CN9000/CN6000 系列
/S6820/S6550E/S6220/S5560V2/SC9606H 系列
配置指导手册

浪潮思科网络科技有限公司（以下简称“浪潮网络”）为客户提供全方位的技术支持和服务。直接向浪潮网络购买产品的用户，如果在使用过程中有任何问题，可与浪潮网络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网络产品的问题，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

客户投诉热线：　400-691-1766

公司总部地址：　山东省济南市历下区浪潮路 1036 号

邮政编码：　　250000

声　　明

此为 A 级产品，在生活环境中，该产品可能会造成无线电干扰。在这种情况下，可能需要用户对其干扰采取切实可行的措施。

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

前 言

概述

本文档系统介绍了三层以太网交换机设备支持的特性及其相关配置。主要内容包括基础配置、以太网、环网保护、IP 业务、IP 路由、可靠性、安全性、QoS、IPV6 等基本原理和配置过程，并提供相关的配置案例。在本文档的附录中，提供了该文档所涉及的术语和缩略语。

阅读本文档有助于读者系统掌握设备的原理和各种配置信息，以及如何应用该设备进行组网。

该手册适用于以下交换机系列型号，包括：

数据中心 CN9000 系列（含 CN9408H/CN9300-48Y8C/CN9008-48YC-S/CN9100-48X8C；不含 CN93240）、CN6000 系列（含 CN61108PC-V-H；不含 CN61108PC-V、CN6132、CN61108TC-V 等设备）

园区网 S6820 系列（S6820-24XQ-E）、S6550E 系列（含 S6550E-48T4X-C/S6550E-48TS4X-C/S6550E-48S4X-C）、S6220 系列（含 S6220-24TQ-S-PWR/S6220-48TQ-S-PWR/S6220-24TQ-S/S6220-48TQ-S/S6220-24S4X-S）、S5560V2 系列（含 S5560V2-48T4X-S/ S5560V2-48T4S-S/S5560V2-24T4X-S/S5560V2-24T4S-S/S5560V2-24TS-L-PWR/S5560V2-24T4X-HS）；园区网核心交换机 SC9606H

注：每款产品所支持特性有差异，具体请以产品实际支持功能为准。

版本更新说明

手册版本	更新说明
V1.0	手册第一次发行
V1.1	新增定时任务配置、PoE 配置功能、MAC 认证功能、堆叠配置；调整版式和风格

约定

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号	说明
	以本标志开始的文本表示有潜在危险，如果不能避免，可能导致人员伤害。
	以本标志开始的文本表示有潜在风险，如果忽视这些文本，可能导致设备损坏、数据丢失、设备性能降低或不可预知的结果。
	以本标志开始的文本是正文的附加信息，是对正文的强调和补充。
	以本标志开始的文本能帮助您解决某个问题或节省您的时间。

通用格式约定

格式	说明
宋体	正文采用宋体表示。
黑体	一级标题、二级标题、三级标题、Block 采用**黑体**表示。
楷体	警告、提示等内容用楷体表示。
“Lucida Console”格式	“Lucida Console”格式表示屏幕输出信息。此外，屏幕输出信息中夹杂的用户从终端输入的信息采用加粗字体表示。

命令行格式约定

格式	说明
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**粗体**表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从两个或多个选项中选取一个。
[x | y | ...]	表示从两个或多个选项中选取一个或者不选。

格式	说明
{ x | y | ... } *	表示从两个或多个选项中选取多个，最少选取一个，最多选取所有选项。
[x | y | ...] *	表示从两个或多个选项中选取多个或者不选。

目录

1 CLI 简介

1.1 命令行接口

命令行接口（Command Line Interface，简称CLI）为用户提供了可视化的交互界面，通过CLI界面的提示，用户可以在终端窗口输入特定的命令，查看输出的信息和配置结果。当用户成功访问设备后，界面如下所示：

```
**********************************************************************************
User Access Verification
Login: admin
Password: <password>
Inspur INOP Software, CN61108, Version 6.6.6.R1.34
Copyright (C) Inspur-Cisco Networking Technology Co. Ltd.    All rights reserved.
The current running image is flash:/boot/CN61108PC-V-H-48-4-6.6.6.R1.34.bin
Switch#

**********************************************************************************
```

1.2 命令模式

1.2.1 命令模式简介

设备提供了丰富的功能，不同的命令模式可以配置和查询不同的命令。根据功能对命令进行分类，当用户需要配置某个功能的某条命令时，需要先进入对应的命令模式。用户第一次登录设备时，会直接进入特权模式。在特权模式下（Switch#），用户可以通过**show**命令查看已配置的信息，以及其他未保存在设备中的命令。

设备支持多种方式登录设备，成功登录后可进入命令行接口界面，例如：

- Console口
- Telnet
- SSH

一般来说，不同的命令模式下可以配置的命令是有限的，但对于一些常用的命令可以在所有配置模式下使用，例如**end**、**exit**、**quit**等。

说明

当用户不清楚某命令模式可以支持的命令时，可以键入“？”获取想要了解的信息。更多详细信息可参照“CLI简介命令行在线帮助”。

1.2.2 全局配置模式

全局配置模式为用户提供多种命令的访问，该模式可以体现设备整体的特性或功能。用户可以在全局配置模式下输入特定的命令，对设备进行全局配置。也可以通过全局配置模式进入其他视图配置特定的元素，如接口或协议等。

表1-1 全局配置模式

命令	操作	说明
configure terminal	进入全局配置模式	该命令在特权模式下执行

当命令提示符由“switch#”变为“switch(config)#”时，表示成功从特权模式进入全局配置模式。

1.2.3 接口配置模式

全局配置模式下，可以进入接口配置模式。

表1-2 接口配置模式

命令	操作	说明
interface *interface-number*	进入接口配置模式	该命令在全局配置模式下执行

1.2.4 返回上一级命令模式

当前模式下的功能配置完成，使用 **quit** 可以退出当前模式返回到上一级模式。例如，全局配置模式下执行 **quit** 命令，可以退出至特权模式。

表1-3 返回上一级命令模式

命令	操作	说明
quit	从当前模式返回上一级命令模式	该命令可在任意模式下执行

1.2.5 返回特权模式

本命令为用户提供了一种从任意模式（非特权模式）返回到特权模式的快捷方式，而不需要多次执行 **quit** 命令逐级返回。用户也可以直接使用组合键<Ctrl+Z>从当前模式返回特权模式。

表1-4 返回特权模式

命令	操作	说明
end	返回特权模式	该命令可在任意的非特权模式下执行

1.3 命令行在线帮助

在输入命令时，用户可以在任意位置输入“？”以获得详尽的在线帮助。下面给出常见的在线帮助应用场景，供参考使用。

(1) 在任意视图下，输入“？”即可获取该视图下可以使用的所有命令及其说明。例如：

```
Switch# ?
Exec commands:
  boot          Specify boot parameter
  cd            System command cd
  clear         Reset functions
  configure     Enter configuration mode
  copy          Copy
  debug         Debugging functions
  delete        System command delete
  dir           System command ls
  disable       Turn off privileged mode command
  dot1x         IEEE 802.1X Port-Based Access Control
  enable        Turn on privileged mode command
  ethernet      Ethernet Configuration Commands
  exit          from the EXEC
  ftp           Use FTP to transfer file
  generate
  help          Description of the interactive help system
  l2            Layer 2 ping
  logging       Specify logging parameter
  logout        Exit from the EXEC
  ls            System command ls
  mkdir         System command mkdir
--More--
```

(2) 输入部分命令形式，使用空格分隔，再输入“？”。例如：

a.

```
Switch (config)# ftp password ?
  8        Specifies a hidden password will follow
  LINE     Password string
```

b.

```
Switch # dir ?
  flash:    Directory name or file name
  udisk:    Directory name or file name
  <cr>
```

此处的“<cr>”表示当前命令行是完整的，输入回车即可运行该命令。

(3) 输入命令的不完整关键字，其后紧接“？”，不需要空格，即可显示以该字符串开头的所有命令关键字及其帮助信息。例如：

```
Switch(config)# f?
fan                Fan speed configuration
flow               IPFIX flow information
flow-policer       Specify the number of flow policer resource
format             Format a filesystem
ftp                Specify FTP parameters
ftpd               FTP server
```

1.4 命令模式总结

主要的命令模式和功能特性如下表所示：

表1-5 命令模式总结

命令模式	提示符	进入命令	退出命令
特权模式	Switch#	与设备建立连接时即可进入该模式	**exit**/**quit** 可以退出登录，需要重新输入用户名/密码
全局配置模式	Switch(config)#	特权模式下键入 **configure terminal** 命令	**exit**/**quit** 返回特权用户配置视图
接口配置模式	Switch(config-if)#	全局配置模式下键入 **interface** *interface-number* 命令	**exit**/**quit** 返回全局配置视图

1.5 命令行输入

1.5.1 特殊字符

表1-6列出了具有特殊意义的字符。

表1-6 特殊字符

字符	说明
%	百分比
#	井号或数字
...	省略号
|	竖线
< >	小于或大于
[ ]	方括号
{ }	花括号

1.5.2 快捷键

表 1-7 列出了命令行的快捷键及功能。

表 1-7 快捷键

快捷键	功能
<Ctrl+A>	将光标移动至行首
<Ctrl+B>	将光标向左移动一个字符。当输入的命令超过一行时，可以反复按左键或<Ctrl+B>键
<Ctrl+C>	取消命令并返回到命令提示符
<Ctrl+D>	删除当前光标所在位置的字符
<Ctrl+E>	将光标移动到当前行的末尾
<Ctrl+F>	将光标向右移动一个字符
<Ctrl+H>	删除光标左侧的一个字符
<Ctrl+L>	重新显示当前的命令行
<Ctrl+N>	显示历史缓冲区中的下一条命令
<Ctrl+O>	清除终端屏幕
<Ctrl+P>	显示历史缓冲区中的上一条命令
<Ctrl+R>	重新显示当前行信息
<Ctrl+U>	删除从命令行开头至光标位置的所有字符

快捷键	功能
<Ctrl+W>	删除光标左侧连续字符串内的所有字符
<Ctrl+Z>	退回到特权视图
<Esc+B>	将光标移动到左侧连续字符串的首字符处
<Esc+D>	删除光标所在位置及其右侧连续字符串内的所有字符
上光标键<↑>	显示上一条历史命令
下光标键<↓>	显示下一条历史命令
左光标键<←>	光标向左移动一个字符位置
右光标键<→>	光标向右移动一个字符位置
?	显示可用命令的列表
<Tab>	输入不完整的关键字后按下<Tab>键，系统自动补全关键字： • 如果与之匹配的关键字唯一，则系统用此完整的关键字替代原输入并换行显示 • 如果与之匹配的关键字不唯一，则多次按<Tab>键，系统会循环显示所有以输入字符串开头的关键字 • 如果没有与之匹配的关键字，系统会不作任何修改，重新换行显示原输入

1.5.3 命令行的缩略形式

用户可以通过输入命令的前几个字符来缩略命令和关键词。使用的缩写必须包括足够的字符，能够与其他命令或关键词区别区分开来。如果在输入命令时遇到困难，请查看系统提示，并输入问号（?）以获得可用的命令列表。可以按<Tab>键由系统自动补全关键字的全部字符，确认是否为所需的关键字。

表1-8列出了命令行缩写形式的实例。

表1-8 命令行缩写形式

命令	缩写形式
configure terminal	**conf t**
show vrrp	**sh vr**
interface eth-0-1	**int eth-0-1**
show version	**sh ve**

1.6 命令的 no 形式

很多配置命令都有对应的 **no** 形式，命令的 **no** 形式一般可以用来恢复缺省情况、关闭某个功能或者删除某项设置。例如：

- 恢复缺省情况

添加接口到 VLAN 11 中：

```
Switch(config-if)# switchport access vlan 11
Switch(config-if)#
```

恢复接口到默认的 VLAN 1 中：

```
Switch(config-if)# no switchport access vlan
Switch(config-if)#
```

- 关闭某个功能

在端口上启用 VOICE VLAN 功能：

```
Switch(config-if)# voice vlan enable
Switch(config-if)#
```

关闭在端口上的 VOICE VLAN 功能：

```
Switch(config-if)# no voice vlan enable
Switch(config-if)#
```

- 删除某项设置

添加规则 1 至 VLAN 分类规则组 1：

```
Switch(config)# vlan classifier group 1 add rule 1
Switch(config)#
```

删除 VLAN 分类规则组 1：

```
Switch(config)# no vlan classifier group 1
Switch(config)#
```

1.7 命令行错误提示信息

命令行输入完毕后，键入Enter运行该命令，如输入的命令行形式正确，则不会弹出错误提示，命令执行成功；如果输入的命令行有误，则会根据错误的类型弹出不同的错误信息，常见的错误信息如表1-9所示。

表1-9 命令行常见错误信息表

英文错误信息	错误原因
% Unrecognized command found at '^' position.	命令无法解析，符号“^”指示位置出错
% Incomplete command found at '^' position.	符号“^”指示位置的参数输入不完整
% Ambiguous command found at '^' position.	符号“^”指示位置的关键字不明确，存在二义性
% Too many parameters.	输入过多参数
% Wrong parameter found at '^' position.	在符号“^”指示位置的参数错误

1.8 便捷地查看显示信息

1.8.1 分屏显示

1.控制分屏显示

当显示信息较多并超过一屏时，系统会将信息分屏显示，并在屏间显示“--More--”信息，表示这一屏信息已经显示完毕，自动暂停，方便查看显示信息。这时用户可以使用下表所示的按键来选择下一步操作。

表1-10 分屏显示功能表

按键	功能
空格键	继续显示下一屏信息
回车键	继续显示下一行信息
<Ctrl+C>	停止显示，退回到命令行编辑状态

特权模式下，也可以使用命令 terminal length screen-length用来设置用户终端屏幕的显示行数。screen-length的取值范围为0~512，“0”表示不限制屏幕显示行数。

2.关闭分屏显示功能

可以通过以下配置关闭当前登录用户的分屏显示功能。分屏显示功能处于关闭状态时，会一次显示

所有信息，如果信息较多，则会连续刷屏，不方便查看。

表1-11 关闭分屏显示

操作	命令	说明
terminal no length	关闭当前用户的分屏	此命令可以用来关闭当前用户的分屏显示功能。缺省情况下，系统默认不设置用户终端屏幕的显示行数。 重新登录后将恢复到缺省情况

1.9 查看历史命令

特权模式下，使用 **show history** 命令可以访问当前用户会话的命令历史，例如：

```
Switch# show history
    1 terminal length 40
    2 ter length 40

    3 terminal no length
    4 show history
    5 clear
```

设备保存历史命令时，遵循以下原则：

- 如果用户输入的命令为不完整形式，设备保存的历史命令也是不完整形式。例如，历史命令中的第二条“**ter length 40**”。
- 如果用户连续多次执行重复的命令，输入**show history**命令后，终端屏幕只显示一条命令。例如，连续多次执行 **terminal length 40** 命令， 设备只保存一条历史命令。但如果输入的命令本质为一条命令，但输入的形式不同（完整的命令与其缩写形式），设备会保存这两种形式的命令。例如，分别执行 **terminal length 40** 命令和它的不完整形式 **ter length 40**，设备将保存为两条历史命令。

2 登录设备方式介绍

设备支持 CLI（Console 口、Telnet、SSH）和 Simple Network Management Protocol（SNMP，简单网络管理协议）等登录方式：

- 通过CLI 登录设备后，可以直接输入命令行，来配置和管理设备。CLI 方式下又根据使用的登录接口以及登录协议不同，分为：通过Console 口、Telnet、SSH 登录方式。
- 通过 SNMP 登录设备后，网络管理员可以利用 SNMP 平台在网络上的节点检索信息、修改信息、发现故障、完成故障诊断、进行容量规划和生成报告。

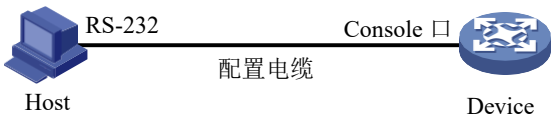
表 2-1 登录方式介绍

登录方式	简单描述
配置通过Console口本地登录设备	将交换机串口与PC或其他终端的串口相连，且PC或终端的串口配置与交换机串口默认配置一致
配置通过管理口登录设备	通过配置交换机管理口IPv4/IPv6地址登录设备
配置通过Telnet登录设备（具体可见“基础配置指导”的Telnet配置）	主要从以下四个方面介绍Telnet配置： • 开启设备的 Telnet 功能； • 通过带内口Telnet到其他交换机； • 通过管理口Telnet到其他交换机； • 交换机本身即是一个Telnet服务器
配置通过SSH登录设备（具体可见“基础配置指导”的SSH配置）	主要从以下三个方面介绍SSH配置： • 创建一个SSH key并进入相关配置模式； • 创建SSH 密匙、导入密匙； • 显示相关配置
配置通过SNMP登录设备	主要从以下五个方面介绍SNMP配置： • 启用SNMP服务 • 配置团体字符串 • 配置SNMPV3组 • 配置SNMPV1 / SNMPV2通告 • 配置SNMPV3通告

3 通过 Console 口登录设备

用户可以通过管理端口管理交换机。交换机有两类管理端口：以太网口和串口。通过串口登录设备是最基本的登录方式之一。Console口是一个异步串行端口，连接到这个端口的设备必须能够进行异步传输，如下图所示。

图3-1 将设备与PC 通过配置口电缆进行连接



3.1 Console 口初始配置

3.1.1 配置方法

缺省情况下，交换机的默认串口配置如下：

- 波特率为 **115200**
- 数据位为 **8**
- 停止位为 **1**
- 无奇偶校验
- 无流量控制

在配置交换机之前，请先确认已经将交换机串口与 PC 或其他终端的串口相连，且 PC 或终端的串口配置与上述交换机串口默认配置一致。当登录到交换机上后，可以修改串口配置参数。

表3-1 配置串口

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# line console 0	进入串口配置模式	-

命令举例	操作	说明
Switch(config-line)# speed 19200	设置串口波特率	-

说明

完成上述配置后，串口参数已经被修改，此时 PC 或终端无法再通过串口配置交换机。必须修改 PC 或终端的串口属性，将波特率从 115200 修改为 19200，才能够重新连上交换机进行配置。

3.2 串口配置模式下的应用

3.2.1 配置无活动的超时时间

表3-2 配置步骤

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# line console 0	进入串口配置模式	-
Switch(config-line)# exec-timeout 3200	设置用户无活动的超时时间	缺省情况下，默认 600 秒无操作会被强制退出；该配置在重新登录后生效

3.2.2 配置服务类型

表3-3 配置步骤

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# line console 0	进入串口配置模式	-
Switch(config-line)# transport input telnet	设置终端允许承载的服务类型	缺省情况下，默认支持所有服务类型，包括 SSH 服务、Telnet 服务

3.2.3 安全配置

表3-4 配置步骤

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# line console 0	进入串口配置模式	-
Switch(config-line)# access-class test in	设置终端绑定的 ACL 条目	该命令用到的 ACL 只能是 IPv4 访问控制列表

4 通过管理口登录设备

为了通过带外管理端口配置交换机，必须先通过串口为带外管理端口配置管理IP地址。

4.1 配置管理口

4.1.1 配置管理口 IPv4 地址

表4-1 配置步骤

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# management ip address 192.168.100.100/24	配置交换机管理口 IPv4 地址	-
Switch(config)# exit	退出全局配置模式	-

4.1.2 配置管理口 IPv6 地址

表4-2 配置步骤

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# management ipv6 address 2001:1000::1000/96	配置交换机管理口 IPv6 地址	-
Switch(config)# exit	退出全局配置模式	-

4.1.3 查看管理口 IPv4/IPv6 地址

表4-3 验证管理口IPv4/IPv6地址

命令	操作	说明
show management ip address	验证设置的管理口 IPv4 地址	-
show management ipv6 address	验证设置的管理口 IPv6 地址	-

完成上述配置后，可在命令行中输入“**show management ip address**” 或“**show management ipv6 address**”来查看配置的管理口 IP 地址。也可以通过 PC 执行 **ping** *ip-address* 指令来验证该 IP 地址。

显示交换机管理口 IPv4/IPv6 地址：

```
Switch# show management ip address
   Management IP address is:    192.168.100.100/24
   Gateway: 192.168.100.254
Switch# show management ipv6 address
   Management IPv6 address is:    2001:1000::1000/96
   Gateway: 2001:1000::1
Switch#
```

5 开启 HTTP/HTTPS 服务

5.1 HTTP/HTTPS 简介

Hypertext Transfer Protocol（HTTP），即超文本传输协议。HTTP 可以在互联网上传递页面信息，是互联网上应用最为广泛的协议。通过 Transmission Control Protocol（传输控制协议，TCP），客户端的浏览器能建立网络和服务器之间的连接，使浏览器的运行更加高效，极大地减少网络传输。

Hypertext Transfer Protocol Secure（HTTPS），即超文本传输协议的安全版本。HTTPS协议是由Secure Sockets Layer（SSL）和HTTP协议共同构建而来，可进行加密传输、身份认证的网络协议。与HTTP协议相比，HTTPS协议更加安全可靠，既可以保证数据传输的安全性，同时也能确认网站的真实性。

5.2 开启 HTTP 服务

表5-1 开 启 HTTP 服务

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# http server load flash:/webImage.bin	加载 WEB 镜像	使能 HTTP 服务需要先加载 WEB 镜像
Switch(config)# service http enable	开启 HTTP 服务	缺省情况下，HTTP 服务处于关闭状态
Switch(config)# http timeout 30	（可选）配置 Web 服务器的超时时间	缺省情况下，超时时间为 20 分钟
Switch(config)# http server source port 2000	配置 HTTP 服务器源端口	端口号的取值范围为 1025~65535

5.3 开启 HTTPS 服务

表5-2 开 启 HTTPS 服务

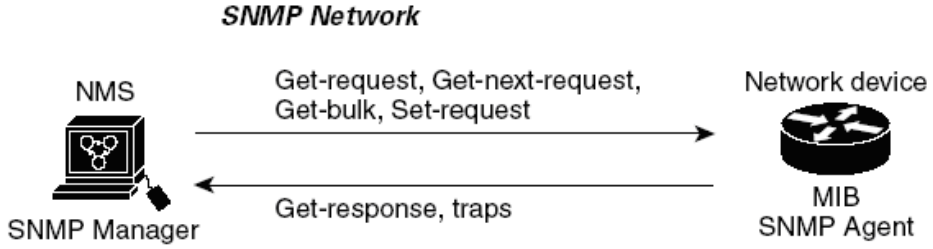
命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# http server load flash:/webImage.bin	加载 WEB 镜像	使能 HTTPS 服务需要先加载 WEB 镜像
Switch(config)# service https enable	开启 HTTPS 服务	缺省情况下，HTTPS 服务处于关闭状态

6 通过 SNMP 登录设备

6.1 SNMP 简介

SNMP是管理进程（NMS）和代理进程（Agent）之间的通信协议。它规定了在网络环境中对设备进行监视和管理的标准化管理框架、通信的公共语言、相应的安全和访问控制机制。网络管理员使用SNMP功能可以查询设备信息、修改设备的参数值、监控设备状态、自动发现网络故障、生成报告等。

图6-1 通过 SNMP 登录设备组网图



SNMP 具有以下技术优点：

- 基于 TCP/IP 互联网的标准协议，传输层协议一般采用 UDP。
- 自动化网络管理。网络管理员可以利用 SNMP 平台在网络上的节点检索信息、修改信息、发现故障、完成故障诊断、进行容量规划和生成报告。
- 屏蔽不同设备的物理差异，实现对不同厂商产品的自动化管理。SNMP 只提供最基本的功能集，使得管理任务与被管设备的物理特性和实际网络类型相对独立，从而实现对不同厂商设备的管理。
- 简单的请求—应答方式和主动通告方式相结合，并有超时和重传机制。
- 报文种类少，报文格式简单，方便解析，易于实现。
- SNMPv3 版本提供了认证和加密安全机制，以及基于用户和视图的访问控制功能，增强了安全性。

6.2 SNMP 参考

SNMP基于以下RFC：

SNMPv1：在RFC1157中定义

SNMPv2C：在RFC1901中定义

SNMPv3：在RFC2273至2275中定义

6.3 术语解释

以下简单描述了 SNMP 协议的条目和概念。

Agent: Agent 是网络设备中的一个应用模块，用于维护被管理设备的信息数据并响应 NMS 的请求，把管理数据汇报给发送请求的 NMS。Agent 接收到 NMS 的请求信息后，完成查询或修改操作，并把操作结果发送给 NMS，完成响应。同时，当设备发生故障或者其他事件时，Agent 会主动发送 Trap 信息给 NMS，通知设备当前的状态变化。

Management Information Base (MIB): 任何一个被管理的资源都表示为一个对象，称为被管理的对象。MIB 是被管理对象的集合。它定义了被管理对象的一系列属性：对象的名称、对象的访问权限和对象的数据类型等。每个 Agent 都有自己的 MIB。MIB 也可以看作是 NMS 和 Agent 之间的一个接口，通过这个接口，NMS 可以对 Agent 中的每一个被管理对象进行读/写操作，从而达到管理和监控设备的目的。

Engine ID: 缺省情况下，Engine ID 是由企业编号和默认的 MAC 地址组成的。对于管理域来说，Engine ID 在一个网络节点中具有唯一性，即每个设备都有一个专属 Engine ID。当 Engine ID 发生变化时，所有配置的用户和组也会被清除。

Trap: Trap 是 Agent 主动向 NMS 发送的信息，用于报告一些紧急的重要事件（如被管理设备重新启动等）。Trap 报文有两种：通用 Trap 和企业自定义 Trap。设备支持的通用 Trap 包括 authentication、coldstart、linkdown、linkup 和 warmstart 五种，其它均为企业自定义 Trap。企业自定义 Trap 由模块生成。因为 Trap 信息通常较多，会占用设备内存，从而影响设备性能，所以建议用户根据需要开启指定模块的 Trap 功能，生成相应的 Trap 报文。

6.4 启用 SNMP 服务

6.4.1 配置步骤

在全局配置模式下，启用 SNMP 服务。

表 6-1 开启 SNMP 服务

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# snmp-server enable	启用 SNMP 服务	缺省情况下，SNMP 功能默认为关闭状态
Switch(config)# end	退出全局配置模式	-

6.4.2 命令验证

表 6-2 查看当前所有配置

命令	操作	说明
show running-config	显示当前所有配置	–

显示当前所有配置：

```
Switch# show running-config
snmp-server enable
```

6.5 团体字符串配置

您可以使用 SNMP 团体字符串来定义 SNMP 管理者和代理之间的关系。团体字符串的功能类似于一串密码，允许用户访问代理交换机。您可以指定一个或多个团体字符。

- 一个 MIB 视图，它定义了所有给定团体可访问的 MIB 对象子集。
- 设置访问的 MIB 对象的读、写权限。

在特权模式下，按照下列步骤来配置交换机上的一个团体字符串，以下步骤配置完成后，就可以实现 SNMP 的基本读写功能。

6.5.1 配置步骤

表 6-3 配置团体字符串

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# snmp-server view DUT included 1	（可选）配置一个视图名字“DUT”	-
Switch(config)# snmp-server community public read-write (view DUT)	配置团体名字“public”读写权限，可访问的视图为“DUT”.括号内为可选字段	缺省情况下，未设置团体名
Switch(config)# end	退出全局配置模式	-

6.5.2 命令验证

查看当前配置：

```
Switch# show running-config

snmp-server enable
snmp-server view DUT included .1
snmp-server community public read-only view DUT
```

6.6 SNMPV3 组配置

您可以为 SNMP 服务器指定一个 (Engine ID)，创建一个 SNMP 组，在 SNMP 组中加入成员并设置权限。

在特权 EXEC 模式下，开始按照下列步骤操作，在交换机上配置 SNMP。

6.6.1 配置步骤

表 6-4 配置 SNMPV3 组

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch (config)# snmp-server engineID 8000123456	（可选）配置 Engine ID	-
Switch(config)# snmp-server usm-user usr1 authentication md5 mypassword	配置用户名和密码以及验证类型	要使配置的用户生效，必须要指定远程

命令举例	操作	说明
privacy des yourpassword		代理设备的 IP 地址或端口号
Switch(config)# snmp-server group grp1 user usr1 security-model usm	创建 SNMP 组	-
Switch(config)# snmp-server access grp1 security-model usm noauth	设置组内成员的权限	-
Switch(config)# end	退出全局配置模式	-

6.6.2 命令验证

查看当前配置：

```
Switch# show running-config

snmp-server engineID 8000123456
snmp-server usm-user usr1 authentication md5 mypassword privacy des yourpassword
snmp-server group grp1 user usr1 security-model usm
snmp-server access grp1 security-model usm noauth
```

6.7 SNMPV1/SNMPV2 通告配置

在特权 EXEC 模式下，按照下列步骤配置 SNMPV1 和 SNMPV2 通告。

6.7.1 配置步骤

表6-5 配置SNMPV1/SNMPV2通告

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# snmp-server trap enable all	开启所有 Trap	缺省情况下，默认关闭此功能
Switch(config)# snmp-server trap target-address 10.0.0.2 community public	配置目的 IPv4 地址以及团体名 Public	缺省情况下，默认无此配置
Switch(config)# snmp-server trap target-address 2001:1000::1 community public	配置目的 IPv6 地址以及团体名 Public	缺省情况下，默认无此配置
Switch(config)# end	退出全局配置模式	-

6.7.2 命令验证

显示当前配置：

```
Switch# show running-config

snmp-server trap target-address 10.0.0.2 community public
snmp-server trap target-address 2001:1000::1 community public
snmp-server trap enable vrrp
snmp-server trap enable igmp snooping
snmp-server trap enable ospf
snmp-server trap enable pim
snmp-server trap enable stp
snmp-server trap enable system
snmp-server trap enable coldstart
snmp-server trap enable warmstart
snmp-server trap enable linkdown
snmp-server trap enable linkup
```

6.8 SNMPV3 通告配置

6.8.1 配置步骤

表6-6 配置SNMPV3通告

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# snmp-server trap enable all	开启所有 Trap	缺省情况下，默认关闭此功能
Switch(config)# snmp-server notify notif1 tag tmptag trap	创建一个 Trap 消息条目	缺省情况下，默认无此配置
Switch(config)# snmp-server target-address targ1 param parm1 10.0.0.2 taglist tmptag	配置目的 IPv4 地址以及团体名 Public	-
Switch(config)# snmp-server target-address t1 param p1 2001:1000::1 taglist tag1	配置目的 IPv6 地址以及团体名 Public	-
Switch(config)# snmp-server target-params parm1 user usr1 security-model v3 message-processing v3 noauth	加入一个用户到 SNMP 组内	-
Switch(config)# end	退出全局配置模式	-

6.8.2 命令验证

查看当前配置：

```
Switch# show running-config

snmp-server notify notif1 tag tmptag trap
snmp-server target-address t1 param p1    2001:1000::1 taglist tag1
snmp-server target-address targ1 param parm1    10.0.0.2 taglist tmptag
snmp-server target-params parm1 user usr1 security-model v3 message-processing v3 noauth
snmp-server trap enable vrrp
snmp-server trap enable igmp snooping
snmp-server trap enable ospf
snmp-server trap enable pim
snmp-server trap enable stp
snmp-server trap enable system
snmp-server trap enable coldstart
snmp-server trap enable warmstart
snmp-server trap enable linkdown
snmp-server trap enable linkup
```

7 对登录用户的控制

通过引用访问控制列表（Access Control List，ACL），可以对访问设备的用户进行控制。主要应用于实现流识别、访问控制功能。

7.1 配置对 Telnet/SSH 用户的控制

7.1.1 配置准备

ACL 通过一系列的匹配条件对数据包进行分类，这些条件可以是数据包的源地址、目的地址、端口号等。

7.1.2 配置对 Telnet/SSH 用户的控制

表7-1 配置对 Telnet 用户的控制

命令	操作	说明
configure terminal	进入全局配置模式	-
telnet server acl *name*	过滤 Telnet client IP	缺省情况下，不过滤任何 Telnet client IP

表7-2 配置对 SSH 用户的控制

命令	操作	说明
configure terminal	进入全局配置模式	-
ssh server acl *name*	过滤 SSH client IP	缺省情况下，不过滤任何 SSH client IP

7.1.3 配置举例

1. 组网需求

通过源IP 对Telnet 进行控制，仅允许源IP地址为1.1.1.1 0.0.0.255帧通过，拒绝其他报文通过。

2. 配置步骤

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# mac access-list mac	创建并进入 MAC ACL 配置模式
Switch(config-mac-acl)# permit src-mac host 0000.0000.1111 dest-mac any	添加条目，设置允许源 MAC 地址为 0000.0000.1111 帧通过
Switch(config-mac-acl)# deny src-mac any dest-mac any	添加条目，设置拒绝任何 MAC 帧通过
Switch(config-mac-acl)# exit	退出 ACL 配置模式
Switch(config)# ip access-list ipv4	创建并进入 IPv4 ACL 配置模式
Switch(config-ip-acl)# permit any 1.1.1.1 0.0.0.255 any	添加条目，设置允许源 IP 地址为 1.1.1.1 0.0.0.255 帧通过
Switch(config-ip-acl)# deny any any any	添加条目，设置拒绝任何帧通过
Switch(config-ip-acl)# exit	退出 ACL 配置模式

7.2 配置对 NMS 的控制

7.2.1 配置准备

确定对 NMS 的控制策略，包括数据包的源地址、目的地址、端口号等。

7.2.2 配置对 NMS 的控制

表7-3 SNMP配置对 NMS 的控制

命令	操作	说明
configure terminal	进入全局配置模式	-
snmp-server access-group *name* **in**	在 SNMP 模块中应用 ACL 功能	缺省情况下，关闭 ACL 过滤访问控制功能

7.2.3 配置举例

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch# snmp-server enable	启用 SNMP 服务	缺省情况下，SNMP 功能默认为关闭状态
Switch(config)# snmp-server community newstring read-write	创建一个名为 newstring 的团体，该团体对 MIB 有读写权限	缺省情况下，未配置 SNMP 团体名
Switch(config)# snmp-server access manage security-model usm auth write _all_ read _all_	配置访问安全控制属性	缺省情况下，未配置访问控制
Switch(config)# snmp-server access-group abc in	在 SNMP 模块中应用 ACL 功能	缺省情况下，关闭 ACL 过滤访问控制功能

7.3 AAA 认证与授权功能

7.3.1 配置步骤

系统可以使用AAA认证的方法，验证访问网络和网络服务的用户。AAA认证方法有很多，如Tacacs+、Radius等认证方法可供用户选择。用户登录设备后，成功启用AAA认证方式，可设置鉴权方式和授权功能，如此便限制了命令行的使用，用户只能执行授权后的命令。具体配置的步骤可参考下表。

表7-4 AAA认证与授权功能

命令	操作	说明
configure terminal	进入全局配置模式	-
aaa new-model	启用 AAA 协议	使能 AAA 访问控制模块
aaa authentication login { **default** | *list-name* } { **enable** | **line** | **none** | **radius** | **local** | **tacacs-plus** }	设置 AAA 验证的模式	list-name 为鉴权方式链表名
aaa authorization exec { **default** | *list-name* } { **none** | **radius** | **local** | **tacacs-plus** }	设置 AAA 授权模式	list-name 为鉴权方式链表名

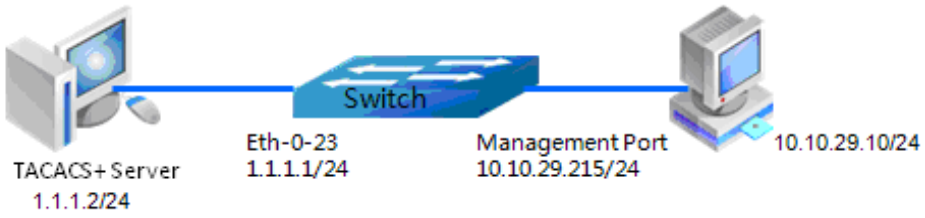
7.3.2 配置举例

1. 介绍

下图是TACACS+的网络拓扑。一台PC机作为 TACACS+服务器，配置网卡1.1.1.2/24。设置Switch的eth-0-23接口的IP地址为1.1.1.1/24。配置交换机的管理口IP地址为10.10.29.215，连接交换机管理口（仅限带内管理口）的PC机IP地址为10.10.29.10。

2. 组网图

图7-1 命令行授权配置组网图



3. 配置TACACS+服务器

步骤 1 下载 TACACS+服务器代码， DEVEL.201105261843.tar.bz2。

步骤 2 编译 TACACS+服务器代码。

步骤 3 修改配置文件，增加用户名和密码。

```
#!../obj.linux-2.6.9-89.29.1.elsmp-x86_64/tac_plus
id = spawnd {
        listen = { port = 49 }
        spawn = {
                instances min = 1
                instances max = 10
        }
        background = no
}
        user = aaa {
                password = clear bbb
                member = guest
        }
```

步骤 4 运行 TACACS+服务器程序。

```
[disciple: ~]$ ./tac_plus ./tac_plus.cfg.in -d 1
```

步骤 5 使用 **Ping** 命令检查连通结果。

```
C:\Documents and Settings\mac>ping 10.10.29.215

Pinging 10.10.29.215 with 32 bytes of data:

Reply from 10.10.29.215: bytes=32 time<1ms TTL=63
Reply from 10.10.29.215: bytes=32 time<1ms TTL=63
Reply from 10.10.29.215: bytes=32 time<1ms TTL=63
Reply from 10.10.29.215: bytes=32 time<1ms TTL=63

Ping statistics for 10.10.29.215:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

7.3.3 命令验证

使用 **show aaa status** 命令检查配置：

```
Switch# show aaa status

aaa stats:
      Authentication enable
```

使用 **show aaa method-lists authentication** 命令检查 AAA 配置：

```
Switch# show aaa method-lists authentication
authen queue=AAA_ML_AUTHEN_LOGIN
    Name = default    state = ALIVE :     local
Name = tac-login    state = ALIVE :     tacacs-plus local
```

7.4 AAA 认证与计费功能

系统可以使用 AAA 认证的方法去验证访问网络和网络服务的用户。TACACS+认证是 AAA 认证方法之一。TACACS+可以防止未经授权的访问，确保网络安全的分布式客户机/服务器系统。TACACS+为网络环境中广泛使用的协议。它通常用于嵌入式网络设备如路由器，调制解调器服务器，交换机等支持 TACACS+的路由器和交换机上运行的客户。客户端发送认证请求到 TACACS+服务器，TACACS+服务器包含所有的用户认证和网络服务访问信息。

7.4.1 配置步骤

表7-5 AAA认证与计费功能

命令	操作	说明
configure terminal	进入全局配置模式	-
aaa new-model	启用 AAA 协议	使能 AAA 访问控制模块

命令	操作	说明
aaa authentication login { **default** | *list-name* } { **enable** | **line** | **none** | **radius** | **local** | **tacacs-plus** }	设置 AAA 验证的模式	list-name 为计费方式链表名
aaa accounting exec { **default** | *list-name* } { **start-stop** | **stop-only** } { **radius** | **tacacs-plus** } [**none**]	设置 AAA EXEC 计费	list-name 为计费方式链表名; none: 前面计费方式失败则不计费（否则如果计费失败会强制用户下线）

7.4.2 配置举例

1. 介绍

客户端发送认证请求到TACACS+服务器，TACACS+服务器包含所有的用户认证和网络服务访问信息。

2. 组网图

图7-2 命令行计费配置组网图

3. 配置步骤

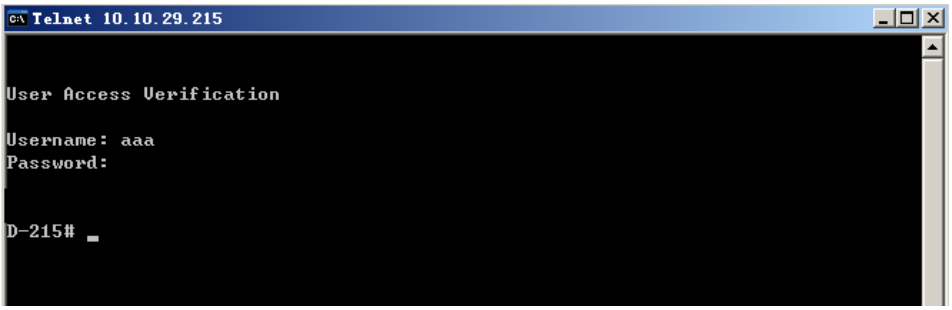
命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# tacacs-server host 1.1.1.2 port 123 key keyname	设置 TACACS+服务器的 IP 地址,验证端口和密码
Switch(config)# interface eth-0-23	进入接口模式
Switch(config-if)# no switchport	设置端口为三层端口
Switch(config-if)# ip address 1.1.1.1/24	配置 IP 地址
Switch(config-if)# quit	退出接口模式
Switch(config)# line vty 0 7	进入 VTY 模式
Switch(config-line)#login authentication tac-login Switch(config-line)#privilege level 4 Switch(config-line)#no line-password	配置验证方式

说明

TACACS+服务器的配置可参考配置举例。

7.4.3 显示结果

进行 Telnet 测试：如配置正确，则 Telnet 连接的结果信息类似下图所示。



基础配置指导目录

1 系统管理配置

1.1 MOTD 简介

每日提示（Message-of-the-Day，MOTD）信息和登录提示信息都是可配置的，可以显示给所有登录到系统的用户。如果某用户出现了不当操作可能影响到网上所有的用户，给该用户发送提示信息是非常有必要的，比如注销系统。登录提示信息会在终端用户登录到系统时显示。

1.2 配置提示信息

用户可以创建一个或多个提示信息，还可以配置登录 Banner、退出 Banner 以及显示当前配置。

1.2.1 配置每日提示消息

用户创建的提示信息会显示在已登录用户的终端上，可以通过以下步骤配置此功能。

表1-1 配置消息Banner

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# banner motd c message c	创建每日提示信息	指定相应的字符串，最多 255 个字符串
Switch(config)# exit	退出配置模式	-

1.2.2 配置登录提示消息

用户可以配置一条登录提示信息，以显示给所有登录到系统的用户，可以通过以下步骤配置此功能。

表1-2 配置登录Banner

命令举例	操作	说明
Switch# configure terminal	进入配置模式	-
Switch(config)# banner login c message c	配置登录提示信息	指定相应的字符串，最多 255 个字符串
Switch(config)# exit	退出配置模式	-

1.2.3 配置退出提示信息

用户可以配置一条 EXEC 模式的提示信息，以显示给所有登录到 EXEC 模式的用户，可以通过以下步骤配置此功能。

表1-3 配置退出Banner

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# banner exec c message c	配置一条 EXEC 模式的提示信息	指定相应的字符串，最多 255 个字符串
Switch(config)# exit	退出全局配置模式	-

1.2.4 查看提示信息

完成上述配置后，可以通过命令显示当前所有的配置。

表1-4 显示Banner信息

命令	操作	说明
show running-config	显示系统当前的配置	-

显示系统当前的配置：

```
Switch# show running-config
!
banner motd c message c

banner exec c message c

banner login c message c

!
--More--
```

1.3 配置主机名

除了设置登录信息外，用户可以根据自己的喜好设置交换机主机名，系统默认为 Switch。将主机名修改为独特的名称，用户可以从命令行界面的提示符中轻松识别设备。

1.3.1 配置方法

表 1-5 修改主机名

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# hostname sandbox	修改主机名为 sandbox	主机名必须符合 ARPANET 网络关于主机名的约定。包括英文字符，数字，连字号以及下划线。字数不能超过 64 个字符。

说明

如果用户需要恢复默认的主机名Switch，在全局配置模式下使用**no hostname**命令即可。

1.3.2 命令验证

修改主机名成功后，终端显示如下：

```
Switch (config)# hostname sandbox
sandbox(config)#
```

1.4 配置系统重启

用户可以使用命令重启系统，不仅可以直接重启，还能通过设置特定的时间来重启设备。

1.4.1 立即重启

表1-6 重启系统

命令举例	操作	说明
Switch# reboot	重启系统	重启系统前，请先保存好系统的配置。

1.4.2 配置系统重启时间

表1-7 配置系统重启时间

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# schedule reboot at 12:12 2021/12/25	指定系统重启的具体时间	缺省情况下，系统默认未设置重启时间。

说明

如果指定月份和日期，系统将在指定的月份和日期内的指定时间重启。如果没有指定月份和日期，系统将在当日的指定时间重启。

1.4.3 配置系统延迟重启时间

表1-8 配置系统延迟重启时间

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# schedule reboot delay 300	配置系统延迟重启的时间	缺省情况下，系统默认未设置延迟重启的时间。

2 用户管理配置

2.1 简介

用户管理功能可用来增加系统的安全性，用户可以通过密码来登录。系统会限制登录用户的数量。交换机上有三种模式登录：“no login”模式，任何人都可以直接登录交换机并且不需要密码；“login”模式，只有默认的用户登录；“login local”模式，假如用户想登录交换机，必须在系统中创建一个用户帐号。在本地创建用户帐号和密码可以帮助用户登录交换机。每个交换机只有 32 个账户。在用户启用本地账户验证之前，必须提前创建一个账户。

用户可以为每个用户名设置不同的密码。每个用户名不能超过 32 个字符。用户可以设置每个账户的等级，有效的等级为 1~4。只有一个账户可以进入配置模式。

2.2 配置用户等级

可以创建具有特权等级和密码的账户。

2.2.1 用户等级配置方法

表2-1 配置步骤

命令	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# line vty 0 7	进入 VTY 配置模式	-
Switch(config-line)# login local	设置验证模式	-
Switch(config-line)# exit	退出 VTY 配置模式	-
Switch(config)# username testname privilege 4 password 123abc<>	创建用户名和密码	设置账户特权等级，特权等级范围为 1~4
Switch(config)# exit	退出全局配置模式	-

2.2.2 命令验证

经过以上配置，登录交换机时，系统会提示类似如下验证信息：

```
Username: testname
Password:
```

2.3 配置用户管理

该配置可以使用不带用户名的密码登录设备。

2.3.1 配置登录密码

表2-2 配置步骤

命令	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# line vty 0 7	进入 VTY 配置模式	-
Switch(config-line)# login	设置验证模式	-
Switch(config-line)# line-password abc	设置登录密码为 abc	-
Switch(config-line)# end	退出 VTY 配置模式	-

2.3.2 命令验证

经过以上配置后，登录交换机时系统会提示类似如下的验证信息，用户可以使用之前创建的密码来登录交换机。

```
Password:
```

2.4 配置密码安全等级

2.4.1 配置方法

表 2-3 配置步骤

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

命令	操作	说明
cipher detect { **strong** | **normal** | **none** }	设置密码的安全等级	strong：密码必须包含数字，普通字符和自定字符；normal：密码必须包含数字和普通字符; none：关闭安全检查。

说明

本命令会清除所有等级不够强的密码。

2.4.2 命令验证

设置密码的安全等级为 strong：

```
Switch(config)#cipher detect strong
Switch(config)#
```

2.5 配置密码最小长度

2.5.1 配置方法

表2-4 配置步骤

命令	操作	说明
configure terminal	进入全局配置模式	-
cipher detect { **strong** | **normal** | **none** }	设置密码的安全等级	本命令会清除所有等级不够强的密码
cipher detect length *length-value*	设置安全等级为 normal 或者 strong 时密码的最小长度。	该命令配合 **cipher detect** 命令使用，在配置 **cipher detect** 模式为 normal 或者 strong 时该限制生效。

2.5.2 命令验证

设置安全等级为 normal 或者 strong 时密码的最小长度为 10：

```
Switch(config)#cipher detect length 10
Switch(config)#
```

2.6 配置密码有效周期

用户创建并配置该命令后，若管理员在配置时间内未修改密码，会导致密码超时无法使用。修改用户密码后重新开始计时。

2.6.1 配置方法

表2-5 配置步骤

命令	操作	说明
configure terminal	进入全局配置模式	-
username *WORD* **active-period** *time-value*	设置用户密码的有效周期	缺省情况下，未设置用户密码的有效周期

2.6.2 命令验证

设置用户名为testName的密码有效周期为129600分钟：

```
Switch(config)#username testName active-period 129600
Switch(config)#
```

2.7 配置登录失败最大次数及解锁方法

为了提高登录设备的安全性，用户可以配置允许登录失败的最大次数，以此来限制输入密码错误的次数。但是，用户配置该功能后，因为失误次数太多导致超过了配置的门限值，那么可能就需要用到以下办法来解锁。

2.7.1 配置登录失败最大次数

表2-6 配置步骤

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

命令	操作	说明
username *WORD* **retry-times** *times-value*	设置允许用户连续登录失败的最大次数	允许用户连续登录失败最大次数范围为 1~99；缺省情况下，系统未设置登陆失败的最大次数

2.7.2 配置锁定时长

当设置了允许登录失败的最大次数后，用户登录失败的次数超过配置的 retry-times，用户会被锁定。默认锁定时间是 30 分钟。如果用户在这之前设置了 lock-time，达到配置的锁定时长，就会解除锁定。

表2-7 配置步骤

命令	操作	说明
configure terminal	进入全局配置模式	-
username *WORD* **lock-time** *time-value*	设置用户登录失败被锁定后的时长	time-value 取值范围为 5~1440，单位：分钟；默认锁定时间是 30 分钟

2.7.3 配置快速解除锁定

如果用户配置了允许登录失败的最大次数，且用户登录失败次数超过了配置的上限，可以通过此配置快速解除锁定状态，减少等待时间。

表2-8 配置步骤

命令	操作	说明
configure terminal	进入全局配置模式	-
username *WORD* **unlock**	解除被锁定的用户	-

3 FTP 配置

3.1 FTP 简介

File Transfer Protocol (FTP)，即文件传输协议，在 FTP 服务器和FTP 客户端之间传输文件，是IP网络上传输文件的通用协议。

用户可从 FTP 服务器下载一个交换机配置文件，或从交换机上传文件到 FTP 服务器上。从 FTP 服务器下载一个交换机的配置文件以升级交换机的配置，只需用新的文件覆盖当前的启动配置文件即可。交换机配置文件上传到服务器可以起到备份作用，如后续需要，可下载到本交换机或者相同类型的交换机，以更新交换机的配置。

图3-1 FTP 组网应用示意图

窍门

在建立 FTP 连接前，请确保FTP 服务器与 FTP 客户端之间路由可达，否则，连接建立失败。

3.2 配置 FTP 服务器

当设备作为 FTP 服务器时，至少要开启 FTP 服务器功能，并配置FTP 服务器的认证和授权，其它命令请根据需要选择配置。

配置了FTP服务器的账号和密码后，用户有权进行FTP下载或上传配置文件，未配置的用户没有权限进行如下操作。默认的匿名用户不可以登录。

3.2.1 FTP 服务器基本配置

表3-1 FTP 服务器基本配置

命令	操作	说明
configure terminal	进入全局配置模式	-
service ftpd enable	启动 FTP 服务器功能	缺省情况下，FTP 服务器功能处于关闭状态
ftpd username *WORD* **password** [**8**] *LINE*	配置 FTP 服务器的账号和密码	配置”8”选项后，后面配置的密码必须为加密过的密码，否则配置失败。可以通过 **username secret** 命令来获取加密后的密码。配置用户后，在运行的 FTP Client 端输入相应的用户名及密码登入设备

3.3 配置 FTP 客户端

3.3.1 准备 FTP 下载或上传配置文件

用户可以复制或上传文件到 FTP 服务器。

FTP 协议要求 FTP 客户端每次发送 FTP 请求到服务器时都要包含远程用户名和密码。在用户开始使用 FTP 上传或下载一个配置文件前，必须完成以下操作：

1. 确保交换机到 FTP 服务器之间有一个可达路由。如果用户的网络中不存在子网间路由通信，交换机和 FTP 服务器就必须要在同一网络中，通过 **ping** 命令检查 FTP 服务器的连通性。
2. 如果用户正通过控制台或 Telnet 访问交换机，需确保当前的 FTP 用户名有效，是一个可以使用 FTP 下载功能的用户名。
3. 当用户上传配置文件到 FTP 服务器，用户必须正确配置 FTP 服务器以接受来自交换机用户的写请求。

i. 通过 FTP 下载配置文件

用户可以下载一个新的配置文件来覆盖当前的配置。

表3-2 FTP 下载配置文件（IPv4 组网环境）

命令举例	操作
Switch# configure terminal	进入全局配置模式
Switch(config)# ftp username test	（可选）创建一个用户“test”
Switch(config)# ftp password test	（可选）创建一个密码 “test”
Switch(config)# end	退出 EXEC 模式
Switch# copy mgmt-if ftp://test:test@10.10.10.163/ startup-config.conf flash:/startup-config.conf	从远程 FTP 服务器下载启动配置文件，用户名“test”，密码“test”
Switch# show startup-config	显示配置

表3-3 FTP 下载配置文件（IPv6 组网环境）

命令举例	操作
Switch# copy ftp://root: root@2001:1000::2/startup-config.conf flash:/startup-config.conf	从远程 FTP 服务器下载启动配置文件，用户名“root”，密码“root”
Switch# show startup-config	显示配置

ii. 通过 FTP 上传配置文件

用户可以从一个FTP服务器上传一个配置文件，稍后从这个交换机或其它交换机下载这个配置。

表3-4 FTP 上传配置文件（IPv4 组网环境）

命令举例	操作
Switch# configure terminal	进入全局配置模式
Switch(config)# ftp username test	（可选）创建一个用户“test”
Switch(config)# ftp password test	（可选）创建一个密码“test”
Switch(config)# end	退出 EXEC 模式
Switch# copy flash:/startup-config.conf mgmt-if ftp://test:test@10.10.10.163/startup-config.conf	向远程 FTP 服务器上传配置文件，用户名“test”，密码“test”

表3-5 FTP 上传配置文件（IPv6 组网环境）

命令举例	操作
Switch# copy flash:/startup-config.conf mgmt-if ftp://root:root@2001:1000::2 startup-config.conf	向远程 FTP 服务器上传配置文件，用户名“root”，密码“root”

3.3.2 操作FTP 服务器上的目录

当设备作为 FTP 客户端，与FTP 服务器成功建立连接后，在 FTP 服务器的授权目录下，用户可以进行创建、删除文件夹等操作。

表3-6 操 作 FTP 服务器上的目录

命令	操作	说明
dir [**flash:** | **udisk:**]	查看FTP服务器上的flash文件系统/USB存储设备的详细信息	如果系统没有USB存储设备。该命令将无法执行
ls [**flash:** | **udisk:**]		
more [**flash:** | **udisk:**]		
cd [**flash:** | **udisk:**]	切换FTP服务器上的工作路径	设置当前路径为flash或者USB
pwd	显示当前用户正在访问的FTP服务器上的路径	-
mkdir *directory*	在FTP服务器上创建目录	-
rmdir *directory*	删除FTP服务器上指定的目录	-

3.3.3 操作 FTP 服务器上的文件

当设备作为 FTP 客户端，与FTP 服务器成功建立连接后，在 FTP 服务器的授权目录下，用户可以通过以下操作，向FTP 服务器上传或从 FTP 服务器下载文件，推荐使用以下步骤：

(1) 使用 **dir** 或者 **ls** 命令了解 FTP 服务器上的目录结构以及文件所处的位置。

(2) 删除过时文件，以便有效利用存储空间。

(3) 设置传输模式。

(4) 进行上传/下载操作。

表3-7 操 作 FTP 服务器上的文件

命令	操作	说明
dir [**flash*:*** | **udisk*:***] **ls** [**flash*:*** | **udisk*:***] **more** [**flash*:*** | **udisk*:***]	查看FTP服务器上的flash文件系统/USB存储设备的详细信息	如果系统没有USB存储设备。该命令将无法执行
delete *file-name*	删除FTP服务器上的文件	-
ftp passive	显示当前用户正在访问的FTP服务器上的路径	-
rename *old-filename new-filename*	在FTP服务器上创建目录	-

3.3.4 更改登录用户

当设备作为 FTP 客户端，与 FTP 服务器连接建立成功后，可以更改登录用户。全局配置模式下，使用命令创建FTP用户和密码。

表3-8 更改登录用户

命令	操作	说明
ftp username *user-name*	为FTP用户创建用户名	用户名必须以字母开头，包括英文字母，数字和下划线，不多于31个字符
ftp password	为FTP用户创建密码	-

3.3.5 删除 FTP 用户名和密码

用户可以使用 **no** 形式的命令删除 FTP 用户名和密码。

表3-9 删除FTP用户名和密码

命令	操作	说明
no ftp username	删除 FTP 用户名	-
no ftp password	删除 FTP 密码	-

3.4 查看 FTP 相关配置

表3-10 查看FTP配置信息

命令	操作	说明
show ftp	查看FTP的配置信息	该命令直接在特权配置模式下执行

查看FTP的配置信息：

```
Switch# show ftp
ftp passive mode: on
ftp username: root
ftp password: unencrypted， abc
Switch#
```

4 TFTP 配置

4.1 TFTP 简介

Trivial File Transfer Protocol（TFTP，简单文件传输协议），是 TCP/IP 协议族中的一个用来在客户机与服务器之间进行简单文件传输的协议，提供不复杂、开销不大的文件传输服务。端口号为 69。

此协议是为小文件传输而设计的。因此它不具备许多常见的 FTP 功能，它只能从文件服务器上获得或写入文件，不能列出目录和进行认证，传输 8 位数据。

图4-1 TFTP 组网应用示意图

4.2 配置 TFTP 服务器

当设备作为 TFTP 客户端时，可以把设备的文件上传到 TFTP 服务器，还可以从 TFTP 服务器下载文件到设备。

4.2.1 TFTP 服务器基本配置

在进行上传下载之前，需要执行如下操作：

- 确保作为 TFTP 服务器的工作站配置正确。
- 确保 Switch 到 TFTP 服务器的路由可达。如果子网间不存在进行路由通信的路由器，交换机和 TFTP 服务器必须在同一网络中。**ping** 命令可以检查是否能连接到 TFTP 服务器。
- 确保要下载的配置文件在 TFTP 服务器上的正确目录下。
- 下载操作，确保该文件的权限设置正确。
- 上传操作，如果要覆盖服务器上现有的文件（包括空文件），确保该文件的权限设置正确。

表4-1 通过 TFTP 服务器下载文件

命令举例	操作
Switch# copy mgmt-if tftp://10.10.10.163/startup-config.conf flash:/startup-config.conf	指定 TFTP 服务器的 IPv4 地址以及相应的文件
Switch# copy mgmt-if tftp://2001:1000::2/startup-config.conf flash:/startup-config.conf	指定 TFTP 服务器的 IPv6 地址以及相应的文件
Switch# show startup-config	检查下载的文件

表4-2 通过 TFTP 服务器上传文件

命令举例	操作
Switch# copy flash:/startup-config.conf mgmt-if tftp://10.10.10.163/startup-config.conf	指定上传的文件以及服务器的 IPv4 地址
Switch# copy flash:/startup-config.conf mgmt-if tftp://2001:1000::2/startup-config.conf	指定上传的文件以及服务器的 IPv6 地址

5 Telnet 配置

5.1 Telnet 简介

Telnet 协议是 TCP/IP 协议族中的一员，是 Internet 远程登录服务的标准协议和主要方式。它为用户提供了在本地计算机上完成远程登录主机工作的能力。在终端用户的电脑上使用 Telnet 程序，用它连接到服务器。终端用户可以在 Telnet 程序中输入命令，这些命令会在服务器上运行，就像直接在服务器的控制台上输入一样。通过 Telnet 程序，用户在本地就能控制服务器。要开始一个 Telnet 会话，必须输入用户名和密码来登录服务器。Telnet 是常用的远程控制 Web 服务器的方法。

图5-1 通过设备登录到其他设备

5.2 配置 Telnet

此配置可以开启 Telnet 服务，可以让交换机访问网络上其他的设备。

5.2.1 Telnet 基本配置

步骤 1 通过带内口 Telnet 到其他交换机。

命令举例	操作
Switch# telnet 10.10.29.247	通过带内口 Telnet 到其他交换机（IPv4）
Switch# telnet 2001:1000::71	通过带内口 Telnet 到其他交换机（IPv6）

步骤 2 通过管理口 Telnet 到其他交换机。

命令举例	操作
Switch# telnet mgmt-if 10.10.29.247	通过管理口 Telnet 到其他交换机（IPv4）
Switch# telnet mgmt-if 2001:1000::2	通过管理口 Telnet 到其他交换机（IPv6）

步骤 3 交换机同样也是一个 Telnet 服务器。

命令举例	操作
Switch# configure terminal	进入配置模式
Switch(config)# service telnet enable	启用 Telnet 服务

表5-1 TFTP 服务器下载文件

命令举例	操作
Switch# copy mgmt-if tftp://10.10.10.163/startup-config.conf flash:/startup-config.conf	指定 TFTP 服务器的 IPv4 地址以及相应的文件
Switch# copy mgmt-if tftp://2001:1000::2/startup-config.conf flash:/startup-config.conf	指定 TFTP 服务器的 IPv6 地址以及相应的文件
Switch# show startup-config	检查下载的文件

表5-2 TFTP 服务器上传文件

命令举例	操作
Switch# copy flash:/startup-config.conf mgmt-if tftp://10.10.10.163/startup-config.conf	指定上传的文件以及服务器的 IPv4 地址
Switch# copy flash:/startup-config.conf mgmt-if tftp://2001:1000::2/startup-config.conf	指定上传的文件以及服务器的 IPv6 地址

5.2.2 命令验证

交换机访问网络上其他的设备：

```
    Switch# telnet mgmt-if 10.10.38.1

Entering character mode
Escape character is '^]'.
Switch #

    Switch# telnet 2001:1000::71

Entering character mode
Escape character is '^]'.
Switch #
```

6 SSH 配置

6.1 SSH 简介

安全 shell（SSH）是一种协议，可为用户提供一个安全环境，远程连接到设备。当设备进行远程访问时，SSH 提供了比 Telnet 更强大的加密功能，SSH 支持数据加密标准（DES）加密算法，三重 DES（3DES）加密算法，并且提供基于密码的用户认证。

图6-1 SSH系统应用

此配置可以开启 SSH 服务，进行远程访问。

6.2 配置 SSH 基本功能

表6-1 开启/关闭 SSH 服务

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# ip ssh server enable	开启 SSH 服务	缺省情况下，SSH 服务处于开启状态
Switch(config)# ip ssh server disable	关闭 SSH 服务	使用此命令关闭 SSH 服务

6.3 配置 SSH 认证

SSH 登录时所支持的认证方式包括密码认证方式、SSHv2 公钥认证方式以及 SSHv1RSA 认证方式。

6.3.1 配置 SSH 认证方式

表6-2 配置步骤

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# ip ssh server authentication-type password all	设置使用 SSH 登录时所支持的认证方式	缺省情况下，登录时支持所有认证方式

说明

当使用 SSH 协议进行登录时，在开始建立连接时会协商所使用的加密方式；如果某一端设置所使用的加密方式为 all，则协商的结果由对端所使用的加密方式来决定。

6.3.2 配置 SSH 认证失败次数

表6-3 配置步骤

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# ip ssh server authentication-retries 3	设置使用 SSH 登录时允许认证失败的次数	缺省情况下，允许认证失败的最大次数为 6 次

6.3.3 配置 SSH 认证超时时间

表6-4 配置步骤

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# ip ssh server authentication-timeout 100	设置无操作时系统断开连接的等待时间	缺省情况下，无操作时系统断开连接的等待时间为 120 秒

6.4 配置 SSH 源 IP 地址

表6-5 配置步骤

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# ip ssh server source address vrf vpn1 10.10.10.1	设置 SSH 服务器的源 IP 地址	该命令可以修改 SSH 服务器的源 IP 地址，指定提供 SSH 服务的 VRF。源地址只能是 loopback 口的地址或者 0.0.0.0，当配置为 0.0.0.0 表示不指定 IP 作为 SSH 服务器地址。

6.5 配置 SSH 源端口

6.5.1 配置带内 SSH 源端口

表 6-6 配置步骤

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# ip ssh server source port 2222	配置带内 SSH 服务器的源端口号	使用 **no ip ssh server source port** 会配置带内 SSH 服务器的源端口号为默认值 22

6.5.2 配置带外 SSH 源端口

表6-7 配置步骤

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# ip ssh server source mgmt-ifport 2222	配置带外 SSH 服务器的源端口号	使用 **no ip ssh server source mgmt-ifport** 会配置带外 SSH 服务器的源端口号为默认值 22

6.6 显示 SSH 会话信息

表6-8 查看 SSH 会话信息

命令举例	操作	说明
show ip ssh server session	查看 SSH 会话信息	-

查看当前的 SSH 会话信息：

```
Switch# show ip ssh server session
Version Encryption     Hmac          User        IP              State
=================================================================
2。0      aes128-cbc    hmac-md5      abc         10.10.29.22     Session started
```

6.7 配置 SSH 协议版本

设备支持的 SSH 协议版本包括 version 1 和 version 2，用户可以指定支持 version 1 或者 version 2，也可以配置两种版本都支持。

表6-9 配置 SSH 协议版本

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# ip ssh server version 1	设置 SSH 协议的版本	缺省情况下，设备使用 version 2 版本

说明

当使用 SSH 协议登录时，客户端和服务端在开始建立连接时会协商所使用的协议版本；如果协商失败，则不会建立连接；如果某一端设置所使用的 SSH 协议为 all，则协商的结果以对端所支持的 SSH 协议的最高版本来决定。

6.8 显示 SSH 配置信息

表6-10 查看 SSH 配置信息

命令	操作	说明
show ip ssh server status	查看 SSH 配置信息	-

查看 SSH 配置信息：

```
Switch# show ip ssh server status
  SSH server enabled
  Version: 1.99
  Authentication timeout: 33 second(s)
  Authentication retries: 6 time(s)
  Server key lifetime: 60 minute(s)
  Authentication type: password， public-key
```

6.9 创建 SSH 密匙

创建一个 key 并且进入 key 的自定义配置模式。

表 6-11 进入 RSA key 配置模式

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# rsa key key1	创建一个 key 并进入 key1 的自定义配置模式
Switch(config-rsa-key)#	成功进入 RSA key 配置模式

说明

此处创建的 keyname 应以字母开头，后可接数字，且不超过 32 个字符；否则会创建失败，出现如下错误提示“% Invalid key name: starting with alphabetic and can only include [0-9a-zA-Z.-_]. Its length range is [1, 32)”。

在 RSA key 配置模式下，可以配置 key 的格式（der 格式或 pem 格式）和类型（公匙或私匙）。

表 6-12 配置 key 的格式与类型

命令举例	操作步骤
Switch(config)# rsa key key1	进入 RSA key 配置模式
Switch(config-rsa-key)# key format der	设置生成的 key 的格式为 der 格式
Switch(config-rsa-key)# key type public	设置生成的 key 类型为公匙

表 6-13 退出 RSA key 配置模式

命令举例	操作步骤
Switch(config)# rsa key key1	进入 RSA key 配置模式
Switch(config-rsa-key)# key string end	退出当前 key 配置模式
Switch(config)#	退回至全局配置视图

以下表格列出了创建 SSH 密匙、导入密匙的操作步骤。

表 6-14 创建 SSH 密匙

命令举例	操作步骤
Switch# configure terminal	进入配置模式
Switch(config)# rsa key a generate	创建一个 key 并进入 key 的自定义配置模式
Switch(config)# rsa key a export url flash:/a.pri private ssh2	从 Flash 里面取一个 a.pri 私有 key
Switch(config)# rsa key a export url flash:/a.pub public ssh2	从 Flash 里面取一个 a.pub 公有 key

表 6-15 导入密匙

命令举例	操作步骤
Switch(config)# rsa key importKey import url flash:/a.pub public ssh2	导入一个 key 名字为 a.pub
Switch(config)# username aaa privilege 4 password abc	创建用户名为 aaa
Switch(config)# username aaa assign rsa key importKey	指定 SSH 用户名为 aaa

6.9.1 命令验证

在 SSH 客户端进行如下操作：

- 下载 a.pri key
- 加载交换机

```
[root@test1 tftpboot]# ssh -i a.pri aaa@10.10.39.101
aaa@10.10.39.101's password:
Switch#
```

6.9.2 显示密匙信息

i. 查看 key 的详细信息

命令	操作
show rsa key *keyname*	查看 key 的详细信息

查看 key1 的详细信息：

```
Switch# show rsa key KEY1
RSA key information:
============================================================
Name: KEY1
Type: private
Modulus: 1024 bit
Usage count: 0
Private key DER code:
30820258
      0201
         00
      028180
         9B3E9726 6405BD54 692F172A901F3879 C947366E 5703D282 AA31707F 214D38C9
Switch#
```

ii. 查看所有 key 的简要信息

命令	操作
show rsa keys	查看所有 key 的简要信息

显示所有 key 的简要信息：

```
Switch# show rsa keys
Name                                Type       Usage     Modulus
============================================================
key1                                private    0         1024
key2                                public     0         1024
Switch#
```

7 NETCONF SSH 配置

7.1 NETCONF SSH 简介

Netconf 功能的实现依赖于 SSH 提供的特定端口监听服务，默认 830 端口。通过控制 SSH 830 端口监听服务的开启/关闭实现 Netconf 功能。

图7-1 Netconf-SSH 系统应用

7.2 配置 NETCONF SSH

此配置可以启动 Netconf SSH 功能，使能端口监听服务。

7.2.1 NETCONF SSH 基本配置

表 7-1 启动/关闭 NETCONF SSH 监听服务

命令举例	操作
Switch# configure terminal	进入配置模式
Switch(config)# netconf ssh enable	使能 NETCONF 功能 SSH 监听服务
Switch(config)# netconf ssh disable	去使能 NETCONF 功能 SSH 监听服务

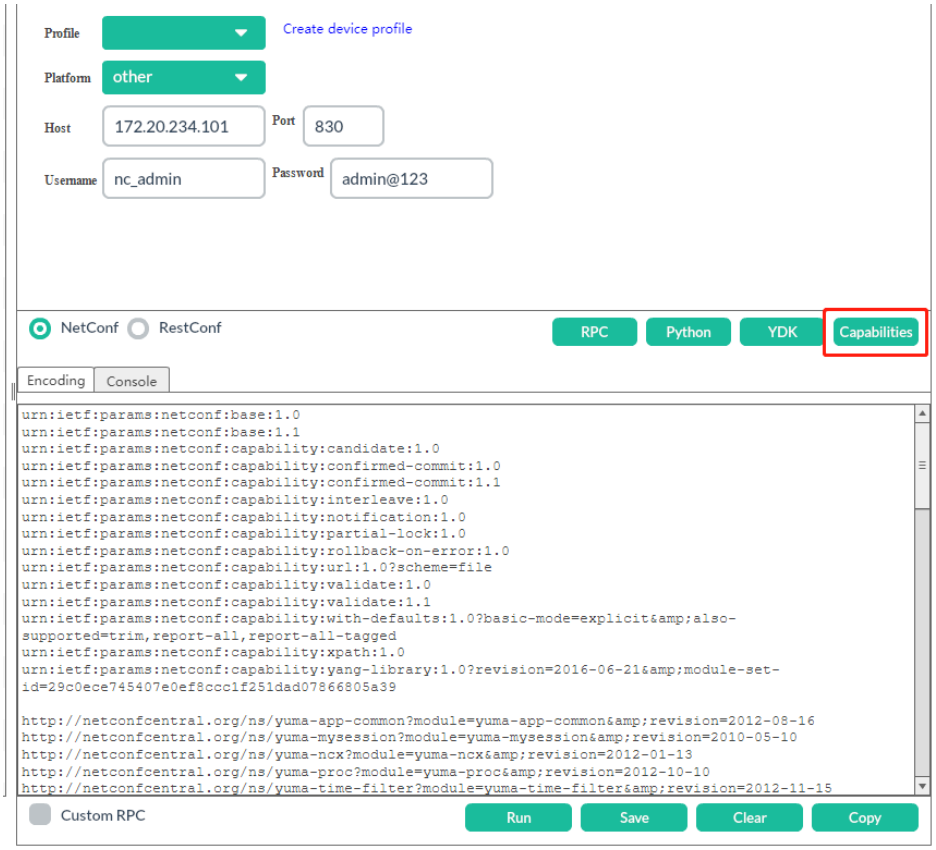
7.2.2 命令验证

查看 NETCONF SSH 监听功能状态：

```
router# show run | include netconf
router# config terminal
```

```
Enter configuration commands, one per line.   End with CNTL/Z.
router(config)# netconf ssh enable
router(config)# exit
router# show run | include netconf
netconf ssh enable
```

利用第三方工具 yang-explorer 可与交换机实现 NETCONF 协议通信：



7.3 配置 NETCONF 超级用户功能

7.3.1 基本配置

表7-2 启动/关闭 NETCONF 超级用户功能

命令举例	操作步骤
Switch# configure terminal	进入配置模式

命令举例	操作步骤
Switch(config)# netconf super-user admin	指定 NETCONF 管理功能超级用户为 admin
Switch(config)# no netconf super-user	关闭 NETCONF 超级用户功能

7.3.2 命令验证

如果开启了 NETCONF 管理超级用户的功能，可以查看当前配置：

```
router# show run | include netconf
netconf super-user admin
```

8 系统时间配置

8.1 简介

为了保证与其他设备协调工作，用户需要将系统时间设置准确。在没有其他外部时间源的情况下，您可以在系统启动后手动的设置时间和日期。如果您还有其他的同步时间的方式，比如网络时钟协议（Network Time Protocol，NTP），不建议您进行手动设置。

8.2 配置时间与时区

8.2.1 配置步骤

表 8-1 配置步骤

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# clock set datetime 11:30:00 10 26 2013	设置系统当前时间	缺省情况下，缺省为 UTC (Universal Time Coordinated) 时间，即协调世界时。在需要严格获取绝对时间的应用环境中，必须设定设备当前日期和时钟。
Switch (config)# clock set timezone ZZZ add 5	设置本地时区名称为 ZZZ，比 UTC 标准时间增加 5 小时	缺省情况下，缺省为 UTC 标准时间
Switch(config)# clock set summer-time dst date 6 1 2013 02:00:00 10 31 2013 02:00:00 120	设置夏令时的起止时间	缺省情况下，未开启夏令时功能。夏令时的第一部分用来说明起始时间和日期，第二部分用来说明结束时间和日期。所有的时间都是基于当前时区。开始时间是基于当前的标准时间，而结束时间是基于夏令时的。如果设置的开始时间大于结束时间，表示您处于南半球。
Switch(config)#exit	退出全局配置模式	-

命令举例	操作	说明
Switch# show clock detail	显示当前日期和时间的详细信息	-

8.2.2 命令验证

表 8-2 查看当前日期和时间的详细信息

命令	操作	说明
show clock detail	显示当前日期和时间的详细信息	-

显示当前系统的时间和日期：

```
Switch# show clock detail

13:31:10 dst Sat Oct 26 2013
Time zone: (GMT + 08:00:00)  beijing
Summer time starts at beijing 02:00:00  06/01/2013
Summer time ends at dst 02:00:00  10/31/2013
Summer time offset:  120 minutes
```

8.3 显示时区配置

表 8-3 查看所有时区

命令	操作	说明
show timezones	显示所有的时区	-

查看所有的时区：

```
Switch#show timezones
(GMT+00:06:04)      Europe/Andorra
(GMT+03:41:12)      Asia/Dubai
(GMT+04:36:48)      Asia/Kabul
(GMT-04:07:12)      America/Antigua
(GMT-04:12:16)      America/Anguilla
```

(GMT+01:19:20) Europe/Tirane
(GMT+02:58:00) Asia/Yerevan
(GMT-04:36:00) America/Curacao
(GMT+00:52:56) Africa/Luanda
(GMT+11:06:24) Antarctica/McMurdo McMurdo Station, Ross Island
==========
(GMT+00:00:00) Antarctica/South_Pole Amundsen-Scott Station, South Pole
(GMT-04:32:32) Antarctica/Rothera Rothera Station, Adelaide Island
(GMT-04:16:24) Antarctica/Palmer Palmer Station, Anvers Island

9 证书配置

9.1 简介

交换机的高级功能特性需要使用证书认证才可以使用，每台交换机有自己专属的证书来防止未授权的用户使用高级特性造成未知错误。一共有 3 类证书：Enterprise Base, Metro Service, and Metro Advanced。不同种类的证书包含不同的功能特性，用户可以根据需要来申请不同种类的证书。如果交换机没有证书，该交换机只能使用 L2 相关的功能特性。

不同的交换机不能共享同一份证书，为了能够获得指定交换机的证书，首先需要生成指定交换机的设备唯一标识符(UDI)， 将 UDI 发送给设备商来申请该交换机的证书。获得证书后将其应用到对应交换机上即可。

9.2 配置 UDI

9.2.1 创建 UDI

表 9-1 创建 UDI

命令举例	操作	说明
Switch# generate device identifier mgmt-if ftp://test:test@10.10.25.33/device.udi	为当前交换机创建 UDI 并且发送到 FTP 服务器上	该命令可以生成交换机的设备唯一标识符(UDI)，使用对应交换机的 UDI，可以向设备商申请该交换机可用的各类证书。

9.2.2 申请及使用证书

将UDI文件发送给设备商，设备商将根据客户需求来生成相应的证书并发送给客户。客户收到证书之后，使用时应注意：

- 必须重启交换机才能让证书生效。
- 如果交换机没有有效证书，只能使用 L2 相关功能特性
- 如果交换机有多张有效证书，则可以使用所有证书中包含的功能特性。

表 9-2 使用证书

命令举例	操作
Switch# copy mgmt-if ftp://test:test@10.10.25.33/device.lic flash:/device.lic	将证书从 FTP 服务器拷贝到本地
Switch# reload	重启系统

9.3 命令验证

表 9-3 查看证书

命令	操作
show license	查看交换机上的证书

显示交换机上的证书：

```
Switch# show license

License files:
============================================================================
flash:/ma.lic:
   Created Time: Fri Dec    6 17:22:23 CST 2013
   Vendor:             centec
   Customer:           centec
   Device MAC:       00:1E:08:09:03:00
   Feature Set:    QINQ MVR ERPS MEF ETHOAM
                         VPWS VPLS HVPLS SMLK TPOAM
                         OSPF PIM_SM IGMP VRF MPLS
                         LDP BGP RSVP OSPF_TE EXTEND_ACL
                         PTP BFD SSM IPV6 OSPF6
                         PIM_SM6 MVR6 RIPNG TUNNEL_V6
```

10 定时任务配置

10.1 定时任务简介

定时任务（KRON）功能可创建 KRON 策略，并进入 KRON 策略模式。在此模式下，允许用户使用 **command** 命令执行 EXEC 模式下的命令，并可以在指定的时间或周期内运行，也可以在系统启动时运行。不仅如此，用户还可以设置执行策略的次数，执行一次或者循环执行多次。

这一功能最初是为思科网络服务命令而设计的，现在有了更广泛的应用。使用思科网络服务的图像代理功能，处于防火墙外或使用网络地址转换（NAT）地址的远程设备可以使用该功能，在一定时间内启动 CLI，以更新设备中运行的图像。

定时任务功能的应用可以增强设备的可用性，使设备在无人看守的情况下运行自如。不仅增强了设备的控制性和可调节性，也起到了节能的作用。

10.2 配置定时任务

10.2.1 配置准备

执行这项任务前，需要先配置定时任务策略列表，再配置任务执行的周期，即运行的时间或间隔。

10.2.2 配置 KRON 策略

策略列表由一行或多行EXEC模式下的命令组成。当执行了**kron occurrence**命令后，所有策略中的命令都会被执行，对于在不同时间运行的CLI命令，需要使用单独的策略列表。用户无法编辑策略列表，需要按照配置的顺序运行。如果要删除一个条目，可以使用CLI命令的**no**形式进行删除，设备本身不检查命令的正确性，因此用户需要保证执行的 EXEC 命令是正确的。如果使用现有的策略列表名称，新条目会被添加到策略列表的末尾。要查看策略列表中的条目，可以使用 **show running-config** 命令。如果一个策略列表被安排运行的次数为一次，那么执行 **show running-config** 命令将不会显示该条目的信息。

10.2.3 执行 KRON 策略

在执行KRON策略之前，必须在路由设备上设置时钟时间。如果没有设置时钟时间，输入**kron occurrence**命令后，控制台屏幕上会出现一个警告信息：使用时钟命令或网络时间协议（NTP）来设置时钟时间。

如果在执行过程中，出现任何命令语法错误，所有策略列表将会被删除。比如，输入的**kron policy-list**命令关键字出错时，设备将停止执行该命令。

10.2.4 配置步骤

下表列出了周期保存交换机的配置，并通过管理口将配置文件发送至FTP服务器。

表 10-1 配置步骤

命令举例	说明
Switch# configure terminal	进入全局配置模式
Switch(config)# kron policy-list test	创建 kron policy 策略，并进入 kron policy 配置模式
Switch(config-kron-policy)# command write	首先执行命令为保存交换机配置
Switch(config-kron-policy)# command copy flash:/startup-config.conf mgmt-if ftp://admin:123456@10.69.65.112:21/startup-config.conf	然后在将 flash:/ startup-config.conf 文件通过管理口上传至 FTP 服务器。（该服务器用户名为 admin、密码为：123456，IP 地址为 10.69.65.112、端口号为 21、上传的文件保存至该 FTP 服务器中的名称为 startup-config.conf）
Switch(config-kron-policy)# exit	退出 kron policy 配置模式
Switch(config)# kron occurence policy-list test at 12:0 daily	配置执行周期为每天 12 点执行
Switch(config)# enable kron policy-list test	使能该 kron policy 策略

说明

若先使能 kron policy 后手动更改了交换机时间，需重新配置 kron policy 策略，建议设定完交换机时间后再进行 KRON 配置。

10.2.5 命令验证

表 10-2 查看 KRON 策略信息

命令	操作
show kron policy-list	显示配置的 KRON 策略信息

显示配置的KRON策略信息：

```
Switch# show kron policy-list

kron policy list count              : 1
kron policy list enable count : 1

kron policy list name          : test
kron policy list status       : enable
kron policy list rule          :
        rule 1                        : write
        rule 2                        : copy flash:/startup-config.conf mgmt-if
ftp://admin:123456@10.69.65.112:21/startup-config.conf
kron occurence rule recurring at 12:00 daily

Switch#
```

以太网配置指导目录

1 以太网接口配置

一般来说，交换机有两类管理端口：以太网口和串口。本章节主要介绍以太网接口的配置和功能，具体的接口类型和数量可参考相关的安装指导手册。

1.1 接口简介

以太网接口可以连接到终端或网络管理站（NMS）的网络端口，建立一个现场或远程配置环境。ETH 接口以 10/100/1000 Mbps 的速度工作，可以是全双工或半双工模式。Combo 端口是光电复用的，用户可根据实际组网情况选择其中一种模式使用，但两者不能同时工作，当激活其中一个端口时，另一个端口就自动处于禁用状态。当 Combo 端口在光口模式下工作时，配置速度或双工是无效的。

1.2 接口基本配置简介

表1-1 接口基本配置

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name 为接口名称，详情请参考 1.3 接口名称与编号
description *line*	配置端口的描述信息	描述信息 line 必须小于等于 64 个字符，字符类型必须是“0-9A-Za-z.-_”的格式
speed { **10** | **100** | **1000** | **auto** | **100G** | **10G** | **2G5** | **40G** | **5G** }	配置端口速率	缺省情况下，端口自动检测协商速率（auto）
duplex { **auto** | **full** | **half** }	配置端口的双工模式	缺省情况下，端口的双工模式为自协商模式（auto）
bandwidth *bandwidth-value*	配置端口带宽	端口带宽取值为 1~100000000，单位：kbps

命令	操作	说明
shutdown	配置端口为关闭状态	缺省情况下，端口为 UP 状态

1.3 接口名称与编号

通过输入 **interface** *if-name* 命令，不仅可以进入物理端口，还可以进入聚合端口、VLAN 端口、环回端口等多种形式的端口模式，如下表 1-2 所示。

表1-2 接口名称

接口名称	说明
eth	物理端口
agg	聚合端口
loopback	环回端口
vlan	VLAN 端口
tunnel	Tunnel 端口

if-name 由接口名称和接口编号组成，物理端口的接口编号一般以“-”符号相隔，例如“eth-0-1”，其中“0”表示槽位号，取值为 0；“1”表示端口号，取值为 1~54。

对于其他接口，后面直接加上接口编号即可（接口名称与接口编号之间允许有空格），进入相应接口配置模式的命令形式如下表所示：

表1-3 进入不同的接口配置模式

命令举例	操作
Switch(config)# interface eth-0-1	进入物理端口 eth-0-1
Switch(config)# interface agg1	进入聚合端口 agg1
Switch(config)# interface loopback1	进入环回端口 loopback1
Switch(config)# interface vlan1	进入 VLAN1 端口
Switch(config)# interface tunnel1	进入 Tunnel1 端口

说明

尽管接口的名称不同，但进入接口配置模式后的命令提示符均为 Switch(config-if)#。

1.4 接口基本配置举例

本小节详细介绍了以太网接口的基本配置，包括接口状态、接口速率与双工模式。

1.4.1 配置以太网接口状态

表1-4 接口状态

命令举例	操作
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# no shutdown	配置端口为 UP 状态
Switch(config-if)# interface eth-0-2	进入接口配置模式
Switch(config-if)# shutdown	关闭接口 eth-0-2
Switch(config)# end	退出

1.4.2 配置以太网接口速率

表1-5 接口速率

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-
Switch(config-if)# speed 100	设置接口 eth-0-1 速率为 100M	缺省情况下，端口自动检测协商速率
Switch(config-if)# no shutdown	配置端口为 UP 状态	-
Switch(config-if)# interface eth-0-2	进入接口配置模式	进入物理端口 eth-0-2
Switch(config-if)# no shutdown	配置端口为 UP 状态	-
Switch(config-if)# speed 1000	设置接口 eth-0-2 速率为 1000M.	缺省情况下，端口自动检测协商速率
Switch(config-if)# interface eth-0-	进入接口配置模式	-

命令举例	操作	说明
3		
Switch(config-if)# no shutdown	配置端口为 UP 状态	-
Switch(config-if)# speed auto	设置 eth-0-3 速率为自适应模式	-
Switch(config)# end	退出 EXEC 模式	-

说明

用户可设置的端口速率为 10Mb/s、100Mb/s、1000Mb/s、100Gb/s、10Gb/s、2.5Gb/s、40Gb/s、5Gb/s，默认为自动检测协商速率。但此命令不能在 10G 端口以及复用端口(combo port)上使用。

1.4.3 配置以太网接口双工模式

端口可配置的双工模式为全双工模式、半双工模式和自协商模式。如果用户设定端口双工模式为半双工模式，只能在 10M、100M 的端口上配置。

用户可以根据实际组网情况选择端口的双工模式，大致有以下三种情况可供参考：

- 当需要端口在发送数据包的同时可以接收数据包时，可以将端口设置为全双工（full）属性。
- 当需要端口同一时刻只能发送数据包或接收数据包时，可以将端口设置为半双工（half）属性。
- 当需要端口的双工属性由本端端口和对端端口自动协商决定时，可以将端口设置为自协商（auto）属性。

表1-6 接口双工模式

命令举例	操作
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# no shutdown	配置端口为 UP 状态
Switch(config-if)# duplex full	设置接口 eth-0-1 为全双工模式
Switch(config-if)# interface eth-0-2	进入接口配置模式

命令举例	操作
Switch(config-if)# no shutdown	配置端口为 UP 状态
Switch(config-if)# duplex half	设置接口 eth-0-2 为半双工模式
Switch(config)# interface eth-0-3	进入接口配置模式
Switch(config-if)# no shutdown	配置端口为 UP 状态
Switch(config-if)# duplex auto	设置接口 eth-0-3 为自适应模式
Switch(config-if)# end	退出 EXEC 模式.

1.4.4 查看接口状态

表1-7 查看接口状态

命令	操作
show interface status	显示所有物理端口的状态

查看所有物理端口的状态：

```
Switch# show interface status
Port          Status       Duplex     Speed      Mode       Type
------------------------------------------------------------
eth-0-1       up           full       a-1000     access     1000BASE_T
eth-0-2       up           half       a-100      access     1000BASE_T
eth-0-3       up           a-full     a-1000     access     1000BASE_T
Switch#
```

1.5 接口通用配置

本小节介绍 L2/L3 以太网接口的通用配置。

1.5.1 拆分以太网接口

当 40G 接口拆分为 4 个 10G 的接口使用时，可以提高端口密度，降低用户的使用成本，增强组网灵活性。不拆分时，40G 的接口也可以单独使用，拆分后的 4 个 10G 接口和一般的 10G 接口功能和特性大致相同。

i. 将接口拆分成4个10G接口

命令	操作
configure terminal	进入全局配置模式
split interface *if-name* **10giga**	将接口拆分成 4 个 10G 接口（在需要拆分的端口上配置一次即可）

ii. 将接口拆分成1个40G接口

命令	操作
configure terminal	进入全局配置模式
split interface *if-name* **40giga**	将接口拆分成 1 个 40G 接口

iii. 取消接口的拆分

命令	操作
configure terminal	进入全局配置模式
no split interface	取消接口的拆分

说明

配置接口拆分命令或者取消拆分命令后，需保存配置并重启才能生效。

1.5.2 配置允许长帧通过以太网接口

表1-8 配置允许长帧通过以太网接口

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	-
jumboframe enable	允许长帧通过以太网端口	缺省情况下，不允许长帧通过太网接口

说明

未配置该功能前，最大可以通过的报文的长度是 1632 字节。使能该功能后，端口上最大允许通过的报文长度为 9600 字节。

1.5.3 清除接口报文统计信息

在某些情况下，需要统计一定时间内某端口的流量，这就需要在统计开始前清除该端口原有的统计信息，重新进行统计。如果不指定端口类型和端口号，则清除所有端口的统计信息；如果仅指定端口类型，则清除所有该类型端口的统计信息。

表1-9 清除接口报文统计信息

命令	操作	说明
clear counters [*if-name*]	清除所有接口或指定接口的报文统计信息	该命令在特权模式下执行

1.6 接口批量配置

需要创建多个接口时，用户可键入此命令 **interface range** *if-name-number*，进入接口范围模式，批量创建多个接口，而不必一个一个地创建，可以节省时间，减少工作量。

下表以批量创建物理接口为例：

表1-10 接口批量配置

命令举例	操作	说明
Switch(config)# interface range eth-0-1 – 24	批量创建一系列物理接口，并进入接口范围模式	用“,”或“-”区分的界面范围集

2 三层接口配置

2.1 三层接口简介

系统支持以下三种类型的三层接口：

- VLAN 接口：为需要转发路由的流量，创建任意的 VLAN 接口。
- 路由端口：使用 **no switchport** 命令将物理端口切换为路由端口。
- 三层 link aggregation 端口：链路聚合接口，由路由端口组成。

每一个三层接口都至少会拥有一个 IP 地址，所有三层接口都需要一个 IP 地址进行路由配置，本章节描述了如何配置三层接口，以及如何分配一个 IP 地址到接口。

2.2 配置路由端口

下表描述了如何配置路由端口。

2.1.1 配置步骤

表2-1 配置步骤

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-
Switch(config-if)# no switchport	端口设置为三层接口	缺省情况下，端口为二层接口；当您使用该命令切换端口模式的时候，所有端口上原来的配置将会消失并且不能恢复。
Switch(config-if)# no shutdown	配置端口为 UP 状态	-
Switch(config-if)# ip address 1.1.1.1/24	配置 IP 地址为 1.1.1.1/24	-

命令举例	操作	说明
Switch(config-if)# end	退出 EXEC 模式	-

2.1.2 查看三层接口信息

表2-2 显示三层接口的信息

命令	操作	说明
show ip interface brief	显示三层接口的信息	-

显示三层接口的信息：

```
Switch# show ip interface brief

Interface              IP-Address      Status          Protocol
eth-0-1                1.1.1.1         up              up
Switch# show ip interface
Interface eth-0-1
  Interface current state: UP
  Internet address(es):
    1.1.1.1/24 broadcast 1.1.1.255
  Joined group address(es):
    224.0.0.1
  The maximum transmit unit is 1500 bytes
  ICMP error messages limited to one every 1000 milliseconds
  ICMP redirects are always sent
ICMP unreachables are always sent
  ICMP mask replies are always sent
  ARP timeout 01:00:00,  ARP retry interval 1s
  VRRP master of:  VRRP is not configured on this interface
```

2.3 配置路由端口子接口

下表步骤描述了如何配置路由端口子接口。

2.3.1 配置步骤

表2-3 配置步骤

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-
Switch(config-if)# no switchport	端口设置为三层接口	缺省情况下，端口为二层接口；当您使用该命令切换端口模式的时候，所有端口上原来的配置将会消失并且不能恢复。
Switch(config-if)# no shutdown	配置端口为 UP 状态	-
Switch(config-if)# subif 5 encapsulation-dot1q 5	进入子接口模式	该命令只能在三层 eth、agg 接口上配置
Switch(config-if)# ip address 11.11.11.11/24	配置子接口 IP 地址为 10.10.10.10/24	-
Switch(config-subif)# ip address 100.100.10.10/24 secondary	配置子接口 secondaryIP 地址为 100.100.10.10/24	-
Switch(config-subif)# ip vrf forwarding vpn1	配置子接口 VRF	-
Switch(config-subif)# exit-subif	退出子接口模式	-
Switch(config-if)# end	退出 EXEC 模式	-

2.3.2 查看子接口信息

表2-4 显示子接口的信息

命令	操作	说明
show interface *if-name* [**subif** *sub-number*]	显示接口 eth-0-1 上的子接口信息	-

显示接口 eth-0-1 上的子接口信息：

```
Switch# show interface eth-0-1 subif 5
```

```
Interface eth-0-1 subif 5
  Interface current state: UP
  Hardware is Subif, address is d886.0b00.09d5 (bia d886.0b00.09d5)
  Encapsulation-dot1q 5
  Bandwidth 1000000 kbits
  Index 16901 , Metric 1 , Encapsulation ARPA
  The maximum transmit unit (MTU) is 1500 bytes
  VRF binding: associated with vpn1
  VRRP master of :    VRRP is not configured on this interface
  ARP timeout 01:00:00,    ARP retry interval 1s
  ARP Proxy is disabled, Local ARP Proxy is disabled
```

2.4 配置 VLAN 接口

在一个以太网接口上可以配置多个虚拟 VLAN 接口，创建好的 VLAN 接口和物理接口功能相同，它们可以和物理接口一样进行配置和显示。动态路由协议，如：RIP、OSPF 和 BGP，都可以在整个网络使用 VLAN 接口。

2.4.1 配置步骤

表2-5 配置步骤

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	
Switch(config)# vlan database	进入 VLAN 接口配置模式	当要创建或删除一个 VLAN 时，必须首先使用该命令进入 VLAN 配置模式
Switch(config-vlan)# vlan 10	创建 VLAN 10	-
Switch(config-vlan)# exit	退出 VLAN 接口配置模式	-
Switch(config)# interface eth-0-2	进入接口配置模式	-
Switch(config-if)# switchport mode trunk	设置此接口的交换机特性为 trunk 模式	缺省状态下，接口的工作模式为 access
Switch(config-if)# switchport trunk allowed vlan all	将此端口加入所有 VLAN	-

命令举例	操作	说明
Switch(config-if)# no shutdown	配置端口为 UP 状态	-
Switch(config-if)# exit	退出接口配置模式	-
Switch(config)# interface vlan10	进入 VLAN 接口配置模式	-
Switch(config-if)# ip address 2.2.2.2/24	配置 IP 地址为 2.2.2.2/24	-
Switch(config-if)# end	退出 EXEC 模式	-

2.4.2 查看 VLAN 接口信息

表2-6 显示VLAN接口信息

命令	操作	说明
show ip interface brief	显示 VLAN 接口信息	-

显示 VLAN 接口信息：

```
Switch# show ip interface brief

Interface                IP-Address      Status          Protocol
vlan10                   2.2.2.2         up              up

Switch# show ip interface

Interface vlan10
  Interface current state: UP
  Internet address(es):
    2.2.2.2/24 broadcast 2.2.2.255
  Joined group address(es):
    224.0.0.1
  The maximum transmit unit is 1500 bytes
  ICMP error messages limited to one every 1000 milliseconds
  ICMP redirects are always sent
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are always sent
  ARP timeout 01:00:00,    ARP retry interval 1s
```

```
VRRP master of :    VRRP is not configured on this interface
```

3 接口 Errdisable 配置

3.1 接口 Errdisable 简介

Errdisable 是一种通过关闭异常接口来保护系统的机制。如果一个接口进入 Errdisable 状态，有两种方法可以从 Errdisabled 状态中恢复。方法一：配置 Errdisable 检测之前使能 Errdisable 恢复，配置接口在一定的时间之后自动恢复。但如果先发生 Errdisable，再使能 Errdisable 恢复功能，Errdisable 将不会自动恢复。方法二：在 Errdisable 接口上配置“**no shutdown**”命令。

接口链路状态的摆动抑制是一个潜在的硬件或线路问题造成的错误。管理员还可以配置接口的链路摆动抑制的检测条件。

3.2 配置 Errdisable 检测

3.2.1 配置举例

表3-1 配置举例

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# errdisable detect reason link-flap	使能检测链路摆动抑制 errdisable	缺省情况下，使能对端口的链路错误状态检测功能
Switch(config)# end	退出 EXEC 模式	-

3.2.2 查看 Errdisable 检测状态

表3-2 显示Errdisable检测状态

命令	操作	说明
show errdisable detect	显示 Errdisable 检测状态	-

显示Errdisable检测状态：

```
Switch# show errdisable detect

ErrDisable Reason            Detection status
-----------------            ----------------
bpduguard                      Enabled
bpduloop                       Enabled
link-monitor-failure         Enabled
oam-remote-failure           Enabled
port-security                Enabled
link-flap                    Enabled
monitor-link                 Enabled
udld                           Enabled
fdb-loop                     Enabled
loopback-detection           Enabled
reload-delay                 Enabled
```

3.3 配置 Errdisable 恢复

3.3.1 配置举例

表3-3 配置举例

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# errdisable recovery reason link-flap	使能链路震荡 Errdisable 恢复功能	缺省情况下，不使能链路震荡错误恢复功能
Switch(config)# errdisable recovery interval 30	设置从错误状态恢复的时间间隔为 30 秒	取值范围为 30~86400，单位：秒；默认时间间隔为 300 秒
Switch(config)# end	退出 EXEC 模式	-
Switch# show errdisable recovery	显示 Errdisable 恢复功能	-

3.3.2 查看 Errdisable 恢复

表3-4 查看Errdisable恢复功能

命令	操作	说明
show errdisable recovery	显示 Errdisable 恢复功能	-

显示 Errdisable 恢复功能：

```
Switch# show errdisable recovery

ErrDisable Reason            Timer Status
-----------------            --------------
bpduguard                    Disabled
bpduloop                     Disabled
link-monitor-failure         Disabled
oam-remote-failure           Disabled
port-security                Disabled
link-flap                    Enabled
udld                         Disabled
fdb-loop                     Disabled
loopback-detection           Disabled
Timer interval: 30 seconds
```

3.4 配置 Errdisable 摆动抑制

3.4.1 配置步骤

表3-5 配置步骤

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# errdisable flap reason link-flap 20 60	设置 Errdisable 最大链路震荡次数为 20 次、每秒钟可以震荡的次数为 60 次	缺省情况下，Errdisable 最大链路震荡的次数为 10 次，取值范围为 1~100；默认每秒可以震荡的次数为 10 次，取值范围为 1~120
Switch(config)# end	退出全局配置模式	-

3.4.2 查看 Errdisable 链路震荡信息

表3-6 显示Errdisable链路震荡信息

命令	操作	说明
show errdisable flap	显示 Errdisable 链路震荡信息	-

显示Errdisable链路震荡信息：

```
Switch# show errdisable flap
ErrDisable Reason            Flaps        Time (sec)
----------------             ------       ----------
link-flap                    20           60
```

3.5 控制接口进入 Errdisable 状态功能

管理员可以通过该命令来控制在接口发生 MAC flap 的时候是否进入 Errdisable 状态。

表3-7 配置方法

命令	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-
Switch(config-if)#no errdisable	配置接口发生 MAC flap 时，不进入 Errdisable 状态	缺省情况下，在指定的接口下执行该命令，发生 Mac flap 的时候该接口为开启状态
Switch(config-if)#errdisable	配置接口发生 MAC flap 时，进入 Errdisable 状态	

3.6 查看接口 Errdisable 状态

管理员可以通过两种命令来检查接口 Errdisable 状态，具体参照下面表格中的命令和配置说明。

表3-8 查看接口Errdisable状态

命令	操作	说明
show errdisable recovery	显示 errdisable 回复	-

命令	操作	说明
show interface status	显示接口状态	-

如果使能 Errdisable 恢复，命令行将显示恢复所剩时间，否则将显示没有恢复。

- 例1：使能Errdisable链路摆动抑制

```
Switch# show errdisable recovery
ErrDisable Reason            Timer Status
-----------------            --------------
bpduguard                    Disabled
bpduloop                     Disabled
link-monitor-failure         Disabled
oam-remote-failure           Disabled
port-security                Disabled
link-flap                    Enabled
udld                         Disabled
fdb-loop                     Disabled
loopback-detection           Disabled
Timer interval: 300 seconds
Interfaces that will be enabled at the next timeout:
Interface Errdisable Reason Time Left(sec)
--------- ----------------- --------------
eth-0-3     link-flap              25
```

- 例2：去使能Errdisable链路摆动抑制

```
Switch# show errdisable recovery

ErrDisable Reason            Timer Status
-----------------            --------------
bpduguard                    Disabled
bpduloop                     Disabled
link-monitor-failure         Disabled
oam-remote-failure           Disabled
port-security                Disabled
link-flap                    Disabled
udld                         Disabled
fdb-loop                     Disabled
loopback-detection           Disabled
```

```
Timer interval: 300 seconds
```

用户还可以使用接口状态命令来查看接口的 Errdisable 状态，该命令对接口的 Errdisable 状态有简短的描述。例如：

```
Switch# show interface status
Port          Status       Duplex     Speed      Mode       Type              Description
--------------------------------------------------------------------------------
eth-0-1       up           a-full     a-1000     TRUNK      1000BASE_SX
eth-0-2       down         auto       auto       TRUNK      Unknown
eth-0-3       errdisable a-full     a-1000     TRUNK      1000BASE_SX
eth-0-4       down         auto       auto       ACCESS     Unknown
```

4 MAC 地址表配置

4.1 MAC 地址表简介

Media Access Control（MAC），即媒体访问控制。MAC 地址表中包含交换机端口之间转发流量的地址信息，交换机可以根据地址表将数据帧传输到指定的主机中。如果 MAC 地址表中有数据帧的目标 MAC 地址对应的表项，则会通过该表项中的出接口将数据帧转发出去，即单播方式；反之，如果 MAC 地址表中没有数据帧的目标 MAC 地址对应的表项，则将该数据帧通过所属 VLAN 内除接收接口之外的所有接口转发出去，即广播方式。

4.1.1 MAC 地址表的分类

MAC 地址表包括的地址类型如下：

- 动态地址：由接口通过报文中的源地址学习获得，如果该地址在老化时间后未学习到，进入老化状态。
- 静态地址：由管理员手动添加源地址，表项不会老化。
- 黑洞地址：由用户手动配置，配置黑洞 MAC 地址后，源 MAC 地址或目的 MAC 地址是该 MAC 地址的报文则会被丢弃，表项不会老化。

4.1.2 参考

MAC 地址表参考以下标准文档：

IEEE 802.1D
IEEE 802.1Q

4.1.3 术语解释

以下是用来形容MAC地址表中的术语和概念的简要描述：

- **IVL**：独立VLAN学习：对于一个给定的VLAN，如果某个特定的MAC地址是在一个VLAN学习的，它不能被作为任何其他VLAN地址转发决策。
- **SVL**：共享VLAN学习：对于一个给定的VLAN，如果某个特定的MAC地址是在一个VLAN中学

习的，它可以作为任何其他VLAN地址转发决策。

说明

目前设备只支持独立 VLAN 的学习模式。

4.2 配置 MAC 地址表

本小节介绍了 MAC 地址表的相关配置步骤和验证方法，用户可以根据实际情况进行配置。

4.2.1 配置地址老化时间

地址老化时间不是精确的时间。如果老化时间设置为N，动态地址将在N - 2N间隔后老化。

i. 配置步骤

表4-1 配置步骤

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# mac-address-table ageing-time 10	设置动态地址老化时间为 10 秒	取值范围为 0，10~1000000，单位：秒，“0”表示 MAC 表不老化；默认的老化时间为 300 秒
Switch(config)# end	退出至 EXEC 模式	-

说明

如果没有连续地收到报文，用户可以增加老化时间的值使得设备能够保留更长的时间的动态条目。增加老化时间可以减少主机重复发送报文而引起广播风暴的可能性。

ii. 显示地址老化时间

表4-2 显示地址老化时间

命令	操作	说明
show mac address-table ageing-time	显示地址老化时间	-

查看地址老化时间：

```
Switch# show mac address-table ageing-time
MAC address table ageing time is 10 seconds
```

4.2.2 配置静态单播地址

单播地址表只能在一个端口上绑定。

i. 配置步骤

表4-3 配置步骤

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# mac-address-table 0000.1234.5678 forward eth-0-1 vlan 1	添加静态单播地址	通过该命令配置的静态条目不受老化时间限制
Switch(config)# end	退出至 EXEC 模式	-
Switch# show mac address-table	显示 MAC 地址表	-

ii. 显示单播MAC地址表

表4-4 显示单播MAC地址表

命令	操作	说明
show mac address-table	显示单播 MAC 地址表	-

查看单播 MAC 地址表：

```
Switch# show mac address-table
Mac Address Table
------------------------------------------
(*) - Security Entry
```

```
Vlan       Mac Address          Type         Ports
----        -------------       -------      --------
1          0000.1234.5678       static       eth-0-1
```

4.2.3 配置静态组播地址

组播地址可以绑定在多个端口上。

i. 配置步骤

表4-5 配置步骤

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# mac-address-table 0100.0000.0000 forward eth-0-1 vlan 1	在接口 eth-0-1 添加静态组播地址	通过该命令配置的静态条目不受老化时间限制
Switch(config)# mac-address-table 0100.0000.0000 forward eth-0-2 vlan 1	在接口 eth-0-2 添加静态组播地址	
Switch(config)# end	退出至 EXEC 模式	-

ii. 显示组播MAC地址表

表4-6 显示组播MAC地址表

命令	操作	说明
show mac address-table	显示组播 MAC 地址表	-

查看组播 MAC 地址表：

```
Switch# show mac address-table

    Mac Address Table
-------------------------------------------
(*) - Security Entry
Vlan       Mac Address          Type         Ports
----        -------------       -------      -------
1          0100.0000.0000        static       eth-0-1
                                              eth-0-2
```

4.2.4 配置 MAC 地址过滤

当用户启用了此功能，设备会对源 MAC 地址或者目的 MAC 地址进行过滤，丢弃特定的单播地址，停止转发。

i. 配置步骤

表4-7 配置步骤

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# mac-address-table 0000.1234.5678 discard	添加单播地址被丢弃	设备不支持组播 MAC 地址、广播 MAC 地址和路由 MAC 地址。转发到 CPU 上的报文同样不支持
Switch(config)# end	退出至 EXEC 模式	-

ii. 显示MAC地址过滤条目

表4-8 显示MAC地址过滤条目

命令	操作	说明
show mac-filter address-table	显示所有 mac-filter 的条目总数	-

查看所有 mac-filter 的条目总数：

```
Switch# show mac-filter address-table
        MAC Filter Address Table
----------------------------------
 Current count        : 0
 Max count            : 128
 Left count           : 128
 Filter address list :
----------------------------------
```

4.2.5 清除 MAC 地址条目

配置此命令，可以删除所有的动态（或静态或组播）条目或根据接口/MAC 位址/VLAN 删除部分动态(或静态或组播)条目。下面以删除特定 MAC 地址的动态条目为例。

表4-9 配置步骤

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch# clear mac address-table dynamic address 0008.0070.0007	删除特定 MAC 地址的动态条目	-
Switch(config)# end	退出至 EXEC 模式	-

5 VLAN 配置

5.1 VLAN 简介

传统的以太网以共享介质为基础，使所有的用户处于同一个广播域中，导致网络性能变差、冲突严重、广播泛滥等。通过部署交换式的以太网，可以解决冲突问题，但是对于广播风暴的控制、网络安全的提高和网络质量的提升，还需要使用虚拟局域网（Virtual Local Area Network，缩写：VLAN）技术。

VLAN 是将一个物理的 LAN 在逻辑上分割成不同广播域的通信技术，使数据包只能在被指定为同一个 VLAN 的端口之间进行交换。每个 VLAN 都可以被视为一个逻辑网络，目的地不属于同一个 VLAN 的数据包必须通过路由转发。

VLAN 技术具有以下优点：

- 有利于广播风暴的控制。一个物理的LAN划分为多个逻辑的VLAN,即一个VLAN享有一个广播域，不会影响其他VLAN,互不干扰。
- 有利于增强网络的安全性。由于用户处于不同的VLAN，报文传输时也是相互隔离的，无法和其他VLAN内的用户直接进行通信。
- 有利于网络的稳定性。故障发生时，一个VLAN内的故障不会影响到其他VLAN的使用。
- 有利于轻松地管理网络。网络管理员在管理网络时更加便捷，在短时间内使用命令建立一个工作组，各地的成员都可以灵活地使用VLAN网络。

5.2 配置 VLAN 的基本属性

5.2.1 进入/退出 VLAN 配置模式

表5-1 进入/退出VLAN配置模式

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-

命令举例	操作	说明
Switch(config)# vlan database	进入 VLAN 配置模式	当要创建或删除一个 VLAN 时，必须首先使用该命令进入 VLAN 配置模式
Switch(config-vlan)# exit	退出 VLAN 配置模式	-

5.2.2 配置 VLAN 特性

表5-2 配置VLAN特性

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# vlan database	进入 VLAN 配置模式	当要创建或删除一个 VLAN 时，必须首先使用该命令进入 VLAN 配置模式
Switch(config-vlan)# vlan 11	创建 VLAN 11	缺省情况下，默认为 VLAN 1，不可删除。所有接口默认都添加到 VLAN1 中
Switch(config-vlan)# vlan 11 name vlan11 state enable	（可选）创建 VLAN 11 并且命名为“vlan11”	
Switch(config-vlan)# vlan 100,200,300-400	添加 VLAN 序列 “100,200,300-400”	VLAN 序列以‘-’和‘,’符号相连接，VLAN 的值的范围在 1~4094 之间，并且 VLAN 序列的值需要符合升序的原则
Switch# exit	退出 VLAN 配置模式	-

5.3 配置 VLAN 桥功能

通过使用命令可以关闭特定 VLAN 上的桥功能，使该 VLAN 丢弃所有通过的二层报文。下面介绍了关闭/开启 VLAN 桥功能的方法。

表5-3 开启/关闭VLAN桥功能

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-

命令举例	操作	说明
Switch(config)# vlan database	进入 VLAN 配置模式	当要创建或删除一个 VLAN 时，必须首先使用该命令进入 VLAN 配置模式
Switch(config-vlan)# vlan 2 bridge disable	关闭 VLAN 2 上的桥功能	VLAN 标识取值范围为 1~4094；默认情况下，VLAN 上的桥功能处于开启状态
Switch(config-vlan)# no vlan 2 bridge disable	开启 VLAN 2 上的桥功能	

5.4 配置 VLAN 流量统计功能

在 VLAN 配置视图下，可以使能 VLAN 流量统计功能，可以统计经过特定 VLAN 的报文总个数。用户还可以配置 VLAN 统计报文的间隔时间。

5.4.1 开启/关闭 VLAN 流量统计功能

表5-4 开启/关闭VLAN流量统计功能

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# vlan database	进入 VLAN 配置模式	当要创建或删除一个 VLAN 时，必须首先使用该命令进入 VLAN 配置模式
Switch(config-vlan)# vlan 2 statistics enable	使能 VLAN 2 上的统计功能	缺省情况下，VLAN 流量统计功能处于关闭状态
Switch(config-vlan)# no vlan 2 statistics enable	去使能 VLAN 2 上的统计功能	

5.4.2 配置 VLAN 流量统计间隔时间

表5-5 配置VLAN流量统计间隔时间

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-

命令举例	操作	说明
Switch(config)# vlan database	进入 VLAN 配置模式	当要创建或删除一个 VLAN 时，必须首先使用该命令进入 VLAN 配置模式
Switch(config-vlan)# vlan statistics interval 20	配置 VLAN 统计间隔时间为 20 秒	间隔时间的取值范围为 5~600，单位：秒；缺省情况下，系统默认 VLAN 流量统计的间隔时间为 10 秒

5.4.3 显示 VLAN 流量统计信息

表5-6 显示VLAN流量统计信息

命令	操作	说明
show vlan *vlan-id* **statistics**	查看 VLAN 流量统计信息	-

查看 VLAN2 的流量统计信息：

```
Switch# show vlan 2 statistics
VLAN: 2
------------------------------------------------------------
Item                                    Packets
------------------------------------------------------------
Inbound:                                3654365
Outbound:                               3654365
------------------------------------------------------------
```

5.4.4 清除 VLAN 流量统计信息

配置此命令，可以清除指定 VLAN 端口的流量统计信息。

表5-7 清除VLAN流量统计信息

命令举例	操作	说明
Switch# clear vlan 2 statistics	清空 VLAN2 的统计信息	-

5.5 配置基于端口的 VLAN

基于端口划分 VLAN 是应用最为广泛、最有效的一种方法。网络管理员将设备的不同端口重新分配组合，指定端口加入不同的逻辑网段中即可。

5.5.1 配置基于 Access 端口的 VLAN

表5-8 配置步骤

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# vlan database	进入 VLAN 模式	当要创建或删除一个 VLAN 时，必须首先使用该命令进入 VLAN 配置模式
Switch(config-vlan)# vlan 2	创建 VLAN 2	-
Switch(config-vlan)# exit	退出 VLAN 模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-
Switch(config-if)# switchport mode access	设置接口类型为 Access	access 模式用来连接到终端设备，如：PC。当接口模式更改时，该接口上学习到的动态 MAC 位址和配置的静态位址都将被清空
Switch(config-if)# switchport access vlan 2	指定端口到相应的 VLAN	默认将接口添加到 VLAN 1 中；配置该命令前需要使用 **switchport mode access** 命令将接口设置成 access 接口类型
Switch(config-if)# end	退出全局配置模式	-

5.5.2 配置基于 Trunk 端口的 VLAN

Trunk 端口能接收标记、无标记的、优先级标记的帧，并发送未标记和标记的帧。如果端口收到一个未标记的帧，此帧将分配端口的 PVID 为 VLAN ID ；如果一个帧的 VID 与端口的 PVID 相等，此帧发送时会剥掉 VLAN 标签。

表5-9 配置步骤

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# vlan database	进入 VLAN 模式	当要创建或删除一个 VLAN 时，必须首先使用该命令进入 VLAN 配置模式
Switch(config-vlan)# vlan 10,20	创建 VLAN10，20	VLAN 序列以‘-’和‘,’符号相连接， VLAN 的值的范围在 1~4094 之间，并且 VLAN 序列的值需要符合升序的原则
Switch(config-vlan)# exit	退出 VLAN 模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-
Switch(config-if)# switchport mode trunk	设置端口为 Trunk 模式	Trunk 模式可以用来连接其它交换设备，也可以连接主机设备。当接口模式更改时，该接口上学习到的动态 MAC 位址和配置的静态位址都将被清空
Switch(config-if)# switchport trunk allowed vlan all	设置端口允许所有的 VLAN 通过	默认 Trunk 口禁止所有 VLAN 通过。如果仅配置 **switchport mode trunk** 命令，未配置 **switchport trunk allowed vlan all** 命令，默认只允许 VLAN 1 通过
Switch(config-if)# switchport trunk native vlan 10	设置端口的本地 VLAN 为 10	VLAN ID 取值范围为 2~4094；默认 native VLAN 为 VLAN 1
Switch(config-if)# exit	退出接口配置模式	-

5.5.3 配置基于 Hybrid 端口的 VLAN

与 Trunk 端口一致，Hybrid 端口也能够发送和接收没有 tag 报文的本地 VLAN。

表5-10 配置步骤

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# vlan database	进入 VLAN 模式	当要创建或删除一个 VLAN

命令举例	操作	说明
		时，必须首先使用该命令进入 VLAN 配置模式
Switch(config-vlan)# vlan 10,20	创建 VLAN10，20	VLAN 序列以‘-’ 和‘,’符号相连接，VLAN 的值的范围在 1~4094 之间，并且 VLAN 序列的值需要符合升序的原则
Switch(config-vlan)# exit	退出 VLAN 模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-
Switch(config-if)# switchport mode hybrid	设置端口为 Hybrid 模式	Hybrid 模式用来连接到终端设备，如：PC。当接口模式更改时，该接口上学习到的动态 MAC 位址和配置的静态位址都将被清空
Switch(config-if)# switchport hybrid allowed vlan add 11	允许来自 VLAN 11 的报文通过 Hybrid 接口	-
Switch(config-if)# switchport trunk native vlan 10	设置端口的本地 VLAN 为 10	默认将接口添加到 VLAN 1 中；VLAN ID 取值范围为 2~4094
Switch(config-if)# exit	退出接口配置模式	-

5.5.4 显示 VLAN 相关配置

表5-11 显示VLAN相关配置

命令	功能	说明
show vlan *vlan-id*	显示特定 VLAN 的信息	-
show vlan all	显示所有 VLAN 的信息	-
show vlan brief	显示所有设备 VLAN 的简要信息	VLAN 的简要信息包括静态和动态信息
show interface switchport [**interface** *if-name*]	显示特定交换接口或所有交换接口的 VLAN 配置信息	-

i. 显示所有设备VLAN的简要信息：

```
Switch# show vlan brief
VLAN ID  Name                State    STP ID      Member ports
                                                  (u)-Untagged, (t)-Tagged
=======  ================ =======  =======  ========================
1        default             ACTIVE   0        eth-0-1(t) eth-0-3(u)
                                                  eth-0-4(u) eth-0-5(u)
                                                  eth-0-6(u) eth-0-7(u)
                                                  eth-0-8(u) eth-0-9(u)
                                                  eth-0-10(u) eth-0-11(u)
                                                  eth-0-12(u) eth-0-13(u)
                                                  eth-0-14(u) eth-0-15(u)
                                                  eth-0-16(u) eth-0-17(u)
                                                  eth-0-18(u) eth-0-19(u)
                                                  eth-0-20(u) eth-0-21(u)
                                                  eth-0-22(u) eth-0-23(u)
10       VLAN0010            ACTIVE   0        eth-0-1(t) eth-0-2(u)
20       VLAN0020            ACTIVE   0        eth-0-1(t)
```

ii. 显示特定交换接口的VLAN配置信息：

```
Switch# show interface switchport interface eth-0-1
 Interface name                : eth-0-1
 Switchport mode               : access
 Ingress filter                : enable
 Acceptable frame types        : vlan-untagged only
 Default Vlan                  : 2
 Configured Vlans              :      2
```

iii. 显示所有交换接口的VLAN配置信息：

```
Switch# show interface switchport

 Interface name                : eth-0-1
 Switchport mode               : trunk
 Ingress filter                : enable
 Acceptable frame types        : all
 Default Vlan                  : 10
 Configured Vlans              :      1      10      20
 Interface name                : eth-0-2
 Switchport mode               : access
 Ingress filter                : enable
 Acceptable frame types        : vlan-untagged only
 Default Vlan                  : 10
 Configured Vlans              :      10
```

5.6 配置 VLAN Classification

5.6.1 VLAN Classification 概述

VLAN分类是基于协议或子网标准的具体规则将数据包发送到选定的VLAN。每一个接口可以应用一种规则集。

VLAN分类规则有3种类型：基于MAC、基于IP和基于协议的分类。基于MAC的VLAN分类规则是根据传入数据包的源MAC地址将数据包进行分类；基于IP的VLAN分类规则将根据传入数据包的源IP地址进行分类；基于协议的VLAN分类规则将根据数据包的三层协议类型进行分类，以下三层类型可以支持ARP、IP（V4）、MPLS、MCAST MPLS、PPPoE协议和RARP。

不同类型的VLAN分类规则，可以添加到同一VLAN的分类组。只有一个VLAN分类规则可以在一个交换机端口生效。

5.6.2 VLAN Classification 配置举例

i.介绍

在下面配置的例子中，创建三个 VLAN 分类规则：

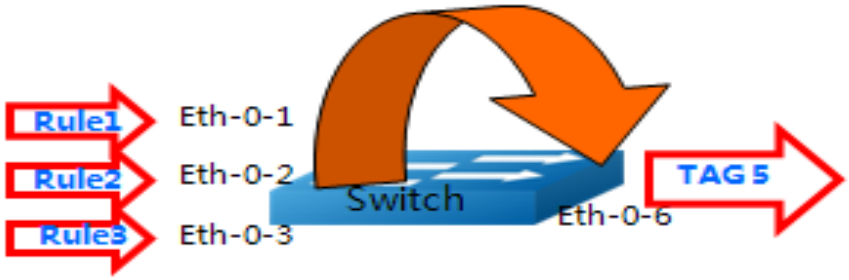
- 第 1 条是基于 MAC 的规则，它将源 MAC 2222.2222.2222 分类到 VLAN 5；
- 第 2 条是基于 IP 的规则，它将源 IP 1.1.1.1 分类到 VLAN 5；
- 第 3 条是基于协议的规则，它将 ARP 的协议数据包分类到 VLAN 5。

把规则 1、2、3 加入到组 31，并且在三个接口上应用组 31。在 eth-0-1、eth-0-2 和 eth-0-3 三个接口上应用不同的分类策略。

- eth-0-1 基于IP分类，意味着匹配IP的数据包在这个接口上将转发到规则对应的VLAN；
- eth-0-2 基于MAC分类，意味着匹配MAC地址的数据包将转发到规则对应的VLAN；
- eth-0-3 基于协议的分类，意味着匹配协议的数据包将转发到规则对应的VLAN。

ii.拓扑

图5-1 VLAN Classificaton示意图



iii.配置步骤

1.创建VLAN分类规则并应用到组

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# vlan database	进入 VLAN 模式
Switch(config-vlan)# vlan 5	创建 VLAN5
Switch(config-vlan)# vlan 6	创建 VLAN6
Switch(config-vlan)# exit	退出 VLAN 模式
Switch(config)# vlan classifier rule 1 mac 2222.2222.2222 vlan 5	创建基于 MAC 的 VLAN 分类规则

命令举例	操作步骤
Switch(config)# vlan classifier rule 2 ip 1.1.1.1 vlan 5	创建基于 IP 的 VLAN 分类规则
Switch(config)# vlan classifier rule 3 protocol arp vlan 5	创建基于协议的 VLAN 分类规则
Switch(config)# vlan classifier group 31 add rule 1	把规则 1 加入到组 31
Switch(config)# vlan classifier group 31 add rule 2	把规则 2 加入到组 31
Switch(config)# vlan classifier group 31 add rule 3	把规则 3 加入到组 31

2.在接口上应用组并配置VLAN划分类型

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# switchport access vlan 6	将 PVID 6 指定给 eth-0-1
Switch(config-if)# switchport access allowed vlan add 5	接口上允许 VLAN5 通过
Switch(config-if)# vlan classifier activate 31 based ip	接口上应用组 31 并且设置接口 VLAN 分类类型为基于 IP 分类
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface eth-0-2	进入接口配置模式
Switch(config-if)# switchport access vlan 6	将 PVID 6 指定给 eth-0-2
Switch(config-if)# switchport access allowed vlan add 5	接口上允许 VLAN5 通过
Switch(config-if)# vlan classifier activate 31 based mac	接口上应用组 31 并且设置接口 VLAN 分类类型为基于 MAC 分类
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface eth-0-3	进入接口配置模式
Switch(config-if)# switchport access vlan 6	将 PVID 6 指定给 eth-0-3
Switch(config-if)# switchport access allowed vlan add 5	接口上允许 VLAN5 通过

命令举例	操作步骤
Switch(config-if)# vlan classifier activate 31 based protocol	接口上应用组 31 并且设置接口 VLAN 分类类型为基于协议分类
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface eth-0-6	进入接口配置模式
Switch(config)#switchport mode trunk	配置端口为 Trunk 模式
Switch(config-if)# switchport trunk allowed vlan add 5	将 eth-0-6 加入到 VLAN5 中
Switch(config-if)# exit	退出接口配置模式

iv.命令验证

命令	操作	说明
show vlan classifier rule [*rule-number*]	显示分类规则的信息	rule-number：分类规则的标识，取值范围 0～4095
show vlan classifier group [*group-number*]	显示 VLAN 分类规则组的信息	group-number：VLAN 分类规则组标识，取值范围 0~31
show vlan classifier interface group [*group-number*]	显示接口上配置的 VLAN 分类信息	group-number：VLAN 分类规则组标识，取值范围 0~31

- 显示分类规则的信息：

```
Switch# show vlan classifier rule

vlan classifier rule 1 mac 2222.2222.2222 vlan 5
vlan classifier rule 2 ip 1.1.1.1 vlan 5
vlan classifier rule 3 protocol arp vlan 5
```

- 显示VLAN分类规则组的信息：

```
Switch# show vlan classifier group

vlan classifier group 31 add rule 1
vlan classifier group 31 add rule 2
vlan classifier group 31 add rule 3
```

- 显示接口上配置的VLAN分类信息：

```
Switch# show vlan classifier interface group

vlan classifier group 31 on interface eth-0-2, based mac
vlan classifier group 31 on interface eth-0-1, based ip
vlan classifier group 31 on interface eth-0-3, based protocol
```

6 Voice VLAN 配置

6.1 Voice VLAN 简介

随着语音技术的日益发展，IP 电话、综合接入设备（Integrated Access Device，缩写：IAD）应用越来越广泛，尤其在宽带小区，网络中经常同时存在语音数据和业务数据两种流量。语音数据在传输时需要具有比业务数据更高的优先级，以减少传输过程中可能产生的时延和丢包现象。

提高语音数据传输优先级的传统处理方法是使用 ACL 对语音数据进行区分，并使用 QoS 保证传输质量。为简化用户配置、更方便的管理语音流的传输策略，设备提供了 Voice VLAN 功能。Voice VLAN 的主要特点就是可以通过报文的源 MAC 地址自动识别出语音流量，保证语音流量传输。

6.2 配置 Voice VLAN

6.2.1 全局启用 Voice VLAN

表6-1 全局启用Voice VLAN

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# vlan database	进入 VLAN 配置模式	当要创建或删除一个 VLAN 时，必须首先使用该命令进入 VLAN 配置模式
Switch(config-vlan)# vlan 2	创建 VLAN2	-
Switch(config-vlan)# exit	退出 VLAN 配置模式，	-
Switch(config)# voice vlan 2	将 VLAN 指定为 VOICE VLAN	缺省情况下，系统未启动此功能

6.2.2 配置 Voice VLAN 的 OUI

OUI 表示一个 MAC 地址段，用户可以配置 Voice VLAN 的 OUI 值，也可以使用掩码和配置掩码长度。

表6-2 配置Voice VLAN的OUI

命令举例	操作	说明
Switch(config)# voice vlan 2	将 VLAN 指定为 VOICE VLAN	缺省情况下，系统未启动此功能
Switch(config)# voice vlan mac-address 0055.0000.0000 ffff.ff00.0000 description test	为 VOICE VLAN 添加 OUI	只有匹配 OUI 的报文才会被认为是语音报文

说明

系统中有五条默认的 OUI：0003-6b00-0000 Cisco phone、000f-e200-0000 H3C Aolynk phone、00d0-1e00-0000 Pingtel phone、00e0-7500-0000 Polycom phone、00e0-bb00-0000 3Com phone

6.2.3 配置基于端口的 Voice VLAN

表6-3 配置基于端口的Voice VLAN

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-1	进入端口 eth-0-1 的配置模式	-
Switch(config-if)# switchport mode trunk	将端口设置为 Trunk 口	-
Switch(config-if)# switchport trunk allowed vlan all	允许端口通过所有带 tag 的 VLAN	-
Switch(config-if)# voice vlan enable	在端口上启用 VLOICE VLAN	缺省情况下，端口未启用 Voice VLAN
Switch(config-if)# interface eth-0-2	进入端口 eth-0-2 的配置模式	-
Switch(config-if)# switchport mode trunk	将端口设置为 Trunk 口	-
Switch(config-if)# switchport trunk	允许端口通过所有带 tag 的	-

allowed vlan all	VLAN	

6.2.4 配置 Voice VLAN 的安全模式

表6-4 启用/关闭Voice VLAN的安全模式

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# voice vlan security enable	启用 VOICE VLAN 的安全模式	缺省情况下，启用 VOICE VLAN 的安全模式；启用安全模式后，VOICE VLAN 中没有匹配 OUI 的所有报文都会被丢弃
Switch(config)# no voice vlan security enable	关闭 VOICE VLAN 的安全模式	

6.2.5 配置通过 Voice VLAN 报文的 COS

Class of Service（服务等级，缩写：COS）可以解决IP网络的质量问题，通过服务的类别对业务进行分类，对报文给予不同的优先级。

表6-5 配置通过Voice VLAN报文的COS

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# voice vlan set cos to 7	将通过 Voice VLAN 报文的 COS 修改为 7	COS 取值范围为 1~7；缺省情况下，通过 Voice VLAN 报文的 COS 为 5

6.2.6 查看 Voice VLAN 配置信息

表6-6 查看Voice VLAN配置信息

命令	操作	说明
show voice vlan state	显示当前系统的 VOICEC VLAN 配置	-

7 VLAN Mapping 配置

7.1 VLAN Mapping 简介

VLAN Mapping 又称为 VLAN Translation 或 VLAN 映射，可以将用户报文中携带的私网 VLAN Tag 封装在公网 VLAN Tag 中，按照公网的网络规划进行传输。对端用户私网收到该报文后，根据同样的规则将 VLAN tag 恢复为私网的 VLAN Tag。VLAN Mapping 由此通过替换报文携带的 VLAN Tag，来实现用户 VLAN 和运营商 VLAN 之间的相互映射。

7.2 配置 VLAN Translation

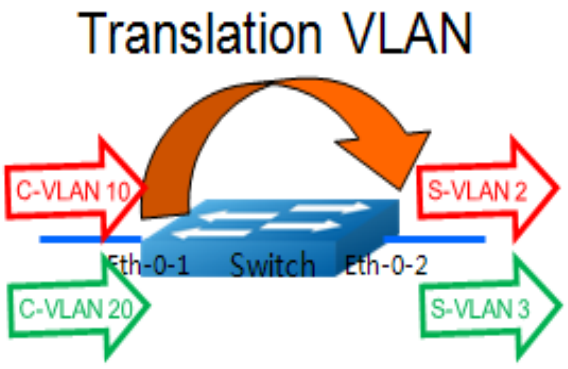
i. 介绍

服务供应商的业务客户往往有特定的 VLAN ID 的要求，同一个网络服务提供商的不同客户的要求的 VLAN 可能会重叠，并且通过服务商设备的用户流量也可能会混合。通过给每一个客户分配不同的 VLAN ID 来映射自己的 VLAN ID，能够区分客户不同应用的通讯。

使用 VLAN 转换功能，服务提供商可以使用一系列的 VLAN 来服务拥有自己 VLAN ID 的客户。客户 VLAN ID 被转换，服务提供商的设备可以区分来自不同应用的客户的流量。

ii. 拓扑

图7-1 VLAN Translation示意图



iii. 配置步骤

表7-1 配置步骤

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# vlan database	进入 VLAN 配置模式
Switch(config-vlan)# vlan 2,3	创建 S-TAG VLAN 2,3
Switch(config)# ethernet evc evc_c1	创建 EVC evc_c1
Switch(config-evc)# dot1q mapped-vlan 2	设置 VLAN2 关联到 EVE evc_c1
Switch(config)# ethernet evc evc_c2	创建 EVC evc_c2
Switch(config-evc)# dot1q mapped-vlan 3	设置 VLAN3 关联到 EVE evc_c2
Switch(config)# vlan mapping table vm	创建 VLAN MAPPING 表 VM
Switch(config-vlan-mapping)# raw-vlan 10 evc evc_c1	设置 C-Tag 为 10 映射到 S-Tag 为 2
Switch(config-vlan-mapping)# raw-vlan 20 evc evc_c2	设置 C-Tag 为 20 映射到 S-Tag 为 3
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# switchport mode trunk	配置端口为 Trunk 模式
Switch(config-if)# switchport trunk vlan-translation	设置 Trunk 模式为 VLAN 转换模式
Switch(config-if)# switchport trunk vlan-translation mapping table vm	在接口上应用 VLAN MAPPING 表
Switch(config-if)# switchport trunk allowed vlan add 2,3	加入 VLAN2,3
Switch(config-if)# interface eth-0-2	进入接口配置模式
Switch(config-if)# switchport mode trunk	设置端口为 Trunk 模式
Switch(config-if)# switchport trunk allowed vlan add 2,3	加入 VLAN2,3
Switch(config-if)# end	退出接口配置模式

iv. 显示与维护

表7-2 显示与维护

命令	配置	说明
show vlan mapping table [*table-name*]	显示 VLAN 映射表的信息	-
show interface switchport [**interface** *if-name*]	检查特定端口的 VLAN 映射表配置	-

- 检查特定端口的VLAN映射表配置：

```
Switch# show interface switchport interface eth-0-1

Interface name                : eth-0-1
  Switchport mode             : trunk
  VLAN traslation             : enable
  VLAN mapping table          : vm
  Ingress filter              : enable
  Acceptable frame types      : all
  Default Vlan                : 1
  Configured Vlans            : 1       2       3
```

- 显示VLAN映射表的信息：

```
Switch# show vlan mapping table
Table Name            EVC Name              Mapped VLAN Raw VLAN
 ================ ================   =========== ======================
vm                    evc_c1              2           10
                      evc_c2              3           20
```

7.3 配置 QinQ

7.3.1 QinQ 简介

QinQ 技术通过在以太帧中堆叠两个 802.1Q 包头，有效地扩展了 VLAN 数目，使 VLAN 的数目最多可达 4096 × 4096 个。同时，多个 VLAN 能够被复用到一个核心 VLAN 中。ISP 通常为每个客户建立一个VLAN 模型，通过通用属性注册协议/通用 VLAN 注册协议（GARP/GVRP）自动监控整个主干网络的 VLAN，并通过扩展生成树协议（STP）来加快网络收敛速度，从而为网络提供弹性。

QinQ 技术作为初始的解决方案是不错的，但随着用户数量的增加，SVLAN 模型也会带来可扩展性的

问题。有些用户可能希望在分支机构间进行数据传输时可以携带自己的 VLAN ID，这就使采用 QinQ 技术的 MSP 面临以下两个问题：第一，第一名客户的 VLAN 标识可能与其他客户冲突；第二，服务提供商将受到客户可使用标识数量的严重限制。如果允许用户按他们自己的方式使用各自的VLAN ID 空间，那么核心网络仍存在4096个 VLAN 的限制。

QinQ 是指将用户私网 VLAN Tag 封装在公网 VLAN Tag 中，使报文带着两层 VLAN Tag 穿越运营商的骨干网络（公网）。在公网中报文只根据外层 VLAN Tag（即公网VLAN Tag）传播，用户的私网 VLAN Tag 被屏蔽。这样，不仅对数据流进行了区分，而且由于私网 VLAN 标签被透明传送，不同的用户 VLAN 标签可以重复使用，只需要外层 VLAN 标签的在公网上唯一即可，实际上也扩大了可利用的 VLAN 标签数量。

封装外层 VLAN 标签有两种方法，一种是标准 QinQ 封装，即基于端口打上外层标签，该端口下所有的用户数据统一封装一个共同的 VLAN 标签，在实际应用中局限性太大。另外一种是灵活 QinQ 封装方法，既可以根据一些特性对用户数据进行流分类，还可以根据不同的类别封装不同的外层 VLAN 标签。

7.3.2 配置基本 QinQ

i. 介绍

下面介绍基本 QinQ 的封装方法，是基于接口方式实现的。接口上开启基本 QinQ 功能后，当该接口收到报文是携带 VLAN Tag 的报文时，该报文就会成为双 Tag 的报文；当接口收到未携带 VLAN Tag 的报文时，该报文就会成为带有本接口缺省 VLAN Tag 的报文。

ii. 拓扑

图 7-2 基本 QinQ 拓扑图

iii. 配置步骤

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# no shutdown	配置端口为 UP 状态
Switch(config-if)# switchport mode dot1q-tunnel	配置接口为 DOT1Q-Tunnel 模式
Switch(config-if)# end	退出接口配置模式

iv. 显示与维护

命令	操作	说明
show interface switchport [**interface** *if-name*]	检查接口的配置	-

显示基本 QinQ 的配置信息：

```
Switch# show interface switchport interface eth-0-1

Interface name                : eth-0-1
  Switchport mode             : dot1q-tunnel(basic)
  Ingress filter              : enable
  Acceptable frame types      : all
  Default Vlan                : 1
  Configured Vlans            : 1
```

7.3.3 配置灵活 QinQ

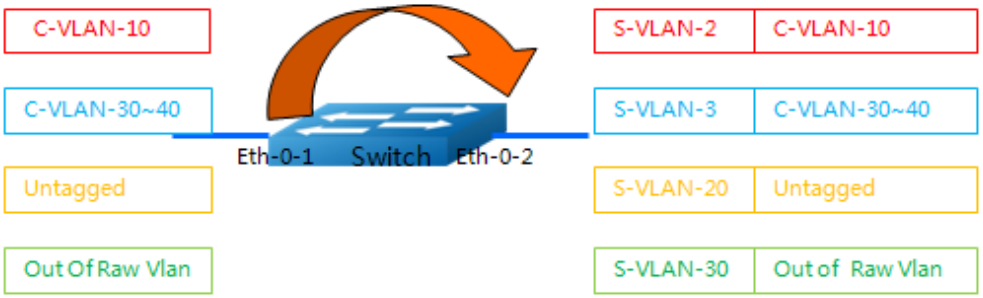
由于基本 QinQ 在实际应用的局限性比较大，下面介绍另外一种封装方式，即灵活 QinQ。这种方式更加灵活，是基于接口和 VLAN 相结合的方式实现的。

a) 加一层Tag

下面介绍加一层 Tag 的配置方法。

i. 拓扑

图7-3 加一层Tag拓扑图



ii. 配置步骤

U-tag 报文加一层 TAG 的配置步骤如下所示。

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# vlan database	进入 VLAN 配置模式
Switch(config-vlan)# vlan 2,3,20,30	创建 S-TAG 2，3，20，30
Switch(config)# ethernet evc evc_c1	创建 EVC evc_c1
Switch(config-evc)# dot1q mapped-vlan 2	设置 S-TAG 2 关联 EVC_C1
Switch(config)# ethernet evc evc_c2	创建 EVC evc_c2
Switch(config-evc)# dot1q mapped-vlan 3	设置 S-TAG 3 关联 EVC_C2
Switch(config)# ethernet evc evc_c3	创建 EVC evc_c3
Switch(config-evc)# dot1q mapped-vlan 20	设置 S-TAG 20 关联 EVC_C3
Switch(config)# ethernet evc evc_c4	创建 EVC evc_c4
Switch(config-evc)# dot1q mapped-vlan 30	设置 S-TAG 30 关联 EVC_C4
Switch(config)# vlan mapping table vm	创建 VLAN Mapping 表
Switch(config-vlan-mapping)# raw-vlan 10 evc evc_c1	设置 C-TAG10 加入 evc_c1
Switch(config-vlan-mapping)# raw-vlan 30-40 evc evc_c2	设置 C-TAG30-40 加入 evc_c2
Switch(config-vlan-mapping)# raw-vlan untagged evc evc_c3	设置 U-TAG 加入 evc_c3
Switch(config-vlan-mapping)# raw-vlan out-of-range evc evc_c4	设置范围之外的 C-TAG 加入 evc_c4
Switch(config)# interface eth-0-1	进入接口配置模式

命令举例	操作步骤
Switch(config-if)# switchport mode dot1q-tunnel	设置接口为 Dot1q-tunnel 模式
Switch(config-if)# switchport dot1q-tunnel type selective	设置接口为灵活 QinQ
Switch(config-if)# switchport dot1q-tunnel vlan mapping table vm	在接口上应用 VLAN Mapping 表 VM
Switch(config-if)# switchport dot1q-tunnel allowed vlan add 2,3,20,30	接口上允许 VLAN 2，3，20，30 通过
Switch(config-if)# interface eth-0-2	进入接口配置模式
Switch(config-if)# switchport mode trunk	设置接口为 Trunk 模式
Switch(config-if)# switchport trunk allowed vlan add 2,3,20,30	接口上允许 VLAN 2，3，20，30 通过
Switch(config-if)# end	退出接口配置模式

iii. 显示与维护

命令	配置	说明
show vlan mapping table [*table-name*]	显示 VLAN 映射表的信息	-
show interface switchport [**interface** *if-name*]	检查接口的配置	-

- 显示灵活QinQ的配置信息：

```
Switch# show interface switchport interface eth-0-1

 Interface name                : eth-0-1
 Switchport mode               : dot1q-tunnel(selective)
 VLAN mapping table            : vm
 Ingress filter                : enable
 Acceptable frame types        : all
 Default Vlan                  : 1
 Configured Vlans              : 1       2       3       20      30
```

- 显示VLAN映射表的信息：

```
Switch# show vlan mapping table
Table Name          EVC Name              Mapped VLAN Raw VLAN
```

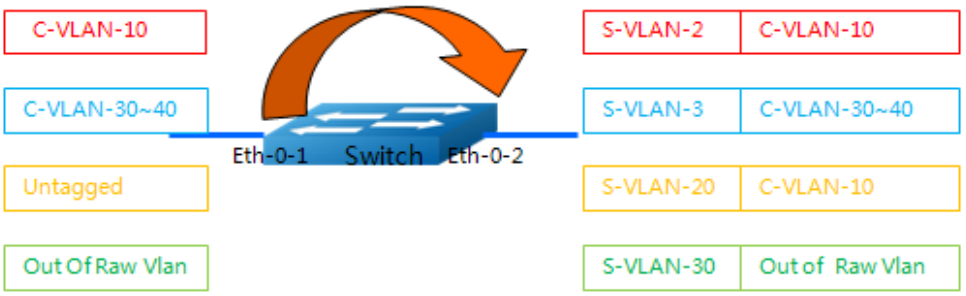
```
================ ================ =========== ============================
vm               evc_c1           2           10
                 evc_c2           3           30-40
                 evc_c3           20          untagged
                 evc_c4           30          out-of-range
```

b) 加两层Tag

下面介绍加两层 Tag 的配置方法。

i. 拓扑

图7-4 加两层Tag拓扑图



ii. 配置步骤

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# vlan database	进入 VLAN 配置模式
Switch(config-vlan)# vlan 2,3,10,20,30	创建 S-TAG 2，3，10，20，30
Switch(config)# ethernet evc evc_c1	创建 EVC evc_c1
Switch(config-evc)# dot1q mapped-vlan 2	设置 S-TAG 2 关联 evc_c1
Switch(config-evc)# exit	退出 EVC 模式
Switch(config)# ethernet evc evc_c2	创建 EVC evc_c2
Switch(config-evc)# dot1q mapped-vlan 3	设置 S-TAG 3 关联 evc_c2
Switch(config-evc)# exit	退出 EVC 模式

命令举例	操作步骤
Switch(config)# ethernet evc evc_c3	创建 EVC evc_c3
Switch(config-evc)# dot1q mapped-double-vlan 10 20	设置 C-TAG 10, S-TAG 20 关联 evc_c3
Switch(config-evc)# exit	退出 EVC 模式
Switch(config)# ethernet evc evc_c4	创建 EVC
Switch(config-evc)# dot1q mapped-vlan 30	设置 S-TAG 30 关联 evc_c4
Switch(config-evc)# exit	退出 EVC 模式
Switch(config)# vlan mapping table vm	创建 VLAN mapping 表
Switch(config-vlan-mapping)# raw-vlan 10 evc evc_c1	设置 C-TAG10 加入 evc_c1
Switch(config-vlan-mapping)# raw-vlan 30-40 evc evc_c2	设置 C-TAG30-40 加入 evc_c2
Switch(config-vlan-mapping)# raw-vlan untagged evc evc_c3	设置 U-TAG 加入 evc_c3
Switch(config-vlan-mapping)# raw-vlan out-of-range evc evc_c4	设置范围之外的 C-TAG 加入 evc_c4
Switch(config-vlan-mapping)# exit	退出 VLAN Mapping 配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# switchport mode dot1q-tunnel	配置接口为 do1q-tunnel
Switch(config-if)# switchport dot1q-tunnel type selective	设置端口为灵活 QinQ
Switch(config-if)# switchport dot1q-tunnel vlan mapping table vm	在接口上应用 VLAN Mapping 表 vm
Switch(config-if)# switchport dot1q-tunnel native inner-vlan 10	配置 dot1q-tunnel 端口的默认的 VLAN ID 为 10
Switch(config-if)# switchport dot1q-tunnel allowed vlan add 2,3,20,30	接口上允许 VLAN 2，3，20，30 通过
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface eth-0-2	进入接口配置模式
Switch(config-if)# switchport mode trunk	设置接口为 Trunk 模式
Switch(config-if)# switchport trunk allowed vlan add 2,3,20,30	接口上允许 VLAN 2，3，20，30 通过

命令举例	操作步骤
Switch(config-if)# end	退出接口配置模式

iii. 显示与配置

命令	操作	说明
show vlan mapping table [*table-name*]	显示 VLAN 映射表的信息	-
show interface switchport [**interface** *if-name*]	检查接口的配置	-

- 显示灵活QinQ的配置信息：

```
Switch# show interface switchport interface eth-0-1

 Interface name                : eth-0-1
 Switchport mode               : dot1q-tunnel(selective)
 VLAN mapping table            : vm
 Ingress filter                : enable
 Acceptable frame types        : all
 Default Vlan                  : 10
 Configured Vlans              : 1       2       3       20      30
```

- 显示VLAN映射表的信息：

```
Switch# show vlan mapping table
  Table Name           EVC Name              Mapped VLAN Raw VLAN
  ================ ================ ===========
=================================
  vm                    evc_c1               2              10
                        evc_c2               3              30-40
                        evc_c3               20(10)         untagged
                        evc_c4               30             out-of-range
```

8 链路聚合配置

8.1 链路聚合简介

链路聚合（Link Aggregation，缩写：LA）指将多条物理链路汇聚在一起，形成一条逻辑链路，实现增加链路带宽及提高链路可靠性的目的。

本章介绍了一个链路聚合控制协议（LACP）配置示例。LACP 是基于 IEEE802.3ad 规范的协议，能够实现链路动态汇聚。它允许多个物理接口的捆绑，形成一个单一的逻辑通道，提供增强的性能和冗余。聚合接口被视为单一链路与交换机相连，生成树将它视为一个接口。当有一个物理接口出现故障，其他接口正常连接，链路不会中断，可以在单一的逻辑通道上支持最多 16 个物理以太网链路。LACP 协议使设备可以管理与符合 IEEE802.3ad 的协议的其他设备之间的链路聚合组。使用 LACP 协议，交换机学习支持 LACP 成员识别的每个端口的能力。然后，具有相同的属性动态组端口捆绑到一个单一逻辑链路。

8.1.1 基本概念

1. 聚合组、成员端口

由链路聚合而成的逻辑链路称为一个聚合组，在一个聚合组内有若干个以太网接口，这些捆绑的以太网接口即该聚合组的成员端口。

2. 成员端口的状态

聚合组内的成员端口有有两种状态：Selected 状态（也称为活动状态、Active 状态）和 Unselected 状态（也称为非活动状态、Backup 状态、Standby 状态）。处于 Selected 状态的成员端口可以转发数据，而处于 Unselected 状态的成员端口不能转发数据。

3. 操作Key

所有成员端口都有一个操作 key，它是结合了成员端口的信息自动生成的，如端口速率、双工模式、UP/DOWN 状态、协议类配置等。协议类的配置包括生成树、MAC 地址学习等。

4. 聚合模式

链路聚合模式有两种：静态聚合模式与动态聚合模式。静态聚合又称为手工聚合，需要分别在聚合链路的两端设备配置聚合组，并加入成员端口，在这一过程中没有 LACP 协议的应用，两端的设备不交互聚合信息；动态聚合一般指静态 LACP 聚合，也需要手工创建聚合组，开启 LACP 协议并加入成员端口，两端的设备通过互发链路聚合控制协议数据单元（Link Aggregation Control Protocol Data Unit，缩写：LACPDU）来交互链路聚合的信息。

8.1.2 静态聚合模式

静态聚合模式的工作机制如下：

首先，需要选择参考端口，在聚合组的所有成员端口中，端口号最小的端口称为参考端口。参考端口为 Selected 状态，其他的成员端口和参考端口的操作 Key 一致，均为 Selected 状态且不超过静态聚合组内选中端口的最大数量。如果成员端口的数量大于能够配置的最大端口数量，按照端口号从小到大的排序方式优先选择 Selected 状态的端口，其余的端口则为 Unselected 端口。

8.1.3 动态聚合模式

动态聚合模式的工作机制如下：

动态聚合模式由聚合链路的两端交换机通过聚合组内所有成员端口，向对端发送 LACP 报文来实现。同样需要选择参考端口，可以从聚合端口两端端口状态为 UP 的成员端口中选出，其他成员端口将参照端口的操作 Key，若和参考端口一致，则可以被选中参与数据转发。

LACP 报文的主要内容有设备 ID，端口 ID 和操作 Key。设备 ID 由系统的 LACP 优先级和 MAC 地址构成，端口 ID 由优先级和端口号构成。

首先，比较聚合链路两端的设备 ID，选择较小的一端，再比较 LACP 优先级。如果 LACP 优先级相同，再来比较 MAC 地址。LACP 优先级的值和 MAC 地址越小，设备 ID 也越小。

确定了较小的设备 ID 后，需要比较聚合组内各成员端口的端口 ID。比较端口的优先级后，优先级相同的情况下，再比较端口号。端口的优先级数值和端口号越小，端口 ID 也越小。端口 ID 最小、操作 Key 与参考端口一致，且不超过动态聚合组内选中端口的最大数量时，两端均为 Selected 状态。

说明

所有成员端口退出聚合组后，聚合端口不会被删除，该配置支持 CN9300、CN9408H、S6550E 系列设备的主线分支及使用该分支的后续设备。如需删除聚合端口，可使用 **no interface agg** 命令。其他设备无此配置。

8.2 配置聚合组

下面介绍配置这两种聚合组的方法。

8.2.1 拓扑

如下图所示，两个交换机 Switch（S1）和 Switch（S2）之间配置三条以太网物理链路。这三个链路都分配在同一个管理中心，使他们能聚合形成一个逻辑链路 Link Aggregation 1。

图 8-1 链路聚合示意图

8.2.2 配置静态链路聚合组

配置两端的交换机 Switch1 和 Switch2 的静态聚合组，下表以 Switch1 为例。

表8-1 配置步骤

命令举例	操作	说明
Switch1# configure terminal	进入全局配置模式	-
Switch1(config)# interface eth-0-1	进入接口配置模式	-
Switch1(config-if)# no shutdown	配置端口为 UP 状态	-
Switch1(config-if)# static-channel-group 1	添加接口 eth-0-1 到静态聚合组 channel group 1	静态聚合组 ID 的取值范围为 1~31

命令举例	操作	说明
Switch1(config-if)# exit	退出接口配置模式	-
Switch1(config)# interface eth-0-2	进入接口配置模式	-
Switch1(config-if)# static-channel-group 1	添加接口 eth-0-2 到静态聚合组 channel group 1	静态聚合组 ID 的取值范围为 1~31
Switch1(config-if)# no shutdown	配置端口为 UP 状态	-
Switch1(config-if)# exit	退出接口配置模式	-
Switch1(config)# interface eth-0-3	进入接口配置模式	-
Switch1(config-if)# static-channel-group 1	添加接口 eth-0-3 到静态聚合组 channel group 1	静态聚合组 ID 的取值范围为 1~31
Switch1(config-if)# no shutdown	配置端口为 UP 状态	-
Switch1(config-if)# end	退出接口配置模式	-

8.2.3 配置动态链路聚合组

配置两端的交换机Switch1和Switch2的动态聚合组，下表以Switch1为例。

表8-2 配置步骤

命令举例	操作	说明
Switch1# configure terminal	进入全局配置模式	-
Switch1(config)# lacp system-priority 2000	配置系统的 LACP 协议优先级	默认优先级为 32768。数值越低，优先级越高
Switch1(config)# port-channel load-balance hash-field-select macsa	通过源 MAC 地址实现负载均衡	系统默认 IP hash，即根据报文的源和目的 IP 位址做 hash 的方式决定报文从 LACP 的哪一个成员端口出去。用户还可以选择根据目的 MAC、源 MAC、源 MAC 和目的 MAC 相结合来做 hash；或者根据目的 IP、源 IP 来做 hash
Switch1(config)# interface eth-0-1	进入接口配置模式	-
Switch1(config-if)# no shutdown	配置端口为 UP 状态	-

命令举例	操作	说明
Switch1(config-if)# channel-group 1 mode active	添加接口 eth-0-1 到 channel group 1，启用动态链路聚合，模式为主动模式。因此可以通过本地系统选择聚合	动态聚合组 ID 的取值范围范围为 1~31；LACP 的工作模式分为 active（使能接口的动态链路聚合）和 passive（去使能接口的动态链路聚合）
Switch1(config-if)# exit	退出接口配置模式	-
Switch1(config)# interface eth-0-2	进入接口配置模式	-
Switch1(config-if)# channel-group 1 mode active	添加接口 eth-0-2 到 channel group 1 启用动态链路聚合	动态聚合组 ID 的取值范围范围为 1~31；LACP 的工作模式分为 active（使能接口的动态链路聚合）和 passive（去使能接口的动态链路聚合）
Switch1(config-if)# no shutdown	配置端口为 UP 状态	-
Switch1(config-if)# exit	退出接口配置模式	-
Switch1(config)# interface eth-0-3	进入接口配置模式	-
Switch1(config-if)# channel-group 1 mode active	添加接口 eth-0-3 到 channel group 1，启用动态链路聚合	动态聚合组 ID 的取值范围范围为 1~31；LACP 的工作模式分为 active（使能接口的动态链路聚合）和 passive（去使能接口的动态链路聚合）
Switch1(config-if)# no shutdown	配置端口为 UP 状态	-
Switch1(config-if)# end	退出接口配置模式	-

8.2.4 显示链路聚合组信息

表8-3 显示链路聚合组信息

命令	操作	说明
show channel-group [*channel-group-number*] **summary**	显示所有的聚合组或者指定的聚合组的配置信息	聚合组 ID 的取值范围为 1～31

- 显示所有静态聚合组的配置信息：

```
Switch1# show channel-group summary

port-channel load-balance hash-arithmetic: xor
port-channel load-balance hash-field-select:
        macsa
Flags:   s - suspend                T - standby
           D - down/admin down      B - in Bundle
           R - Layer3               S - Layer2
           w - wait                 U - in use
Mode:     SLB   - static load balance
           DLB   - dynamic load balance
           SHLB - self-healing load balance
           RR     - round robin load balance
Aggregator Name   Mode          Protocol        Ports
----------------+---------+------------+-----------------------------------------------
agg1(SU)              SLB           Static              eth-0-1(B) eth-0-2(B) eth-0-3(B)
```

- 显示所有动态聚合组的配置信息：

```
Switch1# show channel-group summary

port-channel load-balance hash-arithmetic: xor
port-channel load-balance hash-field-select:
        macsa
Flags:   s - suspend                T - standby
           D - down/admin down      B - in Bundle
           R - Layer3               S - Layer2
           w - wait                 U - in use
Mode:     SLB   - static load balance
           DLB   - dynamic load balance
           SHLB - self-healing load balance
           RR     - round robin load balance
Aggregator Name   Mode          Protocol        Ports
----------------+---------+------------+-----------------------------------------------
agg1(SU)              SLB           LACP              eth-0-1(B) eth-0-2(B) eth-0-3(B)
```

9 流量控制配置

9.1 流量控制简介

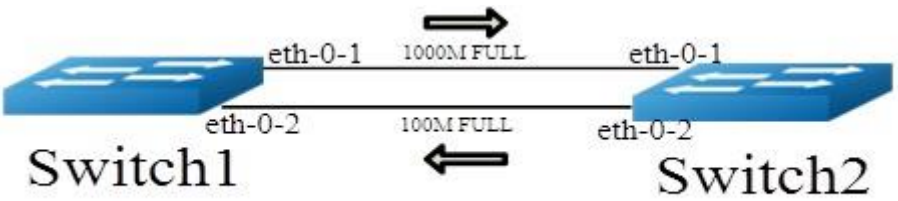
流量控制即防止丢包现象的技术。该技术在直连的以太端口上启用，在拥塞期间允许另一端拥塞的节点暂停链路运作来控制流量速率。当本地设备在本地检测到了任何拥塞，他能够发送一个暂停帧通知链路伙伴或者远程设备已发生拥塞。紧随收到暂停帧之后，远程设备停止发送任何数据包，这样防止在拥塞期间丢弃任何一个数据包。在自协商链路上，本地的流控制能力能通过链路断开/连接来通知对方。

9.2 配置流量控制

下面介绍了配置发送/接收流量控制报文的步骤以及如何查看已配置的流量控制信息。

9.2.1 拓扑

图 9-1 流量控制拓扑图



9.2.2 配置发送流量控制报文

表9-1 配置步骤

命令举例	操作	说明
Switch2# configure terminal	进入全局配置模式	-
Switch2(config)# interface eth-0-1	进入接口配置模式	-

命令举例	操作	说明
Switch2(config-if)# flowcontrol send on	在端口使能发送流量控制报文	缺省情况下，不启用发送流量控制报文功能
Switch2 (config-if)# exit	返回全局配置模式	-

9.2.3 配置接收流量控制报文

表9-2 配置步骤

命令举例	操作	说明
Switch1# configure terminal	进入全局配置模式	-
Switch1(config)# interface eth-0-1	进入接口配置模式	-
Switch1(config-if)# flowcontrol receive on	在端口使能接收流量控制报文	缺省情况下，不启用接收流量控制报文功能
Switch1(config-if)# exit	返回全局配置模式	-

说明

流控制仅在物理接口的全双工链路下有效。

9.2.4 显示流量控制报文信息

表9-3 显示流量控制报文信息

命令	配置	说明
show flowcontrol [*if-name*]	查看指定端口或全部端口的流量控制报文信息	-

- 查看全部端口发送流量控制报文的信息：

```
Switch2# show flowcontrol
Port        Receive FlowControl    Send FlowControl      RxPause      TxPause
              admin      oper        admin      oper
```

```
---------  -------- --------  -------- --------  -----------  -----------
eth-0-1    off      off       on       on        0            0
eth-0-2    off      off       off      off       0            0
eth-0-3    off      off       off      off       0            0
```

- 查看指定端口发送流量控制报文的信息：

```
Switch2# show flowcontrol eth-0-1

Port          Receive FlowControl    Send FlowControl      RxPause      TxPause
                admin       oper         admin       oper
---------  -------- --------  -------- --------  -----------  -----------
eth-0-1    off      off       on       on        0            0
```

- 查看全部端口接收流量控制报文的信息：

```
Switch1# show flowcontrol

Port          Receive FlowControl    Send FlowControl      RxPause      TxPause
                admin       oper         admin       oper
---------  -------- --------  -------- --------  -----------  -----------
eth-0-1    on       on        off      off       0            0
eth-0-2    off      off       off      off       0            0
eth-0-3    off      off       off      off       0            0
```

- 查看指定端口接收流量控制报文的信息：

```
Switch1# show flowcontrol eth-0-1

Port          Receive FlowControl    Send FlowControl      RxPause      TxPause
                admin       oper         admin       oper
---------  -------- --------  -------- --------  -----------  -----------
eth-0-1    on       on        off      off       0            0
```

10 环回检测配置

10.1 环回检测简介

网络中的环路会导致设备对广播、组播以及未知单播等报文进行重复发送，造成网络资源的浪费甚至导致网络瘫痪。为了能够及时发现二层网络中的环路，以避免对整个网络造成严重影响，需要提供一种检测功能，使网络中出现环路时能及时通知用户检查网络连接和配置情况，并能够将出问题的接口受控。

环回检测（Loopback Detection）功能可以检测设备的接口是否发生环回，它通过从接口定时发送检测报文，并检测该报文是否会从发出去的接口收到，如果收到从该接口发出的检测报文，则认为当设备的此接口存在环路，可以及时通过发送告警信息到网管系统，使管理人员及时发现并解决网络环路问题，避免长时间的网络异常。此外，设备还可以进行接口受控，根据需求选择配置Trap、关闭接口等处理方式，能迅速将环回对网络的影响降低至最小。

10.2 配置使能环回检测

默认情况下，Loopback Detection 功能未使能，使能接口 Loopback Detection 功能后，接口才会发送环回检测报文来进行接口环回检测。默认检测报文发送间隔为 5 秒。

10.2.1 配置步骤

表10-1 配置步骤

命令举例	操作	说明
Switch#configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-
Switch(config-if)# loopback-detect enable	使能环回检测功能	缺省情况下，去使能环回检测功能
Switch(config-if)#end	退出接口配置模式	-

10.2.2 显示环回检测的状态

表10-2 显示环回检测的状态

命令	操作	说明
show loopback-detect [**interface** *if-name* | **packet-interval**]	查看环回检测的状态	-

查看环回检测的状态：

```
Switch# show loopback-detect
Loopback detection packet interval(second): 5
Loopback detection recovery time(second):     15
Interface            Action                Status
eth-0-2               shutdown              NORMAL
```

10.3 配置环回检测报文的发送周期

由于网络时刻处于变化中，因此环回检测是一个持续的过程，接口以一定的时间间隔发送环回检测报文，这个时间间隔即 Loopback Detection 报文发送周期。

10.3.1 配置步骤

表10-3 配置步骤

命令举例	操作	说明
Switch#configure terminal	进入全局配置模式	-
Switch(config)# loopback-detect packet-interval 10	设置环回检测报文的发送间隔为 10 秒	取值范围为 1~300，单位：秒；默认环回检测报文的发送间隔为 5 秒
Switch(config-if)# end	退出接口配置模式	-

10.3.2 显示环回检测报文的发送周期

表10-4 显示环回检测报文的发送周期

命令	操作	说明
show loopback-detect [**interface** *if-name* | **packet-interval**]	查看环回检测报文发送间隔	-

查看环回检测报文发送间隔：

```
Switch# show loopback-detect packet-interval
Loopback detection packet interval(second): 10
Loopback detection recovery time(second):     30
```

10.4 配置环回检测的处理动作

如果发现接口有环回，设备会将该接口设置为处于环回检测工作状态，可配置发送告警、关闭接口等处理动作。

10.4.1 配置步骤

表10-5 配置步骤

命令举例	操作	说明
Switch#configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-
Switch(config-if)# loopback-detect action shutdown	配置环回检测的处理动作为 shutdown	缺省情况下，环回检测的处理动作为 Trap（发送告警）
Switch(config-if)# end	退出接口配置模式	-

10.4.2 显示接口的环回检测信息

表10-6 显示接口的环回检测信息

命令	操作	说明
show loopback-detect [**interface** *if-name* | **packet-interval**]	查看接口上的环回检测状态和配置信息	-

查看接口上的环回检测状态和配置信息：

```
Switch# show loopback-detect interface eth-0-1
Interface          Action          Status
eth-0-1            shutdown        NORMAL
```

10.5 配置对指定 VLAN 的环回检测功能

接口开启 Loopback Detection 功能后，系统默认发送的为 Untagged 检测报文，即不对任何指定 VLAN 进行环回检测。当接口是以 Tagged 方式加入 VLAN 时，接口发出去 Untagged 检测报文在链路上会被丢弃，接口将收不到环回回来的报文，因此需要配置对指定的 VLAN 进行环回检测。

配置对指定 VLAN 的 Loopback Detection 功能，接口会定时发送1份 Untagged 检测报文和多份带指定 VLAN Tag 的检测报文，一个接口最多可发送8份带指定 VLAN Tag 的检测报文。

10.5.1 配置步骤

表10-7 配置步骤

命令举例	操作	说明
Switch#configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-
Switch(config-if)# loopback-detect packet vlan 20	配置该接口下 VLAN 20 的环回检测功能	取值范围为 1~4094；缺省情况下，未配置对指定 VLAN 的环回检测功能
Switch(config-if)# end	退出接口配置模式	-

10.5.2 显示对指定 VLAN 的环回检测信息

表10-8 显示对指定VLAN的环回检测信息

命令	操作	说明
show running-config interface *if-name*	查看对指定 VLAN 的环回检测信息	-

查看对指定 VLAN 的环回检测信息：

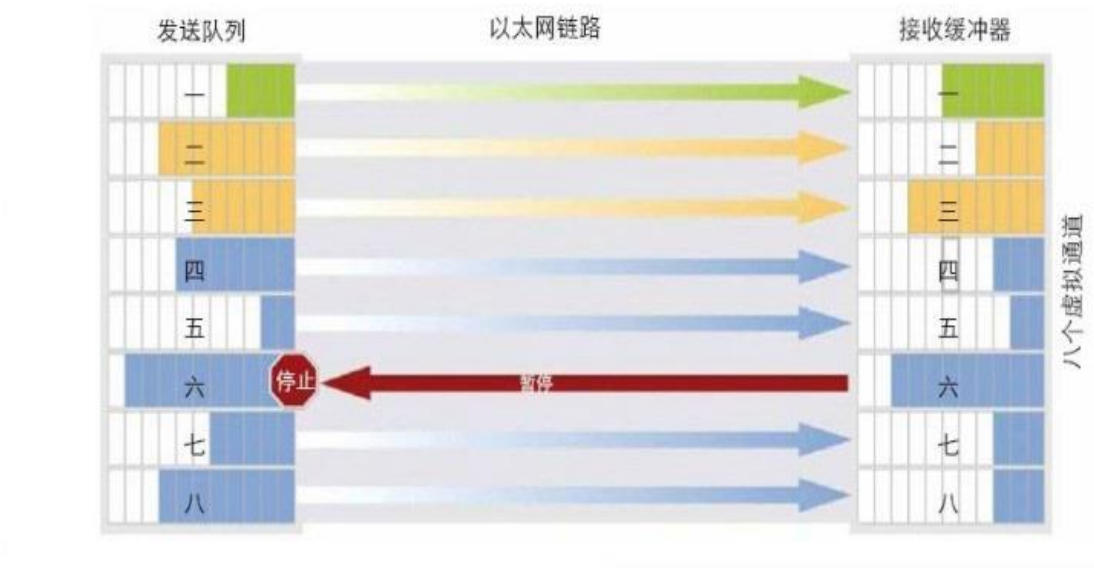
```
Switch# show running-config interface eth-0-1
Building configuration...
!
interface eth-0-1
  loopback-detect enable
loopback-detect packet vlan 2
```

11 PFC 配置

11.1 PFC 简介

基于优先级的流量控制（Priority-based Flow Control，缩写：PFC）是一种更精密的流量控制机制，强化了传统 flow control 机制的功能（如图 11-1）。当前以太网暂停选择（IEEE 802.3 Annex 31B）也能达到无丢包的要求，但它会阻止一条链路上的所有流量，本质上来讲，它会暂停整条链路。PFC 允许在一条以太网链路上创建 8 个虚拟通道，并为每条虚拟通道指定一个 IEEE 802.1p 优先等级，允许单独暂停和重启任意一条虚拟通道，同时允许其它虚拟通道的流量无中断通过。这一机制使网络能够为单个虚拟链路创建无丢包类别的服务，使其能够与同一接口上的其它流量类型共存。

图 11-1 PFC 工作原理



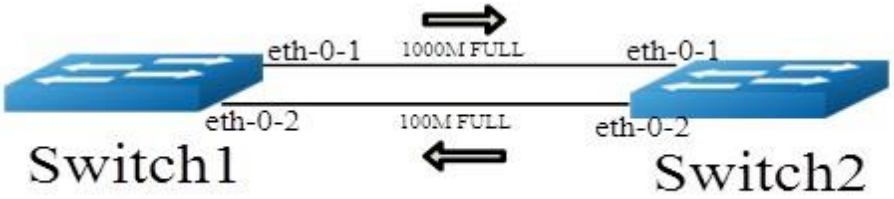
当本端发生拥塞时，设备根据本端接收报文的 802.1p 优先级进行处理。如果接收报文的 802.1p 优先级使能了 PFC 功能，则接收报文并向对端发送 PFC PAUSE 帧，对端设备收到 PFC PAUSE 帧会暂停向本端发送该类报文。此过程会持续直至拥塞结束；如果未使能 PFC 功能，该类报文将直接被丢弃。

11.2 配置 PFC 功能

当本端和对端的 PFC 功能均为开启状态时，PFC 功能才会生效。用户可以对报文经过的所有端口配置一致的 PFC 功能，可以避免传输过程中出现丢包的现象。

11.2.1 拓扑

图11-2 PFC示意图



11.2.2 使能 PFC 功能

使能两端的交换机 Switch1 和 Switch2 的 PFC 功能，下面以 Switch1 为例。

表11-1 配置步骤

命令举例	操作	说明
Switch1# configure terminal	进入全局配置模式	-
Switch1(config)# lldp enable	全局使能 LLDP	缺省情况下，未开启该功能
Switch1(config)# interface eth-0-1	进入接口配置模式	-
Switch1(config-if)#lldp enable	在接口下使能 LLDP	缺省情况下，未开启该功能
Switch1(config-if)# lldp tlv 8021-org-specific dcbx	在接口下使能 dcbx tlv	除 Link Aggregation TLV 的所有 IEEE 802.1 TLV 都已使能
Switch1(config-if)# priority-flow-control mode on	在端口 1 上使能 PFC，不与对端协商	缺省情况下，未启用该功能
Switch1(config-if)# priority-flow-control enable priority 2 3 4	配置在 priority 2 3 4 上使能 PFC	缺省情况下，未启用该功能
Switch1(config)# interface eth-0-2	进入接口配置模式	-
Switch1(config-if)#lldp enable	在接口下使能 lldp	缺省情况下，未开启该功能
Switch1(config-if)# lldp tlv 8021-	在接口下使能 dcbx tlv	除 Link Aggregation TLV 的所

命令举例	操作	说明
org-specific dcbx		有 IEEE 802.1 TLV 都已使能
Switch1(config-if)# priority-flow-control mode auto	在端口 2 上使能 PFC，需要与对端协商成功才能启用	缺省情况下，未启用该功能
Switch1(config-if)# priority-flow-control enable priority 2 3 4	配置在 priority 2 3 4 上使能 PFC	缺省情况下，未启用该功能
Switch1(config-if)# exit	退出接口配置模式	-

说明

- 基于优先级的流控制仅在物理接口的全双工链路下有效。
- 更多LLDP相关内容请详见网络管理部分的“LLDP配置”

11.2.3 显示 PFC 的状态信息

表11-2 显示PFC的状态信息

命令	操作	说明
show priority-flow-control [*if-name*]	查看 PFC 的状态信息	-

查看 PFC 的状态信息：

```
Switch# show priority-flow-control
Port                PFC-enable          PFC-enable on priority
                    admin     oper      admin     oper
------------------------------------------------------------
eth-0-1             on        on        234       234
eth-0-2             auto      off       234       234
eth-0-3             off       off       off       off
eth-0-4             off       off       off       off
```

12 风暴控制配置

12.1 风暴控制简介

风暴控制是指在指定接口上，通过对接收的最大广播、最大未知组播以及最大未知单播流量进行限制，防止泛洪消耗过多的交换机资源，确保业务正常运行。

可以使用以下两种方式进行风暴控制：

- 百分比模式 (Level)：报文占可用带宽的最大百分比
- 包速率模式 (Packets per second，缩写：PPS)：每秒钟发送报文的最大数量

12.2 配置风暴控制

12.2.1 使用百分比模式配置风暴控制

表12-1 使用百分比模式配置风暴控制

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-
Switch(config-if)# storm-control unicast level 0.1	设置限制未知单播报文的百分比	取值范围为 0.00~100.00；缺省情况下，未在二层端口上配置风暴控制
Switch(config-if)# storm-control multicast level 1	设置限制组播报文的百分比	
Switch(config-if)# storm-control broadcast level 10	设置限制广播报文的百分比	
Switch(config-if)# end	退出到 EXEC 模式	-

12.2.2 使用包速率模式配置风暴控制

表12-2 使用包速率模式配置风暴控制

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-
Switch(config-if)# storm-control unicast pps 1000	设置未知单播报文每秒通过 1000 个	取值范围为 0~1000000000；缺省情况下，未在二层端口上配置风暴控制
Switch(config-if)# storm-control multicast pps 10000	设置组播报文每秒通过 10000 个	
Switch(config-if)# storm-control broadcast pps 100000	设置广播报文每秒通过 100000 个	
Switch(config-if)# end	退出到 EXEC 模式	-

12.2.3 显示风暴控制的配置信息

表12-3 显示风暴控制的配置信息

命令	操作	说明
show storm-control [**interface** *if-name*]	显示风暴控制在接口上的配置信息	-

- 显示风暴控制在接口上的配置信息（百分比模式）：

```
Switch# show storm-control interface eth-0-1

Port        ucastMode ucastLevel bcastMode bcastLevel mcastMode mcastLevel
eth-0-1 Level                 0.10 Level                10.00 Level                1.00
```

- 显示风暴控制在接口上的配置信息（包速率模式）：

```
Switch# show storm-control interface eth-0-1

Port        ucastMode ucastLevel bcastMode bcastLevel mcastMode mcastLevel
eth-0-1 PPS             1000              PPS             100000          PPS             10000
```

13 二层协议透明传输配置

13.1 二层协议透传简介

二层协议透明传输通过替换用户私网的二层协议报文的组播目的 MAC 地址为特定的组播 MAC 地址，使用户在不同站点上连接运营商网络时能正常运行二层协议。换言之，运营商网络能透明传输 STP/RSTP/MSTP 报文，因此用户可以跨越运营商网络构建自己的 STP 树，切断冗余链路。

当二层协议报文透传功能被启用后，在运营商网络边缘的交换机会使用一个新的二层头封装二层协议报文，然后向运营商网络传输。在运营商的网络里，该封装后的报文作为普通报文传输。当报文到达运营商网络边缘时，该报文新加的二层头被剥去，然后二层协议报文被转发给用户交换机处理。

二层协议报文透传功能可以独立使用也可以和 QinQ 功能一起使用。

13.2 配置二层协议透传

13.2.1 配置透传指定的二层协议报文

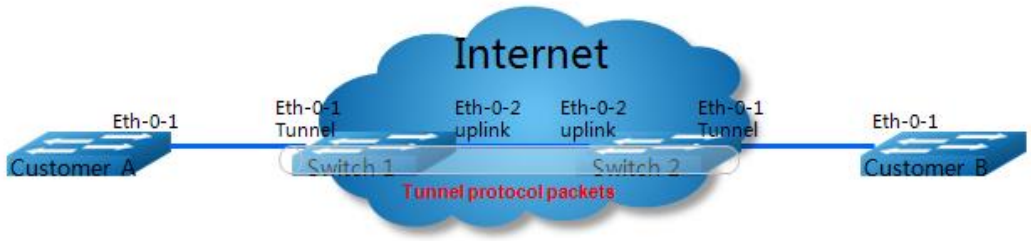
i. 介绍

指定的二层协议报文包括 STP BPDU 报文，Slow Protocol 报文，802.1x EAPOL 报文和 CFM 报文。在下面的例子中，配置 Switch1 eth-0-1 和 Switch2 eth-0-1 为 Tunnel 端口。配置 Switch1 eth-0-2 和 Switch2 eth-0-2 为上联口。如果在 Switch1 的 eth-0-1 口上收到这四种协议报文，协议报文会加上新的二层头然后从上联口发出。

在新的二层头中：目的 MAC 地址是 tunnel dmac；源 MAC 地址是交换机的 route-mac；VLAN ID 是 tunnel evc 所对应的 VLAN ID；VLAN priority 是配置的 Layer 2 protocol COS；Ethertype 是 0xFFEE。如果在 Switch2 的 eth-0-2 上收到带上新二层头的协议报文，协议报文上所带的新二层头会被剥去，然后从 Switch2 的 eth-0-1 发出。

ii. 拓扑

图13-1 配置透传指定的二层协议报文示意图



iii. **配置步骤**

使用下表所示的命令配置 Switch 1 和 Switch 2。

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# vlan database	进入 VLAN 配置模式
Switch(config-vlan)# vlan 2-5	创建 vlan 2-5
Switch(config)# ethernet evc evc_c1	创建 EVC evc_c1
Switch(config-evc)# dot1q mapped-vlan 2	配置 evc_c1 对应的 VLAN ID 为 2
Switch(config)# ethernet evc evc_c2	创建 EVC evc_c2
Switch(config-evc)# dot1q mapped-vlan 3	配置 evc_c2 对应的 VLAN ID 为 3
Switch(config)# ethernet evc evc_c3	创建 EVC evc_c3
Switch(config-evc)# dot1q mapped-vlan 4	配置 evc_c3 对应的 VLAN ID 为 4
Switch(config)# ethernet evc evc_c4	创建 EVC evc_c4
Switch(config-evc)# dot1q mapped-vlan 5	配置 evc_c3 对应的 VLAN ID 为 5
Switch(config)# l2protocol enable	全局使能二层协议报文透传
Switch(config)# l2protocol tunnel-dmac 0100.0CCD.CDD2	全局配置 tunnel dmac
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# no shutdown	配置端口为 UP 状态
Switch(config-if)# switchport mode trunk	配置端口为 Trunk 口
Switch(config-if)# switchport trunk allowed vlan add 2-5	配置端口允许 VLAN 2-5 通过

命令举例	操作步骤
Switch(config-if)# spanning-tree port disable	在端口上关闭 STP 协议
Switch(config-if)# l2protocol stp tunnel evc evc_c1	配置 STP BPDU 报文 tunnel 到 evc_c1
Switch(config-if)# l2protocol slow-proto tunnel evc evc_c	配置 Slow Protocol 报文 tunnel 到 evc_c2
Switch(config-if)# l2protocol dot1x tunnel evc evc_c3	配置 dot1x EAPOL 报文 tunnel 到 evc_c3
Switch(config-if)# l2protocol cfm tunnel evc evc_c4	配置 CFM 报文 tunnel 到 evc_c4
Switch(config)# interface eth-0-2	进入接口配置模式
Switch(config-if)# no shutdown	配置端口为 UP 状态
Switch(config-if)# switchport mode trunk	配置端口为 Trunk 口
Switch(config-if)# switchport trunk allowed vlan add 2-5	配置端口允许 VLAN 2-5 通过
Switch(config-if)# l2protocol uplink enable	配置端口为二层协议报文透传时的上联口

iv. 显示与维护

命令	操作
show l2protocol [**interface** *if-name* | **tunnel-dmac**]	显示二层协议报文透传功能的配置

显示二层协议报文透传功能的配置：

```
Switch1# show l2protocol interface eth-0-1

Interface    PDU Address        MASK                 Status       EVC
=========   ==============   ==============   ========   ================
eth-0-1       stp                FFFF.FFFF.FFFF    Tunnel       evc_c1
eth-0-1       slow-proto         FFFF.FFFF.FFFF    Tunnel       evc_c2
eth-0-1       dot1x              FFFF.FFFF.FFFF    Tunnel       evc_c3
eth-0-1       cfm                FFFF.FFFF.FFFF    Tunnel       evc_c4

Switch1# show l2protocol interface eth-0-2

Interface    PDU Address        MASK                 Status       EVC
=========   ==============   ==============   ========    ================
eth-0-2       stp                FFFF.FFFF.FFFF    Peer         N/A
eth-0-2       slow-proto         FFFF.FFFF.FFFF    Peer         N/A
eth-0-2       dot1x              FFFF.FFFF.FFFF    Peer         N/A
eth-0-2       cfm                FFFF.FFFF.FFFF    Peer         N/A
```

eth-0-2	N/A	N/A	Uplink	N/A

Switch1# show l2protocol tunnel-dmac

Layer2 protocols tunnel destination MAC address is 0100.0ccd.cdd2

13.2.2 配置透传可配的二层协议报文

i. 介绍

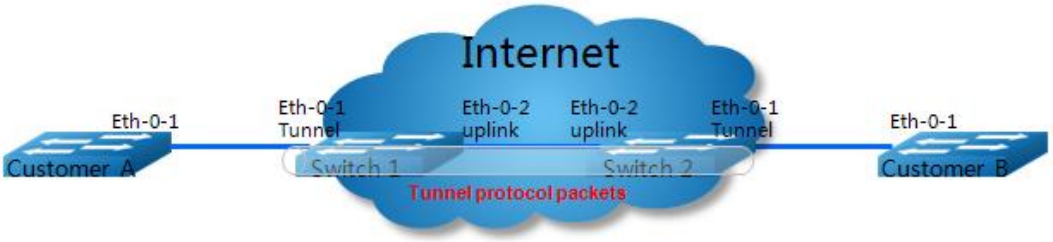
可配的二层协议报文是指地址是0180.c200.0000 – 0x0180.c2ff.ffff间的报文，全MAC地址协议报文是指地址是0000.0000.0000 – ffff.ffff.fff间的报文。

在下面的例子中，Switch1 eth-0-1和Switch2 eth-0-1配置成Tunnel端口。Switch1 eth-0-2和Switch2 eth-0-2配置成上联口。如果在Switch 1的eth-0-1口上收到协议报文符合配置的MAC地址，协议报文会加上新的二层头然后从上联口发出。

在新的二层头中：目的MAC地址是tunnel dmac；源MAC地址是交换机的route-mac；VLAN ID是tunnel evc所对应的VLAN ID；VLAN priority是配置的Layer 2 protocol COS；Ethertype是0xFFEE。如果在Switch2的eth-0-2上收到带上新二层头的协议报文，协议报文上所带的新二层头会被剥去，然后从Switch2的eth-0-1发出。

ii. 拓扑

图13-2 配置透传可配的二层协议报文拓扑图



iii. 配置举例

使用下表所示的命令，配置Switch 1和Switch 2。

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# vlan database	进入 VLAN 配置模式

命令举例	操作步骤
Switch(config-vlan)# vlan 2-4	创建 VLAN 2-4
Switch(config)# ethernet evc evc_c1	创建 EVC evc_c1
Switch(config-evc)# dot1q mapped-vlan 2	配置 evc_c1 对应的 VLAN ID 为 2
Switch(config)# ethernet evc evc_c2	创建 EVC evc_c2
Switch(config-evc)# dot1q mapped-vlan 3	配置 evc_c2 对应的 VLAN ID 为 3
Switch(config)# ethernet evc evc_c3	创建 EVC evc_c3
Switch(config-evc)# dot1q mapped-vlan 4	配置 evc_c2 对应的 VLAN ID 为 4
Switch(config)# l2protocol enable	全局使能二层协议报文透传
Switch(config)# l2protocol tunnel-dmac 0100.0CCD.CDD2	全局配置 tunnel dmac
Switch(config)# l2protocol mac 3 0180.C200.0008	配置可透传的二层协议报文 3 的 mac 地址为 0180.C200.0008
Switch(config)# l2protocol mac 4 0180.C200.0009	配置可透传的二层协议报文 4 的 mac 地址为 0180.C200.0009
Switch(config)# l2protocol full-mac 0100.0CCC.CCCC	配置可透传全 mac 地址为 0100.0CCC.CCCC
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# no shutdown	配置端口为 UP 状态
Switch(config-if)# switchport mode trunk	配置端口为 Trunk 口
Switch(config-if)# switchport trunk allowed vlan add 2-4	配置端口允许 VLAN 2-4 通过
Switch(config-if)# spanning-tree port disable	在端口上关闭 STP 协议
Switch(config-if)# l2protocol mac 3 tunnel evc evc_c1	配置将二层协议报文 3 透传到 evc_c1
Switch(config-if)# l2protocol mac 4 tunnel evc evc_c2	配置将二层协议报文 4 透传到 evc_c2
Switch(config-if)# l2protocol full-mac tunnel evc evc_c3	配置将全 mac 地址透传到 evc_c3
Switch(config)# interface eth-0-2	进入端口模式

命令举例	操作步骤
Switch(config-if)# no shutdown	配置端口为 UP 状态
Switch(config-if)# switchport mode trunk	配置端口为 Trunk 口
Switch(config-if)# switchport trunk allowed vlan add 2-4	配置端口允许 VLAN 2-4 通过
Switch(config-if)# l2protocol uplink enable	配置端口为二层协议报文透传时的上联口

iv. 显示与维护

命令	操作
show l2protocol [**interface** *if-name* | **tunnel-dmac**]	显示二层协议报文透传功能的配置

显示二层协议报文透传功能的配置：

```
Switch# show l2protocol interface eth-0-1

Interface    PDU Address        MASK                Status      EVC
=========    ==============   ==============   ========   ================
eth-0-1      0180.c200.0008   FFFF.FFFF.FFFF   Tunnel      evc_c1
eth-0-1      0180.c200.0009   FFFF.FFFF.FFFF   Tunnel      evc_c2
eth-0-1      0100.0ccc.cccc   FFFF.FFFF.FFFF   Tunnel      evc_c3
eth-0-1      stp              FFFF.FFFF.FFFF   Peer        N/A
eth-0-1      slow-proto       FFFF.FFFF.FFFF   Peer        N/A
eth-0-1      dot1x            FFFF.FFFF.FFFF   Peer        N/A
eth-0-1      cfm              FFFF.FFFF.FFFF   Peer        N/A

Switch# show l2protocol interface eth-0-2

Interface    PDU Address        MASK                Status      EVC
=========    ==============   ==============   ========   ================
eth-0-2      0180.c200.0008   FFFF.FFFF.FFFF   Peer        N/A
eth-0-2      0180.c200.0009   FFFF.FFFF.FFFF   Peer        N/A
eth-0-2      0100.0ccc.cccc   FFFF.FFFF.FFFF   Peer        N/A
eth-0-2      stp              FFFF.FFFF.FFFF   Peer        N/A
eth-0-2      slow-proto       FFFF.FFFF.FFFF   Peer        N/A
eth-0-2      dot1x            FFFF.FFFF.FFFF   Peer        N/A
eth-0-2      cfm              FFFF.FFFF.FFFF   Peer        N/A
eth-0-2      N/A              N/A              Uplink      N/A
```

```
Switch# show l2protocol tunnel-dmac
Layer2 protocols tunnel destination MAC address is 0100.0ccd.cdd2
```

14 MSTP 配置

14.1 MSTP 简介

多生成树（Multiple Spanning Tree，缩写：MST）是把 IEEE 802.1w 的快速生成树（Rapid Spanning Tree，缩写：RST）算法扩展而得到的。MST 能够通过 Trunk 链路建立多个生成树，关联 VLANs 到相关的生成树实例，并且每个生成树实例可以具备区别于其他实例的拓扑结构。MST 提供了多个数据转发路径和负载均衡，提高了网络容错能力。因为一个实例（转发路径）的故障不会影响其他实例（转发路径）。一个生成树实例只能存在于一致的 VLAN 实例分配的桥中，必须用同样的 MST 配置信息来配置一组桥，使这些桥处于同一组生成树实例中，具备同样的 MST 配置信息的互连的桥构成多生成树区（MST Region）。

多生成树协议（Multiple Spanning Tree Protocol，缩写：MSTP）将环路网络修剪成为一个无环的树型网络，避免报文在环路网络中的增生和无限循环，同时还提供了数据转发的多个冗余路径，在数据转发过程中实现 VLAN 数据的负载均衡。MSTP 兼容 STP 和 RSTP，并且可以弥补 STP 和 RSTP 的缺陷。它既可以快速收敛，也能使不同 VLAN 的流量沿各自的路径分发，从而为冗余链路提供了更好的负载分担机制。

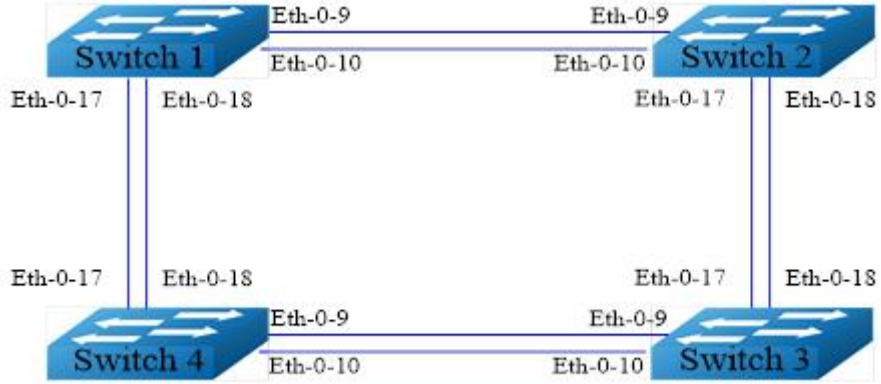
14.2 配置 MSTP 基本功能

14.2.1 介绍

此配置示例假定您正在运行的二层协议。如果您使用的是非二层协议，必须在每个端口上运行的交换机端口命令来设置二层协议。MSTP 的基本功能包括：配置设备的 MSTP 工作模式、创建 MSTP域、创建 MSTP 用例、配置 STP 的优先级等。

14.2.2 拓扑

图14-1 MSTP拓扑示例



14.2.3 配置步骤

表14-1 配置步骤

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# spanning-tree mode mstp	配置 STP 的工作模式	可以配置的工作模式：STP 模式、RSTP 模式或 MSTP 模式；默认为 STP 模式
Switch(config)# vlan database	进入 VLAN 模式	-
Switch(config-vlan)# vlan 10	创建 VLAN10	-
Switch(config-vlan)# vlan 20	创建 VLAN20	-
Switch(config-vlan)# exit	退出 VLAN 模式	-
Switch(config)# spanning-tree mst configuration	进入 MSTP 配置模式	-
Switch(config-mst)# region RegionName	配置 MSTP 的区域名字	默认域名为空字符串
Switch(config-mst)# instance 1 vlan 10	配置 MSTP 的实例 1 关联 VLAN10	在 VLANs 映射到 MST 用例之前，确保已经创建 VLANs，否则配置不会生效；这些 VLANs 被删除时，对应的 MST 用例也将被删除
Switch(config-mst)# instance 2 vlan 20	配置 MSTP 的实例 2 关联 VLAN20	
Switch(config-mst)# exit	退出 MSTP 配置模式	-
Switch(config)# interface eth-0-9	进入接口配置模式	-

命令举例	操作	说明
Switch(config-if)# switchport mode trunk	设置接口为 Trunk	-
Switch(config-if)# switchport trunk allowed vlan all	配置 Trunk 允许所有的 VLAN 通过	-
Switch(config-if)# no shutdown	配置端口为 UP 状态	-
Switch(config-if)# exit	退出接口配置模式	-
Switch(config)# interface eth-0-10	进入接口配置模式	-
Switch(config-if)# switchport mode trunk	设置接口为 Trunk	-
Switch(config-if)# switchport trunk allowed vlan all	配置 Trunk 允许所有的 VLAN 通过	-
Switch(config-if)# no shutdown	配置端口为 UP 状态	-
Switch(config-if)# exit	退出接口配置模式	-
Switch(config)# interface eth-0-17	进入接口配置模式	-
Switch(config-if)# switchport mode trunk	设置端口为 Trunk 模式	-
Switch(config-if)# switchport trunk allowed vlan all	配置 Trunk 允许所有的 VLAN 通过	-
Switch(config-if)# no shutdown	配置端口为 UP 状态	-
Switch(config-if)# exit	退出接口配置模式	-
Switch(config)# interface eth-0-18	进入接口配置模式	-
Switch(config-if)# switchport mode trunk	设置端口为 Trunk 模式	-
Switch(config-if)# switchport trunk allowed vlan all	配置 Trunk 允许所有的 VLAN 通过	-
Switch(config-if)# no shutdown	配置端口为 UP 状态	-
Switch(config-if)# exit	退出接口配置模式	-
Switch(config)# exit	退出全局配置模式	-

下表配置了 Switch 1的 STP 优先级、Switch 2 和 Switch 3 的 STP 用例的优先级值，并全局启用Switch 1~Switch 4 的 STP 功能。

Switch 1：

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# spanning-tree priority 0	设置 STP 的优先级为 0	STP 优先级的默认值 32768 (或十六进制 0x8000)。数值越小，优先级越高
Switch(config)# spanning-tree enable	全局启用 STP 功能	缺省情况下，系统默认关闭 STP

Switch 2：

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# spanning-tree instance 1 priority 0	配置 STP 实例 1 的优先级为 0	每个用例优先级值默认为 32768。数值越小，优先级越高
Switch(config)# spanning-tree enable	全局启用 STP 功能	缺省情况下，系统默认关闭 STP

Switch 3：

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# spanning-tree instance 2 priority 0	设置 STP 实例 2 的优先级为 0	每个用例优先级值默认为 32768。数值越小，优先级越高
Switch(config)# spanning-tree enable	全局启用 STP 功能	缺省情况下，系统默认关闭 STP

Switch 4：

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# spanning-tree enable	全局启用 STP 功能	缺省情况下，系统默认关闭 STP

14.2.4 显示 MSTP 端口状态

表14-2 显示MSTP端口状态

命令	操作	说明
show spanning-tree mst brief [**interface** *if-name* | **instance** *instance-id*]	显示 MSTP 的简略信息	-

显示MSTP的端口的状态：

```
Switch# show spanning-tree mst brief

##### MST0:    Vlans: 1
Multiple spanning tree protocol Enabled
Root ID        Priority          0 (0x0000)
                Address         2225.fa28.c900
                Hello Time    2 sec    Max Age    20 sec Forward Delay 15 sec
Bridge ID      Priority          0 (0x0000)
                Address         2225.fa28.c900
                Hello Time    2 sec    Max Age    20 sec Forward Delay 15 sec
                Aging Time    300 sec
Interface      Role              State              Cost         Priority.Number       Type
--------------------------------------------------------------------------------
eth-0-9        Designated        Forwarding         20000              128.9           P2p
eth-0-10       Designated        Forwarding         20000              128.10          P2p
eth-0-17       Designated        Forwarding         20000              128.17          P2p
eth-0-18       Designated        Forwarding         20000              128.18          P2p
##### MST1:    Vlans: 10
Root ID        Priority          1 (0x0001)
                Address         9c9a.7d91.9f00
Bridge ID      Priority        32769 (0x8001)
                Address         2225.fa28.c900
Interface      Role              State              Cost         Priority.Number       Type
--------------------------------------------------------------------------------
eth-0-9        Rootport          Forwarding         20000              128.9           P2p
eth-0-10       Alternate         Discarding         20000              128.10          P2p
eth-0-17       Designated        Forwarding         20000              128.17          P2p
eth-0-18       Designated        Forwarding         20000              128.18          P2p
##### MST2:    Vlans: 20
Root ID        Priority          2 (0x0002)
                Address         304c.275b.b200
Bridge ID      Priority        32770 (0x8002)
                Address         2225.fa28.c900
Interface      Role              State              Cost         Priority.Number       Type
```

```
---------------------------------------------------------------------------
eth-0-9     Alternate    Discarding    20000      128.9      P2p
eth-0-10    Alternate    Discarding    20000      128.10     P2p
eth-0-17    Rootport     Forwarding    20000      128.17     P2p
eth-0-18    Alternate    Discarding    20000      128.18     P2p
```

14.3 配置影响 MSTP 收敛的参数

MSTP 吸收了 STP 和 RSTP 的优点，既可以实现快速收敛，又提供了数据转发的各个冗余路径。通过合理配置 MSTP 定时器、BPDU 报文所允许的最大跳数、端口的链路类型等可以更快速地实现拓扑收敛。

14.3.1 配置 MSTP 定时器

本小节介绍了如何配置生成树计算的三个时间参数：Forward Time、Hello Time 以及 Max Age。

i. 配置Forward Time时间

Forward Time 时间，即根桥上每个端口从监听状态转化为学习状态或从学习状态转化为转发状态的时间间隔。

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# spanning-tree forward-time 16	配置 Forward Time 时间	取值范围为 4～30，单位：秒；默认值是 15 秒。建议配置的时间间隔在 7 秒以上

ii. 配置Hello Time时间

Hello Time 时间，即根桥上定期发送 BPDU 报文的时间间隔。

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# spanning-tree hello-time 5	配置 Hello Time 时间	取值范围为 1～10，单位：秒；默认值为 2 秒

iii. 配置Max Age时间

最大超时时间可以用来确定配置消息是否超时，有效地避免了报文环回。

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# spanning-tree max-age 12	配置 Max Age 时间	取值范围是 6～40，单位：秒；默认值为 20 秒

为了防止网络频繁发生震荡，配置 Max Age 时间需要遵循以下公式：

- Max Age ≥ 2 × (Hello Time + 1s)
- Max Age ≤ 2 × (Forward Time – 1s)

14.3.2 配置端口的链路类型

用户可以在端口上配置三种链路类型：auto、point-to- point 以及 shared。

表14-3 配置端口的链路类型

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-
Switch(config-if)# spanning-tree link-type shared	配置 STP 的链路类型为共享链路	缺省情况下，链路类型为 auto

14.3.3 配置最大 BPDU 数目

表14-4 配置最大BPDU数目

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# spanning-tree transmit-holdcount 5	配置 1 秒内允许发出的最大 BPDU 数目	取值范围为 1～10，默认值为 3 个

14.3.4 配置 BPDU 报文过滤功能

i. 全局模式下配置BPDU报文过滤功能

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# spanning-tree edgeport bpdu-filter	配置边缘端口过滤 BPDU 报文	默认关闭 BPDU 报文过滤功能；配置 BPDU 报文过滤的端口不会接收和发送 BPDU 报文

ii. 接口模式下配置边缘端口和BPDU报文过滤功能

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-
Switch(config-if)# spanning-tree edgeport	配置端口为边缘端口	缺省情况下，未配置端口为边缘端口
Switch(config)# spanning-tree edgeport bpdu-filter enable	在边缘端口上启用 BPDU 报文过滤功能	如果同时配置了 BPDU 保护和 BPDU 报文过滤功能，则 BPDU 报文过滤功能起作用

14.3.5 配置 BPDU 报文允许的最大跳数

指定最大跳数是为了防止 BPDU 报文在网络中环回。当交换机收到的报文超过最大跳数，将丢弃 BPDU 报文。

表14-5 配置BPDU报文允许的最大跳数

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# spanning-tree max-hops 25	配置 BPDU 报文所允许的最大跳数	最大跳数取值范围为 1~40，默认值为 20

14.4 配置 MSTP 保护功能

本小节介绍了 MSTP 相关的保护功能，用户可根据实际情况选择配置其中一种或多种保护功能。

14.4.1 配置 BPDU 保护功能

用户可以通过命令全局配置 BPDU 保护功能，或者配置边缘端口后，开启边缘端口的 BPDU 保护功能。

表14-6 全局模式下配置BPDU保护功能

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# spanning-tree edgeport bpdu-guard	开启 BPDU 保护功能	缺省情况下，BPDU 保护功能是关闭的。当 BPDU 保护功能打开时，如果接收到 BPDU 报文，则端口会 shutdown 。用户可以通过 **no shutdown** 命令重新开启端口或配置 errdisable 定时器功能，重新开启端口

表14-7 配置边缘端口的BPDU保护功能

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-
Switch(config-if)# spanning-tree edgeport	配置端口为边缘端口	缺省情况下，未配置端口为边缘端口
Switch(config-if)# spanning-tree edgeport bpdu-guard enable	开启 BPDU 保护功能	缺省情况下，BPDU 保护功能是关闭的

14.4.2 配置 TC 消息保护功能

当启用 TC 保护时，在每个 hello-time 间隔内，处理的 TC 消息数目不大于系统的 TC 保护门限值。

表14-8 配置TC消息保护功能

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# spanning-tree tc-protection	开启 TC 消息保护功能	缺省情况下，TC 消息保护功能是关闭的
Switch(config)# spanning-tree hello-time 5	配置根桥定期发送 BPDU 报文的时间间隔	取值范围为 1～10，单位：秒；默认时间间隔为 2 秒
Switch(config)# spanning-tree tc-protection threshold 255	配置 TC 消息保护的门限值	门限值的取值范围为 1~255，默认值为 1

14.4.3 配置端口的 Root 保护功能

开启这个功能后，交换机将不会接收优先级高的 BPDU 报文。如果运行 STP 协议，就会转入监听状态；如果运行 RSTP 和 MSTP，就会转入阻塞状态。

表14-9 配置端口的Root保护功能

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-
Switch(config-if)# spanning-tree guard root	开启 Root 保护功能	缺省情况下，Root 保护功能处于关闭状态

14.4.4 配置端口的环路保护功能

开启这个功能后，交换机能够防止在网络中形成数据转发环路的形成。

表14-10 配置端口的环路保护功能

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-

命令举例	操作	说明
Switch(config-if)# spanning-tree guard loop	开启环路保护功能	缺省情况下，环路保护功能处于关闭状态

说明

环路保护功能需要在非指定端口上启用。当非指定端口上启用了环路保护功能，并且在最大超时时间内没有收到 BPDU 报文，该端口将会进入 loop-inconsistent 阻塞状态，而不是监听、学习、转发等一系列的状态转换。一旦端口进入 loop-inconsistent 状态，该端口将不能转发业务数据。

14.4.5 显示 STP 详细信息

表14-11 显示STP详细信息

命令	操作	说明
show spanning-tree	显示 STP 的详细信息	-

显示 STP 的详细信息：

```
Switch# show spanning-tree
  Bridge up - Spanning Tree Enabled
 Mode - Multiple spanning tree protocol
 Path Cost Standard - dot1t
 CIST Root Path Cost 0 - CIST Root Port 0 -   CIST Bridge Priority 32768
 Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
 Tx Hold Count 6
 CIST Root Id 80008afa58e9cb00
 CIST Reg Root Id 80008afa58e9cb00
 CIST Bridge Id 80008afa58e9cb00
 Edgeport bpdu-filter disabled
 Edgeport bpdu-guard disabled
 eth-0-1: Port 1 - Id 8001 - Role Designated - State Forwarding
 eth-0-1: Designated External Path Cost 0 -Internal Path Cost 0
 eth-0-1: Configured Path Cost 20000 - Add type Explicit ref count 1
 eth-0-1: Designated Port Id 8001 - CIST Priority 128
 eth-0-1: CIST Root 80008afa58e9cb00
 eth-0-1: Regional Root 80008afa58e9cb00
 eth-0-1: Designated Bridge 80008afa58e9cb00
```

```
  eth-0-1: Message Age 0 - Max Age 20
  eth-0-1: CIST Hello Time 2 - Forward Delay 15
  eth-0-1: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change t
imer 0
  eth-0-1: Forward-transitions 2
  eth-0-1: BPDU sent 373 - BPDU received 0
  eth-0-1: Version Multiple spanning tree protocol - Received None - Send MSTP
  eth-0-1: No edgeport configured - Current edgeport off
  eth-0-1: Edgeport bpdu-guard    Default - Current edgeport bpdu-guard off
  eth-0-1: Edgeport bpdu-filter Default - Current edgeport bpdu-filter off
  eth-0-1: No root guard configured - Current root guard off
  eth-0-1: No loop guard configured - Current loop guard off
  eth-0-1: Configured Link Type auto - Current point-to-point
```

15 M-LAG 配置

15.1 M-LAG 简介

跨设备链路聚合组（Multichassis Link Aggregation Group，缩写：M-LAG），不同设备之间通过链路连接，实现跨设备链路聚合。在高可靠性的数据中心拓扑中，典型的会通过两台聚合交换机来连接 TOR 交换机和服务器以提供冗余保护。在这样的拓扑结构中，生成树协议通过 block 聚合交换机的一半的端口来防止网络环路，但这样做会降低 50%的带宽。

通过部署 MLAG 可以解决这个问题。在两台聚合交换机的中间通过一条 peer-link 链路进行连接，使其在逻辑上如同一台设备。两台设备上的端口共同形成聚合口，使得所有端口可以共同参与数据流量的转发。

M-LAG 机制具备以下优点：

- 在网络流量增加的时候提供了更高的带宽；
- 通过减少被 STP block 的端口的方式更加高效地利用了网络带宽；
- 使用静态 LAG 或者 LACP 来连接其他交换机或者服务器，而不需要借助其他协议；
- 支持通过生成树协议来防止环路

15.2 配置 M-LAG

15.2.1 进入 M-LAG 配置模式

表15-1 进入M-LAG配置模式

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# mlag configuration	进入 M-LAG 配置模式	使用 **exit** 命令可以退出该模式，该操作不影响该模式下的配置。使用 **no** 命令删除该模式，该模式下的所

命令举例	操作	说明
		有配置均会被删除。

15.2.2 配置 peer-link

此命令用来指定连接 M-LAG 邻居所使用的接口。要形成 M-LAG 邻居，需要有两台互联的设备，中间用来连接彼此的接口称作 peer-link。Peer-link 上既承载了协议报文，也承载了数据报文。详细的示例请见 15.2.4 配置举例。

表15-2 配置peer-link

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# mlag configuration	进入 M-LAG 配置模式	使用 **exit** 命令可以退出该模式，该操作不影响该模式下的配置。使用 **no** 命令删除该模式，该模式下的所有配置均会被删除。
Switch(config-mlag)# peer-link eth-0-9	指定连接 M-LAG 邻居所用的接口	只能设置成普通物理口或者聚合口

15.2.3 配置指定 MLAG ID

此命令用来在聚合口上指定 MLAG ID。每个聚合口只能指定一个 MLAG ID，每个 MLAG ID 只能同时被一个聚合口使用。

表15-3 配置指定MLAG ID

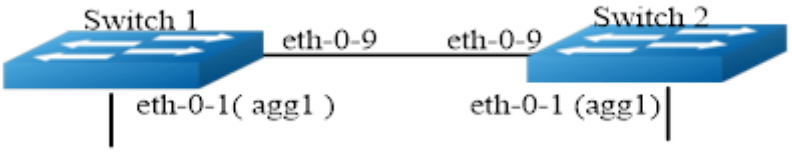
命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# interface agg1	进入聚合 agg1 接口模式	-
Switch(config-if)# mlag 1	在聚合口上指定 MLAG ID	MLAG ID 取值范围为 1~ 55

15.2.4 配置举例

i. 介绍

在 Switch 1 和 Switch 2 之间部署一条 peer-link 聚合链路,两台设备上的端口共同形成聚合口，共同参与数据流量的转发，如下图所示。

ii. 拓扑



iii. 配置Switch 1与Switch 2

Switch 1：

命令举例	操作步骤
Switch1 (config)# vlan database	进入 VLAN 模式
Switch1 (config-vlan)# vlan 10,4094	创建 VLAN10 和 VLAN4094
Switch1(config-vlan)# exit	退出 VLAN 模式并返回全局配置模式
Switch1 (config)# interface eth-0-1	进入接口配置模式
Switch1(config-if)# static-channel-group 1	将此接口加入静态 agg1 组
Switch1(config-if)# no shutdown	配置端口 UP
Switch1(config-if)# exit	退出接口配置模式并返回全局配置模式
Switch1 (config)# interface eth-0-9	进入接口配置模式
Switch1(config-if)# switchport mode trunk	配置接口为 Trunk 口
Switch1(config-if)# switchport trunk allowed vlan all	在此 Trunk 口允许所有 VLAN 通过
Switch1(config-if)# spanning-tree port disable	去使能接口的生成树协议
Switch1(config-if)# no shutdown	配置端口 UP
Switch1(config-if)# exit	退出接口配置模式并返回全局配置模式
Switch1 (config)# interface agg1	进入聚合 agg1 接口模式
Switch1(config-if)# switchport mode trunk	配置为 Trunk 口
Switch1(config-if)# switchport trunk allowed vlan add 10	在此端口上允许 VLAN10 通过
Switch1(config-if)# mlag 1	绑定此接口到 MLAG1 上

命令举例	操作步骤
Switch1(config-if)# exit	退出接口配置模式并返回全局配置模式
Switch1 (config)# interface vlan4094	创建三层接口 VLAN4094
Switch1(config-if)# ip address 12.1.1.1/24	配置 IP 地址为 12.1.1.1/24
Switch1(config-if)# exit	退出接口配置模式并返回全局配置模式
Switch1 (config)# mlag configuration	进入 M-LAG 配置模式
Switch1 (config-mlag)# peer-link eth-0-9	配置 peer link 链路
Switch1 (config-mlag)# peer-address 12.1.1.2	配置 peer 邻居地址
Switch1 (config-mlag)# exit	退出 M-LAG 配置模式

Switch 2：

命令举例	操作步骤
Switch2 (config)# vlan database	进入 VLAN 模式
Switch2 (config-vlan)# vlan 10,4094	创建 VLAN10 和 vlan4094
Switch2(config-vlan)# exit	返回全局配置模式
Switch2 (config)# interface eth-0-1	进入接口配置模式
Switch2(config-if)# static-channel-group 1	将此接口加入到静态 agg1 中
Switch2(config-if)# no shutdown	使能接口 UP
Switch2(config-if)# exit	返回全局配置模式
Switch2 (config)# interface eth-0-9	进入接口配置模式
Switch2(config-if)# switchport mode trunk	配置接口为 Trunk 模式
Switch2(config-if)# switchport trunk allowed vlan all	在此 Trunk 口允许所有 VLAN 通过
Switch2(config-if)# spanning-tree port disable	去使能接口的生成树协议
Switch2(config-if)# no shutdown	使能接口 UP
Switch2(config-if)# exit	返回至全局配置模式
Switch2 (config)# interface agg1	进入 Agg 接口配置模式
Switch2(config-if)# switchport mode trunk	配置接口为 Trunk 口
Switch2(config-if)# switchport trunk allowed vlan add 10	在此接口上允许 VLAN10 通过

命令举例	操作步骤
Switch2(config-if)# mlag 1	绑定此接口到 MLAG1 上
Switch2(config-if)# exit	返回至全局配置模式
Switch2 (config)# interface vlan4094	创建 interface vlan4094
Switch2(config-if)# ip address 12.1.1.2/24	配置 IP 地址 12.1.1.2/24
Switch2(config-if)# exit	返回到全局配置模式
Switch2 (config)# mlag configuration	进入 M-LAG 配置模式
Switch2 (config-mlag)# peer-link eth-0-9	配置 peer link 链路
Switch2 (config-mlag)# peer-address 12.1.1.1	配置 peer 邻居地址
Switch2 (config-mlag)# end	返回至特权模式

iv. 显示配置结果

命令	操作
show mlag	显示 M-LAG 的相关配置信息
show mlag interface	显示 M-LAG 接口信息
show mlag peer	显示 M-LAG 邻居信息

显示 Switch 1 的 M-LAG 配置信息：

```
Switch1# show mlag
MLAG configuration:
----------------
role              : Master
local_sysid : ea90.aecc.cc00
mlag_sysid    : ea90.aecc.cc00
peer-link      : eth-0-9
peer conf      : Yes
Switch1# show mlag interface
mlagid    local-if    local-state       remote-state
1             agg1          up                    up
Switch1# show mlag peer
MLAG neighbor is 12.1.1.2, MLAG version 1
MLAG state = Established, up for 00:13:07
Last read 00:00:48, hold time is 240, keepalive interval is 60 seconds
Received 19 messages,Sent 23 messages
```

```
Open          : received 1, sent 2
KAlive      : received 15, sent 16
Fdb sync : received 0, sent 0
Failover : received 0, sent 0
Conf          : received 1, sent 1
STP Total: received 2, sent 4
  Global    : received 2, sent 3
  Packet    : received 0, sent 0
  Instance: received 0, sent 0
  State      : received 0, sent 1
Connections established 1; dropped 0
Local host: 12.1.1.1, Local port: 61000
Foreign host: 12.1.1.2, Foreign port: 46157
remote_sysid: baa7.8606.8b00
Switch1# show mac address-table
                Mac Address Table
------------------------------------------
(*) - Security Entry
Vlan       Mac Address            Type              Ports
----       -----------            --------       -----
```

显示 Switch 2 的 M-LAG 配置信息：

```
Switch2# show mlag
MLAG configuration:
-----------------
role               : Slave
local_sysid : baa7.8606.8b00
mlag_sysid    : ea90.aecc.cc00
peer-link      : eth-0-9
peer conf      : Yes
Switch2# show mlag interface
mlagid    local-if    local-state        remote-state
1             agg1           up                    up
Switch2# show mlag peer
MLAG neighbor is 12.1.1.1, MLAG version 1
MLAG state = Established, up for 00:14:29
Last read 00:00:48, hold time is 240, keepalive interval is 60 seconds
Received 23 messages,Sent 21 messages
Open          : received 1, sent 1
KAlive      : received 17, sent 17
Fdb sync : received 0, sent 0
Failover : received 0, sent 0
Conf          : received 1, sent 1
```

```
STP Total: received 4, sent 2
  Global    : received 3, sent 2
  Packet    : received 0, sent 0
  Instance: received 0, sent 0
  State     : received 1, sent 0
Connections established 1; dropped 0
Local host: 12.1.1.2, Local port: 46157
Foreign host: 12.1.1.1, Foreign port: 61000
remote_sysid: ea90.aecc.cc00
Switch2# show mac address-table
                Mac Address Table
------------------------------------------
(*) - Security Entry
Vlan       Mac Address           Type             Ports
----       -----------           --------       -----
```

16 PoE 配置

16.1 PoE 简介

16.1.1 定义

Power over Ethernet（PoE），即以太网供电。在不改动以太网布线架构的情况下，PoE 技术既能为基于 IP 的终端传输数据信号，还可以对设备进行远程供电。

16.1.2 基本概念

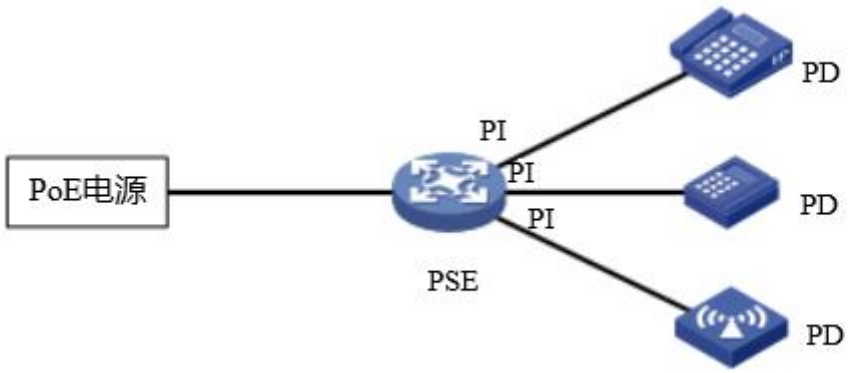
一个完整的 PoE 系统主要由 PoE 电源、PSE、PI 及 PD 组成。其概念如下：

- PoE电源：为整个系统供电。
- PSE：供电端设备（Power Sourcing Equipment，缩写：PSE），为以太网客户端设备供电，管理着整个PoE以太网供电过程。
- PI：电源接口（Power Interface，缩写：PI），是具备PoE供电能力的接口。
- PD：受电端设备（Powered Device，缩写：PD），PoE系统的客户端设备，如IP电话、网络安全摄像机、移动电话充电器及掌上电脑等。

16.1.3 PoE 系统示意图

PoE 系统如图 16-1 所示。

图 16-1 PoE 系统示意图



16.1.4 PoE 供电的优点

PoE 供电主要有以下优点：

- 易于网络设备的远程管理。
- 安全性高，PoE 供电端设备只为需要供电的设备供电，在线路上可以消除漏电的风险。
- 节约成本，不需要为设备提供本地电源，降低部署成本。

16.2 配置 PoE

16.2.1 开启/关闭 PoE 功能

表16-1全局使能/关闭PoE功能

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# power inline enable	开启全局 PoE 供电功能	缺省情况下，开启全局 PoE 供电功能；全局关闭后，不论端口的供电状态是打开还是关闭，均不会对外供电
Switch(config)# no power inline enable	关闭全局 PoE 供电功能	

表16-2端口使能/关闭PoE功能

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch (config)# interface eth-0-1	进入接口配置模式	-
Switch(config-if)# power inline enable	开启端口 PoE 供电功能	缺省情况下，端口的 PoE 供电功能处于开启状态。有 auto 和 static 两种模式供选择
Switch(config-if)# no power inline enable	关闭端口 PoE 供电功能	

说明

- 使用时：自动检测。处于该状态时，PSE自动检测PD，并自动进行分类，然后根据分类进行供电。当PSE检测到有PD连接时，如果此时有足够的剩余功率，则给该PD指定的输出功率，并更新LED的指示；如果没有足够的功率，则由功率分配机制决定是否供电。当在该状态正常供电

过程中，PD有额外申请功率并超过最高设定阈值，则断开对该PD的供电，并更新LED的指示。当正常断开PD与PSE的连接时，则PSE停止对外供电，并更新LED的指示。

- 关闭时：禁止供电。关闭PSE供电功能，无论是否有PD连接都不对其进行供电。此时端口为普通以太网的数据端口，不影响数据的转发。

16.2.2 配置 PoE 电源的最大输出功率

设定 PoE 电源的全局最大输出功率，以保证电源供电安全，也可用于有效控制。

表16-3全局设定最大输出功率

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch (config)# power inline max 100	全局设定最大输出功率为100W	最大功率值全局可设置范围为37~180W，单位为W，粒度为1W；缺省情况下，全局最大输出功率为180W

配合全局最大输出功率，有效控制各个端口的输出功率。

表16-4端口设定最大输出功率

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch (config)# interface eth-0-1	进入接口配置模式	-
Switch (config-if)# power inline port max 1000	设定端口最大输出功率为1000mW	端口可设置范围为 1~15400mW。单位：mW；缺省情况下，端口最大输出功率为15400mW

16.2.3 开启非标准 PD 检测功能

开启该功能时，交换机可以兼容非IEEE标准的PD，并对其进行正常供电。

表16-5开启非标准PD检测功能

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch (config)# interface eth-0-1	进入接口配置模式	-

命令举例	操作	说明
Switch (config-if)# power inline legacy enable	开启非 IEEE 标准 PD 检测功能	缺省情况下，不对非 IEEE 标准 PD 供电

16.2.4 配置 PoE 功率管理模式

当开启功率优先级管理策略时，可对端口的优先级进行单独配置。端口优先级有三种：low、critical、high。

表16-6 配置PoE功率管理模式

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch (config)# power inline policy enable	开启功率优先级管理策略模式	缺省情况下，功率优先级管理策略模式处于开启状态
Switch (config)# interface eth-0-1	进入接口配置模式	-
Switch (config-if)# power inline priority high	设置端口供电优先级为 high	缺省情况下，端口优先级为 low。开启功率优先级管理策略模式后该命令生效，当剩余功率不足以对新接入的 PD 供电时，对优先级高的端口优先供电

16.2.5 配置允许上电瞬间高冲击电流

不规范的 PD 上电瞬间会产生高冲击电流，导致设备启动自我保护，而将 PD 断电。在这种情况下，若一定要给此 PD 供电，需要允许上电瞬间的高冲击电流。关闭设备的自我保护功能，允许上电瞬间的高冲击电流，可能会对设备器件造成损害。

表16-7 开启/关闭允许上电瞬间高冲击电流

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch (config)# interface eth-0-1	进入接口配置模式	-
Switch (config-if)# power inline high-inrush enable	使能允许上电瞬间高冲击电流	缺省情况下，使能允许上电瞬间高冲击电流
Switch (config-if)# no power	关闭允许上电瞬间高冲击电流	

命令举例	操作	说明
inline high-inrush enable		

16.3 PoE 显示与维护

表16-8 PoE显示与维护

命令	操作	说明
show power inline [*port-number*]	显示全局或端口 PoE 设置与状态	port-number：物理接口号，取值范围为<0-0>-<1-28>
show environment	显示供电模块温度	-

可靠性配置指导目录

1 BHM 配置

1.1 BHM 简介

Beat heart Monitor（BHM）是用于监控其他协议进程的一个模块，当某个受监控进程长时间（30秒）无响应时，BHM模块会采取措施恢复系统，或者提示用户恢复系统。

BHM监控的协议模块有：RIP，RIPNG，OSPF，OSPF6，BGP，LDP，RSVP，PIM，PIM6，802.1X，LACP，MSTP，DHCP-RELAY，DHCP-RELAY6，RMON，OAM，ONM，SSH，SNMP，PTP，SSM，以及一些系统进程：NSM，MI，CHSM，HSRVD。

1.2 配置 BHM

1.2.1 配置系统监控功能

表1-1 使能/去使能系统监控功能

命令	操作	说明
sysmon enable	使能系统监控功能	缺省情况下，使能系统监控功能
no sysmon enable	去使能系统监控功能	

1.2.2 配置 BHM 模块功能

表1-2 使能/去使能BHM模块功能

命令	操作	说明
heart-beat-monitor enable	使能 BHM 模块功能	缺省情况下，使能 BHM 模块功能
no heart-beat-monitor enable	去使能 BHM 模块功能	

1.2.3 配置监控措施

当系统在程序无响应时，有三种可以采取的措施：reload system（重启系统）、shutdown port（关闭所有的端口）、warning（在终端打印警告信息）。

表1-3 配置监控措施

命令	操作	说明
heart-beat-monitor reactivate { **reload system | shutdown port | warning** }	配置当某个程序无响应时系统采取的措施	缺省情况下，使能 BHM 的重启系统

1.2.4 配置举例

表1-4 配置举例

命令举例	操作
Switch# configure terminal	进入全局配置模式
Switch(config)# sysmon enable	使能系统监控功能
Switch(config)# heart-beat-monitor enable	使能 BHM 模块功能
Switch(config)# heart-beat-monitor reactivate reload system	配置监控措施为“重启系统”

1.3 显示与维护

表1-5 显示与维护

命令	操作	说明
show sysmon	查看系统监控功能的状态	-
show heart-beat-monitor	查看程序监控状态	-

查看系统监控功能的状态：

```
Switch# show sysmon
System monitor enable.
```

查看程序监控状态：

```
Switch# show heart-beat-monitor

heart-beat-monitor enable.
heart-beat-monitor reactivation: restart system.
```

2 CFM 配置

2.1 CFM 简介

Connectivity Fault Management（CFM）是操作管理维护（缩写：OAM）模块的一部分。CFM 能够根据 802.1ag 协议去检测、验证、定位和通知以太网中的连接故障，也能够发现和验证以太网中的路径。CFM 对用户数据报文是透明的并且能最大限度地发现连接错误。

CFM 使用标准的以太网报文，仅以太网协议类型不同。支持的 CFM 消息如下：

- 连续性检查（CC）消息

  连续性检查消息周期性发送，使维护域端点 MEP 和维护域中间节点 MIP 可以发现其它 MEP。它用于检测任何一对 MEP 间的连续性丢失（LOC）。

- 以太网环回（LB）消息

  MEP 发送一个 LB 消息来验证另一个 MEP 或 MIP 是否可达。LB 消息和 ICMP ping 消息类似。

- 以太网链路追踪（LT）消息

  MEP 发送 LT 消息以追踪到一个目的 MEP/MIP 中间每一跳的 MIP。LT 消息类似 UDP 链路追踪消息。

- 以太网帧延时测量（DM）消息

  ETH-DM 可用于按需的 OAM，测量帧时延和帧时延变化。帧时延和帧时延变化的测量是通过向对等 MEP 周期性地发送带有 ETH-DM 信息的帧，并在诊断间隔内从对等 MEP 接收带有 ETH-DM 信息的帧来完成的。每一个 MEP 都可以进行帧时延和帧时延变化的测量。

  当一个 MEP 能产生带有 ETH-DM 信息的帧时，它向同一 ME 内对等的 MEP 周期地发送带有 ETH-DM 信息的帧。当一个 MEP 产生带有 ETH-DM 信息的帧时，它也预期在同一 ME 中从对等的 MEP 接收带有 ETH-DM 信息的帧。

- 以太网锁定信号（LCK）消息

以太网锁定信号功能（ETH-LCK）用于通告服务器层（子层）MEP 的管理性锁定以及随后的数据业务流中断，该业务流送往期待接收业务流的 MEP。它使得接收带有 ETH-LCK 信息的帧的 MEP 能区分是故障情况，还是服务器层（子层）MEP 的管理性锁定动作。

- 以太网客户端信号失败功能（CSF）

  以太网客户端信号失败功能是由服务器 MEP 将客户端检查到的失败或错误通知到对应服务器 MEP，再由对端服务器 MEP 通知对端的客户端 MEP。通常应用于客户端 MEP 无法直接通知到对端 MEP 的情况，此时 CC 或 AIS 是均无法使用的。CSF 消息是由服务器 MEP 发给对端服务器的 MEP 的消息。CSF 仅应用于点对点的以太网传输中。

- 以太网帧丢失测量（LM）消息

  ETH-LM 用于收集计数器的数值，应用于入口和出口处的服务帧，此时计数器在一对 MEP 之间保持着发送和接收的数据帧的计数。

  ETH-LM 是通过向其对等 MEP 发送带有 ETH-LM 信息的帧，并从对等 MEP 接收带有 ETH-LM 信息的帧实现的。

2.2 参考

CFM 参考以下标准文档：

IEEE 802.1ag/D8.1

2.3 配置 CFM 的基本功能

2.3.1 全局启用/关闭 CFM 功能

表2-1 全局启用/关闭CFM功能

命令	操作	说明
ethernet cfm enable	全局启用 CFM 功能	缺省情况下，CFM 功能处于关闭状态
no ethernet cfm enable	关闭 CFM 功能	

2.3.2 创建/删除维护域

下表的命令可以创建一个维护域（MD），每个维护域对应一个等级，不同等级提供不同的功能。

表2-2 创建/删除维护域

命令	操作	说明
ethernet cfm domain *domain-name* **level** *level-value*	创建一个维护域并进入 CFM 配置模式	维护域取值范围为 0~7，定义如下： 0~2（运营商等级） 3~4（提供商等级） 5~7（客户等级）
no ethernet cfm domain *domain-name*	删除维护域	

2.3.3 创建/删除维护联盟

下表的命令可以创建或删除一个维护联盟（MA）。

表2-3 创建/删除维护联盟

命令	操作	说明
service *csi-id* **vlan** *vlan-id*	创建一个维护联盟	CSI_ID：服务名；VLAN 标识的取值范围为 1~4094。该命令在 CFM 配置模式下执行
no service *csi-id*	删除维护联盟	

2.3.4 创建/删除维护端点 MEP

在同一个服务内，每一个 MEP 和远端 MEP 必须有一个唯一的标识。如果在同一台交换机上配置相同标识的 MEP，设备会提示重复，不允许配置。

表2-4 创建/删除维护端点MEP

命令	操作	说明
ethernet cfm mep { **down** | **up** } **mpid** *mep-id* **domain** *domain-name* **vlan** *vlan-id* **interval** { **1** | **2** | **3** | **4** | **5** | **6** | **7** }	创建一个维护联盟	MEP 标识的取值范围为 1~8191；VLAN 标识的取值范围为 1~4094
no ethernet cfm mep { **down** | **up** } **mpid** *mep-id* **domain** *domain-name* **vlan** *vlan-id* **interval** { **1** | **2** | **3** | **4** | **5** | **6** | **7** }	删除维护联盟	

说明

上方表格内的数字 1~7 分别表示 CCM 发送周期为 3.3 毫秒、10 毫秒、100 毫秒、1 秒、10 秒、1 分钟、10 分钟

2.3.5 创建/删除远端 MEP

表2-5 创建/删除远端MEP

命令	操作	说明
ethernet cfm mep crosscheck mpid *mep-id* **domain** *domain-name* **vlan** *vlan-id* **mac** *mac-address*	创建远端 MEP	MEP 标识的取值范围为 1~8191；VLAN 标识的取值范围为 1~4094
no ethernet cfm mep crosscheck mpid *mep-id* **domain** *domain-name* **vlan** *vlan-id*	删除远端 MEP	

2.3.6 创建/删除 MIP

表2-6 创建/删除MIP

命令	操作	说明
ethernet cfm mip level *level-value* **vlan** *vlan-id*	创建 MIP	维护域等级的取值范围为 1~7；VLAN 标识的取值范围为 1~4094
no ethernet cfm mip level *level-value* **vlan** *vlan-id*	删除 MIP	

2.3.7 配置连续性检查功能

表2-7 配置连续性检查功能

命令	操作	说明
ethernet cfm cc enable domain *domain-name* **vlan** *vlan-id*	启动维护域内某个服务的连续性检查功能	VLAN 标识的取值范围为 1~4094

命令	操作	说明
no ethernet cfm cc enable domain *domain-name* **vlan** *vlan-id*	关闭连续性检查功能	

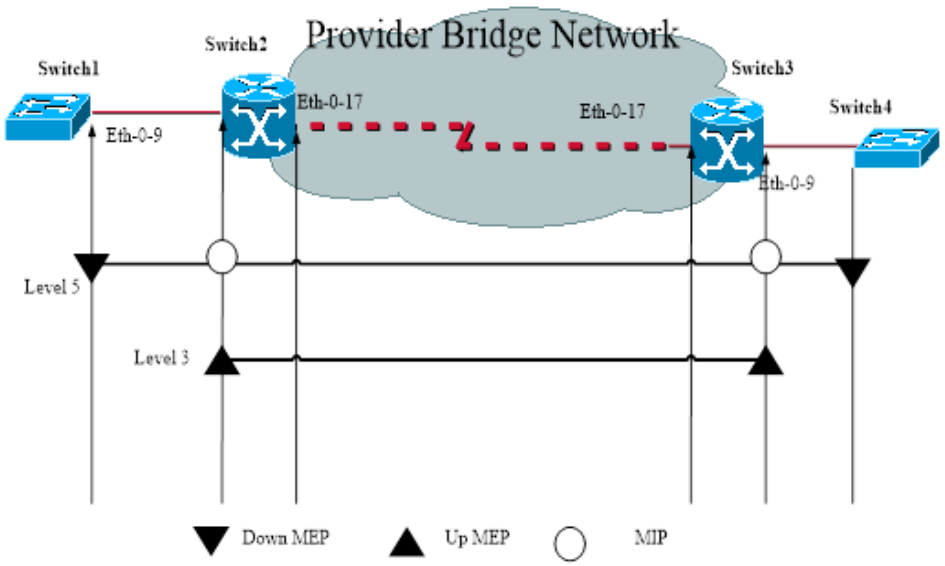
2.4 配置 CC/LB/LT/AIS/DM

2.4.1 介绍

以太网 Service OAM 主要从故障管理（CC/LB/LT/LCK/AIS）和性能监测（LM/DM）两个方面，实现端到端的以太网虚连接的管理与维护。

2.4.2 拓扑

图 2-1 CFM 示意图



2.4.3 配置步骤

下面分别对 Switch 1、Switch 2、Switch 3、Switch 4 进行配置。

Switch 1：

命令举例	操作步骤
Switch1# configure terminal	进入全局配置模式
Switch1(config)# vlan database	进入 VLAN 配置模式
Switch1(config vlan)# vlan 30	创建 VLAN 30
Switch1(config vlan)# exit	退出 VLAN 配置模式
Switch1(config)# ethernet cfm enable	全局使能 CFM
Switch1(config)# ethernet cfm mode y1731	配置 CFM 模式
Switch1(config)# ethernet cfm domain cust level 5	创建维护域 cust
Switch1(config-ether-cfm)# service cst vlan 30	创建服务 cst
Switch1(config-ether-cfm)# exit	退出 CFM 配置模式
Switch1(config)# interface eth-0-9	进入接口配置模式
Switch1(config-if)# switchport mode trunk	配置端口为 Trunk 口
Switch1(config-if)# switchport trunk allowed vlan add 30	配置端口允许 VLAN 30 通过
Switch1(config-if)# ethernet cfm mep down mpid 66 domain cust vlan 30 interval 1	创建维护域端点
Switch1(config-if)# ethernet cfm mep crosscheck mpid 99 domain cust vlan 30 mac d036.4567.8009	创建维护域远端节点，MAC 为远端 MEP 的 MAC
Switch1(config-if)# no shutdown	配置端口为 UP 状态
Switch1(config-if)# exit	退出接口配置模式
Switch1(config)# ethernet cfm cc enable domain cust vlan 30	启用维护域 cust 的服务 cst 的连续性检查功能
Switch1(config)# ethernet cfm ais suppress alarm enable domain cust vlan 30	配置当收到告警指示信号 AIS 报文且存在 loc 错误时抑制其它 loc error
Switch1(config)# end	退出全局配置模式

Switch 2：

命令举例	操作步骤
Switch2# configure terminal	进入全局配置模式
Switch2(config)# vlan database	进入 VLAN 配置模式
Switch2(config-vlan)# vlan 30	创建 VLAN 30
Switch2(config-vlan)# exit	退出 VLAN 配置模式
Switch2(config)# ethernet cfm enable	全局使能 CFM
Switch2(config)# ethernet cfm mode y1731	配置 CFM 模式
Switch2(config)# ethernet cfm domain cust level 5	创建维护域 cust
Switch2(config-ether-cfm)# service cst vlan 30	创建服务 cst
Switch2(config-ether-cfm)# exit	退出 CFM 配置模式
Switch2(config)# ethernet cfm domain provid level 3	创建维护域 provid
Switch2(config-ether-cfm)# service cst vlan 30	创建服务 cst
Switch2(config-ether-cfm)# exit	退出 CFM 配置模式
Switch2(config)# interface eth-0-9	进入接口模式
Switch2(config-if)# switchport mode trunk	配置端口为 Trunk 口
Switch2(config-if)# switchport trunk allowed vlan add 30	配置端口允许 VLAN 30 通过
Switch2(config-if)# ethernet cfm mip level 5 vlan 30	创建维护域中间节点
Switch2(config-if)# ethernet cfm mep up mpid 666 domain provid vlan 30 interval 1	创建维护域端点
Switch2(config-if)# ethernet cfm mep crosscheck mpid 999 domain provid vlan 30 mac 6a08.051e.bd09	创建维护域远端节点，MAC 为远端 mep 的 MAC
Switch2(config-if)# ethernet cfm ais status enable all domain provid vlan 30 level 5 multicast	使能 AIS
Switch2(config-if)# ethernet cfm server-ais status enable level 5 interval 1	配置 AIS 服务器
Switch2(config-if)# no shutdown	配置端口为 UP 状态

命令举例	操作步骤
Switch2(config-if)# exit	退出接口配置模式
Switch2(config)# interface eth-0-17	进入接口配置模式
Switch2(config-if)# switchport mode trunk	配置端口为 Trunk 口
Switch2(config-if)# switchport trunk allowed vlan add 30	配置端口允许 VLAN 30 通过
Switch2(config-if)# no shutdown	配置端口为 UP 状态
Switch2(config-if)# exit	退出接口配置模式
Switch2(config)# ethernet cfm cc enable domain provid vlan 30	启用维护域 provid 的服务 cst 的连续性检查功能
Switch2(config)# end	退出全局配置模式

Switch 3：

命令举例	操作步骤
Switch3# configure terminal	进入全局配置模式
Switch3(config)# vlan database	进入 VLAN 配置模式
Switch3(config-vlan)# vlan 30	创建 VLAN 30
Switch3(config-vlan)# exit	退出 VLAN 配置模式
Switch3(config)# ethernet cfm enable	全局使能 CFM
Switch3(config)# ethernet cfm mode y1731	配置 CFM 模式
Switch3(config)# ethernet cfm domain cust level 5	创建维护域 cust
Switch3(config-ether-cfm)# service cst vlan 30	创建服务 cst
Switch3(config-ether-cfm)# exit	退出 CFM 配置模式
Switch3(config)# ethernet cfm domain provid level 3	创建维护域 provid
Switch3(config-ether-cfm)# service cst vlan 30	创建服务 cst
Switch3(config-ether-cfm)# exit	退出 CFM 配置模式
Switch3(config)# interface eth-0-9	进入接口配置模式
Switch3(config-if)# switchport mode trunk	配置端口为 Trunk 口

命令举例	操作步骤
Switch3(config-if)# switchport trunk allowed vlan add 30	配置端口允许 VLAN 30 通过
Switch3(config-if)# ethernet cfm mip level 5 vlan 30	创建维护域中间节点
Switch3(config-if)# ethernet cfm mep up mpid 999 domain provid vlan 30 interval 1	创建维护域端点
Switch3(config-if)# ethernet cfm mep crosscheck mpid 666 domain provid vlan 30 mac 0e1d.a7d7.fb09	创建维护域远端节点，MAC 为远端 mep 的 MAC
Switch3(config-if)# no shutdown	配置端口为 UP 状态
Switch3(config-if)# exit	退出接口配置模式
Switch3(config)# interface eth-0-17	进入接口配置模式
Switch3(config-if)# switchport mode trunk	配置端口为 Trunk 口
Switch3(config-if)# switchport trunk allowed vlan add 30	配置端口允许 vlan 30 通过
Switch3(config-if)# no shutdown	配置端口为 UP 状态
Switch3(config-if)# exit	退出接口配置模式
Switch3(config)# ethernet cfm cc enable domain provid vlan 30	启用维护域 provid 的服务 cst 的连续性检查功能
Switch3(config)# end	退出全局配置模式

Switch 4：

命令举例	操作步骤
Switch4# configure terminal	进入全局配置模式
Switch4(config)# vlan database	进入 VLAN 配置模式
Switch4(config vlan)# vlan 30	创建 VLAN 30
Switch4(config vlan)# exit	退出 VLAN 配置模式
Switch4(config)# ethernet cfm enable	全局使能 CFM
Switch4(config)# ethernet cfm mode y1731	配置 CFM 模式
Switch4(config)# ethernet cfm domain cust level 5	创建维护域 cust

命令举例	操作步骤
Switch4(config-ether-cfm)# service cst vlan 30	创建服务 cst
Switch4(config-ether-cfm)# exit	退出 CFM 配置模式
Switch4(config)# interface eth-0-9	进入接口配置模式
Switch4(config-if)# switchport mode trunk	配置端口为 Trunk 口
Switch4(config-if)# switchport trunk allowed vlan add 30	配置端口允许 VLAN 30 通过
Switch4(config-if)# ethernet cfm mep down mpid 99 domain cust vlan 30 interval 1	创建维护域端点
Switch4(config-if)# ethernet cfm mep crosscheck mpid 66 domain cust vlan 30 mac fa02.cdff.6a09	创建维护域远端节点，MAC 为远端 mep 的 MAC
Switch4(config-if)# no shutdown	配置端口为 UP 状态
Switch4(config-if)# exit	退出接口配置模式
Switch4(config)# ethernet cfm cc enable domain cust vlan 30	启用维护域 cust 的服务 cst 的连续性检查功能
Switch4(config)# end	退出全局配置模式

2.4.4 检查配置结果

命令	操作
show ethernet cfm maintenance-points	显示相关的 MEP、远端 MEP 和 MIP 的信息
show ethernet cfm maintenance-points local { **mep** | **mip** } { **interface** *if-name* | **domain** *domain-name* | **level** *level-value* }	显示本地 MEP 和 MIP 的相关信息
show ethernet cfm errors [**domain** *domain-name* | **level** *level-value*]	显示 CFM 的错误信息
show ethernet cfm ais mep *mep-id* **domain** *domain-name* **vlan** *vlan-id*	显示 MEP 的 AIS 相关信息

i. 检查MEP和MIP

查看 Switch1 和 Switch2 上 MEP 和 MIP 的相关信息：

```
Switch1# show ethernet cfm maintenance-points

######Local MEP:
MPID Direction DOMAIN LEVEL TYPE VLAN PORT        CC-Status Mac-address       RDI
Interval
--------------------------------------------------------------------------------
66    Down MEP    cust      5         MEP   30     eth-0-9   enabled     fa02.cdff.6a09 True
3.33ms
######Local MIP:
Level    VID   TYPE      PORT                MAC
------------------------------------------------
######Remote MEP:
MPID   LEVEL VLAN ACTIVE Remote Mac        RDI     FLAGS       STATE
------------------------------------------------------
99      5       30     Yes      d036.4567.8009 True    Learnt      UP

Switch2# show ethernet cfm maintenance-points

######Local MEP:
MPID Direction DOMAIN LEVEL TYPE VLAN PORT        CC-Status Mac-address       RDI
------------------------------------------------------------------------------
666   Up MEP       provid 3        MEP   30      eth-0-9   enabled     0e1d.a7d7.fb09 False
######Local MIP:
Level    VID   TYPE      PORT                MAC
------------------------------------------------
5          30      MIP       eth-0-9             0e1d.a7d7.fb09
######Remote MEP:
MPID   LEVEL VLAN ACTIVE Remote Mac         RDI     FLAGS       STATE
------------------------------------------------------
999    3         30      Yes      6a08.051e.bd09    True    Learnt      UP
```

ii. **检查以太网环回（LB）**

根据远端 MEP 的地址/组播地址回环远端 MEP：

```
Switch1# ethernet cfm loopback mac d036.4567.8009 unicast mepid 66 domain cust vlan 30
Sending 1 Ethernet CFM loopback messages, timeout is 5 seconds:
(! Pass . Fail)
!
 Loopback completed.
 ----------------------------------
Success rate is 100 percent(1/1)
```

根据组播地址回环远端 MEP：

```
Switch1# ethernet cfm loopback multicast mepid 66 domain cust vlan 30
Sending 1 Ethernet CFM loopback messages, timeout is 5 seconds:
(! Pass . Fail)
Host MEP: 66
Number of RMEPs that replied to mcast frame = 1
LBR received from the following
   9667.bb68.f308
  success rate is    100 (1/1)
```

根据远端 MEP 的标识回环远端 MEP：

```
Switch1# ethernet cfm loopback unicast rmepid 99 mepid 66 domain cust vlan 30
Sending 1 Ethernet CFM loopback messages, timeout is 5 seconds:
(! Pass . Fail)
!
  Loopback completed.
  ----------------------------------
  Success rate is 100 percent(1/1)
```

根据远端 MIP 的地址回环远端 MIP：

```
Switch1# ethernet cfm loopback mac 0e1d.a7d7.fb09 unicast mepid 66 domain cust vlan 30
Sending 1 Ethernet CFM loopback messages, timeout is 5 seconds:
(! Pass . Fail)
!
  Loopback completed.
  ----------------------------------
  Success rate is 100 percent(1/1)
```

iii. **检查远端故障指示（ADI）**

显示 RDI 的信息：

```
Switch1# show ethernet cfm maintenance-points local mep domain cust
MPID Direction DOMAIN LEVEL TYPE VLAN PORT       CC-Status Mac-address       RDI
Interval
--------------------------------------------------------------------------------
66     Down MEP    cust     5    MEP    30     eth-0-9    enabled     fa02.cdff.6a09 True 3.33ms
```

iv. **检查错误信息**

在清除本地 MEP 错误前，错误信息显示如下所示：

```
Switch1# show ethernet cfm errors domain cust
Level Vlan MPID RemoteMac          Reason                                    ServiceId
5     30   66   d036.4567.8009 errorCCMdefect: rmep not found          cst
5     30   66   d036.4567.8009 errorCCMdefect: rmep not found clear cst
Time
2011/05/27 3:19:18
2011/05/27 3:19:32
```

以下命令用于清除错误信息。当清除本地 MEP 的错误信息后，错误信息如下所示：

```
Switch1# clear ethernet cfm errors domain cust
Level Vlan MPID RemoteMac          Reason                                    ServiceId
```

v. 检查AIS

以下命令关闭 Switch 1 和 Switch 3 上的连续性检查功能。检查 Switch 2、Switch 1 上的 AIS 的状态：

```
Switch1(config)# no ethernet cfm cc enable domain cust vlan 30
Switch3(config)# no ethernet cfm cc enable domain cust vlan 30
Switch2# show ethernet cfm ais mep 666 domain cust vlan 30
AIS-Status: Enabled
AIS Period: 1
Level to transmit AIS: 7
AIS Condition: No
-------------------------------------------------
   Configured defect condition        detected(yes/no)
-------------------------------------------------
   unexpected-period                  no
   unexpected-MEG level               no
   unexpected-MEP                        no
   Mismerge                              no
   LOC                                yes

Switch1# show ethernet cfm ais mep 66 domain cust vlan 30
AIS-Status: Disabled
AIS Condition: Yes
```

vi. 检查LinkTrace（LT）

根据远端 MEP 的地址追踪远端 MEP：

```
Switch1# ethernet cfm linktrace mac d036.4567.8009 mepid 66 domain cust vlan 30
Sending Ethernet CFM linktrace messages,TTL is 64.Per-Hop Timeout is 5 seconds:
Please wait a moment
------------------------------
Received Hops: 1
------------------------------
TTL                         : 63
Fowarded                        : True
Terminal MEP                : False
Relay Action                : Rly FDB
Ingress Action              : IngOk
Ingress MAC address         : 0e1d.a7d7.fb09
Ingress Port ID Type        : ifName
Ingress Port ID             : eth-0-9
------------------------------
Received Hops: 2
------------------------------
TTL                         : 62
Fowarded                    : True
Terminal MEP                : False
Relay Action                : Rly FDB
Egress Action               : EgrOk
Egress MAC address          : 6a08.051e.bd09
Egress Port ID Type         : ifName
Egress Port ID              : eth-0-9
------------------------------
Received Hops: 3
------------------------------
TTL                         : 61
Fowarded                    : False
Terminal MEP                : True
Relay Action                : Rly Hit
Ingress Action              : IngOk
Ingress MAC address         : d036.4567.8009
Ingress Port ID Type        : ifName
Ingress Port ID             : eth-0-9
```

根据远端 MEP 的标识追踪远端 MEP：

```
Switch1# ethernet cfm linktrace rmepid 99 mepid 66 domain cust vlan 30
Sending Ethernet CFM linktrace messages,TTL is 64.Per-Hop Timeout is 5 seconds:
Please wait a moment
------------------------------
Received Hops: 1
------------------------------
TTL                         : 63
```

```
Fowarded                        : True
Terminal MEP                    : False
Relay Action                    : Rly FDB
Ingress Action                  : IngOk
Ingress MAC address             : 0e1d.a7d7.fb09
Ingress Port ID Type            : ifName
Ingress Port ID                 : eth-0-9
------------------------------
Received Hops: 2
------------------------------
TTL                             : 62
Fowarded                        : True
Terminal MEP                    : False
Relay Action                    : Rly FDB
Egress Action                   : EgrOk
Egress MAC address              : 6a08.051e.bd09
Egress Port ID Type             : ifName
Egress Port ID                  : eth-0-9
------------------------------
Received Hops: 3
------------------------------
TTL                             : 61
Fowarded                        : False
Terminal MEP                    : True
Relay Action                    : Rly Hit
Ingress Action                  : IngOk
Ingress MAC address             : d036.4567.8009
Ingress Port ID Type            : ifName
Ingress Port ID                 : eth-0-9
```

根据远端 MIP 的地址追踪远端 MIP：

```
Switch1# ethernet cfm linktrace 6a08.051e.bd09 mepid 66 domain cust vlan 30
Sending Ethernet CFM linktrace messages,TTL is 64.Per-Hop Timeout is 5 seconds:
Please wait a moment
------------------------------
Received Hops: 1
------------------------------
TTL                             : 63
Fowarded                        : True
Terminal MEP                    : False
Relay Action                    : Rly FDB
Ingress Action                  : IngOk
Ingress MAC address             : 0e1d.a7d7.fb09
Ingress Port ID Type            : ifName
Ingress Port ID                 : eth-0-9
------------------------------
```

```
Received Hops: 2
-----------------------------
TTL                          : 62
Fowarded                     : False
Terminal MEP                 : False
Relay Action                 : Rly Hit
Egress Action                : EgrOk
Egress MAC address           : 6a08.051e.bd09
Egress Port ID Type          : ifName
Egress Port ID               : eth-0-9
```

vii. **检查帧时延测量（DM）**

测量双向的延时和延时变化：

```
Switch1# ethernet cfm dmm    rmepid 99 mepid 66 count 5 domain cust vlan 30
    Delay measurement statistics:
     DMM Packets transmitted          : 5
     Valid DMR packets received       : 5
     Index        Two-way delay       Two-way delay variation
          1            4288 usec                    0 usec
          2            4312 usec                   24 usec
          3            4296 usec                   16 usec
          4            4320 usec                   24 usec
          5            4264 usec                   56 usec
     Average delay                    : 4296 usec
     Average delay variation          : 24 usec
     Best case delay                  : 4264 usec
     Worst case delay                 : 4320 usec
```

在启用单向时延测量前，时钟应该同步。以下命令显示了在 Switch 1 上启用了单向时延测量：

```
Switch1#ethernet cfm 1dm rmepid 99 mepid 66 count 5 domain cust vlan 30
```

在 Switch 4 上显示了单向时延测量的结果：

```
Switch4# show ethernet cfm delaymeasurement cache
    Remote MEP          : 66
     Remote MEP vlan    : 30
     Remote MEP level : 5
     DMM Packets transmitted          : 0
     Valid DMR packets received       : 0
     Valid 1DM packets received       : 5
     Index     One-way delay     One-way delay variation     Received Time
```

```
1        16832 usec              0 usec     2011/07/19 17:27:46
2        16176 usec            656 usec     2011/07/19 17:27:47
3        15448 usec            728 usec     2011/07/19 17:27:48
4        14800 usec            648 usec     2011/07/19 17:27:49
5        15406 usec            606 usec     2011/07/19 17:27:50
Average delay                  : 15732 usec
Average delay variation        : 527 usec
Best case delay                : 14800 usec
Worst case delay               : 16832 usec
```

2.5 配置 LCK

配置 LCK 命令可以锁定 MEP，使数据报文无法通过。可参考 2.4.2 图 2-1 拓扑。以下示例在 Switch 2 上配置锁定。

2.5.1 配置方法

表2-8 配置方法

命令举例	操作
Switch2# configure terminal	进入全局配置模式
Switch2(config)# interface eth-0-9	进入接口配置模式
Switch2(config-if)# ethernet cfm lck enable mep 666 domain provid vlan 30 tx-level 5 interval 1	配置锁定 MEP 666，并指定向等级 5 上按周期 1 秒发锁定报文
Switch2(config-if)# end	退出接口配置模式

2.5.2 显示与维护

表2-9 显示与维护

命令	操作
show ethernet cfm lck	显示 LCK 的信息

显示 Switch 2 上 LCK 状态：

```
Switch2# show ethernet cfm lck

En-LCK Enable, Y(Yes)/N(No)
Rx-LC, Receive LCK packets and enter LCK condition, Y(Yes)/N(No)
Rx-I, The period which is gotten from LCK packets
```

```
Tx-Domain, frames with ETH-LCK information are sent to this Domain
Tx-I, Transmit Interval
--------------------------------------------------------------------------
MPID Domain          VLAN En Rx-LC Rx-I Tx-Domain      Tx-I
--------------------------------------------------------------------------
666  provid          30   Y  N     N/A  cust           1
```

显示 Switch 1 上 LCK 状态：

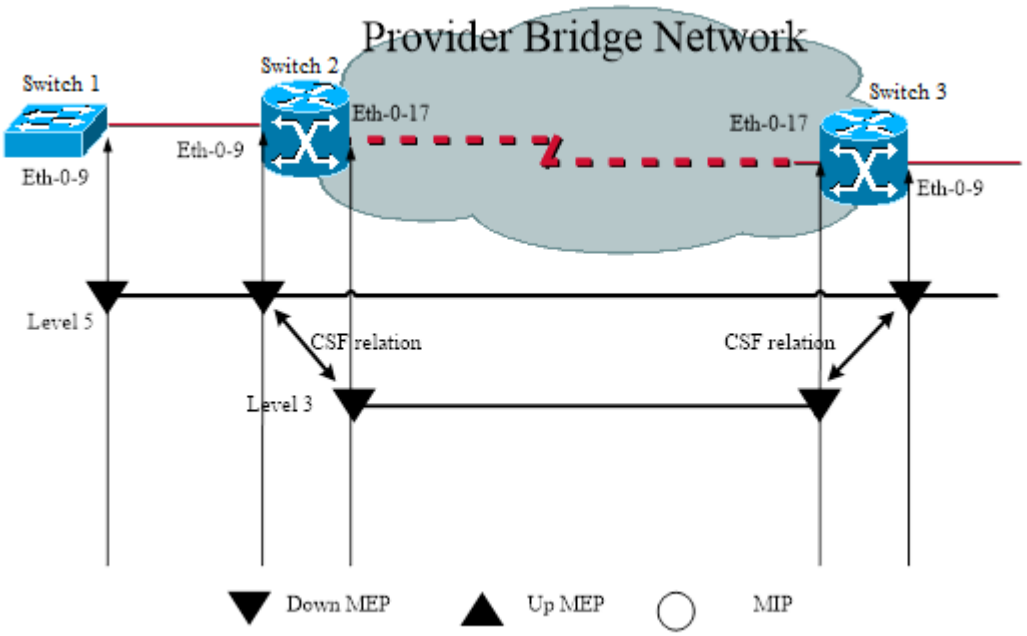
```
Switch1# show ethernet cfm lck

En-LCK Enable, Y(Yes)/N(No)
Rx-LC, Receive LCK packets and enter LCK condition, Y(Yes)/N(No)
Rx-I, The period which is gotten from LCK packets
Tx-Domain, frames with ETH-LCK information are sent to this Domain
Tx-I, Transmit Interval
--------------------------------------------------------------------------
MPID Domain          VLAN En Rx-LC Rx-I Tx-Domain      Tx-I
--------------------------------------------------------------------------
66   cust            30   N  Y     1    N/A            N/A
```

2.6 配置 CSF

在客户 MEP 和服务器 MEP 之间，配置客户信号失败（CSF）关系。

2.6.1 拓扑

图 2-2 CSF 示意图



2.6.2 配置方法

分别对 Switch 1、Switch 2、Switch 3 进行如下配置。

Switch 1：

命令举例	操作
Switch1# configure terminal	进入全局配置模式
Switch1(config)# vlan database	进入 VLAN 配置模式
Switch1(config vlan)# vlan 30	创建 VLAN 30
Switch1(config vlan)# exit	退出 VLAN 配置模式
Switch1(config)# ethernet cfm enable	全局使能 CFM
Switch1(config)# ethernet cfm mode y1731	配置 CFM 模式
Switch1(config)# ethernet cfm domain cust level 5	创建维护域 cust
Switch1(config-ether-cfm)# service cst vlan 30	创建服务 cst
Switch1(config-ether-cfm)# exit	退出 CFM 配置模式
Switch1(config)# interface eth-0-9	进入接口配置模式

命令举例	操作
Switch1(config-if)# switchport mode trunk	配置端口为 Trunk 口
Switch1(config-if)# switchport trunk allowed vlan add 30	配置端口允许 VLAN 30 通过
Switch1(config-if)# ethernet cfm mep down mpid 66 domain cust vlan 30 interval 1	创建维护域端点
Switch1(config-if)# ethernet cfm mep crosscheck mpid 99 domain cust vlan 30 mac d036.4567.8009	创建维护域远端节点，MAC 为远端 mep 的 MAC
Switch1(config-if)# no shutdown	配置端口为 UP 状态
Switch1(config-if)# exit	退出接口配置模式
Switch1(config)# ethernet cfm cc enable domain cust vlan 30	启用维护域 cust 的服务 cst 的连续性检查功能
Switch1(config)# end	退出全局配置模式

Switch 2：

命令举例	操作
Switch2# configure terminal	进入全局配置模式
Switch2(config)# vlan database	进入 VLAN 配置模式
Switch2(config vlan)# vlan 20,30	创建 VLAN 20,30
Switch2(config vlan)# exit	退出 VLAN 配置模式
Switch2(config)# ethernet cfm enable	全局使能 CFM
Switch2(config)# ethernet cfm mode y1731	配置 CFM 模式
Switch2(config)# ethernet cfm domain cust level 5	创建维护域 cust
Switch2(config-ether-cfm)# service cst vlan 30	创建服务 cst
Switch2(config)# ethernet cfm domain provid level 3	创建维护域 provid
Switch2(config-ether-cfm)# service cst vlan 20	创建服务 cst
Switch2(config-ether-cfm)# exit	退出 CFM 配置模式
Switch2(config)# interface eth-0-9	进入接口配置模式
Switch2(config-if)# switchport mode trunk	配置端口为 Trunk 口

命令举例	操作
Switch2(config-if)# switchport trunk allowed vlan add 30	配置端口允许 VLAN 30 通过
Switch2(config-if)# ethernet cfm mep down mpid 99 domain cust vlan 30 interval 1	创建维护域端点
Switch2(config-if)# ethernet cfm mep crosscheck mpid 66 domain cust vlan 30 mac fa02.cdff.6a09	创建维护域远端节点，MAC 为远端 MEP 的 MAC
Switch2(config-if)# no shutdown	配置端口为 UP 状态
Switch2(config-if)# exit	退出接口配置模式
Switch2 (config)#interface eth-0-17	进入接口配置模式
Switch2 (config-if)# switchport mode trunk	配置端口为 Trunk 口
Switch2 (config-if)# switchport trunk allowed vlan add 20	配置端口允许 VLAN 20 通过
Switch2 (config-if)# ethernet cfm mep down mpid 666 domain provid vlan 20 interval 1	创建维护域端点
Switch2 (config-if)# no shutdown	配置端口为 UP 状态
Switch2(config)# ethernet cfm cc enable domain cust vlan 30	启用维护域 cust 的服务 cst 的连续性检查功能
DUT (config)# ethernet cfm csf client domain cust vlan 30 mepid 99 server domain provid vlan 20 mepid 666 interval 1	配置 CSF 连接关系
Switch2(config)# end	退出全局配置模式

Switch 3：

命令举例	操作
Switch3# configure terminal	进入全局配置模式
Switch3(config)# vlan database	进入 VLAN 配置模式
Switch3(config vlan)# vlan 20,30	创建 VLAN 20,30
Switch3(config vlan)# exit	退出 VLAN 配置模式
Switch3(config)# ethernet cfm enable	全局使能 CFM
Switch3(config)# ethernet cfm mode y1731	配置 CFM 模式
Switch3(config)# ethernet cfm domain cust level 5	创建维护域 cust

命令举例	操作
Switch3(config-ether-cfm)# service cst vlan 30	创建服务 cst
Switch3(config)# ethernet cfm domain provid level 3	创建维护域 provid
Switch3(config-ether-cfm)# service cst vlan 20	创建服务 cst
Switch3(config-ether-cfm)# exit	退出 CFM 配置模式
Switch3(config)# interface eth-0-9	进入接口配置模式
Switch3(config-if)# switchport mode trunk	配置端口为 Trunk 口
Switch3(config-if)# switchport trunk allowed vlan add 30	配置端口允许 VLAN 30 通过
Switch3(config-if)# ethernet cfm mep down mpid 88 domain cust vlan 30 interval 1	创建维护域端点
Switch3(config-if)# no shutdown	配置端口为 UP 状态
Switch3(config-if)# exit	退出接口配置模式
Switch3(config)#interface eth-0-17	进入接口配置模式
Switch3(config-if)# switchport mode trunk	配置端口为 Trunk 口
Switch3(config-if)# switchport trunk allowed vlan add 20	配置端口允许 VLAN 20 通过
Switch3(config-if)# ethernet cfm mep down mpid 999 domain provid vlan 20 interval 1	创建维护域端点
Switch3(config-if)# no shutdown	配置端口为 UP 状态
Switch3(config)# ethernet cfm cc enable domain cust vlan 30	启用维护域 cust 的服务 cst 的连续性检查功能
Switch3(config)# ethernet cfm csf client domain cust vlan 30 mepid 88 server domain provid vlan 20 mepid 999 interval 1	配置 CSF 连接关系
Switch3(config)# end	退出全局配置模式

2.6.3 显示与维护

命令	操作
show ethernet cfm csf	显示 CSF 的关系和状态

关闭 Switch 1 上的连续性检查，使 Switch 2 上触发 loc 错误：

```
Switch1 (config)#no ethernet cfm cc enable domain cust vlan 30
```

Switch 2 上的 MEP 99 会上报 loc，引发 MEP 666 发送 CSF 报文(原因 los)：

以下命令用来显示 Switch 2 上 CSF 状态：

```
Switch2# show ethernet cfm csf
En-CSF Enable, Y(Yes)/N(No)
CTR-Client Trigger reason, L(los)/F(fdi)/R(rdi)/D(dci) or N/A
ECC-Enter CSF Condition, Y(Yes)/N(No)
SRR-Server Rx Reason, L(los)/F(fdi)/R(rdi)/D(dci) or N/A
Tx-I, Transmit Interval
Rx-I, The period which is gotten from CSF packets
---------------------------------------------------------------------
Client Mep                                Server Mep
MPID Cli-Domain     VLAN CTR     ECC MPID Srv-Domain     VLAN SRR     Tx-I Rx-I
---------------------------------------------------------------------
99     cust             30     L         N     666    provid          20     N/A     1       N/A
```

在 Switch 3 上，MEP 999 会收到 CSF 的报文并通知客户 MEP 88，然后客户 MEP 会进入 CSF 状态。

以下命令用来显示 Switch 3 上 CSF 状态：

```
Switch3# show ethernet cfm csf
En-CSF Enable, Y(Yes)/N(No)
CTR-Client Trigger reason, L(los)/F(fdi)/R(rdi)/D(dci) or N/A
ECC-Enter CSF Condition, Y(Yes)/N(No)
SRR-Server Rx Reason, L(los)/F(fdi)/R(rdi)/D(dci) or N/A
Tx-I, Transmit Interval
Rx-I, The period which is gotten from CSF packets
---------------------------------------------------------------------
Client Mep                                Server Mep
MPID Cli-Domain     VLAN CTR     ECC MPID Srv-Domain     VLAN SRR     Tx-I Rx-I
---------------------------------------------------------------------
88     cust             30     N/A       Y     999    provid          20     L       1       1
```

2.7 配置双端/单端 LM

本小节介绍了双端和单端两种方式的帧丢失测量。请参考图 2-1 拓扑。

2.7.1 配置双端 LM

在Switch 1和 Switch 4上使能双端LM功能。

Switch 1：

命令举例	操作
Switch1# configure terminal	进入全局配置模式
Switch1(config)# ethernet cfm lm enable dual-ended domain cust vlan 30 mepid 66 all-cos cache-size 10	配置双端 LM 功能
Switch1(config)# end	退出全局配置模式

Switch 4：

命令举例	操作
Switch4# configure terminal	进入全局配置模式
Switch4(config)# ethernet cfm lm enable dual-ended domain cust vlan 30 mepid 99 all-cos cache-size 10	配置双端 LM 功能
Switch4(config)# end	退出全局配置模式

2.7.2 配置单端 LM

在 Switch 1 和 Switch 4 上使能单端 LM 功能。

Switch 1：

命令举例	操作
Switch1# configure terminal	进入全局配置模式
Switch1(config)# ethernet cfm lm enable single-ended domain cust vlan 30 mepid 66 all-cos	配置单端 LM 功能
Switch1(config)# end	退出全局配置模式

Switch 4：

命令举例	操作
Switch4# configure terminal	进入全局配置模式
Switch4(config)# ethernet cfm lm enable single-ended domain cust vlan 30 mepid 99 all-cos	配置单端 LM 功能

命令举例	操作
Switch4(config)# end	退出全局配置模式

2.7.3 检测配置结果

命令	操作
show ethernet cfm lm domain *domain-name* **vlan** *vlan-id* **mepid** *mep-id*	显示双端帧丢失测量的结果

显示 Switch 1 上双端帧丢失测量的结果：

```
Switch1# show ethernet cfm lm domain cust vlan 30 mepid 66
DOMAIN        : cust
VLAN          : 30
MEPID         : 66
Start Time : 2013/07/16 1:36:56
End Time      : 2013/07/16 1:37:07
Notes         : 1. When the difference of Tx is less than the difference of Rx,
                    the node is invalid, loss and loss ratio should be "-";
                2. When loc is reported for mep, the loss should be "-" and loss
                    ratio should be 100%;
                3. When calculate average loss and loss ratio, invalid or loc nodes
                    will be excluded;
Latest dual-ended loss statistics:
--------------------------------------------------------------------------------
Index Cos Local-loss Local-loss ratio Remote-loss Remote-loss ratio Time
--------------------------------------------------------------------------------
1     all 0          000.0000%       0           000.0000% 01:36:57
2     all 0          000.0000%       0           000.0000% 01:36:58
3     all 0          000.0000%       0           000.0000% 01:36:59
4     all 0          000.0000%       0           000.0000% 01:37:00
5     all 0          000.0000%       0           000.0000% 01:37:01
6     all 0          000.0000%       0           000.0000% 01:37:02
7     all 0          000.0000%       0           000.0000% 01:37:03
8     all 0          000.0000%       0           000.0000% 01:37:04
9     all 0          000.0000%       0           000.0000% 01:37:05
10    all 0          000.0000%       0           000.0000% 01:37:07
--------------------------------------------------------------------------------
```

```
Maximum Local-loss    : 0              Maximum Local-loss Ratio    : 000.0000%
Minimum Local-loss    : 0              Minimum Local-loss Ratio    : 000.0000%
Average Local-loss    : 0              Average Local-loss Ratio    : 000.0000%
Maximum Remote-loss : 0                Maximum Remote-loss Ratio : 000.0000%
Minimum Remote-loss : 0                Minimum Remote-loss Ratio : 000.0000%
Average Remote-loss : 0                Average Remote-loss Ratio : 000.0000%
```

显示 Switch 4 上双端帧丢失测量的结果：

```
Switch4# show ethernet cfm lm domain cust vlan 30 mepid 99
DOMAIN        : cust
VLAN          : 30
MEPID         : 99
Start Time : 2013/07/16 1:37:11
End Time      : 2013/07/16 1:37:22
Notes         : 1. When the difference of Tx is less than the difference of Rx,
                   the node is invalid, loss and loss ratio should be "-";
                2. When loc is reported for mep, the loss should be "-" and loss
                   ratio should be 100%;
                3. When calculate average loss and loss ratio, invalid or loc nodes
                   will be excluded;
Latest dual-ended loss statistics:
--------------------------------------------------------------------------------
Index Cos Local-loss Local-loss ratio Remote-loss Remote-loss ratio Time
--------------------------------------------------------------------------------
1     all          0          000.0000%          0          000.0000% 01:37:12
2     all          0          000.0000%          0          000.0000% 01:37:13
3     all          0          000.0000%          0          000.0000% 01:37:14
4     all          0          000.0000%          0          000.0000% 01:37:16
5     all          0          000.0000%          0          000.0000% 01:37:17
6     all          0          000.0000%          0          000.0000% 01:37:18
7     all          0          000.0000%          0          000.0000% 01:37:19
8     all          0          000.0000%          0          000.0000% 01:37:20
9     all          0          000.0000%          0          000.0000% 01:37:21
10    all          0          000.0000%          0          000.0000% 01:37:22
--------------------------------------------------------------------------------
Maximum Local-loss    : 0              Maximum Local-loss Ratio    : 000.0000%
Minimum Local-loss    : 0              Minimum Local-loss Ratio    : 000.0000%
Average Local-loss    : 0              Average Local-loss Ratio    : 000.0000%
Maximum Remote-loss : 0                Maximum Remote-loss Ratio : 000.0000%
Minimum Remote-loss : 0                Minimum Remote-loss Ratio : 000.0000%
```

```
Average Remote-loss : 0              Average Remote-loss Ratio : 000.0000%
```

从 Switch 1 发送单端帧丢失测量消息，并显示 LM 的结果：

```
Switch1# ethernet cfm lm single-ended domain cust vlan 30 rmepid 99 mepid 66 count 10
DOMAIN        : cust
VLAN          : 30
MEPID         : 66
Start Time : 2013/07/16 1:39:38
End Time      : 2013/07/16 1:39:38
Notes         : 1. When the difference of Tx is less than the difference of Rx,
                   the node is invalid, loss and loss ratio should be "-";
                2. When loc is reported for mep, the loss should be "-" and loss
                   ratio should be 100%;
                3. When calculate average loss and loss ratio, invalid or loc nodes
                   will be excluded;
Latest single-ended loss statistics:
--------------------------------------------------------------------------------
Index Cos Local-loss Local-loss ratio Remote-loss Remote-loss ratio
--------------------------------------------------------------------------------
1     all          0          000.0000%          0          000.0000%
2     all          0          000.0000%          0          000.0000%
3     all          0          000.0000%          0          000.0000%
4     all          0          000.0000%          0          000.0000%
5     all          0          000.0000%          0          000.0000%
6     all          0          000.0000%          0          000.0000%
7     all          0          000.0000%          0          000.0000%
8     all          0          000.0000%          0          000.0000%
9     all          0          000.0000%          0          000.0000%
--------------------------------------------------------------------------------
Maximum Local-loss    : 0              Maximum Local-loss Ratio    : 000.0000%
Minimum Local-loss    : 0              Minimum Local-loss Ratio    : 000.0000%
Average Local-loss    : 0              Average Local-loss Ratio    : 000.0000%
Maximum Remote-loss : 0                Maximum Remote-loss Ratio : 000.0000%
Minimum Remote-loss : 0                Minimum Remote-loss Ratio : 000.0000%
Average Remote-loss : 0                Average Remote-loss Ratio : 000.0000%
```

2.8 配置 Test

该配置可以使能以太网测试信号（ETH-Test）发送功能。请参考图 2-1 拓扑。

2.8.1 配置方法

在Switch 1和 Switch 4上使能Test功能。

Switch 1：

命令举例	操作
Switch1# configure terminal	进入全局配置模式
Switch1(config)# ethernet cfm tst transmission enable domain cust vlan 30 mep 66 tx-mode continuous pattern-type random packet-size 64	配置 Test 发送功能
Switch1(config)# end	退出全局配置模式

Switch 4：

命令举例	操作
Switch4# configure terminal	进入全局配置模式
Switch4(config)# ethernet cfm tst reception enable domain cust vlan 30 mep 99	配置 Test 接收功能
Switch4(config)# end	退出配置模式

2.8.2 显示与维护

命令	操作
show ethernet cfm tst	显示 Test 的信息

从 Switch1 上发送 Test 消息，并显示 Test 的信息：

```
Switch1# ethernet cfm tst start rate 1000 time second 1
Switch1# show ethernet cfm tst
DOMAIN                : cust
VLAN                  : 30
MEPID                 : 66
Transmission          : Enabled
Reception             : Disabled
```

```
Status                : Non-Running
Start Time            : 06:32:48
Predict End Time : 06:33:18
Actual End Time    : 06:33:18
Packet Type          : TST
Rate                    : 1000 mbps
Packet Size          : 64 bytes
Tx Number             : 29
Tx Bytes              : 1856
Rx Number             : 0
Rx Bytes              : 0
```

在 Switch 4 上显示 Test 的信息：

```
Switch4# show ethernet cfm tst
DOMAIN                 : cust
VLAN                   : 30
MEPID                  : 99
Transmission        : Disabled
Reception             : Enabled
Status                : Non-Running
Start Time            : null
End Time               : null
Packet Type          : null
Rate                    : null
Packet Size          : null
Tx Number             : 0
Tx Bytes              : 0
Rx Number             : 29
Rx Bytes              : 1856
```

3 CPU Traffic 配置

3.1 CPU Traffic 简介

本章介绍了配置CPU流量限制及查看CPU流量的方法。

CPU流量限制是一种很有用的保护CPU的机制，通过对进入CPU的报文的流量进行限制实现。

CPU流量限制包含两个级别的CPU保护措施：

其一，限制各个进入 CPU 的 reason 的流量。在芯片中，是通过配置这个 reason 对应的 queue shaping 实现的。

其二，限制所有进入 CPU 的报文的流量。芯片中是通过配置 CPU 端口上的 shaping 实现的。

下表列出了各种 reason 和对应的描述：

表3-1 协议报文类型与描述

reason	描述
arp	ARP 协议报文
bpdu	BPDU 协议报文(包括 STP, RSTP, MSTP)
dhcp	DHCP 协议报文
eapol	Dot1x 协议报文
erps	ERPS 协议报文
fwd-to-cpu	转发到 CPU 的报文
icmp-redirect	ICMP 重定向
igmp	IGMP 或者 IGMP Snooping 报文
ip-option	带有可选字段的 IP 报文
ipda	IPDA 协议报文
ldp	LDP 协议报文
macsa-mismatch	与一个端口 security entry 不匹配时的学习报文

reason	描述
mcast-rpf-fail	组播报文 RPF 检查失败
mld	MLD 协议报文
mpls-ttl-fail	TTL 失效 MPLS 报文
ip-mtu-fail	需要分片的报文
ospf	OSPF 协议报文
pim	PIM 协议报文
port-security-discard	端口 security entry 学满时的学习报文
rip	RIP 协议报文
sflow-egress	在出口方向 sFlow 的采样报文
sflow-ingress	在入口方向 sFlow 的采样报文
slow-protocol	Slow 协议报文.(包括 EFM, LACP，SYNCE) TTL 失效的组播报文
smart-link	Smart Link 协议报文
ucast-ttl-fail	TTL 失效的单播 IP 报文
udld	UDLD 协议报文
vlan-security-discard	VLAN 内学习的 mac 达到限制是的学习报文
vrrp	VRRP 协议报文
bfd-learning	BFD 学习报文

说明

这里提到的 reason，意思是各种协议报文的类型，比如 bgp、ospf、rip 等分别是不同的 reason。

3.2 缺省配置

默认速率和优先级配置如下表所示：

表3-2 缺省配置

reason	rate(pps)	class	reason	rate(pps)	class
arp	640	1	mpls-ttl-fail	64	0
bpdu	64	3	ip-mtu-fail	64	0
dhcp	128	0	ospf	256	1
eapol	128	0	pim	128	1
erps	128	2	port-security-discard	128	0
fwd-to-cpu	64	0	rip	64	1
icmp-redirect	128	0	sflow-egress	128	0
igmp	128	2	sflow-ingress	128	0
ip-option	512	0	slow-protocol	128	1
ipda	1024	0	smart-link	128	2
ldp	512	1	ucast-ttl-fail	64	0
macsa-mismatch	128	0	udld	128	3
mcast-rpf-fail	128	1	vlan-security-discard	128	0
mld	128	2	vrrp	512	1
bfd-learning	128	1	-	-	-

3.3 配置 CPU Traffic

3.3.1 配置总限速

表3-3 配置总限速

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# cpu-traffic-limit total rate 3000	设置 CPU 流量总限速	总限速的取值范围范围为 0~1000000，单位：pps；缺省情况下，CPU 流量总限速为 2048pps

3.3.2 配置单个速率

表3-4 配置单个速率

命令	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# cpu-traffic-limit reason rip rate 500	设置 RIP PDU 限速	Protocol Data Unit（协议数据单元，缩写：PDU）

3.3.3 配置优先级类别

表3-5 配置优先级类别

命令	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# cpu-traffic-limit reason rip class 3	修改 RIP PDU 优先级类别	调度优先级类别的取值范围为 0~3，3 表示调度优先级最高

3.4 显示与维护

表3-6 显示与维护

命令	操作	说明
show cpu traffic-limit	查看 CPU traffic limit 的配置	-
show cpu traffic-statistics receive all	显示所有 CPU 报文的统计信息	-

查看 CPU traffic limit 的配置：

```
Switch# show cpu traffic-limit
reason                    rate (pps)     class
dot1x-mac-bypass          64             2
bpdu                      64             3
slow-protocol             128            1
eapol                     128            0
erps                      128            2
smart-link                128            2
```

```
udld                    128          3
loopback-detection      64           3
arp                     256          1
dhcp                    128          0
rip                     500          3
ldp                     512          1
ospf                    256          1
pim                     128          1
vrrp                    512          1
ipda                    1024         0
icmp-redirect           128          0
mcast-rpf-fail          128          1
macsa-mismatch          128          0
port-security-discard   128          0
vlan-security-discard   128          0
mtu-dontfrag            64           0
mtu-frag                64           0
ip-mtu-fail             64           0
bfd-learning            128          1
ip-option               512          0
ucast-ttl-fail          64           0
mpls-ttl-fail           64           0
igmp                    128          2
sflow-ingress           128          0
sflow-egress            128          0
fwd-to-cpu              64           0
l2protocol-tunnel       1024         0

Total rate:         3000 (pps)
```

显示所有上送 CPU 报文的统计信息：

```
Switch# show cpu traffic-statistics receive all
statistics rate time is 5 second(s)
reason                  count(packets)      rate(pps)
dot1x-mac-bypass        0                   0
bpdu                    0                   0
slow-protocol           0                   0
eapol                   0                   0
erps                    0                   0
smart-link              0                   0
udld                    0                   0
loopback-detection      0                   0
arp                     0                   0
dhcp                    0                   0
rip                     0                   0
ldp                     0                   0
ospf                    0                   0
```

pim	0	0
bgp	0	0
vrrp	0	0
rsvp	0	0
ipda	0	0
icmp-redirect	0	0
mcast-rpf-fail	0	0
macsa-mismatch	0	0
port-security-discard	0	0
vlan-security-discard	0	0
ip-mtu-fail	0	0
bfd-learning	0	0
ptp	0	0
ip-option	0	0
tunnel-gre-keepalive	0	0
ucast-ttl-fail	0	0
mpls-ttl-fail	0	0
igmp	0	0
sflow-ingress	0	0
sflow-egress	0	0
fwd-to-cpu	0	0
l2protocol-tunnel	0	0
mirror-to-cpu	0	0
mpls-tp-pwoam	0	0
other	0	0
Total	0	0

4 UDLD 配置

4.1 UDLD 简介

Unidirectional Link Detection（单向链路检测，缩写：UDLD）是一种可以检测和禁用单向链路的轻量级的协议。当出现单向链路时，一条链路上有两个端口，只能往一个方向的传输数据，即有且只有一个端口可以接收到数据。通过使用 UDLD 可以防止生成树等协议在单向链接时产生的异常情况，如回环等。

4.2 配置 UDLD

下面介绍了 UDLD 的相关配置，包括使能 UDLD 功能、设置 UDLD 消息间隔、重启所有被 UDLD 关闭的接口等，用户可以根据实际情况进行配置。

4.2.1 开启 UDLD 功能

UDLD功能既可以在全局配置模式下启用，也可以在接口配置模式下启用。

i. 全局开启/关闭UDLD功能

表4-1 全局开启/关闭UDLD功能

命令	操作	说明
udld enable	全局使能 UDLD 功能	缺省情况下，UDLD 功能处于关闭状态
no udld enable	关闭 UDLD 功能	

ii. 接口上开启/关闭UDLD功能

表4-2 接口上开启/关闭UDLD功能

命令	操作	说明
udld port [**aggressive**]	在指定接口上使能 UDLD 功能	缺省情况下，接口上的

命令	操作	说明
no udld port	关闭接口上的 UDLD 功能	UDLD 功能处于关闭状态；aggressive：UDLD 激进模式，不加 aggressive 即为普通模式

说明

在实际配置中，链路两端的设备需要同时开启 UDLD 功能，确保双通状态。

4.2.2 配置 UDLD 消息间隔时间

表4-3 配置UDLD消息间隔时间

命令	操作	说明
udld message interval *interval-value*	设置 UDLD 消息间隔时间	interval-value：UDLD 消息间隔时间，取值范围是 1~90，单位：秒；默认 UDLD 消息间隔时间为 15 秒
no udld message interval	取消 UDLD 消息间隔的配置，恢复默认值	

4.2.3 重置 UDLD 关闭的接口

表4-4 重启UDLD关闭的接口

命令	操作	说明
udld reset	重置被 UDLD 禁用的接口	该命令在特权模式下进行

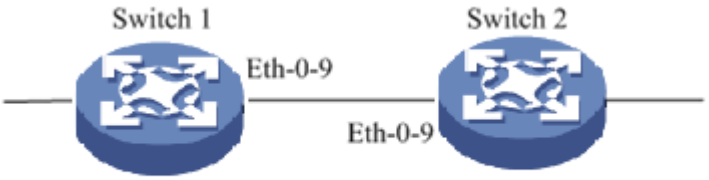
4.3 配置举例

4.3.1 介绍

分别对 Switch 1、Switch 2 配置 UDLD 相关的功能，请参考图 4-1。

4.3.2 拓扑

图 4-1 UDLD 典型拓扑图



4.3.3 配置步骤

Switch 1：

在 Switch 1 的 eth-0-9 接口上使能 UDLD 协议。

命令举例	操作步骤
Switch1# configure terminal	进入全局配置模式
Switch1(config)# interface eth-0-9	进入接口配置模式
Switch1(config-if)# no shutdown	配置端口为 UP 状态
Switch1(config-if)# udld port	在接口上使能 UDLD 协议
Switch1(config-if)# exit	退出接口配置模式
Switch1(config)# udld enable	全局使能 UDLD 协议
Switch1(config)# udld message interval 10	设置 UDLD 消息发送间隔时间

Switch 2：

在 Switch 2 的 eth-0-9 接口上使能 UDLD 协议。

命令举例	操作步骤
Switch2# configure terminal	进入全局配置模式
Switch2(config)# interface eth-0-9	进入接口配置模式
Switch2(config-if)# no shutdown	配置端口为 UP 状态
Switch2(config-if)# udld port	在接口上使能 UDLD 协议
Switch2(config-if)# exit	退出接口配置模式

命令举例	操作步骤
Switch2(config)# udld enable	全局使能 UDLD 协议
Switch2(config)# udld message interval 10	设置 UDLD 消息发送间隔

4.3.4 显示与维护

命令	操作
show udld [*if-name*]	显示接口的 UDLD 信息

下面分别列举配置举例中 Switch 1、Switch 2 的配置结果。

在 Switch 1 上显示接口的 UDLD 信息：

```
Switch# show udld eth-0-9
Interface eth-0-9
---
UDLD mode                : normal
Operation state    : Bidirectional
Message interval : 10
Message timeout      : 3
   Neighbor 1
   ---
   Device ID             : 4c7b.8510.ab00
   Port ID               : eth-0-9
   Device Name         : Switch
   Message interval: 10
   Message timeout : 3
   Link Status         : bidirectional
   Expiration time : 29
```

在 Switch 2 上显示接口的 UDLD 信息：

```
Switch# show udld eth-0-9
Interface eth-0-9
---
UDLD mode            : normal
Operation state : Bidirectional
Message interval: 10
Message timeout : 3
   Neighbor 1
```

```
---
Device ID            : 28bc.83db.8400
Port ID              : eth-0-9
Device Name          : Switch
Message interval: 10
Message timeout : 3
Link Status          : bidirectional
Expiration time : 23
```

5 Smart Link 配置

5.1 Smart Link 简介

Smart Link，中文译为灵活链路，又称为备份链路，是一种为链路双上行提供可靠高效的备份和切换机制的解决方案，常用于双上行组网。相比生成树协议（Spanning Tree Protocol，缩写：STP），Smart Link 技术能够提供更快速的收敛性能，相比ERPS，Smart Link 技术提供了更简洁的配置使用方式。该功能还可以提供链路负载均衡的功能。

5.2 配置 Smart Link

5.2.1 创建 Smart Link 组

表5-1 创建Smart Link组

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# smart-link group 1	创建一个 Smart link 组，并进入 Smart link 组配置模式	Smart link 组 ID 的取值范围为 1~16
Switch(config-smlk-group)# exit	退出 Smart link 组配置模式	-

5.2.2 配置主端口/副端口

每个 Smart-link 组都应该有两个端口（主端口 Master 和副端口 Slave）。端口类型可以是物理接口或 Agg 接口。下表以配置主端口为例。

表5-2 配置主端口/副端口

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-9	进入接口配置模式	-

命令举例	操作	说明
Switch(config-if)# spanning-tree port disable	关闭 STP 功能	端口必须关闭 STP 后才可以加入 Smart Link 组
Switch(config-if)# exit	退出接口配置模式	-
Switch(config)# smart-link group 1	创建一个 Smart Link 组，并进入 Smart Link 组配置模式	Smart Link 组 ID 的取值范围为 1~16
Switch(config-smlk-group)# interface eth-0-9 master	为 Smart Link 组设置主端口	缺省情况下，未指定任何端口

5.2.3 配置 Smart Link 组保护的 MSTP

Smart Link 只保护指定的 MSTP instance。如果 VLAN 没有加入任何 MSTP instance 则会默认加入 instance 0。

表5-3 配置Smart Link组保护的MSTP

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# smart-link group 1	创建一个 Smart Link 组，并进入 Smart Link 组配置模式	Smart Link 组 ID 的取值范围为 1~16
Switch(config-smlk-group)# protected mstp instance 0	设置 Smart Link 组保护的 MSTP 实例	MSTP 实例 ID 的取值范围为 0～4094；缺省情况下，未保护任何组的 MSTP 实例
Switch(config-smlk-group)# protected mstp instance 10		

说明

如果将加入 MSTP 实例的 VLAN 删除,那么在 Smart Link 组内被自动删除。

5.2.4 开启发送/接收 Flush 报文功能

i. 开启发送Flush报文功能

当主（转发）链路出现故障，流量切换到副端口时发送Flush FDB报文通知上游更新FDB。

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# smart-link group 1	创建一个 Smart Link 组，并进入 Smart Link 组配置模式	Smart Link 组 ID 的取值范围为 1~16
Switch(config-smlk-group)# flush send control-vlan 4 password simple test	开启发送 Flush 报文功能，并设置 Smart-link 发送更新报文的密码为 test	VLAN ID 的取值范围是 1～4094，更新报文的密码，长度为 1～15；缺省情况下，不发送 Smart Link 更新报文

ii. 开启接收Flush报文功能

收到的更新包应该与接收设备有相同的VLAN ID和密码。否则，数据包将被丢弃。

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-9	进入接口配置模式	-
Switch(config-if)# smart-link flush receive control-vlan 4 password simple test	开启接收 Flush 报文功能，并设置 Smart-link 组的接收更新报文的密码为 test	VLAN ID 的取值范围是 1～4094，更新报文的密码，长度为 1～15；缺省情况下，不接收 Smart Link 更新报文

5.3 配置举例

5.3.1 介绍

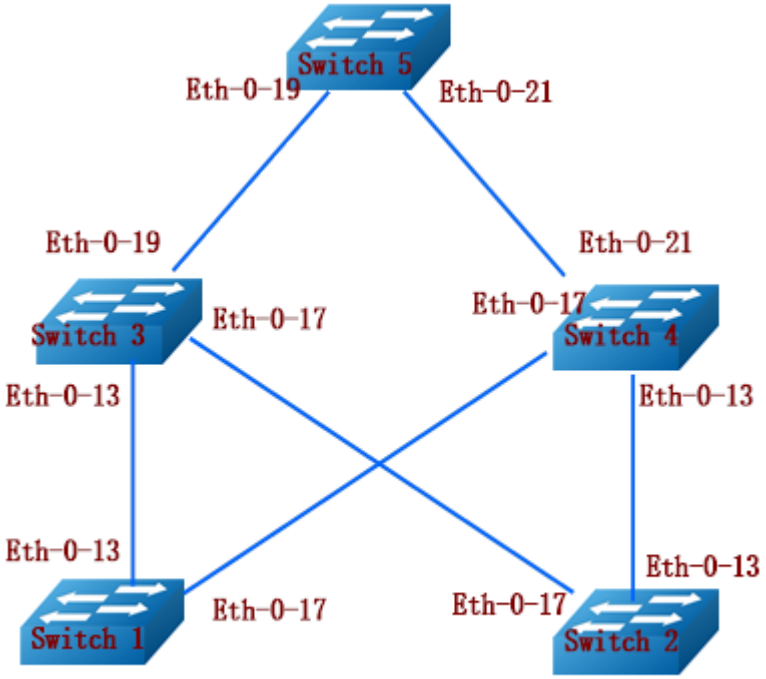
说明

- Smart Link 组的控制 VLAN 和保护 VLAN 必须提前用 **vlan database** 命令创建完成。
- Smart Link 组的端口必须把 STP 关闭。
- Smart Link 组的保护实例必须在配置 MSTP 模块前先创建完成。

下面的示例给出了 Smart Link 链路双上行保护的配置，给每台交换机配置 VLAN 1-20，MSTP instance 1-3。如**图** 5-1 所示。

5.3.2 拓扑

图 5-1 Smart Link 典型拓扑图



5.3.3 配置方法

上图是一个Smart-link的典型配置，交换机1和2配置Smart-link组；交换机3、4和5配置Smart-link的报文接收。其中，Switch 1与Switch 2的配置相同，下表以Switch 1为例。

Switch 1：

命令举例	操作步骤
Switch1# configure terminal	进入全局配置模式
Switch1(config)# vlan database	进入 VLAN 模式
Switch1(config- vlan)# vlan 2-20	创建 VLAN 2 到 20
Switch1(config- vlan)# exit	退出 VLAN 模式
Switch1(config)# spanning-tree mode mstp	配置 STP 的模式
Switch1(config)# spanning-tree mst configuration	进入 MSTP 配置模式

命令举例	操作步骤
Switch1(config-mst)# instance 1 vlan 1	配置 MSTP 的实例 1 关联 VLAN 1
Switch1(config-mst)# instance 2 vlan 2	配置 MSTP 的实例 2 关联 VLAN 2
Switch1(config-mst)# instance 3 vlan 3	配置 MSTP 的实例 3 关联 VLAN 3
Switch1(config-mst)# exit	退出 MSTP 配置模式
Switch1(config)# interface eth-0-13	进入端口 13
Switch1(config-if)# switchport mode trunk	配置端口为 Trunk 口
Switch1(config-if)# switchport trunk allowed vlan all	配置端口允许所有 VLAN 通过
Switch1(config-if)# spanning-tree port disable	关口端口上的 STP 功能
Switch1(config-if)# no shutdown	打开接口
Switch1(config-if)# exit	退出接口配置模式
Switch1(config)# interface eth-0-17	进入端口 17
Switch1(config-if)# switchport mode trunk	配置端口为 Trunk 口
Switch1(config-if)# switchport trunk allowed vlan all	配置端口允许所有 VLAN 通过
Switch1(config-if)# spanning-tree port disable	关口端口上的 STP 功能
Switch1(config-if)# no shutdown	打开接口
Switch1(config-if)# exit	退出接口配置模式
Switch1(config)# smart-link group 1	创建 Smart-link 组 1，并进入 Smart-link 组配置模式
Switch1(config-smlk-group)# interface eth-0-13 master	指定接口为 Master 端口
Switch1(config-smlk-group)# interface eth-0-17 slave	指定接口为 Slave 端口
Switch1(config-smlk-group)# protected mstp instance 1	指定保护的 MSTP Instance
Switch1(config-smlk-group)# protected mstp instance 2	指定保护的 MSTP Instance
Switch1(config-smlk-group)# protected mstp instance 3	指定保护的 MSTP Instance
Switch1(config-smlk-group)# load-balance instance 3	使能负载均衡的 Instance
Switch1(config-smlk-group)# restore time 40	设置自动倒换等待时间，取值范围为 30~1200s

命令举例	操作步骤
Switch1(config-smlk-group)# restore enable	启用自动倒换的功能
Switch1(config-smlk-group)# flush send control-vlan 10 password simple test	设置控制 VLAN 并指定 Smart-link 接收端的密码
Switch1(config-smlk-group)# group enable	启用 Smart-link 组
Switch1(config-smlk-group)# end	退出 Smart-link 组配置模式

Switch 3 与 Switch 4 的配置相同，下表以 Switch 3 为例。

Switch 3：

命令举例	操作步骤
Switch3# configure terminal	进入全局配置模式
Switch3(config)# interface eth-0-13	进入端口 13
Switch3(config-if)# switchport mode trunk	配置端口为 Trunk 口
Switch3(config-if)# no shutdown	打开接口
Switch3(config-if)# switchport trunk allowed vlan all	配置端口允许所有 VLAN 通过
Switch3(config-if)# smart-link flush receive control-vlan 10 password simple test	设置控制 VLAN 并指定 Smart-link 接收端的密码
Switch3(config-if)# exit	退出接口配置模式
Switch3(config)# interface eth-0-17	进入端口 17
Switch3(config-if)# no shutdown	打开接口
Switch3(config-if)# switchport mode trunk	配置端口为 Trunk 口
Switch3(config-if)# switchport trunk allowed vlan all	配置端口允许所有 VLAN 通过
Switch3(config-if)# smart-link flush receive control-vlan 10 password simple test	设置控制 VLAN 并指定 Smart-link 接收端的密码
Switch3 (config-if)# exit	退出接口配置模式

Switch 5：

命令举例	操作步骤
Switch5# configure terminal	进入全局配置模式

命令举例	操作步骤
Switch5(config)# interface eth-0-19	进入端口 19
Switch5(config-if)# switchport mode trunk	配置端口为 Trunk 口
Switch5(config-if)# no shutdown	打开端口
Switch5(config-if)# switchport trunk allowed vlan all	配置端口允许所有 VLAN 通过
Switch5(config-if)# smart-link flush receive control-vlan 10 password simple test	设置控制 VLAN 并指定 Smart-link 接收端的密码
Switch5(config-if)# exit	退出接口配置模式
Switch5(config)# interface eth-0-21	进入端口 21
Switch5(config-if)# switchport mode trunk	配置端口为 Trunk 口
Switch5(config-if)# no shutdown	打开端口
Switch5(config-if)# switchport trunk allowed vlan all	配置端口允许所有 VLAN 通过
Switch5(config-if)# smart-link flush receive control-vlan 10 password simple test	设置控制 VLAN 并指定 Smart-link 接收端的密码
Switch5(config-if)# exit	退出接口配置模式
Switch5(config)# no smart-link relay enable	取消 relay 功能

5.3.4 显示与维护

表5-4 显示与维护

命令	操作	说明
show smart-link	显示 Smart-link 的概要信息	-
show smart-link group [*group-id*]	显示指定 Smart-link 组或者全部 Smart-link 组的详细信息	Smart Link 组 ID 的取值范围为 1～16
clear smart-link statistic	清除 Smart-link 的统计	-

下面分别列举配置举例中 Switch 1~Switch 5 的配置结果。

- 显示Switch 1上Smart-link组1信息：

```
Switch1# show smart-link group 1

Smart-link group 1 information:
 The smart-link group was enabled.
 ============================================================
 Auto-restore:
   state          time                 count       Last-time
   enabled          40                   0          N/A
 ============================================================
 Protected instance: 1    2    3
 Load balance instance: 3
 Flush sender , Control-vlan ID: 10       Password:test
 ============================================================
 INTERFACE:
 Role     Member       DownCount Last-Down-Time    FlushCount Last-Flush-Time
 MASTER eth-0-13        0          N/A                 0         N/A
 SLAVE    eth-0-17      0          N/A                 0         N/A
 ============================================================
 Instance states in the member interfaces:
    A - ACTIVE ,      B -BLOCK    , D-The interface is link-down
 Map-instance-ID      MASTER(eth-0-13)       SLAVE(eth-0-17)
         1                   A                      B
         2                   A                      B
         3                   B                      A
```

- 显示Switch 2上Smart-link组1信息：

```
Switch2# show smart-link group 1

Smart-link group 1 information:
 The smart-link group was enabled.
 ============================================================
 Auto-restore:
   state          time                 count       Last-time
   enabled          40                   0          N/A
 ============================================================
 Protected instance: 1    2    3
 Load balance instance: 3
 Flush sender , Control-vlan ID: 10       Password:test
 ============================================================
 INTERFACE:
 Role     Member       DownCount Last-Down-Time    FlushCount Last-Flush-Time
 MASTER eth-0-13        0          N/A                 0         N/A
 SLAVE    eth-0-17      0          N/A                 0         N/A
 ============================================================
 Instance states in the member interfaces:
    A - ACTIVE ,      B -BLOCK    , D-The interface is link-down
 Map-instance-ID      MASTER(eth-0-13)       SLAVE(eth-0-17)
```

1	A	B
2	A	B
3	B	A

- 显示Switch 3上Smart-link的简略信息：

```
Switch3# show smart-link

 Relay smart-link flush packet is enabled
 Smart-link flush receiver interface:
     eth-0-13     control-vlan:10     password:test
     eth-0-17     control-vlan:10     password:test
Smart-link received flush packet number:0
Smart-link processed flush packet number:0
Smart link Group Number is 0.
```

- 显示Switch 4上Smart-link的简略信息：

```
Switch4# show smart-link

 Relay smart-link flush packet is enabled
 Smart-link flush receiver interface:
     eth-0-13     control-vlan:10     password:test
     eth-0-17     control-vlan:10     password:test
Smart-link received flush packet number:0
Smart-link processed flush packet number:0
Smart link Group Number is 0.
```

- 显示Switch 5上Smart-link的简略信息：

```
Switch5# show smart-link

 Relay smart-link flush packet is disabled
 Smart-link flush receiver interface:
     eth-0-21     control-vlan:10     password: test
     eth-0-19     control-vlan:10     password:test
Smart-link received flush packet number:0
Smart-link processed flush packet number:0
 Smart link Group Number is 0.
```

6 Multi-Link 配置

6.1 Multi-Link 简介

Multi-Link，中文译为多链路，又称为多备份链路，是一种为链路多上行提供可靠高效的备份和切换机制的解决方案。多备份链路的接入可以增加带宽，起到分流的作用。该计划功能和 Smart Link 类似，备份的链路从一条扩充为多条，最多可以有4个成员。如果其中一条链路出现问题，则会切换到其他线路。

该功能还可以提供链路负载均衡的功能。

6.2 配置 Multi-Link

6.2.1 创建 Multi-Link 组

表6-1 创建Multi-Link组

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# multi-link group 1	创建一个 Multi-Link 组，并进入 Multi-Link 组配置模式	Multi-Link 组 ID 的取值范围为 1~16
Switch(config-multilk-group)# exit	退出 Multi-Link 组配置模式	-

6.2.2 配置指定接口的优先级

每个Multi-link组都至少有两个端口。端口类型可以是物理接口或Agg接口。

表6-2 配置指定接口的优先级

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-

命令举例	操作	说明
Switch(config)# interface eth-0-9	进入接口配置模式	-
Switch(config-if)# spanning-tree port disable	关闭 STP 功能	端口必须关闭 STP 后才可以加入 Multi-Link 组
Switch(config-if)# exit	退出接口配置模式	-
Switch(config)# multi-link group 1	创建一个 Multi-Link 组，并进入 Multi-Link 组配置模式	Multi-Link 组 ID 的取值范围为 1~16
Switch(config-multilk-group)# interface eth-0-9 priority 1	指定接口 eth-0-9 的优先级为 1	缺省情况下，未指定任何接口的优先级

6.2.3 配置 Multi-Link 组保护的 MSTP

Multi-link 只保护指定的 MSTP instance。如果 VLAN 没有加入任何 MSTP instance 则会默认加入 instance 0。

表5-3 配置Multi-Link组保护的MSTP

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# multi-link group 1	创建一个 Multi-Link 组，并进入 Multi-Link 组配置模式	Multi-Link 组 ID 的取值范围为 1~16
Switch(config-multilk-group)# protected mstp instance 0	设置 Multi-Link 组保护的 MSTP 实例	MSTP 实例 ID 的取值范围为 0～4094；缺省情况下，未保护任何组的 MSTP 实例
Switch(config-multilk-group)# protected mstp instance 10		

说明

如果将加入 MSTP 实例的 VLAN 删除,那么在 Multi-Link 组内被自动删除。

6.2.4 开启发送/接收 Flush 报文功能

i. 开启发送Flush报文功能

当主（转发）链路出现故障，流量切换到副端口时发送Flush FDB报文通知上游更新FDB。

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# multi-link group 1	创建一个 Multi-Link 组，并进入 Multi-Link 组配置模式	Multi-Link 组 ID 的取值范围为 1~16
Switch(config-smlk-group)# flush send control-vlan 4 password simple test	开启发送 Flush 报文功能，并设置 Multi-link 发送更新报文的密码为 test	VLAN ID 的取值范围是 1～4094，更新报文的密码，长度为 1～15；缺省情况下，不发送 Multi-Link 更新报文

ii. **开启接收Flush报文功能**

收到的更新包应该与接收设备有相同的VLAN ID和密码。否则，数据包将被丢弃。

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-9	进入接口配置模式	-
Switch(config-if)# multi-link flush receive control-vlan 4 password simple test	开启接收 Flush 报文功能，并设置 Multi-link 组的接收更新报文的密码为 test	VLAN ID 的取值范围是 1～4094，更新报文的密码，长度为 1～15；缺省情况下，不接收 Multi-Link 更新报文

6.3 Multi-Link 配置举例

6.3.1 介绍

说明

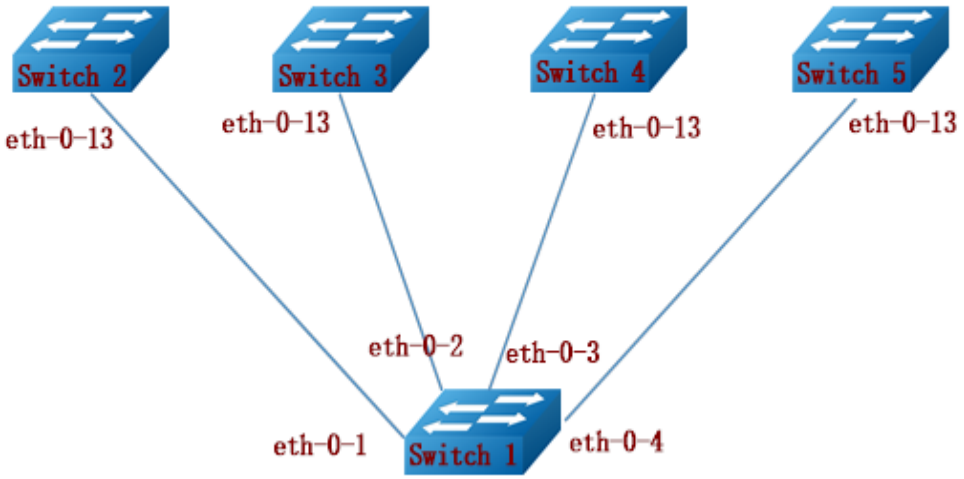
- Multi-Link 组的控制 VLAN 和保护 VLAN 必须先用 **vlan database** 命令创建完成。
- Multi-Link 组的端口必须把 STP 关闭。
- Multi-Link 组的保护实例必须在配置 MSTP 模块前先创建完成。

下面的示例给出了Multi-Link链路多上行保护的配置，给每台交换机配置VLAN 2-10，MSTP instance 1-

4，如图 6-1所示。

6.3.2 拓扑

图 6-1 Multi-Link 典型拓扑图



6.3.3 配置方法

下表介绍了 Mulit-link 的典型配置，交换机 1 配置 Multi-link 组；交换机 2、3、4 和 5 配置 Multi-link 的报文接收。

Switch 1：

命令举例	操作步骤
Switch1# configure terminal	进入全局配置模式
Switch1(config)# vlan database	进入 VLAN 配置模式
Switch1(config- vlan)# vlan 2-10	创建 VLAN 2 到 10
Switch1(config- vlan)# exit	退出 VLAN 配置模式
Switch1(config)# spanning-tree mode mstp	配置 STP 的模式
Switch1(config)# spanning-tree mst configuration	进入 MSTP 配置模式
Switch1(config-mst)# instance 1 vlan 1	配置 MSTP 的实例 1 关联 VLAN 1

命令举例	操作步骤
Switch1(config-mst)# instance 2 vlan 2	配置 MSTP 的实例 2 关联 VLAN 2
Switch1(config-mst)# instance 3 vlan 3	配置 MSTP 的实例 3 关联 VLAN 3
Switch1(config-mst)# instance 4 vlan 4-10	配置 MSTP 的实例 4 关联 VLAN 4
Switch1(config-mst)# exit	退出 MSTP 配置模式
Switch1(config)# interface range eth-0-1 - 4	进入端口 1-4
Switch1(config-if)# switchport mode trunk	配置端口为 Trunk 口
Switch1(config-if)# switchport trunk allowed vlan all	配置端口允许所有 VLAN 通过
Switch1(config-if)# spanning-tree port disable	关口端口上的 STP 功能
Switch1(config-if)# no shutdown	打开接口
Switch1(config-if)# exit	退出接口配置模式
Switch1(config)# multi-link group 1	创建 Multi-Link 组 1
Switch1(config-multilk-group)# interface eth-0-1 priority 1	指定接口 1 优先级为 1
Switch1(config-multilk-group)# interface eth-0-2 priority 2	指定接口 2 优先级为 2
Switch1(config-multilk-group)# interface eth-0-3 priority 3	指定接口 3 优先级为 3
Switch1(config-multilk-group)# interface eth-0-4 priority 4	指定接口 4 优先级为 4
Switch1(config-multilk-group)# protected mstp instance 1	指定保护的 MSTP Instance
Switch1(config-multilk-group)# protected mstp instance 2	指定保护的 MSTP Instance
Switch1(config-multilk-group)# protected mstp instance 3	指定保护的 MSTP Instance
Switch1(config-multilk-group)# protected mstp instance 4	指定保护的 MSTP Instance
Switch1(config-multilk-group)# load-balance instance 2 priority 2	使能负载均衡的 Instance
Switch1(config-multilk-group)# load-balance instance 3	使能负载均衡的 Instance

命令举例	操作步骤
priority 3	
Switch1(config-multilk-group)# load-balance instance 4 priority 4	使能负载均衡的 Instance
Switch1(config-multilk-group)# restore time 40	设置自动倒换等待时间，取值范围为 30~1200s
Switch1(config-multilk-group)# restore enable	启用自动倒换的功能
Switch1(config-multilk-group)# flush send control-vlan 10 password simple test	设置控制 VLAN 并指定 Multi-Link 接收端的密码
Switch1(config-multilk-group)# group enable	启用 Multi-Link 组
Switch1(config-multilk-group)# end	退出 Multi-Link 组模式

下表为 Switch 2 的配置，Switch 3~ Switch 5 的配置与 Switch 2 一致。

Switch 2：

命令举例	操作步骤
Switch2# configure terminal	进入全局配置模式
Switch2(config)# interface eth-0-13	进入端口 13
Switch2(config-if)# switchport mode trunk	配置端口为 Trunk 口
Switch2(config-if)# switchport trunk allowed vlan all	配置端口允许所有 VLAN 通过
Switch2(config-if)# no shutdown	打开接口
Switch2(config-if)# switchport trunk allowed vlan all	配置端口允许所有 VLAN 通过
Switch2(config-if)# multi-link flush receive control-vlan 10 password simple test	设置控制 VLAN 并指定 Multi-Link 接收端的密码
Switch2(config-if)# exit	退出接口配置模式

6.3.4 显示与维护

命令	操作	说明
show multi-link	显示 Multi-link 的简要信息	-

命令	操作	说明
show multi-link group [*group-id*]	显示指定 Multi-link 组或者全部 Multi-link 组的详细信息	Multi-Link 组 ID 的取值范围为 1～16
clear multi-link statistic	清除 Multi-link 的统计信息	-

显示 Switch 1 上 Multi-link 组 1 信息：

```
Switch1# show multi-link group 1

Multi-link group 1 information:
 The multi-link group was enabled.
 ============================================================
 Auto-restore:
   state          time                 count       Last-time
   enabled         40                    0          N/A
 ============================================================
 Protected instance: 1   2   3   4
 Load balance instance: 2(to P2)   3(to P3)   4(to P4)
 Flush sender , Control-vlan ID: 10       Password:test
 ============================================================
 INTERFACE:
 Role    Member      DownCount Last-Down-Time          FlushCount Last-Flush-Time
 PRI1    eth-0-1     0             N/A                 1          2016/09/05,07:13:24
 PRI2    eth-0-2     0             N/A                 1          2016/09/05,07:13:24
 PRI3    eth-0-3     0             N/A                 1          2016/09/05,07:13:24
 PRI4    eth-0-4     0             N/A                 1          2016/09/05,07:13:24
 ============================================================
 Instance states in the member interfaces:
    A - ACTIVE ,     B -BLOCK    , D-The interface is link-down
 Map-instance-ID   P1(eth-0-1 )   P2(eth-0-2 )   P3(eth-0-3 )   P4(eth-0-4 )
 1                   A               B               B               B
 2                   B               A               B               B
 3                   B               B               A               B
 4                   B               B               B               A
```

显示 Switch 2 上 Multi-link 的简要信息：

```
Switch2# show multi-link

Relay multi-link flush packet is enabled
 Multi-link flush receiver interface:
     eth-0-13     control-vlan:10     password:test
 Multi-link received flush packet number:0
 Multi-link processed flush packet number:0
 Multi-link tcn is disabled
```

```
Multi-link tcn query count       :2
Multi-link tcn query interval :10
Multi-link Group Number is 0.
```

6.4 Multi-Link 增强配置举例

6.4.1 介绍

当分布在不同交换机的两组 Mulit-Link 作相互链路备份时，会由于一方的 Mulit-Link 成员的保护实例被 block 住而无法进行链路相互备份。

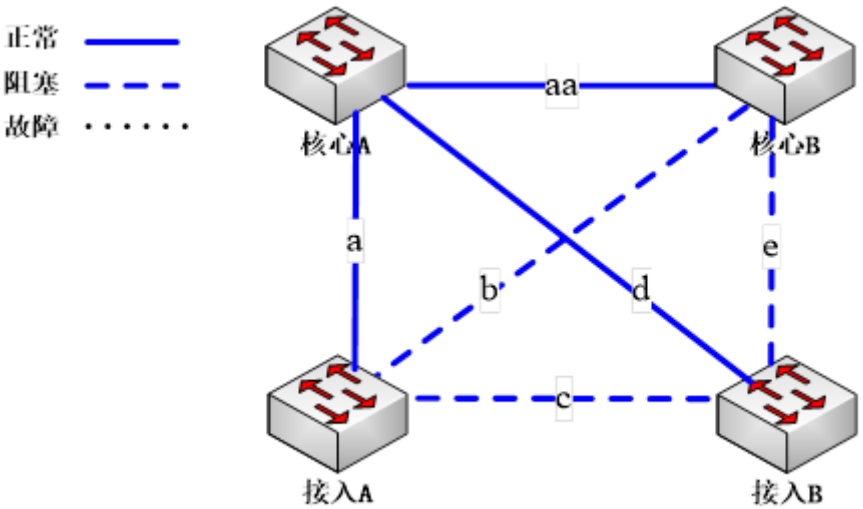
用户场景：

核心交换机A、核心交换机B、接入交换机A、接入交换机B形成全网状拓扑。

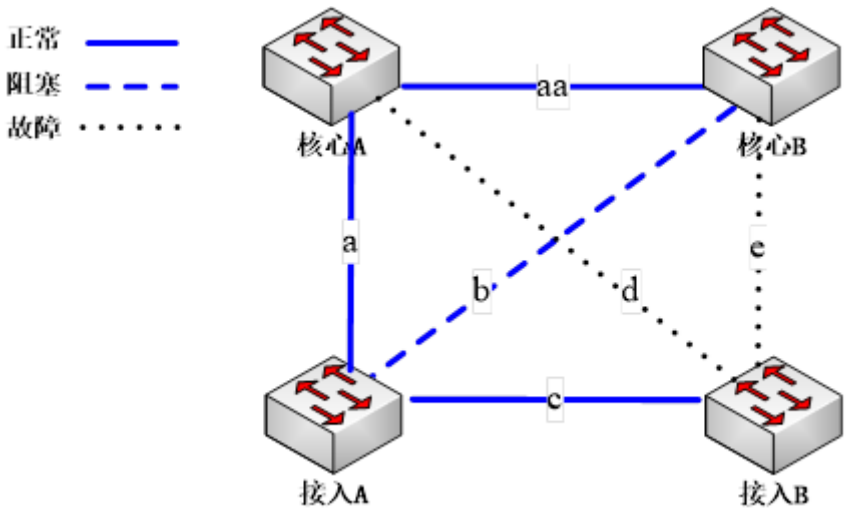
接入交换机A配置 Mulit-Link 协议，链路a、b、c优先级分别为1、2、3；

接入交换机B配置 Mulit-Link 协议，链路d、e优先级分别为1、2；

正常情况下，链路b、c、e处于block状态，链路a、d处于 active 状态，如下图所示。



当接入交换机 B 链路 d、e 全部断掉后，仅余下链路 c 与接入交换机 A 连接，如下图所示：



此时，接入交换机 A 链路 a 处于 active 状态，接入交换机对应链路 c 的端口处于 block 状态，接入交换机 B 处于孤岛状态。

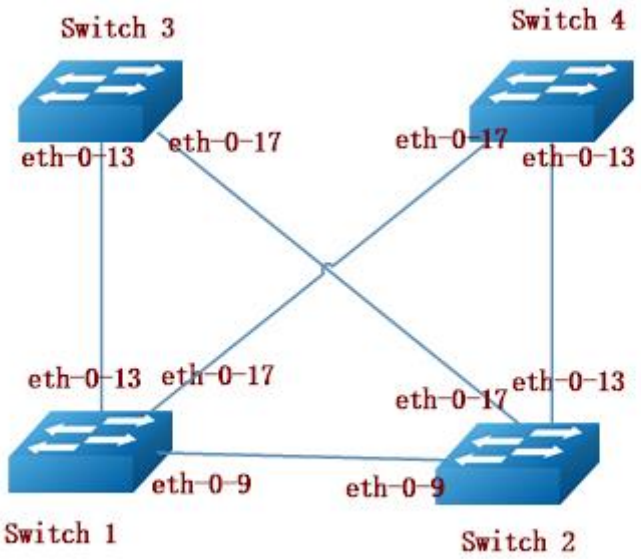
说明

- Multi-Link 组的控制 VLAN 和保护 VLAN 必须先用 **vlan database** 命令创建完成。
- Multi-Link 组的端口必须把 STP 关闭。
- Multi-Link 组的保护实例必须在配置 MSTP 模块前先创建完成。
- Multi-Link 组中应先配置 **flush send** 的 control vlan 和 password，然后才能配置 Multi-Link 增强。

6.4.2 拓扑

下面是一个 Mulit-Link 的典型配置，交换机1, 2均配置 Multi-Link 组。Switch 1 Multi-Link 组里面配有三个成员 ，且优先级最低的成员为 Mulit-Link 增强的接收口。Switch 2 Mulit-Link 组里面配有两个成员，此外还配有 Mulit-Link 增强的发送口。如图 6-2所示。

图 6-2 Mulit-Link 增强典型拓扑图



6.4.3 配置方法

下面的示例给出了 Multi-Link 链路多上行保护的配置，给每台交换机配置 VLAN 10, 20, 30, 40，MSTP instance 1,2。

Switch 1：

命令举例	操作步骤
Switch1# configure terminal	进入全局配置模式
Switch1(config)# vlan database	进入 VLAN 配置模式
Switch1(config- vlan)# vlan 10	创建 VLAN 10
Switch1(config- vlan)# vlan 20	创建 VLAN 20
Switch1(config- vlan)# vlan 30	创建 VLAN 30
Switch1(config- vlan)# vlan 40	创建 VLAN 40
Switch1(config- vlan)# exit	退出 VLAN 模式
Switch1(config)# spanning-tree mode mstp	配置 STP 的模式
Switch1(config)# spanning-tree mst configuration	进入 MSTP 配置模式

命令举例	操作步骤
Switch1(config-mst)# instance 1 vlan 10	配置 MSTP 的实例 1 关联 VLAN 10
Switch1(config-mst)# instance 1 vlan 30	配置 MSTP 的实例 1 关联 VLAN 30
Switch1(config-mst)# instance 2 vlan 20	配置 MSTP 的实例 2 关联 VLAN 20
Switch1(config-mst)# instance 2 vlan 40	配置 MSTP 的实例 2 关联 VLAN 40
Switch1(config-mst)# exit	退出 MSTP 配置模式
Switch1(config)# interface range eth-0-9	进入端口 9
Switch1(config-if)# switchport mode trunk	配置端口为 Trunk 口
Switch1(config-if)# switchport trunk allowed vlan all	配置端口允许所有 VLAN 通过
Switch1(config-if)# spanning-tree port disable	关口端口上的 STP 功能
Switch1(config-if)# no shutdown	打开接口
Switch1(config-if)# exit	退出接口配置模式
Switch1(config)# interface range eth-0-13	进入端口 13
Switch1(config-if)# switchport mode trunk	配置端口为 Trunk 口
Switch1(config-if)# switchport trunk allowed vlan all	配置端口允许所有 VLAN 通过
Switch1(config-if)# spanning-tree port disable	关口端口上的 STP 功能
Switch1(config-if)# no shutdown	打开接口
Switch1(config-if)# exit	退出接口配置模式
Switch1(config)# interface range eth-0-17	进入端口 17
Switch1(config-if)# switchport mode trunk	配置端口为 Trunk 口
Switch1(config-if)# switchport trunk allowed vlan all	配置端口允许所有 VLAN 通过
Switch1(config-if)# spanning-tree port disable	关口端口上的 STP 功能
Switch1(config-if)# no shutdown	打开接口
Switch1(config-if)# exit	退出接口配置模式
Switch1(config)# multi-link group 1	创建 Multi-Link 组 1
Switch1(config-multilk-group)# interface eth-0-13 priority 1	指定接口 13 优先级为 1

命令举例	操作步骤
Switch1(config-multilk-group)# interface eth-0-17 priority 2	指定接口 17 优先级为 2
Switch1(config-multilk-group)# interface eth-0-9 priority 3	指定接口 9 优先级为 3
Switch1(config-multilk-group)# protected mstp instance 1	指定保护的 MSTP Instance
Switch1(config-multilk-group)# protected mstp instance 2	指定保护的 MSTP Instance
Switch1(config-multilk-group)# flush send control-vlan 30 password simple a	设置控制 VLAN 并指定 Multi-Link 发送端的密码
Switch1(config-multilk-group)# multilink-enhance receive control-vlan 10 password b interface eth-0-9	启用 eth-0-9 口接收 multilink-enhance 报文
Switch1(config-multilk-group)# group enable	启用 Multi-Link 组
Switch1(config-multilk-group)# end	退出 Multi-Link 组模式

Switch 2：

命令举例	操作步骤
Switch2# configure terminal	进入全局配置模式
Switch2(config)# vlan database	进入 VLAN 配置模式
Switch2(config- vlan)# vlan 10	创建 VLAN 10
Switch2(config- vlan)# vlan 20	创建 VLAN 20
Switch2(config- vlan)# exit	退出 VLAN 配置模式
Switch2(config)# spanning-tree mode mstp	配置 STP 的模式
Switch2(config)# spanning-tree mst configuration	进入 MSTP 配置模式
Switch2(config-mst)# instance 1 vlan 10	配置 MSTP 的实例 1 关联 VLAN 10
Switch2(config-mst)# instance 2 vlan 20	配置 MSTP 的实例 2 关联 VLAN 20
Switch2(config-mst)# exit	退出 MSTP 配置模式
Switch2(config)# interface eth-0-13	进入端口 13
Switch2(config-if)# switchport mode trunk	配置端口为 Trunk 口

命令举例	操作步骤
Switch2(config-if)# switchport trunk allowed vlan all	配置端口允许所有 VLAN 通过
Switch2(config-if)# no shutdown	打开接口
Switch2(config-if)# exit	退出接口配置模式
Switch2(config)# interface eth-0-17	进入端口 13
Switch2(config-if)# switchport mode trunk	配置端口为 Trunk 口
Switch2(config-if)# switchport trunk allowed vlan all	配置端口允许所有 VLAN 通过
Switch2(config-if)# no shutdown	打开接口
Switch2(config-if)# exit	退出接口配置模式
Switch2(config)# multi-link group 1	创建 Multi-Link 组 1
Switch2(config-multilk-group)# interface eth-0-13 priority 1	指定接口 13 优先级为 1
Switch2(config-multilk-group)# interface eth-0-17 priority 2	指定接口 17 优先级为 2
Switch2(config-multilk-group)# protected mstp instance 1	指定保护的 MSTP Instance
Switch2(config-multilk-group)# protected mstp instance 2	指定保护的 MSTP Instance
Switch2(config-multilk-group)# flush send control-vlan 10 password simple b	设置控制 VLAN 并指定 Multi-Link 发送端的密码
Switch2(config-multilk-group)# multilink-enhance interface eth-0-9	设置发送 Multi-Link 增强报文的接口
Switch2(config-multilk-group)# group enable	启用 Multi-link 组
Switch2(config-multilk-group)# exit	退出 Multi-Link 组模式
Switch2(config)# interface eth-0-9	进入接口配置模式下
Switch2(config-if)# multi-link flush receive control-vlan 30 password simple a	配置该接口可以接收 Flush 报文，control vlan id 和 passward 要和 Switch 1 配置 **flush send** 一致
Switch2(config-if)#end	退出接口配置模式

说明

Switch 3 和 Switch 4 只需要配置接收 Flush 报文即可。

6.4.4 显示与维护

命令	操作	说明
show multi-link	显示 Multi-link 的简要信息	-
show multi-link group [*group-id*]	显示指定 Multi-link 组或者全部 Multi-link 组的详细信息	Multi-Link 组 ID 的取值范围为 1～16
clear multi-link statistic	清除 Multi-link 的统计信息	-

显示 Switch 1 上 Multi-link 组 1 信息：

```
Switch1# show multi-link group 1

Multi-link group 1 information:
 The multi-link group was enabled.
 ============================================================
 Auto-restore:
   state          time                count       Last-time
   disabled       60                   0           N/A
 ============================================================
 Protected instance: 1    2
 Load balance instance:
 Flush sender , Control-vlan ID: 30       Password: a
 ============================================================
 INTERFACE:
 Role     Member       DownCount Last-Down-Time          FlushCount Last-Flush-Time
 PRI1     eth-0-13   0             N/A                      5             2017/05/15,07:50:11
 PRI2     eth-0-17   0             N/A                      0             N/A
 PRI3     eth-0-9    1             2017/05/15,07:48:46 5             2017/05/15,07:50:11
 PRI4     N/A          0             N/A                      0             N/A
 ============================================================
 Instance states in the member interfaces:
    A-ACTIVE ,      B-BLOCK ,   A(E)-ENHANCE_ACTIVE      D-The interface is link-down
 Map-instance-ID   P1(eth-0-13)      P2(eth-0-17)      P3(eth-0-9)       P4(N/A)
 1                      A                    B                   B                   D
```

```
2                A                B                B                D
```

显示 Switch 1 上 Multi-link 的简要信息：

```
Switch1# show multi-link
Relay multi-link flush packet is enabled
 Multi-link enhance receiver interface:
     eth-0-9      control-vlan:10     password:b
 Multi-link received flush packet number : 0
 Multi-link processed flush packet number: 0
 Multi-link received enhance packet number : 4
 Multi-link processed enhance packet number: 4
 Multi-link tcn is disabled
 Multi-link tcn query count       : 2
 Multi-link tcn query interval : 10
 Multi-link Group Number is 1.
  Group-ID      State          Pri-1         Pri-2         Pri-3         Pri-4
  1             enabled        eth-0-13      eth-0-17      eth-0-9       N/A
```

显示 Switch 2 上 Multi-link 组 1 信息：

```
Switch2# show multi-link group1

Multi-link group 1 information:
 The multi-link group was enabled.
 ============================================================
 Auto-restore:
   state          time                 count        Last-time
   disabled       60                    0            N/A
 ============================================================
 Protected instance: 1    2
 Load balance instance:
 Flush sender , Control-vlan ID: 10       Password: b
 Multilk enhance interface: eth-0-9, Control-vlan ID: 10    Password: b
 ============================================================
 INTERFACE:
 Role     Member      DownCount Last-Down-Time          FlushCount Last-Flush-Time
 PRI1     eth-0-13    1             2017/05/15,07:49:15 0             N/A
 PRI2     eth-0-17    2             2017/05/15,07:50:03 3             2017/05/15,07:50:11
 PRI3     N/A           0             N/A                           0             N/A
 PRI4     N/A           0             N/A                           0             N/A
 ============================================================
ENHANCE INTERFACE:
 Role     Member      DownCount Last-Down-Time          EnhanceCount Last-SendEnhance-Ti
```

```
me
 M-En     eth-0-9     0            N/A                    0              N/A

 ============================================================
 Instance states in the member interfaces:
    A-ACTIVE ,      B-BLOCK ,   A(E)-ENHANCE_ACTIVE      D-The interface is link-down
 Map-instance-ID   P1(eth-0-13)     P2(eth-0-17)     P3(N/A)          P4(N/A)
 1                    A                  B                D                D
 2                    A                  B                D                D
```

显示 Switch 2 上 Multi-link 的简要信息：

```
Switch2# show multi-link
Relay multi-link flush packet is enabled
 Multi-link received flush packet number : 0
 Multi-link processed flush packet number: 0
 Multi-link received enhance packet number : 0
 Multi-link processed enhance packet number: 0
 Multi-link tcn is disabled
 Multi-link tcn query count       : 2
 Multi-link tcn query interval : 10
 Multi-link Group Number is 1.
  Group-ID      State         Pri-1        Pri-2       Pri-3       Pri-4
  1             enabled       eth-0-13     eth-0-17    N/A          N/A
```

7 Monitor Link 配置

7.1 Monitor Link 简介

Monitor Link 是对 Smart Link 进行补充而引入的端口联动方案，用于扩展 Smart Link 的链路备份的范围。通过监控上行链路对下行链路进行同步设置，如果上行链路出现故障，这一变化会迅速传达给下行设备，从而触发 Smart Link 的主备链路切换，防止长时间因上行链路故障而出现流量丢失。

7.2 配置 Monitor Link

7.2.1 创建 Monitor Link 组

表7-1 创建Monitor Link组

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# monitor-link group 1	创建一个 Monitor Link 组，并进入 Monitor Link 组配置模式	Monitor Link 组 ID 的取值范围为 1~16
Switch(config-mtlk-group)# exit	退出 Monitor Link 组配置模式	-

7.2.2 创建上联/下联端口

各类端口中只有物理端口和 Agg 端口才可以作为 Monitor Link 的上联端口。

表7-2 创建上联端口

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# monitor-link group 1	创建一个 Monitor Link 组，并进入 Monitor Link 组配置模式	Monitor Link 组 ID 的取值范围为 1~16

命令举例	操作	说明
Switch(config-mtlk-group)# monitor-link uplink interface eth-0-1	为 Monitor Link 组添加上联端口 eth-0-1	缺省情况下，未指定 Monitor Link 组的上联端口

表7-3 创建下联端口

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# monitor-link group 1	创建一个 Monitor Link 组，并进入 Monitor Link 组配置模式	Monitor Link 组 ID 的取值范围为 1~16
Switch(config-mtlk-group)# monitor-link downlink interface eth-0-1	为 monitor link 组添加下联端口 eth-0-1	缺省情况下，未指定 Monitor Link 组的下联端口

7.2.3 配置下联端口恢复时间

如果上联端口状态恢复为 up，所有的下联端口状态也将在指定的恢复时间后改为 up。以防止上联端口不停 up/down 导致下联端口频繁改变状态。

表7-4 配置下联端口恢复时间

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# monitor-link recover-time 1	配置 Monitor Link 组下联端口恢复时间为 1 秒	Monitor Link 组下联端口恢复时间的取值范围为 0~60，单位：秒；缺省情况下，下联端口恢复时间为 3 秒

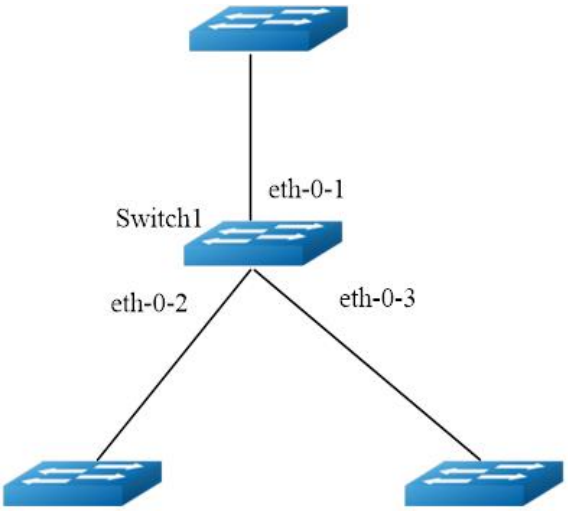
7.3 配置举例

7.3.1 介绍

在 Switch 1 上为 Monitor Link 组创建上联和下联端口，如图 7-1 所示。

7.3.2 拓扑

图 7-1 Monitor Link 典型拓扑图



7.3.3 配置方法

命令举例	操作步骤
Switch1# configure terminal	进入全局配置模式
Switch1(config)# interface range eth-0-1 - 3	进入接口配置模式
Switch1(config-if-range)# no shutdown	打开端口
Switch1(config-if-range)# exit	退出接口配置模式
Switch1(config)# monitor-link group 1	创建 Monitor Link 组 1，并进入 Monitor Link 组配置模式
Switch1(config-mtlk-group)# monitor-link uplink interface eth-0-1	将端口 eth-0-1 作为上联端口
Switch1(config-mtlk-group)# monitor-link downlink interface eth-0-2	将端口 eth-0-2 作为下联端口
Switch1(config-mtlk-group)# monitor-link downlink interface eth-0-3	将端口 eth-0-3 作为下联端口
Switch1(config-mtlk-group)# end	退出 Monitor Link 组配置模式

7.3.4 显示与维护

命令	操作	说明
show monitor-link group [*group-id*]	显示指定 Monitor Link 组或者全部 Monitor Link 组的信息	Monitor Link 组 ID 的取值范围为 1～16

显示 Switch 1 上的 Monitor Link 组的信息：

```
Switch1# show monitor-link group

Group Id: 1
Monitor link status: UP
Role      Member    Last-up-time          Last-down-time          upcount    downcount
UpLk 1    eth-0-1   2011/07/15,02:07:31   2011/07/15,02:07:31     2          1
DwLk 1    eth-0-2   2011/07/15,02:07:34   2011/07/15,02:07:31     1          1
DwLk 2    eth-0-3   N/A                   N/A                     0          0
```

8 VRRP 配置

8.1 VRRP 简介

一般情况下，子网内的所有主机都会设置一条相同的到网关的缺省路由。主机发出的所有不在本网段的目的地址的报文将通过缺省路由发往网关，从而实现主机与外部网络的通信。当网关发生故障时，本网段内所有以网关为缺省路由的主机将中断与外部网络的通信。

缺省路由为用户的配置操作提供了方便，但是对缺省网关设备提出了很高的稳定性要求。出口网关的增加可以提高系统的可靠性，而如何能在多个出口之间选择 IP 路由的问题还有待解决。

虚拟路由器冗余协议（Virtual Router Redundancy Protocol，缩写：VRRP）可以解决以上问题。在具有多播或广播能力的局域网（如以太网）中，借助 VRRP 能在某台设备出现故障时仍然提供高可靠的缺省链路，而无需修改用户的配置信息。

VRRP 将局域网内的一组路由器（包括一个 Master 路由器和若干个 Backup 路由器）组成一个备份组，功能上相当于一台虚拟路由器。

VRRP 备份组具有以下特点：

- 局域网内的主机仅需要获取这个虚拟路由器的 IP 地址，并将其设置为缺省路由的下一跳地址。
- 网络内的主机通过这个虚拟路由器与外部网络进行通信。
- 备份组内的路由器根据一定的选举机制，分别承担网关的功能。当备份组内承担网关功能的路由器发生故障时，其余的路由器将取代它继续履行网关职责。

8.1.1 参考

VRRP 参考文档如下：

RFC 3768（VRRP）：Knight, S., et.al "Virtual Router Redundancy Protocol (VRRP)

8.1.2 术语解释

Backup Router：VRRP 备份路由器。当 Master 路由器转发失败的时候启用备份路由器。

Critical IP：VRRP 路由器发送/接收一个特定的会话信息的 IP 地址。

IP Address Owner：VRRP 路由器将虚拟路由器的 IP 地址作为真实的接口地址。当这台设备正常工作时，它会响应目的地址是虚拟 IP 地址的报文，如 ping、TCP 连接等。

Master Router：拥有虚拟 IP 地址的路由器。此时它成为主机的默认网关，负责转发数据流。

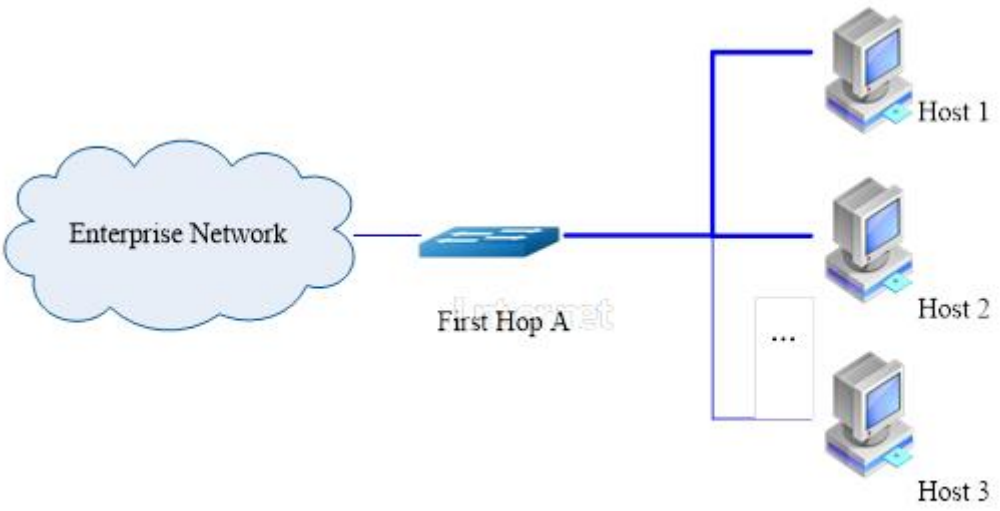
Virtual IP：虚拟路由器的 IP 地址，一个虚拟路由器可以有一个 IP 地址，由用户配置。

Virtual Router：由 VRRP 管理的抽象设备，又称为 VRRP 备份组，被当作一个共享局域网内主机的缺省网关。它包括了一个虚拟路由器标识符和一个虚拟 IP 地址。

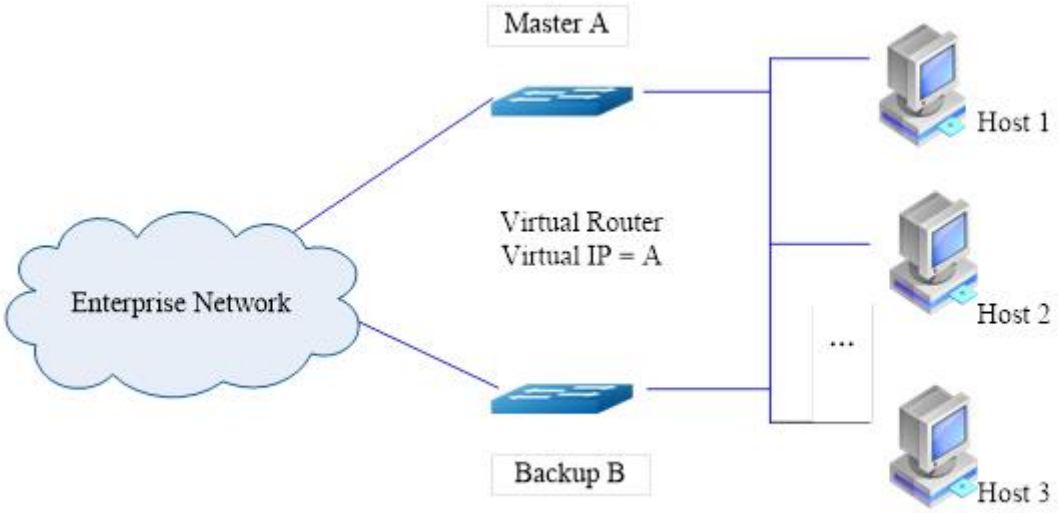
VRRP Router：运行 VRRP 的设备，它可能属于一个或多个虚拟路由器。

8.1.3 VRRP Process

通常情况下，终端主机是通过将在同一个局域网内的路由器作为其第一个下一跳连接到企业网的。终端主机最常见的配置就是静态配置这个默认网关。这可以最大限度地减少配置和处理开销。如果第一跳路由器出现问题，它会产生一个单点故障。



虚拟路由器冗余协议试图通过引入一个虚拟路由器的概念来解决这个问题，它通常由在同一子网中的两个或两个以上的 VRRP 路由器组成。同时它还引入了一个虚拟 IP 地址的概念，终端主机使用这个 IP 作为它们的默认网关地址。只有主路由器负责转发数据包，在主路由器出现故障时，其他路由器（备份）中的一个代替主路由器负责转发。



上述配置概述可能不是非常有用，因为它的成本增加一倍，并且一台路由器在大部分时间都处于闲置的状态。然而，我们可以创建两个虚拟路由器进行负载分担来避免这个问题。详情请参考配置举例中的 8.3.2。

说明

VRRP 不支持 MD5 验证。

8.2 配置 VRRP

8.2.1 创建虚拟路由器组

在同一个虚拟路由器组内的路由器，必须配置相同的虚拟路由器组标识符。在使用 **no** 命令退出指定的虚拟路由器之前，必须先 disable VRRP，使其处于 init 状态。

表8-1 创建虚拟路由器组

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# router vrrp 1	创建虚拟路由器组 1 并进入其配置模式	VRRP 组标识符的取值范围为 1~255
Switch(config-router)# exit	退出路由配置模式	-

8.2.2 配置虚拟 IP 地址

表8-2 创建虚拟IP地址

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# router vrrp 1	创建虚拟路由器组 1 并进入其配置模式	VRRP 组标识符的取值范围为 1~255
Switch(config-router)#virtual-ip 10.0.1.20	配置虚拟 IP 地址	VRRP 组中的所有路由器都必须与这个虚拟路由器使用相同的主网络地址

8.2.3 配置端口启用 VRRP

表8-3 配置端口启用VRRP

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# router vrrp 1	创建虚拟路由器组 1 并进入其配置模式	VRRP 组标识符的取值范围为 1~255
Switch(config-router)# interface eth-0-1	设置在端口 eth-0-1 上启动 VRRP	在同一个接口上，启用 VRRP 的数量不要超过 3 个

8.2.4 开启/关闭 VRRP

表8-4 开启/关闭VRRP

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# router vrrp 1	创建虚拟路由器组 1 并进入其配置模式	VRRP 组标识符的取值范围为 1~255
Switch(config-router)# enable	开启 VRRP 功能	-
Switch(config-router)# disable	关闭 VRRP 功能	

8.3 配置举例

8.3.1 配置一个虚拟路由器

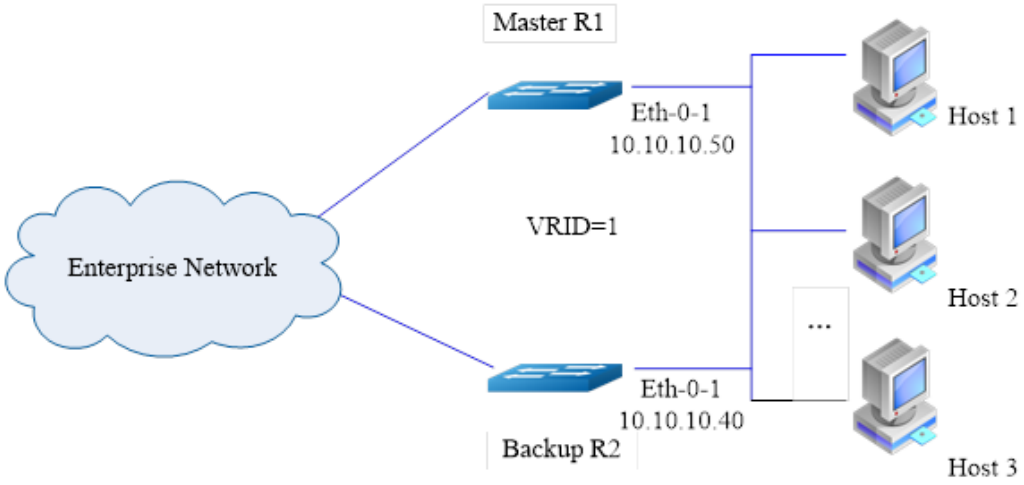
i. 介绍

主备备份方式表示业务仅由 Master 路由器承担。当 Master 路由器出现故障时，才会从其他 Backup 路由器选举出一个接替工作。主备备份方式仅需要一个备份组，不同路由器在该备份组中拥有不同优先级，优先级最高的路由器将成为 Master 路由器。

如图 8-1所示，所有的终端主机将虚拟路由器 1 作为其默认网关。路由器 R1 和 R2 都运行了 VRRP 协议。R1 配置为虚拟路由器 1（VRID = 1）的主路由器，R2 作为虚拟路由器 1 的备份路由器。如果 R1 出现问题，R2 将接管转发，并为主机提供不间断的服务。这样的配置只有一个虚拟路由器，R2 被闲置。

ii. 拓扑

图 8-1 配置单虚拟路由



iii. 配置方法

配置 R1 为虚拟路由器 1 的主路由器，R2 为虚拟路由器 1 的备份路由器。

R1：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# no switchport	设置端口为三层接口
Switch(config-if)# ip address 10.10.10.50/24	设置 IP 地址
Switch(config-if)# exit	退出接口配置模式
Switch(config)# router vrrp 1	创建虚拟路由器组 1
Switch(config-router)# virtual-ip 10.10.10.50	设置虚拟 IP 地址
Switch(config-router)# interface eth-0-1	配置 VRRP 组的应用端口
Switch(config-router)# preempt-mode true	设置抢占模式
Switch(config-router)# advertisement-interval 5	配置通告时间间隔
Switch (config-router)# bfd 10.10.10.40	配置 BFD 会话
Switch(config-router)# enable	使能 VRRP 组 1

R2：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# no switchport	设置端口为三层接口
Switch(config-if)# ip address 10.10.10.40/24	设置 IP 地址
Switch(config-if)# exit	退出接口配置模式
Switch(config)# router vrrp 1	创建 VRRP 虚拟路由器组 1
Switch(config-router)# virtual-ip 10.10.10.50	设置虚拟 IP 地址
Switch(config-router)# interface eth-0-1	配置 VRRP 组的应用端口
Switch(config-router)# priority 200	配置 VRRP 的优先级
Switch(config-router)# preempt-mode true	设置抢占模式
Switch(config-router)# advertisement-interval 5	配置通告时间间隔
Switch (config-router)# bfd 10.10.10.50	配置 BFD 会话
Switch(config-router)# enable	使能 VRRP 组 1

8.3.2 配置两个虚拟路由器

i. 介绍

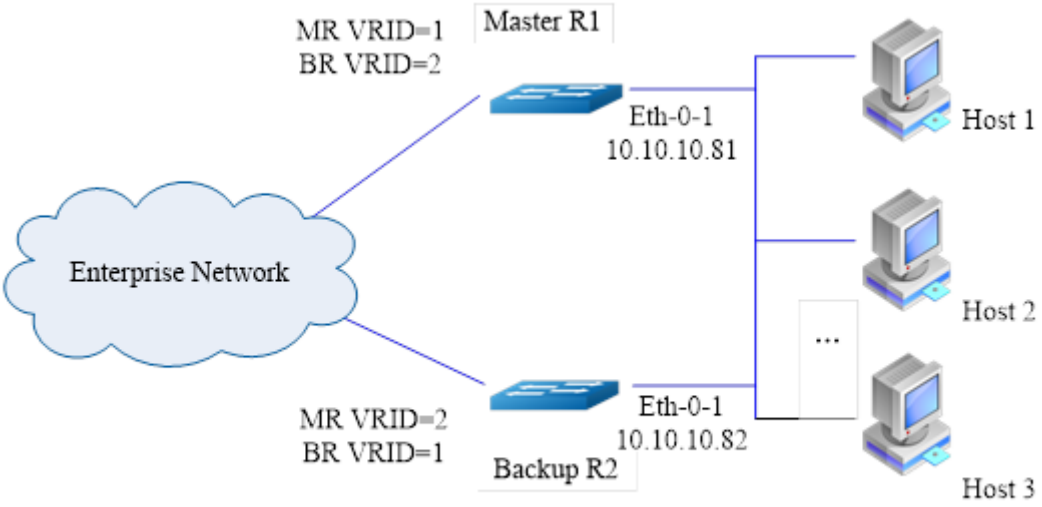
在路由器的一个接口上可以创建多个备份组，使得该路由器可以在一个备份组中作为 Master 路由器，在其他的备份组中作为 Backup 路由器。

负载分担方式是指多台路由器同时承担业务，因此负载分担方式需要两个或者两个以上的备份组，每个备份组都包括一个 Master 路由器和若干个 Backup 路由器，各备份组的 Master 路由器可以各不相同。

下面的例子讲述如何使用两个虚拟路由器进行负载分担。R1 和 R2 各自转发不同的流量，它们之间互为备份，确保流量的负载均衡。

ii. 拓扑

图 8-2 配置两个虚拟路由器



iii. 配置方法

R1：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# no switchport	设置端口为三层接口
Switch(config-if)# ip address 10.10.10.81/24	配置 IP 地址
Switch(config-if)# exit	退出接口配置模式
Switch(config)# router vrrp 1	创建 VRRP 虚拟路由器组 1
Switch(config-router)# virtual-ip 10.10.10.81	设置虚拟 IP 地址
Switch(config-router)# interface eth-0-1	配置 VRRP 组的应用端口
Switch(config-router)# preempt-mode true	设置抢占模式
Switch(config-router)# advertisement-interval 5	配置通告时间间隔为 5 秒

命令举例	操作步骤
Switch(config-router)# enable	使能 VRRP 组 1
Switch(config-router)# exit	退出路由配置模式
Switch(config)# router vrrp 2	创建 VRRP 虚拟路由器组 2
Switch(config-router)# virtual-ip 10.10.10.82	设置虚拟 IP 地址
Switch(config-router)# interface eth-0-1	配置 VRRP 组的应用端口
Switch(config-router)# priority 200	配置 VRRP 的优先级
Switch(config-router)# preempt-mode true	设置抢占模式
Switch(config-router)# advertisement-interval 5	配置通告时间间隔 5 秒
Switch (config-router)# bfd 10.10.10.82	配置 BFD 会话
Switch(config-router)# enable	使能 VRRP 组 2

R2：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# no switchport	设置三层接口
Switch(config-if)# ip address 10.10.10.82/24	配置 IP 地址
Switch(config-if)# exit	退出接口配置模式
Switch(config)# router vrrp 1	创建 VRRP 虚拟路由器组 1
Switch(config-router)# virtual-ip 10.10.10.81	设置虚拟 IP 地址
Switch(config-router)# interface eth-0-1	配置 VRRP 组应用端口
Switch(config-router)# priority 200	设置 VRRP 的优先级
Switch(config-router)# preempt-mode true	设置抢占模式
Switch(config-router)# advertisement-interval 5	配置通告时间间隔 5 秒
Switch(config-router)# enable	使能 VRRP 组 1
Switch(config-router)# exit	退出路由配置模式

命令举例	操作步骤
Switch(config)# router vrrp 2	创建 VRRP 虚拟路由器组 2
Switch(config-router)# virtual-ip 10.10.10.82	设置虚拟 IP 地址
Switch(config-router)# interface eth-0-1	配置 VRRP 组应用端口
Switch(config-router)# preempt-mode true	设置抢占模式
Switch(config-router)# advertisement-interval 5	配置通告时间间隔 5 秒
Switch (config-router)# bfd 10.10.10.81	配置 BFD 会话
Switch(config-router)# enable	使能 VRRP 组 2

8.3.3 配置 VRRP Circuit Failover

i. 介绍

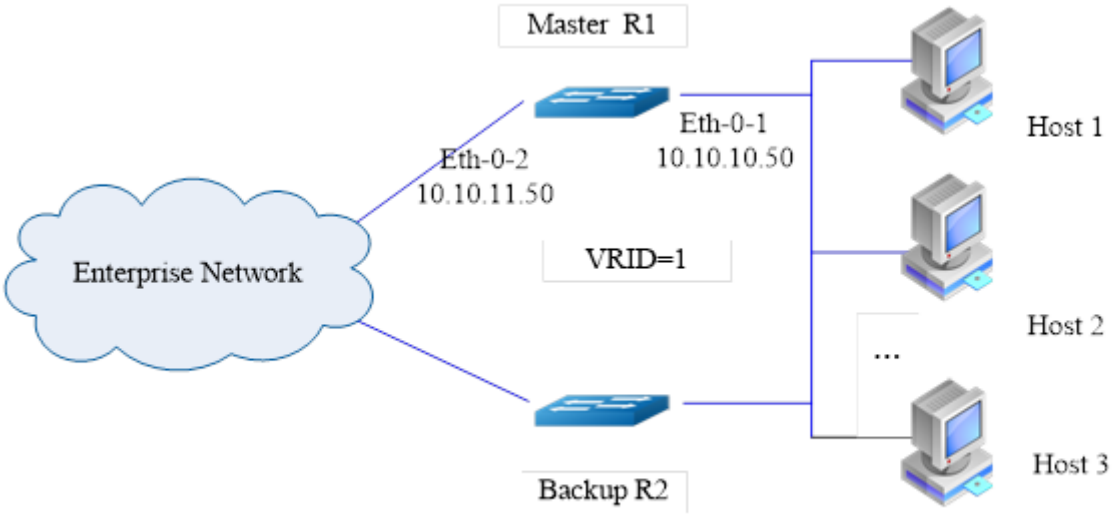
之所以需要 VRRP 链路故障检测功能，是由于 VRRPv2 无法跟踪网关上行链路状态。引入对上行链路的监控可以有效地驱动虚拟路由器的切换，从而避免“黑洞路由”。当主路由器上行接口链路发生故障时，原来的 Master 路由器将切换为 Backup 路由器，而原来的 Backup 路由器将接替成为 Master 路由器。

为了实现 VRRP 链路故障检测功能，我们需要为监视的接口配置一个 priority-delta 值，这个值将被附加到 Master 路由器中，实现 VRRP 路由器从 Master 与 Backup 之间的切换。

在下面的例子中，两个路由器 R1 和 R2 配置了不同的优先级值，priority-delta 的配置要大于 R1 和 R2 优先级之间的差值。R1 配置有一个 100 的优先级，R2 有一个 90 的优先级，由于 R1 优先级较高成为 Master 路由器。priority-delta 值配置为 20，当 R1 的上行接口 eth2 发生故障，R1 的优先级将变为 80（100－20）。此时由于 R2 比 R1 有更大的优先级，R2 则成为 Master 路由器。当 R1 恢复后，R1 优先级为100，重新成为 Master 路由器。

ii. 拓扑

图 8-3 配置 VRRP Circuit Failover 示意图



iii. 配置方法

R1：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# no switchport	设置三层接口
Switch(config-if)# ip address 10.10.10.50/24	配置 IP 地址
Switch(config-if)# exit	退出接口地址
Switch(config)# interface eth-0-2	进入接口配置模式
Switch(config-if)# no switchport	设置三层接口
Switch(config-if)# ip address 10.10.11.50/24	配置 IP 地址
Switch(config-if)# exit	退出接口配置模式
Switch(config)# track 10 interface eth-0-2 linkstate	创建跟踪条件为端口的链路状态
Switch(config)# router vrrp 1	创建 VRRP 组 1

命令举例	操作步骤
Switch(config-router)# virtual-ip 10.10.10.1	指定虚拟 IP 地址
Switch(config-router)# interface eth-0-1	配置 VRRP 组应用端口
Switch(config-router)# preempt-mode true	设置抢占模式
Switch(config-router)# advertisement-interval 5	配置通告时间间隔为 5 秒
Switch(config-router)# priority 100	配置 VRRP 的优先级为 100
Switch(config-router)# track 10 decrement 20	跟踪 track10 并且 priority-delta 值为 20
Switch(config-router)# enable	使能 VRRP 组 1

R2：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# no switchport	设置三层接口
Switch(config-if)# ip address 10.10.10.40/24	配置 IP 地址
Switch(config-if)# exit	退出接口配置模式
Switch(config)# router vrrp 1	创建 VRRP 组 1
Switch(config-router)# virtual-ip 10.10.10.1	设置虚拟 IP 地址
Switch(config-router)# interface eth-0-1	配置 VRRP 组应用端口
Switch(config-router)# preempt-mode true	设置抢占模式
Switch(config-router)# advertisement-interval 5	配置通告时间间隔为 5 秒
Switch(config-router)# priority 90	配置 VRRP 的优先级为 90
Switch(config-router)# enable	使能 VRRP 组 1

8.4 显示 VRRP

命令	操作	说明
show vrrp [*group-id*]	查看 VRRP 协议的配置信息	group-id: VRRP 组编号；如果未指定，则查看所有 VRRP 组配置信息

以 8.3.2 中的配置为例，显示的 VRRP 协议的配置信息如下：

```
Switch# show vrrp 1
VRID <1>
  State                  : Initialize(Interface down)
  Virtual IP             : 10.10.10.81(IP owner)
  Interface              : eth-0-1
  VMAC                   : 0000.5e00.0101
  VRF                    : Default
  Advt timer             : 5 second(s)
  Preempt mode           : TRUE
  Conf pri               : Unset          Run pri     : 255
  Master router ip       : Unknown
  Master priority        : Unknown
  Master advt timer      : Unknown
  Master down timer      : Unknown
  Preempt delay          : 0 second(s)
  Learn master mode      : FALSE
Switch# show vrrp 2
VRID <2>
  State                  : Initialize(Interface down)
  Virtual IP             : 10.10.10.82(Not IP owner)
  Interface              : eth-0-1
  VMAC                   : 0000.5e00.0102
  VRF                    : Default
  Advt timer             : 5 second(s)
  Preempt mode           : TRUE
  Conf pri               : 200            Run pri     : 200
  Master router ip       : Unknown
  Master priority        : Unknown
  Master advt timer      : Unknown
  Master down timer      : Unknown
  Preempt delay          : 0 second(s)
  Learn master mode      : FALSE
```

9 Track 配置

9.1 Track 简介

Track 是一种追踪技术，主要用于在不同模块之间建立关联，如监控模块与应用模块，实现模块间的关联动作。建立的联动充分发挥监控模块的作用，对网络性能进行监测，Track 技术再将监测的结果通知给应用模块，以便应用模块及时作出处理动作。

本章节的内容主要介绍与 Track 联合的配置举例，如配置 IP SLA、创建 Track BFD、VRRP Track 以及静态路由与 Track 的联合应用等。

9.2 配置 Track

9.2.1 启用 IP SLA 监测

表9-1 启用IP SLA监测

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# ip sla monitor 1	创建一个 IP SLA 并进入 IP SLA 配置模式	IP SLA 标识的取值范围为 1~255
Switch(config-ipsla)# exit	退出 IP SLA 配置模式	-
Switch(config)# ip sla monitor schedule 1	启用 IP SLA 监测	IP SLA 标识的取值范围为 1~255

9.2.2 配置 Track 与接口联动

表 9-2 配置 Track 与接口联动

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# track 1 interface eth-0-1 linkstate	在端口 eth-0-1 上创建一个 Track 对象	Track 对象标识的取值范围为 1~500

9.2.3 配置 Track 与 BFD 联动

当 BFD 会话的状态为 up 时，Track 对象处于 up 状态；否则，Track 对象就处于 down 状态。

表9-3 配置Track与BFD联动

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch (config)# interface eth-0-9	进入接口配置模式	-
Switch (config-if)# no switchport	设置端口为三层接口	源端口必须是一个三层接口，且已配置 IP 地址
Switch (config-if)# no shutdown	使能端口	
Switch (config-if)# ip address 9.9.9.1/24	配置 IP 地址	
Switch (config-if)# quit	退出接口配置模式	-
Switch (config)# track 1 bfd source interface eth-0-9 destination 9.9.9.2	创建一个用于 Track BFD 监视条目的 Track 对象	Track 对象标识的取值范围为 1~500；目的 IP 地址必须和源端口的 IP 地址在同一网段内

9.2.4 配置 VRRP 组监视端口

使用 Track 来监视一个处于 up 状态的端口，一般这个端口是报文的上行链路。 当这个端口 down 掉的时候，Master 路由器的优先级将会减少，相应的设置了抢占模式为 TRUE 的 Backup 路由器就可以成为 Master 路由器。因此，递减值的设置一定要大于 Master 和 Backup 路由器的优先级之差。

一个特定的 VRRP 组中只能有一个 Track 对象，后一个配置的 Track 对象总是会将前一个覆盖。

表 9-4 配置 VRRP 组监视端口

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)#track 10 interface eth-0-1 linkstate	在端口 eth-0-1 上创建一个 track 对象	Track 对象标识的取值范围为 1~500
Switch(config)# router vrrp 1	创建 VRRP 条目	VRRP 组标识符的取值范围为 1~255
Switch(config-router)#track 10	配置 VRRP 组的监视端口	跟踪对象 ID 的取值范围为 1~500

9.2.5 配置静态路由与 Track 条目

表9-5 配置静态路由与Track条目

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)#ip route 10.10.10.0/24 192.168.1.11 track 1	配置静态路由并指定 Track 条目	Track 对象标识的取值范围为 1~500；缺省情况下，未配置静态路由
Switch(config)# exit	退出全局配置模式	-

9.3 Track 典型配置举例

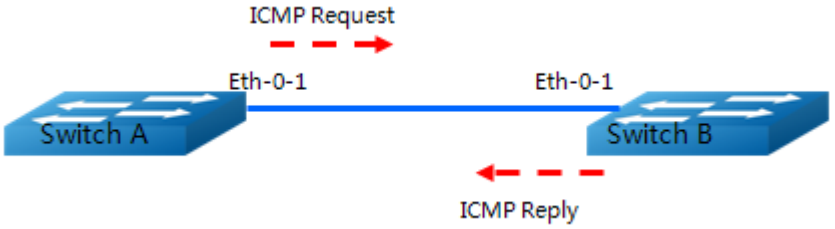
9.3.1 配置 IP SLA 举例

i. 介绍

IP SLA (Service Level Agreement) 是通过“动态监测”的方式对网络性能进行测量和诊断的工具。“动态监测”是指在交换机中，用 ping 的方式来衡量网络是否连通和网络的性能。每一个 IP SLA 均维护其各自操作时生成的一个返回值。这个返回值将会被 tracking 进程所中断。返回值可以是 OK，超过阈值，还有其他返回代码。不同的操作可以有不同的返回值。因此在系统中，只使用操作类型共通的返回值。在 IP SLA 中，我们可以通过使用 ICMP echo 来检查状态或路由的可达性。

ii. 拓扑

图 9-1 IP SLA 拓扑图



iii. 配置方法

1. 配置VRF接口

Switch A:

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# ip vrf vpn1	创建 VRF 条目
Switch(config-vrf)# exit	退出 VRF 模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# ip vrf forwarding vpn1	在接口上启用 VRF 转发表
Switch(config-if)# ip address 192.168.0.2/24	配置 IP 地址
Switch(config)# ip sla monitor 1	创建一个 IP SLA 条目，并进入 IP SLA 配置模式
Switch(config-ipsla)# type icmp-echo 192.168.0.1	定义一个 ICMP 报文的 echo 操作，并输入它的目的 IP 地址
Switch(config-ipsla)# frequency 35	设置发送间隔
Switch(config-ipsla)# timeout 6	设置超时时间
Switch(config-ipsla)# threshold 6000	设置阈值时间
Switch(config-ipsla)# ttl 65	设置 ttl
Switch(config-ipsla)# tos 1	设置 tos

命令举例	操作步骤
Switch(config-ipsla)# data-size 29	设置 data size
Switch(config-ipsla)# data-pattern abababab	设置 data pattern
Switch(config-ipsla)# fail-percent 90	设置 fail 百分比
Switch(config-ipsla)# packets-per-test 4	设置单次检测探针数
Switch(config-ipsla)# interval 9	设置探针之间时间间隔
Switch(config-ipsla)# statistics packet 10	设置 packet 统计数
Switch(config-ipsla)# statistics test 3	设置保存最近几次测试结果
Switch(config-ipsla)# vrf vpn1	应用 VPN1
Switch(config-ipsla)# exit	退出 IP SLA 模式
Switch(config)# ip sla monitor schedule 1	启用 IP SLA 功能
Switch(config)# exit	退出全局配置模式

Switch B:

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# ip vrf vpn1	创建 VRF 条目
Switch(config-vrf)# exit	退出 VRF 模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# ip vrf forwarding vpn1	在接口上启用 VRF 转发表
Switch(config-if)# ip address 192.168.0.1/24	配置 IP 地址

2. 配置三层接口

Switch A:

命令举例	操作步骤
Switch#configure terminal	进入全局配置模式

命令举例	操作步骤
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# ip address 192.168.0.2/24	配置 IP 地址
Switch(config)# ip sla monitor 1	创建一个 IP SLA 条目，并进入 IP SLA 配置模式
Switch(config-ipsla)# type icmp-echo 192.168.0.1	定义一个 ICMP 报文的 echo 操作，并输入它的目的 IP 地址或者主机名
Switch(config-ipsla)#frequency 10	设置发送间隔
Switch(config-ipsla)#timeout 5	设置超时时间
Switch(config-ipsla)#threshold 1	设置阀值时间
Switch(config-ipsla)#exit	退出 IP SLA 模式
Switch(config)# ip sla monitor schedule 1	启用 IP SLA 功能
Switch(config)#exit	退出全局配置模式

Switch B:

命令举例	操作步骤
Switch#configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# ip address 192.168.0.1/24	配置 IP 地址

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# shutdown	打开端口

3. 配置静态路由的端口

Switch A:

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# ip address 192.168.0.2/24	配置 IP 地址
Switch(config)# ip sla monitor 2	创建 SLA 条目
Switch(config-ipsla)# type icmp-echo 1.1.1.1	定义一个 ICMP 报文的 echo 操作，并输入它的目的 IP 地址或者主机名
Switch(config-ipsla)# frequency 10	设置发送间隔
Switch(config-ipsla)# timeout 5	设置超时时间
Switch(config-ipsla)# threshold 1	设置阀值时间
Switch(config-ipsla)# exit	退出 IP SLA 模式
Switch(config)# ip sla monitor schedule 2	启用 IP SLA 功能
Switch(config)# exit	退出全局配置模式

命令举例	操作步骤
Switch#configure terminal	进入全局配置模式
Switch(config)# ip route 1.1.1.1/32 192.168.0.1	配置静态路由

iv. 命令验证

命令	操作	说明
show ip sla monitor [*entry-number*]	显示 IP SLA 监视条目	entry-number: IP SLA 监视条目的标识符，取值范围为 1~255

根据上述的配置方法，显示的结果分别如下：

(1)

```
Switch# show ip sla monitor 1
Entry 1
        Type                        : Echo
        Admin state                 : Disable
```

```
    Destination address    : 192.168.0.1
    Frequency              : 35s
    Timeout                : 6s
    Threshold              : 6000ms
    Interval               : 9s
    Packet per test        : 4
    TTL                    : 65
    TOS                    : 1
    Data Size              : 29 bytes
    Fail Percent           : 90%
    Packet Item Cnt        : 10
    Test Item Cnt          : 3
    Vrf                    : vpn1
    Return code            : Unknown
```

(2)

```
Switch# show ip sla monitor
Entry 1
    Type                   : Echo
    Admin state            : Enable
    Destination address    : 192.168.0.1
    Frequency              : 10 seconds
    Timeout                : 5 seconds
    Threshold              : 5 seconds
    Running Frequency      : 8 seconds
Return code                : OK
Switch# ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=0.846 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=64 time=0.643 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=64 time=0.978 ms
64 bytes from 192.168.0.1: icmp_seq=4 ttl=64 time=0.640 ms
64 bytes from 192.168.0.1: icmp_seq=5 ttl=64 time=0.704 ms
```

```
Switch# show ip sla monitor
Entry 1
    Type                   : Echo
    Admin state            : Enable
    Destination address    : 192.168.0.1
    Frequency              : 10 seconds
    Timeout                : 5 seconds
    Threshold              : 5 seconds
    Running Frequency      : 9 seconds
    Running Timeout        : 4 seconds
    Running Threshold      : 4 seconds
```

```
Return code                    : Timeout
```

(3)

```
Switch# show ip sla monitor 2
Entry 2
    Type                       : Echo
    Admin state                : Enable
    Destination address        : 1.1.1.1
    Frequency                  : 10 seconds
    Timeout                    : 5 seconds
    Threshold                      : 5 seconds
    Running Frequency          : 1 seconds
    Return code                : Unreachable
Switch# ping 1.1.1.1
connect: Network is unreachable
```

```
Switch# ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=64 time=1.03 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=64 time=1.63 ms
64 bytes from 1.1.1.1: icmp_seq=3 ttl=64 time=0.661 ms
64 bytes from 1.1.1.1: icmp_seq=4 ttl=64 time=0.762 ms
64 bytes from 1.1.1.1: icmp_seq=5 ttl=64 time=0.942 ms
Switch# show ip sla monitor 2
Entry 2
    Type                       : Echo
    Admin state                : Enable
    Destination address        : 1.1.1.1
    Frequency                  : 10 seconds
    Timeout                    : 5 seconds
    Threshold                      : 5 seconds
    Running Frequency          : 8 seconds
    Return code                : OK
```

9.3.2 配置 Track 与 IP SLA 联动举例

1. 配置Track

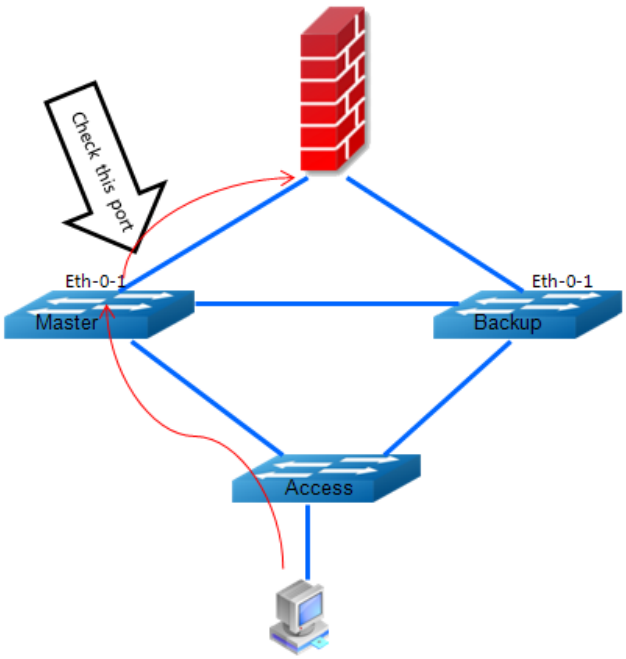
i. 介绍

VRRP 的监视接口功能更好地扩充了备份功能。当备份组中某路由器的接口出现故障时，VRRP 的监

视接口可以提供备份功能；当路由器的其它接口（如连接上行链路的接口）不可用时，它也能提供备份功能。路由器连接上行链路的接口出现故障时，备份组无法感知上行链路的故障，如果该路由器此时处于 Master 状态，将会导致局域网内的主机无法访问外部网络。通过监视指定接口的功能，可以解决该问题。当连接上行链路的接口处于 down 状态时，路由器主动降低自己的优先级，使得备份组内其它路由器的优先级高于这个路由器，以便优先级最高的路由器成为 Master，承担转发任务。

ii. 拓扑

图 9-2 Track 拓扑图



iii. 配置方法

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# track 1 interface eth-0-1 linkstate	创建跟踪的条目
Switch(config-track)# delay up 30	从 Down 到 Up 的时间
Switch(config-track)# delay down 30	从 Up 到 Down 的时间
Switch(config-track)#exit	退出监控模式

命令举例	操作步骤
Switch(config)# exit	退出全局配置模式

iv. 命令验证

命令	操作	说明
show track [*object-id*]	显示 track 对象的信息	object-id: track 对象的标识，取值范围为 1~500

显示 track 对象的信息：

```
Switch#show track

Track 2
        Type                    : Interface Link state
        Interface               : eth-0-1
        State                   : down
        Delay up                : 30 seconds
Delay down                      : 30 seconds
```

2. 配置Track与IP SLA

i. 拓扑

图 9-3 Track Timeout 示意图

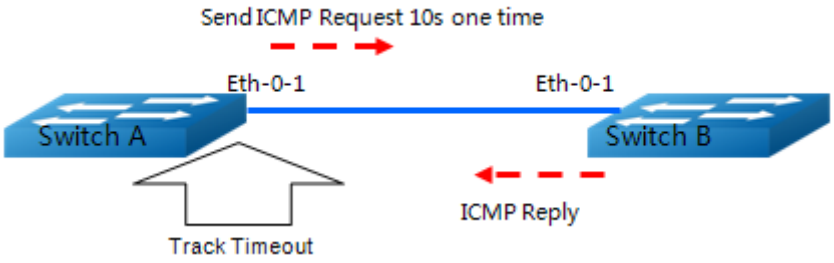
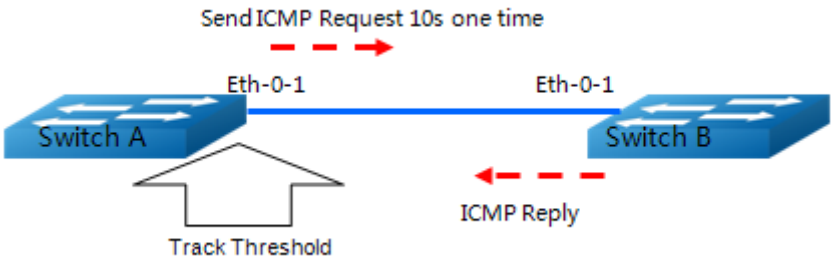


图 9-4 Track Threshold 示意图



ii. 配置方法

a) 配置Track的可达性

Switch A:

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# track 1 rtr 1 reachability	配置 Track 的可达性
Switch(config-track)# delay up 30	从 Down 到 Up 的时间
Switch(config-track)# delay down 30	从 Up 到 Down 的时间
Switch(config-track)#exit	退出监控模式
Switch(config)#exit	退出全局配置模式
Switch#configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# ip address 192.168.0.2/24	配置 IP 地址
Switch(config)# ip sla monitor 1	创建 SLA 的条目
Switch(config-ipsla)# type icmp-echo 192.168.0.1	定义一个 ICMP 报文的 echo 操作，并输入它的目的 IP 地址
Switch(config-ipsla)# frequency 10	设置发送间隔
Switch(config-ipsla)# timeout 5	设置超时时间
Switch(config-ipsla)# threshold 1	设置阀值时间
Switch(config-ipsla)# exit	退出 SLA 模式

命令举例	操作步骤
Switch(config)# ip sla monitor schedule 1	启用 IP SLA 功能
Switch(config)# exit	退出全局配置模式

Switch B:

命令举例	操作步骤
Switch#configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# ip address 192.168.0.1/24	配置 IP 地址

b) 配置Track的状态

Switch A:

命令举例	操作步骤
Switch#configure terminal	进入全局配置模式
Switch(config)# track 1 rtr 1 state	配置 Track 的状态
Switch(config-track)# delay up 30	从 Down 到 Up 的时间
Switch(config-track)# delay down 30	从 Up 到 Down 的时间
Switch(config-track)#exit	退出 Track 模式
Switch(config)#exit	退出全局配置模式
Switch#configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# ip address 192.168.0.2/24	配置 IP 地址
Switch(config)# ip sla monitor 1	创建 IP SLA 的条目
Switch(config-ipsla)# type icmp-echo 192.168.0.1	定义 IP SLA 的协议类型
Switch(config-ipsla)#frequency 10	设置发送间隔
Switch(config-ipsla)#timeout 5	设置超时时间
Switch(config-ipsla)#threshold 1	设置阀值时间

命令举例	操作步骤
Switch(config-ipsla)#exit	退出 IP SLA 模式
Switch(config)# ip sla monitor schedule 1	启用 IP SLA 的监控
Switch(config)#exit	退出全局配置模式

Switch B:

命令举例	操作步骤
Switch#configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# ip address 192.168.0.1/24	配置 IP 地址

iii. 命令验证

命令	操作	说明
show track [*object-id*]	显示 track 对象信息	object-id: track 对象的标识，取值范围为 1~500

a)

```
Switch#show track
Track 1
    Type                    : Response Time Reporter(RTR) Reachability
    RTR entry number        : 1
    State                   : up
    Delay up                : 30 seconds
Delay down                  : 30 seconds
```

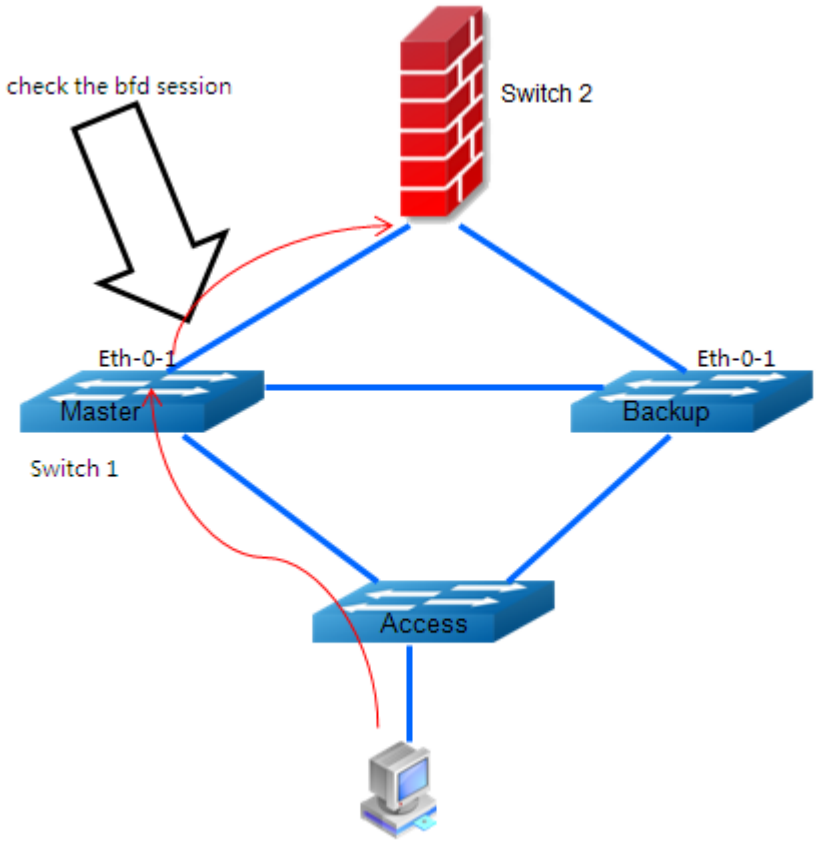
b)

```
Switch# show track
Track 1
    Type                    : Response Time Reporter(RTR) State
    RTR entry number        : 1
    State                   : up
    Delay up                : 30 seconds
Delay down                  : 30 seconds
```

9.3.3 配置 Track BFD 举例

i. 拓扑

图 9-5 Track BFD 示意图



ii. 配置方法

Switch 1:

命令举例	操作步骤
Switch1# configure terminal	进入全局配置模式
Switch1(config)# interface eth-0-1	进入接口配置模式
Switch1(config-if)# no switchport	设置端口为三层接口

命令举例	操作步骤
Switch1(config-if)# no shutdown	使能端口
Switch1(config-if)# ip address 9.9.9.1/24	配置 IP 地址
Switch1(config-if)# quit	退出接口配置模式
Switch1(config)# track 1 bfd source interface eth-0-1 destination 9.9.9.2	创建 BFD session 的 track 对象
Switch1(config-track)# delay up 30	从 Down 到 Up 的时间
Switch1(config-track)# delay down 30	从 Up 到 Down 的时间
Switch1(config-track)# exit	退出 Track 模式
Switch1(config)# exit	退出全局配置模式

Switch 2:

命令举例	操作步骤
Switch2# configure terminal	进入全局配置模式
Switch2(config)# interface eth-0-1	进入接口配置模式
Switch2(config-if)# no switchport	设置端口为三层接口
Switch2(config-if)# no shutdown	使能端口
Switch2(config-if)# ip address 9.9.9.2/24	配置 IP 地址
Switch2(config-if)# quit	退出接口配置模式
Switch2(config)# track 1 bfd source interface eth-0-1 destination 9.9.9.1	创建 BFD session 的 Track 对象
Switch2(config-track)# delay up 30	从 Down 到 Up 的时间
Switch2(config-track)# delay down 30	从 Up 到 Down 的时间
Switch2(config-track)# exit	退出 Track 模式
Switch2(config)# exit	退出全局配置模式

iii. 命令验证

显示 Switch 1 上的 Track BFD 的配置：

```
Switch1 #show track
Track 1
        Type                    : BFD state
        Source interface        : eth-0-1
        Destination IP          : 9.9.9.2
        BFD Local discr         : 1
        State                   : up
```

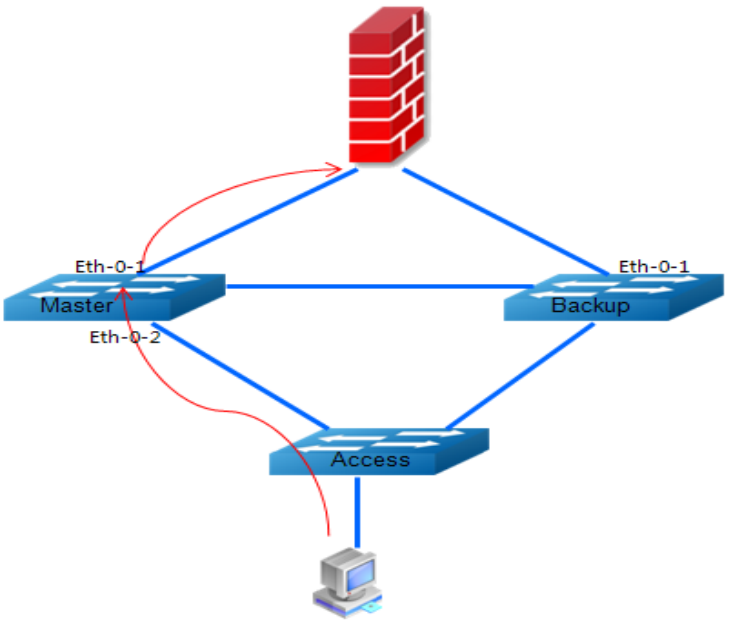
显示 Switch 2 上的 Track BFD 的配置：

```
Switch2 # show track
Track 1
        Type                    : BFD state
        Source interface        : eth-0-1
        Destination IP          : 9.9.9.1
        BFD Local discr         : 1
        State                   : up
```

9.3.4 配置 VRRP Track 举例

i. 拓扑

图 9-6 VRRP Track 示意图



ii. 配置方法

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# track 1 interface eth-0-1 linkstate	配置 Track 条目
Switch(config-track)# exit	退出 Track 模式
Switch(config)# router vrrp 1	创建 VRRP 条目
Switch(config-router)# track 1 decrement 30	设置 VRRP 的规则
Switch(config-router)# exit	退出路由配置模式
Switch(config)# exit	退出全局配置模式

iii. 命令验证

命令	操作	说明
show vrrp [*group-id*]	查看 VRRP 协议的配置信息	VRRP 组编号；如果未指定，则查看所有 VRRP 组配置信息

查看VRRP协议的配置信息：

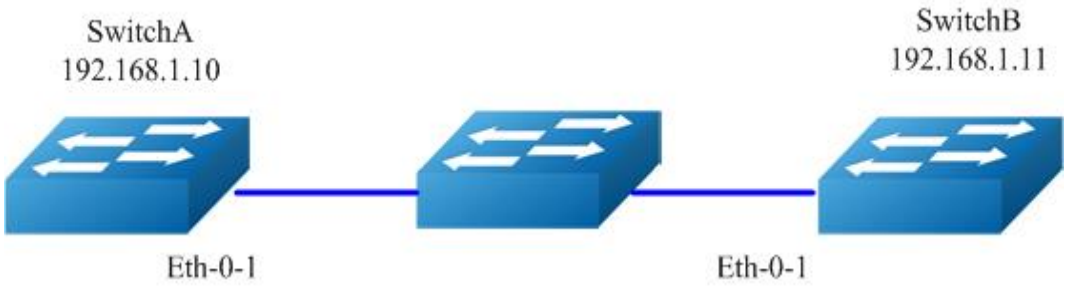
```
Switch# show vrrp
VRID <1>
  State                : Master
  Virtual IP           : 172.16.10.100(Not IP owner)
  Interface            : eth-0-2
  VMAC                       : 0000.5e00.0101
  Advt timer           : 1
  Preempt mode         : TRUE
  Auth type            : NONE
  Conf pri             : Unset              Run pri     : 70
  Track Object         : 1
```

```
Delta pri            : 30
Master router ip     : 172.16.10.1
Master priority      : 70
Master advt timer    : 1
Master down timer    : 4
Learn master mode    : FALSE
```

9.3.5 配置 Track 与静态路由联动举例

i. 拓扑

图 9-7 Track 与静态路由联动配置组网图



ii. 配置方法

Switch A:

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)#interface eth-0-1	进入接口配置模式
Switch(config-if)# no switchport	将端口配置为三层接口
Switch(config-if)# no shutdown	打开端口
Switch(config-if)# ip address 192.168.1.10/24	配置接口 IP 地址
Switch(config-if)# exit	退出接口配置模式
Switch(config)# ip sla monitor 1	创建一条 IP SLA 条目，并进入 IP SLA 配置模式

命令举例	操作步骤
Switch(config-ipsla)# type icmp-echo 192.168.1.11	定义一个 ICMP 报文的 echo 操作，并输入它的目的 IP 地址
Switch(config-ipsla)# exit	退出 IP SLA 配置模式
Switch(config)# ip sla monitor schedule 1	启用 IP SLA 功能
Switch(config)# track 1 rtr 1 reachability	配置 Track 条目，并进入 Track 配置模式
Switch(config-track)# exit	退出 Track 配置模式
Switch(config)#ip route 10.10.10.0/24 192.168.1.11 track 1	配置静态路由并指定 Track 条目
Switch(config)# exit	退出全局配置模式

Switch B:

a)

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# no switchport	将端口配置为三层接口
Switch(config-if)# no shutdown	打开端口
Switch(config-if)# ip address 192.168.1.11/24	配置接口 IP 地址

b)

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# shutdown	关闭端口

iii. 命令验证

a)

```
Switch# show ip sla monitor 1
Entry 1
        Type                        : Echo
        Admin state                 : Enable
        Destination address    : 192.168.1.11
        Frequency                   : 60 seconds
        Timeout                     : 5 seconds
        Threshold                   : 5 seconds
        Running Frequency       : 49 seconds
Return code                 : OK
Switch# show track 1
Track 1
        Type                        : Response Time Reporter(RTR) Reachability
        RTR entry number        : 1
        State                       : up
Switch# show ip route static
S               10.10.10.0/24 [1/0] via 192.168.1.11, eth-0-1
```

b)

```
Switch# show ip sla monitor 1
Entry 1
        Type                        : Echo
        Admin state                 : Enable
        Destination address    : 192.168.1.11
        Frequency                   : 60 seconds
        Timeout                     : 5 seconds
        Threshold                   : 5 seconds
        Running Frequency       : 8 seconds
Return code                 : Timeout
Switch# show track 1
Track 1
        Type                        : Response Time Reporter(RTR) Reachability
        RTR entry number        : 1
        State                       : down
Switch# show ip route static
Switch#
```

10 BFD 配置

10.1 BFD 简介

随着对网络的可靠性要求越来越高，快速寻找、切换到备份链路保证网络通畅也显得越来越重要。但是很多硬件或者软件无法提供这个功能，比如以太网。还有一些无法实现路径检测，比如转发引擎或者接口等，无法实现端到端的检测。

目前的网络一般采用慢 Hello 机制，尤其在路由协议中，在没有硬件帮助下，检测时间会很长。当数据速率越来越大，故障感应时间长代表着大量数据的丢失，并且对于不允许路由协议的节点没有办法检测链路的状态。同时，在现有的 IP 网络中并不具备秒以下的间歇性故障修复功能，而且传统路由架构对实时应用（如语音）进行准确故障检测方面的能力也十分有限。

BFD（双向链路检测），提出了一种轻载的、快速的链路状态检测的解决方案。BFD 能够在系统之间的任何类型通道上进行故障检测，这些通道包括直接的物理链路、虚电路、隧道、MPLS LSP、多跳路由通道，以及非直接的通道。

说明

当物理口上配置了 CFM 的 MEP 并且使能了 LM，同时，IP BFD 配置在 VLAN 接口上且该物理口是 VLAN 接口的成员，则 IP BFD 无法正常工作。当关闭 LM 后，IP BFD 可以正常工作。

10.2 配置 BFD

10.2.1 配置收发包速率及检测倍数

此配置将影响接口上所有的BFD会话。实际的收发包速率需要和会话的对端协商决定。

表 10-1 配置步骤

命令举例	操作	说明
Switch#configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-
Switch (config-if)# bfd interval mintx 3 minrx 3 multiplier 3	配置接口期望的收包速率和发包速率为 3 毫秒，检测间隔倍数为 3	收发包速率的取值范围为 3~1000，单位：毫秒；间隔倍数的取值范围为 2~15。缺省情况下，默认发送速率和接收速率为 20 毫秒；默认检测间隔倍数为 3
Switch(config-if)#end	退出接口配置模式	-

10.2.2 配置 BFD 会话

可以用来配置单跳和多跳 BFD 会话。创建静态单跳/多跳 BFD，如果创建的 BFD 配置参数满足条件，即可以创建 BFD 会话。当不满足条件时，配置保存，但是不会创建 BFD 会话。

表10-2 配置单跳BFD会话

命令	操作	说明
Switch#configure terminal	进入全局配置模式	-
Switch (config)# bfd test peer-ip 9.9.9.2 interface eth-0-9 local 10 remote 20	创建一个名为 test 的单跳 BFD 会话	缺省情况下，系统不会创建单跳 BFD 会话

表10-3 配置多跳BFD会话

命令	操作	说明
Switch#configure terminal	进入全局配置模式	-
Switch (config)# bfd test peer-ip 9.9.9.2 source 10.10.10.1 local 10 remote 20	创建一个名为 test 的多跳 BFD 会话	缺省情况下，系统不会创建多跳 BFD 会话

说明

创建的 BFD 配置参数需满足以下条件：

1. 目的 IP 地址与绑定接口的 IP 地址在同网段内。
2. 若配置 VRF 信息，则 VRF 要与绑定的接口在同一个 VRF 内。若没有配置，则获取接口上的 VRF 信息。
3. 若指定源 IP 地址，则该指定的源 IP 地址为绑定接口上的 IP 地址。若没有配置，则获取与目的 IP 地址同网段的 IP 地址。
4. 若指定本地和源端标识符，则使用指定的标识符。若没有指定，系统会自动分配本地标识符。

10.2.3 配置 BFD 与 OSPF 联动

配置本命令可以在接口上使能 BFD 和 OSPF 联动。当 OSPF 邻居建立时，并且状态达到 two-way 以后（不包含 two-way），系统会建立 BFD 会话。当删除 OSPF 邻居或者状态回到 two-way 及以前（包含 two-way），会删除 BFD 会话。

表10-4 配置BFD与OSPF联动

命令举例	操作	说明
Switch#configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-
Switch (config-if)# ip ospf bfd	接口上使能 BFD 和 OSPF 联动	缺省情况下，去使能 BFD 和 OSPF 的联动功能

10.2.4 配置 BFD 与 VRRP 联动

此命令可以在单个 VRRP 实例中使能 BFD，BFD 会话在两端 VRRP 接口都配置了虚拟 IP 以后开始建立。如果链路断开或者 VRRP 配置被删掉，BFD 会话也会被删掉。

表10-5 配置BFD与VRRP联动

命令举例	操作	说明
Switch#configure terminal	进入全局配置模式	-
Switch(config)#router vrrp 1	创建虚拟路由器组 1	-
Switch(config-router)#virtual-ip 11.11.11.100	设置虚拟 IP 地址	-
Switch(config-router)#interface eth-0-11	配置 VRRP 组的应用端口	-

命令举例	操作	说明
Switch(config-router)# bfd 11.11.11.2	配置 BFD 与 VRRP 联动	缺省情况下，去使能 BFD 和 VRRP 的联动功能

10.3 BFD 典型配置举例

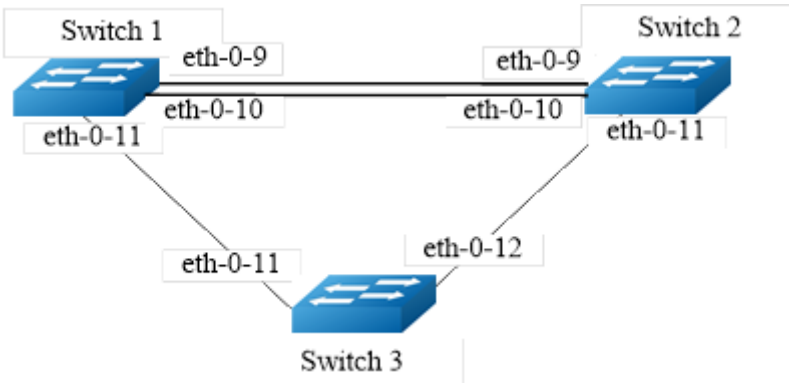
10.3.1 配置 BFD 单跳会话

i. 介绍

如图 10-1 所示，这个拓扑包含 3 条 BFD 会话，其中一条基于静态配置且绑定静态路由，一条基于 OSPF，一条基于 BFD 与 VRRP 联动。

ii. 拓扑

图 10-1 BFD 单跳会话基本配置拓扑图



iii. 配置方法

Switch 1、Switch 2、Switch 3 的配置如下表所示。

Switch 1：

命令举例	操作步骤
Switch1# configure terminal	进入全局配置模式
Switch1(config)# interface eth-0-9	进入 eth-0-9 接口配置模式
Switch1(config-if)# no switchport	将接口设置为非二层口
Switch1(config-if)# no shutdown	使能接口

命令举例	操作步骤
Switch1(config-if)# ip address 9.9.9.1/24	配置接口 IP 地址
Switch1(config-if)# bfd interval mintx 1 minrx 1 multiplier 3	配置接口的 BFD 收发包速率和检测倍数
Switch1(config-if)# exit	退出接口配置模式
Switch1(config)# interface eth-0-10	进入 eth-0-10 接口配置模式
Switch1(config-if)# no switchport	将接口设置为非二层口
Switch1(config-if)# no shutdown	使能接口
Switch1(config-if)# ip address 10.10.10.1/24	配置接口 IP 地址
Switch1(config-if)# bfd interval mintx 2 minrx 2 multiplier 3	配置接口的 BFD 收发包速率和检测倍数
Switch1(config-if)# ip ospf bfd	使能基于 OSPF 的 BFD
Switch1(config-if)# exit	退出接口配置模式
Switch1(config)# router ospf	进入 OSPF 模式
Switch1(config-router)# network 10.10.10.0/24 area 0	配置 OSPF 网段
Switch1(config-router)# exit	退出 OSPF 模式
Switch1(config)#interface eth-0-11	进入接口配置模式
Switch1(config-if)#no switchport	设置端口为三层接口
Switch1(config-if)#ip address 11.11.11.1/24	设置 IP 地址
Switch1(config-if)#exit	退出接口配置模式
Switch1(config)#router vrrp 1	创建虚拟路由器组 1
Switch1(config-router)#virtual-ip 11.11.11.100	设置虚拟 IP 地址
Switch1(config-router)#interface eth-0-11	配置 VRRP 组的应用端口
Switch1(config-router)# bfd 11.11.11.2	配置 VRRP 和 BFD 联动
Switch1(config-router)# enable	使能 VRRP 组 1
Switch1(config)# bfd test peer-ip 9.9.9.2 interface eth-0-9 auto	创建单跳 BFD 会话
Switch1(config)# ip route 1.1.1.0/24 9.9.9.2 bind bfd test	配置静态路由并绑定 BFD 会话

命令举例	操作步骤
Switch1(config)# end	退出全局配置模式

Switch 2：

命令举例	操作步骤
Switch2# configure terminal	进入全局配置模式
Switch2(config)# interface eth-0-9	进入 eth-0-9 接口配置模式
Switch2(config-if)# no switchport	将接口设置为非二层口
Switch2(config-if)# no shutdown	使能接口
Switch2(config-if)# ip address 9.9.9.2/24	配置接口 IP 地址
Switch2(config-if)# bfd interval mintx 1 minrx 1 multiplier 3	配置接口的 BFD 收发包速率和检测倍数
Switch2(config-if)# exit	退出接口配置模式
Switch2(config)# interface eth-0-10	进入 eth-0-10 接口配置模式
Switch2(config-if)# no switchport	将接口设置为非二层口
Switch2(config-if)# no shutdown	使能接口
Switch2(config-if)# ip address 10.10.10.2/24	配置接口 IP 地址
Switch2(config-if)# bfd interval mintx 2 minrx 2 multiplier 3	配置接口的 BFD 收发包速率和检测倍数
Switch2(config-if)# ip ospf bfd	使能基于 OSPF 的 BFD
Switch2(config-if)# exit	退出接口配置模式
Switch2(config)# router ospf	进入 OSPF 模式
Switch2(config-router)# network 10.10.10.0/24 area 0	配置 OSPF 网段
Switch2(config-router)# exit	退出 OSPF 模式
Switch2(config)#interface eth-0-11	进入接口配置模式
Switch2(config-if)#no switchport	设置端口为三层接口
Switch2(config-if)#ip address 11.11.11.2/24	设置 IP 地址
Switch2(config-if)#exit	退出接口配置模式

命令举例	操作步骤
Switch2(config)#router vrrp 1	创建虚拟路由器组 1
Switch2(config-router)#virtual-ip 11.11.11.100	设置虚拟 IP 地址
Switch2(config-router)#interface eth-0-11	配置 VRRP 组的应用端口
Switch2(config-router)# bfd 11.11.11.1	配置 BFD 会话
Switch2(config-router)# enable	使能 VRRP 组 1
Switch2(config)# bfd test peer-ip 9.9.9.1 interface eth-0-9 auto	创建单跳 BFD 会话
Switch2(config)# ip route 2.2.2.0/24 9.9.9.1 bind bfd test	配置静态路由并绑定 BFD 会话
Switch2(config)# end	退出全局配置模式

Switch 3：

命令举例	操作步骤
Switch3# configure terminal	进入全局配置模式
Switch3(config)# interface eth-0-11	进入 eth-0-11 接口配置模式
Switch3(config-if)# no shutdown	使能接口
Switch3(config-if)#exit	退出接口配置模式
Switch3(config)# interface eth-0-12	进入 eth-0-12 接口配置模式
Switch3(config-if)# no shutdown	使能接口
Switch3(config-if)#exit	退出接口配置模式

iv. 命令验证

可以通过指定源端、目的端IP地址和会话所在的接口过滤显示结果。

命令	操作	说明
show bfd session [**detail**]	显示 BFD 的会话信息	使用关键字“detail”显示详细信息

显示 BFD 的会话信息：

```
Switch# show bfd session
```

```
abbreviation:
LD: local Discriminator.       RD: Discriminator
S: single hop session.       M: multi hop session.
SD: Static Discriminator.    DD: Dynamic Discriminator
A: Admin down.       D:down.       I:init.       U:up.
=====================================================
LD     RD     TYPE ST     UP-Time       Remote-Addr              vrf
1      1      S-DD U      00:01:05      9.9.9.2          default
2      2      S-DD U      00:00:25      10.10.10.2       default
3      3      S-DD U      00:00:25      11.11.11.2       default
Number of Sessions:      3

Switch# show bfd session
abbreviation:
LD: local Discriminator.       RD: Discriminator
S: single hop session.       M: multi hop session.
SD: Static Discriminator.    DD: Dynamic Discriminator
A: Admin down.       D:down.       I:init.       U:up.
=====================================================
LD     RD     TYPE ST     UP-Time       Remote-Addr              vrf
1      1      S-DD        U      00:01:27      9.9.9.1          default
2      2      S-DD        U      00:00:46      10.10.10.1       default
3      3      S-DD        U      00:00:25      11.11.11.3       default
Number of Sessions:      3
```

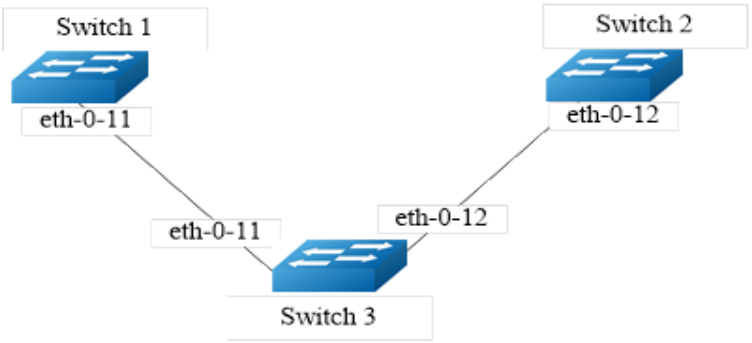
10.3.2 配置 BFD 多跳会话

i. 介绍

这个拓扑包含静态配置的多跳 BFD 会话且绑定静态路由。

ii. 拓扑

图 10-2 BFD 多跳会话基本配置拓扑图



iii. 配置方法

Switch 1、Switch 2、Switch 3 的配置如下表所示。

Switch 1：

命令举例	操作步骤
Switch1# configure terminal	进入全局配置模式
Switch1(config)# interface eth-0-11	进入 eth-0-11 接口配置模式
Switch1(config-if)# no switchport	将接口设置为非二层口
Switch1(config-if)# no shutdown	使能接口
Switch1(config-if)#ip address 11.11.11.1/24	配置接口上的 IP 地址
Switch1(config-if)#exit	退出接口配置模式
Switch1(config)#ip route 12.12.12.2/24 11.11.11.2	配置到达 Switch 3 的静态路由
Switch1(config)# bfd test peer-ip 12.12.12.2/24 source 11.11.11.1 local 10 remote 20	配置静态多跳 BFD 且指定本地标识符
Switch1(config)# ip route 192.168.1.1/24 12.12.12.2 bind bfd test	将 BFD 与某个静态路由绑定

Switch 2：

命令举例	操作步骤
Switch2# configure terminal	进入全局配置模式
Switch2(config)# interface eth-0-11	进入 eth-0-11 接口配置模式
Switch2(config-if)# no switchport	将接口设置为非二层口
Switch2(config-if)# no shutdown	使能接口
Switch2(config-if)#ip address 11.11.11.2/24	配置接口 IP 地址
Switch2(config-if)#exit	退出接口配置模式
Switch2(config)#interface eth-0-12	进入 eth-0-12 接口配置模式
Switch2(config-if)#no switchport	将接口设置为非二层口
Switch2(config-if)#no shutdown	使能接口
Switch2(config-if)#ip address 12.12.12.1/24	配置接口 IP 地址

命令举例	操作步骤
Switch2(config-if)#exit	退出接口配置模式

Switch 3：

命令举例	操作步骤
Switch2# configure terminal	进入全局配置模式
Switch2(config)# interface eth-0-12	进入 eth-0-11 接口配置模式
Switch2(config-if)#no switchport	将接口设置为非二层口
Switch2(config-if)#no shutdown	使能接口
Switch2(config-if)#ip address 12.12.12.2/24	配置接口 IP 地址
Switch2(config-if)#exit	退出接口配置模式
Switch2(config)#ip route 11.11.11.1/24 12.12.12.1	配置到达 Switch 1 的静态路由
Switch2(config)#bfd test peer-ip 11.11.11.1 source-ip 12.12.12.2 local 20 remote 10	配置静态多跳 BFD
Switch2(config)#ip route 2.2.2.2/24 11.11.11.1 bind bfd test	配置静态路由绑定 BFD

iv. 命令验证

显示 BFD 的会话信息：

```
Switch# show bfd session
abbreviation:
LD: local Discriminator.       RD: Discriminator
S: single hop session.       M: multi hop session.
SD: Static Discriminator.    DD: Dynamic Discriminator
A: Admin down.       D:down.       I:init.       U:up.
=====================================================
LD     RD     TYPE ST     UP-Time       Remote-Addr              vrf
10     20     S-SD U      00:01:27      12.12.12.2           default
Switch# show bfd session
abbreviation:
LD: local Discriminator.       RD: Discriminator
S: single hop session.       M: multi hop session.
SD: Static Discriminator.    DD: Dynamic Discriminator
A: Admin down.       D:down.       I:init.       U:up.
=====================================================
```

```
LD     RD     TYPE ST     UP-Time       Remote-Addr          vrf
20     10     S-SD U      00:01:27      11.11.11.1           default
```

11 VARP 配置

11.1 VARP 简介

虚拟 ARP（Virtual-ARP，缩写：VARP）允许多台交换机根据相同的目的 MAC 地址同时转发报文。每台交换机都会配置相同的虚拟 MAC 地址，作为 VLAN 接口上虚拟 IP 地址的对应 MAC 地址。因为虚拟 ARP 在 active-active 模式下工作，并且没有额外的开销，所以在 MLAG 的应用环境中优于 VRRP。

对于虚拟 IP 地址的 ARP 和 GARP 请求，虚拟 ARP 将会使用虚拟 MAC 地址回应。虚拟 MAC 地址只会在入方向的报文里出现，不会在出方向的报文源 IP 字段中出现。

11.2 配置 VARP

11.2.1 配置虚拟 MAC 地址

虚拟 MAC 地址为相应的虚拟 IP 地址提供对应的二层地址。这个地址只有在接收报文的时候使用，对于交换机发出或转发的普通报文不会使用该地址。对于 ARP 报文，只有在回复虚拟 IP 地址的请求时会使用虚拟 MAC 地址。

表11-1 配置虚拟MAC地址

命令	操作	说明
ip virtual-router mac *mac-address*	配置虚拟 MAC 地址	mac-address:虚拟 MAC 地址
no ip virtual-router mac	使用 **no** 命令配置为默认值	-

11.2.2 配置虚拟 IP 地址

本命令配置端口上的虚拟 IP 地址。该虚拟地址需要和端口上的地址在一个网段。如果虚拟 MAC

没有配置，系统不会回复虚拟 IP 地址的 ARP 请求。

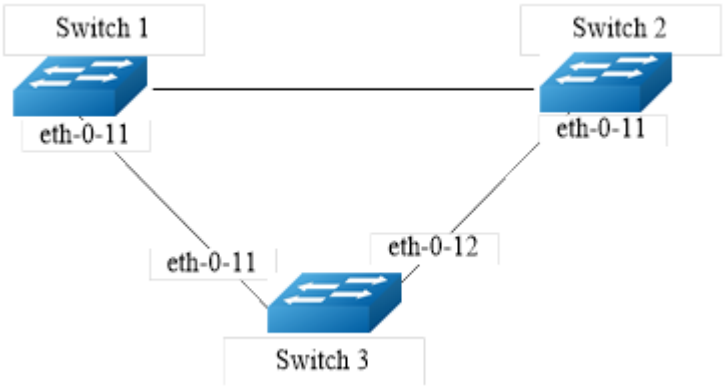
表11-2 配置虚拟IP地址

命令	操作	说明
ip virtual-router address *ip-address*	配置虚拟 IP 地址	ip-address:虚拟 IP 地址
no ip virtual-router address	使用 **no** 命令配置为默认值	-

11.3 VARP 典型配置举例

11.3.1 拓扑

图 11-1 VRRP 配置拓扑图



11.3.2 配置方法

下面以 Switch 1 和 Switch 2 的配置为例。

Switch 1:

命令举例	操作步骤
Switch1# configure terminal	进入全局配置模式
Switch1(config)# ip virtual-router mac a.a.a	配置虚拟 MAC 地址
Switch1(config)# vlan database	进入 VLAN 配置模式
Switch1(config-vlan)# vlan 2	创建 VLAN 2

命令举例	操作步骤
Switch1(config-vlan)# exit	退出 VLAN 配置模式
Switch1(config)# interface eth-0-11	进入 eth-0-11 的接口配置模式
Switch1(config-if)# switchport access vlan 2	将接口加入 VLAN 2
Switch1(config-if)# no shutdown	使能接口
Switch1(config-if)# interface vlan 2	进入 VLAN 2 的接口配置模式
Switch1(config-if)# ip address 10.10.10.1/24	配置 IP 地址
Switch1(config-if)# ip virtual-router address 10.10.10.254	配置虚拟 IP 地址
Switch1(config-if)# end	退出接口配置模式

Switch 2:

命令举例	操作步骤
Switch2# configure terminal	进入全局配置模式
Switch2(config)# ip virtual-router mac a.a.a	配置虚拟 MAC 地址
Switch2(config)# vlan database	进入 VLAN 配置模式
Switch2(config-vlan)# vlan 2	创建 VLAN 2
Switch2(config-vlan)# exit	退出 VLAN 配置模式
Switch2(config)# interface eth-0-11	进入 eth-0-11 的接口配置模式
Switch2(config-if)# switchport access vlan 2	将接口加入 VLAN 2
Switch2(config-if)# no shutdown	使能接口
Switch2(config-if)# interface vlan 2	进入 VLAN 2 的接口配置模式
Switch2(config-if)# ip address 10.10.10.2/24	配置 IP 地址
Switch2(config-if)# ip virtual-router address 10.10.10.254	配置虚拟 IP 地址
Switch2(config-if)# end	退出接口配置模式

11.3.3 命令验证

命令	操作	说明
show ip arp	显示所有的 ARP 表项信息	-

查看虚拟 ARP 表项信息：

```
Switch1# show ip arp
  Protocol       Address          Age (min)    Hardware Addr      Interface
  Internet       10.10.10.1           -        cef0.12da.8100     vlan2
  Internet       10.10.10.254         -        000a.000a.000a     vlan2
Switch2#    show ip arp
  Protocol       Address          Age (min)    Hardware Addr      Interface
  Internet       10.10.10.2           -        66d1.4c26.e100     vlan2
  Internet       10.10.10.254         -        000a.000a.000a     vlan2
```

安全配置指导目录

1 端口安全配置

1.1 端口安全简介

端口安全功能可以用来限制一个特定接口上的可靠 MAC 地址的数量。该接口将只向前转发源 MAC 地址，匹配这些安全地址的数据包。MAC 地址可以通过手动创建或自动学习的方式获取。MAC 地址的数量达到安全 MAC 地址数量的限制后，新的 MAC 地址在接口上不能学到。如果接口又接收到新的数据包，且数据包源 MAC 地址与任何安全地址都不相同，则视为违反端口安全。

端口安全将 MAC 地址绑定到端口，如果源 MAC 地址不是这个 MAC 地址表中的该端口的 MAC 地址，从端口进入后则不会被转发。如果安全 MAC 地址在接口上已学习到，但该 MAC 地址又试图从别的接口学习或配置到其它的接口中，这也被认为是违反端口安全。

1.2 安全 MAC 地址

支持三种类型的安全 MAC 地址：

静态安全 MAC 地址：手动配置的 MAC 地址，该配置会存储在交换机 MAC 地址表中，并添加至运行的配置文件中。保存配置后，交换机重启后配置的 MAC 地址不会丢失。

动态安全 MAC 地址：动态学习 MAC 地址，该配置只存储于交换机 MAC 地址表中，且在交换机重启后会自动清除学习到的 MAC 地址。

粘滞安全 MAC 地址：将动态学习到的 MAC 地址变成“粘滞状态”，形成静态地址表项。该配置存储于运行的配置文件中。

1.3 违反端口安全的处理

如果违反端口安全，需要转发的数据包将被丢弃。违反 MAC 安全采取的措施有三种：

保护（protect）：当 MAC 地址的数量达到安全 MAC 地址数量的限制时，丢弃带有未知源地址报文。

限制（restrict）：当 MAC 地址的数量达到安全 MAC 地址数量的限制时，丢弃带有未知源地址报文，且记录到日志中。

错误禁用（errdisable）：接口立即变为 errdisable 状态，丢弃报文并记录到日志中。

说明

如果安全端口处于 errdisable 状态，可以手动输入 **shutdown** 命令，再运行 **no shutdown** 命令即可恢复接口的状态。

1.4 配置端口安全功能

1.4.1 启用/关闭端口安全

表1-1 启用端口安全

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-
Switch(config-if)# switchport port-security	启用端口安全	缺省情况下，端口安全处于关闭状态

表1-2 关闭端口安全

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-
Switch(config-if)# no switchport port-security	关闭端口安全	缺省情况下，端口安全处于关闭状态；当关闭端口安全功能时，所有动态学习的安全 MAC 地址将被清除。静态的 MAC 地址不会被清除，但将被配置为无效。

1.4.2 配置端口允许的安全 MAC 地址最大值

如果新配置的安全MAC地址的最大值小于已存在的安全MAC地址的条数，则不允许修改；如果端口上的安全MAC地址达到最大值，不会在端口上学到更多的MAC地址。

为了保证端口的动态学习MAC地址安全，配置允许端口上的安全MAC地址的最大值为0，这样端口就不会学习MAC地址，只允许配置静态安全MAC地址。

表1-3 配置举例

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-
Switch(config-if)# switchport port-security maximum 1024	配置端口上允许的安全 MAC 地址的最大值为 1024	端口上允许的安全 MAC 地址的最大值，取值范围为 0~16384；默认值为 1

1.4.3 配置静态安全地址表项

下表描述了配置静态安全 MAC 地址的方法。由于接口的 up/down，通过动态学习的 MAC 地址构成的安全地址表项会被清除。手工配置比较繁琐，此时使用 sticky 功能可以将动态学习的 MAC 地址“粘滞”，成为静态地址表项。

表 1-4 手动添加静态安全 MAC 地址

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-
Switch(config-if)# switchport port-security mac-address 0.0.1 vlan 1	手动添加静态安全 MAC 地址	MAC 地址所关联的 VLAN ID，取值范围为 1~4094

表 1-5 使用 sticky 功能添加静态安全 MAC 地址

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-
Switch(config-if)# switchport port-security	启用端口安全	缺省情况下，端口安全处于关闭状态

命令举例	操作	说明
Switch(config-if)# switchport port-security sticky	当端口学习到安全 MAC 地址时，自动转变为静态 MAC 地址	缺省情况下，此功能处于关闭状态。使用该命令前，应先在端口上启用端口安全功能
Switch(config-if)# switchport port-security sticky mac-address 1.0.0.1 vlan 1	使用 sticky 功能添加静态安全 MAC 地址	使用该命令前，先在端口上启用 **port-security sticky** 功能

1.4.4 配置违反端口安全的处理动作

违反端口安全时，一般有三种处理动作：protect、restrict 和 errdisable。具体的解释可参考 1.3 **违反端口安全的处理**。下表以 protect 为例。

表 1-6 配置违反端口安全的处理动作

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-
Switch(config-if)# switchport port-security	启用端口安全	缺省情况下，端口安全处于关闭状态
Switch(config-if)# switch port-security violation protect	配置违反端口安全时，采取 protect 措施	缺省情况下，违反端口安全的处理动作为 protect。使用该命令前，先在端口上启用端口安全

1.4.5 显示与维护

表 1-7 显示与维护

命令举例	操作	说明
show port-security address-table [**dynamic** | **static**] [**address** *mac-address* | **interface** *if-name* | **vlan** *vlan-id*]	显示安全 MAC 地址条目	mac-address: 显示特定 MAC 地址的条目； vlan-id: VLAN ID，取值范围为 1~4094

命令举例	操作	说明
show port-security current mac-num interface *if-name*	显示端口上现有的安全 MAC 地址条数	-
show port-security [**interface** *if-name*]	显示全部或特定端口上的端口安全信息	-
show port-security maximum mac-num interface *if-name*	显示端口上允许配置的安全 MAC 地址的最大值	-
clear port-security address-table static [**address** *mac-address* | **interface** *if-name* | **vlan** *vlan-id*]	清除静态的安全 MAC 地址	mac-address: 显示特定 MAC 地址的条目； vlan-id: VLAN ID，取值范围为 1~4094

1.5 配置举例

1.5.1 配置方法

按下列步骤配置端口安全：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# switchport	设置端口为二层端口
Switch(config-if)# switchport port-security	启用端口安全功能
Switch(config-if)# switchport port-security maximum 3	配置端口上允许的安全 MAC 地址的最大值
Switch(config-if)# switchport port-security mac-address 0000.1111.2222 vlan 1	绑定 MAC 地址到接口
Switch(config-if)# switchport port-security mac-address 0000.aaaa.bbbb vlan 1	绑定 MAC 地址到接口
Switch(config-if)# switchport port-security violation restrict	设置端口的限制模式
Switch(config-if)# end	退出接口配置模式

1.5.2 查看端口安全信息

根据上述的配置步骤，查看端口安全信息：

```
Switch# show port-security

Secure Port    MaxSecureAddr    CurrentAddr    SecurityViolationMode
                    (Count)          (Count)
-----------------------------------------------------------
   eth-0-1              3                2          restrict
Switch# show port-security address-table
              Secure MAC address table
-----------------------------------------------------------
Vlan       Mac Address           Type                  Ports
----       -----------       -------                -------
1          0000.1111.2222    SecureConfigured       eth-0-1
1          0000.aaaa.bbbb    SecureConfigured       eth-0-1

Switch# show port-security interface eth-0-1

Port security                    : enabled
Violation mode                        : discard packet and log
Maximum MAC addresses                 : 3
Total MAC addresses                   : 2
Static configured MAC addresses  : 2
```

2 VLAN 安全配置

2.1 VLAN 安全简介

VLAN 安全通过限制 VLAN 内 MAC 地址的数量达到保护 VLAN 的目的。MAC 地址可以通过用户手动添加获得，也可以通过自动学习获得。VLAN 内 MAC 地址达到数量限制后，未知源 MAC 地址的报文就会被丢弃（可指定行为）。

系统支持两种类型的 MAC 地址：

- 静态 MAC 地址：手工配置的 MAC 地址
- 动态 MAC 地址：通过动态学习的 MAC 地址

用户可以指定当VLAN内MAC达到限制数量时的如下行为之一：

- discard：进入此 VLAN 的未知源 MAC 的报文将会被丢弃，并且不会进行 FDB 学习
- warn：进入此 VLAN 的未知源 MAC 的报文将会被丢弃，不会进行 FDB 学习，并在 syslog 中打印信息
- forward：进入此 VLAN 的未知源 MAC 的报文将会进行转发，并且不会进行 FDB 学习

系统还支持开、关VLAN内MAC地址学习功能。

2.2 配置 VLAN 安全

2.2.1 配置指定 VLAN 内最大的 FDB 数目

配置该命令前，必须先创建限制 FDB 的 VLAN。如果不使用此命令配置 FDB 限制，VLAN 内的 FDB 数目不受限。

表 2-1 配置指定 VLAN 内最大的 FDB 数目

命令	操作	说明
vlan *vlan-id* **mac-limit maximum** *maximum-number*	配置指定 VLAN 内最大的 FDB 数目	VLAN ID 的取值范围为 1~4094；最大 FDB 数目的

命令	操作	说明
no vlan *VLAN-id* **mac-limit maximum**	取消配置的数目限制	取值范围为 1~65535。缺省情况下，所有 VLAN 内 FDB 数目不受限制

2.2.2 配置 VLAN 内 FDB 数目达到限制的动作

当 VLAN 内 FDB 数目达到限制时，一般有三种处理动作：discard、warn、forward。具体的解释可参考 2.1 VLAN 安全简介。

表 2-2 配置 VLAN 内 FDB 数目达到限制的动作

命令	操作	说明
vlan *vlan-id* **mac-limit action** { **discard** | **warn** | **forward** }	配置 VLAN 内 FDB 数目达到限制时的动作	VLAN ID 的取值范围为 1~4094；缺省情况下，默认动作为 forward。使用此命令前，必须先创建 VLAN
no vlan *vlan-id* **mac-limit action**	使用此命令的 no 形式恢复默认值	

2.2.3 配置 VLAN 内 FDB 的学习功能

表 2-3 配置 VLAN 内 FDB 的学习功能

命令	操作	说明
vlan *vlan-id* **mac learning** { **enable** | **disable** }	配置 VLAN 内 FDB 的学习功能	VLAN ID 的取值范围为 1~4094；缺省情况下，使能所有 VLAN 的 MAC 学习功能。使用此命令前，必须先创建 VLAN

2.2.4 显示与维护

使用此命令可以查看所有 VLAN 的 MAC 地址的学习状态、指定 VLAN 内最大和当前的 FDB 数目、VLAN 内 FDB 数目达到限制的动作等信息。

表 2-4 显示与维护

命令	操作	说明
show vlan-security [**vlan** *vlan-id*]	查看 VLAN 安全的配置	VLAN ID 的取值范围为 1~4094

2.3 配置举例

2.3.1 配置 VLAN MAC 地址限制

通过以下操作配置 VLAN 的 MAC 地址限制功能：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# vlan database	进入 VLAN 配置模式
Switch(config)# vlan 2	创建 VLAN2
Switch(config-vlan)# vlan 2 mac-limit maximum 100	配置 VLAN2 的最大 MAC 地址数量
Switch(config-vlan)# vlan 2 mac-limit action discard	配置 MAC 地址学满后的动作为丢弃
Switch(config-vlan)#end	退出 VLAN 配置模式

2.3.2 配置 VLAN MAC 地址学习

通过以下操作关闭 VLAN 的 MAC 地址学习功能：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# vlan database	进入 VLAN 配置模式
Switch(config)# vlan 2	创建 VLAN2
Switch(config-vlan)# vlan 2 mac learning disable	取消 MAC 地址学习
Switch(config-vlan)#end	退出 VLAN 配置模式

2.3.3 查看配置结果

查看 VLAN 安全的相关配置信息：

```
Switch# show vlan-security
  Vlan   learning-en   max-mac-count   cur-mac-count   action
  ------------------------------------------------------
  2      Disable       100             0               Discard
```

3 Time Range 配置

3.1 Time Range 简介

时间段（Time Range）限定了一个时间范围。这个范围是用于确保某业务在规定时间范围内的有效性。这个时间范围可以分为两种不同的类型：绝对时间范围与周期性时间范围。绝对时间范围即指定某个时间段内的有效范围。周期时间范围即一个周期内某个时间段循环生效的时间范围，以一周为周期进行。

Time Range 本身没有意义，通常被用在基于时间的协议或者应用中，例如 ACL。在实际应用中，它可以表示在这段时间内某些规则或操作有效。Time Range 定义的时间依赖于系统时钟。

3.2 配置时间段

3.2.1 创建/删除时间段

表3-1 创建/删除时间段

命令	操作	说明
time-range *time-range-name*	创建一个时间段，并进入时间段配置模式	time-range-name：定义的名字不超过 40 个字符
no time-range	删除配置的时间段	-

3.2.2 创建绝对时间段

表3-2 创建绝对时间段

命令	操作	说明
absolute start *HH:MM:SS MONTH YEAR* **end** *HH:MM:SS MONTH YEAR*	创建一个绝对时间段	HH:MM:SS：小时:分钟:秒； MONTH：月份，取值范围为 1~31； YEAR：年份，取值范围为

命令	操作	说明
		2000~2037

3.2.3 创建周期时间段

表3-3 创建周期时间段

命令	操作	说明
periodic *HH:MM WEEKDAY* **to** *HH:MM WEEKDAY* **periodic** *HH:MM* { **weekdays** | **weekend** | **daily** } **to** *HH:MM*	创建一个周期时间段	HH:MM：小时:分钟；WEEKDAY：定义一周的周一至周五

3.2.4 显示与维护

表3-4 显示与维护

命令	操作	说明
show time-range [*time-range-name*]	查看时间访问控制列表	如果 ACL 没有在端口上被引用，则不会生效

说明

时间范围的格式均采取 24 小时制。

3.3 配置举例

3.3.1 配置绝对时间段

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# time-range test-absolute	创建一个名为 test-absolute 的时间范围，进入

命令举例	操作步骤
	时间段配置模式
Switch(config-tm-range)# absolute start 01:01:02 jan 01 2012 end 01:01:03 jan 07 2012	定义开始时刻为 2012 年 1 月 1 日 1 时 1 分 2 秒，结束时刻为 2012 年 1 月 7 日 1 时 1 分 3 秒的时间段
Switch(config-tm-range)# end	退出时间段配置模式

3.3.2 配置周期时间段

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# time-range test-periodic	创建一个名为 test-periodic 的时间范围，进入时间段配置模式
Switch(config-tm-range)# periodic 01:01 mon to 01:01 wed	定义开始时间为周一的 1 时 1 分，结束时间为周三的 1 时 1 分的时间段
Switch(config-tm-range)# end	退出时间段配置模式

3.3.3 查看配置结果

显示 Time Range 的配置信息：

```
Switch# show time-range

time-range test-absolute
    absolute start 01:01:02 Jan 01 2012 end 01:01:03 Jan 07 2012
time-range test-periodic
    periodic 01:01 Mon to 01:01 Wed
```

4 ACL 配置

4.1 ACL 简介

ACL（Access Control List，访问控制列表）主要用来实现流识别、访问控制功能。网络设备为了过滤数据包，需要配置一系列的匹配规则，以识别需要过滤的报文。在识别出特定的报文之后，才能根据预先设定的策略允许或禁止相应的数据包通过。ACL 通过一系列的匹配条件对数据包进行分类，这些条件可以是数据包的源地址、目的地址、端口号等。

4.2 术语解释

下面简要介绍用于描述ACL相关的术语和概念。

访问控制条目（ACE）：每一个 ACE 包括一个动作元素（允许或者拒绝）和一个基于标准过滤元素，例如源地址、目的地址、协议、特定协议参数等。

MAC ACL：MAC ACL 可以根据 MAC-SA 和 MAC-DA 过滤报文，MAC 地址可以配置掩码，或者配置为主机 MAC 地址。MAC ACL 也可以根据其他二层字段过滤报文，例如 COS、VLAN-ID、INNER-COS、INNER-VLAN-ID、L2 type、L3 type。

IPv4 ACL：IPv4 ACL 可以根据 IP-SA 和 IP-DA 过滤报文，IP 地址可以配置掩码或者配置为主机 IP 地址。IPv4 ACL 也可以根据其他三层字段过滤报文，例如 DSCP、L4 Protocol 字段以及其他字段（TCP 端口、UDP 端口等）。

时间段：定义一个时间周期，在这个时间段内，ACE 是有效的。

4.3 配置 MAC ACL

下面介绍了 MAC ACL 配置模式及相关功能，用户可以根据实际情况进行配置。如果访问控制列表名称为一个已经存在的名称，则此命令表示进入 MAC 访问控制列表配置模式；如果访问控制列表名称为新名称，则此命令表示创建此列表并进入 MAC 访问控制列表配置模式；此处创建的访问控制列表可以配合 **match access-group** 命令使用，具体见流量管理配置指导章节。

4.3.1 创建/删除 MAC ACL

表4-1 创建MAC ACL

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# mac access-list list_mac_1	创建一个名为 list_mac_1 的 MAC 访问控制列表，并进入 MAC ACL 配置模式	MAC 访问控制列表的名称不超过 40 个字符
Switch(config-mac-acl)# end	退出至 EXEC 模式	-

表4-2 删除MAC ACL

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# no mac access-list list_mac_1	删除一个名为 list_mac_1 的 MAC 访问控制列表	MAC 访问控制列表的名称不超过 40 个字符

4.3.2 配置允许/拒绝源 MAC 地址的报文通过

使用此命令在 MAC 访问控制列表中添加访问控制规则，此规则在 MAC 访问控制列表中的顺序用数字表示;如果没有指定此项,则系统会自动给此规则分配顺序号。它以现有的最大顺序号为基础进行递增，且有固定的增量。比如目前最大的顺序号是 100，则分配的顺序号就为 110（以 10 为增量）。如果当前存在的最大的顺序号加上 10 之后，超过可配顺序号的最大值，则添加失败。指定的 Ether type 在出方向不支持。

表4-3 配置允许源MAC地址的报文通过

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# mac access-list list_mac_1	创建一个名为 list_mac_1 的 MAC 访问控制列表，并进入 MAC ACL 配置模式	MAC 访问控制列表的名称不超过 40 个字符
Switch(config-mac-acl)# 1 permit src-mac host 001A.A02C.A1DF	添加一条规则：允许源 MAC 地址为 001A.A02C.A1DF 的	顺序号的取值范围为 1～131071

命令举例	操作	说明
	报文通过	

表4-4 配置拒绝源MAC地址的报文通过

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# mac access-list list_mac_1	创建一个名为 list_mac_1 的 MAC 访问控制列表并进入配置模式	MAC 访问控制列表名称不超过 40 个字符
Switch(config-mac-acl)# 1 deny src-mac host 001A.A02C.A1DF	添加一条规则：拒绝源 MAC 地址为 001A.A02C.A1DF 的报文通过	顺序号的取值范围为 1～131071

4.3.3 查看 MAC ACL

表4-5 查看MAC ACL

命令	操作	说明
show access-list mac [*acl-name*]	查看 MAC 访问控制列表的内容	acl-name: MAC 访问控制列表名称

4.4 配置 IPv4 ACL

类似地，如果访问控制列表名称为一个已经存在的名称，则此命令表示进入IPv4访问控制列表配置模式；如果访问控制列表名称为新名称，则此命令表示创建此列表并进入IPv4访问控制列表配置模式；此处创建的访问控制列可以配合**match access-group**命令使用，具体见流量管理配置指导章节。

4.4.1 创建/删除 IPv4 ACL

表4-6 创建IPv4 ACL

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-

命令举例	操作	说明
Switch(config)# ip access-list list_ipv4_1	创建一个名为 list_ipv4_1 的 IPv4 访问控制列表并进入配置模式	IPv4 访问控制列表的名称不超过 40 个字符
Switch(config-ip-acl)# end	退出至 EXEC 模式	-

表4-7 删除IPv4 ACL

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# no ip access-list list_ipv4_1	删除一个名为 list_ipv4_1 的 IPv4 访问控制列表	IPv4 访问控制列表的名称不超过 40 个字符

4.4.2 配置允许/拒绝符合规则的 IPv4 报文通过

此处创建的访问控制列表不仅可以匹配报文所使用的协议，而且可以匹配源地址和目的地址；地址掩码中，为1的部分是无关部分，为0的部分是要求严格匹配的部分；使用地址掩码可以指定某一类的IP地址，比如10.10.10.0 0.0.0.255，这个表示地址从10.10.10.0～10.10.10.255的地址都符合要求。

如果顺序号为空，交换机会自动给此规则分配顺序号。它以现有的最大顺序号为基础进行递增，且有固定的增量。比如目前最大的顺序号是 100，则分配的顺序号就为 110（以 10 为增量）。

表4-8 配置允许符合规则的IPv4报文通过

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# ip access-list list_ipv4_1	创建一个名为 list_ipv4_1 的 IPv4 访问控制列表，并进入 IPv4 ACL 配置模式	IPv4 访问控制列表的名称不超过 40 个字符
Switch(config-ip-acl)# 10 permit any any any	添加一条规则：允许使用任何协议的任何报文通过	顺序号的取值范围为 1～131071；第一处”any”是指使用任何协议的 IPv4 报文；第二处”any”是指源地址可以为任何地址的主机；第三处”any”是指目的地址可以为任何地址的主

命令举例	操作	说明
		机

表4-9 配置拒绝符合规则的IPv4报文通过

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# ip access-list list_ipv4_1	创建一个名为 list_ipv4_1 的 IPv4 访问控制列表，并进入 IPv4 ACL 配置模式	IPv4 访问控制列表的名称不超过 40 个字符
Switch(config-ip-acl)# 1 deny any any any	添加一条规则：拒绝使用任何协议的任何报文通过	顺序号的取值范围为 1～131071；第一处”any”是指使用任何协议的 IPv4 报文；第二处”any”是指源地址可以为任何地址的主机；第三处”any”是指目的地址可以为任何地址的主机

4.4.3 查看 IPv4 ACL

表4-10 查看IPv4 ACL

命令	操作	说明
show access-list ip [*acl-name*]	查看 IPv4 访问控制列表的内容	acl-name: IPv4 访问控制列表名称

4.5 配置举例

4.5.1 介绍

在端口 eth-0-1 上应用入方向的 MAC ACL，允许源 MAC 地址为 0000.0000.1111 的报文通过，拒绝其他报文通过。在 eth-0-2 上应用入方向的 IPv4 ACL，允许源 IP 地址为 1.1.1.1/24 的报文通过，拒绝其他报文通过。

4.5.2 配置方法

ACL 配置细则如下表所示：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# mac access-list mac	创建并进入 MAC ACL 配置模式
Switch(config-mac-acl)# permit src-mac host 0000.0000.1111 dest-mac any	添加一条规则：设置允许源 MAC 地址为 0000.0000.1111 帧通过
Switch(config-mac-acl)# deny src-mac any dest-mac any	添加一条规则：设置拒绝任何 MAC 帧通过
Switch(config-mac-acl)# exit	退出 MAC ACL 配置模式
Switch(config)# ip access-list ipv4	创建并进入 IPv4 ACL 配置模式
Switch(config-ip-acl)# permit any 1.1.1.1 0.0.0.255 any	添加一条规则：设置允许源 IP 地址为 1.1.1.1 0.0.0.255 帧通过
Switch(config-ip-acl)# deny any any any	添加一条规则：设置拒绝任何帧通过
Switch(config-ip-acl)# exit	退出 IPv4 ACL 配置模式

接口配置细则如下表所示：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# class-map cmap1	创建分类映射表 cmap1，并且进入分类映射表配置模式
Switch(config-cmap)# match access-group mac	将 MAC ACL 加入 cmap1
Switch(config-cmap)# exit	退出分类映射表配置模式
Switch(config)# policy-map pmap1	创建策略表 pmap1，并且进入策略表配置模式
Switch(config-pmap)# class cmap1	将流分类映射表 cmap1 加入策略映射表 pmap1，并且进入策略表中的分类映射表配置模式
Switch(config-pmap-c)# exit	退出策略表中的分类映射表配置模式

命令举例	操作步骤
Switch(config-pmap)# exit	退出策略表配置模式
Switch(config)# interface eth-0-1	进入应用此 ACL 的接口配置模式
Switch(config-if)# service-policy input pmap1	将策略表 pmap1 应用到接口（该接口应用 MAC ACL）
Switch(config-if)# exit	退出接口配置模式
Switch(config)# class-map cmap2	创建分类映射表 cmap2, 并且进入分类映射表配置模式
Switch(config-cmap)# match access-group ipv4	将 IPv4 ACL 加入 cmap2
Switch(config-cmap)# exit	退出分类映射表配置模式
Switch(config)# policy-map pmap2	创建策略表 pmap2, 并且进入策略表配置模式
Switch(config-pmap)# class cmap2	将流分类映射表 cmap2 加入策略映射表 pmap2, 并且进入策略表中的分类映射表配置模式
Switch(config-pmap-c)# exit	退出策略表中的分类映射表配置模式
Switch(config-pmap)# exit	退出策略表配置模式
Switch(config-if)# interface eth-0-2	进入应用此 ACL 的接口配置模式
Switch(config-if)# service-policy input pmap2	将策略表 pmap2 应用到接口（该接口应用 IPv4 ACL）

4.5.3 命令验证

检查上述配置的结果：

```
Switch# show running-config

mac access-list mac
   10 permit src-mac host 0000.0000.1111 dest-mac any
   20 deny src-mac any dest-mac any
!
ip access-list ipv4
   10 permit any 1.1.1.0 0.0.0.255 any
   20 deny any any any
```

```
!
class-map match-any cmap1
  match access-group mac
!
class-map match-any cmap2
  match access-group ipv4
!
policy-map pmap1
  class cmap1
!
policy-map pmap2
  class cmap2
!
interface eth-0-1
  service-policy input pmap1
!
interface eth-0-2
  service-policy input pmap2
!
```

5 拓展 ACL 配置

5.1 拓展 ACL 简介

ACL 配置可以实现流量过滤，但标准 ACL 的功能十分有限。标准 ACL 在网络层将源 IP 地址的所有流量过滤，无法过滤部分流量。而且只能对数据包的源 IP 地址进行过滤，配置时需要尽可能接近目的地址的接口，但一般来说只有管理员有此操作权限。

扩展 ACL 能解决以上问题，可以在传输层和网络层进行配置，即可以对某种协议进行过滤。而且它能对目的地址进行过滤，降低网络负担；拓展 ACL 也能更加靠近源 IP 地址进行配置，方便管理员更好地规划 ACL 策略。

5.2 术语解释

下面介绍了扩展 ACL 有关的术语和概念。

扩展IPV4 ACL：包含MAC ACE和IP ACE，MAC ACE匹配所有非IPv6和非MPLS报文，IP ACE匹配所有IPv4报文。

MAC ACE：可以根据 MAC-SA 和 MAC-DA 过滤报文，MAC 地址可以配置掩码，或者配置为主机 MAC；也可以根据其他二层字段过滤报文，例如 COS、VLAN-ID、INNER-COS、INNER-VLAN-ID、L2 type、L3 type。

IPv4 ACE：可以根据 IP-SA 和 IP-DA 过滤报文，IP 地址可以配置掩码或者配置为主机 IP 地址；也可以根据其他三层字段过滤报文，例如 DSCP、L4 Protocol 字段以及其他字段（TCP 端口、UDP 端口等等）。

用户可以通过 MAC ACE 和 IP ACE 各种组合、以及不同的顺序实现不同的需求。

5.3 配置拓展 IPv4 ACL

类似地，如果访问控制列表名称为一个已经存在的名称，则此命令表示进入扩展IPv4访问控制列表

配置模式；如果访问控制列表名称为新名称，则此命令表示创建此列表并进入扩展IPv4访问控制列表配置模式。此处创建的访问控制列可以配合**match access-group**命令使用，具体见流量管理配置指导章节。

5.3.1 创建/删除扩展 IPv4 ACL

表5-1 创建拓展IPv4 ACL

命令举例	操作
Switch# configure terminal	进入全局配置模式
Switch(config)# ip access-list list_ipv4_1 extend	创建一个名为 list_ipv4_1 的扩展 IPv4 访问控制列表，并进入拓展 IPv4 ACL 配置模式
Switch(config-ex-ip-acl)# end	退出至 EXEC 模式

表5-2 删除拓展IPv4 ACL

命令举例	操作
Switch# configure terminal	进入全局配置模式
Switch(config)# no ip access-list list_ipv4_1 extend	删除名称为 list_ipv4_1 的扩展 IPv4 访问控制列表

5.3.2 配置允许/拒绝符合规则的 IPv4 报文通过

表5-3 配置允许符合规则的IPv4报文通过

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# ip access-list list_ipv4_1 extend	创建一个名为 list_ipv4_1 的扩展 IPv4 访问控制列表，并进入拓展 IPv4 ACL 配置模式	-
Switch(config-ex-ip-acl)# 10 permit any any any	添加一条规则：允许使用任何协议的任何报文通过	顺序号的取值范围为 1～131071；第一处”any”是指使用任何协议的 IPv4 报文；第二处”any”是指源地址可以为任何地址的主机；第三处”any”是指目的地址可以

命令举例	操作	说明
		为任何地址的主机

表5-4 配置拒绝符合规则的IPv4报文通过

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# ip access-list list_ipv4_1 extend	创建一个名为 list_ipv4_1 的扩展 IPv4 访问控制列表，并进入拓展 IPv4 ACL 配置模式	-
Switch(config-ex-ip-acl)# 1 deny any any any	添加一条规则：拒绝使用任何协议的任何报文通过	顺序号的取值范围为 1～131071；第一处”any”是指使用任何协议的 IPv4 报文；第二处”any”是指源地址可以为任何地址的主机；第三处”any”是指目的地址可以为任何地址的主机

5.3.3 配置允许/拒绝符合规则的 TCP 报文通过

表5-5 配置允许符合规则的TCP报文通过

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# ip access-list list_ipv4_1 extend	创建一个名为 list_ipv4_1 的扩展 IPv4 访问控制列表，并进入拓展 IPv4 ACL 配置模式	-
Switch(config-ex-ip-acl)# 10 permit tcp any any	添加一条规则：允许任何 TCP 报文通过	顺序号的取值范围为 1～131071

表5-6 配置拒绝符合规则的TCP报文通过

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# ip access-list list_ipv4_1 extend	创建一个名为 list_ipv4_1 的扩展 IPv4 访问控制列表，并进入拓展 IPv4 ACL 配置模式	-

Switch(config-ex-ip-acl)# 1 deny tcp any any	添加一条规则:拒绝任何 TCP 报文通过	顺序号的取值范围为 1～131071

5.3.4 查看拓展 IPv4 ACL

表 5-7 查看拓展 IPv4 ACL

命令	操作	说明
show access-list ip [*acl-name* **extend**]	查看拓展 IPv4 访问控制列表的信息	acl-name: 拓展 IPv4 访问控制列表名称

5.4 配置举例

5.4.1 介绍

通过扩展 IPv4 ACL，在端口 eth-0-1 上配置允许源 MAC 地址为 0.0.1111、COS 为 2 的报文通过，允许所有 TCP 的报文通过，禁止其他报文进入系统。

5.4.2 配置方法

拓展 ACL 配置细则：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# ip access-list ipxacl extend	定义一个名称为 ipxacl 的扩展 IPv4 ACL
Switch(config-ex-ip-acl)# permit src-mac host 0000.0000.1111 dest-mac any cos 2	添加一条允许源 MAC 地址为 0.0.1111、COS 为 2 报文的 ACE
Switch(config-ex-ip-acl)# permit tcp any any	添加一条允许 TCP 报文的 ACE
Switch(config-ex-ip-acl)# deny src-mac any dest-mac any	添加一条拒绝所有报文的 ACE
Switch(config-ex-ip-acl)# end	退出至特权模式

接口配置细则：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# class-map cmap	创建分类映射表 cmap，并且进入分类映射表配置模式
Switch(config-cmap)# match access-group ipxacl	将 ipxacl ACL 加入 cmap
Switch(config-cmap)# exit	退出分类映射表配置模式
Switch(config)# policy-map pmap	创建策略表 pmap，并且进入策略表配置模式
Switch(config-pmap)# class cmap	将流分类映射表 cmap 加入策略映射表 pmap，并且进入策略表中的分类映射表配置模式
Switch(config-pmap-c)# exit	退出策略表中的分类映射表配置模式
Switch(config-pmap)# exit	退出策略表配置模式
Switch(config)# interface eth-0-1	进入应用此 ACL 的接口配置模式
Switch(config-if)# service-policy input pmap	将策略表 pmap 应用到接口（该接口应用 IPv4 ACL）
Switch(config-if)# exit	退出接口配置模式

5.4.3 命令验证

查看上述的配置结果：

```
Switch# show running-config

ip access-list ipxacl extend
    10 permit src-mac host 0000.0000.1111 dest-mac any cos 2
    20 permit tcp any any
    30 deny src-mac any dest-mac any
!
class-map match-any cmap
  match access-group ipxacl
!
policy-map pmap
  class cmap
!
interface eth-0-1
  service-policy input pmap
!
Switch# show access-list ip
ip access-list ipxacl extend
    10 permit src-mac host 0000.0000.1111 dest-mac any cos 2
    20 permit tcp any any
    30 deny src-mac any dest-mac any
```

6 ACLv6 配置

6.1 ACLv6 简介

ACL 通过一系列的匹配条件对数据包进行分类，这些条件可以是数据包的源地址、目的地址、端口号等。ACLv6 支持 IPv6 协议，主要用来实现 IPv6 流识别、访问控制功能。网络设备为了过滤数据包，需要配置一系列的匹配规则，以识别需要过滤的报文。在识别出特定的报文之后，才能根据预先设定的策略允许或禁止相应的数据包通过。

6.2 术语解释

下面简要介绍用于描述 ACLv6 相关的术语和概念。

访问控制条目（ACE）：每一个 ACE 包括一个动作元素（允许或者拒绝）和一个基于标准过滤元素，例如源地址、目的地址、协议、特定协议参数等。

IPv6 ACL：IPv6 ACL 可以使用报文的源 IPv6 地址、目的 IPv6 地址过滤报文，支持特定协议的过滤，例如 ICMPv6 协议的类型，以及其他协议（TCP 端口、UDP 端口等）

时间段：定义一个时间周期，在这个时间段内，ACE是有效的。

说明

在全局启用 IPv6 后，IPv6 报文将不被 MAC ACL 所影响。

6.3 配置 IPv6 ACL

如果访问控制列表名称为一个已经存在的名称，则此命令表示进入IPv6访问控制列表配置模式；如果访问控制列表名称为新名称，则此命令表示创建此列表并进入IPv6访问控制列表配置模式。此处

创建的访问控制列可以配合**match access-group**命令使用，具体见流量管理配置指导章节。

6.3.1 创建/删除 IPv6 ACL

表6-1 创建IPv6 ACL

命令举例	操作
Switch# configure terminal	进入全局配置模式
Switch(config)# ipv6 access-list list_ipv6_1	创建一个名为 list_ipv6_1 的 IPv6 访问控制列表，并进入 IPv6 ACL 配置模式
Switch(config-ipv6-acl)# end	退出至 EXEC 模式

表6-2 删除IPv6 ACL

命令举例	操作
Switch# configure terminal	进入全局配置模式
Switch(config)# no ipv6 access-list list_ipv6_1	删除一个名为 list_ipv6_1 的 IPv6 访问控制列表

6.3.2 配置允许/拒绝符合规则的 IPv6 报文通过

表6-3 配置允许符合规则的IPv6报文通过

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# ipv6 access-list list_ipv6_1	创建一个名为 list_ipv6_1 的 IPv6 访问控制列表，并进入 IPv6 ACL 配置模式	-
Switch(config-ipv6-acl)# 1 permit any any any	添加一条规则：允许使用任何协议的任何报文通过	顺序号的取值范围为 1～131071；第一处”any”是指使用任何协议的 IPv6 报文；第二处”any”是指源地址可以为任何地址的主机；第三处”any”是指目的地址可以为任何地址的主机

表6-4 配置拒绝符合规则的IPv6报文通过

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# ipv6 access-list list_ipv6_1	创建一个名为 list_ipv6_1 的 IPv6 访问控制列表，并进入 IPv6 ACL 配置模式	-
Switch(config-ipv6-acl)# 1 deny any any any	添加一条规则：拒绝使用任何协议的任何报文通过	顺序号的取值范围为 1～131071；第一处”any”是指使用任何协议的 IPv6 报文；第二处”any”是指源地址可以为任何地址的主机；第三处”any”是指目的地址可以为任何地址的主机

6.3.3 查看 IPv6 ACL

表6-5 查看IPv6 ACL

命令	操作	说明
show access-list ipv6 [*acl-name*]	查看 IPv6 访问控制列表的内容	acl-name: IPv6 访问控制列表名称

6.4 配置举例

6.4.1 介绍

在端口eth-0-1上使用 MAC ACL，允许源 MAC 地址为 0000.0000.1111 的非 IPv6 报文通过，拒绝其他非 IPv6 报文通过。在 eth-0-2 使用 IPv6 ACL，允许源 IP 地址为 2001::/64 的报文通过，拒绝其他报文通过。

6.4.2 配置方法

ACLv6 配置细则：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式

命令举例	操作步骤
Switch# ipv6 enable	全局启用 IPv6 功能
Switch(config)# mac access-list mac	创建并进入 MAC ACL 配置模式
Switch(config-mac-acl)# permit src-mac host 0000.0000.1111 dest-mac any	添加一条规则：配置允许目的 MAC 地址为 0000.0000.1111 帧通过
Switch(config-mac-acl)# deny src-mac any dest-mac any	添加一条规则：配置拒绝任何 MAC 帧通过
Switch(config-mac-acl)# exit	退出 MAC ACL 配置模式
Switch(config)# ipv6 access-list ipv6	创建并进入 IPv6 ACL 配置模式
Switch(config-ipv6-acl)# permit any 2001::/64 any	添加一条规则：设置允许源 IPv6 地址为 2001::/64 帧通过
Switch(config-ipv6-acl)# deny any any any	添加一条规则：设置拒绝任何帧通过
Switch(config-ipv6-acl)# exit	退出 IPv6 ACL 配置模式

接口配置细则：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# class-map cmap1	创建分类映射表 cmap1，并且进入分类映射表配置模式
Switch(config-cmap)# match access-group mac	将 MAC ACL 加入 cmap1
Switch(config-cmap)# exit	退出分类映射表配置模式
Switch(config)# policy-map pmap1	创建策略表 pmap1，并且进入策略表配置模式
Switch(config-pmap)# class cmap1	将流分类映射表 cmap1 加入策略映射表 pmap1，并且进入策略表中的分类映射表配置模式
Switch(config-pmap-c)# exit	退出策略表中的分类映射表配置模式
Switch(config-pmap)# exit	退出策略表配置模式
Switch(config)# interface eth-0-1	进入应用此 ACL 的接口配置模式
Switch(config-if)# service-policy input pmap1	将策略表 pmap1 应用到接口（该接口应用

命令举例	操作步骤
	MAC ACL）
Switch(config-if)# exit	退出接口配置模式
Switch(config)# class-map cmap2	创建分类映射表 cmap2，并且进入分类映射表配置模式
Switch(config-cmap)# match access-group ipv6	将 ACL IPv6 加入 cmap2
Switch(config-cmap)# exit	退出分类映射表配置模式
Switch(config)# policy-map pmap2	创建策略表 pmap2，并且进入策略表配置模式
Switch(config-pmap)# class cmap2	将流分类映射表 cmap2 加入策略映射表 pmap2，并且进入策略表中的分类映射表配置模式
Switch(config-pmap-c)# exit	退出策略表中的分类映射表配置模式
Switch(config-pmap)# exit	退出策略表配置模式
Switch(config-if)# interface eth-0-2	进入应用此 ACL 的接口配置模式
Switch(config-if)# service-policy input pmap2	将策略表 pmap2 应用到接口（该接口应用的 IPv6 ACL）

6.4.3 命令验证

查看上述的配置结果：

```
Switch# show running-config

mac access-list mac
   10 permit src-mac host 0000.0000.1111 dest-mac any
   20 deny src-mac any dest-mac any
!
ipv6 access-list ipv6
   10 permit any 2001::/64 any
   20 deny any any any
!
class-map match-any cmap1
  match access-group mac
!
class-map match-any cmap2
```

```
  match access-group ipv4
!
policy-map pmap1
  class cmap1
!
policy-map pmap2
  class cmap2
!
interface eth-0-1
  service-policy input pmap1
!
interface eth-0-2
  service-policy input pmap2
!
```

7 Dot1x 配置

7.1 Dot1x 简介

IEEE 802 网络在实际部署中，不可避免的会出现未经授权的设备在物理上接入到网络中。

802.1x 协议提供一种基于端口的网络接入控制协议（Port Based Network Access Control Protocol）。“基于端口的网络接入控制”是指在局域网接入设备的端口对所接入的用户设备进行的认证和控制。如果在端口上连接的用户设备能通过认证，就可以访问局域网中的资源；如果不能通过认证，则无法访问局域网中的资源。

使用 802.1x 的系统为典型的 Client/Server 体系结构，包括三个实体：

客户端：客户端—设备（PC）请求访问 LAN 和交换机服务，响应来自交换机的请求。工作站必须运行符合 802.1x 客户端软件，如 Linux 的 xsupplicant。

认证服务器：执行客户端的实际认证。认证服务器验证客户的身份，并通知交换机客户端是否具有访问 LAN 和交换机服务的权限。由于交换机作为代理，认证服务对客户端是透明的。在此版本中，支持可扩展身份验证协议（EAP）的远程身份验证拨号用户服务，RADIUS 服务器是唯一支持的认证服务器。RADIUS 工作于客户机/服务器模式，服务器和多个 RADIUS 客户端之间交换安全的身份验证信息。

交换机（边缘交换机或无线接入点）：控制基于客户端的认证状态网络的物理访问。交换机作为客户端和认证服务器之间的中介（代理），从客户端请求身份信息，通过认证服务器检查这些信息，并将认证结果返回到客户端。交换机包含 RADIUS 客户端，负责 EAP 帧的封装和解封，以及与认证服务器之间的交互。当交换机收到 EAPOL 帧并中继到身份验证服务器时，以太网报头被剥离，剩下的 EAP 帧则重新封装为 RADIUS 格式。EAP 帧在封装期间不会被修改或审查，并且验证服务器必须支持 EAP 在本机的帧格式。当交换机接收到来自验证服务器的报文时，将服务器的帧头去掉，然后将剩下的 EAP 帧封装为以太网报文格式并发送到客户端。用户还可以在路由端口上配置 dot1x。

7.2 配置 dot1x

7.2.1 全局开启 dot1x 认证功能

表7-1 全局模式下开启dot1x认证功能

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# dot1x system-auth-ctrl	全局开启 dot1x 认证功能	缺省情况下，dot1x 认证功能处于关闭状态

7.2.2 端口开启 dot1x 认证功能

配置此命令在端口上启用 dot1x 认证功能，有三种授权状态供用户选择：auto（设置本端口根据认证结果自动设置端口状态）, force-authorized（强制本端口的状态为已认证）以及 force-unauthorized（强制本端口的状态为未认证）。

表7-2 接口模式下开启dot1x认证功能

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-
Switch(config-if)# dot1x port-control auto	端口开启 dot1x 认证功能	缺省情况下，dot1x 认证功能处于关闭状态；使用本命令前，必须全局使能 dot1x 认证功能

7.2.3 初始化端口的 dot1x 认证状态

使用该命令来初始化一个端口上的 IEEE 802.1x 状态机，这个端口将开始一个全新的认证过程，配置后可以指定端口上的认证状态恢复到未授权状态。

表7-3 端口重启dot1x认证功能

命令举例	操作	说明
Switch# dot1x initialize interface eth-0-1	特权模式下，重启 eth-0-1 的 dot1x 认证	-

7.2.4 查看 dot1x 配置信息

表7-4 查看dot1x配置信息

命令	操作	说明
show dot1x [**interface** *if-name*]	显示 dot1x 的配置信息	-

7.3 配置 Radius 服务器

7.3.1 添加认证服务器

用户可以使用" **radius-server host** "命令添加多个认证服务器。系统会以配置先后顺序依次向这些服务器发起认证请求。如果没有单独为某个服务器指定超时时间、重传次数、密钥等，系统将会使用全局配置的属性。如果指定源接口或者源IP地址，将会使用对应的IP地作为发出报文的源IP地址。

表7-5 添加认证服务器

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# radius-server host 10.10.1.1 key abcde	添加认证服务器，地址为 10.10.1.1，密钥为 abcde	可以为 Radius 服务器配置 IPv4 地址或 IPv6 地址

7.3.2 配置共享密钥

配置该命令可以设置交换机与认证服务器交互的共享密钥。

表7-6 配置共享密匙

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-

命令举例	操作	说明
Switch(config)# radius-server key simple-key	设置交换机与认证服务器交互的共享密钥为“simple-key”	缺省情况下，系统未配置共享密匙；共享密钥长度的取值范围为 1~64

7.4 配置举例

7.4.1 拓扑

图 7-1 Dot1x 基本拓扑图

7.4.2 配置方法

在普通的二层端口上使能dot1x，配置步骤如下表所示。

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# dot1x system-auth-ctrl	全局启用 dot1x 认证控制
Switch(config)# interface eth-0-25	指定要配置的接口，进入接口配置模式
Switch(config)# switchport mode access	设置 eth-0-25 为 access 模式
Switch(config-if)# dot1x port-control auto	在接口上启用 dot1x 端口控制
Switch(config-if)# no shutdown	确定端口使能
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface vlan 1	进入 VLAN 1
Switch(config-if)# ip address 192.168.100.1/24	设置 VLAN 1 的 IP 地址
Switch(config)# interface eth-0-26	进入接口配置模式.

命令举例	操作步骤
Switch(config-if)# no switchport	配置接口为路由端口
Switch(config-if)# ip address 202.38.100.1/24	在此接口上配置 IP 地址
Switch(config-if)# no shutdown	确定端口使能
Switch(config-if)# exit	退出接口配置模式.
Switch(config)# radius-server host 202.38.100.7	为 RADIUS 服务器配置 IPv4 地址
Switch(config)# radius-server host 2001:1000::1	为 RADIUS 服务器配置 IPv6 地址
Switch(config)# radius-server key test	配置 RADIUS 服务器的共享密钥
Switch(config)# end	退出全局配置模式

若要在路由端口上启用 dot1x，交换机配置步骤如下表所示。

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# dot1x system-auth-ctrl	全局使能 dot1x 身份验证控制
Switch(config)# interface eth-0-25	进入接口配置模式
Switch(config-if)# no switchport	配置接口为路由端口
Switch(config-if)# ip address 192.168.100.1/24	在此接口上配置 IP 地址
Switch(config-if)# dot1x port-control auto	在接口上使能 dot1x 端口控制，允许端口访问协商认证
Switch(config-if)# no shutdown	确定端口使能
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface eth-0-26	进入接口配置模式
Switch(config-if)# no switchport	配置接口为路由端口
Switch(config-if)# ip address 202.38.100.1/24	在此接口上配置 IP 地址
Switch(config-if)# no shutdown	确定端口使能
Switch(config-if)# exit	退出接口配置模式
Switch(config)# radius-server host 202.38.100.7	为 RADIUS 服务器配置 IPv4 地址

命令举例	操作步骤
Switch(config)# radius-server host 2001:1000::1	为 RADIUS 服务器配置 IPv6 地址
Switch(config)# radius-server key test	配置 RADIUS 服务器的共享密钥
Switch(config)# end	退出全局配置模式

采用强制授权模式，交换机配置步骤如下表所示。

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# dot1x system-auth-ctrl	全局使能 dot1x 身份验证控制
Switch(config)# interface eth-0-25	进入接口配置模式
Switch(config-if)# dot1x port-control force-authorized	在接口上使能 dot1x 端口控制，强制状态一直被授权
Switch(config-if)# no shutdown	确定端口使能
Switch(config-if)# end	退出接口配置模式

可选参数设置步骤如下表所示。

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# radius-server deadtime 10	设置重新激活 RADIUS 服务器的等待时间
Switch(config)# radius-server retransmit 5	设置 RADIUS 请求发送到服务器的最大可以失败的次数
Switch(config)# radius-server timeout 10	设置 RADIUS 服务器无响应的超时时间
Switch(config)# interface eth-0-25	进入接口配置模式
Switch(config-if)# dot1x max-req 5	未经授权之前，指定重新验证尝试的次数
Switch(config-if)# dot1x protocol-version 1	设置协议版本
Switch(config-if)# dot1x quiet-period 120	在 HELD 状态下的静默时间
Switch(config-if)# dot1x reauthentication	在一个端口上使能重新认证
Switch(config-if)# dot1x timeout re-authperiod 1800	指定重新认证的时间间隔

命令举例	操作步骤
Switch(config-if)# dot1x timeout server-timeout 60	指定认证服务器响应超时时间
Switch(config-if)# dot1x timeout supp-timeout 60	指定客户端响应超时时间
Switch(config-if)# dot1x timeout tx-period 60	指定向客户端请求身份信息的时间间隔

服务器软件设置步骤及参数，详细配置信息参见图 7-2、图 7-3、图 7-4。

图 7-2 选择 Setting-> System

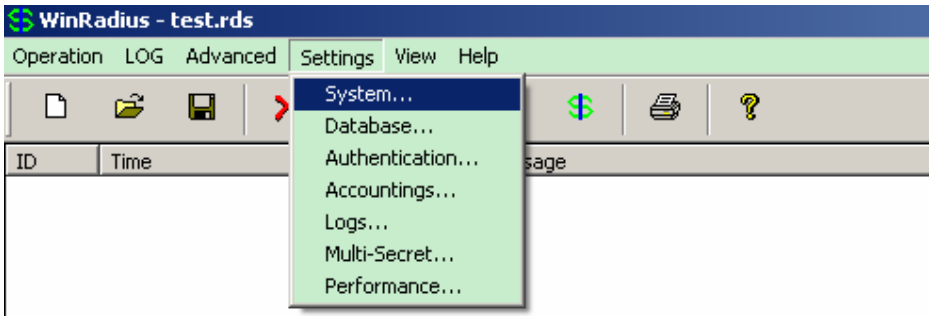


图 7-3 配置 Radius 服务器的密码共享密钥、认证端口和计费端口

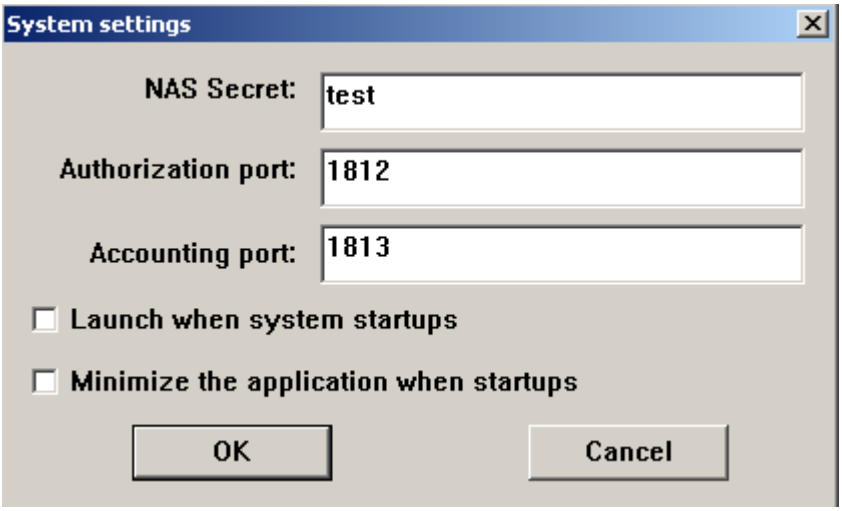
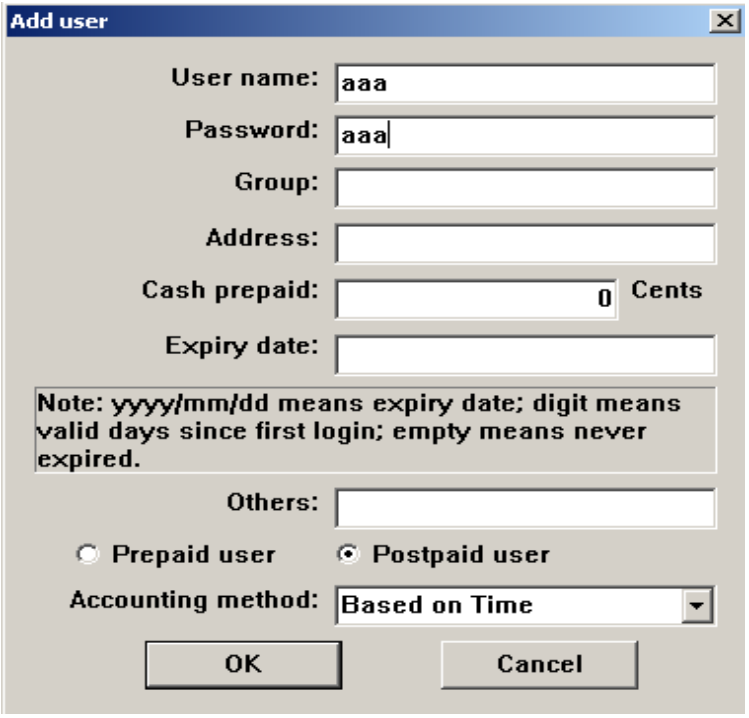


图 7-4 服务器端配置用户名和密码



7.4.3 命令验证

查看上述的配置结果：

```
Switch# show dot1x

802.1X Port-Based Authentication Enabled
   RADIUS server address: 2001:1000::1:1812
   Next radius message ID: 0
   RADIUS server address: 202.38.100.7:1812
   Next radius message ID: 0
Switch# show dot1x interface eth-0-25
802.1X info for interface eth-0-25
   Supplicant name: aaa
   Supplicant address: 0011.11e1.9a3f
   portEnabled: true - portControl: Auto
   portStatus: Authorized - currentId: 42
   reAuthenticate: disabled
   reAuthPeriod: 3600
   abort:F fail:F start:F timeout:F success:T
   PAE: state: Authenticated - portMode: Auto
   PAE: reAuthCount: 0 - rxRespId: 0
   PAE: quietPeriod: 60 - reauthMax: 2 - txPeriod: 30
   BE: state: Idle - reqCount: 0 - idFromServer: 41
```

```
BE: suppTimeout: 30 - serverTimeout: 30
CD: adminControlledDirections: in - operControlledDirections: in
CD: bridgeDetected: false
```

8 Guest VLAN 配置

8.1 Guest VLAN 简介

如果用户因为没有专用的认证客户端或者客户端版本过低等原因，导致无法认证成功，用户所在的端口会被加入Guest VLAN。Guest VLAN 是一个不经认证也可以访问的VLAN。在该VLAN 内，用户可以进行客户端下载以及升级等操作。当用户利用这些资源，安装或者升级了认证客户端后，又可以进行正常的认证过程，从而访问其他的网络资源。开启802.1x 特性、正确配置 Guest VLAN 后，设备会从某一端口发送触发认证报文。

当 EAP-Request/Identity 超过设定的最大次数而没有收到客户端的任何回应报文时，该端口会被加入到Guest VLAN 内。此时用户发起认证，若认证失败，则端口仍然处于Guest VLAN 中；如果认证成功，则端口返回到用户配置的VLAN。

说明

Guest VLAN 的功能只能在 Access 端口上配置，不能在三层物理口(routed port)或者 Trunk 端口上配置。

8.2 配置 Guest VLAN 功能

配置一个 Guest VLAN 后，使能 dot1x 认证的端口，在客户端通过认证之前都属于该VLAN。

表8-1 配置Guest VLAN功能

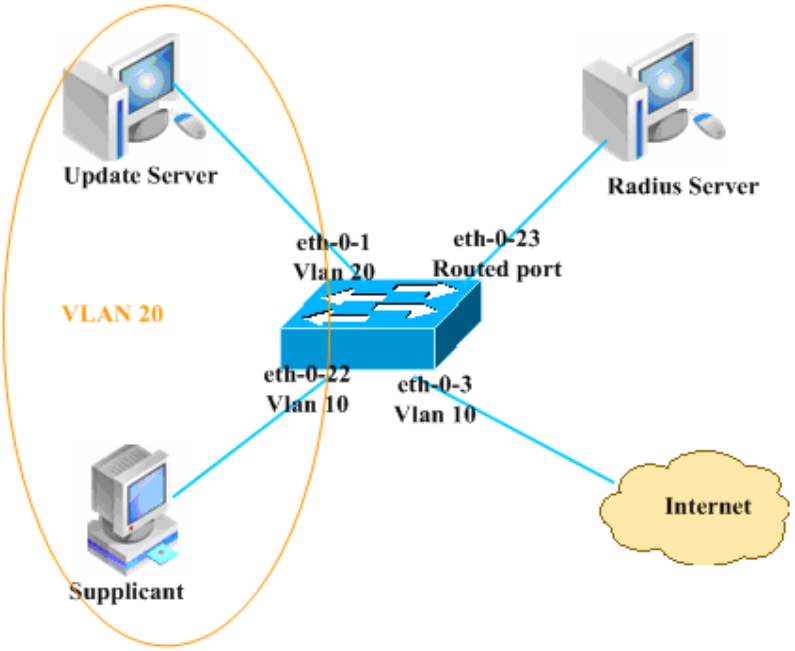
命令	操作	说明
dot1x guest-vlan *vlan-id*	配置 Guest VLAN 功能	dot1x Guest VLAN，取值范围为 2~4094；缺省情况下，系统没有配置 Guest VLAN

8.3 配置举例

8.3.1 拓扑

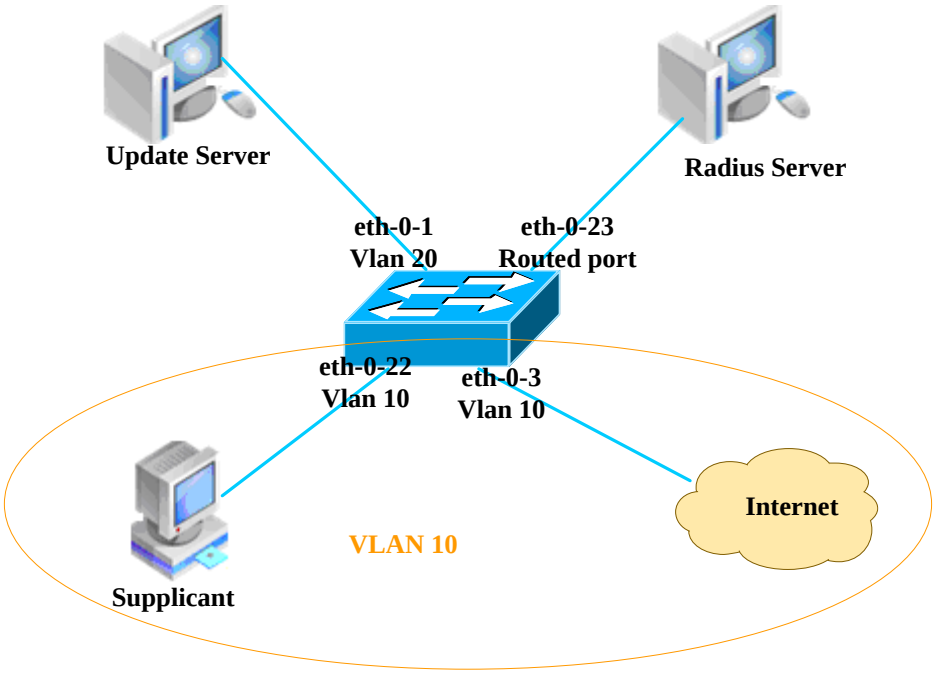
如图 8-1 所示，eth-0-22 是一个使能了 802.1x 功能的端口，它处于 VLAN 10 内。Update server 是用于客户端下载和升级的服务器，处于 VLAN 20 内。在 eth-0-22 上使能 Guest VLAN 特性，当设备从端口触发认证报文超过设定的最大次数而没有收到任何回应报文后，端口被加入 Guest VLAN 20 中。此时客户端和 update server 都在 VLAN 20 内，客户端可以访问 update server 并下载 802.1x 客户端。

图 8-1 Guest VLAN 拓扑图



连接认证服务器 Radius server 的上行端口 eth-0-23，使能一个三层物理口，它的 IP 地址为 202.38.100.1，Radius server 的地址为 202.38.100.7。当认证成功之后，端口 eth-0-22 重新处于 VLAN 10 内，客户端即可以访问 Internet，如图 8-2 所示。

图 8-2 Radius 服务器认证成功拓扑图



8.3.2 配置方法

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# vlan database	进入 VLAN 配置模式
Switch(config-vlan)# vlan 10	创建 VLAN 10
Switch(config-vlan)# vlan 20	创建 VLAN 20
Switch(config-vlan)# exit	退出 VLAN 配置模式
Switch(config)# dot1x system-auth-ctrl	全局启用 dot1x 认证控制
Switch(config)# interface eth-0-22	指定要配置的接口，进入接口配置模式
Switch(config-if)# switchport mode access	设置接口为 access 模式
Switch(config-if)# switchport access vlan 10	设置接口允许 VLAN 10 通过
Switch(config-if)# dot1x port-control auto	在接口上使能 dot1x 端口控制，允许端口访问协商认证

命令举例	操作步骤
Switch(config-if)# no shutdown	确定端口使能
Switch(config-if)# dot1x guest vlan 20	配置 Guest VLAN 为 VLAN 20
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface eth-0-23	指定要配置的接口，进入接口配置模式
Switch(config-if)# no switchport	配置接口为路由端口
Switch(config-if)# ip address 202.38.100.1/24	在此接口上配置 IP 地址
Switch(config-if)# no shutdown	确定端口使能
Switch(config-if)# exit	退出接口配置模式
Switch(config)# radius-server host 202.38.100.7	为 RADIUS 服务器配置 IP 地址
Switch(config)# radius-server key test	配置 RADIUS 服务器的共享密钥
Switch(config)#end	退出配置模式

8.3.3 命令验证

i. 配置 Guest VLAN 之前的初始状态如命令 **show running-config** 的屏显内容所示：

```
Switch# show running-config

dot1x system-auth-ctrl
radius-server host 202.38.100.7 key test
vlan database
  vlan 10,20
!
interface eth-0-22
  switchport access vlan 10
  dot1x port-control auto
  dot1x guest-vlan 20
!
interface eth-0-23
  no switchport
  ip address 202.38.100.1/24
!
Switch# show dot1x interface eth-0-22
802.1X info for interface eth-0-22
    portEnabled: true - portControl: Auto
    portStatus: Unauthorized - currentId: 1
```

```
   reAuthenticate: disabled
   reAuthPeriod: 3600
   Guest VLAN:20
   abort:F fail:F start:F timeout:F success:F
   PAE: state: Connecting - portMode: Auto
   PAE: reAuthCount: 1 - rxRespId: 0
   PAE: quietPeriod: 60 - reauthMax: 2 - txPeriod: 30
   BE: state: Idle - reqCount: 0 - idFromServer: 19
   BE: suppTimeout: 30 - serverTimeout: 30
   CD: adminControlledDirections: in - operControlledDirections: in
   CD: bridgeDetected: false
Switch# show vlan brief
VLAN ID  Name                State    STP ID  DSCP      Member ports
                                                       (u)-Untagged, (t)-Tagged
======= ================ ======= ======= ======= ========================
1        default             ACTIVE   0       Disable eth-0-1(u) eth-0-2(u)
                                                      eth-0-3(u) eth-0-4(u)
                                                      eth-0-5(u) eth-0-6(u)
                                                      eth-0-7(u) eth-0-8(u)
                                                      eth-0-9(u) eth-0-10(u)
                                                      eth-0-11(u) eth-0-12(u)
                                                      eth-0-13(u) eth-0-14(u)
                                                      eth-0-15(u) eth-0-16(u)
                                                      eth-0-17(u) eth-0-18(u)
                                                      eth-0-19(u) eth-0-20(u)
                                                      eth-0-21(u) eth-0-24(u)
                                                      eth-0-25(u) eth-0-26(u)
                                                      eth-0-27(u) eth-0-28(u)
                                                      eth-0-29(u) eth-0-30(u)
                                                      eth-0-31(u) eth-0-32(u)
                                                      eth-0-33(u) eth-0-34(u)
                                                      eth-0-35(u) eth-0-36(u)
                                                      eth-0-37(u) eth-0-38(u)
                                                      eth-0-39(u) eth-0-40(u)
                                                      eth-0-41(u) eth-0-42(u)
                                                      eth-0-43(u) eth-0-44(u)
                                                      eth-0-45(u) eth-0-46(u)
                                                      eth-0-47(u) eth-0-48(u)
10       VLAN0010            ACTIVE   0       Disable eth-0-22(u)
20       VLAN0020            ACTIVE   0       Disable
```

ii. Guest VLAN 客户端的状态信息如下面屏幕回显信息所示：

```
Switch# show dot1x interface eth-0-22

802.1X info for interface eth-0-22
   portEnabled: true - portControl: Auto
```

```
   portStatus: Unauthorized - currentId: 2
   reAuthenticate: disabled
   reAuthPeriod: 3600
   Guest VLAN:20(Port Authorized by guest vlan)
   abort:F fail:F start:F timeout:F success:F
   PAE: state: Connecting - portMode: Auto
   PAE: reAuthCount: 2 - rxRespId: 0
   PAE: quietPeriod: 60 - reauthMax: 2 - txPeriod: 30
   BE: state: Idle - reqCount: 0 - idFromServer: 19
   BE: suppTimeout: 30 - serverTimeout: 30
   CD: adminControlledDirections: in - operControlledDirections: in
   CD: bridgeDetected: false
Switch# show vlan brief
VLAN ID  Name                State    STP ID  DSCP    Member ports
                                                     (u)-Untagged, (t)-Tagged
======= ================ ======= ======= ======= ========================
1        default             ACTIVE   0       Disable eth-0-1(u) eth-0-2(u)
                                                     eth-0-3(u) eth-0-4(u)
                                                     eth-0-5(u) eth-0-6(u)
                                                     eth-0-7(u) eth-0-8(u)
                                                     eth-0-9(u) eth-0-10(u)
                                                     eth-0-11(u) eth-0-12(u)
                                                     eth-0-13(u) eth-0-14(u)
                                                     eth-0-15(u) eth-0-16(u)
                                                     eth-0-17(u) eth-0-18(u)
                                                     eth-0-19(u) eth-0-20(u)
                                                     eth-0-21(u) eth-0-24(u)
                                                     eth-0-25(u) eth-0-26(u)
                                                     eth-0-27(u) eth-0-28(u)
                                                     eth-0-29(u) eth-0-30(u)
                                                     eth-0-31(u) eth-0-32(u)
                                                     eth-0-33(u) eth-0-34(u)
                                                     eth-0-35(u) eth-0-36(u)
                                                     eth-0-37(u) eth-0-38(u)
                                                     eth-0-39(u) eth-0-40(u)
                                                     eth-0-41(u) eth-0-42(u)
                                                     eth-0-43(u) eth-0-44(u)
                                                     eth-0-45(u) eth-0-46(u)
                                                     eth-0-47(u) eth-0-48(u)
10       VLAN0010            ACTIVE   0       Disable
20       VLAN0020            ACTIVE   0       Disable eth-0-22(u)
```

iii. Guest VLAN 客户端认证成功后的配置结果如下所示：

```
Switch# show dot1x interface eth-0-22

802.1X info for interface eth-0-22
   Supplicant name: ychen
```

```
    Supplicant address: ae38.3288.f046
    portEnabled: true - portControl: Auto
    portStatus: Authorized - currentId: 6
    reAuthenticate: disabled
    reAuthPeriod: 3600
    Guest VLAN:20
    abort:F fail:F start:F timeout:F success:T
    PAE: state: Authenticated - portMode: Auto
    PAE: reAuthCount: 0 - rxRespId: 0
    PAE: quietPeriod: 60 - reauthMax: 2 - txPeriod: 30
    BE: state: Idle - reqCount: 0 - idFromServer: 5
    BE: suppTimeout: 30 - serverTimeout: 30
    CD: adminControlledDirections: in - operControlledDirections: in
    CD: bridgeDetected: false
Switch# show vlan brief
VLAN ID  Name                State    STP ID  DSCP    Member ports
                                                     (u)-Untagged, (t)-Tagged
======= ================ ======= ======= ======= ========================
1        default             ACTIVE   0       Disable eth-0-1(u) eth-0-2(u)
                                                     eth-0-3(u) eth-0-4(u)
                                                     eth-0-5(u) eth-0-6(u)
                                                     eth-0-7(u) eth-0-8(u)
                                                     eth-0-9(u) eth-0-10(u)
                                                     eth-0-11(u) eth-0-12(u)
                                                     eth-0-13(u) eth-0-14(u)
                                                     eth-0-15(u) eth-0-16(u)
                                                     eth-0-17(u) eth-0-18(u)
                                                     eth-0-19(u) eth-0-20(u)
                                                     eth-0-21(u) eth-0-24(u)
                                                     eth-0-25(u) eth-0-26(u)
                                                     eth-0-27(u) eth-0-28(u)
                                                     eth-0-29(u) eth-0-30(u)
                                                     eth-0-31(u) eth-0-32(u)
                                                     eth-0-33(u) eth-0-34(u)
                                                     eth-0-35(u) eth-0-36(u)
                                                     eth-0-37(u) eth-0-38(u)
                                                     eth-0-39(u) eth-0-40(u)
                                                     eth-0-41(u) eth-0-42(u)
                                                     eth-0-43(u) eth-0-44(u)
                                                     eth-0-45(u) eth-0-46(u)
                                                     eth-0-47(u) eth-0-48(u)
10       VLAN0010            ACTIVE   0       Disable eth-0-22(u)
20       VLAN0020            ACTIVE   0       Disable

Switch# show dot1x

802.1X Port-Based Authentication Enabled
    RADIUS server address: 202.38.100.7:1812
    Next radius message ID: 0
```

```
Switch# show dot1x statistics
====================================
802.1X statistics for interface eth-0-22
   EAPOL Frames Rx: 52 - EAPOL Frames Tx: 4270
   EAPOL Start Frames Rx: 18 - EAPOL Logoff Frames Rx: 2
   EAP Rsp/Id Frames Rx: 29 - EAP Response Frames Rx: 3
   EAP Req/Id Frames Tx: 3196 - EAP Request Frames Tx: 3
   Invalid EAPOL Frames Rx: 0 - EAP Length Error Frames Rx: 0
   EAPOL Last Frame Version Rx: 2 - EAPOL Last Frame Src: ae38.3288.f046
```

9 ARP Inspection 配置

9.1 ARP Inspection 简介

缺省情况下，所有的 ARP 报文都将按照规则通过交换机。用户可以通过启用 ARP Inspection 功能监控 ARP 报文；该功能可以通过对 ARP 报文的有效性检查来过滤无效的 ARP 报文，也可以通过设置规则，让特定 ARP 报文通过，或者丢弃特定的 ARP 报文，以提高系统的安全性，并在一定程度上抑制 ARP 报文攻击。

ARP 检测可以在网络中验证 ARP 报文的安全特性，还能检查日志、丢弃无效 IP 与 MAC 捆绑的ARP报文。这些功能可以保护网络免受人为攻击。ARP 检测确保只执行有效的 ARP 请求和响应，交换机执行的行为包括：在不信任端口上拦截所有 ARP 请求和响应。

在更新本地 ARP 缓存或者转发到特定目的地址的报文之前，需要验证每个检测的报文是否有效。如果无效，需要丢弃无效的 ARP 报文。ARP 检测是根据现存的 DHCP Snooping 数据库中有效 IP对应 MAC 地址的条目，判断一个 ARP 报文的有效性。交换机在信任端口转发报文不需要任何检查，而在不信任端口时，交换机只在有效情况下实现转发。

9.2 术语解释

下面简要介绍用于描述 ARP Inspection 相关的术语和概念。

DHCP Snooping: DHCP Snooping 是一个在不可信主机和可信 DHCP 服务器之间执行防火墙功能的安全特性，这个特性建立和维护 DHCP Snooping 数据库，这个数据库包含租用 IP 地址的不信任主机信息。

Address Resolution Protocol (ARP): ARP 通过映射 IP 地址和 MAC 地址，提供在二层广播域的 IP 通信。例如主机 B 想要发送信息到主机 A 上，但是没有主机 A 的 MAC 地址，主机 B 在广播域内产生一个广播报文对所有主机获取主机 A 的 MAC 地址。在广播域内的所有主机接收 ARP 请求，主机 A 返回它的 MAC 地址。

9.3 配置 ARP 检测

9.3.1 配置可信任端口

如果设置端口为可信端口，则启用 ARP Inspection 以后，交换机不会验证通过此端口的 ARP 报文。

表9-1 配置可信任端口

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-
Switch(config-if)# ip arp inspection trust	配置 eth-0-1 为可信任端口	缺省情况下，端口为不可信任端口

9.3.2 配置指定 VLAN 上启用 ARP 检测

配置该命令前，需要创建 VLAN 以及添加接口至 VLAN。详情请见 9.5 配置举例。

表9-2 配置指定VLAN上启用ARP检测

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# ip arp inspection vlan 2	在 VLAN 2 上启用 ARP 检测功能	VLAN 范围，例如: 1,3-5,7,9-11

9.3.3 配置过滤 ARP 检测的日志信息

配置该命令对 ARP 检测的日志进行过滤，有 matchlog 和 none 两种方式。matchlog 表示将匹配的信息记录日志文件，none 表示将不匹配的信息记录日志文件。

表9-3 配置过滤ARP检测的日志信息

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# ip arp inspection vlan 2 logging acl-match matchlog	配置过滤 ARP 检测的日志信息，将匹配的信息记录日志文	VLAN 范围，例如: 1,3-5,7,9-11

命令举例	操作	说明
	件	

9.3.4 配置验证 ARP 报文中的指定字段

表9-4 配置验证ARP报文中的指定字段

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# ip arp inspection validate dst-mac	配置验证 ARP 报文的目的 MAC 地址	缺省情况下，ARP Inspection 不验证 ARP 报文的任何字段

说明

src-mac：检查以太网报头中的源 MAC，检查 ARP 请求和响应。一旦启用，如果发现不匹配的源 MAC 将被丢弃。

dst-mac：检查以太网报头中的目的 MAC，检查 ARP 请求和响应。一旦启用，如果发现不匹配的目的 mac 将被丢弃。

ip：检查以太网报文中的目的 IP 字段是否合法。

9.4 配置 ARP ACL

9.4.1 创建 ARP ACL

表9-5 创建ARP ACL

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# arp access-list acl1	创建一个 ARP 访问控制列表，并进入 ARP ACL 配置模式	ACL 名称不超过 40 个字符；在非 DHCP 环境中，动态 ARP 检测可以通过设置访问控制列表来验证

命令举例	操作	说明
		ARP 报文
Switch(config-arp-acl)# exit	退出 ARP ACL 配置模式	-

9.4.2 配置 ARP ACE

表9-6 配置ARP ACE

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# arp access-list acl1	创建一个 ARP 访问控制列表，并进入 ARP ACL 配置模式	ACL 名称不超过 40 个字符；在非 DHCP 环境中，动态 ARP 检测可以通过设置访问控制列表来验证 ARP 报文
Switch(config-arp-acl)# permit ip host 192.168.1.1 mac any	添加一个条目：允许来自 192.168.1.1 ARP 请求的 ACE	-

9.4.3 配置指定 VLAN 添加 ARP ACL

配置该命令前，需要创建VLAN以及添加接口至VLAN。详情请见9.5配置举例。

表9-7 配置指定VLAN添加ARP ACL

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# ip arp inspection filter acl vlan 2 static	在 VLAN2 上引用 ARP 访问控制列表	缺省情况下，VLAN 上不指定任何的 ARP 访问控制列表

9.5 配置举例

9.5.1 配置步骤

i. 创建VLAN

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# vlan database	配置 VLAN 数据库
Switch(config-vlan)# vlan 2	创建 VLAN 2
Switch(config-vlan)# exit	退出 VLAN 配置模式
Switch(config)# exit	退出全局配置模式

ii. 添加接口到VLAN

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式，开始配置端口 eth-0-1
Switch(config-if)# switchport access vlan 2	添加端口到 VLAN2
Switch(config-if)# interface eth-0-2	开始配置端口 eth-0-2
Switch(config-if)# switchport access vlan 2	添加端口到 VLAN2
Switch(config-if)# interface eth-0-3	开始配置端口 eth-0-3
Switch(config-if)# switchport access vlan 2	添加端口到 VLAN 2
Switch(config-if)# interface eth-0-4	开始配置 eth-0-4
Switch(config-if)# switchport access vlan 2	添加端口到 VLAN 2
Switch(config-if)# exit	退出接口配置模式

iii. 配置ARP检测

命令举例	操作步骤
Switch(config)# interface eth-0-1	进入接口配置模式，开始配置端口 eth-0-1
Switch(config-if)# ip arp inspection trust	配置端口为信任状态（通常把互联的交换机端口配置为可信任）
Switch(config-if)# exit	退出接口配置模式
Switch(config)# ip arp inspection vlan 2	在 VLAN2 上使能 ARP 检测
Switch(config)# ip arp inspection vlan 2 logging acl-match matchlog	配置 VLAN2 上过滤 ARP 检测的日志信

命令举例	操作步骤
	息，将匹配的信息记录日志文件
Switch(config)# ip arp inspection validate src-mac ip dst-mac	在 ARP 报文中验证源 MAC 地址、IP 地址、目的 MAC 地址

iv. 添加ARP ACL

命令举例	操作步骤
Switch(config)# arp access-list test	创建名为 test 的 ARP ACL
Switch(config-arp-acl)# deny request ip host 1.1.1.1 mac any	添加一个条目：拒绝来自 1.1.1.1 ARP 请求的 ACL 条目
Switch(config-arp-acl)# exit	退出 ARP ACL 配置模式
Switch(config)# ip arp inspection filter test vlan 2	在 VLAN2 上使能 ARP ACL
Switch(config)# exit	退出全局配置模式

9.5.2 显示与维护

命令	操作	说明
show ip arp inspection	显示 ARP 检测的配置及其统计信息	-
show ip arp inspection log [*log-number*]	显示所有 ARP Inspection 日志消息	log-number: 指定消息的条目，取值范围为 1~1024

显示 ARP 检测的配置及其统计信息：

```
Switch# show ip arp inspection

Source Mac Validation      : Enabled
Destination Mac Validation : Enabled
IP Address Validation      : Enabled
Vlan      Configuration    ACL Match        Static ACL
================================================================
2         enabled          test
Vlan      ACL Logging      DHCP Logging
================================================================
2         deny             deny
Vlan      Forwarded        Dropped     DHCP Drops      ACL Drops
================================================================
2         0                0           0               0
Vlan      DHCP Permits     ACL Permits     Source MAC Failures
```

```
===============================================================
2          0                      0                     0
Vlan    Dest MAC Failures    IP Validation Failures    Invalid Protocol Data
===============================================================
2         0                           0                                 0
```

显示所有 ARP Inspection 日志消息：

```
Switch# show ip arp inspection log

Total Log Buffer Size : 32
Syslog rate : 5 entries per 1 seconds.
1970-01-02 00:30:47 : Drop an ARP packet by ACL on vlan 2
1970-01-02 00:30:47 : Drop an ARP packet by ACL on vlan 2
1970-01-02 00:30:47 : Drop an ARP packet by ACL on vlan 2
1970-01-02 00:30:47 : Drop an ARP packet by ACL on vlan 2
1970-01-02 00:30:47 : Drop an ARP packet by ACL on vlan 2
1970-01-02 00:30:47 : Drop an ARP packet by ACL on vlan 2
1970-01-02 00:30:47 : Drop an ARP packet by ACL on vlan 2
1970-01-02 00:30:47 : Drop an ARP packet by ACL on vlan 2
1970-01-02 00:30:47 : Drop an ARP packet by ACL on vlan 2
1970-01-02 00:30:47 : Drop an ARP packet by ACL on vlan 2
1970-01-02 00:30:47 : Drop an ARP packet by ACL on vlan 2
```

10 DHCP Snooping 配置

10.1 DHCP Snooping 简介

DHCP Snooping 是一种安全功能，如不受信任的主机和信任的 DHCP 服务器之间的防火墙行为，DHCP Snooping 功能执行如下：

- 验证 DHCP 消息接收来自不信任的源和过滤掉无效消息。
- 建立和维护 DHCP Snooping 绑定数据库，其中包含不信任主机租用的 IP 地址信息。
- 利用 DHCP Snooping 绑定数据库来验证来自不受信任的主机的后续请求。
- 其他的安全功能。例如，动态 ARP 监测，也可以使用 DHCP Snooping 绑定数据库中存储的信息，每个 VLAN 的基础上启用 DHCP Snooping 功能，该功能默认在所有 VLAN 上都无效。用户可以在一个单独的 VLAN 或者 VLAN 范围使能该功能，DHCP Snooping 功能可以在软件中实现，所有 DHCP 消息在芯片中被拦截直接发往 CPU 进行处理。

10.2 配置 DHCP Snooping 基本功能

10.2.1 全局启用 DHCP Snooping

表10-1 全局启用DHCP Snooping

命令举例	操作	说明
Switch#configure terminal	进入全局配置模式	-
Switch(config)# dhcp snooping	全局启用 DHCP Snooping 功能	缺省情况下，DHCP Snooping 功能处于关闭状态

10.2.2 配置信任端口

配置连接DHCP服务器或其他交换机或路由器的接口为信任接口。配置连接DHCP客户端的接口为不信任接口。

表10-2 配置信任端口

命令举例	操作	说明
Switch#configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-
Switch(config-if)# dhcp snooping trust	配置接口为 DHCP Snooping 信任接口	默认情况下，接口为 DHCP Snooping 不信任接口

10.3 配置 DHCP Snooping 支持 Option 82 功能

10.3.1 使能插入 DHCP Option 82 数据

用户必须在全局配置模式下使用**dhcp snooping**命令，有关DHCP Snooping的配置才会生效。当Option82功能使能时，交换机收到主机发送的DHCP请求报文，会在报文中加入Option82选项信息。Option82选项信息包含交换机的MAC地址（远端ID选项），收到DHCP报文端口的ID（电路ID选项），该端口为VLAN配置模式的端口。交换机转发包含Option 82选项的DHCP请求报文给DHCP服务器。

当DHCP服务器收到报文，可以使用远端ID、电路ID，或分配IP地址和执行政策，例如限制IP地址的数目可以分配到一个单独的远端ID或电路ID。之后DHCP服务器回复带有Option 82选项的DHCP回复报文。

如果DHCP请求报文由中继转发给服务器，DHCP服务器单播DHCP回复报文给交换机。当DHCP客户端和DHCP服务器在同一子网时，DHCP服务器广播DHCP回复报文。交换机检测远端ID，以及可能存在的电路ID来检测DHCP报文是否原先就包含Option 82选项。交换机移除报文的Option 82选项，转发报文到发送DHCP请求报文主机的端口。

表10-3 配置步骤

命令举例	操作	说明
Switch#configure terminal	进入全局配置模式	-
Switch(config)# dhcp snooping	全局启用 DHCP Snooping 功能	缺省情况下，DHCP Snooping 功能处于关闭状态

命令举例	操作	说明
Switch(config)# dhcp snooping information option	使能插入 DHCP Option 82 数据	缺省情况下，不插入 DHCP Option 82 数据

10.3.2 配置不信任端口接收含有 Option82 的 DHCP 报文

用户可能需要一个边缘交换机连接的主机，可以在边缘网络的DHCP报文中插入Option 82选项。也可能需要在一个汇聚交换机上使能DHCP安全特性，例如DHCP Snooping，IP源地址绑定或动态ARP检测。但是，如果在一个汇聚交换机上使能DHCP Snooping，交换机会丢弃从不信任接口收到的含有Option 82选项的DHCP报文，无法学到连接信任接口设备的DHCP Snooping绑定信息。

如果需要汇聚交换机启用 DHCP Snooping 功能，并能接收从边缘交换机连接主机发来的带有 Option82 选项的 DHCP 报文，使用 **dhcp snooping information option allow-untrusted** 命令配置汇聚交换机。汇聚交换机可以学到从不信任端口收到的 DHCP 报文的绑定信息。用户也可以在汇聚交换机使能 DHCP 安全特性。边缘交换机连接到汇聚交换机的端口必须被配置为信任端口。

表10-4 配置步骤

命令举例	操作	说明
Switch#configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-
Switch(config-if)# dhcp snooping trust	配置接口为 DHCP Snooping 信任接口	默认情况下，接口为 DHCP Snooping 不信任接口
Switch(config-if)# quit	返回至上一级配置模式	-
Switch(config)# dhcp snooping	全局启用 DHCP Snooping 功能	缺省情况下，DHCP Snooping 功能处于关闭状态
Switch(config)# dhcp snooping information option allow-untrusted	配置接入交换机接收不信任端口收到的从边缘交换机发来的含有 Option82 的 DHCP 报文	缺省情况下，交换机丢弃不信任接口接收到的含有 Option82 的 DHCP 报文，该不信任接口可能连接到一个边缘交换机

10.3.3 配置 Option82 的电路 ID

配置该命令前，必须先全局使能 DHCP Snooping，才可以使 DHCP Snooping 的配置生效。

表10-5 配置步骤

命令举例	操作	说明
Switch#configure terminal	进入全局配置模式	-
Switch(config)# dhcp snooping	全局启用 DHCP Snooping 功能	缺省情况下，DHCP Snooping 功能处于关闭状态
Switch(config)# interface eth-0-1	进入接口配置模式	-
Switch(config-if)# dhcp snooping vlan 2 information option format-type circuit-id string vlan2	配置 Option82 中的电路 ID 为 vlan2	VLAN ID 取值范围为 1~4094；ASCII 字符串的取值范围为 1~63

10.3.4 配置 Option82 的远端 ID

类似地，必须先全局使能 DHCP Snooping，才可以使 DHCP Snooping 的配置生效。

表10-6 配置步骤

命令举例	操作	说明
Switch#configure terminal	进入全局配置模式	-
Switch(config)# dhcp snooping	全局启用 DHCP Snooping 功能	缺省情况下，DHCP Snooping 功能处于关闭状态
Switch(config)# dhcp snooping information option format remote-id hostname	配置 Option82 的远端 ID 为 hostname	ASCII 字符串的取值范围为 1~63

10.4 显示与维护

表10-7 显示与维护

命令	操作	说明
show dhcp snooping config	查看 DHCP Snooping 配置信息	-

命令	操作	说明
show dhcp snooping statistics	查看 DHCP Snooping 统计信息	-
show dhcp snooping trusted-sources	查看 DHCP Snooping 信任端口信息	-
show dhcp snooping binding all	查看 DHCP Snooping 绑定信息	-

10.5 典型配置举例

10.5.1 配置步骤

i. 配置VLAN

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# vlan database	配置 VLAN 数据库
Switch(config-vlan)# vlan 12	创建 VLAN 12
Switch(config-vlan)# exit	退出全局配置模式

ii. 配置接口eth-0-12

命令举例	操作步骤
Switch(config)# interface eth-0-12	进入接口配置模式
Switch(config-if)# switchport	设置为交换接口
Switch(config-if)# switchport access vlan 12	添加接口到 VLAN 12
Switch(config-if)# dhcp snooping trust	配置接口为信任状态
Switch(config-if)# no shutdown	使能接口
Switch(config-if)# exit	退出全局配置模式

iii. 配置接口eth-0-11

命令举例	操作步骤
Switch(config)# interface eth-0-11	进入接口配置模式

命令举例	操作步骤
Switch(config-if)# switchport	设置为交换接口
Switch(config-if)# switchport access vlan 12	添加接口到 VLAN 12
Switch(config-if)# no shutdown	使能接口
Switch(config-if)# exit	退出全局配置模式

iv. 配置VLAN12接口

命令举例	操作步骤
Switch(config)# interface vlan 12	进入接口配置模式
Switch(config-if)# ip address 12.1.1.1/24	设置 VLAN 12 的 IP 地址
Switch(config-if)# exit	退出接口配置模式

v. 配置DHCP特性

命令举例	操作步骤
Switch(config)# dhcp snooping verify mac-address	检查 DHCP 用户上送的请求报文头 MAC 地址是否合法

vi. 使能DHCP Snooping全局特性

命令举例	操作步骤
Switch(config)# service dhcp enable	使能 DHCP 服务
Switch(config)# dhcp snooping	使能 DHCP Snooping 特性
Switch(config)# dhcp snooping vlan 12	在 VLAN 12 上使能 DHCP Snooping 特性

10.5.2 命令验证

- 检查接口配置是否正确：

```
Switch(config)# show running-config interface eth-0-12

!
interface eth-0-12
 dhcp snooping trust
 switchport access vlan 12
!
```

```
Switch(config)# show running-config interface eth-0-11
!
interface eth-0-11
  switchport access vlan 12
!
```

- 检查DHCP服务状态：

```
Switch# show services

Networking services configuration:
Service Name                Status
============================================================
dhcp                        enable
```

- 检查当前DHCP Snooping配置信息：

```
Switch# show dhcp snooping config

dhcp snooping service: enabled
dhcp snooping switch: enabled
Verification of hwaddr field: enabled
Insertion of relay agent information (option 82): disable
Relay agent information (option 82) on untrusted port: not allowed
dhcp snooping vlan 12
```

- 检查DHCP Snooping的统计信息：

```
Switch# show dhcp snooping statistics

DHCP snooping statistics:
============================================================
DHCP packets                                17
BOOTP packets                               0
Packets forwarded                           30
Packets invalid                             0
Packets MAC address verify failed           0
Packets dropped                             0
```

- 显示DHCP Snooping绑定信息：

```
Switch# show dhcp snooping binding all

DHCP snooping binding table:
VLAN MAC Address       Interface    Lease(s)     IP Address
============================================================
```

12	0016.76a1.7ed9	eth-0-11	691190	12.1.1.65

11 IP Source Guard 配置

11.1 IP Source Guard 简介

通过 IP Source Guard 绑定功能，可以对端口转发的报文进行过滤控制，防止非法 IP 地址和 MAC 地址的报文通过端口，提高了端口的安全性。端口接收到报文后，通过查找 IP Source Guard 绑定表项，对报文进行如下处理：

- 对于 IP+Port 的绑定表项，如果报文中的源 IP 地址与绑定表项中记录的 IP 地址相同，端口将转发该报文；若不相同，则丢弃该报文；
- 对于 IP+Port+MAC 的绑定表项，如果报文中的源 MAC 地址和源 IP 地址与绑定表项中记录的 MAC 地址和 IP 地址相同，端口将转发该报文；若不相同，则丢弃该报文；
- 对于 IP+Port+MAC+VLAN 的绑定表项，如果报文中的源 MAC 地址，源 IP 地址和 VLAN 与绑定表项中记录的 MAC 地址，IP 地址和 VLAN 相同，端口将转发该报文；若不相同，则丢弃该报文。

11.2 术语解释

以下是关于 IP Source Guard 的术语和概念的简要描述：

动态主机配置协议 (DHCP)：是一个客户机/服务器的协议，它会自动提供 IP 地址以及其它相关的子网掩码和默认网关等信息给一个互联网协议（IP）的主机。

DHCP Snooping: 是一种安全功能，如不受信任的主机和信任的 DHCP 服务器之间的防火墙行为。此功能建立和维护 DHCP Snooping 绑定数据库，其中包含不可信主机租用的 IP 地址信息。

ACL: 访问控制条目。

11.3 配置 IP Source Guard 绑定功能

11.3.1 添加/删除静态 IP 绑定条目

一条静态的 IP 绑定条目包括一个 IP 地址，一个 MAC 地址，以及 VLAN ID 和接口名字。同一个 IP 地址或 MAC 地址只能出现在一个绑定条目中，不允许重复出现。绑定条目配置以后不能修改，只能删除后重新配置。

表11-1 添加静态IP绑定条目

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# ip source binding mac 0001.1234.1234 vlan 1 ip 172.20.50.5 interface eth-0-1	绑定 MAC 地址 0001.1234.1234，VLAN 1，IP 地址 172.20.50.5 和接口 eth-0-1 到一个绑定条目中	缺省情况下，系统未配置任何绑定条目

可以使用命令删除配置的 VLAN 和接口，如果不指定 VLAN 或者接口，那么所有的绑定条目都将被删除。下表以删除所有绑定条目为例，详细举例可参考 11.5 典型配置举例。

表11-2 删除静态IP绑定条目

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# no ip source binding entries	删除所有绑定条目	缺省情况下，系统未配置任何绑定条目

11.3.2 配置端口绑定的最大条目数

表11-3 配置端口绑定的最大条目数

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# ip source maximal binding number per-port 20	设置每个端口上绑定的最大条目数为 20	绑定条目的取值范围为 0～30，0 表示不限定；缺省情况下，绑定的最大条目数为 10

命令举例	操作	说明
		条

11.3.3 端口使能 IP 绑定检查功能

配置该命令可以在接口上使能 IP 绑定检查功能，并指定检查项。检查项包括：ip（检查源 IP 地址）、ip-mac（检查源 IP 地址和源 MAC 地址）、ip-vlan（检查源 IP 地址和源 VLAN）、ip-mac-vlan（检查源 IP 地址、源 MAC 地址和源 VLAN）。

表11-4 端口使能IP绑定检查功能

命令举例	操作	说明
Switch#configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-
Switch(config-if)# ip verify source ip-mac	在接口上使能 IP 绑定检查功能，检查源 IP 和 MAC	在 Access 端口上，不带 tag 的报文可以通过源 VLAN 检查。缺省情况下，接口 IP 绑定检查功能处于关闭状态

11.4 显示与维护

表11-5 显示与维护

命令	操作	说明
show ip source binding [**interface** *if-name*]	显示 IP 绑定检查的功能的相关配置和绑定条目	如果不指定端口，那么所有绑定表项都会被显示出来

11.5 典型配置举例

11.5.1 配置步骤

i. 配置VLAN信息

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# vlan database	进入 VLAN 配置模式
Switch(config-vlan)# vlan 3	创建 VLAN3
Switch(config-vlan)# exit	退出 VLAN 配置模式
Switch(config)# interface eth-0-16	进入接口配置模式
Switch(config-if)# switchport	设置端口为二层端口
Switch(config-if)# no shutdown	打开端口
Switch(config-if)# switchport access vlan 3	设置端口属于 VLAN3
Switch(config-if)# exit	退出接口配置模式

ii. 配置IP Source Guard

命令举例	操作步骤
Switch(config)# ip source maximal binding number per-port 15	设置每个端口最大绑定的条目为 15 条
Switch(config)# ip source binding mac 1111.1111.1111 vlan 3 ip 10.0.0.2 interface eth-0-16	配置 IP Source Guard 绑定表项
Switch(config)# interface eth-0-16	进入接口配置模式
Switch(config-if)# ip verify source ip	在接口下使能 IP+Port 绑定检查
Switch(config-if)# exit	退出接口配置模式

iii. 删除配置

命令举例	操作步骤
Switch(config)# no ip source binding mac 1111.1111.1111 vlan 3 ip 10.0.0.2 interface eth-0-16	删除单条 IP Source Guard 绑定表项
Switch(config)# no ip source binding entries interface eth-0-16	删除所有绑定到 eth-0-16 的表项
Switch(config)# no ip source binding entries vlan 3	删除所有绑定到 VLAN 3 的表项
Switch(config)# no ip source binding entries	清除所有的绑定表项

11.5.2 命令验证

显示上述配置结果：

```
Switch#show running-config interface eth-0-16

!
interface eth-0-16
  ip verify source ip
  switchport access vlan 3
```

12 私有 VLAN 配置

12.1 私有 VLAN 简介

私有 VLAN 属性能在同一 VLAN 内部实现二层流量的隔离和互通，能够节约 IP 地址、隔离广播风暴、防止病毒攻击等，增强了网络安全。

私有 VLAN 将一个 VLAN 的二层广播域划分为多个子域，每个子域都包含一个私有 VLAN 对，即主 VLAN 和辅助 VLAN，辅助 VLAN 又分为隔离 VLAN 和群体 VLAN。同一个隔离 VLAN 中的主机之间不能相互通信，一个私有 VLAN 域中只有一个隔离 VLAN。而同一个群体 VLAN 中的主机之前可以相互通信，一个私有 VLAN 域中可以有多个群体 VLAN。隔离 VLAN 与群体 VLAN 之间不能相互访问。

一个私有 VLAN 域内一般有三种类型的端口：隔离端口、群体端口以及混杂端口。

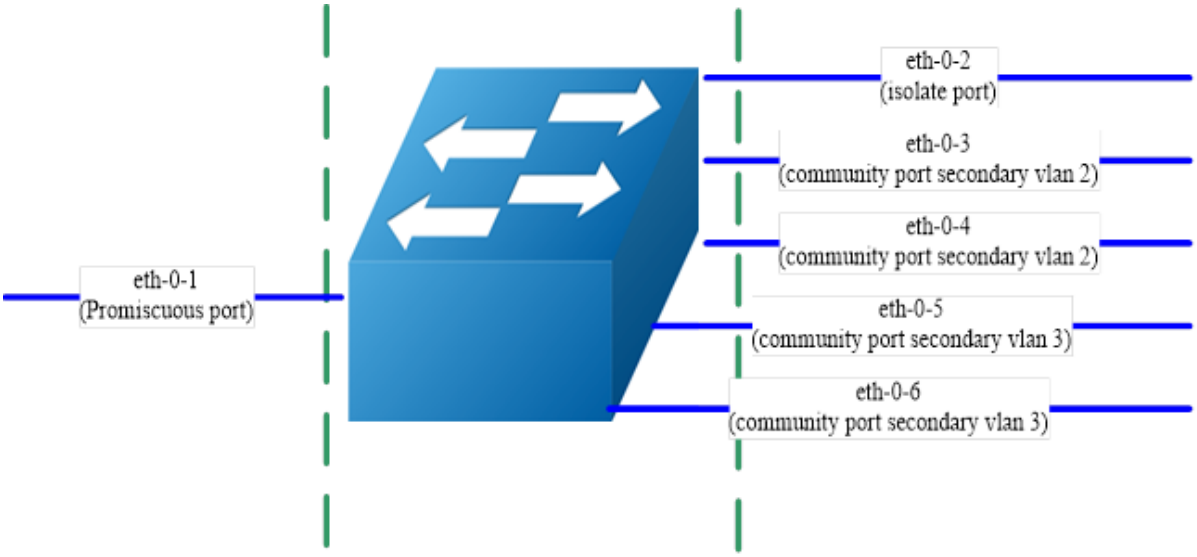
12.2 配置私有 VLAN

12.2.1 介绍

如图 12-1所示，所有端口在同一私有VLAN中。端口 1 是混杂端口，可与同一私有 VLAN 中所有其他端口互通。端口 2 是隔离端口，它与同一私有 VLAN 中所有其他端口都互相隔离，除了混杂端口（端口1）。端口 3 和 4 是互通端口，属于子 VLAN 2，端口 3 和 4 彼此可以互通，还可以和混杂端口互通、同一私有 VLAN 的其他端口都互相隔离。端口5和6 是互通端口，属于子 VLAN 3，端口 5 和 6 彼此可以互通，还可以和混杂端口互通，与同一私有VLAN的其他端口都互相隔离。

12.2.2 拓扑

图 12-1 私有 VLAN 基本拓扑图



12.2.3 配置方法

命令举例	操作步骤
Switch# configure terminal	进入配置模式
Switch (config)# vlan database	进入 VLAN 配置模式
Switch (config-vlan)# vlan 2	创建 VLAN 2
Switch (config-vlan)# quit	退出 VLAN 配置模式
Switch (config)# interface eth-0-1	进入接口配置模式
Switch (config-if)# switchport mode private-vlan promiscuous	配置私有 VLAN 模式为混杂端口
Switch (config-if)# switchport private-vlan 2	配置主 VLAN 2
Switch (config-if)# quit	退出接口配置模式
Switch (config)# interface eth-0-2	进入接口配置模式
Switch (config-if)# switchport mode private-vlan host	配置私有 VLAN 模式为主机端口
Switch (config-if)# switchport private-vlan 2	配置私有 VLAN 模式为隔离端口，配置主

命令举例	操作步骤
isolate	VLAN 为 2
Switch (config-if)# quit	退出接口配置模式
Switch (config)# interface eth-0-3	进入接口配置模式
Switch (config-if)# switchport mode private-vlan host	配置私有 VLAN 模式为主机端口
Switch (config-if)# switchport private-vlan 2 community-vlan 2	配置私有 VLAN 模式为互通端口，配置主 VLAN 和子 VLAN 为 2
Switch (config-if)# quit	退出接口配置模式
Switch (config)# interface eth-0-4	进入接口配置模式
Switch (config-if)# switchport mode private-vlan host	配置私有 VLAN 模式为主机端口
Switch (config-if)# switchport private-vlan 2 community-vlan 2	配置私有 VLAN 模式为隔离端口，配置主 VLAN 为 2
Switch (config-if)# quit	退出接口配置模式
Switch (config)# interface eth-0-5	进入接口配置模式
Switch (config-if)# switchport mode private-vlan host	配置私有 VLAN 模式为主机端口
Switch (config-if)# switchport private-vlan 2 community-vlan 3	配置私有 VLAN 模式为隔离端口，配置主 VLAN 为 3
Switch (config-if)# quit	退出接口配置模式
Switch (config)# interface eth-0-6	进入接口配置模式
Switch (config-if)# switchport mode private-vlan host	配置私有 VLAN 模式为主机端口
Switch (config-if)# switchport private-vlan 2 community-vlan 3	配置私有 VLAN 模式为隔离端口，配置主 VLAN 为 3
Switch (config-if)# quit	退出接口配置模式

12.2.4 命令验证

显示上述配置结果：

```
Switch # show private-vlan
Primary      Secondary Type                 Ports
------------------------------------------------------------------------------
2            N/A       promiscuous          eth-0-1
2            N/A       isloate              eth-0-2
2            2         community            eth-0-3     eth-0-4
2            3         community            eth-0-5     eth-0-6
```

13 AAA 配置

13.1 AAA 简介

AAA 是认证（Authentication）、授权（Authorization）、计费（Accounting）的简称，它提供了认证、授权和计费三种安全功能，可以实现对网络安全的管理：

- 认证：确定用户是否有权限访问网络服务器，需要进行合法性检查，如验证用户名和密码等。
- 授权：用户提供访问特定网络或设备的权限，限制用户对网络或设备的使用。
- 计费：记录用户在网络中进行的所有操作和使用网络资源的情况。

13.1.1 认证

AAA 支持三种认证方式：

不认证：对用户完全信任，无需认证即可直接访问网络服务器。一般不采用此方式。

本地认证：将用户信息在设备上进行配置，运行速度快，但存储信息的容量根据设备差异会有所不同。

远端认证：将用户信息在远端服务器上进行配置，可以通过 RADIUS 协议或 TACACS+协议进行远端认证。

如果采用多种认证方式，按配置的先后顺序生效。

13.1.2 授权

AAA 支持以下三种授权方式：

直接授权：对用户完全信任，直接授权访问网络服务器。

本地授权：根据设备对本地用户相关属性的配置进行授权。

远端授权：通过 TACACS+服务器对用户进行授权，或者 RADIUS 认证成功后授权（RADIUS 协议的认证和授权功能绑定在一起，不能单独进行授权）

13.1.3 计费

AAA 支持两种计费方式：

不计费：不对用户的操作或者网络资源的占用情况进行计费。

远端计费：可以通过 TACACS+服务器或者 RADIUS 服务器进行远端计费。

13.2 配置 AAA

13.2.1 配置 AAA 访问控制模块

表13-1 全局启用AAA访问控制模块

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	缺省情况下，AAA 访问控制模块处于关闭状态
Switch(config)#aaa new-model	使能 AAA 访问控制模块	

13.2.2 AAA 显示与维护

表13-2 AAA显示与维护

命令	操作	说明
show aaa status	显示认证、授权、计费（AAA）的状态信息	-
show aaa method-lists authentication	显示一系列的认证方式的相关信息	-

13.3 典型配置举例

13.3.1 配置 AAA 与 RADIUS

i. 介绍

系统可以使用AAA认证的方法验证访问网络和网络服务的用户。RADIUS认证是AAA认证方法之一。RADIUS使用UDP，传输效率高。它将认证和授权结合，防止未经授权的访问，确保网络安全的分布式客户机/服务器系统。RADIUS为网络环境中广泛使用的协议。它通常用于嵌入式网络设备，如路由器、调制解调器、交换机等。RADIUS客户端通常在支持RADIUS的路由器和交换机上运行。客户端发送认证请求到RADIUS服务器，RADIUS服务器包含所有的用户认证和网络服务访问信息。

ii. 拓扑

图 13-1 RADIUS 拓扑图

iii. 配置方法

图 13-1为 RADIUS 的网络拓扑。一台 PC 机作为 RADIUS 服务器， 配置网卡 1.1.1.2/24。设置 Switch 的 Eth-0-23 接口的 IP 地址为 1.1.1.1/24。配置交换机的管理口 IP 地址为 10.10.29.215，连接交换机管理口的 PC 机 IP 地址为 10.10.29.10。

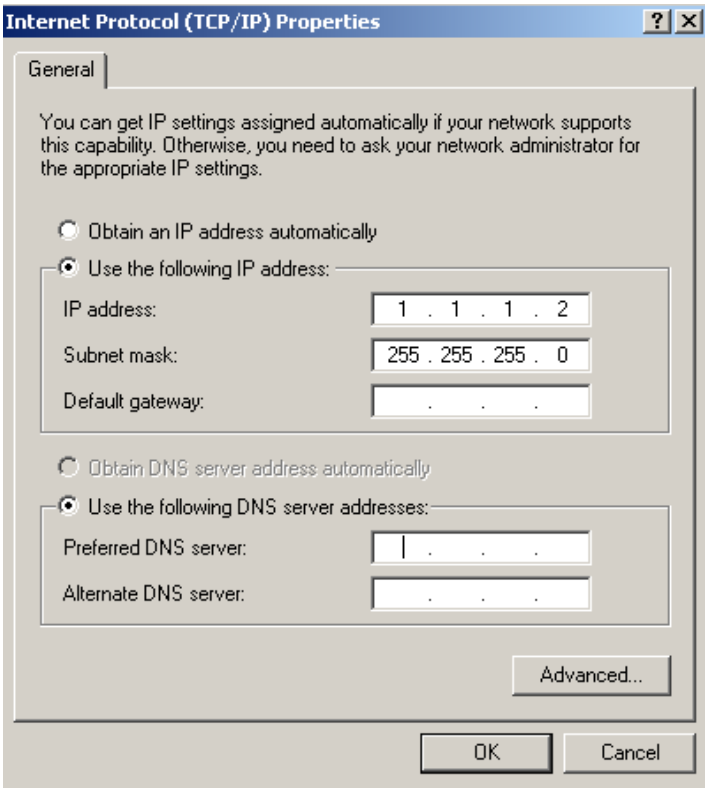
1. 配置AAA+RADIUS

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# aaa new-model	启用 AAA 协议
Switch(config)# aaa authentication login radius-login radius local	设置 AAA 认证的模式
Switch(config)# radius-server host 1.1.1.2 auth-port 1819 key keyname	配置 RADIUS 服务器参数
Switch(config)# radius-server host 2001:1000::1 auth-port 1819 key keyname	（可选）配置 RADIUS 服务器参数
Switch(config)# interface eth-0-23	进入接口配置模式
Switch(config-if)# no switchport	设置端口为三层端口
Switch(config-if)# ip address 1.1.1.1/24	配置 IP 地址
Switch(config-if)# quit	退出接口配置模式
Switch(config)# line vty 0 7	进入 VTY 模式
Switch(config-line)#login authentication radius-login Switch(config-line)#privilege level 4 Switch(config-line)#no line-password	配置登录认证方式

2. 配置PC及WinRADIUS

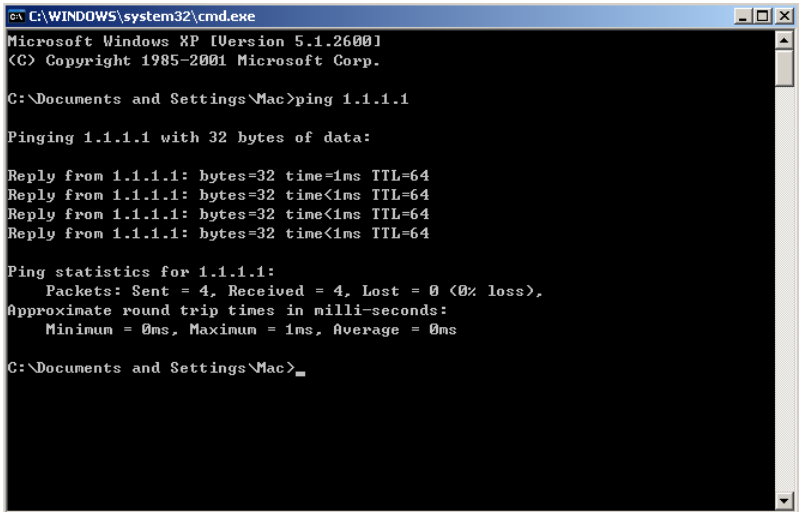
- 配置IP地址，详细步骤如下图 13-2所示：

图 13-2 配置 IP 地址



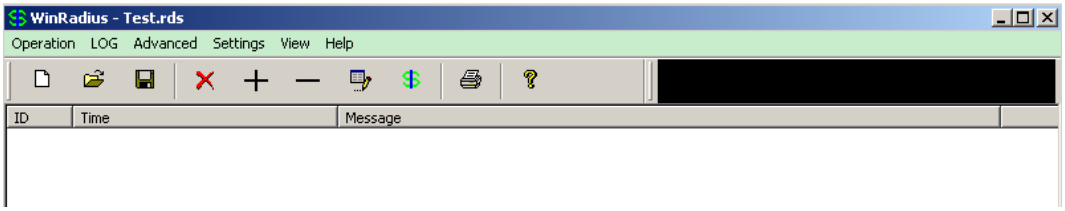
- 测试客户机与服务端之间的连通性，如图 13-3所示：

图 13-3 连通性检查结果



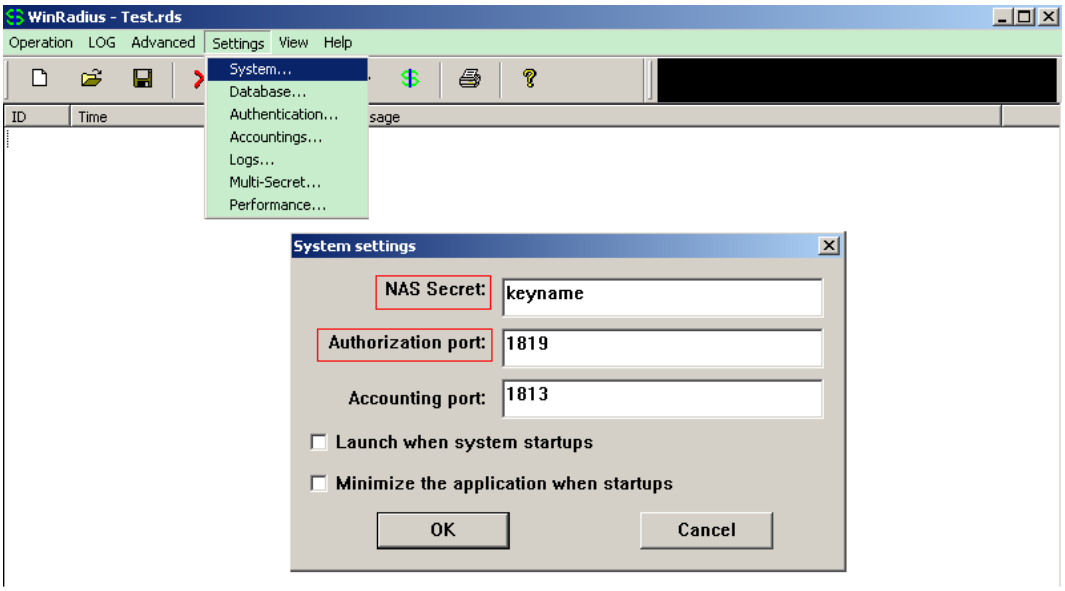
- 打开服务器上的软件，如图 13-4所示：

图 13-4 打开服务器软件



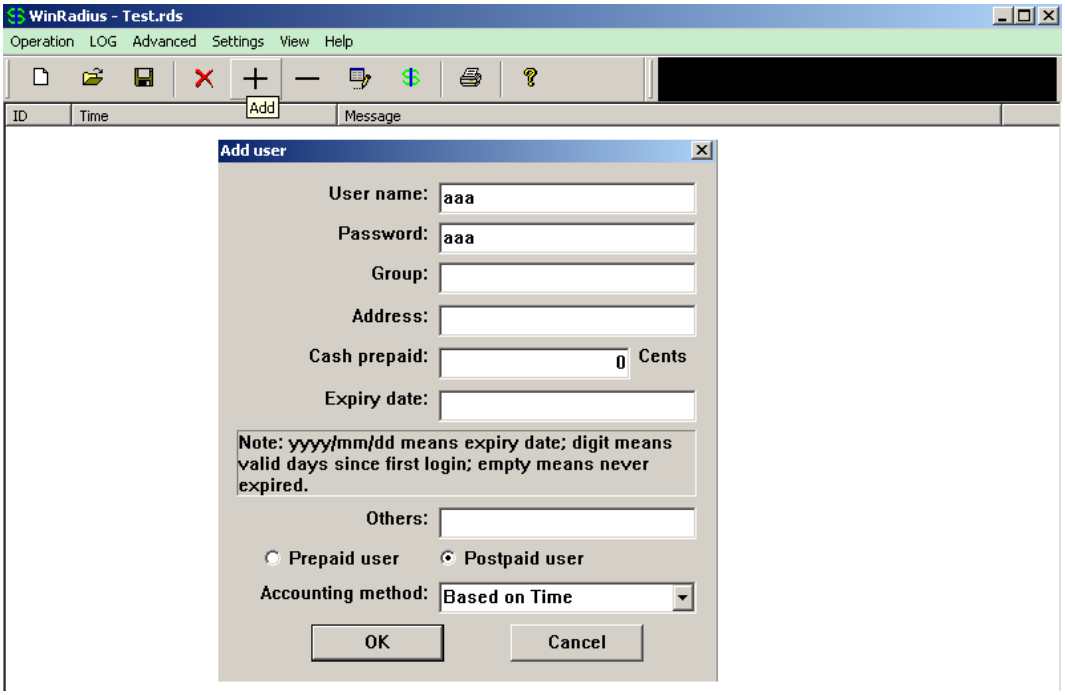
- 如图 13-5所示，单击设置→系统，完成以下配置：

图 13-5 系统配置



- 输入用户名和密码以及其他相关信息后，单击**OK**，如图 13-6所示：

图 13-6 添加用户信息



- 使用**ping**命令检测连通结果，如图 13-7所示：

图 13-7 检测连通结果

```
C:\Documents and Settings\mac>ping 10.10.29.215

Pinging 10.10.29.215 with 32 bytes of data:

Reply from 10.10.29.215: bytes=32 time<1ms TTL=63
Reply from 10.10.29.215: bytes=32 time<1ms TTL=63
Reply from 10.10.29.215: bytes=32 time<1ms TTL=63
Reply from 10.10.29.215: bytes=32 time<1ms TTL=63

Ping statistics for 10.10.29.215:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

iv. 命令验证

- 显示认证、授权、计费（AAA）的状态信息：

```
Switch# show aaa status

aaa stats:
        Authentication enable
```

- 显示一系列的认证方式的相关信息：

```
Switch# show aaa method-lists authentication

authen queue=AAA_ML_AUTHEN_LOGIN
      Name = default    state = ALIVE :      local
Name = radius-login    state = ALIVE :      radius    local
```

说明

1.注意开启 RADIUS 验证功能。

2.确认线缆连接的正确性。

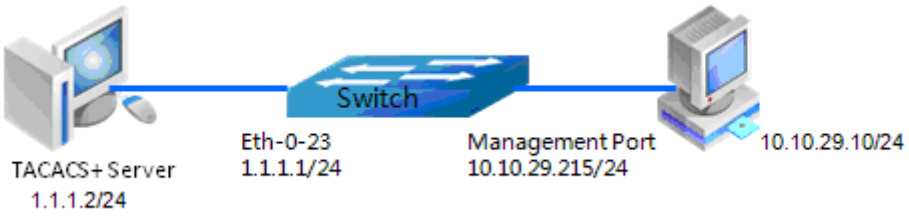
13.3.2 配置 AAA 与 TACACS+

i. 介绍

TACACS+认证是 AAA 认证方法之一。TACACS+协议属于私有协议，协议报文较为复杂。使用 TCP，传输更为可靠。与 RADIUS 协议不同，RADIUS 仅对从客户端到服务器的认证报文中的口令加密，其余部分未加密。而 TACACS+对报文主体全部加密，将认证与授权相分离。

ii. 拓扑

图 13-8 TACACS+拓扑图



iii. 配置方法

图 13-8是TACACS+的网络拓扑。一台PC机作为 TACACS+服务器，配置网卡1.1.1.2/24。设置Switch的eth-0-23接口的IP地址为1.1.1.1/24。配置交换机的管理口IP地址为10.10.29.215，连接交换机管理口（仅限带内管理口）的PC机IP地址为10.10.29.10。

1. 配置AAA与TACACS+

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# aaa new-model	启用 AAA 协议
Switch(config)# aaa authentication login tac-login tacacs-plus local	设置 AAA 认证的模式
Switch(config)# aaa authorization exec default tacacs-plus	设置 AAA 授权模式
Switch(config)# aaa accounting exec default start-stop tacacs-plus	设置 AAA EXEC 计费
Switch(config)# aaa accounting commands default tacacs-plus	设置 AAA 命令行计费
Switch(config)# tacacs-server host 1.1.1.2 port 123 key keyname	设置 TACACS+服务器的 IP 地址，验证端口和密码
Switch(config)# interface eth-0-23	进入接口配置模式
Switch(config-if)# no switchport	设置端口为三层端口
Switch(config-if)# ip address 1.1.1.1/24	配置 IP 地址
Switch(config-if)# quit	退出接口配置模式
Switch(config)# line vty 0 7	进入 VTY 模式
Switch(config-line)#login authentication tac-login Switch(config-line)#privilege level 4 Switch(config-line)#no line-password	配置验证方式

2. 配置TACACS+服务器

- 下载TACACS+服务器代码，DEVEL.201105261843.tar.bz2。
- 编译TACACS+服务器代码。
- 修改配置文件，增加用户名和密码。

```
#!../obj.linux-2.6.9-89.29.1.elsmp-x86_64/tac_plus
id = spawnd {
        listen = { port = 49 }
        spawn = {
                instances min = 1
                instances max = 10
        }
        background = no
```

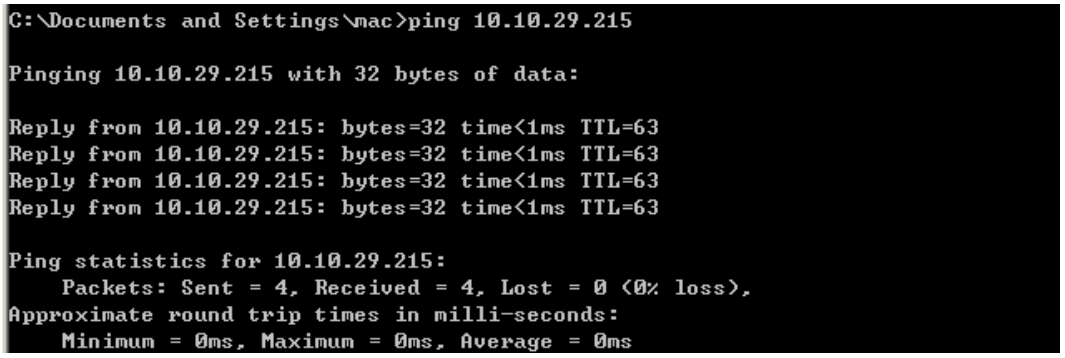
```
}
        user = aaa {
                password = clear bbb
                member = guest
        }
```

- 允许TACACS+服务器程序。

  [disciple: ~]$ ./tac_plus ./tac_plus.cfg.in -d 1

- 使用**ping**命令检查连通结果，如图 13-9所示。

图 13-9 连通性检测结果



iv. 命令验证

- 显示认证、授权、计费（AAA）的状态信息：

```
Switch# show aaa status
aaa stats:
        Authentication enable
```

- 显示一系列的认证方式的相关信息：

```
Switch# show aaa method-lists authentication
authen queue=AAA_ML_AUTHEN_LOGIN
      Name = default    state = ALIVE :      local
Name = tac-login    state = ALIVE :      tacacs-plus local
```

14 端口隔离配置

14.1 端口隔离简介

用户可以将不同的端口加入至不同的 VLAN，实现端口间的二层隔离，但这样会造成 VLAN 资源的浪费。通过端口隔离的特性，用户可以将不同的端口加入至同一个 VLAN 中，但是不同端口之间不能互通。用户只需要采用端口隔离功能，将端口加入到隔离组中，实现隔离组内端口之间的二层数据的隔离。从而增强了网络的安全性，提供了灵活的组网方案，同时节省了大量的 VLAN 资源。

14.2 配置端口隔离

14.2.1 配置端口加入隔离组

属于同一隔离组的两个端口之间将受到端口隔离功能的控制。属于不同隔离组的两个端口不受该功能影响。隔离组可以在物理端口或者聚合端口上配置。

表14-1 配置端口加入隔离组

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config-if)# interface eth-0-1	进入接口配置模式	-
Switch(config-if)# port-isolate group 1	配置端口属于隔离组 1	隔离组号的取值范围范围 1~30；缺省情况下，系统未配置隔离组

14.2.2 配置端口隔离模式

端口隔离模式有两种可供选择：隔离二层报文（l2）和全部隔离（all）。如果隔离模式为隔离二层，三层报文将不受影响。如果隔离模式为全部隔离，所有报文都将受端口隔离功能的控制。

表14-2 配置端口隔离模式

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-

命令举例	操作	说明
Switch(config)# port-isolate mode all	配置端口隔离模式为全部隔离	缺省情况下，仅隔离二层报文

14.2.3 端口隔离显示与维护

表14-3 端口隔离显示与维护

命令	操作	说明
show port-isolate [**group** *isolate-group-id*]	显示端口隔离相关配置信息	隔离组号的取值范围范围 1~30

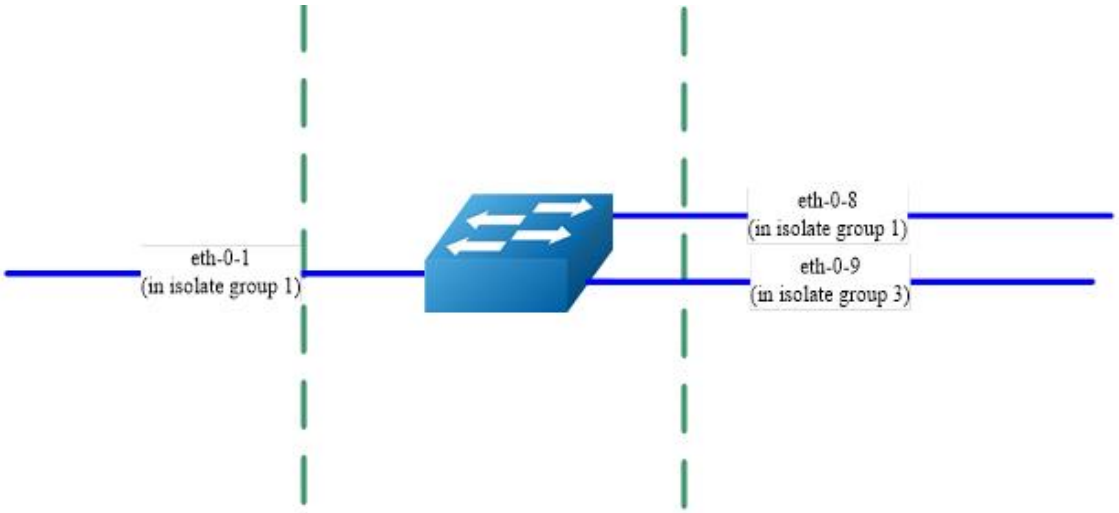
14.3 典型配置举例

14.3.1 介绍

如下图 14-1，端口1和端口8在同一个隔离组1，所以端口1和端口8不能互相通信。端口9在隔离组3，所以端口9能和端口1、端口8互相通信。

14.3.2 拓扑

图 14-1 端口隔离基本拓扑图



14.3.3 配置方法

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# port-isolate mode l2	设置端口隔离的模式
Switch(config-if)# interface eth-0-1	进入接口配置模式
Switch(config-if)# port-isolate group 1	配置端口属于隔离组 1
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface eth-0-8	进入接口配置模式
Switch(config-if)# port-isolate group 1	配置端口属于隔离组 1
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface eth-0-9	进入接口配置模式
Switch(config-if)# port-isolate group 3	配置端口属于隔离组 3
Switch(config-if)# exit	退出接口配置模式
Switch(config)# end	退出全局配置模式

14.3.4 命令验证

显示端口隔离相关配置信息：

```
Switch# show port-isolate
------------------------------------------------------------------
  Port Isolate Groups:
------------------------------------------------------------------
  Groups ID: 1
eth-0-1，eth-0-8
------------------------------------------------------------------
Groups ID: 3
eth-0-9
------------------------------------------------------------------
```

15 DDoS 攻击与防御配置

15.1 DDoS 攻击与防御简介

Distributed Denial of Service（分布式拒绝服务，缩写：DDoS）攻击是由传统的 Denial of Service（拒绝服务，缩写：DoS）攻击发展而来，攻击原理是利用合理的服务请求来占用过多的服务资源，从而使主机或者服务器无法处理合法用户的指令。相比之下，DDoS 攻击的流量增强且攻击的方式更为隐蔽，增大了防御的难度。DDoS 攻击通常以报文泛洪的形式体现，这些不同来源的恶意的报文将造成网络资源浪费、链路带宽堵塞、服务器资源耗尽导致的业务中断等。

DDoS 防御特性可以保护我们交换机抵挡以下类型的攻击，拦截不同类型攻击对应的数据包：

- ICMP 泛洪攻击：该攻击通过向目标 IP 发送大量 ICMP 报文，占用带宽造成网络堵塞，从而导致合法报文无法达到目的地，服务器无法正常处理业务。
- Smurf 攻击：攻击者先使用受害主机的地址，向一个广播地址发送 ICMP 回响请求，在此广播网络上，潜在的计算机会做出响应，大量响应将发送到受害主机。此攻击后果与 ICMP 泛洪攻击类似，最终造成网络阻塞，但比 ICMP 泛洪攻击更为隐秘。
- SYN 泛洪攻击：蓄意侵入 TCP 三次握手并打开大量的 TCP/IP 连接而进行的攻击，该攻击利用 IP 欺骗，向受害主机的系统发送看起来合法的 SYN 请求，而事实上该源地址不存在或当时不在线，因而回应的 ACK 消息无法到达目的。而受害主机的系统被大量的数据流量阻塞，或造成资源消耗，导致无法为合法的用户提供服务。
- UDP 泛洪攻击：该攻击通过向目标 IP 发送大量 UDP 报文，占用带宽，消耗资源。
- Fraggle 攻击：该攻击是 Smurf 的变种，针对防火墙对 ICMP 报文检查比较严格的前提下，不再向广播地址发 ICMP 请求报文，而是改为发送 UDP 报文。
- Small-packet 攻击：IP 小报文攻击是发送大量的小报文到被攻击系统来消耗系统的资源。
- bad mac intercept ：目的 MAC 地址等于源 MAC 地址的报文攻击。
- bad ip equal：目的 IP 地址等于源 IP 地址的报文攻击。

15.2 配置 DDoS 防御

15.2.1 配置抵御 ICMP 泛洪攻击

使用该条命令可以配置系统限制接收 ICMP 报文的速率。

表15-1 配置步骤

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# ip icmp intercept maxcount 100	使能 ICMP 泛洪检测，设置每秒最多可接收 ICMP 报文的个数为 100	每秒接收相应数据包的个数，取值范围为 0~1000，默认值为 500；缺省情况下，未配置抵御 ICMP 泛洪攻击
Switch(config)# end	退出全局配置模式	-

15.2.2 配置防御 Smuf 攻击

表15-2 配置步骤

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# ip smurf intercept	使能 Smurf 攻击检测	缺省情况下，未使能 Smurf 攻击检测
Switch(config)# end	退出全局配置模式	-

15.2.3 配置 SYN 泛洪攻击

使用该条命令可以设置系统限制接收 TCP 协议的 SYN 报文的速率。

表15-3 配置步骤

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# ip tcp intercept maxcount 100	使能 SYN 泛洪检测，设置每秒接收 TCP 的 SYN 报文个数最大为 100	每秒接收相应数据包的个数，取值范围为 0~1000，默认值为 500；缺省情况下，未配置抵御 SYN 泛洪攻击

命令举例	操作	说明
Switch(config)# end	退出全局配置模式	-

15.2.4 配置 UDP 泛洪攻击

使用该条命令可以设置系统限制接收 UDP 报文的速率。

表15-4 配置步骤

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# ip udp intercept maxcount 100	使能 UDP 泛洪检测，设置每秒接收 UDP 报文个数最大为 100	每秒接收相应数据包的个数，取值范围为 0~1000，默认值为 500；缺省情况下，未配置抵御 UDP 泛洪攻击
Switch(config)# end	退出全局配置模式	-

15.2.5 配置防御 Fraggle 攻击

表15-5 配置步骤

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# ip fraggle intercept	使能 Fraggle 攻击	缺省情况下，未使能 Fraggle 攻击检测
Switch(config)# end	退出全局配置模式	-

15.2.6 配置抵御 Small-packet 攻击

如果检测到 IP 报文长度小于设定的长度，则丢弃该报文。

表15-6 配置步骤

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# ip small-packet intercept maxlength 32	使能 Small-packet 攻击检测，设置接收 IP 报文长度最小为	接收 IP 报文的最小长度，取值范围为 28~65535，默认值为 28；缺省情

命令举例	操作	说明
	32 字节	况下，未使能 Small-packet 攻击检测
Switch(config)# end	退出全局配置模式	-

15.2.7 配置过滤相同 IP/MAC 地址报文

表15-7 配置过滤相同IP地址报文

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# ip ipeq intercept	使能检测源 IP 地址等于目的 IP 地址的报文攻击	缺省情况下，未使能检测源 IP 地址等于目的 IP 地址的报文攻击
Switch(config)# end	退出全局配置模式	-

表15-8 配置过滤相同MAC地址报文

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# ip maceq intercept	使能检测源 MAC 地址等于目的 MAC 地址的报文攻击	缺省情况下，未使能检测源 MAC 地址等于目的 MAC 地址的报文攻击
Switch(config)# end	退出全局配置模式	-

15.3 显示与维护

表15-9 显示与维护

命令	操作	说明
show ip-intercept config	显示系统当前 DDoS 防御配置	-
show ip-intercept statistics	显示当前攻击检测丢包的统计信息	-
clear ip-intercept statistics	清除攻击检测丢包统计信息	-

根据 15.2 上述配置，显示系统当前 DDoS 防御配置：

```
Switch# show ip-intercept config
```

```
Current DDoS Prevent configuration:
============================================================
ICMP Flood Intercept                :Enable    Maxcount:100
UDP Flood Intercept                 :Enable    Maxcount:100
SYN Flood Intercept                 :Enable    Maxcount:100
Small-packet Attack Intercept       :Enable    Packet Length:32
Sumrf Attack Intercept              :Enable
Fraggle Attack Intercept            :Disable
MAC Equal Intercept                 :Enable
IP Equal Intercept                  :Enable
Switch# show ip-intercept statistics
Current DDoS Prevent statistics:
============================================================
Resist Small-packet Attack packets number      :   65
Resist ICMP Flood packets number                   :   0
Resist Smurf Attack packets number             :   0
Resist SYN Flood packets number                    :   0
Resist UDP Flood packets number                    :   0
```

16 Key Chain 配置

16.1 Key Chain 简介

Key Chain（密钥链）是一种通用的认证方法，适用于需要共享密钥的实体在建立相互信任之前交换密钥、完成认证。这种认证方法通常被用在路由协议和网络应用中，可以增强对等体之间通信的安全性。

密钥链提供了一种包含密钥控制和基于生命周期的安全机制，它将一连串的密钥通过生命周期联系在一起，并将它们按照序号挂在密钥链里。密钥链在使用时会依次比对链中的各个密钥，找到密钥则通过验证。

为了发挥生命周期的作用，在使用密钥链之前，必须要定义密钥的有效时间。并且为了保持稳定性，最好能同时使用一个以上的有效密钥。

16.2 配置 Key Chain

16.2.1 创建/删除密匙链

表16-1 创建/删除密匙链

命令	操作	说明
key chain *keychain-name*	创建密钥链，并进入密匙链配置模式	keychain-name: 密匙链名称，不超过 20 个字符；缺省情况下，未创建密匙链
no key chain *keychain-name*	删除创建的密匙链	

16.2.2 创建/删除密匙

只有密钥中配置了密钥字符串，该密钥才会被使用。

表16-2 创建/删除密匙

命令	操作	说明
key *key-id*	创建密匙，并进入密匙配置模式	key-id: 密匙 ID，取值范围为 1~31；缺省情况下，密钥链中未创建密钥

命令	操作	说明
no key *key-id*	删除创建的密匙	

16.2.3 创建/删除密匙字符串

在密匙配置模式下，使用下表的命令配置密钥的字符串，如果不设置发送或接收的有效时间，则密钥永久有效。

表16-3 创建/删除密匙字符串

命令	操作	说明
key-string *string*	创建密匙字符串	string: 密钥字符串，取值范围为 0～255；缺省情况下，未配置密匙字符串
no key-string *string*	删除创建的密匙字符串	

16.2.4 配置密匙有效接收/发送时间

下表的命令配置密钥有效接收/发送的时间，当时间到期以后该密钥无效。start-time和end-time格式的规则请参考配置举例。

表16-4 配置密匙有效接收时间

命令	操作	说明
accept-lifetime *start-time end-time*	配置密钥的有效接收时间	start-time: 密钥有效接收开始时间，end-time: 密匙有效接收结束时间；格式可以为：HH:MM:SS <1-31> MONTH <1993-2035> 或HH:MM:SS MONTH <1-31> <1993-2035>； 缺省情况下，密钥接收永久有效
no accept-lifetime	删除配置的密匙有效接收时间	

16-5 配置密匙有效发送时间

命令	操作	说明
send-lifetime *start-time end-time*	配置密钥的有效发送时间	start-time: 密钥有效发送开始时间，end-time: 密匙有效发送结束时间；格式可以为：HH:MM:SS <1-31> MONTH <1993-2035> 或HH:MM:SS
no send-lifetime	删除配置的密匙有效发送时间	

命令	操作	说明
		MONTH <1-31> <1993-2035>； 缺省情况下，密钥发送永久有效

16.3 Key Chain 显示与维护

表16-6 Key Chain显示与维护

命令	操作	说明
show key chain [*keychain-name*]	显示密钥链的配置信息	keychain-name: 密匙链名称，不超过 20 个字符

16.4 配置举例

16.4.1 配置步骤

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# key chain test	创建名为 test 的密钥链，并且进入密钥链配置模式
Switch(config-keychain)# key 1	创建 ID 为 1 的密钥，并且进入密钥配置模式
Switch(config-keychain-key)# key-string ##test_keystring_1##	配置密钥字符串
Switch(config-keychain-key)# accept-lifetime 0:0:1 1 jan 2012 infinite	配置密钥的合法接收时间
Switch(config-keychain)# key 2	创建 ID 为 2 的密钥，并且进入密钥配置模式
Switch(config-keychain-key)# key-string ##test_keystring_2##	配置密钥字符串
Switch(config-keychain-key)# send-lifetime 0:0:1 2 jan 2012 infinite	配置密钥的合法发送时间

16.4.2 命令验证

根据上述配置步骤，显示密钥链信息：

```
Switch # show key chain
```

```
key chain test:
    key 1 -- text "key-string ##test_keystring_1##"
      accept-lifetime <00:00:01 Jan 01 2012> - <infinite>
      send-lifetime <always valid> - <always valid> [valid now]
    key 2 -- text "key-string ##test_keystring_2##"
      accept-lifetime <always valid> - <always valid> [valid now]
      send-lifetime <00:00:01 Jan 02 2012> - <infinite>
```

17 Port-Block 配置

17.1 Port-Block 简介

Port-block 只对二层组播报文有效，包含三层头信息的组播报文将不被阻塞。默认情况下，端口泛洪报文都是没有目的 MAC 地址的。如果这些报文被送到保护端口上，将有可能出现安全问题。为了避免目的 MAC 地址未知或者已知的单播或组播传输到其他端口，可以阻塞该端口以避免发送单播或者组播出去。

17.2 配置 Port Block

17.2.1 创建端口阻塞

用户可以根据实际情况，选择配置以下五种不同的端口阻塞：known-unicast（对目的 MAC 地址已知的单播进行阻塞）；known-multicast（对目的 MAC 地址已知的组播进行阻塞）、unknown-unicast（对目的 MAC 地址未知的单播进行阻塞）、unknown-multicast（对目的 MAC 地址未知的组播进行阻塞）以及 broadcast（对广播进行阻塞）。

表17-1 创建端口阻塞

命令	操作	说明
port-block { **known-unicast** | **known-multicast** | **unknown-unicast** | **unknown-multicast** | **broadcast** }	创建端口阻塞	缺省情况下，对 MAC 地址已知的单播和组播都是不阻塞的；对 MAC 地址未知的单播和组播都是不阻塞的；对广播也是不阻塞的
no port-block { **known-unicast** | **known-multicast** | **unknown-unicast** | **unknown-multicast** | **broadcast** }	删除配置的端口阻塞	

17.2.2 显示端口阻塞信息

表17-2 显示端口阻塞信息

命令	操作	说明
show port-block [**interface** *if-name*]	显示所有端口或指定端口的 port-block 配置信息	此处 if-name 只能为物理端口或 AGG 端口

17.3 配置举例

17.3.1 配置步骤

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# port-block unknown-unicast	对 MAC 地址未知的单播阻塞
Switch(config-if)# end	退出全局配置模式

17.3.2 验证配置

显示端口的port-block配置信息：

```
Switch # show port-block interface eth-0-1
  Known unicast blocked: Enabled
  Known multicast blocked: Disabled
  Unknown unicast blocked: Disabled
  Unknown multicast blocked: Disabled
  Broadcast blocked: Disabled
```

18 MAC 地址认证配置

18.1 MAC 地址认证简介

MAC 认证是一种基于接口和 MAC 地址对用户的网络访问权限进行控制的认证方法，不需要用户在终端安装客户端，也不用手动输入用户名和密码。当接口启用了 MAC 认证，且设备在该接口上检测到用户的 MAC 地址后，就会开启对用户的认证操作。若该用户认证成功，则能通过端口访问网络；如果失败，该用户的 MAC 地址就会被设置为静默 MAC 地址。该认证方法的操作比较简单，存在一定的安全隐患，用户的 MAC 地址容易遭到仿冒。可通过静默定时器的设置，在静默期内不对认证失败用户的报文进行认证处理，直接丢弃。

目前设备支持的 MAC 认证方式有：RADIUS 服务器认证方式与本地认证方式。RADIUS 服务器认证方式需要将设备作为 RADIUS 客户端，与 RADIUS 服务器进行配合共同完成 MAC 认证操作；本地认证则只需要在设备上进行认证，设置用户名与密码即可。

总体来说，MAC 认证方法不适用于大型网络，建议用户在中小型网络中使用。例如，可以在网络打印机或者 IP 电话等终端设备上使用。

18.2 开启 MAC 地址认证

18.2.1 全局开启 MAC 地址认证

表18-1 全局开启MAC地址认证

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# auth-mac system-auth-ctrl	全局模式下，开启 MAC 地址认证功能	缺省情况下，全局的 MAC 地址认证功能处于关闭状态

18.2.2 接口开启 MAC 地址认证

表18-2 接口开启MAC地址认证

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-
Switch(config-if)# auth-mac port-control	接口配置模式下，开启 MAC 地址认证功能	缺省情况下，接口的 MAC 地址认证功能处于关闭状态

18.3 配置 MAC 认证域

18.3.1 指定 MAC 默认认证域

使用**domain**命令添加了相关域后，用户可以使用**auth-mac domain default enable**命令配置MAC认证默认的域。

表18-3 指定MAC默认认证域

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# auth-mac domain default enable test	全局模式下，指定 MAC 默认认证域	-

18.3.2 指定接口的 MAC 认证域

使用**domain**命令添加了相关域后，用户可以使用**auth-mac mandatory-domain**命令配置指定的端口认证所属的域，否则采用默认的MAC认证域。

表18-4 指定接口的MAC认证域

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-

命令举例	操作	说明
Switch(config-if)# auth-mac mandatory-domain test	指定接口的 MAC 认证域	缺省情况下，未指定 MAC 地址认证用户使用的认证域，采用默认的 MAC 认证域

18.4 配置 MAC 地址认证定时器

配置MAC地址认证定时器参数信息：

- 下线检测定时器（**offline-detect**）：用来设置在线用户空闲超时的时间间隔，取值范围为10~65535，单位为秒。若设备在一个下线检测定时器间隔之内没有收到在线用户的报文，将切断该用户的连接，下线检测定时器默认的值为300秒。需要注意的是，MAC老化的默认时间也为300秒，尽量不要主动更改MAC老化的时间，否则会导致MAC下线时间异常。
- 静默定时器（**quiet**）：用来设置用户认证失败以后，设备需要等待的时间间隔，取值范围为1~65535，单位为秒。在静默期间，设备不对来自认证失败用户的报文进行认证处理，直接丢弃。静默期后，如果设备再次收到该用户的报文，则依然可以对其进行认证处理。

表18-5 配置MAC地址认证定时器

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# auth-mac timeout offline-detect 180	配置下线检测定时器的值	缺省情况下，下线检测定时器的值为 300 秒，静默定时器的值为 60 秒

18.5 配置端口的 MAC 地址认证下线检测功能

表18-6 配置端口的MAC地址认证下线检测功能

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-

命令举例	操作	说明
Switch(config-if)# auth-mac offline-detect enable	配置端口的 MAC 地址认证下线检测功能	缺省情况下，端口开启 MAC 地址认证下线检测功能

18.6 显示与维护

完成上述配置后，可以使用下面的命令显示MAC认证运行的情况。显示的信息主要包括：全局及端口的配置信息、认证报文统计信息以及认证用户信息。

表18-7 显示与维护

命令	操作	说明
show auth-mac [**interface** *if-number*]	显示全局及指定端口的 MAC 地址认证相关信息	if-number: 端口编号；若指定的端口上未使能MAC地址认证，则不显示该端口任何信息
show auth-mac session	显示当前 MAC 地址认证在线用户的详细信息	-

18.7 配置举例

18.7.1 简介

下面的例子使用 RADIUS 服务器认证方式进行 MAC 认证，将 Switch 作为 RADIUS 客户端，与 RADIUS 服务器进行配合完成用户的认证操作。

18.7.2 拓扑

图 18-1 MAC 认证基本拓扑图

18.7.3 配置步骤

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# auth-mac system-auth-ctrl	全局启用 MAC 认证控制
Switch(config)# interface eth-0-25	指定要配置的接口，进入接口配置模式
Switch(config)# switchport mode access	设置 Eth-0-25 为 access 模式
Switch(config-if)# auth-mac port-control	在接口上启用 MAC 认证
Switch(config-if)# no shutdown	确定端口使能
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface vlan 1	进入 VLAN 1
Switch(config-if)# ip address 192.168.100.1/24	设置 VLAN 1 的 IP 地址
Switch(config)# interface eth-0-26	进入接口配置模式.
Switch(config-if)# no switchport	配置接口为路由端口
Switch(config-if)# ip address 202.38.100.1/24	在此接口上配置 IP 地址
Switch(config-if)# no shutdown	确定端口使能
Switch(config-if)# exit	退出接口配置模式.
Switch(config)# radius-server host 202.38.100.7	为 RADIUS 服务器配置 IPv4 地址
Switch(config)# radius-server host 2001:1000::1	为 RADIUS 服务器配置 IPv6 地址
Switch(config)# radius-server key test	配置 RADIUS 服务器的共享密钥
Switch(config)#radius scheme mac-server	配置名为 mac-server 的模板
Switch(config-scheme)# authentication server 202.38.100.7	关联认证服务器 202.38.100.7
Switch(config-scheme)# exit	退出模板配置模式
Switch(config)#domain domain1	配置名为 domain1 的域名
Switch(config-domain)# authentication radius-scheme mac-server	关联模板 mac-server
Switch(config-domain)#exit	退出域配置模式

命令举例	操作步骤
Switch(config)# auth-mac domain default enable domain1	配置 MAC 认证的默认域为 domain1
Switch(config)# end	退出全局配置模式
Switch# show auth-mac	验证管理 MAC 认证的配置
Switch# show auth-mac interface eth-0-25	验证在 eth-0-25 的 MAC 认证的配置

可选参数设置步骤如下表所示：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# radius-server deadtime 10	设置重新激活 RADIUS 服务器的等待时间
Switch(config)# radius-server retransmit 5	设置 RADIUS 请求发送到服务器的最大可以失败的次数
Switch(config)# radius-server timeout 10	设置 RADIUS 服务器无响应的超时时间
Switch(config)# auth-mac timeout offline-detect 300	指定 MAC 认证下线检测超时时间
Switch(config)# auth-mac timeout quiet 60	指定 MAC 认证静默超时时间
Switch(config)# interface eth-0-25	进入接口配置模式
Switch(config-if)# auth-mac offline-detect enable	开启下线检测功能
Switch(config-if)# auth-mac mandatory-domain domain1	接口下指定 MAC 认证域，若不指定则使用默认域

18.7.4 命令验证

通过如下步骤，显示 MAC 认证的配置结果：

```
Switch# show auth-mac
Global MAC authentication information:
   Mac Authentication              : Enabled
   RADIUS server address: 202.38.100.7:1812
   Next radius message ID: 46
   RADIUS server address: 2001:1000::1
   Next radius message ID: 0
   Default domain name             : domain1
   Offline detect timeout          : 300
   Quiet period                    : 60
   Online users                    : 1
```

```
Switch# show auth-mac interface eth-0-25

 MAC authentication info for interface      : eth-0-25
   Authentication state                     : Enabled
   Domain name                              : Default domain
   Offline detection                        : enable
   Current online users                     : 1
```

IP 路由配置指导目录

1 IP 单播路由配置

路由是通信网络中常见的要素之一，IP 路由的过程即根据 IP 地址转发报文的过程。通过路由器可以实现报文转发和路由选择，路由器支持静态路由与动态路由。本章节的内容主要介绍静态路由以及 ECMP 负载均衡的相关配置。

1.1 静态路由简介

静态路由一般由用户或管理员手工配置，使数据包通过预设的路径到达指定的目的地址。静态路由主要应用于小型网络中，当设备或者路由数量有限时，只需考虑使用静态路由就可以满足工作需求。合理设置和使用静态路由可以改进网络性能，并可为重要的网络应用保证带宽。静态路由也存在一定的局限性，当网络发生故障或者拓扑发生变化后，可能会出现路由不可达，从而导致网络中断。此时必须由网络管理员手工修改静态路由的配置。

1.2 配置静态路由

1.2.1 配置 IP 地址

配置静态路由之前，需要先配置 IP 地址。一个接口上可以有一个主 IP 地址和多个从 IP 地址。交换机产生的报文使用主 IP 地址。因此，在同一网段的所有的交换机和接入服务器可以实现网络共享。

用户可以使用 **no ip address** 命令删除接口的 IP 地址，从而禁用该端口上的 IP 路由功能。如果系统检测到另外一个主机正在使用这个 IP 地址，系统将会在控制台上输出错误消息。

表1-1 配置IP地址

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-

命令举例	操作	说明
Switch(config-if)# ip address 10.108.1.27 255.255.255.0	配置 10.108.1.27 为主 IP 地址、192.31.7.17 和 192.31.8.17 为从 IP 地址	缺省情况下，接口上未配置 IP 地址；secondary 这个关键字允许用户配置最多 15 个从 IP 地址
Switch(config-if)# ip address 192.31.7.17/24 secondary		
Switch(config-if)# ip address 192.31.8.17 255.255.255.0 secondary		

1.2.2 创建静态路由

当交换机无法动态地与目的地址建立路由时，使用静态路由是个不错的选择。

表1-2 创建静态路由

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# ip route 172.31.0.0 255.255.0.0 172.31.6.6	创建一条静态路由	缺省情况下，未配置静态路由

用户还可以配置路由泄露，如下表所示。

表1-3 配置静态路由泄露

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# ip route 22.12.31.0/24 23.0.0.2	创建一条静态路由	缺省情况下，未配置静态路由
Switch(config)# ip route vrf test1 23.12.31.0/24 11.15.0.15	配置静态路由泄露	-

1.2.3 配置静态路由条目数的最大值

用户可配置的最大静态路由条目不得小于当前已配置的静态路由条目数，且不得大于系统的路由规格。

表1-4 配置静态路由条目数的最大值

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# max-static-routes 10	配置静态路由条目数的最大值为 10	静态路由条目数的取值范围为 1～65535；缺省情况下，默认值为 1024 条

1.2.4 显示与维护

将路由加入路由表后，用户可以使用 **show ip route** 或者 **show ip route static** 命令显示任何有效的动态和静态路由。

表1-5 显示与维护

命令	操作	说明
show ip route [**vrf** *vrf-name*] [*ip-address* | *prefix/prefix-length* | *protocol-name*]	显示当前的路由表状态	vrf-name: VRF 实例名； protocol-name: 路由协议名，可以是关键字 **connected**、**static** 或者 **summary**。如果指定一个路由协议，使用其中的一个关键字：**bgp**，**ospf**，或者 **rip**
show ip route [**vrf** *vrf-name*] **summary**	显示各种类型路由的汇总信息	vrf-name: VRF 实例名

1.3 配置 ECMP 负载均衡

ECMP 路由全称为等价多路径路由，当存在等价多条路径到达同一目的地址时，为目的地址增加规则对应多个下一跳地址，通过这些路径转发数据、增加带宽。

1.3.1 配置 ECMP 负载均衡模式

用户可以根据实际情况，配置 ECMP 动态或静态负载均衡模式。

表1-6 配置ECMP动态负载均衡模式

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# ecmp load-balance-mode dynamic	配置 ECMP 动态负载均衡模式	缺省情况下，系统默认为静态负载均衡模式

表1-7 配置ECMP静态负载均衡模式

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# ecmp load-balance-mode static	配置 ECMP 静态负载均衡模式	缺省情况下，系统默认为静态负载均衡模式

说明

配置 ECMP 静态或动态负载均衡模式时，交换机路由信息必须为空。

1.3.2 配置 ECMP 的 HASH 计算

下表显示了配置 ECMP 负载均衡模式使用外层头的源 IP 地址，目的 IP 地址以及内层头的目的 IP 地址来计算 HASH 值。

表1-8 配置ECMP的HASH计算

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# ecmp hash-field-select ipda ipsa inner-ipda	配置 ECMP 的 HASH 计算	缺省情况下，系统默认为 ipsa、ipda

说明

可以使用这些字段计算 HASH 值：ipda、ipsa、ip-protocol、sourceport、destport、vxlan-vni、nvgre-vsid、inner-ipda、inner-ipsa、inner-ip-protocol、inner-sourceport、inner-destport

1.3.3 检查 ECMP 配置信息

表1-9 检查ECMP配置信息

命令	操作	说明
show ecmp information	显示当前 ECMP 的配置信息	-

1.4 配置举例

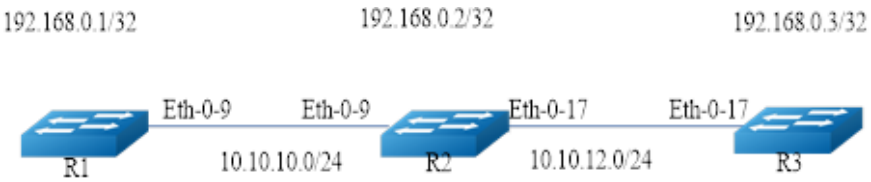
1.4.1 介绍

本小节介绍了在一个简单的网络拓扑结构下使能静态路由的实例。静态路由在小型网络中非常有用，可提供若干个目的地可达的简单解决方案，而大型网络一般使用动态路由协议。静态路由是由网络前缀（主机地址）和下一跳（网关）组成。

路由器 R1 上配置了三个静态路由，一个是远程网络地址10.10.12.0/24，另外两个是路由器 R2 和 R3 的环回地址（主机地址）。路由器 R3 上配置了一条默认地静态路由，相当于单独的静态路由配置使用相同的网关或下一跳地址。路由器 R2 有两条路由，每一条路由的目的地址都是远端路由器的环回口地址。

1.4.2 拓扑

图 1-1 静态路由配置拓扑图



1.4.3 配置步骤

R1 的配置步骤如下：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-9	进入接口配置模式
Switch(config-if)# no shutdown	端口 UP
Switch(config-if)# no switchport	设置为三层接口
Switch(config-if)# ip address 10.10.10.1/24	配置 IP 地址
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface loopback 0	指定需要配置的环回接口
Switch(config-if)# ip address 192.168.0.1/32	配置 IP 地址和 32bit 掩码，作为主机地址
Switch(config-if)# exit	退出接口配置模式
Switch(config)# ip route 10.10.12.0/24 10.10.10.2 Switch(config)# ip route 192.168.0.2/32 10.10.10.2 Switch(config)# ip route 192.168.0.3/32 10.10.10.2	指定目的前缀和掩码网关所需网络，例如，10.10.12.0/24，为它们添加网关（对此所有情况下为 10.10.10.2）。由于 R2 是唯一可用的下一跳，可以配置默认路由而不是配置为单独的地址，见 R3 配置

R2 的配置步骤如下：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-9	进入接口配置模式
Switch(config-if)# no shutdown	端口 UP
Switch(config-if)# no switchport	设置为三层接口
Switch(config-if)# ip address 10.10.10.2/24	配置 IP 地址
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface eth-0-17	进入接口配置模式
Switch(config-if)# no shutdown	端口 UP
Switch(config-if)# no switchport	设置为三层接口
Switch(config-if)# ip address 10.10.12.2/24	设置 IP 地址

命令举例	操作步骤
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface loopback 0	指定需要配置的环回接口
Switch(config-if)# ip address 192.168.0.2/32	配置 IP 地址和 32bit 掩码，作为主机地址
Switch(config-if)# exit	退出接口配置模式
Switch(config)# ip route 192.168.0.1/32 10.10.10.1 Switch(config)# ip route 192.168.0.3/32 10.10.12.3	指定目的和掩码，添加网关

R3 的配置步骤如下：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-17	进入接口配置模式
Switch(config-if)# no shutdown	端口 UP
Switch(config-if)# no switchport	设置为三层接口
Switch(config-if)# ip address 10.10.12.3/24	设置 IP 地址
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface loopback 0	指定需要配置的环回接口
Switch(config-if)# ip add 192.168.0.3/32	配置 IP 地址和 32bit 掩码，作为主机地址
Switch(config-if)# exit	退出接口配置模式
Switch(config)# ip route 0.0.0.0/0 10.10.12.2	指定 10.10.12.2 作为到达任意网络的默认网关，因为 10.10.12.2 是唯一的一条可以指定的默认网关，而不是单个网络或主机的指定网关

1.4.4 命令验证

1. 根据上述R1的配置步骤，显示当前的路由表状态：

```
R1# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
```

```
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        [*] - [AD/Metric]
        * - candidate default
C       10.10.10.0/24 is directly connected, eth-0-9
C       10.10.10.1/32 is in local loopback, eth-0-9
S       10.10.12.0/24 [1/0] via 10.10.10.2, eth-0-9
C       192.168.0.1/32 is directly connected, loopback0
S       192.168.0.2/32 [1/0] via 10.10.10.2, eth-0-9
S       192.168.0.3/32 [1/0] via 10.10.10.2, eth-0-9
```

2. 根据上述R2的配置步骤，显示当前的路由表状态：

```
R2# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        [*] - [AD/Metric]
        * - candidate default
C       10.10.10.0/24 is directly connected, eth-0-9
C       10.10.10.2/32 is in local loopback, eth-0-9
C       10.10.12.0/24 is directly connected, eth-0-17
C       10.10.12.2/32 is in local loopback, eth-0-17S       192.168.0.1/32 [1/0] via
10.10.10.1, eth-0-9
C       192.168.0.2/32 is directly connected, loopback0
S       192.168.0.3/32 [1/0] via 10.10.12.3, eth-0-17
```

3. 根据上述R3的配置步骤，显示当前的路由表状态：

```
R3# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        [*] - [AD/Metric]
        * - candidate default
```

```
Gateway of last resort is 10.10.12.2 to network 0.0.0.0
S*      0.0.0.0/0 [1/0] via 10.10.12.2, eth-0-17
C       10.10.12.0/24 is directly connected, eth-0-17
C       10.10.12.3/32 is in local loopback, eth-0-17
C       192.168.0.3/32 is directly connected, loopback0
```

2 RIP 配置

2.1 RIP 简介

RIP（Routing Information Protocol，路由信息协议）是一种较为简单的内部网关协议（Interior Gateway Protocol，IGP），主要用于规模较小的网络中。

RIP 是一种基于距离矢量（Distance-Vector）算法的协议，它通过 UDP 报文进行路由信息的交换。RIP 使用跳数（Hop Count）来衡量到达目的地址的距离，称为路由权（Routing Cost）。在 RIP 中，路由器到与它直接相连网络的跳数为 0，通过一个路由器可达的网络的跳数为 1，其余依此类推。为限制收敛时间，RIP 规定 Cost 的取值为 0～15 之间的整数，Cost 取值大于或等于 16 的跳数被定义为无穷大，即目的网络或主机不可达。

为提高性能，防止产生路由环路，RIP 支持水平分割（Split Horizon）。RIP 还可引入其它路由协议所得到的路由。

2.2 配置 RIP 的基本功能

2.2.1 开启 RIP 路由协议

表 2-1 全局开启 RIP 路由协议

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# router rip	全局开启 RIP 路由协议，并进入 RIP 协议配置模式	只有开启 RIP 路由协议，RIP 相关配置才能生效
Switch(config-router)# end	退出 RIP 协议配置模式	-

2.2.2 指定网段内使能 RIP 路由协议

系统对配置 RIP 网段的数量没有限制。可以在指定的网段内或接口上使能 RIP 路由协议。

表 2-2 指定网段内使能 RIP 路由协议

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# router rip	全局开启 RIP 路由协议，并进入 RIP 协议配置模式	只有开启 RIP 路由协议，RIP 相关配置才能生效
Switch(config-router)# network 10.99.0.0/16	在网段 10.99.0.0/16 和 192.168.7.0/24 使能 RIP 路由协议	-
Switch(config-router)# network 192.168.7.0/24		

2.2.3 配置 NBMA 网络的 RIP 邻居

此命令用来配置 NBMA（Non-Broadcast Multi-Access，非广播多点可达）网络中 RIP 邻居的 IP 地址，并以单播的形式更新报文发送到对端，而不采用正常的组播或广播的形式。通常情况下，要结合 Passive Interface（被动接口）一起使用。用户可以配置多个 RIP 邻居。

下表的例子中，RIP 更新报文将会在网段 10.108.0.0/16 相关的所有接口上发送，但是接口 eth-0-1 除外。在这种情况下，可以使用 **neighbor** 命令，系统将会发送路由更新报文到指定的邻居。

表 2-3 配置 NBMA 网络的 RIP 邻居

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# router rip	全局开启 RIP 路由协议，并进入 RIP 协议配置模式	只有开启 RIP 路由协议，RIP 相关配置才能生效
Switch(config-router)# network 10.108.0.0/16	在网段 10.108.0.0/16 使能 RIP 路由协议	-
Switch(config-router)# passive-interface eth-0-1	设置端口上禁止发送 RIP 报文	-
Switch(config-router)# neighbor 10.108.20.4	发送路由更新报文到指定的邻居 IP 地址	-

2.2.4 配置 RIP 协议版本信息

RIP 有两种版本号：RIPv1 和 RIPv2。一般只需全局配置 RIP 版本号即可，接口上指定 RIP 的发送和接收的版本信息会覆盖路由模式下配置的 RIP 版本信息。接口的 RIP 版本号详见 2.9.2 配置接口的 RIP 版本号示例。

表 2-4 配置 RIP 协议版本信息

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# router rip	全局开启 RIP 路由协议，并进入 RIP 协议配置模式	只有开启 RIP 路由协议，RIP 相关配置才能生效
Switch(config-router)# version 2	指定 RIP 路由中发送和接收的版本为 v2	缺省情况下，系统默认接收 v1 和 v2 的报文，只发送 v2 的报文

2.3 配置 RIPv2 特性

2.3.1 使能 RIPv2 的认证功能

在接口模式下，配置该命令使能 RIPv2 的认证功能。配置发送和接收 RIP 报文的方式：MD5 认证使用的钥匙链（key-chain）或者明文认证使用的密码（string）。如果 key-chain 或者 string 后面没有添加任何的内容，那么在该接口上接收和发送报文不需要进行认证。key-chain 和 string 不能同时出现，用户配置该功能时，只使用一种认证功能即可。

表 2-5 使能 RIPv2 的认证功能

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-
Switch(config-if)# no switchport	设置接口为三层接口	-
Switch(config-if)# ip rip authentication key-chain trees	发送和接收 RIP 报文时，使用钥匙链 trees	缺省情况下，未使能 RIPv2 的认证功能

2.3.2 配置 RIPv2 的认证方式

RIPv2 有两种认证方式：明文验证（text）和 MD5 加密认证（md5）。具体的配置步骤见 2.9.7 配置 RIPv2 认证示例。

表 2-6 配置 RIPv2 的认证方式

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-
Switch(config-if)# no switchport	设置接口为三层接口	-
Switch(config-if)# ip rip authentication mode md5	配置接口 RIP 验证的类型为 MD5	缺省情况下，未配置 RIPv2 的认证方式

2.4 配置防止 RIP 路由环路的方式

设置端口防止形成路由环路的方式：毒性逆转或水平分割。

2.4.1 配置水平分割

表 2-7 配置水平分割

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-
Switch(config-if)# ip rip split-horizon	配置水平分割来防止路由环路	缺省情况下，端口采用毒性逆转防止路由环路

2.4.2 配置毒性逆转

表 2-8 配置毒性逆转

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-

命令举例	操作	说明
Switch(config-if)# ip rip split-horizon poisoned	配置毒性逆转来防止路由环路	缺省情况下，端口采用毒性逆转防止路由环路

2.5 配置 RIP 路由控制

配置 RIP 的基本功能后，可配控制 RIP 路由选路的属性。

2.5.1 配置 RIP 路由的管理距离

管理距离表明了对一个路由源的信任度，它是从0到255之间的一个整数。一般情况下，这个值越高，信任等级越低。如果管理距离为255，说明不信任这个路由源，忽略从该路由源获得的所有路由。用户配置了管理距离后，当路由准备加入路由表时，系统就会根据发布路由更新的交换机IP地址进行过滤，同时对符合条件的路由修改管理距离。

表 2-9 配置 RIP 路由的管理距离

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# router rip	全局开启 RIP 路由协议，并进入 RIP 协议配置模式	只有开启 RIP 路由协议，RIP 相关配置才能生效
Switch(config-router)# network 10.10.0.0/24	在网段 10.10.0.0/24 使能 RIP 路由协议	-
Switch(config-router)# network 20.20.0.0/24	在网段 20.20.0.0/24 使能 RIP 路由协议	-
Switch(config-router)# distance 200 20.20.0.0/24	配置从 20.20.0.0 的网段来的路由的管理距离值为 200	缺省情况下，管理距离的值为 120

2.5.2 配置接口的附加度量值

使用命令配置接口接收（in）或发送（out）RIP路由时的附加度量值，下表以配置接口在发送路由时附加的度量值为例。偏移量列表可以用来改变路由的度量值，以达到某些目的（如备份链路或者负载均衡）。更多相关配置详见2.9.3配置Metric参数示例。

表 2-10 配置接口的附加度量值

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-
Switch(config-if)# no switchport	设置接口为三层接口	-
Switch(config-if)# exit	退出接口配置模式	-
Switch(config)# router rip	全局开启 RIP 路由协议，并进入 RIP 协议配置模式	只有开启 RIP 路由协议，RIP 相关配置才能生效
Switch(config-router)# offset-list 21 out 10	配置接口在发送路由时附加的度量值为 10	缺省情况下，未配置接口的附加度量值

2.6 控制 RIP 路由的发送和接收

2.6.1 配置 RIP 生成默认路由

该命令生成的默认路由不会下载到 FIB 表中，只会被 RIP 邻居学到。

表 2-11 配置 RIP 生成默认路由

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# router rip	全局开启 RIP 路由协议，并进入 RIP 协议配置模式	只有开启 RIP 路由协议，RIP 相关配置才能生效
Switch(config-router)# version 2	指定 RIP 路由中发送和接收的版本为 v2	缺省情况下，系统默认接收 v1 和 v2 的报文，只发送 v2 的报文
Switch(config-router)# network 192.168.16.0/24	在网段 192.168.16.0/24 使能 RIP 路由协议	-
Switch(config-router)# default-information originate	配置 RIP 路由表中生成一条默认路由	-

2.6.2 禁用接口发送/接收 RIP 报文

表 2-12 禁用接口发送 RIP 报文

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-
Switch(config-if)# no switchport	设置接口为三层接口	-
Switch(config-if)# ip rip send-packet	禁用接口发送 RIP 报文	缺省情况下，端口可发送 RIP 报文

表 2-13 禁用接口接收 RIP 报文

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-
Switch(config-if)# no switchport	设置接口为三层接口	-
Switch(config-if)# ip rip receive-packet	禁用接口接收 RIP 报文	缺省情况下，端口可接收 RIP 报文

2.6.3 过滤发送/接收 RIP 路由

使用关键字 out 用于过滤发送的 RIP 路由，而关键字 in 用于过滤接收的 RIP 路由。更多相关配置详见 2.9.6 配置 RIP 路由过滤列表示例。

表 2-14 过滤发送 RIP 路由

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# router rip	全局开启 RIP 路由协议，并进入 RIP 协议配置模式	只有开启 RIP 路由协议，RIP 相关配置才能生效
Switch(config-router)# distribute-list prefix 1 out	过滤发送的 RIP 路由	“1”为前缀列表名

表 2-15 过滤接收 RIP 路由

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-

命令举例	操作	说明
Switch(config)# router rip	全局开启 RIP 路由协议，并进入 RIP 协议配置模式	只有开启 RIP 路由协议，RIP 相关配置才能生效
Switch(config-router)# distribute-list prefix 2 in	过滤接收的 RIP 路由	“2”为前缀列表名

2.7 配置 RIP 定时器

通过配置 RIP 各个定时器 Update、Timeout 和 Invalid 的值，调整路由协议的性能，提升 RIP 网络性能。

这三个定时器的定义如下：

- Update：路由更新时间；
- Timeout：路由老化时间，如果在老化时间内没有收到关于某条路由的更新报文，则该条路由在路由表中的度量值将会被设置为16，此时该条路由将不能用于转发报文；
- Invalid：路由的垃圾回收时间，定义了一条路由从度量值变为 16 时，直到它从路由表里被删除所经过的时间。在垃圾回收时间内，RIP 以 16 作为度量值向外发送这条路由的更新，如果垃圾回收定时器超时，该路由仍没有得到更新，则该路由将从路由表中被彻底删除。

表 2-16 配置 RIP 定时器

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# router rip	全局开启 RIP 路由协议，并进入 RIP 协议配置模式	只有开启 RIP 路由协议，RIP 相关配置才能生效
Switch(config-router)# timers basic 5 15 15	设置 RIP 路由的报文更新时间 5 秒，当超过 15 秒没有收到路由更新报文时，路由将失效。再过 15 秒，将路由从 RIP 路由表中删除	Update、Timeout 和 Invalid 的取值范围为 5~214748364，单位：秒。 Update：默认 30 秒； Timeout：默认 180 秒； Invalid：默认 120 秒

2.8 RIP 显示与维护

表 2-17 RIP 显示与维护

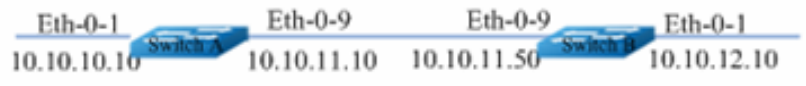
命令	操作	说明
show ip rip database [**vrf** *vrf-name*]	查看 RIP 的数据库	vrf-name：VRF 实例名
show ip rip interface [*if-name*]	显示接口的 RIP 信息	if-name：接口名称
show ip protocol rip	显示 RIP 协议的信息	-
show ip rip database database-summary [**vrf** *vrf-name*]	显示 RIP 路由的统计值	vrf-name：VRF 实例名
show resource rip	显示 RIP 路由占用的硬件资源统计	-

2.9 RIP 配置举例

2.6.1 配置 RIP 基本功能示例

i. 拓扑

图 2-1 RIP 基本配置拓扑图



ii. 配置步骤

Switch A的配置步骤如下：

命令举例	操作步骤
SwitchA# configure terminal	进入全局配置模式
SwitchA(config)# interface eth-0-1	进入接口配置模式
SwitchA(config-if)# no switchport	设置接口为三层接口
SwitchA(config-if)# ip address 10.10.10.10/24	配置 IP 地址
SwitchA(config-if)# exit	退出接口配置模式

命令举例	操作步骤
SwitchA(config)# interface eth-0-9	进入接口配置模式
SwitchA(config-if)# no switchport	设置接口为三层接口
SwitchA(config-if)# ip address 10.10.11.10/24	配置 IP 地址
SwitchA(config-if)# exit	退出接口配置模式
SwitchA(config)# router rip	启用 RIP 路由协议
SwitchA(config-router)# network 10.10.10.0/24	发布 10.10.10.0 网段到 RIP 路由协议中
SwitchA(config-router)# network 10.10.11.0/24	发布 10.10.11.0 网段到 RIP 路由协议中

Switch B的配置步骤如下：

命令举例	操作步骤
SwitchB# configure terminal	进入全局配置模式
SwitchB(config)# interface eth-0-1	进入接口配置模式
SwitchB(config-if)# no switchport	设置接口为三层接口
SwitchB(config-if)# ip address 10.10.12.10/24	配置 IP 地址
SwitchB(config-if)# exit	退出接口配置模式
SwitchB(config)# interface eth-0-9	进入接口配置模式
SwitchB(config-if)# no switchport	设置接口为三层接口
SwitchB(config-if)# ip address 10.10.11.50/24	设置 IP 地址
SwitchB(config)# router rip	启用 RIP 路由协议
SwitchB(config-router)# network 10.10.11.0/24	发布 10.10.11.0 网段到 RIP 路由协议中
SwitchB(config-router)# network 10.10.12.0/24	发布 10.10.12.0 网段到 RIP 路由协议中

iii. 命令验证

上述 Switch A 的配置结果如下：

```
SwitchA# show ip rip database
Codes: R - RIP, Rc - RIP connected, Rs - RIP static, K - Kernel,
       C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP
    Network          Next Hop        Metric From          If          Time
Rc 10.10.10.0/24                       1                  eth-0-1
Rc 10.10.11.0/24                       1                  eth-0-9
R  10.10.12.0/24    10.10.11.50        2 10.10.11.50      eth-0-9   00:02:52
SwitchA# show ip protocols rip
Routing protocol is "rip"
  Sending updates every 30 seconds with +/-5 seconds, next due in 17 seconds
  Timeout after 180 seconds, Garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Default redistribution metric is 1
  Redistributing:
  Default version control: send version 2, receive version 2
    Interface        Send    Recv    Key-chain
    eth-0-1          2       2
    eth-0-9          2       2
  Routing for Networks:
    10.10.10.0/24
    10.10.11.0/24
  Routing Information Sources:
    Gateway          Distance    Last Update    Bad Packets    Bad Routes
    10.10.11.50           120    00:00:22                 0             0
  Number of routes (including connected): 3
  Distance: (default is 120)
SwitchA# show ip rip interface
eth-0-1 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIP packets
    Send RIP packets
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IP interface address:
      10.10.10.10/24
eth-0-9 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIP packets
    Send RIP packets
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IP interface address:
      10.10.11.10/24
SwitchA# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       [*] - [AD/Metric]
       * - candidate default
C        10.10.10.0/24 is directly connected, eth-0-1
C        10.10.10.10/32 is in local loopback, eth-0-1
C        10.10.11.0/24 is directly connected, eth-0-9
C        10.10.11.10/32 is in local loopback, eth-0-9
R        10.10.12.0/24 [120/2] via 10.10.11.50, eth-0-9, 00:25:50
```

2.6.2 配置接口的 RIP 版本号示例

i. 拓扑

图 2-2 配置 RIP 版本号拓扑图

ii. 配置步骤

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# router rip	启用 RIP 路由协议.
Switch(config-router)# exit	退出路由模式
Switch(config)# interface eth-0-9	进入接口配置模式
Switch(config-if)# ip rip send version 1 2	设置接口发送的 RIP 版本信息
Switch(config-if)# ip rip receive version 1 2	设置接口接收的 RIP 版本信息
Switch(config-if)# quit	退出接口配置模式
Switch(config)# interface eth-0-20	进入接口配置模式
Switch(config-if)# ip rip send version 1 2	设置接口发送的 RIP 版本信息
Switch(config-if)# ip rip receive version 1 2	设置接口接收的 RIP 版本信息

iii. 命令验证

- Switch A的配置结果显示如下：

```
Switch# show running-config
interface eth-0-9
 no switchport
 ip address 10.10.11.10/24
!
router rip
 network 10.10.11.0/24
```

- Switch B的配置结果显示如下：

```
Switch# show ip rip database
Codes: R - RIP, Rc - RIP connected, Rs - RIP static, K - Kernel,
       C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP
    Network          Next Hop        Metric From          If          Time
R   10.0.0.0/8                            1               eth-0-9
Rc 10.10.11.0/24                         1              eth-0-9
Rc 10.10.12.0/24                         1              eth-0-20
Switch# show ip protocols rip
Routing protocol is "rip"
  Sending updates every 30 seconds with +/-5 seconds, next due in 1 seconds
  Timeout after 180 seconds, Garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Default redistribution metric is 1
  Redistributing:
  Default version control: send version 2, receive version 2
    Interface        Send      Recv     Key-chain
    eth-0-9          1 2       1 2
    eth-0-20         1 2       1 2
  Routing for Networks:
    10.10.11.0/24
    10.10.12.0/24
  Routing Information Sources:
    Gateway          Distance   Last Update   Bad Packets   Bad Routes
    10.10.11.10           120   00:00:22                0             0
    10.10.12.50           120   00:00:27                0             0
  Number of routes (including connected): 3
  Distance: (default is 120)
Switch# show ip rip inter
eth-0-9 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIPv1 and RIPv2 packets
    Send RIPv1 and RIPv2 packets
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IP interface address:
```

```
        10.10.11.50/24
eth-0-20 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIPv1 and RIPv2 packets
    Send RIPv1 and RIPv2 packets
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IP interface address:
      10.10.12.10/24
Switch# show run
interface eth-0-9
 no switchport
 ip address 10.10.11.50/24
 ip rip send version 1 2
 ip rip receive version 1 2
!
interface eth-0-20
 no switchport
 ip address 10.10.12.10/24
 ip rip send version 1 2
 ip rip receive version 1 2
!
router rip
 network 10.10.11.0/24
 network 10.10.12.0/24
```

- Switch C的配置结果显示如下：

```
Switch# show running-config
interface eth-0-20
 no switchport
 ip address 10.10.12.50/24
!
router rip
 network 10.10.12.0/24
```

2.6.3 配置 Metric 参数示例

i. 介绍

附加度量值是附加在 RIP 路由上的输入、输出度量值，包括发送附加度量值和接收附加度量值。发送附加度量值不会改变路由表中的路由度量值，仅当接口发送 RIP 路由信息时才会添加到发送路由上；接收附加度量值会影响接收到的路由度量值，接口接收到一条合法的 RIP 路由时，在将其加入路由表前会把度量值附加到该路由上。附加度量值一般包括如下的参数：

- 指定增加路由 Metric 的 ACL 参数说明如下：

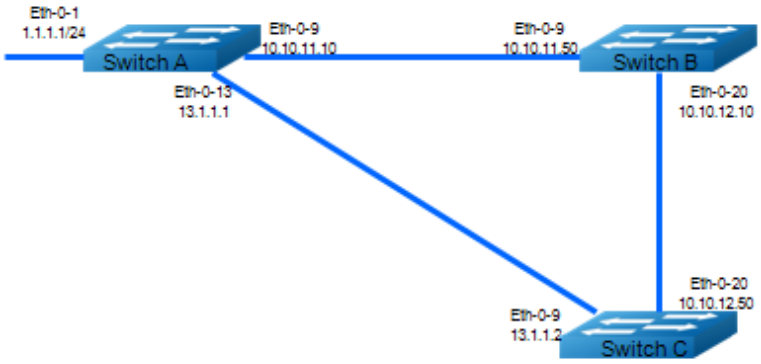
- **In**：应用在从邻居路由器学习到的 RIP 的路由上
- **Out**：应用在发布给邻居路由器 RIP 通告上

- 匹配 ACL 路由的偏移值 Metric
- 应用偏移列表的接口

如果有一个路由匹配全局偏移表（不指定接口）和一个基于接口的偏移列表，此时基于接口的偏移列表优先。在这种情况下，基于接口的偏移列表的度量值会被加到路由上。

ii. 拓扑

图 2-3 配置 Metric 参数拓扑图



iii. 配置文件

Switch A：

```
interface eth-0-1
no switchport
ip address 1.1.1.1/24
!
interface eth-0-9
no switchport
ip address 10.10.11.10/24
!
interface eth-0-13
no switchport
ip address 13.1.1.1/24
```

```
!
router rip
network 1.1.1.0/24
network 10.10.11.0/24
network 13.1.1.0/24
```

Switch B：

```
interface eth-0-9
no switchport
ip address 10.10.11.50/24
!
interface eth-0-20
no switchport
ip address 10.10.12.10/24
!
router rip
network 10.10.11.0/24
network 10.10.12.0/24
```

Switch C：

```
interface eth-0-13
no switchport
ip address 13.1.1.2/24
!
interface eth-0-20
no switchport
ip address 10.10.12.50/24
!
router rip
network 10.10.12.0/24
network 13.1.1.0/24
```

iv. 配置示例

查看Switch C的RIP路由表：

```
Switch# show ip route rip
R        1.1.1.0/24 [120/2] via 13.1.1.1, eth-0-13, 00:07:46
R        10.10.11.0/24 [120/2] via 13.1.1.1, eth-0-13, 00:07:39
                               [120/2] via 10.10.12.10, eth-0-20, 00:07:39
Change router 1.1.1.0/24 via 10.10.12.10
```

例：在 Switch A 上将 1.1.1.0 在 Eth-0-13 接口上增加 metric 3：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)#ip access-list ripoffset	创建 ACL
Switch(config-ip-acl)#permit any 1.1.1.0 0.0.0.255 any	匹配相应的网段
Switch(config-ip-acl)# router rip	启用 RIP 路由协议
Switch(config-router)# offset-list ripoffset out 3 eth-0-13	设置偏移列表的 Metric 值

v. 命令验证

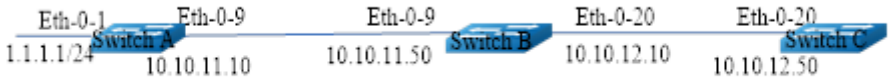
Switch C 的配置结果如下：

```
Switch# show ip route rip

R       1.1.1.0/24 [120/3] via 10.10.12.10, eth-0-20, 00:00:02
R       10.10.11.0/24 [120/2] via 13.1.1.1, eth-0-13, 00:11:40
                      [120/2] via 10.10.12.10, eth-0-20, 00:11:40
```

2.6.4 配置管理距离示例

i. 拓扑

图 2-4 配置管理距离示例



ii. 配置文件

Switch A：

```
interface eth-0-1
no switchport
ip address 1.1.1.1/24
!
interface eth-0-9
no switchport
```

```
ip address 10.10.11.10/24
!
router ospf
network 1.1.1.0/24 area 0
network 10.10.11.0/24 area 0
!
router rip
network 1.1.1.0/24
network 10.10.11.0/24
```

Switch B：

```
interface eth-0-9
no switchport
ip address 10.10.11.50/24
!
interface eth-0-20
no switchport
ip address 10.10.12.10/24
!
router ospf
network 10.10.11.0/24 area 0
network 10.10.12.0/24 area 0
!
router rip
network 10.10.11.0/24
network 10.10.12.0/24
```

Switch C：

```
interface eth-0-20
no switchport
ip address 10.10.12.50/24
!
router ospf
network 10.10.12.0/24 area 0
!
router rip
network 10.10.12.0/24
```

iii. 配置示例

查看Switch C的RIP路由表：

```
Switch# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
```

```
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        [*] - [AD/Metric]
        * - candidate default
O         1.1.1.0/24 [110/3] via 10.10.12.10, eth-0-20, 01:05:49
O         10.10.11.0/24 [110/2] via 10.10.12.10, eth-0-20, 01:05:49
C         10.10.12.0/24 is directly connected, eth-0-20
C         10.10.12.50/32 is in local loopback, eth-0-20
```

通过以下步骤改变交换机C上的1.1.1.0网段的RIP管理距离：

命令举例	操作步骤
Switch# configure terminal	进入配置模式
Switch(config)#ip access-list ripdistancelist	创建 ACL
Switch(config-ip-acl)#permit any 1.1.1.0 0.0.0.255 any	匹配相应的网段
Switch(config-ip-acl)# router rip	启用 RIP 路由协议
Switch(config-router)# distance 100 0.0.0.0/0 ripdistancelist	设置 RIP 路由的管理距离为 100 （0.0.0.0/0 是源 IP 前缀，所有匹配这个网段的路由的管理距离将被设为 100）

iv. 命令验证

Switch C 的配置结果如下：

```
Switch# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       [*] - [AD/Metric]
       * - candidate default
R         1.1.1.0/24 [100/3] via 10.10.12.10, eth-0-20, 00:00:02
O         10.10.11.0/24 [110/2] via 10.10.12.10, eth-0-20, 01:10:42
C         10.10.12.0/24 is directly connected, eth-0-20
C         10.10.12.50/32 is in local loopback, eth-0-20
```

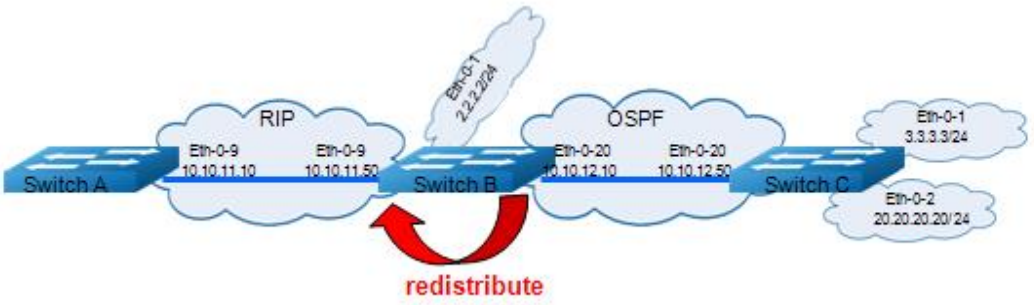
2.6.5 配置路由重分布示例

i. 介绍

用户可以将静态路由、直连路由以及其他路由协议，例如OSPF的路由，重分布到RIP中并发送给它的邻居。默认RIP重发布的Metric为1，最大值为16。将特定的路由重发布到RIP上，其度量值可以是默认的，也可以是修改后的。下面例子讲述如何重分布其他的路由信息到RIP。

ii. 拓扑

图 2-5 配置重分布拓扑图



v. 配置文件

Switch A：

```
interface eth-0-9
no switchport
ip address 10.10.11.10/24
!
router rip
network 10.10.11.0/24
```

Switch B：

```
interface eth-0-1
no switchport
ip address 2.2.2.2/24
!
interface eth-0-9
no switchport
ip address 10.10.11.50/24
!
interface eth-0-20
no switchport
ip address 10.10.12.10/24
!
```

```
router ospf
network 10.10.12.0/24 area 0
!
router rip
network 10.10.11.0/24
!
ip route 20.20.20.0/24 10.10.12.50
```

Switch C：

```
interface eth-0-1
no switchport
ip address 3.3.3.3/24
!
interface eth-0-2
no switchport
ip address 20.20.20.20/24
!
interface eth-0-20
no switchport
ip address 10.10.12.50/24
!
router ospf
network 3.3.3.0/24 area 0
network 10.10.12.0/24 area 0
```

iii. 配置示例

显示Switch A的路由表信息：

```
Switch# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       [*] - [AD/Metric]
       * - candidate default
C        10.10.11.0/24 is directly connected, eth-0-9
C        10.10.11.10/32 is in local loopback, eth-0-9
```

显示Switch B的路由表信息：

```
Switch# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
```

```
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        [*] - [AD/Metric]
        * - candidate default
C         2.2.2.0/24 is directly connected, eth-0-1
C         2.2.2.02/32 is in local loopback, eth-0-1
O         3.3.3.0/24 [110/2] via 10.10.12.50, eth-0-20, 01:05:41
C         10.10.11.0/24 is directly connected, eth-0-9
C         10.10.11.50/32 is in local loopback, eth-0-9
C         10.10.12.0/24 is directly connected, eth-0-20
C         10.10.12.10/24 is in local loopback, eth-0-20
S         20.20.20.0/24 [1/0] via 10.10.12.50, eth-0-20
```

Switch B的配置如下：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# router rip	启用 RIP 路由协议
Switch(config-router)#default-metric 2	指定默认的 Metric
Switch(config-router)# redistribute static	重分布静态路由
Switch(config-router)# redistribute connected	重分布直连路由
Switch(config-router)#redistribute ospf metric 5	重分布 OSPF 路由到 RIP 中
Switch(config)# router ospf	启用 OSPF 路由协议
Switch(config-router)# redistribute connected	重分布直连路由

iv. 命令验证

检查Switch A的配置结果：

```
Switch# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        [*] - [AD/Metric]
        * - candidate default
R         2.2.2.0/24 [120/3] via 10.10.11.50, eth-0-9, 00:02:36
R         3.3.3.0/24 [120/6] via 10.10.11.50, eth-0-9, 00:02:26
C         10.10.11.0/24 is directly connected, eth-0-9
C         10.10.11.10/32 is in local loopback eth-0-9
```

```
R       10.10.12.0/24 [120/3] via 10.10.11.50, eth-0-9, 00:02:36
R       20.20.20.0/24 [120/3] via 10.10.11.50, eth-0-9, 00:02:41
```

2.6.6 配置 RIP 路由过滤列表示例

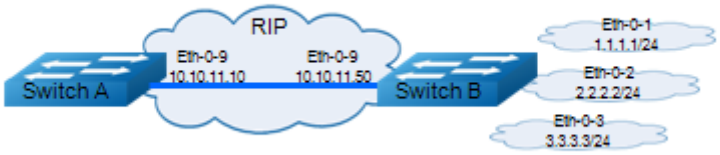
i. 介绍

路由器提供路由信息过滤功能，通过指定访问控制列表和地址前缀列表，可以配置入口或出口过滤策略，对接收或发布的路由进行过滤。一个路由过滤列表通常包括如下参数：

- 一个被用作过滤器的 ACL 或 Prefix List。
- In 方向：过滤器被应用在学习到的路由上；Out 方向：过滤器被应用在发布的路由上。
- 应用过滤器的接口（可选）。

ii. 拓扑

图 2-6 配置 RIP 路由过滤列表拓扑图



iii. 配置文件

Switch A：

```
interface eth-0-9
no switchport
ip address 10.10.11.10/24
!
router rip
network 10.10.11.0/24
```

Switch B：

```
interface eth-0-1
no switchport
ip address 1.1.1.1/24
```

```
!
interface eth-0-2
no switchport
ip address 2.2.2.2/24
!
interface eth-0-3
no switchport
ip address 3.3.3.3/24
!
interface eth-0-9
no switchport
ip address 10.10.11.50/24
!
router rip
network 1.1.1.0/24
network 2.2.2.0/24
network 3.3.3.0/24
network 10.10.11.0/24
```

iv. 配置示例

Switch A的路由表信息如下：

```
Switch# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       [*] - [AD/Metric]
       * - candidate default
R        1.1.1.0/24 [120/2] via 10.10.11.50, eth-0-9, 00:01:50
R        2.2.2.0/24 [120/2] via 10.10.11.50, eth-0-9, 00:01:50
R        3.3.3.0/24 [120/2] via 10.10.11.50, eth-0-9, 00:01:50
C        10.10.11.0/24 is directly connected, eth-0-9
C        10.10.11.10/32 is in local loopback, eth-0-9
```

参照如下表中的命令，配置 Switch B：

命令举例	操作步骤
Switch# configure terminal	进入配置模式
Switch(config)# ip prefix-list 1 deny 1.1.1.0/24 Switch(config)# ip prefix-list 1 permit any	创建地址前缀列表
Switch(config)# router rip	启用 RIP 路由协议

Switch(config-router)# distribute-list prefix 1 out	过滤 RIP 发送的路由

v. 命令验证

检查Switch A的配置结果：

```
Switch# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       [*] - [AD/Metric]
       * - candidate default
R        2.2.2.0/24 [120/2] via 10.10.11.50, eth-0-9, 00:00:08
R        3.3.3.0/24 [120/2] via 10.10.11.50, eth-0-9, 00:00:08
C        10.10.11.0/24 is directly connected, eth-0-9
C        10.10.11.10/32 is in local loopback, eth-0-9
```

2.6.7 配置 RIPv2 认证示例

RIPv2 支持两种认证方式：明文认证和MD5密文认证。

1. 明文认证

i. 介绍

Switch A和B是在运行RIP路由协议，如果要在交换机上配置明文认证，需要执行如下步骤：

- 指定一个接口，然后定义该接口的密码。
- 指定认证模式为明文。

任何从这个指定接口接收的RIP数据包应该有相同的字符串作为密码。同样的，Switch B上也要定义相同的密码和身份验证模式。

ii. 拓扑

图 2-7 配置 RIPv2 明文认证拓扑图

iii. 配置步骤

Switch A：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	配置接口 eth-0-1
Switch(config-if)# ip address 1.1.1.1/24	配置 IP 地址
Switch(config-if)# exit	退出接口配置模式
Switch(config-if)# interface eth-0-9	配置接口 eth-0-9
Switch(config-if)# ip address 10.10.11.10/24	配置 IP 地址
Switch(config-if)# exit	退出接口配置模式
Switch(config)# router rip	启用 RIP 路由协议
Switch(config-router)# network 10.10.11.0/24	发布网段到 RIP 路由中
Switch(config-router)# redistribute connected	重分布直连路由
Switch(config-router)# exit	退出路由模式
Switch(config)# interface eth-0-9	进入接口配置模式
Switch(config-if)# ip rip authentication string Auth1	指定验证的字符串
Switch(config-if)# ip rip authentication mode text	指定认证的模式为明文认证

Switch B：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	配置接口 eth-0-1
Switch(config-if)# ip address 2.2.2.2/24	配置 IP 地址
Switch(config-if)# exit	退出接口配置模式
Switch(config-if)# interface eth-0-9	配置接口 eth-0-9
Switch(config-if)# ip address 10.10.11.50/24	配置 IP 地址
Switch(config-if)# exit	退出接口配置模式
Switch(config)# router rip	启用 RIP 路由协议

命令举例	操作步骤
Switch(config-router)# network 10.10.11.0/24	发布网段到 RIP 路由中
Switch(config-router)# redistribute connected	重分布直连路由
Switch(config-router)# exit	退出路由模式
Switch(config)# interface eth-0-9	进入接口配置模式
Switch(config-if)# ip rip authentication string Auth1	指定验证的字符串
Switch(config-if)# ip rip authentication mode text	指定认证的模式为明文认证

2. MD5密文认证

i. 介绍

下面的例子介绍使用 MD5 进行 RIP 路由信息交换过程中的验证。对于需要使用 MD5 认证的 Switch A 和 B 来说，首先需要定义一个钥匙链，然后指定 key 并且配置认证的字符串或密码，再通过指定接收或者发送的时间来定义 key 生效的时间。最后将该钥匙链应用到接口上并且指定接口的认证模式为MD5。Switch A和B的密钥配置必须保持一致，才能保证RIP 路由更新信息交换成功。在MD5 认证中，key ID 和 key 字符串需要同时匹配。在下面的例子中，还配置了 key 生效的时间。配置成功后，每隔 5 天 key 就会更新一次。

ii. 拓扑

图 2-8 配置 RIPv2 MD5 密文认证拓扑图

iii. 配置步骤

Switch A：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	配置接口 eth-0-1

命令举例	操作步骤
Switch(config-if)# ip address 1.1.1.1/24	配置 IP 地址
Switch(config-if)# exit	退出接口配置模式
Switch(config-if)# interface eth-0-9	配置接口 eth-0-9
Switch(config-if)# ip address 10.10.11.10/24	配置 IP 地址
Switch(config-if)# exit	退出接口配置模式
Switch(config)# router rip	启用 RIP 路由协议
Switch(config-router)# network 10.10.11.0/24	发布网段到 RIP 路由中
Switch(config-router)# redistribute connected	重分布直连路由
Switch(config-router)# exit	退出路由模式
Switch(config)# key chain SUN	定义 KEY 密匙链
Switch(config-keychain)# key 1	创建 key id 1
Switch(config-keychain-key)# key-string key1	设置密码
Switch(config-keychain-key)# accept-lifetime 12:00:00 Mar 2 2012 14:00:00 Mar 7 2012	设置应用时间范围
Switch(config-keychain-key)# send-lifetime 12:00:00 Mar 2 2012 12:00:00 Mar 7 2012	设置应用时间范围
Switch(config-keychain-key)# exit	退出密匙链配置模式
Switch(config-keychain)# key 2	创建 key id 2
Switch(config-keychain-key)# key-string Earth	设置密码
Switch(config-keychain-key)# accept-lifetime 12:00:00 Mar 7 2012 14:00:00 Mar 12 2012	设置应用时间范围
Switch(config-keychain-key)# send-lifetime 12:00:00 Mar 7 2012 12:00:00 Mar 12 2012	设置应用时间范围
Switch(config-keychain-key)# end	退出密匙链配置模式
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-9	进入接口配置模式
Switch(config-if)# ip rip authentication key-chain SUN	定义接口上用验证名字

命令举例	操作步骤
Switch(config-if)# ip rip authentication mode md5	定义接口上的认证方式为 MD5 密文认证

Switch B：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	配置接口 eth-0-1
Switch(config-if)# ip address 2.2.2.2/24	配置 IP 地址
Switch(config-if)# exit	退出接口配置模式
Switch(config-if)# interface eth-0-9	配置接口 eth-0-9
Switch(config-if)# ip address 10.10.11.50/24	配置 IP 地址
Switch(config-if)# exit	退出接口配置模式
Switch(config)# router rip	启用 RIP 路由协议
Switch(config-router)# network 10.10.11.0/24	发布网段到 RIP 路由中
Switch(config-router)# redistribute connected	重分布直连路由
Switch(config-router)# exit	退出路由模式
Switch(config)# key chain SUN	定义 KEY 密匙链
Switch(config-keychain)# key 1	创建 key id 1
Switch(config-keychain-key)# key-string key1	设置密码
Switch(config-keychain-key)# accept-lifetime 12:00:00 Mar 2 2012 14:00:00 Mar 7 2012	设置应用时间范围
Switch(config-keychain-key)# send-lifetime 12:00:00 Mar 2 2012 12:00:00 Mar 7 2012	设置应用时间范围
Switch(config-keychain-key)# exit	退出密匙链配置模式
Switch(config-keychain)# key 2	创建 key id 2
Switch(config-keychain-key)# key-string Earth	设置密码
Switch(config-keychain-key)# accept-lifetime 12:00:00 Mar 7 2012 14:00:00 Mar 12 2012	设置应用时间范围

命令举例	操作步骤
Switch(config-keychain-key)# send-lifetime 12:00:00 Mar 7 2012 12:00:00 Mar 12 2012	设置应用时间范围
Switch(config-keychain-key)# end	退出密匙链配置模式
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-9	进入接口配置模式
Switch(config-if)# ip rip authentication key-chain SUN	定义接口上用验证名字
Switch(config-if)# ip rip authentication mode md5	定义接口上的认证方式为 MD5 密文认证

iv. 命令验证

- 检查Switch A的配置的结果：

```
Switch# show key chain
key chain SUN:
    key 1 -- text "key1"
      accept-lifetime <12:00:00 Mar 02 2012> - <14:00:00 Mar 07 2012>
      send-lifetime <12:00:00 Mar 02 2012> - < 12:00:00 Mar 07 2012>
    key 2 -- text "Earth"
      accept-lifetime <12:00:00 Mar 07 2012> - <14:00:00 Mar 12 2012>
      send-lifetime <12:00:00 Mar 07 2012> - < 12:00:00 Mar 12 2012>
Switch#
```

- 检查Switch B的配置的结果：

```
Switch# show key chain
key chain SUN:
    key 1 -- text "key1"
      accept-lifetime <12:00:00 Mar 02 2012> - <14:00:00 Mar 07 2012>
      send-lifetime <12:00:00 Mar 02 2012> - < 12:00:00 Mar 07 2012>
    key 2 -- text "Earth"
      accept-lifetime <12:00:00 Mar 07 2012> - <14:00:00 Mar 12 2012>
      send-lifetime <12:00:00 Mar 07 2012> - < 12:00:00 Mar 12 2012>
```

3 OSPF 配置

3.1 OSPF 简介

RIP 协议主要应用于小型网络中，有一定的局限性，如收敛慢、故障恢复时间较长、缺乏全局性、跳数限制等问题。而 OSPF 适用于大型网络，可以有效地解决这些问题。OSPF 的定义及特性如下：

3.1.1 定义

开放最短路径优先协议（Open Shortest Path First，缩写：OSPF）是 IETF 组织开发的一个基于链路状态的内部网关协议，它支持 IP 子网化以及对外部路由做标记。目前使用的是版本 2（RFC2328），其特性如下：

- 适应范围：支持各种规模的网络，尤其是中大型网络，最多可支持几百台路由器。
- 快速收敛：收到链路状态信息后立即发送更新报文，使这一变化在自治系统中同步。
- 无环路：由于OSPF根据收集到的链路状态用最短路径树算法计算路由，从算法本身保证了无环路。
- 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化，从而减少了占用的网络带宽。
- 等价路由：支持到同一目的地址的多条等价路由。
- 路由分级：使用4类不同的路由，按优先顺序来说分别是：区域内路由、区域间路由、第一类外部路由、第二类外部路由。
- 支持验证：支持基于接口的报文验证以保证路由计算的安全性。
- 组播发送：协议报文支持以组播形式发送。

3.1.2 特性

当前的系统支持如下 OSPF 特性：

- 支持末梢区域：支持路由重分布，这包括将其他路由协议学到的路由导入 OSPF 或者将 OSPF 学到的路由导出到其他路由协议中。
- 支持明文和 MD5 两种认证模式：支持 OSPF 接口上的参数配置，包括输出度量值、重传时间、发送延时时间、路由器优先级、路由器 Hello 报文时间间隔以及认证密码等。
- 支持 NSSA 区域：支持指定某区域为 NSSA (Not-So-Stubby Area) 区域。

OSPF 需要多个路由器协同工作，包括区域边界路由器(ABR)，自治系统边界路由器(ASBR)，内部路由器等。最简单的 OSPF 配置只需要使用默认的参数，并且将所有的 OSPF 接口加入同一个区域即可。

3.2 配置 OSPF 的基本功能

3.2.1 创建 OSPF 进程

用户可以在一台路由器上创建多个OSPF进程，如果没有指定进程编号，则创建默认的0号进程。

表3-1 创建OSPF进程

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# router ospf 109	创建 OSPF 进程并进入 OSPF 配置模式	如果未指定 OSPF 进程号，则进入 0 号进程。使用关键字 **no** 关闭 OSPF 进程时，如果没有指定进程编号，则关闭 OSPF 的 0 号进程；否则只关闭指定的 OSPF 进程。缺省情况下，未创建 OSPF 进程
Switch(config-router)# end	退出 OSPF 配置模式	-

3.2.2 创建 OSPF 区域

表3-2 创建OSPF区域

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-

命令举例	操作	说明
Switch(config-if)# no switchport	设置接口为三层接口	-
Switch(config-if)# ip address 10.108.20.1/24	配置 IP 地址	-
Switch(config-if)# exit	退出接口配置模式	-
Switch(config)# router ospf 109	创建 OSPF 进程并进入 OSPF 配置模式	如果未指定 OSPF 进程号，则进入 0 号进程。使用关键字 **no** 关闭 OSPF 进程时，如果没有指定进程编号，则关闭 OSPF 的 0 号进程；否则只关闭指定的 OSPF 进程。缺省情况下，未创建 OSPF 进程
Switch(config-router)# network 10.108.20.0/24 area 10.9.50.0	将接口加入指定的 OSPF 区域：10.9.50.0 和 2	area-id: 区域 ID，可以用十进制或 IP 地址表示
Switch(config-router)# network 10.108.0.0/16 area 2		

3.2.3 创建路由器 ID

路由器 ID (Router-id) 参数是 OSPF 协议中一个很重要的参数。在 OSPF 协议中，路由器 ID 号是一个 32 比特无符号整数，是一台路由器在 OSPF 自治系统中的唯一标识。用户可以自行指定路由器 ID 号。如果用户没有指定路由器 ID 号，则路由器会自动从已配置的接口的 IP 地址中选一个作为本机的 ID 号。

在选择路由器 ID 时，环回接口上的 IP 地址优于普通接口上的 IP 地址；若都是普通接口，则选择接口的最大 IP 地址作为路由器 ID。若路由器的所有接口上都未配置 IP 地址，则必须在 OSPF 模式下配置路由器 ID 号，否则 OSPF 将无法运行。在手工设置路由器 ID 号时，必须保证自治系统中任意两台路由器ID 号都不相同。为此，不妨选择某个接口的 IP 地址作为本机 ID 号。若在已经有邻居的路由器上用此命令更改了路由器 ID，则该 ID 必须重新启用 OSPF 协议才能生效。

表3-3 创建路由器ID

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-

命令举例	操作	说明
Switch(config)# router ospf 109	创建 OSPF 进程并进入 OSPF 配置模式	如果未指定 OSPF 进程号，则进入 0 号进程。使用关键字 **no** 关闭 OSPF 进程时，如果没有指定进程编号，则关闭 OSPF 的 0 号进程；否则只关闭指定的 OSPF 进程。缺省情况下，未创建 OSPF 进程
Switch(config-router)# router-id 10.1.1.1	配置 OSPF 的路由器 ID	-

3.3 配置 OSPF 邻居或邻接参数

3.3.1 配置 LSA 报文交换的重传时间

当一个路由器发送LSA报文到它的邻居时，它会缓存该报文直到收到邻居的确认报文。如果在重传时间间隔内没有收到确认报文，该LSA将被重传。设置该值必须要谨慎，以免引起不必要的重传。通常，这个值要大于两个路由器之间的报文往返延迟的值。

表3-4 配置LSA报文交换的重传时间

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-
Switch(config-if)# no switchport	设置接口为三层接口	-
Switch(config-if)# ip ospf retransmit-interval 8	配置接口的 LSA 报文交换时的重传时间	重传时间间隔的取值范围为 1~65535，单位：秒；缺省情况下，重传时间间隔为 5 秒

3.3.2 配置 MTU 字段检测

OSPF 检查邻居是否使用相同的 MTU 值。这个检查发生在互相交换数据库描述报文时，如果在接收到的 DD 报文里的 MTU 高于入接口上配置的 MTU，OSPF 邻接将无法建立。

表3-5 配置MTU字段检测

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-
Switch(config-if)# no switchport	设置接口为三层接口	-
Switch(config-if)# no ip ospf mtu-ignore	配置在端口上接收到 DD 报文时，对 MTU 值进行检测	缺省情况下，默认接口启用 MTU 的匹配功能

3.4 配置接口的网络类型

缺省情况下，接口的网络类型根据物理接口而定。以太网接口的网络类型为 Broadcast，串口的网络类型为 P2P，ATM 接口的网络类型为NBMA。如果在广播网络上有不支持组播地址的路由器，可以将接口的网络类型改为NBMA；也可以将接口的网络类型由NBMA 改为广播。这样，就不必再配置邻居路由器。

一个 NBMA 类型的网络可以改为广播类型的条件是：任意两台路由器之间都有一条虚电路直接可达，或者说，这个网络是全连通的。如果网络不满足这个条件，必须将接口的网络类型改为点到多点。这样，两台不能直接可达的路由器之间可以通过一台与两者都直接可达的路由器来交换路由信息。接口的网络类型改为点到多点后，就不必再配置邻居路由器。如果同一网段内只有两台路由器运行OSPF 协议，也可以将接口的网络类型改为点到点。下表以配置 OSPF 的 NBMA 网络为例。

表3-6 配置接口的网络类型

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-
Switch(config-if)# no switchport	设置接口为三层接口	-
Switch(config-if)# ip address 192.168.77.17/24	配置 IP 地址	-
Switch(config-if)# ip ospf network non-broadcast	配置 OSPF 的 NBMA 网络	可以配置的网络类型有：broadcast、non- broadcast、point-to-multipoint、point-to-point

3.5 配置 OSPF 的 Stub 区域

有两种 Stub 区域的路由配置命令：**stub** 和 **default-cost** 命令。更多关于 OSPF 的区域参数配置可参考 3.8.3 配置 OSPF 区域参数示例。

表3-7 配置步骤

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-
Switch(config-if)# no switchport	设置接口为三层接口	-
Switch(config-if)# ip address 10.56.0.201/16	配置 IP 地址	-
Switch(config-if)# exit	退出接口配置模式	-
Switch(config)# router ospf 201	创建 OSPF 进程并进入 OSPF 配置模式	如果未指定 OSPF 进程号，则进入 0 号进程。使用关键字 **no** 关闭 OSPF 进程时，如果没有指定进程编号，则关闭 OSPF 的 0 号进程；否则只关闭指定的 OSPF 进程。缺省情况下，未创建 OSPF 进程
Switch(config-router)# network 10.0.0.0/8 area 10.0.0.0	将接口加入指定的 OSPF 区域	area-id: 区域 ID，可以用十进制或 IP 地址表示
Switch(config-router)# area 10.0.0.0 stub	设置指定区域为 Stub（存根）区域	缺省情况下，没有区域被设置为 Stub（存根）区域；tub 区域的所有路由器都必须用 **area stub** 进行设置
Switch(config-router)# area 10.0.0.0 default-cost 20	配置 Stub 区域的 Cost 值	开销值的取值范围为 0~16777214；默认值为 1

说明

常用的LSA类型有6种：1类 (Router-Lsa)、2类 (Network Lsa)、3类 (Summary Lsa)、4类 (ASBR-Summary-

LSA)、5类 (AS-External- LSA)以及7类 (NSSA- LSA)。配置 Stub 区域后只学习类型为1类 (Router-Lsa)、2类(Network Lsa)和3类(Summary Lsa)的LSA。

3.6 配置 OSPF 的 NSSA 区域

NSSA区域能够将自治域外部路由引入并传播到整个OSPF自治域中，同时又不会学习来自OSPF网络其它区域的外部路由。可配置的关键字有路由器选举（candidate、never、always）、不分发external-LSA 到NSSA（no-redistribution）、度量值（metric-value）、度量值类型（type-value）以及配置NSSA区域为完全存根区域（no-summary）。下表以配置 no-redistribution 为例。

表3-8 创建OSPF的NSSA区域

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# router ospf 109	创建 OSPF 进程并进入 OSPF 配置模式	如果未指定 OSPF 进程号，则进入 0 号进程。使用关键字 **no** 关闭 OSPF 进程时，如果没有指定进程编号，则关闭 OSPF 的 0 号进程；否则只关闭指定的 OSPF 进程。缺省情况下，未创建 OSPF 进程
Switch(config-router)# area 10.0.0.0 nssa no-redistribution	配置不分发 external-LSA 到 NSSA	缺省情况下，没有区域被设置为 NSSA 区域。NSSA 区域的所有路由器都必须用 **area nssa** 进行设置

说明

1. candidate 表示如果路由器被选举为translator，可以转换7类 (NSSA- LSA) 为5类 (AS-External- LSA)；
2. never 表示路由器永不进行7类 (NSSA- LSA) 到5类 (AS-External- LSA) 的转换；
3. always 表示路由器总是进行7类 (NSSA- LSA) 到5类 (AS-External- LSA) 的转换。

缺省情况下为candidate。

3.7 OSPF 显示与维护

用户可以通过命令查看具体的统计数据，如 IP 路由表的内容、缓存和数据库。

表3-9 OSPF显示与维护

命令	操作	说明
show ip ospf [*process-id*]	显示 OSPF 进程信息	process-id: OSPF 进程号 link-state-id: 链路状态 IP（点分十进制） ip-address: 宣告路由器的 IP 地址
show ip ospf *process-id* **database router** *link-state-id* **adv-router** *ip-address* **show ip ospf** *process-id* **database network self-originate** **show ip ospf** *process-id* **database summary** **show ip ospf** *process-id* **database asbr-summary** **show ip ospf** *process-id* **database external**	显示 OSPF 链路状态信息库	
show ip ospf border-routes	显示边界路由器的 OSPF 信息	-
show ip ospf interface *if-name*	显示 OSPF 接口信息	if-name: 接口名称
show ip ospf neighbor *neighbor-id*	显示 OSPF 邻居信息	neighbor-id: 邻居 ID（点分十进制）

3.8 OSPF 配置举例

3.8.1 配置接口启用 OSPF 示例

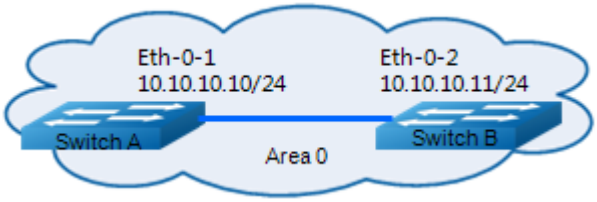
下面的例子描述了一个接口上启用 OSPF 所需的最低配置。

说明

一个接口只属于一个区域，不同的接口可以属于不同的区域。

i. 拓扑

图 3-1 配置接口启用 OSPF 拓扑图



ii. 配置步骤

Switch A:

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# ip address 10.10.10.10/24	配置 IP 地址
Switch(config-if)# exit	退出接口配置模式
Switch(config)# router ospf 100	创建 OSPF 进程号 100
Switch(config-router)# network 10.10.10.0/24 area 0	发布 10.10.10.0/24 网段至 OSPF 区域 0

Switch B:

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-2	进入接口配置模式
Switch(config-if)# ip address 10.10.10.11/24	配置 IP 地址
Switch(config-if)# exit	退出接口配置模式
Switch(config)# router ospf 200	创建 OSPF 进程号 200
Switch(config-router)# network 10.10.10.0/24 area 0	发布 10.10.10.0/24 网段至 OSPF 区域 0

iii. 命令验证

- 检查Switch A的配置结果：

```
Switch# show ip ospf database
                OSPF Router with ID (10.10.10.10) (Process ID 100)
                    Router Link States (Area 0)
Link ID         ADV Router      Age  Seq#       CkSum  Link count
10.10.10.10     10.10.10.10     51 0x80000002 0xd012  1
Switch# show running-config router ospf
Building configuration...
!
router ospf 100
  network 10.10.10.0/24 area 0
!
```

- 检查Switch B的配置结果：

```
Switch# show ip ospf database
                OSPF Router with ID (10.10.10.10) (Process ID 200)
                    Router Link States (Area 0)
Link ID         ADV Router      Age  Seq#       CkSum  Link count
10.10.10.10     10.10.10.10     267 0x80000002 0xd012 1
Switch# show running-config router ospf
Building configuration...
!
router ospf 200
  network 10.10.10.0/24 area 0
!
```

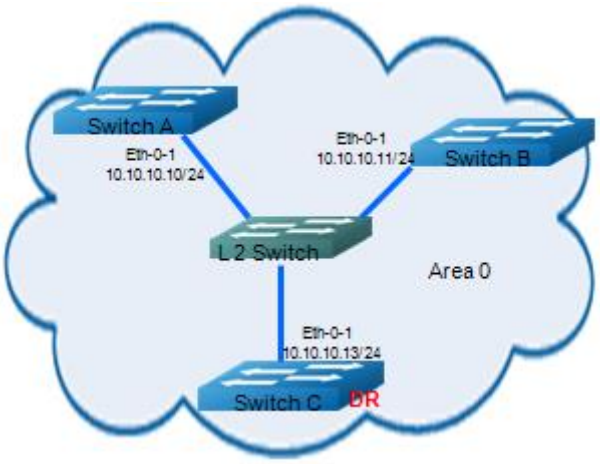
3.8.2 配置 OSPF 优先级示例

i. 介绍

本小节主要介绍接口优先级的配置，优先级高的成为 DR。优先级为 0 的不参与 DR 选举。Switch C 的优先级是 10，这比 Switch A 和 Switch B 的默认优先级 1 要高，因此 Switch C 将成为这个网络内的 DR。

ii. 拓扑

图 3-2 配置 OSPF 优先级拓扑图



iii. 配置方法

Switch C：

命令举例	操作步骤
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# ip ospf priority 10	设置接口优先级
Switch(config-if)# exit	退出接口配置模式
Switch(config)# router ospf 100	创建 OSPF 进程号 100
Switch(config-router)# network 10.10.10.0/24 area 0	发布 10.10.10.0/24 网段至 OSPF 区域 0

Switch B：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# router ospf 100	创建 OSPF 进程号 100
Switch(config-router)# network 10.10.10.0/24 area 0	发布 10.10.10.0/24 网段至 OSPF 区域 0

Switch A：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# router ospf 200	创建 OSPF 进程号 100
Switch(config-router)# network 10.10.10.0/24 area 0	发布 10.10.10.0/24 网段至 OSPF 区域 0

iv. 命令验证

检查 Switch C 的配置结果：

```
Switch# show ip ospf neighbor
OSPF process 0:
Neighbor ID     Pri   State           Dead Time   Address         Interface
10.10.10.10       1   Full/DROther    00:00:32    10.10.10.10     eth-0-1
10.10.10.11       1   Full/BDR        00:00:31    10.10.10.11     eth-0-1
Switch# show ip ospf interface
eth-0-10 is up, line protocol is up
  Internet Address 10.10.10.13/24, Area 0, MTU 1500
  Process ID 0, Router ID 10.10.10.13, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 10, TE Metric 1
  Designated Router (ID) 10.10.10.13, Interface Address 10.10.10.13
  Backup Designated Router (ID) 10.10.10.11, Interface Address 10.10.10.11
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:07
  Neighbor Count is 2, Adjacent neighbor count is 2
  Crypt Sequence Number is 1301567281
  Hello received 188 sent 110, DD received 34 sent 23
  LS-Req received 8 sent 6, LS-Upd received 28 sent 26
  LS-Ack received 32 sent 15, Discarded 0
```

3.8.3 配置 OSPF 区域参数示例

i. 介绍

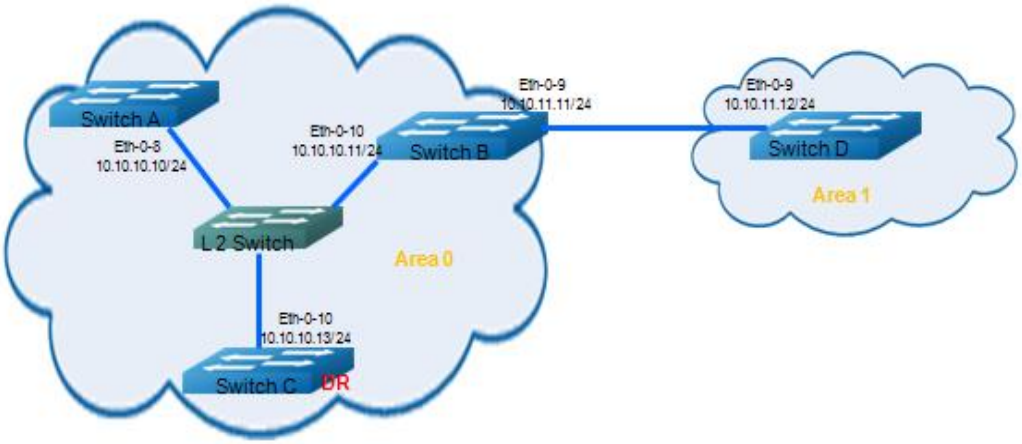
用户可以选择性地配置多个 OSPF 区域参数。这些参数包括用于防止访问未经授权的区域的认证密码，以及将区域配置为末梢区域 (Stub)。Stub 区域是一些特定的区域，Stub 区域的 ABR 不传播它们接收到的自治系统外部路由，在这些区域中路由器的路由表规模以及路由信息传递的数量都会大大减少。为保证到自治系统外的路由依旧可达，该区域的 ABR 将生成一条缺省路由，并发布给 Stub 区域中的其他非 ABR 路由器。

路由聚合是指 ABR 或 ASBR 将具有相同前缀的路由信息聚合，只发布一条路由到其它区域。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。如果网络号是连续的，用户可以使用 **area range** 命令将这些连续的网段聚合成一个网段。这样 ABR 只发送一条聚合后的 LSA，所有属于本命令指定的聚合网段范围的 LSA 将不再会被单独发送出去，这样可减少其它区域中 LSDB 的规模。

ii. 拓扑

图 3-3 配置 OSPF 区域拓扑图



iii. 配置步骤

Switch A:

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)#interface eth-0-8	进入接口配置模式
Switch(config-if)#no switchport	设置接口为三层接口
Switch(config-if)#ip address 10.10.10.10/24	设置端口的 IP 地址
Switch(config-if)# exit	退出接口配置模式
Switch(config)# router ospf 100	创建 OSPF 进程号 100
Switch(config-router)# network 10.10.10.0/24 area 0	发布 10.10.10.0/24 网段至 OSPF 区域 0

Switch B:

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)#interface eth-0-10	进入接口配置模式
Switch(config-if)#no switchport	设置接口为三层接口
Switch(config-if)#ip address 10.10.10.11/24	设置端口的 IP 地址
Switch(config-if)# exit	退出接口配置模式
Switch(config)#interface eth-0-9	进入接口配置模式
Switch(config-if)#no switchport	设置接口为三层接口
Switch(config-if)#ip address 10.10.11.11/24	设置端口的 IP 地址
Switch(config-if)# exit	退出接口配置模式
Switch(config)# router ospf 100	创建 OSPF 进程号 100
Switch(config-router)# network 10.10.10.0/24 area 0	发布 10.10.10.0/24 网段至 OSPF 区域 0
Switch(config-router)# network 10.10.11.0/24 area 1	发布 10.10.11.0/24 网段至 OSPF 区域 1
Switch(config-router)# area 0 range 10.10.10.0/24	指定一段 IP 网段发布至 OSPF 区域 0
Switch(config-router)# area 1 stub no-summary	将区域 1 设置为 Stub 区域
Switch(config-router)# end	退出 OSPF 配置模式

Switch C：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)#interface eth-0-10	进入接口配置模式
Switch(config-if)#no switchport	设置接口为三层接口
Switch(config-if)#ip address 10.10.10.13/24	设置端口的 IP 地址
Switch(config-if)# ip ospf priority 10	设置 OSPF 接口优先级
Switch(config-if)# exit	退出接口配置模式
Switch(config)# router ospf 100	创建 OSPF 进程号 100

命令举例	操作步骤
Switch(config-router)# network 10.10.10.0/24 area 0	发布 10.10.10.0/24 网段至 OSPF 区域 0

Switch D：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)#interface eth-0-9	进入接口配置模式
Switch(config-if)#no switchport	设置接口为三层接口
Switch(config-if)#ip address 10.10.11.12/24	设置端口的 IP 地址
Switch(config-if)# exit	退出接口配置模式
Switch(config)# router ospf 200	创建 OSPF 进程号 200
Switch(config-router)# network 10.10.11.0/24 area 1	发布 10.10.11.0/24 网段至 OSPF 区域 1
Switch(config-router)# area 1 stub no-summary	将区域 1 设置为 Stub 区域

iv. 命令验证

- Switch A的配置结果如下：

```
Switch# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       [*] - [AD/Metric]
       * - candidate default
C        10.10.10.0/24 is directly connected, eth-0-8
C        10.10.10.10/32 is in local loopback, eth-0-8
O IA     10.10.11.0/24 [110/2] via 10.10.10.11, eth-0-8, 00:14:46
```

- Switch B的配置结果如下：

```
Switch# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
```

```
            [*] - [AD/Metric]
            * - candidate default
C             10.10.10.0/24 is directly connected, eth-0-10
C             10.10.10.11/32 is in local loopback, eth-0-10
C             10.10.11.0/24 is directly connected, eth-0-9
C             10.10.11.11/32 is in local loopback, eth-0-9
```

- Switch C的配置结果如下：

```
Switch# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       [*] - [AD/Metric]
       * - candidate default
C        10.10.10.0/24 is directly connected, eth-0-10
C        10.10.10.13/32 is in local loopback, eth-0-10
O IA     10.10.11.0/24 [110/2] via 10.10.10.11, eth-0-10, 00:20:35
```

- Switch D的配置结果如下：

```
Switch# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       [*] - [AD/Metric]
       * - candidate default
Gateway of last resort is 10.10.11.11 to network 0.0.0.0
O*IA     0.0.0.0/0 [110/2] via 10.10.11.11, eth-0-9, 00:12:46
C        10.10.11.0/24 is directly connected, eth-0-9
C        10.10.11.12/32 is in local loopback, eth-0-9
```

3.8.4 配置 OSPF 路由重分布示例

i. 介绍

区域内和区域间路由描述的是AS 内部的网络结构，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。

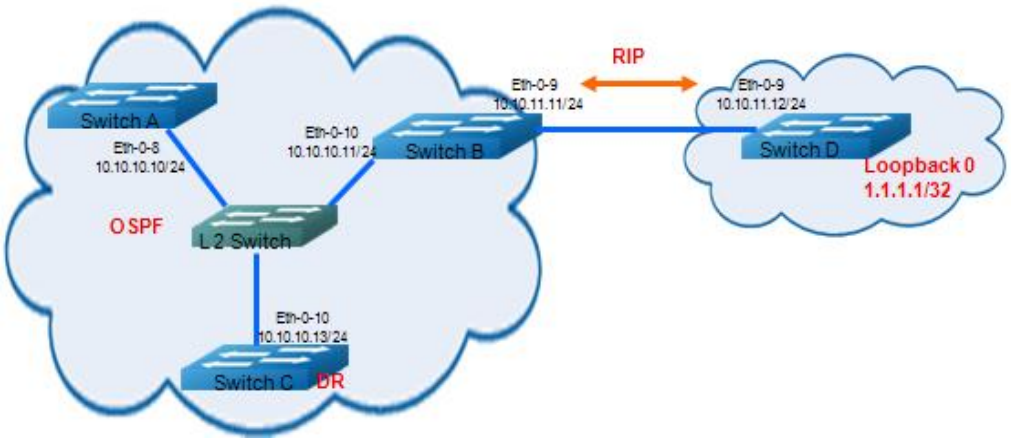
第一类外部路由是指接收的是IGP（Interior Gateway Protocol，内部网关协议）路由（例如静态路由和

RIP 路由）。由于这类路由的可信程度较高，并且和OSPF 自身路由的开销具有可比性，所以到第一类外部路由的开销等于本路由器到相应的ASBR 的开销与ASBR 到该路由目的地址的开销之和。

第二类外部路由是指接收的是EGP（Exterior Gateway Protocol，外部网关协议）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。如果计算出开销值相等的两条路由，再考虑本路由器到相应的ASBR 的开销。下面例子介绍 RIP 路由将作为外部路由被重分布到OSPF 网络中。

ii. 拓扑

图 3-4 OSPF 路由重分布拓扑图



iii. 配置步骤

Switch A:

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)#interface eth-0-8	进入接口配置模式
Switch(config-if)#no switchport	设置接口为三层接口
Switch(config-if)#ip address 10.10.10.10/24	设置端口的 IP 地址
Switch(config-if)# exit	退出接口配置模式

命令举例	操作步骤
Switch(config)# router ospf 100	创建 OSPF 进程号 100
Switch(config-router)# network 10.10.10.0/24 area 0	发布 10.10.10.0/24 网段至 OSPF 区域 0

Switch B:

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)#interface eth-0-10	进入接口配置模式
Switch(config-if)#no switchport	设置接口为三层接口
Switch(config-if)#ip address 10.10.10.11/24	设置端口的 IP 地址
Switch(config-if)# exit	退出接口配置模式
Switch(config)#interface eth-0-9	进入接口配置模式
Switch(config-if)#no switchport	设置接口为三层接口
Switch(config-if)#ip address 10.10.11.11/24	设置端口的 IP 地址
Switch(config-if)# exit	退出接口配置模式
Switch(config)# router ospf 100	创建 OSPF 进程号 100
Switch(config-router)# network 10.10.10.0/24 area 0	发布 10.10.10.0/24 网段至 OSPF 区域 0
Switch(config-router)# redistribute connected	重分布直连路由
Switch(config-router)#redistribute rip	重分布 RIP 路由
Switch(config-router)# exit	返回至全局配置模式
Switch(config)# router rip	创建 RIP 路由
Switch(config-router)# network 10.10.11.0/24	发布网段至 RIP 路由
Switch(config-router)#redistribute connected	重分布直连路由

Switch C:

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)#interface eth-0-10	进入接口配置模式
Switch(config-if)#no switchport	设置接口为三层接口
Switch(config-if)#ip address 10.10.10.13/24	设置端口的 IP 地址
Switch(config-if)# ip ospf priority 10	设置 OSPF 接口优先级
Switch(config-if)# exit	退出接口配置模式
Switch(config)# router ospf 100	创建 OSPF 进程号 100
Switch(config-router)# network 10.10.10.0/24 area 0	发布 10.10.10.0/24 网段至 OSPF 区域 0

Switch D:

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)#interface eth-0-9	进入接口配置模式
Switch(config-if)#no switchport	设置接口为三层接口
Switch(config-if)#ip address 10.10.11.12/24	设置端口的 IP 地址
Switch(config-if)# exit	退出接口配置模式
Switch(config)# router rip	创建 RIP 路由
Switch(config-router)# network 10.10.11.0/24	发布网段到 RIP 路由中
Switch(config-router)# network 1.1.1.1/32	发布网段到 RIP 路由中
Switch(config-router)#redistribute connected	重分布直连路由

iv. 命令验证

- 检查Switch A的配置结果：

```
Switch# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
```

```
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        [*] - [AD/Metric]
        * - candidate default
O E2     1.1.1.1/32 [110/20] via 10.10.10.11, eth-0-8, 00:21:00
C        10.10.10.0/24 is directly connected, eth-0-8
C        10.10.10.10/32 is in local loopback, eth-0-8
O E2     10.10.11.0/24 [110/20] via 10.10.10.11, eth-0-8, 00:13:25
Switch# show ip ospf database external
                OSPF Router with ID (10.10.10.10) (Process ID 100)
                    AS External Link States
  LS age: 1447
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: AS-external-LSA
  Link State ID: 1.1.1.1 (External Network Number)
  Advertising Router: 10.10.11.11
  LS Seq Number: 80000002
  Checksum: 0x414e
  Length: 36
  Network Mask: /32
        Metric Type: 2 (Larger than any link state path)
        TOS: 0
        Metric: 20
        Forward Address: 0.0.0.0
        External Route Tag: 0
  LS age: 993
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: AS-external-LSA
  Link State ID: 10.10.11.0 (External Network Number)
  Advertising Router: 10.10.11.11
  LS Seq Number: 80000001
  Checksum: 0xfc78
  Length: 36
  Network Mask: /24
        Metric Type: 2 (Larger than any link state path)
        TOS: 0
        Metric: 20
        Forward Address: 0.0.0.0
        External Route Tag: 0
```

- 检查Switch B的配置结果：

```
Switch# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       [*] - [AD/Metric]
```

```
        * - candidate default
R         1.1.1.1/32 [120/2] via 10.10.11.12, eth-0-9, 00:24:52
C         10.10.10.0/24 is directly connected, eth-0-10
C         10.10.10.11/32 is in local loopback, eth-0-10
C         10.10.11.0/24 is directly connected, eth-0-9
C         10.10.11.11/32 is in local loopback, eth-0-9
```

- 检查Switch C的配置结果：

```
Switch# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       [*] - [AD/Metric]
       * - candidate default
O E2     1.1.1.1/32 [110/20] via 10.10.10.11, eth-0-10, 00:22:38
C        10.10.10.0/24 is directly connected, eth-0-10
C        10.10.10.13/32 is in local loopback, eth-0-10
O E2     10.10.11.0/24 [110/20] via 10.10.10.11, eth-0-10, 00:15:04
```

- 检查Switch D的配置结果：

```
Switch# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       [*] - [AD/Metric]
       * - candidate default
C        1.1.1.1/32 is directly connected, loopback0
R        10.10.10.0/24 [120/2] via 10.10.11.11, eth-0-9, 00:17:36
C        10.10.11.0/24 is directly connected, eth-0-9
C        10.10.11.12/32 is in local loopback, eth-0-9
```

3.8.5 配置 OSPF 开销值示例

i. 介绍

用户可以通过修改接口的COST 值来使路由成为最优路由。在下面的例子中，通过修改COST 值可以使Switch B 成为Switch A 的下一跳。

默认接口的COST 值是1 (1000M speed)。如图 3-5所示，Switch B 的 Eth-0-2 优先级为100，Switch

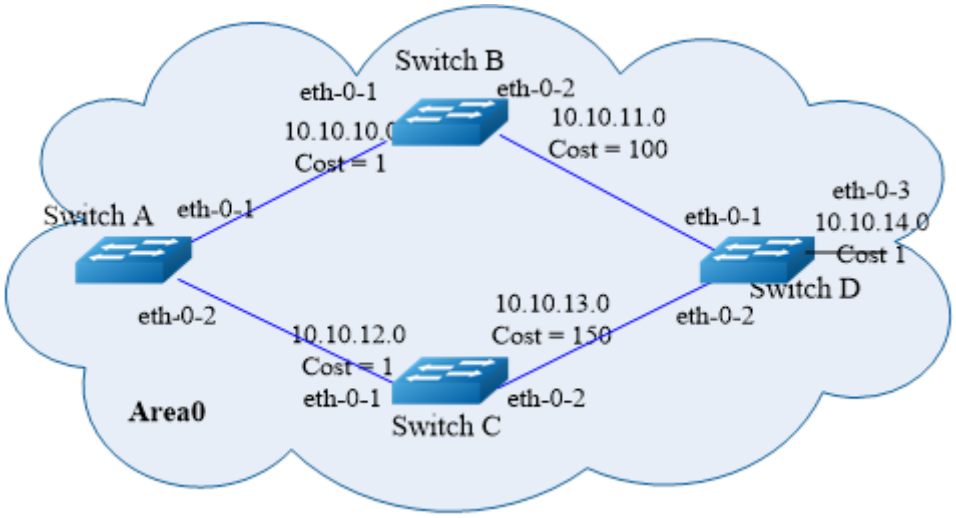
C的Eth-0-2 优先级为 150，那么到达Switch D 的网络10.10.14.0 的COST 值将不一样：

Switch B: 1+1+100 = 102

Switch C: 1+1+150 = 152

ii. 拓扑

图 3-5 配置 OSPF 开销值拓扑图



iii. 配置步骤

Switch A:

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# no switchport	设置接口为三层接口
Switch(config-if)# ip address 10.10.10.1/24	设置端口的 IP 地址
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface eth-0-2	进入接口配置模式
Switch(config-if)# no switchport	设置接口为三层接口
Switch(config-if)# ip address 10.10.12.1/24	设置端口的 IP 地址

命令举例	操作步骤
Switch(config-if)# exit	退出接口配置模式
Switch(config)# router ospf 100	创建 OSPF 进程号 100
Switch(config-router)# network 10.10.10.0/24 area 0 Switch(config-router)# network 10.10.12.0/24 area 0	发布 10.10.10.0/24, 10.10.12.0/24 网段至 OSPF 区域 0

Switch B:

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# no switchport	设置接口为三层接口
Switch(config-if)# ip address 10.10.10.2/24	设置端口的 IP 地址
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface eth-0-2	进入接口配置模式
Switch(config-if)# no switchport	设置接口为三层接口
Switch(config-if)# ip address 10.10.11.2/24	设置端口的 IP 地址
Switch(config-if)# ip ospf cost 100	设置 OSPF 的接口的 COST
Switch(config)# router ospf 100	创建 OSPF 进程号 100
Switch(config-router)# network 10.10.10.0/24 area 0 Switch(config-router)# network 10.10.11.0/24 area 0	发布 10.10.10.0/24、10.10.11.0/24 网段至 OSPF 区域 0

Switch C:

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# no switchport	设置接口为三层接口
Switch(config-if)# ip address 10.10.12.2/24	设置端口的 IP 地址

命令举例	操作步骤
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface eth-0-2	进入接口配置模式
Switch(config-if)# no switchport	设置接口为三层接口
Switch(config-if)# ip address 10.10.13.2/24	设置端口的 IP 地址
Switch(config-if)# ip ospf cost 150	设置 OSPF 的接口的 COST
Switch(config-if)# exit	退出接口配置模式
Switch(config)# router ospf 100	创建 OSPF 进程号 100
Switch(config-router)# network 10.10.12.0/24 area 0 Switch(config-router)# network 10.10.13.0/24 area 0	发布 10.10.12.0/24、10.10.13.0/24 网段至 OSPF 区域 0

Switch D:

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# no switchport	设置接口为三层接口
Switch(config-if)# ip address 10.10.11.1/24	设置端口的 IP 地址
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface eth-0-2	进入接口配置模式
Switch(config-if)# no switchport	设置接口为三层接口
Switch(config-if)# ip address 10.10.13.1/24	设置端口的 IP 地址
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface eth-0-3	进入接口配置模式
Switch(config-if)# no switchport	设置接口为三层接口
Switch(config-if)# ip address 10.10.14.1/24	设置端口的 IP 地址
Switch(config-if)# exit	退出接口配置模式

命令举例	操作步骤
Switch(config)# router ospf 100	创建 OSPF 进程号 100
Switch(config-router)# network 10.10.11.0/24 area 0 Switch(config-router)# network 10.10.13.0/24 area 0 Switch(config-router)# network 10.10.14.0/24 area 0	发布 10.10.11.0/24，10.10.13.0/24、10.10.14.0/24 网段至 OSPF 区域 0

iv. 命令验证

- 检查Switch A的配置结果：

```
Switch# show ip ospf route
OSPF process 0:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
C   10.10.10.0/24 [1] is directly connected, eth-0-1, Area 0
O   10.10.11.0/24 [101] via 10.10.10.2, eth-0-1, Area 0
C   10.10.12.0/24 [1] is directly connected, eth-0-2, Area 0
O   10.10.13.0/24 [102] via 10.10.10.2, eth-0-1, Area 0
O   10.10.14.0/24 [102] via 10.10.10.2, eth-0-1, Area 0
```

- 检查Switch B的配置结果：

```
Switch# show ip ospf route
OSPF process 100:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
C   10.10.10.0/24 [10] is directly connected, eth-0-1, Area 0
C   10.10.11.0/24 [100] is directly connected, eth-0-2, Area 0
O   10.10.12.0/24 [11] via 10.10.10.1, eth-0-1, Area 0
O   10.10.13.0/24 [101] via 10.10.11.1, eth-0-2, Area 0
O   10.10.14.0/24 [101] via 10.10.11.1, eth-0-2, Area 0
```

- 检查Switch C的配置结果：

```
Switch# show ip ospf route
OSPF process 100:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
```

```
O   10.10.10.0/24 [1] via 10.10.12.1, eth-0-1, Area 0
O   10.10.11.0/24 [101] via 10.10.12.1, eth-0-1, Area 0
C   10.10.12.0/24 [1] is directly connected, eth-0-1, Area 0
O   10.10.13.0/24 [102] via 10.10.12.1, eth-0-1, Area 0
O   10.10.14.0/24 [102] via 10.10.12.1, eth-0-1, Area 0
```

- 检查Switch D的配置结果：

```
Switch# show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       [*] - [AD/Metric]
       * - candidate default
O        10.10.10.0/24 [110/1] via 10.10.11.2, eth-0-1, 00:06:27
C        10.10.11.0/24 is directly connected, eth-0-1
O        10.10.12.0/24 [110/1] via 10.10.13.2, eth-0-2, 00:06:17
C        10.10.13.0/24 is directly connected, eth-0-2
C        10.10.14.0/24 is directly connected, eth-0-3
```

3.8.6 配置 OSPF 认证示例

i. 介绍

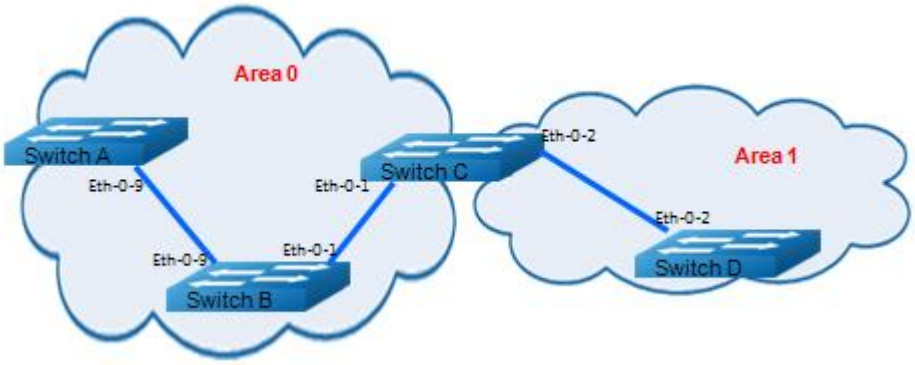
系统目前支持三种类型的OSPF 认证：无认证（类型0），明文认证（类型1）和MD5 认证（类型2）。无认证表示网络中的路由信息交换不需要经过任何认证。明文认证表示所有的路由器上配置的认证模式和密码都必须是一样的。MD5 认证表示用户需要在每台路由器上配置相同的密钥和密钥ID。路由器会根据密钥、密钥ID 和OSPF 报文内容生成消息摘要，添加加至OSPF 报文中。

认证类型可以基于区域内配置，也可以基于接口配置，这两者可以同时使用。如果接口上配置的认证类型和区域内配置的认证类型不一样，则优先使用接口上的认证类型。如果接口上没有配置认证类型，那么就使用区域内配置的认证类型。

下面的例子简单地介绍OSPF 的三种类型的认证。如图 3-6所示，配置Switch A 和Switch B 之间不使用认证；Switch B 和Switch C 之间使用明文认证；Switch C 和Switch D 之间使用MD5认证。

ii. 拓扑

图 3-6 配置 OSPF 认证拓扑图



iii. 配置步骤

Switch A：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)#interface eth-0-9	进入接口配置模式
Switch(config-if)#no switchport	设置接口为三层接口
Switch(config-if)#ip address 9.9.9.1/24	设置 IP 地址
Switch(config-if)#ip ospf authentication	接口上启用验证功能
Switch(config-if)#ip ospf authentication null	指定接口验证类型为空
Switch(config-if)# exit	退出接口配置模式
Switch(config)# router ospf	创建 OSPF 进程
Switch(config-router)# network 9.9.9.0/24 area 0	发布网段到 OSPF 中
Switch(config-router)# end	退出路由模式

Switch B：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)#interface eth-0-9	进入接口配置模式

命令举例	操作步骤
Switch(config-if)#no switchport	设置接口为三层接口
Switch(config-if)#ip address 9.9.9.2/24	设置 IP 地址
Switch(config-if)#ip ospf authentication	接口上启用验证功能
Switch(config-if)#ip ospf authentication null	指定接口验证类型为空
Switch(config-if)# exit	退出接口配置模式
Switch(config)#interface eth-0-1	进入接口配置模式
Switch(config-if)#no switchport	设置接口为三层接口
Switch(config-if)#ip address 1.1.1.1/24	设置 IP 地址
Switch(config-if)#ip ospf authentication	接口上启用明文验证功能
Switch(config-if)# ip ospf authentication-key test	指定接口认证密码
Switch(config-if)# exit	退出接口配置模式
Switch(config)# router ospf	创建 OSPF 进程
Switch(config-router)# network 9.9.9.0/24 area 0 Switch(config-router)# network 1.1.1.0/24 area 0	发布网段到 OSPF 中
Switch(config-router)# end	退出路由模式

Switch C：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)#interface eth-0-2	进入接口配置模式
Switch(config-if)#no switchport	设置接口为三层接口
Switch(config-if)#ip address 2.2.2.1/24	设置 IP 地址
Switch(config-if)# ip ospf message-digest-key 2 md5 ospf	设置接口的 OSPF 验证 KEY
Switch(config-if)# exit	退出接口配置模式
Switch(config)#interface eth-0-1	进入接口配置模式

命令举例	操作步骤
Switch(config-if)#no switchport	设置接口为三层接口
Switch(config-if)#ip address 1.1.1.2/24	设置 IP 地址
Switch(config-if)#ip ospf authentication	接口上启用明文验证功能
Switch(config-if)# ip ospf authentication-key test	设置接口的 OSPF 认证密码
Switch(config-if)# exit	退出接口配置模式
Switch(config)# router ospf	创建 OSPF 进程
Switch(config-router)# area 1 authentication message-digest Switch(config-router)# network 2.2.2.0/24 area 1 Switch(config-router)# network 1.1.1.0/24 area 0	发布网段到 OSPF 中，配置 area 1 的认证类型为 MD5
Switch(config-router)# end	退出路由模式

Switch D：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)#interface eth-0-2	进入接口配置模式
Switch(config-if)#no switchport	设置接口为三层接口
Switch(config-if)#ip address 2.2.2.2/24	设置 IP 地址
Switch(config-if)# ip ospf message-digest-key 2 md5 ospf	设置接口的 OSPF 验证 KEY
Switch(config-if)# exit	退出接口配置模式
Switch(config)# router ospf	创建 OSPF 进程
Switch(config-router)# area 1 authentication message-digest Switch(config-router)# network 2.2.2.0/24 area 1	发布网段到 OSPF 中，配置 area 1 的认证类型为 MD5
Switch(config-router)# end	退出路由模式

iv. 命令验证

- 检查Switch A的配置结果：

```
Switch# show ip ospf neighbor
OSPF process 0:
Neighbor ID     Pri   State           Dead Time   Address         Interface
9.9.9.2           1   Full/DR         00:00:38    9.9.9.2         eth-0-9
```

- 检查Switch B的配置结果：

```
Switch# show ip ospf neighbor
OSPF process 0:
Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.1           1   Full/Backup     00:00:35    1.1.1.2         eth-0-1
1.1.1.1           1   Full/Backup     00:00:38    9.9.9.1         eth-0-9
```

- 检查Switch C的配置结果：

```
Switch# show ip ospf neighbor
OSPF process 0:
Neighbor ID     Pri   State           Dead Time   Address         Interface
9.9.9.2           1   Full/DR         00:00:35    1.1.1.1         eth-0-1
2.2.2.2           1   Full/DR         00:00:38    2.2.2.2         eth-0-2
Switch# show ip ospf interface
eth-0-1 is up, line protocol is up
  Internet Address 1.1.1.2/24, Area 0, MTU 1500
  Process ID 0, Router ID 2.2.2.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State Backup, Priority 1, TE Metric 1
  Designated Router (ID) 9.9.9.2, Interface Address 1.1.1.1
  Backup Designated Router (ID) 2.2.2.1, Interface Address 1.1.1.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:01
  Neighbor Count is 1, Adjacent neighbor count is 1
  Crypt Sequence Number is 1301244696
  Hello received 385 sent 384, DD received 3 sent 5
  LS-Req received 1 sent 1, LS-Upd received 11 sent 14
  LS-Ack received 12 sent 10, Discarded 1
  Simple password authentication enabled
Switch# show ip ospf
 Routing Process "ospf 0" with ID 2.2.2.1
 Process uptime is 1 hour 7 minutes
 Process bound to VRF default
 Conforms to RFC2328, and RFC1583 Compatibility flag is disabled
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 This router is an ABR, ABR Type is Alternative Cisco (RFC3509)
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Refresh timer 10 secs
 Number of incomming current DD exchange neighbors 0/5
 Number of outgoing current DD exchange neighbors 0/5
```

```
Number of external LSA 0. Checksum 0x000000
Number of opaque AS LSA 0. Checksum 0x000000
Number of non-default external LSA 0
External LSA database is unlimited.
Number of LSA originated 17
Number of LSA received 57
Number of areas attached to this router: 2
    Area 0 (BACKBONE)
        Number of interfaces in this area is 1(1)
        Number of fully adjacent neighbors in this area is 1
        Area has no authentication
        SPF algorithm last executed 01:06:56.340 ago
        SPF algorithm executed 16 times
        Number of LSA 6. Checksum 0x034b09
    Area 1
        Number of interfaces in this area is 1(1)
        Number of fully adjacent neighbors in this area is 1
        Number of fully adjacent virtual neighbors through this area is 0
        Area has message digest authentication
        SPF algorithm last executed 00:03:29.430 ago
        SPF algorithm executed 17 times
        Number of LSA 5. Checksum 0x0230e3
```

- 检查Switch D的配置结果：

```
Switch# show ip ospf neighbor
OSPF process 0:
Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.1           1   Full/Backup     00:00:35    2.2.2.1         eth-0-2
```

4 IPv4 地址前缀列表配置

4.1 地址前缀列表简介

路由策略（Routing Policy）是为了改变网络流量所经过的途径而修改路由信息的技术，主要通过改变路由属性（包括可达性）来实现。地址前缀列表是路由策略的一种，作用比较灵活。一个地址前缀列表由前缀列表名标识。每个前缀列表可以包含多个表项，每个表项可以独立指定一个网络前缀形式的匹配范围，并用一个索引号来标识，索引号指明了进行匹配检查的顺序。在匹配的过程中，交换机按升序依次检查由索引号标识的各个表项。只要有某一表项满足条件，就意味着本次匹配过程结束，而不再进行下一个表项的匹配。

4.2 配置 IPv4 地址前缀列表

4.2.1 创建地址前缀列表

地址前缀列表用于 IP 地址过滤。同一个地址前缀列表可包含多个表项，一个表项包括地址和掩码位数。命令中的 deny 和 permit 关键字指定该匹配结果是拒绝或者允许。此时，多个表项之间是“或”的关系，即通过一个表项就可通过该地址前缀列表的过滤。没有通过任何一个表项的过滤就意味着没有通过该地址前缀列表的过滤。

地址前缀范围包括两个部分，分别由 mask-length、ge-length 与 le-length 决定。如果指定了这两部分，要被过滤的 IP 地址必须匹配这两部分规定的前缀范围。具体的匹配公式如下：

ip-address/mask-length < ge-length < le-length <= 32

例如，只指定 ge-length，则匹配范围为[ge-length,32]；只指定 le-length，则匹配范围为[ip-address/mask-length,le-length]；如果两者都指定，则匹配范围为[ge-length, le-length]。

如果在输入命令中没有指定序号，则交换机会自动为表项添加默认序号。默认序号从 5 开始，并且每次递增 5，例如，5、10、15。默认序号将从当前大于已分配的序号中选择，并且是其中的最小值。

表 4-1 创建地址前缀列表

命令	操作	说明
configure terminal	进入全局配置模式	-
ip prefix-list *prefix-list-name* [**seq** *sequence-number*] { **deny** | **permit** } { **any** | *ip-address/mask-length* } [**ge** *ge-length* | **le** *le-length*]	创建地址前缀列表	prefix-list-name: 地址前缀列表名称； sequence-number: 地址前缀列表表项序号，取值范围 1~65535； ip-address/mask-length: 网络地址和掩码位数。掩码位数的取值范围为 0~32； ge-length: 指定地址匹配的最小前缀长度，取值范围为 0~32； le-length: 指定地址匹配的最大前缀长度，取值范围为 0~32； 缺省情况下，未创建地址前缀列表

4.2.2 添加地址前缀列表描述

表 4-2 添加地址前缀列表描述

命令	操作	说明
configure terminal	进入全局配置模式	-
ip prefix-list *prefix-list-name* **description** *description-info*	添加地址前缀列表描述信息	prefix-list-name: 地址前缀列表名称； description-info: 地址前缀列表描述，取值范围为 0～80； 缺省情况下，未添加地址前缀列表描述信息

4.2.3 启用地址前缀列表序号

表4-3 启用地址前缀列表序号

命令	操作	说明
configure terminal	进入全局配置模式	-
ip prefix-list sequence-number	配置地址前缀列表显示序号	缺省情况下，地址前缀列表默认使用序号

4.3 显示与维护

4.3.1 查看地址前缀列表信息

表4-4 查看地址前缀列表信息

命令	操作	说明
show ip prefix-list [**summary** | **detail**] [*prefix-list-name*]	显示地址前缀列表的配置信息	如选择了关键字 summary 或 detail，可以显示前缀列表的统计摘要或详细统计信息
show ip prefix-list *prefix-list-name* [**seq** *sequence-number* | *ip-address/mask-length* [**longer** | **first-match**]]		prefix-list-name: 地址前缀列表名称； sequence-number: 地址前缀列表表项序号，取值范围 1~65535； ip-address/mask-length: 网络地址/掩码位数 e.g., 35.0.0.0/8； longer: 只显示掩码位数大于 mask-length 的表项； first-match: 只显示第一个匹配的表项

4.3.2 清除地址前缀列表信息

表4-5 清除地址前缀列表信息

命令	操作	说明
clear ip prefix-list [*prefix-list-name*] [*ip-address/mask-length*]	清除地址前缀列表的配置信息	prefix-list-name: 地址前缀列表名称； ip-address/mask-length: 网络地址/掩码位数 e.g., 35.0.0.0/8

4.4 配置举例

4.4.1 配置 Prefix-List 基本功能

i. 配置步骤

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# ip prefix-list test seq 1 deny 35.0.0.0/8 le 16	创建地址前缀列表 test，并创建一条长度为[8,16]、地址为 35.0.0.0/8 的拒绝表项，指定序号为 1
Switch(config)# ip prefix-list test permit any	指定地址前缀列表的匹配模式为允许，防止不匹配条目出现时拒绝通过
Switch(config)# ip prefix-list test description this prefix list is for test	添加地址前缀列表的描述信息
Switch(config)# ip prefix-list test permit 36.0.0.0/24	配置匹配 36.0.0.0/24 的允许表项
Switch(config)# exit	退出全局配置模式

ii. 命令验证

显示地址前缀列表的详细信息：

```
Switch# show ip prefix-list detail
Prefix-list list number: 1
Prefix-list entry number: 3
Prefix-list with the last deletion/insertion: test
ip prefix-list test:
    Description: this prefix list is for test
    count: 3, range entries: 0, sequences: 1 - 10
      seq 1 deny 35.0.0.0/8 le 16 (hit count: 0, refcount: 0)
      seq 5 permit any (hit count: 0, refcount: 0)
      seq 10 permit 36.0.0.0/24 (hit count: 0, refcount: 0)
```

4.4.2 配置 Prefix-list 与 RIP 的简单应用

i. 配置步骤

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式

命令举例	操作步骤
Switch(config)# ip prefix-list aa seq 11 deny 35.0.0.0/8 le 16	创建地址前缀列表 aa，并创建一条长度为[8,16]、地址为 35.0.0.0/8 的拒绝表项，指定序号为 11
Switch(config)# ip prefix-list aa permit any	指定地址前缀列表的匹配模式为允许，防止不匹配条目出现时拒绝通过
Switch(config)# router rip	进入 RIP 路由模式
Switch(config-router)# distribute-list prefix aa out	过滤所有 RIP 发送的路由
Switch(config-router)# end	退出 RIP 路由模式

ii. 命令验证

显示地址前缀列表的配置信息：

```
Switch# show ip prefix-list

ip prefix-list aa: 2 entries
        seq 11 deny 35.0.0.0/8 le 16
        seq 15 permit any
Switch# show running-config
Building configuration...
…
ip prefix-list aa seq 11 deny 35.0.0.0/8 le 16
ip prefix-list aa seq 15 permit any
…
router rip
  distribute-list prefix aa out
```

4.4.3 配置 Prefix-list 与 Route-map 的应用

i. 配置步骤

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# ip prefix-list aa seq 11 deny 3.3.3.0/8 le 24	创建地址前缀列表 aa，并创建一条长度为[8,24]、地址为 3.3.3.0/8 的拒绝表项，指定序号为 11

命令举例	操作步骤
Switch(config)# ip prefix-list aa permit any	指定地址前缀列表的匹配模式为允许，防止不匹配条目出现时拒绝通过
Switch(config)# route-map abc permit	创建 route-map 并进入 route-map 配置模式
Switch(config-route-map)# match ip address prefix-list aa	匹配地址前缀列表 aa
Switch(config-route-map)# set local-preference 200	设置本地优先级为 200
Switch(config-route-map)# exit	退出 route-map 配置模式
Switch(config)# route-map abc permit 20	重新定义一个策略，防止不匹配条目出现时拒绝通过
Switch(config-route-map)# exit	退出 route-map 配置模式
Switch(config)# router bgp 1	进入 BGP 路由模式
Switch(config-router)# neighbor 1.1.1.2 remote-as 1	配置 BGP 邻居
Switch(config-router)# neighbor 1.1.1.2 route-map abc out	在 BGP 路由上应用路由策略
Switch(config-router)# network 2.2.2.2/32	BGP 路由中宣告网段
Switch(config-router)# network 3.3.3.3/32	BGP 路由中宣告网段
Switch(config-router)# end	退出 BGP 路由模式

ii. 命令验证

显示 Route-map 的配置信息：

```
Switch# show route-map

route-map abc, permit, sequence 10
  Match clauses:
    ip address prefix-list aa
  Set clauses:
    local-preference 200
route-map abc, permit, sequence 20
  Match clauses:
Set clauses:
Switch# show running-config
Building configuration...
…
```

```
ip prefix-list aa seq 11 deny 3.3.3.0/8 le 24
ip prefix-list aa seq 15 permit any
!
!
route-map abc permit 10
  match ip address prefix-list aa
  set local-preference 200
!
route-map abc permit 20
…
router bgp 1
  neighbor 1.1.1.2 remote-as 1
  !
  address-family ipv4
  no synchronization
  network 2.2.2.2 mask 255.255.255.255
  network 3.3.3.3 mask 255.255.255.255
  neighbor 1.1.1.2 activate
  neighbor 1.1.1.2 route-map abc out
  exit-address-family
  !
  address-family vpnv4 unicast
  no synchronization
  exit-address-family
```

说明

更多关于Route-map的介绍及配置请见第五章“Route-map配置”。

5 Route-map 配置

5.1 Route-map 简介

路由策略（Routing Policy）是为了改变网络流量所经过的途径而修改路由信息的技术，主要通过改变路由属性（包括可达性）来实现。

路由器在发布与接收路由信息时，可能需要实施一些策略，以便对路由信息进行过滤，例如只接收或发布满足一定条件的路由信息。一种路由协议可能需要引入其它的路由协议发现的路由信息，路由器在引入其它路由协议的路由信息时，可能只需要引入一部分满足条件的路由信息，并控制所引入的路由信息的某些属性，以使其满足本协议的要求。

为实现路由策略，首先要定义将要实施路由策略的路由信息的特征，即定义一组匹配规则，又称为 match 语句。如果匹配条件，就会执行 set 指定的相关动作。这个动作不是必要的，可以使用路由信息中的不同属性作为匹配依据进行设置，如目的地址、发布路由信息的路由器地址等。匹配规则可以预先设置好，然后再将它们应用于路由的发布、接收和引入等过程的路由策略中。

5.2 配置 Route-map

5.3.1 创建 Route-map

表5-1 创建Route-map

命令	操作	说明
configure terminal	进入全局配置模式	-
route-map *map-tag* [**permit** | **deny**] [*sequence-number*]	如何创建一个 Route-map 并进入 Route-map 配置模式	map-tag: route-map 名称，长度不得超过 20 个字符，并且它的首字母必须是'a'-'z', 'A'-'Z'或者'0'-'9'； sequence-number: route-map 的序列号，取值范围为 1~65535

5.3.2 配置 match 语句

如果指定了一个 permit 的 match 规则，路由将会被像 set 规则指定的那样进行重发布或者进行控制。相反，如果制定了相应的 deny 规则，满足条件的路由将不会被重发布或者控制。如果没有匹配到任何规则的话，路由将不会被接受或者转发。

被策略指定的路由不能和路由协议指定的路由相同，指定的策略让报文能够按照他们的长度及内容通过不同的路由进行转发。相对于路由表指定的路径来说，报文将会优先以配置的策略来进行转发。

1. 通过ACL或者IP地址前缀列表匹配路由

表5-2 功能配置与参数说明

命令	操作	说明
configure terminal	进入全局配置模式	-
route-map *map-tag* [**permit** | **deny**] [*sequence-number*]	如何创建一个 route-map 并进入 route-map 配置模式	map-tag: route-map 名称，长度不得超过 20 个字符，并且它的首字母必须是'a'-'z', 'A'-'Z'或者'0'-'9'； sequence-number: route-map 的序列号，取值范围为 1~65535
match ip address *ipv4-acl-name*	指定匹配一个 ACL 的规则	ipv4-acl-name: 指定 IPV4 ACL 名；缺省情况下，未配置该规则
match ip next-hop *ipv4-acl-name*	指定匹配一个下一跳的 IP 地址	
match ip address prefix-list *list-name*	匹配一个前缀列表条目	list-name: IP 前缀列表名；缺省情况下，未配置该规则
match ip next-hop prefix-list *list-name*	匹配下一跳的前缀列表条目	

2. 配置通过度量值匹配路由

表5-3 功能配置与参数说明

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

命令	操作	说明
route-map *map-tag* [**permit** | **deny**] [*sequence-number*]	如何创建一个 route-map 并进入 route-map 配置模式	map-tag: route-map 名称，长度不得超过 20 个字符，并且它的首字母必须是'a'-'z', 'A'-'Z'或者'0'-'9'； sequence-number: route-map 的序列号，取值范围为 1~65535
match metric *metric-value*	指定度量值匹配路由	metric-value: 度量值，取值范围为 0~4294967295；缺省情况下，未配置该规则

3. 配置BGP协议中生效的匹配条件

表5-4 功能配置与参数说明

命令	操作	说明
configure terminal	进入全局配置模式	-
route-map *map-tag* [**permit** | **deny**] [*sequence-number*]	如何创建一个 route-map 并进入 route-map 配置模式	map-tag: route-map 名称，长度不得超过 20 个字符，并且它的首字母必须是'a'-'z', 'A'-'Z'或者'0'-'9'； sequence-number: route-map 的序列号，取值范围为 1~65535
match as-path *list-name*	指定自治系统匹配的路径	list-name: 指定自治系统路径的 ACL 名；缺省情况下，未配置该规则
match community *community-list-name*	指定匹配的团体属性(Community)号	community-list-name: Community 列表名；缺省情况下，未配置该规则
match interface *if-name*	指定接口的匹配规则	if-name: 接口名；缺省情况下，未配置该规则
match local-preference *preference-level*	指定本地优先级的匹配规则	preference-level: 本地优先级，取值范围为 0~4294967295；缺省情况下，未配置该规则
match origin { **egp** | **igp** | **incomplete** }	匹配 BGP 路由的起始(origin)属性	egp：表明这一条路由的起始信息是从外部网关协议(EGP)中学习到的； igp:表示起始路径信息是通过内部网关协议(IGP)学习到的。 incomplete: 这个路由的原始路径是通过不清楚或者其他别的方式来学

命令	操作	说明
		习到的。比如，一个静态路由被重发布到 BGP 时，那它的原始路由就是不完整的； 缺省情况下，未配置该规则

4. 配置基于路由信息的匹配条件

表5-5 功能配置与参数说明

命令	操作	说明
configure terminal	进入全局配置模式	-
route-map *map-tag* [**permit** | **deny**] [*sequence-number*]	如何创建一个 route-map 并进入 route-map 配置模式	map-tag: route-map 名称，长度不得超过 20 个字符，并且它的首字母必须是'a'-'z', 'A'-'Z'或者'0'-'9'； sequence-number: route-map 的序列号，取值范围为 1~65535
match route-type external { **type-1** | **type-2** }	根据路由信息匹配指定的外部路由类型	自治系统外部 LSA 即类型 1 或者类型 2。外部类型 1 值匹配类型 1 的外部路由，外部类型 2 只匹配类型 2 的外部路由；缺省情况下，未配置该规则
match tag *tag-value*	根据路由信息匹配指定的 tag	tag-value: 取值范围为 0~4294967295；缺省情况下，未配置该规则

5.3.3 配置 set 动作

1. 配置BGP路由属性

表5-6 功能配置与参数说明

命令	操作	说明
configure terminal	进入全局配置模式	-
route-map *map-tag* [**permit** | **deny**] [*sequence-number*]	如何创建一个 route-map 并进入 route-map 配置模	map-tag: route-map 名称，长度不得超过 20 个字符，并且它的首字母必须是

命令	操作	说明
	式	'a'-'z', 'A'-'Z'或者'0'-'9'； sequence-number: route-map 的序列号，取值范围为 1~65535
set aggregator as *as-number ip-address*	配置 route-map 和 router ID 的 AS 号	自治系统(AS)是一个网络管理机构控制下的路由器和网络群组。它们被不同的区域所分离，被指派了一个独特的 16 位的号码； as-number: 指定集合的 AS 号；缺省情况下，未配置该规则
set as-path prepend *as-number* [*as-number*]	修改自治系统(AS)的路径	通过指定 AS-Path 的长度，路由器可以影响路径的最佳路径选择。在这个命令中使用 prepend 参数，来在已有的 AS-Path 中，再追加一个指定的 AS-Path。缺省情况下，未配置该规则
set comm-list { *std-list-num* | *ext-list-num* | *list-name* } **delete**	删除匹配条件的团体属性	std-list-num: 标准 community 列表号； ext-list-num: 扩展 community 列表号； list-name: community 列表名； 缺省情况下，未配置该规则
set community [*aa:nn* | **internet** | **local-AS** | **no-advertise** | **no-export**]	配置团体属性	aa: AS 号； nn: 指定的 community 号； 缺省情况下，未配置该规则
set extcommunity { **rt** | **soo**} *ext-comm-number* [*extcomm-number*]	配置扩展团体属性	extcomm-number: 数字或 IP 地址形式的 AS 号；缺省情况下，未配置该规则
set local-preference *preference-level*	配置本地优先级属性	preference-level: 本地优先级，取值范围为 0~4294967295；缺省情况下，未配置该规则
set origin { **egp** | **igp** | **incomplete** }	配置 BGP 路由的 Origin 属性	缺省情况下，未配置该规则

2. 配置路由的度量值属性

表5-7 功能配置与参数说明

命令	操作	说明
configure terminal	进入全局配置模式	-
route-map *map-tag* [**permit** | **deny**] [*sequence-number*]	如何创建一个 route-map 并进入 route-map 配置模式	map-tag: route-map 名称，长度不得超过 20 个字符，并且它的首字母必须是'a'-'z', 'A'-'Z'或者'0'-'9'； sequence-number: route-map 的序列号，取值范围为 1~65535
set metric *metric-value*	配置一条路由的 metric 值，以及一个关于 AS 的首选路径影响的外部邻居	metric-value: 度量值，取值范围为 0~4294967295；缺省情况下，未配置该规则

3. 配置路由信息的下一跳地址

表5-8 功能配置与参数说明

命令	操作	说明
configure terminal	进入全局配置模式	-
route-map *map-tag* [**permit** | **deny**] [*sequence-number*]	如何创建一个 route-map 并进入 route-map 配置模式	map-tag: route-map 名称，长度不得超过 20 个字符，并且它的首字母必须是'a'-'z', 'A'-'Z'或者'0'-'9'； sequence-number: route-map 的序列号，取值范围为 1~65535
set ip next-hop *next-hop-address*	配置指定的下一跳地址	next-hop-address: 下一跳的 IP 地址；缺省情况下，未配置该规则

4. 配置目的路由协议的metric类型

表5-9 功能配置与参数说明

命令	操作	说明
configure terminal	进入全局配置模式	-
route-map *map-tag* [**permit** | **deny**] [*sequence-number*]	如何创建一个 route-map 并进入 route-map 配置模式	map-tag: route-map 名称，长度不得超过 20 个字符，并且它的首字母必须是'a'-'z', 'A'-'Z'或者'0'-'9'； sequence-number: route-map 的序列号，取值范围为 1~65535

命令	操作	说明
set metric-type { **type1** | **type2** }	配置目的路由协议的 metric 类型	缺省情况下，未配置该规则

5. 配置路由信息的tag值

表5-10 功能配置与参数说明

命令	操作	说明
configure terminal	进入全局配置模式	-
route-map *map-tag* [**permit** | **deny**] [*sequence-number*]	如何创建一个 route-map 并进入 route-map 配置模式	map-tag: route-map 名称，长度不得超过 20 个字符，并且它的首字母必须是'a'-'z', 'A'-'Z'或者'0'-'9'； sequence-number: route-map 的序列号，取值范围为 1~65535
set tag *tag-value*	配置路由信息的 tag 值	tag-value: 取值范围为 0~4294967295；缺省情况下，未配置该规则

5.3 显示与维护

表5-11 显示与维护

命令	操作	说明
show route-map [*map-tag*]	显示 Route-map 配置信息	map-tag: route-map 名称，长度不得超过 20 个字符，并且它的首字母必须是'a'-'z', 'A'-'Z'或者'0'-'9'

5.4 配置举例

5.4.1. 配置 Route-map 应用至 OSPF

i. 配置步骤

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# route-map abc permit	创建一个路由策略并进入 Route-map 配置模式
Switch(config-route-map)# match metric 20	指定度量值匹配路由
Switch(config-route-map)# set tag 2	配置路由信息的 tag 值
Switch(config-route-map)# exit	退出 Route-map 配置模式
Switch(config)# route-map abc permit 20	重新定义一个策略，防止不匹配条目出现时拒绝通过
Switch(config-route-map)# exit	退出 Route-map 配置模式
Switch(config)# router ospf 100	进入 OSPF 路由模式
Switch(config-router)# redistribute rip route-map abc	将 RIP 协议重分布到 OSPF 中，并且使用策略 abc
Switch(config-router)# end	退出 OSPF 路由模式

ii. 命令验证

显示 Route-map 配置信息：

```
Switch# show route-map

route-map abc, permit, sequence 10
  Match clauses:
    metric 20
  Set clauses:
    tag 2
route-map abc, permit, sequence 20
  Match clauses:
  Set clauses:
```

5.4.2. 配置 Route-map 应用至 BGP

i. 配置步骤

命令举例	操作步骤
DUT# configure terminal	进入全局配置模式
DUT(config)# ip access-list acl1	创建 IPv4 访问控制列表，并进入访问控制列表配置模式
DUT(config-ip-acl)# permit any 3.3.3.0 0.0.0.255 any	设置匹配的条目
DUT(config-ip-acl)# exit	退出 IPv4 ACL 配置模式
DUT(config)# route-map abc permit	创建路由策略
DUT(config-route-map)# match ip address acl1	匹配一个 ACL 的规则
DUT(config-route-map)# set local-preference 200	配置本地优先级属性
DUT(config-route-map)# exit	退出 Route-map 配置模式
DUT(config)# route-map abc permit 20	重新定义一个策略，防止不匹配条目出现时拒绝通过
DUT(config-route-map)# exit	退出 Route-map 配置模式
DUT(config)# router bgp 1	进入 BGP 路由模式
DUT(config-router)# neighbor 1.1.1.2 remote-as 1	配置 BGP 邻居
DUT(config-router)# neighbor 1.1.1.2 route-map abc out	在 BGP 路由上应用路由策略
DUT(config-router)# network 2.2.2.2/32	BGP 路由中宣告网段
DUT(config-router)# network 3.3.3.3/32	BGP 路由中宣告网段
DUT(config-router)# end	退出 BGP 路由模式

ii. 命令验证

显示 Route-map 配置信息：

```
DUT1# show route-map

route-map abc, permit, sequence 10
  Match clauses:
    ip address acl1
  Set clauses:
    local-preference 200
route-map abc, permit, sequence 20
  Match clauses:
```

```
  Set clauses:
DUT2# show ip bgp
BGP table version is 6, local router ID is 1.1.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*>i2.2.2.2/32       1.1.1.1                  0    100      0 i
*>i3.3.3.3/32       1.1.1.1                  0    200      0 i
```

6 策略路由配置

6.1 策略路由简介

与单纯基于 IP 报文的目的地址进行转发不同，策略路由（Policy-Based Routing，缩写：PBR）提供更灵活的路由转发的机制。它可以依照匹配的条件，如 IP 报文的源地址、度量值、tag、报文长度等进行路由选择，执行指定的操作。一般来说，策略路由的优先级比普通路由高，报文到达后会根据配置策略路由进行转发。如果不满足匹配的条件，则按照普通路由转发。

策略路由一般可分为两种类型：本地策略路由与转发策略路由。本地策略路由只对本设备发出的报文进行策略路由，对于外部设备发送给本机的报文没有影响；而转发策略路由只对接口接收的报文进行策略路由，对于从该接口转发出去的报文不受影响。

6.2 配置策略路由

6.2.1 启用/关闭策略路由功能

若要启用 PBR，用户需要配置一个有 match 和 set 语句的 route-map，然后才能在一个三层端口上启用 PBR 功能。所有进入这个端口的报文，都会去匹配这个 route-map 指定的 match 策略。如果报文满足 match 策略，将会按照 set 指定的规则进行相应的转发处理。具体可参见 6.3 配置举例。

表6-1 启用/关闭PBR功能

命令	操作	说明
ip policy route-map *map-name*	在设备上启用 PBR	map-name：策略路由映射名；缺省情况下，PBR 功能处于关闭状态
no ip policy route-map	关闭 PBR 功能	

6.2.2 查看策略路由配置信息

表6-2 查看策略路由配置信息

命令	操作	说明
show ip policy route-map	显示策略路由的配置信息	-

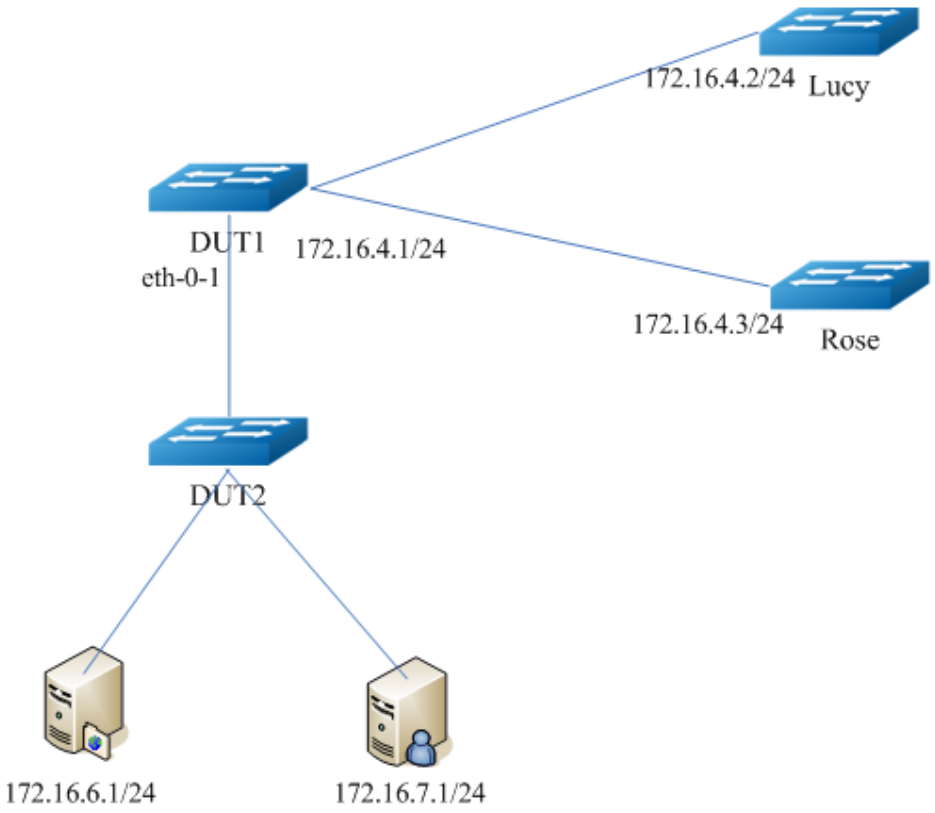
6.3 配置举例

6.3.1 介绍

下图是策略路由的一个典型配置：在Switch的eth-0-1端口上应用一个PBR，源地址为172.16.6.1的报文将会被转发给Lucy,，源地址是172.16.7.1将会进行正常的路由转发。

6.3.2 拓扑

图 6-1 策略路由典型拓扑图



6.3.3 配置步骤

命令举例	操作步骤
DUT# configure terminal	进入全局配置模式
DUT(config)# ip access-list acl1	定义一个 IPV4 ACL 并且进入 ACL 配置模式
DUT(config-ip-acl)# 10 permit any 172.16.6.0 0.0.0.255 any	配置一个允许源地址为 172.16.6.0 的报文进入的 ACE
DUT(config-ip-acl)# exit	退出 ACL 配置模式
DUT(config)# route-map richard permit 10	创建一个名为 Richard 的 route-map 并且进入 route-map 配置模式
DUT(config-route-map)# match ip address acl1	配置一个匹配 acl1 的 match 语句
DUT(config-route-map)# set ip next-hop 172.16.4.2	设置满足匹配条件的数据包的转发地址为 172.16.4.2
DUT(config-route-map)# exit	退出 Route-map 配置模式
DUT(config)# interface eth-0-1	进入接口配置模式
DUT(config-if)# no switchport	将端口设置为三层口
DUT(config-if)# ip address 172.16.5.2/24	设置接口的 IP 地址
DUT(config-if)# no shutdown	启用这个接口
DUT(config-if)# ip policy route-map richard	在这个接口上应用 Richard 这个策略
DUT(config-if)# exit	退出接口配置模式

6.3.4 命令验证

显示 Route-map 的配置信息：

```
Switch# show ip policy route-map
Route-map                       interface
richard                         eth-0-1
```

7 BGP 配置

7.1 BGP 简介

边界网关协议（Border Gateway Protocol，缩写：BGP）是运行于TCP上的一种内部自治系统路由协议。BGP通告系统的主要功能是在不同的自治系统（AS）来交换网络上的可达信息，在AS之间实现路由信息的交互。这些信息能有效地避免路由环路，以及在这个AS级别上实施强制性的策略。

按照运行方式的不同，BGP可以分为IBGP（Internal/Interior BGP）和EBGP（External/Exterior BGP）两类，它们的定义分别为：

- IBGP:：在一个自治系统内的两个或多个对等体之间运行的BGP，即在相同的AS内建立BGP连接，完成同一AS内路由信息的传递。
- EBGP：在不同的自治系统的对等体之间运行的BGP，即在不同AS之间建立的BGP连接，完成不同AS之间路由信息的交换。

BGP-4 是 BGP 的第四版，提供了一组新的机制支持无类域内路由（CIDR）[RFC1518, RFC1519]。这些机制包括发布一组 IP 前缀的目的地址以及消除 BGP 中“类”的概念。BGP-4 也引入了一些支持路由聚合（包括 AS 路径的聚合）的机制。

7.2 配置 BGP 的基本功能

7.2.1 启动 BGP 进程

表7-1启动BGP进程

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# router bgp 12	启动 BGP 路由进程	AS 号的取值范围为

命令举例	操作	说明
		1~4294967295
Switch(config-router)# end	退出路由模式	-

7.2.2 创建 BGP 路由器 ID

表7-2 创建BGP Router ID

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# router bgp 12	启动 BGP 路由进程	AS 号的取值范围为 1~4294967295
Switch(config-router) bgp router-id 1.1.2.3	创建 BGP 的路由器标识	router-id: 点分十进制

说明

如果配置了环回接口，route-id 将会设置为环回接口的地址，否则，最高的 IP 地址将会设置为 router-id。

7.2.3 配置 BGP 对等体

BGP 对等体也称为 BGP 邻居，指定 BGP 邻居后才能建立的内部或者外部的 BGP（IBGP 或者 EBGP）的 TCP 会话。

表7-3 配置BGP对等体

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# router bgp 12	启动 BGP 路由进程	AS 号的取值范围为 1~4294967295
Switch(config-router)# neighbor 10.10.0.73 remote-as 345	指定 BGP 邻居	以 IP 地址格式来指定 BGP 邻居的地址

7.2.4 创建对等体组

配置该命令可以更新各种策略，使用**neighbor**命令来简单的配置对等体组。任何对对等体组的修改会对所有的成员产生影响。创建对等体组后，用户可根据实际情况增加一个邻居。

表7-4 创建对等体组

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# router bgp 12	启动 BGP 路由进程	AS 号的取值范围为 1~4294967295
Switch(config-router)# neighbor group1 peer-group	创建对等体组	group1: 对等体组名
Switch(config-router)# neighbor 10.10.0.63 peer-group group1	将邻居 10.10.0.63 加入对等体组 group1	以 IP 地址格式来指定 BGP 邻居的地址

7.2.5 配置重分布路由

可引入的源路由协议，包括OSPF路由、BGP路由，还有静态路由和直连路由。可以通过该命令配置重分布的度量值、路由映射等。

表7-5 配置重分布路由

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# router bgp 12	启动 BGP 路由进程	AS 号的取值范围为 1~4294967295
Switch(config-router)# address family ipv4 vrf evpn-tenant-1	进入 IPv4 地址族配置模式	vrf evpn-tenant-1: VPN 路由/转发实例名
Switch(config-router-af)# redistribute connected	重分布直连路由到 BGP	默认不使能重发布，度量值的默认值为 1

说明

在路由模式下，可以进入不同的地址族配置模式:

- 使用 **address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*] 命令，进入IPv4地址族配置模式;
- 使用 **address-family vpnv4** [**unicast**] 命令，进入VPNv4地址族配置模式;

退出该模式使用相应的 **exit** 或者 **exit-address-family** 命令。

7.3 配置 RR 与 BGP 联盟 ID

7.3.1 配置路由反射器 (RR)

路由反射器（RR）可以解决 AS 中的 IBGP 对等体爆炸式增长的问题。通过 RR，在 AS 中 IBGP 对等体的数量会减少。使用 **neighbor route-reflector-client** 命令，来配置指定邻居作为 client 以及本地路由作为 RR。

表7-6 配置路由反射器

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# router bgp 12	启动 BGP 路由进程	AS 号的取值范围为 1~4294967295
Switch(config-router)# neighbor 10.10.0.72 route-reflector-client	配置 BGP 路由反射器及其客户端 (client)	以 IP 地址格式来指定 BGP 邻居的地址

缺省情况下，路由反射器使用自己的 Route-id 作为集群ID。但是为了增加冗余，一个集群可能会有多个RR。当配置一个以上的RR时，执行 **bgp cluster-id** *cluster-id* 命令，配置路由反射器的集群 ID；且当配置了 RR 时，默认客户端之间的路由反射处于开启状态，用户也可执行 **no bgp client-to-client reflection** 关闭客户端之间的路由反射。

7.3.2 配置 BGP 联盟 ID

由于从 IBGP 邻居收到的路由无法转发给其它 IBGP 邻居，而从 EBGP 邻居接收的路由可以转发给任何邻居，包括 IBGP。因此，在拥有多个路由器的大型 AS 中，可以通过配置 BGP 联盟解决路由限制的问题。联盟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。配置联盟后，原 AS 号将作为每个路由器的联盟 ID。

表7-7 配置BGP联盟ID

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# router bgp 12	启动 BGP 路由进程	AS 号的取值范围为 1~4294967295
Switch(config-router) bgp confederation identifier 1	配置 BGP 的联盟 ID	BGP 联盟 ID 的取值范围为 1~65535

7.4 配置 BGP 路由选路

7.4.1 配置 BGP 的管理距离

管理距离标识了一个路由器的可靠性，这个值越高越不可靠。用户可以对外部、内部和本地的路由设置管理距离。外部路径是从 AS 外部邻居学习到的路由，内部路由是在同一个 AS 的另外一个路由器中学习到的路由；而本地路由则是本路由器从别的进程中通过重发布学习到的路由。如果修改了管理距离，路由表中会出现矛盾，并且阻塞路由。

表7-8 配置BGP管理距离

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# router bgp 12	启动 BGP 路由进程	AS 号的取值范围为 1~4294967295
Switch(config-router) distance 34 10.10.0.0/24 mylist	配置 BGP 的管理距离	管理距离的取值范围为 1~255

7.4.2 配置下一跳属性

当 BGP 路由器通过 EBGP 获取路由，并且这些路由需要广播给一个 IBGP 邻居时，发送的下一跳信息并不改变。使用这个命令，BGP 路由器可以改变发送给 IBGP 对等体的下一跳信息，将下一跳信息设置为这个邻居进行通信的接口的 IP 地址。

表7-9 配置下一跳属性

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# router bgp 12	启动 BGP 路由进程	AS 号的取值范围为 1~4294967295
Switch(config-router)# neighbor 10.10.0.72 remote-as 100	指定 BGP 邻居	以 IP 地址格式来指定 BGP 邻居的地址
Switch(config-router)# neighbor 10.10.0.72 next-hop-self	配置 BGP 设备向 IBGP 对等体（组）发布路由时，将下一跳地址设置为自身的 IP 地址	

根据实际组网情况，可以执行 **neighbor** *neighbor-id* **attribute-unchanged** { **as-path** | **next-hop** | **med** }命令，配置发布路由时不改变下一跳地址。

7.4.3 配置默认本地优先级

当存在通往同一个目的的多条路径时，可以配置优先级比较高的那条路径。这个优先级对本地AS的所有路由器和接入服务器有效。

表7-10 配置默认本地优先级

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# router bgp 12	启动 BGP 路由进程	AS 号的取值范围为 1~4294967295
Switch(config-router) bgp default local-preference 2345555	修改默认的本地优先级	优先级的取值范围为 0~4294967295，缺省情况下为 100

7.4.4 配置 MED 属性

使用这个命令来指定 Multi Exit Discriminator (MED) 的两个属性：confed 和 missing-as-worst。confed 属性使 MED 通过联盟对等体中学到的路径来进行比较。MED 仅在没有扩展的 AS 路径中比较，不在联盟 AS 路径中比较。如果存在一个扩展的 AS，MED 比较就不会进行。

missing-as-worst 属性则将丢失的 MED 作为路径中为无限大的值，将丢失了 MED 的路径作为最差的路径来考虑。如果没有使能 missing-as-worst，丢失的 MED 值是 0，由此这条路径就是 BGP 的最佳路径。

表7-11 配置MED属性

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# router bgp 12	启动 BGP 路由进程	AS 号的取值范围为 1~4294967295
Switch(config-router) bgp bestpath med missing-as-worst	将丢失的 MED 作为优先选择的对象	-

MED 只在相同的 AS 的路径中进行比较，在本地 AS 的路由器上使能 **bgp deterministic-med** 命令，可以获取一个比较结果。使用 **bgp always-compare-med** 命令能在不同的 AS 之间比较 MED。选择最佳路径以后才可以使用 MED 参数，拥有较低 MED 的路径会被优先使用。

7.4.5 配置 BGP 团体属性

BGP 团体（community）属性用于实现策略路由。这是个可选的属性，并且可以促进本地策略通过不同的 AS 来传输。可以配置有两种团体属性：扩展团体属性和标准团体属性。

表7-12 配置BGP团体属性

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# ip community-list 20 permit 7675:80 7675:90	新增一个团体列表条目	以 AA:NN 格式来呈现： AA = AS 号； NN = 指定的 community 号

标准的团体列表被编译为二进制格式，并且直接和 BGP 更新的团体属性相比较。这个比较过程比扩展团体列表要快。任何不匹配标准团体属性的值都会自动被视为扩展团体值。

表7-13 配置BGP标准团体属性

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-

命令举例	操作	说明
Switch(config)# ip community-list standard CLIST permit 7675:80 7675:90 no-export	新增一个标准团体列表条目	以 AA:NN 格式来呈现： AA = AS 号； NN = 指定的 community 号

表7-14 配置BGP扩展团体属性

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# ip community-list expanded CLIST permit .*	新增一个扩展团体列表条目	指定使用常规表述来描述团体列表

7.5 控制 BGP 路由的发送和接收

7.5.1 配置 BGP 邻居路由的过滤

表7-15 配置BGP邻居路由的过滤

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# router bgp 12	启动 BGP 路由进程	AS 号的取值范围为 1~4294967295
Switch(config-router)# neighbor 1.2.3.4 distribute-list mylist out	配置对发布的邻居路由进行过滤	以 IP 地址格式来指定 BGP 邻居的地址。 in：表示过滤接收的宣告路由； out：表示过滤发布的宣告路由

7.5.2 配置基于 AS 路径的过滤

表7-16 配置基于AS路径的过滤

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-

命令举例	操作	说明
Switch(config)# router bgp 12	启动 BGP 路由进程	AS 号的取值范围为 1~4294967295
Switch(config-router)# neighbor 10.10.0.34 filter-list listname out	创建 AS 路径的过滤器，对发布的路由进行过滤	以 IP 地址格式来指定 BGP 邻居的地址。 in：表示过滤接收的宣告路由； out：表示过滤发布的宣告路由

7.5.3 配置基于前缀列表的过滤

这个命令用于过滤 BGP 宣告路由的前缀列表。如果没有匹配到任何前缀列表的条目，就会拒绝这个路由的访问。当多个前缀列表的条目满足条件时，就会选择最小序列号的条目进行匹配。路由器从前缀列表的最上方（序号 1）开始搜索，一旦匹配 match 或者 deny，便不再继续往下搜索。

表7-17 配置基于前缀列表的过滤

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# ip prefix-list list1 deny 30.0.0.0/24	指定地址前缀列表的匹配模式为拒绝	掩码位数的取值范围为 0~32
Switch(config)# router bgp 12	启动 BGP 路由进程	AS 号的取值范围为 1~4294967295
Switch(config-router)# neighbor 10.10.10.10 prefix-list list1 in	配置过滤接收的 BGP 宣告路由的前缀列表	以 IP 地址格式来指定 BGP 邻居的地址。 in：表示过滤接收的宣告路由； out：表示过滤发布的宣告路由

7.6 配置 BGP 定时器

7.6.1 配置全局定时器

全局使用该命令可以设定 BGP 的存活时间（keepalive）和保持时间（holdtime）的值。

表7-18 配置全局定时器

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# router bgp 12	启动 BGP 路由进程	AS 号的取值范围为 1~4294967295
Switch(config-router)# timers bgp 40 120	全局设定 BGP keepalive 定时器和 holdtime 定时器的值	keepalive-time：信息被送往邻居的频率，取值范围为 0~65535，单位：秒；默认值为 60s； hold-time：当未接收到 keepalive 信息时，邻居会话中断的间隔时间。取值范围为 3~65535，单位：秒；默认值为 180s

7.6.2 配置邻居定时器

配置该命令可以设定 BGP 对等体（邻居）的定时器，即存活时间（keepalive）和保持时间（holdtime）的值。

表7-19 配置邻居定时器

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# router bgp 12	启动 BGP 路由进程	AS 号的取值范围为 1~4294967295
Switch(config-router)# neighbor 10.10.10.10 timers 60 120	设定 BGP 对等体 keepalive 定时器和 holdtime 定时器的值	以 IP 地址格式来指定 BGP 邻居的地址； keepalive-time：信息被送往邻居的间隔时间，取值范围为 0~65535，单位：秒；默认值为 60s； hold-time：当未接收到 keepalive 信息时，邻居会话中断的间隔时间。取值范围为 3~65535，单位：秒；默

命令举例	操作	说明
		认值为 180s

7.7 配置 BGP 路由聚合

聚合用于将路由表的规模最小化。聚合通过一些特征，将不同的路由聚合起来，并宣告为一条路由。如果更确定的BGP路由在可选择的范围内，**aggregate-address**命令在BGP路由表中创建了一个聚合条目。使用参数summary-only只宣告前缀，对所有邻居抑制更确定的路由。

表7-20 配置BGP路由聚合

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# router bgp 12	启动 BGP 路由进程	AS 号的取值范围为 1~4294967295
Switch(config-router)# aggregate-address 10.0.0.0/8 as-set summary-only	配置 BGP 聚合条目	A.B.C.D/M 指定聚合的 IP 前缀；summary-only：在更新过程中过滤更多的指定路由

7.8 配置向 BGP 邻居发送缺省路由

每个路由器都应该有默认的路由，它用于向非本地 IP 路由表中的网络发送数据包。确保路由器有缺省路由的方法有两种。方法一：给所有路由器配置一个静态路由，确保每个路由器都有一个默认路由。方法二：创建一个默认路由，并把这个路由广播到 BGP 邻居中。

表7-21 配置向BGP邻居发送缺省路由

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# router bgp 12	启动 BGP 路由进程	AS 号的取值范围为 1~4294967295
Switch(config-router)# neighbor 10.10.10.1 default-originate route-map myroute	配置 BGP 聚合条目	以 IP 地址格式来指定 BGP 邻居的地址； myroute：路由映射名

7.9 显示与维护

表7-22 显示与维护

命令	操作	说明
show ip bgp [*ip-address*] **show ip bgp ipv4** { **unicast** | **multicast** }[*ip-address*]	显示 BGP 网络信息	ip-address: 指定 IP 地址
show ip bgp community *type* [**exact-match**] **show ip bgp ipv4** { **unicast** | **multicast** } **community** *type* [**exact-match**]	显示匹配团体的路由	type: AA:NN、local-AS、no-advertise、no-export
show ip bgp filter-list *list-name* **show ip bgp ipv4** { **unicast** | **multicast** } **filter-list** *list-name*	显示符合过滤列表的路由	list-name: 指定 ACL 名的常规表述
show ip bgp neighbors [*ip-address* [**advertised-routes** | **received** | **received-routes** | **routes**] **show ip bgp ipv4** { **unicast** | **multicast** } **neighbors** [*ip-address* [**advertised-routes** | **received** | **received-routes** | **routes**]	显示 TCP 和 BGP 邻居连接的详细信息	ip-address: 指定 IPv4 的 IP 地址
show ip bgp prefix-list *list-name* **show ip bgp ipv4** { **unicast** | **multicast** } **prefix-list** *list-name*	显示匹配 prefix-list 的路由	list-name: 指定 IP 前缀列表名
show ip bgp summary **show ip bgp ipv4** { **unicast** | **multicast** } **summary**	显示 BGP 邻居状态的汇总信息	-
clear ip bgp * [**in** | **out** | **soft**]	重置所有对等体的 BGP 连接	*:清除所有的 BGP 对等体； in：清除接收的宣告路由； out：清除发布的宣告路由； soft：清除发布/接收的宣告路由

命令	操作	说明
clear ip bgp *ip-address* [**in** | **out** | **soft**]	通过指定的 IP 地址重置 IPV4 BGP 的连接	ip-address: 需要清除的 BGP 路由的 IP 地址

7.10 配置举例

7.10.1 配置 EBGP

i. 基本拓扑

图 7-1 EBGP 基本拓扑图 1

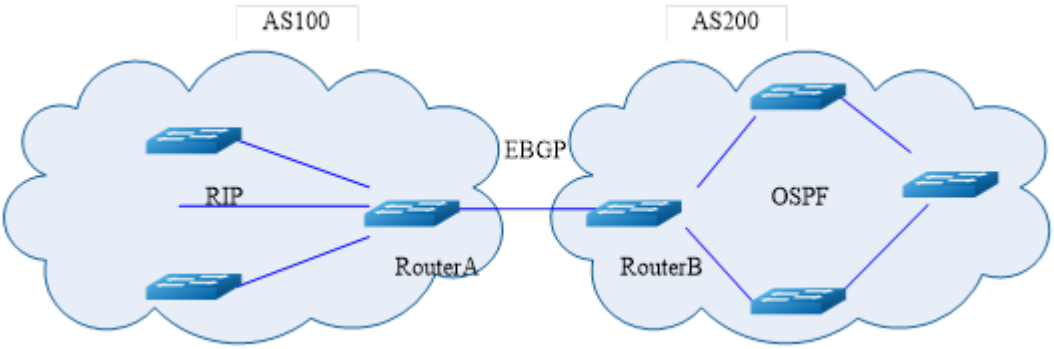
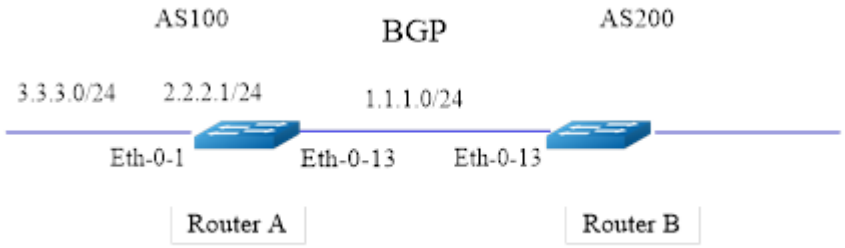


图 7-2 EBGP 基本拓扑图 2



ii. 配置步骤

Router A:

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式

命令举例	操作步骤
Switch(config)# interface eth-0-13	进入接口配置模式
Switch(config-if)# no shutdown	启用端口
Switch(config-if)# no switchport	将该端口转换为三层端口
Switch(config-if)# ip address 1.1.1.1/24	配置 IP 地址为 1.1.1.1/24
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# no shutdown	启用端口
Switch(config-if)# no switchport	将该端口转换为三层端口
Switch(config-if)# ip address 2.2.2.1/24	配置 IP 地址为 2.2.2.1/24
Switch(config-if)# exit	退出接口配置模式
Switch(config)# ip route 3.3.3.0/24 2.2.2.2	增加一条静态路由
Switch(config)# router bgp 100	创建 BGP 100 并进入路由模式
Switch(config-router)# bgp router-id 10.10.10.10	配置 BGP router-id
Switch(config-router)# neighbor 1.1.1.2 remote-as 200	配置 EBGP 邻居号 200
Switch(config)# neighbor 1.1.1.2 ebgp-multihop	配置邻居为 ebgp-multihop
Switch(config-router)# network 4.0.0.0/8	指定 BGP 路由进程宣告的网络
Switch(config-router)# redistribute static	重分布静态路由到 BGP
Switch(config-router)# redistribute connected	重分布直连路由到 BGP
Switch(config-router)# exit	退出路由模式

Router B:

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-13	进入接口配置模式
Switch(config-if)# no shutdown	启用端口

命令举例	操作步骤
Switch(config-if) # no switchport	将该端口转换为三层端口
Switch(config-if) # ip address 1.1.1.2/24	配置 IP 地址为 1.1.1.2/24
Switch(config-if)# exit	退出接口配置模式
Switch(config)# router bgp 200	创建 BGP 200 并进入路由模式
Switch(config-router)# bgp router-id 11.11.11.11	配置 BGP router-id
Switch(config-router)# neighbor 1.1.1.1 remote-as 100	配置 EBGP 邻居号 100
Switch(config)# neighbor 1.1.1.1 ebgp-multihop	配置邻居为 ebgp-multihop
Switch(config-router)# redistribute connected	重分布直连路由到 BGP
Switch(config-router)# exit	退出路由模式

iii. 命令验证

- 查看Router A的配置结果：

```
SwitchA# show ip bgp neighbors

BGP neighbor is 1.1.1.2, remote AS 200, local AS 100, external link
  BGP version 4, remote router ID 0.0.0.0
  BGP state = Active
  Last read 00:26:00, hold time is 180, keepalive interval is 60 seconds
  Received 0 messages, 0 notifications, 0 in queue
  Sent 0 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 0
  Index 1, Offset 0, Mask 0x2
  0 accepted prefixes
  0 announced prefixes
 Connections established 0; dropped 0
  External BGP neighbor may be up to 255 hops away.
Next connect timer due in 87 seconds
```

- 查看Router B的配置结果：

```
SwitchB# show ip bgp neighbors
BGP neighbor is 1.1.1.1, remote AS 100, local AS 200, external link
  BGP version 4, remote router ID 0.0.0.0
```

```
  BGP state = Active
  Last read 00:21:39, hold time is 180, keepalive interval is 60 seconds
  Received 0 messages, 0 notifications, 0 in queue
  Sent 0 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
 For address family: IPv4 Unicast
  BGP table version 1, neighbor version 0
  Index 1, Offset 0, Mask 0x2
  0 accepted prefixes
  0 announced prefixes
 Connections established 0; dropped 0
  External BGP neighbor may be up to 255 hops away.
Next connect timer due in 97 seconds
```

7.10.2 配置 IBGP

i. 基本拓扑

图 7-3 IBGP 基本拓扑图 1

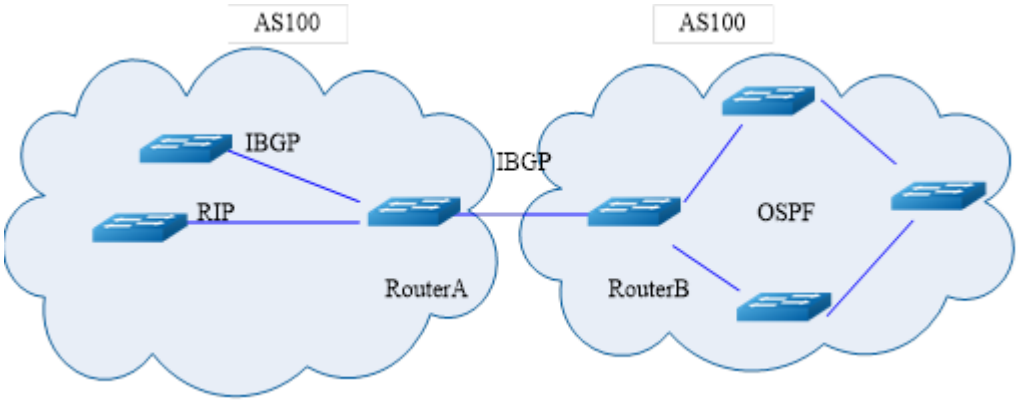
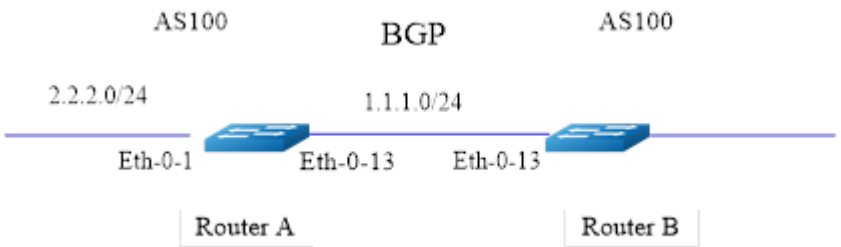


图 7-4 IBGP 基本拓扑图 2



ii. 配置步骤

Router A：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-13	进入接口配置模式
Switch(config-if)# no shutdown	启用端口
Switch(config-if)# no switchport	将该端口转换为三层端口
Switch(config-if) # ip address 1.1.1.1/24	配置 IP 地址为 1.1.1.1/24
Switch(config-if)# exit	退出接口模式
Switch(config)# interface loopback 0	进入接口配置模式
Switch(config-if) # ip address 10.10.10.10/32	配置 IP 地址为 10.10.10.10/32
Switch(config-if)# exit	退出接口配置模式
Switch(config)# ip route 11.11.11.11/32 1.1.1.2	增加一条静态路由
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# no shutdown	启用端口
Switch(config-if) # no switchport	将该端口转换为三层端口
Switch(config-if) # ip address 2.2.2.1/24	配置 IP 地址为 2.2.2.1/24
Switch(config-if)# exit	退出接口配置模式
Switch(config)# ip route 3.3.3.0/24 2.2.2.2	增加一条静态路由
Switch(config)# router bgp 100	创建 BGP 100 并进入路由模式。
Switch(config-router)# bgp router-id 10.10.10.10	配置 BGP router-id
Switch(config-router)# neighbor 11.11.11.11 remote-as 100	配置 IBGP 邻居 AS 号 100
Switch(config-router)# neighbor 11.11.11.11 update-source loopback 0	配置 loopback0 为更新源端口
Switch(config-router)# network 4.0.0.0/8	指定 BGP 路由进程宣告的网络
Switch(config-router)# redistribute static	重分布静态路由到 BGP
Switch(config-router)# redistribute connected	重分布直连路由到 BGP
Switch(config-router)# exit	退出路由模式

Router B：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-13	进入接口配置模式
Switch(config-if)# no shutdown	启用端口
Switch(config-if)# no switchport	将该端口转换为三层端口
Switch(config-if)# ip address 1.1.1.2/24	配置 IP 地址为 1.1.1.2/24
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface loopback 0	进入接口配置模式
Switch(config-if)# ip address 11.11.11.11/32	配置 IP 地址为 11.11.11.11/32
Switch(config-if)# exit	退出接口配置模式
Switch(config)# ip route 10.10.10.10/32 1.1.1.1	增加一条静态路由
Switch(config)# router bgp 100	创建 BGP 100 并进入路由模式
Switch(config-router)# bgp router-id 11.11.11.11	配置 BGP router-id
Switch(config-router)# neighbor 10.10.10.10 remote-as 100	配置 IBGP 邻居 AS 号 100
Switch(config-router)# neighbor 10.10.10.10 update-source loopback 0	配置 loopback0 为更新源端口
Switch(config-router)# redistribute connected	重分布直连路由到 BGP
Switch(config-router)# exit	退出路由模式

iii. 命令验证

- 检查Router A的配置结果：

```
SwitchA# show ip bgp neighbors

BGP neighbor is 11.11.11.11, remote AS 100, local AS 100, internal link
  BGP version 4, remote router ID 0.0.0.0
  BGP state = Active
  Last read 00:02:32, hold time is 180, keepalive interval is 60 seconds
  Received 0 messages, 0 notifications, 0 in queue
  Sent 0 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
```

```
    Update source is loopback0
  For address family: IPv4 Unicast
    BGP table version 1, neighbor version 0
    Index 1, Offset 0, Mask 0x2
    0 accepted prefixes
    0 announced prefixes
  Connections established 0; dropped 0
Next connect timer due in 62 seconds
```

- 检查Router B的配置结果：

```
SwitchB# show ip bgp neighbors
BGP neighbor is 10.10.10.10, remote AS 100, local AS 100, internal link
    BGP version 4, remote router ID 0.0.0.0
    BGP state = Active
    Last read 00:01:58, hold time is 180, keepalive interval is 60 seconds
    Received 0 messages, 0 notifications, 0 in queue
    Sent 0 messages, 0 notifications, 0 in queue
    Route refresh request: received 0, sent 0
    Minimum time between advertisement runs is 5 seconds
    Update source is loopback0
  For address family: IPv4 Unicast
    BGP table version 1, neighbor version 0
    Index 1, Offset 0, Mask 0x2
    0 accepted prefixes
    0 announced prefixes
  Connections established 0; dropped 0
Next connect timer due in 17 seconds
```

8 IS-IS 配置

8.1 IS-IS 简介

IS-IS（Intermediate system to intermediate system，中间系统到中间系统）是一种内部网关协议（Interior Gateway Protocol），也是一种链路状态路由协议，使用SPF（Shortest Path First，最短路径优先）算法计算路由。标准的IS-IS是由ISO（国际标准化组织）制定，专为CLNP（无连接网络服务）设计，并不适用于IP网络。由于IP网络的广泛应用，IETF组织在RFC1195中定义了使用IP网络的IS-IS协议，能同时应用于TCP/IP与开放式系统互联（Open System Interconnection，OSI）中，称作集成IS-IS。

IS-IS应用于大型网络中，在自治系统内有两种分层结构：骨干区域与非骨干区域。通常来说，可以将IS-IS路由域划分为多个区域，不同路由域的路由等级不同。处于区域内的路由为Level-1路由，处于不同区域的路由称为Level-3路由，介于相同路由域与不同路由域之间的路由为Level-2路由。Level-1的路由器一般部署在非骨干区域，将Level-2与Level-1-2路由器部署在骨干区域，非骨干区域的路由器都需要通过Level-1-2路由器与骨干区域相连。

8.2 配置 IS-IS 的基本功能

8.2.1 创建 IS-IS 进程

用户可以在一台路由器上创建多个 ISIS 进程，如果没有指定进程编号，则创建默认的 0 号进程。

表8-1 创建IS-IS进程

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# router isis test	创建 ISIS 进程并进入 ISIS 配置模式	test: ISIS 路由区域标签

8.2.2 配置网络实体名(NET)

区域地址用来唯一标识路由域中的不同区域，同一 Level-1 区域内所有无线接入控制器必须有相同的区域地址，Level-2 区域内的无线接入控制器可以有不同的区域地址。由于一个 IS-IS 进程中最多可配置 3 个区域地址，所以最多也只能配 3 个 NET。配置多个 NET 时，它们的系统 ID 必须保持一致。

表8-2 配置NET

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# router isis test	创建 ISIS 进程并进入 ISIS 配置模式	test: ISIS 路由区域标签
Switch(config-router))# net 49.0124.0000.0000.0014.00	配置 IS-IS 进程的网络实体名称 NET（Network Entity Title）	网络实体名称的格式为 X…X.XXXX.XXXX.XXXX.00，前面的“X…X”是区域地址，中间的 12 个“X”是无线接入控制器的 System ID，最后的“00”是 SEL。

8.2.3 配置 Level 类型

IS-IS 进程的 Level 类型有以下三种：

Level-1: 配置路由器工作在 Level-1，它只计算区域内路由，维护 L1 的 LSDB。

Level-2: 配置路由器工作在 Level-1-2，同时参与 L1 和 L2 的路由计算，维护 L1 和 L2 两个 LSDB。

level-2-only: 配置路由器工作在 Level-2，只参加 L2 的 LSP 交换和 L2 的路由计算，维护 L2 的 LSDB。

如果只有一个区域，建议用户将所有路由器的 Level 配置为 Level-1 或者 Level-2-only，因为没有必要让所有路由器同时维护两个相同的数据库。在 IP 网络中使用该命令时，建议将所有的路由器都配置为 Level-2-only，这样有利于以后的扩展。

表8-3 配置Level类型

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# router isis test	创建 ISIS 进程并进入 ISIS 配置模式	test: ISIS 路由区域标签

命令举例	操作	说明
Switch(config-router)# is-type level-2-only	配置 Level 类型	缺省情况下，未配置 IS-IS 进程的 Level 类型

8.2.4 配置接口使能 IS-IS 功能

在全局配置模式下完成 IS-IS 进程的配置之后，为了使 IS-IS 协议正常运行，还需要在运行 IS-IS 协议的链路接口上使能 IS-IS 并与指定进程相关联。

表8-4 配置接口使能IS-IS功能

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-
Switch(config-if)# ip router isis test	在接口上使能 IS-IS 功能并指定要关联的 IS-IS 进程	test: IS-IS 路由进程标签

8.3 配置 IS-IS 认证

8.3.1 配置接口的认证

通常情况下，IS-IS 不对发送的 IS-IS 报文封装认证信息，也不对收到的报文做认证检查。当有恶意报文对网络进行攻击时，可能会导致整个网络的信息被窃取。因此，需要配置 IS-IS 认证提高网络的安全性。

表8-5 配置接口的认证

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-
Switch(config-if)# isis authentication mode md5 level-1	配置 IS-IS 接口的认证模式为 md5	可选的认证模式有 MD5 认证、SM3 认证及 Text 认证，可以指定对 level-1 或 level-2 类型的报文进行加密

用户也可根据实际情况，执行命令 **isis authentication key-chain** *name* [**level-1** | **level-2**]，对单个 IS-IS 接口使用密匙链的模式；或者执行命令 **isis authentication send-only** [**level-1** | **level-2**]，在接口上只对发送的 Hello 报文加载认证信息，不对接收的 Hello 报文进行认证。

8.3.2 配置报文的认证

表8-6 配置报文的认证

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# router isis test	创建 ISIS 进程并进入 ISIS 配置模式	test: ISIS 路由区域标签
Switch(config-router)# authentication mode md5 level-1	配置 ISIS 报文的认证类型为 md5	可选的认证模式有 MD5 认证、SM3 认证及 Text 认证，可以指定对 level-1 或 level-2 类型的报文进行加密

类似地，用户也可根据实际情况，执行命令 **authentication key-chain** *name* [**level-1** | **level-2**]，在路由模式下配置密匙链的认证类型；或者执行命令 **authentication send-only** [**level-1** | **level-2**]，只对发送的 Hello 报文加载认证信息，不对接收的 Hello 报文进行认证。

8.3.3 配置区域或路由域密码

配置此密码插入到 2 级 PDU 链路状态 PDU (LSP)、完整序列号 PDU (CSNP) 和部分序列号 PDU (PSNP) 中。如果指定 authenticate snp 以及 validate 或 send-only 关键字，IS-IS 路由协议会将密码插入序列号 PDU (SNP)。

1. 配置区域认证密码

表8-7 配置区域认证密码

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# router isis test	创建 ISIS 进程并进入 ISIS 配置模式	test: ISIS 路由区域标签
Switch(config-router)# area-password test	配置区域认证密码	缺省情况下，未配置区域认证密码

2. 配置路由域认证密码

表8-8 配置路由域认证密码

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# router isis test	创建 ISIS 进程并进入 ISIS 配置模式	test: ISIS 路由区域标签
Switch(config-router)# domain-password test	配置路由域认证密码	缺省情况下，未配置路由域认证密码

说明

如果先配置了认证模式命令，后使用区域密码或路由域密码命令配置了明文认证，认证模式命令会覆盖这两个命令。请使用 **no authentication mode** { **md5** | **sm3** | **text** } [**level-1** | **level-2**]命令后再配置区域密码或路由域密码认证。

8.4 配置 IS-IS 路由选路

8.4.1 配置路由器的优先级

配置用来配置接口上的 ISIS 路由器的优先级，如果为 0，不能被选为 DR。

表8-9 配置路由器的优先级

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-
Switch(config-if)# isis priority 222 level-1	配置 ISIS 路由器的优先级	ISIS DR 选举优先级的取值范围为 0~127

8.4.2 配置接口的度量值

配置接口的度量值之前，需要先配置 IS-IS 设备接收和发送路由的开销类型。在实际应用中，为了方便 IS-IS 实现其扩展功能，通常将 IS-IS 的路由开销类型设置为 wide 模式。

表8-10 配置接口的度量值

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# router isis test	创建 ISIS 进程并进入 ISIS 配置模式	test: ISIS 路由区域标签
Switch(config-router)# metric-style wide	配置 IS-IS 接收和发送路由的开销类型为 wide	IS-IS 设备接收和发送路由的开销类型（narrow 或 wide），以及传输期间 TLVs 的种类
Switch(config-router)# quit	退出路由配置模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-
Switch(config-if)# isis wide-metric 10	配置接口的度量值	度量值的取值范围为 1~16777214

8.4.3 配置管理距离

表8-11 配置管理距离

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# router isis test	创建 ISIS 进程并进入 ISIS 配置模式	test: ISIS 路由区域标签
Switch(config-router)# distance 233	配置 ISIS 的管理距离（Administrative Distance）	距离值的范围为 1~255。用户还可以配置 ISIS 的系统 ID，使用 ACL 进行控制

8.5 配置 IS-IS 路由信息的引入

8.5.1 配置发布缺省路由

表8-12 配置管理距离

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# router isis test	创建 ISIS 进程并进入 ISIS 配置模式	test: ISIS 路由区域标签
Switch(config-router)# distance 233	配置 ISIS 缺省路由的重分发	缺省情况下，不发布 ISIS 缺省路由

8.5.2 配置路由重发布

配置该命令可以将其他的路由协议生成的路由引入到 ISIS 路由域，可引入的路由包括包含静态路由、直连路由、RIP、BGP 路由、OSPF 路由。

ISIS 有两种类型的外部路由：

Type-1 外部路由：指接收的 IGP 路由，如 RIP 和 Static。此类路由有较高的可靠性，所以外部路由开销的计算结果等于自治系统的内部路由开销。

Type-2 外部路由：指接收的 EGP 路由。

表8-13 配置路由重发布

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# router isis test	创建 ISIS 进程并进入 ISIS 配置模式	test: ISIS 路由区域标签
Switch(config-router)# redistribute static metric 10	配置 ISIS 路由重发布	该命令里配置的 metric 值将覆盖用命令 default metric 配置的值；如未选择配置外部路由的类型，默认为 Type-2

8.6 配置 IS-IS 路由聚合

可以针对给定级别聚合多组地址，还可以聚合从其他路由协议中学习到的路由。此命令有助于减小路由表的大小。

表8-14 配置IS-IS路由聚合

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# router isis test	创建 ISIS 进程并进入 ISIS 配置模式	test: ISIS 路由区域标签
Switch(config-router)# summary-address 10.1.0.0/16 level-1	配置 IS-IS 路由聚合	汇总路由 10.1.0.0 包括子网 10.1.1.0、10.1.2.0、10.1.3.0 等。此时，只会发布 10.1.0.0 这条聚合路由； 缺省情况下，不对外部路由进行聚合

8.7 配置 IS-IS 报文属性

8.7.1 配置 Hello 报文属性

配置 IS-IS 的 Hello 报文的发送间隔时间以及邻居保持时间，主要用于建立和维护邻接关系，有助于更好地规划网络，增强网络可用性。

表8-15 配置Hello报文属性

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-
Switch(config-if)# isis hello-interval 777 level-1	配置 Hello 报文的发送间隔时间	发送时间间隔的取值范围为 1~65535
Switch(config-if)# isis hello-multiplier 6 level-1	配置 IS-IS 的邻居保持时间，即邻居保持时间为 Hello 报文发送间隔的 6 倍	该倍数值的取值范围为 2~100

8.7.2 配置 LSP 报文属性

LSP报文主要用来分发链路状态的详细信息，配置LSP报文的发送间隔时间，能够更好地规划网络。

表8-16 配置LSP报文属性

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-
Switch(config-if)# isis lsp-interval 777	配置 LSP 报文的发送间隔时间	发送时间间隔的取值范围为1~4294967295，单位：毫秒

8.7.3 配置 CNSP 报文属性

CNSP报文可以同步链路状态数据库，包括LSP的摘要信息。配置CNSP报文的发送间隔时间，也能增强网络的可用性。

表8-17 配置CNSP报文属性

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-
Switch(config-if)# isis csnp-interval 666 level-1	配置 CSNP 报文的发送间隔时间	发送时间间隔的取值范围为1~65535

8.8 IS-IS 显示与维护

表8-18 IS-IS显示与维护

命令	操作	说明
show ip isis [*area-tag*] **route**	查看 ISIS 进程路由相关信息	area-tag: 区域路由名 lsp-id: LSP ID，格式为xxxx.xxxx.xxxx.xx-xx if-name: 接口名
show isis [*area-tag*] **database** [**detail** | **verbose**] [*lsp-id*] [**l1** | **l2** | **level-1** | **level-2**]	查看指定 ISIS 路由进程的链路状态数据库信息	

命令	操作	说明
show isis interface *if-name*	显示 ISIS 接口的信息	process-id: 路由进程名
show isis interface counter	显示 ISIS 接口的统计信息	
show clns [*area-tag*] **neighbors** [*if-name*] [**detail**]	查看指定 CLNS 的邻居信息	
show clns [*area-tag*] **is-neighbors** [*if-name*] [**detail**]	查看指定 CLNS 的 IS 邻居信息	
show isis counter	显示 ISIS 的统计信息	
show isis hostname	显示 ISIS 的主机名	
show isis topology [**l1** | **l2** | **level-1** | **level-2**]	查看指定 ISIS 到中间系统的路径	
clear ip isis [*process-id*] **route** { **redistribution** | **all** }	清除 IS-IS 路由表项	

网络管理配置指导目录

1 网络诊断配置

一般来说，用户可以使用 Ping 功能和 Traceroute 功能检测网络的连通性。当用户使用 **ping** 命令测试发现网络出现故障后，可以用 **traceroute** 命令分析出现故障的网络节点。本章节主要介绍 Ping 功能和 Traceroute 功能及其配置。

1.1 Ping 功能简介

Ping 是一个计算机网络的管理工具，用于测试一台主机通过 IP 协议的可达性和衡量每次从源主机到目的主机的时间 (Round-Trip Time, RTT)。

Ping 通过向目的主机发送 ICMP Echo 请求报文，等待 ICMP 回应来实现。在运作过程中，它会测量每一次发送到接收到响应的时间间隔 (Round-Trip Time, RTT)，并且记录所有的丢包。如果源主机在有效时间间隔内收到来自目的主机的 ICMP Echo 应答消息，则说明目的地可达；反之，则不可达。如果目的地可达，用户能根据测试结果汇总的数据诊断网络质量。这个结果会显示接收到的所有报文的情况，包括最小、最大和平均的 RRT，有时系统会打印平均的标准偏差值。

1.1.1. Ping 配置

配置 **ping** 命令来检测到一个网络内的某个主机的可达性以及统计信息。如不可达，一般可能有五种结果：目标不可达、网段不可达、主机不可达、端口不可达或超时。该命令可以在公网内或 VRF 内配置。

表1-1 Ping配置

命令	操作	说明
ping [**ip** | **mgmt-if**] *host-address*	检测一个网络内的某个主机的可达性以及统计信息	host-address：要检测的主机地址，支持 IPv4 和 IPv6 地址
ping vrf *vrf-name* [**-a** *source-ip-address* | **-si** *if-name* | **-m** *interval* | **-c** *count* | **-s**		vrf-name：VRF 实例名

命令	操作	说明
data-size | **-f** | **-tos** *tos-value* | **-h** *ttl-value* | **-t** *timeout* | **-p** *pattern*] * *host-address* **ping** [**mgmt-if**] **ipv6** *host-address* [**interface** *if-name*] **ping ipv6** [**-a** *source-ip-address* | **-m** *interval* | **-c** *count* | **-s** *data-size* | **-h** *ttl-value* | **-t** *timeout* | **-tc** *traffic-class* | **-p** *pattern*] * *host-address* [**interface** *if-name*]		source-ip-address：源 IP 地址 **si** if-name: 指定 ping 报文的源端口 interval：指定报文发送间隔，单位：毫秒，取值范围为 10~10000 count：指定发送报文数量，取值范围为 1~4294967295 data-size：指定发送报文的数据长度，单位：字节，取值范围是 20~9600 tos-value：指定报文中 TOS 值，取值范围为 0~255 ttl-value：指定报文中 TTL 值，取值范为 1~255 timeout：指定请求报文的超时时间，单位：毫秒，取值范围是 0~65535。当前只支持 1000 的整数倍 pattern：指定最多 16 个填充字节 traffic-class：配置 ping 报文的流量级别 **interface** if-name：接口名

说明

ping 命令支持 IPv4 网络环境，**ping ipv6** 支持 IPv6 网络环境。

1.1.2. 配置举例

1. Ping内部接口的IP地址

命令举例	操作
DUT# ping 10.10.29.247	Ping 内部接口的 IPv4 地址 10.10.29.247
DUT# ping ipv6 2001:1000::1	Ping 内部接口的 IPv6 地址 2001:1000::1

2. Ping管理口的IP地址

命令举例	操作
DUT# ping mgmt-if 10.10.29.247	Ping 带外管理口的 IPv4 地址 10.10.29.247
DUT# ping mgmt-if ipv6 2001:1000::1	Ping 带外管理口的 IPv6 地址 2001:1000::1

3. Ping VRF实例的IP地址

命令举例	操作
DUT# ping vrf vrf1 10.10.10.1	Ping VRF 实例的 IP 地址 10.10.10.1

1.1.3. 命令验证

在管理口上检测一个主机的可达性：

```
Switch# ping mgmt-if 10.10.29.247
PING 10.10.29.247 (10.10.29.247) 56(84) bytes of data.
64 bytes from 10.10.29.247: icmp_seq=1 ttl=64 time=0.194 ms
64 bytes from 10.10.29.247: icmp_seq=2 ttl=64 time=0.131 ms
64 bytes from 10.10.29.247: icmp_seq=3 ttl=64 time=0.134 ms
64 bytes from 10.10.29.247: icmp_seq=4 ttl=64 time=0.121 ms
64 bytes from 10.10.29.247: icmp_seq=5 ttl=64 time=0.135 ms
--- 10.10.29.247 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3996ms
rtt min/avg/max/mdev = 0.121/0.143/0.194/0.025 ms
Switch # ping mgmt-if ipv6 2001:1000::1
PING 2001:1000::1(2001:1000::1) 56 data bytes
64 bytes from 2001:1000::1: icmp_seq=1 ttl=64 time=0.291 ms
64 bytes from 2001:1000::1: icmp_seq=2 ttl=64 time=0.262 ms
64 bytes from 2001:1000::1: icmp_seq=3 ttl=64 time=0.264 ms
64 bytes from 2001:1000::1: icmp_seq=4 ttl=64 time=0.270 ms
64 bytes from 2001:1000::1: icmp_seq=5 ttl=64 time=0.274 ms
--- 2001:1000::1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3997ms
rtt min/avg/max/mdev = 0.262/0.272/0.291/0.014 ms
```

1.2 Traceroute 功能简介

Traceroute 是一个在 IP 网络中用于测量路由选路和报文传输时间的工具。Traceroute 向目的主机发送一个 ICMP 序列报文，通过 TTL 参数跟踪通过的中间路由。中间路由器减少通过报文的 TTL 参数值，当 TTL 值为 0 时丢弃报文并回送一个 ICMP 超时报文 (ICMP Timer Exceeded) 给发送源。

1.2.1 Traceroute 配置

该命令用来查看 IPv4 或 IPv6 报文从当前设备传到目的设备所经过的路径。

表1-2 Traceroute配置

命令	操作	说明
traceroute [**ip** | **ipv6** | **mgmt-if**] *host-address*	查看从当前设备传到目的设备所经过的路径	vrf-name：VRF 实例名 host-address：需要检测的主机地址 source-ip-address：指定源 IP 地址，默认为出端口的 IP 地址 if-name：指定 traceroute 报文的源端口
traceroute vrf *vrf-name* [**-a** *source-ip-address* | **-si** *if-name*] *host-address*		

说明

traceroute 命令支持 IPv4 网络环境，**traceroute ipv6** 支持 IPv6 网络环境。

1.2.2 配置举例

Traceroute 内部接口的 IP 地址：

命令举例	操作
DUT# traceroute 1.1.1.2	Traceroute 内部接口的 IP 1.1.1.2
DUT# traceroute ipv6 2001:1000::1	Traceroute 内部接口的 IP 2001:1000::1

1.2.3 命令验证

查看到1.1.1.2这个主机所经过的路径：

```
Switch# traceroute 1.1.1.2
traceroute to 1.1.1.2 (1.1.1.2), 30 hops max, 38 byte packets
 1  1.1.1.2 (1.1.1.2)  112.465 ms  102.257 ms  131.948 ms
```

2 NTP 配置

2.1 NTP 简介

当交换机的系统时间不准确时，通过手工配置可以修改系统时间，但在大型网络应用中不适合采用这种方法，设备数量的增多会导致工作量增加、效率低下且极易存在误差。

NTP（Network Time Protocol，网络时间协议）为不同网络设备之间实现时间同步的协议。通过 NTP 能测量内网的传输延迟以及客户端与服务器之间的时间差。NTP 使 LAN 内的设备时间同步，精度达到毫秒级，也可以使 WAN 上的设备时间同步，精度达到百毫秒级。NTP 时间分布式的分层特性使用户能通过一个 Stratum（层级）选择需要的精度。一台时间服务器，放置在这个架构的高端（低层级），提供了高精度的 UTC 标准时间。

NTP 的工作模式有客户端/服务器模式、对等体模式、广播模式等，其中，最常用的工作模式即客户端/服务器模式。主机可作为时间服务器，提供精准的时间到其他主机；主机也可作为客户端，向服务器请求时间同步。在同一条链路的主机也可既充当客户端又当服务器，将精准的时间从一个主机转发到另一个主机上。例如，将交换机作为客户端，内网网络设备（交换机、路由器或专门的 NTP 服务器）作为服务器，使客户端与服务器之间实现时间同步。配置 NTP 客户端之前请确认 NTP 服务器已开启 NTP 服务。

2.2 配置 NTP

2.2.1 配置 NTP 服务器与 NTP 对端

如下表，配置设备同步 NTP 服务器/NTP 对端，可以指定版本号等信息。如果指定源接口或者源 IP 地址，将会使用对应的 IP 地作为发出报文的源 IP 地址。

表 2-1 配置 NTP 服务器

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

命令	操作	说明
ntp server { *host-name* | *ip-address* } [**key** *key-id* | **prefer** | **version** *number*] * [**source-interface** *if-name* | **source-ip** *source-ip-address*]	配置设备与 NTP 服务器同步	host-name：NTP 服务器的主机名 ip-address：NTP 服务器的 IPv4 地址 ipv6-address：NTP 服务器的 IPv6 地址 key-id：定义认证 key 的值，取值范围是 1～64000 number：NTP 版本(1～3) if-name：指定源接口名称 source-ip-address：指定源 IP 地址 缺省情况下，设备未与 NTP 服务器同步
ntp server { *host-name* | *ipv6-address* } [**key** *key-id* | **prefer** | **version** *number*] * [**source-interface** *if-name* | **source-ip** *source-ip-address*]	配置设备与 IPv6 NTP 服务器同步	

NTP 支持客户端/服务器模式，还支持对等体模式。用户根据实际情况可以选择一种或多种工作模式配置时间同步。

表 2-2 配置 NTP 对端

命令	操作	说明
configure terminal	进入全局配置模式	-
ntp peer { *host-name* | *ip-address* } [**key** *key-id* | **prefer** | **version** *number*] * [**source-interface** *if-name* | **source-ip** *source-ip-address*]	配置设备与 NTP 对端同步	host-name：NTP 对端的主机名 ip-address：NTP 对端的 IPv4 地址 ipv6-address：NTP 对端的 IPv6 地址 key-id：定义认证 key 的值，取值范围是 1～64000 number：NTP 版本(1～3) if-name：指定源接口名称 source-ip-address：指定源 IP 地址 缺省情况下，设备未与 NTP
ntp peer { *host-name* | *ipv6-address* } [**key** *key-id* | **prefer** | **version** *number*] * [**source-interface** *if-name* | **source-ip** *source-ip-address*]	配置设备与 IPv6 NTP 对端同步	

命令	操作	说明
		对端同步

说明

配置设备与 NTP 服务器和 NTP 对端同步的区别：

客户端/服务器模式中，客户端能和 NTP 服务器的时间同步，但 NTP 服务器不能与客户端的时间同步。而对端模式下的本设备和对端设备可以实现相互同步。

2.2.2 配置 NTP 认证

当使能 NTP 认证功能时，设备会使用信任的 key 加密与 NTP server 同步时间。

表 2-3 配置 NTP 认证

命令	操作	说明
configure terminal	进入全局配置模式	-
ntp authentication enable	使能 NTP 认证	缺省情况下，未使能 NTP 认证功能
ntp key *key-id value*	配置 NTP 认证 key	key-id：定义认证 key 的值，取值范围是 1～64000 value：认证 key 值 缺省情况下，未配置 NTP 认证 key
ntp trustedkey *key-id*	配置 NTP 信任的认证 key	key-id：定义认证 key 的值，取值范围是 1～64000 缺省情况下，未配置 NTP 信任的认证 key

2.2.3 配置 NTP 访问控制条目

表 2-4 配置 NTP ACE

命令	操作	说明
configure terminal	进入全局配置模式	-
ntp ace { *host-name* | *ip-address* } [**mask** *mask-address*] { **version** | **kod** | **ignore** | **noquery** | **nomodify** | **notrap** | **noserve** | **nopeer** | **notrust** | **limited** | none }	创建 NTP 访问控制条目	ip-address: NTP 服务器/对端设备的 IP 地址 host-name: NTP 服务器/对端设备的名称 mask-address: 掩码地址 ipv6-address: NTP 服务器/对端设备的 IPv6 地址
ntp ace { *host-name* | *ipv6-address* } [**mask** *mask-address*] { **version** | **kod** | **ignore** | **noquery** | **nomodify** | **notrap** | **noserve** | **nopeer** | **notrust** | **limited** | none }	创建 IPv6 NTP 访问控制条目	

2.2.4 配置端口禁止/允许接收 NTP 报文

用户可以配置端口不处理接收的 NTP 报文，该配置为一个可选配置。

表 2-5 配置端口禁止/允许接收 NTP 报文

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	-
ntp disable	在端口上禁止接收 NTP 报文	缺省情况下，所有接口都接收 NTP 报文
no ntp disable	在端口上允许接收 NTP 报文	

2.2.5 配置 NTP 外部时钟源

表 2-6 配置 NTP 外部时钟源

命令	操作	说明
configure terminal	进入全局配置模式	-
ntp refclock stratum *number*	配置 NTP 外部时钟源	number：配置 NTP 层级，取值范围为 1~15

命令	操作	说明
		缺省情况下，未配置 NTP 外部时钟源

2.3 NTP 显示与维护

表 2-8 NTP 显示与维护

命令	操作	说明
show ntp	显示当前 NTP 配置信息	-
show ntp ace	显示 NTP 的访问控制条目信息	-
show ntp associations	显示 NTP 邻居的状态	-
show ntp key	显示 NTP 密匙的信息	-
show ntp status	显示 NTP 的状态信息	-
show ntp statistics	显示 NTP 的统计信息	-
clear ntp statistics	清除 NTP 的统计信息	-

2.4 配置举例

2.4.1 配置步骤

i. 配置接口VLAN 10

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# vlan database	进入 VLAN 配置模式
Switch(config-vlan)# vlan 10	添加 VLAN 10 到数据库
Switch(config-vlan)# exit	退出 VLAN 配置模式
Switch(config)# interface eth-0-26	进入接口配置模式
Switch(config-if)# switch access vlan 10	添加端口到 VLAN 10

命令举例	操作步骤
Switch(config-if)# no shutdown	端口 UP
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface vlan10	进入 VLAN 配置模式
Switch(config-if)# ip address 6.6.6.5/24	设置 IP 地址
Switch(config-if)# exit	退出 VLAN 配置模式

ii. 配置NTP客户端

命令举例	操作步骤
Switch(config)# ntp key 1 serverkey	配置 NTP 信任的认证 key
Switch(config)# ntp server 6.6.6.6 key 1	配置 NTP 服务器的 IP 地址
Switch(config)# ntp authentication enable	使能 NTP 认证功能
Switch(config)# ntp trustedkey 1	一旦使能认证功能，客户端交换机仅发送 time-of-day 请求到信任 NTP 服务器
Switch(config)# ntp ace 6.6.6.6 none	配置 NTP 的访问控制条目

iii. 配置NTP服务器

1 显示接口eth1的IP地址

```
[root@localhost octeon]# ifconfig eth1
eth1      Link encap:Ethernet  HWaddr 00:08:C7:89:4B:AA
          inet addr:6.6.6.6  Bcast:6.6.6.255  Mask:255.255.255.0
          inet6 addr: fe80::208:c7ff:fe89:4baa/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3453 errors:1 dropped:0 overruns:0 frame:1
          TX packets:3459 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:368070 (359.4 KiB)  TX bytes:318042 (310.5 KiB)
```

2 通过ping检查网络连接

```
[root@localhost octeon]# ping 6.6.6.5
PING 6.6.6.5 (6.6.6.5) 56(84) bytes of data.
```

```
64 bytes from 6.6.6.5: icmp_seq=0 ttl=64 time=0.951 ms
64 bytes from 6.6.6.5: icmp_seq=1 ttl=64 time=0.811 ms
64 bytes from 6.6.6.5: icmp_seq=2 ttl=64 time=0.790 ms
```

3 配置ntp.conf

```
[root@localhost octeon]# vi /etc/ntp.conf

server    127.127.1.0 # local clock
fudge      127.127.1.0 stratum 5
#
# Drift file.    Put this in a directory which the daemon can write to.
# No symbolic links allowed, either, since the daemon updates the file
# by creating a temporary in the same directory and then rename()'ing
# it to the file.
#
driftfile /var/lib/ntp/drift
broadcastdelay    0.008
broadcast 6.6.6.255
#
# PLEASE DO NOT USE THE DEFAULT VALUES HERE. Pick your own, or remote
# systems might be able to reset your clock at will. Note also that
# ntpd is started with a -A flag, disabling authentication, that
# will have to be removed as well.
#
#disable auth
keys              /etc/ntp/keys
trustedkey 1
```

4 配置keys

```
[root@localhost octeon]# vi /etc/ntp/keys

#
# PLEASE DO NOT USE THE DEFAULT VALUES HERE. Pick your own, or remote
# systems might be able to reset your clock at will. Note also that
# ntpd is started with a -A flag, disabling authentication, that
# will have to be removed as well.
#
1 M serverkey
```

5 启动NTPD服务器

```
[root@localhost octeon]# ntpd
```

说明

- 如果用户不需要使用认证功能，可以在ntp.conf文件以及在设备上去使能NTP认证功能；
- NTP服务器的Stratum号必须小于当前客户端的Stratum号

2.4.2 命令验证

显示当前 NTP 的配置信息：

```
Switch# show ntp
Current NTP configuration:
============================================================
NTP access control list:
   6.6.6.6 none
Unicast peer:
Unicast server:
   6.6.6.6 key 1
Authentication: enabled
Local reference clock:
Switch# show ntp status
Current NTP status:
============================================================
clock is synchronized
stratum:              7
reference clock: 6.6.6.6
frequency:            17.365 ppm
precision:            2**20
reference time:    d14797dd.70b196a2    ( 1:54:37.440 UTC      Thu Apr    7 2011)
root delay:           0.787 ms
root dispersion: 23.993 ms
peer dispersion: 57.717 ms
clock offset:        -0.231 ms
stability:            6.222 ppm
Switch# show ntp associations
Current NTP associations:
     remote                refid          st     when poll reach      delay      offset    disp
================================================================================
*6.6.6.6              127.127.1.0       6      50    128      37          0.778      -0.234    71.945
synchronized, + candidate, # selected, x falsetick, . excess, - outlier
```

3 PHY Loopback 配置

3.1 PHY Loopback 简介

Loopback 是比较常见的调试及诊断的功能，可以用来诊断 CPU 端、MAC 与 PHY 的连通情况。PHY loopback 是一个私有的模块，实现物理层的环回功能。它包含两个级别的环回：一种是通过 PHY 硬件实现环回（包括 internal 和 external 两种模式），另一种是端口级别的环回，通过芯片实现。

PHY loopback 只能配置在物理口上：

- 如果配置为 External PHY 模式，所有进入此端口的报文被环回回去。
- 如果配置为 Internal PHY 模式，所有期望从此端口出去的报文被环回到另外一个指定的端口。
- 如果配置为 Port Loopback 模式，所有进入此端口的报文被环回回去，此模式还可以指定是否进行源、目的 MAC 地址的交换，如果进行 MAC 地址的交换，芯片会重新计算 CRC 校验和。

3.2 配置 PHY Loopback

3.2.1 配置接口的环回模式

一个接口只能配置一种Loopback模式，新的配置会覆盖掉原有配置。

表3-1 配置接口的PHY环回模式

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	-
interface phy { internal *if-name* | **external** }	配置接口的 PHY 环回模式	if-name: 物理接口名称 可选 External PHY 或 Internal PHY 模式

配置为port loopback模式后从网络上收到的报文会转发回网络，swap字段指定是否进行源MAC地址和目的MAC地址之间的互换。

表3-2 配置接口为Port Loopback模式

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	-
loopback port [**mac-address swap**]	配置接口为 Port Loopback 模式	mac-address swap: 源 MAC 地址和目的 MAC 地址互换，并更新 FCS

可以使用**no loopback**命令取消接口的PHY环回模式或端口级别的环回模式，PHY Loopback不同模式的配置定义请参见3.1 PHY Loopback简介。

3.2.2 查看 PHY 环回配置信息

表3-3 查看PHY Loopback配置信息

命令	操作	说明
show phy loopback	显示 PHY Loopback 的配置信息	-

3.3 配置接口的环回模式示例

3.3.1 配置步骤

i. 配置External PHY环回模式

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch (config)# interface eth-0-1	进入接口配置模式
Switch (config-if)# no shutdown	配置端口管理 UP
Switch (config-if)# loopback phy external	配置端口为 External PHY 环回模式
Switch (config-if)# end	退出到特权模式

ii. 配置Internal PHY环回模式

命令举例	操作步骤
Switch # configure terminal	进入全局配置模式
Switch (config)# interface eth-0-2	进入接口配置模式
Switch (config-if)# no shutdown	配置端口管理 UP
Switch (config-if)# exit	退出到全局配置模式
Switch (config)# interface eth-0-1	进入接口配置模式
Switch (config-if)# no shutdown	配置端口管理 UP
Switch (config-if)# loopback phy internal eth-0-2	配置端口为 Internal PHY 环回模式，并指定 interface 2 为目的端口
Switch (config-if)# end	退出到特权模式

iii. **配置**Port Loopback**模式**

命令举例	操作步骤
Switch # configure terminal	进入全局配置模式
Switch (config)# interface eth-0-1	进入接口配置模式
Switch (config-if)# no shutdown	配置端口管理 UP
Switch (config-if)# loopback port mac-address swap	配置端口为 Port Loopback 环回模式，并且指定进行源 MAC 地址与目的 MAC 地址的交换
Switch (config-if)# end	退出到特权模式

3.3.2 命令验证

显示PHY Loopback的配置信息：

```
Switch# show phy loopback
Interface   Type          DestIntf    SwapMac
--------------------------------------------
eth-0-1     external      -           -
--------------------------------------------
```

3.4 配置 L2 ping 示例

3.4.1 介绍

L2 ping 是一个用于检测交换机间的连通性的工具。Window、Linux 上的 IP ping 是通过 ICMP 协议实现，在 3 层网络上工作，而 L2 ping 在二层网络上工作。

当系统发出 L2 Ping 请求时，以 ether type 0x9009 为标志的协议报文将进入二层网络，当通过二层网络到达对端指定目的端口时，如果该端口上使能了 l2 ping response，对端系统就会回复 l2 ping 请求。

3.4.2 配置步骤

Switch 1：

命令举例	操作步骤
Switch1# configure terminal	进入全局配置模式
Switch1(config)# interface eth-0-2	进入接口配置模式
Switch1(config-if)# no shutdown	配置端口管理 UP
Switch1(config-if)# l2 ping response enable	使能 L2 ping 回复功能
Switch1(config-if)# end	退出到特权模式

Switch 2：

命令举例	操作步骤
Switch2# configure terminal	进入全局配置模式
Switch2(config)# interface eth-0-1	进入端口配置模式
Switch2(config-if)# no shutdown	配置端口管理 UP
Switch2(config-if)# end	退出到特权模式
Switch2# l2 ping 001e.0808.58f1 interface eth-0-1 count 10 interval 1000 timeout 2000	001e.0808.58f1 是对端端口 eth-0-2 的接口地址； 用户可以指定 ping 的次数、间隔、以及超时时间

3.4.3 命令验证

Switch 2 的配置结果如下：

```
Switch2# l2 ping 001e.0808.58f1 interface eth-0-1 count 10 interval 1000 timeout 2000

Sending 10 L2 ping message(s):
64 bytes from 001e.0808.58f1: sequence = 0, time = 10ms
64 bytes from 001e.0808.58f1: sequence = 1, time = 15ms
64 bytes from 001e.0808.58f1: sequence = 2, time = 13ms
64 bytes from 001e.0808.58f1: sequence = 3, time = 12ms
64 bytes from 001e.0808.58f1: sequence = 4, time = 20ms
64 bytes from 001e.0808.58f1: sequence = 5, time = 21ms
64 bytes from 001e.0808.58f1: sequence = 6, time = 12ms
64 bytes from 001e.0808.58f1: sequence = 7, time = 16ms
64 bytes from 001e.0808.58f1: sequence = 8, time = 14ms
64 bytes from 001e.0808.58f1: sequence = 9, time = 17ms
L2 ping completed.
---------------------------------
10 packet(s) transmitted, 10 received, 0 % packet loss
```

4 RMON 配置

4.1 RMON 简介

RMON（Remote Network Monitoring）是 Internet 工程任务组（IETF）定义的监测规范，它可以使网络监控器和控制台系统之间交换网络监测数据。用户可以结合 RMON 和交换机中的简单网络管理协议（SNMP）代理来监控网络中流经交换机的数据流量。RMON 是一种标准的监测规范，在 SNMP 的基础上与其框架兼容，拓展了 SNMP 的功能，更有效地对远程设备进行管理和监测。监控者可以通过控制台系统或监测器收集数据，更好地规划网络、优化性能，还可以提供全面的网络故障诊断。

RMON 在网络管理中对监控的设备主要实现统计功能与告警功能。统计功能主要用于监测端口的使用情况，如网络冲突数、过大或过小的数据报文数量、广播或多播的报文数量、接收字节数等；告警功能对告警变量进行监控，如端口的统计数据。当监控的 MIB 值超过上限阈值时，通过 SNMP 模块给管理设备发送告警信息。

4.2 配置 RMON

4.2.1 配置 RMON 统计功能

根据统计对象的不同，进一步划分 RMON 的统计功能，可以分为以太网统计功能及历史统计功能。

表 4-1 配置 RMON 以太网统计功能

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	-
rmon collection stats *stats-id* [**owner** *word*]	为端口创建一条统计表项	stats-id: RMON 统计的 ID，取值范围为 1～65535 word: 指定统计的归属人信息 缺省情况下，未创建统计表项

下表的命令用于创建历史控制表项，收集端口在指定时间内收到的各类报文。buckets 用于指定保留的统计量，interval 用于指定收集报文的周期。

表 4-2 配置 RMON 历史统计功能

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	-
rmon collection history *index* [**buckets** *numbs*] [**interval** *values*] [**owner** *word*]	为端口创建一条历史控制表项	index: RMON 历史统计的 ID，取值范围为 1～65535 numbs: 设置保留历史记录数量，取值范围为 1～65535 values: 统计的频率，单位：秒，取值范围为 1～3600 word: 指定统计的归属人信息 缺省情况下，未创建历史控制表项

4.2.2 配置 RMON 告警功能

当监控数据的值达到阈值时，会产生 RMON 告警事件，此时会根据事件的定义对告警进行处理，即指定该事件被触发时进行的操作（记录日志、发送工作）。

表 4-3 创建事件表项

命令	操作	说明
configure terminal	进入全局配置模式	-
rmon event *index* [**description** *info*] [**log**] [**trap** *string*] [**owner** *word*]	创建事件表项	index: 事件 ID，取值范围为 1～65535 string: Trap 的 community 参数 info: 对事件的描述或注释 word: 事件的归属人信息 缺省情况下，未创建事件表项

表 4-4 创建告警表项

命令	操作	说明
configure terminal	进入全局配置模式	-
rmon alarm *index variables* **interval** *values* { **delta** | **absolute** } **rising-threshold** *holds1* [**event** *numbs1*] **falling-threshold** *holds2* [event *numbs2*] [**owner** *word*]	创建告警表项	index: 警告 ID，取值范围为 1～65535 variables: 警告监控的 MIB 节点(etherStatsEntry.m.n) values: 指定警告监控 MIB 节点的周期，单位：秒，取值范围为 1～65535 holds1: 设置上限阀值，取值范围为-2147483648~2147483646 numbs1: 指定警告上限阀值触发的 RMON 事件，取值范围为 1～65535 holds2: 设置下限阀值，取值范围为-2147483648~2147483646 numbs2: 指定警告下限阀值触发的 RMON 事件，取值范围为 1～65535 word: 事件的归属人信息 缺省情况下，未创建告警表项

4.3 RMON 显示与维护

表4-5 RMON显示与维护

命令	操作	说明
show rmon statistics [*statistics-id*]	显示 RMON 所有或指定的的统计信息	statistics-id: 统计 ID，取值范围为 1～65535
show rmon history [*history-id*]	显示 RMON 所有或指定的历史信息	history-id: 历史记录 ID，取值范围为 1～65535
show rmon event [*event-id*]	显示 RMON 所有或指定的事件	event-id: 事件 ID，取值范围为 1～65535
show rmon alarm [*alarm-id*]	显示 RMON 所有或指定的告警	alarm-id: 告警 ID，取值范围为 1～65535

4.4 配置举例

4.4.1 配置举例

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# rmon collection stats 1 owner test	创建一条统计表项：统计 ID 为 1，用于记录端口的统计
Switch(config-if)# rmon collection history 1 buckets 100 interval 1000 owner test	在端口创建一条统计历史记录表项：编号为 1，每 1000 秒记录一次端口统计值，一共保留 100 次
Switch(config-if)# exit	退出接口配置模式
Switch(config)# rmon event 1 log trap public description test_event owner test	创建一条事件表项：事件 ID 为 1。如果触发该事件系统会发送日志和告警
Switch(config)# rmon alarm 1 etherStatsEntry.6.1 interval 1000 delta rising-threshold 1000 event 1 falling-threshold 1 event 1 owner test	创建一条警告表项，关注 ETHERSTATSBROADCASTPKTS 这个值，每 1000 秒统计一次，如果超过 1000 或者低于 1 都会触发事件 1

4.4.2 命令验证

- 显示RMON所有的统计信息：

```
Switch# show rmon statistics

  Rmon collection index 1
        Statistics ifindex = 1, Owner: test
        Input packets 0, octets 0, dropped 0
        Broadcast packets 0, multicast packets 0, CRC alignment errors 0, collisions 0
        Undersized packets 0, oversized packets 0, fragments 0, jabbers 0
        # of packets received of length (in octets):
        64: 0,    65-127: 0, 128-255: 0
        256-511: 0,    512-1023: 0, 1024-max: 0
```

- 显示RMON所有的历史信息：

```
Switch# show rmon history

  History index = 1
        Data source ifindex = 1
        Buckets requested = 100
        Buckets granted = 100
        Interval = 1000
        Owner: test
```

- 显示RMON所有的事件信息：

```
Switch# show rmon event

  Event Index = 1
        Description: test_event
        Event type Log & Trap
        Event community name: public
        Last Time Sent = 00:00:00
        Owner: test
```

- 显示RMON所有的告警信息：

```
Switch# show rmon alarm

  Alarm Index = 1
  Alarm status = VALID
  Alarm Interval = 1000
  Alarm Type is Delta
  Alarm Value = 00
  Alarm Rising Threshold = 1000
  Alarm Rising Event = 1
  Alarm Falling Threshold = 1
  Alarm Falling Event = 1
  Alarm Owner is test
```

5 SNMP 配置

5.1 SNMP 简介

SNMP（Simple Network Management Protocol，简单网络管理协议）是网络管理系统（NMS）和代理进程（Agent）之间的通信协议。它规定了在网络环境中对设备进行监视和管理的标准化管理框架、通信的公共语言、相应的安全和访问控制机制。网络管理员使用SNMP功能可以查询设备信息、修改设备的参数值、监控设备状态、自动发现网络故障、生成报告等。

5.1.1 SNMP 技术优势

SNMP 具有以下技术优点：

- 基于 TCP/IP 互联网的标准协议，传输层协议一般采用 UDP。
- 自动化网络管理。网络管理员可以利用 SNMP 平台在网络上的节点检索信息、修改信息、发现故障、完成故障诊断、进行容量规划和生成报告。
- 屏蔽不同设备的物理差异，实现对不同厂商产品的自动化管理。SNMP 只提供最基本的功能集，使得管理任务与被管设备的物理特性和实际网络类型相对独立，从而实现对不同厂商设备的管理。
- 简单的请求—应答方式和主动通告方式相结合，并有超时和重传机制。
- 报文种类少，报文格式简单，方便解析，易于实现。
- SNMPv3 版本提供了认证和加密安全机制，以及基于用户和视图的访问控制功能，增强了安全性。

5.1.2 SNMP 结构

SNMP的主要架构可分为NMS、Agent和MIB，它们的定义如下：

NMS（Network Management System，网络管理系统）：网管系统的控制台，又称为管理站。能够向管理者提供统一的用户界面，以获取设备的相关信息。

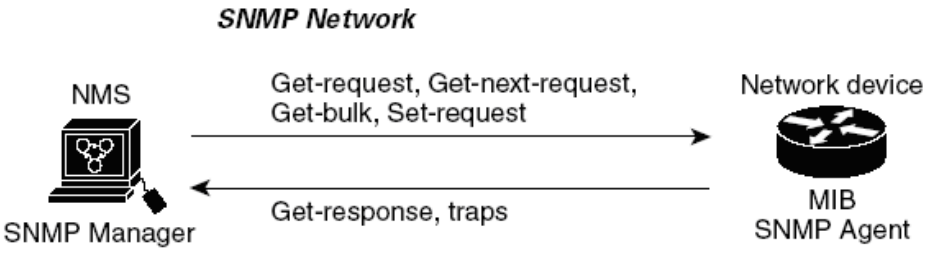
Agent：是SNMP的访问代理，实现设备与NMS之间的通信。Agent收到NMS的请求信息后，将查询或修改的结果发送给NMS。如遇设备故障或事件发生时，Agent也会发送Trap信息给NMS，告知设备的

状态和变化。

MIB（Management Information Base，管理信息库）：MIB是被管理对象的集合，定义了代理进程中能够查询与修改的参数。管理站和代理通过MIB进行接口的统一，NMS可对代理中的管理对象进行读/写操作，从而实现对代理的管理和控制。

NMS、Agent与MIB的关系如图 5-1所示：

图 5-1 SNMP 网络拓扑图



5.1.3 SNMP 版本

SNMP共有SNMPv1、SNMPv2c与SNMPv3三个版本。SNMPv1与SNMPv2c都具备读/写MIB的功能，采用团体名认证机制。SNMPv2c对SNMPv1进行了功能的拓展，比如批量获取数据、增加警报等。SNMPv3在SNMPv2c的基础上增加了USM（User-Based Security Model，基于用户的安全模型）认证机制，通过数据加密和用户认证的功能，增强了NMS与Agent之间通信的安全性。

5.2 配置 SNMP

5.2.1 配置 SNMPv1/SNMPv2c 的属性

1. 配置SNMPv1/ SNMPv2c的基本属性

表5-1 配置SNMPv1/ SNMPv2c的基本属性

命令	操作	说明
configure terminal	进入全局配置模式	-
snmp-server enable	使能 SNMP 功能	缺省情况下，SNMP 功能处于关闭状态

命令	操作	说明
snmp-server system-contact *text*	（可选）配置设备管理者联系方式	缺省情况下，未配置管理者联系方式。可通过配置文件查看管理员的联系方式
snmp-server system-location *text*	（可选）配置设备放置位置的描述信息	缺省情况下，未配置该描述信息。可通过配置文件查看描述信息
snmp-server version { **all** | **v1** | **v2c** | **v3** }	启用 SNMPv1/ SNMPv2c 版本	缺省情况下，配置系统支持的 SNMP 的版本为 all
snmp-server engineID *engineid-string*	（可选）配置本地设备的 SNMP 的引擎 ID	engineid-string: 引擎 ID 字符串必须为偶数个十六进制数。取值范围为 10~64 个字符
snmp-server view *view-name* { **included** | **excluded** } *sub-tree* [**mask** *subtree-mask*]	（可选）创建或更新 SNMP 视图	view-name: 创建或更新的视图名称 sub-tree: MIB 对象子树 subtree-mask: MIB 对象子树掩码 缺省情况下，未创建 SNMP 视图
snmp-server community *string* { **read-only** | **read-write**} [**view** *view-name*]	配置 SNMP 的团体属性	string: 团体名，取值为 1~256 个字符的字符串。空格表示不允许访问；缺省情况下，未配置 SNMP 的团体属性
snmp-server context *context-name*	（可选）配置 SNMP 的上下文	context-name: 上下文名称 缺省情况下，未配置 SNMP 的上下文

2. 配置SNMPv1/ SNMPv2c的通告属性

表5-2 配置SNMPv1/ SNMPv2c的通告属性

命令	操作	说明
configure terminal	进入全局配置模式	-
snmp-server trap enable *notification-type*	使能相关的 SNMP 通告类型	缺省情况下，关闭设备发送指定类型的 Trap
snmp-server trap target-address [**mgmt-if**] { *ipv4-address* | *ipv6-address* }	配置系统产生的 Trap 发送到指定的服务器	Trap 支持接收服务器的 IPv4 地址 /IPv6 地址；

命令	操作	说明
community *string* [**udpport** *number*]		string：团体名称 number：Trap 发送的端口号，默认端口号为 162

5.2.2 配置 SNMPv3 的属性

1. 配置SNMPv3的基本属性

表5-3 配置SNMPv3的基本属性

命令	操作	说明
configure terminal	进入全局配置模式	-
snmp-server enable	使能 SNMP 功能	缺省情况下，SNMP 功能处于关闭状态
snmp-server system-contact *text*	（可选）配置设备管理者联系方式	缺省情况下，未配置管理者联系方式。可通过配置文件查看管理员的联系方式
snmp-server system-location *text*	（可选）配置设备放置位置的描述信息	缺省情况下，未配置该描述信息。可通过配置文件查看该描述符
snmp-server version { **all** | **v1** | **v2c** | **v3** }	启用 SNMPv3 版本	缺省情况下，配置系统支持的 SNMP 的版本为 all
snmp-server engineID *engineid-string*	（可选）配置本地设备的 SNMP 的引擎 ID	engineid-string: 引擎 ID 字符串必须为偶数个十六进制数。取值范围为 10~64 个字符
snmp-server view *view-name* { **included** | **excluded** } *sub-tree* [**mask** *subtree-mask*]	（可选）创建或更新 SNMP 视图	view-name: 创建或更新的视图名称 sub-tree: MIB 对象子树 subtree-mask: MIB 对象子树掩码 缺省情况下，未创建 SNMP 视图
snmp-server usm-user *user-name* [**remote** *engine-id*] [**authentication** { **md5** | **sha** }]	配置 SNMPv3 用户	user-name: 连接到代理设备的用户名 engine-id: 用户所属远程设备的引擎 ID

命令	操作	说明
[8] *auth-passsword* [**privacy** { **aes** | **des** } [8] *privpassword*]		auth-passsword: 配置认证密码 privpassword: 指定加密密码
snmp-server group *group-name* **user** *user-name* **security-model usm**	（可选）创建 SNMPv3 组	group-name: SNMPv3 组名 user-name: 用户名
snmp-server access *group-name* **security-model usm** { **auth** | **noauth** | **priv** }	（可选）配置 MIB 视图的访问控制属性	group-name: SNMPv3 组名
snmp-server community *string* { **read-only** | **read-write**} [**view** *view-name*]	配置 SNMP 的团体属性	string: 团体名，取值为 1~256 个字符的字符串。空格表示不允许访问缺省情况下，未配置 SNMP 的团体属性
snmp-server context *context-name*	（可选）配置 SNMP 的上下文	context-name: 上下文名称 缺省情况下，未配置 SNMP 的上下文

2. 配置SNMPv3的通告属性

表5-4 配置SNMPv3的通告属性

命令	操作	说明
configure terminal	进入全局配置模式	-
snmp-server trap enable *notification-type*	使能相关的 SNMP 通告类型	notification-type:通告类型，如果使用“all”参数。系统将使能使用该命令的所有通告类型。 缺省情况下，关闭设备发送指定类型的 Trap
snmp-server notify *notify-name* **tag** *tag-name* [**inform** | **trap**]	配置 SNMPv3 的通告	notify-name: 通告名 tag-name: 标记名
snmp-server target-address *host-name* **param** *param-name* [mgmt-if]{ *ipv4-address* | *ipv6-address*} [**udpport** *port* | **timeout** *number* | **retries** *times*] * [**taglist** *line*]	指定允许接收 SNMP 请求报文的目的主机	host-name: 远程目的主机名称 param-name: 地址参数表名（必须是本地已经配置的地址参数名） port: UDP 端口号，默认值 162 number: 超时时间，取值范围为

命令	操作	说明
		0~65535，默认值为 1500 times: 重传次数，取值范围为 0~255，默认值为 3 line: 标记列表，用于标识发送通告和转发消息到其上的目的地址，可以配置多个值，中间使用空格隔开（最多支持 128 个），最大长度 255 个字符
snmp-server target-params *params-name* **user** *user-name* **security-model v3 message-processing** { **auth | noauth | priv** }	将用户加入 SNMPv3 组内	params-name: 地址参数表名 user-name: 用户名

5.3 SNMP 显示与维护

表5-5 SNMP显示与维护

命令	操作	说明
show snmp	显示 SNMP 的服务信息	-
show snmp-server access [*group-name*]	显示 SNMP 的访问控制信息	group-name: 指定组名
show snmp-server community	显示 SNMP 团体信息	-
show snmp-server context	显示 SNMP 的上下文信息	-
show snmp-server engineID	显示 SNMP 的引擎 ID 信息	-
show snmp-server group [*group-name*]	显示 SNMP 组的信息，如组名、安全模式、视图、存储类型等	group-name: 指定组名
show snmp-server notify [*group-name*]	显示 SNMP 通告信息	group-name: 指定组名

命令	操作	说明
show snmp-server trap-receiver	显示 SNMP 的 traps 接收主机	-
show snmp-server usm-user [*user-name*]	显示 SNMP 的用户信息	user-name: 指定用户名
show snmp-server version	显示支持的 SNMP 版本	-
show snmp-server view [*view-name*]	显示 SNMP 视图配置信息	view-name: 指定视图名

5.4 配置举例

5.4.1 启用 SNMP 服务

i. 配置步骤

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# snmp-server enable	启用 SNMP 服务
Switch(config)# end	退出全局配置模式

ii. 命令验证

显示 SNMP 配置信息：

```
Switch# show running-config
snmp-server enable
```

5.4.2 配置团体字符串

用户可以使用 SNMP 团体字符串来定义 SNMP 管理者和代理之间的关系。团体字符串的作用和密码类似，通过配置团体字符串允许访问代理交换机。用户可以指定一个或多个团体字符：

- 一个 MIB 视图定义了所有团体可访问的 MIB 对象子集。
- 设置访问的 MIB 对象的读/写权限。

按照下列步骤在交换机上配置团体字符串，以下步骤配置完成后，就可以实现 SNMP 的基本读写功能。

i. 配置步骤

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# snmp-server view DUT included 1	（可选）配置一个视图名“DUT”
Switch(config)# snmp-server community public read-write view DUT	配置团体名字 “public”，读写权限，可访问的视图为 “DUT”
Switch(config)# end	退出全局配置模式

ii. 命令验证

查看配置后的团体名信息：

```
Switch# show running-config

snmp-server enable
snmp-server view DUT included .1
snmp-server community public read-only view DUT
```

5.4.3 配置 SNMPv1/SNMPv2c/SNMPv3 通告

i. 配置SNMPv1/SNMPv2c通告

1. 配置步骤

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# snmp-server trap enable all	开启所有 Trap
Switch(config)# snmp-server trap target-address 10.0.0.2 community public	配置目的 IPv4 地址以及团体名 Public
Switch(config)# snmp-server trap target-address 2001:1000::1 community public	配置目的 IPv6 地址以及团体名 Public

命令举例	操作步骤
Switch(config)# end	退出全局配置模式

2. 命令验证

查看配置 SNMPv1/SNMPv2c 通告后的信息：

```
Switch# show running-config

snmp-server trap target-address 10.0.0.2 community public
snmp-server trap target-address 2001:1000::1 community public
snmp-server trap enable vrrp
snmp-server trap enable igmp snooping
snmp-server trap enable ospf
snmp-server trap enable pim
snmp-server trap enable stp
snmp-server trap enable system
snmp-server trap enable coldstart
snmp-server trap enable warmstart
snmp-server trap enable linkdown
snmp-server trap enable linkup
```

ii. 配置SNMPv3通告

1. 配置步骤

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# snmp-server trap enable all	开启所有 Trap
Switch(config)# snmp-server notify notif1 tag tmptag trap	创建一个 Trap 消息条目
Switch(config)# snmp-server target-address targ1 param parm1 10.0.0.2 taglist tmptag	配置目的 IPv4 地址以及团体名 Public
Switch(config)# snmp-server target-address t1 param p1 2001:1000::1 taglist tag1	配置目的 IPv6 地址以及团体名 Public
Switch(config)# snmp-server target-params parm1 user usr1 security-model v3 message-processing v3 noauth	将用户加入到 SNMPv3 组内
Switch(config)# end	退出全局配置模式

2. 命令验证

查看配置 SNMPv3 通告后的信息：

```
Switch# show running-config

snmp-server notify notif1 tag tmptag trap
snmp-server target-address t1 param p1    2001:1000::1 taglist tag1
snmp-server target-address targ1 param parm1    10.0.0.2 taglist tmptag
snmp-server target-params parm1 user usr1 security-model v3 message-processing v3 noauth
snmp-server trap enable vrrp
snmp-server trap enable igmp snooping
snmp-server trap enable ospf
snmp-server trap enable pim
snmp-server trap enable stp
snmp-server trap enable system
snmp-server trap enable coldstart
snmp-server trap enable warmstart
snmp-server trap enable linkdown
snmp-server trap enable linkup
```

5.4.4 配置 SNMPv3 的基本属性

i. 配置步骤

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch (config)# snmp-server engineID 8000123456	配置 engine ID
Switch(config)# snmp-server usm-user usr1 authentication md5 mypassword privacy des yourpassword	配置用户名和密码以及验证类型
Switch(config)# snmp-server group grp1 user usr1 security-model usm	创建 SNMPv3 组
Switch(config)# snmp-server access grp1 security-model usm noauth	设置组内成员的权限
Switch(config)# end	退出全局模式

ii. 命令验证

显示 SNMPv3 组的相关配置信息：

```
Switch# show running-config

snmp-server engineID 8000123456
snmp-server usm-user usr1 authentication md5 mypassword privacy des yourpassword
snmp-server group grp1 user usr1 security-model usm
snmp-server access grp1 security-model usm noauth
```

6 sFlow 配置

6.1 sFlow 简介

sFlow 即 Sampled Flow，是一种监控网络设备流量转发情况的技术。sFlow 系统中包含多个 sFlow Agent 与一个 sFlow Collector，通过一种采样机制以一定速率采样，获取设备流量转发的统计信息。然后将采样信息发送到监控的 sFlow Collector 进行分析。一个 sFlow Collector 可以对若干个 sFlow Agent 进行分析并得出结果，在 Server 端可以参看多个 Agent 的流量情况。

sFlow 为用户提供两种类型的采样机制分析流量的转发情况：

Flow 采样：基于数据包的流量进行采样，在指定端口根据特定的采样方向和报文进行比对和分析，通过 sFlow 报文将分析的结果发送给 sFlow Collector。

Counter 采样：基于端口的统计信息进行采样，周期性地获取端口的统计信息并通过 sFlow 报文发送给 sFlow Collector。

6.2 配置 sFlow

6.2.1 全局使能 sFlow

在进行 sFlow 的其他配置前，必须先使用此命令全局使能 sFlow 服务。如果使用此命令的 **no** 形式，所有 sFlow 的配置将会被清空。

表6-1 全局使能sFlow

命令	操作	说明
configure terminal	进入全局配置模式	-
sflow enable	全局开启 sFlow 服务	缺省情况下，sFlow 服务处于关闭状态

6.2.2 配置 sFlow Agent 与 sFlow Collector

表6-2 配置sFlow Agent与sFlow Collector

命令	操作	说明
configure terminal	进入全局配置模式	-
sflow enable	全局开启 sFlow 服务	缺省情况下，sFlow 服务处于关闭状态
sflow agent { **ip** *ipv4-address* | **ipv6** *ipv6-addres* }	配置 sFlow Agent 的 IP 地址	如果没有配置 sFlow 代理地址，系统将会使用第一个合法的 router-id 作为代理地址，并且不会再改变
sflow collector { *ipv4-address* | *ipv6-address* } [*port-number*]	配置 sFlow Collector 的 IP 地址	port-number: 收集服务器的接收 UDP 端口号，取值范围为 1~65535。如果未指定，使用默认值 6343

6.2.3 配置 Flow 采样

Flow 采样速率数值可以简单地理解为一次有多少个报文可以进入芯片采样。数值 1 表示 100%采样。但由于芯片是通过计算概率的方式实现，所以并不一定严格按照这个数字进行采样。系统对报文进行采样时会将报文的前 256 字节封装到 sFlow 协议报文中。系统对基于统计和基于报文的采样都是通过软件实现的，如果采样速率配置的很低，CPU 利用率就会非常高。另外 CPU 流量控制模块将 sFlow 采样报文上 CPU 的速率限制为 400kbps，如果用户要求高的采样速率可以修改这个值。

下面的命令可以在非 link agg 成员的物理口上配置，也可以在 link agg 端口上配置。

表6-3 配置Flow采样

命令	操作	说明
configure terminal	进入全局配置模式	-
sflow enable	全局开启 sFlow 服务	缺省情况下，sFlow 服务处于关闭状态
interface *if-name*	进入接口配置模式	-
sflow flow-sampling rate *rate-value*	配置基于报文的采样的速率	rate-value: 基于报文采样的速率必须是 2 的整数幂，可配范围为 1~8192。采样速率的默认值为 8192
sflow flow-sampling enable { **input** | **output** | **both** }	在端口上使能基于报文的采样功能	缺省情况下，去使能基于报文的采样功能

6.2.4 配置 Counter 采样

基于统计的采样是指每个采样间隔内，系统会将端口上的统计信息通过 sFlow 协议报文送往采样收集服务器。

表 6-4 配置 Counter 采样

命令	操作	说明
configure terminal	进入全局配置模式	-
sflow enable	全局开启 sFlow 服务	缺省情况下，sFlow 服务处于关闭状态
sflow counter interval *interval-value*	配置基于统计的采样间隔	interval-value: 采样间隔，单位：秒，可配范围为 1~2000。默认值为 20s
interface *if-name*	进入接口配置模式	-
sflow counter-sampling enable	在端口上使能基于统计的采样功能	缺省情况下，去使能基于统计的采样功能

6.3 sFlow 显示与维护

表 6-5 sFlow 显示与维护

命令	操作	说明
show sflow	查看 sFlow 的配置信息	-

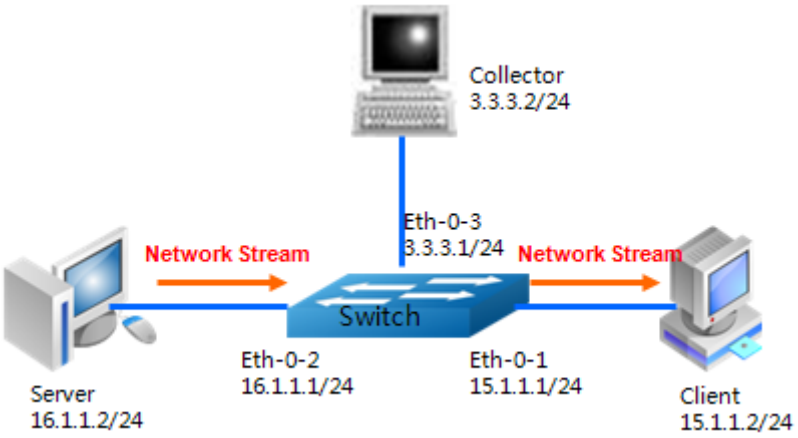
6.4 配置举例

6.4.1 介绍

下图是 sFlow 的一个基本配置：所有进入端口 eth-0-1 的报文将会以一定速率采样，然后发送给 Collector PC 3.3.3.2。

6.4.2 拓扑

图 6-1 sFlow 基本配置拓扑图



6.4.3 配置步骤

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# sflow enable	全局使能 sFlow
Switch(config)# sflow counter interval 20	配置基于统计的采样间隔
Switch(config)# sflow agent ip 3.3.3.1	配置 sFlow Agent 的 IPv4 地址
Switch(config)# sflow collector 3.3.3.2 6342	配置 sFlow Collector 的 IPv4 地址及 UDP 端口号
Switch(config)# sflow collector 2001:1000::1	配置 sFlow Collector 的 IPv6 地址
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# sflow flow-sampling rate 8192	配置基于报文的采样速率
Switch(config-if)# sflow flow-sampling enable input	端口上使能基于报文的采样功能
Switch(config-if)# sflow counter-sampling enable	端口上使能基于统计的采样功能
Switch(config-if)# no switchport	将端口切换到 3 层口
Switch(config-if)# ip address 15.1.1.1/24	配置端口的 IP 地址

命令举例	操作步骤
Switch(config-if)# exit	退出至全局配置模式
Switch(config)# interface eth-0-2	进入接口配置模式
Switch(config-if)#no switchport	切换到 3 层口
Switch(config-if)# ip address 16.1.1.1/24	配置端口的 IP 地址
Switch(config-if)# exit	退出至全局配置模式
Switch(config)# interface eth-0-3	进入接口配置模式
Switch(config-if)# no switchport	切换到 3 层口
Switch(config-if)# ip address 3.1.1.1/24	配置端口的 IP 地址

6.4.4 命令验证

显示 sFlow 的配置信息：

```
Switch# show sflow

sFlow Global Information:
  Agent IP address                : 2.2.2.1
  Agent IPv6 address              : 2026::2
  Counter Sampling Interval       : 20 seconds
  Collector 1:
    Address: 3.3.3.2
    Port: 6342
  Collector 2:
    Address: 2001:1000::1
    Port: 6343
sFlow Port Information:
                                                 Flow-Sample     Flow-Sample
  Port            Counter       Flow         Direction        Rate
  ---------------------------------------------------------
  eth-0-1         Enable        Enable       Input            8192
```

7 LLDP 配置

7.1 LLDP 简介

链路层发现协议 LLDP（Link Layer Discovery Protocol）是 IEEE 802.1ab 中定义的第二层发现协议。第二层发现（Layer 2 Discovery）可以准确定位设备附带有哪些接口，以及设备之间相互连接等二层信息，例如端口的 VLAN 属性和支持的协议类型等，并显示出客户端、交换机、路由器和应用服务器以及网络服务器之间的路径。这些详细的信息以 MIB（Management Information Base，管理信息库）的方式存储，对快速获取相连设备的拓扑状态、设备间的配置冲突、查询网络失败的根源很有帮助。

7.1.1 工作原理

LLDP 实体主要维护本地设备与远端设备的 MIB 信息，通过与物理拓展 MIB、实体 MIB、接口 MIB 等信息库之间的交互更新与维护本地设备的 MIB，再将本地设备的信息封装为 LLDP 帧发送至远端设备，远端设备收到这些信息后会将其更新至远端系统 MIB。当本地或远端系统的 MIB 发生变化时，会触发通告事件。

7.1.2 基本概念

LLDPDU: 封装有 LLDP 数据单元的报文称为 LLDP 帧，有两种封装格式：Ethernet II 和 SNAP（Subnetwork Access Protocol，子网访问协议）。

TLV: LLDPDU 采用 TLV (Type + Length + Value) 的格式。TLV 包括多种类型，基本类型中有端口描述 TLV、系统名称 TLV、系统描述 TLV、系统能力 TLV、管理地址 TLV，这些是强制性的 TLV，还包括组织定义的 TLV 以及 MED TLV。

7.1.3 收发机制

LLDP 发送报文机制：开启 LLDP 功能后，设备会周期性地发送 LLDP 报文至邻居设备。当本地设备的配置有变时，邻居设备会收到来自本地设备的 LLDP 报文。由于可能产生因本地信息的变化过多，导致

频繁发送报文的情况，每次发送一个 LLDP 报文会有延迟，经过这个延迟时间后才会发送下一个 LLDP 报文。

LLDP 接收报文机制：开启 LLDP 功能后，设备对接收的 LLDP 报文及其 TLV 进行检查，有效性检查通过后才会将信息保存回本地，并按照 Time To Live（TTL，生存时间）设置邻居在本地设备的老化时间。当 TTL 的值为零时，邻居信息会立即被老化。

7.2 配置 LLDP

7.2.1 使能 LLDP 功能

在启用 LLDP 功能前，必须同时在全局和接口上使能 LLDP。

表7-1 全局与接口使能LLDP功能

命令	操作	说明
configure terminal	进入全局配置模式	-
lldp enable	全局使能 LLDP 功能	缺省情况下，全局 LLDP 功能处于关闭状态
interface *if-name*	进入接口配置模式	-
lldp enable { **txonly** | **txrx** | **rxonly** }	接口使能 LLDP 功能	缺省情况下，接口上的 LLDP 功能处于关闭状态

7.2.2 配置 LLDP 系统信息

表7-2 配置LLDP系统名称与描述

命令	操作	说明
configure terminal	进入全局配置模式	-
lldp system-name *name*	配置 LLDP 系统名称信息	name: 系统名称，取值范围为 1~64
lldp system-description *des*	配置 LLDP 系统描述信息	des: 系统描述，长度范围为 1~255，允许空格

7.2.3 配置 LLDP 管理地址

配置的管理地址优先于配置的接口，如果两者都没有配置，系统将会按照环回接口、管理口、其他三层接口、系统 MAC 地址的顺序，使用默认管理地址。同类接口中将使用 IP 地址较小的接口。

表7-3 配置LLDP管理地址

命令举例	操作	说明
configure terminal	进入全局配置模式	-
lldp management { **ip** *ip-address* | **interface** *if-name* }	配置管理 IP 地址	ip-address: IPv4 地址 if-name: 接口名，需为三层端口

7.2.4 配置 LLDP 报文发送参数

表7-4 配置LLDP报文发送参数

命令	操作	说明
configure terminal	进入全局配置模式	-
lldp msg-tx-hold *number*	配置 tx TTL 的值	number: 取值范围为 2~ 10，默认值为 4
lldp timer msg-tx-interval *interval-value*	配置传送周期的时间间隔	interval-value: 取值范围为 5~32768，默认值为 30s
lldp timer tx-delay *delay-time*	配置传输延迟	delay-time: 取值范围为 1~8192，默认值为 2s。tx-delay 的值需要遵守公式：1 <= tx-delay <= (0.25)* msg-tx-interval

7.2.5 配置 TLV 类型

可以配置的基本 TLV 类型包括端口描述 TLV、系统名称 TLV、系统描述 TLV、系统能力 TLV、管理地址 TLV 以及所有基本 TLV。

表7-5 配置基本TLV

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

命令	操作	说明
interface *if-name*	进入接口配置模式	-
lldp tlv basic { **port-description** | **system-name** | **system-description** | **system-capabilities** | **management-address** | **all** }	配置基本 TLV	缺省情况下，配置基本 TLV 为 all

用户还可以配置IEEE 802.1组织定义的TLV、802.3组织定义的TLV。

表7-6 配置组织定义的TLV

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	-
lldp tlv 8021-org-specific { **port-vlan** | **protocol-vlan** | **vlan-name** | **protocol-id** | **link-aggregation** | **dcbx** | **all** }	配置 IEEE 802.1 组织定义的 TLV	缺省情况下，除 Link Aggregation TLV 的所有 IEEE 802.1 TLV 都已使能
lldp tlv 8023-org-specific { **mac-phy-cfg** | **power** | **link-aggregation** | **max-frame-size** | **all** }	配置 IEEE 802.3 组织定义的 TLV	缺省情况下，配置 IEEE 802.3 TLV 为 all

根据实际情况，可以选择配置媒体终端发现（MED：Media Endpoint Discovery）TLV。当选择配置 MED 的某一个 TLV 时，LLDP-MED Capabilities TLV 会自动被选择；而当没有选择其他的 MED TLV 时，会自动取消 LLDP-MED Capabilities TLV 的选择。

表7-7 配置MED TLV与MED Location-id TLV

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	-
lldp tlv med { **network-policy** | **ext-power** | **inventory** | **all** }	配置 MED TLV	缺省情况下，配置 MED TLV 为 all
lldp tlv med location-id { **ecs-elin** *value* | **civic** *dev-type code ca-type ca-value* }	配置 MED Location-id TLV	dev-type: 设备类型，有效值为-2，0 表示配置设备类型为 DHCP server，1 表示配置设备类型为

命令	操作	说明
		switch，2 表示配置设备类型为 lldp-med endpoint code: 国家编码，取值范围请参考 ISO 3166。 ca-type ca-value: 地址信息，最多可以有 10 组, ca-type 的范围是 0~255，ca-value 的长度范围是 1~232

7.3 LLDP 显示与维护

表 7-8 LLDP 显示与维护

命令	操作	说明
show lldp local { **config** | **tlv-info** } [**interface** *if-name*]	显示 LLDP 的本地信息	if-name: 物理端口名称
show lldp neighbor [**interface** *if-name*] [**brief**]	显示 LLDP 邻居信息	
show lldp statistics [**interface** *if-name*]	显示 LLDP 统计信息	
clear lldp statistics [**interface** *if-name*]	清除 LLDP 统计信息	

7.4 配置举例

7.4.1 LLDP 基本配置举例

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# lldp enable	全局使能 LLDP
Switch(config)# interface eth-0-9	进入接口配置模式
Switch(config)# no shutdown	打开端口

命令举例	操作步骤
Switch(config-if)# no lldp tlv 8021-org-specific vlan-name	取消配置 IEEE 802.1 TLV 中的 VLAN Name TLV
Switch(config-if)# lldp tlv med location-id ecs-elin 1234567890	选择并配置 MED TLV 中的 Location ID TLV
Switch(config-if)# lldp enable txrx	端口使能 LLDP，并配置模式为 txrx

7.4.2 LLDP 状态配置举例

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# lldp timer msg-tx-interval 40	配置 LLDP 报文传输间隔为 40 秒
Switch(config)# lldp timer tx-delay 3	配置 LLDP 报文传输延迟为 3 秒
Switch(config)# lldp timer reinit-delay 1	配置 LLDP 重新使能的延迟时间为 1 秒

7.4.3 命令验证

检查上述 LLDP 配置后的结果：

```
Switch# show lldp local config
LLDP global configuration:
============================================================
LLDP function global enabled : YES
LLDP msgTxHold         : 4
LLDP msgTxInterval : 40
LLDP reinitDelay     : 1
LLDP txDelay           : 3
Switch# show lldp local config interface eth-0-9
LLDP configuration on interface eth-0-9 :
============================================================
LLDP admin status : TXRX
Basic optional TLV Enabled:
    Port Description TLV
    System Name TLV
    System Description TLV
    System Capabilities TLV
    Management Address TLV
IEEE 802.1 TLV Enabled:
    Port Vlan ID TLV
```

```
        Port and Protocol Vlan ID TLV
        Protocol Identity TLV
    IEEE 802.3 TLV Enabled:
        MAC/PHY Configuration/Status TLV
        Power Via MDI TLV
        Link Aggregation TLV
        Maximum Frame Size TLV
    LLDP-MED TLV Enabled:
        Med Capabilities TLV
        Network Policy TLV
        Location Identification TLV
        Extended Power-via-MDI TLV
        Inventory TLV
    Switch# show running-config
    !
    lldp enable
    lldp timer msg-tx-interval 40
    lldp timer reinit-delay 1
    lldp timer tx-delay 3
    …
    interface eth-0-9
    lldp enable txrx
      no lldp tlv 8021-org-specific vlan-name
      lldp tlv med location-id ecs-elin 1234567890
    !
    Switch# show lldp neighbor
    Remote LLDP Information
    ============================================================
    Chassis ID type: Mac address
    Chassis ID         : 48:16:be:a4:d7:09
    Port ID type      : Interface Name
    Port ID             : eth-0-9
    TTL : 160
    Expired time: 134
    …
    Location Identification :
    ECS ELIN: 123456789
```

8 Telemetry 配置

8.1 Telemetry 简介

随着网络的发展和新技术的广泛应用，用户对业务质量的要求也越来越高。但是网络规模的日益增大，同时也增加了网络部署的难度。传统的网络监测技术存在一定局限性，例如 SNMP、CLI 等，在监控设备的数量和内容上有限，获取数据的速度有待提升。

Telemetry 是一种新型的远程网络监控与高速采集技术，能够更准确地对物理设备或虚拟设备的网络性能进行监控，快速定位故障，更加精准、实时监测数据。Telemetry 支持订阅一次后持续上报数据的功能，充分反映网络的实时状态，而不必每次上报数据都需要进行查询，降低了设备查询的次数和处理请求的压力。

8.2 配置 Telemetry

本小节介绍 IPv4 采集器的相关配置。设备（客户端）发起对采集器（服务端）的连接，进行数据采集的上送。

8.2.1 配置上送目标组与目标采集器

成功创建上送目标组后，可以执行此命令配置目标采集器信息条目。同一个上送目标组下配置的采集器数量上限为 5 条。当采集器条目达到配置上限时，无法再增加新条目。

表 8-1 配置上送目标组与目标采集器

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# destination-group dst1	创建名为 dst1 的上送目标组，并进入 destination-group 模式	dst1: 上送目标组名称。字符串形式，区分大小写，由字母、数字或字母和数字的组合组成，字母或数字之间不允许有空格，长度范围是 1～64；

命令举例	操作	说明
		上送目标组创建数量上限为 16 个
Switch(config-telemetry-destination-group)# ipv4-address 10.0.0.1 port 50001 protocol grpc	为上送目标组 dst1 创建目标采集器	目标采集器端口号为整数形式，取值范围为 50000~65535

说明

使用该命令 **ipv4-address** *ip-address* **port** *port-number* **protocol grpc** 指定数据上送协议为 gRPC。目前仅支持 gRPC，且无加密。

8.2.2 配置传感器组及采样路径

成功创建采样传感器组后，可以执行此命令配置采样路径。同一个采样传感器组下配置的路径数量上限为 5 条。当采样路径达到配置上限时，无法再增加新条目。

表 8-2 配置传感器及采样路径

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# sensor-group sensor1	创建名为 sensor1 的传感器组，并进入 sensor-group 模式	sensor1: 采样传感器组名称。字符串形式，区分大小写，由字母、数字或字母和数字的组合组成，字母或数字之间不允许有空格，长度范围是 1～64; 采样传感器组创建数量的上限为 16 个
Switch(config-telemetry-sensor-group)# sensor-path inspur-device:device-info/performance/cpu-use-rate	为采样传感器组 sensor1 创建采样路径（CPU 使用率）	采样路径名称为字符串形式，区分大小写，长度范围是 1～255。支持基于YANG模型的采样路径

8.2.3 创建 Telemetry 静态订阅

下表描述了基于 gRPC 协议创建的静态订阅。将采样传感器组和上送目标组关联，完成采样数据上送。

表 8-3 创建 Telemetry 静态订阅

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# subscription subs1	创建名称为 subs1 的静态订阅，并进入 subscription 模式	subs1: 订阅名称。字符串形式，区分大小写，由字母、数字或字母和数字的组合组成，字母或数字之间不允许有空格，长度范围是 1～64； 订阅创建数量的上限为 16 个
Switch(config-telemetry-subscription)# subs-sensor-group sensor1 sample-interval 10000	关联采样传感器组，配置该采样传感器组的采样周期	取值必须是已经在全局配置模式下创建成功的采样传感器组名称； 采样时间间隔。整数形式，取值范围是 100～1800000，单位：毫秒。目前仅支持配置 1000、5000、10000、30000、60000 、 180000 、 300000 、 900000 、 1800000 。 缺省值 10000ms
Switch(config-telemetry-subscription)# subs-destination-group dst1	配置关联上送目标组	取值必须是已经在全局配置模式下创建成功的上送目标组名称； 同一订阅下关联的目标组上限为 5 个

说明

- 关联的采样传感器组必须是已在全局配置模式下创建成功的采样传感器组，否则会关联失败。
- 关联的上送目标组必须是已在全局配置模式下创建成功的上送目标组，否则会关联失败。
- 如果配置的采样周期小于采样路径的最小采样精度，则设备会按照最小采样精度进行数据上报；

如果配置的采样周期大于最小采样精度，则设备按照配置的采样周期进行数据上报。

例如：inspur-device:device-info/performance/cpu-use-rate采样路径的最小采样精度为10000，如果执行命令设置的*sample-interval*参数的值为5000，则设备按照10000ms的周期进行数据上报，如果设置的值为60000，则设备按照60000ms的周期进行数据上报。

8.2.4 全局使能 Telemetry 采样动作

在完成 Telemetry 所有配置后使用此命令全局使能采样上送功能。修改订阅配置前需先去使能采样上送功能。

表 8-4 全局使能 Telemetry 采样动作

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# telemetry-sample enable	全局使能 Telemetry 采样动作	缺省情况下，未使能 Telemetry 采样动作

8.3 Telemetry 显示与维护

表 8-5 Telemetry 显示与维护

命令	操作	说明
show telemetry sensor-path	查看设备支持的采样路径	可查看目前设备支持的采样路径、对应采样类型和最小采样精度
show telemetry sensor	查看采样传感器组信息	采样传感器组信息包括名称、订阅状态、采样路径
show telemetry destination	查看上送目标组信息	上送目标组信息包括名称、订阅状态、包含目标采集器 IP 地址、端口号和支持协议
show telemetry subscription	查看订阅信息	查看订阅的名称、关联采样传感器组名称和采样周期、关联上送目标组名称

设备管理配置指导目录

1 STM 配置

1.1 STM 简介

交换机表项管理（STM）是通过配置交换机的系统资源支持优化的特定功能。用户可以选择一个配置文件提供来发挥系统的最大功能，例如，使用默认的配置文件以平衡资源；使用 VLAN 配置文件，以获得最大的 MAC 条目；或者选择 STM 模版，最大程度的支持（QoS）以及访问控制条目数（ACE）。为了在不同的场合下最大限度地利用 TCAM 资源，STM 提供了不同特性的系统优化功能。目前的版本中支持的 STM 模版包括：

- Layer 3：路由模板，支持最大数目的路由，通常应用在网络中心的路由器或聚合层。
- Layer 2：VLAN 模板，支持单播 MAC 地址的最大数量。它通常会被选定为第 2 层交换机。
- Default：默认模板，提供所有特性的平衡。
- IPv6：IPv6 模板，支持 IPv6 协议及 V4 和 V6 双栈使用。通常用于 IPv6 网络。

说明

如果配置（或当前使用）的 STM 模式不在下一个要启动的 image 中，那么当这个 image 启动时就会使用默认的硬编码配置，这个配置可能与正常的 Default 模式不一致。

1.2 配置 STM

1.2.1 配置系统表项资源

用户可以使用 STM prefer 命令来合理配置交换机的表项资源，以便最大程度地支持应用程序正在使用的功能。

表1-1 配置系统表项资源

命令	操作	说明
configure terminal	进入全局配置模式	-
stm prefer *profile*	配置交换机的表项资源	Profile 模式包括 default，ipv6，layer2 以及 layer3； 改变配置后，必须重启交换机配置才能生效

1.2.2 显示系统资源分配信息

如果该命令后不带参数，则显示当前正在使用的系统配置信息以及重启之后准备使用的系统资源分配情况。

表 1-2 显示系统资源分配信息

命令	操作	说明
show stm prefer [*profile*]	显示特定模版的系统资源分配信息	Profile 模式包括 default，ipv6，layer2 以及 layer3； 如果改变配置，但是未重启交换机，那么显示的是当前正在使用的系统资源信息。重启交换机之后，配置才会真正生效

1.3 配置举例

1.3.1 配置步骤

通过配置指南来选择正确的 STM 模板：

- 修改配置后必须重启交换机。
- STM Layer 2 模板一般适用于 2 层交换机且没有路由交换的场合。
- 当交换机上没有使能路由功能时，不需要切换到 Layer 3 模版。

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# stm prefer layer3	设置 STM Profile 为 layer3

命令举例	操作步骤
Switch(config)# end	退出全局配置模式
Switch# reload	重启系统

1.3.2 命令验证

显示使用路由模版后的输出结果：

```
Switch# show stm prefer

Current profile is :default
    number of vlan instance                          : 1/4094
    number of unicast & multicast mac address        : 0/65536
    number of backhole mac address                   : 0/128
    number of max applied vlan mapping               : 0/1024
    number of mac based vlan class                   : 0/512
    number of ipv4 based vlan class                  : 0/512
    number of dot1x mac based                        : 0/2048
    number of unicast ipv4 host routes               : 0/4096
    number of unicast ipv4 indirect routes           : 0/8192
    number of unicast ipv4 ecmp groups               : 0/256
    number of unicast ipv4 policy based routes       : 0/16
    number of unicast ip tunnel peers                : 0/8
    number of multicast ipv4 routes                  : 0/1023
    number of multicast ipv4 routes member           : 0/1024
    number of ipv4 source guard entries              : 0/1024
    number of ipv4 acl/qos flow entries              : 0/511
    number of link aggregation (static & lacp)       : 0/55
The profile stored for use after the next reload is the layer3 profile.
    number of vlan instance                          : 1/4094
    number of unicast & multicast mac address        : 0/32768
    number of backhole mac address                   : 0/128
    number of max applied vlan mapping               : 0/1024
    number of mac based vlan class                   : 0/512
    number of ipv4 based vlan class                  : 0/1024
    number of dot1x mac based                        : 0/512
    number of unicast ipv4 host routes               : 0/20480
    number of unicast ipv4 indirect routes           : 0/8192
    number of unicast ipv4 ecmp groups               : 0/256
    number of unicast ipv4 policy based routes       : 0/64
    number of unicast ip tunnel peers                : 0/8
    number of multicast ipv4 routes                  : 0/1024
    number of multicast ipv4 routes member           : 0/1024
    number of ipv4 source guard entries              : 0/512
```

```
number of ipv4 acl/qos flow entries          : 0/1536
number of link aggregation (static & lacp)   : 0/55
number of ipfix cache                        : 0/16384
```

2 系统日志配置

2.1 系统日志简介

系统消息可以保存在日志文件中，也可以发送到其他服务器设备。系统消息管理模块的功能如下：

- 记录日志信息以便监测和排除故障
- 可以选择记录日志信息的类型
- 可以选择日志的目的地

默认情况下，交换机会将重要的系统信息记录到其内部缓冲区，同时也会发送到系统控制台。用户可以指定保存的消息级别，且每条消息都会添加发生时间，有利于实时调试和提高管理性。

用户可以使用交换机的命令行界面（CLI）来读取系统消息，也可以通过将它保存到一个日志服务器的形式来获取消息。交换机的日志缓冲区最多可存储 1000 条信息。用户可以通过 Telnet 或控制台端口登录设备，登录成功后打开终端监控来实时监控系统日志。

2.2 配置系统日志

2.2.1 配置日志文件与严重级别

配置启用日志文件功能后，系统每隔 10 分钟会将产生的日志信息写入到 flash/log 文件中。

表 2-1 配置日志文件

命令	操作	说明
configure terminal	进入全局配置模式	-
logging file { **enable | disable** }	配置是否将日志信息写入到日志文件中	缺省情况下，系统会将日志信息写入到日志文件中

使能日志文件命令后，可以配置日志消息的阈值，高于等于此阈值的日志消息会被记录到日志文件，而低于此阈值的消息不会被记入日志文件。如果指定 debug，则所有日志消息都将被记入日志文件中。严重等级由高至低的定义如下表所示。

表 2-2 严重等级定义

严重等级	定义
emergency	系统无法使用
alert	必须立即采取行动
critical	严重事件
error	错误事件
warning	警告事件
notice	正常但重要的事件
information	信息
debug	调试级别的消息

表 2-3 配置严重等级

命令	操作	说明
configure terminal	进入全局配置模式	-
logging file enable	配置将日志信息写入到日志文件中	缺省情况下，系统会将日志信息写入到日志文件中
logging level file{ **alert | critical | debug | emergency | error | information | notice | warning |** *severity-level* }	配置日志消息的严重等级	severity-level：严重等级的取值范围为 0～7； 缺省情况下，严重等级为 warning

2.2.2 配置日志服务器

配置使用远程日志服务器后，需要配置日志服务器的 IP 地址、发往远程日志服务器的日志信息的阈值以及日志的守护进程。进程名与其编号的对应关系如下表所示。

表 2-4 进程名与其编号的对应关系

进程名	进程名编号	描述
auth	4	认证系统
authpriv	10	私有的安全/验证系统

进程名	进程名编号	描述
cron	9	时钟进程
daemon	3	系统进程
ftp	11	FTP 进程
kern	0	Kernel 消息
local0–7	16-23	保留本地定义的信息
lpr	6	行式打印机子系统
mail	2	邮件系统
news	7	网络新闻子系统
syslog	5	通过 syslogd 生成系统内部消息
user	1	随机用户等级消息
uucp	8	UUCP 子系统

表 2-5 配置日志服务器

命令	操作	说明
configure terminal	进入全局配置模式	-
logging server enable	使能远程日志服务器	缺省情况下，未使能远程日志服务器
logging server address [**mgmt-if**] { *ipv4-address* | *ipv6-address* } [**source-interface** *if-name* | **source-ip** *src-ip-address*]	配置日志服务器的 IP 地址	如果指定源接口或者源 IP 地址，将会使用对应的 IP 地作为发出报文的源 IP 地址
logging server severity { **alert** | **critical** | **debug** | **emergency** | **error** | **information** | **notice** | **warning** | *severity-level* }	配置远程日志服务器的日志信息等级	severity-level：严重等级的取值范围为 0～7； 如果设置阈值为 debug，则所有日志消息都将被发往日志服务器；缺省情况下，严重等级为 information
logging server facility *facility-type*	配置服务器的日志守护进程	缺省情况下，默认进程为 local4

2.2.3 配置缓冲区的日志条目数

表 2-6 配置缓冲区的日志条目数

命令	操作	说明
configure terminal	进入全局配置模式	-
logging buffer *buffersize*	配置系统临时缓冲区保存的日志数量	日志数量的取值范围为 10~1000，默认值为 500

2.3 显示与维护

表 2-7 显示与维护

命令	操作	说明
show logging	显示系统日志管理的配置信息	-
show logging buffer [*number* | **statistics**]	显示系统的日志缓冲区的配置信息	number：显示存储在日志缓冲区的条目
clear logging buffer	清除日志缓冲区中的记录	-

2.4 配置举例

2.4.1 配置日志服务器示例

i. 配置步骤

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# logging server enable	启用 LOG Server
Switch(config)# logging server address 1.1.1.1	指定 LOG Server IPv4 地址
Switch(config)# logging server address 2001:1000::2	指定 LOG Server IPv6 地址
Switch(config)# logging server severity debug	配置日志服务器的日志信息等级
Switch(config)# logging server facility mail	配置服务器的日志守护进程为 mail

ii. 命令验证

显示系统日志管理的配置信息：

```
Switch# show logging

Current logging configuration:
============================================================
logging buffer 500
logging timestamp bsd
logging file enable
logging level file warning
logging level module debug
logging server enable
logging server severity debug
logging server facility mail
logging server address 1.1.1.1
logging server address 2001:1000::2
logging alarm-trap enable
logging alarm-trap level middle
logging merge enable
logging merge fifo-size 1024
logging merge timeout 10
logging operate disable
```

2.4.2 配置缓冲区日志条目

i. 配置步骤

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# logging buffer 700	配置日志缓冲区的条目数为 700

ii. 命令验证

显示配置缓冲区日志条目数后的信息：

```
Switch# show logging
Current logging configuration:
============================================================
logging buffer 700
logging timestamp bsd
logging file enable
```

```
logging level file warning
logging level module debug
logging server enable
logging server severity debug
logging server facility mail
logging server address 1.1.1.1
logging alarm-trap enable
logging alarm-trap level middle
logging merge enable
logging merge fifo-size 1024
logging merge timeout 10
logging operate disable
```

说明

用户可以通过 **show** 命令来检查显示日志配置。配置 syslog 服务器时，请确保连线正确，这个可以通过使用 **ping** 命令来验证。同时用户也需要在日志服务器上配置 syslog 软件来接收日志。

3 镜像配置

3.1 镜像简介

镜像功能通过将某一端口、某一 VLAN 或 CPU 收/发端的报文复制一份，从设备的另一个端口上发送出去，在这个端口连上测试仪或其他报文收集设备，可达到对原始报文进行捕获和分析的目的。

只有指定端口、VLAN 或 CPU 收发端的报文可以通过镜像复制，这些被监控的对象（源端口、源 VLAN 或源 CPU）称作镜像源。镜像功能监测的是镜像源，而不是流量的“源”。例如，对一个 VLAN 的入方向流量做镜像时，从其他 VLAN 转发到这个 VLAN 的报文不会被复制，而这个 VLAN 收到并转发去其他 VLAN 的流量会被复制。

镜像功能不影响交换机源端口或源 VLAN 上原始的网络流量，通过源端口发送或接收的报文可以被复制，复制出来的流量将发送到指定的目的端口。

3.1.1 术语解释

1. 镜像会话

镜像会话的定义与特性如下：

- 镜像会话是一组镜像源和一个镜像目的的集合，其中镜像源可以是任意端口或者VLAN，镜像目的可以是二层或者三层物理接口。
- 系统最多支持三组镜像会话。
- 镜像功能不应干扰正常业务。

在一组镜像会话中，如果镜像源的总流量超过了镜像目的端口的转发能力，就会产生丢包现象。例如，用一个最大速率为 10Mbps 的目的端口去监控 100Mbps 的流量，将会产生丢包。一个正常工作的镜像会话需要配置镜像目的端口，以及至少一个镜像源。

2. 流量类型

镜像会话包括三种流量类型：

- 接收方向镜像（RX）：对一个端口或VLAN做接收方向的镜像，在系统对这些报文做任何修改和处理之前，将这个端口或VLAN上的收到的流量尽可能完整、真实地复制出来。
  对于镜像源端口来说，存在一定限制：无法通过镜像复制CRC错误的报文；对于镜像源VLAN来说，也有一定的限制：BPDU、LACPDU、BMGPDU报文、IP-MAC绑定检查不通过的报文以及CRC错误的报文，不能被镜像复制。复制到目的端口的报文，应该和镜像源收到的报文完全一致。
- 发送方向镜像（TX）：对一个端口或VLAN做发送方向的镜像，尽可能真实地将这个端口或VLAN上的发送出去的流量复制出来。从端口或VLAN送出之前就被丢弃的报文，不会被镜像复制。当镜像源为VLAN时，来自CPU的报文不能被镜像复制。
- 双向镜像（BOTH）：在一个镜像会话中，用户可以监控同一个镜像源上接收和发送两个方向的报文流量。

3. 镜像源

源端口（也称为被监测端口）是一个需要被监控或分析的二层或三层端口。源 VLAN（也称为被监测 VLAN）是一个需要被监控或分析的 VLAN。在一个镜像会话中，用户可以监控一个或多个镜像源上接收（RX）、发送（TX）、或双向的流量。系统支持任意多个镜像源端口（等同于系统最多可用端口数）和任意多个镜像源 VLAN（等同于系统最多可用 VLAN 数）。

源端口特性如下：

- 可以是任何端口类型（例如，以太网端口）
- 只能在一个镜像会话中被监视
- 不能为一个镜像会话的目的端口

每个镜像源端口或镜像源 VLAN 可以配置不同的方向（入口、出口或双向）来监视。对于端口聚合组，监控方向适用于该组中的所有物理端口。

需要注意以下三点内容：

- 镜像源端口可以在相同或不同的 VLAN 中。
- 要配置镜像源 VLAN，必须先创建 VLAN 接口。
- 聚合组的成员端口不能单独配置成镜像源。

4. 目的端口

每个镜像会话必须有一个目的端口（也称为监测端口），接收镜像功能复制出来的报文。目的端口特性如下：

- 必须和镜像源处在同一台设备上。
- 可以是任何物理端口。
- 聚合组的成员端口不能配置为镜像目的端口。
- 只能在一个镜像会话中作为目的端口。
- 不能配置为任何镜像会话的镜像源端口。
- 端口不能传输任何镜像功能以外的流量。
- 当镜像会话在执行时，该端口不能使用 STP。
- 该端口的所有其他系统功能的相关配置继续保留，但是不能工作。直到此端口不再作为镜像会话的目的端口。
- 镜像目的端口不学习 MAC。
- 实时速率/双工状态可能会和显示的数值不一致。

3.1.2 镜像类型

根据源端口与目地端口所处的位置（是否处于一台设备上），镜像可分为本地镜像与远程镜像：

- 本地镜像：源端口与目标端口处在同一台设备上，实现源端口数据报文到目标端口的镜像，连接在目标端口上的监控设备对经过源端口的数据报文进行监控分析。
- 远程镜像：源端口与目标端口处在不同的设备上通过二层网络连接，源端口将报文发送到目的端口后，由目的端口发送报文到监控设备，实现跨设备的数据报文分析。

3.2 配置镜像源

3.2.1 配置镜像源端口

镜像源端口可以是物理端口，也可以是聚合端口。

表3-1 配置镜像源端口

命令	操作	说明
configure terminal	进入全局配置模式	-
monitor session *session-id* **source interface** *if-name* [**both** | **tx** |**rx**]	配置镜像源端口	session-id: 镜像会话编号，取值范围为 1~3

命令	操作	说明
		如果没有指明方向（双向、发送、接收），那么默认为双向

3.2.2 配置镜像源 VLAN

配置镜像源 VLAN 之前，必须先在“vlan database”模式下创建 VLAN，且在全局创建 VLAN 接口。下表 3-2 仅显示该命令功能及参数解释。详细的配置步骤可参见 3.6.1 配置本地镜像示例。

表3-2 配置镜像源VLAN

命令	操作	说明
configure terminal	进入全局配置模式	-
monitor session *session-id* **source vlan** *vlan-id* [**both** | **tx** |**rx**]	配置镜像源 VLAN	session-id: 镜像会话编号，取值范围为 1~3 vlan-id: 镜像源 VLAN，取值范围为 1~4094 如果没有指明方向（双向、发送、接收），那么默认为双向

3.2.3 配置镜像源 CPU

表3-3 配置镜像源CPU

命令	操作	说明
configure terminal	进入全局配置模式	-
monitor session *session-id* **source cpu** [**both** | **tx** |**rx**]	配置镜像源 VLAN	session-id: 镜像会话编号，有效值为 1，只支持在 session 1 上配置； 如果没有指明方向（双向、发送、接收），那么默认为双向

3.3 配置镜像目的

3.3.1 配置镜像目的端口

镜像目的端口只能是物理端口，不能为 VLAN 端口或者聚合端口。同一个镜像会话只能有一个镜像目的，不能同时配置本地镜像目的端口和远程镜像目的 VLAN。

表3-4 配置镜像目的端口

命令	操作	说明
configure terminal	进入全局配置模式	-
monitor session *session-id* **destination interface** *if-name*	配置镜像目的端口	session-id: 镜像会话编号，取值范围为 1~3

3.3.2 配置镜像目的为 CPU

表 3-5 配置镜像目的为 CPU

命令	操作	说明
configure terminal	进入全局配置模式	-
monitor session *session-id* **destination cpu**	配置镜像目的为 CPU	session-id: 镜像会话编号，取值范围为 1~3

说明

配置镜像 CPU 的目的端口与镜像源后，还可在全局配置模式下配置以下命令：

1.使用 **monitor cpu set packet buffer** *number* 命令配置镜像 CPU 的报文存储空间大小；

2.使用 **cpu-traffic-limit reason mirror-to-cpu rate** *rate-value* 与 **cpu-traffic-limit reason mirror-to-cpu class** *class-value* 命令，配置镜像报文的速率和优先级；

3.使用 **monitor cpu capture strategy** { **replace** | **drop** }命令，配置镜像 CPU 的抓包策略。

3.3.3 创建镜像目的端口组

只有一个镜像会话可以配置为镜像目的端口组，一个目的端口组可以配置多个镜像目的端口。

表 3-6 创建镜像目的端口组

命令	操作	说明
configure terminal	进入全局配置模式	-
monitor session *session-id* **destination group** *group-id*	创建镜像目的端口组	session-id: 镜像会话编号，取值范围为 1~3 group-id: 镜像目的端口组编号，取值范围为 1~32

3.3.4 配置接口加入目的端口组

创建目的端口组后，可以配置镜像目的组的目的端口，在配置多目的端口镜像时会使用该命令，详细配置请参见3.6.2 配置多目的端口镜像示例。

表 3-7 配置接口加入目的端口组

命令	操作	说明
configure terminal	进入全局配置模式	-
monitor session *session-id* **destination group** *group-id*	创建镜像目的端口组	session-id: 镜像会话编号，取值范围为 1~3 group-id: 镜像目的端口组编号，取值范围为 1~32
member *if-name*	配置接口加入目的端口组，成为目的端口组的成员	if-name: 镜像目的端口组成员端口

3.4 配置远程镜像

3.4.4 配置远程镜像的目的 VLAN 与出端口

在配置远程端口镜像目的 VLAN 之前，必须先在"vlan database"中配置该 VLAN，且出端口只能是物理端口。为了防止出端口中出现泛洪的报文，影响观察结果，可以将默认 VLAN 移出该端口。下表仅介绍命令功能与参数解释，远程镜像的详细配置请参见 3.6.3 配置远程镜像示例。

表 3-8 配置目的 VLAN 与出端口

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

命令	操作	说明
monitor session *session-id* **destination remote vlan** *vlan-id* **interface** *if-name*	创建远程镜像的目的VLAN与出端口	session-id: 镜像会话编号，取值范围为1~3 vlan-id: 远程端口镜像的目的VLAN，有效范围2-4094 if-name: 镜像报文的出端口

3.4.5 配置 MAC Escape 功能

MAC Escape 表项只对远程镜像有效，不影响本地镜像。配置了 MAC Escape 表项以后，报文的目的地址匹配到表项时，就不会被远程镜像复制。

全局最多支持两个表项。删除的时候如果不指定 MAC 地址和 MAC 地址掩码，将会删除所有表项。

表 3-9 配置 MAC Escape 功能

命令	操作	说明
configure terminal	进入全局配置模式	-
monitor mac escape *mac-address mask-address*	创建远程镜像的 MAC Escape 功能	mac-address: MAC 地址，格式为 HHHH. HHHH. HHHH mask-address: MAC 地址掩码，格式为 HHHH. HHHH. HHHH

3.5 显示与维护

表 3-10 显示与维护

命令	操作	说明
show monitor [**session** *session-id*]	显示镜像的相关配置信息	session-id: 镜像会话编号，取值范围为1~3； 如果不指定镜像会话号，所有表项都会被显示
show monitor mac escape	显示远程镜像 MAC Escape 的表项	-

命令	操作	说明
show monitor cpu packet { **all** | *packet-id* }	显示镜像 CPU 内存中存储的报文	packet-id: 显示指定报文 ID 的信息
show monitor cpu packet buffer-size	显示镜像 CPU 当前申请的内存空间大小	-
show monitor cpu capture strategy	显示镜像 CPU 当前的抓包策略	-
clear monitor cpu packet all	清除镜像 CPU 内存中存储的报文	-

3.6 配置举例

3.6.1 配置本地镜像示例

i. 配置步骤

命令举例	操作步骤
Switch #configure terminal	进入全局配置模式
Switch(config)# vlan database	进入 VLAN 配置模式
Switch(config-vlan)# vlan 10	创建 VLAN
Switch(config-vlan)# exit	退出 VLAN 配置模式
Switch(config)# interface vlan10	创建 VLAN 接口
Switch(config-if)# exit	退出 VLAN 接口配置模式
Switch(config)# interface eth-0-2	进入接口配置模式
Switch(config-if)# no shutdown	端口 UP
Switch(config-if)# exit	退出接口配置模式
Switch(config)# monitor session 1 destination interface eth-0-2	指定镜像会话的目的端口
Switch(config)# monitor session 1 source interface eth-0-1 both	指定镜像会话、源端口和监控方向
Switch(config)# monitor session 1 source vlan 10	指定镜像会话和源 VLAN

命令举例	操作步骤
rx	
Switch(config)# end	退出全局配置模式

ii. 命令验证

上述表格中创建了会话 1，用来监控源端口和源 VLAN 的流量。显示镜像会话的相关配置信息：

```
Switch # show monitor session 1

Session     1
---------
Status                  :   Valid
Type                    :   Local Session
Source Ports        :
   Receive Only      :
   Transmit Only     :
   Both                 : eth-0-1
Source VLANs         :
   Receive Only      : 10
   Transmit Only     :
   Both                 :
Destination Port    : eth-0-2
```

3.6.2 配置多目的端口镜像示例

i. 配置步骤

命令举例	操作步骤
Switch #configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# no shutdown	端口 UP
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface eth-0-2	进入接口配置模式
Switch(config-if)# no shutdown	端口 UP
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface eth-0-3	进入接口配置模式

命令举例	操作步骤
Switch(config-if)# no shutdown	端口 UP
Switch(config-if)# exit	退出接口配置模式
Switch(config)# monitor session 1 destination group 1	创建镜像会话的目的端口组
Switch(config-monitor-d-group)# member eth-0-2	将接口 eth-0-2 加入目的端口组
Switch(config-monitor-d-group)# member eth-0-3	将接口 eth-0-3 加入目的端口组
Switch(config)# monitor session 1 source interface eth-0-1	指定镜像会话、源端口和监控方向
Switch(config)# end	退出全局配置模式

ii. 命令验证

上述表格创建了会话 1 用以监控源端口流量。显示镜像会话的相关配置信息：

```
Switch # show monitor session 1

Session     1
---------
Status                  :   Valid
Type                    :   Local Session
Source Ports        :
   Receive Only     :
   Transmit Only    :
   Both             : eth-0-1
Source VLANs        :
   Receive Only     :
   Transmit Only    :
   Both             :
Destination Port    : eth-0-2 eth-0-3
```

3.6.3 配置远程镜像示例

1. 配置远程镜像

i. 远程镜像会话简介

远程镜像会话是一组镜像源和一个远程镜像目的的集合，其中远程镜像目的包括一个物理出接口以及一个 VLAN。

在远程镜像源会话中，源端口和 VLAN 的概念和本地镜像一样。

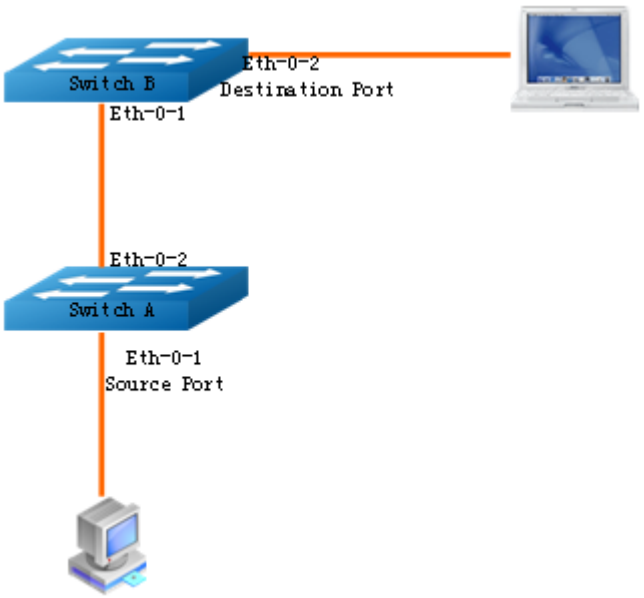
一个远程镜像目的特性如下：

- 是一个指定的端口和一个 VLAN 的组合。
- 远程 VLAN 范围为 2~4094，如果在系统中没有创建 VLAN，用户不能将这个 VLAN 作为远程镜像 VLAN。
- 出端口是一个普通的物理端口，需要用户的配置来保证这个端口可以传输镜像报文，并且不受其他功能的流量所干扰。
- 镜像源的报文将被加上指定的远程 VLAN ID Tag，然后从指定的出接口发出去，到达远端设备。
- 建议使用二层接口为远程镜像的目的端口，并且用户需要将这个端口加入到指定的远程 VLAN 中，否则无法成功发送镜像报文。

ii. 拓扑

如下图 3-1，镜像源端口在 Switch A 上，不同的镜像会话通过将镜像复制的报文封装在指定的 VLAN 中，通过网络传递到远端设备 Switch B。

图 3-1 远程镜像拓扑图



iii. 配置方法

Switch A：

命令举例	操作步骤
SwitchA# configure terminal	进入全局配置模式
SwitchA(config)# vlan database	进入 VLAN 配置模式
SwitchA(config-vlan)# vlan 10	创建 VLAN 10
SwitchA(config-vlan)# vlan 15	创建 VLAN 15
SwitchA(config-vlan)# exit	退出 VLAN 配置模式
SwitchA(config-if)# exit	退出接口配置模式
SwitchA(config)# interface eth-0-2	进入接口配置模式
SwitchA(config-if)# no shutdown	端口 UP
SwitchA(config-if)# switchport mode trunk	端口模式为 Trunk
SwitchA(config-if)# switchport trunk allowed vlan add 15	添加 eth-0-2 到 VLAN 15
SwitchA(config-if)# exit	退出接口配置模式
SwitchA(config)# interface eth-0-1	进入接口配置模式
SwitchA(config-if)# switchport mode access	端口模式为 Access
SwitchA(config-if)# switchport access vlan 10	添加 eth-0-1 到 VLAN 10
SwitchA(config)# monitor session 1 destination remote vlan 15 interface eth-0-2	指定镜像会话、远程目的 VLAN 和出端口
SwitchA(config)# monitor session 1 source interface eth-0-1 both	指定镜像会话和源端口（镜像端口）
SwitchA(config)# end	退出 EXEC 模式

Switch B：

方法一：使用 **monitor session** *session-id* **source vlan** *vlan-id* 命令得到一份远程镜像报文的拷贝，报文是加标签的。

命令举例	操作步骤
SwitchB# configure terminal	进入全局配置模式
SwitchB(config)# vlan database	进入 VLAN 配置模式
SwitchB(config-vlan)# vlan 15	创建 VLAN 15
SwitchB(config-vlan)# exit	退出 VLAN 配置模式
SwitchB(config)# interface vlan15	进入 VLAN 配置模式
SwitchB(config-if)# exit	退出 VLAN 配置模式
SwitchB(config)# interface eth-0-2	进入接口配置模式
SwitchB(config-if)# no shutdown	端口 UP
SwitchB(config-if)# switchport mode access	端口模式为 Access
SwitchB(config-if)# switchport access vlan 15	添加 eth-0-2 到 VLAN 15
SwitchB(config)# interface eth-0-1	进入接口配置模式
SwitchB(config-if)# no shutdown	端口 UP
SwitchB(config-if)# switchport mode trunk	端口模式为 Trunk
SwitchB(config-if)# switchport trunk allowed vlan add 15	添加 eth-0-1 到 VLAN 15
SwitchB(config-if)# exit	退出接口配置模式
SwitchB(config)# monitor session 1 destination interface eth-0-2	指定镜像会话和目的地址
SwitchB(config)# monitor session 1 source vlan 15 rx	指定镜像会话和源 VLAN
SwitchB(config)# end	退出 EXEC 模式

方法二：使用 Access 端口获取目的报文（在 Switch B 不需要配置任何镜像会话）

命令举例	操作步骤
SwitchB# configure terminal	进入全局配置模式
SwitchB(config)# no spanning-tree enable	禁止 STP
SwitchB(config)# vlan database	进入 VLAN 配置模式
SwitchB(config-vlan)# vlan 15	创建 VLAN 15

命令举例	操作步骤
SwitchB(config-vlan)# exit	退出 VLAN 配置模式
SwitchB(config)# interface eth-0-2	进入接口配置模式
SwitchB(config-if)# no shutdown	端口 up
SwitchB(config-if)# switchport mode access	端口模式为 Access
SwitchB(config-if)# switchport access vlan 15	添加 eth-0-2 到 VLAN 15
SwitchB(config)# interface eth-0-1	进入接口配置模式
SwitchB(config-if)# no shutdown	端口 UP
SwitchB(config-if)# switchport mode trunk	端口模式为 Trunk
SwitchB(config-if)# switchport trunk allowed vlan add 15	添加 eth-0-1 到 VLAN 15
SwitchB(config-if)# exit	退出接口配置模式

方法三：使用 Trunk 端口获取目的报文（在 Switch B 不需要配置任何镜像会话）

命令举例	操作步骤
SwitchB# configure terminal	进入全局配置模式
SwitchB(config)# no spanning-tree enable	禁止 STP
SwitchB(config)# vlan database	进入 VLAN 配置模式
SwitchB(config-vlan)# vlan 15	创建 VLAN 15
SwitchB(config-vlan)# exit	退出 VLAN 配置模式
SwitchB(config)# interface eth-0-2	进入接口配置模式
SwitchB(config-if)# no shutdown	端口 UP
SwitchB(config-if)# switchport mode trunk	端口模式为 Trunk
SwitchB(config-if)# switchport trunk allowed vlan add 15	添加 eth-0-2 到 VLAN 15
SwitchB(config)# interface eth-0-1	进入接口配置模式
SwitchB(config-if)# no shutdown	端口 UP
SwitchB(config-if)# switchport mode trunk	端口模式为 Trunk

命令举例	操作步骤
SwitchB(config-if)# switchport trunk allowed vlan add 15	添加 eth-0-1 到 VLAN 15
SwitchB(config-if)# exit	退出接口配置模式

说明

如果使用方法二和方法三，系统会学习镜像报文的 MAC，有可能导致 FDB 表资源耗尽。

iv. 命令验证

方法一中创建了会话 1，用以监控源端口和源 VLAN 的流量。查看镜像的相关配置信息：

```
SwitchA# show monitor session 1

Session     1
----------
Status                  : Valid
Type                      :   Remote Session
Source Ports          :
   Receive Only       :
   Transmit Only      :
   Both                    : eth-0-1
Source VLANs          :
   Receive Only       :
   Transmit Only      :
   Both                    :
Destination Port     : eth-0-2
Destination remote VLAN : 15
SwitchB# show monitor session 1
Session     1
----------
Status                  : Valid
Type                      :   Local Session
Source Ports          :
   Receive Only       :
   Transmit Only      :
   Both                    :
Source VLANs          :
   Receive Only       : 15
   Transmit Only      :
   Both                    :
```

```
Destination Port     : eth-0-2
```

2. 配置MAC Escape远程镜像

i. 简介

MAC Escape 是远程镜像的子功能，它只会影响远程镜像的结果。一个 MAC Escape 条目包括一个 MAC 地址和一个 MAC 掩码。创建 MAC Escape 条目后，MAC-DA 报文相匹配的条目不会镜像到远程目的 VLAN。用户可以通过 MAC Escape 条目防止协议报文镜像到达远端。全局最多可配置两个 MAC Escape 条目。

ii. 配置方法

命令举例	操作步骤
SwitchA# configure terminal	进入全局配置模式
SwitchA(config)# monitor mac escape 00cc.12A9.33D8 ffff.ffff.ffff	创建 MAC Escape 条目
SwitchA(config)# monitor mac escape 00cc.159E.24F0 ffff.ffff.ffff	创建另一个 MAC Escape 条目
SwitchA(config)# end	退出全局配置模式

iii. 命令验证

显示远程镜像 MAC Escape 的表项：

```
SwitchA# show monitor mac escape

-------------------------------------------------------------
                  monitor rspan mac escape database
-------------------------------------------------------------
count     : 2
-------------------------------------------------------------
  Mac         : 00:cc:12:a9:33:d8
  Mask        : ff:ff:ff:ff:ff:ff
  Mac         : 00:cc:15:9e:24:f0
  Mask        : ff:ff:ff:ff:ff:ff
```

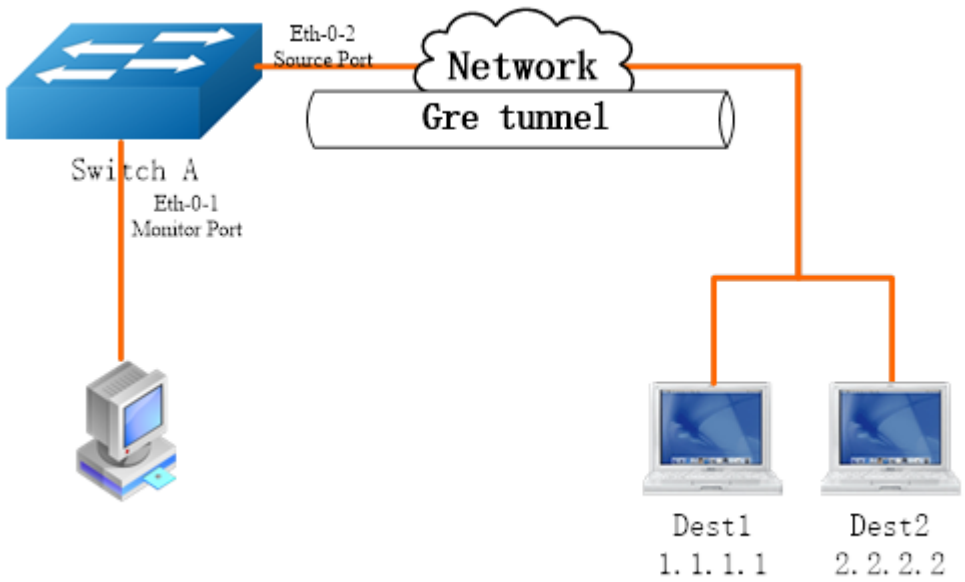
3. 配置ERSPAN远程镜像

i. 简介

在处理一些数据时，需要将交换机上某些端口收发的数据通过三层网络发送给远端的分析仪进行分析。ERSPAN 可以通过 GRE 通道将数据添加 GRE 头部信息后发送给分析仪，监控的过程中不影响数据的正常传输。如果发送的数据很多，ERSPAN 为了降低负载，可以设置将报文负载分担到多个目的分析设备，如图 3-2 所示。

ii. 拓扑

图 3-2 ERSPAN 远程镜像拓扑图



iii. 配置方法

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)#no shutdown	端口 UP
Switch(config-if)#exit	退出接口配置模式
Switch(config)#interface eth-0-2	进入接口配置模式
Switch(config-if)#no switchport	端口模式为 Trunk
Switch(config-if)# ip address 10.10.10.1/24	配置端口 IP 地址

命令举例	操作步骤
Switch(config-if)#no shutdown	端口 UP
Switch(config-if)#exit	退出接口配置模式
Switch(config)# interface tunnel1	创建 Tunnel 1 并进入其配置模式
Switch(config-if)# tunnel source eth-0-2	指定 Tunnel 源端口
Switch(config-if)# tunnel multi-destination 1.1.1.1	指定 Tunnel 目的 IP 地址 1
Switch(config-if)# tunnel multi-destination 2.2.2.2	指定 Tunnel 目的 IP 地址 2
Switch(config-if)# tunnel gre key 3333	设定 gre key
Switch(config-if)#exit	退出 Tunnel 1 配置模式
Switch(config)# arp 10.10.10.2 0000.0000.0001	配置 ARP 信息
Switch(config)# arp 11.11.11.2 0000.0000.0002	配置 ARP 信息
Switch(config)# ip route 1.1.1.0/24 10.10.10.2	配置路由信息
Switch(config)# ip route 2.2.2.0/24 10.10.10.2	配置路由信息
Switch(config)# monitor session 1 destination interface tunnel1	指定镜像会话的目的端口
Switch(config)# monitor session 1 source interface eth-0-1 both	指定镜像会话的源端口
Switch(config)# end	退出全局配置模式

iv. 命令验证

显示上述配置的结果：

```
SwitchA# show monitor session 1
Session      1
---------
Status                  : Valid
Type                    : Local Session
Source Ports            :
   Receive Only         :
   Transmit Only        :
   Both                 : eth-0-1
Source VLANs            :
   Receive Only         :
```

```
    Transmit Only       :
    Both                :
Destination Port      : tunnel1
SwitchA# show running-config interface tunnel 1
Building configuration...
!
interface tunnel1
  tunnel source eth-0-2
  tunnel multi-destination 1.1.1.1
  tunnel multi-destination 2.2.2.2
  tunnel gre key 3333
!
```

3.6.4 配置 CPU 镜像示例

1. 配置CPU为镜像目的端口

i. 简介

用户可以将某一端口或某一 VLAN 收、发的报文复制一份，从设备的另一个端口上发送出去。接着在这个端口连上测试仪或其他报文收集设备，可达到对原始报文进行捕获和分析的目的。当该端口无法连接测试仪或其他报文收集设备，或者设备资源紧张时，需要将被复制报文发送到 CPU 并被保存下来，便于用户或程序员快速分析报文。将报文复制一份送到 CPU 可以解决硬件资源紧张的问题。目前镜像报文上送 CPU 的速率是系统默认限制速率，也可以由用户指定限制速率。

ii. 配置方法

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# monitor session 1 destination cpu	配置 CPU 为 session 1 镜像目的端口
Switch(config)# monitor session 1 source interface eth-0-1 both	配置 eth-0-1 为 session 1 的镜像源，方向为 both
Switch(config)# monitor cpu set packet buffer 100	配置 mirror cpu 的内存存储空间大小，最多为 100 个数据包
Switch(config)# cpu-traffic-limit reason mirror-to-cpu rate 128	配置 mirror 到 cpu 的包的速率为 128pps
Switch# exit	退出全局配置模式

配置 mirror cpu 的抓包策略为 drop，其中 replace 为默认值。

命令举例	操作步骤
Switch(config)# monitor cpu capture strategy drop	配置 mirror cpu 的抓包策略为 drop (当内存空间写满之后，丢弃新的数据包)
Switch(config)# monitor cpu capture strategy replace	配置 mirror cpu 的抓包策略为 replace (当内存空间写满之后，新的数据包替换最旧的数据包)

iii. 命令验证

1. 示例中创建了会话 1 用以监控源端口 eth-0-1 的流量，并通过 **show** 命令查看镜像至 CPU 的报文。可以使用显示会话命令查看配置信息：

```
Switch# show monitor session 1
DUT1# show monitor session 1
Session      1
----------
Status                    : Valid
Type                      : Cpu Session
Source Ports              :
   Receive Only           :
   Transmit Only          :
   Both                   : eth-0-1
Source VLANs              :
   Receive Only           :
   Transmit Only          :
   Both                   :
Destination Port      : cpu
```

2. 查看报文镜像到 CPU 后内存存储的数据包：

```
Switch# show monitor cpu packet all
-----------------show all mirror to cpu packet info-----------------
packet: 1
Source port: eth-0-1
MACDA:264e.ad52.d800, MACSA:0000.0000.1111
vlan tag:100
IPv4 Packet, IP Protocol is 0
IPDA:3.3.3.3, IPSA: 10.0.0.2
Data length: 47
Data:
  264e ad52 d800 0000 0000 1111 8100 0064
  0800 4500 001d 0001 0000 4000 6ad9 0a00
```

```
0002 0303 0303 6365 6e74 6563 796f    75
```

3. 查看配置 mirror cpu 内存 buffer 大小

```
Switch# show monitor cpu packet buffer
----------------------show packet buffer size ----------------------
The mirror-to-cpu packet buffer size of user set is: 100
```

4. 查看配置 mirror cpu 的报文上 CPU 的速率

```
Switch# show cpu traffic-limit | include mirror-to-cpu
mirror-to-cpu                    128                0
```

5. 查看 mirror cpu 报文的存储文件

```
Switch# ls flash:/mirror
Directory of flash:/mirror

total 8
-rw-r-----    1 2287 Dec 23 01:16 MirCpuPkt-2016-12-23-01-15-54.txt
-rw-r-----    1 2568 Jan    3 11:41 MirCpuPkt-2017-01-03-11-41-33.txt
14.8T bytes total (7.9T bytes free)
DUT1# more flash:/mirror/ MirCpuPkt-2017-01-03-11-41-33.txt
sequence    srcPort
1                eth-0-1
++++++++1483443444:648884
8c 1d cd 93 51 00 00 00 00 00 11 11 08 00 45 00
00 26 00 01 00 00 40 00 72 d0 01 01 01 01 03 03
03 03 63 65 6e 74 65 63 79 6f 75 63 65 6e 74 65
63 79 6f 75
--------
sequence    srcPort
2                eth-0-1
++++++++1483443445:546440
8c 1d cd 93 51 00 00 00 00 00 11 11 08 00 45 00
00 26 00 01 00 00 40 00 72 d0 01 01 01 01 03 03
03 03 63 65 6e 74 65 63 79 6f 75 63 65 6e 74 65
63 79 6f 75
```

6. 在转换成 pcap 文件后，可以通过 wireshark 打开

```
Switch#ls flash:/mirror
Directory of flash:/mirror
```

```
total 12
-rw-r-----    1 2287 Dec 23 01:16 MirCpuPkt-2016-12-23-01-15-54.txt
-rw-r-----    1 2568 Jan    3 11:41 MirCpuPkt-2017-01-03-11-41-33.txt
-rw-r--r--    1    704 Jan    3 13:07 test.pcap
14.8T bytes total (7.9T bytes free)
```

7. 查看 mirror cpu 的抓包策略

```
Switch# show monitor cpu capture strategy
The capture strategy of cpu mirror is: replace (add new packet and remove oldest
  packet when buffer is full)
```

2. 配置CPU为镜像源

i. 简介

用户可以将 CPU 作为镜像源配置，包含 ingress、egress 以及 both 三种方向。当需要将上报 CPU 报文或者将 CPU 下发的报文通过镜像复制某一个端口时，可以启用 CPU 镜像源配置，值得注意的是镜像复制出来的是 **cpu-traffic-limit** 限速之前的报文。目前只允许 session 1 配置 CPU 镜像源。

ii. 配置方法

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# monitor session 1 source cpu both	配置 CPU 为 session 1 镜像源，方向为 both
Switch(config)# monitor session 1 destination interface eth-0-1	配置物理口 eth-0-1 为 session 1 的镜像目的端口
Switch# exit	退出全局配置模式

iii. 命令验证

显示上述步骤的配置结果：

```
Switch# show monitor session 1
Session      1
----------
```

```
Status                  : Valid
Type                    : Cpu Session
Source Ports            :
   Receive Only         :
   Transmit Only        :
   Both                 : cpu
Source VLANs            :
   Receive Only         :
   Transmit Only        :
   Both                 :
Destination Port        : eth-0-1
```

4 设备管理配置

4.1 设备管理简介

用户可以通过管理端口的方式管理交换机，交换机有以太网口和串口两类管理端口（该部分可参见“登录设备方式介绍”章节）。通过设备管理功能，可以对交换机的温度、风扇、电源、光模块等进行管理。

4.2 配置温度管理

4.2.1 配置步骤

交换机支持温度告警管理功能。用户可以设置 3 个温度阀值：低温告警阀值，高温告警阀值，超高温断电保护阀值。当交换机温度低于低温告警阀值，或者高于高温告警阀值时，交换机将自动产生告警信息。当交换机温度高于超高温断电保护阀值，交换机将通过自动切断电源来保护系统。

表 4-1 配置温度管理

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	
Switch(config)# temperature 5 70 90	配置系统温度阈值	low: 低温温度的取值范围为 0~50 high: 高温温度的取值范围为 50~85 critical: 高危温度的取值范围为 55~90 缺省情况下，低温温度为 5，高温温度为 75，高危温度为 90，单位：摄氏度
Switch(config)#exit	退出全局配置模式	-

4.2.2 命令验证

表 4-2 显示硬件环境信息

命令	操作	说明
show environment [**slot** *slot-id*]	显示硬件环境信息	slot-id: 堆叠情况下的槽位号，非堆叠情况下不支持 slot-id

根据上述步骤，验证结果如下：

```
Switch# show environment

-------------------------------------------------------
Sensor status (Degree Centigrade):
Index Temperature    Lower_alarm    Upper_alarm Critical_limit
1        50                  5                  70                 90
```

4.3 配置风扇管理

交换机支持自动管理风扇。当风扇盘不在位或者风扇故障时，交换机会自动产生告警信息。如果风扇盘支持风扇速度调节，交换机将根据系统内部的实时温度值自动调节风扇转速。交换机风扇速度调节也有3 个温度阀值：Tlow=50 度, Thigh=65 度, Tcrit=80 度。当实时温度<Tlow 时，风扇将停止转动；当 Tlow<=实时温度<Thigh 时，风扇将以 30%的速率转动；当 Thigh<=实时温度<Tcrit 时，风扇将以 70%的速率转动；当 Tcrit<=实时温度时，风扇将全速转动。并且这里风扇自动调节还支持温度迟滞 Thyst=2 度。当之前的温度高于某阀值，风扇转速会上升一个级别；当温度又下降到低于该阀值时，风扇转速不会立即下降一个级别，必须等到实时温度比 Thigh-Thyst 的值还低时，才会调节风扇转速，下降一个级别。举例如下：

当前温度为 58 摄氏度，风扇转速为 30%；(Tlow<58<Thigh)。

当温度上升到 65 摄氏度时，风扇转速自动调节为 70%；（Thigh==65)

当温度又下降到 63 摄氏度时，风扇转速仍旧为 70%；(Thigh-Thyst ==63)

当温度下降到 62 摄氏度时，风扇转速降为 3%；(62<Thigh-Thyst)

说明

Tlow、Thigh、Tcrit 和 Thyst 以及对应的风扇转速都是系统预定义的，不支持用户调节。

虽然不支持用户调节，但可以使用 **show environment** 命令查看风扇状态：

```
Switch# show environment

Fan tray status:
Index       Status
1           PRESENT
FanIndex    Status SpeedRate Mode
1-1         OK     30%       Auto
1-2         OK     30%       Auto
1-3         OK     30%       Auto
1-4         OK     30%       Auto
-------------------------------------------------------
```

4.4 配置电源管理

交换机支持自动电源管理。当某个电源坏掉（双电源模式时）或者电源风扇坏掉，交换机能够自动发出告警信息。当电源模块拔插时，交换机也会发出通告信息。

同样地，用户可以通过命令行指令来查看电源的运行状态：

```
Switch# show environment

-------------------------------------------------------
Power status:
Index     Status     Power     Type       Fans     Control
1         PRESENT    OK        AC         -        -
2         ABSENT     -         -          -        -
3         PRESENT    OK        DC(PoE)    -        -
-------------------------------------------------------
```

4.5 配置光模块

交换机支持管理光模块信息，这些管理信息包括基本信息和诊断信息。其中基本信息包括光模块类型、生产厂商名称、序列号、产品号以及相应支持的光波长和链路长度。诊断信息包括光模块的实时温度、

电压、电流、发送光功率和接收光功率，以及这些实时信息对应的厂商预定义正常工作范围、提醒阀值和告警阀值。当光模块拔插或者实时信息超出正常工作范围，交换机将自动发出通告或告警信息。

表 4-3 显示光模块收发器信息

命令	操作	说明
show transceiver [**detail**]	显示光模块收发器信息	detail: 显示包括 DDM 信息在内的详细信息

用户可以通过命令行指令来查看电源的运行状态：

```
Switch# show transceiver detail
Port eth-1-2 transceiver info:
Transceiver Type: 10G Base-SR
Transceiver Vendor Name : OEM
Transceiver PN                : SFP-10GB-SR
Transceiver S/N               : 201033PST1077C
Transceiver Output Wavelength: 850 nm
Supported Link Type and Length:
        Link Length for 50/125um multi-mode fiber: 80 m
        Link Length for 62.5/125um multi-mode fiber: 30 m
--------------------------------------------------------------------------------
Transceiver is internally calibrated.
mA: milliamperes, dBm: decibels (milliwatts), NA or N/A: not applicable.
++ : high alarm, +   : high warning, -   : low warning, -- : low alarm.
The threshold values are calibrated.
--------------------------------------------------------------------------------
                    High Alarm      High Warn      Low Warn       Low Alarm
Temperature      Threshold       Threshold       Threshold       Threshold
Port   (Celsius)          (Celsius)       (Celsius)       (Celsius)          (Celsius)
--------- ------------------   ----------   ----------   ----------   ----------
eth-1-2   25.92            95.00             90.00          -20.00            -25.00
```

```
-------------------------------------------------------------------------------------------
                                 High Alarm    High Warn     Low Warn      Low Alarm
          Voltage                Threshold     Threshold     Threshold     Threshold
Port      (Volts)                (Volts)       (Volts)       (Volts)       (Volts)
--------- ---------------------- ------------- ------------- ------------- -------------
eth-1-2   3.32                   3.80          3.70          2.90          2.80
-------------------------------------------------------------------------------------------
                                 High Alarm    High Warn     Low Warn      Low Alarm
          Current                Threshold     Threshold     Threshold     Threshold
Port      (milliamperes)         (mA)          (mA)          (mA)          (mA)
--------- ---------------------- ------------- ------------- ------------- -------------
eth-1-2   6.41                   20.00         18.00         1.00          0.50
-------------------------------------------------------------------------------------------
          Optical                High Alarm    High Warn     Low Warn      Low Alarm
          Transmit Power         Threshold     Threshold     Threshold     Threshold
Port      (dBm)                  (dBm)         (dBm)         (dBm)         (dBm)
--------- ---------------------- ------------- ------------- ------------- -------------
eth-1-2   -2.41                  2.01          1.00          -6.99         -7.96
-------------------------------------------------------------------------------------------
          Optical                High Alarm    High Warn     Low Warn      Low Alarm
          Receive Power          Threshold     Threshold     Threshold     Threshold
Port      (dBm)                  (dBm)         (dBm)         (dBm)         (dBm)
--------- ---------------------- ------------- ------------- ------------- -------------
eth-1-2   -12                -   1.00          0.00          -19.00        -20.00
-------------------------------------------------------------------------------------------
```

4.6 配置程序升级

4.6.1 升级 BootROM 程序

交换机支持在线升级 BootROM 程序，升级完成后，必须重启后才能生效。更多关于 BootROM 的介绍，请参考 5 Route-map 配置。

i. 配置步骤

命令举例	操作步骤
Switch# copy mgmt-if tftp://10.10.29.160/ bootrom.bin flash:/boot/	从 TFTP 服务器拷贝 BootROM 程序到本地 Flash 存储介质上
Switch# configure terminal	进入全局配置模式
Switch(config)# update bootrom flash:/boot/bootrom.bin	升级指定的 BootROM 程序
Switch(config)# exit	退出全局配置模式
Switch# reboot	重启系统

ii. 命令验证

完成上述配置且重启系统后，可查看系统当前运行的 BootROM 版本号：

```
Switch# show version
……
EPLD Version is 1
BootRom Version is 3.0.2
```

4.6.2 升级 EPLD 程序

交换机支持在线升级 EPLD 程序，当升级完成后，必须断电重启系统，否则系统将无法正常工作。

i. 配置步骤

命令举例	操作步骤
Switch# copy mgmt-if tftp://10.10.29.160/ vme_v1.0 flash:/boot/ vme_v1.0	从 TFTP 服务器拷贝 EPLD 程序到本地 flash 存储介质上
Switch# configure terminal	进入全局配置模式
Switch(config)# update epld flash:/boot/ vme_v1.0	升级指定 EPLD 程序

命令举例	操作步骤
Switch(config)# exit	退出全局配置模式
Switch# reboot	重启系统

ii. 命令验证

完成上述配置且重启系统后，可查看系统当前运行的 EPLD 版本号：

```
Switch# show version

……
EPLD Version is 1
BootRom Version is 3.0.2
```

4.7 显示设备重启记录

4.7.1 简介

Centec 交换机支持显示重启记录，从重启记录可以判断板子的重启类型，如掉电重启、手动重启、或者是其他原因导致的重启。用户也可以通过命令来清除重启记录。

4.7.2 重启类型与说明

重启记录的说明如下表所示：

表4-4 重启类型与说明

重启类型	说明
POWER	断电重启
MANUAL	系统下手动 reboot/reload 重启
HIGH-TMPR	高温异常重启
BHMDOG	BHM Watchdog 重启，用于监控系统各个功能模块
LCMDOG	LCM Watchdog 重启，用于监控 LC
SCHEDULE	定时重启
SNMP-RELOAD	SNMP 重启

重启类型	说明
HALFAIL	HAGT 与 HSRV 通讯异常重启，需要开启 stack 功能
ABNORMAL	系统非正常方式重启，包括 shell 下的 reboot
CTCINTR	按键重启
LCATTACH	LC 匹配异常重启
OTHER	其他重启

4.7.3 查看重启记录

表 4-5 显示重启记录

命令	操作	说明
show reboot-info	查看交换机的重启记录	-

显示交换机的重启记录：

```
Switch# show reboot-info
Times       Reboot Type       Reboot Time(DST)
1           MANUAL            2000/01/01 01:21:35
2           MANUAL            2000/01/01 02:07:52
3           MANUAL            2000/01/01 02:24:59
4           MANUAL            2000/01/01 03:28:58
5           MANUAL            2000/01/01 03:43:02
6           MANUAL            2000/01/01 03:49:51
7           MANUAL            2000/01/01 04:01:23
8           MANUAL            2000/01/01 04:42:40
9           MANUAL            2000/01/01 04:49:27
10          MANUAL            2000/01/01 20:59:20
```

用户可以在全局配置模式下使用 **reset reboot-info** 命令清除重启记录。

说明

如上方回显所示，使用该命令最多显示 10 条重启记录。如果要查看更多的重启记录，可以在该文件中查看：flash:/reboot-info/reboot_info.log

5 BootROM 配置

5.1 BootROM 简介

BootROM（Boot Read-Only Memory）是固化在芯片内部的 ROM，可以初始化各种接口。U-boot 的主要功能是简单地初始化板子和在启动时加载系统镜像。在 U-boot 模式下，用户可以使用命令实现一些功能。U-boot 既能从 TFTP 服务器上加载系统镜像，又能从硬盘中加载镜像，例如 Flash。如果用户从 TFTP 服务器上启动系统，可以配置本地设备和指定 TFTP 服务器的 IP 地址。

5.2 配置 BootROM 环境变量

5.2.1 配置通过 TFTP 服务器加载镜像

i. 配置步骤

1. 通过TFTP服务器加载镜像 OS-ms-v3.1.9.it.r.bin

命令举例	操作	说明
bootrom:> setenv bootcmd boot_tftp OS-ms-v3.1.9.it.r.bin	从 TFTP 服务器上加载镜像 OS-ms-v3.1.9.it.r.bin 启动系统	-
bootrom:> saveenv	在本地保存配置	-
bootrom:> reset	重启板子	-

2. 不使用密码通过TFTP服务器加载镜像 OS-ms-v3.1.9.it.r.bin

命令举例	操作	说明
bootrom:> setenv bootcmd boot_tftp_nopass OS-ms-v3.1.9.it.r.bin	不使用密码，从 TFTP 服务器上加载镜像 OS-ms-v3.1.9.it.r.bin 启动系统	-
bootrom:> saveenv	在本地保存配置	-
bootrom:> reset	重启板子	-

3. 通过TFTP服务器加载镜像 OS-ms-v3.1.9.it.r.bin 后直接重启板子

命令举例	操作	说明
bootrom:> boot_tftp OS-ms-v3.1.9.it.r.bin	从 TFTP 服务器上加载镜像 OS-ms-v3.1.9.it.r.bin 后直接重启板子	-

4. 不使用密码通过TFTP服务器加载镜像 OS-ms-v3.1.9.it.r.bin 后直接重启板子

命令举例	操作	说明
bootrom:> boot_tftp_nopass OS-ms-v3.1.9.it.r.bin	不使用密码从 TFTP 服务器上加载镜像 OS-ms-v3.1.9.it.r.bin 后直接重启板子	-

ii. 命令验证

完成上述配置步骤后，验证配置信息：

```
bootrom:> reset
……..
TFTP from server 10.10.29.160; our IP address is 10.10.29.118
Filename 'OS-ms-v3.1.9.it.r.bin'.
Load address: 0xaa00000
Loading: octeth0: Up 100 Mbps Full duplex (port    0)
#################################################################
             ####################
done
Bytes transferred = 12314539 (bbe7ab hex), 1829 Kbytes/sec
```

5.2.2 配置通过 Flash 加载镜像

i. 配置步骤

1. 通过Flash加载镜像 OS-ms-v3.1.9.it.r.bin 启动系统

命令举例	操作	说明
bootrom:> setenv bootcmd boot_flash OS-ms-v3.1.9.it.r.bin	从 Flash 加载镜像 OS-ms-v3.1.9.it.r.bin 启动系统	-
bootrom:> saveenv	在本地保存配置	-

命令举例	操作	说明
bootrom:> reset	重启板子	-

2. 通过Flash加载镜像 OS-ms-v3.1.9.it.r.bin 启动系统，并恢复系统默认登录密码配置

命令举例	操作	说明
bootrom:> setenv bootcmd boot_flash_nopass OS-ms-v3.1.9.it.r.bin	不需要密码从 Flash 加载镜像 OS-ms-v3.1.9.it.r.bin 启动系统	-
bootrom:> saveenv	在本地保存配置.	-
bootrom:> reset	重启板子	-
Do you want to revert to the default config file ? [Y|N|E]:Y	Y：恢复默认配置文件 N：仅恢复默认登录密码配置 E：退出设置	-

3. 通过Flash加载镜像 OS-ms-v3.1.9.it.r.bin 后直接启动系统

命令举例	操作	说明
bootrom:> boot_flash OS-ms-v3.1.9.it.r.bin	从 Flash 加载镜像 OS-ms-v3.1.9.it.r.bin 后直接启动系统	-

4. 通过Flash加载镜像 OS-ms-v3.1.9.it.r.bin from flash 后直接启动系统，并恢复系统默认登录密码配置

命令举例	操作	说明
bootrom:> boot_flash_nopass OS-ms-v3.1.9.it.r.bin	不需要密码从 flash 加载镜像 OS-ms-v3.1.9.it.r.bin from flash 后直接启动系统	-
Do you want to revert to the default config file ? [Y|N|E]:Y	Y：恢复默认配置文件 N：仅恢复默认登录密码配置 E：退出设置	-

ii. 命令验证

完成上述配置步骤后，验证配置信息：

```
bootrom:> reset

……
Do you want to revert to the default config file ? [Y|N|E]:Y
### JFFS2 loading '/boot/OS-ms-v3.1.9.it.r.bin' to 0xaa00000
Scanning JFFS2 FS: . done.
### JFFS2 load complete: 12314539 bytes loaded to 0xaa00000
## Booting image at 0aa00000 ...
    Verifying Checksum ... OK
    Uncompressing Kernel Image ... OK
……
```

5.2.3 配置 Boot IP 地址

i. 配置步骤

1 配置本地设备的IP地址

命令举例	操作	说明
bootrom:> setenv ipaddr 10.10.29.101	配置本地设备的 IP 地址	-
bootrom:> saveenv	在本地保存配置	-

2 配置TFTP服务器的IP地址

命令举例	操作	说明
bootrom:> setenv serverip 10.10.29.160	指定 TFTP 服务器的 IP 地址	-
bootrom:> saveenv	在本地保存配置	-

ii. 命令验证

完成上述配置后，验证配置信息：

```
bootrom:> printenv

printenv
bootdelay=5
baudrate=9600
download_baudrate=9600
……
stderr=serial
ipaddr=10.10.29.101
ipserver=10.10.29.160
```

```
Environment size: 856/2044 bytes
```

5.2.4 配置 BootROM 网关地址

i. 配置步骤

1 配置本地设备的网关地址

命令举例	操作	说明
bootrom:> setenv gatewayip 10.10.37.1	配置交换机 BootROM 的网关地址	-
bootrom:> saveenv	在本地保存配置	-

2 配置本地设备的子网掩码

命令举例	操作	说明
bootrom:> setenv netmask 255.255.255.0	配置子网掩码	-
bootrom:> saveenv	在本地保存配置	-

ii. 命令验证

完成上述配置后，验证配置信息：

```
bootrom:> printenv

printenv
bootdelay=5
baudrate=9600
download_baudrate=9600
……
stderr=serial
gatewayip=10.10.38.1
netmask=255.255.255.0
Environment size: 856/2044 bytes
```

5.3 在线升级 BootROM

5.3.1 配置步骤

命令举例	操作	说明
bootrom:> upgrade_uboot bootrom.bin	通过 TFTP 服务器在线升级 Bootrom	-

5.3.2 命令验证

完成上述配置命令之后，验证配置信息：

```
bootrom:> version

version
Bootrom 3.0.3 (Development build) (Build time: Aug  4 2011 - 11:47:06)
```

6 启动诊断配置

6.1 启动诊断简介

启动诊断可以在交换机重新启动后，帮助用户诊断交换机的各个硬件组件是否工作正常。其中诊断项包括：EPLD，EEPROM，PHY，MAC 等。

6.2 配置启动诊断

6.2.1 配置启动诊断等级

表6-1 配置启动诊断等级

命令	操作	说明
configure terminal	进入全局配置模式	-
diagnostic bootup level { **minimal** | **complete** }	配置启动诊断等级	-

6.2.2 查看启动诊断等级与结果

表6-2 查看启动诊断等级与结果

命令	操作	说明
show diagnostic bootup level	查看启动诊断等级	-
show diagnostic bootup result [**slot** *slot-id*]	配置启动诊断后，显示启动诊断结果	slot-id: 堆叠情况下的成员编号
show diagnostic bootup result detail [**slot** *slot-id*]	配置启动诊断后，显示启动诊断结果的详细信息	

6.3 配置举例

6.3.1 配置步骤

配置启动诊断的流程如下表所示。

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# diagnostic bootup level minimal	设置诊断等级为 minimal
Switch(config)# exit	退出诊断模式
Switch# show diagnostic bootup level	查看配置的诊断等级是否正确
Switch# reboot	重启系统

6.3.2 命令验证

查看启动诊断的结果：

```
Switch# show diagnostic bootup result detail

############################################################
Item Name                       Attribute Result Time(usec)
1       EPLD TEST                C         Pass     57
2       EEPROM0 TEST              C          Pass     101262
3       PHY TEST                 C         Pass     1161
4       FAN TEST                 C         Pass     4668
5       SENSOR TEST               C          Pass     5472
6       PSU TEST                 C         Pass     1370
7       L2 UCAST FUNC TEST          C          Pass     40126
```

7 Bootstrap 配置

7.1 Bootstrap 简介

Bootstrap 是一种智能初始化配置方法。配置启用 Bootstrap 功能后，交换机启动时发现没有 startup-config.conf 文件或 Bootstrap 功能开关开启，则开始从 TFTP 服务器上下载配置文件或 image 文件。如果发现需要下载不同版本的 image 文件，则需要重新启动系统。

用户通过 python 脚本文件控制交换机下载的 image 文件和配置文件，交换机将会从 python 格式的脚本文件里，找到需要下载的文件。脚本文件的名称为 bootstrap.py，用户应根据需求完成配置，需要填入的信息如下：

```
options = {
    # tftp server ip
    "hostname": "192.168.1.254",

    # new target system image name
    "target_system_image": "XXXXXX.bin",

    # new target system image md5sum
    "image_md5sum": "f7ea31029b33d3f77d7c2156a814e6d7",

    # tftp server config path
    #config_sw=1 get config, config_sw=0 no get config
    "config_sw": 1,
    "config_path": "/tftpboot/",

    # tftp server target system image path
    "target_image_path": "/tftpboot/",
```

```
    "destination_path": "/mnt/flash/boot/",
}
```

其中红色字体部分需要用户自行设置：

hostname：TFTP 服务器的 IP 地址。

target_system_image：需要升级的版本文件名称。

image_md5sum：image 文件的 MD5 值，若为空则表示不进行 image 的 MD5 校验，否则进行 image 的 MD5 校验。

config_sw：下载配置文件的开关，“1”表示下载配置文件，“0”表示不下载配置文件。

config_path：下载配置文件的路径，注意这里路径不需要填写配置文件名称。

target_image_path：下载 image 文件的路径，同样地，这里不需要填写 image 文件名称。

配置好 python 文件后，当 python 脚本中 target_system_image 和交换机中版本一致时，不进行 image 下载操作，只做配置文件下载并更新配置操作。当版本不一致时，先进行 image 文件下载，更新 image 版本后重启，待重启后进行配置下载更新操作。

说明

完成了一次配置更新后，如果还需要重复应用该配置文件，则需要手动删除/mnt/flash/boot/increment-config.cfg 文件，再进行 Bootstrap 功能。当没有 startup-config.conf 文件即空配置启动时会自动删除 increment-config.cfg 文件。

7.2 配置 Bootstrap

7.2.1 使能 Bootstrap 功能

Bootstrap 是设备启动时自动完成初始化配置的功能。设备在启动时如果没有 startup-config 文件，或者启用 Bootstrap 功能，则开始启动 Bootstrap 工作流程。

表7-1 使能Bootstrap功能

命令	操作	说明
configure terminal	进入全局配置模式	-
bootstrap enable	全局使能 Bootstrap 功能	缺省情况下，Bootstrap 功能处于关闭状态

7.2.2 显示 smart-config 配置信息

表7-2 显示smart-config配置信息

命令	操作	说明
show smart-config config	查看 smart-config 的配置信息	-

7.3 配置举例

7.3.1 简介

默认 Bootstrap 功能处于关闭状态，当 startup-config.conf 文件不存在或开启了 Bootstrap 开关时，交换机才会在启动时开始 Bootstrap 工作流程。也可以手动删除 startup-config.conf 文件，这样在下次启动时，Bootstrap 就会开始工作。

7.3.2 拓扑

图 7-1 Bootstrap 配置拓扑图

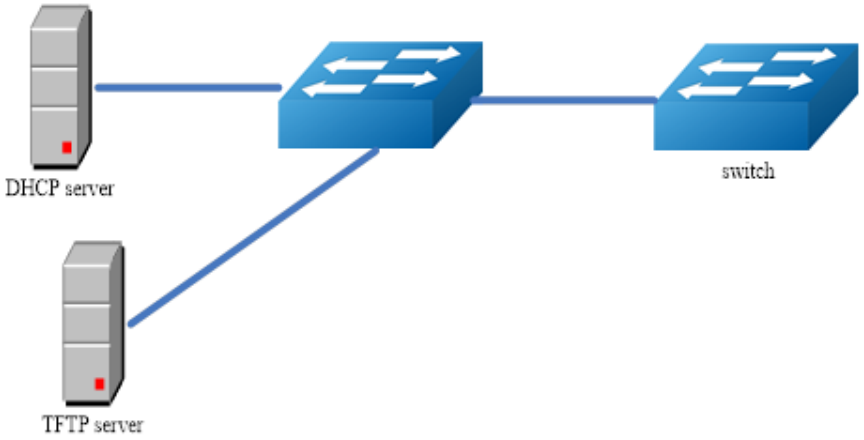


图 7-1 为测试 Bootstrap 的网络拓扑，需要两台交换机和两台 PC 构建测试环境。Switch 是启用 Bootstrap 功能的交换机。需要注意的是，上图中 DHCP Server 提供的 TFTP Server 地址必须是 Switch 可以直接连接或者通过路由器连接的地址。

7.3.3 配置步骤

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# bootstrap enable	设置启用 Bootstrap
Switch (config)# exit	退出全局配置模式

具体的配置步骤如下：

1.配置 DHCP Server，必须要设置 option 66：tftp-server name 和 option 67：bootfile-name 选项；其中 option 66 字段必须设置为 IP 地址格式，如 10.0.0.1 或者 http://10.0.0.1。option 67 字段为下载 python 脚本文件的路径名称，如/tftpboot/boostrap.py。

2.通过 DHCP Server 端的信息从 TFTP 服务器下载脚本文件 bootstrap.py，该 python 脚本内容需根据用户需求事先完成定义，将需要升级的 image 文件与配置文件放到 python 脚本中对应的 TFTP Server 上。

- image文件名需要和python脚本文件中填入的target_system_image一致。

- 配置文件名称的格式：设备SN号.cfg，例如：U50R9390071.cfg。也可以为设备的MAC地址.cfg例如：6cec5a084e93.cfg

注意：设备 SN 号区分大小写，设备 MAC 地址为设备管理口 MAC 地址且字母均为小写。（可用 **show management interface** 命令查看）

3.确保交换机没有 startup-config.conf 文件或者开启了 Bootstrap 功能开关。

说明

当存在 startup-config.conf 文件但开启了 Bootstrap 开关时，管理口需配成 DHCP 模式后再重启，空配置启动时无此限制。

4.启动或重启系统。

7.3.4 命令验证

检查上述 Bootstrap 配置后的结果：

```
Switch# show running-config

!
bootstrap enable
!
line con 0
  no line-password
  no login
line vty 0 7
  exec-timeout 35791 0
  privilege level 4
  no line-password
  no login
!
end
```

组播配置指导目录

1 IP 组播路由配置

1.1 IP 组播路由简介

随着网络的不断发展，网络数据、语音、视频信息等多种交互业务与日俱增。另外，新兴的电子商务、网上会议、网上拍卖、视频点播、远程教学等对带宽和实时数据交互要求较高的服务逐渐兴起，这些服务对信息安全性、可计费性、网络带宽提出了更高的要求。

当网络中需要某信息的用户量不确定时，单播和广播方式的效率会很低，IP 组播技术的出现改变了这一现状。当网络中的某些用户需要特定信息时，组播信息发送者（即组播源）仅发送一次信息，借助组播路由协议为组播数据包建立树型路由，被传递的信息在距离用户端尽可能近的节点才开始复制和分发。

通过组播路由协议，多个接收者能跨越不同网络接收到组播数据。

- IGMP（Internet Group Management Protocol，因特网组管理协议）是 TCP/IP 协议族中负责 IP 组播成员管理的协议。该协议在 IP 主机和与其直接相邻的组播路由器之间建立，维护组播组成员关系。
- PIM（Protocol Independent Multicast，协议无关组播），用于组播路由器或多层交换机中，为 IP 组播提供路由的单播路由协议可以是静态路由、RIP、OSPF、IS-IS、BGP 等，组播路由和单播路由协议无关，只要单播路由协议能产生路由表项即可。借助 RPF（Reverse Path Forwarding，逆向路径转发）机制，PIM 实现了在网络中传递组播信息。为了描述上的方便，由支持 PIM 协议的组播路由器所组成的网络称为 PIM 组播域。

  PIM 有两种模式：密集模式和稀疏模式。密集模式主要应用于组成员密集的局域网中，而稀疏模式适用于大型网络。

1.2 配置 IP 组播路由

1.2.1 使能 IP 组播路由

表1-1 使能IP组播路由

命令	操作	说明
configure terminal	进入全局配置模式	-
ip multicast-routing	启用交换机的组播路由功能	缺省情况下，IP 组播路由功能处于开启状态

1.2.2 配置组播路由的最大数目

当 IP 组播路由的最大数目超过阈值时，会生成警告消息，该阈值应小于组播路由的最大数量。

表 1-2 配置组播路由的最大数目

命令	操作	说明
configure terminal	进入全局配置模式	-
ip multicast route-limit *route-number* [*threshold-number*]	配置组播路由的最大数目	组播路由最大数目的取值范围为 1~2048；缺省情况下，最大数目为 2048。默认阈值应与组播路由的最大数量相同

1.2.3 配置组播静态路由

表 1-3 配置组播静态路由

命令	操作	说明
configure terminal	进入全局配置模式	-
ip mroute-rpf *source-address/mask-length* [**static** | **rip** | **ospf**] *rpf-nbr-address* [*distance*]	配置组播静态路由	source-address: 组播源地址 mask-length: 掩码长度 rpf-nbr-address: RPF 邻居的 IP 地址 distance: 路由优先级，取值范围为 1~255

1.3 显示与维护

表 1-4 显示与维护

命令	操作	说明
show ip mroute [**sparse**] [**count** | **summary**] **show ip mroute** *ip-address* [**sparse**] [**count** | **summary**]	显示组播路由表信息	sparse: 查看稀疏模式的组播路由 count: 查看路由和数据包的统计情况 summary: 查看组播路由的总体情况 ip-address: 查看源 IP 地址或者组播 IP 地址的路由
show ip mroute route-limit	查看路由数目的最大值	-
show ip mvif [*if-name*]	查看 IP 组播的接口信息	if-name: 接口名称
show ip multicast groups count	查看组播组数目	-
show ip mroute-rpf *source-address*	查看组播路由的反向路径查询	source-address: 组播源地址
show resource mcast	查看组播路由资源使用情况	-

1.4 配置举例

1.4.1. 配置步骤

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# ip multicast route-limit 1000	配置组播路由的最大数目为 1000

1.4.2. 命令验证

显示上述步骤后组播路由的最大数目：

```
Switch# show ip multicast groups count
```

```
multicast group record count:    1
multicast source record count: 0
multicast total record count:    1
multicast max record count:        1000
```

2 IGMP 配置

2.1 IGMP 简介

IGMP（Internet Group Management Protocol，因特网组管理协议）负责管理 IP 组播成员的协议，参与建立、维护接收者主机与其相邻路由器之间的组播组成员关系。该协议定义了查询器和主机的角色：

- 网络设备的查询器发送查询消息给网络中特定组来发现组播中的成员。
- 主机发送IGMP报告报文（响应查询报文），通知查询者主机要加入相应的组播组列表中。
- 一个组播组的成员是动态的，主机可以随时加入或离开。在一个组播组成员的位置或数量上没有限制。

2.1.1 IGMP 版本

IGMP 目前有 IGMPv1、IGMPv2 与 IGMPv3 三种版本。这三个版本均可适用于任意信源组播（ASM），IGMPv3 可以直接应用于指定信源组播（SSM）。而 IGMPv1、IGMPv2 需要通过 IGMP SSM Mapping 功能才可以应用于 SSM。其中，IGMPv2 协议应用最为广泛。

IGMPv1：主要以查询与响应的方式管理组播组成员；

IGMPv2：增强了查询器的选举机制与离开组机制；

IGMPv3：在 IGMPv1 与 IGMPv2 的基础上，将主机的控制能力进一步加强，查询与报告报文的能力也与之增强。

2.1.2 IGMP 报文特性

IGMP 报文使用下面的组播地址：

- IGMP普通组查询以224.0.0.1为目的地址（在一个子网中的所有系统）。
- IGMP特定组的查询以特定组IP地址为目的查询。
- IGMP组成员发送Report报文给特定的组播IP地址。

- IGMPv2离开组播组时，主动给目标IP地址224.0.0.2发送离开报文。

2.1.3 参考协议

IGMP 的版本是基于以下 RFC 定义：

- RFC 1112（定义 IGMPv1）
- RFC 2236（定义 IGMPv2）
- RFC 3376（定义 IGMPv3）

2.2 使能 IGMP 功能

IGMP 的使能是依赖于组播路由协议的使能，当接口上使能 PIM 或者其他组播路由协议，IGMP 将会在接口上自动启用，反之亦然。但是请注意，IGMP 在工作之前，IP 组播路由必须在全局模式启用。系统支持动态学习 IGMP 组记录，也可以配置静态 IGMP 组记录。

表 2-1 使能 IGMP 功能

命令	操作	说明
configure terminal	进入全局配置模式	-
ip multicast-routing	启用交换机的组播路由功能	缺省情况下，IP 组播路由功能处于开启状态
interface *if-name*	进入接口配置模式	if-name: 接口名称
no switchport	配置接口为三层接口	-
ip address *ip-address/mask-length*	设置 IP 地址	ip-address: IPv4 地址 mask-length: 掩码长度
ip pim sparse-mode	接口上启用 PIM-SM 协议	缺省情况下，未使能 PIM-SM 协议

2.3 配置 IGMP 基本功能

2.3.1 配置 IGMP 版本

表 2-2 配置 IGMP 版本

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
ip igmp version *number*	配置端口使用的 IGMP 协议的版本	number: 端口所使用的 IGMP 协议版本，取值范围为 1~3；缺省情况下，端口使用 IGMPv2 版本

2.3.2 配置静态组播(源)组

表 2-3 配置静态组播（源）组

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
ip igmp static-group *group-address* [**source** *source-address*]	配置端口上的静态组播组或静态组播源组	group-address: 组播地址 source-address: 组播源地址

2.3.3 配置过滤组播组

使用 IP 访问控制列表来控制 IGMP 报文的学习，对加入组播组的主机或可以加入的组播组进行限制。

表 2-4 配置过滤组播组

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
ip igmp access-group *acl-list*	配置组播组的过滤	acl-list: 访问控制列表名称

2.4 配置 IGMP 接口参数

2.4.3 配置 IGMP 查询与响应

表 2-5 配置 IGMP 查询与响应

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
ip igmp robustness-variable *value*	配置 IGMP 查询器的健壮系数	value: IGMP 报文的健壮程度，取值范围是 2~7，默认值为 2
ip igmp query-interval *interval*	配置端口发送查询报文的时间间隔	interval:该时间间隔的取值范围为 2~18000，单位：秒；默认值为 125 秒
ip igmp last-member-query-interval *interval*	配置 IGMP 最后组成员的查询间隔	interval: 该时间间隔的取值范围为 1000~25500，单位：毫秒；默认值为 1000 毫秒
ip igmp last-member-query-count *count*	配置 IGMP 的最后组成员的查询计数	count: 特定组查询报文的数目，取值范围为 2~7；默认值为 2
ip igmp query-max-response-time *interval*	配置 IGMP 查询报文的最大响应时间	interval: 最大响应时间的取值范围为 1~25，单位：秒；默认值为 10 秒

2.4.4 配置组播组成员快速离开功能

根据访问控制列表，可配置组播组成员快速离开的功能，快速响应主机的离开组报文。

表 2-6 配置组播组成员快速离开功能

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
ip igmp immediate-leave group-list *acl-list*	配置组播组成员快速离开的功能	acl-list: 访问控制列表名称

2.5 配置 IGMP SSM Mapping

2.5.1 使能 IGMP SSM Mapping 功能

表 2-7 使能 IGMP SSM Mapping 功能

命令	操作	说明
configure terminal	进入全局配置模式	-
ip igmp ssm-map enable	全局开启 IGMP SSM Mapping 功能	缺省情况下，IGMP SSM Mapping 功能处于关闭状态

2.5.2 配置 IGMP SSM Mapping 规则

表 2-8 配置 IGMP SSM Mapping 规则

命令	操作	说明
configure terminal	进入全局配置模式	-
ip igmp ssm-map enable	全局开启 IGMP SSM Mapping 功能	缺省情况下，IGMP SSM Mapping 功能处于关闭状态
ip igmp ssm-map static *acl-list source-address*	配置 IGMP SSM Mapping 的规则	acl-list: 访问控制列表名称 source-address: 组播源地址 缺省情况下，未配置 IGMP SSM Mapping 规则

2.6 配置加入组播组的最大数目

2.6.1 全局配置组播组的最大数目

表 2-9 全局配置组播组的最大数目

命令	操作	说明
configure terminal	进入全局配置模式	-
ip igmp limit *number* **except** *acl-list*	全局配置模式下，配置加入组播组的最大数目	number: 最大数目的取值范围为 1~2048；默认值为 2048 acl-list: 访问控制列表名称

2.6.2 接口上配置组播组的最大数目

表 2-10 接口配置组播组的最大数目

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
ip igmp limit *number* **except** *acl-list*	接口配置模式下，配置加入组播组的最大数目	number: 最大数目的取值范围为 1~2048；默认值为 2048 acl-list: 访问控制列表名称

2.7 配置 IGMP 代理

表 2-11 配置 IGMP 代理

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
no switchport	配置接口为三层接口	-
ip pim sparse-mode	接口上启用 PIM-SM 协议	缺省情况下，未使能 PIM-SM 协议
ip igmp proxy-service	启用端口的 IGMP 代理服务	缺省情况下，IGMP 代理服务处于关闭状态
ip igmp mroute-proxy *if-name*	配置本端口的上行端口	if-name: 接口名称。一个端口只能设置一个上行代理端口。多次设置时，会覆盖前面的配置

2.8 显示与维护

表 2-12 显示与维护

命令	操作	说明
show ip igmp groups [*group-address*] [**detail**]	显示组播组信息	group-address: 指定组播组地址 if-name: 接口名称 *: 所有组播组信息
show ip igmp groups *if-name* [*group-address*] [**detail**]	显示端口的组播组信息	
show ip igmp groups *if-name* **count**	显示组播组的数量	
show ip igmp interface *if-name*	查看组播组端口的信息	
clear ip igmp [* | **group** *group-address*]	清除动态学习的组播组信息	
clear ip igmp [**group** *group-address* | **interface** *if-name*]	清除指定端口上动态学习的组播组信息	

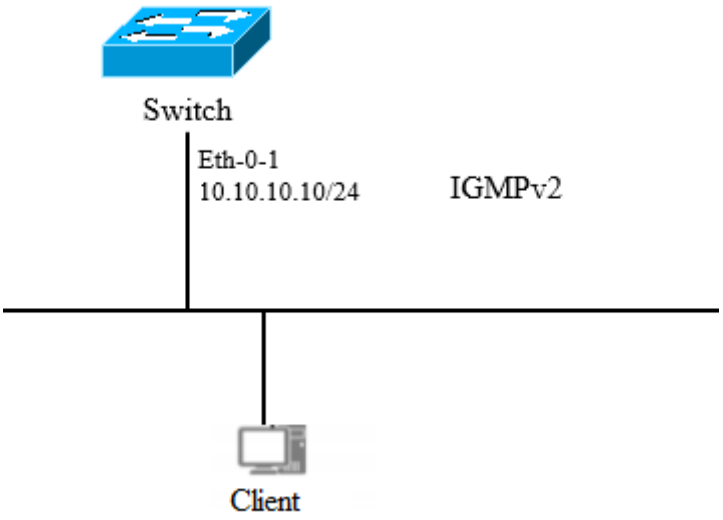
2.9 配置举例

2.9.1 简介

如下图，开启组播功能后，进接口 eth-0-1 开启 IGMP 功能和版本号，并配置 IGMP 查询与响应的相关功能。

2.9.2 拓扑

图 7-2 IGMP 配置拓扑图



2.9.3 配置步骤

1. 启用 IGMP 功能示例

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# ip multicast-routing	全局模式下启用组播路由
Switch(config)# interface eth-0-1	进入接口 eth-0-1 配置模式
Switch(config-if)# no switchport	配置接口为三层接口
Switch(config-if)# ip address 10.10.10.10/24	配置 IP 地址
Switch(config-if)# ip pim sparse-mode	接口上启用 PIM-SM

2. 配置 IGMP 接口参数示例

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# ip igmp version 2	配置 IGMP 版本

命令举例	操作步骤
Switch(config-if)# ip igmp query-interval 120	配置 IGMP 查询时间间隔
Switch(config-if)# ip igmp query-max-response-time 12	配置 IGMP 查询最大响应时间
Switch(config-if)# ip igmp robustness-variable 3	配置 IGMP 查询器的健壮系数
Switch(config-if)# ip igmp last-member-query-count 3	配置 IGMP 最后组成员查询计数
Switch(config-if)# ip igmp last-member-query-interval 2000	配置 IGMP 最后组成员查询间隔

3. 配置静态组播组示例

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# ip igmp static-group 228.1.1.1	配置 IGMP 静态组播组

4. 配置 IGMP 代理示例

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# no switchport	设置接口为三层接口
Switch(config-if)# ip pim sparse-mode	在接口上启用 PIM-SM
Switch(config-if)# ip igmp proxy-service	启用端口的 IGMP 代理服务，设置 IGMP 代理上联口为 eth-0-1
Switch(config)# interface eth-0-2	进入接口配置模式
Switch(config-if)# no switchport	设置接口为三层接口
Switch(config-if)# ip pim sparse-mode	接口上启用 PIM-SM
Switch(config-if)# ip igmp mroute-proxy eth-0-1	设置 eth-0-2 为 IGMP 代理下联口

2.9.4 命令验证

- 显示IGMP接口信息：

```
Switch# show ip igmp interface

Interface eth-0-1 (Index 1)
  IGMP Inactive, Version 2 (default) proxy-service
  IGMP host version 2
  IGMP global limit is 2000
  IGMP global limit states count is currently 0
  IGMP interface limit is 1000
  IGMP interface has 0 group-record states
  IGMP activity: 0 joins, 0 leaves
  IGMP query interval is 120 seconds
  IGMP querier timeout is 366 seconds
  IGMP max query response time is 12 seconds
  Last member query response interval is 2000 milliseconds
  Group Membership interval is 372 seconds
  Last memeber query count is 3
  Robustness Variable is 3
Interface eth-0-2 (Index 2)
  IGMP Inactive, Version 2 (default)
  IGMP mroute-proxy interface is eth-0-1
  IGMP global limit is 2000
  IGMP global limit states count is currently 0
  IGMP interface limit is 16384
  IGMP interface has 0 group-record states
  IGMP activity: 0 joins, 0 leaves
  IGMP query interval is 125 seconds
  IGMP querier timeout is 255 seconds
  IGMP max query response time is 10 seconds
  Last member query response interval is 1000 milliseconds
  Group Membership interval is 260 seconds
  Last memeber query count is 2
  Robustness Variable is 2
```

- 显示IGMP组播组信息：

```
Switch# show ip igmp groups

IGMP Connected Group Membership
Group Address    Interface          Uptime    Expires Last Reporter
228.1.1.1        eth-0-1            00:00:05 stopped   -
```

3 PIM 配置

3.1 PIM 简介

发送组播报文时，接收者可能存在于网络中的任意位置。如果静态配置组播路由，可能导致灵活性不足、时效性差等问题。为了更高效、准确地转发组播报文，需要运行组播路由协议。PIM（Protocol Independent Multicast，协议无关组播），用于组播路由器或多层交换机中，为 IP 组播提供路由的单播路由协议可以是静态路由、RIP、OSPF、IS-IS、BGP 等，组播路由和单播路由协议无关，只要单播路由协议能产生路由表项即可。借助 RPF（Reverse Path Forwarding，逆向路径转发）机制，PIM 实现了在网络中传递组播信息。为了描述上的方便，由支持 PIM 协议的组播路由器所组成的网络称为 PIM 组播域。

PIM 有两种模式：PIM-SM（稀疏模式）和 PIM-DM（密集模式）。密集模式主要应用于组成员密集的局域网中，而稀疏模式适用于大型网络。

3.1.1 PIM-SM 简介

PIM-SM（协议无关组播稀疏模式）是一个组播路由协议，用来将稀疏分散的组播设备联系起来协同工作。这样有助于分散的网络节点节约带宽，通过发送单一流量到多个接收者，达到降低网络流量的目的。

PIM-SM 使用接收者发起成员的 IP 组播模型，支持共享和最短路径树，并使用软状态机制，以适应不断变化的网络条件。它依赖于单播路由协议来建立和维护路由器间的组播路由。

1. 术语解释

以下是 PIM-SM 协议概念的简要描述：

- **汇聚点 (RP)**：RP（Rendezvous Point）在SM模式中作为组播的汇聚点，发送者和接收者在RP处进行汇聚。对于所有的组播路由器，需要明确每一个组播组与RP的对应关系。

  所有的组播数据需要在RP上注册，然后所有需要组播数据的接收者通过向RP发送Join报文来请求数据。

- **组播路由信息库 (MRIB)**：组播路由表是从单播路由表的获得的。在PIM-SM中，MRIB是用来决定向何处发送加入/剪枝消息。它还提供了目的网络的路由度量。发送和处理的Assert消息时将使用这

些度量。

- **反向路径转发 (RPF)**：反向路径转发是指路由器在接收数据包从源A通过接口IF1时，只有IF1是到达源A的出接口时才会接收这个包。反向路径转发通过使用单播路由表来决定入端口是否正确。这个数据包将被转发是由于单播路由表表明了接口IF1是到达源A的最短路径。单播路由表为组播数据选择最短路径。
- **组播树状态信息库 (TIB)**：组播树状态信息库是组播路由器上保存所有组播转发树信息的信息库，通过收到PIM加入/剪枝消息、Assert消息和IGMP消息建立起来。
- **上游 (Upstream)**：朝向树根，树根可能是源或RP。
- **下游 (Downstream)**：远离树根，树根可能是源或RP。
- **基于源的树**：基于源的树的转发路径是到达源的最短转发路径，如果单播路由以跳数为度量，基于源的树的转发路径的跳数最小；如果单播路由以延迟为度量，基于源的树的转发路径的延迟最小。

  每个组播源都有一个对应的组播转发树直接将源和接收者连接起来。所有发往指定组的流量沿着对应的转发树进行转发。
- **共享树**：共享树依赖于汇聚点(RP)，所有流量从源都发文至汇聚点，然后汇聚点再将流量发送给接收者。对于每一个组播组来说，不管有多少个源，只有一个转发树。共享树是单向的，流量只会从RP流向接收者。如果一个源要发送组播数据，首先RP要成功接收发送的组播数据，然后才能从RP发送到接收者。
- **自举路由器 (BSR)**：当一个组播源开始发送组播数据或者一个接收者开始发送加入信息到RP时，组播路由器必须获取汇聚点的信息。在PIM-SM网络启动自举路由器后，负责收集网络内的RP信息，为每个组选举出RP，然后将RP集（即组-RP映射数据库）发布到整个PIM-SM网络。
- **数据流从源到接收者发送Hello消息**：PIM路由器定期地发送Hello消息来发现PIM路由器邻居。Hello消息是组播报文，使用224.0.0.13这个地址。PIM路由器对Hello消息进行响应，Hello消息中的Hold时间来决定信息的有效时间。
- **选举指定路由器**：在一个多路访问的网络中如果有多个组播路由器，只能有一个组播路由器被选为指定路由器，负责为本地网络的组播接收者往RP发送加入/剪枝消息。
- **RP发现**：PIM-SM通过自举路由器来产生自举消息，然后发布RP信息给所有的组播路由器。组播路由器接收和保存自举消息，当DR从直连主机收到一个IGMP报文或组播数据，DR计算出该组播组

的RP，然后发送加入/剪枝到RP或者封装注册报文到RP。在小型网络环境中可以静态指定RP。

- **加入共享树**：要加入一个组播组，主机发送一个IGMP消息给上游路由器，组播路由器向RP方向的上游的PIM邻居发送加入报文。当组播路由器接收到下游设备的加入请求后，检查本地的组播组是否存在。如果存在，说明加入消息被送到共享树，收到消息的接口就会加入至出接口列表；如果不存在，条目将被创建，收到的消息接口被加入到出接口中并再次向RP方向上游的PIM邻居发送加入报文。
- **组播源注册**：与组播源S直接相连的路由器接收到该组播报文后，就将该报文封装成Register注册报文，并以单播形式发送给对应的RP。当RP接收到来自组播源S的注册消息后，一方面解封装注册消息并将组播信息沿着RPT树转发到接收者，另一方面朝组播源S逐跳发送（S，G）加入消息，从而让RP和组播源S之间的所有路由器上都生成了（S，G）表项，这些沿途经过的路由器就形成了SPT树的一个分支。SPT源树以组播源S为根，以RP为目的。组播源S发出的组播信息沿着已经建立好的SPT树到达RP，然后由RP将信息沿着RPT共享树进行转发。
- **发送注册停止消息**：当RP从组播源接收到注册报文后也收到未封装的组播报文，将发送注册停止消息给组播源一侧的DR，当DR收到注册停止消息后将不再发送注册消息给RP。
- **剪枝端口**：接收者侧的组播路由器向RP方向上游的PIM邻居发送剪枝报文，当上联组播路由器收到剪枝报文后，将收到剪枝报文的端口从转发端口中删除，当本路由器上没有其他接收者后会继续向RP方向上游的PIM邻居发送剪枝报文。
- **转发组播数据**：PIM-SM路由器将组播数据发往那些已经明确表示加入组播组的接收者。组播路由器将进行RPF检查，只有检查通过的组播数据包才将通过出端口发送出去。

2. 参考协议

与 PIM-SM 模块相关的协议规范为：

RFC 4601

3.1.2 PIM-DM 简介

PIM-DM（协议无关组播密集模式）是一个组播路由协议，用来将密集分布的组播设备联系起来协同工作。

设想当一个组播源开始发送组播流的时候，所有的下游系统都期望接收这个组播流。当组播流泛洪到整个网络时，PIM-DM 使用 RPF 来防止组播流的环路。如果某些网络区域没有该组播组的接收成员，PIM-DM 会把转发分支通过剪枝来删除掉。

剪枝状态有一个生命周期，当生命周期超时后，组播数据将再一次开始转发，每个(S,G)对应的组播组都有自己的剪枝状态。当某个组播组有新的接收者出现在已经被剪枝的区域里，路由器会通过朝组播源发送”graft”消息将剪枝状态转换成转发路径。

1. 参考协议

与 PIM-DM 模块相关的协议规范有：

RFC 3973

3.1.3 PIM-SSM 简介

PIM-SSM 是借助 PIM-SM 的部分技术和 IGMPv3 来实现的，其建立组播转发树的过程与 PIM-SM 创建 SPT 树的过程相似，即接收者 DR 获取组播数据源的具体位置后，直接向组播数据源发送 Join 消息，将组播数据流发送到接收者。

默认情况下，SSM 组播组地址的范围为 232.0.0.0~232.255.255.255。当用户加入的组播组属于 SSM 组地址范围内，会通过 PIM-SSM 的进行处理；当用户加入的组播组不属于 SSM 组地址范围，则通过 PIM-SM 的进行处理。

1. 特性

PIM-SSM 的特点是用户能够预先知道组播源的具体位置。因此用户在加入组播组时，可以明确指定接收信息的源。组成员端 DR 了解到用户的需求后，直接向组播源的方向发送 Join 消息。Join 消息逐跳向上传输，在源与组成员之间建立 SPT。

PIM-SSM 只使用了 PIM-SM 的部分技术：无需维护 RP、无需构建 RPT、无需注册组播源，可以直接在源与组成员之间建立 SPT。PIM-SSM 可以与 PIM-SM 在组播路由器上一起工作。

3.2 配置 PIM-SM

3.2.1 使能 PIM-SM

表3-1 使能PIM-SM

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

命令	操作	说明
interface *if-name*	进入接口配置模式	if-name: 接口名称
no shutdown	端口 UP	-
no switchport	配置接口为三层接口	-
ip address *ip-address/mask-length*	设置 IP 地址	ip-address: IPv4 地址 mask-length: 掩码长度
ip pim sparse-mode [**passive**]	接口上启用 PIM-SM 协议	缺省情况下，未使能 PIM-SM 协议。如选择 **passive** 关键字，工作在被动模式的端口不会发送 PIM Hello 报文

3.2.2 配置 RP

1. 配置静态RP

表3-2 配置静态RP地址

命令	操作	说明
configure terminal	进入全局配置模式	-
ip pim rp-address *address* [*acl-list* | **override**]	配置静态 RP 地址	address: RP 地址 acl-list: 访问控制列表

2. 配置动态RP

表3-3 配置候选RP

命令	操作	说明
configure terminal	进入全局配置模式	-
ip pim rp-candidate *if-name* [**priority** *priority-value* | **interval** *interval-value* | **group-list** *acl-list*]	配置候选 RP	if-name: 接口名称，此端口的 IP 地址会作为候选的 RP 在网络上被广播 priority-value: 候选 RP 的优先权，取值范围为 0~255 interval-value: 发送宣告报文的时间间隔，取值范围为 1~16383，单位：秒

命令	操作	说明
		acl-list: 访问控制列表，限制注册到此 RP 的组播组

3.2.3 配置 BSR

每个组播组需要有一个与之服务的 RP，这个 RP 作为基于组播组的分发树的根。为了组播数据能从发送者到达接收者，在一个组播域内的组播路由器需要使用同样的组播组-RP 的映射。为了选择指定组播组的 RP，组播路由器需要维护一系列的组播组-RP 的映射关系，这被称为 RP 集。BSR（自举路由器）的机制就是用来让在同一个组播域内的组播路由器能够学习到这个 RP 集。

表3-4 配置BSR

命令	操作	说明
configure terminal	进入全局配置模式	-
ip pim bsr-candidate *if-name* [*hash-mask* [*priority-value*]]	配置自举路由器	if-name: 接口名称，支持物理接口、agg 接口、loopback 和 VLAN 接口 hash-mask: RP 选举时候 HASH 的掩码长度，取值范围为 0~32 priority-value: 候选 BSR 路由器的优先级，取值范围为 0~255。默认优先级为 64

3.2.4 配置组播源注册

配置下表的功能可以防止未经认证的用户注册到交换机，例如，可以通过访问控制列表配置注册报文的过滤规则，有利于更好地控制组播组，提高安全性。

表3-5 配置组播源注册

命令	操作	说明
configure terminal	进入全局配置模式	-
ip pim accept-register list *acl-list*	根据访问控制列表限制 RP 可接收的 PIM 注册报文	acl-list: 访问控制列表；当其用此功能后，如果一个未经认证的主机发送一个 PIM 注册报文给交换机，此交换机会立即发送一个 Stop 报文回去阻止其继续发送报文注

命令	操作	说明
		册。此命令可以让网络中众多 RP 进行负载分担，通过 ACL 的设置控制不同的组播组
ip pim cisco-register-checksum [**group-list** *acl-list*]	配置 DR 发送注册报文时使用 CISCO Register Checksum	acl-list: 访问控制列表；缺省情况下，使用 RFC 规定的 Register Checksum，如果配置了访问控制列表，只有通过验证的报文才能以 CISCO Register Checksum 的方式发送
ip pim register-rate-limit *limit*	配置 DR 发往 RP 的 PIM 注册报文的最大速度	limit: 取值范围为 1~65535；缺省情况下，DR 发往 RP 的 PIM 注册报文的速度不受限制。如果设定了此项，则超过此速度的 PIM 注册报文在 RP 处会被丢弃
ip pim register-suppression *time*	配置 DR 停止发送 PIM 注册报文的时间间隔	time: 抑制时间间隔的取值范围为 11~18000，单位：秒，默认值为 60 秒

3.2.5 配置禁止 SPT 切换

表3-6 配置禁止SPT切换

命令	操作	说明
configure terminal	进入全局配置模式	-
ip pim spt-switch-threshold infinity [**group-list** *acl-list*]	配置无法切换至 SPT	acl-list: 访问控制列表；缺省情况下，DR 收到第一个组播流后立即切换为最短路径树

3.3 配置 PIM-DM

PIM-DM 和 PIM-SM 模式在同一个端口上是互斥的。因此，一次只能选择一种模式进行配置。

3.3.1 使能 PIM-DM

表3-7 使能PIM-DM

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
no shutdown	端口 UP	-
no switchport	配置接口为三层接口	-
ip address *ip-address/mask-length*	设置 IP 地址	ip-address: IPv4 地址 mask-length: 掩码长度
ip pim dense-mode [**passive**]	接口上启用 PIM-DM 协议	缺省情况下，未使能 PIM-DM 协议。如选择 **passive** 关键字，工作在被动模式的端口不会发送 PIM Hello 报文

3.3.2 配置 Hello 报文保持时间

Hello 报文的保持时间会随着端口发送 Hello 报文的时间改变而发生变化。当未配置 Hello 报文的保持时间，默认是发送 Hello 报文时间的 3.5 倍。如果配置的 Hello 报文保持时间小于当前 Hello 报文发送的时间间隔，则配置错误。

表 3-8 配置 Hello 报文保持时间

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
ip pim hello-holdtime *time*	配置 Hello 报文的保持时间	time: 保持时间的取值范围为 1~65535, ; 默认值为 3.5*Hello 报文发送的时间间隔

说明

用户可以使用 **ip pim hello-interval** *interval-value* 配置 Hello 报文发送的时间间隔，默认值为 30 秒。

3.3.3 配置端口传播延时

当一个网络上所有的路由器都支持剪枝延迟选项时，PIM-DM 路由器将用接收到的所有的传播延时来修正加入和剪枝的覆盖间隔。

表 3-9 配置端口传播延时

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
ip pim propagation-delay *delay-time*	配置 PIM-DM 的端口传播延时	delay-time: 传播延时的取值范围为 100~5000，单位：毫秒

3.3.4 配置状态刷新时间

PIM的状态刷新（SR）消息是由与组播源直接相连的路由器发送的，此命令可以控制SR消息的发送间隔。

表 3-10 配置状态刷新时间

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
ip pim state-refresh origination-interval *interval-value*	配置状态刷新的时间间隔	interval-value: SR 消息的间隔，取值范围 1~100，默认值为 60 秒

3.4 使能 PIM-SSM

表 3-11 使能 PIM-SSM

命令	操作	说明
configure terminal	进入全局配置模式	-
ip pim ssm [**default** | **range** *list*]	使能 PIM-SSM	default: 使用默认的 SSM 组播组

命令	操作	说明
		范围（232.0.0.0~232.255.255.255） list: 使用访问控制列表中的组播组范围作为 SSM 组播组范围。缺省情况下，未使能 PIM-SSM

3.5 显示与维护

表 3-12 显示与维护

命令	操作	说明
show ip pim sparse-mode bsr-router	查看自举路由器信息	-
show ip pim sparse-mode interface [**detail**]	查看稀疏模式下的端口信息	-
show ip pim sparse-mode local-member [*if-name*]	查看稀疏模式下的本地成员信息	if-name: 接口名称
show ip pim sparse-mode mroute [*source-address* | *group-address*] [**detail**]	查看 SM 模式下的组播路由	source-address: 组播路由源地址 group-address: 组播路由目的地址
show ip pim sparse-mode neighbor	查看稀疏模式下的邻居信息	-
show ip pim sparse-mode rp mapping	查看组播组与 RP 的对应关系	-
show ip pim sparse-mode rp-hash *group-address*	查看指定组播组的 RP 信息	group-address: 组播组地址
show ip pim sparse-mode spt-threshold	查看从共享树切换为最短路径树的阈值	-
show ip pim dense-mode interface [**detail**]	查看 PIM-DM 的接口信息	-
show ip pim dense-mode mroute	查看 PIM-DM 的组播路由表	-

命令	操作	说明
show ip pim sparse-mode neighbor [detail]	查看 PIM-DM 的邻居	-
show ip pim sparse-mode nexthop	查看 PIM-DM 的下一跳信息	-

3.6 配置举例

3.6.1 配置 PIM-SM 示例

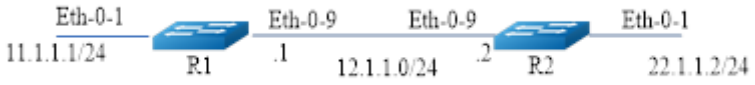
1.配置静态 RP

i. 介绍

PIM-SM 是一个软状态协议。通过静态或动态的方法在所需的接口上启用 PIM-SM 协议，并正确配置的 RP 信息。所有组播组的 IGMP 报告/离开和 PIM 加入/剪枝消息保持动态。目前，只支持一个 RP 上所有的组播组（224.0.0.0 / 4）。

ii. 拓扑

图 7-3 PIM-SM 配置拓扑图



iii. 配置步骤

以上例子中 R1 是 RP，所有的路由器都配置静态 RP：

- 每个路由器配置静态 RP 地址 11.1.1.1。
- 所有接口上必须启用 PIM-SM 功能。

R1 的配置如下：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式

命令举例	操作步骤
Switch(config-if)# no shutdown	打开接口
Switch(config-if)# no switchport	设置接口为三层接口
Switch(config-if)# ip address 11.1.1.1/24	配置 IP 地址
Switch(config-if)# ip pim sparse-mode	在接口上启用 PIM-SM
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface eth-0-9	进入接口配置模式
Switch(config-if)# no shutdown	打开接口
Switch(config-if)# no switchport	设置接口为三层接口
Switch(config-if)# ip address 12.1.1.1/24	配置 IP 地址
Switch(config-if)# ip pim sparse-mode	在接口上启用 PIM-SM
Switch(config-if)# exit	退出接口配置模式
Switch(config)# ip route 22.1.1.0/24 12.1.1.2	配置静态单播路由
Switch(config)# ip pim rp-address 11.1.1.1	配置静态 RP 地址

R2 的配置如下：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# no shutdown	打开接口
Switch(config-if)# no switchport	设置接口为三层接口
Switch(config-if)# ip address 22.1.1.2/24	配置 IP 地址
Switch(config-if)# ip pim sparse-mode	在接口上启用 PIM-SM
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface eth-0-9	进入接口配置模式
Switch(config-if)# no shutdown	打开接口
Switch(config-if)# no switchport	设置接口为三层接口

命令举例	操作步骤
Switch(config-if)# ip address 12.1.1.2/24	配置 IP 地址
Switch(config-if)# ip pim sparse-mode	在接口上启用 PIM-SM
Switch(config-if)# exit	退出接口配置模式
Switch(config)# ip route 11.1.1.0/24 12.1.1.1	配置静态单播路由
Switch(config)# ip pim rp-address 11.1.1.1	配置静态 RP 地址

iv. 命令验证

所有的路由器配置使用相同的 RP 地址 11.1.1.1，使用以下命令来验证 RP 的配置，接口的详细信息和组播路由表。

- 在R1上显示PIM稀疏模式RP映射的命令，表明11.1.1.1是对所有组播组224.0.0.0 / 4静态配置的RP。所有其他路由器都会有类似的输出：

```
R1# show ip pim sparse-mode rp mapping

PIM group-to-RP mappings
Group(s): 224.0.0.0/4, Static
      RP: 11.1.1.1
            Uptime: 00:08:21
```

- 显示R1接口的组播信息：

```
R1# show ip pim sparse-mode interface
Address          Interface VIFindex Ver/   Nbr    DR              HoldTime
                                    Mode    Count  Prior
11.1.1.1         eth-0-1   2        v2/S    0      1      11.1.1.1        105
12.1.1.1         eth-0-9   0        v2/S    1      1      12.1.1.2        105
```

- 显示PIM-SM的组播路由表：

```
R1# show ip pim sparse-mode mroute detail

IP Multicast Routing Table
(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 0
(S,G,rpt) Entries: 0
FCR Entries: 0
(*, 224.1.1.1) Uptime: 00:01:32
```

```
    RP: 11.1.1.1, RPF nbr: None, RPF idx: None
    Upstream:
      State: JOINED, SPT Switch: Enabled, JT: off
      Macro state: Join Desired,
    Downstream:
      eth-0-9:
        State: JOINED, ET Expiry: 179 secs, PPT: off
        Assert State: NO INFO, AT: off
          Winner: 0.0.0.0, Metric: 4294967295, Pref: 4294967295, RPT bit: on
        Macro state: Could Assert, Assert Track
    Join Olist:
      eth-0-9

R2# show ip pim sparse-mode mroute detail

IP Multicast Routing Table
(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 0
(S,G,rpt) Entries: 0
FCR Entries: 0
(*, 224.1.1.1) Uptime: 00:00:43
    RP: 11.1.1.1, RPF nbr: 12.1.1.1, RPF idx: eth-0-9
    Upstream:
      State: JOINED, SPT Switch: Enabled, JT Expiry: 18 secs
      Macro state: Join Desired,
    Downstream:
      eth-0-1:
        State: NO INFO, ET: off, PPT: off
        Assert State: NO INFO, AT: off
          Winner: 0.0.0.0, Metric: 4294967295, Pref: 4294967295, RPT bit: on
        Macro state: Could Assert, Assert Track
    Local Olist:
      eth-0-1
```

2.配置动态 RP

i. 介绍

在小型并且简单的网络中，组播信息量少，全网络仅依靠一个 RP 进行信息转发即可，此时可以在 SM 域中各路由器上静态指定 RP 位置。但是，通常情况下，PIM-SM 网络规模都比较大，通过 RP 转发的组播信息量也较多。为了缓解 RP 负担的同时优化共享树的拓扑结构，不同组播组应对应不同的 RP，此时就需要自举机制来动态选举 RP。

R1 的配置如下：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# no shutdown	打开接口
Switch(config-if)# no switchport	设置接口为三层接口
Switch(config-if)# ip address 11.1.1.1/24	配置 IP 地址
Switch(config-if)# ip pim sparse-mode	在接口上启用 PIM-SM
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface eth-0-9	进入接口配置模式
Switch(config-if)# no shutdown	打开接口
Switch(config-if)# no switchport	设置接口为三层接口
Switch(config-if)# ip address 12.1.1.1/24	配置 IP 地址
Switch(config-if)# ip pim sparse-mode	在接口上启用 PIM-SM
Switch(config-if)# exit	退出接口配置模式
Switch(config)# ip route 22.1.1.0/24 12.1.1.2	配置静态单播路由
Switch(config)# ip pim rp-candidate eth-0-1	配置候选 RP 接口

R2 的配置如下：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# no shutdown	打开接口
Switch(config-if)# no switchport	配置接口为三层接口
Switch(config-if)# ip address 22.1.1.2/24	配置 IP 地址
Switch(config-if)# ip pim sparse-mode	在接口上启用 PIM-SM
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface eth-0-9	进入接口配置模式

命令举例	操作步骤
Switch(config-if)# no shutdown	打开接口
Switch(config-if)# no switchport	设置接口为三层接口
Switch(config-if)# ip address 12.1.1.2/24	配置 IP 地址
Switch(config-if)# ip pim sparse-mode	在接口上启用 PIM-SM
Switch(config-if)# exit	退出接口模式
Switch(config)# ip route 11.1.1.0/24 12.1.1.1	配置静态单播路由
Switch(config)# ip pim rp-candidate eth-0-9	配置候选 RP 接口
Switch(config)# ip pim bsr-candidate eth-0-9	配置候选 BSR 接口

说明

一般选择最高优先级的路由器为 RP。如果有两个或多个路由器的优先级相同，会运用 BSR 机制中的哈希函数选择 RP，以确保在 PIM 域的所有路由器对应同一组的 RP。使用 **ip pim rp-candidate** *if-name* **priority** *priority-value* 命令来改变候选 RP 的默认优先级。

ii. 命令验证

使用 **show ip pim sparse-mode rp mapping** 命令显示组-RP 映射的详细信息，输出内容是候选 RP 信息。对应该范围 224.0.0.0 / 4 的组有两个候选 RP。候选 RP 11.1.1.1 默认的优先级 192，而候选 RP 12.1.1.2 的优先级为 2。由于候选 RP 12.1.1.2 由于具有更高的优先权，它被选中作为组播组 224.0.0.0/24 的 RP。

```
R2# show ip pim sparse-mode rp mapping

PIM group-to-RP mappings
This system is the bootstrap router (v2)
Group(s): 224.0.0.0/4
   RP: 12.1.1.2
      Info source: 12.1.1.2, via bootstrap, priority 2
            Uptime: 01:55:20, expires: 00:02:17
   RP: 11.1.1.1
      Info source: 11.1.1.1, via bootstrap, priority 192
            Uptime: 01:55:23, expires: 00:02:13
```

使用下面的命令显示特定组的 RP 路由器的信息。此输出显示已选择 12.1.1.2 为组播组 224.1.1.1 的 RP。

```
R2# show ip pim sparse-mode rp-hash 224.1.1.1

    RP: 12.1.1.2
    Info source: 12.1.1.2, via bootstrap
```

RP 信息达到域中的所有 PIM 路由器后，各状态机保持所有路由从组成员的加入/剪枝的结果。若需显示接口的详细信息和组播路由表的信息，请参见配置静态 RP 的部分。

3.6.2 配置自举路由器示例

i. 介绍

BSR 是 PIM-SM 网络里的管理核心，主要负责以下内容：

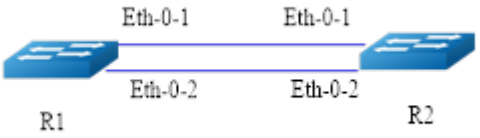
- 收集网络中Candidate-RP（C-RP）发来的Advertisement宣告信息。
- 为每个组播组选择部分C-RP信息以组成RP-Set集（即组播组和RP的映射数据库）。
- 发布到整个PIM-SM网络，从而使网络内的所有路由器（包括DR）都会定位RP的位置。

在一个 PIM 域中，需要配置一个或多个候选 BSR，候选 BSR 之间通过自动选举，产生自举路由器 BSR，负责收集并发布 RP 信息。下面简单描述一下候选 BSR 之间的自动选举：

- 在将路由器配置为候选BSR时，必须同时指定一个启动了PIM-SM的接口。
- 每个候选BSR开始都以自身作为本PIM-SM的BSR，并使用这个接口的IP地址作为BSR地址，发送自举报文。
- 当候选BSR收到其它路由器发来的自举报文时，它将新收到的自举报文的BSR地址与自己的BSR地址进行比较，比较标准包括优先级和IP地址，优先级相同的情况下，优先选择拥有较大的IP地址的报文。如果前者优先级更高或IP地址更大，则将这个新的BSR地址替换自己的BSR地址，并且不再作为自己的BSR。否则，保留自己的BSR地址，继续将自己视为BSR。
- 备选RP将自己的RP信息报告给自举路由器，然后自举路由器将汇聚的RP集通过自举报文发布到整个组播域的路由器。

ii. 拓扑

图 7-4 BSR 配置拓扑图



iii. 配置步骤

R1 的配置如下：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# ip pim bsr-candidate eth-0-1	指定 BSR 的候选接口（默认优先级 64）

R2 的配置如下：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# ip pim bsr-candidate eth-0-1 10 25	配置 HASH 掩码长度为 10、优先级为 25 的 BSR 候选接口
Switch(config)# ip pim rp-candidate eth-0-1 priority 0	配置优先级为 0 的 RP 候选接口

通过命令 **ip pim unicast-bsm** 配置接口以单播方式发送和接收 BSM 消息。

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# ip pim dr-priority 10	配置接口 DR 的优先级
Switch(config-if)# ip pim unicast-bsm	配置接口以单播方式发送和接收 BSM 消息

iv. 命令验证

1.检查候选 BSR 的信息：

```
Switch# show ip pim sparse-mode bsr-router

PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
BSR address: 20.0.1.21
Uptime: 00:37:12, BSR Priority: 64, Hash mask length: 10
Next bootstrap message in 00:00:04
Role: Candidate BSR
State: Elected BSR

Switch# show ip pim sparse-mode bsr-router

PIMv2 Bootstrap information
BSR address: 20.0.1.21
Uptime: 00:02:39, BSR Priority: 64, Hash mask length: 10
Expires: 00:00:03
Role: Candidate BSR
State: Pending BSR
Switch# show ip pim sparse-mode bsr-router
PIMv2 Bootstrap information
BSR address: 20.0.1.21
Uptime: 00:40:20, BSR Priority: 64, Hash mask length: 10
Expires: 00:02:07
Role: Candidate BSR
State: Candidate BSR
```

2.在 E-BSR 上检查 RP:

```
Switch# show ip pim sparse-mode rp mapping

PIM Group-to-RP Mappings
This system is the Bootstrap Router (v2)
Group(s): 224.0.0.0/4
RP: 20.0.1.11
Info source: 20.0.1.11, via bootstrap, priority 0
Uptime: 00:00:30, expires: 00:02:04
```

3.在 C-BSR 上检查 RP:

```
Switch# show ip pim sparse-mode rp mapping

PIM Group-to-RP Mappings
Group(s): 224.0.0.0/4
RP: 20.0.1.11
Info source: 20.0.1.21, via bootstrap, priority 0
Uptime: 00:00:12, expires: 00:02:18
```

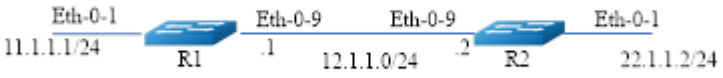
3.6.3 配置 PIM-DM 示例

i. 介绍

PIM-DM 是一个软状态协议。在所需的接口上启用 PIM-DM 协议。所有组播组的状态通过 IGMP 报告/离开和 PIM 消息来动态的维护。如下图 7-5，组播流从 R1 的 eth-0-1 口进来，接收者来与 R2 的 eth-0-1 相连。

ii. 拓扑

图 7-5 PIM-DM 配置拓扑图



iii. 配置方法

R1 的配置如下：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入 eth-0-1 的接口配置模式
Switch(config-if)# no shutdown	启用端口
Switch(config-if)# no switchport	配置接口为三层接口
Switch(config-if)# ip address 11.1.1.1/24	配置接口的 IP 地址
Switch(config-if)# ip pim dense-mode	使能接口的 PIM-DM 功能
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface eth-0-9	进入 eth-0-9 的接口配置模式
Switch(config-if)# no shutdown	启用端口
Switch(config-if)# no switchport	设置接口为三层接口
Switch(config-if)# ip address 12.1.1.1/24	配置接口的 IP 地址
Switch(config-if)# ip pim dense-mode	使能接口的 PIM-DM 功能

命令举例	操作步骤
Switch(config-if)# exit	退出接口配置模式
Switch(config)# ip route 22.1.1.0/24 12.1.1.2	配置静态路由

R2 的配置如下：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入 eth-0-1 的接口模式
Switch(config-if)# no shutdown	启用端口
Switch(config-if)# no switchport	设置接口为三层接口
Switch(config-if)# ip address 22.1.1.2/24	配置接口的 IP 地址
Switch(config-if)# ip pim dense-mode	使能接口的 PIM-DM 功能
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface eth-0-9	进入 eth-0-9 的接口模式
Switch(config-if)# no shutdown	启用端口
Switch(config-if)# no switchport	设置接口为三层接口
Switch(config-if)# ip address 12.1.1.2/24	配置接口的 IP 地址
Switch(config-if)# ip pim dense-mode	使能接口的 PIM-DM 功能
Switch(config-if)# exit	退出接口配置模式
Switch(config)# ip route 11.1.1.0/24 12.1.1.1	配置静态路由

iv. 命令验证

1. 显示 R1 上接口的详细信息：

```
R1# show ip pim dense-mode interface
Address          Interface VIFIndex Ver/   Nbr
                                    Mode   Count
11.1.1.1         eth-0-1   0        v2/D   0
12.1.1.1         eth-0-9   1        v2/D   1
```

2. 显示 R1 上邻居的详细信息：

```
R1# show ip pim dense -mode neighbor

Neighbor-Address Interface              Uptime/Expires       Ver
12.1.1.2         eth-0-9                00:01:00/00:01:44 v2
```

3. 显示 R1 上 PIM-DM 组播路由表的信息：

```
R1# show ip pim dense-mode mroute

PIM-DM Multicast Routing Table
(11.1.1.2, 225.1.1.1)
   Source directly connected on eth-0-1
   State-Refresh Originator State: Originator
   Upstream IF: eth-0-1
      Upstream State: Forwarding
      Assert State: NoInfo
   Downstream IF List:
      eth-0-9, in 'olist':
         Downstream State: NoInfo
         Assert State: NoInfo
```

4. 显示 R2 上 PIM-DM 组播路由表的信息：

```
R2# show ip pim dense-mode mroute

PIM-DM Multicast Routing Table
(11.1.1.2, 225.1.1.1)
   RPF Neighbor: none
   Upstream IF: eth-0-9
      Upstream State: AckPending
      Assert State: NoInfo
   Downstream IF List:
      eth-0-1, in 'olist':
         Downstream State: NoInfo
         Assert State: NoInfo
```

4 IGMP Snooping 配置

4.1 IGMP Snooping 简介

IGMP Snooping（Internet Group Management Protocol Snooping，互联网组管理协议窥探）是运行在二层以太网交换机上的组播约束机制，帮助设备建立和维护二层组播转发表，使组播报文按需在数据链路层转发。

由于二层交换机无法学到组播 MAC 地址，组播报文在二层网络中被广播时，同一广播域的组播成员与非组播成员都能收到组播组报文。二层交换机通过 IGMP Snooping 可以有效地控制组播流量的泛洪，节省网络带宽的同时也提高了网络信息的安全性。当二层以太网交换收到主机和路由器之间传递的 IGMP 报文时，IGMP Snooping 将对 IGMP 报文所带的信息进行分析，将端口和 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。组播路由器定期发送通用组查询来维护组播组成员关系。所有接收者将发送 IGMP 报告报文来响应这个查询，交换机通过这个监听 IGMP 报告报文来建立转发表项。

二层的组播组可以通过 IGMP 报文动态建立，也可以静态配置。静态配置的组播组将覆盖动态学的组播组。

说明

VRRP，RIP，OSPF 等协议使用了组播 IP 地址，因此在使能了 IGMP Snooping 的网络中，要避免使用这样的组播 IP 地址，它们映射出来的 MAC 地址和协议模块使用的组播 IP 地址映射出来的 MAC 地址一致。例如：

VRRP 使用了 224.0.0.18，在 IGMP Snooping 和 VRRP 网络中，避免使用组播 MAC 地址 0100.5E00.0012 映射出的组播 IP 地址；

RIP 使用了 224.0.0.9，在 IGMP Snooping 和 RIP 网络中，避免使用组播 MAC 地址 0100.5E00.0009 映射出的组播 IP 地址；

OSPF 使用了 224.0.0.5，在 IGMP Snooping 和 OSPF 网络中，避免使用组播 MAC 地址 0100.5E00.0005 映射出的组播 IP 地址

4.2 配置 IGMP Snooping 基本功能

4.2.1 使能 IGMP Snooping

用户可以在全局模式下或者单 VLAN 模式下启用 IGMP Snooping 功能。如果在全局模式下关闭 IGMP Snooping 功能，即使在单 VLAN 模式下启用 IGMP Snooping 也是无效的。如果在全局模式下开启该功能，可以在某个 VLAN 下关闭 IGMP Snooping。全局配置可以覆盖单 VLAN 配置。

表 4-1 使能 IGMP Snooping

命令	操作	说明
configure terminal	进入全局配置模式	-
ip igmp snooping [**vlan** *vlan-id*]	全局模式或单 VLAN 模式下开启 IGMP Snooping 功能	vlan-id: VLAN ID 的取值范围为 1~4094 默认情况下，IGMP Snooping 在全局模式下和每个 VLAN 上使能

4.2.2 配置 IGMP Snooping 版本

表 4-2 配置 IGMP Snooping 版本

命令	操作	说明
configure terminal	进入全局配置模式	-
ip igmp snooping [**vlan** *vlan-id*] **version** *version-number*	配置 IGMP Snooping 运行版本	vlan-id: VLAN ID 的取值范围为 1~4094 version-number: IGMP Snooping 版本号，取值范围为 1~3；默认值为 2

4.3 配置 IGMP Snooping 组播路由端口

组播路由端口是交换机上连接到组播路由器的端口，可以动态学习或者静态配置。当某个 VLAN 的端口上收到 IGMP 通用组查询报文或者是 PIMv2 Hello 报文，该端口成为这个 VLAN 的组播路由端口。所

有从组播路由端口上收到的 IGMP 查询报文要在所属 VLAN 内广播。所有 VLAN 上收到 IGMP 报告/离开报文也将从组播路由端口转发（报文抑制关闭的情况下），另外所有从该 VLAN 上收到的组播流量将从组播路由端口转发。

4.3.1 配置动态组播路由端口老化时间

表 4-3 配置动态组播路由端口老化时间

命令	操作	说明
configure terminal	进入全局配置模式	-
ip igmp snooping vlan *vlan-id* **mrouter-aging-interval** *interval-value*	配置 VLAN 上的动态组播路由端口的老化时间间隔	vlan-id: VLAN ID 的取值范围为 1~4094 interval-value: 老化时间间隔，取值范围为 1~65535，单位：秒；默认值为 255 秒

4.3.2 配置静态成员端口

交换机在二层端口上收到 IGMP 报文时会建立 IGMP Snooping 的组记录。目前系统也支持静态配置 IGMP Snooping 的组记录，在静态配置时需要指定组地址、二层端口以及二层端口所属的 VLAN。

表 4-4 配置静态成员端口

命令	操作	说明
configure terminal	进入全局配置模式	-
ip igmp snooping vlan *vlan-id* **static-group** *group-address* [**source** *source-address*] **interface** *if-name*	配置 VLAN 的成员端口加入组播组或组播源组	vlan-id: VLAN ID 的取值范围为 1~4094 group-address: 组播组地址 source-address: 组播源地址 if-name: VLAN 的成员端口名称

4.3.3 配置静态组播路由端口

表 4-5 配置静态组播路由端口

命令	操作	说明
configure terminal	进入全局配置模式	-
ip igmp snooping vlan *vlan-id* **mrouter interface** *if-name*	配置 VLAN 上的静态组播路由端口	vlan-id: VLAN ID 的取值范围为 1~4094 if-name: 接口名称

4.3.4 配置 IGMP Snooping 快速离开功能

正常情况下，IGMP Snooping 在接收到 IGMP 离开报文后不会直接将端口从组播组中删除，而是发送 IGMP 特定组查询报文，如果等待一段时间后没有得到响应，才会将该端口从组播组中删除。启动快速删除功能后，IGMP Snooping 收到 IGMP 离开报文时，直接将端口从组播组中删除。当端口下只有一个用户时，快速删除可以节省带宽。

表 4-6 配置 IGMP Snooping 快速离开功能

命令	操作	说明
configure terminal	进入全局配置模式	-
ip igmp snooping [**vlan** *vlan-id*] **fast-leave**	配置 IGMP Snooping 快速离开功能	vlan-id: VLAN ID 的取值范围为 1~4094 缺省情况下，IGMP Snooping 快速离开功能处于关闭状态

4.4 配置 IGMP Snooping 查询参数

三层交换机在所连接的网段上周期性地发送 IGMP 通用查询报文，通过解析返回的 IGMP 主机报告报文，获知该网段内的组播组成员信息。组播路由器周期性地发送查询报文，当得到某一组成员的 IGMP 主机报告报文的时候，刷新该网段相应的组成员关系信息。

4.4.1 配置 IGMP 查询与响应

用户可以选择在全局配置模式或者单个 VLAN 模式下配置 IGMP 的查询与响应。

表 4-7 配置 IGMP 查询与响应

命令	操作	说明
configure terminal	进入全局配置模式	-
ip igmp snooping [**vlan** *vlan-id*] **query-interval** *interval-value*	配置 IGMP 通用查询报文发送的时间间隔	vlan-id: VLAN ID 的取值范围为 1~4094 interval-value: 查询间隔的取值范围为 2~18000；默认值为 125 秒。 查询的间隔时间不能小于 IGMP Snooping 查询最大的响应时间
ip igmp snooping [**vlan** *vlan-id*] **query-max-response-time** *time*	配置等待查询应答报文的超时时间	vlan-id: VLAN ID 的取值范围为 1~4094 time: 超时时间的取值范围为 1~25，单位：秒；默认值为 10 秒
ip igmp snooping [**vlan** *vlan-id*] l**ast-member-query-interval** *interval-value*	配置最后成员查询报文的时间间隔	vlan-id: VLAN ID 的取值范围为 1~4094 interval-value: 查询间隔的范围为 1000~25500，单位：毫秒；默认值为 1000 毫秒

4.4.2 配置 IGMP 查询器

表 4-8 配置 IGMP 查询器

命令	操作	说明
configure terminal	进入全局配置模式	-
ip igmp snooping vlan *vlan-id* **querier address** *source-address*	配置 VLAN 上组播查询器的源地址	vlan-id: VLAN ID 的取值范围为 1~4094 source-address: 组播查询器源地址
ip igmp snooping vlan *vlan-id* **querier**	使能 VLAN 上的组播查询器功能	vlan-id: VLAN ID 的取值范围为 1~4094

命令	操作	说明
		缺省情况下，组播查询器功能处于关闭状态
ip igmp snooping vlan *vlan-id* **querier-timeout** *interval-value*	配置 VLAN 上查询器老化时间	vlan-id: VLAN ID 的取值范围为 1~4094 interval-value: 查询器老化时间间隔，取值范围为 60~300，单位：秒；默认值为 255 秒

4.4.3 配置查询器源 IP 地址

表 4-9 配置查询器源 IP 地址

命令	操作	说明
configure terminal	进入全局配置模式	-
ip igmp snooping global source-address *address*	配置 IGMP Snooping 查询器源地址	address: 查询器源 IP 地址 缺省情况下，IGMP Snooping 查询器源 IP 地址为 0.0.0.0

4.4.4 配置 TCN 查询参数

可以通过配置 TCN 的时间间隔以及查询次数来适应 STP 收敛拓扑后的组播组学习以及更新。

表 4-10 配置 TCN 查询参数

命令	操作	说明
configure terminal	进入全局配置模式	-
ip igmp snooping querier tcn { **enable** | **query-count** *count* | **query-interval** *interval-value* | **query-max-response-time** *time* }	配置 IGMP Snooping TCN 查询参数	count: TCN 查询次数，取值范围为 1~10，默认值为 2 interval-value: TCN 查询间隔，取值范围为 1~255，单位：秒；默认值为 10 秒

命令	操作	说明
		time: TCN 查询最大响应时间，取值范围为 1~10，单位：秒；默认值为 5 秒

4.5 配置组播组控制规则

4.5.1 配置组播组过滤

表 4-11 配置组播组过滤

命令	操作	说明
configure terminal	进入全局配置模式	-
ip igmp snooping vlan *vlan-id* **access-group** *acl-list*	配置允许加入的组播组范围	vlan-id: VLAN ID 的取值范围为 1~4094 acl-list: 访问控制列表名称

4.5.2 配置丢弃未知组播流量

表 4-12 配置丢弃未知组播流量

命令	操作	说明
configure terminal	进入全局配置模式	-
ip igmp snooping [**vlan** *vlan-id*] **discard-unknown**	配置丢弃未知组播流量	vlan-id: VLAN ID 的取值范围为 1~4094 缺省情况下，未知组播流量在 VLAN 内泛洪

4.5.3 配置报告报文抑制

交换机使用 IGMP 报告报文抑制功能，抑制重复发送同一个 IGMP 报文至组播路由器。当 IGMP 路由器抑制使能时（默认），交换机将第一个 IGMP 报告报文发送给组播路由器，其余相同的 IGMP 报告报文将不再发送给组播路由器。

表 4-13 配置报告报文抑制

命令	操作	说明
configure terminal	进入全局配置模式	-
ip igmp snooping [**vlan** *vlan-id*] **report-suppression**	配置设置端口对 IGMPv1/v2 的成员报告报文进行抑制	vlan-id: VLAN ID 的取值范围为 1~4094 缺省情况下，报告报文抑制功能处于开启状态； IGMP Snooping 在 V3 模式工作时，成员报告报文不进行抑制

4.6 显示与维护

表 4-14 显示与维护

命令	操作	说明
show ip igmp snooping global	查看 IGMP Snooping 的全局配置	-
show ip igmp snooping groups	显示 IGMP snooping 组播组信息	-
show ip igmp snooping groups vlan *vlan-id* [*group-address*]	显示指定 VLAN 上的组播组信息	vlan-id: VLAN ID 的取值范围为 1~4094 group-address: 组播组地址
show ip igmp snooping groups vlan *vlan-id* **count**	显示 IGMP Snooping 组播组数目	vlan-id: VLAN ID 的取值范围为 1~4094
show ip igmp snooping querier [**vlan** *vlan-id*]	显示 IGMP Snooping 查询器相关信息	
show ip igmp snooping mrouter [**vlan** *vlan-id*]	显示组播路由端口信息	
show ip igmp snooping vlan *vlan-id*	显示 VLAN 上的 IGMP Snooping 信息	

命令	操作	说明
show resource l2mcast	显示二层组播资源使用情况	-
clear ip igmp snooping group *	删除所有的 IGMP Snooping 组信息	*: 所有组信息
clear ip igmp snooping vlan *vlan-id*	删除指定 VLAN 上的组播组信息	vlan-id: VLAN ID 的取值范围为 1~4094

4.7 配置举例

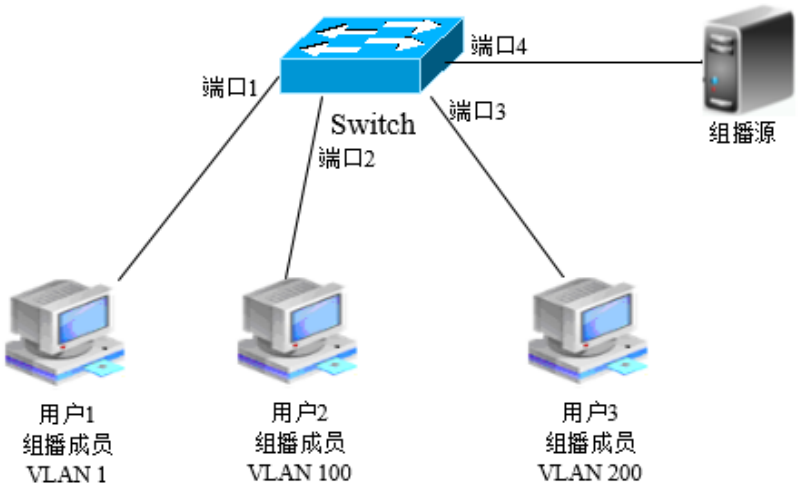
4.7.1 配置启用 IGMP Snooping

i. 简介

如下图，Switch 对组播组 VLAN 1、VLAN 200、VLAN 300 进行监控，成员 1、成员 2、成员 3 能够加入/离开组播组。

ii. 拓扑

图 7-6 IGMP Snooping 配置拓扑图



iii. 配置步骤

1. 创建VLAN与配置端口VLAN

命令举例	操作步骤
Switch#configure terminal	进入全局配置模式
Switch(config)# vlan database	进入 VLAN 配置模式
Switch(config-vlan)# vlan 100,200	创建 VLAN 100,200
Switch(config-vlan)# quit	退出 VLAN 配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# switchport mode access	设置接口为 Access 类型
Switch(config-if)# quit	退出接口配置模式
Switch(config)# interface eth-0-2	进入接口配置模式
Switch(config-if)# switchport access vlan 100	将 Access 接口添加到 VLAN 100
Switch(config-if)# quit	退出接口配置模式
Switch(config)# interface eth-0-3	进入接口配置模式
Switch(config-if)# switchport access vlan 200	将 Access 接口添加到 VLAN 200
Switch(config-if)# quit	退出接口配置模式
Switch(config)# interface eth-0-4	进入接口配置模式
Switch(config-if)# switchport mode trunk	设置接口成为 Trunk 类型
Switch(config-if)# switchport trunk allowed vlan all	允许所有 VLAN 的报文在 Trunk 类型的接口上传送
Switch(config-if)# quit	退出接口配置模式

2. 使能IGMP Snooping

命令举例	操作步骤
Switch(config)# ip igmp snooping	全局模式下启用 IGMP Snooping
Switch(config)#ip igmp snooping vlan 1	在单 VLAN 模式下启用 IGMP Snooping
Switch(config)#ip igmp snooping vlan 100	在单 VLAN 模式下启用 IGMP Snooping
Switch(config)#ip igmp snooping vlan 200	在单 VLAN 模式下启用 IGMP Snooping

3. 配置IGMP Snooping快速离开

命令举例	操作步骤
Switch(config)#ip igmp snooping fast-leave	全局模式下启用快速离开功能
Switch(config)#ip igmp snooping vlan 1 fast-leave	在 VLAN 模式下启用快速离开功能
Switch(config)#ip igmp snooping vlan 100 fast-leave	在 VLAN 模式下启用快速离开功能
Switch(config)#ip igmp snooping vlan 200 fast-leave	在 VLAN 模式下启用快速离开功能

iv. 命令验证

显示 VLAN 1、VLAN 100、VLAN 200 上 IGMP Snooping 的信息：

```
Switch# show ip igmp snooping vlan 1
Global Igmp Snooping Configuration
-----------------------------------------------
Igmp Snooping                                :Enabled
Igmp Snooping Fast-Leave                     :Enabled
Igmp Snooping Version                        :2
Igmp Snooping Robustness Variable            :2
Igmp Snooping Max-Member-Number              :2048
Igmp Snooping Unknown Multicast Behavior     :Flood
Igmp Snooping Report-Suppression             :Enabled
Vlan 1
----------
Igmp Snooping                                :Enabled
Igmp Snooping Fast-Leave                     :Enabled
Igmp Snooping Report-Suppression             :Enabled
Igmp Snooping Version                        :2
Igmp Snooping Robustness Variable            :2
Igmp Snooping Max-Member-Number              :2048
Igmp Snooping Unknown Multicast Behavior     :Flood
Igmp Snooping Group Access-list              :N/A
Igmp Snooping Mrouter Port                   :
Igmp Snooping Mrouter Port Aging Interval(sec) :255

Switch# show ip igmp snooping vlan 100
Global Igmp Snooping Configuration
-----------------------------------------------
Igmp Snooping                                :Enabled
Igmp Snooping Fast-Leave                     :Enabled
Igmp Snooping Version                        :2
Igmp Snooping Robustness Variable            :2
Igmp Snooping Max-Member-Number              :2048
Igmp Snooping Unknown Multicast Behavior     :Flood
Igmp Snooping Report-Suppression             :Enabled
```

```
Vlan 100
----------
Igmp Snooping                                  :Enabled
Igmp Snooping Fast-Leave                       :Enabled
Igmp Snooping Report-Suppression               :Enabled
Igmp Snooping Version                          :2
Igmp Snooping Robustness Variable              :2
Igmp Snooping Max-Member-Number                :2048
Igmp Snooping Unknown Multicast Behavior       :Flood
Igmp Snooping Group Access-list                :N/A
Igmp Snooping Mrouter Port                     :
Igmp Snooping Mrouter Port Aging Interval(sec) :255

Switch# show ip igmp snooping vlan 200
Global Igmp Snooping Configuration
------------------------------------------------
Igmp Snooping                                  :Enabled
Igmp Snooping Fast-Leave                       :Enabled
Igmp Snooping Version                          :2
Igmp Snooping Robustness Variable              :2
Igmp Snooping Max-Member-Number                :2048
Igmp Snooping Unknown Multicast Behavior       :Flood
Igmp Snooping Report-Suppression               :Enabled
Vlan 200
----------
Igmp Snooping                                  :Enabled
Igmp Snooping Fast-Leave                       :Enabled
Igmp Snooping Report-Suppression               :Enabled
Igmp Snooping Version                          :2
Igmp Snooping Robustness Variable              :2
Igmp Snooping Max-Member-Number                :2048
Igmp Snooping Unknown Multicast Behavior       :Flood
Igmp Snooping Group Access-list                :N/A
Igmp Snooping Mrouter Port                     :
Igmp Snooping Mrouter Port Aging Interval(sec) :255
Switch #
```

4.7.2 配置组播路由端口示例

i. 配置步骤

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# ip igmp snooping report-suppression	启用 IGMP Snooping 的报告抑制功能
Switch(config)# ip igmp snooping vlan 1 mrouter	配置静态组播路由端口

命令举例	操作步骤
interface eth-0-1	
Switch(config)# ip igmp snooping vlan 1 report-suppression	在 VLAN1 上启用报告抑制功能
Switch(config)# ip igmp snooping vlan 1 mrouter-aging-interval 200	配置动态组播路由端口老化时间

ii. 命令验证

显示 VLAN1 上 IGMP Snooping 的信息：

```
Switch# show ip igmp snooping vlan 1

Global Igmp Snooping Configuration
------------------------------------------------
Igmp Snooping                                :Enabled
Igmp Snooping Fast-Leave                     :Disabled
Igmp Snooping Version                        :2
Igmp Snooping Robustness Variable            :2
Igmp Snooping Max-Member-Number              :2048
Igmp Snooping Unknown Multicast Behavior     :Flood
Igmp Snooping Report-Suppression             :Enabled
Vlan 1
----------
Igmp Snooping                                :Enabled
Igmp Snooping Fast-Leave                     :Disabled
Igmp Snooping Report-Suppression             :Enabled
Igmp Snooping Version                        :2
Igmp Snooping Robustness Variable            :2
Igmp Snooping Max-Member-Number              :2048
Igmp Snooping Unknown Multicast Behavior     :Flood
Igmp Snooping Group Access-list              :N/A
Igmp Snooping Mrouter Port                   :eth-0-1
Igmp Snooping Mrouter Port Aging Interval(sec) :200
```

4.7.3 配置 IGMP Snooping 查询参数示例

i. 配置步骤

命令举例	操作步骤
Switch #configure terminal	进入全局配置模式
Switch(config)# ip igmp snooping query-interval 100	配置查询时间间隔是 100 秒

命令举例	操作步骤
Switch(config)# ip igmp snooping query-max-response-time 5	配置查询的最大响应时间 5 秒
Switch(config)#ip igmp snooping last-member-query-interval 2000	配置当仅存最后一个成员时的查询间隔
Switch(config)#ip igmp snooping vlan 1 querier address 10.10.10.1	在 VLAN1 上配置 IGMP Snooping 的查询地址
Switch(config)#ip igmp snooping vlan 1 querier	在 VLAN1 上启用 IGMP Snooping 的查询功能
Switch(config)#ip igmp snooping vlan 1 query-interval 200	在 VLAN1 上配置查询时间间隔为 200 秒
Switch(config)#ip igmp snooping vlan 1 query-max-response-time 5	在 VLAN1 上配置查询的最大响应时间为 5 秒
Switch(config)#ip igmp snooping vlan 1 querier-timeout 100	在 VLAN1 上配置查询超时时间为 100 秒
Switch(config)#ip igmp snooping vlan 1 last-member-query-interval 2000	在 VLAN1 上配置特定组的查询间隔为 2000 秒
Switch(config)# ip igmp snooping vlan 1 discard-unknown	在 VLAN1 上配置丢弃未知组播报文
Switch(config)# ip igmp snooping discard-unknown	在全局模式下配置丢弃未知组播报文

ii. 命令验证

显示 IGMP Snooping 查询器相关信息：

```
Switch # show ip igmp snooping querier

Global Igmp Snooping Querier Configuration
-----------------------------------------------
Version                                 :2
Last-Member-Query-Interval (msec) :2000
Last-Member-Query-Count                 :2
Max-Query-Response-Time (sec)        :5
Query-Interval (sec)                    :100
Global Source-Address                   :0.0.0.0
TCN Query Count                         :2
TCN Query Interval (sec)                :10
TCN Query Max Respose Time (sec)    :5
Vlan 1:      IGMP snooping querier status
-----------------------------------------
```

```
Elected querier is : 0.0.0.0
----------------------------------------
Admin state                          :Enabled
Admin version                        :2
Operational state                    :Non-Querier
Querier operational address          :10.10.10.1
Querier configure address            :10.10.10.1
Last-Member-Query-Interval (msec) :2000
Last-Member-Query-Count              :2
Max-Query-Response-Time (sec)        :5
Query-Interval (sec)                 :200
Querier-Timeout (sec)                :100
```

4.7.4 配置 TCN 查询示例

i. 配置步骤

命令举例	操作步骤
Switch#configure terminal	进入全局配置模式
Switch(config)# ip igmp snooping querier tcn query-count 5	配置 TCN 的查询次数为 5
Switch(config)# ip igmp snooping querier tcn query-interval 20	配置 TCN 的查询时间间隔为 20 秒

ii. 命令验证

显示 IGMP Snooping 查询器相关信息：

```
Switch # show ip igmp snooping querier

Global Igmp Snooping Querier Configuration
-------------------------------------------------
Version                              :2
Last-Member-Query-Interval (msec) :1000
Max-Query-Response-Time (sec)        :10
Query-Interval (sec)                 :125
Global Source-Address                :0.0.0.0
TCN Query Count                      :5
TCN Query Interval (sec)             :20
Vlan 1:     IGMP snooping querier status
----------------------------------------
Elected querier is : 0.0.0.0
----------------------------------------
Admin state                          :Disabled
Admin version                        :2
```

```
Operational state                    :Non-Querier
Querier operational address          :0.0.0.0
Querier configure address            :N/A
Last-Member-Query-Interval (msec) :1000
Max-Query-Response-Time (sec)        :10
Query-Interval (sec)                 :125
Querier-Timeout (sec)                :255
```

4.7.5 配置静态组播组示例

i. 配置步骤

命令举例	操作步骤
Switch#configure terminal	进入全局配置模式
Switch(config)# ip igmp snooping vlan 1 static-group 229.1.1.1 interface eth-0-2	配置静态组播组 229.1.1.1，VLAN1 的成员端口为 eth-0-2

ii. 命令验证

显示 IGMP Snooping 组播组信息：

```
Switch# show ip igmp snooping groups

VLAN    Interface       Group-Address       Uptime      Expires-time
1       eth-0-2         229.1.1.1           00:01:08    stopped
```

5 MVR 配置

5.1 MVR 简介

在传统的组播点播方式下，汇聚组播路由器下连一些接入交换机，接入交换机上连接了分布在不同 VLAN 中的用户。当这些属于不同 VLAN 的用户点播相同 Group 的节目时，汇聚的组播路由器需要为每个 VLAN 内的用户复制一份数据，每个 VLAN 的组播流量都要占用接入交换机的带宽。这样既增加了汇聚路由器的负担，也浪费了接入设备的带宽。

MVR（组播 VLAN 注册）功能能够很大程度地解决这个问题。在靠近用户侧的接入交换机上启用组播 VLAN，汇聚路由器只需把组播数据在源 VLAN 内发送给接入交换机，而不必在每个用户 VLAN 内都复制一份，接入交换机收到组播数据后再根据用户请求进行复制，给每个 VLAN 内的用户发送一份组播数据。从而节省了网络带宽，也减轻了三层设备的负担。

MVR 依赖于 IGMP Snooping 进行工作，而且只有 MVR 全局配置的 Group 才会生效。如果在 MVR 的下游接口接收的 IGMP 报文中组播组不在 MVR 全局 Group 中，该报文将被忽略。通过在 MVR 的下游接口接收的 IGMP 报告/离开报文来维护接收者信息，MVR 上游接口收到组播数据后，根据下游接口的组播组信息来决定转发组播数据的 VLAN 端口。

5.2 术语解释

配置 MVR 功能所涉及的术语如下：

MVR：组播 VLAN 注册

源 VLAN（Source VLAN）：组播 VLAN 的源 VLAN

源端口（Source Port）：MVR 网络中的上游接口，连接组播路由器的端口

接收端口（Receiver Port）：MVR 网络中的下游接口，连接接收者的端口。用来监控组播主机连接至交换机的端口。

5.3 配置 MVR

MVR 功能需要配置 IGMP Snooping 后才能生效，下面介绍 MVR 相关的配置功能及说明，具体的配置步骤请参考 5.5 配置举例。

5.3.1 使能 MVR

在使能 MVR 功能之前，需要关闭组播路由功能。

表 5-1 使能 MVR

命令	操作	说明
configure terminal	进入全局配置模式	-
no ip multicast-routing	关闭组播路由功能	缺省情况下，组播路由功能处于开启状态
mvr	使能 MVR 功能	缺省情况下，MVR 功能处于关闭状态

5.3.2 配置 MVR 的源 VLAN

在指定 MVR 的源 VLAN 前，需要创建 VLAN 及其接口。

表 5-2 配置 MVR 的源 VLAN

命令	操作	说明
configure terminal	进入全局配置模式	-
vlan database	进入 VLAN 配置模式	-
vlan *vlan-id*	创建 VLAN ID	默认为 VLAN 1
exit	退出 VLAN 配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
exit	退出接口配置模式	-
mvr vlan *vlan-id*	配置 MVR 的源 VLAN	vlan-id: VLAN ID 的取值范围为 1~4094

5.3.3 创建 MVR 组播组

通过该配置可以指定发送数据流的组播组地址以及组播组的数量。

表 5-3 配置 MVR 组播组

命令	操作	说明
configure terminal	进入全局配置模式	-
mvr group *group-address* [*count*]	创建 MVR 组播组	group-address: 组播组地址 count: 组播组数量，取值范围为 1~64

5.3.4 配置 MVR 源地址

表 5-4 配置 MVR 源地址

命令	操作	说明
configure terminal	进入全局配置模式	-
mvr source-address *address*	配置 MVR 源地址	address: MVR 发送组播报文主机地址；默认源地址为 10.0.0.1

5.3.5 配置 MVR 源端口/接收端口

在配置某个端口作为 MVR 的源端口或接收端口时，源端口必须在 MVR 源 VLAN 中，接收端口不能为 MVR 源 VLAN 中的端口。

1. 配置MVR源端口

表 5-5 配置 MVR 源端口

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
mvr type source	配置 MVR 的源端口	-

2. 配置MVR接收端口

表 5-6 配置 MVR 接收端口

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
mvr type receiver vlan *vlan-id*	配置 MVR 的接收端口	vlan-id: VLAN ID 的取值范围为 1~4094

5.4 显示与维护

表 5-7 显示与维护

命令	操作	说明
show mvr	显示 MVR 相关配置信息	-
show mvr interface	显示 MVR 端口的相关信息	-
show mvr group [**vlan** *vlan-id*] [*group-address*]	显示从 MVR 接收端口上学习到的组播组信息	vlan-id: VLAN ID 的取值范围为 1~4094 group-address: 组播组地址
show mvr group static global	显示 MVR 全局配置的静态组播组信息	-
show resource mvr	显示 MVR 的资源使用情况	-

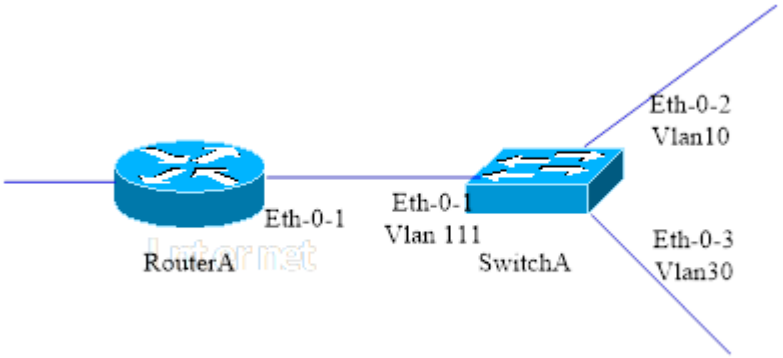
5.5 配置举例

5.5.1 介绍

如下图 7-7，在 Router A 的 eth-0-1 上启用 IGMP 和 PIM-SM。配置 Switch A 的 eth-0-1 属于 VLAN111，eth-0-2 属于 VLAN10，eth-0-3 属于 VLAN30。在 Switch A 启用 MVR，从 Router A 到 Switch A 上拷贝一份组播流，在 Switch A 上再将这个组播流进行复制，从 eth-0-2 和 eth-0-3 发送出去。

5.5.2 拓扑

图 7-7 组播 VLAN 拓扑图



5.5.3 配置步骤

Router A:

在接口上启用 IGMP 与 PIM-SM 协议。

命令举例	操作步骤
RouterA# configure terminal	进入全局配置模式
RouterA(config)# interface eth-0-1	进入接口配置模式
RouterA(config-if)# no switchport	设置端口为三层端口
RouterA(config-if)# no shutdown	使能端口
RouterA(config-if)# ip address 12.12.12.12/24	配置 IP 地址
RouterA(config-if)# ip pim sparse-mode	启用 PIM-SM 协议
RouterA(config-if)# end	退出接口配置模式

Switch A:

配置 eth-0-1 属于 VLAN111，eth-0-2 属于 VLAN10，eth-0-3 属于 VLAN30。

命令举例	操作步骤
SwitchA# configure terminal	进入全局配置模式
SwitchA(config)# vlan database	进入 VLAN 配置模式

命令举例	操作步骤
SwitchA(config-vlan)# vlan 111,10,30	创建 VLAN 111，10，30
SwitchA(config-vlan)# quit	退出 VLAN 配置模式
SwitchA(config)# interface vlan 111	进入 VLAN 接口配置模式
SwitchA(config-if)# exit	退出 VLAN 接口配置模式
SwitchA(config)# interface vlan 10	进入 VLAN 接口配置模式
SwitchA(config-if)# exit	退出 VLAN 接口配置模式
SwitchA(config)# interface vlan 30	进入 VLAN 接口配置模式
SwitchA(config-if)# exit	退出 VLAN 接口配置模式
SwitchA(config)# interface eth-0-1	进入接口配置模式
SwitchA(config-if)# switchport access vlan111	配置端口属于 VLAN111
SwitchA(config)# interface eth-0-2	进入接口配置模式
SwitchA(config-if)# switchport access vlan10	配置端口属于 VLAN10
SwitchA(config)# interface eth-0-3	进入接口配置模式
SwitchA(config-if)# switchport access vlan30	配置端口属于 VLAN30
SwitchA(config-if)# end	退出接口配置模式

在 Switch A 启用 MVR，这样从 Router A 到 Switch A 只会拷贝一份组播流，在 Switch A 上再将这个组播流从 eth-0-2 和 eth-0-3 发送出去。

命令举例	操作步骤
SwitchA # configure terminal	进入全局配置模式
SwitchA(config)# no ip multicast-routing	关闭 IP 组播路由
SwitchA(config)# mvr	启用 MVR
SwitchA(config)# mvr vlan 111	创建 MVR 的 VLAN
SwitchA(config)# mvr group 238.255.0.1 64	创建组播组
SwitchA(config)# mvr source-address 12.12.12.1	配置 MVR 源地址

命令举例	操作步骤
SwitchA(config)# interface eth-0-1	进入接口配置模式
SwitchA(config-if)# mvr type source	配置接口为 MVR 的源端口
SwitchA(config)# interface eth-0-2	进入接口配置模式
SwitchA(config-if)# mvr type receiver vlan 10	配置接口为 MVR 的接收端口
SwitchA(config)# interface eth-0-3	进入接口配置模式
SwitchA(config-if)# mvr type receiver vlan 30	配置接口为 MVR 的接收端口
SwitchA(config-if)# end	退出接口配置模式

5.5.4 命令验证

- 显示Router A上的配置信息：

```
RouterA # show ip igmp groups

IGMP Connected Group Membership
Group Address      Interface              Uptime    Expires   Last Reporter
238.255.0.1        eth-0-1                00:01:16 00:03:49 12.12.12.1
238.255.0.2        eth-0-1                00:01:16 00:03:49 12.12.12.1
238.255.0.3        eth-0-1                00:01:16 00:03:49 12.12.12.1
238.255.0.4        eth-0-1                00:01:16 00:03:49 12.12.12.1
238.255.0.5        eth-0-1                00:01:16 00:03:49 12.12.12.1
238.255.0.6        eth-0-1                00:01:16 00:03:49 12.12.12.1
238.255.0.7        eth-0-1                00:01:16 00:03:49 12.12.12.1
238.255.0.8        eth-0-1                00:01:16 00:03:49 12.12.12.1
238.255.0.9        eth-0-1                00:01:16 00:03:49 12.12.12.1
238.255.0.10       eth-0-1                00:01:16 00:03:49 12.12.12.1
……
238.255.0.64       eth-0-1                00:01:16 00:03:49 12.12.12.1
```

- 显示Switch A上的配置信息：

```
SwitchA# show mvr

MVR Running: TRUE
MVR Multicast VLAN: 111
MVR Source-address: 12.12.12.1
MVR Max Multicast Groups: 1024
MVR Hw Rt Limit: 508
MVR Current Multicast Groups: 255
```

SwitchA# show mvr groups

VLAN	Interface	Group-Address	Uptime	Expires-time
10	eth-0-2	238.255.0.1	00:03:23	00:02:03
10	eth-0-2	238.255.0.2	00:02:16	00:02:03
10	eth-0-2	238.255.0.3	00:02:16	00:02:03
10	eth-0-2	238.255.0.4	00:02:16	00:02:03
10	eth-0-2	238.255.0.5	00:02:16	00:02:03
10	eth-0-2	238.255.0.6	00:02:16	00:02:04
10	eth-0-2	238.255.0.7	00:02:16	00:02:04
10	eth-0-2	238.255.0.8	00:02:16	00:02:04
10	eth-0-2	238.255.0.9	00:02:16	00:02:04
10	eth-0-2	238.255.0.10	00:02:16	00:02:04
……				
10	eth-0-2	238.255.0.64	00:01:50	00:02:2

VPN 配置指导目录

1 VRF 配置

1.1 VRF 简介

VRF（Virtual Routing and Forwarding）又称为 VPN 路由转发表，也称作 VPN Instance（VPN 实例），是运营商边缘路由器（PE）为直接相连的站点建立并维护的一个专门实体，每个站点在 PE 上都有自己的 VPN 实例，每个 VPN 实例包含一个或多个与该 PE 直接相连的用户边缘路由器（CE）的路由和转发表。P 路由器是运营商网络主干路由器，负责快速转发数据，不与 CE 直接相连。CE、PE 和 P 路由器构成了 MPLS VPN 网络，根据 PE 路由器是否参与用户的路由，MPLS VPN 分为二层 MPLS VPN 和三层 MPLS VPN，其中三层 MPLS VPN 使用 BGP 在 PE 路由器之间分发路由信息，利用 MPLS 技术在 VPN 站点间传输数据，因此又称为 BGP/MPLS VPN。

VRF 可以把一台路由器在逻辑上划分为多台虚拟的路由器，每台虚拟的路由器就像单独的一台路由器一样工作，有自己独立的路由表和相应的参与数据转发的接口，并且彼此业务隔离。这从根本上满足了多种业务并存于一台物理设备且又需要隔离用户的需求，能够节省用户在设备及通信资源方面的投入。

1.2 配置 VRF

1.2.1 创建 VRF 路由转发表

表1-1 创建VRF路由转发表

命令	操作	说明
configure terminal	进入全局配置模式	-
ip vrf *vrf-name*	创建 VRF 路由转发表，并进入 VRF 配置模式	缺省情况下，未创建 VRF 路由转发表

1.2.2 创建 RD

RD（Route Distinguisher）即路由区分符，如果一台 PE 接收到远端 PE 发来的不同 VRF 的相同路由时，会在路由前面加上特殊信息。RD 值一共有 8 个字节，8 个字节的 RD 加上 4 个字节的 IPv4 地址组成 96 位 VPNv4 路由，使不唯一的 IPv4 地址转化为唯一的 VPN-IPv4 地址。在 PE 发布路由时加上这些信息，远端 PE 接收到路由后放在本地路由表中，与之后接收到的路由进行比较，避免地址冲突。

表 1-2 创建 RD

命令	操作	说明
configure terminal	进入全局配置模式	-
ip vrf *vrf-name*	创建 VRF 路由转发表，并进入 VRF 配置模式	缺省情况下，未创建 VRF 路由转发表
rd *rd-value*	创建 RD	rd-value: RD 值的格式为 ASN:NN 或 IP-address:NN

1.2.3 创建 Router ID

在 VRF 模式下，创建 Router ID（路由器标识符）可以识别路由域的标识符。

表 1-3 创建 Router ID

命令	操作	说明
configure terminal	进入全局配置模式	-
ip vrf *vrf-name*	创建 VRF 路由转发表，并进入 VRF 配置模式	缺省情况下，未创建 VRF 路由转发表
router-id *ip-address*	创建 Router ID	ip-address: 以 IP 地址表示的路由器标志符

1.2.4 创建 RT

RT（Route Target），通过路由目标可以实现不同 VRF 之间的路由互通。其本质就是 BGP 的团体属性。

表 1-4 创建 RT

命令	操作	说明
configure terminal	进入全局配置模式	-
ip vrf *vrf-name*	创建 VRF 路由转发表，并进入 VRF 配置模式	缺省情况下，未创建 VRF 路由转发表
route-target { **both** | **export** | **import** } *rt-value*	创建 RT	rt-value: RT 值的格式为 ASN:NN 或 IP-address:NN

1.3 配置接口加入 VPN 转发实例

使用该命令将会删除接口上原来的 IP 地址，用户必须重新配置 IP 地址。

表 1-7 配置接口加入 VPN 转发实例

命令	操作	说明
configure terminal	进入全局配置模式	-
ip vrf *vrf-name*	创建 VRF 路由转发表，并进入 VRF 配置模式	缺省情况下，未创建 VRF 路由转发表
exit	退出 VRF 配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
no switchport	配置接口为三层接口	-
ip vrf forwarding *vrf-name*	配置将三层接口加入 VPN 转发实例	vrf-name: VPN 路由转发实例名

1.4 显示与维护

表 1-8 显示与维护

命令	操作	说明
show ip vrf [**bgp** [**brief** | **detail**] | **interfaces** | **ospf** | **rip** | *vrf-name*]	显示 VRF 以及相关的接口信息	vrf-name: VPN 路由转发实例名

1.5 配置举例

1.5.1 配置步骤

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# ip vrf vpn1	创建 VRF 并进入 VRF 配置模式
Switch(config-vrf)# rd 100:1	创建 RD
Switch(config-vrf)# router-id 1.1.1.1	配置路由器标志
Switch(config-vrf)# route-target both 100:1	创建 RT
Switch(config-vrf)# interface eth-0-1	进入接口配置模式
Switch(config-if)# no shutdown	配置端口 UP
Switch(config-if)# no switchport	配置端口为三层端口
Switch(config-if)# ip vrf forwarding vpn1	配置将三层接口加入 VPN 转发实例 vpn1
Switch(config-if)# ip add 1.1.1.1/24	配置 IP 地址
Switch(config-if)# end	退出接口配置模式

1.5.2 命令验证

完成上述步骤后，显示 VRF 以及相关的接口信息：

```
Switch# show ip vrf
VRF vpn1, FIB ID 1
Router ID: 1.1.1.1 (config)
Interfaces:
  eth-0-1
DUT1# show ip vrf interfaces vpn1
Interface              IP-Address      VRF                    Protocol
eth-0-1                1.1.1.1         vpn1                   up
Switch# show ip vrf bgp brief
Name                        Default RD          Interfaces
vpn1                        100:1               eth-0-1
Switch# show ip vrf bgp detail
VRF vpn1; default RD 100:1
Interfaces:
```

```
    eth-0-1
  VRF Table ID = 1
  Export VPN route-target communities
    RT:100:1
  Import VPN route-target communities
    RT:100:1
```

2 IPv4 over IPv4 GRE 隧道配置

2.1 隧道技术简介

隧道技术是一种封装技术，它利用一种网络协议来传输另一种网络协议，即一种网络协议将其他网络协议的数据报文封装在自己的报文中，然后在网络中传输。封装后的数据报文在网络中传输的路径，称为隧道。隧道是一条虚拟的点对点连接，隧道的两端需要对数据报文进行封装及解封装。隧道技术就是指包括数据封装、传输和解封装在内的全过程。

2.1.1 IPv4 GRE 隧道定义

当两个相隔离的 IPv4 网络需要相互通信，此时就需要在两个网络之间创建一个隧道机制。在 IPv4 网络上用于连接两个相隔离 IPv4 孤岛的 GRE 隧道，称为 IPv4 GRE 隧道，即 IPv4 报文通过 GRE 协议被封装起来，实现 IPv4 报文的透明传输。GRE 隧道协议在封装 IPv4 报文时会添加 GRE 头，GRE 头中包含 Key、Sequence、Checksum 等可选信息。为了实现 GRE 隧道，需要在 IPv4 网络与 IPv4 网络交界的边界交换机上启动 IPv4 双协议栈。

GRE 隧道的源地址和目的地址是手工指定的，它提供了一个点到点的连接。GRE 隧道可以建立在两个边界路由器之间为被 IPv4 网络分离的 IPv4 网络提供稳定的连接，或建立在终端系统与边界路由器之间为终端系统访问 IPv4 网络提供连接。

2.1.2 IPv4 GRE 工作原理

IPv4 GRE over IPv4 隧道对报文的处理过程如下：

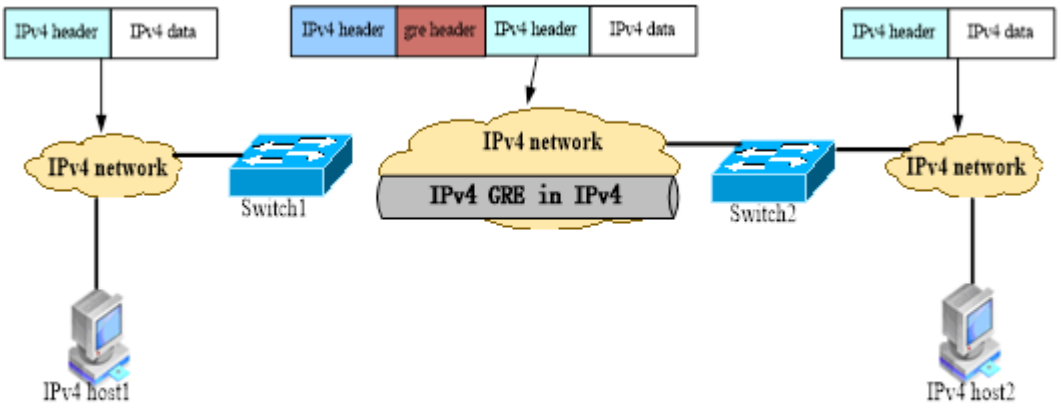
如下图，IPv4 网络中的设备发送 IPv4 报文，该报文到达隧道的源端设备 Switch 1。Switch 1 根据路由表判定该报文要通过隧道进行转发后，在 IPv4 报文前先封装上 GRE 头然后再封装外层 IPv4 的报文头，通过隧道的实际物理接口将报文转发出去。

封装报文通过隧道到达隧道目的端设备 Switch 2，Switch 2 判断该封装报文的目的地是本设备后，将对报文进行解封装。

Switch 2 根据解封装后的 IPv4 报文的目的地址转发该 IPv4 报文。如果目的地就是本设备，则将 IPv4 报文转给上层协议处理。在解封装过程中，会校验 GRE 头中的 Key 选项，只有当 Key 相匹配时才会对该 IPv4 报文作处理，否则丢弃该报文。

这种技术的优点是，当 IPv4/IPv4 网络的边缘设备实现隧道功能，便可以将报文从一端透传到另外一端并可以进行报文校验，可以极大利用现有的 IPv4 网络资源。

图 7-8 IPv4 GRE over IPv4 隧道原理图



2.2 配置 IPv4 GRE 隧道

1.2.1 配置隧道接口

如果要通过 IPv4 网络来连接两个隔离的 IPv4 网络，首先要创建 Tunnel 接口。使能后就可以转发封装后的 IPv4 报文。当配置 Tunnel 的模式为 GRE 时，必须要手动配置 Tunnel 源地址和 Tunnel 目的地址，不支持自动隧道。只有先配置隧道模式，才能继续配置 Tunnel 上的其他参数。配置其他属性之后，此 Tunnel 接口可用。

表1-1 配置隧道接口

命令	操作	说明
configure terminal	进入全局配置模式	-
interface tunnel *tunnel-id*	创建 Tunnel 接口，并进入 Tunnel 接口配置模式	tunnel-id: 接口编号，取值范围为 0～1023

命令	操作	说明
tunnel mode gre	配置隧道模式为 GRE	当配置 Tunnel 的模式为 GRE，即通用路由封装协议，目前暂时只支持 IPv4 GRE Tunnel，即针对 IPv4 报文进行封装，且封装后的报文依然为 IPv4
tunnel source { *source-ip-address* | *if-name* }	配置隧道的源地址	source-ip-address: 隧道的源地址为 IPv4 地址格式 if-name: 指定隧道的源地址从接口 IPv4 地址中获得，如果接口上有多个地址，则只获取主 IP 地址。接口可以为路由接口、VLAN 虚拟接口、环回接口
tunnel destination *dst-ip-address*	配置隧道的目的地址	dst-ip-address: 指定 Tunnel 接口的目的 IPv4 地址
tunnel gre key *key-value*	配置 GRE 隧道的关键字	key-value: 该关键字的取值范围为 1~4294967295
ip address *ip-address/mask-length*	配置 Tunnel 接口的 IP 地址	ip-address: IPv4 地址 mask-length: 掩码长度

说明

创建的 Tunnel 接口没有配置隧道模式之前，不能进行有关接口上的任何操作，此时接口不具备任何功能，只是单纯地创建了接口结构体。

1.2.2 配置隧道路由

为了保证本端设备与远端设备路由的互通性，必须有经过隧道接口转发的路由。

表 1-2 配置隧道路由

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

命令	操作	说明
ip route *ip-address/mask-length* **tunnel** *tunnel-id*	配置隧道的静态路由	ip-address: IPv4 地址 mask-length: 掩码长度 tunnel-id: 接口编号，取值范围为 0～1023

1.2.3 配置 GRE 的 Keepalive 功能

配置该功能可以检测对端 GRE Tunnel 是否处于有效 UP 状态，以及 Tunnel 之间的链路是否可通或者可达。Keepalive 只支持在 GRE Tunnel 上使能，不支持其他类型的 Tunnel。使能 Keepalive 功能后，只有当 Tunnel 接口上配有隧道源地址与目的地址时，才会发送 Keepalive 报文。

表 1-3 配置 GRE 的 Keepalive 功能

命令	操作	说明
configure terminal	进入全局配置模式	-
interface tunnel *tunnel-id*	创建 Tunnel 接口，并进入 Tunnel 接口配置模式	tunnel-id: 接口编号，取值范围为 0～1023
keepalive *period-value retry-value*	使能 Keepalive 功能	period-value: Keepalive 发包的间隔时间，取值范围为 1~32767 retry-value: Keepalive 发包的超时次数，取值范围为 1~255

1.2.4 使能隧道报文解封装

表 1-4 使能隧道报文解封装

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
tunnel enable	使能解封装接口上的隧道报文	缺省情况下，不会对收到的隧道报文解封装

2.3 显示与维护

表 1-5 显示与维护

命令	操作	说明
show interface tunnel *tunnel-id*	显示 Tunnel 接口的信息	tunnel-id: 接口编号，取值范围为 0～1023
show resource tunnel	显示 Tunnel 资源的使用信息	-
show tunnel keepalive statistics [**interface** *tunnel-id*]	显示 GRE 隧道 Keepalive 报文的统计信息	tunnel-id: 接口编号，取值范围为 0～1023
clear tunnel keepalive statistics { **all** | **interface** *tunnel-id* }	清空 GRE 隧道 Keepalive 报文的统计信息	
clear tunnel statistics { **all** | **interface** *tunnel-id* }	清空 GRE 隧道封装/解封装的统计信息	

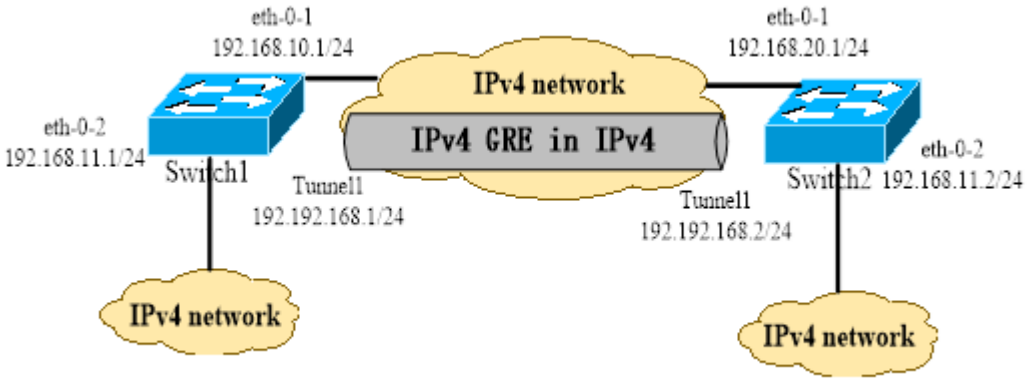
2.4 配置举例

2.4.1 介绍

如下**图**，两个 IPv4 网络分别通过 Switch 1 和 Switch 2 与 IPv4 网络连接，要求在 Switch 1 和 Switch 2 之间建立 IPv4 GRE 隧道，使两个 IPv4 网络可以互通。

2.4.2 拓扑

图 7-9 配置 IPv4 GRE 隧道



2.4.3 配置步骤

Switch 1 的配置如下：

1. 配置IPv4地址，使报文路由三层可达

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# no switchport	将 eth-0-1 配置为 3 层路由口
Switch(config-if)# ip address 192.168.10.1/24	配置接口的 IPv4 地址
Switch(config)# ip route 192.168.20.0/24 192.168.10.2	配置到达对端的 IPv4 静态路由
Switch(config)# arp 192.168.10.2 0.0.2222	配置静态 ARP，0.0.2222 为下一跳的系统 MAC 地址（该 ARP 条目也可以通过动态学习得到）

2. 配置eth-0-2的IPv4地址

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-2	进入接口配置模式
Switch(config-if)# no switchport	将 eth-0-2 配置为 3 层路由口

命令举例	操作步骤
Switch(config-if)# ip address 192.168.11.1/24	配置接口的 IPv4 地址

3. 配置Tunnel接口

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface tunnel1	创建 Tunnel 虚接口
Switch(config-if)# tunnel mode gre	配置 Tunnel 模式为 GRE
Switch(config-if)# tunnel source eth-0-1	将 eth-0-1 口作为 Tunnel 的源
Switch(config-if)# tunnel destination 192.168.20.1	配置 Tunnel 的目的地
Switch(config-if)# tunnel gre key 100	配置 Tunnel 的 GRE Key 为 100
Switch(config-if)# ip address192.192.168.1/24	配置 Tunnel 接口的 IPv4 地址

4. 配置Tunnel的Keepalive功能

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface tunnel1	进入 Tunnel1 的接口配置模式
Switch(config-if)# keepalive 5 3	使能 Tunnel1 的 Keepalive 功能

5. 使能Tunnel报文解封装

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# tunnel enable	使能 eth-0-1 接口 Tunnel 解封装

6. 配置到达对端的静态IPv4路由

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# ip route 3.3.3.3/24 tunnel1	配置到达隧道对端的静态路由

类似地，Switch 2 的配置如下：

1. 配置IPv4地址，使报文路由三层可达

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口模式
Switch(config-if)# no switchport	将 eth-0-1 配置为 3 层路由口
Switch(config-if)# ip address 192.168.20.1/24	配置接口的 IPv4 地址
Switch(config)# ip route 192.168.10.0/24 192.168.20.2	配置到达对端的 IPv4 静态路由
Switch(config)# arp 192.168.20.2 0.0.1111	配置静态 ARP, 0.0.1111 为下一跳的系统 MAC 地址。（该 ARP 条目也可以通过动态学习得到）

2. 配置eth-0-2的IPv4地址

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-2	进入接口配置模式
Switch(config-if)# no switchport	将 eth-0-2 配置为 3 层路由口
Switch(config-if)# ip address 192.168.11.2/24	配置接口的 IPv4 地址

3. 配置Tunnel接口

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface tunnel1	创建 Tunnel 虚接口
Switch(config-if)# tunnel mode gre	配置 Tunnel 模式为 GRE
Switch(config-if)# tunnel source eth-0-1	配置 Tunnel 的源地址
Switch(config-if)# tunnel destination 192.168.10.1	配置 Tunnel 的目的地址
Switch(config-if)# tunnel gre key 100	配置 Tunnel 的 GRE Key 为 100
Switch(config-if)# ip address192.192.168.2/24	配置 Tunnel 接口的 IPv4 地址

4. 配置Tunnel的Keepalive功能

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface tunnel1	进入 Tunnel1 的接口模式
Switch(config-if)# keepalive 5 3	使能 Tunnel1 的 Keepalive 功能

5. 配置Tunnel报文解封装

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# tunnel enable	使能 eth-0-1 接口 Tunnel 解封装

6. 配置到达对端的静态IPv4路由

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# ip route 4.4.4.4/24 tunnel1	配置到达隧道对端的静态路由

2.4.4 命令验证

- 显示Switch 1上Tunnel接口的信息：

```
Switch1# show interface tunnel1
Interface tunnel1
   Interface current state: UP
   Hardware is Tunnel
   Index 8193 , Metric 1 , Encapsulation TUNNEL
   VRF binding: not bound
   Internet primary address:
      192.192.168.1/24 pointopoint 192.192.168.255
   Tunnel protocol/transport GRE/IP, Status Valid
   Tunnel source 192.168.10.1(eth-0-1), destination 192.168.20.1
   Tunnel DSCP inherit,    Tunnel TTL 255
   Tunnel GRE key enable: 100
   Tunnel GRE keepalive enable, Send period: 5, Retry times: 3
   0 packets input, 0 bytes
   0 packets output, 0 bytes
```

- 显示Switch 2上Tunnel接口的信息：

```
Switch2# show interface tunnel1
Interface tunnel1
   Interface current state: UP
   Hardware is Tunnel
   Index 8193 , Metric 1 , Encapsulation TUNNEL
   VRF binding: not bound
   Internet primary address:
     192.192.168.2/24 pointopoint 192.192.168.255
   Tunnel protocol/transport GRE/IP, Status Valid
   Tunnel source 192.168.20.1(eth-0-1), destination 192.168.10.1
   Tunnel DSCP inherit,    Tunnel TTL 255
   Tunnel GRE key enable: 100
   Tunnel GRE keepalive enable, Send period: 5, Retry times: 3
   0 packets input, 0 bytes
   0 packets output, 0 bytes
```

说明

必须使 IPv4 报文三层路由可达，否则会造成 Tunnel 报文转发失败。Tunnel 接口上必须配置 IPv4 地址，否则配置在该接口上的路由无效。

IP 业务配置指导目录

1 ARP 配置

1.1 ARP 简介

ARP（Address Resolution Protocol，地址解析协议）用于将网络层的 IP 地址解析为数据链路层的物理地址（MAC 地址）。

ARP 协议有两个基本功能：将 IPv4 地址解析为 MAC 地址、维护 IP 地址和 MAC 地址映射的缓存。当一个接口请求的地址映射不在缓存中，则设备将会缓存接收到的报文并在相应的子网内广播一个地址请求，如果获得响应，则生成新的地址映射并且发送缓存的报文。ARP 在等待地址映射回应消息的时候最多缓存一个报文，而且只有最近传输的报文才会被保存。如果目的主机在 3 次请求后都无法响应，则主机被认为故障，同时相应的错误消息将被返回。如果目的主机在一段时间内（通常为一小时）不发送消息，主机可能出现问题，在删除 ARP 表项之前请求（一般为 6 个：3 个单播和 3 个广播）将被发送到主机上。

ARP 表项可以分为动态 ARP 表项与静态 ARP 表项两种类型。

动态 ARP 表项：由 ARP 协议通过 ARP 报文自动生成与维护，可以被老化、可以被 ARP 报文更新、也能被静态 ARP 表项覆盖；

静态 ARP 表项：可以通过手工添加、删除、修改。手工添加的表项是永久的，不会老化或者被动态 ARP 表项所覆盖。

1.2 配置 ARP

1.2.1 添加静态 ARP 表项

添加的 IP 地址不能为广播地址、多播地址或者本地环回地址、或者形如 0.X.X.X/8 的地址；所添加的 MAC 地址不能为广播地址、多播地址、设备本身地址或者全 0 地址；添加的静态 ARP 不能被 **clear arp-cache** 命令删除。

表1-1 添加静态ARP表项

命令	操作	说明
configure terminal	进入全局配置模式	-
arp [**vrf** *vrf-name*] *ip-address hardware-address*	添加静态 ARP 表项	vrf-name: VRF 实例名称 ip-address: 添加的静态映射的 IP 地址 hardware-address: 添加的静态映射的 MAC 地址，格式为”HHHH.HHHH.HHHH”

1.2.2 配置发送 ARP 请求报文的时间间隔

此功能不能配置在二层端口上，使用 **no switchport** 命令关闭端口的二层功能。

表 1-2 配置发送 ARP 请求报文的时间间隔

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
no switchport	配置接口为三层接口	-
arp retry-interval *seconds*	配置发送 ARP 请求报文的时间间隔	seconds: 发送 ARP 请求报文的时间间隔，取值范围为 1~10，单位：秒；默认值为 10 秒

1.2.3 配置动态 ARP 表项的老化时间

此功能不能配置在二层端口上，使用 **no switchport** 命令关闭端口的二层功能。

表 1-3 配置动态 ARP 表项的老化时间

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
no switchport	配置接口为三层接口	-

命令	操作	说明
arp timeout *seconds*	配置动态 ARP 表项的老化时间	seconds: 动态 ARP 表项的老化时间，取值范围为 1~2147483，单位：秒；默认值为 3600 秒

1.3 配置代理 ARP

代理 ARP 是由 ARP 协议演变而来。如果计算机没有配置缺省网关，又需要和其他网络中的计算机实现通信，网关收到源计算机的 ARP 请求后，会使用自己的 MAC 地址与目标计算机的 IP 地址对源计算机进行应答。代理 ARP 就是将一个主机作为对另一个主机 ARP 进行应答。

代理 ARP 又分为普通代理 ARP 和本地代理 ARP。

同一网段内连接到设备的不同 VLAN 接口的主机，可以利用设备的代理 ARP 功能，通过三层转发实现互通。为了实现三层互通，如果以太网交换机或其下挂的交换机开启了二层端口隔离功能，则需要开启本地代理 ARP 功能。

说明

开启本地 ARP 代理功能后，ICMP 重定向功能将自动关闭。

1.3.1 配置普通代理 ARP

如果未启用 ARP 代理功能，只有当目的 IP 地址属于设备自己的 ARP 请求报文时，设备才会回应。

表 1-4 配置普通代理 ARP

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
no switchport	配置接口为三层接口	-

命令	操作	说明
no shutdown	端口 UP	-
ip address *ip-address/mask-length*	设置 IP 地址	ip-address: IPv4 地址 mask-length: 掩码长度
proxy-arp enable	开启普通代理 ARP 功能	缺省情况下，普通 ARP 代理功能处于关闭状态

1.3.2 配置本地代理 ARP

本地 ARP 代理功能使得三层设备对目的 IP 地址和接收端口属于同一个子网的 ARP 请求报文作出回应。本地 ARP 代理最常见的应用场景是交换机或其下挂的交换机开启了二层端口隔离功能。使能本地 ARP 代理功能时，ICMP 重定向功能被自动关闭。

表 1-5 配置本地代理 ARP

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
no switchport	配置接口为三层接口	-
no shutdown	端口 UP	-
ip address *ip-address/mask-length*	配置 IP 地址	ip-address: IPv4 地址 mask-length: 掩码长度
local-proxy-arp enable	开启本地代理 ARP 功能	缺省情况下，本地 ARP 代理功能处于关闭状态

1.4 显示与维护

表 1-6 显示与维护

命令	操作	说明
clear arp-cache [**vrf** *vrf-name* | **interface** *if-name* | **force-delete**] *	更新公网内所有动态 ARP 表项	vrf-name: VRF 实例名称 if-name: 接口名称 ip-address: 动态 ARP 表项的 IP 地址 使用此命令后，系统将探测 ARP cache 中的各项，探测失败的项将被清除
clear ip arp [**vrf** *vrf-name*] *ip-address* [**force-delete**]	更新某个指定的动态 ARP 表项	
clear ip arp [**vrf** *vrf-name*] **statistics**	清除 ARP 报文统计消息	vrf-name: VRF 实例名称
show ip arp [**vrf** *vrf-name*] **interface** *if-name*	查看所有 ARP 条目，包括动态和静态表项	vrf-name: VRF 实例名称 if-name: 接口名称
show ip arp [**vrf** *vrf-name*] **summary**	查看 ARP 表项的统计信息	vrf-name: VRF 实例名称

1.5 配置举例

1.5.1 添加静态 ARP 表项示例

i. 配置步骤

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# no switchport	配置端口为三层接口
Switch(config-if)# ip address 11.11.11.1/24	配置端口的 IP 地址
Switch(config-if)# arp timeout 1200	配置动态 ARP 表项的老化时间
Switch(config-if)# arp retry-interval 2	配置发送 ARP 请求报文的时间间隔
Switch(config)# arp 11.11.11.2 1a.a011.eca2	添加静态 ARP 条目

ii. 命令验证

- 查看所有ARP表项以及统计信息：

```
Switch# show ip arp

 Protocol      Address              Age (min)   Hardware Addr     Interface
 Internet      11.11.11.2                 -     001a.a011.eca2      eth-0-1

Switch# show ip arp summary

  1 IP ARP entries, with 0 of them incomplete
(Static:0,    Dyamic:0, Interface:1)
  ARP Pkt Received is: 0
  ARP Pkt Send number is: 0
  ARP Pkt Dicard number is: 0
```

- 查看ARP请求重发时延与老化时间：

```
Switch# show interface eth-0-1

Interface eth-0-1
    Interface current state: Administratively DOWN
    Hardware is Ethernet, address is 6c02.530c.2300 (bia 6c02.530c.2300)
    Bandwidth 1000000 kbits
    Index 1 , Metric 1 , Encapsulation ARPA
    Speed - Auto , Duplex - Auto    , Media type is 1000BASE_T
    Link speed type is autonegotiation, Link duplex type is autonegotiation
    Input flow-control is off, output flow-control is off
    The Maximum Frame Size is 1534 bytes
    VRF binding: not bound
    Label switching is disabled
    No virtual circuit configured
    VRRP master of :    VRRP is not configured on this interface
    ARP timeout 00:20:00,    ARP retry interval 2s
    5 minute input rate 0 bits/sec, 0 packets/sec
    5 minute output rate 0 bits/sec, 0 packets/sec
       0 packets input, 0 bytes
       Received 0 unicast, 0 broadcast, 0 multicast
       0 runts, 0 giants, 0 input errors, 0 CRC
       0 frame, 0 overrun, 0 pause input
       0 input packets with dribble condition detected
       0 packets output, 0 bytes
       Transmitted 0 unicast, 0 broadcast, 0 multicast
0 underruns, 0 output errors, 0 pause output
```

1.5.2 配置代理 ARP 示例

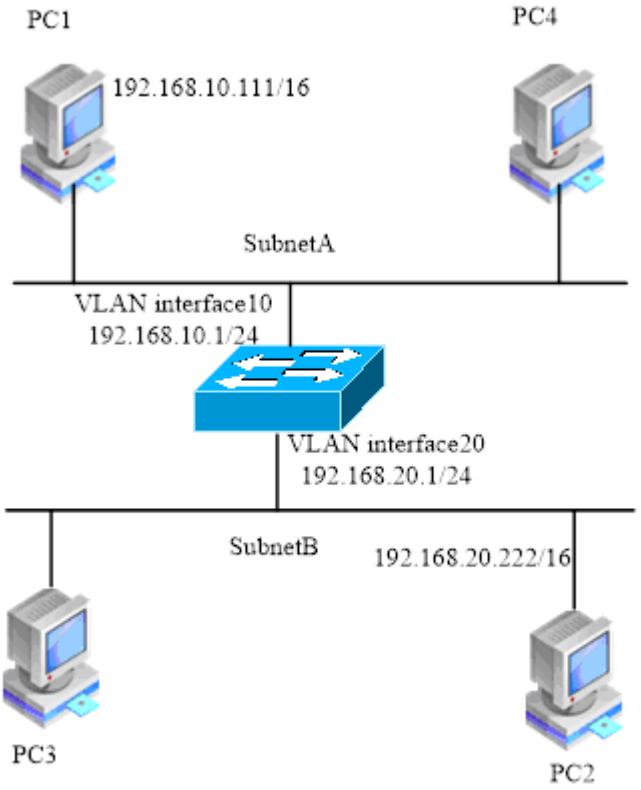
1. 配置普通代理ARP

i. 介绍

如下图所示，PC1 属于 VLAN10，PC2 属于 VLAN20，在 VLAN interface10 和 VLAN interface 20 上各自配置代理 ARP，实现 PC1 和 PC2 之间的互通。

ii. 拓扑

图 1-1 普通代理 ARP 拓扑图



iii. 配置步骤

按照下面的配置步骤在 VLAN10 和 VLAN 20 上使能 ARP 代理功能。

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式

命令举例	操作步骤
Switch(config)# vlan database	进入 VLAN 配置模式
Switch(config-vlan)# vlan 10,20	创建 VLAN 10, VLAN 20
Switch(config-vlan)# exit	退出 VLAN 配置模式
Switch(config)# interface eth-0-22	进入接口配置模式
Switch(config-if)# switchport access vlan 10	将接口加到 VLAN 10 中
Switch(config-if)# no shutdown	使能接口
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface eth-0-23	进入接口配置模式
Switch(config-if)# switchport access vlan 20	将接口加到 VLAN 20 中
Switch(config-if)# no shutdown	使能接口
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface vlan 10	创建三层 VLAN 接口 10，进入接口配置模式
Switch(config-if)# ip address 192.168.10.1/24	配置接口地址
Switch(config-if)# proxy-arp enable	使能普通代理 ARP 功能
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface vlan 20	创建三层 VLAN 接口 20，进入接口配置模式
Switch(config-if)# ip address 192.168.20.1/24	配置接口地址
Switch(config-if)# proxy-arp enable	使能普通代理 ARP 功能
Switch(config-if)# exit	退出接口配置模式

2. 配置本地代理ARP

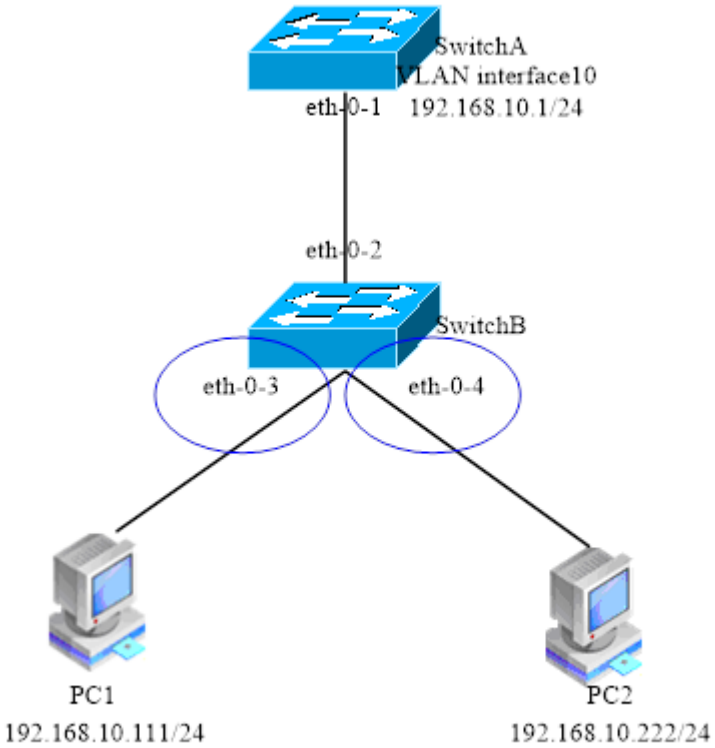
i. 介绍

如下图所示，Switch B 上的 3 个 2 层端口 eth-0-2、eth-0-3 和 eth-0-4 都属于 VLAN 10，其中 eth-0-3 和 eth-0-4 在同一个隔离组 1，所以 eth-0-3 和 eth-0-4 之间不能互相通信。eth-0-2 在隔离组 3，所以 eth-0-

2 能和 eth-0-3、eth-0-4 互相通信。PC1 和 PC2 分别连接到 Switch B 的 eth-0-3 和 eth-0-4 端口，且均属于 VLAN10。

ii. 拓扑

图 1-2 本地代理 ARP 拓扑图



iii. 配置步骤

Switch B 的配置如下：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# vlan database	进入 VLAN 配置模式
Switch(config-vlan)# vlan 10	创建 VLAN 10
Switch(config-vlan)# exit	退出 VLAN 配置模式

命令举例	操作步骤
Switch(config)# interface eth-0-3	进入接口配置模式
Switch(config-if)# switchport access vlan 10	将接口加到 VLAN 10
Switch(config-if)# no shutdown	使能接口
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface eth-0-4	进入接口配置模式
Switch(config-if)# switchport access vlan 10	将接口加到 VLAN 10
Switch(config-if)# no shutdown	使能接口
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface eth-0-2	进入接口配置模式
Switch(config-if)# switchport access vlan 10	将接口加到 VLAN 10
Switch(config-if)# no shutdown	使能接口
Switch(config-if)# exit	退出接口配置模式
Switch(config)# port-isolate mode l2	配置端口隔离模式
Switch(config-if)# interface eth-0-3	进入接口配置模式
Switch(config-if)# port-isolate group 1	配置端口属于隔离组 1
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface eth-0-4	进入接口配置模式
Switch(config-if)# port-isolate group 1	配置端口属于隔离组 1
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface eth-0-2	进入接口配置模式
Switch(config-if)# port-isolate group 3	配置端口属于隔离组 3
Switch(config-if)# exit	退出接口配置模式

Switch A 的配置如下：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式

命令举例	操作步骤
Switch(config)# vlan database	进入 VLAN 配置模式
Switch(config-vlan)# vlan 10	创建 VLAN 10
Switch(config-vlan)# exit	退出 VLAN 配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# switchport access vlan 10	将接口加到 VLAN 10
Switch(config-if)# no shutdown	使能接口
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface vlan 10	创建 3 层接口 VLAN 10，进入 VLAN 接口配置模式
Switch(config-if)# ip address 192.168.10.1/24	配置接口的 3 层地址
Switch(config-if)# local-proxy-arp enable	使能本地 ARP 代理
Switch(config-if)# exit	退出接口配置模式

iv. 命令验证

- 查看交换机Switch A上的输出结果：

```
Switch# show ip arp

 Protocol      Address            Age (min)   Hardware Addr     Interface
 Internet      192.168.10.1             -     eeb4.2a8d.6c00    vlan10
 Internet      192.168.10.111           0     34b0.b279.5f67    vlan10
 Internet      192.168.10.222           0     2a65.9618.57fa    vlan10

Switch# show ip interface vlan 10

Interface vlan10
   Interface current state: UP
   Internet address(es):
      192.168.10.1/24 broadcast 192.168.10.255
   Joined group address(es):
      224.0.0.1
   The maximum transmit unit is 1500 bytes
   ICMP error messages limited to one every 1000 milliseconds
   ICMP redirects are never sent
   ICMP unreachables are always sent
   ICMP mask replies are always sent
   ARP timeout 01:00:00,    ARP retry interval 1s
```

```
ARP Proxy is disabled, Local ARP Proxy is enabled
VRRP master of :    VRRP is not configured on this interface
```

- 查看主机PC1上的输出结果：

```
[Host: ~]$ ifconfig eth0

eth0        Link encap:Ethernet    HWaddr 34:B0:B2:79:5F:67
            inet addr:192.168.10.111    Bcast:192.168.10.255    Mask:255.255.255.0
            UP BROADCAST RUNNING MULTICAST    MTU:1600    Metric:1
            RX packets:22 errors:0 dropped:0 overruns:0 frame:0
            TX packets:28 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:1344 (1.3 KiB)    TX bytes:2240 (2.1 KiB)
            Interrupt:5

[Host: ~]$ arp -a

? (192.168.10.222) at ee:b4:2a:8d:6c:00 [ether] on eth0

[Host: ~]$ ping 192.168.10.222

PING 192.168.10.222 (192.168.10.222) 56(84) bytes of data.
64 bytes from 192.168.10.222: icmp_seq=0 ttl=63 time=131 ms
64 bytes from 192.168.10.222: icmp_seq=1 ttl=63 time=159 ms
--- 192.168.10.222 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1003ms
rtt min/avg/max/mdev = 131.078/145.266/159.454/14.188 ms, pipe 2
```

- 查看主机PC2上的输出结果：

```
[Host:~]$ ifconfig eth0

eth0        Link encap:Ethernet    HWaddr 2A:65:96:18:57:FA
            inet addr:192.168.10.222    Bcast:192.168.10.255    Mask:255.255.255.0
            UP BROADCAST RUNNING MULTICAST    MTU:1600    Metric:1
            RX packets:19 errors:0 dropped:0 overruns:0 frame:0
            TX packets:20 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:1148 (1.1 KiB)    TX bytes:1524 (1.4 KiB)
            Interrupt:5

[Host:~]$ arp -a

? (192.168.10.111) at ee:b4:2a:8d:6c:00 [ether] on eth0

[Host: ~]$ ping 192.168.10.111

PING 192.168.10.111 (192.168.10.111) 56(84) bytes of data.
64 bytes from 192.168.10.111: icmp_seq=0 ttl=63 time=198 ms
```

```
64 bytes from 192.168.10.111: icmp_seq=1 ttl=63 time=140 ms
64 bytes from 192.168.10.111: icmp_seq=2 ttl=63 time=146 ms
--- 192.168.10.111 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2008ms
rtt min/avg/max/mdev = 140.196/161.959/198.912/26.267 ms, pipe 2
```

2 DHCP Client 配置

2.1 DHCP Client 简介

DHCP（Dynamic Host Configuration Protocol）Client 通过 DHCP 协议从 DHCP Server 动态获得 IP 地址和配置参数。若客户端和服务器都在一个子网内，则客户端和服务器之间可以直接进行 DHCP 协议的交互，否则需要有 DHCP Relay Agent 转发 DHCP 消息。

DHCP Client 通过 DHCP 广播报文向 DHCP Server 请求 IP 地址，在获得 IP 地址和相应的租期后，配置地址并设置租期的时间。在租期过半的时候开始发送 DHCP 报文请求继续使用当前的 IP 地址，并期望获得新的租期。在成功续租后，DHCP Client 更新租期的时间。

2.2 开启 DHCP Client 功能

2.2.1 配置接口启用 DHCP Client 功能

配置在接口上通过 DHCP 协议获取 IP 地址的功能。如果接口处于打开状态，则立即开始通过 DHCP 获得 IP 地址。

表 2-1 配置接口启用 DHCP Client 功能

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
ip address dhcp	配置接口启用 DHCP Client 功能	缺省情况下，接口未启用 DHCP Client 功能

2.2.2 配置管理口启用 DHCP Client 功能

配置在管理口上通过 DHCP 协议获取 IP 地址的功能。

表 2-2 配置管理口启用 DHCP Client 功能

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
management ip address dhcp	配置管理口启用 DHCP Client 功能	缺省情况下，管理口未启用 DHCP Client 功能

2.3 配置 DHCP Client 属性

2.3.1 配置 DHCP Client 主机名

此命令需要在 **ip address dhcp** 之前执行，否则只有配置下一条 **ip address dhcp** 命令后才会生效。

表 2-3 配置 DHCP Client 主机名

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
dhcp client hostname *word*	配置 DHCP Client 的主机名	word: 主机名称 缺省情况下，使用系统主机名称

2.3.2 配置接口使用的 DHCP Client ID

该命令需要在 **ip address dhcp** 之前执行，否则只有配置下一条 **ip address dhcp** 命令后才会生效。

表 2-4 配置接口使用的 DHCP Client ID

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
dhcp client client-id { **ascii** *word* | **hex** *hex-string* | **vlan** *vlan-id* | **agg** *port-number* | *if-name* }	配置接口使用的 DHCP Client ID	word: ASCII 字符串 hex-string: 十六进制字符串

命令	操作	说明
		vlan-id: VLAN 接口号，取值范围为 1~4094 port-number: 聚合端口号，取值范围为 1~55 缺省采用格式“Switch-HWADDR-IFNAME”

2.3.3 配置 DHCP Class ID

DHCP Client 使用 Class ID 标记所需的配置参数类型。不同的厂商会定义自己的 Class ID，标记其特殊配置，DHCP Client 通过 Class ID 向 Server 请求这些与厂商相关的配置参数。此命令需要在 **ip address dhcp** 之前执行，否则只有配置下一条 **ip address dhcp** 命令后才会生效。

表 2-5 配置 DHCP Class ID

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
dhcp client class-id { *word* | **hex** *hex-string* }	配置组播组成员快速离开的功能	word: ASCII 字符串 hex-string: 十六进制字符串

2.4 配置 DHCP Client 的期望租期

配置 DHCP Client 期望获得的租期，DHCP Server 可以接受该租期，也可以忽略 Client 的请求，分配自己设置的租期。此命令需要在 **ip address dhcp** 之前执行，否则只有配置下一条 **ip address dhcp** 命令后才会生效。

表 2-6 配置 DHCP Client 的期望租期

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称

命令	操作	说明
dhcp client lease [*days* | *hours* | *minutes*] * [**infinite**]	配置 DHCP Client 的期望租期	days: 租期时间，单位：天 hours: 租期时间，单位：小时 minutes: 租期时间，单位：分钟 如选定关键字 **infinite**，则表示租期时间为永久

2.5 配置 DHCP Client 请求的选项信息

此命令向 DHCP Server 请求指定的配置参数，可以分多次指定所需要的参数，也可以一次指定所有需要的参数。此命令需要在 **ip address dhcp** 之前执行，否则只有配置下一条 **ip address dhcp** 命令后才会生效。

表 2-7 DHCP 报文的选项信息说明

选项号	字段名	说明
3	router	默认路由器选项
33	static-route	静态路由选项
121	classless-static-route	无类静态路由选项
249	classless-static-route-ms	Microsoft 无类静态路由选项
150	tftp-server-address	TFTP 服务器 IP 地址选项
6	dns-nameserver	DNS 服务器选项
15	domain-name	域名选项
44	netbios-nameserver	NetBIOS 服务器选项
43	vendor-specific	厂商相关配置选项

选项 33、121、249 之间存在优先级关系：选项 121 优先于选项 33 和选项 249，选项 249 优先于选项 33。

表 2-8 配置 DHCP Client 请求的选项信息

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
dhcp client request [**router** | **static-route** | **classless-static-route** | **classless-static-route-ms** | **tftp-server-address** | **dns-nameserver** | **domain-name** | **netbios-nameserver** | **vendor-specific**]	配置 DHCP Client 请求的选项信息	router、static-route、classless-static-route、classless-static-route-ms、tftp-server-address 为默认请求

2.6 显示与维护

表 2-9 显示与维护

命令	操作	说明
show dhcp client [**management** | **vlan** *vlan-id* | **agg** *port-number* | *if-name*] [**verbose**]	显示 DHCP Client 的工作状态	vlan-id: VLAN 接口号，取值范围为 1~4094 port-number: 聚合端口号，取值范围为 1~55 if-name: 物理接口及名称
show dhcp client statistics	查看 DHCP Client 统计信息	-
clear dhcp client statistics	清除 DHCP Client 计数器	-

2.7 配置举例

2.7.1 配置步骤

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式

命令举例	操作步骤
Switch(config-if)# no switchport	将接口配置为三层接口
Switch(config-if)# no shutdown	使能接口
Switch(config-if)# no dhcp client request static-route	取消 static-route 选项请求
Switch(config-if)# ip address dhcp	启用 DHCP Client
Switch(config-if)# end	退出至特权模式

2.7.2 命令验证

- 查看接口上的配置信息：

```
Switch# show running-config interface eth-0-1

Building configuration...
!
interface eth-0-1
  no switchport
  ip address dhcp
  no dhcp client request static-route
!
```

- 显示DHCP Client的工作状态：

```
Switch# show dhcp client verbose

DHCP client informations:
============================================================
eth-0-1 DHCP client information:
   Current state: BOUND
   Allocated IP: 4.4.4.199 255.255.255.0
   Lease/renewal/rebinding: 1187/517/1037 seconds
   Lease from 2011-11-18 05:59:59 to 2011-11-18 06:19:59
   Will Renewal in 0 days 0 hours 8 minutes 37 seconds
   DHCP server: 4.4.4.1
   Transaction ID: 0x68857f54
   Client ID: switch-7e39.3457.b700-eth-0-1
```

- 显示DHCP Client的统计信息：

```
Switch# show dhcp client statistics

DHCP client packet statistics:
============================================================
```

```
DHCP OFFERS       received: 1
DHCP ACKs         received: 2
DHCP NAKs         received: 0
DHCP Others       received: 0
DHCP DISCOVER     sent: 1
DHCP DECLINE      sent: 0
DHCP RELEASE      sent: 0
DHCP REQUEST      sent: 2
DHCP packet send failed: 0
```

3 DHCP Relay 配置

3.1 DHCP Relay 简介

DHCP 服务器和客户端都在一个子网内，则客户端和服务器之间可以直接进行 DHCP 协议的交互，这时不需要启动 DHCP Relay 功能。如果 DHCP 服务器和客户端不在一个子网内，则需要启动 DHCP Relay 功能将 DHCP 报文转发到外部的 DHCP 服务器。

DHCP Relay 转发同正常的 IP 路由转发不同，IP 路由转发的 IP 数据包在网络之间透明交换，而 DHCP Relay 代理接收 DHCP 消息同时产生一个新的 DHCP 消息发送到另一个接口。DHCP Relay 代理在报文中设置网关地址，添加中继代理信息（Option82），转发到 DHCP 服务器端。通过 DHCP Relay 代理，在收到服务器响应的消息时，会移除消息中 Option82 内容后，再转发给客户端。

3.2 开启 DHCP 功能

service dhcp 命令是 DHCP 相关命令的总开关，只有执行 **service dhcp** 命令使能 DHCP 服务，DHCP Snooping、DHCP Relay 等 DHCP 功能才会生效。

3.2.1 使能 DHCP 服务

表3-1 使能DHCP服务

命令	操作	说明
configure terminal	进入全局配置模式	-
service dhcp enable	使能 DHCP 功能	缺省情况下，未使能 DHCP 功能

3.2.2 开启 DHCP Relay 服务

在启用 DHCP Relay 服务前，需先使用 **service dhcp** 命令使能 DHCP 功能，DHCP Relay 功能在系统使能 DHCP 功能后才生效。

表3-2 开启DHCP Relay服务

命令	操作	说明
configure terminal	进入全局配置模式	-
service dhcp enable	使能 DHCP 功能	缺省情况下，未使能 DHCP 功能
dhcp relay	使能 DHCP Relay 服务	缺省情况下，未使能 DHCP 中继功能

3.3 创建 DHCP 服务器组

可以在全局配置模式和接口配置模式下创建 DHCP 服务器组。注意 DHCP Server 功能和 DHCP Snooping 功能不要在同一个 VLAN 上设置。

3.3.1 全局配置 DHCP 服务器组

表3-3 全局配置DHCP服务器组

命令	操作	说明
configure terminal	进入全局配置模式	-
dhcp-server *number server-list*	创建 DHCP 服务器组	number: DHCP 服务器组的序号，取值范围为 1~16 server-list: 加入服务器组中的 DHCP 服务器的 IP 地址列表。一个服务器组下 DHCP 服务器个数的范围为 1~16

3.3.2 接口配置 DHCP 服务器组

表 3-4 接口配置 DHCP 服务器组

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
dhcp-server *number*	接口模式下配置 DHCP 服务器组	number: DHCP 服务器组的序号，取值范围为 1~16

3.4 配置接口启用 DHCP Relay Option 82 功能

如果接口开启 DHCP 中继 Option 82 功能，DHCP 服务器会对携带该选项信息的报文予以响应，收到的 DHCP DISCOVER 或者 DHCP REQUEST 报文会按照普通的 DHCP 中继操作被转发到 DHCP 服务器组所配置的地址。

表 3-5 配置接口启用 DHCP Relay Option 82 功能

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
dhcp relay information trusted	配置接口为 DHCP 中继代理信息选项的信任源接口	缺省情况下，接口未启用 DHCP Relay Option 82 功能

3.5 显示与维护

表 3-6 显示与维护

命令	操作	说明
show dhcp-server	查看 DHCP 服务器组的配置信息	-
show dhcp relay interfaces	显示 DHCP 服务器组下的接口属性	-
show dhcp relay information config	显示 DHCP 中继信息（Option 82 选项）配置信息	-
show dhcp relay information trusted-sources	显示所有接口是否配置为 DHCP 中继信息选项的信任源信息	-
show dhcp relay statistics	显示交换机中继的 DHCP 报文统计信息	-
clear dhcp relay statistics	清除交换机中继的 DHCP 报文统计信息	-

3.6 配置举例

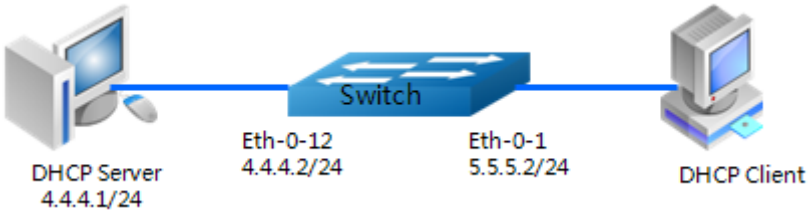
3.6.1 介绍

下图为测试 DHCP 中继代理功能的网络拓扑，需要两台 PC 机和一台交换机构建测试环境。

- 计算机 A 作为 DHCP 服务器
- 计算机 B 作为 DHCP 客户端
- 交换机作为 DHCP 中继代理

3.6.2 拓扑

图 3-1 DHCP Relay 拓扑图



3.6.3 配置步骤

1. 配置接口 eth-0-12

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-12	进入接口配置模式
Switch(config-if)# no switchport	将接口设置三层接口
Switch(config-if)# ip address 4.4.4.2/24	设置 IP 地址
Switch(config-if)# no shutdown	使能接口
Switch(config-if)# exit	退出接口配置模式

2. 配置 DHCP 服务器组

命令举例	操作步骤
Switch(config)# dhcp-server 1 4.4.4.1	创建 DHCP 服务器组

3. 配置接口 eth-0-1

命令举例	操作步骤
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# no switchport	将接口设置三层接口.
Switch(config-if)# ip address 5.5.5.2/24	设置 IP 地址
Switch(config-if)# no shutdown	使能接口
Switch(config-if)# dhcp relay information trusted	设置接口启用 DHCP 中继 Option 82 功能
Switch(config-if)# dhcp-server 1	设置 DHCP 服务器
Switch(config-if)# exit	退出接口配置模式

4. 使能 DHCP 中继服务

命令举例	操作步骤
Switch(config)# service dhcp enable	使能 DHCP 服务器
Switch(config)# dhcp relay	使能 DHCP Relay 功能

3.6.4 命令验证

1. 检查接口配置

```
Switch# show running-config interface eth-0-12

!
interface eth-0-12
 no switchport
 ip address 4.4.4.2/24
!
Switch# show running-config interface eth-0-1
!
interface eth-0-1
 no switchport
 dhcp relay information trusted
 dhcp-server 1
 ip address 5.5.5.2/24
!
```

2. 检查 DHCP 服务器的状态

```
Switch# show services

Networking services configuration:
Service Name              Status
============================================================
```

```
dhcp                    enable
```

3. 检查 DHCP 服务器组的配置

```
Switch# show dhcp-server

DHCP server group information:
=========================================================
group 1 ip address list:
[1] 4.4.4.1
```

4. 检查 DHCP 中继统计信息

```
Switch# show dhcp relay statistics

DHCP relay packet statistics:
=========================================================
Client relayed packets:    20
Server relayed packets:    20
Client error packets:      20
Server error packets:      0
Bogus GIADDR drops:        0
Bad circuit ID packets:    0
Corrupted agent options:   0
Missing agent options:     0
Missing circuit IDs:       0
```

5. 检查计算机从 DHCP 服务器获取的 IP 地址

```
Ipconfig /all

Dhcp Enabled. . . . . . . . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . . . . . . . . : 5.5.5.1
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 5.5.5.2
DHCP Server . . . . . . . . . . . : 4.4.4.1
DNS Servers . . . . . . . . . . . : 4.4.4.1
```

4 DHCP Server 配置

4.1 DHCP Server 简介

DHCP Server 通过 DHCP 协议为 Client 提供 IP 地址和网络配置参数。为了能够给客户端提供 DHCP 服务，DHCP Server 需要完成一些基本的配置，例如，地址池的分配、默认网关的设置、网络参数的设置等。在实际工作时，DHCP Server 会从设置的地址池内找到可用的地址分配给请求地址的 DHCP Client，同时，将 Client 请求的网络配置参数发送给 Client。这些分配的地址和参数都有一个有效期限（租约），Client 需要在到期之前向 Server 发出续约请求，保留自己的 IP 地址，同时更新租约。

在实际环境中，若 DHCP Server 和 DHCP Client 在同一子网内，则 DHCP Server 在直接相连后就可以正常工作。若它们不在同一网段内，则 DHCP Server 需要 DHCP Relay 协助转发 DHCP 消息，才能为 Client 提供 DHCP 服务。

DHCP Server 支持的主要 Option 包括：bootfile-name、dns-server、domain-name、gateway、netbios-name-server、netbios-node-type、tftp-server-address。同时，支持部分 Raw Option。

4.2 开启 DHCP 功能

service dhcp 命令是 DHCP 相关命令的总开关，只有执行 **service dhcp** 命令使能 DHCP 服务，DHCP Server、DHCP Snooping、DHCP Relay 等 DHCP 功能才会生效。

表 4-1 开启 DHCP 功能

命令	操作	说明
configure terminal	进入全局配置模式	-
service dhcp enable	使能 DHCP 功能	缺省情况下，未使能 DHCP 功能

4.3 使能 DHCP Server 功能

4.3.1 全局使能 DHCP Server 功能

在使能 DHCP Server 功能前，必需先使用 **service dhcp** 命令使能 DHCP 功能，DHCP Server 功能要在系统使能 DHCP 功能后才生效。注意 DHCP Server 功能和 DHCP Snooping 功能不要在同一个 VLAN 上设置。

表 4-2 全局使能 DHCP Server 功能

命令	操作	说明
configure terminal	进入全局配置模式	-
service dhcp enable	使能 DHCP 功能	缺省情况下，未使能 DHCP 功能
dhcp-server	全局使能 DHCP Server 功能	缺省情况下，未使能 DHCP Server 功能

4.3.2 接口启用 DHCP Server 功能

表 4-3 接口启用 DHCP Server 功能

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
dhcp server enable	接口上启用 DHCP Server 功能	缺省情况下，接口上的 DHCP Server 模式处于关闭状态

4.4 配置 DHCP Server 的地址池

创建 DHCP 服务器的地址池后，会进入 DHCP 地址池配置模式。在 DHCP 地址池配置模式下，可以配置地址池的参数，例如，可分配的子网地址段、默认网关等。

4.4.1 创建 DHCP 地址池

表 4-4 创建 DHCP 地址池

命令	操作	说明
configure terminal	进入全局配置模式	-
dhcp pool *pool-name*	创建 DHCP 地址池，并进入 DHCP 地址池配置模式	pool-name: DHCP 地址池名称，需满足以下条件： 1) 名称长度范围 [1, 32) 2) 名称合法的字符 [0-9a-zA-Z.-_] 3) 名称必须以字母开头，字母或数字结束

4.4.2 配置静态绑定

该命令会使当前 DHCP 地址池成为静态地址池。每个静态地址池中，只能配置一条静态绑定地址。如果配置多条静态绑定地址，会覆盖之前的配置。

表 4-5 配置静态绑定

命令	操作	说明
configure terminal	进入全局配置模式	-
dhcp pool *pool-name*	创建 DHCP 地址池，并进入 DHCP 地址池配置模式	pool-name: DHCP 地址池名称，需满足以下条件： 1) 名称长度范围 [1, 32) 2) 名称合法的字符 [0-9a-zA-Z.-_], 3) 名称必须以字母开头，字母或数字结束
static-bind ip-address { *IP-ADDRESS wildcard-mask* | *ip-address*/*prefix-length* } { **mac-address** *MAC-ADDRESS* | **client-identifier** { **ascii** *ascii-string* | **hex** *hex-string* } }	配置静态绑定的地址	缺省情况下，未配置静态绑定的地址 IP-ADDRESS: IP 地址 wildcard-mask: 掩码地址 prefix-length: 掩码长度 MAC-ADDRESS: DHCP Client 的 MAC 地址

命令	操作	说明
		ascii-string: ASCII 形式的 Client ID hex-string: Hex String 形式的 Client ID
lease *days* [*hours*] [*minutes*]	（可选）配置地址池中分配地址的租约时间	days: 天数，取值范围为 0~365 hours: 小时数，取值范围为 0~23 minutes: 分钟数，取值范围为 0~59

4.4.3 配置可分配的地址段

该命令配置地址池中可分配的地址段。所有的主机地址都是可分配的，可以使用命令 **dhcp excluded-address** 禁止分配其中的地址。不同地址池的地址段不能有重叠，并且不能再配置静态绑定。

表 4-6 配置可分配的地址段

命令	操作	说明
configure terminal	进入全局配置模式	-
dhcp pool *pool-name*	创建 DHCP 地址池，并进入 DHCP 地址池配置模式	pool-name: DHCP 地址池名称，需满足以下条件： 1) 名称长度范围 [1, 32) 2) 名称合法的字符 [0-9a-zA-Z.-_] 3) 名称必须以字母开头，字母或数字结束
network { *ip-address wildcard-mask* | *ip-address/prefix-length* }	配置地址池中可分配的地址段	缺省情况下，未配置地址池中可分配的地址段 ip-address: IP 地址 wildcard-mask: 掩码地址 prefix-length: 掩码长度

4.4.4 配置默认网关地址

默认网关地址需要和地址池中的地址在同一子网内。最多可以设置 8 个默认网关地址。列表中地址按照先后顺序使用。

表 4-7 配置默认网关地址

命令	操作	说明
configure terminal	进入全局配置模式	-
dhcp pool *pool-name*	创建 DHCP 地址池，并进入 DHCP 地址池配置模式	pool-name: DHCP 地址池名称，需满足以下条件： 1) 名称长度范围 [1, 32) 2) 名称合法的字符 [0-9a-zA-Z.-_], 3) 名称必须以字母开头，字母或数字结束
gateway *ip-address* & <1-8>	配置默认网关地址	ip-address & <1-8>: IP 地址，最多可设置 8 个

4.4.5 配置 DHCP 客户端使用的域名

DHCP 客户端只需要输入部分域名，系统会自动添加设置的域名前缀。

表 4-8 配置 DHCP 客户端使用的域名

命令	操作	说明
configure terminal	进入全局配置模式	-
dhcp pool *pool-name*	创建 DHCP 地址池，并进入 DHCP 地址池配置模式	pool-name: DHCP 地址池名称，需满足以下条件： 1) 名称长度范围 [1, 32) 2) 名称合法的字符 [0-9a-zA-Z.-_], 3) 名称必须以字母开头，字母或数字结束
domain-name *name*	配置 DHCP 客户端使用的域名	缺省情况下，DHCP 地址池没有配置域名 name: DHCP 客户端使用的域名前缀，需满足以下条件： 1) 名称长度范围 [1, 64) 2) 名称合法的字符 [0-9a-zA-Z.-_] 3) 名称必须以字母开头，字母或数字结束

4.4.6 配置 DNS Server 的 IP 地址

表 4-9 配置 DNS Server 的 IP 地址

命令	操作	说明
configure terminal	进入全局配置模式	-
dhcp pool *pool-name*	创建 DHCP 地址池，并进入 DHCP 地址池配置模式	pool-name: DHCP 地址池名称，需满足以下条件： 1) 名称长度范围 [1, 32) 2) 名称合法的字符 [0-9a-zA-Z.-_] 3) 名称必须以字母开头，字母或数字结束
dns-server *ip-address*&<1-8>	配置 DNS 服务器的 IP 地址	缺省情况下，DHCP 地址池没有配置 DNS 服务器的 IP 地址 ip-address&<1-8>: DNS 服务器 IP 地址，最多可设置 8 个

4.4.7 配置 NetBIOS 节点类型

配置地址池中 NetBIOS 节点类型参数，可选的节点类型有：b-node（广播）、p-node（点到点）、m-node（mixed, 混合）、h-node（hybrid, 混合），推荐使用 h-node 模式。

表 4-10 配置 NetBIOS 节点类型

命令	操作	说明
configure terminal	进入全局配置模式	-
dhcp pool *pool-name*	创建 DHCP 地址池，并进入 DHCP 地址池配置模式	pool-name: DHCP 地址池名称，需满足以下条件： 1) 名称长度范围 [1, 32) 2) 名称合法的字符 [0-9a-zA-Z.-_] 3) 名称必须以字母开头，字母或数字结束
netbios-node-type { **b-node | p-node | m-node | h-node** }	配置 NetBIOS 节点类型	缺省情况下，未配置 NetBIOS 节点类型

4.4.8 配置 TFTP 服务器地址及启动文件名

通过配置地址池中的 TFTP 服务器地址和启动文件名称，DHCP 客户端可以从 TFTP 服务器请求启动文件，完成自动配置。

表 4-11 配置 TFTP 服务器地址及启动文件名

命令	操作	说明
configure terminal	进入全局配置模式	-
dhcp pool *pool-name*	创建 DHCP 地址池，并进入 DHCP 地址池配置模式	pool-name: DHCP 地址池名称，需满足以下条件： 1) 名称长度范围 [1, 32) 2) 名称合法的字符 [0-9a-zA-Z.-_] 3) 名称必须以字母开头，字母或数字结束
tftp-server-address *ip-address*&<1-8>	配置 TFTP 服务器地址	缺省情况下，未配置 TFTP 服务器地址 ip-address&<1-8>: TFTP 服务器 IP 地址，最多可设置 8 个
bootfile-name *name*	配置 DHCP 客户端需要的启动镜像文件名	name: 启动文件的文件名，需满足以下条件： 1) 名称长度范围[1, 64) 2) 名称合法的字符[0-9a-zA-Z.-_] 3) 名称必须以字母开头，字母或数字结束

4.4.9 配置 DHCP 地址池选项

DHCP 提供一个 TCP/IP 网络上的参数配置框架。不同的参数以 DHCP 选项的形式存储。

表 4-12 配置 DHCP 地址池选项

命令	操作	说明
configure terminal	进入全局配置模式	-
dhcp pool *pool-name*	创建 DHCP 地址池，并进入 DHCP 地址池配置模式	pool-name: DHCP 地址池名称，需满足以下条件：

命令	操作	说明
		1) 名称长度范围 [1, 32) 2) 名称合法的字符 [0-9a-zA-Z.-_] 3) 名称必须以字母开头，字母或数字结束
option *code* { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *IP-ADDRESS* }	配置 DHCP 地址池选项	code: DHCP 选项代码 ascii-string: ASCII 字符串 hex-string: 十六进制字符串 IP-ADDRESS: IP 地址

4.5 配置 IP 地址冲突检测

为防止 IP 地址发生冲突，DHCP Server 在分配地址之前会 ping 所要分配的地址。用户可以指定 ping 发出的包的个数，如果这些包都没有回应，则将地址分配给 DHCP Client，否则不回应。还能指定等待的时间，如果在指定时间内没有回应，则认为该地址没有被使用。

表 4-13 配置 IP 地址冲突检测

命令	操作	说明
configure terminal	进入全局配置模式	-
dhcp ping packets *number*	（可选）配置 DHCP Server 发送 ICMP 消息的个数	number: DHCP Server 发送 ICMP 消息的个数，取值范围为 0~10 缺省情况下，DHCP Server 发送 ICMP 消息的个数为 1
dhcp ping timeout *time*	（可选）配置 DHCP Server 等待 ICMP 响应报文的时间	time: DHCP Server 等待 ICMP 响应报文的时间，单位：秒 缺省情况下，超时等待时间为 1 秒

4.6 显示与维护

表 4-14 显示与维护

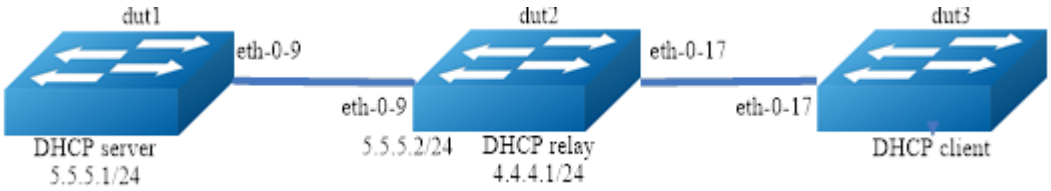
命令	操作	说明
show dhcp server conflict { **ip** *ip-address* | **all** }	显示发现并记录的冲突地址	ip-address: IP 地址 DHCP 服务器在分配地址之前，会检测地址是否已使用，并将冲突的地址记录下来
show dhcp server binding { **ip** *ip-address* | **pool** *pool-name* | **all** }	显示 DHCP 服务器中绑定的地址信息	ip-address: IP 地址 pool-name: 地址池名称 绑定地址的信息包括 IP 地址、MAC 地址、租约时间、地址类型
show dhcp server statistics	显示 DHCP 服务器统计信息	-
show dhcp server config	显示 DHCP 服务器配置信息	-
clear dhcp server conflict { **ip** *ip-address* | **all** }	清除记录的冲突地址	ip-address: IP 地址 pool-name: 地址池名称
clear dhcp server binding { **ip** *ip-address* | **pool** *pool-name* | **all** }	清除 DHCP 服务器数据库中动态绑定的地址	
clear dhcp server statistics	清除 DHCP 服务器统计信息	-

4.7 配置举例

4.7.1 拓扑

图 4-1 DHCP Server 基本拓扑图

图 4-2 DHCP Relay 参与的拓扑图



4.7.2 配置步骤

1. 如上图 4-1，分别对DUT1和DUT2进行配置

DHCP Server (DUT1):

命令举例	操作步骤
Switch#configure terminal	进入全局配置模式
Switch(config)#service dhcp enable	全局启用 DHCP 服务
Switch(config)#dhcp server	全局启用 DHCP Server
Switch(config)#dhcp pool pool5	创建 DHCP 地址池，并进入 DHCP 地址池配置模式
Switch(dhcp-config)#network 5.5.5.0/24	配置地址池中可分配的地址段
Switch(dhcp-config)#gateway 5.5.5.1	配置 Option：默认网关
Switch(dhcp-config)#exit	退出 DHCP 地址池配置模式
Switch(config)#interface eth-0-9	进入接口配置模式
Switch (config-if)#no switchport	将接口设置三层接口
Switch (config-if)# no shutdown	使能接口
Switch (config-if)# ip address 5.5.5.1/24	配置 IP 地址
Switch (config-if)# dhcp server enable	启用 DHCP Server
Switch (config-if)#exit	退出接口配置模式

DHCP Client (DUT2):

命令举例	操作步骤
Switch#configure terminal	进入全局配置模式
Switch(config)#interface eth-0-9	进入接口配置模式

命令举例	操作步骤
Switch (config-if)#no switchport	将接口设置三层接口
Switch (config-if)# no shutdown	使能接口
Switch (config-if)# ip address dhcp	启用 DHCP Client
Switch (config-if)#exit	退出接口配置模式

2. 如上图 4-2，分别对DUT1、DUT2和DUT3进行配置

DHCP Server (DUT1):

命令举例	操作步骤
Switch#configure terminal	进入全局配置模式
Switch(config)#service dhcp enable	全局启用 DHCP 服务
Switch(config)#dhcp server	全局启用 DHCP Server
Switch(config)#dhcp pool pool4	创建 DHCP 地址池，并进入 DHCP 地址池配置模式
Switch(dhcp-config)#network 4.4.4.0/24	配置地址池中可分配的地址段
Switch(dhcp-config)#gateway 4.4.4.1	配置 Option：默认网关
Switch(dhcp-config)#exit	退出 DHCP 地址池配置模式
Switch(config)#ip route 4.4.4.0/24 5.5.5.2	添加路由
Switch(config)#interface eth-0-9	进入接口配置模式
Switch (config-if)#no switchport	将接口设置三层接口
Switch (config-if)# no shutdown	使能接口
Switch (config-if)# ip address 5.5.5.1/24	配置 IP 地址
Switch (config-if)# dhcp server enable	启用 DHCP Server
Switch (config-if)#exit	退出接口配置模式

DHCP Relay (DUT2):

命令举例	操作步骤
Switch#configure terminal	进入全局配置模式
Switch(config)#service dhcp enable	全局启用 DHCP 服务
Switch(config)#dhcp relay	全局启用 DHCP Relay

命令举例	操作步骤
Switch(config)#dhcp-server 1 5.5.5.1	添加 DHCP Server 组
Switch(config)#interface eth-0-17	进入接口配置模式
Switch (config-if)#no switchport	将接口设置成三层口
Switch (config-if)# no shutdown	使能接口
Switch (config-if)# ip address 4.4.4.1/24	配置 IP 地址
Switch (config-if)# dhcp-server 1	选择 DHCP Server 组
Switch (config-if)#interface eth-0-9	进入接口配置模式
Switch (config-if)#no switchport	将接口设置成三层接口
Switch (config-if)# no shutdown	使能接口
Switch (config-if)# ip address 5.5.5.2/24	配置 IP 地址
Switch (config-if)#exit	退出接口配置模式

DHCP Client (DUT3):

命令举例	操作步骤
Switch#configure terminal	进入全局配置模式
Switch(config)#interface eth-0-17	进入接口配置模式
Switch (config-if)#no switchport	将接口设置三层接口
Switch (config-if)# no shutdown	使能接口
Switch (config-if)# ip address dhcp	启用 DHCP Client
Switch (config-if)#exit	退出接口配置模式

4.7.3 命令验证

1. 显示图 4-1中的配置结果：

- 查看DHCP Server的详细配置信息：

```
Switch# show running-config
!
service dhcp enable
!
interface eth-0-9
```

```
 no switchport
 dhcp server enable
 ip address 5.5.5.1/24!
!
dhcp server
dhcp pool pool5
 network 5.5.5.0/24
 gateway 5.5.5.1
```

- 查看DHCP Client的详细配置信息：

```
Switch# show dhcp client verbose

DHCP client informations:
============================================================
eth-0-9 DHCP client information:
   Current state: BOUND
   Allocated IP: 5.5.5.2 255.255.255.0
   Lease/renewal/rebinding: 1194/546/1044 seconds
   Lease from 2012-02-04 07:40:12 to 2012-02-04 08:00:12
   Will Renewal in 0 days 0 hours 9 minutes 6 seconds
   DHCP server: 5.5.5.1
   Transaction ID: 0x45b0b27b
   Default router: 5.5.5.1
   Classless static route:
      Destination: 5.5.4.0, mask: 255.255.255.0, Nexthop: 5.5.5.1
   TFTP server addresses: 5.5.5.3
Client ID: switch-6e6e.361f.8400-eth-0-9
```

- 查看DHCP Server的统计信息：

```
Switch# show dhcp server statistics

DHCP server packet statistics:
============================================================
Message Received:
BOOTREQUEST:    0
DHCPDISCOVER:    1
DHCPREQUEST:    1
DHCPDECLINE:    0
DHCPRELEASE:    0
DHCPINFORM:    0
Message Sent:
BOOTREPLY:    0
DHCPOFFER:    1
DHCPACK:    1
DHCPNAK:    0
```

- 查看DHCP Server地址分配及接口信息：

```
Switch# show dhcp server binding all
 IP address      Client-ID/              Lease expiration          Type
                   Hardware address
 5.5.5.2         6e:6e:36:1f:84:00       Sat 2012.02.04 08:00:12   Dynamic

Switch# show dhcp server interfaces

List of DHCP server enabled interface(s):
DHCP server service status: enabled
Interface Name
============================================================
eth-0-9
```

2. 显示图 4-2中的配置结果：

- 查看DHCP Relay的验证信息：

```
Switch# show running-config

!
service dhcp enable
!
interface eth-0-9
  no switchport
  dhcp server enable
  ip address 5.5.5.1/24!
!
ip route 4.4.4.0/24 5.5.5.2
!
dhcp server
dhcp pool pool4
  network 4.4.4.0/24
  gateway 4.4.4.1
```

- 查看DHCP Client的详细配置信息：

```
Switch# show dhcp client verbose

DHCP client informations:
============================================================
eth-0-17 DHCP client information:
    Current state: BOUND
    Allocated IP: 4.4.4.5 255.255.255.0
    Lease/renewal/rebinding: 1199/517/1049 seconds
    Lease from 2012-02-06 05:23:09 to 2012-02-06 05:43:09
```

```
Will Renewal in 0 days 0 hours 8 minutes 37 seconds
DHCP server: 5.5.5.1
Transaction ID: 0x192a4f7d
Default router: 4.4.4.1
Classless static route:
   Destination: 5.5.4.0, mask: 255.255.255.0, Nexthop: 4.4.4.1
TFTP server addresses: 5.5.5.3
Client ID: switch-3c9a.b29a.ba00-eth-0-17
```

- 查看DHCP Server的统计信息：

```
Switch# show dhcp server statistics

DHCP server packet statistics:
=============================================================
Message Received:
BOOTREQUEST:    0
DHCPDISCOVER:    1
DHCPREQUEST:    1
DHCPDECLINE:    0
DHCPRELEASE:    0
DHCPINFORM:    0
Message Sent:
BOOTREPLY:    0
DHCPOFFER:    1
DHCPACK:    1
DHCPNAK:    0
```

- 查看DHCP Server地址分配及接口信息：

```
Switch# show dhcp server binding all

IP address        Client-ID/                Lease expiration                Type
                      Hardware address
 4.4.4.5           3c:9a:b2:9a:ba:00       Mon 2012.02.06 05:43:09         Dynamic

Switch# show dhcp server interfaces

List of DHCP server enabled interface(s):
DHCP server service status: enabled
Interface Name
=============================================================
eth-0-9
```

5 DNS 配置

5.1 DNS 简介

DNS 是域名系统(Domain Name System)的缩写，通过这个分布式数据库，用户可以将主机名称映射到 IP 地址，将域名映射到 IP 地址的过程称为域名解析。由于一个主机可能存在多个 IP 地址，为了方便记忆，在交换机上配置 DNS 时，可以使用与 IP 相关的命令，如 **ping**、**telnet** 以及 Telnet 支持的其他相关操作，通过主机名替代 IP 地址的方式可以提高可读性。配置域名时，需要使用点(.)分隔。

如果要解析域名，必须要定义一个域名服务器，该服务器保存了将域名解析为 IP 地址的域名缓存或数据库。为了能够将域名解析为 IP 地址，用户必须指定本网络中有效的服务器，然后再启用 DNS。

5.2 配置 DNS

5.2.1 配置域名解析

如需对域名进行解析，需要配置域名服务器。下表的命令最多能添加三个域名解析服务器。如果指定源接口或者源 IP 地址，将会使用对应的 IP 地作为发出报文的源 IP 地址。如果当前域名缓存中不存在此对应关系，系统会自动创建。

表 5-1 配置域名解析

命令	操作	说明
configure terminal	进入全局配置模式	-
dns domain *domain-name*	在域名系统(DNS)下设置一个缺省域名	缺省情况下，为配置缺省域名 domain-name: 域名
dns server *ip-address* [**source-interface** *if-name* | **source-ip** *source-ip-address*]	在域名系统(DNS)的域名服务器列表中新增一个域名服务器	缺省情况下，域名服务器列表中不存在域名服务器 ip-address: 域名服务器的 IP 地址

命令	操作	说明
		if-name: 源接口名称 source-ip-address: 源 IP 地址
ip host *hostname ip-address*	在域名系统(DNS)中设置主机名及其对应的 IP 地址	缺省情况下，域名缓存中无静态配置的主机名及其对应的 IP 地址 hostname: 主机名 ip-address: 与主机名对应的 IP 地址

5.2.2 全局使能 DNS 功能

表 5-2 全局使能 DNS 功能

命令	操作	说明
configure terminal	进入全局配置模式	-
ip dns server	全局使能 DNS 功能	缺省情况下，全局 DNS 功能处于关闭状态

5.3 显示与维护

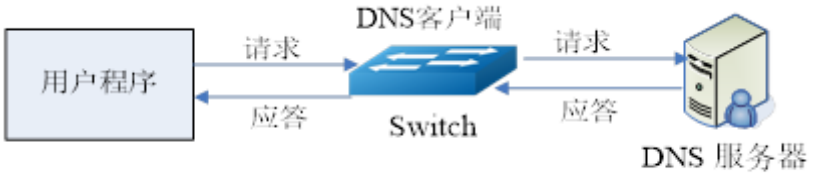
表 5-3 显示与维护

命令	操作	说明
show dns { **domain** | **server** }	显示域名系统(DNS)的配置信息	-
show ip host	显示指定 IP 主机的配置信息	-
show ip dns servers	显示 DNS 的状态及配置条目	使用本命令之前，必须用 **ip dns server** 命令打开 DNS 功能

5.4 配置举例

5.4.1 拓扑

图 5-1 DNS 典型拓扑图



5.4.2 配置步骤

命令举例	操作步骤
Switch#configure terminal	进入全局配置模式
Switch(config)#dns domain server1	定义一个默认域名系统的的名称，该程序将主机域名（非点分十进制的字符串）映射到 IP 地址
Switch(config)#dns server 202.100.10.20	配置域名系统(DNS)中的域名服务器的 IPv4 地址，域名系统用来解决内部的域名查询
Switch(config)# ip host www.example1.com 192.0.2.141	设置静态域名解析表中主机名及其对应的主机 IPv4 地址

5.4.3 命令验证

显示域名系统(DNS)的配置信息：

```
Switch# show dns server
Current DNS name server configuration:
        Server                  IP Address
------------------------------------------------------------
1       nameserver              202.100.10.20
```

6 NAT 配置

6.1 NAT 简介

NAT (Network Address Translation) 即网络地址转换，属接入广域网 (WAN) 技术，是将 IP 数据报文头中的 IP 地址转换为另一个 IP 地址的过程。NAT 主要用于实现内部网络（私有 IP 地址）访问外部网络（公有 IP 地址）的功能，通过这种转换的方式可以减少 IP 地址空间的使用，还能保护内部网络的计算机受到外部的攻击。

NAPT (Network Address Port Translation) 即网络地址端口转换，多应用于接入设备中，可以实现并发的地址转换。它允许多个内部地址映射到同一个公有地址上，因此也可以称为“多对一地址转换”或“地址复用”。NAPT 方式属于多对一的地址转换，它通过使用 IP 地址与端口号组合的形式进行转换，使多个私网的用户可共用一个公网 IP 地址访问外网。Basic NAT 是进行一对一 IP 地址的转换，而 NAPT 可以实现多个私有 IP 地址映射到同一个公有 IP 地址上。

6.2 使能 NAT 功能

使能内网 NAT 转换与使能外网 NAT 转换相对应，指明路由器工作时的数据流向。通过如下的命令，可以转换从外网向内网传输的 IP 数据包的源地址。使用对应的命令也可以转换从内网向外网方向传输的 IP 数据包的目标地址。

6.2.1 使能内网 NAT 转换

表 6-1 使能内网 NAT 转换

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
no switchport	配置接口为三层接口	-

命令	操作	说明
ip nat inside	使能内网 NAT 转换	缺省情况下，未使能 NAT 内网转换功能

6.2.2 使能外网 NAT 转换

表 6-2 使能外网 NAT 转换

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
no switchport	配置接口为三层接口	-
ip nat outside	使能外网 NAT 转换	缺省情况下，未使能 NAT 外网转换功能

6.3 全局配置源 NAT 条目

表 6-3 全局配置源 NAT 条目

命令	操作	说明
configure terminal	进入全局配置模式	-
ip nat-sa *inside-ip-address* **outside-ip** *outside-ip-address* [**dynamic** | **static**]	全局配置源 NAT 条目	inside-ip-address: 源 IP 地址 outside-ip-address: NAT 转换后的外网 IP 地址

6.4 全局配置目的 NAT 条目

1. 全局配置目的NAT条目（无端口号）

表 6-4 配置目的 NAT 条目（无端口号）

命令	操作	说明
configure terminal	进入全局配置模式	-
ip nat-da *outside-ip-address* **inside** *inside-ip-address*	全局配置目的 NAT 条目	outside-ip-address: 外网 IP 地址 inside-ip-address: NAT 转换后的内网 IP 地址

2. 全局配置目的NAT条目（有端口号及协议）

表 6-5 配置目的 NAT 条目（有端口号及协议）

命令	操作	说明
configure terminal	进入全局配置模式	-
ip nat-da *outside-ip-address outside-port-number* **protocol** { **tcp** | **udp** } *inside-ip-address inside-port-number*	全局配置目的 NAT 条目	outside-ip-address: 转换后的 IP 地址 outside-port-number: 转换后的端口，取值范围为 1~65535 inside-ip-address: 源 IP 地址 inside-port-number: 源端口，取值范围为 1~65535

6.5 配置 NAT 会话

6.5.1 配置 NAT 会话阈值

表 6-6 配置 NAT 会话阈值

命令	操作	说明
configure terminal	进入全局配置模式	-
nat session max-count *max-count-value*	配置 NAT 会话阈值	NAT 会话阈值，取值范围为 1000~5000，默认值为 3000

6.5.2 配置 NAT 老化定时器周期

表 6-7 配置 NAT 老化定时器周期

命令	操作	说明
configure terminal	进入全局配置模式	-
nat session aging-timer { **0** | *aging-timer-value* }	配置 NAT 老化定时器周期	0: NAT 会话不老化 NAT 会话老化时间，取值范围为 10~1000000，单位为秒，默认 60s

6.5.3 配置 NAT 会话同步

将本设备上的 NAT 会话同步到对端，即 MLAG 主用设备的 NAT 会话手动同步到 MLAG 备用设备。

表 6-8 配置 NAT 会话同步

命令	操作	说明
configure terminal	进入全局配置模式	-
nat session sync [*inside-ip-address*] [*inside-port-number*]	配置 NAT 会话同步	inside-ip-address: 源 IP 地址 inside-port-number: 源端口号

6.6 显示与维护

表 6-9 显示与维护

命令	操作	说明
show ip nat session [*inside-ip-address*]	显示全部或指定 IP 地址的 NAT 会话	inside-ip-address: 源 IP 地址
show ip nat session statistics	显示全部 NAT 会话统计信息	-
show resource nat	显示全部 NAT 资源使用信息	-

6.7 配置举例

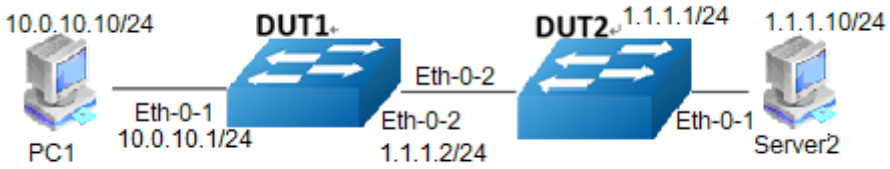
6.7.1 配置源 NAT

1. 介绍

Server 端开启 HTTP 或 Telnet 服务，从 PC1 左侧的 Client 端发起到 Server (1.1.1.10)的 Telnet 或 HTTP 请求（Client 端需有到 Server 服务端的路由），TCP 会话服务建立成功。在 DUT1 上 **show ip nat session** 可以查看到相应的会话建立成功。

2. 拓扑

图 6-1 源 NAT 配置拓扑图



3. 配置步骤

命令举例	操作步骤
Switch#configure terminal	进入全局配置模式
Switch(config)# vlan database	进入 VLAN 配置模式
Switch(config-vlan)# vlan 10,20	创建 VLAN10，20
Switch(config-vlan)# exit	退出 VLAN 配置模式
Switch(config)# ip nat-sa 10.0.10.100 outside-ip 1.1.1.2 dynamic	全局配置源 NAT 条目
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# switchport access vlan 10	添加 eth-0-1 到 VLAN 10
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface eth-0-2	进入接口配置模式
Switch(config-if)# switchport access vlan 20	添加 eth-0-2 到 VLAN 20
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface vlan 10	进入 VLAN 接口配置模式
Switch(config-if)# ip address 10.0.10.1/24	设置 VLAN 10 的 IP 地址
Switch(config-if)# ip nat inside	使能内网 NAT 转换功能

命令举例	操作步骤
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface vlan 20	进入 VLAN 接口配置模式
Switch(config-if)# ip address 1.1.1.2/24	设置 VLAN 20 的 IP 地址
Switch(config-if)# ip nat outside	使能外网 NAT 转换功能

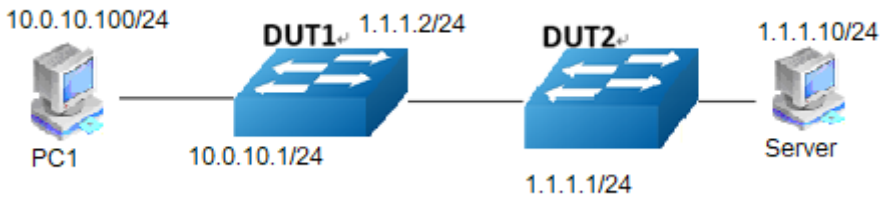
6.7.2 配置目的 NAT

1. 介绍

PC1 端开启 Telnet 服务（监听 TCP 的 23 端口），并配置有到外网 Server 端（1.1.1.10）的路由，从 Server 端（模拟外网）发起到 DUT1 的 1.1.1.2 的 Telnet 请求，查看 Telnet 会话建立成功。在 DUT1 上 **show ip nat session** 可以查看到相应的会话建立成功。

2. 拓扑

图 6-2 目的 NAT 配置拓扑图



3. 配置步骤

命令举例	操作步骤
Switch#configure terminal	进入全局配置模式
Switch(config)# vlan database	进入 VLAN 配置模式
Switch(config-vlan)# vlan 10,20	创建 VLAN10，20
Switch(config-vlan)# exit	退出 VLAN 配置模式
Switch(config)# ip nat-da 1.1.1.2 50 protocol tcp 10.0.10.100 23	配置到内网 Client 端 Telnet 服务（TCP 23 端口）

命令举例	操作步骤
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# switchport access vlan 10	添加 eth-0-1 到 VLAN 10
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface eth-0-2	进入接口配置模式
Switch(config-if)# switchport access vlan 20	添加 eth-0-2 到 VLAN 20
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface vlan 10	进入 VLAN 接口配置模式
Switch(config-if)# ip address 10.0.10.1/24	设置 VLAN 10 的 IP 地址
Switch(config-if)# ip nat inside	使能内网 NAT 转换功能
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface vlan 20	进入 VLAN 接口配置模式
Switch(config-if)# ip address 1.1.1.2/24	设置 VLAN 20 的 IP 地址
Switch(config-if)# ip nat outside	使能外网 NAT 转换功能

流量管理配置指导目录

1 QoS 配置

1.1 QoS 简介

QoS（Quality of Service，服务质量）是各种存在服务供需关系的场合中普遍存在的概念，它评估服务方满足客户服务需求的能力。评估通常不是精确的评分，而是注重分析在何种条件下服务的质量比较高，以及可能存在不足的情况，以便有针对性地改进。在因特网中，QoS 所评估的就是网络投递分组的服务能力。由于网络提供的服务是多样的，因此可以基于不同层面对 QoS 进行评估。通常所说的 QoS，是对分组投递过程中为延迟、延迟抖动、丢包率等核心需求提供支持的服务能力的评估。QoS 是网络的一种安全机制，是用来解决网络延迟和阻塞等问题的一种技术。在正常情况下，如果网络只用于特定的无时间限制的应用系统，并不需要 QoS，比如 Web 应用，或 E-mail 设置等。但是对关键应用和多媒体应用就十分必要。当网络过载或拥塞时，QoS 能确保重要业务量不受延迟或丢弃，同时保证网络的高效运行。

1.2 术语解释

以下是用来形容QoS的术语和概念的简要描述：

1. **访问控制列表**（ACLs）：具有相同特征的流量进行分类。IP ACL用来分类IP流量，MAC ACL用来分类除了IPv6和MPLS以外的所有流量。

2. **服务种类**（CoS）：在网络的第二层中确定报文优先级的字段。QOS可以通过设置不同的COS值来区分不同优先级的流量。802.1Q二层报文中可以携带2字节的VLAN标签，最高的3个比特用于用户指定的优先级。其它类型的报文不能携带VLAN标签。CoS有3个比特，取值范围为0~7。

3. **差分服务代码点**（DSCP）：有6个比特位，用来区分三层网络中的报文的优先级。DSCP值范围是0~63。

4. **IP-Precedence**：有3个比特位，用来区分三层网络中报文的优先级。IP-Precedence的取值范围为0~7。

5. **EXP**：有3个比特位，用来区分MPLS网络中的报文的优先级。MPLS EXP的取值范围为0~7。

6. **流分类**（Traffic Classification）：指采用一定的规则识别出符合某类特征的报文。分类规则（Classification Rule）是用户根据管理需求配置的过滤规则。报文进入系统时，流分类处理引擎会为报文分配一个内部优先级，基于这个优先级，系统对报文进行一系列的处理。系统可以基于报文中的CoS、inner-CoS、DSCP、IP-Precedence，或者端口上的配置的默认CoS，或者依据policy-map配置映射出的内部优先级。

7. **流量整形**（Shaping）：是通过缓存报文来改变并调节入方向的流速率，从而使出方向的流速率表现得更加平滑的一种方法。当入方向的流量出现高突发的时候，就需要将报文缓存并在后面发送，从而使出方向的流更加平滑，因此Shaping可能会增加报文的抖动。

   流量整形可以应用在以下角色：

   物理接口（Port Shaping）

   出方向的队列（Queue Shaping）

   当 Queue 应用双速率的 Shaping 时，需要保证该接口下所有 Queue 的 CIR 之和不大于端口速率，并且不大于接口 Shaping 的速率。

8. **流量监管**（Policing）：会对流量进行测速，从而决定报文是保证速率内还是保证速率外，保证速率外的流量可能会被丢弃。

   系统支持两种类型的策略器（Policer）：

   配置在 class-map 中，用于对匹配某个 class-map 的流量限制带宽。

   配置一个聚合 Policer，用户可以将匹配 class-map 的流量加入这个 Policer 中。聚合 Policer 限制的是其中所有流量的带宽。

9. **标记**（Marking）：定义了对超出保证速率的流量的处理行为。系统采用两种行为中的一种：给报文标记颜色，后面会继续处理；直接丢弃报文。标记能够在进口和出口方向使用。
10. **队列**（Queueing）：Basic和Enterprise模式下每个出端口有8个队列，范围为0~7，优先级最高是7，最低是0。Enterprise Advance模式下每个出端口有12个队列，范围为0~11，其中0~7是单播流量队列，8~11是组播流量队列，单播流量队列中优先级最高是7，最低是0。组播流量队列中优

先级最高的是11，最低是8。每个Queue中支持3个丢弃优先级。队列长度的单位是缓冲单元（Buffer Cell）。Buffer Cell是报文的存储粒度单位，其大小为256字节，报文越大，占用的缓冲单元越多。

11. **队尾丢弃算法**（Tail Drop）：是一种简单的丢弃算法，即队列中报文达到一定阈值（可配置）时，后来的报文会被丢弃。默认情况下，端口上的丢弃算法就是Tail Drop。系统支持在每个端口上为每个Queue丢弃的优先级制定一个Tail Drop的阈值。

12. **加权随机先期检测**（WRED：Weighted Random Early Detection）：可以提前以一定概率丢弃报文，达到避免拥塞的目的，通过提前丢弃报文，WRED模式可以避免短时间内丢弃大量报文，导致大量TCP连接同时触发慢启动和拥塞退避，网络带宽利用率瞬间降低的现象。系统支持在端口上为每个Queue丢弃的优先级制定两个阈值。这两个阈值前者小于后者。当队列中报文达到前者时报文开始丢弃，队列中报文越多，丢弃概率越大。当队列中报文大于后一阈值时，报文全部丢弃。

13. **调度**（Scheduling）：系统为每个队列分配一个优先级（Class），范围是0~7，数字越高表示优先级越高。Basic模式下端口上的8个队列的优先级是可配置的。

    一个端口上，不同的优先级之间使用的 SP 调度，即高优先级队列先被调度，当高优先级队列为空时才会调度低优先级队列。相同的优先级内的队列采用 WDRR 调度。用户可以为各个队列设置权重。

    说明

    启用 QoS 时，Basic 模式下队列 0 到 7 对应的优先级为：0/1/2/3/4/5/6/7；Enterprise 模式下队列 0 到 7 对应的优先级为：3/3/4/4/4/4/5/7；Enterprise Advance 模式下队列 0 到 11 对应的优先级为：3/3/4/4/4/4/5/7/0/1/2/3。禁用 QoS 时，所有队列的优先级均为 0。

    启用 QoS 时，Basic 模式下队列 0 到 7 对应的 WDRR 权重为：1::1:1:1:1:1:1:1；Enterprise 模式下队列 0 到 7 对应的 WDRR 权重为：1:1:4:10:10:10:1:1；Enterprise Advance 模式下队列 0 到 11 对应的 WDRR 权重为：1:1:4:10:10:10:1:1:1:1:1:1。

14. **类映射**（Class Map）：通过指定一些ACL定义一组流。这些ACL可以是match-all或match-any，分

别表示流量要同时匹配所有的ACL或匹配任意的ACL。

15. **策略映射**（Policy Map）：用来指定不同种类流量的具体行为，可实现如下需求：

将流按照指定的优先级和颜色区分出来

为相应的优先级和颜色设置指定的信任策略

为满足某个信任策略的流按照预先的配置进行流量监管

为指定的流做重定向

为指定的流做镜像

为指定的流做统计

Policy Map 有如下属性：

一个 Policy Map 可以包含多个流分类定义，并给出单独的行为

每一个流分类定义可以匹配接口上的每一种流量

每一个端口的每一个方向只能应用一个 Policy Map。相同的 Policy Map 可以在不同端口的不同方向上应用。

Policy Map 必须附加到一个端口上才能生效。

一个 Policy Map 可以应用于物理接口（非聚合端口成员），聚合端口以及 VLAN 接口。

16. **映射表**（Mapping Table）：在QoS处理中，交换机将所有流量都映射到内部优先级处理。

在流分类时，QoS 使用可配置的映射表进行报文映射，内部优先级共 6 个比特，是从 CoS、EXP、DSCP、IP-Precedence 的值映射而来，这些映射表包含了 CoS-Priority-Color/COS-PHB 表、EXP-Priority-Color/EXP-PHB 表、DSCP-Priority-Color/DSCP-PHB 表和 IP-Precedence-Priority-Color/IP-PREC-PHB。

在流量监管时，QoS 给报文分配一个新的优先级和颜色，比如依据 Class-Map。

当流量结束调度阶段后，如果替换 CoS 或者 DSCP 被搁置，那么 QoS 使用 Priority-Color-Cos/PHB-COS 或者 Priority-Color-DSCP/PHB-DSCP 根据内部的优先级和颜色重新映射到 CoS 或者 DSCP

每一个 QoS 域的上述行为不一致

17. **时间范围**（Time Range）：通过使用Time-Range，Class-Map的行为可以按照每周的特定时间来启用或者禁用。首先，定义Time-Range的名称并设置其在一周内的时间，然后将其应用到ACE。可以使用Time-Range来制定Class-Map中独立的一条ACE在每周的制定时间生效。

18. **RTCM**: 单速率三色标记（Single Rate Three Color Marker）

19. **TRTCM**: 双速率三色标记（Two Rate Three Color Marker）

20. **CIR**: 提交信息速率（Committed Information Rate）

21. **CBS**: 提交组量大小（Committed Burst Size）

22. **EBS**: 超量组量大小（Excess Burst Size）

23. **PIR**: 峰值信息速率（Peak Information Rate）

1.3 配置 Class Map

该类型的 class-map 使用不同流类型区别流，对不同类型的数据流进行分组。创建 Class Map 后，在 Class Map 配置模式下，使用特定的 QoS 流类型值作为匹配条件。

表1-1 创建Class Map

命令	操作	说明
configure terminal	进入全局配置模式	-
class-map type traffic-class *name*	创建或配置一个 Class Map，并进入该目录的配置模式	name: 类映射名。最大支持 40 个字节，只能由字母、数字、连字符、下划线组成
match traffic-class *class-id*	配置流优先级	class-id: 指定的流类型值，取值范围为 1~6

1.4 创建 Policy Map

创建的 Policy Map 使用多个不同的流分类区别流，可以与 Class Map 匹配，依据流类型将流以不同属性加以划分，如优先级、带宽等。与 Class Map 不同，Policy Map 是对已经分类的数据流设定规则的映射。

表 1-2 创建 Policy Map

命令	操作	说明
configure terminal	进入全局配置模式	-
policy-map type traffic-class *name*	创建 Policy Map，并进入 Policy Map 配置模式	if-name: 接口名称
class type traffic-class *name*	引入存在的类映射，并进入该目录的配置模式	name: Class Map 类型的目录名。最大支持 40 个字节，只能由字母、数字、连字符、下划线组成

1.5 配置基于接口的应用策略

1.5.1 应用 QoS 策略

用于将队列和优先流控制参数应用于接口上。

表 1-3 应用 QoS 策略

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
service-policy type traffic-class *name*	应用 QoS 策略	name: Policy Map 名称

1.5.2 配置策略表应用至接口

创建 Class Map 后，在指定接口上对输入和输出的流量应用策略表。

表 1-4 配置策略表应用至接口

命令	操作	说明
configure terminal	进入全局配置模式	-
class-map type qos *name*	定义一个 Class Map 并用于 QoS policy	name: Class Map 名
quit	退出至全局配置模式	-
policy-map type qos *name*	创建策略表，并进入策略表配置模式	name: Policy Map 名称
class type qos *name*	创建流分类的 Class Map 并进入其配置模式	name: 流分类目录名。
policer { **color-blind** | **color-aware** } **cir** *CIR* [**cbs** *CBS*] [**eir** *EIR*] [**ebs** *EBS*] { **exceed** | **violate** } **drop** [**statistics**]	配置该接口的保证速率	cir: 承诺信息速率，取值范围为 0~100000000 kbps cbs: 承诺突发尺寸，取值范围为 0~640000 bytes eir: 额外信息速率，取值范围为 0~100000000 kbps ebs: 超额突发尺寸，取值范围为 0~640000 bytes
quit	退出两次至全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
service-policy type qos input *name*	将策略表应用至接口	name: Policy Map 名称

1.6 配置聚合策略

用来应用一个或多个策略表中的多个流分类策略的聚合策略。

表 1-5 配置策略表应用至接口

命令	操作	说明
configure terminal	进入全局配置模式	-
class-map type qos *name*	定义一个 Class Map 并用于 QoS policy	name: Class Map 名
quit	退出至全局配置模式	-
policy-map type qos *name*	创建策略表，并进入策略表配置模式	name: Policy Map 名称
class type qos *name*	创建流分类的 Class Map 并进入其配置模式	name: 流分类目录名
aggregate-policer *name*	配置聚合策略	name: 聚合策略实例名

1.7 显示与维护

表 1-6 显示与维护

命令	操作	说明
show qos aggregator-policer *name* [**statistics**]	显示聚合策略信息	name: 聚合策略名
show qos interface *name* **egress**	显示接口上流分类的配置信息	name: 接口名
show qos interface *name* **statistics policer flow**	显示基于类型区分的流策略状态和流统计信息	
show qos interface *name* **statistics policer port** { **input** | **output** }	显示端口策略统计信息	
show qos interface *name* **statistics queue**	显示接口上的流分类统计信息	

1.8 配置举例

1.8.1 配置出口队列

i. 配置Tail Drop

1. 介绍

尾丢弃是默认的每个出口队列拥塞避免技术。在没有超过队列长度的时候，报文会在队列中缓存。

2. 配置步骤

根据不同的丢弃优先级配置尾丢弃阈值：

- 进入全局配置模式；
- 创建 class-map 类流优先级，并配置优先级；
- 创建 policy-map 类流优先级，并关联之前定义的 class-map；
- 在 policy-map 优先级模式下，设置该优先级的尾丢弃上限值；
- **interface** *if-name* 进入匹配相应策略表的接口，其中 *if-name* 是该接口的名称。

下面是对流优先级为 3 的尾丢弃上限的配置实例，例子中的尾丢弃上限为 2000。

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# class-map type traffic-class tc3	创建 class-map 并进入其配置模式
Switch(config-cmap-tc)# match traffic-class 3	设置流优先级为 3
Switch(config-cmap-tc)# exit	退出该配置模式
Switch(config)# policy-map type traffic-class tc	创建 policy-map 并进入其配置模式
Switch(config-pmap-tc)# class type traffic-class tc3	关联 class-map
Switch(config-pmap-tc-c)# queue-limit 2000	配置丢包上限为 2000
Switch(config-pmap-tc-c)# exit	退出该配置模式
Switch(config-pmap-tc)# exit	退出到全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# service-policy type traffic-class tc	应用 QoS policy
Switch(config-if)# end	退出至特权模式

3. 命令验证

显示接口上流分类的配置信息：

```
Switch# show qos interface eth-0-1 egress

TC Priority Bandwidth Shaping(kbps) Drop-Mode     Max-Queue-Limit(Cell)  ECN
0  0        -         -             dynamic      level 0                -
1  0        -         -             dynamic      level 0                -
2  0        -         -             dynamic      level 0                -
3  0        -         -             tail-drop    2000                   2000
4  0        -         -             dynamic      level 0                -
5  0        -         -             dynamic      level 0                -
6  0        -         -             dynamic      level 0                -
7  7        -         -             tail-drop    64                     -
```

ii. 配置WRED

1. 介绍

WRED 通过选择性地丢弃部分报文，降低接口拥塞时发生尾丢弃的概率。通过早期选择性地丢弃部分报文而不是在队列缓冲区满时才开始丢弃，WRED 可以避免出现 TCP 同步丢包的问题，从而提高网络的吞吐量。

2. 配置步骤

针对不同颜色的报文配置相应的 WRED 阈值：

- 进入全局配置模式；
- 创建 class-map 类流优先级，并配置优先级；
- 创建 policy-map 类流优先级，并关联之前定义的 class-map；
- 在 policy-map 优先级模式下配置对应流优先级的 WRED 丢包上限；
- **interface** *if-name* 进入匹配相应策略表的接口，其中 *if-name* 是该接口的名称

下面的例子所示的是对流优先级为 1 设定其 WRED 丢包上限。其最大丢包上限为 596，最小丢包上限为 596/8=71。如果缓冲区中的报文超过最小丢包上限，后续收到的报文将随机丢弃。

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式

命令举例	操作步骤
Switch(config)# class-map type traffic-class tc1	创建 class-map 并进入其配置模式
Switch(config-cmap-tc)# match traffic-class 1	设置流优先级为 1
Switch(config-cmap-tc)# exit	退出该配置模式
Switch(config)# policy-map type traffic-class tc	创建 policy-map 并进入其配置模式
Switch(config-pmap-tc)# class type traffic-class tc1	关联 class-map
Switch(config-pmap-tc-c)# random-detect maximum-threshold 596	配置丢包上限 596
Switch(config-pmap-tc-c)# exit	退出该配置模式
Switch(config-pmap-tc)# exit	退出到全局配置模式
Switch(config)# interface eth-0-1	进入端口配置模式
Switch(config-if)# service-policy type traffic-class tc	应用 QoS policy
Switch(config-if)# end	退出至特权模式

3. 命令验证

显示接口上流分类的配置信息：

```
Switch# show qos interface eth-0-1 egress

TC Priority Bandwidth Shaping(kbps) Drop-Mode      Max-Queue-Limit(Cell)      ECN
0  0        -         -             dynamic        level 0                    -
1  0        -         -             random-drop 596                           Disable
2  0        -         -             dynamic        level 0                    -
3  0        -         -             tail-drop      2000                       2000
4  0        -         -             dynamic        level 0                    -
5  0        -         -             dynamic        level 0                    -
6  0        -         -             dynamic        level 0                    -
7  7        -         -             tail-drop      64                         -
```

iii. 配置调度

1. 介绍

在不同的 Class 之间，报文是按照 SP（严格优先级）调度的；在同一个 Class 之间，报文是按照 WDRR 调度的。

2. 配置步骤

下面的例子显示了将队列映射到不同的 Class 中间并且配置 WDRR 调度的权重。

- 进入全局配置模式；
- 创建 class-map 类流优先级，并配置优先级；
- 创建 policy-map 类流优先级，并关联之前定义的 class-map；
- 在 policy-map 优先级模式下配置对应流优先级的调度优先级；
- 在 policy-map 优先级模式下配置对应流优先级的带宽；
- **interface** *if-name* 进入匹配相应策略表的接口，其中 *if-name* 是该接口的名称。

下面例子显示了出队列调度参数的配置。编号为 5 和 6 的流的优先级是最高的值 6，编号为 2 的流的优先级是 2，带宽为 link 带宽的 20%。

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# class-map type traffic-class tc5	创建 class-map 并进入其配置模式
Switch(config-cmap-tc)# match traffic-class 5	设置流优先级为 5
Switch(config-cmap-tc)# exit	退出该配置模式
Switch(config)# class-map type traffic-class tc6	创建 class-map 并进入其配置模式
Switch(config-cmap-tc)# match traffic-class 6	设置流优先级为 6
Switch(config-cmap-tc)# exit	退出该配置模式
Switch(config)# class-map type traffic-class tc2	创建 class-map 并进入其配置模式
Switch(config-cmap-tc)# match traffic-class 2	设置流优先级为 2
Switch(config-cmap-tc)# exit	退出该配置模式
Switch(config)# policy-map type traffic-class tc	创建 policy-map 并进入其配置模式
Switch(config-pmap-tc)# class type traffic-class tc5	关联 class-map tc5
Switch(config-pmap-tc-c)# priority level 6	设置优先级为 6
Switch(config-pmap-tc-c)# exit	退出到 policy-map 模式
Switch(config-pmap-tc)# class type traffic-class tc6	关联 class-map tc6

命令举例	操作步骤
Switch(config-pmap-tc-c)# priority level 6	设置优先级为 6
Switch(config-pmap-tc-c)# exit	退出到 policy-map 模式
Switch(config-pmap-tc)# class type traffic-class tc2	关联 class-map tc2
Switch(config-pmap-tc-c)# bandwidth percentage 20	配置带宽为 link 带宽的 20%
Switch(config-pmap-tc-c)# exit	退出至 policy-map 模式
Switch(config-pmap-tc)# exit	退出该配置模式
Switch(config)# interface eth-0-1	进入端口配置模式
Switch(config-if)# service-policy type traffic-class tc	应用 QoS policy
Switch(config-if)# end	退出至特权模式

3. 命令验证

显示接口上流分类的配置信息：

```
Switch# show qos interface eth-0-1 egress

TC Priority Bandwidth Shaping(kbps) Drop-Mode      Max-Queue-Limit(Cell)     ECN
0  0        -         -              dynamic        level 0                   -
1  0        -         -              random-drop 596                          Disable
2  0        20        -              dynamic        level 0                   -
3  0        -         -              tail-drop      2000                      2000
4  0        -         -              dynamic        level 0                   -
5  6        -         -              dynamic        level 0                   -
6  6        -         -              dynamic        level 0                   -
7  7        -         -              tail-drop      64                        -
```

iv. 配置端口的流量监管策略

1. 介绍

经过交换机物理接口的所有流量都可以设置保证速率，超过保证速率的流量都会被丢弃。

2. 配置步骤

配置端口 Policer 来实现保证速率：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# qos policer input color-blind cir 48000 cbs 10000 ebs 20000 violate drop	配置该接口的保证速率为 48000kbps
Switch(config-if)# end	退出至特权模式

3. 命令验证

显示端口策略统计信息：

```
Switch# show qos interface eth-0-1 statistics policer port input

Interface: eth-0-1
   input port policer:
     color blind
       CIR 48000 kbps, CBS 10000 bytes, EBS 20000 bytes
       drop violate packets
```

1.8.2 配置 Shaping

i. 配置端口流量整形

1. 介绍

经过交换机物理接口的所有流量都可以被整形，超过整形速率的流量会被缓存，但是如果缓存耗尽，则后续的报文会被丢弃直到缓存被释放。

2. 配置步骤

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# qos shape rate 1000000	配置端口流量速率超过 1000Mbps 时，将被丢弃
Switch(config-if)# end	退出至特权模式

3. 命令验证

查看上述步骤后的配置信息：

```
Switch# show running-config interface eth-0-1

Building configuration...
!
interface eth-0-1
  service-policy type traffic-class tc
  qos policer input color-blind cir 48000 cbs 10000 ebs 20000 violate drop
  qos shape rate 1000000
!
```

ii. 配置出方向队列整形

1. 介绍

流量在经过交换机出方向的队列的时候可以被整形，超过整形速率的流量会被缓存，但是如果缓存耗尽，则后续的报文会被丢弃直到缓存被释放。

2. 配置步骤

在出方向队列上配置流量整形：

- 进入全局配置模式；
- 创建 class-map 类流优先级，并配置优先级；
- 创建 policy-map 类流优先级，并关联之前定义的 class-map；
- 在 policy-map 优先级模式下配置对应流优先级的流量整形；
- **interface** *if-name* 进入匹配相应策略表的接口，其中 *if-name* 是该接口的名称

示例显示对队列 3 进行队列整形的配置。当队列 3 中流速率超过 1000Mbps，将丢弃报文。

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# class-map type traffic-class tc3	创建 class-map 并进入其配置模式
Switch(config-cmap-tc)# match traffic-class 3	配置流优先级为 3
Switch(config-cmap-tc)# exit	退出该配置模式
Switch(config)# policy-map type traffic-class tc	创建 policy-map 并进入其配置模式
Switch(config-pmap-tc)# class type traffic-class tc3	关联 class-map
Switch(config-pmap-tc-c)# shape rate 1000000	按 1000Mbps 速率进行队列整形

命令举例	操作步骤
Switch(config-pmap-tc-c)# exit	退出至 policy-map 模式
Switch(config-pmap-tc)# exit	退出至配置模式
Switch(config)# interface eth-0-1	进入端口配置模式
Switch(config-if)# service-policy type traffic-class tc	应用 QoS policies
Switch(config-if)# end	退出至特权模式

3. 配置步骤

显示接口上流分类的配置信息：

```
Switch# show qos interface eth-0-1 egress

TC Priority Bandwidth Shaping(kbps) Drop-Mode      Max-Queue-Limit(Cell)     ECN
0  0        -         -             dynamic        level 0                   -
1  0        -         -             random-drop 596                          Disable
2  0        20        -             dynamic        level 0                   -
3  0        -         1000000       tail-drop      2000                      2000
4  0        -         -             dynamic        level 0                   -
5  6        -         -             dynamic        level 0                   -
6  6        -         -             dynamic        level 0                   -
7  7        -         -             tail-drop      64                        -
```

1.8.3 配置 QoS 流量策略

在部署 QoS 流量策略时需要执行如下几个步骤。

- 识别并区分流量到不同的类别；
- 对不同的流量类别配置策略；
- 在接口上应用策略。

说明

接口下一个方向只允许配置一个策略映射表。

i. 使用ACL实现流量分类

1. 介绍

IP 流量使用 IP ACL 作流量分类。

2. 配置步骤

创建 IP ACL 来区分不同的流量并将其分类：

- **configure terminal**
- **ip access-list** *access-list-name* 创建 ACL，其中 *access-list-name* 为 ACL 名。
- 根据需要创建一到多条 ACE，详细方法请参见“ACL 用户配置指导”。

示例显示允许三类 IP 地址的主机访问，网络地址主机部分对应为通配符。如果一台主机的 IP 地址不在 list 的匹配范围，则该主机将被拒绝访问。

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# ip access-list ip-acl	进入 IP ACL 配置模式
Switch(config-ip-acl)# permit any 128.88.12.0 0.0.0.255 any	配置允许源 IP 地址 128.88.12.x 的流量
Switch(config-ip-acl)# permit any 28.88.0.0 0.0.255.255 any	配置允许源 IP 地址 28.88.x.x 的流量
Switch(config-ip-acl)# permit any 11.0.0.0 0.255.255.255 any	配置允许源 IP 地址 11.xx.x.x 的流量
Switch(config-ip-acl)# end	退出到特权模式
Switch# show access-list ip ip-acl	显示 ACL 配置状态

3. 命令验证

显示ACL配置状态：

```
Switch# show access-list ip ip-acl

ip access-list ip-acl
   10 permit any 128.88.12.0 0.0.0.255 any
   20 permit any 28.88.0.0 0.0.255.255 any
   30 permit any 11.0.0.0 0.255.255.255 any
```

ii. 创建分类映射表

1. 配置步骤

将指定接口的 IP 流量按照分类表作流量分类，期间涉及到创建分类映射表以及匹配准则：

- 进入全局配置模式；
- **ip access-list** *access-list-name* 创建 ACL，其中 *access-list-name* 为 ACL 名。
- 根据需要创建一至多条 ACE。详细方法请参见“ACL 用户配置指导”。
- **class-map** { **match-any** | **match-all** } *name* 用来创建分类映射表。match-any 表示映射表中的分类按照逻辑或的关系进行匹配，即分类映射表中至少匹配一条即可分类。match-all 表示映射表中的分类按照逻辑与的关系进行匹配，即分类映射表中必须所有都匹配才可分类。*name* 表示分类映射表的名称。缺省情况下，按照 match-any 的方式进行流量分类。
- **match access-group** *name* 用来定义分类标准，*name* 表示需要关联的 ACL 表名

示例显示使用 **ip access list** 创建一个名为 cmap1 的分类映射表，允许任意源主机到目的主机的流量传输。

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# ip access-list ip-acl	进入 IP ACL 配置模式.
Switch(config-ip-acl)# permit any any any	允许所有报文通过
Switch(config-ip-acl)# quit	退出到全局配置模式
Switch(config)# class-map cmap1	创建 cmap1 并进入分类映射表配置模式
Switch (config-cmap)# match access-group ip-acl	将 ip-acl 加入到 cmap1 中
Switch (config-cmap)# quit	退出到特权模式
Switch# show class-map cmap1	显示分类表配置

2. 命令举例

显示分类表配置信息：

```
Switch# show class-map cmap1
    CLASS-MAP-NAME: cmap1 (match-any)
```

match access-group: ip-acl

iii. 创建策略表

1. 配置步骤

创建策略表用于对流量进行分类、标记和限流。下表创建了一个策略表，并应用到一个端口的进口流量。配置的 IP ACL 允许来自 10.1.00 地址的流量，如果这些流量的平均速率超过 48000-kbps，将被丢弃。

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# ip access-list ip-acl	进入 IP ACL 配置模式.
Switch(config-ip-acl)# permit any 10.1.0.0 0.0.255.255 any	配置允许源 IP 地址 10.1.x.x 的流量
Switch(config-ip-acl)# quit	退出到全局配置模式
Switch(config)# class-map type qos cmap1	创建 cmap1 并进入分类映射表配置模式
Switch(config-cmap)# match access-group ip-acl	将 ip-acl 加入到 cmap1 中
Switch(config-cmap)# quit	退出到全局配置模式
Switch(config)# policy-map type qos pmap1	配置策略表 pmap1 并进入策略表配置模式
Switch(config-pmap)# class type qos cmap1	将流分类映射表 cmap1 加入策略表 pmap1
Switch(config-pmap-c)# policer color-blind cir 48000 cbs 10000 ebs 16000 violate drop	配置该接口的保证速率为 48000kbps
Switch(config-pmap-c)# quit	退出到策略表配置模式
Switch(config-pmap)# quit	退出到全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# service-policy type qos input pmap1	将策略表 pmap1 应用到接口
Switch(config-if)# end	退出至特权模式

2. 命令举例

显示策略表配置：

```
Switch# show policy-map pmap1

  POLICY-MAP-NAME: pmap1 ( type qos)
    State: attached
    CLASS-MAP-NAME: cmap1
      match access-group: ip-acl
        policer color-blind cir 48000 cbs 10000 ebs 16000 violate drop
```

iv. 创建聚合策略

1. 配置步骤

创建聚合策略表用于对流量进行分类，标记和限流。下表显示创建了一条聚合策略，并运用于策略表中的多个表项。示例中，IP ACLs 允许来自网络地址 10.1.0.0 和主机地址为 11.3.1.1 的流量，且配置了其平均速率。当流量平均速率超过 48000-kbps 且流量大小超过 8000-byte，该流量将被丢弃。该策略表运用于端口的进流量。

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# ip access-list ip-acl1	进入 IP ACL 配置模式.
Switch(config-ip-acl)# permit any 10.1.0.0 0.0.255.255 any	配置允许源 IP 地址 10.1.x.x 的流量
Switch(config-ip-acl)# exit	退出到全局配置模式
Switch(config)# ip access-list ip-acl2	进入 IP ACL 配置模式.
Switch(config-ip-acl)# permit any host 11.3.1.1 any	配置允许源 IP 地址 11.3.1.1 的流量
Switch(config-ip-acl)# exit	退出到全局配置模式
Switch(config)# qos aggregate-policer transmit1 color-blind cir 48000 cbs 8000 ebs 10000 violate drop	配置聚合策略的保证速率为 48000kbps
Switch(config)# class-map type qos cmap1	创建 cmap1 并进入分类映射表配置模式
Switch(config-cmap)# match access-group ip-acl1	将 ip-acl1 加入到 cmap1 中

命令举例	操作步骤
Switch(config-cmap)# exit	退出到全局配置模式
Switch(config)# class-map type qos cmap2	创建 cmap2 并进入分类映射表配置模式
Switch(config-cmap)# match access-group ip-acl2	将 ip-acl2 加入到 cmap2 中
Switch(config-cmap)# exit	退出到全局配置模式
Switch(config)# policy-map type qos aggflow1	配置策略表 aggflow1 并进入策略表配置模式
Switch(config-pmap)# class type qos cmap1	将流分类映射表 cmap1 加入策略表 aggflow1
Switch(config-pmap-c)# aggregate-policer transmit1	将 cmap1 设置为聚合策略 transmit1
Switch(config-pmap-c)# exit	退出到策略表配置模式
Switch(config-pmap)# class type qos cmap2	将流分类映射表 cmap2 加入策略表 pmap1
Switch(config-pmap-c)# aggregate-policer transmit1	将 cmap2 设置为聚合策略 transmit1
Switch(config-pmap-c)# exit	退出到策略表配置模式
Switch(config-pmap)# exit	退出到全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# service-policy type qos input aggflow1	将聚合策略 aggflow1 应用到接口
Switch(config-if)# exit	退出到端口配置模式
Switch(config)# exit	退出到全局配置模式

2. 命令验证

显示聚合策略配置状态：

```
Switch# show qos aggregate-policer

Aggreate policer: transmit1
   color blind
   CIR 48000 kbps, CBS 8000 bytes, EBS 10000 bytes

   drop violate packets
```

2 FEC 配置

2.1 FEC 简介

为降低信号传输中传输距离的影响，FEC（Forward Error Correction，前向纠错）由此出现，它是一种误码纠错技术。FEC 适用于高速率通信，由于光信号在传输时可能会发生变化，FEC 功能在发送端为数据报文提供纠错信息，并在接收端利用这些信息定位和纠正传输中的误码。通过这样的方式，可以提高信号的质量。但是，在纠正误码时可能存在一定的延时。因此，不是所有的光模块都需要开启此功能，用户需要根据实际情况来启用或者关闭 FEC 功能。

2.2 配置 FEC

2.2.1 使能/关闭 FEC 功能

一般情况下，100G 端口仅支持 RS-FEC 功能，50G 端口仅支持 FC-FEC，25G 端口可支持 RS-FEC 和 FC-FEC，其他速率类型端口不支持 FEC 设置。

1. 使能FEC功能

表 2-1 使能 FC-FEC 功能

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
fec fc-fec	使能 FC-FEC 功能	缺省情况下，25G 端口默认使能 FC-FEC

表 2-2 使能 RS-FEC 功能

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
fec rs-fec	使能 RS-FEC 功能	缺省情况下，100G 端口默认使能 RS-FEC

2. 关闭FEC功能

表 2-3 关闭 FEC 功能

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
fec off	关闭 FEC 功能	缺省情况下，100G 端口默认使能 RS-FEC，25G 端口默认使能 FC-FEC

2.2.2 去使能端口的 FEC 功能

表 2-4 去使能端口的 FEC 功能

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
no fec	关闭端口的 FEC 功能	-

IPv6 安全配置指导目录

1 DHCPv6 Snooping 配置

1.1 DHCPv6 Snooping 简介

DHCPv6 Snooping 是一种安全功能，只有本地链路的报文和完全匹配 IP 地址、MAC 地址、端口的 IPv6 报文才能够进行转发，不符合条件的报文则会被丢弃。DHCPv6 Snooping 功能允许配置某个端口为信任或不信任的端口。信任端口收到报文时会正常接收以及转发，不信任端口接收到报文后会进行丢弃。如不受信任的 DHCPv6 客户端和信任的 DHCPv6 服务器之间的防火墙行为，DHCPv6 Snooping 功能执行如下：

- 验证DHCPv6消息接收来自不信任的源和过滤掉无效消息。
- 建立和维护DHCPv6 Snooping绑定数据库，其中包含DHCPv6客户端租用的IPv6地址信息。
- DHCPv6 Snooping功能在软件中实现，所有DHCPv6消息在芯片中被拦截直接发往CPU进行处理。

1.2 配置 DHCPv6 Snooping 基本功能

1.2.1 全局启用 DHCPv6 Snooping

必须使用 **service dhcpv6 enable** 在全局使能 DHCPv6 Snooping，才可以使 DHCPv6 Snooping 的配置生效。

表1-1 全局启用DHCPv6 Snooping

命令	操作	说明
configure terminal	进入全局配置模式	-
dhcpv6 snooping	全局使能 DHCPv6 Snooping	缺省情况下，DHCPv6 Snooping 处于关闭状态

1.2.2 配置 DHCPv6 Snooping 信任端口

配置连接 DHCPv6 服务器或其他交换机或路由器的接口为信任接口。配置连接 DHCPv6 客户端的接口为不信任接口。

表 1-2 配置 DHCPv6 Snooping 信任端口

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
dhcpv6 snooping trust	配置接口为 DHCPv6 Snooping 信任接口	缺省情况下，接口为 DHCPv6 Snooping 不信任接口

1.2.3 配置在 VLAN 上使能 DHCPv6 Snooping 特性

可以输入 VLAN 序号指定单独一个 VLAN ID，或者输入几个 VLAN 序号使用逗号间隔，也可以输入一个 VLAN 范围（使用连字符“-”间隔），或使用空格间隔输入 VLAN 开始 ID 和 VLAN 结束 ID。在 VLAN 上使能 DHCPv6 Snooping 前，必须先全局使能 DHCPv6 Snooping。

表 1-3 配置在 VLAN 上使能 DHCPv6 Snooping 特性

命令	操作	说明
configure terminal	进入全局配置模式	-
dhcpv6 snooping vlan *vlan-id*	配置在 VLAN 上使能 DHCPv6 Snooping 特性	vlan-id: VLAN ID 取值范围为 1~4094

说明

注意不要在同一个 VLAN 上设置 DHCPv6 Snooping 功能和 DHCPv6 Server 功能。

1.3 显示与维护

表1-4 显示与维护

命令	操作	说明
show dhcpv6 snooping binding { **all** | **manual** | **learning** } [**ipv6** *ipv6-address* | **mac** *mac-address* | **vlan** *vlan-id* | **interface** *if-name*] **show dhcpv6 snooping binding summary**	显示设备 DHCPv6 Snooping 绑定数据库和所有接口的配置信息	ipv6-address: 指定 IPv6 地址 mac-address: 指定 MAC 地址 vlan-id: 指定 VLAN ID，取值范围为 1~4094 if-name: 指定添加或删除绑定条目的接口
show dhcpv6 snooping config	显示 DHCPv6 Snooping 的配置信息	-
show dhcpv6 snooping trusted-sources	显示 DHCPv6 Snooping 的信任端口	-
show dhcpv6 snooping statistics	显示 DHCPv6 Snooping 统计信息	-
clear dhcpv6 snooping statistics	清除 DHCPv6 Snooping 统计信息	

1.4 配置举例

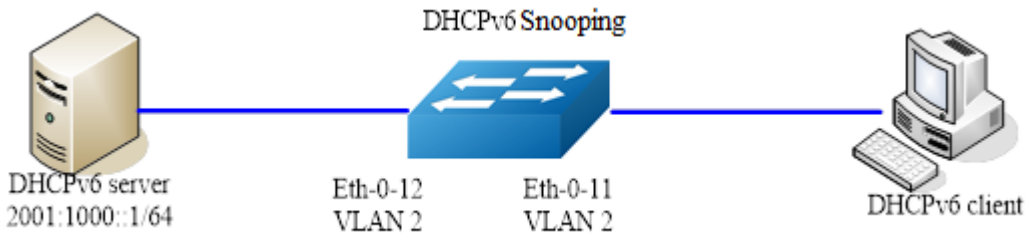
1.4.1. 介绍

下图 1-1 为测试 DHCPv6 Snooping 功能的网络拓扑，需要两台 PC 机和一台交换机构建测试环境，具体分配可参照如下描述：

- 计算机A作为DHCPv6服务器
- 计算机B作为DHCPv6客户端
- 交换机作为DHCPv6 Snooping

1.4.2. 拓扑

图 1-1 DHCPv6 Snooping 拓扑图



1.4.3. 配置步骤

1. 配置VLAN

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# vlan database	配置 VLAN 数据库
Switch(config-vlan)# vlan 2	创建 VLAN 2
Switch(config-vlan)# exit	退出至全局配置模式

2. 配置接口eth-0-12

命令举例	操作步骤
Switch(config)# interface eth-0-12	进入接口配置模式
Switch(config-if)# switchport	设置为交换接口
Switch(config-if)# switchport access vlan 2	添加接口到 VLAN 2
Switch(config-if)# dhcpv6 snooping trust	配置接口为信任状态
Switch(config-if)# no shutdown	使能接口
Switch(config-if)# exit	退出至全局配置模式

3. 配置接口eth-0-11

命令举例	操作步骤
Switch(config)# interface eth-0-11	进入接口配置模式
Switch(config-if)# switchport	设置为交换接口
Switch(config-if)# switchport access vlan 2	添加接口到 VLAN 2
Switch(config-if)# no shutdown	使能接口
Switch(config-if)# exit	退出至全局配置模式

4. 使能DHCPv6 Snooping全局特性

命令举例	操作步骤
Switch(config)# service dhcpv6 enable	使能 DHCPv6 服务
Switch(config)# dhcpv6 snooping	使能 DHCPv6 Snooping 特性
Switch(config)# dhcpv6 snooping vlan 2	在 VLAN 2 上使能 DHCPv6 Snooping 特性

1.4.4. 命令验证

1. 根据如下步骤，检查接口配置是否正确：

```
Switch# show running-config interface eth-0-12

!
interface eth-0-12
switchport access vlan 2
dhcpv6 snooping trust
!

Switch# show running-config interface eth-0-11

!
interface eth-0-11
 switchport access vlan 2
!
```

2. 检查DHCPv6的服务状态：

```
Switch# show services

Networking services configuration:
```

```
Service Name            Status
============================================================
dhcp                    disable
dhcpv6                  enable
```

3. 打印DHCPv6 Snooping配置，检查当前配置：

```
Switch# show dhcpv6 snooping config

dhcpv6 snooping service: enabled
dhcpv6 snooping switch: enabled
dhcpv6 snooping vlan 2
```

4. 检查DHCPv6 Snooping的统计信息：

```
Switch# show dhcpv6 snooping statistics

DHCPv6 snooping statistics:
============================================================
DHCPv6 packets                          21
Packets forwarded                       21
Packets invalid                         0
Packets dropped                         0
```

5. 检查DHCPv6 Snooping的绑定信息：

```
Switch# show dhcpv6 snooping binding all

DHCPv6 snooping binding table:
VLAN MAC Address       Lease(s)       Interface      IPv6 Address
============================================================

2       0016.76a1.7ed9 978             eth-0-11       2001:1000::2
```

IPv6 路由配置指导目录

1 IPv6 单播路由配置

1.1 静态路由简介

静态路由一般由用户或管理员手工配置，使数据包通过预设的路径到达指定的目的地址。静态路由主要应用于小型网络中，当设备或者路由数量有限时，只需考虑使用静态路由就可以满足工作需求。合理设置和使用静态路由可以改进网络性能，并可为重要的网络应用保证带宽。静态路由也存在一定的局限性，当网络发生故障或者拓扑发生变化后，可能会出现路由不可达，从而导致网络中断。此时必须由网络管理员手工修改静态路由的配置。

IPv6 静态路由与 IPv4 静态路由类似，适用于小型的 IPv6 网络，通过配置 IPv6 静态路由实现网络互连。

1.2 配置静态路由

1.2.1 使能 IPv6 路由功能

当未使能 IPv6 路由功能时，IPv6 报文会被当做普通二层报文处理。

表1-1 使能IPv6路由功能

命令	操作	说明
configure terminal	进入全局配置模式	-
ipv6 enable	全局使能 IPv6 功能	缺省情况下，IPv6 功能处于关闭状态

1.2.2 配置接口的 IPv6 地址

当接口上没有任何 IPv6 地址的时候，使用 **auto** 关键字可自动生成链路本地地址。当接口上没有任何全球单播地址时，使用该命令的 **no** 格式、配合 **auto** 关键字，可删除自动生成的链路本地地址；如果配置全球单播地址时，接口上不存在链路本地地址，那么会自动生成一个链路本地地址。如果之后用

户又手动指定链路本地地址，当用户指定的优先级高于自动生成的优先级时，将会覆盖原有的链路本地地址。

表1-2 配置接口的IPv6地址

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
no switchport	设置接口为三层接口	-
no shutdown	打开接口	-
ipv6 address *global-prefix* [**eui-64** | **anycast**] **ipv6 address** *link-local* **link-local** **ipv6 address auto link-local**	配置接口上的 IPv6 地址	缺省情况下，接口上未配置 IPv6 地址； global-prefix: 全球单播地址，格式为 X:X::X:X/M format link-local: 链路本地地址，格式为 X:X::X:X 每个接口最多可配 1 个链路本地地址，8 个全球单播地址

1.2.3 创建 IPv6 静态路由

启用IPv6功能并在接口上配置IPv6地址后，就可以创建IPv6静态路由。

表1-3 创建IPv6静态路由

命令	操作	说明
configure terminal	进入全局配置模式	-
ipv6 route *dest-prefix* { *nexthop* | *if-tunnel* } [*admin-distance*] **ipv6 route** *dest-prefix nexthop if-name* [*admin-distance*]	创建 IPv6 静态路由	缺省情况下，未配置静态路由 dest-prefix: 目的地址前缀，格式为 X:X::X:X/M nexthop: 下一跳 IPv6 地址，格式为 X:X::X:X if-tunnel: IPv6 路由出口的隧道接口名称 if-name: IPv6 路由出接口名称

命令	操作	说明
		admin-distance: 管理距离，取值范围为 1~255，默认值为 1

1.2.4 配置 IPv6 静态路由条目数的最大值

用户可配置的 IPv6 静态路由条目数的最大值，受限于当前的 TCAM Profile 和已经存在的静态路由条目数。

表1-4 配置IPv6静态路由条目数的最大值

命令	操作	说明
configure terminal	进入全局配置模式	-
max-static-v6routes *count*	配置 IPv6 静态路由条目数的最大值	count: IPv6 静态路由条目数的取值范围为 1～65535; 根据不同的 TCAM Profile，默认值可能有所不同

1.3 显示与维护

将路由加入路由表后，用户可以使用 **show ipv6 route** 或者 **show ipv6 route static** 命令显示任何有效的动态和静态路由。

表1-5 显示与维护

命令	操作	说明
show ipv6 route [**database**] **show ipv6 route** [**database**] [**bgp** | **connected** | **ospf** | **rip** | **static**] **show ipv6 route** *ipv6-address* **show ipv6 route** *ipv6-prefix* **show ipv6 route** **show ipv6 route summary**	显示 IPv6 路由表状态	ipv6-address: IPv6 地址，格式为 X:X::X:X ipv6-prefix: IPv6 前缀，格式为 X:X::X:X/M
show ipv6 interface [*if-name*] [**brief**]	显示接口的 IPv6 状态与配置	if-name: 接口名称

1.4 配置举例

1.4.1 介绍

本例介绍了在一个简单的网络拓扑结构下如何使能静态路由。静态路由在小型网络中非常有用。静态路由可提供使多个目的地可达的简单解决方案。大型网络使用动态路由协议。静态路由是由网络前缀（主机地址）和下一跳（网关）组成。

1.4.2 拓扑

图 1-1 IPv6 静态路由拓扑图

1.4.3 配置步骤

1. Switch1的配置步骤如下：

命令举例	操作步骤
Switch1# configure terminal	进入全局配置模式
Switch1 (config)# ipv6 enable	使能 IPv6
Switch1 (config)# interface eth-0-9	进入接口配置模式
Switch1 (config-if)# no switchport	设置接口为三层接口
Switch1 (config-if)# no shutdown	打开接口
Switch1 (config-if)# ipv6 address auto link-local	配置自动生成链路本地地址
Switch1 (config-if)# ipv6 address 2001:1::1/64	配置全球单播地址
Switch1 (config-if)# exit	退出接口配置模式
Switch1 (config)# ipv6 route 2001:2::/64 2001:1::2	配置 IPv6 静态路由
Switch1 (config)# end	退出全局配置模式

2. Switch2的配置步骤如下：

命令举例	操作步骤
Switch2# configure terminal	进入全局配置模式
Switch2 (config)# ipv6 enable	使能 IPv6
Switch2 (config)# interface eth-0-9	进入接口配置模式
Switch2 (config-if)# no switchport	设置接口为三层接口
Switch2 (config-if)# no shutdown	打开接口
Switch2 (config-if)# ipv6 address auto link-local	配置自动生成链路本地地址
Switch2 (config-if)# ipv6 address 2001:1::2/64	配置全球单播地址
Switch2 (config-if)# exit	退出接口配置模式
Switch2 (config)# interface eth-0-17	进入接口配置模式
Switch2 (config-if)# no switchport	设置接口为三层接口
Switch2 (config-if)# no shutdown	打开接口
Switch2 (config-if)# ipv6 address auto link-local	配置自动生成链路本地地址
Switch2 (config-if)# ipv6 address 2001:2::2/64	配置全球单播地址
Switch2 (config-if)# exit	退出接口配置模式
Switch2 (config)# end	退出全局配置模式

3. Switch3的配置步骤如下：

命令举例	操作步骤
Switch3# configure terminal	进入全局配置模式
Switch3 (config)# ipv6 enable	使能 IPv6
Switch3 (config)# interface eth-0-17	进入接口模式
Switch3 (config-if)# no switchport	设置接口为三层接口
Switch3 (config-if)# no shutdown	打开接口
Switch3 (config-if)# ipv6 address auto link-local	配置自动生成链路本地地址

命令举例	操作步骤
Switch3 (config-if)# ipv6 address 2001:2::3/64	配置全球单播地址
Switch3 (config-if)# exit	退出接口配置模式
Switch3 (config)# ipv6 route 2001:1::/64 2001:2::2	配置 IPv6 静态路由
Switch3 (config)# end	退出全局配置模式

1.4.4 命令验证

4. 根据上述Switch1的配置步骤，显示当前的IPv6路由表状态：

```
Switch1# show ipv6 route

IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, O - OSPF, I - IS-IS, B - BGP
       [*] - [AD/Metric]
Timers: Uptime
C        2001:1::/64
       via ::, eth-0-9, 02:08:50
C        2001:1::1/128
       via ::1, eth-0-9, 02:08:50
S        2001:2::/64 [1/0]
       via 2001:1::2, eth-0-9, 02:05:36
C        fe80::/10
       via ::, Null0, 02:09:11
```

5. 根据上述Switch2的配置步骤，显示当前的IPv6路由表状态：

```
Switch2# show ipv6 route

IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, O - OSPF, I - IS-IS, B - BGP
       [*] - [AD/Metric]
Timers: Uptime
C        2001:1::/64
       via ::, eth-0-9, 00:03:37
C        2001:1::2/128
       via ::1, eth-0-9, 00:03:37
C        2001:2::/64
       via ::, eth-0-17, 00:03:21
C        2001:2::2/128
       via ::1, eth-0-17, 00:03:21
C        fe80::/10
       via ::, Null0, 00:03:44
```

6. 根据上述Switch3的配置步骤，显示当前的IPv6路由表状态：

```
Switch3# show ipv6 route

IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, O - OSPF, I - IS-IS, B - BGP
       [*] - [AD/Metric]
Timers: Uptime
S       2001:1::/64 [1/0]
       via 2001:2::2, eth-0-17, 00:02:14
C       2001:2::/64
       via ::, eth-0-17, 00:03:28
C       2001:2::3/128
       via ::1, eth-0-17, 00:03:28
C       fe80::/10
       via ::, Null0, 00:03:53
```

7. 在Switch1上验证Switch3的网络可达性：

```
Switch1# ping ipv6 2001:2::3

PING 2001:2::3(2001:2::3) 56 data bytes
64 bytes from 2001:2::3: icmp_seq=0 ttl=63 time=127 ms
64 bytes from 2001:2::3: icmp_seq=1 ttl=63 time=132 ms
64 bytes from 2001:2::3: icmp_seq=2 ttl=63 time=124 ms
64 bytes from 2001:2::3: icmp_seq=3 ttl=63 time=137 ms
64 bytes from 2001:2::3: icmp_seq=4 ttl=63 time=141 ms
--- 2001:2::3 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4010ms
rtt min/avg/max/mdev = 124.950/132.719/141.251/5.923 ms, pipe 2
```

2 RIPng 配置

2.1 RIPng 简介

RIPng（Routing Information Protocol Next Generation），又称为下一代 RIP 协议，是一种较为简单的内部网关协议（Interior Gateway Protocol，IGP），主要用于规模较小的网络，在 IPv6 网络中提供路由功能。RIPng 模块遵循的标准为 RFC 2080 – RIPng for IPv6。

RIPng 是一种基于距离矢量（Distance Vector）算法的协议，它通过 UDP 报文进行路由信息的交换。RIPng 使用跳数（Hop Count）来衡量到达目的地址的距离，称为路由权（Routing Cost）。在 RIPng 中，路由器到与它直接相连网络的跳数为 0，通过一个路由器可达的网络的跳数为 1，其余依此类推。为限制收敛时间，RIP 规定 COST 的取值为 0～15 之间的整数，COST 取值大于或等于 16 的跳数被定义为无穷大，即目的网络或主机不可达。

为提高性能，防止产生路由环，RIPng 支持水平分割（Split Horizon）。RIPng 还可引入其它路由协议所得到的路由。

为了在 IPv6 网络中应用，RIPng 对原有的 RIP 协议进行了修改：

- UDP 端口号：使用 UDP 的 521 端口发送和接收路由信息。
- 组播地址：使用 FF02::9 作为链路本地范围内的 RIPng 路由器组播地址
- 下一跳地址：使用 128 比特的 IPv6 地址
- 源地址：使用链路本地地址 FE80::/10 作为源地址发送 RIPng 路由信息更新报文。

2.2 配置 RIPng 的基本功能

2.2.1 开启 RIPng 功能

表 2-1 开启 RIPng 功能

命令	操作	说明
configure terminal	进入全局配置模式	-
router ipv6 rip	开启 RIPng 功能，并进入 RIPng 配置模式	缺省情况下，RIPng 功能处于关闭状态

2.2.2 配置接口使能 RIPng 功能

表2-2 配置接口使能RIPng功能

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
no switchport	设置接口为三层接口	-
ipv6 router rip	配置接口使能 RIPng 功能	缺省情况下，接口上的 RIPng 功能处于关闭状态

2.3 配置 RIPng 特性

2.3.1 配置接口附加度量值

当收到一条合法的 RIPng 路由，在其加入到路由表之前，接口接收度量值会附加到该路由上，再加入路由表中，因此路由表中的度量值发生变化。也就是说，增加一个接口的接收度量值，该接口收到的 RIPng 路由度量值也会相应增加。

表2-3 配置接口附加度量值

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
ipv6 rip metric-offset *number-value*	配置接口接收 RIPng 路由时的附加度量值	number-value: 取值范围是 1～16，默认附加度量值是 1

2.3.2 配置接口偏移度量值

如果偏移度量值生效，那么接口接收附加度量值的增加被忽略。偏移量列表可以用来改变路由的度量值，以达到某些目的（如备份链路或者负载均衡）。

表2-4 配置接口偏移度量值

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
no switchport	设置接口为三层接口	-
offset-list *accesss-list-name* { **in** | **out** } *metric-offset* [*if-name*]	配置接口接收或发送 RIPng 路由时的偏移度量值	accesss-list-name: 访问控制列表名 metric-offset: 应用到路由的偏移度量值 if-name: 接口名称

2.3.3 配置 RIPng 路由聚合

在接口上配置路由聚合时，如果一条路由的前缀和前缀长度与定义的 IPv6 前缀匹配，则这个自定义的 IPv6 前缀将取代原来的路由被发布出去。那么多条路由将由一条路由所代替，并且这条路由的度量值是原多条路由中最低的。

通过指定 **avoid-feedback** 关键字，本接口将不再学习到与已发布的聚合 IP 地址相同的聚合路由，从而可以起到防止产生路由环路的作用。该命令只有在接口为三层口时才生效。

表 2-5 配置 RIPng 路由聚合

命令	操作	说明
configure terminal	进入全局配置模式	-
router ipv6 rip	开启 RIPng 功能，并进入 RIPng 配置模式	缺省情况下，RIPng 功能处于关闭状态
aggregate-address *ipv6-address* [**avoid-feedback**] *if-name*	配置 RIPng 在接口发布聚合 IPv6 地址	ipv6-address: 指定的聚合地址 if-name: 接口名称

2.3.4 配置 RIPng 发布缺省路由

生成的 RIPng 缺省路由将强制通过指定接口的路由更新报文发布出去。

表 2-6 配置 RIPng 发布缺省路由

命令	操作	说明
configure terminal	进入全局配置模式	-
router ipv6 rip	开启 RIPng 功能，并进入 RIPng 配置模式	缺省情况下，RIPng 功能处于关闭状态
default-information originate [**route-map** *name*]	配置 RIPng 发布缺省路由	name: 路由策略名称 缺省情况下，RIPng 不发布缺省路由

2.3.5 配置 RIPng 过滤接收/发布的路由

表 2-7 配置 RIPng 过滤接收/发布的缺省路由

命令	操作	说明
configure terminal	进入全局配置模式	-
router ipv6 rip	开启 RIPng 功能，并进入 RIPng 配置模式	缺省情况下，RIPng 功能处于关闭状态
distribute-list { **prefix** *name* | *accesss-list-name* } { **in** | **out** } [*if-name*]	配置 RIPng 对接收或者发送的路由进行过滤	name: 过滤列表名 access-list-name: 访问控制列表名 if-name: 接口名称 缺省情况下，RIPng 不对接收或发布的路由进行过滤

2.3.6 配置 RIPng 管理距离

管理距离表明了对一个路由源的信任度，它是从 0 到 255 之间的一个整数。一般情况下，值越高，信任等级越低。如果管理距离为 255，说明设备不信任这个路由源，忽略来自该路由源的路由。

表 2-8 配置 RIPng 管理距离

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

命令	操作	说明
router ipv6 rip	开启 RIPng 功能，并进入 RIPng 配置模式	缺省情况下，RIPng 功能处于关闭状态
distance *DISTANCE*	配置 RIPng 的管理距离	DISTANCE: 管理值范围为 1~255，管理距离为 255 的路由无效；默认值为 120

2.3.7 配置路由重发布

通常情况下，RIPng 引入外部路由的命令需要和缺省度量值一起配置，这可以使再发布引入的路由的度量值保持一致。

表 2-9 配置路由重发布

命令	操作	说明
configure terminal	进入全局配置模式	-
router ipv6 rip	开启 RIPng 功能，并进入 RIPng 配置模式	缺省情况下，RIPng 功能处于关闭状态
default-metric *value*	配置引入路由的缺省度量值	value:取值范围为 1～16，默认度量值是 1
redistribute *protocol* { [**metric** *value*] | **route-map** *word* }	配置 RIPng 引入外部路由	protocol: 可引入的源路由协议，包括 OSPF、BGP、static、connected value: 发布路由的度量值 word: 路由策略名

2.4 优化 RIPng 网络性能

可以通过配置 RIPng 定时器、配置水平分割或者毒性逆转的方式，调整和优化 RIPng 网络。

2.4.1 配置 RIPng 定时器

配置 RIPng 各个定时器的值，可通过调节 RIPng 定时器来调整路由协议的性能，以满足网络需要。

RIPng 定时器的相关参数解释如下：

- update: 路由更新时间；

- timeout: 路由老化时间，如果在老化时间内没有收到关于某条路由的更新报文，则该条路由在路由表中的度量值将会被设置为 16，此时该条路由将不能用于转发报文；
- invalid: 路由的垃圾回收时间，定义了一条路由从度量值变为 16 开始，直到它从路由表里被删除所经过的时间。在垃圾回收时间内，RIPng 以 16 作为度量值向外发送这条路由的更新，如果垃圾回收定时器超时，该路由仍没有得到更新，则该路由将从路由表中被彻底删除。

表 2-10 配置 RIPng 定时器

命令	操作	说明
configure terminal	进入全局配置模式	-
router ipv6 rip	开启 RIPng 功能，并进入 RIPng 配置模式	缺省情况下，RIPng 功能处于关闭状态
timers basic *update timeout garbage-collection*	配置 RIP 定时器	update: 路由更新时间，缺省值为 30 秒 timeout: 路由老化时间，缺省值为 180 秒 garbage collection: 路由的垃圾回收时间，缺省值为 120 秒

2.4.2 配置水平分割/毒性逆转

当使能毒性逆转时，从一个接口学到的路由还可以从这个接口向外发布，但度量值必须为 16。当配置水平分割功能时，从一个接口学到的路由不能通过此接口向外发布。

表 2-11 配置水平分割/毒性逆转

命令举例	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
ip rip split-horizon [**poisoned**]	配置水平分割/毒性逆转	缺省情况下，端口采用毒性逆转防止路由环路

2.5 RIPng 显示与维护

表 2-12 RIPng 显示与维护

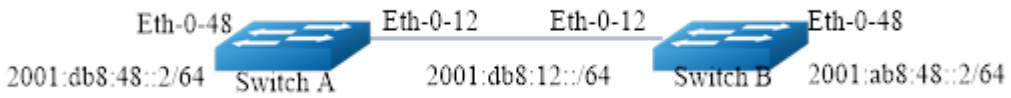
命令	操作	说明
show ipv6 rip database	显示 RIPng 域的信息	-
show ipv6 rip interface [*if-name*]	显示接口的 RIPng 信息	if-name：接口名称
show ipv6 rip database database-summary	显示 RIPng 域的概要信息	-
show ipv6 protocol rip	显示 RIPng 协议的信息	-
clear ipv6 rip route { *ipv6-address* | **connected** | **static** | **ospfv3** | **bgp** | **all** }	清除 RIPng 域中的路由	ipv6-address: 指定地址的路由

2.6 RIPng 配置举例

2.6.1 配置启用 RIPng

i. 拓扑

图 2-1 RIPng 基本配置拓扑图



ii. 配置步骤

Switch A的配置步骤如下：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# router ipv6 rip	启用 RIPng
Switch(config-router)# exit	退出路由配置模式
Switch(config)# interface eth-0-12	进入接口配置模式
Switch(config-if)# no switchport	使能三层接口属性

命令举例	操作步骤
Switch(config-if)# no shutdown	端口 UP
Switch(config-if)# ipv6 address 2001:db8:12::1/64	配置 IPv6 地址
Switch(config-if)# ipv6 router rip	配置端口使能 RIPng
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface eth-0-48	进入接口配置模式
Switch(config-if)# no switchport	使能三层接口属性
Switch(config-if)# no shutdown	端口 UP
Switch(config-if)# ipv6 address 2001:db8:48::2/64	配置 IPv6 地址
Switch(config-if)# ipv6 router rip	配置端口使能 RIPng

Switch B的配置步骤如下：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# router ipv6 rip	启用 RIPng
Switch(config-router)# exit	退出路由配置模式
Switch(config)# interface eth-0-12	进入接口配置模式
Switch(config-if)# no switchport	使能三层接口属性
Switch(config-if)# no shutdown	端口 UP
Switch(config-if)# ipv6 address 2001:db8:12::2/64	配置 IPv6 地址
Switch(config-if)# ipv6 router rip	配置端口使能 RIPng
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface eth-0-48	进入接口配置模式
Switch(config-if)# no switchport	使能三层接口属性
Switch(config-if)# no shutdown	端口 UP
Switch(config-if)# ipv6 address 2001:ab8:49::2/64	配置 IPv6 地址
Switch(config-if)# ipv6 router rip	配置端口使能 RIPng

iii. 命令验证

使用如下命令 **show ipv6 rip database**、**show ipv6 rip interface**、**show ipv6 protocols rip**、**show ipv6 route rip**，验证上述配置。

1. 上述 Switch A 的配置结果如下：

```
Switch# show ipv6 rip database

Codes: R - RIP, Rc - RIP connected, Rs - RIP static, Ra - RIP aggregated,
       Rcx - RIP connect suppressed, Rsx - RIP static suppressed,
       K - Kernel, C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP
    Network                    Next Hop                  If          Met Tag Time
R   2001:ab8:49::/64          fe80::1271:d1ff:fec8:3300 eth-0-12 5     0   00:02:34
Rc 2001:db8:12::/64           ::                        eth-0-12 1     0
Rc 2001:db8:48::/64           ::                        eth-0-48 1     0

Switch# show ipv6 rip interface

eth-0-12 is up, line protocol is up
  Routing Protocol: RIPng
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IPv6 interface address:
      2001:db8:12::1/64
      fe80::7e14:63ff:fe76:8900/10
eth-0-48 is up, line protocol is up
  Routing Protocol: RIPng
    Passive interface: Disabled
    Split horizon: Enabled with Poisoned Reversed
    IPv6 interface address:
      2001:db8:48::2/64
      fe80::7e14:63ff:fe76:8900/10

Switch# show ipv6 protocols rip

Routing Protocol is "ripng"
  Sending updates every 30 seconds with +/-5 seconds, next due in 7 seconds
  Timeout after 180 seconds, garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Default redistribute metric is 1
  Redistributing:
  Interface
    eth-0-12
    eth-0-48
  Routing for Networks:
  Number of routes (including connected): 3
```

```
   Distance: (default is 120)

Switch# show ipv6 route rip

IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, I - IS-IS, B - BGP
          O - OSPF, IA - OSPF inter area
          N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
          E1 - OSPF external type 1, E2 - OSPF external type 2
          Dr - DHCPV6 Relay
          [*] - [AD/Metric]
Timers: Uptime
R           2001:ab8:49::/64 [120/5]
          via fe80::1271:d1ff:fec8:3300, eth-0-12, 00:26:05
```

2. 上述 Switch B 的配置结果如下：

```
Switch# show ipv6 rip database

Codes: R - RIP, Rc - RIP connected, Rs - RIP static, Ra - RIP aggregated,
          Rcx - RIP connect suppressed, Rsx - RIP static suppressed,
          K - Kernel, C - Connected, S - Static, O - OSPF, I - IS-IS, B - BGP
    Network                    Next Hop                  If          Met Tag Time
Rc 2001:ab8:49::/64            ::                        eth-0-48 1     0
Rc 2001:db8:12::/64            ::                        eth-0-12 1     0
R   2001:db8:48::/64           fe80::7e14:63ff:fe76:8900 eth-0-12 2     0    00:02:33

Switch# show ipv6 rip interface

eth-0-12 is up, line protocol is up
   Routing Protocol: RIPng
      Passive interface: Disabled
      Split horizon: Enabled with Poisoned Reversed
      IPv6 interface address:
         2001:db8:12::2/64
         fe80::1271:d1ff:fec8:3300/10
eth-0-48 is up, line protocol is up
   Routing Protocol: RIPng
      Passive interface: Disabled
      Split horizon: Enabled with Poisoned Reversed
      IPv6 interface address:
         2001:ab8:49::2/64
         fe80::1271:d1ff:fec8:3300/10

Switch# show ipv6 protocols rip

Routing Protocol is "ripng"
   Sending updates every 30 seconds with +/-5 seconds, next due in 13 seconds
   Timeout after 180 seconds, garbage collect after 120 seconds
   Outgoing update filter list for all interface is not set
   Incoming update filter list for all interface is not set
```

```
    Outgoing routes will have 3 added to metric if on list ripng_acl
    Default redistribute metric is 1
    Redistributing:
    Interface
      eth-0-12
      eth-0-48
    Routing for Networks:
    Number of routes (including connected): 3
    Distance: (default is 120)

Switch# show ipv6 route rip

IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, I - IS-IS, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       Dr - DHCPV6 Relay
       [*] - [AD/Metric]
Timers: Uptime
R        2001:db8:48::/64 [120/2]
       via fe80::7e14:63ff:fe76:8900, eth-0-12, 00:23:31
```

2.6.2 配置 Metric 参数

i. 介绍

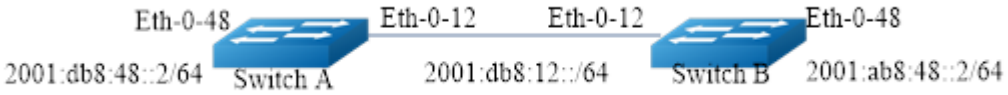
偏移度量值是附加在 RIPng 路由上的输入输出度量值，包括发送偏移度量值和接收偏移度量值。发送偏移度量值不会改变路由表中的路由度量值，仅当接口发送 RIP 路由信息时才会添加到发送路由上；接收偏移度量值会影响接收到的路由度量值，接口接收到一条合法的 RIP 路由时，在将其加入路由表前会把度量值附加到该路由上。偏移度量值一般包括如下的参数：

- 指定增加路由 Metric 的 ACL 参数说明如下。
  - **In**：应用在从邻居路由器学习到的 RIPng 的路由上
  - **Out**：应用在发布给邻居路由器 RIPng 通告上
- 匹配 ACL 路由的偏移值 Metric
- 应用偏移列表的接口

如果一个路由匹配全局偏移表（不指定接口）和一个基于接口的偏移列表，此时基于接口的偏移列表优先。在这种情况下，基于接口的偏移列表的度量值会被加到路由上。

ii. 拓扑

图 2-2 配置 Metric 参数拓扑图



iii. 配置文件

Switch A：

```
Switch# show run

interface eth-0-12
 no switchport
 ipv6 address auto link-local
 ipv6 address 2001:db8:12::1/64
 ipv6 router rip
!
interface eth-0-48
 no switchport
 ipv6 nd ra mtu suppress
 ipv6 address auto link-local
 ipv6 address 2001:db8:48::2/64
 ipv6 router rip
!
router ipv6 rip
!
```

Switch B：

```
Switch# show run

interface eth-0-12
 no switchport
 ipv6 address auto link-local
 ipv6 address 2001:db8:12::2/64
 ipv6 router rip
!
interface eth-0-48
```

```
 no switchport
 ipv6 nd ra mtu suppress
 ipv6 address auto link-local
 ipv6 address 2001:ab8:48::2/64
 ipv6 router rip
!
router ipv6 rip
!
```

iv. 配置示例

查看Switch B的RIPng路由表：

```
Switch# show ipv6 route rip

R        2001:db8:48::/64 [120/2]
         via fe80::7e14:63ff:fe76:8900, eth-0-12, 00:44:47
```

Switch A：配置 2001:db8:48::2/6 4 在 Eth-0-12 接口上增加 Metric 3：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)#ipv6 access-list ripngoffset	创建 ACL
Switch(config-ipv6-acl)# permit any 2001:db8:48::/64 any	匹配相应的网段
Switch(config-ipv6-acl)# router ipv6 rip	启用 RIPng 路由协议
Switch(config-router)# offset-list ripngoffset out 3 eth-0-12	设置偏移列表的 Metric 值

v. 命令验证

Switch B 的配置结果如下：

```
Switch# show ipv6 route rip

R        2001:db8:48::/64 [120/5]
         via fe80::7e14:63ff:fe76:8900, eth-0-12, 00:00:07
```

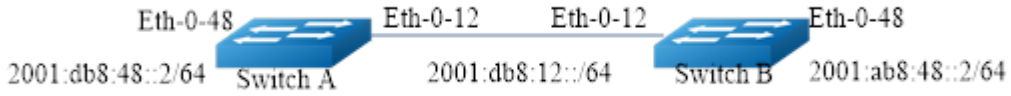
2.6.3 配置管理距离

i. 介绍

默认情况下，RIPng 的管理距离是 120。比较路由时，管理距离越低，路由越容易被选中。本小节介绍如何修改 RIPng 的管理距离。

ii. 拓扑

图 2-3 配置管理距离拓扑图



iii. 配置文件

Switch A：

```
Switch# show running-config

interface eth-0-12
 no switchport
 ipv6 address auto link-local
 ipv6 address 2001:db8:12::1/64
 ipv6 router rip
!
interface eth-0-48
 no switchport
 ipv6 nd ra mtu suppress
 ipv6 address auto link-local
 ipv6 address 2001:db8:48::2/64
 ipv6 router rip
!
router ipv6 rip
!
```

Switch B：

```
Switch# show running-config

interface eth-0-12
 no switchport
 ipv6 address auto link-local
 ipv6 address 2001:db8:12::2/64
 ipv6 router rip
!
interface eth-0-48
```

```
 no switchport
 ipv6 nd ra mtu suppress
 ipv6 address auto link-local
 ipv6 address 2001:ab8:48::2/64
 ipv6 router rip
!
router ipv6 rip
!
```

iv. 配置示例

查看Switch B 的RIPng路由表：

```
Switch# show ipv6 route rip

R          2001:db8:48::/64 [120/2]
           via fe80::7e14:63ff:fe76:8900, eth-0-12, 00:44:47
```

通过以下步骤改变交换机B的RIPng管理距离：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# router ipv6 rip	启用 RIPng 路由协议
Switch(config-router)# distance 100	配置 RIPng 路由的管理距离为 100

v. 命令验证

Switch B 的配置结果如下：

```
Switch# show ipv6 route rip

R          2001:db8:48::/64 [100/2]
           via fe80::7e14:63ff:fe76:8900, eth-0-12, 00:00:09
```

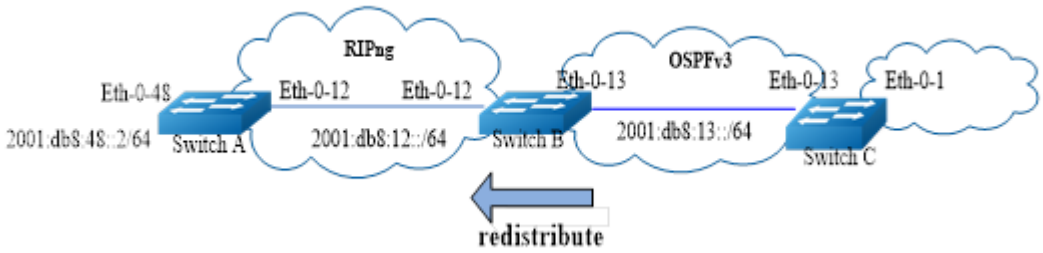
2.6.4 配置路由重分布

i. 介绍

用户可以将静态路由、直连路由以及其他路由协议（如 OSPFv3）的路由重分布到 RIP 中并被 RIPng 发送给它的邻居。默认 RIPng 的重发布 Metric 为 1，最大 16。将特定的路由重发布到 RIPng 上，其度量值可以是默认的，也可以是修改后的。下面例子讲述如何重分布其他的路由信息到 RIPng。

ii. 拓扑

图 2-4 配置路由重分布拓扑图



iii. 配置文件

Switch A：

```
Switch# show running-config

interface eth-0-12
 no switchport
 ipv6 address auto link-local
 ipv6 address 2001:db8:12::1/64
 ipv6 router rip
!
interface eth-0-48
 no switchport
 ipv6 nd ra mtu suppress
 ipv6 address auto link-local
 ipv6 address 2001:db8:48::2/64
 ipv6 router rip
!
router ipv6 rip
!
```

Switch B：

```
Switch# show running-config

interface eth-0-12
 no switchport
 ipv6 address auto link-local
 ipv6 address 2001:db8:12::2/64
 ipv6 router rip
!
interface eth-0-13
```

```
  no switchport
  ipv6 address auto link-local
  ipv6 address 2001:db8:13::1/64
  ipv6 router ospf area 0
!
interface eth-0-48
  no switchport
  ipv6 nd ra mtu suppress
  ipv6 address auto link-local
  ipv6 address 2001:ab8:48::2/64
  ipv6 router rip
!
router ipv6 rip
!
router ipv6 ospf
  router-id 1.1.1.1
```

Switch C：

```
Switch# show running-config

interface eth-0-1
  no switchport
ipv6 address auto link-local
  ipv6 address 2001:db8:1::1/64
  ipv6 router ospf area 0
!
interface eth-0-13
  no switchport
  ipv6 address 2001:db8:13::2/64
  ipv6 router ospf area 0
!
router ipv6 ospf
  router-id 2.2.2.2
!
```

iv. 配置示例

显示Switch A的路由表信息：

```
Switch# show ipv6 route rip

R          2001:ab8:48::/64 [120/5]
          via fe80::1271:d1ff:fec8:3300, eth-0-12, 01:43:37
```

显示Switch B的路由表信息：

```
Switch# show ipv6 route

O       2001:db8:1::/64 [110/2]
        via fe80::5c37:1dff:febe:2d00, eth-0-13, 00:31:17
R       2001:db8:48::/64 [120/5]
        via fe80::7e14:63ff:fe76:8900, eth-0-12, 00:49:57
```

Switch B的配置如下：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# router ipv6 rip	启用 RIPng 路由协议
Switch(config-router)#default-metric 2	指定默认的 Metric
Switch(config-router)#redistribute ospfv3 metric 5	重分布 OSPFv3 路由到 RIPng 中

v. 命令验证

检查Switch A的配置结果：

```
Switch# show ipv6 route rip

R       2001:ab8:48::/64 [120/5]
        via fe80::1271:d1ff:fec8:3300, eth-0-12, 01:48:23
R       2001:db8:1::/64 [120/6]
        via fe80::1271:d1ff:fec8:3300, eth-0-12, 00:00:19
```

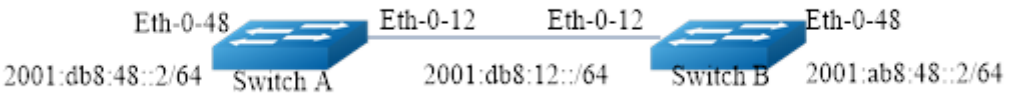
2.6.5 配置水平分割参数

i. 介绍

通常情况下，连接到组播网络并且使用距离矢量路由协议的路由器，使用水平分割机制来避免环路。配置水平分割可以使得从一个接口学到的路由不能通过此接口向外发布，这通常优化了多个路由器之间的通信，尤其在链路中断时。配置毒性逆转可以使得从一个接口学到的路由还可以从这个接口向外发布，但这些路由的度量值已设置为 16，即不可达。

ii. 拓扑

图 2-5 配置水平分割参数拓扑图



iii. 配置文件

Switch A：

```
Switch# show running-config

interface eth-0-12
 no switchport
 ipv6 address auto link-local
 ipv6 address 2001:db8:12::1/64
 ipv6 router rip
!
interface eth-0-48
 no switchport
 ipv6 nd ra mtu suppress
 ipv6 address auto link-local
 ipv6 address 2001:db8:48::2/64
 ipv6 router rip
!
router ipv6 rip
!
```

Switch B：

```
Switch# show running-config

interface eth-0-12
 no switchport
 ipv6 address auto link-local
 ipv6 address 2001:db8:12::2/64
 ipv6 router rip
!
interface eth-0-48
 no switchport
 ipv6 nd ra mtu suppress
 ipv6 address auto link-local
 ipv6 address 2001:ab8:48::2/64
 ipv6 router rip
```

```
!
router ipv6 rip
!
```

iv. 配置示例

Switch B:

1. 配置禁用水平分割

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)#interface eth-0-12	配置接口 eth-0-12
Switch(config-if)# no ipv6 rip split-horizon	禁用水平分割

2. 配置启用水平分割

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)#interface eth-0-12	配置接口 eth-0-12
Switch(config-if)# ipv6 rip split-horizon	启用水平分割

v. 命令验证

使用如下命令，验证上述配置：

show running-config

show ipv6 rip interface

2.6.6 配置 RIPng 路由过滤列表

i. 介绍

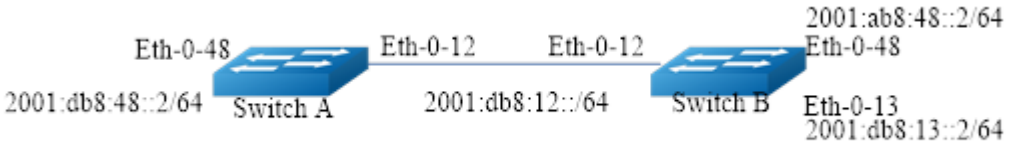
路由器提供路由信息过滤功能，通过指定访问控制列表和地址前缀列表，可以配置入口或出口过滤策略，对接收或发布的路由进行过滤。一个路由过滤列表通常包括如下参数：

- 一个被用作过滤器的 ACL 或 Prefix List。
- In 方向：过滤器被应用在学习到的路由上；Out 方向：过滤器被应用在发布的路由上。

- 应用过滤器的接口（可选）。

ii. 拓扑

图 2-6 配置 RIPng 路由过滤列表拓扑图



iii. 配置文件

Switch A：

```
Switch# show running-config

interface eth-0-12
 no switchport
 ipv6 address auto link-local
 ipv6 address 2001:db8:12::1/64
 ipv6 router rip
!
interface eth-0-48
 no switchport
 ipv6 nd ra mtu suppress
 ipv6 address auto link-local
 ipv6 address 2001:db8:48::2/64
 ipv6 router rip
!
router ipv6 rip
!
```

Switch B：

```
Switch# show running-config

interface eth-0-12
 no switchport
 ipv6 address auto link-local
 ipv6 address 2001:db8:12::2/64
 ipv6 router rip
!
```

```
interface eth-0-13
  no switchport
  ipv6 address auto link-local
  ipv6 address 2001:db8:13::1/64
  ipv6 router rip
!
interface eth-0-48
  no switchport
  ipv6 nd ra mtu suppress
  ipv6 address auto link-local
  ipv6 address 2001:ab8:48::2/64
  ipv6 router rip
!
router ipv6 rip
!
```

iv. 配置示例

Switch A的路由表信息如下：

```
Switch# show ipv6 route rip

R          2001:ab8:48::/64 [120/5]
           via fe80::1271:d1ff:fec8:3300, eth-0-12, 00:18:29
R          2001:db8:13::/64 [120/2]
           via fe80::1271:d1ff:fec8:3300, eth-0-12, 00:03:37
```

参照如下表中的命令，配置 Switch B：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# ipv6 prefix-list ripngfilter seq 5 deny 2001:db8:48::/64 Switch(config)# ipv6 prefix-list ripngfilter seq 10 permit any	建立列表
Switch(config)# router ipv6 rip	启用 RIPng 路由协议
Switch(config-router)# distribute-list prefix ripngfilter out eth-0-12	应用策略

v. 命令验证

检查Switch A的配置结果：

```
Switch# show ipv6 route rip

R          2001:db8:13::/64 [120/2]
           via fe80::1271:d1ff:fec8:3300, eth-0-12, 00:03:37
```

3 OSPFv3 配置

3.1 OSPFv3 简介

RIP 协议主要应用于小型网络中，有一定的局限性，如收敛慢、故障恢复时间较长、缺乏全局性、跳数限制等问题。而 OSPF 适用于大型网络，可以有效地解决这些问题。OSPF 协议为 IP 协议提供路由功能，OSPFv2（OSPF 版本 2）路由协议支持 IPv4，为了使 OSPF 协议支持 IPv6，技术人员开发了 OSPFv3（OSPF 版本 3）路由协议，OSPFv3 的定义及特性如下：

3.1.1 定义

开放最短路径优先协议 OSPF（Open Shortest Path First）是 IETF 组织开发的一个基于链路状态的内部网关协议，OSPFv3 是 OSPF 版本 3 的简称，主要提供对 IPv6 路由的支持，遵循的标准是 RFC5340 (OSPF for IPv6)，OSPFv3 和 OSPFv2 有很多方面是相同的，例如：

- Router ID，Area ID，LSA Link State ID 仍然是 32 位的。
- 协议报文类型一致，包括 Hello 报文、DD 报文、LSR 报文、LSU 报文和 LSAck 报文。
- 邻居发现和邻接建立机制相同。
- LSA 泛洪和老化机制相同。

OSPFv3 和 OSPFv2 有如下不同点：

- OSPFv3 是基于链路运行的，而 OSPFv2 是基于子网运行的。
- OSPFv3 在同一个链路上可以运行多个实例。
- OSPFv3 的拓扑关系和 IPv6 前缀信息分离。
- 使用 Link Local 地址作为路由下一跳。
- 新增了 Link LSA 以及本地链路泛洪范围。

3.1.2 特性

- 支持末梢区域:支持路由重分布,包括将其他路由协议学到的路由导入 OSPFv3 或者将 OSPFv3 学到的路由导出到其他路由协议中。
- 支持 OSPFv3 多进程。
- 支持在一条链路上运行多实例。

3.2 配置 OSPFv3 的基本功能

3.2.1 创建 OSPFv3 进程

只有在OSPFv3模式下配置了Router ID，OSPFv3进程才能正常运行，否则只能看到该进程，但无法生成LSA。

表3-1 创建OSPFv3进程

命令	操作	说明
configure terminal	进入全局配置模式	-
router ipv6 ospf [*process-id*]	创建 OSPFv3 进程并进入 OSPFv3 配置模式	process-id: OSPFv3 进程号，整数形式，取值范围是 1～65535。如果不指定进程号，缺省使用进程号 0

3.2.2 创建路由器 ID

此参数是 OSPFv3 协议中一个很重要的参数。在 OSPFv3 协议中，路由器 ID 号是一个 32 比特无符号整数，是一台路由器在 OSPFv3 自治系统中的唯一标识。用户必须在 OSPFv3 模式下配置路由器 ID 号，否则 OSPFv3 将无法运行。在手工设置路由器 ID 号时，必须保证自治系统中任意两台路由器 ID 号都不相同。若在已经有邻居的路由器上用此命令更改了路由器 ID，则该 ID 必须重新启用 OSPF 协议才能生效。

表3-2 创建路由器ID

命令	操作	说明
configure terminal	进入全局配置模式	-
router ipv6 ospf [*process-id*]	创建 OSPFv3 进程并进入	process-id: OSPFv3 进程号，整数形式，取值范

命令	操作	说明
	OSPFv3 配置模式	围是 1～65535。如果不指定进程号，缺省使用进程号 0
router-id *ip-address*	配置 OSPFv3 的路由器 ID	ip-address: IP 地址

3.2.3 配置接口使能 OSPFv3 功能

全局使能 IPv6 功能后，创建 OSPFv3 进程和路由器 ID。然后进入接口配置模式配置 IPv6 地址，将端口进入到创建的 OSPFv3 进程中，即可启用 OSPFv3 功能。

表3-3 配置接口使能OSPFv3功能

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
no switchport	使能三层接口属性	
no shutdown	开启端口	
ipv6 address *global-prefix* [**eui-64** | **anycast**]	配置接口上的 IPv6 地址	缺省情况下，接口上未配置 IPv6 地址； global-prefix: 全球单播地址，格式为 X:X::X:X/M format
ipv6 router ospf *process-id* **area** *area-id* [**instance** *instance-id*]	在接口上使能 OSPFv3 功能	process-id: OSPFv3 进程号，整数形式，取值范围是 1～65535 area-id: 区域标识符，标识符可以是十进制的或者是 IP 地址 instance-id: 实例 ID，取值范围是 0～255，缺省值是 0

3.3 配置 OSPFv3 的 Stub 区域

有两种 Stub 区域的路由配置命令：**stub** 和 **default-cost** 命令。更多关于 OSPFv3 的区域参数配置可参考 3.7.3 配置 OSPF 区域参数示例。

表3-4 配置OSFPv3的Stub区域

命令	操作	说明
configure terminal	进入全局配置模式	-
router ipv6 ospf [*process-id*]	创建 OSPFv3 进程并进入 OSPFv3 配置模式	process-id: OSPFv3 进程号，整数形式，取值范围是 1～65535。如果不指定进程号，缺省使用进程号 0
area *area-id* **stub** [**no-summary**]	配置指定区域为 Stub（存根）区域	缺省情况下，没有区域被设置为 Stub（存根）区域 area-id: 以 ID 或者 IP 地址标识的 OSPF 区域
area *area-id* **default-cost** *cost*	配置 Stub 区域及其 Cost 值	area-id: 区域标识符，可以是十进制的或者是 IP 地址 cost: 取值范围为 0~16777215

说明

配置 Stub 区域后只学习类型为 1 类 (Router-Lsa)，2 类 (Network Lsa)和 3 类 (Summary Lsa)的 LSA。

3.4 配置 OSPFv3 路由信息控制

3.4.1 配置 OSPFv3 路由聚合

1. 配置ABR路由聚合

只能在ABR路由器上使用**area range**命令，对当前区域进行路由聚合。聚合的结果是由ABR把单一的汇总路由宣告给其他区域。一个区域可配置多条聚合网段，这样OSPFv3可对多个网段进行聚合。

表3-5 配置ABR路由聚合

命令	操作	说明
configure terminal	进入全局配置模式	-
router ipv6 ospf [*process-id*]	创建 OSPFv3 进程并进入 OSPFv3 配置模式	process-id: OSPFv3 进程号，整数形式，取值范围是 1～65535。如果不指定进程号，缺省使用进程号 0
area *area-id* **range** *ipv6-address*/*mask* [**not-advertise**]	配置 ABR 路由聚合	缺省情况下，不对路由进行聚合 area-id: 以 ID 标识的 OSPF 区域 ipv6-address/mask: 聚合路由的目的 IPv6 地址/地址前缀长度

2. 配置ASBR路由聚合

从其他路由协议学到的路由可以在 ASBR 上进行汇总，汇总路由里的 metric 值选择的是所有被汇总的路由中的最大值。该命令可以用来帮助减少路由表的大小。配置 **summary-address** 命令后，对处于聚合地址范围内的外部路由，本地路由器只向邻居路由器发布一条聚合后的路由。用户可以使用命令 **area range** 对 OSPF 区域间的路由进行汇总。

表3-6 配置ASBR路由聚合

命令	操作	说明
configure terminal	进入全局配置模式	-
router ipv6 ospf [*process-id*]	创建 OSPFv3 进程并进入 OSPFv3 配置模式	process-id: OSPFv3 进程号，整数形式，取值范围是 1～65535。如果不指定进程号，缺省使用进程号 0
summary-address *prefix*/*prefix-length* [**not-advertise**] [**tag** *tag-value*]	配置 ASBR 路由聚合	缺省情况下，不对外部路由进行聚合 prefix/prefix-length: IPv6 路由的前缀/前缀长度 tag-value: 路由标记，取值范围为 0~4294967295，默认值

命令	操作	说明
		为 0

3.4.2 配置 OSPFv3 引入外部路由

1. 配置OSPFv3引入其他协议的路由

外部路由是指到达自治系统外部的路由，有以下两种：

Type-1 外部路由指接收的 IGP 路由，如 RIPng 和 STATIC。此类路由有较高的可靠性，所以外部路由开销的计算结果等于自治系统的内部路由开销，并可与 OSPF 本身的路由开销相比较。也就是说，到达 Type-1 外部路由的开销等于路由器到达对应 ASBR 的开销加上 ASBR 到达目的地址的开销。

Type-2 外部路由指接收的 EGP 路由。此类路由可靠性较低，所以 OSPF 协议认为从 ASBR 到达自治系统外部的路由开销要远远高于自治系统内部到达 ASBR 的路由开销。因此在计算路由开销时主要考虑前者。也就是说，到达 Type-2 外部路由的开销等于 ASBR 到达目的地址的开销。

表3-7 配置OSPFv3引入其他协议的路由

命令	操作	说明
configure terminal	进入全局配置模式	-
router ipv6 ospf [*process-id*]	创建 OSPFv3 进程并进入 OSPFv3 配置模式	process-id: OSPFv3 进程号，整数形式，取值范围是 1～65535。如果不指定进程号，缺省使用进程号 0
default-metric *metric-value*	配置 OSPFv3 引入外部路由时的开销	metric-value: 指定的路由开销值，默认为 20
redistribute { bgp | connected | ripng | static | ospfv3 [*process-id*] } [**route-map** *word*] [**tag** *tag-value*] [**metric** *metric-value*] [**metric-type** *type-value*]	配置路由重发布，将其他协议的路由引入到 OSPFv3 路由域	process-id: OSPFv3 的进程 ID word: 路由策略名 tag-value: 路由标记值 metric-value: 重发布路由时的度量值，默认为 20 type-value: Type-1 外部路由和 Type-2 外部路由；缺省情况下，引

命令	操作	说明
		入类型 2 的外部路由。目前不支持 BGP 和 route-map

2. 配置OSPFv3引入缺省路由

表3-8 配置OSPFv3引入缺省路由

命令	操作	说明
configure terminal	进入全局配置模式	-
router ipv6 ospf [*process-id*]	创建 OSPFv3 进程并进入 OSPFv3 配置模式	process-id: OSPFv3 进程号，整数形式，取值范围是 1～65535。如果不指定进程号，缺省使用进程号 0
default-information originate [**route-map** *word*] [**always**] [**metric** *metric-value*] [**metric-type** *type-value*]	配置 OSPFv3 引入缺省路由	缺省情况下，未引入缺省路由 word: 路由策略，目前不支持 IPv6 的 route-map，如果配置了 route-map，会当作不存在处理 metric-value: 生成默认路由的 Metric，未指定时，默认值是 1 type-value: Type-1 外部路由和 Type-2 外部路由；缺省情况下，引入类型 2 的外部路由

3.4.3 配置接口的开销值

表3-9 配置接口的开销值

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
no switchport	使能三层接口属性	
ipv6 ospf cost *interface-cost* [**instance** *instance-id*]	配置接口的开销值	interface-cost: 取值范围为 1 ~ 65535 instance-id: 指定接口所属的实

命令	操作	说明
		例 ID，取值范围是 0～255，缺省值为 0

3.4.4 配置带宽参考值

使用 **ipv6 ospf cost** 命令设置的端口Cost值将会覆盖用该命令计算出来的cost值。计算链路开销的公式为：参考带宽/端口速率。

表3-10 配置带宽参考值

命令	操作	说明
configure terminal	进入全局配置模式	-
router ipv6 ospf [*process-id*]	创建 OSPFv3 进程并进入 OSPFv3 配置模式	process-id: OSPFv3 进程号，整数形式，取值范围是 1～65535。如果不指定进程号，缺省使用进程号 0
auto-cost reference-bandwidth *rate*	配置计算链路开销时所依据的带宽参考值	rate: 取值范围为 1 ~4294967，单位：Mbps；默认是 100

3.5 优化 OSPFv3 网络性能

3.5.1 配置接口发送 LSA 报文的延迟时间

LSA 在本路由器的链路状态数据库（LSDB）中会随时间老化（每秒钟加1），但在网络的传输过程中却不会，所以有必要在发送之前在LSA 的老化时间上增加一定的延迟时间。此配置对低速率的网络尤其重要。

表3-11 配置接口发送LSA报文的延迟时间

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
no switchport	设置接口为三层接口	-

命令	操作	说明
ipv6 ospf transmit-delay *seconds* [**instance** *instance-id*]	配置接口发送 LSA 报文的延迟时间	seconds: 延迟时间，取值范围为 1~65535，单位：秒，缺省值为 1 秒 instance-id: 指定接口所属的实例 ID，取值范围为 0～255，缺省值为 0

3.5.2 配置 SPF 计算时间间隔

表3-12 配置SPF计算时间间隔

命令	操作	说明
configure terminal	进入全局配置模式	-
router ipv6 ospf [*process-id*]	创建 OSPFv3 进程并进入 OSPFv3 配置模式	process-id: OSPFv3 进程号，整数形式，取值范围是 1～65535。如果不指定进程号，缺省使用进程号 0
timers spf exp *spf-hold-min spf-hold-max*	配置 SPF 计算时间间隔	spf-hold-min: SPF 计算的最小时间间隔 spf-hold-max: SPF 计算的最大时间间隔

3.5.3 配置 LSA 重传时间间隔

当一个路由器发送 LSA 报文到它的邻居时，它会缓存该报文直到收到邻居的确认报文。如果在重传时间间隔内没有收到确认报文，该 LSA 将被重传。设置该值必须要谨慎，以免引起不必要的重传。通常，这个值要大于两个路由器之间的报文往返延迟。

表3-13 配置LSA重传时间间隔

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
no switchport	设置接口为三层接口	-

命令	操作	说明
ipv6 ospf retransmit-interval *seconds* [**instance** *instance-id*]	配置 LSA 重传时间间隔	seconds: 重传时间间隔，取值范围为 1~65535，单位：秒，缺省值为 5 秒 instance-id: 指定接口所属的实例 ID，取值范围为 0～255，缺省值为 0

3.5.4 配置端口 DR 的优先级

端口的优先级主要用来选举网络中的 DR 和 BDR，优先级高的会被选举为 DR。如果优先级相等，则 Router-ID 值较大的会被选举为 DR；如果某一个端口的优先级被设置为 0，则此端口不会参加 DR 和 BDR 的选举。端口优先级只在多路访问的网络中起作用，即对点对点网络无效。

表3-14 配置端口的优先级

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
no switchport	设置接口为三层接口	-
ipv6 ospf priority *priority-value* [**instance** *instance-id*]	配置端口 DR 的优先级	priority-value: 优先级的取值范围为 0～255，默认值是 1 instance-id: 指定接口所属的实例 ID，取值范围为 0～255，缺省值为 0

3.5.5 忽略 DD 报文中的 MTU 检测

OSPFv3 检查邻居是否使用相同的 MTU 值。这个检查在互相交换数据库描述（DD）报文时产生，如果在接收到的 DD 报文里的 MTU 高于入接口上配置的 MTU，OSPFv3 邻接将无法建立。

表3-15 配置端口的优先级

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称

命令	操作	说明
no switchport	设置接口为三层接口	-
ipv6 ospf mtu-ignore [**instance** *instance-id*]	忽略 DD 报文中的 MTU 检测	缺省情况下，默认接口启用 MTU 的匹配功能 instance-id: 指定接口所属的实例 ID，取值范围是 0～255，缺省值是 0

3.6 OSPFv3 显示与维护

表3-16 OSPF显示与维护

命令	操作	说明
show ipv6 ospf [*process-id*]	查看全部或指定 OSPFv3 路由进程相关信息	process-id: OSPFv3 进程号
show ipv6 ospf [*process-id*] **database** [**external | inter-prefix | inter-router | intra-prefix | link | network | router**] [*link-state-id*] [**adv-router** *router-id* | **self-originate**] **show ipv6 ospf** [*process-id*] **database max-age**	显示 OSPFv3 路由进程的链路状态数据库信息	process-id: OSPFv3 进程号 link-state-id: 查看自治系统边界路由器的汇总 LSA 信息 router-id: 查看指定 OSPFv3 宣告路由器的 LSA 信息
show ipv6 ospf interface [*if-name*]	显示 OSPFv3 接口的信息	if-name: 接口名称 neighbor-id: 邻居 ID（点分十进制）
show ipv6 ospf neighbor [*if-name*] [*neighbor-id*] [**detail**]	显示 OSPFv3 邻居信息	
show ipv6 ospf [*process-id*] **database database-summary**	显示 OSPFv3 数据库信息的摘要和汇总	process-id: OSPFv3 进程号
show ipv6 ospf [*process-id*] **route**	显示 OSPFv3 路由的信息	
show ipv6 ospf [*process-id*] **route summary**	显示 OSPFv3 路由的信息汇总	

命令	操作	说明
show ipv6 protocols ospf	查看 OSPFv3 协议的参数设置信息	-

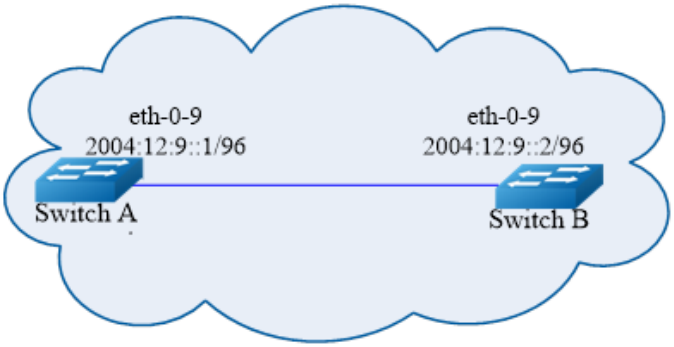
3.7 OSPFv3 配置举例

3.7.1 配置接口启用 OSPFv3

下面的例子描述了一个接口上启用 OSPFv3 所需的最低配置。

i. 拓扑

图 3-1 配置接口启用 OSPFv3 拓扑图



ii. 配置步骤

Switch A:

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch (config)# ipv6 enable	使能 IPv6
Switch(config)# router ipv6 ospf 100	创建 OSPFv3 进程号 100
Switch(config-router)# router-id 1.1.1.1	指定 Router ID
Switch(config-router)# exit	退出 OSPFv3 配置模式

命令举例	操作步骤
Switch(config)# interface eth-0-9	进入接口配置模式
Switch(config-if)# no switchport	使能三层接口属性
Switch(config-if)# no shutdown	端口 UP
Switch(config-if)# ipv6 address 2004:12:9::1/96	配置 IPv6 地址
Switch(config-if)# ipv6 router ospf 100 area 0 instance 0	将该端口加入到 OSPFv3 process 100、area 0、instance 0 中
Switch(config-if)# end	退出至特权模式

Switch B:

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch (config)# ipv6 enable	使能 IPv6
Switch(config)# router ipv6 ospf 200	创建 OSPFv3 进程号 200
Switch(config-router)# router-id 2.2.2.2	指定 Router ID
Switch(config-router)# exit	退出 OSPFv3 配置模式
Switch(config)# interface eth-0-9	进入接口配置模式
Switch(config-if)# no switchport	使能三层接口属性
Switch(config-if)# no shutdown	端口 UP
Switch(config-if)# ipv6 address 2004:12:9::2/96	配置 IPv6 地址
Switch(config-if)# ipv6 router ospf 200 area 0 instance 0	将该端口加入到 OSPFv3 process 200、area 0、instance 0 中
Switch(config-if)# end	退出至特权模式

iii. 命令验证

使用 **show ipv6 ospf database**、**show ipv6 ospf interface**、**show ipv6 ospf neighbor**、**show ipv6 ospf route** 命令，验证上述配置。

- 检查Switch A的配置结果：

```
Switch# show ipv6 ospf database

            OSPFv3 Router with ID (1.1.1.1) (Process 100)
                Link-LSA (Interface eth-0-9)
Link State ID   ADV Router      Age  Seq#       CkSum  Prefix
0.0.0.9         1.1.1.1         614 0x80000001 0x6a40  1
0.0.0.9         2.2.2.2          68 0x80000001 0x4316  1
                Router-LSA (Area 0.0.0.0)
Link State ID   ADV Router      Age  Seq#       CkSum  Link
0.0.0.0         1.1.1.1          54 0x80000003 0xb74b  1
0.0.0.0         2.2.2.2          55 0x80000003 0x9965  1
                Network-LSA (Area 0.0.0.0)
Link State ID   ADV Router      Age  Seq#       CkSum
0.0.0.9         1.1.1.1          54 0x80000001 0x3ed1
                Intra-Area-Prefix-LSA (Area 0.0.0.0)
Link State ID   ADV Router      Age  Seq#       CkSum  Prefix  Reference
0.0.0.2         1.1.1.1          53 0x80000001 0x450a  1  Network-LSA

Switch# show ipv6 ospf neighbor

OSPFv3 Process (100)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
2.2.2.2           1   Full/Backup      00:00:33   eth-0-9    0

Switch# show ipv6 ospf route

OSPFv3 Process (100)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2
    Destination                                        Metric
      Next-hop
C   2004:12:9::/96                                        1
      directly connected, eth-0-9, Area 0.0.0.0
```

- 检查Switch B的配置结果：

```
Switch# show ipv6 ospf database

            OSPFv3 Router with ID (2.2.2.2) (Process 200)
                Link-LSA (Interface eth-0-9)
Link State ID   ADV Router      Age  Seq#       CkSum  Prefix
0.0.0.9         1.1.1.1         774 0x80000001 0x6a40  1
0.0.0.9         2.2.2.2         228 0x80000001 0x4316  1
                Router-LSA (Area 0.0.0.0)
Link State ID   ADV Router      Age  Seq#       CkSum  Link
0.0.0.0         1.1.1.1         217 0x80000003 0xb74b  1
0.0.0.0         2.2.2.2         214 0x80000003 0x9965  1
                Network-LSA (Area 0.0.0.0)
Link State ID   ADV Router      Age  Seq#       CkSum
```

```
0.0.0.9          1.1.1.1          215 0x80000001 0x3ed1
                  Intra-Area-Prefix-LSA (Area 0.0.0.0)
Link State ID    ADV Router       Age  Seq#       CkSum  Prefix  Reference
0.0.0.2          1.1.1.1          214 0x80000001 0x450a      1   Network-LSA

Switch# show ipv6 ospf neighbor

OSPFv3 Process (200)
Neighbor ID     Pri   State           Dead Time   Interface  Instance ID
1.1.1.1           1   Full/DR         00:00:35    eth-0-9    0

Switch# show ipv6 ospf route

OSPFv3 Process (200)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2
    Destination                                        Metric
      Next-hop
C   2004:12:9::/96                                        1
      directly connected, eth-0-9, Area 0.0.0.0
```

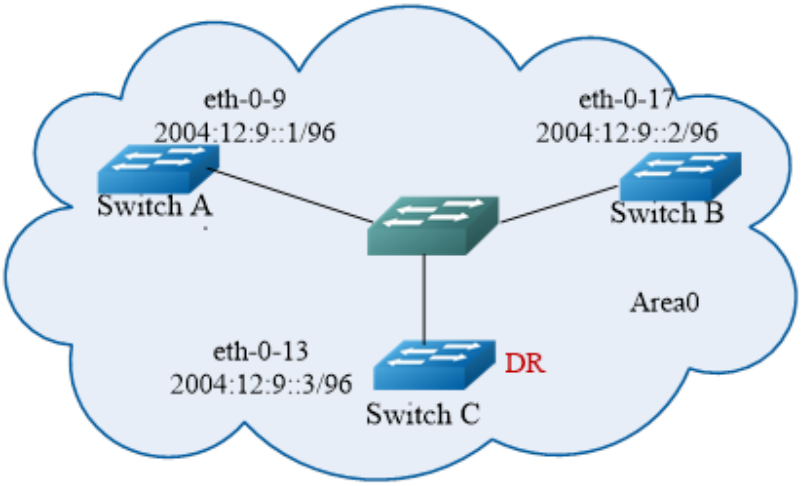
3.7.2 配置 OSPFv3 优先级

i. 介绍

本小节主要讲述如何配置接口优先级，优先级高的成为 DR。优先级为 0 的不参与 DR 选举。Switch C 的优先级是 10，比 Switch A 和 Switch B 的默认优先级 1 要高，因此 Switch C 将成为这个网络内的 DR。

ii. 拓扑

图 3-2 配置 OSPFv3 优先级拓扑图



iii. 配置方法

Switch A：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# ipv6 enable	使能 IPv6
Switch(config)# router ipv6 ospf 100	创建 OSPFv3 进程号 100
Switch(config-router)# router-id 1.1.1.1	指定 Router ID
Switch(config-router)# exit	退出 OSPFv3 配置模式
Switch(config)# interface eth-0-9	进入接口配置模式
Switch(config-if)# no switchport	使能三层接口属性
Switch(config-if)# no shutdown	端口 UP
Switch(config-if)# ipv6 address 2004:12:9::1/96	配置 IPv6 地址
Switch(config-if)# ipv6 router ospf 100 area 0 instance 0	将该端口加入到 OSPFv3 process 100、area 0、instance0 中
Switch(config-if)# end	退出至特权模式

Switch B：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# ipv6 enable	使能 IPv6
Switch(config)# router ipv6 ospf 200	创建 OSPFv3 进程号 200
Switch(config-router)# router-id 2.2.2.2	指定 Router ID
Switch(config-router)# exit	退出 OSPFv3 配置模式
Switch(config)# interface eth-0-17	进入接口配置模式
Switch(config-if)# no switchport	使能三层接口属性
Switch(config-if)# no shutdown	端口 UP
Switch(config-if)# ipv6 address 2004:12:9::2/96	配置 IPv6 地址
Switch(config-if)# ipv6 router ospf 200 area 0 instance 0	将该端口加入到 OSPFv3 process 200、area 0、instance 0 中
Switch(config-if)# end	退出至特权模式

Switch C：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# ipv6 enable	使能 IPv6
Switch(config)# router ipv6 ospf 300	创建 OSPFv3 进程号 300
Switch(config-router)# router-id 3.3.3.3	指定 Router ID
Switch(config-router)# exit	退出 OSPFv3 配置模式
Switch(config)# interface eth-0-13	进入接口配置模式
Switch(config-if)# no switchport	使能三层接口属性
Switch(config-if)# no shutdown	端口 UP
Switch(config-if)# ipv6 address 2004:12:9::3/96	配置 IPv6 地址
Switch(config-if)# ipv6 router ospf 300 area 0 instance 0	将该端口加入到 OSPFv3 process300、area 0、instance0 中

命令举例	操作步骤
Switch(config-if)# end	退出至特权模式

iv. 命令验证

使用 **show ipv6 ospf neighbor**、**show ipv6 ospf interface** 命令，验证以上配置是否正确。

检查 Switch C 的配置结果：

```
Switch# show ipv6 ospf interface

eth-0-13 is up, line protocol is up
  Interface ID 13
  IPv6 Prefixes
    fe80::ee66:91ff:fe45:db00/10 (Link-Local Address)
    2004:12:9::3/96
  OSPFv3 Process (300), Area 0.0.0.0, Instance ID 0
    Router ID 3.3.3.3, Network Type BROADCAST, Cost: 1
    Transmit Delay is 1 sec, State DR, Priority 10
    Designated Router (ID) 3.3.3.3
      Interface Address fe80::ee66:91ff:fe45:db00
    Backup Designated Router (ID) 2.2.2.2
      Interface Address fe80::c629:f2ff:fe02:3600
    Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit 5
      Hello due in 00:00:01
Neighbor Count is 2, Adjacent neighbor count is 2

Switch# show ipv6 ospf neighbor

OSPFv3 Process (300)
Neighbor ID     Pri   State           Dead Time   Interface   Instance ID
1.1.1.1           1   Full/DROther    00:00:32    eth-0-13    0
2.2.2.2           1   Full/Backup     00:00:36    eth-0-13    0
```

3.7.3 配置 OSPFv3 区域参数

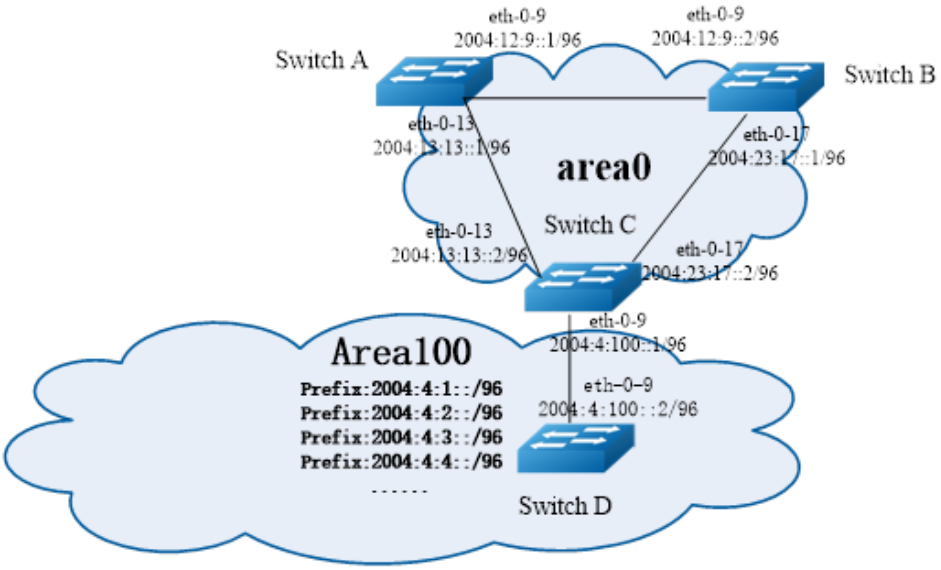
i. 介绍

用户可以选择性地配置多个 OSPFv3 区域参数。这些参数将区域配置为末梢区域(Stub)。Stub 区域是一些特定的区域，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都会大大减少。为保证到自治系统外的路由依旧可达，该区域的 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。

路由聚合是指 ABR 或 ASBR 将具有相同前缀的路由信息聚合，只发布一条路由到其它区域。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。如果网络号是连续的，你可以使用 **area range** 命令将这些连续的网段聚合成一个网段。这样 ABR 只发送一条聚合后的 LSA，所有属于本命令指定的聚合网段范围的 LSA 将不再会被单独发送出去，可减少其它区域中 LSDB 的规模。

ii. 拓扑

图 3-3 配置 OSPFv3 区域拓扑图



iii. 配置步骤

Switch A:

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# ipv6 enable	使能 IPv6
Switch(config)# router ipv6 ospf 100	创建 OSPFv3 进程号 100
Switch(config-router)# router-id 1.1.1.1	指定 Router ID

命令举例	操作步骤
Switch(config-router)# exit	退出 OSPFv3 配置模式
Switch(config)# interface eth-0-9	进入接口配置模式
Switch(config-if)# no switchport	使能三层接口属性
Switch(config-if)# no shutdown	端口 UP
Switch(config-if)# ipv6 address 2004:12:9::1/96	配置 IPv6 地址
Switch(config-if)# ipv6 router ospf 100 area 0 instance 0	将该端口加入到 OSPFv3 process 100、area 0、instance 0 中
Switch(config-if)# end	退出至特权模式
Switch# configure terminal	进入全局配置模式.
Switch(config)#interface eth-0-13	进入接口配置模式
Switch(config-if)#no switchport	设置接口为三层接口
Switch(config-if)#no shutdown	端口 UP
Switch(config-if)# ipv6 address 2004:13:13::2/96	设置端口的 IP 地址
Switch(config-if)# ipv6 router ospf 100 area 0 instance 0	将该端口加入到 OSPFv3 process100、area0、instance0 中
Switch(config-if)# end	退出至特权模式

Switch B:

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# ipv6 enable	使能 IPv6
Switch(config)# router ipv6 ospf 200	创建 OSPFv3 进程号 200
Switch(config-router)# router-id 2.2.2.2	指定 Router ID
Switch(config-router)# exit	退出 OSPFv3 配置模式
Switch(config)# interface eth-0-9	进入接口配置模式
Switch(config-if)# no switchport	使能三层接口属性

命令举例	操作步骤
Switch(config-if)# no shutdown	端口 UP
Switch(config-if)# ipv6 address 2004:12:9::2/96	配置 IPv6 地址
Switch(config-if)# ipv6 router ospf 200 area 0 instance 0	将该端口加入到 OSPFv3 process 200、area 0、instance 0 中
Switch(config-if)# end	退出至特权模式
Switch# configure terminal	进入全局配置模式.
Switch(config)#interface eth-0-17	进入接口配置模式
Switch(config-if)#no switchport	设置接口为三层接口
Switch(config-if)#no shutdown	端口 UP
Switch(config-if)# ipv6 address 2004:23:17::1/96	设置端口的 IP 地址
Switch(config-if)# ipv6 router ospf 200 area 0 instance 0	将该端口加入到 OSPFv3 process 200、area 0、instance 0 中
Switch(config-if)# end	退出至特权模式

Switch C：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch (config)# ipv6 enable	使能 IPv6
Switch(config)# router ipv6 ospf 300	创建 OSPFv3 进程号 300
Switch(config-router)# router-id 3.3.3.3	指定 Router ID
Switch(config-router)# exit	退出 OSPFv3 配置模式
Switch(config)# interface eth-0-13	进入接口配置模式
Switch(config-if)# no switchport	使能三层接口属性
Switch(config-if)# no shutdown	端口 UP
Switch(config-if)# ipv6 address 2004:13:13::2/96	配置 IPv6 地址
Switch(config-if)# ipv6 router ospf 300 area 0 instance 0	将该端口加入到 OSPFv3 process 300、area 0、instance 0 中

命令举例	操作步骤
Switch(config-if)# end	退出至特权模式
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-17	进入接口配置模式
Switch(config-if)# no switchport	使能三层接口属性
Switch(config-if)# no shutdown	端口 UP
Switch(config-if)# ipv6 address 2004:23:17::2/96	配置 IPv6 地址
Switch(config-if)# ipv6 router ospf 300 area 0 instance 0	将该端口加入到 OSPFv3 process 300、area 0、instance 0 中
Switch(config-if)# end	退出至特权模式
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-9	进入接口配置模式
Switch(config-if)# no switchport	使能三层接口属性
Switch(config-if)# no shutdown	端口 UP
Switch(config-if)# ipv6 address 2004:4:100::1/96	配置 IPv6 地址
Switch(config-if)# ipv6 router ospf 300 area 100 instance 0	将该端口加入到 OSPFv3 process 300、area 100、instance 0 中
Switch(config-if)# end	退出至特权模式
Switch# configure terminal	进入全局配置模式
Switch(config)# router ipv6 ospf 300	进入 OSPF 进程号 300
Switch(config-router)# area 100 range 2004:4::/32	指定一段 prefix 发布到 OSPFv3 区域 0
Switch(config-router)# area 100 stub no-summary	区域 100 设置成 Stub 区域
Switch(config-router)# end	退出 OSPFv3 配置模式

Switch D：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式

命令举例	操作步骤
Switch (config)# ipv6 enable	使能 IPv6
Switch(config)# router ipv6 ospf 400	创建 OSPFv3 进程号 400
Switch(config-router)# router-id 4.4.4.4	指定 Router ID
Switch(config-router)# area 100 stub no-summary	区域 100 设置成 Stub 区域
Switch(config-router)# exit	退出 OSPFv3 配置模式
Switch(config)# interface eth-0-9	进入接口配置模式
Switch(config-if)# no switchport	使能三层接口属性
Switch(config-if)# no shutdown	端口 UP
Switch(config-if)# ipv6 address 2004:4:100::2/96	配置 IPv6 地址
Switch(config-if)# ipv6 router ospf 400 area 100 instance 0	将该端口加入到 OSPFv3 process 300、area 100、instance0 中
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# no switchport	使能三层接口属性
Switch(config-if)# no shutdown	端口 UP
Switch(config-if)# ipv6 address 2004:4:1::1/96	配置 IPv6 地址
Switch(config-if)# ipv6 router ospf 400 area 100 instance 0	将该端口加入到 OSPFv3 process 300、area 100、instance 0 中
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface eth-0-2	进入接口配置模式
Switch(config-if)# no switchport	使能三层接口属性
Switch(config-if)# no shutdown	端口 UP
Switch(config-if)# ipv6 address 2004:4:2::1/96	配置 IPv6 地址
Switch(config-if)# ipv6 router ospf 400 area 100 instance 0	将该端口加入到 OSPFv3 process 300、area 100、instance 0 中
Switch(config-if)# exit	退出接口配置模式

命令举例	操作步骤
Switch(config)# interface eth-0-3	进入接口配置模式
Switch(config-if)# no switchport	使能三层接口属性
Switch(config-if)# no shutdown	端口 UP
Switch(config-if)# ipv6 address 2004:4:3::1/96	配置 IPv6 地址
Switch(config-if)# ipv6 router ospf 400 area 100 instance 0	将该端口加入到 OSPFv3 process 300、area 100、instance0 中
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface eth-0-4	进入接口配置模式
Switch(config-if)# no switchport	使能三层接口属性
Switch(config-if)# no shutdown	端口 UP
Switch(config-if)# ipv6 address 2004:4:4::1/96	配置 IPv6 地址
Switch(config-if)# ipv6 router ospf 400 area 100 instance 0	将该端口加入到 OSPFv3 process 300、area 100、instance 0 中
Switch(config-if)# end	退出至特权模式

iv. 命令验证

使用**show ipv6 route**命令验证上述配置。

- Switch A的配置结果如下：

```
Switch# show ipv6 route

IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, I - IS-IS, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       Dr - DHCPV6 Relay
       [*] - [AD/Metric]
Timers: Uptime
O IA     2004:4::/32 [110/3]
       via fe80::c629:f2ff:fe02:3600, eth-0-13, 00:01:00
C        2004:12:9::/96
       via ::, eth-0-9, 00:15:56
C        2004:12:9::1/128
```

```
          via ::1, eth-0-9, 00:15:56
C           2004:13:13::/96
          via ::, eth-0-13, 00:15:55
C           2004:13:13::2/128
          via ::1, eth-0-13, 00:15:55
O           2004:23:17::/96 [110/2]
          via fe80::bc22:aeff:fe64:aa00, eth-0-9, 00:08:10
          via fe80::c629:f2ff:fe02:3600, eth-0-13, 00:08:10
C           fe80::/10
          via ::, Null0, 00:15:57
```

- Switch B的配置结果如下：

```
Switch# show ipv6 route

IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, I - IS-IS, B - BGP
          O - OSPF, IA - OSPF inter area
          N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
          E1 - OSPF external type 1, E2 - OSPF external type 2
          Dr - DHCPV6 Relay
          [*] - [AD/Metric]
Timers: Uptime
O IA      2004:4::/32 [110/3]
          via fe80::c629:f2ff:fe02:3600, eth-0-17, 00:00:57
C           2004:12:9::/96
          via ::, eth-0-9, 00:12:24
C           2004:12:9::2/128
          via ::1, eth-0-9, 00:12:24
O           2004:13:13::/96 [110/2]
          via fe80::b242:55ff:fe05:ff00, eth-0-9, 00:07:52
          via fe80::c629:f2ff:fe02:3600, eth-0-17, 00:07:52
C           2004:23:17::/96
          via ::, eth-0-17, 00:12:24
C           2004:23:17::1/128
          via ::1, eth-0-17, 00:12:24
C           fe80::/10
          via ::, Null0, 00:12:26
```

- Switch C的配置结果如下：

```
Switch# show ipv6 route

IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, I - IS-IS, B - BGP
          O - OSPF, IA - OSPF inter area
          N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
        E1 - OSPF external type 1, E2 - OSPF external type 2
        Dr - DHCPV6 Relay
        [*] - [AD/Metric]
Timers: Uptime
O         2004:4::/32 [110/0]
        via ::, Null0, 00:08:31
O         2004:4:1::/96 [110/2]
        via fe80::ee66:91ff:fe45:db00, eth-0-9, 00:01:08
O         2004:4:2::/96 [110/2]
        via fe80::ee66:91ff:fe45:db00, eth-0-9, 00:01:08
O         2004:4:3::/96 [110/2]
        via fe80::ee66:91ff:fe45:db00, eth-0-9, 00:01:08
O         2004:4:4::/96 [110/2]
        via fe80::ee66:91ff:fe45:db00, eth-0-9, 00:01:08
C         2004:4:100::/96
        via ::, eth-0-9, 00:08:32
C         2004:4:100::1/128
        via ::1, eth-0-9, 00:08:32
O         2004:12:9::/96 [110/2]
        via fe80::b242:55ff:fe05:ff00, eth-0-13, 00:08:03
        via fe80::bc22:aeff:fe64:aa00, eth-0-17, 00:08:03
O         2004:13:13::/96 [110/1]
        via fe80::b242:55ff:fe05:ff00, eth-0-13, 00:08:18
C         2004:23:17::/96
        via ::, eth-0-17, 00:08:32
C         2004:23:17::2/128
        via ::1, eth-0-17, 00:08:32
C         fe80::/10
        via ::, Null0, 00:08:34
```

- Switch D的配置结果如下：

```
Switch# show ipv6 route

IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, I - IS-IS, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        Dr - DHCPV6 Relay
        [*] - [AD/Metric]
Timers: Uptime
O IA      ::/0 [110/2]
        via fe80::c629:f2ff:fe02:3600, eth-0-9, 00:00:53
C         2004:4:1::/96
        via ::, eth-0-1, 00:03:09
C         2004:4:1::1/128
        via ::1, eth-0-1, 00:03:09
```

```
C        2004:4:2::/96
         via ::, eth-0-2, 00:03:08
C        2004:4:2::1/128
         via ::1, eth-0-2, 00:03:08
C        2004:4:3::/96
         via ::, eth-0-3, 00:03:08
C        2004:4:3::1/128
         via ::1, eth-0-3, 00:03:08
C        2004:4:4::/96
         via ::, eth-0-4, 00:03:09
C        2004:4:4::1/128
         via ::1, eth-0-4, 00:03:09
C        2004:4:100::/96
         via ::, eth-0-9, 00:03:09
C        2004:4:100::2/128
         via ::1, eth-0-9, 00:03:09
C        fe80::/10
         via ::, Null0, 00:03:10
```

3.7.4 配置 OSPFv3 路由重分布示例

i. 介绍

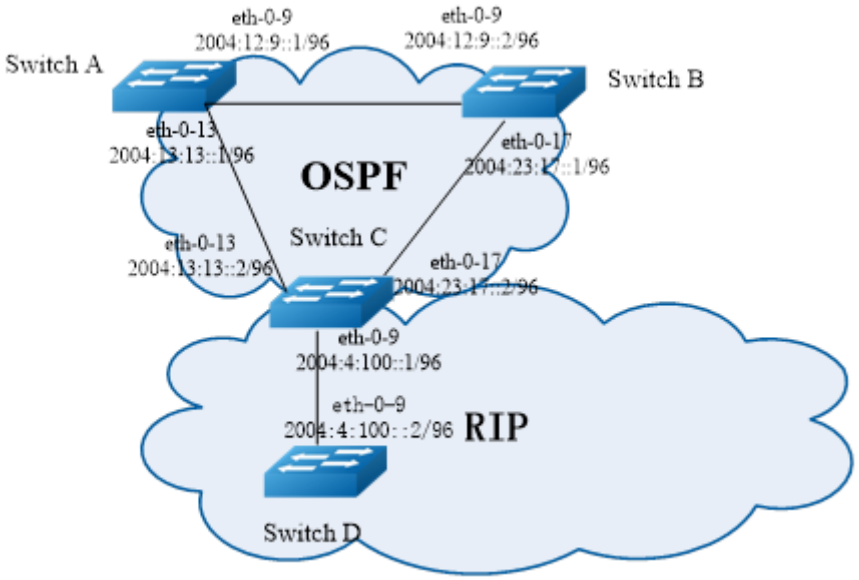
区域内和区域间路由描述的是 AS 内部的网络结构，外部路由则描述了应该如何选择到 AS 以外目的地址的路由。OSPF 将引入的 AS 外部路由分为两类：Type1 和 Type2。

第一类外部路由是指接收的是 IGP（Interior Gateway Protocol，内部网关协议）路由（例如静态路由和 RIPng 路由）。由于这类路由的可信程度较高，并且和 OSPFv3 自身路由的开销具有可比性，所以到第一类外部路由的开销等于本路由器到相应的 ASBR 的开销与 ASBR 到该路由目的地址的开销之和。

第二类外部路由是指接收的是 EGP（Exterior Gateway Protocol，外部网关协议）路由。由于这类路由的可信度比较低，所以 OSPFv3 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。如果计算出开销值相等的两条路由，再考虑本路由器到相应的 ASBR 的开销。本例 RIP 路由将作为外部路由被重分布到 OSPFv3 网络中。

ii. 拓扑

图 3-4 OSPFv3 路由重分布拓扑图



iii. 配置步骤

Switch A:

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch (config)# ipv6 enable	使能 IPv6
Switch(config)# router ipv6 ospf 100	创建 OSPFv3 进程号 100
Switch(config-router)# router-id 1.1.1.1	指定 Router ID
Switch(config-router)# exit	退出 OSPFv3 配置模式
Switch(config)# interface eth-0-9	进入接口配置模式
Switch(config-if)# no switchport	使能三层接口属性
Switch(config-if)# no shutdown	端口 UP
Switch(config-if)# ipv6 address 2004:12:9::1/96	配置 IPv6 地址
Switch(config-if)# ipv6 router ospf 100 area 0 instance 0	将该端口加入到 OSPFv3 process 100、area 0、instance 0 中

命令举例	操作步骤
Switch(config-if)# end	退出接口配置模式
Switch# configure terminal	进入全局配置模式
Switch(config)#interface eth-0-13	进入接口配置模式
Switch(config-if)#no switchport	设置接口为三层接口
Switch(config-if)#no shutdown	端口 UP
Switch(config-if)# ipv6 address 2004:13:13::2/96	设置端口的 IPv6 地址
Switch(config-if)# ipv6 router ospf 100 area 0 instance 0	将该端口加入到 OSPFv3 process 100、area 0、instance 0 中
Switch(config-if)# end	退出至特权模式

Switch B:

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch (config)# ipv6 enable	使能 IPv6
Switch(config)# router ipv6 ospf 200	创建 OSPFv3 进程号 200
Switch(config-router)# router-id 2.2.2.2	指定 Router ID
Switch(config-router)# exit	退出 OSPFv3 配置模式
Switch(config)# interface eth-0-9	进入接口配置模式
Switch(config-if)# no switchport	使能三层接口属性
Switch(config-if)# no shutdown	端口 UP
Switch(config-if)# ipv6 address 2004:12:9::2/96	配置 IPv6 地址
Switch(config-if)# ipv6 router ospf 200 area 0 instance 0	将该端口加入到 OSPFv3 process 200、area 0、instance 0 中
Switch(config-if)# end	退出至特权模式
Switch# configure terminal	进入全局配置模式
Switch(config)#interface eth-0-17	进入接口配置模式

命令举例	操作步骤
Switch(config-if)#no switchport	设置接口为三层接口
Switch(config-if)#no shutdown	端口 UP
Switch(config-if)# ipv6 address 2004:23:17::1/96	设置端口的 IPv6 地址
Switch(config-if)# ipv6 router ospf 200 area 0 instance 0	将该端口加入到 OSPFv3 process 200、area 0、instance 0 中
Switch(config-if)# end	退出至特权模式

Switch C:

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch (config)# ipv6 enable	使能 IPv6
Switch(config)# router ipv6 ospf 300	创建 OSPFv3 进程号 300
Switch(config-router)# router-id 3.3.3.3	指定 Router ID
Switch(config-router)# redistribute ripng	重发布 RIPng 到 OSPF 中
Switch(config-router)# exit	退出 OSPFv3 配置模式
Switch(config)# interface eth-0-13	进入接口配置模式
Switch(config-if)# no switchport	使能三层接口属性
Switch(config-if)# no shutdown	端口 UP
Switch(config-if)# ipv6 address 2004:13:13::2/96	配置 IPv6 地址
Switch(config-if)# ipv6 router ospf 300 area 0 instance 0	将该端口加入到 OSPFv3 process 300、area 0、instance 0 中
Switch(config-if)# end	退出至特权模式
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-17	进入接口配置模式
Switch(config-if)# no switchport	使能三层接口属性
Switch(config-if)# no shutdown	端口 UP

命令举例	操作步骤
Switch(config-if)# ipv6 address 2004:23:17::2/96	配置 IPv6 地址
Switch(config-if)# ipv6 router ospf 300 area 0 instance 0	将该端口加入到 OSPFv3 process 300、area 0、instance 0 中
Switch(config-if)# end	退出至特权模式
Switch# configure terminal	进入全局配置模式
Switch(config)# router ipv6 rip	使能 RIPng
Switch(config)# interface eth-0-9	进入接口配置模式
Switch(config-if)# no switchport	使能三层接口属性
Switch(config-if)# no shutdown	端口 UP
Switch(config-if)# ipv6 address 2004:4:100::1/96	配置 IPv6 地址
Switch(config-if)# ipv6 router rip	将该端口加入到 RIPng 路由域中
Switch(config-if)# end	退出至特权模式

Switch D:

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch (config)# ipv6 enable	使能 IPv6
Switch(config)# router ipv6 rip	使能 RIPng
Switch(config-router)# exit	退出 OSPFv3 配置模式
Switch(config)# interface eth-0-9	进入接口配置模式
Switch(config-if)# no switchport	使能三层接口属性
Switch(config-if)# no shutdown	端口 UP
Switch(config-if)# ipv6 address 2004:4:100::2/96	配置 IPv6 地址
Switch(config-if)# ipv6 router rip	将该端口加入到 RIPng 路由域中
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface eth-0-1	进入接口配置模式

命令举例	操作步骤
Switch(config-if)# no switchport	使能三层接口属性
Switch(config-if)# no shutdown	端口 UP
Switch(config-if)# ipv6 address 2004:4:1::1/96	配置 IPv6 地址
Switch(config-if)# ipv6 router rip	将该端口加入到 RIPng 路由域中
Switch(config-if)# end	退出至特权模式

iv. 命令验证

使用 **show ipv6 ospf database external** 与 **show ipv6 route** 命令，验证上述配置。

- 检查Switch A的配置结果：

```
Switch# show ipv6 route

IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, I - IS-IS, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       Dr - DHCPV6 Relay
       [*] - [AD/Metric]
Timers: Uptime
O E2     2004:4:1::/96 [110/20]
       via fe80::c629:f2ff:fe02:3600, eth-0-13, 00:00:03
C          2004:12:9::/96
       via ::, eth-0-9, 00:34:20
C          2004:12:9::1/128
       via ::1, eth-0-9, 00:34:20
C          2004:13:13::/96
       via ::, eth-0-13, 00:34:19
C          2004:13:13::2/128
       via ::1, eth-0-13, 00:34:19
O          2004:23:17::/96 [110/2]
       via fe80::bc22:aeff:fe64:aa00, eth-0-9, 00:26:34
       via fe80::c629:f2ff:fe02:3600, eth-0-13, 00:26:34
C          fe80::/10
       via ::, Null0, 00:34:21

Switch# show ipv6 ospf database external

            OSPFv3 Router with ID (1.1.1.1) (Process 100)
                AS-external-LSA
  LS age: 140
```

```
   LS Type: AS-External-LSA
   Link State ID: 0.0.0.1
   Advertising Router: 3.3.3.3
   LS Seq Number: 0x80000001
   Checksum: 0x66F7
   Length: 44
      Metric Type: 2 (Larger than any link state path)
      Metric: 20
      Prefix: 2004:4:1::/96
      Prefix Options: 0 (-|-|-|-)
      External Route Tag: 0
```

- 检查Switch B的配置结果：

```
Switch# show ipv6 route

IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, I - IS-IS, B - BGP
          O - OSPF, IA - OSPF inter area
          N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
          E1 - OSPF external type 1, E2 - OSPF external type 2
          Dr - DHCPV6 Relay
          [*] - [AD/Metric]
Timers: Uptime
O E2      2004:4:1::/96 [110/20]
          via fe80::c629:f2ff:fe02:3600, eth-0-17, 00:02:43
C           2004:12:9::/96
          via ::, eth-0-9, 00:33:31
C           2004:12:9::2/128
          via ::1, eth-0-9, 00:33:31
O           2004:13:13::/96 [110/2]
          via fe80::b242:55ff:fe05:ff00, eth-0-9, 00:28:59
          via fe80::c629:f2ff:fe02:3600, eth-0-17, 00:28:59
C           2004:23:17::/96
          via ::, eth-0-17, 00:33:31
C           2004:23:17::1/128
          via ::1, eth-0-17, 00:33:31
C           fe80::/10
          via ::, Null0, 00:33:33

Switch# show ipv6 ospf database external

show ipv6 ospf database external
                OSPFv3 Router with ID (2.2.2.2) (Process 200)
                    AS-external-LSA
   LS age: 195
   LS Type: AS-External-LSA
   Link State ID: 0.0.0.1
```

```
   Advertising Router: 3.3.3.3
   LS Seq Number: 0x80000001
   Checksum: 0x66F7
   Length: 44
      Metric Type: 2 (Larger than any link state path)
      Metric: 20
      Prefix: 2004:4:1::/96
      Prefix Options: 0 (-|-|-|-)
      External Route Tag: 0
```

- 检查Switch C的配置结果：

```
Switch# show ipv6 route

IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, I - IS-IS, B - BGP
          O - OSPF, IA - OSPF inter area
          N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
          E1 - OSPF external type 1, E2 - OSPF external type 2
          Dr - DHCPV6 Relay
          [*] - [AD/Metric]
Timers: Uptime
R           2004:4:1::/96 [120/2]
          via fe80::ee66:91ff:fe45:db00, eth-0-9, 00:03:43
C           2004:4:100::/96
          via ::, eth-0-9, 00:07:01
C           2004:4:100::1/128
          via ::1, eth-0-9, 00:07:01
O           2004:12:9::/96 [110/2]
          via fe80::b242:55ff:fe05:ff00, eth-0-13, 00:29:57
          via fe80::bc22:aeff:fe64:aa00, eth-0-17, 00:29:57
O           2004:13:13::/96 [110/1]
          via fe80::b242:55ff:fe05:ff00, eth-0-13, 00:30:12
C           2004:23:17::/96
          via ::, eth-0-17, 00:30:26
C           2004:23:17::2/128
          via ::1, eth-0-17, 00:30:26
C           fe80::/10
          via ::, Null0, 00:30:28

Switch# show ipv6 ospf database external

show ipv6 ospf database external
                OSPFv3 Router with ID (3.3.3.3) (Process 300)
                    AS-external-LSA
   LS age: 250
   LS Type: AS-External-LSA
   Link State ID: 0.0.0.1
```

```
   Advertising Router: 3.3.3.3
   LS Seq Number: 0x80000001
   Checksum: 0x66F7
   Length: 44
      Metric Type: 2 (Larger than any link state path)
      Metric: 20
      Prefix: 2004:4:1::/96
      Prefix Options: 0 (-|-|-|-)
      External Route Tag: 0
```

- 检查Switch D的配置结果：

```
Switch# show ipv6 route

IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, I - IS-IS, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       Dr - DHCPV6 Relay
       [*] - [AD/Metric]
Timers: Uptime
C          2004:4:1::/96
       via ::, eth-0-1, 00:04:48
C          2004:4:1::1/128
       via ::1, eth-0-1, 00:04:48
C          2004:4:100::/96
       via ::, eth-0-9, 00:06:59
C          2004:4:100::2/128
       via ::1, eth-0-9, 00:06:59
C          fe80::/10
       via ::, Null0, 00:07:00
```

3.7.5 配置 OSPFv3 接口的开销值

i. 介绍

用户可以通过修改接口的 COST 值来使路由成为最优路由。在下面的例子中，通过修改 COST 值可以使 Switch B 成为 Switch A 的下一跳。

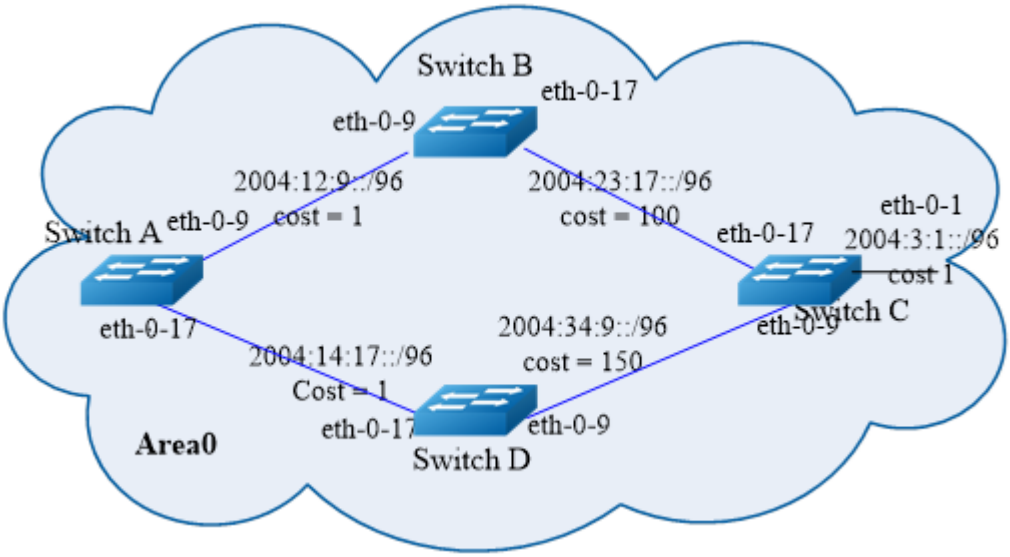
默认接口的 COST 值是 1 (1000M speed)。Switch B 的 eth-0-17 优先级 100，Switch D 的 eth-0-9 优先级 150，那么到达 Switch C 的网络 2004:3:1::/96 的 COST 值将发生变化：

Switch A -Switch B - Switch C: 1+1+100 = 102

Switch A -Switch D - Switch C: 1+1+150 = 152

ii. 拓扑

图 3-5 配置 OSPFv3 接口的开销值



iii. 配置步骤

Switch A:

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch (config)# ipv6 enable	使能 IPv6
Switch(config)# router ipv6 ospf 100	创建 OSPFv3 进程号 100
Switch(config-router)# router-id 1.1.1.1	指定 Router ID
Switch(config-router)# exit	退出 OSPFv3 配置模式
Switch(config)# interface eth-0-9	进入接口配置模式
Switch(config-if)# no switchport	使能三层接口属性

命令举例	操作步骤
Switch(config-if)# no shutdown	端口 UP
Switch(config-if)# ipv6 address 2004:12:9::1/96	配置 IPv6 地址
Switch(config-if)# ipv6 router ospf 100 area 0 instance 0	将该端口加入到 OSPFv3 process 100、area 0、instance 0 中
Switch(config-if)# end	退出至特权模式
Switch# configure terminal	进入全局配置模式
Switch(config)#interface eth-0-17	进入接口配置模式
Switch(config-if)#no switchport	设置接口为三层接口
Switch(config-if)#no shutdown	端口 UP
Switch(config-if)# ipv6 address 2004:14:17::1/96	设置端口的 IPv6 地址
Switch(config-if)# ipv6 router ospf 100 area 0 instance 0	将该端口加入到 OSPFv3 process 100、area 0、instance 0 中
Switch(config-if)# end	退出至特权模式

Switch B:

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch (config)# ipv6 enable	使能 IPv6
Switch(config)# router ipv6 ospf 200	创建 OSPFv3 进程号 200
Switch(config-router)# router-id 2.2.2.2	指定 Router ID
Switch(config-router)# exit	退出 OSPFv3 配置模式
Switch(config)# interface eth-0-9	进入接口配置模式
Switch(config-if)# no switchport	使能三层接口属性
Switch(config-if)# no shutdown	端口 UP
Switch(config-if)# ipv6 address 2004:12:9::2/96	配置 IPv6 地址
Switch(config-if)# ipv6 router ospf 200 area 0 instance 0	将该端口加入到 OSPFv3 process 200、area 0、instance 0 中

命令举例	操作步骤
Switch(config-if)# end	退出至特权模式
Switch# configure terminal	进入全局配置模式
Switch(config)#interface eth-0-17	进入接口配置模式
Switch(config-if)#no switchport	设置接口为三层接口
Switch(config-if)#no shutdown	端口 UP
Switch(config-if)# ipv6 address 2004:23:17::1/96	设置端口的 IPv6 地址
Switch(config-if)# ipv6 router ospf 200 area 0 instance 0	将该端口加入到 OSPFv3 process 200、area 0、instance 0 中
Switch(config-if)# ipv6 ospf cost 100	配置 OSPFv3 接口的开销值
Switch(config-if)# end	退出至特权模式

Switch C:

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch (config)# ipv6 enable	使能 IPv6
Switch(config)# router ipv6 ospf 300	创建 OSPFv3 进程号 300
Switch(config-router)# router-id 3.3.3.3	指定 Router ID
Switch(config-router)# exit	退出 OSPFv3 配置模式
Switch(config)# interface eth-0-17	进入接口配置模式
Switch(config-if)# no switchport	使能三层接口属性
Switch(config-if)# no shutdown	端口 UP
Switch(config-if)# ipv6 address 2004:23:17::2/96	配置 IPv6 地址
Switch(config-if)# ipv6 router ospf 300 area 0 instance 0	将该端口加入到 OSPFv3 process 300、area 0、instance 0 中
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface eth-0-9	进入接口配置模式

命令举例	操作步骤
Switch(config-if)# no switchport	使能三层接口属性
Switch(config-if)# no shutdown	端口 UP
Switch(config-if)# ipv6 address 2004:34:9::1/96	配置 IPv6 地址
Switch(config-if)# ipv6 router ospf 300 area 0 instance 0	将该端口加入到 OSPFv3 process 300、area 0、instance 0 中
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# no switchport	使能三层接口属性
Switch(config-if)# no shutdown	端口 UP
Switch(config-if)# ipv6 address 2004:3:1::1/96	配置 IPv6 地址
Switch(config-if)# ipv6 router ospf 300 area 0 instance 0	将该端口加入到 OSPFv3 process 300、area 0、instance 0 中
Switch(config-if)# end	退出至特权模式

Switch D:

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch (config)# ipv6 enable	使能 IPv6
Switch(config)# router ipv6 ospf 400	创建 OSPFv3 进程号 400
Switch(config-router)# router-id 4.4.4.4	指定 Router ID
Switch(config-router)# exit	退出 OSPFv3 配置模式
Switch(config)# interface eth-0-9	进入接口配置模式
Switch(config-if)# no switchport	使能三层接口属性
Switch(config-if)# no shutdown	端口 UP
Switch(config-if)# ipv6 address 2004:34:9::2/96	配置 IPv6 地址
Switch(config-if)# ipv6 router ospf 400 area 0 instance 0	将该端口加入到 OSPFv3 process 300、area 0、instance 0 中

命令举例	操作步骤
Switch(config-if)# ipv6 ospf cost 150	配置 OSPFv3 接口的开销值
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface eth-0-17	进入接口配置模式
Switch(config-if)# no switchport	使能三层接口属性
Switch(config-if)# no shutdown	端口 UP
Switch(config-if)# ipv6 address 2004:14:17::2/96	配置 IPv6 地址
Switch(config-if)# ipv6 router ospf 400 area 0 instance 0	将该端口加入到 OSPFv3 process 300、area 0、instance 0 中
Switch(config-if)# end	退出至特权模式

iv. 命令验证

使用命令**show ipv6 ospf route** 验证以上配置。

- 检查Switch A的配置结果：

```
Switch# show ipv6 ospf route

IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, I - IS-IS, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       Dr - DHCPV6 Relay
       [*] - [AD/Metric]
Timers: Uptime
O        2004:3:1::/96 [110/102]
       via fe80::bc22:aeff:fe64:aa00, eth-0-9, 00:08:06
C        2004:12:9::/96
       via ::, eth-0-9, 01:15:43
C        2004:12:9::1/128
       via ::1, eth-0-9, 01:15:43
C        2004:14:17::/96
       via ::, eth-0-17, 00:18:38
C        2004:14:17::1/128
       via ::1, eth-0-17, 00:18:38
O        2004:23:17::/96 [110/101]
       via fe80::bc22:aeff:fe64:aa00, eth-0-9, 00:08:06
O        2004:34:9::/96 [110/102]
       via fe80::bc22:aeff:fe64:aa00, eth-0-9, 00:03:56
```

```
C           fe80::/10
            via ::, Null0, 01:15:44
```

- 检查Switch B的配置结果：

```
Switch# show ipv6 ospf route

IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, I - IS-IS, B - BGP
           O - OSPF, IA - OSPF inter area
           N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
           E1 - OSPF external type 1, E2 - OSPF external type 2
           Dr - DHCPV6 Relay
           [*] - [AD/Metric]
Timers: Uptime
O           2004:3:1::/96 [110/101]
            via fe80::c629:f2ff:fe02:3600, eth-0-17, 00:08:33
C           2004:12:9::/96
            via ::, eth-0-9, 01:12:40
C           2004:12:9::2/128
            via ::1, eth-0-9, 01:12:40
O           2004:14:17::/96 [110/2]
            via fe80::b242:55ff:fe05:ff00, eth-0-9, 00:18:43
C           2004:23:17::/96
            via ::, eth-0-17, 01:12:40
C           2004:23:17::1/128
            via ::1, eth-0-17, 01:12:40
O           2004:34:9::/96 [110/101]
            via fe80::c629:f2ff:fe02:3600, eth-0-17, 00:04:23
C           fe80::/10
            via ::, Null0, 01:12:42
```

- 检查Switch C的配置结果：

```
Switch# show ipv6 ospf route

IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, I - IS-IS, B - BGP
           O - OSPF, IA - OSPF inter area
           N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
           E1 - OSPF external type 1, E2 - OSPF external type 2
           Dr - DHCPV6 Relay
           [*] - [AD/Metric]
Timers: Uptime
C           2004:3:1::/96
            via ::, eth-0-1, 00:13:54
```

```
C          2004:3:1::1/128
           via ::1, eth-0-1, 00:13:54
O          2004:12:9::/96 [110/2]
           via fe80::bc22:aeff:fe64:aa00, eth-0-17, 00:19:47
O          2004:14:17::/96 [110/2]
           via fe80::ee66:91ff:fe45:db00, eth-0-9, 00:02:27
C          2004:23:17::/96
           via ::, eth-0-17, 01:09:02
C          2004:23:17::2/128
           via ::1, eth-0-17, 01:09:02
C          2004:34:9::/96
           via ::, eth-0-9, 00:04:52
C          2004:34:9::1/128
           via ::1, eth-0-9, 00:04:52
C          fe80::/10
           via ::, Null0, 01:09:04
```

- 检查Switch D的配置结果：

```
Switch# show ipv6 route

IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, I - IS-IS, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       Dr - DHCPV6 Relay
       [*] - [AD/Metric]
Timers: Uptime
O          2004:3:1::/96 [110/103]
           via fe80::b242:55ff:fe05:ff00, eth-0-17, 00:02:35
O          2004:12:9::/96 [110/2]
           via fe80::b242:55ff:fe05:ff00, eth-0-17, 00:02:35
C          2004:14:17::/96
           via ::, eth-0-17, 00:04:09
C          2004:14:17::2/128
           via ::1, eth-0-17, 00:04:09
O          2004:23:17::/96 [110/102]
           via fe80::b242:55ff:fe05:ff00, eth-0-17, 00:02:35
C          2004:34:9::/96
           via ::, eth-0-9, 00:06:06
C          2004:34:9::2/128
           via ::1, eth-0-9, 00:06:06
C          fe80::/10
           via ::, Null0, 00:44:59
```

4 IPv6 地址前缀列表配置

4.1 地址前缀列表简介

地址前缀列表是路由策略的一种，作用比较灵活。一个地址前缀列表由前缀列表名标识。每个前缀列表可以包含多个表项，每个表项可以独立指定一个网络前缀形式的匹配范围，并用一个索引号来标识，索引号指明了进行匹配检查的顺序。在匹配的过程中，交换机按升序依次检查由索引号标识的各个表项。只要有某一表项满足条件，就意味着本次匹配过程结束，而不再进行下一个表项的匹配。

4.2 配置 IPv6 地址前缀列表

4.2.1 创建地址前缀列表

地址前缀列表用于 IPv6 地址过滤。同一个地址前缀列表可包含多个表项，一个表项包括地址和掩码位数。命令中的 **deny** 和 **permit** 关键字指定该匹配结果是拒绝或者允许。此时，多个表项之间是“或”的关系，即通过一个表项就可通过该地址前缀列表的过滤。没有通过任何一个表项的过滤就意味着没有通过该地址前缀列表的过滤。

地址前缀范围包括两个部分，分别由 mask-length 和[greater-equal-value,less-equal-value]决定。如果指定了这两部分，要被过滤的 IPv6 地址必须匹配这两部分规定的前缀范围。具体的匹配公式如下：

ipv6-address/mask-length < ge ge-length < le le-length <= 128

例如，只指定 ge-length，则匹配范围为[ge-length,128]；只指定 le-length，则匹配范围为[ipv6-address/mask-length,le-length]；如果两者都指定，则匹配范围为[ge-length, le-length]。

如果在输入命令中没有指定序号，则交换机会自动为表项添加默认序号。默认序号从 5 开始，并且每次递增 5，例如，5、10、15。默认序号将从当前大于已分配的序号中选择，并且是其中的最小值。

表 4-1 创建地址前缀列表

命令	操作	说明
configure terminal	进入全局配置模式	-
ipv6 prefix-list *prefix-list-name* [**seq** *sequence-number*] { **deny** | **permit** } { **any** | *ipv6-address/mask-length* } [**ge** *ge-length* | **le** *le-length*]	创建地址前缀列表	prefix-list-name: 地址前缀列表名称； sequence-number: 地址前缀列表表项序号，取值范围 1~65535； ipv6-address/mask-length: 网络地址和掩码位数。掩码位数的取值范围为 0~128 ge-length: 指定地址匹配的最小前缀长度 le-length: 指定地址匹配的最大前缀长度 缺省情况下，未创建地址前缀列表

4.2.2 添加地址前缀列表描述

如果该地址前缀列表不存在，交换机将会自动创建。

表 4-2 添加地址前缀列表描述

命令	操作	说明
configure terminal	进入全局配置模式	-
ipv6 prefix-list *prefix-list-name* **description** *description-info*	添加地址前缀列表描述信息	prefix-list-name: 地址前缀列表名称； description-info: 地址前缀列表描述，取值范围为 0～80； 缺省情况下，未添加地址前缀列表描述信息

4.2.3 启用地址前缀列表序号

表4-3 启用地址前缀列表序号

命令	操作	说明
configure terminal	进入全局配置模式	-
ipv6 prefix-list sequence-number	配置地址前缀列表显示序号	缺省情况下，地址前缀列表默认使用序号

4.3 显示与维护

4.3.1 查看地址前缀列表信息

表4-4 查看地址前缀列表信息

命令	操作	说明
show ipv6 prefix-list [**summary** | **detail**] [*prefix-list-name*]	显示地址前缀列表的配置信息	如选择了关键字 summary 或 detail，可以显示前缀列表的统计摘要或详细统计信息
show ipv6 prefix-list *prefix-list-name* [**seq** *sequence-number* | *ipv6-address/mask-length* [**longer** | **first-match**]]		prefix-list-name: 地址前缀列表名称； sequence-number: 地址前缀列表表项序号，取值范围 1~65535； ip-address/mask-length: 网络地址/掩码位数 e.g., 2001:db8::/32 longer: 只显示掩码位数大于 mask-length 的表项； first-match: 只显示第一个匹配的表项

4.3.2 清除地址前缀列表信息

表4-5 清除地址前缀列表信息

命令	操作	说明
clear ipv6 prefix-list [*prefix-list-name*] [*ipv6-address/mask-length*]	清除地址前缀列表的配置信息	prefix-list-name: 地址前缀列表名称； ipv6-address/mask-length: 网络地址/掩码位数 e.g., 2001:db8::/32

4.4 配置举例

4.4.1 配置 IPv6 Prefix-List 基本功能

i. 配置步骤

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# ipv6 prefix-list test seq 1 deny 2001:db8::1/32 le 48	创建地址前缀列表 test，并创建一条表项，指定序号为 1
Switch(config)# ipv6 prefix-list test permit any	创建一个表项：防止不匹配条目出现时遭到拒绝
Switch(config)# ipv6 prefix-list test description this ipv6 prefix list is for test	添加地址前缀列表描述
Switch(config)# ipv6 prefix-list test permit 2001:abc::1/32 le 48	创建一条表项，使用默认序号
Switch(config)# exit	退出全局配置模式

ii. 命令验证

显示IPv6地址前缀列表的详细信息：

```
    Switch# show ipv6 prefix-list detail

Prefix-list list number: 1
Prefix-list entry number: 3
Prefix-list with the last deletion/insertion: test
ipv6 prefix-list test:
    Description: this ipv6 prefix list is for test
    count: 3, range entries: 0, sequences: 1 - 10
       seq 1 deny 2001:db8::1/32 le 48 (hit count: 0, refcount: 0)
       seq 5 permit any (hit count: 0, refcount: 0)
       seq 10 permit 2001:abc::1/32 le 48 (hit count: 0, refcount: 0)
```

4.4.2 配置 IPv6 Prefix-list 与 RIPng 的简单应用

i. 配置步骤

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# ipv6 prefix-list aa seq 11 deny 2001:db8::1/32 le 48	创建地址前缀列表 aa，并创建一条表项

命令举例	操作步骤
Switch(config)# ipv6 prefix-list aa permit any	创建一个表项：防止不匹配条目出现时遭到拒绝
Switch(config)# router ipv6 rip	进入 RIPng 路由配置模式
Switch(config-router)# distribute-list prefix aa out	应用策略
Switch(config-router)# end	退出至特权模式

ii. 命令验证

显示IPv6地址前缀列表的配置信息：

```
    Switch# show ipv6 prefix-list

ipv6 prefix-list aa: 2 entries
       seq 11 deny 1:db8::1/32 le 48
       seq 15 permit any

    Switch# show running-config

Building configuration...
    …
ipv6 prefix-list aa seq 11 deny 1:db8::1/32 le 48
ipv6 prefix-list aa seq 15 permit any
    …
router ipv6 rip
distribute-list prefix aa out
```

5 Route-map 配置

5.1 Route-map 简介

路由策略（Routing Policy）是为了改变网络流量所经过的途径而修改路由信息的技术，主要通过改变路由属性（包括可达性）来实现。

路由器在发布与接收路由信息时，可能需要实施一些策略，以便对路由信息进行过滤，例如只接收或发布满足一定条件的路由信息。一种路由协议可能需要引入其它的路由协议发现的路由信息，路由器在引入其它路由协议的路由信息时，可能只需要引入一部分满足条件的路由信息，并控制所引入的路由信息的某些属性，以使其满足本协议的要求。

为实现路由策略，首先要定义将要实施路由策略的路由信息的特征，即定义一组匹配规则，又称为 match 语句。如果匹配条件，就会执行 set 指定的相关动作。这个动作不是必要的，可以使用路由信息中的不同属性作为匹配依据进行设置，如目的地址、发布路由信息的路由器地址等。匹配规则可以预先设置好，然后再将它们应用于路由的发布、接收和引入等过程的路由策略中。

5.2 配置 Route-map

5.2.1 创建 Route-map

表5-1 创建Route-map

命令	操作	说明
configure terminal	进入全局配置模式	-
route-map *map-tag* [**permit** | **deny**] [*sequence-number*]	如何创建一个 Route-map 并进入 Route-map 配置模式	map-tag: route-map 名称，长度不得超过 20 个字符，并且它的首字母必须是'a'-'z', 'A'-'Z'或者'0'-'9'； sequence-number: route-map 的序列号，取值范围为 1~65535

5.2.2 配置 match 语句

如果指定了一个 permit 的 match 规则，路由将会被像 set 规则指定的那样进行重发布或者进行控制。相反，如果制定了相应的 deny 规则，满足条件的路由将不会被重发布或者控制。如果没有匹配到任何规则的话，路由将不会被接收或者转发。

被策略指定的路由不能和路由协议指定的路由相同，指定的策略让报文能够按照他们的长度及内容通过不同的路由进行转发。相对于路由表指定的路径来说，报文将会优先以配置的策略来进行转发。

1. 通过ACL或者IPv6地址前缀列表匹配路由

表5-2 功能配置与参数说明

命令	操作	说明
configure terminal	进入全局配置模式	-
route-map *map-tag* [**permit** | **deny**] [*sequence-number*]	如何创建一个 route-map 并进入 route-map 配置模式	map-tag: route-map 名称，长度不得超过 20 个字符，并且它的首字母必须是'a'-'z', 'A'-'Z'或者'0'-'9'； sequence-number: route-map 的序列号，取值范围为 1~65535
match ipv6 address *ipv6-acl-name*	指定匹配一个 IPv6 ACL 的规则	ipv6-acl-name: 指定 IPV6 ACL 名；缺省情况下，未配置该规则
match ipv6 next-hop *ipv6-acl-name*	指定匹配一个下一跳的 IPv6 地址	
match ipv6 address prefix-list *list-name*	匹配一个 IPv6 前缀列表条目	list-name: IPv6 前缀列表名；缺省情况下，未配置该规则
match ipv6 next-hop prefix-list *list-name*	匹配下一跳的 IPv6 前缀列表条目	

2. 配置通过度量值匹配路由

表5-3 功能配置与参数说明

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

命令	操作	说明
route-map *map-tag* [**permit** | **deny**] [*sequence-number*]	如何创建一个 route-map 并进入 route-map 配置模式	map-tag: route-map 名称，长度不得超过 20 个字符，并且它的首字母必须是'a'-'z', 'A'-'Z'或者'0'-'9'； sequence-number: route-map 的序列号，取值范围为 1~65535
match metric *metric-value*	指定度量值匹配路由	metric-value: 度量值，取值范围为 0~4294967295；缺省情况下，未配置该规则

3. 配置BGP协议中生效的匹配条件

表5-4 功能配置与参数说明

命令	操作	说明
configure terminal	进入全局配置模式	-
route-map *map-tag* [**permit** | **deny**] [*sequence-number*]	如何创建一个 route-map 并进入 route-map 配置模式	map-tag: route-map 名称，长度不得超过 20 个字符，并且它的首字母必须是'a'-'z', 'A'-'Z'或者'0'-'9'； sequence-number: route-map 的序列号，取值范围为 1~65535
match as-path *list-name*	指定自治系统匹配的路径	list-name: 指定自治系统路径的 ACL 名；缺省情况下，未配置该规则
match community *community-list-name*	指定匹配的团体属性(Community)号	community-list-name: Community 列表名；缺省情况下，未配置该规则
match interface *if-name*	指定接口的匹配规则	if-name: 接口名；缺省情况下，未配置该规则
match local-preference *preference-level*	指定本地优先级的匹配规则	preference-level: 本地优先级，取值范围为 0~4294967295；缺省情况下，未配置该规则
match origin { **egp** | **igp** | **incomplete** }	匹配 BGP 路由的起始(origin)属性	egp：表明这一条路由的起始信息是从外部网关协议(EGP)中学习到的； igp:表示起始路径信息是通过内部网关协议(IGP)学习到的。 incomplete: 这个路由的原始路径是通过不清楚或者其他别的方式来学

命令	操作	说明
		习到的。比如，一个静态路由被重发布到 BGP 时，那它的原始路由就是不完整的； 缺省情况下，未配置该规则

4. 配置基于路由信息的匹配条件

表5-5 功能配置与参数说明

命令	操作	说明
configure terminal	进入全局配置模式	-
route-map *map-tag* [**permit** | **deny**] [*sequence-number*]	如何创建一个 route-map 并进入 route-map 配置模式	map-tag: route-map 名称，长度不得超过 20 个字符，并且它的首字母必须是'a'-'z', 'A'-'Z'或者'0'-'9'； sequence-number: route-map 的序列号，取值范围为 1~65535
match route-type external { **type-1** | **type-2** }	根据路由信息匹配指定的外部路由类型	自治系统外部 LSA 即类型 1 或者类型 2。外部类型 1 值匹配类型 1 的外部路由，外部类型 2 只匹配类型 2 的外部路由；缺省情况下，未配置该规则
match tag *tag-value*	根据路由信息匹配指定的 tag	tag-value: 取值范围为 0~4294967295；缺省情况下，未配置该规则

5.2.3 配置 set 动作

1. 配置BGP路由属性

表5-6 功能配置与参数说明

命令	操作	说明
configure terminal	进入全局配置模式	-
route-map *map-tag* [**permit** | **deny**] [*sequence-number*]	如何创建一个 route-map 并进入 route-map 配置模	map-tag: route-map 名称，长度不得超过 20 个字符，并且它的首字母必须是

命令	操作	说明
	式	'a'-'z', 'A'-'Z'或者'0'-'9'； sequence-number: route-map 的序列号，取值范围为 1~65535
set ipv6 aggregator as *as-number ipv6-address*	配置 route-map 和 router ID 的 AS 号	自治系统(AS)是一个网络管理机构控制下的路由器和网络群组。它们被不同的区域所分离，被指派了一个独特的 16 位的号码； as-number: 指定集合的 AS 号；缺省情况下，未配置该规则 ipv6-address: 指定集合的 IPv6 地址
set as-path prepend *as-number* [*as-number*]	修改自治系统(AS)的路径	通过指定 AS-Path 的长度，路由器可以影响路径的最佳路径选择。在这个命令中使用 prepend 参数，来在已有的 AS-Path 中，再追加一个指定的 AS-Path。缺省情况下，未配置该规则
set comm-list { *std-list-num* | *ext-list-num* | *list-name* } **delete**	删除匹配条件的团体属性	std-list-num: 标准 community 列表号； ext-list-num: 扩展 community 列表号； list-name: community 列表名； 缺省情况下，未配置该规则
set community [*aa:nn* | **internet** | **local-AS** | **no-advertise** | **no-export**]	配置团体属性	aa: AS 号； nn: 指定的 community 号； 缺省情况下，未配置该规则
set extcommunity { **rt** | **soo** } *ext-comm-number* [*ext-comm-number*]	配置扩展团体属性	ext-comm-number: 数字或 IP 地址形式的 AS 号；缺省情况下，未配置该规则
set local-preference *preference-level*	配置本地优先级属性	preference-level: 本地优先级，取值范围为 0~4294967295；缺省情况下，未配置该规则
set origin { **egp** | **igp** | **incomplete** }	配置 BGP 路由的 Origin 属性	缺省情况下，未配置该规则

2. 配置路由的度量值属性

表5-7 功能配置与参数说明

命令	操作	说明
configure terminal	进入全局配置模式	-
route-map *map-tag* [**permit** | **deny**] [*sequence-number*]	如何创建一个 route-map 并进入 route-map 配置模式	map-tag: route-map 名称，长度不得超过 20 个字符，并且它的首字母必须是'a'-'z', 'A'-'Z'或者'0'-'9'； sequence-number: route-map 的序列号，取值范围为 1~65535
set metric *metric-value*	配置一条路由的 metric 值，以及一个关于 AS 的首选路径影响的外部邻居	metric-value: 度量值，取值范围为 0~4294967295；缺省情况下，未配置该规则

3. 配置路由信息的下一跳地址

表5-8 功能配置与参数说明

命令	操作	说明
configure terminal	进入全局配置模式	-
route-map *map-tag* [**permit** | **deny**] [*sequence-number*]	如何创建一个 route-map 并进入 route-map 配置模式	map-tag: route-map 名称，长度不得超过 20 个字符，并且它的首字母必须是'a'-'z', 'A'-'Z'或者'0'-'9'； sequence-number: route-map 的序列号，取值范围为 1~65535
set ipv6 next-hop [**local**] *ipv6-address*	配置指定的 IPv6 下一跳地址	ipv6-address: 下一跳的 IPv6 地址；缺省情况下，未配置该规则

4. 配置目的路由协议的metric类型

表5-9 功能配置与参数说明

命令	操作	说明
configure terminal	进入全局配置模式	-
route-map *map-tag* [**permit** | **deny**] [*sequence-number*]	如何创建一个 route-map 并进入 route-map 配置模式	map-tag: route-map 名称，长度不得超过 20 个字符，并且它的首字母必须是'a'-'z', 'A'-'Z'或者'0'-'9'； sequence-number: route-map 的序列号，取值范围为 1~65535

命令	操作	说明
set metric-type { **type1** | **type2** }	配置目的路由协议的 metric 类型	缺省情况下，未配置该规则

5. 配置路由信息的tag值

表5-10 功能配置与参数说明

命令	操作	说明
configure terminal	进入全局配置模式	-
route-map *map-tag* [**permit** | **deny**] [*sequence-number*]	如何创建一个 route-map 并进入 route-map 配置模式	map-tag: route-map 名称，长度不得超过 20 个字符，并且它的首字母必须是'a'-'z', 'A'-'Z'或者'0'-'9'； sequence-number: route-map 的序列号，取值范围为 1~65535
set tag *tag-value*	配置路由信息的 tag 值	tag-value: 取值范围为 0~4294967295；缺省情况下，未配置该规则

5.3 显示与维护

表5-11 显示与维护

命令	操作	说明
show route-map [*map-tag*]	显示 Route-map 配置信息	map-tag: route-map 名称，长度不得超过 20 个字符，并且它的首字母必须是'a'-'z', 'A'-'Z'或者'0'-'9'

5.4 配置 Route-map 简单应用

5.4.1 配置步骤

配置将 IPv6 前缀列表应用至 Route Map 中：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式

命令举例	操作步骤
Switch(config)# ipv6 prefix-list ripng_pre_1 seq 11 permit fe80::a8f0:d8ff:fe7d:c501/128	创建地址前缀列表 ripng_pre_1，并创建一条表项
Switch(config)# ipv6 prefix-list ripng_pre_1 permit any	创建一个表项：防止不匹配条目出现时遭到拒绝
Switch(config)# route-map ripng_rmap permit	创建 Route Map
Switch(config-route-map)# match ipv6 address prefix-list ripng_pre_1	匹配 IPv6 地址前缀列表 ripng_rmap
Switch(config-route-map)# set local-preference 200	配置本地优先级
Switch(config-route-map)# exit	退出路由配置模式
Switch(config)# router ipv6 rip	进入 RIPng 路由模式
Switch(config-router)# redistribute static route-map ripng_rmap	配置重发布静态路由
Switch(config-router)# end	退出 RIPng 路由模式

5.4.2 命令验证

- 显示Route-map配置信息：

```
    Switch # show route-map

route-map ripng_rmap, permit, sequence 10
  Match clauses:
    ipv6 next-hop prefix-list ripng_pre_1
  Set clauses:
    ipv6 next-hop local fe80::1
```

- 显示设备当前的配置信息：

```
    Switch # show running-config

Building configuration...
    …
ipv6 prefix-list ripng_pre_1 seq 11 permit fe80::a8f0:d8ff:fe7d:c501/128
ipv6 prefix-list ripng_pre_1 seq 15 permit any
!
!
route-map ripng_rmap permit 10
 match ipv6 next-hop prefix-list ripng_pre_1
 set ipv6 next-hop local fe80::1
```

```
!
 router ipv6 rip
  redistribute static route-map ripng_rmap
 !
 ipv6 route 2001:dbc::/64 fe80::a8f0:d8ff:fe7d:c501 eth-0-9
 !
```

- 显示RIPng域的信息：

```
Switch# show ipv6 rip database
S    2001:dbc::/64                fe80::1                      eth-0-9    1      0
```

6 IPv6 IS-IS 配置

6.1 IPv6 IS-IS 简介

IS-IS（Intermediate system to intermediate system，中间系统到中间系统）是一种内部网关协议（Interior Gateway Protocol），也是一种链路状态路由协议，使用SPF（Shortest Path First，最短路径优先）算法计算路由。标准的IS-IS是由ISO（国际标准化组织）制定，专为CLNP（无连接网络服务）设计，并不适用于IP网络。由于IP网络的广泛应用，IETF组织在RFC1195中定义了使用IP网络的IS-IS协议，能同时应用于TCP/IP与开放式系统互联（Open System Interconnection，OSI）中，称作集成IS-IS。

IS-IS支持多种网络层的协议，包括IPv6协议。IPv6 IS-IS动态路由协议是在IPv4 IS-IS基础上的延伸，能够发布IPv6路由信息，实现IPv6网络的互连。IPv4 IS-IS相关的配置请详见“IP路由配置指导”章节。

6.2 配置 IPv6 IS-IS 的基本功能

6.2.1 创建 IS-IS 进程

用户可以在一台路由器上创建多个 ISIS 进程，如果没有指定进程编号，则创建默认的 0 号进程。

表6-1 创建IS-IS进程

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# router isis test	创建 ISIS 进程并进入 ISIS 配置模式	test: ISIS 路由区域标签

6.2.2 配置网络实体名(NET)

区域地址用来唯一标识路由域中的不同区域，同一 Level-1 区域内所有无线接入控制器必须有相同的区域地址，Level-2 区域内的无线接入控制器可以有不同的区域地址。由于一个 IS-IS 进程中最多可配置 3 个区域地址，所以最多也只能配 3 个 NET。配置多个 NET 时，它们的系统 ID 必须保持一致。

表6-2 配置NET

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# router isis test	创建 ISIS 进程并进入 ISIS 配置模式	test: ISIS 路由区域标签
Switch(config-router))# net 49.0124.0000.0000.0014.00	配置 IS-IS 进程的网络实体名称 NET（Network Entity Title）	网络实体名称的格式为 X…X.XXXX.XXXX.XXXX.00，前面的“X…X”是区域地址，中间的 12 个“X”是无线接入控制器的 System ID，最后的“00”是 SEL。

6.2.3 配置 Level 类型

IS-IS 进程的 Level 类型有以下三种：

Level-1: 配置路由器工作在 Level-1，它只计算区域内路由，维护 L1 的 LSDB。

Level-2: 配置路由器工作在 Level-1-2，同时参与 L1 和 L2 的路由计算，维护 L1 和 L2 两个 LSDB。

level-2-only: 配置路由器工作在 Level-2，只参加 L2 的 LSP 交换和 L2 的路由计算，维护 L2 的 LSDB。

如果只有一个区域，建议用户将所有路由器的 Level 配置为 Level-1 或者 Level-2-only，因为没有必要让所有路由器同时维护两个相同的数据库。在 IP 网络中使用该命令时，建议将所有的路由器都配置为 Level-2-only，这样有利于以后的扩展。

表6-3 配置Level类型

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# router isis test	创建 ISIS 进程并进入 ISIS 配置模式	test: ISIS 路由区域标签
Switch(config-router)# is-type level-2-only	配置 Level 类型	缺省情况下，未配置 IS-IS 进程的 Level 类型

6.2.4 配置接口使能 IPv6 IS-IS 功能

在全局配置模式下完成 IS-IS 进程的配置之后，为了使 IS-IS 协议正常运行，还需要在运行 IS-IS 协议的链路接口上使能 IS-IS 并与指定进程相关联。

表6-4 配置接口使能IPv6 IS-IS功能

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# interface eth-0-1	进入接口配置模式	-
Switch(config-if)# ipv6 router isis test	在接口上使能 IPv6 IS-IS 功能并指定要关联的 IS-IS 进程	test: IS-IS 路由进程标签

6.3 配置 IPv6 IS-IS 路由聚合

可以针对给定级别聚合多组地址，还可以聚合从其他路由协议中学习到的路由。此命令有助于减小路由表的大小。

表6-5 配置IPv6 IS-IS路由聚合

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# router isis test	创建 ISIS 进程并进入 ISIS 配置模式	test: ISIS 路由区域标签
Switch(config-router)# address-family ipv6	创建 IS-IS IPv6 地址族，并进入 IS-IS IPv6 地址族模式	启用 IPv6 ISIS 的功能，将 IPv4 与 IPv6 的配置分开
Switch(config-router-af)# summary-prefix 2001:1:1::/48	配置 IPv6 IS-IS 聚合路由	聚合路由 2001:1:1::/48 包括了子网 2001:1:1:1::/64 ，2001:1:1:2::/64 等。此时，只有 2001:1:1::/48 这条聚合路由会发布出去。 缺省情况下，不对外部路由进行聚合

6.4 配置禁用 IS-IS 邻居检查功能

对于单拓扑 IS-IS IPv6，必须将路由器配置为运行同一组地址族。IS-IS 对 Hello 数据包执行一致性检查，并且将拒绝没有相同配置的地址族集的 Hello 数据包。例如，同时为 IPv4 和 IPv6 运行 IS-IS 的路由器不会与只为 IPv4 或 IPv6 运行 IS-IS 的路由器形成邻接关系。为了允许在不匹配的地址族网络

中形成邻接，必须禁用 IPv6 地址族配置模式下的**adjacency-check**命令。

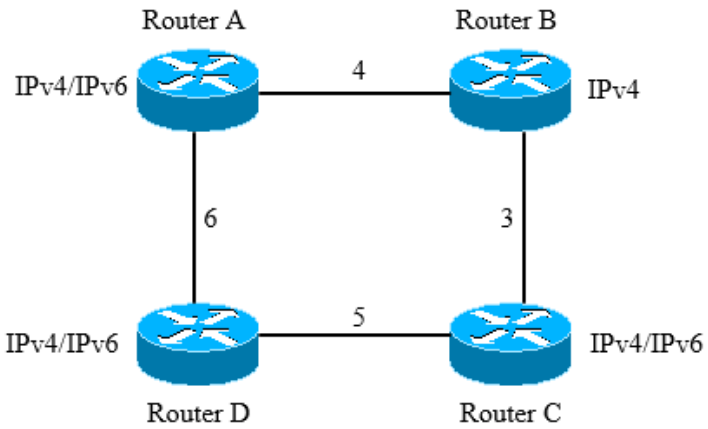
表6-6 配置禁用IS-IS邻居检查功能

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# router isis test	创建 ISIS 进程并进入 ISIS 配置模式	test: ISIS 路由区域标签
Switch(config-router)# address-family ipv6	创建 IS-IS IPv6 地址族，并进入 IS-IS IPv6 地址族模式	启用 IPv6 ISIS 的功能，将 IPv4 与 IPv6 的配置分开
Switch(config-router-af)# no adjacency-check	配置禁用 IS-IS 邻居检查功能	缺省情况下，IS-IS 邻居检查功能处于开启状态

6.5 配置 IS-IS 多拓扑

IS-IS多拓扑是指在一个IS-IS自治域中有多个独立的IP拓扑运行，如IPv4拓扑和IPv6拓扑。在IS-IS在路由计算中能够根据实际组网情况将IPv4与IPv6进行分拓扑计算，根据链路支持的协议类型，不同拓扑运行各自的SPF计算，实现IPv4和IPv6网络的相互屏蔽。

图 6-1 IS-IS 多拓扑示意图



如上图所示，图中的数值表示对应链路上的开销值，Router A、Router C、Router D支持IPv4/IPv6双协

议栈，Router B只支持IPv4协议，无法转发IPv6报文。

如果Router A不支持IS-IS多拓扑，进行SPF计算时只需要考虑单一的拓扑，则RA-RC最短路径是Router A-Router B-Router C，但是由于Router B不支持IPv6，因此Router A发送的IPv6报文无法通过Router B传送到Router C；如果Router A上开启IS-IS多拓扑特性，Router A进行SPF计算时会根据不同拓扑分别计算。当Router A需要发送IPv6报文给Router C时，Router A只需要根据IPv6链路确定IPv6报文转发的路径，那么Router A-Router C的IPv6路径为Router A-Router D-Router C。

表6-7 配置IS-IS多拓扑

命令举例	操作	说明
Switch# configure terminal	进入全局配置模式	-
Switch(config)# router isis test	创建 ISIS 进程并进入 ISIS 配置模式	test: ISIS 路由区域标签
Switch(config-router)# address-family ipv6	创建 IS-IS IPv6 地址族，并进入 IS-IS IPv6 地址族模式	启用 IPv6 ISIS 的功能，将 IPv4 与 IPv6 的配置分开
Switch(config-router-af)# multi-topology level-1-2	开启 IS-IS 多拓扑	缺省情况下，IS-IS 多拓扑处于关闭状态

EVPN 配置指导目录

1 VXLAN 配置

1.1 VXLAN 简介

VXLAN (Virtual eXtensible Local Area Network，虚拟扩展局域网) 是一种隧道网络技术，其将基于 MAC 的二层以太网数据报文封装在三层 UDP 的数据报文中，通过三层路由网络实现承载在三层网络上的二层网络通信。VXLAN 技术把逻辑网络的数量扩大到 1600 万个，并且支持异地跨 IP 的二层互联。在 VXLAN 网络中的终端都有 VTEP (VXLAN Tunnel End Point) 设备，通过 VXLAN 网络使终端所在的路由器之间形成一条虚拟隧道，负责对 VXLAN 协议报文进行加封装和解封装。

从网络架构上来看，VXLAN 技术通过三层网络来承载和构建虚拟的二层网络，即为 Overlay 网络，尽可能地减少对网络进行修改的情况下，主要基于 IP 网络技术，实现应用在网络上的承载，将其与网络业务分离。

1.2 配置 VXLAN

1.2.1 使能 VLAN 的 Overlay 功能

配置 Overlay 的 VLAN 和 VNI 的映射关系之前，需要先使能 VLAN 的 Overlay 功能。

表1-1 使能VLAN的Overlay功能

命令	操作	说明
configure terminal	进入全局配置模式	-
vlan database	进入 VLAN 配置模式	-
vlan *vlan-id*	创建 VLAN ID	vlan-id: VLAN ID，取值范围为 1~4094
vlan *vlan-id* **overlay enable**	使能 VLAN 的 Overlay 功能	vlan-id: VLAN ID，取值范围为 2~4094 缺省情况下，去使能 VLAN 的 Overlay 功能

1.2.2 进入 Overlay 配置模式

表 1-2 进入 Overlay 配置模式

命令	操作	说明
configure terminal	进入全局配置模式	-
overlay	进入 Overlay 配置模式	使用 **exit** 命令退出 Overlay 配置模式

1.2.3 配置 Overlay 映射

该命令用于绑定 VLAN 和 Overlay 的 VNI 的关系，一旦一个 VLAN 和 VNI 绑定，VLAN 下所有的端口属于 VNI 的广播域，并且可以在 VNI 的广播域内进行单播、组播和广播。

表 1-3 配置 Overlay 映射

命令	操作	说明
configure terminal	进入全局配置模式	-
overlay	进入 Overlay 配置模式	使用 **exit** 命令退出 Overlay 配置模式
vlan *vlan-id* **vni** *vni-id*	配置 VLAN 和 VNI 的映射关系	vlan-id: VLAN ID，取值范围为 2~4094 vni-id: VXLAN 网络标识符，取值范围为 1~16777215

1.2.4 配置 Overlay 源/远端 VTEP

Overlay VTEP 的源地址用于对 Overlay 的原始报文进行加封装和解封装。建议源地址采用三层口地址（比如环回口），并保证该地址的路由可达。

创建 Overlay 的远端 VTEP 的类型和地址时，管理员应该知晓整个数据中心网络上的所有邻居，并且保证路由的可达性。

表 1-4 配置 Overlay 源/远端 VTEP

命令	操作	说明
configure terminal	进入全局配置模式	-
overlay	进入 Overlay 配置模式	使用 **exit** 命令退出 Overlay 配置模式

命令	操作	说明
source *ip-addresss*	配置 Overlay 的源地址	ip-address: Overlay 的 VTEP 的源地址，必须是一个有效的 IP 地址
remote-vtep *index* **ip-address** *remote-ip-address* **type vxlan** [**src-ip** *source-ip-address* | **split-horizon-disable** | **keep-vlan-tag**]	配置 Overlay 远端 VTEP 的类型和地址	index: 远端 VTEP 的索引，取值范围为 1~65535 remote-ip-address: Overlay 远端 VTEP 的地址 source-ip-address: Overlay 源端 VTEP 的地址
vlan *vlan-id* **vni** *vni-id*	配置 VLAN 和 VNI 的映射关系	vlan-id: VLAN ID，取值范围为 2~4094 vni-id: VXLAN 网络标识符，取值范围为 1~16777215
vlan *vlan-id* **remote-vtep** *index*	配置 Overlay VLAN 的远端 VTEP 邻居	vlan-id: VLAN ID，取值范围为 2~4094 index: 远端 VTEP 的索引，取值范围为 1~65535 使用此命令前，必须先创建该索引对应的远端 VTEP

1.2.5 配置 Overlay 的上联口

该命令只能在以太类型的端口上使用，如果该端口是三层路由端口或者三层链路聚合的路由端口，则其能同时在普通和增强型的 Overlay 的负载分担模式下工作，如果该端口为 VLAN 端口，则只能在普通的 Overlay 负载分担模式下工作。

表 1-5 配置 Overlay 的上联口

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 以太网类型端口名称
overlay uplink { **enable** | **disable** }	配置 Overlay 的上联口	缺省情况下，去使能 Overlay 的上联口

说明

普通的负载分担模式可以支持所有类型的上联口，但是仅能支持 1K 个远端 VTEP。推荐在小型的传统数据中心中使用。而增强型的负载分担模式则无法支持 vlan interface 作为上联口，但是能支持超过 4K 的远端 VTEP，推荐在大型的新型 spine-leaf 架构的数据中心中使用。

1.3 显示与维护

表 1-6 显示与维护

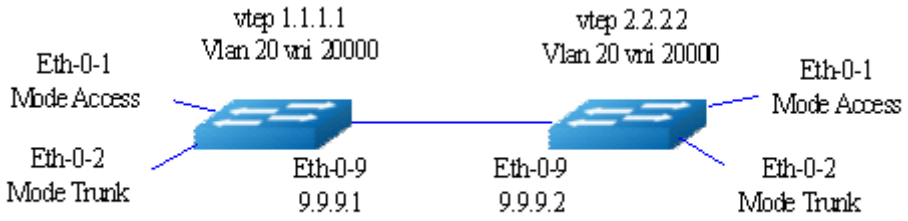
命令	操作	说明
show overlay [**vlan** *vlan-id*]	显示 Overlay 相关信息	vlan-id: VLAN ID，取值范围为 2~4094

1.4 配置举例

1.4.1 配置 VXLAN 示例

1. 拓扑

图 1-1 配置 VXLAN 拓扑图



2. 配置步骤

DUT1:

命令举例	操作步骤
DUT1# configure terminal	进入全局配置模式
DUT1 (config)# vlan database	进入 VLAN 配置模式
DUT1 (config-vlan)# vlan 20	创建 VLAN 20
DUT1 (config-vlan)# vlan 20 overlay enable	使能 VLAN 20 的 Overlay 功能

命令举例	操作步骤
DUT1 (config-vlan)# exit	返回全局配置模式
DUT1 (config)# interface eth-0-1	进入端口 eth-0-1 配置
DUT1 (config-if)# switchport access vlan 20	端口加入 VLAN 20
DUT1 (config-if)# no shutdown	打开端口
DUT1 (config-if)# interface eth-0-2	进入端口 eth-0-2 配置
DUT1 (config-if)# switchport mode trunk	更改端口为 trunk 模式
DUT1 (config-if)# switchport trunk allowed vlan add 20	端口加入 VLAN 20
DUT1 (config-if)# no shutdown	打开端口
DUT1 (config-if)# interface eth-0-9	进入端口 eth-0-9 配置
DUT1 (config-if)# no switchport	更改成路由端口
DUT1 (config-if)# ip address 9.9.9.1/24	配置 IP 地址
DUT1 (config-if)# overlay uplink enable	使能 Overlay 的上联口
DUT1 (config-if)# no shutdown	打开端口
DUT1 (config-if)# interface loopback0	创建环回口
DUT1 (config-if)# ip address 1.1.1.1/32	配置 IP 地址
DUT1 (config-if)# exit	返回全局配置模式
DUT1 (config)# ip route 2.2.2.0/24 9.9.9.2	配置静态路由
DUT1 (config)# overlay	进入 Overlay 配置模式
DUT1 (config-overlay)# source 1.1.1.1	配置 VXLAN 的源 VTEP 地址
DUT1 (config-overlay)# remote-vtep 1 ip-address 2.2.2.2 type vxlan	创建远端 VXLAN 的 VTEP
DUT1 (config-overlay)# vlan 20 vni 20000	配置 VLAN 和 VNI 的映射
DUT1 (config-overlay)# vlan 20 remote-vtep 1	配置 VLAN 的 VXLAN 远端 VTEP 邻居

DUT2:

命令举例	操作步骤
DUT2# configure terminal	进入全局配置模式

命令举例	操作步骤
DUT2 (config)# vlan database	进入 VLAN 配置模式
DUT2 (config-vlan)# vlan 20	创建 VLAN 20
DUT2 (config-vlan)# vlan 20 overlay enable	使能 VLAN 20 的 Overlay 功能
DUT2 (config-vlan)# exit	返回全局配置模式
DUT2 (config)# interface eth-0-1	进入端口 eth-0-1 配置
DUT2 (config-if)# switchport access vlan 20	端口加入 VLAN 20
DUT2 (config-if)# no shutdown	打开端口
DUT2 (config-if)# interface eth-0-2	进入端口 eth-0-2 配置
DUT2 (config-if)# switchport mode trunk	更改端口到 trunk 模式
DUT2 (config-if)# switchport trunk allowed vlan add 20	端口加入 VLAN 20
DUT2 (config-if)# no shutdown	打开端口
DUT2 (config-if)# interface eth-0-9	进入端口 eth-0-9 配置
DUT2 (config-if)# no switchport	更改成路由端口
DUT2 (config-if)# ip address 9.9.9.2/24	配置 IP 地址
DUT2 (config-if)# overlay uplink enable	使能 Overlay 的上联口
DUT2 (config-if)# no shutdown	打开端口
DUT2 (config-if)# interface loopback0	创建环回口
DUT2 (config-if)# ip address 2.2.2.2/32	配置 IP 地址
DUT2 (config-if)# exit	返回全局配置模式
DUT2 (config)# ip route 1.1.1.0/24 9.9.9.1	配置静态路由
DUT2 (config)# overlay	进入 Overlay 配置模式
DUT2 (config-overlay)# source 2.2.2.2	配置 VXLAN 的源 VTEP 地址
DUT2 (config-overlay)# remote-vtep 1 ip-address 1.1.1.1 type vxlan	创建 VXLAN 的远端 VTEP
DUT2 (config-overlay)# vlan 20 vni 20000	配置 VLAN 和 VNI 的映射
DUT2 (config-overlay)# vlan 20 remote-vtep 1	配置 VLAN 的 VXLAN 远端 VTEP 邻居

3. 命令验证

完成上述步骤后，显示 Overlay 相关信息：

```
DUT1# show overlay vlan 20

------------------------------------------------------------
ECMP Mode              : Normal
Source VTEP          : 1.1.1.1
Remote VTEP Index: 1, Ip address: 2.2.2.2, Type: VxLAN
------------------------------------------------------------
VLAN ID              : 2
VNI                  : 20000
Remote VTEP NUM: 1
                Index: 1, Ip address: 2.2.2.2,    Type: VxLAN
DVR Gateway NUM: 0
------------------------------------------------------------
```

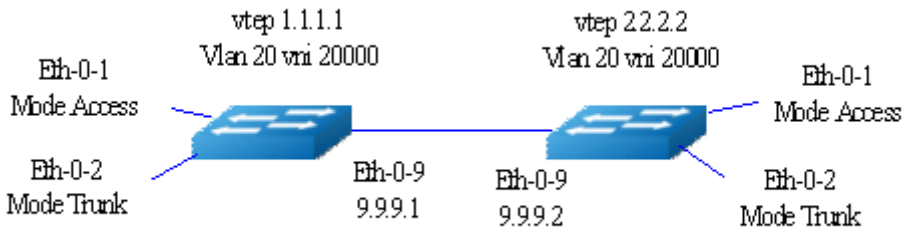
1.4.2 配置 Overlay 支持多上联

1. 介绍

Overlay 支持多上联，是为了满足用户针对不同的公网而设定不同的源 IP 地址，提高 Overlay 的可靠性。

2. 拓扑

图 1-2 配置 Overlay 多上联拓扑图



3. 配置步骤

DUT1:

命令举例	操作步骤
DUT1# configure terminal	进入全局配置模式
DUT1 (config)# vlan database	进入 VLAN 配置模式
DUT1 (config-vlan)# vlan 20	创建 VLAN 20
DUT1 (config-vlan)# vlan 20 overlay enable	使能 VLAN 20 的 Overlay 功能
DUT1 (config-vlan)# exit	返回全局配置模式
DUT1 (config)# interface eth-0-1	进入端口 eth-0-1 配置
DUT1 (config-if)# switchport access vlan 20	端口加入 VLAN 20
DUT1 (config-if)# no shutdown	打开端口
DUT1 (config-if)# interface eth-0-2	进入端口 eth-0-2 配置
DUT1 (config-if)# switchport mode trunk	更改端口为 trunk 模式
DUT1 (config-if)# switchport trunk allowed vlan add 20	端口加入 VLAN 20
DUT1 (config-if)# no shutdown	打开端口
DUT1 (config-if)# interface eth-0-9	进入端口 eth-0-9 配置
DUT1 (config-if)# no switchport	更改成路由端口
DUT1 (config-if)# ip address 9.9.9.1/24	配置 IP 地址
DUT1 (config-if)# overlay uplink enable	使能 Overlay 的上联口
DUT1 (config-if)# no shutdown	打开端口
DUT1 (config-if)# interface loopback0	创建环回口
DUT1 (config-if)# ip address 1.1.1.1/32	配置 IP 地址
DUT1 (config-if)# exit	返回全局配置模式
DUT1 (config)# ip route 2.2.2.0/24 9.9.9.2	配置静态路由
DUT1 (config)# overlay	进入 Overlay 配置模式
DUT1 (config-overlay)# source 1.1.1.1	配置 VXLAN 的源 VTEP 地址
DUT1 (config-overlay)# remote-vtep 1 ip-address 2.2.2.2 type vxlan	创建远端 VXLAN 的 VTEP，缺省情况下使用全局源 IP 地址 1.1.1.1
DUT1 (config-overlay)# vlan 20 vni 20000	配置 VLAN 和 VNI 的映射

命令举例	操作步骤
DUT1 (config-overlay)# vlan 20 remote-vtep 1	配置 VLAN 的 VXLAN 远端 VTEP 邻居
DUT1 (config-overlay)# vlan 20 remote-vtep 2	配置 VLAN 的 VXLAN 远端 VTEP 邻居，且 VTEP 指定自身的源 IP 地址

DUT2:

命令举例	操作步骤
DUT2# configure terminal	进入全局配置模式
DUT2 (config)# vlan database	进入 VLAN 配置模式
DUT2 (config-vlan)# vlan 20	创建 VLAN 20
DUT2 (config-vlan)# vlan 20 overlay enable	使能 VLAN 20 的 Overlay 功能
DUT2 (config-vlan)# exit	返回全局配置模式
DUT2 (config)# interface eth-0-1	进入端口 eth-0-1 配置
DUT2 (config-if)# switchport access vlan 20	端口加入 VLAN 20
DUT2 (config-if)# no shutdown	打开端口
DUT2 (config-if)# interface eth-0-2	进入端口 eth-0-2 配置
DUT2 (config-if)# switchport mode trunk	更改端口为 trunk 模式
DUT2 (config-if)# switchport trunk allowed vlan add 20	端口加入 VLAN 20
DUT2 (config-if)# no shutdown	打开端口
DUT2 (config-if)# interface eth-0-9	进入端口 eth-0-9 配置
DUT2 (config-if)# no switchport	更改成路由端口
DUT2 (config-if)# ip address 9.9.9.2/24	配置 IP 地址
DUT2 (config-if)# overlay uplink enable	使能 Overlay 的上联口
DUT2 (config-if)# no shutdown	打开端口
DUT2 (config-if)# interface loopback0	创建环回口
DUT2 (config-if)# ip address 2.2.2.2/32	配置 IP 地址
DUT2 (config-if)# exit	返回全局配置模式
DUT2 (config)# ip route 1.1.1.0/24 9.9.9.1	配置静态路由

命令举例	操作步骤
DUT2 (config)# overlay	进入 Overlay 配置模式
DUT2 (config-overlay)# source 2.2.2.2	配置 VXLAN 的源 VTEP 地址
DUT2 (config-overlay)# remote-vtep 1 ip-address 1.1.1.1 type vxlan	创建 VXLAN 的远端 VTEP
DUT2 (config-overlay)# vlan 20 vni 20000	配置 VLAN 和 VNI 的映射
DUT2 (config-overlay)# vlan 20 remote-vtep 1	配置 VLAN 的 VXLAN 远端 VTEP 邻居

4. 命令验证

- 完成上述步骤后，显示DUT1 Overlay相关信息：

```
DUT1# show overlay vlan 20

------------------------------------------------------------
ECMP Mode              : Normal
Source VTEP          : 1.1.1.1
------------------------------------------------------------
VLAN ID              : 2
VNI                  : 20000
Remote VTEP NUM: 1
            Index: 1, Ip address: 2.2.2.2, Source ip: 1.1.1.1, Type: VxLAN
DVR Gateway NUM: 0

------------------------------------------------------------
```

- 显示DUT2 Overlay相关信息：

```
DUT2# show overlay vlan 20

------------------------------------------------------------
ECMP Mode              : Normal
Source VTEP          : 2.2.2.2
------------------------------------------------------------
VLAN ID              : 2
VNI                  : 20000
Remote VTEP NUM: 1
            Index: 1, Ip address: 1.1.1.1 Source ip: 2.2.2.2, Type: VxLAN
DVR Gateway NUM: 0

------------------------------------------------------------
```

2 EVPN 配置

2.1 EVPN 简介

EVPN（Ethernet Virtual Private Network）是一种用于二层网络互联的 VPN 技术。它在 BGP 协议的基础上定义了一种新的 NLRI（Network Layer Reachability Information，网络层可达信息），即 EVPN NLRI。EVPN NLRI 定义了几种新的 BGP EVPN 路由类型，目前支持 TYPE-2、TYPE-3、TYPE-5 路由，用于处在二层网络的不同站点之间同步主机路由信息。

2.2 配置 EVPN

2.2.1 使能 EVPN 功能

配置该命令可以使能EVPN功能。在进入EVPN配置模式后，可以创建EVPN实例。当EVPN功能关闭后，所有的EVPN实例将被删除。

表2-1 使能EVPN功能

命令	操作	说明
configure terminal	进入全局配置模式	-
evpn	使能 EVPN 功能并进入 EVPN 配置模式	缺省情况下，未使能 EVPN 功能
vni *value*	创建 EVPN 实例，并进入 EVPN 实例配置模式	value: 指定 VNI，有效范围为 1~16777215
rd { **auto** | *rd-value* }	配置 EVPN 实例的 RD	rd-value: 指定 EVPN 实例的 RD, 格式为“ASN:nn or IP:nn”
route-target [**import** | **export** | **both**] { **auto** | *rt-value* }	配置 EVPN 实例的 Route Target	rt-value: 指定 EVPN 实例的 Route Target，格式为“ASN:nn or IP:nn”

说明

创建 EVPN 实例后，需要配置 EVPN 实例的 RD 和 Route Target，路由才会发布和学习。

2.2.2 配置 EVPN 地址族

进入 EVPN 地址族配置模式之前，需要在全局配置模式下，使能 EVPN 功能。

表 2-2 配置 EVPN 地址族

命令	操作	说明
configure terminal	进入全局配置模式	-
router bgp *as-number*	配置 BGP 路由进程	指定 AS 号，取值范围为 1~4294967295
address-family l2vpn evpn	配置 EVPN 地址族，并进入 EVPN 地址族配置模式	缺省情况下，未配置 EVPN 地址族

2.2.3 配置 BGP 邻居属性

在 TCP 连接被邻居打开以后，**neighbor activate** 用于使能和邻居路由器之间指定 AF 信息交换。

表 2-3 配置 BGP 邻居属性

命令	操作	说明
configure terminal	进入全局配置模式	-
router bgp *as-number*	配置 BGP 路由进程	as-number: 指定 AS 号，取值范围为 1~4294967295
neighbor *neighbor-id* **remote-as** *as-number*	创建对等体组	neighbor-id: BGP 邻居 IP 地址 as-number: 指定 AS 号，取值范围为 1~4294967295
address-family l2vpn evpn	配置 EVPN 地址族，并进入 EVPN 地址族配置模式	缺省情况下，未配置 EVPN 地址族
neighbor *neighbor-id* **activate**	使能与邻居交换路由信息	neighbor-id: BGP 邻居 IP 地址

命令	操作	说明
neighbor { *neighbor-id* | *peer-group-name* } **send-community** [**both** | **extended** | **standard**]	配置向 BGP 邻居发送团体属性	peer-group-name: 对等体组名

2.2.4 使能 EVPN 主机信息搜集功能

在使能 EVPN 主机信息搜集功能后，还需要配置 EVPN 实例的 RD 和 Route Target，然后从 ARP 中获得的主机信息，才会通过 BGP 形成 EVPN 的 MAC/IP Advertisement 路由并发布出去。

表 2-4 使能 EVPN 主机信息搜集功能

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
overlay host-collect enable	使能 EVPN 主机信息搜集功能	缺省情况下，未使能 EVPN 主机信息搜集功能

2.3 显示与维护

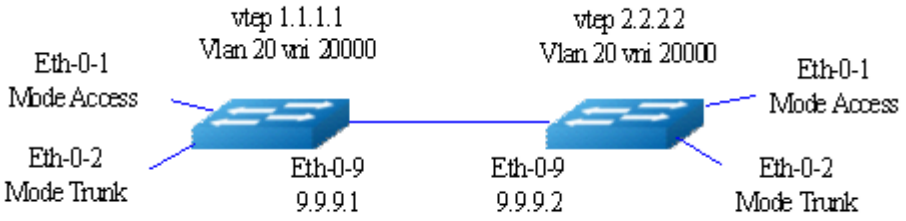
表 2-5 显示与维护

命令	操作	说明
show bgp evpn all	显示所有 EVPN 路由信息	-
show bgp evpn neighbors summary	显示 EVPN BGP 邻居摘要信息	-
show overlay host-information vni *value*	显示通过 EVPN 学习到的主机信息	value: 指定 VNI，有效范围为 1~16777215

2.4 配置举例

2.4.1 拓扑

图 2-1 配置 BGP EVPN



2.4.2 配置步骤

1. VXLAN的配置如下：

DUT1:

命令举例	操作步骤
DUT1# configure terminal	进入全局配置模式
DUT1(config)# ip vrf test	创建 VRF
DUT1(config-vrf)# vni 50000 l3	创建 L3 VNI
DUT1(config-vrf)# rd 1:50000	配置 L3 VNI RD
DUT1(config-vrf)#route-target both 50:50000	配置 L3 VNI RT
DUT1(config-vrf)# exit	返回全局配置模式
DUT1 (config)# vlan database	进入 VLAN 配置模式
DUT1 (config-vlan)# vlan 20	创建 VLAN 20
DUT1 (config-vlan)# vlan 20 overlay enable	使能 VLAN 20 的 Overlay 功能
DUT1 (config-vlan)# exit	返回全局配置模式
DUT1 (config)# interface eth-0-9	进入端口 eth-0-9 配置
DUT1 (config-if)# no switchport	更改成路由端口
DUT1 (config-if)# ip address 9.9.9.1/24	配置 IP 地址

命令举例	操作步骤
DUT1 (config-if)# overlay uplink enable	使能 Overlay 的上联口
DUT1 (config-if)# no shutdown	打开端口
DUT1 (config-if)# interface loopback0	创建环回口
DUT1 (config-if)# ip address 1.1.1.1/32	配置 IP 地址
DUT1 (config-if)# exit	返回全局配置模式
DUT1 (config)# ip route 2.2.2.0/24 9.9.9.2	配置静态路由
DUT1 (config)# overlay	进入 Overlay 配置模式
DUT1 (config-overlay)# source 1.1.1.1	配置 VXLAN 的源 VTEP 地址
DUT1 (config-overlay)# vtep reachability protocol bgp	开启动态建 VxLAN 隧道功能
DUT1 (config-overlay)# vlan 20 vni 20000	配置 VLAN 和 VNI 的映射
DUT1 (config- overlay)# exit	返回全局配置模式
DUT1(config)# evpn	进入 EVPN 配置模式
DUT1(config-evpn)# vni 20000	创建 L2 VNI
DUT1(config-evi)# rd auto	配置自动生成 RD
DUT1(config-evi)# route-target both auto	配置自动生成 RT
DUT1(config-evi)# exit	返回 EVPN 配置模式
DUT1(config-evpn)# exit	返回全局配置模式
DUT1 (config)# interface vlan 20	进入接口 VLANIF 20 的配置
DUT1 (config-if)# ip address 10.10.10.1/24	配置接口 VLANIF 20 的地址
DUT1 (config-if)# overlay host-collect enable	使能主机信息搜集功能
DUT1(config- router)# exit	返回全局配置模式

DUT2:

命令举例	操作步骤
DUT2# configure terminal	进入全局配置模式
DUT2(config)# ip vrf test	创建 VRF

命令举例	操作步骤
DUT2(config-vrf)# vni 50000 l3	创建 L3 VNI
DUT2(config-vrf)# rd 1:50000	配置 L3 VNI RD
DUT2(config-vrf)#route-target both 50:50000	配置 L3 VNI RT
DUT2(config-vrf)# exit	返回全局配置模式
DUT2 (config)# vlan database	进入 VLAN 配置模式
DUT2 (config-vlan)# vlan 20	创建 VLAN 20
DUT2 (config-vlan)# vlan 20 overlay enable	使能 VLAN 20 的 Overlay 功能
DUT2 (config-vlan)# exit	返回全局配置模式
DUT2 (config)# interface eth-0-9	进入端口 eth-0-9 配置
DUT2 (config-if)# no switchport	更改成路由端口
DUT2 (config-if)# ip address 9.9.9.2/24	配置 IP 地址
DUT2 (config-if)# overlay uplink enable	使能 Overlay 的上联口
DUT2 (config-if)# no shutdown	打开端口
DUT2 (config-if)# interface loopback0	创建环回口
DUT2 (config-if)# ip address 2.2.2.2/32	配置 IP 地址
DUT2 (config-if)# exit	返回全局配置模式
DUT2 (config)# ip route 1.1.1.0/24 9.9.9.1	配置静态路由
DUT2 (config)# overlay	进入 Overlay 配置模式
DUT2 (config-overlay)# source 2.2.2.2	配置 VXLAN 的源 VTEP 地址
DUT2 (config-overlay)# vtep reachability protocol bgp	开启动态建 VxLAN 隧道功能
DUT2 (config-overlay)# vlan 20 vni 20000	配置 VLAN 和 VNI 的映射
DUT2 (config- overlay)# exit	返回全局配置模式
DUT2(config)# evpn	进入 EVPN 配置模式
DUT2(config-evpn)# vni 20000	创建 L2 VNI
DUT2(config-evi)# rd auto	配置自动生成 RD

命令举例	操作步骤
DUT2(config-evi)# route-target both auto	配置自动生成 RT
DUT2(config-evi)# exit	返回 EVPN 配置模式
DUT2(config-evpn)# exit	返回全局配置模式
DUT2 (config)# interface vlan 20	进入接口 VLANIF 20 的配置
DUT2 (config-if)# ip address 10.10.10.2/24	配置接口 VLANIF 20 的地址
DUT2 (config-if)# overlay host-collect enable	使能主机信息搜集功能
DUT2(config- router)# exit	返回全局配置模式

2. BGP的配置如下：

DUT1:

命令举例	操作步骤
DUT1# configure terminal	进入全局配置模式
DUT1 (config)# router bgp 100	创建 BGP 100 并进入路由配置模式
DUT1 (config-router)# neighbor 2.2.2.2 remote-as 100	创建 IBGP 邻居
DUT1(config-router)# neighbor 2.2.2.2 update-source loopback0	指定更新源端口
DUT1 (config- router)# address-family l2vpn evpn	进入 EVPN 地址族配置模式
DUT1 (config- router-af)# neighbor 2.2.2.2 activate	使能与邻居交换路由信息
DUT1 (config- router-af)# exit	使能发送扩展团体属性
DUT1(config-router)# address-family ipv4 vrf test	进入 IPV4 VRF 地址族配置模式
DUT1(config-router-af)# redistribute connected	配置路由重发布
DUT1(config-router-af)# advertise l2vpn	配置重发布路由引入 EVPN
DUT1(config-router-af)# exit	返回路由配置模式
DUT1(config- router)# exit	返回全局配置模式

DUT2:

命令举例	操作步骤
DUT2# configure terminal	进入全局配置模式
DUT2 (config)# router bgp 100	创建 BGP 100 并进入路由配置模式
DUT2 (config-router)# neighbor 1.1.1.1 remote-as 100	创建 IBGP 邻居
DUT2(config-router)# neighbor 1.1.1.1 update-source loopback0	指定更新源端口
DUT2 (config- router)# address-family l2vpn evpn	进入 EVPN 地址族配置模式
DUT2 (config- router-af)# neighbor 1.1.1.1 activate	使能与邻居交换路由信息
DUT2 (config- router-af)# exit	使能发送扩展团体属性
DUT2(config-router)# address-family ipv4 vrf test	进入 IPV4 VRF 地址族配置模式
DUT2(config-router-af)# redistribute connected	配置路由重发布
DUT2(config-router-af)# advertise l2vpn	配置重发布路由引入 EVPN
DUT2(config-router-af)# exit	返回路由配置模式
DUT2(config- router)# exit	返回全局配置模式

2.4.3 命令验证

- 显示所有EVPN路由信息：

```
DUT1# show bgp evpn all

Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:20000 (VNI 20000)
*>i[2]:[0]:[48]:[04cd.a0ac.7b00]:[32]:[10.10.10.10]/136
                    2.2.2.2                  100      0 i
Route Distinguisher: 1:20000
*>i[2]:[0]:[48]:[04cd.a0ac.7b00]:[32]:[10.10.10.10]/136
                    2.2.2.2                  100      0 i
```

- 显示当前的路由表状态：

```
DUT1# show ip route

Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       Dc - DHCP Client
       [*] - [AD/Metric]
       * - candidate default
C        1.1.1.1/32 is directly connected, loopback0
S        2.2.2.0/24 [1/0] via 9.9.9.2, eth-0-9
C        9.9.9.0/24 is directly connected, eth-0-9
C        9.9.9.1/32 is in local loopback, eth-0-9
C        10.10.10.0/24 is directly connected, vlan20
C        10.10.10.1/32 is in local loopback, vlan20
B        10.10.10.10/32 is in overlay remote vxlan vtep:1.1.1.1->2.2.2.2, vni:20000
```

IPv6 业务配置指导目录

1 IPv6 over IPv4 隧道配置

1.1 隧道技术简介

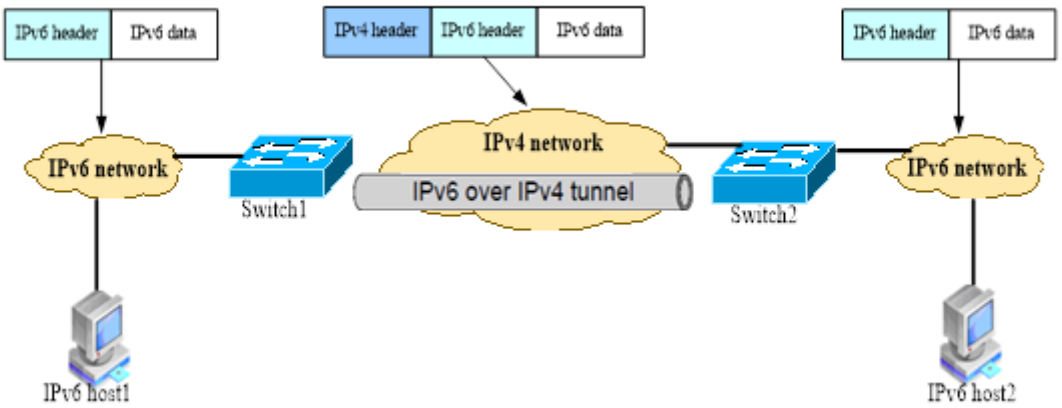
隧道技术是一种封装技术，它利用一种网络协议来传输另一种网络协议，即一种网络协议将其他网络协议的数据报文封装在自己的报文中，然后在网络中传输。封装后的数据报文在网络中传输的路径，称为隧道。隧道是一条虚拟的点对点连接，隧道的两端需要对数据报文进行封装及解封装。隧道技术就是指包括数据封装、传输和解封装在内的全过程。

1.1.1 IPv6 over IPv4 隧道定义

在 IPv4 Internet 向 IPv6 Internet 过渡的初期，IPv4 网络已被大量部署，而 IPv6 网络只是散布在世界各地的一些孤岛。在 IPv4 网络上用于连接 IPv6 孤岛的隧道，称为 IPv6 over IPv4 隧道，即 IPv6 报文被封装在 IPv4 报文中，实现 IPv6 报文的透明传输。为了实现 IPv6 over IPv4 隧道，需要在 IPv4 网络与 IPv6 网络交界的边界交换机上启动 IPv4/IPv6 双协议栈。

1.1.2 IPv6 over IPv4 隧道工作原理

图 1-1 IPv6 over IPv4 隧道原理图



如上图，IPv6 over IPv4 隧道对报文的处理过程如下：

- IPv6 网络中的设备发送 IPv6 报文，该报文到达隧道的源端设备 Switch1。

- Switch1 根据路由表判定该报文要通过隧道进行转发后，在 IPv6 报文前封装上 IPv4 的报文头，通过隧道的实际物理接口将报文转发出去。
- 封装报文通过隧道到达隧道目的端设备 Switch2，Switch2 判断该封装报文的目的地是本设备后，将对报文进行解封装。
- Switch2 根据解封装后的 IPv6 报文的目的地址转发该 IPv6 报文。如果目的地就是本设备，则将 IPv6 报文转给上层协议处理。

  该技术的优点：不必将所有的设备都升级为双栈，只要求 IPv4/IPv6 网络的边缘设备实现双栈和隧道功能即可。除边缘节点外，其它节点不需要支持双协议栈。可以大大利用现有的 IPv4 网络资源。

根据隧道终点的 IPv4 地址的获取方式不同，隧道分为“配置隧道”和“自动隧道”。

- 如果 IPv6 over IPv4 隧道的终点地址不能从 IPv6 报文的目的地址中自动获取，需要进行手工配置，这样的隧道称为“配置隧道”。
- 如果 IPv6 over IPv4 隧道的终点地址采用内嵌 IPv4 地址的特殊 IPv6 地址形式，则可以从 IPv6 报文的目的地址中自动获取隧道终点的 IPv4 地址，这样的隧道称为“自动隧道”。
- 目前，常用的 IPv6 over IPv4 隧道模式有以下三种：
  - IPv6 over IPv4 手动隧道
  - 6to4 隧道
  - ISATAP 隧道

1. IPv6 over IPv4 **手动隧道**

   IPv6 手工配置隧道的源和目的地址是手工指定的，它提供了一个点到点的连接。IPv6 手工配置隧道可以建立在两个边界路由器之间为被 IPv4 网络分离的 IPv6 网络提供稳定的连接，或建立在终端系统与边界路由器之间为终端系统访问 IPv6 网络提供连接。隧道的端点设备必须支持 IPv4/IPv6 双协议栈。其它设备只需实现单协议栈即可。

   IPv6 手工配置隧道要求在设备上手工配置隧道的源地址和目的地址，如果一个边界设备要与多个设备建立手工隧道，就需要在设备上配置多个隧道。所以手工隧道通常用于两个边界路由器之间，为两个 IPv6 网络提供连接。

2. 6to4 隧道

- 普通 6to4 隧道

  6to4 隧道是点到多点的自动隧道，主要用于将多个 IPv6 孤岛通过 IPv4 网络连接到 IPv6 网络。6to4 隧道通过在 IPv6 报文的目的地址中嵌入 IPv4 地址，来实现自动获取隧道终点的 IPv4 地址。

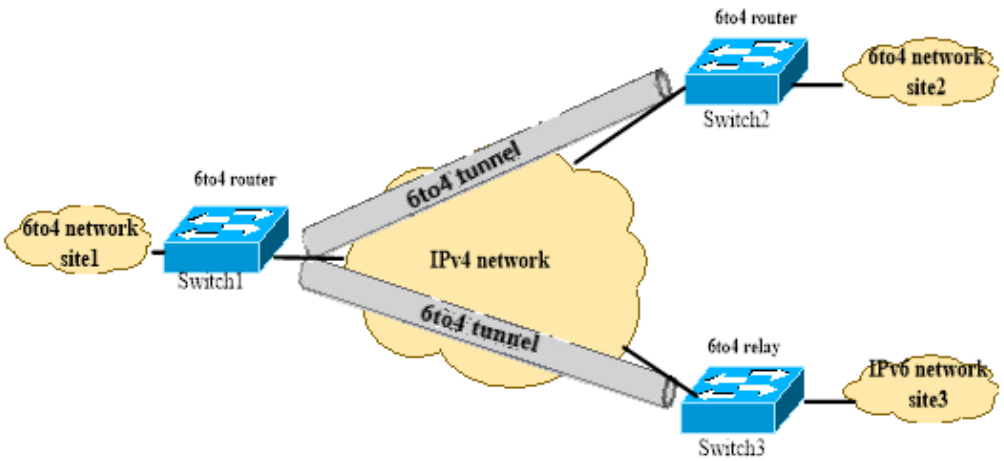
  6to4 隧道使用了一种特殊的 IPv6 地址，即 6to4 地址，其格式为：2002:IPv4 地址:子网 ID:接口 ID。

  6to4 地址的前缀是 2002:IPv4 地址，前缀长度为 48bits。其中 IPv4 地址是为 IPv6 孤岛申请的一个全球唯一的 IPv4 地址。在 IPv6/IPv4 边界交换机与 IPv4 网络连接的物理接口上必须配置该 IPv4 地址。子网 ID 的长度为 16bits，接口 ID 的长度为 64bits，均由用户在 IPv6 孤岛内分配。

- 6to4 中继

  6to4 隧道只能用于前缀为 2002::/16 的 6to4 网络之间的通信，但在 IPv6 网络中也会使用像 2001::/16 这样的 IPv6 网络地址。为了实现 6to4 网络和其它 IPv6 网络的通信，必须有一台 6to4 路由器作为网关转发到 IPv6 网络的报文，这台路由器就叫做 6to4 中继（6to4 Relay）路由器。（如果 IPv6 报文的目的地址不是 6to4 地址，但下一跳是 6to4 地址，则从下一跳地址中取出 IPv4 地址作为隧道的目的地址。）

图 1-2 6to4 隧道示意图



如上图所示，IPv6 报文在到达边界路由器后，根据报文的 IPv6 目的地址查找转发表，如果出接口是 6to4 自动隧道的 Tunnel 虚接口，且报文的目的地址是 6to4 地址或下一跳是 6to4 地址，则从 6to4 地址中取出 IPv4 地址作为隧道报文的目的地址，隧道报文的源地址是 Tunnel 接口上配置的。

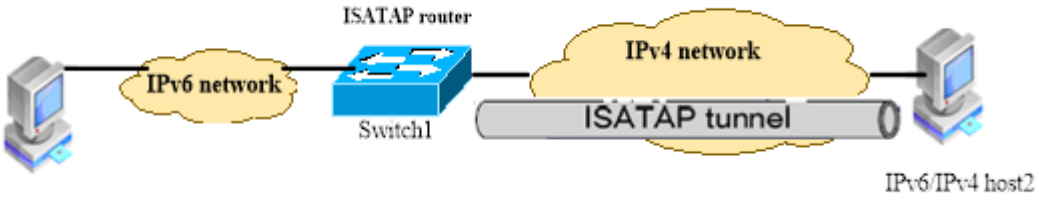
3. ISATAP 隧道

随着 IPv6 技术的推广，现有的 IPv4 网络中将会出现越来越多的 IPv6 主机，ISATAP 隧道技术为这种应用提供了一个较好的解决方案。ISATAP 隧道是点到多点的自动隧道技术，通过在 IPv6 报文的目的地址中嵌入的 IPv4 地址，可以自动获取隧道的终点。

使用 ISATAP 隧道时，IPv6 报文的目的地址和隧道接口的 IPv6 地址都要采用特殊的 ISATAP 地址。其格式为：Prefix(64bit)::5EFE:IPv4-Address。

在创建 ISATAP 隧道时，由于 IPv4/IPv6 主机和 ISATAP 交换机在同一个 IPv4 网络中，ISATAP 地址中嵌入的 IPv4 地址可以是公网地址，也可以是私网地址。ISATAP 隧道主要用于在 IPv4 网络中 IPv6 路由器—IPv6 路由器、IPv6 主机—IPv6 路由器的连接。

图 1-3 ISATAP 隧道示意图



如上图所示，IPv4/IPv6 主机获得 IPv6 地址的过程如下：

1. IPv4/IPv6主机发送交换机请求消息IPv4/IPv6主机使用ISATAP格式的链路本地地址向ISATAP交换机发送交换机请求消息，该交换机请求消息被封装在IPv4报文中。
2. ISATAP交换机响应请求ISATAP交换机使用交换机通告消息响应主机的交换机请求。交换机通告消息中包含ISATAP前缀（ISATAP前缀在交换机上通过人工配置）。
3. IPv4/IPv6主机将ISATAP前缀与5EFE:IPv4-Address组合得到自己的IPv6地址，并用此地址访问IPv6主机。

1.2 配置 IPv6 over IPv4 隧道

1.2.1 配置隧道接口

如果要通过IPv4网络来连接两个隔离的IPv6网络，首先要创建Tunnel接口。配置其他属性之后，此Tunnel接口可用。使能IPv6后就可以转发IPv6报文。

表1-1 配置隧道接口

命令	操作	说明
configure terminal	进入全局配置模式	-
interface tunnel *tunnel-id*	创建 Tunnel 接口，并进入 Tunnel 接口配置模式	tunnel-id: 接口编号，取值范围为 0～1023
tunnel source { *source-ip-address* | *source-ipv6-address* | *if-name* }	配置隧道的源地址	source-ip-address: 隧道的源地址为 IPv4 地址格式 source-ipv6-address: 指定隧道的源地址为 IPv6 地址格式 if-name: 指定隧道的源地址从接口 IPv4/IPv6 地址中获得，如果接口上有多个地址，则只取主 IP 地址。接口可以为：路由口、VLAN 虚拟口、环回口
tunnel mode ipv6ip [**6to4** | **isatap** | **gre** | **multi-dst-gre**]	配置隧道模式	当指定 **6to4** 或 **isatap** 关键字时为自动隧道模式，指定 **gre** 或 **multi-dst-gre** 为手工隧道模式
tunnel destination { *dst-ip-address* | *dst-ipv6-address* }	配置隧道的目的地址	dst-ip-address: 指定 Tunnel 接口的目的 IPv4 地址 dst-ipv6-address: 指定 tunnel 接口的目的 IPv6 地址 当隧道模式为手工隧道时，才需要配置隧道目的地址
ipv6 address *ipv6-address/mask-length*	配置 Tunnel 接口的 IPv6 地址	ipv6-address: IPv6 地址 mask-length: 掩码长度

说明

创建的 Tunnel 接口没有配置隧道模式之前，不能进行有关接口上的任何操作，此时接口不具备任何功能，只是单纯地创建了接口结构体。

1.2.2 使能隧道报文解封装

表 1-2 使能隧道报文解封装

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
tunnel enable	使能解封装接口上的隧道报文	缺省情况下，不会对收到的隧道报文解封装

1.2.3 配置隧道路由

为了保证本端设备与远端设备路由的互通性，必须有经过隧道接口转发的路由。

表 1-3 配置隧道路由

命令	操作	说明
configure terminal	进入全局配置模式	-
ipv6 route *ipv6-address/mask-length* **tunnel** *tunnel-id*	配置隧道的静态路由	ipv6-address: IPv6 地址 mask-length: 掩码长度 tunnel-id: 接口编号，取值范围为 0～1023

1.3 显示与维护

表 1-4 显示与维护

命令	操作	说明
show interface tunnel *tunnel-id*	显示 Tunnel 接口的信息	tunnel-id: 接口编号，取值范围为 0～1023
show resource tunnel	显示 Tunnel 资源的使用信息	-

1.4 配置举例

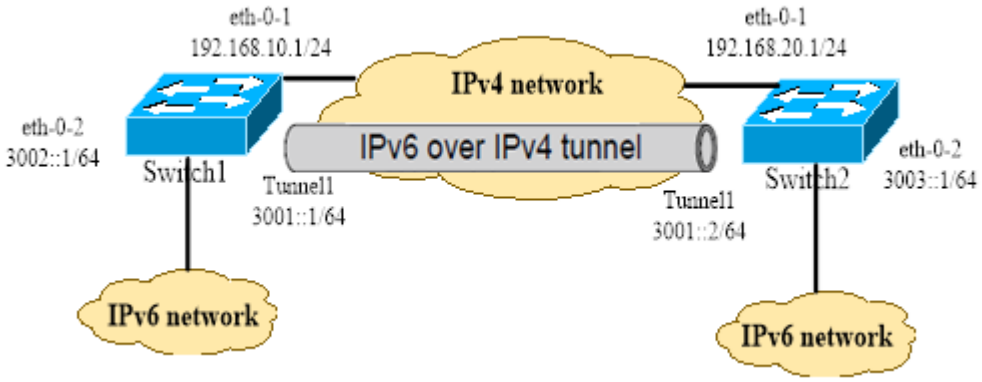
1.4.1 配置手工隧道

i. 简介

如下图所示，两个 IPv6 网络分别通过 Switch1 和 Switch2 与 IPv4 网络连接，要求在 Switch1 和 Switch2 之间建立 IPv6 手动隧道，使两个 IPv6 网络可以互通。

ii. 拓扑

图 1-4 配置手工隧道拓扑图



iii. 配置步骤

Switch 1 的配置如下：

1. 使能IPv6功能

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# ipv6 enable	全局使能 IPv6

2. 配置IPv4地址，使报文路由3层可达

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# no switchport	将 eth-0-1 配置为 3 层路由口
Switch(config-if)# ip address 192.168.10.1/24	配置接口的 IPv4 地址
Switch(config)# ip route 192.168.20.0/24 192.168.10.2	配置到达对端的 IPv4 静态路由
Switch(config)# arp 192.168.10.2 0.0.2222	配置静态 ARP，0.0.2222 为下一跳的系统 MAC 地址（该 ARP 条目也可以通过动态学习得到）

3. 配置eth-0-2的IPv6地址

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-2	进入接口配置模式
Switch(config-if)# no switchport	将 eth-0-2 配置为 3 层路由口
Switch(config-if)# ipv6 address 3002::1/64	配置接口的 IPv6 地址

4. 配置Tunnel接口

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface tunnel1	创建 Tunnel 虚接口
Switch(config-if)# tunnel source eth-0-1	将 eth-0-1 口作为 Tunnel 的源
Switch(config-if)# tunnel destination 192.168.20.1	配置 Tunnel 的目的地
Switch(config-if)# tunnel mode ipv6ip	配置 Tunnel 模式为手工隧道
Switch(config-if)# ipv6 address 3001::1/64	配置 Tunnel 接口的 IPv6 地址

5. 使能Tunnel报文解封装

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式

命令举例	操作步骤
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# tunnel enable	使能 eth-0-1 接口 Tunnel 解封装

6. 配置到达对端的静态IPv6路由

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# ipv6 route 3003::/16 tunnel1	配置到达隧道对端的静态路由

类似地，Switch 2 的配置如下：

1. 使能IPv6功能

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# ipv6 enable	全局使能 IPv6

2. 配置IPv4地址，使报文路由3层可达

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# no switchport	将 eth-0-1 配置为 3 层路由口
Switch(config-if)# ip address 192.168.20.1/24	配置接口的 IPv4 地址
Switch(config)# ip route 192.168.10.0/24 192.168.20.2	配置到达对端的 IPv4 静态路由
Switch(config)# arp 192.168.20.2 0.0.1111	配置静态 ARP，0.0.1111 为下一跳的系统 MAC 地址（该 ARP 条目也可以通过动态学习得到）

3. 配置eth-0-2的IPv6地址

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-2	进入接口配置模式
Switch(config-if)# no switchport	将 eth-0-2 配置为 3 层路由口

命令举例	操作步骤
Switch(config-if)# ipv6 address 3003::1/64	配置接口的 IPv6 地址

4. 配置Tunnel接口

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface tunnel1	创建 Tunnel 虚接口
Switch(config-if)# tunnel source eth-0-1	将 eth-0-1 口作为 Tunnel 的源
Switch(config-if)# tunnel destination 192.168.10.1	配置 Tunnel 的目的地
Switch(config-if)# tunnel mode ipv6ip	配置 Tunnel 模式为手工隧道
Switch(config-if)# ipv6 address 3001::2/64	配置 Tunnel 接口的 IPv6 地址

5. 配置Tunnel报文解封装

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# tunnel enable	使能 eth-0-1 接口 Tunnel 解封装

6. 配置到达对端的静态IPv6路由

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# ipv6 route 3002::/16 tunnel1	配置到达隧道对端的静态路由

iv. 命令验证

Switch 1：

- 显示Switch 1上Tunnel接口的信息：

```
Switch1# show interface tunnel1
Interface tunnel1
   Interface current state: UP
   Hardware is Tunnel
   Index 8193 , Metric 1 , Encapsulation TUNNEL
   VRF binding: not bound
   Tunnel protocol/transport IPv6/IP, Status Valid
```

```
    Tunnel source 192.168.10.1(eth-0-1), destination 192.168.20.1
    Tunnel DSCP inherit,    Tunnel TTL 64
    Tunnel transport MTU 1480 bytes
```

- 显示Switch 1上Tunnel接口的IPv6状态：

```
Switch1# show ipv6 interface tunnel1
  Interface current state: UP
  The maximum transmit unit is 1480 bytes
  IPv6 is enabled, link-local address is fe80::c0a8:a01
  Global unicast address(es):
    3001::1, subnet is 3001::/64
  ICMP error messages limited to one every 1000 milliseconds
  ICMP redirects are always sent
  ND DAD is enabled, number of DAD attempts: 1
  ND router advertisement is disabled
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND retransmit interval is 1000 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements max interval: 600 secs
  ND router advertisements min interval: 198 secs
  ND router advertisements live for 1800 seconds
  ND router advertisements hop-limit is 0
  Hosts use stateless autoconfig for addresses.
```

Switch 2：

- 显示Switch 2上Tunnel接口的信息：

```
Switch# show interface tunnel1

Interface tunnel1
  Interface current state: UP
  Hardware is Tunnel
  Index 8193 , Metric 1 , Encapsulation TUNNEL
  VRF binding: not bound
  Tunnel protocol/transport IPv6/IP, Status Valid
  Tunnel source 192.168.20.1(eth-0-1), destination 192.168.10.1
  Tunnel DSCP inherit,    Tunnel TTL 64
  Tunnel transport MTU 1480 bytes
```

- 显示Switch 2上Tunnel接口的IPv6状态：

```
Switch# show ipv6 interface tunnel1

  Interface current state: UP
  The maximum transmit unit is 1480 bytes
  IPv6 is enabled, link-local address is fe80::c0a8:1401
```

```
Global unicast address(es):
  3001::2, subnet is 3001::/64
ICMP error messages limited to one every 1000 milliseconds
ICMP redirects are always sent
ND DAD is enabled, number of DAD attempts: 1
ND router advertisement is disabled
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements max interval: 600 secs
ND router advertisements min interval: 198 secs
ND router advertisements live for 1800 seconds
ND router advertisements hop-limit is 0
Hosts use stateless autoconfig for addresses.
```

说明

1. 在配置之前，必须全局使能IPv6功能；
2. 必须使IPv4报文3层路由可达，否则会造成Tunnel报文转发失败。
3. Tunnel接口上必须配置IPv6地址，否则配置在该接口上的路由无效。

1.4.2 配置 6to4 隧道

i. 简介

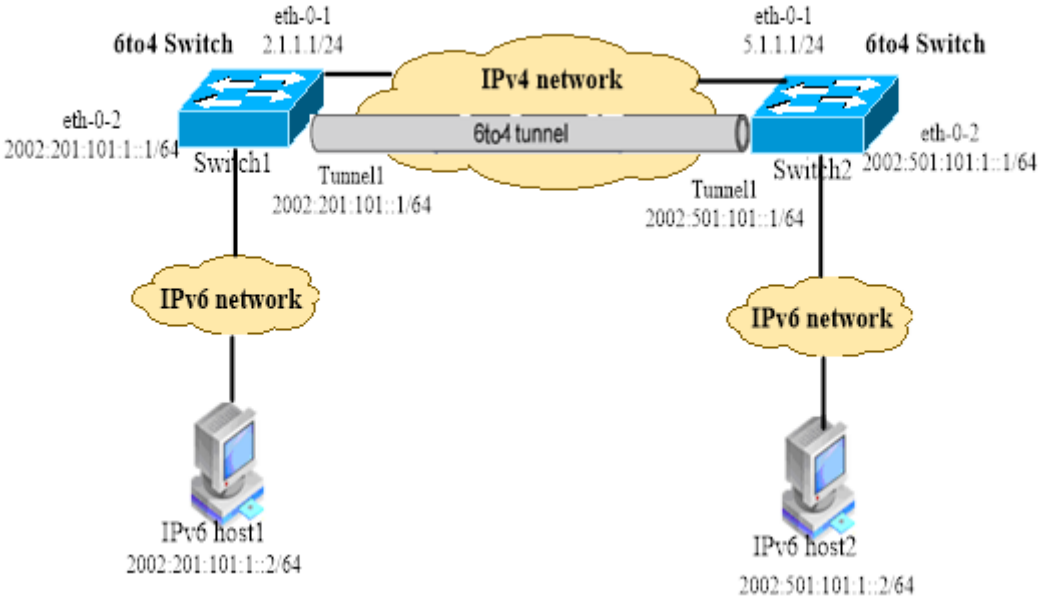
如下图所示，两个 6to4 网络通过网络边缘 6to4 Switch（Switch1 和 Switch2）与 IPv4 网络相连。在 Switch1 和 Switch2 之间建立 6to4 隧道，实现 6to4 网络中的主机 Host1 和 Host2 之间的互通。

为了实现 6to4 网络之间的互通，除了配置 6to4 隧道外，还需要为 6to4 网络内的主机及 6to4 路由器配置 6to4 地址。

- Switch1 上接口 eth-0-1 的 IPv4 地址为 2.1.1.1/24，转换成 IPv6 地址后使用 6to4 前缀 2002:0201:0101::/48。对此前缀进行子网划分，Tunnel1 使用 2002:0201:0101::/64 子网，eth-0-2 使用 2002:0201:0101:1::/64 子网。
- Switch2 上接口 eth-0-1 的 IPv4 地址为 5.1.1.1/24，转换成 IPv6 地址后使用 6to4 前缀 2002:0501:0101::/48。对此前缀进行子网划分，Tunnel1 使用 2002:0501:0101::/64 子网，eth-0-2 使用 2002:0501:0101:1::/64 子网。

ii. 拓扑

图 1-5 配置 6to4 隧道拓扑图



iii. 配置步骤

Switch 1 的配置如下：

1. 使能IPv6功能

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# ipv6 enable	全局使能 IPv6

2. 配置IPv4地址，使报文路由3层可达

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# no switchport	将 eth-0-1 配置为 3 层路由口
Switch(config-if)# ip address 2.1.1.1/24	配置接口的 IPv4 地址
Switch(config)# ip route 5.1.1.0/24 2.1.1.2	配置到达对端的 IPv4 静态路由

命令举例	操作步骤
Switch(config)# arp 2.1.1.2 0.0.2222	配置静态 ARP，0.0.2222 为下一跳的系统 MAC 地址（该 ARP 条目也可以通过动态学习得到）

3. 配置eth-0-2的IPv6地址

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-2	进入接口配置模式
Switch(config-if)# no switchport	将 eth-0-2 配置为 3 层路由口
Switch(config-if)# ipv6 address 2002:201:101:1::1/64	配置接口的 IPv6 地址

4. 配置Tunnel接口

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface tunnel1	创建 Tunnel 虚接口
Switch(config-if)# tunnel source eth-0-1	将 eth-0-1 口作为 Tunnel 的源
Switch(config-if)# tunnel mode ipv6ip 6to4	配置 Tunnel 模式为 6to4 隧道
Switch(config-if)# ipv6 address 2002:201:101::1/64	配置 Tunnel 接口的 IPv6 地址

5. 使能Tunnel报文解封装

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# tunnel enable	使能 eth-0-1 接口 Tunnel 解封装

6. 配置到达对端的静态IPv6路由

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# ipv6 route 2002::/16 tunnel1	配置到达隧道对端的静态路由

类似地，Switch 2 的配置如下：

1. 使能IPv6功能

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# ipv6 enable	全局使能 IPv6

2. 配置IPv4地址，使报文路由3层可达

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# no switchport	将 eth-0-1 配置为 3 层路由口
Switch(config-if)# ip address 5.1.1.1/24	配置接口的 IPv4 地址
Switch(config)# ip route 2.1.1.0/24 5.1.1.2	配置到达对端的 IPv4 静态路由
Switch(config)# arp 5.1.1.2 0.0.1111	配置静态 ARP，0.0.1111 为下一跳的系统 MAC 地址（该 ARP 条目也可以通过动态学习得到）

3. 配置eth-0-2的IPv6地址

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-2	进入接口配置模式
Switch(config-if)# no switchport	将 eth-0-2 配置为 3 层路由口
Switch(config-if)# ipv6 address 2002:501:101:1::1/64	配置接口的 IPv6 地址

4. 配置Tunnel接口

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface tunnel1	创建 Tunnel 虚接口
Switch(config-if)# tunnel source eth-0-1	将 eth-0-1 口作为 Tunnel 的源
Switch(config-if)# tunnel mode ipv6ip 6to4	配置 Tunnel 模式为 6to4 隧道
Switch(config-if)# ipv6 address 2002:501:101::1/64	配置 Tunnel 接口的 IPv6 地址

5. 配置Tunnel报文解封装

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# tunnel enable	使能 eth-0-1 接口 Tunnel 解封装

6. 配置到达对端的静态IPv6路由

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# ipv6 route 2002::/16 tunnel1	配置到达隧道对端的静态路由

v. 命令验证

- 显示Switch 1上Tunnel接口的信息：

```
Switch1# show interface tunnel1

Interface tunnel1
   Interface current state: UP
   Hardware is Tunnel
   Index 8193 , Metric 1 , Encapsulation TUNNEL
   VRF binding: not bound
   Tunnel protocol/transport IPv6/IP 6to4, Status Valid
   Tunnel source 2.1.1.1(eth-0-1), destination UNKNOWN
   Tunnel DSCP inherit,    Tunnel TTL 64
   Tunnel transport MTU 1480 bytes
```

- 显示Switch 2上Tunnel接口的信息：

```
Switch1# show interface tunnel1

Interface tunnel1
   Interface current state: UP
   Hardware is Tunnel
   Index 8193 , Metric 1 , Encapsulation TUNNEL
   VRF binding: not bound
   Tunnel protocol/transport IPv6/IP 6to4, Status Valid
   Tunnel source 5.1.1.1(eth-0-1), destination UNKNOWN
   Tunnel DSCP inherit,    Tunnel TTL 64
   Tunnel transport MTU 1480 bytes
```

说明

1. 6to4隧道无需配置目的地址；
2. 对于自动隧道，使用同种封装协议的Tunnel 接口不能同时配置完全相同的源地址。
3. 如果封装前 IPv6 报文的目的IPv6 地址与Tunnel 接口的IPv6 地址不在同一个网段，则必须配置通过Tunnel 接口到达目的IPv6 地址的转发路由，以便需要进行封装的报文能正常转发。对于自动隧道，用户只能配置静态路由，指定到达目的IPv6 地址的路由出接口为本端Tunnel 接口或下一跳为对端Tunnel 接口地址，不支持动态路由。
4. 一台交换机上只允许存在一条6to4隧道。

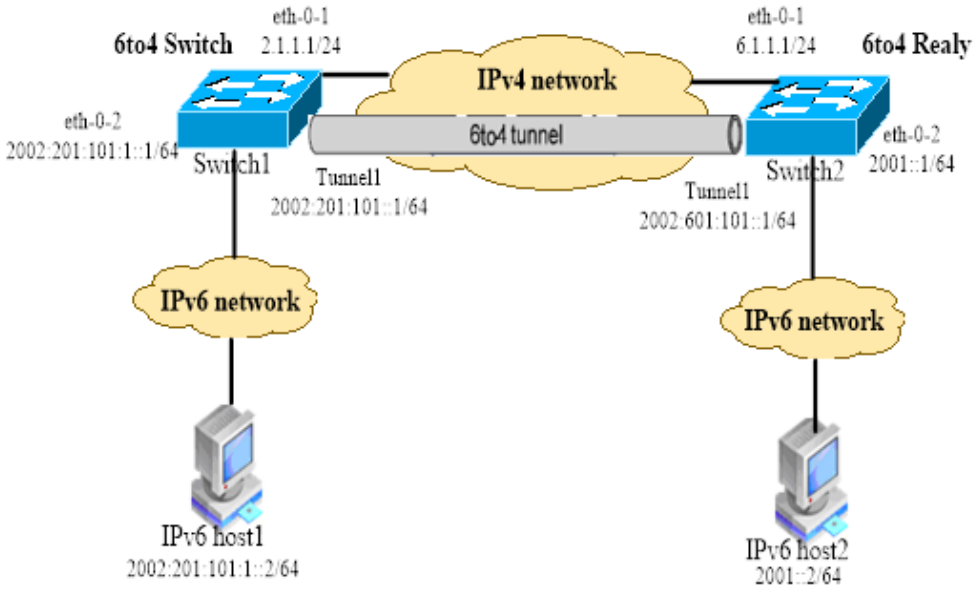
1.4.3 配置 6to4 中继

i. 简介

如下图所示，Switch1为6to4 交换机，其IPv6 侧的网络使用6to4 地址。Switch2作为6to4 中继交换机，它和IPv6 网络（2001::/16）相连。要求在Switch1和Switch2之间配置6to4 隧道，使得6to4 网络中的主机与IPv6 网络中的主机互通。

ii. 拓扑

图 1-6 配置 6to4 中继拓扑图



iii. 配置步骤

Switch 1 的配置如下：

1. 使能IPv6功能

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# ipv6 enable	全局使能 IPv6

2. 配置IPv4地址，使报文路由3层可达

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# no switchport	将 eth-0-1 配置为 3 层路由口
Switch(config-if)# ip address 2.1.1.1/24	配置接口的 IPv4 地址
Switch(config)# ip route 6.1.1.0/24 2.1.1.2	配置到达对端的 IPv4 静态路由
Switch(config)# arp 2.1.1.2 0.0.2222	配置静态 ARP，0.0.2222 为下一跳的系统 MAC 地址（该 ARP 条目也可以通过动态学习得到）

3. 配置eth-0-2的IPv6地址

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-2	进入接口配置模式
Switch(config-if)# no switchport	将 eth-0-2 配置为 3 层路由口
Switch(config-if)# ipv6 address 2002:201:101:1::1/64	配置接口的 IPv6 地址

4. 配置Tunnel接口

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface tunnel1	创建 Tunnel 虚接口

命令举例	操作步骤
Switch(config-if)# tunnel source eth-0-1	将 eth-0-1 口作为 Tunnel 的源
Switch(config-if)# tunnel mode ipv6ip 6to4	配置 Tunnel 模式为 6to4 隧道
Switch(config-if)# ipv6 address 2002:201:101::1/64	配置 Tunnel 接口的 IPv6 地址

5. 使能Tunnel报文解封装

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# tunnel enable	使能 eth-0-1 接口 Tunnel 解封装

6. 配置到达对端的静态IPv6路由

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# ipv6 route 2001::/16 2002:601:101::1	配置到纯 IPv6 网络的静态路由
Switch(config)# ipv6 route 2002:601:101::/48 tunnel1	配置到 6to4 中继的静态路由

类似地，Switch 2 的配置如下：

1. 使能IPv6功能

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# ipv6 enable	全局使能 IPv6

2. 配置IPv4地址，使报文路由3层可达

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# no switchport	将 eth-0-1 配置为 3 层路由口
Switch(config-if)# ip address 6.1.1.1/24	配置接口的 IPv4 地址
Switch(config)# ip route 2.1.1.0/24 6.1.1.2	配置到达对端的 IPv4 静态路由

命令举例	操作步骤
Switch(config)# arp 6.1.1.2 0.0.1111	配置静态 ARP，0.0.1111 为下一跳的系统 MAC 地址（该 ARP 条目也可以通过动态学习得到）

3. 配置eth-0-2的IPv6地址

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-2	进入接口配置模式
Switch(config-if)# no switchport	将 eth-0-2 配置为 3 层路由口
Switch(config-if)# ipv6 address 2001::1/64	配置接口的 IPv6 地址

4. 配置Tunnel接口

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface tunnel1	创建 Tunnel 虚接口
Switch(config-if)# tunnel source eth-0-1	将 eth-0-1 口作为 Tunnel 的源
Switch(config-if)# tunnel mode ipv6ip 6to4	配置 Tunnel 模式为 6to4 隧道
Switch(config-if)# ipv6 address 2002:601:101::1/64	配置 Tunnel 接口的 IPv6 地址

5. 配置Tunnel报文解封装

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# tunnel enable	使能 eth-0-1 接口 Tunnel 解封装

6. 配置到达对端的静态IPv6路由

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# ipv6 route 2002::/16 tunnel1	配置到达隧道对端的静态路由

vi. 命令验证

Switch 1：

- 显示Switch 1上Tunnel接口的信息：

```
Switch1# show interface tunnel1

Interface tunnel1
   Interface current state: UP
   Hardware is Tunnel
   Index 8193 , Metric 1 , Encapsulation TUNNEL
   VRF binding: not bound
   Tunnel protocol/transport IPv6/IP 6to4, Status Valid
   Tunnel source 2.1.1.1(eth-0-1), destination UNKNOWN
   Tunnel DSCP inherit,    Tunnel TTL 64
   Tunnel transport MTU 1480 bytes
```

- 显示Switch 1上IPv6路由信息：

```
Switch1# show ipv6 route

IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, O - OSPF, I - IS-IS, B - BGP
          [*] - [AD/Metric]
Timers: Uptime
S           2001::/16 [1/0]
          via 2002:601:101::1 (recursive via ::, tunnel1), 00:00:32
C           2002:201:101::/64
          via ::, tunnel1, 00:00:04
C           2002:201:101::1/128
          via ::1, tunnel1, 00:00:04
S           2002:601:101::/48 [1/0]
          via ::, tunnel1, 00:00:22
```

- 显示Switch 1上Tunnel接口的IPv6状态：

```
Switch1# show ipv6 interface tunnel1

Interface tunnel1
   Interface current state: UP
   The maximum transmit unit is 1480 bytes
   IPv6 is enabled, link-local address is fe80::201:101
   Global unicast address(es):
      2002:201:101::1, subnet is 2002:201:101::/64
   ICMP error messages limited to one every 1000 milliseconds
   ICMP redirects are always sent
```

```
ND DAD is enabled, number of DAD attempts: 1
ND router advertisement is disabled
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements max interval: 600 secs
ND router advertisements min interval: 198 secs
ND router advertisements live for 1800 seconds
ND router advertisements hop-limit is 0
Hosts use stateless autoconfig for addresses.
```

Switch 2：

- 显示Switch 2上Tunnel接口的信息：

```
Switch2# show interface tunnel1
Interface tunnel1
  Interface current state: UP
  Hardware is Tunnel
  Index 8193 , Metric 1 , Encapsulation TUNNEL
  VRF binding: not bound
  Tunnel protocol/transport IPv6/IP 6to4, Status Valid
  Tunnel source 6.1.1.1(eth-0-1), destination UNKNOWN
  Tunnel DSCP inherit,   Tunnel TTL 64
  Tunnel transport MTU 1480 bytes
```

说明

1. 6to4 中继交换机的配置与6to4 交换机的配置相同，但为实现6to4 网络与IPv6 网络的互通，需要在6to4 交换机上配置到IPv6 网络的路由。
2. 当交换机上存在到达6to4 中继的路由时，不能切换隧道模式。

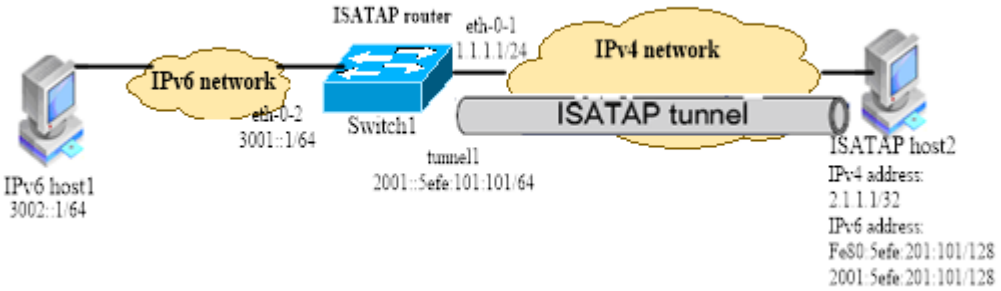
1.4.4 配置 ISATAP 隧道

i. 简介

如上图所示，IPv6 网络和IPv4 网络通过ISATAP交换机相连，在IPv4 网络侧分布着一些IPv6 主机。要求将IPv4 网络中的IPv6 主机通过ISATAP隧道接入到IPv6 网络。

ii. 拓扑

图 1-7 配置 ISATAP 隧道拓扑图



iii. 配置步骤

Switch 1 的配置如下：

1. 使能IPv6功能

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# ipv6 enable	全局使能 IPv6

2. 配置IPv4地址，使报文路由3层可达

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# no switchport	将 eth-0-1 配置为 3 层路由口
Switch(config-if)# ip address 1.1.1.1/24	配置接口的 IPv4 地址
Switch(config)# ip route 2.1.1.0/24 1.1.1.2	配置到达对端的 IPv4 静态路由
Switch(config)# arp 1.1.1.2 0.0.2222	配置静态 ARP，0.0.2222 为下一跳的系统 MAC 地址（该 ARP 条目也可以通过动态学习得到）

3. 配置eth-0-2的IPv6地址

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式

命令举例	操作步骤
Switch(config)# interface eth-0-2	进入接口配置模式
Switch(config-if)# no switchport	将 eth-0-2 配置为 3 层路由口
Switch(config-if)# ipv6 address 3001::1/64	配置接口的 IPv6 地址

4. 配置Tunnel接口

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface tunnel1	创建 Tunnel 虚接口
Switch(config-if)# tunnel source eth-0-1	将 eth-0-1 口作为 Tunnel 的源
Switch(config-if)# tunnel mode ipv6ip isatap	配置 Tunnel 模式为 ISATAP 隧道
Switch(config-if)# ipv6 address 2001::/64 eui-64	配置 Tunnel 接口的 IPv6 地址
Switch(config-if)# no ipv6 nd ra suppress	取消对 RA 消息发布的抑制，使主机可以通过交换机发布的 RA 消息获取地址前缀等信息

5. 使能Tunnel报文解封装

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# tunnel enable	使能 eth-0-1 接口 Tunnel 解封装

6. 配置到达对端的静态IPv6路由

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# ipv6 route 2001::/16 tunnel1	配置到 ISATAP 主机的静态路由

配置 ISATAP 主机：

ISATAP 主机上的具体配置与主机的操作系统有关，下面仅以 Windows XP 操作系统为例进行说明。

在主机上安装 IPv6 协议。

C:\>ipv6 install

在 Windows XP 上，ISATAP 接口通常为接口 2，只要在该接口上配置 ISATAP 交换机的 IPv4 地址即可完成主机侧的配置。显示 ISATAP 接口的信息：

```
Interface 2: Automatic Tunneling Pseudo-Interface
    Guid {48FCE3FC-EC30-E50E-F1A7-71172AEEE3AE}
    does not use Neighbor Discovery
    does not use Router Discovery
    routing preference 1
    EUI-64 embedded IPv4 address: 0.0.0.0
    router link-layer address: 0.0.0.0
        preferred link-local fe80::5efe:2.1.1.1, life infinite
    link MTU 1280 (true link MTU 65515)
    current hop limit 128
    reachable time 25000ms (base 30000ms)
    retransmission interval 1000ms
    DAD transmits 0
    default site prefix length 48
```

C:\>ipv6 rlu 2 1.1.1.1

只需要这么一个命令，就完成了主机的配置，此时 ISATAP 接口的信息显示如下：

```
Interface 2: Automatic Tunneling Pseudo-Interface
    Guid {48FCE3FC-EC30-E50E-F1A7-71172AEEE3AE}
    does not use Neighbor Discovery
    does not use Router Discovery
    routing preference 1
    EUI-64 embedded IPv4 address: 2.1.1.1
    router link-layer address: 1.1.1.1
preferred global 2001::5efe:2.1.1.1, life 29d23h59m46s/6d23h59m46s (public)
        preferred link-local fe80::5efe:2.1.1.1, life infinite
    link MTU 1280 (true link MTU 65515)
    current hop limit 128
    reachable time 25000ms (base 30000ms)
    retransmission interval 1000ms
    DAD transmits 0
    default site prefix length 48
```

iv. 命令验证

Switch 1：

- 显示Switch 1上Tunnel接口的信息：

```
Switch# show interface tunnel1

Interface tunnel1
    Interface current state: UP
    Hardware is Tunnel
    Index 8193 , Metric 1 , Encapsulation TUNNEL
```

```
VRF binding: not bound
Tunnel protocol/transport IPv6/IP ISATAP, Status Valid
Tunnel source 1.1.1.1(eth-0-1), destination UNKNOWN
Tunnel DSCP inherit,  Tunnel TTL 64
Tunnel transport MTU 1480 bytes
```

- 显示Switch 1上Tunnel接口的IPv6状态：

```
Switch# show ipv6 interface tunnel1

Interface tunnel1
  Interface current state: UP
  The maximum transmit unit is 1480 bytes
  IPv6 is enabled, link-local address is fe80::101:101
  Global unicast address(es):
    2001::101:101, subnet is 2001::/64 [EUI]
  ICMP error messages limited to one every 1000 milliseconds
  ICMP redirects are always sent
  ND DAD is enabled, number of DAD attempts: 1
  ND router advertisement is enabled
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND retransmit interval is 1000 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements max interval: 600 secs
  ND router advertisements min interval: 198 secs
  ND next router advertisement due in 359 secs.
  ND router advertisements live for 1800 seconds
  ND router advertisements hop-limit is 0
  Hosts use stateless autoconfig for addresses.
```

说明

1. 对于自动隧道，使用同种封装协议的 Tunnel 接口不能同时配置完全相同的源地址。
2. 如果封装前 IPv6 报文的目的IPv6 地址与Tunnel 接口的IPv6 地址不在同一个网段，则必须配置通过Tunnel 接口到达目的IPv6 地址的转发路由，以便需要进行封装的报文能正常转发。对于自动隧道，用户只能配置静态路由，指定到达目的IPv6 地址的路由出接口为本端Tunnel 接口或下一跳为对端Tunnel 接口地址，不支持动态路由。

2 NDP 配置

2.1 NDP 简介

网络节点（主机和路由器）使用 NDP（Neighbor Discovery Protocol，邻居发现协议）来探测直连邻居的链路层地址。并且提供一种机制，快速验证一个已经缓存在表项中的邻居的有效性。主机还能使用 ND 来找到邻居的路由器。

NDP 主要提供了五种功能：地址解析、跟踪邻居状态、重复地址检测、路由器发现以及重定向等。网络节点之间利用该协议作为一种保活机制，定期探测邻居的有效性，探测邻居链路层地址的改变或邻居失效事件。

2.2 配置 NDP

2.2.1 配置静态邻居

用户可以通过手工配置静态邻居表项的方式，获取链路层地址。如果 IPv6 地址是一个链路本地地址，必须同时指定接口。

表2-1 配置静态邻居

命令	操作	说明
configure terminal	进入全局配置模式	-
ipv6 neighbor *ipv6-address mac-address* [*if-name*]	配置静态邻居表项	ipv6-address: IPv6 地址，格式为 X:X::X:X mac-address: MAC 地址，格式为 HHHH.HHHH.HHHH if-name: 接口名称

2.2.2 配置 IPv6 邻居发现参数

可根据实际情况，配置业务所需要的邻居发现参数（可选）。

表2-2 配置IPv6邻居发现参数

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
ipv6 nd ra hop-limit *hop-limit*	配置 RA 报文中的“Current hop limit”字段	hop-limit: 跳数限制，取值范围为 0~255
ipv6 nd ns-interval *NS-INTERVAL*	配置发送 NS 报文的时间间隔	NS-INTERVAL: NS 报文的间隔，取值范围为 1000~3600000，单位：毫秒。缺省值为 1000
ipv6 nd ra interval *max-interval* [*min-interval*]	配置发送 RA 报文的时间间隔	max-interval: 最大报文间隔，取值范围为 4~1800，单位：秒。缺省值为 600 秒 min-interval: 最小报文间隔，取值范围为 3~1350。缺省值为最大报文间隔*0.33
ipv6 nd managed-config-flag	配置报文的“管理地址配置”标志位	缺省情况下，未设置“管理地址配置”标志位
ipv6 nd other-config-flag	配置报文的“其他有状态配置”标志位	缺省情况下，未设置“其他有状态配置”标志位
ipv6 nd reachable-time *REACHABLE-TIME*	配置邻居处于可达状态的时间	REACHABLE-TIME: 可达状态时间，取值范围为 0~3600000，单位：毫秒。配置“0”时表示使用默认值 30000
ipv6 nd ra lifetime *life-time*	配置 RA 报文的存活时间	life-time: 存活时间，取值范围为 0~9000，单位：秒
ipv6 nd dad attempts *dad-attempts*	配置重复地址探测（DAD）次数	dad-attempts: 探测次数，取值范围为 0~600。“0”表示不探测，默认值为 1

2.3 显示与维护

表2-3 显示与维护

命令	操作	说明
show ipv6 interface *if-name* **prefix**	显示指定接口上 RA 报文发布的前缀信息	if-name: 指定需要显示的接口名
show ipv6 neighbors [**dynamic** | **static** | **interface** *if-name* | *ipv6-address* | **statistics**]	显示邻居表项信息	if-name: 指定需要显示的接口名 ipv6-address: IPv6 地址，格式为 X:X::X:X
clear ipv6 neighbors [**interface** *if-name*] **clear ipv6 neighbors** *ipv6-address* [*if-name*]	清除动态邻居表项	**interface** if-name: 清除指定接口的邻居表项 ipv6-address: 清除指定地址的邻居表项 if-name: 为链路本地地址指定出接口

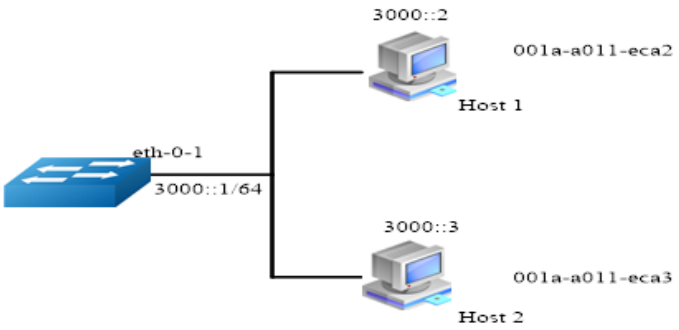
2.4 配置举例

2.4.1 介绍

在这个例子中，接口 eth-0-1 的地址是 3000::1/64。在 3000::/64 网段中有两台主机，地址分别是 3000::2 和 3000::2。MAC 地址分别是 001a-a011-eca2 和 001a-a011-eca3。其中 3000::2 配置了静态邻居，3000::3 通过动态协议学习。配置 eth-0-1 的老化时间为 10 分钟，NS 报文的发送间隔为 2 秒。

2.4.2 拓扑

图 2-1 NDP 配置拓扑图



2.4.3 配置步骤

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch (config)# interface eth-0-1	进入接口配置模式
Switch (config-if)# no switchport	将接口配置为 3 层路由口
Switch (config-if)# no shutdown	打开接口
Switch (config-if)# ipv6 address 3000::1/64	配置 IPv6 地址
Switch (config-if)# ipv6 nd reachable-time 600	配置邻居老化时间
Switch (config-if)# ipv6 nd ns-interval 2000	配置 NS 报文间隔
Switch (config-if)# exit	退出接口配置模式
Switch (config)# ipv6 neighbor 3000::2 001a.a011.eca2	配置静态邻居表项
Switch(config)# end	退出全局配置模式

2.4.4 命令验证

显示邻居表项信息：

```
Switch # show ipv6 neighbors

IPv6 address                              Age         Link-Layer Addr State Interface
3000::2                                     -           001a-a011-eca2  REACH eth-0-1
3000::3                                     6           001a-a011-eca3  REACH eth-0-1
fe80::6d8:e8ff:fe4c:e700                    6           001a-a011-eca3  STALE eth-0-1
```

3 DHCPv6 Relay 配置

3.1 DHCPv6 Relay 简介

DHCPv6 服务器和客户端都在一个子网内，则客户端和服务器之间可以直接进行 DHCPv6 协议的交互，这时不需要启动 DHCPv6 中继功能。如果 DHCPv6 服务器和客户端不在一个子网内，则需要启动 DHCPv6 中继功能将 DHCPv6 报文转发到外部的 DHCPv6 服务器。

DHCPv6 中继转发同正常的 IPv6 路由转发不同，IPv6 路由转发的 IPv6 数据包在网络之间透明交换，而 DHCPv6 中继接收 DHCPv6 消息的同时，会产生一个新的 DHCPv6 消息发送到另一个接口。DHCPv6 中继在报文中设置中继地址，同时可以添加中继信息（Remote-id），转发到 DHCPv6 服务器端。

3.2 配置 DHCPv6 Relay

3.2.1 全局使能 DHCPv6 Relay

只有使用 **service dhcpv6 enable** 命令总开关使能 DHCPv6 服务后，DHCPv6 中继等 DHCPv6 功能才会生效。

表3-1 全局使能DHCPv6 Relay

命令	操作	说明
configure terminal	进入全局配置模式	-
service dhcpv6 enable	使能 DHCPv6 中继代理总开关	缺省情况下，未使能 DHCPv6 中继代理总开关
dhcpv6 relay	启用 DHCPv6 中继服务	缺省情况下，未使能 DHCPv6 功能
dhcpv6 relay remote-id option	配置 DHCPv6 中继启用 remote-id 选项	缺省情况下，未启用 remote-id 选项
dhcpv6 relay pd route	启用中继通过 PD（前	缺省情况下，中继不会学习路由

命令	操作	说明
	缀委派）学习路由	

3.2.2 配置 DHCPv6 服务器组

可在全局配置模式或接口配置模式下添加服务器组。

1. 全局配置模式下添加DHCPv6服务器组

表3-2 全局模式下添加DHCPv6服务器组

命令	操作	说明
configure terminal	进入全局配置模式	-
dhcpv6-server *number ipv6-address* **interface** *if-name*	创建 DHCPv6 服务器组	缺省情况下，系统未设置任何 DHCPv6 服务器组

2. 接口配置模式下添加DHCPv6服务器组

表3-3 接口模式下添加DHCPv6服务器组

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
dhcpv6-server *number*	将接口添加到 DHCPv6 服务器组中	缺省情况下，接口没有添加任何 DHCPv6 服务器组

3.3 显示与维护

表3-4 显示与维护

命令	操作	说明
show dhcpv6-server	查看 DHCPv6 服务器组的配置信息	-
show dhcpv6 relay interfaces	显示 DHCPv6 服务器组下的接口属性	-

命令	操作	说明
show dhcpv6 relay pd client	显示 DHCPv6 中继通过 PD（前缀委派）学到的路由信息	-
show dhcpv6 relay statistics	显示交换机中继的 DHCPv6 报文统计信息	-
clear dhcpv6 relay statistics	清除交换机中继的 DHCPv6 报文统计信息	-
clear dhcpv6 relay pd route [**prefix** *PREFIX*] [**interface** *if-name*] [*ipv6-address*]	清除交换机中继学习到的路由	PREFIX: DHCPv6 服务器分配给客户端的前缀 ipv6-address: DHCPv6 客户端的 IPv6 地址 if-name: 支持的端口名称

3.4 配置举例

3.4.1 介绍

下图为测试 DHCPv6 中继代理功能的网络拓扑，需要两台 PC 机和一台交换机构建测试环境。

- 计算机 A 作为 DHCPv6 服务器
- 计算机 B 作为 DHCPv6 客户端
- 交换机作为 DHCPv6 中继

3.4.2 拓扑

图 3-1 DHCPv6 中继拓扑图

3.4.3 配置步骤

1. 全局使能DHCPv6中继服务

命令举例	操作步骤
Switch(config)# service dhcpv6 enable	使能 DHCPv6 服务器
Switch(config)# dhcpv6 relay	使能 DHCPv6 Relay 功能
Switch(config)# dhcpv6 relay remote-id option	使能 DHCPv6 Remote-id 选项
Switch(config)# dhcpv6 relay pd route	使能 DHCPv6 前缀委派路由学习

2. 配置DHCPv6服务器组

命令举例	操作步骤
Switch(config)# dhcpv6-server 1 2001:1000::1	创建 DHCPv6 服务器组

3. 配置接口eth-0-12

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-12	进入接口配置模式
Switch(config-if)# no switchport	将接口设置三层接口
Switch(config-if)# ipv6 address 2001:1000::2/64	设置 IPv6 地址
Switch(config-if)# no shutdown	使能接口
Switch(config-if)# exit	退出接口配置模式

4. 配置接口eth-0-11

命令举例	操作步骤
Switch(config)# interface eth-0-11	进入接口配置模式
Switch(config-if)# no switchport	将接口设置三层接口.
Switch(config-if)# ipv6 address 2001:1001::1/64	设置 IPv6 地址
Switch(config-if)# no shutdown	使能接口
Switch(config-if)# dhcpv6-server 1	设置 DHCPv6 服务器组
Switch(config-if)# exit	退出接口配置模式

3.4.4 命令验证

1. 检查接口配置：

```
Switch# show running-config interface eth-0-12
!
interface eth-0-12
  no switchport
  ipv6 address 2001:1000::1/64

!

Switch # show running-config interface eth-0-11
!
interface eth-0-11
  no switchport
  ipv6 address 2001:1001::1/64
  dhcpv6-server 1
!
```

2. 检查DHCPv6服务器状态：

```
Switch# show services
Networking services configuration:
Service Name              Status
============================================================
dhcp                        disable
dhcpv6                      enable
```

3. 检查DHCPv6服务器组配置：

```
Switch# show dhcpv6-server
DHCPv6 server group information:
============================================================
group 1 ipv6 address list:

[1] 2001:1000::1
```

4. 显示DHCPv6中继统计信息：

```
Switch# show dhcpv6 relay statistics
DHCPv6 relay packet statistics:
============================================================
Client relayed packets :   8
Server relayed packets :   8
Client error packets     :   0
Server error packets     :   0
```

5. 显示DHCPv6中继通过PD（前缀委派）学到的路由信息：

```
Switch# show dhcpv6 relay pd client
DHCPv6 prefix-delegation client information:
============================================================
Interface   : eth-0-11
Client DUID   : 000100011804ff38c2428f04970
Client IPv6 address   : fe80::beac:d8ff:fedf:c600
      IA ID   : d8dfc60
            IA Prefix :   2002:2:9:eebe::/64
                  prefered/max lifetime : 280/300
                  expired time :   2001-1-1 09:10:58
============================================================
```

IPv6 组播配置指导目录

1 IPv6 组播路由配置

1.1 IPv6 组播路由简介

随着网络的不断发展，网络数据、语音、视频信息等多种交互业务与日俱增。另外，新兴的电子商务、网上会议、网上拍卖、视频点播、远程教学等对带宽和实时数据交互要求较高的服务逐渐兴起，这些服务对信息安全性、可计费性、网络带宽提出了更高的要求。

当网络中需要某信息的用户量不确定时，单播和广播方式的效率会很低，IPv6 组播技术的出现改变了这一现状。当网络中的某些用户需要特定信息时，组播信息发送者（即组播源）仅发送一次信息，借助组播路由协议为组播数据包建立树型路由，被传递的信息在距离用户端尽可能近的节点才开始复制和分发。

通过组播路由协议，多个接收者能跨越不同网络接收到组播数据。

- MLD (Multicast Listener Discovery，组播侦听发现协议) 是 IPv6 协议族中负责 IPv6 组播成员管理的协议。它用来在 IPv6 主机和与其直接相邻的组播路由器之间建立、维护组播组成员关系。
- PIMv6 (Protocol Independent Multicast，协议无关组播)，用于 IPv6 组播路由器或多层交换机之间。为 IPv6 组播提供路由的单播路由协议可以是静态路由、RIPng、OSPFv3 等，组播路由和单播路由协议无关，只要单播路由协议能产生路由表项即可。借助 RPF（Reverse Path Forwarding，逆向路径转发）机制，PIMv6 实现了在网络中传递组播信息。为了描述上的方便，由支持 PIMv6 协议的组播路由器所组成的网络称为 PIMv6 组播域。PIMv6 有两种模式：密集模式和稀疏模式，目前仅支持稀疏模式。

1.2 配置 IPv6 组播路由

1.2.1 使能 IPv6 组播路由

表1-1 使能IPv6组播路由

命令	操作	说明
configure terminal	进入全局配置模式	-
ipv6 multicast-routing	启用交换机的组播路由功能	缺省情况下，IPv6 组播路由功能处于开启状态

1.2.2 配置 IPv6 组播路由的最大数目

当 IPv6 组播路由的最大数目超过阈值时，会生成警告消息，该阈值应小于组播路由的最大数量。

表 1-2 配置 IPv6 组播路由的最大数目

命令	操作	说明
configure terminal	进入全局配置模式	-
ipv6 multicast route-limit *route-number* [*threshold-number*]	配置 IPv6 组播路由的最大数目	IPv6 组播路由最大数目的取值范围为 1~2048；缺省情况下，最大数目为 2048。默认阈值应与组播路由的最大数量相同

1.2.3 配置 IPv6 组播静态路由

表 1-3 配置 IPv6 组播静态路由

命令	操作	说明
configure terminal	进入全局配置模式	-
ipv6 mroute-rpf *source-address/mask-length* [**static** | **ripng** | **ospfv3**] *rpf-nbr-address* [*distance*]	配置 IPv6 组播静态路由	source-address: 组播源地址 mask-length: 掩码长度 rpf-nbr-address: RPF 邻居的 IPv6 地址 distance: 路由优先级，取值范围为 1~255

1.3 显示与维护

表 1-4 显示与维护

命令	操作	说明
show ipv6 mroute [**sparse**] [**count** | **summary**] **show ipv6 mroute** *ipv6-address* [**sparse**] [**count** | **summary**]	显示组播路由表信息	sparse: 查看稀疏模式的组播路由 count: 查看路由和数据包的统计情况 summary: 查看组播路由的总体情况 ipv6-address: 查看 IPv6 源地址或者 IPv6 组播地址的路由
show ipv6 mroute route-limit	查看路由数目的最大值	-
show ipv6 mif [*if-name*]	查看 IPv6 组播的接口信息	if-name: 接口名称
show ipv6 multicast groups count	查看 IPv6 组播组数目	-
show ipv6 mroute-rpf *source-address*	查看组播路由的反向路径查询	source-address: IPv6 组播源地址
show resource mcast6	查看 IPv6 组播路由资源使用情况	-

1.4 配置举例

1.4.3. 配置步骤

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# ipv6 multicast route-limit 1000	配置最大组播限制条目

1.4.4. 命令验证

查看 IPv6 组播路由表：

```
Switch# show ipv6 mroute 2001:1::1234

IPv6 Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry
```

```
Interface State: Interface
2001:1::1234, ff0e::1234:5678
uptime 00:00:31, stat expires 00:03:08
Owner PIM-SMv6, Flags: TF
  Incoming interface: eth-0-1
  Outgoing interface list:
    Register
    eth-0-2
2001:1::1234, ff0e::6666:6666
uptime 00:00:00, stat expires 00:03:30
Owner PIM-SMv6, Flags: TF
  Incoming interface: eth-0-1
  Outgoing interface list:
    Register
```

2 MLD 配置

2.1 MLD 简介

MLD（Multicast Listener Discovery，组播侦听者发现协议）负责 IPv6 组播成员的管理，建立、维护 IPv6 成员主机与其相邻路由器之间的组播组成员关系。参与 IPv6 组播的主机、路由器、多层交换机必须具备 MLD 功能。该协议定义了查询器和主机角色：

- 网络设备的查询器发送查询消息给网络中特定组来发现组播中的成员。
- 主机发送 MLD 报告报文（响应查询报文）来通知查询者主机要加入相应的组播组列表中。
- 一个组播组的成员是动态的，主机可以随时加入和离开。一个组播组成员在位置或数量上没有限制。

2.1.1 MLD 版本

MLD 目前有 MLDv1 和 MLDv2 两种版本。这两个版本均可适用于任意信源组播（ASM），MLDv2 可以直接应用于指定信源组播（SSM）。而 MLDv1 需要通过 MLD SSM Mapping 功能才可以应用于 SSM。

MLDv1：与 IGMPv2 的工作机制相同，通过查询和相应机制管理 IPv6 组播组成员；

MLDv2：在 MLDv1 的基础上增加一些功能，主要功能为成员主机可以指定接收或不接收来自某组播源的报文；

2.1.2 MLD 报文特性

MLD 报文使用下面的组播地址：

- MLD 普通组查询以 ff02::1 为目的地址（在一个子网中的所有系统）。
- MLD 特定组的查询以特定组 IPv6 地址为目的查询。
- MLD 组成员发送 Report 报文给特定的组播 IPv6 地址。
- MLD 版本 1 (MLDv1) 离开组播组时，发送离开消息给 ff02::2。

2.1.3 参考协议

MLD 的版本是基于以下 RFC 定义：

- RFC 2710（定义 MLDv1）
- RFC 3810（定义 MLDv2）

2.2 使能 MLD 功能

MLD 的使能是依赖于组播路由协议的使能，当接口上使能 PIMv6 或者其他组播路由协议，MLD 将会在接口上自动启用，反之亦然。但是请注意，MLD 在工作之前，IPv6 组播路由必须在全局模式启用。系统支持动态学习 MLD 组记录，也可以配置静态 MLD 组记录。

表 2-1 使能 MLD 功能

命令	操作	说明
configure terminal	进入全局配置模式	-
ipv6 multicast-routing	启用交换机的 IPv6 组播路由功能	缺省情况下，IPv6 组播路由功能处于开启状态
interface *if-name*	进入接口配置模式	if-name: 接口名称
no switchport	配置接口为三层接口	-
ipv6 address *ipv6-address/mask-length*	设置 IPv6 地址	ipv6-address: IPv6 地址 mask-length: 掩码长度
ipv6 pim sparse-mode	接口上启用 PIMv6-SM 协议	缺省情况下，未使能 PIMv6-SM 协议

2.3 配置 MLD 基本功能

2.3.1 配置 MLD 版本

表 2-2 配置 MLD 版本

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称

命令	操作	说明
ipv6 mld version *number*	配置端口使用的 MLD 协议的版本	number: 端口所使用的 MLD 协议版本，取值范围为 1~2；缺省情况下，端口使用 MLDv1 版本

2.3.2 配置静态组播(源)组

表 2-3 配置静态组播（源）组

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
ipv6 mld static-group *group-address* [**source** *source-address*]	配置端口上的静态组播组或静态组播源组	group-address: 组播地址 source-address: 组播源地址

2.3.3 配置过滤组播组

使用 IPv6 访问控制列表来控制 MLD 报文的学习，对加入组播组的主机或可以加入的组播组进行限制。

表 2-4 配置过滤组播组

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
ipv6 mld access-group *acl-list*	配置组播组的过滤	acl-list: 访问控制列表名称

2.4 配置 MLD 接口参数

2.4.1 配置 MLD 查询与响应

表 2-5 配置 MLD 查询与响应

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称

命令	操作	说明
ipv6 mld robustness-variable *value*	配置 MLD 查询器的健壮系数	value: MLD 报文的健壮程度，取值范围是 2~7，默认值为 2
ipv6 mld query-interval *interval*	配置端口发送查询报文的时间间隔	interval: 该时间间隔的取值范围为 2~18000，单位：秒；默认值为 125 秒
ipv6 mld last-member-query-interval *interval*	配置 MLD 最后组成员的查询间隔	interval: 该时间间隔的取值范围为 1000~25500，单位：毫秒；默认值为 1000 毫秒
ipv6 mld last-member-query-count *count*	配置 MLD 的最后组成员的查询计数	count: 特定组查询报文的数目，取值范围为 2~7；默认值为 2
ipv6 mld query-max-response-time *interval*	配置 MLD 查询报文的最大响应时间	interval: 最大响应时间的取值范围为 1~25，单位：秒；默认值为 10 秒

2.4.2 配置组播组成员快速离开功能

根据访问控制列表，可配置组播组成员快速离开的功能，快速响应主机的离开组报文。

表 2-6 配置组播组成员快速离开功能

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
ipv6 mld immediate-leave group-list *acl-list*	配置组播组成员快速离开的功能	acl-list: 访问控制列表名称

2.5 配置 MLD SSM Mapping

2.5.1 使能 MLD SSM Mapping 功能

表 2-7 使能 MLD SSM Mapping 功能

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

命令	操作	说明
ipv6 mld ssm-map enable	全局开启 MLD SSM Mapping 功能	缺省情况下，MLD SSM Mapping 功能处于关闭状态

2.5.2 配置 MLD SSM Mapping 规则

表 2-8 配置 MLD SSM Mapping 规则

命令	操作	说明
configure terminal	进入全局配置模式	-
ipv6 mld ssm-map enable	全局开启 MLD SSM Mapping 功能	缺省情况下，MLD SSM Mapping 功能处于关闭状态
ipv6 mld ssm-map static *acl-list source-address*	配置 MLD SSM Mapping 的规则	acl-list: 访问控制列表名称 source-address: 组播源地址 缺省情况下，未配置 MLD SSM Mapping 规则

2.6 配置加入 IPv6 组播组的最大数目

2.6.1 全局配置 IPv6 组播组的最大数目

表 2-9 全局配置 IPv6 组播组的最大数目

命令	操作	说明
configure terminal	进入全局配置模式	-
ipv6 mld limit *number* **except** *acl-list*	全局配置模式下，配置加入 IPv6 组播组的最大数目	number: 全局可加入的组播组的最大个数，默认值为 4096 acl-list: 访问控制列表名称

2.6.2 接口上配置 IPv6 组播组的最大数目

表 2-10 接口配置 IPv6 组播组的最大数目

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称

命令	操作	说明
ipv6 mld limit *number* **except** *acl-list*	接口配置模式下，配置加入 IPv6 组播组的最大数目	number: 全局可加入的组播组的最大个数，默认值为 4096 acl-list: 访问控制列表名称

2.7 配置 MLD 代理

表 2-11 配置 MLD 代理

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
no switchport	配置接口为三层接口	-
ipv6 pim sparse-mode	接口上启用 PIMv6-SM 协议	缺省情况下，未使能 PIMv6-SM 协议
ipv6 mld proxy-service	启用端口的 MLD 代理服务	缺省情况下，MLD 代理服务处于关闭状态
ipv6 mld mroute-proxy *if-name*	配置本端口 MLD 代理的上行端口	if-name: 上行端口名称。一个端口只能设置一个上行代理端口。多次设置时，会覆盖前面的配置

2.8 显示与维护

表 2-12 显示与维护

命令	操作	说明
show ipv6 mld groups [*group-address*] [**detail**]	显示 IPv6 组播组信息	group-address: 指定 IPv6 组播组地址 if-name: 接口名称 *: 所有组播组信息
show ipv6 mld groups *if-name* [*group-address*] [**detail**]	显示端口的 IPv6 组播组信息	
show ipv6 mld groups *if-name* **count**	显示 IPv6 组播组的数量	

命令	操作	说明
show ipv6 mld interface *if-name*	查看 IPv6 组播组端口的信息	
clear ipv6 mld [* | **group** *group-address*]	清除动态学习的 IPv6 组播组信息	
clear ipv6 mld [**group** *group-address* | **interface** *if-name*]	清除指定端口上动态学习的 IPv6 组播组信息	

2.9 配置举例

2.9.1 配置步骤

5. 启用 MLD 功能示例

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# ipv6 multicast-routing	全局模式下启用 IPv6 组播路由
Switch(config)# interface eth-0-1	进入接口 Eth-0-1
Switch(config-if)# no switchport	配置接口为三层接口
Switch(config-if)# ipv6 address 2001:1::1/64	配置 IPv6 地址
Switch(config-if)# ipv6 pim sparse-mode	接口上启用 PIMv6-SM

6. 配置 MLD 接口参数示例

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# ipv6 mld version 2	配置 MLD 版本
Switch(config-if)# ipv6 mld query-interval 120	配置 MLD 查询时间间隔
Switch(config-if)# ipv6 mld query-max-response-time 12	配置 MLD 查询最大响应时间

命令举例	操作步骤
Switch(config-if)# ipv6 mld robustness-variable 3	配置 MLD 查询器的健壮系数
Switch(config-if)# ipv6 mld last-member-query-count 3	配置 MLD 最后组成员查询计数
Switch(config-if)# ipv6 mld last-member-query-interval 2000	配置 MLD 最后组成员查询间隔

7. 配置最大 MLD 组播组数目

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# ipv6 mld limit 2000	配置全局最大 MLD 组播组数目
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# ipv6 mld limit 1000	配置接口下最大 MLD 组播组数目

8. 配置静态 MLD 组播组示例

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# ipv6 mld static-group ff0e::1234	配置静态 MLD 组播组

9. 配置 MLD 代理示例

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# no switchport	设置接口为三层接口
Switch(config-if)# ipv6 pim sparse-mode	在接口上启用 PIMv6-SM
Switch(config-if)# ipv6 mld proxy-service	启用接口为 MLD 代理上游口
Switch(config)# interface eth-0-2	进入接口配置模式
Switch(config-if)# no switchport	设置接口为三层接口
Switch(config-if)# ipv6 pim sparse-mode	接口上启用 PIMv6-SM

命令举例	操作步骤
Switch(config-if)# ipv6 mld mroute-proxy eth-0-1	设置 eth-0-2 为 MLD 代理下游口，MLD 代理上游口为 eth-0-1

2.9.2 命令验证

- 显示MLD接口信息：

```
Switch# show ipv6 mld interface
Interface eth-0-1 (Index 1)
  MLD Active, Querier, Version 1 (default)
  Internet address is fe80::8c8e:dbff:feef:1900
  MLD interface has 0 group-record states
  MLD activity: 0 joins, 0 leaves
  MLD query interval is 125 seconds
  MLD querier timeout is 255 seconds
  MLD max query response time is 10 seconds
  Last member query response interval is 1000 milliseconds
  Group Membership interval is 260 seconds
Interface eth-0-9 (Index 9)
  MLD Active, Querier, Version 1 (default)
  Internet address is fe80::8c8e:dbff:feef:1900
  MLD interface has 0 group-record states
  MLD activity: 0 joins, 0 leaves
  MLD query interval is 125 seconds
  MLD querier timeout is 255 seconds
  MLD max query response time is 10 seconds
  Last member query response interval is 1000 milliseconds
  Group Membership interval is 260 seconds
```

- 显示MLD组播组信息：

```
Switch# show ipv6 mld groups
MLD Connected Group Membership
Group Address                 Interface            Expires
ff0e::1234:5678               eth-0-2              00:03:01
```

3 PIMv6 配置

3.1 PIMv6 简介

发送组播报文时，接收者可能存在于网络中的任意位置。如果静态配置组播路由，可能导致灵活性不足、时效性差等问题。为了更高效、准确地转发组播报文，需要运行组播路由协议。PIMv6 即 IPv6 PIM（IPv6 Protocol Independent Multicast，IPv6 协议无关组播），用于组播路由器或多层交换机中，为 IPv6 组播提供路由的单播路由协议，IPv6 组播路由和单播路由协议无关，只要 IPv6 单播路由协议能产生 IPv6 组播路由表项即可。借助 RPF（Reverse Path Forwarding，逆向路径转发）机制，PIMv6 实现了在网络中传递组播信息。

PIMv6 有两种模式：PIMv6-SM（稀疏模式）和 PIMv6-DM（密集模式）。密集模式主要应用于组成员密集的局域网中，而稀疏模式适用于大型网络。

3.1.1 PIMv6-SM 简介

PIMv6-SM（协议无关组播稀疏模式）是一个组播路由协议，用来将稀疏分散的组播设备联系起来协同工作。这样有助于分散的网络节点节约带宽，通过发送单一流量到多个接收者，达到降低网络流量的目的。

PIMv6-SM 使用接收者发起成员的 IPv6 组播模型，支持共享和最短路径树，并使用软状态机制，以适应不断变化的网络条件。它依赖于单播路由协议来建立和维护路由器间的组播路由。

1. 术语解释

以下是 PIMv6-SM 协议概念的简要描述：

- **汇聚点 (RP)**：RP（Rendezvous Point）在 SM 模式中作为组播的汇聚点，发送者和接收者在 RP 处进行汇聚。对于所有的组播路由器，需要明确每一个组播组与 RP 的对应关系。

  所有的组播数据需要在 RP 上注册，然后所有需要组播数据的接收者通过向 RP 发送 Join 报文来请求数据。

- **组播路由信息库 (MRIB)**：组播路由表是从单播路由表的获得的。在 PIMv6-SM 中，MRIB 是用来决定向何处发送加入/剪枝消息。它还提供了目的网络的路由度量。发送和处理的 Assert 消息时将使用这些度量。
- **反向路径转发 (RPF)**：反向路径转发是指路由器在接受数据包从源 A 通过接口 IF1 时，只有 IF1 是到达源 A 的出接口时才会接受这个包。反向路径转发通过使用单播路由表来决定入端口是否正确。这个数据包将被转发是由于单播路由表表明了接口 IF1 是到达源 A 的最短路径。单播路由表为组播数据选择最短路径。
- **组播树状态信息库 (TIB)**：组播树状态信息库是组播路由器上保存所有组播转发树信息的信息库，通过收到 PIMv6 加入/剪枝消息、Assert 消息和 MLD 消息建立起来。
- **上游 (Upstream)**：朝向树根，树根可能是源或 RP。
- **下游 (Downstream)**：远离树根，树根可能是源或 RP。
- **基于源的树**：基于源的树的转发路径是到达源的最短转发路径，如果单播路由以跳数为度量，基于源的树的转发路径的跳数最小；如果单播路由以延迟为度量，基于源的树的转发路径的延迟最小。

  每个组播源都有一个对应的组播转发树直接将源和接收者连接起来。所有发往指定组的流量沿着对应的转发树进行转发。
- **共享树**：共享树依赖于汇聚点(RP)，所有流量从源都发文至汇聚点，然后汇聚点再将流量发送给接收者。对于每一个组播组来说，不管有多少个源，只有一个转发树。共享树是单向的，流量只会从 RP 流向接收者。如果一个源要发送组播数据，首先 RP 要成功接收发送的组播数据，然后才能从 RP 发送到接收者。
- **自举路由器 (BSR)**：当一个组播源开始发送组播数据或者一个接收者开始发送加入信息到 RP 时，组播路由器必须获取汇聚点的信息。在 PIMv6-SM 网络启动自举路由器后，负责收集网络内的 RP 信息，为每个组选举出 RP，然后将 RP 集（即组-RP 映射数据库）发布到整个 PIMv6-SM 网络。
- **数据流从源到接收者发送 Hello 消息**：PIMv6 路由器定期地发送 Hello 消息来发现 PIMv6 路由器邻居。Hello 消息是组播报文，使用 224.0.0.13 这个地址。PIMv6 路由器对 Hello 消息进行响应，Hello 消息中的 Hold 时间来决定信息的有效时间。
- **选举指定路由器**：在一个多路访问的网络中如果有多个组播路由器，只能有一个组播路由器被选为指定路由器，负责为本地网络的组播接收者往 RP 发送加入/剪枝消息。

- **RP 发现**：PIMv6-SM 通过自举路由器来产生自举消息，然后发布 RP 信息给所有的组播路由器。组播路由器接收和保存自举消息，当 DR 从直连主机收到一个 MLD 报文或组播数据，DR 计算出该组播组的 RP，然后发送加入/剪枝到 RP 或者封装注册报文到 RP。在小型网络环境中可以静态指定 RP。
- **加入共享树**：要加入一个组播组，主机发送一个 MLD 消息给上游路由器，组播路由器向 RP 方向的上游的 PIMv6 邻居发送加入报文。当组播路由器接收到下游设备的加入请求后，检查本地的组播组是否存在。如果存在，说明加入消息被送到共享树，收到消息的接口就会加入至出接口列表；如果不存在，条目将被创建，收到的消息接口被加入到出接口中并再次向 RP 方向上游的 PIMv6 邻居发送加入报文。
- **组播源注册**：与组播源 S 直接相连的路由器接收到该组播报文后，就将该报文封装成 Register 注册报文，并以单播形式发送给对应的 RP。当 RP 接收到来自组播源 S 的注册消息后，一方面解封装注册消息并将组播信息沿着 RPT 树转发到接收者，另一方面朝组播源 S 逐跳发送（S，G）加入消息，从而让 RP 和组播源 S 之间的所有路由器上都生成了（S，G）表项，这些沿途经过的路由器就形成了 SPT 树的一个分支。SPT 源树以组播源 S 为根，以 RP 为目的。组播源 S 发出的组播信息沿着已经建立好的 SPT 树到达 RP，然后由 RP 将信息沿着 RPT 共享树进行转发。
- **发送注册停止消息**：当 RP 从组播源接收到注册报文后也收到未封装的组播报文，将发送注册停止消息给组播源一侧的 DR，当 DR 收到注册停止消息后将不再发送注册消息给 RP。
- **剪枝端口**：接收者侧的组播路由器向 RP 方向上游的 PIMv6 邻居发送剪枝报文，当上联组播路由器收到剪枝报文后，将收到剪枝报文的端口从转发端口中删除，当本路由器上没有其他接收者后会继续向 RP 方向上游的 PIMv6 邻居发送剪枝报文。
- **转发组播数据**：PIMv6-SM 路由器将组播数据发往那些已经明确表示加入组播组的接收者。组播路由器将进行 RPF 检查，只有检查通过的组播数据包才将通过出端口发送出去。

2. 参考协议

与 PIMv6-SM 模块相关的协议规范为：

RFC 4601

3.1.2 PIMv6-DM 简介

PIMv6-DM（协议无关组播密集模式）是一个组播路由协议，用来将密集分布的组播设备联系起来协同工作。

设想当一个组播源开始发送组播流的时候，所有的下游系统都期望接收这个组播流。当组播流泛洪到整个网络时，PIMv6-DM 使用 RPF 来防止组播流的环路。如果某些网络区域没有该组播组的接收成员，PIMv6-DM 会把转发分支通过剪枝来删除掉。

剪枝状态有一个生命周期，当生命周期超时后，组播数据将再一次开始转发，每个(S,G)对应的组播组都有自己的剪枝状态。当某个组播组有新的接收者出现在已经被剪枝的区域里，路由器会通过向组播源发送”graft”消息将剪枝状态转换成转发路径。

1. 参考协议

与 PIMv6-DM 模块相关的协议规范有：

RFC 3973

3.1.3 PIMv6-SSM 简介

PIMv6-SSM 是借助 PIMv6-SM 的部分技术和 MLDv2 来实现的，其建立组播转发树的过程与 PIMv6-SM 创建 SPT 树的过程相似，即接收者 DR 获取组播数据源的具体位置后，直接向组播数据源发送 Join 消息，将组播数据流发送到接收者。

PIMv6-SSM 可以与 PIMv6-SM 在组播路由器上一起工作。

3.2 配置 PIMv6-SM

3.2.1 使能 PIMv6-SM

表3-1 使能PIMv6-SM

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
no shutdown	端口 UP	-
no switchport	配置接口为三层接口	-
ipv6 address *ipv6-address/mask-length*	设置 IPv6 地址	ipv6-address: IPv6 地址 mask-length: 掩码长度
ipv6 pim sparse-mode [**passive**]	接口上启用 PIMv6-SM 协议	缺省情况下，未使能 PIMv6-SM 协议。如选择 **passive** 关键字，

命令	操作	说明
		工作在被动模式的端口不会发送 PIMv6 Hello 报文

3.2.2 配置 RP

1. 配置静态RP

表3-2 配置静态RP地址

命令	操作	说明
configure terminal	进入全局配置模式	-
ipv6 pim rp-address *address* [*acl-list* | **override**]	配置静态 RP 地址	address: RP 地址 acl-list: 访问控制列表

2. 配置动态RP

表3-3 配置候选RP

命令	操作	说明
configure terminal	进入全局配置模式	-
ipv6 pim rp-candidate *if-name* [**priority** *priority-value* | **interval** *interval-value* | **group-list** *acl-list*]	配置候选 RP	if-name: 接口名称，此端口的 IPv6 地址会作为候选的 RP 在网络上被广播 priority-value: 候选 RP 的优先权，取值范围为 0~255 interval-value: 发送宣告报文的时间间隔，取值范围为 1~16383，单位：秒 acl-list: 访问控制列表，限制注册到此 RP 的组播组

3.2.3 配置 BSR

每个组播组需要有一个与之服务的 RP，这个 RP 作为基于组播组的分发树的根。为了组播数据能从发送者到达接收者，在一个组播域内的组播路由器需要使用同样的组播组-RP 的映射。为了选择指定组播组的

RP，组播路由器需要维护一系列的组播组-RP 的映射关系，这被称为 RP 集。BSR（自举路由器）的机制就是用来让在同一个组播域内的组播路由器能够学习到这个 RP 集。

表3-4 配置BSR

命令	操作	说明
configure terminal	进入全局配置模式	-
ipv6 pim bsr-candidate *if-name* [*hash-mask* [*priority-value*]]	配置自举路由器	if-name: 接口名称 hash-mask: RP 选举时候 HASH 的掩码长度，取值范围为 0~32 priority-value: 候选 BSR 路由器的优先级，取值范围为 0~255。默认优先级为 64

3.2.4 配置 IPv6 组播源注册

配置下表的功能可以防止未经认证的用户注册到交换机，例如，可以通过访问控制列表配置注册报文的过滤规则，有利于更好地控制 IPv6 组播组，提高安全性。

表3-5 配置IPv6组播源注册

命令	操作	说明
configure terminal	进入全局配置模式	-
ipv6 pim accept-register list *acl-list*	根据访问控制列表限制 RP 可接受的 PIMv6 注册报文	acl-list: 访问控制列表；使用此功能后，如果一个未经认证的主机发送一个 PIMv6 注册报文给交换机，此交换机会立即发送一个 Stop 报文回去阻止其继续发送报文注册。此命令可以让网络中众多 RP 进行负载分担，通过 ACL 的设置控制不同的组播组
ipv6 pim cisco-register-checksum [**group-list** *acl-list*]	配置 DR 发送注册报文时使用 CISCO Register Checksum	acl-list: 访问控制列表；缺省情况下，使用 RFC 规定的 Register Checksum，如果配置了访问控制列表，只有通过验证的报文才能以 CISCO Register Checksum 的方式发送
ipv6 pim register-rate-limit *limit*	配置 DR 发往 RP 的 PIMv6	limit: 取值范围为 1~65535；缺省情况下，DR 发往 RP 的 PIMv6 注

命令	操作	说明
	注册报文的最大速度	册报文的速度不受限制。如果设定了此项,则超过此速度的 PIMv6 注册报文在 RP 处会被丢弃
ipv6 pim register-suppression *time*	配置 DR 停止发送 PIMv6 注册报文的时间间隔	time: 抑制时间间隔的取值范围为 11~18000，单位：秒，默认值为 60 秒

3.2.5 配置禁止 SPT 切换

表3-6 配置禁止SPT切换

命令	操作	说明
configure terminal	进入全局配置模式	-
ipv6 pim spt-switch-threshold infinity [**group-list** *acl-list*]	配置无法切换至 SPT	acl-list: 访问控制列表；缺省情况下，DR 收到第一个组播流后立即切换为最短路径树

3.3 使能 PIMv6-DM

PIMv6-DM 和 PIMv6-SM 模式在同一个端口上是互斥的。因此，一次只能选择一种模式进行配置。

表3-7 使能PIMv6-DM

命令	操作	说明
configure terminal	进入全局配置模式	-
ipv6 enable	使能 IPv6	缺省情况下，未使能 IPv6
interface *if-name*	进入接口配置模式	if-name: 接口名称
no shutdown	端口 UP	-
no switchport	配置接口为三层接口	-
ipv6 address *ipv6-address/mask-length*	设置 IPv6 地址	ipv6-address: IPv6 地址 mask-length: 掩码长度
ipv6 pim dense-mode [**passive**]	接口上启用 PIMv6-DM 协议	缺省情况下，未使能 PIMv6-DM 协议。如选择 **passive** 关键字，工作在被动模式的端口不会发

命令	操作	说明
		送 PIMv6 Hello 报文

3.4 使能 PIMv6-SSM

表 3-8 使能 PIMv6-SSM

命令	操作	说明
configure terminal	进入全局配置模式	-
ipv6 pim ssm [**default** | **range** *list*]	使能 PIMv6-SSM	default: 使用默认的 SSM 组播组范围 list: 使用访问控制列表中的组播组范围作为 SSM IPv6 组播组范围。缺省情况下，未使能 PIMv6-SSM

3.5 显示与维护

表 3-9 显示与维护

命令	操作	说明
show ipv6 pim sparse-mode bsr-router	查看自举路由器信息	-
show ipv6 pim sparse-mode interface [**detail**]	查看稀疏模式下的端口信息	-
show ipv6 pim sparse-mode local-member [*if-name*]	查看稀疏模式下的本地成员信息	if-name: 接口名称
show ipv6 pim sparse-mode mroute [*source-address* | *group-address*] [**detail**]	查看稀疏模式下的 IPv6 组播路由	source-address: IPv6 组播路由源地址 group-address: IPv6 组播路由目的地址
show ipv6 pim sparse-mode neighbor	查看稀疏模式下的邻居信息	-

命令	操作	说明
show ipv6 pim sparse-mode rp mapping	查看 IPv6 组播组与 RP 的对应关系	-
show ipv6 pim sparse-mode rp-hash *group-address*	查看指定 IPv6 组播组的 RP 信息	group-address: IPv6 组播组地址
show ipv6 pim sparse-mode spt-threshold	查看从共享树切换为最短路径树的阈值	-
show ipv6 pim dense-mode interface [**detail**]	查看 PIMv6-DM 的接口信息	-
show ipv6 pim dense-mode mroute	查看 PIMv6-DM 的组播路由表	-
show ipv6 pim dense-mode neighbor [**detail**]	查看 PIMv6-DM 的邻居	-

3.6 配置举例

3.6.1 配置 PIMv6-SM 示例

1.配置静态 RP

i. 介绍

PIMv6-SM 是一个软状态协议。通过静态或动态的方法在所需的接口上启用 PIMv6-SM 协议，并正确配置的 RP 信息。所有组播组的 MLD 报告/离开和 PIMv6 加入/剪枝消息保持动态。目前，只支持一个 RP 上所有的组播组（ff00::/8）。

ii. 拓扑

图 3-1 PIMv6-SM 配置拓扑图

iii. 配置步骤

以上例子中 R1 是 RP，所有的路由器都配置静态 RP：

- 每个路由器配置静态 RP 地址 2001:1::1。
- 所有接口上必须启用 PIMv6-SM 功能。

R1 的配置如下：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# no shutdown	打开接口
Switch(config-if)# no switchport	设置接口为三层接口
Switch(config-if)# ipv6 address 2001:1::1/64	配置 IPv6 地址
Switch(config-if)# ipv6 pim sparse-mode	在接口上启用 PIMv6-SM
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface eth-0-9	进入接口配置模式
Switch(config-if)# no shutdown	打开接口
Switch(config-if)# no switchport	设置接口为三层接口
Switch(config-if)# ipv6 address 2001:9::1/64	配置 IPv6 地址
Switch(config-if)# ipv6 pim sparse-mode	在接口上启用 PIMv6-SM
Switch(config-if)# exit	退出接口配置模式
Switch(config)# ipv6 route 2001:2::/64 2001:9::2	配置静态单播路由
Switch(config)# ipv6 pim rp-address 2001:1::1	配置静态 RP 地址

R2 的配置如下：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# no shutdown	打开接口
Switch(config-if)# no switchport	设置接口为三层接口

命令举例	操作步骤
Switch(config-if)# ipv6 address 2001:2::1/64	配置 IPv6 地址
Switch(config-if)# ipv6 pim sparse-mode	在接口上启用 PIMv6-SM
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface eth-0-9	进入接口配置模式
Switch(config-if)# no shutdown	打开接口
Switch(config-if)# no switchport	设置接口为三层接口
Switch(config-if)# ipv6 address 2001:9::2/64	配置 IPv6 地址
Switch(config-if)# ipv6 pim sparse-mode	在接口上启用 PIMv6-SM
Switch(config-if)# exit	退出接口配置模式
Switch(config)# ipv6 route 2001:1::/64 2001:9::1	配置静态单播路由
Switch(config)# ipv6 pim rp-address 2001:1::1	配置静态 RP 地址

iv. 命令验证

所有的路由器配置使用相同的 RP 地址 2001:1::1，使用以下命令来验证 RP 的配置、接口的详细信息和组播路由表。

- 在R1上显示PIMv6稀疏模式RP映射的命令，表明2001:1::1是对所有组播组ff00::/8静态配置的RP。所有其他路由器都会有类似的输出：

```
R1# show ipv6 pim sparse-mode rp mapping

PIM Group-to-RP Mappings
Group(s): ff00::/8, Static
      RP: 2001:1::1
            Uptime: 00:00:04
Embedded RP Groups:
```

- 显示R1接口的组播信息：

```
R1# show ipv6 pim sparse-mode interface

Interface       VIFindex Ver/      Nbr       DR
                         Mode      Count     Prior
eth-0-1         2        v2/S      0         1
```

```
        Address           : fe80::fc94:efff:fe96:2600
        Global Address: 2001:1::1
        DR                  : this system
eth-0-9         0           v2/S    0         1
        Address           : fe80::fc94:efff:fe96:2600
        Global Address: 2001:9::1
        DR                  : this system
```

- 显示PIMv6-SM的组播路由表：

```
R1# show ipv6 pim sparse-mode mroute detail

IPv6 Multicast Routing Table
(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 0
(S,G,rpt) Entries: 0
FCR Entries: 0
*, ff0e::1234:5678
Type: (*,G)
Uptime: 00:01:37
   RP: 2001:1::1, RPF nbr: None, RPF idx: None
   Upstream:
    State: JOINED, SPT Switch: Enabled, JT: off
    Macro state: Join Desired,
   Downstream:
    eth-0-1:
       State: NO INFO, ET: off, PPT: off
       Assert State: NO INFO, AT: off
         Winner: ::, Metric: 4294967295, Pref: 4294967295, RPT bit: on
       Macro state: Could Assert, Assert Track
   Local Olist:
    eth-0-1

R2# show ipv6 pim sparse-mode mroute detail

IPv6 Multicast Routing Table
(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 0
(S,G,rpt) Entries: 0
FCR Entries: 0
*, ff0e::1234:5678
Type: (*,G)
Uptime: 00:00:06
   RP: 2001:1::1, RPF nbr: None, RPF idx: None
   Upstream:
    State: JOINED, SPT Switch: Enabled, JT: off
    Macro state: Join Desired,
```

```
Downstream:
  eth-0-1:
     State: NO INFO, ET: off, PPT: off
     Assert State: NO INFO, AT: off
       Winner: ::, Metric: 4294967295, Pref: 4294967295, RPT bit: on
     Macro state: Could Assert, Assert Track
Local Olist:
  eth-0-1
```

2.配置动态 RP

i. 介绍

在小型并且简单的网络中，组播信息量少，全网络仅依靠一个 RP 进行信息转发即可，此时可以在 SM 域中各路由器上静态指定 RP 位置。但是，通常情况下，PIMv6-SM 网络规模都比较大，通过 RP 转发的组播信息量也较多。为了缓解 RP 负担的同时优化共享树的拓扑结构，不同组播组应对应不同的 RP，此时就需要自举机制来动态选举 RP。

R1 的配置如下：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# no shutdown	打开接口
Switch(config-if)# no switchport	设置接口为三层接口
Switch(config-if)# ipv6 address 2001:1::1/64	配置 IPv6 地址
Switch(config-if)# ipv6 pim sparse-mode	在接口上启用 PIMv6-SM
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface eth-0-9	进入接口配置模式
Switch(config-if)# no shutdown	打开接口
Switch(config-if)# no switchport	设置接口为三层接口
Switch(config-if)# ipv6 address 2001:9::1/64	配置 IPv6 地址
Switch(config-if)# ipv6 pim sparse-mode	在接口上启用 PIMv6-SM

命令举例	操作步骤
Switch(config-if)# exit	退出接口配置模式
Switch(config)# ipv6 route 2001:1::/64 2001:9::1	配置静态单播路由
Switch(config)# ipv6 pim rp-candidate eth-0-1	配置候选 RP 接口

R2 的配置如下：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# no shutdown	打开接口
Switch(config-if)# no switchport	设置接口为三层接口
Switch(config-if)# ipv6 address 2001:2::1/64	配置 IPv6 地址
Switch(config-if)# ipv6 pim sparse-mode	在接口上启用 PIMv6-SM
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface eth-0-9	进入接口配置模式
Switch(config-if)# no shutdown	打开接口
Switch(config-if)# no switchport	设置接口为三层接口
Switch(config-if)# ipv6 address 2001:9::2/64	配置 IPv6 地址
Switch(config-if)# ipv6 pim sparse-mode	在接口上启用 PIMv6-SM
Switch(config-if)# exit	退出接口配置模式
Switch(config)# ipv6 route 2001:1::/64 2001:9::1	配置静态单播路由
Switch(config)# ipv6 pim rp-candidate eth-0-9	配置候选 RP 接口
Switch(config)# ipv6 pim bsr-candidate eth-0-9	配置候选 BSR 接口

说明

一般选择最高优先级的路由器为 RP。如果有两个或多个路由器的优先级相同，会运用 BSR 机制中的哈希函数选择 RP，以确保在 PIMv6 域的所有路由器对应同一组的 RP。使用 **ipv6 pim rp-candidate** *if-name* **priority** *priority-value* 命令来改变候选 RP 的默认优先级。

ii. 命令验证

使用 **show ipv6 pim sparse-mode rp mapping** 命令显示组-RP 映射的详细信息，输出内容是候选 RP 信息。对应该范围 ff00::/8 的组有两个候选 RP。候选 RP 2001:1::1 默认的优先级 192，而候选 RP 2001:9::2 的优先级为 2。由于候选 RP 2001:1::1 由于具有更高的优先权，它被选中作为组播组 ff00::/8 的 RP。

```
R2# show ipv6 pim sparse-mode rp mapping

PIM Group-to-RP Mappings
This system is the Bootstrap Router (v2)
Group(s): ff00::/8
   RP: 2001:9::2
      Info source: 2001:9::2, via bootstrap, priority 2
            Uptime: 00:00:32, expires: 00:02:02
   RP: 2001:1::1
      Info source: 2001:1::1, via bootstrap, priority 192
            Uptime: 00:00:31, expires: 00:02:03
Embedded RP Groups:
```

使用下面的命令显示特定组的 RP 路由器的信息。此输出显示已选择 2001:9::2 为组播组 ff02::1234 的 RP。

```
R2# show ipv6 pim sparse-mode rp-hash ff02::1234

      RP: 2001:9::2
      Info source: 2001:9::2, via bootstrap
```

RP 信息达到域中的所有 PIM 路由器后，各状态机保持所有路由从组成员的加入/剪枝的结果。若需显示接口的详细信息和组播路由表的信息，请参见配置静态 RP 的部分。

3.6.2 配置自举路由器示例

i. 介绍

BSR 是 PIMv6-SM 网络里的管理核心，主要负责以下内容：

- 收集网络中 Candidate-RP（C-RP）发来的 Advertisement 宣告信息。

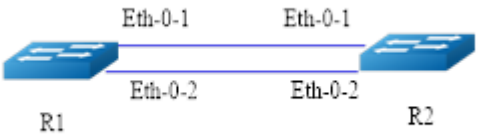
- 为每个组播组选择部分 C-RP 信息以组成 RP-Set 集（即组播组和 RP 的映射数据库）。
- 发布到整个 PIMv6-SM 网络，从而使网络内的所有路由器（包括 DR）都会定位 RP 的位置。

在一个 PIMv6 域中，需要配置一个或多个候选 BSR，候选 BSR 之间通过自动选举，产生自举路由器 BSR，负责收集并发布 RP 信息。下面简单描述一下候选 BSR 之间的自动选举：

- 在将路由器配置为候选 BSR 时，必须同时指定一个启动了 PIMv6-SM 的接口。
- 每个候选 BSR 开始都以自身作为本 PIMv6-SM 的 BSR，并使用这个接口的 IPv6 地址作为 BSR 地址，发送自举报文。
- 当候选 BSR 收到其它路由器发来的自举报文时，它将新收到的自举报文的 BSR 地址与自己的 BSR 地址进行比较，比较标准包括优先级和 IPv6 地址，优先级相同的情况下，优先选择拥有较大的 IPv6 地址的报文。如果前者优先级更高或 IPv6 地址更大，则将这个新的 BSR 地址替换自己的 BSR 地址，并且不再作为自己的 BSR。否则，保留自己的 BSR 地址，继续将自己视为 BSR。
- 备选 RP 将自己的 RP 信息报告给自举路由器，然后自举路由器将汇聚的 RP 集通过自举报文发布到整个组播域的路由器。

ii. 拓扑

图 3-2 BSR 配置拓扑图



iii. 配置步骤

R1 的配置如下：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# ipv6 pim bsr-candidate eth-0-1	指定 BSR 的候选接口（默认优先级 64）

R2 的配置如下：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# ipv6 pim bsr-candidate eth-0-1 10 25	配置 HASH 掩码长度为 10、优先级为 25 的 BSR 候选接口
Switch(config)# ipv6 pim rp-candidate eth-0-1 priority 0	配置优先级为 0 的 RP 候选接口

通过命令 **ipv6 pim unicast-bsm** 配置接口以单播方式发送和接收 BSM 消息。

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# interface eth-0-1	进入接口配置模式
Switch(config-if)# ipv6 pim dr-priority 10	配置接口 DR 的优先级
Switch(config-if)# ipv6 pim unicast-bsm	配置接口以单播方式发送和接收 BSM 消息

iv. 命令验证

1.检查候选 BSR 的信息：

```
Switch# show ipv6 pim sparse-mode bsr-router

PIM6v2 Bootstrap information
This system is the Bootstrap Router (BSR)
  BSR address: 2001:9::1 (?)
  Uptime:          00:01:27, BSR Priority: 64, Hash mask length: 126
  Next bootstrap message in 00:00:16
  Role: Candidate BSR
  State: Elected BSR

Switch# show ipv6 pim sparse-mode bsr-router
PIM6v2 Bootstrap information
  BSR address: 2001:9::1 (?)
  Uptime:          00:01:34, BSR Priority: 64, Hash mask length: 126
  Expires:         00:01:51
  Role: Candidate BSR
  State: Candidate BSR
  Candidate RP: 2001:9::2(eth-0-9)
    Advertisement interval 60 seconds
    Next C-RP advertisement in 00:00:35
```

2.在 E-BSR 上检查 RP:

```
Switch# show ipv6 pim sparse-mode rp mapping
PIM Group-to-RP Mappings
This system is the Bootstrap Router (v2)
Group(s): ff00::/8
   RP: 2001:9::2
      Info source: 2001:9::2, via bootstrap, priority 0
            Uptime: 00:45:37, expires: 00:02:29
Embedded RP Groups:
```

3.在 C-BSR 上检查 RP:

```
Switch# show ipv6 pim sparse-mode rp mapping

PIM Group-to-RP Mappings
Group(s): ff00::/8
   RP: 2001:9::2
      Info source: 2001:9::1, via bootstrap, priority 0
            Uptime: 00:03:14, expires: 00:01:51
Embedded RP Groups:
```

3.6.3 配置 PIMv6-DM 示例

i. 介绍

PIMv6-DM 是一个软状态协议。在所需的接口上启用 PIMv6-DM 协议。所有组播组的状态通过 MLD 报告/离开和 PIMv6 消息来动态的维护。如下图 7-5，组播流从 R1 的 eth-0-1 口进来，接收者来与 R2 的 eth-0-1 相连。

ii. 拓扑

图 3-3 PIMv6-DM 配置拓扑图

iii. 配置方法

R1 的配置如下：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# ipv6 enable	使能 IPv6
Switch(config)# interface eth-0-1	进入 eth-0-1 的接口配置模式
Switch(config-if)# no shutdown	启用端口
Switch(config-if)# no switchport	设置接口为三层接口
Switch(config-if)# ipv6 address 2001:1::1/64	配置接口的 IPv6 地址
Switch(config-if)# ipv6 pim dense-mode	使能接口的 PIMv6 DM 功能
Switch(config-if)# exit	退出接口配置模式
Switch(config)# interface eth-0-9	进入 eth-0-9 的接口配置模式
Switch(config-if)# no shutdown	启用端口
Switch(config-if)# no switchport	设置接口为三层接口
Switch(config-if)# ipv6 address 2001:2::1/64	配置接口的 IPv6 地址
Switch(config-if)# ipv6 pim dense-mode	使能接口的 PIMv6 DM 功能
Switch(config-if)# exit	退出接口配置模式
Switch(config)# ipv6 route 2001:3::/64 2001:2::2	配置一条静态路由

R2 的配置如下：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# ipv6 enable	使能 IPv6
Switch(config)# interface eth-0-1	进入 eth-0-1 的接口配置模式
Switch(config-if)# no shutdown	启用端口
Switch(config-if)# no switchport	设置接口为三层接口
Switch(config-if)# ipv6 address 2001:3::1/64	配置接口的 IPv6 地址
Switch(config-if)# ipv6 pim dense-mode	使能接口的 PIMv6 DM 功能
Switch(config-if)# exit	退出接口配置模式

命令举例	操作步骤
Switch(config)# interface eth-0-9	进入 eth-0-9 的接口配置模式
Switch(config-if)# no shutdown	启用端口
Switch(config-if)# no switchport	设置接口为三层接口
Switch(config-if)# ipv6 address 2001:2::2/64	配置接口的 IPv6 地址
Switch(config-if)# ipv6 pim dense-mode	使能接口的 PIMv6 DM 功能
Switch(config-if)# exit	退出接口配置模式
Switch(config)# ipv6 route 2001:1::/64 2001:2::1	配置一条静态路由

iv. 命令验证

1. 显示 R1 上接口的详细信息：

```
R1# show ipv6 pim dense-mode interface
Neighbor Address                Interface     VIFIndex Ver/     Nbr
                                                       Mode      Count
fe80::326f:c9ff:fef2:8200       eth-0-1       0        v2/D     0
fe80::326f:c9ff:fef2:8200       eth-0-9       2        v2/D     1
```

2. 显示 R1 上邻居的详细信息：

```
R1# show ipv6 pim dense-mode neighbor
Neighbor Address                Interface     Uptime/Expires     Ver
fe80::ce47:6eff:feb7:1400       eth-0-9       00:51:51/00:01:24 v2
```

3. 显示 R1 上 PIMv6-DM 组播路由表的信息：

```
R1# show ipv6 pim dense-mode mroute

PIM-DM Multicast Routing Table
(2001:1::2, ff0e::1)
   Source directly connected on eth-0-1
   State-Refresh Originator State: Originator
   Upstream IF: eth-0-1
      Upstream State: Forwarding
      Assert State: NoInfo
   Downstream IF List:
      eth-0-9, in 'olist':
```

```
        Downstream State: NoInfo
        Assert State: NoInfo
```

4. 显示 R2 上 PIMv6-DM 组播路由表的信息：

```
R2# show ipv6 pim dense-mode mroute

PIM-DM Multicast Routing Table
(2001:1::2, ff0e::1)
  RPF Neighbor: none
  Upstream IF: eth-0-9
    Upstream State: AckPending
    Assert State: Loser
  Downstream IF List:
    eth-0-1, in 'olist':
      Downstream State: NoInfo
      Assert State: NoInfo
```

4 MLD Snooping 配置

4.1 MLD Snooping 简介

MLD Snooping（Multicast Listener Discovery Snooping）即组播侦听者发现协议窥探，是运行在二层以太网交换机上的 IPv6 组播约束机制，用于管理和控制 IPv6 组播组。

二层交换机通过 MLD Snooping 来控制 IPv6 组播流量的泛洪。当二层以太网交换收到主机和路由器之间传递的 MLD 报文时，MLD Snooping 将对 MLD 报文所带的信息进行分析，将端口和 MAC 组播地址建立起映射关系，并根据这样的映射关系转发 IPv6 组播数据。IPv6 组播路由器定期发送通用组查询维护 IPv6 组播组成员关系。所有接收者将发送 MLD 报告报文响应这个查询，交换机通过这个监听 MLD 报告报文建立转发表项。

二层的组播组可以通过 MLD 报文动态建立，也可以静态配置。静态配置的组播组将覆盖动态学的组播组。

说明

VRRP、RIPng、OSPFv3 等协议使用了组播 IPv6 地址，因此在使能了 MLD Snooping 的网络中，要避免使用这样的组播 IPv6 地址，它们映射出来的 MAC 地址和协议模块使用的组播 IPv6 地址映射出来的 MAC 地址一致。例如：

VRRP 使用了 ff02::12，在 MLD Snooping 和 VRRP 网络中，避免使用组播 MAC 地址 3333.0000.0012 映射出的组播 IPv6 地址；

RIPv6 使用了 ff02::9，在 MLD Snooping 和 RIPng 网络中，避免使用组播 MAC 地址 3333.0000.0009 映射出的组播 IPv6 地址；

OSPFv3 使用了 ff02::5，在 MLD Snooping 和 OSPFv3 网络中，避免使用组播 MAC 地址 3333.0000.0005 映射出的组播 IPv6 地址。

4.2 配置 MLD Snooping 基本功能

4.2.1 使能 MLD Snooping

用户可以在全局模式下或者单 VLAN 模式下启用 MLD Snooping 功能。如果在全局模式下关闭 MLD Snooping 功能，即使在单 VLAN 模式下启用 MLD Snooping 也是无效的。如果在全局模式下开启该功能，可以在某个 VLAN 下关闭 MLD Snooping。全局配置可以覆盖单 VLAN 配置。

表 4-1 使能 MLD Snooping

命令	操作	说明
configure terminal	进入全局配置模式	-
ipv6 mld snooping [**vlan** *vlan-id*]	全局模式或单 VLAN 模式下开启 MLD Snooping 功能	vlan-id: VLAN ID 的取值范围为 1~4094 默认情况下，MLD Snooping 在全局模式下和每个 VLAN 上使能

4.2.2 配置 MLD Snooping 版本

表 4-2 配置 MLD Snooping 版本

命令	操作	说明
configure terminal	进入全局配置模式	-
ipv6 mld snooping [**vlan** *vlan-id*] **version** *version-number*	配置 MLD Snooping 运行版本	vlan-id: VLAN ID 的取值范围为 1~4094 version-number: MLD Snooping 版本号，取值范围为 1~2；默认值为 1

4.3 配置 MLD Snooping 组播路由端口

组播路由端口是交换机上连接到组播路由器的端口，可以动态学习或者静态配置。当某个 VLAN 的端口上收到 MLD 通用组查询报文或者是 PIMv6 Hello 报文，该端口成为这个 VLAN 的组播路由端口。所有从组播路由端口上收到的 MLD 查询报文要在所属 VLAN 内广播。所有 VLAN 上收到 MLD 报告/离

开报文也将从组播路由端口转发（报文抑制关闭的情况下），另外所有从该 VLAN 上收到的组播流量将从组播路由端口转发。

4.3.1 配置动态 IPv6 组播路由端口老化时间

表 4-3 配置动态 IPv6 组播路由端口老化时间

命令	操作	说明
configure terminal	进入全局配置模式	-
ipv6 mld snooping vlan *vlan-id* **mrouter-aging-interval** *interval-value*	配置 VLAN 上的动态 IPv6 组播路由端口的老化时间间隔	vlan-id: VLAN ID 的取值范围为 1~4094 interval-value: 老化时间间隔，取值范围为 1~65535，单位：秒；默认值为 255 秒

4.3.2 配置静态成员端口

交换机在二层端口上收到 MLD 报文时会建立 MLD Snooping 的组记录。目前系统也支持静态配置 MLD Snooping 的组记录，在静态配置时需要指定组地址、二层端口以及二层端口所属的 VLAN。

表 4-4 配置静态成员端口

命令	操作	说明
configure terminal	进入全局配置模式	-
ipv6 mld snooping vlan *vlan-id* **static-group** *group-address* [**source** *source-address*] **interface** *if-name*	配置 VLAN 的成员端口加入 IPv6 组播组或组播源组	vlan-id: VLAN ID 的取值范围为 1~4094 group-address: IPv6 组播组地址 source-address: IPv6 组播源地址 if-name: VLAN 的成员端口名称

4.3.3 配置静态组播路由端口

表 4-5 配置静态组播路由端口

命令	操作	说明
configure terminal	进入全局配置模式	-
ipv6 mld snooping vlan *vlan-id* **mrouter interface** *if-name*	配置 VLAN 上的静态组播路由端口	vlan-id: VLAN ID 的取值范围为 1~4094 if-name: 接口名称

4.3.4 配置 MLD Snooping 快速离开功能

正常情况下，MLD Snooping 在接收到 MLD 离开报文后不会直接将端口从组播组中删除，而是发送 MLD 特定组查询报文，如果等待一段时间后没有得到响应，才会将该端口从组播组中删除。启动快速删除功能后，MLD Snooping 收到 MLD 离开报文时，直接将端口从组播组中删除。当端口下只有一个用户时，快速删除可以节省带宽。

表 4-6 配置 MLD Snooping 快速离开功能

命令	操作	说明
configure terminal	进入全局配置模式	-
ipv6 mld snooping [**vlan** *vlan-id*] **fast-leave**	配置 MLD Snooping 快速离开功能	vlan-id: VLAN ID 的取值范围为 1~4094 缺省情况下，MLD Snooping 快速离开功能处于关闭状态

4.4 配置 MLD Snooping 查询参数

三层交换机在所连接的网段上周期性地发送 MLD 通用查询报文，通过解析返回的 MLD 主机报告报文，获知该网段内的组播组成员信息。组播路由器周期性地发送查询报文，当得到某一组成员的 MLD 主机报告报文的时候，刷新该网段相应的组成员关系信息。

4.4.1 配置 MLD 查询与响应

表 4-7 配置 MLD 查询与响应

命令	操作	说明
configure terminal	进入全局配置模式	-
ipv6 mld snooping [**vlan** *vlan-id*] **query-interval** *interval-value*	配置 MLD 通用查询报文发送的时间间隔	vlan-id: VLAN ID 的取值范围为 1~4094 interval-value: 查询间隔的取值范围为 2~18000；默认值为 125 秒。 查询的间隔时间不能小于 MLD Snooping 查询最大的响应时间
ipv6 mld snooping [**vlan** *vlan-id*] **query-max-response-time** *time*	配置等待查询应答报文的超时时间	vlan-id: VLAN ID 的取值范围为 1~4094 time: 超时时间的取值范围为 1~25，单位：秒；默认值为 10 秒
ipv6 mld snooping [**vlan** *vlan-id*] l**ast-member-query-interval** *interval-value*	配置最后成员查询报文的时间间隔	vlan-id: VLAN ID 的取值范围为 1~4094 interval-value: 查询间隔的范围为 1000~25500，单位：毫秒；默认值为 1000 毫秒

4.4.2 配置 MLD 查询器

表 4-8 配置 MLD 查询器

命令	操作	说明
configure terminal	进入全局配置模式	-
ipv6 mld snooping vlan *vlan-id* **querier address** *source-address*	配置 VLAN 上 IPv6 组播查询器的源地址	vlan-id: VLAN ID 的取值范围为 1~4094 source-address: IPv6 组播查询器源地址
ipv6 mld snooping vlan *vlan-id* **querier**	使能 VLAN 上的 IPv6 组播查询器功能	vlan-id: VLAN ID 的取值范围为 1~4094

命令	操作	说明
		缺省情况下，IPv6 组播查询器功能处于关闭状态
ipv6 mld snooping vlan *vlan-id* **querier-timeout** *interval-value*	配置 VLAN 上查询器老化时间	vlan-id: VLAN ID 的取值范围为 1~4094 interval-value: 查询器老化时间间隔，取值范围为 60~300，单位：秒；默认值为 255 秒

4.4.3 配置查询器源 IPv6 地址

表 4-9 配置查询器源 IPv6 地址

命令	操作	说明
configure terminal	进入全局配置模式	-
ipv6 mld snooping global source-address *source-address*	配置 MLD Snooping 查询器源地址	source-address: 查询器源 IPv6 地址

4.4.4 配置 TCN 查询参数

用户可以通过配置 TCN 的时间间隔以及查询次数来适应 STP 收敛拓扑后的组播组学习以及更新。

表 4-10 配置 TCN 查询参数

命令	操作	说明
configure terminal	进入全局配置模式	-
ipv6 mld snooping querier tcn { **query-count** *count* | **query-interval** *interval-value* }	配置 MLD Snooping TCN 查询参数	count: TCN 查询次数，取值范围为 1~10，默认值为 2 秒 interval-value: TCN 查询间隔，取值范围为 1~255，单位：秒；默认值为 10 秒

4.5 配置 IPv6 组播组控制规则

4.5.1 配置 IPv6 组播组过滤

表 4-11 配置 IPv6 组播组过滤

命令	操作	说明
configure terminal	进入全局配置模式	-
ipv6 mld snooping vlan *vlan-id* **access-group** *acl-list*	配置允许加入的 IPv6 组播组范围	vlan-id: VLAN ID 的取值范围为 1~4094 acl-list: 访问控制列表名称

4.5.2 配置丢弃未知 IPv6 组播流量

表 4-12 配置丢弃未知 IPv6 组播流量

命令	操作	说明
configure terminal	进入全局配置模式	-
ipv6 mld snooping [**vlan** *vlan-id*] **discard-unknown**	配置丢弃未知的 IPv6 组播流量	vlan-id: VLAN ID 的取值范围为 1~4094 缺省情况下，未知 IPv6 组播流量在 VLAN 内泛洪

4.5.3 配置报告报文抑制

交换机使用 MLD 报告报文抑制功能，抑制重复发送同一个 MLD 报文至组播路由器。当 MLD 路由器抑制使能时（默认），交换机将第一个 MLD 报告报文发送给组播路由器，其余相同的 MLD 报告报文将不再发送给组播路由器。

表 4-13 配置报告报文抑制

命令	操作	说明
configure terminal	进入全局配置模式	-
ipv6 mld snooping [**vlan** *vlan-id*] **report-suppression**	配置设置端口对 MLDv1/v2 的成员报告报文进行抑制	vlan-id: VLAN ID 的取值范围为 1~4094

命令	操作	说明
		缺省情况下，报告报文抑制功能处于开启状态； MLD Snooping 在 V2 模式工作时，成员报告报文不进行抑制

4.6 显示与维护

表 4-14 显示与维护

命令	操作	说明
show ipv6 mld snooping global	查看 MLD Snooping 的全局配置	-
show ipv6 mld snooping groups	显示 MLD Snooping 组播组信息	-
show ipv6 mld snooping groups vlan *vlan-id* [*group-address*]	显示指定 VLAN 上的 IPv6 组播组信息	vlan-id: VLAN ID 的取值范围为 1~4094 group-address: IPv6 组播组地址
show ipv6 mld snooping groups vlan *vlan-id* **count**	显示 MLD Snooping 组播组数目	vlan-id: VLAN ID 的取值范围为 1~4094
show ipv6 mld snooping querier [**vlan** *vlan-id*]	显示 MLD Snooping 查询器相关信息	
show ipv6 mld snooping mrouter [**vlan** *vlan-id*]	显示 IPv6 组播路由端口信息	
show ipv6 mld snooping vlan *vlan-id*	显示 VLAN 上的 MLD Snooping 信息	
show resource l2mcast	显示二层组播资源使用情况	-
clear ipv6 mld snooping group *	删除所有的 MLD Snooping 组信息	*****: 所有组信息

命令	操作	说明
clear ipv6 mld snooping vlan *vlan-id*	删除指定 VLAN 上的组播组信息	vlan-id: VLAN ID 的取值范围为 1~4094

4.7 配置举例

4.7.1 配置启用 MLD Snooping 示例

i. 配置步骤

命令举例	操作步骤
Switch#configure terminal	进入全局配置模式
Switch(config)# ipv6 mld snooping	全局模式下启用 MLD Snooping
Switch(config)#ipv6 mld snooping vlan 1	在单 VLAN 模式下启用 MLD Snooping

ii. 命令验证

显示 VLAN 1 上 MLD Snooping 的信息：

```
Switch # show ipv6 mld snooping vlan 1

Global Mld Snooping Configuration
------------------------------------------------
Mld Snooping                                :Enabled
Mld Snooping Fast-Leave                     :Disabled
Mld Snooping Version                        :1
Mld Snooping Max-Member-Number              :4096
Mld Snooping Unknown Multicast Behavior     :Flood
Mld Snooping Report-Suppression             :Enabled
Vlan 1
-----------
Mld Snooping                                :Enabled
Mld Snooping Fast-Leave                     :Disabled
Mld Snooping Report-Suppression             :Enabled
Mld Snooping Version                        :1
Mld Snooping Max-Member-Number              :4096
Mld Snooping Unknown Multicast Behavior     :Flood
Mld Snooping Group Access-list              :N/A
Mld Snooping Mrouter Port                   :
Mld Snooping Mrouter Port Aging Interval(sec) :255
```

4.7.2 配置 MLD Snooping 快速离开示例

i. 配置步骤

命令举例	操作步骤
Switch#configure terminal	进入全局配置模式
Switch(config)#ipv6 mld snooping fast-leave	全局模式下启用快速离开功能
Switch(config)#ipv6 mld snooping vlan 1 fast-leave	在 VLAN 模式下启用快速离开功能

ii. 命令验证

显示 VLAN 1 上 MLD Snooping 的信息：

```
Switch # show ipv6 mld snooping vlan 1
Global Mld Snooping Configuration
------------------------------------------------
Mld Snooping                                :Enabled
Mld Snooping Fast-Leave                     :Enabled
Mld Snooping Version                        :1
Mld Snooping Max-Member-Number              :4096
Mld Snooping Unknown Multicast Behavior     :Flood
Mld Snooping Report-Suppression             :Enabled
Vlan 1
----------
Mld Snooping                                :Enabled
Mld Snooping Fast-Leave                     :Enabled
Mld Snooping Report-Suppression             :Enabled
Mld Snooping Version                        :1
Mld Snooping Max-Member-Number              :4096
Mld Snooping Unknown Multicast Behavior     :Flood
Mld Snooping Group Access-list              :N/A
Mld Snooping Mrouter Port                   :
Mld Snooping Mrouter Port Aging Interval(sec) :255
```

4.7.3 配置 MLD Snooping 组播路由端口示例

i. 配置步骤

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# ipv6 mld snooping report-suppression	启用 MLD Snooping 的报告抑制功能

命令举例	操作步骤
Switch(config)# ipv6 mld snooping vlan 1 mrouter interface eth-0-1	配置静态组播路由端口
Switch(config)# ipv6 mld snooping vlan 1 report-suppression	在 VLAN 1 上启用报告抑制功能
Switch(config)# ipv6 mld snooping vlan 1 mrouter-aging-interval 200	配置动态组播路由端口老化时间

ii. 命令验证

显示 VLAN 1 上 MLD Snooping 的信息：

```
Switch# show ipv6 mld snooping vlan 1
Global Mld Snooping Configuration
------------------------------------------------
Mld Snooping                                :Enabled
Mld Snooping Fast-Leave                     :Enabled
Mld Snooping Version                        :1
Mld Snooping Max-Member-Number              :4096
Mld Snooping Unknown Multicast Behavior     :Discard
Mld Snooping Report-Suppression             :Enabled
Vlan 1
----------
Mld Snooping                                :Enabled
Mld Snooping Fast-Leave                     :Enabled
Mld Snooping Report-Suppression             :Enabled
Mld Snooping Version                        :1
Mld Snooping Max-Member-Number              :4096
Mld Snooping Unknown Multicast Behavior     :Discard
Mld Snooping Group Access-list              :N/A
Mld Snooping Mrouter Port                   :eth-0-1(static)
Mld Snooping Mrouter Port Aging Interval(sec) :200
```

4.7.4 配置 MLD Snooping 查询参数示例

i. 配置步骤

命令举例	操作步骤
Switch #configure terminal	进入全局配置模式
Switch(config)# ipv6 mld snooping query-interval 100	设置查询时间间隔是 100 秒
Switch(config)# ipv6 mld snooping query-max-	设置查询的最大响应时间 5 秒

命令举例	操作步骤
response-time 5	
Switch(config)#ipv6 mld snooping last-member-query-interval 2000	设置当仅存最后一个成员时的查询间隔
Switch(config)#ipv6 mld snooping vlan 1 querier address fe80::1	在 VLAN1 上配置 MLD Snooping 的查询地址
Switch(config)#ipv6 mld snooping vlan 1 querier	在 VLAN1 上启用 MLD Snooping 的查询功能
Switch(config)#ipv6 mld snooping vlan 1 query-interval 200	在 VLAN1 上设置查询时间间隔是 200 秒
Switch(config)#ipv6 mld snooping vlan 1 query-max-response-time 5	在 VLAN1 上设置查询的最大响应时间 5 秒
Switch(config)#ipv6 mld snooping vlan 1 querier-timeout 100	在 VLAN1 上设置查询超时时间 100 秒
Switch(config)#ipv6 mld snooping vlan 1 last-member-query-interval 2000	在 VLAN1 上设置特定组的查询间隔 2000 秒
Switch(config)# ipv6 mld snooping vlan 1 discard-unknown	在 VLAN1 上丢弃未知组播报文
Switch(config)# ipv6 mld snooping discard-unknown	在全局模式下设置丢弃未知组播报文

ii. 命令验证

显示 MLD Snooping 查询器相关信息：

```
Switch # show ipv6 mld snooping querier
Global Mld Snooping Querier Configuration
-----------------------------------------------
Version                                  :1
Last-Member-Query-Interval (msec) :2000
Max-Query-Response-Time (sec)        :5
Query-Interval (sec)                    :100
Global Source-Address                    :::
TCN Query Count                           :2
TCN Query Interval (sec)                :10
Vlan 1:     MLD snooping querier status
----------------------------------------
Elected querier is : fe80::1
----------------------------------------
Admin state                               :Enabled
```

```
Admin version                          :1
Operational state                      :Querier
Querier operational address            :fe80::1
Querier configure address              :fe80::1
Last-Member-Query-Interval (msec) :2000
Max-Query-Response-Time (sec)          :5
Query-Interval (sec)                   :200
Querier-Timeout (sec)                  :100
```

4.7.5 配置 TCN 查询示例

i. 配置步骤

命令举例	操作步骤
Switch#configure terminal	进入全局配置模式
Switch(config)# ipv6 mld snooping querier tcn query-count 5	设置 TCN 的查询次数为 5
Switch(config)# ipv6 mld snooping querier tcn query-interval 20	设置 TCN 的查询时间间隔 20 秒

ii. 命令验证

显示 MLD Snooping 查询器相关信息：

```
Switch # show ipv6 mld snooping querier
Global Mld Snooping Querier Configuration
-----------------------------------------------
Version                                :1
Last-Member-Query-Interval (msec) :2000
Max-Query-Response-Time (sec)          :5
Query-Interval (sec)                   :100
Global Source-Address                  :::
TCN Query Count                        :5
TCN Query Interval (sec)               :20
Vlan 1:     MLD snooping querier status
-----------------------------------------
Elected querier is : fe80::1
-----------------------------------------
Admin state                            :Enabled
Admin version                          :1
Operational state                      :Querier
Querier operational address            :fe80::1
Querier configure address              :fe80::1
Last-Member-Query-Interval (msec) :2000
```

```
Max-Query-Response-Time (sec)      :5
Query-Interval (sec)               :200
Querier-Timeout (sec)              :100
```

4.7.6 配置静态组播组示例

i. 配置步骤

命令举例	操作步骤
Switch#configure terminal	进入全局配置模式
Switch(config)# ipv6 mld snooping vlan 1 static-group ff0e::1234 interface eth-0-2	配置静态组播组 ff0e::1234，成员端口是 VLAN1 的 eth-0-2

ii. 命令验证

显示 MLD Snooping 组播组信息：

```
Switch# show ipv6 mld snooping groups

VLAN   Interface   Group Address                          Uptime      Expire-time
1      eth-0-2     ff0e::1234                             00:00:02    stopped
```

5 MVR6 配置

5.1 MVR6 简介

在传统的 IPv6 组播点播方式下，汇聚组播路由器下连一些接入交换机，接入交换机上连接了分布在不同 VLAN 中的用户。当这些属于不同 VLAN 的用户点播相同 Group 的节目时，汇聚的组播路由器需要为每个 VLAN 内的用户复制一份数据，每个 VLAN 的组播流量都要占用接入交换机的带宽。这样既增加了汇聚路由器的负担，也浪费了接入设备的带宽。

MVR6（IPv6 组播 VLAN 注册）功能能够很大程度地解决这个问题。在靠近用户侧的接入交换机上启用组播 VLAN，汇聚路由器只需把组播数据在源 VLAN 内发送给接入交换机，而不必在每个用户 VLAN 内都复制一份，接入交换机收到组播数据后再根据用户请求进行复制，给每个 VLAN 内的用户发送一份组播数据。从而节省了网络带宽，也减轻了三层设备的负担。

MVR6 依赖于 MLD Snooping 进行工作，而且只有 MVR 全局配置的 Group 才会生效。如果在 MVR6 的下游接口接收的 MLD 报文中组播组不在 MVR6 全局 Group 中，该报文将被忽略。通过在 MVR6 的下游接口接收的 MLD 报告/离开报文来维护接收者信息，MVR6 上游接口收到组播数据后，根据下游接口的 IPv6 组播组信息来决定转发组播数据的 VLAN 端口。

5.2 术语解释

配置 MVR6 功能所涉及的术语如下：

MVR6：IPv6 组播 VLAN 注册

源 VLAN（Source VLAN）：组播 VLAN 的源 VLAN

源端口（Source Port）：MVR6 网络中的上游接口，连接组播路由器的端口

接收端口（Receiver Port）：MVR6 网络中的下游接口，连接接收者的端口。用来监控组播主机连接至交换机的端口。

5.3 配置 MVR6

下面介绍 MVR6 相关的配置功能及说明，具体的配置步骤请参考 5.5 配置举例。

5.3.1 使能 MVR6

在使能 MVR6 功能之前，需要关闭 IPv6 组播路由功能。

表 5-1 使能 MVR6

命令	操作	说明
configure terminal	进入全局配置模式	-
no ipv6 multicast-routing	关闭 IPv6 组播路由功能	缺省情况下，IPv6 组播路由功能处于开启状态
mvr6	使能 MVR6 功能	缺省情况下，MVR6 功能处于关闭状态

5.3.2 配置 MVR6 的源 VLAN

在指定 MVR6 的源 VLAN 前，需要创建 VLAN 及其接口。

表 5-2 配置 MVR6 的源 VLAN

命令	操作	说明
configure terminal	进入全局配置模式	-
vlan database	进入 VLAN 配置模式	-
vlan *vlan-id*	创建 VLAN ID	默认为 VLAN 1
exit	退出 VLAN 配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
exit	退出接口配置模式	-
mvr6 vlan *vlan-id*	配置 MVR6 的源 VLAN	vlan-id: VLAN ID 的取值范围为 1~4094

5.3.3 创建 MVR6 组播组

通过该配置可以指定发送数据流的 IPv6 组播组地址以及 IPv6 组播组的数量。

表 5-3 配置 MVR6 组播组

命令	操作	说明
configure terminal	进入全局配置模式	-
mvr6 group *group-address* [*count*]	创建 MVR6 组播组	group-address: IPv6 组播组地址 count: IPv6 组播组数量，取值范围为 1~64

5.3.4 配置 MVR6 源地址

表 5-4 配置 MVR6 源地址

命令	操作	说明
configure terminal	进入全局配置模式	-
mvr6 source-address *address*	配置 MVR6 源地址	address: MVR6 上报组播报文的源地址

5.3.5 配置 MVR6 源端口/接收端口

在配置某个端口作为 MVR6 的源端口或接收端口时，源端口必须在 MVR6 源 VLAN 中，接收端口不能为 MVR6 源 VLAN 中的端口。

1. 配置MVR6源端口

表 5-5 配置 MVR6 源端口

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
mvr6 type source	配置 MVR 的源端口	-

2. 配置MVR6接收端口

表 5-6 配置 MVR6 接收端口

命令	操作	说明
configure terminal	进入全局配置模式	-
interface *if-name*	进入接口配置模式	if-name: 接口名称
mvr6 type receiver vlan *vlan-id*	配置 MVR6 的接收端口	vlan-id: VLAN ID 的取值范围为 1~4094

5.4 显示与维护

表 5-7 显示与维护

命令	操作	说明
show mvr6	显示 MVR6 相关配置信息	-
show mvr6 interface	显示 MVR6 端口的相关信息	-
show mvr6 groups [**vlan** *vlan-id*] [*group-address*]	显示从 MVR6 接收端口上学习到的组播组信息	vlan-id: VLAN ID 的取值范围为 1~4094 group-address: IPv6 组播组地址
show mvr6 group static global	显示 MVR6 全局配置的静态组播组信息	-
show resource mvr6	显示 MVR6 的资源使用情况	-

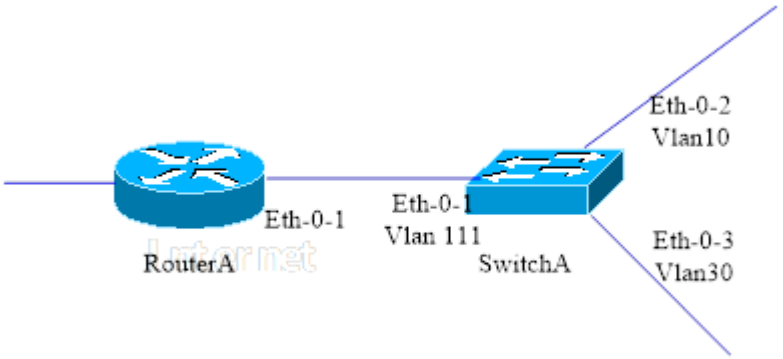
5.5 配置举例

5.5.1 介绍

如下图 7-7，在 Router A 的 eth-0-1 上启用 MLD 和 PIMv6-SM。配置 Switch A 的 eth-0-1 属于 VLAN111，eth-0-2 属于 VLAN10，eth-0-3 属于 VLAN30。在 Switch A 启用 MVR6，从 Router A 到 Switch A 上拷贝一份组播流，在 Switch A 上再将这个组播流进行复制，从 eth-0-2 和 eth-0-3 发送出去。

5.5.2 拓扑

图 5-1 IPv6 组播 VLAN 拓扑图



5.5.3 配置步骤

Router A:

在接口上启用 MLD 与 PIMv6-SM 协议。

命令举例	操作步骤
RouterA# configure terminal	进入全局配置模式
RouterA(config)# interface eth-0-1	进入接口配置模式
RouterA(config-if)# no switchport	设置端口为三层端口
RouterA(config-if)# no shutdown	使能端口
RouterA(config-if)# ipv6 address 2001:1::1/64	配置 IPv6 地址
RouterA(config-if)# ipv6 pim sparse-mode	启用 PIMv6-SM 协议
RouterA(config-if)# end	返回至全局配置模式

Switch A:

配置 eth-0-1 属于 VLAN111，eth-0-2 属于 VLAN10，eth-0-3 属于 VLAN30。

命令举例	操作步骤
SwitchA# configure terminal	进入全局配置模式
SwitchA(config)# vlan database	进入 VLAN 配置模式

命令举例	操作步骤
SwitchA(config-vlan)# vlan 111,10,30	创建 VLAN 111，10，30
SwitchA(config-vlan)# quit	退出 VLAN 配置模式
SwitchA(config)# interface vlan 111	进入 VLAN 接口配置模式
SwitchA(config-if)# exit	退出 VLAN 接口配置模式
SwitchA(config)# interface vlan 10	进入 VLAN 接口配置模式
SwitchA(config-if)# exit	退出 VLAN 接口配置模式
SwitchA(config)# interface vlan 30	进入 VLAN 接口配置模式
SwitchA(config-if)# exit	退出 VLAN 接口配置模式
SwitchA(config)# interface eth-0-1	进入接口配置模式
SwitchA(config-if)# switchport access vlan111	配置端口属于 VLAN111
SwitchA(config)# interface eth-0-2	进入接口配置模式
SwitchA(config-if)# switchport access vlan10	配置端口属于 VLAN10
SwitchA(config)# interface eth-0-3	进入接口配置模式
SwitchA(config-if)# switchport access vlan30	配置端口属于 VLAN30
SwitchA(config-if)# end	退出接口配置模式

在 Switch A 启用 MVR6，这样从 Router A 到 Switch A 只会拷贝一份组播流，在 Switch A 上再将这个组播流从 eth-0-2 和 eth-0-3 发送出去。

命令举例	操作步骤
SwitchA # configure terminal	进入全局配置模式
SwitchA(config)# no ipv6 multicast-routing	关闭 IPv6 组播路由
SwitchA(config)# mvr6	启用 MVR6
SwitchA(config)# mvr6 vlan 111	创建 MVR6 的 VLAN
SwitchA(config)# mvr6 group ff0e::1234 64	创建 IPv6 组播组
SwitchA(config)# mvr6 source-address fe80::1111	配置 MVR6 源地址

命令举例	操作步骤
SwitchA(config)# interface eth-0-1	进入接口配置模式
SwitchA(config-if)# mvr6 type source	配置接口为 MVR6 的源端口
SwitchA(config)# interface eth-0-2	进入接口配置模式
SwitchA(config-if)# mvr6 type receiver vlan 10	配置接口为 MVR6 的接收端口
SwitchA(config)# interface eth-0-3	进入接口配置模式
SwitchA(config-if)# mvr6 type receiver vlan 30	配置接口为 MVR6 的接收端口
SwitchA(config-if)# end	退出接口配置模式

5.5.4 命令验证

- 显示Router A上的配置信息：

```
RouterA # show ipv6 mld groups
MLD Connected Group Membership
Group Address                    Interface            Expires
ff0e::1234                       eth-0-2              00:03:01
ff0e::1235                       eth-0-2              00:03:01
ff0e::1236                       eth-0-2              00:03:01
ff0e::1237                       eth-0-2              00:03:01
ff0e::1238                       eth-0-2              00:03:01
……
ff0e::1273                       eth-0-2              00:03:01
```

- 显示Switch A上的配置信息：

```
SwitchA# show mvr6
MVR6 Running: TRUE
MVR6 Multicast VLAN: 111
MVR6 Source-address: fe80::111
MVR6 Max Multicast Groups: 1024
MVR6 Hw Rt Limit: 224
MVR6 Current Multicast Groups: 64
SwitchA# show mvr6 groups
VLAN    Interface    Group Address                    Uptime      Expire-time
10      eth-0-2      ff0e::1234                       00:03:23    00:02:03
10      eth-0-2      ff0e::1235                       00:03:23    00:02:03
10      eth-0-2      ff0e::1236                       00:03:23    00:02:03
10      eth-0-2      ff0e::1237                       00:03:23    00:02:03
10      eth-0-2      ff0e::1238                       00:03:23    00:02:03
```

```
10      eth-0-2   ff0e::1239                          00:03:23   00:02:03
……
10      eth-0-2   ff0e::1273                          00:03:23   00:02:03
```

堆叠配置指导目录

1 SCF 堆叠配置

1.1 SCF 简介

SCF（Switch Cluster Framework）即交换集群框架。在配置 SCF 之后，不仅可以提高交换机的易操作性，同时还能提升接入层和汇聚层的网络故障恢复率，从而提供不间断通信能力，保证流量业务。

SCF 是将通过堆叠端口连接起来的多个交换机作为一个交换机来进行管理，用户通过主交换机可以对堆叠内所有成员交换机进行管理，实现设备横向虚拟化。用户通过堆叠方式在扩展了端口后，不需要对每台交换机进行分别管理，而只需要将串口接在主机上，或者通过配置管理 IP 进行 telnet 管理，在统一的界面下，即可以对整个堆叠系统中的所有端口进行统一的配置，同时，整个堆叠系统将共享同一个 MAC 地址表和路由表，也就是说，整个堆叠系统共享二层和三层的转发策略。

1.1.1 堆叠 SCF

堆叠 SCF（Switch Cluster Framework）是指将多台支持堆叠特性的交换机设备组合在一起，从逻辑上组合成一台交换设备。堆叠系统建立之前，每台交换机都是单独的实体，有自己独立的 IP 地址和 MAC 地址，对外体现为多台交换机，用户需要独立的管理所有的交换机.堆叠建立后堆叠成员对外体现为一个统一的逻辑实体，用户使用一个 IP 地址对堆叠中的所有交换机进行管理和维护。通过交换机堆叠，可以提升转发能力，实现网络大数据量转发，同时提升网络高可靠性，简化组网和网络管理。

1.1.2 SCF 部署

SCF 的部署突破了机框的限制，使管理和组网部署更加具备可操作性，在安全性上也有极大的提升，实现了流量在 SCF 系统中的负载分担和冗余备份。SCF 系统设备角色定义：堆叠中每台交换机都是成员设备，分为：

- 主设备：对整个SCF系统进行管理
- 从设备：主设备的备用设备，当主用设备出现故障时，系统自动选举出一个新的设备作为主用设备，保证业务的运行。
- 成员设备：除主设备和从设备以外的其他成员设备

1.2 SCF 基本配置

1.2.1 配置堆叠域 ID

在一个网络中可以配置多个SCF，使用堆叠域 ID 区别不同的 SCF。所有 SCF 成员的域 ID 必须一致。配置重启后生效。

表1-1 配置堆叠域ID

命令	操作	说明
configure terminal	进入全局配置模式	-
scf domain *domain-id*	配置 SCF 堆叠域 ID	堆叠域 ID，取值范围为 1~255；缺省情况下，堆叠域 ID 为 1

1.2.2 配置堆叠成员编号与优先级

每个成员设备的 ID 必须不同，配置重启后生效。优先级的值越小，被选举成为主设备的概率越大。

表1-2 配置堆叠成员编号与优先级

命令	操作	说明
configure terminal	进入全局配置模式	-
scf domain *domain-id*	配置 SCF 堆叠域 ID，并进入域名模式	堆叠域 ID，取值范围为 1~255；缺省情况下，堆叠域 ID 为 1
scf member *member-id*	配置 SCF 堆叠成员编号	堆叠成员编号，取值范围为 1~9；缺省情况下，成员编号为 1
scf priority *PRIORITY*	配置 SCF 堆叠成员的优先级	堆叠成员优先级，取值范围为 1~255；缺省情况下，成员优先级为 100

1.2.3 配置堆叠端口

只能选择一条或者两条 VSL 链路，且链路带宽、类型要一致，VSL 编号本地有效。在堆叠端口配置模式下，可以绑定对应的物理口成员。

表1-3 创建堆叠端口

命令	操作	说明
configure terminal	进入全局配置模式	-
interface scf *port-number*	创建 SCF 堆叠端口，并进入堆叠端口配置模式	堆叠端口号，取值范围为 1~2

在堆叠口模式下，可以绑定或者删除对应的物理端口成员。

表1-4 绑定/删物理端口成员

命令	操作	说明
configure terminal	进入全局配置模式	-
interface scf *port-number*	创建 SCF 堆叠端口，并进入堆叠端口配置模式	堆叠端口号，取值范围为 1~2
port-member interface *eth-number*	绑定对应的物理端口成员	物理端口号，取值范围为 1~8
no port-member interface *eth-number*	删除配置的物理端口成员	

1.2.4 配置 SCF 工作模式

交换机有两种运行模式：独立模式和堆叠模式。模式切换需要重启设备才会生效。

表1-5 配置SCF工作模式

命令	操作	说明
switch convert mode scf	将工作模式切换到 SCF 模式	-

1.3 升级成员设备

以主控设备版本为最新版本，针对某一成员或全部成员进行版本升级同步。

表1-6 升级成员设备

命令	操作	说明
scf sync image to { **all |** *member-id* }	对所有或指定成员设备进行升级	指定的成员设备编号，取值范围为 1~9

1.4 重启成员设备

表1-7 升级成员设备

命令	操作	说明
reboot { **all |** *member-id* }	重启所有的堆叠设备或者重启某个成员设备	指定的成员设备编号，取值范围为 1~9

1.5 配置主备倒换

使用该命令可以将堆叠系统中 standby 成员转化为 active，原本的 active 成员设备会重启。

表1-8 升级成员设备

命令	操作	说明
scf redundancy switch	配置堆叠主备倒换	指定的成员设备编号，取值范围为 1~9

1.6 SCF 显示与维护

完成上述配置后，可以通过 SCF 相关的显示和维护命令，查看配置的结果。

表1-9 SCF显示与维护

命令	操作	说明
show scf upgdate progress	查看版本同步升级进度	版本升级状态，ready 表示开始传输版本，wait reboot 表示传输完成等待重启
show scf	显示 SCF 中所有堆叠成员的相关信息	堆叠成员相关信息包括成员 ID、域 ID，优先级、状态、角色等信息，在选举完成后才能正常显示。选举未完成时，提示”% The election is not completed, please try again later.”

命令	操作	说明
show scf topology	查看堆叠拓扑信息	堆叠拓扑信息包括：堆叠口连接情况以及各堆叠成员简要信息
show running-config scf	显示本设备堆叠相关配置	-
show scf config	显示 SCF 系统各成员设备的堆叠相关配置	-

1.7 配置举例

1.7.1 堆叠基本配置

i. 配置步骤

设备在空配置的独立模式下，直接切换到堆叠模式，保存重启：

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# switch convert mode scf	将独立模式切换到堆叠模式
Switch(config)# end	退出至 EXEC 模式
Switch# write Building configuration... [OK]	保存当前配置

ii. 命令验证

待堆叠选举完成后，使用堆叠的缺省配置形成单机堆叠。

1. 显示SCF中所有堆叠成员的相关信息：

```
Switch# show scf
 Member    Domain    Priority    MAC              Status      Version
-------------------------------------------------------------------------------------------------
  1         1         100        c0a6.6d07.f861   ACTIVE      11.001.001.T4
```

2. 查看堆叠拓扑信息：

```
Switch# show scf topolopy
Introduction:
'[num]' means member num, '(num)' means scf aggregate port num.

Topology:
[1]
Member      Status            MAC
-----------------------------------------------------
1           ACTIVE            c0a6.6d07.f861
```

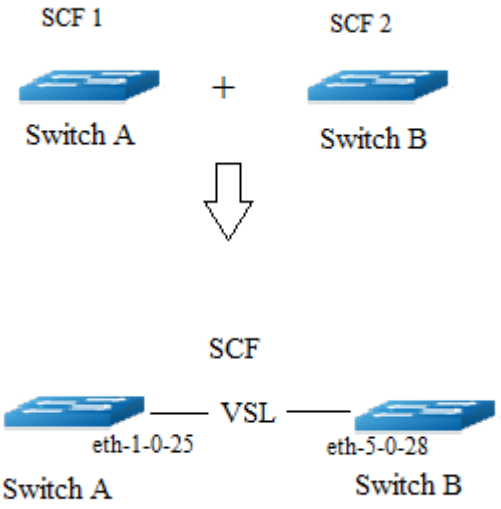
1.7.2 配置链式堆叠

i. 介绍

如下图所示：2台设备形成链式堆叠，两个各自稳定运行的SCF，如果它们的Domain ID相同，则可以通过在两SCF之间增加VSL链接来使其合并成为一个SCF。

ii. 拓扑

图 5-2 SCF 堆叠拓扑图（链式连接）



iii. 配置步骤

Switch A的配置如下：

命令举例	操作步骤
SwitchA# config terminal	进入全局配置模式
SwitchA(config)# scf domain 255	配置堆叠域 ID 为 255，并进入域名模式
SwitchA(config-scf-domain)# scf member 1	配置 SCF 堆叠成员编号为 1
SwitchA(config-scf-domain)# scf priority 1	配置堆叠成员的优先级为 1
SwitchA(config-scf-domain)# end	退出至特权模式
SwitchA# switch convert mode scf	切换工作模式到 SCF 模式
SwitchA# config terminal	进入全局配置模式
SwitchA(config)# interface scf 1	创建 SCF 堆叠口，并进入堆叠口配置模式
SwitchA(config-scf-if)# port-member interface eth-1-0-25	在堆叠口模式下，绑定对应的物理口成员
SwitchA(config-scf-if)# end	退出至特权模式

Switch B的配置如下：

命令举例	操作步骤
SwitchA# config terminal	进入全局配置模式
SwitchA(config)# scf domain 255	配置堆叠域 ID 为 255，并进入域名模式
SwitchA(config-scf-domain)# scf member 5	配置 SCF 堆叠成员编号为 5
SwitchA(config-scf-domain)# scf priority 125	配置堆叠成员的优先级为 125
SwitchA(config-scf-domain)# end	退出至特权模式
SwitchA# switch convert mode scf	切换工作模式到 SCF 模式
SwitchA# config terminal	进入全局配置模式
SwitchA(config)# interface scf 1	创建 SCF 堆叠口，并进入堆叠口配置模式
SwitchA(config-scf-if)# port-member interface eth-5-0-28	在堆叠口模式下，绑定对应的物理口成员
SwitchA(config-scf-if)# quit	返回至全局配置模式

命令举例	操作步骤
SwitchA(config)# interface scf 2	创建 SCF 堆叠口，并进入堆叠口配置模式
SwitchA(config-scf-if)# port-member interface eth-5-0-25	在堆叠口模式下，绑定对应的物理口成员
SwitchA(config-scf-if)# end	退出至特权模式

iv. 命令验证

1. 显示SCF中所有堆叠成员的相关信息：

```
Switch# show scf
 Member    Domain    Priority    MAC              Status      Version
-------------------------------------------------------------------------------------------------------
   1         255         1      c0a6.6d07.d301   ACTIVE      11.001.001.T4
   5         255         125    c0a6.6d07.d321   STANDBY     11.001.001.T4
```

2. 查看堆叠拓扑信息：

```
Switch# show scf topolopy
Introduction:
'[num]' means member num, '(num)' means scf aggregate port num.

Topology:
[1] (1) ------ (2) [5]
Member    Status          MAC
-------------------------------------------------
1         ACTIVE          c0a6.6d07.d301
5         STANDBY         c0a6.6d07.d321
```

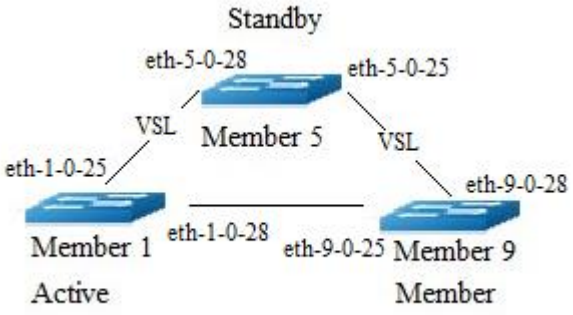
1.7.3 配置环式堆叠

i. 介绍

如下图所示：3台设备形成环式堆叠，Member 1为控设备，Member 5为备份主控，Member 9 为其他成员设备。

ii. 拓扑

图 5-3 SCF 堆叠拓扑（环式连接）



iii. 配置步骤

Active的配置如下：

命令举例	操作步骤
Switch# config terminal	进入全局配置模式
Switch(config)# scf domain 255	配置堆叠域 ID 为 255，并进入域名模式
Switch(config-scf-domain)# scf member 1	配置 SCF 堆叠成员编号为 1
Switch(config-scf-domain)# scf priority 1	配置堆叠成员的优先级为 1
Switch(config-scf-domain)# end	退出至特权模式
Switch# switch convert mode scf	切换工作模式到 SCF 模式
Switch# config terminal	进入全局配置模式
Switch(config)# interface scf 1	创建 SCF 堆叠口，并进入堆叠口配置模式
Switch(config-scf-if)# port-member interface eth-1-0-25	在堆叠口模式下，绑定对应的物理口成员
Switch(config-scf-if)# quit	返回至全局配置模式
Switch(config)# interface scf 2	创建 SCF 堆叠口，并进入堆叠口配置模式
Switch(config-scf-if)# port-member interface eth-1-0-28	在堆叠口模式下，绑定对应的物理口成员

Standby的配置如下：

命令举例	操作步骤
Switch# config terminal	进入全局配置模式
Switch(config)# scf domain 255	配置堆叠域 ID 为 255，并进入域名模式
Switch(config-scf-domain)# scf member 5	配置 SCF 堆叠成员编号为 5
Switch(config-scf-domain)# scf priority 125	配置堆叠成员的优先级为 125
Switch(config-scf-domain)# end	退出至特权模式
Switch# switch convert mode scf	切换工作模式到 SCF 模式
Switch# config terminal	进入全局配置模式
Switch(config)# interface scf 1	创建 SCF 堆叠口，并进入堆叠口配置模式
Switch(config-scf-if)# port-member interface eth-5-0-28	在堆叠口模式下，绑定对应的物理口成员
Switch(config-scf-if)# quit	返回至全局配置模式
Switch(config)# interface scf 2	创建 SCF 堆叠口，并进入堆叠口配置模式
Switch(config-scf-if)# port-member interface eth-5-0-25	在堆叠口模式下，绑定对应的物理口成员
Switch(config-scf-if)# end	退出至特权模式

Member的配置如下：

命令举例	操作步骤
Switch# config terminal	进入全局配置模式
Switch(config)# scf domain 255	配置堆叠域 ID 为 255，并进入域名模式
Switch(config-scf-domain)# scf member 9	配置 SCF 堆叠成员编号为 9
Switch(config-scf-domain)# scf priority 255	配置堆叠成员的优先级为 255
Switch(config-scf-domain)# end	退出至特权模式
Switch# switch convert mode scf	切换工作模式到 SCF 模式
Switch# config terminal	进入全局配置模式
Switch(config)# interface scf 1	创建 SCF 堆叠口，并进入堆叠口配置模式
Switch(config-scf-if)# port-member interface eth-9-0-25	在堆叠口模式下，绑定对应的物理口成员

命令举例	操作步骤
Switch(config-scf-if)# quit	返回至全局配置模式
Switch(config)# interface scf 2	创建 SCF 堆叠口，并进入堆叠口配置模式
Switch(config-scf-if)# port-member interface eth-9-0-28	在堆叠口模式下，绑定对应的物理口成员
Switch(config-scf-if)# end	退出至特权模式

iv. 命令验证

1. 显示SCF中所有堆叠成员的相关信息：

```
Switch# show scf
 Member    Domain    Priority    MAC               Status        Version
-------------------------------------------------------------------------------------------------
   1         255         1      c0a6.6d07.d301    ACTIVE      11.001.001.T4
   5         255         125    c0a6.6d07.d321    STANDBY     11.001.001.T4
   9         255         255    c0a6.6d07.f861     MEMBER     11.001.001.T4
```

2. 查看堆叠拓扑信息：

```
Switch# show scf topolopy
Introduction:
'[num]' means member num, '(num)' means scf aggregate port num.

Topology:
[1] (1) ------ (2) [5] (1) ------ (2) [9] (1) ------ (2) [1]
Member     Status          MAC
-------------------------------------------------
1          ACTIVE          c0a6.6d07.d301
5          STANDBY         c0a6.6d07.d321
9          MEMBER          c0a6.6d07.f861
```

RPC API 配置指导目录

1 RPC API 配置

1.1 RPC API 简介

RPC API 服务提供用户通过软件远程控制交换机的能力。目前只支持 JSON-RPC over HTTP 和 HTTP 基本认证。

1.2 配置 RPC API 服务

1.2.1 启动 RPC API 服务

表1-1 启动RPC API服务

命令	操作	说明
configure terminal	进入全局配置模式	-
service rpc-api enable port *port-number*	启动 RPC API 服务	port-number: API 端口 ID，默认使用 80 端口

1.2.2 关闭 RPC API 服务

表 1-2 关闭 RPC API 服务

命令	操作	说明
configure terminal	进入全局配置模式	-
service rpc-api disable	关闭 RPC API 服务	-

1.3 配置 RPC API 服务的 HTTP 基本认证

启用或关闭 HTTP 认证后，用户需要手动重启 RPC API 服务或者重启交换机，配置才能生效。目前只支持 HTTP 基本认证。如果用户认证失败，服务器将返回 401 状态码。

1.3.1 启动 RPC API 服务的 HTTP 基本认证

表 1-3 启动 RPC API 服务的 HTTP 基本认证

命令	操作	说明
configure terminal	进入全局配置模式	-
service rpc-api auth-mode basic	启用 RPC API 服务的 HTTP 基本认证	缺省情况下，RPC API 服务的 HTTP 基本认证处于关闭状态

1.3.2 关闭 RPC API 服务的 HTTP 基本认证

表 1-4 关闭 RPC API 服务的 HTTP 基本认证

命令	操作	说明
configure terminal	进入全局配置模式	-
no service rpc-api auth-mode	关闭 RPC API 服务的 HTTP 基本认证	缺省情况下，RPC API 服务的 HTTP 基本认证处于关闭状态

1.4 显示与维护

表 1-5 显示与维护

命令	操作	说明
show services rpc-api	显示系统当前的 RPC API 服务配置	-

1.5 配置举例

1.5.1 配置 RPC API 服务

1. 启用RPC API服务

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# service rpc-api enable port 80	启动 RPC API 服务，使用 TCP 80 (HTTP) 端口

命令举例	操作步骤
Switch(config)# exit	退出全局配置模式

2. 关闭RPC API服务

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# service rpc-api disable	关闭 RPC API 服务
Switch(config)# exit	退出全局配置模式

1.5.2 配置 RPC API 服务的 HTTP 认证

1. 启用RPC API服务的HTTP基本认证

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# username centec password centec	配置交换机的用户名 (centec) 和密码 (centec)，可以用于 HTTP 认证
Switch(config)# service rpc-api auth-mode basic	启用 RPC API 服务的 HTTP 基本认证
Switch(config)# exit	退出全局配置模式

2. 取消配置RPC API服务的HTTP基本认证

命令举例	操作步骤
Switch# configure terminal	进入全局配置模式
Switch(config)# no service rpc-api auth-mode	关闭 RPC API 服务的 HTTP 认证
Switch(config)# exit	退出全局配置模式

说明

启用或关闭 HTTP 认证后，用户需要手动重启 RPC API 服务或者重启交换机，配置才能生效。

启用 RPC API 后会占用 2 个 imish 资源下发命令，当 show users 时 RPC API 占用 imish 的 idle time 一直是 0。

完成上述步骤后，显示当前 RPC API 的配置信息：

```
Switch# show services rpc-api
RPC API services configuration:
HTTP server:       running, port: 80, authentication mode: none
```

2 RPC API 规范

2.1 概述

RPC API 服务，使用了标准的 JSON-RPC 规范。可以通过 JSON RPC method: ‘executeCmds’执行交换机的 CLI 命令行。默认初始模式为 EXEC(#)特权模式。

用户需要通过发送 JSON-RPC (over HTTP)请求 URL: ***http://<交换机管理口 IP 地址>:<端口号>/command-api***, 请求和返回的 JSON-RPC 格式如下所示。

2.1.1 JSON-RPC Request

JSON-RPC 请求及解释如下：

```
{
    "params":[                                              命令参数
        {
            "format":"text",            期望命令返回格式, 可以是’text’或者’json’, 默认’text’
            "version":1,                                    命令版本号
            "cmds":[                                        命令列表
                "show run",                                 命令行 1
                "config t",                                 命令行 2
                "vlan database",                            命令行 3
                "vlan 1-8",                                 命令行 4
                "interface eth-0-1",                        命令行 5
                "switchport mode trunk",                    命令行 6
                "switchport trunk allowed vlan add 2",      命令行 7
                "shutdown",                                 命令行 8
                "end",                                      命令行 9
                "show interface switchport"                 命令行 10
            ]
        }
    ],
    "jsonrpc":"2.0",                                        JSON RPC 协议版本号
    "method":"executeCmds",                                 运行交换机 CLI 命令的方法
    "id":"70853aff-af77-420e-8f3c-fa9430733a19"             JSON RPC 协议中的 UID
}
```

2.1.2 JSON-RPC Response

JSON-RPC 返回及解释如下：

```
{
    "jsonrpc":"2.0",                                    JSON RPC 协议版本号
    "id":"70853aff-af77-420e-8f3c-fa9430733a19",        JSON RPC 协议中的 UID
    "result":[                                          JSON RPC 返回值列表
        {
            "sourceDetails":"version 5.1.6.fcs\n!\n …",      命令行 1 的返回值。

如果运行成功，原始文本输出在”sourceDetails” 属性中。
            "errorCode":-1003,                                          如果有错，会输出在
            "errorDesc":"unsupported command…",          warnings/errorCode/errorDesc 属性中。
"warnings":"% Invalid …",

JSON 格式化对象也会输出到这里。
        },
        { },                                            命令行 2 的返回值。
        { },                                            命令行 3 的返回值。
        { },                                            命令行 4 的返回值。
        { },                                            命令行 5 的返回值。
        { },                                            命令行 6 的返回值。
        { },                                            命令行 7 的返回值。
        { },                                            命令行 8 的返回值。
        { },                                            命令行 9 的返回值。
        {
            "sourceDetails":" Interface name            : eth-0-1\n Switchport mode          :
trunk\n …\n"
        }                                               命令行 10 的返回值。
    ]
}
```

2.2 Python Client 代码示例

以 pyjsonrpc 库为例，示例代码如下：

```
import pyjsonrpc
import json
http_client = pyjsonrpc.HttpClient(
    url = "http://10.10.39.64:80/command-api",
    username = "centec",
    password = "centec"
)
cmds = {}
```

```
cmd_list = ["show run", "config t", "vlan database", "vlan 1-8", "interface eth-0-1", "switchport mode trunk",
"switchport trunk allowed vlan add 2", "shutdown", "end", "show interface switchport"]
cmds['cmds'] = cmd_list
cmds['format'] = 'text'
cmds['version'] = 1
try:
        response = http_client.call("executeCmds", cmds)
        print("json response:");
        json_result = json.dumps(response, indent=4)
        print(json_result)
except Exception, e:
        if e.code == 401:
                print "Unauthorized user"
        else:
                print e.message
                print e.data
```

2.3 JSON-RPC 错误码

下表列出了JSON-RPC 2.0的错误码：

2-1 JSON-RPC 错误码

错误码	描述
-32700	JSON 解析错误
-32600	无效请求
-32601	方法无效
-32602	无效参数
-32603	内部错误

2.4 RPC-API 错误码

下表列出了RPC-API的错误码：

2-2 RPC-API 错误码

错误码	描述
-1000	普通错误

错误码	描述
-2001	不支持的 JSON RPC API 版本
-2002	JSON RPC 中必须指定’params’ 和 ‘cmds’
-2003	不支持的 JSON 返回格式
-3001	命令执行错误: 超时
-3002	命令执行错误: 不支持该命令
-3003	命令执行错误: 该命令未授权
-3004	命令执行错误: 找不到该命令
-3005	命令执行错误: 不能够转换为 JSON 格式
-3006	命令执行错误: 命令行数目太少
-3007	命令执行错误: 命令行数目太多