no debug ospf (global all lsa hello packet neighbor interface ip-route rtm spf syn graceful-restart frr nbrchange) process all</code>	缺省情况下，该调试功能是关闭的。

#### 4.4.2.5 查看 OSPF 配置信息

##### 目的

本节介绍如何查看 OSPF 配置信息。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
显示 OSPF 简要信息	1. 进入普通用户视图或特权用户视图； 2. 执行命令 <code>show ip ospf brief</code> <code>show ip ospf brief process &lt;1-2047&gt;</code>	-
显示 OSPF 配置信息	1. 进入普通用户视图或特权用户视图； 2. 执行命令 <code>show ip ospf config</code>	-
显示 OSPF 接口信息	1. 进入普通用户视图或特权用户视图； 2. 执行命令 <code>show ip ospf interface</code>	-

目的	步骤	参数说明
	<pre>show ip ospf interface (A.B.C.D) show ip ospf interface count show ip ospf interface process &lt;1-2047&gt;</pre>	
显示 OSPF 邻居信息	<p>1. 进入普通用户视图或特权用户视图；</p> <p>2. 执行命令</p> <pre>show ip ospf neighbor show ip ospf neighbor (A.B.C.D) show ip ospf neighbor process &lt;1-2047&gt; show ip ospf neighbor state statistic show ip ospf neighbor state count</pre>	-
显示 OSPF 区域信息	<p>1. 进入普通用户视图或特权用户视图；</p> <p>2. 执行命令</p> <pre>show ip ospf area show ip ospf area (A.B.C.D) show ip ospf area &lt;0-4294967295&gt; show ip ospf area process &lt;1-2047&gt;</pre>	-
显示 OSPF 数据库信息	<p>1. 进入普通用户视图或特权用户视图；</p> <p>2. 执行命令</p> <pre>show ip ospf database show ip ospf database process &lt;1-2047&gt; show ip ospf database area area-id show ip ospf database area area-id process &lt;1-2047&gt; show ip ospf database count show ip ospf database count process &lt;1-2047&gt; show ip ospf database total count show ip ospf database expire show ip ospf database expire count show ip ospf database expire process &lt;1-2047&gt; show ip ospf database router show ip ospf database router (A.B.C.D) (A.B.C.D) area-id show ip ospf database router (A.B.C.D) (A.B.C.D) area-id &lt;1-2047&gt; show ip ospf database router process &lt;1-2047&gt; show ip ospf database netw ork show ip ospf database netw ork (A.B.C.D) (A.B.C.D) area-id show ip ospf database netw ork (A.B.C.D) (A.B.C.D) area-id &lt;1-2047&gt; show ip ospf database netw ork process &lt;1-2047&gt; show ip ospf database summary-netw ork</pre>	-

目的	步骤	参数说明
	<pre> show ip ospf database summary-netw ork (A.B.C.D) (A.B.C.D) area-id show ip ospf database summary-netw ork (A.B.C.D) (A.B.C.D) area-id &lt;1-2047&gt; show ip ospf database summary-netw ork process &lt;1-2047&gt; show ip ospf database summary-asbr show ip ospf database summary-asbr (A.B.C.D) (A.B.C.D) area-id show ip ospf database summary-asbr (A.B.C.D) (A.B.C.D) area-id &lt;1-2048&gt; show ip ospf database summary-asbr process &lt;1-2047&gt; show ip ospf database nssa-lsa show ip ospf database nssa-lsa (A.B.C.D) (A.B.C.D) area-id show ip ospf database nssa-lsa (A.B.C.D) (A.B.C.D) area-id &lt;1-2047&gt; show ip ospf database nssa-lsa process &lt;1-2047&gt; show ip ospf database as-external-lsa show ip ospf database as-external-lsa (A.B.C.D) (A.B.C.D) show ip ospf database as-external-lsa (A.B.C.D) (A.B.C.D) &lt;1-2047&gt; show ip ospf database as-external-lsa process &lt;1-2047&gt; show ip ospf database type9 show ip ospf database type9 (A.B.C.D) (A.B.C.D) show ip ospf database type9 (A.B.C.D) (A.B.C.D) &lt;1-2047&gt; show ip ospf database type9 process &lt;1-2047&gt; show ip ospf database type9 show ip ospf database type9 (A.B.C.D) (A.B.C.D) show ip ospf database type9 (A.B.C.D) (A.B.C.D) &lt;1-2047&gt; show ip ospf database type9 process &lt;1-2047&gt; show ip ospf database type10 show ip ospf database type10 (A.B.C.D) (A.B.C.D) area-id show ip ospf database type10 (A.B.C.D) (A.B.C.D) area-id &lt;1-2047&gt; show ip ospf database type10 process &lt;1-2047&gt; show ip ospf database type11                     </pre>	

目的	步骤	参数说明
	<pre>show ip ospf database type11 (A.B.C.D) (A.B.C.D) show ip ospf database type11 (A.B.C.D) (A.B.C.D) &lt;1-2047&gt; show ip ospf database type11 process &lt;1-2047&gt;</pre>	
显示 OSPF 路由信息	<ol style="list-style-type: none"> <li>1. 进入普通用户视图或特权用户视图;</li> <li>2. 执行命令</li> </ol> <pre>show ip ospf route show ip ospf route count show ip ospf route count process &lt;1-2047&gt; show ip ospf route process &lt;1-2047&gt; show ip ospf route total count</pre>	-
显示 OSPF 虚链路信息	<ol style="list-style-type: none"> <li>1. 进入普通用户视图或特权用户视图;</li> <li>2. 执行命令</li> </ol> <pre>show ip ospf virtual interface show ip ospf virtual interface area-id (A.B.C.D) show ip ospf virtual interface process &lt;1-2047&gt; show ip ospf virtual neighbor show ip ospf virtual neighbor process &lt;1-2047&gt;</pre>	-
显示 OSPF BFD 信息	<ol style="list-style-type: none"> <li>1. 进入普通用户视图或特权用户视图;</li> <li>2. 执行命令</li> </ol> <pre>show ip ospf bfd session</pre>	-
显示 OSPF trap 信息	<ol style="list-style-type: none"> <li>1. 进入普通用户视图或特权用户视图;</li> <li>2. 执行命令</li> </ol> <pre>show ip ospf trap</pre>	-
显示 ospf bfd 会话相关信息	<ol style="list-style-type: none"> <li>1. 进入普通用户视图或特权用户视图;</li> <li>2. 执行命令</li> </ol> <pre>show ip ospf bfd session</pre>	-

### 4.4.3 OSPF 配置举例

#### 4.4.3.1 配置 OSPF 基本功能

##### 组网要求

如图 4-11所示，所有的设备都运行 OSPF，并将整个自治系统划分为 3 个区域，其中 SC9600\_1 和 SC9600\_2 为 ABR 来转发区域之间的路由。

配置完成后，每台 router 都应学到自治系统内的到所有网段的路由。

##### 组网图

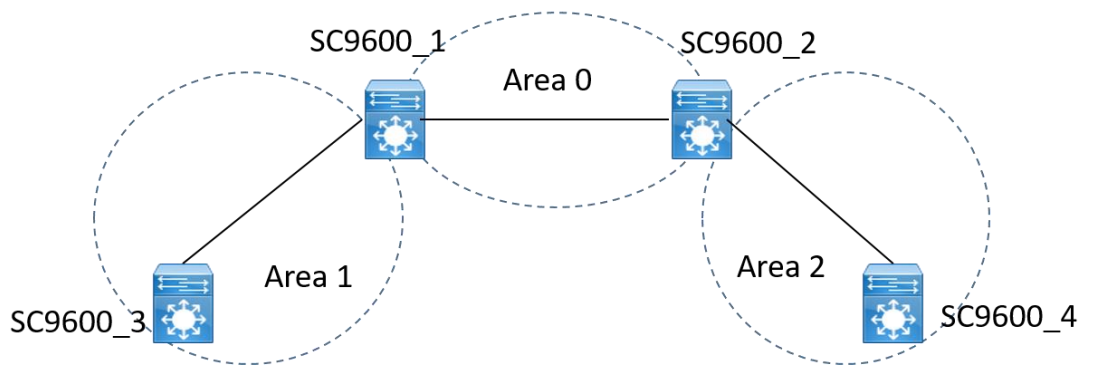


图 4-11 OSPF 基本配置组网图

### 配置步骤

#### 说明

SC9600\_1 的两个接口地址：1.1.1.1/24 和 3.1.1.1/24

SC9600\_2 的两个接口地址：1.1.1.2/24 和 4.1.1.2/24

SC9600\_3 的两个接口地址：3.1.1.3/24

SC9600\_4 的两个接口地址：4.1.1.4/24

SC9600\_1:

```
SC9600_1(config)#router ospf
```

```
SC9600_1(config-ospf-1)#router-id 1.1.1.1
```

```
SC9600_1(config-ospf-1)#network 1.1.1.0 255.255.255.0 area 0
```

```
SC9600_1(config-ospf-1)#network 3.1.1.0 255.255.255.0 area 1
```

```
SC9600_1(config)#
```

SC9600\_2:

```
SC9600_2(config)#router ospf
```

```
SC9600_2(config-ospf-1)#router-id 1.1.1.2
```

```
SC9600_2(config-ospf-1)#network 1.1.1.0 255.255.255.0 area 0
```

```
SC9600_2(config-ospf-1)#network 4.1.1.0 255.255.255.0 area 2
```

```
SC9600_2(config)#
```

SC9600\_3:

```
SC9600_3(config)#router ospf
```

```
SC9600_3(config-ospf-1)#router-id 3.1.1.3
```

```
SC9600_3(config-ospf-1)#network 3.1.1.0 255.255.255.0 area 1
```

```
SC9600_3(config)#
```

SC9600\_4:

```
SC9600_4(config)#router ospf
SC9600_4(config-ospf-1)#router-id 4.1.1.4
SC9600_4(config-ospf-1)#network 4.1.1.0 255.255.255.0 area 2
SC9600_4(config)#
```

### 验证配置结果

使用 show ip ospf neighbor 命令可看到 OSPF 的信息如下:

OSPF Process 1

IpAddress	NeighborID	Option	Priority	State	Event	Aging
1.1.1.2	1.1.1.2	2	1	full	6	39
3.1.1.3	3.1.1.3	2	1	full	6	30

使用 show ip ospf database 命令可看到 OSPF 的信息如下:

Database of OSPF Process 1

#### Router LSA (area 0)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
1.1.1.1	1.1.1.1	146	0x80000003	0xdbff	36
1.1.1.2	1.1.1.2	147	0x80000003	0xd9fe	36

#### Network LSA (area 0)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
1.1.1.2	1.1.1.2	147	0x80000001	0x83c3	32

#### SummaryNetwork LSA (area 0)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
3.1.1.0	1.1.1.1	146	0x80000002	0xf8f5	28
4.1.1.0	1.1.1.2	138	0x80000001	0xe706	28

#### Router LSA (area 1)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
1.1.1.1	1.1.1.1	147	0x80000002	0xccb	36
3.1.1.3	3.1.1.3	139	0x80000004	0xd66c	48

#### Network LSA (area 1)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
3.1.1.3	3.1.1.3	147	0x80000001	0x5fde	32

#### SummaryNetwork LSA (area 1)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
1.1.1.0	1.1.1.1	187	0x80000001	0x15dc	28
4.1.1.0	1.1.1.1	136	0x80000002	0xd7b1	28

使用 show ip ospf route 命令可看到 OSPF 的信息如下:

OSPF Instance 1

Dest	Mask	Nexthop	Type	PathType	Areaid
1.1.1.2	255.255.255.255	1.1.1.2	ABR	INTRA	0
1.1.1.0	255.255.255.0	1.1.1.1	Netw ork	INTRA	
3.1.1.0	255.255.255.0	3.1.1.1	Netw ork	INTRA	
4.1.1.0	255.255.255.0	1.1.1.2	Netw ork	INTER	

#### 4.4.3.2 配置 OSPF 的 Stub 区域

##### 组网要求

如图 4-12所示，所有的设备都运行 OSPF，并将整个自治系统划分为 3 个区域，其中 SC9600\_1 和 SC9600\_2 为 ABR 来转发区域之间的路由。

配置完成后，每台设备都应学到自治系统内的到所有网段的路由。

##### 组网图

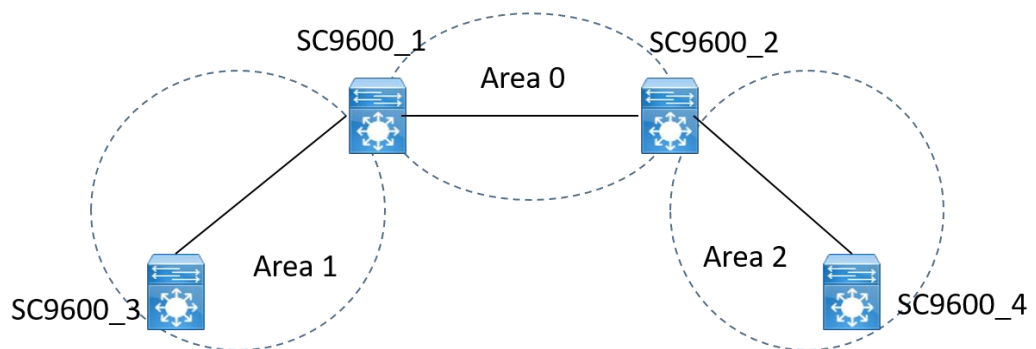


图 4-12 OSPF Stub 区域组网图

##### 配置步骤

基本配置和拓扑同4.4.3.1 配置 OSPF 基本功能。

配置 area 1 为 stub:

```

SC9600_1:
SC9600_1(config)#router ospf
SC9600_1(config-ospf-1)#area 1 stub
SC9600_1(config)#
SC9600_3:
SC9600_3(config)#router ospf
SC9600_3(config-ospf-1)# area 1 stub
SC9600_3(config)#
    
```



在 SC9600\_4 引入 100.1.1.1 的 5 类 LSA

### 验证配置结果

1. 当 SC9600\_3 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。变成 stub 区域后，比正常区域多一个缺省的 3 类 LSA，看不到 AS 外部的 LSA。

SC9600\_3# show ip ospf route

```
OSPF Instance 0
```

Dest	Mask	Nexthop	Type	PathType	Areaid
1.1.1.1	255.255.255.255	3.1.1.1	ABR	INTRA	1
1.1.1.0	255.255.255.0	3.1.1.1	Netw ork	INTER	
3.1.1.0	255.255.255.0	3.1.1.3	Netw ork	INTRA	
4.1.1.0	255.255.255.0	3.1.1.1	Netw ork	INTER	
100.1.1.0	255.255.255.0	1.1.1.2	Netw ork	ASE	

2. 当 SC9600\_3 所在区域配置为 Stub 区域时，已经看不到 AS 外部的路由，取而代之的是一条通往区域外部的缺省路由。

SC9600\_3# show ip ospf route

```
OSPF Instance 0
```

Dest	Mask	Nexthop	Type	PathType	Areaid
1.1.1.1	255.255.255.255	3.1.1.1	ABR	INTRA	1
0.0.0.0	0.0.0.0	3.1.1.1	Netw ork	INTER	
1.1.1.0	255.255.255.0	3.1.1.1	Netw ork	INTER	
3.1.1.0	255.255.255.0	3.1.1.3	Netw ork	INTRA	
4.1.1.0	255.255.255.0	3.1.1.1	Netw ork	INTER	

#### 4.4.3.3 配置 OSPF 的 NSSA 区域

### 组网要求

如图 4-13所示，所有的设备都运行 OSPF，并将整个自治系统划分为 3 个区域，其中 SC9600\_1 和 SC9600\_2 为 ABR 来转发区域之间的路由。

配置完成后，每台设备都应学到自治系统内的到所有网段的路由。

### 组网图

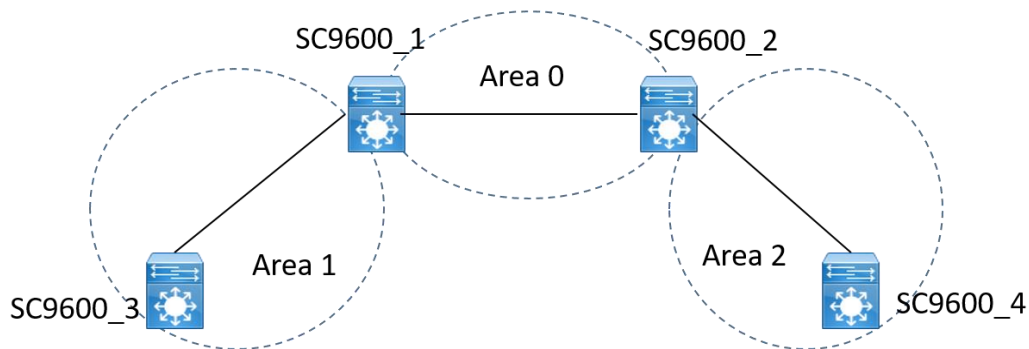


图 4-13 OSPF nssa 区域组网图

### 配置步骤

基本配置和拓扑同4.4.3.1 配置 OSPF 基本功能。

配置 area 1 为 nssa:

SC9600\_1:

```
SC9600_1(config)#router ospf
SC9600_1(config-ospf-1)#area 1 nssa
SC9600_1(config)#
```

SC9600\_3:

```
SC9600_3(config)#router ospf
SC9600_3(config-ospf-1)# area 1 nssa
SC9600_3(config)#
```

### 验证配置结果

1. nssa 区域的数据库比正常区域的数据库多一个缺省 NSSA 类型 LSA

SC9600\_3(config-ospf-1)#show ip ospf database

Database of OSPF Process 1

Router LSA (area 1)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
1.1.1.1	1.1.1.1	134	0x80000002	0x9934	36
3.1.1.3	3.1.1.3	133	0x80000002	0x6066	36

Netw ork LSA (area 1)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
3.1.1.3	3.1.1.3	133	0x80000001	0xe64f	32

SummaryNetw ork LSA (area 1)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
1.1.1.0	1.1.1.1	178	0x80000001	0x9c4d	28

4.1.1.0            1.1.1.1            178    0x80000001    0x6121    28

NSSA LSA (area 1)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
0.0.0.0	1.1.1.1	178	0x80000001	0xc608	36

2. 在 SC9600\_3 引入 100.1.1.1 的静态路由 ip route-static 100.1.1.0 255.255.255.0 3.1.1.1, 重分配静态路由,

数据库:

NSSA LSA (area 1)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
0.0.0.0	1.1.1.1	374	0x80000001	0x7550	36
100.1.1.0	3.1.1.3	0	0x80000001	0x70c4	36

ASExternal LSA

LinkId	ADV Router	Age	Seq#	CheckSum	Len
100.1.1.0	3.1.1.3	1	0x80000001	0xe656	36

路由:

SC9600\_3# show ip ospf route

OSPF Instance 0

Dest	Mask	Nexthop	Type	PathType	AreaId
1.1.1.1	255.255.255.255	3.1.1.1	ABR	INTRA	1
1.1.1.1	255.255.255.255	3.1.1.1	ASBR	INTRA	1
0.0.0.0	0.0.0.0	3.1.1.1	Network	ASE2	
1.1.1.0	255.255.255.0	3.1.1.1	Network	INTER	
3.1.1.0	255.255.255.0	3.1.1.3	Network	INTRA	
4.1.1.0	255.255.255.0	3.1.1.1	Network	INTER	

在 SC9600\_4 上查看

数据库:

SC9600\_4#

ASExternal LSA

LinkId	ADV Router	Age	Seq#	CheckSum	Len
100.1.1.0	1.1.1.1	412	0x80000001	0x4701	36

路由：

SC9600\_4# show ip ospf route

OSPF Instance 0

Dest	Mask	Nexthop	Type	PathType	Areaid
1.1.1.2	255.255.255.255	4.1.1.2	ABR	INTRA	2
1.1.1.0	255.255.255.0	4.1.1.2	Netw ork	INTER	
3.1.1.0	255.255.255.0	4.1.1.2	Netw ork	INTER	
4.1.1.0	255.255.255.0	4.1.1.4	Netw ork	INTRA	
100.1.1.0	255.255.255.0	4.1.1.2	Netw ork	ASE	

3. 在 SC9600\_4 引入 200.1.1.1 的静态路由，查看 SC9600\_3 是否拥有外部路由

在 SC9600\_4 查看数据库

ASExternal LSA

Linkld	ADV Router	Age	Seq#	CheckSum	Len
100.1.1.0	1.1.1.1	823	0x80000001	0x4701	36
200.1.1.0	4.1.1.4	4	0x80000001	0xb933	36

在 SC9600\_3 查看数据库

SC9600\_3

ASExternal LSA

Linkld	ADV Router	Age	Seq#	CheckSum	Len
100.1.1.0	3.1.1.3	836	0x80000001	0xe656	36

没有 200.1.1.0 的外部路由

#### 4.4.3.4 配置重分配

##### 组网要求

如图 4-14所示，2 个设备都运行 OSPF，并将所有都配置为区域 0。假定 SC9600\_1 需要向 OSPF 导入外部路由，但是对外部路由有如下要求：

- 1 接受所有直连路由，并采用默认配置；
- 2 接收所有静态路由，并为路由配置开销 2000，类型 2；10.1.1.0/24 的静态路由开销为 100；
- 3 拒绝 20.1.1.0/24 的 RIP 路由，并对属于 30.1.0.0/16 的 RIP 路由进行聚合；

配置完成后，每台设备都应学到自治系统内的到所有网段的路由。

### 组网图

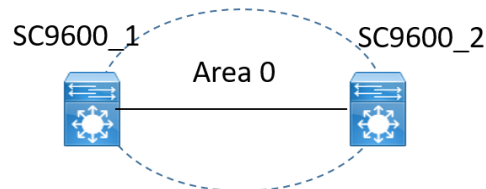


图 4-14 OSPF 重分配组网图

### 配置步骤

#### 1. 基本配置

SC9600\_1:

```
SC9600_1(config)#router ospf
SC9600_1(config-ospf-1)#router-id 1.1.1.1
SC9600_1(config-ospf-1)#network 1.1.1.0 255.255.255.0 area 0
SC9600_1(config-ospf-1)#network 3.1.1.0 255.255.255.0 area 1
SC9600_1(config)#
```

SC9600\_2:

```
SC9600_2(config)#router ospf
SC9600_2(config-ospf-1)#router-id 1.1.1.2
SC9600_2(config-ospf-1)#network 1.1.1.0 255.255.255.0 area 0
SC9600_2(config-ospf-1)#network 4.1.1.0 255.255.255.0 area 2
SC9600_2(config)#
```

#### 2. 重分配配置

```
SC9600_2(config-ospf-1)#redistribute connected
SC9600_2(config-ospf-1)#redistribute static metric 2000 type 2
SC9600_2(config-ospf-1)#redistribute static 10.1.1.0 255.255.255.0 100 2
SC9600_2(config-ospf-1)#redistribute static
SC9600_2(config-ospf-1)#redistribute rip 20.1.1.0 255.255.255.0 not-advertise
SC9600_2(config-ospf-1)#redistribute rip 30.1.0.0 255.255.0.0 1000 2 summary-only
SC9600_2(config-ospf-1)#redistribute rip
```

### 验证配置结果

执行上述配置后，可以观察 A 的数据库，检查导入的外部 LSA 是否满足要求。

### 4.4.3.5 配置聚合

#### 组网要求

如图 4-15，网络要求：

- 区域 1 中存在 10.1.1.0/24,10.1.2.0/24,20.1.1.0/24,20.1.2.0/24 的区域内路由，希望将 10.1.1.0/24 和 10.1.2.0/24 聚合为 10.1.0.0/16 通告；而希望 20.1.1.0/24 和 20.1.2.0/24 不导入其他区域。
- 区域 2 的设备能力较差，不能接受大量外部路由，但是具有 30.1.1.0/24 的外部路由，希望将此路由通告给其他区域。
- 区域 3 与区域 2 相似，但是没有需要通告的外部路由

根据上述要求，我们可以为区域 1 配置聚合条目和过滤条目，为区域 2 配置 NSSA 属性，为区域 3 配置 Stub 属性。

#### 组网图

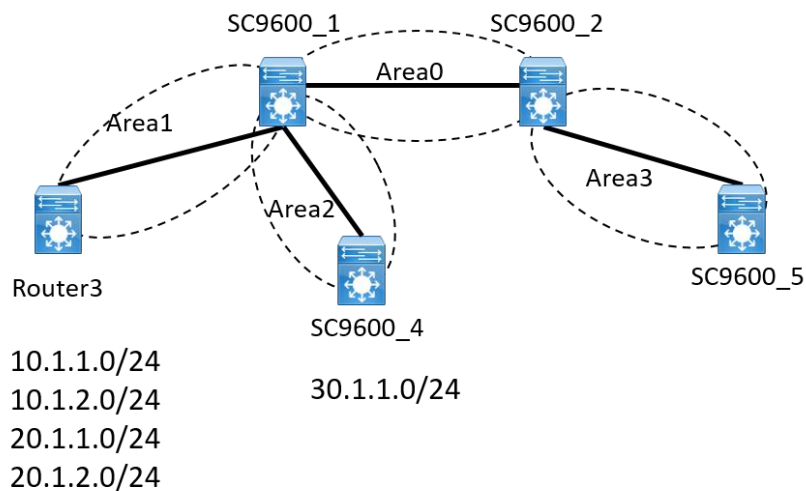


图 4-15 OSPF 聚合组网图

#### 配置步骤

OSPF 基本配置见4.4.3.1 配置 OSPF 基本功能节。

SC9600\_1:

```
SC9600_1(config-ospf-1)#area 1 range 10.1.0.0 255.255.0.0 advertise
```

```
SC9600_1(config-ospf-1)#area 1 range 20.1.0.0 255.255.0.0 no-advertise
```

```
SC9600_1(config-ospf-1)#area 2 nssa//区域 2 的路由器均需要此配置
```

SC9600\_2:

```
SC9600_2(config-ospf-1)#area 2 stub
```

或

```
SC9600_2(config-ospf-1)#area 2 stub no-summary
```

### 验证配置结果

以上配置完成后，可检查数据库来判断：

- 1 区域 0 中包含 10.1.0.0/16 的 SummaryLSA
- 2 区域 0 中不包含 10.1.1.0,10.1.2.0,20.1.1.0.20.1.2.0 的 SummaryLSA
- 3 区域 0 中包含 30.1.1.0/16 的 5 类 LSA
- 4 区域 2 中包含 30.1.1.0/16 的 7 类 LSA
- 5 区域 2 中包含 0.0.0.0/0 的 LSA
- 6 区域 3 中包含 0.0.0.0/0 的 Summary LSA

7 如果区域 3 不指定 nosummary，则区域 3 中包含 10.1.0.0/16 的 SummaryLSA，否则不包含。

### 组网要求

如图 4-16所示，SC9600\_1 连接区域 0 和区域 1；SC9600\_4 连接区域 1 和区域 2。

在正常情况下，区域 0 内无法学习到区域 2 的内部路由；区域 2 也无法学习到区域 0 的内部路由和其他区域的路由。此时需要在 A 和 C 间配置虚链路。

### 组网图

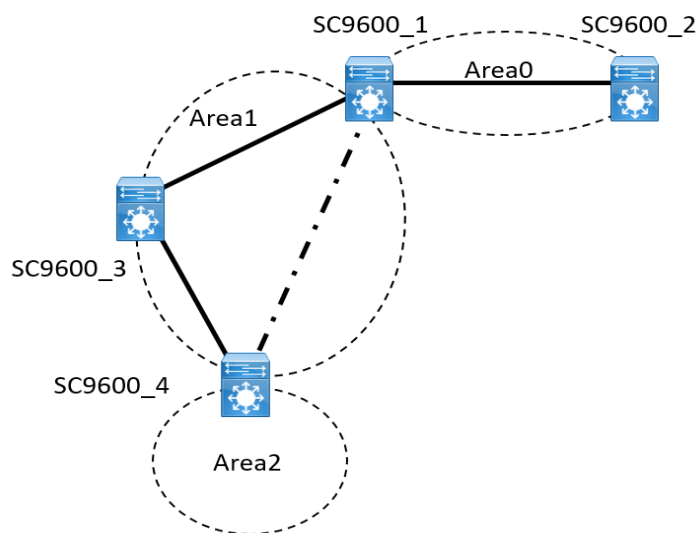


图 4-16 OSPF 虚接口组网图

### 配置步骤

注意，必须先配置虚链路 `area 1 virtual-link (A.B.C.D)` 以后，才能进行虚链路的认证，虚链路的接口属性配置，如 `area 1 virtual-link (A.B.C.D) hello-interval` 等。

#### 1. 虚接口基本配置

SC9600\_1:

```
SC9600_1(config)#router ospf
```

```
SC9600_1(config-ospf-1)#area 1 virtual-link 1.1.1.2
```

SC9600\_4:

```
SC9600_4(config)#router ospf
```

```
SC9600_4(config-ospf-1)#area 1 virtual-link 1.1.1.1
```

#### 2. 虚接口其他配置

这里的配置都是在配了步骤 2 的虚接口基本配置后，才能进行配置

SC9600\_1:

```
SC9600_1(config)#router ospf
```

```
SC9600_1(config-ospf-1)#area 1 virtual-link 1.1.1.2 authentication md5 aaa 100
```

```
SC9600_1(config-ospf-1)#area 1 virtual-link 1.1.1.2 hello-interval 15
```

```
SC9600_1(config-ospf-1)#area 1 virtual-link 1.1.1.2 dead-interval 60
```

```
SC9600_1(config-ospf-1)#area 1 virtual-link 1.1.1.2 retransmit-interval 10
```

SC9600\_4:

```
SC9600_4(config)#router ospf
```

```
SC9600_4(config-ospf-1)#area 1 virtual-link 1.1.1.1 authentication md5 aaa 100
```

```
SC9600_4(config-ospf-1)#area 1 virtual-link 1.1.1.1 hello-interval 15
```

```
SC9600_4(config-ospf-1)#area 1 virtual-link 1.1.1.1 dead-interval 60
```

```
SC9600_4(config-ospf-1)#area 1 virtual-link 1.1.1.1 retransmit-interval 10
```

### 验证配置结果

SC9600\_1 和 SC9600\_4 是否建立链路

#### 4.4.3.6 配置认证模式

### 组网要求

如图 4-17，配置要求：

1 SC9600\_1 与 SC9600\_2 间采用简单密码认证，密码为 test

2 SC9600\_1 与 SC9600\_4 建立虚链路，采用 MD5 认证，密码为 aaa, ID 为 100

3 SC9600\_2 与 SC9600\_3 采用 MD5 认证，密码为 ccc，ID 为 110



组网图

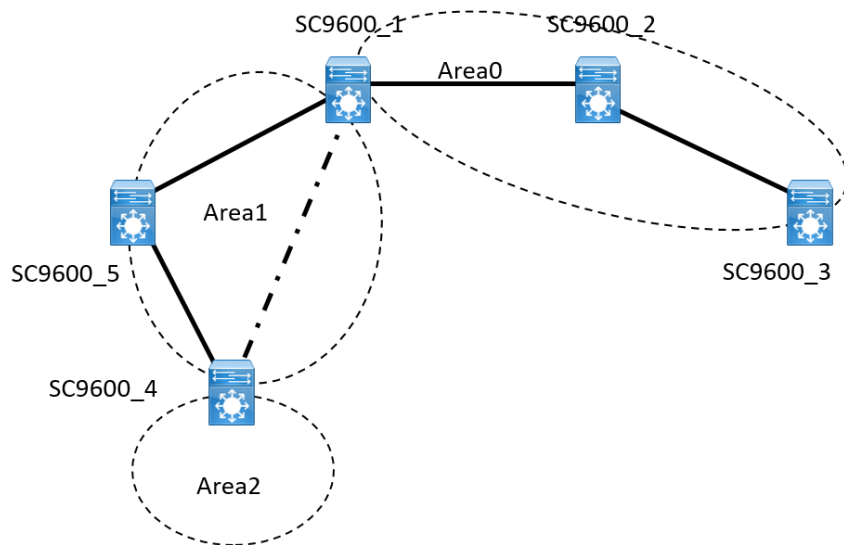


图 4-17 OSPF 认证模式组网图

配置步骤

OSPF 基本配置见4.4.3.1 配置 OSPF 基本功能节。

SC9600\_1:

```
SC9600_1(config)#interface vlan 1
```

```
SC9600_1(config-vlan-1)#ip ospf authentication simple-password test
```

```
SC9600_1(config-vlan-1)#exit
```

```
SC9600_1(config)#router ospf
```

```
SC9600_1(config-ospf-1)#area 1 virtual-link 1.1.1.2 authentication md5 aaa 100
```

SC9600\_2:

```
SC9600_2(config)#interface vlan 1
```

```
SC9600_2(config-vlan-1)#ip ospf authentication simple-password test
```

```
SC9600_2(config-vlan-1)#exit
```

```
SC9600_2(config)#interface vlan 2
```

```
SC9600_2(config-vlan-1)#ip ospf authentication md5 110 ccc
```

```
SC9600_2(config-vlan-1)#exit
```

SC9600\_3:

```
SC9600_3(config-vlan-1)#router ospf
```

```
SC9600_3(config-ospf-1)#area 0 authentication md5 110 ccc
```

SC9600\_4:

```
SC9600_4(config)#router ospf
```

```
SC9600_4(config-ospf-1)#area 1 virtual-link 1.1.1.1 authentication md5 aaa 100
```

#### 验证配置结果

配置之后，检查邻居关系正常。

#### 4.4.3.7 配置 BFD

##### 组网要求

如

图 4-18所示，2 个设备都运行 OSPF，并将所有都配置为区域 0。

##### 组网图

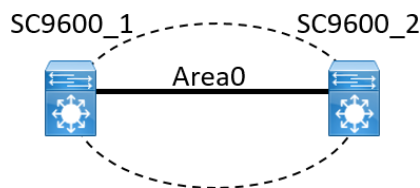


图 4-18 OSPF BFD 组网图

##### 配置步骤

1. OSPF 基本配置见4.4.3.1 配置 OSPF 基本功能节。
2. BFD 配置

SC9600\_1:

```
SC9600_1(config)#interface vlan 4
```

```
SC9600_1(config-vlan-4)#bfd enable
```

```
SC9600_1(config-vlan-4)#ip ospf bfd enable
```

```

SC9600_2:

SC9600_2(config)#interface vlan 4

SC9600_2(config-vlan-4)#bfd enable

SC9600_2(config-vlan-4)#ip ospf bfd enable
    
```

#### 验证配置结果

```

SC9600_1(config-vlan-4)#sho ip ospf bfd session
OSPF Process 1
NeighborAddress      NeighborID           BFDState
1.1.1.2              1.1.1.2             UP
SC9600_2(config-vlan-4)#sho ip ospf bfd session
OSPF Process 1
NeighborAddress      NeighborID           BFDState
1.1.1.1              1.1.1.1             UP
    
```

### 4.4.3.8 配置 GR

#### 组网要求

如图 4-19所示，2 个设备都运行 OSPF，并将有个都配置为区域 0。

测试 GR 重启需要 2 台设备，一台为 GR 重启者，一台为 GR 帮助者。GR 测试重启者采用双主控，拔插卡的方式测试。帮助者无限制。

#### 组网图

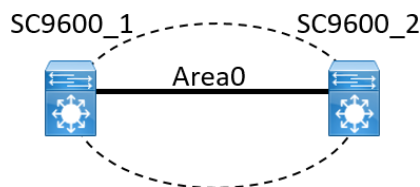


图 4-19 OSPF GR 组网图

#### 配置步骤

1. OSPF 基本配置见4.4.3.1 配置 OSPF 基本功能节。
2. GR 配置

```

SC9600_1:

SC9600_1(config)#router ospf
    
```

```
SC9600_1(config-ospf-1)# graceful-restart
SC9600_1(config-ospf-1)# graceful-restart period 60
SC9600_2:
SC9600_2(config)#router ospf
SC9600_2(config-ospf-1)# graceful-restart helper
```

#### 验证配置结果

采用插拔卡进行测试，GR 重启者和 GR 帮助者上的配置以后，将 GR 重启者的主用主控拔掉，这时设备间原有的流量应不发生中断。

## 4.5 IPv6 OSPFv3 配置

### 4.5.1 OSPFv3 简介

#### 4.5.1.1 OSPFv3 基本概念

OSPFv3 协议在一个自治系统内部运行。为了减小路由信息的数量，在 OSPFv3 中，将一个 AS 划分为不同的区域(Area)，每一个区域由一个区域 ID(Area-ID)进行标识，在这里，我们规定区域 ID 采用 IPv4 地址格式。

图 4-20 给出了一个区域划分的例子。

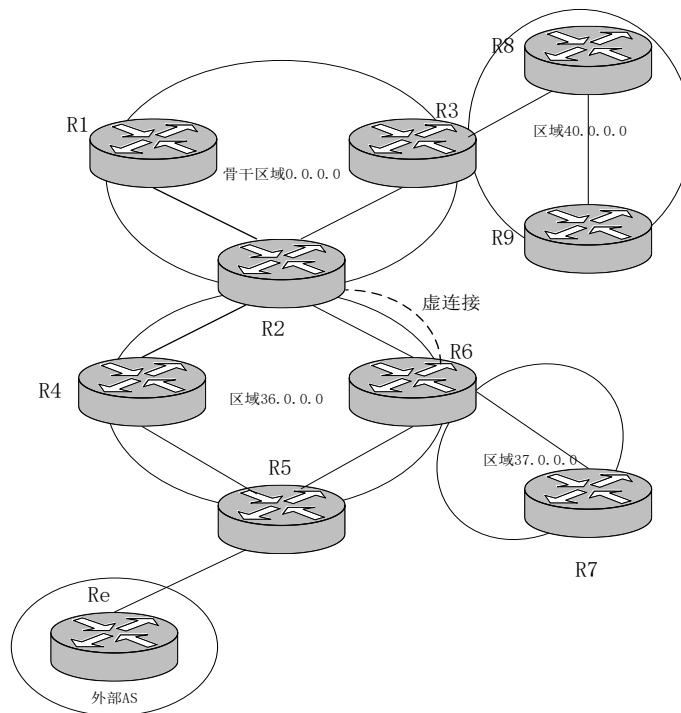


图 4-20 OSPFv3 区域划分

在

图 4-20中，一个 AS 被划分为 4 个区域，R1，R2 和 R3 的部分接口属于骨干区域 0.0.0.0，R2，R4，R5，R6 的部分接口属于区域 36.0.0.0，R6 和 R7 部分接口属于区域 37.0.0.0，而 R3，R8 和 R9 则组成了区域 40.0.0.0。

在 OSPFv3 中，区域 0.0.0.0(即区域 ID 为 0.0.0.0 的区域，以下同)是一个很特殊的区域，被称为骨干区域(Backbone Area)。为了 OSPFv3 协议正常工作，骨干区域必须是连续的，一旦骨干区域被隔离（如骨干区域中的某些链路故障导致不连续），则路由计算不能正常进行。其他的区域必须和骨干区域相连。如

图 4-20中的区域 36.0.0.0 和区域 40.0.0.0，分别通过 R2 和 R3 与骨干区域连接。这样，我们看到，R2 和 R3 都分别连接了两个区域，在 OSPFv3 中，连接两个或者更多区域的路由器被称为区域边界路由器(ABR)。

图 4-20中我们还可以看到，路由器 R6 连接了区域 36.0.0.0 和区域 37.0.0.0，因此它也是一个区域边界路由器，但是此时区域 37.0.0.0 并没有和骨干区域连接，这样会造成路由的丢失。为解决这个问题，OSPFv3 提出了虚链路的概念(virtual link)，虚链路在两个路由器之间指定，它属于骨干区域。

图 4-20中，可以看到，在 R2 和 R6 之间建立了一条虚链路，这样，R6 实际上连接了三个区域，即区域 36.0.0.0，区域 37.0.0.0，骨干区域，这样，区域 37.0.0.0 和骨干区域就建立了连接。因为这一条虚链路是通过区域 36.0.0.0 建立的，此时将区域 36.0.0.0 称为虚链路的透传区域(transit area)。

图 4-20中我们还可以看到，区域 37.0.0.0 与骨干区域的连接只有一条链路，而区域 36.0.0.0 则有两条。在 OSPFv3 中，与骨干区域只有一条连接的区域可以被配置为残桩区域(stub area)，配置残桩区域的目的是减少路由信息的数量。但是还需要注意的是，即使区域 36.0.0.0 与骨干区域只有一条链路连接，它也不能被配置为残桩区域，因为此时区域 36.0.0.0 已经作为一条虚链路的透传区域，而残桩区域是不能够作为透传区域的。

由于 OSPFv3 运行在一个自治系统内部，因此涉及到与其他 AS 的路由交换。

图 4-20中，R5 与其他 AS 的路由器有连接，此时，R5 被称为自治系统边界路由器(ASBR)。与其他自治系统的路由交互大部分情况是通过 BGP 进行的。

OSPFv3 中的每一个路由器都具有一个路由器 ID(Router ID)，这个路由器 ID 唯一标识这个路由器。路由器 ID 是 IPv4 地址格式的，由用户自行指定，0.0.0.0 作为预留，不能使用。

在 OSPFv3 中，存在邻居(Neighbor)和邻接(Adjacency)的概念。邻居是指路由器通过某一个接口可以直接到达的路由器，而邻接则是 OSPFv3 协议中能够交换协议消息的逻辑实体。对于点到点链路(包括虚链路)而言，链路的另一端只有一个邻居，因此也只有一个邻接。但是对于以太网这样的广播链路而言，情况不是这样，一条链路上可能连接多个路由器，为了减少路由信息，OSPFv3 定义了指定路由器(DR)和备份指定路由器(BDR)，所有路由器只能够与 DR 和 BDR 建立邻接关系，而网络的路由信息则由 DR 负责通告，BDR 用于 DR 失效的情况下取代原有的 DR。图 4-21给出了一个例子，图中，4 个路由器在以太网链路上形成邻居，其中 R1 为 DR，R2 为 BDR，图中的虚线表示实际形成的邻接关系，可以看到，R3 和 R4 之间并没有形成邻接关系。OSPFv3 中的 DR 和 BDR 由协议过程自动选择，作为操作者，如果希望某一个接口成为 DR，则可以人为规定此接口的 DR 优先级。

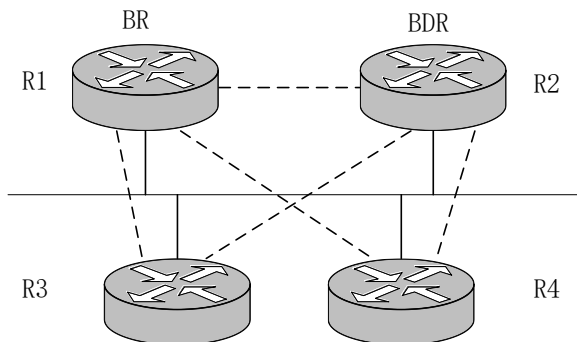


图 4-21 以太网链路上的邻接关系

#### 4.5.1.2 路由信息扩散

OSPFv3 的工作基本上划分为邻接建立过程和随后的触发更新过程。OSPFv3 使用 5 种类型的协议消息来完成协议功能。这些消息是：Hello 消息，DDP 消息，LSR 消息，LACK 消息和 LSU 消息。Hello 消息的作用是检测邻居的状态，以及协商邻接建立参数，以及 DR 和 BDR 的选择。DDP 消息用于 OSPFv3 邻接建立过程中，路由器将自己维护的路由信息的摘要信息置于 DDP 消息中发送给邻居，邻居比较 DDP 消息中的路由信息和自己维护的路由信息，以决定需要向邻居请求哪些路由信息。一旦邻居做了这样的决定，邻居就可以发送 LSR 消息来请求相应的路由信息，收到这样的请求，路由器将发送 LSU 消息通告详细的路由信息。LACK 消息则用于 LSU 消息的确认，因为路由协议基于 IP 这个不保证到达的协议，因此确认是必要的。LSU 消息和 LACK 消息还出现在邻接建立之后的路由变化通告当中。图 4-22 显示了以上所述过程。

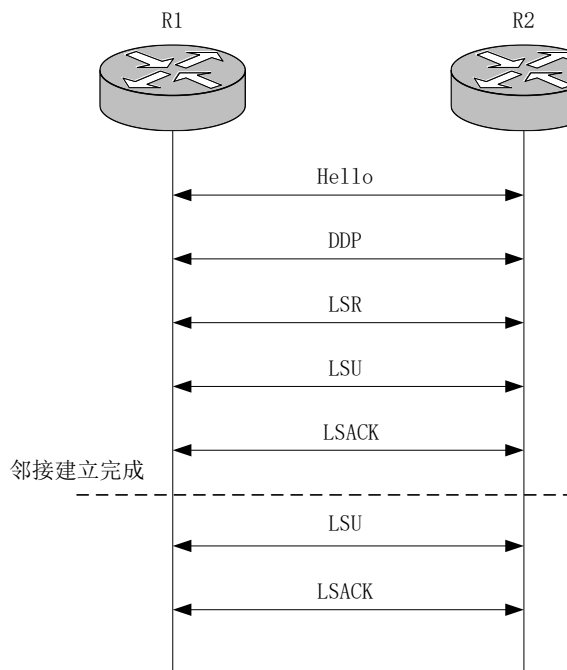


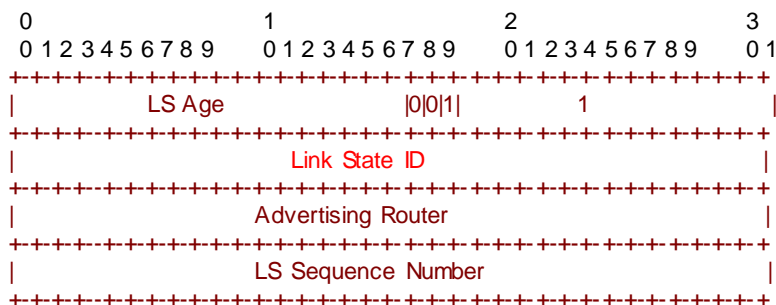
图 4-22 OSPFv3 协议工作过程

除了 Hello 消息之外，其余的 OSPFv3 消息都和路由信息有关，在 OSPFv3 中，承载路由信息的信息单元称为链路状态通告(LSA)。基本的 LSA 有 7 类，即路由器 LSA，网络 LSA，域内前缀 LSA、域内路由器 LSA、外部 LSA、链路状态 LSA、域间前缀 LSA。这些 LSA 具有不同的涵义，从而可以灵活地进行路由计算。这些 LSA 中，外部 LSA 是针对整个自治系统而言的，它不属于任何区域，而其他的 LSA 则都属于特定的区域。一旦 LSA 的扩散过程完成，则路由器可以进行路由计算，从而最终形成路由转发表中的条目。

### 4.5.1.3 OSPFv3 LSA 类型

#### Router-LSAs

Router-LSA 帧格式如图 4-23所示：





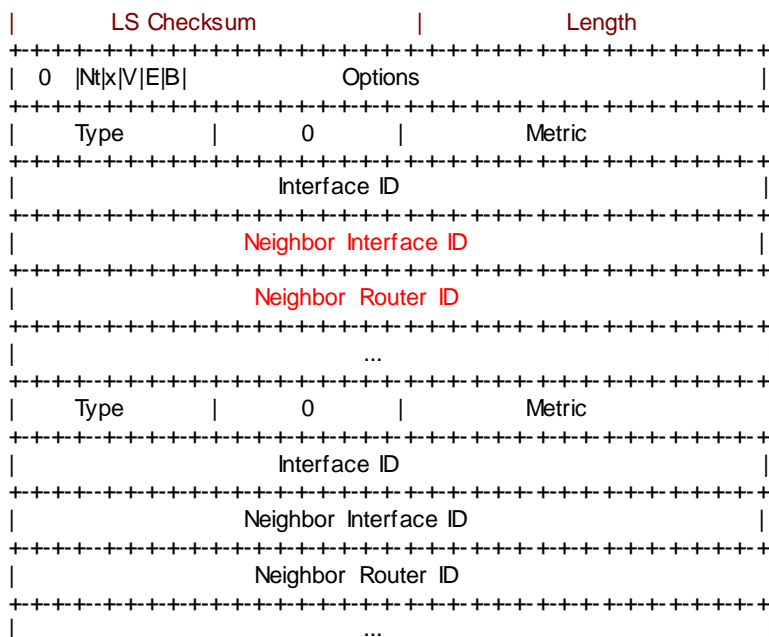


图 4-23 Router-LSA 帧格式

与 OSPFv2 不同的地方在于：

1. LSID 字段的意义。ospfv3 中考虑了分片的处理，路由器可以为一个区域生成一个或多个 RouterLSA，LSID 用来区分生成的多个 router-LSA。这样可以避免 ospfv2 中由于区域中的接口太多而产生大包，导致底层 ip 分片；

一个 routerLSA 可以包含的链路个数可以设计为(接口 MTU—IP 头部长度 40—LSA 头部长度 16—routerLSA 头部长度 24) / 每个 LINK 长度 16 = (1500—40—20—24) / 16=88 个；

这里假定接口 MTU 为 1500；

2. 处于 DOWN，Loopback 状态的接口不包含在 RouterLSA 中，没有 FULL 邻接的接口也不包含在 RouterLSA 中。OSPFv3 要求只有 FULL 邻接的接口才能包含在 Router LSA 中，ospfv2 没有此限制；
3. 对于广播和 NBMA 类型的链路，增加 transit 类型的 link 到 router LSA 时，LINK 中的字段：邻居接口 ID 设置为 DR 的的接口 ID，邻居 RouterID 设置为 DR 的路由器 ID。

### Network-LSAs

Network-LSA 帧格式如图 4-24所示（通告的开销为 0）：

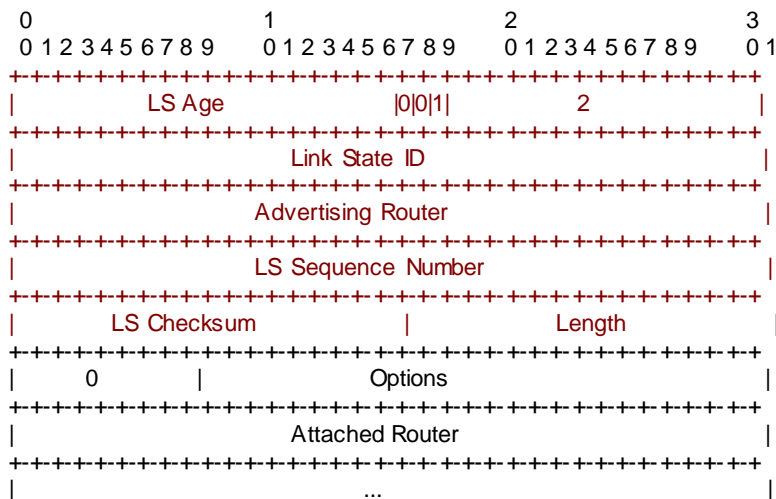


图 4-24 Network-LSA 帧格式

Network LSA 生成与 OSPFv2 相同，有以下改变：

1. LSID 设置为 DR 的接口 ID。ospfv2 中 LSID 设置为 DR 路由器的接口地址；
2. 不包含掩码信息，少了 Net MASK 字段；
3. 选项字段是链路上 FULL 邻居通告的 LINKLSA 中选项的逻辑 OR。

### Inter-Area-Prefix-LSAs

Inter-Area-Prefix-LSA 帧格式如图 4-25所示：

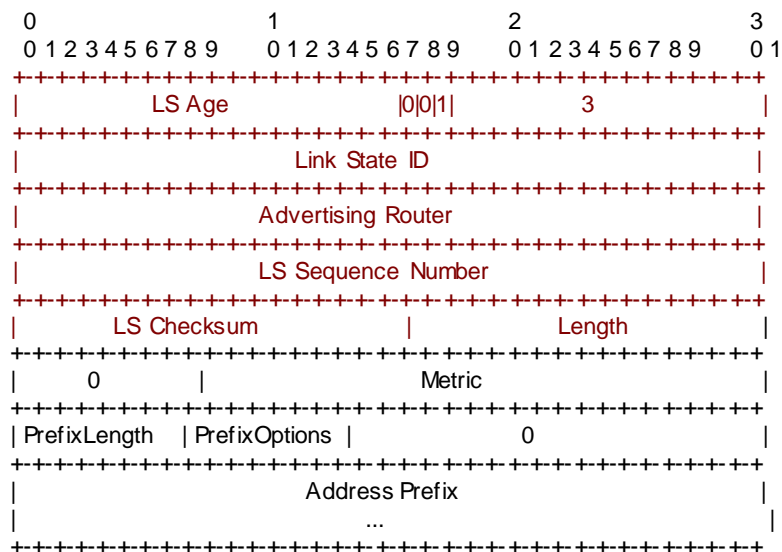


图 4-25 Inter-Area-Prefix -LSA 帧格式

此 LSA 等效于 OSPFv2 中的 3 类 LSA。生成前缀的过程和 OSPFv2 基本一致，主要有以下不同：

LSID 不具有地址意义，只是区分不同的 LSA。因此，设计时可以在目标区域设置一个 InterPrefixID 参数，初始化为 1；

如果是新增加的路由，则递增序号；

如果是已有的路由，则使用前缀进行搜索。

### Inter-Area-Router-LSAs

Inter-Area-Router-LSA 帧格式如图 4-26所示：

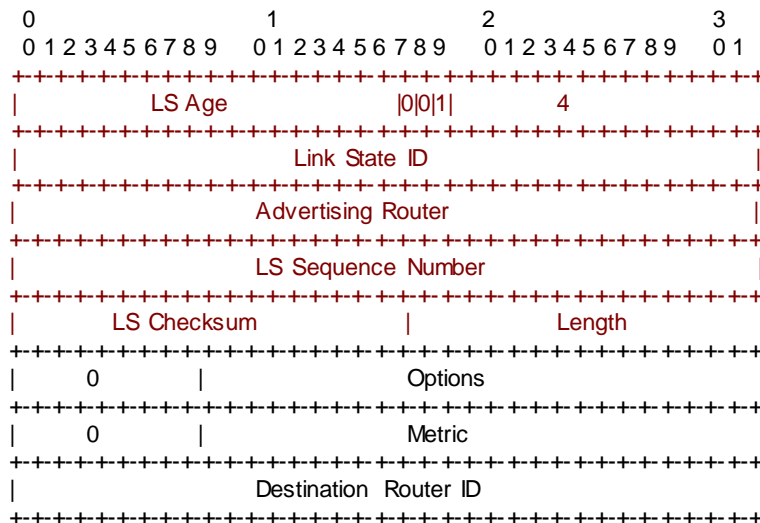


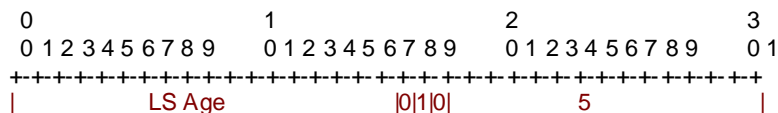
图 4-26 Inter-Area-Router -LSA 帧格式

生成过程和 OSPFv2 基本一致，有以下不同：

1. LSID 不再描述路由器的 ID，而只是用于区分不同的 LSA。设计时可以同域间前缀 LSA；
2. 目的路由器 ID 用 LSA 内容中 Destination Router ID 来标识；
3. 比 OSPFv2 多了选项字段，设置为目的路由器 RouterLSA 中的选项。

### AS-External-LSAs

AS-External-LSA 帧格式如图 4-27所示：



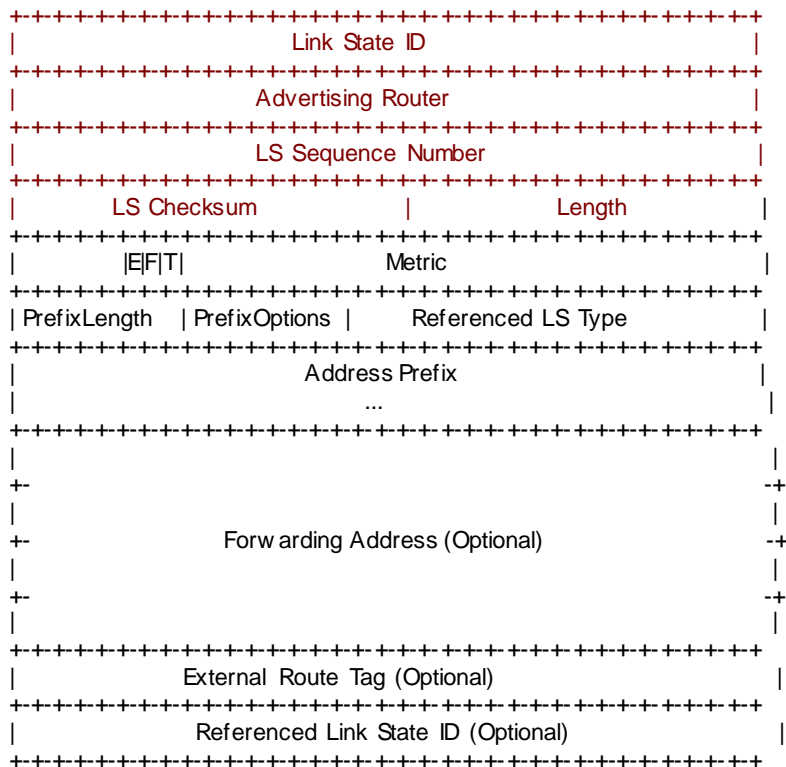


图 4-27 AS-External-LSA 帧格式

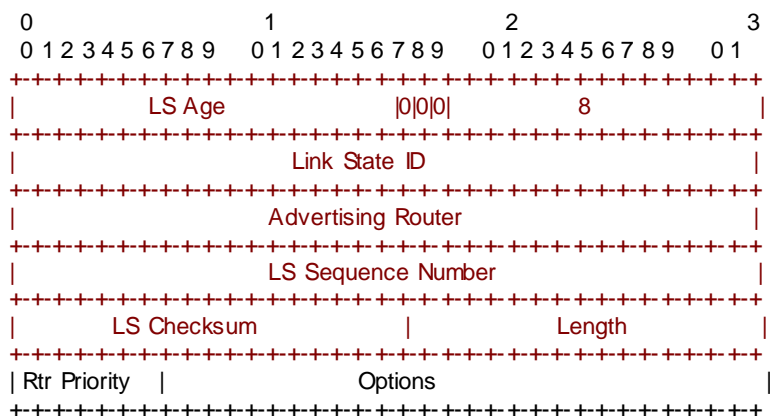
LSID 不再描述路由器的 ID，而只是用于区分不同的 LSA。目的 ID 用 LSABody 中的地址前缀来标识。

### NSSA-LSAs

格式同 5 类，与 OSPFv2 生成方式相同。

### Link-LSAs

Link-LSA 帧格式如图 4-28所示：



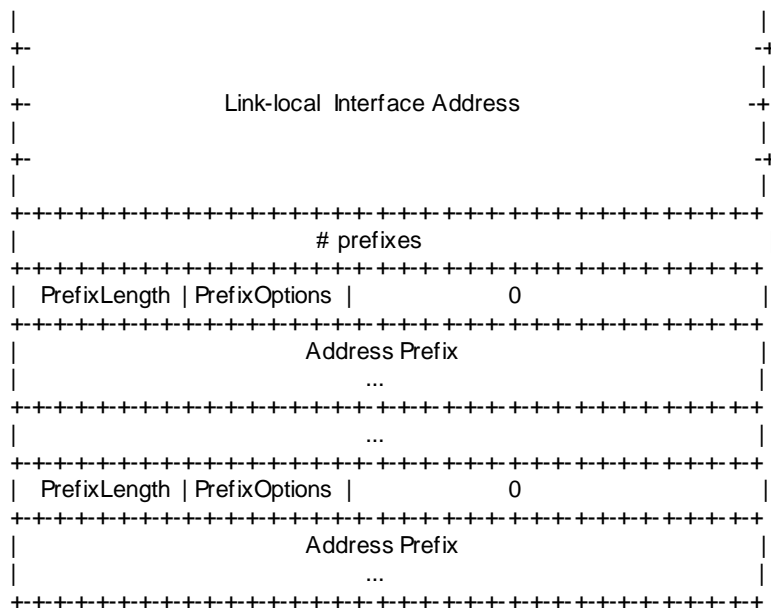


图 4-28 Link-LSA 帧格式

Link-LSA 是 OSPFv2 所没有的。

路由器为每一链路生成 LinkLSA，故设备启动后只要接口 IP，就应该有 LINK-LSA 生成。虚链路不应生成 LINKLSA。LSID 为路由器的接口 ID。

LINKLSA 有 3 个目的：

1. 提供链路本地地址，以 fe80 开始的地址；
2. 提供本地连接的 ipv6 前缀；
3. 提供选项。

为链路 L 构造 LinkLSA 的过程如下：

- LSID 设置为路由器为 L 设置的接口 ID
- LinkLSA 包含 L 的优先级
- 选项设置为路由器的能力。在广播接口上，DR 生成 NetworkLSA 时，将对所有 FULL 状态邻居的选项进行逻辑或操作。
- 路由器在 LinkLSA 中包含 L 的链路本地地址。此信息用于下一跳计算。
- 包含 L 上配置的所有 ipv6 地址前缀，指定前缀长度，选项，前缀。

构造之后，将 LSA 加载到链路数据库中，并在链路上扩散。链路上其他节点收到 LSA 后，进行存储，但是不会再次洪泛。

### Intra-Area-Prefix-LSAs

Intra-Area-Prefix-LSA 帧格式如图 4-29所示（LSID 没有地址含义）：

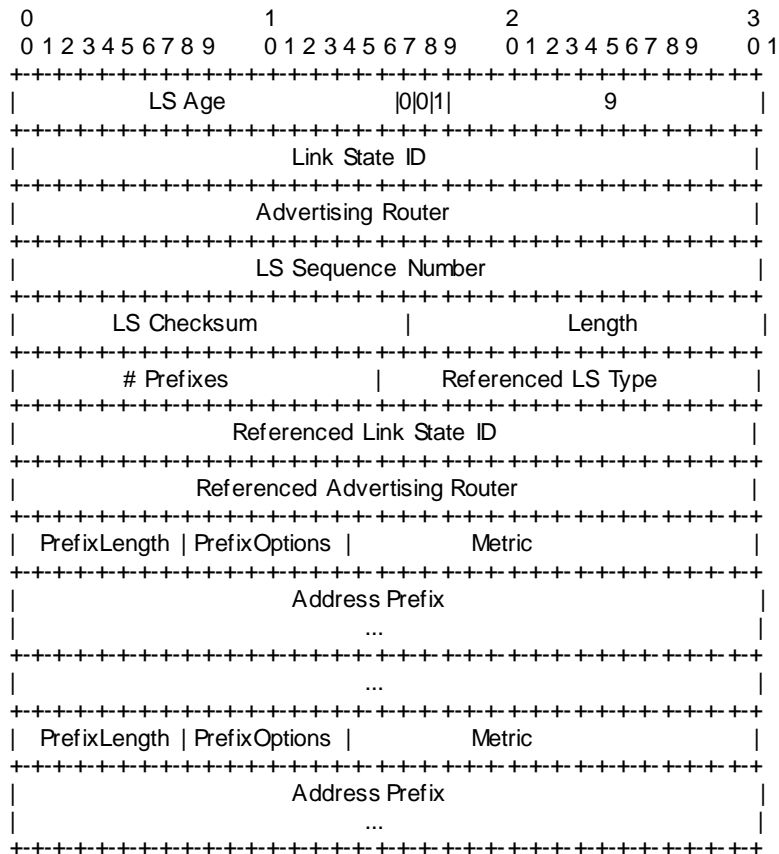


图 4-29 Intra-Area-Prefix-LSA 帧格式

Intra-area-prefix-LSA 与 ospfv2 中的 9 类 LSA 意思完全不一样，ospfv2 中的 9 类 LSA 用于 graceful restart，是接口洪泛范围。intra-area-prefix-LSA 类型描述一个网络上的前缀，或者一个路由器上的前缀，具有区域洪泛范围。LSID 也是用来区分不同的 LSA：

1. 描述一个网络的前缀

Stub 接口——引用的是当前的 RouterLSA。引用 LSID 为 0，引用路由器 ID 为路由器自己的 ID。

2. 描述一个路由器上的前缀

具有 FULL 邻居的 BCAST 接口——引用的是 NetworkLSA。引用 LSID 为 DR 在 L 上的接口 ID，引用路由器 ID 设置为 DR 的 ID。当路由器是 DR 且有 FULL 邻居时，才生成。

链路的 DR 向区域生成一个或多个 LSA，用于通告链路上的前缀。对链路 L，L 上的 DR 按照以下过程构造 LSA：

- 为表明前缀与 L 对应，引用 LS 类型，引用 LSID 和引用路由器 ID 设置为 L 的 NetworkLSA 上的相应字段。即引用 LS 类型为 0x2002，引用 LSID 为 DR 在 L 上的接口 ID，引用路由器 ID 设置为 DR 的 ID。
- 检查 L 上的每一个 LinkLSA。如果 LinkLSA 的通告路由器与 DR 建立了 FULL 邻居，并且 LSID 与邻居的接口 ID 相同，则拷贝 LINKLSA 中的前缀到新 LSA 中。如果前缀设置了 NU 比特或者 LA 比特选项，则不应拷贝，另外链路本地地址也不应拷贝。如果出现相同的前缀(前缀长度，前缀相同)，则将其选项进行逻辑或操作，得到最后的前缀选项。

所有前缀的开销均为 0。

- "# prefixes" 字段设置为 LSA 中的前缀数目。如果有必要，可以将前缀分布到多个 LSA 中以减少 LSA 的大小。

路由器为其 Stub 链路上的前缀构造 intra-area-prefix-LSA。路由器按照以下方法构造 LSA：

- 引用 LS 类型为 0x2001，引用 LSID 为 0，引用路由器 ID 为路由器自己的 ID；
- 检查自己的区域的接口。如果接口状态为 DOWN，不包含接口的前缀；  
如果接口包含在 2 类链路中，则前缀将包含在接口 DR 通告的 LSA 中，跳过接口；  
如果前缀设置了 LA 比特，则需要包含此前缀；  
前缀的开销设置为对应接口的开销；
- LSA 中包含直连的主机(这个可以不管)；
- 如果具有经过此区域的一个或多个虚链路，则包含一个全球 ipv6 接口地址(如果没有配置的话)，选项中设置 LA 比特，前缀长度为 128，开销为 0。此信息可用于虚链路两端相互学习地址；
- "# prefixes" 设置为前缀数目。

## 4.5.2 OSPFv3 配置

### 4.5.2.1 配置全局 OSPFv3

#### 4.5.2.1.1 使能 OSPFv3 进程

##### 目的

本节介绍如何启动和关闭（使能/去使能）OSPFv3 进程。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
启动默认 OSPFv3 进程	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>router ipv6 ospf</b>	-
启动指定 OSPFv3 进程	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>router ipv6 ospf process id</b>	process id: SC9600 支持的 OSPFv3 进程 ID, 取值范围为: 1-2047
关闭默认 OSPFv3 进程	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>no router ipv6 ospf</b>	-
关闭指定 OSPFv3 进程	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>no router ipv6 ospf process id</b>	process id: SC9600 支持的 OSPFv3 进程 ID, 取值范围为: 1-2047
关闭所有 OSPFv3 进程	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>no router ipv6 ospf all</b>	-

#### 4.5.2.1.2 使能 OSPFv3 进程指定 VPN 实例

##### 目的

本节介绍如何启动（使能）OSPFv3 进程指定的 VPN 实例。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
启动指定 OSPFv3 进程指	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；	process id: SC9600 支持的 OSPFv3 进程 ID, 取值范围为:



目的	步骤	参数说明
定 VPN 实例	2. 执行命令 <b>router ipv6 ospf process id vpn-instance NAME</b>	1-2047; NAME: VPN 实例名, 命名规则为少于 31 字符
启动默认 OSPFv3 进程指定 VPN 实例	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>router ipv6 ospf vpn-instance NAME</b>	NAME: VPN 实例名, 命名规则为少于 31 字符

#### 4.5.2.1.3 复位 OSPFv3 进程

##### 目的

本节介绍如何复位 OSPFv3 进程。

##### 过程

根据不同目的, 执行相应步骤, 具体参见下表。

目的	步骤	参数说明
复位 OSPFv3 进程	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>reset ipv6 ospf</b>	-
复位指定 OSPFv3 进程	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>reset ipv6 ospf process id</b>	process id: SC9600 支持的 OSPFv3 进程 ID, 取值范围为: 1-2047

#### 4.5.2.1.4 清除 OSPFv3 统计信息

##### 目的

本节介绍如何清除 OSPFv3 统计信息。

##### 过程

根据不同目的, 执行相应步骤, 具体参见下表。

目的	步骤	参数说明
清除 OSPFv3 统计信息	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>reset ipv6 ospf counters</b>	-

#### 4.5.2.2 配置 OSPFv3 节点

##### 4.5.2.2.1 配置路由器 ID

##### 目的

本节介绍如何配置路由器 ID。

### 背景信息

配置的路由器 ID 必须为本地 IP 地址之一。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置路由器 ID	<ol style="list-style-type: none"> <li>在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>执行命令 <b>router ipv6 ospf</b>，进入 OSPFv3 配置视图；</li> <li>执行命令 <b>router-id router-id</b></li> </ol>	<b>router-id</b> : 路由器 ID，点分十进制形式，形如：(A.B.C.D)，其中 A~D 为整数形式，取值范围为 1-255

#### 4.5.2.2.2 配置 Stub 区域

### 目的

本节介绍如何配置 Stub 区域。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置普通 Stub 区域	<ol style="list-style-type: none"> <li>在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>执行命令 <b>router ipv6 ospf</b>，进入 OSPFv3 配置视图；</li> <li>执行命令 <b>area area-id stub</b></li> </ol>	<b>area-id</b> : OSPFv3 区域 ID，点分十进制形式，形如：(A.B.C.D)，其中 A~D 为整数形式，取值范围为 1-255(大于 65535 的区域) 或者整数形式，取值范围为 0-4294967295(小于 65535 的区域)
配置 totalStub 区域	<ol style="list-style-type: none"> <li>在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>执行命令 <b>router ipv6 ospf</b>，进入 OSPFv3 配置视图；</li> <li>执行命令 <b>area area-id stub no-summary</b></li> </ol>	<b>area-id</b> : OSPFv3 区域 ID，点分十进制形式，形如：(A.B.C.D)，其中 A~D 为整数形式，取值范围为 1-255(大于 65535 的区域) 或者整数形式，取值范围为 0-4294967295(小于 65535 的区域)
删除 Stub 区域	<ol style="list-style-type: none"> <li>在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>执行命令 <b>router ipv6 ospf</b>，进入 OSPFv3 配置视图；</li> </ol>	<b>area-id</b> : OSPFv3 区域 ID，点分十进制形式，形如：(A.B.C.D)，其中 A~D 为整数形式，取值范围为 1-255(大于 65535 的区域) 或

目的	步骤	参数说明
	3. 执行命令 <b>no area area-id stub</b>	者 整 数 形 式 ， 取 值 范 围 为 0-4294967295(小于 65535 的区域)

#### 4.5.2.2.3 配置 NSSA 区域

##### 目的

本节介绍如何配置 NSSA 区域。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置 NSSA 区域	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>router ipv6 ospf</b> ，进入 OSPFv3 配置视图； 3. 执行命令 <b>area area-id nssa</b>	<b>area-id</b> : OSPFv3 区域 ID，点分十进制形式，形如：(A.B.C.D)，其中 A~D 为整数形式，取值范围为 1-255(大于 65535 的区域) 或者 整数形式，取值范围为 0-4294967295(小于 65535 的区域)
配置 no summary NSSA 区域	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>router ipv6 ospf</b> ，进入 OSPFv3 配置视图； 3. 执行命令 <b>area area-id nssa no-summary</b>	<b>area-id</b> : OSPFv3 区域 ID，点分十进制形式，形如：(A.B.C.D)，其中 A~D 为整数形式，取值范围为 1-255(大于 65535 的区域) 或者 整数形式，取值范围为 0-4294967295(小于 65535 的区域)
配置 NSSA 区域聚合通告/不通告	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>router ipv6 ospf</b> ，进入 OSPFv3 配置视图； 3. 执行命令 <b>area area-id nssa range dst-address dst-mask { advertise   no-advertise }</b>	<b>area-id</b> : OSPFv3 区域 ID，点分十进制形式，形如：(A.B.C.D)，其中 A~D 为整数形式，取值范围为 1-255(大于 65535 的区域) 或者 整数形式，取值范围为 0-4294967295(小于 65535 的区域)； <b>dst-address</b> : 目的地址，点分十进制形式，形如：(A.B.C.D)，其中 A~D 为整数形式，取值范围为 1-255； <b>dst-mask</b> : 目的地址掩码，点分十进制形式，形如：(A.B.C.D)，其中 A~D 为整数形式，取值范围为

目的	步骤	参数说明
		<p>1-255;</p> <p><b>advertise:</b> 将匹配到该网段的且非自己生成的 NSSA LSA 转换聚合成一条 5 类 LSA;</p> <p><b>No-advertise:</b> 将匹配到该网段的且非自己生成的 NSSA LSA 不转换为 5 类 LSA</p>
配置 NSSA 指定转换路由器或者候选转换路由器	<ol style="list-style-type: none"> <li>在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;</li> <li>执行命令 <b>router ipv6 ospf</b>, 进入 OSPFv3 配置视图;</li> <li>执行命令 <b>area area-id nssa translator { always   candidate }</b></li> </ol>	<p><b>area-id:</b> OSPFv3 区域 ID, 点分十进制形式, 形如: (A.B.C.D), 其中 A~D 为整数形式, 取值范围为 1-255(大于 65535 的区域) 或者整数形式, 取值范围为 0-4294967295(小于 65535 的区域);</p> <p><b>always:</b> 在 NSSA 区域的 ABR 中, 指定转换路由器。允许将 NSSA 区域中的多个 ABR 配置成转换路由器;</p> <p><b>candidate:</b> 在 NSSA 区域的 ABR 中, 为候选转换路由器。如果在当前区域中, 都没有指定转换路由器, 则由所有的候选路由器进行选举产生转换路由器</p>
删除 NSSA 区域	<ol style="list-style-type: none"> <li>在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;</li> <li>执行命令 <b>router ipv6 ospf</b>, 进入 OSPFv3 配置视图;</li> <li>执行命令 <b>no area area-id nssa</b></li> </ol>	<p><b>area-id:</b> OSPFv3 区域 ID, 点分十进制形式, 形如: (A.B.C.D), 其中 A~D 为整数形式, 取值范围为 1-255(大于 65535 的区域) 或者整数形式, 取值范围为 0-4294967295(小于 65535 的区域)</p>
删除 NSSA 区域聚合	<ol style="list-style-type: none"> <li>在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;</li> <li>执行命令 <b>router ipv6 ospf</b>, 进入 OSPFv3 配置视图;</li> <li>执行命令 <b>no area area-id nssa range dst-address dst-mask</b></li> </ol>	<p><b>area-id:</b> OSPFv3 区域 ID, 点分十进制形式, 形如: (A.B.C.D), 其中 A~D 为整数形式, 取值范围为 1-255(大于 65535 的区域) 或者整数形式, 取值范围为 0-4294967295(小于 65535 的区域);</p> <p><b>dst-address:</b> 目的地址, 点分十进制形式, 形如: (A.B.C.D), 其中 A~D 为整数形式, 取值范围为</p>

目的	步骤	参数说明
		1-255; dst-mask: 目的地址掩码, 点分十进制形式, 形如: (A.B.C.D), 其中 A~D 为整数形式, 取值范围为 1-255;

#### 4.5.2.2.4 创建及配置 OSPFv3 虚接口

##### 目的

本节介绍如何配置 OSPFv3 虚接口。

##### 过程

根据不同目的, 执行相应步骤, 具体参见下表。

目的	步骤	参数说明
创建 OSPFv3 虚接口	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>router ipv6 ospf</b> , 进入 OSPFv3 配置视图; 3. 执行命令 <b>area area-id virtual-link remote-address</b>	<b>area-id</b> : OSPFv3 区域 ID, 点分十进制形式, 形如: (A.B.C.D), 其中 A~D 为整数形式, 取值范围为 1-255(大于 65535 的区域) 或者整数形式, 取值范围为 0-4294967295(小于 65535 的区域); <b>remote-address</b> : 虚链路对端 OSPFv3 路由器的 ID, 点分十进制形式, 形如: (A.B.C.D), 其中 A~D 为整数形式, 取值范围为 1-255;
删除 OSPFv3 虚接口	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>router ipv6 ospf</b> , 进入 OSPFv3 配置视图; 3. 执行命令 <b>no area area-id virtual-link remote-address</b>	<b>area-id</b> : OSPFv3 区域 ID, 点分十进制形式, 形如: (A.B.C.D), 其中 A~D 为整数形式, 取值范围为 1-255(大于 65535 的区域) 或者整数形式, 取值范围为 0-4294967295(小于 65535 的区域); <b>remote-address</b> : 虚链路对端 OSPFv3 路由器的 ID, 点分十进制形式, 形如: (A.B.C.D), 其中 A~D 为整数形式, 取值范围为 1-255;
配置 OSPFv3 虚接口邻居超时时间	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>router ipv6 ospf</b> , 进入 OSPFv3 配置视图;	<b>area-id</b> : OSPFv3 区域 ID, 点分十进制形式, 形如: (A.B.C.D), 其中 A~D 为整数形式, 取值范围为 1-255(大于 65535 的区域) 或

目的	步骤	参数说明
	3. 执行命令 <b>area area-id virtual-link remote-address dead-interval</b> 或 <b>area area-id virtual-link remote-address dead-interval default</b>	者整数形式，取值范围为 0-4294967295(小于 65535 的区域)； remote-address：虚链路对端 OSPFv3 路由器的 ID,点分十进制形式，形如：(A.B.C.D)，其中 A~D 为整数形式，取值范围为 1-255； dead-interval：虚邻居的死亡时间，整数形式，取值范围是 0-2147483647，单位：秒
配置 OSPFv3 虚接口 Hello 间隔时间	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>router ipv6 ospf</b> ，进入 OSPFv3 配置视图； 3. 执行命令 <b>area area-id virtual-link remote-address hello-interval</b> 或 <b>area area-id virtual-link remote-address hello-interval default</b>	area-id：OSPFv3 区域 ID，点分十进制形式，形如：(A.B.C.D)，其中 A~D 为整数形式，取值范围为 1-255(大于 65535 的区域) 或者整数形式，取值范围为 0-4294967295(小于 65535 的区域)； remote-address：虚链路对端 OSPFv3 路由器的 ID,点分十进制形式，形如：(A.B.C.D)，其中 A~D 为整数形式，取值范围为 1-255； hello-interval：呼叫虚邻居的时间间隔，整数形式，取值范围是 1~65535，单位：秒
配置 OSPFv3 虚接口重传间隔时间	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>router ipv6 ospf</b> ，进入 OSPFv3 配置视图； 3. 执行命令 <b>area area-id virtual-link remote-address retransmit-interval</b> 或 <b>area area-id virtual-link remote-address retransmit-interval default</b>	area-id：OSPFv3 区域 ID，点分十进制形式，形如：(A.B.C.D)，其中 A~D 为整数形式，取值范围为 1-255(大于 65535 的区域) 或者整数形式，取值范围为 0-4294967295(小于 65535 的区域)； remote-address：虚链路对端 OSPFv3 路由器的 ID,点分十进制形式，形如：(A.B.C.D)，其中 A~D 为整数形式，取值范围为 1-255； retransmit-interval：链路状态通告的重传时间间隔，整数形式，取值范围是 1-3600，单位：秒
配置 OSPFv3 虚接口传输时延	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；	area-id：OSPFv3 区域 ID，点分十进制形式，形如：(A.B.C.D)，

目的	步骤	参数说明
	2. 执行命令 <b>router ipv6 ospf</b> ，进入 OSPFv3 配置视图； 3. 执行命令 <b>area area-id virtual-link remote-address transmit-delay transmit-delay</b> 或 <b>area area-id virtual-link remote-address transmit-delay default</b>	其中 A~D 为整数形式，取值范围为 1-255(大于 65535 的区域) 或者整数形式，取值范围为 0-4294967295(小于 65535 的区域)； remote-address：虚链路对端 OSPFv3 路由器的 ID,点分十进制形式，形如：(A.B.C.D)，其中 A~D 为整数形式，取值范围为 1-255； transmit-delay：链路状态通告的传输时延，整数形式，取值范围是 1-3600，单位：秒

#### 4.5.2.2.5 配置区域聚合

##### 目的

本节介绍如何配置区域聚合。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
区域聚合	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>router ipv6 ospf</b> ，进入 OSPFv3 配置视图； 3. 执行命令 <b>area area-id range dst-address dst-mask { advertise   no-advertise }</b>	area-id: OSPFv3 区域 ID，点分十进制形式，形如：(A.B.C.D)，其中 A~D 为整数形式，取值范围为 1-255(大于 65535 的区域) 或者整数形式，取值范围为 0-4294967295(小于 65535 的区域)； advertise：为聚合条目生成 Summary LSA； no-advertise：不生成聚合条目对应的 Summary LSA
删除区域聚合	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>router ipv6 ospf</b> ，进入 OSPFv3 配置视图； 3. 执行命令 <b>no area area-id range dst-address dst-mask</b>	area-id: OSPFv3 区域 ID，点分十进制形式，形如：(A.B.C.D)，其中 A~D 为整数形式，取值范围为 1-255(大于 65535 的区域) 或者整数形式，取值范围为 0-4294967295(小于 65535 的区域)； dst-address: 目的地址，点分十

目的	步骤	参数说明
		进制形式，形如：(A.B.C.D)，其中 A~D 为整数形式，取值范围为 1-255； dst-mask: 目的地址掩码，点分十进制形式，形如：(A.B.C.D)，其中 A~D 为整数形式，取值范围为 1-255

#### 4.5.2.2.6 配置 GR 重启

##### 目的

本节介绍如何配置 GR(Graceful Restart)重启。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
使能 GR	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>router ipv6 ospf</b>，进入 OSPFv3 配置视图；</li> <li>3. 执行命令 <b>graceful-restart</b></li> </ol>	-
配置 GR 周期	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>router ipv6 ospf</b>，进入 OSPFv3 配置视图；</li> <li>3. 执行命令 <b>graceful-restart period restart-time</b></li> </ol>	<b>restart-time</b> : 重启过程时间，整数形式，取值范围是 40~1800，单位为秒
使能 GR helper	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>router ipv6 ospf</b>，进入 OSPFv3 配置视图；</li> <li>3. 执行命令 <b>graceful-restart helper</b></li> </ol>	-
去使能 GR 重启	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>router ipv6 ospf</b>，进入 OSPFv3 配置视图；</li> <li>3. 执行命令 <b>no graceful-restart</b></li> </ol>	-
去使能 GR helper	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> </ol>	-



目的	步骤	参数说明
	2. 执行命令 <b>router ipv6 ospf</b> ，进入 OSPFv3 配置视图； 3. 执行命令 <b>no graceful-restart helper</b>	
执行 GR 重启	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>router ipv6 ospf</b> ，进入 OSPFv3 配置视图； 3. 执行命令 <b>graceful-restart begin</b>	-

#### 4.5.2.2.7 配置路由计算间隔

##### 目的

本节介绍如何配置路由计算间隔。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置路由计算间隔	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>router ipv6 ospf</b> ，进入 OSPFv3 配置视图； 3. 执行命令 <b>spf-running-interval interval</b> 或 <b>spf-running-interval default</b>	<b>Interval</b> : 指定路由计算间隔时间，整数形式，取值范围是 1~60，单位为 ms

#### 4.5.2.2.8 配置 OSPFv3 重分配

##### 目的

本节介绍如何配置 OSPFv3 重分配。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置 OSPFv3 重分配	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>router ipv6 ospf</b> ，进入 OSPFv3 配置视图；	参数分别代表将直联路由、静态路由、RIP 路由、BGP 路由和 ISIS 路由重分配到 OSPFv3 数据库

目的	步骤	参数说明
	3. 执行命令 <b>redistribute { connect   static   rip   bgp   isis }</b>	
删除 OSPFv3 重分配	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>router ipv6 ospf</b> , 进入 OSPFv3 配置视图; 3. 执行命令 <b>no redistribute { connect   static   rip   bgp   isis }</b>	参数分别代表将直联路由、静态路由、RIP 路由、BGP 路由和 ISIS 路由重分配到 OSPFv3 数据库
配置重分配路由策略	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>router ipv6 ospf</b> , 进入 OSPFv3 配置视图; 3. 执行命令 <b>redistribute { connect   static   rip   bgp   isis } route-policy policy-name</b>	policy-name: 路由策略的名字, 字符串, 不超过 20 个字节
删除重分配路由策略	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>router ipv6 ospf</b> , 进入 OSPFv3 配置视图; 3. 执行命令 <b>no redistribute { connect   static   rip   bgp   isis } route-policy policy-name</b>	policy-name: 路由策略的名字, 字符串, 不超过 20 个字节

#### 4.5.2.2.9 使能 OSPFv3 上报 trap

##### 目的

本节介绍如何使能 OSPFv3 上报 trap。

##### 过程

根据不同目的, 执行相应步骤, 具体参见下表。

目的	步骤	参数说明
使能/去使能 OSPFv3 上报 trap 功能	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>router ipv6 ospf</b> , 进入 OSPFv3 配置视图; 3. 执行命令 <b>snmp-trap (enable   disable)</b>	-
使能/去使能 OSPFv3 上报	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;	-

目的	步骤	参数说明
trap 具体功能	2. 执行命令 <b>router ipv6 ospf</b> ，进入 OSPFv3 配置视图； 3. 执行命令 <b>snmp-trap (enable   disable) trap-name (ospfifauthfailure   ospfifconfigerror   ospfifrxbadpacket   ospfifstatechange   ospflsdbapproachingoverflow   ospflsdboverflow   ospfmaxagelsa   ospfnbrrestarthelperstatuschange   ospfnbrstatechange   ospfnssatranslatorsstatuschange   ospforiginatelsa   ospfrestartstatuschange   ospftxretransmit   ospfvirtifauthfailure   ospfvirtifconfigerror   ospfvirtifrxbadpacket   ospfvirtifstatechange   ospfvirtiftxretransmit   ospfvirtnbrrestarthelperstatuschange   ospfvirtnbrstatechange)</b>	

#### 4.5.2.3 配置 OSPFv3 端口

##### 4.5.2.3.1 配置 OSPFv3 接口参数

###### 目的

本节介绍如何配置 OSPFv3 接口参数。

###### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
将接口加入到指定的区域中	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>interface vlan N</b> ，进入 VLAN IF 配置视图； 3. 执行命令 <b>ipv6 ospf area area-id</b>	N: vlan ID，整数形式，取值范围为 1~4094； area-id: OSPFv3 区域 ID，点分十进制形式，形如：(A.B.C.D)，其中 A~D 为整数形式，取值范围为 1-255(大于 65535 的区域) 或者整数形式，取值范围为 0-4294967295(小于 65535 的区域)；

目的	步骤	参数说明
将接口加入到指定的进程中	<ol style="list-style-type: none"> <li>在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;</li> <li>执行命令 <b>interface vlan N</b>, 进入 VLAN IF 配置视图;</li> <li>执行命令 <b>ipv6 ospf area area-id process process-id</b> 或 <b>ipv6 ospf area area-id process process-id instance instance-id</b></li> </ol>	<p>N: vlan ID, 整数形式, 取值范围为 1~4094;</p> <p>area-id: OSPFv3 区域 ID, 点分十进制形式, 形如: (A.B.C.D), 其中 A~D 为整数形式, 取值范围为 1-255(大于 65535 的区域) 或者整数形式, 取值范围为 0-4294967295(小于 65535 的区域);</p> <p>process-id: 指定启动的 OSPFv3 进程号, 整数形式, 取值范围为 1~2047;</p> <p>instance-id: 指定启动的实例号, 整数形式, 取值范围为 1~255</p>
配置 OSPFv3 接口类型	<ol style="list-style-type: none"> <li>在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;</li> <li>执行命令 <b>interface vlan N</b>, 进入 VLAN IF 配置视图;</li> <li>执行命令 <b>ipv6 ospf if-type&lt;broadcast   nbma   p2p   p2multip &gt;</b></li> </ol>	<p>N: vlan ID, 整数形式, 取值范围为 1~4094;</p> <p>参数分别表示将接口的网络类型更改为广播、将接口的网络类型更改为 NBMA、将接口的网络类型更改为点到点以及将接口的网络类型更改为点到多点</p>
配置 OSPFv3 接口优先级	<ol style="list-style-type: none"> <li>在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;</li> <li>执行命令 <b>interface vlan N</b>, 进入 VLAN IF 配置视图;</li> <li>执行命令 <b>ipv6 ospf priority priority</b> 或 <b>ip ospf priority default</b></li> </ol>	<p>N: vlan ID, 整数形式, 取值范围为 1~4094;</p> <p>priority: ospf 的接口优先级, 整数形式, 取值范围是 1~255, 单位为每秒字节数</p>
配置 OSPFv3 接口开销	<ol style="list-style-type: none"> <li>在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;</li> <li>执行命令 <b>interface vlan N</b>, 进入 VLAN IF 配置视图;</li> <li>执行命令 <b>ipv6 ospf cost cost</b> 或 <b>ip ospf cost default</b></li> </ol>	<p>N: vlan ID, 整数形式, 取值范围为 1~4094;</p> <p>cost: 运行 OSPFv3 协议所需的开销, 整数形式, 取值范围是 0-65535</p>
配置 OSPFv3 接口 Hello 间隔时间	<ol style="list-style-type: none"> <li>在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;</li> <li>执行命令 <b>interface vlan N</b>, 进入 VLAN IF 配置视图;</li> <li>执行命令 <b>ipv6 ospf hello-interval</b></li> </ol>	<p>N: vlan ID, 整数形式, 取值范围为 1~4094;</p> <p>hello-interval: 配置 OSPFv3 接口 Hello 间隔时间, 整数形式, 取值范围是 1-65535</p>

目的	步骤	参数说明
	<i>hello-interval</i> 或 <b>ip ospf hello-interval default</b>	
配置 OSPFv3 接口邻居超时时间	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>interface vlan N</b> , 进入 VLAN IF 配置视图; 3. 执行命令 <b>ipv6 ospf dead-interval dead-interval</b> 或 <b>ip ospf dead-interval default</b>	N: vlan ID, 整数形式, 取值范围为 1~4094; dead-interval: 指定 OSPFv3 接口邻居超时时间, 整数形式, 取值范围是 0-2147483647
配置 OSPFv3 接口重传间隔	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>interface vlan N</b> , 进入 VLAN IF 配置视图; 3. 执行命令 <b>ipv6 ospf retransmit-interval retransmit-interval</b> 或 <b>ip ospf retransmit-interval default</b>	N: vlan ID, 整数形式, 取值范围为 1~4094; retransmit-interval: 接口重传间隔, 整数形式, 取值范围是 0-3600, 单位为秒
配置 OSPFv3 接口传输时延	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>interface vlan N</b> , 进入 VLAN IF 配置视图; 3. 执行命令 <b>ipv6 ospf transmit-delay transmit-delay</b> 或 <b>ip ospf transmit-delay default</b>	N: vlan ID, 整数形式, 取值范围为 1~4094; transmit-delay: 接口传输时延, 整数形式, 取值范围是 0~3600, 单位为秒

#### 4.5.2.3.2 配置 BFD

##### 目的

本节介绍如何配置 BFD。

##### 过程

根据不同目的, 执行相应步骤, 具体参见下表。

目的	步骤	参数说明
配置 BFD	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>interface vlan N</b> , 进入	N: vlan ID, 整数形式, 取值范围为 1~4094; enable 表示在 vlan 接口下使能

目的	步骤	参数说明
	VLAN IF 配置视图; 3. 执行命令 <b>ipv6 ospf bfd (enable   disable)</b>	BGP 特性, <b>disable</b> 表示在 vlan 接口下去使能 BGP 特性

#### 4.5.2.3.3 配置 OSPFv3 接口 MTU

##### 目的

本节介绍如何配置 OSPFv3 接口 MTU。

##### 过程

根据不同目的, 执行相应步骤, 具体参见下表。

目的	步骤	参数说明
配置 OSPFv3 接口 MTU	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>interface vlan N</b> , 进入 VLAN IF 配置视图; 3. 执行命令 <b>ipv6 ospf mtu mtu</b> 或 <b>ipv6 ospf mtu default</b>	N: vlan ID, 整数形式, 取值范围为 1~4094; mtu: ospf 的接口 MTU 值, 整数形式, 取值范围是 572-1500
配置 MTU 检测	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>interface vlan N</b> , 进入 VLAN IF 配置视图; 3. 执行命令 <b>ipv6 ospf mtu-ignore (enable   disable)</b>	N: vlan ID, 整数形式, 取值范围为 1~4094; <b>enable</b> 表示忽略 MTU 检测, <b>disable</b> 表示不忽略 MTU 检测

#### 4.5.2.3.4 配置 passive 接口

##### 目的

本节介绍如何配置 passive 接口。

##### 背景信息

被动接口是指不收发协议消息的 OSPFv3 接口, 在此接口上不建立任何邻居, 但是接口路由将包含在 RouterLSA 中作为内部路由传播。可用于 Stub 路由。

##### 过程

根据不同目的, 执行相应步骤, 具体参见下表。

目的	步骤	参数说明
----	----	------

目的	步骤	参数说明
配置 passive 接口	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>interface vlan N</b> ，进入 VLAN IF 配置视图； 3. 执行命令 <b>ipv6 ospf passive-interface</b>	N: vlan ID，整数形式，取值范围为 1~4094；
删除 passive 接口配置	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>interface vlan N</b> ，进入 VLAN IF 配置视图； 3. 执行命令 <b>no ipv6 ospf passive-interface</b>	N: vlan ID，整数形式，取值范围为 1~4094；

#### 4.5.2.4 配置 OSPFv3 调试功能

##### 目的

本节介绍如何配置 OSPFv3 调试功能。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
开启全局 debug 信息	1. 进入特权用户视图； 2. 执行命令 <b>debug ospf (global all lsa hello packet neighbor interface ip-route rtm spf syn graceful-restart frr nbrchange)</b>	缺省情况下，该调试功能 是关闭的。
开启具体实例 debug 信息	1. 进入特权用户视图； 2. 执行命令 <b>debug ospf (global all lsa hello packet neighbor interface ip-route rtm spf syn graceful-restart frr nbrchange) process process-id</b>	process id: SC9600 支持的 OSPFv3 进程 ID，取值范围为：1-2047 缺省情况下，该调试功能 是关闭的。
开启所有实例 debug 信息	1. 进入特权用户视图； 2. 执行命令 <b>debug ospf (global all lsa hello packet neighbor interface ip-route rtm spf syn graceful-restart frr nbrchange) process all</b>	缺省情况下，该调试功能 是关闭的。
关闭全局 debug 信息	1. 进入特权用户视图； 2. 执行命令 <b>no debug ospf (global all lsa hello packet neighbor interface ip-route rtm spf syn graceful-restart frr nbrchange)</b>	缺省情况下，该调试功能 是关闭的。

目的	步骤	参数说明
关闭具体实例 debug 信息	1. 进入特权用户视图; 2. 执行命令 <b>no debug ospf (global all lsa hello packet neighbor interface ip-route rtm spf) syn graceful-restart frr nbrchange) process process-id</b>	process id: SC9600 支持的 OSPFv3 进程 ID, 取值范围为: 1-2047 缺省情况下, 该调试功能是关闭的。
关闭所有实例 debug 信息	1. 进入特权用户视图; 2. 执行命令 <b>no debug ospf (global all lsa hello packet neighbor interface ip-route rtm spf) syn graceful-restart frr nbrchange) process all</b>	缺省情况下, 该调试功能是关闭的。

#### 4.5.2.5 查看 OSPFv3 配置信息

##### 目的

本节介绍如何查看 OSPFv3 配置信息。

##### 过程

根据不同目的, 执行相应步骤, 具体参见下表。

目的	步骤	参数说明
显示 OSPFv3 简要信息	1. 进入普通用户视图或特权用户视图; 2. 执行命令 <b>show ip ospf brief</b> <b>show ip ospf brief process &lt;1-2048&gt;</b>	-
显示 OSPFv3 配置信息	1. 进入普通用户视图或特权用户视图; 2. 执行命令 <b>show ip ospf config</b>	-
显示 OSPFv3 接口信息	1. 进入普通用户视图或特权用户视图; 2. 执行命令 <b>show ip ospf interface</b> <b>show ip ospf interface (A.B.C.D)</b> <b>show ip ospf interface count</b> <b>show ip ospf interface process process-id</b>	process id: SC9600 支持的 OSPFv3 进程 ID, 取值范围为: 1-2047
显示 OSPFv3 邻居信息	1. 进入普通用户视图或特权用户视图; 2. 执行命令 <b>show ip ospf neighbor</b> <b>show ip ospf neighbor nbr-address</b> <b>show ip ospf neighbor process process-id</b> <b>show ip ospf neighbor state statistic</b> <b>show ip ospf neighbor state count</b>	nbr-address: 邻居 IP 地址, 点分十进制形式, 形如: (A.B.C.D), 其中 A~D 为整数形式 process id: SC9600 支持的 OSPFv3 进程 ID, 取值范围为: 1-2047



目的	步骤	参数说明
显示 OSPFv3 区域信息	1. 进入普通用户视图或特权用户视图; 2. 执行命令 <b>show ip ospf area</b> <b>show ip ospf area area-id</b> <b>show ip ospf area process process-id</b>	area-id: OSPFv3 区域 ID, 点分十进制形式, 形如: (A.B.C.D), 其中 A~D 为整数形式, 取值范围为 1-255(大于 65535 的区域) 或者整数形式, 取值范围为 0-4294967295(小于 65535 的区域) process id: SC9600 支持的 OSPFv3 进程 ID, 取值范围为: 1-2047
显示 OSPFv3 数据库信息	1. 进入普通用户视图或特权用户视图; 2. 执行命令 <b>show ip ospf database</b> <b>show ip ospf database process process-id</b> <b>show ip ospf database area area-id</b> <b>show ip ospf database area area-id process process-id</b> <b>show ip ospf database count</b> <b>show ip ospf database count process process-id</b> <b>show ip ospf database total count</b> <b>show ip ospf database expire</b> <b>show ip ospf database expire count</b> <b>show ip ospf database expire process process-id</b> <b>show ip ospf database router</b> <b>show ip ospf database router LS-id router-id area-id</b> <b>show ip ospf database router LS-id router-id area-id process-id</b> <b>show ip ospf database router process &lt; process-id</b> <b>show ip ospf database network</b> <b>show ip ospf database network LS-id router-id area-id</b> <b>show ip ospf database network LS-id router-id area-id process-id</b> <b>show ip ospf database network process process-id</b> <b>show ip ospf database summary-network</b>	area-id: OSPFv3 区域 ID, 点分十进制形式, 形如: (A.B.C.D), 其中 A~D 为整数形式, 取值范围为 1-255(大于 65535 的区域) 或者整数形式, 取值范围为 0-4294967295(小于 65535 的区域) process id: SC9600 支持的 OSPFv3 进程 ID, 取值范围为: 1-2047 LS-id: 指定 LS ID, 形如: (A.B.C.D), 其中 A~D 为整数形式, 取值范围为 1-255; router-id: 指定通告路由 ID, 形如: (A.B.C.D), 其中 A~D 为整数形式, 取值范围为 1-255

目的	步骤	参数说明
	<p><b>show ip ospf database summary-network</b> <i>LS-id router-id area-id</i></p> <p><b>show ip ospf database summary-network</b> <i>LS-id router-id area-id process-id</i></p> <p><b>show ip ospf database summary-network process process-id</b></p> <p><b>show ip ospf database summary-asbr</b> <b>show ip ospf database summary-asbr</b> <i>LS-id router-id area-id</i></p> <p><b>show ip ospf database summary-asbr</b> <i>LS-id router-id area-id process-id</i></p> <p><b>show ip ospf database summary-asbr process process-id</b></p> <p><b>show ip ospf database nssa-lsa</b> <b>show ip ospf database nssa-lsa</b> <i>LS-id router-id area-id</i></p> <p><b>show ip ospf database nssa-lsa</b> <i>LS-id router-id area-id process-id</i></p> <p><b>show ip ospf database nssa-lsa process process-id</b></p> <p><b>show ip ospf database as-external-lsa</b> <b>show ip ospf database as-external-lsa</b> <i>LS-id router-id</i></p> <p><b>show ip ospf database as-external-lsa</b> <i>LS-id router-id process-id</i></p> <p><b>show ip ospf database as-external-lsa process process-id</b></p> <p><b>show ip ospf database type9</b> <b>show ip ospf database type9</b> <i>LS-id router-id</i></p> <p><b>show ip ospf database type9</b> <i>LS-id router-id process-id</i></p> <p><b>show ip ospf database type9 process process-id</b></p> <p><b>show ip ospf database type9</b> <b>show ip ospf database type9</b> <i>LS-id router-id</i></p> <p><b>show ip ospf database type9</b> <i>LS-id router-id process-id</i></p> <p><b>show ip ospf database type9 process</b></p>	

目的	步骤	参数说明
	<p><i>process-id</i></p> <p><b>show ip ospf database type10</b></p> <p><b>show ip ospf database type10</b> <i>LS-id</i></p> <p><i>router-id area-id</i></p> <p><b>show ip ospf database type10</b> <i>LS-id</i></p> <p><i>router-id area-id process-id</i></p> <p><b>show ip ospf database type10 process</b></p> <p><i>process-id</i></p> <p><b>show ip ospf database type11</b></p> <p><b>show ip ospf database type11</b> <i>LS-id</i></p> <p><i>router-id</i></p> <p><b>show ip ospf database type11</b> <i>LS-id</i></p> <p><i>router-id process-id</i></p> <p><b>show ip ospf database type11 process</b></p> <p><i>process-id</i></p>	
显示 OSPFv3 路由信息	<p>1. 进入普通用户视图或特权用户视图;</p> <p>2. 执行命令</p> <p><b>show ip ospf route</b></p> <p><b>show ip ospf route count</b></p> <p><b>show ip ospf route count process</b></p> <p><i>process-id</i></p> <p><b>show ip ospf route process</b> <i>process-id</i></p> <p><b>show ip ospf route total count</b></p>	<p>process id: SC9600 支持的 OSPFv3 进程 ID, 取值范围为: 1-2047</p>
显示 OSPFv3 虚链路信息	<p>1. 进入普通用户视图或特权用户视图;</p> <p>2. 执行命令</p> <p><b>show ip ospf virtual interface</b></p> <p><b>show ip ospf virtual interface</b> <i>area-id</i></p> <p><i>router-id</i></p> <p><b>show ip ospf virtual interface process</b></p> <p><i>process-id</i></p> <p><b>show ip ospf virtual neighbor</b></p> <p><b>show ip ospf virtual neighbor process</b></p> <p><i>process-id</i></p>	<p>area-id: OSPFv3 区域 ID, 点分十进制形式, 形如: (A.B.C.D), 其中 A~D 为整数形式, 取值范围为 1-255(大于 65535 的区域) 或者整数形式, 取值范围为 0-4294967295(小于 65535 的区域)</p> <p>process id: SC9600 支持的 OSPFv3 进程 ID, 取值范围为: 1-2047;</p> <p>router-id: 指定通告路由 ID, 形如: (A.B.C.D), 其中 A~D 为整数形式, 取值范围为 1-255</p>
显示 OSPFv3 BFD 信息	<p>1. 进入普通用户视图或特权用户视图;</p> <p>2. 执行命令</p> <p><b>show ip ospf bfd session</b></p>	-

目的	步骤	参数说明
显示 OSPFv3 trap 信息	1. 进入普通用户视图或特权用户视图; 2. 执行命令 <b>show ip ospf trap</b>	-
显示 ospf bfd 会话相关信息	1. 进入普通用户视图或特权用户视图; 2. 执行命令 <b>show ip ospf bfd session</b>	-

### 4.5.3 OSPFv3 配置举例

#### 4.5.3.1 配置 OSPFv3 基本功能

##### 组网要求

本案例的任务是完成 OSPFv3 最基本的配置，通过该配置熟悉 OSPFv3 的配置过程，拓扑图如图 4-30所示。

##### 组网图

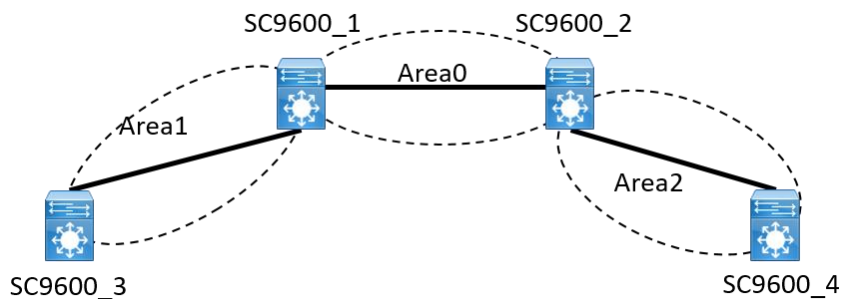


图 4-30 OSPFv3 基本配置拓扑图

##### 配置思路

所有的设备都运行 OSPFv3，并将整个自治系统划分为 3 个区域，其中，SC9600\_1 和 SC9600\_2 为 ABR 来转发区域之间的路由。

配置完成后，每台设备都应学到自治系统内的到所有网段的路由。

##### 数据准备

SC9600\_1 的两个接口地址：2001::1/64 和 2003::1/64

SC9600\_2 的两个接口地址：2001::2/64 和 2004::2/64

SC9600\_3 的两个接口地址：2003::3/64

SC9600\_4 的两个接口地址：2004::4/64。

#### 配置步骤

SC9600\_1:

```
SC9600_1(config)#router ipv6 ospf
SC9600_1(config-ospfv3-1)#router-id 1.1.1.1
SC9600_1(config-ospfv3-1)#quit
SC9600_1(config)#interface vlan 10
SC9600_1(config-if-vlan10)#ipv6 ospf area 0
SC9600_1(config-if-vlan10)#quit
SC9600_1(config)#
SC9600_1(config)#interface vlan 30
SC9600_1(config-if-vlan 30)#ipv6 ospf area 0
```

SC9600\_2:

```
SC9600_2(config)#router ipv6 ospf
SC9600_2(config-ospfv3-1)#router-id 2.1.1.2
SC9600_2(config-ospfv3-1)#quit
SC9600_2(config)#interface vlan 10
SC9600_2(config-if-vlan10)#ipv6 ospf area 0
SC9600_1(config-if-vlan10)#quit
SC9600_1(config)#
SC9600_1(config)#interface vlan 40
SC9600_1(config-if-vlan 40)#ipv6 ospf area 0
```

SC9600\_3:

```
SC9600_3(config)#router ipv6 ospf
SC9600_3(config-ospfv3-1)#router-id 3.1.1.3
SC9600_3(config-ospfv3-1)#quit
SC9600_3(config)#interface vlan 30
SC9600_3(config-if-vlan30)#ipv6 ospf area 0
```

SC9600\_4:

```
SC9600_4(config)#router ipv6 ospf
SC9600_4(config-ospfv3-1)#router-id 4.1.1.4
```

```
SC9600_4(config-ospfv3-1)#quit
SC9600_4(config)#interface vlan 40
SC9600_4(config-if-vlan40)#ipv6 ospf area 0
```

### 验证配置结果

使用 show ipv6 ospf neighbor 命令可看到 OSPFv3 的信息如下:

```
Ospfv3 Process 1
```

NeighborId UpTime	Priority IpAddress	State	Interface	Instance	Aging
1.1.1.2 0:01:38	1 fe80::b8:1	Full	vlan10	0	32

使用 show ip ospf database 命令可看到 OSPFv3 的信息如下:

#### Database of OSPFv3 Process 1

##### Router Link State (Area 0.0.0.1)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
0.0.0.0	1.1.1.1	196	0x80000002	0x49f7	40
0.0.0.0	3.1.1.3	197	0x80000002	0x43fc	40

##### Network Link State (Area 0.0.0.1)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
0.0.39.17	3.1.13	197	0x80000001	0x11d1	32

##### Intra Area Prefix Link State (Area 0.0.0.1)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
0.0.3.232	3.1.1.3	197	0x80000001	0x1a6c	44

##### Link(Type-8) State(interface vlan1 Area 0.0.0.1)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
0.0.39.17	1.1.1.1	236	0x80000001	0xf91	76
0.0.39.17	3.1.1.3	237	0x80000001	0x6155	76

### 4.5.3.2 配置 Stub 区域

#### 组网要求

本案例的任务是完成 OSPFv3 Stub 区域的配置，通过该配置熟悉 OSPFv3 Stub 区域的配置过程，拓扑图如图 4-31所示。

#### 组网图

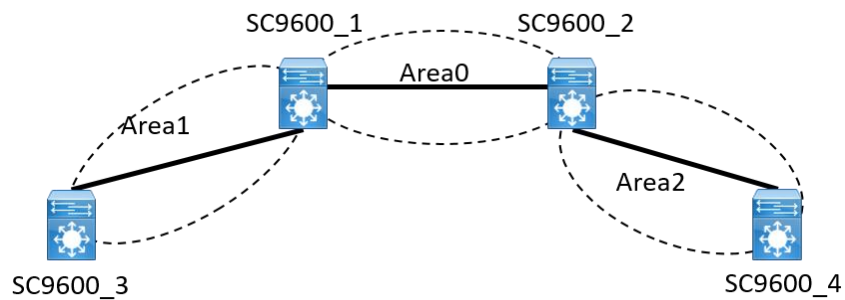


图 4-31 Stub 区域拓扑图

#### 配置思路

所有的设备都运行 OSPFv3，并将整个自治系统划分为 3 个区域，其中 SC9600\_1 和 SC9600\_2 为 ABR 来转发区域之间的路由。

配置完成后，每台设备都应学到自治系统内的到所有网段的路由。

#### 数据准备

SC9600\_1 的两个接口地址：2001::1/64 和 2003::1/64

SC9600\_2 的两个接口地址：2001::2/64 和 2004::2/64

SC9600\_3 的两个接口地址：2003::3/64

SC9600\_4 的两个接口地址：2004::4/64。

#### 配置步骤

基本配置和拓扑同4.5.3.1 配置 OSPFv3 基本功能。

配置 area 1 为 stub:

SC9600\_1:

```
SC9600_1(config)#router ipv6 ospf
```

```
SC9600_1(config-ospfv3-1)#area 1 stub
```

```

SC9600_1(config)#
SC9600_3:
SC9600_3(config)#router ipv6 ospf
SC9600_3(config-ospfv3-1)# area 1 stub
SC9600_3(config)#
在 SC9600_4 引入 2013:0122::1/64 的 5 类 LSA
SC9600_4:
SC9600_4(config-ospfv3-1)#redistribute static
    
```

#### 验证配置结果

- 1) 当 SC9600\_3 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。变成 stub 区域后，比正常区域多一个缺省的 3 类 Inter-Area-Prefix-LSAs，看不到 AS 外部的 LSA。
- 2) 当 SC9600\_3 所在区域配置为 Stub 区域时，已经看不到 AS 外部的路由，取而代之的是一条通往区域外部的缺省路由。

### 4.5.3.3 配置 NSSA 区域

#### 组网要求

本案例的任务是完成 OSPFv3 Stub 区域的配置，通过该配置熟悉 OSPFv3 Stub 区域的配置过程，拓扑图如图 4-32 所示。

#### 组网图

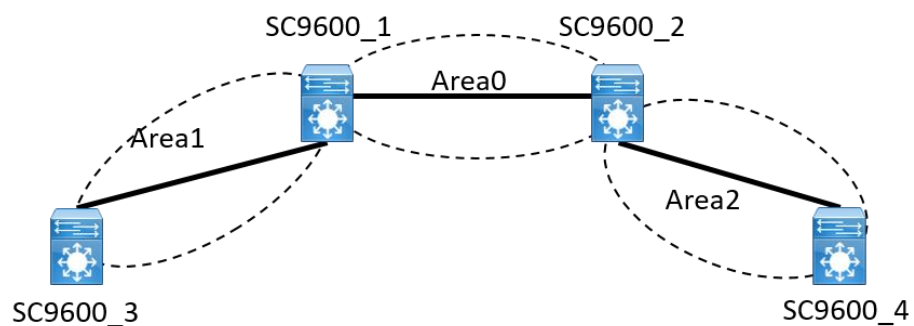


图 4-32 NSSA 区域拓扑图

#### 配置思路



所有的设备都运行 OSPFv3，并将整个自治系统划分为 3 个区域，其中 SC9600\_1 和 SC9600\_2 为 ABR 来转发区域之间的路由。

配置完成后，每台设备都应学到自治系统内的到所有网段的路由。

#### 数据准备

SC9600\_1 的两个接口地址：2001::1/64 和 2003::1/64

SC9600\_2 的两个接口地址：2001::2/64 和 2004::2/64

SC9600\_3 的两个接口地址：2003::3/64

SC9600\_4 的两个接口地址：2004::4/64。

#### 配置步骤

基本配置和拓扑同 4.5.3.1 配置 OSPFv3 基本功能。

配置 area 1 为 nssa:

SC9600\_1:

```
SC9600_1(config)#router ipv6 ospf
```

```
SC9600_1(config-ospfv3-1)#area 1 nssa
```

```
SC9600_1(config)#
```

SC9600\_3:

```
SC9600_3(config)#router ipv6 ospf
```

```
SC9600_3(config-ospfv3-1)# area 1 nssa
```

```
SC9600_3(config)#
```

#### 验证配置结果

- 1) nssa 区域的数据库比正常区域的数据库多一个缺省 NSSA 类型 LSA
- 2) 在 SC9600\_3 引入 1111:1011::1/64 的静态路由，重分配静态路由。
- 3) 在 SC9600\_4 引入 2222:1011::1/64 的静态路由，查看 SC9600\_3 是否拥有外部路由。

#### 4.5.3.4 配置虚接口

##### 组网要求

本案例的任务是完成 OSPFv3 虚接口的配置，通过该配置熟悉 OSPFv3 虚接口的配置过程，拓扑图如图 4-33 所示。

组网图

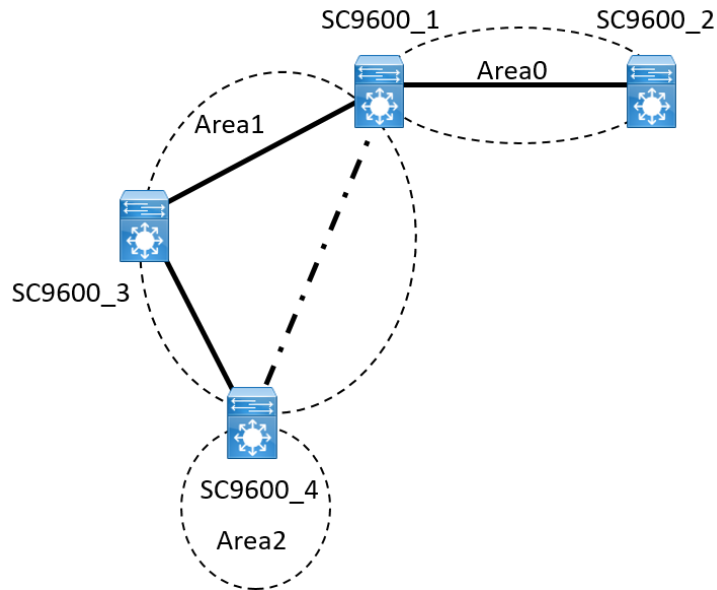


图 4-33 虚接口拓扑图

配置思路

SC9600\_1 连接区域 0 和区域 1；SC9600\_4 连接区域 1 和区域 2。

在正常情况下，区域 0 内无法学习到区域 2 的内部路由；区域 2 也无法学习到区域 0 的内部路由和其他区域的路由。此时需要在 SC9600\_1 和 SC9600\_4 间配置虚链路。



注意：

必须先配置虚链路 area 1 virtual-link (A.B.C.D)以后，才能进行虚链路的认证，虚链路的接口属性配置,如 area 1 virtual-link (A.B.C.D) hello-interval 等表。

数据准备

SC9600\_1 的两个接口地址：2001::1/64 和 2003::1/64

SC9600\_2 的两个接口地址：2001::2/64 和 2004::2/64

SC9600\_3 的两个接口地址：2003::3/64

SC9600\_4 的两个接口地址：2004::4/64。

配置步骤

## 1) 基本配置:

```
SC9600_1:
SC9600_1(config)#router ipv6 ospf
SC9600_1(config-ospfv3-1)#router-id 1.1.1.1
SC9600_1(config-ospfv3-1)#quit
SC9600_1(config)#interface vlan 10
SC9600_1(config- vlan-10)#ipv6 ospf area 0
SC9600_1(config- vlan-10)#quit
SC9600_1(config)#
SC9600_1(config)#interface vlan 30
SC9600_1(config- vlan-30)#ipv6 ospf area 0
```

```
SC9600_2
SC9600_2(config)#router ipv6 ospf
SC9600_2(config-ospfv3-1)#router-id 2.1.1.2
SC9600_2(config-ospfv3-1)#quit
SC9600_2(config)#interface vlan 10
SC9600_2(config- vlan-10)#ipv6 ospf area 0
```

```
SC9600_3:
SC9600_3(config)#router ipv6 ospf
SC9600_3(config-ospfv3-1)#router-id 3.1.1.3
SC9600_3(config-ospfv3-1)#quit
SC9600_3(config)#interface vlan 10
SC9600_3(config- vlan-10)#ipv6 ospf area 0
SC9600_3(config- vlan-10)#quit
SC9600_3(config)#
SC9600_3(config)#interface vlan 30
SC9600_3(config- vlan-30)#ipv6 ospf area 0
```

```
SC9600_4:
SC9600_4(config)#router ipv6 ospf
SC9600_4(config-ospfv3-1)#router-id 4.1.1.4
SC9600_4(config-ospfv3-1)#quit
```

```
SC9600_4(config)#interface vlan 30
SC9600_4(config-vlan-30)#ipv6 ospf area 0
SC9600_4(config-vlan-30)#quit
SC9600_4(config)#
SC9600_4(config)#interface vlan 40
SC9600_4(config-vlan-40)#ipv6 ospf area 0
```

## 2) 虚接口基本配置

```
SC9600_1:
SC9600_1(config)#router ipv6 ospf
SC9600_1(config-ospfv3-1)#area 1 virtual-link 4.1.1.4
```

```
SC9600_4:
SC9600_4(config)#router ospf
SC9600_4(config-ospfv3-1)#area 1 virtual-link 1.1.1.1
```

## 3) 虚接口其他配置



注意：

这里的配置都是在配了步骤 2 的虚接口基本配置后，才能进行配置表。

---

```
SC9600_1:
SC9600_1(config)#router ospf
SC9600_1(config-ospf-1)#area 1 virtual-link 4.1.1.4 hello-interval 15
SC9600_1(config-ospf-1)#area 1 virtual-link 4.1.1.4 dead-interval 60
SC9600_1(config-ospf-1)#area 1 virtual-link 4.1.1.4 retransmit-interval 10
SC9600_4:
SC9600_4(config)#router ospf
SC9600_4(config-ospf-1)#area 1 virtual-link 1.1.1.1 hello-interval 15
SC9600_4(config-ospf-1)#area 1 virtual-link 1.1.1.1 dead-interval 60
SC9600_4(config-ospf-1)#area 1 virtual-link 1.1.1.1 retransmit-interval 10
```

## 验证配置结果

进行上述配置后，SC9600\_1 和 SC9600\_4 建立虚链路。

### 4.5.3.5 配置 BFD 功能

#### 组网要求

本案例的任务是完成 OSPFv3 BFD 功能的配置，通过该配置熟悉 OSPFv3 BFD 功能的配置过程，拓扑图如图 4-34所示。

#### 组网图

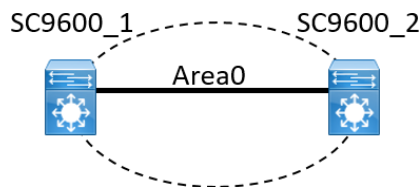


图 4-34 BFD 功能案例拓扑图

#### 配置思路

2 个设备都运行 OSPFv3，并将有个都配置为区域 0。

#### 数据准备

SC9600\_1 的两个接口地址：2001::1/64 和 2003::1/64

SC9600\_2 的两个接口地址：2001::2/64 和 2004::2/64

SC9600\_3 的两个接口地址：2003::3/64

SC9600\_4 的两个接口地址：2004::4/64。

#### 配置步骤

1) 基本配置：

SC9600\_1:

```
SC9600_1(config)#router ipv6 ospf
SC9600_1(config-ospfv3-1)#router-id 1.1.1.1
SC9600_1(config-ospfv3-1)#quit
SC9600_1(config)#interface vlan 10
SC9600_1(config- vlan-10)#ipv6 ospf area 0
SC9600_1(config- vlan-10)#quit
```

SC9600\_2:

```
SC9600_2(config)#router ipv6 ospf
SC9600_2(config-ospfv3-1)#router-id 2.1.1.2
SC9600_2(config-ospfv3-1)#quit
SC9600_2(config)#interface vlan 10
SC9600_2(config-vlan-10)#ipv6 ospf area 0
SC9600_2(config-vlan-10)#quit
```

#### 2) BFD 配置:

```
SC9600_1:
SC9600_1(config)#interface vlan 4
SC9600_1(config-vlan-10)#bfd enable
SC9600_1(config-vlan-10)#ipv6 ospf bfd enable
SC9600_2:
SC9600_2(config)#interface vlan 4
SC9600_2(config-vlan-10)#bfd enable
SC9600_2(config-vlan-10)#ipv6 ospf bfd enable
```

#### 验证配置结果

```
SC9600_1#sho ipv6 ospf bfd session
  OSPF Process 1
  NeighborAddress      NeighborID           BFDState
  fe80::b8:2          2.1.1.2             UP
SC9600_2#sho ipv6 ospf bfd session
  OSPF Process 1
  NeighborAddress      NeighborID           BFDState
  fe80::b8:1          1.1.1.1             UP
```

### 4.5.3.6 配置 GR 功能

#### 组网要求

本案例的任务是完成 OSPFv3 GR 功能的配置, 通过该配置熟悉 OSPFv3 GR 功能的配置过程, 拓扑图如图 4-35所示。

#### 组网图

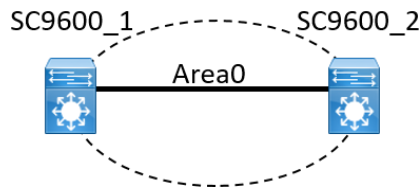


图 4-35 GR 功能案例拓扑图

### 配置思路

2 个设备都运行 OSPFv3，并将有个都配置为区域 0。

测试 GR 重启需要 2 台设备，一台为 GR 重启者，一台为 GR 帮助者。GR 测试重启者采用双主控，拔插卡的方式测试。帮助者无限制。

### 数据准备

SC9600\_1 的两个接口地址：2001::1/64 和 2003::1/64

SC9600\_2 的两个接口地址：2001::2/64 和 2004::2/64

SC9600\_3 的两个接口地址：2003::3/64

SC9600\_4 的两个接口地址：2004::4/64。

### 配置步骤

1) 拓扑同图 4-35，基本配置同4.5.3.1 配置 OSPFv3 基本功能。

2) GR 配置

SC9600\_1:

```
SC9600_1(config)#router ipv6 ospf
```

```
SC9600_1(config-ospfv3-1)# graceful-restart
```

```
SC9600_1(config-ospfv3-1)# graceful-restart period 60
```

SC9600\_2:

```
SC9600_2(config)#router ipv6 ospf
```

```
SC9600_2(config-ospfv3-1)# graceful-restart helper
```

### 验证配置结果

采用插拔卡进行测试，GR 重启者和 GR 帮助者上的配置以后，将 GR 重启者的主用主控拔掉，这时设备间原有的流量应不发生中断。

## 4.6 BGP 配置

### 4.6.1 BGP 简介

#### 4.6.1.1 产生背景

BGP 协议主要用于控制路由的传播和选择最佳路由。

BGP (Border Gateway Protocol) 是一种用于自治系统 AS (Autonomous System) 之间的动态路由协议。早期发布的三个版本分别是 BGP-1 (RFC1105)、BGP-2 (RFC1163) 和 BGP-3 (RFC1267)，当前使用的版本是 BGP-4 (RFC4271)。

BGP-4 作为事实上的 Internet 外部路由协议标准，被广泛应用于 ISP (Internet Service Provider) 之间。

#### 4.6.1.2 协议特点

BGP 特性描述如下：

- BGP 是一种外部网关协议 (EGP)，与 OSPF、RIP 等内部网关协议 (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 支持无类别域间路由 CIDR (Classless Inter-Domain Routing)。
- 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。

BGP 在交换机上以下列两种方式运行：

- IBGP (Internal BGP)
- EBGP (External BGP)

当 BGP 运行于同一自治系统内部时，被称为 IBGP；当 BGP 运行于不同自治系统之间时，称为 EBGP。



### 4.6.1.3 基本概念

BGP-4 提供了一套新的机制支持无类域间路由。这些机制包括支持网络前缀的广播、取消 BGP 网络中“类”的概念。BGP-4 也引入机制支持路由聚合,包括 AS 路径的聚合。这些改变为建议的超网方案提供了支持。

几种主要的路由属性

- 源 (Origin) 属性
- AS 路径 (AS\_Path) 属性
- 下一跳 (Next\_Hop) 属性
- MED (Multi-Exit-Discriminator)
- 本地优先 (Local\_Pref) 属性
- 团体 (Community) 属性

### 4.6.1.4 BGP4 技术介绍

#### 4.6.1.4.1 BGP4 邻居

BGP 邻居又称为对等体,分为两种。如果两个交换 BGP 报文的对等体属于不同的自治系统,那么这两个对等体就是 EBGP 对等体(External BGP)。如果两个交换 BGP 报文的对等体属于同一个自治系统,那么这两个对等体就是 IBGP 对等体体(Internal BGP)。一个 AS 内的不同边界路由器之间也要建立 BGP 连接,只有这样才能实现路由信息在整个 AS 内的传递。

IBGP 对等体之间不一定是物理上直连的但必须保证逻辑上全连接。EBGP 对等体之间在绝大多数情况下是有物理上的直连链路的但是如果实在无法实现也可以配置逻辑链接。图 1 显示了 BGP 邻居的例子,图中,AS100 内的 R1 和 R3 构成 IBGP 邻居,R2 和 R3 也构成 IBGP 邻居,而 AS100 的 R3 和 AS200 的 R4 构成 EBGP 邻居。

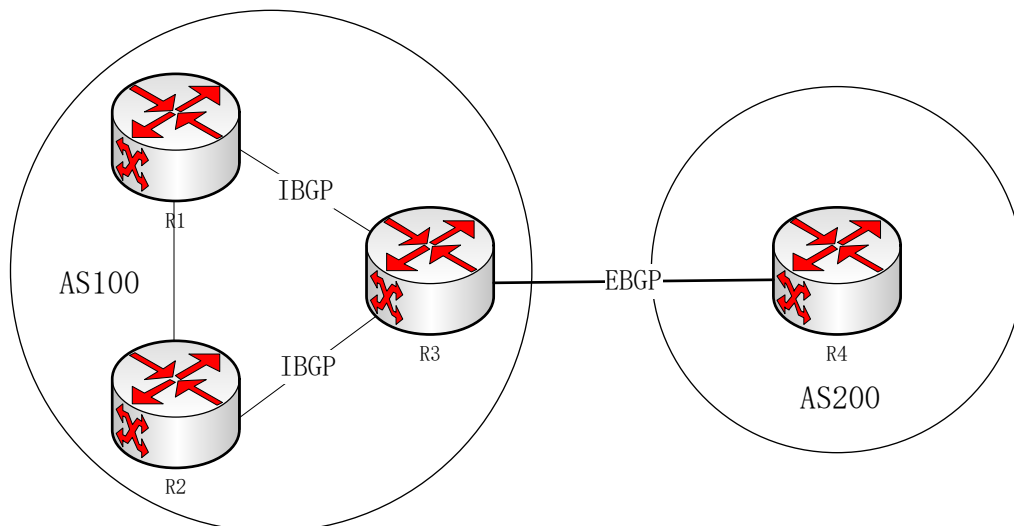


图 4-36 BGP 邻居

BGP 把从 EBGP 获得的路由向它所有的 BGP 对等体通告，包括 IBGP 和 EBGP，而把从 IBGP 获得的路由不向它的 IBGP 对等体通告，向 EBGP 通告时要保证 IGP 同 BGP 同步。同步是指 BGP 一直要等到 IGP 在本 AS 中传播了同一条路由后，再给其它各 AS 通告这条路由。也就是说在通告给其它 AS 一条路由时先要保证本 AS 内部的路由器要知道该路由。

#### 4.6.1.4.2 BGP4 路由通告

一条路由在一般情况下是从 AS 内部产生的，它由某种内部路由协议发现和计算传递到自治系统的边界，由自治系统边界路由器(ASBR)通过 EBGP 连接传播到其它自治系统中。

路由在传播过程中可能会经过若干个自治系统，这些自治系统称为过渡自治系统。若这个自治系统有多个边界路由器，这些路由器之间运行 IBGP 来交换路由信息。这时内部的路由器并不需要知道这些外部路由，它们只需要在边界路由器之间维护 IP 连通性。路由到达自治系统边界后，若内部路由器需要知道这些外部路由，ASBR 可以将路由引入内部路由协议。外部路由的数量是很大的，通常会超出内部路由器的处理能力，因此引入外部路由时一般需要过滤或聚合以减少路由的数量，极端的情况是使用默认路由。

图 2 显示了 BGP 选路时的步骤，我们看到 BGP 并没有计算路由，而是根据特定的策略选择路由。

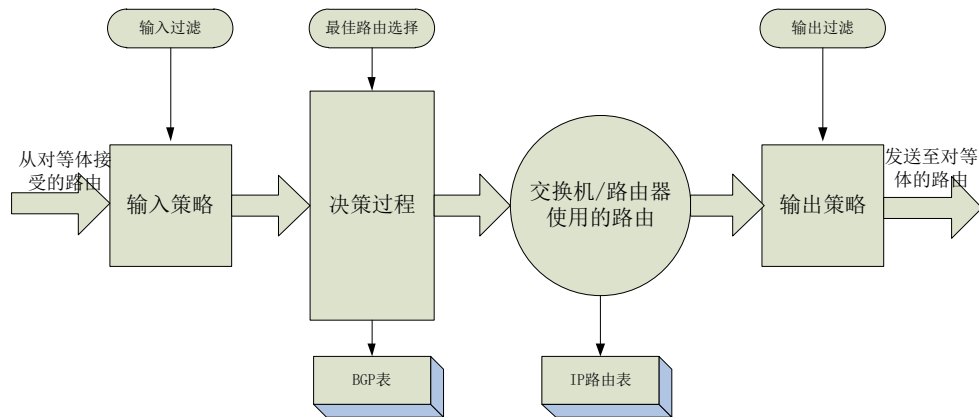


图 4-37 BGP 路由选择过程

#### 4.6.1.4.3 BGP4 消息

BGP 协议包含以下消息：Open 消息，KeepAlive 消息，Update 消息，Notification 消息。所有消息均使用 TCP 作为传输协议。

##### 1. Open 消息

Open 消息是 BGP 邻居使用的 TCP 连接建立之后的第一个消息，其内容包括当前的协议版本，自治系统，路由器标识符，以及一些可选参数。如果对方对消息中的某些参数不能达成一致，则无法建立 BGP 邻居。

##### 2. KeepAlive 消息

一旦双方对 Open 消息的内容达成一致，则开始周期性发送 KeepAlive 消息，此消息用于检测邻居的状态，一定时间内没有收到邻居发送的 KeepAlive 消息，则认为邻居发生故障。

##### 3. Update 消息

Update 消息用于承载路由信息，包括路由的各种属性，BGP 使用这个消息向邻居通告路由信息。

##### 4. Notification 消息

一旦 BGP 运行过程中发生了差错，就会发送 Notification 消息，消息中指明了差错的原因。

#### 4.6.1.4.4 BGP4 属性

BGP 为路由定义了大量的属性以更详细地描述路由，在选路的过程中，BGP 需要对路由的属性作出判断，以选择符合特定策略要求的路由。

## 1. ORIGIN

ORIGIN 属性规定了路径信息的起源。可以取以下的值：

IGP—网络可达信息在原始自治系统的内部。

EGP—通过 EGP 得到网络可达信息

INCOMLETE—通过其他方式获得网络可达信息

## 2. AS-PATH

AS-PATH 由自治系统路径分片组成。每个自治系统路径分片由〈路径分片类型，路径分片长度，路径分片值〉的组合体组成。路径分片类型是个 1 字节长的域，具有以下规定的值：

(1) AS-SET：路由经过的一系列无序的自治系统。

(2) AS-SEQUENCE：路由经过的一系列有序的自治系统。

路径分片长度是个 1 字节长的域，包含路径分片值域中的自治系统数目。路径分片值域包含一个或更多的自治系统号，每个都封装在 2 字节长的域中。

## 3. NEXT-HOP

NEXT-HOP 规定了边界路由器的 IP 地址，该地址被用做寻路时下一跳的 IP 地址。

## 4. MULTI-EXIT-DISC

一个四比特的非 0 整数。BGP 发起者执行决策处理来区别到邻居自治系统的多路径时用到该特性的值。

## 5. LOCAL-PREF

一个四比特非 0 整数。BGP 参与者用它来通知自治系统中的其它 BGP 参与者。

## 6. ATOMIC-AGGREGATE

BGP 参与者用它通知其它 BGP 参与者本地系统选择了一个相对不明确的路由而不是比较明确的路由。

## 7. AGGREGATOR

包含形成聚合路由的最后一个自治系统号（用两字节封装），跟在后面的是形成聚合路由的 BGP 参与者的 IP 地址。（用四字节封装）。

#### 4.6.1.4.5 BGP4 选择路由策略

1. 优选本地优先级（Local\_Pref）最高的路由；
2. 优选聚合路由（聚合路由优先级高于非聚合路由）；
3. 优选 AS 路径（AS\_Path）最短的路由；
4. 比较 Origin 属性，依次选择 Origin 类型为 IGP、EGP、Incomplete 的路由；
5. 优选 MED 值最低的路由；
6. 优选从 EBGP 学来的路由（EBGP 路由优先级高于 IBGP 路由）；
7. 优选 AS 内部 IGP 的 Metric 最低的路由；
8. 优选 Router ID 最小的交换机发布的路由；
9. 比较对等体的 IP Address，优选从具有较小 IP Address 的对等体学来的路由。

#### 4.6.1.4.6 BGP4 发布路由策略

1. 存在多条活跃路由时，BGP 发言者（BGP Speaker）只将最优路由发布给对等体；
2. BGP 发言者只把自己使用的路由发布给对等体；
3. BGP 发言者从 EBGP 获得的路由会向它所有 BGP 对等体发布，但不会向通告该路由的对等体发布（包括 EBGP 对等体和 IBGP 对等体）；
4. BGP 发言者从 IBGP 获得的路由不向它的 IBGP 对等体发布；
5. BGP 发言者从 IBGP 获得的路由发布给它的 EBGP 对等体（在不使能 BGP 与 IGP 同步特性的情况下）；
6. 连接一旦建立，BGP 发言者将把自己所有 BGP 路由发布给新对等体。

#### 4.6.1.4.7 BGP4 路由聚合

在大规模的网络中，BGP 路由表十分庞大，使用路由聚合（Routes Aggregation）可以大大减小路由表的规模。

路由聚合实际上是将多条路由合并的过程。这样 BGP 在向对等体通告路由时，可以只通告聚合后的路由，而不是将所有体的具体路由都通告出去。

#### 4.6.1.4.8 BGP4 的 IBGP 和 IGP 同步

同步是指 IBGP 和 IGP 之间的同步，其目的是为了避免出现误导外部 AS 路由器的现象。

如果设置了同步特性，在 IBGP 路由加入路由表并发布给 EBGP 对等体之前，会先检查 IGP 路由表。只有在 IGP 也知道这条 IBGP 路由时，它才会被加入到路由表，并发布给 EBGP 对等体。

在下面的情况中，可以安全地关闭同步特性。

- 本 AS 不是过渡 AS
- 本 AS 内所有交换机建立 IBGP 全连接

#### 4.6.1.4.9 BGP4 团体

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过滤器过滤自定义扩展团体属性，以便更为灵活的控制路由策略。

#### 4.6.1.4.10 BGP4 路由反射器

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  $n$  台交换机，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，其中一台交换机作为路由反射器 RR (Route Reflector)，其它交换机作为客户机 (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。

#### 4.6.1.4.11 BGP4 联盟

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：从非联盟向联盟方案转变时，要求交换机重新进行配置，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。

#### 4.6.1.4.12 BGP4 的 MP-BGP

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 MP-BGP，目前的 MP-BGP 标准是 RFC2858（Multiprotocol Extensions for BGP-4，BGP-4 的多协议扩展）。

MP-BGP 前向兼容，即支持 BGP 扩展的交换机与不支持 BGP 扩展的交换机可以互通。

##### 1. MP-BGP 的扩展属性

BGP-4 使用的报文中，与 IPv4 相关的三条信息都由 Update 报文携带，这三条信息分别是：NLRI、路径属性中的 Next\_Hop、路径属性中的 Aggregator（该属性中包含形成聚合路由的 BGP 发言者的 IP 地址）。

为实现对多种网络层协议的支持，BGP-4 需要将网络层协议的信息反映到 NLRI 及 Next\_Hop。MP-BGP 中引入了两个新的路径属性：

**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。

这两种属性都是可选非过渡（Optional non-transitive）的，因此，不提供多协议能力的 BGP 发言者将忽略这两个属性的信息，不把它们传递给其它邻居。

##### 2. 地址族

BGP 采用地址族（Address Family）来区分不同的网络层协议，关于地址族的一些取值可以参考 RFC1700（Assigned Numbers）。MP-BGP 扩展应用，包括对 VPN 的扩展、对 IPv6 的扩展等，不同的扩展应在各自的地址族视图下配置。

#### 4.6.1.4.13 BFD for BGP 特性

在 IPv4 中使用 BFD（Bidirectional Forwarding Detection）为 BGP 协议提供更快速的链路故障检测。

BFD 能够快速检测到 BGP 对等体间的链路故障，并报告给 BGP 协议，从而实现 BGP 路由的快速收敛。

#### 4.6.1.4.14 BGP GR

当 BGP 协议重启时会导致对等体关系重新建立和转发中断,使能平滑重启 GR(Graceful Restart) 功能后可以避免流量中断。

### 4.6.2 BGP 配置

#### 4.6.2.1 配置 BGP4 的基本功能

##### 目的

本节介绍如何配置 BGP4 的基本功能。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
进入或创建 BGP 节点	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图;</li> <li>2. 执行命令 <code>router bgp AS-id</code>, 进入 BGP 配置视图</li> </ol>	<b>AS-id:</b> BGP 自制域 ID, 整数形式, 取值范围为 1-65535
指定 BGP 的 router id	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图;</li> <li>2. 执行命令 <code>router bgp N</code>, 进入 BGP 配置视图, 其中 N 代表 BGP 自制域 ID</li> <li>3. 执行命令 <code>router-id router-id</code></li> </ol>	<b>Router-id:</b> 路由器 ID, 需为本地网络已配置的 IP 地址
恢复 BGP 的 router id 为默认值	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图;</li> <li>2. 执行命令 <code>router bgp N</code>, 进入 BGP 配置视图, 其中 N 代表 BGP 自制域 ID</li> <li>3. 执行命令 <code>no router-id</code></li> </ol>	-
创建 BGP 邻居	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图;</li> <li>2. 执行命令 <code>router bgp N</code>, 进入 BGP 配置视图, 其中 N 代表 BGP 自制域 ID</li> <li>3. 执行命令 <code>neighbor neighbor-address remote-as AS-id</code></li> </ol>	<b>Neighbor-address:</b> 邻居 IP 地址, 点分十进制形式, 如: (A.B.C.D), 其中 A~D 为 0~255 十进制数。或者 IPV6 地址包括 128 比特, 由使用冒号分隔的 16 比特的十六进制数表示; <b>AS-id:</b> BGP 自制域 ID, 整数形式, 取值范围为 1-65535



目的	步骤	参数说明
删除 BGP 邻居	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>router bgp N</code>, 进入 BGP 配置视图, 其中 N 代表 BGP 自制域 ID</li> <li>3. 执行命令 <code>no neighbor neighbor-address</code></li> </ol>	<p><b>Neighbor-address:</b> 邻居 IP 地址, 点分十进制形式, 如: (A.B.C.D), 其中 A~D 为 0~255 十进制数。或者 IPV6 地址包括 128 比特, 由使用由冒号分隔的 16 比特的十六进制数表示</p>
关闭 BGP 邻居	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>router bgp N</code>, 进入 BGP 配置视图, 其中 N 代表 BGP 自制域 ID</li> <li>3. 执行命令 <code>neighbor neighbor-address shutdown n</code></li> </ol>	<p><b>Neighbor-address:</b> 邻居 IP 地址, 点分十进制形式, 如: (A.B.C.D), 其中 A~D 为 0~255 十进制数。或者 IPV6 地址包括 128 比特, 由使用由冒号分隔的 16 比特的十六进制数表示</p>
删除关闭 BGP 邻居	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>router bgp N</code>, 进入 BGP 配置视图, 其中 N 代表 BGP 自制域 ID</li> <li>3. 执行命令 <code>no neighbor neighbor-address shutdown n</code></li> </ol>	<p><b>Neighbor-address:</b> 邻居 IP 地址, 点分十进制形式, 如: (A.B.C.D), 其中 A~D 为 0~255 十进制数。或者 IPV6 地址包括 128 比特, 由使用由冒号分隔的 16 比特的十六进制数表示</p>
重启 BGP 邻居	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>router bgp N</code>, 进入 BGP 配置视图, 其中 N 代表 BGP 自制域 ID</li> <li>3. 执行命令 <code>neighbor neighbor-address restart</code></li> </ol>	<p><b>Neighbor-address:</b> 邻居 IP 地址, 点分十进制形式, 如: (A.B.C.D), 其中 A~D 为 0~255 十进制数。或者 IPV6 地址包括 128 比特, 由使用由冒号分隔的 16 比特的十六进制数表示</p>
配置邻居的 MD5 验证	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>router bgp N</code>, 进入 BGP 配置视图, 其中 N 代表 BGP 自制域 ID</li> <li>3. 执行命令 <code>neighbor neighbor-address password password</code></li> </ol>	<p><b>Neighbor-address:</b> 邻居 IP 地址, 点分十进制形式, 如: (A.B.C.D), 其中 A~D 为 0~255 十进制数。或者 IPV6 地址包括 128 比特, 由使用由冒号分隔的 16 比特的十六进制数表示；</p> <p><b>Password:</b> 对等体密码, 最大支持 80 个字符。</p>
删除邻居的 MD5 验证	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>router bgp N</code>, 进入 BGP 配置视图, 其中 N 代表 BGP 自制域 ID</li> <li>3. 执行命令 <code>no neighbor neighbor-address password password</code></li> </ol>	<p><b>Neighbor-address:</b> 邻居 IP 地址, 点分十进制形式, 如: (A.B.C.D), 其中 A~D 为 0~255 十进制数。或者 IPV6 地址包括 128 比特, 由使用由冒号分隔的 16 比特的十六进制数表示；</p> <p><b>Password:</b> 对等体密码, 最大支持 80 个字符。</p>

目的	步骤	参数说明
配置邻居的最大保持时间和向邻居发送 keepalive 的间隔	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图;</li> <li>2. 执行命令 <code>router bgp N</code>, 进入 BGP 配置视图, 其中 N 代表 BGP 自制域 ID</li> <li>3. 执行命令 <code>neighbor neighbor-address keepalive-timer (keepalive-timer  default) hold-timer (hold-timer  default)</code></li> </ol>	<p><b>Neighbor-address:</b> 邻居 IP 地址, 点分十进制形式, 如: (A.B.C.D), 其中 A~D 为 0~255 十进制数。或者 IPV6 地址包括 128 比特, 由使用由冒号分隔的 16 比特的十六进制数表示;</p> <p><b>Keepalive-timer:</b> 保活时间, 整数形式, 取值范围为 1-21845, 单位为秒, 默认为 90 秒;</p> <p><b>Hold-timer:</b> 连接保持时间, 整数形式, 取值范围为 3-65535, 单位为秒, 默认为 30 秒</p>
指定邻居的更新源地址	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图;</li> <li>2. 执行命令 <code>router bgp N</code>, 进入 BGP 配置视图, 其中 N 代表 BGP 自制域 ID</li> <li>3. 执行命令 <code>neighbor neighbor-address update-source source-address</code></li> </ol>	<p><b>Neighbor-address:</b> 邻居 IP 地址, 点分十进制形式, 如: (A.B.C.D), 其中 A~D 为 0~255 十进制数。或者 IPV6 地址包括 128 比特, 由使用由冒号分隔的 16 比特的十六进制数表示;</p> <p><b>source-address:</b> 邻居的本地连接 IPV4 或者 IPV6 地址, 即源地址, 点分十进制形式, 如: (A.B.C.D), 其中 A~D 为 0~255 十进制数。或者 IPV6 地址包括 128 比特, 由使用由冒号分隔的 16 比特的十六进制数表示</p>
删除邻居的更新源地址	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图;</li> <li>2. 执行命令 <code>router bgp N</code>, 进入 BGP 配置视图, 其中 N 代表 BGP 自制域 ID</li> <li>3. 执行命令 <code>no neighbor neighbor-address update-source source-address</code></li> </ol>	<p><b>Neighbor-address:</b> 邻居 IP 地址, 点分十进制形式, 如: (A.B.C.D), 其中 A~D 为 0~255 十进制数。或者 IPV6 地址包括 128 比特, 由使用由冒号分隔的 16 比特的十六进制数表示;</p> <p><b>Source-address:</b> 邻居的本地连接 IPV4 或者 IPV6 地址, 即源地址, 点分十进制形式, 如: (A.B.C.D), 其中 A~D 为 0~255 十进制数。或者 IPV6 地址包括 128 比特, 由使用由冒号分隔的 16 比特的十六进制数表示</p>
检测邻居的有效 ttl 跳数	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图;</li> </ol>	<p><b>Neighbor-address:</b> 邻居 IP 地址, 点分十进制形式, 如:</p>

目的	步骤	参数说明
	2. 执行命令 <code>router bgp N</code> , 进入 BGP 配置视图, 其中 N 代表 BGP 自制域 ID 3. 执行命令 <code>neighbor neighbor-address valid-ttl-hops hop</code> 或 <code>neighbor neighbor-address valid-ttl-hops default</code>	(A.B.C.D), 其中 A~D 为 0~255 十进制数。或者 IPV6 地址包括 128 比特, 由使用由冒号分隔的 16 比特的十六进制数表示; Hop: 指定合法的 TTL 跳数值, 整数形式, 取值范围是 1~255, 默认值为 255
更改邻居的 AS 号	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图; 2. 执行命令 <code>router bgp N</code> , 进入 BGP 配置视图, 其中 N 代表 BGP 自制域 ID 3. 执行命令 <code>neighbor neighbor-address ebgp AS-id</code>	Neighbor-address: 邻居 IP 地址, 点分十进制形式, 如: (A.B.C.D), 其中 A~D 为 0~255 十进制数。或者 IPV6 地址包括 128 比特, 由使用由冒号分隔的 16 比特的十六进制数表示; AS-id: BGP 自制域 ID, 整数形式, 取值范围为 1-65535

#### 4.6.2.2 配置 BGP4 的路由的发布

##### 目的

本节介绍如何配置 BGP4 的路由的发布。

##### 过程

根据不同目的, 执行相应步骤, 具体参见下表。

目的	步骤	参数说明
配置路由聚合, 并指定是只发送聚合后的路由或是聚合后的和未聚合的都发送	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图; 2. 执行命令 <code>router bgp AS-id</code> , 进入 BGP 配置视图 3. 执行命令 <code>aggregate aggregate-address mask-length (summaryonly all)</code>	Aggregate-address: 聚合 IP 地址, 点分十进制形式, 如: (A.B.C.D), 其中 A~D 为 0~255 十进制数。或者 IPV6 地址包括 128 比特, 由使用由冒号分隔的 16 比特的十六进制数表示; Mask-length: IP 地址掩码长度, 整数形式, 取值范围是 0~32(IPV 4) 或者 0~128(IPV6); Summaryonly all: 表示是只发送聚合后的路由, 还是聚合路由与具体路由一起发送
配置管理路由聚合的状态, 使能或关闭	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图; 2. 执行命令 <code>router bgp AS-id</code> , 进入 BGP	Aggregate-address: 聚合 IP 地址, 点分十进制形式, 如: (A.B.C.D), 其中 A~D 为 0~255

目的	步骤	参数说明
	配置视图 3. 执行命令 <code>aggregate aggregate-address mask-length adminstatus (up down)</code>	十进制数。或者 IPV6 地址包括 128 比特，由使用冒号分隔的 16 比特的十六进制数表示； Mask-length: IP 地址掩码长度，整数形式，取值范围是 0~32(IPV 4) 或者 0~128(IPV6)； Up down: 表示管理状态
删除路由聚合	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图； 2. 执行命令 <code>router bgp AS-id</code> , 进入 BGP 配置视图 3. 执行命令 <code>no aggregate aggregate-address mask-length</code>	Aggregate-address: 聚合 IP 地址，点分十进制形式，如：(A.B.C.D)，其中 A~D 为 0~255 十进制数。或者 IPV6 地址包括 128 比特，由使用冒号分隔的 16 比特的十六进制数表示； Mask-length: IP 地址掩码长度，整数形式，取值范围是 0~32(IPV 4) 或者 0~128(IPV6)
将发送给邻居路由的下一跳更改为本地地址	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图； 2. 执行命令 <code>router bgp AS-id</code> , 进入 BGP 配置视图 3. 执行命令 <code>aggregate aggregate-address next-hop-local</code>	Aggregate-address: 聚合 IP 地址，点分十进制形式，如：(A.B.C.D)，其中 A~D 为 0~255 十进制数。或者 IPV6 地址包括 128 比特，由使用冒号分隔的 16 比特的十六进制数表示
删除将发送给邻居路由的下一跳更改为本地地址的配置	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图； 2. 执行命令 <code>router bgp AS-id</code> , 进入 BGP 配置视图 3. 执行命令 <code>no aggregate aggregate-address next-hop-local</code>	Aggregate-address: 聚合 IP 地址，点分十进制形式，如：(A.B.C.D)，其中 A~D 为 0~255 十进制数。或者 IPV6 地址包括 128 比特，由使用冒号分隔的 16 比特的十六进制数表示
配置邻居的路由刷新能力	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图； 2. 执行命令 <code>router bgp AS-id</code> , 进入 BGP 配置视图 3. 执行命令 <code>aggregate aggregate-address route-refresh</code>	Aggregate-address: 聚合 IP 地址，点分十进制形式，如：(A.B.C.D)，其中 A~D 为 0~255 十进制数。或者 IPV6 地址包括 128 比特，由使用冒号分隔的 16 比特的十六进制数表示
删除邻居的路由刷新能力	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图； 2. 执行命令 <code>router bgp AS-id</code> , 进入 BGP 配置视图 3. 执行命令 <code>no aggregate aggregate-address route-refresh</code>	Aggregate-address: 聚合 IP 地址，点分十进制形式，如：(A.B.C.D)，其中 A~D 为 0~255 十进制数。或者 IPV6 地址包括 128 比特，由使用冒号分隔的 16 比特的十六进制数表示

目的	步骤	参数说明
发布指定的路由	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图;</li> <li>2. 执行命令 <code>router bgp AS-id</code>, 进入 BGP 配置视图</li> <li>3. 执行命令 <code>network network-address network-mask</code></li> </ol>	<p><b>Network-address:</b> BGP 发布指定的静态网络地址, 点分十进制形式, 如: (A.B.C.D), 其中 A~D 为 0~255 十进制数;</p> <p><b>Network-mask:</b> BGP 发布指定的静态网络地址掩码, 点分十进制形式, 如: (A.B.C.D), 其中 A~D 为 0~255 十进制数。</p>
删除发布的指定路由	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图;</li> <li>2. 执行命令 <code>router bgp AS-id</code>, 进入 BGP 配置视图</li> <li>3. 执行命令 <code>no network network-address network-mask</code></li> </ol>	<p><b>Network-address:</b> BGP 发布指定的静态网络地址, 点分十进制形式, 如: (A.B.C.D), 其中 A~D 为 0~255 十进制数;</p> <p><b>Network-mask:</b> BGP 发布指定的静态网络地址掩码, 点分十进制形式, 如: (A.B.C.D), 其中 A~D 为 0~255 十进制数。</p>
向 BGP 引入静态或直连路由	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图;</li> <li>2. 执行命令 <code>router bgp AS-id</code>, 进入 BGP 配置视图</li> <li>3. 执行命令 <code>redistribute (static connected rip ospf isis)</code></li> </ol>	<p><b>Static connected rip ospf isis :</b> 分别代表静态、直连、rip 协议、ospf 协议、isis 协议路由</p>
根据策略向 BGP 引入静态或直连路由	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图;</li> <li>2. 执行命令 <code>router bgp AS-id</code>, 进入 BGP 配置视图</li> <li>3. 执行命令 <code>redistribute (static connected rip ospf isis) route-policy route-policy-name</code></li> </ol>	<p><b>Route-policy-name:</b> 表示路由策略名, 字符串形式</p>
修改向 BGP 引入静态或直连路由的 med 值	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图;</li> <li>2. 执行命令 <code>router bgp AS-id</code>, 进入 BGP 配置视图</li> <li>3. 执行命令 <code>redistribute (static connected rip ospf isis) med med</code></li> </ol>	<p><b>Med:</b> med 的值, 整数形式, 取值范围是 1-4294967295</p>
删除向 BGP 引入路由	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图;</li> <li>2. 执行命令 <code>router bgp AS-id</code>, 进入 BGP 配置视图</li> <li>3. 执行命令 <code>no redistribute</code></li> </ol>	-

目的	步骤	参数说明
	(static connected rip ospf isis)	
删除根据策略向 BGP 引入路由	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图;</li> <li>2. 执行命令 <code>router bgp AS-id</code>, 进入 BGP 配置视图</li> <li>3. 执行命令 <code>no redistribute (static connected rip ospf isis) route-policy route-policy-name</code></li> </ol>	Route-policy-name: 表示路由策略名, 字符串形式
使能或去使能 IGP 同步功能	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图;</li> <li>2. 执行命令 <code>router bgp AS-id</code>, 进入 BGP 配置视图</li> <li>3. 执行命令 <code>synchronization (enable disable)</code></li> </ol>	-

#### 4.6.2.3 配置 BGP4 的路径属性

##### 目的

本节介绍如何配置 BGP4 的路径属性。

##### 过程

根据不同目的, 执行相应步骤, 具体参见下表。

目的	步骤	参数说明
配置默认 med 值	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图;</li> <li>2. 执行命令 <code>router bgp AS-id</code>, 进入 BGP 配置视图</li> <li>3. 执行命令 <code>default local-med local-med</code> 或 <code>default local-med default</code></li> </ol>	Local-med: 本地 med 属性值, 整数形式, 取值范围是 1-20000, 默认为 100
配置默认 local-preference 值	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图;</li> <li>2. 执行命令 <code>router bgp AS-id</code>, 进入 BGP 配置视图</li> <li>3. 执行命令 <code>default local-preference local-preference</code> 或</li> </ol>	Local-preference : 本地 preference 属性值, 整数形式, 取值范围是 1-4294967295, 默认为 100

目的	步骤	参数说明
	default local-med default	
配置 BGP 的团体属性	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>router bgp AS-id</code>, 进入 BGP 配置视图</li> <li>3. 执行命令 <code>community (community noadvertise noexport) (additive replace none)</code></li> </ol>	<p><b>Community: community</b> 属性范围的值，整数形式，取值范围是 0~4294967295；</p> <p><b>Noadvertise noexport</b>：代表 community 中最常用的两个值，值为 0Xffffff01 和 0Xffffff02，当接收到的路由更新消息中 community 的值为 noadvertise 时，该条路由不再发送给其他的对等体，当值为 noexport 时，该条路由不再发送给外部对等体；</p> <p><b>Additive replace none</b>：发送 community 属性给对方的方式，additive 是将所设置的属性添加在原有属性的后面；replace 是只发送所设置的属性值；none 是不发送 community 属性</p>
删除 BGP 的团体属性	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>router bgp AS-id</code>, 进入 BGP 配置视图</li> <li>3. 执行命令 <code>no community</code></li> </ol>	-
向邻居发送团体属性	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>router bgp AS-id</code>, 进入 BGP 配置视图</li> <li>3. 执行命令 <code>neighbor neighbor-address send-community</code></li> </ol>	<p><b>Neighbor-address</b>: 邻居 IP 地址，点分十进制形式，如：(A.B.C.D)，其中 A~D 为 0~255 十进制数。或者 IPV6 地址包括 128 比特，由使用冒号分隔的 16 比特的十六进制数表示</p>
不向邻居发送团体属性	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>router bgp AS-id</code>, 进入 BGP 配置视图</li> <li>3. 执行命令 <code>no neighbor neighbor-address send-community</code></li> </ol>	<p><b>Neighbor-address</b>: 邻居 IP 地址，点分十进制形式，如：(A.B.C.D)，其中 A~D 为 0~255 十进制数。或者 IPV6 地址包括 128 比特，由使用冒号分隔的 16 比特的十六进制数表示</p>
允许本地 AS 编号重复出现次数	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>router bgp AS-id</code>, 进入 BGP 配置视图</li> </ol>	<p><b>Neighbor-address</b>: 邻居 IP 地址，点分十进制形式，如：(A.B.C.D)，其中 A~D 为 0~255 十进制数。或者 IPV6 地址包括 128 十进制数。或者 IPV6 地址包括 128</p>

目的	步骤	参数说明
	3. 执行命令 <code>neighbor neighbor-address allow-as-loop loop-number</code> 或 <code>neighbor neighbor-address allow-as-loop default</code>	比特，由使用冒号分隔的 16 比特的十六进制数表示； Loop-number: 允许本地 AS 编号重复出现的次数范围，整数形式，取值范围为 1-10，默认为 1
为本端对等体指定一个伪 AS 号	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图； 2. 执行命令 <code>router bgp AS-id</code> , 进入 BGP 配置视图 3. 执行命令 <code>neighbor neighbor-address fake-as fake-as-number</code>	Neighbor-address: 邻居 IP 地址，点分十进制形式，如：(A.B.C.D)，其中 A~D 为 0~255 十进制数。或者 IPV6 地址包括 128 比特，由使用冒号分隔的 16 比特的十六进制数表示； Fake-as-number: 为本端对等体指定的伪 AS 号，整数形式，取值范围为 1-65535
BGP 更新报文时不携带私有自治系统号，仅携带公有 AS 号	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图； 2. 执行命令 <code>router bgp AS-id</code> , 进入 BGP 配置视图 3. 执行命令 <code>neighbor neighbor-address public-as-only</code>	Neighbor-address: 邻居 IP 地址，点分十进制形式，如：(A.B.C.D)，其中 A~D 为 0~255 十进制数。或者 IPV6 地址包括 128 比特，由使用冒号分隔的 16 比特的十六进制数表示

#### 4.6.2.4 配置 BGP4 的路由策略

##### 目的

本节介绍如何配置 BGP4 的路由策略。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置 BGP 全局入或出过滤策略	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图； 2. 执行命令 <code>router bgp AS-id</code> , 进入 BGP 配置视图 3. 执行命令 <code>filter-policy (export  import) route-policy route-policy-name</code>	Export  import: 表示应用到通告/学习的路由更新信息； Route-policy-name: 表示路由策略名，字符串形式
根据协议类型指定 BGP 全局出过滤策略	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图； 2. 执行命令 <code>router bgp AS-id</code> , 进入 BGP 配置视图	Static connected rip ospf isis : 表示静态、直连、rip 协议、ospf 协议、isis 协议路由； Route-policy-name: 表示路由



目的	步骤	参数说明
	3. 执行命令 <code>filter-policy export (static connected rip ospf isis) route-policy route-policy-name</code>	策略名，字符串形式
删除 BGP 全局入或出过滤策略	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图； 2. 执行命令 <code>router bgp AS-id</code> , 进入 BGP 配置视图 3. 执行命令 <code>no filter-policy (export  import ) route-policy route-policy-name</code>	<b>Route-policy-name:</b> 表示路由策略名，字符串形式
删除根据协议类型指定的 BGP 全局出过滤策略	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图； 2. 执行命令 <code>router bgp AS-id</code> , 进入 BGP 配置视图 3. 执行命令 <code>no filter-policy export (static connected rip ospf isis) route-policy route-policy-name</code>	<b>Static connected rip ospf isis :</b> 表示静态、直连、rip 协议、ospf 协议、isis 协议路由； <b>Route-policy-name:</b> 表示路由策略名，字符串形式
针对指定邻居配置入或出路由策略	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图； 2. 执行命令 <code>router bgp AS-id</code> , 进入 BGP 配置视图 3. 执行命令 <code>neighbor neighbor-address route-policy route-policy-name (export  import )</code>	<b>Neighbor-address:</b> 邻居 IP 地址，点分十进制形式，如：(A.B.C.D)，其中 A~D 为 0~255 十进制数。或者 IPV6 地址包括 128 比特，由使用冒号分隔的 16 比特的十六进制数表示； <b>Route-policy-name:</b> 表示路由策略名，字符串形式； <b>Export  import:</b> 表示应用到通告/学习的路由更新信息；
删除针对指定邻居的入或出路由策略	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图； 2. 执行命令 <code>router bgp AS-id</code> , 进入 BGP 配置视图 3. 执行命令 <code>no neighbor neighbor-address route-policy route-policy-name (export  import )</code>	<b>Neighbor-address:</b> 邻居 IP 地址，点分十进制形式，如：(A.B.C.D)，其中 A~D 为 0~255 十进制数。或者 IPV6 地址包括 128 比特，由使用冒号分隔的 16 比特的十六进制数表示； <b>Route-policy-name:</b> 表示路由策略名，字符串形式； <b>Export  import:</b> 表示应用到通告/学习的路由更新信息；

#### 4.6.2.5 配置 BFD for BGP

##### 目的

本节介绍如何配置 BFD for BGP。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
针对邻居使能或去使能 BFD 功能	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>router bgp AS-id</code>, 进入 BGP 配置视图</li> <li>3. 执行命令 <code>neighbor neighbor-address bfd (enable disable)</code></li> </ol>	<b>Neighbor-address:</b> 邻居 IP 地址，点分十进制形式，如：(A.B.C.D)，其中 A~D 为 0~255 十进制数。或者 IPV6 地址包括 128 比特，由使用由冒号分隔的 16 比特的十六进制数表示

#### 4.6.2.6 配置 BGP4 路由反射器

### 目的

本节介绍如何配置 BGP4 路由反射器。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置路由反射器的簇 id	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>router bgp AS-id</code>, 进入 BGP 配置视图</li> <li>3. 执行命令 <code>cluster-id router-id</code></li> </ol>	<b>Router-id:</b> 簇的标记号，点分十进制形式，如：(A.B.C.D)，其中 A~D 为 0~255 十进制数
指定邻居作为反射器的客户端	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>router bgp AS-id</code>, 进入 BGP 配置视图</li> <li>3. 执行命令 <code>neighbor neighbor-address route-reflector-client</code></li> </ol>	<b>Neighbor-address:</b> 邻居 IP 地址，点分十进制形式，如：(A.B.C.D)，其中 A~D 为 0~255 十进制数。或者 IPV6 地址包括 128 比特，由使用由冒号分隔的 16 比特的十六进制数表示
删除路由反射器的簇 id	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>router bgp AS-id</code>, 进入 BGP 配置视图</li> <li>3. 执行命令 <code>no cluster-id router-id</code></li> </ol>	<b>Router-id:</b> 簇的标记号，点分十进制形式，如：(A.B.C.D)，其中 A~D 为 0~255 十进制数
删除邻居作为反射器的客户端	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>router bgp AS-id</code>, 进入 BGP 配置视图</li> </ol>	<b>Neighbor-address:</b> 邻居 IP 地址，点分十进制形式，如：(A.B.C.D)，其中 A~D 为 0~255 十进制数。或者 IPV6 地址包括 128

目的	步骤	参数说明
	3. 执行命令 <code>no neighbor neighbor-address route-reflector-client</code>	比特, 由使用由冒号分隔的 16 比特的十六进制数表示

#### 4.6.2.7 配置 BGP4 联盟

##### 目的

本节介绍如何配置 BGP4 联盟。

##### 过程

根据不同目的, 执行相应步骤, 具体参见下表。

目的	步骤	参数说明
配置联盟的 AS 号	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图;</li> <li>2. 执行命令 <code>router bgp AS-id</code>, 进入 BGP 配置视图</li> <li>3. 执行命令 <code>confederation identifier autonomy-system-number</code></li> </ol>	Autonomy-system-number: 联盟的自治系统号, 整数形式, 取值范围是 1~65535
指定联盟成员的 AS 号	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图;</li> <li>2. 执行命令 <code>router bgp AS-id</code>, 进入 BGP 配置视图</li> <li>3. 执行命令 <code>confederation peer-as PEERASLIST</code></li> </ol>	PEERASLIST: 联盟内部小自治系统的自治系统号, 在联盟内部必须唯一, 取值形式如 1, 3, 5-7
删除联盟的 AS 号	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图;</li> <li>2. 执行命令 <code>router bgp AS-id</code>, 进入 BGP 配置视图</li> <li>3. 执行命令 <code>no confederation identifier autonomy-system-number</code></li> </ol>	Autonomy-system-number: 联盟的自治系统号, 整数形式, 取值范围是 1~65535
删除指定联盟成员	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图;</li> <li>2. 执行命令 <code>router bgp AS-id</code>, 进入 BGP 配置视图</li> <li>3. 执行命令 <code>no confederation peer-as PEERASLIST</code></li> </ol>	PEERASLIST: 联盟内部小自治系统的自治系统号, 在联盟内部必须唯一, 取值形式如 1, 3, 5-7

#### 4.6.2.8 配置 BGP4 GR

##### 目的

本节介绍如何配置 BGP4 GR。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
使能或关闭 BGP 的 GR 功能	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图； 2. 执行命令 <code>router bgp AS-id</code> , 进入 BGP 配置视图 3. 执行命令 <code>graceful-restart (enable disable)</code>	-
配置重建 BGP 会话的最大时间	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图； 2. 执行命令 <code>router bgp AS-id</code> , 进入 BGP 配置视图 3. 执行命令 <code>graceful-restart timer restart restart-time</code> 或 <code>graceful-restart timer restart default</code>	Restart-time: 等待时间范围, 整数形式, 取值范围是 3-600, 单位为秒, 默认为 150 秒
配置重启侧 (Restarting Speaker) 和接收侧 (Receiving Speaker) 等待 End-of-RIB 消息的时间	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图； 2. 执行命令 <code>router bgp AS-id</code> , 进入 BGP 配置视图 3. 执行命令 <code>graceful-restart timer selection-deferral select-time</code> 或 <code>graceful-restart timer selection-deferral default</code>	Select-time: 指定选择等待时间值, 整数形式, 取值范围是 3-3000, 单位为秒, 默认为 600 秒

4.6.2.9 配置 BGP 的地址族

目的

本节介绍如何配置 BGP 的地址族。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
进入 ipv4 单播地址族视图	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图； 2. 执行命令 <code>router bgp AS-id</code> , 进入 BGP	-

目的	步骤	参数说明
	配置视图 3. 执行命令 <code>ipv4-family unicast</code>	
将指定的 VPN 实例与 IPv4 地址族进行关联，进入 BGP-VPN 实例视图	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图； 2. 执行命令 <code>router bgp AS-id</code> ，进入 BGP 配置视图 3. 执行命令 <code>ipv4-family vpn-instance instance-name</code>	Instance-name: BGP-VPN 实例名，字符串形式
进入 BGP-VPNv4 地址族视图	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图； 2. 执行命令 <code>router bgp AS-id</code> ，进入 BGP 配置视图 3. 执行命令 <code>ipv4-family vpnv4</code>	-
地址族节点下使能或去使能地址组	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图； 2. 执行命令 <code>router bgp AS-id</code> ，进入 BGP 配置视图 3. 执行命令 <code>ipv4-family unicast</code> ，进入地址族视图 3. 执行命令 <code>neighbor neighbor-address (enable disable)</code>	Neighbor-address: 邻居 IP 地址，点分十进制形式，如：(A.B.C.D)，其中 A~D 为 0~255 十进制数。或者 IPV6 地址包括 128 比特，由使用由冒号分隔的 16 比特的十六进制数表示

#### 4.6.2.10 配置 BGP4 调试功能

##### 目的

本节介绍如何配置 BGP4 调试功能。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
开启 BGP 的 DEBUG 功能功能	1. 进入特权用户视图； 2. 执行命令 <code>debug bgp (update rib-tree route event tcp packet all prf graceful-restart socket)</code>	-
关闭 BGP 的 DEBUG 功能功能	1. 进入特权用户视图； 2. 执行命令 <code>no debug bgp (update rib-tree route event tcp packet all prf graceful-restart socket)</code>	-

#### 4.6.2.11 查看 BGP4 配置信息

##### 目的

本节介绍如何查看 BGP4 配置信息。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
显示 BGP 的 vpnv4 的路由标签	1. 进入普通用户视图或特权用户视图； 2. 执行命令 <code>show ip bgp vpnv4 route label</code>	-
显示 BGP 的聚合表	1. 进入普通用户视图或特权用户视图； 2. 执行命令 <code>show ip bgp aggregate</code>	-
显示 BGP 的基本配置	1. 进入普通用户视图或特权用户视图； 2. 执行命令 <code>show ip bgp config</code>	
显示 BGP 的所有对等体	1. 进入普通用户视图或特权用户视图； 2. 执行命令 <code>show ip bgp neighbor</code>	
显示 BGP 指定对等体的状态	1. 进入普通用户视图或特权用户视图； 2. 执行命令 <code>show ip bgp neighbor neighbor-address</code>	<b>Neighbor-address</b> : 邻居 IP 地址，点分十进制形式，如：(A.B.C.D)，其中 A~D 为 0~255 十进制数。或者 IPV6 地址包括 128 比特，由使用由冒号分隔的 16 比特的十六进制数表示
显示 BGP 的资源统计信息	1. 进入普通用户视图或特权用户视图； 2. 执行命令 <code>show ip bgp resource</code>	
显示 BGP 的路由表	1. 进入普通用户视图或特权用户视图； 2. 执行命令 <code>show ip bgp route</code>	
显示 BGP 的路	1. 进入普通用户视图或特权用户视图； 2. 执行命令	

目的	步骤	参数说明
由标签	show ip bgp route label	
显示 BGP 的路由统计信息	1. 进入普通用户视图或特权用户视图; 2. 执行命令 show ip bgp summary	
显示 BGP 的 VPN 实例的对等体	1. 进入普通用户视图或特权用户视图; 2. 执行命令 show ip bgp vpn-instance <i>instance-name</i> neighbor	Instance-name : BGP-VPN 实例名, 字符串形式
显示 BGP 的 VPN 实例的路由信息	1. 进入普通用户视图或特权用户视图; 2. 执行命令 show ip bgp vpn-instance <i>instance-name</i> route	Instance-name : BGP-VPN 实例名, 字符串形式
显示 BGP VPNv4 的路由信息	1. 进入普通用户视图或特权用户视图; 2. 执行命令 show ip bgp vpnv4 route	

## 4.6.3 BGP 配置举例

### 4.6.3.1 配置基本 BGP4

#### 组网要求

如图 4-38所示, 所有 SC9600 均运行 BGP 协议, R1、R2 之间建立 EBGP 连接, R2、R3 和 R4 之间建立 IBGP 全连接。

#### 组网图

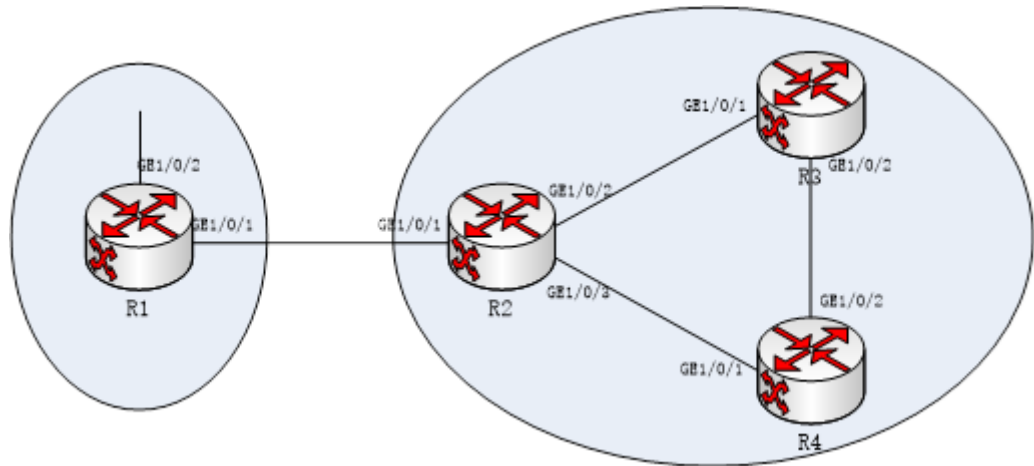


图 4-38 配置 BGP 基本组网图

Switch	接口	对应的 VLAN	IP 地址
R1	GigabitEthernet1/0/1	VLAN 10	192.1.1.2/24
R1	GigabitEthernet1/0/2	VLAN 50	20.1.1.1/8
R2	GigabitEthernet1/0/1	VLAN 10	192.1.1.1/24
R2	GigabitEthernet1/0/2	VLAN 20	10.1.3.1/24
R2	GigabitEthernet1/0/3	VLAN 30	10.1.1.1/24
R3	GigabitEthernet1/0/1	VLAN 20	10.1.3.2/24
R3	GigabitEthernet1/0/2	VLAN 40	10.1.2.1/24
R4	GigabitEthernet1/0/1	VLAN 30	10.1.1.2/24
R4	GigabitEthernet1/0/2	VLAN 40	10.1.2.2/24

#### 配置思路

采用如下的思路配置 BGP 的基本功能：

1. 在 R2、R3 和 R4 间配置 IBGP 连接。
2. 在 R1 和 R2 之间配置 EBGP 连接。
3. 在 R1 通过 network 命令发布路由，查看 R1、R2 和 R3 路由表信息。
4. 在 R2 配置 BGP 引入直连路由，查看 R1 和 R3 路由表信息。

#### 数据准备



为完成此配置例，需准备如下的数据：

各接口所属的 VLAN ID，具体数据如图 4-38 所示。

各 VLAN 接口的 IP 地址，具体数据如图 4-38 所示。

R1 的 Router ID 1.1.1.1，所在的 AS 号 65008。

R2、R3 和 R4 的 router id 分别为 2.2.2.2、3.3.3.3、4.4.4.4，所在的 AS 号 65009。

### 配置步骤

#### 步骤 1 配置 IBGP 连接

配置 R2。

```
R2(config)#router bgp 65009
```

```
R2(config-bgp)#router-id 2.2.2.2
```

```
R2(config-bgp)#neighbor 10.1.1.2 remote-as 65009
```

```
R2(config-bgp)#neighbor 10.1.3.2 remote-as 65009
```

配置 R3。

```
R3(config)#router bgp 65009
```

```
R3(config -bgp)#router-id 3.3.3.3
```

```
R3(config -bgp)#neighbor 10.1.3.1 remote-as 65009
```

```
R3(config -bgp)#neighbor 10.1.2.2 remote-as 65009
```

```
R3(config -bgp)#quit
```

配置 R4。

```
R4(config)#router bgp 65009
```

```
R4(config -bgp)#router-id 4.4.4.4
```

```
R4(config -bgp)#neighbor 10.1.1.1 remote-as 65009
```

```
R4(config -bgp)#neighbor 10.1.2.1 remote-as 65009
```

```
R4(config -bgp)#quit
```

#### 步骤 2 配置 EBGP

配置 R1。

```
R1(config)# router bgp 65008
```

```
R1(config -bgp)#router-id 1.1.1.1
```

```
R1(config -bgp)#neighbor 192.1.1.1 remote-as 65009
```

配置 R2。

```
R2(config -bgp)#neighbor 192.1.1.2 remote-as 65008
```

```
R2(config -bgp)#quit
```

查看 BGP 对等体的连接状态。

```
R1(config)#show ip bgp neighbor
```

步骤 3 配置 R1 发布路由 20.0.0.0/8

配置 R1 发布路由。

```
R1(config -bgp)#network 20.0.0.0 255.0.0.0
```

```
R1(config -bgp)#quit
```

查看 R1 路由表信息。

```
R1(config)#show ip bgp route
```

查看 R2 的路由表。

```
R2(config)#show ip bgp route
```

查看 R3 的路由表。

```
R1(config)#show ip bgp route
```

从路由表可以看出，R3 然学到了 AS65008 中的 20.0.0.0 的路由，但因为下一跳 192.1.1.2 不可达，所以也不是有效路由。

步骤 4 配置 BGP 引入直连路由

配置 R2。

```
R2(config)#router bgp 65009
```

```
R2(config -bgp)#redistribute connect
```

```
R2(config -bgp)#quit
```

查看 R1 的 BGP 路由表。

```
R1(config)#show ip bgp route
```

查看 R3 的路由表。

```
R3(config)#show ip bgp route
```

可以看出，到 20.0.0.0 的路由变为有效路由，下一跳为 R1 的地址。

#### 4.6.3.2 配置 BGP4 与 IGP 交互

##### 组网要求

如图 4-39所示，在 AS65009 内使用 OSPF 作为 IGP 协议，R1 和 R2 建立 EBGP 连接，R3 运行 OSPF 而不运行 BGP。

##### 组网图

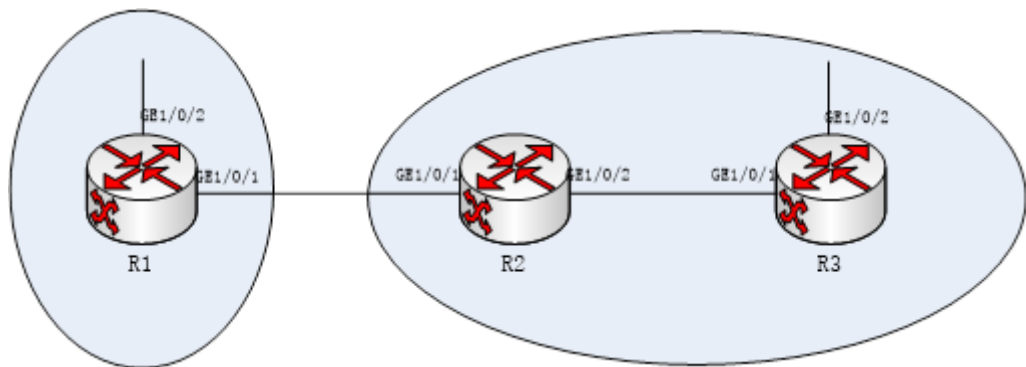


图 4-39 BGP 与 IGP 交互配置组网图

Switch	接口	对应的 VLAN	IP 地址
R1	GigabitEthernet1/0/1	VLAN 10	30.1.1.2/24
R1	GigabitEthernet1/0/2	VLAN 30	20.1.1.1/24
R2	GigabitEthernet1/0/1	VLAN 10	30.1.1.1/24
R2	GigabitEthernet1/0/2	VLAN 20	10.1.1.1/24

R3	GigabitEthernet1/0/1	VLAN 20	10.1.1.2/24
R3	GigabitEthernet1/0/2	VLAN 40	10.1.2.1/24

### 配置思路

采用如下的思路配置 BGP 与 IGP 交互：

1. 在 R2 和 R3 上配置 OSPF 协议。
2. 在 R1 和 R2 上配置 EBGP 连接。
3. 在 R2 配置 BGP 与 OSPF 互相引入，查看路由信息。
4. 在 R2 配置 BGP 路由聚合，简化 BGP 路由表。

### 数据准备

为完成此配置例，需准备如下的数据：

各接口所属的 VLAN ID，具体数据如图 4-39 所示。

各 VLAN 接口的 IP 地址，具体数据如图 4-39 所示。

R1 的 Router ID 1.1.1.1，所在 AS 号 65008。

R2、R3 的 Router ID 分别为 2.2.2.2、3.3.3.3，所在 AS 号 65009。

### 配置步骤

#### 步骤 1 配置 OSPF

配置 R1。

```
R1(config)#router ospf
R1(config-ospf-1)#network 9.1.1.0 255.255.255.0 area 0
R1(config-ospf-1)#quit
```

配置 R2。

```
R1(config)#router ospf
R1(config-ospf-1)#network 9.1.1.0 255.255.255.0 area 0
R1(config-ospf-1)#network 9.1.2.0 255.255.255.0 area 0
R1(config-ospf-1)#quit
```

### 步骤 2 配置 EBGP 连接

配置 R1。

```
R1(config)#router bgp 65008
```

```
R1(config-bgp)#router-id 1.1.1.1
```

```
R1(config-bgp)#neighbor 3.1.1.1 remote-as 65009
```

```
R1(config-bgp)#network 8.1.1.0 255.255.255.0
```

```
R1(config-bgp)#quit
```

配置 R2。

```
R2(config)#router bgp 65009
```

```
R2(config-bgp)#router-id 2.2.2.2
```

```
R2(config-bgp)#neighbor 3.1.1.2 remote-as 65008
```

### 步骤 3 配置 BGP 与 IGP 交互

在 R2 配置 BGP 引入 OSPF 路由。

```
R2(config-bgp)#redistribute ospf
```

```
R2(config-bgp)#quit
```

查看 R1 的路由表。

```
R1(config)#show ip bgp route
```

在 R2 配置 OSPF 引入 BGP 路由。

```
R2(config)#router ospf
```

```
R2(config-ospf-1)#redistribute bgp
```

```
R2(config-ospf-1)#quit
```

查看 R3 的路由表。

```
R3(config)#show ip route
```

### 步骤 4 配置路由聚合

配置 R2。

```
R2(config)#router bgp 65009
```

```
R2(config-bgp)#aggregate 9.0.0.0 8 summaryonly
```

```
R2(config-bgp)#aggregate 9.0.0.0 8 adminstatus up
```

```
R2(config-bgp)#quit
```

查看 R1 的 BGP 路由表。

```
R1(config)#show ip bgp route
```

#### 4.6.3.3 配置 BGP4 路由反射器

##### 组网要求

如图 4-40所示，R1 为非客户机，R2 是 Cluster1 的路由反射器，R4 和 R5 是它的两个客户机。由于他们两者之间建立了 IBGP 连接，所以不需要在客户机之间反射路由。R3 为 Cluster2 的路由反射器，R6、R7 和 R8 是它的客户机。要求使用对等体组来简化配置和管理。

##### 组网图

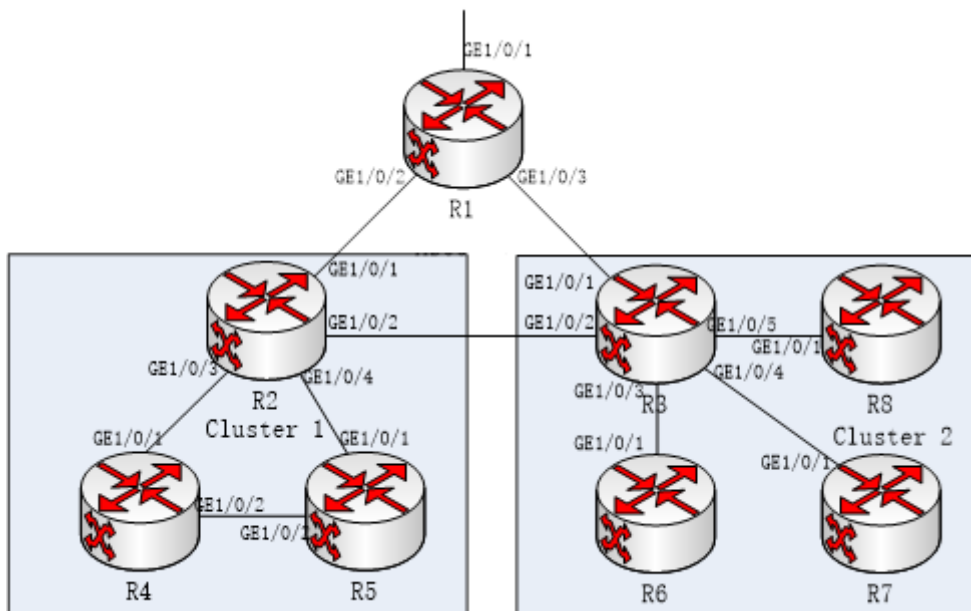


图 4-40 配置 BGP 路由反射器组网图

Switch	接口	对应的 VLAN	IP 地址
--------	----	----------	-------

R1	GigabitEthernet 1/0/1	VLAN 10	10.1.1.2/24
R1	GigabitEthernet 1/0/2	VLAN 30	10.1.3.2/24
R1	GigabitEthernet 1/0/3	VLAN 100	9.1.1.1/24
R2	GigabitEthernet 1/0/1	VLAN 10	10.1.1.1/24
R2	GigabitEthernet 1/0/2	VLAN 20	10.1.2.1/24
R2	GigabitEthernet 1/0/3	VLAN 40	10.1.4.1/24
R2	GigabitEthernet 1/0/4	VLAN 50	10.1.5.1/24
R3	GigabitEthernet 1/0/1	VLAN 30	10.1.3.1/24
R3	GigabitEthernet 1/0/2	VLAN 20	10.1.2.2/24
R3	GigabitEthernet 1/0/3	VLAN 70	10.1.7.1/24
R3	GigabitEthernet 1/0/4	VLAN 80	10.1.8.1/24
R3	GigabitEthernet 1/0/5	VLAN 90	10.1.9.1/24
R4	GigabitEthernet 1/0/1	VLAN 40	10.1.4.2/24
R4	GigabitEthernet 1/0/2	VLAN 60	10.1.6.1/24
R5	GigabitEthernet 1/0/1	VLAN 50	10.1.5.2/24
R5	GigabitEthernet 1/0/2	VLAN 60	10.1.6.2/24
R6	GigabitEthernet 1/0/1	VLAN 70	10.1.7.2/24
R7	GigabitEthernet 1/0/1	VLAN 80	10.1.8.2/24
R8	GigabitEthernet 1/0/1	VLAN 90	10.1.9.2/24

### 配置思路

采用如下的思路配置 BGP 路由反射器：

1. 配置客户机与路由反射器之间，非客户机与路由反射器之间建立 IBGP 连接。
2. 在 R2 和 R3 上配置路由反射器功能，指定客户机，查看路由信息。

### 数据准备

为完成此配置例，需准备如下的数据：

各接口所属的 VLAN ID，具体数据如图 4-40 所示。

各 VLANIF 接口的 IP 地址，具体数据如图 4-40所示。

所有交换机的自治系统号为 AS10。

R1、R2、R3、R4、R5、R6、R7、R8 的 Router ID 分别为 1.1.1.1、2.2.2.2、3.3.3.3、4.4.4.4、5.5.5.5、6.6.6.6、7.7.7.7、8.8.8.8。

R2 所在集群的 Cluster-id 为 1，R3 在集群的 Cluster-id 为 2。

### 配置步骤

步骤 1 配置客户机、非客户机与路由反射器之间的 IBGP 连接（略）

步骤 2 配置 R1 发布的本地网络路由 9.1.1.0/24（略）

步骤 3 配置路由反射器

配置 R2。

```
R2(config)#router bgp 65010
```

```
R2(config-bgp)#router-id 2.2.2.2
```

```
R2(config-bgp)#neighbor 10.1.4.2 route-reflector-client
```

```
R2(config-bgp)#neighbor 10.1.5.2 route-reflector-client
```

```
R2(config-bgp)#cluster-id 10.10.10.10
```

```
R2(config-bgp)#quit
```

配置 R3。

```
R3(config)#router bgp 65010
```

```
R3(config-bgp)#router-id 3.3.3.3
```

```
R3(config-bgp)#neighbor 10.1.7.2 route-reflector-client
```

```
R3(config-bgp)#neighbor 10.1.8.2 route-reflector-client
```

```
R3(config-bgp)#neighbor 10.1.9.2 route-reflector-client
```

```
R3(config-bgp)#cluster-id 20.20.20.20
```

```
R3(config-bgp)#quit
```

查看 R4 的路由表。

```
R4(config)#show ip bgp route
```



从路由表中可以看到，R4 从 R2 里学到了 R1 告的路由。

#### 4.6.3.4 配置 BGP4 联盟

##### 组网要求

如图 4-41所示，网络中有多台设备运行 BGP，为了减少 IBGP 的连接数，现将他们划分为 3 个子自治系统：AS1、AS2 和 AS3。其中 AS1 内的三台设备建立 IBGP 全连接。

##### 组网图

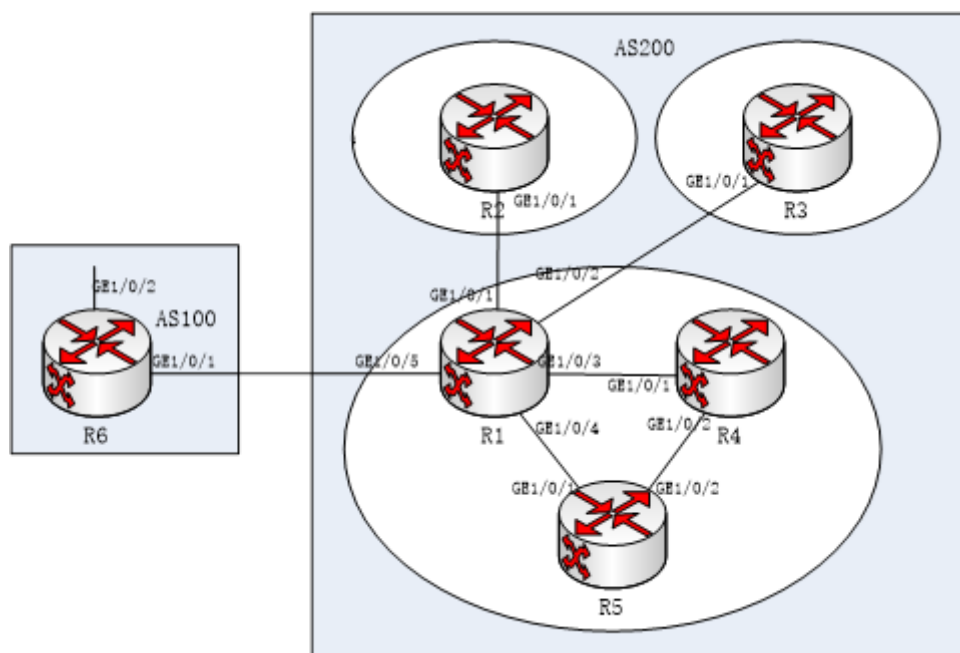


图 4-41 配置联盟组网图

Switch	接口	对应的 VLAN	IP 地址
R1	GigabitEthernet 1/0/1	VLAN 10	10.1.1.1/24
R1	GigabitEthernet 1/0/2	VLAN 20	10.1.2.1/24
R1	GigabitEthernet 1/0/3	VLAN 30	10.1.3.1/24
R1	GigabitEthernet 1/0/4	VLAN 40	10.1.4.1/24
R1	GigabitEthernet 1/0/5	VLAN 60	200.1.1.1/24
R2	GigabitEthernet 1/0/1	VLAN 10	10.1.1.2/24

R3	GigabitEthernet 1/0/1	VLAN 20	10.1.2.2/24
R4	GigabitEthernet 1/0/1	VLAN 30	10.1.3.2/24
R4	GigabitEthernet 1/0/2	VLAN 50	10.1.5.1/24
R5	GigabitEthernet 1/0/1	VLAN 40	10.1.4.2/24
R5	GigabitEthernet 1/0/2	VLAN 50	10.1.5.2/24
R6	GigabitEthernet 1/0/1	VLAN 60	200.1.1.2/24
R6	GigabitEthernet 1/0/2	VLAN 70	9.1.1.1/24

### 配置思路

采用如下的思路配置 BGP 联盟：

1. 在 AS200 中的各 Switch 上配置 BGP 联盟。
2. 在 AS1 中配置 IBGP 连接。
3. 在 AS100 和 AS200 之间配置 EBGP 连接，查看路由信息。

### 数据准备

为完成此配置例，需准备如下的数据：

各接口所属的 VLAN ID，具体数据如图 4-41 所示。

各 VLANIF 接口的 IP 地址，具体数据如图 4-41 所示。

R1、R2、R3、R4、R5、R6 的 router id 分别为 1.1.1.1、2.2.2.2、3.3.3.3、4.4.4.4、5.5.5.5、6.6.6.6。

自治系统号 AS100，自治系统号 AS200，AS200 中的 3 个子自治系统号 AS65001，AS65002，AS65003。

### 配置步骤

步骤 1 配置 BGP 联盟

配置 R1。

```
R1(config)#router bgp 65001
```

```
R1(config-bgp)#router-id 1.1.1.1
```

```
R1(config-bgp)#confederation identifier 200
```

```
R1(config-bgp)#confederation peer-as 65002
R1(config-bgp)#confederation peer-as 65003
R1(config-bgp)#neighbor 10.1.1.2 remote-as 65002
R1(config-bgp)#neighbor 10.1.2.2 remote-as 65003
R1(config-bgp)#neighbor 10.1.1.2 next-hop-local
R1(config-bgp)#neighbor 10.1.2.2 next-hop-local
R1(config-bgp)#quit
```

配置 R2。

```
R2(config)#router bgp 65002
R2(config-bgp)#router-id 2.2.2.2
R2(config-bgp)#confederation identifier 200
R2(config-bgp)#confederation peer-as 65001
R2(config-bgp)#confederation peer-as 65003
R2(config-bgp)#neighbor 10.1.1.1 remote-as 65001
R2(config-bgp)#quit
```

配置 R3

```
R3(config)#router bgp 65003
R3(config-bgp)#router-id 3.3.3.3
R3(config-bgp)#confederation identifier 200
R3(config-bgp)#confederation peer-as 65001
R3(config-bgp)#confederation peer-as 65002
R3(config-bgp)#neighbor 10.1.2.1 remote-as 65001
R3(config-bgp)#quit
```

步骤 2 配置 AS65001 内的 IBGP 连接

配置 R1。

```
R1(config)#router bgp 65001
R1(config-bgp)#neighbor 10.1.3.2 remote-as 65001
R1(config-bgp)#neighbor 10.1.4.2 remote-as 65001
R1(config-bgp)#neighbor 10.1.3.2 next-hop-local
R1(config-bgp)#neighbor 10.1.4.2 next-hop-local
R1(config-bgp)#quit
```

配置 R4。

```
R4(config)#router bgp 65001
R4(config-bgp)#router-id 4.4.4.4
R4(config-bgp)#neighbor 10.1.3.1 remote-as 65001
R4(config-bgp)#neighbor 10.1.5.2 remote-as 65001
R4(config-bgp)#quit
```

配置 R5。

```
R5(config)#router bgp 65001
R5(config-bgp)#router-id 5.5.5.5
R5(config-bgp)#neighbor 10.1.4.1 remote-as 65001
R5(config-bgp)#neighbor 10.1.5.1 remote-as 65001
R5(config-bgp)#quit
```

步骤 3 配置 AS100 和 AS200 之间的 EBGP 连接

配置 R1。

```
R1(config)#router bgp 65001
R1(config-bgp)#neighbor 200.1.1.2 remote-as 100
R1(config-bgp)#quit
```

配置 R6。

```
R6(config)#router bgp 100
```

```
R6(config-bgp)#router-id 6.6.6.6
R6(config-bgp)#neighbor 200.1.1.1 remote-as 200
R6(config-bgp)#network 9.1.1.0 255.255.255.0
R6(config-bgp)#quit
```

步骤 4 查看配置结果

查看 R2 的 BGP 路由表。

```
R2(config)#show ip bgp route
```

查看 R4 的 BGP 路由表。

```
R4(config)#show ip bgp route
```

#### 4.6.3.5 配置 BFD for BGP

##### 组网要求

如图 4-42, R1 属于 AS100, R2 和 R3 属于 AS200, R1 和 R2, R1 和 R3 建立 EBGP 连接。业务流量在主链路 R1→R2 上传送, 链路 R1→R3→R2 作为备份链路。使用 BFD 检测 R1 和 R2 之间的 BGP 邻居关系, 当 R1 和 R2 之间的链路发生故障时, BFD 能够快速检测到故障并通告给 BGP 协议, 使业务流量使用备份链路传送。

##### 组网图

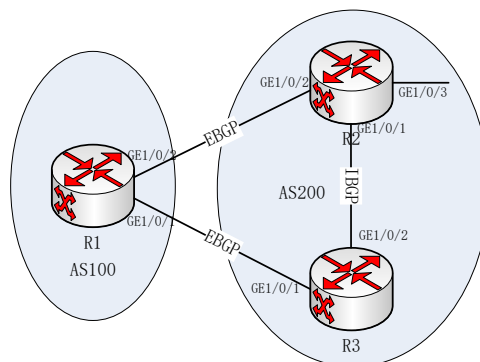


图 4-42 配置 BFD for BGP 组网图

Switch	接口	对应的 VLAN	IP 地址
R1	GigabitEthernet 1/0/1	VLAN 10	200.1.2.1/24

R1	GigabitEthernet 1/0/2	VLAN 20	200.1.1.1/24
R2	GigabitEthernet 1/0/1	VLAN 30	9.1.1.1/24
R2	GigabitEthernet 1/0/2	VLAN 20	200.1.1.2/24
R2	GigabitEthernet 1/0/3	VLAN 40	192.1.1.1/24
R3	GigabitEthernet 1/0/1	VLAN 10	200.1.2.2/24
R3	GigabitEthernet 1/0/2	VLAN 30	9.1.1.2/24

### 配置思路

采用如下思路配置 BFD for BGP 功能：

1. 在各 Switch 上配置 BGP 基本功能。
2. 配置 MED 属性控制路由的选路功能。
3. 在 R1 和 R2 上使能 BFD 检测机制。

### 数据准备

为完成此配置例，需准备如下的数据：

R1、R2 和 R3 的 Router ID 和所在 AS 号。

BFD 检测的对端 IP 地址。

BFD 控制报文的最小发送间隔、最小接收间隔、本地检测倍数。

### 配置步骤

步骤 1 配置 BGP 基本功能，在 R1 和 R2，R1 和 R3 之间建立 EBGP 连接，R2 和 R3 间建立 IBGP 连接

配置 R1。

```
R1(config)#router bgp 100
```

```
R1(config-bgp)#router-id 1.1.1.1
```

```
R1(config-bgp)#neighbor 200.1.1.2 remote-as 200
```

```
R1(config-bgp)#neighbor 200.1.2.2 remote-as 200
```

```
R1(config-bgp)#quit
```

配置 R2。

```
R2(config)#router bgp 200
R2(config-bgp)#router-id 2.2.2.2
R2(config-bgp)#neighbor 200.1.1.1 remote-as 100
R2(config-bgp)#neighbor 9.1.1.2 remote-as 200
R2(config-bgp)#network 9.1.1.0 255.255.255.0
R2(config-bgp)#quit
```

配置 R3。

```
R3(config)#router bgp 200
R3(config-bgp)#router-id 3.3.3.3
R3(config-bgp)#neighbor 200.1.2.1 remote-as 100
R3(config-bgp)#neighbor 9.1.1.1 remote-as 200
R3(config-bgp)#network 9.1.1.0 255.255.255.0
R3(config-bgp)#network 192.1.1.0 255.255.255.0
R3(config-bgp)#quit
```

在 R1 查看，BGP 邻居已经建立（Established）。

```
R1(config-bgp)#show ip bgp neighbor
```

#### 步骤 2 配置 MED 属性

通过策略配置 R2 和 R3 送给 R1 的 MED 值。

配置 R2。

```
R2(config)#route-policy 10 permit node 10
R2(config-route-policy)#apply cost 100
R2(config-route-policy)#quit
R2(config)#router bgp 200
R2(config-bgp)#neighbor 200.1.1.2 route-policy 10 export
```

配置 R3。

```
R3(config)#route-policy 10 permit node 10
R3(config-route-policy)#apply cost 150
R3(config-route-policy)#quit
R3(config)#router bgp 200
R3(config-bgp)#neighbor 200.1.2.2 route-policy 10 export
```

查看 R1 上 BGP 的所有路由信息。

```
R1(config-bgp)#show ip bgp route
```

从 BGP 路由表可以看出，去往 192.1.1.0/24 的路由下一跳地址为 200.1.1.2，流量在主链路 R1R2 上传输。

步骤 3 配置 BFD 检测功能、发送和接收间隔、本地检测时间倍数

在 R1 使能 BFD 功能。

```
R1(config)#bfd enable
R1(config)#router bgp 100
R1(config-bgp)#neighbor 200.1.1.2 bfd enable
```

在 R2 使能 BFD 功能。

```
R2(config)#bfd enable
R2(config)#router bgp 200
R2(config-bgp)#neighbor 200.1.1.1 bfd enable
```

在 R1 显示 BGP 建立的所有 BFD 会话。

```
R1(config)#show ip bfd session
```

步骤 4 查看配置结果

对 R2 的 VLAN20 接口执行 shutdown 命令，模拟主链路故障。

```
R2(config)#interface vlan 20
R2(config-Vlan-20)#shutdown
```



在交换机 R1 上，查看 bgp 路由表

```
R1(config)#show ip bgp route
```

从 BGP 路由表可以看出，在主链路失效后，备份链路 R1→R3→R2 生效，去往 192.1.1.0/24 的路由下一跳地址为 200.1.2.2。

## 4.7 ISIS 配置

### 4.7.1 ISIS 简介

#### 4.7.1.1 产生背景

随着 Internet 的飞速发展，Internet 正在被越来越多的具有不同需求的用户使用，成千上万的网络终端使用 Internet 保持联系。所以在网络的中间设备(路由器，三层交换机)上需要动态路由协议来指导报文转发，为报文的转发提供准确有效的路由信息，IS-IS 路由协议结合自身具有良好的扩展性的特点，实现了对 IP/IPv6 网络层协议的支持。

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)。

#### 4.7.1.2 协议介绍

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。IS-IS 路由协议的基本术语包括：

1. IS (Intermediate System)，中间系统。相当于 TCP/IP 中的路由器，是 IS-IS 协议中生成路由和传播路由信息的基本单元。在下文中 IS 和路由器具有相同的含义。
2. RD (Routing Domain)，路由域。在一个路由域中一群 IS 通过相同的路由协议来交换路由信息。
3. Area，区域，路由域的细分单元，IS-IS 允许将整个路由域分为多个区域。 z

4. LSDB (Link State Database), 链路状态数据库。所有的网络内连接状态组成了链路状态数据库, 在每一个 IS 中都至少有一个 LSDB。IS 使用 SPF 算法, 利用 LSDB 来生成自己的路由。
5. LSP (Link State Protocol Data Unit), 链路状态报文。在 IS-IS 中, 每一个 IS 都会生成至少一个 LSP, 这些 LSP 包含了本 IS 的所有链路状态信息。每个 IS 收集本区域内所有的 LSP 与自己本地生成的 LSP 构成自己的 LSDB。

#### 4.7.1.3 功能特性

IS-IS 直接运行于链路层之上。其工作过程包括: 邻居关系建立; 链路状态数据库的同步; 路由计算三个方面。

邻居关系的形成过程因网络类型不同而不同, 建立邻接的条件:

- 只有同一层的相邻路由器才能成为邻居路由器;
- 对于 level-1 路由器来说要求 area 地址一致;
- 同一网段检查;

链路状态数据库的同步通过 LSP、CSNP 和 PSNP 三种协议报文来完成。在一个 LAN 中必须有一台路由器被选举为 DIS, 由 DIS 来负责在广播网络中创建和更新伪节点, 维护一个 LAN 中的链路状态数据库。

对于 level-1-2 设备同时维护 level-1 和 level-2 两个数据库, level-1 和 level-2 运行相同 SPF 算法。IS-IS 在链路状态数据库的基础上, 使用 SPF (最短路径优先) 算法计算出到达网络拓扑中其他设备的最短路径, 根据最短路径树可以建立路由表。

#### 4.7.1.4 协议描述

IS-IS 可以运行在点到点链路 (Point to Point Links), 如 PPP、HDLC 等; 也可以运行在广播链路 (Broadcast Links), 如 Ethernet、Token-Ring 等; 对于 NBMA (Non-Broadcast Multi-Access) 网络, 如 ATM, 也被当作 P2P 链路进行处理, 对于这种链路, 用户只能通过 CLNS MAP 命令配置一条 PVC, 当然也可以对这种接口配置子接口, 只要将子接口类型配置为 P2P 或广播网络即可; IS-IS 不能在点到多点链路 (Point to MultiPoint Links) 上运行。

为了支持大规模的路由网络, IS-IS 在路由域内采用两级的分层结构。一个大的路由域被分成一个或多个区域 (Areas)。区域内的路由通过 Level-1 路由器管理, 区域间的路由通过 Level-2 路由器管理。

1. **Level-1 路由器：**Level-1 路由器负责区域内的路由，它只与同一区域的 Level-1 路由器形成邻接关系，维护一个 Level-1 的 LSDB，该 LSDB 包含本区域的路由信息，到区域外的报文转发给最近的 Level-1-2 路由器。
2. **Level-2 路由器：**Level-2 路由器负责区域间的路由，可以与其它区域的 Level-2 路由器形成邻接关系，维护一个 Level-2 的 LSDB，该 LSDB 包含区域间的路由信息。所有 Level-2 路由器和 Level-1-2 路由器组成路由域的骨干网，负责在不同区域间通信，路由域中的 Level-2 路由器必须是物理连续的，以保证骨干网的连续性。
3. **Level-1-2 路由器：**同时属于 Level-1 和 Level-2 的路由器称为 Level-1-2 路由器，每个区域至少有一个 Level-1-2 路由器，以将区域连在骨干网上。它维护两个 LSDB，Level-1 的 LSDB 用于区域内路由，Level-2 的 LSDB 用于区域间路由。

图 4-43所示为一个运行 IS-IS 协议的经典网络拓扑，其中 Area5 是骨干区域，该区域中的所有路由器均是 Level-2路由器。另外4个区域为非骨干区域，它们都通过 Level-1-2 路由器与骨干路由器相连。

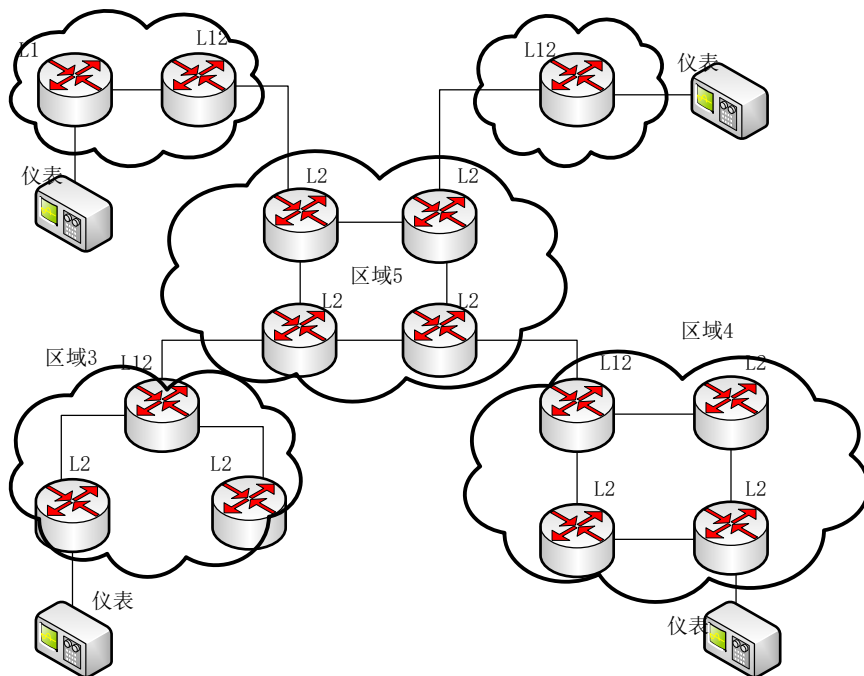


图 4-43 IS-IS 经典网络拓扑图

IS-IS 报文直接封装在数据链路帧中，主要分 3 类：

1. Hello 报文：用于建立和维持邻接关系，也称为 IIH（IS-to-IS Hello PDUs）。其中，广播网中的 Level-1 路由器使用 Level-1 LAN IIH，广播网中的 Level-2 路由器使用 Level-2 LAN IIH，点到点网络中的路由器则使用 P2P IIH。
2. LSP（Link State PDUs，链路状态报文）：用于交换链路状态信息。LSP 分为两种：Level-1 LSP 和 Level-2 LSP。Level-1 路由器传送 Level-1 LSP，Level-2 路由器传送 Level-2 LSP，Level-1-2 路由器则可传送以上两种 LSP。
3. SNP（Sequence Number PDUs，时序报文）：用于确认邻居之间最新接收的 LSP，作用类似于确认（Acknowledge）报文，但更有效。SNP 包括 CSNP（Complete SNP，全时序报文）和 PSNP（Partial SNP，部分时序报文），进一步又可分为 Level-1 CSNP、Level-2 CSNP、Level-1 PSNP 和 Level-2 PSNP。CSNP 包括 LSDB 中所有 LSP 的摘要信息，从而可以在相邻路由器间保持 LSDB 的同步。在广播网络上，CSNP 由 DIS 定期发送（缺省的发送周期为 10 秒）；在点到点链路上，CSNP 只在第一次建立邻接关系时发送。PSNP 只列举最近收到的一个或多个 LSP 的序号，它能够一次对多个 LSP 进行确认。当发现 LSDB 不同步时，也用 PSNP 来请求邻居发送新的 LSP。

根据 RFC1195，集成 IS-IS 协议实现在 OSI 和 IP 的双环境下同时运行，它不仅仅可以动态发现和生成 IP 路由，同时也可以发现和生成 CLNS 路由。ISISv6 则可以在 IPv4 和 IPv6 双环境下同时运行，它不仅仅可以动态发现和生成 IPv4 路由，同时也可以发现和生成 IPv6 路由。

IS-IS 使用 Hello 报文来发现同一条链路上的邻居路由器并建立邻接关系，使能 ISIS 功能的路由器周期性从每个使能 ISIS 功能的接口发送 Hello 报文，如果从同一条链路上的路由器收到了 IS-IS Hello 报文，且对端路由器发送的 Hello 报文通过了支持协议检查和接口地址检查，将与对方建立起邻接关系。图 4-44 和图 4-45 分别显示了 LAN 接口和点到点接口建立邻居的过程。建立邻接关系完毕后，将继续周期性的发送 Hello 报文来维持邻接关系。IS 之间可以只建立 IPv4 邻接关系、IPv6 邻接关系，或者同时建立 IPv4 和 IPv6 的邻接关系：

1. 如果 IS 之间需要建立 IPv4 邻接关系（IPv4-only），则需要双方接口都配置了合法的 IPv4 地址并且在同一网段（当网络类型为 P2P 时，如果设置了在 PPP 协议接口上接收 Hello 报文时不检查对端 IP 地址的功能，两端路由器的 IP 地址可以不在同一个网段）并且都使能了 IS-IS 功能。
2. 如果 IS 之间需要建立 IPv6 邻接关系（IPv6-only），则需要双方接口都配置了合法的 IPv6 链路本地地址并且双方的链路本地地址不相同并且都使能了 ISISv6 功能。

3. 如果 IS 之间需要同时建立 IPv4 和 IPv6 的邻接关系，则需要同时满足以上两个条件。

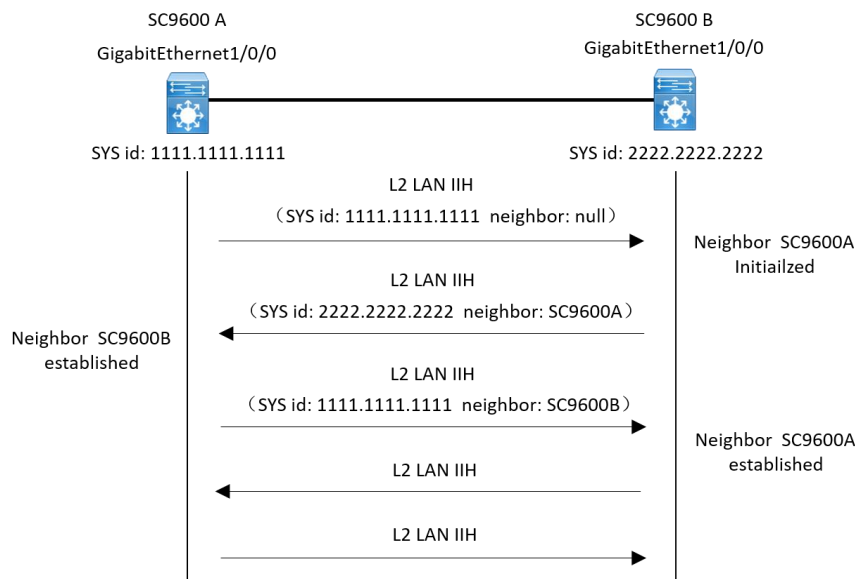


图 4-44 广播链路上的建邻过程

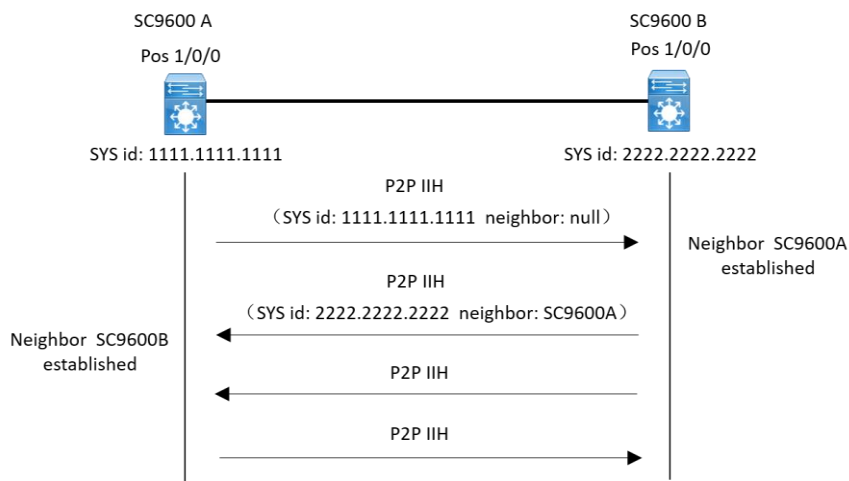


图 4-45 点到点链路上的建邻过程

ISIS 建立邻居后，对于广播链路会选出 DIS，由 DIS 负责维护数据库更新，并使用 LSP 泛洪和 SNP 报文进行数据库同步，点到点链路则直接使用 CSNP 和 PSNP 进行数据库同步。LSP 报文的“泛洪”指当一个路由器向相邻路由器报告自己的 LSP 后，相邻路由器再将同样的 LSP 报文传送到除发送该 LSP 的路由器外的其它邻居，并这样逐级将 LSP 传送到整个层次内的一种方式。通过这种“泛洪”，整个层次内的每一个路由器就都

可以拥有相同的 LSP 信息，并保持 LSDB 的同步。图 4-46和图 4-47分别显示了 ISIS 在广播链路和点到点链路上的数据库同步过程：

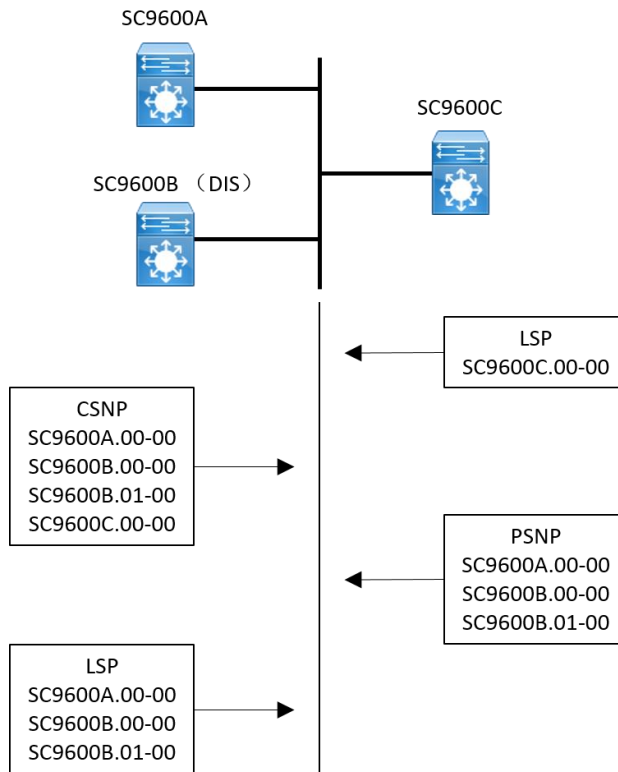


图 4-46 广播链路数据库同步过程

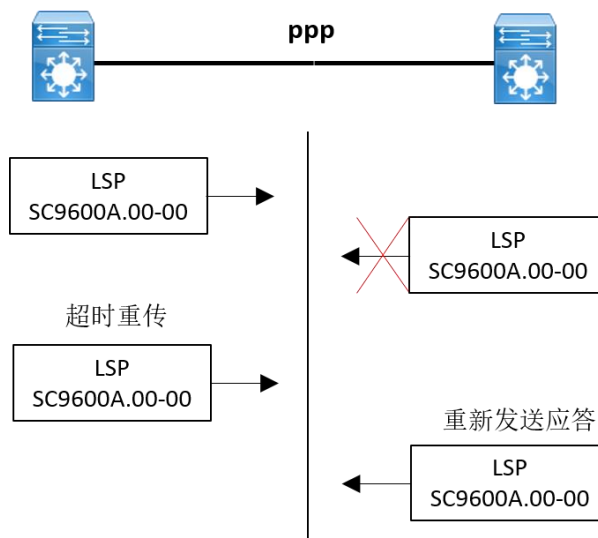


图 4-47 点到点链路数据库同步过程

IS-IS 完成数据库同步后，根据数据库中链路状态信息，使用 SPF 算法计算出无环最短路径优先树，并根据与邻居建立的邻接关系类型对路由计算类型作出限制：

1. 当与邻居只建立了 IPv4 的邻接关系时，只进行 IPv4 的路由计算，仅生成 IPv4 路由。
2. 当与邻居只建立了 IPv6 的邻接关系时，只进行 IPv6 的路由计算，仅生成 IPv6 路由。
3. 只有当与邻居同时建立 IPv4 和 IPv6 的邻接关系时，才会同时进行 IPv4 和 IPv6 的路由计算，同时生成 IPv4 和 IPv6 路由。

#### 4.7.1.5 功能约束

为了使得 ISIS 能在 IPv4-Only、IPv6-Only 或 IPv4 与 IPv6 共存的网络环境中都能够正常运行，保证 IPv4 与 IPv6 的路由信息不互相干扰，使得最终生成的 IPv4 和 IPv6 路由连续、完整和准确，需要对 IS-IS 组网作出一些约束：

1. 同一区域内所有 IS 必须同时使能 IS-IS 功能或 ISISv6 功能，不允许同一区域中的一些 IS 使能了 IS-IS 功能，而其它 IS 使能 ISISv6 功能；同一路由器上所有使能 IS-IS 功能的接口必须同时使能 IS-IS 功能或 ISISv6 功能，不允许同一路由器上的一些接口使能了 IS-IS 功能，而其它接口使能 ISISv6 功能。
2. 根据区域中的路由器使能的 IS-IS 功能是 IPv4 还是 IPv6 的可以将区域分为三种类型：
  - IPv4-Only 区域，即区域内所有的 IS 只使能了 IS-IS 功能，只有 IPv4 数据被正确转发，如图 4-43 中的 Aera 49.0001、Aera 49.0004；
  - IPv6-Only 区域，即区域内所有的 IS 只使能了 ISISv6 功能，只有 IPv6 数据被正确转发，如图 4-43 中的 49.0002；
  - Dual IP 区域，即区域内所有的 IS 都使能了 IS-IS 功能和 ISISv6 功能，IPv4 和 IPv6 数据均可以被正确转发，如图 4-43 中的 49.0003。
3. 路由域也可以分为 IPv4-Only、IPv6-Only、Dual IP 三种类型：
  - IPv4-Only 路由域，骨干区和 Level-1 区域均为 IPv4-Only 区，只有 IPv4 数据能够被正确转发；
  - IPv6-Only 路由域，骨干区和 Level-1 区域均为 IPv6-Only 区，只有 IPv6 数据被正确转发；

- Dual IP 路由域,骨干区必须为 Dual IP 区,L1 区域可以是 IPv4-Only、IPv6-Only 以及 Dual IP 三种类型中的任意一种。在 Dual IP 路由域中, IPv4-Only 区域 (Level-1)、Dual IP (Level-1) 区域可以通过骨干区之间可以实现 IPv4 互通; IPv6-Only 区域 (Level-1)、Dual IP 区域 (Level-1) 以及骨干区之间可以实现 IPv6 互通。
4. 一个路由域 (Domain) 内不能同时存在两个互相独立的 IPv4-Only 骨干区和 IPv6-Only 骨干区, 如果需要骨干区同时具有 IPv4 路由能力和 IPv6 路由能力, 则必须将该骨干区配置为 Dual IP。

## 4.7.2 ISIS 配置

### 4.7.2.1 ISIS 基本配置

#### 目的

本节介绍 ISIS 基本配置, 包括全局启动 ISIS 实例, 接口使能 ISIS 功能并启动 ISIS 进程, 配置网络实体标题, 以及全局设置 ISIS 过载位。

#### 过程

根据不同目的, 执行相应步骤, 具体参见下表。

目的	步骤	参数说明
启动 ISIS 实例	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>router isis</b> , 进入 ISIS 配置视图 或 执行命令 <b>router isis isis-instance-id</b> , 启动特定实例号的 ISIS 实例	isis-instance-id: SC9600 支持的 ISIS 实例 ID, 取值范围为: 1-2047
关闭 ISIS 实例	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>no router isis isis-instance-id</b> , 关闭特定实例号的 ISIS 实例	isis-instance-id: SC9600 支持的 ISIS 实例 ID, 取值范围为: 1-2047
在接口上使能接口的 IS-IS 能力并指定要关联的 IS-IS 进程号	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>interface vlan N</b> , 进入 VLANIF 配置视图, 其中 N 为 VLAN ID; 3. 执行命令 <b>ip router isis isis-instance-id</b>	N: VLAN ID, 整数形式, 取值范围是 1~4094; isis-instance-id: SC9600 支持的 ISIS 实例 ID, 取值范围为: 1-2047



目的	步骤	参数说明
	或 <b>ipv6 router isis isis-instance-id</b>	
在接口上取消接口的 IS-IS 能力并指定要关联的 IS-IS 进程号	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>interface vlan N</b> , 进入 VLANIF 配置视图, 其中 N 为 VLAN ID; 3. 执行命令 <b>no ip router isis isis-instance-id</b> 或 <b>no ipv6 router isis isis-instance-id</b>	N: VLAN ID, 整数形式, 取值范围是 1~4094; isis-instance-id: SC9600 支持的 ISIS 实例 ID, 取值范围为: 1-2047
配置 ISIS 网络实体标题	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>router isis</b> , 进入 ISIS 配置视图; 3. 执行命令 <b>net network-entity-title</b>	<b>network-entity-title</b> : 网络实体标题的名称 (地址或者名字)
取消 ISIS 网络实体标题	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>router isis</b> , 进入 ISIS 配置视图; 3. 执行命令 <b>no net network-entity-title</b>	<b>network-entity-title</b> : 网络实体标题的名称 (地址或者名字)
设置 ISIS 全局的过载位	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>router isis</b> , 进入 ISIS 配置视图; 3. 执行命令 <b>set-overload-bit</b>	-
取消 ISIS 全局的过载位	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>router isis</b> , 进入 ISIS 配置视图; 3. 执行命令 <b>no set-overload-bit</b>	-
向堆叠接口中添加成员端口	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>interface iss-trunk N</b> , 进入 ISS-trunk 接口配置视图, 其中 N 为 trunk ID; 2. 执行命令 <b>add { gigasethernet   xgigasethernet } interface-number</b> 。	
删除已添加的成员端口	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>interface iss-trunk N</b> , 进入	<b>interface-number</b> <b>interface-number1</b> <b>interface-number2</b> 指定成员以

目的	步骤	参数说明
	ISS-trunk 接口配置视图，其中 $N$ 为 trunk ID； 2. 执行如下命令： <ul style="list-style-type: none"> <li>● <b>no { gigabitEthernet   xgigabitEthernet } interface-number</b></li> <li>● <b>no { gigabitEthernet   xgigabitEthernet } interface-number1 to { gigabitEthernet   xgigabitEthernet } interface-number2</b></li> </ul>	以太网接口号 整数形式，固化接口取值范围 <1-1>/<0-0>/<1-24> 或者 <1-1>/<0-0>/<1-48>；插卡接口取值范围是 <1-1>/<0-2>/<1-2>

#### 4.7.2.2 配置 ISIS 基本参数

##### 目的

本节介绍 ISIS 基本参数的配置，包括配置接口状态、接口优先级、报文时间间隔等。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置 / 取消 ISIS 在广播网络上发送 csnp 报文的时间间隔	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>interface vlan N</b> ，进入 VLANIF 配置视图，其中 $N$ 为 VLAN ID； 3. 执行命令 <b>isis csnp-interval (level-1   level-2) csnp-interval</b> 或 <b>no isis csnp-interval (level-1   level-2)</b>	N: VLAN ID, 整数形式, 取值范围是 1~4094; csnp-interval: 发送 csnp 报文的时间间隔范围, 取值范围为 1-600, 默认值为 10 秒
使能 / 关闭 ISIS 接口的被动状态, 即抑制该接口发送 IS-IS 报文	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>interface vlan N</b> ，进入 VLANIF 配置视图，其中 $N$ 为 VLAN ID； 3. 执行命令 <b>isis passive-interface</b> 或 <b>no isis passive-interface</b>	N: VLAN ID, 整数形式, 取值范围是 1~4094;
配置 / 取消 ISIS 接口下发 hello 报文的时间间隔	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>interface vlan N</b> ，进入 VLANIF 配置视图，其中 $N$ 为 VLAN ID；	N: VLAN ID, 整数形式, 取值范围是 1~4094; hello-interval: SC9600 支持的 hello 报文时间间隔, 取值范围为:

目的	步骤	参数说明
	3. 执行命令 <b>isis hello-interval (level-1   level-2) hello-interval</b> 或 <b>no isis hello-interval (level-1   level-2)</b>	3-255, 默认值为 10 秒
配置 / 取消 ISIS 通告邻居超时前没有收到的 hello 报文个数	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>interface vlan N</b> , 进入 VLANIF 配置视图, 其中 N 为 VLAN ID; 3. 执行命令 <b>isis hello-multiplier (level-1   level-2) multiplier</b> 或 <b>no isis hello-multiplier (level-1   level-2)</b>	N: VLAN ID, 整数形式, 取值范围是 1~4094; multiplier: Hello 层级, 等待的 hello 个数, 取值范围为: 2-100, 默认值为 3 个
配置 / 取消 ISIS 接口下的链路开销	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>interface vlan N</b> , 进入 VLANIF 配置视图, 其中 N 为 VLAN ID; 3. 执行命令 <b>isis default-metric (level-1   level-2) metric</b> 或 <b>no isis default-metric (level-1   level-2)</b>	N: VLAN ID, 整数形式, 取值范围是 1~4094; metric: 开销应用层级, 默认开销值, 取值范围为: 0-63, 默认值为 10
配置 / 取消接口下的宽开销值	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>interface vlan N</b> , 进入 VLANIF 配置视图, 其中 N 为 VLAN ID; 3. 执行命令 <b>isis wide-metric (level-1   level-2) wide-metric</b> 或 <b>no isis wide-metric (level-1   level-2)</b>	N: VLAN ID, 整数形式, 取值范围是 1~4094; wide-metric: 开销应用层级, 宽开销值, 取值范围为: 0-16777215, 默认值为 10
配置 / 取消 ISIS 接口优先级, 用于 DIS 选举	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>interface vlan N</b> , 进入 VLANIF 配置视图, 其中 N 为 VLAN ID; 3. 执行命令 <b>isis priority (level-1   level-2) priority</b> 或 <b>no isis priority (level-1   level-2)</b>	N: VLAN ID, 整数形式, 取值范围是 1~4094; priority: 优先级应用级别, 接口优先级大小, 取值范围为 0-127。缺省情况下, 广播接口在 Level-1 和 Level-2 级别的 DIS 优先级为 64。
使能 / 取消 ISIS 接口下的	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;	N: VLAN ID, 整数形式, 取值范围是 1~4094;

目的	步骤	参数说明
三次握手功能， 只针对 p2p 接口	2. 执行命令 <b>interface vlan N</b> ，进入 VLANIF 配置视图，其中 N 为 VLAN ID； 3. 执行命令 <b>isis three-way-handshake</b> 或 <b>no isis three-way-handshake</b>	
配置 / 取消 ISIS 接口下 psnp 报文发送 间隔	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>interface vlan N</b> ，进入 VLANIF 配置视图，其中 N 为 VLAN ID； 3. 执行命令 <b>isis psnp-interval (level-1   level-2) psnp-interval</b> 或 <b>no isis psnp-interval (level-1   level-2)</b>	N: VLAN ID，整数形式，取值范围是 1~4094； psnp-interval: psnp 报文发送层级，发送时间间隔，取值范围是 1-120，缺省值为 2 秒。
配置一个 ISIS 接口的电 路类型	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>interface vlan N</b> ，进入 VLANIF 配置视图，其中 N 为 VLAN ID； 3. 执行命令 <b>isis circuit-type (broadcast   ppp)</b>	N: VLAN ID，整数形式，取值范围是 1~4094；
使能 / 取消 ISIS 接口下发 发送 hello 报文的 自动填充功能	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>interface vlan N</b> ，进入 VLANIF 配置视图，其中 N 为 VLAN ID； 3. 执行命令 <b>isis hello padding</b> 或 <b>no isis hello padding</b>	N: VLAN ID，整数形式，取值范围是 1~4094；
配置 / 取消 ISIS 接口加入 指定的 mesh-group	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>interface vlan N</b> ，进入 VLANIF 配置视图，其中 N 为 VLAN ID； 3. 执行命令 <b>isis mesh-group group-number</b> 或 <b>no isis mesh-group</b>	N: VLAN ID，整数形式，取值范围是 1~4094； group-number: mesh group 组 ID，取值范围为 1-65535，默认接口不在任何 mesh-group 组中，接口正常进行 LSP 的扩散。
使能 ISIS 接 口下的 mesh-group 阻 塞功能	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>interface vlan N</b> ，进入 VLANIF 配置视图，其中 N 为 VLAN ID； 3. 执行命令 <b>isis mesh-group blocked</b>	N: VLAN ID，整数形式，取值范围是 1~4094；

### 4.7.2.3 配置 ISIS 层级

#### 目的

本节介绍 ISIS 层级配置，包括配置全局系统层级、接口层级以及层级出入开销类型等。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置/恢复一个 ISIS 接口层级	<ol style="list-style-type: none"> <li>在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>执行命令 <b>interface vlan N</b>，进入 VLANIF 配置视图，其中 N 为 VLAN ID；</li> <li>执行命令 <b>isis circuit-level (level-1   level-2   level-1-2)</b> 或 <b>no isis circuit-level</b></li> </ol>	<p>N: VLAN ID, 整数形式, 取值范围是 1~4094;</p> <p>缺省情况下, 接口链路类型为 Level-1-2, 可以同时建立 Level-1 和 Level-2 的邻接关系。</p>
配置 ISIS 全局的系统层级	<ol style="list-style-type: none"> <li>在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>执行命令 <b>router isis</b>，进入 ISIS 配置视图；</li> <li>执行命令 <b>is-type (level-1   level-2   level-1-2)</b></li> </ol>	缺省情况下, IS-IS 路由器工作在 Level-1 和 Level-2
配置 ISIS 层级的出开销类型	<ol style="list-style-type: none"> <li>在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>执行命令 <b>router isis</b>，进入 ISIS 配置视图；</li> <li>执行命令 <b>metric-style (narrow both wide) (level-1 level-2)</b></li> </ol>	<p>(narrow both wide): isis 开销类型</p> <p>(level-1 level-2): isis 开销类型的应用层级</p>
配置 ISIS 层级的入开销类型	<ol style="list-style-type: none"> <li>在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>执行命令 <b>router isis</b>，进入 ISIS 配置视图；</li> <li>执行命令 <b>spf metric-style (narrow both wide) (level-1 level-2)</b></li> </ol>	<p>(narrow both wide): isis 开销类型</p> <p>(level-1 level-2): isis 开销类型的应用层级</p>

### 4.7.2.4 配置 ISIS LSP

#### 目的

本节介绍 ISIS 的 LSP 配置，包括配置 LSP 刷新时间间隔、最大生存时间、全局接收 LSP 报文检查校验、以及全局接收 LSP 报文 MTU 等。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置 / 取消 ISIS 全局下 lsp 刷新时间间隔	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>router isis</b> ，进入 ISIS 配置视图； 3. 执行命令 <b>lsp-refresh-interval refresh-interval</b> 或 <b>no lsp-refresh-interval</b>	<b>refresh-interval</b> : LSP 刷新时间间隔，取值范围为 1-65235，缺省值为 900 秒
配置 / 取消 ISIS 全局 lsp 最大生存时间	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>router isis</b> ，进入 ISIS 配置视图； 3. 执行命令 <b>max-lsp-lifetime lifetime</b> 或 <b>no max-lsp-lifetime</b>	<b>lifetime</b> : LSP 最大生存时间，取值范围为 350-65535，缺省值为 1200 秒
使能 / 取消 ISIS 全局下接收 lsp 报文的校验 和检查	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>router isis</b> ，进入 ISIS 配置视图； 3. 执行命令 <b>ignore-lsp-errors (level-1   level-2)</b> 或 <b>no ignore-lsp-errors (level-1   level-2)</b>	默认为不忽略 ISIS 全局接收 LSP 报文检查和校验
设置 / 取消 ISIS 全局下接收 lsp 报文的 mtu	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>interface vlan N</b> ，进入 VLANIF 配置视图，其中 N 为 VLAN ID； 3. 执行命令 <b>lsp-mtu lsp-mtu</b> 或 <b>no lsp-mtu</b>	<b>N</b> : VLAN ID，整数形式，取值范围是 1~4094； <b>lsp mtu</b> : LSP 报文 MTU，取值范围为 1492-16000，默认为 1200

4.7.2.5 配置 ISIS 重分配

目的

本节介绍 ISIS 的重分配配置，包括使能/取消路由重分配以及使能/取消 ISIS 的 level-2 到 level-1 的路由渗透功能等。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
使能/取消路由重分配功能，引入其他路由协议的路由信息	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>router isis</b> ，进入 ISIS 配置视图； 3. 执行命令 <b>redistribute (connect static rip bgp ospf) (level-1 level-2 level-1-2)</b> 或 <b>redistribute ipv6 (connect static rip bgp ospf) (level-1 level-2 level-1-2)</b> 或 <b>no redistribute (connect static rip bgp ospf)</b> 或 <b>no redistribute ipv6 (connect static rip bgp ospf)</b>	-
使能/取消 ISIS 的 level-2 到 level-1 的路由渗透功能	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>router isis</b> ，进入 ISIS 配置视图； 3. 执行命令 <b>redistribute level-2 to level-1</b> 或 <b>no redistribute level-2 to level-1</b>	-

4.7.2.6 配置 ISIS 路由汇总

目的

本节介绍 ISIS 的路由汇总配置，包括配置/取消一个 ISIS 汇总路由。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置/取消一个 ISIS 汇总路由	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；	<b>ip-address</b> : 汇总的 IP 地址，点分十进制形式，如：(A, B, C, D),

目的	步骤	参数说明
由	2. 执行命令 <b>router isis</b> ，进入 ISIS 配置视图； 3. 执行命令 <b>summary-address</b> <i>ip-address mask-address</i> 或 <b>no summary-address</b> <i>ip-address mask-address</i>	其中 A~D 为 0~255 十进制数。 mask-address: 汇总 IP 地址的子网掩码，点分十进制形式，如：(A,B,C,D), 其中 A~D 为 0~255 十进制数。

#### 4.7.2.7 配置 ISIS 认证

##### 目的

本节介绍 ISIS 的认证配置，包括配置/取消 ISIS 全局下的区域认证、配置/取消 ISIS 全局下的域间认证、配置/取消 ISIS 接口以指定的方式和密码验证 Hello 报文以及配置/取消 ISIS 识别 LSP 报文中主机名称的能力等。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置 / 取消 ISIS 全局下的区域认证	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>router isis</b> ，进入 ISIS 配置视图； 3. 执行命令 <b>area-password</b> <b>{ simple md5 } PASSWORD</b> 或 <b>no area-password PASSWORD</b>	PASSWORD: 给定的区域认证密码
配置 / 取消 ISIS 全局下的域间认证	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>router isis</b> ，进入 ISIS 配置视图； 3. 执行命令 <b>domain-password</b> <b>{ simple md5 } PASSWORD</b> 或 <b>no domain-password PASSWORD</b>	PASSWORD: 给定的区域认证密码
配置 / 取消 ISIS 接口以指定的方式和密码验证 Hello 报文	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>interface vlan N</b> ，进入 VLANIF 配置视图，其中 N 为 VLAN ID； 3. 执行命令 <b>isis password</b>	PASSWORD: 给定的区域认证密码



目的	步骤	参数说明
	<b>(simple md5) PASSWORD level-1   level-2</b> 或 <b>no isis password (level-1   level-2)</b>	
配置 / 取消 ISIS 识别 LSP 报文中主机名称的能力, 同时为本地交换机上 IS-IS 系统配置动态主机名, 并以 LSP 报文的方式发布出去	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>hostname hostname</b> 或 <b>no hostname</b>	hostname: Isis 主机名, 字符串形式, 长度范围是 1 ~ 32 字节

#### 4.7.2.8 配置 ISIS BFD

##### 目的

本节介绍 ISIS 的 BFD 配置, 包括使能/关闭 ISIS 接口下的 bfd 功能。

##### 过程

根据不同目的, 执行相应步骤, 具体参见下表。

目的	步骤	参数说明
使能 / 关闭 ISIS 接口下的 bfd 功能	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>interface vlan N</b> , 进入 VLANIF 配置视图, 其中 N 为 VLAN ID; 3. 执行命令 <b>isis bfd (enable disable)</b>	-

#### 4.7.2.9 配置 ISIS GR

##### 目的

本节介绍 ISIS 的 GR 重启配置, 包括使能/取消 ISIS 全局下的 GR 功能。

##### 过程

根据不同目的, 执行相应步骤, 具体参见下表。

目的	步骤	参数说明
使能 / 取消 ISIS 全局下的 GR 功能	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>router isis</b> , 进入 ISIS 配置	默认不使能

目的	步骤	参数说明
	视图： 3. 执行命令 <b>graceful-restart (enable disable)</b>	

#### 4.7.2.10 使能 ISIS 其他功能模块

##### 目的

本节介绍 ISIS 的其他功能模块使能/去使能配置，包括使能/去使能全局 TE、FRR 以及 SNMP 告警功能。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
使能 / 取消 ISIS 全局下的 TE 功能	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>router isis</b> ，进入 ISIS 配置视图； 3. 执行命令 <b>traffic-engineer (enable disable)</b>	默认不使能
使能 / 取消 ISIS 全局下的 FRR 功能	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>router isis</b> ，进入 ISIS 配置视图； 3. 执行命令 <b>frr (enable disable)</b>	默认不使能
使能 / 取消 ISIS 全局下的 SNMP 告警功能	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>router isis</b> ，进入 ISIS 配置视图； 3. 执行命令 <b>snmp-trap (enable disable)</b>	默认不使能

#### 4.7.2.11 配置 ISIS 调试功能

##### 目的

本节介绍 ISIS 的调试功能配置。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
----	----	------

目的	步骤	参数说明
调试 isis hello 报文收发信息	1. 进入特权用户视图; 2. 执行命令 <b>debug isis hello</b>	-
调试 isis csnp 报文收发信息	1. 进入特权用户视图; 2. 执行命令 <b>debug isis csnp</b>	-
调试 isis psnp 报文收发信息	1. 进入特权用户视图; 2. 执行命令 <b>debug isis psnp</b>	-
调试 isis lsp 报文收发信息	1. 进入特权用户视图; 2. 执行命令 <b>debug isis lsp</b>	-
结合上述四种报文类型调试命令查看收发报文的详细内容打印	1. 进入特权用户视图; 2. 执行命令 <b>debug isis pdu</b>	-
调试 isis 接口动作, 如添加删除接口, up/down, dis 选举等	1. 进入特权用户视图; 2. 执行命令 <b>debug isis interface</b>	-
调试 isis 邻居信息, 如添加删除邻居, 邻居状态变化, 超时等	1. 进入特权用户视图; 2. 执行命令 <b>debug isis adj</b>	-
调试生成 ipv4 路由的信息	1. 进入特权用户视图; 2. 执行命令 <b>debug isis route4</b>	-
调试生成 ipv6 路由的信息	1. 进入特权用户视图; 2. 执行命令 <b>debug isis route6</b>	-
调试主备同步的信息, 如收发同步包, 包解析, 同步实例接口邻居等	1. 进入特权用户视图; 2. 执行命令 <b>debug isis sync</b>	-

目的	步骤	参数说明
调试路由泄露的信息	1. 进入特权用户视图; 2. 执行命令 <b>debug isis leak</b>	-
调试产生填充删除 tlv 的信息	1. 进入特权用户视图; 2. 执行命令 <b>debug isis tlv</b>	-
调试 spf 计算的信息	1. 进入特权用户视图; 2. 执行命令 <b>debug isis spf</b>	-
调试 isis 内存信息	1. 进入特权用户视图; 2. 执行命令 <b>debug isis memory</b>	-
调试 isis 路由下表信息, 如添加删除出错等	1. 进入特权用户视图; 2. 执行命令 <b>debug isis sys</b>	-
调试计算 FRR 路由的信息	1. 进入特权用户视图; 2. 执行命令 <b>debug isis frr</b>	-
调试 isis 接口下 bfd 信息, 如 bfd 绑定, 解绑定, up/down 状态	1. 进入特权用户视图; 2. 执行命令 <b>debug isis bfd</b>	-
调试 isis 的一些全局信息	1. 进入特权用户视图; 2. 执行命令 <b>debug isis global</b>	-
调试打印以上全部信息	1. 进入特权用户视图; 2. 执行命令 <b>debug isis all</b>	-
打开 iss debug 开关	1. 进入特权用户视图; 2. 执行命令 <b>debug iss { in out timer link-change conflict election all}</b>	in 接收报文 out 发送报文 timer 定时器 link-change 链路状态改变
关闭 iss debug 开关	1. 进入特权用户视图; 2. 执行命令 <b>no debug iss { in out timer link-change conflict election all}</b>	conflict 冲突 election 选择器 all 以上所有

#### 4.7.2.12 查看 ISIS 配置信息

##### 目的

本节介绍 ISIS 的配置信息查看。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
显示指定 level 的 isis database 信息	1. 进入普通用户视图或特权用户视图； 2. 执行命令 <b>show ip isis database {level-1 level-2} isis-instance-id</b>	isis-instance-id: SC9600 支持的 ISIS 实例 ID，取值范围为：1-2047
显示链路状态数据库信息	1. 进入普通用户视图或特权用户视图； 2. 执行命令 <b>show ip isis database</b> <b>show ip isis database verbose</b> <b>show ip isis database verbose lsp-index</b>	lsp-index: 指定 LSP 索引号，整数形式，取值范围是<1-65535>
显示 ISIS 数据库统计信息	1. 进入普通用户视图或特权用户视图； 2. 执行命令 <b>show ip isis database count</b>	-
显示 ISIS 邻居的详细信息	1. 进入普通用户视图或特权用户视图； 2. 执行命令 <b>show ip isis neighbor verbose</b>	-
显示 ISIS 的邻居信息	1. 进入普通用户视图或特权用户视图； 2. 执行命令 <b>show ip isis neighbor</b>	-
显示 ISIS 的基本配置信息	1. 进入普通用户视图或特权用户视图； 2. 执行命令 <b>show ip isis config</b>	-
显示 ISIS 动态主机映射	1. 进入普通用户视图或特权用户视图； 2. 执行命令 <b>show ip isis hostname</b>	-
显示 ISIS 接口信息	1. 进入普通用户视图或特权用户视图； 2. 执行命令 <b>show ip isis interface</b>	-
显示 ISIS 接口详细信息	1. 进入普通用户视图或特权用户视图； 2. 执行命令 <b>show ip isis interface verbose</b>	-
显示 ISIS 实例信息	1. 进入普通用户视图或特权用户视图； 2. 执行命令 <b>show ip isis isis-instance-id</b>	isis-instance-id: SC9600 支持的 ISIS 实例 ID，取值范围为：1-2047

目的	步骤	参数说明
显示 ISIS 学到的路由信息	1. 进入普通用户视图或特权用户视图; 2. 执行命令 <b>show ip isis route</b> <b>show ip isis { level-1 level-2}</b> <b>show ip isis ipv4-address</b> <b>show ip isis route all</b>	ipv4-address: 指定接口的 IPV4 地址, 点分十进制
显示 ISIS 学到的 IPV6 路由信息	1. 进入普通用户视图或特权用户视图; 2. 执行命令 <b>show ipv6 isis route</b> <b>show ipv6 isis route ipv6-address</b> <b>show ipv6 isis route {level-1 level-2}</b> <b>show ipv6 isis route all</b>	ipv6-address: 指定接口的 IPV6 地址, 在这种形式中, 128 位的 IP 地址被分为 8 组, 每组的 16 位用 4 个十六进制字符 (0~9, A~F) 来表示, 组和组之间用冒号 (:) 隔开。其中每个“X”代表一组十六进制数值
显示 ISIS 统计信息以及 ISIS 接口统计信息	1. 进入普通用户视图或特权用户视图; 2. 执行命令 <b>show ipv6 isis statistic</b> <b>show ipv6 isis statistic interface</b>	-
查看最短路径树是否完整	1. 进入普通用户视图或特权用户视图; 2. 执行命令 <b>show ipv6 isis spf-tree</b>	-
显示 ISIS FRR 信息	1. 进入普通用户视图或特权用户视图; 2. 执行命令 <b>show ip isis frr route</b> <b>show ip isis frr route (level-1 level-2)</b> <b>show ipv6 isis frr route</b> <b>show ipv6 isis frr route (level-1 level-2)</b>	-

### 4.7.3 ISIS 配置举例

#### 4.7.3.1 ISIS 基本功能配置

##### 组网要求

本案例的任务是完成 ISIS 最基本的配置, 通过该配置熟悉 ISIS 的配置过程, 了解 ISIS 配置中 AREA、LEVEL、SYSID 等参数的作用, 拓扑图如图 4-48 所示。

##### 组网图

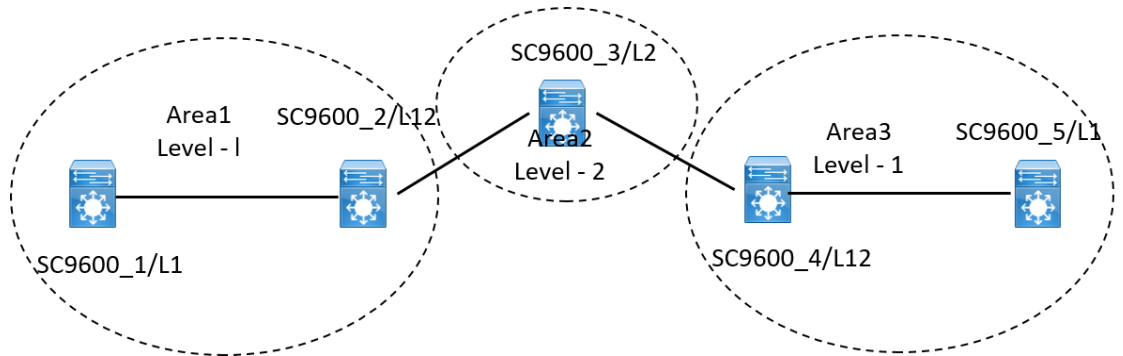


图 4-48 ISIS 基本配置拓扑图

### 配置思路

所有的设备都运行 ISIS，并将整个自治系统划分为 3 个区域，其中

SC9600\_2 和 SC9600\_4 为 DIS 来转发区域之间的路由。

配置完成后，每台 Level-1 类型设备都应只学到本区域内全部路由，Level-1-2 和 Level-2 类型设备都能学到自治系统内到所有网段的路由。

### 数据准备

Area1 和 Area2 为 Level-1 区域，Area0 为 Level-2 区域

Area1 区域地址为 10，Area2 区域地址为 20，Area0 区域地址为 30

SC9600\_1 NET 为 10.0001.0001.0001.00，接口地址：1.1.1.1/24

SC9600\_2 NET 为 10.0002.0002.0002.00，两个接口地址：1.1.1.2/24 和 2.1.1.2/24

SC9600\_3 NET 为 20.0003.0003.0003.00，两个接口地址：2.1.1.1/24 和 3.1.1.1/24

SC9600\_4 NET 为 30.0004.0004.0004.00，两个接口地址：3.1.1.2/24 和 4.1.1.2/24

SC9600\_5 NET 为 30.0005.0005.0005.00，接口地址：4.1.1.1/24

### 配置步骤

SC9600\_1:

```
SC9600_1(config)#router isis
```

```
SC9600_1(config-isis-1)#net 10.0001.0001.0001.00
```

```
SC9600_1(config-isis-1)# is-type level-1
```

```
SC9600_1(config-isis-1)#exit
```

```
SC9600_1(config)#int vlan 1
```

```
SC9600_1(config-vlan-1)#ip router isis
```

```
SC9600_2:
SC9600_2 (config)#router isis
SC9600_2 (config-isis-1)#net 10.0002.0002.0002.00
SC9600_2 (config-isis-1)# is-type level-1-2
SC9600_2 (config-isis-1)#exit
SC9600_2 (config)#int vlan 1
SC9600_2 (config-vlan-1)#ip router isis
SC9600_2 (config-vlan-1)#exit
SC9600_2 (config)#int vlan 2
SC9600_2 (config-vlan-2)#ip router isis
```

```
SC9600_3:
SC9600_3 (config)#router isis
SC9600_3 (config-isis-2)#net 20.0003.0003.0003.00
SC9600_3 (config-isis-2)# is-type level-2
SC9600_3 (config-isis-2)#exit
SC9600_3 (config)#int vlan 2
SC9600_3 (config-vlan-2)#ip router isis
SC9600_3 (config-vlan-2)#exit
SC9600_3 (config)#int vlan 3
SC9600_3 (config-vlan-3)#ip router isis
```

```
SC9600_4:
SC9600_4 (config)#router isis
SC9600_4 (config-isis-2)#net 30.0004.0004.0004.00
SC9600_4 (config-isis-2)# is-type level-1-2
SC9600_4 (config-isis-2)#exit
SC9600_4 (config)#int vlan 3
SC9600_4 (config-vlan-3)#ip router isis
SC9600_4 (config-vlan-1)#exit
SC9600_4 (config)#int vlan 4
SC9600_4 (config-vlan-4)#ip router isis
```



```
SC9600_5:
SC9600_5 (config)#router isis
SC9600_5 (config-isis-1)#net 30.0005.0005.0005.00
SC9600_5 (config-isis-1)# is-type level-1
SC9600_5 (config-isis-1)#exit
SC9600_5 (config)#int Vlan 4
SC9600_5 (config-Vlan-4)#ip router isis
```

#### 验证配置结果

用 show ip isis neighbor 、 show ip isis database 、 show ip isis route 命令验证运行结果。

### 4.7.3.2 配置 ISIS 重分配

#### 组网要求

本案例的任务是完成 ISIS 重分配的配置，通过该配置熟悉 ISIS 重分配的配置过程，拓扑图如图 4-49所示。

#### 组网图

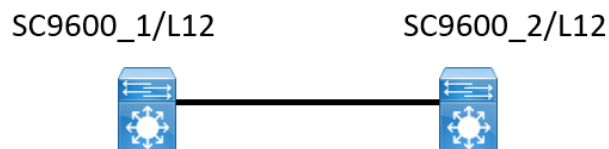


图 4-49 ISIS 重分配拓扑图

#### 配置思路

2 个设备都运行 ISIS，并将两个都配置为同一区域。假定 SC9600\_1 上有通过其他路由协议学习到的外部路由并需要向 ISIS 导入，但是对外部路由有如下要求：

- 1) 接受所有直连路由，并重分配到 level-1；
- 2) 接收所有 RIP 路由，并重分配到 evel-2；

配置完成后，每台设备都应学到自治系统内的到所有网段的路由。。

#### 配置步骤

参照 ISIS 基本配置，另外在 SC9600\_1 上配置重分配：

```
r1(config-isis-1)#redistribute connect level-1
```

```
r1(config-isis-1)#redistribute rip level-2
```

#### 验证配置结果

用 show ip isis database、show ip isis route 命令验证运行结果。

### 4.7.3.3 配置 ISIS 路由汇总

#### 组网要求

本案例的任务是完成 ISIS 路由汇总的配置,通过该配置熟悉 ISIS 路由汇总的配置过程,拓扑图如图 4-50所示。

#### 组网图

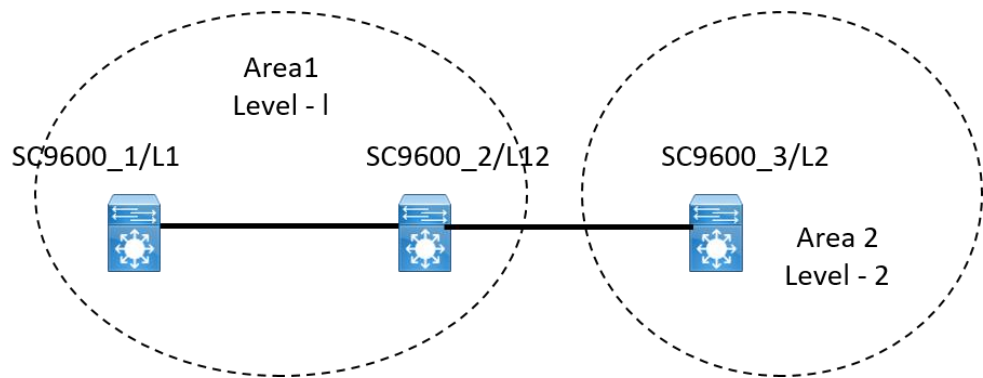


图 4-50 ISIS 路由汇总拓扑图

#### 配置思路

SC9600\_1 上有 10.1.1.0/24—10.1.10.0/24 这 10 条路由,希望减小 SC9600\_3 的路由表容量,让 SC9600\_2 在向 Area2 通告 Area1 路由时汇总为 10.1.0.0/16 一条,因此可以在 SC9600\_2 上配置路由汇总命令,配置完后 SC9600\_3 仅从 Area1 学习到 10.1.0.0/16 一条路由。

#### 配置步骤

参照 ISIS 基本配置,另外在 SC9600\_2 上配置路由汇总:

```
r2(config)# router isis
r2(config-isis-1)#summary-address 10.1.0.0 16
```

#### 验证配置结果

用 show ip isis database、show ip isis route 命令验证运行结果。

### 4.7.3.4 配置 ISIS 认证

#### 组网要求

本案例的任务是完成 ISIS 认证的配置，通过该配置熟悉 ISIS 中 level-1/level-2 类型的 Hello 和 Lsp 认证的配置过程，拓扑图如图 4-51所示。

#### 组网图

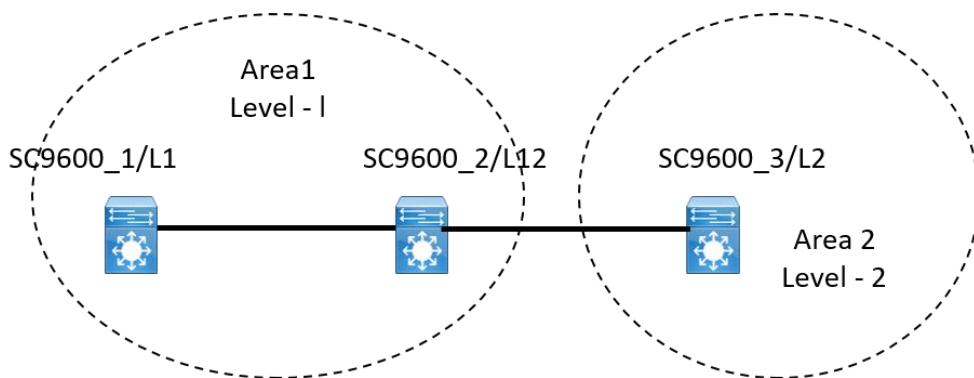


图 4-51 ISIS 认证拓扑图

#### 配置思路

要求 SC9600\_1 和 SC9600\_2 之间：

level-1 hello 采用简单密码认证，密码为 123456；

level-2 hello 采用 MD5 认证，密码为 fhn；

level-1 Lsp 采用简单密码认证，密码为 12345；

level-2 Lsp 采用 MD5 认证，密码为 cmcc；

配置完成后要求 SC9600\_1 和 SC9600\_2 之间正常建立 level-1 和 level-2 邻居，正常通告 level-1 路由和 level-2 路由。。

#### 配置步骤

参照 ISIS 基本配置，另外再增加认证配置：

SC9600\_1:

```
R1(config)# router isis
```

```
R1(config-isis-1)#area-password simple 12345
```

```
R1(config-isis-1)#domain-password md5 cmcc
```

```
R1(config-isis-1)#q
```

```
R1(config)# int Vlan 1
R1(config- vlan-1)# isis password simple 123456 level-1
R1(config- vlan-1)# isis password md5 fhn level-2
```

SC9600\_2:

```
r2(config)# router isis
r2(config-isis-1)#area-password simple 12345
r2(config-isis-1)#domain-password md5 cmcc
r2(config-isis-1)#q
r2(config)# int Vlan 1
r2(config- vlan-1)# isis password simple 123456 level-1
r2(config- vlan-1)# isis password md5 fhn level-2
```

#### 验证配置结果

用 show ip isis neighbor 、 show ip isis database 、 show ip isis route 命令验证运行结果。

### 4.7.3.5 配置 ISIS BFD

#### 组网要求

本案例的任务是完成 ISIS BFD 的配置，通过该配置熟悉 ISIS 中 BFD 的配置过程，拓扑图如图 4-52所示。

#### 组网图



图 4-52 ISIS BFD 拓扑图

#### 配置思路

2 个设备都运行 ISIS，并使能全局 BFD 功能，然后在 ISIS 接口下使能 BFD 功能，配置完成后，邻居和 BFD 绑定，并且连接断开后邻居迅速超时。。

#### 配置步骤

参照 ISIS 基本配置，另外再增加 BFD 配置：

```
SC9600_1:
SC9600_1(config)#interface vlan 2
SC9600_1(config-vlan-2)#bfd enable
SC9600_1(config-vlan-2)# isis bfd enable
```

```
SC9600_2:
SC9600_2(config)#interface vlan 2
SC9600_2(config-vlan-2)#bfd enable
SC9600_2(config-vlan-2)# isis bfd enable
```

#### 验证配置结果

用 show ip isis neighbor 、 show ip isis database 、 show ip isis route 命令验证运行结果。

### 4.7.3.6 配置 ISIS GR

#### 组网要求

本案例的任务是完成 ISIS GR 的配置，通过该配置熟悉 ISIS 中 GR 的配置过程，拓扑图如图 4-53 所示。

#### 组网图

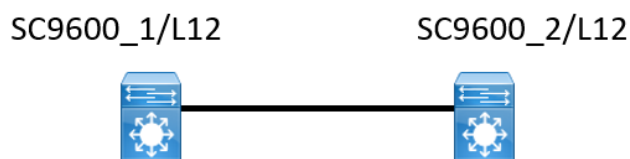


图 4-53 ISIS GR 拓扑图

#### 配置思路

2 个设备都运行 ISIS，并将有个都配置同一 Area，SC9600\_1 和 SC9600\_2 都需要使用 GR 功能，互相之间发双向流量，待数据库和流量稳定后开始测 GR。

测试 GR 重启需要 2 台设备，一台为 GR 重启者，一台为 GR 帮助者。GR 测试重启者采用双主控，拔插卡的方式测试。帮助者无限制。

#### 配置步骤

参照 ISIS 基本配置，另外再增加 GR 配置：

```
SC9600_1:
SC9600_1(config)#router isis
SC9600_1(config-isis-1)# graceful-restart enable
SC9600_2:
SC9600_2(config)#router isis
SC9600_2(config-isis-1)# graceful-restart enable
```

#### 验证配置结果

采用插拔卡进行测试，GR 重启者和 GR 帮助者都配置完成以后，将 GR 重启者的主用主控拔掉，这时起到新的备用主控重启完成后期间，设备间原有的流量应不发生中断。

## 4.8 路由策略配置

### 4.8.1 路由策略概述

#### 路由策略

路由策略是为了改变网络流量所经过的途径而对路由信息采用的方法。

为了实现路由策略，通过定义一组匹配规则和设置规则，然后将他们应用到路由的发布、接收和引入等过程的路由策略中。

#### SC9600 支持的路由策略方式

配置路由策略时，可选择使用的过滤器：访问控制列表、地址前缀列表和 Router-Policy。

- 访问控制列表

访问控制列表是针对 IP 报文的 ACL。用户在定义 ACL 时可以指定 IP 地址和子网范围，用于匹配路由信息的目的网段地址或者下一跳地址。

- 地址前缀列表

地址前缀列表的作用类似于 ACL，但它更为灵活，且更易于用户理解。使用地址前缀列表过滤路由信息时，其匹配对象为路由信息的目的地址信息域；另外，用户可以指定路由器选项，指明只接收某些路由器发布的路由信息。

- 路由映射

路由映射是一种比较复杂的过滤器，它不仅可以匹配路由信息的某些属性，还可以在条件满足时改变路由信息的属性。

一个路由映射可以由多个节点（node）构成，每个节点是匹配检查的一个单元，在匹配过程中，系统按节点序号升序依次检查各个节点。每个节点可以由一组 **match** 和 **apply** 子句组成。**match** 子句定义匹配规则，匹配对象是路由信息的一些属性。同一节点中的不同 **match** 子句是“与”的关系，只有满足节点内所有 **match** 子句指定的匹配条件，才能通过该节点的匹配测试。**apply** 子句指定动作，也就是在通过节点的匹配后，对路由信息的一些属性进行设置。一个路由映射的不同节点间是“或”的关系，如果通过了其中一节点，就意味着通过该路由映射，不再对其他节点进行匹配测试。

### 4.8.2 配置地址前缀列表

#### 目的

使用本节操作配置地址前缀列表，实现路由信息的过滤，其匹配对象为路由信息目的地址域。

#### 过程



注意：

- 根据参数 *list-name* 及 IP 类型区分不同表。
- 任意规则匹配后直接返回。
- 匹配操作按照 *index* 增序进行，不设置 *index* 时自动取 *index* 值为表中最大  $index - index \% 10 + 10$  值。
- 对表中表项关系逻辑矛盾不检测，配置时需要操作人员自行安排。
- 配置已有 *index* 上规则时将覆盖原来位置上规则。

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
创建一条过滤规则，完全匹配前 MASKLEN 长度的网段地址	1. 执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>ip prefix-list list-name [ index index-number ] { permit   deny } ip-address/mask-length</b> 或执行命令 <b>ipv6 prefix-list list-name [ index index-number ] { permit   deny } ipv6-address/mask-length</b> 创建一条过滤规则，完全匹配前 MASKLEN 长度的网段地址； 3. 结束。
创建一条过滤规则，路由地址掩码长度大于等于指定的最小值且完全匹配前缀掩码	1. 执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>ip prefix-list list-name [ index index-number ] { permit   deny } ip-address/mask-length greater-equal min</b> 创建一条过滤规则，路由地址掩码长度大于等于指定的最小值且完全匹配前缀掩码长度的网

目的	步骤
长度的网段地址	段地址 <code>-range</code> 或执行命令 <code>ipv6 prefix-list list-name [ index index-number ] { permit   deny } ipv6-address/mask-length greater-equal min-range;</code> 3. 结束。
创建一条过滤规则，路由地址掩码长度小于等于指定的最大值且完全匹配前缀掩码长度的网段地址	1. 执行命令 <code>configure</code> 进入全局配置视图； 2. 执行命令 <code>ip prefix-list list-name [ index index-number ] { permit   deny } ip-address/mask-length less-equal max-range</code> 或执行命令 <code>ipv6 prefix-list list-name [ index index-number ] { permit   deny } ipv6-address/mask-length less-equal max-range</code> 创建一条过滤规则，路由地址掩码长度小于等于指定的最大值且完全匹配前缀掩码长度的网段地址； 3. 结束。
创建一条过滤规则，路由地址掩码长度小于等于指定的最小值与最大值范围内且完全匹配前缀掩码长度的网段地址	1. 执行命令 <code>configure</code> 进入全局配置视图； 2. 执行命令 <code>ip prefix-list list-name [ index index-number ] { permit   deny } ip-address/mask-length greater-equal min-range less-equal max-range</code> 或执行命令 <code>ipv6 prefix-list list-name [ index index-number ] { permit   deny } ipv6-address/mask-length greater-equal min-range less-equal max-range</code> 创建一条过滤规则，路由地址掩码长度小于等于指定的最小值与最大值范围内且完全匹配前缀掩码长度的网段地址； 3. 结束。

附表：

参数	说明	取值
list-name	创建的路由规则所在表的名字 IP 类型，区分不同表	必须唯一，长度 1-32 字符
permit	指定路由过滤的规则模式为允许	-
deny	指定路由过滤的规则模式为拒绝	-
index-number	指定过滤规则在的表中索引位置	整数形式，取值范围是 1-65535
ipv6-address	IPv6 地址	-
ip-address	IPv4 地址	-
mask-length	地址掩码长度	前缀匹配长度，IP 类型地址时不大于 32，IPv6 类型时不大于 128
index-number	指定过滤规则在的表中索引位置	整数形式，取值范围是 1-65535
min-range	地址掩码最小长度	IP 类型地址时，取值范围是 0~32； IPv6 类型地址时，取值范围是 0~128
max-range	地址掩码最大长度	IP 类型地址时，取值范围是 0~32； IPv6 类型地址时，取值范围是 0~128



### 4.8.3 配置 Route-Policy

#### 前提条件

配置 Route-Policy 之前，还需要配置 ACL 的 filter 规则，请参考本手册 7.2.3 配置三层 ACL 的配置。

#### 目的

使用本节操作配置 Route-Policy 用来匹配给定的路由信息或者路由信息的某些属性，并在条件满足时改变这些路由信息的属性。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
创建路由策略并进入该路由策略 route-policy 配置视图	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>route-policy policy-name { permit   deny } node node-number</b> 创建路由策略并进入该路由策略配置视图；</li> <li>3. 结束。</li> </ol>
（用户可以根据需要）配置相应 match 子句	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>route-policy policy-name { permit   deny } node node-number</b> 进入路由策略配置视图；</li> <li>3. 选择执行以下命令配置 Router Policy 中的 match 子句； <ul style="list-style-type: none"> <li>● match cost cost-value</li> <li>● match ip filter-list ipv4-filter-list-number</li> <li>● match ipv6 filter-list ipv6-filter-list-number</li> <li>● match ip { next-hop   route-source } filter-list ipv4-filter-list-number</li> <li>● match ipv6 { next-hop   route-source } filter-list ipv6-filter-list-number</li> <li>● match ip-prefix prefix-name</li> <li>● match ip { next-hop   route-source } ip-prefix prefix-name</li> <li>● match ipv6 { address   next-hop   route-source } ip-prefix prefix-name</li> <li>● match route-type { internal   external-type1   external-type2   external-type1 or2   nssa-external-type   nssa-external-type2   nssa-external-type1 or2 }</li> <li>● match tag tag-value</li> </ul> </li> <li>4. 结束。</li> </ol>
（用户可以根据需要）配置相应 apply 子句	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>route-policy policy-name { permit   deny } node node-number</b> 进入路由策略配置视图；</li> </ol>

目的	步骤
	3. 选择执行以下命令配置 Router Policy 中的 apply 子句； <ul style="list-style-type: none"> <li>● apply cost <i>cost-value</i></li> <li>● apply cost { plus   minus } <i>cost-value</i></li> <li>● apply cost-type { type-1   type-2 }</li> <li>● apply local-preference <i>local-priority</i></li> <li>● apply origin { igp   incomplete }</li> <li>● apply origin egp <i>as-number</i></li> <li>● apply ospf { translate   not-translate }</li> <li>● apply preferred-value <i>preferred-value</i></li> <li>● apply tag <i>tag-value</i></li> </ul> 4. 结束。

附表：

参数	说明	取值
cost-value	指定路由开销的取值	整数形式，取值范围是 0~16777215
policy-name	路由策略名称，唯一标识一个路由策略	字符串形式，1~20 个字符
ipv4-filter-list-number	指定基于 IPv4 的 filter 号	整数形式，取值范围是 1001~3000
ipv6-filter-list-number	指定基于 IPv6 的 filter 号	整数形式，取值范围是 2001~4000
next-hop	表示匹配路由的下一跳地址	
route-source	表示匹配路由发布的源地址	
prefix-name	指定基于 IP 地址前缀列表名称	字符串形式
address	表示匹配 IPv6 路由信息的目的地址	address
internal	表示内部路由，包括 OSPF 区域间和区域内路由	-
external-type1	表示 OSPF Type1 的外部路由	-
external-type2	表示 OSPF Type2 的外部路由	-
external-type1or2	表示 OSPF 的外部路由	-
nssa-external-type	表示 OSPF NSSA Type1 的外部路由	-
nssa-external-type2	表示 OSPF NSSA Type2 的外部路由	-
nssa-external-type1or2	表示 OSPF NSSA 的外部路由	-

参数	说明	取值
tag-value	指定标记值	整数形式，取值范围是 0~4294967295
community-string	指定团体属性值	以空格分割的字符串（最多可以有 31 个空格），字符串可以是 0~4294967295 之间的整数或 <0-65535>:<0-65535> 的字符串
additive	表示追加路由的团体属性	-
none	表示删除路由的所有团体属性	-
cost-value	指定路由开销的取值	整数形式，取值范围是 0~16777215
plus	表示增加开销值	-
minus	表示减少开销值	-
type-1	表示设置为 OSPF 的外部 Type-1 路由	-
type-2	表示设置为 OSPF 的外部 Type-2 路由	-
community-string	指定扩展团体属性值	以空格分割的字符串（最多可以有 15 个空格），字符串可以是 IP<A.B.C.D>:NN<0-65535> 或 AS<0-65535>:NN<0-65535> 或 AS<0-65535>.<0-65535>:NN<0-65535> 的输入形式
local-priority	指定 BGP 路由的本地优先级	整数形式，取值范围是 0~4294967295
igp	表示 BGP 路由信息源为内部路由	-
incomplete	表示 BGP 路由信息源为未知源	-
egp	表示 BGP 路由信息源为外部路由	-
as-number	指定 BGP 外部路由的 AS 号	整数形式，取值范围是 1~65535
translate	表示 OSPF 为翻译模式	-
not-translate	表示 OSPF 为非翻译模式	-
preferred-value	指定 BGP 的首选值	整数形式，取值范围是 0~65535
tag-value	指定路由信息标记	整数形式，取值范围是 0~4294967295

#### 4.8.4 对 OSPF 路由协议应用路由策略

##### 目的

使用本节操作配置 OSPF 协议中的路由策略命令引用 ACL 或地址前缀列表，对接收的路由进行过滤，仅接收满足条件的部分路由。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
对 OSPF 发布的路由应用路由策略	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>router ospf process-id</b> 进入 OSPF 配置视图；</li> <li>3. 执行命令 <b>filter route-policy policy-name</b> 用来配置路由协议的过滤策略，只有通过过滤的路由才能被加入更新报文中发布出去；</li> <li>4. 结束。</li> </ol>
对 OSPF 引入外部路由时应用路由策略	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>router ospf process-id</b> 进入 OSPF 配置视图；</li> <li>3. 执行命令 <b>redistribute { static   connect   rip   bgp   isis } route-policy policy-name</b> 用来配置引入不同的路由策略；</li> <li>4. 结束。</li> </ol>

附表：

参数	说明	取值
process-id	IPV4 OSPF 进程号	整数形式，取值范围是 1—2047 如果不输入实例号，默认为实例 1
policy-name	指定的路由策略名，必须是路由策略里面已经配置的。	字符串形式，1~20 个字符

## 4.8.5 对 BGP 路由协议应用路由策略

### 目的

使用本节操作配置 BGP 协议中的路由策略命令引用 ACL 或地址前缀列表，对接收的路由进行过滤，仅接收满足条件的部分路由。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
对 BGP 接收的路由应用路由策略	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>router bgp AS-value</b> 进入 BGP 配置视图；</li> <li>3. 执行命令 <b>filter-policy import route-policy policy-name</b> 或执行命令 <b>filter-policy import ipv6 route-policy policy-name</b> 用来配置路由过滤策略命令；</li> <li>4. 结束。</li> </ol>

目的	步骤
对 BGP 邻居接收的路由应用路由策略	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>router bgp AS-value</b> 进入 BGP 配置视图;</li> <li>3. 执行命令 <b>neighbor ipv4-address ipv4 route-policy policy-name import</b> 或执行命令 <b>neighbor ipv6-address ipv6 route-policy policy-name import</b> 用来配置路由过滤策略命令;</li> <li>4. 结束。</li> </ol>
对 BGP 发布的路由应用路由策略	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>router bgp AS-value</b> 进入 BGP 配置视图;</li> <li>【步骤 3 和步骤 4, 用户根据实际情况任选】</li> <li>3. 执行命令 <b>filter-policy export route-policy policy-name</b> 或执行命令 <b>filter-policy export ipv6 route-policy policy-name</b> 用来配置路由过滤策略命令;</li> <li>4. 执行命令 <b>filter-policy export {static connected rip ospf isis} route-policy policy-name</b> 或执行命令 <b>filter-policy export ipv6 (static connected rip ospf isis) route-policy policy-name</b> 用来配置路由过滤策略命令;</li> <li>5. 结束。</li> </ol>
对 BGP 邻居发布的路由应用路由策略	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>router bgp AS-value</b> 进入 BGP 配置视图;</li> <li>3. 执行命令 <b>neighbor ipv4-address ipv4 route-policy policy-name export</b> 或执行命令 <b>neighbor ipv6-address ipv6 route-policy policy-name export</b> 用来配置路由过滤策略命令;</li> <li>4. 结束。</li> </ol>
对 BGP 引入外部路由时应用路由策略	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>router bgp AS-value</b> 进入 BGP 配置视图;</li> <li>3. 执行命令 <b>redistribute { static   connected   rip   ospf   isis} route-policy policy-name</b> 用来配置引入不同的路由策略;</li> <li>4. 结束。</li> </ol>

附表:

参数	说明	取值
AS-value	地自治系统号取值范围	整数形式, 取值范围是 1~65535
export  import	应用到通告/学习的路由更新信息	-
policy-name	表示路由策略名	-
(static  connected  rip  ospf  isis)	静态、直连、rip 协议、ospf 协议、isis 协议路由	-
ipv4-address	邻居 ipv4 地址	点分十进制形式, 如: (A.B.C.D), 其中 A~D 为 0~255 十进制数。
ipv6-address	邻居 ipv6 地址	IPV6 地址包括 128 比特, 由使用

参数	说明	取值
		由冒号分隔的 16 比特的十六进制数表示
export  import	应用到通告/学习的路由更新信息	-

#### 4.8.6 维护及调试

##### 目的

当路由策略功能不正常，需要进行查看、调试或定位问题时，可以使用本小节操作。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
打开路由策略调试开关	<ol style="list-style-type: none"> <li>1. 保持当前特权用户视图；</li> <li>2. 执行命令 <code>debug route-policy { error   trace   match   apply   all }</code> 打开路由策略调试开关；</li> <li>3. 结束。</li> </ol>
关闭路由策略调试开关	<ol style="list-style-type: none"> <li>1. 保持当前特权用户视图；</li> <li>2. 执行命令 <code>no debug route-policy { error   trace   match   apply   all }</code> 关闭路由策略调试开关；</li> <li>3. 结束。</li> </ol>
查看路由策略的全局信息	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code> 进入全局配置视图，或执行命令 <code>route-policy policy-name { permit   deny } node node-number</code> 进入路由策略配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <code>show route-policy information</code> 用来显示路由策略的全局信息；</li> <li>3. 结束。</li> </ol>
查看配置的路由策略信息	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code> 进入全局配置视图，或执行命令 <code>route-policy policy-name { permit   deny } node node-number</code> 进入路由策略配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <code>show route-policy config</code> 或 <code>show route-policy policy-name</code> 或 <code>show route-policy policy-name node node-number</code> 用来显示配置的路由策略信息；</li> <li>3. 结束。</li> </ol>

附表：

参数	说明	取值
error	表示配置路由策略中产生的错误信息	-
trace	表示内部运行的调试信息	-
match	表示匹配路由策略过程中产生的错误信息	-

参数	说明	取值
apply	表示执行路由策略规则过程中产生的错误信息	-
all	表示以上所有错误信息	-
policy-name	指定路由策略名	1~20 个字符字符串形式
node-number	指定路由策略的节点值	整数形式，取值范围是 0~65535

## 4.8.7 配置举例

### 4.8.7.1 配置 BGP4 ECMP 和路由策略示例

#### 组网要求

所有交换机都配置 BGP，R1 在 AS65008 中，R2 和 R3 在 AS65009 中。R1 与 R2、R3 之间运行 EBGP，R2 和 R3 之间运行 IBGP。

#### 组网图

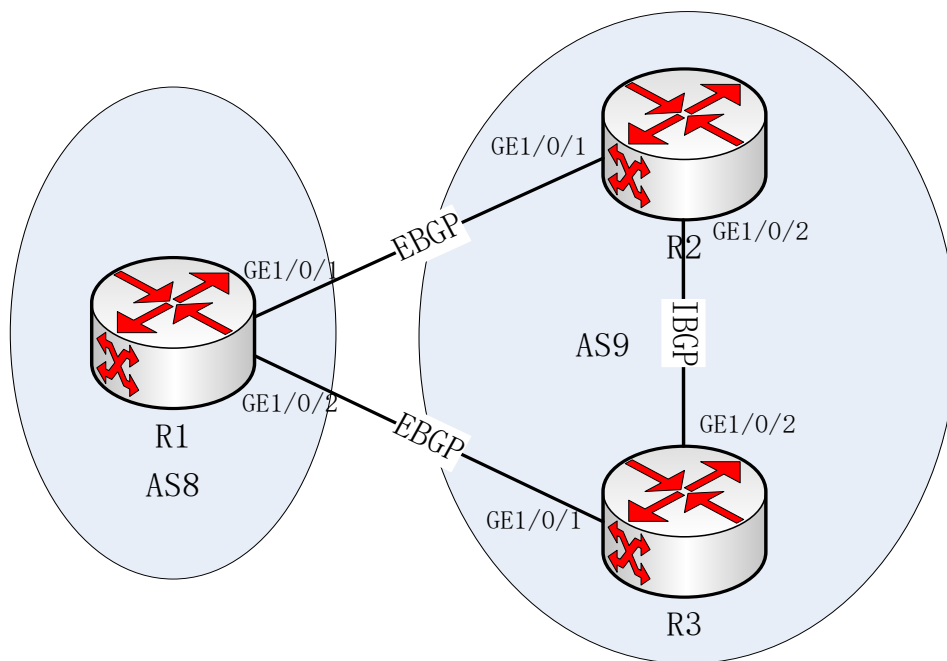


图 4-54 配置 BGP 路径选择的组网图

Switch	接口	对应的 VLAN	IP 地址
R1	GigabitEthernet1/0/1	VLAN 10	200.1.1.2/24
R1	GigabitEthernet1/0/2	VLAN 20	200.1.2.2/24
R2	GigabitEthernet1/0/1	VLAN 10	200.1.1.1/24

R2	GigabitEthernet1/0/2	VLAN 30	10.1.1.1/24
R3	GigabitEthernet1/0/1	VLAN 20	200.1.2.1/24
R3	GigabitEthernet1/0/2	VLAN 30	10.1.1.2/24

### 配置思路

采用如下的思路配置 BGP 负载分担和运用路由策略更改 MED 属性：

1. 在 R1 和 R2、R1 和 R3 之间配置 EBGP 连接；在 R2 和 R3 之间配置 IBGP 连接。
2. 在 R1 运用路由策略更改 MED 值，查看路由信息。

### 数据准备

为完成此配置例，需准备如下的数据：

各接口所属的 VLAN ID，具体数据如图 4-54 所示。

各 VLANIF 接口的 IP 地址，具体数据如图 4-54 所示。

R1 的 Router ID 为 1.1.1.1，所在 AS 号 65008，负载分担条数 2。

R2、R3 的 Router ID 分别为 2.2.2.2、3.3.3.3，所在 AS 号 65009，R2 缺省 MED 值 100。

### 配置步骤

- 1、配置 BGP 连接。

//配置 R1。

```
R1 (config)#router bgp 65008
R1 (config-bgp)#router-id 1.1.1.1
R1 (config-bgp)#neighbor 200.1.1.1 remote-as 65009
R1 (config-bgp)#neighbor 200.1.2.1 remote-as 65009
R1 (config-bgp)#quit
```

//配置 R2。

```
R2 (config)#router bgp 65009
R2 (config-bgp)#router-id 2.2.2.2
R2 (config-bgp)#neighbor 200.1.1.2 remote-as 65008
R2 (config-bgp)#neighbor 10.1.1.2 remote-as 65009
R2 (config-bgp)#network 10.1.1.0 255.255.255.0
R2 (config-bgp)#quit
```

//配置 R3。

```
R3 (config)#router bgp 65009
```



```
R3 (config-bgp)#router-id 3.3.3.3
R3 (config-bgp)#neighbor 200.1.2.2 remote-as 65008
R3 (config-bgp)#neighbor 10.1.1.1 remote-as 65009
R3 (config-bgp)#network 10.1.1.0 255.255.255.0
R3 (config-bgp)#quit
```

//查看 R1 的路由表。从路由表中可以看到，BGP 路由 10.1.1.0/24 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。

```
R1 (config)#show ip bgp route
```

2、配置 MED 属性。

//通过策略配置 R2 发送给 R1 的 MED 值。

```
R2 (config)#route-policy 10 permit node 10
R2 (config-route-policy)#apply cost 100
R2 (config-route-policy)#quit
R2 (config)#router bgp 65009
R2 (config-bgp)#neighbor 200.1.1.2 route-policy 10 export
```

//查看 R1 的路由表。从路由表中可以看出，由于下一跳为 200.1.1.1（R2 的路由 MED 值为 100，而下一跳为 200.1.2.1 的 MED 值为 0，所以 BGP 优先选择 MED 值较小的路由。

```
R1 (config)#show ip bgp route
```

#### 4.8.7.2 配置 OSPF 路由策略示例

##### 组网要求

所有交换机都配置 OSPF，并将有个都配置为区域 0。SC9600\_1 和 SC9600\_2 为 ABR 来转发区域之间的路由。要求对 OSPF 协议发布路由时应用路由策略。

##### 组网图

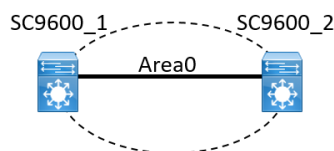


图 4-55 配置 OSPF 路由策略组网图

SC9600\_1 的两个接口地址：1.1.1.1/24 和 3.1.1.1/24

SC9600\_2 的两个接口地址：1.1.1.2/24 和 4.1.1.2/24

**配置步骤**

## 1、配置 SC9600\_1。

```
SC9600_1(config)#router ospf
SC9600_1(config-ospf-1)#router-id 1.1.1.1
SC9600_1(config-ospf-1)#network 1.1.1.0 255.255.255.0 area 0
SC9600_1(config-ospf-1)#network 3.1.1.0 255.255.255.0 area 1
SC9600_1(config)#
```

## 2、配置 SC9600\_2。

```
SC9600_2(config)#router ospf
SC9600_2(config-ospf-1)#router-id 1.1.1.2
SC9600_2(config-ospf-1)#network 1.1.1.0 255.255.255.0 area 0
SC9600_2(config-ospf-1)#network 4.1.1.0 255.255.255.0 area 2
SC9600_2(config)#
```

## 3、配置路由策略。

```
SC9600_1(config)#filter-list 1001
SC9600_1(configure-filter-ipv4-1001)#filter 1 ip 18.1.1.0/24 any
SC9600_1(configure-filter-ipv4-1001)#filter 1 action permit
SC9600_1(configure-filter-ipv4-1001)#quit
SC9600_1(config)# route-policy fhn deny node 1
SC9600_1(configure-route-policy)# match ip filter-list 1001
SC9600_1(configure-route-policy)# quit
SC9600_1(config)# route-policy fhn permit node 2
SC9600_1(configure-route-policy)# quit
```

## 4、OSPF 里应用路由策略。

```
SC9600_1(config)#router ospf
SC9600_1(config-ospf-1)# filter route-policy fhn
```

## 第5章 QoS 配置

### 5.1 概述

本章介绍了 SC9600 系列高端交换机 QoS 的基本内容、配置过程和配置举例。

本章包括如下主题：

内容	页码
5.1 概述	5-1
5.2 Diffserv 配置	5-1
5.3 流量监管和流量整形配置	5-12
5.4 队列调度和拥塞控制配置	5-14

### 5.2 Diffserv 配置

#### 5.2.1 Diffserv 简介

在传统的 IP 网络中，所有的报文都被无区别的等同对待，每个路由器对所有的报文均采用先入先出（FIFO）的策略进行处理，它尽最大的努力（Best-Effort）将报文送到目的地，但对报文传送的可靠性、传送延迟等性能不提供任何保证。

网络发展日新月异，随着 IP 网络上新应用的不断出现，对 IP 网络的服务质量也提出了新的要求，例如 VoIP（Voice over IP，IP 语音）等实时业务就对报文的传输延迟提出了较高要求，如果报文传送延迟太长，将是用户所不能接受的（相对而言，E-Mail 和 FTP 业务对时间延迟并不敏感）。为了支持具有不同服务需求的语音、视频以及数据等业务，要求网络能够区分出不同的通信，进而为之提供相应的服务。传统 IP 网络的尽力服务不可能识别和区分出网络中的各种通信类别，而具备通信类别的区分能力正式为不同的通信提供不同服务的前提，所以说传统网络的尽力服务模式已不能满足应用的需要。QoS(Quality of Service,服务质量)技术的出现便致力于解决这个问题。

一般来讲，在提供 IP 网络的 QoS 时，为了实现规模适应性，在 IP 骨干网往往需要采用 Diffserv 体系结构，在 IP 边缘网可以有两种选择：采用 Diffserv 体系结构或采用 Intserv

体系结构。目前在 IP 边缘网络采用哪一种 QoS 体系结构还没有定论，也许这两种会同时并存于 IP 边缘网中。在 IP 边缘网采用 Diffserv 体系结构的情况下，IP 骨干网与 IP 边缘网之间的互通没有问题。在 IP 边缘网采用 Interserv 体系结构的情况下，需要解决 Interserv 与 Diffserv 之间的互通问题，包括 Intserv 支持的业务与 Diffserv 支持的 PHB（Per-Hop Behavior，单中继段行为）之间的映射。

在 SC9600 中，用户可以根据 DiffServ（Differentiated Services）域中定义的报文优先级与 PHB(Per-Hop Behavior)行为之间的映射关系对报文进行简单流分类。对于来自上游设备的报文，在报文的入接口上绑定 DiffServ 域，在 DiffServ 域中将报文携带的优先级信息映射到相应的 PHB 行为、颜色，在设备内部，根据报文的 PHB 行为进行拥塞管理，根据报文的颜色进行拥塞避免；对于流向下游设备的报文，在报文的出接口上绑定 DiffServ 域，在 DiffServ 域中将报文的 PHB 行为、颜色映射为相应的优先级，下游设备根据报文的优先级提供相应的 QoS 服务。

简单流分类的分类依据有：

- VLAN 报文中的 802.1p 优先级
- IP 报文中的 DSCP 优先级
- MPLS 报文中的 EXP 优先级

## 5.2.2 Diffserv 配置

### 5.2.2.1 建立配置任务

#### 目的

使用本节操作建立配置任务，进行 diffserv 相关配置。对于来自上游设备的报文，用户可以根据报文携带的优先级进行分类，分类依据可以是 802.1p 优先级、dscp 优先级。在 DiffServ 域中定义优先级到 PHB 行为、颜色的映射关系，作为分类依据。将 DiffServ 域绑定到报文的入接口后，QoS 将能够在报文的出接口上根据报文的 PHB 行为和颜色进行拥塞管理和拥塞避免。

对于流向下游设备的报文，用户可以根据报文的 PHB 行为、颜色进行分类。在 DiffServ 域中定义 PHB 行为、颜色到优先级的映射关系，作为分类依据。将 DiffServ 域绑定到报文的出接口后，下游设备将能够根据报文的优先级提供相应的 QoS 服务。

### 5.2.2.2 创建 DiffServ 域并配置优先级映射关系

#### 目的

本节介绍如何创建 DiffServ 域并配置优先级映射关系。DiffServ 域由一组相连的 DiffServ 节点组成，这些相连的 DiffServ 节点采用相同的服务提供策略并实现相同 PHB 组集合。

当 SC9600 作为 DiffServ 域和其他网络的边界节点时，需要配置内部优先级（以 DiffServ 服务等级和颜色表示）和外部优先级（如 802.1p、DSCP）的相互映射关系。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
创建 Diffserv 域	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>diffServ domain default ds-domain-name</code>，创建 DiffServ 域并进入 DiffServ 域视图。</li> </ol>	<p><code>ds-domain-name</code>：diffserv 域的名称；</p> <p><code>default</code>：默认 Diffserv 域名。Default 域定义了缺省情况下报文的优先级和 PHB 行为、颜色之间的映射关系。用户可以修改 default 域中定义的映射关系，但不能删除 default 域；</p>
删除 Diffserv 域	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>no diffServ domain default ds-domain-name</code></li> </ol>	<p><code>ds-domain-name</code>：diffserv 域的名称；</p>
在报文的入接口，将 VLAN 报文的 802.1p 优先级映射为 PHB 行为，并为报文着色	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>diffServ domain (default ds-domain-name)</code>，创建 DiffServ 域并进入 DiffServ 域视图。</li> <li>3. 执行命令 <code>8021p-inbound 8021p-value phb service-class [color]</code></li> </ol>	<p><code>ds-domain-name</code>：diffserv 域的名称；</p> <p><code>default</code>：默认 Diffserv 域名。Default 域定义了缺省情况下报文的优先级和 PHB 行为、颜色之间的映射关系。用户可以修改 default 域中定义的映射关系，但不能删除 default 域；</p> <p><code>8021p-value</code>：VLAN 数据包里 8021p 协议优先级范围，整数形式，取值范围是 0~7；</p> <p><code>service-class</code>：phb 行为条目，包括 be af1 af2 af3 af4 ef cs6 cs7；</p> <p><code>[color]</code>：报文颜色标记，包括 green   yellow   red；</p>
在报文的出接口，将 PHB 行为、颜色映射为	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>diffServ domain</code></li> </ol>	<p><code>ds-domain-name</code>：diffserv 域的名称；</p> <p><code>default</code>：默认 Diffserv 域名。</p>

目的	步骤	参数说明
VLAN 报文的 802.1p 优先级	<p>(default ds-domain-name), 创建 DiffServ 域并进入 DiffServ 域视图。</p> <p>3. 执行命令 8021p-outbound service-class color map 8021p-value</p>	<p>Default 域定义了缺省情况下报文的优先级和 PHB 行为、颜色之间的映射关系。用户可以修改 default 域中定义的映射关系,但不能删除 default 域;</p> <p>8021p-value: VLAN 数据包里 8021p 协议优先级范围, 整数形式, 取值范围是 0~7;</p> <p>service-class: phb 行为条目, 包括 be af 1 af 2 af 3 af 4 ef  cs 6 cs 7;</p> <p>[color]: 报文颜色标记, 包括 green   yellow   red;</p>
在报文的入接口, 将 IP 报文的 DSCP 优先级映射为 PHB 行为, 并为报文着色	<p>1. 在特权用户视图下执行命令 configure 进入全局配置视图;</p> <p>2. 执行命令 diffServ domain (default ds-domain-name), 创建 DiffServ 域并进入 DiffServ 域视图。</p> <p>3. 执行命令 ip-dscp-inbound dscp-value phb service-class [color]</p>	<p>ds-domain-name: diffserv 域的名称;</p> <p>default: 默认 Diffserv 域名。</p> <p>Default 域定义了缺省情况下报文的优先级和 PHB 行为、颜色之间的映射关系。用户可以修改 default 域中定义的映射关系,但不能删除 default 域;</p> <p>dscp-value: IP 报文的 DSCP 优先级, 整数形式, 取值范围是 0~63;</p> <p>service-class: phb 行为条目, 包括 be af 1 af 2 af 3 af 4 ef  cs 6 cs 7;</p> <p>[color]: 报文颜色标记, 包括 green   yellow   red;</p>
在报文的出接口, 将 PHB 行为、颜色映射为 IP 报文的 DSCP 优先级	<p>1. 在特权用户视图下执行命令 configure 进入全局配置视图;</p> <p>2. 执行命令 diffServ domain (default ds-domain-name), 创建 DiffServ 域并进入 DiffServ 域视图。</p> <p>3. 执行命令 ip-dscp-outbound service-class color map dscp-value</p>	<p>ds-domain-name: diffserv 域的名称;</p> <p>default: 默认 Diffserv 域名。</p> <p>Default 域定义了缺省情况下报文的优先级和 PHB 行为、颜色之间的映射关系。用户可以修改 default 域中定义的映射关系,但不能删除 default 域;</p> <p>dscp-value: IP 报文的 DSCP 优先级, 整数形式, 取值范围是 0~63;</p>

目的	步骤	参数说明
		service-class: phb 行为条目，包 括 be af 1 af 2 af 3 af 4 ef  cs 6 cs 7; [color]: 报文颜色标记，包括 green   yellow   red;

### 5.2.2.3 配置端口信任的报文优先级

#### 目的

本节介绍如何配置端口信任的报文优先级。

SC9600 提供两种优先级信任模式：

#### 1. 信任报文的 802.1p 优先级

对于带 VLAN Tag 的报文，根据报文的 802.1p 优先级，查找 802.1p 优先级到内部优先级映射表，然后报文标记内部优先级，对于不带 VLAN Tag 的报文，SC9600 将使用端口的缺省 802.1p 优先级，根据此优先级查找 802.1p 优先级到内部优先级映射表，然后为报文标记内部优先级。

#### 2. 信任报文的 DSCP 优先级

根据报文的 DSCP 优先级，查找 DSCP 优先级到内部优先级映射表，为报文标记内部优先级。

说明：内部优先级以 DiffServ 模型的服务等级和颜色表示。

如果多个接口需要配置相同的信任报文优先级，可通过端口组进行配置，以减少重复配置工作。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置端口信任的报文优先级	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图； 2. 执行命令 <code>interface interface-type interface-number</code> 进入接口配置视图； 3. 执行命令 <code>trust [dot1p (inner outer)][DSCP]</code>	interface-type: 包括 3 种端口类型： fastethernet gigaehternet xgigaehternet interface-number: SC9600 系列交换机支持以下 3 种型号的接口配置范围：

目的	步骤	参数说明
		SC9603 : 取值范围是 <1-3>/<0-4>/<1-48> SC9608 : 取值范围是 <1-8>/<0-4>/<1-48> SC9612 : 取值范围是 <1-12>/<0-4>/<1-48> Inner outer: 采用内层或外层 802.1p 优先级; [[DSCP]: 对报文按照某类优先级进行映射; 缺省情况下, 端口不信任报文优先级;

### 5.2.2.4 应用 DiffServ 域

#### 目的

本节介绍如何应用 DiffServ 域。

当需要根据 DiffServ 域中定义的映射关系, 对来自上游设备的报文进行优先级到 PHB 行为和颜色之间的映射操作时, 可以将 DiffServ 域绑定到报文的入接口, 系统会根据 DiffServ 域中的映射关系将报文的优先级映射为相应的 PHB 行为和颜色。

当需要根据 DiffServ 域中定义的映射关系, 对流向下游设备的报文进行 PHB 行为到优先级之间的映射操作时, 可以将 DiffServ 域绑定到报文的出接口, 系统会根据 DiffServ 域中的映射关系将报文的 PHB 行为和颜色映射为优先级。

如果接口上配置了 trust diffServ domain recover 命令, 系统对出入该接口的报文恢复默认优先级映射。缺省情况下, 端口上不绑定 DiffServ 域, 系统采用缺省的优先级映射关系对出入接口的 报文进行优先级映射。

#### 过程

根据不同目的, 执行相应步骤, 具体参见下表。

目的	步骤	参数说明
在接口上绑定 DiffServ 域	1. 在特权用户视图下执行命令 configure 进入全局配置视图; 2. 执行命令 interface interface-type interface-number 进入接口配置视图; 3. 执行命令 trust diffServ domain [ds-domain-name default recover]	interface-type: 包括 3 种端口类型: fastethernet gigaehternet xgigaehternet interface-number: SC9600 系



目的	步骤	参数说明
		列交换机支持以下 3 种型号的接口配置范围： SC9603：取值范围是 <1-3>/<0-4>/<1-48> SC9608：取值范围是 <1-8>/<0-4>/<1-48> SC9612：取值范围是 <1-12>/<0-4>/<1-48> ds-domain-name: diffserv 域的名称； recover: 恢复缺省配置，即系统按缺省的映射关系进行优先级映射，用户未修改的最初的缺省配置； default: 默认 Diffserv 域名。缺省的 diffserv 域的名称，用户可以对其映射关系进行修改操作；
取消对报文按照某类优先级进行的映射	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图； 2. 执行命令 <code>interface interface-type interface-number</code> 进入接口配置视图； 3. 执行命令 <code>trust none</code>	-

### 5.2.2.5 检查配置结果

#### 目的

本节介绍如何检查配置结果。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
检查配置结果	1. 在特权用户视图下执行命令 <code>configure</code> 进入全局配置视图； 2. 执行命令 <code>show diffServ domain [configall domain]</code> 或 <code>show diffServ domain interface interface-type interface-number</code>	interface-type: 包括 3 种端口类型： fastethernet gigaehternet xgigaehternet interface-number: SC9600 系列交换机支持以下 3 种型号的接

目的	步骤	参数说明
	或 show diffServ domain name ds-domain-name	口配置范围： SC9603：取值范围是 <1-3>/<0-4>/<1-48> SC9608：取值范围是 <1-8>/<0-4>/<1-48> SC9612：取值范围是 <1-12>/<0-4>/<1-48> ds-domain-name: diffserv 域的 名称;

### 5.2.3 配置举例

#### 组网要求

SC9600 通过接口 GE2/0/1 与路由器互连, 企业用户和住宅用户可经由 SC9600 和路由器访问网络。企业用户和住宅用户的 VLAN ID 分别为 100, 200。由于企业用户需要得到更好的 QoS 保证, 因此将来自企业用户的数据报文优先级映射为 4, 将来自住宅用户的数据报文优先级映射为 2, 以提供差分服务。

#### 组网图



图 5-1 配置 Diffserv 的组网图

### 配置思路

采用如下的思路配置基于简单流分类的优先级映射：

1. 创建 VLAN，并配置各接口，使企业用户和住宅用户都能够通过 SC9600 访问网络。
2. 创建 DiffServ 域，将 802.1p 优先级映射为 PHB 行为和颜色。
3. 在 SC9600 入接口 GE1/0/1 和 GE1/0/2 上配置信任报文优先级。
4. 在 SC9600 入接口 GE1/0/1 和 GE1/0/2 上绑定 diffServ 域。

### 数据准备

为完成此配置例，需要准备如下的数据：

DiffServ 域的名称。

企业用户和住宅用户的报文的 802.1p 优先级。

企业用户和住宅用户的服务等级。

### 配置步骤

- 1、创建 VLAN 并配置各接口。
- 2、创建并配置 DiffServ 域。在 SC9600 上创建 DiffServ 域 ds1、ds2，并配置将企业用户和住宅用户的 802.1p 优先级映射到服务等级。

```
SC9600(config)#diffserv domain ds1
```

```
SC9600(config-dsdomain-ds1)#8021p-inbound 0 phb af4 green
```

```
SC9600(config-dsdomain-ds1)#quit
```

```
SC9600(config)#diffserv domain ds2
```

```
SC9600(config-dsdomain-ds2)#8021p-inbound 0 phb af2 green
```

```
SC9600(config-dsdomain-ds2)#quit
```

- 3、配置端口信任的报文优先级

```
SC9600(config)#interface gigabitethernet 1/0/1
```

```
SC9600(config-ge1/0/1)#trust dot1p outer
```

```
SC9600(config-ge1/0/1)#quit
```

```
SC9600(config)#interface gigabitethernet 1/0/2
```

```
SC9600(config-ge1/0/2)#trust dot1p outer
```

```
SC9600(config-ge1/0/2)#quit
```

4、将 DiffServ 域绑定到接口

将 DiffServ 域 ds1 和 ds2 分别绑定到接口 GE1/0/1、GE 1/0/2。

```
SC9600(config)#interface gigabitethernet 1/0/1
```

```
SC9600(config-ge1/0/1)#trust diffServ domain ds1
```

```
SC9600(config-ge1/0/1)#quit
```

```
SC9600(config)#interface gigabitethernet 1/0/2
```

```
SC9600(config-ge1/0/2)#trust diffServ domain ds2
```

```
SC9600(config-ge1/0/2)#quit
```

说明

缺省情况下，DiffServ 域中接口入方向上 VLAN 报文的 802.1p 优先级和 PHB 行为、颜色之间的映射关系：

802.1p 优先级	PHB 行为	Color
0	BE	green
1	AF1	green
2	AF2	green
3	AF3	green
4	AF4	green
5	EF	green
6	CS6	green
7	CS7	green

缺省情况下，DiffServ 域中接口出方向上 VLAN 报文的 PHB 行为、颜色和 802.1p 优先级之间的映射关系：

PHB 行为	Color	802.1p 优先级
BE	green	0
BE	yellow	0
BE	red	0
AF1	green	1
AF1	yellow	1
AF1	red	1
AF2	green	2
AF2	yellow	2
AF2	red	2
AF3	green	3
AF3	yellow	3
AF3	red	3
AF4	green	4
AF4	yellow	4

PHB 行为	Color	802.1p 优先级
AF4	red	4
EF	green	5
EF	yellow	5
EF	red	5
CS6	green	6
CS6	yellow	6
CS6	red	6
CS7	green	7
CS7	yellow	7
CS7	red	7

缺省情况下，DiffServ 域中接口入方向上 IP 报文的 DSCP 优先级和 PHB 行为、颜色之间的映射关系：

DSCP	PHB 行为	Color	DSCP	PHB 行为	Color
0	BE	green	32	AF4	green
1	BE	green	33	BE	green
2	BE	green	34	AF4	green
3	BE	green	35	BE	green
4	BE	green	36	AF4	yellow
5	BE	green	37	BE	green
6	BE	green	38	AF4	red
7	BE	green	39	BE	green
8	AF1	green	40	EF	green
9	BE	green	41	BE	green
10	AF1	green	42	BE	green
11	BE	green	43	BE	green
12	AF1	yellow	44	BE	green
13	BE	green	45	BE	green
14	AF1	red	46	EF	green
15	BE	green	47	BE	green
16	AF2	green	48	CS6	green
17	BE	green	49	BE	green
18	AF2	green	50	BE	green
19	BE	green	51	BE	green
20	AF2	yellow	52	BE	green
21	BE	green	53	BE	green
22	AF2	red	54	BE	green
23	BE	green	55	BE	green
24	AF3	green	56	CS7	green
25	BE	green	57	BE	green
26	AF3	green	58	BE	green
27	BE	green	59	BE	green
28	AF3	yellow	60	BE	green
29	BE	green	61	BE	green
30	AF3	red	62	BE	green
31	BE	green	63	BE	green

缺省情况下，DiffServ 域中接口出方向上 IP 报文的 PHB 行为、颜色和 DSCP 优先级之间的映射关系：

PHB 行为	Color	DSCP
BE	green	0
BE	yellow	0

PHB 行为	Color	DSCP
BE	red	0
AF1	green	10
AF1	yellow	12
AF1	red	14
AF2	green	18
AF2	yellow	20
AF2	red	22
AF3	green	26
AF3	yellow	28
AF3	red	30
AF4	green	34
AF4	yellow	36
AF4	red	38
EF	green	46
EF	yellow	46
EF	red	46
CS6	green	48
CS6	yellow	48
CS6	red	48
CS7	green	56
CS7	yellow	56
CS7	red	56

### 5.3 流量监管和流量整形配置

#### 目的

基于流的流量监管是指在设备上经过流分类后，对符合流分类的流量进行速率限制。通过监督进入设备的该类流量速率，丢弃超出速率限制的部分，使进入设备的该类流量被限制在一个合理的范围之内，从而保护网络资源和运营商的利益。基于流的流量监管采用双令牌桶技术。

通过 Meter 指定限速规则，包括 CIR、CBS、PIR 和 PBS，然后通过 ACL 指定流类型，并与 Meter 进行关联，ACL 即可以在物理接口（包括 Trunk）上使能，也可以在 VLAN 接口上使能。

SC9600 支持端口整形、端口队列整形两种流量整形，可根据需要选择配置。两种流量整形共存时，需要保证端口整形承诺信息速率（CIR）大于等于端口队列整形 CIR 之和；否则，流量整形会出现异常现象（如低优先级队列抢占高优先级队列的带宽）。

该命令用来配置 QoS CAR 模板（CIR、CBS、PIR、PBS），并应用于端口出方向和入方向。QoS CAR 应用在物理接口或 Eth-Trunk 接口上后，系统对该物理接口或 Eth-Trunk 接口上的所有上行报文进行限流。

接口上 QoS CAR 的优先级高于 VLAN 下的 QoS CAR，因此，如果接口上和 VLAN 下同时应用了 QoS CAR，系统优先选择接口上的 QoS CAR。

**cir-value**

指定承诺信息速率，即保证能够通过平均速率。

整数形式，取值范围是 64~4294967295，单位为 kbit/s。

**cbs-value**

指定承诺突发尺寸，即瞬间能够通过承诺突发流量。

整数形式，取值范围是 10000~4294967295，单位是 byte

**pir-value** 指定峰值信息速率

整数形式，取值范围是 64~4294967295，单位为 kbit/s。pir-value 必须大于等于 cir-value。pir-value 必须大于等于 cir-value，缺省等于 cir-value。如果指定的 pir-value 等于 cir-value，pbs-value 缺省为 0byte；否则，pbs-value 缺省为 pir-value 的 125 倍。

**pbs-value** 指定峰值突发尺寸。

整数形式，取值范围是 10000~4294967295，单位为 byte。pbs-value 必须大于等于 cbs-value。

**过程**

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置对某个 meter 进行绑定和解除绑定	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code>，进入全局视图。</li> <li>2. 执行命令 <code>filter-list number</code> 进入 filter 配置视图。</li> <li>3. 执行命令 <code>filter filter-number meter meter-number.</code></li> </ol>	缺省情况下，严格优先级调度算法。 <b>filter-number</b> 指定过滤器 filter 条目 整数形式，取值范围是 1~512
取消 filter 与某个 meter 的绑定关系	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code>，进入全局视图。</li> <li>2. 执行命令 <code>filter-list number</code> 进入 filter 配置视图。</li> <li>3. 执行命令 <code>no filter filter-number meter.</code></li> </ol>	<b>meter-number</b> 指定 meter 号 整数形式，取值范围是 1~112 <b>dscp</b> 指定 DSCP 值 整数形式，取值范围是 0-63
配置与 meter 绑定的 filter 条目的外部处理动作	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code>，进入全局视图。</li> <li>2. 执行命令 <code>filter-list number</code> 进入 filter 配置视图。</li> <li>3. 执行如下命令（根据需要）：  <code>filter filter-number outaction { red   yellow } drop</code>  <code>filter filter-number outaction { red   yellow } remark-dscp dscp</code> </li> </ol>	<b>meter-number</b> meter 号 整数形式，取值范围是 1~256 <b>cir-number</b> CIR 条目 整数形式，取值范围是 64-1024000

目的	步骤	参数说明
取消与 meter 绑定的 filter 条目的外部处理动作	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code>，进入全局视图。</li> <li>2. 执行命令 <code>filter-list number</code> 进入 filter 配置视图。</li> <li>3. 执行命令 <code>no filter filter-number outaction</code>。</li> </ol>	<p><code>cbs-number</code> CBS 条目 整数形式，取值范围是&lt;10000-4294967295&gt;</p> <p><code>ebs-number</code> EBS 条目 整数形式，取值范围是&lt;10000-4294967295&gt;</p>
配置通过 meter 对包括 CIR、CBS、PIR、EBS 和 PBS 的限速规则的指定。	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code>，进入全局视图。</li> <li>2. 执行如下命令（根据需要）：  <pre>meter meter-number cir cir-number cbs cbs-number ebs ebs-number meter meter-number cir cir-number cbs cbs-number ebs ebs-number { aware   blind } meter meter-number cir cir-number cbs cbs-number pbs pbs-number pir pir-number meter meter-number cir cir-number cbs cbs-number pbs pbs-number pir pir-number { aware   blind } no meter meter-number</pre> </li> </ol>	<p><code>pbs-number</code> PBS 条目 整数形式，取值范围是&lt;10000-4294967295&gt;</p> <p><code>pir-number</code> PIR 条目 整数形式，取值范围是&lt;64-1024000&gt;</p>

## 5.4 队列调度和拥塞控制配置

### 5.4.1 队列调度和拥塞控制概述

#### 拥塞影响

所谓拥塞，是指由于供给资源的相对不足而造成转发速率下降、引入额外的延迟的一种现象。

链路带宽的瓶颈会导致拥塞，任何用以正常转发处理的资源的不足，如可分配的处理时间、缓冲区、内存资源的不足，都会造成拥塞。在目前多业务应用的复杂网络环境下，拥塞极为常见。

拥塞有可能会引发一系列的负面影响：

- 拥塞增加了报文传输的延迟和抖动，过高的延迟会引起报文重传。
- 拥塞使网络的有效吞吐率降低，造成网络资源的利用率降低。
- 拥塞加剧会耗费大量的网络资源（特别是存储资源），不合理的资源分配甚至可能导致系统陷入资源死锁而崩溃。



队列技术

拥塞管理的中心内容：当拥塞发生时如何制定一个资源的调度策略，决定报文转发的处理次序。对于拥塞管理，一般采用队列技术，使用一个队列算法对流量进行分类，之后用某种优先级算法将这些流量发送出去。每种队列算法都是用以解决特定的网络流量问题，并对带宽资源的分配、延迟、抖动等有着十分重要的影响。

SC9600 支持的队列调度算法

- SP 严格优先级队列

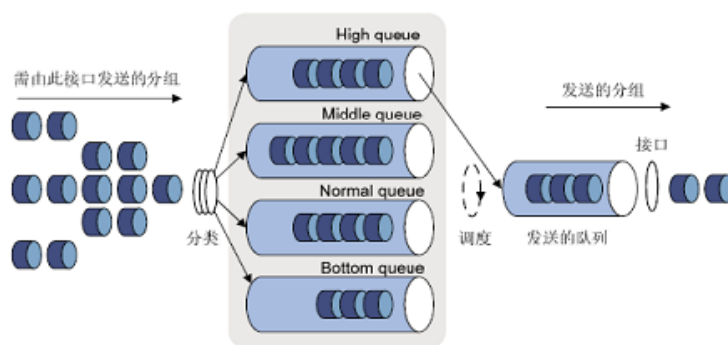


图 5-2 SP 队列调度

在 SP (STRICT PRIORITY) 队列调度时，严格按照优先级从高到低的次序，优先发送较高优先级队列中的分组，当较高优先级队列为空时，再发送较低优先级队列中的分组。

将关键业务的分组放入较高优先级的队列，将非关键业务的分组放入较低优先级的队列，可以保证关键业务的分组被优先传送，非关键业务的分组在处理关键业务数据的空闲间隙被传送。通常交换芯片支持最大 8 个队列。

- RR 轮换调度队列

ROUND ROBIN,即轮换调度，出现拥塞时,各非空输出队列的输出带宽相同,总量等于端口带宽。

- WRR 加权平均队列

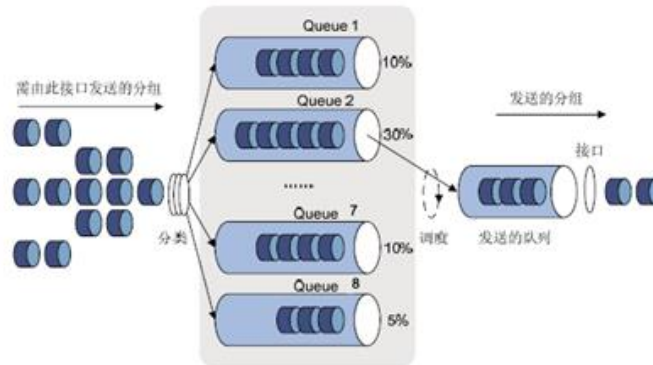


图 5-3 WRR 队列调度

WRR (WEIGHTED ROUND ROBIN) 算法在端口队列之间进行轮流调度，保证每个队列都得到一定的服务时间。出现拥塞时，各非空输出队列的按照设定的比例输出带宽，总量等于端口可用带宽。

优点 1：这样可以保证最低优先级队列至少获得部分带宽，避免了采用 SP 调度时低优先级队列中的报文可能长时间得不到服务的缺点。

优点 2：虽然多个队列的调度是轮循进行的，但对每个队列不是固定地分配服务时间片；如果某个队列为空，那么马上换到下一个队列调度，这样带宽资源可以得到充分的利用。

- DRR 调度队列

DRR (Deficit Round Robin) 调度实现原理与 WRR 调度基本相同。

DRR 与 WRR 的区别是：WRR 调度是按照报文个数进行调度，而 DRR 是按照报文长度进行调度。如果报文长度超过了队列的调度能力，DRR 调度允许出现负权重，以保证长报文也能够得到调度。但下次轮循调度时该队列将不会被调度，直到权重为正，该队列才会参与 DRR 调度。

## 5.4.2 配置队列调度及拥塞控制

### 前提条件

配置队列调度及拥塞控制之前，还需要配置 ACL 的 filter 规则，请参考本手册 7.2ACL 配置的相关操作来配置 ACL 规则的处理动作为指定数据包通过的端口队列优先级。

### 目的

使用本节操作配置队列调度及拥塞控制，当网络中发生拥塞时，SC9600 将按照是定的调度策略决定报文转发时的处理次序，从而均衡各类报文的延迟和延迟抖动，保证关键业务的报文能够得到优先处理且非关键业务相同优先级业务得到公平处理。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
(可选)配置端口队列的调度优先级	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>interface { fastethernet   gig Ethernet   xgig Ethernet } interface-number</b> 进入接口配置视图;</li> <li>3. 执行命令 <b>cos queue queue-number priority { priority   default }</b> 或执行命令 <b>cos queue queue-list priority { priority   default }</b> 配置端口队列的调度优先级;</li> <li>4. 结束。</li> </ol>
(可选)配置端口最大队列数	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>cos max-queue { 1 / 8 }</b> 配置端口最大队列数;</li> <li>3. 结束。</li> </ol>
置端口队列的调度模式	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>interface { fastethernet   gig Ethernet   xgig Ethernet } interface-number</b> 进入接口配置视图;</li> <li>3. 执行命令 <b>cos scheduling { sp   rr   wrr   drr }</b> 或执行命令 <b>cos scheduling { sp+rr   sp+wrr   sp+drr } queue-list</b> 配置端口队列的调度模式;</li> <li>4. 结束。</li> </ol>
(可选)配置端口队列的权重	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>interface { fastethernet   gig Ethernet   xgig Ethernet } interface-number</b> 进入接口配置视图;</li> <li>3. 执行命令 <b>cos queue queue-number weight weight</b> 或执行命令 <b>cos queue queue-list weight weight</b> 配置端口队列的权重;</li> <li>4. 结束。</li> </ol>
(可选)配置队列的有效带宽	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>interface { fastethernet   gig Ethernet   xgig Ethernet } interface-number</b> 进入接口配置视图;</li> <li>3. 执行命令 <b>cos queue { queue-number   queue-list } { min-bandwidth   max-bandwidth } 64kbps bandwidth-value1</b> 或执行命令 <b>cos queue { queue-number   queue-list } { min-bandwidth   max-bandwidth } mbps bandwidth-value2</b> 配置队列的有效带宽;</li> <li>4. 结束。</li> </ol>

附表:

参数	说明	取值
1	队列条数为 1	-
8	队列条数为 8	-
queue-number	队列号	整数形式, 取值范围是 0-7
priority	优先级条目	整数形式, 取值范围是 0-7
default	缺省值	1
queue-list	指定队列序列	整数形式, 形如: 1,2, 取值范围是 0~7
weight	权重条目	整数形式, 取值范围是 0-100
sp	Strict Priority, 严格优先级模式	-
rr	Round Robin, 轮询调度模式	-
wrr	Weighted Round Robin, 权重轮询调度模式	-
drr	Deficit Round Robin, 变长双轮询调度模式	-
bandwidth-value1	指定以 64Kbps 为粒度的带宽值	整数形式, 取值范围是 1~16000
bandwidth-value2	指定以 1Mbps 为粒度的带宽值	整数形式, 取值范围是 1~1000

### 5.4.3 维护及调试

#### 目的

当队列调度及拥塞控制功能不正常, 需要进行查看、调试或定位问题时, 可以使用本节操作。

#### 过程

根据不同目的, 执行相应步骤, 具体参见下表。

目的	步骤
查看接口 QoS 配置信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图, 或执行命令 <b>configure</b> 进入全局配置视图, 或执行命令 <b>interface tunnel tunnel-num</b> 进入 tunnel 接口配置视图, 或不执行任何命令保持当前特权用户视图;</li> <li>2. 执行命令 <b>show cos interface</b> 或执行命令 <b>show cos interface { fastethernet   gigabitethernet   xgigabitethernet } interface-number</b> 用来显示接口 QoS 配置信息;</li> <li>3. 结束。</li> </ol>

附表:

参数	说明	取值
interface-number	指定接口号	SC9600 系列交换机支持以下 3 种型号的接口配置范围:

参数	说明	取值
		SC9603: 取值范围是<1-3>/<0-4>/<1-48>
		SC9608: 取值范围是<1-8>/<0-4>/<1-48>
		SC9612: 取值范围是<1-12>/<0-4>/<1-48>

## 5.4.4 配置举例

### 5.4.4.1 SP 调度配置示例

#### 组网要求

流量从站点的端口口 1/0/1、1/0/2、1/0/3 上到站点 2 后，在端口 1/0/1 产生拥塞，要求使用调度算法为 SP。

#### 组网图

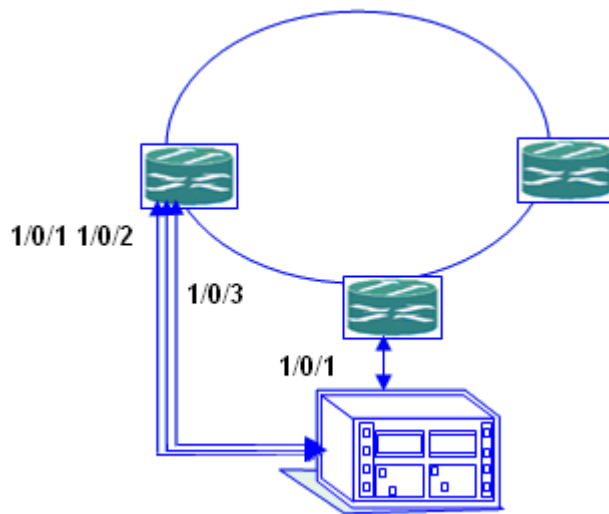


图 5-4 配置端口队列优先级调度组网图

#### 配置步骤

1、 站点 1 的配置。

//端口 1/0、1 的配置

```
S1#configure
```

```
S1(config)#interface gigabitEthernet 1/0/1
```

```
S1(config-ge1/0/1)#priority 1
```

```
S1(config-ge1/0/1)#quit
```

```
退出端口 1/0/1 的配置
//端口 1/0/2 的配置
S1#configure
S1(config)#interface gigabitEthernet 1/0/2
S1(config-ge1/0/2)#priority 2
S1(config-ge1/0/2)#quit
退出端口 1/0/2 的配置
//端口 1/0/3 的配置
S1#configure
S1(config)#interface gigabitEthernet 1/0/3
S1(config-ge1/0/3)#priority 3
S1(config-ge1/0/3)#quit
退出端口 1/0/3 的配置
2、站点 2 的配置。
//配置 ACL 规则
S2#configure
S2(config)#filter-list 1001
S2(config-filter-ipv4-1001)#filter 1 ip 10.164.1.0/24 10.164.9.9/32
S2(config-filter1)#filter 1 action cos 7
//配置端口 1/0/1
S2#configure
S2(config)#interface ge 1/0/1
S2(config-ge1/0/1)#cos schedule sp
S2(config-ge1/0/1)#filter-list in 1
```

## 第6章 组播配置

### 6.1 概述

本章介绍了 SC9600 系列高端交换机组播配置操作。

本章包括如下主题：

内容	页码
6.1 概述	6-1
6.2 IGMP Snooping 配置	6-1
6.3 MLD Snooping 配置	6-20

### 6.2 IGMP Snooping 配置

#### 6.2.1 IGMP Snooping 简介

##### IGMP Snooping 基本原理

IGMP Snooping 是 Internet Group Management Protocol Snooping（互联网组管理协议窥探）的简称。它是运行在二层设备上的组播约束机制。该协议通过侦听网络上用户主机和路由器间传递的 IGMP 报文，通过对收到的 IGMP 报文进行分析，为端口和 MAC 组播地址建立起映射关系，并根据这样的映射关系转发组播数据，从而管理和控制组播组。

当二层设备没有运行 IGMP Snooping 时，组播数据在二层被广播；当二层设备运行了 IGMP Snooping 后，已知组播组的组播数据不会在二层被广播，而在二层被组播给指定的接收者。

##### IGMP Snooping 优点

IGMP Snooping 具有优点：

- 增强了组播信息的安全性

- 减少了二层网络中的广播报文，节约了带宽
- 为实现每台用户主机的单独计费提供了方便

### SC9600 支持的 IGMP Snooping 特性

- 支持静态二层组播

以太网在传输组播报文时，报文的目的地不是一个具体的接收者，而是一个成员不确定的组。因此当组播报文由网络层转发到链路层时，无法生成组播转发表项，从而导致组播报文在链路层采用广播方式。当设备部署在路由器和用户主机之间，应用二层转发特性时，配置静态二层组播（即手工配置转发表项），可以把组播数据转发给需要长期接收该数据的用户。

静态二层组播的特点：

配置接口静态加入组播组，可以避免协议报文的攻击。

采用直接查找组播报文转发表转发报文的机制，可以减少网络的延时。

避免未注册用户收到组播报文，提供有偿服务。

- 支持组播 VLAN 复制

在传统组播转发方式下，属于不同 VLAN 的用户分别点播统一组播源时，需要交换机为每个 VLAN 都复制一份组播数据，再分别传送给每个 VLAN。配置了组播 VLAN 复制功能后，属于不同 VLAN 的用户分别点播同一组播源时，设备将这些 VLAN 的都配置对应一个组播 VLAN。这样，上层路由器只需把一份组播数据传送给该组播 VLAN 即可，而不必再为每个 VLAN 都复制一份组播数据。

应用组播 VLAN 复制功能便于对组播源和组播组成员进行管理和控制，同时也可以减少带宽的浪费，减小网络的额外负担。

- 支持基于 VLAN 的 IGMP Snooping

IGMP 版本可以配置 V1/V2/V3

组播转发模式可配

支持静态路由接口

支持 IGMP 查询功能

支持 IGMP 报文抑制

支持接口快速离开



- 路由接口老化时间可配
- 组成员最大响应时间可配
- 组播策略可配
- Router Alert 选项可配
- 发送 IGMP 报文的源 IP 地址可配
- 支持 IGMP Proxy 功能

## 6.2.2 配置静态二层组播

### 背景信息

在城域以太网中，当用户主机需要长期接收某个组播组的组播数据流时，可以配置接口静态加入组播组。

### 目的

配置该功能后，用户能够长期、稳定、及时的收到已注册的组播数据流。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
全局使能 IGMP Snooping	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>igmp-snooping start</b> 全局使能组播监听功能；</li> <li>3. 结束。</li> </ol>
创建组播 VLAN	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>vlan vlan-list</b> 创建需要使能 IGMP Snooping 的 VLAN；</li> <li>3. 执行命令 <b>igmp-snooping mvlan vlan-id</b> 创建相应组播 VLAN 并进入组播 VLAN 配置视图 ；</li> <li>4. 结束。</li> </ol>
（可选）配置组播 VLAN 中组播数据转发模式	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>igmp-snooping mvlan vlan-id</b> 进入组播 VLAN 配置视图 ；</li> <li>3. 执行命令 <b>igmp-snooping forwarding-mode { ip   mac }</b>配置组播数据转发模式；</li> <li>4. 结束。</li> </ol>
配置接口加入 VLAN 并在接口上使能 IGMP Snooping 协议	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface { fastethernet   gigasethernet   xgigaethernet } interface-number</b> 进入接口配置视图；</li> <li>3. 执行命令 <b>port hybrid vlan vlan-list { tagged   untagged }</b>配置接口加</li> </ol>

目的	步骤
	入 VLAN; 4. 执行命令 <b>igmp-snooping enable</b> 配置在接口上使能组播监听; 5. 结束。
配置接口静态加入组播组	1. 执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b> 进入接口配置视图; 3. 执行命令 <b>igmp-snooping static-group group-address group-address mvlan vlan-id</b> 配置接口静态加入组播组; 4. 结束。

附表:

参数	说明	取值
vlan-id	VLAN 条目	整数形式, 取值范围是 1-4094。
interface-number	以太网 slot 号/ Card 号/ port 号	SC9600 系列交换机支持以下 3 种型号的接口配置范围: SC9603 : 取值范围是 <1-3>/<0-4>/<1-48> SC9608 : 取值范围是 <1-8>/<0-4>/<1-48> SC9612 : 取值范围是 <1-12>/<0-4>/<1-48>
group-address	组播 IP 地址	组地址范围为: 224.0.0.0 — 239.255.255.255
ip	表示组播数据按 IP 地址转发	-
mac	表示组播数据按 MAC 地址转发。	-

### 6.2.3 配置组播 VLAN 复制

#### 背景信息

通过组播 VLAN 复制功能, 可以对组播源和组播组成员进行管理和控制, 实现不同 VLAN 内的用户接收相同的组播流, 同时也可以减少带宽浪费。

组播 VLAN 复制功能中的 VLAN 分为组播 VLAN 和用户 VLAN。组播 VLAN 是交换机与组播源相连的接口所属的 VLAN, 用于实现组播流的汇聚; 用户 VLAN 是与组播组成员主机相连的接口所属的 VLAN, 用于接收组播 VLAN 的数据流。

#### 目的

通过配置各参数, 以满足在不同应用环境中的需求。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
全局使能 IGMP Snooping	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>igmp-snooping start</b> 全局使能组播监听功能；</li> <li>3. 结束。</li> </ol>
创建组播 VLAN	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>vlan vlan-list</b> 创建需要使能 IGMP Snooping 的 VLAN；</li> <li>3. 执行命令 <b>igmp-snooping mvlan vlan-id</b> 创建相应组播 VLAN 并进入组播 VLAN 配置视图；</li> <li>4. 结束。</li> </ol>
配置组播 VLAN 中组播数据转发模式为 IP	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>igmp-snooping mvlan vlan-id</b> 进入组播 VLAN 配置视图；</li> <li>3. 执行命令 <b>igmp-snooping forwarding-mode ip</b> 配置组播数据转发模式为 IP 模式；</li> <li>4. 结束。</li> </ol>
使能组播 VLAN 的组播复制功能	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>igmp-snooping mvlan vlan-id</b> 进入组播 VLAN 配置视图；</li> <li>3. 执行命令 <b>igmp-snooping multicast-vlan enable</b> 使能组播 VLAN 复制功能；</li> <li>4. 结束。</li> </ol>
配置用户 VLAN	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>igmp-snooping mvlan vlan-id</b> 进入组播 VLAN 配置视图；</li> <li>3. 执行命令 <b>igmp-snooping multicast user-vlan vlan-list</b> 配置用户 VLAN；</li> <li>4. 结束。</li> </ol>
配置接口加入 VLAN 并在接口上使能 IGMP Snooping 协议	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface { fastethernet   gigaethernet   xgigaethernet } interface-number</b> 进入接口配置视图；</li> <li>3. 执行命令 <b>port hybrid vlan vlan-list { tagged   untagged }</b> 配置接口加入 VLAN；</li> <li>4. 执行命令 <b>igmp-snooping enable</b> 配置在接口上使能组播监听；</li> <li>5. 结束。</li> </ol>

附表：

参数	说明	取值
vlan-id	VLAN 条目	整数形式，取值范围是 1-4094。
vlan-list	VLAN 列表	整数形式，取值范围是 1~4094，形如：1,3-5

## 6.2.4 配置 IGMP Snooping

背景信息

基于 VLAN 的 IGMP Snooping 运行在位于路由器和用户主机之间的交换机上，通过侦听上层路由器和主机之间发送的组播协议报文来维护组播报文的转发表项，从而管理和控制组播数据报文的转发，实现二层组播。

### 目的

通过配置各参数，以满足在不同应用环境中的需求。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
全局使能 IGMP Snooping	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>igmp-snooping start</b> 全局使能组播监听功能；</li> <li>3. 结束。</li> </ol>
创建组播 VLAN	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>vlan vlan-list</b> 创建需要使能 IGMP Snooping 的 VLAN；</li> <li>3. 执行命令 <b>igmp-snooping mvlan vlan-id</b> 创建相应组播 VLAN 并进入组播 VLAN 配置视图；</li> <li>4. 结束。</li> </ol>
（可选）配置组播 VLAN 中组播数据转发模式	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>igmp-snooping mvlan vlan-id</b> 进入组播 VLAN 配置视图；</li> <li>3. 执行命令 <b>igmp-snooping forwarding-mode { ip   mac }</b> 配置组播数据转发模式；</li> <li>4. 结束。</li> </ol>
（可选）配置 IGMP 版本	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>igmp-snooping mvlan vlan-id</b> 进入组播 VLAN 配置视图；</li> <li>3. 执行命令 <b>igmp-snooping version { v1   v2   v3 }</b> 配置 IGMP 版本；</li> <li>4. 结束。</li> </ol>
（可选）配置静态路由器接口	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>igmp-snooping mvlan vlan-id</b> 进入组播 VLAN 配置视图；</li> <li>3. 执行命令 <b>igmp-snooping uplink-port { fastethernet   gigasethernet   xgigasethernet } interface-number</b> 配置静态路由器接口；</li> <li>4. 结束。</li> </ol>
（可选）配置查询器	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>igmp-snooping query-interval query-interval</b> 配置查询器发送查询报文间隔（各组播 VLAN 共用此参数）；</li> <li>3. 执行命令 <b>igmp-snooping robust-count robust-count</b> 配置查询器的 IGMP 健壮系数（各组播 VLAN 共用此参数）；</li> <li>4. 执行命令 <b>igmp-snooping lastmember-queryinterval query-Interval</b> 配置特定组查询的查询间隔（各组播 VLAN 共用此参数）；</li> <li>5. 执行命令 <b>igmp-snooping lastmember-querynumber query-number</b></li> </ol>

目的	步骤
	配置特定查询的次数（各组播 VLAN 共用此参数）； 6. 执行命令 <b>igmp-snooping mvlan <i>vlan-id</i></b> ，进入组播 VLAN 配置视图； 7. 执行命令 <b>igmp-snooping querier { enable   disable }</b> 配置 IGMP snooping 查询器的使能状态； 8. 执行命令 <b>igmp-snooping max-response-time <i>response-time</i></b> 配置通用查询报文中最大响应时间字段值； 9. 结束。
（可选）配置组播策略	1. 执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>igmp-snooping mvlan <i>vlan-id</i></b> 进入组播 VLAN 配置视图； 3. 执行命令 <b>igmp-snooping group-policy filter-list <i>filter-number version version-List</i></b> 配置组播策略； 4. 结束。
（可选）配置协议报文抑制	1. 执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>igmp-snooping mvlan <i>vlan-id</i></b> 进入组播 VLAN 配置视图； 3. 执行命令 <b>igmp-snooping report-suppress { enable   disable }</b> 配置 VLAN 内报文抑制使能状态； 4. 结束。
（可选）配置查询报文中的源 IP	1. 执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>igmp-snooping mvlan <i>vlan-id</i></b> ，进入组播 VLAN 配置视图； 3. 执行命令 <b>igmp-snooping proxy-ip <i>ip-address</i></b> 配置查询报文中的源 IP，此配置只要在开启了报文抑制，或者工作在 proxy 时才生效； 4. 结束。
（可选）配置 router-alert 选项需求	1. 执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>igmp-snooping mvlan <i>vlan-id</i></b> ，进入组播 VLAN 配置视图； 3. 执行命令 <b>igmp-snooping require-router-alert { enable   disable }</b> 配置 router-alert 需求，此配置使能后只处理携带 router-alert 选项的 IGMP 协议报文； 4. 结束。
（可选）配置组播 VLAN 工作模式	1. 执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>igmp-snooping mvlan <i>vlan-id</i></b> ，进入组播 VLAN 配置视图； 3. 执行命令 <b>igmp-snooping workmode { igmp-proxy   igmp-snooping }</b> 配置组播 VLAN 工作模式为 snooping 模式或者 proxy 模式； 4. 结束。
（可选）配置接口快速离开	1. 执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } <i>interface-number</i></b> 进入接口配置视图； 3. 执行命令 <b>igmp-snooping fast-leave { enable   disable }</b> 配置接口快速离开功能； 4. 结束。

附表：

参数	说明	取值
vlan-id	VLAN 条目	整数形式，取值范围是 1-4094。
interface-number	以太网 slot 号/ Card 号/ port 号	SC9600 系列交换机支持以下 3 种型号的接口配置范围： SC9603：取值范围是 <1-3>/<0-4>/<1-48> SC9608：取值范围是 <1-8>/<0-4>/<1-48> SC9612：取值范围是 <1-12>/<0-4>/<1-48>
query-interval	查询间隔时间范围	整数形式，取值范围是 10-65535
robust-count	发送特定查询报文的次数，用来指示当前 VLAN 内的 IGMP 健壮系数	整数形式，取值范围是 2-5
query-number	特定查询次数范围	整数形式，取值范围是 2-16。
query-interval	特定查询间隔范围	整数形式，取值为秒，范围是 1-5
max-response-time	最大响应时间范围	整数形式，取值为秒，取值范围是 1-25。
ip-address	目的 IP 地址	点分十进制形式，如：(A.B.C.D)，其中 A~D 为 0~255 十进制数。

## 6.2.5 维护及调试

### 目的

当 IGMP Snooping 功能不正常，需要进行查看、调试或定位问题时，可以使用本小节操作。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
打开 IGMP Snooping 调试功能	1. 执行命令 <b>disable</b> 退出到普通用户视图或不执行任何命令保持当前特权用户视图； 2. 执行命令 <b>debug igmpsnoop</b> 打开 IGMP Snooping 调试功能； 3. 结束。
关闭 IGMP Snooping 调试功能	1. 执行命令 <b>disable</b> 退出到普通用户视图或不执行任何命令保持当前特权用户视图； 2. 执行命令 <b>no debug igmpsnoop</b> 关闭 IGMP Snooping 调试功能； 3. 结束。

目的	步骤
查看 IGMP Snooping 配置文件信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图或执行命令 <b>configure</b> 进入全局配置视图或执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b> 进入接口配置视图；</li> <li>2. 执行命令 <b>show igmp-snooping config</b> 显示 IGMP Snooping 配置文件信息</li> <li>4. 结束。</li> </ol>
查看 IGMP Snooping 接口配置文件信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图或执行命令 <b>configure</b> 进入全局配置视图或执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b> 进入接口配置视图；</li> <li>2. 执行命令 <b>show igmp-snooping interface</b> 显示 IGMP Snooping 接口配置文件信息</li> <li>3. 结束。</li> </ol>
查看 IGMP Snooping 组播 VLAN 配置文件信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图或执行命令 <b>configure</b> 进入全局配置视图或执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b> 进入接口配置视图；</li> <li>2. 执行命令 <b>show igmp-snooping mvlan</b> 显示 IGMP Snooping 组播 vlan 配置文件信息</li> <li>3. 结束。</li> </ol>
查看 IGMP Snooping 路由端口配置文件信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图或执行命令 <b>configure</b> 进入全局配置视图或执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b> 进入接口配置视图；</li> <li>2. 执行命令 <b>show igmp-snooping uplinkport</b> 显示 IGMP Snooping 路由端口配置文件信息</li> <li>3. 结束。</li> </ol>
查看 IGMP Snooping 全部、指定接口或指定 VLAN 出端口表项信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图或执行命令 <b>configure</b> 进入全局配置视图或执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b> 进入接口配置视图；</li> <li>2. 执行命令 <b>show igmp-snooping egress-port</b> 或 <b>show igmp-snooping egress-port mvlan vlan-id</b> 或 <b>show igmp-snooping egress-port interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b> 显示 IGMP Snooping 出端口表项信息；</li> <li>3. 结束。</li> </ol>
查看 IGMP Snooping 组播组表项信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图或执行命令 <b>configure</b> 进入全局配置视图或执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b> 进入接口配置视图；</li> <li>2. 执行命令 <b>show igmp-snooping group</b> 显示 IGMP Snooping 组播组表项信息</li> <li>3. 结束。</li> </ol>
查看 IGMP Snooping 组播源表项信	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图或执行命令 <b>configure</b> 进入全局配置视图或执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b> 进入接口配置视图；</li> </ol>

目的	步骤
息 (version 3 时有效)	2. 执行命令 <code>show igmp-snooping source-address</code> 显示 IGMP Snooping 组播组表项信息 3. 结束。

附表:

参数	说明	取值
interface-number	以太网 slot 号/ Card 号/ port 号	SC9600 系列交换机支持以下 3 种型号的接口配置范围: SC9603 : 取值范围是 <1-3>/<0-4>/<1-48> SC9608 : 取值范围是 <1-8>/<0-4>/<1-48> SC9612 : 取值范围是 <1-12>/<0-4>/<1-48>
vlan-id	VLAN 条目	整数形式, 取值范围是 1-4094。

## 6.2.6 配置举例

### 6.2.6.1 配置静态二层组播举例

#### 组网要求

交换机接口 GE1/0/1 连接组播源测路由器, 接口 GE1/0/2 连接用户主机, 要求通 VLAN 100 内的所有主机能长期接收组地址为 225.1.1.1 的组播数据。

#### 组网图



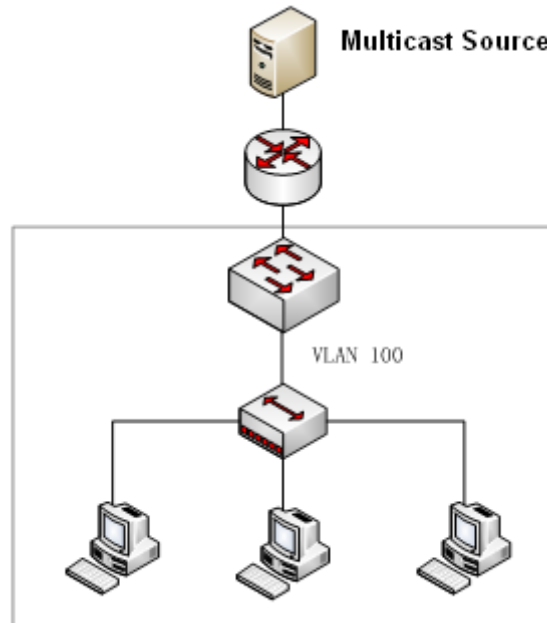


图 6-1 静态二层组播组网图

### 配置步骤

#### 1、全局使能 IGMP snooping 协议。

```
SC9600#configure
SC9600(config)# igmp-snooping start;
SC9600(config)#
```

#### 2、创建 VLAN 和相应的组播 VLAN，配置接口加入 VLAN。

```
SC9600(config)#Vlan 100
SC9600(vlan-100)#quit
SC9600(config)#interface gigabitEthernet 1/0/1
SC9600(config-gigabitEthernet1/0/1)#port hybrid vlan 100 tagged
SC9600(config-gigabitEthernet1/0/1)#quit
SC9600(config)#interface gigabitEthernet 1/0/2
SC9600(config-gigabitEthernet1/0/2)#port hybrid vlan 100 tagged
SC9600(config-gigabitEthernet1/0/2)#quit
SC9600(config)# igmp-snooping mVlan 100
SC9600(config-igmp-snooping-mVlan100)#quit
SC9600(config)#
```

#### 3、在接口下使能 IGMP Snooping 协议。

```
SC9600(config)#interface gigabitEthernet 1/0/1
SC9600(config-gigabitEthernet1/0/1)#igmp-snooping enable
SC9600(config-gigabitEthernet1/0/1)#quit
SC9600(config)#interface gigabitEthernet 1/0/2
SC9600(config-gigabitEthernet1/0/2)#igmp-snooping enable
SC9600(config-gigabitEthernet1/0/2)#quit
SC9600(config)#
```

**4、配置 GE1/0/1 为静态路由器接口。**

```
SC9600(config)#igmp-snooping mVlan 100
SC9600(config-igmp-snooping-mVlan100)#igmp-snooping uplink-port gigabitEthernet 1/0/1
SC9600(config-igmp-snooping-mVlan100)#quit
SC9600(config)#
```

**5、配置静态组播组。**

```
SC9600(config)#interface gigabitEthernet 1/0/2
SC9600(config-gigabitEthernet1/0/2)#igmp-snooping static-group group-address 225.1.1.1 mVlan 100
SC9600(config-gigabitEthernet1/0/2)#quit
SC9600(config)#
```

**6、配置结束，检查组播组表和出端口表信息。**

```
SC9600#show igmp-snooping group
Total Entry(s) : 1
Group Address   MVlan  Pre-join  MemNum  V3FilterMode
225.1.1.1      100    disable   1        invalid
```

```
SC9600#show igmp-snooping egress-port
```

```
Total Entry(s) : 1
```

```
Group Address : 225.1.1.1
```

```
MVlan : 100
```

```
Source Address : *
```

```
Interface : ge-1/0/2
```

```
Type : static
```

```
Expires : ---
```

```
OutVlan : 100
```

```
V3 Mode : invalid
```

### 6.2.6.2 配置 IGMP Snooping 举例

#### 组网要求

交换机接口 GE1/0/1 连接组播源测路由器，接口 GE1/0/2 连接用户主机，要求通过配置 IGMP Snooping 功能实现 VLAN100 内的三台主机能长期接收组地址为 225.1.1.1~225.1.1.2 的组播数据

#### 组网图

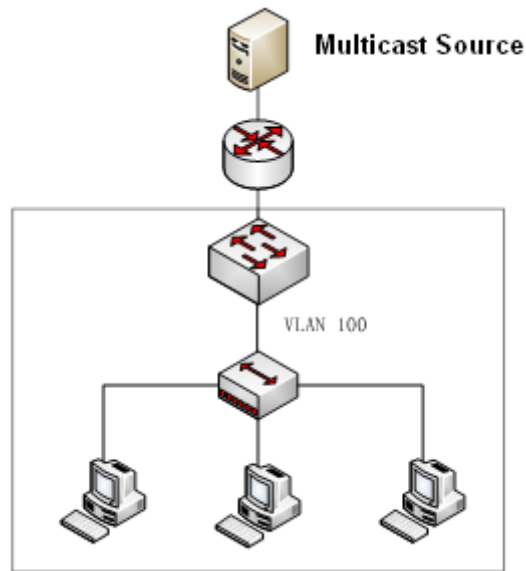


图 6-2 igmp-snooping 配置组网图

#### 配置步骤

1、全局使能 IGMP snooping 协议。

```
SC9600#configure
SC9600(config)#igmp-snooping start;
SC9600(config)#
```

2、创建 VLAN 和相应的组播 VLAN，配置接口加入 VLAN。

```
SC9600(config)#vlan 100
SC9600(vlan-100)#quit
SC9600(config)#interface gigabitEthernet 1/0/1
SC9600(config-gigabitEthernet 1/0/1)#port hybrid vlan 100 tagged
SC9600(config-gigabitEthernet 1/0/1)#quit
SC9600(config)#interface gigabitEthernet 1/0/2
```

```
SC9600(config-ge1/0/2)#port hybrid vlan 100 tagged
```

```
SC9600(config-ge1/0/2)#quit
```

```
SC9600(config)# igmp-snooping mvlan 100
```

```
SC9600(config-igmpsnoop-mvlan100)#quit
```

```
SC9600(config)#
```

3、在接口下使能 IGMP Snooping 协议。

```
SC9600(config)#interface gigaethernet 1/0/1
```

```
SC9600(config-ge1/0/1)#igmp-snooping enable
```

```
SC9600(config-ge1/0/1)#quit
```

```
SC9600(config)#interface gigaethernet 1/0/2
```

```
SC9600(config-ge1/0/2)#igmp-snooping enable
```

```
SC9600(config-ge1/0/2)#quit
```

```
SC9600(config)#
```

4、配置 GE1/0/1 为静态路由器接口。

```
SC9600(config)#igmp-snooping mvlan 100
```

```
SC9600(config-igmpsnoop-mvlan100)#igmp-snooping uplink-port gigaethernet 1/0/1
```

```
SC9600(config-igmpsnoop-mvlan100)#quit
```

```
SC9600(config)#
```

5、配置静态组播组。

```
SC9600(config)#interface gigaethernet 1/0/2
```

```
SC9600(config-ge1/0/2)#igmp-snooping static-group group-address 225.1.1.1 mvlan 100
```

```
SC9600(config-ge1/0/2)#igmp-snooping static-group group-address 225.1.1.2 mvlan 100
```

```
SC9600(config-ge1/0/2)#quit
```

```
SC9600(config)#
```

6、配置结束，检查组播组表和出端口表信息。

```
SC9600#show igmp-snooping group
```

```
Total Entry(s) : 2
```

Group Address	MVlan	Pre-join	MemNum	V3FilterMode
225.1.1.1	100	disable	1	invalid
225.1.1.2	100	disable	1	invalid

```
SC9600#show igmp-snooping egress-port
```

```
Total Entry(s) : 2
```

```
Group Address : 225.1.1.1
MVlan : 100
Source Address : *
Interface : ge-1/0/2
    Type : static
    Expires : ---
    OutVlan : 100
    V3 Mode : invalid
Group Address : 225.1.1.2
MVlan : 100
Source Address : *
Interface : ge-1/0/2
    Type : static
    Expires : ---
    OutVlan : 100
    V3 Mode : invalid
```

### 6.2.6.3 配置组播 VLAN 复制举例

#### 组网要求

交换机接口 GE1/0/1 连接组播源测路由器属于 vlan 100，接口 GE1/0/2 和 GE10/3 连接用户主机，分别属于 vlan2 和 vlan3，要求连接在交换机下的 4 台主机能接收组地址为 225.0.0.1~225.0.0.3 的组播数据。其中 vlan 100 为组播 vlan ， vlan3 和 vlan 4 为用户 vlan。

#### 组网图

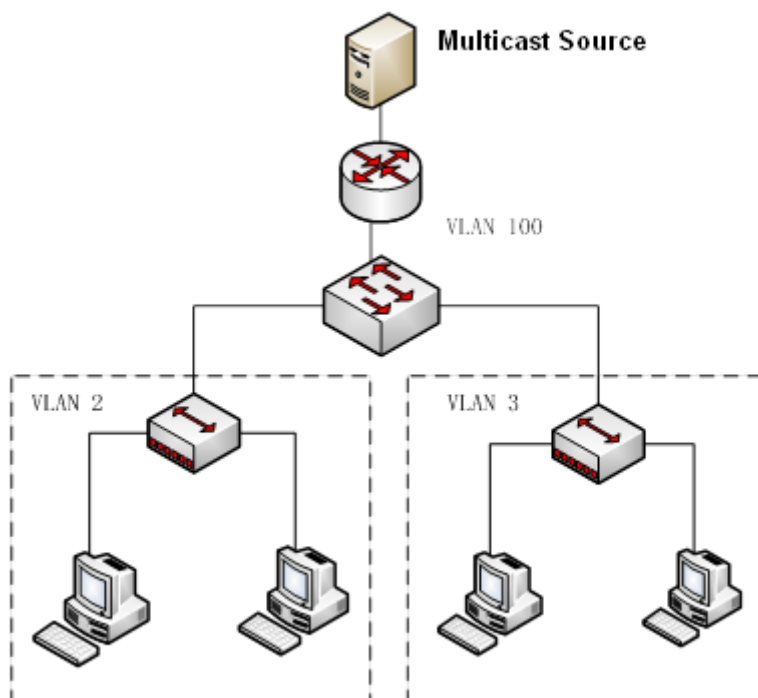


图 6-3 组播复制拓扑图

### 配置步骤

1、全局使能 IGMP snooping 协议。

```
SC9600#configure
```

```
SC9600(config)# igmp-snooping start
```

```
SC9600(config)#
```

2、创建 VLAN 和相应的组播 VLAN，配置接口加入 VLAN。

```
SC9600(config)#Vlan 2,3,100
```

```
SC9600(config)#interface gigabitEthernet 1/0/1
```

```
SC9600(config-ge1/0/1)#port hybrid vlan 100 tagged
```

```
SC9600(config-ge1/0/1)#quit
```

```
SC9600(config)#interface gigabitEthernet 1/0/2
```

```
SC9600(config-ge1/0/2)#port hybrid vlan 2 tagged
```

```
SC9600(config-ge1/0/2)#quit
```

```
SC9600(config)#interface gigabitEthernet 1/0/3
```

```
SC9600(config-ge1/0/3)#port hybrid vlan 3 tagged
```

```
SC9600(config-ge1/0/3)#quit
```

```
SC9600(config)# igmp-snooping mvlan 100
```

```
SC9600(config-igmpsnoop-mvlan100)#quit
```

```
SC9600(config)#
```

3、在接口下使能 IGMP Snooping 协议。

```
SC9600(config)#interface gigabitEthernet 1/0/1
```

```
SC9600(config-ge1/0/1)#igmp-snooping enable
```

```
SC9600(config-ge1/0/1)#quit
```

```
SC9600(config)#interface gigabitEthernet 1/0/2
```

```
SC9600(config-ge1/0/2)#igmp-snooping enable
```

```
SC9600(config-ge1/0/2)#quit
```

```
SC9600(config)#interface gigabitEthernet 1/0/3
```

```
SC9600(config-ge1/0/3)#igmp-snooping enable
```

```
SC9600(config-ge1/0/3)#quit
```

```
SC9600(config)#
```

4、在组播 VLAN 下使能组播复制功能，并配置用户 VLAN。

```
SC9600(config)#igmp-snooping mVlan 100
```

```
SC9600(config-igmpsnoop-mvlan100)#igmp-snooping forwarding-mode ip
```

```
SC9600(config-igmpsnoop-mvlan100)#igmp-snooping multicast-vlan enable
```

```
SC9600(config-igmpsnoop-mvlan100)#igmp-snooping multicast user-vlan 2,3
```

```
SC9600(config-igmpsnoop-mvlan100)#quit
```

```
SC9600(config)#
```

5、配置 GE1/0/1 为静态路由器接口。

```
SC9600(config)#igmp-snooping mVlan 100
```

```
SC9600(config-igmpsnoop-mvlan100)#igmp-snooping uplink-port gigabitEthernet 1/0/1
```

```
SC9600(config-igmpsnoop-mvlan100)#quit
```

```
SC9600(config)#
```

6、配置静态组播组。

```
SC9600(config)#interface gigabitEthernet 1/0/2
```

```
SC9600(config-ge1/0/2)#igmp-snooping static-group group-address 225.0.0.1 mVlan 100 user-vlan 2
```

```
SC9600(config-ge1/0/2)#igmp-snooping static-group group-address 225.0.0.2 mVlan 100 user-vlan 2
```

```
SC9600(config-ge1/0/2)#igmp-snooping static-group group-address 225.0.0.3 mVlan 100 user-vlan 2
```

```
SC9600(config-ge1/0/2)#quit
```

```
SC9600(config)#interface gigabitEthernet 1/0/3
```

```
SC9600(config-ge1/0/3)#igmp-snooping static-group group-address 225.0.0.1 mVlan
100 user-vlan 3
```

```
SC9600(config-ge1/0/3)#igmp-snooping static-group group-address 225.0.0.2 mVlan
100 user-vlan 3
```

```
SC9600(config-ge1/0/3)#igmp-snooping static-group group-address 225.0.0.3 mVlan
100 user-vlan 3
```

```
SC9600(config-ge1/0/3)#quit
```

7、配置完成，检查组播组表和出端口表信息。

```
SC9600#show igmp-snooping group
```

```
Total Entry(s) : 3
```

Group Address	MVlan	Pre-join	MemNum	V3FilterMode
225.0.0.1	100	disable	2	invalid
225.0.0.2	100	disable	2	invalid
225.0.0.3	100	disable	2	invalid

```
SC9600#show igmp-snooping egress-port
```

```
Total Entry(s) : 6
```

```
Group Address : 225.0.0.1
```

```
MVlan : 100
```

```
Source Address : *
```

```
Interface : ge-1/0/2
```

```
Type : static
```

```
Expires : ---
```

```
OutVlan : 2
```

```
V3 Mode : invalid
```

```
Group Address : 225.0.0.1
```

```
MVlan : 100
```

```
Source Address : *
```

```
Interface : ge-1/0/3
```

```
Type : static
```

```
Expires : ---
```

```
OutVlan : 3
```

```
V3 Mode : invalid
```

```
Group Address : 225.0.0.2
```



---

MVlan : 100  
Source Address : \*  
Interface : ge-1/0/2  
Type : static  
Expires : ---  
OutVlan : 2  
V3 Mode : invalid  
Group Address : 225.0.0.2

MVlan : 100  
Source Address : \*  
Interface : ge-1/0/3  
Type : static  
Expires : ---  
OutVlan : 3  
V3 Mode : invalid  
Group Address : 225.0.0.3

MVlan : 100  
Source Address : \*  
Interface : ge-1/0/2  
Type : static  
Expires : ---  
OutVlan : 2  
V3 Mode : invalid  
Group Address : 225.0.0.3

MVlan : 100  
Source Address : \*  
Interface : ge-1/0/3  
Type : static  
Expires : ---  
OutVlan : 3  
V3 Mode : invalid

## 6.3 MLD Snooping 配置

### 6.3.1 MLD Snooping 简介

#### 6.3.1.1 协议介绍

MLD Snooping 通过侦听路由器和主机之间发送的组播协议报文来维护组播报文的出接口信息，从而管理和控制组播数据报文的转发，实现二层组播。

静态二层组播以太网在传输组播报文时，报文的目的地不是一个具体的接收者，而是一个成员不确定的组。所以当组播报文由网络层转发到链路层时，无法生成组播转发表项，导致组播报文在链路层采用广播方式。这样不仅浪费带宽，而且不利于对用户服务进行计费，还对信息的安全性存在威胁。当设备部署在路由器和用户主机之间，应用二层转发特性时，通过配置静态二层组播，即手工配置转发表项，可以把组播数据转发给需要长期接收该数据的用户。

在传统的组播转发方式下，属于不同 VLAN 的用户分别点播同一组播源时，需要交换机为每个 VLAN 都复制一份组播数据，再分别传送给每个 VLAN。这样既造成了带宽的浪费，也增加了额外的负担。在配置了组播 VLAN 复制功能后，属于不同 VLAN 的用户分别点播同一组播源时，设备将这些 VLAN 都配置对应一个组播 VLAN。这样，上层路由器只需把一份组播数据传送给该组播 VLAN 即可，而不必再为每个 VLAN 都复制一份。

MLD Snooping 通过侦听路由器和主机之间发送的组播协议报文来维护组播报文的接口信息，从而管理和控制组播数据报文的转发，实现二层组播。

#### 6.3.1.2 功能特性

该协议具有以下特点：

1. 静态二层组播：配置接口静态加入组播组，可以避免协议报文的攻击；采用直接查找组播报文转发表转发报文的机制，可以减少网络的延时。
2. 组播 vlan 复制：通过组播 VLAN 复制功能，可以实现组播数据在不同的 VLAN 内传送，便于对组播源和组播组成员的管理和控制，同时也可以减少带宽浪费。
3. MLD snooping：支持基于 vlan 的 MLD snooping 功能；
  - 1) MLD 版本可配置 v1/v2；
  - 2) 组播转发模式可配置；
  - 3) 支持静态路由接口；

- 4) 支持 MLD 查询功能
- 5) 支持 MLD 报文抑制
- 6) 支持接口快速离开
- 7) 路由接口老化时间可配置；
- 8) 组成员最大响应世家可配置；
- 9) 组播策略可配置；
- 10) Router Alert 选项可配置

### 6.3.2 MLD Snooping 配置

#### 6.3.2.1 MLD Snooping 全局参数配置

##### 目的

本节介绍 MLD Snooping 全局参数配置，包括全局使能/去使能组播功能、配置特定查询个数、查询间隔、通用查询间隔、出端口表项健壮系数以及配置路由器端口老化时间等。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
全局使能/去使能组播功能	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>mld-snooping { start   stop }</b>	-
配置特定查询个数	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>mld-snooping lastmember-querynumber { querynumber-value   default }</b>	querynumber-value: 指定源组查询最后查询次数，整数形式，取值范围是 2~16，单位：次 缺省为 2 次
配置特定查询间隔	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>mld-snooping lastmember-queryinterval { queryinterval-value   default }</b>	queryinterval-value: 指定全局特定查询间隔，整数形式，取值范围是 1~5，单位：秒 默认为 1 秒
配置通用查询间隔	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>mld-snooping query-interval</b>	queryinterval-value: 指定组播监听全局通用查询间隔时间，整数形式，取值范围是

目的	步骤	参数说明
	{ <i>queryinterval-value</i>   default }	10~65535, 单位: 秒 默认为 60 秒
配置出端口表项健壮系数	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>mld-snooping robust-count {robust-count-num   default}</b>	<b>robust-count-num</b> : 发送特定查询报文的次数, 整数形式, 取值范围是 2~5 缺省为 2
配置路由器端口老化时间	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>mld-snooping router-aging-time { router-aging-time   default}</b>	<b>router-aging-time</b> : 发送特定查询报文的次数, 整数形式, 取值范围是 1~1000, 单位为秒 默认为 180 秒

### 6.3.2.2 配置 MLD Snooping 端口

#### 目的

本节介绍 MLD Snooping 在端口上的配置, 包括在端口上使能组播协议、在端口上使能快速离开以及在端口上配置静态组播组等。

#### 过程

根据不同目的, 执行相应步骤, 具体参见下表。

目的	步骤	参数说明
在端口上使能组播协议	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b> 进入接口配置视图; 3. 执行命令 <b>mld-snooping { enable   disable }</b>	<b>interface-number</b> : SC9600 系列交换机支持以下 3 种型号的接口配置范围: SC9603: 取值范围是 <1-3>/<0-4>/<1-48> SC9608: 取值范围是 <1-8>/<0-4>/<1-48> SC9612: 取值范围是 <1-12>/<0-4>/<1-48>
在端口上使能快速离开	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b> 进入接口配置视图; 3. 执行命令 <b>mld-snooping fast-leave { enable   disable }</b>	<b>interface-number</b> : SC9600 系列交换机支持以下 3 种型号的接口配置范围: SC9603: 取值范围是 <1-3>/<0-4>/<1-48> SC9608: 取值范围是 <1-8>/<0-4>/<1-48> SC9612: 取值范围是 <1-12>/<0-4>/<1-48>

目的	步骤	参数说明
在端口上配置静态组播组	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b> 进入接口配置视图；</li> <li>3. 执行命令 <b>mld-snooping static-group group-ipv6-address mvlan vlan-id</b> 或 <b>no mld-snooping static-group group-ipv6-address mvlan vlan-id</b></li> </ol>	<p>interface-number: SC9600 系列交换机支持以下 3 种型号的接口配置范围：</p> <p>SC9603：取值范围是 &lt;1-3&gt;/&lt;0-4&gt;/&lt;1-48&gt;</p> <p>SC9608：取值范围是 &lt;1-8&gt;/&lt;0-4&gt;/&lt;1-48&gt;</p> <p>SC9612：取值范围是 &lt;1-12&gt;/&lt;0-4&gt;/&lt;1-48&gt;</p> <p>group-ipv6-address：指定组地址，组地址范围是 FF00::/8</p> <p>vlan-id：指定 VLAN ID，整数形式，取值范围是 1~4094</p>

### 6.3.2.3 配置 MLD Snooping 组播 VLAN

#### 目的

本节介绍组播 VLAN 的 MLD Snooping 配置，包括创建组播 vlan、配置组播 vlan 的转发模式、配置组播 vlan 内的组播策略等。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
创建组播 vlan，进入组播 vlan 配置视图	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>mld-snooping mvlan vlan-id</b> 或 <b>no mld-snooping mvlan vlan-id</b></li> </ol>	vlan-id：指定 MLD Snooping 的组 VLAN，整数形式，取值范围是 1~4094。
配置组播 vlan 的转发模式	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>mld-snooping mvlan vlan-id</b>，进入 MVLAN 配置视图；</li> <li>3. 执行命令 <b>mld-snooping forwarding-mode { ip mac }</b></li> </ol>	vlan-id：指定 MLD Snooping 的组 VLAN，整数形式，取值范围是 1~4094。
配置组播 vlan 内的组播策略	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>mld-snooping mvlan vlan-id</b>，进入 MVLAN 配置视图；</li> <li>3. 执行命令 <b>mld-snooping</b></li> </ol>	<p>vlan-id：指定 MLD Snooping 的组 VLAN，整数形式，取值范围是 1~4094。</p> <p>filter-list-number：组播策略绑定的 filter-list 号，取值范围为</p>

目的	步骤	参数说明
	<b>group-policy filter-list filter-list-number</b>	3001-4000
配置组播vlan内的通用查询最大响应时间	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>mld-snooping max-response-time { responsetime-value   default }</b></li> </ol>	responsetime-value : 指定 MLD Snooping 模块 MLD 报文最大响应时间, 整数形式, 取值范围是 1~25, 单位: 秒 默认为 1 秒
配置组播vlan内的组播复制功能使能/去使能	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>mld-snooping mvlan vlan-id</b>, 进入 MVLAN 配置视图;</li> <li>3. 执行命令 <b>mld-snooping multicast-vlan { enable   disable }</b></li> </ol>	vlan-id: 指定 MLD Snooping 的组 VLAN, 整数形式, 取值范围是 1~4094。
配置组播vlan内的报文抑制功能	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>mld-snooping mvlan vlan-id</b>, 进入 MVLAN 配置视图;</li> <li>3. 执行命令 <b>mld-snooping report-suppress { enable   disable }</b></li> </ol>	vlan-id: 指定 MLD Snooping 的组 VLAN, 整数形式, 取值范围是 1~4094。
配置组播vlan的查询器使能和去使能	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>mld-snooping mvlan vlan-id</b>, 进入 MVLAN 配置视图;</li> <li>3. 执行命令 <b>mld-snooping querier { enable   disable }</b></li> </ol>	vlan-id: 指定 MLD Snooping 的组 VLAN, 整数形式, 取值范围是 1~4094。
配置组播vlan的router-alert检查功能	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>mld-snooping mvlan vlan-id</b>, 进入 MVLAN 配置视图;</li> <li>3. 执行命令 <b>mld-snooping require-router-alert { enable   disable }</b></li> </ol>	vlan-id: 指定 MLD Snooping 的组 VLAN, 整数形式, 取值范围是 1~4094。
配置组播vlan的ssm-maping功能	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>mld-snooping mvlan vlan-id</b>, 进入 MVLAN 配置视图;</li> <li>3. 执行命令 <b>mld-snooping ssm-mapping { enable   disable }</b></li> </ol>	vlan-id: 指定 MLD Snooping 的组 VLAN, 整数形式, 取值范围是 1~4094。
配置组播vlan的ssm-maping映	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>mld-snooping mvlan</b></li> </ol>	vlan-id: 指定 MLD Snooping 的组 VLAN, 整数形式, 取值范围是 1~4094。

目的	步骤	参数说明
射关系表	<i>vlan-id</i> , 进入 MVLAN 配置视图; 3. 执行命令 <b>mld-snooping ssm-mapping filter-list <i>filter-list-number</i> source-address <i>source-address</i></b>	<b>filter-list-number</b> : 组播策略绑定的 filter-list 号, 取值范围为 3001-4000 <b>source-address</b> : 源地址, IPv6 格式。
配置组播vlan的上联端口(路由器端口)	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>mld-snooping mvlan <i>vlan-id</i></b> , 进入 MVLAN 配置视图; 3. 执行命令 <b>mld-snooping uplink-port {fastethernet gigaethernet xgigaethernet eth-trunk}</b> 或 <b>no mld-snooping uplink-port {fastethernet gigaethernet xgigaethernet eth-trunk}</b>	<b>vlan-id</b> : 指定 MLD Snooping 的组 VLAN, 整数形式, 取值范围是 1~4094。
配置组播vlan的协议版本	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>mld-snooping mvlan <i>vlan-id</i></b> , 进入 MVLAN 配置视图; 3. 执行命令 <b>mld-snooping version { v1   v2 }</b>	<b>vlan-id</b> : 指定 MLD Snooping 的组 VLAN, 整数形式, 取值范围是 1~4094。
配置组播vlan的协议工作模式	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>mld-snooping mvlan <i>vlan-id</i></b> , 进入 MVLAN 配置视图; 3. 执行命令 <b>mld-snooping workmode { mld-snooping mld-proxy}</b>	<b>vlan-id</b> : 指定 MLD Snooping 的组 VLAN, 整数形式, 取值范围是 1~4094。
配置组播vlan的代理ip	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>mld-snooping mvlan <i>vlan-id</i></b> , 进入 MVLAN 配置视图; 3. 执行命令 <b>mld-snooping proxy-ip <i>ipv4 address</i></b>	<b>vlan-id</b> : 指定 MLD Snooping 的组 VLAN, 整数形式, 取值范围是 1~4094。 <b>ipv4 address</b> : IPV4 地址, 点分十进制

### 6.3.2.4 配置 MLD Snooping 调试功能

#### 目的

本节介绍 MLD Snooping 的调试功能配置。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
打 开 MLDSNOOP 协 议调试功能	1. 进入特权用户视图； 2. 执行命令 <b>debug mldsnop</b> 或 <b>no debug mldsnop</b>	-

### 6.3.2.5 查看 MLD Snooping 配置信息

目的

本节介绍 MLD Snooping 的配置信息查看。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
显示组播配置 信息	1. 进入普通用户视图或特权用户视图； 2. 执行命令 <b>show mld-snooping config</b>	-
显示组播出端 口表信息	1. 进入普通用户视图或特权用户视图； 2. 执行命令 <b>show mld-snooping egress-port</b>	-
显示组播组表 信息	1. 进入普通用户视图或特权用户视图； 2. 执行命令 <b>show mld-snooping group</b>	-
显示组播接口 表信息	1. 进入普通用户视图或特权用户视图； 2. 执行命令 <b>show mld-snooping interface</b>	-
显示组播 vlan 表信息	1. 进入普通用户视图或特权用户视图； 2. 执行命令 <b>show mld-snooping mvlan</b>	-
显示组播源表 信息	1. 进入普通用户视图或特权用户视图； 2. 执行命令 <b>show mld-snooping source-address</b>	-
显示组播上联 口表信息	1. 进入普通用户视图或特权用户视图； 2. 执行命令 <b>show mld-snooping uplinkport</b>	-



### 6.3.3 MLD Snooping 配置举例

#### 6.3.3.1 配置 MLD Snooping 举例

##### 组网要求

如图 6-4所示,交换机接口 GE1/0/1 连接组播源测路由器,接口 GE1/0/2 连接用户主机,要求通过配置 MLD Snooping 功能实现 VLAN 100 内的三台主机能长期接收组地址为 FF1E::1 ~ FF1E::2 的组播数据。

##### 组网图

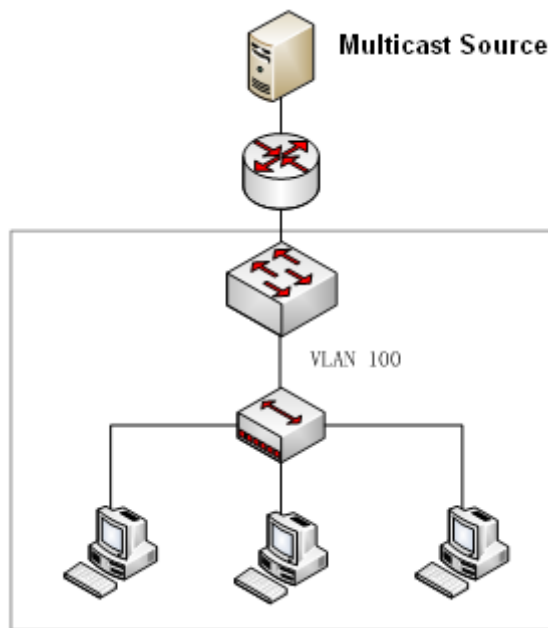


图 6-4 mld-snooping 配置组网图

##### 配置步骤

1. 全局使能 MLD snooping 协议:

```
SC9600#configure
```

```
SC9600(config)# mld-snooping start;
```

```
SC9600 (config)#
```

2. 创建 vlan 和相应的组播 vlan, 配置接口加入 vlan:

```
SC9600 (config)#vlan 100
```

```
SC9600 (vlan-100)#quit
```

```
SC9600(config)#interface gigabitEthernet 1/0/1
SC9600(config-gigabitEthernet1/0/1)#port hybrid vlan 100 tagged
SC9600(config-gigabitEthernet1/0/1)#quit
SC9600(config)#interface gigabitEthernet 1/0/2
SC9600(config-gigabitEthernet1/0/2)#port hybrid vlan 100 tagged
SC9600(config-gigabitEthernet1/0/2)#quit
SC9600 (config)# mld-snooping mVlan 100
SC9600 (config-mld-snooping-mVlan100)#quit
SC9600 (config)#
```

### 3. 在接口下使能 MLD Snooping 协议

```
SC9600(config)#interface gigabitEthernet 1/0/1
SC9600(config-gigabitEthernet1/0/1)#mld-snooping enable
SC9600(config-gigabitEthernet1/0/1)#quit
SC9600(config)#interface gigabitEthernet 1/0/2
SC9600(config-gigabitEthernet1/0/2)#mld-snooping enable
SC9600(config-gigabitEthernet1/0/2)#quit
SC9600 (config)#
```

### 4. 配置 GE1/0/1 为静态路由器接口

```
SC9600(config)#mld-snooping mVlan 100
SC9600(config-mld-snooping-mVlan100)#mld-snooping uplink-port gigabitEthernet 1/0/1
SC9600(config-mld-snooping-mVlan100)#quit
SC9600 (config)#
```

### 5. 配置静态组播组

```
SC9600(config)#interface gigabitEthernet 1/0/2
SC9600(config-gigabitEthernet1/0/2)#mld-snooping static-group group-address FF1E::1 mVlan
100
SC9600(config-gigabitEthernet1/0/2)#mld-snooping static-group group-address FF1E::2 mVlan
100
SC9600(config-gigabitEthernet1/0/2)#quit
SC9600(config)#
```

### 6. 配置结束，检查组播组表和出端口表信息

```
Total Entry(s) : 1
```

```

Group Address          MVlan    Pre-join  MemNum  V2FilterMode
ff1e::1                100      disable   1        invalid
ff1e::2                100      disable   1        invalid

```

SC9600#show mld-snooping egress-port

Total Entry(s) : 2

Group Address : ff1e::1

MVlan : 100

Source Address : \*

Interface : ge-1/0/2

Type : static

Expires : ---

OutVlan : 100

V2 Mode : invalid

Group Address : ff1e::2

MVlan : 100

Source Address : \*

Interface : ge-1/0/2

Type : static

Expires : ---

OutVlan : 100

V2 Mode : invalid

### 6.3.3.2 配置静态二层组播举例

#### 组网要求

如图 6-5所示，交换机接口 GE1/0/1 连接组播源测路由器，接口 GE1/0/2 连接用户主机，要求通 VLAN 100 内的所有主机能长期接收组地址为 FF1E::1 的组播数据。

#### 组网图

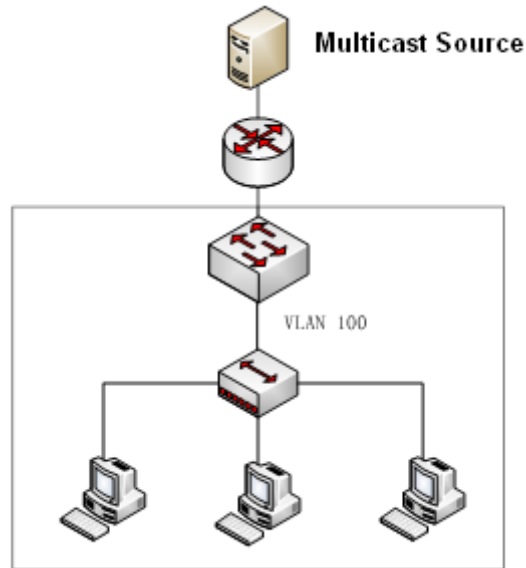


图 6-5 静态二层组播组网图

### 配置步骤

1. 全局使能 MLD snooping 协议;

```
SC9600#configure
```

```
SC9600(config)# mld-snooping start;
```

```
SC9600 (config)#
```

2. 创建 vlan 和相应的组播 vlan，配置接口加入 vlan;

```
SC9600 (config)#vlan 100
```

```
SC9600 (vlan-100)#quit
```

```
SC9600(config)#interface gigabitEthernet 1/0/1
```

```
SC9600(config-ge1/0/1)#port hybrid vlan 100 tagged
```

```
SC9600(config-ge1/0/1)#quit
```

```
SC9600(config)#interface gigabitEthernet 1/0/2
```

```
SC9600(config-ge1/0/2)#port hybrid vlan 100 tagged
```

```
SC9600(config-ge1/0/2)#quit
```

```
SC9600 (config)# mld-snooping mVlan 100
```

```
SC9600 (config-mlsnoop-mVlan100)#quit
```

```
SC9600 (config)#
```

## 3. 在接口下使能 MLD Snooping 协议

```
SC9600(config)#interface gigabitEthernet 1/0/1
SC9600(config-gigabitEthernet1/0/1)#mld-snooping enable
SC9600(config-gigabitEthernet1/0/1)#quit
SC9600(config)#interface gigabitEthernet 1/0/2
SC9600(config-gigabitEthernet1/0/2)#mld-snooping enable
SC9600(config-gigabitEthernet1/0/2)#quit
SC9600 (config)#
```

## 4. 配置 GE1/0/1 为静态路由器接口

```
SC9600(config)#mld-snooping mVlan 100
SC9600(config-mld-snoop-mVlan100)#mld-snooping uplink-port gigabitEthernet 1/0/1
SC9600(config-mld-snoop-mVlan100)#quit
SC9600(config)#
```

## 5. 配置静态组播组

```
SC9600(config)#interface gigabitEthernet 1/0/2
SC9600(config-gigabitEthernet1/0/2)#mld-snooping static-group group-address FF1E::1 mVlan
100
SC9600(config-gigabitEthernet1/0/2)#quit
SC9600(config)#
```

## 6. 配置结束，检查组播组表和出端口表信息

```
SC9600#show mld-snooping group
```

```
Total Entry(s) : 1
```

Group Address	MVlan	Pre-join	MemNum	V2FilterMode
ff1e::1	100	disable	1	invalid

```
SC9600#show mld-snooping egress-port
```

```
Total Entry(s) : 1
```

```
Group Address : ff1e::1
```

```
MVlan : 100
```

```
Source Address : *
```

```
Interface : ge-1/0/2
Type : static
Expires : ---
OutVlan : 100
V2 Mode : invalid
```

### 6.3.3.3 配置组播 VLAN 配置举例

#### 组网要求

如图 6-6所示，交换机接口 GE1/0/1 连接组播源测路由器属于 vlan 100，接口 GE1/0/2 和 GE10/3 连接用户主机，分别属于 vlan2 和 vlan3，要求连接在交换机下的 4 台主机能接收组地址为 FF1E::1~FF1E::3 的组播数据。其中 vlan 100 为组播 vlan ， vlan3 和 vlan 4 为用户 vlan。

#### 组网图

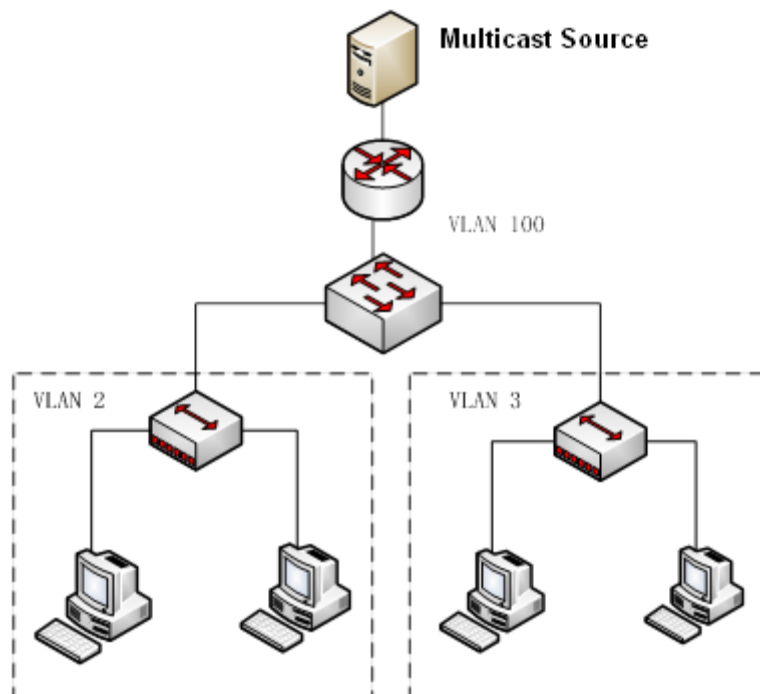


图 6-6 组播复制拓扑图

#### 配置步骤

1. 全局使能 MLD snooping 协议；

```
SC9600#configure
```

```
SC9600(config)# mld-snooping start;  
SC9600 (config)#
```

2. 创建 vlan 和相应的组播 vlan，配置接口加入 vlan；

```
SC9600(config)#Vlan 2,3,100  
SC9600(config)#interface gigabitEthernet 1/0/1  
SC9600(config-gigabitEthernet 1/0/1)#port hybrid vlan 100 tagged  
SC9600(config-gigabitEthernet 1/0/1)#quit  
SC9600(config)#interface gigabitEthernet 1/0/2  
SC9600(config-gigabitEthernet 1/0/2)#port hybrid vlan 2 tagged  
SC9600(config-gigabitEthernet 1/0/2)#quit  
SC9600(config)#interface gigabitEthernet 1/0/3  
SC9600(config-gigabitEthernet 1/0/3)#port hybrid vlan 3 tagged  
SC9600(config-gigabitEthernet 1/0/3)#quit  
SC9600 (config)# mld-snooping mVlan 100  
SC9600 (config-mldsnop-mVlan100)#quit  
SC9600 (config)#
```

3. 在接口下使能 MLD Snooping 协议

```
SC9600(config)#interface gigabitEthernet 1/0/1  
SC9600(config-gigabitEthernet 1/0/1)#mld-snooping enable  
SC9600(config-gigabitEthernet 1/0/1)#quit  
SC9600(config)#interface gigabitEthernet 1/0/2  
SC9600(config-gigabitEthernet 1/0/2)#mld-snooping enable  
SC9600(config-gigabitEthernet 1/0/2)#quit  
SC9600(config)#interface gigabitEthernet 1/0/3  
SC9600(config-gigabitEthernet 1/0/3)#mld-snooping enable  
SC9600(config-gigabitEthernet 1/0/3)#quit  
SC9600 (config)#
```

4. 在组播 vlan 下使能组播复制功能，并配置用户 vlan

```
SC9600(config)#mld-snooping mVlan 100  
SC9600(config-mldsnop-mVlan100)#mld-snooping forwarding-mode ip  
SC9600(config-mldsnop-mVlan100)#mld-snooping multicast-vlan enable
```

```
SC9600(config-mldsnop-mvlan100)#mld-snooping multicast user-vlan 2,3
SC9600(config-mldsnop-mvlan100)#quit
SC9600(config)#
```

4. 配置 GE1/0/1 为静态路由器接口

```
SC9600(config)#mld-snooping mvlan 100
SC9600(config-mldsnop-mvlan100)#mld-snooping uplink-port gigabitEthernet 1/0/1
SC9600(config-mldsnop-mvlan100)#quit
SC9600(config)#
```

5. 配置静态组播组

```
SC9600(config)#interface gigabitEthernet 1/0/2
SC9600(config-ge1/0/2)#mld-snooping static-group group-address FF1E::1 mvlan
100 user-vlan 2
SC9600(config-ge1/0/2)#mld-snooping static-group group-address FF1E::2 mvlan
100 user-vlan 2
SC9600(config-ge1/0/2)#mld-snooping static-group group-address FF1E::3 mvlan
100 user-vlan 2
SC9600(config-ge1/0/2)#quit
SC9600(config)#interface gigabitEthernet 1/0/3
SC9600(config-ge1/0/3)#mld-snooping static-group group-address FF1E::1 mvlan
100 user-vlan 3
SC9600(config-ge1/0/3)#mld-snooping static-group group-address FF1E::2 mvlan
100 user-vlan 3
SC9600(config-ge1/0/3)#mld-snooping static-group group-address FF1E::3 mvlan
100 user-vlan 3
SC9600(config-ge1/0/3)#quit
```

6. 配置完成，检查组播组表和出端口表信息

```
SC9600#show mld-snooping group
Total Entry(s) : 3
Group Address          Mvlan    Pre-join  MemNum    V2FilterMode
ff1e::1                100      disable   2         invalid
ff1e::2                100      disable   2         invalid
ff1e::3                100      disable   2         invalid
```



---

```
SC9600#show mld-snooping egress-port
```

```
Total Entry(s) : 6
```

```
Group Address : ff1e::1
```

```
MVlan : 100
```

```
Source Address : *
```

```
Interface : ge-1/0/2
```

```
    Type : static
```

```
    Expires : ---
```

```
    OutVlan : 100
```

```
    V2 Mode : invalid
```

```
Group Address : ff1e::1
```

```
MVlan : 100
```

```
Source Address : *
```

```
Interface : ge-1/0/3
```

```
    Type : static
```

```
    Expires : ---
```

```
    OutVlan : 100
```

```
    V2 Mode : invalid
```

```
Group Address : ff1e::2
```

```
MVlan : 100
```

```
Source Address : *
```

```
Interface : ge-1/0/2
```

```
    Type : static
```

```
    Expires : ---
```

```
    OutVlan : 100
```

```
    V2 Mode : invalid
```

```
Group Address : ff1e::2
```

```
MVlan : 100
```

```
Source Address : *
```

```
Interface : ge-1/0/3
```

```
    Type : static
```

```
    Expires : ---
```

```
    OutVlan : 100
```

V2 Mode : invalid  
Group Address : ff1e::3  
MVlan : 100  
Source Address : \*  
Interface : ge-1/0/2  
Type : static  
Expires : ---  
OutVlan : 100  
V2 Mode : invalid  
Group Address : ff1e::3  
MVlan : 100  
Source Address : \*  
Interface : ge-1/0/3  
Type : static  
Expires : ---  
OutVlan : 100  
V2 Mode : invalid

## 第7章 安全配置

### 7.1 概述

本章介绍了 SC9600 系列高端交换机安全性相关的基本内容、配置过程和配置举例。

本章包括如下主题：

内容	页码
7.1 概述	7-1
7.2 ACL 配置	7-1
7.3 IP Source Guard 配置	7-27

### 7.2 ACL 配置



说明：

本小节中，ACL 指用于过滤 IPv4 报文的访问控制列表，ACL6 指用于过滤 IPv6 报文的访问控制列表。

#### 7.2.1 ACL 概述

##### ACL 功能

SC9600 通过配置访问控制列表 ACL（Access Control List）的规则和动作来决定什么样的数据包能够通过，什么样的数据包要拒绝等，从而实现控制数据的传输、提高网络性能、保障业务安全。

ACL 是由二层 MAC，三层 IP 组成的一系列有顺序的规则和动作，这些规则根据数据包的源地址、目的地址、端口号等来对数据包进行过滤。ACL 通过这些规则对数据包进行分类，这些规则应用到 SC9600 上，SC9600 根据这些规则判断哪些数据包可以接收，哪些数据包需要拒绝以及其他动作。

### SC9600 支持的 ACL 分类

SC9600 支持二层 ACL，三层 ACL，混合 ACL 和三层 ACL6。

- 二层 ACL：主要基于源 MAC 地址，目的 MAC 地址，VLAN，优先级，协议类型、限速模板、时间段模板等信息对数据包进行分类定义。
- 三层 ACL：主要基于源 IP 地址，目的 IP 地址，源端口号、目的端口号、协议类型、优先级、分片、生存时间、限速模板、时间段模板等信息对数据包进行更为细致的分类定义。
- 混合 ACL：主要基于源 MAC 地址，目的 MAC 地址，源 IP 地址，目的 IP 地址，源端口号，目的端口号，协议类型，优先级，VLAN、限速模板、时间段模板等信息对数据包进行分类定义。
- 三层 ACL6：主要基于源 IPv6 地址、目的 IPv6 地址、源端口号、目的端口号、协议类型、跳数限制、下一个首部、通信量类、流标号、限速模板、时间段模板等信息对数据包进行分类定义。

## 7.2.2 配置二层 ACL

### 背景信息

一条 ACL 是由若干规则和动作组成的一系列的列表，若干个规则列表构成一条 ACL。

配置二层 ACL 的规则之前，首先需要创建一条二层 ACL 并指定 ACL 种类标示编号为 1~1000。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
创建一条二层 ACL	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>filter-list acl-number</b> 使用编号创建一条二层 ACL（访问控制列表），并进入二层 ACL 配置视图；</li> <li>3. 结束。</li> </ol>
配置二层 ACL 规则	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>filter-list acl-number</b> 进入二层 ACL 配置视图；</li> <li>3. 执行以下命令用来配置 MAC 条目匹配的 ACL 规则（用户根据需要自行从以下命令中选择配置）：  <b>filter filter number mac (src-mac-address/M any) (dst-mac-address/M any)</b>  <b>filter filter number src-mac src-mac-address src-mask src-mac-mask</b> </li> </ol>

目的	步骤
	<p><b>dst-mac dst-mac-address dst-mask dst-mac-mask</b></p> <pre> filter filter number mac (src-mac-address/M any) (dst-mac-address/M  any) (customer provider)(any &lt;1-4094&gt; &lt;1-4094&gt; &lt;1-4094&gt;) (any &lt;0-7&gt;)  filter filter number src-mac src-mac-address src-mask src-mac-mask dst-mac dst-mac-address dst-mask dst-mac-mask (customer provider) (any &lt;1-4094&gt; &lt;1-4094&gt; &lt;1-4094&gt;) (any &lt;0-7&gt;)  filter filter number mac (src-mac-address/M any) (dst-mac-address/M  any) eth-type (ip arp &lt;0x1-0xffe&gt;)  filter filter number src-mac src-mac-address src-mask src-mac-mask dst-mac dst-mac-address dst-mask dst-mac-mask eth-type (ip arp &lt;0x1-0xffe&gt;)  filter filter number mac (src-mac-address/M any) (dst-mac-address/M  any) provider (any &lt;1-4094&gt;) (any &lt;0-7&gt;) customer (any &lt;1-4094&gt;)(any &lt;0-7&gt;)  filter filter number mac (src-mac-address/M any) (dst-mac-address/M  any) provider (&lt;1-4094&gt; &lt;1-4094&gt;) (any &lt;0-7&gt;) customer (any &lt;1-4094&gt;)(any &lt;0-7&gt;)  filter filter number mac (src-mac-address/M any) (dst-mac-address/M  any) provider (any &lt;1-4094&gt;) (any &lt;0-7&gt;) customer (&lt;1-4094&gt; &lt;1-4094&gt;) (any &lt;0-7&gt;)  filter filter number src-mac(src-mac-address/M any) src-mask src-mac-mask dst-mac dst-mac-address dst-mask dst-mac-mask provider (any &lt;1-4094&gt;) (any &lt;0-7&gt;) customer (any &lt;1-4094&gt;)(any &lt;0-7&gt;)  filter filter number src-mac (src-mac-address/M any) src-mask src-mac-mask dst-mac dst-mac-address dst-mask dst-mac-mask provider (&lt;1-4094&gt; &lt;1-4094&gt;) (any &lt;0-7&gt;) customer (any &lt;1-4094&gt;)(any &lt;0-7&gt;)  filter filter number src-mac (src-mac-address/M any) src-mask src-mac-mask dst-mac dst-mac-address dst-mask dst-mac-mask provider (any &lt;1-4094&gt;) (any &lt;0-7&gt;) customer (&lt;1-4094&gt; &lt;1-4094&gt;)(any &lt;0-7&gt;)  filter filter number mac (src-mac-address/M any) (dst-mac-address/M  any) provider (any &lt;1-4094&gt; &lt;1-4094&gt; &lt;1-4094&gt;) (any &lt;0-7&gt;) isid (any &lt;1-16777215&gt;)  filter filter number src-mac (src-mac-address/M any) src-mask src-mac-mask dst-mac dst-mac-address dst-mask dst-mac-mask provider (any &lt;1-4094&gt; &lt;1-4094&gt; &lt;1-4094&gt;) (any &lt;0-7&gt;) isid (any &lt;1-16777215&gt;)                     </pre>

目的	步骤
配置二层 ACL 动作	<p>4. 结束。</p> <p>1. 执行命令 <b>configure</b> 进入全局配置视图；</p> <p>2. 执行命令 <b>filter-list acl-number</b> 进入二层 ACL 配置视图；</p> <p>3. 执行以下命令配置 ACL 处理动作；</p> <pre>filter rule-number action { permit   deny } filter rule-number action redirect cpu filter rule-number action mirror cpu filter rule-number action mirror group group-number filter rule-number action redirect { fastethernet   gigasethernet   xgigasethernet   eth-trunk } slot/port filter rule-number action redirect eth-trunk trunk number filter rule-number action redirect ip-nexthop ip-address <b>filter rule-number action redirect ip-multihop ip-address ip-address</b> <b>filter rule-number action redirect ip-multihop ip-address ip-address</b> ip-address <b>filter rule-number action redirect ip-multihop ip-address ip-address</b> ip-address ip-address filter rule-number action { insert-outer-vid   replace-outer-vid } vlan-id filter rule-number action { insert-inner-vid   replace-inner-vid   remove-inner-vid } filter rule-number action vfp { insert-inner-vid   replace-inner-vid   insert-outer-vid   replace-outer-vid   deny   remove-inner-vid } Vlan ID filter rule-number action vfp filter rule-number action { cos   precedence   outer-tag-priority   inner-tag-priority } priority-value filter rule-number action { outer-tag-priority   inner-tag-priority } Priority-value filter rule-number action outer-tag-priority inner-tag-priority filter rule-number action dscp dscp filter rule-number action { precedence-priority   priority-precedence } <b>filter rule-number action counter counter number</b></pre> <p>4. 结束。</p>
绑定二层 ACL	<p>1. 执行命令 <b>configure</b> 进入全局配置视图；</p> <p>2. 执行命令 <b>filter-list global { in   out } acl-number</b> 用来全局绑定到指定的 ACL；</p> <p>3. 或执行命令 <b>filter-list acl-number</b> 进入二层 ACL 配置视图，再执行命令 <b>filter-list { in   out } acl-number</b> 用来将 ACL 应用到物理端口，trunk 接口或者 VLAN 端口；</p> <p>4. 结束。</p>

附表：

参数	说明	取值
acl-number	表示访问控制列表的序号。	整数形式，取值范围是 1~4000，其中： <1-1000>是设置二层 ACL。 <1001-2000>是设置 IPv4 ACL。 <2001-3000>是设置混合 ACL。 <3001-4000>是设置 IPv6 ACL。
rule-number	指定的访问控制列表的规则序号。	整数形式，取值范围是 1~16384。
src-mac-address/M   any	指定的 ACL 规则的源 MAC 地址信息。	M 为整数形式，范围为 1~24。 any 代表任意源 MAC 地址。
dst-mac-address/M   any	指定的 ACL 规则的目的 MAC 地址信息。	M 为整数形式，范围为 1~24。 any 代表任意目的 MAC 地址。
src-mac-mask	指定的 ACL 规则的源 MAC 地址掩码信息。	点分十进制形式。
dst-mac-mask	指定的 ACL 规则的目的 MAC 地址掩码信息。	点分十进制形式。
provider (<1-4094>/<1-4094>) (any <0-7>) customer (any <1-4094>)(any <0-7>)	VID 号/VID 范围或者任何以上两者取值	-
rule-number	指定的访问控制列表的规则序号。	整数形式，取值范围是 1~16384。
VLAN ID	VLAN 号	整数形式，取值范围是 1~4094

### 7.2.3 配置三层 ACL

#### 背景信息

一条 ACL 是由若干规则和动作组成的一系列的列表，若干个规则列表构成一条 ACL。

配置三层 ACL 的规则之前，首先需要创建一条三层 ACL 并指定 ACL 种类标示编号为 1001~2000。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
创建一条三层 ACL	1. 执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>filter-list acl-number</b> 使用编号创建一条三层 ACL（访问控

目的	步骤
	制列表), 并进入三层 ACL 配置视图; 3. 结束。
配置三层 ACL 规则	1. 执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>filter-list acl-number</b> 进入三层 ACL 配置视图; 【用户可以从步骤 3~步骤 8 中根据需要任选配置】 3. (可选) 执行以下命令用来配置 IP 匹配的 ACL 规则 (用户根据需要自行从以下命令中选择配置); <pre> <b>filter rule-number ip</b> { src-ip-address/M   <b>any</b> } { dst-ip-address/M   <b>any</b> } <b>filter rule-number src-ip</b> {src-ip-address   <b>any</b>} <b>src-mask</b> {src-ip-mask   <b>any</b>} <b>dst-ip</b> {dst-ip-address   <b>any</b>} <b>dst-mask</b> {dst-ip-mask   <b>any</b>} <b>filter rule-number ip</b> { src-ip-address/M   <b>any</b> } { dst-ip-address/M   <b>any</b> } <b>precedence</b> tos-priority <b>filter rule-number src-ip</b> { src-ip-address   <b>any</b>} <b>src-mask</b> {src-ip-mask   <b>any</b>} <b>dst-ip</b> {dst-ip-address   <b>any</b>} <b>dst-mask</b> {dst-ip-mask   <b>any</b>} <b>precedence</b> tos-priority <b>filter rule-number ip</b> { src-ip-address/M   <b>any</b> } { dst-ip-address/M   <b>any</b> } <b>dscp</b> dscp <b>filter rule-number src-ip</b> { src-ip-address   <b>any</b>} <b>src-mask</b> {src-ip-mask   <b>any</b>} <b>dst-ip</b> {dst-ip-address   <b>any</b>} <b>dst-mask</b> {dst-ip-mask   <b>any</b>} <b>dscp</b> dscp <b>filter rule-number ip</b> { src-ip-address/M   <b>any</b> } { dst-ip-address/M   <b>any</b> } <b>fragment</b> <b>filter rule-number src-ip</b> { src-ip-address   <b>any</b>} <b>src-mask</b> {src-ip-mask   <b>any</b>} <b>dst-ip</b> {dst-ip-address   <b>any</b>} <b>dst-mask</b> {dst-ip-mask   <b>any</b>} <b>fragment</b> <b>filter filter number ip</b> (src-ip-address/M  <b>any</b>) (dst-ip-address M <b>any</b>) <b>precedence</b> tos <b>field fragment</b> <b>filter filter number src-ip</b> { src-ip-address   <b>any</b>} <b>src-mask</b> {src-ip-mask   <b>any</b>} <b>dst-ip</b> {dst-ip-address   <b>any</b>} <b>dst-mask</b> {dst-ip-mask   <b>any</b>} <b>precedence</b> tos <b>field fragment</b> <b>filter filter number ip</b> (src-ip-address/M  <b>any</b>) (dst-ip-address M  <b>any</b>) <b>dscp</b> (dscp field af11 af12 af13 af21 af22 af23 af31 af32 af33 af41 af42 af43 cs1 cs2 cs3 cs4 cs5 cs6 cs7 default ef) <b>fragment</b> <b>filter filter number src-ip</b> { src-ip-address   <b>any</b>} <b>src-mask</b> {src-ip-mask   <b>any</b>} <b>dst-ip</b> {dst-ip-address   <b>any</b>} <b>dst-mask</b> {dst-ip-mask   <b>any</b>} <b>dscp</b>(dscp field af11 af12 af13 af21 af22 af23 af31 af32 af33 af41 af42 af43 cs1 cs2 cs3                     </pre>



目的	步骤
	<p> cs4 cs5 cs6 cs7 default ef) fragment</p> <p><b>filter</b> filter number <b>ip</b> (src-ip-address/M  any) (dst-ip-address M  any)</p> <p><b>proto-type</b> proto-type field</p> <p><b>filter</b> filter number <b>src-ip</b> { src-ip-address   any} <b>src-mask</b> {src-ip-mask   any} <b>dst-ip</b> {dst-ip-address   any} <b>dst-mask</b> {dst-ip-mask   any} <b>proto-type</b> proto-type field</p> <p><b>filter</b> filter number <b>ip</b> (src-ip-address/M  any) (dst-ip-address M  any)</p> <p><b>ttl</b> ttl field</p> <p><b>filter</b> filter number <b>src-ip</b> { src-ip-address   any} <b>src-mask</b> {src-ip-mask   any} <b>dst-ip</b> {dst-ip-address   any} <b>dst-mask</b> {dst-ip-mask   any} <b>ttl</b> ttl field</p> <p>4. (可选) 执行以下命令用来配置 TCP 匹配的 ACL 规则 (用户根据需要自行从以下命令中选择配置):</p> <pre>filter filter number tcp (src-ip-address/M  any) (&lt;0-65535&gt; &lt;0-65535&gt;/&lt;0-65535&gt; any) (dst-ip-address/M  any) (&lt;0-65535&gt; &lt;0-65535&gt;/&lt;0-65535&gt; any)</pre> <p><b>filter</b> filter number <b>tcp src-ip</b> { src-ip-address   any} <b>src-mask</b> src-ip-mask (&lt;0-65535&gt; any) <b>dst-ip</b> { src-ip-mask   any} <b>dst-mask</b> dst-ip-mask (&lt;0-65535&gt; any)</p> <pre>filter filter number tcp (src-ip-address/M  any) (&lt;0-65535&gt; &lt;0-65535&gt;/&lt;0-65535&gt; any) (dst-ip-address/M  any) (&lt;0-65535&gt; &lt;0-65535&gt;/&lt;0-65535&gt; any) fragment (syn synack ack fin finack psh rst urg field)</pre> <p><b>filter</b> filter number tcp src-ip { src-ip-address   any} src-mask src-ip-mask (&lt;0-65535&gt; any) dst-ip dst-ip-address dst-mask dst-ip-mask (&lt;0-65535&gt; any) (syn synack ack fin finack psh rst urg  field) fragment</p> <p>5. (可选) 执行以下命令用来配置 ICMP 匹配的 ACL 规则 (用户根据需要自行从以下命令中选择配置):</p> <p><b>filter</b> filter number <b>icmp</b> (src-ip-address/M  any) (dst-ip-address M  any)</p> <p><b>filter</b> filter number <b>icmp src-ip</b> { src-ip-address   any} <b>src-mask</b> { src-ip-mask   any} <b>dst-ip</b> src-ip-mask <b>dst-mask</b> {dst-ip-mask }</p> <p><b>filter</b> filter number <b>icmp</b> (src-ip-address/M  any) (dst-ip-address M  any) (icmp type any) (icmp code any)</p> <p><b>filter</b> filter number <b>icmp src-ip</b> src-ip-address <b>src-mask</b> { src-ip-mask   any} <b>dst-ip</b> src-ip-mask <b>dst-mask</b> dst-ip-mask icmp type (icmp code  any)</p> <p>6. (可选) 执行以下命令用来配置 IGMP 匹配的 ACL 规则 (用户根据需要自行从以下命令中选择配置):</p> <p><b>filter</b> filter number <b>igmp</b> (src-ip-address/M  any) (dst-ip-address M</p>

目的	步骤
	<p><b> any)</b></p> <p><b>filter filter number igmp src-ip src-ip-address src-mask src-ip-mask dst-ip src-ip-mask dst-mask dst-ip-mask</b></p> <p>7. (可选) 执行以下命令用来配置 UDP 匹配的 ACL 规则 (用户根据需要自行从以下命令中选择配置):</p> <pre>filter filter number udp (src-ip-address/M  any) (&lt;0-65535&gt; &lt;0-65535&gt;/&lt;0-65535&gt; any) (dst-ip-address/M  any) (&lt;0-65535&gt; &lt;0-65535&gt;/&lt;0-65535&gt; any) [fragment</pre> <pre>filter filter number udp src-ip { src-ip-address   any} src-mask src-ip-mask (&lt;0-65535&gt; any) dst-ip { src-ip-mask   any} dst-mask {dst-ip-mask   any} (&lt;0-65535&gt; any) [fragment</pre> <p>8. (可选) 执行以下命令用来配置 ARP 匹配的 ACL 规则 (用户根据需要自行从以下命令中选择配置):</p> <pre>filter filter number arp (request response any) (src-ip-address/M  any) (dst-ip-address/M  any)</pre> <pre>filter filter number arp (request response any) src-ip src-ip-address src-mask { src-ip-mask   any} dst-ip src-ip-mask dst-mask dst-ip-mask</pre> <p>9. 结束。</p>
配置三层 ACL 动作	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>filter-list acl-number</b> 进入三层 ACL 配置视图;</li> <li>3. 执行以下命令配置 ACL 处理动作;</li> </ol> <pre>filter rule-number action { permit   deny }</pre> <pre>filter rule-number action redirect cpu</pre> <pre>filter rule-number action mirror cpu</pre> <pre>filter rule-number action mirror group group-number</pre> <pre>filter rule-number action redirect { fastethernet   gigaehternet   xgigaehternet   eth-trunk } slot/port</pre> <pre>filter rule-number action redirect eth-trunk trunk number</pre> <pre>filter rule-number action redirect ip-nexthop ip-address</pre> <pre><b>filter rule-number action redirect ip-multihop ip-address ip-address</b></pre> <pre><b>filter rule-number action redirect ip-multihop ip-address ip-address ip-address</b></pre> <pre><b>filter rule-number action redirect ip-multihop ip-address ip-address ip-address ip-address</b></pre> <pre>filter rule-number action { insert-outer-vid   replace-outer-vid } vlan-id</pre> <pre>filter rule-number action { insert-inner-vid   replace-inner-vid   remove-inner-vid }</pre> <pre>filter rule-number action vfp { insert-inner-vid   replace-inner-vid  insert-outer-vid   replace-outer-vid  deny   remove-inner-vid } Vlan ID</pre> <pre>filter rule-number action vfp</pre>

目的	步骤
	<pre>filter rule-number action { cos   precedence   outer-tag-priority   inner-tag-priority } priority-value</pre> <pre>filter rule-number action { outer-tag-priority   inner-tag-priority } Priority-value</pre> <pre>filter rule-number action outer-tag-priority inner-tag-priority</pre> <pre>filter rule-number action dscp dscp</pre> <pre>filter rule-number action { precedence-priority   priority-precedence }</pre> <pre>filter rule-number action counter counter number</pre> <p>4. 结束。</p>
绑定三层 ACL	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>filter-list global { in   out } acl-number</b> 用来全局绑定到指定的 ACL；</li> <li>3. 或执行命令 <b>filter-list acl-number</b> 进入三层 ACL 配置视图，再执行命令 <b>filter-list { in   out } acl-number</b> 用来将 ACL 应用到物理端口，trunk 接口或者 VLAN 端口；</li> <li>4. 结束。</li> </ol>

附表：

参数	说明	取值
acl-number	表示访问控制列表的序号。	整数形式，取值范围是 1~4000，其中： <1-1000>是设置二层 ACL。 <1001-2000>是设置 IPv4 ACL。 <2001-3000>是设置混合 ACL。 <3001-4000>是设置 IPv6 ACL。
rule-number	指定的访问控制列表的规则序号。	整数形式，取值范围是 1~16384。
src-ip-address/M   any	指定的 ACL 规则的源 IP 地址信息。	<i>src-ip-address</i> 为点分十进制形式； <i>M</i> 为整数形式，范围为 1~24。 <b>any</b> 代表任意源 IP 地址。
dst-ip-address/M   any	指定的 ACL 规则的目的 IP 地址信息。	<i>dst-ip-address</i> 为点分十进制形式； <i>M</i> 为整数形式，范围为 1~24。 <b>any</b> 代表任意目的 IP 地址。
src-ip-mask/ any	指定的 ACL 规则的源 IP 地址掩码信息。	点分十进制形式。
dst-ip-mask/ any	指定的 ACL 规则的目的 IP 地址掩码信息。	点分十进制形式。
tos-priority	指定 TOS 字段优先级值。	整数形式，取值范围是 0~7。
dscp	表示区分服务代码点的取值。	<i>dscp</i> 的取值形式是整数形式或名称，其中：

参数	说明	取值
		采用整数形式时，取值范围是 0~63。 采用名称时，取值为如下关键字 af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1, cs2, cs3, cs4, cs5, cs6, cs7, default 或 ef。
tos field	制定的 ACL 规则的 ToS 字段	整数形式，取值范围是 0-7。
fragment	指定该规则是否仅对非首片分片报文有效。	-
proto-type field	制定的 ACL 规则的协议类型字段	整数形式，取值范围是 1-255。
ttl field	制定的 ACL 规则的 TTL 字段	整数形式，取值范围是 1-255。

## 7.2.4 配置混合 ACL

### 背景信息

一条 ACL 是由若干规则和动作组成的一系列的列表，若干个规则列表构成一条 ACL。

配置混合 ACL 的规则之前，首先需要创建一条混合 ACL 并指定 ACL 种类标示编号为 2001~3000。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
创建一条混合 ACL	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>filter-list acl-number</b> 使用编号创建一条混合 ACL（访问控制列表），并进入混合 ACL 配置视图；</li> <li>3. 结束。</li> </ol>
配置混合 ACL 规则	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>filter-list acl-number</b> 进入混合 ACL 配置视图；</li> <li>3. 混合模式可以配置二层和三层的 ACL 规则，请参考本手册 7.2.2 和 7.2.3 小节 ACL 规则的配置命令；</li> <li>4. 结束。</li> </ol>
配置混合 ACL 动作	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>filter-list acl-number</b> 进入混合 ACL 配置视图；</li> <li>3. 执行以下命令配置 ACL 处理动作； <b>filter rule-number action { permit   deny }</b> <b>filter rule-number action redirect cpu</b></li> </ol>

目的	步骤
	<pre> filter rule-number action mirror cpu filter rule-number action mirror group group-number filter rule-number action redirect { fastethernet   gigaethernet   xgigaethernet   eth-trunk } slot/port filter rule-number action redirect eth-trunk trunk number filter rule-number action redirect ip-nextthop ip-address <b>filter rule-number action redirect ip-multihop ip-address ip-address</b> <b>filter rule-number action redirect ip-multihop ip-address ip-address</b> ip-address <b>filter rule-number action redirect ip-multihop ip-address ip-address</b> ip-address ip-address filter rule-number action { insert-outer-vid   replace-outer-vid } vlan-id filter rule-number action { insert-inner-vid   replace-inner-vid   remove-inner-vid } filter rule-number action vfp { insert-inner-vid   replace-inner-vid  insert-outer-vid   replace-outer-vid  deny   remove-inner-vid } Vlan ID filter rule-number action vfp filter rule-number action { cos   precedence   outer-tag-priority   inner-tag-priority } priority-value filter rule-number action { outer-tag-priority inner-tag-priority } Priority-value filter rule-number action outer-tag-priority inner-tag-priority filter rule-number action dscp dscp filter rule-number action { precedence-priority   priority-precedence } <b>filter rule-number action counter counter number</b> 4. 结束。 </pre>
绑定混合 ACL	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>filter-list global { in   out } acl-number</b> 用来全局绑定到指定的 ACL；</li> <li>3. 或执行命令 <b>filter-list acl-number</b> 进入混合 ACL 配置视图，再执行命令 <b>filter-list { in   out } acl-number</b> 用来将 ACL 应用到物理端口，trunk 接口或者 VLAN 端口；</li> <li>4. 结束。</li> </ol>

附表：

参数	说明	取值
acl-number	表示访问控制列表的序号。	整数形式，取值范围是 1~4000，其中： <1-1000>是设置二层 ACL。 <1001-2000>是设置 IPv4 ACL。

参数	说明	取值
		<2001-3000>是设置混合 ACL。 <3001-4000>是设置 IPv6 ACL。
rule-number	指定的访问控制列表的规则序号。	整数形式，取值范围是 1~16384。
src-mac-address/M   any	指定的 ACL 规则的源 MAC 地址信息。	M 为整数形式，范围为 1~24。 any 代表任意源 MAC 地址。
dst-mac-address/M   any	指定的 ACL 规则的目的 MAC 地址信息。	M 为整数形式，范围为 1~24。 any 代表任意目的 MAC 地址。
src-mac-mask	指定的 ACL 规则的源 MAC 地址掩码信息。	点分十进制形式。
dst-mac-mask	指定的 ACL 规则的目的 MAC 地址掩码信息。	点分十进制形式。
provider (<1-4094>/<1-4094>) (any <0-7>) customer (any <1-4094>)(any <0-7>)	VID 号/VID 范围或者任何以上两者取值	-
rule-number	指定的访问控制列表的规则序号。	整数形式，取值范围是 1~16384。
VLAN ID	VLAN 号	整数形式，取值范围是 1~4094

## 7.2.5 配置三层 ACL6

### 背景信息

一条 ACL 是由若干规则和动作组成的一系列的列表，若干个规则列表构成一条 ACL。

配置三层 ACL6 的规则之前，首先需要创建一条三层 ACL6 并指定 ACL6 种类标示编号为 3001~4000。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
创建一条三层 ACL6	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>filter-list acl-number</b> 使用编号创建一条三层 ACL6（访问控制列表），并进入三层 ACL6 配置视图；</li> <li>3. 结束。</li> </ol>
配置三层 ACL6 规则	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>filter-list acl-number</b> 进入三层 ACL6 配置视图； 【用户可以从步骤 3~步骤 8 中根据需要任选配置】</li> <li>3. （可选）执行以下命令用来配置 IP6 匹配的 ACL 规则（用户根据需</li> </ol>

目的	步骤
	<p>要自行从以下命令中选择配置)；</p> <pre>filter rule-number ip6 { src-ip6-address/M   any } { dst-ip6-address/M   any }</pre> <pre>filter rule-number ip6 { src-ip6-address/M   any } { dst-ip6-address/M   any } next-header next-header value</pre> <pre>filter rule-number ip6 { src-ip6-address/M   any } { dst-ip6-address/M   any } hop-limit hop-limit value</pre> <p>4. (可选) 执行以下命令用来配置 TCP6 匹配的 ACL 规则 (用户根据需要自行从以下命令中选择配置)；</p> <pre>filter filter number tcp6 (src-ip6-address/M  any) (&lt;0-65535&gt; &lt;0-65535&gt;/&lt;0-65535&gt; any) (dst-ip6-address/M  any) (&lt;0-65535&gt; &lt;0-65535&gt;/&lt;0-65535&gt; any)</pre> <pre>filter filter number tcp6 (src-ip6-address/M  any) (&lt;0-65535&gt; &lt;0-65535&gt;/&lt;0-65535&gt; any) (dst-ip6-address/M  any) (&lt;0-65535&gt; &lt;0-65535&gt;/&lt;0-65535&gt; any)</pre> <p>(syn synack ack fin finack psh rst urg field) fragment</p> <p>5. (可选) 执行以下命令用来配置 ICMP6 匹配的 ACL 规则 (用户根据需要自行从以下命令中选择配置)；</p> <pre>filter filter number icmp6 (src-ip6-address/M  any) (dst-ip6-address M  any)</pre> <pre>filter filter number icmp6 (src-ip6-address/M  any) (dst-ip6-address M  any) (icmp type any) (icmp code any)</pre> <p>6. (可选) 执行以下命令用来配置 IGMP6 匹配的 ACL 规则 (用户根据需要自行从以下命令中选择配置)；</p> <pre>filter filter number igmp6 (src-ip6-address/M  any) (dst-ip6-address M  any)</pre> <p>7. (可选) 执行以下命令用来配置 UDP6 匹配的 ACL 规则 (用户根据需要自行从以下命令中选择配置)；</p> <pre>filter filter number udp6 (src-ip6-address/M  any) (&lt;0-65535&gt; &lt;0-65535&gt;/&lt;0-65535&gt; any) (dst-ip6-address/M  any) (&lt;0-65535&gt; &lt;0-65535&gt;/&lt;0-65535&gt; any) fragment</pre> <p>8. 结束。</p>
配置三层 ACL6 动作	<p>1. 执行命令 <b>configure</b> 进入全局配置视图；</p> <p>2. 执行命令 <b>filter-list acl-number</b> 进入三层 ACL6 配置视图；</p> <p>3. 执行以下命令配置 ACL 处理动作；</p> <pre>filter rule-number action { permit   deny }</pre> <pre>filter rule-number action redirect cpu</pre> <pre>filter rule-number action mirror cpu</pre> <pre>filter rule-number action mirror group group-number</pre> <pre>filter rule-number action redirect { fastethernet   gigabitethernet  </pre>

目的	步骤
	<pre>xgigaehternet   eth-trunk } slot/port filter rule-number action redirect eth-trunk trunk number filter rule-number action redirect ip-nexthop ip-address <b>filter rule-number action redirect ip-multihop ip-address ip-address</b> <b>filter rule-number action redirect ip-multihop ip-address ip-address</b> ip-address <b>filter rule-number action redirect ip-multihop ip-address ip-address</b> ip-address ip-address ip-address ip-address filter rule-number action { insert-outer-vid   replace-outer-vid } vlan-id filter rule-number action { insert-inner-vid   replace-inner-vid   remove-inner-vid } filter rule-number action vfp { insert-inner-vid   replace-inner-vid  insert-outer-vid   replace-outer-vid  deny   remove-inner-vid } Vlan ID filter rule-number action vfp filter rule-number action { cos   precedence   outer-tag-priority   inner-tag-priority } priority-value filter rule-number action { outer-tag-priority  inner-tag-priority } Priority-value filter rule-number action outer-tag-priority inner-tag-priority filter rule-number action dscp dscp filter rule-number action { precedence-priority   priority-precedence } <b>filter rule-number action counter counter number</b> 4. 结束。</pre>
绑定三层 ACL6	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>filter-list global { in   out } acl-number</b> 用来全局绑定到指定的 ACL；</li> <li>3. 或执行命令 <b>filter-list acl-number</b> 进入三层 ACL6 配置视图，再执行命令 <b>filter-list { in   out } acl-number</b> 用来将 ACL6 应用到物理端口 ,trunk 接口或者 VLAN 端口；</li> <li>4. 结束。</li> </ol>

附表：

参数	说明	取值
acl-number	表示访问控制列表的序号。	整数形式，取值范围是 1~4000，其中： <1-1000>是设置二层 ACL。 <1001-2000>是设置 IPv4A CL。 <2001-3000>是设置混合 ACL。 <3001-4000>是设置 IPv6A CL。
rule-number	指定的访问控制列表的规	整数形式，取值范围是 1~16384。



参数	说明	取值
	则序号。	
src-ip6-address/M   any	指定的 ACL 规则的源 IP 地址信息。	src-ip6-address 为点分十六进制形式，形如 X: X:: X: X, M 为整数形式，范围为 1~128。 any 代表任意源 IP 地址。
dst-ip6-address/M   any	指定的 ACL 规则的目的 IP 地址信息。	dst-ip6-address 为点分十六进制形式，形如 X: X:: X: X, M 为整数形式，范围为 1~128。 any 代表任意目的 IP 地址。
next-header value	下一个报头的值	整数形式，取值范围是 1~255。
hop-limit value	跳数限制值	整数形式，取值范围是 1~255。
icmp type	制定的 ACL 规则的 ICMP 类型范围	整数形式，取值范围是 1-255。
icmp code	制定的 ACL 规则的 ICMP 编码范围	整数形式，取值范围是 1-255。
(<0-65535> <0-65535>/<0-65535> any)	目的端口号/端口范围	-
field	字段范围，包括 syn、synack、ack、fin、finack、psh、rst 以及 urg 字段	<0-63>: 整数形式，取值范围是 0-63。
fragment	指定该规则是否仅对非首片分片报文有效。	-
(request response any)	ARP 请求消息/响应消息或者任何以上两种	-

## 7.2.6 配置 ACL 可选功能项

### 背景信息

ACL 可选功能项包括：

- 创建 ACL 生效时间段

创建 ACL 生效时间段以后，当配置 ACL 规则时引用该时间段，该 ACL 规则才会在这个时间段内生效；如果配置规则时不指定时间段，则该规则不受时间范围限制，除非删除该 ACL。

- 创建 ACL 限速模板

创建限速模板之后，当配置 ACL 规则时与限速模板绑定，该 ACL 规则才会根据不同的限速规则对数据包进行过滤。

- 创建 ACL 计数模板

创建计数模板之后，当配置 ACL 规则时与计数模板绑定，该 ACL 规则才会根据不同的计数类型对数据包进行统计。

### 目的

根据实际应用情况，配置 ACL 可选项功能可以为用户提供丰富的数据包过滤方法。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
创建 ACL 生效时间段	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>time-range list LIST-NUMBER</b> 用来进入某条 time-range 配置视图；</li> <li>3. 执行以下命令用来配置 time-range 模块起始结束的绝对时间： <b>time-range RANGE-NUMBER absolute from hh:mm:ss YY/MMDD</b> 或 <b>time-range RANGE-NUMBER absolute from hh:mm:ss YY/MMDD to hh:mm:ss YY/MMDD</b>；</li> <li>4. 执行命令 <b>time-range RANGE-NUMBER everyday hh:mm:ss to hh:mm:ss</b> 用来配置 time-range 模块每日时间范围；</li> <li>5. 执行命令 <b>time-range RANGE-NUMBER everyhour mm:ss to mm:ss</b> 用来配置 time-range 模块每小时时间范围；</li> <li>6. 执行命令 <b>time-range RANGE-NUMBER everymonth hh:mm:ss MM to hh:mm:ss MM</b> 用来配置 time-range 模块每月时间范围；</li> <li>7. 执行命令</li> <li>8. 执行命令 <b>time-range RANGE-NUMBER everyweek hh:mm:ss (mon tue wed thu fri sat sun) to hh:mm:ss (mon tue wed thu fri sat sun)</b> 用来配置 time-range 模块每周时间范围；</li> <li>9. 执行命令 <b>time-range RANGE-NUMBER everyweekday hh:mm:ss to hh:mm:ss</b> 用来配置 time-range 模块每周除周末以外的时间范围；</li> <li>10. 执行命令 <b>time-range RANGE-NUMBER everyweekend hh:mm:ss to hh:mm:ss</b> 用来配置 time-range 模块每周末的时间范围；</li> <li>11. 执行命令 <b>time-range RANGE-NUMBER everyyear hh:mm:ss MM/DD to hh:mm:ss MM/DD</b> 用来配置 time-range 模块每年的时间范围；</li> <li>12. 执行命令 <b>quit</b> 退出到全局配置视图；</li> <li>13. 执行命令 <b>filter-list acl-number</b> 进入 ACL 配置视图；</li> <li>14. 执行命令 <b>time-tange list time-range acl-number</b> 用来时间段模板与 ACL 绑定；</li> <li>15. 结束。</li> </ol>

目的	步骤
创建 ACL 限速模板	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行以下命令用来配置配置 Meter 模板：  <pre>meter meter-number cir CIR-number cbs CBS-number ebs EBS-number meter meter-number cir CIR-number cbs CBS-number ebs EBS-number (aware blind) meter meter-number cir CIR-number cbs CBS-number pbs PBS-number pir PIR number meter meter-number cir CIR-number cbs CBS-number pbs PBS-number pir PIR number (aware blind)</pre> </li> <li>3. 执行命令 <b>filter-list acl-number</b> 进入 ACL 配置视图；</li> <li>4. 执行命令 <b>filter rule-number meter meter-number</b> 用来配置 ACL 规则和某个 meter 模板绑定；</li> <li>5. 执行命令用来配置根据限速模板着色后包的处理：  <pre>filter rule-number outaction { red   yellow } drop filter rule-number outaction { red   yellow } remark-dscp dscp filter rule-number outaction { red   yellow } remark-dot1p priority filter rule-number car car-value outaction drop</pre> </li> <li>6. 结束。</li> </ol>
创建 ACL 计数模板	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>counter counter-number (packet/byte all) sort (green/red/greenred/greenyellow/redyellow  total)</b> 用来配置 Counter 模板</li> <li>3. 执行命令 <b>filter-list acl-number</b> 进入 ACL 配置视图；</li> <li>4. 执行命令 <b>filter rule-number action counter counter-number</b> 用来配置计数模板与 ACL 绑定；</li> <li>5. 结束。</li> </ol>

附表：

参数	说明	取值
LIST-NUMBER	time-range 模块列表名。	整数形式，取值范围是 1~128。
RANGE-NUMBER	range 号。	整数形式，取值范围是 1~16。
hh:mm:ss	起始或结束的时间（时：分：秒）。	整数形式，取值范围分别是 <0-23> : <0-59> : <0-59>。
YY/MM/DD	起始或结束的时间（年/月/日）。	整数形式，取值范围分别是 <2000-2100>: <1-12>: <1-31>。
mm:ss	起始或结束的时间（分：秒）。	整数形式，取值范围分别是 <0-59>: <0-59>。

参数	说明	取值
MM	日期。	整数形式，取值范围为 <1-31>。
(mon tue wed thu fri sat sun)	星期。	-
MM/DD	起始或结束的时间（月/日）。	整数形式，取值范围分别是 <1-12>: <1-31>。
acl-number	表示访问控制列表的序号。	整数形式，取值范围是 1~4000，其中： <1-1000> 是设置二层 ACL。 <1001-2000> 是设置 IPv4 ACL。 <2001-3000> 是设置混合 ACL。 <3001-4000> 是设置 IPv6 ACL。
meter number	meter 号	整数形式，取值范围是 1-256。
CIR number	CIR 条目	整数形式，取值范围是 8-4294967295。
CBS number	CBS 条目	整数形式，取值范围是 10000-4294967295。
EBS number	EBS 条目	整数形式，取值范围是 10000-4294967295。
PBS number	PBS 条目	整数形式，取值范围是 10000-4294967295。
PIR number	PIR 条目	整数形式，取值范围是 8-4294967295。
aware	对配置的限速规则和定色规则作出反应	-
blind	不对配置的限速规则和定色规则作出任何反应	-
counter number	计数器号	整数形式，取值范围是 1~1024。
packet/byte all	计数器的数据包类型、字节类型	-
green/red/greenred/greenyellow/redyellow total	计数器状态显示类型，包括绿、红色、绿/红色、绿/黄色和红/黄色	-
redyellow	表示数据包被标记的颜色。	-
drop	表示丢弃数据包。	-
remark-dscp	表示重置 dscp 值。	-

参数	说明	取值
dscp	表示区分服务代码点的取值。	<b>dscp</b> 的取值形式是整数形式或名称，其中： 采用整数形式时，取值范围是 0~63。 采用名称时，取值为如下关键字 af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1, cs2, cs3, cs4, cs5, cs6, cs7, default 或 ef。
remark-dot1p	表示重置 802.1p 优先级的值。	-
priority	表示 VLAN Tag 字段中 802.1p 优先级的取值。	整数形式，取值范围是 0~7。.

## 7.2.7 维护及调试

### 目的

当 ACL 功能不正常，需要进行查看、调试或定位问题时，可以使用本小节操作。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
清除 ACL 的统计信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行以下命令用来重置 ACL（访问控制列表）的过滤器条目计数；  <code>reset counter filte-list acl-number filter filter-number { in   out }</code>  <code>reset counter filte-list acl-number filter filter-number port (fastethernet gigaethernet xgigaethernet) slot-number port-number { in   out }</code>  <code>reset counter filte-list acl-number filter filter-number port eth-trunk trunk-number { in   out }</code>  <code>reset counter filte-list acl-number filter filter-number vlan VLANID { in   out }</code> </li> <li>3. 结束。</li> </ol>
删除 ACL 动作	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>filter-list acl-number</b> 进入 ACL 配置视图；</li> <li>3. 执行命令 <b>no filter rule-number action</b> 用来删除 ACL 规则对应的处理动作；</li> <li>4. 结束。</li> </ol>

目的	步骤
删除 ACL 规则	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>filter-list acl-number</b> 进入 ACL 配置视图；</li> <li>3. 执行命令 <b>no filter rule-number</b> 用来删除 ACL 规则；</li> <li>4. 结束。</li> </ol>
查看访问控制列表的配置信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b>或<b>interface eth-trunk trunk-number</b>进入接口配置视图，或执行命令 <b>filter-list acl-number</b> 进入 ACL 配置视图，或不执行任何命令保持当前特权用户视图； <ol style="list-style-type: none"> <li>2. 执行命令 <b>show filter-list</b> 或 <b>show filter-list acl-number</b> 用来显示访问控制列表的配置信息；</li> <li>3. 结束。</li> </ol> </li> </ol>
查看 ACL 配置文件信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b>或<b>interface eth-trunk trunk-number</b>进入接口配置视图，或执行命令 <b>filter-list acl-number</b> 进入 ACL 配置视图，或不执行任何命令保持当前特权用户视图； <ol style="list-style-type: none"> <li>2. 执行命令 <b>show filter-list config</b> 显示 ACL 配置文件信息；</li> <li>3. 结束。</li> </ol> </li> </ol>
查看访问控制列表的统计信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b>或<b>interface eth-trunk trunk-number</b>进入接口配置视图，或执行命令 <b>filter-list acl-number</b> 进入 ACL 配置视图，或不执行任何命令保持当前特权用户视图； <ol style="list-style-type: none"> <li>2. 执行命令 <b>show filter-list statistic</b> 用来显示访问控制列表的统计信息；</li> <li>3. 结束。</li> </ol> </li> </ol>
查看所有应用了访问控制列表的端口信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b>或<b>interface eth-trunk trunk-number</b>进入接口配置视图，或执行命令 <b>filter-list acl-number</b> 进入 ACL 配置视图，或不执行任何命令保持当前特权用户视图； <ol style="list-style-type: none"> <li>2. 执行命令 <b>show filter-list interface</b> 用来显示所有应用了访问控制列表的端口信息；</li> <li>3. 结束。</li> </ol> </li> </ol>
查看访问控制列表全局配置情况	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b>或<b>interface eth-trunk trunk-number</b>进入接口配置视图，或执行命令 <b>filter-list acl-number</b> 进入 ACL 配置视图，或不执行任何命令保持当前特权用户视图； <ol style="list-style-type: none"> <li>2. 执行命令 <b>show filter-list global</b> 访问控制列表全局配置情况；</li> </ol> </li> </ol>

目的	步骤
	3. 结束。
查看统计表信息、配置信息	1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或不执行任何命令保持当前特权用户视图； 2. 执行命令 <b>show counter config</b> 或 <b>show counter counter-id</b> 或 <b>show counter</b> 用来显示统计表信息、配置信息； 3. 结束。

附表：

参数	说明	取值
acl-number	可选参数，指定要查看的访问控制列表的编号。	整数形式，取值范围是 1~4000。
counter-id	统计表 ID	整数形式，取值范围是 1~1024

## 7.2.8 配置举例

### 7.2.8.1 配置二层 ACL 示例

#### 组网要求

SC9600 作为网关设备，下挂用户 PC。要求配置 ACL，禁止源 MAC 地址为 0001-0203-0405、目的 MAC 地址为 0102-0304-0506 的报文通过。

#### 组网图

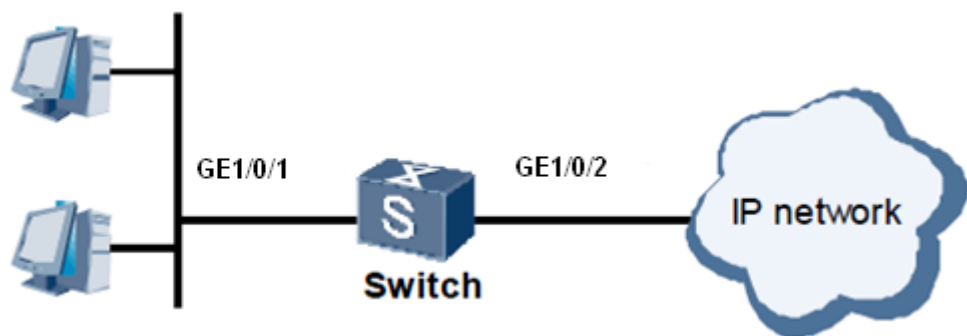


图 7-1 二层 ACL 示例图

#### 配置步骤

1、创建二层 ACL。

```
SC9600#configure
```

```
SC9600(config)#filter-list 1
SC9600(configure-filter-l2-1)#
```

2、配置二层 ACL 规则。

```
SC9600(configure-filter-l2-1)#filter 1 mac 00:01:02:03:04:05/48 01:02:03:04:05:06/48
```

3、配置二层 ACL 动作。

```
SC9600(configure-filter-l2-1)#filter 1 action deny
```

4、端口绑定 ACL。

```
SC9600(configure-filter-l2-1)#quit
SC9600(config)#interface gigabitEthernet 1/0/1
SC9600(config-ge1/0/1)#filter-list in 1
```

### 7.2.8.2 配置三层 ACL 示例

#### 组网要求

公司企业网通过 Switch 实现各部门之间的互连。要求正确配置 IPv4 ACL，禁止研发部门在上班时间（8:30 至 17:30）访问工资查询服务器（IP 地址为 10.164.9.9），而总裁办公室不受限制，可以随时访问。

#### 组网图

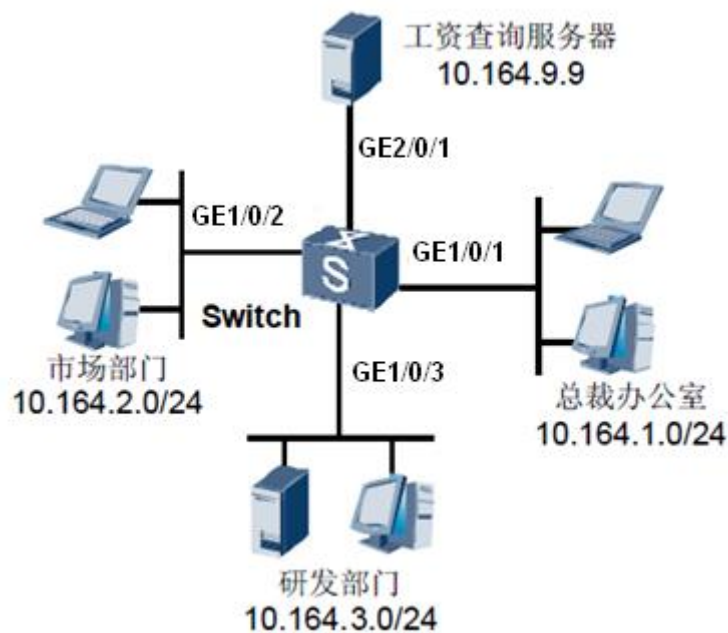


图 7-2 三层 ACL 示例图



**配置步骤**

1、配置 time-range。

```
SC9600#configure
SC9600(config)#time-range list 1
SC9600(config-timerange1)#time-range 1 everyweekday 8:30:00 to 17:30:00
SC9600(config-timerange1)#quit
```

2、配置总裁办公室允许访问工资查询服务器的 ACL。

```
SC9600(config)# filter-list 1001
SC9600(configure-filter-ipv4-1001)#filter 1 ip 10.164.1.0/24 10.164.9.9/32
SC9600(configure-filter-ipv4-1001)#filter 1 action permit
SC9600(configure-filter-ipv4-1001)#quit
```

3、配置市场部门禁止访问工资查询服务器的 ACL。

```
SC9600(config)#filter-list 1002
SC9600(configure-filter-ipv4-1002)#filter 1 ip 10.164.2.0/24 10.164.9.9/32
SC9600(configure-filter-ipv4-1002)#filter 1 action deny
```

4、配置市场部门在指定时间段内禁止访问工资查询服务器。

```
SC9600(configure-filter-ipv4-1002)#filter 1 time-range 1
SC9600(configure-filter-ipv4-1002)#quit
```

5、配置研发部门禁止访问工资查询服务器的 ACL。

```
SC9600(configure)# filter-list 1003
SC9600(configure-filter-ipv4-1003)#filter 1 ip 10.164.3.0/24 10.164.9.9/32
SC9600(configure-filter-ipv4-1003)#filter 1 action deny
```

6、配置研发部门在指定时间段内禁止访问工资查询服务器。

```
SC9600(configure-filter-ipv4-1003)#filter 1 time-range 1
SC9600(configure-filter-ipv4-1003)#quit
```

7、将 ACL 应用到端口上。

```
SC9600(config)#interface gigabitEthernet 1/0/1
SC9600(config-ge1/0/1)#filter-list in 1001
SC9600(config-ge1/0/1)#quit
SC9600(config)#interface gigabitEthernet 1/0/2
SC9600(config-ge1/0/2)#filter-list in 1002
SC9600(config-ge1/0/2)#quit
SC9600(config)#interface gigabitEthernet 1/0/3
```

SC9600(config-ge1/0/3)#filter-list in 1003

### 7.2.8.3 配置混合 ACL 示例

#### 组网要求

SC9600 作为网关设备，下挂用户 PC。要求配置 ACL，将源 MAC 地址为 00:01:02:00:00:00/24 网段、源 IP 地址为 1.2.3.1/24 网段的报文送 CPU。

#### 组网图

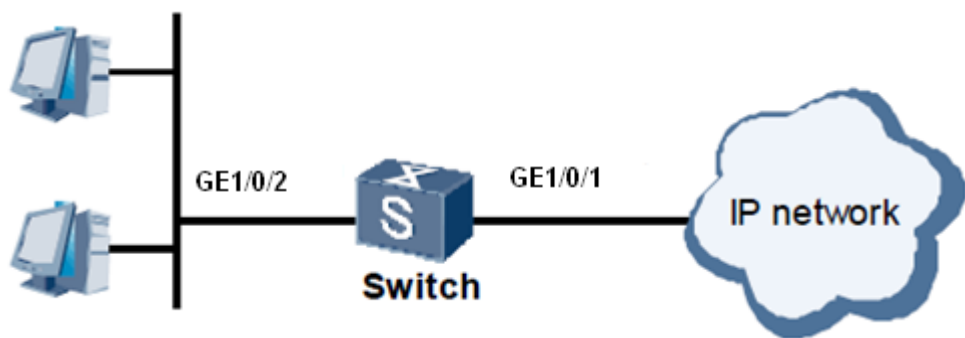


图 7-3 混合 ACL 示例图

#### 配置步骤

1、创建混合 ACL。

```
SC9600#configure
SC9600(config)#filter-list 2001
SC9600(configure-filter-hybrid-2001)#
```

2、配置二层 ACL 规则。

```
SC9600(configure-filter-hybrid-2001)#filter 1 mac 00:01:02:00:00:00/24 any eth-type
any provider any any customer any any ip 1.2.3.1/24 any proto-type any
```

3、配置二层 ACL 动作。

```
SC9600(configure-filter-hybrid-2001)#filter 1 action cpu
```

4、端口绑定 ACL。

```
SC9600(configure-filter-hybrid-2001)#quit
SC9600(config)#interface gigaethernet 1/0/2
SC9600(config-ge1/0/2)#filter-list in 2001
```

### 7.2.8.4 配置三层 ACL6 示例

#### 组网要求

SC9600 A 通过 GE 接口与 SC9600 B 相连。在 SC9600 A 上配置 ACL6 规则，禁止源地址为 3001::2 的 IPv6 报文进入 SC9600 A 的 GE1/0/1 接口。

#### 组网图

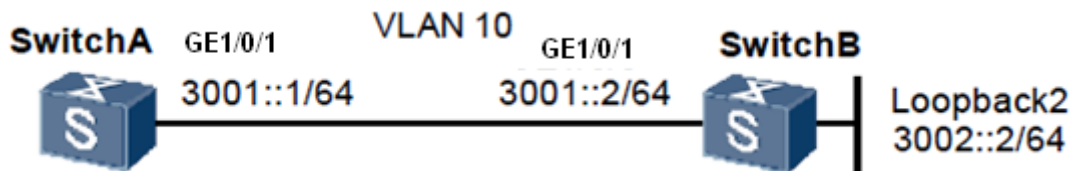


图 7-4 三层 ACL6 示例图

#### 配置步骤

1、创建三层 ACL6。

```
SC9600#configure
SC9600(config)#filter-list 3001
SC9600(configure-filter-ipv6-3001)#
```

2、配置三层 ACL6 规则。

```
SC9600(configure-filter-ipv6-3001)#filter 1 ip6 3001::2/64 any
```

3、配置三层 ACL6 动作。

```
SC9600(configure-filter-ipv6-3001)#filter 1 ac deny
```

4、在 SC9600 A 的 GE1/1 接口的入方向绑定该 ACL。

```
SC9600(configure-filter-ipv6-3001)#quit
SC9600(config)#interface gigaethernet 1/0/1
SC9600(config-ge1/0/1)#filter-list in 3001
```

### 7.2.8.5 配置限速模板示例

#### 组网要求

SC9600 作为网关设备，下挂用户 PC。要求配置 ACL，对 SC9600 的 GE 1/0/2 端口收到源 MAC 地址为 0001-0203-0405 的报文进行限速，黄色报文 dscp 的值修改为 AF11。

#### 组网图

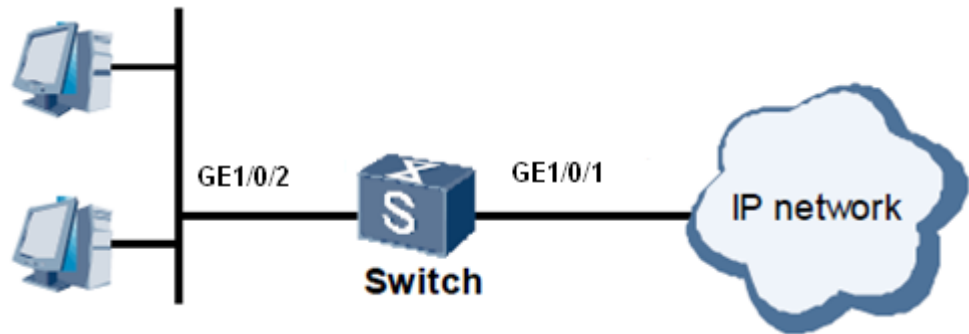


图 7-5 限速模板示例图

### 配置步骤

1、配置限速模板。

```
SC9600#configure
```

```
SC9600(config)#meter 1 cir 64 cbs 10000 pbs 10000 pir 64
```

2、创建 ACL。

```
SC9600(config)#filter-list 1
```

```
SC9600(configure-filter-l2-1)#
```

3、配置 ACL 规则。

```
SC9600(configure-filter-l2-1)#filter 1 mac 00:01:02:03:04:05/48 any
```

4、将限速模板与该 ACL 绑定。

```
SC9600(configure-filter-l2-1)#filter 1 meter 1
```

5、配置 ACL 动作。

```
SC9600(configure-filter-l2-1)#filter 1 outaction yellow remark-dscp af11
```

6、绑定 ACL 到端口。

```
SC9600(configure-filter-l2-1)#quit
```

```
SC9600(config)#interface gigabitEthernet 1/0/2
```

```
SC9600(config-ge1/0/2)#filter-list in 1
```

### 7.2.8.6 配置计数模板示例

#### 组网要求

SC9600 作为网关设备，下挂用户 PC。要求配置 ACL，对 SC9600 A 的 GE1/0/2 端口收到源 IP 地址为 10.1.1.1/24 网段的报文进行计数，统计报文的个数。

#### 组网图

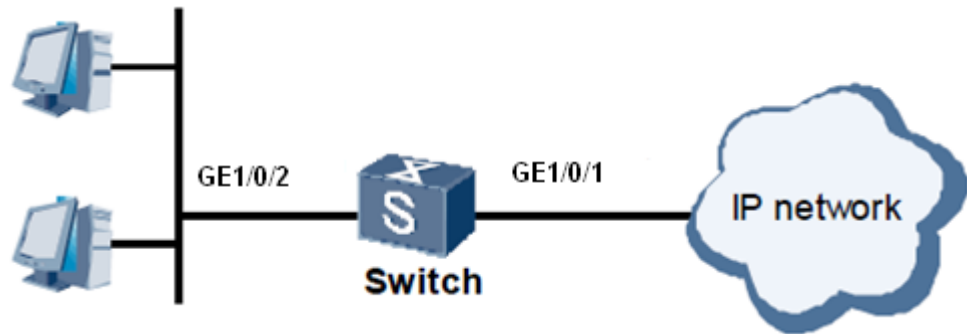


图 7-6 计数模板示例图

### 配置步骤

1、配置计数模板。

```
SC9600#configure
```

```
SC9600(config)# counter 1 packet sort total
```

2、创建 ACL。

```
SC9600(config)#filter-list 1001
```

```
SC9600(configure-filter-ipv4-1001)#
```

3、配置 ACL 规则。

```
SC9600(configure-filter-ipv4-1001)#filter 1 ip 10.1.1.1/24 any
```

4、将计数模板与该 ACL 绑定。

```
SC9600(configure-filter-ipv4-1001)#filter 1 action counter 1
```

5、端口绑定 ACL。

```
SC9600(configure-filter-ipv4-1001)#quit
```

```
SC9600(config)#interface gigaethernet 1/0/2
```

```
SC9600(config-ge1/0/2)#filter-list in 1
```

## 7.3 IP Source Guard 配置

### 7.3.1 IP Source Guard 简介

#### 7.3.1.1 技术背景

IP 地址的盗用方法多种多样，其常用方法主要有以下几种：

1. 静态修改 IP 地址

对于任何一个 TCP/IP 实现来说，IP 地址都是其用户配置的必选项。如果用户在配置 TCP/IP 或修改 TCP/IP 配置时，使用的不是授权分配的 IP 地址，就形成了 IP 地址盗用。由于 IP 地址是一个逻辑地址，因此无法限制用户对于其主机 IP 地址的静态修改。

2. 成对修改 IP-MAC 地址对于静态修改 IP 地址的问题，现在很多单位都采用 IP 与 MAC 绑定技术加以解决。针对绑定技术，IP 盗用技术又有了新的发展，即成对修改 IP-MAC 地址。现在的一些兼容网卡，其 MAC 地址可以使用网卡配置程序进行修改。如果将一台计算机的 IP 地址和 MAC 地址都改为另外一台合法主机的 IP 地址和 MAC 地址，其同样可以接入网络。

另外，对于那些 MAC 地址不能直接修改的网卡来说，用户还可以采用软件的办法来修改 MAC 地址，即通过修改底层网络软件达到欺骗上层网络软件的目的。

3. 动态修改 IP 地址某些攻击程序在网络上收发数据包，可以绕过上层网络软件，动态修改自己的 IP 地址（或 IP-MAC 地址对），以达到 IP 欺骗。

IPSG 特性是一种二层接口特性，能够提供检测机制来确保单个接口所接受到的数据包能够被各个接口所接受。如果检查成功通过，那么就将许可数据包；否则将会发生违背策略的活动。IPSG 不仅能够确保第二层网络中终端设备的 IP 地址不被劫持，而且还能确保非授权设备不能通过自己指定 IP 地址的方式来访问网络或导致网络崩溃及瘫痪。

通过配置 IPSG，在链路 UP 的时候，只有 DHCP 数据包被许可通过。一旦 DHCP 服务器分配了 IP 地址，那么就将更新 DHCP 绑定表。IPSG 然后自动在接口加载基于端口的 ACL。上述过程能够将客户端流量限定到绑定表中所配置的源 IP 地址。对于来自源 IP 绑定之外的其他源 IP 地址的主机端口的流量，他们都将过滤。过滤能够限制主机从相邻主机夺取 IP 地址实现网络攻击的功能。

IP Source Guard 是基于 IP/MAC 的端口流量过滤技术，可以防止局域网内的 IP 地址欺骗攻击。交换机内部有一个 IP source binding table 作为每个端口接受到的数据包的检测标准，只有在两种情况下，交换机会转发数据——或者所接收到的 IP 包满足 IP source binding table 中 port/IP/MAC 的对应关系，或者是接收到的是 DHCP 数据包，其余数据包将被交换机做丢弃处理。IP source binding table 可以由用户在交换机上静态的配置，也可以由交换机从 DHCP Snooping 自动学习获得。静态配置是一种简单而固定的方式，灵活性很差，因此建议用户最好结合 DHCP Snooping 使用 IP Source Guard，由 DHCP Snooping Binding Database 生成 IP source binding table。

### 7.3.1.2 基本概念

#### IP Source Guard

IP 源防护，相当于在端口上添加了一条 ACL 表项，默认过滤该端口上所有用户发送的 IP 报文（除 DHCP 报文外）。当用户通过 DHCP 交互申请 IP 地址后，会在该端口上添加一条过滤表项，允许该用户使用该地址进行 IP 报文的通讯，其他用户依然禁止通讯。

### DHCP Snooping

意为 DHCP 窥探，通过对 Client 和服务器之间的 DHCP 交互报文进行窥探，实现对用户的监控，同时 DHCP Snooping 起到一个 DHCP 报文过滤的功能，通过合理的配置实现对非法服务器的过滤。

### IP Source Binding Table

IP 源绑定表可以由用户在交换机上静态添加，或者由交换机从 DHCP 监听绑定表（DHCP Snooping Binding Table）自动学习获得。静态配置是一种简单而固定的方式，但灵活性很差，因此建议用户最好结合 DHCP Snooping 技术使用 IP Source Guard，由 DHCP 监听绑定表生成 IP 源绑定表。

### ACL

访问控制列表是应用在路由器接口的指令列表，这些指令列表用来告诉路由器哪些数据包可以接收、哪些数据包需要拒绝。至于数据包是被接收还是被拒绝，可以由类似于源地址、目的地址、端口号、协议等特定指示条件来决定。

#### 7.3.1.3 功能特性

IP Source Guard 功能特性如表 7-1所示：

表 7-1 IP Source Guard 功能特性

序号	功能名称	功能描述
1	源 IP+PORT 过滤	根据源 IP 地址和端口对 IP 流量进行过滤，只有当流与绑定条目匹配时才允许通过。当端口创建、修改、删除新的 IP 源绑定条目的时候，IP 源地址过滤器将发生变化。为了能够反映 IP 源绑定的变更，端口 ACL 将被重新修改并重新应用到端口上。默认情况下，如果端口在没有存在 IP 源绑定条目的情况下启用了 IP 源防护功能，默认的 ACL 将拒绝端口的所有流量（实际上是除 DHCP 报文以外的所有 IP 流量）。
2	源 IP+PORT+MAC 过滤	同上
3	源 IP+PORT+VLAN 过滤	同上

序号	功能名称	功能描述
4	源 IP+PORT+MAC+VLAN 过滤	同上

### 7.3.1.4 系统特点

IP Source Guard 系统特点如下：

- IP+PORT+MAC+VLAN 多元组合绑定来过滤 IP 流量；
- 可以结合 DHCP Snooping 的动态表项来配合使用，也可以单独发挥作用；
- IP SOURCE GUARD 的配置优先级高于 DHCP Snooping；
- IP SOURCE GUARD 和 DHCP Snooping 共用配置上限；
- 具有强大的 DEBUG 功能；

## 7.3.2 IP Source Guard 配置

### 7.3.2.1 使能 IP Source Guard 功能

#### 目的

本节介绍使能 IP Source Guard 功能的配置。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
使能 IP Source Guard 功能	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet }</b> <i>interface-number</i> 进入接口配置视图；</li> <li>3. 执行命令 <b>user-bind (enable disable)</b></li> </ol>	<p><b>interface-number</b>：SC9600 系列交换机支持以下 3 种型号的接口配置范围：</p> <p>SC9603：取值范围是 &lt;1-3&gt;/&lt;0-4&gt;/&lt;1-48&gt;</p> <p>SC9608：取值范围是 &lt;1-8&gt;/&lt;0-4&gt;/&lt;1-48&gt;</p> <p>SC9612：取值范围是 &lt;1-12&gt;/&lt;0-4&gt;/&lt;1-48&gt;</p>

### 7.3.2.2 配置/删除静态绑定表项

#### 目的

本节介绍配置/删除静态绑定表项。



过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置/删除静态绑定表项	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b> 进入接口配置视图； 3. 执行命令 <b>user-bind ip ipv4-address mac (mac-address any) vid (vlan-id  vlan-id / vlan-id  any) 或 user-bind ip6 ipv6-address mac (mac-address any) vid (vlan-id  vlan-id / vlan-id  any) 或 no user-bind ip ipv4-address 或 no user-bind ip6 ipv6-address</b>	interface-number: SC9600 系列交换机支持以下 3 种型号的接口配置范围： SC9603 : 取值范围是 <1-3>/<0-4>/<1-48> SC9608 : 取值范围是 <1-8>/<0-4>/<1-48> SC9612 : 取值范围是 <1-12>/<0-4>/<1-48> ipv4-address: 目的 IPv4 地址，点分十进制形式，如：(A.B.C.D)，其中 A~D 为 0~255 十进制数。 ipv6-address: 目的 IPv6 地址，点分十六进制形式，形如 X: X:: X: X。 mac-address : 形如 AA:BB:CC:DD:EE:FF/M，点分十进制形式；M 为整数形式，范围为 1~128。 <b>any</b> 代表任意源 MAC 地址。 vlan id  vlan id / vlan id any: <1-4094>: 整数形式，取值范围是 1~4094。 <b>any</b> 代表任意 VID

7.3.2.3 配置 IP Source Guard 调试功能

目的

本节介绍 IP Source Guard 的调试功能配置。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
显示 ip source guard 模块的调试信息	1. 进入特权用户视图； 2. 执行命令 <b>debug ipsg</b>	-

目的	步骤	参数说明
关闭 ip source guard 模块的调试信息	1. 进入特权用户视图; 2. 执行命令 <b>no debug ips</b> g	-

### 7.3.2.4 查看 IP Source Guard 配置信息

#### 目的

本节介绍 IP Source Guard 的配置信息查看。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
查看所有绑定表项	1. 进入普通用户视图或特权用户视图; 2. 执行命令 <b>show user-bind</b>	-
查看所有启用接口	1. 进入普通用户视图或特权用户视图; 2. 执行命令 <b>show user-bind interface</b>	-

### 7.3.3 IP Source Guard 配置举例

#### 组网要求

如图 7-7所示，主机 A 和 B 分别通过接口 ge 1/0/1 、 ge 1/0/2 与交换机相连，保证主机 B 不能仿冒 A 的 IP 和 MAC 欺骗服务器，保证主机 A 的报文能正常上送。

#### 组网图

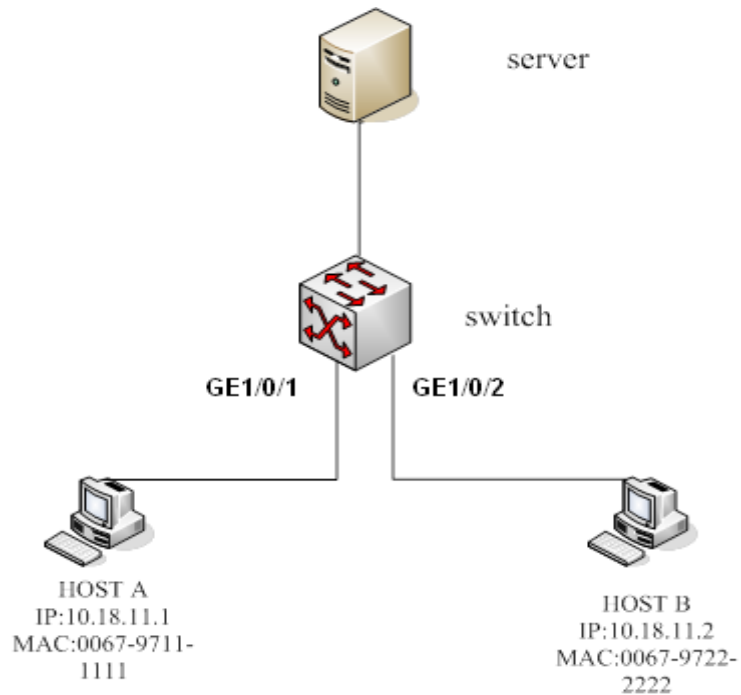


图 7-7 IP Source Guard 组网图

### 配置思路

采用如下思路配置 IP SOURCE GUARD 功能（假设用户的 IP 是静态配置的）：

1. 接口 1 和接口 2 都要使能 IP SOURCE GUARD 功能；
2. 配置静态绑定表项。

### 数据准备

为完成此配置举例，需要准备以下数据：

1. 主机 A 和 B 的 IP 和 MAC；
2. 连接交换机的两个端口 GE 1/0/1 和 GE 1/0/2；
3. 所在 VLAN 1。

### 配置步骤

```

Fengine(config-ge1/0/1)#user-bind enable
Fengine(config-ge1/0/1)##user-bind ip 10.18.11.1 mac 00:67:97:11:11:11/48 vid 1
Fengine(config-ge1/0/2)#user-bind enable
    
```

主机 A 在绑定表中，主机 B 不在，主机 B 发出的包不能被转发。

## 第8章 可靠性配置

### 8.1 概述

本章介绍了 SC9600 系列高端交换机可靠性管理的基本内容、配置过程和配置举例。

本章包括如下主题：

内容	页码
8.1 概述	8-1
8.2 MSTP 配置	8-1
8.3 RLINK 配置	8-23
8.4 BFD 配置	8-38
8.5 VRRP	8-48
8.6 G.8032 配置	8-60
8.7 ESR 配置	8-83
8.8 EFM 配置	8-101
8.9 CFM 配置	8-114
8.10 Y.1731 配置	8-138

### 8.2 MSTP 配置

#### 8.2.1 STP 简介

##### STP 产生的原因

在二层交换网络中，一旦存在环路就会造成报文在环路内不断循环和增生，产生广播风暴，从而占用所有有效带宽，使网络变得不可用。

这种环境下 STP 协议应运而生，IEEE 于 1998 年发布的 802.1D 标准定义了 STP (Spanning Tree Protocol)。

##### STP 工作过程

首先进行根桥的选举。选举的依据是网桥优先级和网桥 MAC 地址组合成的桥 ID，桥 ID 最小的网桥将成为网络中的根桥，它的所有端口都连接到下游桥，所以端口角色都成为指定端口。接下来，连接根桥的下游网桥将各自选择一条“最粗壮”的树枝作为到根桥的路径，相应端口的角色就成为根端口。循环这个过程到网络的边缘，指定端口和根端口确定之后一棵树就生成了。生成树经过一段时间（默认值是 30 秒左右）稳定之后，指定端口和根端口进入转发状态，其他端口进入阻塞状态。STP BPDUs 会定时从各个网桥的指定端口发出，以维护链路的状态。如果网络拓扑发生变化，生成树就会重新计算，端口状态也会随之改变。这就是生成树的基本原理。

### STP 的缺点

随着应用的深入和网络技术的发展，STP 的缺点在应用中也暴露了出来。STP 协议的缺陷主要表现在收敛速度上。

当拓扑发生变化，新的配置消息要经过一定的时延才能传播到整个网络，这个时延称为 Forward Delay，协议默认值是 15 秒。在所有网桥收到这个变化的消息之前，若旧拓扑结构中处于转发的端口还没有发现自己应该在新的拓扑中停止转发，则可能存在临时环路。为了解决临时环路的问题，STP 使用了一种定时器策略，即在端口从阻塞状态到转发状态中间加上一个只学习 MAC 地址但不参与转发的中间状态，两次状态切换的时间长度都是 Forward Delay，这样就可以保证在拓扑变化的时候不会产生临时环路。但是，这个看似良好的解决方案实际上带来的却是至少两倍 Forward Delay 的收敛时间，这在某些实时业务（如音视频）中是不能接受的。

## 8.2.2 RSTP 简介

### RSTP 的优点

为了解决 STP 协议的收敛速度缺陷，2001 年 IEEE 定义了基于 IEEE 802.1w 标准的快速生成树协议 RSTP。RSTP 协议在 STP 协议基础上做了三点重要改进，加快了收敛速度（最快可在 1 秒以内）：

- 为根端口和指定端口设置了快速切换用的替换端口（Alternate Port）和备份端口（Backup Port）两种角色。当根端口失效的情况下，替换端口就会快速转换为新的根端口并无时延地进入转发状态；当指定端口失效的情况下，备份端口就会快速转换为新的指定端口并无时延地进入转发状态。
- 在只连接了两个交换端口的点对点链路中，指定端口只需与下游网桥进行一次握手就可以无时延地进入转发状态。如果是连接了三个以上网桥的共享链路，下游网桥

是不会响应上游指定端口发出的握手请求的，只能等待两倍 Forward Delay 时间进入转发状态。

- 直接与终端相连而不与其他网桥相连的端口定义为边缘端口（Edge Port）。边缘端口可以直接进入转发状态，不需要任何延时。由于网桥无法知道端口是否是直接与终端相连，所以需要人工配置。

### RSTP 的缺点

RSTP 协议相对于 STP 协议的确有很多改进，并且向下兼容 STP 协议，可以混合组网。但是，RSTP 和 STP 一样同属于单生成树 SST（Single Spanning Tree），有它自身的诸多缺陷，主要表现在三个方面：

- 由于整个交换网络只有一棵生成树，在网络规模比较大的时候会导致较长的收敛时间。
- 因为 RSTP 是单生成树协议，所有 VLAN 共享一棵生成树，为了保证 VLAN 内部可以正常通信，网络内每个 VLAN 都必须沿着生成树的路径方向连续分布，否则将会出现有的 VLAN 由于内部链路被阻塞而被分隔开，从而导致 VLAN 内部无法通信的问题。
- 当某条链路被阻塞后将不承载任何流量，无法实现负载均衡，造成了带宽的极大浪费。

这些缺陷都是单生成树无法克服的，于是支持 VLAN 的多生成树协议 MSTP 出现了。

## 8.2.3 MSTP 简介

### MSTP 的优点

多生成树协议 MSTP 是 IEEE 于 2002 年发布的 802.1s 标准中定义的一种新型生成树协议，相对于 STP 和 RSTP，优势非常明显。MSTP 的特点如下：

- MSTP 引入“域”的概念，把一个交换网络划分成多个域。每个域内形成多棵生成树，生成树之间彼此独立；在域间，MSTP 利用 CIST 保证全网络拓扑结构的无环路存在。
- MSTP 引入“实例（Instance）”的概念，将多个 VLAN 映射到一个实例中，以节省通信开销和资源占用率。MSTP 各个实例拓扑的计算是独立的（每个实例对应一棵单独的生成树），在这些实例上就可以实现 VLAN 数据的负载分担。
- MSTP 可以实现类似 RSTP 的端口状态快速迁移机制。

- MSTP 兼容 STP 和 RSTP。

### MSTP 的算法实现

#### 1. 初始状态

各台设备的各个端口在初始时会生成以自己为根桥的配置消息，总根和域根都是本桥 ID，外部根路径开销和内部根路径开销全为 0，指定桥 ID 为本桥 ID，指定端口为本端口，接收 BPDU 报文的端口为 0。

#### 2. 端口角色的选择原则

端口角色的选择原则如表 8-1 所示。

表 8-1 端口角色的选择原则

端口角色	选择原则
根端口	端口的端口优先级向量优于其指定优先级向量，且设备的根优先级向量取自该端口的根路径优先级向量
指定端口	端口的指定优先级向量优于其端口优先级向量
Master 端口	域边界根端口在 MSTI 实例上的角色就是 Master 端口
Alternate 端口	端口的端口优先级向量优于其指定优先级向量，但设备的根优先级向量不是取自该端口的根路径优先级向量
Backup 端口	端口的端口优先级向量优于其指定优先级向量，但端口优先级向量中的指定桥 ID 为本设备的桥 ID

#### 3. 优先级向量计算

所有网桥的 MSTP 角色都是通过报文中携带的信息计算出来的，其中报文中携带的最重要的信息就是生成树的优先级向量。下面将分别介绍一下 CIST 优先级向量和 MSTI 优先级向量的计算方法。

##### a) CIST 优先级向量计算

在 CIST 中优先级向量由总根、外部根路径开销、域根、内部根路径开销、指定桥 ID、指定端口 ID 和接收 BPDU 报文的端口 ID 组成。

为了方便后续描述，现做如下假设：

- 初始情况下，网桥 B 的端口 PB 对外发送报文中携带的信息如下：总根为 RB，外部根路径开销为 ERCB，域根为 RRB，内部根路径开销为 IRCB，指定桥 ID 为 B，指定端口 ID 为 PB，接收 BPDU 报文的端口 ID 为 PB；

- 网桥 B 的端口 PB 收到网桥 D 的端口 PD 发送过来的报文中携带的信息如下：总根为 RD，外部根路径开销为 ERCD，域根为 RRD，内部根路径开销为 IRCD，指定桥 ID 为 D，指定端口 ID 为 PD，接收 BPDU 报文的端口 ID 为 PB；
- 网桥 B 的端口 PB 收到的网桥 D 的端口 PD 发送过来的报文的优先级较高。

根据上述假设，下面将逐一介绍各优先级向量的计算方法。

#### (1) 消息优先级向量

消息优先级向量是 MSTP 协议报文中所携带的优先级向量。根据假设，网桥 B 的端口 PB 收到的消息优先级向量即为： $\{RD : ERCD : RRD : IRCD : D : PD : PB\}$ 。如果网桥 B 和网桥 D 不在同一个域，那么内部根路径开销对网桥 B 而言是毫无意义的，它会被赋值为 0。

#### (2) 端口优先级向量

在初始情况下，端口优先级向量的信息是以自己为根。端口 PB 的端口优先级向量为： $\{RB : ERCPB : RRB : IRCPB : B : PB : PB\}$ 。

端口优先级向量是随端口收到的消息优先级向量更新的：如果端口收到的消息优先级向量优于端口优先级向量，则将端口优先级向量更新为消息优先级向量；否则，端口优先级向量保持不变。由于端口 PB 收到的消息优先级向量优于端口优先级向量，所以端口优先级向量更新为： $\{RD : ERCD : RRD : IRCD : D : PD : PB\}$ 。

#### (3) 根路径优先级向量

根路径优先级向量由端口优先级向量计算所得：

- 如果端口的优先级向量来自不同域的网桥，根路径优先级向量的外部根路径开销为端口的路径开销和端口优先级向量的外部根路径开销之和，根路径优先级向量的域根为本桥的域根，内部根路径开销为 0。假设网桥 B 的端口 PB 的路径开销为 PCPB，则端口 PB 的根路径优先级向量为： $\{RD : ERCD + PCPB : B : 0 : D : PD : PB\}$ ；
- 如果端口优先级向量来自同一域的网桥，根路径优先级向量的内部路径开销为端口优先级向量的内部根路径开销和端口路径开销之和，计算后端口 PB 的根路径优先级向量为： $\{RD : ERCD : RRD : IRCD + PCPB : D : PD : PB\}$ 。

#### (4) 桥优先级向量



桥优先级向量中总根 ID、域根 ID 以及指定桥 ID 都是本桥 ID，外部根路径开销和内部根路径开销为 0，指定端口 ID 和接收端口 ID 也全为 0。网桥 B 的桥优先级向量为：{B： 0： B： 0： B： 0： 0}。

#### (5) 根优先级向量

根优先级向量是桥优先级向量和所有指定桥 ID 和本桥 ID 值不相同的根路径优先级向量的最优值，如果本桥优先级向量比较优，那么本桥就为 CIST 总根。假设网桥 B 的桥优先级向量最优，则网桥 B 的根优先级向量为：{B： 0： B： 0： B： 0： 0}。

#### (6) 指定优先级向量

端口的指定优先级向量由根优先级向量计算所得，将根优先级向量的指定桥 ID 替换为本桥 ID，指定端口 ID 替换为自己的端口 ID。网桥 B 的端口 PB 的指定优先级向量为：{B： 0： B： 0： B： PB： 0}。

#### b) MSTI 优先级向量计算

MSTI 的各优先级向量计算的规则和 CIST 优先级向量计算规则是基本一致的，存在两点区别：

- MSTI 优先级向量中没有总根和外部根路径开销，仅由域根、内部根路径开销、指定桥 ID、指定端口 ID 和接收 BPDU 报文的端口 ID 组成。
- MSTI 只处理来自同一域的消息优先级向量。

### 4. 角色选择过程

下面结合图 8-1 的组网对 CIST 实例的计算过程进行简要说明。假设，网桥的优先级为 SC9600 A 优于 SC9600 B，SC9600 B 优于 SC9600 C，4、5、10 分别为链路的路径开销。SC9600 A 和 SC9600 B 属于同一域，SC9600 C 单独一个域。

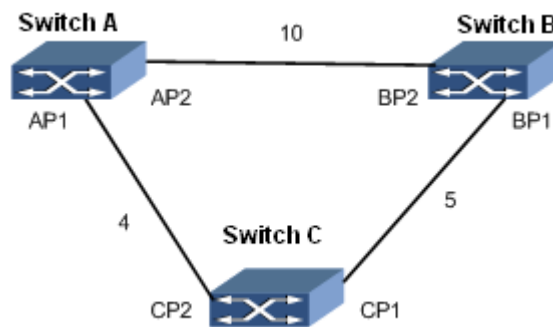


图 8-1 MSTP 算法计算过程组网图

图 8-1 中各设备的初始情况下对外发送的报文中携带的消息优先级向量如表 8-2 所示。

表 8-2 各台设备的初始状态

设备	端口	报文中的消息优先级向量
Switch A	AP1	{A:0:A:0:A:AP1:0}
	AP2	{A:0:A:0:A:AP2:0}
Switch B	BP1	{B:0:B:0:B:BP1:0}
	BP2	{B:0:B:0:B:BP2:0}
Switch C	CP1	{C:0:C:0:C:CP2:0}
	CP2	{C:0:C:0:C:CP2:0}

设备各端口的端口优先级向量与消息优先级向量在初始情况下是保持一致的。

在初始情况下各设备的端口都会被计算为指定端口且对外发送以自己为根桥的消息优先级向量。

a) Switch A 的角色选择过程

Switch A 的端口 AP1 和端口 AP2 会分别收到来自 Switch B 和 Switch C 的报文, Switch A 会将端口 AP1 以及 AP2 的端口优先级向量和收到的来自其它交换机的消息优先级向量进行比较, 由于 AP1 和 AP2 的端口优先级向量优于报文中携带的消息优先级向量, 端口 AP1 和 AP2 端口角色不变仍为指定端口, 设备 Switch A 为总根且为 Switch A 和 Switch B 所在域的域根。此后端口定时对外传播以自己为根的消息。

b) Switch B 的角色选择过程

Switch B 的端口 BP1 收到来自 Switch C 的端口 CP1 的报文后, 将消息优先级向量和端口优先级向量比较, 由于端口优先级向量优于消息优先级向量, 端口角色不更新。

Switch B 的端口 BP2 收到来自 Switch A 的端口 AP2 的报文后, 处理过程如下:

- (1) 将端口的消息优先级向量和端口优先级向量进行比较。由于端口的消息优先级向量优于端口优先级向量，将端口的端口优先级向量更新为消息优先级向量 {A:0:A:0:A:AP2:BP2};
- (2) 计算端口的根路径优先级向量。Switch A 和 Switch B 在同一域内，端口的根路径优先级向量为 {A:0:A:10:A:AP2:BP2};
- (3) 计算 Switch B 的根优先级向量。只有端口 BP2 的根路径优先级向量是来自其它设备，由于端口 BP2 的根路径优先级向量优于 Switch B 的桥优先级向量，Switch B 的根优先级向量为 {A:0:A:10:A:AP2:BP2};
- (4) 指定优先级向量计算。端口 BP1 的指定优先级向量为 {A:0:A:10:B:BP1:BP2}，端口 BP2 的指定优先级向量为 {A:0:A:10:B:BP2:BP2}。

端口角色的确定：将端口 BP1 和 BP2 的指定优先级向量和端口优先级向量进行比较，由于 BP1 的指定优先级向量优于端口优先级向量，则 BP1 角色为指定端口，定时对外发送以 Switch A 为总根和域根的指定优先级向量 {A:0:A:10:B:BP1:BP2}; 由于 BP2 的端口优先级向量优于指定优先级向量、且根优先级向量取自端口 BP2 的根路径优先级向量，则 BP2 角色为根端口。

#### c) Switch C 的角色选择过程

Switch C 的端口 CP1 收到来自 Switch B 未更新前的消息优先级向量 {B:0:B:0:B:BP1:CP1}，端口 CP2 收到来自 Switch A 的消息优先级向量 {A:0:A:0:A:AP1:CP2}，经过分别比较，CP1 和 CP2 的消息优先级向量均优于端口优先级向量，因此分别更新 CP1 和 CP2 的端口优先级向量为 {B:0:B:0:B:BP1:CP1} 和 {A:0:A:0:A:AP1:CP2}。由于 Switch C 与 Switch A 和 Switch B 不在同一域，端口 CP1 的根路径优先级向量为 {B:5:C:0:B:BP1:CP1}，端口 CP2 的根路径优先级向量为 {A:4:C:0:A:AP1:CP2}，CP2 的根路径优先级向量优于 CP1 的根路径优先级向量，则根优先级向量为 {A:4:C:0:A:AP1:CP2}。端口 CP1 和 CP2 的指定优先级向量分别为 {A:4:C:0:C:CP1:CP2} 和 {A:4:C:0:C:CP2:CP2}，端口 CP1 被计算为指定端口，CP2 被计算为根端口。

Switch C 的端口 CP1 收到来自 BP1 更新后的消息优先级向量 {A:0:A:10:B:BP1:CP1} 后，经过比较 CP1 的消息优先级向量优于端口优先级向量，更新端口优先级向量为 {A:0:A:10:B:BP1:CP1}，端口 CP1 计算后的根路径优先级向量为 {A:5:C:0:B:BP1:CP1}。由于端口 CP2 收到的消息优先级向量没有变化，根据前面的计算，端口 CP2 的根路径优先级向量保持为 {A:4:C:0:A:AP1:CP2}，CP2 的根路径优先级向量优于 CP1 的根路径优先级向量，则根优先级向量为 {A:4:C:0:A:AP1:CP2}。端口 CP1 和 CP2 的指定优先级

向量分别为{A:4:C:0:C:CP1:CP2}和{A:4:C:0:C:CP2:CP2}。CP1 的端口优先级向量优于其指定优先级向量、但根优先级向量不是取自端口 CP1 的根路径优先级向量，故 CP1 角色为 Alternate 端口。CP2 仍为根端口。

### 5. 计算结果

设备和端口的角色确定之后，整个树形拓扑就建立完毕了。经过上述计算后的流量转发线路如图 8-2所示。

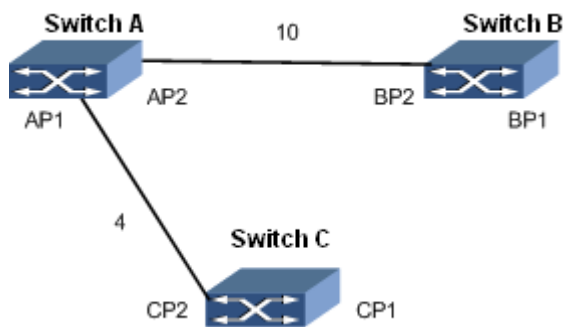


图 8-2 计算后流量转发线路

## 8.2.4 配置设备加入指定的 MST 域

### 背景信息

只要以下配置相同，两台交换机就属于同一个域：

- MST 域名
- MSTI 和 VLAN 的映射关系
- MST 域的修订级别

在配置交换机加入指定 MST 域之前，需完成端口物理特性及端口 VLAN 特性的配置。

### 目的

本节介绍交换机加入 MST 域的配置方法。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置交换机生成树的工作模式	1. 执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>stp</b> 进入 STP 配置视图；

目的	步骤
	<ol style="list-style-type: none"> <li>3. 执行命令 <b>stp mode { stp   rstp   mstp   default }</b> 用来设置交换机生成树的工作模式;</li> <li>4. 结束。</li> </ol>
配置 MST 域	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>stp</b> 进入 STP 配置视图;</li> <li>3. 执行命令 <b>stp config-name string</b> 用来设置生成树域名;</li> <li>4. 执行命令 <b>stp instance instance-id vlan vlan-list</b> 用来设置 MSTI 应用的 VLAN;</li> <li>5. 执行命令 <b>stp revision-level { range   default }</b> 用来设置设备 MSTP 修订级别;</li> <li>6. 结束。</li> </ol>
配置是否使能端口生成树功能	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b> 或 <b>interface eth-trunk trunk-number</b> 进入接口配置视图;</li> <li>3. 执行命令 <b>stp { enable   disable }</b> 用来使能或去使能端口生成树功能;</li> <li>4. 结束。</li> </ol>
(可选) 配置交换机在指定 MSTI 中的优先级	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>stp</b> 进入 STP 配置视图;</li> <li>3. 执行命令 <b>stp instance instance-id priority { priority   default }</b> 用来设置交换机在指定 MSTI 中的优先级;</li> <li>4. 结束。</li> </ol>
(可选) 配置 CIST 实例 0 的优先级	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>stp</b> 进入 STP 配置视图;</li> <li>3. 执行命令 <b>stp priority { priority   default }</b> 用来设置 CIST 实例 0 的优先级;</li> <li>4. 结束。</li> </ol>
(可选) 配置端口优先级	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b> 或 <b>interface eth-trunk trunk-number</b> 进入接口配置视图;</li> <li>3. 执行命令 <b>stp priority { priority   default }</b> 用来设置端口优先级;</li> <li>4. 结束。</li> </ol>

附表:

参数	说明	取值
string	指定生成树域名	字符串形式, 不支持空格
instance-id	指定生成树实例 ID	整数形式, 取值范围是 1~63
range	指定生成树修订级别	整数形式, 取值范围是 0~65535
priority	指定 SC9600 的优先级, 优先级值越小, 则优先级越高	整数形式, 取值范围是 0~61440, 步长为 4096, 即可以配置 16 个优先级取值, 如 0、4096、8192 等

参数	说明	取值
customer	指定网桥类型为客户模式	-
provider	指定网桥类型为运营商模式	-
priority	指定接口的优先级	整数形式，取值范围是 0~240

## 8.2.5 配置 MSTP 参数

### 背景信息

在调整交换机的 MSTP 参数前，需要完成以下配置任务：

- 配置端口的物理特性
- 配置端口加入的 VLAN
- 配置交换机加入指定 MST 域

### 目的

本节介绍调整部分 MSTP 参数的配置方法。

在一些特定的网络环境里，可以通过调整部分交换机的 MSTP 参数以达到最佳效果。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置生成树转发时延	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>stp</b> 进入 STP 配置视图；</li> <li>3. 执行命令 <b>stp forward-delay { forward-delay   default }</b> 用来设置生成树转发时延；</li> <li>4. 结束。</li> </ol>
配置协议发送 hello 报文间隔时间	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>stp</b> 进入 STP 配置视图；</li> <li>3. 执行命令 <b>stp hello-time { hello-interval   default }</b> 用来设置协议发送 hello 报文间隔时间；</li> <li>4. 结束。</li> </ol>
配置交换机生成树的最大老化时间	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>stp</b> 进入 STP 配置视图；</li> <li>3. 执行命令 <b>stp max-age { max-age   default }</b> 用来设置交换机生成树的最大老化时间；</li> <li>4. 结束。</li> </ol>
配置 MST 域内生成树最大跳数	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>stp</b> 进入 STP 配置视图；</li> </ol>

目的	步骤
	<ol style="list-style-type: none"> <li>3. 执行命令 <b>stp max-hop { max-hop   default }</b> 用来设置 MST 域内生成树最大跳数;</li> <li>4. 结束。</li> </ol>
配置是否为边缘端口	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b> 或 <b>interface eth-trunk trunk-number</b> 进入接口配置视图;</li> <li>3. 执行命令 <b>stp { enable   disable }</b> 用来使能或去使能端口生成树功能;</li> <li>4. 执行命令 <b>stp edge-port { enable   disable }</b> 用来使能或去使能接口为边缘端口;</li> <li>5. 结束。</li> </ol>
配置接口是否点到点管理	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b> 或 <b>interface eth-trunk trunk-number</b> 进入接口配置视图;</li> <li>3. 执行命令 <b>stp { enable   disable }</b> 用来使能或去使能端口生成树功能;</li> <li>4. 执行命令 <b>stp point-to-point { true   false }</b> 用来设置接口链路类型;</li> <li>5. 结束。</li> </ol>
配置当前接口在指定 MSTI 上的优先级	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b> 或 <b>interface eth-trunk trunk-number</b> 进入接口配置视图;</li> <li>3. 执行命令 <b>stp { enable   disable }</b> 用来使能或去使能端口生成树功能;</li> <li>4. 执行命令 <b>stp instance instance-id priority { priority   default }</b> 用来设置当前接口在指定 MSTI 上的优先级;</li> <li>5. 结束。</li> </ol>
配置当前接口在指定 MSTI(MST 实例) 上的管理路径开销	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b> 或 <b>interface eth-trunk trunk-number</b> 进入接口配置视图;</li> <li>3. 执行命令 <b>stp { enable   disable }</b> 用来使能或去使能端口生成树功能;</li> <li>4. 执行命令 <b>stp instance instance-id path-cost { path-cost   default }</b> 用来设置当前接口在指定 MSTI (MST 实例) 上的管理路径开销;</li> <li>5. 结束。</li> </ol>
配置生成树 Hello Time 周期内发包次数 (即发送的 BPDU 的个数)	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>stp</b> 进入 STP 配置视图;</li> <li>3. 执行命令 <b>stp transmit-limit { transmit-limit   default }</b> 用来设置生成树 Hello Time 周期内发包次数;</li> <li>4. 结束。</li> </ol>
配置接口在实例 0 上的管理路径开销值	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b> 或 <b>interface eth-trunk trunk-number</b> 进入接口配置视图;</li> <li>3. 执行命令 <b>stp { enable   disable }</b> 用来使能或去使能端口生成树功能;</li> <li>4. 执行命令 <b>stp path-cost { cost   default }</b> 用来设置接口在实例 0 上的</li> </ol>

目的	步骤
	管理路径开销值； 5. 结束。
配置 STP 端口路径开销计算的标准	1. 执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>stp</b> 进入 STP 配置视图； 3. 执行命令 <b>stp pathcost-standard { dot1t   dot1d-1998 }</b> 用来设置 STP 端口路径开销计算的标准； 4. 结束。
配置当前接口执行模式检查操作	1. 执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>interface { fastethernet   gigaethernet   xgigaethernet } interface-number</b> 或 <b>interface eth-trunk trunk-number</b> 进入接口配置视图； 3. 执行命令 <b>stp { enable   disable }</b> 用来使能或去使能端口生成树功能； 4. 执行命令 <b>stp mcheck</b> 用来设置当前接口执行模式检查操作； 5. 结束。
配置生成树协议转换周期	1. 执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>stp</b> 进入 STP 配置视图； 3. 执行命令 <b>stp migration-time { migration-time   default }</b> 用来设置生成树协议转换周期； 4. 结束。
配置是否使能点到点链路检测开关	1. 执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>stp</b> 进入 STP 配置视图； 3. 执行命令 <b>stp link-detection { enable   disable }</b> 用来使能或去使能点到点链路检测开关； 4. 结束。
配置是否使能生成树 Trap 告警功能	1. 执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>stp</b> 进入 STP 配置视图； 3. 执行命令 <b>stp trap { enable   disable }</b> 用来使能或去使能生成树 Trap 告警功能； 4. 结束。

附表：

参数	说明	取值
forward-delay	指定生成树转发时延	整数形式，取值范围是 4~30，单位：秒
default	表示默认值	15 秒
hello-interval	指定生成树 hello 报文间隔时间	整数形式，取值范围是 1~10，单位：秒
default	表示默认间隔时间	2 秒
max-age	指定生成树最大老化时间	整数形式，取值范围是 6~40，单位：秒
default	表示默认最大老化时间	20 秒
max-hop	指定生成树最大跳数	整数形式，取值范围是 4~30，单位：跳
default	指定默认最大跳数值	20 跳
instance-id	指定生成树实例 ID	整数形式，取值范围是 1~63



参数	说明	取值
priority	指定接口的优先级	整数形式，取值范围是 0~240，步长为 16
default	指定为缺省值	128
path-cost	指定的端口开销	整数形式，取值范围是 0~200000
default	指定为缺省值	取值为 0
transmit-limit	指定生成树 hello 周期发包次数	整数形式，取值范围是 1~255，单位：次
default	指定为缺省值	3 次
cost	指定接口路径开销	整数，取值范围是 0~200000
default	指定为缺省值	0
{ dot1t   dot1d-1998 }	指定 STP 端口路径开销计算的标准 其中，dot1t 表示 IEEE 802.1t 标准方法，dot1d-1998 表示 IEEE 802.1D 标准方法。	-
migration-time	指定生成树协议转换周期	整数形式，取值范围是 1~10，单位：秒
default	指定为缺省值	3 秒
interface-number	指定作为观察端口以太网接口号	SC9600 系列交换机支持以下 3 种型号的接口配置范围： SC9603 : 取值范围是 <1-3>/<0-4>/<1-48> SC9608 : 取值范围是 <1-8>/<0-4>/<1-48> SC9612 : 取值范围是 <1-12>/<0-4>/<1-48>
trunk-number	指定 trunk 接口号	整数形式，取值范围是 1~128

## 8.2.6 配置 MSTP 保护功能

### 背景信息

- BPDU 保护

对于接入层设备，接入端口一般直接与用户终端（如 PC 机）或文件服务器相连，此时可以设置接入端口为边缘端口以实现这些端口的快速迁移。正常情况下，边缘端口不会收到生成树协议的配置消息（BPDU 报文），但是，如果有人伪造配置消息，恶意攻击交换机，当边缘端口接收到配置消息时，系统会自动将这些端口设置为非边缘端口，重新进行生成树的计算，这将引起网络拓扑的震荡。BPDU 保护功能可以防止这种网络攻击。

- 环路保护

在交换机上，根端口和其他阻塞端口状态是依靠不断接收来自上游交换机的 **BPDU** 来维持的。当由于链路拥塞或者单向链路故障导致这些端口收不到来自上游交换机的 **BPDU** 时，此时交换机会重新选择根端口。原先的根端口会转变为指定端口，而原先的阻塞端口会迁移到转发状态，从而造成交换网络中可能产生环路。

环路保护功能会抑制这种环路的产生。在启动了环路保护功能后，如果根端口收不到来自上游的 **BPDU** 时，根端口会被设置进入阻塞状态；而阻塞端口则会一直保持在阻塞状态，不转发报文，从而不会在网络中形成环路。

#### ● Root 保护

根节点保护功能可以用来防止来历不明的 **BPDU** 使网络拓扑变化。

由于维护人员的错误配置或网络中的恶意攻击，网络中的合法根桥有可能会收到优先级更高的配置消息，这样当前根桥会失去根桥的地位，引起网络拓扑结构的错误变动。假设原来的流量是经过高速链路转发的，这种不合法的变动，会导致原来通过高速链路的流量被牵引到低速链路上，导致网络拥塞。**Root** 保护功能可以防止这种情况的发生。

对于设置了 **Root** 保护功能的端口，端口角色只能保持为指定端口。一旦这种端口上收到了优先级高的配置消息，这些端口的状态将被设置为侦听状态，不再转发报文（相当于将此端口相连的链路断开）。当在足够长的时间内没有收到更优的配置消息时，端口会恢复原来的状态。

#### ● TC 保护

交换机在接收到 **TC-BPDU** 报文后，会执行 **MAC** 地址表项和 **ARP** 表项的删除操作。如果有人伪造 **TC-BPDU** 报文恶意攻击交换机时，交换机短时间内会收到很多 **TC-BPD** 报文，频繁的删除操作会给设备造成很大的负担，给网络的稳定带来很大隐患。

启用防 **TC-BPDU** 报文攻击功能后，在单位时间内，**MSTP** 进程处理 **TC** 类型 **BPDU** 报文的次数可配置。如果在单位时间内，**MSTP** 进程在收到 **TC** 类型 **BPDU** 报文数量大于配置的阈值，那么 **MSTP** 进程只会处理阈值指定的次数。对于其他超出阈值的 **TC** 类型 **BPDU** 报文，定时器到期后，**MSTP** 进程只对其统一处理一次。这样可以避免频繁的删除 **MAC** 地址表项和 **ARP** 表项，从而达到保护交换机的目的。

#### 目的

当用户需要配置 **MSTP** 保护功能时，可以使用本节操作。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置交换机 BPDU 保护功能	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>stp</b> 进入 STP 配置视图；</li> <li>3. 执行命令 <b>stp bpdu-guard { enable   disable }</b> 设置交换机 BPDU 保护功能；</li> <li>4. 结束。</li> </ol>
开放 BPDU 保护阻塞端口	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface { fastethernet   gigasethernet   xgigasethernet } interface-number</b> 或 <b>interface eth-trunk trunk-number</b> 进入接口配置视图；</li> <li>3. 执行命令 <b>stp bpdu-guard-forward</b> 用来开放 BPDU 保护阻塞端口；</li> <li>4. 结束。</li> </ol>
配置交换机环路保护功能	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>stp</b> 进入 STP 配置视图；</li> <li>3. 执行命令 <b>stp loop-protection { enable   disable }</b> 设置交换机环路保护功能；</li> <li>4. 结束。</li> </ol>
配置交换机根保护功能	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>stp</b> 进入 STP 配置视图；</li> <li>3. 执行命令 <b>stp root-protection { enable   disable }</b> 设置交换机根保护功能；</li> <li>4. 结束。</li> </ol>
配置指定 MSTI 的根节点保护功能	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>stp</b> 进入 STP 配置视图；</li> <li>3. 执行命令 <b>stp instance instance-id root-protection { enable   disable }</b> 用来设置指定 MSTI 的根节点保护功能；</li> <li>4. 结束。</li> </ol>
配置交换机 TC 保护功能	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>stp</b> 进入 STP 配置视图；</li> <li>3. 执行命令 <b>stp tc-protection { enable   disable }</b> 设置交换机 TC 保护功能；</li> <li>4. 执行命令 <b>stp tc-hold-off { time   default }</b> 设置拓扑改变延迟/抑制时间；</li> <li>5. 结束。</li> </ol>

附表：

参数	说明	取值
time	指定延迟/抑制的时间	整数形式，取值范围是 4-30，单位：秒
default	指定为缺省值	10 秒
instance-id	生成树实例 ID	整数形式，取值范围是 1-63

## 8.2.7 维护及调试

### 目的

当 MSTP 功能不正常，需要进行查看、调试或定位问题时，可以使用本小节操作。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
打开调试生成树功能	<ol style="list-style-type: none"> <li>1. 保持当前特权用户视图；</li> <li>2. 执行命令 <code>debug stp { error   statemachine   timer   in   out   packet   protocol   event   all }</code> 打开生成树调试开关；</li> <li>3. 结束。</li> </ol>
关闭调试生成树功能	<ol style="list-style-type: none"> <li>1. 保持当前特权用户视图；</li> <li>2. 执行命令 <code>no debug stp { error   statemachine   timer   in   out   packet   protocol   event   all }</code> 关闭生成树调试开关；</li> <li>3. 结束。</li> </ol>
查看交换机生成树协议的配置信息	<ol style="list-style-type: none"> <li>1. 执行命令 <code>disable</code> 退出到普通用户视图，或执行命令 <code>configure</code> 进入全局配置视图，或执行命令 <code>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</code> 或 <code>interface eth-trunk trunk-number</code> 进入接口配置视图，或执行命令 <code>stp</code> 进入 STP 配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <code>show stp</code> 显示交换机生成树协议的配置信息；</li> <li>3. 结束。</li> </ol>
查看交换机生成树协议的配置文件信息	<ol style="list-style-type: none"> <li>1. 执行命令 <code>disable</code> 退出到普通用户视图，或执行命令 <code>configure</code> 进入全局配置视图，或执行命令 <code>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</code> 或 <code>interface eth-trunk trunk-number</code> 进入接口配置视图，或执行命令 <code>stp</code> 进入 STP 配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <code>show stp config</code> 显示交换机生成树协议的配置文件信息；</li> <li>3. 结束。</li> </ol>
查看交换机生成树协议的相关信息	<ol style="list-style-type: none"> <li>1. 执行命令 <code>disable</code> 退出到普通用户视图，或执行命令 <code>configure</code> 进入全局配置视图，或执行命令 <code>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</code> 或 <code>interface eth-trunk trunk-number</code> 进入接口配置视图，或执行命令 <code>stp</code> 进入 STP 配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <code>show stp information</code> 显示交换机生成树协议的相关信息；</li> <li>3. 结束。</li> </ol>
查看交换机生成树协议实例在全部接口或指定接口的配置信息	<ol style="list-style-type: none"> <li>1. 执行命令 <code>disable</code> 退出到普通用户视图，或执行命令 <code>configure</code> 进入全局配置视图，或执行命令 <code>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</code> 或 <code>interface eth-trunk trunk-number</code> 进入接口配置视图，或执行命令 <code>stp</code> 进入 STP 配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <code>show stp instance instance-id interface</code> 显示交换机生成树协议实例在全部接口的配置信息</li> </ol>

目的	步骤
	或执行命令 <code>show stp instance instance-id interface { fastethernet   gigaethernet   xgigaethernet } interface-number</code> 显示交换机生成树协议实例指定接口的配置信息； 3. 结束。
查看交换机全部接口生成树协议的配置信息	1. 执行命令 <code>disable</code> 退出到普通用户视图，或执行命令 <code>configure</code> 进入全局配置视图，或执行命令 <code>interface { fastethernet   gigaethernet   xgigaethernet } interface-number</code> 或 <code>interface eth-trunk trunk-number</code> 进入接口配置视图，或执行命令 <code>stp</code> 进入 STP 配置视图，或不执行任何命令保持当前特权用户视图； 2. 执行命令 <code>show stp interface</code> 显示交换机全部接口生成树协议的配置信息； 3. 结束。
查看交换机指定接口的生成树协议的相关配置信息	1. 执行命令 <code>disable</code> 退出到普通用户视图，或执行命令 <code>configure</code> 进入全局配置视图，或执行命令 <code>interface { fastethernet   gigaethernet   xgigaethernet } interface-number</code> 或 <code>interface eth-trunk trunk-number</code> 进入接口配置视图，或执行命令 <code>stp</code> 进入 STP 配置视图，或不执行任何命令保持当前特权用户视图； 2. 执行命令 <code>show stp interface { fastethernet   gigaethernet   xgigaethernet } interface-number</code> 或执行命令 <code>show stp interface eth-trunk trunk-number</code> 显示交换机指定接口的生成树协议的相关配置信息； 3. 结束。

附表：

参数	说明	取值
interface-number	指定作为观察端口以太网接口号	SC9600 系列交换机支持以下 3 种型号的接口配置范围： SC9603 : 取值范围是 <1-3>/<0-4>/<1-48> SC9608 : 取值范围是 <1-8>/<0-4>/<1-48> SC9612 : 取值范围是 <1-12>/<0-4>/<1-48>
trunk-number	指定 trunk 接口号	整数形式，取值范围是 1~128
instance-id	指定 MSTI 的编号	整数形式，取值范围是 1~63

### 8.2.8 配置举例

#### 组网要求

现有四台支持 MSTP 协议的 SC9600 系列交换机，分别为 SC9600A、SC9600B、SC9600C、SC9600D。按照如下组网示意图连接，配置 MSTP 基本功能：

- SC9600A 和 SC9600C 划分在同一个域内，域名为 Domain1 并创建实例 1。

- SC9600B 和 SC9600D 划分在另一个域内，域名为 Domain2 并创建实例 1。
- SC9600A 为 CIST 总根。
- Domain1 内，SC9600A 为 CIST 域根，为实例 1 的域根。且在 SC9600A 的 ge1/0/1 和 ge1/0/2 端口上配置根保护功能。
- Domain2 内，SC9600B 为 CIST 域根，SC9600D 为实例 1 的域根。
- SC9600C 和 SC9600D 的 ge1/0/1 端口配置为边缘端口，同时应用 BPDU 保护功能。

### 组网图

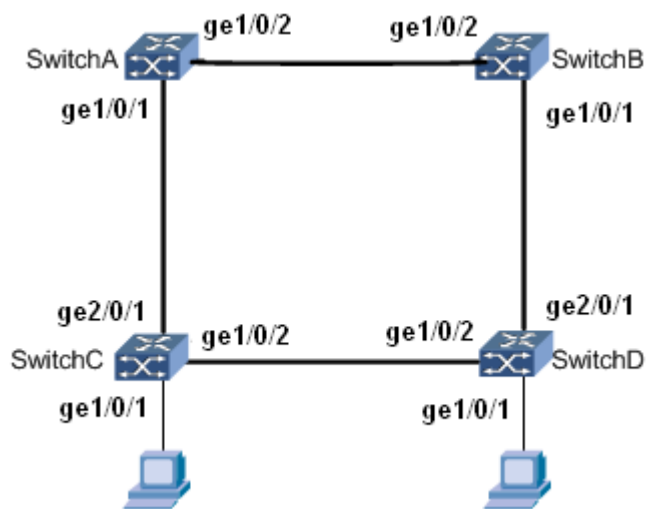


图 8-3 MSTP 组网示意图

### 配置步骤

1、配置 SC9600A。

# 配置 SC9600A 加入域 Domain1。

```
SC9600A#configure
```

```
    %Enter configuration commands.End with Ctrl+Z or command "quit" & "end"
```

```
SC9600A(config)#stp
```

```
SC9600A(config-stp)#stp mode mstp
```

```
SC9600A(config-stp)#stp config-name Domain1
```

```
SC9600A(config-stp)#stp instance 1 vlan 1-10
```

```
SC9600A(config-stp)#stp revision-level 1
```

# 配置 SC9600A 在实例 0 中的优先级为 0 以保证 SC9600A 作为 CIST 的总根。

```
SC9600A(config-stp)#stp priority 0
```

# 配置 SC9600A 在实例 1 中的优先级为 0，保证 SC9600A 作为实例 1 的域根。

```
SC9600A(config-stp)#stp instance 1 priority 0
```

# 创建 VLAN 2 到 20，并将 SC9600A 的端口 ge1/0/1 和 ge1/0/2 分别加入 1 到 20，使能端口生成树功能，启动端口根保护功能。

```
SC9600A(config)#Vlan 2-20
```

```
SC9600A(config)#interface gigaethernet1/0/1
```

```
SC9600A(config-ge1/0/1)#port link-type trunk
```

```
SC9600A(config-ge1/0/1)#port trunk allow-pass vlan 1-20
```

```
SC9600A(config-ge1/0/1)#stp enable
```

```
SC9600A(config-ge1/0/1)#quit
```

```
SC9600A(config)#stp
```

```
SC9600A(config-stp)#stp instance 1 root-protection enable
```

```
SC9600A(config-stp)#stp root-protection enable
```

```
SC9600A(config)#interface gigaethernet1/0/2
```

```
SC9600A(config-ge1/0/2)#port link-type trunk
```

```
SC9600A(config-ge1/0/2)#port trunk allow-pass vlan 1-20
```

```
SC9600A(config-ge1/0/2)#stp enable
```

```
SC9600A(config-ge1/0/2)#quit
```

```
SC9600A(config)#stp
```

```
SC9600A(config-stp)#stp instance 1 root-protection enable
```

```
SC9600A(config-stp)#stp root-protection enable
```

```
SC9600A(config-stp)#
```

## 2、配置 SC9600B。

# 配置 SC9600B 加入域 Domain2。

```
SC9600B#configure
```

```
    %Enter configuration commands.End with Ctrl+Z or command "quit" & "end"
```

```
SC9600B(config)#stp
```

```
SC9600B(config-stp)#stp mode mstp
```

```
SC9600B(config-stp)#stp config-name Domain2
```

```
SC9600B(config-stp)#stp instance 1 vlan 1-10
```

```
SC9600B(config-stp)#stp revision-level 2
```

# 配置 SC9600B 在实例 0 中的优先级为 4096 以保证 SC9600B 作为 CIST 的总根。

```
SC9600B(config-stp)#stp priority 4096
```

# 创建 VLAN 2 到 20，并将 SC9600B 的端口 ge1/0/1 和 ge1/0/2 分别加入 1 到 20，使能端口生成树功能，启动端口根保护功能。

```
SC9600B(config)#Vlan 2-20
```

```
SC9600B(config)#interface gigaethernet1/0/1
```

```
SC9600B(config-ge1/0/1)#port link-type trunk
```

```
SC9600B(config-ge1/0/1)#port trunk allow-pass vlan 1-20
```

```
SC9600B(config-ge1/0/1)#stp enable
```

```
SC9600B(config-ge1/0/1)#quit
```

```
SC9600B(config)#interface gigaethernet1/0/2
```

```
SC9600B(config-ge1/0/2)#port link-type trunk
```

```
SC9600B(config-ge1/0/2)#port trunk allow-pass vlan 1-20
```

```
SC9600B(config-ge1/0/2)#stp enable
```

```
SC9600B(config-ge1/0/2)#quit
```

```
SC9600B(config)#
```

3、配置 SC9600C。

# 配置 SC9600C 加入域 Domain1。

```
SC9600C#configure
```

```
  %Enter configuration commands.End with Ctrl+Z or command "quit" & "end"
```

```
SC9600C(config)#stp
```

```
SC9600C(config-stp)#stp mode mstp
```

```
SC9600C(config-stp)#stp config-name Domain1
```

```
SC9600C(config-stp)#stp instance 1 vlan 1-10
```

```
SC9600C(config-stp)#stp revision-level 1
```

# 启动 BPDU 保护功能。

```
SC9600C(config-stp)#stp bpdu-guard enable
```

# 创建 VLAN 2 到 20，并将 SC9600C 的端口 ge1/0/2 和 ge2/0/1 分别加入 1 到 20，使能端口生成树功能，将端口 ge1/1 配置为边缘端口。

```
SC9600C(config)#Vlan 2-20
```

```
SC9600C(config)#interface gigaethernet2/0/1
```

```
SC9600C(config-ge2/0/1)#port link-type trunk
```

```
SC9600C(config-ge2/0/1)#port trunk allow-pass vlan 1-20
```

```
SC9600C(config-ge2/0/1)#stp enable
```

```
SC9600C(config-ge2/0/1)#quit
```

```
SC9600C(config)#interface gigaethernet1/0/2
```



```
SC9600C(config-ge1/0/2)#port link-type trunk
SC9600C(config-ge1/0/2)#port trunk allow-pass vlan 1-20
SC9600C(config-ge1/0/2)#stp enable
SC9600C(config-ge1/0/2)#quit
SC9600C(config)#interface gigabitEthernet1/0/1
SC9600C(config-ge1/0/1)#stp enable
SC9600C(config-ge1/0/1)#edged-port enable
SC9600C(config-ge1/0/1)#port hybrid pvid 20
SC9600C(config-ge1/0/1)#port hybrid vlan 20 untagged
SC9600C(config-ge1/0/1)#quit
SC9600C(config)#
```

#### 4、配置 SC9600D。

# 配置 SC9600D 加入域 Domain2。

```
SC9600D#configure
    %Enter configuration commands.End with Ctrl+Z or command "quit" & "end"
```

```
SC9600D(config)#stp
SC9600D(config-stp)#stp mode mstp
SC9600D(config-stp)#stp config-name Domain2
SC9600D(config-stp)#stp instance 1 vlan 1-10
SC9600D(config-stp)#stp revision-level 2
```

# 配置 SC9600D 在实例 1 中的优先级为 0，保证 SC9600D 作为实例 1 的域根。

```
SC9600D(config-stp)#stp instance 1 priority 0
```

# 启动 BPDU 保护功能。

```
SC9600D(config-stp)#stp bpdu-guard enable
```

# 创建 VLAN 2 到 20，并将 SC9600D 的端口 ge1/0/2 和 ge2/0/1 分别加入 1 到 20，使能端口生成树功能，将端口 ge1/0/1 配置为边缘端口。

```
SC9600D(config)#vlan 2-20
SC9600D(config)#interface gigabitEthernet2/0/1
SC9600D(config-ge2/0/1)#port link-type trunk
SC9600D(config-ge2/0/1)#port trunk allow-pass vlan 1-20
SC9600D(config-ge2/0/1)#stp enable
SC9600D(config-ge2/0/1)#quit
SC9600D(config)#interface gigabitEthernet1/0/2
SC9600D(config-ge1/0/2)#port link-type trunk
```

```
SC9600D(config-ge1/0/2)#port trunk allow-pass vlan 1-20
SC9600D(config-ge1/0/2)#stp enable
SC9600D(config-ge1/0/2)#quit
SC9600C(config)#interface gigaethernet1/0/1
SC9600C(config-ge1/0/1)#stp enable
SC9600C(config-ge1/0/1)#edged-port enable
SC9600C(config-ge1/0/1)#port hybrid pvid 10
SC9600C(config-ge1/0/1)#port hybrid vlan 10 untagged
SC9600C(config-ge1/0/1)#quit
SC9600C(config)#
```

## 8.3 RLINK 配置

### 8.3.1 RLINK 概述

#### RLINK 产生的背景

双上行组网是用于提供链路备份的常用组网方式，该组网一般通过生成树协议阻塞冗余链路，消除环路从而避免引起广播风暴。但是这种方案在性能上却不能达到用户需求，不适合对收敛时间有很高要求的组网环境。基于上述原因，我们提出了 RLINK 解决方案。

#### Resilient Link

Resilient Link 简称为 RLINK 即弹性链路。该解决方案是专门针对双上行组网实现主备链路的冗余备份及快速倒换。

#### Monitor Link

Monitor Link 简称为 Mlink, 是对 RLINK 进行补充而引入的一种接口联动方案, 使 RLINK 工作在更为安全和稳定的环境下。

RLINK 协议通过使用 MLINK 功能模块对上行链路进行监控，以达到同步上行链路和下行链路状态的目的。当上行链路接口出现故障后，Monitor Link 组会自动 shutdown 下行链路接口。当上行链路接口恢复后也会将下行链路接口恢复。

#### SC9600 支持的 RLINK 特性

- 链路冗余备份

为双上行组网环境下提供链路的冗余和备份功能。**RLINK** 能够实现在双上行组网的两条链路正常的情况下，只有一条处于转发状态，另一条处于阻塞状态，从而防止该组网环境下环路引起的广播风暴。

- 快速倒换

当主用链路发生故障后，流量会在毫秒级的时间内快速倒换到备用链路上，保证了数据的正常转发，避免大量丢包。

- 灵活组网

**RLINK** 协议提供了单点上联模式和双点上联模式两种运行模式，使用户可以根据不同的应用场景，选择合适的组网机制。

- 负载分担

**RLINK** 协议通过基于 **VLAN** 的分流保护，实现了负载分担的目的，即不同的 **VLAN** 流量通过不同路径转发。

- 上行链路监控

**RLINK** 协议中的联动功能 **MLINK**，能监控上上链路的变化，从而同步下行链路的状态，进一步减少流量的丢失。

- 配置简单、成本低

该方案为双上行组网量身定做，既保证了性能又简化了配置。

### 8.3.2 配置 Resilient Link 组功能

#### 背景信息



注意：

用户在使用 **RLINK** 功能时，请确保配置 **RLINK** 功能的接口没有使能 **MSTP** 功能。接口使能了 **STP**，**G8031**，**G8032**，**RER**，**ALB**，**ESR** 等协议，则不能使能 **RLink** 协议。

两条上行链路必须使用 **BFD** 或 **MLink** 对整条链路进行监控，否则可能造成主备端口无法正确识别真正出现故障的链路，致使链路正常后主备端口都为转发状态而成环的问题。

**RLINK** 组处于激活状态时，不能修改 **RLINK** 组模式。

#### 目的

使用本节操作配置 Resilient Link 组及其基本功能，实现双上行组网环境下的冗余链路备份及快速倒换功能。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
创建 RLINK 组并进入其配置视图	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>rlink group rlink-group-number</b> 创建 Resilient Link 组并进入其配置视图，若待创建的组已存在，则直接进入其配置视图；</li> <li>3. 结束。</li> </ol>
配置 RLINK 组模式为单点模式或双点模式	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>rlink group rlink-group-number</b> 进入已创建的 RLINK 配置视图；</li> <li>3. 执行命令 <b>type { single   double }</b> 配置 RLINK 组模式；</li> <li>4. 结束。</li> </ol>
配置 RLINK 组的主从接口	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface { fastethernet   gig Ethernet   xgig Ethernet } interface-number</b> 进入接口配置视图；</li> <li>3. 执行命令 <b>join rlink rlink-group-number { master   slave   sender }</b> 将端口加入 Resilient Link 组，并指定该接口为主端口或从端口或发包端口；</li> <li>4. 结束。</li> </ol>
(可选)配置 RLINK 协议包发送时所携带的 VLAN ID	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface { fastethernet   gig Ethernet   xgig Ethernet } interface-number</b> 进入接口配置视图；</li> <li>3. 执行命令 <b>rlink group rlink-group-number send-vlan vlan-id</b> 配置协议包携带的 VLAN ID；</li> <li>4. 结束。</li> </ol>
配置 RLINK 实例的保护 VLAN	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>rlink group rlink-group-number</b> 进入已创建的 RLINK 配置视图；</li> <li>3. 执行命令 <b>protect-vlan vlan-list</b> 配置 RLINK 实例的保护 VLAN；</li> <li>4. 结束。</li> </ol>

附表：

参数	说明	取值
interface-number	指定作为观察端口以太网接口号	SC9600 系列交换机支持以下 3 种型号的接口配置范围： SC9603 : 取值范围是 <1-3>/<0-4>/<1-48> SC9608 : 取值范围是

参数	说明	取值
		<1-8>/<0-4>/<1-48> SC9612 : 取值范围是 <1-12>/<0-4>/<1-48>
rlink-group-number	指定 RLINK 组号	整数形式, 取值范围是 1~16
master	指定为 RLINK 组中用于流量转发的主成员端口	-
slave	指定为 RLINK 组中用于流量转发的备用成员端口	-
sender	指定为 RLINK 组的发包端口	
group-list	镜像组列表序号	整数形式, 取值范围是 1~8, 形如: 1,3-5
vlan-list	指定保护 VLAN 列表	形如: 1,3,10-20, 整数形式, 取值范围是 1~4094
vlan-id	指定协议包所携带的 VLAN ID	整数形式, 取值范围是 1~4094

### 8.3.3 配置 Monitor Link 组功能

#### 背景信息



注意:

一个接口可以成为多个 MLink 组中的 Uplink 端口, 但是只能成为一个 MLink 组中的 downlink 端口。一个接口不能同时为 uplink 端口和 downlink 端口。

MLink 组配置规则如下:

- 一个接口可以同时是多个 MLink 组的 Uplink 端口
- 一个接口只能是一个组的 Downlink 端口
- 一个接口不能同时为 Uplink 和 Downlink 端口
- 接口已加入到 eth-trunk 中, 则不能再加入 MLINK 组

#### 目的

使用本节操作配置 Monitor Link 组及其基本功能, 实现接口联动功能。

#### 过程

根据不同目的, 执行相应步骤, 具体参见下表。

目的	步骤
创建 MLINK	1. 执行命令 <b>configure</b> 进入全局配置视图;

目的	步骤
组并进入其配置视图	2. 执行命令 <b>mink group mlink-group-number</b> 创建 Monitor Link 组并进入其配置视图，若待创建的组已存在，则直接进入其配置视图； 3. 结束。
配置 MLINK 组的上行和下行接口	1. 执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b> 进入接口配置视图； 3. 执行命令 <b>join mink mlink-group-number role { uplink   downlink }</b> 将端口加入 Monitor Link 组，并指定该接口所在链路为上行或下行链路； 4. 结束。
配置接口是否使能 MLINK 联动功能	1. 执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b> 进入接口配置视图； 3. 执行命令 <b>mink { enable   disable }</b> 使能或去使能接口 MLINK 联动功能； 4. 结束。

附表：

参数	说明	取值
mink-group-number	指定 MLINK 组号	整数形式，取值范围是 1~16
interface-number	指定作为观察端口以太网接口号	SC9600 系列交换机支持以下 3 种型号的接口配置范围： SC9603 : 取值范围是 <1-3>/<0-4>/<1-48> SC9608 : 取值范围是 <1-8>/<0-4>/<1-48> SC9612 : 取值范围是 <1-12>/<0-4>/<1-48>
uplink	指定为 MLINK 组的上行链路成员端口	-
downlink	指定为 MLINK 组的下行链路成员端口	-

### 8.3.4 配置 RLINK 其他功能参数

#### 背景信息

当 RLINK 组中主链路出现故障时，会自动切换到从链路。当原来的主链路故障恢复以后，一般情况下为了保持流量的稳定，主链路仍维持在阻塞状态而不会进行抢占。若需要将其恢复为主链路，可以通过以下两种方法实现：

- 使能 RLINK 组回切功能，在回切定时器超时会自动切换到主链路。
- 使用手动执行 Resilient Link 组主备链路的倒换命令，强制执行链路倒换。



注意：

对于手动链路倒换的处理，根据 RLink 组的类型不同，分为单点模式手动倒换和双点模式手动倒换。

成功实现主备倒换需要满足如下条件：

- Resilient Link 组中必须存在主从端口
- 链路状态必须允许强制倒换，即 master 和 slave 的链路状态都必须为 linkup 状态（如：master 为 up，slave 为 down，若想强制转换为 master 为 down，slave 为 up，则 slave 的链路必须为 linkup 状态）

### 目的

使用本节操作配置 Resilient Link 其他相关功能参数，该节的配置步骤可根据用户需求自行选用，前提必须先配置好 RLINK 组或 MLINK 组功能。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置手动执行 Resilient Link 组主备链路的倒换	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>rlink group rlink-group-number</b> 进入 RLINK 配置视图；</li> <li>3. 执行命令 <b>manual-change</b> 通过网管命令触发链路倒换；</li> <li>4. 结束。</li> </ol>
配置 Resilient Link 组接收对端协议包超时时间倍数值	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>rlink group rlink-group-number</b> 进入 RLINK 配置视图；</li> <li>3. 执行命令 <b>receive-timeout timeout-value</b> 配置协议包超时时间倍数值；</li> <li>4. 结束。</li> </ol>
配置使能或去使能 Resilient Link 组的回切功能	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>rlink group rlink-group-number</b> 进入 RLINK 配置视图；</li> <li>3. 执行命令 <b>reverse {enable   disable}</b> 使能或去使能 RLINK 组回切功能；</li> <li>4. 结束。</li> </ol>
配置 Resilient Link 组的回切时间	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>rlink group rlink-group-number</b> 进入 RLINK 配置视图；</li> <li>3. 执行命令 <b>reverse-time time-value</b> 配置 RLINK 组回切时间；</li> <li>4. 结束。</li> </ol>
配置协议包发间隔时间	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>rlink group rlink-group-number</b> 进入 RLINK 配置视图；</li> <li>3. 执行命令 <b>send-interval time-interval</b> 配置协议包发间隔时间；</li> <li>4. 结束。</li> </ol>
配置是否使能	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> </ol>

目的	步骤
RLINK 或 MLINK 上报告警功能	2. 执行命令 <b>rlink group rlink-group-number</b> 进入 RLINK 配置视图或执行命令 <b>m link group mlink-group-number</b> 进入 MLINK 配置视图； 3. 执行命令 <b>trap { enable   disable }</b> 使能或去使能 RLINK 或 MLINK 上报告警功能； 4. 结束。

附表：

参数	说明	取值
timeout-value	指定接收对端协议包超时时间倍数	整数形式，取值范围是 10~50
time-value	指定 Resilient Link 回切时间	整数形式，取值范围是 3~60，单位：秒
time-interval	指定发包间隔时间	整数形式，取值范围是 50~10000，单位：毫秒

### 8.3.5 维护及调试

#### 目的

当 RLINK 功能不正常，需要进行查看、调试或定位问题时，可以使用本小节操作。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
打开 RLINK 调试功能	1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gigasethernet   xgigasethernet } interface-number</b> 或 <b>interface eth-trunk trunk-number</b> 进入接口配置视图，或不执行任何命令保持当前特权用户视图； 2. 执行命令 <b>debug rlink { receive   send   timer   linkchange   all }</b> 打开双上行链路冗余备份功能调试开关； 3. 结束。
关闭 RLINK 调试功能	1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gigasethernet   xgigasethernet } interface-number</b> 或 <b>interface eth-trunk trunk-number</b> 进入接口配置视图，或不执行任何命令保持当前特权用户视图； 2. 执行命令 <b>no debug rlink { receive   send   timer   linkchange   all }</b> 关闭双上行链路冗余备份功能调试开关； 3. 结束。
打开 MLINK 调试功能	1. 执行命令 <b>disable</b> 退出到普通用户视图，或不执行任何命令保持当前特权用户视图； 2. 执行命令 <b>debug m link { linkchange   all }</b> 打开上行链路监控功能调试开关；



目的	步骤
	3. 结束。
关闭 MLINK 调试功能	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>no debug mlink { linkchange   all }</b> 打开上行链路监控功能调试开关；</li> <li>3. 结束。</li> </ol>
查看 RLINK 配置文件信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gigasethernet   xgigasethernet } interface-number</b> 或 <b>interface eth-trunk trunk-number</b> 进入接口配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show rlink config</b> 显示双上行链路冗余备份功能配置文件的信息；</li> <li>3. 结束。</li> </ol>
查看 RLINK 全部或指定组信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gigasethernet   xgigasethernet } interface-number</b> 或 <b>interface eth-trunk trunk-number</b> 进入接口配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show rlink group [ rlink-group-number ]</b> 显示指定的 RLINK 组或全部 RLINK 组的状态信息；</li> <li>3. 结束。</li> </ol>
查看 RLINK 所有或指定接口的配置信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gigasethernet   xgigasethernet } interface-number</b> 或 <b>interface eth-trunk trunk-number</b> 进入接口配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show rlink interface</b> 或 <b>show rlink interface { fastethernet   gigasethernet   xgigasethernet } interface-number</b> 显示指定的 RLINK 组或全部 RLINK 组的状态信息；</li> <li>3. 结束。</li> </ol>
查看 MLINK 配置文件信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gigasethernet   xgigasethernet } interface-number</b> 或 <b>interface eth-trunk trunk-number</b> 进入接口配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show mlink config</b> 显示上行链路监控功能配置文件的信息；</li> <li>3. 结束。</li> </ol>
查看 MLINK 全部或指定组信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gigasethernet   xgigasethernet } interface-number</b> 或 <b>interface eth-trunk trunk-number</b> 进入接口配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show mlink group [ mlink-group-number ]</b> 显示指定的 MLINK 组或全部 MLINK 组的信息；</li> <li>3. 结束。</li> </ol>

目的	步骤
查看 MLINK 所有或指定接口的配置信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gigaethernet   xgigaethernet } interface-number</b> 或 <b>interface eth-trunk trunk-number</b> 进入接口配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show mlink interface</b> 或 <b>show mlink interface { fastethernet   gigaethernet   xgigaethernet } interface-number</b> 显示指定的 RLINK 组或全部 RLINK 组的状态信息；</li> <li>3. 结束。</li> </ol>

附表：

参数	说明	取值
receive	收到的数据包	-
send	发送的数据包	-
timer	定时器	-
linkchange	链接变化	-
all	所有信息	-
interface-number	指定接口号	SC9600 系列交换机支持以下 3 种型号的接口配置范围： SC9603：取值范围是<1-3>/<0-4>/<1-48> SC9608：取值范围是<1-8>/<0-4>/<1-48> SC9612：取值范围是<1-12>/<0-4>/<1-48>

## 8.3.6 配置举例

### 8.3.6.1 配置单点上联举例

#### 组网要求

SC9600 系列高端交换机在单点上联组网环境中，配置 RLINK 功能，其主从端口在同一台交换机上，分别为接口 1/0/1，接口 1/0/2。

#### 组网图

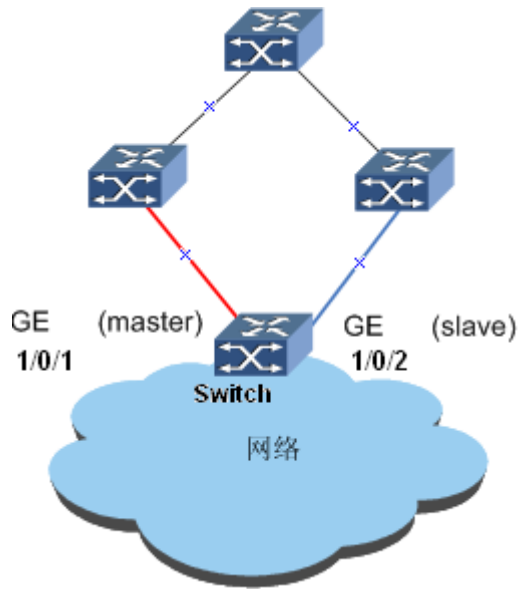


图 8-4 单点上联组网环境示意图

### 配置步骤

1、创建 RLINK 组 1。

```
SC9600#configure
```

```
SC9600(config)#rlink group 1
```

```
SC9600(config-rlink1)#type single //该步骤可选，因为默认为单点模式
```

```
SC9600(config-rlink1)#protect-vlan 1,2,3,4,5 //设置保护 VLAN 即为基于 VLAN 的  
RLink 组)
```

```
SC9600(config-rlink1)#active //激活 RLINK 组 1
```

```
SC9600(config-rlink1)#quit
```

```
SC9600(config)#
```

2、将接口 1/0/1 加入 RLINK 组 1 并指定为主端口。

```
SC9600(config)#interface gigabitEthernet 1/0/1
```

```
SC9600(config-gigabitEthernet 1/0/1)#join rlink group 1 master
```

```
SC9600(config-gigabitEthernet 1/0/1)#rlink enable
```

```
SC9600(config-gigabitEthernet 1/0/1)#quit
```

```
SC9600(config)#
```

3、将接口 1/0/2 加入 RLINK 组 1 并指定为从端口。

```
SC9600(config)#interface gigabitEthernet 1/0/2
```

```
SC9600(config-gigabitEthernet 1/0/2)#join rlink group 1 slave
```

```
SC9600(config-ge1/0/2)#rlink enable
SC9600(config-ge1/0/2)#quit
SC9600(config)#
```

4、配置结束，查看 RLINK 组 1 的信息。

```
SC9600#show rlink group 1
```

Rlink group 1 information:

Group status: active

Group type: single

Group Manlist:

Reverse: disable

Reverse time: 0

Member	Role	State	Status	Linkstate
ge-1/0/1	MASTER	FORWARD	ACTIVE	up/up
ge-1/0/2	SLAVE	BLOCK	ACTIVE	up/down

```
SC9600#
```

### 8.3.6.2 配置双点上联举例

#### 组网要求

SC9600 系列高端交换机在双点上联组网环境中，配置 RLINK 功能，主动端口分别配置在设备 M1 和 M2 上，其中主端口为 M1 上的接口 1/0/1，从端口为 M2 上的接口 1/0/2。

#### 组网图

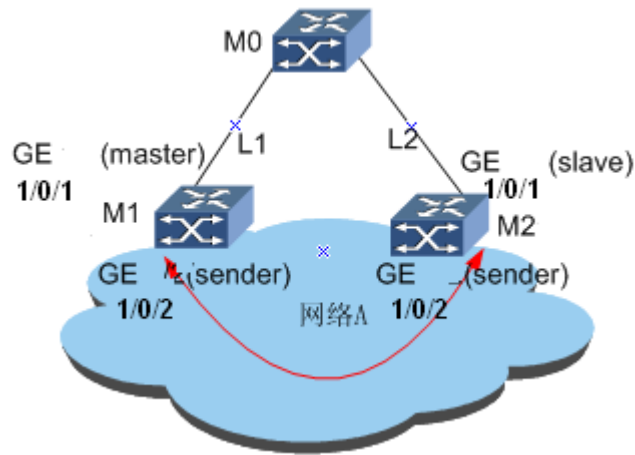


图 8-5 双点上联组网环境示意图

### 配置步骤

1、配置设备 M1。

#创建 RLINK 组 1。

```
M1#configure
M1(config)#rlink group 1
M1(config-rlink1)#type double
M1(config-rlink1)#active
M1(config-rlink1)#quit
M1(config)#
```

#将接口 1/0/1 加入 RLINK 组 1 并指定为主端口。

```
M1(config)#interface gigabitEthernet 1/0/1
M1(config-gigabitEthernet1/0/1)#join rlink group 1 master
M1(config-gigabitEthernet1/0/1)#rlink enable
M1(config-gigabitEthernet1/0/1)#quit
M1(config)#
```

#将接口 1/0/2 加入 RLINK 组 1 并指定为 sender 端口。

```
M1(config)#interface gigabitEthernet 1/0/2
M1(config-gigabitEthernet1/0/2)#join rlink group 1 sender
M1(config-gigabitEthernet1/0/2)#rlink enable
M1(config-gigabitEthernet1/0/2)#quit
M1(config)#
```

2、配置设备 M2。

#创建 RLINK 组 1。

```
M2#configure
```

```
M2(config)#rlink group 1
```

```
M2(config-rlink1)#type double
```

```
M2(config-rlink1)#active
```

```
M2(config-rlink1)#quit
```

```
M2(config)#
```

#将接口 1/0/1 加入 RLIN 组 1 并指定为主端口。

```
M2(config)#interface gigabitEthernet 1/0/1
```

```
M2(config-ge1/0/1)#join rlink group 1 slave
```

```
M2(config-ge1/0/1)#rlink enable
```

```
M2(config-ge1/0/1)#quit
```

```
M2(config)#
```

#将接口 1/0/2 加入 RLINK 组 1 并指定为 sender 端口。

```
M2(config)#interface gigabitEthernet 1/0/2
```

```
M2(config-ge1/0/2)#join rlink group 1 sender
```

```
M2(config-ge1/0/2)#rlink enable
```

```
M2(config-ge1/0/2)#quit
```

```
M2(config)#
```

3、配置结束，查看 M1 上 RLINK 组 1 的信息。

```
M1#show rlink group
```

```
Rlink group 1 information:
```

```
Group status: active
```

```
Group type: double
```

```
Group vlanlist:
```

```
Reverse: disable
```

```
Reverse time: 0
```

```
Receive timeout: 15
```

```
Send interval: 2000
```

```
Peer exist: EXIST
```

```
Peer mac: 0:4:67:97:db:83
```

```
Peer role: SLAVE
```

```
Peer state: BLOCK
```

Peer Reverse: disable  
 Peer send interval: 2000  
 Peer linkstate: up

Member	Role	State	Sendvid	Status
ge-1/0/1	MASTER	FORWARD	0	ACTIVE
ge-1/0/2	SENDER	FORWARD	0	ACTIVE

### 8.3.6.3 配置 MLINK 举例

#### 组网要求

在 SC9600 设备上配置 MLINK，其中接口 1/0/1 为 uplink1 端口，接口 1/0/2 为 uplink2 端口，接口 1/0/3 为 downlink1 端口，接口 1/0/4 为 downlink2 端口。

#### 组网图

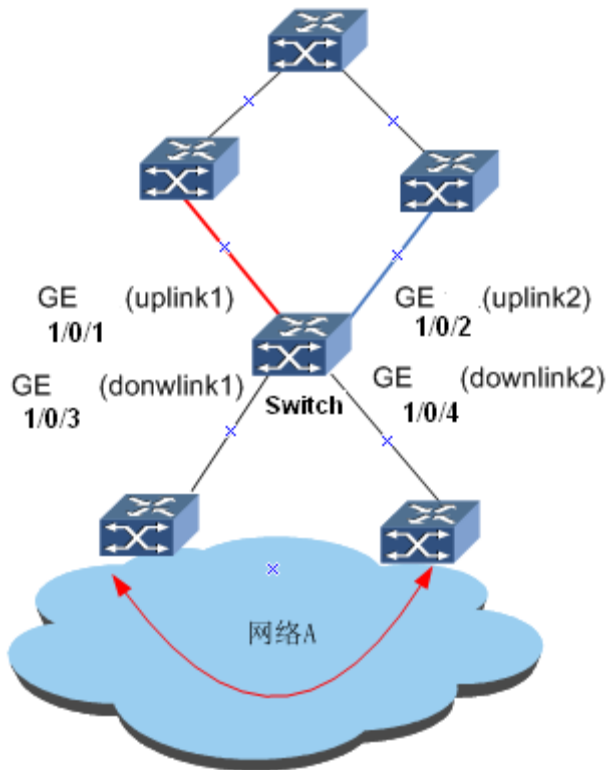


图 8-6 MLINK 联动功能示意图

#### 配置步骤

1、创建 MLINK 组。

```
SC9600#configure
SC9600(config)#mlink group 1
SC9600(config-mlink1)#quit
SC9600(config)#
```

2、将接口 1/0/1 加入 MLINK 组 1 并指定为 uplink1 端口

```
SC9600(config)#interface gigaethernet 1/0/1
SC9600(config-ge1/0/1)#join mlink group 1 uplink
SC9600(config-ge1/0/1)#mlink enable
SC9600(config-ge1/0/1)#quit
SC9600(config)#
```

3、将接口 1/0/2 加入 MLINK 组 1 并指定为 uplink2 端口

```
SC9600(config)#interface gigaethernet 1/0/2
SC9600(config-ge1/0/2)#join mlink group 1 uplink
SC9600(config-ge1/0/2)#mlink enable
SC9600(config-ge1/0/2)#quit
SC9600(config)#
```

4、将接口 1/0/3 加入 MLINK 组 1 并指定为 downlink1 端口

```
SC9600(config)#interface gigaethernet 1/0/3
SC9600(config-ge1/0/3)#join mlink group 1 downlink
SC9600(config-ge1/0/3)#mlink enable
SC9600(config-ge1/0/3)#quit
SC9600(config)#
```

5、将接口 1/0/4 加入 MLINK 组 1 并指定为 downlink2 端口

```
SC9600(config)#interface gigaethernet 1/0/4
SC9600(config-ge1/0/4)#join mlink group 1 downlink
SC9600(config-ge1/0/4)#mlink enable
SC9600(config-ge1/0/4)#quit
SC9600(config)#
```

6、配置结束，查看 MLINK 组配置信息。

```
SC9600#show mlink group 1
```

Mlink group 1 information:



Group status: active

Member	Role	State	Status	Linkstate
ge-1/0/1	UPLINK	FORWARD	ACTIVE	up/up
ge-1/0/2	UPLINK	FORWARD	ACTIVE	up/up
ge-1/0/3	DOWNLINK	FORWARD	ACTIVE	up/up
ge-1/0/4	DOWNLINK	FORWARD	ACTIVE	up/up

S7808#

## 8.4 BFD 配置

### 8.4.1 BFD 概述

#### 基本概念

BFD (Bidirectional Forwarding Detection) 双向转发检测是一套全网统一的用于检测转发设备之间通信故障的检测机制。BFD 能够为相邻转发设备之间的通道故障提供轻负荷、持续时间短的检测；可以对任何介质及协议层进行实时检测。

#### SC9600 支持的 BFD 特性

- 单跳检测

单跳检测是指检测两台直连设备间转发链路的连通性。

- 多跳检测

多跳检测是指检测两台非直连设备间任意路径的 IP 连通性。多跳检测一般用来检查两台设备之间是否存在可达路由。

- BFD for VRRP

使用 BFD 检测、监控网络中链路或者 IP 路由转发状况，VRRP 绑定 BFD 会话，BFD 通告会话状态，触发 VRRP 快速切换并进行处理。

- BFD for OSPF

OSPF 绑定 BFD 会话，BFD 通告会话状态，OSPF 负责处理。

- BFD for IS-IS

IS-IS 绑定 BFD 会话，BFD 通告会话状态，IS-IS 负责处理。

- BFD for BGP

BGP 绑定 BFD 会话，BFD 通告会话状态，BGP 负责处理。

- BFD for PIM

PIM 绑定 BFD 会话，BFD 通告会话状态，PIM 负责处理。

- BFD for VPLS

- 动态修改 BFD 参数

BFD 会话建立后，用户仍可以修改 BFD 相关参数的配置，如：BFD 报文期望发送间隔、最小接收间隔以及本地检测倍数。修改参数后不会影响会话当前的状态。

### ECHO 功能

BFD 具有两种检测模式异步模式和按需模式，与这两个模式相关的附加功能是 ECHO 功能。

使用 ECHO 功能时，节点向邻居发送一系列 BFD ECHO 包，邻居将这些包反射回发送节点。如果一段时间内没收到回应的 ECHO（或者丢失了大量的 ECHO 包），则通告会话关闭。使用 ECHO 时，ECHO 包用于检测故障，因此可减少 BFD 控制包的速度（异步模式）或完全停止发送 BFD 控制包（按需模式）。

纯粹的异步模式相对 ECHO 有一个优势：为达到同样的检测时间，异步模式需要的 BFD 控制包数目是 ECHO 包数目的一半。如果因为某种原因不能使用 ECHO 功能，也需要使用异步模式。

ECHO 功能的优点是，他只检测邻居上的转发路径。这可以减小往返时间抖动，可以实现更快的检测时间，并可检测一些其他方法无法检测的故障。

ECHO 功能可在两个方向上单独使能。在一个特定方向上使能 ECHO 功能的前提条件是：执行反射 ECHO 操作的节点表明自己允许运行 ECHO 功能，而发送 ECHO 的节点表明自己希望执行 ECHO 功能。

## 8.4.2 配置 BFD 检测功能

### 前提条件

在配置 BFD 检测功能之前必须先配置接口 VLAN 以及 IP 地址。如果用户还需要检测网络层的连通性，则需要先配置好路由协议。

### 背景信息

目前高端交换机不支持 demand 模式。

若单独使用 BFD 功能或 BFD 配合 VRRP 使用，需配置 `bfd track` 命令。

若 BFD 配合其他协议动态触发使用，则不需要再配置 `bfd track` 命令。

配置角色时，对于 BFD 会话建立过程中的初始化阶段，两端是主动角色还是被动角色是由应用来决定的，但是至少有一端为主动角色。

### 目的

当用户需要快速检测和监控网络中直连或设备间 IP 路由的联通状况，可以使用本节操作配置 BFD 检测功能。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
全局使能或去使能 BFD 功能	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>bfd { start   stop }</code> 全局启动或停止 BFD 功能；</li> <li>3. 结束。</li> </ol>
配置 BFD 会话	<p>检测二层链路：</p> <ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>bfd track track-number { fastethernet   gigasethernet   xgigasethernet } interface-number [ remote-mac mac-address ]</code> 或执行命令 <code>bfd track track-number eth-trunk trunk-number [ remote-mac mac-address ]</code> 添加基于 MAC 地址的静态 BFD 会话；</li> <li>3. 结束。</li> </ol> <p>检测三层链路：</p> <ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>bfd track track-number vlan vlan-id remote-ip ipv4-address1 local-ip ipv4-address2</code> 或执行命令 <code>bfd track track-number vlan vlan-id remote-ip6 ipv6-address1 local-ip6 ipv6-address2</code> 添加基于 IP 地址的静态 BFD 会话；</li> <li>3. 结束。</li> </ol>
接口使能或去使能 BFD 协议	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>interface { fastethernet   gigasethernet   xgigasethernet } interface-number</code> 进入接口配置视图或执行命令 <code>interface vlan vlan-id</code> 进入 VLANIF 接口配置视图；</li> <li>3. 执行命令 <code>bfd { enable   disable }</code> 使能或去使能接口 BFD；</li> <li>4. 结束。</li> </ol>
配置 BFD 角色模式	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>interface { fastethernet   gigasethernet   xgigasethernet } interface-number</code> 进入接口配置视图或执行命令 <code>interface vlan vlan-id</code> 进入</li> </ol>

目的	步骤
	VLANIF 接口配置视图； 3. 执行命令 <code>bfd role { active   passive }</code> 配置 BFD 角色； 4. 结束。
(可选) 配置 BFD 会话状态告警功能	1. 执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <code>bfd trap { enable   disable }</code> 使能或去使能 BFD 会话状态 (up 或 down) 告警功能； 3. 结束。

附表：

参数	说明	取值
track-number	指定静态 BFD 会话 ID	整数形式，取值范围是 1~2000
vlan-id	指定 VLAN ID	整数形式，取值范围是 1~4094
ipv4-address1	指定远端 IPv4 地址	点分十进制
ipv4-address2	指定本端 IPv4 地址	点分十进制
ipv6-address1	指定远端 IPv6 地址	-
ipv6-address2	指定本端 IPv6 地址	-
interface-number	指定接口号	SC9600 系列交换机支持以下 3 种型号的接口配置范围： SC9603: 取值范围是<1-3>/<0-4>/<1-48> SC9608: 取值范围是<1-8>/<0-4>/<1-48> SC9612: 取值范围是<1-12>/<0-4>/<1-48>
trunk-number	指定 trunk 接口号	整数形式，取值范围是 1~128
mac-address	指定远端 MAC 地址	形如 AA:BB:CC:DD:EE:FF, 其中 A~F 为一位十六进制数

### 8.4.3 配置 BFD 检测参数

#### 目的

当在建立 BFD 会话时，可以根据网络状况和性能需求，调整设备的 BFD 报文期望发送间隔、最小接收间隔以及本地检测倍数，可以使用本小节操作。

通常情况下，使用系统的缺省配置即可。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置 BFD 明文认证的	1. 执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <code>interface { fastethernet   gigaehternet   xgigaehternet }</code>

目的	步骤
密码或 MD5 认证的 KEY ID 及密钥	<p><i>interface-number</i> 进入接口配置视图或执行命令 <b>interface vlan <i>vlan-id</i></b> 进入 VLANIF 接口配置视图；</p> <p>3. 执行命令 <b>bfd authentication md5 <i>key-id</i> <i>key-string</i></b> 配置 MD5 认证的 KEY ID 及密钥或执行命令 <b>bfd authentication text <i>simple-password</i></b> 配置 BFD 明文认证的密码；</p> <p>4. 结束。</p>
配置 BFD 最小发包间隔时间、最小收包间隔时间以及检测超时倍数。	<p>1. 执行命令 <b>configure</b> 进入全局配置视图；</p> <p>2. 执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } <i>interface-number</i></b> 进入接口配置视图或执行命令 <b>interface vlan <i>vlan-id</i></b> 进入 VLANIF 接口配置视图；</p> <p>3. 执行命令 <b>bfd min-tx <i>tx-interval</i> min-rx <i>rx-interval</i> multiplier <i>timeout-multiple</i></b> 调整 BFD 最小发包间隔时间、最小收包间隔时间以及检测超时倍数；</p> <p>4. 结束。</p>
配置最小 ECHO 报文接收间隔时间	<p>1. 执行命令 <b>configure</b> 进入全局配置视图；</p> <p>2. 执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } <i>interface-number</i></b> 进入接口配置视图或执行命令 <b>interface vlan <i>vlan-id</i></b> 进入 VLANIF 接口配置视图；</p> <p>3. 执行命令 <b>bfd min-echo <i>echo-interval</i></b> 调整最小 ECHO 报文接收间隔时间；</p> <p>4. 结束。</p>

附表：

参数	说明	取值
<i>interface-number</i>	指定接口号	<p>SC9600 系列交换机支持以下 3 种型号的接口配置范围：</p> <p>SC9603 : 取值范围是 &lt;1-3&gt;/&lt;0-4&gt;/&lt;1-48&gt;</p> <p>SC9608 : 取值范围是 &lt;1-8&gt;/&lt;0-4&gt;/&lt;1-48&gt;</p> <p>SC9612 : 取值范围是 &lt;1-12&gt;/&lt;0-4&gt;/&lt;1-48&gt;</p>
<i>vlan-id</i>	指定 VLAN ID	整数形式，取值范围是 1~4094
<i>key-id</i>	指定 MD5 认证的 key ID	整数形式，取值范围是 1~255
<i>key-string</i>	指定 MD5 认证的密钥	字符串形式
<i>simple-passw ord</i>	指定明文认证的密码	字符串形式，不含空格
<i>tx-interval</i>	指定 BFD 最小发包间隔时间	整数形式，取值范围是 5~999，单位：毫秒
<i>rx-interval</i>	指定 BFD 最小收包间隔时间	整数形式，取值范围是 1~999，单位：毫秒
<i>timeout-multiple</i>	指定检测超时倍数	整数形式，取值范围是 1~255

参数	说明	取值
echo-interval	指定最小 ECHO 报文接收间隔时间	整数形式，取值范围是 0~999，其中 0 表示去使能回声功能，单位：毫秒

### 8.4.4 维护及调试

#### 目的

当 BFD 功能不正常，需要进行查看、调试或定位问题时，可以使用本小节操作。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
打开 BFD 调试功能	<ol style="list-style-type: none"> <li>1. 保持当前特权用户视图；</li> <li>2. 执行命令 <code>debug bfd { session   in   out }</code> 打开 BFD 功能调试开关；</li> <li>3. 结束。</li> </ol>
关闭 BFD 调试功能	<ol style="list-style-type: none"> <li>1. 保持当前特权用户视图；</li> <li>2. 执行命令 <code>no debug bfd { session   in   out }</code> 关闭 BFD 能调试开关；</li> <li>3. 结束。</li> </ol>
查看配置了 BFD 的接口信息	<ol style="list-style-type: none"> <li>1. 执行命令 <code>disable</code> 退出到普通用户视图，或执行命令 <code>configure</code> 进入全局配置视图，或执行命令 <code>interface { fastethernet   gigasethernet   xgigasethernet } interface-number</code> 或 <code>interface eth-trunk trunk-number</code> 进入接口配置视图，或执行命令 <code>interface vlan vlan-id</code> 进入 VLANIF 配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <code>show bfd interface</code> 显示使能了 BFD 的接口信息；</li> <li>3. 结束。</li> </ol>
查看动态建立的 BFD 会话信息	<ol style="list-style-type: none"> <li>1. 执行命令 <code>disable</code> 退出到普通用户视图，或执行命令 <code>configure</code> 进入全局配置视图，或执行命令 <code>interface { fastethernet   gigasethernet   xgigasethernet } interface-number</code> 或 <code>interface eth-trunk trunk-number</code> 进入接口配置视图，或执行命令 <code>interface vlan vlan-id</code> 进入 VLANIF 配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <code>show bfd session</code> 显示动态建立的 BFD 会话信息；</li> <li>3. 结束。</li> </ol>
查看静态 BFD 会话信息	<ol style="list-style-type: none"> <li>1. 执行命令 <code>disable</code> 退出到普通用户视图，或执行命令 <code>configure</code> 进入全局配置视图，或执行命令 <code>interface { fastethernet   gigasethernet   xgigasethernet } interface-number</code> 或 <code>interface eth-trunk trunk-number</code> 进入接口配置视图，或执行命令 <code>interface vlan vlan-id</code> 进入 VLANIF 配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <code>show bfd track track-number</code> 或 <code>show bfd track</code> 显示静态 BFD 会话信息；</li> <li>3. 结束。</li> </ol>

附表：

参数	说明	取值
session	调试 BFD 会话信息	-
pkt	调试 BFD 报文信息	-
track-number	指定静态 BFD 会话 ID	整数形式，取值范围是 1~2000

### 8.4.5 配置举例



注意：

在 VLAN 接口下配置 BFD 时，首先要保证两台设备相互能够 Ping 通。

#### 8.4.5.1 单跳检测应用

##### 组网要求

两台 SC9600 通过二层接口直连，为了检测二层转发链路的连通性，可以配置 BFD 单跳检测，使 BFD 会话绑定二层接口。

##### 组网图



图 8-7 BFD 单跳检测二层链路组网图

##### 配置步骤

1、配置 SC9600A 端 BFD 会话及参数。

//全局使能 BFD。

```
SC9600A#configure
```

```
SC9600A(config)#bfd start
```

//配置 BFD 会话。

```
SC9600A(config)#bfd track 1 gig ethernet 1/0/1 00:04:67:00:00:02
```

//配置 BFD 会话参数（注：工作模式、BFD 控制报文的最小发送间隔、最小接收间隔、本地检测倍数等也可以使用缺省值）。

```
SC9600A(config)#interface gigabitEthernet 1/0/1
```

```
SC9600A(config-ge1/0/1)#bfd enable
```

//以下是可选配置。

```
SC9600A(config-ge1/0/1)#bfd role active
```

```
SC9600A(config-ge1/0/1)#bfd min-tx 300 min-rx 300 multiplier 3
```

2、配置 SC9600B 端 BFD 会话及参数。

//全局使能 BFD。

```
SC9600B#configure
```

```
SC9600B(config)#bfd start
```

//配置 BFD 会话。

```
SC9600B(config)#bfd track 1 gigabitEthernet 1/0/1 00:04:67:00:00:01
```

//配置 BFD 会话参数（注：工作模式、BFD 控制报文的最小发送间隔、最小接收间隔、本地检测倍数等也可以使用缺省值）。

```
SC9600B(config)#interface gigabitEthernet 1/0/1
```

```
SC9600B(config-ge1/0/1)#bfd enable
```

//以下是可选配置。

```
SC9600B(config-ge1/0/1)#bfd role active (也可以是 passive)
```

```
SC9600B(config-ge1/0/1)#bfd min-tx 300 min-rx 300 multiplier 3
```

#### 8.4.5.2 多跳检测应用

##### 组网要求

三台 SC9600 相连如下图所示，配置 BFD 多跳检测，用于检测 SC9600A、SC9600C 之间的多跳路径，需将接口加入 VLAN、创建接口 VLANIF 并在其上配置 IP 地址。

##### 组网图

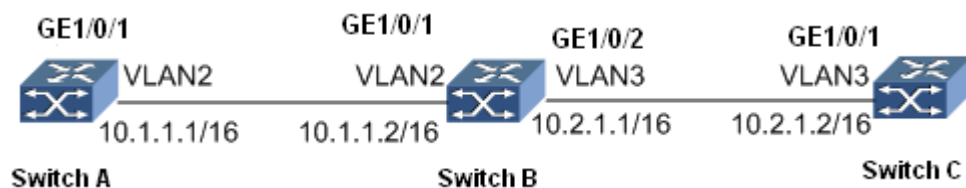


图 8-8 BFD 多跳检测组网图



**配置步骤**

## 1、配置 SwichA。

//将接口 gigaethernet1/0/1 加入 VLAN2，并配置 IP 地址为 10.1.1.1/16。

```
SwichA#configure
SwichA(config)#interface vlan 2
SwichA(config-vlan-2)#ip address 10.1.1.1/16
SwichA(config-vlan-2)#quit
SwichA(config)#interface gigaethernet 1/0/1
SwichA(config-ge1/0/1)#port hybrid pvid vlan 2
SwichA(config-ge1/0/1)#port hybrid vlan 2 untagged
SwichA(config-ge1/0/1)#quit
SwichA(config)#
```

//配置静态路由，使 SC9600A 与 SC9600C 之间路由可达。

```
SwichA(config)#ip route-static 10.2.0.0 16 10.1.1.2
```

//配置 BFD 会话参数，A 端（主动）。

```
SwichA(config)#bfd start
SwichA(config)#bfd track 1 vlan 2 remote-ip 10.2.1.2 local-ip 10.1.1.1
SwichA(config)#interface vlan 2
SwichA(config-vlan-2)#bfd enable
```

//以下是可选配置。

```
SwichA(config-vlan-2)#bfd role active
SwichA(config-vlan-2)#bfd min-tx 300 min-rx 300 multiplier 3
SwichA(config-vlan-2)#quit
SwichA(config)#
```

## 2、配置 SwichB。

//将接口 gigaethernet1/0/1 加入 VLAN2，并配置 IP 地址为 10.1.1.2/16。

```
SwichB#configure
SwichB(config)#interface vlan 2
SwichB(config-vlan-2)#ip address 10.1.1.2/16
SwichB(config-vlan-2)#quit
SwichB(config)#interface gigaethernet 1/0/1
SwichB(config-ge1/0/1)#port hybrid pvid vlan 2
SwichB(config-ge1/0/1)#port hybrid vlan 2 untagged
```

```
SwichB(config-ge1/0/1)#quit
SwichB(config)#
//将接口 gigaethernet1/0/2 加入 VLAN3, 并配置 IP 地址为 10.2.1.1/16
SwichB(config)#interface vlan 3
SwichB(config-vlan-3)#ip address 10.2.1.1/16
SwichB(config-vlan-3)#quit
SwichB(config)#interface gigaethernet 1/0/2
SwichB(config-ge1/0/2)#port hybrid pvid vlan 3
SwichB(config-ge1/0/2)#port hybrid vlan 3 untagged
SwichB(config-ge1/0/2)#quit
SwichB(config)#
```

### 3、配置 SwichC。

//将接口 gigaethernet1/0/1 加入 VLAN3, 并配置 IP 地址为 10.2.1.2/16。

```
SwichC#configure
SwichC(config)#interface vlan 3
SwichC(config-vlan-3)#ip address 10.2.1.2/16
SwichC(config-vlan-3)#quit
SwichC(config)#interface gigaethernet 1/0/1
SwichC(config-ge1/0/1)#port hybrid pvid vlan 3
SwichC(config-ge1/0/1)#port hybrid vlan 3 untagged
SwichC(config-ge1/0/1)#quit
SwichC(config)#
//配置静态路由, 使 SC9600C 与 SC9600A 之间路由可达。
SwichC(config)#ip route-static 10.1.0.0 16 10.2.1.1
//配置 BFD 会话参数, C 端 (主动或被动)。
SwichC(config)#bfd start
SwichC(config)#bfd track 1 vlan 3 remote-ip 10.1.1.1 local-ip 10.2.1.2
SwichC(config)#interface vlan 3
SwichC(config-vlan-3)#bfd enable
//以下是可选配置。
SwichC(config-vlan-3)#bfd role passive (也可以是 active)
SwichC(config-vlan-3)#bfd min-tx 300 min-rx 300 multiplier 3
SwichC(config-vlan-2)#quit
SwichC(config)#
```

## 8.5 VRRP

### 8.5.1 VRRP 概述

#### VRRP 基本概念

如图 8-9所示，通常一个网络内的所有主机都设置一条缺省路由（图中的缺省路由下一跳地址为 10.100.10.1），主机发往外部网络的报文将通过缺省路由发往三层交换机 Switch，从而实现了主机与外部网络的通信。当交换机 Switch 发生故障时，本网段内所有以 Switch 为缺省路由下一跳的主机将断掉与外部的通信。

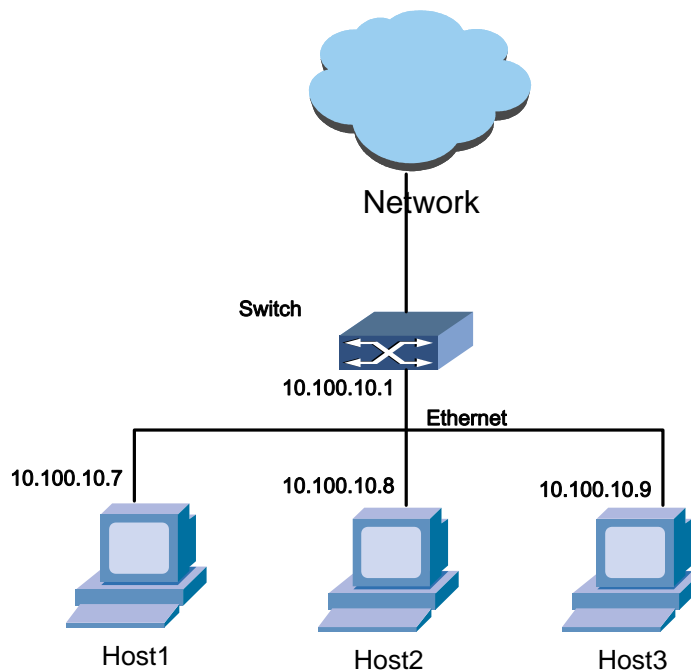


图 8-9 局域网组网方案

VRRP（Virtual Router Redundancy Protocol，虚拟路由冗余协议）是 RFC3768 定义的一种容错协议，就是为解决上述问题而提出的。

通过物理设备和逻辑设备的分离，实现在多个出口网关之间的选路，VRRP 为具有多播或广播能力的局域网（如以太网）提供逻辑网关。在无需修改路由协议配置的情况下，还能够解决因某网关设备故障带来的业务中断。

#### VRRP 工作原理

如图 8-10所示，VRRP 将局域网的一组交换机（包括一个 Master 即主交换机和若干个 Backup 即备份交换机）组织成一个虚拟路由器，这组交换机被称为一个备份组。虚拟的交换机拥有自己的 IP 地址 10.100.10.1（这个 IP 地址可以和备份组内的某个交换机的接口地址相同）和专用的 MAC 地址，备份组内的交换机也有自己的 IP 地址（如 Master 的 IP 地址为 10.100.10.2，Backup 的 IP 地址为 10.100.10.3）。局域网内的主机仅仅知道这个虚拟路由器的 IP 地址 10.100.10.1（通常被称为备份组的虚拟 IP 地址），而不知道具体的 Master 交换机的 IP 地址 10.100.10.2 以及 Backup 交换机的 IP 地址 10.100.10.3。局域网内的主机将自己的缺省路由下一跳设置为该虚拟路由器的 IP 地址 10.100.10.1。于是，网络内的主机就通过这个虚拟的交换机与其它网络进行通信。在正常情况下，Master 对虚拟地址 ARP 请求进行应答，当备份组内的 Master 交换机不能正常工作时，备份组内的其它 Backup 交换机将接替不能正常工作的 Master 交换机成为新的 Master 交换机，继续向网络内的主机提供路由服务，同时保持虚拟地址的 ARP 条目不变，从而实现网络内的主机不间断地与外部网络进行通信。

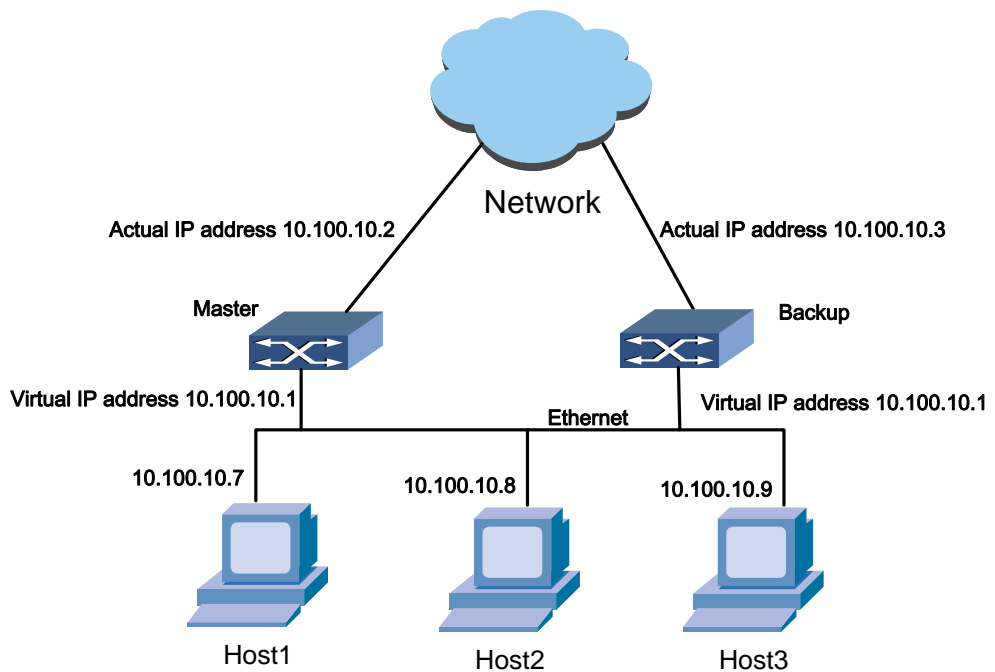


图 8-10 虚拟路由器示意图

### SC9600 支持的 VRRP 特性

- VRRP 主备备份

该功能是 VRRP 提供 IP 地址备份功能的基本方式。通过建立一个虚拟路由器，包括一个 Master 和若干 Backup 设备，由这些设备构成一个备份组。正常情况下，由 Master 转发全部业务流，当 Master 出现故障时，由 Backup 接替其工作。

- VRRP 负载分担

负载分担方式是指建立两个或多个备份组，多台交换机同时承担通讯业务。其中允许一台交换机为多个备份组作备份，在不同备份组中有不同的优先级。通过多虚拟交换机设置可以实现负载分担。每个备份组都包括一个 Master 设备和若干 Backup 设备。各备份组的 Master 可以不同。

- VRRP 接口联动

通过配置关联接口，在上行接口断开的情况下，将下行接口的 VRRP 强制设置为 Backup，这样从 VRRP 接口上收到的包将通过另外一个节点进行转发。

- VRRP 快速切换

SC9600 通过 BFD 机制能够快速检测、监控网络中链路或者 IP 路由的连通状况。VRRP 可以通过监视 BFD 会话状态实现主备快速切换。

- VRRP 安全功能

为增强 VRRP 的安全性，可以对 VRRP 采用认证。在一个安全的网络环境中，可以不对 VRRP 报文进行任何认证；在有可能受到安全威胁的网络环境中，VRRP 可以提供简单字符认证或 MD5 认证方式。

## 8.5.2 配置 VRRP 备份组

### 背景信息

VRRP 实例的优先级表明成为 Master 的优先程度。VRRP 备份组中的设备首先会根据优先级字段进行判断，选择优先级最高的设备；如果出现相同优先级，则根据 IP 地址进行比较。如果管理员认为某一设备应该作为 Master（比如接口带宽较高），则可为其设置较高的优先级，从而强制此设备成为 Master。

设置 VRRP 虚拟路由器的 IP 地址，此 IP 地址将作为直连主机的默认网关。



说明：

目前 SC9600 只有 VLANIF 接口支持 VRRP 功能。

配置的虚拟 IP 地址必须和当前接口 IP 地址在同一网段。

### 前提条件

配置 VRRP 备份组之前，请配置好以下任务：

- 配置接口物理参数及链路属性
- 配置接口的网络层属性，使网络连通

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
创建 VRRP 记录表项	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface vlan vlan-id</b> 进入 VLANIF 配置视图；</li> <li>3. 执行命令 <b>ip vrrp virtual-route-id</b>（适用于 IPv4）或执行命令 <b>ipv6 vrrp virtual-route-id</b>（适用于 IPv6）创建备份组；</li> <li>4. 结束。</li> </ol>
配置关联的虚拟 IP 地址	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface vlan vlan-id</b> 进入 VLANIF 配置视图；</li> <li>3. 执行命令 <b>ip vrrp virtual-route-id associate-address ip-address</b>（适用于 IPv4）或执行命令 <b>ipv6 vrrp virtual-route-id associate-address ip-address</b>（适用于 IPv6）配置和虚拟路由器相关联的虚拟 IP 地址；</li> <li>4. 结束。</li> </ol>
配置 VRRP 选举主虚拟路由器的优先级	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface vlan vlan-id</b> 进入 VLANIF 配置视图；</li> <li>3. 执行命令 <b>ip vrrp virtual-route-id priority { priority   default }</b>（适用于 IPv4）或执行命令 <b>ipv6 vrrp virtual-route-id priority { priority   default }</b>（适用于 IPv6）配置交换机在备份组中的优先级；</li> <li>4. 结束。</li> </ol>

附表：

参数	说明	取值
vlan-id	指定 VLAN 接口	整数形式，取值范围是 1~4094
virtual-route-id	指定虚拟路由器的全局 ID 号	整数形式，取值范围是 1~255
ip-address	指定和虚拟路由器相关联的 IP 地址	点分十进制
priority	指定 VRRP 选举主虚拟路由器的优先级	整数形式，取值范围是 1~254
default	表示默认优先级	100

## 8.5.3 配置 VRRP 认证方式

### 背景信息

在安全的网路环境下，可以不需要对 VRRP 报文进行认证字的设置，SC9600 不对发送或接收的报文进行认证处理，认为都是真实的合法的 VRRP 报文。

在有可能受到安全威胁的网络环境下，VRRP 提供简单字符和 MD5 两种认证方式。

### 前提条件

配置 VRRP 认证方式之前，请配置好以下任务：

- 配置接口物理参数及链路属性
- 配置接口的网络层属性，使网络连通
- 配置 VRRP 备份组

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置 VRRP 认证方式	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface vlan <i>vlan-id</i></b> 进入 VLANIF 配置视图；</li> <li>3. 执行命令 <b>ip vrrp <i>virtual-route-id</i> authentication-mode { simple   md5 } key</b> 指定 VRRP 实例的认证模式及对应密钥；</li> <li>4. 结束。</li> </ol>
删除 VRRP 认证功能	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface vlan <i>vlan-id</i></b> 进入 VLANIF 配置视图；</li> <li>3. 执行命令 <b>no ip vrrp <i>virtual-route-id</i> authentication-mode</b> 删除交换机上配置的 VRRP 认证功能；</li> <li>4. 结束。</li> </ol>

附表：

参数	说明	取值
vlan-id	指定 VLAN 接口	整数形式，取值范围是 1~4094
virtual-route-id	指定虚拟路由器的全局 ID 号	整数形式，取值范围是 1~255
key	指定 VRRP 实例认证模式对应的密钥	字符串形式，长度为最大 8 字节
simple	表示简单字符认证方式	-
md5	表示 MD5 认证方式	-

## 8.5.4 配置 VRRP 参数

### 背景信息

通过调整 VRRP 报文的相关参数可以优化备份组功能：

- VRRP 实例的每一个接口都周期性向接口上发送 VRRP 组播报文。这个周期性间隔时间决定了 VRRP 主备倒换操作的速度，一般使用默认值即可，但在特定情况下，可以使用本操作改变默认的通告间隔时间。对于此时间的设置，如果设置的时间较短，则会使 VRRP 的灵敏度很高，这样可以缩短主备之间切换的时间，减少数据的丢失。如果时间设置较长，发送通告数据包的时间间隔增大，则可以减轻网络的负担。
- 如果需要高优先级的设备能够主动成为 Master，则应将设备配置为抢占模式。



说明：

建议备份组中所有设备采用相同的通告间隔时间。

### 前提条件

配置 VRRP 认证方式之前，请配置好以下任务：

- 配置接口物理参数及链路属性
- 配置接口的网络层属性，使网络连通
- 配置 VRRP 备份组

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置 VRRP 协议通告报文的发送间隔时间	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface vlan <i>vlan-id</i></b> 进入 VLANIF 配置视图；</li> <li>3. 执行命令 <b>ip vrrp <i>virtual-route-id</i> advertise-interval { <i>interval-time</i>   default }</b>（适用于 IPv4）或执行命令 <b>ipv6 vrrp <i>virtual-route-id</i> advertise-interval { <i>interval-time</i>   default }</b>（适用于 IPv6）指定 VRRP 通告报文的发送间隔时间；</li> <li>4. 结束。</li> </ol>
使能 VRRP 抢占模式	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface vlan <i>vlan-id</i></b> 进入 VLANIF 配置视图；</li> <li>3. 执行命令 <b>ip vrrp <i>virtual-route-id</i> preemptenable</b> 使能 VRRP 抢占模式；</li> <li>4. 结束。</li> </ol>
去使能 VRRP 抢占模式	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface vlan <i>vlan-id</i></b> 进入 VLANIF 配置视图；</li> <li>3. 执行命令 <b>ip vrrp <i>virtual-route-id</i> preemptdisable</b> 去使能 VRRP 抢占模式；</li> <li>4. 结束。</li> </ol>



附表：

参数	说明	取值
vlan-id	指定 VLAN 接口	整数形式，取值范围是 1~4094
virtual-route-id	指定虚拟路由器的全局 ID 号	整数形式，取值范围是 1~255
interval-time	指定发送间隔时间	整数形式，取值范围是 1~40，单位：秒
default	指定为默认值	1 秒

### 8.5.5 配置 VRRP 监视 BFD 会话状态

#### 背景信息

使用 VRRP 监视 BFD 会话，当 BFD 会话状态在改变后会通知 VRRP 模块，实现 VRRP 快速切换功能。

#### 前提条件

配置 VRRP 认证方式之前，请配置好以下任务：

- 配置接口的网络层属性，使网络连通
- 配置 VRRP 备份组
- 配置 BFD 会话

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
绑定 BFD 会话与 VRRP 实例	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface vlan vlan-id</b> 进入 VLANIF 配置视图；</li> <li>3. 执行命令 <b>ip vrrp virtual-route-id track bfd-session bfdsession-id</b>（适用于 IPv4）或执行命令 <b>ipv6 vrrp virtual-route-id track bfd-session bfdsession-id</b>（适用于 IPv6）绑定 BFD 会话与 VRRP 实例；</li> <li>4. 结束。</li> </ol>
解除 BFD 会话与 VRRP 实例的绑定关系	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface vlan vlan-id</b> 进入 VLANIF 配置视图；</li> <li>3. 执行命令 <b>no ip vrrp virtual-route-id track bfd-session</b>（适用于 IPv4）或执行命令 <b>no ipv6 vrrp virtual-route-id track bfd-session</b>（适用于 IPv6）解除绑定关系；</li> <li>4. 结束。</li> </ol>

附表：

参数	说明	取值
vlan-id	指定 VLAN 接口	整数形式，取值范围是 1~4094

参数	说明	取值
virtual-route-id	指定虚拟路由器的全局 ID 号	整数形式，取值范围是 1~255
bfdsession-id	指定 BFD 会话的实例号	整数形式，取值范围是 1~255

### 8.5.6 维护及调试

#### 目的

当 VRRP 功能不正常，需要进行查看、调试或定位问题时，可以使用本小节操作。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
打开 VRRP 调试功能	<ol style="list-style-type: none"> <li>1. 保持当前特权用户视图；</li> <li>2. 执行命令 <code>debug vrrp { global   detail   packet   all }</code> 打开 VRRP 功能调试开关；</li> <li>3. 结束。</li> </ol>
关闭 VRRP 调试功能	<ol style="list-style-type: none"> <li>1. 保持当前特权用户视图；</li> <li>2. 执行命令 <code>no debug vrrp { global   detail   packet   all }</code> 关闭 VRRP 能调试开关；</li> <li>3. 结束。</li> </ol>
查看 VRRP 配置信息	<ol style="list-style-type: none"> <li>1. 执行命令 <code>disable</code> 退出到普通用户视图，或执行命令 <code>configure</code> 进入全局配置视图，或执行命令 <code>interface vlan vlan-id</code> 进入 VLANIF 配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <code>show ip vrrp</code> 显示 IPv4 的 VRRP 配置信息或执行命令 <code>show ipv6 vrrp</code> 显示 IPv6d VRRP 配置信息；</li> <li>3. 结束。</li> </ol>
查看 VRRP 相关联的接口信息	<ol style="list-style-type: none"> <li>1. 执行命令 <code>disable</code> 退出到普通用户视图，或执行命令 <code>configure</code> 进入全局配置视图，或执行命令 <code>interface vlan vlan-id</code> 进入 VLANIF 配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <code>show ip vrrp associate interface</code> 显示 VRRP 相关联的接口信息；</li> <li>3. 结束。</li> </ol>
查看 VRRP 运行的配置信息	<ol style="list-style-type: none"> <li>1. 执行命令 <code>disable</code> 退出到普通用户视图，或执行命令 <code>configure</code> 进入全局配置视图，或执行命令 <code>interface vlan vlan-id</code> 进入 VLANIF 配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <code>show ip vrrp config</code> 显示 VRRP 运行的配置信息；</li> <li>3. 结束。</li> </ol>
查看 VRRP 路由器详细信息	<ol style="list-style-type: none"> <li>1. 执行命令 <code>disable</code> 退出到普通用户视图，或执行命令 <code>configure</code> 进入全局配置视图，或执行命令 <code>interface vlan vlan-id</code> 进入 VLANIF 配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <code>show ip vrrp vlan vlan-id virtual-route-id</code> 显示 VRRP 路由器详细信息（适用于 IPv4）或执行命令 <code>show ipv6 vrrp vlan vlan-id virtual-route-id</code> 显示 VRRP 路由器详细信息（适用于 IPv6）。</li> </ol>

目的	步骤
	3. 结束。

附表：

参数	说明	取值
virtual-route-id	指定虚拟路由器的全局 ID 号	整数形式，取值范围是 1~255
vlan-id	指定 VLAN ID	整数形式，取值范围是 1~4094

## 8.5.7 配置举例

### 8.5.7.1 配置 VRRP 主备备份

#### 组网要求

主机 Host1、Host2、Host3 通过 SC9600A 访问外部网络。SC9600A 和 SC9600B 根据配置的优先级来确定 VRRP 备份组内的 Master。当 Master 状态变为 Down，则 Backup 将替换 Master 使主机可以与外网通信。

#### 组网图

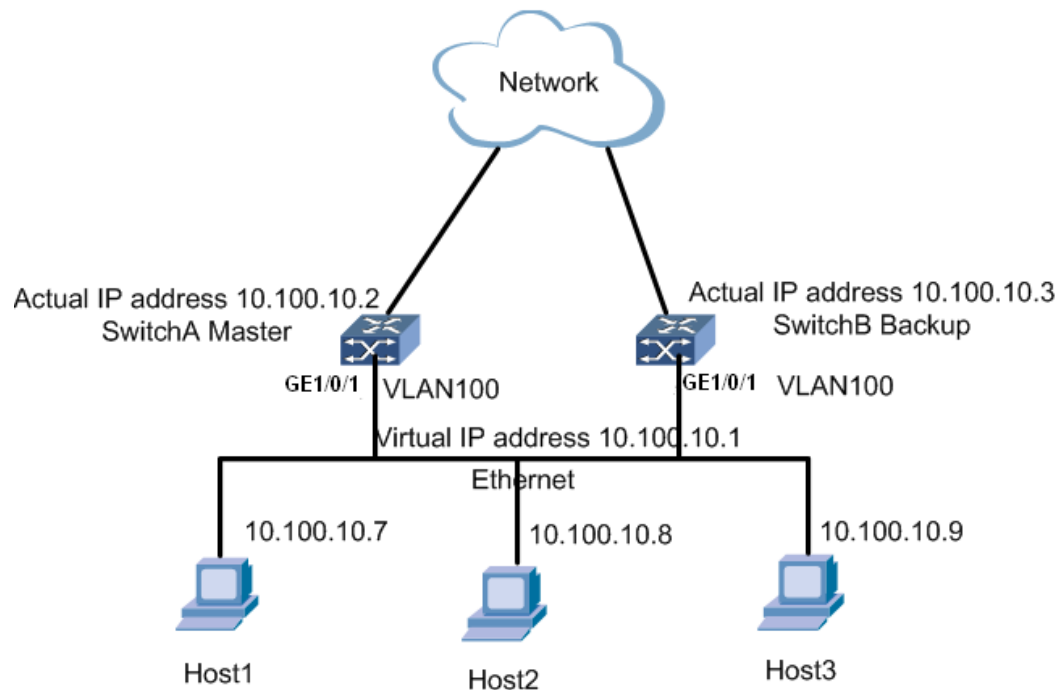


图 8-11 VRRP 主备备份组网图

#### 配置步骤

### 1、配置 SC9600A。

//配置接口实际的 IP 地址。

```
SwichA#configure
```

```
SwichA(config)#interface gigabitEthernet 1/0/1
```

```
SwichA(config-ge1/0/1)#port hybrid pvid 100
```

```
SwichA(config-ge1/0/1)#port hybrid vlan 100 untagged
```

```
SwichA(config-ge1/0/1)#quit
```

```
SwichA(config)#interface vlan 100
```

```
SwichA(config-vlan-100)#ip address 10.100.10.2
```

//创建 VRRP 记录表项即备份组。

```
SwichA(config-vlan-100)#ip vrrp 1
```

//配置接口虚拟 IP 地址。

```
SwichA(config-vlan-100)#ip vrrp 1 associate-address 10.100.10.1
```

### 2、配置 SC9600B。

//配置接口实际的 IP 地址。

```
SwichB#configure
```

```
SwichB(config)#interface gigabitEthernet 1/0/1
```

```
SwichB(config-ge1/0/1)#port hybrid pvid 100
```

```
SwichB(config-ge1/0/1)#port hybrid vlan 100 untagged
```

```
SwichB(config-ge1/0/1)#quit
```

```
SwichB(config)#interface vlan 100
```

```
SwichB(config-vlan-100)#ip address 10.100.10.3
```

//创建 VRRP 记录表项即备份组。

```
SwichB(config-vlan-100)#ip vrrp 1
```

//配置接口虚拟 IP 地址。

```
SwichB(config-vlan-100)#ip vrrp 1 associate-address 10.100.10.1
```

//配置选举优先级低于 SC9600A。

```
SwichB(config-vlan-100)#ip vrrp 1 priority 25
```

## 8.5.7.2 配置 VRRP 快速切换

### 组网要求

主机 Host1、Host2、Host3 通过 SC9600A 访问外部网络。SC9600A 和 SC9600B 根据配置的优先级来确定 VRRP 备份组内的 Master。同时，在作为 Backup 的 SC9600B

上配置 VRRP 监视 BFD Session，当 Master 状态变为 Down，则 Backup 将快速进行主备切换替换 Master 使主机可以与外网通信。

组网图

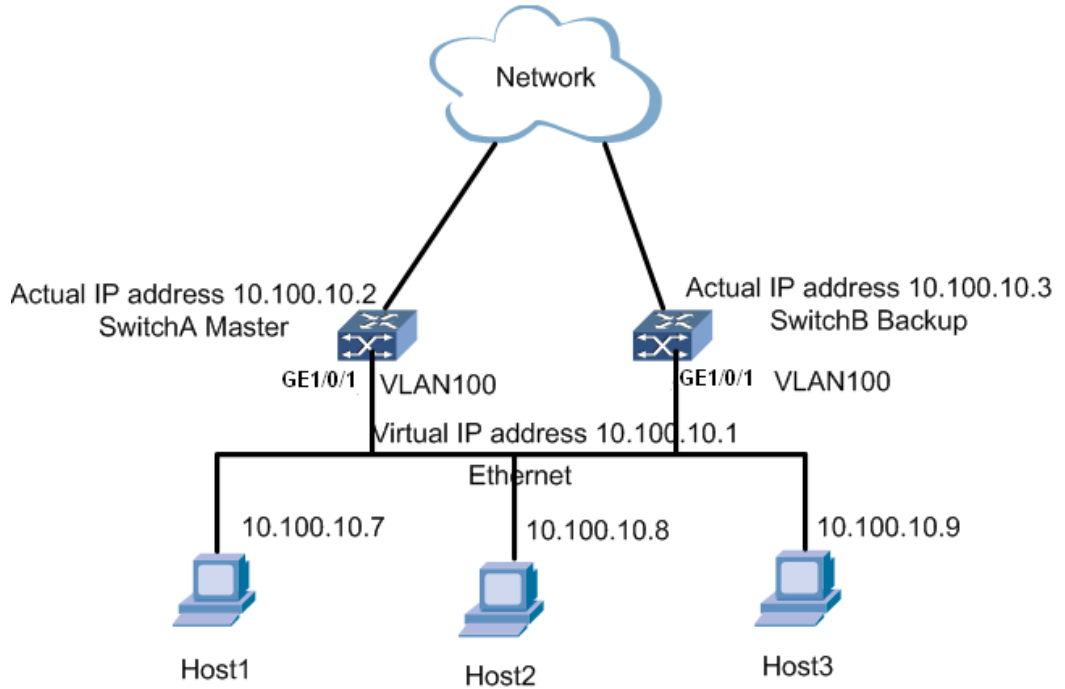


图 8-12 VRRP 主备备份组网图

配置步骤

1、配置 SC9600A。

//配置接口实际的 IP 地址。

```
SwichA#configure
```

```
SwichA(config)#interface gig ethernet 1/0/1
```

```
SwichA(config-ge1/0/1)#port hybrid pvid 100
```

```
SwichA(config-ge1/0/1)#port hybrid vlan 100 untagged
```

```
SwichA(config-ge1/0/1)#quit
```

```
SwichA(config)#interface vlan 100
```

```
SwichA(config-vlan-100)#ip address 10.100.10.2
```

//创建 VRRP 记录表项即备份组。

```
SwichA(config-vlan-100)#ip vrrp 1
```

//配置接口虚拟 IP 地址。

```
SwichA(config-vlan-100)#ip vrrp 1 associate-address 10.100.10.1
SwichA(config-vlan-100)#quit
SwichA(config)#
//配置 BFD 会话。
SwichA(config)#bfd start
SwichA(config)#bfd track 1 vlan 100 remote-ip 10.100.10.3 local-ip 10.100.10.2
SwichA(config)#interface vlan 100
SwichA(config-vlan-100)#bfd enable
```

## 2、配置 SC9600B。

```
//配置接口实际的 IP 地址。
SwichB#configure
SwichB(config)#interface gigabitEthernet 1/0/1
SwichB(config-ge1/0/1)#port hybrid pvid 100
SwichB(config-ge1/0/1)#port hybrid vlan 100 untagged
SwichB(config-ge1/0/1)#quit
SwichB(config)#interface vlan 100
SwichB(config-vlan-100)#ip address 10.100.10.3
//创建 VRRP 记录表项即备份组。
SwichB(config-vlan-100)#ip vrrp 1
//配置接口虚拟 IP 地址。
SwichB(config-vlan-100)#ip vrrp 1 associate-address 10.100.10.1
//配置选举优先级低于 SC9600A。
SwichB(config-vlan-100)#ip vrrp 1 priority 25
SwichB(config-vlan-100)#quit
SwichB(config)#
//配置 BFD 会话。
SwichB(config)#bfd start
SwichB(config)#bfd track 1 vlan 100 remote-ip 10.100.10.2 local-ip 10.100.10.3
SwichB(config)#interface vlan 100
SwichB(config-vlan-100)#bfd enable
//配置 VRRP 监视 BFD 会话。
SwichB(config-vlan-100)#ip vrrp 1 track bfd-session 1
```

## 8.6 G.8032 配置

### 8.6.1 G.8032 概述

#### G.8032 的优点

ITU-T G.8032 定义了以太环网自动保护切换机制，克服了 IETF RFC3619 EAPS 的两个明显弱点：

- 故障通告丢失或因某种原因未能触发故障通告，依靠 Polling 机制检测发现故障时间较长，不能满足 50ms 保护倒换要求；
- 若链路故障是单向的，Polling 机制可能检测不到该故障并不触发保护倒换。

#### G.8032 基本概念

在正常状态下，要在环网内设置阻塞链路，以防止成环。当其他链路发生故障时，这段阻塞链路打开，流量倒换到环上的另一侧路径进行传输，实现倒换保护。在 ITU-T G.8032 中，这段链路被称为环路保护链路（RPL， Ring Protection Link），负责阻塞这段链路两端的节点，一端被称为 RPL 拥有节点（RPL Owner），另一端被称为 RPL 节点（RPL Node）。节点通过 RAPS 报文进行通信，传送 RAPS 报文的通道称为 RAPS Channel，业务流量在 Traffic Channel 中传送，与 RAPS channel 具有相同的转发状态。G.8032 能够对简单环路的进行保护的同时，同时通过子环模型实现多级环路的保护。

#### G.8032 术语解释

- Ethernet ring（以太环网）：一个环物理上对应一个环节点形连接的以太网拓扑，是一组相互连接成环的以太网交换机集合。
- ERP instance(ERP 实例)：ERP 实例是一个实体，它负责保护一个以太网环上的一组 VLAN 集。
- interconnection node（互连节点）：环上连接多个环的节点。
- major ring（主环）：连接互连节点的两个端口的以太网环。
- R-APS virtual channel（R-APS 虚通道）：子环在互连节点之间的 R-APS 信令通道。
- ring MEL（层级）：环 R-APS 信令通道对应的 MEG 的 level。
- ring protection link (RPL)：在正常状态下，要在环网内设置阻塞链路，以防止成环，当其他链路发生故障时，这段阻塞链路打开，流量倒换到环上的另一侧路径进行传输，实现倒换保护，这段链路被称为环路保护链路。

- RPL neighbour node (RPL 邻居节点)：如果配置了 RPL 邻居节点，它负责阻塞 RPL 的一个端口。
- RPL owner node (RPL 拥有节点)：环上连接 RPL 的一端并负责控制其转发状态的节点被称为 RPL 拥有节点。
- sub-ring (子环)：通过互连节点与其他环或网络连接构成的环。子环并不闭合，互连节点不属于子环。
- sub-ring link (子环链路)：连接到子环节点的链路。
- wait to block timer: 当手动倒换或者强制倒换被清除后，RPL owner 节点用 WTB 计时器来延迟恢复。

### 环保护参数介绍

1. G.8032 中定义的环节点有五种状态。
  - 1) Pending 状态：等待状态，在恢复到正常状态前的一个状态；
  - 2) Idle 状态：空闲状态，表示环路中没有任何保护请求；
  - 3) Protect 状态：保护状态，表示环路中有链路故障；
  - 4) Manual Switch 状态：手工倒换保护状态；
  - 5) Forced Switch 状态：强制保护倒换状态；
2. 环保护倒换通过两种方式触发。一种是链路保护请求，一种是通过人工保护请求。
  - 链路保护请求有：
    - 1) SF (Signal fail)：链路故障。
    - 2) NR (No request)：表示没有本地保护请求；
  - 人工保护请求是通过命令行实现的，有以下几种：
    - 1) Forced switch (FS)：强制倒换，这个命令会阻塞发起请求的端口，使业务切换；
    - 2) Manual switch (MS)：手工倒换，优先级较低，如果以太环中不存在链路故障或者强制倒换状态，就阻塞发起请求的端口，使业务切换。
    - 3) Clear：清除命令。它的作用是：1、清除人工保护请求命令即 FS 或 MS；2、在可恢复模式下，在 WTR 或者 WTB 计时器超时之前恢复到正常状态；3、在不可恢复模式下，触发环路恢复到正常状态。



3. G.8032 定义了两种保护倒换模式，可恢复模式和不可恢复模式。

### 8.6.2 G.8032 故障检测机制

G.8032 采用 Y.1731 或 IEEE 802.1ag 中定义的连续性检测（CC）进行链路双向转发检测，能够定位故障点并检测故障是单向还是双向的。当用于保护倒换时，CC 帧默认的传输周期是 3.33 ms（即每秒 300 帧的传输速率）。如图 8-13 相邻节点发送 CC 进行故障检测示意图所示。

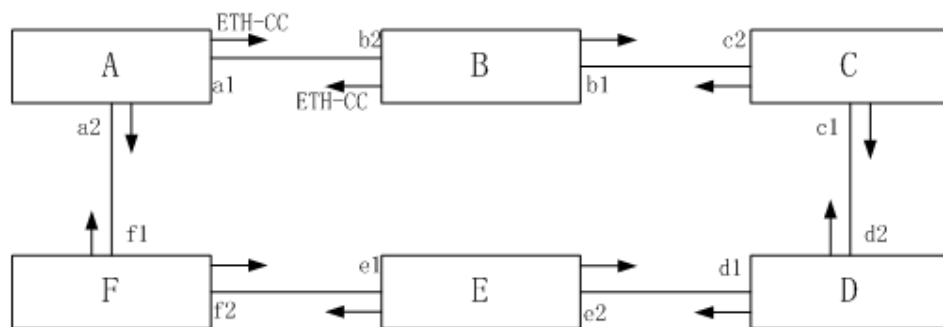


图 8-13 相邻节点发送 CC 进行故障检测示意图

两个相邻节点间周期性的从物理端口发送连续性检测（CC）帧以检测故障，当一个节点在特定的时间内检测到 CC 帧丢失，即检测到了一个故障。节点 A、B 不能收到对方发送的 CC 检测到各自端口 a1、b2 故障。如图 8-14 检测到 CC 丢失示意图所示。

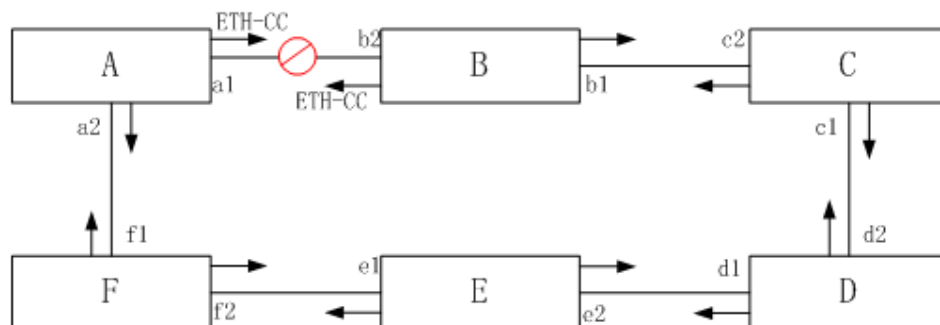


图 8-14 检测到 CC 丢失示意图

节点从检测到故障的端口发送 RDI（Remote Defect Indication）帧，如果是单向故障，链路下行的节点将检测到该 RDI 帧。节点 B 检测到来自 A 的 CC 丢失，检测到端口 b2 故障，通告 RDI 给 A。如图 8-15 单方向链路故障检测示意图所示。

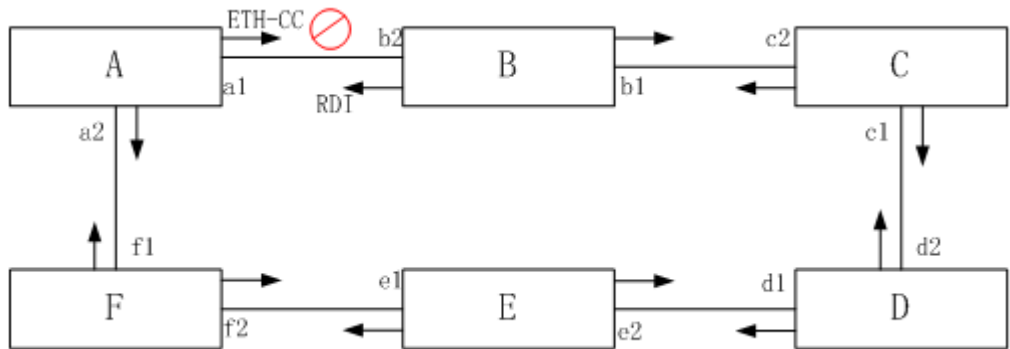


图 8-15 单方向链路故障检测示意图

如果是节点出现故障，故障节点两边相邻的节点将在特定时间内检测到 CC 帧丢失。如图 8-16 节点故障示意图所示。

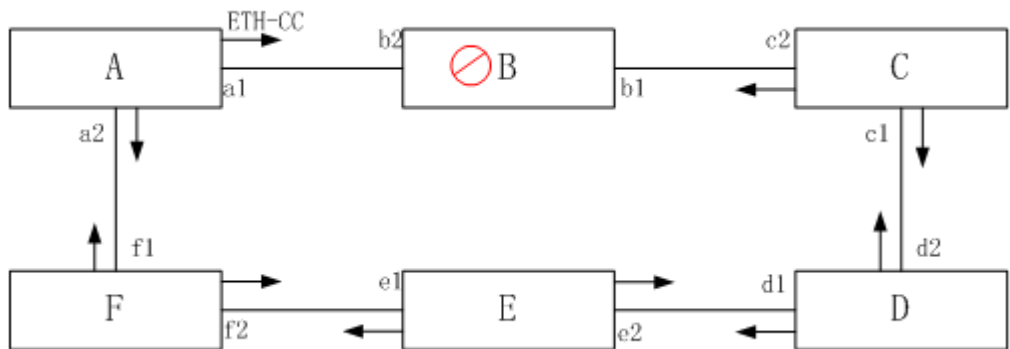


图 8-16 节点故障示意图

### 8.6.3 G.8032 单环保护倒换机制

在正常状态下，RPL 链路阻塞，如图 8-17所示。

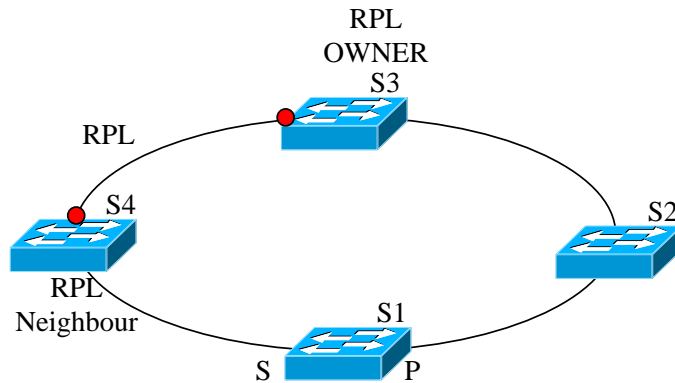


图 8-17 单环链路正常状态

环路可以通过链路故障、手工倒换和强制倒换三种方式进行倒换。这三种方式的优先级从高到低依次为：强制倒换、链路故障、手工倒换。

### 8.6.3.1 强制倒换

在环路处于 Idle 状态下，如果对环中的某个节点进行强制倒换操作，将阻塞该端口，并打开另一个端口，如果另一个端口已经处于打开状态，则不作处理。如果没有更高优先级的命令，则在两个端口都发送 FS 消息，并且刷新 MAC。

环中的其他节点接收到 RAPS-MS 消息，如果没有更高优先级的请求，则打开所有非故障阻塞端口，并且根据刷新 MAC 机制来刷新 MAC。这样，就将 RPL 链路打开了，完成了切换动作。

如果环路处于正常状态，如图 8-17所示。对 S1 的 S 端口进行强制倒换，则将该端口阻塞，并发送 RAPS-FS 消息通告环中其他节点。Owner 节点收到 RAPS-FS 消息，打开 RPL 阻塞端口，流量切换到 RPL 链路，完成了切换动作。如图 8-18所示。

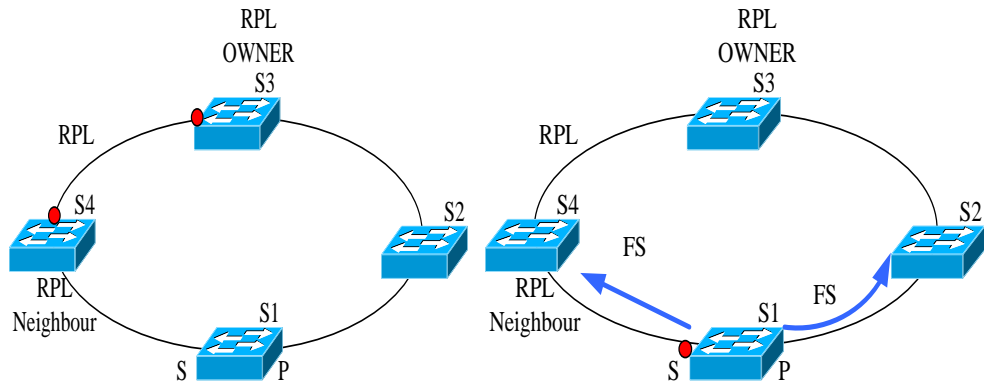


图 8-18 Idle 状态下，对 S1 强制倒换后的状态变化



注意：

- 1、如果某节点的其中一个端口已经输入了强制倒换命令，不能再对另一个端口进行强制倒换，如图 5 所示，S1 节点的 S 端口已经强制倒换了，就不能再对 P 端口再强制倒换。
- 2、如果环路中已经有一个节点强制倒换了，其他节点还可以再强制倒换，但是这样环路中就会有多处链路阻塞，会造成流量中断。

强制倒换状态可以通过 **Clear** 命令来清除。S1 接收到 **Clear** 命令之后，仍然阻塞 S 端口，并发送 NR 消息。

如果是可恢复模式，RPL Owner 节点接收到 RAPS-NR 消息之后，启动 WTB 计时器。当 WTB 计时器超时之后，产生 WTB Expires 信号，Owner 节点接收到该信号，会阻塞 RPL 端口，并发送 NR, RB 消息，其他节点接收到 NR, RB 消息，打开非故障阻塞端口。环路恢复到 Idle 状态。

如果是不可恢复模式，RPL Owner 节点接收到 RAPS-NR 消息之后，不做任何处理。如果操作者在 RPL Owner 节点上输入 **Clear** 命令时，不可恢复模式被清除，按照可恢复模式处理。

### 8.6.3.2 通过链路故障检测自动保护倒换

当检测到链路时，阻塞检测到故障的端口，同时发送 SF 信号。环中的其他节点接收到 RAPS-SF 信号，打开非故障端口，这样 RPL Owner 节点打开阻塞端口，流量切换到 RPL 链路，完成了保护倒换。整个环工作在保护状态，如图 8-19所示。

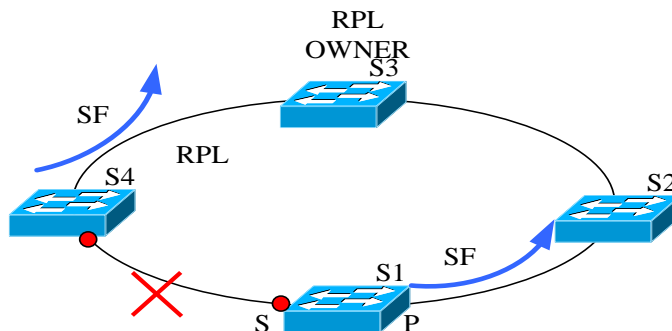


图 8-19 链路故障时环路状态

当故障链路恢复时，如果是可恢复模式，恢复链路两邻接节点仍然将端口阻塞，并发送 RAPS(NR)消息通告故障恢复，收到 RAPS(NR)的环节点转发，当 RPL Owner 收到 RAPS(NR)后，启动 WTR 定时器，等待 WTR 超时后，阻塞 RPL 端口，同时发送 RAPS(NR, RB)，此时环处于 Pending 状态，如图 8-20所示。

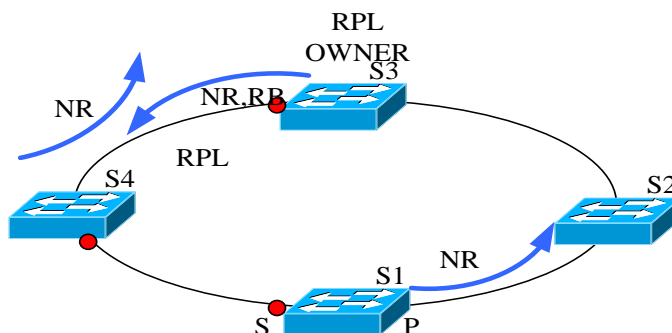


图 8-20 链路恢复时 RPL Owner 节点阻塞 RPL 端口并通告

环中节点收到 RAPS(NR, RB)消息后, 刷新 FDB, 解除阻塞端口, RPL 另一端非 RPL Owner 节点收到 RAPS(NR, RB)消息后阻塞 RPL 端口刷新 FDB, 整个环重新恢复到 Idle 状态, 如图 8-21所示。

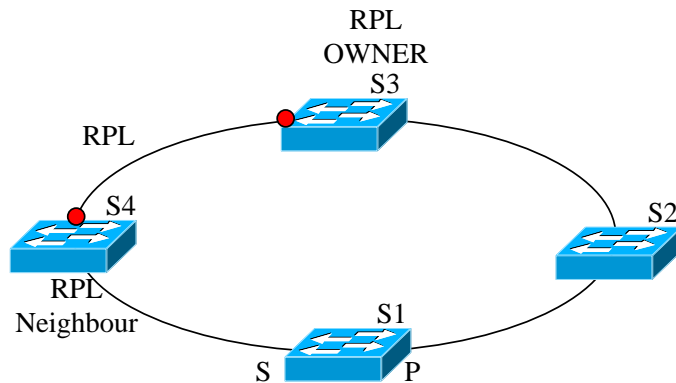


图 8-21 WTR 超时后恢复到 Idle 状态

如果是不可恢复模式, 当链路故障恢复时, 恢复链路两邻接节点仍然将端口阻塞, 并发送 RAPS-NR 消息通告故障恢复, 其他节点接收到 RAPS-NR 消息时, 不做处理。环路还是处于 Pending 状态。

当人工输入 clear 命令时, 不可恢复模式被清除, 按照可恢复模式处理。

### 8.6.3.3 手工倒换

在环路处于 Idle 状态下, 如果对环中的某个节点进行手工倒换操作, 将阻塞该端口, 并打开另一个端口, 如果另一个端口已经处于打开状态, 则不作处理。如果没有更高优先级的命令, 则在两个端口都发送 MS 消息, 并且刷新 MAC。

环中的其他节点接收到 RAPS-MS 消息, 如果没有更高优先级的请求, 则打开所有非故障阻塞端口, 并且根据刷新 MAC 机制来刷新 MAC。这样, 就将 RPL 链路打开了, 完成了切换动作。

如果环路处于正常状态, 如图 8-17所示。对 S1 的 S 端口进行手工倒换操作, 则将该端口阻塞, 并发送 RAPS-MS 消息通告环中其他节点。Owner 节点收到 RAPS-MS 消息, 打开 RPL 阻塞端口, 流量切换到 RPL 链路, 完成了切换动作。如图 8-22所示。

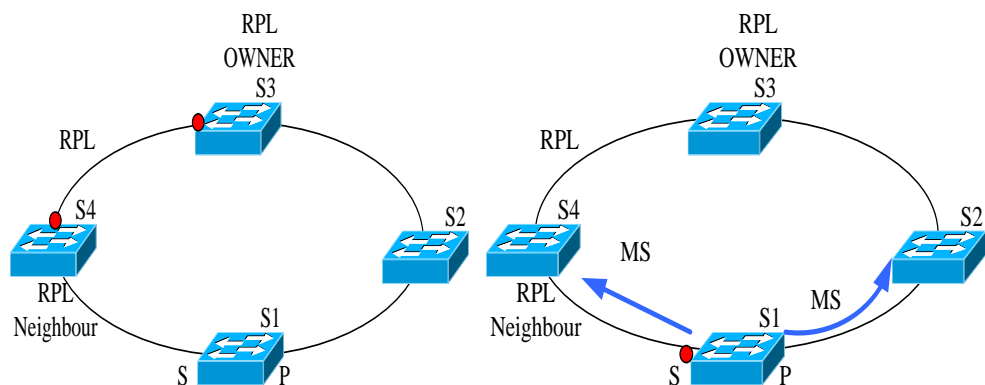


图 8-22 Idle 状态下对 S1 手工倒换后的状态变化



注意：

- 1、如果环路已经处于手工倒换状态，再对其它节点进行手工倒换，该请求将被拒绝。
- 2、发起手工倒换请求的节点，如果接收到优先级更高的命令，将清除手工倒换请求，处理优先级较高的请求。手工倒换的优先级最低。

手工倒换状态可以通过 **Clear** 命令来清除。S1 接收到 **Clear** 命令之后，仍然阻塞 S 端口，并发送 NR 消息。

如果是可恢复模式，RPL Owner 节点接收到 RAPS-NR 消息之后，启动 WTB 计时器。当 WTB 计时器超时之后，产生 WTB Expires 信号，Owner 节点接收到该信号，会阻塞 RPL 端口，并发送 NR, RB 消息，其他节点接收到 NR, RB 消息，打开非故障阻塞端口。环路恢复到 Idle 状态。

如果是不可恢复模式，RPL Owner 节点接收到 RAPS-NR 消息之后，不做任何处理。如果操作者在 RPL Owner 节点上输入 **clear** 命令时，不可恢复模式被清除，按照可恢复模式处理。

### 8.6.4 G.8032 多环单点故障保护倒换机制

G.8032 能够对单点相切的多环拓扑或通过一条共享的线路(Shared Link)互联的多环拓扑进行链路保护倒换。单点相切的多环拓扑中每一个环的保护倒换遵从简单环的保护倒换机制，而通过一条共享的线路(Shared Link)互联的多环被划分为主环和子环，Shared

Link 属于主环而不属于子环，Shared Link 的两端节点被称为互连节点，子环上互连节点之间的部分称为子环链路，子环通过互连节点在主环上的虚链路与子环链路构成一个闭合的环。通过 Shared Link 互联的环路如图 8-22所示。

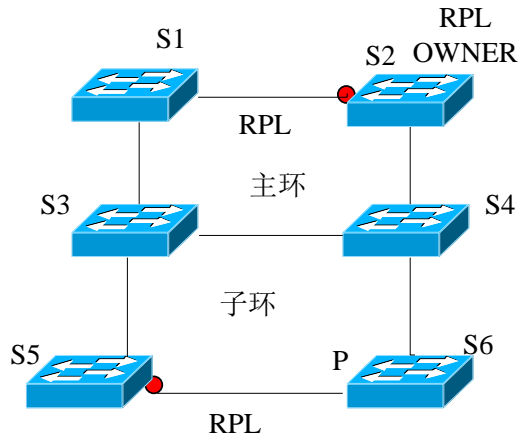


图 8-23 相交环无链路故障的状态

在图 8-23中，S3 和 S4 为互连节点，S3 和 S4 之间的链路为共享链路，共享链路属于主环。主环的链路包括 S1-S2-S4-S3-S1，子环不是一个闭合的环路，子环链路为 S5-S6，子环通过子环链路以及在主环上的虚链路构成一个环。虚链路是主环上的一条冗余链路，它是连接互连节点的链路。主环和子环中需各自配置 RPL Owner 节点，以避免成环。

如果共享链路故障，因为共享链路属于主环，主环对该故障做处理。和单环中的链路故障处理机制一样，打开 RPL 阻塞端口，完成流量切换。而子环不需要做任何动作。如图 8-24所示。



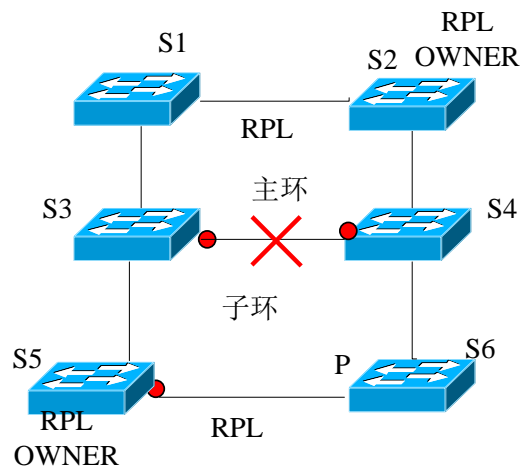


图 8-24 共享链路故障

如果子环链路故障，也是按照单环故障保护倒换机制处理。

强制倒换和手工倒换也同样适用于多环，和单环处理机制一样。

## 8.6.5 G.8032 相交环多点故障保护倒换机制

### 8.6.5.1 虚链路故障检测机制

G.8032 采用 Y.1731 中定义的连续性检测(CC)进行链路双向转发检测，能够定位故障点并检测故障是单向还是双向的，并且用于保护倒换时，CC 的发送间隔为 3.33ms。

虚链路是连接互连节点之间的链路。如图 8-25所示，虚链路有两条走向，一条是 C→D，另外一条是 C→A→B→D。如果 CD 链路故障，主环切换到保护状态，子环不做处理。在 CD 链路恢复之前，C、A、B、D 节点之间有任何一条链路故障，则判定为虚链路故障。此时，子环切换到保护状态，主环上的节点通过子环互相通信。

Y.1731 协议中规定，如果节点在 CC 发送间隔的 3.5 倍的时间内，还没接收到对端回送的 CC，就判定为链路故障。在实际工程中，环网很难在 10ms (3.33×3.5) 内完成保护倒换动作。这样，会产生一个问题。如图 8-25所示，CD 链路故障，如果主环在 10ms 内没切换到保护状态，CC 就判定主环中 AB 链路故障。这样，子环认为虚链路已经故障，就切换到保护状态。而当主环完成了保护倒换的动作时，就会形成 A→C→E→F→D→B→A 的环路，即超环。

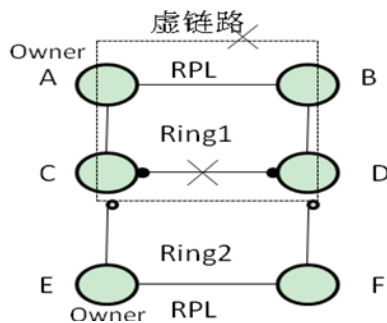


图 8-25 主环链路故障时超环的形成

为了避免这种现象，在原来的检测机之上，引入了 Holdoff timer 计时器。如图 4 所示，如果环路监测到虚链路故障，就启动 Holdoff timer。在计时器运行期间，子环不做处理，让主环有充分的时间完成保护倒换动作。这样，就避免了上述现象的发生。当计时器超时之后，如果监测到链路上还有故障，就正常通告处理。

### 8.6.5.2 多点故障保护倒换机制

虚链路故障时，子环切换到保护状态，主环通过子环进行通信。

虚链路恢复时，为了防止形成超环，当互连节点 C、D 检测到虚链路恢复时，阻塞端口 c3 和 d3，同时通告 RAPS(NR)，节点 E 作为 RPL Owner 启动 WTR 计时器，如图 8-26 所示。

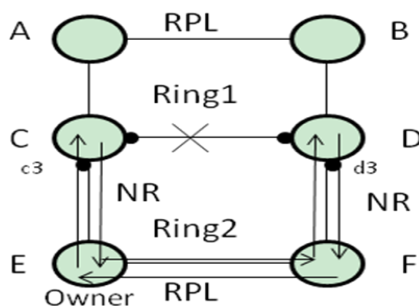


图 8-26 虚链路子环消息通告

这时由于 C、D 分别阻塞了 c3 和 c4，子环链路与主环失去了连通性，为防止这一情况的发生，引入一种新的机制。当环节点收到 RAPS(NR)或 RAPS(SF)时，如果对端的 MAC 比自己大，就开放非故障阻塞端口。按照新引入的机制，节点 C、D 收到 RAPS(NR)后，比较远端 MAC 与自己 MAC，假设节点 D 的 MAC > 节点 C 的 MAC，这时节点 C 将开放端口 c3，如图 8-27 所示。

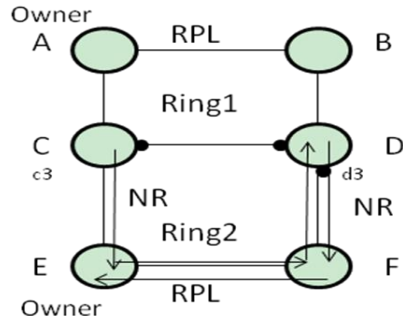


图 8-27 虚链路恢复时孤岛链路防止

当 E 节点的 WTR 超时后，阻塞 RPL 端口，并通告 RAPS(NR, RB)，按照简单环路恢复过程处理。这样，就实现了虚链路的保护。

### 8.6.6 配置 G.8032 基本功能

#### 目的

用户可以执行本节操作配置 G.8032 基本功能。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置 G8032 实例的节点角色	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>g8032</b> 从全局配置视图进入 G8032 配置视图；</li> <li>3. 执行命令 <b>g8032 instance instance-number role { rpl-owner-node   none }</b>设置 G8032 实例的节点角色；</li> <li>4. 结束。</li> </ol>
配置 G8032 实例控制通道	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>g8032</b> 从全局配置视图进入 G8032 配置视图；</li> <li>3. 执行命令 <b>g8032 instance instance-number channel channel-number</b> 设置 G8032 实例控制通道；</li> <li>4. 结束。</li> </ol>
配置 G8032 实例映射的 VLAN 列表	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>g8032</b> 从全局配置视图进入 G8032 配置视图；</li> <li>3. 执行命令 <b>g8032 instance instance-number vlan vlan-list</b> 设置 G8032 实例映射的 VLAN 列表；</li> <li>4. 结束。</li> </ol>
删除 G8032 实例映射的 VLAN	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>g8032</b> 从全局配置视图进入 G8032 配置视图；</li> </ol>

目的	步骤
列表	3. 执行命令 <b>no g8032 instance instance-num vlan vlan-list</b> 删除已配置的 G8032 实例映射的 VLAN 列表； 4. 结束。
配置接口为 G8032 实例的 port1 或 port2	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>g8032</b> 从全局配置视图进入 G8032 配置视图； 3. 执行命令 <b>g8032 instance instance-num { port1   port2 }</b> 设置接口为 G8032 实例的 port1 或 port2； 4. 结束。
对 8032 实例中的某个端口进行强制倒换	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>g8032</b> 从全局配置视图进入 G8032 配置视图； 3. 执行命令 <b>g8032 instance instance-number { port1   port2 } fs</b> 对 8032 实例中的某个端口进行强制倒换； 4. 结束。
对 G8032 实例中某个端口进行手工倒换	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>g8032</b> 从全局配置视图进入 G8032 配置视图； 3. 执行命令 <b>g8032 instance instance-number { port1   port2 } ms</b> 对 G8032 实例中某个端口进行手工倒换； 4. 结束。
配置 G8032 实例 RPL 端口	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>g8032</b> 从全局配置视图进入 G8032 配置视图； 3. 执行命令 <b>g8032 instance instance-number rpl { port1   port2   none }</b> 设置 G8032 实例 RPL 端口； 4. 结束。
配置 G8032 实例虚通道	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>g8032</b> 从全局配置视图进入 G8032 配置视图； 3. 执行命令 <b>g8032 instance instance-number virtual-channel virtual-channel-number</b> 设置 G8032 实例虚通道； 4. 结束。

附表：

参数	说明	取值
instance-number	实例号	整数形式，取值范围是<1-16>
(rpl-owner-node none)	G8032 实例的节点角色	-
channel-number	控制通道号	整数形式，取值范围是 1~4094
vlan-list	指定 VLAN 列表	整数形式，取值范围是 1~4094
(port1 port2)	G8032 实例的 PORT1 或 PORT2	-
interface-number	以太网接口号	SC9600 系列交换机支持以下 3 种型号的接口配置范围： SC9603：取值范围是

参数	说明	取值
		<1-3>/<0-4>/<1-48> SC9608 : 取值范围是 <1-8>/<0-4>/<1-48> SC9612 : 取值范围是 <1-12>/<0-4>/<1-48>
(port1 port2 none)	G8032 实例的 RPL 端口	-
virtual-channel-number	G8032 实例虚通道号	整数形式, 取值范围是 0~4094

### 8.6.7 配置 G.8032 定时器参数

#### 目的

用户可以执行本节操作配置 G.8032 定时器参数值, 调整定时器值适应网络需要。

#### 过程

根据不同目的, 执行相应步骤, 具体参见下表。

目的	步骤
配置 G8032 实例虚通道 holdoff 定时器时间	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>g8032</b> 从全局配置视图进入 G8032 配置视图;</li> <li>3. 执行命令 <b>g8032 instance instance-num vc-holdoff-timer vc-holdoff-timer</b> 设置 G8032 实例虚通道 holdoff 定时器时间;</li> <li>4. 结束。</li> </ol>
配置 G8032 实例 WTR 定时器周期值	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>g8032</b> 从全局配置视图进入 G8032 配置视图;</li> <li>3. 执行命令 <b>g8032 instance instance-number wtr-timer wtr-timer</b> 设置 G8032 实例 WTR 定时器周期值;</li> <li>4. 结束。</li> </ol>
配置 G8032 实例 Guard-Timer 定时器周期值	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>g8032</b> 从全局配置视图进入 G8032 配置视图;</li> <li>3. 执行命令 <b>g8032 instance instance-number guard-timer guard-timer</b> 设置 G8032 实例 Guard-Timer 定时器周期值;</li> <li>4. 结束。</li> </ol>
配置 G8032 实例 Hold-off-Timer 定时器周期值	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>g8032</b> 从全局配置视图进入 G8032 配置视图;</li> <li>3. 执行命令 <b>g8032 instance instance-number hold-off-timer hold-off-timer</b> 设置 G8032 实例 Hold-off-Timer 定时器周期值;</li> <li>4. 结束。</li> </ol>

附表:

参数	说明	取值
instance-num	G8032 实例号	整数形式，取值范围是 1~16
vc-holdoff-timer	holdoff 定时器时间（单位为毫秒）	整数形式，取值范围是 0~10000
w tr-timer	G8032 实例 WTR 定时器周期值	整数形式，取值范围是 5~12，单位为分钟。缺省值为 5 分钟。
guard-timer	Guard-Timer 定时器周期值	整数形式，取值范围是 10~2000，单位为毫秒。缺省值为 500ms
hold-off-timer	Hold-off-Timer 定时器周期值	整数形式，取值范围是 0~10000，单位为毫秒。缺省值为 1000ms

### 8.6.8 配置 G.8032 可选功能

#### 目的

用户可以执行本节操作配置 G.8032 可选功能，根据用户实际情况选配。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置 G8032 是否自动绑定 Y1731	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>g8032</b> 从全局配置视图进入 G8032 配置视图；</li> <li>3. 执行命令 <b>g8032 auto-bind-y1731 { enable   disable }</b> 设置 G8032 是否自动绑定 Y1731；</li> <li>4. 结束。</li> </ol>
添加或删除 G8032 实例虚通道 UP MEP 的 MIP 端口	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>g8032</b> 从全局配置视图进入 G8032 配置视图；</li> <li>3. 执行命令 <b>g8032 instance instance-num add mip-port { fastethernet   gigaethernet   xgigaethernet } mip-port -number</b> 用来添加 G8032 实例虚通道 UP MEP 的 MIP 端口或执行命令 <b>g8032 instance instance-num remove mip-port { fastethernet   gigaethernet   xgigaethernet } mip-port -number</b> 删除 G8032 实例虚通道 UP MEP 的 MIP 端口；</li> <li>4. 结束。</li> </ol>
配置 G8032 实例协议通道层级	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>g8032</b> 从全局配置视图进入 G8032 配置视图；</li> <li>3. 执行命令 <b>g8032 instance instance-num mel mel-num</b> 设置 G8032 实例协议通道层级；</li> <li>4. 结束。</li> </ol>
配置 G8032 实例的节点模式为可恢复或不可恢复	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>g8032</b> 从全局配置视图进入 G8032 配置视图；</li> <li>3. 执行命令 <b>g8032 instance instance-number mode { revertive   non-revertive }</b> 设置 G8032 实例的节点模式；</li> </ol>

目的	步骤
配置 G8032 是否自动绑定 Y1731	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>g8032</b> 从全局配置视图进入 G8032 配置视图;</li> <li>3. 执行命令 <b>g8032 auto-bind-y1731 { enable   disable }</b> 设置 G8032 是否自动绑定 Y1731;</li> <li>4. 结束。</li> </ol>
配置 G8032 实例虚通道层级	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>g8032</b> 从全局配置视图进入 G8032 配置视图;</li> <li>3. 执行命令 <b>g8032 instance instance-num vc-mel vc -mel-num</b> 设置 G8032 实例虚通道层级;</li> <li>4. 结束</li> </ol>
配置 G8032 实例虚通道 MEP 端口	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>g8032</b> 从全局配置视图进入 G8032 配置视图;</li> <li>3. 执行命令 <b>g8032 instance instance-num vc-mep { port1   port2   none }</b> 设置 G8032 实例虚通道 MEP 端口;</li> <li>4. 结束。</li> </ol>
配置 G8032 告警使能或去使能	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>g8032</b> 从全局配置视图进入 G8032 配置视图;</li> <li>3. 执行命令 <b>g8032 trap { enable   disable }</b> 设置 G8032 告警使能或去使能;</li> <li>4. 结束。</li> </ol>
配置虚链路切换开关	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>g8032</b> 从全局配置视图进入 G8032 配置视图;</li> <li>3. 执行命令 <b>g8032 vs-switch { enable   disable }</b> 设置虚链路切换开关;</li> <li>4. 结束。</li> </ol>
删除 G8032 实例	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>g8032</b> 从全局配置视图进入 G8032 配置视图;</li> <li>3. 执行命令 <b>no g8032 instance instance-num</b> 删除 G8032 实例;</li> <li>4. 结束。</li> </ol>
配置 G8032 实例版本号	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>g8032</b> 从全局配置视图进入 G8032 配置视图;</li> <li>3. 执行命令 <b>g8032 instance instance-number version { v1   v2 }</b> 配置 G8032 实例版本号;</li> <li>4. 结束。</li> </ol>
清除 G8032 实例状态	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>g8032</b> 从全局配置视图进入 G8032 配置视图;</li> <li>3. 执行命令 <b>g8032 instance instance-number clear</b> 清除 G8032 实例状态;</li> <li>4. 结束。</li> </ol>

附表：

参数	说明	取值
instance-num	G8032 实例号	整数形式，取值范围是 1-16
mip-port -number	以太网接口号	整数形式，取值范围是 <1-12>/<1-48>
mel-num	G8032 实例协议通道层级	整数形式，取值范围是 0~7
(revertive non-revertive)	G8032 实例的节点模式，分为可恢复和不可恢复	-
vc-mel-num	G8032 实例虚通道层级	整数形式，取值范围是 0~7

### 8.6.9 维护及调试

#### 目的

当 G.8032 功能不正常，需要进行查看、调试或定位问题时，可以使用本小节操作。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
打开 G8032 调试功能调试开关	<ol style="list-style-type: none"> <li>保持当前特权用户视图；</li> <li>执行命令 <b>debug g8032 { in   out   packet   sm   timer   event   all }</b> 打开 G8032 调试功能调试开关；</li> <li>结束。</li> </ol>
关闭 G8032 调试功能调试开关	<ol style="list-style-type: none"> <li>保持当前特权用户视图；</li> <li>执行命令 <b>no debug g8032 { in   out   packet   sm   timer   event   all }</b> 关闭 G8032 调试功能调试开关；</li> <li>结束。</li> </ol>
查看 G8032 的所有信息	<ol style="list-style-type: none"> <li>执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gigaethernet   xgigaethernet } interface-numbe</b>，或执行命令 <b>g8032</b> 从全局配置视图进入 G8032 配置视图或不执行任何命令保持当前特权用户视图；</li> <li>执行命令 <b>show g8032</b> 显示 G8032 的所有信息；</li> <li>结束。</li> </ol>
查看 G8032 某个实例信息或所有实例的信息	<ol style="list-style-type: none"> <li>执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gigaethernet   xgigaethernet } interface-numbe</b>，或执行命令 <b>g8032</b> 从全局配置视图进入 G8032 配置视图或不执行任何命令保持当前特权用户视图；</li> <li>执行命令 <b>show g8032 instance instance-num</b> 或执行命令 <b>show g8032 instance</b> 显示 G8032 某个实例信息或所有实例的信息；</li> <li>结束。</li> </ol>



目的	步骤
查看 G8032 实例的接口信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图, 或执行命令 <b>configure</b> 进入全局配置视图, 或执行命令 <b>interface { fastethernet   gigaethernet   xgigaethernet } interface-numbe</b>, 或执行命令 <b>g8032</b> 从全局配置视图进入 G8032 配置视图或不执行任何命令保持当前特权用户视图;</li> <li>2. 执行命令 <b>show g8032 instance instance-num interface</b> 或执行命令 <b>show g8032 instance interface</b> 显示 G8032 实例的接口信息;</li> <li>3. 结束。</li> </ol>
查看 G8032 接口信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图, 或执行命令 <b>configure</b> 进入全局配置视图, 或执行命令 <b>interface { fastethernet   gigaethernet   xgigaethernet } interface-numbe</b>, 或执行命令 <b>g8032</b> 从全局配置视图进入 G8032 配置视图或不执行任何命令保持当前特权用户视图;</li> <li>2. 执行命令 <b>show g8032 interface</b> 显示 G8032 接口信息;</li> <li>3. 结束。</li> </ol>

附表:

参数	说明	取值
interface-number	指定物理接口号	SC9600 系列交换机支持以下 3 种型号的接口配置范围: SC9603 : 取值范围是 <1-3>/<0-4>/<1-48> SC9608 : 取值范围是 <1-8>/<0-4>/<1-48> SC9612 : 取值范围是 <1-12>/<0-4>/<1-48>
timer	表示定时器的调试信息	-
in	表示协议收包的调试信息	-
out	表示协议发包的调试信息	-
packet	表示协议报文的调试信息	-
event	表示事件的调试信息	-
all	表示上述所有类型的调试信息	-
instance-num	G8032 实例号	整数形式, 取值范围是 1-16

### 8.6.10 配置举例

#### 组网要求

有三台 SC9600 高端交换机 S1、S2、S3 连接成一个单环拓扑, 如下组网图所示。现在交换机上通过配置 G.8032 功能实现环网保护功能。

组网图

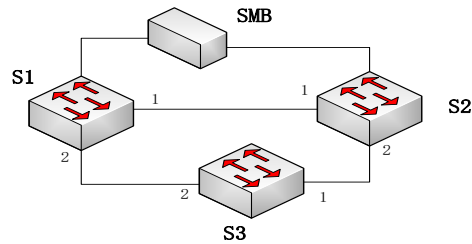


图 8-28 单环拓扑示意图

MAC 地址如下所示:

S1: 00:04:67:11:11:11、S2: 00:04:67:22:22:22、S3: 00:04:67:33:33:33

配置步骤

1、配置站点 S1。

# 配置站点 S1 的 filter 规则。

```
SC9600#config
SC9600(config)#filter-list 1
SC9600(configure-filter-l2-1)#filter 1 mac any any eth-type 0x8902
SC9600(configure-filter-l2-1)#filter 1 action redirect cpu
SC9600(configure-filter-l2-1)#quit
SC9600(config)#
```

# 配置站点 S1 的 Y.1731 功能。

```
SC9600(config)#y1731
SC9600(config-y1731)#meg vlan 1 level 6 icc v1 umc fhn1
SC9600(config-meg-v1-fhn1)#remote-mep mep-id 1 mac 00:04:67:22:22:22
SC9600(config-meg-v1-fhn1)#remote-mep mep-id 10 mac 00:04:67:33:33:33
SC9600(config-meg-v1-fhn1)#quit
SC9600(config-y1731)#quit
SC9600(config)#
```

# 配置站点 S1 的端口 1/0/1。

```
SC9600(config)#interface gigabitEthernet 1/0/1
SC9600(config-ge1/0/1)#port hybrid vlan 1-4094 tagged
```

```
SC9600(config-ge1/0/1)#filter-list in 1
SC9600(config-ge1/0/1)#y1731 mep vlan 1 level 6 mepid 1 ccm enable
SC9600(config-ge1/0/1)#y1731 mep vlan 1 level 6 mepid 1 ais enable
SC9600(config-ge1/0/1)#quit
SC9600(config)#
```

# 配置站点 S1 的端口 1/0/2。

```
SC9600(config)#interface gigabitEthernet 1/0/2
SC9600(config-ge1/0/2)# port hybrid vlan 1-4094 tagged
SC9600(config-ge1/0/2)#filter-list in 1
SC9600(config-ge1/0/2)#y1731 mep vlan 1 level 6 mepid 10 ccm enable
SC9600(config-ge1/0/2)#y1731 mep vlan 1 level 6 mepid 10 ais enable
SC9600(config-ge1/0/2)#quit
SC9600(config)#
```

# 配置站点 S1 的 G.8032 功能。

```
SC9600(config)#g8032
SC9600(config-g8032)#g8032 instance 1 role rpl-owner-node
SC9600(config-g8032)#g8032 instance 1 channel 1
SC9600(config-g8032)#g8032 instance 1 vlan 2-4094
SC9600(config-g8032)#g8032 instance 1 port1 gigabitEthernet 1/0/1
SC9600(config-g8032)#g8032 instance 1 port2 gigabitEthernet 1/0/2
SC9600(config-g8032)#g8032 instance 1 rpl port1
```

2、配置站点 S2。

# 配置站点 S2 的 filter 规则。

```
SC9600#config
SC9600(config)#filter-list 1
SC9600(config-filter-l2-1)#filter 1 mac any any eth-type 0x8902
SC9600(config-filter-l2-1)#filter 1 action redirect cpu
SC9600(config-filter-l2-1)#quit
SC9600(config)#
```

# 配置站点 S2 的 Y.1731 功能。

```
SC9600(config)#y1731
SC9600(config-y1731)#meg vlan 1 level 6 icc v1 umc fhn1
SC9600(config-meg-v1-fhn1)#remote-mep mep-id 1 mac 00:04:67:11:11:11
SC9600(config-meg-v1-fhn1)#remote-mep mep-id 10 mac 00:04:67:33:33:33
SC9600(config-meg-v1-fhn1)#quit
SC9600(config-y1731)#quit
SC9600(config)#
```

# 配置站点 S2 的端口 1/0/1。

```
SC9600(config)#interface gigabitEthernet 1/0/1
SC9600(config-gigabitEthernet 1/0/1)#port hybrid vlan 1-4094 tagged
SC9600(config-gigabitEthernet 1/0/1)#filter-list in 1
SC9600(config-gigabitEthernet 1/0/1)#y1731 mep vlan 1 level 6 mepid 2 ccm enable
SC9600(config-gigabitEthernet 1/0/1)#y1731 mep vlan 1 level 6 mepid 2 ais enable
SC9600(config-gigabitEthernet 1/0/1)#quit
SC9600(config)#
```

# 配置站点 S2 的端口 1/0/2。

```
SC9600(config)#interface gigabitEthernet 1/0/2
SC9600(config-gigabitEthernet 1/0/2)#port hybrid vlan 1-4094 tagged
SC9600(config-gigabitEthernet 1/0/2)#filter-list in 1
SC9600(config-gigabitEthernet 1/0/2)#y1731 mep vlan 1 level 6 mepid 20 ccm enable
SC9600(config-gigabitEthernet 1/0/2)#y1731 mep vlan 1 level 6 mepid 20 ais enable
SC9600(config-gigabitEthernet 1/0/2)#quit
SC9600(config)#
```

# 配置站点 S2 的 G.8032 功能。

```
SC9600(config)#g8032
SC9600(config-g8032)#g8032 instance 1 channel 1
SC9600(config-g8032)#g8032 instance 1 vlan 2-4094
SC9600(config-g8032)#g8032 instance 1 port1 gigabitEthernet 1/0/1
SC9600(config-g8032)#g8032 instance 1 port2 gigabitEthernet 1/0/2
```

3、配置站点 S3。

# 配置站点 S3 的 filter 规则。

```
SC9600#config
SC9600(config)#filter-list 1
SC9600(config-filter-l2-1)#filter 1 mac any any eth-type 0x8902
SC9600(config-filter-l2-1)#filter 1 action redirect cpu
SC9600(config-filter-l2-1)#quit
SC9600(config)#
```

# 配置站点 S3 的 Y.1731。

```
SC9600(config)#y1731
SC9600(config-y1731)# mep vlan 1 level 6 icc v1 umc fhn1
SC9600(config-meg-v1-fhn1)#remote-mep mep-id 1 mac 00:04:67:11:11:11
SC9600(config-meg-v1-fhn1)#remote-mep mep-id 10 mac 00:04:67:22:22:22
SC9600(config-y1731)#quit
SC9600(config)#
```

# 配置站点 S3 的端口 1/0/1。

```
SC9600(config)#interface gigabitEthernet 1/0/1
SC9600(config-ge1/0/1)#port hybrid vlan 1-4094 tagged
SC9600(config-ge1/0/1)#filter-list in 1
SC9600(config-ge1/0/1)#y1731 mep vlan 1 level 6 mepid 3 ccm enable
SC9600(config-ge1/0/1)#y1731 mep vlan 1 level 6 mepid 3 ais enable
SC9600(config-ge1/0/1)#quit
SC9600(config)#
```

# 配置站点 S3 的端口 1/0/2。

```
SC9600(config)#interface gigabitEthernet 1/0/2
SC9600(config-ge1/0/2)#port hybrid vlan 1-4094 tagged
SC9600(config-ge1/0/2)#filter-list in 1
SC9600(config-ge1/0/2)#y1731 mep vlan 1 level 6 mepid 30 ccm enable
SC9600(config-ge1/0/2)#y1731 mep vlan 1 level 6 mepid 30 ais enable
SC9600(config-ge1/0/2)#quit
SC9600(config)#
```

```
# 配置站点 S3 的 G.8032 功能。
SC9600(config)g8032
SC9600(config-g8032)#g8032 instance 1 channel 1
SC9600(config-g8032)#g8032 instance 1 vlan 2-4094
SC9600(config-g8032)#g8032 instance 1 port1 gigabitEthernet 1/0/1
SC9600(config-g8032)#g8032 instance 1 port2 gigabitEthernet 1/0/2
```

## 8.7 ESR 配置

### 8.7.1 ESR 概述

#### ESR 用途

以太网环路保护协议 ESR (Ethernet Service Ring) 是一个专门应用于以太网环的链路层协议。当以太网环上一条链路断开时，能迅速启用备份链路恢复环网上各个节点之间的链路通信；当以太网环完整时也能够防止数据环路引起的广播风暴。

#### ESR 优点

ESR 相较于 MSTP 而言，缩短了链路切换的收敛时间，能达到快速的保护倒换要求，满足语音、视频等高服务质量业务的需求。同时，ESR 采用多域的方式实现了链路共享，最大限度的对链路资源进行了合理利用。

#### ESR 基本概念

- ESR 域

一组配置了相同域 ID (由整数表示) 和控制 VLAN 且相互联通的交换机群体构成一个 ESR 域。

一个完整的 ESR 域包括如下组成要素：ESR 环、ESR 控制 VLAN、主节点、传输节点、边缘节点。

- ESR 环

每一个 ESR 环，物理上对应一个环形连接的以太网拓扑，由整数 ID 来表示。一个 ESR 域由彼此相接的多个 ESR 环构成，其中分为一个主环和多个子环，主环和子环通过配置时指定的级别来区分，主环的级别配置为 0，子环的级别配置为 1。

- ESR 控制 VLAN

控制 VLAN 是相对于数据 VLAN 来说的，在 ESR 域中，控制 VLAN 只用来传递 ESR 协议报文。每个 ESR 域配有两个控制 VLAN，分别为主控制 VLAN 和子控制 VLAN。主环协议报文在主控制 VLAN 中传播，子环协议报文在子控制 VLAN 中传播。

- 主节点

主节点是 ESR 环上的主要决策和控制节点。每个 ESR 环上必须有一个主节点，而且只能有一个。主节点是 Polling 机制（环网状态主动检测机制）的发起者，也是网络拓扑发生改变后执行操作的决策者。

- 传输节点

一个 ESR 环上除主节点之外的其它节点都可以称为传输节点（边缘节点和辅助边缘节点实际上是特殊的传输节点）。

传输节点负责监测自己的直连 ESR 链路的状态，并把链路变化通知主节点，然后由主节点来决策如何处理。

- 边缘节点

子环和主环会的两个交点处的交换机叫做边缘节点。

- 公共端口

公共端口是边缘节点上主环和子环公共链路两端的端口。公共链路是主环上的链路，不是子环上的链路，公共链路的状态变化只通报给主环主节点。

- 主/从端口

主节点和传输节点接入以太网环的两个端口中，一个为主端口，另一个为从端口，端口的角色由用户的配置决定。

当边缘节点做主节点时，公共端口不能作为从端口，而只能作为主端口。

## 8.7.2 配置 ESR 基本功能

### 背景信息

配置 ESR 基本功能之前，需要将接入环网的接口加入到控制 VLAN 和实例保护 VLAN 列表中。



注意：

不要将 VLAN1 作为 ESR 环的控制 VLAN 或保护 VLAN。

如果控制 VLAN 出了 ESR 协议使用外，还被其他业务所占用，则需要将其加入到保护 VLAN 列表中，以防止控制 VLAN 成环。一般情况下则不需要加入。

主环上的所有端口都需要加入主控制 VLAN 和子控制 VLAN，而子环上的端口只需要加入子控制 VLAN。子控制 VLAN 的值是主控制 VLAN 的值加 1。主控制 VLAN 和子控制 VLAN 的接口上都不允许配置 IP 地址。

子环上节点 level 值比主环节点上 level 值大，同层次环上的 level 必须一致。

### 目的

使用本节操作配置 ESR 基本功能，实现以太环网快速的链路保护倒换功能。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
创建 ESR 实例并配置其名称	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>esr</b> 进入 ESR 配置视图；</li> <li>3. 执行命令 <b>esr domain-id/ring-id name name-string</b> 配置 ESR 实例的名称；</li> <li>4. 结束。</li> </ol>
配置 ESR 实例的控制 VLAN	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>esr</b> 进入 ESR 配置视图；</li> <li>3. 执行命令 <b>esr domain-id/ring-id ctrl-vlan vlan-id</b> 配置控制 VLAN；</li> <li>4. 结束。</li> </ol>
配置 ESR 实例的保护 VLAN 列表	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>esr</b> 进入 ESR 配置视图；</li> <li>3. 执行命令 <b>esr domain-id/ring-id vlan vlan-list</b> 配置保护 VLAN 列表；</li> <li>4. 结束。</li> </ol>
配置 ESR 实例的主/从端口	<p>方法一：</p> <ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>esr</b> 进入 ESR 配置视图；</li> <li>3. 执行命令 <b>esr domain-id/ring-id { primary-port   secondary-port } { fastethernet   gigaethernet   xgigaethernet } interface-number</b> 或执行命令 <b>esr domain-id/ring-id { primary-port   secondary-port } eth-trunk trunk-number</b> 配置主/从端口；</li> <li>4. 结束。</li> </ol> <p>方法二：</p> <ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface { fastethernet   gigaethernet   xgigaethernet }</b></li> </ol>



目的	步骤
	<p><i>interface-number</i> 进入接口配置视图；</p> <p>3. 执行命令 <b>esr domain-id/ring-id { primary-port   secondary-port }</b>配置主/从端口；</p> <p>4. 结束。</p>
配置实例节点类型及环类型	<p>1. 执行命令 <b>configure</b> 进入全局配置视图；</p> <p>2. 执行命令 <b>esr</b> 进入 ESR 配置视图；</p> <p>3. 执行命令 <b>esr domain-id/ring-id mode { master   transit } level level-value</b> 使能或去使能接口 RLINK 协议；</p> <p>4. 结束。</p>
使能或去使能指定 ESR 环实例	<p>1. 执行命令 <b>configure</b> 进入全局配置视图；</p> <p>2. 执行命令 <b>esr</b> 进入 ESR 配置视图；</p> <p>3. 执行命令 <b>esr domain-id/ring-id { disable   enable }</b>使能或去使能 ESR 环实例；</p> <p>4. 结束。</p>

附表：

参数	说明	取值
interface-number	指定作为观察端口以太网接口号	<p>SC9600 系列交换机支持以下 3 种型号的接口配置范围：</p> <p>SC9603 : 取值范围是 &lt;1-3&gt;/&lt;0-4&gt;/&lt;1-48&gt;</p> <p>SC9608 : 取值范围是 &lt;1-8&gt;/&lt;0-4&gt;/&lt;1-48&gt;</p> <p>SC9612 : 取值范围是 &lt;1-12&gt;/&lt;0-4&gt;/&lt;1-48&gt;</p>
trunk-number	指定 trunk 接口号	整数形式，取值范围是 1~128
domain-id/ring-id	指定域 ID/环 ID	整数形式，取值范围是 <1-48>/<1-64>
name-string	指定 ESR 实例名称	字符串形式，不超过 16 个字符
vlan-id	指定 VLAN ID	整数形式，取值范围是 1~4094
vlan-list	指定 VLAN 列表 ID	整数形式，取值范围是 1~4094，形如：1,3,5-10
level-value	指定环等级	整数形式，取值为 0~255
master	指定为主节点	-
transit	指定为传输节点	-

### 8.7.3 配置 ESR 定时器参数

#### 背景信息



注意：

- 一般情况下只需配置主环的主节点上的 Fail 定时器值，其他站点使用默认配置即可。
- 在未使能 Fail 定时器时，直接配置 Fail 定时器值，则 Fail 定时器将自动使能。
- 建议 Fail 定时器的值为 Hello 定时器值的 3 倍以上。环中各个节点的定时器要求与主节点一致。
- 建议配置 ESR 实例的邻居节点发现定时器值在 1.5 秒以内。配置 ESR 定时器参数之前，不要使用命令 `esr enable` 使能实例，否则禁止改变定时器参数值。

### 目的

使用本节操作配置 ESR 定时器参数值。

本节操作为可选操作，用户根据实际应用情况选配。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置 Hello 报文发送失败的定时器的超时时间	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>esr</code> 进入 ESR 配置视图；</li> <li>3. 执行命令 <code>esr domain-id/ring-id fail-timer { enable   disable   fail-value }</code> 配置 Hello 报文发送失败的定时器超时时间；</li> <li>4. 结束。</li> </ol>
配置 ESR 实例的邻居节点发现定时器	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>esr</code> 进入 ESR 配置视图；</li> <li>3. 执行命令 <code>esr domain-id/ring-id hello-peer { enable   disable   peer-value }</code> 配置 ESR 实例邻居节点发现定时器值；</li> <li>4. 结束。</li> </ol>
配置 Hello 定时器超时时间	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>esr</code> 进入 ESR 配置视图；</li> <li>3. 执行命令 <code>esr domain-id/ring-id hello-timer hello-value</code> 配置 Hello 定时器超时时间值；</li> <li>4. 结束。</li> </ol>

附表：

参数	说明	取值
<code>domain-id/ring-id</code>	指定域 ID/环 ID	整数形式，取值范围是 <1-48>/<1-64>
<code>enable</code>	使能 Fail 定时器且使用默认值	-

参数	说明	取值
disable	去使能 Fail 定时器	-
fail-value	表示直接使能计时且指定 Fail 定时器超时时间	整数形式,取值范围是 340~65535,单位: 毫秒
peer-value	指定 ESR 实例的邻居节点发现定时器	整数形式,取值范围是 200~65535,单位: 毫秒
hello-value	指定 Hello 定时器超时时间	整数形式,取值范围是 200~65535,单位: 毫秒

### 8.7.4 配置 ESR 其他参数

#### 背景信息



注意:

配置 ESR 前向转发功能及其计时器时间值,此操作只能用于主环上在 transmit 节点上设置 preforward 计时器时间值,一般推荐此时间值为三倍 master 的 hello time。主要是为了,在 transmit 节点端口 up 后,没有收到 hello 报文时等待一段时间再转发,防止 hello 报文丢失时节点端口一直等待 hello 报文。

#### 目的

通过本节操作配置 ESR 相关的其他参数,包括: ESR 使用的标准、ESR 前向转发功能及其转发时间、删除已配置的 ESR 实例。

本节操作根据用户需要自行选择。

#### 过程

根据不同目的,执行相应步骤,具体参见下表。

目的	步骤
配置 ESR 使用的标准	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>esr</b> 进入 ESR 配置视图;</li> <li>3. 执行命令 <b>esr capability { default   rfc3619   huawei }</b>选择 ESR 使用的标准;</li> <li>4. 结束。</li> </ol>
使能或去使能 ESR 前向转发功能	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>esr</b> 进入 ESR 配置视图;</li> <li>3. 执行命令 <b>esr domain-id/ring-id preforward { enable   disable }</b>使能或去使能 ESR 前向转发功能;</li> </ol>

目的	步骤
	4. 结束。
配置 ESR 前向转发时间	1. 执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>esr</b> 进入 ESR 配置视图； 3. 执行命令 <b>esr esr domain-id/ring-id preforward preforward-time</b> 配置前向转发计时器值； 4. 结束。
删除所有 ESR 实例	1. 执行命令 <b>configure</b> 进入全局配置视图； 2. <b>no esr</b> 删除所有 ESR 实例； 3. 结束。
删除指定 ESR 实例的配置	1. 执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>esr</b> 进入 ESR 配置视图； 3. 执行命令 <b>no esr domain-id/ring-id</b> 删除指定 ESR 实例； 4. 结束。
解除特定接口下的指定 ESR 实例的配置	1. 执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>interface { fastethernet   gig Ethernet   xgig Ethernet } interface-number</b> 进入接口配置视图； 3. 执行命令 <b>no esr domain-id/ring-id</b> 解除特定接口下的指定 ESR 实例的配置； 4. 结束。

附表：

参数	说明	取值
default	表示电信标准	-
rfc3619	表示 RFC3619 标准	-
huaw ei	表示兼容华为标准	-
domain-id/ring-id	指定域 ID/环 ID	整数形式，取值范围是 <1-48>/<1-64>
enable	表示使能 ESR 前向转发功能	-
disable	表示去使能 ESR 前向转发功能	-
preforw ard-time	指定前向转发时间	整数形式，取值为 600~65535

### 8.7.5 维护及调试

#### 目的

当 ESR 功能不正常，需要进行查看、调试或定位问题时，可以使用本小节操作。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
----	----

目的	步骤
打开 ESR 调试功能	<ol style="list-style-type: none"> <li>1. 保持当前特权用户视图；</li> <li>2. 执行命令 <b>debug esr { in   out   protocol   packet }</b> 打开 ESR 功能调试开关；</li> <li>3. 结束。</li> </ol>
关闭 ESR 调试功能	<ol style="list-style-type: none"> <li>1. 保持当前特权用户视图；</li> <li>2. 执行命令 <b>no debug esr</b> 关闭 ESR 能调试开关；</li> <li>3. 结束。</li> </ol>
查看 ESR 配置文件信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b> 或 <b>interface eth-trunk trunk-number</b> 进入接口配置视图，或执行命令 <b>esr</b> 进入 ESR 配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show esr config</b> 显示双上行链路冗余备份功能配置文件的信息；</li> <li>3. 结束。</li> </ol>
查看 ESR 实例的端口信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b> 或 <b>interface eth-trunk trunk-number</b> 进入接口配置视图，或执行命令 <b>esr</b> 进入 ESR 配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show esr interface</b> 显示指定的 RLINK 组或全部 RLINK 组的状态信息；</li> <li>3. 结束。</li> </ol>
查看 ESR 所有环实例或指定环实例的配置信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b> 或 <b>interface eth-trunk trunk-number</b> 进入接口配置视图，或执行命令 <b>esr</b> 进入 ESR 配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show esr ring domain-id/ring-id</b> 或 <b>show esr ring</b> 显示指定的 RLINK 组或全部 RLINK 组的状态信息；</li> <li>3. 结束。</li> </ol>

附表：

参数	说明	取值
in	表示打印 ESR 环端口接收的控制报文类型	-
out	表示打印 ESR 环端口发送的控制报文类型	-
protocol	表示打印 ESR 协议内部工作情况，如定时器超时、端口状态改变、环状态改变等信息	-
packet	表示打印 ESR 数据包信息	-
domain-id/ring-id	指定域 ID/环 ID	整数形式，取值范围是 <1-48>/<1-64>
interface-number	指定接口号	SC9600 系列交换机支持以下 3 种型号的接口配置范围： SC9603：取值范围是 <1-3>/<0-4>/<1-48>

参数	说明	取值
		SC9608：取值范围是 <1-8>/<0-4>/<1-48> SC9612：取值范围是 <1-12>/<0-4>/<1-48>
trunk-number	指定 trunk 接口号	整数形式,取值范围是 1~128

## 8.7.6 配置举例

### 8.7.6.1 单环单域组网举例

#### 组网要求

六台交换机组成一个单环，在这个单环上只存在一个保护域 Domain1（保护 VLAN 为 1001~1500），主节点为 S2。

在单环拓扑中，除了主节点配置稍有不同外，其他所有传输节点的配置基本一样，即在图 8-29 中，S1、S3、S4、S5 和 S6 的配置相同。环上所有节点端口都要加入控制 VLAN2。

#### 组网图

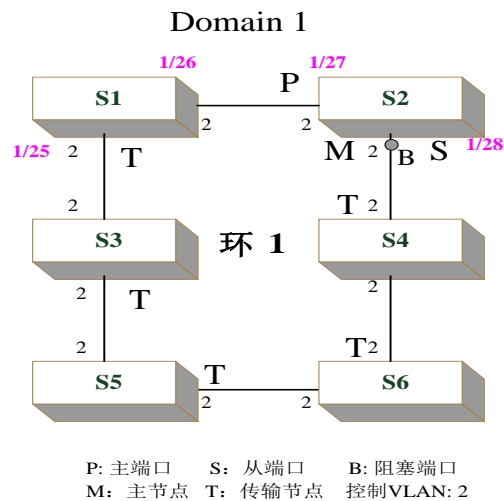


图 8-29 单环单域保护示意图

#### 配置步骤

1、配置主节点 S2。

```
S2#configure
```

```
S2(config)#esr
S2(config-esr)#esr 1/0/1 vlan 1001-1500
S2(config-esr)#esr 1/0/1 ctrl-vlan 2
S2(config-esr)# esr 1/0/1 primary-port gigabitEthernet 1/0/27
S2(config-esr)#esr 1/0/1 secondary-port gigabitEthernet 1/0/28
S2(config-esr)#esr 1/0/1 mode master level 0
S2(config-esr)#esr 1/0/1 fail-timer enable
S2(config-esr)#esr 1/0/1 enable
```

2、配置传输节点 S1。（S3/S4/S5/S6 配置类同）

```
S1#configure
S1(config)#esr
S1(config-esr)#esr 1/0/1 vlan 1001-1500
S1(config-esr)#esr 1/0/1 ctrl-vlan 2
S1(config-esr)#esr 1/0/1 primary-port gigabitEthernet 1/0/25
S1(config-esr)#esr 1/0/1 secondary-port gigabitEthernet 1/0/26
S1(config-esr)#esr 1/0/1 mode transit level 0
S1(config-esr)#esr 1/0/1 enable
```

### 8.7.6.2 多环单域组网举例

#### 组网要求

这是一个三环两点相交拓扑，在这个相交拓扑中存在三个环，这三个环都工作在一个保护域中，即域 Domain1（保护 VLAN 为 1001~1500）。主环为环 1，其主节点为 S2，环 2 和环 3 均为子环，主节点分别为 S5 和 S6。相交环需要两个控制 VLAN，即主控制 VLAN 和子控制 VLAN，主环的所有节点端口需要加入这两个 VLAN 中，而子环的所有节点端口只需要加入子控制 VLAN。公共端口在逻辑上属于主环，也要加入两个控制 VLAN 中，详细的控制 VLAN 设置，图 8-30 中已经标明。

#### 组网图

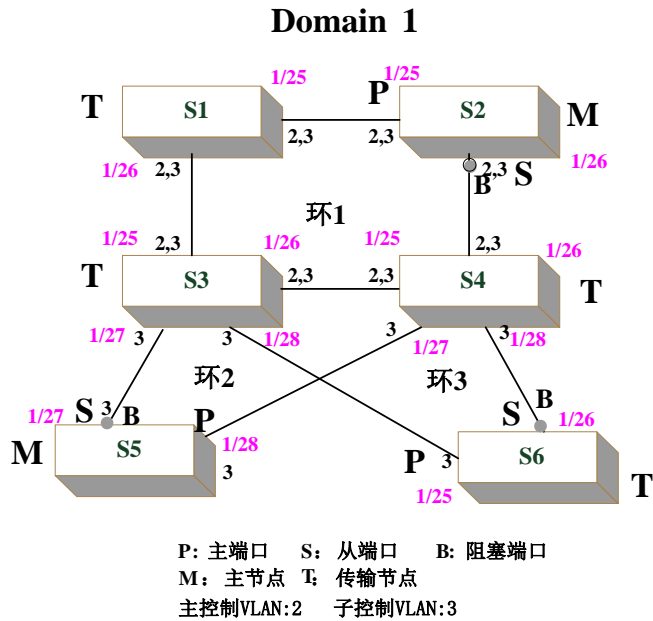


图 8-30 多环单域保护示意图

### 配置步骤

1、配置主环 1 上传输节点 S1。

```

S1#configure
S1(config)#esr
S1(config-esr)#esr 1/0/1 vlan 1001-1500
S1(config-esr)#esr 1/0/1 ctrl-vlan 2
S1(config-esr)#esr 1/0/1 primary-port gigabitEthernet 1/0/25
S1(config-esr)#esr 1/0/1 secondary-port gigabitEthernet 1/0/26
S1(config-esr)#esr 1/0/1 mode transit level 0
S1(config-esr)#esr 1/0/1 enable
  
```

2、配置主环 1 上主节点 S2。

```

S2#configure
S2(config)#esr
S2(config-esr)#esr 1/0/1 vlan 1001-1500
S2(config-esr)#esr 1/0/1 ctrl-vlan 2
S2(config-esr)#esr 1/0/1 primary-port gigabitEthernet 1/0/25
S2(config-esr)#esr 1/0/1 secondary-port gigabitEthernet 1/0/26
S2(config-esr)#esr 1/0/1 mode master level 0
  
```



```
S2(config-esr)#esr 1/0/1 fail-timer enable
```

```
S2(config-esr)#esr 1/0/1 enable
```

3、配置主环 1 上传输节点 S3。

```
S3#configure
```

```
S3(config)#esr
```

```
S3(config-esr)#esr 1/0/1 vlan 1001-1500
```

```
S3(config-esr)#esr 1/0/1 ctrl-vlan 2
```

```
S3(config-esr)#esr 1/0/1 primary-port gigabitEthernet 1/0/25
```

```
S3(config-esr)#esr 1/0/1 secondary-port gigabitEthernet 1/0/26
```

```
S3(config-esr)#esr 1/0/1 mode transit level 0
```

```
S3(config-esr)#esr 1/0/1 enable
```

4、配置子环 2 上传输节点 S3。

```
S3(config-esr)#esr 1/0/2 vlan 1001-1500
```

```
S3(config-esr)#esr 1/0/2 ctrl-vlan 3
```

```
S3(config-esr)#esr 1/0/2 primary-port gigabitEthernet 1/0/26
```

```
S3(config-esr)#esr 1/0/2 secondary-port gigabitEthernet 1/0/27
```

```
S3(config-esr)#esr 1/0/2 mode transit level 1
```

```
S3(config-esr)#esr 1/0/2 enable
```

5、配置子环 3 上传输节点 S3。

```
S3(config-esr)#esr 1/0/3 vlan 1001-1500
```

```
S3(config-esr)#esr 1/0/3 ctrl-vlan 3
```

```
S3(config-esr)#esr 1/0/3 primary-port gigabitEthernet 1/0/26
```

```
S3(config-esr)#esr 1/0/3 secondary-port gigabitEthernet 1/0/28
```

```
S3(config-esr)#esr 1/0/3 mode transit level 1
```

```
S3(config-esr)#esr 1/0/3 enable
```

6、配置主环 1 上传输节点 S4。

```
S4#configure
```

```
S4(config)#esr
```

```
S4(config-esr)#esr 1/0/1 vlan 1001-1500
```

```
S4(config-esr)#esr 1/0/1 ctrl-vlan 2
```

```
S4(config-esr)#esr 1/0/1 primary-port gigabitEthernet 1/0/25
```

```
S4(config-esr)#esr 1/0/1 secondary-port gigabitEthernet 1/0/26
```

```
S4(config-esr)#esr 1/0/1 mode transit level 0
```

```
S4(config-esr)#esr 1/0/1 enable
```

7、配置子环 2 上传输节点 S4。

```
S4(config-esr)#esr 1/0/2 vlan 1001-1500
```

```
S4(config-esr)#esr 1/0/2 ctrl-vlan 3
```

```
S4(config-esr)#esr 1/0/2 primary-port gigabitEthernet 1/0/25
```

```
S4(config-esr)#esr 1/0/2 secondary-port gigabitEthernet 1/0/27
```

```
S4(config-esr)#esr 1/0/2 mode transit level 1
```

```
S4(config-esr)#esr 1/0/2 enable
```

8、配置子环 3 上传输节点 S4。

```
S4(config-esr)#esr 1/0/3 vlan 1001-1500
```

```
S4(config-esr)#esr 1/0/3 ctrl-vlan 3
```

```
S4(config-esr)#esr 1/0/3 primary-port gigabitEthernet 1/0/25
```

```
S4(config-esr)#esr 1/0/3 secondary-port gigabitEthernet 1/0/28
```

```
S4(config-esr)#esr 1/0/3 mode transit level 1
```

```
S4(config-esr)#esr 1/0/3 enable
```

9、配置子环 2 上主节点 S5。

```
S5#configure
```

```
S5(config)#esr
```

```
S5(config-esr)#esr 1/0/2 vlan 1001-1500
```

```
S5(config-esr)#esr 1/0/2 ctrl-vlan 3
```

```
S5(config-esr)#esr 1/0/2 primary-port gigabitEthernet 1/0/28
```

```
S5(config-esr)#esr 1/0/2 secondary-port gigabitEthernet 1/0/27
```

```
S5(config-esr)#esr 1/0/2 mode master level 1
```

```
S5(config-esr)#esr 1/0/2 enable
```

10、配置子环 3 上主节点 S6。

```
S6#configure
```

```
S6(config)#esr
```

```
S6(config-esr)#esr 1/0/3 vlan 1001-1500
```

```
S6(config-esr)#esr 1/0/3 ctrl-vlan 3
```

```
S6(config-esr)#esr 1/0/3 primary-port gigabitEthernet 1/0/25
```

```
S6(config-esr)#esr 1/0/3 secondary-port gigabitEthernet 1/0/26
```

```
S6(config-esr)#esr 1/0/3 mode master level 1
```

```
S6(config-esr)#esr 1/0/3 enable
```

### 8.7.6.3 单环多域组网举例

#### 组网要求

在环 1 上，存在两个 ESR 保护域，域 1 和域 2，主节点分别为 S2 和 S5。控制 VLAN 分别为 VLAN 2 和 VLAN10，因为所有环端口即属于域 1 也属于域 2，所以所有环端口都应该加入 VLAN 2 和 VLAN10。

域 1 保护 VLAN 为 1000~2000，域 2 的保护 VLAN 为 2001~3000。

#### 组网图

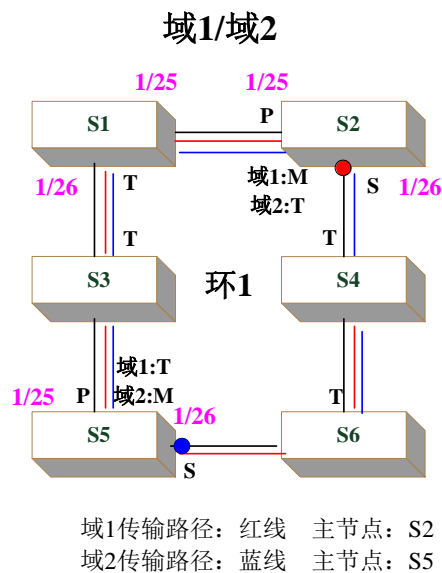


图 8-31 单环多域保护示意图

#### 配置步骤

1、配置域 1 主节点 S2。

//S2 为域 1 主节点。

```
S2#configure
```

```
S2(config)#esr
```

```
S2(config-esr)#esr 1/0/1 vlan 1000-2000
```

```
S2(config-esr)#esr 1/0/1 ctrl-vlan 2
```

```
S2(config-esr)#esr 1/0/1 primary-port gigabitEthernet 1/0/25
```

```
S2(config-esr)#esr 1/0/1 secondary-port gigabitEthernet 1/0/26
```

```
S2(config-esr)#esr 1/0/1 mode master level 0
```

```
S2(config-esr)#esr 1/0/1 fail-timer enable
```

```
S2(config-esr)#esr 1/0/1 enable
```

//S2 为域 2 传输节点。

```
S2(config-esr)#esr 2/0/1 vlan 2001-3000
```

```
S2(config-esr)#esr 2/0/1 ctrl-vlan 10
```

```
S2(config-esr)#esr 2/0/1 primary-port gigabitEthernet 1/0/25
```

```
S2(config-esr)#esr 2/0/1 secondary-port gigabitEthernet 1/0/26
```

```
S2(config-esr)#esr 2/0/1 mode transit level 0
```

```
S2(config-esr)#esr 2/0/1 enable
```

2、配置域 2 主节点 S5。

//S5 为域 1 传输节点。

```
S5#configure
```

```
S5(config)#esr
```

```
S5(config-esr)#esr 1/0/1 vlan 1000-2000
```

```
S5(config-esr)#esr 1/0/1 ctrl-vlan 2
```

```
S5(config-esr)#esr 1/0/1 primary-port gigabitEthernet 1/0/25
```

```
S5(config-esr)#esr 1/0/1 secondary-port gigabitEthernet 1/0/26
```

```
S5(config-esr)#esr 1/0/1 mode transit level 0
```

```
S5(config-esr)#esr 1/0/1 enable
```

//S5 为域 2 主节点。

```
S5(config-esr)#esr 2/0/1 vlan 2001-3000
```

```
S5(config-esr)#esr 2/0/1 ctrl-vlan 10
```

```
S5(config-esr)#esr 2/0/1 primary-port gigabitEthernet 1/0/25
```

```
S5(config-esr)#esr 2/0/1 secondary-port gigabitEthernet 1/0/26
```

```
S5(config-esr)#esr 2/0/1 mode master level 0
```

```
S5(config-esr)#esr 2/0/1 fail-timer enable
```

```
S5(config-esr)#esr 2/0/1 enable
```

3、配置其他节点。

//由于其他节点为域 1 和域 2 的传输节点，因此以 S1 为例进行说明，其他节点与 S1 的配置基本相同。

```
S1#configure
```

```
S1(config)#esr
```

```
S1(config-esr)#esr 1/0/1 vlan 1000-2000
```

```
S1(config-esr)#esr 1/0/1 ctrl-vlan 2
S1(config-esr)#esr 1/0/1 primary-port gigabitEthernet 1/0/25
S1(config-esr)#esr 1/0/1 secondary-port gigabitEthernet 1/0/26
S1(config-esr)#esr 1/0/1 mode transit level 0
S1(config-esr)#esr 1/0/1 enable
```

```
S1(config-esr)#esr 2/0/1 vlan 2001-3000
S1(config-esr)#esr 2/0/1 ctrl-vlan 10
S1(config-esr)#esr 2/0/1 primary-port gigabitEthernet 1/0/25
S1(config-esr)#esr 2/0/1 secondary-port gigabitEthernet 1/0/26
S1(config-esr)#esr 2/0/1 mode transit level 0
S1(config-esr)#esr 2/0/1 enable
```

#### 8.7.6.4 多环多域组网举例

##### 组网要求

整个拓扑存在两个 ESR 保护域，域 1 和域 2。

域 1 的保护 VLAN 为 1000~2000，域 2 的保护 VLAN 为 2001~3000。对于域 1 而言，环 1 为主环且主节点为 S2，环 2 为子环且主节点为 S5；对于域 2 而言，环 1 为主环且主节点为 S1，环 2 为子环且主节点为 S5。因此，环 1 上所有端口都应该加入域 1 的两个控制 vlan（即 VLAN 2，3）和域 2 的两个控制 vlan（即 VLAN 7，8），而环 2 的端口只需要加入域 1 的子控制 VLAN（即 VLAN 3）和域 2 的子控制 VLAN（VLAN 8），如图上标识所示。

##### 组网图

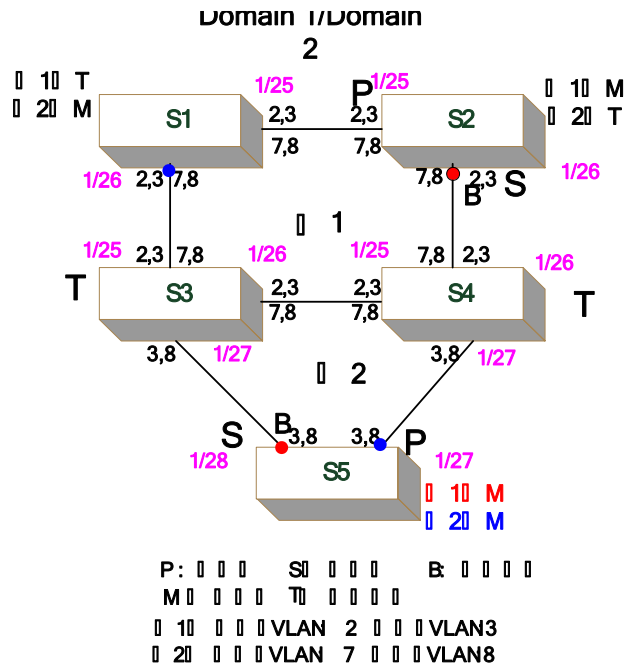


图 8-32 多环多域保护示意图

### 配置步骤

#### 1、配置 S1。

```
S1(config-esr)#esr 1/0/1 vlan 1000-2000
S1(config-esr)#esr 1/0/1 ctrl-vlan 2
S1(config-esr)#esr 1/0/1 primary-port gigabernet 1/0/25
S1(config-esr)#esr 1/0/1 secondary-port gigabernet 1/0/26
S1(config-esr)#esr 1/0/1 mode transit level 0
S1(config-esr)#esr 1/0/1 enable
```

```
S1(config-esr)#esr 2/0/1 vlan 2001-3000
S1(config-esr)#esr 2/0/1 ctrl-vlan 7
S1(config-esr)#esr 2/0/1 primary-port gigabernet 1/0/25
S1(config-esr)#esr 2/0/1 secondary-port gigabernet 1/0/26
S1(config-esr)#esr 2/0/1 mode master level 0
S1(config-esr)#esr 2/0/1 fail-timer enable
S1(config-esr)#esr 2/0/1 enable
```

#### 2、配置 S2。

```
S2(config-esr)#esr 1/0/1 vlan 1000-2000
S2(config-esr)#esr 1/0/1 ctrl-vlan 2
S2(config-esr)#esr 1/0/1 primary-port gigabitEthernet 1/0/25
S2(config-esr)#esr 1/0/1 secondary-port gigabitEthernet 1/0/26
S2(config-esr)#esr 1/0/1 mode master level 0
S2(config-esr)#esr 1/0/1 fail-timer enable
S2(config-esr)#esr 1/0/1 enable
```

```
S2(config-esr)#esr 2/0/1 vlan 2001-3000
S2(config-esr)#esr 2/0/1 ctrl-vlan 7
S2(config-esr)#esr 2/0/1 primary-port gigabitEthernet 1/0/25
S2(config-esr)#esr 2/0/1 secondary-port gigabitEthernet 1/0/26
S2(config-esr)#esr 2/0/1 mode transit level 0
S2(config-esr)#esr 2/0/1 enable
```

### 3、配置 S3。

\*\*\*\*\* S3 上域 1 的配置 \*\*\*\*\*

```
S3(config-esr)#esr 1/0/1 vlan 1000-2000
S3(config-esr)#esr 1/0/1 ctrl-vlan 2
S3(config-esr)#esr 1/0/1 primary-port gigabitEthernet 1/0/25
S3(config-esr)#esr 1/0/1 secondary-port gigabitEthernet 1/0/26
S3(config-esr)#esr 1/0/1 mode transit level 0
S3(config-esr)#esr 1/0/1 enable
```

```
S3(config-esr)#esr 1/0/2 vlan 1000-2000
S3(config-esr)#esr 1/0/2 ctrl-vlan 3
S3(config-esr)#esr 1/0/2 primary-port gigabitEthernet 1/0/26
S3(config-esr)#esr 1/0/2 secondary-port gigabitEthernet 1/0/27
S3(config-esr)#esr 1/0/2 mode transit level 1
S3(config-esr)#esr 1/0/2 enable
```

\*\*\*\*\* S3 上域 2 的配置 \*\*\*\*\*

```
S3(config-esr)#esr 2/0/1 vlan 2001-3000
S3(config-esr)#esr 2/0/1 ctrl-vlan 7
```

```
S3(config-esr)#esr 2/0/1 primary-port gigabitEthernet 1/0/25
S3(config-esr)#esr 2/0/1 secondary-port gigabitEthernet 1/0/26
S3(config-esr)#esr 2/0/1 mode transit level 0
S3(config-esr)#esr 2/0/1 enable
```

```
S3(config-esr)#esr 2/0/2 vlan 2001-3000
S3(config-esr)#esr 2/0/2 ctrl-vlan 8
S3(config-esr)#esr 2/0/2 primary-port gigabitEthernet 1/0/26
S3(config-esr)#esr 2/0/2 secondary-port gigabitEthernet 1/0/27
S3(config-esr)#esr 2/0/2 mode transit level 1
S3(config-esr)#esr 2/0/2 enable
```

#### 4、配置 S4。

S4 的配置与 S3 基本相同，请参考 S3 的配置。

#### 5、配置 S5。

```
S5(config-esr)#esr 1/0/2 vlan 1000-2000
S5(config-esr)#esr 1/0/2 ctrl-vlan 3
S5(config-esr)#esr 1/0/2 primary-port gigabitEthernet 1/0/27
S5(config-esr)#esr 1/0/2 secondary-port gigabitEthernet 1/0/28
S5(config-esr)#esr 1/0/2 mode master level 1
S5(config-esr)#esr 1/0/2 enable
```

```
S5(config-esr)#esr 2/0/2 vlan 2001-3000
S5(config-esr)#esr 2/0/2 ctrl-vlan 8
S5(config-esr)#esr 2/0/2 primary-port gigabitEthernet 1/0/28
S5(config-esr)#esr 2/0/2 secondary-port gigabitEthernet 1/0/27
S5(config-esr)#esr 2/0/2 mode master level 1
S5(config-esr)#esr 2/0/2 enable
```

## 8.8 EFM 配置

### 8.8.1 EFM 概述

#### EFM 的用途



EFM(Ethernet in the First Mile)是 IEEE802.3ah 协议 OAM(Operations Administration and Maintenance)部分的简称。EFM 主要定义用户接入网络(Subscriber Access Network)的 OAM,可以用于安装、监测和维护以太网和城域网,能够运行在任何全双工的点到点或者仿真的点到点以太网链路上,但不能在一个以太网中的多跳之间传播。

### EFM 支持的三种类型协议报文

目前我司支持的 EFM 报文有以下三种类型:

- Information EFM PDU: 将本地 EFM 信息通告给对端设备;
- Link Event Notification EFM PDU: EFM 实例检测到差的链路性能后通告给对端设备;
- Remote LoopBack Control EFM PDU: 控制对端使能或禁用环回模式。



说明:

IEEE 802.3ah 协议常用的简称是 EFM、Link OAM。

以太网 OAM 协议是一类协议族的统称。

## 8.8.2 SC9600 支持的 EFM 特性

### 链路发现

EFM 建立链接的过程也叫作 Discovery 过程,Discovery 阶段是以太网 EFM 的第一阶段。在这个过程中,相连的以太网 EFM 实例通过交互 Information PDU 向对端通告自己的 EFM 配置信息及本地节点支持的 EFM 能力信息。EFM 实例收到对端的信息后,决定是否同意建立连接,如果两端都是 PASSIVE 模式,则不会建立连接。若两端都同意了对端的 EFM 信息,连接成功并开始工作。

EFM 连接建立成功之后,两端仍然会在一定间隔时间内发送 EFM PDU 来保持连接信息,如果在 link\_lost\_time 时间内没有收到对方的 EFM PDU,则认为连接失败。

### 远端环回

EFM 实例通过发送 loopback control EFM PDU 能够将远端设置为环回模式。环回模式能够帮助管理人员在安装和检测以太网故障时保证链路的质量。在环回模式下,除了 EFM PDU 和 Pause 帧以外的其它所有接收到的帧都从原端口发送回去,环回状态期间,仍然需要周期性的交互 EFM PDU 来维持 EFM 链路发现功能。

对端 EFM 实例收到环回命令后，必须在一定时间间隔内通过响应一个环回状态相关标志设置的 Information EFM PDU 来通告自己处于环回模式，否则发送方将认为设置超时。管理人员能够通过它来估算链路是否满足服务级要求，同时它能够帮助测试延时、抖动和吞吐量。

当接口处于环回模式时，接口将不再参与二层和三层协议的运行，比如生成树协议和 OSPF 协议，因为当两个端口处于环回阶段时，除了 EFM PDU 外的其它数据帧都不会送往 CPU，非 EFM PDU 在 MAC 层就被环回或者丢弃。



注意：

只有 Active 模式的 EFM 实体才有权限设置对端为环回状态。如果两端都是 Active，一端已经发出远端环回命令，并且正在等待对端响应时又收到了对端的远端环回命令，则比较两端的 MAC 地址大小，如果本地 MAC 地址小，则不予理睬；否则本地进入环回状态。

### 链路监控

链路监控用于检测和发现链路层的故障。当本地发生一个设置完成的链路故障时，将会向对端发送一个 Event Notification PDU 通告对方本地发生的错误，同时将此错误记录在错误日志中。错误事件包括以下四种：

- 错误 symbol 周期：检测单位时间内的错误 symbol 数量是否超出了设置的阈值。根据 IEEE 802.3ah 协议，这里的检测窗口大小设置为单位时间内总的 symbol 数量，该错误事件相当于检测在一定 symbol 数量中错误的 symbol 数量。
- 错误帧：检测在指定帧数量中错误的帧数量是否超出了设置的阈值。
- 错误帧周期：检测单位时间内的错误帧数量是否超出了设置的阈值。
- 错误帧秒：检测指定时间内（秒的倍数）错误秒的数量是否超出了设置的阈值。

### 链路故障通告

链路故障通告是指当 EFM 实例所在接口发生严重故障事件后，发送一个带有特殊标志位的故障消息通告对端设备，同时将故障事件记入日志。对端 EFM 实例接收故障消息后，也会将故障事件记入日志。

以下三种错误事件会通告对端：

- **Link Fault**（链路故障）：接受端检测到信号的丢失。比如对端的光信号故障。这个功能仅仅当链路支持发送和接受相互独立（即单向传输）时才能够支持。目前暂不支持 IEEE 802.3ah 在非单向传输的情况下实现 Link Fault。
- **Dying Gasp**（致命错误）：指电源中断时的最后一口气。（目前版本暂不支持）
- **Critical Event**（用户自定义的紧急事件）：由各厂家来决定此紧急事件的类型。目前我司已支持 IEEE 802.3ah 提供的如下自定义关键事件：接口禁用 IEEE 802.3ah（包括网管禁能、协议强制禁能、物理接口加入聚合接口、热插拔等）和设备热重启（如网管重启、设备异常重启等。）

### 8.8.3 配置 EFM 链路发现

#### 背景信息

使能接口的 EFM 协议之后，接口的参数都采用默认值如下所示：

- EFM 模式：Active
- EFMPDU 的最大发送速率：10/每间隔
- EFMPDU 的最小发送间隔：1 秒
- EFM 的发现超时时间：5 秒
- 环回功能：不支持
- 链路检测：支持

若在发现过程完成后再设置 EFM 模式，将重新开始发现过程；若两端设备接口是 passive 模式，则发现过程将失败。

#### 目的

本节介绍如何配置 EFM 链路发现功能，包括：使能与禁用接口 EFM 协议、设置接口 EFM 模式、EFM PDU 最大发送速率、EFM PDU 最小发送间隔和 EFM 发现超时时间等操作。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
使能或禁用接口 EFM 协议	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface gigabitEthernet interface-number</b> 进入以太网接口配置视图或执行命令 <b>interface eth-trunk trunk-number</b> 进入 trunk 接口配置视图；</li> </ol>

目的	步骤
	3. 执行命令 <b>efm { enable   disable }</b> 使能或禁用接口 EFM 协议； 4. 结束。
设置接口 EFM 模式	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>interface gigabitEthernet interface-number</b> 进入以太网接口配置视图或执行命令 <b>interface eth-trunk trunk-number</b> 进入 trunk 接口配置视图； 3. 执行命令 <b>efm mode { active   passive }</b> 指定接口 EFM 模式； 4. 结束。
设置 EFM 协议数据单元最大发送速率	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>interface gigabitEthernet interface-number</b> 进入以太网接口配置视图或执行命令 <b>interface eth-trunk trunk-number</b> 进入 trunk 接口配置视图； 3. 执行命令 <b>efm max-rate { rate   default }</b> 指定 EFM PDU 最大发送速率； 4. 结束。
设置 EFM 协议数据单元最小发送间隔	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>interface gigabitEthernet interface-number</b> 进入以太网接口配置视图或执行命令 <b>interface eth-trunk trunk-number</b> 进入 trunk 接口配置视图； 3. 执行命令 <b>efm min-rate { rate   default }</b> 指定 EFM PDU 最小发送间隔； 4. 结束。
设置 EFM 的发现超时时间	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>interface gigabitEthernet interface-number</b> 进入以太网接口配置视图或执行命令 <b>interface eth-trunk trunk-number</b> 进入 trunk 接口配置视图； 3. 执行命令 <b>efm timeout { timeout-value   default }</b> 指定 EFM 发现超时时间； 4. 结束。

附表：

参数	说明	取值
interface-number	以太网接口号	SC9600 系列交换机支持以下 3 种型号的接口配置范围： SC9603: 取值范围是<1-3>/<0-4>/<1-48> SC9608: 取值范围是<1-8>/<0-4>/<1-48> SC9612: 取值范围是<1-12>/<0-4>/<1-48>
trunk-number	汇聚接口号	整数形式，取值范围是<1-8>
active	指定为主动模式	-
passive	指定为被动模式	-
rate	指定 EFMPDU 的最大发送速率	整数形式，取值范围是 1~10
default	指定为默认值	10
rate	指定 EFMPDU 的最小发送间隔	整数形式，取值范围是 1~10

参数	说明	取值
default	指定为默认值	1 秒
timeout-value	指定 EFM 发现超时时间	整数形式，取值范围是 2~30，单位：秒
defult	指定为默认值	5 秒

### 8.8.4 配置 EFM 远端环回

#### 背景信息

- 使能远端环回必须先保证两端的 EFM 实例都支持 EFM 远端环回功能，否则设置失败。
- 只有 Active 模式的 EFM 实例才能发起远端环回命令。如果 Active 已经处于了环回状态，即有另一个 Active 模式的 EFM 实例设置本地为远端环回，则在本地 EFM 实例上使能与禁用远端环回是无效的，只能通过对端来使能和禁用。
- EFM 远端环回具有超时自动取消功能，可以避免用户忘记停止禁用 EFM 远端环回而造成链路长时间无法正常转发业务数据。

#### 目的

本节介绍如何配置 EFM 远端环回功能，包括：使能或禁用环回功能、配置是否支持环回功能、环响应超时时间、远端环回持续时间等操作。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
开启 EFM 远端环回功能	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface gigæthernet interface-number</b> 进入以太网接口配置视图或执行命令 <b>interface eth-trunk trunk-number</b> 进入 trunk 接口配置视图；</li> <li>3. 执行命令 <b>efm remote-loopback start</b> 开启远端环回功能；</li> <li>4. 结束。</li> </ol>
关闭 EFM 远端环回功能	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface gigæthernet interface-number</b> 进入以太网接口配置视图或执行命令 <b>interface eth-trunk trunk-number</b> 进入 trunk 接口配置视图；</li> <li>3. 执行命令 <b>efm remote-loopback stop</b> 开启远端环回功能；</li> <li>4. 结束。</li> </ol>
配置接口支持或不支持 EFM 远端环回功能	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface gigæthernet interface-number</b> 进入以太网接口配置视图或执行命令 <b>interface eth-trunk trunk-number</b> 进入 trunk 接口配置视图；</li> <li>3. 执行命令 <b>efm remote-loopback { supported   unsupported }</b>指定接口是否</li> </ol>

目的	步骤
	支持远端环回功能； 4. 结束。
设置 EFM 远端环回响应超时时间	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>interface gigabitEthernet interface-number</b> 进入以太网接口配置视图或执行命令 <b>interface eth-trunk trunk-number</b> 进入 trunk 接口配置视图； 3. 执行命令 <b>efm remote-loopback timeout { timeout-value   default }</b> 指定远端环回响应超时时间； 4. 结束。
设置 EFM 远端环回持续时间	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>interface gigabitEthernet interface-number</b> 进入以太网接口配置视图或执行命令 <b>interface eth-trunk trunk-number</b> 进入 trunk 接口配置视图； 3. 执行命令 <b>efm remote-loopback start holdtime { holdtime-value   default }</b> 指定远端环回持续时间； 4. 结束。

附表：

参数	说明	取值
interface-number	以太网接口号	SC9600 系列交换机支持以下 3 种型号的接口配置范围： SC9603: 取值范围是<1-3>/<0-4>/<1-48> SC9608: 取值范围是<1-8>/<0-4>/<1-48> SC9612: 取值范围是<1-12>/<0-4>/<1-48>
trunk-number	汇聚接口号	整数形式，取值范围是<1-8>
supported	表示支持远端环回	-
unsupported	表示不支持远端环回	-
timeout-value	指定远端环回响应超时时间	整数形式，取值范围是 1~10，单位：秒
default	指定为默认值	1 秒
holdtime-value	指定远端环回持续时间	整数形式，取值范围是 0~1000，单位：分钟
default	指定为默认值	20 分钟

### 8.8.5 配置 EFM 链路监控

#### 目的

本节介绍如何配置 EFM 链路监控功能，包括：配置是否支持链路检测功能、错误 symbol 周期的窗口与门限、错误帧的窗口与门限、错误帧周期的窗口与门限、错误帧秒的窗口与门限、错误发生时的操作（接口联动）以及 EFM 联动接口自动恢复为 UP 的延迟时间等操作。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置是否支持 EFM 链路检测功能	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface gigabernet interface-number</b> 进入以太网接口配置视图或执行命令 <b>interface eth-trunk trunk-number</b> 进入 trunk 接口配置视图；</li> <li>3. 执行命令 <b>efm link-monitor { supported   unsupported }</b> 指定支持或不支持链路检测功能；</li> <li>4. 结束。</li> </ol>
配置错误帧的窗口与门限	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface gigabernet interface-number</b> 进入以太网接口配置视图或执行命令 <b>interface eth-trunk trunk-number</b> 进入 trunk 接口配置视图；</li> <li>3. 执行命令 <b>efm link-monitor frame threshold threshold value rangewindow window {window value range  default}</b> 指定错误帧的窗口与门限；</li> <li>4. 结束。</li> </ol>
配置禁用 EFM 错误帧检测功能	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface gigabernet interface-number</b> 进入以太网接口配置视图或执行命令 <b>interface eth-trunk trunk-number</b> 进入 trunk 接口配置视图；</li> <li>3. 执行命令 <b>no efm link-monitor frame</b> 禁用错误帧检测功能；</li> <li>4. 结束。</li> </ol>
配置错误帧周期的窗口和门限	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface gigabernet interface-number</b> 进入以太网接口配置视图或执行命令 <b>interface eth-trunk trunk-number</b> 进入 trunk 接口配置视图；</li> <li>3. 执行命令 <b>efm link-monitor frame-period threshold threshold value rangewindow window {window value range  default}</b> 指定错误帧周期的窗口和门限；</li> <li>4. 结束。</li> </ol>
配置禁用 EFM 错误帧周期检测功能	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface gigabernet interface-number</b> 进入以太网接口配置视图或执行命令 <b>interface eth-trunk trunk-number</b> 进入 trunk 接口配置视图；</li> <li>3. 执行命令 <b>no efm link-monitor frame-period</b> 禁用错误帧周期检测；</li> <li>4. 结束。</li> </ol>
配置错误帧秒的窗口和门限	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface gigabernet interface-number</b> 进入以太网接口配置视图或执行命令 <b>interface eth-trunk trunk-number</b> 进入 trunk 接口配置视图；</li> <li>3. 执行命令 <b>efm link-monitor frame-seconds threshold threshold value rangewindow window {window value range  default}</b> 指定错误帧秒的窗口和门限；</li> <li>4. 结束。</li> </ol>
配置禁用 EFM 错误帧秒的检测功能	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface gigabernet interface-number</b> 进入以太网接口配置视图或执行命令 <b>interface eth-trunk trunk-number</b> 进入 trunk 接口配置视图；</li> </ol>

目的	步骤
	<ol style="list-style-type: none"> <li>3. 执行命令 <code>no efm link-monitor frame-seconds</code> 禁用 EFM 错误帧秒检测；</li> <li>4. 结束。</li> </ol>
配置 EFM 错误 symbol 周期的窗口和门限	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface gig Ethernet interface-number</b> 进入以太网接口配置视图或执行命令 <b>interface eth-trunk trunk-number</b> 进入 trunk 接口配置视图；</li> <li>3. 执行命令 <b>efm link-monitor symbol-period threshold threshold window window value</b> 指定错误 symbol 周期的窗口和门限；</li> <li>4. 结束。</li> </ol>
配置禁用错误 symbol 周期的检测功能	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface gig Ethernet interface-number</b> 进入以太网接口配置视图或执行命令 <b>interface eth-trunk trunk-number</b> 进入 trunk 接口配置视图；</li> <li>3. 执行命令 <code>no efm link-monitor symbol-period</code> 禁用错误 symbol 周期的检测；</li> <li>4. 结束。</li> </ol>
配置发生错误时的操作	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface gig Ethernet interface-number</b> 进入以太网接口配置视图或执行命令 <b>interface eth-trunk trunk-number</b> 进入 trunk 接口配置视图；</li> <li>3. 执行命令 <code>efm link-monitor high-threshold action { disable-on-error   trap   all }</code> 指定发生错误时的操作；</li> <li>4. 结束。</li> </ol>
取消配置发生错误时的操作	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface gig Ethernet interface-number</b> 进入以太网接口配置视图或执行命令 <b>interface eth-trunk trunk-number</b> 进入 trunk 接口配置视图；</li> <li>3. 执行命令 <code>no efm link-monitor high-threshold action { disable-on-error   trap   all }</code> 取消发生错误时的操作；</li> <li>4. 结束。</li> </ol>
配置 EFM 接口联动时间	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface gig Ethernet interface-number</b> 进入以太网接口配置视图或执行命令 <b>interface eth-trunk trunk-number</b> 进入 trunk 接口配置视图；</li> <li>3. 执行命令 <code>efm link-monitor recover-period { recover time   default }</code> 指定接口联动时间；</li> <li>4. 结束。</li> </ol>
取消配置 EFM 接口联动时间（永久关闭接口）	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface gig Ethernet interface-number</b> 进入以太网接口配置视图或执行命令 <b>interface eth-trunk trunk-number</b> 进入 trunk 接口配置视图；</li> <li>3. 执行命令 <code>efm link-monitor never recover</code> 永久关闭接口；</li> <li>4. 结束。</li> </ol>

附表：

参数	说明	取值
interface-number	以太网接口号	SC9600 系列交换机支持以下 3 种型号



参数	说明	取值
		的接口配置范围： SC9603 : 取值范围是 <1-3>/<0-4>/<1-48> SC9608 : 取值范围是 <1-8>/<0-4>/<1-48> SC9612 : 取值范围是 <1-12>/<0-4>/<1-48>
trunk-number	汇聚接口号	整数形式，取值范围是<1-8>
supported	支持链路检测功能	-
unsupported	不支持链路检测功能	-
threshold value rangew indow	错误帧的门限值	整数形式，取值范围是 1-65535
w indow value range	错误帧的窗口值	整数形式，取值范围是 10-600
default	指定为默认值	1s
threshold value rangew indow	错误帧周期的门限值	整数形式，取值范围是 1-65535
w indow value range	错误帧周期窗口值	整数形式，取值范围是 165535
default	指定为默认值	10
threshold value rangew indow	错误帧秒的周期值	整数形式，取值范围是 1-900
w indow value range	错误帧秒窗口门限值	整数形式，取值范围是 100-9000
default	指定为默认值	-
threshold	配置错误帧门限值	整数形式，取值范围是 1~65535
w indow	配置错误帧窗口值	整数形式，取值范围是 1~65535
recover time	EFM 接口联动时间	整数形式，取值范围是 3~86400
default	指定为默认值	默认为 3 秒

### 8.8.6 配置 EFM 链路故障通告

#### 目的

本节介绍如何配置 EFM 链路故障通告功能。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置接口支持紧急事件	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface gigæthernet interface-number</b> 进入以太网接口配置视图或执行命令 <b>interface eth-trunk trunk-number</b> 进入 trunk 接口配置视图；</li> <li>3. 执行命令 <b>efm critical-event supported</b> 指定接口支持紧急链路故障通告功能；</li> <li>4. 结束。</li> </ol>

目的	步骤
配置接口 不支持紧急 事件	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface gigæthernet interface-number</b> 进入以太网接口配置视图或执行命令 <b>interface eth-trunk trunk-number</b> 进入 trunk 接口配置视图；</li> <li>3. 执行命令 <b>efm critical-event unsupported</b> 指定接口不支持紧急链路故障通告功能；</li> <li>4. 结束。</li> </ol>

附表：

参数	说明	取值
interface-number	以太网接口号	SC9600 系列交换机支持以下 3 种型号的接口配置范围： SC9603：取值范围是<1-3>/<0-4>/<1-48> SC9608：取值范围是<1-8>/<0-4>/<1-48> SC9612：取值范围是<1-12>/<0-4>/<1-48>
trunk-number	汇聚接口号	整数形式，取值范围是<1-8>
supported	支持紧急事件	-
unsupported	不支持紧急事件	-

### 8.8.7 维护及调试

#### 目的

当 EFM 功能不正常，需要进行查看、调试或定位问题时，可以使用本小节操作。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
打 开 EFM 调试 功能	<ol style="list-style-type: none"> <li>1. 保持当前特权用户视图；</li> <li>2. 执行命令 <b>debug efm { error   event   fsm   timer   pktsend   pktrecv   test   system   all }</b>打开 EFM 功能调试开关；</li> <li>3. 结束。</li> </ol>
关 闭 EFM 调试 功能	<ol style="list-style-type: none"> <li>1. 保持当前特权用户视图；</li> <li>2. 执行命令 <b>no debug efm { error   event   fsm   timer   pktsend   pktrecv   test   system   all }</b>关闭 EFM 功能调试开关；</li> <li>3. 结束。</li> </ol>
查看本地 EFM 实体的 具体错误 日志信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gigæthernet } interface-number</b> 或执行命令 <b>interface eth-trunk trunk-number</b> 进入接口配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show efm fault-logs all</b> 或执行命令 <b>show efm fault-logs interface { fastethernet   gigæthernet } interface-number</b> 或执行命令 <b>show efm fault-logs</b></li> </ol>

目的	步骤
	<p><b>interface eth-trunk trunk-number</b> 显示本地 EFM 实体的具体错误日志信息；</p> <p>3. 结束。</p>
查看指定接口和对端的 EFM OAM 会话信息	<p>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gigaehternet } interface-number</b> 或执行命令 <b>interface eth-trunk trunk-number</b> 进入接口配置视图，或不执行任何命令保持当前特权用户视图；</p> <p>2. 执行命令 <b>show efm session all</b> 或执行命令 <b>show efm session interface { fastethernet   gigaehternet } interface-number</b> 或执行命令 <b>show efm session interface eth-trunk trunk-number</b> 显示指定接口和对端的 EFM OAM 会话信息；</p> <p>3. 结束。</p>
查看本地 EFM 实体各种 EFMPDU 的发送和接受数量以及本地和远端的错误统计总数	<p>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gigaehternet } interface-number</b> 或执行命令 <b>interface eth-trunk trunk-number</b> 进入接口配置视图，或不执行任何命令保持当前特权用户视图；</p> <p>2. 执行命令 <b>show efm statistic all</b> 或执行命令 <b>show efm statistic interface { fastethernet   gigaehternet } interface-number</b> 或执行命令 <b>show efm statistic interface eth-trunk trunk-number</b> 显示本地 EFM 实体各种 EFMPDU 的发送和接受数量以及本地和远端的错误统计总数；</p> <p>3. 结束。</p>
查看本地接口配置信息	<p>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gigaehternet } interface-number</b> 或执行命令 <b>interface eth-trunk trunk-number</b> 进入接口配置视图，或不执行任何命令保持当前特权用户视图；</p> <p>2. 执行命令 <b>show efm status all</b> 或执行命令 <b>show efm status interface { fastethernet   gigaehternet } interface-number</b> 或执行命令 <b>show efm status interface eth-trunk trunk-number</b> 显示本地接口配置信息；</p> <p>3. 结束。</p>
查看本地设备上所有使能 EFM 的接口概要信息	<p>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gigaehternet } interface-number</b> 或执行命令 <b>interface eth-trunk trunk-number</b> 进入接口配置视图，或不执行任何命令保持当前特权用户视图；</p> <p>2. 执行命令 <b>show efm summary</b> 显示本地设备上所有使能 EFM 的接口概要信息；</p> <p>3. 结束。</p>
清除接口 EFM 日志	<p>1. 保持当前特权用户视图；</p> <p>2. 执行命令 <b>efm fault-logs clear</b> 清除接口 EFM 日志；</p> <p>3. 结束。</p>
清除设备 EFM 日志	<p>1. 保持当前特权用户视图；</p> <p>2. 执行命令 <b>efm fault-logs clear all</b> 清除设备 EFM 日志；</p> <p>3. 结束。</p>

附表：

参数	说明	取值
error	表示运行中的错误信息	-
event	表示运行中的特殊事件信息	-
fsm	表示状态机变化信息	-
timer	表示定时器溢出信息	-
pktsend	表示发包信息	-
pktrcv	表示收包信息	-
test	表示自测调试信息	-
system	表示系统调试信息	-
all	表示所有调试信息	-
interface-number	指定以太网接口号	SC9600 系列交换机支持以下 3 种型号的接口配置范围： SC9603：取值范围是<1-3>/<0-4>/<1-48> SC9608：取值范围是<1-8>/<0-4>/<1-48> SC9612：取值范围是<1-12>/<0-4>/<1-48>
trunk-number	指定汇聚接口号	整数形式，取值范围是 1~8

### 8.8.8 配置举例

#### 组网要求

用户网络通过 SwitchA 与 SwitchB 连接到 ISP 网络上。要实现以下功能：

- SwitchA 和 SwitchB 之间能够进行连通性故障检测功能，并能将检测到的错误记录到日志中。
- SwitchB 能监测本设备上接口 gigasethernet1/0/1 的错误帧、错误帧周期、错误帧秒以及错误 symbol 周期。

#### 组网图

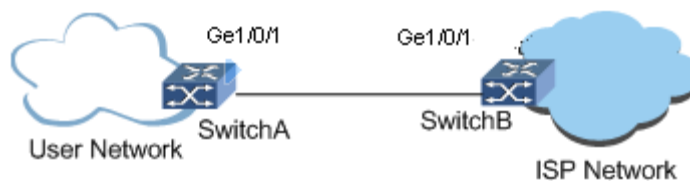


图 8-33 EFM 配置拓扑示意图

### 配置步骤

1、配置 SwitchA。

//使能 SwitchA 接口 gigaethernet1/0/1 上的 EFM 协议。

```
SC9600A#configure
```

```
SC9600A(config)#interface gigaethernet 1/0/1
```

```
SC9600A(config-ge1/0/1)#efm enable
```

//配置接口 gigaethernet1/0/1 上 EFM 模式为被动模式。

```
SC9600A(config-ge1/0/1)#efm mode passive
```

2、配置 SwitchB。

//使能 SwitchB 接口 gigaethernet1/0/1 上的 EFM 协议。

```
SC9600B#configure
```

```
SC9600B(config)#interface gigaethernet 1/0/1
```

```
SC9600B(config-ge1/0/1)#efm enable
```

//（选配）默认接口 gigaethernet1/0/1 上 EFM 模式为主动模式。

```
SC9600B(config-ge1/0/1)#efm mode active
```

//配置接口 gigaethernet1/0/1 支持链路检测功能。

```
SC9600B(config-ge1/0/1)#efm link-monitor supported
```

//配置接口 gigaethernet1/0/1 监控错误帧、错误帧周期、错误帧秒以及错误 symbol 周期。

```
SC9600B(config-ge1/0/1)#efm link-monitor frame threshold 10 window 5
```

```
SC9600B(config-ge1/0/1)#efm link-monitor frame-period threshold 10 window 5
```

```
SC9600B(config-ge1/0/1)#efm link-monitor frame-seconds threshold 10 window 100
```

```
SC9600B(config-ge1/0/1)# efm link-monitor symbol-period threshold 100 window 200
```

## 8.9 CFM 配置

### CFM 简介

IEEE 802.1ag Connectivity Fault Management（简称 CFM）定义了基于以太网承载网络的连通性故障检测、故障确认、故障定位和故障指示的 OAM 功能，适用于大规模组网的端到端场景，是网络级的 OAM。

### CFM 连通性故障管理技术的特点

CFM 连通性故障管理技术具有如下特点：

- CFM 连通性故障管理技术既是三层（IP 层）OAM 技术理念向二层以太网的延伸，也是以太网向城域网和广域网扩展的客观需要。CFM 连通性故障管理定义的故障管理功能都可以找到对应的三层 OAM 功能，如 BFD 对应连通性检测（Continuity Check Protocol）、IP Ping 对应故障确认（Loopback Protocol）、IP Trace 对应故障定位（Linktrace Protocol）等。
- CFM 定义的连通性故障检测功能支持每秒 300Hz 的发包频率，并且对不同的服务实例通过 VLAN 标记（Tagged）字段加以区分，因此特别适用于电信级以太网的保护倒换需求。

### 8.9.1 CFM 基本概念

CFM 连通性故障管理实例的基本概念介绍如下：

#### 维护域 MD（Maintenance Domain）

- MD 是指对其实施以太网连通性故障管理的一个网络或一个网络的一部分。MD 是进行 CFM 连通性故障管理的一个 VLAN 组合。维护域 MD 可以近似地理解为三层 IP 协议中的自治系统（AS），在维护域自身发出的 CFM 报文总是起始或终止于该维护域。
- 一般情况下，同一个网桥配置多个 MD，可以通过 VLAN 标记字段来区分每个 MD 的 CFM 报文。当不能通过 VLAN 标记加以区分客户、提供商及运营商数据通道的以太网业务流时，定义的 8 个 MD 等级可以用来区分属于客户、提供商及运营商的相互嵌套 MD 的 CFM 报文。
- 在客户、提供商和运营商角色之间，MD 等级默认的分配如下：  
客户角色分配三个 MD 等级：7、6 和 5；  
提供商角色分配两个 MD 等级：4 和 3；  
运营商角色分配三个 MD 等级：2、1 和 0。



注意：

在网络中划分多个维护域要注意各维护域的位置关系可以是嵌套、相切或互不相交，但绝对不允许相交的情况。

当一个网桥配置有多个 MD 时，网桥端口上的 MD 允许所属 MD 以外的带有较高等级的 CFM 报文透明地穿越而不做任何处理，并阻断所属 MD 以外的带有相同或较低等级的 CFM 报文。

### 维护联盟 MA (Maintenance Association)

MA 是 MD 的一个部分。一个 MD 可以划分一个或多个 MA，每个 MA 映射一个 VLAN，以太网 CFM 对每个 MA 分别进行连通性故障检测。

### 维护联盟边缘节点 MEP (Maintenance Association End Point)

- MEP 是 MA 的边缘节点。MEP 用于确定 CFM 连通性故障管理中每个 MA 的边界，发出和终止 CFM 报文，从而实现故障管理。
- 对于网络中运行以太网 CFM 的任意网桥，该网桥上的 MEP 称为本地 MEP，同一 MA 内其它网桥上的 MEP 相对本网桥而言，称为远端维护联盟边缘节点 RMEP (Remote Maintenance association End Point)。
- 在未配置 MEP 的网桥端口上，CFM 报文和具有相同 VLAN 标记的以太网业务流转流程相同。而在配置 MEP 的网桥端口上，MEP 可以监控和自己相同 VLAN 标记的以太网业务流 (例如对以太网业务流进行连通性检测)，并利用和自己相同 VLAN 标记与层级(MD Level)的 CFM 报文实现故障管理和性能监控。MEP 一般情况下不终止以太网业务流或更改以太网业务流的内容。
- CFM 连通性故障管理定义了两种类型 MEP 的方向：UP MEP 和 DOWN MEP。UP MEP 也称 inward MEP，可以理解为以太网业务流的上联口，关联 UNI。UP MEP 通过网桥的转发中继功能 (浪潮网络科技有限公司出品的交换机及其相关产品是通过 MEP 对应的 MIP) 发送和接收 CFM 报文，UP MEP 自身所在端口并不发送和接收 CFM 报文。这样接收的 CFM 报文看起来是在网桥内部转发的过程中终结的，因此称作 inward MEP。DOWN MEP 也称 outward MEP，可以理解为以太网业务流的下联口，关联 NNI。DOWN MEP 通过所在端口直接向以太网发送和接收 CFM 报文，不需要经由 MIP (网桥) 中继。

### 维护联盟中间节点 MIP (Maintenance Association Intermediate Point)

MIP 是 MA 中的一个中间节点，用于对某些 CFM 报文 (故障确认 CFM 报文 LBR/LBM、故障定位 CFM 报文 LTR/LTM) 做出回应。MIP 本身并不主动发送 CFM 报文。除了满足 MIP 匹配条件的故障确认和故障定位 CFM 报文外，其它 CFM 报文和以太网业务流均是透明地穿越 MIP，不做任何处理。

### CFM 连通性故障管理使用的组播 MAC 种类

- Multicast Class 1 DA:

01:80:C2:00:00:30—01:80:C2:00:00:37

- Multicast Class 2 DA:

01:80:C2:00:00:38—01:80:C2:00:00:3F



说明：

CFM 连通性故障管理既有使用单播 MAC 的操作码，也有使用组播 MAC 的操作码。其中。

---

### 8.9.2 SC9600 支持的 CFM 特性

SC9600 支持 CFM 连通性故障检测、故障确认、故障定位及故障指示等特性功能，详述如下。

#### CCM 连通性检测（CFM 连通性故障检测）

以太网连通性检测（ETH-CC, Ethernet Continuity Check）是一种主动性的 OAM 功能，是 CFM 中的一个最基本也是最重要的功能，它为 CFM 的实现提供了可能。可以将其理解为三层的 BFD 协议在二层以太网的延伸，通常使用 1 类组播 MAC。

它用于检测一个 MA 中任何一对 MEP 间连续性的丢失（LOC）。ETH-CC 也可以检测两个 MA 之间不希望有的连通性（错误混入），在 MA 内与一个不要求的 MEP（非期望的 MEP）间不希望有的连通性，以及其它故障情况（例如非期望 MD 等级、非期望的周期等）。ETH-CC 可应用于故障管理（ETH-CC 以太网连通性检测、ETH-RDI，以太网远端故障指示）或保护转换（G.8031/G.8032）的应用。CCM 帧用于支持 ETH-CC 功能、ETH-RDI 功能。ETH-CC 定义的传输周期从 3.33ms 到 10min 共 7 种，常用的有 3 种：

- 差错管理：默认的传输周期是 1 s（即每秒 1 帧的传输速率）。
- 性能监控：默认的传输周期是 100 ms（即每秒 10 帧的传输速率）。
- 保护转换：默认的传输周期是 3.33 ms（即每秒 300 帧的传输速率）。



注意：

根据 CFM 的有关定义，MEP 或 MIP 不能处理、发送或转发超过 128 字节的 CCM。

---

#### LBR/LBM 环回（CFM 连通性故障确认）



CFM 故障确认，也称以太网故障确认功能（ETH-LB），是一种按需的 CFM 功能，可以理解为 IP Ping 在二层以太网的延伸，是基于 VLAN 的二层 MAC-Ping 协议。CFM 连通性故障管理故障确认通过发送查询报文 LBM 和接收应答报文 LBR 来检测同一个 MA 内本地设备 MEP 到目的设备 MEP 或 MIP 的连通性。

CFM 故障确认消息从 MEP 发到指定 MEP（MIP），帮助 MEP 在 MA 中精确定位故障位置。故障位置前的 MIP（MEP）能够响应故障确认消息，而故障位置后的 MIP（MEP）不能够响应故障确认消息，从而实现故障的定位。

CFM 连通性故障管理故障确认有两种类型：

- 单播 Unicast ETH-LB 是基于 VLAN 的二层 MAC-Ping-MAC 协议；
- 组播 Multicast ETH-LB 使用 1 类组播 MAC，是基于 VLAN 的二层 MAC-Ping-MACs-in-VLAN 协议，LBR 都是使用单播地址。

#### LTR/LTM 链路跟踪（CFM 连通性故障定位）

CFM 故障定位，也称以太网链路追踪功能（ETH-LT），是一种按需的 CFM 功能，可以理解为 IP Trace 在二层以太网的延伸，是基于 VLAN 的二层 MAC-Trace 协议。CFM 故障确认通过发送查询报文 LTM 和接收应答报文 LTR 来检测同一个 MA 内本地设备 MEP 到目的设备 MEP 或 MIP 的路径或定位故障点。CFM 故障定位 LTM 使用 2 类组播 MAC，LTR 都是使用单播地址。

本地 MEP 发起 CFM 故障定位查询报文后，链路中所有中间 MIP 以及终结 MEP 向本地 MEP 发送 CFM 故障定位应答消息，其中 MIP 还会转发 CFM 故障定位查询消息，直到到达目的 MIP/MEP。通过 CFM 故障定位应答消息，本地 MEP 可以得到 MA 上所有 MIP 的 MAC 地址与相对发起 MEP 的位置，以及出现链路故障的位置区间。

### 8.9.3 配置 CFM 基本功能

#### 背景信息

为了实现 CFM 连通性故障管理的基本功能，最简配置步骤如下：

1. 进入 CFM 配置视图；
2. 创建 MD；
3. 创建 MA 及配置 MA 映射的 VLAN；
4. 创建 MEP 或 MIP；
5. 使能 ETH-CC。



说明：

建议在配置上述步骤之前将 MEP 或 MIP 所在端口加入事先规划好的所属 MA 对应的 VLAN，并打开该端口。当然也可以在上述步骤配置完成之后再行此配置。

在同一网桥的同一个 MA 内，创建 MEP 有如下要求：

- inward 接口型 MEP 和 outward 接口型 MEP 不能同时存在；
- 同一个 MA 内的 MEP 和 RMEP 在同一设备不能同时存在；
- 同一个 MA 内的 MEP 和 MIP 在同一个接口不能同时存在；
- 同一个 MA 内的 MEP 在同一个接口最多只有一个；
- 同一个接口下若配置了 Y.1731 的 MEP 或 MIP，则不能再配置 CFM 的 MEP。

在同一台设备的同一个 MA 内，对创建 MIP 有如下要求：

- 同一个 MA 内的 MIP 和 MEP 在同一个接口不能同时存在；
- 同一个 MA 内的 MIP 在同一个接口最多只能有一个；
- 同一个接口下创建了 Y1731 的 MIP 或 MEP，则不能再创建 CFM 的 MIP。

### 目的

在需要实现端到端的连通性检测或直连链路的连通性检测时，用户可以执行本节操作配置 CFM 基本功能。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
创建 MD 并进入 MD 配置视图	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>cfm</b> 从全局配置视图进入 CFM 配置视图；</li> <li>3. 执行命令 <b>md name name level level</b> 用来创建 MD 并进入 MD 配置视图，若该 MD 已存在，则用来进入 MD 配置视图；</li> <li>4. 结束。</li> </ol>
（根据需要选配）删除指定的 MD 或所有 MD	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>cfm</b> 从全局配置视图进入 CFM 配置视图；</li> <li>3. 执行命令 <b>no md name name</b> 删除指定的 MD 或执行命令 <b>no md all</b> 删除所有的 MD；</li> <li>4. 结束。</li> </ol>

目的	步骤
创建 MA 并进入 MA 配置视图及配置 MA 映射的 VLAN	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>cfm</b> 从全局配置视图进入 CFM 配置视图;</li> <li>3. 执行命令 <b>md name name level level</b> 用来进入 MD 配置视图;</li> <li>4. 执行命令 <b>ma name name vlan vlan-id</b> 用来创建 MA 并进入 MA 配置视图; 若该 MA 已存在, 则用来进入 MA 配置视图; 或执行命令 <b>ma vlan vlan-list</b> 批量创建 MA;</li> <li>5. 结束。</li> </ol>
(根据需要选配)删除指定 MA 或所有 MA 或批量删除指定 MA	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>cfm</b> 从全局配置视图进入 CFM 配置视图;</li> <li>3. 执行命令 <b>md name name level level</b> 用来进入 MD 配置视图;</li> <li>4. 执行命令 <b>no ma name name</b> 删除指定 MA 或执行命令 <b>no ma all</b> 删除所有 MA; 或执行命令 <b>no ma vlan vlan-list level level-value</b> 批量删除指定 MA;</li> <li>5. 结束。</li> </ol>
创建 MEP	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>interface gigæthernet interface-number</b> 进入以太网接口配置视图或执行命令 <b>interface eth-trunk trunk-number</b> 进入 trunk 接口配置视图;</li> <li>3. 执行命令 <b>cfm mep vlan vlan-id level level mepid mep-id { inward   outward }</b> 或执行命令 <b>cfm mep vlan vlan-id level level mepid mep-id</b> 创建 MEP;</li> <li>4. 结束。</li> </ol>
(根据需要选配)删除已创建的 MEP	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>interface gigæthernet interface-number</b> 进入以太网接口配置视图或执行命令 <b>interface eth-trunk trunk-number</b> 进入 trunk 接口配置视图;</li> <li>3. 执行命令 <b>no cfm mep vlan vlan-id level level mepid mep-id</b> 删除已创建的 MEP;</li> <li>4. 结束。</li> </ol>
(根据需要选配)删除指定 MA 下的所有 MEP	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>cfm</b> 从全局配置视图进入 CFM 配置视图;</li> <li>3. 执行命令 <b>md name name level level</b> 用来进入 MD 配置视图;</li> <li>4. 执行命令 <b>ma name name vlan vlan-id</b> 用来进入 MA 配置视图;</li> <li>5. 执行命令 <b>no mep all</b> 删除指定 MA 下的所有 MEP;</li> <li>6. 结束。</li> </ol>
创建 MIP	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>interface gigæthernet interface-number</b> 进入以太网接口配置视图或执行命令 <b>interface eth-trunk trunk-number</b> 进入 trunk 接口配置视图;</li> <li>3. 执行命令 <b>cfm mip vlan vlan-id level level</b> 创建 MIP;</li> <li>4. 结束。</li> </ol>
(根据需要选配)删除 MIP	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>interface gigæthernet interface-number</b> 进入以太网接口配置</li> </ol>

目的	步骤
	视图或执行命令 <b>interface eth-trunk trunk-number</b> 进入 trunk 接口配置视图； 3. 执行命令 <b>no cfm mip vlan vlan-id level level</b> 删除 MIP； 4. 结束。
（根据需要选配）删除指定 MA 下所有 MIP	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>cfm</b> 从全局配置视图进入 CFM 配置视图； 3. 执行命令 <b>md name name level level</b> 用来进入 MD 配置视图； 4. 执行命令 <b>ma name name vlan vlan-id</b> 用来进入 MA 配置视图； 5. 执行命令 <b>no mip all</b> 删除指定 MA 下所有 MIP； 6. 结束。
（根据需要选配）配置 MEP 的 MAC 地址	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>interface gigæthernet interface-number</b> 进入以太网接口配置视图或执行命令 <b>interface eth-trunk trunk-number</b> 进入 trunk 接口配置视图； 3. 执行命令 <b>cfm mep vlan vlan-id level level mepid mep-id mac mac-address</b> 配置 MEP 的 MAC 地址； 4. 结束。
（根据需要选配）配置 MIP 的 MAC 地址	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>interface gigæthernet interface-number</b> 进入以太网接口配置视图或执行命令 <b>interface eth-trunk trunk-number</b> 进入 trunk 接口配置视图； 3. 执行命令 <b>cfm mip vlan vlan-id level level mac mac-address</b> 配置 MIP 的 MAC 地址； 4. 结束。
（根据需要选配）创建或删除 MIP 自动生成的 VLAN 映射表	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>cfm</b> 从全局配置视图进入 CFM 配置视图； 3. 执行命令 <b>mip auto-config vlan vlan-list</b> 创建 MIP 自动生成的 VLAN 映射表或执行命令 <b>no mip auto-config vlan vlan-list</b> 删除 MIP 自动生成的 VLAN 映射表； 4. 结束。
（根据需要选配）创建当前 MA 内的 RMEP	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>cfm</b> 从全局配置视图进入 CFM 配置视图； 3. 执行命令 <b>md name name level level</b> 用来进入 MD 配置视图； 4. 执行命令 <b>ma name name vlan vlan-id</b> 用来进入 MA 配置视图； 5. 执行命令 <b>remote-mep mep-id mep-id mac mac-address</b> 创建当前 MA 内的 RMEP 或执行命令 <b>remote-mep mep-id mep-id-list</b> 批量创建当前 MA 内的 RMEP； 6. 结束。
（根据需要选配）删除当前 MA 内的 RMEP	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>cfm</b> 从全局配置视图进入 CFM 配置视图； 3. 执行命令 <b>md name name level level</b> 用来进入 MD 配置视图； 4. 执行命令 <b>ma name name vlan vlan-id</b> 用来进入 MA 配置视图； 5. 执行命令 <b>no remote-mep all</b> 删除指定 MA 下的所有 RMEP 或执行命令

目的	步骤
	<p><b>no remote-mep mep-id mep-id-list</b> 批量删除指定 MA 下的 RMEP;</p> <p>6. 结束。</p>
使能或禁止 MEP 的 CC 检测功能	<p>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;</p> <p>2. 执行命令 <b>interface gigæether net interface-number</b> 进入以太网接口配置视图或执行命令 <b>interface eth-trunk trunk-number</b> 进入 trunk 接口配置视图;</p> <p>3. 执行命令 <b>cfm mep vlan vlan-id level level mepid mep-id ccm priority priority { enable   disable }</b> 或执行命令 <b>cfm mep vlan vlan-id level level mepid mep-id ccm { enable   disable }</b> 使能或禁止 MEP 的 CC 检测功能;</p> <p>4. 结束。</p>
使能或禁用 MA 下所有 MEP 的 CC 检测功能	<p>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;</p> <p>2. 执行命令 <b>cfm</b> 从全局配置视图进入 CFM 配置视图;</p> <p>3. 执行命令 <b>md name name level level</b> 用来进入 MD 配置视图;</p> <p>4. 执行命令 <b>ma name name vlan vlan-id</b> 用来进入 MA 配置视图;</p> <p>5. 执行命令 <b>ccm { enable   disable }</b> 使能或禁用 MA 下所有 MEP 的 CC 检测功能;</p> <p>6. 结束。</p>

附表:

参数	说明	取值
name	指定 MD 的名称	字符串形式
level	指定 MD 级别	整数形式, 取值范围是 0~7
name	指定 MA 的名称	字符串形式
vlan-id	指定 MA 映射的 VLAN ID	整数形式, 取值范围是 1~4094
vlan-list	指定批量创建的 MAC 映射的 VLAN 列表	整数形式, 取值范围是 1~4094
level	指定 MA 级别	整数形式, 取值范围是 0~7
vlan-id	指定 VLAN ID	整数形式, 取值范围是 1~4094
level	指定级别	整数形式, 取值范围是 0~7
mep-id	指定本地 MEP ID	整数形式, 取值范围是 1~8191
inward	表示 up 方向	-
outward	表示 down 方向	-
mac-address	指定 MEP 的 MAC 地址	形如 AA:BB:CC:DD:EE:FF, 其中 A~F 取值为 一位十六进制数
mac-address	指定 MIP 的 MAC 地址	形如 AA:BB:CC:DD:EE:FF, 其中 A~F 取值为 一位十六进制数
vlan-list	指定 VLAN 映射表	整数形式, 取值范围是 1~4094
mep-id	指定 RMEP 的 ID	整数形式, 取值范围是 1~1891
mep-id-list	指定 RMEP 的 ID 列表	整数形式, 取值范围是 1~1891
mac-address	指定 RMEP 所在设备的桥 MAC 地址	形如 AA:BB:CC:DD:EE:FF, 其中 A~F 为 一位十六进制数

参数	说明	取值
all	表示当前 MA 下所有 RMEP	-

### 8.9.4 配置 CFM 相关参数

#### 目的

通过对以太网 CFM 的相关参数进行调整，可以在以太网中更好地实现端到端的连通性故障检测。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
清除 MEP 的 CFM 报文计数	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface gigæthernet interface-number</b> 进入以太网接口配置视图或执行命令 <b>interface eth-trunk trunk-number</b> 进入 trunk 接口配置视图；</li> <li>3. 执行命令 <b>cfm mep vlan vlan-id level level mepid mep-id reset counter</b> 清除 MEP 的 CFM 报文计数；</li> <li>4. 结束。</li> </ol>
配置当前 MA 内 MEP 发送 CC 消息的周期	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>cfm</b> 从全局配置视图进入 CFM 配置视图；</li> <li>3. 执行命令 <b>md name name level level</b> 用来进入 MD 配置视图；</li> <li>4. 执行命令 <b>ma name name vlan vlan-id</b> 用来进入 MA 配置视图；</li> <li>5. 执行命令 <b>ccm-interval { 300Hz   10ms   100ms   10s   1min   10min   default }</b>配置当前 MA 内 MEP 发送 CC 消息的周期；</li> <li>6. 结束。</li> </ol>
配置当前 MA 内 MEP 的 CC 丢失阈值	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>cfm</b> 从全局配置视图进入 CFM 配置视图；</li> <li>3. 执行命令 <b>md name name level level</b> 用来进入 MD 配置视图；</li> <li>4. 执行命令 <b>ma name name vlan vlan-id</b> 用来进入 MA 配置视图；</li> <li>5. 执行命令 <b>ccm loss-threshold { threshold-value   default }</b>配置当前 MA 内 MEP 的 CC 丢失阈值；</li> <li>6. 结束。</li> </ol>
清除接口的 CFM 报文计数	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface gigæthernet interface-number</b> 进入以太网接口配置视图或执行命令 <b>interface eth-trunk trunk-number</b> 进入 trunk 接口配置视图；</li> <li>3. 执行命令 <b>cfm reset counter</b> 清除接口的 CFM 报文计数；</li> <li>4. 结束。</li> </ol>
使能或禁止静态 RMEP 校验功能	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>cfm</b> 从全局配置视图进入 CFM 配置视图；</li> <li>3. 执行命令 <b>md name name level level</b> 用来进入 MD 配置视图；</li> </ol>

目的	步骤
	<ol style="list-style-type: none"> <li>4. 执行命令 <b>ma name name vlan vlan-id</b> 用来进入 MA 配置视图;</li> <li>5. 执行命令 <b>cross-check { enable   disable }</b> 使能或禁止静态 RMEP 校验功能;</li> <li>6. 结束。</li> </ol>
配置 RMEP 的激活时间	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>cfm</b> 从全局配置视图进入 CFM 配置视图;</li> <li>3. 执行命令 <b>md name name level level</b> 用来进入 MD 配置视图;</li> <li>4. 执行命令 <b>ma name name vlan vlan-id</b> 用来进入 MA 配置视图;</li> <li>5. 执行命令 <b>cross-check start-delay { delay-value   default }</b> 配置 RMEP 的激活时间;</li> <li>6. 结束。</li> </ol>
配置 MIP CCDB 的老化时间	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>cfm</b> 从全局配置视图进入 CFM 配置视图;</li> <li>3. 执行命令 <b>md name name level level</b> 用来进入 MD 配置视图;</li> <li>4. 执行命令 <b>ma name name vlan vlan-id</b> 用来进入 MA 配置视图;</li> <li>5. 执行命令 <b>mip-ccdb aging-time { aging-time   default }</b> 配置 MIP CCDB 的老化时间;</li> <li>6. 结束。</li> </ol>
配置动态 RMEP 的老化时间	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>cfm</b> 从全局配置视图进入 CFM 配置视图;</li> <li>3. 执行命令 <b>md name name level level</b> 用来进入 MD 配置视图;</li> <li>4. 执行命令 <b>ma name name vlan vlan-id</b> 用来进入 MA 配置视图;</li> <li>5. 执行命令 <b>remote-mep aging-time { aging-time   default }</b> 配置动态 RMEP 的老化时间;</li> <li>6. 结束。</li> </ol>
清除 MA 的 CFM 报文计数	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>cfm</b> 从全局配置视图进入 CFM 配置视图;</li> <li>3. 执行命令 <b>md name name level level</b> 用来进入 MD 配置视图;</li> <li>4. 执行命令 <b>ma name name vlan vlan-id</b> 用来进入 MA 配置视图;</li> <li>5. 执行命令 <b>reset counter</b> 清除 MA 的 CFM 报文计数;</li> <li>6. 结束。</li> </ol>
配置 CFM 报文的 Sender ID TLV 类型	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>cfm</b> 从全局配置视图进入 CFM 配置视图;</li> <li>3. 执行命令 <b>md name name level level</b> 用来进入 MD 配置视图;</li> <li>4. 执行命令 <b>senderid-tlv-type { none   chassis   manage   chassis-manage   defer }</b> 配置 CFM 报文的 Sender ID TLV 类型;</li> <li>5. 结束。</li> </ol>
配置 LTR 应答响应的老化时间	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>cfm</b> 从全局配置视图进入 CFM 配置视图;</li> <li>3. 执行命令 <b>md name name level level</b> 用来进入 MD 配置视图;</li> </ol>

目的	步骤
	4. 执行命令 <b>ma name name vlan vlan-id</b> 用来进入 MA 配置视图； 5. 执行命令 <b>trace-replay aging-time { aging-time   default }</b> 配置 LTR 应答响应的老化时间； 6. 结束。

附表：

参数	说明	取值
vlan-id	指定 VLAN ID	整数形式，取值范围是 1~4094
level	指定级别	整数形式，取值范围是 0~7
mep-id	指定本地 MEP ID	整数形式，取值范围是 1~8191
threshold-value	指定 CC 丢失阈值	整数形式，取值范围是 2~255，以 CC 发送周期为单位
default	CC 默认丢失阈值	为 3.5 倍 CC 发送周期
delay-value	指定激活时间	整数形式，取值范围是 1~65535，单位：秒
default	表示默认值	0 秒
aging-time	指定动态 RMEP 的老化时间	整数形式，取值范围是 1~65535，单位：秒
default	表示默认老化时间	1000 秒
none	表示发送的 CFM 报文中不包含 Sender ID TLV 类型	-
chassis	表示发送的 CFM 报文中含有 Chassis ID 相关信息	-
manage	表示发送的 CFM 报文中含有管理地址相关信息	-
chassis-manage	表示发送的 CFM 报文中含有 Chassis ID 和管理地址相关信息	-
defer	表示 Sender ID TLV 的内容由 MD 管理对象决定	-
aging-time	指定 LTR 应答响应的老化时间	整数形式，取值范围是 1~65535，单位：秒
default	表示 LTR 应答响应的默认老化时间	1000 秒

### 8.9.5 配置 CFM 故障确认

#### 目的

当需要手动检测两台设备之间的链路连通性时，可以使用本节操作发送测试报文和接收应答报文，从而检测从本设备到目的设备是否可达。





注意：

对于本地 UP MEP，如果关联两个及两个以上 MIP，应确保 MIP 连接的网络只有一条二层数据业务通路(这通常是由生成树或以太网环协议来保证的)，否则 CFM 故障确认结果是不可预知的。

配置 CFM 连通性故障管理故障确认在设备根节点下进行，如需终止发送 LBM，可按 <Ctrl+C> 快捷键。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置通过 PING MAC 确认 CFM 连通性故障	1. 保持当前特权用户视图； 2. 执行命令 <b>cfm ping mac mac-address mep vlan vlan-id level level mepid mep-id -c packet-count -s packet-size -t packet-timeout</b> 或执行命令 <b>cfm ping mac mac-address mep vlan vlan-id level level mepid mep-id priority priority-value -c packet-count -s packet-size -t packet-timeout</b> 或执行命令 <b>cfm ping mac mac-address mep vlan vlan-id level level mepid mep-id</b> 通过 PING MAC 确认 CFM 连通性故障； 3. 结束。
配置通过 PING Remote MEP 确认 CFM 连通性故障	1. 保持当前特权用户视图； 2. 执行命令 <b>cfm ping remote-mep remote-mep-id mep vlan vlan-id level level mepid local-mep-id -c packet-count -s packet-size -t packet-timeout</b> 或执行命令 <b>cfm ping remote-mep remote-mep-id mep vlan vlan-id level level mepid local-mep-id priority priority -c packet-count -s packet-size -t packet-timeout</b> 或执行命令 <b>cfm ping remote-mep remote-mep-id mep vlan vlan-id level level mepid local-mep-id</b> 通过 PING Remote MEP 确认 CFM 连通性故障； 3. 结束。
配置通过 PING All Remote MEP 确认 CFM 连通性故障	1. 保持当前特权用户视图； 2. 执行命令 <b>cfm ping all remote-mep vlan vlan-id level level mepid local-mep-id-s packet-size-t packet-timeout</b> 或执行命令 <b>cfm ping all remote-mep vlan vlan-id level level mepid local-mep-id priority priority-s packet-size-t packet-timeout</b> 或执行命令 <b>cfm ping all remote-mep vlan vlan-id level level mepid local-mep-id</b> 通过 PING All Remote MEP 确认 CFM 连通性故障； 3. 结束。

附表：

参数	说明	取值
vlan-id	指定 VLAN ID	整数形式，取值范围是 1~4094
level	指定级别	整数形式，取值范围是 0~7
mac-address	指定远端 MEP 或 MIP 的 MAC	形如 AA:BB:CC:DD:EE:FF，其中 A~F 为一位十六进制数
mep-id	指定本地网桥发起 PING 操作的 MEP	整数形式，取值范围是 1~1891
remote-mep-id	指定远端网桥的 MEP ID	整数形式，取值范围是 1~1891
priority-value	指定优先级	整数形式，取值范围是 0~7
packet-count	指定 PING 的次数	整数形式，取值范围是 1~1024
packet-size	指定发送 PING 报文的大小，改大小是指包括二层报文头部的报文大小	整数形式，取值范围是 64~1518，默认为 64
packet-timeout	指定等待应答报文的超时时间	整数形式，取值范围是 1~60，单位：秒，默认为 5 秒

### 8.9.6 配置 CFM 故障定位

#### 目的

当需要定位两台设备之间的链路连通性故障时，可以使用本节操作发送测试报文和接收应答报文，从而检测从本设备到目的设备的路径或定位故障点。



注意：

对于本地 UP MEP，如果关联两个及两个以上 MIP，应确保 MIP 连接的网络只有一条二层数据业务通路(这通常是由生成树或以太网环协议来保证的)，否则 CFM 故障确认结果是不可预知的。

配置 CFM 故障定位在设备根节点下进行，Trace 结果正确会立刻列出。如果 Trace 结果不正确，可能会在设置的超时时间后给出一个参考结果，此时若提前终止 Trace，可按 <Ctrl+C> 快捷键。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置通过 Trace MAC 进行 CFM 连通性故障定位	1. 保持当前特权用户视图； 2. 执行命令 <b>cfm trace mac mac-address mep vlan vlan-id level level mepid local-mep-id</b> 或执行命令 <b>cfm trace mac mac-address mep vlan vlan-id level level mepid local-mep-id priority priority</b>

目的	步骤
	<p>或执行命令 <b>cfm trace mac mac-address mep vlan vlan-id level level mepid local-mep-id -t packet-timeout</b></p> <p>或执行命令 <b>cfm trace mac mac-address mep vlan vlan-id level level mepid local-mep-id priority priority -t packet-timeout { fdb-only   ccdb }</b></p> <p>或执行命令 <b>cfm trace mac mac-address mep vlan vlan-id level level mepid local-mep-id { fdb-only   ccdb }</b></p> <p>或执行命令 <b>cfm trace mac mac-address mep vlan vlan-id level level mepid local-mep-id priority priority { fdb-only   ccdb }</b></p> <p>或执行命令 <b>cfm trace mac mac-address mep vlan vlan-id level level mepid local-mep-id -t packet-timeout</b></p> <p>或执行命令 <b>cfm trace mac mac-address mep vlan vlan-id level level mepid local-mep-id -t packet-timeout { fdb-only   ccdb }</b></p> <p>或执行命令 <b>cfm trace mac mac-address mep vlan vlan-id level level mepid local-mep-id ttl ttl-value</b></p> <p>或执行命令 <b>cfm trace mac mac-address mep vlan vlan-id level level mepid local-mep-id priority priority ttl ttl-value</b></p> <p>或执行命令 <b>cfm trace mac mac-address mep vlan vlan-id level level mepid local-mep-id priority priority ttl ttl-value { fdb-only   ccdb }</b></p> <p>或执行命令 <b>cfm trace mac mac-address mep vlan vlan-id level level mepid local-mep-id ttl ttl-value { fdb-only   ccdb }</b>通过 Trace MAC 进行 CFM 连通性故障定位；</p> <p>3. 结束。</p>
<p>配置通过 Trace Remote MEP 进行 CFM 连通性故障定位</p>	<p>1. 保持当前特权用户视图；</p> <p>2. 执行命令 <b>cfm trace remote-mep remote-mep-id mep vlan vlan-id level level mepid local-mep-id</b></p> <p>或执行命令 <b>cfm trace remote-mep remote-mep-id mep vlan vlan-id level level mepid local-mep-id priority priority</b></p> <p>或执行命令 <b>cfm trace remote-mep remote-mep-id mep vlan vlan-id level level mepid local-mep-id priority priority -t packet-timeout</b></p> <p>或执行命令 <b>cfm trace remote-mep remote-mep-id mep vlan vlan-id level level mepid local-mep-id priority priority -t packet-timeout { fdb-only   ccdb }</b></p> <p>或执行命令 <b>cfm trace remote-mep remote-mep-id mep vlan vlan-id level level mepid local-mep-id { fdb-only   ccdb }</b></p> <p>或执行命令 <b>cfm trace remote-mep remote-mep-id mep vlan vlan-id level level mepid local-mep-id priority priority { fdb-only   ccdb }</b></p> <p>或执行命令 <b>cfm trace remote-mep remote-mep-id mep vlan vlan-id level level mepid local-mep-id -t packet-timeout</b></p> <p>或执行命令 <b>cfm trace remote-mep remote-mep-id mep vlan vlan-id</b></p>

目的	步骤
	<p><b>level level mepid local-mep-id-t packet-timeout { fdb-only   ccdb }</b> 或执行命令 <b>cfm trace remote-mep remote-mep-id mep vlan vlan-id</b></p> <p><b>level level mepid local-mep-idttl ttl-value</b> 或执行命令 <b>cfm trace remote-mep remote-mep-id mep vlan vlan-id</b></p> <p><b>level level mepid local-mep-idpriority priorityttl ttl-value</b> 或执行命令 <b>cfm trace remote-mep remote-mep-id mep vlan vlan-id</b></p> <p><b>level level mepid local-mep-id priority priority ttl ttl-value { fdb-only   ccdb }</b> 或执行命令 <b>cfm trace remote-mep remote-mep-id mep vlan vlan-id</b></p> <p><b>level level mepid local-mep-id ttl ttl-value { fdb-only   ccdb }</b>通过 Trace Remote MEP 进行 CFM 连通性故障定位；</p> <p>3. 结束。</p>

附表：

参数	说明	取值
mac-address	指定远端 MEP 或 MIP 的 MAC	形如 AA:BB:CC:DD:EE:FF, 其中 A~F 为一位十六进制数
vlan-id	指定 VLAN ID	整数形式, 取值范围是 1~4094
level	指定级别	整数形式, 取值范围是 0~7
remote-mep-id	指定远端网桥的 MEP ID	整数形式, 取值范围是 1~1891
local-mep-id	指定本地网桥发起 Trace 操作的 MEP ID	整数形式, 取值范围是 1~1891
priority	指定优先级	整数形式, 取值范围是 0~7
packet-timeout	指定等待应答报文的超时时间	整数形式, 取值范围是 1~60, 单位: 秒, 默认为 5 秒
ttl-value	指定 Trace 跟踪的最大跳数	整数形式, 取值范围是 1~255, 默认为 64 跳
fdb-only	表示仅仅使用 MAC 转发表转发 LTM	-
ccdb	表示转发表转发 LTM 失败时, 使用 MIP CCDB 转发 LTM, 这是发起 Trace 的默认选项	-

### 8.9.7 维护及调试

#### 目的

当 CFM 功能不正常, 需要进行查看、调试或定位问题时, 可以使用本小节操作。

#### 过程

根据不同目的, 执行相应步骤, 具体参见下表。

目的	步骤
----	----



目的	步骤
CCDB 的概要或详细信息	<p>行命令 <b>interface eth-trunk trunk-number</b> 进入接口配置视图, 或执行命令 <b>md name name level level</b> 进入 MD 配置视图, 或执行命令 <b>ma name name vlan vlan-id</b> 进入 MA 配置视图或不执行任何命令保持当前特权用户视图;</p> <p>2. 执行命令 <b>show cfm error ccdb</b> 或执行命令 <b>show cfm error ccdb remote-mep-id vlan vlan-id level level mepid mep-id</b> 显示 MEP ERROR CCDB 的概要或详细信息;</p> <p>3. 结束。</p>
查看 MA 概要或详细信息	<p>1. 执行命令 <b>disable</b> 退出到普通用户视图, 或执行命令 <b>configure</b> 进入全局配置视图, 或执行命令 <b>interface { fastethernet   gigaethernet } interface-number</b> 或执行命令 <b>interface eth-trunk trunk-number</b> 进入接口配置视图, 或执行命令 <b>md name name level level</b> 进入 MD 配置视图, 或执行命令 <b>ma name name vlan vlan-id</b> 进入 MA 配置视图或不执行任何命令保持当前特权用户视图;</p> <p>2. 执行命令 <b>show cfm ma</b> 或执行命令 <b>show cfm ma name vlan vlan-id</b> 显示 MA 概要或详细信息;</p> <p>3. 结束。</p>
查看 MD 概要或详细信息	<p>1. 执行命令 <b>disable</b> 退出到普通用户视图, 或执行命令 <b>configure</b> 进入全局配置视图, 或执行命令 <b>interface { fastethernet   gigaethernet } interface-number</b> 或执行命令 <b>interface eth-trunk trunk-number</b> 进入接口配置视图, 或执行命令 <b>md name name level level</b> 进入 MD 配置视图, 或执行命令 <b>ma name name vlan vlan-id</b> 进入 MA 配置视图或不执行任何命令保持当前特权用户视图;</p> <p>2. 执行命令 <b>show cfm md</b> 或执行命令 <b>show cfm md name</b> 显示 MD 概要或详细信息;</p> <p>3. 结束。</p>
查看 MEP 概要或详细信息	<p>1. 执行命令 <b>disable</b> 退出到普通用户视图, 或执行命令 <b>configure</b> 进入全局配置视图, 或执行命令 <b>interface { fastethernet   gigaethernet } interface-number</b> 或执行命令 <b>interface eth-trunk trunk-number</b> 进入接口配置视图, 或执行命令 <b>md name name level level</b> 进入 MD 配置视图, 或执行命令 <b>ma name name vlan vlan-id</b> 进入 MA 配置视图或不执行任何命令保持当前特权用户视图;</p> <p>2. 执行命令 <b>show cfm mep</b> 或执行命令 <b>show cfm mep vlan vlan-id level level mepid mep-id</b> 显示 MEP 概要或详细信息;</p> <p>3. 结束。</p>
查看 MEP CCDB 的概要或详细信息	<p>1. 执行命令 <b>disable</b> 退出到普通用户视图, 或执行命令 <b>configure</b> 进入全局配置视图, 或执行命令 <b>interface { fastethernet   gigaethernet } interface-number</b> 或执行命令 <b>interface eth-trunk trunk-number</b> 进入接口配置视图, 或执行命令 <b>md name name level level</b> 进入 MD 配置视图, 或执行命令 <b>ma name name vlan vlan-id</b> 进入 MA 配置视图或不执行任何命令保持当前特权用户视图;</p> <p>2. 执行命令 <b>show cfm mep ccdb</b> 或执行命令 <b>show cfm mep ccdb remote-mep-id vlan vlan-id level level mepid mep-id</b> 显示 MEP CCDB 的概要或详细信息;</p> <p>3. 结束。</p>

目的	步骤
查看网桥配置的所有 MIP 的信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gigaehternet } interface-number</b> 或执行命令 <b>interface eth-trunk trunk-number</b> 进入接口配置视图，或执行命令 <b>md name name level level</b> 进入 MD 配置视图，或执行命令 <b>ma name name vlan vlan-id</b> 进入 MA 配置视图或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show cfm mip</b> 显示网桥配置的所有 MIP 的信息；</li> <li>3. 结束。</li> </ol>
查看 MIP CCDB 的概要信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gigaehternet } interface-number</b> 或执行命令 <b>interface eth-trunk trunk-number</b> 进入接口配置视图，或执行命令 <b>md name name level level</b> 进入 MD 配置视图，或执行命令 <b>ma name name vlan vlan-id</b> 进入 MA 配置视图或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show cfm mip ccdb</b> 显示 MIP CCDB 的概要信息；</li> <li>3. 结束。</li> </ol>
查看接口 CFM 报文统计信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gigaehternet } interface-number</b> 或执行命令 <b>interface eth-trunk trunk-number</b> 进入接口配置视图，或执行命令 <b>md name name level level</b> 进入 MD 配置视图，或执行命令 <b>ma name name vlan vlan-id</b> 进入 MA 配置视图或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show cfm pdu-statistic interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b> 或执行命令 <b>show cfm pdu-statistic interface eth-trunk trunk-number</b> 或执行命令 <b>show cfm pdu-statistic interface</b> 显示接口 CFM 报文统计信息；</li> <li>3. 结束。</li> </ol>
查看 RMEP 概要或详细信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gigaehternet } interface-number</b> 或执行命令 <b>interface eth-trunk trunk-number</b> 进入接口配置视图，或执行命令 <b>md name name level level</b> 进入 MD 配置视图，或执行命令 <b>ma name name vlan vlan-id</b> 进入 MA 配置视图或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show cfm remote-mep</b> 或执行命令 <b>show cfm remote-mep vlan vlan-id level level mepid mep-id</b> 显示 RMEP 概要或详细信息；</li> <li>3. 结束。</li> </ol>
查看网桥 MEP 最近一次故障定位查询的结果	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gigaehternet } interface-number</b> 或执行命令 <b>interface eth-trunk trunk-number</b> 进入接口配置视图，或执行命令 <b>md name name level level</b> 进入 MD 配置视图，或执行命令 <b>ma name name vlan vlan-id</b> 进入 MA 配置视图或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show cfm trace-result mep vlan vlan-id level level mepid mep-id</b> 显示网桥 MEP 最近一次故障定位查询的结果；</li> <li>3. 结束。</li> </ol>

目的	步骤
使能或禁止 CFM 上报 SNMP 告警功能	<ol style="list-style-type: none"> <li>1. 执行命令 <b>cfm</b> 进入 CFM 配置视图；</li> <li>2. 执行命令 <b>snmp-trap {enable   disable}</b> 使能或禁止 CFM 上报 SNMP 告警功能；</li> <li>3. 结束。</li> </ol>

附表：

参数	说明	取值
interface-number	指定物理接口号	SC9600 系列交换机支持以下 3 种型号的接口配置范围： SC9603：取值范围是<1-3>/<0-4>/<1-48> SC9608：取值范围是<1-8>/<0-4>/<1-48> SC9612：取值范围是<1-12>/<0-4>/<1-48>
trunk-number	指定 trunk 接口号	整数形式，取值范围是 1~8
remote-mep-id	指定远端 MEP ID	整数形式，取值范围是 1~1891
vlan-id	指定 VLAN ID	整数形式，取值范围是 1~4094
level	指定 MEP 级别	整数形式，取值范围是 0~7
mep-id	指定本地 MEP ID	整数形式，取值范围是 1~1891
name	指定 MA 名称	字符串形式
name	指定 MD 名称	字符串形式
remote-mep-id	指定远端 MEP ID	整数形式，取值范围是 1~1891

### 8.9.8 配置举例

#### 组网要求

本示例主要介绍多维护域情况下 CFM 连通性故障管理的配置。

将设备 wh-SC9600、cs、nc、hf、zz 划归维护域 MD1，配置 MD 等级 1；

将设备 cd、gz、sh、bj 划归维护域 MD2，配置 MD 等级 6。每个维护域下可以任意添加自己的维护组合（MA）。由于维护域的 MD2 等级高于维护域 MD1 的维护域等级，所以维护域 MD2 的 CFM 报文可以透明穿越维护域 MD1，二者互不干扰。

划分完维护域，即可根据图 8-34 所示拓扑确定维护域边界，同时可以确定各维护域 MEP 的配置接口，只要保证维护域下 MEP ID 不重复即可。

如果需要对维护域中间点进行 CFM 连通性故障管理的话，只需要将维护域中间点配置为 MIP 即可，对维护域 MD1 边界 MEP 所在接口，还要配置维护域 MD2 的中间点 MIP。

#### 组网图



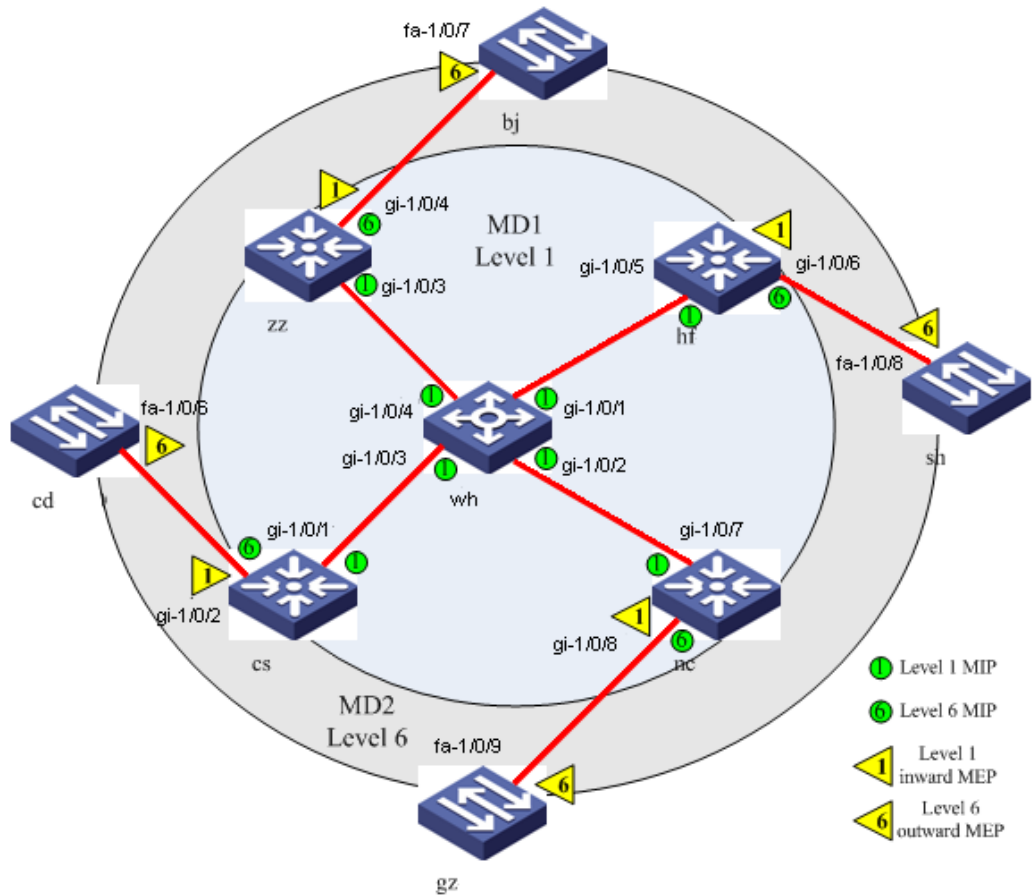


图 8-34 CFM 配置组网图

### 配置步骤

每台网桥配置如下：

#### 1、配置维护域 MD1。

##### 1) 配置 wh-SC9600

```
wh-SC9600#configure
wh-SC9600(config)#cfm
wh-SC9600(config-cfm)#md name md1 level 1
wh-SC9600(config-md-md1)#ma name ma1 vlan 1
wh-SC9600(config-md-md1-ma-ma1)#quit
wh-SC9600(config)#interface gigabitEthernet 1/0/1 to gigabitEthernet 1/0/4
wh-SC9600(config-ge1/0/1->ge1/0/4)#cfm mip vlan 1 level 1
```

##### 2) 配置 cs

```
cs#configure
cs(config)#cfm
cs(config-cfm)#md name md1 level 1
cs(config-md-md1)#ma name ma1 vlan 1
cs(config-md-md1-ma-ma1)#quit
cs(config-cfm)#md name md2 level 6
cs(config-md-md2)#ma name ma2 vlan 1
cs(config-md-md2-ma-ma2)#quit
cs(config)#interface gigabitEthernet 1/0/1
cs(config-ge1/0/1)#cfm mip vlan 1 level 1
cs(config-ge1/0/1)#quit
cs(config)#interface gigabitEthernet 1/0/2
cs(config-ge1/0/2)# cfm mip vlan 1 level 6
cs(config-ge1/0/2)#cfm mep vlan 1 level 1 mepid 1 inward
cs(config-ge1/0/2)#cfm mep vlan 1 level 1 mepid 1 ccm enable
```

### 3) 配置 nc

```
nc#configure
nc(config)#cfm
nc(config-cfm)#md name md1 level 1
nc(config-md-md1)#ma name ma1 vlan 1
nc(config-md-md1-ma-ma1)#quit
nc(config-cfm)#md name md2 level 6
nc(config-md-md2)#ma name ma2 vlan 1
nc(config-md-md2-ma-ma2)#quit
nc(config)#interface gigabitEthernet 1/0/7
nc(config-ge1/0/7)#cfm mip vlan 1 level 1
nc(config-ge1/0/7)#quit
nc(config)#interface gigabitEthernet 1/0/8
nc(config-ge1/0/8)# cfm mip vlan 1 level 6
nc(config-ge1/0/8)#cfm mep vlan 1 level 1 mepid 100 inward
nc(config-ge1/0/8)#cfm mep vlan 1 level 1 mepid 100 ccm enable
```

### 4) 配置 hf

```
hf#configure
hf(config)#cfm
hf(config-cfm)#md name md1 level 1
hf(config-md-md1)#ma name ma1 vlan 1
hf(config-md-md1-ma-ma1)# quit
hf(config-cfm)#md name md2 level 6
hf(config-md-md2)#ma name ma2 vlan 1
hf(config-md-md2-ma-ma2)# quit
hf(config)#interface gigabitEthernet 1/0/5
hf(config-ge1/0/5)#cfm mip vlan 1 level 1
hf(config-ge1/0/5)# quit
hf(config)#int gigabitEthernet 1/0/6
hf(config-ge1/0/6)# cfm mip vlan 1 level 6
hf(config-ge1/0/6)#cfm mep vlan 1 level 1 mepid 1000 inward
hf(config-ge1/0/6)#cfm mep vlan 1 level 1 mepid 1000 ccm enable
```

#### 5) 配置 zz

```
zz#configure
zz(config)#cfm
zz(config-cfm)#md name md1 level 1
zz(config-md-md1)#ma name ma1 vlan 1
zz(config-md-md1-ma-ma1)#quit
zz(config-cfm)#md name md2 level 6
zz(config-md-md2)#ma name ma2 vlan 1
zz(config-md-md2-ma-ma2)#quit
zz(config)#interface gigabitEthernet 1/0/3
zz(config-ge1/0/3)#cfm mip vlan 1 level 1
zz(config-ge1/0/3)#quit
zz(config)#interface gigabitEthernet 1/0/4
zz(config-ge1/0/4)# cfm mip vlan 1 level 6
zz(config-ge1/0/4)#cfm mep vlan 1 level 1 mepid 7777 inward
zz(config-ge1/0/4)#cfm mep vlan 1 level 1 mepid 7777 ccm enable
```

#### 2、配置维护域 MD2。

## 1) 配置 cd

```
cd#configure
cd(config)#cfm
cd(config-cfm)#md name md2 level 6
cd(config-md-md2)#ma name ma2 vlan 1
cd(config-md-md2-ma-ma2)#quit
cd(config)#interface fastethernet 1/0/6
cd(config-fe1/0/6)#cfm mep vlan 1 level 6 mepid 1
cd(config-fe1/0/6)#cfm mep vlan 1 level 6 mepid 1 ccm enable
```

## 2) 配置 gz

```
gz#configure
gz(config)#cfm
gz(config-cfm)#md name md2 level 6
gz(config-md-md2)#ma name ma2 vlan 1
gz(config-md-md2-ma-ma2)#quit
gz(config)#interface fastethernet 1/0/9
gz(config-fe1/0/9)#cfm mep vlan 1 level 6 mepid 1
gz(config-fe1/0/9)#cfm mep vlan 1 level 6 mepid 1 ccm enable
```

## 3) 配置 sh

```
sh#configure
sh(config)#cfm
sh(config-cfm)#md name md2 level 6
sh(config-md-md2)#ma name ma2 vlan 1
sh(config-md-md2-ma-ma2)#quit
sh(config)#interface fastethernet 1/0/8
sh(config-fe1/0/8)#cfm mep vlan 1 level 6 mepid 1
sh(config-fe1/0/8)#cfm mep vlan 1 level 6 mepid 1 ccm enable
```

## 4) 配置 bj

```
bj#configure
bj(config)#cfm
bj(config-cfm)#md name md2 level 6
```

```

bj(config-md-md2)#ma name ma2 vlan 1
bj(config-md-md2-ma-ma2)#quit
bj(config)#interface fastethernet 1/0/7
bj(config-fe1/0/7)#cfm mep vlan 1 level 6 mepid 1
bj(config-fe1/0/7)#cfm mep vlan 1 level 6 mepid 1 ccm enable
    
```

## 8.10 Y.1731 配置

### 8.10.1 Y.1731 概述

#### Y.1731 故障管理协议简介

以太网原来主要用于 LAN 环境，OAM（operation, administration and management）能力较弱。为了实现与传统电信级传送网相同的服务水平，ITU-T SG13 制定了 Y.1731，定义了基于以太网承载网络的连通性故障检测、故障确认、故障定位和故障指示的 OAM 功能，适用于大规模组网的端到端场景，是网络级的 OAM。

IEEE、ITU-T 和 MEF 统一了一个多域的 OAM 网络模型，如图 8-35 OAM 多域网络模型所示。电信级以太网被分为用户、提供商和运营商 3 个维护等级，分别对应不同的管理域。提供商负责端到端的业务管理，运营商提供业务传送。

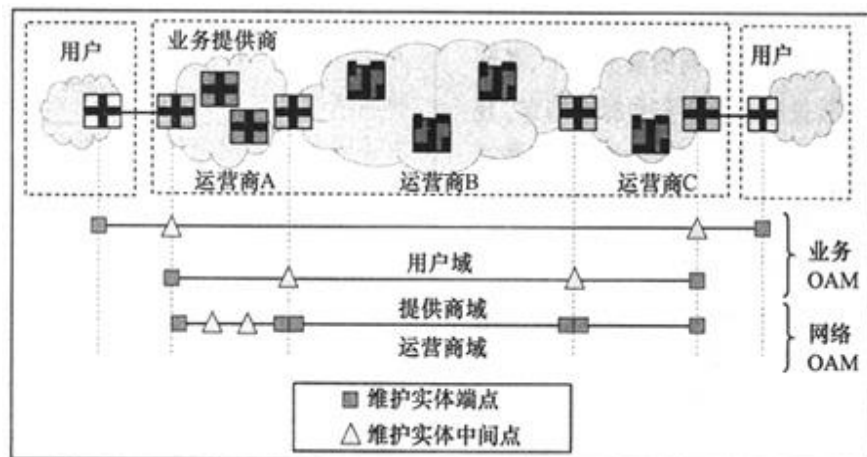


图 8-35 OAM 多域网络模型

#### Y.1731 故障管理技术特点

Y.1731 故障管理技术具有如下特点：

- Y.1731 故障管理技术既是三层（IP 层）OAM 技术理念向二层以太网的延伸，也是以太网向城域网和广域网扩展的客观需要。Y.1731 定义的故障管理功能都可以找到对应的三层 OAM 功能，如 BFD 对应连通性检测、IP Ping 对应故障确认（Y.1731 loopback）、IP Trace 对应故障定位（Y.1731 linktrace）等；
- ITU-T Y.1731 的连通性故障检测定义支持每秒 300Hz 的发包频率，并且对不同的服务实例通过 VLAN 标记（Tagged）字段加以区分，因此特别适用于电信级以太网的保护倒换需求；
- Y.1731 连通性检测报文已经成为 I-TUT 提出的 G.8031/G.8032 标准的连通性检测标准，理论上可以为目前设备供应商各自定义的以太网阻塞性协议（如 Ethernet Ring、Smart Link）提供统一的连通性检测标准，从而使设备供应商各自定义的以太网阻塞性协议互通成为可能，减少运营商的网络运行、管理和维护成本。

### 8.10.2 Y.1731 故障管理实例基本概念

#### 维护实体组合 MEG

MEG 是进行 Y.1731 故障管理的一个虚拟网络，可以理解为用字符串（在 Y.1731 故障管理中成为 MEG ID）表示的一个服务实例（Service Instance 在 Y.1731 故障管理中就是 MEG 映射的 VLAN）。



注意：

在网络中划分多个 MEG 要注意各 MEG 的位置关系可以是嵌套、相切或互不相交，但绝对不允许相交的情况。

#### MEG 名称（MEG ID）

MEG 的名称具有多种格式，具体由 MEG ID 格式字段来识别。SC9600 系列产品的 Y.1731 协议的 MEG ID 采用国际电联运营商编码（ICC）的格式。

基于 ICC 的 MEG ID 格式由两个子字段构成：国际电联运营商编码（ICC），由 1-8 个以左侧为准的字符、字母或者首位字母再加后面的数字所组成；随后是一个唯一的 MEG ID 编码（UMC），由 7-12 个字母连同后面的 NULL（0）组成，使 MEG ID 正好为 13 个字符。基于 ICC 的 MEG ID 格式在 ETH-CC 报文中如图 8-36 所示。

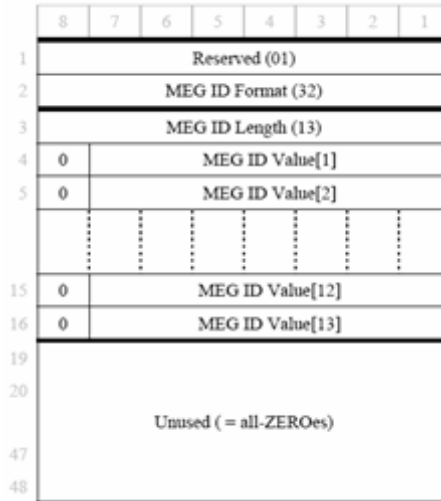


图 8-36 基于 ICC 的 MEG ID 格式

### MEG 等级 (MEL)

一般情况下，一个配置了多个 MEG 的网桥，是通过 VLAN 标记字段来区分不同 MEG 的 Y.1731 的数据帧的。当不能通过 VLAN 标记加以区分时，可以通过配置 MEG 等级对多个 MEG 的 Y.1731 的数据帧进行区分。

Y.1731 定义了 8 个 MEG 等级用来区分属于客户、提供商和运营商的相互嵌套 MEG 的 Y.1731 帧，以满足网络部署的不同情景。

在客户、提供商和运营商角色之间，MEG 等级默认的分配如下：

- 客户角色分配三个 MEG 等级：7、6 和 5。
- 提供商角色分配两个 MEG 等级：4 和 3。
- 运营商角色分配三个 MEG 等级：2、1 和 0。



注意：

当一个网桥配置有多个 MEG 时，网桥端口上的 MEP 允许所属 MEG 以外的带有较高 MEL 的 Y.1731 帧透明地穿越而不做任何处理，并阻断所属 MEG 以外的带有相同或较低 MEL 的 Y.1731 帧。

### MEG 端点 (MEP)

MEP 表示一个 MEG 的端点，用于确定 Y.1731 故障管理中每个 MEG 的边界，其功能是发出和终止 Y.1731 数据帧，从而实现故障管理和性能监控。

在未配置 MEP 的网桥端口上，Y.1731 数据帧和具有相同 VLAN 标记的以太网业务转发流程相同。

在配置了 MEP 的网桥端口上，MEP 可以监控和自己相同 VLAN 标记的以太网业务流且一般情况下不终止以太网业务流或更改以太网业务流的内容，同时可以利用和自己相同 VLAN 标记的与层级（MEL）的 Y.1731 数据帧实现故障管理和性能监控。

### MEP 方向（MEP DIRECTION）

Y.1731 定义了两种类型 MEP 的方向：UP MEP 和 DOWN MEP；

- UP MEP 也称 inward MEP，可以理解为以太网业务流的上联口，关联 UNI。UP MEP 通过网桥的转发中继功能（现行设备是通过 MEP 对应的 MIP）发送和接收 Y.1731 帧，UP MEP 自身所在端口并不发送和接收 Y.1731 帧。这样接收的 Y.1731 帧看起来是在网桥内部转发的过程中终结的，因此称作 inward MEP。
- DOWN MEP 也称 outward MEP，可以理解为以太网业务流的下联口，关联 NNI。DOWN MEP 通过所在端口直接向以太网发送和接收 Y.1731 帧，不需要经由 MIP（网桥）中继。

### MEG 中间点（MIP）

MIP 是 MEG 中的一个中间节点，用于对某些 Y.1731 帧（故障确认 Y.1731 帧 LBR/LBM、故障定位 Y.1731 帧 LTR/LTM）做出回应。MIP 本身并不发送 Y.1731 帧。除了满足 MIP 匹配条件的故障确认和故障定位 Y.1731 帧外，其它 Y.1731 帧和以太网业务流均是透明地穿越 MIP，不做任何处理。

### Y.1731 帧目的 MAC（DA）

Y.1731 既有使用单播 MAC 的操作码，也有使用组播 MAC 的操作码。其中，Y.1731 的组播 MAC 有两类：

- Multicast Class 1 DA:

01:80:C2:00:00:30—01:80:C2:00:00:37

- Multicast Class 2 DA:

01:80:C2:00:00:38—01:80:C2:00:00:3F



OAM Type	DAs for frames with OAM PDU
CCM	Multicast Class 1 DA or Unicast DA
LBM	Unicast DA or Multicast Class 1 DA
LBR	Unicast DA
LTM	Multicast Class 2 DA
LTR	Unicast DA
AIS	Multicast Class 1 DA or Unicast DA
LCK	Multicast Class 1 DA or Unicast DA
TST	Unicast DA or Multicast Class 1 DA
Linear APS	Multicast Class 1 DA or Unicast DA
Ring APS	Multicast Class 1 DA or Unicast DA
MCC	Unicast DA or Multicast Class 1 DA
LMM	Unicast DA or Multicast Class 1 DA
LMR	Unicast DA
IDM	Unicast DA or Multicast Class 1 DA
DMM	Unicast DA or Multicast Class 1 DA
DMR	Unicast DA
EXM, EXR, VSM, VSR	Outside the scope of this Recommendation

图 8-37 Y.1731 操作码对应的目的 MAC

### 8.10.3 SC9600 支持的 Y.1731 特性



注意：

浪潮网络科技有限公司出品的交换机及其相关产品不支持处理超过 256 字节的 ETH-CC/ETH-LTR/ETH-LTM/ETH-AIS/ETH-LCK 报文。

#### ETH-CC 以太网连通性检测

以太网连续性检测（ETH-CC）是一种主动 OAM（ProactiveOAM）功能。它可以用于检测处于一个 MEG 中的任一对 MEP 间的连续性丢失（LOC），可用于检测两个 MEG 之间的错误连接，也可用于检测在一个 MEG 中出现与错误 MEP 相连的情况，以及其他一些故障情况。连续性检查消息可应用于故障管理（ETH-CC 以太网连通性检测、ETH-RDI，以太网远程端故障指示）、性能监控（双端 ETH-LM）或保护转换（G.8031/G.8032）的应用。

ETH-CC 定义的传输周期从 3.33ms 到 10min 共 7 种，常用的有 3 种：

- 差错管理：默认的传输周期是 1 s（即每秒 1 帧的传输速率）。
- 性能监控：默认的传输周期是 100 ms（即每秒 10 帧的传输速率）。
- 保护转换：默认的传输周期是 3.33 ms（即每秒 300 帧的传输速率）。



注意：

根据 Y.1731 的有关定义，MEP 或 MIP 不能处理、发送或转发超过 128 字节的 CCM 帧。

### ETH-LBR/LBM 以太网故障确认

以太网故障确认是一种按需的 OAM 功能。Y.1731 故障确认通过发送查询报文 LBM 和接收应答报文 LBR 来检测同一个 MEG 内本地设备 MEP 到目的设备 MEP 或 MIP 的连通性。

Y.1731 故障确认有两种类型：

- 单播 Unicast ETH-LB 是基于 VLAN 的二层 MAC-Ping-MAC 协议；
- 组播 Multicast ETH-LB 使用 1 类组播 MAC，是基于 VLAN 的二层 MAC-Ping-MACs-in-VLAN 协议，LBR 都是使用单播地址。

Y.1731 故障确认消息从 MEP 发到指定 MEP（MIP），帮助 MEP 在 MEG 中精确定位故障位置。故障位置前的 MIP（MEP）能够响应故障确认消息，而故障位置后的 MIP（MEP）不能够响应故障确认消息，从而实现故障的定位。单播和组播的 Y.1731 故障确认原理分别如图 8-38、图 8-39 所示。

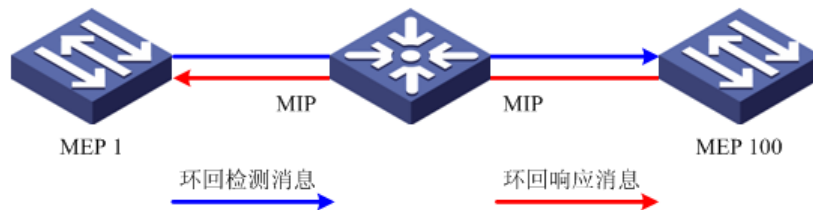


图 8-38 Y.1731 单播故障确认基本原理

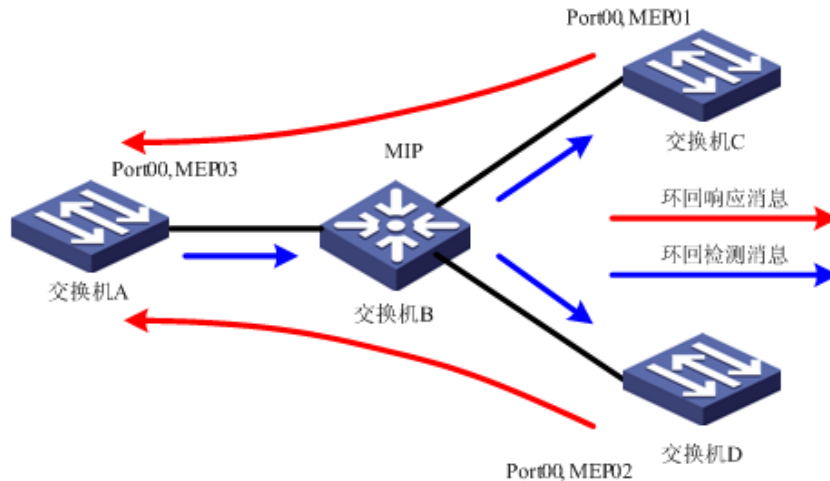


图 8-39 Y.1731 组播故障确认基本原理

### ETH-LTR/LTM 以太网故障定位

Y.1731 故障定位也称为以太网链路追踪 (ETH-LT), 也是一种按需的 OAM 功能。Y.1731 故障定位通过发送查询报文 LTM (使用 2 类组播 MAC) 和接收应答报文 LTR (使用单播地址) 来检测同一个 MEG 内本地设备 MEP 到目的设备 MEP 或 MIP 的路径或定位故障点。

本地 MEP 发起 Y.1731 故障定位查询报文后, 链路中所有中间 MIP 以及终结 MEP 向本地 MEP 发送 Y.1731 故障定位应答消息, 其中 MIP 还会转发 Y.1731 故障定位查询消息, 直到到达目的 MIP/MEP。通过 Y.1731 故障定位应答消息, 本地 MEP 可以得到 MEG 上所有 MIP 的 MAC 地址与相对发起 MEP 的位置, 以及出现链路故障的位置区间。如图 8-40 所示。

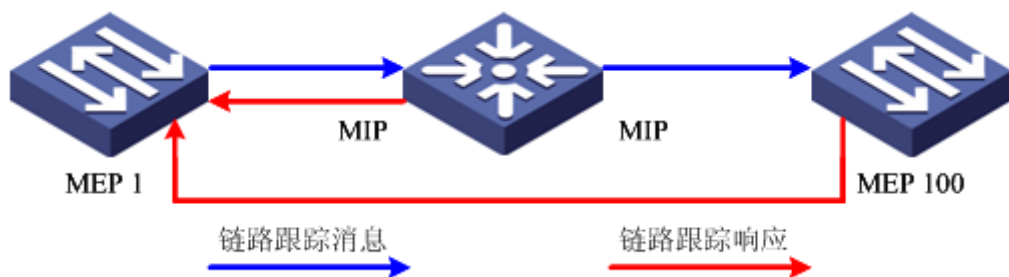


图 8-40 Y.1731 故障定位基本原理

### ETH-AIS 以太网告警指示信号

以太网告警指示信号，使用 1 类组播 MAC，用于在服务器层（子层）检测到连通性故障情况后抑制告警（Traps）。带有 ETH-AIS 信息的 Y.1731 帧的传输在由 MEP（或服务器 MEP）发送或停止。ETH-AIS 不用于 STP 环境。

带有 ETH-AIS 的 Y.1731 帧可以由 MEP（包括服务器 MEP）在检测到故障情况时在客户的 MEG 等级上发出。图 8-41 中，红色表示的数据流为以太网告警指示信号 ETH-AIS，其 MEL 总是高于发送它的 MEP 所在的 MEL。

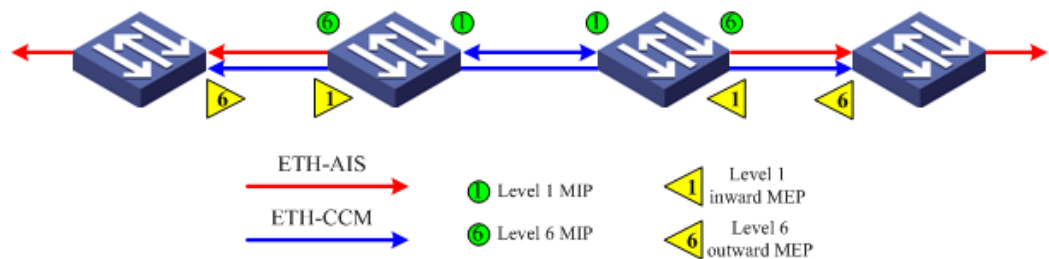


图 8-41 Y.1731 告警指示信号基本原理

作为例子，故障情况有以下两种：

1. 在 MEG 内执行 ETH-CC 的信号异常情况，主要包括：
  - 一个 MEG 中任何一对 MEP 间连续性的丢失（LOC）；
  - 两个 MEG 之间不希望有的连通性（错误混入，MEG ID 不同）；
  - 在 MEG 内与一个不要求的 MEP（非期望的 MEP）间不希望有的连通性；
  - 非期望 MEG 等级（本地 MEP 检测到一个较低 MEL 的 ETH-CC）；
  - 非期望的周期等（在 MEG 内本地 MEP 和远端 MEP 周期不一致）；
  - ETH-CC 滞环（在 MEG 内本地 MEP 接收到自己发生的 ETH-CC）。
2. MEG 内关闭 ETH-CC 出现的 AIS 情况或 LCK 情况，一般需要其它以太网链路检测协议触发，目前仅支持 IEEE 802.3ah 发现功能失败后触发 AIS。



注意：

对于上述两种故障情况，满足 ETH-AIS 发送还必须保证发送 AIS 的 MEP 所在接口上配置了大于该 MEP 等级的 MIP。

### ETH-LCK 以太网锁定信号

以太网锁定信号功能（ETH-LCK）用于通告服务器层（子层）MEP 的管理性锁定以及随后的数据业务流中断，该业务流是送往期待接收这业务流的 MEP 的。它使得接收带有 ETH-LCK 信息的帧的 MEP 能区分是故障情况，还是服务器层（子层）MEP 的管理性锁定动作。以太网锁定信号使用的目的 MAC 为 1 类组播 MAC。

当 MEP 使能 LCK 功能后，MEP 所在端口的以太网业务流自动中断。此时 MEP 会向高层级 MEP 发送 LCK 包，高层级 MEP 收到 LCK 包后，会自动将 MEP 所在端口的以太网业务流全部中断。LCK 禁用后以太网业务流自动恢复。



注意：

在阻塞性协议运行的环境下，LCK 可能会导致端口转发状态与实际期望的端口转发状态存在二义性问题，因此在阻塞性协议运行的场景中应尽量限制 LCK 的使用。

## 8.10.4 配置 Y.1731 基本功能

### 背景信息

为了实现 Y.1731 故障管理的基本功能，最简配置步骤如下：

1. 进入 Y.1731 配置视图；
2. 创建 MEG；
3. 创建 MEP 或 MIP；（可选）
4. 使能 ETH-CC。



说明：

建议在配置上述步骤之前先创建好 MEG 需要映射的 VLAN（即创建相应 VLAN）；再将 MEP 或 MIP 所在端口加入事先规划好的所属 MEG 对应的 VLAN（即端口加入相应 VLAN）；最后打开该端口（no shutdown）。当然也可以在上述步骤配置完成之后再行此配置。

- 同一个 MEG 内的 MIP 和 MEP 在同一个接口不能同时存在。

- 同一个 MEG 内的 MIP 在同一个接口最多只有一个。
- 同一个接口下配置了 CFM 的 MIP 或 MEP，则不能再配置 Y.1731 的 MIP。

### 目的

在需要实现端到端的连通性检测或直连链路的连通性检测时，用户可以执行本节操作配置 Y.1731 基本功能。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
创建 MEG 并进入 MEG 配置视图	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>y1731</b> 从全局配置视图进入 Y.1731 配置视图；</li> <li>3. 执行命令 <b>meg vlan <i>vlan-id</i> level <i>level</i> icc <i>icc string</i> umc <i>umc string</i></b> 创建 MEG 并进入 MEG 配置视图 或执行命令 <b>meg vlan <i>VLANLIST</i> level <i>level</i></b> 批量创建 MEG；</li> <li>4. 结束。</li> </ol>
创建 MEP	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface gigasethernet <i>interface-number</i></b> 进入以太网接口配置视图或执行命令 <b>interface eth-trunk <i>trunk-number</i></b> 进入 trunk 接口配置视图；</li> <li>3. 执行命令 <b>y1731 mep vlan <i>vlan-id</i> level <i>level</i></b> 或执行命令 <b>y1731 mep vlan <i>vlan-id</i> level <i>level</i> mepid <i>mepid-id</i></b> 或执行命令 <b>y1731 mep vlan <i>vlan-id</i> level <i>level</i> mepid <i>mepid-id</i> { inward   outward }</b> 用来创建 MEP；</li> <li>4. 结束。</li> </ol>
(可选)使能或去使能 MEP 的 AIS 功能	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface gigasethernet <i>interface-number</i></b> 进入以太网接口配置视图或执行命令 <b>interface eth-trunk <i>trunk-number</i></b> 进入 trunk 接口配置视图；</li> <li>3. 执行命令 <b>y1731 mep vlan <i>vlan-id</i> level <i>level</i> mepid <i>mep-id</i> ais { enable   disable }</b> 或执行命令 <b>y1731 mep vlan <i>vlan-id</i> level <i>level</i> mepid <i>mep-id</i> ais priority <i>priority</i> { enable   disable }</b> 用来配置是否使能 MEP 的 AIS 功能；</li> <li>4. 结束。</li> </ol>
(可选)使能或去使能 AIS 的外部触发功能	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface gigasethernet <i>interface-number</i></b> 进入以太网接口配置视图或执行命令 <b>interface eth-trunk <i>trunk-number</i></b> 进入 trunk 接口配置视图；</li> <li>3. 执行命令 <b>y1731 mep vlan <i>vlan-id</i> level <i>level</i> mepid <i>mep-id</i> ais 8023ah-cause { enable   disable }</b> 用来配置是否使能 AIS 的外部触发功能；</li> <li>4. 结束。</li> </ol>

目的	步骤
使能或者禁用 MEP 的 CCM 检测	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface gigabitEthernet interface-number</b> 进入以太网接口配置视图或执行命令 <b>interface eth-trunk trunk-number</b> 进入 trunk 接口配置视图；</li> <li>3. 执行命令 <b>y1731 mep vlan vlan-id level level mepid mepid-id ccm { enable   disable }</b> 或执行命令 <b>y1731 mep vlan vlan-id level level mepid mepid-id ccm priority priority { enable   disable }</b> 用来配置是否使能 MEP 的 CCM 检测；</li> <li>4. 结束。</li> </ol>
(可选)使能或者禁用 MEP 的 LCK 功能	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface gigabitEthernet interface-number</b> 进入以太网接口配置视图或执行命令 <b>interface eth-trunk trunk-number</b> 进入 trunk 接口配置视图；</li> <li>3. 执行命令 <b>y1731 mep vlan vlan-id level level mepid mepid-id lock { enable   disable }</b> 或执行命令 <b>y1731 mep vlan vlan-id level level mepid mepid-id lock priority priority { enable   disable }</b> 用来配置是否使能 MEP 的 LCK 功能；</li> <li>4. 结束。</li> </ol>
(可选) 配置 MEP 的 MAC 地址	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface gigabitEthernet interface-number</b> 进入以太网接口配置视图或执行命令 <b>interface eth-trunk trunk-number</b> 进入 trunk 接口配置视图；</li> <li>3. 执行命令 <b>y1731 mep vlan vlan-id level level mepid mepid-id mac mac-address</b> 用来配置 MEP 的 MAC 地址；</li> <li>4. 结束。</li> </ol>
创建 MIP	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface gigabitEthernet interface-number</b> 进入以太网接口配置视图或执行命令 <b>interface eth-trunk trunk-number</b> 进入 trunk 接口配置视图；</li> <li>3. 执行命令 <b>y1731 mip vlan vlan-id level level</b> 用来创建 MIP；</li> <li>4. 结束。</li> </ol>
(可选) 配置 MIP 的 MAC 地址	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface gigabitEthernet interface-number</b> 进入以太网接口配置视图或执行命令 <b>interface eth-trunk trunk-number</b> 进入 trunk 接口配置视图；</li> <li>3. 执行命令 <b>y1731 mip vlan vlan-id level level mac mac-address</b> 用来配置 MIP 的 MAC 地址；</li> <li>4. 结束。</li> </ol>
(可选) 创建 MIP 自动生成的 VLAN 映射表	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>y1731</b> 从全局配置视图进入 Y.1731 配置视图；</li> <li>3. 执行命令 <b>mip auto-config vlan vlan-list</b> 用来创建 MIP 自动生成的 VLAN 映射表；</li> <li>4. 结束。</li> </ol>
(可选)使能或者禁用 MEG 的	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>y1731</b> 从全局配置视图进入 Y.1731 配置视图；</li> </ol>

目的	步骤
CCM 功能	<ol style="list-style-type: none"> <li>3. 执行命令 <b>meg vlan <i>vlan-id</i> level <i>level</i> icc <i>icc string</i> umc <i>umc string</i></b> 进入已创建的 MEG 配置视图；</li> <li>4. 执行命令 <b>ccm { enable   disable }</b> 用来配置是否使能 MEG 的 CCM 功能；</li> <li>5. 结束。</li> </ol>
(可选)使能或者禁用 MEG 的 AIS 功能	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>y1731</b> 从全局配置视图进入 Y.1731 配置视图；</li> <li>3. 执行命令 <b>meg vlan <i>vlan-id</i> level <i>level</i> icc <i>icc string</i> umc <i>umc string</i></b> 进入已创建的 MEG 配置视图；</li> <li>4. 执行命令 <b>ais { enable   disable }</b> 用来配置是否使能 MEG 的 AIS 功能；</li> <li>5. 结束。</li> </ol>
(可选)使能或者禁用静态 RMEP 校验	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>y1731</b> 从全局配置视图进入 Y.1731 配置视图；</li> <li>3. 执行命令 <b>meg vlan <i>vlan-id</i> level <i>level</i> icc <i>icc string</i> umc <i>umc string</i></b> 进入已创建的 MEG 配置视图；</li> <li>4. 执行命令 <b>cross-check { enable   disable }</b> 用来配置是否使能静态 RMEP 校验；</li> <li>5. 结束。</li> </ol>
(可选)使能或者禁用 MEG 的 LCK 功能	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>y1731</b> 从全局配置视图进入 Y.1731 配置视图；</li> <li>3. 执行命令 <b>meg vlan <i>vlan-id</i> level <i>level</i> icc <i>icc string</i> umc <i>umc string</i></b> 进入已创建的 MEG 配置视图；</li> <li>4. 执行命令 <b>lock { enable   disable }</b> 用来配置是否使能 MEG 的 LCK 功能；</li> <li>5. 结束。</li> </ol>
(可选)创建一个 RMEP	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>y1731</b> 从全局配置视图进入 Y.1731 配置视图；</li> <li>3. 执行命令 <b>meg vlan <i>vlan-id</i> level <i>level</i> icc <i>icc string</i> umc <i>umc string</i></b> 进入已创建的 MEG 配置视图；</li> <li>4. 执行命令 <b>remote-mep <i>mep-id</i> <i>mep-id</i> mac <i>mac address</i></b> 用来创建一个 RMEP；</li> <li>5. 结束。</li> </ol>
(可选)批量创建 RMEP	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>y1731</b> 从全局配置视图进入 Y.1731 配置视图；</li> <li>3. 执行命令 <b>meg vlan <i>vlan-id</i> level <i>level</i> icc <i>icc string</i> umc <i>umc string</i></b> 进入已创建的 MEG 配置视图；</li> <li>4. 执行命令 <b>remote-mep <i>mep-id</i> IDLIST</b> 用来批量创建 RMEP；</li> <li>5. 结束。</li> </ol>

附表：



参数	说明	取值
interface-number	指定物理接口号	SC9600 系列交换机支持以下 3 种型号的接口配置范围： SC9603: 取值范围是<1-3>/<0-4>/<1-48> SC9608: 取值范围是<1-8>/<0-4>/<1-48> SC9612: 取值范围是<1-12>/<0-4>/<1-48>
trunk-number	汇聚接口号	整数形式，取值范围是<1-8>
vlan-id	单个创建 MEG 对应的 VLAN ID	整数形式，取值范围是 1~4094
VLANLIST	批量创建 MEG 对应的多个 VLAN ID	整数形式，取值范围是 1~4094，多个 VLAN 之间用-分隔，比如 vlan 1-100
level	MEG 等级，一共有 8 个等级	整数形式，取值范围是 0~7 MEG 等级默认的分配如下： 客户角色分配三个 MEG 等级：7、6 和 5 提供商角色分配两个 MEG 等级：4 和 3 运营商角色分配三个 MEG 等级：2、1 和 0
lcc string	国际电联运营商编码	1-8 个字符、字母或者首位字母再加后面的数字所组成
umc string	唯一的 MEG ID 编码	由 7-12 个字母连同后面的 NULL (0) 组成

### 8.10.5 配置 Y.1731 相关参数

#### 目的

通过对 Y.1731 的相关参数进行调整，可以在以太网中更好地实现端到端的连通性故障检测。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
删除所有 MEG	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>y1731</b> 从全局配置视图进入 Y.1731 配置视图；</li> <li>3. 执行命令 <b>no meg all</b> 用来删除所有 MEG；</li> <li>4. 结束。</li> </ol>
使能或禁止 Y.1731 上报 SNMP 告警功能	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>y1731</b> 从全局配置视图进入 Y.1731 配置视图；</li> <li>3. 执行命令 <b>snmp trap { enable   disable }</b> 用来配置是否使能 Y.1731 上报 SNMP 告警功能；</li> <li>4. 结束。</li> </ol>
清除 MEG 的	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> </ol>

目的	步骤
Y.1731 帧计数	<ol style="list-style-type: none"> <li>2. 执行命令 <b>interface gigabernet interface-number</b> 进入以太网接口配置视图或执行命令 <b>interface eth-trunk trunk-number</b> 进入 trunk 接口配置视图；</li> <li>3. 执行命令 <b>y1731 mep vlan vlan-id level level mepid mepid-id reset counter</b> 用来清除 MEG 的 Y.1731 帧计数；</li> <li>4. 结束。</li> </ol>
清除接口的 Y.1731 帧计数	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface gigabernet interface-number</b> 进入以太网接口配置视图或执行命令 <b>interface eth-trunk trunk-number</b> 进入 trunk 接口配置视图；</li> <li>3. 执行命令 <b>y1731 reset counter</b> 用来清除接口的 Y.1731 帧计数；</li> <li>4. 结束。</li> </ol>
配置 MEP 的 AIS 丢失阈值	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>y1731</b> 从全局配置视图进入 Y.1731 配置视图；</li> <li>3. 执行命令 <b>meg vlan vlan-id level level icc icc string umc umc string</b> 进入已创建的 MEG 配置视图；</li> <li>4. 执行命令 <b>ais loss-threshold { loss-threshold   default }</b> 用来配置 MEP 的 AIS 丢失阈值；</li> <li>5. 结束。</li> </ol>
配置 MEP 的 AIS 发送周期	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>y1731</b> 从全局配置视图进入 Y.1731 配置视图；</li> <li>3. 执行命令 <b>meg vlan vlan-id level level icc icc string umc umc string</b> 进入已创建的 MEG 配置视图；</li> <li>4. 执行命令 <b>ais-interval { 1s   1min }</b> 用来配置 MEP 的 AIS 发送周期；</li> <li>5. 结束。</li> </ol>
配置 MEP 的 CCM 丢失阈值	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>y1731</b> 从全局配置视图进入 Y.1731 配置视图；</li> <li>3. 执行命令 <b>meg vlan vlan-id level level icc icc string umc umc string</b> 进入已创建的 MEG 配置视图；</li> <li>4. 执行命令 <b>ccm loss-threshold { loss-threshold   default }</b> 用来配置 MEP 的 CCM 丢失阈值；</li> <li>5. 结束。</li> </ol>
配置 MEP 的 CCM 发送周期	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>y1731</b> 从全局配置视图进入 Y.1731 配置视图；</li> <li>3. 执行命令 <b>meg vlan vlan-id level level icc icc string umc umc string</b> 进入已创建的 MEG 配置视图；</li> <li>4. 执行命令 <b>ccm-interval { 300Hz   10ms   100ms   1s   10s   1min   10min   default }</b> 用来配置 MEP 的 CCM 发送周期；</li> <li>5. 结束。</li> </ol>
配置静态 RMEP 的激活时间	<ol style="list-style-type: none"> <li>1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>y1731</b> 从全局配置视图进入 Y.1731 配置视图；</li> <li>3. 执行命令 <b>meg vlan vlan-id level level icc icc string umc umc string</b> 进入</li> </ol>

目的	步骤
	已创建的 MEG 配置视图； 4. 执行命令 <b>cross-check start-delay</b> { <i>start-delay-time</i>   <b>default</b> } 用来配置静态 RMEP 的激活时间； 5. 结束。
配置 MEP 的 LCK 丢失阈值	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>y1731</b> 从全局配置视图进入 Y.1731 配置视图； 3. 执行命令 <b>meg vlan</b> <i>vlan-id level level icc icc string umc umc string</i> 进入已创建的 MEG 配置视图； 4. 执行命令 <b>lock loss-threshold</b> { <i>loss-threshold</i>   <b>default</b> } 用来配置 MEP 的 LCK 丢失阈值； 5. 结束。
配置 MEP 的 LCK 发送周期	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>y1731</b> 从全局配置视图进入 Y.1731 配置视图； 3. 执行命令 <b>meg vlan</b> <i>vlan-id level level icc icc string umc umc string</i> 进入已创建的 MEG 配置视图； 4. 执行命令 <b>lock-interval</b> { <i>1s</i>   <i>1min</i> } 用来配置 MEP 的 LCK 发送周期； 5. 结束。
删除指定 MEG 下某个 RMEP 或者所有 RMEP 或删除指定 MEG 下 RMEP	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>y1731</b> 从全局配置视图进入 Y.1731 配置视图； 3. 执行命令 <b>meg vlan</b> <i>vlan-id level level icc icc string umc umc string</i> 进入已创建的 MEG 配置视图； 4. 执行命令 <b>no remote-mep</b> <i>mep-id</i> 用来删除指定 MEG 下某个 RMEP 或者所有 RMEP 或执行命令 <b>no remote-mep all</b> 用来删除指定 MEG 下 RMEP； 5. 结束。
删除指定 MEG 下所有 MEP	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>y1731</b> 从全局配置视图进入 Y.1731 配置视图； 3. 执行命令 <b>meg vlan</b> <i>vlan-id level level icc icc string umc umc string</i> 进入已创建的 MEG 配置视图； 4. 执行命令 <b>no y1731 mep all</b> 用来删除指定 MEG 下所有 MEP； 5. 结束。
删除指定 MEG 下所有 MIP	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>y1731</b> 从全局配置视图进入 Y.1731 配置视图； 3. 执行命令 <b>meg vlan</b> <i>vlan-id level level icc icc string umc umc string</i> 进入已创建的 MEG 配置视图； 4. 执行命令 <b>no y1731 mip all</b> 用来删除指定 MEG 下所有 MIP； 5. 结束。
配置动态 RMEP 的老化时间	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>y1731</b> 从全局配置视图进入 Y.1731 配置视图； 3. 执行命令 <b>meg vlan</b> <i>vlan-id level level icc icc string umc umc string</i> 进入

目的	步骤
	已创建的 MEG 配置视图； 4. 执行命令 <b>remote-mep aging-time { aging-time   default }</b> 用来配置动态 RMEP 的老化时间； 5. 结束。
配置 LTR 应答响应的老化时间	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>y1731</b> 从全局配置视图进入 Y.1731 配置视图； 3. 执行命令 <b>meg vlan vlan-id level level icc icc string umc umc string</b> 进入已创建的 MEG 配置视图； 4. 执行命令 <b>trace-reply aging-time { aging-time   default }</b> 用来配置 LTR 应答响应的老化时间； 5. 结束。
清除 MEG 的 Y.1731 帧计数	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>y1731</b> 从全局配置视图进入 Y.1731 配置视图； 3. 执行命令 <b>meg vlan vlan-id level level icc icc string umc umc string</b> 进入已创建的 MEG 配置视图； 4. 执行命令 <b>reset counter</b> 用来清除 MEG 的 Y.1731 帧计数； 5. 结束。
配置 Y.1731 报文的 Sender ID TLV 类型	1. 在特权用户视图下执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>y1731</b> 从全局配置视图进入 Y.1731 配置视图； 3. 执行命令 <b>meg vlan vlan-id level level icc icc string umc umc string</b> 进入已创建的 MEG 配置视图； 4. 执行命令 <b>senderid-tlv-type { none   chassis   manage   chassis-manage   defer }</b> 用来配置 Y.1731 报文的 Sender ID TLV 类型； 5. 结束。

附表：

参数	说明	取值
interface-number	指定物理接口号	SC9600 系列交换机支持以下 3 种型号的接口配置范围： SC9603: 取值范围是<1-3>/<0-4>/<1-48> SC9608: 取值范围是<1-8>/<0-4>/<1-48> SC9612: 取值范围是<1-12>/<0-4>/<1-48>
trunk-number	汇聚接口号	整数形式，取值范围是<1-8>
vlan-id	指定 MA 映射的 VLAN ID	整数形式，取值范围是 1~4094
level	指定 MA 级别	整数形式，取值范围是 0~7
mepid-id	mep 对应的 meg，默认 mep 为 outward	整数形式，取值范围是 1~8191
loss-threshold	AIS 丢失阈值	整数取值，取值范围是 2-255
default	表示默认 AIS 丢失阈值	3.5
loss-threshold	CCM 丢失阈值	整数取值，取值范围是 2-255

参数	说明	取值
default	表示默认 CCM 丢失阈值	3.5
start-delay-time	静态 RMEP 的激活时间	整数取值，取值范围是 1-65535，单位为秒
default	表示默认激活时间	0
loss-threshold	AIS 丢失阈值	整数取值，取值范围是 2-255
default	表示默认 LCK 丢失阈值	3.5
aging-time	动态 RMEP 的老化时间	整数取值，取值范围是 1-65535，单位为秒
default	表示默认值	1000 秒
aging-time	指定 LTR 应答响应的老化时间	整数形式，取值范围是 1~65535
default	指定 LTR 应答响应的默认老化时间	1000 秒

### 8.10.6 配置 Y.1731 故障确认

#### 目的

当需要手动检测两台设备之间的链路连通性时，可以使用本节操作发送测试报文和接收应答报文，从而检测从本设备到目的设备是否可达。



注意：

对于本地 UP MEP，如果关联两个及两个以上 MIP，应确保 MIP 连接的网络只有一条二层数据业务通路（这通常是由生成树或以太网环协议来保证的），否则 Y.1731 的故障确认结果是不可预知的。

配置 Y.1731 故障确认在设备根节点下进行，如需终止发送 LBM，可按 <Ctrl+C> 快捷键。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置通过 PING MAC 确认 Y.1731 连通性故障	<ol style="list-style-type: none"> <li>保持当前特权用户视图；</li> <li>执行命令 <code>y1731 ping mac mac-address mep vlan vlan-id level level mepid mep-id</code> 或执行命令 <code>y1731 ping mac mac-address mep vlan vlan-id level level mepid mep-id -c packet-count -s packet-size -t packet-timeout</code> 或执行命令 <code>y1731 ping mac mac-address mep vlan vlan-id level level mepid mep-id priority priority -c packet-count -s packet-size -t packet-timeout</code> 通过 PING MAC 确认 Y.1731 连通性故障；</li> <li>结束。</li> </ol>

目的	步骤
配置通过 PING Remote MEP 确认 Y.1731 连通性故障	1. 保持当前特权用户视图； 2. 执行命令 <b>y1731 ping remote-mep remote-mep-id mep vlan vlan-id level level mepid mep-id</b> 或执行命令 <b>y1731 ping remote-mep remote-mep-id mep vlan vlan-id level level mepid mep-id -c packet-count -s packet-size -t packet-timeout</b> 或执行命令 <b>y1731 ping remote-mep remote-mep-id mep vlan vlan-id level level mepid mep-id priority priority -c packet-count -s packet-size -t packet-timeout</b> 通过 PING Remote MEP 确认 Y.1731 连通性故障； 3. 结束。
配置通过 PING All Remote MEP 确认 Y.1731 连通性故障	1. 保持当前特权用户视图； 2. 执行命令 <b>y1731 ping all remote-mep vlan vlan-id level level mepid mep-id</b> 或执行命令 <b>y1731 ping all remote-mep vlan vlan-id level level mepid mep-id -s packet-size -t packet-timeout</b> 或执行命令 <b>y1731 ping all remote-mep vlan vlan-id level level mepid mep-id priority priority -s packet-size -t packet-timeout</b> 通过 PING All Remote MEP 确认 Y.1731 连通性故障； 3. 结束。

附表：

参数	说明	取值
vlan-id	指定 MA 映射的 VLAN ID	整数形式，取值范围是 1~4094
level	指定 MA 级别	整数形式，取值范围是 0~7
mep-id	指定 mep 对应的 meg	整数形式，取值范围是 1~8191
remote-mep-id	指定 remote mep 对应的 meg	整数形式，取值范围是 1~8191
priority	指定优先级	整数形式，取值范围是 0~7
packet-size	指定发送 PING 报文的大小，改大小是指包括二层报文头部的报文大小	整数形式，取值范围是 64~1518
packet-timeout	指定等待应答报文的超时时间	整数形式，取值范围是 1~60
packet-count	指定 PING 的次数	整数形式，取值范围是 1~1024

### 8.10.7 配置 Y.1731 故障定位

#### 目的

当需要定位两台设备之间的链路连通性故障时，可以使用本节操作发送测试报文和接收应答报文，从而检测从本设备到目的设备的路径或定位故障点。



注意：

对于本地 UP MEP，如果关联两个及两个以上 MIP，应确保 MIP 连接的网络只有一条二层数据业务通路（这通常是由生成树或以太网环协议来保证的），否则 Y.1731 的故障定位结果是不可预知的。

配置 Y.1731 故障定位在设备根节点下进行，Trace 结果在设置的超时时间后自动列出。如需提前终止 Trace，可按 <Ctrl+C> 快捷键。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置通过 Trace MAC 进行 Y.1731 连通性故障定位	1. 保持当前特权用户视图； 2. 执行命令 <b>y1731 trace mac mac-address mep vlan vlan-id level level mepid mep-id</b> 或执行命令 <b>y1731 trace mac mac-address mep vlan vlan-id level level mepid mep-id -t packet-timeout</b> 或执行命令 <b>y1731 trace mac mac-address mep vlan vlan-id level level mepid mep-id priority priority</b> 或执行命令 <b>y1731 trace mac mac-address mep vlan vlan-id level level mepid mep-id priority priority t packet-timeout</b> 或执行命令 <b>y1731 trace mac mac-address mep vlan vlan-id level level mepid mep-id priority priority ttl ttl-value</b> 或执行命令 <b>y1731 trace mac mac-address mep vlan vlan-id level level mepid mep-id -ttl ttl-value</b> 通过 Trace MAC 进行 Y.1731 连通性故障定位； 3. 结束。
配置通过 Trace Remote MEP 进行 Y.1731 连通性故障定位	1. 保持当前特权用户视图； 2. 执行命令 <b>y1731 trace remote-mep remote-mep-id mep vlan vlan-id level level mepid mep-id</b> 或执行命令 <b>y1731 trace remote-mep remote-mep-id mep vlan vlan-id level level mepid mep-id -t packet-timeout</b> 或执行命令 <b>y1731 trace remote-mep remote-mep-id mep vlan vlan-id level level mepid mep-id priority priority</b> 或执行命令 <b>y1731 trace remote-mep remote-mep-id mep vlan vlan-id level level mepid mep-id priority priority -t packet-timeout</b> 或执行命令 <b>y1731 trace remote-mep remote-mep-id mep vlan vlan-id level level mepid mep-id priority priority ttl ttl-value</b> 或执行命令 <b>y1731 trace remote-mep remote-mep-id mep vlan vlan-id level level mepid mep-id ttl ttl-value</b> 通过 Trace Remote MEP 进行 Y.1731 连通性故障定位；

目的	步骤
	3. 结束。

附表：

参数	说明	取值
mac-address	指定远端 MEP 或 MIP 的 MAC	形如 AA:BB:CC:DD:EE:FF，其中 A~F 为一位十六进制数
vlan-id	指定 VLAN ID	整数形式，取值范围是 1~4094
level	指定级别	整数形式，取值范围是 0~7
remote-mep-id	指定远端网桥的 MEP ID	整数形式，取值范围是 1~8191
mep-id	指定本地网桥发起 Trace 操作的 MEP ID	整数形式，取值范围是 1~8191
priority	指定优先级	整数形式，取值范围是 0~7
packet-timeout	指定等待应答报文的超时时间	整数形式，取值范围是 1~60，单位：秒，默认为 5 秒
ttr-value	指定 Trace 跟踪的最大跳数	整数形式，取值范围是 1~255，默认为 64 跳

### 8.10.8 配置单向丢包率测试

#### 目的

用于测试一对 MEP 所在物理接口链路间的丢包率过程，可以使用本节单向丢包率测试操作。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置单向丢包率测试	1. 保持当前特权用户视图； 2. 执行命令 <b>y1731 single-ended-lm mac mac-address mep vlan vlan-id level level mepid mep-id</b> 或执行命令 <b>y1731 single-ended-lm mac mac-address mep vlan vlan-id level level mepid mep-id hold-time hold-time</b> 或执行命令 <b>y1731 single-ended-lm mac mac-address mep vlan vlan-id level level mepid mep-id lmm-interval { 100ms   1s } hold-time hold-time</b> 或执行命令 <b>y1731 single-ended-lm mac mac-address mep vlan vlan-id level level mepid mep-id priority priority</b> 或执行命令 <b>y1731 single-ended-lm mac mac-address mep vlan vlan-id level level mepid mep-id priority priority hold-time hold-time</b> 或执行命令 <b>y1731 single-ended-lm mac mac-address mep vlan vlan-id</b>



目的	步骤
	<p><b>level level mepid mep-id priority priority lmm-interval { 100ms   1s }</b> 或执行命令 <b>y1731 single-ended-lm mac mac-address mep vlan vlan-id level level mepid mep-id priority priority lmm-interval { 100ms   1s } hold-time hold-time</b> 配置单向丢包率测试；</p> <p>3. 结束。</p>
	<p>1. 保持当前特权用户视图；</p> <p>2. 执行命令 <b>y1731 single-ended-lm remote-mep remotemep-id mep vlan vlan-id level level mepid mep-id</b> 或执行命令 <b>y1731 single-ended-lm remote-mep remotemep-id mep vlan vlan-id level level mepid mep-id hold-time hold-time</b> 或执行命令 <b>y1731 single-ended-lm remote-mep remotemep-id mep vlan vlan-id level level mepid mep-id lmm-interval { 100ms   1s } hold-time hold-time</b> 或执行命令 <b>y1731 single-ended-lm remote-mep remotemep-id mep vlan vlan-id level level mepid mep-id priority priority</b> 或执行命令 <b>y1731 single-ended-lm remote-mep remotemep-id mep vlan vlan-id level level mepid mep-id priority priority hold-time hold-time</b> 或执行命令 <b>y1731 single-ended-lm remote-mep remotemep-id mep vlan vlan-id level level mepid mep-id priority priority lmm-interval { 100ms   1s }</b> 或执行命令 <b>y1731 single-ended-lm remote-mep remotemep-id mep vlan vlan-id level level mepid mep-id priority priority lmm-interval { 100ms   1s } hold-time hold-time</b> 配置单向丢包率测试；</p> <p>3. 结束。</p>

附表：

参数	说明	取值
remote-mep-id	指定远端 MEP ID	整数形式，取值范围是 1~8191
vlan-id	指定 MEP 所属 MEG 的 VLAN ID	整数形式，取值范围是 1~4094
level	指定 MEP 所属 MEG 的级别	整数形式，取值范围是 0~7
mep-id	指定发起单向丢包率测试 MEP 的 ID	整数形式，取值范围是 1~8191
mac-address	指定远端 MEP 的 MAC 地址	形如 AA:BB:CC:DD:EE:FF，其中 A~F 分别为一位十六进制数
priority	指定单向丢包率测试发包优先级	整数形式，取值范围是 0~7
lmm-interval	表示单向丢包率测试发包频率	-
hold-time	指定单向丢包率测试时间	整数形式，取值范围是 10~255s

### 8.10.9 配置双向时延/抖动测试

目的

用于测试一对 MEP 所在物理接口链路间的时延/抖动，可以使用本节双向时延/抖动测试操作。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置双向时延/抖动测试	<p>1. 保持当前特权用户视图；</p> <p>2. 执行命令 <b>y1731 two-way-dm mac mac-address mep vlan vlan-id level level mepid mep-id</b>                      或执行命令 <b>y1731 two-way-dm mac mac-address mep vlan vlan-id level level mepid mep-id hold-time hold-time</b>                      或执行命令 <b>y1731 two-way-dm mac mac-address mep vlan vlan-id level level mepid mep-id dmm-interval { 100ms   1s } hold-time hold-time</b>                      或执行命令 <b>y1731 two-way-dm mac mac-address mep vlan vlan-id level level mepid mep-id priority priority</b>                      或执行命令 <b>y1731 two-way-dm mac mac-address mep vlan vlan-id level level mepid mep-id priority priority dmm-interval { 100ms   1s }</b>                      或执行命令 <b>y1731 two-way-dm mac mac-address mep vlan vlan-id level level mepid mep-id priority priority dmm-interval { 100ms   1s } hold-time hold-time</b>                      或执行命令 <b>y1731 two-way-dm mac mac-address mep vlan vlan-id level level mepid mep-id priority priority hold-time hold-time</b> 配置双向时延/抖动测试；</p> <p>3. 结束。</p>
	<p>1. 保持当前特权用户视图；</p> <p>2. 执行命令 <b>y1731 two-way-dm remote-mep remotemep-id mep vlan vlan-id level level mepid mep-id</b>                      或执行命令 <b>y1731 two-way-dm remote-mep remotemep-id mep vlan vlan-id level level mepid mep-id dmm-interval { 100ms   1s } hold-time hold-time</b>                      或执行命令 <b>y1731 two-way-dm remote-mep remotemep-id mep vlan vlan-id level level mepid mep-id hold-time hold-time</b>                      或执行命令 <b>y1731 two-way-dm remote-mep remotemep-id mep vlan vlan-id level level mepid mep-id priority priority</b>                      或执行命令 <b>y1731 two-way-dm remote-mep remotemep-id mep vlan vlan-id level level mepid mep-id priority priority dmm-interval { 100ms   1s }</b>                      或执行命令 <b>y1731 two-way-dm remote-mep remotemep-id mep vlan vlan-id level level mepid mep-id priority priority dmm-interval { 100ms   1s } hold-time hold-time</b>                      或执行命令 <b>y1731 two-way-dm remote-mep remotemep-id mep vlan vlan-id level level mepid mep-id priority priority hold-time hold-time</b> 配置双向时延/抖</p>

目的	步骤
	动测试； 3. 结束。

附表：

参数	说明	取值
remote-mep-id	指定远端 MEP ID	整数形式，取值范围是 1~8191
vlan-id	指定 MEP 所属 MEG 的 VLAN ID	整数形式，取值范围是 1~4094
level	指定 MEP 所属 MEG 的级别	整数形式，取值范围是 0~7
mep-id	指定发起双向时延/抖动测试 MEP 的 ID	整数形式，取值范围是 1~8191
mac-address	指定远端 MEP 的 MAC 地址	形如 AA:BB:CC:DD:EE:FF，其中 A~F 分别为一位十六进制数
priority	指定双向时延/抖动测试发包优先级	整数形式，取值范围是 0~7
dmm-interval	表示双向时延/抖动测试发包频率	-
hold-time	指定双向时延/抖动测试时间	整数形式，取值范围是 10~255

### 8.10.10 配置双向吞吐量测试

#### 目的

用于测试一对 MEP 所在物理接口链路间的吞吐量，可以使用本节双向吞吐量测试操作。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置双向吞吐量测试	1. 保持当前特权用户视图； 2. 执行命令 <b>y1731 lbtst-throughput mac mac-address mep vlan vlan-id level level mepid mep-id -s packet-size</b> 或执行命令 <b>y1731 lbtst-throughput mac mac-address mep vlan vlan-id level level mepid mep-id priority priority -s packet-size</b> 配置双向吞吐量测试； 3. 结束。
	1. 保持当前特权用户视图； 2. 执行命令 <b>y1731 lbtst-throughput remote-mep remotemep-id mep vlan vlan-id level level mepid mep-id -s packet-size</b> 或执行命令 <b>y1731 lbtst-throughput remote-mep remotemep-id mep vlan vlan-id level level mepid mep-id priority priority -s packet-size</b> 配置双向吞吐量测试； 3. 结束。

附表：

参数	说明	取值
remote-mep-id	指定远端 MEP ID	整数形式，取值范围是 1~8191
vlan-id	指定 MEP 所属 MEG 的 VLAN ID	整数形式，取值范围是 1~4094
level	指定 MEP 所属 MEG 的级别	整数形式，取值范围是 0~7
mep-id	指定发起双向吞吐量测试 MEP 的 ID	整数形式，取值范围是 1~8191
mac-address	指定远端 MEP 的 MAC 地址	形如 AA:BB:CC:DD:EE:FF，其中 A~F 分别为一位十六进制数
priority	指定双向吞吐量测试发包优先级	整数形式，取值范围是 0~7
packet-size	指定双向吞吐量测试报文长度	整数形式，取值范围是 64~1518

### 8.10.11 维护及调试

#### 目的

当 Y.1731 功能不正常，需要进行查看、调试或定位问题时，可以使用本小节操作。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
打开 Y1731 接口数据包调试功能	<ol style="list-style-type: none"> <li>保持当前特权用户视图；</li> <li>执行命令 <code>debug y1731 packet { ccm-tx   ccm-rx   lbr-tx   lbr-rx   lbrm-tx   lbrm-rx   ltr-rx   ltr-tx   ltm-rx   ltm-tx   ais-tx   ais-rx   lock-tx   lock-rx   tst-tx   tst-rx   mcc-tx   mcc-rx   lmr-tx   lmr-rx   lmm-tx   lmm-rx   1dm   dmr-tx   dmr-rx   dmm-tx   dmm-rx   exp   vsp   all } interface { fastethernet gigaethernet xgigaethernet } interface-number</code> 或执行命令 <code>debug y1731 packet { ccm-tx   ccm-rx   lbr-tx   lbr-rx   lbrm-tx   lbrm-rx   ltr-rx   ltr-tx   ltm-rx   ltm-tx   ais-tx   ais-rx   lock-tx   lock-rx   tst-tx   tst-rx   mcc-tx   mcc-rx   lmr-tx   lmr-rx   lmm-tx   lmm-rx   1dm   dmr-tx   dmr-rx   dmm-tx   dmm-rx   exp   vsp   all } interface eth-trunk trunk-number</code> 打开 Y1731 接口数据包调试功能；</li> <li>结束。</li> </ol>
关闭 Y1731 接口数据包调试功能	<ol style="list-style-type: none"> <li>保持当前特权用户视图；</li> <li>执行命令 <code>no debug y1731 packet { ccm-tx   ccm-rx   lbr-tx   lbr-rx   lbrm-tx   lbrm-rx   ltr-rx   ltr-tx   ltm-rx   ltm-tx   ais-tx   ais-rx   lock-tx   lock-rx   tst-tx   tst-rx   mcc-tx   mcc-rx   lmr-tx   lmr-rx   lmm-tx   lmm-rx   1dm   dmr-tx   dmr-rx   dmm-tx   dmm-rx   exp   vsp   all } interface { fastethernet gigaethernet xgigaethernet } interface-number</code> <code>o debug y1731 packet { ccm-tx   ccm-rx   lbr-tx   lbr-rx   lbrm-tx   lbrm-rx   ltr-rx   ltr-tx   ltm-rx   ltm-tx   ais-tx   ais-rx   lock-tx   lock-rx   tst-tx   tst-rx   mcc-tx   mcc-rx   lmr-tx   lmr-rx   lmm-tx   lmm-rx   1dm   dmr-tx   dmr-rx   dmm-tx   dmm-rx   exp   vsp   all } interface eth-trunk</code></li> </ol>

目的	步骤
	<p><i>trunk-number</i> 关闭 Y1731 接口数据包调试功能;</p> <p>3. 结束。</p>
打开 Y1731 模块调试功能	<p>1. 保持当前特权用户视图;</p> <p>2. 执行命令 <b>debug y1731 module { nm   main   trap   ccm-tx   ccm-rx   lbr-tx   lbr-rx   lbr-tx   lbr-rx   ltr-tx   ltr-rx   ltm-tx   ltm-rx   ais-tx   ais-rx   lock-tx   lock-rx   tst-tx   tst-rx   mcc-tx   mcc-rx   lmr-tx   lmr-rx   lmm-tx   lmm-rx   1dm   dmr-tx   dmr-rx   dmm-tx   dmm-rx   exp   vsp   all }</b>打开 Y1731 模块调试功能;</p> <p>3. 结束。</p>
关闭 Y1731 模块调试功能	<p>1. 保持当前特权用户视图;</p> <p>2. 执行命令 <b>no debug y1731 module { nm   main   trap   ccm-tx   ccm-rx   lbr-tx   lbr-rx   lbr-tx   lbr-rx   ltr-tx   ltr-rx   ltm-tx   ltm-rx   ais-tx   ais-rx   lock-tx   lock-rx   tst-tx   tst-rx   mcc-tx   mcc-rx   lmr-tx   lmr-rx   lmm-tx   lmm-rx   1dm   dmr-t x   dmr-rx   dmm-tx   dmm-rx   exp   vsp   all }</b>关闭 Y1731 模块调试功能;</p> <p>3. 结束。</p>
查看 Y.1731 全局配置信息	<p>1.执行命令 <b>interface { fastethernet   gigasethernet   xgigasethernet } interface-number</b> 或执行命令 <b>interface eth-trunk trunk-number</b> 进入接口配置视图, 或执行命令 <b>meg vlan VLANLIST level level</b> 或执行命令 <b>meg vlan vlan-id level level icc icc string umc umc string</b> 创建并进入 MEG 配置视图, 或不执行任何命令保持当前特权用户视图;</p> <p>2. 执行命令 <b>show y1731</b> 显示 Y.1731 全局配置信息;</p> <p>3. 结束。</p>
查看 MEP CCDB 的概要或详细信息	<p>1.执行命令 <b>interface { fastethernet   gigasethernet   xgigasethernet } interface-number</b> 或执行命令 <b>interface eth-trunk trunk-number</b> 进入接口配置视图, 或执行命令 <b>meg vlan VLANLIST level level</b> 或执行命令 <b>meg vlan vlan-id level level icc icc string umc umc string</b> 创建并进入 MEG 配置视图, 或不执行任何命令保持当前特权用户视图;</p> <p>2. 执行命令 <b>show y1731 ccdb</b> 显示 MEP CCDB 的概要信息或执行命令 <b>show y1731 ccdb remote-mep-id vlan vlan-id level level mepid mep-id</b> 显示 MEP CCDB 详细信息;</p> <p>3. 结束。</p>
查看 Y.1731 配置文件的信息	<p>1.执行命令 <b>interface { fastethernet   gigasethernet   xgigasethernet } interface-number</b> 或执行命令 <b>interface eth-trunk trunk-number</b> 进入接口配置视图, 或执行命令 <b>meg vlan VLANLIST level level</b> 或执行命令 <b>meg vlan vlan-id level level icc icc string umc umc string</b> 创建并进入 MEG 配置视图, 或不执行任何命令保持当前特权用户视图;</p> <p>2. 执行命令 <b>show y1731 config</b> 显示 Y.1731 配置文件的信息;</p> <p>3. 结束。</p>

目的	步骤
查看设备配置的所有 MEP 的 error ccdb 概要信息或具体 MEP 的 error ccdb 详细信息	<ol style="list-style-type: none"> <li>1. 执行命令 <code>interface { fastethernet   gig Ethernet   xgig Ethernet } interface-number</code> 或执行命令 <code>interface eth-trunk trunk-number</code> 进入接口配置视图，或执行命令 <code>meg vlan VLANLIST level level</code> 或执行命令 <code>meg vlan vlan-id level level icc icc string umc umc string</code> 创建并进入 MEG 配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <code>show y1731 error ccdb</code> 显示设备配置的所有 MEP 的 error ccdb 概要信息或执行命令 <code>show y1731 error ccdb remote-mep-id vlan vlan-id level level mepid mep-id</code> 显示设备配置的具体 MEP 的 error ccdb 详细信息；</li> <li>3. 结束。</li> </ol>
查看设备配置的所有 MEG	<ol style="list-style-type: none"> <li>1. 执行命令 <code>interface { fastethernet   gig Ethernet   xgig Ethernet } interface-number</code> 或执行命令 <code>interface eth-trunk trunk-number</code> 进入接口配置视图，或执行命令 <code>meg vlan VLANLIST level level</code> 或执行命令 <code>meg vlan vlan-id level level icc icc string umc umc string</code> 创建并进入 MEG 配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <code>show y1731 meg</code> 或执行命令 <code>show y1731 meg vlan vlan-id level level</code> 显示设备配置的所有 MEG；</li> <li>3. 结束。</li> </ol>
查看 MEP 概要信息或 MEP 详细信息	<ol style="list-style-type: none"> <li>1. 执行命令 <code>interface { fastethernet   gig Ethernet   xgig Ethernet } interface-number</code> 或执行命令 <code>interface eth-trunk trunk-number</code> 进入接口配置视图，或执行命令 <code>meg vlan VLANLIST level level</code> 或执行命令 <code>meg vlan vlan-id level level icc icc string umc umc string</code> 创建并进入 MEG 配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <code>show y1731 mep</code> 显示 MEP 概要信息或执行命令 <code>show y1731 mep vlan vlan-id level level mepid mep-id</code> 显示 MEP 详细信息；</li> <li>3. 结束。</li> </ol>
查看设备配置的所有 MIP 的信息	<ol style="list-style-type: none"> <li>1. 执行命令 <code>interface { fastethernet   gig Ethernet   xgig Ethernet } interface-number</code> 或执行命令 <code>interface eth-trunk trunk-number</code> 进入接口配置视图，或执行命令 <code>meg vlan VLANLIST level level</code> 或执行命令 <code>meg vlan vlan-id level level icc icc string umc umc string</code> 创建并进入 MEG 配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <code>show y1731 mip</code> 显示设备配置的所有 MIP 的信息；</li> <li>3. 结束。</li> </ol>
查看接口 Y.1731 帧统计结果	<ol style="list-style-type: none"> <li>1. 执行命令 <code>interface { fastethernet   gig Ethernet   xgig Ethernet } interface-number</code> 或执行命令 <code>interface eth-trunk trunk-number</code> 进入接口配置视图，或执行命令 <code>meg vlan VLANLIST level level</code> 或执行命令 <code>meg vlan vlan-id level level icc icc string umc umc string</code> 创建并进入 MEG 配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <code>show y1731 pdu-statistic interface</code> 或执行命令 <code>show y1731 pdu-statistic interface { fastethernet   gig Ethernet   xgig Ethernet }</code></li> </ol>

目的	步骤
	<p><code>interface-number</code> 或执行命令 <code>show y1731 pdu-statistic interface eth-trunk trunk-number</code> 显示接口 Y.1731 帧统计结果;</p> <p>3. 结束。</p>
查看设备配置的所有 remote-mep 的概要信息或具体 remote-mep 的详细信息	<p>1. 执行命令 <code>interface { fastethernet   gigasethernet   xgigasethernet } interface-number</code> 或执行命令 <code>interface eth-trunk trunk-number</code> 进入接口配置视图, 或执行命令 <code>meg vlan VLANLIST level level</code> 或执行命令 <code>meg vlan vlan-id level level icc icc string umc umc string</code> 创建并进入 MEG 配置视图, 或不执行任何命令保持当前特权用户视图;</p> <p>2. 执行命令 <code>show y1731 remote-mep</code> 显示设备配置的所有 remote-mep 的概要信息或执行命令 <code>show y1731 remote-mep vlan vlan-id level level mepid mep-id</code> 显示设备配置的具体 remote-mep 的详细信息;</p> <p>3. 结束。</p>
查看设备配置的 MEP 最近一次故障定位查询的结果	<p>1. 执行命令 <code>interface { fastethernet   gigasethernet   xgigasethernet } interface-number</code> 或执行命令 <code>interface eth-trunk trunk-number</code> 进入接口配置视图, 或执行命令 <code>meg vlan VLANLIST level level</code> 或执行命令 <code>meg vlan vlan-id level level icc icc string umc umc string</code> 创建并进入 MEG 配置视图, 或不执行任何命令保持当前特权用户视图;</p> <p>2. 执行命令 <code>show y1731 trace-result mep vlan vlan-id level level mepid mep-id</code> 显示设备配置的 MEP 最近一次故障定位查询的结果;</p> <p>3. 结束。</p>

附表:

参数	说明	取值
interface-number	指定物理接口号	SC9600 系列交换机支持以下 3 种型号的接口配置范围: SC9603: 取值范围是<1-3>/<0-4>/<1-48> SC9608: 取值范围是<1-8>/<0-4>/<1-48> SC9612: 取值范围是<1-12>/<0-4>/<1-48>
trunk-number	指定 trunk 接口号	整数形式, 取值范围是 1~8
remote-mep-id	指定远端 MEP ID	整数形式, 取值范围是 1~8191
vlan-id	指定 VLAN ID	整数形式, 取值范围是 1~4094
level	指定 MEP 级别	整数形式, 取值范围是 0~7
mep-id	指定本地 MEP ID	整数形式, 取值范围是 1~8191

### 8.10.12 配置举例

#### 组网要求

本示例主要介绍多维护实体组合情况下 Y.1731 连通性故障管理的配置。

将设备 wh-SC9600、cs、nc、hf、zz 划归维护实体组合 icc v1 umc fhn1，配置 MEG 等级为 1；

将设备 cd、gz、sh、bj 划归维护实体组合 icc v1 umc fhn6，配置 MEG 等级为 6，由于其维护实体组合的 MEG 等级高于维护实体组合 icc v1 umc fhn1 的维护实体组合等级，所以维护实体组合 icc v1 umc fhn6 的 Y.1731 报文可以透明穿越维护实体组合 icc v1 umc fhn1，二者互不干扰。

划分完维护实体组合，即可根据图 8-42所示拓扑确定维护实体组合边界，同时可以确定各维护实体组合 MEP 的配置接口，只要保证维护实体组合下 MEP ID 不重复即可。

如果需要对维护实体中间点进行 Y.1731 故障管理的话，只需要将维护实体组合中间点配置为 MIP 即可，对维护实体组合 icc v1 umc fhn1 边界 MEP 所在接口配置维护实体组合 icc v1 umc fhn6 的中间点 MIP。

组网图

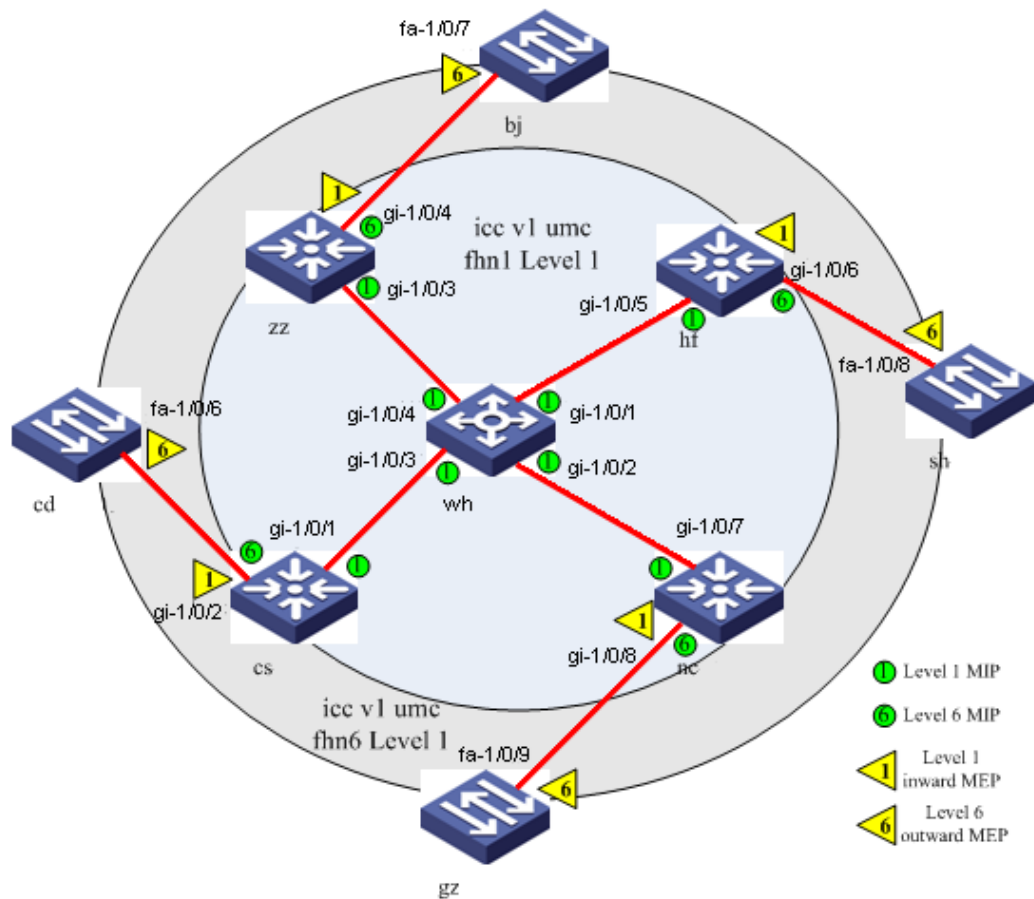


图 8-42 Y1731 配置组网图



**配置步骤**

每台网桥配置如下：

1、配置维护实体组合 icc v1 umc fhn1。

1) 配置 wh-SC9600

```
wh-SC9600#configure
wh-SC9600(config)#y1731
wh-SC9600(config-y1731)#meg vlan 1 level 1 icc v1 umc fhn1
wh-SC9600(config-meg-v1-fhn1)#quit
wh-SC9600(config)#interface gigabitEthernet 1/0/1 to gigabitEthernet 1/0/4
wh-SC9600(config-ge1/0/1->ge1/0/4)#y1731 mip vlan 1 level 1
```

2) 配置 cs

```
cs#configure
cs(config)#y1731
cs(config-y1731)#meg vlan 1 level 1 icc v1 umc fhn1
cs(config-meg-v1-fhn1)#quit
cs(config-y1731)#meg vlan 1 level 6 icc v1 umc fhn6
cs(config-meg-v1-fhn6)#quit
cs(config)#interface gigabitEthernet 1/0/1
cs(config-ge1/0/1)#y1731 mip vlan 1 level 1
cs(config-ge1/0/1)#quit
cs(config)#interface gigabitEthernet 1/0/2
cs(config-ge1/0/2)#y1731 mip vlan 1 level 6
cs(config-ge1/0/2)#y1731 mep vlan 1 level 1 mepid 1 inward
cs(config-ge1/0/2)#y1731 mep vlan 1 level 1 mepid 1 ccm enable
cs(config-ge1/0/2)#y1731 mep vlan 1 level 1 mepid 1 ais enable
```

3) 配置 nc

```
nc#configure
nc(config)#y1731
nc(config-y1731)#meg vlan 1 level 1 icc v1 umc fhn1
nc(config-meg-v1-fhn1)#quit
nc(config-y1731)#meg vlan 1 level 6 icc v1 umc fhn6
nc(config-meg-v1-fhn6)#quit
```

```
nc(config)#interface gigabitEthernet 1/0/7
nc(config-ge1/0/7)#y1731 mip vlan 1 level 1
nc(config-ge1/0/7)#quit
nc(config)#interface gigabitEthernet 1/0/8
nc(config-ge1/0/8)#y1731 mip vlan 1 level 6
nc(config-ge1/0/8)#y1731 mep vlan 1 level 1 mepid 100 inward
nc(config-ge1/0/8)#y1731 mep vlan 1 level 1 mepid 100 ccm enable
nc(config-ge1/0/8)#y1731 mep vlan 1 level 1 mepid 100 ais enable
```

#### 4) 配置 hf

```
hf#configure
hf(config)#y1731
hf(config-y1731)#mep vlan 1 level 1 icc v1 umc fhn1
hf(config-mep-v1-fhn1)#quit
hf(config-y1731)#mep vlan 1 level 6 icc v1 umc fhn6
hf(config-mep-v1-fhn6)#quit
hf(config)#interface gigabitEthernet 1/0/5
hf(config-ge1/0/5)#y1731 mip vlan 1 level 1
hf(config-ge1/0/5)#quit
hf(config)#interface gigabitEthernet 1/0/6
hf(config-ge1/0/6)# y1731 mip vlan 1 level 6
hf(config-ge1/0/6)#y1731 mep vlan 1 level 1 mepid 1000 inward
hf(config-ge1/0/6)#y1731 mep vlan 1 level 1 mepid 1000 ccm enable
hf(config-ge1/0/6)#y1731 mep vlan 1 level 1 mepid 1000 ais enable
```

#### 5) 配置 zz

```
zz#configure
zz(config)#y1731
zz(config-y1731)#mep vlan 1 level 1 icc v1 umc fhn1
zz(config-mep-v1-fhn1)#quit
zz(config-y1731)#mep vlan 1 level 6 icc v1 umc fhn6
zz(config-mep-v1-fhn6)#quit
zz(config)#interface gigabitEthernet 1/0/3
zz(config-ge1/0/3)#y1731 mip vlan 1 level 1
```

```
zz(config-ge1/0/3)#quit
zz(config)#interface gigabitEthernet 1/0/4
zz(config-ge1/0/4)#y1731 mip vlan 1 level 6
zz(config-ge1/0/4)#y1731 mep vlan 1 level 1 mepid 7777 inward
zz(config-ge1/0/4)#y1731 mep vlan 1 level 1 mepid 7777 ccm enable
zz(config-ge1/0/4)#y1731 mep vlan 1 level 1 mepid 7777 ais enable
```

2、配置维护实体组合 icc v1 umc fhn6。

6) 配置 cd

```
cd#configure
cd(config)#y1731
cd(config-y1731)#mep vlan 1 level 6 icc v1 umc fhn6
cd(config-mep-v1-fhn6)#quit
cd(config)#interface fastEthernet 1/0/6
cd(config-fe1/0/6)#y1731 mep vlan 1 level 6 mepid 1
cd(config-fe1/0/6)#y1731 mep vlan 1 level 6 mepid 1 ccm enable
```

7) 配置 gz

```
gz#configure
gz(config)#y1731
gz(config-y1731)#mep vlan 1 level 6 icc v1 umc fhn6
gz(config-mep-v1-fhn6)#quit
gz(config)#interface fastEthernet 1/0/9
gz(config-fe1/0/9)# y1731 mep vlan 1 level 6 mepid 10
gz(config-fe1/0/9)#y1731 mep vlan 1 level 6 mepid 10 ccm enable
```

8) 配置 sh

```
sh#configure
sh(config)#y1731
sh(config-y1731)#mep vlan 1 level 6 icc v1 umc fhn6
sh(config-mep-v1-fhn6)#quit
sh(config)#interface fastEthernet 1/0/8
sh(config-fe1/0/8)#y1731 mep vlan 1 level 6 mepid 100
sh(config-fe1/0/8)#y1731 mep vlan 1 level 6 mepid 100 ccm enable
```

## 9) 配置 bj

```
bj#configure
```

```
bj(config)#y1731
```

```
bj(config-y1731)# meg vlan 1 level 6 icc v1 umc fhn6
```

```
bj(config-meg-v1-fhn6)#quit
```

```
bj(config)#interface fastethernet 1/0/7
```

```
bj(config-fe1/0/7)#y1731 mep vlan 1 level 6 mepid 1000
```

```
bj(config-fe1/0/7)#y1731 mep vlan 1 level 6 mepid 1000 ccm enable
```

## 第9章 设备管理配置

### 9.1 概述

本章介绍了 SC9600 系列高端交换机设备管理的基本内容、配置过程和配置举例。

本章包括如下主题：

内容	页码
9.1 概述	9-1
9.2 设备线卡及硬件配置	9-1
9.3 镜像配置	9-12
9.4 系统补丁配置	9-27
9.5 日志管理配置	9-31
9.6 DDM 配置	9-34
9.7 MMU 管理配置	9-38

### 9.2 设备线卡及硬件配置

#### 9.2.1 硬件配置概述

SC9600 系列高端交换机设备的硬件配置是指硬件安装完毕后，在设备运行过程中，用户可以通过命令来对硬件资源，包括：CPU、风扇、内存、温度以及接口板外扩 TCAM 线卡等硬件资源进行操作。

硬件配置便于硬件资源的利用以及提高硬件资源的可靠性。

#### 9.2.2 配置接口板外扩 TCAM 的资源模式

##### 背景信息

外扩 TCAM（Ternary Content Addressable Memory，三态内容可寻址寄存器）的工作模式，解释如下：

- 0——Close ALL: 关闭外扩 TCAM 的工作模式，即不使用外扩 TCAM
- 1——Big MAC: 仅配置 MAC 表项
- 2——Big IPV4: 仅配置 IPV4 的 IP 表项
- 3——MACACL: 配置 MAC 和 ACL 表项
- 4——IPV4ACL: 配置 IPV4 的 IP 表项和 ACL 表项
- 5——Big IPV6: 仅配置 IPV6 表项
- 6——IPV6ACL: 配置 IPV6 表项和 ACL 表项
- 7——IPV4NAC: 配置三层 ACL 表项
- 8——L2 ACL: 配置二层 ACL 表项
- 9——IPV4IPV6MAC: 配置 MAC 表项、配置 IPV4 的 IP 表项以及配置 IPV6 的表项

### 目的

当内置 TCAM 的 MAC、IP 或 ACL 表项不能满足业务需求时，可以通过本节操作配置外扩 TCAM 的工作模式以获得更大的配置表项。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
全局配置视图下设置接口板外扩 TCAM 的资源模式	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>assign resource-mode { tcam-mode   default } slot slot-number</b> 设置资源模式；</li> <li>3. 结束。</li> </ol>
槽位配置视图下设置接口板外扩 TCAM 的资源模式	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>slot slot-number</b> 进入槽位配置视图；</li> <li>3. 执行命令 <b>assign resource-mode { tcam-mode   default }</b> 设置资源模式；</li> <li>4. 结束。</li> </ol>
查看配置结果	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show resource-assign</b> 查看所有接口板资源分配情况；</li> <li>3. 执行命令 <b>show resource-assign slot slot-number</b> 查看指定槽位的接口板资源分配情况；</li> <li>4. 结束。</li> </ol>

以上两种不同配置视图下的执行的命令虽然不同，但是操作结果所做出的影响是一致的，用户可以自由选择使用。

附表：

参数	说明	取值
tcam-mode	指定 TCAM 表的资源模式	整数形式，取值范围是 0~9
default	指定为缺省值	取值为 0
slot-number	指定单板所在槽位号	SC9600 系列交换机支持以下 3 种型号的槽位配置范围： SC9603：取值范围是<1-3> SC9608：取值范围是<1-8> SC9612：取值范围是<1-12>

### 9.2.3 配置设备 CPU

#### 目的

用户可以通过本节操作了解 CPU 运行情况或控制 CPU 使用情况。包括：通过设置 CPU 监控及告警上报功能、通过设置 CPU 使用率的上下限阈值。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
设置 CPU 监控功能及 CPU 告警上报功能	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>cpu monitor { enable   disable }</b>使能或去使能 CPU 监控功能；</li> <li>3. 执行命令 <b>cpu trap { cpu-number   all } { enable   disable }</b>使能或去使能 CPU 上报告警功能；</li> <li>4. 结束。</li> </ol>
设置 CPU 使用率的上限阈值和下限阈值	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>cpu high-threshold { cpu-number   all } high-threshold</b> 设置 CPU 使用率的上限阈值；</li> <li>3. 执行命令 <b>cpu low-threshold { cpu-number   all } low-threshold</b> CPU 使用率的下限阈值；</li> <li>4. 结束。</li> </ol>
查看配置结果	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show cpu</b> 查看 CPU 使用情况和配置信息；</li> <li>3. 执行命令 <b>show cpu config</b> 查看设备 CPU 当前的配置文件信息；</li> <li>4. 执行命令 <b>show cpu statistic</b> 查看 CPU 占用率的统计信息；</li> </ol>

目的	步骤
	5. 结束。

附表：

参数	说明	取值
cpu-number	指定 CPU 号	整数形式，取值范围是 1~12
all	表示所有 CPU	-
high-threshold	指定 CPU 使用上限阈值	整数形式，取值范围是 1~100
low -threshold	指定 CPU 使用下限阈值	整数形式，取值范围是 1~100

## 9.2.4 配置设备风扇

### 目的

用户可以通过本节操作设置风扇转速阈值，并通过风扇监控及上报告警功能及时了解设备风扇当前的运转情况。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
设置风扇监控功能及风扇告警上报功能	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>fan monitor { enable   disable }</b>使能或去使能风扇监控功能；</li> <li>3. 执行命令 <b>fan trap { fan-number   all } { enable   disable }</b>使能或去使能风扇上报告警功能；</li> <li>4. 结束。</li> </ol>
设置风扇转速阈值	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>fan { fan-number   all } threshold low-threshold high-threshold</b>设置风扇转速阈值；</li> <li>3. 结束。</li> </ol>
查看配置结果	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show fan</b> 查看风扇状态；</li> <li>3. 结束。</li> </ol>

附表：

参数	说明	取值
fan-number	指定风扇号	整数形式，取值范围是 1~12
all	表示所有风扇	-
low -threshold	指定风扇转速下限阈值	整数形式，取值范围是 1~4800
high-threshold	指定风扇转速上限阈值	整数形式，取值范围是 1~4800



## 9.2.5 配置设备内存

### 目的

用户可以通过本节操作设置内存使用率的上下限阈值，并通过内存监控及上报告警功能及时了解设备内存当前的使用情况。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
设置内存监控功能及内存告警上报功能	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>memory monitor { enable   disable }</b>使能或去使能内存监控功能；</li> <li>3. 执行命令 <b>memory trap { memory-pool-number   all } { enable   disable }</b>使能或去使能内存上报告警功能；</li> <li>4. 结束。</li> </ol>
设置内存使用率的上限阈值和下限阈值	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>memory high-threshold { memory-pool-number   all } high-threshold</b> 设置内存上限阈值；</li> <li>3. 执行命令 <b>memory low-threshold { memory-pool-number   all } low-threshold</b> 设置内存下限阈值；</li> <li>4. 结束。</li> </ol>
查看配置结果	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show memory cli</b> 查看设备本卡上 CLI 模块内存使用情况；</li> <li>3. 执行命令 <b>show memory pool</b> 查看当前所有在位卡的内存使用情况；</li> <li>4. 执行命令 <b>show memory snmp</b> 查看本卡上 SNMP 模块的内存使用情况；</li> <li>5. 结束。</li> </ol>

附表：

参数	说明	取值
memory-pool-number	指定业务线卡槽位号	整数形式，取值范围是 1~10
all	表示所有内存池	-
high-threshold	指定内存使用上限阈值	整数形式，取值范围是 1~100
low -threshold	指定内存使用下限阈值	整数形式，取值范围是 0~100

## 9.2.6 配置设备温度

### 目的

用户可以通过本节操作控制设备温度变化时是否上报告警以及设备温度达到多少时才上报告警。

**过程**

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
设置温度监控功能及温度告警上报功能	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <code>temperature monitor { enable   disable }</code>使能或去使能温度监控功能；</li> <li>3. 执行命令 <code>temperature trap { temperature-number   all } { enable   disable }</code>使能或去使能温度上报告警功能；</li> <li>4. 结束。</li> </ol>
设置温度的高低阈值	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <code>temperature { temperature-number   all } threshold low-threshold high-threshold</code> 设置温度高低阈值；</li> <li>4. 结束。</li> </ol>
查看配置结果	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show temperature</b> 查看设备风扇所有单板的温度信息；</li> <li>3. 执行命令 <code>show temperature config</code> 查看设备温度的配置文件信息；</li> <li>4. 结束。</li> </ol>

附表：

参数	说明	取值
temperature-number	指定温度号	整数形式，取值范围是 1~5
all	表示所有温度	-
low -threshold	指定温度下限阈值	整数形式，取值范围是 1~65
high-threshold	指定温度上限阈值	整数形式，取值范围是 30~65

### 9.2.7 配置其他硬件参数

**目的**

用户可以通过本节操作对设备硬件的其他参数进行配置。

**过程**

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
重置驱动统计的 CPU 收发	<ol style="list-style-type: none"> <li>1. 保持在当前特权用户视图下；</li> <li>2. <code>reset driver statistic interface { fastethernet   gigasethernet   xgigasethernet }</code></li> </ol>

目的	步骤
包的相关信息	<i>interface-number</i> 重置驱动统计的 cpu 收发包的相关信息； 4. 结束。
重置内部控制协议的统计信息	1. 保持在当前特权用户视图下； 2. 执行命令 <b>reset control statistic</b> 重置内部控制协议的统计信息； 4. 结束。
查看配置结果	1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或不执行任何命令保持当前特权用户视图； 2. 执行命令 <b>show ha statistic</b> 查看 HA 相关统计信息； 3. 执行命令 <b>show driver statistic interface { fastethernet   gigasethernet   xgigasethernet } interface-number</b> 查看驱动统计的 CPU 收发包的相关信息； 4. 执行命令 <b>show dcp statistic</b> 查看 DCP 的收发包的统计信息； 5. 执行命令 <b>show control statistic</b> 或 <b>show control statistic slot-number</b> 查看内部控制协议的统计信息； 6. 结束。

附表：

参数	说明	取值
<i>interface-number</i>	以太网接口号	SC9600 系列交换机支持以下 3 种型号的接口配置范围： SC9603 : 取值范围是 <1-3>/<0-4>/<1-48> SC9608 : 取值范围是 <1-8>/<0-4>/<1-48> SC9612 : 取值范围是 <1-12>/<0-4>/<1-48>
<i>slot-number</i>	线卡取值范围，根据高端型号确定具体取值范围	SC9600 系列交换机支持以下 3 种型号的槽位配置范围： SC9603: 取值范围是<1-3> SC9608: 取值范围是<1-8> SC9612: 取值范围是<1-12>

## 9.2.8 配置线卡 MAC 地址学习的 Hash 算法

### 目的

用户可以通过本节操作配置产生二层表索引的 Hash 算法，达到产生 MAC 地址冲突的情况最少。

通常情况下，用户无需配置，主要用于调测设备时使用。

- 若线卡收到有序 MAC 地址的数据流，建议用户使用二层 MAC 地址学习的 Hash 算法为 lsb 模式
- 若线卡收到非有序 MAC 地址的数据流为例，建议用户使用二层 MAC 地址学习 Hash 算法的默认模式（即 crc32-upper 模式）

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
槽位配置视图下配置线卡二层 MAC 地址学习的 Hash 算法	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>slot slot-number</b> 进入槽位配置视图；</li> <li>3. 执行命令 <b>l2-hash mode { crc32-upper   crc32-low er   lsb   crc16-low er   crc16-upper   default }</b>配置线卡二层 MAC 地址学习的 Hash 算法；</li> <li>4. 结束。</li> </ol>
全局配置视图下配置指定线卡二层 MAC 地址学习的 Hash 算法	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>l2-hash slot linecard-number mode { crc32-upper   crc32-low er   lsb   crc16-low er   crc16-upper   default }</b>配置线卡二层 MAC 地址学习的 Hash 算法；</li> <li>3. 结束。</li> </ol>
查看配置结果	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show slot config</b> 查看系统当前槽位线卡配置信息或执行命令 <b>show hash mode</b> 查看线卡地址学习的 Hash 算法；</li> <li>3. 结束。</li> </ol>

附表：

参数	说明	取值
linecard-number	指定线卡所在槽位号	SC9600 系列交换机支持以下 3 种型号的槽位配置范围： SC9603: 取值范围是<1-3> SC9608: 取值范围是<1-8> SC9612 : 取值范围是<1-12>
crc32-upper	表示对 MAC+VLAN+PORT 进行 CRC32 计算，取高位作为 L2 表的索引	-
crc32-low er	表示对 MAC+VLAN+PORT 进行 CRC32 计算，取低位作为 L2 表的索引	-
lsb	表示取 MA C+VLAN+PORT 的低位，不进行 CRC 计算	-

参数	说明	取值
crc16-low er	表示对 MAC+VLAN+PORT 进行 CRC16 计算，取低位作为 L2 表的索引	-
crc16-upper	表示对 MAC+VLAN+PORT 进行 CRC16 计算，取高位作为 L2 表的索引	-

### 9.2.9 配置线卡 IP 地址学习的 Hash 算法

#### 目的

用户可以通过本节操作配置产生三层表索引的 Hash 算法，达到产生 IP 地址冲突的情况最少。

通常情况下，用户无需配置，主要用于调测设备时使用。

- 若线卡收到有序 IP 地址的数据流，建议用户使用三层 IP 地址学习的 Hash 算法为 lsb 模式
- 若线卡收到非有序 IP 地址的数据流为例，建议用户使用三层 IP 地址学习 Hash 算法的默认模式（即 crc32-upper 模式）

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
槽位配置视图下配置线卡三层 IP 地址学习的 Hash 算法	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>slot slot-number</b> 进入槽位配置视图；</li> <li>3. 执行命令 <b>l3-hash mode { crc32-upper   crc32-low er   lsb   crc16-low er   crc16-upper   default }</b>配置线卡三层 IP 地址学习的 Hash 算法；</li> <li>4. 结束。</li> </ol>
全局配置视图下配置指定线卡三层 IP 地址学习的 Hash 算法	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>l3-hash slot linecard-number mode { crc32-upper   crc32-low er   lsb   crc16-low er   crc16-upper   default }</b>配置线卡三层 IP 地址学习的 Hash 算法；</li> <li>3. 结束。</li> </ol>
查看配置结果	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show slot config</b> 查看系统当前槽位线卡配置信息或执行命令 <b>show hash mode</b> 查看线卡地址学习的 Hash 算法；</li> <li>3. 结束。</li> </ol>

附表：

参数	说明	取值
linecard-number	指定线卡所在槽位号	SC9600 系列交换机支持以下 3 种型号的槽位配置范围： SC9603: 取值范围是<1-3> SC9608: 取值范围是<1-8> SC9612 : 取值范围是<1-12>
crc32-upper	表示对 IP+VLAN+PORT 进行 CRC32 计算，取高位作为 L2 表的索引	-
crc32-low er	表示对 IP+VLAN+PORT 进行 CRC32 计算，取低位作为 L2 表的索引	-
lsb	表示取 IP+VLAN+PORT 的低位，不进行 CRC 计算	-
crc16-low er	表示对 IP+VLAN+PORT 进行 CRC16 计算，取低位作为 L2 表的索引	-
crc16-upper	表示对 IP+VLAN+PORT 进行 CRC16 计算，取高位作为 L2 表的索引	-

### 9.2.10 配置线卡复位

#### 目的

当线卡工作不正常或需要升级版本时，用户可以进行本节操作进行线卡复位。



注意：

在业务线卡工作不正常时，应尽量排除故障，不要轻易复位业务线卡，以免对业务造成影响。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
复位线卡	<ol style="list-style-type: none"> <li>1. 不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>reboot slot linecard-number</b> 重启并复位线卡；</li> <li>3. 结束。</li> </ol>
查看设备部件类型及系统	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或不执行任何命令保持当前特权用户视图；</li> </ol>

目的	步骤
状态信息	2. 执行命令 <b>show device</b> 查看设备部件类型及系统状态信息； 3. 结束。

附表：

参数	说明	取值
linecard-number	指定线卡所在槽位号	SC9600 系列交换机支持以下 3 种型号的槽位配置范围： SC9603: 取值范围是<1-3> SC9608: 取值范围是<1-8> SC9612: 取值范围是<1-12>

### 9.2.11 配置主备倒换

#### 目的

在双主控环境下，用户可以进行本节操作强制进行主备倒换。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
强制进行主备板倒换	1. 不执行任何命令保持当前特权用户视图； 2. 执行命令 <b>rsp switch</b> 强制进行主备板倒换； 3. 结束。
查看设备部件类型及系统状态信息	1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或不执行任何命令保持当前特权用户视图； 2. 执行命令 <b>show device</b> 查看设备部件类型及系统状态信息； 3. 结束。

附表：

参数	说明	取值
linecard-number	指定线卡所在槽位号	整数形式，取值范围为 1~10

### 9.2.12 维护及调试

#### 目的

用户可以通过本节操作对设备硬件参数进行调试，用于定位问题。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
打开 DCP 协议的调试开关	<ol style="list-style-type: none"> <li>1. 保持在当前特权用户视图下；</li> <li>2. 执行命令 <b>debug dcp all</b> 打开 DCP 协议的调试开关；</li> <li>3. 结束。</li> </ol>
关闭 DCP 协议的调试开关	<ol style="list-style-type: none"> <li>1. 保持在当前特权用户视图下；</li> <li>2. 执行命令 <b>no debug dcp all</b> 关闭 DCP 协议的调试开关；</li> <li>3. 结束。</li> </ol>
打开 HA 协议的调试开关	<ol style="list-style-type: none"> <li>1. 保持在当前特权用户视图下；</li> <li>2. 执行命令 <b>debug ha all</b> 打开 HA 协议的调试开关；</li> <li>3. 结束。</li> </ol>
关闭 HA 协议的调试开关	<ol style="list-style-type: none"> <li>1. 保持在当前特权用户视图下；</li> <li>2. 执行命令 <b>no debug ha all</b> 关闭 HA 协议的调试开关；</li> <li>3. 结束。</li> </ol>
查看版本信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show version</b> 或 <b>show version slot-number</b> 查看版本信息；</li> <li>3. 结束。</li> </ol>

## 9.3 镜像配置

### 9.3.1 镜像概述

镜像是指将数据流复制到镜像目的端口。镜像技术主要用来实现数据流的监控功能，以便排除网络故障。

SC9600 支持卡间的镜像、支持 Trunk 的镜像、支持镜像到 Trunk、可以支持单板 Trunk，也可以支持跨卡的 Trunk。

SC9600 的观察端口最多可以设置为 8 个，但是每单板上端口只能镜像到至多两个观察端口。

SC9600 支持跨板镜像，观察端口和镜像端口可以配置在同一台设备的不同接口板上。

SC9600 支持将多个端口的报文镜像到一个观察端口。

SC9600 每块单板最多可以同时运用 3 个观察端口，若同一端口即用于镜像上行流量又用于镜像下行流量则视为使用了 2 个观察端口。

SC9600 支持同一端口入方向和不同方向的流镜像到 2 个不同的观察端口，不支持对镜像报文进行再次镜像。



### 9.3.2 镜像分类

SC9600 系列高端交换机支持端口镜像和流镜像。

其中，端口镜像又分为本地镜像和远程镜像：

- 本地端口镜像：又叫 Local Switched Port Analyzer (SPAN)，指镜像源和目的端口在同一台交换机上。
- 远程端口镜像：又叫 Remote SPAN (RSPAN)，指镜像源和目的端口在不同的交换机上。



说明

- 源交换机：被监控端口所在的交换机，将流量镜像到 REMOTE-VLAN 中，然后二层转发给中间交换机。
- 中间交换机：网络中处于源交换机和目的交换机之间的交换机，通过 REMOTE-VLAN 把流量传输给下一个中间交换机和目的交换机。如果源交换机与目的交换机直接相连，则不存在中间交换机。
- 目的交换机：远程镜像目的端口所在的交换机，将从 REMOTE-VLAN 接收到的镜像流量通过镜像目的端口转发给监控设备。

流镜像也分为两种，分别是流镜像到 CPU 和流镜像到端口：

- 流镜像到 CPU：是指把通过配置了流镜像接口上的符合匹配要求的报文复制一份发送到 CPU，以供分析诊断。
- 流镜像到端口：是指把通过配置了流镜像接口上的符合匹配要求的报文复制一份发送到目的端口，以供分析诊断。



说明：

同端口镜像一样，流镜像也分为本地流镜像和远程流镜像。

---

### 9.3.3 配置本地端口镜像

#### 目的

当用户需要监控或分析流经设备上某端口的报文，且镜像源端口与镜像目的端口在同一台设备上时，可以配置本地端口镜像功能。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置本地端口镜像	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>mirror group groupnum { fastethernet   gigaehternet   gigaehternet   xgigaehternet } interface-number/</b> 或执行命令 <b>mirror group groupnum eth-trunk trunk-number</b> 创建本地镜像组及其观察端口；</li> <li>3. 执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b> 或 <b>interface trunk trunk-number</b> 进入接口配置视图；</li> <li>4. 执行命令 <b>mirror { ingress   egress   both } group group-list</b> 在镜像源端口设置该接口的镜像功能；</li> <li>5. 结束。</li> </ol>
取消端口本地镜像功能并删除本地镜像组及其观察端口	<ol style="list-style-type: none"> <li>1. 执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b> 或 <b>interface trunk trunk-number</b> 进入接口配置视图；</li> <li>2. 执行命令 <b>no mirror { ingress   egress   both } group-list</b> 取消端口本地镜像功能；</li> <li>3. 执行命令 <b>quit</b> 或 <b>exit</b> 退出到全局配置视图；</li> <li>4. 执行命令 <b>no mirror group [ groupnum ]</b> 删除本地镜像组及其观察端口的配置；</li> <li>5. 结束。</li> </ol>
查看配置结果	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或不执行任何命令保持当前特权用户视图，或执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b> 或 <b>interface trunk trunk-number</b> 进入接口配置视图；</li> <li>2. 执行命令 <b>show mirror config</b> 查看镜像功能的配置文件信息。</li> <li>3. 执行命令 <b>show mirror group</b> 查看镜像组信息。</li> <li>4. 执行命令 <b>show mirror interface</b> 查看镜像端口信息。</li> <li>5. 结束。</li> </ol>

附表：

参数	说明	取值
groupnum	指定镜像组 ID	整数形式，取值范围是 1~8
interface-number	指定作为观察端口以太网接口号	SC9600 系列交换机支持以下 3 种型号的接口配置范围： SC9603：取值范围是 <1-3>/<0-4>/<1-48> SC9608：取值范围是 <1-8>/<0-4>/<1-48> SC9612：取值范围是 <1-12>/<0-4>/<1-48>

参数	说明	取值
trunk-number	指定作为观察端口的聚合端口号	整数形式,取值范围是 1~128
ingress	对接口入方向的报文进行镜像	-
egress	对接口出方向的报文进行镜像	-
both	对接口出/入两个方向的报文进行镜像	-
group-list	镜像组列表序号	整数形式,取值范围是 1~8,形如: 1,3-5

### 9.3.4 配置远程端口镜像

#### 背景信息

SC9600 系列高端交换机支持的远程端口镜像分为基于 VLAN 方式和基于 IP 方式两种。

#### 目的

当用户需要监控或分析流经设备上某端口的报文,且镜像源端口与镜像目的端口在不同设备上时,可以配置远程端口镜像功能。



说明:

配置远程端口镜像之前,需保证设备之间二层网络连通或三层网络可达。

#### 过程

根据不同目的,执行相应步骤,具体参见下表。

目的	步骤
配置二层端口 远程镜像	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>mirror group groupnum { fastethernet   gigasethernet   gigasethernet   xgigasethernet } interface-number rspan vlan-id</b> 或执行命令 <b>mirror group groupnum { fastethernet   gigasethernet   gigasethernet   xgigasethernet } interface-number rspan vlan-id tpid { standard   protocol-id }</b> 或执行命令 <b>mirror group groupnum eth-trunk trunk-number rspan vlan-id</b> 或执行命令 <b>mirror group groupnum eth-trunk trunk-number rspan vlan-id tpid { standard   protocol-id }</b>创建远程镜像组及其观察端口;</li> <li>3. 执行命令 <b>interface { fastethernet   gigasethernet   xgigasethernet } interface-number</b> 或 <b>interface trunk trunk-number</b> 进入接口配置视图;</li> <li>4. 执行命令 <b>mirror { ingress   egress   both } group group-list</b> 在镜像源端口设置该接口的镜像功能;</li> </ol>

目的	步骤
	5. 结束。
配置三层端口 远程镜像	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>mirror group groupnum { fastethernet   gigaethernet   xgigaethernet } interface-number dest-ip dest-ipaddress src-ip src-ipaddress</b> 或执行命令 <b>mirror group groupnum { fastethernet   gigaethernet   xgigaethernet } interface-number dest-ip dest-ipaddress src-ip src-ipaddress dscp dscp</b> 或执行命令 <b>mirror group groupnum { fastethernet   gigaethernet   xgigaethernet } interface-number dest-ip dest-ipaddress src-ip src-ipaddress dscp dscp vlan vlan-id</b> 或执行命令 <b>mirror group groupnum { fastethernet   gigaethernet   xgigaethernet } interface-number dest-ip dest-ipaddress src-ip src-ipaddress vlan vlan-id</b> 或执行命令 <b>mirror group groupnum eth-trunk trunk-number dest-ip dest-ipaddress src-ip src-ipaddress</b> 或执行命令 <b>mirror group groupnum eth-trunk trunk-number dest-ip dest-ipaddress src-ip src-ipaddress dscp dscp</b> 或执行命令 <b>mirror group groupnum eth-trunk trunk-number dest-ip dest-ipaddress src-ip src-ipaddress dscp dscp vlan vlan-id</b> 或执行命令 <b>mirror group groupnum eth-trunk trunk-number dest-ip dest-ipaddress src-ip src-ipaddress vlan vlan-id</b></li> <li>3. 执行命令 <b>interface { fastethernet   gigaethernet   xgigaethernet } interface-number</b> 或 <b>interface trunk trunk-number</b> 进入接口配置视图；</li> <li>4. 执行命令 <b>mirror { ingress   egress   both } group group-list</b> 在镜像源端口设置该接口的镜像功能；</li> <li>5. 结束。</li> </ol>
取消端口远程 镜像功能并删除 本地镜像组及其 观察端口	<ol style="list-style-type: none"> <li>1. 执行命令 <b>interface { fastethernet   gigaethernet   xgigaethernet } interface-number</b> 或 <b>interface trunk trunk-number</b> 进入接口配置视图；</li> <li>2. 执行命令 <b>no mirror { ingress   egress   both } group-list</b> 取消端口本地镜像功能；</li> <li>3. 执行命令 <b>quit</b> 或 <b>exit</b> 退出到全局配置视图；</li> <li>4. 执行命令 <b>no mirror group [ groupnum ]</b> 删除本地镜像组及其观察端口的配置；</li> <li>5. 结束。</li> </ol>
查看配置结果	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或不执行任何命令保持当前特权用户视图，或执行命令 <b>interface { fastethernet   gigaethernet   xgigaethernet } interface-number</b> 或 <b>interface trunk trunk-number</b> 进入接口配置视图；</li> <li>2. 执行命令 <b>show mirror config</b> 查看镜像功能的配置文件信息。</li> </ol>

目的	步骤
	3. 执行命令 <code>show mirror group</code> 查看镜像组信息。 4. 执行命令 <code>show mirror interface</code> 查看镜像端口信息。 5. 结束。

附表：

参数	说明	取值
groupnum	指定镜像组 ID	整数形式，取值范围是 1~8
interface-number	指定远程观察端口	SC9600 系列交换机支持以下 3 种型号的接口配置范围： SC9603：取值范围是 <1-3>/<0-4>/<1-48> SC9608：取值范围是 <1-8>/<0-4>/<1-48> SC9612：取值范围是 <1-12>/<0-4>/<1-48>
trunk-number	指定作为远程观察端口的聚合端口号	整数形式，取值范围是 1~128
dest-ipaddress	指定目的 IP 地址，即远端观察设备接口的 IP 地址	点分十进制
src-ipaddress	指定源 IP 地址，即被观察设备的接口 IP 地址	点分十进制
dscp	指定报文的 DSCP 值	整数形式，取值范围是 0~63
vlan-id	指定 VLAN ID	整数形式，取值范围是 1~4094
protocol-id	当前接口的外层 Tag 的标签协议标识	十六进制数形式，取值范围是 <0x1-0xffff>
standard	标准值	0x8100
group-list	镜像组列表序号	整数形式，取值范围是 1~8，形如：1,3-5

### 9.3.5 配置流镜像

#### 目的

当用户需要监控或分析流经设备的且具有某些特性的报文，可以配置流镜像功能。



#### 说明：

配置远程流镜像之前，需保证设备之间二层网络连通或三层网络可达。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置本地流镜像	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>mirror group groupnum { fastethernet   gigaethernet   gigaethernet   xgigaethernet } interface-number/</b> 或执行命令 <b>mirror group groupnum eth-trunk trunk-number</b> 创建本地镜像组及其观察端口；</li> <li>3. 执行命令 <b>filter-list acl-number</b> 创建一条 ACL（访问控制列表），并进入 ACL 视图；</li> <li>4. 请根据实际应用情形，参考第 9 章 ACL 配置，选择合适的流分类规则；</li> <li>5. 执行命令 <b>filter rule-number action mirror cpu</b> 或执行命令 <b>filter rule-number action mirror group group-number</b> 配置流镜像处理动作；</li> <li>6. 执行命令 <b>quit</b> 或 <b>exit</b> 退出 ACL 视图到全局配置视图；</li> <li>7. 执行命令 <b>interface { fastethernet   gigaethernet   xgigaethernet } interface-number</b> 或 <b>interface trunk trunk-number</b> 进入接口配置视图；</li> <li>8. 执行命令 <b>filter-list in acl-number</b> 将 ACL 应用到该物理端口或 trunk 接口；</li> <li>9. 执行命令 <b>mirror { ingress   egress   both } group group-list</b> 在镜像源端口设置该接口的镜像功能；</li> <li>10. 结束。</li> </ol>
配置基于 VLAN 的远程流镜像	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>mirror group groupnum { fastethernet   gigaethernet   gigaethernet   xgigaethernet } interface-number rspan vlan-id</b> 或执行命令 <b>mirror group groupnum { fastethernet   gigaethernet   gigaethernet   xgigaethernet } interface-number rspan vlan-id tpid { standard   protocol-id }</b> 或执行命令 <b>mirror group groupnum eth-trunk trunk-number rspan vlan-id</b> 或执行命令 <b>mirror group groupnum eth-trunk trunk-number rspan vlan-id tpid { standard   protocol-id }</b> 创建远程镜像组及其观察端口；</li> <li>3. 执行命令 <b>filter-list acl-number</b> 创建一条 ACL（访问控制列表），并进入 ACL 视图；</li> <li>4. 请根据实际应用情形，参考第 9 章 ACL 配置，选择合适的流分类规则；</li> <li>5. 执行命令 <b>filter rule-number action mirror cpu</b> 或执行命令 <b>filter rule-number action mirror group group-number</b> 配置流镜像处理动作；</li> <li>6. 执行命令 <b>quit</b> 或 <b>exit</b> 退出 ACL 视图到全局配置视图；</li> <li>7. 执行命令 <b>interface { fastethernet   gigaethernet   xgigaethernet } interface-number</b> 或 <b>interface trunk trunk-number</b> 进入接口配置视图；</li> <li>8. 执行命令 <b>filter-list in acl-number</b> 将 ACL 应用到该物理端口或 trunk 接口；</li> <li>9. 执行命令 <b>mirror { ingress   egress   both } group group-list</b> 在镜像源端口设置该接口的镜像功能；</li> </ol>

目的	步骤
	10. 结束。
配置基于 IP 地址的远程流镜像	<p>1. 执行命令 <b>configure</b> 进入全局配置视图；</p> <p>2. 执行命令 <b>mirror group groupnum { fastethernet   gigaehternet   xgigaehternet } interface-number dest-ip dest-ipaddress src-ip src-ipaddress</b> 或执行命令 <b>mirror group groupnum { fastethernet   gigaehternet   xgigaehternet } interface-number dest-ip dest-ipaddress src-ip src-ipaddress dscp dscp</b> 或执行命令 <b>mirror group groupnum { fastethernet   gigaehternet   xgigaehternet } interface-number dest-ip dest-ipaddress src-ip src-ipaddress dscp dscp vlan vlan-id</b> 或执行命令 <b>mirror group groupnum { fastethernet   gigaehternet   xgigaehternet } interface-number dest-ip dest-ipaddress src-ip src-ipaddress vlan vlan-id</b> 或执行命令 <b>mirror group groupnum eth-trunk trunk-number dest-ip dest-ipaddress src-ip src-ipaddress</b> 或执行命令 <b>mirror group groupnum eth-trunk trunk-number dest-ip dest-ipaddress src-ip src-ipaddress dscp dscp</b> 或执行命令 <b>mirror group groupnum eth-trunk trunk-number dest-ip dest-ipaddress src-ip src-ipaddress dscp dscp vlan vlan-id</b> 或执行命令 <b>mirror group groupnum eth-trunk trunk-number dest-ip dest-ipaddress src-ip src-ipaddress vlan vlan-id</b> 创建远程镜像组及其观察端口；</p> <p>3. 执行命令 <b>filter-list acl-number</b> 创建一条 ACL（访问控制列表），并进入 ACL 视图；</p> <p>4. 请根据实际应用情形，参考第 9 章 ACL 配置，选择合适的流分类规则；</p> <p>5. 执行命令 <b>filter rule-number action mirror cpu</b> 或执行命令 <b>filter rule-number action mirror group group-number</b> 配置流镜像处理动作；</p> <p>6. 执行命令 <b>quit</b> 或 <b>exit</b> 退出 ACL 视图到全局配置视图；</p> <p>7. 执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b> 或 <b>interface trunk trunk-number</b> 进入接口配置视图；</p> <p>8. 执行命令 <b>filter-list in acl-number</b> 将 ACL 应用到该物理端口或 trunk 接口；</p> <p>9. 执行命令 <b>mirror { ingress   egress   both } group group-list</b> 在镜像源端口设置该接口的镜像功能；</p> <p>10. 结束。</p>
取消端口远程镜像功能并删除本地镜像组及其观察端口	<p>1. 执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b> 或 <b>interface trunk trunk-number</b> 进入接口配置视图；</p> <p>2. 执行命令 <b>no mirror { ingress   egress   both } group-list</b> 取消端口本地镜像功能；</p> <p>3. 执行命令 <b>quit</b> 或 <b>exit</b> 退出到全局配置视图；</p> <p>4. 执行命令 <b>no mirror group [ groupnum ]</b> 删除本地镜像组及其观察端口的配</p>

目的	步骤
	置： 5. 结束。
查看配置结果	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或不执行任何命令保持当前特权用户视图，或执行命令 <b>interface { fastethernet   gigaethernet   xgigaethernet } interface-number</b> 或 <b>interface trunk trunk-number</b> 进入接口配置视图；</li> <li>2. 执行命令 <b>show mirror config</b> 查看镜像功能的配置文件信息。</li> <li>3. 执行命令 <b>show mirror group</b> 查看镜像组信息。</li> <li>4. 执行命令 <b>show mirror interface</b> 查看镜像端口信息</li> <li>5. 结束。</li> </ol>

附表：

参数	说明	取值
groupnum	指定镜像组 ID	整数形式，取值范围是 1~8
interface-number	指定本地或远程观察端口	SC9600 系列交换机支持以下 3 种型号的接口配置范围： SC9603：取值范围是 <1-3>/<0-4>/<1-48> SC9608：取值范围是 <1-8>/<0-4>/<1-48> SC9612：取值范围是 <1-12>/<0-4>/<1-48>
trunk-number	指定作为本地或远程观察端口的聚合端口号	整数形式，取值范围是 1~128
dest-ipaddress	指定目的 IP 地址，即远端观察设备接口的 IP 地址	点分十进制
src-ipaddress	指定源 IP 地址，即被观察设备的接口 IP 地址	点分十进制
dscp	指定报文的 DSCP 值	整数形式，取值范围是 0~63
vlan-id	指定 VLAN ID	整数形式，取值范围是 1~4094
protocol-id	当前接口的外层 Tag 的标签协议标识	十六进制数形式，取值范围是 <0x1-0xffff>
standard	标准值	0x8100
group-list	镜像组列表序号	整数形式，取值范围是 1~8，形如：1,3-5

### 9.3.6 维护及调试

目的



当镜像功能不正常，需要进行调试或定位问题是，可以使用本小节操作。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
打开镜像调试功能	1. 不执行任何命令保持当前特权用户视图； 2. 执行命令 <b>debug mirror</b> 打开镜像调试功能； 3. 结束。
关闭镜像调试功能	1. 不执行任何命令保持当前特权用户视图； 2. 执行命令 <b>no debug mirror</b> 打开镜像调试功能； 3. 结束。

## 9.3.7 配置举例

### 9.3.7.1 配置本地端口镜像举例

#### 组网要求

某集团公司部门 A 和部门 B 分别通过接口 1/0/1、1/0/2 连接到交换机 SC9600A。数据监控设备通过接口 1/0/3 连接到交换机 SC9600A。要求使用本地端口镜像功能来实现数据监控设备对部门 A 和部门 B 发送到交换机 SC9600A 上的报文的监控。

#### 组网图

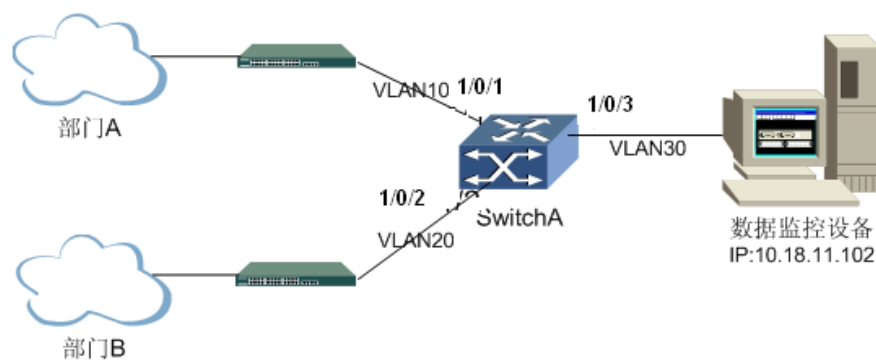


图 9-1 本地端口镜像配置组网图

#### 配置步骤

- 1、配置各接口，使两个部门都能与数据监控设备互通。

#创建 VLAN10、VLAN20、VLAN30，并将端口 1/0/1、1/0/2、1/0/3 分别加入 VLAN10、VLAN20、VLAN30。

```
SC9600A#configure
SC9600A (config)#Vlan 10
SC9600A (config-vlan-10)#quit
SC9600A (config)#Vlan 20
SC9600A (config-vlan-20)#quit
SC9600A (config)#Vlan 30
SC9600A (config-vlan-30)#quit
SC9600A (config)#interface gigabitEthernet 1/0/1
SC9600A (config-ge1/0/1)#port link-type trunk
SC9600A (config-ge1/0/1)#port trunk pvid 10
SC9600A (config-ge1/0/1)#port trunk allow-pass vlan 10
SC9600A (config-ge1/0/1)#quit
SC9600A (config)#interface gigabitEthernet 1/0/2
SC9600A (config-ge1/0/2)# port link-type trunk
SC9600A (config-ge1/0/2)#port trunk pvid 20
SC9600A (config-ge1/0/2)#port trunk allow-pass vlan 20
SC9600A (config-ge1/0/2)#quit
SC9600A (config)#interface gigabitEthernet 1/0/3
SC9600A (config-ge1/0/3)# port link-type trunk
SC9600A (config-ge1/0/3)#port trunk allow-pass vlan 10,20,30
SC9600A (config-ge1/0/3)#quit
SC9600A (config)#interface vlan 30
SC9600A (config-vlan-3)#ip address 10.18.11.1/24
SC9600A (config-vlan-3)#quit
SC9600A (config)#
```

2、创建本地镜像组及其观察端口。

#在 SC9600A 上创建本地镜像组 1 及配置其观察端口为 1/0/3。

```
SC9600A (config)#mirror group 1 gigabitEthernet 1/0/3
```

3、在镜像源端口设置该端口的镜像功能。

#在 SC9600A 上配置端口 1/0/1 和 1/0/2 为镜像源端口，以监控部门 A 和部门 B 发送的数据报文。

```

SC9600A (config)#interface gigabitEthernet 1/0/1
SC9600A (config-ge1/0/1)#mirror ingress group 1
SC9600A (config-ge1/0/1)#quit
SC9600A (config)#interface gigabitEthernet 1/0/2
SC9600A (config-ge1/0/2)#mirror ingress group 1
SC9600A (config-ge1/0/2)#quit
SC9600A (config)#
    
```

4、配置结束。

### 9.3.7.2 配置远程端口镜像举例

#### 组网要求

部门 A 通过 SC9600A 的端口 1/0/2 接入 Internet。数据监控设备通过端口 1/0/2 连接到 SC9600B 上。SC9600A 和 SC9600B 通过 Trunk 端口相连。要求使用远程端口镜像功能来实现数据监控设备对部门 A 发送到 SC9600A 上的报文的监控。（监控设备与部门 A 二层互通）

#### 组网图

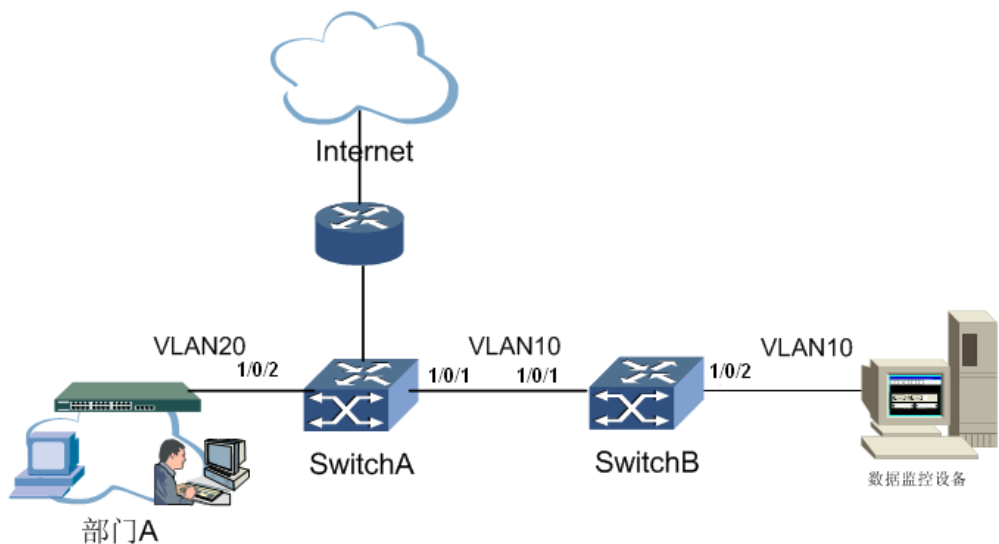


图 9-2 远程端口镜像配置组网图

#### 配置步骤

1、配置交换机各接口，使各交换机间二层可达。

#配置 SC9600A，创建 VLAN10、VLAN20，并将端口 1/0/1、1/0/2 加入 VLAN10、VLAN20。

```
SC9600A#configure
SC9600A (config)#Vlan 10
SC9600A (config-vlan-10)#quit
SC9600A (config)#Vlan 20
SC9600A (config-vlan-20)#quit
SC9600A (config)#interface gigabitEthernet 1/0/1
SC9600A (config-ge1/0/1)#port link-type trunk
SC9600A (config-ge1/0/1)#port trunk pvid 10
SC9600A (config-ge1/0/1)#port trunk allow-pass vlan 10
SC9600A (config-ge1/0/1)#quit
SC9600A (config)#interface gigabitEthernet 1/0/2
SC9600A (config-ge1/0/2)# port link-type trunk
SC9600A (config-ge1/0/2)#port trunk pvid 20
SC9600A (config-ge1/0/2)#port trunk allow-pass vlan 20
SC9600A (config-ge1/0/2)#quit
SC9600A (config)#
```

#配置 SC9600B，创建 VLAN10，并将端口 1/0/1、1/0/2 加入 VLAN10。

```
SC9600B (config)#Vlan 10
SC9600B (config-vlan-10)#quit
SC9600B (config)#interface gigabitEthernet 1/0/1
SC9600B (config-ge1/0/1)#port link-type trunk
SC9600B (config-ge1/0/1)#port trunk pvid 10
SC9600B (config-ge1/0/1)#port trunk allow-pass vlan 10
SC9600B (config-ge1/0/1)#quit
SC9600B (config)#interface gigabitEthernet 1/0/2
SC9600B (config-ge1/0/2)#port link-type trunk
SC9600B (config-ge1/0/2)#port trunk pvid 10
SC9600B (config-ge1/0/2)#port trunk allow-pass vlan 10
SC9600B (config-ge1/0/2)#quit
SC9600B (config)#
```

2、创建远程镜像组及其观察端口。

#在 SC9600A 上创建远程镜像组 1 及配置其观察端口为 1/0/1。

```
SC9600A (config)#mirror group 1 gigabernet 1/0/1 rspan 10
```

3、在镜像源端口设置该端口的镜像功能。

#在 SC9600A 上配置端口 1/0/2 为镜像源端口，以监控部门 A 发送的数据报文。

```
SC9600A (config)#interface gigabernet 1/0/2
```

```
SC9600A (config-ge1/0/2)#mirror ingress group 1
```

```
SC9600A (config-ge1/0/2)#quit
```

```
SC9600A (config)#
```

4、配置结束。

### 9.3.7.3 配置本地流镜像举例

#### 组网要求

某集团公司部门 A 和部门 B 分别通过接口 1/0/1、1/0/2 连接到交换机 SC9600A。数据监控设备通过接口 1/0/3 连接到交换机 SC9600A。要求使用本地流镜像功能来实现数据监控设备对部门 A 和部门 B 发送到交换机 SC9600A 上的源 MAC 地址为任意，目的 MAC 地址为 00:00:00:01:02:03 报文的监控。

#### 组网图

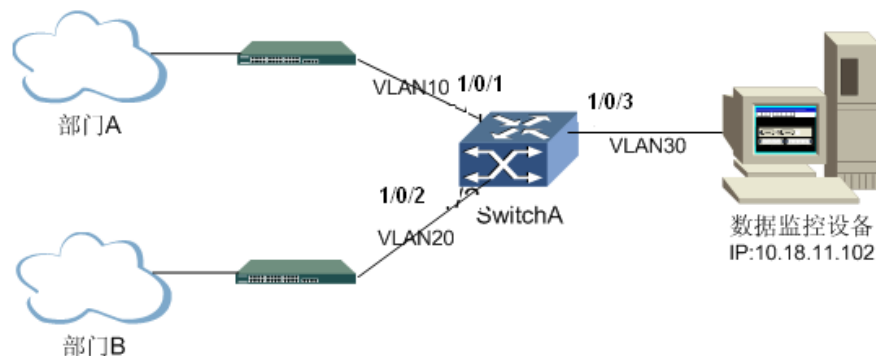


图 9-3 本地流镜像配置组网图

#### 配置步骤

1、配置各接口，使各两个部门都能与数据监控设备互通。

#创建 VLAN10、VLAN20、VLAN30，并将端口 1/0/1、1/0/2、1/0/3 分别加入 VLAN10、VLAN20、VLAN30。

```
SC9600A#configure
```

```
SC9600A (config)#Vlan 10
SC9600A (config-vlan-10)#quit
SC9600A (config)#Vlan 20
SC9600A (config-vlan-20)#quit
SC9600A (config)#Vlan 30
SC9600A (config-vlan-30)#quit
SC9600A (config)#interface gigabitEthernet 1/0/1
SC9600A (config-ge1/0/1)#port link-type trunk
SC9600A (config-ge1/0/1)#port trunk pvid 10
SC9600A8(config-ge1/0/1)#port trunk allow-pass vlan 10
SC9600A (config-ge1/0/1)#quit
SC9600A (config)#interface gigabitEthernet 1/0/2
SC9600A (config-ge1/0/2)# port link-type trunk
SC9600A (config-ge1/0/2)#port trunk pvid 20
SC9600A (config-ge1/0/2)#port trunk allow-pass vlan 20
SC9600A (config-ge1/0/2)#quit
SC9600A (config)#interface gigabitEthernet 1/0/3
SC9600A (config-ge1/0/3)# port link-type trunk
SC9600A (config-ge1/0/3)#port trunk allow-pass vlan 10,20,30
SC9600A (config-ge1/0/3)#quit
SC9600A (config)#interface vlan 30
SC9600A (config-vlan-30)#ip address 10.18.11.1/24
SC9600A8(config-vlan-30)#quit
SC9600A (config)#
```

2、创建本地镜像组及其观察端口。

#在 SC9600A 上创建本地镜像组 1 及配置其观察端口为 1/0/3。

```
SC9600A (config)#mirror group 1 gigabitEthernet 1/0/3
```

3、配置流分类规则及流镜像处理动作，并将策略应用到镜像源端口。

#在 SC9600A 上创建 ACL100，配置其匹配规则及处理动作，并应用到镜像源端口。

```
SC9600A (config)#filter-list 100
SC9600A (configure-filter-l2-100)#filter 1 mac any 00:00:00:01:02:03
SC9600A (configure-filter-l2-100)#filter action mirror group 1
SC9600A (configure-filter-l2-100)#quit
SC9600A (config)#interface gigabitEthernet 1/0/1
```

```
SC9600A (config-ge1/0/1)#filter-list in 100
SC9600A (config-ge1/0/1)#quit
SC9600A (config)#interface gigabitEthernet 1/0/2
SC9600A (config-ge1/0/2)# filter-list in 100
SC9600A (config-ge1/0/2)#quit
SC9600A (config)#
```

4、在镜像源端口设置该端口的镜像功能。

#在 SC9600A 上配置端口 1/0/1 和 1/0/2 为镜像源端口，以实现部门 A 和部门 B 发送到交换机 SC9600A 上的源 MAC 地址为任意，目的 MAC 地址为 00:00:00:01:02:03 报文的监控。

```
SC9600A (config)#interface gigabitEthernet 1/0/1
SC9600A (config-ge1/0/1)#mirror ingress group 1
SC9600A (config-ge1/0/1)#quit
SC9600A (config)#interface gigabitEthernet 1/0/2
SC9600A (config-ge1/0/2)#mirror ingress group 1
SC9600A8(config-ge1/0/2)#quit
SC9600A (config)#
```

5、配置结束。

## 9.4 系统补丁配置

### 9.4.1 系统补丁概述

补丁是一种与系统软件兼容的软件，用于解决系统软件的 Bug。设备支持 Deactive、Active 和 Running 这 3 种补丁状态。

### 9.4.2 加载单板补丁

#### 背景信息

在加载补丁之前系统要对补丁包进行解析，检查补丁包中补丁文件的合法性，并获取补丁文件的属性（包括补丁类型、单板类型、版本信息）。

为单板加载补丁时，系统会根据补丁文件的属性在补丁包中查找匹配的补丁文件，查找成功，则进行加载操作。如果补丁包中没有适合某类型单板的补丁，则不加载。

补丁文件必须在主控板根目录下。

当备用主控板正在注册中且尚未注册成功时，如果进行补丁加载操作，则系统会提示：是否确认继续执行补丁操作。

### 目的

用户可以通过本节操作进行补丁加载配置。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
在单板上加载补丁包中与单板匹配的补丁	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>patch patch-number load file file-name funcname func-name</b> 在单板上加载补丁包中与单板匹配的补丁；</li> <li>3. 结束。</li> </ol>
查看配置结果	<ol style="list-style-type: none"> <li>1. 不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show patch information</b> 查看系统当前所有补丁信息；</li> <li>3. 结束。</li> </ol>

附表：

参数	说明	取值
patch-number	指定补丁号	整数形式，取值范围是 1~100
file-name	指定补丁文件路径及名称	字符串形式
func-name	指定补丁函数名称，有问题的函数和补丁函数的名称必须相同	字符串形式

## 9.4.3 配置是否激活补丁

### 准备

激活补丁之前，必须先进行加载单板补丁操作，参见9.4.2小节。

### 背景信息

目前的补丁功能只针对对主控上软件打补丁，只要主控软件系统起来后就可以加载或激活补丁，与线卡无关。

去激活补丁时，补丁必须存在且已被激活后，去激活补丁才有效。

### 目的

用户可以通过本节操作进行补丁激活或去激活配置。

### 过程



根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
激活补丁	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>patch patch-number active</b> 激活在位单板上指定的已加载的补丁；</li> <li>3. 结束。</li> </ol>
去激活补丁	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>patch patch-number deactivate</b> 去激活补丁；</li> <li>3. 结束。</li> </ol>
查看配置结果	<ol style="list-style-type: none"> <li>1. 不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show patch information</b> 查看系统当前所有补丁信息；</li> <li>3. 结束。</li> </ol>

附表：

参数	说明	取值
patch-number	指定补丁号	整数形式，取值范围是 1~100

#### 9.4.4 配置运行补丁

##### 准备

运行补丁之前，必须激活补丁操作，参见9.4.3小节。

##### 目的

用户可以通过本节操作运行已激活的补丁。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
激活补丁	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>patch patch-number run</b> 来运行补丁；</li> <li>3. 结束。</li> </ol>
查看配置结果	<ol style="list-style-type: none"> <li>1. 不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show patch information</b> 查看系统当前所有补丁信息；</li> <li>3. 结束。</li> </ol>

附表：

参数	说明	取值
patch-number	指定补丁号	整数形式，取值范围是 1~100

### 9.4.5 删除系统补丁

#### 背景信息

目前删除系统补丁有两种方式：

- **patch delete** 方式，不论补丁处于任何状态，补丁文件都将被删除，并且将已激活的补丁去激活状态。
- **patch remove-file** 方式，仅被激活过的补丁文件才能被删除，此方式可以避免用户因误操作而导致系统异常。

#### 目的

用户可以通过本节操作进行补丁删除配置。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
直接删除补丁文件	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>patch patch-number delete</b> 删除补丁文件；</li> <li>3. 结束。</li> </ol>
删除以 FTP 或其他方式加载到设备内存的补丁文件。	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>patch patch-number remove-file</b> 删除补丁文件；</li> <li>3. 结束。</li> </ol>

附表：

参数	说明	取值
patch-number	指定补丁号	整数形式，取值范围是 1~100

### 9.4.6 配置恢复补丁

#### 目的

用户可以通过本节操作进行补丁恢复配置。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
激活补丁	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>patch patch-number resume</b> 恢复补丁；</li> <li>3. 结束。</li> </ol>

目的	步骤
查看配置结果	<ol style="list-style-type: none"> <li>1. 不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show patch information</b> 查看系统当前所有补丁信息；</li> <li>3. 结束。</li> </ol>

附表：

参数	说明	取值
patch-number	指定补丁号	整数形式,取值范围是 1~100

## 9.5 日志管理配置

### 9.5.1 日志管理简介

为了跟踪系统的运行状况及当前系统的状态可以打开系统日志记录功能，使之自动记录系统的状态，从而可以掌握系统的运行状况进行相应的操作。该日志文件可以连续记录 2000 条记录，当记录超出 4000 条时，自动删除日期最久的记录。所以为了使系统不丢失记录，建议用户定期把日志文件导出。

### 9.5.2 配置日志管理

#### 9.5.2.1 启动或取消日志管理功能

##### 目的

本操作用于启动或取消交换机日志管理功能。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
启动系统记录日志功能	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code></li> <li>2. 执行命令 <code>logging on</code></li> </ol>	-
取消系统记录日志功能	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code></li> <li>2. 执行命令 <code>no logging on</code></li> </ol>	

#### 9.5.2.2 配置日志输出方式

##### 目的

本操作用于配置交换机支持的多种日志输出的方式，用户可根据实际情况选择使用。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置系统日志以邮件方式发布	1. 执行命令 <code>configure</code> 2. 执行命令 <code>logging smtp [ level ]</code>	level: 指定日志级别，整数形式，取值范围是 0~7
配置系统日志输出到 syslog 服务器	1. 执行命令 <code>configure</code> 2. 执行命令 <code>logging syslog [ level ]</code>	
配置系统日志输出到 CLI 终端	1. 执行命令 <code>configure</code> 2. 执行命令 <code>logging terminal [ level ]</code>	

### 9.5.2.3 配置记录日志级别

#### 目的

本操作用于配置交换机记录不同级别的日志信息，包括以下八种不同级别的信息：

- 0—>系统不稳定
- 1—>紧急处理动作
- 2—>紧急信息
- 3—>错误信息
- 4—>Warning 信息
- 5—>一般信息
- 6—>详细信息
- 7—>debug 信息

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置系统记录的日志级别	1. 执行命令 <code>configure</code> 2. 执行命令 <code>logging history [ level ]</code>	level: 指定日志级别，整数形式，取值范围是 0~7
(可选) 恢复为记录缺省级别的信息	1. 执行命令 <code>configure</code> 2. 执行命令 <code>no logging history</code>	

### 9.5.2.4 配置日志存储方式

#### 目的

本操作用于配置交换机日志信息以文件形式在本地 Flash 存储。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置系统记录的日志存储方式	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code></li> <li>2. 执行命令 <code>logging buf2file file-name</code></li> </ol>	<code>file-name</code> : 指定文件名称，字符串形式

## 9.5.2.5 配置 syslog 服务器

### 背景信息

Syslog 服务器接收来自客户端的日志信息，以此达到日志的统一管理与查看，便于对设备信息的监控。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置 syslog 服务器	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code></li> <li>2. 执行命令 <code>syslog server ipv4-address [server-port]</code> 或执行命令 <code>syslog6 server ipv6-address [server-port]</code></li> </ol>	<code>ipv4-address</code> : 指定 syslog 服务器 IPv4 地址，点分十进制 <code>ipv6-address</code> : 指定 syslog 服务器 IPv6 地址，形如 X:X::X:X
删除 syslog 服务器	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code></li> <li>2. 执行命令 <code>no syslog server ipv4-address</code> 或执行命令 <code>no syslog6 server ipv6-address</code></li> </ol>	<code>server-port</code> : 指定 syslog 服务器端口号，整数形式，取值范围是 1~65535

## 9.5.2.6 查看日志配置信息

### 目的

当用户配置完成日志管理功能及其相关参数后，若需要查看配置是否正确，可使用本节介绍的操作查看相关信息。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
查看系统日志的信息	<ol style="list-style-type: none"> <li>1. 启动设备，输入用户名及密码后进入特权用户视图或执行命令 <code>disable</code> 退出到普通用户视图或执行 <code>configure</code> 进入全局配置视图</li> <li>2. 执行命令 <code>show logging</code></li> </ol>	-

目的	步骤	参数说明
查看系统日志的具体内容	<ol style="list-style-type: none"> <li>1. 启动设备,输入用户名及密码后进入特权用户视图或执行命令 <code>disable</code> 退出到普通用户视图或执行 <code>configure</code> 进入全局配置视图</li> <li>2. 执行命令 <code>show logging history</code> 或执行命令 <code>show logging history item</code> 或执行命令 <code>show logging history (include exclude) substring STRING</code></li> </ol>	
查看 syslog 服务器配置信息	<ol style="list-style-type: none"> <li>1. 启动设备,输入用户名及密码后进入特权用户视图或执行命令 <code>disable</code> 退出到普通用户视图或执行 <code>configure</code> 进入全局配置视图</li> <li>2. 执行命令 <code>show syslog server</code></li> </ol>	

## 9.6 DDM 配置

### 9.6.1 DDM 概述

在光链路中，定位故障的发生位置对业务的快速加载至关重要。利用智能化的光模块，网络管理单元可以实时监测收发模块的温度、供电电压、激光偏置电流以及发射和接收光功率。这些参量的测量，可以帮助管理单元找出光纤链路中发生故障的位置，简化维护工作，提高系统的可靠性。

总之，通过数字诊断功能，可以定位故障。在故障定位中，需要对 Tx\_power, Rx\_power, Temp, Vcc, Tx\_Bias 的警告和告警状态进行综合分析。

### 9.6.2 配置 DDM 基本功能

#### 目的

使用本节操作配置端口实时监测光模块温度、供电电压、激光偏置电流以及发射和接收光功率，以便快速定位光纤链路故障。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置端口光模块的偏置电流高低阈值	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>interface { gig Ethernet   xgig Ethernet } interface-number</code> 进入接口配置视图；</li> <li>3. 执行命令 <code>laser bias-current-threshold low-threshold high-threshold;</code></li> </ol>

目的	步骤
	4. 结束。
配置自动获取端口光模块的偏置电流高低阈值	1. 执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>interface { gig Ethernet   xgig Ethernet } interface-number</b> 进入接口配置视图； 3. 执行命令 <b>laser bias-current-threshold auto</b> ； 4. 结束。
配置端口光模块的接收光功率高低阈值	1. 执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>interface { gig Ethernet   xgig Ethernet } interface-number</b> 进入接口配置视图； 3. 执行命令 <b>laser rx-power-threshold rx-low-threshold rx-high-threshold</b> ； 4. 结束。
配置自动获取端口光模块的接收光功率高低阈值	1. 执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>interface { gig Ethernet   xgig Ethernet } interface-number</b> 进入接口配置视图； 3. 执行命令 <b>laser rx-power-threshold auto</b> ； 4. 结束。
配置端口光模块的温度高低阈值	1. 执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>interface { gig Ethernet   xgig Ethernet } interface-number</b> 进入接口配置视图； 3. 执行命令 <b>laser temperature-threshold low-threshold high-threshold</b> ； 4. 结束。
配置自动获取端口光模块的温度高低阈值	1. 执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>interface { gig Ethernet   xgig Ethernet } interface-number</b> 进入接口配置视图； 3. 执行命令 <b>laser temperature-threshold auto</b> ； 4. 结束。
配置端口光模块的发送光功率高低阈值	1. 执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>interface { gig Ethernet   xgig Ethernet } interface-number</b> 进入接口配置视图； 3. 执行命令 <b>laser tx-power-threshold tx-low-threshold tx-high-threshold</b> ； 4. 结束。
配置自动获取本端口光模块的发送光功率高低阈值	1. 执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>interface { gig Ethernet   xgig Ethernet } interface-number</b> 进入接口配置视图； 3. 执行命令 <b>laser tx-power-threshold auto</b> ； 4. 结束。
配置端口光模块的	1. 执行命令 <b>configure</b> 进入全局配置视图；

目的	步骤
电压高低阈值	2. 执行命令 <code>interface { gig Ethernet   xgig Ethernet } interface-number</code> 进入接口配置视图； 3. 执行命令 <code>laser voltage-threshold low-threshold high-threshold</code> ； 4. 结束。
配置自动获取端口光模块的电压高低阈值	1. 执行命令 <code>configure</code> 进入全局配置视图； 2. 执行命令 <code>interface { gig Ethernet   xgig Ethernet } interface-number</code> 进入接口配置视图； 3. 执行命令 <code>laser voltage-threshold auto</code> ； 4. 结束。
使能或去使能光模块上报 Trap 功能	1. 执行命令 <code>configure</code> 进入全局配置视图； 2. 执行命令 <code>interface { gig Ethernet   xgig Ethernet } interface-number</code> 进入接口配置视图； 3. 执行命令 <code>laser trap { enable   disable }</code> ； 4. 结束。

附表：

参数	说明	取值
low -threshold	指定端口光模块偏置电流低阈值	整数形式，取值范围是 0~80
high-threshold	指定端口光模块偏置电流高阈值	整数形式，取值范围是 0~80
rx-low -threshold	指定端口光模块的接收光功率低阈值	整数形式，取值范围是-25~0
rx-high-threshold	指定端口光模块的接收光功率高阈值	整数形式，取值范围是-25~0
low -threshold	指定端口光模块温度低阈值	整数形式，取值范围是-20~100
high-threshold	指定端口光模块温度高阈值	整数形式，取值范围是-20~100
tx-low -threshold	指定端口光模块的接收光功率低阈值	整数形式，取值范围是-15~5
tx-high-threshold	指定端口光模块的接收光功率高阈值	整数形式，取值范围是-15~5
low -threshold	指定端口光模块电压低阈值	整数形式，取值范围是 0~10
high-threshold	指定端口光模块电压高阈值	整数形式，取值范围是 0~10
interface-number	以太网端口号	SC9600 系列交换机支持以下 3 种型号的接口配置范围： SC9603：取值范围是 <1-3>/<0-4>/<1-48> SC9608：取值范围是 <1-8>/<0-4>/<1-48> SC9612：取值范围是 <1-12>/<0-4>/<1-48>



### 9.6.3 维护及调试

#### 目的

当 DDM 功能不正常，需要进行查看、调试或定位问题时，可以使用本小节操作。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
查看端口（光口）上配置的 DDM 信息，包括电流、电压等的高低门限值	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gig Ethernet   xgig Ethernet } interface-number</b> 进入接口配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show ddm config</b>;</li> <li>3. 结束。</li> </ol>
查看所有插入了光模块的端口的模块常规硬件信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gig Ethernet   xgig Ethernet } interface-number</b> 进入接口配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show laser hardware</b>;</li> <li>3. 结束。</li> </ol>
查看所有插入了光模块的端口的模块详细硬件信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gig Ethernet   xgig Ethernet } interface-number</b> 进入接口配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show laser hardware detailed</b>;</li> <li>3. 结束。</li> </ol>
查看某个具体光模块端口的模块常规硬件信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gig Ethernet   xgig Ethernet } interface-number</b> 进入接口配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show laser hardware { gig Ethernet   xgig Ethernet } interface-number</b>;</li> <li>3. 结束。</li> </ol>
查看某个具体光模块端口的模块详细硬件信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gig Ethernet   xgig Ethernet } interface-number</b> 进入接口配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show laser hardware { gig Ethernet   xgig Ethernet } interface-number detailed</b>;</li> <li>3. 结束。</li> </ol>

附表：

参数	说明	取值
interface-number	以太网端口号	SC9600 系列交换机支持以下 3 种型号的接口配置范围： SC9603：取值范围是<1-3>/<0-4>/<1-48> SC9608：取值范围是<1-8>/<0-4>/<1-48> SC9612：取值范围是<1-12>/<0-4>/<1-48>

## 9.7 MMU 管理配置

### 9.7.1 设置 CPU 口的内存管理单元寄存器的值

#### 目的

本节介绍如何设置 CPU 口的内存管理单元寄存器的值。

#### 过程

设置 CPU 口的内存管理单元寄存器的值的步骤如下：

1. 执行命令 `interface { fastethernet | gigasethernet | xgigasethernet } interface-number` 或 `interface eth-trunk trunk-number` 进入接口配置视图；
2. 执行命令 `mmu-register REGISTERLIST cos COSLIST register-high-value register-low-value`

参数表：

参数	说明	取值
REGISTERLIST	批量寄存器的号	整数形式，取值范围是 0-2000
COSLIST	端口的 cos 调度队列	整数形式，取值范围是 0-500
register-high-value	寄存器高位值	整数形式，取值范围是 0x0-0xffffffff
register-low-value	寄存器低位值	整数形式，取值范围是 0x0-0xffffffff

### 9.7.2 显示内存管理单元寄存器值

#### 目的

本节介绍如何查看 CPU 口的内存管理单元寄存器的值。

#### 过程

查看 CPU 口的内存管理单元寄存器的值的步骤如下：

1. 进入普通用户视图、特权用户视图、全局配置视图、接口配置视图（以太网、trunk）；

2. 执行如下命令：

- **show mmu-register REGISTERLIST cos COSLIST**
- **show mmu-register REGISTERLIST cos COSLIST { gig Ethernet | xgig Ethernet } interface-number**
- **show mmu-register REGISTERLIST cos COSLIST cpu-port**

参数表：

参数	说明	取值
REGISTERLIST	批量寄存器的号	整数形式，取值范围是 0-2000
COSLIST	端口的 cos 调度队列	整数形式，取值范围是 0-500
interface-number	指定以太网接口号	SC9600 系列交换机支持以下 3 种型号的接口配置范围： SC9603：取值范围是<1-3>/<0-4>/<1-48> SC9608：取值范围是<1-8>/<0-4>/<1-48> SC9612：取值范围是<1-12>/<0-4>/<1-48>

## 第10章 运维管理配置

### 10.1 概述

本章介绍了 SC9600 系列高端交换机运维管理的基本内容、配置过程和配置举例。

本章包括如下主题：

内容	页码
10.1 概述	10-1
10.2 SNMP 配置	10-1
10.3 LLDP 配置	10-11
10.4 RMON 配置	10-24
10.5 NTP 配置	10-32
10.6 SMTP 配置	10-41
10.7 CPU 调试配置	10-42
10.8 ISS 堆叠配置	10-44

### 10.2 SNMP 配置

#### 10.2.1 SNMP 概述

##### 协议介绍

SNMP（Simple Network Management Protocol，简单网络管理协议）是目前网络中用得最广泛的网络管理协议，也是被广泛接受并投入使用的工业标准，用于保证管理信息在任意两点间传送，便于网络管理员在网络上的任何节点检索信息、修改信息、寻找故障、完成故障诊断、进行容量规划和生成报告。SNMP 采用轮询机制，只提供最基本的功能集，特别适合在小型、快速和低成本的环境中使用。SNMP 的实现基于无连接的传输层协议 UDP，得到众多产品的支持。

SNMP 分为 NMS 和 Agent 两部分，NMS（Network Management Station），是运行客户端程序的工作站，目前常用的网管平台有 Sun NetManager 和 IBM NetView；Agent

是运行在网络设备上的服务器端软件。NMS 可以向 Agent 发出 GetRequest、GetNextRequest 和 SetRequest 报文，Agent 接收到 NMS 的请求报文后，根据报文类型进行 Read 或 Write 操作，生成 Response 报文，并将报文返回给 NMS。Agent 在设备发生重新启动等异常情况时，也会主动向 NMS 发送 Trap 报文，向 NMS 汇报所发生的事件。

### 支持的 SNMP 版本及 MIB

为了在 SNMP 报文中唯一标识设备中的管理变量，SNMP 用层次结构命名方案来识别管理对象。用层次结构命名的管理对象的集合就象一棵树，树的节点表示管理对象，如下图所示。管理对象可以用从根开始的一条路径唯一地识别。

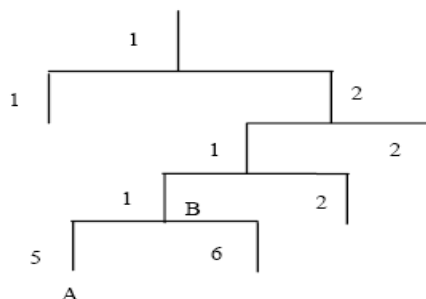


图 10-1 MIB 树结构

MIB (Management Information Base) 的作用就是用来描述树的层次结构，它是所监控网络设备的标准变量定义的集合。在上图中，管理对象 B 可以用一串数字 {1.2.1.1} 唯一确定，这串数字是管理对象的 Object Identifier (客体标识符)。

SC9600 系列高端交换机中的 SNMP Agent 支持 SNMP V1、V2 和 V3，支持的常见 MIB 如下表所示。

表 10-1 交换机支持常见 MIB

MIB 属性	MIB 内容	参见资料
公有 MIB	基于 TCP/IP 网络设备的 MIB II	参见 RFC1213
	RMON MIB	参见 RFC2819
	以太网 MIB	参见 RFC2665
	IF MIB	参见 RFC1573
私有 MIB	DHCP MIB	-
	QAACL MIB	
	ADBM MIB	
	RSTP MIB	

MIB 属性	MIB 内容	参考资料
	VLAN MIB	
	设备管理	
	接口管理	

## 10.2.2 配置 SNMP 维护信息

### 目的

用户通过本节操作配置 SNMP 的维护信息，便于网管对设备的维护。

在交换机出现错误需要紧急解决时，便于联系本地的维护工程师。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
指定管理员的 联系方式	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>snmp contact contact-info</b> 配置管理员的联络方式；</li> <li>3. 结束。</li> </ol>
指定被管理设 备的位置	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>snmp location location-info</b> 配置交换机的位置；</li> <li>3. 结束。</li> </ol>

附表：

参数	说明	取值
contact-info	指定系统维护联系信息	字符串形式
location-info	指定设备所在地址信息	字符串形式

## 10.2.3 配置 SNMP 基本功能

### 目的

用户通过本节操作配置 SNMP 基本功能，实现网管站 NM Station 和 Agent 两部分的正常通信。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
----	----

目的	步骤
使能 SNMP 协议	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>snmp enable</b> 使能 SNMP 协议;</li> <li>3. 结束。</li> </ol>
配置 SNMP 的团体名	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>snmp community name { ro   rw }</b> 或执行命令 <b>snmp community name { ro   rw } view view-name</b> 设置 SNMP 团体名;</li> <li>3. 结束。</li> </ol>
(可选) 使能写团体名功能	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>snmp rw-community enable</b> 使能写团体名功能;</li> <li>3. 结束。</li> </ol>
配置 SNMP 视图	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>snmp view view-name oid-tree { included   excluded }</b> 或执行命令 <b>snmp view view-name oid-tree { included   excluded } mask subtreemask</b> 创建不同的 MIB 视图使网管访问设备时具有不同的访问权限;</li> <li>3. 结束。</li> </ol>
配置 SNMP 组信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>snmp group group-name read-view read-view write-view write-view notify-view notify-view</b> 配置 SNMP 组;</li> <li>3. 结束。</li> </ol>
创建 SNMP 用户	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>snmp user user-name group group-name no-auth-no-priv</b> 或执行命令 <b>snmp user user-name group group-name auth { md5   sha } authkey priv no-priv</b> 或执行命令 <b>snmp user user-name group group-name auth { md5   sha } authkey priv des privkey</b> 创建用户信息, 可以使指定组中的用户对设备进行访问;</li> <li>3. 结束。</li> </ol>
(可选) 配置 SNMP 重认证时间	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>snmp reauth-interval interval</b> 设置 SNMP 验证失败时重新进行认证的间隔时间;</li> <li>3. 结束。</li> </ol>
(可选) 配置 SNMP 认证失败次数	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>snmp fail-count count</b> 设置 SNMP 进行认证失败的次数;</li> <li>3. 结束。</li> </ol>
(可选) 配置 SNMP 端口号	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>{ snmp   snmp6 } port { port-number   default }</b> 设置 SNMP 协议包使用的端口号;</li> <li>3. 结束。</li> </ol>
去使能 SNMP 协议	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>snmp disable</b> 去使能 SNMP 协议;</li> <li>3. 结束。</li> </ol>

目的	步骤
删除 SNMP 团体名	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>no snmp community name</b> 删除已配置的 SNMP 团体名;</li> <li>3. 结束。</li> </ol>
(可选) 去使能写团体名功能	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>snmp rw-community disable</b> 去使能写团体名功能;</li> <li>3. 结束。</li> </ol>
删除 SNMP 用户	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>no snmp user user-name</b> 删除已创建的 SNMP 用户;</li> <li>3. 结束。</li> </ol>
删除 SNMP 组信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>no snmp group group-name</b> 删除已配置的 SNMP 组信息;</li> <li>3. 结束。</li> </ol>
删除 SNMP 视图	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>no snmp view view-name</b> 或执行命令 <b>no snmp view view-name oid-tree</b> 删除已配置的 SNMP 视图;</li> <li>3. 结束。</li> </ol>

附表:

参数	说明	取值
name	指定团体名称	字符串形式, 少于 20 个字符
{ ro   rw }	表明该团体名在指定视图内的权限, ro 表示只有读权限, rw 表示可读可写	-
view-name	指定团体名对应的视图名	字符串形式
oid-tree	指定 oid 字符串, 用来标示视图范围	字符串形式
{ included   excluded }	表示包含/排除	-
subtreemask	指定掩码 oid 字符串	字符串形式
group-name	指定 SNMP 组名称	字符串形式
read-view	指定只读视图名称	字符串形式
write-view	指定读写视图名称	字符串形式
notify-view	指定通告视图名称	字符串形式
user-name	指定用户名	字符串形式
{ md5   sha }	指定认证方式为 MD5 认证或 SHA 认证	-
authkey	指定认证的密钥	字符串形式
privkey	指定加密密钥	字符串形式
no-priv	表示不加密	-
no-auth-no-priv	表示不认证不加密	-
interval	指定重认证时间	整数形式, 取值范围是 3~1440, 单位: 分钟



参数	说明	取值
count	指定 SNMP 认证失败次数	整数形式，取值范围是 3~10
port-number	指定 SNMP 端口号	整数形式，取值范围是 1000~9999
default	指定为缺省值	整数形式，取值为 161

## 10.2.4 配置发送 Trap 功能

### 背景信息

Trap 是被管理设备未经请求而主动向 NMS 发送的消息，用于报告重要紧急的事件。被管理设备必须配置 Trap 功能后才会主动发送这些消息。

### 目的

用户通过本节操作配置设备主动发送 Trap 消息。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
（可选）使能认证失败后发送 Trap 消息的功能	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>snmp auth-trap enable</b> 使能认证 trap 后，如果认证失败则设备会发送 trap 消息；</li> <li>3. 结束。</li> </ol>
（可选）使能 SNMP 丰富告警功能	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>snmp rich-trap enable</b>；</li> <li>3. 结束。</li> </ol>
（可选）配置 SNMP 告警日志操作	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>snmp trap-log action { terminal   syslog   smtp   history   all   default }</b>；</li> <li>3. 结束。</li> </ol>
（可选）配置 SNMP 告警日志的优先级	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>snmp trap-log priority { priority default }</b>；</li> <li>3. 结束。</li> </ol>
指定 SNMP 的 Trap 信息的目标主机	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. （IPv4）执行命令 <b>snmp trap-server ipv4-address security-name { v1   v2   v3 }</b>或执行命令 <b>snmp trap-server ipv4-address port security-name { v1   v2   v3 }</b>或执行命令 <b>snmp trap-server ipv4-address security-name v3 { auth   priv }</b>或执行命令 <b>snmp trap-server ipv4-address port security-name v3 { auth   priv }</b>；</li> <li>3. （IPv6）执行命令 <b>snmp6 trap-server ipv6-address security-name { v1</b></li> </ol>

目的	步骤
	v2   v3 }或执行命令 <b>snmp6 trap-server ipv6-address port security-name { v1   v2   v3 }</b> 或执行命令 <b>snmp6 trap-server ipv6-address security-name v3 { auth   priv }</b> 或执行命令 <b>snmp6 trap-server ipv6-address port security-name v3 { auth   priv }</b> ; 4. 结束。
(可选) 使能将告警记录到告警历史表中的功能	<b>snmp trap-history</b> 1. 执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>snmp trap-history enable</b> ; 3. 结束。
(可选) 配置 SNMP 告警历史表的大小	1. 执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>snmp trap-history history-table-size</b> ; 3. 结束。
(可选) 使能指定告警源 IP 地址功能及配置告警源 IP 地址	<b>snmp source-input</b> 、 <b>snmp trap-source</b> 1. 执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>snmp source-input enable</b> ; 3. 执行命令 <b>snmp trap-source ipv4-address</b> ; 4. 结束。
(可选) 去使能认证失败后发送 Trap 消息的功能	1. 执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>snmp auth-trap disable</b> 去使能认证 trap 后, 如果认证失败设备则不会发送 trap 消息; 3. 结束。
(可选) 去使能 SNMP 丰富告警功能	1. 执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>snmp rich-trap disable</b> ; 3. 结束。
(可选) 去使能将告警记录到告警历史表中的功能	1. 执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>snmp trap-history disable</b> ; 3. 结束。
(可选) 去使能指定告警源 IP 地址功能	1. 执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>snmp source-input disable</b> ; 3. 结束。
删除 SNMP 的 Trap 信息的目标主机	1. 执行命令 <b>configure</b> 进入全局配置视图; 2. (IPv4) 执行命令 <b>no snmp trap-server ipv4-address</b> 或执行命令 <b>no snmp trap-server ipv4-address security-name</b> ; 3. (IPv6) 执行命令 <b>no snmp6 trap-server ipv6-address</b> 或执行命令 <b>no snmp6 trap-server ipv6-address security-name</b> ; 4. 结束。

附表:

参数	说明	取值
terminal	指定告警信息输出到终端	-

参数	说明	取值
syslog	指定告警信息发送到 syslog 服务器	-
sntp	指定告警信息发送到邮件	-
history	指定告警与信息写入日志	-
all	指定支持多有的操作	-
default	指定为默认操作	告警信息写入日志
priority	指定告警日志的优先级	整数形式, 取值范围是 0~7
default	指定为默认优先级	5
ipv4-address	指定接收 trap 信息的主机 IPv4 地址	点分十进制
{ v1   v2   v3 }	指定 snmp 发送的 trap 的版本号	-
security-name	指定团体名	字符串形式
{ auth   priv }	指定鉴权或者私密	-
port	指定发送 trap 的端口号	整数形式, 取值范围是 1-65535 默认是 162
ipv6-address	指定接收 trap 信息的主机 IPv6 地址	-
history-table-size	指定 SNMP 告警历史功能表大小	整数形式, 取值范围是 <0-65535>

## 10.2.5 维护及调试

### 目的

用户可以通过本节操作对 SNMP 协议进行调试, 用于定位问题。

### 过程

根据不同目的, 执行相应步骤, 具体参见下表。

目的	步骤
打开 SNMP 的调试功能	<ol style="list-style-type: none"> <li>1. 保持在当前特权用户视图下;</li> <li>2. 执行命令 <b>debug snmp</b> 打开 SNMP 调试功能;</li> <li>3. 结束。</li> </ol>
关闭 SNMP 的调试功能	<ol style="list-style-type: none"> <li>1. 保持在当前特权用户视图下;</li> <li>2. 执行命令 <b>no debug snmp</b> 关闭 SNMP 调试功能;</li> <li>3. 结束。</li> </ol>
查看 SNMP 的内存利用率	<ol style="list-style-type: none"> <li>1. 保持在当前特权用户视图下, 或执行 <b>disable</b> 退出到普通用户视图, 或执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>show memory snmp</b> 查看当前 SNMP 的内存利用率;</li> <li>3. 结束。</li> </ol>
查看设备 SNMP 的代理信息	<ol style="list-style-type: none"> <li>1. 保持在当前特权用户视图下, 或执行 <b>disable</b> 退出到普通用户视图, 或执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>show snmp agent</b> 查看设备 SNMP 的代理信息;</li> <li>3. 结束。</li> </ol>

目的	步骤
查看 SNMP 的团体配置信息	<ol style="list-style-type: none"> <li>1. 保持在当前特权用户视图下，或执行 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>show snmp community</b> 查看 SNMP 的团体配置信息；</li> <li>3. 结束。</li> </ol>
查看 SNMP 的配置信息	<ol style="list-style-type: none"> <li>1. 保持在当前特权用户视图下，或执行 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>show snmp config</b> 查看 SNMP 的配置信息；</li> <li>3. 结束。</li> </ol>
查看 SNMP 组信息	<ol style="list-style-type: none"> <li>1. 保持在当前特权用户视图下，或执行 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>show snmp group</b> 查看 SNMP 组信息；</li> <li>3. 结束。</li> </ol>
查看 SNMP 的报文处理统计数据信息	<ol style="list-style-type: none"> <li>1. 保持在当前特权用户视图下，或执行 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>show snmp statistic</b> 查看 SNMP 的报文处理统计数据信息；</li> <li>3. 结束。</li> </ol>
查看 SNMP 的告警描述信息	<ol style="list-style-type: none"> <li>1. 保持在当前特权用户视图下，或执行 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>show snmp trap-description</b> 查看 SNMP 的告警描述信息；</li> <li>3. 结束。</li> </ol>
查看 SNMP 的告警历史信息	<ol style="list-style-type: none"> <li>1. 保持在当前特权用户视图下，或执行 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>show snmp trap-history</b> 查看 SNMP 的告警历史信息；</li> <li>3. 结束。</li> </ol>
查看显示接收 trap 信息的主机及版本类型	<ol style="list-style-type: none"> <li>1. 保持在当前特权用户视图下，或执行 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>show snmp trap-server</b> 查看显示接收 trap 信息的主机及版本类型；</li> <li>3. 结束。</li> </ol>
查看 SNMP 用户信息	<ol style="list-style-type: none"> <li>1. 保持在当前特权用户视图下，或执行 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>show snmp user</b> 查看 SNMP 用户信息；</li> <li>3. 结束。</li> </ol>
查看 SNMP 视图信息	<ol style="list-style-type: none"> <li>1. 保持在当前特权用户视图下，或执行 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>show snmp view</b> 查看 SNMP 视图信息；</li> <li>3. 结束。</li> </ol>

## 10.2.6 配置举例

### 组网要求

网管工作站（NMS）与交换机通过以太网相连，网管工作站 IP 地址为 129.102.149.23，交换机的 IP 地址为 129.102.0.1。在交换机上进行如下配置：设置团体名和访问权限、管理员标识以及交换机的位置信息、允许交换机发送 Trap 消息。

### 组网图

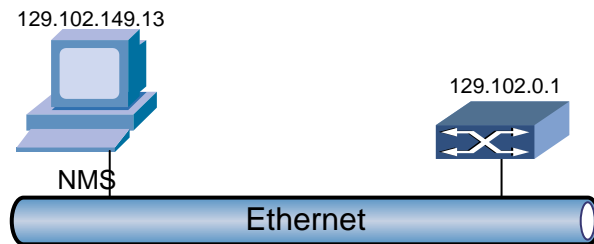


图 10-2 SNMP 配置举例组网图

### 配置步骤

#进入全局配置视图

```
SC9600#config
```

#设置团体、群组 and 用户

```
SC9600(config)#snmp view v3test 1.3.6 include
```

```
SC9600(config)#snmp group aaa read-view v3test write-view v3test notify-view v3test
```

```
SC9600(config)#snmp user admin group aaa no-auth-no-priv
```

#允许向网管工作站（NMS）129.102.149.23 发送 Trap 报文。

```
SC9600(config)#snmp trap enable
```

```
SC9600(config)#snmp trap-server 129.102.149.23 v3
```

### 配置 NMS

网管所在的 PC 机需要进行登录设置。对于 Mib-Browser，登陆设置为：SNMPV1、V2 使用缺省的团体名登录，SNMPV3 使用用户 admin 登陆。用户可利用网管系统完成对交换机的查询和配置操作，具体情况请参考网管产品的配套手册。

## 10.3 LLDP 配置

### 10.3.1 LLDP 概述

#### 背景

目前以太网技术应用越来越广泛，随着大规模组网应用的需求以及日益繁多且配置复杂的网络设备的出现，对网络管理的能力的要求也越来越高。为了使不同厂商的设备能够在网络中相互发现并交互各自的系统及配置信息，需要有一个标准的信息交流平台。但现阶段许多网管软件最多只能分析到第三层网络拓扑结构，无法说明设备的位置以及网络操作方式等信息。LLDP（Link Layer Discovery Protocol，链路层发现协议）就是在这样的背景下产生的。

#### LLDP 简介

LLDP 是 IEEE 802.1ab 中定义的第二层发现协议。它提供了一种标准的链路层发现方式，可以将本端设备的主要能力、管理地址、设备标识、接口标识等信息组织成不同的 TLV（Type/Length/Value，类型/长度/值），并封装在 LLDPDU（Link Layer Discovery Protocol Data Unit，链路层发现协议数据单元）中发布给与自己直连的邻居，邻居收到这些信息后将其以标准 MIB（Management Information Base，管理信息库）的形式保存起来，以供网络管理系统查询及判断链路的通信状况。

通过运行该协议，网络系统可以清晰得知与之相连所有设备的二层信息，这既有利于网管规模迅速扩大，同时也利于掌握更详细的网络拓扑信息及变化信息。LLDP 协议还有助于发现网络中实际存在的不合理的配置并上报给网管系统，及时消除错误配置。

#### LLDP 术语解释

- LLDP: Link Layer Discovery Protocol 链路层发现协议
- LLDPDU: Link Layer Discovery Protocol Data Unit 链路层发现协议数据单元
- MIB: Management Information Base (module)管理系统库
- SNAP: Subnetwork Access Protocol 子网访问协议
- TTL: time to live (value)存活时间

### 10.3.2 LLDP 工作机制

#### LLDP 端口工作模式

LLDP 端口有以下四种工作模式：

- TxRx: 既发送也接收 LLDP 报文。
- Tx: 只发送不接收 LLDP 报文。
- Rx: 只接收不发送 LLDP 报文。
- Disable: 既不发送也不接收 LLDP 报文。



说明:

当端口的 LLDP 工作模式发生变化时，端口将对协议状态机进行初始化操作。为了避免端口工作模式频繁改变而导致端口不断执行初始化操作，可配置端口初始化延迟时间，当端口工作模式改变时延迟一段时间再执行初始化操作。

### LLDP 报文的发送机制

当端口工作在 TxRx 或 Tx 模式时，设备会周期性地向邻居设备发送 LLDP 报文，发送间隔为 msgTxInterval（可配置，缺省值为 30S）。如果设备的本地配置发生变化则立即发送 LLDP 报文，以将本地信息的变化情况尽快通知给邻居设备。但为了防止本地信息的频繁变化而引起 LLDP 报文的大量发送，每发送一个 LLDP 报文后都需延迟一段时间后再继续发送下一个报文，延迟间隔为 TxDelay（可配置，缺省值为 2S）。

### LLDP 报文的发送状态机

当端口工作在 TxRx 或 Tx 模式时，共发送状态机有四个状态：

1. TX\_LLDP\_INITIALIZE: 初始化状态。
2. TX\_IDLE: 闲置状态。
3. TX\_SHUTDOWN\_FRAME: 发送关闭帧的状态。
4. TX\_INFO\_FRAME: 发送消息的状态。

其状态机跳转的流程参见图 10-3。

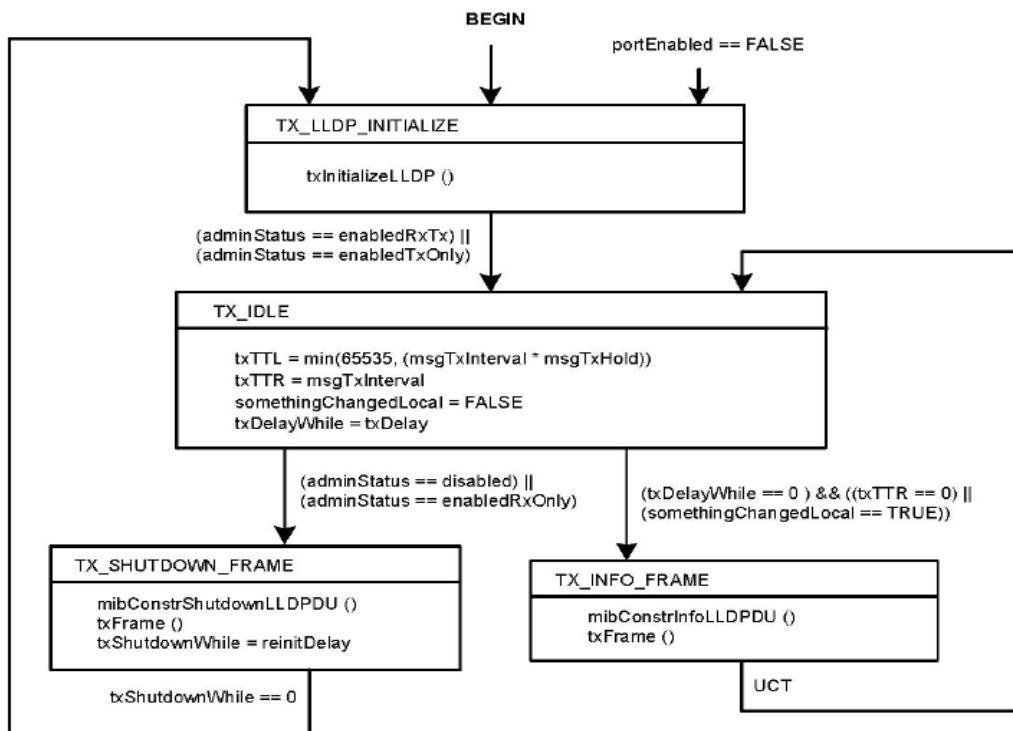


图 10-3 IEEE802.1ab 标准 LLDP 报文的发送状态机

### LLDP 报文的接收机制

当端口工作在 TxRx 或 Rx 模式时，首先初始化设备的接收模式。设备能够接受 LLDP 报文，并对收到的 LLDP 报文及其携带的 TLV 进行有效性检查，通过检查后再将邻居信息保存到本地，并根据 TLV 中 TTL（Time To Live，生存时间）的值来设置邻居信息在本地设备上的老化时间，若该值为零，则立刻老化该邻居信息。（TTL 的值由消息发送时间间隔与 TTL 乘数来决定。即  $TTL = TTL \text{ 乘数} \times \text{LLDPDU 发送周期}$ ，如果 TTL 乘数与 LLDPDU 发送周期的乘积大于 65535，则 TTL 的值取 65535 秒。）

### LLDP 报文的接收状态机

当端口工作在 TxRx 或 Rx 模式时，其接收状态机共有四个状态：

1. LLDP\_WAIT\_PORT\_OPERATIONAL：端口准备状态。
2. LLDP\_RX\_INITIALIZE：接收初始化状态。
3. LLDP\_RX\_WAITFOR\_FRAME：等待接收帧的状态。
4. LLDP\_RX\_FRAME：接收到帧的状态。

其状态机跳转流程为参见。



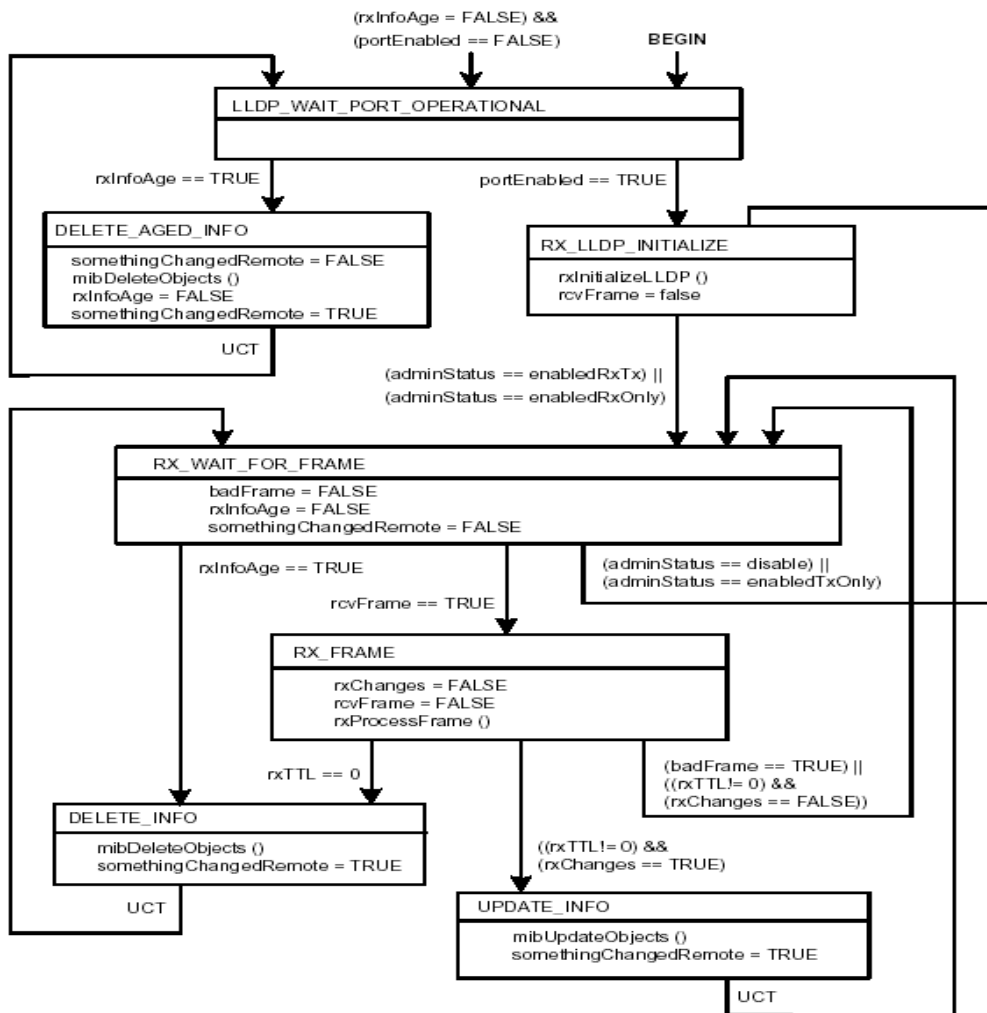


图 10-4 IEEE802.1ab 标准 LLDP 报文的接收状态机

### 10.3.3 配置 LLDP 基本功能

#### 目的

使用本节操作配置 LLDP，以便不同厂商设备可以拓扑发现，获取对端的能力、配置等信息，同时使网络管理系统有办法发现一些影响上层应用交互的配置不一致或错误，帮助定位不一致或错误问题。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
端口下使能或去使能 LLDP 及其管理状态	1. 执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>interface { fastethernet   gig Ethernet   xgig Ethernet } interface-number</b> 进入接口配置视图； 3. 执行命令 <b>lldp admin-status { tx-only   rx-only   rx-tx   disable }</b> 使能或去使能接口 LLDP 及其管理状态； 4. 结束。
配置 LLDP 的管理地址	1. 执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>interface { fastethernet   gig Ethernet   xgig Ethernet } interface-number</b> 进入接口配置视图； 3. 执行命令 <b>lldp management-address ip-address { enable   disable }</b> 配置 LLDP 的管理地址； 4. 结束。

附表：

参数	说明	取值
tx-only	只发送	-
rx-only	只接收	-
rx-tx	发送和接收	-
disable	不发送也不接收	-
interface-number	指定以太网接口号	SC9600 系列交换机支持以下 3 种型号的接口配置范围： SC9603：取值范围是<1-3>/<0-4>/<1-48> SC9608：取值范围是<1-8>/<0-4>/<1-48> SC9612：取值范围是<1-12>/<0-4>/<1-48>
ip-address	指定 IP 地址	点分十进制
enable	使能 lldp 管理地址	-
disable	去使能 lldp 管理地址	-

### 10.3.4 配置 LLDP 参数

目的

用户可以使用本节操作，根据网络负载及时调整 LLDP 报文发送、延迟时间等 LLDP 相关参数。

本节操作均可根据实际情况选配。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
(可选)配置 lldp 帧发送时间间隔	1. 执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>lldp tx-interval { tx-interval   default }</b> 配置 LLDP 帧发送时间间隔; 3. 结束。
(可选)配置 LLDP 帧发送间隔的倍数	1. 执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>lldp tx-hold { tx-hold   default }</b> 配置 LLDP 帧发送间隔的倍数; 3. 结束。
(可选)配置 LLDP 端口状态重新初始化的时延	1. 执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>lldp reinit-delay { reinit-delay   default }</b> 配置 LLDP 端口状态重新初始化的时延; 3. 结束。
(可选)配置设备发送 LLDP 报文的延迟时间	1. 执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>lldp tx-delay { tx-delay   default }</b> 配置设备发送 LLDP 报文的延迟时间; 3. 结束。
(可选)全局配置告警发送时间间隔	1. 执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>lldp notification-interval { notification-interval   default }</b> 全局配置告警发送时间间隔; 3. 结束。
(可选)配置 LLDP MED 设备类型	1. 执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>lldp device-class { generic-endpoint   media-endpoint   communication-endpoint   network-connectivity }</b> 配置 LLDP MED 设备类型; 3. 结束。
(可选)配置 LLDP MED 快速发包个数	1. 执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>lldp faststart-count { faststart-count   default }</b> 配置 LLDP MED 快速发包个数; 3. 结束。
(可选)使能或去使能端口 LLDP 告警功能	1. 执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>interface { fastethernet   gigasethernet   xgigasethernet } interface-number</b> 进入接口配置视图; 3. 执行命令 <b>lldp notification { enable   disable }</b> 使能或去使能端口 LLDP 告警功能; 4. 结束。
(可选)使能或去使能	1. 执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>interface { fastethernet   gigasethernet   xgigasethernet }</b>

目的	步骤
端口 LLDP MED 告警功能	<p><i>interface-number</i> 进入接口配置视图;</p> <p>3. 执行命令 <b>lldp med-notification { enable   disable }</b>使能或去使能端口 LLDP MED 告警功能;</p> <p>4. 结束。</p>
(可选)配置端口下与 MED 相关的信息	<p>1. 执行命令 <b>configure</b> 进入全局配置视图;</p> <p>2. 执行命令 <b>interface { fastethernet   gigasethernet   xgigasethernet } <i>interface-number</i></b> 进入接口配置视图;</p> <p>3. 执行命令 <b>lldp med-tlv-tx { capabilities   network-policy   location   extended-pse   extended-pd   inventory   all } { enable   disable }</b>配置端口下与 MED 相关的信息;</p> <p>4. 结束。</p>
(可选)配置接口下 LLDP 的基本 TLV	<p>1. 执行命令 <b>configure</b> 进入全局配置视图;</p> <p>2. 执行命令 <b>interface { fastethernet   gigasethernet   xgigasethernet } <i>interface-number</i></b> 进入接口配置视图;</p> <p>3. 执行命令 <b>lldp med-tlv-tx { capabilities   network-policy   location   extended-pse   extended-pd   inventory   all } { enable   disable }</b>配置端口下与 MED 相关的信息;</p> <p>4. 结束。</p>
(可选)配置接口下 LLDP 的基本 TLV	<p>1. 执行命令 <b>configure</b> 进入全局配置视图;</p> <p>2. 执行命令 <b>interface { fastethernet   gigasethernet   xgigasethernet } <i>interface-number</i></b> 进入接口配置视图;</p> <p>3. 执行命令 <b>lldp basic-tlv-tx { port-description   system-name   system-description   system-capability   all } { enable   disable }</b>配置接口下 LLDP 的基本 TLV;</p> <p>4. 结束。</p>
(可选)配置 IEEE802.1 可选 TLV 的端口 VLAN ID 功能	<p>1. 执行命令 <b>configure</b> 进入全局配置视图;</p> <p>2. 执行命令 <b>interface { fastethernet   gigasethernet   xgigasethernet } <i>interface-number</i></b> 进入接口配置视图;</p> <p>3. 执行命令 <b>lldp dot1-tlv-tx port-vid { enable   disable }</b>或 <b>lldp dot1-tlv-tx port-vid <i>vlanlist</i> { enable   disable }</b>配置 IEEE802.1 可选 TLV 的端口 VLAN ID 功能;</p> <p>4. 结束。</p>
(可选)配置 IEEE802.1 可选 TLV 的 VLAN 名字功能	<p>1. 执行命令 <b>configure</b> 进入全局配置视图;</p> <p>2. 执行命令 <b>interface { fastethernet   gigasethernet   xgigasethernet } <i>interface-number</i></b> 进入接口配置视图;</p> <p>3. 执行命令 <b>lldp dot1-tlv-tx <i>vlan-name</i> <i>vlanlist</i> { enable   disable }</b>配置 IEEE802.1 可选 TLV 的 VLAN 名字功能;</p> <p>4. 结束。</p>
(可选)配置	<p>1. 执行命令 <b>configure</b> 进入全局配置视图;</p> <p>2. 执行命令 <b>interface { fastethernet   gigasethernet   xgigasethernet }</b></p>

目的	步骤
IEEE802.1 可选 TLV 的协议 VLAN ID 的功能	<p><i>interface-number</i> 进入接口配置视图；</p> <p>3. 执行命令 <b>lldp dot1-tlv-tx protocol-vid vlanlist { enable   disable }</b>配置 IEEE802.1 可选 TLV 的协议 VLAN ID 的功能；</p> <p>4. 结束。</p>
(可选)配置 IEEE802.3 组织定义的 TLV 的相关信息	<p>1. 执行命令 <b>configure</b> 进入全局配置视图；</p> <p>2. 执行命令 <b>interface { fastethernet   gigasethernet   xgigasethernet } interface-number</b> 进入接口配置视图；</p> <p>3. 执行命令 <b>lldp dot3-tlv-tx { mac-phy   power   link-aggregation   max-frame-size   all } { enable   disable }</b>配置 IEEE802.3 组织定义的 TLV 的相关信息；</p> <p>4. 结束。</p>

附表：

参数	说明	取值
tx-interval	lldp 帧发送间隔，单位：秒	整数形式，取值范围是 5~32768
default	表示默认大小	30s
tx-hold	LLDP 帧发送间隔的倍数	整数形式，取值范围是 2~10
default	表示默认大小	4
reinit-delay	LLDP 端口状态重新初始化的时延	整数形式，取值范围是 1~10
default	表示默认大小	2s
tx-delay	配置设备发送 LLDP 报文的延迟时间	整数形式，取值范围是 1~8192
default	表示默认大小	2s
notification-interval	配置通告发送时间间隔	整数形式，取值范围是 5~3600
default	表示默认大小	4s
generic-endpoint	一般终端设备	1
media-endpoint	媒体终端设备	2
communication-endpoint	通讯终端设备	3
network-connectivity	网络连接设备	4
faststart-count	lldp med 快速发包个数	整数形式，取值范围是 1~10
default	表示默认大小	4s
enable	使能端口 LLDP 告警功能	-
disable	去使能端口 LLDP 告警功能	-
enable	使能端口 LLDP MED 告警功能	-
disable	去使能端口 LLDP MED 告警功能	-
capabilities	表示能力级	-

参数	说明	取值
netw ork-policy	表示支持的应用	-
location	表示端口位置标识信息	-
extended-pse	表示供电能力	-
inventory	表示详细目录	-
all	表示以上所有项目	-
enable	使能端口下与 MED 相关的信息	-
disable	去使能端口下与 MED 相关的信息	-
port-description	表示端口描述	-
system-name	表示系统名称	-
system-description	表示系统描述	-
system-capability	表示系统能力	-
all	表示以上所有项目	-
enable	使能接口下 LLDP 的基本 TLV	-
disable	去使能接口下 LLDP 的基本 TLV	-
vlanlist	VLAN ID	整数取值，取值范围是 1-4094
enable	使能 IEEE802.1 可选 TLV 的端口 vid 功能	-
disable	去使能 IEEE802.1 可选 TLV 的端口 vid 功能	-
enable	使能 IEEE802.1 可选 TLV 的 vlan 名字功能	-
disable	去使能 IEEE802.1 可选 TLV 的 vlan 名字功能	-
enable	使能 IEEE802.1 可选 TLV 的协议 VID 的功能	-
disable	去使能 IEEE802.1 可选 TLV 的协议 VID 的功能	-
mac-phy	表示端口的速率	-
power	表示端口的供电能力	-
link-aggregation	表示链路聚合	-
max-frame-size	表示最大帧长	-
all	表示以上所有项目	-
enable	使能 IEEE802.1 可选 TLV 的协议 VID 的功能	-
disable	去使能 IEEE802.1 可选 TLV 的协议 VID 的功能	-
interface-number	指定以太网接口号	SC9600 系列交换机支持以下 3 种型号的接口配置范围： SC9603：取值范围是

参数	说明	取值
		<1-3>/<0-4>/<1-48> SC9608 : 取值范围是 <1-8>/<0-4>/<1-48> SC9612 : 取值范围是 <1-12>/<0-4>/<1-48>

### 10.3.5 维护及调试

#### 目的

当 LLDP 功能不正常，需要进行查看、调试或定位问题时，可以使用本小节操作。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
打开 LLDP 调试功能	1. 不执行任何命令保持当前特权用户视图； 2. 执行命令 <b>debug lldp { config   rxstate   txstate   rxpkt   all }</b> 打开 LLDP 调试功能； 3. 结束。
关闭 LLDP 调试开关	1. 不执行任何命令保持当前特权用户视图； 2. 执行命令 <b>no debug lldp { config   rxstate   txstate   rxpkt   all }</b> 关闭 LLDP 调试开关； 3. 结束。
查看 LLDP 端口信息	1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gigasethernet   xgigasethernet } interface-number</b> 进入接口配置视图，或不执行任何命令保持当前特权用户视图； 2. 执行命令 <b>show lldp interface</b> 或 <b>show lldp interface { gigasethernet   xgigasethernet } interface-number</b> 或 <b>show lldp interface eth-trunk trunk-number</b> 或 <b>show lldp interface verbose</b> ； 3. 结束。
查看 LLDP 统计信息	1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gigasethernet   xgigasethernet } interface-number</b> 进入接口配置视图，或不执行任何命令保持当前特权用户视图； 2. 执行命令 <b>show lldp statistic</b> 或 <b>show lldp statistic interface { gigasethernet   xgigasethernet } interface-number</b> 或 <b>show lldp statistic interface eth-trunk trunk-number</b> ； 3. 结束。
查看所有邻居或者指定邻居的设备信息	1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gigasethernet   xgigasethernet } interface-number</b> 进入接口配置视图，或不执行任何命令保持当前特权用户视图；

目的	步骤
	<ol style="list-style-type: none"> <li>2. 执行命令 <b>show lldp remote</b> 或 <b>show lldp remote verbose</b> 或 <b>show lldp remote remote-number</b>;</li> <li>3. 结束。</li> </ol>
查看 LLDP 内存利用率	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b> 进入接口配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show memory lldp</b> 查看 LLDP 内存利用率；</li> <li>3. 结束。</li> </ol>
查看 LLDP 本地信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b> 进入接口配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show lldp local</b> 查看 LLDP 本地信息；</li> <li>3. 结束。</li> </ol>
查看 LLDP 的配置信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b> 进入接口配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show lldp config</b> 查看 LLDP 的配置信息；</li> <li>3. 结束。</li> </ol>
查看指定接口邻居信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b> 进入接口配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show lldp remote interface { gigaehternet   xgigaehternet } interface-number</b> 或 <b>show lldp remote interface eth-trunk trunk-number</b>;</li> <li>3. 结束。</li> </ol>
查看指定接口配置信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b> 进入接口配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show lldp config interface { gigaehternet   xgigaehternet } interface-number</b> 或 <b>show lldp config interface eth-trunk trunk-number</b>;</li> <li>3. 结束。</li> </ol>
查看指定接口本地设备信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b> 进入接口配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show lldp local interface { gigaehternet   xgigaehternet } interface-number</b> 或 <b>show lldp local interface eth-trunk trunk-number</b>;</li> <li>3. 结束。</li> </ol>
清零 LLDP 端口的统计计数	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface { fastethernet   gigaehternet   xgigaehternet } interface-number</b> 进入接口配置视图；</li> <li>3. 执行命令 <b>reset lldp counter</b> 清零 LLDP 端口的统计计数；</li> </ol>



目的	步骤
	4. 结束。

附表：

参数	说明	取值
interface-number	指定以太网接口号	SC9600 系列交换机支持以下 3 种型号的接口配置范围： SC9603: 取值范围是<1-3>/<0-4>/<1-48> SC9608: 取值范围是<1-8>/<0-4>/<1-48> SC9612: 取值范围是<1-12>/<0-4>/<1-48>
trunk-number	指定 trunk 口接口号	整数形式，取值范围是<1-32>
remote-number	指定邻居信息 ID	整数形式，取值范围是 1-2147483647

### 10.3.6 配置举例

#### 组网要求

- 1) switch A、switch B、switch C、switch D、switch E 五台交换机分别将自己的 Chassis ID、端口号 ID、TTL、管理地址以及其他的配置信息公告给其他设备。
- 2) 每一台设备都可以将获得的信息存储至本地 MIB 数据库中，并可通过 SNMP 访问。
- 3) PC 通过 SNMP 访问 switch A，可得知 switch B、switch C 是与 switch A 的设备，由此可得出与 switch A 直连的拓扑。并通过 switch B、switch C 公告的消息中得知 switch B、switch C 的管理地址，分别为 10.1.1.2 与 10.1.1.3，进而访问 switch B 与 switch C。
- 4) 访问 switch B，可知与 switch B 直连的设备有 switch D，由此可得出与 switch B 直连的拓扑。并且可通过 switch D 公告的消息中得知 switch D 的管理地址，为 10.1.1.4，进而可继续访问 switch D。
- 5) 访问 switch C，可知与 switch C 直连的设备有 switch E，由此可得出与 switch C 直连的拓扑。并且可通过 switch E 公告的消息中得知 switch E 的管理地址为 10.1.1.5，进而可继续访问 switch E。
- 6) 按以上步骤，可得出一个全面的拓扑图，并且可知道各个设备的相关配置信息。

#### 组网图

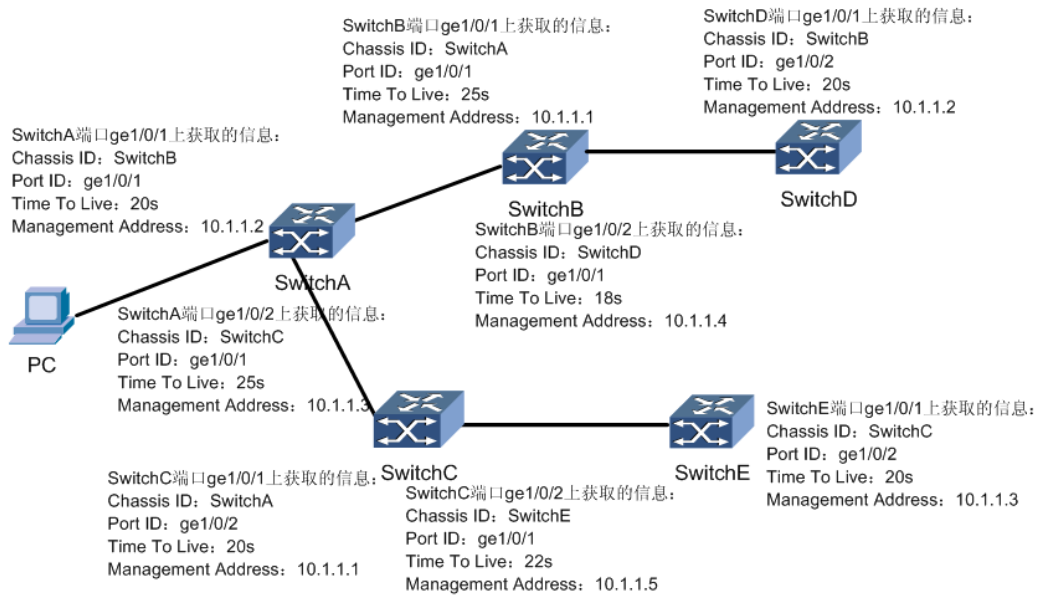


图 10-5 LLDP 配置示意图

### 配置思路

- 在 SC9600 A 设置 LLDP 工作模式为 rx-tx，并配置管理地址为 10.1.1.1。
- 在 SC9600 B 设置 LLDP 工作模式为 rx-tx，并配置管理地址为 10.1.1.2。
- 在 SC9600 C 设置 LLDP 工作模式为 rx-tx，并配置管理地址为 10.1.1.3。
- 在 SC9600 D 设置 LLDP 工作模式为 rx-tx，并配置管理地址为 10.1.1.4。
- 在 SC9600 E 设置 LLDP 工作模式为 rx-tx，并配置管理地址为 10.1.1.5。

### 配置步骤

#### 1、配置 SC9600A。

```
SC9600A(config)#interface gigabitEthernet 1/0/1
SC9600A(config-gigabitEthernet 1/0/1)#no shutdown
SC9600A(config-gigabitEthernet 1/0/1)#lldp admin-status rx-tx
SC9600A(config-gigabitEthernet 1/0/1)#lldp management-address 10.1.1.1 enable
```

#### 2、配置 SC9600B。

```
SC9600B(config)#interface gigabitEthernet 1/0/1
SC9600B(config-gigabitEthernet 1/0/1)#no shutdown
SC9600B(config-gigabitEthernet 1/0/1)#lldp admin-status rx-tx
SC9600B(config-gigabitEthernet 1/0/1)#lldp management-address 10.1.1.2 enable
```

### 3、配置 SC9600C。

```
SC9600C(config)#interface gigabitEthernet 1/0/1
SC9600C(config-gigabitEthernet 1/0/1)#no shutdown
SC9600C(config-gigabitEthernet 1/0/1)#lldp admin-status rx-tx
SC9600C(config-gigabitEthernet 1/0/1)#lldp management-address 10.1.1.3 enable
```

### 4、配置 SC9600D。

```
SC9600D(config)#interface gigabitEthernet 1/0/1
SC9600D(config-gigabitEthernet 1/0/1)#no shutdown
SC9600D(config-gigabitEthernet 1/0/1)#lldp admin-status rx-tx
SC9600D(config-gigabitEthernet 1/0/1)#lldp management-address 10.1.1.4 enable
```

### 5、配置 SC9600E。

```
SC9600E(config)#interface gigabitEthernet 1/0/1
SC9600E(config-gigabitEthernet 1/0/1)#no shutdown
SC9600E(config-gigabitEthernet 1/0/1)#lldp admin-status rx-tx
SC9600E(config-gigabitEthernet 1/0/1)#lldp management-address 10.1.1.5 enable
```

## 10.4 RMON 配置

### 10.4.1 RMON 概述

#### 简介

远程监控（RMON）是一个标准监控规范，它可以使各种网络监控器和控制台系统之间交换网络监控数据。RMON 为网络管理员选择符合特殊网络需求的控制台和网络监控探测器提供了更多的自由。

当前 RMON 有两种版本：RMON v1 和 RMONv2。RMON v1 在目前使用较为广泛的网络硬件中都能发现，它定义了 9 个 MIB 组服务于基本网络监控；RMON v2 是 RMON 的扩展，专注于 MAC 层以上更高的流量层，它主要强调 IP 流量和应用程序层流量。RMON v2 允许网络管理应用程序监控所有网络层的信息包，这与 RMONv1 不同，后者只允许监控 MAC 及其以下层的信息包。



注意：

目前我司设备使用 RMON v1，只实现了 group 1/2/3/9（统计、历史、告警和事件）。

### RMON 的实现方式

RMON 基于简单网络管理协议 SNMP 体系结构实现，与现存 SNMP 框架兼容，包括网管工作站 NMS 和运行在各网络设备上的代理 Agent 两部分。

RMON Agent 跟踪统计网络中的各种流量信息，例如，某段时间内某网段上的报文总数，或发往某台主机的正确报文总数等。它使 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手段。减少了网管站与代理 Agent 间的通讯流量，从而实现更简单有效地管理大型网络。

RMON 允许有多个监控者，它可用两种方法收集数据。

- 通过专用的 RMON Probe（探测仪）。NMS 直接从 RMON Probe 获取管理信息并控制网络资源，这种方式可以获取 RMON MIB 的全部信息。
- 将 RMON Agent 直接嵌入网络设备（例如交换机）中，使它们成为带 RMON Probe 功能的网络设备。NMS 是用 SNMP 基本命令与其交换数据信息，收集网络管理信息。这种方式受设备资源限制，一般无法获取 RMON MIB 的所有数据，大多数只收集四个组（告警、事件、历史和统计）的信息。



注意：

目前我司设备采用 RMON Agent 方式。

### RMON1 MIB 组

RMON1 MIB 组	功能	元素
统计量	包括探测器为该设备每个监控的接口测量的统计值。	数据包丢弃、数据包发送、广播数据包、CRC 错误、大小块、冲突以及计数器的数据包。范围从 64~128、128~256、256~512、512~1024 以及 1024~1518 字节。
历史	定期地收集统计网络值地记录并存储起来以便日后提取。	取样周期、样品数目和项目。提供有关网段流量、错误包、广播包、利用率以及碰撞次数等其他统计信息的历史数据。
告警	定期从探测器的变量选取统计例子。并与前面配的阈值相比较。	告警类型、间隔、阈值上限、阈值下限
主机	包括网络上发现的与每个主机相关的统计值。	主机地址、数据包、接收字节、传输字节、广播传送等。
Host To	准备描述主机的表，根据一	统计值、主机、周期的开始和结束、速率基值、持续

pN	个统计值排序列表。	时间。
真值表	记录关于子网上两个主机之间流量的信息，该信息以矩阵形式存储起来。	源地址和目的地址对、数据包、字节和每一对的错误。
过滤器	允许监视器观测与一过滤器相匹配的数据包。	字节过滤器类型、过滤器表达式等。
捕获包	数据包在流过一个信道之后被捕获。	捕获所有通过过滤器的数据包或简单地记下基于这些数据包的统计。
事件	控制在此处事件的产生和报告。	事件类型、描述、事件最后一个发送的时间
令牌环	支持令牌环	不常使用

### 10.4.2 配置统计表

#### 目的

使用本节操作配置 RMON，可以收集接口流量信息。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置 RMON 统计记录控制	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface { fastethernet   gig Ethernet   xgig Ethernet } interface-number</b> 进入接口配置视图；</li> <li>3. 执行命令 <b>rmon statistics statistics-id [owner]</b> 配置 RMON 统计记录控制；</li> <li>4. 结束。</li> </ol>
删除已配置 RMON 统计记录控制	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface { fastethernet   gig Ethernet   xgig Ethernet } interface-number</b> 进入接口配置视图；</li> <li>3. 执行命令 <b>no rmon statistics statistics-id</b> 删除已配置 RMON 统计记录控制；</li> <li>4. 结束。</li> </ol>

附表：

参数	说明	取值
statistics-id	指定 RMON 统计控制条目 ID	整数形式，取值范围是 1-65535
[owner]	指定请求 RMON 信息的用户（可选参数）	字符串形式
interface-number	指定以太网接口号	SC9600 系列交换机支持以下 3 种型号的接口配置范围：

参数	说明	取值
		SC9603 : 取值范围是 <1-3>/<0-4>/<1-48> SC9608 : 取值范围是 <1-8>/<0-4>/<1-48> SC9612 : 取值范围是 <1-12>/<0-4>/<1-48>

### 10.4.3 配置历史控制表

#### 目的

使用本节操作配置 RMON，可以定期对指定的端口进行数据采集并将采集到的信息保存到历史表中以备查看。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置 RMON 历史记录控制	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface { fastethernet   gig Ethernet   xgig Ethernet } interface-number</b> 进入接口配置视图；</li> <li>3. 执行命令 <b>rmon history history-id sampling-interval sample-number [owner]</b> 配置 RMON 历史记录控制；</li> <li>4. 结束。</li> </ol>
删除已配置 RMON 历史记录控制	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface { fastethernet   gig Ethernet   xgig Ethernet } interface-number</b> 进入接口配置视图；</li> <li>3. 执行命令 <b>no rmon history history-id</b> 删除已配置 RMON 历史记录控制；</li> <li>4. 结束。</li> </ol>

附表：

参数	说明	取值
history-id	指定 RMON 历史记录控制条目 ID	整数形式，取值范围是 1~65535
sampling-interval	指定取样时间间隔	整数形式，取值范围是 1~3600，单位：秒
sample-number	指定保存样例的数量	整数形式，取值范围是 1~65535
[owner]	指定请求 RMON 信息的用户（可选参数）	字符串形式
interface-number	指定以太网接口号	SC9600 系列交换机支持以下 3 种型

参数	说明	取值
		号的接口配置范围： SC9603 : 取值范围是 <1-3>/<0-4>/<1-48> SC9608 : 取值范围是 <1-8>/<0-4>/<1-48> SC9612 : 取值范围是 <1-12>/<0-4>/<1-48>

### 10.4.4 配置告警表

#### 目的

使用本节操作配置 RMON，可以以按照指定的采样间隔对指定的告警变量（用此变量的 OID 指定）进行监视，当被监视数据的值越过定义的阈值时会产生告警事件。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置 RMON 告警条目	1. 执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>rmon alarm alarm-id object-id query-interval { absolute   delta } rising-threshold falling-threshold rising-event falling-event [ owner ]</b> 配置 RMON 告警条目； 3. 结束。
删除已配置 RMON 告警条目	1. 执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>no rmon alarm alarm-id</b> 删除已配置 RMON 告警条目； 3. 结束。

附表：

参数	说明	取值
alarm-id	指定 RMON 告警条目 ID	整数形式，取值范围是 1~65535
object-id	指定告警对象 ID（只有可以解析为 ASN.1 中 INTEGER 的数据类型的变量才能作为告警对象的 ID）	字符串形式，格式为节点 OID 的点分格式，如 1.3.6.1.2.1.2.2.1.8.2
query-interval	指定告警查询时间间隔	整数形式，取值范围是 2~2000000，单位：秒
{ absolute   delta }	表示绝对值或相对值（增量值）	-
rising-threshold	指定上升阈值	整数形式，取值范围是 0~4294967295
falling-threshold	指定下降阈值	整数形式，取值范围是 0~65535

参数	说明	取值
rising-event	指定上升事件条目号	整数形式，取值范围是 0~4294967295
falling-event	指定下降时间条目号	整数形式，取值范围是 0~65535
[owner]	定义 RMON 告警的用户（可选参数）	字符串形式，取值范围是 0~127 个字符

### 10.4.5 配置事件表

#### 目的

使用本节操作配置 RMON，当事件超过告警阈值时，设备可以记录日志或者产生告警，或者同时记录日志和产生告警。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置 RMON 事件控制条目	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>rmon event event-id { log   trap   both } [ description ]</b> 配置 RMON 事件控制条目；</li> <li>3. 结束。</li> </ol>
删除已配置 RMON 事件控制条目	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>no rmon event event-id</b> 删除已配置 RMON 事件控制条目；</li> <li>3. 结束。</li> </ol>

附表：

参数	说明	取值
event-id	指定 RMON 事件控制条目 ID	整数形式，取值范围是 1~65535
{ log   trap   both }	指定事件的类型 log: 产生事件的日志 trap: 产生事件的告警 both: 同时产生事件日志和告警	-
[description]	指定事件的描述信息（可选参数）	字符串形式

### 10.4.6 维护及调试

#### 目的

当 RMON 功能不正常，需要进行查看、调试或定位问题时，可以使用本小节操作。

#### 过程



根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
查看 RMON 告警控制条目的配置信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gigasethernet   xgigasethernet } interface-number</b> 进入接口配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show rmon alarm</b>；</li> <li>3. 结束。</li> </ol>
查看 RMON 事件的配置信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gigasethernet   xgigasethernet } interface-number</b> 进入接口配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show rmon config</b>；</li> <li>3. 结束。</li> </ol>
查看 RMON 事件控制条目的配置信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gigasethernet   xgigasethernet } interface-number</b> 进入接口配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show rmon event</b>；</li> <li>3. 结束。</li> </ol>
查看 RMON 历史控制条目的配置信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gigasethernet   xgigasethernet } interface-number</b> 进入接口配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show rmon history [ history-id ]</b>；</li> <li>3. 结束。</li> </ol>
查看 RMON 历史记录控制条目的统计信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gigasethernet   xgigasethernet } interface-number</b> 进入接口配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show rmon history statistics</b>；</li> <li>3. 结束。</li> </ol>
查看 RMON 事件的日志信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gigasethernet   xgigasethernet } interface-number</b> 进入接口配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show rmon log</b>；</li> <li>3. 结束。</li> </ol>
查看 RMON 统计表信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface { fastethernet   gigasethernet   xgigasethernet } interface-number</b> 进入接口配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show rmon statistics</b>；</li> <li>3. 结束。</li> </ol>

附表：

参数	说明	取值
----	----	----

参数	说明	取值
interface-number	指定以太网接口号	SC9600 系列交换机支持以下 3 种型号的接口配置范围： SC9603 : 取值范围是 <1-3>/<0-4>/<1-48> SC9608 : 取值范围是 <1-8>/<0-4>/<1-48> SC9612 : 取值范围是 <1-12>/<0-4>/<1-48>
history-id	指定 RMON 历史记录控制条目 ID	整数形式，取值范围是 1~65535

### 10.4.7 配置举例

#### 组网要求

现通过 SC9600 端口 Ge1/0/2 对其连接的子网进行监控，包括：流量和各种类型包数据量的实时和历史统计信息；对此接口流量的字节数设置告警监控，超过设定值时记录日志；对超过告警设置值主动向 NMS 上报告警信息。

#### 组网图

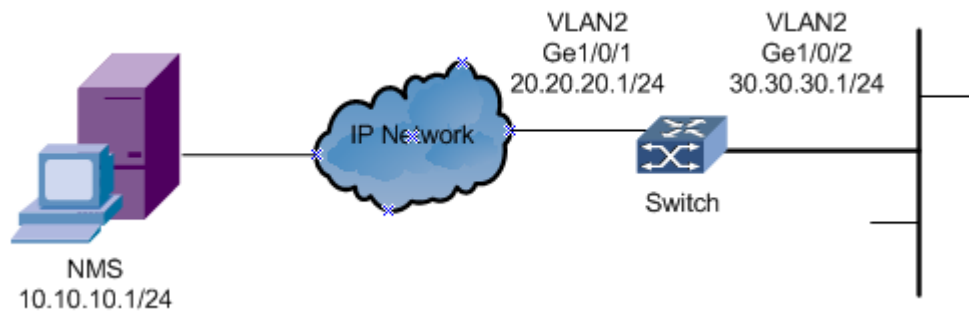


图 10-6 RMON 配置示意图

#### 前提配置

1. 配置好 SC9600 的接口 Ge1/0/1 和 Ge1/0/2 的 IP 地址；
2. 配置好 SC9600 和 NMS 路由可达；
3. 配置好 SC9600 的 SNMP。

#### 配置步骤

1、配置 SC9600 统计表。

```
SC9600#configure
SC9600(config)#interface gigabitEthernet 1/0/2
SC9600(config-gigabitEthernet1/0/2)#rmon statistics 1
SC9600(config-gigabitEthernet1/0/2)#
```

2、配置 SC9600 历史控制表。

```
SC9600(config-gigabitEthernet1/0/2)#rmon history 1 10 30
SC9600(config-gigabitEthernet1/0/2)#quit
SC9600(config)#
```

3、配置 SC9600 告警表。

```
SC9600(config)#rmon alarm 1 1.3.6.1.2.1.2.2.1.8.2 2 absolute 1 1 2 1
SC9600(config)#
```

4、配置 SC9600 事件表。

```
SC9600(config)#rmon event 1 both CLI
SC9600(config)#
```

## 10.5 NTP 配置

### 10.5.1 NTP 概述

Network Time Protocol (NTP) 为交换机提供网络时钟同步功能，该功能包括 NTP 服务器和 NTP 客户端。通过配置 NTP，可以保持网络中设备的时钟运行一致。

#### NTP 协议支持的四种运行模式

- 单播模式

在该模式下，进行如下的处理：**unicast** 的 **client** 周期性的发送 NTP 请求报文到 **server**，并且期望从 **server** 得到请求答复报文；**client** 在收到 **server** 服务器回应报文后，根据 **server** 和 **client** 的往返传播延迟计算本地时钟补偿；**client** 根据 **server** 的时间以及往返传播延迟计算的本地时钟补偿的关系进行时间计算并设置为本地时间。**server** 等待 **client** 端周期性发送的请求，根据接收到请求消息的地址构造请求消息应答报文并发送，**server** 不会自动的周期性的发送通告报文。

- 对等体模式

对等体模式下，主动对等体和被动对等体可以互相同步，等级低（层数大）的对等体向等级高（层数小）的对等体同步。主动对等体向被动对等体发送同步请求报文，报文中的 **Mode** 字段设置为 **1**（主动对等体）。被动对等体收到请求报文后，自动工作在被动对等体模式，并发送应答报文，报文中的 **Mode** 字段设置为 **2**（被动对等体）。

- 组播模式

客户端侦听来自服务器的组播消息包；当客户端接收到第一个组播消息包后，为估计网络延迟，客户端先启用一个短暂的服务器/客户端模式与远程服务器交换消息；客户端进入组播客户端模式，继续侦听组播消息包的到来，根据到来的组播消息包对本地时钟进行同步。对于 **IPv4** 的服务器端周期性向组播目的地址 **224.0.1.1** 发送时钟同步报文；对于 **IPv6** 的服务器端周期性向组播目的地址以 **0xFF02** 开头，**0x65** 结尾，发送时钟同步报文。

- 广播模式

客户端侦听来自服务器的广播消息包。客户端接收到第一个广播消息包后，为估计网络延迟，客户端先启用一个短暂的服务器/客户端模式与远程服务器交换消息。客户端进入广播客户模式，继续侦听广播消息包的到来，根据到来的广播消息包对本地时钟进行同步。对于 **IPv6** 的服务器端周期性向组播目的地址以 **0xFF02** 开头，**0x65** 结尾，发送时钟同步报文；对于 **IPv4** 的服务器端周期性向广播地址 **255.255.255.255** 或子网广播地址发送时钟同步报文。

### NTP 的优点

- 支持采用单播、组播或广播方式发送协议报文。
- 支持 MD5 验证。
- 采用分层（Stratum）的方法来定义时钟的准确性，可以迅速同步网络中各台设备的时间。

## 10.5.2 配置 NTP 基本功能

### 目的

使用本节操作配置 NTP 基本功能，用户可以了解到如何配置 NTP 的工作模式。

### 前提配置

配置网络中设备链路层协议、网络层 IP 地址或路由协议，保证设备间 NTP 报文可达。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
指定设备为主时钟	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>ntp</b> 进入 NTP 配置视图；</li> <li>3. 执行命令 <b>master</b> 指定设备为主时钟；</li> <li>4. 结束。</li> </ol>
配置 NTP 层级	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>ntp</b> 进入 NTP 配置视图；</li> <li>3. 执行命令 <b>stratum { layer-number   default }</b>指定 NTP 层级，服务器端（主时钟）配置的层数一定要小于客户端所在的层数，否则客户端无法同步服务器端的时钟；</li> <li>4. 结束。</li> </ol>
配置 NTP 单播模式	<p>配置 NTP 客户端（指定单播 NTP 服务器后，本地交换机自动工作在客户端模式。其中步骤 3 和步骤 4，用户根据实际情况选用）：</p> <ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>ntp</b> 进入 NTP 配置视图；</li> <li>3. （IPv4）执行命令 <b>ntp unicast-server ipv4-address</b> 或 <b>ntp unicast-server ipv4-address version { 1   2   3   4 }</b>或 <b>ntp unicast-server vpn-instance vpn-instance-name</b> 或 <b>ntp unicast-server ipv4-address version { 1   2   3   4 } vpn-instance vpn-instance-name</b>；</li> <li>4. （IPv6）执行命令 <b>ntp6 unicast-server ipv6-address</b> 或 <b>ntp6 unicast-server ipv6-address version { 1   2   3   4 }</b>或 <b>ntp6 unicast-server vpn-instance vpn-instance-name</b> 或 <b>ntp6 unicast-server ipv6-address version { 1   2   3   4 } vpn-instance vpn-instance-name</b>；</li> <li>5. 结束。</li> </ol> <p>配置 NTP 服务器端： 服务器端除配置 NTP 主时钟外，不需要专门配置。</p>
配置 NTP 广播模式（适用于局域网）	<p>配置 NTP 广播客户端：</p> <ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface vlan vlan-id</b> 进入 VLANIF 配置视图；</li> <li>3. （IPv4）执行命令 <b>ntp broadcast-client</b> 或 <b>ntp broadcast-client ipv4-address</b>；</li> <li>4. 结束。</li> </ol> <p>配置 NTP 广播服务器端：</p> <ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface vlan vlan-id</b> 进入 VLANIF 配置视图；</li> <li>3. （IPv4）执行命令 <b>ntp broadcast-server</b> 或 <b>ntp broadcast-server ipv4-address</b> 或 <b>ntp broadcast-server version { 1   2   3   4 }</b>或 <b>ntp broadcast-server version { 1   2   3   4 } ipv4-address</b>；</li> </ol>

目的	步骤
	4. 结束。
配置 NTP 组播模式	<p>配置 NTP 组播客户端：</p> <ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface vlan <i>vlan-id</i></b> 进入 VLANIF 配置视图；</li> <li>3. （IPv4）执行命令 <b>ntp multicast-client</b> 或 <b>ntp multicast-client <i>ipv4-address</i></b>；</li> <li>4. （IPv6）执行命令 <b>ntp6 multicast-client</b> 或 <b>ntp6 multicast-client <i>ipv6-address</i></b>；</li> <li>5. 结束。</li> </ol> <p>配置 NTP 组播服务器端：</p> <ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface vlan <i>vlan-id</i></b> 进入 VLANIF 配置视图；</li> <li>3. （IPv4）执行命令 <b>ntp multicast-server</b> 或 <b>ntp multicast-server <i>ipv4-address</i></b> 或 <b>ntp multicast-server version { 1   2   3   4 }</b> 或 <b>ntp multicast-server version { 1   2   3   4 } <i>ipv4-address</i></b> 或 <b>ntp multicast-server ttl <i>ttl-value</i></b> 或 <b>ntp multicast-server ttl <i>ttl-value</i> <i>ipv4-address</i></b> 或 <b>ntp multicast-server version { 1   2   3   4 } ttl <i>ttl-value</i></b> 或 <b>ntp multicast-server version { 1   2   3   4 } ttl <i>ttl-value</i> <i>ipv4-address</i></b>；</li> <li>4. （IPv6）执行命令 <b>ntp6 multicast-server</b> 或 <b>ntp6 multicast-server <i>ipv6-address</i></b> 或 <b>ntp6 multicast-server version { 1   2   3   4 }</b> 或 <b>ntp6 multicast-server version { 1   2   3   4 } <i>ipv6-address</i></b> 或 <b>ntp6 multicast-server ttl <i>ttl-value</i></b> 或 <b>ntp6 multicast-server ttl <i>ttl-value</i> <i>ipv6-address</i></b> 或 <b>ntp6 multicast-server version { 1   2   3   4 } ttl <i>ttl-value</i></b> 或 <b>ntp6 multicast-server version { 1   2   3   4 } ttl <i>ttl-value</i> <i>ipv6-address</i></b>；</li> <li>5. 结束。</li> </ol>
配置 NTP 对等体模式	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>ntp</b> 进入 NTP 配置视图；</li> <li>3. （IPv4）执行命令 <b>ntp unicast-peer <i>ipv4-address</i></b> 或 <b>ntp unicast-peer <i>ipv4-address</i> version { 1   2   3   4 }</b> 或 <b>ntp unicast-peer <i>ipv4-address</i> vpn-instance <i>vpn-instance-name</i></b> 或 <b>ntp unicast-peer <i>ipv4-address</i> version { 1   2   3   4 } vpn-instance <i>vpn-instance-name</i></b>；</li> <li>4. （IPv6）执行命令 <b>ntp6 unicast-peer <i>ipv6-address</i></b> 或 <b>ntp6 unicast-peer <i>ipv6-address</i> version { 1   2   3   4 }</b> 或 <b>ntp6 unicast-peer <i>ipv6-address</i> vpn-instance <i>vpn-instance-name</i></b> 或 <b>ntp6 unicast-peer <i>ipv6-address</i> version { 1   2   3   4 } vpn-instance <i>vpn-instance-name</i></b>；</li> <li>5. 结束。</li> </ol>
配置 NTP 客户端更新间隔	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>ntp</b> 进入 NTP 配置视图；</li> <li>3. 执行命令 <b>client update-interval { <i>update-interval-time</i>   default }</b>；</li> <li>4. 结束。</li> </ol>

目的	步骤
配置 NTP 服务器端的广播间隔	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>ntp</b> 进入 NTP 配置视图;</li> <li>3. 执行命令 <b>server broadcast -interval {interval  default}</b>;</li> <li>4. 结束。</li> </ol>

附表:

参数	说明	取值
update-interval-time	NTP 客户端更新间隔	整数形式, 取值范围是 4~17, 2 的 n 次方秒
default	NTP 客户端更新间隔默认值	字符串形式
vlan-id	VLAN ID	整数形式, 取值范围是 1~4094
interval	ntp server 通告时间	整数形式, 取值范围是 4-17, 单位: 秒
ipv4-address	广播或单播 IP 地址	默认值是 255.255.255.0
ipv4-address	组播 IP 地址	点分十进制, 默认值是 224.0.1.1
ipv6-address	组播或单播 IPV6 地址	默认值是 ff02:: 65
version {1   2   3   4}	指定 NTP 协议版本	默认值是 3
tll-value	组播包的生存期	整数, 取值范围是 1-255 默认值是 8
vpn-instance-name	VPN 实例名称	字符串, 最大长度为 30

### 10.5.3 配置 NTP 安全机制

#### 目的

使用本节操作配置 NTP 安全机制, 在对安全性要求比较高的网络中, 可以实现可靠的时钟同步。

#### 过程

根据不同目的, 执行相应步骤, 具体参见下表。

目的	步骤
全局使能或去使能 MD5 认证功能	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>ntp</b> 进入 NTP 配置视图;</li> <li>3. 执行命令 <b>authentication { enable   disable }</b>;</li> <li>4. 结束。</li> </ol>
配置一条 NTP 验证密钥	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>ntp</b> 进入 NTP 配置视图;</li> <li>3. 执行命令 <b>authentication-keyid key-id md5 key key-string</b>;</li> <li>4. 结束。</li> </ol>
使能或者	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> </ol>

目的	步骤
禁止信任一条 MD5 认证密钥	<ol style="list-style-type: none"> <li>2. 执行命令 <b>ntp</b> 进入 NTP 配置视图;</li> <li>3. 执行命令 <b>trusted-keyid trusted-keyid time { enable   disable };</b></li> <li>4. 结束。</li> </ol>
配置 NTP 单播模式的验证	<p>配置 NTP 客户端(指定单播 NTP 服务器后,本地交换机自动工作在客户端模式。其中步骤 3 和步骤 4,用户根据实际情况选用):</p> <ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>ntp</b> 进入 NTP 配置视图;</li> <li>3. (IPv4) 执行命令 <b>ntp unicast-server ipv4-address version { 1   2   3   4 } authentication-keyid key-id</b> 或 <b>ntp unicast-server ipv4-address authentication-keyid key-id</b> 或 <b>ntp unicast-server ipv4-address version { 1   2   3   4 } authentication-keyid key-id vpn-instance vpn-instance-name</b> 或 <b>ntp unicast-server ipv4-address authentication-keyid key-id vpn-instance vpn-instance-name;</b></li> <li>4. (IPv6) 执行命令 <b>ntp6 unicast-server ipv6-address version { 1   2   3   4 } authentication-keyid key-id</b> 或 <b>ntp6 unicast-server ipv6-address authentication-keyid key-id</b> 或 <b>ntp6 unicast-server ipv6-address version { 1   2   3   4 } authentication-keyid key-id vpn-instance vpn-instance-name</b> 或 <b>ntp6 unicast-server ipv6-address authentication-keyid key-id vpn-instance vpn-instance-name;</b></li> <li>5. 结束。</li> </ol> <p>配置 NTP 服务器端: 服务器端除配置 NTP 主时钟外,不需要专门配置。</p>
配置 NTP 广播模式的验证(适用于局域网)	<p>配置 NTP 广播客户端:</p> <ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>interface vlan vlan-id</b> 进入 VLANIF 配置视图;</li> <li>3. (IPv4) 执行命令 <b>ntp broadcast-client authentication-keyid key-id</b> 或 <b>ntp broadcast-client authentication-keyid key-id ipv4-address;</b></li> <li>4. 结束。</li> </ol> <p>配置 NTP 广播服务器端:</p> <ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>interface vlan vlan-id</b> 进入 VLANIF 配置视图;</li> <li>3. (IPv4) 执行命令 <b>ntp broadcast-server authentication-keyid keyid</b> 或 <b>ntp broadcast-server authentication-keyid key-id ipv4-address</b> 或 <b>ntp broadcast-server authentication-keyid key-id version { 1   2   3   4 }</b> 或 <b>ntp broadcast-server authentication-keyid key-id version { 1   2   3   4 } ipv4-address;</b></li> <li>4. 结束。</li> </ol>
配置 NTP 组播模式的验证	<p>配置 NTP 组播客户端:</p> <ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>interface vlan vlan-id</b> 进入 VLANIF 配置视图;</li> </ol>



目的	步骤
	<p>3. (IPv4) 执行命令 <b>ntp multicast-client authentication-keyid key-id</b> 或 <b>ntp multicast-client authentication-keyid key-id ipv4-address</b>;</p> <p>4. (IPv6) 执行命令 <b>ntp6 multicast-client authentication-keyid key-id</b> 或 <b>ntp6 multicast-client authentication-keyid key-id ipv6-address</b>;</p> <p>5. 结束。</p>
	<p>配置 NTP 组播服务器端:</p> <p>1. 执行命令 <b>configure</b> 进入全局配置视图;</p> <p>2. 执行命令 <b>interface vlan vlan-id</b> 进入 VLANIF 配置视图;</p> <p>3. (IPv4) 执行命令 <b>ntp multicast-server authentication-keyid key-id</b> 或 <b>ntp multicast-server authentication-keyid key-id ipv4-address</b> 或 <b>ntp multicast-server authentication-keyid key-id version { 1   2   3   4 } ttl ttl-value</b> 或 <b>ntp multicast-server authentication-keyid key-id version { 1   2   3   4 } ttl ttl-value ipv4-address</b>;</p> <p>4. (IPv6) 执行命令 <b>ntp6 multicast-server authentication-keyid key-id</b> 或 <b>ntp6 multicast-server authentication-keyid key-id ipv6-address</b> 或 <b>ntp6 multicast-server authentication-keyid key-id version { 1   2   3   4 } ttl ttl-value</b> 或 <b>ntp6 multicast-server authentication-keyid key-id version { 1   2   3   4 } ttl ttl-value ipv6-address</b>;</p> <p>5. 结束。</p>
配置 NTP 对等体模式的验证	<p>1. 执行命令 <b>configure</b> 进入全局配置视图;</p> <p>2. 执行命令 <b>ntp</b> 进入 NTP 配置视图;</p> <p>3. (IPv4) 执行命令 <b>ntp unicast-peer ipv4-address version { 1   2   3   4 } authentication-keyid key-id</b> 或 <b>ntp unicast-peer ipv4-address authentication-keyid key-id</b> 或 <b>ntp unicast-peer ipv4-address version { 1   2   3   4 } authentication-keyid key-id vpn-instance vpn-instance-name</b> 或 <b>ntp unicast-peer ipv4-address authentication-keyid key-id vpn-instance vpn-instance-name</b>;</p> <p>4. (IPv6) 执行命令 <b>ntp6 unicast-peer ipv6-address version { 1   2   3   4 } authentication-keyid key-id</b> 或 <b>ntp6 unicast-peer ipv6-address authentication-keyid key-id</b> 或 <b>ntp6 unicast-peer ipv6-address version { 1   2   3   4 } authentication-keyid key-id vpn-instance vpn-instance-name</b> 或 <b>ntp6 unicast-peer ipv6-address authentication-keyid key-id vpn-instance vpn-instance-name</b>;</p> <p>5. 结束。</p>

附表:

参数	说明	取值
vlan-id	VLAN ID	整数形式, 取值范围是 1~4094
ipv4-address	广播或单播 IP 地址	默认值是 255.255.255.0
ipv4-address	组播 IP 地址	点分十进制, 默认值是 224.0.1.1

参数	说明	取值
<code>ipv6-address</code>	组播或单播 IPV 6 地址	默认值是 ff02:: 65
<code>version {1   2   3   4}</code>	指定 NTP 协议版本	默认值是 3
<code>tll-value</code>	组播包的生存期	整数，取值范围是 1-255 默认值是 8
<code>vpn-instance-name</code>	VPN 实例名称	字符串，最大长度为 30
<code>key-id</code>	密钥 ID	整数形式，取值范围是 1~4294967295
<code>key-string</code>	密钥字	字符串形式，小于 16 个字符
<code>trusted-keyid time</code>	MD5 认证密钥	整数形式，取值范围是 1~ 4294967295

## 10.5.4 维护及调试

### 目的

当 NTP 功能不正常，需要进行查看、调试或定位问题时，可以使用本小节操作。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
打开 NTP 协议调试功能	<ol style="list-style-type: none"> <li>1. 不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>debug ntp { error   pkt   warning   event   auth   all }</b>；</li> <li>3. 结束。</li> </ol>
关闭 NTP 协议调试功能	<ol style="list-style-type: none"> <li>1. 不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>no debug ntp { error   pkt   warning   event   auth   all }</b>；</li> <li>3. 结束。</li> </ol>
查看 NTP 全局配置信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>vlan <i>vlan-id</i></b> 进入 VLAN 配置视图，或执行命令 <b>ntp</b> 进入 NTP 配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show ntp</b>；</li> <li>3. 结束。</li> </ol>
查看 NTP 服务信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>vlan <i>vlan-id</i></b> 进入 VLAN 配置视图，或执行命令 <b>ntp</b> 进入 NTP 配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show ntp service</b>；</li> <li>3. 结束。</li> </ol>
查看 NTP 服务详细配置信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>vlan <i>vlan-id</i></b> 进入 VLAN 配置视图，或执行命令 <b>ntp</b> 进入 NTP 配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show ntp service verbose</b>；</li> <li>3. 结束。</li> </ol>

附表：

参数	说明	取值
vlan-id	VLAN ID	整数形式，取值范围是 1~4094

### 10.5.5 配置举例

#### 组网要求

NTP 协议是典型的工作在 Server-Client 模式下的协议，Client 与 Server 相连，Client 从 Server 处获得当前的时间。

#### 组网图

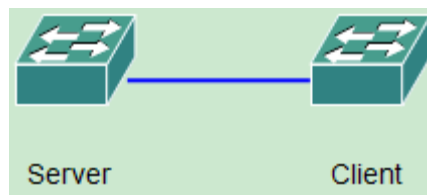


图 10-7 NTP 配置示意图

#### 配置步骤

步骤 1：（略）配置 NTP 服务器和客户端的 VLAN 和接口，使服务器和客户端之间能够 ping 通。

步骤 2：配置 NTP 服务器为主时钟和层数

```
Server(config-ntp)#master
```

```
Server(config-ntp)#stratum 2
```

步骤 3：配置 NTP 客户端的层数

```
Client(config-ntp)#stratum 9
```

步骤 4：配置 NTP 客户端的模式和 IP 地址（单播模式）

```
Client(config-ntp)#ntp unicast-server A.B.C.D（服务器的 IP 地址）
```



注意：

其他模式类似配置步骤，不同在于多播和广播模式需要在服务器上指定模式。

## 10.6 SMTP 配置

### 10.6.1 SMTP 简介

SMTP（Simple Mail Transfer Protocol）即简单邮件传输协议，它是一组用于由源地址到目的地址传送邮件的规则，由它来控制信件的中转方式。SMTP 协议属于 TCP/IP 协议族，它帮助每台计算机在发送或中转信件时找到下一个目的地。通过 SMTP 协议所指定的服务器，就可以把 E-mail 寄到收信人的服务器上了，整个过程只要几分钟。SMTP 服务器则是遵循 SMTP 协议的发送邮件服务器，用来发送或中转发出的电子邮件。

### 10.6.2 配置 SMTP

#### 10.6.2.1 配置 SMTP 邮件服务器

##### 目的

配置本命令后，配合日志功能，日志记录可以发送到 SMTP 邮件服务器上方便用户进行查看相关信息。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
设置 SMTP 邮件服务器	1. 执行命令 <code>configure</code> 2. 执行命令 <code>smtp mailbox email-address smtpserver-ipaddress [ server-port ]</code> 或执行命令 <code>smtp mailbox email-address smtpserver-ipaddress [ server-port ] authentication user password</code> 或执行命令 <code>smtp mailto email-address mailbox smtp-mailaddress</code>	<b>email-address</b> : 指定邮箱地址，形如***@***.com.cn <b>smtpserver-ipaddress</b> : 指定邮件服务器 IPv4 地址或 IPv6，点分十进制 <b>[ server-port ]</b> : 指定邮件服务器端口号，整数形式，取值范围是 1-65535 <b>user</b> : 指定邮件服务器用户名，字符串形式
（可选）删除已配置 SMTP 邮件服务器	1. 执行命令 <code>configure</code> 2. 执行命令 <code>no smtp mailbox email-address</code> 或执行命令 <code>no smtp mailto email-address mailbox smtp-mailaddress</code>	<b>password</b> : 指定密码，字符串形式 <b>smtp-mailaddress</b> : 指定邮件服务器 IPv4 地址或 IPv6，点分十进制

### 10.6.2.2 查看 SMTP 配置信息

#### 目的

当用户配置完成 SMTP 功能及其相关参数后，若需要查看配置是否正确，可使用本节介绍的操作查看相关信息。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
查看 SMTP 配置信息	<ol style="list-style-type: none"> <li>1. 启动设备，输入用户名及密码后进入特权用户视图或执行命令 <code>disable</code> 退出到普通用户视图</li> <li>2. 执行命令 <code>show smtp config</code> 或执行命令 <code>show smtp mailbox</code> 或执行命令 <code>show smtp mailto</code></li> </ol>	-

### 10.6.2.3 调试 SMTP 功能

#### 目的

当 SMTP 功能出现异常或不能正确转发邮件时，可以使用本节命令打开 SMTP 调试功能。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
打开 SMTP 调试功能	<ol style="list-style-type: none"> <li>1. 启动设备，输入用户名及密码后进入特权用户视图</li> <li>2. 执行命令 <code>debug smtp</code></li> </ol>	-
关闭 SMTP 调试功能	<ol style="list-style-type: none"> <li>1. 启动设备，输入用户名及密码后进入特权用户视图</li> <li>2. 执行命令 <code>no debug smtp</code></li> </ol>	

## 10.7 CPU 调试配置

### 10.7.1 CPU 调试概述

用户使用设备的 CPU 调试功能，可以查看 CPU 收发包详细信息。该功能可以供用户在设备出现问题时，调试设备使用。

### 10.7.2 维护及调试

#### 目的

当设备功能不正常，用户需要查看设备送往 CPU 的数据包时，可以使用本小节操作。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
调试设置 CPU 收发包的抓包时间	<ol style="list-style-type: none"> <li>1. 不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>debug cpupkt interface { gigasetherne   xgigasetherne } interface-number capture begin time time</b> 或 <b>debug cpupkt interface { mc   lc   outband } capture begin time time</b>;</li> <li>3. 结束。</li> </ol>
停止调试 CPU 抓包	<ol style="list-style-type: none"> <li>1. 不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>debug cpupkt interface { gigasetherne   xgigasetherne } interface-number capture stop</b> 或 <b>debug cpupkt interface { mc   lc   outband } capture stop</b>;</li> <li>3. 结束。</li> </ol>
开启 CPU 收发包的调试功能	<ol style="list-style-type: none"> <li>1. 不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>debug cpupkt interface { fastetherne   gigasetherne   xgigasetherne } interface-number { loopback   sgm   dot3ah   lacp   dot1x   cfm   y1731   g8032   g8031   eaps   dcp   ha   spanningtree   rer   other   arp   ip   ospf   igmp   icmp   udp   dhcp   tcp   alltype   bfd-eth   vrrpv2   bfd-ip   udp6   tcp6   bfd-ipv6   vrrpv3 } { in   out   all   capture }</b> 或 <b>debug cpupkt interface { mc   lc   outband } { loopback   sgm   dot3ah   lacp   dot1x   cfm   y1731   g8032   g8031   eaps   dcp   ha   spanningtree   rer   other   arp   ip   ospf   igmp   icmp   udp   dhcp   tcp   alltype   bfd-eth   vrrpv2   bfd-ip   udp6   tcp6   bfd-ipv6   vrrpv3 } { in   out   all   capture }</b>;</li> <li>3. 结束。</li> </ol>
关闭 CPU 收发包的调试功能	<ol style="list-style-type: none"> <li>1. 不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>no debug cpupkt interface { fastetherne   gigasetherne   xgigasetherne } interface-number { loopback   sgm   dot3ah   lacp   dot1x   cfm   y1731   g8032   g8031   eaps   dcp   ha   spanningtree   rer   other   arp   ip   ospf   igmp   icmp   udp   dhcp   tcp   alltype   bfd-eth   vrrpv2   bfd-ip   udp6   tcp6   bfd-ipv6   vrrpv3 } { in   out   all   capture }</b> 或 <b>no debug cpupkt interface { mc   lc   outband } { loopback   sgm   dot3ah   lacp   dot1x   cfm   y1731   g8032   g8031   eaps   dcp   ha   spanningtree   rer   other   arp   ip   ospf   igmp   icmp   udp   dhcp   tcp   alltype   bfd-eth   vrrpv2   bfd-ip   udp6   tcp6   bfd-ipv6   vrrpv3 } { in   out   all   capture }</b>;</li> <li>3. 结束。</li> </ol>
查看 CPU 收发包的接口统计信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或不执行任何命令保持当前特权用户视图；</li> <li>2. 执行命令 <b>show cpupkt interface { fastetherne   gigasetherne  </b></li> </ol>

目的	步骤
	<p><code>xgigaethernet } interface-number { loopback   sgm   dot3ah   lacp   dot1x   cfm   y1731   g8032   g8031   eaps   dcp   ha   spanningtree   rer   other   arp   ip   ospf   igmp   icmp   udp   dhcp   tcp   alltype   bfd-eth   vrrpv2   bfd-ip   udp6   tcp6   bfd-ipv6   vrrpv3 } statistic</code> 或 <code>show cpupkt interface { mc   lc   outband } { loopback   sgm   dot3ah   lacp   dot1x   cfm   y1731   g8032   g8031   eaps   dcp   ha   spanningtree   rer   other   arp   ip   ospf   igmp   icmp   udp   dhcp   tcp   alltype   bfd-eth   vrrpv2   bfd-ip   udp6   tcp6   bfd-ipv6   vrrpv3 } statistic;</code></p> <p>3. 结束。</p>

附表:

参数	说明	取值
interface-number	以太网端口号	SC9600 系列交换机支持以下 3 种型号的接口配置范围: SC9603: 取值范围是<1-3>/<0-4>/<1-48> SC9608: 取值范围是<1-8>/<0-4>/<1-48> SC9612: 取值范围是<1-12>/<0-4>/<1-48>
mc	到另一块主控的接口	-
lc	到线卡的接口	-
outband	到带外	-
time	抓包时间	整数形式, 取值范围是 1-3600。

## 10.8 ISS 堆叠配置

### 10.8.1 堆叠简介

ISS 协议具有以下主要特点:

- 强大的网络扩展能力。通过增加成员设备, 可以轻松自如的扩展堆叠系统的端口数、带宽和处
- 理能力。
- 保护用户投资。由于具有强大的扩展能力, 当用户进行网络升级时, 不需要替换掉原有设备, 只需要增加新设备既可。很好的保护了用户投资。
- 低成本: ISS 技术可以将一些较低端的设备虚拟成为一个相对高端的设备使用, 从而具有高端设备的端口密度和带宽, 以及低端设备的成本。

- 简化管理。堆叠系统形成之后，用户通过任意成员设备的任意端口均可以登录 IRF 系统，对 IRF 内所有成员设备进行统一管理。而不用物理连接到每台成员设备上分别对它们进行配置和管理。
- 简化网络运行。ISS 形成的虚拟设备中运行的各种控制协议也是作为单一设备统一运行的，例如路由协议会作为单一设备统一计算。这样省去了设备间大量协议报文的交互，简化了网络运行，缩短了网络动荡时的收敛时间。
- 高可靠性。ISS 系统由多台成员设备组成，Slave 设备在作为备份的同时也可以处理业务，一旦 Master 设备故障，系统会迅速自动选举新的 Master，以保证通过系统的业务不中断，从而实现了设备的 1:N 备份。

## 10.8.2 配置堆叠

### 目的

用户可以通过本节操作对堆叠进行配置。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
配置设备的运行模式	<ol style="list-style-type: none"> <li>1. 保持在当前特权用户视图下；；</li> <li>2. 执行命令 <code>iss mode {independent iss}</code>；</li> <li>3. 结束。</li> </ol>	<p><code>independent</code>: 独立运行模式</p> <p><code>iss</code>: 堆叠模式</p>
<p>配置堆叠域 ID</p> <p>如果用户不配置，协议初始化时，默认会赋值。</p> <p>堆叠域 ID 配置成功以后，如果是堆叠模式，则下次重启才能生效；如果是独立模式，</p> <p>则切换到堆叠模式以后才能生效</p>	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>iss domain &lt;1-8&gt;</code>；</li> <li>3. 结束。</li> </ol>	堆叠域 ID 值，整数形式，取值范围是 1-8
<p>配置设备的堆叠成员编号</p> <p>必须先配置成员编号，才能从独立模式切换到堆叠模式。</p> <p>堆叠成员 ID 配置成功以后，如果是堆叠模式，则</p>	<ol style="list-style-type: none"> <li>1. 执行命令 <code>configure</code> 进入全局配置视图；</li> <li>2. 执行命令 <code>iss member &lt;1-8&gt;</code>；</li> <li>3. 结束。</li> </ol>	堆叠成员编号，整数形式，取值范围是 1-8



目的	步骤	参数说明
下次重启才能生效；如果是独立模式， 则切换到堆叠模式以后才能生效。		
配置设备的堆叠优先级 全局配置视图下配置。必须先配置成员编号，才能从独立模式切换到堆叠模式。 堆叠成员 ID 配置成功以后，如果是堆叠模式，则下次重启才能生效；如果是独立模式， 则切换到堆叠模式以后才能生效。	1. 执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>iss priority &lt;1-8&gt;</b> ； 3. 结束。	堆叠成员编号，整数形式，取值范围是 1-8
配置设备指定的 Master 必须先配置成员编号，才能从独立模式切换到堆叠模式。	1. 执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>iss master</b> ； 3. 结束。	-
配置 hello 报文发送间隔	1. 执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>iss hello-interval (&lt;1-10&gt; default)</b> ； 3. 结束。	整数取值，取值范围 1-10，单位：秒
配置 hello 报文发送间隔	1. 执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>erase iss-config</b> ； 3. 结束。	整数取值，取值范围 1-10，单位：秒
创建堆叠组	1. 执行命令 <b>configure</b> 进入全局配置视图； 2. 执行如下命令： <b>interface iss-trunk iss-group-id1</b> （独立模式时） <b>interface iss-trunk iss-group-id2</b> （堆叠模式时） 3. 结束。	<b>iss-group-id1</b> 堆叠组 ID1 整数型是，取值范围<1-1> <b>iss-group-id2</b> 堆叠组 ID2 整数型是，取值范围<1-8>/<1-1>
删除堆叠组	1. 执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>no interface iss-trunk iss-group-id</b> ； 3. 结束。	<b>iss-group-id</b> 堆叠组 ID 整数型是，取值范围 1~2
重置当前设备的堆叠配置	1. 执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>iss reset-configure</b> ； 3. 结束。	-
配置重启堆叠系统成员	1. 保持在当前特权用户视图下；	<b>member-id</b> 堆叠成员编号

目的	步骤	参数说明
	2. 执行命令 <b>reboot member member-id</b> ; 3. 结束。	整数形式，取值范围是 1~8
配置同步堆叠的 OS 文件	1. 执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>iss synchronize-file</b> ; 3. 结束。	-
配置堆叠系统指定接口为保留端口	1. 执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>iss dual-active exclude interface { gigabitEthernet   xgigabitEthernet } interface-number</b> <b>iss dual-active exclude interface { gigabitEthernet   xgigabitEthernet } interface-number to { gigabitEthernet   xgigabitEthernet } interface-number</b> <b>no iss dual-active exclude interface { gigabitEthernet   xgigabitEthernet } interface-number</b> <b>no iss dual-active exclude interface { gigabitEthernet   xgigabitEthernet } interface-number to { gigabitEthernet   xgigabitEthernet } interface-number</b> ; 3. 结束。	interface-number 以太网接口号 整数形式，固化接口取值范围<1-1>/<0-0>/<1-24> 或者 <1-1>/<0-0>/<1-48>; 插卡接口取值范围是<1-1>/<0-2>/<1-2>
配置将堆叠分裂后进入 Recovery 状态的设备被关闭的所有端口重新恢复正常	1. 执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>iss dual-active restore</b> ; 3. 结束。	-
将以太网接口加入堆叠组	1. 执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>interface { fastEthernet   gigabitEthernet   xgigabitEthernet } interface-number</b> 进入接口配置视图; 3. 执行命令 <b>join iss-trunk iss-group-id</b> ;	iss-group-id 堆叠组 ID 整数型是，取值范围<1-1>或者 <1-8>/<1-1>
将以太网接口从堆叠组中删除	1. 执行命令 <b>configure</b> 进入全局配置视图; 2. 执行命令 <b>interface { fastEthernet   gigabitEthernet   xgigabitEthernet } interface-number</b> 进入接口配置视图; 3. 执行命令 <b>no join iss-trunk iss-group-id</b> ;	

### 10.8.3 维护及调试

#### 目的

用户可以通过本节操作对堆叠进行维护及调试。

### 过程

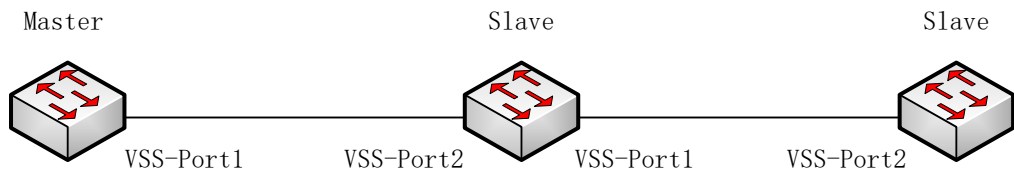
根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数说明
打开 iss debug 开关	<ol style="list-style-type: none"> <li>1. 保持在当前特权用户视图下；</li> <li>2. 执行命令 <code>debug iss{in out timer link-change conflict election all}</code>；</li> <li>3. 结束。</li> </ol>	in: 接收报文 out: 发送报文 timer: 定时器 link-change: 链路状态改变
关闭 iss debug 开关	<ol style="list-style-type: none"> <li>1. 保持在当前特权用户视图下；</li> <li>2. 执行命令 <code>no debug iss {in out timer link-change conflict election all}</code>；</li> <li>3. 结束。</li> </ol>	conflict: 冲突 election: 选择器 all: 以上所有
显示使能堆叠功能的接口表项信息	<ol style="list-style-type: none"> <li>1. 执行命令进入全局配置视图、特权用户视图、接口配置视图下；</li> <li>2. 执行命令 <code>show iss interface</code> 或者 <code>show iss interface local</code>；</li> <li>3. 结束。</li> </ol>	independent: 独立运行模式 -
显示设备堆叠的拓扑信息	<ol style="list-style-type: none"> <li>1. 执行命令进入全局配置视图、特权用户视图、接口配置视图下；</li> <li>2. 执行以下命令： <code>show iss topo</code> <code>show iss topo interface iss-trunk isstrunk-number</code> <code>show iss topo interface iss-trunk isstrunk-number hops</code></li> <li>3. 结束。</li> </ol>	isstrunk-number 指定作为观察端口以太网接口号整数形式，取值范围 <1-8>/<1-1>
显示设备堆叠的拓扑信息	<ol style="list-style-type: none"> <li>1. 执行命令进入全局配置视图、特权用户视图、接口配置视图下；</li> <li>2. 执行命令 <code>show iss member</code>；</li> <li>3. 结束。</li> </ol>	member 指定 member 的 id 值 整数取值，取值范围是 1-4
显示本台设备的堆叠信息	<ol style="list-style-type: none"> <li>1. 执行命令进入全局配置视图、特权用户视图、接口配置视图下；</li> <li>2. 执行命令 <code>show iss</code>；</li> <li>3. 结束。</li> </ol>	-
显示在 flash 中堆叠变量信息	<ol style="list-style-type: none"> <li>1. 执行命令进入全局配置视图、特权用户视图、接口配置视图下；</li> <li>2. 执行命令 <code>show iss flash</code>；</li> <li>3. 结束。</li> </ol>	-
显示堆叠接口的统计信息	<ol style="list-style-type: none"> <li>1. 执行命令进入全局配置视图、特权用户视图；</li> <li>2. 执行命令 <code>show iss statistic</code> <code>show iss statistic iss-trunk isstrunk-number</code></li> </ol>	isstrunk-number 堆叠 trunk 取值范围 整数形式，取值范

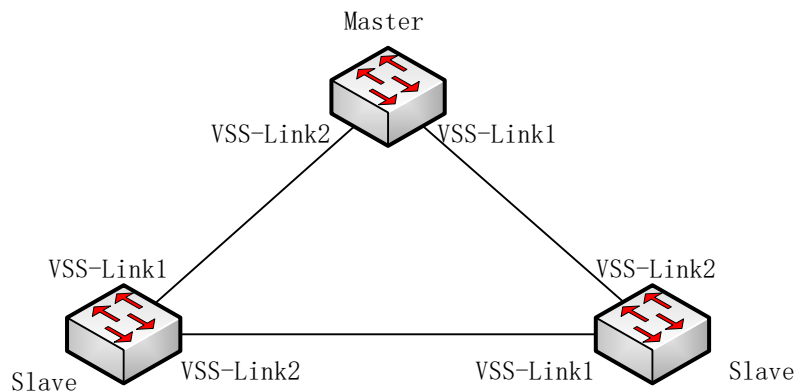
目的	步骤	参数说明
	<pre>show iss statistic brief</pre> <pre>show iss statistic brief iss-trunk isstrunk-number ;</pre> 3. 结束。	围<1-2>
显示 ISS 配置信息	1. 执行命令进入全局配置视图、特权用户视图和 ISS-trunk 接口配置视图； 2. 执行命令 <b>show iss-config</b> ； 3. 结束。	-

### 10.8.4 堆叠配置举例

#### 链型堆叠测试拓扑



#### 环形堆叠测试拓扑



要求三台设备在连接拓扑后均能形成稳定的堆叠系统。

#### 配置步骤

##### 1 对于链型拓扑

站点 1 的 1 号口与站点 2 的 1 号口相连，站点 2 的 2 号口与站点 3 的 1 号口相连。

站点 1 的配置:

(1) 设置 memberId

```
SC9600#conf
```

```
SC9600(config)#iss member 1
```

(2) 配置选举优先级

```
SC9600(config)#iss priority 3
```

(3) 使能堆叠口 (站点 1 使能一个堆叠口)

```
SC9600(config)interface iss-trunk 1
```

```
SC9600(config-iss-trunk-1)q
```

```
SC9600(config)#int gi 1/0/1
```

```
SC9600(config-ge1/0/1)#join iss-trunk 1
```

```
SC9600(config-ge1/0/1)#q
```

(4) 切换到堆叠模式 (需重启, 选择“Y”)

```
SC9600 (config)#iss mode iss
```

站点 2 的配置:

设置 memberId

```
SC9600#conf
```

```
SC9600(config)#iss member 1
```

(2) 配置选举优先级

```
SC9600(config)#iss priority 2
```

(3) 使能堆叠口 (站点 2 使能两个堆叠口)

```
SC9600(config)interface iss-trunk 1
```

```
SC9600(config-iss-trunk-1)q
```

```
SC9600(config)#int gi 1/0/1
```

```
SC9600(config-ge1/0/1)#join iss-trunk 1
```

```
SC9600(config-ge1/0/1)#q
```

```
SC9600(config)interface iss-trunk 2
```

```
SC9600(config-iss-trunk-2)q
```

```
SC9600(config)#int gi 1/0/2
```

```
SC9600(config-ge1/0/2)#join iss-trunk 2
```

```
SC9600(config-ge1/0/2)#q
```

(4) 切换到堆叠模式 (需重启, 选择“Y”)

```
SC9600 (config)#iss mode iss
```

站点 3 的配置:

(1) 设置 memberId

```
SC9600 #conf
```

```
SC9600 (config)#iss member 3
```

(2) 配置选举优先级

```
SC9600 (config)#iss priority 1
```

(3) 使能堆叠口 (站点 2 使能一个堆叠口)

```
SC9600 (config)#interface iss-trunk 1
```

```
SC9600 (config-iss-trunk-1)#q
```

```
SC9600 (config)#int gi 1/0/2
```

```
SC9600 (config-ge1/0/2)#join iss-trunk 1
```

(4) 切换到堆叠模式 (需重启, 选择“Y”)

```
SC9600 (config-ge1/0/2)#q
```

```
SC9600 (config)#iss mode iss
```

## 2 对于环形拓扑

站点 1 的 1 号口与站点 2 的 1 号口相连, 2 号口与站点 3 的 1 号口相连。站点 2 的 1 号口与站点 3 的 2 号口相连。

站点 1 的配置:

(1) 设置 memberId

```
SC9600#conf
```

```
SC9600 (config)#iss member 1
```

(2) 配置选举优先级

```
S3624 (config)#iss priority 3
```

(3) 使能堆叠口 (站点 1 使能两个堆叠口)

```
SC9600 (config)#interface iss-trunk 1
```

```
SC9600 (config-iss-trunk-1)#q
```

```
SC9600 (config)#int gi 1/0/1
```

```
SC9600 (config-ge1/0/1)#join iss-trunk 1
```

```
SC9600 (config-ge1/0/1)#q
```

```
SC9600 (config)interface iss-trunk 2
```

```
SC9600 (config-iss-trunk-2)#q
```

```
SC9600 (config)#int gi 1/0/2
```

```
SC9600 (config-ge1/0/2)#join iss-trunk 2
```

(4) 切换到堆叠模式 (需重启, 选择“Y”)

```
SC9600 (config)#iss mode iss
```

站点 2 的配置:

(1) 设置 memberId

```
SC9600#conf
```

```
SC9600 (config)#iss member 2
```

(2) 配置选举优先级

```
SC9600 (config)#iss priority 2
```

(3) 使能堆叠口 (站点 2 使能两个堆叠口)

```
SC9600 (config)interface iss-trunk 1
SC9600(config-iss-trunk-1)#q
SC9600 (config)#int ge1/0/1
SC9600 (config- ge1/0/1)#join iss-trunk 1
SC9600 (config-ge1/0/1)#q
SC9600 (config)#interface iss-trunk 2
SC9600 (config-iss-trunk-2)#q
SC9600 (config)#int gi 1/0/2
SC9600 (config- ge1/0/2)#join iss-trunk 2
SC9600(config- ge1/0/2)#q
```

(4) 切换到堆叠模式 (需重启, 选择“Y”)

```
SC9600 (config)#iss mode iss
```

站点 3 的配置:

(1) 设置 memberId

```
SC9600#conf
SC9600 (config)#iss member 2
```

(2) 配置选举优先级

```
SC9600 (config)#iss priority 1
```

(3) 使能堆叠口 (站点 2 使能两个堆叠口)

```
SC9600 (config)interface iss-trunk 1
SC9600(config-iss-trunk-1)#q
SC9600 (config)#int ge1/0/1
SC9600 (config- ge1/0/1)#join iss-trunk 1
SC9600 (config-ge1/0/1)#q
```



```
SC9600 (config)#interface iss-trunk 2
```

```
SC9600 (config-iss-trunk-2)#q
```

```
SC9600 (config)#int gi 1/0/2
```

```
SC9600 (config- ge1/0/2)#join iss-trunk 2
```

```
SC9600(config- ge1/0/2)#q
```

（4）切换到堆叠模式（需重启，选择“Y”）

```
SC9600 (config)#iss mode iss
```

## 第11章 VPN 配置

### 11.1 概述

本章介绍了 SC9600 系列高端交换机 VPN 隧道管理的基本内容、配置过程和配置举例。

本章包括如下主题：

内容	页码
11.1 概述	11-1
11.2 L3VPN 配置	11-1
11.3 VPN 隧道管理配置	11-14

### 11.2 L3VPN 配置

#### 11.2.1 L3VPN 简介

##### 协议介绍

MPLS L3VPN 是服务提供商 VPN 解决方案中一种基于 PE 的 L3VPN 技术，它使用 BGP 在服务提供商骨干网上发布 VPN 路由，使用 MPLS 在服务提供商骨干网上转发 VPN 报文。MPLS L3VPN 组网方式灵活、可扩展性好，并能够方便地支持 MPLS QoS 和 MPLS TE。

MPLS L3VPN 模块当前最新版本为 1.0。

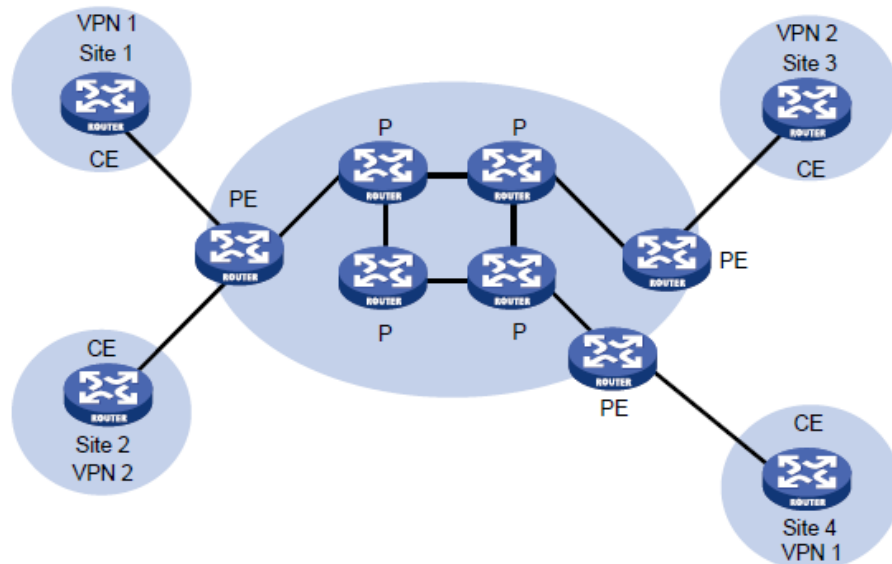


图 11-1 MPLS L3VPN 组网

MPLS L3VPN 组网方案示意图如图 11-1。MPLS L3VPN 模型由三部分组成：CE、PE 和 P。

- CE（Customer Edge）设备：用户网络边缘设备，有接口直接与 SP（Service Provider，服务提供商）相连。CE 可以是路由器或交换机，也可以是一台主机。CE“感知”不到 VPN 的存在，也不需要必须支持 MPLS。
- PE（Provider Edge）路由器：服务提供商边缘路由器，是服务提供商网络的边缘设备，与用户的 CE 直接相连。在 MPLS 网络中，对 VPN 的所有处理都发生在 PE 上。
- P（Provider）路由器：服务提供商网络中的骨干路由器，不与 CE 直接相连。P 设备只需要具备基本 MPLS 转发能力。

CE 和 PE 的划分主要是根据 SP 与用户的管理范围，CE 和 PE 是两者管理范围的边界。

CE 设备通常是一台路由器，当 CE 与直接相连的 PE 建立邻接关系后，CE 把本站点的 VPN 路由发布给 PE，并从 PE 学到远端 VPN 的路由。CE 与 PE 之间使用 BGP/IGP 交换路由信息，也可以使用静态路由。

PE 从 CE 学到 CE 本地的 VPN 路由信息后，通过 BGP 与其它 PE 交换 VPN 路由信息。PE 路由器只维护与它直接相连的 VPN 的路由信息，不维护服务提供商网络中的所有 VPN 路由。

P 路由器只维护到 PE 的路由，不需要了解任何 VPN 路由信息。

当在 MPLS 骨干网上传输 VPN 流量时，入口 PE 做为 Ingress LSR (Label Switch Router, 标签交换路由器)，出口 PE 做为 Egress LSR, P 路由器则做为 Transit LSR。

### 报文转发

在基本 MPLS L3VPN 应用中 (不包括跨域的情况), VPN 报文转发采用两层标签方式:

- 第一层 (外层) 标签在骨干网内部进行交换, 指示从 PE 到对端 PE 的一条 LSP。
- 第二层 (内层) 标签在从对端 PE 到达 CE 时使用, 指示报文应被送到哪个 Site, 或者更具体一些, 到达哪一个 CE。这样, 对端 PE 根据内层标签可以找到转发报文的接口。

特殊情况下, 属于同一个 VPN 的两个 Site 连接到同一个 PE, 这种情况下只需要知道如何到达对端 CE。

以图 11-2 为例, 说明 VPN 报文的转发:

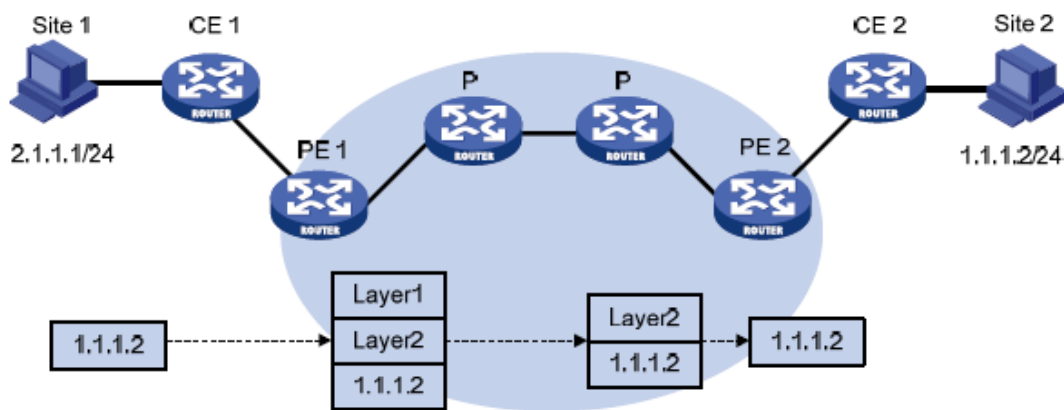


图 11-2 VPN 报文转发示意图

- 1) Site 1 发出一个目的地址为 1.1.1.2 的 IP 报文, 由 CE 1 将报文发送至 PE 1。
- 2) PE 1 根据报文到达的接口及目的地址查找 VPN 实例表项, 匹配后将报文转发出去, 同时打上内层和外层两个标签。
- 3) MPLS 网络利用报文的外层标签, 将报文传送到 PE 2 (报文在到达 PE 2 前一跳时已经被剥离外层标签, 仅含内层标签)。

- 4) PE 2 根据内层标签和目的地址查找 VPN 实例表项，确定报文的出接口，将报文转发至 CE 2。
- 5) CE 2 根据正常的 IP 转发过程将报文传送到目的地。

### 路由信息发布

在基本 MPLS L3VPN 组网中，VPN 路由信息的发布涉及 CE 和 PE，P 路由器只维护骨干网的路由，不需要了解任何 VPN 路由信息。PE 路由器也只维护与它直接相连的 VPN 的路由信息，不维护所有 VPN 路由。因此，MPLS L3VPN 网络具有良好的可扩展性。

VPN 路由信息的发布过程包括三部分：本地 CE 到入口 PE、入口 PE 到出口 PE、出口 PE 到远端 CE。完成这三部分后，本地 CE 与远端 CE 之间将建立可达路由，VPN 私网路由信息能够在骨干网上发布。

下面分别对这三部分进行介绍。

- 1) 本地 CE 到入口 PE 的路由信息交换

CE 与直接相连的 PE 建立邻接关系后，把本站点的 VPN 路由发布给 PE。

CE 与 PE 之间可以使用静态路由、RIP、OSPF、IS-IS 或 EBGP。无论使用哪种路由协议，CE 发布给 PE 的都是标准的 IPv4 路由。

- 2) 入口 PE 到出口 PE 的路由信息交换

PE 从 CE 学到 VPN 路由信息后，为这些标准 IPv4 路由增加 RD 和 VPN Target 属性，形成 VPN-IPv4 路由，存放为 CE 创建的 VPN 实例中。

- 3) 出口 PE 到远端 CE 的路由信息交换

远端 CE 有多种方式可以从出口 PE 学习 VPN 路由，包括静态路由、RIP、OSPF、IS-IS 和 EBGP，与本地 CE 到入口 PE 的路由信息交换相同。

## 11.2.2 L3VPN 配置

MPLS L3VPN 由运营商经营 MPLS VPN 骨干网，通过 PE 设备提供 VPN 服务。VPN 用户通过 CE 设备与运营商的 PE 设备互连，接入 MPLS VPN 网络，实现属于用户 VPN 的不同 Site 之间的通信。MPLS L3VPN 的基本配置步骤如下：

1. 在 P 网络中配置 IGP 协议，及部署 MPLS LDP
2. 在 PE 上为 VPN 客户创建 VRF 及指定 RD，及 RT 的导入导出策略

3. 在 PE 上启用 MP-BGP，并建立 VPNV4 邻居
4. 运行 PE-CE 路由选择协议
5. 将 PE-CE 协议相互重发布

MPLS L3VPN 模块实现上述第二步骤，即 MPLS L3VPN 的 VPN 实例配置的相关内容。

### 11.2.2.1 创建 VPN 实例

#### 目的

创建一条 VPN 实例并进入 VPN 实例视图。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
创建 VPN 实例	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>ip vpn-instance NAME</b>，创建一条 VPN 实例</li> <li>3. 结束。</li> </ol>
删除 VPN 实例	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>no ip vpn-instance NAME</b>，删除一条指定实例名的 VPN 实例；</li> <li>3. 结束。</li> </ol>

附表：

参数	说明	取值
NAME	指定 VPN 实例名称	字符串形式，长度范围 1~31

### 11.2.2.2 配置 RD

#### 目的

配置路由标识（RD，Route Distinguisher）。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置路由标识	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>ip vpn-instance NAME</b>，创建一条 VPN 实例并进入 VPN 实例配置视图；</li> <li>3. 执行命令 <b>route-distinguisher RD-STRING</b>；</li> <li>4. 结束。</li> </ol>

附表：

参数	说明	取值
NAME	指定 VPN 实例名称	字符串形式，长度范围 1~31
RD-STRING	指定路由标识的值	路由标识的值有三种形式： 1) 16 位自治系统号:32 位用户自定义数，例如：101:3。自治系统号的取值范围是 0~65535；用户自定义数的取值范围是 0~4294967295。其中，自治系统号和用户自定义数不能同时为 0，即 RD 的值不能是 0:0。 2) 32bits 自治系统号:16bits 用户自定义数字，例如：100.5:1。32bits 自治系统号通常写成 x.y 的形式，即 0~65535.0~65535；用户自定义数的取值范围是 0~65535。其中，自治系统号和用户自定义数不能同时为 0，即 RD 的值不能是 0.0:0。 3) 32 位 IP 地址:16 位用户自定义数，例如：192.168.122.15:1。IP 地址的取值范围是 0.0.0.0~255.255.255.255；用户自定义数的取值范围是 0~65535。



注意：

路由标识没有缺省值，必需在创建 VPN 实例时配置。

### 11.2.2.3 配置 VPN Target

#### 目的

配置 VPN Target。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置 VPN Target	1. 执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>ip vpn-instance NAME</b> ，创建一条 VPN 实例并进入 VPN 实例配置视图； 3. 执行命令 <b>vpn-target TARGET {both   export-extcommunity</b>

目的	步骤
	<pre> import-extcommunity};</pre> <p>4. 结束。</p>
删除当前 VPN 实例关联的所有 VPN target	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>ip vpn-instance NAME</b>, 创建一条 VPN 实例并进入 VPN 实例配置视图;</li> <li>3. 执行命令 <b>no vpn-target</b>;</li> <li>4. 结束。</li> </ol>
删除指定的 VPN Target	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图;</li> <li>2. 执行命令 <b>ip vpn-instance NAME</b>, 创建一条 VPN 实例并进入 VPN 实例配置视图;</li> <li>3. 执行命令 <b>no vpn-target TARGET {both  export-extcommunity  import-extcommunity}</b>;</li> <li>4. 结束。</li> </ol>

附表:

参数	说明	取值
NAME	指定 VPN 实例名称	字符串形式, 长度范围 1~31
TARGET	指定添加 VPN Target 扩展团体属性到 VPN 实例入或出方向 VPN Target 扩展团体列表, 或是出入方向 VPN Target 扩展团体	<p>用户可以使用以下三种格式之一来表示 VPN Target 值:</p> <ol style="list-style-type: none"> <li>1) 16 位自治系统号:32 位用户自定义数, 例如: 1:3。自治系统号的取值范围是 0~65535; 用户自定义数的取值范围是 0~4294967295。其中, 自治系统号 and 用户自定义数不能同时为 0, 即 VPN Target 的值不能是 0:0。</li> <li>2) 32 位 IP 地址:16 位用户自定义数, 例如: 192.168.122.15:1。IP 地址的取值范围是 0.0.0.0~255.255.255.255; 用户自定义数的取值范围是 0~65535。</li> <li>3) 32bits 自治系统号:16bits 用户自定义数字, 例如: 100.5:1。32bits 自治系统号通常写成 x.y 的形式, 即 0~65535.0~65535; 用户自定义数的取值范围是 0~65535。其中, 自治系统号 and 用户自定义数不能同时为 0, 即 VPN Target 的值不能是 0.0:0。</li> </ol>
both	指定添加 vpn-target 扩展团体属性到 VPN 实例入方向和出方向的扩展团体属性列	-



参数	说明	取值
	表中	
export-extracommunity	指定出方向到目的 VPN 的路由信息的扩展团体属性值	-
import-extracommunity	定义可以接收带有指定扩展团体属性值的路由信息	-



注意：

VPN Target 没有缺省值，必须在创建 VPN 实例时配置。

#### 11.2.2.4 配置 VPN 实例的描述信息

##### 目的

配置 VPN 实例的描述信息。

##### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置 VPN 实例的描述信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>ip vpn-instance NAME</b>, 创建一条 VPN 实例并进入 VPN 实例配置视图；</li> <li>3. 执行命令 <b>description DESCRIPTION</b>;</li> <li>4. 结束。</li> </ol>
删除 VPN 实例的描述信息	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>ip vpn-instance NAME</b>, 创建一条 VPN 实例并进入 VPN 实例配置视图；</li> <li>3. 执行命令 <b>no description</b>;</li> <li>4. 结束。</li> </ol>

附表：

参数	说明	取值
NAME	指定 VPN 实例名称	字符串形式，长度范围 1~31
DESCRIPTION	指定 VPN 实例描述信息	字符串形式，长度范围 1~31

#### 11.2.2.5 配置 VPN 路由策略为每实例

##### 目的

配置当前 VPN 实例下所有发往对端 PE 的路由都使用同一个标签。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置 VPN 路由策略为每实例	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>ip vpn-instance NAME</b>, 创建一条 VPN 实例并进入 VPN 实例配置视图；</li> <li>3. 执行命令 <b>apply-label per-instance</b>;</li> <li>4. 结束。</li> </ol>
取消当前 VPN 实例下所有发往对端 PE 的路由都使用同一个标签，恢复为默认值，即每条路由分配一个标签	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>ip vpn-instance NAME</b>, 创建一条 VPN 实例并进入 VPN 实例配置视图；</li> <li>3. 执行命令 <b>no apply-label per-instance</b>;</li> <li>4. 结束。</li> </ol>

附表：

参数	说明	取值
NAME	指定 VPN 实例名称	字符串形式，长度范围 1~31

### 11.2.2.6 配置接口与指定 VPN 实例绑定

#### 目的

配置接口与指定 VPN 实例绑定。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置 VPN 路由策略为每实例	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>ip vpn-instance NAME</b>, 创建一条 VPN 实例并进入 VPN 实例配置视图；</li> <li>3. 执行命令 <b>ip binding vpn-instance NAME</b>;</li> <li>4. 结束。</li> </ol>
取消接口与 VPN 实例的绑定	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>ip vpn-instance NAME</b>, 创建一条 VPN 实例并进入 VPN 实例配置视图；</li> <li>3. 执行命令 <b>no ip binding vpn-instance NAME</b>;</li> </ol>

目的	步骤
	4. 结束。

附表：

参数	说明	取值
NAME	指定 VPN 实例名称	字符串形式，长度范围 1~31



注意：

- 1 执行 `ip binding vpn-instance` 命令将删除接口上已经配置的 IP 地址、路由协议等三层特性，如果需要应重新配置。
- 2 同一个接口不能既作为 L2VPN 的 AC 接口又作为 L3VPN 的 AC 接口。当某个接口绑定 L2VPN 后，该接口上配置的 IP 地址、路由协议等三层特性会全部变为无效。
- 3 配置 VPN 实例后，需要将本设备上属于该 VPN 的接口与该 VPN 实例关联，否则该接口将属于公网接口。
- 4 在接口上配置与 VPN 实例关联或取消已建立的关联都将清除该接口的 IP 地址、路由协议等三层特性，如果需要应重新配置。
- 5 在接口上取消已建立的关联将清除该接口的 IP 地址、路由协议等三层特性，如果需要应重新配置。

### 11.2.3 维护及调试

#### 目的

当 MPLS L3VPN 功能不正常，需要进行查看、调试或定位问题时，可以使用本小节操作。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
显示 VPN 实例配置情况	<ol style="list-style-type: none"> <li>1. 不执行任何命令保持当前特权用户视图，或执行命令 <code>configure</code> 进入全局配置视图；或在全局配置视图下执行命令 <code>ip vpn-instance NAME</code> 进入 VPN 实例配置视图；</li> <li>2. 执行命令 <code>show ip vpn-instance</code>；</li> <li>3. 结束。</li> </ol>
显示 VPN 实例详细信息	<ol style="list-style-type: none"> <li>1. 不执行任何命令保持当前特权用户视图，或执行命令 <code>configure</code> 进入全局配置视图；或在全局配置视图下执行命令 <code>ip vpn-instance NAME</code> 进入 VPN 实例配置视图；</li> <li>2. 执行命令 <code>show ip vpn-instance verbose</code>；</li> <li>3. 结束。</li> </ol>
显示 VPN	<ol style="list-style-type: none"> <li>1. 不执行任何命令保持当前特权用户视图，或执行命令 <code>configure</code> 进入全局配置视</li> </ol>

目的	步骤
实例配置信息	图；或在全局配置视图下执行命令 <b>ip vpn-instance NAME</b> 进入 VPN 实例配置视图； 2. 执行命令 <b>show ip vpn-instance config</b> ； 3. 结束。
显示具备指定入口 vpn target 属性的 VPN 实例	1. 不执行任何命令保持当前特权用户视图，或执行命令 <b>configure</b> 进入全局配置视图；或在全局配置视图下执行命令 <b>ip vpn-instance NAME</b> 进入 VPN 实例配置视图； 2. 执行命令 <b>show ip vpn-instance import-vt TARGET</b> ； 3. 结束。
打开 L3VPN 调试功能	1. 不执行任何命令保持当前特权用户视图，或执行命令 <b>configure</b> 进入全局配置视图；或在全局配置视图下执行命令 <b>ip vpn-instance NAME</b> 进入 VPN 实例配置视图； 2. 执行命令 <b>debug l3vpn</b> ； 3. 结束。
关闭 L3VPN 调试功能	1. 不执行任何命令保持当前特权用户视图，或执行命令 <b>configure</b> 进入全局配置视图；或在全局配置视图下执行命令 <b>ip vpn-instance NAME</b> 进入 VPN 实例配置视图； 2. 执行命令 <b>no debug l3vpn</b> ； 3. 结束。

附表：

参数	说明	取值
TARGET	指定添加 VPN Target 扩展团体属性到 VPN 实例入或出方向 VPN Target 扩展团体列表，或是出入方向 VPN Target 扩展团体	用户可以使用以下三种格式之一来表示 VPN Target 值： 1) 16 位自治系统号:32 位用户自定义数，例如：1:3。自治系统号的取值范围是 0~65535；用户自定义数的取值范围是 0~4294967295。其中，自治系统号和用户自定义数不能同时为 0，即 VPN Target 的值不能是 0:0。 2) 32 位 IP 地址:16 位用户自定义数，例如：192.168.122.15:1。IP 地址的取值范围是 0.0.0.0 ~ 255.255.255.255；用户自定义数的取值范围是 0~65535。 3) 32bits 自治系统号:16bits 用户自定义数字，例如：100.5:1。32bits 自治系统号通常写成 x.y 的形式，即 0~65535.0~65535；用户自定义数的取值范围是 0~65535。其中，自治系统号和用户自定义数不能同时为 0，即 VPN Target 的值不能是 0.0:0。

### 11.2.4 配置举例

#### 组网要求

MPLS L3VPN 组网方案示意图如下，MPLS L3VPN 在 PE 上进行配置。

#### 组网图

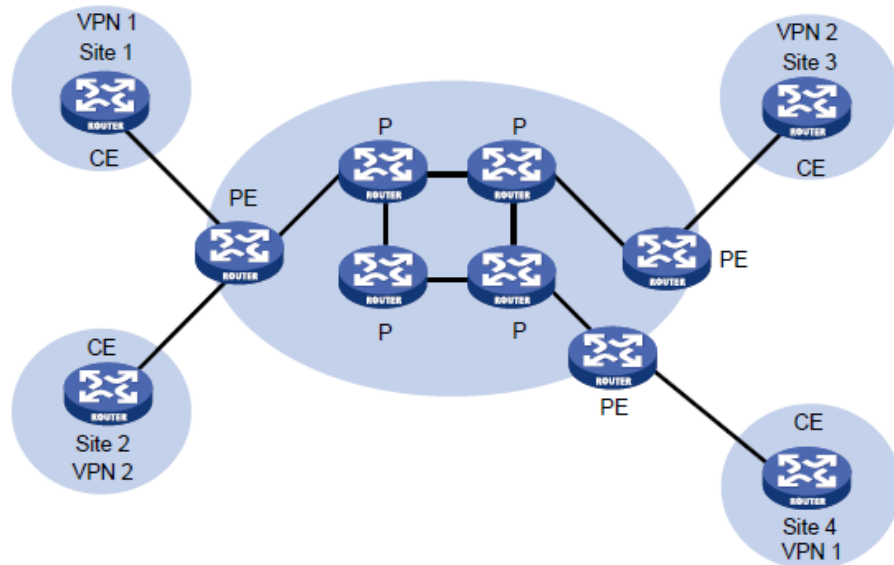


图 11-3 MPLS L3VPN 组网示意图

#### 配置步骤

```
Swich(config)#ip vpn-instance vpn1
Swich(config-vpn-instance-vpn1)#route-distinguisher 100:1
Swich(config-vpn-instance-vpn1)#vpn-target 1000:1 import-extcommunity
Swich(config-vpn-instance-vpn1)#vpn-target 1000:2 export-extcommunity
Swich(config-vpn-instance-vpn1)#vpn-target 1000:3 both
Swich(config-vpn-instance-vpn1)#vpn-target 2000:1 import-extcommunity
Swich(config-vpn-instance-vpn1)#show ip vpn-instance
```

Total VPN-Instances configured : 1

VPN-Instance Name	RD	Creation Time
-------------------	----	---------------

```

vpn1                                100:1                                2014-02-04 09:35:29

Swich(config-vpn-instance-vpn1)#show ip vpn-instance verbose

VPN-Instance Name and ID: vpn1, 1

  Creation Time: 2014-02-04 09:35:29

  Route Distinguisher: 100:1

  Description: --

  Apply Label Per Instance: Disable

  Vpn Target : 1000:1 import-extcommunity
                1000:2 export-extcommunity
                1000:3 import-extcommunity
                1000:3 export-extcommunity
                2000:1 import-extcommunity

Swich(config-vpn-instance-vpn1)#show ip vpn-instance config

ip vpn-instance snmp-trap enable

ip vpn-instance vpn1

route-distinguisher 100:1

vpn-target 1000:1 import-extcommunity
vpn-target 1000:2 export-extcommunity
vpn-target 1000:3 import-extcommunity
vpn-target 1000:3 export-extcommunity
vpn-target 2000:1 import-extcommunity

Swich(config-vpn-instance-vpn1)#q

Swich(config)#ip vpn-instance vpn2

Swich(config-vpn-instance-vpn2)#route-distinguisher 200:1

Swich(config-vpn-instance-vpn2)#vpn-target 2000:1 import-extcommunity

Swich(config-vpn-instance-vpn2)#q

```

```
Swich(config)#show ip vpn-instance import-vt 2000:1
```

The vpn-instances are :

VPN-Instance Name and ID : vpn1, 1

VPN-Instance Name and ID : vpn2, 2

## 11.3 VPN 隧道管理配置

### 11.3.1 IPv6 隧道管理配置

#### 11.3.1.1 6RD 隧道管理概述

##### VPN 产生的背景

由于部署了 6to4 的 ISP 不能保证从本地 IPv6 站点发出的分组到达用户站点，从而阻碍了 ISPs 使用 6to4 对他们的用户提供完全 IPv6 单播连接。其服务质量对于其他 6to4 ISPs 用户毫无保证。

IPv6 的部署需要经历一个渐进的过程，从更最初的 IPv6 孤岛逐渐聚合成为骨干 IPv6 网络，最终通过隧道连接 IPv6 占据主导地位。

##### 6RD (IPv6 Rapid Deployment) 工作原理

用户家庭的 6RD 网关（即 6RD-CE）将用户网络中 IPv6 主机发出的上行 IPv6 报文，在其 WAN 接口直接封装为 IPv4 报文的净荷（RFC4213）。该报文外层 IPv4 报文头的源地址为 6RD-CE 的 WAN 接口 IPv4 地址，目的地址是 6RD-BR 的 IPv4 互联网侧接口的 IPv4 地址。该报文在 IPv4 互联网上与普通 IPv4 报文采用相同的路由寻址方式。

6RD-BR 在收到该报文后，去掉外层 IPv4 的封装包头，将用户主机发出的 IPv6 报文转发进入 IPv6 互联网。当 6RD-BR 收到指向 6RD 用户网络中 IPv6 主机的 IPv6 报文后，在其 IPv4 互联网侧接口同样将这个 IPv6 报文封装成 IPv4 报文的净荷。该报文外层 IPv4 报文头的源地址为 6RD-BR 的 IPv4 互联网侧的接口地址，其目的地址是连接目标用户网络的 6RD-CE 的 WAN 接口的 IPv4 地址。

根据上述 6RD 用户主机编址规则，该 IPv4 目的地址可直接从转发的 IPv6 报文头中 IPv6 目的地址中的 IPv4 地址字段中获取。6RD-CE 在收到该报文后，去掉外层 IPv4 的封装包头，再将 IPv6 报文转发至用户网络中相应的 IPv6 主机。

#### 11.3.1.2 配置 Tunnel 6RD

##### 背景信息



注意：

配置超过 64 的目的地址前缀长度的路由最多只能配 128 条。

### 目的

使用本节操作配置 Tunnel 6RD，实现 IPv6 快速部署隧道功能。

### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
创建并进入隧道接口视图	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface tunnel tunnel-num</b> 创建并进入 tunnel 接口配置视图；</li> <li>3. 结束。</li> </ol>
配置隧道模式为 6RD	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface tunnel tunnel-num</b> 进入 tunnel 接口配置视图；</li> <li>3. 执行命令 <b>tunnel protocol { gre-ipv4   gre-ipv6   ipv6-ipv4 [ 6to4   isatap   6rd ]   ipv4-ipv6   ipsec   none   default }</b> 配置隧道模式为 6RD；</li> <li>4. 结束。</li> </ol>
配置 tunnel 接口的源地址或源接口	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface tunnel tunnel-num</b> 进入 tunnel 接口配置视图；</li> <li>3. 执行命令 <b>tunnel source { ipv4-address   ipv6-address }</b> 用来配置 tunnel 接口的源地址，执行命令 <b>tunnel source interface vlan vlan-id</b> 或 <b>tunnel source interface loopback loopback-id</b> 用来配置 tunnel 接口的源接口；</li> <li>4. 结束。</li> </ol>
（可选）配置全局 6RD 老化时间	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>tunnel 6rd { tunnel-6rd   default }</b> 用来配置全局 6rd 老化时间；</li> <li>3. 结束。</li> </ol>
配置 6RD 隧道的 IPv6 前缀	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface tunnel tunnel-num</b> 进入 tunnel 接口配置视图；</li> <li>3. 执行命令 <b>tunnel 6rd ipv6 prefix ipv6-address mask</b> 用来配置 6RD 隧道的 IPv6 前缀；</li> <li>4. 结束。</li> </ol>
配置 6RD 隧道的 IPv4 前缀长度	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface tunnel tunnel-num</b> 进入 tunnel 接口配置视图；</li> <li>3. 执行命令 <b>tunnel 6rd ipv4 prefix-length prefix</b> 用来配置 6RD 隧道的 IPv4 前缀长度；</li> <li>4. 结束。</li> </ol>
配置 6RD 隧道的 BR 地址	<ol style="list-style-type: none"> <li>1. 执行命令 <b>configure</b> 进入全局配置视图；</li> <li>2. 执行命令 <b>interface tunnel tunnel-num</b> 进入 tunnel 接口配置视图；</li> </ol>



目的	步骤
	3. 执行命令 <b>tunnel 6rd br ipv4-address</b> 用来配置 6RD 隧道的 BR 地址； 4. 结束。
配置 IPv6 静态路由 下一跳为隧道接口	1. 执行命令 <b>configure</b> 进入全局配置视图； 2. 执行命令 <b>ipv6 route-static ipv6-address mask-length interface tunnel tunnel-interface-number</b> 配置 IPv6 静态路由下一跳为隧道接口； 3. 结束。

附表：

参数	说明	取值
tunnel-num	表示 Tunnel 接口的取值范围	整数取值，取值范围是 1-1024
ipv4-address	Tunnel 的源 IPv4 地址或前缀地址	IPv4 地址，点分十进制
ipv6-address	IPv6 前缀地址	在这种形式中，128 位的 IP 地址被分为 8 组，每组的 16 位用 4 个十六进制字符（0~9，A~F）来表示，组和组之间用冒号（:）隔开。其中每个“X”代表一组十六进制数值
vlan id	vlan 端口号	整数取值，取值范围是 1-4094
loopback id	loopback 端口号取值范围	整数取值，取值范围是 1-1024
tunnel-6rd	老化时间取值范围，单位是秒	整数取值，取值范围是 60-1800
mask	IPv6 掩码长度	整数取值，取值范围是 0-128
prefix	IPv6 掩码长度	整数取值，取值范围是 0-128
mask-length	目的 IP 地址的掩码长度	整数形式，取值范围是 0~128
tunnel-interface-number	tunnel 接口 ID	整数形式，取值范围是 1~1024

### 11.3.1.3 维护及调试

#### 目的

当 Tunnel 6RD 功能不正常，需要进行查看、调试或定位问题时，可以使用本小节操作。

#### 过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
查看所有 Tunnel 或者指定 Tunnel 接口的信息	1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface tunnel tunnel-num</b> 进入 tunnel 接口配置视图，或不执行任何命令保持当前特权用户视图； 2. 执行命令 <b>show interface tunnel</b> 显示所有 Tunnel 接口的信息或执行命令 <b>show interface tunnel tunnel-num</b> 显示指定 Tunnel 接口的信息；

目的	步骤
	3. 结束。
查看所有 Tunnel 接口的配置信息	1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface tunnel tunnel-num</b> 进入 tunnel 接口配置视图，或不执行任何命令保持当前特权用户视图； 2. 执行命令 <b>show interface tunnel config</b> 用来显示所有 Tunnel 接口的配置信息； 3. 结束。
查看所有的 Tunnel 接口中 ipv6 快速部署的配置信息	1. 执行命令 <b>disable</b> 退出到普通用户视图，或执行命令 <b>configure</b> 进入全局配置视图，或执行命令 <b>interface tunnel tunnel-num</b> 进入 tunnel 接口配置视图，或不执行任何命令保持当前特权用户视图； 2. 执行命令 <b>show interface tunnel 6rd</b> 或 <b>show interface tunnel tunnel-num 6rd</b> 用来显示所有的 Tunnel 接口中 ipv6 快速部署的配置信息； 3. 结束。

附表：

参数	说明	取值
tunnel-num	表示 Tunnel 接口的取值范围	整数取值，取值范围是 1-1024

### 11.3.1.4 配置举例

#### 组网要求

CE、BR 的 Tunnel 类型均为 6RD。现 6RD 隧道配置如图 11-4所示。

#### 组网图

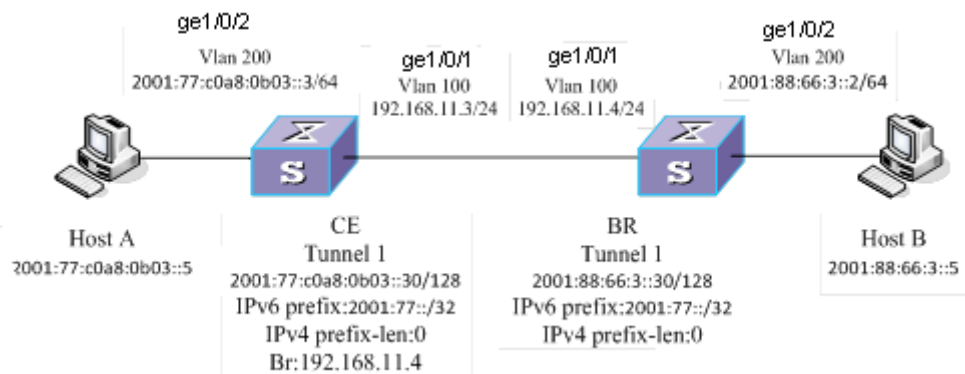


图 11-4 6RD 配置拓扑图

#### 配置步骤

1、配置 VLAN 接口的 IP 地址。

```
SC9600#configure
SC9600(config)#interface vlan 100
SC9600(config-vlan-100)#port hybrid pvid 100
SC9600(config-vlan-100)#ip address 192.168.11.4/24
SC9600(config-vlan-100)#quit
SC9600(config)#interface vlan 200
SC9600(config-vlan-200)#ipv6 enable
SC9600(config-vlan-200)#ipv6 address 2001:88:66:3::2/64
SC9600(config-vlan-200)#quit
SC9600(config)#
SC9600(config)#interface gigabitEthernet 1/0/1
SC9600(config-gigabitEthernet-1/0/1)#port hybrid vlan 100 untagged
SC9600(config-gigabitEthernet-1/0/1)#port hybrid pvid 100
SC9600(config-gigabitEthernet-1/0/1)#quit
SC9600(config)# interface gigabitEthernet 1/0/2
SC9600(config-gigabitEthernet-1/0/2)#port hybrid vlan 200 untagged
SC9600(config-gigabitEthernet-1/0/2)# port hybrid pvid 200
SC9600(config-gigabitEthernet-1/0/2)#quit
SC9600(config)#
```

## 2、配置 6RD 隧道参数。

```
SC9600#configure
SC9600(config)#interface tunnel 1
SC9600(config-tunnel-1)#tunnel protocol ipv6-ipv4 6rd
SC9600(config-tunnel-1)#tunnel source interface vlan 100
SC9600(config-tunnel-1)#tunnel 6rd ipv6 prefix 2001:77::/32
SC9600(config-tunnel-1)#tunnel 6rd ipv4 prefix-length 0
SC9600(config-tunnel-1)#ipv6 enable
SC9600(config-tunnel-1)#ipv6 address 2001:88:66:3::30/128
SC9600(config-tunnel-1)#quit
SC9600(config)#
```

## 3、配置静态路由。

```
SC9600(config)#ipv6 route 2001:77:: 32 interface tunnel 1
```

## 4、配置 HostA。

//方法一：手动在 HostA 上进行配置。

配置 HostA 的 IPv6 地址：2001:77:c0a8:0b03::4

配置 Host A 的静态路由：ipv6 adu ::/0 2001:77:c0a8:0b03::3

//方法二：HostA 的 IPv6 地址由 CE 进行自动分配，需在 CE 上进行如下配置。

```
SC9600(config)#interface vlan 200
```

```
SC9600(config-Man-200)#ipv6 nd ra enable
```

```
SC9600(config-Man-200)#end
```

```
SC9600#
```

5、配置 HostB。

//方法一：手动在 HostB 上进行配置。

配置 HostB 的 IPv6 地址：2001:88:66:3::3

配置 Host B 的静态路由：ipv6 adu ::/0 2001:88:66:3::2

//方法二：HostB 的 IPv6 地址由 BR 进行自动分配，需在 BR 上进行如下配置。

```
SC9600(config)#interface vlan 200
```

```
SC9600(config-Man-200)#ipv6 nd ra enable
```

```
SC9600(config-Man-200)#end
```

```
SC9600#
```