SC9600E 系列

高端交换机

操作手册

版本：A/02

浪潮思科网络科技有限公司

二零二三年十月

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

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

公司网址：　　http://www.inspur.com/

技术支持热线：　400-691-1766

技术支持邮箱：　inspur_network@inspur.com

技术文档邮箱：　inspur_network@inspur.com

客户投诉热线：　400-691-1766

公司总部地址：　山东省济南市高新区浪潮路 1036 号

邮政编码：　　250000

声　　明

前　言

手册说明

本手册介绍SC9600E系列高端交换机（以下简称为SC9600E）的各种功能模块和业务特性基于CLI的操作指南，包括SC9600E的基本配置操作、二层以太网功能配置操作、IP业务、路由、QoS配置操作、组播、安全、可靠性、设备管理以及运维管理、VPN、数据中心特性等配置操作。从简单技术原理、功能配置过程和配置举例三方面进行介绍。这些配置操作的介绍旨在帮助用户掌握SC9600E的配置方法和了解其应用场景，更全面系统的掌握SC9600E的使用、维护以及管理。

本操作手册适用于以下高端交换机产品型号：

- SC9606E
- SC9610E

本手册适用于以下人员：工程设计人员、产品开通人员、产品维护人员。

符号约定

符号	含义	说明
	提示	重要的特征或操作指导。
	注意	可能会对人身造成伤害，或给系统造成损害，或造成业务中断或丢失。
	警告	可能会对人身造成重大伤害。

版本说明

版本	说明
A/02	初始版本

免责声明

本手册依据现有信息制作其内容，如有更改恕不另行通知。浪潮思科网络科技有限公司在编写该手册的时候已尽最大努力保证其内容准确可靠，但浪潮思科网络科技有限公司不对本手册中的遗漏、不准确或错误导致的损失和损害承担责任。

目 录

1 基础配置

本章主要介绍SC9600E系列交换机的接口和基础配置操作。

1.1 登录交换机

通过Console口、Telnet方式登录高端交换机，用户可以对设备进行日常管理和维护。

1.1.1 通过 Console 口登录交换机

组网环境

请使用一根串口线连接PC串口和SC9600E高端交换机主用主控卡的Console口（CON标识口），如图 1-1所示。

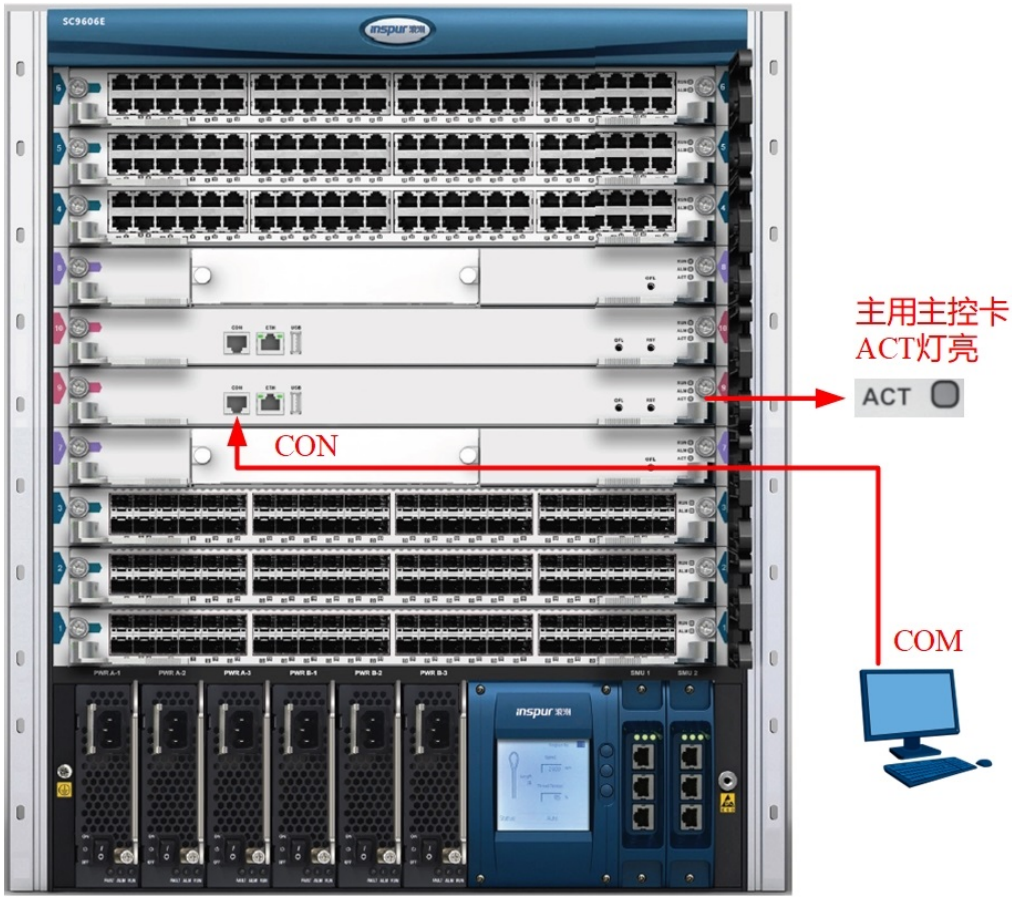


图 1-1　通过Console串口登录SC9600E高端交换机

前置准备

在配置用户通过Console口登录SC9600E高端交换机之前，需完成以下任务：

- 准备好Console通信电缆。
- PC端准备好终端仿真软件（PC系统自带或第三方终端仿真软件均可）。
- SC9600E高端交换机已烧录了正确的OS和BIOS版本。

操作步骤

以SecureCRT终端软件配置为例进行介绍。

1. 右键单击PC上“计算机”，选择“属性”→“设备管理器”→“端口（COM和LTP）”。用户在PC上查看与交换机相连的串口号，以COM5为例。

2. 打开SecureCRT，设置COM5串口属性，选择“文件”→“快速连接”，属性值配置如图 1-2所示。

图 1-2 新建连接

3. 单击“连接”按钮，如果连接正常，输入用户名和密码（初始用户名为admin，密码为12345），如图 1-3所示。

图 1-3 通过Console串口成功登录交换机

1.1.2 通过带外口Telnet方式登录交换机

Telnet支持用户本地和远程登录，易于设备维护。

组网环境

使用带外口登录：请使用网线直连或通过Hub连接PC与高端交换机主用主控板卡的带外口，如图 1-4所示。

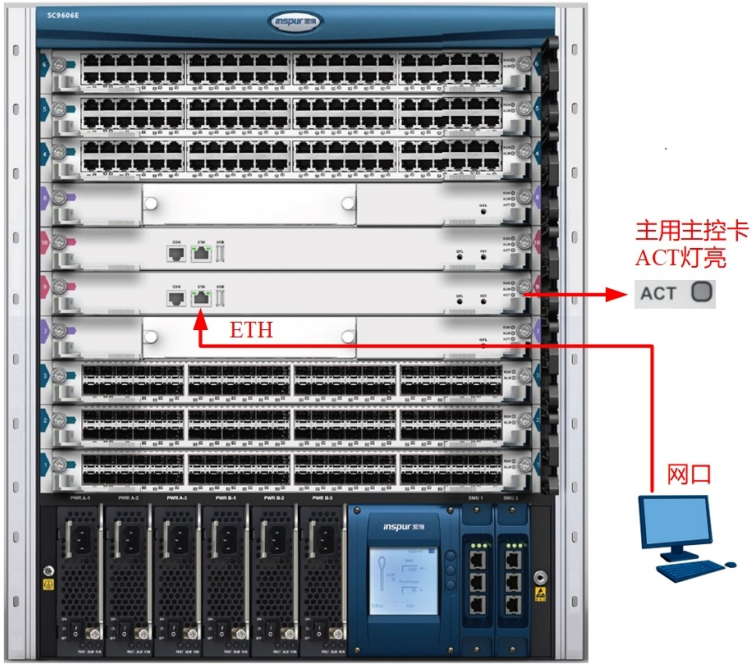


图 1-4 通过带外口Telnet登录SC9600E高端交换机

前置准备

在配置用户通过Telnet登录SC9600E高端交换机之前，需要完成以下任务：

- SC9600E高端交换机已烧录了正确的OS和BIOS版本。
- 已通过Console口登录设备完成Telnet服务及用户设置。

1. 输入用户名和密码（初始用户名为admin，密码为12345），登录SC9600E高端交换机。

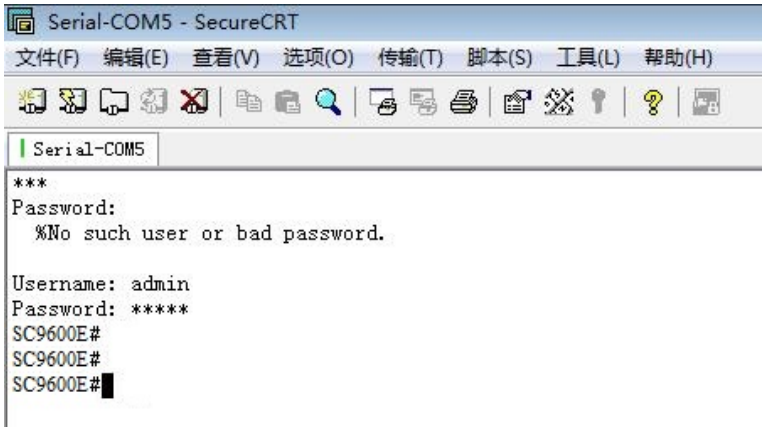


图 1-5 Console口方式登录SC9600E高端交换机

2. 配置带外口ETH。

1) 配置SC9600E高端交换机ethernet 0/0/0的IP地址。

2) 配置ETH端口**no shutdown**，以供Telnet用户访问。

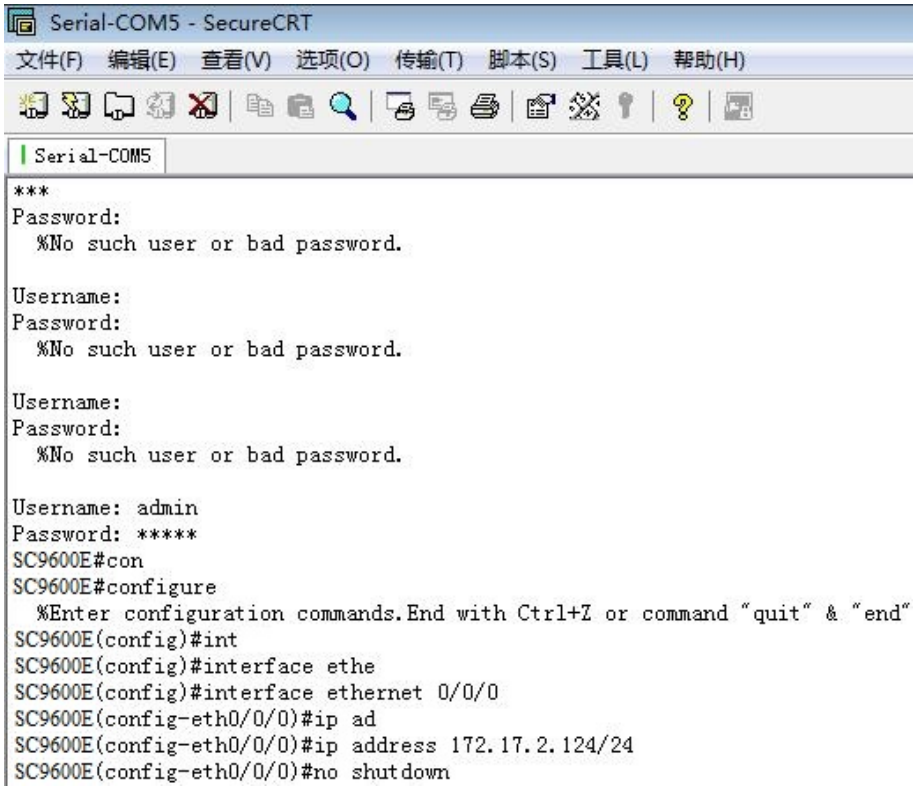


图 1-6 配置SC9600E高端交换机带外口ETH的IP地址

操作步骤

1. 在Windows环境下，打开SecureCRT，单击“文件”→“快速连接”，设置如下。
   - 协议：选择Telnet；
   - 主机名：输入带外口IP地址或管理VLAN的IP地址；
   - 端口：默认值23；
   - 防火墙：无。

图 1-7 Telnet登录连接

2. 单击“连接”按钮，启动Telnet客户端。如果网络连接正常，输入用户名和密码（初始用户名为admin，密码为12345）。

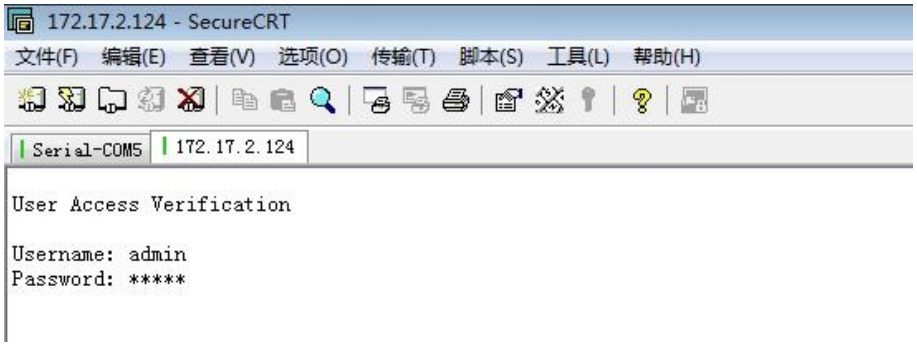


图 1-8 Telnet登录高端交换机

1.1.3 通过带内口Telnet方式登录交换机

Telnet支持用户本地和远程登录，易于设备维护。

组网环境

使用带内口登录：PC通过网络与SC9600E高端交换机互通，如图 1-9所示。

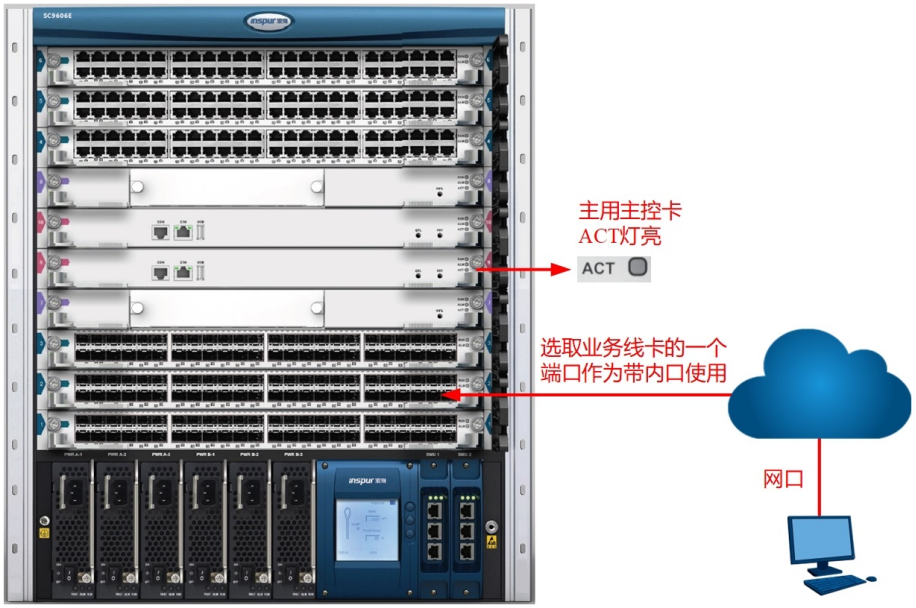


图 1-9 通过带内口Telnet登录SC9600E高端交换机

前置准备

在配置用户通过Telnet登录SC9600E高端交换机之前，需要完成以下任务：

- SC9600E高端交换机已烧录了正确的OS和BIOS版本。
- 终端与设备之间路由可达。
- 已通过Console口登录设备完成Telnet服务及用户设置。

1. 输入用户名和密码（初始用户名为admin，密码为12345），登录SC9600E高端交换机；

图 1-10 Console口方式登录SC9600E高端交换机

2. 配置带内口。

   1) 配置SC9600E高端交换机管理VLAN的IP地址。

   2) 将业务线卡上一个端口（以XGE4/0/47为例）以access模式加入管理VLAN。

   3) 配置端口**no shutdown**，以供Telnet用户访问。

```
SC9600E(config)#interface vlan 100
SC9600E(config-vlan-100)#ip address 10.18.12.12/24
SC9600E(config-vlan-100)#quit
SC9600E(config)#interface xgigaethernet 4/0/47
SC9600E(config-xge4/0/47)#port link-type access
SC9600E(config-xge4/0/47)#port default vlan 100
SC9600E(config-xge4/0/47)#no shutdown
SC9600E(config-xge4/0/47)#quit
SC9600E(config)#
```

图 1-11 配置SC9600E高端交换机管理VLAN的IP地址（带内口）

操作步骤

1. 在Windows环境下，打开SecureCRT，单击“文件”→“快速连接”，设置如下。

   - 协议：选择Telnet；
   - 主机名：输入带外口IP地址或管理VLAN的IP地址；
   - 端口：默认值23；
   - 防火墙：无。

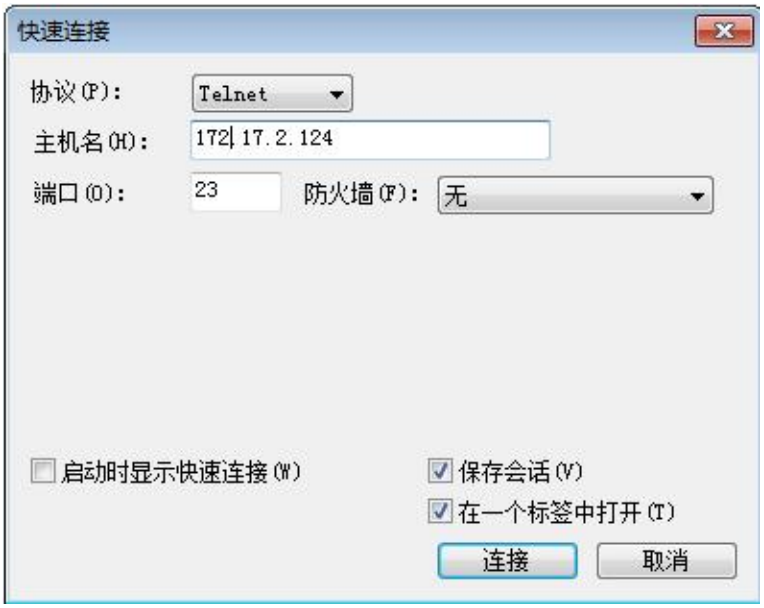


图 1-12 Telnet登录连接

2. 单击“连接”按钮，启动Telnet客户端。如果网络连接正常，输入用户名和密码（初始用户名为admin，密码为12345）。

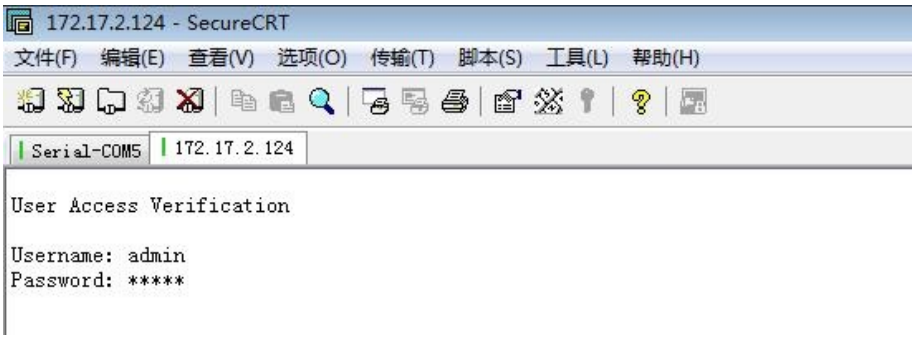


图 1-13 Telnet登录高端交换机

1.2 配置接口

接口是SC9600E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。

1.2.1 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SC9600E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

SC9600E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接口	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接口	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。

1.2.2 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SC9600E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

SC9600E高端交换机目前支持物理接口包括：

- Console接口
- ETH接口
- GE（Gigabit Ethernet）接口
- 10GE 接口
- 40GE接口

1.3 基本配置

1.3.1 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
- 更新系统或配置文件
- 日志配置命令
- 配置访问控制列表

1.3.1.1 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**reboot**命令来复位。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，而直接在远程就可以重启设备。该命令可导致网络工作在短时间内瘫痪，在一般情况下，禁止使用。

另外在重启设备时，要确认配置文件是否需要保存，如需保存，请在用户视图下执行**write file**配置，然后执行命令**y**。

过程

目的	步骤
复位交换机	1. 在特权用户模式下执行命令**reboot**； 2. 执行命令**y**。

1.3.1.2 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 get**命令把所要升级的文件下载到设备中。该命令应在技术人员的指导下使用。

过程

更新系统或配置文件的步骤如下所示，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
升级系统文件或配置文件	1. 进入全局配置视图； 2. 执行命令**upgrade { os | config }**。

1.3.1.3 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

配置访问控制列表的过程如下表所示，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
使能或者配置访问控制列表	1. 进入全局配置视图； 2. 执行如下命令： ▶ **management acl enable** ▶ **management acl IPV4-ADDRESS** ▶ **management acl IPV4-ADDRESS/M** ▶ **management acl IPV4-ADDRESS IPV4-ADDRESS-MASK** ▶ **management acl IPV4-ADDRESS IPV4-ADDRESS-MASK (telnet | snmp | ssh | tftp | ftp | all)** ▶ **management acl IPV4-ADDRESS/M (telnet | snmp | ssh | tftp | ftp | all)**
取消使能或者取消配置访问控制列表	1. 进入全局配置视图； 2. 执行如下命令： ▶ **management acl disable** ▶ **no management acl IPV4-ADDRESS/M** ▶ **no management acl IPV4-ADDRESS IPV4-ADDRESS-MASK** ▶ **no management acl IPV4-ADDRESS IPV4-ADDRESS-MASK (telnet | snmp | ssh | tftp | ftp | all)** ▶ **no management acl IPV4-ADDRESS/M (telnet | snmp | ssh | tftp | ftp | all)**

1.3.2 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。

1.3.2.1 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
设置交换机的系统名	1. 进入全局配置视图； 2. 执行命令**hostname HOST-NAME**。
恢复交换机系统名的缺省值	1. 进入全局配置视图； 2. 执行命令**no hostname**。

1.3.2.2 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见下表，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
设置系统时钟	1. 进入全局配置视图； 2. 执行如下命令： ▶ **clock set HH:MM:SS YYYY/MM/DD** ▶ **clock set HH:MM:SS DD MM YYYY**

1.3.2.3 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

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
设置夏令时	1. 进入全局配置视图； 2. 执行如下命令： ▶ **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	1. 进入全局配置视图； 2. 执行命令**no clock summer-time**。

1.3.2.4 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如下所示，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
设置本地时区信息	1. 进入全局配置视图； 2. 执行命令**clock timezone TIME-ZONE-NAME（add | minus）OFFSET**。

1.3.3 显示系统基本信息

1.3.3.1 显示设备管理运行信息

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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
显示当前生效的系统配置参数	1. 进入特权用户视图、全局配置视图、普通用户视图； 2. 执行如下命令： ▶ **show running-config** ▶ **show running-config include-default**

1.3.3.2 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所示。

目的	步骤
查看当前配置视图下的所有可用命令	1. 进入当前配置视图； 2. 执行命令**list**。

1.3.3.3 显示用户所用过的历史命令

目的

本节介绍如何查看用户所用过的历史命令。

过程

查看用户所用过的历史命令步骤如下所示。

目的	步骤
显示用户所用过的历史命令	1. 进入普通用户视图、特权用户视图或者全局配置视图； 2. 执行命令**show history**。

1.3.3.4 显示系统版本信息

目的

本节介绍如何显示系统版本信息。

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所示。

目的	步骤
显示系统当前的软硬件版本号、编译时间、内存大小等信息	1. 进入普通用户视图、特权用户视图或者全局配置视图； 2. 执行命令**show version**。

1.3.3.5 查看当前时间和设备已经运行的时间

目的

本节介绍用户如何查看当前时间和设备已经运行的时间。

过程

查看当前时间和设备已经运行的时间的步骤如下所示，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
显示当前时间和设备已经运行的时间	1. 进入普通用户视图、特权用户视图或者全局配置视图； 2. 执行如下命令： ▶ **show clock**

1.3.3.6 查看当前登录用户的个数

目的

本节介绍如何查看当前登录用户的个数。

过程

查看当前登录用户的个数的步骤如下所示。

目的	步骤
显示当前登录用户的个数	1. 进入普通用户视图、特权用户视图或者全局配置视图； 2. 执行命令**show login-type count**。

1.3.3.7 查看SC9600E的电源状态

目的

本节介绍如何查看SC9600E的电源状态。

过程

查看SC9600E的电源状态的步骤如下所示。

目的	步骤
查看电源状态	1. 进入特权用户视图、全局配置视图、普通用户视图、接口组配置视图、接口配置视图； 2. 执行命令**show power**。

1.3.3.8 查看MAC地址信息

目的

本节介绍如何查看SC9600E的默认MAC地址信息和正在使用的MAC地址信息。

过程

查看SC9600E的默认MAC地址信息和正在使用的MAC地址信息的步骤如下所示。

目的	步骤
查看默认MAC地址信息和正在使用的MAC地址信息	1. 进入普通用户视图、特权用户视图或者全局配置视图； 2. 执行命令**show system**。

1.3.3.9 查看访问控制列表的配置信息

目的

本节介绍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所示。

目的	步骤
查看访问控制列表的配置信息	1. 进入普通用户视图、特权用户视图或者全局配置视图； 2. 执行命令**show management acl**。

1.3.4 密码管理配置

SC9600E系列数据中心交换机能够向用户提供密码管理功能，在登录SC9600E系列数据中心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录系统，登录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，命令行显示为明文，配置文件中显示为密文。

1.3.4.1 分配用户权限

目的

本节介绍了登录SC9600E后，如何增加用户名及其权限和密码。

SC9600E对登录用户划分为4种等级，如表 1-1所示。隶属于Administrators组中的用户才有权限新增用户。

表 1-1 SC9600E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。
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，sntp，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无法查询到一些比较重要的显示信息，如**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。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
增加用户名及其权限和密码	1. 进入全局配置视图； 2. 执行命令**username USERNAME group（administrators | operators | users | guests）password PASSWORD**。
删除用户名及其权限和密码	1. 进入全局配置视图； 2. 执行命令**no username USERNAME**。
修改当前登录用户的密码	1. 进入普通用户视图、特权用户视图或者全局配置视图； 2. 执行命令**password PASSWORD**。

1.3.4.2 用户权限配置举例

组网需求

一台PC同一台SC9600E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

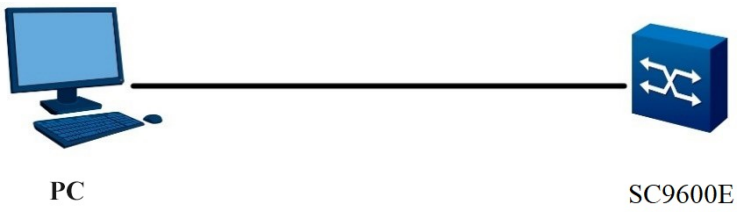


图 1-14 用户权限配置示例

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Administrators，密码为Admin123456的缺省用户。

配置步骤如下：

```
SC9600E#config
SC9600E(config)#username 123 group Administrators password Admin123456
#退出登录
SC9600E(config)#quit
SC9600E#quit
#用前面配置的用户名123，密码Admin123456可以登录成功
Uername：123
Password：***********
SC9600E#
```

1.3.5 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调试信息
- 设置虚拟终端的的登录方式
- 设置虚拟终端的超时时间

1.3.5.1 设置终端接收调试信息的功能开关

目的

本节介绍如何打开或者关闭命令行终端接收调试信息的功能。

过程

打开或者关闭命令行终端接收调试信息的步骤如下所示。

目的	步骤
打开命令行终端接收调试信息	1. 进入line配置视图； 2. 执行命令**monitor**。
关闭命令行终端接收调试信息	1. 进入line配置视图； 2. 执行命令**no monitor**。

1.3.5.2 用户进入或取消终端配置

目的

本节介绍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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
进入终端配置模式	1. 进入全局配置视图、line配置视图； 2. 执行命令**line vty VTY-NUMBER1 VTY-NUMBER2**。
取消终端配置	1. 进入全局配置视图、line配置视图； 2. 执行命令**no line vty VTY-NUMBER**。

1.3.5.3 进入串口终端配置视图

目的

本节介绍如何进入串口终端配置视图。

过程

配置进入串口终端配置视图的步骤如下所示，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
进入串口终端配置视图	1. 进入全局配置视图、line配置视图； 2. 执行命令**line console NUMBER**。

1.3.5.4 关闭一个虚终端

目的

本节介绍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。

vty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或ssh登录设备。

过程

配置如何关闭一个虚终端的步骤如下所示，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
关闭一个虚终端	1. 进入全局配置视图； 2. 执行命令**kill vty VTY-NUMBER**。

1.3.5.5 配置终端显示命令行的行数

目的

本节介绍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的行数。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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置终端显示行的数目	1. 进入全局配置视图； 2. 执行命令**terminal length (0 | TERMINAL-LENGTH | default)**。
恢复缺省值	1. 进入全局配置视图； 2. 执行命令**no terminal length**。
临时配置终端显示行的数目	1. 进入全局配置视图； 2. 执行命令**terminal length (0 | TERMINAL-LENGTH) temporary**。
取消临时配置终端显示行的数目	1. 进入全局配置视图； 2. 执行命令**no terminal length temporary**。

1.3.5.6 配置终端显示的颜色

目的

本节介绍如何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	步骤
配置终端显示的颜色	1. 进入全局配置视图； 2. 执行命令**terminal color (gray | red | green | yellow | blue | purple | water | white)**。

1.3.5.7 配置终端显示的语言

目的

本节介绍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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置终端显示的语言	1. 进入全局配置视图； 2. 执行命令**line concole**或**line vty VTY-NUMBER**或**line vty VTY-NUMBER1 VTY-NUMBER2**。 3. 执行命令**language (chinese | english)**。

1.3.5.8 配置虚拟终端是否接收调试信息

目的

本节介绍如何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	步骤
设置虚拟终端是否接收调试信息	1. 进入特权用户视图； 2. 执行命令**terminal monitor**。
恢复缺省值	1. 进入特权用户视图； 2. 执行命令**no terminal monitor**。

1.3.5.9 设置虚拟终端的超时时间

目的

本节介绍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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
设置虚拟终端的超时时间	1. 进入全局配置视图； 2. 执行命令**line concole**或**line vty**。 3. 执行命令**timeout TIME**。
恢复缺省值	1. 进入全局配置视图； 2. 执行命令**line concole**或**line vty**。 3. 执行命令**no timeout**。

1.3.5.10 设置虚拟终端的无输入的超时时间

目的

本节介绍如何设置虚拟终端的无输入的超时时间。

过程

设置和恢复虚拟终端的无输入的超时时间的步骤如下所示，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
设置虚拟终端的无输入的超时时间	1. 进入全局配置视图； 2. 执行命令**terminal timeout TIME**。
恢复缺省值	1. 进入全局配置视图； 2. 执行命令**no terminal timeout**。

1.3.5.11 显示当前设备登录用户信息

目的

本节介绍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所示。

目的	步骤
显示当前设备登录用户信息	1. 进入特权用户视图、全局配置视图、普通用户视图； 2. 执行命令**show lines**。

1.3.6 配置用户权限

本节介绍了登录SC9600E后，如何管理和分配用户权限。

1.3.6.1 新增用户

目的

本节介绍了登录SC9600E后，如何新增用户。

SC9600E对登录用户划分为4种等级，如表 1-2所示。隶属于Administrators组中的用户才有权限新增用户。

表 1-2 SC9600E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。
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所示，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
增加用户	1. 进入全局配置视图； 2. 执行命令**username USERNAME group (administrators | operators | users | guests)**。

1.3.6.2 删除用户

目的

本节介绍了在SC9600E新增用户后，如果需要删除用户该如何操作。

隶属于Administrators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所示，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
删除用户	1. 进入全局配置视图； 2. 执行命令**no username USERNAME**。

1.3.6.3 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所示，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
查看已创建的本地用户的属性	1. 进入特权用户视图、全局配置视图； 2. 执行命令**show user config**。

1.3.6.4 配置不同的域实现管理用户的登录权限

目的

本节介绍了如何配置不同的域实现管理用户的登录权限。

过程

配置不同的域实现管理用户的登录权限的步骤如下，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置不同的域实现管理用户的登录权限	1. 进入全局配置视图； 2. 执行命令**username USERNAME domain (telnet | ssh | console | all)**。

1.3.6.5 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
提升用户的权限	1. 进入全局配置视图； 2. 执行命令**enable password level LEVEL-VALUE (cipher | plain) PASSWORD**配置权限提升密码； 3. 进入Line配置视图； 4. 执行命令**enable authentication local**使能enable认证功能； 5. 若用户使用低于配置的level权限用户登录时，进入特权用户视图； 6. 执行命令**enable LEVEL-VALUE**后提示输入密码； 7. 输入步骤2中配置的密码即可实现用户权限提升。

1.3.6.6 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所示，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
设置用户密码复杂度	1. 进入全局配置视图； 2. 执行命令**user pwd-complex (PWD-COMPLEX | default)**。

1.3.6.7 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所示，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
设置指定用户或者全局用户的密码长度	1. 进入全局配置视图； 2. 执行命令**user pwd-length (PWD-LENGTH | default)**。

1.3.6.8 设置指定用户登录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录系统失败的最多次数。

过程

设置指定用户登录系统失败的最多次数的步骤如下所示，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
设置指定用户登录系统失败的最多次数	1. 进入全局配置视图； 2. 执行命令**user fail-count FAIL-COUNT-TIME**。

1.3.6.9 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所示，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
设置用户重认证时间间隔	1. 进入全局配置视图； 2. 执行如下命令： ◆ **user reauth-interval REAUTH-INTERVAL-TIME** ◆ **username WORD reauth-interval REAUTH-INTERVAL-TIME**

1.3.6.10 设置用户的FTP路径

目的

本节介绍了如何设置用户的FTP路径。

过程

设置用户的FTP路径的步骤如下所示，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
设置用户的FTP路径	1. 进入全局配置视图； 2. 执行命令**username USERNAME ftp-directory (DIR | default)**设置用户的FTP路径。

1.3.6.11 配置Telnet、SSH和FTP

目的

本节介绍了如何配置Telnet、SSH和FTP。

过程

配置Telnet、SSH和FTP的步骤如下所示，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
设置Telnet、SSH和FTP用户登录系统的最大并发数	1. 进入全局配置视图； 2. 执行命令**user (telnet | ssh) max-count (COUNT-NUMBER | default)**。
打开或关闭SSH文件传输协议调试功能	1. 进入特权用户视图； 2. 执行如下命令： ▶ **debug sftp** ▶ **no debug sftp**
使能或去使能SSH文件传输协议服务	1. 进入全局配置视图； 2. 执行命令**sftp-server (enable | disable)**。
开启设备的SSH功能	1. 进入全局配置视图； 2. 执行如下命令： ▶ **sshd** ▶ **no sshd**
配置SSHD认证方式（包括密码认证和公钥认证）	1. 进入全局配置视图； 2. 执行如下命令： ▶ **sshd auth (password | pubkey)** ▶ **no sshd auth (password | pubkey)**
配置SSHD登录闲置时间	1. 进入全局配置视图； 2. 执行命令**sshd login-grace-time (LOGIN-GRACE-TIME | default)**。

目的	步骤
配置密匙字符串	1. 进入全局配置视图； 2. 执行如下命令： ▶ **key (ssh-dss | ssh-rsa) KEY-STRING** ▶ **key KEY-STRING**
创建公钥	1. 进入全局配置视图； 2. 执行如下命令： ▶ **ssh keygen dsa** ▶ **ssh keygen rsa bits (1024 | 2048 | 3072)**
配置SSH用户密匙	1. 进入全局配置视图； 2. 执行命令**ssh user USER-NAME key begin**。
显示SSH配置信息	1. 进入普通用户视图； 2. 执行命令**show ssh config**。

1.3.6.12 查询用户权限

目的

本节介绍如何查询用户权限。

过程

查询用户权限的步骤如下所示。

目的	步骤
查询用户权限	1. 进入普通用户视图、特权用户视图或全局配置视图； 2. 执行命令**show privilege**查询用户权限。

1.3.7 带内带外网管配置

1.3.7.1 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置带内网管	1. 进入全局配置视图； 2. 进入VLANIF配置视图、Loopback接口配置视图、以太网路由接口配置视图、以太网子接口配置视图、grp路由接口配置视图； 3. 执行如下命令配置带内IP地址： ▶ **ip address IP-ADDRESS/MASK-LENGTH**

1.3.7.2 带外网管配置

目的

本节介绍如何配置带外网管。

注意：

带外IP地址与带内IP地址不能为同网段IP。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置带外网管	1. 进入全局配置视图； 2. 进入带外口配置视图； 3. 执行如下命令配置带外IP地址： ▶ **ip address IP-ADDRESS/MASK-LENGTH**

1.4 系统配置文件操作

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

1.4.1 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所示，参数说明请参考《SC9600E系列交换机命令行手册》。

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**mkdir DIRECTORY**。
删除目录	在特权用户视图或全局配置视图下执行命令**rmdir DIRECTORY**。
显示当前的工作目录	在特权用户视图或全局配置视图下执行命令**pwd**。
改变当前目录	在特权用户视图或全局配置视图下执行命令**cd DIRECTORY**。
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**ls tree DIRECTORY**； 或者在特权用户视图或全局配置视图下执行命令**ls tree DIRECTORY subtree**。

1.4.2 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所示，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
删除文件	在特权用户视图下执行命令**del FILE-NAME**。
永久删除文件	在特权用户视图下执行命令**remove FILENAME**。
重命名文件	在特权用户视图下执行命令**rename OLD-FILENAME NEW-FILENAME**。
拷贝文件夹	在特权用户视图下执行命令**xcopy SRCFILE DESTFILE**。
拷贝文件	在特权用户视图下执行命令**copy SRCFILE DESTFILE**。
显示指定二进制text文件的内容	在特权用户视图下执行命令**type FILENAME (binary | text)**。
清空指定文件的内容	在特权用户视图下执行命令**zero FILENAME**。

1.4.3 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。

1.4.3.1 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. 进入全局配置视图；
2. 执行命令**auth-degenerate**。

1.4.3.2 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. 进入普通用户视图或全局配置视图；
2. 执行命令**write file**。

1.4.3.3 升级及查看系统文件

目的

本节介绍如何升级及查看系统文件。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
更新系统或配置文件	在全局配置视图下执行命令**upgrade (os | config | backup-os) [LOCAL-FILE-NAME]**。
整包升级系统文件	在全局配置视图下执行命令**upgrade os slot (SLOT-ID | group SLOTLIST | self) whole-packet**。
查看单盘升级信息	在普通用户视图下执行命令**show upgrade card-packet info**。
查看整包升级信息	在普通用户视图下执行命令**show upgrade whole-packet info**。

1.4.3.4 查看及删除OS文件

目的

本节介绍如何查看或删除交换机内存里存储的OS文件。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
查看交换机内存里存储的OS文件	1. 进入普通用户视图； 2. 执行命令**show os-file**。
删除交换机内存里存储的所有OS文件或指定文件名的OS文件	1. 进入全局配置视图； 2. 执行如下命令： ▶ **del os-file** ▶ **del os-file NAME**

1.5 设备文件上传及下载

1.5.1 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，用户成功登录交换机后，进入config节点，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，输入ftp get/put X.X.X.X USERNAME PASSWORD FILENAME（X.X.X.X代表远程FTP Server的IP地址）命令，即可对文件进行上传和下载。

本设备支持IPv4网络地址下的FTP功能。

1.5.1.1 启动和关闭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	步骤
启动服务器	1. 进入全局配置视图； 2. 执行命令**ftpd**。
关闭服务器	1. 进入全局配置视图； 2. 执行命令**no ftpd**。

1.5.1.2 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）。

1.5.1.3 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。

设备	配置
Switch	启动FTP Server，并做了用户名、密码等相关配置。
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上做了如下配置：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 1-15　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。

```
SC9600E#config
SC9600E(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。

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。

```
SC9600E#config
SC9600E(config)#upgrade os
SC9600E(config)#quit
SC9600E#reboot
```

1.5.1.4 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
Switch	可以直接使用**ftp**命令登录远端的FTP Server。	用户首先获取FTP用户名和密码，然后登录远端的FTP Server，这样才能取得相应目录和文件。 ◆ **ftp get IPV4-ADDRESS USER PASSWORD REMOTEFILE [PORT-ID]** ◆ **ftp get IPV4-ADDRESS USER PASSWORD REMOTEFILE localfile FILENAME [PORT-ID]** ◆ **ftp put IPV4-ADDRESS USER PASSWORD REMOTEFILE config** ◆ **ftp put IPV4-ADDRESS USER PASSWORD REMOTEFILE localfile FILENAME [PORT-ID]** ◆ **ftp put IPV4-ADDRESS USER PASSWORD REMOTEFILE running-config [PORT-ID]**
PC	启动FTP Server，并做了用户名、密码、用户的权限等相关配置。	

组网需求

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SC9600E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

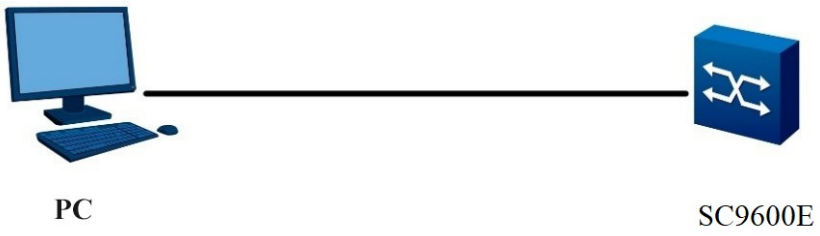


图 1-16　交换机作为FTP client配置组网图

配置步骤

1. 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。

```
SC9600E#config
SC9600E(config)#ftp get 10.18.1.2 123 123 d:\upgrade.z
   Local path is “Ram:/flash/download”.
   Getting data...
 3069212 bytes downloaded
```

2. 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。

```
SC9600E(config)#upgrade os

WARNING:System will upgrade! Continue?[ y/n]
  System now is upgrading,please wait.
  %Local path is “Ram:/flash/download”.
SC9600E(config)#reboot
```

注意：

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。

1.5.2 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器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，并且确保客户端和服务器之间可达。

本设备支持IPv4网络地址下的TFTP功能。

图 1-17 TFTP配置示意图

1.5.2.1 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	步骤
启动设备的TFTP Server功能	1. 进入全局配置视图； 2. 执行命令**tftpd**启动设备的TFTP Server功能。
关闭设备的TFTP Server功能	1. 进入全局配置视图； 2. 执行命令**no tftpd**关闭设备的TFTP Server功能。

1.5.2.2 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
通过TFTP下载远程文件并存储在本地（适用于IPv4）	1. 进入全局配置视图； 2. 执行如下命令： ▶ **tftp get (IPV4-ADDRESS | MAC-ADDRESS) REMOTEFILE [PORT-ID]** ▶ **tftp get (IPV4-ADDRESS | MAC-ADDRESS) REMOTEFILE localfile FILENAME [PORT-ID]** ▶ **tftp get IPV4-ADDRESS vpn-instance NAME REMOTEFILE [PORT-ID]** ▶ **tftp get IPV4-ADDRESS vpn-instance NAME REMOTEFILE localfile FILENAME [PORT-ID]**
使用TFTP协议一键导出文件	1. 进入全局配置视图； 2. 执行命令**file export tftp IPV4-ADDRESS REMOTEDIR LOCALDIR**。

1.5.2.3 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。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
将本地文件上传到远程TFTP Server（适用于IPv4）	1. 进入全局配置视图； 2. 执行如下命令： ▶ **tftp put IPV4-ADDRESS REMOTEFILE running-config [PORT-ID]** ▶ **tftp put (IPV4-ADDRESS | MAC-ADDRESS) REMOTEFILE config** ▶ **tftp put (IPV4-ADDRESS | MAC-ADDRESS) REMOTEFILE localfile FILENAME [PORT-ID]** ▶ **tftp put IPV4-ADDRESS vpn-instance NAME REMOTEFILE config** ▶ **tftp put IPV4-ADDRESS vpn-instance NAME REMOTEFILE localfile FILENAME [PORT-ID]**
开启设备的IPv4 Telnet服务功能	1. 进入全局配置视图； 2. 执行命令**telnetd**开启设备的IPv4 Telnet服务功能。
关闭设备的IPv4 Telnet服务功能	1. 进入全局配置视图； 2. 执行命令**no telnetd**关闭设备的IPv4 Telnet服务功能。
使能IPv4版本的Telnet服务器	1. 进入全局配置视图； 2. 执行命令**telnetd port [PORT-NUMBER | default]**使能IPv4版本的Telnet服务器。

目的	步骤
使能IPv6版本的Telnet服务器	1. 进入全局配置视图； 2. 执行命令**telnet6d port [PORT-NUMBER | default]**使能IPv6版本的Telnet服务器。
使用TFTP协议将设备默认文件夹的内容导出到PC中	1. 进入全局配置视图； 2. 执行命令**file export tftp IPV4-ADDRESS REMOTEDIR LOCALDIR**。

1.5.2.4 TFTP Client配置实例

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

交换机作为TFTP Client实现配置文件的备份和和软件升级配置举例。

设备	配置	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器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，并做了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 1-18 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. 在交换机上配置。

   #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。

```
SC9600E#config
SC9600E(config)#tftp get 1.1.1.2  switch.z
SC9600E(config)#tftp put 1.1.1.2  vrpcfg.txt config
```

2 二层以太网配置

本章介绍了SC9600E系列数据中心交换机二层以太网基本功能配置。

2.1 以太网接口配置

本小节介绍如何配置以太网接口。

2.1.1 以太网接口基本属性配置

2.1.1.1 进入以太网接口视图

背景信息

要对以太网接口进行配置，首先要进入以太网接口视图。本节介绍如何进入以太网接口视图。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
进入以太网接口视图	1. 进入全局配置视图； 2. 执行如下命令： ▶ **interface (ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 40gigaethernet) INTERFACE-NUMBER** ▶ **interface eth-trunk TRUNK-NUMBER**
退出以太网接口视图	1. 进入接口配置视图； 2. 执行命令**quit**。

目的	步骤
进入批量接口配置视图	1. 进入全局配置视图； 2. 执行命令**interface (ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 40gigaethernet) INTERFACE-NUMBER to (ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 40gigaethernet) INTERFACE-NUMBER**。
进入接口组配置视图	1. 进入全局配置视图； 2. 执行命令**interface group PORT-LIST**。

2.1.1.2 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，端口为打开状态。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《SC9600E系列交换机命令行手册》。

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**shutdown**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. 进入全局配置视图； 2. 进入接口配置视图（以太网、Trunk）、接口组配置视图、批量接口配置视图、VLANIF配置视图； 3. 执行命令**shutdown**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**shutdown**和**no shutdown**命令关闭和重启接口，使新配置生效。	1. 进入全局配置视图； 2. 进入接口配置视图（以太网、Trunk）、接口组配置视图、批量接口配置视图、VLANIF配置视图； 3. 执行命令**no shutdown**开启当前以太网。

2.1.1.3 设置以太网端口速率

背景信息

可以使用如下命令对以太网端口的速率进行设置。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置以太网接口速率	1. 进入全局配置视图； 2. 执行命令**port mode 10gi interface 10gigaethernet INTERFACE-NUMBER**设置端口的不同速率。

2.1.1.4 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。可以使用如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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
开启以太网端口流量控制	1. 进入全局配置视图； 2. 进入接口配置视图（以太网接口）、接口组配置视图； 3. 执行命令**flow-control enable**。
关闭以太网端口流量控制	1. 进入全局配置视图； 2. 进入接口配置视图（以太网接口）、接口组配置视图； 3. 执行命令**flow-control disable**。

2.1.1.5 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/未知单播报文。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
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. 进入全局配置视图； 2. 进入接口配置视图（以太网接口、Trunk接口）、接口组配置视图和批量接口配置视图； 3. 执行如下命令： ▶ **storm-control (broadcast | multicast | dlf) cir (gbps | kbps | mbps) CIR-VALUE cbs (bytes | kbytes | mbytes) CBS-VALUE** ▶ **storm-control (broadcast | multicast | dlf) percent VALUE**（只支持以太网接口配置视图） ▶ **storm-control (broadcast | multicast | dlf) pps PPS-VALUE**
取消风暴控制功能	1. 进入全局配置视图； 2. 进入接口配置视图（以太网接口、Trunk接口）、接口组配置视图和批量接口配置视图； 3. 执行命令**no storm-control (broadcast | multicast | dlf)**。

2.1.1.6 设置以太网端口速率抑制功能

背景信息

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

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置以太网端口速率抑制功能	1. 进入全局配置视图； 2. 进入以太网桥接接口配置视图、以太网路由接口配置视图； 3. 执行命令**rate-limit (in | out) percent PERCENT**。
配置合理的带宽告警门限与恢复告警门限	1. 进入全局配置视图； 2. 进入以太网桥接接口配置视图、以太网路由接口配置视图； 3. 执行如下命令： ▶ **rate-limit (in | out) threshold (THRESHOLD-VALUE | default)** ▶ **rate-limit (in | out) threshold (THRESHOLD-VALUE | default) resume-threshold (RESUME-THRESHOLD-VALUE | default)**
取消以太网端口速率抑制功能	1. 进入全局配置视图； 2. 进入以太网桥接接口配置视图、以太网路由接口配置视图、Trunk接口配置视图； 3. 执行命令**no rate-limit (in | out)**。

2.1.1.7 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。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
设置以太网端口的最大传输单元	1. 进入全局配置视图； 2. 进入接口配置视图（以太网接口、Trunk接口）； 3. 执行命令**mtu (MTU-VALUE | default)**。

2.1.1.8 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。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
清除当前接口的统计信息	1. 进入全局配置视图； 2. 进入接口配置视图（以太网接口、Trunk接口）； 3. 执行命令**reset counter**。

2.1.1.9 清除指定接口的统计信息

目的

本操作适用于清除指定接口的统计信息。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
清除指定接口统计信息	1. 进入全局配置视图； 2. 执行如下命令清除指定接口统计信息： ▶ **reset counter interface eth-trunk TRUNK-NUMBER** ▶ **reset counter interface eth-trunk TRUNK-NUMBER.SUB-TRUNK-NUMBER** ▶ **reset counter interface bridge-domain BD-ID** ▶ **reset counter interface (ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 40gigaethernet) INTERFACE-NUMBER** ▶ **reset counter interface all**

2.1.1.10 描述以太网端口

目的

使用如下命令设置端口的描述字符串，以区分各个端口。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
设置以太网端口描述字符串	1. 进入全局配置视图； 2. 进入接口配置视图（以太网接口、Trunk接口）、VLANIF配置视图； 3. 执行命令**alias DESCRIPTION**。
删除以太网端口描述字符串	1. 进入全局配置视图； 2. 进入接口配置视图（以太网接口、Trunk接口）、VLANIF配置视图； 3. 执行命令**no alias**。

2.1.2 以太网接口高级属性配置

2.1.2.1 配置端口CRC检测

目的

使用以下的配置任务可以开启CRC错误报文超过阈值时，自动关断端口，保持关断状态一段时间后，再打开端口。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
使能或去使能CRC错误报文超过阈值时，端口error down	1. 进入以太网桥接接口配置视图、以太网路由接口配置视图、grp桥接接口配置视图、grp路由接口配置视图； 2. 执行命令**port crc-error error-down (enable | disable)**。
配置CRC错误报文告警时间间隔	1. 进入全局配置视图； 2. 执行命令**crc-error protection interval INTERVAL**。
配置端口CRC错误报文告警阈值	1. 进入以太网桥接接口配置视图、以太网路由接口配置视图、grp桥接接口配置视图、grp路由接口配置视图； 2. 执行命令**port crc-error threshold THRESHOLD**。
配置CRC错误报文超过阈值时，端口error down后的自动恢复时间	1. 进入全局配置视图； 2. 执行命令**error-down auto-recovery cause crc-error interval INTERVAL**。
配置CRC错误报文超过阈值时，端口error down后不再自动恢复	1. 进入全局配置视图； 2. 执行命令**no error-down auto-recovery cause crc-error**。
关闭端口CRC错误报文的告警检测	1. 进入以太网桥接接口配置视图、以太网路由接口配置视图、grp桥接接口配置视图、grp路由接口配置视图； 2. 执行命令**no port crc-error threshold**。
关闭CRC错误报文的告警检测	1. 进入全局配置视图； 2. 执行命令**no crc-error protection interval**。
查看CRC校验错误配置	1. 进入普通用户视图； 2. 执行命令**show crc-error config**。

2.1.2.2 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
显示以太网端口状态及相关信息	1. 进入特权用户视图、全局配置视图、普通用户视图、接口配置视图（以太网接口、trunk接口）、接口组配置视图； 2. 执行如下命令： ▶ **show interface** ▶ **show interface (ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 40gigaethernet) INTERFACE-NUMBER** ▶ **show interface (ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 40gigaethernet) INTERFACE-NUMBER config** ▶ **show interface eth-trunk TRUNK-NUMBER** ▶ **show interface eth-trunk TRUNK-NUMBER config**
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	1. 进入特权用户视图、全局配置视图、普通用户视图、接口配置视图（以太网接口、trunk接口）、接口组配置视图； 2. 执行如下命令： ▶ **show interface eth-trunk TRUNK-NUMBER verbose** ▶ **show interface eth-trunk verbose** ▶ **show interface verbose**

2.2 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。

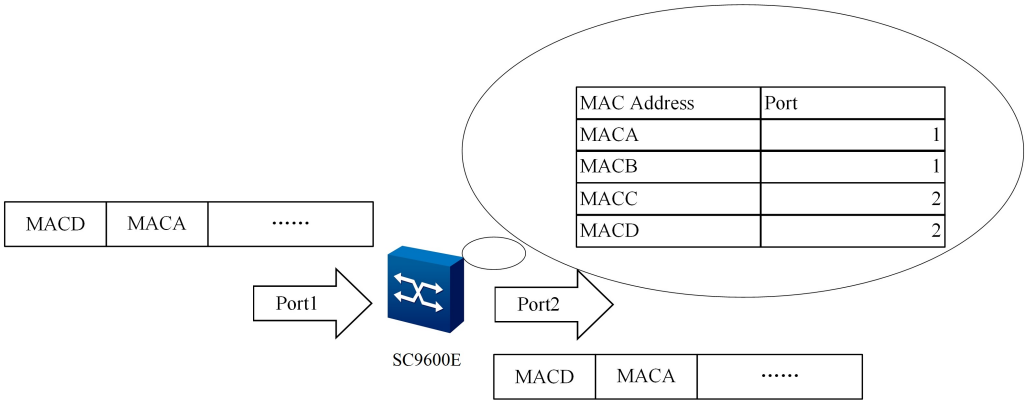


图 2-1 交换机利用转发表转发报文

2.2.1 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
添加黑洞MAC地址表项	1. 进入全局配置视图； 2. 执行命令**mac-address blackhole VLAN-ID MAC-ADDRESS**。
删除黑洞MAC地址表项	1. 进入全局配置视图； 2. 执行如下命令： ▶ **no mac-address blackhole** ▶ **no mac-address blackhole MAC-ADDRESS** ▶ **no mac-address blackhole vlan VLAN-ID** ▶ **no mac-address blackhole vlan VLAN-ID MAC-ADDRESS**
配置系统最大MAC地址学习限制	1. 进入接口配置视图（以太网接口）、接口组配置视图、VLAN配置视图； 2. 执行如下命令： ▶ **mac-limit (LIMIT-VALUE | default)** ▶ **mac-limit (LIMIT-VALUE | default) action (forward | drop)**
添加设备静态MAC地址表项	1. 进入全局配置视图； 2. 执行如下命令： ▶ **mac-address static VLAN-ID MAC-ADDRESS (ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 40gigaethernet) INTERFACE-NUMBER** ▶ **mac-address static VLAN-ID MAC-ADDRESS eth-trunk TRUNK-NUMBER**

目的	步骤
删除设备上静态MAC地址表项	1. 进入全局配置视图（第一条命令也可进入槽位节点视图执行）； 2. 执行如下命令： ▶ **no mac-address static** ▶ **no mac-address static vlan VLAN-ID** ▶ **no mac-address static MAC-ADDRESS** ▶ **no mac-address static vlan VLAN-ID MAC-ADDRESS** ▶ **no mac-address static (ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 40gigaethernet) INTERFACE-NUMBER** ▶ **no mac-address static eth-trunk TRUNK-NUMBER**
删除全局所有MAC地址表项，或根据VLAN、VLAN+MAC以及端口的方式来删除指定接口下的所有MAC地址表项	1. 进入以太网桥接接口配置视图、Trunk接口配置视图； 2. 执行如下命令： ▶ **no mac-address** ▶ **no mac-address (dynamic | static | security | sticky)** ▶ **no mac-address (dynamic | static | security | sticky) vlan VLAN-ID** ▶ **no mac-address (dynamic | static | security | sticky) vlan VLAN-ID MAC-ADDRESS**

2.2.2 设置动态 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，参数说明请参考《SC9600E系列交换机命令行手册》。

提示：

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
设置MAC地址动态表项的老化时间	1. 进入全局配置视图； 2. 执行命令**mac aging-time AGING-TIME**。

2.2.3 配置 MAC 地址漂移检测

目的

该功能可以检测设备上所有的MAC地址是否发生了漂移。若发生漂移，设备会上报告警到网管系统。

背景信息

MAC地址漂移是指设备上一个VLAN内有两个或者三个端口学习到一个MAC地址，后学习到的MAC地址表项覆盖原MAC地址表项的现象。我们通常认为第一个学习到MAC地址的接口是正确的出接口，称为源端口（Original Port），后学习的端口是漂移端口（Move Port），漂移端口通常是在环路上的或者下挂网络中有环路的端口，需要关闭漂移端口或者在漂移端口上配置风暴抑制功能。

缺省情况下，系统会对交换机上所有VLAN进行MAC地址漂移检测。数据中心虚拟化应用场景（主要是指对于虚拟终端的迁移）也会造成MAC地址的漂移现象，但此时的漂移是正常的，这种情况不需要作为MAC地址漂移被检测出来。可以将虚拟终端所在的VLAN加入MAC地址漂移检测白名单，不对该VLAN进行检测。

如果用户修改MAC地址漂移表项的老化时间变长，会导致漂移再次发生，Error-Down的时间变长。为了能够正常检测到MAC地址漂移，可以修改漂移表项的老化时间。

用户网络中由于环路造成了MAC地址漂移，且网络不支持破环协议，可以在相应接口上配置发生MAC地址漂移后的处理动作来实现破环。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置MAC地址漂移检测功能的使能状态，默认为使能状态	1. 进入全局配置视图； 2. 执行命令**mac-address flapping detection (enable | disable)**。
配置MAC地址漂移表项的老化时间	1. 进入全局配置视图； 2. 执行命令**mac-address flapping aging-time (AGING-TIME | default)**。
设置全局MAC地址漂移检测功能	1. 进入全局配置视图； 2. 执行命令**mac-address flapping detection vlan VLAN-ID security-level (high | middle | low)**。
配置MAC地址漂移检测的VLAN白名单，即指定不检测的VLAN	1. 进入全局配置视图； 2. 执行命令**mac-address flapping detection exclude-vlan VLAN-ID**。
使能接口退出VLAN后自动加回该VLAN的功能，并设置接口自动加回VLAN的延时时间	1. 进入全局配置视图； 2. 执行命令**mac-address flapping quit-vlan recover-time (TIME | default)**。
配置使能接口状态自动恢复为UP状态的功能，并设置接口自动恢复为UP的延时时间	1. 进入全局配置视图； 2. 执行命令**error-down auto-recovery cause mac-address-flapping interval INTERVAL**。
配置关闭接口状态自动恢复为UP状态的功能	1. 进入全局配置视图； 2. 执行命令**no error-down auto-recovery cause mac-address-flapping**。
配置接口发生MAC地址漂移后的处理动作	1. 进入以太网桥接接口配置视图、Trunk接口配置视图； 2. 执行命令**mac-address flapping action (quit-vlan | error-down)**。
配置发生MAC地址漂移时接口动作的优先级	1. 进入以太网桥接接口配置视图、Trunk接口配置视图； 2. 执行命令**mac-address flapping action priority (PRIORITY | default)**。
关闭接口发生MAC地址漂移后的处理动作	1. 进入以太网桥接接口配置视图、Trunk接口配置视图； 2. 执行命令**no mac-address flapping action**。

目的	步骤
查看MAC地址漂移的活动记录和老化记录	1. 进入普通用户视图； 2. 执行命令**show mac-address flapping record**。
清除MAC地址漂移老化记录	1. 进入全局配置视图； 2. 执行命令**reset mac-address flapping record**。

2.2.4 配置 MAC 地址学习或老化的告警功能

目的

本节介绍如何配置MAC地址学习或老化的告警功能。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
使能MAC地址学习或老化的告警功能	1. 进入以太网桥接接口配置视图、Trunk接口配置视图； 2. 执行命令**mac-address notification (add | remove | all)**。
去使能MAC地址学习和老化的告警功能	1. 进入以太网桥接接口配置视图、Trunk接口配置视图； 2. 执行命令**no mac-address notification**。
配置设备对MAC地址发生学习或老化的告警条目最大数	1. 进入全局配置视图； 2. 执行命令**mac-address notification history-size HISTORY-SIZE**。
配置设备对MAC地址发生学习或老化的检查周期	1. 进入全局配置视图； 2. 执行命令**mac-address notification interval (INTERVAL-VALUE | default)**。
打开或关闭MAC地址学习功能	1. 进入以太网桥接接口配置视图、Trunk接口配置视图； 2. 执行命令**mac-learning (enable | disable)**。
配置接口禁止MAC地址学习功能后，接口所采取的对于二层数据包的动作	1. 进入以太网桥接接口配置视图、Trunk接口配置视图； 2. 执行命令**mac-learning disable action (forward | drop)**。
显示MAC地址学习或老化的告警条目	1. 进入普通用户视图； 2. 执行命令**show mac-address notification history**。
清除所有MAC地址学习或老化的告警条目	1. 进入全局配置视图； 2. 执行命令**reset mac-address notification history**。

2.2.5 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
显示指定项目的MAC地址的表项信息	1. 进入特权用户视图、全局配置视图、接口配置视图（以太网接口、trunk接口）、普通用户视图、接口组配置视图； 2. 执行如下命令： ▶ **show mac-address vlan VLAN-ID** ▶ **show mac-address vsi VSI-NAME** ▶ **show mac-address [MAC-ADDRESS]** ▶ **show mac-address MAC-ADDRESS vlan VLAN-ID** ▶ **show mac-address (ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 40gigaethernet) INTERFACE-NUMBER** ▶ **show mac-address eth-trunk TRUNK-NUMBER** ▶ **show mac-address (static | security | sticky)**
显示基于接口、基于VLAN或基于槽位的MAC地址数量信息	1. 进入特权用户视图、全局配置视图、普通用户视图、接口配置视图（以太网接口、trunk接口）、接口组配置视图； 2. 执行如下命令： ▶ **show mac-address total-number** ▶ **show mac-address total-number (ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 40gigaethernet) INTERFACE-NUMBER** ▶ **show mac-address total-number eth-trunk TRUNK-NUMBER** ▶ **show mac-address total-number vlan VLAN-ID**

目的	步骤
显示基于接口、基于VLAN的动态MAC地址表项信息	1. 进入特权用户视图、全局配置视图、普通用户视图、接口配置视图（以太网接口、trunk接口）、接口组配置视图； 2. 执行如下命令： ▶ **show mac-address dynamic (ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 40gigaethernet) INTERFACE-NUMBER** ▶ **show mac-address dynamic eth-trunk TRUNK-NUMBER** ▶ **show mac-address dynamic vlan VLAN-ID**
显示已配置的MAC地址学习限制规则	1. 进入特权用户视图、全局配置视图、普通用户视图、接口配置视图（以太网接口、trunk接口）、VLAN配置视图、接口组配置视图； 2. 执行如下命令： ▶ **show mac-limit** ▶ **show mac-limit interface** ▶ **show mac-limit interface (ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 40gigaethernet) INTERFACE-NUMBER** ▶ **show mac-limit interface eth-trunk TRUNK-NUMBER** ▶ **show mac-limit config** ▶ **show mac-limit vlan [VLAN-ID]** ▶ **show mac-limit bridge-domain [BD-ID]**

2.2.6 维护及调试

目的

当MAC相关功能不正常，需要进行查看、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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
打开或关闭MAM模块调试开关	1. 进入特权用户视图； 2. 执行命令**debug mam (error | mac | flush | mac-limit | sync | hw | nm | event | if | history | aging | all)**或**no debug mam (error | mac | flush | mac-limit | sync | hw | nm | event | if | history | aging | all)**。
查看MAC地址基本信息	1. 进入普通用户视图； 2. 执行命令**show mac info**。
查看MAC地址管理模块的各种错误统计信息	1. 进入普通用户视图； 2. 执行命令**show mam error**。
导出MAC管理模块记录的MAC表、接口表信息	1. 进入普通用户视图； 2. 执行命令**dump ha mac-table (mac | if | all)**导出MAC管理模块记录的MAC表、接口表信息。根据导出的信息判断设备两块主控卡上表项是否一致。

2.3 ARP 配置

ARP（Address Resolution Protocol，地址解析协议）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。

2.3.1 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
添加静态ARP映射表项	1. 进入全局配置视图； 2. 执行如下命令： ▶ **ip arp IP-ADDRESS MAC-ADDRESS (ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 40gigaethernet) INTERFACE-NUMBER** ▶ **ip arp IP-ADDRESS MAC-ADDRESS (ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 40gigaethernet) INTERFACE-NUMBER vpn-instance NAME** ▶ **ip arp IP-ADDRESS MAC-ADDRESS eth-trunk TRUNK-NUMBER** ▶ **ip arp IP-ADDRESS MAC-ADDRESS eth-trunk TRUNK-NUMBER vpn-instance NAME** ▶ **ip arp IP-ADDRESS MAC-ADDRESS vlan VLAN-ID** ▶ **ip arp IP-ADDRESS MAC-ADDRESS vlan VLAN-ID vpn-instance NAME** ▶ **ip arp IP-ADDRESS MAC-ADDRESS vlan VLAN-ID inner-vlan INNER-VID** ▶ **ip arp IP-ADDRESS MAC-ADDRESS vlan VLAN-ID inner-vlan INNER-VID vpn-instance NAME** ▶ **ip arp IP-ADDRESS MAC-ADDRESS** ▶ **ip arp IP-ADDRESS MAC-ADDRESS vpn-instance NAME**
删除静态ARP映射表项	1. 进入全局配置视图； 2. 执行如下命令： ▶ **no ip arp IP-ADDRESS** ▶ **no ip arp IP-ADDRESS vpn-instance NAME**

2.3.2 清除动态 ARP 表项

目的

本节介绍如何清除动态ARP映射表项，帮助用户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，可能导致暂时无法访问某些节点，用户需谨慎使用。

过程

清除动态ARP映射表项步骤如下。

目的	步骤
清除动态ARP映射表项	1. 进入全局配置视图； 2. 执行命令**flush arp dynamic**。

2.3.3 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，在一段时间后没有收到更新报文，则老化这种对应关系。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
显示当前所有VLAN的ARP学习模式	1. 进入普通用户视图； 2. 执行命令**show arp learning strict**。
显示ARP相关信息，包括ARP动态地址统计、ARP映射表项的老化时间等，同时也支持多实例VPN情况下配置	1. 进入普通用户视图； 2. 执行如下命令： ▶ **show ip arp** ▶ **show ip arp IP-ADDRESS** ▶ **show ip arp dynamic** ▶ **show ip arp static** ▶ **show ip arp (ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 40gigaethernet) INTERFACE-NUMBER** ▶ **show ip arp eth-trunk TRUNK-NUMBER** ▶ **show ip arp vpn-instance NAME**

2.3.4 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置动态ARP映射表项的老化时间	1. 进入全局配置视图； 2. 执行命令**ip arp aging-time (AGING-TIME | default)**。

2.3.5 配置 ARP 学习功能

目的

本节介绍如何配置ARP学习功能。

过程

配置ARP学习功能的步骤如下。

目的	步骤
配置ARP严格学习功能	方法一： 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**arp learning strict (enable | disable)**。 方法二： 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 VLAN-ID**进入VLANIF配置视图； 3. 执行命令**arp learning strict (force-enable | force-disable | trust)**。

2.4 链路聚合配置

2.4.1 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，以实现流量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（Link Aggregation Control Protocol，链路汇聚控制协议）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SC9600E只支持手工汇聚和静态LACP汇聚功能。

2.4.2 配置汇聚组功能

注意：

改变eth-trunk工作模式前请首先确保该eth-trunk中没有加入任何成员接口，否则无法修改eth-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 eth-trunk**或在Trunk视图下执行命令**remove (ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 40gigaethernet) 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
创建eth-trunk并进入其配置视图	1. 进入全局配置视图； 2. 执行命令**interface eth-trunk TRUNK-NUMBER**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。
配置eth-trunk的工作模式	1. 进入全局配置视图； 2. 进入Trunk接口配置视图； 3. 执行命令**mode (manual | lacp-static)**配置eth-trunk的工作模式。
向eth-trunk中加入成员接口	方法一： 1. 进入全局配置视图； 2. 进入Trunk接口配置视图； 3. 执行命令**add (ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 40gigaethernet) INTERFACE-NUMBER**增加成员接口。 方法二： 1. 进入全局配置视图； 2. 进入接口配置视图、接口组配置视图； 3. 执行命令**join eth-trunk TRUNK-NUMBER**将当前接口加入eth-trunk。

目的	步骤
（可选）配置活动接口数阈值	配置活动接口数上限阈值： 1. 进入全局配置视图； 2. 进入Trunk接口配置视图； 3. 执行命令**active-linknumber max (MAX-NUMBER | default)**，配置链路聚合活动接口数上限阈值。 配置活动接口数下限阈值： 1. 进入全局配置视图； 2. 进入Trunk接口配置视图； 3. 执行命令**active-linknumber min (MIN-NUMBER | default)**，配置链路聚合活动接口数下限阈值。
（可选）配置系统LACP优先级	1. 进入全局配置视图； 2. 执行命令**lacp system-priority (PRIORITY | default)**，配置当前设备的系统LACP优先级。
移除Trunk接口配置视图下的成员接口	1. 进入全局配置视图； 2. 进入Trunk接口配置视图； 3. 执行如下命令： ▶ **remove (ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 40gigaethernet) INTERFACE-NUMBER** ▶ **remove (ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 40gigaethernet) INTERFACE-NUMBER to (ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 40gigaethernet) INTERFACE-NUMBER**
配置LACP模式下Eth-Trunk接口接收LACP协议报文的超时时间	1. 进入全局配置视图； 2. 进入Trunk接口配置视图； 3. 执行命令**lacp timeout TIMEOUT-VALUE**配置LACP模式下Eth-Trunk接口接收LACP协议报文的超时时间。
配置当前LACP聚合组端口号整体偏移量	1. 进入Trunk接口配置视图； 2. 执行命令**lacp port-id extension (EX-VALUE | default)**。
配置trunk接口的LACP系统ID	1. 进入Trunk接口配置视图； 2. 执行命令**lacp system-id SYSTEM-ID-ADDRESS**。

2.4.3 配置增强负载分担

目的

使用本节操作配置增强负载分担功能。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
创建增强负载分担模板，并进入模板视图	1. 进入全局配置视图； 2. 执行命令**schedule-profile default**进入增强负载分担模板视图。
配置负载分担增强模板中IPv4报文的负载分担方式	1. 进入全局配置视图； 2. 进入增强负载分担模板视图； 3. 执行如下命令： ▶ **ip field (protocol | srcdst-ip | all | default)** ▶ **no ip field (protocol | srcdst-ip)**
配置负载分担增强模板中IPv6报文的负载分担方式	1. 进入全局配置视图； 2. 进入增强负载分担模板视图； 3. 执行如下命令： ▶ **ipv6 field (protocol | srcdst-ip | flow-lable | all | default)** ▶ **no ipv6 field (protocol | srcdst-ip | flow-lable)**
配置指定负载分担增强模板中二层报文的负载分担方式	1. 进入全局配置视图； 2. 进入增强负载分担模板视图； 3. 执行如下命令： ▶ **l2 field (all | default | eth-type | srcdst-mac | vlan)** ▶ **no l2 field (eth-type | srcdst-mac | vlan)**
配置指定负载分担增强模板中协议层报文的负载分担方式	1. 进入全局配置视图； 2. 进入增强负载分担模板视图； 3. 执行如下命令： ▶ **l4 field (srcdst-port | all)** ▶ **no l4 field srcdst-port**

2.4.4 维护及调试

目的

当LACP功能不正常，需要进行查看、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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
查看LACP配置文件信息	1. 进入普通用户视图； 2. 执行命令**show lacp config**显示LACP汇聚配置文件的信息。
查看LACP全部或指定组信息	1. 进入普通用户视图； 2. 执行命令**show lacp eth-trunk [TRUNK-NUMBER]**显示指定的LACP汇聚组或全部LACP汇聚组的状态信息。
查看LACP协议相关配置信息	1. 进入普通用户视图； 2. 执行命令**show lacp system**显示LACP协议相关配置信息。
查看所有LACP成员口收发包统计信息	1. 进入普通用户视图； 2. 执行命令**show lacp statistic**查看所有LACP成员口收发包统计信息。
查看LACP模式下的LACP报文收发统计信息	1. 进入普通用户视图； 2. 执行命令**show lacp statistic interface eth-trunk TRUNK-NUMBER**查看LACP模式下的LACP报文收发统计信息。
查看接口的属性配置情况及相关信息	1. 进入普通用户视图； 2. 执行如下命令： ▶ **show interface eth-trunk TRUNK-NUMBER** ▶ **show interface eth-trunk TRUNK-NUMBER config**
查看trunk接口的相关配置信息	1. 进入普通用户视图； 2. 执行如下命令： ▶ **show interface eth-trunk TRUNK-NUMBER verbose** ▶ **show interface eth-trunk verbose** ▶ **show interface eth-trunk TRUNK-NUMBER** ▶ **show interface eth-trunk TRUNK-NUMBER config**
查看接口的统计信息	1. 进入普通用户视图； 2. 执行如下命令： ▶ **show interface statistic brief eth-trunk TRUNK-NUMBER** ▶ **show interface statistic eth-trunk TRUNK-NUMBER**

目的	步骤
打开或关闭负载分担模板调试信息	1. 进入特权用户视图； 2. 执行如下命令： ▶ **debug schedule-profile (config | event | all)** ▶ **no debug schedule-profile (config | event | all)**
查看增强负载分担模板的详细信息	1. 进入普通用户视图； 2. 执行如下命令： ▶ **show schedule-profile** ▶ **show schedule-profile PROFILE-NAME**
打开或关闭LACP模块的相关调试开关	1. 进入特权用户视图； 2. 执行如下命令： ▶ **debug lacp (timer | event | churn | mux | rx | tx | config | logic | sync | all)** ▶ **no debug lacp (timer | event | churn | mux | rx | tx | config | logic | sync | all)**
清除所有接口统计的lacp（链路汇聚协议信息）	1. 进入全局配置视图； 2. 执行命令**reset lacp statistic**清除所有接口统计的lacp（链路汇聚协议信息）。
清除接口统计的链路汇聚协议信息	1. 进入全局配置视图； 2. 执行命令**reset lacp statistic interface (ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 40gigaethernet) INTERFACE-NUMBER**清除接口统计的链路汇聚协议信息。
清除trunk接口统计的链路汇聚协议信息	1. 进入全局配置视图； 2. 执行命令**reset lacp statistic interface eth-trunk TRUNK-NUMBER**清除trunk接口统计的链路汇聚协议信息。

2.4.5 链路聚合典型举例

组网要求

在两台直接相连的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，保持数据传输不中断。

◆ 活动链路具有负载分担的能力。

组网图

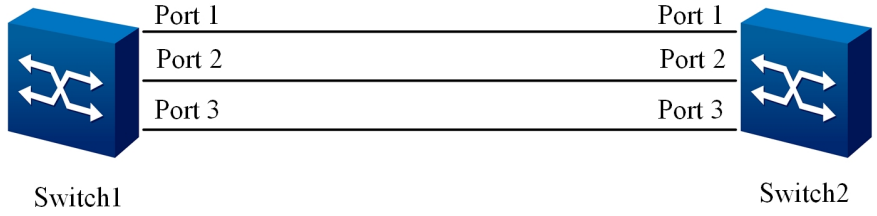


图 2-2 链路聚合配置拓扑图

配置步骤

两端配置一致，这里仅列出一端配置。

1. 创建链路聚合组。

```
SC9600E(config)#interface eth-trunk 1
SC9600E(config-eth-trunk-1)#no shutdown
SC9600E(config-eth-trunk-1)#mode lacp-static
```

2. 接口1-3加入汇聚组。

```
SC9600E(config)#interface 10gigaethernet 1/0/1 to 10gigaethernet 1/0/3
SC9600E(config-10ge1/0/1->xge1/0/3)#no shutdown
SC9600E(config-10ge1/0/1->xge1/0/3)#join eth-trunk 1
```

3. 配置结束，查看汇聚组的信息。

```
SC9600E#show lacp eth-trunk 1
eth-trunk 1:
        LACP Status: master     Port number: 3

gigaethernet-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
```

```
gigaethernet-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

gigaethernet-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
```

2.5 VLAN 配置

2.5.1 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。

2.5.2 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
创建VLAN并进入VLAN视图	1. 进入全局配置视图； 2. 执行命令**vlan VLAN-ID1 [VLAN-ID2]**创建一个或多个VLAN并进入VLAN视图。
创建并进入VLANIF接口配置视图	1. 进入全局配置视图； 2. 执行命令**interface vlan VLAN-ID**创建并进入VLANIF接口配置视图。
删除已创建的VLANIF	1. 进入全局配置视图； 2. 执行命令**no vlan VLAN-ID**删除指定VLANIF接口配置视图。
删除一个或者批量删除多个VLAN	1. 进入全局配置视图； 2. 执行命令**no vlan VLAN-ID1 [VLAN-ID2]**用来删除一个或者批量删除多个VLAN。

2.5.3 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置接口的缺省VLAN并同时加入此VLAN	1. 进入全局配置视图； 2. 进入接口组配置视图（以太网接口、trunk接口）； 3. 执行命令**port link-type TYPE**将link-type配置为access或dot1q-tunnnel类型； 4. 执行命令**port default vlan VLAN-ID**配置接口的缺省VLAN并同时加入此VLAN。
配置Hybrid类型接口所属VLAN	1. 进入全局配置视图； 2. 进入接口组配置视图（以太网接口、trunk接口）； 3. 执行命令**port hybrid vlan VLAN-LIST (tagged | untagged)**配置Hybrid类型接口所属VLAN。
配置Hybrid类型接口的缺省VLAN	1. 进入全局配置视图； 2. 进入接口组配置视图（以太网接口、trunk接口）； 3. 执行命令**port hybrid pvid (VLAN-ID | default)**配置Hybrid类型接口的缺省VLAN。
配置接口的链路类型，也叫接口类型	1. 进入全局配置视图； 2. 进入接口组配置视图（以太网接口、trunk接口）； 3. 执行命令**port link-type (access | trunk | hybrid | default)**配置接口的链路类型。
配置Trunk类型接口的缺省VLAN	1. 进入全局配置视图； 2. 进入接口组配置视图（以太网接口、trunk接口）； 3. 执行命令**port trunk pvid (VLAN-ID | default)**配置Trunk类型接口的缺省VLAN。
配置Trunk类型接口加入VLAN	1. 进入全局配置视图； 2. 进入接口组配置视图（以太网接口、trunk接口）； 3. 执行命令**port trunk allow-pass vlan all**配置Trunk类型接口加入VLAN。

2.5.4 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置VLANIF接口的描述信息	1. 进入全局配置视图； 2. 执行命令**interface vlan VLAN-ID**创建并进入VLANIF接口配置视图； 3. 执行命令**alias DESCRIPTION**配置VLANIF接口的描述信息。
配置VLAN的描述信息	1. 进入全局配置视图； 2. 执行命令**vlan VLAN-ID1 [VLAN-ID2]**创建一个或多个VLAN并进入VLAN视图； 3. 执行命令**alias DESCRIPTION**配置VLAN的描述信息。
配置在VLAN转发过程中对未知单播包的处理	1. 进入全局配置视图； 2. 执行命令**vlan VLAN-ID1 [VLAN-ID2]**创建一个或多个VLAN并进入VLAN视图； 3. 执行命令**unknown-unicast (forward | drop)**用来配置在VLAN转发过程中对未知单播包的处理。
配置在VLAN转发过程中对未知单播包的处理	1. 进入全局配置视图； 2. 执行如下命令配置在VLAN转发过程中对未知单播包的处理： ▶ **unknown-unicast vlan VLAN-LIST (forward | drop)** ▶ **vlan VLAN-ID unknown-unicast (forward | drop)**
配置三层接口延时UP的时间	1. 进入以太网路由接口配置视图、VLAN接口配置视图； 2. 执行命令**protocol up-delay-time (TIME | default)**。

2.5.5 维护及调试

目的

当VLAN功能不正常，需要进行查看、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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
查看VLAN接口配置信息	1. 进入普通用户视图； 2. 执行命令**show interface vlan config**查看VLAN接口配置信息。
查看VLAN的相关信息	1. 进入普通用户视图； 2. 执行如下命令查看VLAN的相关信息： ▶ **show vlan** ▶ **show vlan all** ▶ **show vlan all VLAN-LIST** ▶ **show vlan property** ▶ **show vlan property VLAN-LIST** ▶ **show vlan verbose** ▶ **show vlan VLAN-ID verbose**
查看物理端口的VLAN List信息	1. 进入普通用户视图； 2. 执行如下命令： ▶ **show hwport vlan slot SLOT-ID** ▶ **show hwport vlan slot SLOT-ID interface (ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 40gigaethernet) INTERFACE-NUMBER** ▶ **show hwport vlan slot all**

2.5.6 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SC9600E-1和SC9600E-2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

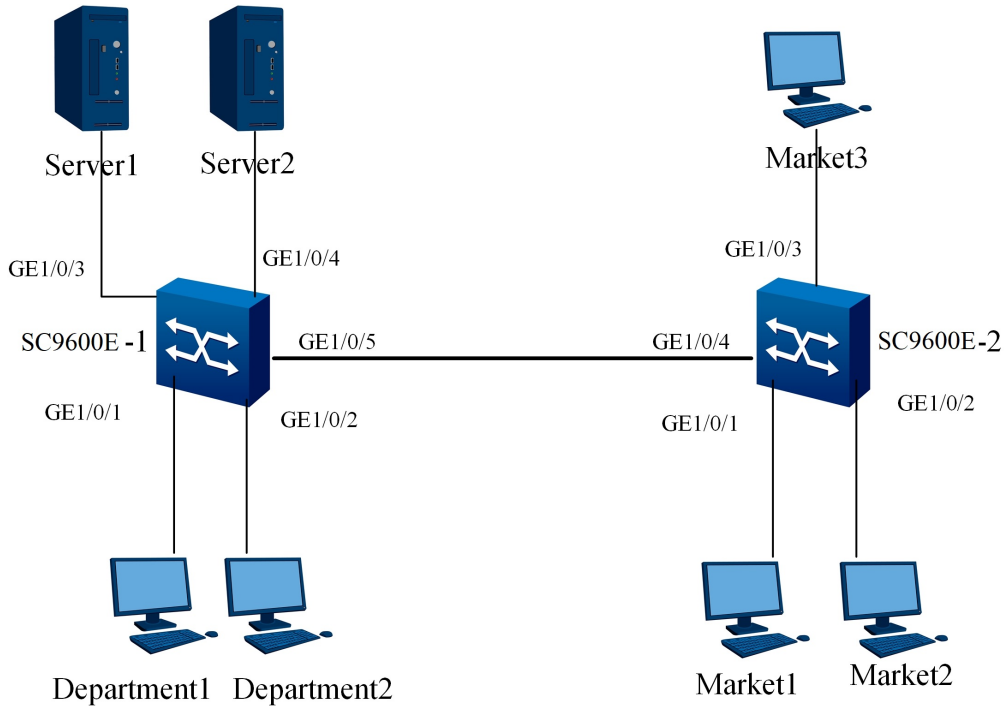


图 2-3 VLAN配置拓扑图

配置步骤

1. 配置SC9600E-1。

```
SC9600E-1#configure
%Enter configuration commands.End with Ctrl+Z or command “quit” & “end”
```

#创建VLAN100 并进入其配置视图。

```
SC9600E-1(config)#interface vlan 100
SC9600E-1(config-vlan-100)#
```

#配置VLAN100描述信息为Development100。

```
SC9600E-1(config-vlan-100)#description Development100
```

#向VLAN100中加入端口xgigaethernet1/0/1、xgigaethernet1/0/2和xgigaethernet1/0/3，并设置VLAN100为端口xgigaethernet1/0/1、xgigaethernet1/0/2和xgigaethernet1/0/3的PVID值。

```
SC9600E-1(config-vlan-100)#quit
SC9600E-1(config)#
SC9600E-1(config)#interface xgigaethernet 1/0/1
SC9600E-1(config-10ge1/0/1)#port hybrid vlan 100 untagged
```

```
SC9600E-1(config-10ge1/0/1)#port hybrid pvid 100
SC9600E-1(config-10ge1/0/1)#quit
SC9600E-1(config)#interface xgigaethernet 1/0/2
SC9600E-1(config-10ge1/0/2)#port hybrid vlan 100 untagged
SC9600E-1(config-10ge1/0/2)#port hybrid pvid 100
SC9600E-1(config-10ge1/0/2)#quit
SC9600E-1(config)#interface 10gigaethernet 1/0/3
SC9600E-1(config-ge1/0/3)#port hybrid vlan 100 untagged
SC9600E-1(config-ge1/0/3)#port hybrid pvid 100
SC9600E-1(config-ge1/0/3)#quit
SC9600E-1(config)#
```

#创建VLAN200并进入其视图。

```
SC9600E-1(config)#interface vlan 200
SC9600E-1(config-vlan-200)#
```

#配置VLAN200描述信息为Market200。

```
SC9600E-1(config-vlan-200)#description Market200
```

#向VLAN100中加入端口gigaethernet1/0/4、gigaethernet1/0/5，并设置VLAN200为端口gigaethernet1/0/4、gigaethernet1/0/5的PVID值。

```
SC9600E-1(config-vlan-100)#quit
SC9600E-1(config)#
SC9600E-1(config)#interface 10gigaethernet 1/0/4
SC9600E-1(config-10ge1/0/4)#port hybrid vlan 200 untagged
SC9600E-1(config-10ge1/0/4#port hybrid pvid 200
SC9600E-1(config-10ge1/0/4)#quit
SC9600E-1(config)#interface 10gigaethernet 1/0/5
SC9600E-1(config-10ge1/0/5)#port hybrid vlan 200 tagged
SC9600E-1(config-10ge1/0/5)#port hybrid pvid 200
SC9600E-1(config-10ge1/0/5)#quit
```

2. 配置SC9600E-2。

#创建VLAN200并进入其配置视图。

```
SC9600E-2#configure
%Enter configuration commands.End with Ctrl+Z or command “quit” & “end”
SC9600E-2(config)#interface vlan 200
```

#配置VLAN200描述信息为Market200。

```
SC9600E-2(config-vlan-200)#description Market200
```

#向VLAN100中加入端口10gigaethernet1/0/1、10gigaethernet1/0/2、10gigaethernet1/0/3和10gigaethernet1/0/4，并设置VLAN100为端口10gigaethernet1/0/1、10gigaethernet1/0/2和10gigaethernet1/0/3的PVID值。

```
SC9600E-2(config-vlan-100)#quit
SC9600E-2(config)#
SC9600E-2(config)#interface 10gigaethernet 1/0/1
SC9600E-2(config-10ge1/0/1)#port hybrid vlan 200 untagged
SC9600E-2(config-10ge1/0/1)#port hybrid pvid 200
SC9600E-2(config-10ge1/0/1)#quit
SC9600E-2(config)#interface 10gigaethernet 1/0/2
SC9600E-2(config-10ge1/0/2)#port hybrid vlan 200 untagged
SC9600E-2(config-10ge1/0/2)#port hybrid pvid 200
SC9600E-2(config-10ge1/0/2)#quit
SC9600E-2(config)#interface 10gigaethernet 1/0/3
SC9600E-2(config-10ge1/0/3)#port hybrid vlan 200 untagged
SC9600E-2(config-10ge1/0/3)#port hybrid pvid 200
SC9600E-2(config-10ge1/0/3)#quit
SC9600E-2(config)#interface 10gigaethernet 1/0/4
SC9600E-2(config-10ge1/0/4)#port hybrid vlan 200 tagged
SC9600E-2(config-10ge1/0/4)#quit
SC9600E-2(config)#
```

2.6 风暴控制配置

2.6.1 配置风暴控制功能

目的

使用本节操作配置风暴控制功能。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置以太网接口对广播、组播或未知单播进行风暴控制	1. 进入以太网桥接接口配置视图或以太网路由接口配置视图； 2. 执行如下命令： ▶ **storm-control (broadcast | multicast | dlf) percent VALUE** ▶ **storm-control (broadcast | multicast | dlf) cir (kbps | mbps | gbps) CIR-VALUE cbs (bytes | kbytes | mbytes) CBS-VALUE** ▶ **storm-control (broadcast | multicast | dlf) pps PPS-VALUE**
取消风暴控制功能	1. 进入以太网桥接接口配置视图或以太网路由接口配置视图； 2. 执行命令**no storm-control (broadcast | multicast | dlf)**。

2.6.2 维护及调试

目的

当风暴控制功能不正常，需要进行查看、调试或定位问题时，可以使用本小节操作。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
打开风暴控制信息调试功能	1. 不执行任何命令保持当前特权用户视图； 2. 执行命令**debug storm-control (nm | if | vlan | vsi | event | all)**打开风暴控制信息调试功能。
关闭风暴控制信息调试功能	1. 不执行任何命令保持当前特权用户视图； 2. 执行命令**no debug storm-control (nm | if | vlan | vsi | event | all)**关闭风暴控制信息调试功能。

目的	步骤
查看接口的风暴控制信息	1. 执行命令**disable**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或执行命令**configure**进入全局配置视图； 2. 执行如下命令： ▶ **show storm-control interface** ▶ **show storm-control interface (ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 40gigaethernet) INTERFACE-NUMBER**
查看VLAN接口的风暴控制信息	1. 执行命令**disable**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或执行命令**configure**进入全局配置视图； 2. 执行命令**show storm-control vlan [VLAN-ID]**。
查看VSI接口的风暴控制信息	1. 执行命令**disable**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或执行命令**configure**进入全局配置视图； 2. 执行命令**show storm-control vsi [VSI-NAME]**。
查看风暴控制配置信息	1. 执行命令**disable**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或执行命令**configure**进入全局配置视图； 2. 执行命令**show storm-control config**。

2.7 ARP MISS 配置

2.7.1 介绍

ARP MISS限速技术主要包括根据源IP地址进行ARP MISS消息限速和针对全局、VLAN和接口的ARP MISS消息限速。

根据源IP地址进行ARP MISS消息限速

当设备检测到某一源IP地址的IP报文在1秒内触发的ARP MISS消息数量超过了ARP MISS消息限速值，就认为此源IP地址存在攻击。

如果指定了IP地址，则针对指定源IP址的ARP MISS消息根据限速值进行限速；如果不指定IP地址，则针对每一个IP地址的ARP MISS消息根据限速值进行限速。

针对全局、VLAN和接口的ARP MISS消息限速

若同时在全局、VLAN或接口下配置ARP MISS消息限速时，设备会先按照接口进行限速，再按照VLAN进行限速，最后按照全局进行限速。

- 针对接口的ARP MISS消息限速：在某个接口出现目标IP地址不能解析的IP报文攻击时，限制处理该接口收到的报文触发的ARP MISS消息数量，配置本功能可以保证不影响其他接口的IP报文转发。
- 针对VLAN的ARP MISS消息限速：在某个VLAN内的所有接口出现目标IP地址不能解析的IP报文攻击时，限制处理该VLAN内报文触发的ARP MISS消息数量，配置本功能可以保证不影响其他VLAN内所有接口的IP报文转发。
- 针对全局的ARP MISS消息限速：在设备出现目标IP地址不能解析的IP报文攻击时，限制全局处理的ARP MISS消息数量。

2.7.2 配置 ARP MISS

目的

本节介绍如何配置ARP MISS消息限速。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置ARP MISS协议反攻击速率限制值	1. 进入全局配置视图、接口配置视图（以太网）； 2. 执行命令**arp-miss anti-attack rate-limit global maximum (MAXIMUM | default)**。 或 1. 进入VLANIF配置视图； 2. 执行命令**arp-miss anti-attack rate-limit maximum (MAXIMUM | default)**。
恢复配置ARP MISS的限速值为默认值	1. 进入全局配置视图、接口配置视图（以太网）； 2. 执行命令**no arp-miss anti-attack rate-limit global**。 或 1. 进入VLANIF配置视图； 2. 执行命令**no arp-miss anti-attack rate-limit**。
配置动态源IP限速	1. 进入全局配置视图； 2. 执行命令**arp-miss anti-attack rate-limit source-ip maximum (MAXIMUM | default) [non-block | block timer TIMER]**。

目的	步骤
配置指定源IP限速	1. 进入全局配置视图； 2. 执行命令**arp-miss anti-attack rate-limit source-ip IP-ADDRESS [MASK-ADDRESS] maximum (MAXIMUM | default) [non-block | block timer TIMER]**。
删除源IP限速配置	1. 进入全局配置视图； 2. 执行命令**no arp-miss anti-attack rate-limit source-ip IP-ADDRESS**。
重置ARP MISS协议统计信息	1. 进入全局配置视图； 2. 执行命令**arp-miss reset statistics**。

2.7.3 维护及调试

目的

当ARP MISS限速功能不正常，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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
显示ARP MISS限速的配置信息	1. 进入普通用户视图、全局配置视图、以太网接口配置视图、Trunk接口配置视图、VLANIF配置视图或特权用户视图； 2. 执行命令**show arp-miss config**。
显示ARP MISS模块的总体信息	1. 进入普通用户视图、全局配置视图、以太网接口配置视图、Trunk接口配置视图、VLANIF配置视图或特权用户视图； 2. 执行命令**show arp-miss info**。

目的	步骤
显示ARP MISS的限速的统计信息	1. 进入普通用户视图、全局配置视图、以太网接口配置视图、Trunk接口配置视图、VLANIF配置视图或特权用户视图； 2. 执行如下命令： ▶ **show arp-miss statistic** ▶ **show arp-miss statistic all** ▶ **show arp-miss statistic interface (ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 40gigaethernet) INTERFACE-NUMBER** ▶ **show arp-miss statistic srcip**
显示ARP MISS协议反攻击速率信息	1. 进入普通用户视图、全局配置视图、以太网接口配置视图、Trunk接口配置视图、VLANIF配置视图或特权用户视图； 2. 执行命令**show arp-miss anti-attack rate-limit**。
显示ARP MISS协议反攻击记录信息	1. 进入普通用户视图、全局配置视图、以太网接口配置视图、Trunk接口配置视图、VLANIF配置视图或特权用户视图； 2. 执行命令**show arp-miss anti-attack record**。
清除ARP MISS协议防攻击记录信息	1. 进入全局配置视图； 2. 执行命令**clear arp-miss anti-attack record**。
打开（关闭）ARP MISS同步调试功能	1. 进入特权用户视图； 2. 执行命令**debug arp-miss**或**no debug arp-miss**。

2.7.4 配置举例

配置步骤

1. 执行命令**configure**，进入全局配置视图，配置全局限速。

```
SC9600E(config)# arp-miss anti-attack rate-limit global pkt-num 100
```

2. 在vlan 1上配置arpmiss限速。

```
SC9600E(config)#interface vlan 1
SC9600E(config-vlan-1)#arp-miss anti-attack rate-limit pkt-num 200
```

3. 在接口 1/0/1上配置arpmiss限速。

```
SC9600E(config)#interface gigaethernet 1/0/1
SC9600E(config-ge1/0/1)#arp-miss anti-attack rate-limit pkt-num 300
SC9600E(config-ge1/0/1)#no shutdown
```

4. 配置动态源IP限速。

```
SC9600E(config)#arp-miss anti-attack rate-limit source-ip maximum 100
block timer 20
```

5. 配置指定源IP限速。

```
SC9600E(config)#arp-miss anti-attack rate-limit source-ip 10.0.0.1
maximum 100 block timer 20
```

6. 验证配置结果。

```
SC9600E(config)#show arp-miss config
```

2.8 环回检测配置

2.8.1 环回检测概述

简介

ALB（Anti-loop Back）是端口环路检测协议。为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），但生成树协议在收敛时间上较长，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，快速地查找到网络中的环，并对环进行处理，消除环或者消除环对本设备的影响。

当在交换机的接口上使能了环路检测功能后，交换机将周期性地在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。

提示：

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。

2.8.2 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	1. 执行命令configure进入全局配置视图； 2. 执行命令**interface (ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 40gigaethernet) interface-number**或**interface eth-trunk trunk-number**进入接口配置视图 3. 执行命令**loop-check (enable | disable)**使能/去使能接口环回检测功能； 4. 结束。
配置设备对指定VLAN进行环回检测	1. 执行命令configure进入全局配置视图； 2. 执行命令**interface (ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 40gigaethernet) interface-number**或**interface eth-trunk trunk-number**进入接口配置视图 3. 执行命令**loop-check vlan vlan-list**设置设备对指定VLAN进行环回检测； 4. 结束。

目的	步骤
配置设备发送环回检测包的时间间隔	1. 执行命令configure进入全局配置视图； 2. 执行命令**loop-check interval (interval-time | default)**设置设备发送环回检测包的时间间隔； 3. 结束。
配置等待时间和发包间隔之间的倍数	1. 执行命令configure进入全局配置视图； 2. 执行命令**loop-check recover-time (recover-time | default)**设置等待时间和发包间隔之间的倍数； 3. 结束。
清除环回检测接口的状态	1. 执行命令configure进入全局配置视图； 2. 执行命令**interface (ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 40gigaethernet) interface-number**或**interface eth-trunk trunk-number**进入接口配置视图 3. 执行命令**loop-check reset**清除环回检测接口的状态； 4. 结束。
使能或去使能环回检测告警功能	1. 执行命令configure进入全局配置视图； 2. 执行命令**loop-check trap (enable | disable)**使能或去使能环回检测告警功能； 3. 结束。
取消设备对指定VLAN进行环回检测	1. 执行命令configure进入接口配置视图； 2. 执行命令**no loop-check vlan vlan-list** ； 3. 结束。

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	-

参数	说明	取值
interface-number	指定以太网接口号	整数形式，取值范围是1-1/0-0/1-10或1-1/0-0/1-28
trunk-number	指定trunk接口号	整数形式，取值范围是1-64
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3-120，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3-1000
default	默认恢复时间	default：5倍
enable	使能环回检测告警功能	-
disable	去使能环回检测告警功能	-

2.8.3 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	1. 不执行任何命令保持当前特权用户视图； 2. 执行命令**debug loop-check (in | in-verbose | out | out-verbose | port-status | event | timer | all)** 打开环回检测收发包调试功能； 3. 结束。
关闭环回检测收发包调试功能	1. 不执行任何命令保持当前特权用户视图； 2. 执行命令**no debug loop-check (in | in-verbose | out | out-verbose | port-status | event | timer | all)**打开环回检测收发包调试功能； 3. 结束。

目的	步骤
查看环回检测功能的各项属性参数配置信息	1. 执行命令**disable**退出到普通用户视图，或执行命令**configure**进入全局配置视图；或执行命令**interface (ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 40gigaethernet) interface-number**或**interface eth-trunk trunk-number**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**show loop-check**显示环回检测功能的各项属性参数配置信息； 3. 结束。
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	1. 执行命令**disable**退出到普通用户视图，或执行命令**configure**进入全局配置视图；或执行命令**interface (ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 40gigaethernet) interface-number**或**interface eth-trunk trunk-number**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**show loop-check interface**或**show loop-check interface gigaethernet interface-number**或**show loop-check interface eth-trunk trunk-number**； 3. 结束。
显示环回检测的配置信息	1. 执行命令**disable**退出到普通用户视图，或执行命令**configure**进入全局配置视图；或执行命令**interface (ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 40gigaethernet) interface-number**或**interface eth-trunk trunk-number**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**show loop-check config**； 3. 结束。

附表：

参数	说明	取值
interface-number	指定以太网接口号	整数形式，取值范围是1-1/0-0/1-10或1-1/0-0/1-28
trunk-number	指定trunk接口号	整数形式，取值范围是1-64
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	-

参数	说明	取值
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	-

2.8.4 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 2-4 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。

```
SC9600E#configure
SC9600E(config)#interface gigaethernet 1/0/1
SC9600E(config-ge1/0/1)#loop-check enable
SC9600E(config-ge1/0/1)#loop-check vlan 1
SC9600E(config-ge1/0/1)#quit
```

SC9600E(config)#interface gigaethernet 1/0/2

SC9600E(config-ge1/0/2)#loop-check enable

SC9600E(config-ge1/0/2)#loop-check vlan 1

SC9600E(config-ge1/0/2)#quit

SC9600E(config)#

2. （可选配）配置设备发送环回检测包的时间间隔。

SC9600E(config)#loop-check interval 50

SC9600E(config)#

3. （可选配）配置等待时间和发包间隔之间的倍数。

SC9600E(config)#loop-check recover-time 20

SC9600E(config)#

4. 结束。

SC9600E#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

提示：

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。

3 IP 业务配置

3.1 IPv4 配置

3.1.1 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置设备的带内/带外/环回IP地址	配置带内IP地址： 1. 进入全局配置视图； 2. 进入VLANIF配置视图； 3. 执行如下命令配置带内IP地址： ▶ **ip address IP-ADDRESS/MASK-LENGTH** 配置带外IP地址： 1. 进入全局配置视图； 2. 进入带外口配置视图； 3. 执行如下命令配置带外IP地址： ▶ **ip address IP-ADDRESS/MASK-LENGTH** 配置环回IP地址： 1. 进入全局配置视图； 2. 进入Loopback接口配置视图； 3. 执行如下命令配置环回IP地址： ▶ **ip address IP-ADDRESS/MASK-LENGTH**

3.1.2 接口 IP 地址的相关配置

目的

本节介绍了各接口IP地址的相关配置。

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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置VLANIF接口的IP地址	1. 进入全局配置视图； 2. 进入VLANIF配置视图、带外口配置视图、Loopback接口配置视图、以太网路由接口配置视图、以太网子接口配置视图或grp路由接口配置视图； 3. 执行如下命令： ▶ **ip address IP-ADDRESS/MASK-LENGTH**
删除VLANIF接口的所有IP地址或指定IP地址	1. 进入全局配置视图； 2. 进入VLANIF配置视图、带外口配置视图、Loopback接口配置视图、以太网路由接口配置视图、以太网子接口配置视图或grp路由接口配置视图； 3. 执行如下命令配置带外IP地址： ▶ **no ip address IP-ADDRESS** ▶ **no ip address**
配置IPv4接口的MTU值	1. 进入全局配置视图； 2. 进入VLANIF配置视图； 3. 执行命令**mtu (MTU-VALUE | default)**。

目的	步骤
配置IPv4的前缀列表表项	1. 进入全局配置视图； 2. 执行如下命令： ▶ **ip prefix-list LISTNAME (deny | permit) IPV4-ADDRESS/MASK-LENGTH** ▶ **ip prefix-list LISTNAME (deny | permit) IPV4-ADDRESS/MASK-LENGTH (greater-equal | less-equal) PREFIX-LENGTH** ▶ **ip prefix-list LISTNAME (deny | permit) IPV4-ADDRESS/MASK-LENGTH greater-equal PREFIX-LENGTH less-equal PREFIX-LENGTH** ▶ **ip prefix-list LISTNAME index INDEX-NUMBER (deny | permit) IPV4-ADDRESS/MASK-LENGTH** ▶ **ip prefix-list LISTNAME index INDEX-NUMBER (deny | permit) IPV4-ADDRESS/MASK-LENGTH (greater-equal | less-equal) PREFIX-LENGTH** ▶ **ip prefix-list LISTNAME index INDEX-NUMBER (deny | permit) IPV4-ADDRESS/MASK-LENGTH greater-equal PREFIX-LENGTH less-equal PREFIX-LENGTH**
取消配置IPv4的前缀列表表项	1. 进入全局配置视图； 2. 执行如下命令： ▶ **no ip prefix-list LISTNAME** ▶ **no ip prefix-list LISTNAME index INDEX-NUMBER**
配置最大TCP连接数目	1. 进入全局配置视图； 2. 执行命令**ip tcp max-conncect MAXNUM**。
使能或去使能ICMP报文上送CPU时带时间戳	1. 进入全局配置视图； 2. 执行命令**icmp timestamp to-cpu (enable | disable)**。

3.1.3 查看 VLAN 接口配置信息

目的

本节介绍如何查看某一指定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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
查看VLAN接口配置信息	1. 进入普通用户视图、特权用户视图、全局配置视图、VLANIF配置视图； 2. 执行命令**show interface vlan config**。

3.1.4 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，包括现实IP统计信息、TCP统计信息、UDP统计信息、ICMP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
查看IP相关的统计信息	1. 进入特权用户视图、全局配置视图、普通用户视图； 2. 执行如下命令： ▶ **show ip statistic** ▶ **show ip tcp statistic** ▶ **show ip udp statistic** ▶ **show ip icmp statistic**

3.1.5 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
查看IPv4的接口信息以及多实例VPN情况下的接口信息	1. 进入特权用户视图、全局配置视图、普通用户视图、VLANIF配置视图； 2. 执行命令**show ip interface [vpn-instance NAME]**。

3.1.6 配置举例

组网要求

交换机SC9600E通过以太网接口10gigaethernet1/0/1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，10.18.11.0/24和10.18.12.0/24。 现要求通过交换机SC9600E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

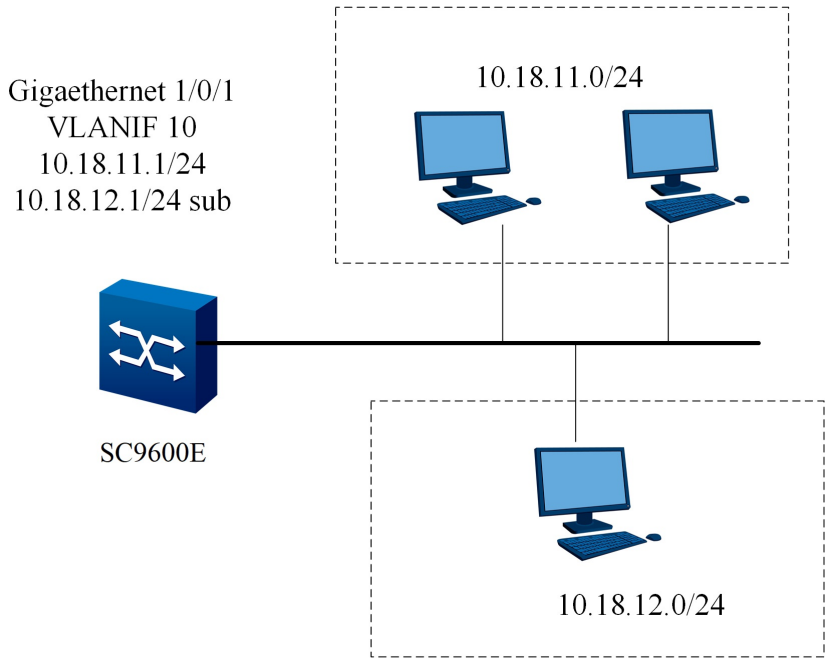


图 3-1 IPv4地址配置拓扑图

配置步骤

配置SC9600E的VLAN10接口的IP地址。

```
SC9600E#configure
SC9600E(config)#interface vlan 10
SC9600E(config-vlan-10)#ip address 10.18.11.1/24
SC9600E(config-vlan-10)#ip address 10.18.12.1/24 sub
SC9600E(config-vlan-10)#quit
SC9600E(config)#
SC9600E(config)#interface 10gigaethernet 1/0/1
SC9600E(config-10ge1/0/1)#port hybrid vlan 10 untagged
SC9600E(config-10ge1/0/1)#port hybrid pvid 10
SC9600E(config-10ge1/0/1)#quit
```

3.2 IPv6 配置

3.2.1 配置 IPv6 基本功能

3.2.1.1 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
手工设置接口的IPv6地址和前缀长度	1. 在特权用户视图下执行命令**configure**进入全局配置视图； 2. 在全局配置视图下执行命令进入VLANIF配置视图、带外口配置视图、以太网路由接口配置视图或Loopback接口配置视图； 3. 执行如下命令： ▶ **ipv6 address IPV6-ADDRESS/PREFIX-LENGTH** ▶ **ipv6 address IPV6-ADDRESS/PREFIX-LENGTH eui-64** ▶ **ipv6 address IPV6-ADDRESS/MASK-LENGTH sub** ▶ **ipv6 address IPV6-ADDRESS/PREFIX-LENGTH eui-64 sub**
删除接口手工设置的IPv6地址及其前缀	1. 在特权用户视图下执行命令**configure**进入全局配置视图； 2. 在全局配置视图下执行命令进入VLANIF配置视图、带外口配置视图、以太网路由接口配置视图或Loopback接口配置视图； 3. 执行如下命令删除接口上所有的地址或指定地址： ▶ **no ipv6 address** ▶ **no ipv6 address IPV6-ADDRESS**
删除已配置的接口IPv6单播地址	1. 在特权用户视图下执行命令**configure**进入全局配置视图； 2. 在全局配置视图下执行命令**interface vlan VLAN-ID**进入VLANIF配置视图； 3. 执行命令**no ipv6 address IPV6-ADDRESS eui-64**。
使能或者去使能接口IPv6功能	1. 在特权用户视图下执行命令**configure**进入全局配置视图； 2. 在全局配置视图下执行命令进入VLANIF配置视图、带外口配置视图、以太网路由接口配置视图或Loopback接口配置视图； 3. 执行命令**ipv6 (enable | disable)**。

3.2.1.2 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
添加一条静态IPv6路由条目，同时也支持多实例VPN情况下配置	1. 在特权用户视图下执行命令**configure**进入全局配置视图； 2. 执行如下命令： ▶ **ipv6 route-static IPV6-ADDRESS PREFIX-LEN IPV6-NEXTHOP-ADDRESS** ▶ **ipv6 route-static IPV6-ADDRESS PREFIX-LEN IPV6-NEXTHOP-ADDRESS preference PREFERENCE-VALUE** ▶ **ipv6 route-static vpn-instance NAME IPV6-ADDRESS PREFIX-LEN IPV6- NEXTHOP-ADDRESS [preference PREFERENCE-VALUE]** ▶ **ipv6 route-static IPV6-ADDRESS PREFIX-LEN vpn-instance NAME IPV6- NEXTHOP-ADDRESS preference PREFERENCE-VALUE**
删除一条静态IPv6路由条目	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**no ipv6 route-static (IPV6-ADDRESS PREFIX-LEN | all)**。

3.2.2 配置 IPv6 其他功能

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
测试IPv6网络连通性及主机可达性检查主机是否可达。发送ICMPv6回应请求报文后，等待接收目的主机发回的回应响应报文。同时也支持多实例VPN情况下配置	1. 进入特权用户视图； 2. 执行如下命令： ▶ **ping6 IPV6-ADDRESS** ▶ **ping6 IPV6-ADDRESS (-n | -l | -w) VALUE [-t]** ▶ **ping6 IPV6-ADDRESS (-n | -l | -w) VALUE (-n | -l | -w) VALUE [-t]** ▶ **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 -s IPV6-SOURCE-ADDRESS** ▶ **ping6 IPV6-ADDRESS (-n | -l | -w) VALUE (-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 -vpn-instance NAME -s IPV6-SOURCE-ADDRESS** ▶ **ping6 IPV6-ADDRESS (-n | -l | -w) value (-n | -l | -w) VALUE -s IPV6-SOURCE-ADDRESS [-t]** ▶ **ping6 IPV6-ADDRESS (-n | -l | -w) VALUE (-n | -l | -w) VALUE -vpn-instance NAME [-t]** ▶ **ping6 IPV6-ADDRESS (-n | -l | -w) VALUE (-n | -l | -w) VALUE -vpn-instance NAME -s IPV6-SOURCE-ADDRESS [-t]** ▶ **ping6 IPV6-ADDRESS (-n | -l | -w) VALUE -s IPV6-SOURCE-ADDRESS [-t]** ▶ **ping6 IPV6-ADDRESS (-n | -l | -w) VALUE -vpn-instance NAME [-t]** ▶ **ping6 IPV6-ADDRESS (-n | -l | -w) VALUE -vpn-instance NAME -s IPV6-SOURCE-ADDRESS [-t]**

目的	步骤
检查IPv6网络是否能够连通，并且ping指定主机直至被手工中断。同时也支持多实例VPN情况下配置	1. 进入特权用户视图； 2. 执行如下命令： ▶ **ping6 IPV6-ADDRESS -s IPV6-SOURCE-ADDRESS** ▶ **ping6 IPV6-ADDRESS -s IPV6-SOURCE-ADDRESS -t** ▶ **ping6 IPV6-ADDRESS -t** ▶ **ping6 IPV6-ADDRESS -vpn-instance NAME** ▶ **ping6 ipv6-address -vpn-instance NAME -s ipv6-source-address** ▶ **ping6 ipv6-address -vpn-instance NAME -s ipv6-source-address -t** ▶ **ping6 IPV6-ADDRESS -vpn-instance NAME -t**
配置链路本地IPv6地址	1. 进入VLANIF配置视图、带外口配置视图、以太网路由接口配置视图或Loopback接口配置视图； 2. 执行命令**ipv6 address IPV6-ADDRESS link-local**。
删除链路本地IPv6地址	1. 进入VLANIF配置视图、带外口配置视图、以太网路由接口配置视图或Loopback接口配置视图； 2. 执行命令**no ipv6 address link-local**。
配置自动生成的链路本地地址	1. 进入VLANIF配置视图、带外口配置视图、以太网路由接口配置视图或Loopback接口配置视图； 2. 执行命令**ipv6 address auto link-local**。
删除自动生成的链路本地地址	1. 进入VLANIF配置视图、带外口配置视图、以太网路由接口配置视图或Loopback接口配置视图； 2. 执行命令**no ipv6 address auto link-local**。

3.2.3 配置 IPv6 邻居发现功能

配置IPv6邻居请求消息发送的最大时间。

目的

本节介绍如何配置IPv6邻居请求消息发送的最长时间。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置flush邻居表（IPv6）中的所有项	1. 在特权用户视图下执行命令**configure**进入全局配置视图； 2. 在全局配置视图下执行命令**flush ipv6 neighbor all**。
配置flush邻居表（IPv6）中的动态项	1. 在特权用户视图下执行命令**configure**进入全局配置视图； 2. 在全局配置视图下执行命令**flush ipv6 neighbor dynamic**。
配置flush邻居表（IPv6）中的静态项	1. 在特权用户视图下执行命令**configure**进入全局配置视图； 2. 在全局配置视图下执行命令**flush ipv6 neighbor static**。

3.2.4 配置 IPv6 调试和维护功能

目的

本节介绍IPv6收发包、邻居发现、路由等调试功能以及IPv6邻居错误统计信息重置功能。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
打开IPv6收发包调试功能	1. 进入特权用户视图； 2. 执行命令**debug ipv6 (in | out | error | all)**打开该调试功能。
关闭IPv6收发包调试功能	1. 进入特权用户视图； 2. 执行命令**no debug ipv6 (in | out | error | all)**打开该调试功能。

3.2.5 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
查看接口IPv6基本信息	1. 进入普通用户视图、特权用户视图、全局配置视图或VLANIF配置视图； 2. 执行如下命令： ▶ **show ipv6 interface** ▶ **show ipv6 interface (ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 40gigaethernet) INTERFACE-NUMBER** ▶ **show ipv6 interface vpn-instance NAME** ▶ **show ipv6 interface vlan VLAN-ID** ▶ **show ipv6 interface loopback LOOPBACK-NUMBER**
查看设备上所有IPv6邻居节点信息，同时也支持显示多实例VPN情况下的信息	1. 进入普通用户视图、特权用户视图、全局配置视图、OSPFv2路由配置视图、VLANIF配置视图或Loopback接口配置视图； 2. 执行如下命令： ▶ **show ipv6 neighbor** ▶ **show ipv6 neighbor (ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 40gigaethernet) INTERFACE-NUMBER** ▶ **show ipv6 neighbor (dynamic | static)** ▶ **show ipv6 neighbor eth-trunk TRUNK-NUMBER** ▶ **show ipv6 neighbor IPV6-ADDRESS** ▶ **show ipv6 neighbor vpn-instance NAME** ▶ **show ipv6 neighbor summary**
查看设备IPv6路由条目信息息	1. 进入普通用户视图、特权用户视图、全局配置视图、OSPFv2路由配置视图、VLANIF配置视图或Loopback接口配置视图； 2. 执行命令**show ipv6 route**。
显示IPv6汇总路由信息	1. 进入普通用户视图、特权用户视图、全局配置视图或VLANIF配置视图； 2. 执行命令**show ipv6 route summary**。

目的	步骤
显示IPv6相关的统计信息	1. 进入普通用户视图、特权用户视图、全局配置视图或VLANIF配置视图； 2. 执行如下命令： ▶ **show ipv6 statistic** ▶ **show ipv6 statistic interface vlan VLAN-ID** ▶ **show ipv6 statistic interface (ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 40gigaethernet)INTERFACE-NUMBER**
显示IPv6 的loopback接口信息	1. 进入普通用户视图、特权用户视图、全局配置视图或VLANIF配置视图； 2. 执行命令**show ipv6 interface loopback LOOPBACK-NUMBER**。
显示IPv6 的VLAN接口信息	1. 进入普通用户视图、特权用户视图、全局配置视图或VLANIF配置视图； 2. 执行命令**show ipv6 interface vlan VLAN-ID**。
显示IPv6地址前缀列表的表项信息	1. 进入普通用户视图、特权用户视图或者全局配置视图； 2. 执行如下命令： ▶ **show ipv6 prefix-list** ▶ **show ipv6 prefix-list LIST-NAME**
通过具体的VLAN显示IPv6的统计信息	1. 进入普通用户视图、特权用户视图、全局配置视图或VLANIF配置视图； 2. 执行如下命令： ▶ **show ipv6 statistic interface vlan VLAN-ID** ▶ **show ipv6 statistic interface (ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 40gigaethernet) INTERFACE-NUMBER** ▶ **show ipv6 statistic interface (ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 40gigaethernet) INTERFACE-NUMBER. SUBINTERFACE**

3.2.6 配置举例

组网需求

两台SC9600E设备通过gigaethenet1/0/1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

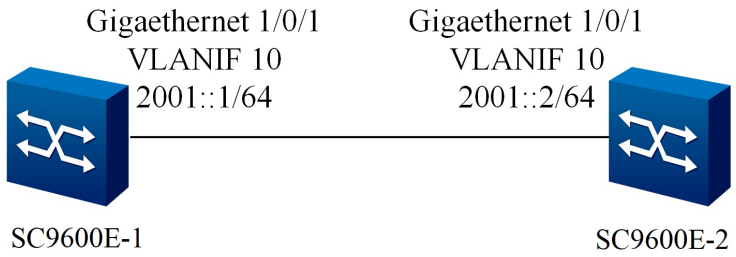


图 3-2 IPv6地址配置拓扑图

配置步骤

1. 配置SC9600E-1的VLAN10接口的IP地址。

```
SC9600E-1#configure
SC9600E-1(config)#interface vlan 10
```

#使能接口IPv6功能。

```
SC9600E-1(config-vlan-10)#ipv6 enable
SC9600E-1(config-vlan-10)#ipv6 address 2001::1/64
SC9600E-1(config-vlan-10)#quit
SC9600E-1(config)#
SC9600E-1(config)#interface 10gigaethernet 1/0/1
SC9600E-1(config-10ge1/0/1)#port hybrid vlan 10 untagged
SC9600E-1(config-10ge1/0/1)#port hybrid pvid 10
SC9600E-1(config-10ge1/0/1)#quit
```

2. 配置SC9600E-2的VLAN10接口的IP地址。

```
SC9600E-2#configure
SC9600E-2(config)#interface vlan 10
```

#使能接口IPv6功能。

```
SC9600E-2(config-vlan-10)#ipv6 enable
SC9600E-2(config-vlan-10)#ipv6 address 2001::2/64
SC9600E-2(config-vlan-10)#quit
SC9600E-2(config)#
```

```
SC9600E-2(config)#interface 10gigaethernet 1/0/1
SC9600E-2(config-10ge1/0/1)#port hybrid vlan 10 untagged
SC9600E-2(config-10ge1/0/1)#port hybrid pvid 10
SC9600E-2(config-10ge1/0/1)#quit
```

3.3 DHCP 配置

3.3.1 DHCP 协议简介

DHCP产生背景

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。

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。

DHCP相关术语

- DHCP服务器

  DHCP服务的提供者，通过DHCP报文与DHCP客户端交互，为各种类型的客户端分配合适的IP地址，并可以根据需要为客户端分配其它网络参数。

- DHCP客户端

  是整个DHCP过程的触发者和驱动者，通过DHCP报文和DHCP服务器交互，得到IP地址和其他网络参数。

- DHCP中继

  DHCP报文的中继转发者。它在处于不同网段间的DHCP客户端和服务器之间承担中继服务，解决了DHCP客户端和DHCP服务器必须位于同一网段的问题。

- DHCP Snooping

  DHCP服务的二层监听功能。利用该功能可以记录用户的IP地址和MAC地址信息。

DHCP常用选项

为了与BOOTP兼容，DHCP保留了BOOTP的消息格式。DHCP和BOOTP消息的不同主要体现在选项（Option）字段。DHCP在BOOTP基础上增加的功能，通过Option字段来实现。

DHCP利用Option字段传递控制信息和网络配置参数，实现地址的动态分配，为客户端提供更加丰富的网络配置信息。

常见的DHCP选项有：

- Option 3：路由器选项，用来指定为客户端分配的网关地址。
- Option 6：DNS服务器选项，用来指定为客户端分配的DNS服务器地址。
- Option 51：IP地址租约选项。
- Option 53：DHCP消息类型选项，标识DHCP消息的类型。
- Option 55：请求参数列表选项。客户端利用该选项指明需要从服务器获取哪些网络配置参数。该选项内容为客户端请求的参数对应的选项值。
- Option 66：TFTP服务器名选项，用来指定为客户端分配的TFTP服务器的域名。
- Option 67：启动文件名选项，用来指定为客户端分配的启动文件名。
- Option 150：TFTP服务器地址选项，用来指定为客户端分配的TFTP服务器的地址。
- Option 121：无分类路由选项。该选项中包含一组无分类静态路由（即目的地址的掩码为任意值，可以通过掩码来划分子网），客户端收到该选项后，将在路由表中添加这些静态路由。
- Option 33：静态路由选项。该选项中包含一组有分类静态路由（即目的地址的掩码固定为自然掩码，不能划分子网），客户端收到该选项后，将在路由表中添加这些静态路由。如果存在Option 121，则忽略该选项。

更多DHCP选项的介绍，请参见RFC 2132。

DHCP优缺点

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。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。

- 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。

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中选择一个地址，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具有如下缺点：

- 当网络上存在多个DHCP 服务器时，一个 DHCP 服务器不能查出已被其它服务器租出去的 IP 地址；
- DHCP 服务器不能跨网段与客户端通信，除非通过 DHCP 中继转发报文。

注意：

- **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。**

3.3.2 DHCP 服务器简介

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：

- 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。
- 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。
- 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地址管理

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 Server安全功能

- 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。

- 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。

- 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。

3.3.3 DHCP 中继简介

DHCP Relay应用环境

原始的DHCP协议要求客户端和服务器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客户端和服务器之间承担中继服务，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。

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

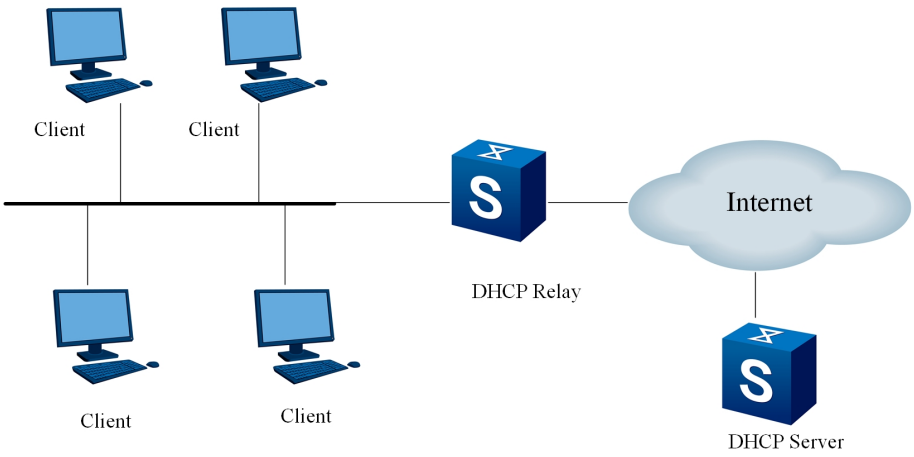


图 3-3 DHCP应用环境示意图

DHCP Relay支持的Option82选项

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

- 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。

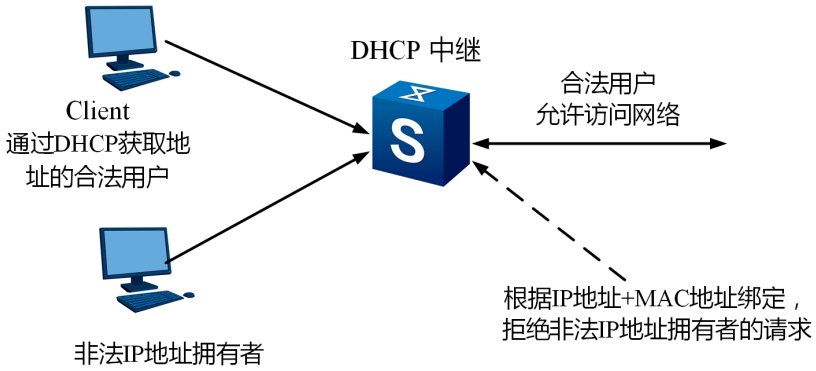


图 3-4　DHCP安全示意图

- 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，来解决这个问题上述问题。

  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。

- 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。

3.3.4 配置 DHCP 服务器

前提条件

保证DHCP Client和SC9600E之间能正常通信。

目的

配置DHCP服务器完成IP地址的分配。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
全局开启设备的DHCP功能	1. 执行命令**configure**进入全局配置视图； 2. 执行命令**dhcp start**全局开启DHCP功能。

3.3.5 配置 DHCP 中继

目的

配置DHCP中继跨网段实现DHCP服务器分配IP地址给用户。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
全局开启设备的DHCP功能	1. 执行命令**configure**进入全局配置视图； 2. 执行命令**dhcp start**全局开启DHCP功能。
配置DHCP接口工作模式为Relay	1. 执行命令**configure**进入全局配置视图； 2. 执行命令**interface vlan VLAN-ID**进入VLANIF配置视图； 3. 执行命令**ip dhcp relay**接口DHCP工作模式为Relay。

目的	步骤
配置DHCP中继所代理的DHCP服务器的IP地址	1. 执行命令**configure**进入全局配置视图； 2. 执行命令**interface vlan VLAN-ID**进入VLANIF配置视图； 3. 执行命令**dhcp relay server-ip IP-ADDRESS**配置DHCP中继所代理的DHCP服务器的IP地址。
配置DHCP中继的用户表项定时刷新的周期	1. 执行命令**configure**进入全局配置视图； 2. 执行命令**dhcp relay user refresh-interval (INTERVAL | default)**配置DHCP中继的用户表项定时刷新的周期。

3.3.6 维护及调试

目的

当DHCP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DHCP Relay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**debug dhcp relay (event | packet | info | error | all)**打开DHCP Relay调试功能。
打开DHCP server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**debug dhcp server (event | packet | info | error | all)**打开DHCP server调试功能。
清除DHCP中继的统计信息	1. 执行命令**configure**进入全局配置视图； 2. 执行命令**reset dhcp relay statistic**清除DHCP中继的统计信息。
查看设备DHCP相关功能参数配置的状态信息	1. 进入普通用户视图、特权用户视图、全局配置视图或VLANIF配置视图； 2. 执行命令**show dhcp**用来显示设备DHCP相关功能参数配置的状态信息。
查看设备DHCP配置信息	1. 进入普通用户视图、特权用户视图、全局配置视图或VLANIF配置视图； 2. 执行命令**show dhcp config**用来显示设备DHCP配置信息。

目的	步骤
查看DHCP中继服务器的配置信息	1. 进入普通用户视图、特权用户视图、全局配置视图或VLANIF配置视图； 2. 执行命令**show dhcp relay**用来显示DHCP中继服务器的配置信息。
查看DHCP中继的统计信息	1. 进入普通用户视图、特权用户视图、全局配置视图或VLANIF配置视图； 2. 执行命令**show dhcp relay statistic**用来显示DHCP中继的统计信息。
查看某个具体VLAN接口下DHCP相关的配置信息	1. 进入普通用户视图、特权用户视图、全局配置视图或VLANIF配置视图； 2. 执行命令**show dhcp vlan VLAN-ID config**用来显示某个具体VLAN接口下DHCP相关的配置信息。

3.3.7 配置举例

组网要求

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10.1.2.1/24。

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

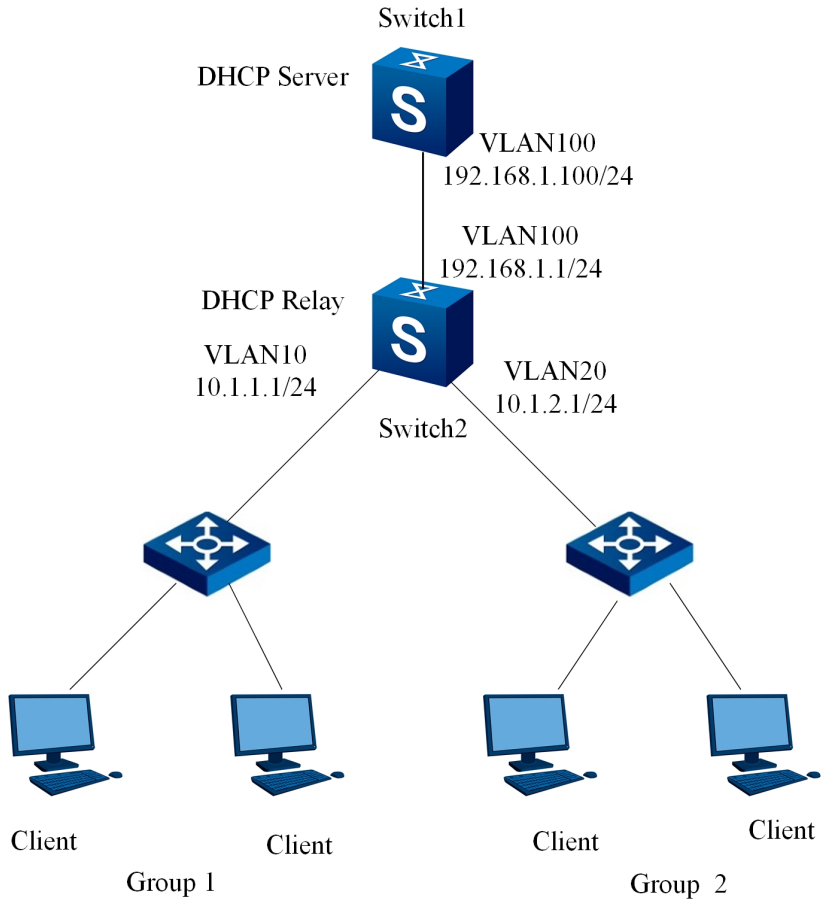


图 3-5 DHCP配置拓扑图

配置步骤

1. 配置DHCP Server。

   //配置DHCP Server的Vlan-interface100接口的IP地址。

```
Switch#configure
Switch(config)#dhcp start
Switch(config)#interface vlan 100
Switch(config-vlan-100)#ip address 192.168.1.100/24
Switch(config-vlan-100)# ip dhcp server
```

2. 配置DHCP Relay。

   //配置DHCP Relay的Vlan-interface10接口的IP地址，并配置为Relay模式。

```
Switch#configure
Switch(config)#dhcp start
```

```
Switch(config)#interface vlan 10
Switch(config-vlan-10)#ip address10.1.1.1/24
Switch(config-vlan-10)#ip dhcp relay
Switch(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。

```
Switch#configure
Switch(config)#interface vlan 20
Switch(config-vlan-20)#ip address 10.1.2.1/24
Switch(config-vlan-20)#ip dhcp relay
Switch(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。

```
Switch#configure
Switch(config)#interface vlan 100
Switch(config-vlan-100)#ip address 192.168.1.1/24
Switch(config-vlan-100)#ip dhcp relay
```

4 三层 IP 路由配置

本章介绍了SC9600E系列数据中心交换机路由相关的基本内容、配置过程和配置举例ipv6动态路由取决于版本情况。

4.1 静态路由配置

4.1.1 IPv4 静态路由配置

目的

本节介绍如何增加或者删除一条IPv4静态路由。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
增加一条IPv4静态路由	1. 进入全局配置视图； 2. 执行如下命令： ▶ **ip route-static A.B.C.D A.B.C.D A.B.C.D**
删除某条或者全部IPv4静态路由	1. 进入全局配置视图； 2. 执行如下命令： ▶ **no ip route-static IP-ADDRESS MASK-ADDRESS**
删除某条IPv4静态路由对应的特定VPN实例	1. 进入全局配置视图； 2. 执行命令**no ip route-static all**。
配置经过NULL接口的IP路由	1. 进入全局配置视图； 2. 执行命令**ip route-static IP-ADDRESS interface null NULL-NUMBER**。

4.1.2 维护及调试

目的

当静态路由配置功能不正常，需要进行查看、定位问题时，用户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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
查看特定的一条或多条路由信息	1. 进入特权用户视图、全局配置视图、普通用户视图； 2. 执行命令： ▶ **show ip route** ▶ **show ip route IP-ADDRESS**
查看IPv4路由表的综合路由统计信息	1. 进入特权用户视图、全局配置视图、普通用户视图； 2. 执行命令**show ip route statistic**。
查看汇总路由信息	1. 进入特权用户视图、全局配置视图、普通用户视图； 2. 执行命令**show ip route summary**。

4.2 OSPF 配置

4.2.1 OSPF 简介

4.2.1.1 产生背景

OSPF（Open Shortest Path First，开发最短路径优先）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支持验证。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，由自治系统边界路由器（ASBR）向自治系统内传递额外的信息。

4.2.1.2 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和系统资源；
- 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。

4.2.1.3 基本概念

OSPF路由器

OSPF路由器可简单描述如下：

- 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。
- 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。
- 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。
- 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，则遵循如下规则：

- 最大的静态环回地址。
- 最大的静态主地址。

- 最大的静态次地址。
- 最大的静态linklocal地址。
- 最大的DHCP分配置的地址。

如果协议获取不到routerID，则routerID为0，对于多实例此时不能进行netwrork的配置。

同时可以使用这个命令来手工配置ID，输入的ID不限于本地IP地址。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。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：

- Hello报文：周期性发送，用于发现和维持OSPF邻居关系。
- 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。
- LSR报文（Link State Request Packet）：向对方请求所需的LSA。
- LSU报文（Link State Update Packet）：向对方发送其所需要的LSA。
- 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：

- 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。
- 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。
- Network Sumary 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。
- 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。

- 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）。
- 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。

- 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。
- 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。

4.2.1.4 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。

- 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。

- 路由器方面的变化
  - LSDB增大。
  - 占用存储空间增加。
  - SPF算法变复杂。
  - CPU负担变重。
- 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 4-1所示。

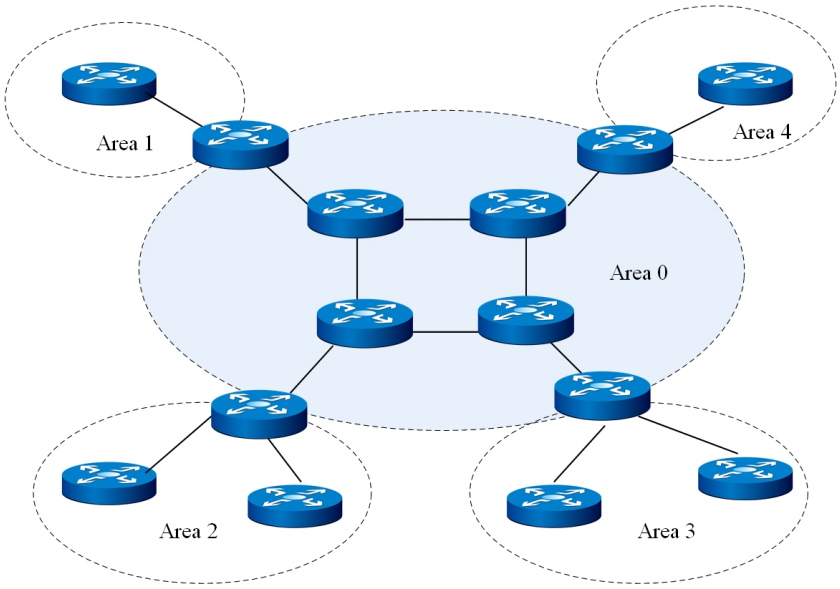


图 4-1　区域划分

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 4-2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：

- 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。

- 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。

- 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。

- 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。

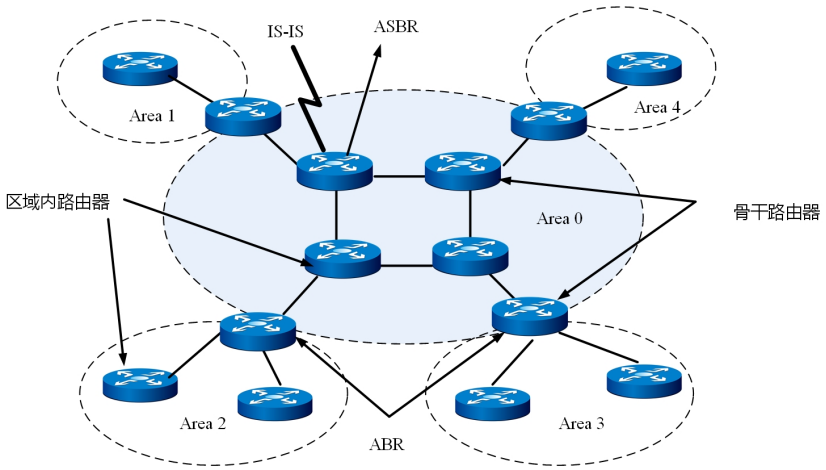


图 4-2 OSPF 路由器的类型

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：

- 虚连接的两端必须是ABR。
- 必须在两端同时配置虚连接，虚连接方能生效。
- 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。

- 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址不是这些路由器，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

- 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。
- 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。

- 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。
- NSSA区域举例：

- 如图 4-3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。

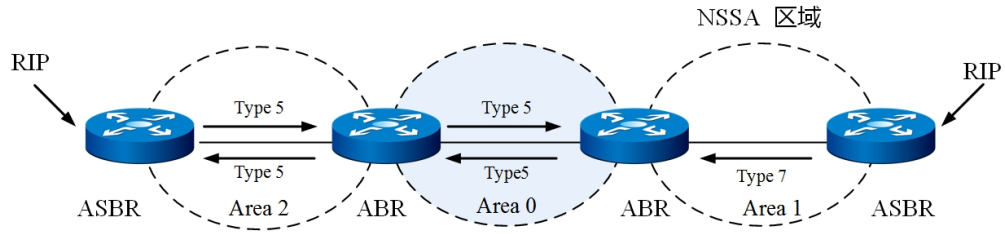


图 4-3 NSSA区域

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）。

- 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。

- 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的开销加上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等于ASBR 到该路由目的地址的开销。如果两条路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。

4.2.1.5 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：

- 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。

- 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。

- 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。

- 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）。

- 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。

- 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。

- 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

- 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。

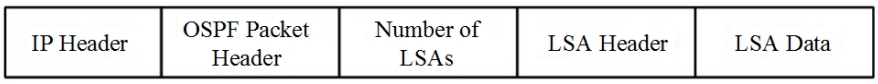
如果处于同一网段的两台路由器同时宣布自己是DR，DR 优先级高者胜出。如果优先级相等，则Router ID大者胜出。如果一台路由器的优先级为0，则它不会被选举为DR或BDR。

- 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不一定就是DR优先级最大的路由器；同理，BDR也不一定就是DR优先级第二大的路由器。

4.2.1.6 OSPF报文格式

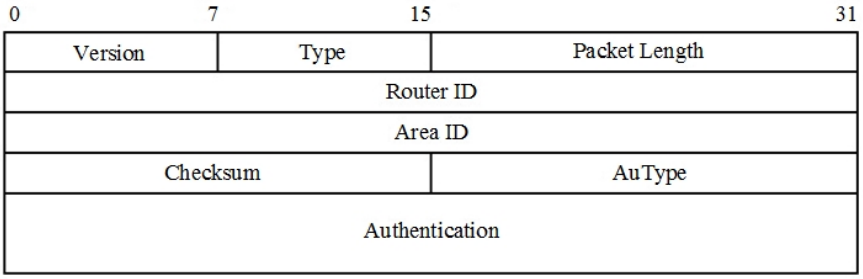
OSPF报文结构

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。

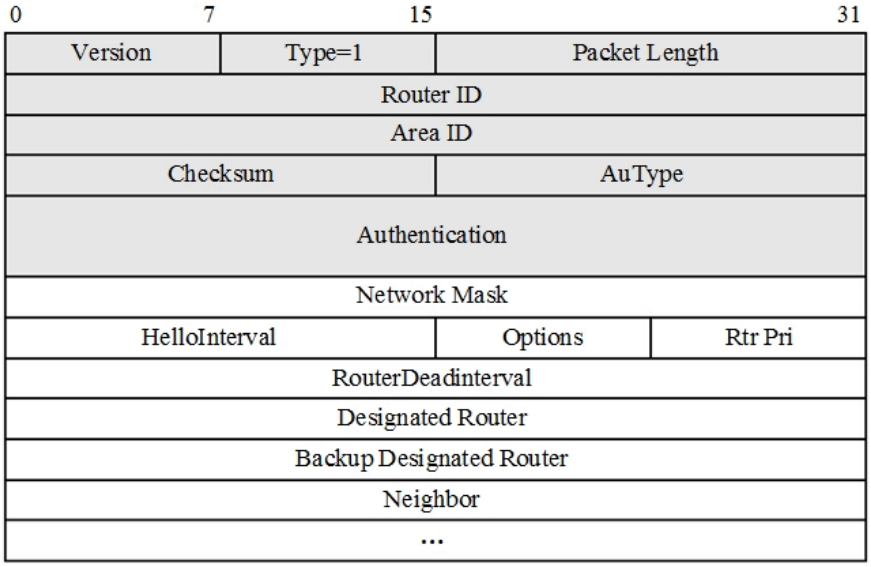
AuType：验证类型。可分为不验证、简单验证和MD5验证，其值分别为0、1、2。

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。



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。

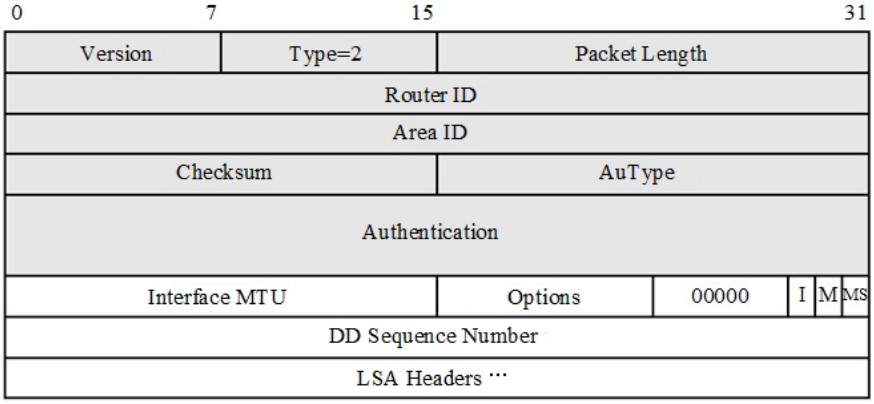
HelloInterval：发送Hello 报文的时间间隔。如果相邻两台路由器的Hello 间隔时间不同，则不能建立邻居关系。

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。

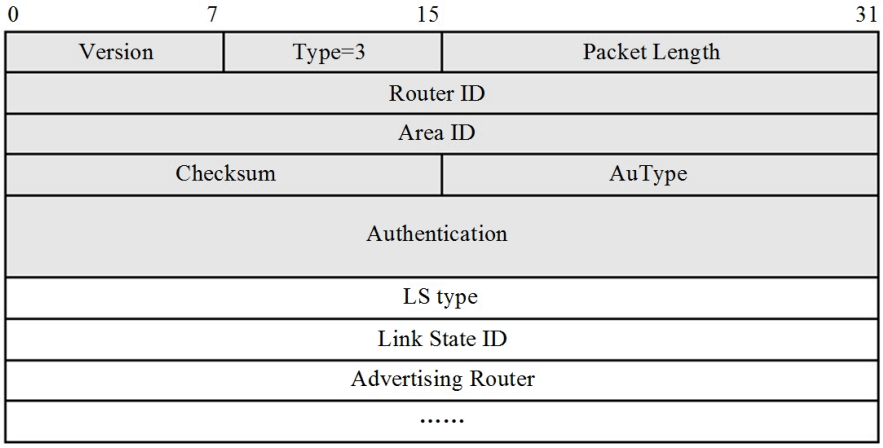
M（More）：当发送连续多个DD报文时，如果这是最后一个DD报文，则置为0，否则置为1；表示后面还有其他的DD报文。

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：

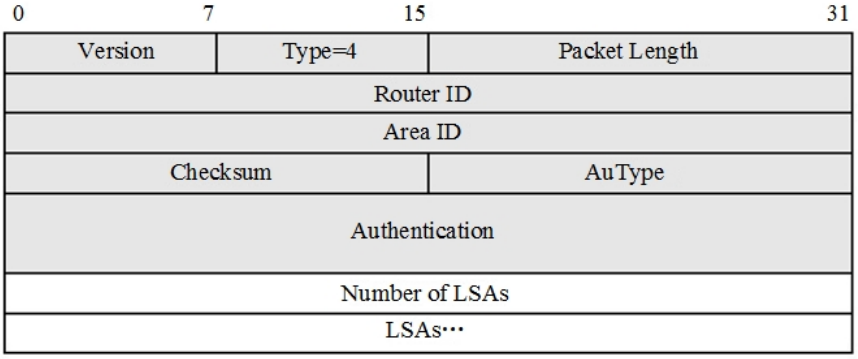
LS type：LSA的类型号。例如Type1表示Router LSA。

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。

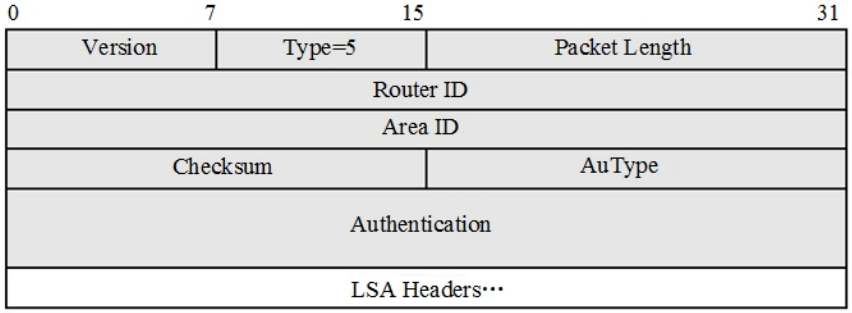
LSU报文

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报文格式如下图所示。



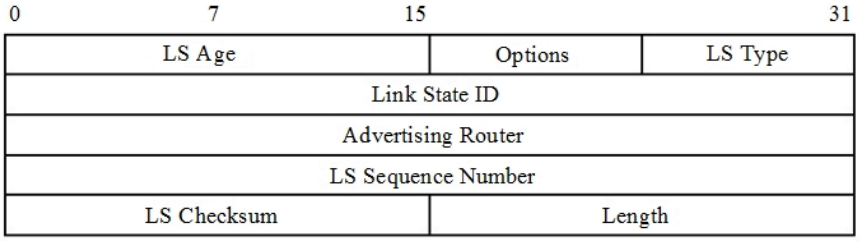
LSAck报文

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）。报文格式如下图所示。



LSA头格式

所有的LSA都有相同的报文头，其格式如下图所示。



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。

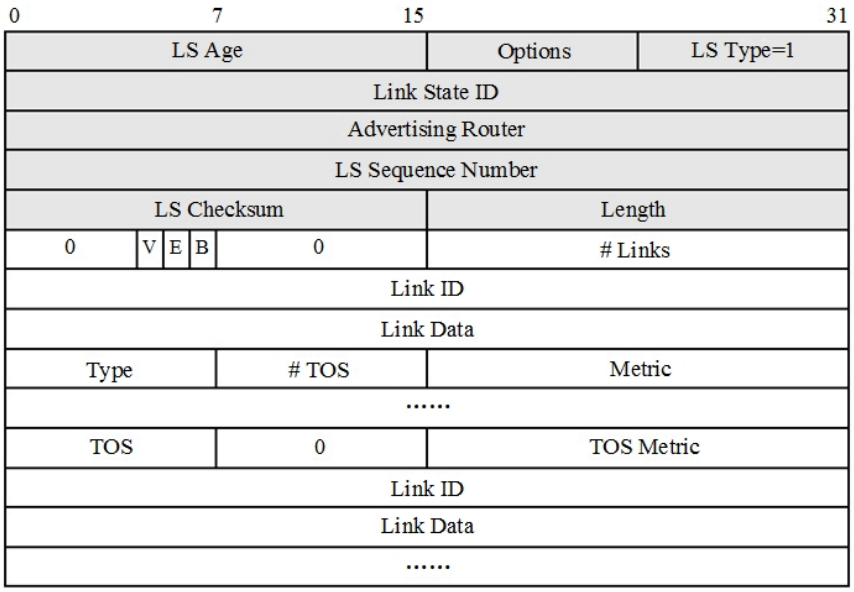
Link State ID：具体数值根据LSA 的类型而定。

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格式如下图所示。



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。

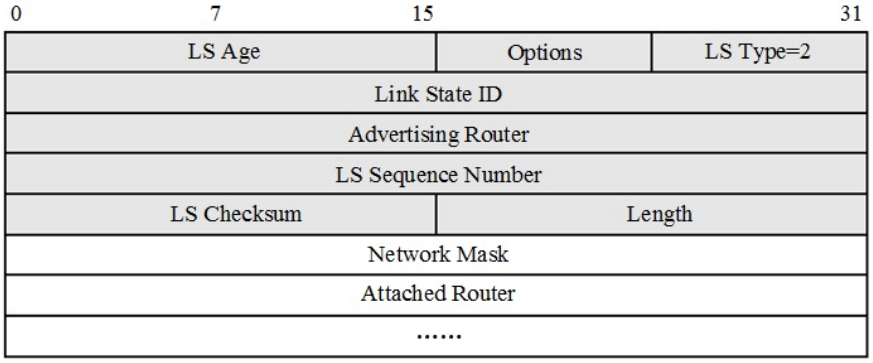
E（External）：如果产生此LSA的路由器是ASBR，则置为1。

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。



主要字段的解释如下：

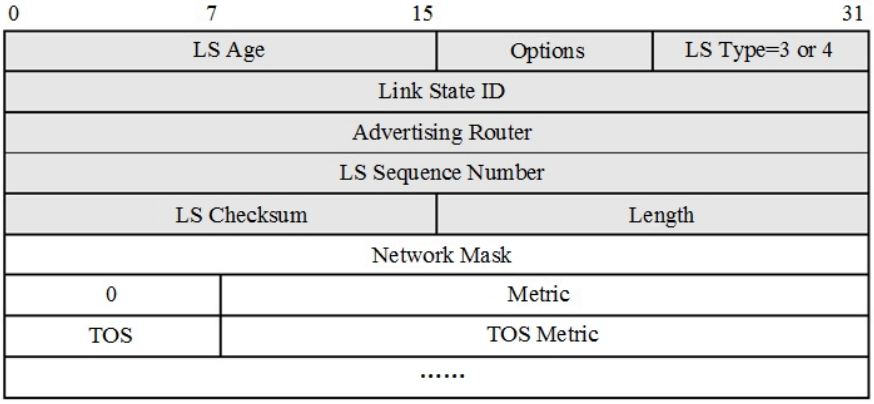
Link State ID：DR路由器的接口地址。

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。如下图所示。



主要字段的解释如下：

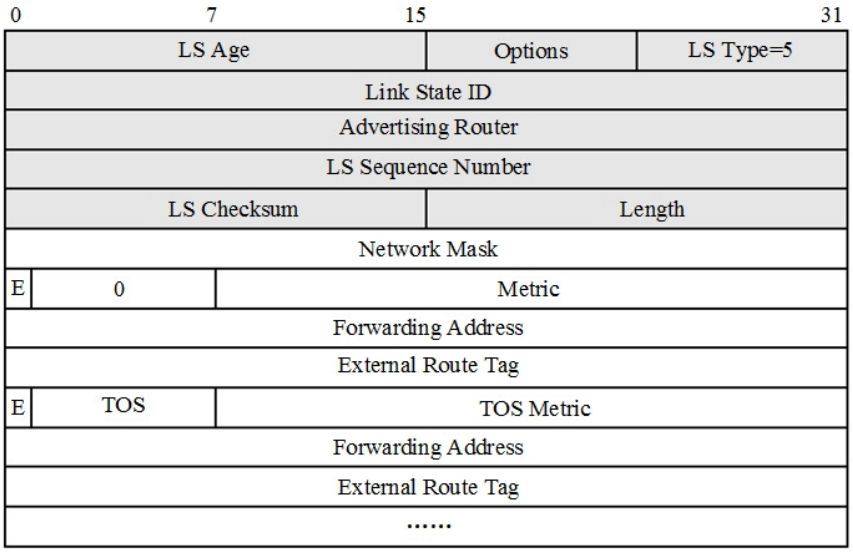
Link State ID：对于Type3 LSA来说，它是所通告的网络地址；对于Type4来说，它是ASBR的Router ID。

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。如下图所示。



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。

4.2.2 OSPF 配置步骤

4.2.2.1 配置全局OSPF

使能OSPF进程

目的

本节介绍如何启动和关闭OSPF进程。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
启动默认OSPF进程	1. 进入全局配置视图； 2. 执行命令**router ospf**。
启动指定OSPF进程	1. 进入全局配置视图； 2. 执行命令**router ospf PROCESS-ID**。
关闭默认OSPF进程	1. 进入全局配置视图； 2. 执行命令**no router ospf**。
关闭指定OSPF进程	1. 进入全局配置视图； 2. 执行命令**no router ospf PROCESS-ID**。
关闭所有OSPF进程	1. 进入全局配置视图； 2. 执行命令**no router ospf all**。

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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
复位OSPF进程	1. 进入特权用户视图； 2. 执行命令**reset ospf**。
复位指定OSPF进程	1. 进入特权用户视图； 2. 执行命令**reset ospf PROCESS-ID**。

清除OSPF统计信息

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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
清除OSPF统计信息	1. 进入特权用户视图、OSPFv2配置视图； 2. 执行命令**reset ospf counters**。

4.2.2.2 配置OSPF节点

配置Router-id或路由器ID

目的

本节介绍如何配置Router-id或路由器ID。

背景信息

缺省情况下，系统不配置Router-id或路由器ID号，运行时从各接口的IP地址中选一个作为ID号。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置交换机ID	1. 进入全局配置视图； 2. 进入OSPFv2配置视图； 3. 执行命令**router-id IP-ADDRESS**。

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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置OSPF接口和区域	1. 进入全局配置视图； 2. 进入OSPFv2配置视图； 3. 执行命令**network NETWORK-ADDRESS NETWORK-MASK area AREA-ID**。
删除OSPF接口	1. 进入全局配置视图； 2. 进入OSPFv2配置视图； 3. 执行命令**no network NETWORK-ADDRESS NETWORK-MASK area AREA-ID**。

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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置普通Stub区域	1. 进入全局配置视图； 2. 进入OSPFv2配置视图； 3. 执行命令**area AREA-ID stub**。
配置区域为完全残桩区域	1. 进入全局配置视图； 2. 进入OSPFv2配置视图； 3. 执行命令**area AREA-ID stub no-summary**。
配置OSPF区域开销值	1. 进入全局配置视图； 2. 进入OSPFv2配置视图； 3. 执行命令**area AREA-ID default-cost (COST | default)**。
删除Stub区域	1. 进入全局配置视图； 2. 进入OSPFv2配置视图； 3. 执行命令**no area AREA-ID stub**。
配置Stub路由器	1. 进入全局配置视图； 2. 进入OSPFv2配置视图； 3. 执行命令**stub-router**。
配置Stub路由器，并设置设备在发生重启或故障时保持为Stub路由器的时间间隔	1. 进入全局配置视图； 2. 进入OSPFv2配置视图； 3. 执行命令**stub-router on-startup [ON-STARTUP-TIME | default]**。
删除Stub路由器	1. 进入全局配置视图； 2. 进入OSPFv2配置视图； 3. 执行命令**no stub-router**。

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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置NSSA区域	1. 进入全局配置视图； 2. 进入OSPFv2配置视图； 3. 执行命令**area AREA-ID nssa**。
配置NSSA默认LSA开销	1. 进入全局配置视图； 2. 进入OSPFv2配置视图； 3. 执行命令**area AREA-ID nssa default-cost (COST-VALUE | default)**。
配置no summary NSSA区域	1. 进入全局配置视图； 2. 进入OSPFv2配置视图； 3. 执行命令**area AREA-ID nssa no-summary**。
配置NSSA区域聚合通告/不通告	1. 进入全局配置视图； 2. 进入OSPFv2配置视图； 3. 执行命令**area AREA-ID nssa range DST-NETWORK DST-MASK (advertise | not-advertise)**。
配置NSSA指定转换路由器或者候选转换路由器	1. 进入全局配置视图； 2. 进入OSPFv2配置视图； 3. 执行命令**area AREA-ID nssa translator (always | candidate)**。
删除NSSA区域	1. 进入全局配置视图； 2. 进入OSPFv2配置视图； 3. 执行命令**no area AREA-ID nssa**。
删除NSSA区域聚合	1. 进入全局配置视图； 2. 进入OSPFv2配置视图； 3. 执行命令**no area AREA-ID nssa range DST-ADDRESS/DST-MASK**。

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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
区域聚合	1. 进入全局配置视图； 2. 进入OSPFv2配置视图； 3. 执行命令**area AREA-ID range DST-ADDRESS DST-MASK (advertise | not-advertise)**。
删除区域聚合	1. 进入全局配置视图； 2. 进入OSPFv2配置视图； 3. 执行命令**no area AREA-ID range DST-ADDRESS DST-MASK**。

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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置路由协议的过滤策略	1. 进入全局配置视图； 2. 进入OSPFv2配置视图； 3. 执行命令**filter route-policy ROUTE-POLICY-NAME**。
取消路由协议的过滤策略	1. 进入全局配置视图； 2. 进入OSPFv2配置视图； 3. 执行命令**no filter route-policy ROUTE-POLICY-NAME**。

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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
使能GR	1. 进入全局配置视图； 2. 进入OSPFv2配置视图； 3. 执行**opaque enable**命令，开启opaque支持功能； 4. 执行命令**graceful-restart**。
配置GR周期	1. 进入全局配置视图； 2. 进入OSPFv2配置视图； 3. 执行**opaque enable**命令，开启opaque支持功能； 4. 执行命令**graceful-restart period RESTART-TIME**。
使能GR helper	1. 进入全局配置视图； 2. 进入OSPFv2配置视图； 3. 执行命令**graceful-restart helper**。
去使能GR重启	1. 进入全局配置视图； 2. 进入OSPFv2配置视图； 3. 执行命令**no graceful-restart**。
去使能GR helper	1. 进入全局配置视图； 2. 进入OSPFv2配置视图； 3. 执行命令**no graceful-restart helper**。
执行GR重启	1. 进入全局配置视图； 2. 进入OSPFv2配置视图； 3. 执行命令**graceful-restart begin**。

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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置opaque功能	1. 进入全局配置视图； 2. 进入OSPFv2配置视图； 3. 执行命令**opaque (enable | disable)**。

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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置路由计算间隔	1. 进入全局配置视图； 2. 进入OSPFv2配置视图； 3. 执行命令**spf-running-interval (INTERVAL | default)**。

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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
设置ospf有效ttl的值	1. 进入全局配置视图； 2. 进入OSPFv2配置视图； 3. 执行命令**valid-ttl-hops (HOPS-NUMBER | default)**。

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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置OSPF重分配	1. 进入全局配置视图； 2. 进入OSPFv2配置视图； 3. 执行命令**redistribute (static | connect | bgp)**。
删除指定网络的重分配	1. 进入全局配置视图； 2. 进入OSPFv2配置视图； 3. 执行命令： ▶ **no redistribute (static | connect | bgp) DST-ADDRESS DST-MASK** ▶ **no redistribute (rip | ospf | isis) PROCESS-ID DST-ADDRESS DST-MASK**
配置重分配路由策略	1. 进入全局配置视图； 2. 进入OSPFv2配置视图； 3. 执行命令**redistribute (static | connect | rip | bgp | isis | ospf) route-policy POLICY-NAME**。
删除重分配路由策略	1. 进入全局配置视图； 2. 进入OSPFv2配置视图； 3. 执行命令**no redistribute (static |connect | rip | bgp | isis | ospf) route-policy POLICY-NAME**。
配置重分配开销	1. 进入全局配置视图； 2. 进入OSPFv2配置视图； 3. 执行命令： ▶ **redistribute (connect | static | bgp) metric ROUTER-COST type COST-TYPE** ▶ **redistribute (rip | ospf | isis) PROCESS-ID metric ROUTER-COST type COST-TYPE**
配置重分配指定网络的开销	1. 进入全局配置视图； 2. 进入OSPFv2配置视图； 3. 执行命令： ▶ **redistribute (connect | static | bgp) DST-NETWORK NETWORK-MASK metric ROUTER-COST type COST-TYPE** ▶ **redistribute (rip | ospf | isis) PROCESS-ID DST-NETWORK NETWORK-MASK metric ROUTER-COST type COST-TYPE**

目的	步骤
配置重分配的translate位	1. 进入全局配置视图； 2. 进入OSPFv2配置视图； 3. 执行命令： ▶ **redistribute (connect | static | bgp) DST-NETWORK NETWORK-MASK (translate | no-translate)** ▶ **redistribute (connect | static | bgp) (translate | no-translate)** ▶ **redistribute (rip | ospf | isis) PROCESS-ID DST-NETWORK NETWORK-MASK (translate | no-translate)**
配置拒绝特定的外部路由	1. 进入全局配置视图； 2. 进入OSPFv2配置视图； 3. 执行命令： ▶ **redistribute (connect | static | bgp) DST-NETWORK NETWORK-MASK (not-advertise | advertise)** ▶ **redistribute (rip | ospf | isis) PROCESS-ID DST-NETWORK NETWORK-MASK (not-advertise | advertise)**
配置重分配路由	1. 进入全局配置视图； 2. 进入OSPFv2配置视图； 3. 执行命令**redistribute (rip | isis | ospf) PROCESS-ID**。
取消重分配路由	1. 进入全局配置视图； 2. 进入OSPFv2配置视图； 3. 执行命令**no redistribute (rip | isis | ospf) PROCESS-ID**。
配置重分配聚合路由条目	1. 进入全局配置视图； 2. 进入OSPFv2配置视图； 3. 执行命令**redistribute (static | connect | rip | bgp | isis | ospf) range RANGE-ADDRESS/M**。
删除重分配聚合路由条目	1. 进入全局配置视图； 2. 进入OSPFv2配置视图； 3. 执行命令**no redistribute (static |connect | rip | bgp | isis | ospf) range RANGE-ADDRESS/M**。

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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
使能/去使能OSPF上报trap功能	1. 进入全局配置视图； 2. 进入OSPFv2配置视图； 3. 执行命令**snmp-trap (enable | disable)**。
使能/去使能OSPF上报trap具体功能	1. 进入全局配置视图； 2. 进入OSPFv2配置视图； 3. 执行命令**snmp-trap (enable | disable) trap-name (ospfifauthfailure | ospfifconfigerror | ospfifrxbadpacket | ospfifstatechange | ospflsdbapproachingoverflow | ospflsdboverflow | ospfmaxagelsa | ospfnbrrestarthelperstatuschange | ospfnbrstatechange | ospfnssatranslatorstatuschange | ospforiginatelsa | ospfrestartstatuschange | ospftxretransmit | ospfvirtifauthfailure | ospfvirtifconfigerror | ospfvirtifrxbadpacket | ospfvirtifstatechange | ospfvirtiftxretransmit | ospfvirtnbrrestarthelperstatuschange | ospfvirtnbrstatechange)**。

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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置OSPF开销参考带宽	1. 进入全局配置视图； 2. 进入OSPFv2配置视图； 3. 执行命令**bandwidth-reference (BANDWIDTH | default)**。

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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置兼容RFC1583	1. 进入全局配置视图； 2. 进入OSPFv2配置视图； 3. 执行命令**rfc1583 compatible (enable | disable)**。

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
配置缺省路由通告	1. 进入全局配置视图； 2. 进入OSPFv2配置视图； 3. 执行命令**default-route-advertise always**。
取消缺省路由通告配置	1. 进入全局配置视图； 2. 进入OSPFv2配置视图； 3. 执行命令**no default-route-advertise**。

4.2.2.3 配置OSPF端口

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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置OSPF接口类型	1. 进入全局配置视图； 2. 进入VLANIF配置视图、Loopback接口配置视图； 3. 执行命令**ip ospf if-type (broadcast | p2p | nbma | p2multip)**。
配置OSPF接口优先级	1. 进入全局配置视图； 2. 进入VLANIF配置视图、Loopback接口配置视图； 3. 执行命令**ip ospf priority (PRIORITY | default)**。
配置OSPF接口开销	1. 进入全局配置视图； 2. 进入VLANIF配置视图、Loopback接口配置视图； 3. 执行命令**ip ospf cost (COST | default)**。
配置OSPF接口Hello间隔时间	1. 进入全局配置视图； 2. 进入VLANIF配置视图、Loopback接口配置视图； 3. 执行命令： ▶ **ip ospf hello-interval HELLO-INTERVAL** ▶ **ip ospf hello-interval default**
配置OSPF接口的wait定时器的间隔时间	1. 进入全局配置视图； 2. 进入VLANIF配置视图； 3. 执行命令**ip ospf wait-interval (WAIT-INTERVAL | default)**。
配置OSPF接口邻居超时时间	1. 进入全局配置视图； 2. 进入VLANIF配置视图、Loopback接口配置视图； 3. 执行命令： ▶ **ip ospf dead-interval INTERVAL** ▶ **ip ospf dead-interval default**
配置OSPF接口重传间隔	1. 进入全局配置视图； 2. 进入VLANIF配置视图、Loopback接口配置视图； 3. 执行命令**ip ospf retransmit-interval (RETRANSMIT-INTERVAL-TIME | default)**。
配置OSPF接口传输时延	1. 进入全局配置视图； 2. 进入VLANIF配置视图、Loopback接口配置视图； 3. 执行命令**ip ospf transmit-delay (TRANSMIT-DELAY-TIME | default)**。

目的	步骤
配置发送轮询报文的时间间隔	1. 进入全局配置视图； 2. 进入VLANIF配置视图、Loopback接口配置视图； 3. 执行命令**ip ospf poll-interval (poll-interval-time | default)**。
配置接口简单密码认证	1. 进入全局配置视图； 2. 进入VLANIF配置视图、Loopback接口配置视图； 3. 执行命令**ip ospf authentication simple-password KEY-VALUE**。
配置接口MD5认证	1. 进入全局配置视图； 2. 进入VLANIF配置视图、Loopback接口配置视图； 3. 执行命令**ip ospf authentication md5 KEY-ID MD5-KEY**。
清除接口认证	1. 进入全局配置视图； 2. 进入VLANIF配置视图、Loopback接口配置视图； 3. 执行命令**no ip ospf authentication**。
指定从IPv4地址为源IPv4地址	1. 进入VLANIF配置视图、以太网子接口配置视图、Trunk子接口配置视图、Loopback接口配置视图、以太网路由接口配置视图、grp路由接口配置视图； 2. 执行命令**no ip ospf source sub-address**。

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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置OSPF接口MTU	1. 进入全局配置视图； 2. 进入VLANIF配置视图； 3. 执行命令**ip ospf mtu (MTU | default)**。
配置MTU检测	1. 进入全局配置视图； 2. 进入VLANIF配置视图、Loopback接口配置视图； 3. 执行命令**ip ospf mtu-ignore (enable | disable)**。

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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置passive接口	1. 进入全局配置视图； 2. 进入VLANIF配置视图、Loopback接口配置视图； 3. 执行命令**ip ospf passive-interface**。

4.2.2.4 维护及调试

目的

当OSPF相关功能不正常，需要进行查看、定位或调试问题时，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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
显示OSPF简要信息	1. 进入普通用户视图、特权用户视图、全局配置视图、OSPFv2路由配置视图、VLANIF配置视图、Loopback接口配置视图； 2. 执行如下命令： ▶ **show ip ospf brief** ▶ **show ip ospf brief process PROCESS**
显示OSPF配置信息	1. 进入普通用户视图、特权用户视图、全局配置视图、OSPFv2路由配置视图、VLANIF配置视图、Loopback接口配置视图； 2. 执行命令**show ip ospf config**。

目的	步骤
显示OSPF接口信息	1. 进入普通用户视图、特权用户视图、全局配置视图、OSPFv2路由配置视图、VLANIF配置视图、Loopback接口配置视图； 2. 执行如下命令： ▶ **show ip ospf interface** ▶ **show ip ospf interface error** ▶ **show ip ospf interface IP-ADDRESS** ▶ **show ip ospf interface count** ▶ **show ip ospf interface process PROCESS**
显示OSPF邻居信息	1. 进入普通用户视图、特权用户视图、全局配置视图、OSPFv2路由配置视图、VLANIF配置视图、Loopback接口配置视图； 2. 执行如下命令： ▶ **show ip ospf neighbor** ▶ **show ip ospf neighbor IP-ADDRESS** ▶ **show ip ospf neighbor process PROCESS** ▶ **show ip ospf neighbor state statistic** ▶ **show ip ospf neighbor state count**
显示OSPF区域信息	1. 进入普通用户视图、特权用户视图、全局配置视图、OSPFv2路由配置视图、VLANIF配置视图、Loopback接口配置视图； 2. 执行如下命令： ▶ **show ip ospf area** ▶ **show ip ospf area AREA-ID** ▶ **show ip ospf area process PROCESS**

目的	步骤
显示OSPF数据库信息	1. 进入普通用户视图、特权用户视图、全局配置视图、OSPFv2路由配置视图、VLANIF配置视图、Loopback接口配置视图； 2. 执行如下命令： ▶ **show ip ospf database** ▶ **show ip ospf database area AREA-ID** ▶ **show ip ospf database area AREA-ID process PROCESS** ▶ **show ip ospf database (as-external-lsa | type9 | type11) LS-ID ADVERROUTER-ID** ▶ **show ip ospf database (as-external-lsa | type9 | type11) LS-ID ADVERROUTER-ID PROCESS** ▶ **show ip ospf database (router | network | summary-network | summary-asbr | as-external-lsa | nssa-lsa | type9 | type10 | type11)** ▶ **show ip ospf database (router | network | summary-network | summary-asbr | as-external-lsa | nssa-lsa | type9 | type10 | type11) process PROCESS** ▶ **show ip ospf database (router | network | summary-network | summary-asbr | nssa-lsa | type10) LS-ID ADVERROUTER-ID AREA-ID** ▶ **show ip ospf database (router | network | summary-network | summary-asbr | nssa-lsa | type10) LS-ID ADVERROUTER-ID AREA-ID PROCESS** ▶ **show ip ospf database age MIN-AGE MAX-AGE** ▶ **show ip ospf database age MIN-AGE MAX-AGE count** ▶ **show ip ospf database count** ▶ **show ip ospf database count process PROCESS** ▶ **show ip ospf database expire** ▶ **show ip ospf database expire count** ▶ **show ip ospf database expire process PROCESS** ▶ **show ip ospf database process PROCESS** ▶ **show ip ospf database total count**

目的	步骤
显示OSPF路由信息	1. 进入普通用户视图、特权用户视图、全局配置视图、OSPFv2路由配置视图、VLANIF配置视图、Loopback接口配置视图； 2. 执行如下命令： ▶ **show ip ospf route** ▶ **show ip ospf route count** ▶ **show ip ospf route count process PROCESS** ▶ **show ip ospf route process PROCESS** ▶ **show ip ospf route total count**
显示OSPF trap信息	1. 进入普通用户视图、特权用户视图、全局配置视图、OSPFv2路由配置视图、VLANIF配置视图、Loopback接口配置视图； 2. 执行命令**show ip ospf trap**。
显示OSPFv2的错误信息	1. 进入普通用户视图、特权用户视图、全局配置视图、OSPFv2路由配置视图、VLANIF配置视图、Loopback接口配置视图； 2. 执行命令**show ip ospf error**。

4.2.3 OSPF 配置举例

4.2.3.1 配置OSPF基本功能

组网要求

如图 4-4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SC9600E_1和SC9600E_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

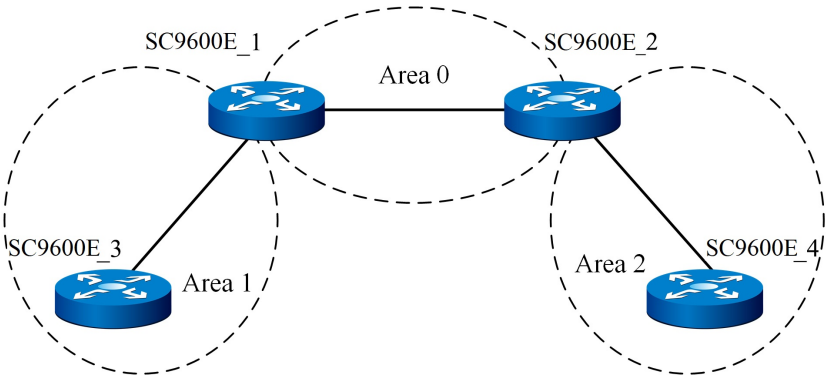


图 4-4　OSPF基本配置组网图

配置数据

SC9600E_1的两个接口地址：1.1.1.1/24和3.1.1.1/24。

SC9600E_2的两个接口地址：1.1.1.2/24和4.1.1.2/24。

SC9600E_3的两个接口地址：3.1.1.3/24。

SC9600E_4的两个接口地址：4.1.1.4/24。

配置步骤

```
SC9600E_1:
SC9600E_1(config)#router ospf
SC9600E_1(config-ospf-1)#router-id 1.1.1.1
SC9600E_1(config-ospf-1)#network 1.1.1.0 255.255.255.0 area 0
SC9600E_1(config-ospf-1)#network 3.1.1.0 255.255.255.0 area 1
SC9600E_1(config)#
SC9600E_2:
SC9600E_2(config)#router ospf
SC9600E_2(config-ospf-1)#router-id 1.1.1.2
SC9600E_2(config-ospf-1)#network 1.1.1.0 255.255.255.0 area 0
SC9600E_2(config-ospf-1)#network 4.1.1.0 255.255.255.0 area 2
SC9600E_2(config)#
SC9600E_3:
SC9600E_3(config)#router ospf
SC9600E_3(config-ospf-1)#router-id 3.1.1.3
SC9600E_3(config-ospf-1)#network 3.1.1.0 255.255.255.0 area 1
SC9600E_3(config)#
SC9600E_4:
```

```
SC9600E_4(config)#router ospf
SC9600E_4(config-ospf-1)#router-id 4.1.1.4
SC9600E_4(config-ospf-1)#network 4.1.1.0 255.255.255.0 area 2
SC9600E_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      Network      INTRA
3.1.1.0     255.255.255.0     3.1.1.1      Network      INTRA
4.1.1.0     255.255.255.0     1.1.1.2      Network      INTER
```

4.2.3.2 配置OSPF的Stub区域

组网要求

如图 4-5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SC9600E_1和SC9600E_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

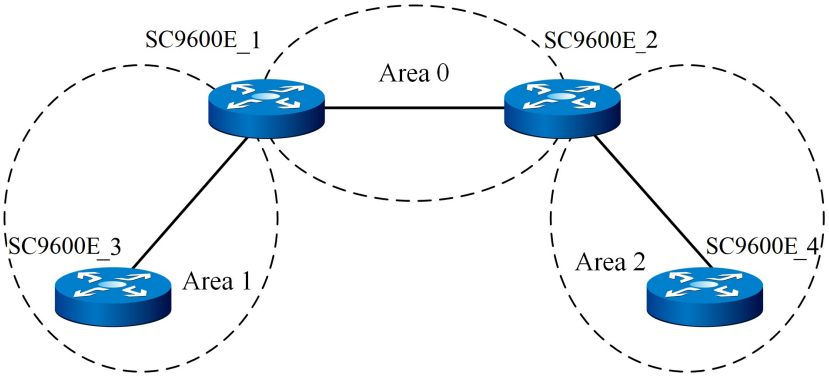


图 4-5 OSPF Stub区域组网图

配置步骤

基本配置和拓扑同4.3.3.1 配置OSPF基本功能。

配置area 1为stub：

```
SC9600E_1:
SC9600E_1(config)#router ospf
SC9600E_1(config-ospf-1)#area 1 stub
SC9600E_1(config)#
SC9600E_3:
SC9600E_3(config)#router ospf
SC9600E_3(config-ospf-1)# area 1 stub
SC9600E_3(config)#
```

在SC9600E_4引入100.1.1.1的5类LSA。

验证配置结果

1. 当SC9600E_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。

```
SC9600E_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   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
100.1.1.0  255.255.255.0    1.1.1.2   Network  ASE
```

2. 当SC9600E_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。

```
SC9600E_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   Network  INTER
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
```

4.2.3.3 配置OSPF的NSSA区域

组网要求

如图 4-6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SC9600E_1和SC9600E_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

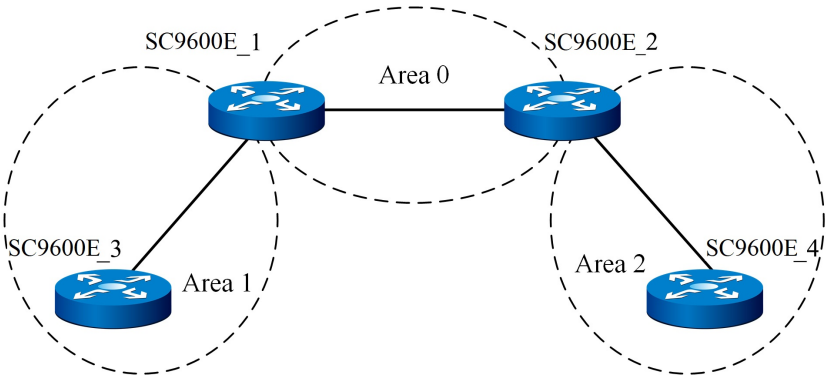


图 4-6　OSPF nssa区域组网图

配置步骤

基本配置和拓扑同配置OSPF基本功能。

配置area 1为nssa：

```
SC9600E_1:
SC9600E_1(config)#router ospf
SC9600E_1(config-ospf-1)#area 1 nssa
SC9600E_1(config)#
SC9600E_3:
SC9600E_3(config)#router ospf
SC9600E_3(config-ospf-1)# area 1 nssa
SC9600E_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。

```
SC9600E_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
                         Network LSA (area 1)
 LinkId      ADV Router    Age     Seq#          CheckSum    Len
 3.1.1.3     3.1.1.3       133     0x80000001    0xe64f      32
                         SummaryNetwork 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SC9600E_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：

```
SC9600E_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SC9600E_4上查看：

   数据库：

```
SC9600E_4#
                          ASExternal LSA
LinkId      ADV Router    Age       Seq#          CheckSum    Len
100.1.1.0   1.1.1.1       412       0x80000001    0x4701      36
```

   路由：

```
SC9600E_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    Network   INTER
3.1.1.0     255.255.255.0      4.1.1.2    Network   INTER
4.1.1.0     255.255.255.0      4.1.1.4    Network   INTRA
```

```
100.1.1.0  255.255.255.0     4.1.1.2   Network  ASE
```

3. 在SC9600E_4引入200.1.1.1的静态路由，查看SC9600E_3是否拥有外部路由。

在SC9600E_4查看数据库：

```
 ASExternal LSA
 LinkId     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SC9600E_3查看数据库：

```
SC9600E_3
                        ASExternal LSA
 LinkId     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。

4.2.3.4 配置重分配

组网要求

如图 4-7所示，2个设备都运行OSPF，并将所有都配置为区域0。假定SC9600E_1需要向OSPF导入外部路由，但是对外部路由有如下要求：

- 接受所有直连路由，并采用默认配置；
- 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；
- 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

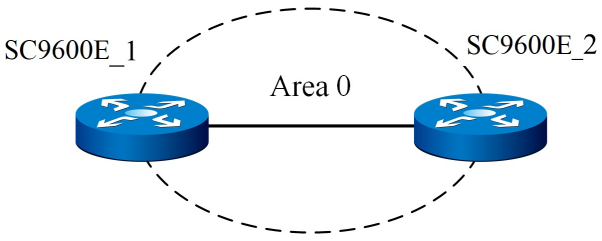


图 4-7 OSPF重分配组网图

配置步骤

1. 基本配置

```
SC9600E_1:
SC9600E_1(config)#router ospf
SC9600E_1(config-ospf-1)#router-id 1.1.1.1
SC9600E_1(config-ospf-1)#network 1.1.1.0 255.255.255.0 area 0
SC9600E_1(config-ospf-1)#network 3.1.1.0 255.255.255.0 area 1
SC9600E_1(config)#
SC9600E_2:
SC9600E_2(config)#router ospf
SC9600E_2(config-ospf-1)#router-id 1.1.1.2
SC9600E_2(config-ospf-1)#network 1.1.1.0 255.255.255.0 area 0
SC9600E_2(config-ospf-1)#network 4.1.1.0 255.255.255.0 area 2
SC9600E_2(config)#
```

2. 重分配配置

```
SC9600E_2(config-ospf-1)#redistribute connected
SC9600E_2(config-ospf-1)#redistribute static metric 2000 type 2
SC9600E_2(config-ospf-1)#redistribute static 10.1.1.0 255.255.255.0
metric 100 type 2
SC9600E_2(config-ospf-1)#redistribute static
SC9600E_2(config-ospf-1)#redistribute rip 20.1.1.0 255.255.255.0
not-advertise
SC9600E_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。

4.2.3.5 配置聚合

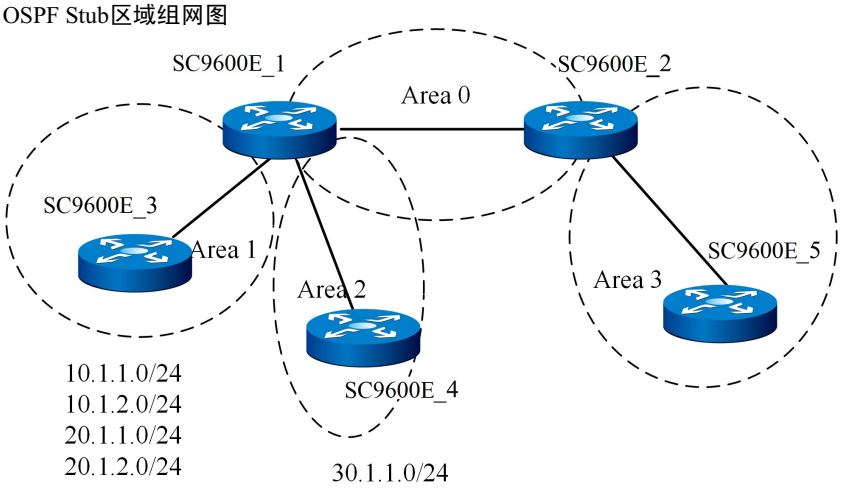
组网要求

- 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 4-8　OSPF Stub区域组网图



配置步骤

OSPF基本配置见配置OSPF基本功能。

```
SC9600E_1:
SC9600E_1(config-ospf-1)#area 1 range 10.1.0.0 255.255.0.0 advertise
SC9600E_1(config-ospf-1)#area 1 range 20.1.0.0 255.255.0.0 no-advertise
SC9600E_1(config-ospf-1)#area 2 nssa
```

#区域2的路由器均需要此配置

```
SC9600E_2:
SC9600E_2(config-ospf-1)#area 3 stub
```

或

```
SC9600E_2(config-ospf-1)#area 3 stub no-summary
```

验证配置结果

以上配置完成后，可检查数据库判断出：

- 区域0中包含10.1.0.0/16的SummaryLSA。
- 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。

- 区域0 中包含30.1.1.0/16的5类LSA。
- 区域2中包含30.1.1.0/16的7类LSA。
- 区域2中包含0.0.0.0/0的LSA。
- 区域3中包含0.0.0.0/0的Summary LSA。
- 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。

4.2.3.6 配置认证模式

组网要求

- SC9600E_1与SC9600E_2间采用简单密码认证，密码为test。
- SC9600E_1与SC9600E_4建立虚链路，采用MD5认证，密码为aaa，ID为100。
- SC9600E_2与SC9600E_3采用MD5认证，密码为ccc，ID为110。

组网图

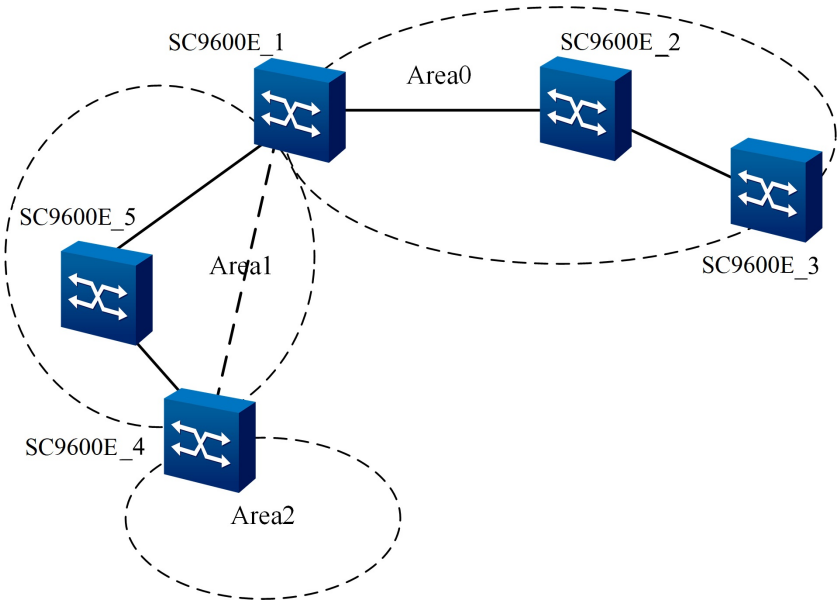


图 4-9 认证模式组网图

配置步骤

OSPF基本配置见配置OSPF基本功能。

SC9600E_1：

```
SC9600E_1(config)#interface vlan 1
SC9600E_1(config-vlan-1)#ip ospf authentication simple-password test
SC9600E_1(config-vlan-1)#exit
SC9600E_1(config)#router ospf
SC9600E_1(config-ospf-1)#area 1 virtual-link 1.1.1.2 authentication md5 aaa 100
SC9600E_2:
SC9600E_2(config)#interface vlan 1
SC9600E_2(config-vlan-1)#ip ospf authentication simple-password test
SC9600E_2(config-vlan-1)#exit
SC9600E_2(config)#interface vlan 2
SC9600E_2(config-vlan-1)#ip ospf authentication md5 110 ccc
SC9600E_2(config-vlan-1)#exit
SC9600E_3:
SC9600E_3(config-vlan-1)#router ospf
SC9600E_3(config-ospf-1)#area 0 authentication md5 110 ccc
SC9600E_4:
SC9600E_4(config)#router ospf
SC9600E_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。

4.2.3.7 配置GR

组网要求

如图 4-10所示，2个设备都运行OSPF，并将两个都配置为区域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

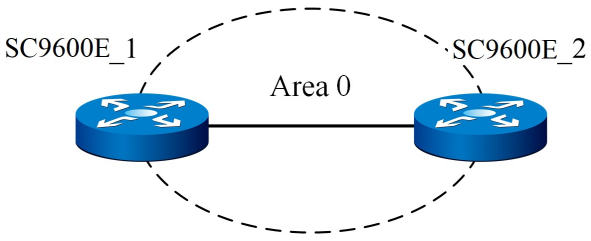


图 4-10 OSPF GR组网图

配置步骤

1. OSPF基本配置见配置OSPF基本功能。

2. GR配置。

```
SC9600E_1:
SC9600E_1(config)#router ospf
SC9600E_1(config-ospf-1)# graceful-restart
SC9600E_1(config-ospf-1)# graceful-restart period 60

SC9600E_2:
SC9600E_2(config)#router ospf
SC9600E_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。

4.3 BGP 配置

4.3.1 BGP 简介

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，边界网关协议）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。

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。

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如下：

- 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

4.3.1.1 BGP4技术介绍

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（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的直连，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 4-11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。

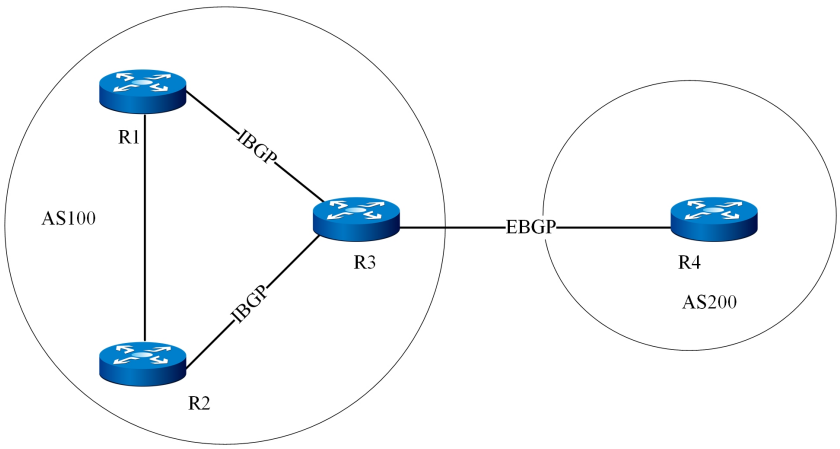


图 4-11 BGP邻居

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。

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 4-12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。

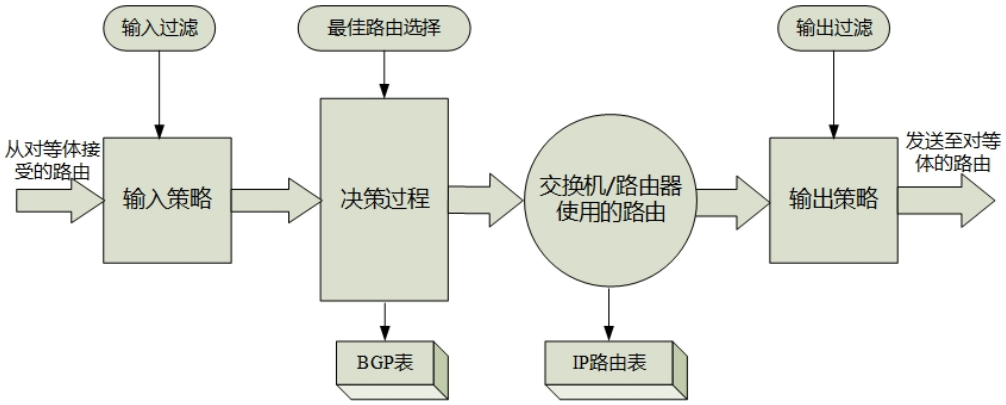


图 4-12　BGP路由选择过程

BGP4消息

BGP协议包含以下消息（所有消息均使用TCP作为传输协议）：

- 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。

- 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。

- 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。

- 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。

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。

- 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。

- 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：

  - AS-SET：路由经过的一系列无序的自治系统。
  - 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。

- 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。

- 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。

- 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。

- 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。

- 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）。

BGP4选择路由策略

- 优选本地优先级（Local_Pref）最高的路由。
- 优选聚合路由（聚合路由优先级高于非聚合路由）。
- 优选AS路径（AS_Path）最短的路由。
- 比较Origin属性，依次选择Origin类型为IGP、EGP、Incomplete的路由。
- 优选MED值最低的路由。
- 优选从EBGP学来的路由（EBGP路由优先级高于IBGP路由）。
- 优选AS内部IGP的Metric最低的路由。
- 优选Router ID最小的交换机发布的路由。
- 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。

BGP4发布路由策略

- 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。
- BGP发言者只把自己使用的路由发布给对等体。
- 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）。
- BGP发言者从IBGP获得的路由不向它的IBGP对等体发布。
- 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）。
- 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。

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，而不是将所有的具体路由都通告出去。

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。

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。

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。

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。

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。

- 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。

- 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，不同的扩展应在各自的地址族视图下配置。

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。

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。

4.3.2 BGP 配置步骤

4.3.2.1 配置BGP4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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
进入或创建BGP节点	1. 进入全局配置视图； 2. 执行命令**router bgp AS-VALUE**，进入BGP配置视图。
指定BGP的router id	1. 进入全局配置视图； 2. 进入BGP配置视图； 3. 执行命令**router-id ROUTER-ID**。
恢复BGP的router id为默认值	1. 进入全局配置视图； 2. 进入BGP配置视图； 3. 执行命令**no router-id**。

目的	步骤
创建BGP邻居	1. 进入全局配置视图； 2. 进入BGP配置视图、BGP-VPN IPv4地址族配置视图； 3. 执行命令**neighbor IPV4-ADDRESS remote-as AS-VALUE**。
删除BGP邻居	1. 进入全局配置视图； 2. 进入BGP配置视图、BGP-VPN IPv4地址族配置视图； 3. 执行命令**no neighbor IPV4-ADDRESS**。
关闭BGP邻居	1. 进入全局配置视图； 2. 执行命令**router bgp AS-VALUE**，进入BGP配置视图、BGP-VPN IPv4地址族配置视图； 3. 执行命令**neighbor IPV4-ADDRESS shutdown**。
删除关闭BGP邻居	1. 进入全局配置视图； 2. 进入BGP配置视图、BGP-VPN IPv4地址族配置视图； 3. 执行命令**no neighbor IPV4-ADDRESS shutdown**。
配置邻居的MD5验证	1. 进入全局配置视图； 2. 进入BGP配置视图、BGP-VPN IPv4地址族配置视图； 3. 执行命令**neighbor IPV4-ADDRESS password PASSWORD**。
删除邻居的MD5验证	1. 进入全局配置视图； 2. 进入BGP配置视图、BGP-VPN IPv4地址族配置视图； 3. 执行命令**no neighbor IPV4-ADDRESS password**。
配置邻居的最大保持时间和向邻居发送keeplive的间隔	1. 进入全局配置视图； 2. 进入BGP配置视图、BGP-VPN IPv4地址族配置视图； 3. 执行命令**neighbor IPV4-ADDRESS keeplive-timer (KEEPLIVE-TIMER | default) hold-timer (HOLD-TIMER | default)**。
指定邻居的更新源地址	1. 进入全局配置视图； 2. 进入BGP配置视图、BGP-VPN地址族视图； 3. 执行命令**neighbor IP-ADDRESS1 update-source IP-ADDRESS2**。
删除邻居的更新源地址	1. 进入全局配置视图； 2. 进入BGP配置视图、BGP-VPN地址族视图； 3. 执行命令**no neighbor IP-ADDRESS1 update-source**。
检测邻居的有效ttl跳数	1. 进入全局配置视图； 2. 进入BGP配置视图、BGP-VPN IPv4地址族配置视图； 3. 执行命令**neighbor IPV4-ADDRESS valid-ttl-hops (HOPS-VALUE | default)**。

4.3.2.2 配置BGP4路由发布

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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
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. 进入全局配置视图； 2. 进入BGP配置视图、BGP-VPN IPv4地址族配置视图； 3. 执行命令**aggregate IPV4-ADDRESS IPV4MASK-LENGTH (summaryonly | all)**。
配置管理路由聚合的状态，使能或关闭	1. 进入全局配置视图； 2. 进入BGP配置视图； 3. 执行命令**aggregate IPV4-ADDRESS IPV4MASK-LENGTH adminstatus (up | down)**。
删除路由聚合	1. 进入全局配置视图； 2. 进入BGP配置视图、BGP-VPN IPv4地址族配置视图； 3. 执行命令**no aggregate IPV4-ADDRESS IPV4MASK-LENGTH**。
将发送给邻居路由的下一跳更改为本地地址	1. 进入全局配置视图； 2. 进入BGP配置视图、BGP-VPN IPv4地址族配置视图； 3. 执行命令**neighbor IPV4-ADDRESS next-hop-local**。
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. 进入全局配置视图； 2. 进入BGP配置视图、BGP-VPN IPv4地址族配置视图； 3. 执行命令**no neighbor IPV4-ADDRESS next-hop-local**。
配置邻居的路由刷新能力	1. 进入全局配置视图； 2. 进入BGP配置视图、BGP-VPN IPv4地址族配置视图； 3. 执行命令**neighbor IPV4-ADDRESS route-refresh**。
删除邻居的路由刷新能力	1. 进入全局配置视图； 2. 进入BGP配置视图、BGP-VPN IPv4地址族配置视图； 3. 执行命令**no neighbor IPV4-ADDRESS route-refresh**。
发布指定的路由	1. 进入全局配置视图； 2. 进入BGP配置视图、BGP-VPN IPv4地址族配置视图； 3. 执行命令**network NETWORK-ADDRESS NETWORK-MASK**。

目的	步骤
删除发布的指定路由	1. 进入全局配置视图； 2. 进入BGP配置视图、BGP-VPN IPv4地址族配置视图； 3. 执行命令**no network NETWORK-ADDRESS NETWORK-MASK**。
向BGP引入静态或直连路由	1. 进入全局配置视图； 2. 进入BGP配置视图； 3. 执行命令**redistribute (static | connected | ospf | isis)**。
根据策略向BGP引入静态或直连路由	1. 进入全局配置视图； 2. 进入BGP配置视图； 3. 执行命令**redistribute (static | connected | ospf | isis) route-policy ROUTE-POLICY-NAME**。
修改向BGP引入静态或直连路由的med值	1. 进入全局配置视图； 2. 进入BGP配置视图； 3. 执行命令**redistribute (static | connected | ospf | isis) med MED-VALUE**。
删除向BGP引入路由	1. 进入全局配置视图； 2. 进入BGP配置视图； 3. 执行命令**no redistribute (static | connected | ospf | isis)**。
删除根据策略向BGP引入路由	1. 进入全局配置视图； 2. 进入BGP配置视图； 3. 执行命令**no redistribute (static | connected | ospf | isis) route-policy ROUTE-POLICY-NAME**。
使能或去使能IGP同步功能	1. 进入全局配置视图； 2. 进入BGP配置视图； 3. 执行命令**synchronization (enable | disable)**。

4.3.2.3 配置BGP4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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置默认med值	1. 进入全局配置视图； 2. 进入BGP配置视图； 3. 执行命令**default local-med (LOCAL-MED | default)**。
配置默认local-preference值	1. 进入全局配置视图； 2. 进入BGP配置视图； 3. 执行命令**default local-preference (LOCAL-PREFERENCE-VALUE | default)**。
配置BGP的团体属性	1. 进入全局配置视图； 2. 进入BGP配置视图； 3. 执行命令**community (COMMUNITY-VALUE | noadvertise | noexport) (additive | replace | none)**。
删除BGP的团体属性	1. 进入全局配置视图； 2. 进入BGP配置视图； 3. 执行命令**no community**。
向邻居发送团体属性	1. 进入全局配置视图； 2. 进入BGP配置视图； 3. 执行命令**neighbor IPV4-ADDRESS send-community**。
不向邻居发送团体属性	1. 进入全局配置视图； 2. 进入BGP配置视图； 3. 执行命令**no neighbor IPV4-ADDRESS send-community**。
允许本地AS编号重复出现次数	1. 进入全局配置视图； 2. 进入BGP配置视图、BGP-VPN IPv4地址族配置视图； 3. 执行命令**neighbor IPV4-ADDRESS allow-as-loop (TIME-VALUE | default)**。
BGP更新报文时不携带私有自治系统号，仅携带公有AS号	1. 进入全局配置视图； 2. 进入BGP配置视图； 3. 执行命令**neighbor IPV4-ADDRESS public-as-only**。

4.3.2.4 配置BGP4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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置BGP全局入或出过滤策略	1. 进入全局配置视图； 2. 进入BGP配置视图、BGP-VPN IPv4地址族配置视图； 3. 执行命令**filter-policy (export | import) route-policy ROUTE-POLICY-NAME**。
根据协议类型指定BGP全局出过滤策略	1. 进入全局配置视图； 2. 进入BGP配置视图、BGP-VPN IPv4地址族配置视图； 3. 执行命令**filter-policy export (static | connected | rip | ospf | isis) route-policy ROUTE-POLICY-NAME**。
删除BGP全局入或出过滤策略	1. 进入全局配置视图； 2. 进入BGP配置视图、BGP-VPN IPv4地址族配置视图； 3. 执行命令**no filter-policy (export | import) route-policy ROUTE-POLICY-NAME**。
删除根据协议类型指定的BGP全局出过滤策略	1. 进入全局配置视图； 2. 进入BGP配置视图、BGP-VPN IPv4地址族配置视图； 3. 执行命令**no filter-policy export (static | connected | rip | ospf | isis) route-policy ROUTE-POLICY-NAME**。
针对指定邻居配置入或出路由策略	1. 进入全局配置视图； 2. 进入BGP配置视图、BGP-VPN IPv4地址族配置视图； 3. 执行命令**neighbor IPV4-ADDRESS route-policy ROUTE-POLICY-NAME (export | import)**。
删除针对指定邻居的入或出路由策略	1. 进入全局配置视图； 2. 进入BGP配置视图； 3. 执行命令**no neighbor IPV4-ADDRESS route-policy ROUTE-POLICY-NAME (export | import)**。

4.3.2.5 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置路由反射器的簇id	1. 进入全局配置视图； 2. 进入BGP-IPv4地址族配置视图、BGP配置视图、BGP-EVPN地址族配置视图、BGP-VPN IPv4地址族配置视图、BGP-VPN IPv6地址族配置视图； 3. 执行命令**cluster-id ROUTER-ID**。
指定邻居作为反射器的客户端	1. 进入全局配置视图； 2. 进入BGP配置视图、BGP-VPN IPv4地址族配置视图； 3. 执行命令**neighbor IPV4-ADDRESS route-reflector-client**。
删除路由反射器的簇id	1. 进入全局配置视图； 2. 进入BGP-IPv4地址族配置视图、BGP配置视图、BGP-EVPN地址族配置视图、BGP-VPN IPv4地址族配置视图、BGP-VPN IPv6地址族配置视图； 3. 执行命令**no cluster-id**。
删除邻居作为反射器的客户端	1. 进入全局配置视图； 2. 进入BGP配置视图、BGP-VPN IPv4地址族配置视图； 3. 执行命令**no neighbor IPV4-ADDRESS route-reflector-client**。

4.3.2.6 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置联盟的AS号	1. 进入全局配置视图； 2. 进入BGP配置视图； 3. 执行命令**confederation identifier (AUTONOMY-SYSTEM-NUMBER | STRING)**。
指定联盟成员	1. 进入全局配置视图； 2. 进入BGP配置视图； 3. 执行命令**confederation peer-as AUTONOMY-SYSTEM-NUMBER**。

目的	步骤
删除联盟的AS号	1. 进入全局配置视图； 2. 进入BGP配置视图； 3. 执行命令**no confederation identifier**。
删除指定联盟成员	1. 进入全局配置视图； 2. 进入BGP配置视图； 3. 执行命令**no confederation peer-as AUTONOMY-SYSTEM-NUMBER**。

4.3.2.7 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
使能或关闭BGP的GR功能	1. 进入全局配置视图； 2. 进入BGP配置视图； 3. 执行命令**graceful-restart (enable | disable)**。
配置重建BGP会话的最大时间	1. 进入全局配置视图； 2. 进入BGP配置视图； 3. 执行命令**graceful-restart timer restart (RESTAR-TIMER | default)**。
配置重启侧（Restarting Speaker）和接收侧（Receiving Speaker）等待End-of-RIB消息的时间	1. 进入全局配置视图； 2. 进入BGP配置视图； 3. 执行命令**graceful-restart timer selection-deferral (SELECT-TIME | default)**。

4.3.2.8 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
进入ipv4单播地址族视图	1. 进入全局配置视图； 2. 进入BGP配置视图； 3. 执行命令**ipv4-family unicast**。
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. 进入全局配置视图； 2. 进入BGP配置视图； 3. 执行命令**ipv4-family vpn-instance NAME**。
地址族节点下使能或去使能地址组	1. 进入全局配置视图； 2. 进入BGP配置视图； 3. 进入地址族视图； 4. 执行命令**neighbor IPV4-ADDRESS (enable | disable)**。

4.3.2.9 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
显示BGP的聚合表	1. 进入普通用户视图、BGP配置视图、特权用户视图、全局配置视图、BGP地址族配置视图、BGP-VPN IPv4地址族配置视图； 2. 执行命令**show ip bgp aggregate**。
显示BGP的基本配置	1. 进入普通用户视图、BGP配置视图、特权用户视图、全局配置视图、BGP地址族配置视图、BGP-VPN IPv4地址族配置视图； 2. 执行命令**show ip bgp config**。
显示BGP的所有对等体	1. 进入普通用户视图、BGP配置视图、特权用户视图、全局配置视图、BGP地址族配置视图、BGP-VPN IPv4地址族配置视图； 2. 执行命令**show ip bgp neighbor**。

目的	步骤
显示BGP指定对等体的状态	1. 进入普通用户视图、BGP配置视图、特权用户视图、全局配置视图、BGP地址族配置视图、BGP-VPN IPv4地址族配置视图； 2. 执行如下命令： ▶ **show ip bgp neighbor IPV4-ADDRESS** ▶ **show ip bgp neighbor orf state** ▶ **show ip bgp neighbor IPV4-ADDRESS error-statistic**
显示BGP的资源统计信息	1. 进入普通用户视图、BGP配置视图、特权用户视图、全局配置视图、BGP地址族配置视图、BGP-VPN IPv4地址族配置视图； 2. 执行命令**show ip bgp resource**。
显示BGP的路由表	1. 进入普通用户视图、BGP配置视图、特权用户视图、全局配置视图、BGP地址族配置视图、BGP-VPN IPv4地址族配置视图； 2. 执行命令**show ip bgp route**。
显示BGP的路由统计信息	1. 进入普通用户视图、BGP配置视图、特权用户视图、全局配置视图、BGP地址族配置视图、BGP-VPN IPv4地址族配置视图； 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 NAME neighbor**。

4.3.2.10 查看BGP6配置信息

目的

本节介绍如何查看BGP6配置信息。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
显示IPv6 BGP的路由信息	1. 进入普通用户视图； 2. 执行命令**show ipv6 bgp route**。

4.3.2.11 维护及调试

目的

当BGP功能不正常，需要进行查看、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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
生成BGP诊断信息文件，用于对比运行状态	1. 进入普通用户视图； 2. 执行命令**dump ha bgp diag-all**用来生成BGP诊断信息文件。

4.3.3 BGP 配置举例

4.3.3.1 配置基本BGP4

组网要求

如图 4-13所示，所有SC9600E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

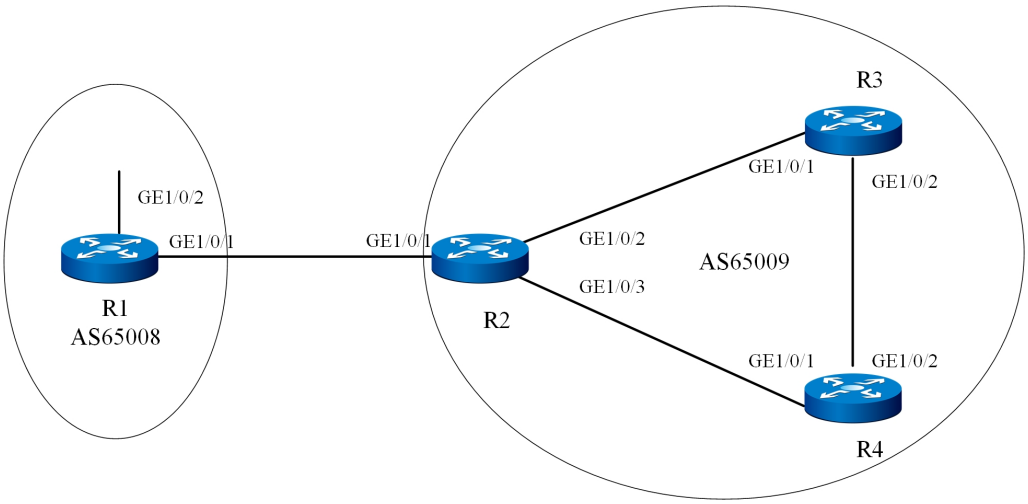


图 4-13 配置BGP基本组网图

Switch	接口	对应的VLAN	IP地址
R1	Gigaethernet1/0/1	VLAN 10	192.1.1.2/24
R1	Gigaethernet1/0/2	VLAN 50	20.1.1.1/8
R2	Gigaethernet1/0/1	VLAN 10	192.1.1.1/24
R2	Gigaethernet1/0/2	VLAN 20	10.1.3.1/24
R2	Gigaethernet1/0/3	VLAN 30	10.1.1.1/24
R3	Gigaethernet1/0/1	VLAN 20	10.1.3.2/24
R3	Gigaethernet1/0/2	VLAN 40	10.1.2.1/24
R4	Gigaethernet1/0/1	VLAN 30	10.1.1.2/24
R4	Gigaethernet1/0/2	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 4-13所示。

各VLAN接口的IP地址，具体数据如图 4-13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

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
```

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
```

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
```

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
```

4.3.3.2 配置BGP4与IGP交互

组网要求

如图 4-14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

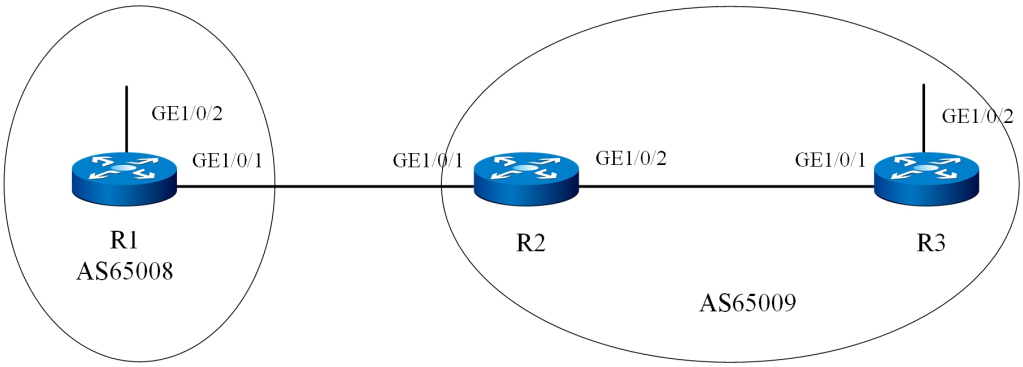


图 4-14 BGP与IGP交互配置组网图

Switch	接口	对应的VLAN	IP地址
R1	Gigaethernet1/0/1	VLAN 10	3.1.1.2/24
R1	Gigaethernet1/0/2	VLAN 30	8.1.1.1/24
R2	Gigaethernet1/0/1	VLAN 10	3.1.1.1/24
R2	Gigaethernet1/0/2	VLAN 20	9.1.1.1/24
R3	Gigaethernet1/0/1	VLAN 20	9.1.1.2/24
R3	Gigaethernet1/0/2	VLAN 40	9.1.2.1/24

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 4-14所示。

各VLAN接口的IP地址，具体数据如图 4-14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

1. 配置OSPF。

   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)#quit
```

   配置R3。

```
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
```

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
```

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
```

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
```

4.3.3.3 配置BGP4路由反射器

组网要求

如图 4-15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

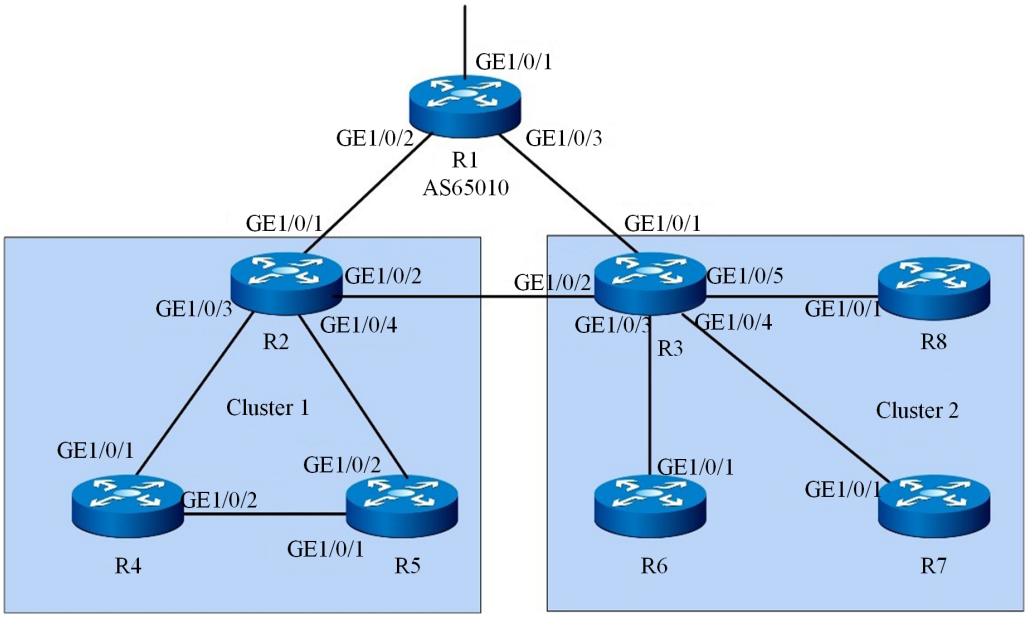


图 4-15 配置BGP路由反射器组网图

Switch	接口	对应的VLAN	IP地址
R1	Gigaethernet 1/0/1	VLAN 10	10.1.1.2/24
R1	Gigaethernet 1/0/2	VLAN 30	10.1.3.2/24
R1	Gigaethernet 1/0/3	VLAN 100	9.1.1.1/24
R2	Gigaethernet 1/0/1	VLAN 10	10.1.1.1/24
R2	Gigaethernet 1/0/2	VLAN 20	10.1.2.1/24
R2	Gigaethernet 1/0/3	VLAN 40	10.1.4.1/24
R2	Gigaethernet 1/0/4	VLAN 50	10.1.5.1/24
R3	Gigaethernet 1/0/1	VLAN 30	10.1.3.1/24
R3	Gigaethernet 1/0/2	VLAN 20	10.1.2.2/24
R3	Gigaethernet 1/0/3	VLAN 70	10.1.7.1/24
R3	Gigaethernet 1/0/4	VLAN 80	10.1.8.1/24
R3	Gigaethernet 1/0/5	VLAN 90	10.1.9.1/24
R4	Gigaethernet 1/0/1	VLAN 40	10.1.4.2/24
R4	Gigaethernet 1/0/2	VLAN 60	10.1.6.1/24
R5	Gigaethernet 1/0/1	VLAN 50	10.1.5.2/24
R5	Gigaethernet 1/0/2	VLAN 60	10.1.6.2/24
R6	Gigaethernet 1/0/1	VLAN 70	10.1.7.2/24
R7	Gigaethernet 1/0/1	VLAN 80	10.1.8.2/24
R8	Gigaethernet 1/0/1	VLAN 90	10.1.9.2/24

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 4-15所示。

各VLANIF接口的IP地址，具体数据如图 4-15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

1. 配置客户机、非客户机与路由反射器之间的IBGP连接（略）。
2. 配置R1发布的本地网络路由9.1.1.0/24（略）。
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。

4.3.3.4 配置BGP4联盟

组网要求

如图 4-16所示，网络中中有多台设备运行BGP，为了减少IBGP的连接数，现将他们划分为3个子自治系：AS65001、AS65002和AS65003。其中AS65001内的三台设备建立IBGP全连接。

组网图

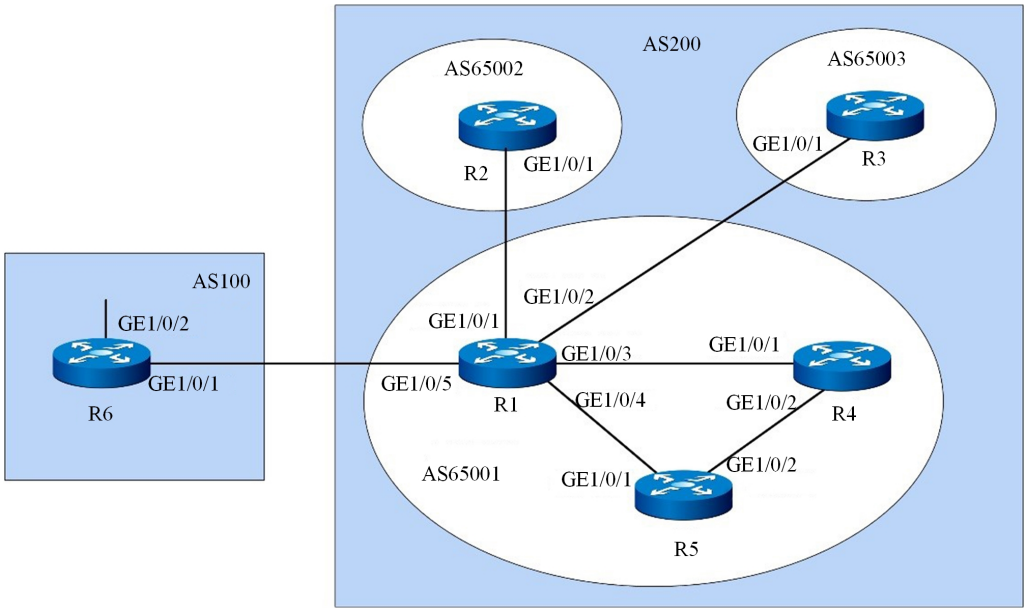


图 4-16 配置联盟组网图

Switch	接口	对应的VLAN	IP地址
R1	Gigaethernet 1/0/1	VLAN 10	10.1.1.1/24
R1	Gigaethernet 1/0/2	VLAN 20	10.1.2.1/24
R1	Gigaethernet 1/0/3	VLAN 30	10.1.3.1/24
R1	Gigaethernet 1/0/4	VLAN 40	10.1.4.1/24
R1	Gigaethernet 1/0/5	VLAN 60	200.1.1.1/24
R2	Gigaethernet 1/0/1	VLAN 10	10.1.1.2/24
R3	Gigaethernet 1/0/1	VLAN 20	10.1.2.2/24
R4	Gigaethernet 1/0/1	VLAN 30	10.1.3.2/24
R4	Gigaethernet 1/0/2	VLAN 50	10.1.5.1/24
R5	Gigaethernet 1/0/1	VLAN 40	10.1.4.2/24
R5	Gigaethernet 1/0/2	VLAN 50	10.1.5.2/24
R6	Gigaethernet 1/0/1	VLAN 60	200.1.1.2/24
R6	Gigaethernet 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AS65001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 4-16所示。

各VLANIF接口的IP地址，具体数据如图 4-16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

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
```

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
```

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
```

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
```

4.4 ISIS 配置

4.4.1 ISIS 简介

4.4.1.1 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）。

4.4.1.2 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：

- 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。
- 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。
- 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。
- 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。
- 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。

4.4.1.3 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。

4.4.1.4 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；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。

- 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。
- 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。
- 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 4-17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。

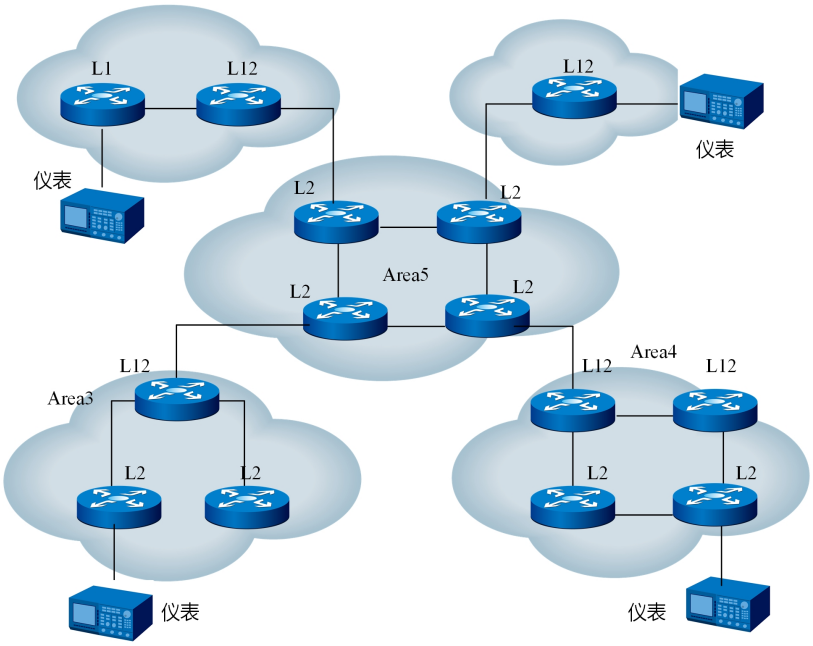


图 4-17 IS-IS经典网络拓扑图

IS-IS报文直接封装在数据链路帧中，主要分3类：

- 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。
- 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。
- 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环境下同时运行，它可以动态发现和生成IPv4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 4-18和图 4-19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之间可以建立IPv4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。

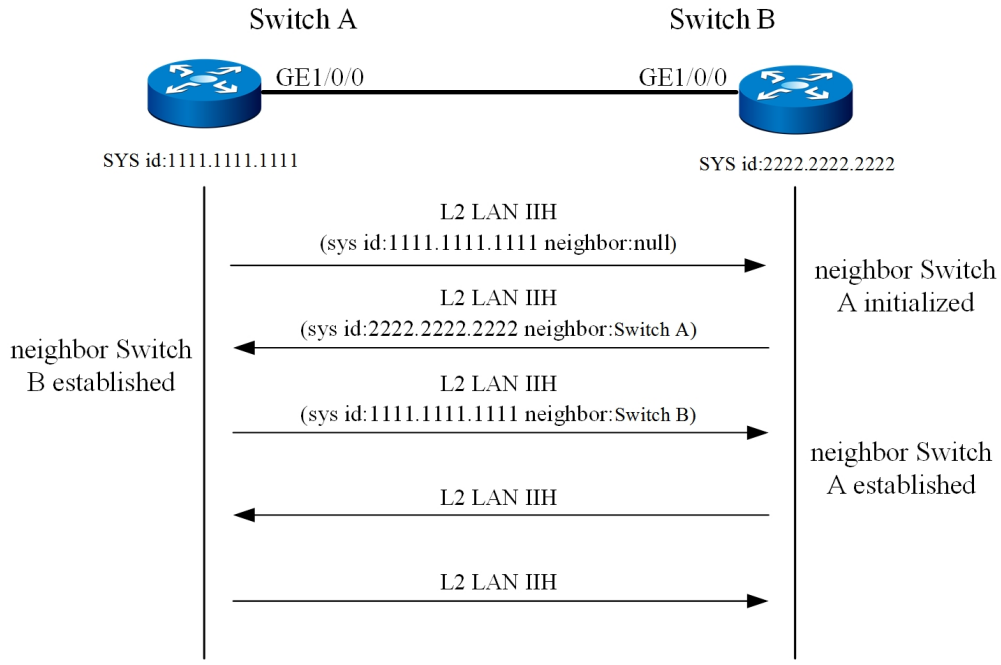


图 4-18　广播链路上的建邻过程

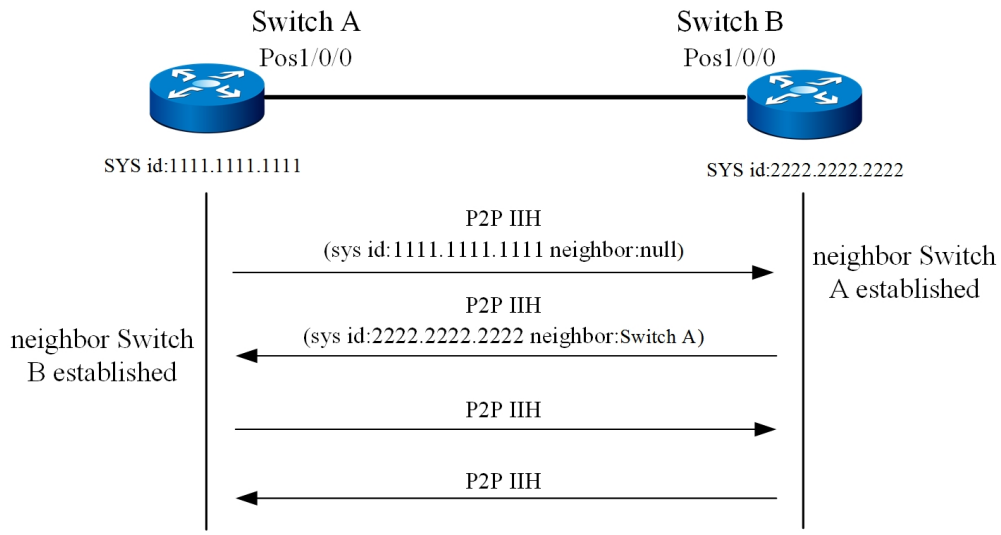


图 4-19 点到点链路上的建邻过程

2. 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 4-20和图 4-21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：

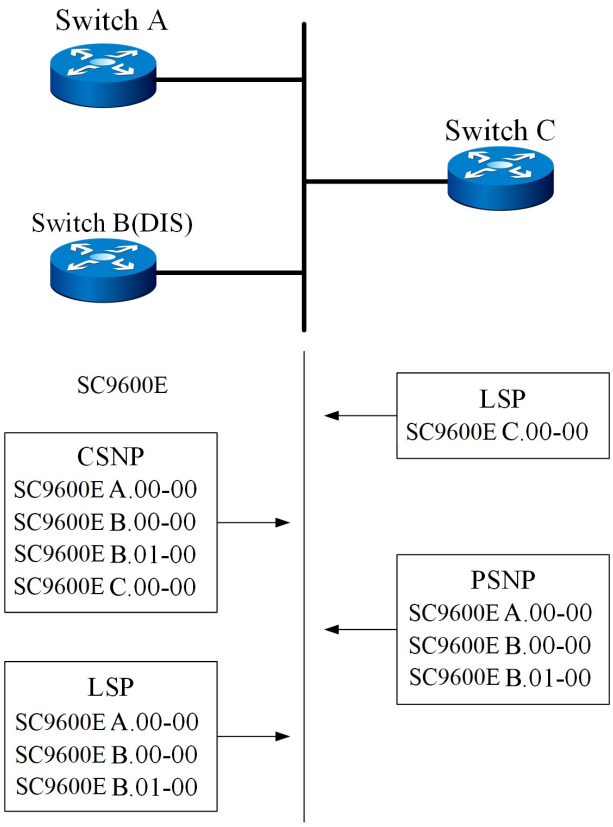


图 4-20　广播链路数据库同步过程

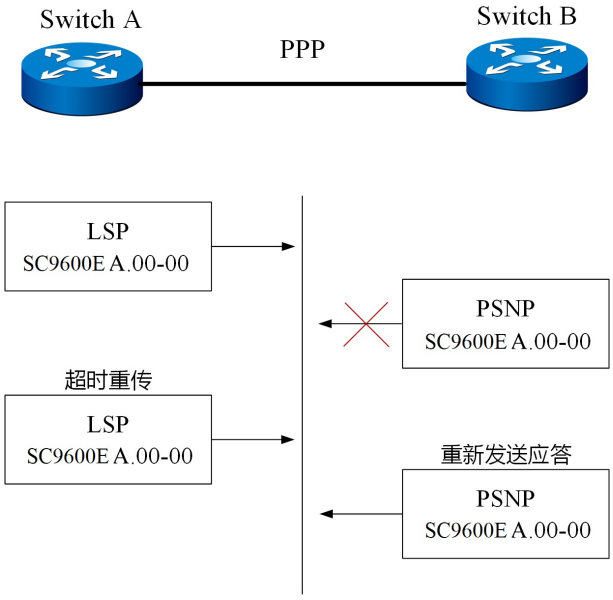


图 4-21　点到点链路数据库同步过程

3. 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：

   当与邻居建立IPv4的邻接关系时，只进行IPv4的路由计算，仅生成IPv4路由。

4.4.2 ISIS 配置步骤

4.4.2.1 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
启动ISIS实例	1. 进入全局配置视图； 2. 执行命令**router isis**进入ISIS配置视图； 3. 执行命令**router isis ISIS-INSTANCE-ID**启动特定实例号的ISIS实例。
关闭ISIS实例	1. 进入全局配置视图； 2. 执行命令**no router isis ISIS-INSTANCE-ID**关闭特定实例号的ISIS实例。
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. 进入全局配置视图； 2. 进入VLANIF配置视图、Loopback接口配置视图； 3. 执行命令**ip router isis [INSTANCE-ID]**。
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. 进入全局配置视图； 2. 进入VLANIF配置视图、Loopback接口配置视图； 3. 执行命令**no ip router isis**。
配置ISIS网络实体标题	1. 进入全局配置视图； 2. 进入ISIS配置视图； 3. 执行命令**net NETWORK-ENTITY-TITLE**。
取消ISIS网络实体标题	1. 进入全局配置视图； 2. 进入ISIS配置视图； 3. 执行命令**no net NETWORK-ENTITY-TITLE**。

目的	步骤
设置ISIS全局的过载位	1. 进入全局配置视图； 2. 进入ISIS配置视图； 3. 执行命令**set-overload-bit**。
取消ISIS全局的过载位	1. 进入全局配置视图； 2. 进入ISIS配置视图； 3. 执行命令**no set-overload-bit**。

4.4.2.2 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置/取消ISIS在广播网络上发送csnp报文的时间间隔	1. 进入全局配置视图； 2. 进入VLANIF配置视图、Loopback接口配置视图； 3. 执行如下命令： ▶ **isis csnp-interval (level-1 | level-2 | ppp) INTERVAL-VALUE** ▶ **no isis csnp-interval (level-1 | level-2 | ppp)**
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. 进入全局配置视图； 2. 进入VLANIF配置视图、Loopback接口配置视图、接口组配置视图； 3. 执行命令**isis passive-interface**或**no isis passive-interface**。
配置/取消ISIS接口下发送hello报文的时间间隔	1. 在特权用户视图下执行命令configure进入全局配置视图； 2. 进入VLANIF配置视图、接口组配置视图、Loopback接口配置视图； 3. 执行如下命令： ▶ **isis hello-interval (level-1 | level-2 | ppp) HELLO-INTERVAL-TIME** ▶ **no isis hello-interval (level-1 | level-2 | ppp)**

目的	步骤
配置/取消ISIS通告邻居超时前没有收到的hello报文个数	1. 进入全局配置视图； 2. 进入VLANIF配置视图、Loopback接口配置视图； 3. 执行如下命令： ▶ **isis hello-multiplier (level-1 | level-2 | ppp) MULTIPLE-VALUEE** ▶ **no isis hello-multiplier (level-1 | level-2 | ppp)**
配置/取消ISIS接口下的链路开销	1. 进入全局配置视图； 2. 进入VLANIF配置视图、接口组配置视图； 3. 执行如下命令： ▶ **isis default-metric (level-1 | level-2 | ppp) DEFAULT-METRIC** ▶ **no isis default-metric (level-1 | level-2 | ppp)**
配置/取消接口下的宽开销值	1. 进入全局配置视图； 2. 进入VLANIF配置视图、Loopback接口配置视图； 3. 执行如下命令： ▶ **isis wide-metric (level-1 | level-2 | ppp) METRIC** ▶ **no isis wide-metric (level-1 | level-2 | ppp)**
配置/取消ISIS接口优先级，用于DIS选举	1. 进入全局配置视图； 2. 进入VLANIF配置视图、Loopback接口配置视图； 3. 执行如下命令： ▶ **isis priority (level-1 | level-2) PRIORITY-VALUE** ▶ **no isis priority (level-1 | level-2)**
使能/取消ISIS接口下的三次握手功能，只针对p2p接口	1. 进入全局配置视图； 2. 进入VLANIF配置视图、Loopback接口配置视图； 3. 执行如下命令： ▶ **isis three-way-handshake** ▶ **no isis three-way-handshake**
配置/取消ISIS接口下psnp报文发送间隔	1. 进入全局配置视图； 2. 进入VLANIF配置视图、Loopback接口配置视图； 3. 执行如下命令： ▶ **isis psnp-interval (level-1 | level-2 | ppp) INTERVAL-VALUE** ▶ **no isis psnp-interval (level-1 | level-2 | ppp)**

目的	步骤
配置一个ISIS接口的电路类型	1. 进入全局配置视图； 2. 进入VLANIF配置视图、Loopback接口配置视图、接口组配置视图、接口组配置视图； 3. 执行命令**isis circuit-type (broadcast | ppp)**
使能/取消ISIS接口下发送hello报文的自动填充功能	1. 进入全局配置视图； 2. 进入VLANIF配置视图、Loopback接口配置视图、接口组配置视图； 3. 执行如下命令： ▶ **isis hello padding** ▶ **no isis hello padding**
配置/取消ISIS接口加入指定的mesh-group	1. 进入全局配置视图； 2. 进入VLANIF配置视图、Loopback接口配置视图、接口组配置视图； 3. 执行如下命令： ▶ **isis mesh-group GROUP-VALUE** ▶ **no isis mesh-group**
使能ISIS接口下的mesh-group阻塞功能	1. 进入全局配置视图； 2. 进入VLANIF配置视图、Loopback接口配置视图、接口组配置视图、接口组配置视图； 3. 执行命令**isis mesh-group blocked**。
重置所有或单个ISIS实例计数信息	1. 进入全局配置视图； 2. 执行命令**reset isis [ISIS-INSTANCE] counter**。

4.4.2.3 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置/恢复一个ISIS接口层级	1. 进入全局配置视图； 2. 进入VLANIF配置视图、Loopback接口配置视图； 3. 执行如下命令。 ▶ **isis circuit-level (level-1 | level-1-2 | level-2)** ▶ **no isis circuit-level**
配置ISIS全局的系统层级	1. 进入全局配置视图； 2. 进入ISIS配置视图； 3. 执行命令**is-type (level-1 | level-1-2 | level-2)**。

4.4.2.4 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置ISIS全局下lsp刷新时间间隔	1. 进入全局配置视图； 2. 进入ISIS配置视图； 3. 执行命令**lsp-refresh-interval INTERVAL-VALUE**。
配置ISIS全局lsp最大生存时间	1. 进入全局配置视图； 2. 进入ISIS配置视图； 3. 执行命令**max-lsp-lifetime LIFETIME**。
使能/取消ISIS全局下接收lsp报文的校验和检查	1. 进入全局配置视图； 2. 进入ISIS配置视图； 3. 执行如下命令： ▶ **ignore-lsp-errors (level-1 | level-2)** ▶ **no ignore-lsp-errors (level-1 | level-2)**

4.4.2.5 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
使能/去使能路由重分配功能，引入其他路由协议的路由信息	1. 进入全局配置视图； 2. 进入ISIS配置视图； 3. 执行如下命令： ▶ **redistribute (connect | static | rip | bgp | ospf | isis) (level-1 | level-2 | level-1-2)** ▶ **no redistribute (connect | static | rip | bgp | ospf | isis)**
使能/去使能ISIS的level-2到level-1的路由渗透功能	1. 进入全局配置视图； 2. 进入ISIS配置视图； 3. 执行如下命令： ▶ **redistribute level-2 to level-1** ▶ **no redistribute level-2 to level-1**

4.4.2.6 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置/取消一个ISIS汇总路由	1. 进入全局配置视图； 2. 进入ISIS配置视图； 3. 执行如下命令： ▶ **summary-address IP-ADDRESS MASK-ADDRESS（level-1 | level-2）** ▶ **no summary-address IP-ADDRESS MASK-ADDRESS（level-1 | level-2）**

4.4.2.7 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报文等。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置/取消ISIS全局下的区域认证	1. 进入全局配置视图； 2. 进入ISIS配置视图； 3. 执行如下命令： ▶ **area-password (simple | md5) PASSWORD** ▶ **no area-password**
配置/取消ISIS全局下的域间认证	1. 进入全局配置视图； 2. 进入ISIS配置视图； 3. 执行如下命令： ▶ **domain-password (simple | md5) PASSWORD** ▶ **no domain-password**
配置/取消ISIS接口以指定的方式和密码验证Hello报文	1. 进入全局配置视图； 2. 进入VLANIF配置视图、Loopback接口配置视图； 3. 执行如下命令： ▶ **isis password (simple | md5) PASSWORD (level-1 | level-2 | ppp)** ▶ **no isis password (level-1 | level-2 | ppp)**

4.4.2.8 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
使能/取消ISIS全局下的GR功能	1. 进入全局配置视图； 2. 进入ISIS配置视图； 3. 执行如下命令： ▶ **graceful-restart enable** ▶ **graceful-restart disable**

4.4.2.9 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
使能/取消ISIS全局下的TE功能	1. 进入全局配置视图； 2. 进入ISIS配置视图； 3. 执行命令**traffic-engineer (enable | disable) (level-1 | level-2)**。
使能/取消ISIS全局下的SNMP告警功能	1. 进入全局配置视图； 2. 进入ISIS配置视图； 3. 执行如下命令： ▶ **snmp-trap enable** ▶ **snmp-trap disable**
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. 进入全局配置视图； 2. 进入ISIS配置视图； 3. 执行如下命令： ▶ **hostname HOST-NAME** ▶ **no hostname**

4.4.2.10 维护及调试

目的

当ISIS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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
显示指定level的isis database信息	1. 进入普通用户视图、特权用户视图、全局配置视图、VLANIF配置视图、Loopback接口配置视图、ISIS配置视图； 2. 执行命令**show ip isis database（level-1 | level-2）INSTANCE-ID**。
显示链路状态数据库信息	1. 进入普通用户视图、特权用户视图、全局配置视图、VLANIF配置视图、Loopback接口配置视图、ISIS配置视图； 2. 执行如下命令： ▶ **show ip isis database** ▶ **show ip isis database verbose** ▶ **show ip isis database verbose LSP-INDEX**
显示ISIS数据库统计信息	1. 进入普通用户视图、特权用户视图、全局配置视图、VLANIF配置视图、Loopback接口配置视图、ISIS配置视图； 2. 执行命令**show ip isis database count**。
显示ISIS邻居的详细信息	1. 进入普通用户视图、特权用户视图、全局配置视图、VLANIF配置视图、Loopback接口配置视图、ISIS配置视图； 2. 执行命令**show ip isis neighbor verbose**。
显示ISIS的邻居信息	1. 进入普通用户视图、特权用户视图、全局配置视图、VLANIF配置视图、Loopback接口配置视图、ISIS配置视图； 2. 执行命令**show ip isis neighbor**。
显示ISIS的基本配置信息	1. 进入普通用户视图、特权用户视图、全局配置视图、VLANIF配置视图、Loopback接口配置视图、ISIS配置视图； 2. 执行命令**show ip isis config**。
显示ISIS动态主机映射	1. 进入普通用户视图、特权用户视图、全局配置视图、VLANIF配置视图、Loopback接口配置视图、ISIS配置视图； 2. 执行命令**show ip isis hostname**。
显示ISIS接口信息	1. 进入普通用户视图、特权用户视图、全局配置视图、VLANIF配置视图、Loopback接口配置视图、ISIS配置视图； 2. 执行命令**show ip isis interface**。
显示ISIS接口详细信息	1. 进入普通用户视图、特权用户视图、全局配置视图、VLANIF配置视图、Loopback接口配置视图、ISIS配置视图； 2. 执行命令**show ip isis interface verbose**。
显示ISIS实例信息	1. 进入普通用户视图、特权用户视图、全局配置视图、VLANIF配置视图、Loopback接口配置视图、ISIS配置视图； 2. 执行命令**show ip isis INSTANCE-ID**。

目的	步骤
显示ISIS学到的路由信息	1. 进入普通用户视图、特权用户视图、全局配置视图、VLANIF配置视图、Loopback接口配置视图、ISIS配置视图； 2. 执行如下命令： ▶ **show ip isis route** ▶ **show ip isis route (level-1 | level-2)** ▶ **show ip isis route DST-IP-ADDRESS** ▶ **show ip isis route all**
导出主备盘上的ISIS数据到uspisis_diagnose_isis文件	1. 进入普通用户视图； 2. 执行命令**dump ha isis table**。

4.4.3 ISIS 配置举例

4.4.3.1 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 4-22所示。

组网图

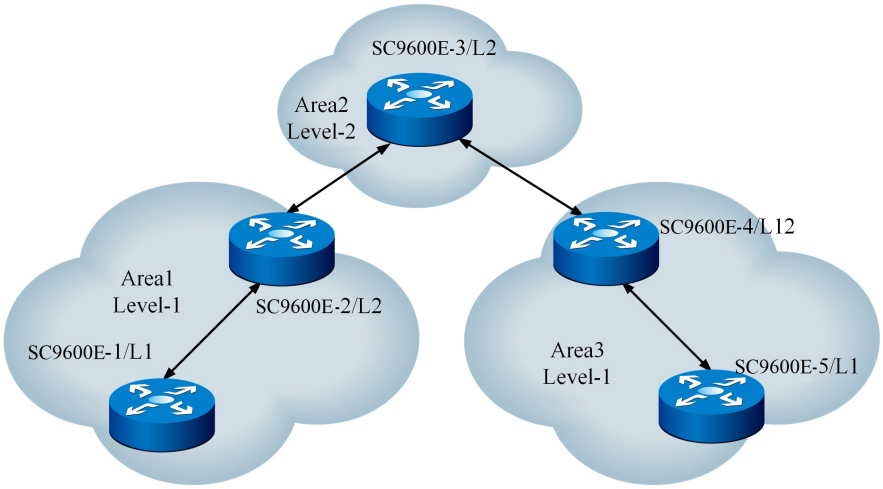


图 4-22 ISIS基本配置拓扑图

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SC9600E_2和SC9600E_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Area3为Level-1区域，Area2为Level-2区域。

Area1区域地址为10，Area2区域地址为20，Area3区域地址为30。

SC9600E_1 NET为10.0001.0001.0001.00，接口地址：1.1.1.1/24。

SC9600E_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。

SC9600E_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。

SC9600E_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。

SC9600E_5 NET为30.0005.0005.0005.00，接口地址：4.1.1.1/24。

配置步骤

```
SC9600E_1:
SC9600E_1(config)#router isis
SC9600E_1(config-isis-1)#net 10.0001.0001.0001.00
SC9600E_1(config-isis-1)#is-type level-1
SC9600E_1(config-isis-1)#exit
SC9600E_1(config)#interface vlan 1
SC9600E_1(config-vlan-1)#ip router isis

SC9600E_2:
SC9600E_2 (config)#router isis
SC9600E_2 (config-isis-1)#net 10.0002.0002.0002.00
SC9600E_2 (config-isis-1)#is-type level-1-2
SC9600E_2 (config-isis-1)#exit
SC9600E_2 (config)#int vlan 1
SC9600E_2 (config-vlan-1)#ip router isis
SC9600E_2 (config-vlan-1)#exit
SC9600E_2 (config)#int vlan 2
SC9600E_2 (config-vlan-2)#ip router isis
```

```
SC9600E_3:
SC9600E_3 (config)#router isis
SC9600E_3 (config-isis-2)#net 20.0003.0003.0003.00
SC9600E_3 (config-isis-2)#is-type level-2
SC9600E_3 (config-isis-2)#exit
SC9600E_3 (config)#int vlan 2
SC9600E_3 (config-vlan-2)#ip router isis
SC9600E_3 (config-vlan-2)#exit
SC9600E_3 (config)#int vlan 3
SC9600E_3 (config-vlan-3)#ip router isis

SC9600E_4:
SC9600E_4 (config)#router isis
SC9600E_4 (config-isis-2)#net 30.0004.0004.0004.00
SC9600E_4 (config-isis-2)#is-type level-1-2
SC9600E_4 (config-isis-2)#exit
SC9600E_4 (config)#int vlan 3
SC9600E_4 (config-vlan-3)#ip router isis
SC9600E_4 (config-vlan-1)#exit
SC9600E_4 (config)#int vlan 4
SC9600E_4 (config-vlan-4)#ip router isis

SC9600E_5:
SC9600E_5 (config)#router isis
SC9600E_5 (config-isis-1)#net 30.0005.0005.0005.00
SC9600E_5 (config-isis-1)#is-type level-1
SC9600E_5 (config-isis-1)#exit
SC9600E_5 (config)#int vlan 4
SC9600E_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。

4.4.3.2 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 4-23所示。

组网图

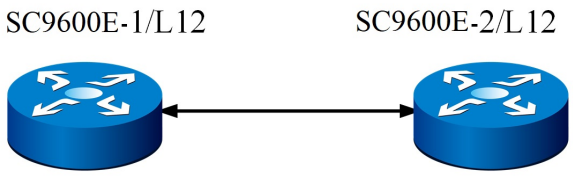


图 4-23　ISIS重分配拓扑图

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SC9600E_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：

- 接受所有直连路由，并重分配到level-1；
- 接收所有RIP路由，并重分配到level-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SC9600E_1上配置重分配：

```
SC9600E_1(config-isis-1)#redistribute connect level-1
SC9600E_1(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。

4.4.3.3　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 4-24所示。

组网图

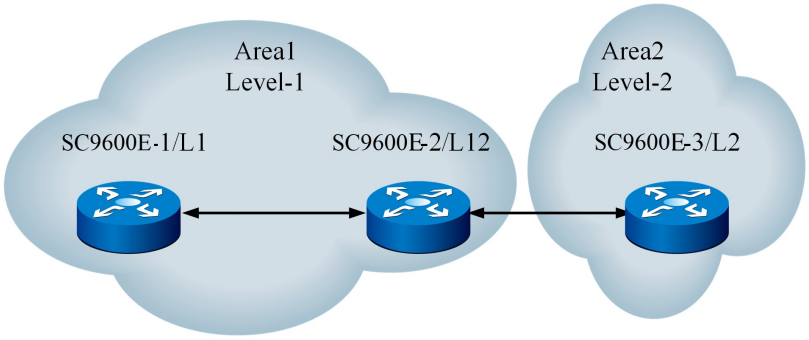


图 4-24 ISIS路由汇总拓扑图

配置思路

SC9600E_1上有10.1.1.0/24~10.1.10.0/24这10条路由，希望减小SC9600E_3的路由表容量，让SC9600E_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SC9600E_2上配置路由汇总命令，配置完后SC9600E_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SC9600E_2上配置路由汇总：

```
SC9600E_2(config)# router isis
SC9600E_2(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。

4.4.3.4 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 4-25所示。

组网图

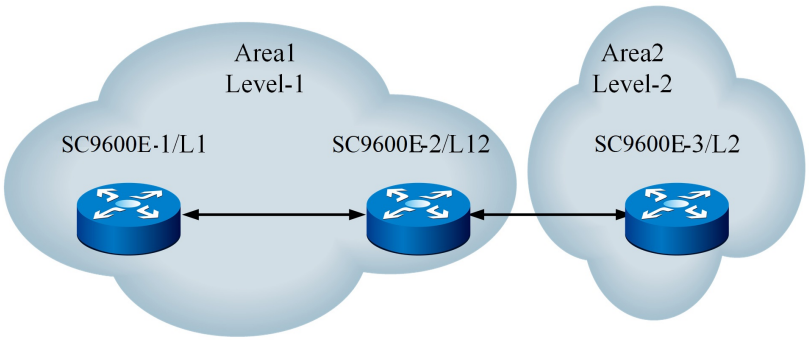


图 4-25　ISIS认证拓扑图

配置思路

要求SC9600E_1和SC9600E_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SC9600E_1和SC9600E_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：

```
SC9600E_1：
SC9600E_1(config)#router isis
SC9600E_1(config-isis-1)#area-password simple 12345
SC9600E_1(config-isis-1)#domain-password md5 cmcc
SC9600E_1(config-isis-1)#quit
SC9600E_1(config)#interface vlan 1
SC9600E_1(config- vlan-1)#isis password simple 123456 level-1
SC9600E_1(config- vlan-1)#isis password md5 fhn level-2

SC9600E_2：
SC9600E_2(config)# router isis
```

```
SC9600E_2(config-isis-1)#area-password simple 12345
SC9600E_2(config-isis-1)#domain-password md5 cmcc
SC9600E_2(config-isis-1)#quit
SC9600E_2(config)#interface vlan 1
SC9600E_2(config- vlan-1)#isis password simple 123456 level-1
SC9600E_2(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。

4.4.3.5 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 4-26所示。

组网图

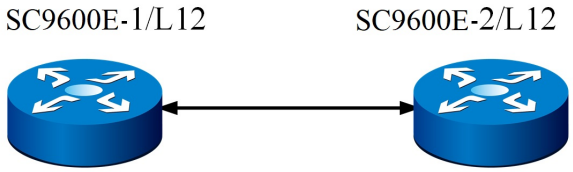


图 4-26 ISIS GR拓扑图

配置思路

2个设备都运行ISIS，并将有个都配置同一Area，SC9600E_1和SC9600E_2都需要使能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：

```
SC9600E_1:
```

```
SC9600E_1(config)#router isis
SC9600E_1(config-isis-1)#graceful-restart enable
SC9600E_2:
SC9600E_2(config)#router isis
SC9600E_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。

4.5 策略路由配置

4.5.1 策略路由概述

Policy Route（策略路由）协议概述

传统上，普通的报文转发是依据报文的目的地址查询转发表来实现的，当遇到需要根据源IP来控制报文转发，根据报文的长度来控制报文转发或根据报文的其他属性来控制报文转发时，就需要一种新的路由机制来控制，也就是策略路由来控制。

所谓策略路由，顾名思义，即是根据一定的策略进行报文转发，因此策略路由是一种比目的路由更灵活的路由机制。在路由器转发一个数据报文时，首先根据配置的规则对报文进行过滤，匹配成功则按照一定的转发策略进行报文转发。这种规则可以是基于标准和扩展访问控制列表，也可以基于报文的长度；而转发策略则是控制报文按照指定的策略路由表进行转发，也可以修改报文的IP优先字段。因此，策略路由是对传统IP路由机制的有效增强。

Policy Route（策略路由）协议介绍

策略路由能满足基于源IP地址、目的IP址、协议字段，甚至于TCP、UDP的源、目的端口等多种组合进行选路。简单点来说，只要IP standard/extended ACL 能设置的，都可以做为策略路由的匹配规则进行转发。

策略路由（Policy Route）在决定一个IP包的下一跳转发地址或是下一跳缺省IP地址时，不是简单的根据目的IP地址决定，而是综合考虑多种因素来决定。如可以根据DSCP（差分服务代码点）字段、源和目的端口号，源IP地址等来为数据包选择路径。策略路由可以在一定程度上实现流量工程，使不同服务质量的流或者不同性质的数据（语音、FTP）走不同的路径。

基于策略的路由为网络管理者提供了比传统路由协议对报文的转发和存储更强的控制能力。传统上，路由器用从路由协议派生出来的路由表，根据目的地址进行报文的转发。基于策略的路由比传统路由能力更强，使用更灵活，它使网络管理者不仅能够根据目的地址而且能够根据协议类型、报文大小、应用或I P源地址来选择转发路径。策略可以定义为通过多路由器的负载平衡或根据总流量在各线上进行报文转发的服务质量（QoS）。

策略路由功能的实现是依靠芯片的支持，策略路由功能是通过命令行或其它配置界面，将软件表项转换为硬件表项存储到芯片上去，当流量通过时，芯片会按照策略路由硬件表来过滤报。

4.5.2 配置策略路由功能

目的

本节介绍配置策略路由的功能的相关操作。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
创建或修改策略路由和策略点，并进入策略路由配置视图	1. 执行命令configure进入全局配置视图； 2. 执行命令**policy-based-route NAME（permit | deny）node NODE-ID**。
删除策略路由	1. 进入全局配置视图； 2. 执行如下命令： ▶ **no policy-based-route NAME** ▶ **no policy-based-route NAME node NODE-ID**

目的	步骤
配置策略路由应用的IP报文优先级	1. 执行命令configure进入全局配置视图； 2. 执行命令**policy-based-route NAME（permit | deny）node NODE-ID**创建或修改策略路由和策略点，并进入策略路由配置视图； 3. 执行命令**no apply ip-precedence**。
配置策略路由应用的报文下一跳IP地址	1. 执行命令configure进入全局配置视图； 2. 执行命令**policy-based-route NAME（permit | deny）node NODE-ID**创建或修改策略路由和策略点，并进入策略路由配置视图； 3. 执行如下命令： ▶ **apply ip-address next-hop IP-ADDRESS1** ▶ **apply ip-address next-hop IP-ADDRESS1 IP-ADDRESS2**
取消策略路由应用的报文下一跳IP地址	1. 执行命令configure进入全局配置视图； 2. 执行命令**policy-based-route NAME（permit | deny）node NODE-ID**创建或修改策略路由和策略点，并进入策略路由配置视图； 3. 执行命令**no apply ip-address next-hop**。
配置重定向的下一跳IP地址	1. 执行命令configure进入全局配置视图； 2. 执行命令**policy-based-route NAME（permit | deny）node NODE-ID**创建或修改策略路由和策略点，并进入策略路由配置视图； 3. 执行命令**apply load-balance ip-address next-hop NEXT-HOP-ADDRESS**。
配置基于访问列表策略路由的ACL匹配条件	1. 执行命令configure进入全局配置视图； 2. 执行命令**policy-based-route NAME（permit | deny）node NODE-ID**创建或修改策略路由和策略点，并进入策略路由配置视图； 3. 执行命令**if-match acl acl-number**。
取消基于访问列表策略路由的ACL匹配条件	1. 执行命令configure进入全局配置视图； 2. 执行命令**policy-based-route NAME（permit | deny）node NODE-ID**创建或修改策略路由和策略点，并进入策略路由配置视图； 3. 执行命令**no if-match acl**。

目的	步骤
删除接口应用的策略路由	1. 执行命令configure进入全局配置视图； 2. 执行命令进入接口配置视图（包括trunk接口、以太网子接口）； 3. 执行命令**no ip policy-based-route POLICYNAME**。
在策略路由的NODE节点下绑定Time Range	1. 执行命令configure进入全局配置视图； 2. 执行命令**policy-based-route NAME (permit | deny) node NODE-ID**创建或修改策略路由和策略点，并进入策略路由配置视图；； 3. 执行命令**bind time-range list LIST-NUMBER**。

4.5.3 对ISIS协议应用路由策略

目的

使用本节操作配置ISIS协议中的路由命令引用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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
重分配路由	1. 进入全局配置视图； 2. 进入ISIS配置视图； 3. 执行命令**redistribute (connect | static | rip | bgp | ospf | isis) route-policy POLICY-NAME**。
配置ISIS路由加入IP路由表时的过滤策略	1. 进入全局配置视图； 2. 进入ISIS配置视图； 3. 执行命令**filter-policy import route-policy ROUTE-POLICY-NAME**。

4.5.4 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
对OSPF发布的路由应用路由策略	1. 进入全局配置视图； 2. 进入OSPFv2配置视图； 3. 执行命令**filter route-policy ROUTE-POLICY-NAME**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。
对OSPF引入外部路由时应用路由策略	1. 进入全局配置视图； 2. 进入OSPFv2配置视图； 3. 执行命令**redistribute (static | connect | rip | bgp | isis | ospf) route-policy POLICY-NAME**用来配置引入不同的路由策略。

4.5.5 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
对BGP邻居接收的路由应用路由策略	1. 进入全局配置视图； 2. 进入BGP配置视图； 3. 执行命令**neighbor IPV4-ADDRESS route-policy ROUTE-POLICY-NAME import**。
对BGP发布的路由应用路由策略	1. 进入全局配置视图； 2. 进入BGP配置视图； 【步骤3和步骤4，用户根据实际情况任选】 3. 执行命令**filter-policy export route-policy POLICY-NAME**用来配置路由过滤策略命令； 4. 执行命令**filter-policy export (static | connected | rip | ospf | isis) route-policy ROUTE-POLICY-NAME**用来配置路由过滤策略命令。
对BGP邻居发布的路由应用路由策略	1. 进入全局配置视图； 2. 进入BGP配置视图； 3. 执行命令**neighbor IPV4-ADDRESS route-policy ROUTE-POLICY-NAME export**用来配置路由过滤策略命令。
对BGP引入外部路由时应用路由策略	1. 进入全局配置视图； 2. 进入BGP配置视图； 3. 执行命令**redistribute (static | connected | rip | ospf | isis) route-policy ROUTE-POLICY-NAME**用来配置路由过滤策略命令。

4.5.6 维护及调试

目的

当策略路由功能不正常，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
显示策略路由信息	1. 进入以下任意一个视图： ▶ 不执行任何命令保持当前特权用户视图 ▶ 执行命令**configure**进入全局配置视图 ▶ 执行命令**disable**退出到普通用户视图 ▶ 执行命令**policy-based-route NAME (permit | deny) node NODE-ID**创建或修改策略路由和策略点，并进入策略路由配置视图； 2. 执行如下命令： ▶ **show ip policy-based-route** ▶ **show ip policy-based-route POLICY-NAME**
显示策略路由配置信息	1. 进入以下任意一个视图： ▶ 不执行任何命令保持当前特权用户视图 ▶ 执行命令**configure**进入全局配置视图 ▶ 执行命令**disable**退出到普通用户视图 ▶ 执行命令**policy-based-route NAME (permit | deny) node NODE-ID**创建或修改策略路由和策略点，并进入策略路由配置视图； 2. 执行命令**show ip policy-based-route config**显示策略路由配置信息。

4.5.7 配置举例

4.5.7.1 配置基于ACL的策略路由

组网需求

如图 4-27所示，定义一条名为aaa的策略路由，所有从以太网接口10GE1/1/2接收的IP报文通过接口10GE1/1/3发送，下一跳IP是1.1.2.2，其它报文仍然按照查找路由表的方式转发。

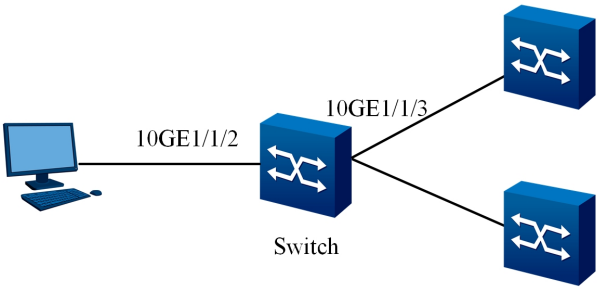


图 4-27 基于ACL的策略路由

配置思路

基于ACL的策略路由配置思路如下：

1. 首先定义ACL；
2. 定义策略路由的规则和动作；
3. 在接口上使能策略路由。

数据准备

完成该配置举例，需要准备如下数据：

- ACL编号及规则
- 策略路由的名称
- 策略路由执行动作所使用的下一跳IP地址

配置步骤

1、配置ACL，定义访问控制列表，ACL filter 1 匹配IP报文。

```
SC9600E(config)#filter-list 1001
SC9600E(configure-filter-ipv4-1001)#filter 1 ip any any
SC9600E(configure-filter-ipv4-1001)#filter 1 action permit
```

2、定义策略的规则和动作。

```
SC9600E(config)#policy-based-route aaa permit node 5
SC9600E(config-policy-based-route-aaa-5)#if-match acl 1001
SC9600E(config-policy-based-route-aaa-5)#apply ip-address next-hop 1.1.2.2
SC9600E(config-policy-based-route-aaa-5)#quit
```

3、在接口上使能策略。

```
SC9600E(config)#interface 10gigaethernet 1/1/2
SC9600E(config-10ge1/1/2)#ip policy-based-route aaa
```

4.6 Hwroute 配置

4.6.1 Hwroute 概述

Hwroute模块仅用于用户进行命令诊断调试所用。

4.6.2 维护及调试

目的

当路由表项不正常，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
打开或关闭路由下硬件的调试功能	1. 不执行任何命令保持当前特权用户视图； 2. 执行如下命令： ▶ **debug hwroute (arp | route | tunnel | ilm | l2vpn | evpn | l3vpn | rtm | all)** ▶ **no debug hwroute (arp | route | tunnel | ilm | l2vpn | evpn | l3vpn | rtm | all)**
查看IPv4路由表项	1. 执行命令disable退出到普通用户视图； 2. 执行如下命令： ▶ **show hwroute hardware route4** ▶ **show hwroute hardware arp** ▶ **show hwroute hardware ilm**

目的	步骤
查看IPv6路由表项	1. 执行命令disable退出到普通用户视图； 2. 执行如下命令： ▶ **show hwroute hardware route6** ▶ **show hwroute hardware nd**
查看因为下一跳不可达IPv4路由表项	1. 执行命令**disable**退出到普通用户视图； 2. 执行命令**show hwroute hardware route4 pend**查看因为下一跳不可达IPv4路由表项。
查看因为下一跳不可达IPv6路由表项	1. 执行命令**disable**退出到普通用户视图； 2. 执行命令**show hwroute hardware route6 pend**查看因为下一跳不可达IPv6路由表项。
查看IPv4或IPv6 ECMP路由组信息	1. 执行命令**disable**退出到普通用户视图； 2. 执行如下命令： ▶ **show hwroute ecmp-group** ▶ **show hwroute ecmp-group6**
查看IPv4或IPv6下一跳ID对应的信息	1. 执行命令**disable**退出到普通用户视图； 2. 执行如下命令： ▶ **show hwroute nexthop ROUTE-ID** ▶ **show hwroute nexthop6 ROUTE-ID**
查看HwRoute模块接收路由消息统计信息	1. 执行命令**disable**退出到普通用户视图； 2. 执行命令**show hwroute statistic rtm**查看HwRoute模块接收路由消息统计信息。
查看HwRoute模块路由消息统计信息	1. 执行命令**disable**退出到普通用户视图； 2. 执行命令**show hwroute statistic route (v4 | v6 | all)**查看HwRoute模块路由消息统计信息。

5 QoS 配置

本章介绍了SC9600E系列数据中心交换机QoS的基本内容、配置过程和配置举例。

5.1 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。

SC9600E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，即保证能够通过的平均速率。整数形式，取值范围是22-4294967295，单位为kbit/s。
- cbs-value：指定承诺突发尺寸，即瞬间能够通过的承诺突发流量。整数形式，取值范围是1-32768，单位是kbit/s。

- pir-value：指定峰值信息速率。整数形式，取值范围是是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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置对某个meter进行绑定	1. 进入全局配置视图； 2. 进入filter配置视图； 3. 执行命令**filter RULE-NUMBER meter METER-NUMBER**。
取消filter与某个meter的绑定关系	1. 进入全局配置视图； 2. 进入filter配置视图； 3. 执行命令**no filter RULE-NUMBER meter**。
配置通过meter对包括CIR、CBS、PIR、EBS和PBS的限速规则的指定	1. 进入全局配置视图； 2. 执行如下命令： ▶ **meter METER-NUMBER cir CIR-NUMBER cbs CBS-NUMBER ebs EBS-NUMBER** ▶ **meter METER-NUMBER cir CIR-NUMBER cbs CBS-NUMBER ebs EBS-NUMBER（ebs | 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（ebs| blind）** ▶ **no meter METER-NUMBER**

5.2 队列调度和拥塞控制配置

5.2.1 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，如可分配的处理器时间、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。

5.2.2 配置队列调度及拥塞控制

目的

使用本节操作配置队列调度及拥塞控制。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置端口队列的调度模式	1. 进入端口配置视图； 2. 执行如下命令配置端口队列的调度模式： ▶ **cos scheduling（sp | rr | wrr | drr | wfq）** ▶ **cos scheduling（sp+rr | sp+wrr | sp+drr | sp+wfq）QUEUE-LIST**
（可选）配置端口队列的权重	1. 进入端口配置视图； 2. 执行命令**cos queue QUEUE-LIST weight WEIGHT**配置端口队列的权重。

5.2.3 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，可以使用本小节操作。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
查看cos配置信息	1. 进入普通用户视图； 2. 执行命令**show cos config**查看cos配置信息。

5.2.4 配置举例

5.2.4.1 SP调度配置示例

组网要求

流量从站点1的端口10GE1/0/1、10GE1/0/2、10GE1/0/3上到站点2后，在端口10GE1/0/1产生拥塞，要求使用调度算法为SP。

组网图

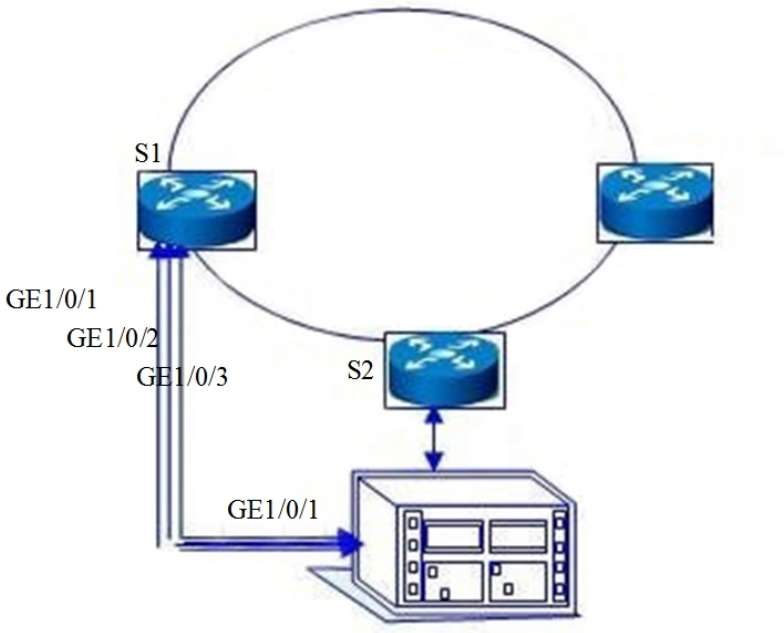


图 5-1　配置端口队列优先级调度组网图

配置步骤

1. 站点1的配置。

#端口10GE1/0/1的配置。

```
S1#configure
S1(config)#interface 10gigaethernet 1/0/1
S1(config-10ge1/0/1)#priority 1
S1(config-10ge1/0/1)#quit
```

退出端口10GE1/0/1的配置。

#端口10GE1/0/2的配置。

```
S1#configure
S1(config)#interface 10gigaethernet 1/0/2
S1(config-10ge1/0/2)#priority 2
S1(config-10ge1/0/2)#quit
```

退出端口GE1/0/2的配置。

#端口10GE1/0/3的配置。

```
S1#configure
```

```
S1(config)#interface 10gigaethernet 1/0/3
S1(config-10ge1/0/3)#priority 3
S1(config-10ge1/0/3#quit
```

退出端口10GE1/0/3的配置。

2. 站点2的配置。

#配置ACL规则。

```
S2#configure
S2(config)#filter-list 1001
S2(configure-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10GE1/0/1。

```
S2#configure
S2(config)#interface 10ge 1/0/1
S2(config-10ge1/0/1)#cos schedule sp
S2(config-10ge1/0/1)#filter-list in 1001
```

6 组播配置

本章介绍了SC9600E系列数据中心交换机组播配置操作。

6.1 IGMP Snooping 配置

6.1.1 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。

SC9600E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

6.1.2 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
全局使能IGMP Snooping	1. 进入全局配置视图； 2. 执行命令**igmp-snooping start**全局使能组播监听功能。
创建组播VLAN	1. 进入全局配置视图； 2. 执行命令**vlan VLAN-LIST**创建需要使能IGMP Snooping的VLAN； 3. 执行命令**igmp-snooping mvlan VLAN-ID**创建相应组播VLAN并进入组播VLAN配置视图。
配置接口加入VLAN并在接口上使能IGMP Snooping协议	1. 进入全局配置视图； 2. 进入接口配置视图（以太网接口、trunk接口）、接口组配置视图； 3. 执行命令**port hybrid vlan VLAN-LIST (tagged | untagged)**配置Hybrid类型接口所属VLAN； 4. 执行命令**igmp-snooping enable**配置在接口上使能组播监听。
配置静态组播地址表成员接口	1. 进入全局配置视图； 2. 进入接口配置视图（以太网接口、trunk接口）、接口组配置视图 3. 执行命令**igmp-snooping static-group group-address GROUP-ADDRESS mvlan VLAN-ID**配置静态组播地址表成员接口。
创建组播预加入组功能	1. 进入全局配置视图； 2. 执行命令**igmp-snooping group-address GROUP-ADDRESS mvlan VLAN-ID**创建组播预加入组功能。

6.1.3 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
全局使能IGMP Snooping	1. 进入全局配置视图； 2. 执行命令**igmp-snooping start**全局使能组播监听功能。
创建组播VLAN	1. 进入全局配置视图； 2. 执行命令**vlan VLAN-LIST**创建需要使能IGMP Snooping的VLAN； 3. 执行命令**igmp-snooping mvlan VLAN-ID**创建相应组播VLAN并进入组播VLAN配置视图。
使能组播VLAN的组播复制功能	1. 进入全局配置视图； 2. 进入组播VLAN配置视图； 3. 执行命令**igmp-snooping multicast-vlan enable**使能组播VLAN复制功能。
配置组播监听上联口	1. 进入全局配置视图； 2. 进入组播VLAN配置视图； 3. 执行命令**igmp-snooping uplink-port (ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 40gigaethernet) INTERFACE-NUMBER**或**igmp-snooping uplink-port eth-trunk TRUNK-NUMBER**配置组播监听上联口。

目的	步骤
配置组播复制用户VLAN	1. 进入全局配置视图； 2. 进入组播VLAN配置视图； 3. 执行命令**igmp-snooping multicast user-vlan VLAN-LIST**配置组播复制用户VLAN。
配置接口加入VLAN并在接口上使能IGMP Snooping协议	1. 进入全局配置视图； 2. 进入接口组配置视图（以太网接口、trunk接口）； 3. 执行命令**port hybrid vlan VLAN-LIST (tagged | untagged)**配置Hybrid类型接口所属VLAN； 4. 执行命令**igmp-snooping enable**配置在接口上使能组播监听。

6.1.4 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
全局使能IGMP Snooping	1. 进入全局配置视图； 2. 执行命令**igmp-snooping start**全局使能组播监听功能。
创建组播VLAN	1. 进入全局配置视图； 2. 执行命令**vlan VLAN-LIST**创建需要使能IGMP Snooping的VLAN； 3. 执行命令**igmp-snooping mvlan VLAN-ID**创建相应组播VLAN并进入组播VLAN配置视图。

目的	步骤
（可选）配置IGMP版本	1. 进入全局配置视图； 2. 进入组播VLAN配置视图； 3. 执行命令**igmp-snooping version (v1 | v2 | v3)**配置IGMP版本。
（可选）配置静态路由器接口	1. 进入全局配置视图； 2. 进入组播VLAN配置视图； 3. 执行命令**igmp-snooping uplink-port (ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 40gigaethernet) INTERFACE-NUMBER**配置静态路由器接口。
配置特定组查询的查询间隔	1. 进入全局配置视图； 2. 进入**IGMP Snooping MVLAN**配置视图； 3. 执行命令**igmp-snooping lastmember-queryinterval (QUERY-INTERVAL | default)**配置特定组查询的查询间隔。
配置特定查询的次数	1. 进入全局配置视图； 2. 进入**IGMP Snooping MVLAN**配置视图； 3. 执行命令**igmp-snooping lastmember-querynumber (QUERY-NUMBER | default)**配置特定查询的次数。
（可选）配置查询器	1. 进入全局配置视图； 2. 执行命令**igmp-snooping query-interval (QUERY-INTERVAL | default)**配置查询器发送查询报文间隔（各组播VLAN共用此参数）； 3. 执行命令**igmp-snooping robust-count (ROBUST-COUNT | default)**配置查询器的IGMP健壮系数（各组播VLAN共用此参数）； 4. 进入组播VLAN配置视图； 5. 执行命令**igmp-snooping querier (enable | disable)**配置IGMP snooping 查询器的使能状态； 6. 执行命令**igmp-snooping max-response-time (MAX-RESPONSE-TIME | default)**配置通用查询报文中最大响应时间字段值。
（可选）配置协议报文抑制	1. 进入全局配置视图； 2. 进入组播VLAN配置视图； 3. 执行命令**igmp-snooping report-suppress (enable | disable)**配置VLAN内报文抑制使能状态。
（可选）配置组播代理地址	1. 进入全局配置视图； 2. 进入组播VLAN配置视图； 3. 执行命令**igmp-snooping proxy-ip IP-ADDRESS**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。

目的	步骤
（可选）配置组播VLAN的Router-Alert检查功能	1. 进入全局配置视图； 2. 进入组播VLAN配置视图； 3. 执行命令**igmp-snooping require-router-alert (enable | disable)**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。
（可选）配置组播监听工作模式	1. 进入全局配置视图； 2. 进入组播VLAN配置视图； 3. 执行命令**igmp-snooping workmode (igmp-snooping | igmp-proxy)**配置组播监听工作模式为snooping模式或者proxy模式。
使能或去使能当stp环拓扑发生变化进行快速切换	1. 进入全局配置视图； 2. 进入组播VLAN配置视图； 3. 执行命令**igmp-snooping fast-switch (enable | disable)**。
使能或去使能当stp环拓扑发生变化进行快速切换时，发送通用查询功能	1. 进入全局配置视图； 2. 进入组播VLAN配置视图； 3. 执行命令**igmp-snooping fast-switch query (enable | disable)**。
使能或去使能禁止向接口发送IGMP查询报文	1. 进入全局配置视图； 2. 进入组播VLAN配置视图； 3. 执行命令**igmp-snooping proxy-uplink-port (enable | disable)**。
配置snooping 模式下的查询报文源IP 地址	1. 进入全局配置视图； 2. 进入组播VLAN配置视图； 3. 执行如下命令： ▶ **igmp-snooping send-query source-address SRC-ADDRESS** ▶ **igmp-snooping send-query source-address default**
使能或去使能禁止在上联口学习组播表项	1. 进入全局配置视图； 2. 进入组播VLAN配置视图； 3. 执行命令**igmp-snooping uplink-port drop-report (enable | disable)**。
配置上联口的数量限制	1. 进入全局配置视图； 2. 进入组播VLAN配置视图； 3. 执行命令**igmp-snooping 8021p priority (VALUE | default)**。

目的	步骤
（可选）配置接口快速离开	1. 进入全局配置视图； 2. 进入接口配置视图（以太网接口、trunk接口）、接口组配置视图； 3. 执行命令**igmp-snooping fast-leave (enable | disable)**配置接口快速离开功能。
配置接口上可控组播	1. 进入全局配置视图； 2. 进入接口配置视图（以太网接口、trunk接口）、接口组配置视图； 3. 执行命令**igmp-snooping ctrlmode (enable | disable)**配置使能或者去使能接口上可控组播。
配置全局路由器端口老化时间	1. 进入全局配置视图； 2. 执行命令**igmp-snooping router-aging-time (ROUTER-AGING-TIME | default)**配置全局路由器端口老化时间。
在组播复制使能时配置用户的静态VLAN	1. 进入全局配置视图； 2. 进入接口配置视图（以太网接口、trunk接口）、接口组配置视图； 3. 执行命令**igmp-snooping static-group group-address GROUP-ADDRESS mvlan VLAN-ID user-vlan VLAN-LIST**在组播复制使能时配置用户的静态VLAN。
删除静态组播中的指定用户VLAN或所有用户VLAN	1. 进入全局配置视图； 2. 进入接口配置视图（以太网接口、trunk接口）、接口组配置视图； 3. 执行如下命令删除静态组播中的指定用户VLAN或所有用户VLAN： ▶ **no igmp-snooping static-group** ▶ **no igmp-snooping static-group group-address GROUP-ADDRESS mvlan VLAN-ID user-vlan VLAN-LIST** ▶ **no igmp-snooping static-group group-address GROUP-ADDRESS mvlan VLAN-ID user-vlan all** ▶ **no igmp-snooping static-group mvlan VLAN-ID**
创建组播VLAN的上行接口	1. 进入全局配置视图； 2. 进入接口配置视图（以太网接口、trunk接口）、接口组配置视图； 3. 执行命令**no igmp-snooping mvlan VLAN-ID uplink-port**创建组播VLAN的上行接口。

目的	步骤
删除组播VLAN的上行接口	1. 进入全局配置视图； 2. 进入接口配置视图（以太网接口、trunk接口）、接口组配置视图； 3. 执行命令**no igmp-snooping mvlan VLAN-ID uplink-port**删除组播VLAN的上行接口。
使能或去使能Query报文复制抑制功能	1. 进入全局配置视图； 2. 进入Trunk接口配置视图、以太网桥接接口配置视图、以太网路由接口配置视图； 3. 执行命令**igmp-snooping query-duplicate-suppress (enable | disable)**。

6.1.5 维护及调试

目的

当IGMP Snooping功能不正常，需要进行查看、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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
查看IGMP Snooping配置文件信息	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）、IGMP Snooping MVLAN配置视图、接口组配置视图； 2. 执行命令**show igmp-snooping config**显示IGMP Snooping配置文件信息。
查看IGMP Snooping接口配置文件信息	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）、IGMP Snooping MVLAN配置视图、接口组配置视图； 2. 执行命令**show igmp-snooping interface**显示IGMP-snooping配置模式下组播接口的配置信息。
查看IGMP-snooping配置模式下组播VLAN的配置信息	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）、IGMP Snooping MVLAN配置视图、接口组配置视图； 2. 执行命令**show igmp-snooping mvlan**显示IGMP-snooping配置模式下组播VLAN的配置信息。

目的	步骤
查看IGMP-snooping配置模式下组播上联口的配置信息	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）、IGMP Snooping MVLAN配置视图、接口组配置视图； 2. 执行命令**show igmp-snooping uplinkport**显示IGMP-snooping配置模式下组播上联口的配置信息。
查看IGMP Snooping全部、指定接口或指定VLAN出端口表项信息	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）、IGMP Snooping MVLAN配置视图、接口组配置视图； 2. 执行如下命令显示IGMP Snooping出端口表项信息： ▶ **show igmp-snooping egress-port** ▶ **show igmp-snooping egress-port mvlan MVLAN-ID** ▶ **show igmp-snooping egress-port interface (ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 40gigaethernet) INTERFACE-NUMBER** ▶ **show igmp-snooping egress-port interface eth-trunk TRUNK-NUMBER**
查看IGMP Snooping组播组表项信息	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）、IGMP Snooping MVLAN配置视图、接口组配置视图； 2. 执行命令**show igmp-snooping group**显示IGMP Snooping组播组表项信息。
查看IGMP Snooping组播源表项信息（version 3时有效	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）、IGMP Snooping MVLAN配置视图、接口组配置视图； 2. 执行命令**show igmp-snooping source-address**显示IGMP Snooping组播组表项信息。
清除igmp-snooping动态的组播组表信息	1. 进入全局配置视图、接口配置视图（以太网、trunk）、IGMP Snooping MVLAN配置视图、接口组配置视图； 2. 执行命令**reset igmp-snooping group**清除动态的组播组表（group、egress-port等）。
显示和查看全局配置信息	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）、IGMP Snooping MVLAN配置视图、接口组配置视图； 2. 执行命令**show igmp-snooping**显示和查看全局配置信息。

目的	步骤
显示和查看IGMP snooping统计信息	1. 进入全局配置视图、接口配置视图（以太网、trunk）、IGMP Snooping MVLAN配置视图、接口组配置视图； 2. 执行如下命令： ▶ **show igmp-snooping statistic** ▶ **show igmp-snooping statistic interface** ▶ **show igmp-snooping statistic interface (ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 40gigaethernet) INTERFACE-NUMBER** ▶ **show igmp-snooping statistic interface eth-trunk TRUNK-NUMBER**
清空IGMP snooping统计信息	1. 进入全局配置视图、接口配置视图（以太网、trunk）、IGMP Snooping MVLAN配置视图、接口组配置视图； 2. 执行命令**reset igmp-snooping statistic**。

6.1.6 配置举例

6.1.6.1 配置静态二层组播举例

组网要求

交换机接口 10GE1/0/1连接组播源测路由器，接口10GE1/0/2连接用户主机，要求通过配置静态二层组播功能实现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，如图 6-1所示。

组网图

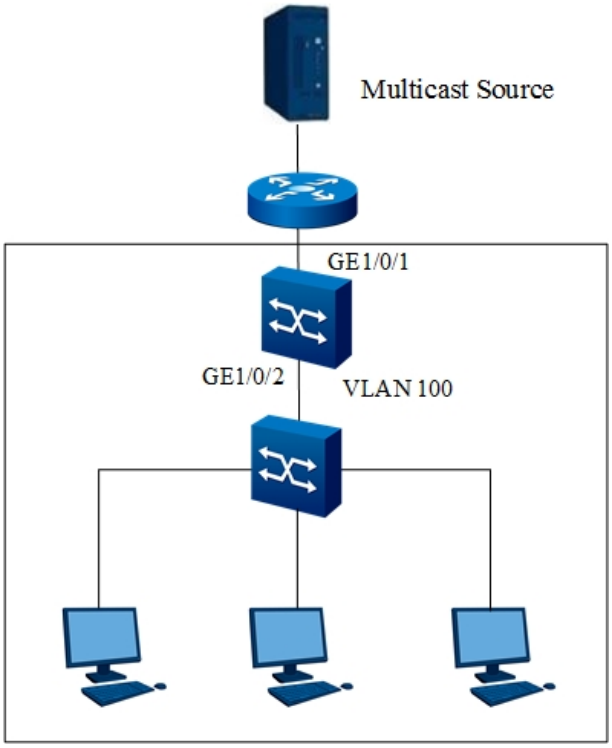


图 6-1 静态二层组播组网图

配置步骤

1. 全局使能IGMP snooping协议。

```
SC9600E#configure
SC9600E(config)#igmp-snooping start
SC9600E(config)#
```

2. 创建VLAN和相应的组播VLAN，配置接口加入VLAN。

```
SC9600E(config)#vlan 100
SC9600E(vlan-100)#quit
SC9600E(config)#interface 10gigaethernet 1/0/1
SC9600E(config-10ge1/0/1)#port hybrid vlan 100 tagged
SC9600E(config-10ge1/0/1)#quit
SC9600E(config)#interface 10gigaethernet 1/0/2
SC9600E(config-10ge1/0/2)#port hybrid vlan 100 tagged
SC9600E(config-10ge1/0/2)#quit
SC9600E(config)# igmp-snooping mvlan 100
SC9600E(config-igmpsnoop-mvlan100)#quit
SC9600E(config)#
```

3. 在接口下使能IGMP Snooping协议。

```
SC9600E(config)#interface 10gigaethernet 1/0/1
SC9600E(config-10ge1/0/1)#igmp-snooping enable
SC9600E(config-10ge1/0/1)#quit
SC9600E(config)#interface 10gigaethernet 1/0/2
SC9600E(config-10ge1/0/2)#igmp-snooping enable
SC9600E(config-10ge1/0/2)#quit
SC9600E(config)#
```

4. 配置GE1/0/1为静态路由器接口。

```
SC9600E(config)#igmp-snooping mvlan 100
SC9600E(config-igmpsnoop-mvlan100)#igmp-snooping uplink-port gigaethernet 1/0/1
SC9600E(config-igmpsnoop-mvlan100)#quit
SC9600E(config)#
```

5. 配置静态组播组。

```
SC9600E(config)#interface 10gigaethernet 1/0/2
SC9600E(config-10ge1/0/2)#igmp-snooping static-group group-address 225.1.1.1
mvlan 100
SC9600E(config-10ge1/0/2)#quit
SC9600E(config)#
```

6. 配置结束，检查组播组表和出端口表信息。

```
SC9600E#show igmp-snooping group
  Total Entry(s) : 1
  Group Address   MVlan  Pre-join  MemNum  V3FilterMode
  225.1.1.1       100    disable   1       invalid

SC9600E#show igmp-snooping egress-port
Total Entry(s) : 1

Group Address : 225.1.1.1
MVlan : 100
Source Address : *
Interface : xge-1/0/2
   Type : static
   Expires : ---
   OutVlan :    100
   V3 Mode : invalid
```

6.1.6.2 配置IGMP Snooping举例

组网要求

交换机接口10GE1/0/1连接组播源测路由器，接口10GE1/0/2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，如图 6-2所示。

组网图

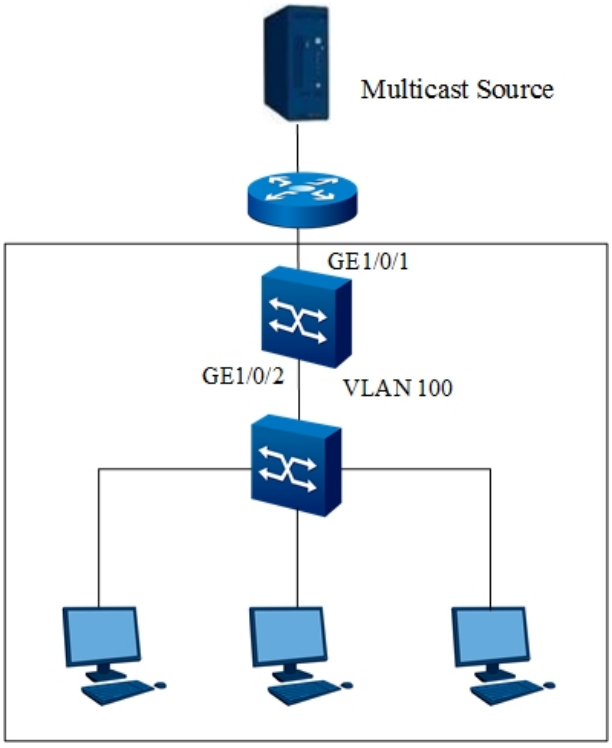


图 6-2 igmp-snooping配置组网图

配置步骤

1. 全局使能IGMP snooping协议。

```
SC9600E#configure
SC9600E(config)#igmp-snooping start
SC9600E(config)#
```

2. 创建VLAN和相应的组播VLAN，配置接口加入VLAN。

```
SC9600E(config)#vlan 100
SC9600E(vlan-100)#quit
SC9600E(config)#interface 10gigaethernet 1/0/1
SC9600E(config-10ge1/0/1)#port hybrid vlan 100 tagged
```

```
SC9600E(config-10ge1/0/1)#quit
SC9600E(config)#interface 10gigaethernet 1/0/2
SC9600E(config-10ge1/0/2)#port hybrid vlan 100 tagged
SC9600E(config-10ge1/0/2)#quit
SC9600E(config)# igmp-snooping mvlan 100
SC9600E(config-igmpsnoop-mvlan100)#quit
SC9600E(config)#
```

3. 在接口下使能IGMP Snooping协议。

```
SC9600E(config)#interface 10gigaethernet 1/0/1
SC9600E(config-10ge1/0/1)#igmp-snooping enable
SC9600E(config-10ge1/0/1)#quit
SC9600E(config)#interface 10gigaethernet 1/0/2
SC9600E(config-10ge1/0/2)#igmp-snooping enable
SC9600E(config-10ge1/0/2)#quit
SC9600E(config)#
```

4. 配置GE1/0/1为静态路由器接口。

```
SC9600E(config)#igmp-snooping mvlan 100
SC9600E(config-igmpsnoop-mvlan100)#igmp-snooping uplink-port gigaethernet 1/0/1
SC9600E(config-igmpsnoop-mvlan100)#quit
SC9600E(config)#
```

5. 配置静态组播组。

```
SC9600E(config)#interface 10gigaethernet 1/0/2
SC9600E(config-10ge1/0/2)#igmp-snooping static-group group-address
225.1.1.1 mvlan 100
SC9600E(config-10ge1/0/2)#igmp-snooping static-group group-address
225.1.1.2 mvlan 100
SC9600E(config-10ge1/0/2)#quit
SC9600E(config)#
```

6. 配置结束，检查组播组表和出端口表信息。

```
SC9600E#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

SC9600E#show igmp-snooping egress-port
Total Entry(s) : 2

Group Address : 225.1.1.1
MVlan : 100
Source Address : *
```

```
Interface : xge-1/0/2
   Type : static
   Expires : ---
   OutVlan :    100
   V3 Mode : invalid
Group Address : 225.1.1.2
MVlan : 100
Source Address : *
Interface : xge-1/0/2
   Type : static
   Expires : ---
   OutVlan :    100
   V3 Mode : invalid
```

6.1.6.3 配置组播VLAN复制举例

组网要求

交换机接口 10GE1/0/1连接组播源测路由器属于VLAN 100，接口10GE1/0/2和10GE10/3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，VLAN2和VLAN3 为用户VLAN，如图 6-3所示。

组网图

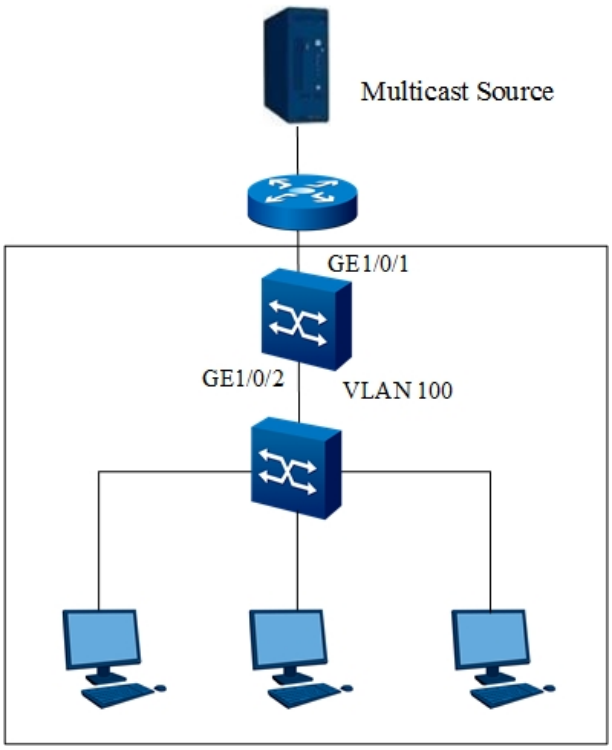


图 6-3　组播复制拓扑图

配置步骤

1. 全局使能IGMP snooping协议。

```
SC9600E#configure
SC9600E(config)#igmp-snooping start
SC9600E(config)#
```

2. 创建VLAN和相应的组播VLAN，配置接口加入VLAN。

```
SC9600E(config)#vlan 2,3,100
SC9600E(config)#interface 10gigaethernet 1/0/1
SC9600E(config-10ge1/0/1)#port hybrid vlan 100 tagged
SC9600E(config-10ge1/0/1)#quit
SC9600E(config)#interface 10gigaethernet 1/0/2
SC9600E(config-10ge1/0/2)#port hybrid vlan 2 tagged
SC9600E(config-10ge1/0/2)#quit
SC9600E(config)#interface 10gigaethernet 1/0/3
SC9600E(config-10ge1/0/3)#port hybrid vlan 3 tagged
SC9600E(config-10ge1/0/3)#quit
SC9600E(config)#igmp-snooping mvlan 100
SC9600E(config-igmpsnoop-mvlan100)#quit
SC9600E(config)#
```

3. 在接口下使能IGMP Snooping协议。

```
SC9600E(config)#interface 10gigaethernet 1/0/1
SC9600E(config-10ge1/0/1)#igmp-snooping enable
SC9600E(config-10ge1/0/1)#quit
SC9600E(config)#interface 10gigaethernet 1/0/2
SC9600E(config-10ge1/0/2)#igmp-snooping enable
SC9600E(config-10ge1/0/2)#quit
SC9600E(config)#interface 10gigaethernet 1/0/3
SC9600E(config-10ge1/0/3)#igmp-snooping enable
SC9600E(config-10ge1/0/3)#quit
SC9600E(config)#
```

4. 在组播VLAN下使能组播复制功能，并配置用户VLAN。

```
SC9600E(config)#igmp-snooping mvlan 100
SC9600E(config-igmpsnoop-mvlan100)#igmp-snooping multicast-vlan enable
SC9600E(config-igmpsnoop-mvlan100)#igmp-snooping multicast user-vlan 2,3
SC9600E(config-igmpsnoop-mvlan100)#quit
SC9600E(config)#
```

5. 配置10GE1/0/1为静态路由器接口。

```
SC9600E(config)#igmp-snooping mvlan 100
SC9600E(config-igmpsnoop-mvlan100)#igmp-snooping uplink-port xgigaethernet 1/0/1
SC9600E(config-igmpsnoop-mvlan100)#quit
SC9600E(config)#
```

6. 配置静态组播组。

```
SC9600E(config)#interface 10gigaethernet 1/0/2
SC9600E(config-10ge1/0/2)#igmp-snooping static-group group-address
225.0.0.1 mvlan 100 user-vlan 2
SC9600E(config-10ge1/0/2)#igmp-snooping static-group group-address
225.0.0.2 mvlan 100 user-vlan 2
SC9600E(config-10ge1/0/2)#igmp-snooping static-group group-address
225.0.0.3 mvlan 100 user-vlan 2
SC9600E(config-10ge1/0/2)#quit
SC9600E(config)#interface 10gigaethernet 1/0/3
SC9600E(config-10ge1/0/3)#igmp-snooping static-group group-address
225.0.0.1 mvlan 100 user-vlan 3
SC9600E(config-10ge1/0/3)#igmp-snooping static-group group-address
225.0.0.2 mvlan 100 user-vlan 3
SC9600E(config-10ge1/0/3)#igmp-snooping static-group group-address
225.0.0.3 mvlan 100 user-vlan 3
SC9600E(config-10ge1/0/3)#quit
```

7. 配置完成，检查组播组表和出端口表信息。

```
SC9600E#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

SC9600E#show igmp-snooping egress-port
Total Entry(s) : 6

Group Address : 225.0.0.1
MVlan : 100
Source Address : *
Interface : xge-1/0/2
   Type : static
   Expires : ---
   OutVlan :    2
   V3 Mode : invalid
Group Address : 225.0.0.1
MVlan : 100
Source Address : *
Interface : xge-1/0/3
   Type : static
   Expires : ---
   OutVlan :    3
   V3 Mode : invalid
Group Address : 225.0.0.2
MVlan : 100
Source Address : *
Interface : xge-1/0/2
   Type : static
   Expires : ---
   OutVlan :    2
   V3 Mode : invalid
Group Address : 225.0.0.2
MVlan : 100
Source Address : *
Interface : xge-1/0/3
   Type : static
   Expires : ---
   OutVlan :    3
   V3 Mode : invalid
Group Address : 225.0.0.3
MVlan : 100
Source Address : *
```

```
Interface : xge-1/0/2
   Type : static
   Expires : ---
   OutVlan :    2
   V3 Mode : invalid
Group Address : 225.0.0.3
MVlan : 100
Source Address : *
Interface : xge-1/0/3
   Type : static
   Expires : ---
   OutVlan :    3
   V3 Mode : invalid
```

7 安全配置

本章介绍了SC9600E系列数据中心交换机安全性相关的基本内容、配置过程和配置举例。

7.1 ACL 配置

提示：

本小节中，ACL规格实际情况根据各产品特性参数表为准。

7.1.1 ACL 概述

ACL功能

SC9600E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SC9600E上，SC9600E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。

SC9600E支持的ACL分类

SC9600E支持二层ACL入方向，三层ACl入方向，混合ACL。

- 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。

7.1.2 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
创建一条二层ACL	1. 进入全局配置视图； 2. 执行命令**filter-list ACL-NUMBER [name FILTER-NAME]**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。

目的	步骤
配置二层ACL规则	1. 进入全局配置视图； 2. 进入二层ACL配置视图； 3. 执行如下命令用来配置MAC条目匹配的ACL规则： ▶ **filter RULE-NUMBER mac (SRC-MAC-ADDRESS/M | any) (DST-MAC-ADDRESS/M | any)** ▶ **filter RULE-NUMBER mac (SRC-MAC-ADDRESS/M | any) (DST-MAC-ADDRESS/M | any) (customer | provider) (any | VLAN-ID | VLAN-ID1/VLAN-ID2) (any | PRIORITY)** ▶ **filter RULE-NUMBER src-mac SRC-MAC-ADDRESS src-mask SRC-MAC-MASK dst-mac DST-MAC-ADDRESS dst-mask DST-MAC-MASK (customer | provider) (any | VLAN-ID | VLAN-ID1/VLAN-ID2) (any | PRIORITY)** ▶ **filter RULE-NUMBER mac (SRC-MAC-ADDRESS/M | any) (DST-MAC-ADDRESS/M | any) eth-type (ip | arp | DIGITIAL-PROTOCOL-VALUE)** ▶ **filter RULE-NUMBER mac (SRC-MAC-ADDRESS/M | any) (DST-MAC-ADDRESS/M | any) provider (any | VLAN-ID) (any | PRIORITY) customer (any | VLAN-ID) (any | PRIORITY)** ▶ **filter RULE-NUMBER mac (SRC-MAC-ADDRESS/M | any) (DST-MAC-ADDRESS/M | any) provider (VLAN-ID1/VLAN-ID2) (any | PRIORITY) customer (any | VLAN-ID) (any | PRIORITY)** ▶ **filter RULE-NUMBER mac (SRC-MAC-ADDRESS/M | any) (DST-MAC-ADDRESS/M | any) provider (any | VLAN-ID) (any | PRIORITY) customer (VLAN-ID1/VLAN-ID2) (any | PRIORITY)** ▶ **filter RULE-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 | VLAN-ID) (any | PRIORITY) customer (any | VLAN-ID) (any | PRIORITY)** ▶ **filter RULE-NUMBER src-mac (SRC-MAC-ADDRESS/M | any) src-mask SRC-MAC-MASK dst-mac DST-MAC-ADDRESS dst-mask DST-MAC-MASK provider (VLAN-ID1/VLAN-ID2) (any | PRIORITY) customer (any | VLAN-ID) (any | PRIORITY)** ▶ **filter RULE-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 | VLAN-ID) (any | PRIORITY) customer (VLAN-ID1/VLAN-ID2) (any | PRIORITY)**

目的	步骤
配置二层ACL动作	1. 进入全局配置视图； 2. 进入二层ACL配置视图； 3. 执行如下命令配置ACL处理动作： ▶ **filter RULE-NUMBER action (permit | deny)** ▶ **filter RULE-NUMBER action redirect cpu** ▶ **filter RULE-NUMBER action cpu** ▶ **filter RULE-NUMBER action mirror group GROUP-NUMBER** ▶ **filter RULE-NUMBER action (cos | precedence | priority) PRIORITY-VALUE** ▶ **filter RULE-NUMBER action dscp DSCP**
删除ACL动作	1. 进入全局配置视图； 2. 进入ACL配置视图； 3. 执行命令**no filter RULE-NUMBER action**用来删除ACL规则对应的处理动作。
删除ACL规则	1. 进入全局配置视图； 2. 进入ACL配置视图； 3. 执行命令**no filter RULE-NUMBER**用来删除ACL规则。
删除ACL访问控制列表	1. 进入全局配置视图； 2. 进入ACL配置视图； 3. 执行命令**no filter-list ACL-NUMBER**用来删除ACL访问控制列表。
绑定二层ACL	1. 进入全局配置视图； 2. 进入以太网接口配置视图或二层ACL配置视图，执行以下命令用来将ACL应用到物理端口，trunk接口或者VLAN端口。 ▶ **filter-list-l2 (in | out) ACL-NUMBER** ▶ **filter-list-l2 (in | out) name ACL-NAME** 或 1. 进入全局配置视图； 2. 执行命令**filter-list-l2 global (in | out) ACL-NUMBER**全局绑定ACL。

7.1.3 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
创建一条三层ACL	1. 进入全局配置视图； 2. 执行命令**filter-list ACL-NUMBER [name FILTER-NAME]**使用编号创建一条三层ACL（访问控制列表），并进入三层ACL配置视图。
配置三层ACL规则（1）	1. 进入全局配置视图； 2. 进入三层ACL配置视图； 【用户可以从步骤3~步骤6中根据需要任选配置】 3. （可选）执行如下命令用来配置IP匹配的ACL规则； ▶ **filter RULE-NUMBER ip (SRC-IP-ADDRESS/M | any) (DST-IP-ADDRESS/M | any) [tos TOS-VALUE | ttl TTL-VALUE | proto-type PROTO-TYPE-VALUE]** ▶ **filter RULE-NUMBER ip (SRC-IP-ADDRESS/M | any) (DST-IP-ADDRESS/M | any) precedence IP-PRECEDENCE [fragment]** ▶ **filter RULE-NUMBER src-ip (SRC-IP-ADDRESS | any) src-mask (SRC-IP-MASK | any) dst-ip (DST-IP-ADDRESS | any) dst-mask (DST-IP-MASK | any) precedence IP-PRECEDENCE [fragment]** ▶ **filter RULE-NUMBER ip (SRC-IP-ADDRESS/M | any) (DST-IP-ADDRESS/M | any) dscp DSCP [fragment]** ▶ **filter RULE-NUMBER src-ip (SRC-IP-ADDRESS | any) src-mask (SRC-IP-MASK | any) dst-ip (DST-IP-ADDRESS | any) dst-mask (DST-IP-MASK | any) dscp DSCP [fragment]** ▶ **filter RULE-NUMBER src-ip (SRC-IP-ADDRESS | any) src-mask (SRC-IP-MASK | any) dst-ip (DST-IP-ADDRESS | any) dst-mask (DST-IP-MASK | any) [ttl TTL-VALUE | proto-type PROTO-TYPE-VALUE]**

目的	步骤
配置三层ACL规则（2）	1. （可选）执行如下命令用来配置TCP匹配的ACL规则； ▶ **filter RULE-NUMBER tcp (SRC-IP-ADDRESS/M | any) (SRC-PORT-NUMBER | any | SOURCE-PORT-NUMBER-RANGE) (DST-IP-ADDRESS/M | any) (DST-PORT-NUMBER | any | DESTINATION-PORT-NUMBER-RANGE) [fragment]** ▶ **filter RULE-NUMBER tcp (SRC-IP-ADDRESS/M | any) (SRC-PORT-NUMBER | any | SOURCE-PORT-NUMBER-RANGE) (DST-IP-ADDRESS/M | any) (DST-PORT-NUMBER | any | DESTINATION-PORT-NUMBER-RANGE) (syn | synack | ack | fin) [fragment]** ▶ **filter RULE-NUMBER tcp src-ip (SRC-IP-ADDRESS | any) src-mask (SRC-IP-MASK | any) (SRC-PORT-NUMBER | SOURCE-PORT-NUMBER-RANGE/DESTINATION-PORT-NUMBER-RANGE | any) dst-ip (SRC-IP-MASK | any) dst-mask (DST-IP-MASK | any) (DST-PORT-NUMBER | any | SOURCE-PORT-NUMBER-RANGE/DESTINATION-PORT-NUMBER-RANGE) [fragment]** ▶ **filter RULE-NUMBER tcp src-ip (SRC-IP-ADDRESS | any) src-mask (SRC-IP-MASK | any) (SRC-PORT-NUMBER | SOURCE-PORT-NUMBER-RANGE/DESTINATION-PORT-NUMBER-RANGE | any) dst-ip (SRC-IP-MASK | any) dst-mask (DST-IP-MASK | any) (DST-PORT-NUMBER | any | SOURCE-PORT-NUMBER-RANGE/DESTINATION-PORT-NUMBER-RANGE) (syn | synack | ack | fin) [fragment]** 2. （可选）执行如下命令用来配置ICMP匹配的ACL规则； ▶ **filter RULE-NUMBER icmp (SRC-IP-ADDRESS/M | any) (DST-IP-ADDRESS/M | any)** ▶ **filter RULE-NUMBER icmp src-ip (SRC-IP-ADDRESS/M | any) src-mask (SRC-IP-MASK | any) dst-ip (SRC-IP-MASK | any) dst-mask (DST-IP-MASK | any)** ▶ **filter RULE-NUMBER icmp (SRC-IP-ADDRESS/M | any) (DST-IP-ADDRESS/M | any) (ICMP TYPE | any) (ICMP CODE | any) [fragment]**
配置三层ACL规则（3）	1. （可选）执行如下命令用来配置UDP匹配的ACL规则。 ▶ **filter RULE-NUMBER udp (SRC-IP-ADDRESS/M | any) (SRC-PORT-NUMBER | any | SOURCE-PORT-NUMBER-RANGE) (DST-IP-ADDRESS/M | any) (DST-PORT-NUMBER | any | DESTINATION-PORT-NUMBER-RANGE) [fragment]**

目的	步骤
配置三层ACL动作	1. 进入全局配置视图； 2. 进入三层ACL配置视图； 3. 执行如下命令配置ACL处理动作： ▶ **filter RULE-NUMBER action (permit | deny)** ▶ **filter RULE-NUMBER action redirect cpu** ▶ **filter RULE-NUMBER action cpu** ▶ **filter RULE-NUMBER action mirror group GROUP-NUMBER** ▶ **filter RULE-NUMBER action redirect (ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 40gigaethernet) INTERFACE-NUMBER** ▶ **filter RULE-NUMBER action redirect eth-trunk TRUNK-NUMBER** ▶ **filter RULE-NUMBER action (cos | precedence | priority) PRIORITY-VALUE** ▶ **filter RULE-NUMBER action dscp DSCP** ▶ **filter RULE-NUMBER action counter COUNTER-NUMBER** ▶ **filter RULE-NUMBER action tos TOS-NUMBER**
绑定三层ACL	1. 进入全局配置视图； 2. 进入以太网接口配置视图，执行以下命令用来将ACL应用到物理端口，trunk接口或者VLAN端口。 ▶ **filter-list-ipv4 (in | out) ACL-NUMBER** ▶ **filter-list-ipv4 (in | out) name ACL-NAME** 或 1. 进入全局配置视图； 2. 执行命令**filter-list-ipv4 global (in | out) ACL-NUMBER**全局绑定ACL。

7.1.4 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
创建一条混合ACL	1. 进入全局配置视图； 2. 执行命令**filter-list ACL-NUMBER [name FILTER-NAME]**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。
配置混合ACL规则	1. 进入全局配置视图； 2. 进入混合ACL配置视图； 3. 混合模式可以配置二层和三层的ACL规则，请参考本手册7.1.2和7.1.3小节ACL规则的配置命令。

目的	步骤
配置混合ACL动作	1. 进入全局配置视图； 2. 进入混合ACL配置视图； 3. 执行如下命令配置ACL处理动作： ▶ **filter RULE-NUMBER action (permit | deny)** ▶ **filter RULE-NUMBER action redirect cpu** ▶ **filter RULE-NUMBER action cpu** ▶ **filter RULE-NUMBER action mirror group GROUP-NUMBER** ▶ **filter RULE-NUMBER action redirect (ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 40gigaethernet) INTERFACE-NUMBER** ▶ **filter RULE-NUMBER action (cos | precedence | priority) PRIORITY-VALUE** ▶ **filter RULE-NUMBER action dscp DSCP** ▶ **filter RULE-NUMBER action counter COUNTER-NUMBER** ▶ **filter RULE-NUMBER action tos TOS-NUMBER**
绑定混合ACL	1. 进入全局配置视图； 2. 进入以太网接口配置视图，执行以下命令用来将ACL应用到物理端口，trunk接口或者VLAN端口。 ▶ **filter-list-hybrid (in | out) ACL-NUMBER** ▶ **filter-list-hybrid (in | out) name ACL-NAME** 或 1. 进入全局配置视图； 2. 执行命令**filter-list-hybrid global (in | out) ACL-NUMBER**全局绑定ACL。

7.1.5 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
创建一条三层ACL6	1. 进入全局配置视图； 2. 执行命令**filter-list ACL-NUMBER [name FILTER-NAME]**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。
配置三层ACL6规则	1. 进入全局配置视图； 2. 进入三层ACL6配置视图； 【用户可以从步骤3~步骤6中根据需要任选配置】 3. （可选）执行如下命令用来配置IP6匹配的ACL规则； ▶ **filter RULE-NUMBER ip6 (SRC-IP6-ADDRESS/M | any) (DST-IP6-ADDRESS/M | any)** ▶ **filter RULE-NUMBER ip6 (SRC-IP6-ADDRESS/M | any) (DST-IP6-ADDRESS/M | any) next-header NEXT-HEADER-VALUE** ▶ **filter RULE-NUMBER ip6 (SRC-IP6-ADDRESS/M | any) (DST-IP6-ADDRESS/M | any) hop-limit HOP-LIMIT-VALUE** 4. （可选）执行如下命令用来配置TCP6匹配的ACL规则； ▶ **filter RULE-NUMBER tcp6 (SRC-IP6-ADDRESS/M | any) (SRC-PORT-NUMBER | any | SRC-PORT-RANGE) (DST-IP6-ADDRESS/M | any) (DST-PORT-NUMBER | any | DST-PORT-RANGE) [fragment]** ▶ **filter RULE-NUMBER tcp6 (SRC-IP6-ADDRESS/M | any) (SRC-PORT-NUMBER | any | SRC-PORT-RANGE) (DST-IP6-ADDRESS/M | any) (DST-PORT-NUMBER | any | DST-PORT-RANGE) (syn | synack | ack | fin) [fragment]** 5. （可选）执行如下命令用来配置ICMP6匹配的ACL规则； ▶ **filter RULE-NUMBER icmp6 (SRC-IP6-ADDRESS/M | any) (DST-IP6-ADDRESS/M | any)** ▶ **filter RULE-NUMBER icmp6 (SRC-IP6-ADDRESS/M | any) (DST-IP6-ADDRESS/M | any) (ICMP-TYPE | any) (ICMP-CODE | any) [fragment]** 6. （可选）执行如下命令用来配置UDP6匹配的ACL规则。 ▶ **filter RULE-NUMBER udp6 (SRC-IP6-ADDRESS/M | any) (SRC-PORT-NUMBER | any | SRC-PORT-RANGE) (DST-IP6-ADDRESS/M | any) (DST-PORT-NUMBER | any | DST-PORT-RANGE) [fragment]**

目的	步骤
配置三层ACL6动作	1. 进入全局配置视图； 2. 进入三层ACL6配置视图； 3. 执行如下命令配置ACL处理动作： ▶ **filter RULE-NUMBER action redirect cpu** ▶ **filter RULE-NUMBER action cpu** ▶ **filter RULE-NUMBER action mirror group GROUP-NUMBER** ▶ **filter RULE-NUMBER action redirect (ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 40gigaethernet) INTERFACE-NUMBER** ▶ **filter RULE-NUMBER action redirect eth-trunk TRUNK-NUMBER** ▶ **filter RULE-NUMBER action dscp DSCP** ▶ **filter RULE-NUMBER action counter COUNTER-NUMBER** ▶ **filter RULE-NUMBER action tos TOS-NUMBER**
绑定三层ACL6	1. 进入全局配置视图； 2. 进入以太网接口配置视图，执行以下命令用来将ACL应用到物理端口，trunk接口或者VLAN端口。 ▶ **filter-list-ipv6 (in | out) ACL-NUMBER** ▶ **filter-list-ipv6 (in | out) name ACL-NAME** 或 1. 进入全局配置视图； 2. 执行命令**filter-list-ipv6 global (in | out) ACL-NUMBER**全局绑定ACL。

7.1.6 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
创建ACL生效时间段	1. 进入全局配置视图； 2. 执行命令**time-range list LIST-NUMBER**用来进入某条time-range配置视图； 3. 执行如下命令配置time-range模块起始结束的绝对时间： ▶ **time-range RANGE-NUMBER absolute from HH:MM:SS YY/MM/DD** ▶ **time-range RANGE-NUMBER absolute from HH:MM:SS YY/MM/DD to HH:MM:SS YY/MM/DD** 4. 执行命令**time-range RANGE-NUMBER everyday HH:MM:SS to HH:MM:SS**用来配置time-range模块每日时间范围； 5. 执行命令**time-range RANGE-NUMBER everyhour MM:SS to MM:SS**用来配置time-range模块每小时时间范围； 6. 执行命令**time-range RANGE-NUMBER everymonth HH:MM:SS MM to HH:MM:SS MM**用来配置time-range模块每月时间范围； 7. 执行命令**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)**用来配置time-range模块每周时间范围； 8. 执行命令**time-range RANGE-NUMBER everyweekday HH:MM:SS to HH:MM:SS**用来配置time-range模块每周除周末以外的时间范围； 9. 执行命令**time-range RANGE-NUMBER everyweekend HH:MM:SS to HH:MM:SS**用来配置time-range模块每周末的时间范围； 10. 执行命令**time-range RANGE-NUMBER everyyear HH:MM:SS MM/DD to HH:MM:SS MM/DD**用来配置time-range模块每年的时间范围； 11. 执行命令**quit**退出到全局配置视图； 12. 进入ACL配置视图； 13. 执行命令**time-range list LIST-NUMBER**用来将时间段模板与ACL绑定。

目的	步骤
创建ACL限速模板	1. 进入全局配置视图； 2. 执行如下命令配置Meter模板： ▶ **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)** 3. 进入ACL配置视图； 4. 执行命令**filter RULE-NUMBER meter METER-NUMBER**用来配置ACL规则和某个meter模板绑定； 5. 执行命令**filter RULE-NUMBER car CAR-VALUE outaction drop**配置根据限速模板着色后包的处理。
创建ACL计数模板	1. 进入全局配置视图； 2. 执行命令**counter COUNTER-NUMBER (packet | byte | all) sort (green | red | greenred | greenyellow | redyellow | total)**用来配置Counter模板； 3. 进入ACL配置视图； 4. 执行命令**filter RULE-NUMBER action counter COUNTER-NUMBER**用来配置计数模板与ACL绑定。

7.1.7 查看及调试

目的

实现对ACL功能的查看、统计或修改。ACL统计用来配合设备进行端口统计监控，可以用于调试设备流量问题或其他模块问题。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
清除ACL的统计信息	1. 进入全局配置视图； 2. 执行如下命令重置ACL（访问控制列表）的过滤器条目计数： ▶ **reset counter filte-list ACL-NUMBER filter RULE-NUMBER [slot SLOT-ID] (in | out)** ▶ **reset counter filte-list ACL-NUMBER filter RULE-NUMBER port (ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 40gigaethernet) INTERFACE-NUMBER (in | out)** ▶ **reset counter filte-list ACL-NUMBER filter RULE-NUMBER port eth-trunk TRUNK-NUMBER (in | out)** ▶ **reset counter filte-list ACL-NUMBER filter RULE-NUMBER vlan VLAN-ID (in | out)**
查看访问控制列表的配置信息	1. 进入普通用户视图、特权用户视图、全局配置视图、filter配置视图、接口配置视图（以太网接口、trunk接口）、VLANIF配置视图、接口组配置视图或批量接口配置视图； 2. 执行如下命令显示访问控制列表的配置信息： ▶ **show filter-list** ▶ **show filter-list ACL-NUMBER**
查看访问控制列表配置文件信息	1. 进入普通用户视图、特权用户视图、全局配置视图、filter配置视图、接口配置视图（以太网接口、trunk接口）、VLANIF配置视图、接口组配置视图或批量接口配置视图； 2. 执行命令**show filter-list config**显示ACL配置文件信息。
查看所有应用了访问控制列表的端口信息	1. 进入普通用户视图、特权用户视图、全局配置视图、filter配置视图、接口配置视图（以太网接口、trunk接口）、VLANIF配置视图、接口组配置视图或批量接口配置视图； 2. 执行命令**show filter-list interface**显示所有应用了访问控制列表的端口信息。
查看统计表信息、配置信息	1. 进入特权用户视图、全局配置视图、普通用户视图、接口组配置视图或批量接口配置视图； 2. 执行如下命令显示统计表信息、配置信息： ▶ **show counter config** ▶ **show counter COUNTER-ID** ▶ **show counter**

7.1.8 配置举例

7.1.8.1 配置二层ACL示例

组网要求

SC9600E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，如图 7-1所示。

组网图

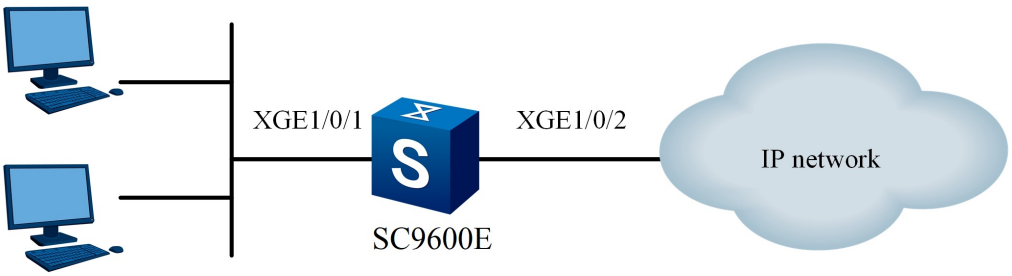


图 7-1 二层ACL示例图

配置步骤

1. 创建二层ACL。

```
SC9600E#configure
SC9600E(config)#filter-list 1
SC9600E(configure-filter-l2-1)#
```

2. 配置二层ACL规则。

```
SC9600E(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。

```
SC9600E(configure-filter-l2-1)#filter 1 action deny
```

4. 端口绑定ACL。

```
SC9600E(configure-filter-l2-1)#quit
SC9600E(config)#interface 10gigaethernet 1/0/1
SC9600E(config-10ge1/0/1)#filter-list-l2 in 1
```

7.1.8.2 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，如图 7-2所示。

组网图

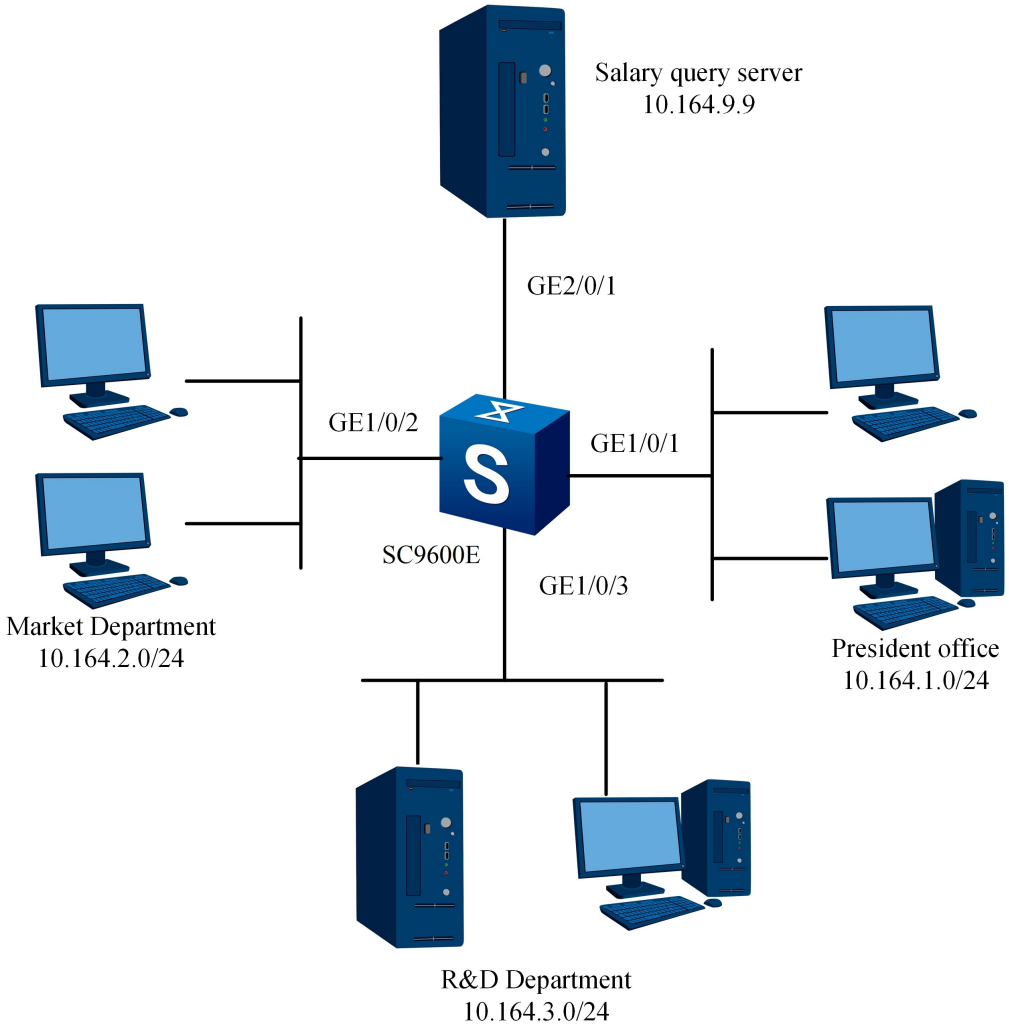


图 7-2 三层ACL示例图

配置步骤

1. 配置time-range。

```
SC9600E#configure
```

```
SC9600E(config)#time-range list 1
SC9600E(config-timerange1)#time-range 1 everyweekday 8:30:00 to 17:30:00
SC9600E(config-timerange1)#quit
```

2. 配置总裁办公室允许访问工资查询服务器的ACL。

```
SC9600E(config)#filter-list 1001
SC9600E(configure-filter-ipv4-1001)#filter 1 ip 10.164.1.0/24 10.164.9.9/32
SC9600E(configure-filter-ipv4-1001)#filter 1 action permit
SC9600E(configure-filter-ipv4-1001)#quit
```

3. 配置市场部门在指定时间段内禁止访问工资查询服务器。

```
SC9600E(config)#filter-list 1002
SC9600E(configure-filter-ipv4-1002)#filter 1 ip 10.164.2.0/24 10.164.9.9/32
SC9600E(configure-filter-ipv4-1002)#filter 1 time-range 1
SC9600E(configure-filter-ipv4-1002)#filter 1 action deny
SC9600E(configure-filter-ipv4-1002)#quit
```

4. 配置研发部门在指定时间段内禁止访问工资查询服务器。

```
SC9600E(configure)# filter-list 1003
SC9600E(configure-filter-ipv4-1003)#filter 1 ip 10.164.3.0/24 10.164.9.9/32
SC9600E(configure-filter-ipv4-1003)#filter 1 time-range 1
SC9600E(configure-filter-ipv4-1003)#filter 1 action deny
SC9600E(configure-filter-ipv4-1003)#quit
```

5. 将ACL应用到端口上。

```
SC9600E(config)#interface xgigaethernet 1/0/1
SC9600E(config-10ge1/0/1)#filter-list-ipv4 in 1001
SC9600E(config-10ge1/0/1)#quit
SC9600E(config)#interface xgigaethernet 1/0/2
SC9600E(config-10ge1/0/2)#filter-list-ipv4 in 1002
SC9600E(config-10ge1/0/2)#quit
SC9600E(config)#interface xgigaethernet 1/0/3
SC9600E(config-10ge1/0/3)#filter-list-ipv4 in 1003
```

7.1.8.3 配置混合ACL示例

组网要求

SC9600E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，如图 7-3所示。

组网图

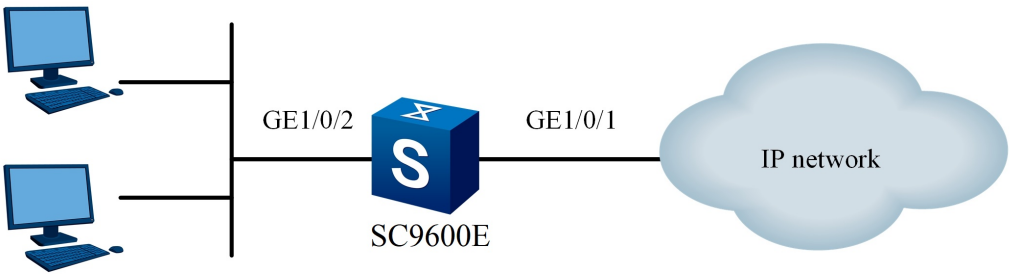


图 7-3　混合ACL示例图

配置步骤

1. 创建混合ACL。

```
SC9600E#configure
SC9600E(config)#filter-list 2001
SC9600E(configure-filter-hybrid-2001)#
```

2. 配置二层ACL规则。

```
SC9600E(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。

```
SC9600E(configure-filter-hybrid-2001)#filter 1 action cpu
```

4. 端口绑定ACL。

```
SC9600E(configure-filter-hybrid-2001)#quit
SC9600E(config)#interface xgigaethernet 1/0/2
SC9600E(config-10ge1/0/2)#filter-list-hybrid in 2001
```

7.1.8.4 配置计数模板示例

组网要求

SC9600E作为网关设备，下挂用户PC。要求配置ACL，对SC9600E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，如图 7-4所示。

组网图

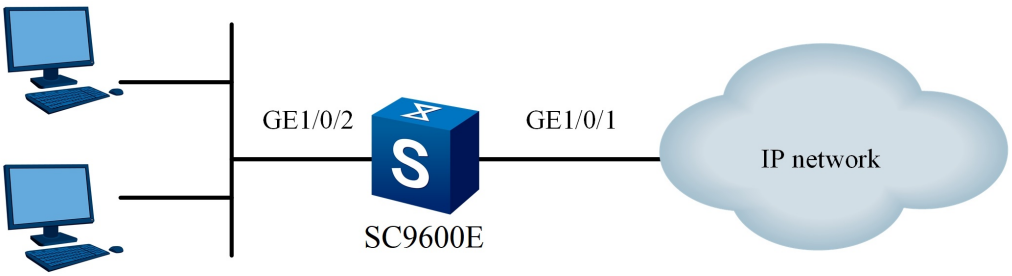


图 7-4 计数模板示例图

配置步骤

1. 配置计数模板。

```
SC9600E#configure
SC9600E(config)# counter 1 packet sort total
```

2. 创建ACL。

```
SC9600E(config)#filter-list 1001
SC9600E(configure-filter-ipv4-1001)#
```

3. 配置ACL规则。

```
SC9600E(configure-filter-ipv4-1001)#filter 1 ip 10.1.1.1/24 any
```

4. 将计数模板与该ACL绑定。

```
SC9600E(configure-filter-ipv4-1001)#filter 1 action counter 1
```

5. 端口绑定ACL。

```
SC9600E(configure-filter-ipv4-1001)#quit
SC9600E(config)#interface xgigaethernet 1/0/2
SC9600E(config-10ge1/0/2)#filter-list-ipv4 in 1001
```

7.2 本机防攻击配置

7.2.1 本机防攻击概述

本模块主要通过以下几种方式实现本机防攻击功能：

- 白名单

白名单指合法用户或者是高优先级用户的集合。通过定义ACL 可以设置白名单，后续匹配白名单特征的报文将被优先处理。这样可以主动保护现有业务、保护高优先级用户业务。可以将确定为正常使用设备的合法用户或者是高优先用户设置到白名单中。

- 黑名单

  黑名单指非法用户的集合。通过ACL 可以设置自定义黑名单，后续匹配黑名单特征的报文会被丢弃。可以将确定为攻击者的非法用户设置到黑名单中。

- 用户自定义流

  用户自定义流指用户自定义防攻击ACL 规则。主要应用于当后续网络中出现不明攻击时，用户可灵活指明攻击流数据特征，将符合此特征的数据流进行上送限制。

  将用户自定义流绑定ACL规则，当网络中出现不明攻击时，用户可以使用**car**命令和**deny**命令对符合此特征的数据流执行上送限速或者丢弃动作。当配置car时，该命令的功能相当于白名单；当配置deny时，该命令的功能相当于黑名单。

- CAR

  CAR用来设置上送CPU的报文的分类限速上送规则，针对每类报文可设置承诺信息速率（CIR，Committed Information Rate）和承诺突发尺寸（CBS，CommittedBurst Size）。通过对不同的报文设置不同的CAR规则，可以降低报文的相互影响，达到保护CPU的目的。CAR还可以设置上送CPU报文的整体速率，当整体上送速率超过阈值后，报文将被丢弃，避免CPU过载。

7.2.2 配置本机防攻击

目的

应用防攻击策略根据产品的不同，应用的场景不同。如果是集中式设备，应用防攻击策略只能应用在全局，如果是分布式设备，应用防攻击策略可以在全局及slot下应用。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置上送CPU报文的速率限制	1. 执行命令进入全局配置视图、VLANIF配置视图、接口配置视图、接口组配置视图、VLAN配置视图； 2. 执行命令**cpu-defend policy POLICY-NAME**进入CPU防攻击策略配置视图； 3. 执行命令**car packet-type (arp | bfd | bfd6 | bgp | bpdutunnel | dhcp6client | dhcp6server | dhcpclient | dhcpserver | fibhit | ftp | ftp6 | icmp | icmp6 | igmp | isis | isis6 | lacp | lldp | mldsnoop | nd-miss | ntp | ntp6 | ospf | ospf6 | snmp | ssh | stp-customer | telnet | telnet6 | tftp | tftp6 | total | vrrp | vrrp6) pps (PPS-VALUE | default)**。
删除配置上送CPU报文的速率限制	1. 执行命令进入全局配置视图、VLANIF配置视图、接口配置视图、接口组配置视图、VLAN配置视图； 2. 执行命令**cpu-defend policy POLICY-NAME**进入CPU防攻击策略配置视图； 3. 执行命令**no car packet-type (arp | bfd | bfd6 | bgp | bpdutunnel | dhcp6client | dhcp6server | dhcpclient | dhcpserver | fibhit | ftp | ftp6 | icmp | icmp6 | igmp | isis | isis6 | lacp | lldp | mldsnoop | nd-miss | ntp | ntp6 | ospf | ospf6 | snmp | ssh | stp-customer | telnet | telnet6 | tftp | tftp6 | total | vrrp | vrrp6)**。
配置CPU防攻击策略的描述信息	1. 进入全局配置视图； 2. 执行命令**cpu-defend policy POLICY-NAME**进入CPU防攻击策略配置视图； 3. 执行命令**description DESCR**。
取消配置CPU防攻击策略的描述信息	1. 进入全局配置视图； 2. 执行命令**cpu-defend policy POLICY-NAME**进入CPU防攻击策略配置视图； 3. 执行命令**no description**。

7.2.3 维护及调试

目的

当本机防攻击功能不正常，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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
显示CPU防攻击配置信息	1. 执行命令进入全局配置视图、特权用户视图、普通用户视图、VLANIF配置视图、接口配置视图、接口组配置视图、VLAN配置视图； 2. 执行命令**show cpu-defend config**。
显示防攻击所有防攻击策略列表信息或者指定防攻击策略的配置信息	1. 执行命令进入全局配置视图、特权用户视图、普通用户视图、VLANIF配置视图、接口配置视图、接口组配置视图、VLAN配置视图； 2. 执行如下命令： ▶ **show cpu-defend policy** ▶ **show cpu-defend policy POLICY-NAME**
显示CPU防攻击报文峰值统计信息	1. 执行命令进入普通用户视图； 2. 执行如下命令： ▶ **show cpu-defend peak-statistic all** ▶ **show cpu-defend peak-statistic [slot SLOT-ID]**
清除CPU防攻击报文峰值统计信息	1. 执行命令进入全局配置视图； 2. 执行命令**reset cpu-defend peak-statistic [slot SLOT-ID]**。

目的	步骤
清除CPU防攻击策略支持的具体报文峰值统计信息	1. 执行命令进入全局配置视图； 2. 执行命令**cpu-defend policy POLICY-NAME**进入CPU防攻击策略配置视图； 3. 执行命令**reset cpu-defend peak-statistic packet-type (arp | bfd | bfd6 | bgp | bpdutunnel | dhcp6client | dhcp6server | dhcpclient | dhcpserver | fibhit | ftp | ftp6 | icmp | icmp6 | igmp | isis | isis6 | lacp | lldp | mldsnoop | nd-miss | ntp | ntp6 | ospf | ospf6 | snmp | ssh | stp-customer | telnet | telnet6 | tftp | tftp6 | total | vrrp | vrrp6)**。
显示CPU防攻击统计信息	1. 执行命令进入全局配置视图、特权用户视图、普通用户视图、VLANIF配置视图、接口配置视图、接口组配置视图、VLAN配置视图； 2. 执行如下命令： ▶ **show cpu-defend statistic all** ▶ **show cpu-defend statistic slot SLOT-ID** ▶ **show cpu-defend statistic packet-type (arp | bfd | bfd6 | bgp | bpdutunnel | dhcpclient | dhcp6client | dhcpserver | dhcp6server | fibhit | ftp | ftp6 | icmp | icmp6 | igmpsnoop | isis | isis6 | lacp | lldp | mldsnoop | nd-miss | ntp | ntp6 | ospf | ospf6 | snmp | ssh | stp-customer | telnet | telnet6 | tftp | tftp6 | total | vrrp | vrrp6)**

7.3 防攻击配置

7.3.1 使能 ARP 防攻击子开关 Table

目的

本节介绍如何使能ARP防攻击子开关。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
使能或去使能报文与ARP表信息匹配检查功能	1. 执行命令进入全局配置视图； 2. 执行命令**arp-antiattack (src-ip | src-mac | arp-cheat | gateway-cheat | gratuitous-arp) (enable | disable)**。
使能或去使能ARP老化单播探测方式	1. 执行命令进入接口配置视图（以太网、trunk）、接口组配置视图； 2. 执行命令**arp detect-mode unicast (enable | disable)**。

7.3.2 配置 ARP 接口防攻击参数

目的

本节介绍如何配置ARP接口防攻击参数。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
使能或去使能ARP老化单播探测方式	1. 执行命令进入接口配置视图（以太网、trunk）、接口组配置视图； 2. 执行命令**arp detect-mode unicast (enable | disable)**。

7.3.3 防攻击模块调试

目的

本节介绍如何显示或者关闭防攻击模块的调试信息。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
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**debug arp-antiattack**。
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**no debug arp-antiattack**。
清除接口下由于不匹配绑定表而造成的报文丢弃计数	1. 进入接口配置视图（以太网、trunk）或接口组配置视图； 2. 执行命令**reset arp-antiattack statistic check user-bind**。
显示ARP报文绑定表匹配检查的项目信息	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）、接口组配置视图、VLAN配置视图； 2. 执行命令**show arp-antiattack check user-bind**。
显示ARP防攻击配置信息	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）、接口组配置视图； 2. 执行命令**show arp-antiattack config**。
显示ARP防攻击统计信息	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）、接口组配置视图； 2. 执行命令**show arp-antiattack statistic**。

7.3.4 查看 ARP 防攻击配置

目的

本节介绍如何查看ARP防攻击配置。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
查看ARP防攻击配置	1. 执行命令进入普通用户视图、特权用户视图、全局配置视图、接口配置视图、VLANIF配置视图（以太网、trunk）、接口组配置视图； 2. 执行命令**show arp-antiattack config**。
显示ARP报文绑定表匹配检查的项目信息	1. 执行命令进入普通用户视图、特权用户视图、全局配置视图、接口配置视图、VLANIF配置视图（以太网、trunk）、接口组配置视图； 2. 执行命令**show arp-antiattack check user-bind**。
显示ARP防攻击统计信息	1. 执行命令进入普通用户视图、特权用户视图、全局配置视图、接口配置视图、VLANIF配置视图（以太网、trunk）、接口组配置视图； 2. 执行命令**show arp-antiattack statistic**。

7.4 AAA Radius配置

7.4.1 AAA简介

AAA是认证、授权和统计（Authentication, Authorization and Accounting）的简称。它提供了一个用来对这三种安全功能进行配置的一致性框架。AAA的配置实际上是对网络安全的一种管理。这里的网络安全主要指访问控制。包括：

- 哪些用户可以访问网络服务器？
- 具有访问权的用户可以得到哪些服务？
- 如何对正在使用网络资源的用户进行记账？

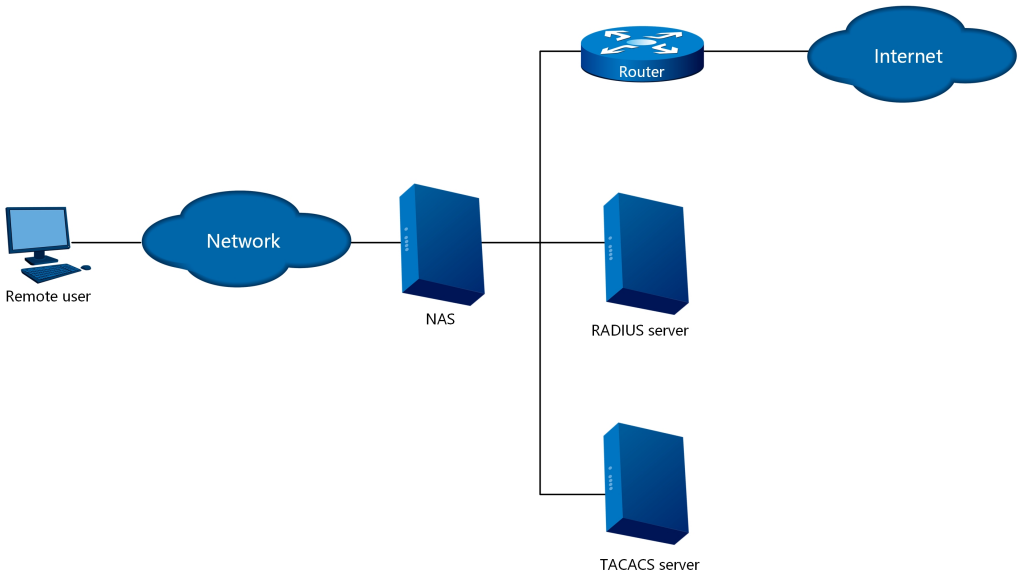


图 7-5 AAA基本架构

AAA一般采用客户机/服务器结构，客户端运行于NAS（Network Access Server，网络接入服务器）上，服务器上则集中管理用户信息。NAS对于用户来讲是服务器端，对于服务器来说是客户端。

认证功能

AAA支持以下认证方式：

- 不认证：对用户非常信任，不对其进行合法性检查，一般情况下不采用这种方式。
- 本地认证：将用户信息（包括本地用户的用户名、密码和各种属性）配置在设备上。本地认证的优点是速度快，可以降低运营成本；缺点是存储信息量受设备硬件条件限制。
- 远端认证：支持通过RADIUS协议或TACACS协议进行远端认证，由设备作为Client端，与RADIUS服务器或TACACS服务器通信。对于RADIUS协议，可以采用标准或扩展的RADIUS协议，与iTELLIN/CAMS等系统配合完成认证。

计费功能

AAA支持以下计费方式：

- 不计费(none)：不对用户计费。

- 本地计费（local）：本地计费是为了支持本地用户的连接数限制管理，实现了对用户接入数的统计功能，没有实际的费用统计功能。本地的接入数管理只对本地计费有效，对本地认证和授权没有作用。
- 远端计费：支持通过RADIUS服务器或TACACS服务器进行远端计费。

AAA一般采用客户机/服务器结构：客户端运行于被管理的资源侧，服务器上集中存放用户信息。因此，AAA框架具有良好的可扩展性，并且容易实现用户信息的集中管理。

AAA可以通过多种协议来实现，目前设备中的AAA是基于RADIUS协议或TACACS协议来实现的。

授权功能

AAA支持以下授权方式：

- 直接授权：对用户非常信任，直接授权通过，此时用户的权限为系统的默认权限。
- 本地授权：根据设备上为本地用户帐号配置的相关属性进行授权。
- TACACS授权：由TACACS服务器对用户进行授权。
- RADIUS授权：RADIUS授权是特殊的流程。RADIUS的认证和授权是在同一个流程里完成的。RADIUS在完成认证的同时会将授权信息封装在RADIUS认证回应报文下发。

7.4.2 配置AAA方法

目的

本节介绍如何创建AAA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	参数
创建AAA方法	1. 进入特权配置视图 2. 执行命令**configure** 3. 执行命令 **aaa** 4. 执行命令 **aaa (authentication|accounting) (dot1x|login|web-auth) method NAME server-group GROUPNAME** **aaa (authentication|accounting) (dot1x|login|web-auth) method NAME server-group GROUPNAME (local|none)** **aaa (authentication|accounting) (dot1x|login|web-auth) method NAME server-group GROUPNAME GROUPNAME** **aaa (authentication|accounting) (dot1x|login|web-auth) method NAME server-group GROUPNAME GROUPNAME (local|none)** **aaa (authentication|accounting) (dot1x|login|web-auth) method NAME server-group GROUPNAME GROUPNAME local none** **aaa (authentication|accounting) (dot1x|login|web-auth) method NAME server-group GROUPNAME local none** **aaa authentication (dot1x|login|web-auth) method NAME local**	Method-name: AAA方法名 Groupname: AAA服务器组名称 Local|none: 是否使能本地认证
配置本地AAA认证方法名	1. 进入特权配置视图 2. 执行命令**configure** 3. 执行命令 **aaa** 4. 执行命令**aaa authentication (ppp | login) method method-name local**	-

目的	步骤	参数
配置RADIUS服务器计费端口	1. 进入特权配置视图 2. 执行命令**configure** 3. 执行命令 **aaa** 4. 执行命令**radius-server servername auth-port（auth-port | default）**	Servername: 服务器名 Auth-port: 认证端口号,整数取值1~65535 缺省值是1812
删除已创建的AAA服务器组	1. 进入特权配置视图 2. 执行命令**configure** 3. 执行命令 **aaa** 4. 执行命令**no aaa method method-name**或**no aaa method method-name server-group groupname**	-

7.4.3 配置AAA计费方法

目的

本节介绍如何创建AAA计费方法。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤	参数
配置远程AAA认证参数	1. 进入特权配置视图 2. 执行命令**configure** 3. 执行命令 **aaa** 4. 执行命令 **aaa (authentication|account) (dot1x|ppp|login|web-auth) method NAME server-group GROUPNAME** **aaa (authentication|account) (dot1x|ppp|login|web-auth) method NAME server-group GROUPNAME (local|none)** **aaa (authentication|account) (dot1x|ppp|login|web-auth) method NAME server-group GROUPNAME GROUPNAME** **aaa (authentication|account) (dot1x|ppp|login|web-auth) method NAME server-group GROUPNAME GROUPNAME (local| none)** **aaa (authentication|account) (dot1x|ppp|login|web-auth) method NAME server-group GROUPNAME GROUPNAME local none** **aaa (authentication|account) (dot1x|ppp|login|web-auth) method NAME server-group GROUPNAME local none** **aaa authentication (dot1x|ppp| login|web-auth) method NAME local**	Method-name: AAA方法名 Groupname: AAA服务器组名称 Local|none: 是否使能本地认证
配置RADIUS服务器计费端口	1. 进入特权配置视图 2. 执行命令**configure** 3. 执行命令 **aaa** 4. 执行命令**radius-server servername acc-port (acc-port | default)**	Servername: 服务器名称 Acc-port: 计费端口号， 整数取值1~65535 Default: default value to be 1813

目的	步骤	参数
配置AAA实时计费上报间隔	1. 进入特权配置视图 2. 执行命令**configure** 3. 执行命令 **aaa** 4. 执行命令**account realtime (realtime | default)**	realtime 指定失效时间 整数形式，取值范围是300~4294967290或0，单位：秒。0表示关闭实时计费功能。 default 指定缺省值 默认为300
配置AAA服务器实时计费失效时间	1. 进入特权配置视图 2. 执行命令**configure** 3. 执行命令 **aaa** 4. 执行命令**accounting realtime (realtime | default)**或**no aaa method method-name server-group groupname**	Realtime:失效时间, 整数取值300~4294967295or 0, 单位为秒. 0 代表关闭实时计费功能 Default: 默认值是300
删除AAA方法名	1. 进入特权配置视图 2. 执行命令**configure** 3. 执行命令 **aaa** 4. 执行命令**no aaa method method-name or no aaa method method-name server-group groupname**	-

7.4.4 创建和删除服务器组

目的

本节介绍如何创建和删除服务器组。

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
创建服务器组包括服务器组协议类型定义并添加服务器	1. 进入特权配置视图 2. 执行命令**configure** 3. 执行命令 **aaa** 4. 执行命令 **server-group groupname radius-server servername**或**server-group name tacacs-server servername**	Groupname: 远程服务器组名 Servername: 服务器组名
在服务器组中删除服务器	1. 进入特权配置视图 2. 执行命令**configure** 3. 执行命令 **aaa** 4. 执行命令**no server-group groupname radius-server servername**	-
删除服务器组	1. 进入特权配置视图 2. 执行命令**configure** 3. 执行命令 **aaa** 4. 执行命令**no server-group groupname**或**server-group name radius-server servername**或**no server-group name tacacs-server servername**	-
从 AAA 服务器组中删除服务器	1. 进入特权配置视图 2. 执行命令**configure** 3. 执行命令 **aaa** 4. 执行命令**no aaa server-group groupname radius-server servername**	-
删除AAA服务器组	1. 进入特权配置视图 2. 执行命令**configure** 3. 执行命令 **aaa** 4. 执行命令**no aaa server-group groupname**	-

7.4.5 配置RADIUS 服务器

目的

本节介绍如何配置Radius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
创建Radius服务器	1. 进入特权配置视图 2. 执行命令**configure** 3. 执行命令 **aaa** 4. 执行命令 **radius-server NAME ip-address ip-address key key**或 **radius-server NAME ip6-address ip6-address key key**	NAME: Radius服务器名 Key: RADIUS通信的共享密钥，最大64位
配置服务器端口	1. 进入特权配置视图 2. 执行命令**configure** 3. 执行命令 **aaa** 4. 执行命令**radius-server NAME ip-address ipv-address key key auth-port（auth-port | default）acc-port（acc-port | default）or radius-server NAME ip6-address ipv6-address key key auth-port（auth-port | default）acc-port（acc-port | default）**	-
配置RADIUS服务器失效时间	1. 进入特权配置视图 2. 执行命令**configure** 3. 执行命令 **aaa** 4. 执行命令**radius-server deadtime（deadtime | default）** radius-server NAME deadtime (deadtime | default)	NAME: Radius服务器名 deadtime: 失效时间，整数取值60~4294967290, 单位为秒
配置RADIUS服务器重传次数	1. 进入特权配置视图 2. 执行命令**configure** 3. 执行命令 **aaa** 4. 执行命令**radius-server max-retransmit（max-retransmit | default）** **radius-server NAME max-retransmit（max-retransmit | default）**	NAME: Radius服务器名 Max-retransmit: RADIUS服务器重传次数, 整数取值范围是0~5 Default: 默认值是 3 次

目的	步骤	参数
配置RADIUS服务器重传时间间隔	1. 进入特权配置视图 2. 执行命令**configure** 3. 执行命令 **aaa** 4. 执行命令**radius-server retransmit-interval (retransmit-interval | default)** **radius-server NAME retransmit-interval (retransmit-interval | default)**	NAME: Radius服务器名 Retransmit-interval: 为重传时间间隔，缺省值为2秒, 整数取值范围是1~10
删除Radius服务器	1. 进入特权配置视图 2. 执行命令**configure** 3. 执行命令 **aaa** 4. 执行命令**no radius-server name**或**no radius-server NAME src-ip**或**no radius-server name src-ipv6**	NAME: Radius服务器名
配置Radius服务器的IP地址	1. 进入特权配置视图 2. 执行命令**configure** 3. 执行命令 **aaa** 4. 执行命令 **radius-server NAME src-ip (A.B.C.D)**或**radius-server NAME src-ip (A.B.C.D) vpn-instance NAME**或**radius-server NAME src-ipv6 (X:X::X:X)**或**radius-server NAME src-ipv6 (X:X::X:X) vpn-instance NAME**	-

7.4.6 配置TACACS服务器

目的

本节介绍如何配置TACACS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
配置TACACS服务器超时时间	1. 进入特权配置视图 2. 执行命令**configure** 3. 执行命令 **aaa** 4. 执行命令 **tacacs-server timeout (timeout –num | default)**	Timeout-num: TACACS服务器超时时间, 单位为秒, 整数取值1-10 Default: 默认值为2s
配置的TACACS+服务器的全局失效时间	1. 进入特权配置视图 2. 执行命令**configure** 3. 执行命令 **aaa** 4. 执行命令**tacacs-server deadtime (deadtime –num | default)** **tacacs-server NAME deadtime (deadtime –num | default)**	NAME: TACACS 服务器名 deadtime: 失效时间，整数取值60~4294967290, unit: second default: 默认值60s
配置TACACS服务器包括名称、IPV4地址和共享密钥	1. 进入特权配置视图 2. 执行命令**configure** 3. 执行命令 **aaa** 4. 执行命令 **tacacs-server NAME ip-address Ipv4 address key key or tacacs-server NAME ip-address Ipv6 address key key**	NAME: TACACS 服务器名 Ip4-address: 服务器ipv4地址 Ipv6-address: 服务器ipv6 地址 Key: 共享密钥, 最大位数为64
配置TACACS服务器单连接检测	1. 进入特权配置视图 2. 执行命令**configure** 3. 执行命令 **aaa** 4. 执行命令**tacacs-server NAME ipv4-address IP address key key port {port-num | default) single-connection {enable|disable} or tacacs-server NAME ipv6-address IP address key key port {port-num | default) single-connection {enable|disable}**	Ip4-address: 服务器ipv4地址 Ipv6-address: 服务器ipv6 地址 Key: 共享密钥, 最大位数为64Port-num: 配置的端口号，默认值为49
配置TACACS服务器端口	1. 进入特权配置视图 2. 执行命令**configure** 3. 执行命令 **aaa** 4. 执行命令 **tacacs-server NAME port {port-number| default)**	NAME: TACACS 服务器名 Port-num: 配置的端口号，default为4

目的	步骤	参数
配置TACACS服务器超时时间	1. 进入特权配置视图 2. 执行命令**configure** 3. 执行命令 **aaa** 4. 执行命令 **tacacs-server NAME timeout {timeout| default)**	NAME: TACACS 服务器名 Timeout: 超时时, 整数取值，范围是3-10 Default: 默认值为2
配置Tacacs服务器单连接功能	1. 进入特权配置视图 2. 执行命令**configure** 3. 执行命令 **aaa** 4. 执行命令**tacacs-server name single-connection (enable | disable)**	-
配置TACACS服务器的IP地址	1. 进入特权配置视图 2. 执行命令**configure** 3. 执行命令 **aaa** 4. 执行命令 **tacacs-server NAME src-ip (A.B.C.D)**或**tacacs-server NAME src-ip (A.B.C.D) vpn-instance NAME**或 **tacacs-server NAME src-ipv6 (X:X::X:X)**或 **tacacs-server NAME src-ipv6 (X:X::X:X) vpn-instance NAME**	-
删除tacacs 服务器	1. 进入特权配置视图 2. 执行命令**configure** 3. 执行命令 **aaa** 4. 执行命令**no tacacs-server name**或**no tacacs-server name src-ipv6**或**no tacacs-server name src-ip**	NAME: TACACS 服务器名

7.4.7 维护及调试

目的

本节介绍AAA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	参数
显示远程用户配置信息	1. 执行命令**show aaa**	-
显示全局配置信息	1. 执行命令**show aaa config**	-
显示AAA方法信息	1. 执行命令**show aaa method** 或**show aaa method method-name**	Method-name: AAA方法名称
AAA方法名称	1. 执行命令**show aaa server**或 **show aaa server server-name**	Server-name: 服务器名称
显示AAA服务器组信息	1. 执行命令 **show aaa server-group** 或**show aaa server-group group-name**	Group-name: 服务器组名称
显示所有客户端信息	1. 执行命令**show aaa show radius client**	-
打开AAA 调试开关	1. 进入特权配置视图 2. 执行命令**debug aaa**	-
关闭AAA 调试开关	1. 进入特权配置视图 2. 执行命令**no debug aaa**	-

7.5 802.1x 配置

7.5.1 802.1x简介

基于端口的网络访问控制技术，在传统以太网设备的基础上，采用IEEE 802.1x协议提供对基于以太网端口点到点连接的用户进行认证、授权的能力，从而使以太网设备可以达到电信运营的要求，尤其在宽带城域网的建设中可以发挥重大的作用。

802.1x协议是基于Client/Server的访问控制和认证协议。它可以限制未经授权的用户/设备通过接入端口访问LAN/MAN。在获得交换机或LAN提供的各种业务之前，802.1x对连接到交换机端口上的用户/设备进行认证。在认证通过之前，802.1x只允许EAPoL(基于局域网的扩展认证协议)数据通过设备连接的交换机端口；认证通过以后，正常的数据可以顺利地通过以太网端口。

基于端口的网络访问技术的基本思想是网络系统可以控制面向最终用户的以太网端口，使得只有网络系统允许并授权的用户可以访问网络系统的各种业务(如以太网连接，网络层路由，Internet接入等业务)。

网络访问技术的核心部分是PAE(端口访问实体)。在访问控制流程中，端口访问实体包含3部分：

- 认证者——对接入的用户/设备进行认证的端口；
- 请求者——被认证的用户/设备；
- 认证服务器——根据认证者的信息，对请求访问网络资源的用户/设备进行实际认证功能的设备。

以太网的每个物理端口被分为受控和不受控的两个逻辑端口，物理端口收到的每个帧都被送到受控和不受控端口。对受控端口的访问，受限于受控端口的授权状态。认证者的PAE根据认证服务器认证过程的结果，控制“受控端口”的授权/未授权状态。处在未授权状态的控制端口，拒绝用户/设备的访问。

7.5.2 配置802.1x授权

7.5.2.1 全局使能或者去使802.1x

目的

本节介绍如何全局使能或者去使能802.1x协议。

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
全局802.1x使能	1. 执行命令**configure** 2. 执行命令**dot1x start**	start: 全局使能802.1x stop: 全局不使能802.1x
全局802.1x去使能	1. 执行命令**configure** 2. 执行命令**dot1x stop**	

7.5.2.2 在端口使能或者去使能802.1x

目的

本节介绍如何在端口使能或者去使能802.1x。

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
端口802.1x使能	1. 执行命令**configure** 2. 执行命令**interface (ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 40gigaethernet) interface-number** 3. 执行命令 **dot1x enable**	interface-number: 整数，取值范围是, 1-1/0-0/1-10或1-1/0-0/1-28
端口802.1x去使能	1. 执行命令**configure** 2. 执行命令**interface (ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 40gigaethernet) interface-number** 3. 执行命令 **dot1x disable**	

7.5.2.3 设置端口最大支持的用户接入数量

目的

本节介绍如何设置端口最大支持的用户接入数量。

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
(可选l) 设置端口最大支持的用户接入数量	1. 执行命令**configure** 2. 执行命令 **interface (ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 40gigaethernet) interface-number** 3. 执行命令**dot1x authenticator max-user max-user**	interface-number: 整数，取值范围是, 1-1/0-0/1-10或1-1/0-0/1-28 max-user: 最大支持的用户接入数量 整数取值，取值范围是1~256 quiet-period: 静默时间, 整数取值，取值范围是 1~120, 单位为秒 srv-name: radius server name, character string reauthenticate-period: 静默时间, 整数取值60~7200, 单位为秒 vlan-id: VLAN ID, 整数取值1~4094 passive: 被动模式，不主动发送request/identity请求 active: 主动模式，会主动在接口上发送认证请求 account-name: AAAA计费方法名 aaa-authenticate: AAA认证方法名
(可选) 设置认证失败后的静默时间	1. 执行命令**configure** 2. 执行命令 **interface (ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 40gigaethernet) interface-number** 3. 执行命令**dot1x authentication quiet-period quiet-period** 4. (可选) 执行命令**dot1x authentication quiet-period default**	
(可选) 设置认证成功之后重新发起认证的时间间隔	1. 执行命令**configure** 2. 执行命令 **interface (ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 40gigaethernet) interface-number** 3. 执行命令**dot1x authentiation reauthenticate-period reauthenticate-period** 4. 执行命令**dot1x authentication reauthenticate-period default**	
(可选) 设置是否允许重新认证	1. 执行命令**configure** 2. 执行命令 **interface (ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 40gigaethernet) interface-number** 3. 执行命令**dot1x reauthenticate (enable|disable)**	
设置端口的工作模式	1. 执行命令**configure** 2. 执行命令 **interface (ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 40gigaethernet) interface-number** 3. 执行命令**dot1x link-mode (passive | active)**	

目的	步骤	参数
端口绑定AAA认证方法名	1. 执行命令**configure** 2. 执行命令 **interface (ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 40gigaethernet) interface-number** 3. 执行命令**dot1x aaa-accounting aacount-name**执行命令 **no dot1x aaa-account**	
port binds AAA authentication method name	1. 执行命令**configure** 2. 执行命令 **interface (ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 40gigaethernet) interface-number** 3. 执行命令**dot1x aaa-authentication auth-name**执行命令 **no dot1x aaa-authentication auth-name**	

7.5.2.4 删除802.1x用户

目的

本节介绍如何删除所有802.1x用户或者本地用户账户。

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802.1x用户或者本地用户账户	1. 执行命令**configure** 2. 执行命令**no dot1x authenticator user all**

7.5.2.5 查看802.1x的配置信息

目的

本节介绍如何查看802.1x的配置信息。

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
显示接入的用户信息	1. 进入特权配置视图 2. 执行命令**show dot1x authenticator user**	interface-number: 接口号, 整数取值1-1/0-0/1-10或1-1/0-0/1-28
显示端口配置	1. 进入特权配置视图 2. 执行命令**show dot1x interface (ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 40gigaethernet) interface-number**	
查看dot1x的配置信息	1. 进入特权配置视图 2. 执行命令**show dot1x config**	
查看 dot1x的用户接口统计信息	1. 进入特权配置视图 2. 执行命令**show dot1x statistic (ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 40gigaethernet) interface-number**	

7.5.2.6 802.1x 调试

目的

本节介绍如何使能或者去使能802.1x调试开关。

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
使能802.1x调试开关	1. 进入特权配置视图 2. 执行命令**debug dot1x (config|out | in | timer | fsm | all)**	(out | in | timer | fsm | all): 发包, 收包 ； 定时包, fsm类型包和所以类型包 packet and packet of all types
去使能802.1x调试开关	1. 进入特权配置视图 2. 执行命令**no debug dot1x (config| out | in | timer | fsm | all)**	

7.6 IP Source Guard配置

7.6.1 概述

通过IP Source Guard绑定功能，可以对端口转发的报文进行过滤控制，防止非法报文通过端口，从而限制了对网络资源的非法使用（比如非法主机仿冒合法用户IP接入网络），提高了端口的安全性。

IP Source Guard包含如下特点：

- IP+PORT+MAC+VLAN多元组合绑定来过滤IP流量；
- 可以结合DHCPSNOOPING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DHCPSNOOPING；
- IP SOURCE GUARD和DHCPSNOOPING共用配置上限；
- 具有强大的DEBUG功能；

7.6.2 配置IP Source Guard功能

目的

IP Source Guard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。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
使能接口下IP报文检查功能 使用本命令检查IP报文是否匹配绑定表，以决定是否将其转发。	1. 执行命令**configure**进入全局配置视图； 2. 执行命令**interface (ethernet | xgigaethernet | 10gigaethernet| gigaethernet) interface-number**进入接口配置视图； 3. 执行命令**ip source check user-bind enable**使能接口下IP报文检查功能； 4. 结束。
取消接口下IP报文检查功能	1. 执行命令**configure**进入全局配置视图； 2. 执行命令**interface (ethernet | xgigaethernet | 10gigaethernet| gigaethernet) interface-number**进入接口配置视图； 3. 执行命令**ip source check user-bind disable**用来取消接口下IP报文检查功能； 4. 结束。
配置IP报文的检查选项	1. 执行命令**configure**进入全局配置视图； 2. 执行命令**interface (ethernet | xgigaethernet | 10gigaethernet| gigaethernet) interface-number**进入接口配置视图； 3. 执行如下任一命令配置IP报文的检查选项（参数说明参见下表）； ▶ **ip source check user-bind check-item (ip-address | mac-address | vlan)** ▶ **ip source check user-bind check-item ip-address mac-address** ▶ **ip source check user-bind check-item ip-address vlan** ▶ **ip source check user-bind check-item mac-address vlan** 4. 结束。
恢复IP报文的检查选项为缺省选项	1. 执行命令**configure**进入全局配置视图； 2. 执行命令**interface (ethernet | xgigaethernet | 10gigaethernet| gigaethernet) interface-number**进入接口配置视图； 3. 执行命令**no ip source check user-bind check-item**用来恢复IP报文的检查选项为缺省选项（参数说明参见下表）； 4. 结束。

目的	步骤
配置静态绑定条目	1. 执行命令**configure**进入全局配置视图； 2. 执行命令如下任一用来配置静态绑定条目（参数说明参见下表）； ▶ **user-bind static ip (ipv4-address | any) mac (src-mac-address/M | any) interface gigaethernet interface-number vlan (any | vlan-id)** ▶ **user-bind static ip (ipv4-address | any) mac (src-mac-address/M | any) vlan (any | vlan-id)** 3. 结束。
删除静态绑定条目	1. 执行命令**configure**进入全局配置视图； 2. 执行命令如下任一用来删除静态绑定条目（参数说明参见下表）； ▶ **no user-bind static ip (ipv4-address | any) mac (src-mac-address/M | any) interface gigaethernet interface-number vlan (any | vlan-id)** ▶ **no user-bind static ip (ipv4-address | any) mac (src-mac-address/M | any) vlan (any | vlan-id)** 3. 结束。
使能或去使能IP报文检查告警功能	1. 执行命令**configure**进入全局配置视图； 2. 执行命令**interface (ethernet | xgigaethernet | 10gigaethernet| gigaethernet) interface-number**进入接口配置视图； 3. 执行命令**ip source check user-bind alarm enable**或**ip source check user-bind alarm disable** 4. 结束。
配置IP报文检查告警阈值	1. 执行命令**configure**进入全局配置视图； 2. 执行命令**interface (ethernet | xgigaethernet | 10gigaethernet| gigaethernet) interface-number**进入接口配置视图； 3. 执行命令**ip source check user-bind alarm threshold (threishold-value | default)** 4. 结束。

附表：

参数	说明	取值
ip-address	表示检查IP报文的IPv4地址或IPv6地址是否匹配绑定表项	-
mac-address	表示检查IP报文的MAC地址是否匹配绑定表项	-
vlan	表示检查IP报文的VLAN是否匹配绑定表项	-
ipv4-address	用户源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。
src-mac-address/M| any	指定的ACL规则的用户源MAC地址信息	src-ip-address为点分十进制形式；M为整数形式，范围为1~128。 **any**代表任意源MAC地址。
any | vlan-id	any表示不匹配该参数 vlan-id指定用户所在的VID条目	整数形式，取值范围是1~4094。 **any**代表任意VID
interface-number	指定用户接入的以太网接口号	整数形式，取值范围1-1/0-0/1-10或1-1/0-0/1-28
threshold-value	IP报文检查告警阈值	整数形式，取值范围是1-1000，单位：pps
default	默认IP报文检查告警阈值	100pps

7.6.3 维护及调试

目的

当IP Source Guard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IP Source Guard调试功能	1. 保持当前特权用户视图； 2. 执行命令**debug ip source check**打开IP Source Guard调试功能； 3. 结束。
关闭IP Source Guard调试功能	1. 保持当前特权用户视图； 2. 执行命令**no debug ip source check**打开IP Source Guard调试功能； 3. 结束。
显示可控频道表信息	1. 执行命令**disable**退出到普通用户视图或执行命令**configure**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**show igmp-control channel**显示可控频道表信息； 3. 结束。
显示IP报文检查功能相关信息	1. 执行命令**disable**退出到普通用户视图或执行命令**configure**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**show ip source check user-bind**显示IP报文检查功能相关信息； 3. 结束。
显示静态绑定条目的配置信息	1. 执行命令**disable**退出到普通用户视图或执行命令**configure**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**show user-bind config**显示静态绑定条目的相关信息； 3. 结束。

7.6.4 配置举例

组网要求

如图 7-6所示，主机A和B分别通过接口GE1/0/1 、GE1/0/2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

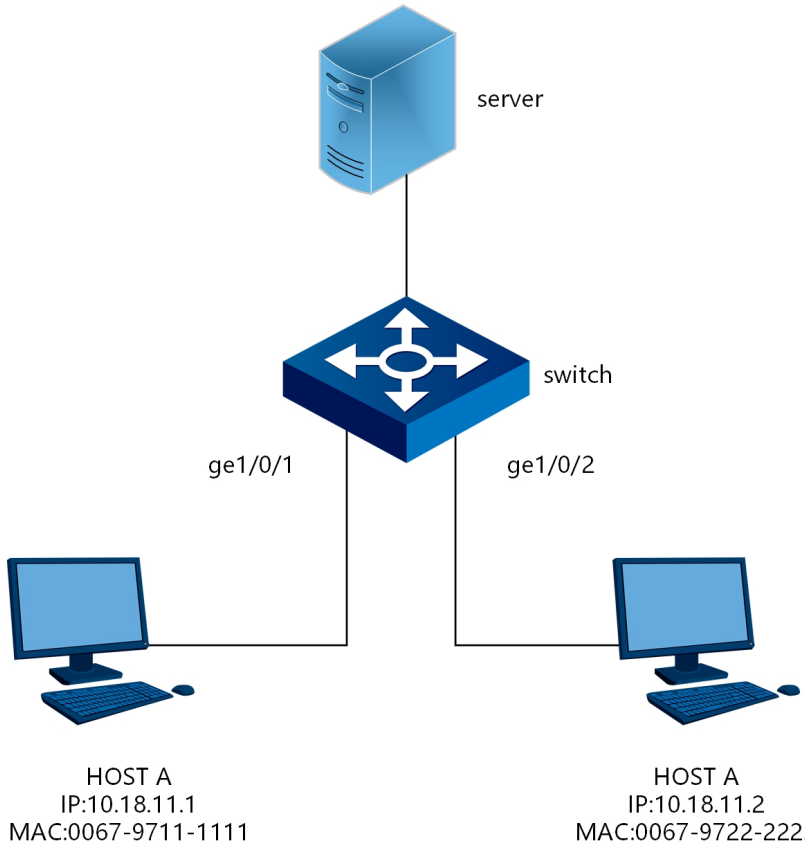


图 7-6 IP Source Guard组网图

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GE1/0/1和GE1/0/2;
3. 所在VLAN 1。

配置步骤

```
Switch(config-ge1/0/1)#user-bind enable
Switch(config-ge1/0/1)##user-bind ip 10.18.11.1 mac 00:67:97:11:11:11/48 vid 1
Switch(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。

7.7 DHCP Snooping配置

7.7.1 DHCP Snooping简介

DHCP Snooping概述

DHCP Snooping主要是为了加强DHCP的安全性而设计的。

DHCP Snooping将交换机端口划分为两类：

非信任端口：通常为连接终端设备的端口，如PC，网络打印机等；

信任端口：连接合法DHCP服务器的端口或者连接汇聚交换机的上行端口。

开启DHCP Snooping功能的交换机通过截获DHCP Client和DHCP Server之间DHCP报文并进行处理，可以过滤不信任的DHCP报文并建立和维护一个DHCP Snooping绑定表项。该表项包括非信任端口的客户端IP地址、MAC地址、端口号以及VLAN ID等信息。

通过开启DHCP Snooping功能，交换机限制用户端口（非信任端口）只能够发送DHCP请求，丢弃来自用户端口的所有其它DHCP报文，例如DHCP Offer报文等。同时，交换机还会比较DHCP 请求报文的源MAC地址和DHCP客户机的硬件地址（即CHADDR字段），只有这两者相同的请求报文才会被转发，否则将被丢弃。这样就防止了DHCP耗竭攻击。信任端口可以接收所有的DHCP报文。通过只将交换机连接到合法DHCP服务器的端口设置为信任端口，其他端口设置为非信任端口，就可以防止用户伪造DHCP服务器来攻击网络。

Option82描述

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。

SC9600E支持的DHCP Snooping特性

- Option82字段配置
- Trusted/Untrusted接口配置
- 静态添加用户绑定条目功能
- MAC地址检测功能

提示：

- 设备只有位于DHCP客户端与DHCP服务器之间，或DHCP客户端与DHCP中继之间时，DHCP Snooping功能配置后才能正常工作；设备位于DHCP服务器与DHCP中继之间时，DHCP Snooping功能配置后不能正常工作。
- 只有使能DHCP Snooping功能之后，DHCP Option 82功能才能生效。
- DHCP Snooping option 82功能建议在最靠近DHCP client的snooping设备上使用，以达到精确定位用户位置的目的。
- 使能DHCP Snooping功能的设备，一般不再作为DHCP服务器或DHCP中继。

7.7.2 配置防止DHCP Server仿冒者攻击

背景信息

网络中存在的DHCP Server仿冒者会回应给DHCP Client仿冒信息，从而使DHCP Client无法正常访问网络或访问不到正确的网络。为避免受到DHCP Server仿冒者的攻击，DHCP Snooping提供Trusted/Untrusted工作模式，将网络侧接口配置为Trusted模式，用户侧接口配置为Untrusted模式。凡是从Untrusted接口收到的DHCP Relay报文全部丢弃。

前提条件

网络上已配置好DHCP Server。

目的

为防止DHCP服务器仿冒者攻击同时定位DHCP Server仿冒者，可使用DHCP Snooping的Trusted/Untrusted工作模式以及DHCP Server探测功能。

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DHCP Snooping功能	1. 执行命令**configure**进入全局配置视图； 2. 执行命令**dhcp-snooping start**全局开启DHCP Snooping功能； 3. 结束。
接口使能DHCP Snooping功能	1. 执行命令**configure**进入全局配置视图； 2. 执行命令**interface (ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 40gigaethernet) interface-number**接口配置视图或执行命令**interface eth-trunk trunk-number**进入Trunk接口配置视图； 3. 执行命令**dhcp-snooping enable**接口使能DHCP Snooping功能； 4. 结束。
配置信任/非信任接口	1. 执行命令**configure**进入全局配置视图； 2. 执行命令**interface (ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 40gigaethernet) interface-number**接口配置视图或执行命令**interface eth-trunk trunk-number**进入Trunk接口配置视图； 3. 执行命令**dhcp-snooping (trust | untrust)**配置设备网络侧接口为Trusted模式，用户侧接口为Untrusted模式； 4. 结束。

附表：

参数	说明	取值
interface-number	指定转发组播数据的出端口	整数形式，取值范围是1-1/0-0/1-10或1-1/0-0/1-28
trust	信任接口	-
untrust	非信任接口	-

7.7.3 配置防止改变CHADDR值的DoS攻击

背景信息

网络上的攻击者如果不是改变数据帧头的源MAC地址，而是通过改变DHCP报文中的CHADDR（Client Hardware Address）值来不断申请IP地址，设备仅根据数据帧头部源MAC来判断该报文，则认为是合法的。这样的攻击报文还是可以被正常转发。

前提条件

网络上已配置好DHCP Server和DHCP Relay。

目的

为了防止攻击者通过改变CHADDR值攻击DHCP Server，可以进行本节操作配置DHCP Snooping功能检查DHCP Request报文中的CHADDR字段（该字段与数据帧头部源MAC一致，则转发此报文；若不一致，则丢弃此报文）。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
全局使能DHCP Snooping功能	1. 执行命令**configure**进入全局配置视图； 2. 执行命令**dhcp-snooping start**全局开启DHCP Snooping功能； 3. 结束。
接口使能DHCP Snooping功能	1. 执行命令**configure**进入全局配置视图； 2. 执行命令**interface (ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 40gigaethernet) interface-number**接口配置视图或执行命令**interface eth-trunk trunk-number**进入Trunk接口配置视图； 3. 执行命令**dhcp-snooping enable**接口使能DHCP Snooping功能； 4. 结束。
使能对报文的CHADDR 值检查功能	1. 执行命令**configure**进入全局配置视图； 2. 执行命令**interface (ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 40gigaethernet) interface-number**接口配置视图或执行命令**interface eth-trunk trunk-number**进入Trunk接口配置视图； 3. 执行命令**dhcp-snooping check mac-address enable**使能检查DHCP用户上送的请求报文头中的MAC地址是否合法的功能； 4. 结束。

附表：

参数	说明	取值
interface-number	指定转发组播数据的出端口	整数形式，取值范围是1-1/0-0/1-10或1-1/0-0/1-28

7.7.4 配置防止仿冒DHCP续租报文攻击

背景信息

网络上的攻击者通过不断发送DHCP Request报文来冒充用户续租IP地址，会导致一些到期的IP地址无法正常回收。

前提条件

网络上已配置好DHCP Server和DHCP Relay。

目的

为了防止攻击者通过仿冒DHCP续租报文来攻击DHCP Server，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
全局使能DHCP Snooping功能	1. 执行命令**configure**进入全局配置视图； 2. 执行命令**dhcp-snooping start**全局开启DHCP Snooping功能； 3. 结束。
接口使能DHCP Snooping功能	1. 执行命令**configure**进入全局配置视图； 2. 执行命令**interface (ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 40gigaethernet) interface-number**进入接口配置视图或执行命令**interface eth-trunk trunk-number**进入Trunk接口配置视图； 3. 执行命令**dhcp-snooping enable**接口使能DHCP Snooping功能； 4. 结束。

目的	步骤
使能对DHCP报文进行绑定表匹配检查的功能	1. 执行命令**configure**进入全局配置视图； 2. 执行命令**interface (ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 40gigaethernet) interface-number**进入接口配置视图 3. 执行命令**dhcp-snooping check user-bind enable**使能DHCP Request 报文检查功能； 4. 结束。
接口下使能/去使能Option82功能	1. 执行命令**configure**进入全局配置视图； 2. 执行命令**interface (ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 40gigaethernet) interface-number**进入接口配置视图或执行命令**interface eth-trunk trunk-number**进入Trunk接口配置视图； 3. 执行命令**dhcp-snooping option82 (enable | disable)**接口下使能/去使能Option82功能； 4. 结束。
配置Option82选项内容	1. 执行命令**configure**进入全局配置视图； 2. 执行命令**interface (ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 40gigaethernet) interface-number**进入接口配置视图或执行命令**interface eth-trunk trunk-number**进入Trunk接口配置视图； 3. 执行命令**dhcp-snooping option82 circuit-id CIRCUITID**配置Option82的circuit-id内容； 4. 执行命令**dhcp-snooping option82 remote-id REMOTEID**配置Option82的remote-id内容； 5. 结束。
接口下使能/去使能子选项sub-option9	1. 执行命令**configure**进入全局配置视图； 2. 执行命令**interface (ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 40gigaethernet) interface-number**进入接口配置视图 3. 执行命令**dhcp-snooping option82 sub-option9 STRING**接口下使能/去使能Option82功能； 4. 结束。

目的	步骤
配置Option82的子选项9的内容	1. 执行命令**configure**进入全局配置视图； 2. 执行命令**interface (ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 40gigaethernet) interface-number**进入接口配置视图或执行命令**interface eth-trunk trunk-number**进入Trunk接口配置视图； 3. 执行命令**dhcp-snooping sub-option9 (enable | disable)**配置Option82的子选项9的内容； 4. 结束。
在接口下构造DHCP报文中插入的Option82选项的格式	1. 执行命令**configure**进入全局配置视图； 2. 执行命令**interface (ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 40gigaethernet) interface-number**进入接口配置视图或执行命令**interface eth-trunk trunk-number**进入Trunk接口配置视图； 3. 执行命令**dhcp-snooping option82 circuit-id format (common | default)**或**dhcp-snooping option82 remote-id format (common | default)**或**dhcp-snooping option82 circuit-id format user-defined txt**或**dhcp-snooping option82 remote-id format user-defined txt** 4. 结束。
配置Option82的策略	1. 执行命令**configure**进入全局配置视图； 2. 执行命令**interface (ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 40gigaethernet) interface-number**进入接口配置视图或执行命令**interface eth-trunk trunk-number**进入Trunk接口配置视图； 3. 执行命令**dhcp-snooping option82 (drop | keep | append)**配置Option82的策略； 4. 结束。
配置在DHCPv6 报文中插入Option18 或Option37 字段	1. 执行命令**configure**进入全局配置视图； 2. 执行命令**interface (ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 40gigaethernet) interface-number**进入接口配置视图或执行命令**interface eth-trunk trunk-number**进入Trunk接口配置视图； 3. 执行命令**dhcp6-snooping option18 (enable | disable)**配置接口下使能/去使能v6的option18选项功能； 4. 执行命令**dhcp6-snooping option37 (enable | disable)**配置接口下使能/去使能v6的option37选项功能； 5. 结束。

目的	步骤
在接口下构造DHCP报文中插入的Option18选项的cicruit-id格式	1. 执行命令**configure**进入全局配置视图； 2. 执行命令**interface (ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 40gigaethernet) interface-number**进入接口配置视图或执行命令**interface eth-trunk trunk-number**进入Trunk接口配置视图； 3. 执行命令**dhcp6-snooping option18 format (common | default)**或**dhcp6-snooping option18 format user-defined txt** 4. 结束。
在接口下构造DHCP报文中插入的Option37子选项的remote-id格式	1. 执行命令**configure**进入全局配置视图； 2. 执行命令**interface (ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 40gigaethernet) interface-number**进入接口配置视图或执行命令**interface eth-trunk trunk-number**进入Trunk接口配置视图； 3. 执行命令**dhcp6-snooping option37 format (common | default)**或**dhcp6-snooping option37 format user-defined txt** 4. 结束。
配置绑定信息	1. 执行命令**configure**进入全局配置视图； 2. 执行命令**dhcp-snooping binding mac-address ipv4-address vlan-id (ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 40gigaethernet) interface-number**或**dhcp-snooping binding mac-address ipv4-address vlan-id eth-trunk trunk-number**或**dhcp6-snooping binding mac-address ipv6-address vid (ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 40gigaethernet) interface-number**或**dhcp6-snooping binding mac-address ipv6-address vid eth-trunk trunk-number** ； 3. 结束。

附表：

参数	说明	取值
interface-number	指定转发组播数据的出端口	整数形式，取值范围1-1/0-0/1-10或1-1/0-0/1-28
CIRCUITID	circuit ID号	-
REMOTEID	remote ID号	-

参数	说明	取值
STRING	sub-option9配置条目	-
(drop|keep|append)	option82策略，分别为丢弃，保留和附加策略。	-

7.7.5 配置DHCP Snooping用户数限制

背景信息

网络上的攻击者为了抑制用户，恶意申请IP地址。配置DHCP Snooping用户数限制功能后，当用户数达到配置的最大值，则任何用户将无法成功申请到IP地址。

前提条件

使能对DHCP报文进行绑定表匹配检查的功能。

目的

为了防止网络上的攻击者通过不断申请IP地址造成合法用户无法上线，可以使用本节操作配置最大用户数限制数量。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
全局使能DHCP Snooping功能	1. 执行命令**configure**进入全局配置视图； 2. 执行命令**dhcp-snooping start**全局开启DHCP Snooping功能； 3. 结束。
接口使能DHCP Snooping功能	1. 执行命令**configure**进入全局配置视图； 2. 执行命令**interface (ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 40gigaethernet) interface-number**进入接口配置视图或执行命令**interface eth-trunk trunk-number**进入Trunk接口配置视图； 3. 执行命令**dhcp-snooping enable**接口使能DHCP Snooping功能； 4. 结束。
配置DHCP Snooping下最大用户使用数目	1. 执行命令**configure**进入全局配置视图； 2. 执行命令**interface (ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 40gigaethernet) interface-number**进入接口配置视图 3. 执行命令**dhcp-snooping max-user-number (max-value | default)**配置DHCP Snooping下最大用户使用数目； 4. 结束。

附表：

参数	说明	取值
interface-number	指定转发组播数据的出端口	整数形式，取值范围是1-1/0-0/1-10或1-1/0-0/1-28
max-value	DHCP用户数限制范围	整数形式，取值范围是1~32768
default	DHCP 用户默认值	默认值为32768

7.7.6 维护及调试

目的

当DHCP 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DHCP Snooping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 **debug dhcp-snooping（in	verbose	all)**打开DHCP Snooping调试功能； 3. 结束。
清除DHCP Snoop统计计数	1. 执行命令**configure**进入全局配置视图或执行命令 **interface（ethernet	gigaethernet	xgigaethernet	10gigaethernet	40gigaethernet ）interface-number** 进入接口配置视图或执行命令**interface eth-trunk trunk-number** 进入Trunk接口配置视图； 2. 执行命令 **reset dhcp-snooping statistic**用于清除DHCP Snoop统计计数； 3. 结束。
查看DHCP Snooping协议的配置信息	1. 执行命令**configure**进入全局配置视图或执行命令 **interface（ethernet	gigaethernet	xgigaethernet	10gigaethernet	40gigaethernet ）interface-number** 进入接口配置视图或执行命令**interface eth-trunk trunk-number** 进入Trunk接口配置视图； 2. 执行命令 **show dhcp-snooping config**用来显示DHCP Snooping协议的配置信息； 3. 结束。
查看DHCP Snooping协议的用户绑定配置信息	1. 执行命令**configure**进入全局配置视图或执行命令 **interface（ethernet	gigaethernet	xgigaethernet	10gigaethernet	40gigaethernet ）interface-number** 进入接口配置视图或执行命令**interface eth-trunk trunk-number** 进入Trunk接口配置视图； 2. 执行命令 **show dhcp-snooping binding**用来显示DHCP Snooping协议的用户绑定配置信息； 3. 结束。

目的	步骤
查看DHCP Snooping协议下的用户接口配置统计信息	1. 执行命令**configure**进入全局配置视图或执行命令**interface (ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 40gigaethernet) interface-number** 进入接口配置视图或执行命令**interface eth-trunk trunk-number** 进入Trunk接口配置视图； 2. 执行命令 **show dhcp-snooping statistic interface (ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 40gigaethernet) interface-number**或执行命令**show dhcp-snooping statistic** 用来显示DHCP Snooping协议下的用户接口配置统计信息； 3. 结束。
查看DHCP Snooping协议下的用户接口配置信息	1. 执行命令**configure**进入全局配置视图或执行命令**interface (ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 40gigaethernet) interface-number** 进入接口配置视图或执行命令**interface eth-trunk trunk-number** 进入Trunk接口配置视图； 2. 执行命令 **show dhcp-snooping interface (ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 40gigaethernet) interface-number**或执行命令**show dhcp-snooping interface** 用来显示DHCP Snooping协议下的用户接口配置信息； 3. 结束。

附表：

参数	说明	取值
interface-number	指定转发组播数据的出端口	整数形式，取值范围是1-1/0-0/1-10或1-1/0-0/1-28
receive	表示收到的数据包	-
detail	表示DHCP Snooping设置的状态细节	-
all	表示所有信息	-

7.7.7 配置举例

组网要求

某公司的办公区域包括三个小组group1、group2和group3，独立地分布在三个房间中。该公司通过DHCP server统一管理IP地址，为不同的小组分配不同范围的地址。

具体需求如下：

- DHCP server为办公室设备分配192.168.1.0/24网段的地址，有效期为12小时，并指定DNS和WINS服务器地址分别为192.168.10.2和192.168.10.3。
- 三个小组group1、group2和group3分别通过端口Ethernet1/0/1、Ethernet1/0/2和Ethernet1/0/3接入DHCP snooping设备，并通过DHCP snooping设备与DHCP server通信。
- DHCP server为group1的用户分配192.168.1.2～192.168.1.30之间的地址；为group2的用户分配192.168.1.100～192.168.1.200之间的地址；为group3的用户分配192.168.1.200～192.168.1.250之间的地址。

组网图

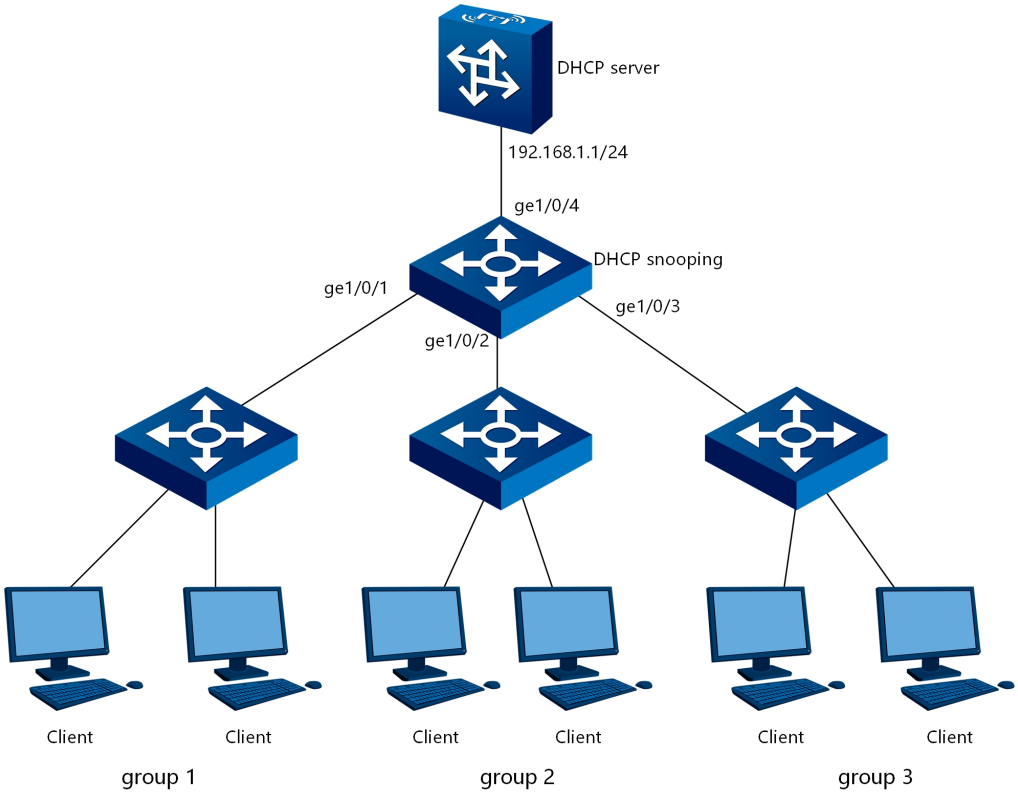


图 7-7　IGMP配置拓扑图

配置思路

- 在DHCP snooping设备上启动Option 82功能。
- 可以通过命令行配置Option 82的子选项内容，使不同小组的用户携带不同的Option 82信息。可以通过用户自定义Circuit ID子选项内容的方式来实现。
- 在DHCP Server上配置IP地址分配策略，使得DHCP Server可以根据Option 82为DHCP Client分配合适的IP地址。

配置步骤

1. 全局使能DHCP Snooping功能。

```
Switch#configure
Switch(config)#dhcp-snooping start
```

2. 配置端口gigaethernet1/0/4为信任端口。

```
Switch(config)#interface gigaethernet 1/0/4
Switch(config-ge1/0/4)#dhcp-snooping enable
```

```
Switch(config-ge1/0/4)#dhcp-snooping trusted
Switch(config-ge1/0/4)#quit
Switch(config)#
```

3. 在端口gigaethernet1/0/1使能Option 82。

```
Switch(config)#interface gigaethernet 1/0/1
Switch(config-ge1/0/1)#dhcp-snooping enable
Switch(config-ge1/0/1)#dhcp-snooping option82 enable
```

4. 在端口gigaethernet1/0/1配置Option 82的Circuit ID填充内容为group1。

```
Switch(config-ge1/0/1)#dhcp-snooping option82 circuit-id group1
```

5. 在端口gigaethernet1/0/2使能Option 82。

```
Switch(config)#interface gigaethernet 1/0/2
Switch(config-ge1/0/2)#dhcp-snooping enable
Switch(config-ge1/0/2)#dhcp-snooping option82 enable
```

6. 在端口gigaethernet1/0/2配置Option 82的Circuit ID填充内容为group2。

```
Switch(config-ge1/0/2)#dhcp-snooping option82 circuit-id group2
Switch(config-ge1/0/2)#quit
Switch(config)#
```

7. 在端口gigaethernet1/0/3使能Option 82。

```
Switch(config)#interface gigaethernet 1/0/3
Switch(config-ge1/0/3)#dhcp-snooping enable
Switch(config-ge1/0/3)#dhcp-snooping option82 enable
```

8. 在端口gigaethernet1/0/3配置Option 82的Circuit ID填充内容为group3。

```
Switch(config-ge1/0/3)#dhcp-snooping option82 circuit-id group3
Switch(config-ge1/0/3)#quit
```

9. 检验配置效果。

```
Swich#show running-config
#
interface gigaethernet1/0/1
dhcp-snooping enable
 dhcp-snooping p option82 enable
 dhcp-snooping option82 circuit-id group1
#
interface gigaethernet1/0/2
 dhcp-snooping enable
 dhcp-snooping option82 enable
dhcp-snooping option82 circuit-id group2

#  interface gigaethernet1/0/3
dhcp-snooping enable
dhcp-snooping option82 enable
```

```
dhcp-snooping option82 circuit-id group3
#
interface gigaethernet1/0/4
 dhcp-snooping trust
#
```

8 可靠性配置

本章介绍了SC9600E系列数据中心交换机可靠性管理的基本内容、配置过程和配置举例。

8.1 MSTP 配置

8.1.1 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，从而占用所有的有效带宽，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

1. 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。
2. 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。
3. 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。
4. 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 BPDU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的缺点在应用中也被暴露了出来。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（如语音视频）中是不能接受的。

8.1.2 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（Rapid Spanning Tree Protocol，快速生成树协议）。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）。改进如下：

- 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。

8.1.3 MSTP 简介

MSTP的优点

MSTP（Multiple Spanning Algorithm and Protocol，多生成树协议）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

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。

1) 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。

- 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。

- 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 ： ERCB ： RRB ： IRCB ： 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}。

- 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}。

- 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}。

- 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}。

- 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}。

2) 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SC9600E_1优于SC9600E_2，SC9600E_2优于SC9600E_3，4、5、10分别为链路的路径开销。SC9600E_1和SC9600E_2属于同一域，SC9600E_3单独一个域。

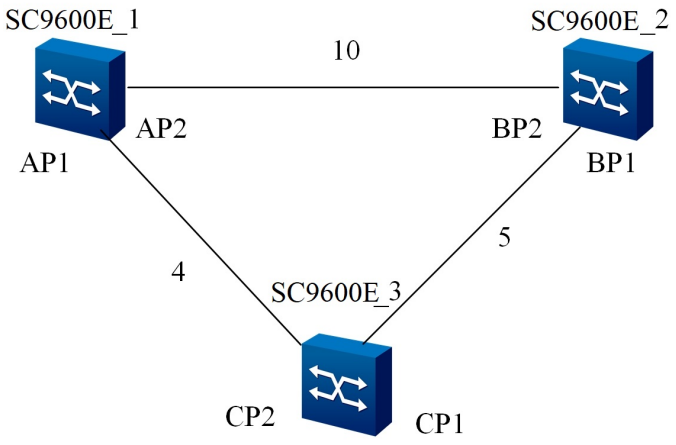


图 8-1 MSTP算法计算过程组网图

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
SC9600E_1	AP1	{A:0:A:0:A:AP1:0}
	AP2	{A:0:A:0:A:AP2:0}
SC9600E_2	BP1	{B:0:B:0:B:BP1:0}
	BP2	{B:0:B:0:B:BP2:0}
SC9600E_3	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。

- SC9600E_1的角色选择过程

  SC9600E_1的端口AP1和端口AP2会分别收到来自SC9600E_2和SC9600E_3的报文，SC9600E_1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SC9600E_1为总根且为SC9600E_1和SC9600E_2所在域的域根。此后端口定时对外传播以自己为根的消息。

- SC9600E_2的角色选择过程

  SC9600E_2的端口BP1收到来自SC9600E_3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。

  SC9600E_2的端口BP2收到来自SC9600E_1的端口AP2的报文后，处理过程如下：

  a) 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}；

  b) 计算端口的根路径优先级向量。SC9600E_1和SC9600E_2在同一域内，端口的根路径优先级向量为{A:0:A:10:A:AP2:BP2}；

  c) 计算SC9600E_2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SC9600E_2的桥优先级向量，SC9600E_2的根优先级向量为{A:0:A:10:A:AP2:BP2}；

d) 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SC9600E_1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。

- SC9600E_3的角色选择过程

SC9600E_3的端口CP1收到来自SC9600E_2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SC9600E_1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SC9600E_3与SC9600E_1和SC9600E_2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。

SC9600E_3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。

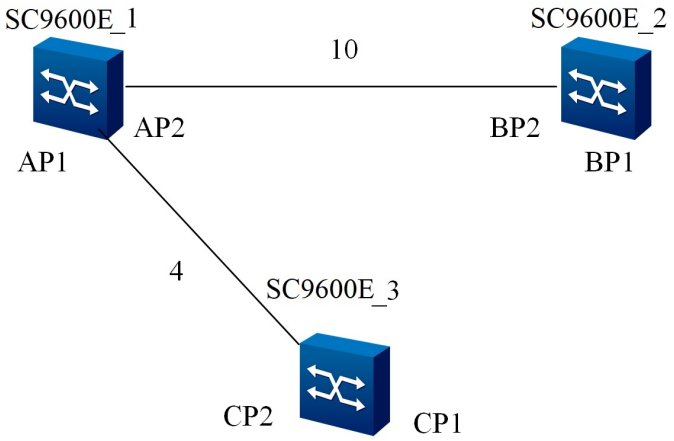


图 8-2 计算后流量转发线路

8.1.4 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置交换机生成树的工作模式	1. 进入全局配置视图； 2. 进入STP配置视图； 3. 执行命令**stp mode (stp | rstp | mstp | default)**用来设置交换机生成树的工作模式。
配置MST域 （需要先配置交换机生成树的工作模式为mstp模式或default模式）	1. 进入全局配置视图； 2. 进入STP配置视图； 3. 执行命令**stp config-name STRING**用来设置生成树域名；缺省情况下，SC9600E生成树域名为F-engine； 4. 执行命令**stp instance INSTANCE-ID vlan VLAN-LIST**用来设置MSTI应用的VLAN； 5. 执行命令**stp revision-level (RANGE | default)**用来设置设备MSTP修订级别。
配置是否使能端口生成树功能 （需要先配置交换机生成树的工作模式为mstp模式或default模式）	1. 进入全局配置视图； 2. 进入接口配置视图（以太网、trunk）、接口组配置视图、批量接口配置视图； 3. 执行命令**stp (enable | disable)**用来使能或去使能端口生成树功能。
（可选）配置交换机在指定MSTI中的优先级	1. 进入全局配置视图； 2. 进入STP配置视图； 3. 执行命令**stp instance INSTANCE-ID priority (PRIORITY | default)**用来设置交换机在指定MSTI中的优先级。
（可选）配置CIST实例0的优先级	1. 进入全局配置视图； 2. 进入STP配置视图； 3. 执行命令**stp priority (PRIORITY | default)**用来设置CIST实例0的优先级。
（可选）配置端口优先级	1. 进入全局配置视图； 2. 进入接口配置视图（以太网、trunk）； 3. 执行如下命令： ▶ **stp priority (PRIORITY | default)** ▶ **stp process PROCESS-ID priority (PRIORITY | default)**
（可选）配置当前接口在指定MSTI（MST实例）上的管理路径开销	1. 进入全局配置视图； 2. 进入接口配置视图（以太网、trunk）、接口组配置视图； 3. 执行命令**stp instance INSTANCE-ID path-cost (PATH-COST | default)**配置当前接口在指定MSTI（MST实例）上的管理路径开销。
（可选）配置当前接口在指定MSTI上的优先级	1. 进入全局配置视图； 2. 进入接口配置视图（以太网、trunk）、接口组配置视图； 3. 执行命令**stp instance INSTANCE-ID priority (PRIORITY | default)**配置当前接口在指定MSTI上的优先级。

8.1.5 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置生成树转发时延	1. 进入全局配置视图； 2. 进入STP配置视图； 3. 执行命令**stp forward-delay (FORWARD-DELAY | default)**用来设置生成树转发时延。
配置协议发送hello报文间隔时间	1. 进入全局配置视图； 2. 进入STP配置视图； 3. 执行命令**stp hello-time (HELLO-INTERVAL | default)**用来设置协议发送hello报文间隔时间。
配置交换机生成树的最大老化时间	1. 进入全局配置视图； 2. 进入STP配置视图； 3. 执行命令**stp max-age (MAX-AGE | default)**用来设置交换机生成树的最大老化时间。
配置MST域内生成树最大跳数	1. 进入全局配置视图； 2. 进入STP配置视图； 3. 执行命令**stp max-hops (MAX-HOP | default)**设置MST域内生成树最大跳数。

目的	步骤
配置是否为边缘端口	1. 进入全局配置视图； 2. 进入接口配置视图（以太网、trunk）、接口组配置视图、批量接口配置视图； 3. 执行命令**stp (enable | disable)**使能或去使能端口生成树功能； 4. 执行命令**stp edge-port (enable | disable)**使能或去使能接口为边缘端口。
配置接口是否点到点管理	1. 进入全局配置视图； 2. 进入接口配置视图（以太网、trunk）、接口组配置视图、批量接口配置视图； 3. 执行命令**stp (enable | disable)**使能或去使能端口生成树功能； 4. 执行命令**stp point-to-point (force-true | force-false | auto)**设置接口链路类型。
配置当前接口在指定MSTI上的优先级	1. 进入全局配置视图； 2. 进入接口配置视图（以太网、trunk）、接口组配置视图、批量接口配置视图； 3. 执行命令**stp (enable | disable)**使能或去使能端口生成树功能； 4. 执行命令**stp instance INSTANCE-ID priority (PRIORITY | default)**设置当前接口在指定MSTI上的优先级。
配置当前接口在指定MSTI（MST实例）上的管理路径开销	1. 进入全局配置视图； 2. 进入接口配置视图（以太网、trunk）、接口组配置视图、批量接口配置视图； 3. 执行命令**stp (enable | disable)**使能或去使能端口生成树功能； 4. 执行命令**stp instance INSTANCE-ID path-cost (PATH-COST | default)**设置当前接口在指定MSTI（MST实例）上的管理路径开销。
配置生成树Hello Time周期内发包次数（即发送的BPDU的个数）	1. 进入全局配置视图； 2. 进入STP配置视图； 3. 执行命令**stp transmit-limit (TRANSMIT-LIMIT | default)**用来设置生成树Hello Time周期内发包次数。
配置接口在实例0上的管理路径开销值	1. 进入全局配置视图； 2. 进入接口配置视图（以太网、trunk）、接口组配置视图、批量接口配置视图； 3. 执行命令**stp (enable | disable)**使能或去使能端口生成树功能； 4. 执行命令**stp path-cost (PATH-COST | default)**或**stp process PROCESS-ID path-cost (PATH-COST | default)**设置接口在实例0上的管理路径开销值。

目的	步骤
配置STP端口路径开销计算的标准	1. 进入全局配置视图； 2. 进入STP配置视图； 3. 执行命令**stp pathcost-standard (dot1t | dot1d-1998)**设置STP端口路径开销计算的标准。
配置当前接口执行模式检查操作	1. 进入全局配置视图； 2. 进入接口配置视图（以太网、trunk）、接口组配置视图、批量接口配置视图； 3. 执行命令**stp (enable | disable)**使能或去使能端口生成树功能； 4. 执行命令**stp mcheck**设置当前接口执行模式检查操作。
配置生成树协议转换周期	1. 进入全局配置视图； 2. 进入STP配置视图； 3. 执行命令**stp migration-time (MIGRATION-TIME | default)**设置生成树协议转换周期。
配置是否使能生成树Trap告警功能	1. 进入全局配置视图； 2. 进入STP配置视图； 3. 执行命令**stp trap (enable | disable)**使能或去使能生成树Trap告警功能。
配置TC防攻击包阈值	1. 进入全局配置视图； 2. 进入STP配置视图； 3. 执行命令**stp tc-protection threshold (THRESHOLD-VALUE | default)**配置TC防攻击包阈值。
删除生成树实例	1. 进入全局配置视图； 2. 进入STP配置视图； 3. 执行命令**no stp instance INSTANCE-ID**删除生成树实例。
配置生成树的超时时间	1. 进入全局配置视图； 2. 进入STP配置视图； 3. 执行命令**stp timer-factor (TIMER-VALUE | default)**配置生成树的超时时间。
使能或去使能BPDU filter功能	1. 进入全局配置视图； 2. 进入接口配置视图（以太网、trunk）、接口组配置视图、批量接口配置视图； 3. 执行命令**stp (enable | disable)**使能或去使能端口生成树功能； 4. 执行命令**stp bpdu-filter (enable | disable)**使能或去使能BPDU filter功能。

目的	步骤
配置端口优先级	1. 进入全局配置视图； 2. 进入接口配置视图（以太网、trunk）、接口组配置视图、批量接口配置视图； 3. 执行命令**stp (enable | disable)**使能或去使能端口生成树功能； 4. 执行命令**stp priority (PRIORITY | default)**配置端口优先级。
使能或去使能STP进入跨设备组合工作模式	1. 进入全局配置视图； 2. 进入STP配置视图； 3. 执行命令**stp v-stp (enable | disable)**使能或去使能STP进入跨设备组合工作模式。
清除STP统计信息	1. 进入全局配置视图； 2. 进入接口配置视图（以太网、trunk）、接口组配置视图、批量接口配置视图； 3. 执行命令**stp (enable | disable)**使能或去使能端口生成树功能； 4. 执行命令**stp reset statistic**清除STP统计信息。
创建MSTP进程并进入该MSTP进程的视图	1. 进入全局配置视图； 2. 进入STP配置视图； 3. 执行命令**stp process PROCESS-ID**创建MSTP进程并进入该MSTP进程的视图。
删除一个指定ID的MSTP进程	1. 进入全局配置视图； 2. 进入STP配置视图； 3. 执行命令**no stp process PROCESS-ID**删除一个指定ID的MSTP进程。
配置MST域内生成树最大跳数	1. 进入全局配置视图； 2. 进入STP配置视图； 3. 执行命令**stp max-hops (MAX-HOP | default)**配置MST域内生成树最大跳数。
使能/去使能生成树接收拓扑改变报文刷新MAC操作	1. 进入全局配置视图； 2. 进入STP配置视图； 3. 执行命令**stp flush (enable | disable)**使能/去使能生成树接收拓扑改变报文刷新MAC操作。
使能或去使能交换设备所有端口为边缘端口	1. 进入全局配置视图； 2. 进入STP配置视图； 3. 执行命令**stp edge-default (enable | disable)**使能或去使能交换设备所有端口为边缘端口。

目的	步骤
配置当前设备参与生成树计算的桥MAC	1. 进入全局配置视图； 2. 进入STP配置视图； 3. 执行命令**stp bridge-address MAC-ADDRESS**配置当前设备参与生成树计算的桥MAC。
使能或去使能STP的增强模式	1. 进入全局配置视图； 2. 进入STP配置视图； 3. 执行命令**stp enhance-mode (enable | disable)**使能或去使能STP的增强模式。

8.1.6 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-BPDU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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置交换机BPDU保护功能	1. 进入全局配置视图； 2. 进入STP配置视图； 3. 执行命令**stp bpdu-guard (enable | disable)**设置交换机BPDU保护功能。
配置交换机的root保护功能	1. 进入全局配置视图； 2. 进入接口配置视图（以太网、trunk）、接口组配置视图； 3. 执行命令**stp root-guard (enable | disable)**设置交换机环路保护功能。
配置交换机TC保护功能	1. 进入全局配置视图； 2. 进入STP配置视图； 3. 执行命令**stp tc-protection (enable | disable)**设置交换机TC保护功能； 4. 执行命令**stp tc-hold-off (TIME | default)**设置拓扑改变延迟/抑制时间。
使能或去使能对tc-flush-arp报文的保护功能	1. 进入全局配置视图； 2. 进入STP配置视图； 3. 执行命令**stp tc-flush-arp (enable | disable)**使能或去使能对tc-flush-arp报文的保护功能。
使能或去使能对TC-BPDU报文的保护功能	1. 进入全局配置视图； 2. 进入STP配置视图； 3. 执行命令**stp tc-protection (enable | disable)**使能或去使能对TC-BPDU报文的保护功能。
使能或去使能端口生成树环路保护功能	1. 进入全局配置视图； 2. 进入接口配置视图（以太网、trunk）、接口组配置视图； 3. 执行命令**stp loop-guard (enable | disable)**使能或去使能端口生成树环路保护功能。
配置接口参与多个MSTP进程的状态计算	1. 进入全局配置视图； 2. 进入接口配置视图（以太网、trunk）、接口组配置视图； 3. 执行命令**stp link-share binding process PROCESS-LIST**配置接口参与多个MSTP进程的状态计算。
将当前端口加入指定ID的生成树进程中	1. 进入全局配置视图； 2. 进入接口配置视图（以太网、trunk）、接口组配置视图； 3. 执行命令**stp binding process PROCESS-ID**将当前端口加入指定ID的生成树进程中。

目的	步骤
将当前端口退出指定ID的生成树进程中	1. 进入全局配置视图； 2. 进入接口配置视图（以太网、trunk）、接口组配置视图； 3. 执行命令**no stp binding process PROCESS-LIST**将当前端口退出指定ID的生成树进程中。
使能或去使能点到点链路检测开关	1. 进入全局配置视图； 2. 进入STP配置视图； 3. 执行命令**stp link-detection (enable | disable)**使能或去使能点到点链路检测开关。

8.1.7 维护及调试

目的

当MSTP功能不正常，需要进行查看、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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
查看交换机生成树协议的配置信息	1. 进入普通用户视图； 2. 执行命令**show stp**显示交换机生成树协议的配置信息。
查看交换机生成树协议的配置文件信息	1. 进入普通用户视图； 2. 执行命令**show stp config**显示交换机生成树协议的配置文件信息。
查看交换机生成树协议的相关信息	1. 进入普通用户视图； 2. 执行命令**show stp information**显示交换机生成树协议的相关信息。
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	1. 进入普通用户视图； 2. 执行命令**show stp instance INSTANCE-ID interface**显示交换机生成树协议实例在全部接口的配置信息； 3. 执行如下命令显示交换机生成树协议实例指定接口的配置信息： ▶ **show stp instance INSTANCE-ID interface (ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 40gigaethernet) INTERFACE-NUMBER** ▶ **show stp instance INSTANCE-ID interface eth-trunk TRUNK-NUMBER**

目的	步骤
查看交换机全部接口生成树协议的配置信息	1. 进入普通用户视图； 2. 执行命令**show stp interface**显示交换机全部接口生成树协议的配置信息。
查看交换机指定接口的生成树协议的相关配置信息	1. 进入普通用户视图； 2. 执行如下命令显示交换机指定接口的生成树协议的相关配置信息： ▶ **show stp interface（ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 40gigaethernet ）INTERFACE-NUMBER** ▶ **show stp interface eth-trunk TRUNK-NUMBER**
查看link up接口以及保护状态接口的生成树状态信息	1. 进入普通用户视图； 2. 执行命令**show stp brief**查看link up接口以及保护状态接口的生成树状态信息。
查看生成树多进程当前工作接口的生成树状态	1. 进入普通用户视图； 2. 执行命令**show stp process PROCESS-ID brief**查看生成树多进程当前工作接口的生成树状态。
查看生成树多进程当前接口的具体信息	1. 进入普通用户视图； 2. 执行如下命令查看生成树多进程当前接口的具体信息： ▶ **show stp process PROCESS-ID interface（ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 40gigaethernet ）INTERFACE-NUMBER** ▶ **show stp process PROCESS-ID interface eth-trunk TRUNK-NUMBER**
查看端口TC/TCN报文收发计数	1. 进入普通用户视图； 2. 执行命令**show stp tc-bpdu statistic**查看端口TC/TCN报文收发计数。

目的	步骤
查看拓扑变化相关的统计信息	1. 进入普通用户视图； 2. 执行命令**show stp topology-change**查看拓扑变化相关的统计信息。
打开或关闭生成树调试功能	1. 进入特权用户视图； 2. 执行如下命令打开或关闭生成树调试功能： ▶ **debug stp (error | statemachine | protection | timer | in | out | packet | protocol | event | sync | ptx | prx | ppm | bdm | pim | prs | prt | pst | tcm | all) interface (ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 40gigaethernet) INTERFACE-NUMBER** ▶ **debug stp (error | statemachine | protection | timer | in | out | packet | protocol | event | sync | ptx | prx | ppm | bdm | pim | prs | prt | pst | tcm | all) interface eth-trunk TRUNK-NUMBER** ▶ **no debug stp (error | statemachine | protection | timer | in | out | packet | protocol | event | sync | ptx | prx | ppm | bdm | pim | prs | prt | pst | tcm | all) interface (ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 40gigaethernet) INTERFACE-NUMBER** ▶ **no debug stp (error | statemachine | protection | timer | in | out | packet | protocol | event | sync | ptx | prx | ppm | bdm | pim | prs | prt | pst | tcm | all) interface eth-trunk TRUNK-NUMBER** ▶ **no debug stp all**

8.1.8 配置举例

组网要求

现有四台支持MSTP协议的SC9600E系列交换机，分别为SC9600E_1、SC9600E_2、SC9600E_3、SC9600E_4。按照如下组网示意图连接，配置MSTP基本功能：

- SC9600E_1和SC9600E_3划分在同一个域内，域名为Domain1并创建实例1。
- SC9600E_2和SC9600E_4划分在另一个域内，域名为Domain2并创建实例1。

- SC9600E_1为CIST总根。
- Domain1内，SC9600E_1为CIST域根，为实例1的域根。且在SC9600E_1的GE1/0/1和GE1/0/2端口上配置根保护功能。
- Domain2内，SC9600E_2为CIST域根，SC9600E_4为实例1的域根。
- SC9600E_3和SC9600E_4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

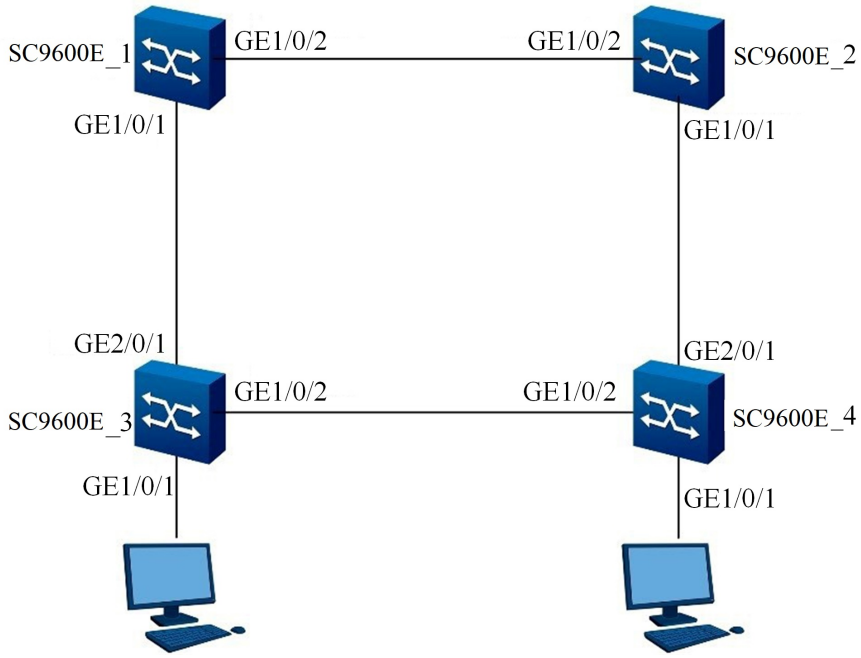


图 8-3 MSTP组网示意图

配置步骤

1. 配置SC9600E_1。

   # 配置SC9600E_1加入域Domain1。

```
SC9600E_1#configure
%Enter configuration commands.End with Ctrl+Z or command "quit" & "end"
SC9600E_1(config)#stp
SC9600E_1(config-stp)#stp mode mstp
SC9600E_1(config-stp)#stp config-name Domain1
SC9600E_1(config-stp)#stp instance 1 vlan 1-10
SC9600E_1(config-stp)#stp revision-level 1
```

配置SC9600E_1在实例0中的优先级为0以保证SC9600E_1作为CIST的总根。

```
SC9600E_1(config-stp)#stp priority 0
```

配置SC9600E_1在实例1中的优先级为0，保证SC9600E_1作为实例1的域根。

```
SC9600E_1(config-stp)#stp instance 1 priority 0
```

创建VLAN 2到20，并将SC9600E_1的端口10GE1/0/1和10GE1/0/2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。

```
SC9600E_1(config)#vlan 2-20
SC9600E_1(config)#interface 10gigaethernet1/0/1
SC9600E_1(config-10ge1/0/1)#port link-type trunk
SC9600E_1(config-10ge1/0/1)#port trunk allow-pass vlan 1-20
SC9600E_1(config-10ge1/0/1)#stp enable
SC9600E_1(config-10ge1/0/1)#stp root-guard enable
SC9600E_1(config-10ge1/0/1)#quit
SC9600E_1(config)#interface 10gigaethernet1/0/2
SC9600E_1(config-10ge1/0/2)#port link-type trunk
SC9600E_1(config-10ge1/0/2)#port trunk allow-pass vlan 1-20
SC9600E_1(config-10ge1/0/2)#stp enable
SC9600E_1(config-10ge1/0/2)# stp root-guard enable
SC9600E_1(config-10ge1/0/2)#quit
SC9600E_1(config)#
```

2. 配置SC9600E_2。

配置SC9600E_2加入域Domain2。

```
SC9600E_2#configure
%Enter configuration commands.End with Ctrl+Z or command "quit" & "end"
SC9600E_2(config)#stp
SC9600E_2(config-stp)#stp mode mstp
SC9600E_2(config-stp)#stp config-name Domain2
SC9600E_2(config-stp)#stp instance 1 vlan 1-10
SC9600E_2(config-stp)#stp revision-level 2
```

配置SC9600E_2在实例0中的优先级为4096以保证SC9600E_2作为CIST的总根。

```
SC9600E_2(config-stp)#stp priority 4096
```

创建VLAN 2到20，并将SC9600E_2的端口10GE1/0/1和10GE1/0/2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。

```
SC9600E_2(config)#vlan 2-20
SC9600E_2(config)#interface 10gigaethernet1/0/1
SC9600E_2(config-10ge1/0/1)#port link-type trunk
SC9600E_2(config-10ge1/0/1)#port trunk allow-pass vlan 1-20
```

```
SC9600E_2(config-10ge1/0/1)#stp enable
SC9600E_2(config-10ge1/0/1)#stp root-guard enable
SC9600E_2(config-10ge1/0/1)#quit
SC9600E_2(config)#interface 10gigaethernet1/0/2
SC9600E_2(config-10ge1/0/2)#port link-type trunk
SC9600E_2(config-10ge1/0/2)#port trunk allow-pass vlan 1-20
SC9600E_2(config-10ge1/0/2)#stp enable
SC9600E_2(config-10ge1/0/2)#stp root-guard enable
SC9600E_2(config-10ge1/0/2)#quit
SC9600E_2(config)#
```

3. 配置SC9600E_3。

配置SC9600E_3加入域Domain1。

```
SC9600E_3#configure
%Enter configuration commands.End with Ctrl+Z or command "quit" & "end"
SC9600E_3(config)#stp
SC9600E_3(config-stp)#stp mode mstp
SC9600E_3(config-stp)#stp config-name Domain1
SC9600E_3(config-stp)#stp instance 1 vlan 1-10
SC9600E_3(config-stp)#stp revision-level 1
```

启动BPDU保护功能。

```
SC9600E_3(config-stp)#stp bpdu-gurad enable
```

创建VLAN 2到20，并将SC9600E_3的端口10GE1/0/2和10GE2/0/1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。

```
SC9600E_3(config)#vlan 2-20
SC9600E_3(config)#interface 10gigaethernet2/0/1
SC9600E_3(config-10ge2/0/1)#port link-type trunk
SC9600E_3(config-10ge2/0/1)#port trunk allow-pass vlan 1-20
SC9600E_3(config-10ge2/0/1)#stp enable
SC9600E_3(config-ge2/0/1)#quit
SC9600E_3(config)#interface 10gigaethernet1/0/2
SC9600E_3(config-10ge1/0/2)#port link-type trunk
SC9600E_3(config-10ge1/0/2)#port trunk allow-pass vlan 1-20
SC9600E_3(config-10ge1/0/2)#stp enable
SC9600E_3(config-10ge1/0/2)#quit
SC9600E_3(config)#interface 10gigaethernet1/0/1
SC9600E_3(config-10ge1/0/1)#stp enable
SC9600E_3(config-10ge1/0/1)#stp edged-port enable
SC9600E_3(config-10ge1/0/1)#port hybrid pvid 20
SC9600E_3(config-10ge1/0/1)#port hybrid vlan 20 untagged
SC9600E_3(config-10ge1/0/1)#quit
```

```
SC9600E_3(config)#
```

4. 配置SC9600E_4。

配置SC9600E_4加入域Domain2。

```
SC9600E_4#configure
%Enter configuration commands.End with Ctrl+Z or command "quit" & "end"
SC9600E_4(config)#stp
SC9600E_4(config-stp)#stp mode mstp
SC9600E_4(config-stp)#stp config-name Domain2
SC9600E_4(config-stp)#stp instance 1 vlan 1-10
SC9600E_4(config-stp)#stp revision-level 2
```

配置SC9600E_4在实例1中的优先级为0，保证SC9600E_4作为实例1的域根。

```
SC9600E_4(config-stp)#stp instance 1 priority 0
```

启动BPDU保护功能。

```
SC9600E_4(config-stp)#stp bpdu-gurad enable
```

创建VLAN 2到20，并将SC9600E_4的端口10GE1/0/2和10GE2/0/1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。

```
SC9600E_4(config)#vlan 2-20
SC9600E_4(config)#interface 10gigaethernet2/0/1
SC9600E_4(config-10ge2/0/1)#port link-type trunk
SC9600E_4(config-10ge2/0/1)#port trunk allow-pass vlan 1-20
SC9600E_4(config-10ge2/0/1)#stp enable
SC9600E_4(config-10ge2/0/1)#quit
SC9600E_4(config)#interface 10gigaethernet1/0/2
SC9600E_4(config-10ge1/0/2)#port link-type trunk
SC9600E_4(config-10ge1/0/2)#port trunk allow-pass vlan 1-20
SC9600E_4(config-10ge1/0/2)#stp enable
SC9600E_4(config-10ge1/0/2)#quit
SC9600E_4(config)#interface 10gigaethernet1/0/1
SC9600E_4(config-10ge1/0/1)#stp enable
SC9600E_4(config-10ge1/0/1)#stp edged-port enable
SC9600E_4(config-10ge1/0/1)#port hybrid pvid 10
SC9600E_4(config-10ge1/0/1)#port hybrid vlan 10 untagged
SC9600E_4(config-10ge1/0/1)#quit
SC9600E_4(config)#
```

9 设备管理配置

本章介绍了SC9600E系列数据中心交换机设备管理的基本内容、配置过程和配置举例。

9.1 设备硬件配置

9.1.1 硬件配置概述

SC9600E系列数据中心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。

9.1.2 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：设置CPU监控及告警上报功能、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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
设置CPU监控功能及CPU告警上报功能	1. 进入全局配置视图； 2. 执行命令**cpu monitor (enable | disable)**使能或去使能CPU监控功能； 3. 执行命令**cpu (SLOT-ID / CPU-NUMBER | all) snmp-trap (enable | disable)**使能或去使能CPU上报告警功能。
设置CPU使用率的上限阈值和下限阈值	1. 进入全局配置视图； 2. 执行命令**cpu (CPU-NUMBER | all) low-threshold LOW-THRESHOLD high-threshold HIGH-THRESHOLD**设置CPU使用率的上下限阈值。
清除设备CPU使用率的历史最大值	1. 进入全局配置视图； 2. 执行命令**cpu (SLOT-ID / CPU-NUMBER | all) maxusage reset**清除设备CPU使用率的历史最大值。
清除设备CPU过载状态的历史信息	1. 进入全局配置视图； 2. 执行命令**reset cpu (SLOT-ID / CPU-NUMBER | all) monitor history**清除设备CPU过载状态的历史信息。
查看设备CPU过载状态的历史信息	1. 进入全局配置视图； 2. 执行命令**show cpu (SLOT-ID / CPU-NUMBER | all) monitor history**查看设备CPU过载状态的历史信息。
查看配置结果	1. 进入普通用户视图、特权用户视图、全局配置视图； 2. 执行命令**show cpu**查看CPU使用情况和配置信息； 3. 执行命令**show cpu config**查看设备CPU当前的配置文件信息； 4. 执行命令**show cpu statistic**查看CPU占用率的统计信息。

9.1.3 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
设置风扇监控功能及风扇告警上报功能	1. 进入全局配置视图； 2. 执行命令**fanctrl monitor (enable | disable)**使能或去使能风扇监控功能； 3. 执行命令**fanctrl (FAN-NUMBER | all)snmp- trap (enable | disable)**使能或去使能风扇上报告警功能。
设置风扇转速阈值	1. 进入全局配置视图； 2. 执行命令**fanctrl (FAN-NUMBER | all) low-threshold LOW-THRESHOLD high-threshold HIGH-THRESHOLD**设置风扇转速阈值。
查看配置结果	1. 进入特权用户视图、全局配置视图； 2. 执行命令**show fan**查看风扇状态和配置信息。

9.1.4 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
设置内存监控功能及内存告警上报功能	1. 进入全局配置视图； 2. 执行命令**memory monitor (enable | disable)**使能或去使能内存监控功能； 3. 执行命令**memory (SLOT-ID / MEMORY-POOL-NUMBER) snmp- trap (enable | disable)**使能或去使能内存上报告警功能。
设置内存使用率的上限阈值和下限阈值	1. 进入全局配置视图； 2. 执行命令**memory (SLOT-ID / MEMORY-POOL-NUMBER) low-threshold (LOW-THRESHOLD | default) high-threshold (HIGH-THRESHOLD | default)**设置内存上下限阈值。
查看配置结果	1. 进入普通用户视图、特权用户视图、全局配置视图； 2. 执行命令**show memory pool**查看当前所有在位卡的内存使用情况。

9.1.5 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
设置温度监控功能及温度告警上报功能	1. 进入全局配置视图； 2. 执行命令**temperature monitor (enable | disable)**使能或去使能温度监控功能； 3. 执行命令**temperature (SLOT-ID / CARD-NUMBER / TEMPERATURE-NUMBER | all) trap (enable | disable)**使能或去使能温度上报告警功能。
查看配置结果	1. 进入普通用户视图、特权用户视图、全局配置视图； 2. 执行命令**show temperature**查看设备风扇所有单板的温度信息； 3. 执行命令**show temperature config**查看设备温度的配置文件信息。
配置设备温度的阈值	1. 进入全局配置视图； 2. 执行命令**temperature (SLOT-ID / CARD-NUMBER / TEMPERATURE-NUMBER | all) low-threshold (LOW-THRESHOLD | default) high-threshold (HIGH-THRESHOLD | default)**配置设备温度的阈值。

9.1.6 查看设备 CPU 占用率

目的

用户可以使用该命令显示设备部件类型及系统状态信息。

执行步骤，具体参见下表，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
显示当前CPU利用率	1. 进入普通用户视图； 2. 执行命令**show cpu statistic**。

9.1.7 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。

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
查看版本信息	1. 进入特权用户视图、全局配置视图； 2. 执行命令**show version**查看版本信息。
查看电源状态	1. 进入普通用户视图； 2. 执行命令**show power**查看电源状态。
清除设备Memory过载状态的历史信息	1. 进入全局配置视图； 2. 执行命令**reset memory (SLOT-ID / MEMORY-NUMBER) monitor history**清除设备Memory过载状态的历史信息。
查看设备Memory过载状态的历史信息	1. 进入全局配置视图； 2. 执行命令**show memory (SLOT-ID / MEMORY-NUMBER) monitor history**查看设备Memory过载状态的历史信息。

9.2 镜像配置

9.2.1 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。

SC9600E支持Trunk的镜像、支持镜像到Trunk。

SC9600E的观察端口最多可以设置为4个。

SC9600E支持将多个端口的报文镜像到一个观察端口。

SC9600E整台设备最多可以同时运用3个观察口，若同一端口既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。

SC9600E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。

9.2.2 镜像分类

SC9600E系列数据中心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。

提示：

- **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。

提示：

同端口镜像一样，流镜像也分为本地流镜像和远程流镜像。

9.2.3 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置本地端口镜像	1. 进入全局配置视图； 2. 执行如下命令创建本地镜像组及其观察端口： ▶ **mirror group GROUPNUM (ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 40gigaethernet) INTERFACE-NUMBER** ▶ **mirror group GROUPNUM eth-trunk TRUNK-NUMBER** 3. 进入接口配置视图、接口组配置视图； 4. 执行命令**mirror (ingress | egress | both) group GROUPNUM**在镜像源端口设置该接口的镜像功能。
取消端口本地镜像功能并删除本地镜像组及其观察端口	1. 进入接口配置视图、接口组配置视图； 2. 执行命令**no mirror (ingress | egress | both) group GROUPNUM**取消端口本地镜像功能； 3. 进入全局配置视图； 4. 执行命令**no mirror group [GROUPNUM]** 删除本地镜像组及其观察端口的配置。
查看配置结果	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（以太网接口、eth-trunk接口）、VLAN配置视图、接口组配置视图； 2. 执行命令**show mirror config**查看镜像功能的配置文件信息； 3. 执行命令**show mirror group**查看镜像组信息； 4. 执行命令**show mirror interface**查看镜像端口信息。

9.2.4 配置流镜像

目的

当用户需要监控或分析流经设备并且具有某些特性的报文，可以配置流镜像功能。

提示：

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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置本地流镜像	1. 进入全局配置视图； 2. 执行如下命令创建本地镜像组及其观察端口： ▶ **mirror group GROUPNUM (ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 40gigaethernet) INTERFACE-NUMBER** ▶ **mirror group GROUPNUM eth-trunk TRUNK-NUMBER** 3. 执行命令**filter-list ACL-NUMBER [name FILTER-NAME]**创建一条ACL（访问控制列表），并进入ACL视图； 4. 请根据实际应用情形，参考ACL 配置，选择合适的流分类规则； 5. 执行命令**filter RULE-NUMBER action mirror group GROUP-NUMBER**配置流镜像处理动作； 6. 执行命令**quit**或**exit**退出ACL视图到全局配置视图； 7. 进入接口配置视图、接口组配置视图、VLAN配置视图； 8. 执行命令**filter-list-(l2 | ipv4 | ipv6 | hybrid) (in | out) ACL-NAME**将ACL应用到该物理端口或trunk接口； 9. 执行命令**mirror (ingress | egress | both) group GROUP-LIST**在镜像源端口设置该接口的镜像功能。
取消流镜像功能并删除本地镜像组及其观察端口	1. 进入接口配置视图、接口组配置视图； 2. 执行命令**no filter-list-(l2 | ipv4 | ipv6 | hybrid) (in | out)**，然后执行命令**no mirror (ingress | egress | both) GROUP-LIST**取消端口本地镜像功能； 3. 进入全局配置视图； 4. 执行命令**no mirror group [GROUPNUM]**删除本地镜像组及其观察端口的配置。
查看配置结果	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（以太网接口、trunk接口）、VLAN配置视图、接口组配置视图； 2. 执行命令**show mirror config**查看镜像功能的配置文件信息； 3. 执行命令**show mirror group**查看镜像组信息； 4. 执行命令**show mirror interface**查看镜像端口信息； 5. 执行命令**show filter-list config**查看镜像规则。

9.2.5 配置举例

9.2.5.1 配置本地端口镜像举例

组网要求

某集团公司部门1和部门2分别通过接口10GE1/0/1、10GE1/0/2连接到交换机SC9600E。数据监控设备通过接口10GE1/0/3连接到交换机SC9600E。要求使用本地端口镜像功能来实现数据监控设备对部门1和部门2发送到交换机SC9600E上的报文的监控，如图 9-1所示。

组网图

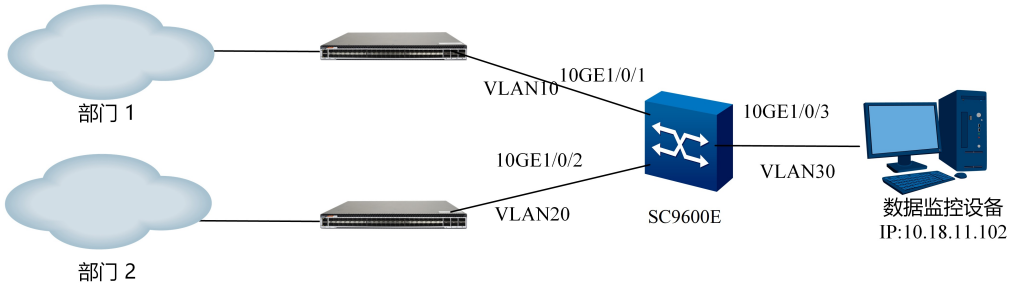


图 9-1 本地端口镜像配置组网图

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10GE1/0/1、10GE1/0/2、10GE1/0/3分别加入VLAN10、VLAN20、VLAN30。

```
SC9600E#configure
SC9600E(config)#vlan 10
SC9600E(config-vlan-10)#quit
SC9600E(config)#vlan 20
SC9600E(config-vlan-20)#quit
SC9600E(config)#vlan 30
SC9600E(config-vlan-30)#quit
SC9600E(config)#interface 10gigaethernet 1/0/1
SC9600E(config-10ge1/0/1)#port link-type trunk
SC9600E(config-10ge1/0/1)#port trunk pvid 10
SC9600E(config-10ge1/0/1)#port trunk allow-pass vlan 10
SC9600E(config-10ge1/0/1)#quit
SC9600E(config)#interface 10gigaethernet 1/0/2
```

```
SC9600E(config-10ge1/0/2)# port link-type trunk
SC9600E(config-10ge1/0/2)#port trunk pvid 20
SC9600E(config-10ge1/0/2)#port trunk allow-pass vlan 20
SC9600E(config-10ge1/0/2)#quit
SC9600E(config)#interface 10gigaethernet 1/0/3
SC9600E(config-10ge1/0/3)# port link-type trunk
SC9600E(config-10ge1/0/3)#port trunk allow-pass vlan 10,20,30
SC9600E(config-10ge1/0/3)#quit
SC9600E(config)#interface vlan 30
SC9600E(config-vlan-3)#ip address 10.18.11.1/24
SC9600E(config-vlan-3)#quit
SC9600E(config)#
```

2. 创建本地镜像组及其观察端口。

   #在SC9600E上创建本地镜像组1及配置其观察端口为10GE1/0/3。

```
SC9600E(config)#mirror group 1 10gigaethernet 1/0/3
```

3. 在镜像源端口设置该端口的镜像功能。

   #在SC9600E上配置端口10GE1/0/1和10GE1/0/2为镜像源端口，以监控部门1和部门2发送的数据报文。

```
SC9600E(config)#interface 10gigaethernet 1/0/1
SC9600E(config-10ge1/0/1)#mirror ingress group 1
SC9600E(config-10ge1/0/1)#quit
SC9600E(config)#interface 10gigaethernet 1/0/2
SC9600E(config-10ge1/0/2)#mirror ingress group 1
SC9600E(config-10ge1/0/2)#quit
SC9600E(config)#
```

4. 配置结束。

9.2.5.2 配置本地流镜像举例

组网要求

某集团公司部门1和部门2分别通过接口10GE1/0/1、10GE1/0/2连接到交换机SC9600E。数据监控设备通过接口10GE1/0/3连接到交换机SC9600E。要求使用本地流镜像功能来实现数据监控设备对部门1和部门2发送到交换机SC9600E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，如图 9-2所示。

组网图

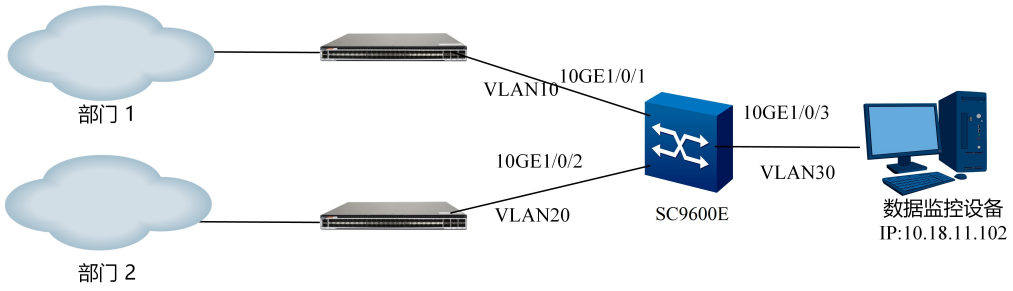


图 9-2　本地流镜像配置组网图

配置步骤

1. 配置各接口，使任意两个部门都能与数据监控设备互通。

   #创建VLAN10、VLAN20、VLAN30，并将端口10GE1/0/1、10GE1/0/2、10GE1/0/3分别加入VLAN10、VLAN20、VLAN30。

```
SC9600E#configure
SC9600E(config)#vlan 10
SC9600E(config-vlan-10)#quit
SC9600E(config)#vlan 20
SC9600E(config-vlan-20)#quit
SC9600E(config)#vlan 30
SC9600E(config-vlan-30)#quit
SC9600E(config)#interface 10gigaethernet 1/0/1
SC9600E(config-10ge1/0/1)#port link-type trunk
SC9600E(config-10ge1/0/1)#port trunk pvid 10
SC9600E(config-10ge1/0/1)#port trunk allow-pass vlan 10
SC9600E(config-10ge1/0/1)#quit
SC9600E(config)#interface 10gigaethernet 1/0/2
SC9600E(config-10ge1/0/2)#port link-type trunk
SC9600E(config-10ge1/0/2)#port trunk pvid 20
SC9600E(config-10ge1/0/2)#port trunk allow-pass vlan 20
SC9600E(config-10ge1/0/2)#quit
SC9600E(config)#interface 10gigaethernet 1/0/3
SC9600E(config-10ge1/0/3)#port link-type trunk
SC9600E(config-10ge1/0/3)#port trunk allow-pass vlan 10,20,30
SC9600E(config-10ge1/0/3)#quit
SC9600E(config)#interface vlan 30
SC9600E(config-vlan-3)#ip address 10.18.11.1/24
SC9600E(config-vlan-3)#quit
SC9600E(config)#
```

2. 创建本地镜像组及其观察端口。

#在SC9600E上创建本地镜像组1及配置其观察端口为10GE1/0/3。

```
SC9600E(config)#mirror group 1 10gigaethernet 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SC9600E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。

```
SC9600E(config)#filter-list 100
SC9600E(configure-filter-l2-100)#filter 1 mac any 00:00:00:01:02:03/48
SC9600E(configure-filter-l2-100)#filter 1 action mirror group 1
SC9600E(configure-filter-l2-100)#quit
SC9600E(config)#interface 10gigaethernet 1/0/1
SC9600E(config-10ge1/0/1)#filter-list-l2 in 100
SC9600E(config-ge1/0/1)#quit
SC9600E(config)#interface 10gigaethernet 1/0/2
SC9600E(config-10ge1/0/2)#filter-list-l2 in 100
SC9600E(config-10ge1/0/2)#quit
SC9600E(config)#
```

4. 配置结束。

9.3 日志管理配置

9.3.1 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4000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。

9.3.2 配置日志管理

9.3.2.1 启动或取消日志记录功能

目的

本操作用于启动或取消交换机日志记录功能。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
启动系统记录日志功能	1. 进入全局配置视图； 2. 执行命令**logging on**。
取消系统记录日志功能	1. 进入全局配置视图； 2. 执行命令**no logging on**。

9.3.2.2 显示或清除日志信息

目的

本操作用于显示或清除日志的信息。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
显示日志缓冲区或告警日志缓冲区中指定模块的日志信息	1. 进入普通用户视图； 2. 执行命令**show (logbuffer | trapbuffer) module (aaa | acl | arp | arp-probe | arp-antiattack | bfd | bgp | cli | counter | cpu | cpu-defend | dcp | ddm | default | devcomm | device | deviceme | dhcp | dhcp-client | dhcpv6 | dhcp-snooping | did | diffserv | dos-antiattack | dxs | evpn | fan | ha | hwarp | hwroute | hwvp | hwvrf | hwbd | ipsg | icmp | icmp6 | ifm | if-ref | igmp-snooping | ip | ipv6 | isis | l3vpn | lacp | link-flap | lldp | llt | mam | memory | mirror | mlag | mld-snooping | mlink | ndp | ntp | ospf | ospf6 | patch | port-isolate | power | policy-route | rawip | rawip6 | route | route-policy | scheduleprofile | slot | snmp | ssh | stg | storm-control | stp | tcp | tcp6 | temperature | time-range | udp | udp6 | udr | uinetsck | vlan-mapping | vlan-stacking | voltage | vrrp | vxlan)**。
清空日志缓冲区	1. 进入全局配置视图； 2. 执行命令**clear logging (logbuffer | trapbuffer)**。

目的	步骤
显示各模块的详细信息	1. 进入普通用户视图； 2. 执行如下命令： ▶ **show logging source** ▶ **show logging source (aaa | acl | arp | arp-probe | arp-antiattack | bfd | bgp | cli | counter | cpu | cpu-defend | dcp | ddm | default | devcomm | device | deviceme | dhcp | dhcp-client | dhcpv6 | dhcp-snooping | did | diffserv | dos-antiattack | dxs | evpn | fan | ha | hwarp | hwroute | hwvp | hwvrf | hwbd | ipsg | icmp | icmp6 | ifm | if-ref | igmp-snooping | ip | ipv6 | isis | l3vpn | lacp | link-flap | lldp | llt | mam | memory | mirror | mlag | mld-snooping | mlink | ndp | ntp | ospf | ospf6 | patch | port-isolate | power | policy-route | rawip | rawip6 | route | route-policy | scheduleprofile | slot | snmp | ssh | stg | storm-control | stp | tcp | tcp6 | temperature | time-range | udp | udp6 | udr | uinetsck | vlan-mapping | vlan-stacking | voltage | vrrp | vxlan)**
清除指定模块的日志信息	1. 进入全局配置视图； 2. 执行命令**clear logging source (aaa | acl | arp | arp-probe | arp-antiattack | bfd | bgp | cli | counter | cpu | cpu-defend | dcp | ddm | default | devcomm | device | dhcp | dhcp-client | dhcpv6 | dhcp-snooping | did | diffserv | dos-antiattack | dxs | evpn | fan | ha | hwarp | hwroute | hwvp | hwvrf | hwbd | ipsg | icmp | icmp6 | ifm | if-ref | igmp-snooping | ip | ipv6 | isis | l3vpn | lacp | link-flap | lldp | llt | mam | memory | mirror | mlag | mld-snooping | mlink | ndp | ntp | ospf | ospf6 | patch | port-isolate | power | policy-route | rawip | rawip6 | route | route-policy | scheduleprofile | slot | snmp | ssh | stg | storm-control | stp | tcp | tcp6 | temperature | time-range | udp | udp6 | udr | uinetsck | vlan-mapping | vlan-stacking | voltage | vrrp | vxlan)**。

9.3.2.3 配置action相关信息

目的

本操作用于配置action相关信息。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置指定模块、指定action、指定类型日志的优先级门槛	1. 进入全局配置视图； 2. 执行如下命令： **logging source (aaa | acl | arp | arp-probe | arp-antiattack | bfd | bgp | cli | counter | cpu | cpu-defend | dcp | ddm | default | devcomm | device | deviceme | dhcp | dhcp-client | dhcpv6 | dhcp-snooping | did | diffserv | dos-antiattack | dxs | evpn | fan | ha | hwarp | hwroute | hwvp | hwvrf | hwbd | ipsg | icmp | icmp6 | ifm | if-ref | igmp-snooping | ip | ipv6 | isis | l3vpn | lacp | link-flap | lldp | llt | mam | memory | mirror | mlag | mld-snooping | mlink | ndp | ntp | ospf | ospf6 | patch | port-isolate | power | policy-route | rawip | rawip6 | route | route-policy | scheduleprofile | slot | snmp | ssh | stg | storm-control | stp | tcp | tcp6 | temperature | time-range | udp | udp6 | udr | uinetsck | vlan-mapping | vlan-stacking | voltage | vrrp | vxlan) action (console | monitor | logfile | logbuffer | trap | trapbuffer | syslog | smtp) (log | debug | trap) level (emergencies | alert | critical | error | warning | notification | information | debugging | default)**
	logging source (aaa | acl | arp | arp-probe | arp-antiattack | bfd | bgp | cli | counter | cpu | cpu-defend | dcp | ddm | default | devcomm | device | deviceme | dhcp | dhcp-client | dhcpv6 | dhcp-snooping | did | diffserv | dos-antiattack | dxs | evpn | fan | ha | hwarp | hwroute | hwvp | hwvrf | hwbd | ipsg | icmp | icmp6 | ifm | if-ref | igmp-snooping | ip | ipv6 | isis | l3vpn | lacp | link-flap | lldp | llt | mam | memory | mirror | mlag | mld-snooping | mlink | ndp | ntp | ospf | ospf6 | patch | port-isolate | power | policy-route | rawip | rawip6 | route | route-policy | scheduleprofile | slot | snmp | ssh | stg | storm-control | stp | tcp | tcp6 | temperature | time-range | udp | udp6 | udr | uinetsck | vlan-mapping | vlan-stacking | voltage | vrrp | vxlan) action (console | monitor | logfile | logbuffer | trap | trapbuffer | syslog | smtp) (log | debug | trap) state (enable | disable | default)

目的	步骤
	logging source (aaa | acl | arp | arp-probe | arp-antiattack | bfd | bgp | cli | counter | cpu | cpu-defend | dcp | ddm | default | devcomm | device | deviceme | dhcp | dhcp-client | dhcpv6 | dhcp-snooping | did | diffserv | dos-antiattack | dxs | evpn | fan | ha | hwarp | hwroute | hwvp | hwvrf | hwbd | ipsg | icmp | icmp6 | ifm | if-ref | igmp-snooping | ip | ipv6 | isis | l3vpn | lacp | link-flap | lldp | llt | mam | memory | mirror | mlag | mld-snooping | mlink | ndp | ntp | ospf | ospf6 | patch | port-isolate | power | policy-route | rawip | rawip6 | route | route-policy | scheduleprofile | slot | snmp | ssh | stg | storm-control | stp | tcp | tcp6 | temperature | time-range | udp | udp6 | udr | uinetsck | vlan-mapping | vlan-stacking | voltage | vrrp | vxlan) action (console | monitor | logfile | logbuffer | trap | trapbuffer | syslog | smtp) (log | debug | trap) state (enable | disable | default) level (emergencies | alert | critical | error | warning | notification | information | debugging | default)
取消指定模块指定动作的日志的配置	1. 进入全局配置视图； 2. 执行命令**no logging source (aaa | acl | arp | arp-probe | arp-antiattack | bfd | bgp | cli | counter | cpu | cpu-defend | dcp | ddm | default | devcomm | device | deviceme | dhcp | dhcp-client | dhcpv6 | dhcp-snooping | did | diffserv | dos-antiattack | dxs | evpn | fan | ha | hwarp | hwroute | hwvp | hwvrf | hwbd | ipsg | icmp | icmp6 | ifm | if-ref | igmp-snooping | ip | ipv6 | isis | l3vpn | lacp | link-flap | lldp | llt | mam | memory | mirror | mlag | mld-snooping | mlink | ndp | ntp | ospf | ospf6 | patch | port-isolate | power | policy-route | rawip | rawip6 | route | route-policy | scheduleprofile | slot | snmp | ssh | stg | storm-control | stp | tcp | tcp6 | temperature | time-range | udp | udp6 | udr | uinetsck | vlan-mapping | vlan-stacking | voltage | vrrp | vxlan) action (console | monitor | logfile | logbuffer | trap | trapbuffer | syslog | smtp)**。

9.3.2.4 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置syslog服务器	1. 进入全局配置视图； 2. 执行命令**syslog server IPV4-ADDRESS [SERVER-PORT]**。
删除syslog服务器	1. 进入全局配置视图； 2. 执行命令**no syslog server IPV4-ADDRESS**。

9.3.2.5 配置日志文件

目的

本操作用于配置日志文件的大小和数量。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置各个模块日志文件的大小	1. 进入全局配置视图； 2. 执行命令**logging source (aaa | acl | arp | arp-probe | arp-antiattack | bfd | bgp | cli | counter | cpu | cpu-defend | dcp | ddm | default | devcomm | device | deviceme | dhcp | dhcp-client | dhcpv6 | dhcp-snooping | did | diffserv | dos-antiattack | dxs | evpn | fan | ha | hwarp | hwroute | hwvp | hwvrf | hwbd | ipsg | icmp | icmp6 | ifm | if-ref | igmp-snooping | ip | ipv6 | isis | l3vpn | lacp | link-flap | lldp | llt | mam | memory | mirror | mlag | mld-snooping | mlink | ndp | ntp | ospf | ospf6 | patch | port-isolate | power | policy-route | rawip | rawip6 | route | route-policy | scheduleprofile | slot | snmp | ssh | stg | storm-control | stp | tcp | tcp6 | temperature | time-range | udp | udp6 | udr | uinetsck | vlan-mapping | vlan-stacking | voltage | vrrp | vxlan) logfile size kbytes (FILE_SIZE | default)**。
配置各个模块日志文件的最大个数	1. 进入全局配置视图； 2. 执行命令**logging source (aaa | acl | arp | arp-probe | arp-antiattack | bfd | bgp | cli | counter | cpu | cpu-defend | dcp | ddm | default | devcomm | device | deviceme | dhcp | dhcp-client | dhcpv6 | dhcp-snooping | did | diffserv | dos-antiattack | dxs | evpn | fan | ha | hwarp | hwroute | hwvp | hwvrf | hwbd | ipsg | icmp | icmp6 | ifm | if-ref | igmp-snooping | ip | ipv6 | isis | l3vpn | lacp | link-flap | lldp | llt | mam | memory | mirror | mlag | mld-snooping | mlink | ndp | ntp | ospf | ospf6 | patch | port-isolate | power | policy-route | rawip | rawip6 | route | route-policy | scheduleprofile | slot | snmp | ssh | stg | storm-control | stp | tcp | tcp6 | temperature | time-range | udp | udp6 | udr | uinetsck | vlan-mapping | vlan-stacking | voltage | vrrp | vxlan) max-number (FILE_NUM | default)**。

9.3.2.6 保存日志文件

目的

本操作用于配置日志文件的保存。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
手动保存日志文件	1. 进入全局配置视图； 2. 执行命令**save logging logfile**。

9.3.2.7 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
查看系统日志的信息	1. 进入普通用户视图、特权用户视图、全局配置视图； 2. 执行命令**show logging**。
查看系统日志action的具体内容	1. 进入普通用户视图、特权用户视图、全局配置视图； 2. 执行如下命令： ▶ **show logging action** ▶ **show logging action（console | monitor | logfile | logbuffer | trap | trapbuffer | syslog | smtp）**
查看系统日志统计信息	1. 进入普通用户视图、特权用户视图、全局配置视图； 2. 执行命令**show logging statistic**。

目的	步骤
显示不同模块的日志文件日志信息	1. 进入普通用户视图； 2. 执行命令**show logfile FILE-NAME module (aaa | acl | arp | arp-probe | arp-antiattack | bfd | bgp | cli | counter | cpu | cpu-defend | dcp | ddm | default | devcomm | device | deviceme | dhcp | dhcp-client | dhcpv6 | dhcp-snooping | did | diffserv | dos-antiattack | dxs | evpn | fan | ha | hwarp | hwroute | hwvp | hwvrf | hwbd | ipsg | icmp | icmp6 | ifm | if-ref | igmp-snooping | ip | ipv6 | isis | l3vpn | lacp | link-flap | lldp | llt | mam | memory | mirror | mlag | mld-snooping | mlink | ndp | ntp | ospf | ospf6 | patch | port-isolate | power | policy-route | rawip | rawip6 | route | route-policy | scheduleprofile | slot | snmp | ssh | stg | storm-control | stp | tcp | tcp6 | temperature | time-range | udp | udp6 | udr | uinetsck | vlan-mapping | vlan-stacking | voltage | vrrp | vxlan)**查看不同模块的日志文件的日志信息。
显示syslog服务器配置文件信息	1. 进入普通用户视图、特权用户视图、全局配置视图； 2. 执行命令**show syslog config**。
显示syslog服务器信息	1. 进入普通用户视图、特权用户视图、全局配置视图； 2. 执行命令**show syslog server**。
查看Log缓冲区记录的信息	1. 进入普通用户视图、特权用户视图、全局配置视图； 2. 执行命令**show logbuffer**。

9.4 DDM 配置

9.4.1 DDM 概述

在光链路中，定位故障的发生位置对业务的快速恢复至关重要。利用智能化的光模块DDM（Digital Diagnostic Monitoring，数字诊断监控），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。

9.4.2 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
使能或去使能获取光模块参数功能	1. 进入全局配置视图； 2. 执行命令**ddm (enable | disable)**。
使能或去使能获取光模块时间间隔	1. 进入全局配置视图； 2. 执行命令**ddm interval (VALUE | default)**。
配置因为接口光功率过低，状态变为down后的自动恢复link up的时间	1. 进入全局配置视图； 2. 执行命令**error-down auto-recovery cause transceiver-power-low interval INTERVAL**。
配置端口光模块的偏置电流高低阈值	1. 进入全局配置视图； 2. 进入接口配置视图； 3. 执行命令**laser bias-current-threshold LOW-THRESHOLD HIGH-THRESHOLD**。
配置自动获取端口光模块的偏置电流高低阈值	1. 进入全局配置视图； 2. 进入接口配置视图； 3. 执行命令**laser bias-current-threshold auto**。
配置端口光模块的接收光功率高低阈值	1. 进入全局配置视图； 2. 进入接口配置视图； 3. 执行命令**laser rx-power-threshold RX-LOW-THRESHOLD RX-HIGH-THRESHOLD**。
配置自动获取端口光模块的接收光功率高低阈值	1. 进入全局配置视图； 2. 进入接口配置视图； 3. 执行命令**laser rx-power-threshold auto**。
配置端口光模块的温度高低阈值	1. 进入全局配置视图； 2. 进入接口配置视图； 3. 执行命令**laser temperature-threshold LOW-THRESHOLD HIGH-THRESHOLD**。
配置自动获取端口光模块的温度高低阈值	1. 进入全局配置视图； 2. 进入接口配置视图； 3. 执行命令**laser temperature-threshold auto**。

目的	步骤
使能或去使能光模块上报Trap功能	1. 进入全局配置视图； 2. 进入接口配置视图； 3. 执行命令**laser snmp-trap** 。
配置端口光模块的发送光功率高低阈值	1. 进入全局配置视图； 2. 进入接口配置视图； 3. 执行命令**laser tx-power-threshold TX-LOW-THRESHOLD TX-HIGH-THRESHOLD**。
配置自动获取本端口光模块的发送光功率高低阈值	1. 进入全局配置视图； 2. 进入接口配置视图； 3. 执行命令**laser tx-power-threshold auto**。
配置端口光模块的电压高低阈值	1. 进入全局配置视图； 2. 进入接口配置视图； 3. 执行命令**laser voltage-threshold LOW-THRESHOLD HIGH-THRESHOLD**。
配置自动获取端口光模块的电压高低阈值	1. 进入全局配置视图； 2. 进入接口配置视图； 3. 执行命令**laser voltage-threshold auto**。
配置使能、去使能指定以太网光接口由于接收光功率过低触发Error-Down功能	1. 进入全局配置视图； 2. 进入接口配置视图； 3. 执行命令**transceiver power low trigger error-down (enable | disable)**。
配置DDM上报轮询间隔时间	1. 进入全局配置视图； 2. 执行命令**ddm report interval (VALUE | default)**。

9.4.3 维护及调试

目的

当DDM功能不正常，需要进行查看、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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
查看所有视图下配置的DDM信息，包括电流、电压等的高低门限值	1. 进入普通用户视图； 2. 执行命令**show ddm config**。
查看所有插入了光模块的端口的模块常规硬件信息	1. 进入普通用户视图； 2. 执行命令**show laser hardware**。
查看所有插入了光模块的端口的模块详细硬件信息	1. 进入普通用户视图； 2. 执行命令**show laser hardware detailed**。
查看某个具体光模块端口的模块常规硬件信息	1. 进入普通用户视图； 2. 执行命令**show laser hardware (ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 40gigaethernet) INTERFACE-NUMBER**。
查看某个具体光模块的端口的模块详细硬件信息	1. 进入普通用户视图； 2. 执行命令**show laser hardware (ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 40gigaethernet) INTERFACE-NUMBER detailed**。
打开或关闭DDM调试功能	1. 进入特权用户视图； 2. 执行命令**debug ddm (poll | event | all)**或**no debug ddm (poll | event | all)**。

9.5 HA 配置

9.5.1 HA 介绍

HA（High Availability）高可用的缩写，用于表示高可用集群。高可用性的系统设计包括硬件系统和软件系统的高可用性。

- 硬件外围系统的高可用性包括机框、风扇、电源等设备的高可用性。
- 软件系统的高可用性包括控制卡和线路卡上软件的备份设计、主备倒换、故障检测、系统容错、在线升级和无中断的业务转发等。

9.5.2 配置主备倒换

目的

在支持双主控热备份的设备软件升级或者系统维护时，用户可以手动进行主用主控板和备用主控板的倒换。执行主备倒换后，设备正在运行的主用主控板将重新启动，且启动后成为备用主控板；设备正在运行的备用主控板将成为主用主控板。通过配置主备倒换，可以实现主用主控板和备用主控板之间的冗余备份。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
在进行主备倒换之前，需要确认设备主控板是否满足主备倒换的条件	1. 进入普通用户视图； 2. 执行命令**show ha global**，查看HA的协商状态； 3. 执行命令**show ha status**，查看MAC管理模块、路由模块的稳定状态。

9.5.3 维护及调试

目的

当HA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HA的运行状态	1. 进入普通用户视图； 2. 执行命令**show ha global**，查看HA的运行状态。
显示MAC管理模块、路由协议模块的运行状态	1. 进入普通用户视图； 2. 执行命令**show ha status**，查看MAC管理模块、路由模块的稳定状态。

9.5.4 配置举例

配置思路

配置主备倒换的配置思路如下：

1. 查看设备的运行状态；
2. 配置主备倒换。

数据准备

要完成该配置举例，设备必须处于稳定运行状态。

配置步骤

1. 显示HA的运行状态。

```
SC9600E#show ha global
SC9600E#
```

2. 查看其他协议的运行状态。

```
SC9600E#show ha status
SC9600E#
```

9.6 系统及指定线卡补丁配置

9.6.1 系统及指定线卡补丁概述

本设备支持系统补丁和给指定槽位的线卡打补丁。

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。本设备支持3种补丁状态：LOAD、ACTIVE、DEACTIVE。

9.6.2 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
在主用/备用主控上加载补丁包中与单板匹配的补丁	1. 进入全局配置视图； 2. 执行命令**patch PATCH-NUMBER load file FILENAME slot SLOT-ID**在主用/备用主控上加载补丁包中与单板匹配的补丁。
查看配置结果	1. 保持当前特权用户视图； 2. 执行命令**show patch information**查看系统当前所有补丁信息。

9.6.3 配置激活补丁

准备

激活补丁之前，必须先进行加载单板补丁操作。

背景信息

目前的补丁功能可针对主控和线卡上软件打补丁，主控补丁只要主控软件系统起来后就可以加载或激活补丁，线卡打补丁需线卡在线，并在命令中指定线卡槽位号。

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。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
激活补丁，可以根据需要配置补丁激活的方式为永久补丁还是临时补丁	1. 进入全局配置视图； 2. 执行命令**patch PATCH-NUMBER active (permanent | temporary) [slot SLOT-ID]**激活在主用或备用主控上指定的已加载的补丁（即补丁生效），以permanent激活的补丁在设备重启后仍可以生效。
查看配置结果	1. 进入特权用户视图； 2. 执行命令**show patch information**查看系统当前所有补丁信息。

9.6.4 配置去激活补丁

准备

去激活补丁之前，必须配置激活补丁操作。

目的

用户可以通过本节操作去激活正在运行的补丁。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
去激活补丁	1. 进入全局配置视图； 2. 执行命令**patch PATCH-NUMBER deactive [slot SLOT-ID]**在主用/备用主控上去激活补丁。
查看配置结果	1. 进入特权用户视图； 2. 执行命令**show patch information**查看系统当前所有补丁信息。

9.6.5 删除补丁

目的

用户可以通过本节操作进行补丁删除配置，对已激活的补丁在删除前会先去激活补丁再将补丁信息删除。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
直接删除补丁文件	1. 进入全局配置视图； 2. 执行命令**patch PATCH-NUMBER delete [slot SLOT-ID]** 在主用/备用主控上删除补丁文件。
查看配置结果	1. 进入特权用户视图； 2. 执行命令**show patch information**查看系统当前所有补丁信息。

9.6.6 查看补丁信息

目的

用户可以通过本节操作查看系统指定槽位补丁信息或所有补丁信息，具体信息包括：补丁单元号、补丁文件名、补丁功能及补丁状态。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
查看系统补丁信息	1. 进入普通用户视图； 2. 执行如下命令： ▶ **show patch information** ▶ **show patch information all** ▶ **show patch information slot SLOT-ID**

10 运维管理配置

本章介绍了SC9600E系列数据中心交换机运维管理的基本内容、配置过程和配置举例。

10.1 NTP 配置

10.1.1 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：

  1) 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；
  2) 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；
  3) 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；
  4) 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。

- 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。

10.1.2 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
指定设备为主时钟	1. 进入全局配置视图； 2. 进入NTP配置视图； 3. 执行命令**master**指定设备为主时钟。
配置NTP层级	1. 进入全局配置视图； 2. 进入NTP配置视图； 3. 执行命令**stratum (LAYER-NUMBER | default)**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。
配置NTP单播模式	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。）： 1. 进入全局配置视图； 2. 进入NTP配置视图； 3. 执行如下命令： ▶ **ntp unicast-server IPV4-ADDRESS** ▶ **ntp unicast-server IPV4-ADDRESS authentication-keyid KEY-ID** ▶ **ntp unicast-server IPV4-ADDRESS authentication-keyid KEY-ID source-interface loopback LOOPBACK-ID** ▶ **ntp unicast-server IPV4-ADDRESS authentication-keyid KEY-ID source-interface vlan VLAN-ID** ▶ **ntp unicast-server IPV4-ADDRESS source-interface loopback LOOPBACK-ID** ▶ **ntp unicast-server IPV4-ADDRESS source-interface vlan VLAN-ID** ▶ **ntp unicast-server IPV4-ADDRESS version VERSION-VALUE** ▶ **ntp unicast-server IPV4-ADDRESS version VERSION-VALUE authentication-keyid KEY-ID [source-ip SRC-IP]** ▶ **ntp unicast-server IPV4-ADDRESS version VERSION-VALUE authentication-keyid KEY-ID source-interface loopback LOOPBACK-ID** ▶ **ntp unicast-server IPV4-ADDRESS version VERSION-VALUE authentication-keyid KEY-ID source-interface vlan VLAN-ID** ▶ **ntp unicast-server IPV4-ADDRESS version VERSION-VALUE source-interface loopback LOOPBACK-ID** ▶ **ntp unicast-server IPV4-ADDRESS version VERSION-VALUE source-interface vlan VLAN-ID**

目的	步骤
	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。
配置NTP广播模式（适用于局域网）	配置NTP广播客户端： 1. 进入全局配置视图； 2. 进入VLANIF配置视图； 3. 执行如下命令： ▶ **ntp broadcast-client** ▶ **ntp broadcast-client IPV4-ADDRESS**
	配置NTP广播服务器端： 1. 进入全局配置视图； 2. 进入VLANIF配置视图； 3. 执行如下命令： ▶ **ntp broadcast-server [IPV4-ADDRESS]** ▶ **ntp broadcast-server authentication-keyid KEY-ID [IPV4-ADDRESS]** ▶ **ntp broadcast-server version VERSION-VALUE [IPV4-ADDRESS]** ▶ **ntp broadcast-server authentication-keyid KEY-ID version VERSION-VALUE [IPV4-ADDRESS]**
配置NTP组播模式	配置NTP组播客户端： 1. 进入全局配置视图； 2. 进入VLANIF配置视图； 3. 执行如下命令： ▶ **ntp multicast-client** ▶ **ntp multicast-client IPV4-ADDRESS**

目的	步骤
配置NTP组播模式	配置NTP组播服务器端： 1. 进入全局配置视图； 2. 进入VLANIF配置视图； 3. 执行如下命令： ▶ **ntp multicast-server [IPV4-ADDRESS]** ▶ **ntp multicast-server authentication-keyid KEY-ID [IPV4-ADDRESS]** ▶ **ntp multicast-server version VERSION-VALUE [IPV4-ADDRESS]** ▶ **ntp multicast-server ttl TTL-VALUE [IPV4-ADDRESS]** ▶ **ntp multicast-server version VERSION-VALUE ttl TTL-VALUE [IPV4-ADDRESS]** ▶ **ntp multicast-server authentication-keyid KEY-ID version VERSION-VALUE ttl TTL-VALUE [IPV4-ADDRESS]**

目的	步骤
增加或者修改一条IPv4 NTP主动对等，也支持配置多实例VPN	1. 进入全局配置视图； 2. 进入NTP配置视图； 3. 执行如下命令： ▶ **ntp unicast-peer IPV4-ADDRESS [source-ip SRC-IP]** ▶ **ntp unicast-peer IPV4-ADDRESS authentication-keyid KEY-ID [source-ip SRC-IP]** ▶ **ntp unicast-peer IPV4-ADDRESS authentication-keyid KEY-ID source-interface loopback LOOPBACK-ID** ▶ **ntp unicast-peer IPV4-ADDRESS authentication-keyid KEY-ID source-interface vlan VLAN-ID** ▶ **ntp unicast-peer IPV4-ADDRESS source-interface loopback LOOPBACK-ID** ▶ **ntp unicast-peer IPV4-ADDRESS source-interface vlan VLAN-ID** ▶ **ntp unicast-peer IPV4-ADDRESS version VERSION-VALUE** ▶ **ntp unicast-peer IPV4-ADDRESS version VERSION-VALUE authentication-keyid KEY-ID [source-ip SRC-IP]** ▶ **ntp unicast-peer IPV4-ADDRESS version VERSION-VALUE authentication-keyid KEY-ID source-interface loopback LOOPBACK-ID** ▶ **ntp unicast-peer IPV4-ADDRESS version VERSION-VALUE authentication-keyid KEY-ID source-interface vlan VLAN-ID** ▶ **ntp unicast-peer IPV4-ADDRESS version VERSION-VALUE source-interface loopback LOOPBACK-ID** ▶ **ntp unicast-peer IPV4-ADDRESS version VERSION-VALUE source-interface vlan VLAN-ID**

10.1.3 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
全局使能或去使能MD5认证功能	1. 进入全局配置视图； 2. 进入NTP配置视图； 3. 执行命令**authentication (enable | disable)**。
配置一条NTP验证密钥	1. 进入全局配置视图； 2. 进入NTP配置视图； 3. 执行如下命令： ▶ **authentication-keyid KEY-ID md5 key KEY-STRING** ▶ **authentication-keyid KEY-ID md5 key (cipher | plain) KEY-STRING**
使能或者禁止信任一条MD5认证密钥	1. 进入全局配置视图； 2. 进入NTP配置视图； 3. 执行命令**trusted-keyid TRUSTED-KEYID (enable | disable)**。
开启或关闭同步报文交互过程中的并发机制	1. 进入全局配置视图； 2. 进入NTP配置视图； 3. 执行命令**oncesync (enable | disable)**。
配置NTP单播模式的验证	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。用户可以根据实际情况选用步骤3中的命令）： 1. 进入全局配置视图； 2. 进入NTP配置视图； 3. 执行如下命令： ▶ **ntp unicast-server IPV4-ADDRESS authentication-keyid KEY-ID** ▶ **ntp unicast-server IPV4-ADDRESS version VERSION-VALUE authentication-keyid KEY-ID [source-ip SRC-IP]** ▶ **ntp unicast-server IPV4-ADDRESS version VERSION-VALUE authentication-keyid KEY-ID vpn-instance VPN-INSTANCE-NAME** ▶ **ntp unicast-server IPV4-ADDRESS authentication-keyid KEY-ID vpn-instance VPN-INSTANCE-NAME**
	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。

目的	步骤
配置NTP广播模式的验证（适用于局域网）	配置NTP广播客户端： 1. 进入全局配置视图； 2. 进入VLANIF配置视图； 3. 执行如下命令： ▶ **ntp broadcast-client** ▶ **ntp broadcast-client IPV4-ADDRESS**
	配置NTP广播服务器端： 1. 进入全局配置视图； 2. 进入VLANIF配置视图； 3. 执行如下命令： ▶ **ntp broadcast-server authentication-keyid KEY-ID** ▶ **ntp broadcast-server authentication-keyid KEY-ID IPV4-ADDRESS** ▶ **ntp broadcast-server authentication-keyid KEY-ID version VERSION-VALUE** ▶ **ntp broadcast-server authentication-keyid KEY-ID version VERSION-VALUE IPV4-ADDRESS**

目的	步骤
配置NTP组播模式的验证	配置NTP组播客户端： 1. 进入全局配置视图； 2. 进入VLANIF配置视图； 3. 执行如下命令： ▶ **ntp multicast-client** ▶ **ntp multicast-client IPV4-ADDRESS**
	配置NTP组播服务器端： 1. 进入全局配置视图； 2. 进入VLANIF配置视图； 3. 执行如下命令： ▶ **ntp multicast-server authentication-keyid KEY-ID** ▶ **ntp multicast-server authentication-keyid KEY-ID IPV4-ADDRESS** ▶ **ntp multicast-server authentication-keyid KEY-ID version VERSION-VALUE ttl TTL-VALUE** ▶ **ntp multicast-server authentication-keyid KEY-ID version VERSION-VALUE ttl TTL-VALUE IPV4-ADDRESS**
配置NTP对等体模式的验证	1. 进入全局配置视图； 2. 进入NTP配置视图； 3. 执行如下命令： ▶ **ntp unicast-peer IPV4-ADDRESS version VERSION-VALUE authentication-keyid KEY-ID [source-ip SRC-IP]** ▶ **ntp unicast-peer IPV4-ADDRESS authentication-keyid KEY-ID [source-ip SRC-IP]** ▶ **ntp unicast-peer IPV4-ADDRESS version VERSION-VALUE authentication-keyid KEY-ID vpn-instance VPN-INSTANCE-NAME** ▶ **ntp unicast-peer IPV4-ADDRESS authentication-keyid KEY-ID vpn-instance VPN-INSTANCE-NAME**

10.1.4 维护及调试

目的

当NTP功能不正常，需要进行查看、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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
查看NTP全局配置信息	1. 进入全局配置视图，NTP配置视图、VLAN配置视图； 2. 执行命令**show ntp**。
查看NTP服务信息	1. 进入全局配置视图，NTP配置视图、VLAN配置视图； 2. 执行命令**show ntp service**。
查看NTP服务详细配置信息	1. 进入全局配置视图，NTP配置视图、VLAN配置视图； 2. 执行命令**show ntp service verbose**。

10.1.5 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，如图 10-1所示。

组网图

图 10-1 NTP配置示意图

配置步骤

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。
2. 配置NTP服务器为主时钟，并配置层数。

```
Server(config-ntp)#master
Server(config-ntp)#stratum 2
```

3. 配置NTP客户端的层数。

```
Client(config-ntp)#stratum 9
```

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）
```

提示：

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。

10.2 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。SNMP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、快速和低价格的环境中使用。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。

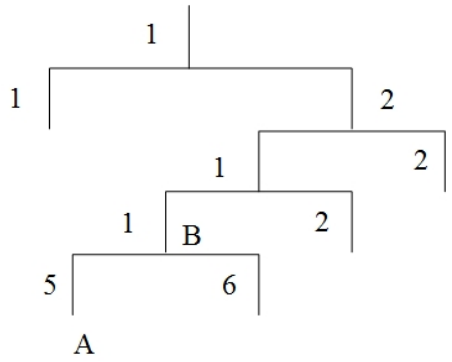


图 10-2 MIB树结构

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）。

SC9600E系列数据中心交换机中的SNMP Agent 支持SNMP V1、V2和V3，支持的常见MIB 如下表所示。

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	-
	QACL MIB	
	ADBM MIB	
	RSTP MIB	
	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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
指定管理员的联系方法	1. 进入全局配置视图； 2. 执行命令**snmp contact CONTACT-INFO**配置管理员的联络方式。
指定被管理设备的位置	1. 进入全局配置视图； 2. 执行命令**snmp location LOCATION-INFO**配置交换机的位置。
配置支持的SNMP协议版本	1. 进入全局配置视图； 2. 执行命令**snmp version (v1 | v2 | v3 | all)**配置支持的SNMP协议版本。
取消配置的SNMP协议版本	1. 进入全局配置视图； 2. 执行命令**no snmp version (v1 | v2 | v3 | all)**取消配置的SNMP协议版本。

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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置SNMP的团体名	1. 进入全局配置视图； 2. 执行如下命令设置SNMP团体名： ▶ **snmp community NAME (ro | rw)** ▶ **snmp community NAME (ro | rw) view VIEW-NAME**
（可选）使能写团体名功能	1. 进入全局配置视图； 2. 执行命令**snmp rw-community enable**使能写团体名功能。

目的	步骤
配置SNMP视图	1. 进入全局配置视图； 2. 执行如下命令创建不同的MIB视图使网管访问设备时具有不同的访问权限： ▶ **snmp view VIEW-NAME OID-TREE (included | excluded)** ▶ **snmp view VIEW-NAME OID-TREE (included | excluded) mask SUBTREEMASK**
配置SNMP组信息	1. 进入全局配置视图； 2. 执行命令**snmp group GROUP-NAME read-view READ-VIEW write-view WRITE-VIEW notify-view NOTIFY-VIEW**配置SNMP组。
创建SNMP用户	1. 进入全局配置视图； 2. 执行如下命令创建用户信息，可以使指定组中的用户对设备进行访问： ▶ **snmp user USER-NAME group GROUP-NAME no-auth-no-priv [filter-list ACL-NUMBER]** ▶ **snmp user USER-NAME group GROUP-NAME auth (md5 | sha) AUTHKEY priv no-priv [filter-list ACL-NUMBER]** ▶ **snmp user USER-NAME group GROUP-NAME auth (md5 | sha) AUTHKEY priv (dea | des) PRIVKEY** ▶ **snmp user USER-NAME group GROUP-NAME auth (md5 | sha) AUTHKEY priv (des | aes) PRIVKEY filter-list ACL-NUMBER**
（可选）配置SNMP重认证时间	1. 进入全局配置视图； 2. 执行命令**snmp reauth-interval INTERVAL**设置SNMP验证失败时重新进行认证的间隔时间。
（可选）配置SNMP认证失败次数	1. 进入全局配置视图； 2. 执行命令**snmp fail-count COUNT**设置SNMP认证失败的次数。
（可选）配置SNMP端口号	1. 进入全局配置视图； 2. 执行命令**snmp port (PORT-NUMBER | default)**设置SNMP协议包使用的端口号。
删除SNMP团体名	1. 进入全局配置视图； 2. 执行命令**no snmp community NAME**删除已配置的SNMP团体名。

目的	步骤
（可选）去使能写团体名功能	1. 进入全局配置视图； 2. 执行命令**snmp rw-community disable**去使能写团体名功能。
删除SNMP用户	1. 进入全局配置视图； 2. 执行命令**no snmp user USER-NAME**删除已创建的SNMP用户。
删除SNMP组信息	1. 进入全局配置视图； 2. 执行命令**no snmp group GROUP-NAME**删除已配置的SNMP组信息。
删除SNMP视图	1. 进入全局配置视图； 2. 执行命令**no snmp view VIEW-NAME**或**no snmp view VIEW-NAME OID-TREE**删除已配置的SNMP视图。
配置SNMP Get Bulk请求的varbind最大个数	1. 进入全局配置视图； 2. 执行命令**snmp bulk max-varbind (VARBIND-NUMBER | default)**配置SNMP Get Bulk请求的varbind最大个数。

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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
（可选）使能认证失败后发送Trap消息的功能	1. 进入全局配置视图； 2. 执行命令**snmp auth-trap enable**使能认证trap后，如果认证失败则设备会发送trap消息。
指定SNMP的Trap信息的目标主机	1. 进入全局配置视图； 2. （IPv4）执行如下命令： ▶ **snmp trap-server IPV4-ADDRESS SECURITY-NAME (v1 | v2 | v3)** ▶ **snmp trap-server IPV4-ADDRESS PORT SECURITY-NAME (v1 | v2 | v3)** ▶ **snmp trap-server IPV4-ADDRESS SECURITY-NAME v3 (auth | priv)** ▶ **snmp trap-server IPV4-ADDRESS PORT SECURITY-NAME v3 (auth | priv)**
删除SNMP Trap消息的发布地址	1. 进入全局配置视图； 2. 执行命令**no snmp trap-source**。
删除SNMP的Trap信息的目标主机	1. 进入全局配置视图； 2. （IPv4）执行如下命令： ▶ **no snmp trap-server IPV4-ADDRESS** ▶ **no snmp trap-server IPV4-ADDRESS SECURITY-NAME**

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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
查看设备SNMP的代理信息	1. 进入普通用户视图、特权用户视图、全局配置视图； 2. 执行命令**show snmp agent**查看设备SNMP的代理信息。
查看SNMP的团体配置信息	1. 进入普通用户视图、特权用户视图、全局配置视图； 2. 执行命令**show snmp community**查看SNMP的团体配置信息。
查看SNMP的配置信息	1. 进入普通用户视图、特权用户视图、全局配置视图； 2. 执行命令**show snmp config**查看SNMP的配置信息。
查看SNMP组信息	1. 进入普通用户视图、特权用户视图、全局配置视图； 2. 执行命令**show snmp group**查看SNMP组信息。
查看SNMP的报文处理统计数据信息	1. 进入普通用户视图、特权用户视图、全局配置视图； 2. 执行命令**show snmp statistic**查看SNMP的报文处理统计数据信息。
查看显示接收trap信息的主机及版本类型	1. 进入普通用户视图、特权用户视图、全局配置视图； 2. 执行命令**show snmp trap-server**查看显示接收trap信息的主机及版本类型。
查看SNMP用户信息	1. 进入普通用户视图、特权用户视图、全局配置视图； 2. 执行命令**show snmp user**查看SNMP用户信息。
查看SNMP视图信息	1. 进入普通用户视图、特权用户视图、全局配置视图； 2. 执行命令**show snmp view**查看SNMP视图信息。
查看网络管理协议的告警信息状态	1. 进入普通用户视图； 2. 执行命令**show snmp trap state**查看网络管理协议的告警信息状态。

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129.102.149.13，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、允许交换机发送Trap消息。

组网图

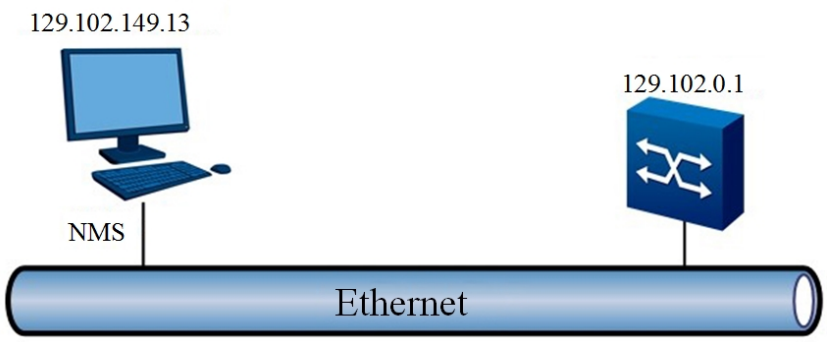


图 10-3 SNMP配置举例组网图

配置交换机

1. 进入全局配置视图。

```
SC9600E#config
```

2. 设置团体、群组和用户。

```
SC9600E(config)#snmp view v3test 1.3.6 include
SC9600E(config)#snmp group aaa read-view v3test write-view v3test
notify-view v3test
SC9600E(config)#snmp user admin group aaa no-auth-no-priv
```

3. 允许向网管工作站（NMS）129.102.149.23 发送Trap报文。

```
SC9600E(config)#snmp trap-server 129.102.149.23 name123 v3
```

配置NMS

网管所在的PC机需要进行登录设置。对于Mib-Browser，登录设置为：SNMPV1、V2 使用缺省的团体名登录，SNMPV3使用用户admin登录。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 NQA配置

10.3.1 NQA概述

NQA具有以下功能：

- 支持测试类型：ICMP-Echo
- 支持联动功能

◆ 支持阈值告警功能

10.3.2 NQA测试机制

ICMP-echo 测试机制

遵循RFC-2925来实现，其实现原理是通过发送ICMP报文来计算网络响应时间及丢包率。

ICMP-echo测试成功的前提条件是目的设备要能够正确响应ICMP echo request报文。NQA客户端会根据设置的探测时间及频率向探测目的IP地址发送ICMP echo request报文，目的地址收到ICMP echo request报文后，回复ICMP echo reply报文。NQA客户端根据ICMP echo reply报文的接收情况，如接收时间戳以及报文个数，可以计算出目的IP地址的响应时间及丢包率，从而反应出当前的网络性能及网络情况。

10.3.3 NQA联动功能

联动功能是指通过建立联动项，对当前所在测试组中的结果进行探测，当连续探测失败次数达到一定数目时，就通过Track模块触发应用模块联动。联动功能的实现如图 10-4所示。

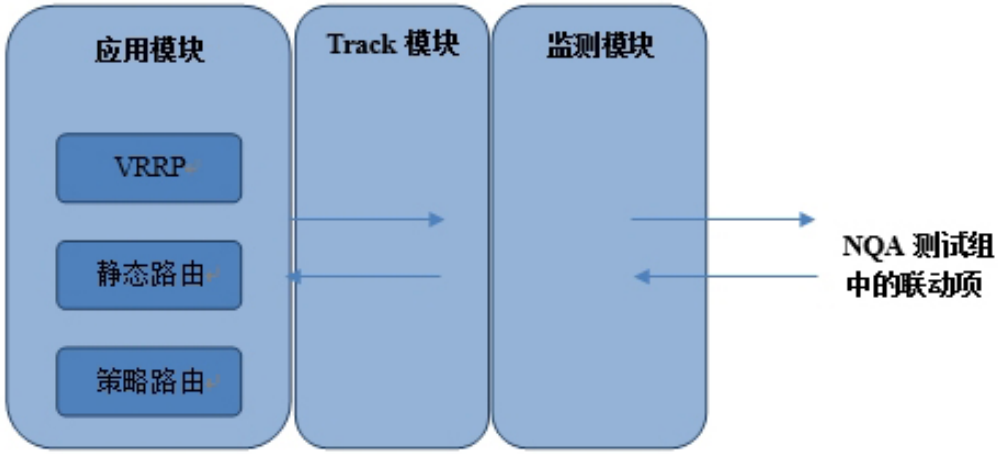


图 10-4 联动功能示意图

联动功能由监测模块、Track模块和应用模块三部分组成：

1. 监测模块负责对链路状态、网络性能等进行监测，并将探测结果通知给Track模块。

2. Track模块接收到监测模块的探测结果后，及时改变Track项状态，并通知应用模块。Track模块位于应用模块和监测模块之间，可以屏蔽不同监测模块的差异，为应用模块提供统一的接口。
3. 应用模块根据Track项的状态，进行相应的处理，从而实现联动。

10.3.4 配置ICMP-echo功能测试

目的

使用NQA进行ICMP-echo测试，测试本端（DUT2）发送的报文是否可以到达指定的目的端（DUT1），以及报文的往返时间。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
创建ICMP-echo类型的NQA测试组并配置相关测试参数	1. 进入全局配置视图； 2. 执行命令 ◆ **DUT2# configure** ◆ **DUT2 (config)#nqa start** ◆ **DUT2 (config)# nqa test-instance 123 456** ◆ **DUT2 (config-nqa-123-456)#type icmp-echo** ◆ **DUT2 (nqa-123-456-icmp-echo)#destination ip 3.3.3.1**
配置可选参数	1. 进入全局配置视图； 2. 执行命令 ◆ **DUT2 (nqa-123-456-icmp-echo)#probe count 10** ◆ **DUT2 (nqa-123-456-icmp-echo)#probe timeout 500** ◆ **DUT2 (nqa-123-456-icmp-echo)# frequency 5000**

目的	步骤
配置NQA历史记录功能	1. 进入全局配置视图； 2. 执行命令 ◆ **DUT2 (nqa-123-456-icmp-echo)#history-record enable** ◆ **DUT2 (nqa-123-456-icmp-echo)# history-record number 10** ◆ **DUT2 (nqa-123-456-icmp-echo)# quit** ◆ **DUT2 (config-nqa-123-456)#quit**
启动ICMP-echo测试操作	1. 进入全局配置视图； 2. 执行命令**nqa schedule 123 456 start-time now life-time forever**启动测试

10.4 LLDP 配置

10.4.1 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。

10.4.2 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。

提示：

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。

10.4.3 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
端口下使能或去使能LLDP及其管理状态	1. 进入全局配置视图； 2. 进入接口组配置视图； 3. 执行命令**lldp admin-status (tx-only | rx-only | rx-tx | disable)**使能或去使能接口LLDP及其管理状态。
配置LLDP的管理地址	1. 进入全局配置视图； 2. 进入接口配置视图、接口组配置视图； 3. 执行如下命令配置LLDP的管理地址： ▶ **lldp management-address IP-ADDRESS (enable | disable)** ▶ **lldp management-address MAC-ADDRESS (enable | disable)**

10.4.4 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
（可选）配置lldp帧发送时间间隔	1. 进入全局配置视图、接口配置视图（以太网）、接口组配置视图； 2. 执行命令**lldp tx-interval (TX-INTERVAL | default)**配置LLDP帧发送时间间隔。
（可选）配置LLDP帧发送间隔的倍数	1. 进入全局配置视图、接口配置视图（以太网）、接口组配置视图； 2. 执行命令**lldp tx-hold (TX-HOLD | default)**配置LLDP帧发送间隔的倍数。
（可选）配置LLDP端口状态重新初始化的时延	1. 进入全局配置视图、接口配置视图（以太网）、接口组配置视图； 2. 执行命令**lldp reinit-delay (REINIT-DELAY | default)**配置LLDP端口状态重新初始化的时延。
（可选）配置设备发送LLDP报文的延迟时间	1. 进入全局配置视图、接口配置视图（以太网）、接口组配置视图； 2. 执行命令**lldp tx-delay (TX-DELAY | default)**配置设备发送LLDP报文的延迟时间。
（可选）全局配置告警发送时间间隔	1. 进入全局配置视图、接口配置视图（以太网）、接口组配置视图； 2. 执行命令**lldp notification-interval (NOTIFICATION-INTERVAL | default)**全局配置告警发送时间间隔。
（可选）配置LLDP MED快速发包个数	1. 进入全局配置视图； 2. 执行命令**lldp faststart-count (FASTSTART-COUNT | default)**配置LLDP MED快速发包个数。
使能或去使能端口LLDP告警功能	1. 进入全局配置视图； 2. 进入接口配置视图、接口组配置视图； 3. 执行命令**lldp trap (enable | disable)**使能或去使能端口LLDP告警功能。
（可选）使能或去使能端口LLDP MED告警功能	1. 进入全局配置视图； 2. 进入接口配置视图、接口组配置视图； 3. 执行命令**lldp med-notification (enable | disable)**使能或去使能端口LLDP MED告警功能。

目的	步骤
（可选）配置端口下与MED相关的信息	1. 进入全局配置视图； 2. 进入接口配置视图、接口组配置视图； 3. 执行命令**lldp med-tlv-tx { capabilities | network-policy | location | extended-pse | extended-pd | inventory | all } { enable | disable }**配置端口下与MED相关的信息。
（可选）配置接口下LLDP的基本TLV	1. 进入全局配置视图； 2. 进入接口配置视图、接口组配置视图； 3. 执行命令**lldp basic-tlv-tx { port-description | system-name | system-description | system-capability | all } { enable | disable }**配置接口下LLDP的基本TLV。
（可选）配置IEEE802.1可选TLV的端口VLAN ID功能	1. 进入全局配置视图； 2. 进入接口配置视图、接口组配置视图； 3. 执行命令**lldp dot1-tlv-tx port-vid { enable | disable }**配置IEEE802.1可选TLV的端口VLAN ID功能。
（可选）配置IEEE802.1可选TLV的VLAN名字功能	1. 进入全局配置视图； 2. 进入接口配置视图、接口组配置视图； 3. 执行命令**lldp dot1-tlv-tx vlan-name VLANLIST { enable | disable }**配置IEEE802.1可选TLV的VLAN名字功能。
（可选）配置IEEE802.1可选TLV的协议VLAN ID的功能	1. 进入全局配置视图； 2. 进入接口配置视图、接口组配置视图； 3. 执行命令**lldp dot1-tlv-tx protocol-id { enable | disable }**或**lldp dot1-tlv-tx protocol-vid VLANLIST { enable | disable }**配置IEEE802.1可选TLV的协议VLAN ID的功能。
（可选）配置IEEE802.3组织定义的TLV的相关信息	1. 进入全局配置视图； 2. 进入接口配置视图、接口组配置视图； 3. 执行命令**lldp dot3-tlv-tx { mac-phy | power | link-aggregation | max-frame-size | all } { enable | disable }**配置IEEE802.3组织定义的TLV的相关信息。

目的	步骤
配置设备自身的位置信息	1. 进入全局配置视图； 2. 进入接口配置视图、接口组配置视图； 3. 执行如下命令配置IEEE802.3组织定义的TLV的相关信息： ▶ **lldp location-id civic-address CIVIC-ADDRESS COUNTRY-CODE CA-TYPE CA-VALUE** ▶ **lldp location-id civic-address CIVIC-ADDRESS COUNTRY-CODE CA-TYPE CA-VALUE CA-TYPE CA-VALUE** ▶ **lldp location-id civic-address CIVIC-ADDRESS COUNTRY-CODE CA-TYPE CA-VALUE CA-TYPE CA-VALUE CA-TYPE CA-VALUE** ▶ **lldp location-id civic-address CIVIC-ADDRESS COUNTRY-CODE CA-TYPE CA-VALUE CA-TYPE CA-VALUE CA-TYPE CA-VALUE CA-TYPE CA-VALUE** ▶ **lldp location-id civic-address CIVIC-ADDRESS COUNTRY-CODE CA-TYPE CA-VALUE CA-TYPE CA-VALUE CA-TYPE CA-VALUE CA-TYPE CA-VALUE CA-TYPE CA-VALUE CA-TYPE CA-VALUE** ▶ **lldp location-id civic-address CIVIC-ADDRESS COUNTRY-CODE CA-TYPE CA-VALUE CA-TYPE CA-VALUE CA-TYPE CA-VALUE CA-TYPE CA-VALUE CA-TYPE CA-VALUE CA-TYPE CA-VALUE CA-TYPE CA-VALUE CA-TYPE CA-VALUE** ▶ **lldp location-id civic-address CIVIC-ADDRESS COUNTRY-CODE CA-TYPE CA-VALUE CA-TYPE CA-VALUE CA-TYPE CA-VALUE CA-TYPE CA-VALUE CA-TYPE CA-VALUE CA-TYPE CA-VALUE CA-TYPE CA-VALUE CA-TYPE CA-VALUE CA-TYPE CA-VALUE CA-TYPE CA-VALUE**
	◆ **lldp location-id civic-address CIVIC-ADDRESS COUNTRY-CODE CA-TYPE CA-VALUE CA-TYPE CA-VALUE CA-TYPE CA-VALUE CA-TYPE CA-VALUE CA-TYPE CA-VALUE CA-TYPE CA-VALUE CA-TYPE CA-VALUE CA-TYPE CA-VALUE CA-TYPE CA-VALUE CA-TYPE CA-VALUE CA-TYPE CA-VALUE** ◆ **lldp location-id civic-address CIVIC-ADDRESS COUNTRY-CODE CA-TYPE CA-VALUE CA-TYPE CA-VALUE CA-TYPE CA-VALUE CA-TYPE CA-VALUE CA-TYPE CA-VALUE CA-TYPE CA-VALUE CA-TYPE CA-VALUE CA-TYPE CA-VALUE CA-TYPE CA-VALUE CA-TYPE CA-VALUE CA-TYPE CA-VALUE** ◆ **lldp location-id elin-address NUMBER**

10.4.5 维护及调试

目的

当LLDP功能不正常，需要进行查看、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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
查看LLDP端口信息	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； 2. 执行如下命令： ▶ **show lldp interface** ▶ **show lldp interface (ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 40gigaethernet) INTERFACE-NUMBER** ▶ **show lldp interface verbose**
查看LLDP统计信息	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； 2. 执行如下命令： ▶ **show lldp statistic** ▶ **show lldp statistic interface (ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 40gigaethernet) INTERFACE-NUMBER**
查看所有邻居或者指定邻居的设备信息	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； 2. 执行如下命令： ▶ **show lldp remote** ▶ **show lldp remote verbose** ▶ **show lldp remote REMOTE-NUMBER**
查看LLDP本地信息	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； 2. 执行命令**show lldp local**查看LLDP本地信息。

目的	步骤
查看LLDP的配置信息	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； 2. 执行命令**show lldp config**查看LLDP的配置信息。
查看指定接口邻居信息	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； 2. 执行命令**show lldp remote interface (ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 40gigaethernet) INTERFACE-NUMBER**查看指定接口邻居信息。
查看指定接口配置信息	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； 2. 执行命令**show lldp config interface (ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 40gigaethernet) INTERFACE-NUMBER**查看指定接口配置信息。
查看指定接口本地设备信息	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； 2. 执行命令**show lldp local interface (ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 40gigaethernet) INTERFACE-NUMBER**查看指定接口本地设备信息。
清零LLDP端口的统计计数	1. 进入全局配置视图； 2. 进入接口配置视图、接口组配置视图； 3. 执行命令**reset lldp counter**清零LLDP端口的统计计数。
打开或关闭LLDP调试开关	1. 进入特权用户视图； 2. 执行命令**debug lldp (config | rxstate | txstate | rxpkt | event | sync | all)**或**no debug lldp (config | rxstate | txstate | rxpkt | event | sync | all)**打开或关闭LLDP调试开关。

10.4.6 配置举例

组网要求

1. SC9600E_1、SC9600E_2、SC9600E_3、SC9600E_4、SC9600E_5五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SC9600E_1，可得知SC9600E_2、SC9600E_3是与SC9600E_1的设备，由此可得出与SC9600E_1直连的拓扑。并通过SC9600E_2、SC9600E_3公告的消息中得知SC9600E_2、SC9600E_3的管理地址，分别为10.1.1.2与10.1.1.3，进而访问SC9600E_2与SC9600E_3。
4. 访问SC9600E_2，可知与SC9600E_2直连的设备有SC9600E_4，由此可得出与SC9600E_2直连的拓扑。并且可通过SC9600E_4公告的消息中得知SC9600E_4的管理地址，为10.1.1.4，进而可继续访问SC9600E_4。
5. 访问SC9600E_3，可知与SC9600E_3直连的设备有SC9600E_5，由此可得出与SC9600E_3直连的拓扑。并且可通过SC9600E_5公告的消息中得知SC9600E_5的管理地址为10.1.1.5，进而可继续访问SC9600E_5。

按以上步骤，可得出一个全面的拓扑图，如图 10-5所示，并且可知道各个设备的相关配置信息。

组网图

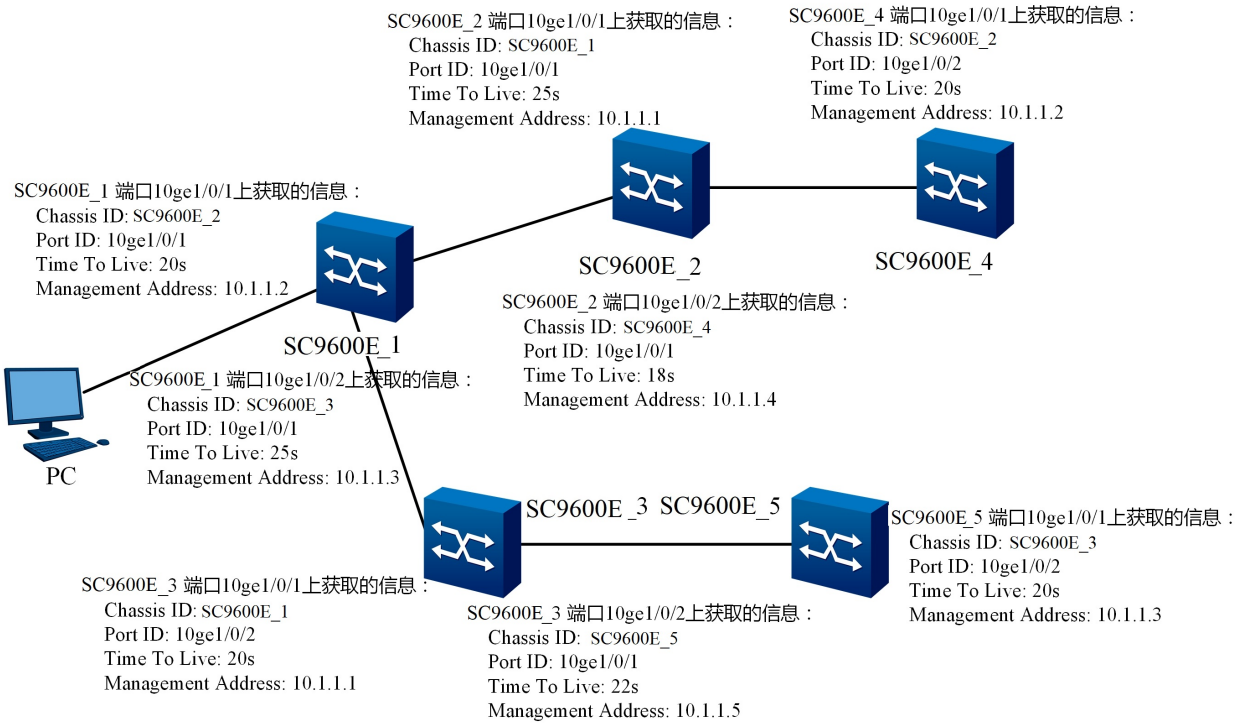


图 10-5 LLDP配置示意图

配置思路

在SC9600E_1设置LLDP工作模式为rx-tx，并配置管理地址为10.1.1.1。

在SC9600E_2设置LLDP工作模式为rx-tx，并配置管理地址为10.1.1.2。

在SC9600E_3设置LLDP工作模式为rx-tx，并配置管理地址为10.1.1.3。

在SC9600E_4设置LLDP工作模式为rx-tx，并配置管理地址为10.1.1.4。

在SC9600E_5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SC9600E_1。

```
SC9600E_1(config)#interface 10gigaethernet 1/0/1
SC9600E_1(config-10ge1/0/1)#no shutdown
SC9600E_1(config-10ge1/0/1)#lldp admin-status rx-tx
SC9600E_1(config-10ge1/0/1)#lldp management-address 10.1.1.1 enable
```

2. 配置SC9600E_2。

```
SC9600E_2(config)#interface 10gigaethernet 1/0/1
SC9600E_2(config-10ge1/0/1)#no shutdown
SC9600E_2(config-10ge1/0/1)#lldp admin-status rx-tx
SC9600E_2(config-10ge1/0/1)#lldp management-address 10.1.1.2 enable
```

3. 配置SC9600E_3。

```
SC9600E_3(config)#interface 10gigaethernet 1/0/1
SC9600E_3(config-10ge1/0/1)#no shutdown
SC9600E_3(config-10ge1/0/1)#lldp admin-status rx-tx
SC9600E_3(config-10ge1/0/1)#lldp management-address 10.1.1.3 enable
```

4. 配置SC9600E_4。

```
SC9600E_4(config)#interface 10gigaethernet 1/0/1
SC9600E_4(config-10ge1/0/1)#no shutdown
SC9600E_4(config-10ge1/0/1)#lldp admin-status rx-tx
SC9600E_4(config-10ge1/0/1)#lldp management-address 10.1.1.4 enable
```

5. 配置SC9600E_5。

```
SC9600E_5(config)#interface 10gigaethernet 1/0/1
SC9600E_5(config-10ge1/0/1)#no shutdown
SC9600E_5(config-10ge1/0/1)#lldp admin-status rx-tx
SC9600E_5(config-10ge1/0/1)#lldp management-address 10.1.1.5 enable
```

10.5 报文捕获配置

10.5.1 CPU 报文捕获概述

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。

10.5.2 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
命令可以用来显示CPU收发包的接口统计信息（1）	1. 在全局配置视图下，执行命令disable退出到普通用户视图； 2. 执行以下命令： ▶ **show cpupkt interface (ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 40gigaethernet) INTERFACE-NUMBER** ▶ **show cpupkt interface (ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 40gigaethernet) INTERFACE-NUMBER (alltype | anydata-dcp | anydata-ha | arp | arpmiss | bfdeth | bfd-ip | bfd-ipv6 | bgp | cfm | dad | dcp | dhcp | dhcpv6 | dot1x | dot3ah | eaps | g8031 | g8032 | ha | hwapi-dcp | hwapi-ha | icmp | icmpv6 | icmpv6-echoreply | icmpv6-echo-request | icmpv6-na | icmpv6-ns | icmpv6-ra | icmpv6-redirect | icmpv6-rs | igmp | ip | ipv6 | isis | iss | lacp | loopback | mlag | ndmiss | ospf | ospfv3 | other | rer | sgm | snmp | spanningtree | stack-kernel | stack-user | sw-dcp | sw-ha | swif-dcp | swif-ha | tcp | tcp6 | udp | udp6 | vrrpv2 | vrrpv3 | y1731) (statistic | change)** ▶ **show cpupkt interface eth-trunk TRUNK-NUMBER (alltype | anydata-dcp | anydata-ha | arp | arpmiss | bfd-eth | bfd-ip | bfd-ipv6 | bgp | cfm | dad | dcp | dhcp | dhcpv6 | dot1x | dot3ah | eaps | g8031 | g8032 | ha | hwapi-dcp | hwapi-ha | icmp | icmpv6 | icmpv6-echo-reply | icmpv6-echo-request | icmpv6-na | icmpv6-ns | icmpv6-ra | icmpv6-redirect | icmpv6-rs | igmp | ip | ipv6 | isis | iss | lacp | loopback | mlag | ndmiss | ospf | ospfv3 | other | rer | sgm | snmp | spanningtree | stack-kernel | stack-user | sw-dcp | sw-ha | swif-dcp | swif-ha | tcp | tcp6 | udp | udp6 | vrrpv2 | vrrpv3 | y1731) statistic** ▶ **show cpupkt interface statistic (alltype | anydata-dcp | anydata-ha | arp | arpmiss | bfd-eth | bfd-ip | bfd-ipv6 | bgp | cfm | dad | dcp | dhcp | dhcpv6 | dot1x | dot3ah | eaps | g8031 | g8032 | ha | hwapi-dcp | hwapi-ha | icmp | icmpv6 | icmpv6-echo-reply | icmpv6-echo-request | icmpv6-na | icmpv6-ns | icmpv6-ra | icmpv6-redirect | icmpv6-rs | igmp | ip | ipv6 | isis | iss | lacp | loopback | mlag | ndmiss | ospf | ospfv3 | other | rer | sgm | snmp | spanningtree | stackkernel | stack-user | sw-dcp | sw-ha | swif-dcp | swif-ha | tcp | tcp6 | udp | udp6 | vrrpv2 | vrrpv3 | y1731) brief [all]**

目的	步骤
命令可以用来显示CPU收发包的接口统计信息（2）	◆ **show cpupkt interface statistic brief all** ◆ **show cpupkt interface (ha | dcp | dcp2)** ◆ **show cpupkt interface outband** ◆ **show cpupkt interface outband (alltype | anydata-dcp | anydata-ha | arp | arpmiss | bfd-eth | bfd-ip | bfd-ipv6 | bgp | cfm | dad | dcp | dhcp | dhcpv6 | dot1x | dot3ah | eaps | g8031 | g8032 | ha | hwapi-dcp | hwapi-ha | icmp | icmpv6 | icmpv6-echo-reply | icmpv6-echo-request | icmpv6-na | icmpv6-ns | icmpv6-ra | icmpv6-redirect | icmpv6-rs | igmp | ip | ipv6 | isis | iss | lacp | loopback | mlag | ndmiss | ospf | ospfv3 | other | rer | sgm | snmp | spanningtree | stackkernel | stack-user | sw-dcp | sw-ha | swif-dcp | swif-ha | tcp | tcp6 | udp | udp6 | vrrpv2 | vrrpv3 | y1731) (statistic | change)

目的	步骤
调试CPU收发包的接口配置	1. 不执行任何命令保持当前特权用户视图； 2. 执行以下命令： ▶ **debug cpupkt interface outband (alltype | anydata-dcp | anydata-ha | arp | arpmiss | bfd-eth | bfd-ip | bfd-ipv6 | bgp | cfm | dad | dcp | dhcp | dhcpv6 | dot1x | dot3ah | eaps | g8031 | g8032 | ha | hwapi-dcp | hwapi-ha | icmp | icmpv6 | icmpv6-echo-reply | icmpv6-echo-request | icmpv6-na | icmpv6-ns | icmpv6-ra | icmpv6-redirect | icmpv6-rs | igmp | ip | ipv6 | isis | iss | lacp | loopback | mlag | ndmiss | ospf | ospfv3 | other | rer | sgm | snmp | spanningtree | stackkernel | stack-user | sw-dcp | sw-ha | swif-dcp | swif-ha | tcp | tcp6 | udp | udp6 | vrrpv2 | vrrpv3 | y1731) (capturein | captureout | captureall)** ▶ **debug cpupkt interface outband (alltype | anydata-dcp | anydata-ha | arp | arpmiss | bfd-eth | bfd-ip | bfd-ipv6 | bgp | cfm | dad | dcp | dhcp | dhcpv6 | dot1x | dot3ah | eaps | g8031 | g8032 | ha | hwapi-dcp | hwapi-ha | icmp | icmpv6 | icmpv6-echo-reply | icmpv6-echo-request | icmpv6-na | icmpv6-ns | icmpv6-ra | icmpv6-redirect | icmpv6-rs | igmp | ip | ipv6 | isis | iss | lacp | loopback | mlag | ndmiss | ospf | ospfv3 | other | rer | sgm | snmp | spanningtree | stack-kernel | stack-user | sw-dcp | sw-ha | swif-dcp | swif-ha | tcp | tcp6 | udp | udp6 | vrrpv2 | vrrpv3 | y1731) (in | out | all)** ▶ **no debug cpupkt interface outband (alltype | anydata-dcp | anydata-ha | arp | arpmiss | bfd-eth | bfd-ip | bfd-ipv6 | bgp | cfm | dad | dcp | dhcp | dhcpv6 | dot1x | dot3ah | eaps | g8031 | g8032 | ha | hwapi-dcp | hwapi-ha | icmp | icmpv6 | icmpv6-echo-reply | icmpv6-echo-request | icmpv6-na | icmpv6-ns | icmpv6-ra | icmpv6-redirect | icmpv6-rs | igmp | ip | ipv6 | isis | iss | lacp | loopback | mlag | ndmiss | ospf | ospfv3 | other | rer | sgm | snmp | spanningtree | stack-kernel | stack-user | sw-dcp | sw-ha | swif-dcp | swif-ha | tcp | tcp6 | udp | udp6 | vrrpv2 | vrrpv3 | y1731)**

目的	步骤
重置CPU抓包信息	1. 不执行任何命令保持当前特权用户视图； 2. 执行以下命令： ▶ **reset cpupkt interface (ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 40gigaethernet) INTERFACE-NUMBER** ▶ **reset cpupkt interface (ha | dcp | dcp2)** ▶ **reset cpupkt interface outband** ▶ **reset cpupkt interface outband (alltype | anydata-dcp | anydata-ha | arp | arpmiss | bfd-eth | bfd-ip | bfd-ipv6 | bgp | cfm | dad | dcp | dhcp | dhcpv6 | dot1x | dot3ah | eaps | g8031 | g8032 | ha | hwapi-dcp | hwapi-ha | icmp | icmpv6 | icmpv6-echo-reply | icmpv6-echo-request | icmpv6-na | icmpv6-ns | icmpv6-ra | icmpv6-redirect | icmpv6-rs | igmp | ip | ipv6 | isis | iss | lacp | loopback | mlag | ndmiss | ospf | ospfv3 | other | rer | sgm | snmp | spanningtree | stackkernel | stack-user | sw-dcp | sw-ha | swif-dcp | swif-ha | tcp | tcp6 | udp | udp6 | vrrpv2 | vrrpv3 | y1731) statistic**
	◆ **reset cpupkt interface (ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 40gigaethernet) INTERFACE-NUMBER (alltype | anydata-dcp | anydata-ha | arp | arpmiss | bfd-eth | bfd-ip | bfd-ipv6 | bgp | cfm | dad | dcp | dhcp | dhcpv6 | dot1x | dot3ah | eaps | g8031 | g8032 | ha | hwapi-dcp | hwapi-ha | icmp | icmpv6 | icmpv6-echo-reply | icmpv6-echo-request | icmpv6-na | icmpv6-ns | icmpv6-ra | icmpv6-redirect | icmpv6-rs | igmp | ip | ipv6 | isis | iss | lacp | loopback | mlag | ndmiss | ospf | ospfv3 | other | rer | sgm | snmp | spanningtree | stack-kernel | stack-user | sw-dcp | sw-ha | swif-dcp | swif-ha | tcp | tcp6 | udp | udp6 | vrrpv2 | vrrpv3 | y1731) statistic** ◆ **reset cpupkt interface eth-trunk TRUNK-NUMBER (alltype | anydata-dcp | anydata-ha | arp | arpmiss | bfd-eth | bfd-ip | bfd-ipv6 | bgp | cfm | dad | dcp | dhcp | dhcpv6 | dot1x | dot3ah | eaps | g8031 | g8032 | ha | hwapi-dcp | hwapi-ha | icmp | icmpv6 | icmpv6-echo-reply | icmpv6-echo-request | icmpv6-na | icmpv6-ns | icmpv6-ra | icmpv6-redirect | icmpv6-rs | igmp | ip | ipv6 | isis | iss | lacp | loopback | mlag | ndmiss | ospf | ospfv3 | other | rer | sgm | snmp | spanningtree | stack-kernel | stack-user | sw-dcp | sw-ha | swif-dcp | swif-ha | tcp | tcp6 | udp | udp6 | vrrpv2 | vrrpv3 | y1731) statistic**

10.6 设备升级与回退

升级准备

详细描述升级所需的必备工具，设备运行状态检查，软、硬件版本检查，软件包检查等升级前的准备工作，降低升级风险。

- OS升级包，文件名为SC9600E_V370R240.bin；
- PC安装好FTP软件；
- PC安装好7zip软件；
- PC安装好winSCP软件；
- SC9600E设备；
- 串口线，带外口线连接好相应端口。

10.6.1 远程升级方法

适用场景

所有板卡在位且正常运行，此时通过网管命令远程升级。

升级前须知

- SC9600E支持整包自动升级，即如果主用主控盘MPU存在整包并稳定运行，插入的所有卡都将被自动刷新成该整包中的相应分包版本。
- 在设备上已存在升级好整包版本并生效的主控盘，只需要升级新插入单盘的场景中，插入新单盘会被自动升级并自动重启生效，无需手动升级和手动重启该单盘，在该单盘自动重启上线后，检查单盘版本信息即可。

升级步骤

1. 启动SC9600E设备，输入命令**interface mgt-eth 0/0/0**进入带外口配置视图后，再输入命令**ip address 192.168.1.200/24**配置交换机IP地址（此地址与PC网卡配置的IP地址属于同一网段即可）。

```
SC9600E(config)#interface mgt-eth 0/0/0
SC9600E(config-mgt-eth-0/0/0)#no shutdown
SC9600E(config-mgt-eth-0/0/0)#ip address 192.168.1.100/24
```

2. 输入命令**exit**退出带外口配置视图。

3. 输入命令**ping 192.168.1.200**查看交换机与PC是否能够互通。

4. 配置FTP服务器，设置好文件路径，用户名（123），密码（123）。

5. 将SC9600E_V370R240.bin文件放置到FTP软件配置的路径下。

6. 进入全局配置视图，使用用户名123/密码123登录192.168.1.200服务器，并从该FTP服务器上下载名为SC9600E_V370R240.bin的文件保存到本地设备上。

```
SC9600E(config)#ftp get 192.168.1.200 123 123 SC9600E_V370R240.bin
localfile SC9600E_V370R240.bin
Getting File “SC9600E_V370R240.bin ” from 192.168.1.200…
 643607522  bytes downloaded.
 If you want to upgrade system,use “upgrade” command!
SC9600E(config)#
```

7. 输入命令**upgrade os file SC9600E_V370R240.bin**进行交换机版本升级。

```
SC9600E-10(config)#up os file SC9600E_V370R240.bin
This operation will upgrade system file.Are you sure?(y/n) [y]y
System now is upgrading,please wait...Upgrading ...
Upgrading with whole packet...100%
Sys            Slot           Status
1                     13                Success.
Upgrading with whole packet...100%
Sys            Slot           Status
1                     14                Success.
```

8. 显示所有卡都升级成功后，使用**reboot**命令重启设备。

```
SC9600E(config)#reboot
   WARNING:System will reboot! Continue?(y/n) [y]y
```

10.6.2 业务验证

1. 升级版本后，设备能正常启动。

2. 正常启动后，登录设备，使用命令**show upgrade card-packet info**查看版本信息是否正确，主要观察Build time与升级时间是否一致。

```
SC9600E(config)#show upgrade card-packet info
Card packet information over local mpu :
Card slot               :13
Packet status           :Success
Packet information      :
Card type              :04000102
Packet name            :SC9600E_MPU_V370R240.bin
Build time             :2023-05-24-21:15:38
Card packet information over peer mpu:
```

```
Card slot                :14
Packet status            :Success
Packet information       :
Card type               :04000102
Packet name             :SC9600E_MPU_V370R240.bin
Build time              :2023-05-24-21:15:38
```

10.6.3 升级回退

如果要回退版本，按照上面的升级操作，通过远程升级或本地升级方法，重新升级为原始软件版本即可。

11 VPN 配置

本章介绍了SC9600E中VPN隧道管理的基本内容、配置过程和配置举例。

11.1 L3VPN 配置

11.1.1 L3VPN 配置

L3VPN由运营商经营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VPN网络，实现属于用户VPN的不同Site之间的通信。L3VPN的基本配置步骤如下：

1. 在P网络中配置IGP协议，及部署 LDP。
2. 在PE上为VPN客户创建VRF及指定RD，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。

L3VPN模块实现上述第二步骤，即L3VPN的VPN实例配置的相关内容。

11.1.1.1 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
创建VPN实例	1. 执行命令**configure**进入全局配置视图； 2. 执行命令**ip vpn-instance NAME**创建一条VPN实例。
删除VPN实例	1. 执行命令**configure**进入全局配置视图； 2. 执行命令**no ip vpn-instance NAME**删除一条指定实例名的VPN实例。

11.1.1.2 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置VPN实例的Route Distinguisher（RD，路由标识）	1. 执行命令**configure**进入全局配置视图； 2. 执行命令**ip vpn-instance NAME**创建一条VPN实例并进入VPN实例配置视图； 3. 执行命令**ipv4-family**或**ipv6-famil**y命令进入vpn-instance-af-ipv4或vpn-instance-af-ipv6配置视图； 4. 执行命令**route-distinguisher RD-STRING**配置VPN实例的Route Distinguisher。

注意：

路由标识没有缺省值，必须在创建VPN实例时配置。

11.1.1.3 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置VPN Target	1. 执行命令**configure**进入全局配置视图； 2. 执行命令**ip vpn-instance NAME**创建一条VPN实例并进入VPN实例配置视图； 3. 执行命令**ipv4-family**或**ipv6-family**命令进入vpn-instance-af-ipv4或vpn-instance-af-ipv6配置视图； 4. 执行命令**vpn-target TARGET (both | export-extcommunity | import-extcommunity)**。
删除当前VPN实例关联的所有VPN target	1. 执行命令**configure**进入全局配置视图； 2. 执行命令**ip vpn-instance NAME**创建一条VPN实例并进入VPN实例配置视图； 3. 执行命令**ipv4-family**或**ipv6-family**命令进入vpn-instance-af-ipv4或vpn-instance-af-ipv6配置视图； 4. 执行命令**no vpn-target**。
删除指定的VPN Target	1. 执行命令**configure**进入全局配置视图； 2. 执行命令**ip vpn-instance NAME**创建一条VPN实例并进入VPN实例配置视图； 3. 执行命令**ipv4-family**或**ipv6-family**命令进入vpn-instance-af-ipv4或vpn-instance-af-ipv6配置视图； 4. 执行命令**no vpn-target TARGET (both | export-extcommunity | import-extcommunity)**。

注意：

VPN Target没有缺省值，必须在创建VPN实例时配置。

11.1.1.4 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置VPN实例的描述信息	1. 执行命令**configure**进入全局配置视图； 2. 执行命令**ip vpn-instance NAME**创建一条VPN实例并进入VPN实例配置视图； 3. 执行命令**description DESCRIPTION**。
删除VPN实例的描述信息	1. 执行命令**configure**进入全局配置视图； 2. 执行命令**ip vpn-instance NAME**创建一条VPN实例并进入VPN实例配置视图； 3. 执行命令**no description**。

11.1.1.5 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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
配置接口与指定VPN实例绑定	1. 执行命令**configure**进入全局配置视图； 2. 执行命令进入VLANIF配置视图、Loopback接口配置视图； 3. 执行命令**ip binding vpn-instance NAME**。
取消接口与VPN实例的绑定	1. 执行命令**configure**进入全局配置视图； 2. 执行命令进入VLANIF配置视图、Loopback接口配置视图； 3. 执行命令**no ip binding vpn-instance NAME**。

注意：

- 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。
- 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。
- 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。
- 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。
- 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。

11.1.2 维护及调试

目的

当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，参数说明请参考《SC9600E系列交换机命令行手册》。

目的	步骤
显示VPN实例配置情况	1. 不执行任何命令保持当前特权用户视图，或执行命令**configure**进入全局配置视图；或在全局配置视图下执行命令**ip vpn-instance NAME**进入VPN实例配置视图； 2. 执行命令**show ip vpn-instance**。
显示VPN实例详细信息	1. 不执行任何命令保持当前特权用户视图，或执行命令**configure**进入全局配置视图；或在全局配置视图下执行命令**ip vpn-instance NAME**进入VPN实例配置视图； 2. 执行如下命令： ▶ **show ip vpn-instance verbose** ▶ **show ip vpn-instance VPN-INSTANCE-NAME verbose**
显示VPN实例配置信息	1. 不执行任何命令保持当前特权用户视图，或执行命令**configure**进入全局配置视图；或在全局配置视图下执行命令**ip vpn-instance NAME**进入VPN实例配置视图； 2. 执行命令**show ip vpn-instance import-vt TARGET**。
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**configure**进入全局配置视图；或在全局配置视图下执行命令**ip vpn-instance NAME**进入VPN实例配置视图； 2. 执行命令**debug l3vpn (io | event | error | nm | route | all)**。
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**configure**进入全局配置视图；或在全局配置视图下执行命令**ip vpn-instance NAME**进入VPN实例配置视图； 2. 执行命令**no debug l3vpn (io | event | error | nm | route | all)**。
使能或去使能L3VPN告警功能	1. 执行命令**configure**进入全局配置视图； 2. 执行命令**ip vpn-instance snmp-trap (enable | disable)**，使能或去使能L3VPN告警功能。

12 虚拟化配置

本章介绍了SC9600E中虚拟化配置的基本内容、配置过程和配置举例。

12.1 堆叠命令配置

12.1.1 堆叠命令概述

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，可以轻松自如地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ISS 系统，对ISS 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。

运行模式

堆叠设备有两种运行模式：独立模式和堆叠模式。独立模式和堆叠模式可以有条件的切换。模式切换会引起设备的重启。

独立模式下可以对堆叠参数进行预配置，这些配置在设备切换到堆叠运行模式后生效。

从独立模式切换到堆叠模式前，需要配置堆叠成员编号。

堆叠模式切换到独立模式会清除所有业务配置以及堆叠相关的配置；独立模式切换到堆叠模式会自动保存堆叠配置。

独立模式下运行的设备和普通的设备没有任何区别。设备只有在堆叠模式下才能和其余处在堆叠模式下的设备形成堆叠。

角色

堆叠中每台设备都是成员设备，成员设备根据功能不同分为两种角色：

- Master：负责管理整个堆叠。
- Slave：作为Master的备份设备运行。当Master故障时，系统会自动从Slave中选举一个新的Master接替原Master工作。

堆叠中的Master和Slave均由角色选举产生。一个堆叠系统中同时只能存在一台Master，其它成员设备都是Slave。

成员站点每次角色选举完成后，都要想平台通告站点的角色以执行配置文件。

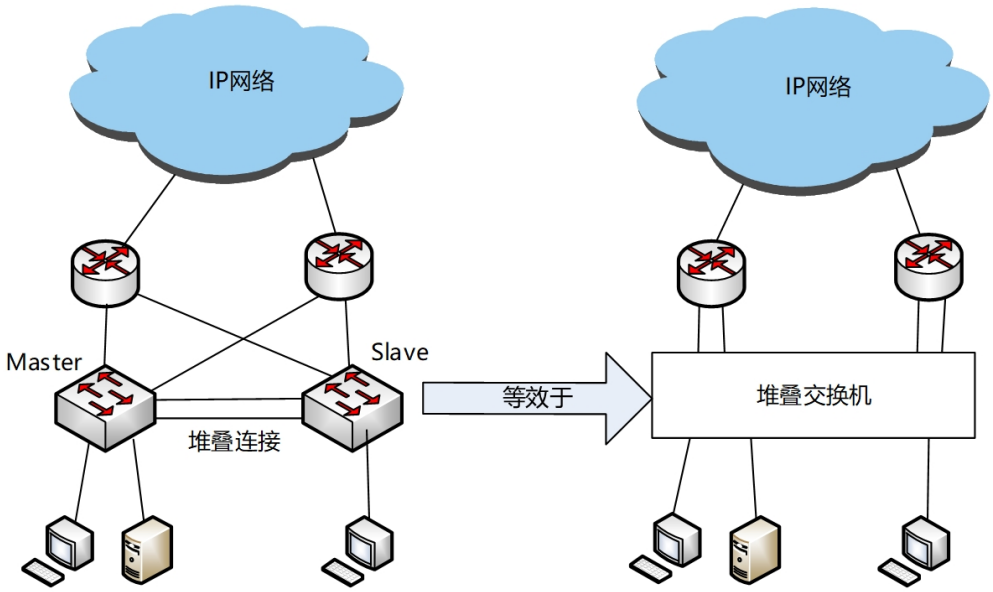


图 12-1 堆叠示意图

堆叠端口

堆叠系统中的成员设备通过堆叠端口进行连接，堆叠端口可以是专用堆叠端口或者是普通业务端口加入ISS聚合口后形成的堆叠端口（当前ISS版本使用后者实现）。

堆叠设备要进行拓扑连接至少需要一个堆叠端口，最多两个堆叠两个。两台成员设备通过堆叠连接组成的堆叠系统如下：

堆叠域

堆叠域ID相同的成员设备才能组成堆叠，设备在使能堆叠时设置默认的堆叠域ID，堆叠域ID是成员设备的一个配置属性。

成员编号

成员编号是成员设备的一个属性，堆叠模式下的每个成员设备都需要有一个唯一的成员编号。该成员编号须在独立模式切换到堆叠模式前先配置好。

独立模式下接口的索引如1/0/1的二维形式，设备切换到堆叠模式后，原来的接口索引增加一级，从1/0/1变成x/1/0/1，其中 x 就是站点成员编号。

此外，在堆叠模式下修改成员编号，须保存配置重启后才能生效。

成员优先级

成员优先级是成员设备的一个属性，主要用于角色选举过程中确定成员设备的角色。优先级越高当选为Master的可能性越大。

指定Maser

指定Master是成员设备的一个配置属性，用于指定某台设备优先被选为Master。

堆叠站点运行状态

成员站点的运行状态有：Init, Collection, Election, Loading和Done状态。

Init：设备的缺省值状态。

Collection：拓扑收集状态。

Election：选举状态。

Loading：配置文件同步状态。

Done：站点稳定运行状态。

堆叠系统状态

堆叠系统的状态分为up/down，当系统中的所有成员站点都为Done状态后，堆叠系统才为UP状态。只有在堆叠系统状态为UP后，才能进行除堆叠以外的业务配置。

12.1.2 堆叠工作原理

堆叠系统的形成

1. 物理连接

   堆叠成员设备之间通过堆叠端口连接，每个设备都有两个缺省的堆叠连接：堆叠连接 1 和堆叠连接 2 。如果设备使用专用堆叠口（如Higig口）则在系统初始检测到堆叠端口时设定堆叠连接，如果设备使用普通业务端口为堆叠端口，需要将普通业务口加入堆叠聚合口。堆叠模块内部记录为堆叠连接1或堆叠连接2。

2. 连接拓扑

   堆叠的基本拓扑结构为链形连接，如图 12-2所示。

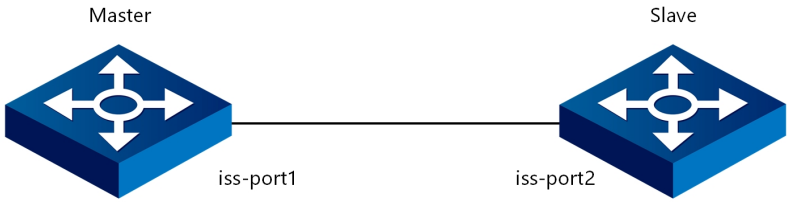


图 12-2 链形连接图

3. 堆叠端口协议状态的建立

堆叠设备通过堆叠口相连后，会互通keepalive报文，只有两端同时收到了对端的keepalive报文后，各堆叠口的协议状态才为up，才能进行hello报文的发送，进行拓扑收集阶段。

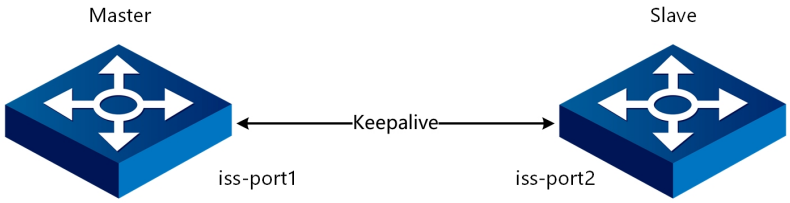


图 12-3 链形连接图

4. 拓扑收集

堆叠中每个成员设备都周期性地通过堆叠端口向所有堆叠成员发送hello报文，每个成员设备都根据收到的hello报文在本地记录收到的拓扑信息，hello报文中只携带自己的信息（域编号，成员编号、是否指定Master、优先级、运行时间和MAC地址等），发送hello报文时跳数设定为1，hello报文每经过一个成员跳数加1，每个成员收到hello报文后判断其源是否自己，如果是自己则终结，如果源不是自己则接收并更新自己的拓扑成员表，然后从另一个堆叠端口转发hello报文并增加报文中的跳数。在堆叠系统初始启动后，经过一段时间的拓扑收集，每个成员都可以得到整个拓扑结构的信息。

成员编号冲突处理在拓扑收集中，如果检测到其它站点和本地站点的成员编号冲突，则按照一定规则进行优先选择。未选择上的冲突站点的堆叠口将被shutdown，自动脱离堆叠系统。

被自动脱离的成员站点，只有等手工干预改变成员编号重启后，才能再次加入堆叠。

成员编号冲突的规则如下：

- 当前Master优于非Master成员
- 指定为Master的成员优先
- 成员优先级高的优先
- 系统运行时间长的优先
- MAC地址小的优先

5. 角色选举

堆叠系统在完成拓扑收集后进入角色选举阶段，根据角色选举原则选出一个Master，其他成员设备都是Slave。

角色选举的规则如下：

- 当前Master优于非Master成员
- 指定为Master的成员优先
- 成员优先级高的优先
- 系统运行时间长的优先
- MAC地址小的优先

6. 配置同步

   选举完成后，成员设备存在两种角色：Master和Slave。Master设备在选举完成后，master为slave导出或者合并配置文件，之后进入站点稳定运行的Done状态，并直接执行本地配置文件。

   Slave设备则需要从Master获取配置文件之后，将收到的配置文件与自己本地的配置文件相比较，如果本地配置文件是master传来配置文件的子集，则更新配置文件。在同步完成之前，站点一直处于Loading状态。在同步完成之后，站点进入done状态，并执行配置文件。

7. 堆叠系统进入稳定运行状态

   各Slave站点配置文件同步完成后依次进入Done状态。当堆叠系统中所有的站点均进入了Done状态后，整个堆叠系统进入稳定运行的UP状态。

   需要注意的是，堆叠系统未形成之前，不能进行除堆叠以外的业务配置。

堆叠系统的维护

堆叠系统的维护主要指堆叠拓扑发生变化时堆叠拓扑的更新及相应处理。

堆叠拓扑的变化主要有以下几种：

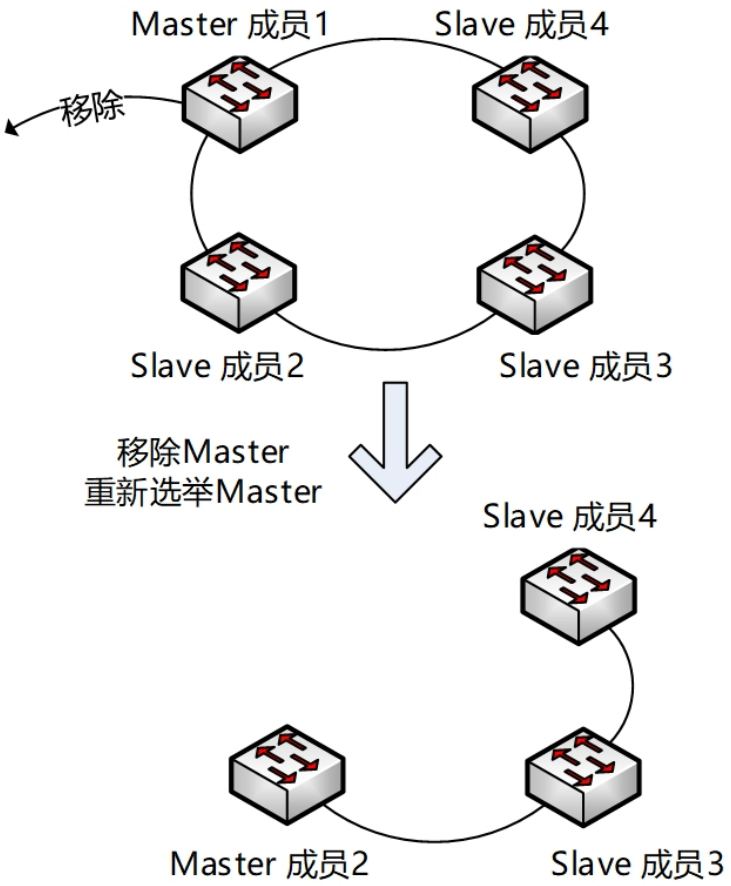
- Master成员的在线移除
- Slave成员的在线添加
- Slave成员的在线移除
- 堆叠的合并
- 堆叠的分裂

需要说明的是，成员站点的在线添加分两种：向已经稳定运行的堆叠系统添加Master站点和slave站点。其中前者按照堆叠的合并进行操作。

Master成员的在线移除

示例图如下所示，堆叠系统的master被移除后，系统重新进行拓扑收集和选举过程，选出新的master成员2。

由于上次Master相同，配置文件已经同步过，因此slave成员不需要重新进行配置同步：

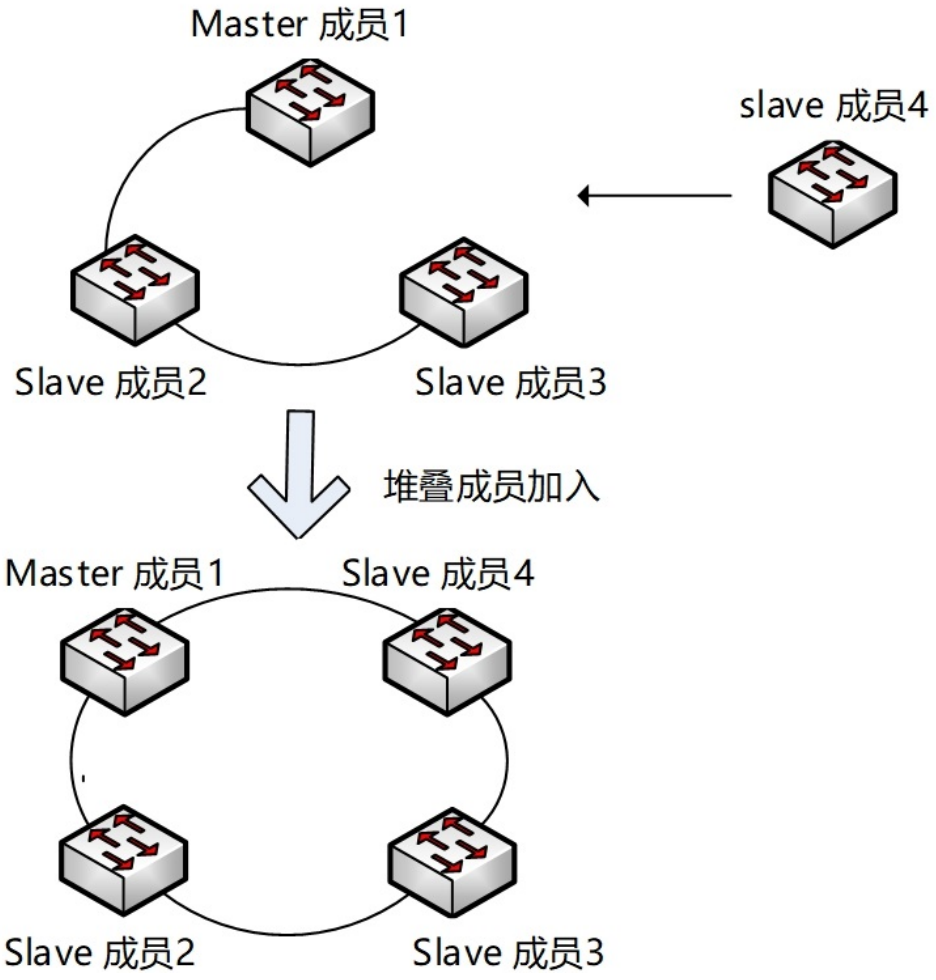


提示：

本系列设备只支持两台设备堆叠，原理图仅做参考。

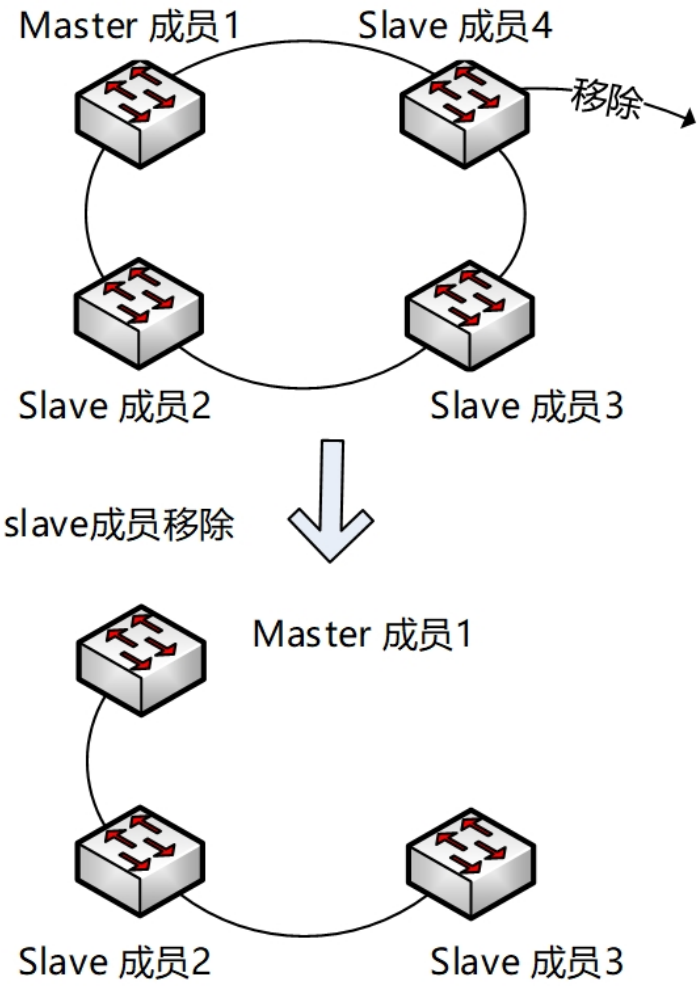
Slave成员的在线添加

示例图如下所示，向堆叠系统加入新站点slave成员4。新成员4加入系统的过程中，在经历了拓扑收集和选举后，还需要进行配置文件的同步。而对于堆叠系统中原有的Slave 成员2和成员3而言，master并未改变，不需要进行配置同步。



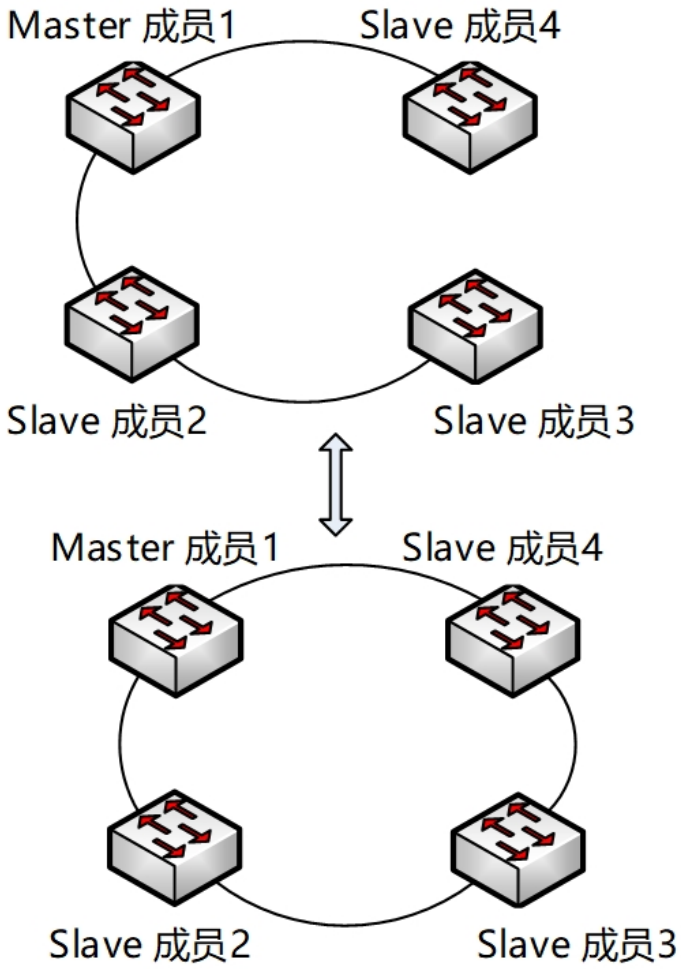
Slave成员的在线移除

示例图如下所示，slave成员4被移除后，其邻居节点master成员1和slave成员3刷新本地拓扑的同时，通过及时hello报文向全网通告链路的变化，其余站点通过该报文更新本地拓扑。



环型变链型拓扑/链型变环形拓扑

环形连接的堆叠系统在一条堆叠连接断开后变成链行连接，或者链型拓扑，将首尾站点相连后变成环形拓扑。在这个拓扑变化的过程中，系统会进行一次拓扑收集、选举的过程。这个过程中，master不会被改变，slave也不需要重新同步配置文件。堆叠系统依然保持正常的工作状态.

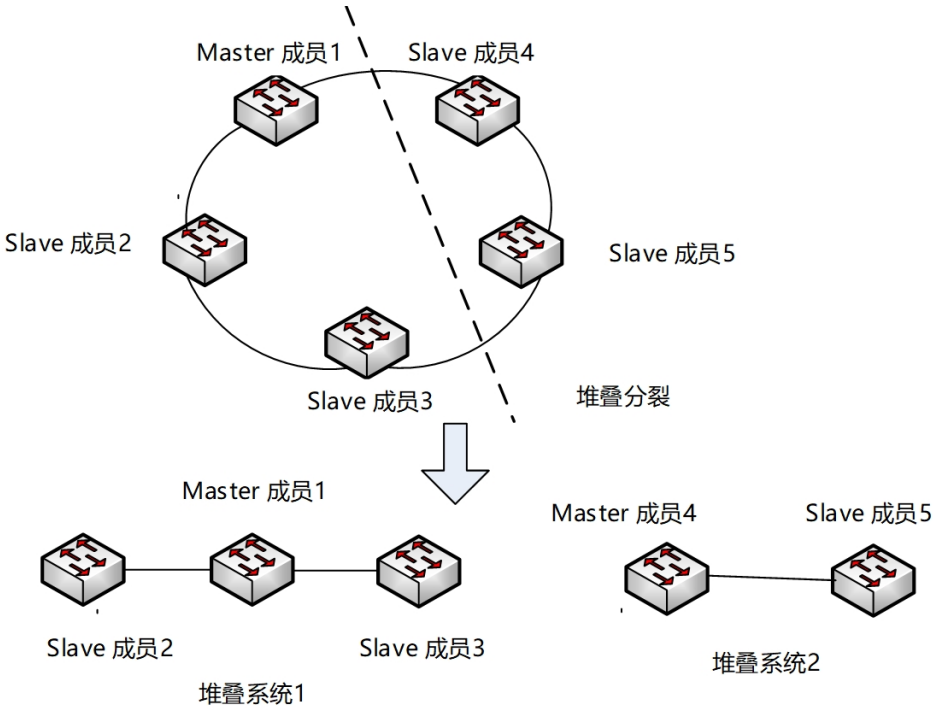


堆叠系统的分裂

链行连接的堆叠系统在一条堆叠连接断开或环形连接的堆叠在多于一条堆叠连接断开的情况下会分裂为两个独立的堆叠。这两个堆叠系统在各自形成自己的堆叠系统时会经历不同的处理过程。

以下图为例，原Master所在的堆叠系统1由于Master并未改变，系统依然正常运行。各成员站点只需重新进行一次拓扑收集和选举的过程，期间master并未被改变，slave也无须进行配置文件的同步。

而堆叠系统2则重新选举成员4为该系统的Master站点，对于slave成员5来说，master的改变则会引起该设备的重启，并进行一次针对堆叠系统2的slave成员在线加入操作。



应该要注意的是，两个独立的堆叠使用相同的系统配置（MAC/IP）可能会导致设备系统的异常，为解决这个问题，ISS堆叠提供了MAC/IP延时修改的功能：

当堆叠系统进行分裂时，如果堆叠系统的当前运行MAC不是其中一个成员站点的原始MAC，Master将会启动修改运行MAC定时器（延时时长默认30分钟），在延时的这段时间内，如果当前运行MAC的所属设备又回到了堆叠中，则关闭该定时器，不进行MAC的修改。如果定时器到时，则堆叠系统的运行MAC修改为Master的原始MAC。（Cisco支持配置堆叠虚拟MAC地址，即堆叠不使用master设备的MAC地址，用户配置使用虚拟MAC地址后系统自动从指定的MAC地址池中获取一个设置为堆叠MAC）。

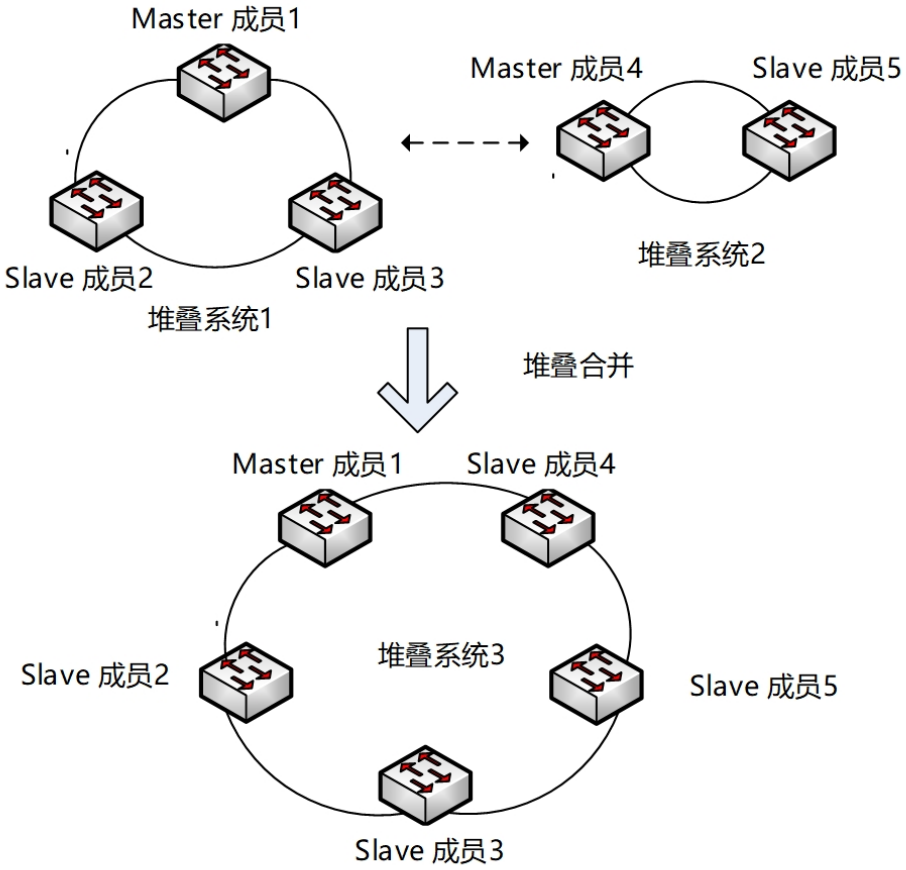
堆叠系统的合并

当两个独立的堆叠系统通过堆叠端口连接后进入堆叠合并，只有堆叠域ID相同的堆叠系统才能合并。新堆叠系统的形成需要经历拓扑收集，选举，设备重启，重新收集，选举等一系列过程。

堆叠的合并示意图如下，两个独立的堆叠系统1和堆叠系统2进行合并，形成新的堆叠系统3。在这个合并的过程中，原堆叠系统1和原堆叠系统2的成员在建立系统的过程中经历了不同步骤。

对于堆叠系统2而言，由于Master成员的改变，在经历了第一阶段的拓扑收集和选举过程后，成员将重启，即原Maste成员4和slave成员5将重启，重启后的设备将以slave成员在线添加的步骤加入堆叠系统3。

而对于堆叠系统1的所有成员而言，由于Master成员没改变，因此不需重启，只是需要经历由于堆叠系统2设备成员重启引起的两次拓扑收集和拓扑选举的过程。



12.1.3 配置链路拓扑

目的

配置链路拓扑。

过程

站点1的1号口与站点2的1号口相连。

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《SC9600E系列交换机命令行手册》。

站点	目的	步骤
站点1	设置memberId	1. 进入全局配置视图。 2. 执行命令 ◆ **SC9600E#conf** ◆ **SC9600E(config)#iss member 1**
	配置选举优先级	1. 进入全局配置视图； 2. 执行命令**SC9600E(config)#iss priority 3**
	使能堆叠口（站点1使能一个堆叠口）	1. 进入全局配置视图； 2. 执行命令 ◆ **SC9600E(config)interface stack-port 1** ◆ **SC9600E(config-stack-port-1) add xgigaethernet 1/0/48** ◆ **SC9600E(config-stack-port-1) no shutdown** ◆ **SC9600E(config-stack-port-1) quit**
	切换到堆叠模式（需重启，选择“Y”）	1. 进入全局配置视图； 2. 执行命令**SC9600E (config)#iss mode iss**
站点2	设置memberId	1. 进入全局配置视图。 2. 执行命令 ◆ **SC9600E#conf** ◆ **SC9600E(config)#iss member 2**
	配置选举优先级	1. 进入全局配置视图； 2. 执行命令**SC9600E(config)#iss priority 2**
	使能堆叠口（站点2使能一个堆叠口）	1. 进入全局配置视图； 2. 执行命令 ◆ **SC9600E(config-stack-port-1) add xgigaethernet 1/0/48** ◆ **SC9600E(config-stack-port-1) no shutdown** ◆ **SC9600E(config-stack-port-1) quit**
	切换到堆叠模式（需重启，选择“Y”）	1. 进入全局配置视图； 2. 执行命令**SC9600E (config)#iss mode iss**