CN12800 系列

数据中心核心交换机

操作手册

版本：A/02

浪潮网络科技（山东）有限公司

二零二三年十月

浪潮网络科技（山东）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

技术文档邮箱：　inspur_network@inspur.com

客户投诉热线：　400-691-1766

公司总部地址：　山东省济南市高新区浪潮路 1036 号

邮政编码：　　250000

声　　明

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

手册说明

本手册介绍 CN12800 系列数据中心核心交换机（以下简称 CN12800）的各种功能模块和业务特性基于 CLI 的操作指南。从简单技术原理、功能配置过程和配置举例三方面进行介绍。这些配置操作的介绍旨在帮助用户掌握 CN12800 的配置方法和了解其应用场景，更全面系统的掌握 CN12800 的使用、维护以及管理。

本手册适用于以下产品型号：

- CN12804
- CN12808
- CN12816

本手册适用的读者对象为：工程技术人员、工程开通人员、设备维护人员、网络管理人员和对该产品有兴趣的其他人员。

内容介绍

描述本手册主要内容，介绍各章重点，指导使用者有针对性地使用本手册。

章名	概要
第 1 章 基础配置	本章介绍了 CN12800 的基本配置，包括：登录交换机、配置接口、基本用户配置、配置文件系统以及设备文件上传及下载。
第 2 章 二层以太网功能配置	本章介绍了 CN12800 的二层以太基本功能配置。
第 3 章 IP 业务配置	本章针对 CN12800 的 IP 业务。
第 4 章 三层 IP 路由功能配置	本章介绍了 CN12800 中路由相关的基本内容、配置过程和配置举例。
第 5 章 QoS 配置	本章介绍了 CN12800 中 QoS 的基本内容、配置过程和配置举例。
第 6 章 组播配置	本章介绍了 CN12800 的组播相关配置。
第 7 章 安全配置	本章介绍了 CN12800 中安全性相关的基本内容、配置过程和配置举例。
第 8 章 可靠性配置	本章介绍了 CN12800 中可靠性管理的基本内容、配置过程和配置举例。
第 9 章 设备管理配置	本章介绍了 CN12800 的设备管理相关配置。
第 10 章 运维管理配置	本章介绍了 CN12800 的运维管理配置。

章名	概要
第 11 章 VPN 配置	本章介绍了 CN12800 中 VPN 隧道管理的基本内容、配置过程和配置举例。
第 12 章 数据中心特性配置	本章介绍了 CN12800 数据中心的相关配置。

版本更新说明

软件版本	手册版本	更新说明
V370R240	A02	第一次发布

本书约定

介绍字体约定、命令行约定、键盘操作约定、鼠标操作约定以及符号约定。

1. 字体约定

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

2. 命令行约定

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

3. 键盘操作约定

格式	意义
加尖括号的字符	表示键名、按钮名。如＜Enter＞、＜Tab＞、＜Backspace＞、＜a＞等分别表示回车、制表、退格、小写字母 a
＜键 1+键 2＞	表示在键盘上同时按下几个键。如＜Ctrl+Alt+A＞表示同时按下“Ctrl”、“Alt”、“A”这三个键

格式	意义
＜键 1，键 2＞	表示先按第一键，释放，再按第二键。如＜Alt，F＞表示先按＜Alt＞键，释放后，紧接着再按＜F＞键

4. 鼠标操作约定

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

5. 符号约定

本书采用三个醒目标志来表示在操作过程中应该特别注意的地方。

 **说明**、  **注意**、  **警告**。

免责声明

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

目 录

第1章 基础配置

本章主要介绍 CN12800 系列交换机的接口和基础配置操作。

1.1 接口简介

接口是提供给用户操作或配置的单元，主要用于接收和发送数据。接口从功能上可以分为管理接口和业务接口，从形态上可以分为物理接口和逻辑接口。

1.1.1 管理接口

背景信息

管理接口为用户提供配置管理功能。用户可以通过管理接口登录到 CN12800 交换机，进行配置和管理操作。管理接口不承担业务传输。

接口类型

CN12800 系列交换机提供 Console、ETH 两种管理接口。

表 1-1 管理接口

接口名	说明	功能
Console 接口	遵循 EIA/TIA-232 标准，接口类型是 DCE。	该接口与配置终端的 COM 串口连接，用于搭建现场配置环境。
ETH 接口	遵循 10/100BASE-TX 标准。	该接口与配置终端或网管站（NMS）的网口连接，用于搭建现场或远程配置环境。

1.1.2 业务接口

背景信息

业务接口为用户提供配置业务功能，承担业务传输。

接口类型

CN12800 交换机目前支持的业务接口包括：

- 万兆以太网接口（XGE）
- 2.5 万兆以太网接口（25GE）

- 4 万兆以太网接口（40GE）
- 10 万兆以太网接口（100GE）

1.2 登录交换机

本节介绍登录 CN12800 交换机的三种方式：Console、Telnet 和 SSH。

1.2.1 通过 Console 口登录交换机

目的

本节介绍在本地 PC 上，通过 Console 口登录 CN12800 交换机的操作步骤。串口登录交换机仅供日常版本上传、升级和维护使用。

前提条件

CN12800 系列交换机已经上传了 OS 和 FPGA 版本。

组网环境

通过 Console 口登录 CN12800 系列交换机，用户需要使用一根串口线连接本地 PC 与交换机上的 Console 接口，如图 1-1 所示。

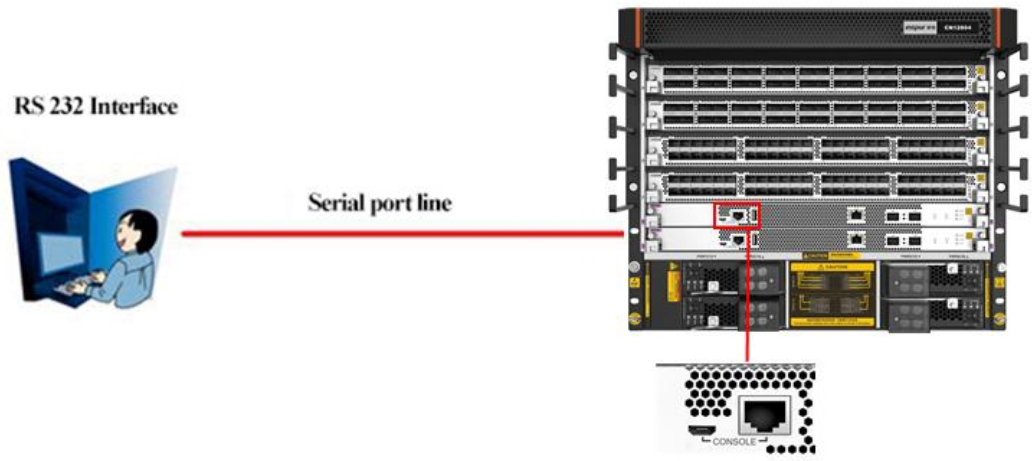


图 1-1 通过 Console 接口登录到 CN12800 交换机

过程

通过 Console 口登录 CN12800 交换机的步骤如下。

1. 如图 1-1 所示，使用一根串口线连接 PC 主机和 CN12800 交换机。
2. 在 PC 机上启动 SecureCRT。
3. 新建连接。

   在菜单栏中单击“文件”→“快速连接”，在“快速连接”界面，根据实际串口线的连接情况选择对应的 COM 口，设置串口属性，然后再单击“连接”按钮，如图 1-2 所示。

图 1-2 设置 CN12800 的端口和串口属性

按照表 1-1 设置参数。

表 1-1 串口属性

参数	值
协议	Serial
波特率	115200
数据位	8
奇偶校验	None
停止位	1

结果

按照以上步骤结束设置后，如果设备运行正常，SecureCRT 会显示如图 1-3 所示界面，表示连接到 CN12800 交换机。

图 1-3 登录 CN12800 交换机的 SecureCRT 界面

1.2.2 通过 Telnet 登录交换机

目的

除了 Console 接口之外，也可以利用 Telnet 方式登录 CN12800 交换机。

本节介绍使用本地 PC 机通过 Telnet 方式登录 CN12800 交换机上的操作步骤。

Telnet 支持本地和远程用户登录，易于维护。

组网环境

用户通过 Telnet 方式登录交换机时，需要使用网线直连或通过 Hub 连接 PC 和交换机（带外管理接口或者业务接口），如图 1-4 所示。

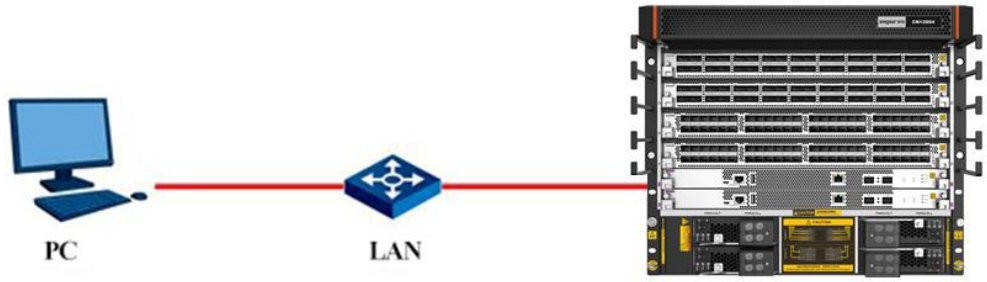


图 1-4 Telnet 方式登陆交换机

登录交换机后，需要配置 CN12800 交换机 Telnet 用户，设置新用户名及其密码。

过程

通过 Telnet 方式登录交换机的步骤如下。

1. 通过 Console 口方式登录 CN12800 交换机，设置新用户名及其密码（密码建议设置为数字、字母和特殊字符的组合，且长度大于等于 8 个字节），命令如下，具体步骤可参考 1.2.1。

```
CN12800(config)#username test group administrators password 123@.com
CN12800(config)#
```

2. 在带外接口配置视图下配置带外接口 IP 地址。

```
CN12800(config)#interface mgt-eth 0/0/0
CN12800(config-mgt-eth-0/0/0)#ip address 223.1.10.103/24
```

3. 在带外接口配置视图下执行 **show** 命令，显示交换机的远程登录 IP 地址，以供 Telnet 用户访问，命令如下。

```
CN12800(config-mgt-eth-0/0/0)#show
!
interface mgt-eth 0/0/0
 ip address 223.1.10.103/24
CN12800(config-mgt-eth-0/0/0)#
```

4. 单击 SecureCRT 中的“快速连接”按钮，在“快速连接”对话窗口中输入相应参数。其中，“协议”下拉选择 Telnet；“主机名”为交换机配置的带内 IP 地址；“端口”为 23；防火墙为 None。如图 1-5 所示。

图 1-5 Telnet 登录

5. 单击“连接”按钮，稍等几秒，启动 Telnet 客户端。输入用户名、密码后如果网络连接正常，会弹出如下信息界面。

```
User Access Verification

Username:
```

6. 输入步骤 1 设置的用户名和密码后，系统进入配置模式。

```
User Access Verification

Username:test
Password:********
CN12800#
```

1.2.3 通过 SSH 登录交换机

目的

本节介绍使用本地 PC 机通过 SSH 方式登录 CN12800 交换机的操作步骤。对用户登录安全性要求较高时，使用 SSH 方式登录交换机。

组网环境

可参考 Console 或 Telnet 登录交换机的组网方式。

前提条件

用户在使用 SSH 方式登录 CN12800 交换机之前，需要确认：

- 在设备第一次上电并通过串口登录设备后，已执行 **sshd** 命令开启设备的 SSH 功能。
- 建议连接之前用电脑 ping 一下交换机，以检测是否能 ping 通。

1.2.3.1 使用本地用户账号进行 SSH 登录

过程

（以使用 Secure CRT 软件为例）

说明：

下述步骤 1~步骤 2，是用户第一次配置 SSH 登录的过程。若 SSH 已经创建好，用户可以从步骤 3 开始执行，进行 SSH 登录。

1. 创建 SSH 登录方式，单击如图 1-6 所示红框标识的按钮。

图 1-6 创建 SSH 登录

2. 在弹出的“快速连接”对话窗口中输入相应参数。其中，“协议”下拉选择 SSH2；“主机名”为交换机配置的带内 IP 地址；“用户名”为 SSH 本地用户账号的用户名，单击“连接”按钮，稍等几秒，如图 1-7 所示。

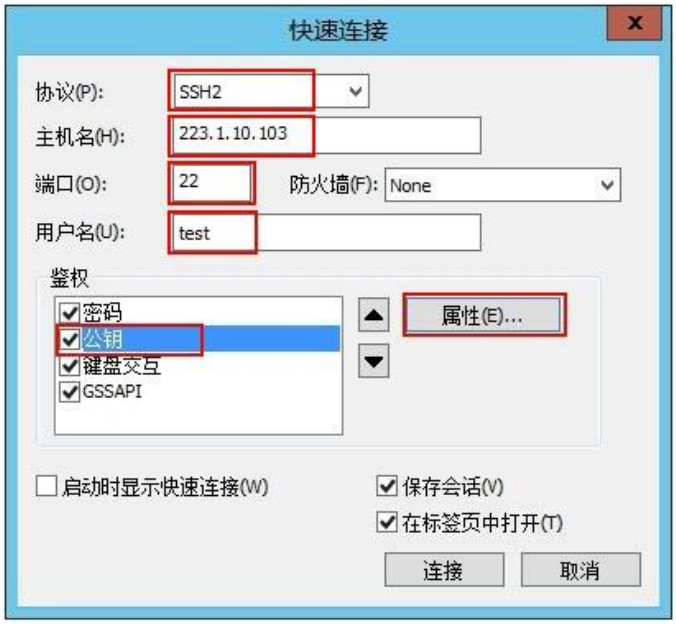


图 1-7 设置 SSH 登录参数

3. 输入 SSH 本地用户账号的密码，若选择保存密码，则下次使用 SSH 登录，则无需再输入密码，再单击“确定”按钮。如图 1-8。

图 1-8 输入 SSH 密码

4. 在弹出的“连接”对话框中，选择如下图所示红框部分的 IP 地址，单击“连接”按钮。

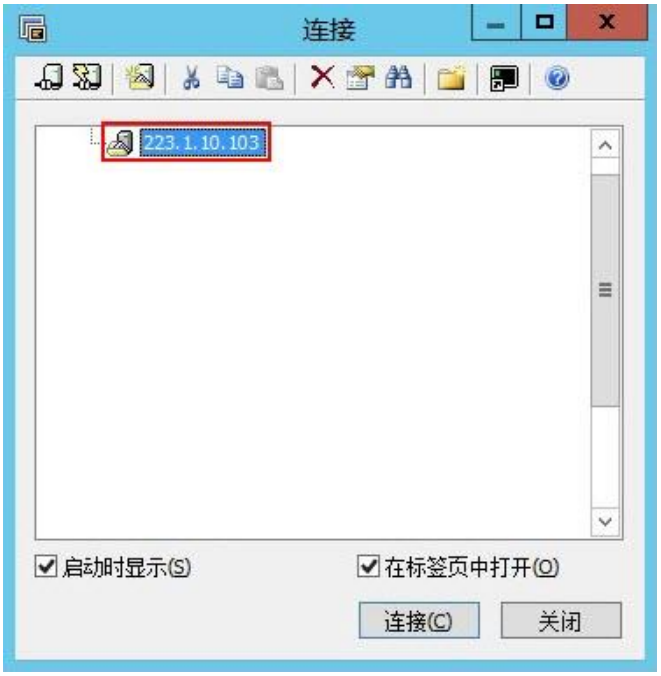


图 1-9 SSH 登录连接

结果

按照以上步骤结束设置后，使用 SSH 成功登录 CN12800 交换机，如图 1-10 所示。

图 1-10 使用本地用户账号 SSH 登录成功

1.2.3.2 使用公钥方式进行 SSH 登录

过程

（以使用 Secure CRT 软件为例）

1. 准备密钥对（例如，使用 Secure CRT 生成的密钥对）。单击 Secure CRT 菜单栏上“工具”→“创建公钥…”选项。

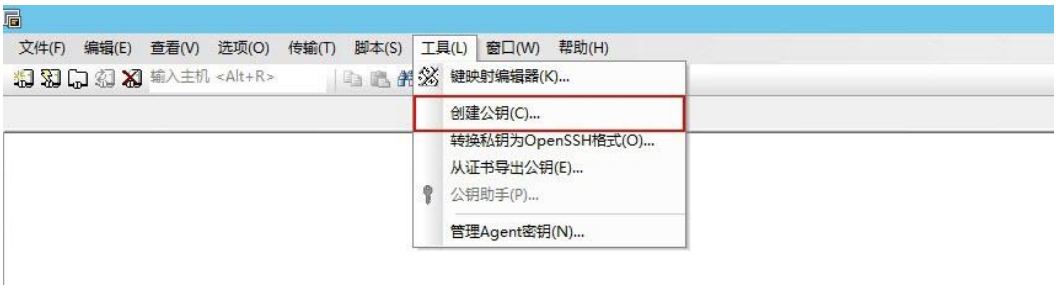


图 1-11 准备 SSH 密钥对

2. 在“密钥生成向导”对话框中，单击“下一步”。

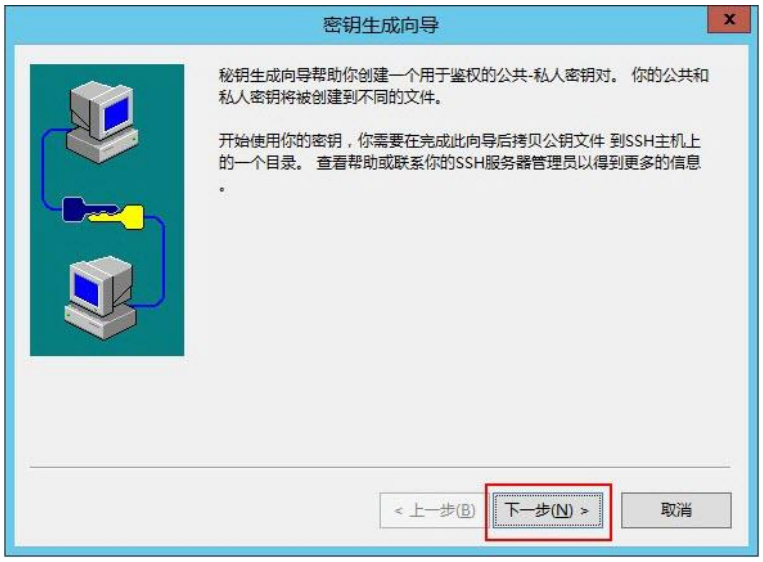


图 1-12 密钥生成向导

3. 选择密钥生成的方式 DSA 或 RSA，确定密钥生成方式后，单击“下一步”按钮。

图 1-13 选择公钥类型

4. 根据需要设置参数“通行短语”、“确认通行短语”和“注释”，记住所填写的通行短语值，再单击“下一步”按钮。

图 1-14 设置通行短语

5. 在弹出的对话框中，选择默认值 1024 即可，单击“下一步”按钮。

说明：

- DSA 支持的密钥长度：512、768、1024、2048；
- RSA 支持的密钥长度：768、1024、2048。

图 1-15 设置密钥位长度

6. 弹出如下对话框表示正在生成密钥对。密钥对生成后，单击“下一步”按钮。

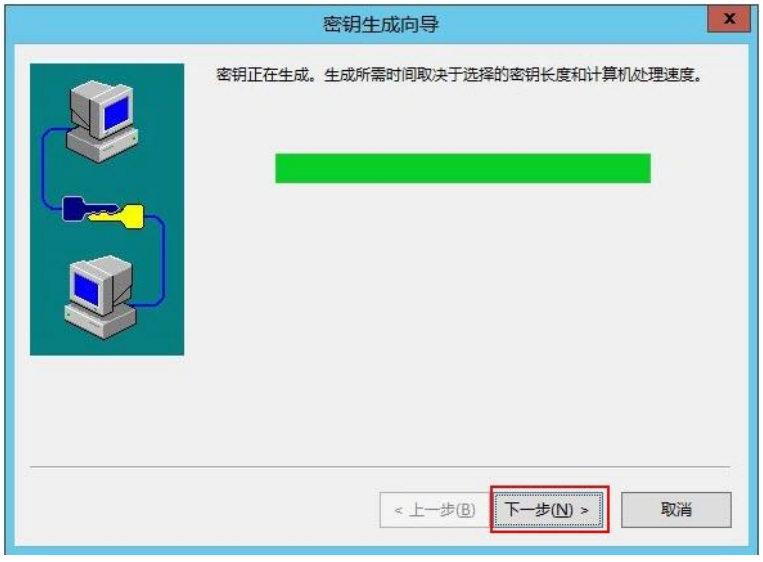


图 1-16 密钥正在生成

注意：

在生成密钥对的过程中，请不停地在对话框所在的范围内移动鼠标，以免进度条进展过慢。

7. 使用 Secure CRT 默认的保存路径保存生成的原始公钥文档，然后单击“完成”。

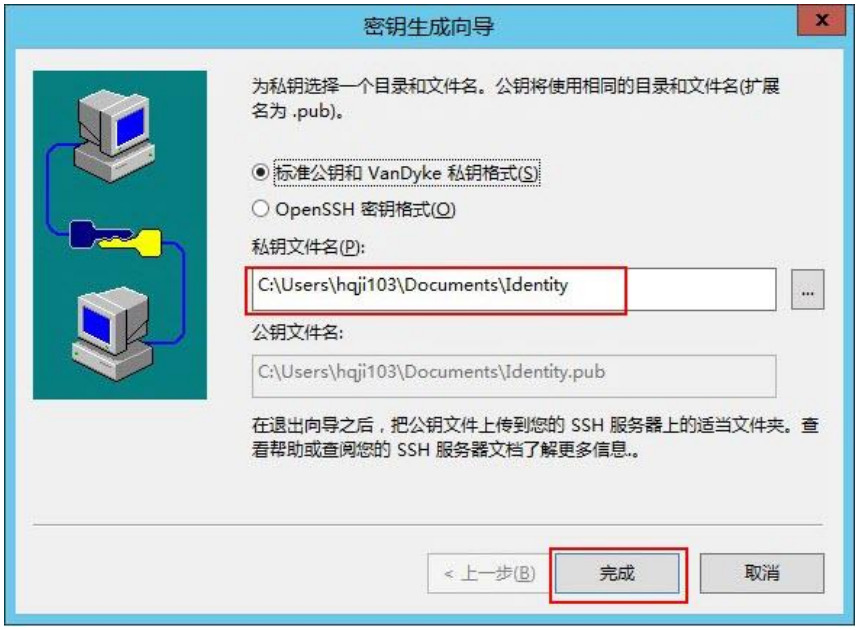


图 1-17 保存密钥

8. 在弹出的对话框中，单击“否”。

9. 修改生成的原始公钥文档 Identity.pub 文件，再通过 FTP 方式下载到设备。

```
CN12800(config)#tftp get 223.1.10.206 Identity.pub
 Local path is “/tmp/ram/download”.
 Getting data…
```

```
715 bytes downloaded %Transmission success.


CN12800(config)#
```

10. 将下载的原始公钥文档拷贝到设备上用户对应的目录下。以将原始公钥文档拷贝到 user 用户对应的目录下为例。

```
CN12800(config)#copy download /user/authorized_keys
  %Copying file /tmp/ram/download - > /tmp/ram//user/authorized_keys


CN12800(config)#
```

注意：

公钥文档在设备上存储的名字必须是“**authorized_keys**”。

11. 使用 SSH 方式登录，在 PC 或配置终端上运行 SSH 的客户端软件，单击图 1-18 所示红框标识的“快速连接”按钮。

图 1-18 SSH 登录

12. 在如下对话框中，设置“协议”为 SSH2，“主机名”为设备的带内 IP 地址，“用户名”为之前公钥文档拷贝到的用户目录对应的用户名，鉴权方式选择“公钥”，单击“属性...”按钮。

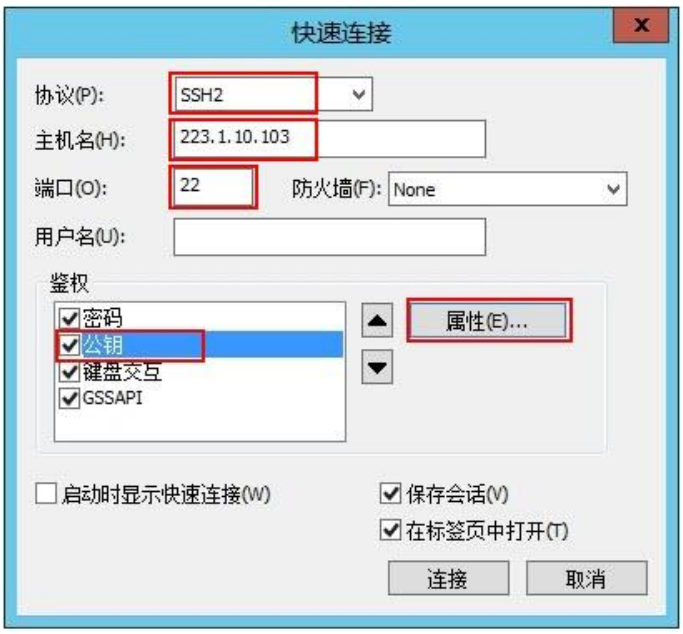


图 1-19 SSH 登录参数设置

13. 在弹出的“公钥属性”对话框中选择“使用身份证或证书文件”，选中步骤 9 中生成的公钥文件，单击“确定”。

14. 在如下对话框中，输入之前创建公钥时用户输入的通行短语（即步骤 4 中输入的值），单击“确定”按钮。

图 1-20 SSH 登录密码设置

说明：

以上使用公钥方式进行 SSH 登录，也可以在 CLI 命令行中使用 ssh keygen/sshd auth/ssh login method 命令进行配置。

结果

按照以上步骤结束设置后，使用 SSH 成功登录交换机，如图 1-21 所示。

图 1-21 使用公钥方式 SSH 登录成功

1.3 基本配置

1.3.1 设备管理配置

设备管理的配置任务主要是对交换机的单板状态、CPU、内存使用状态进行显示。

设备管理的配置任务包括：

- 复位交换机
- 更新系统或配置文件
- 日志配置命令
- 配置访问控制列表

1.3.1.1 复位交换机

目的

当交换机出现故障需要重启的时候可以通过 reboot 命令来复位。该命令的功能与冷启动的效果相同，但在设备的远程维护时，不需要用户到设备所在地重启，而直接在远地就可以重启设备。该命令可导致网络工作在短时间内瘫痪，在一般情况下，禁止使用。另外在重启设备时，要确认配置文件是否需要保存，如需保存，请在用户视图下执行 write file 配置，然后执行命令 **y**。

过程

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

1.3.1.2 更新系统或配置文件

目的

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

过程

更新系统或配置文件的步骤如下所示，参数说明请参考《CN12800 系列交换机命令行手册》。

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

1.3.1.3 配置访问控制列表

目的

本节介绍如何配置访问控制列表。

过程

如何配置访问控制列表的过程如下表所示，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
使能或者配置访问控制列表	1. 进入全局配置视图； 2. 执行如下命令： ● **management acl** { **enable | disable** } ● **management acl** *ipv4-address* ● **management acl** *ipv4-address/M* ● **management acl** *ipv4-address ipv4-address-mask* ● **management acl** *ipv4-address ipv4-address-mask* { **telnet** | **snmp** | **ssh** | **tftp** | **ftp** | **all** } ● **management acl** *ipv4-address/M* { **telnet** | **snmp** | **ssh** | **tftp** | **ftp** | **all** }。
取消使能或者取消配置访问控制列表	1. 进入全局配置视图； 2. 执行如下命令： ● **no management acl** *ipv4-address/M* ● **no management acl** *ipv4-address ipv4-address-mask* ● **no management acl** *ipv4-address ipv4-address-mask* { **telnet** | **snmp** | **ssh** | **tftp** | **ftp** | **all** }

目的	步骤
	● **no management acl** *ipv4-address/M* { **telnet** | **snmp** | **ssh** | **tftp** | **ftp** | **all** }。

1.3.2 系统基本环境配置

系统基本配置和管理包括：

- 设置交换机的名称；
- 设置系统时钟。

1.3.2.1 配置交换机的系统名

目的

本节介绍如何设置交换机的系统名。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

1.3.2.2 配置系统时钟

目的

本节介绍如何设置系统时钟。

过程

设置系统时钟的步骤见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

1.3.2.3 夏时令设置

目的

本节介绍如何设置和取消夏令时的名称和生效起始、终止时间。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
设置夏时令	1. 进入全局配置视图； 2. 执行如下命令： ● **clock summer-time** *summer-time-name* **date** *start-hour:start-minutes start-day start-month start-year end-hour:end-minutes end-day end-month end-year* ● **clock summer-time** *summer-time-name* **date** *start-hour:start-minutes start-year/start-month/start-day end-hour:end-minutes end-year/end-month /end-day* ● **clock summer-time** *summer-time-name* **recurring** { **first** | **second** | **third** | **fourth** | **fifth** | **last** } { **monday** | **tuesday** | **wednesday** | **thursday** | **friday** | **saturday** | **sunday** } { **january** | **february** | **march** | **april** | **may** | **june** | **july** | **august** | **september** | **october** | **november** | **december** } *start-hour:start-minutes* { **first** | **second** | **third** | **fourth** | **fifth** | **last** } { **monday** | **tuesday** | **wednesday** | **thursday** | **friday** | **saturday** | **sunday** } { **january** | **february** | **march** | **april** | **may** | **june** | **july** | **august** | **september** | **october** | **november** | **december** } *end-hour:end-minutes*。
取消夏令时	1. 进入全局配置视图； 2. 执行命令 **no clock summer-time**。

1.3.2.4 设置本地时区信息

目的

本节介绍如何设置本地时区信息。

过程

设置本地时区信息的步骤如下所示，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
设置本地时区信息	1. 进入全局配置视图； 2. 执行命令 **clock timezone** *time-zone-name* { **add** | **minus** } *offset*。

1.3.3 显示系统基本信息

1.3.3.1 显示设备管理运行信息

目的

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

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

1.3.3.2 显示当前配置视图下的所有可用命令

目的

本节介绍如何查看当前配置视图下的所有可用命令。

过程

查看当前配置视图下的所有可用命令步骤如下所示。

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

1.3.3.3 显示用户所用过的历史命令

目的

本节介绍用户如何显示用户所用过的历史命令。

过程

显示用户所用过的历史命令步骤如下所示。

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

1.3.3.4 显示系统版本信息

目的

本节介绍用户如何显示系统版本信息。

过程

显示系统当前的软硬件版本号、编译时间等信息的步骤如下所示。

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

1.3.3.5 查看当前时间和设备已经运行的时间

目的

本节介绍用户如何查看当前时间和设备已经运行的时间。

过程

查看当前时间和设备已经运行的时间的步骤如下所示。

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

1.3.3.6 查看当前登录用户的个数

目的

本节介绍用户如何查看当前登录用户的个数。

过程

查看当前登录用户的个数的步骤如下所示。

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

1.3.3.7 查看 CN12800 的电源状态

目的

本节介绍用户如何查看 CN12800 的电源状态。

过程

查看 CN12800 的电源状态的步骤如下所示。

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

1.3.3.8 查看 MAC 地址信息

目的

本节介绍用户如何查看 CN12800 的默认 MAC 地址信息和正在使用的 MAC 地址信息。

过程

CN12800 的默认 MAC 地址信息和正在使用的 MAC 地址信息的步骤如下所示。

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

1.3.3.9 查看访问控制列表的配置信息

目的

本节介绍用户如何查看访问控制列表的配置信息。

过程

查看访问控制列表的配置信息的步骤如下所示。

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

1.3.4 密码管理配置

CN12800 系列数据中心交换机能够向用户提供密码管理功能，在登录 CN12800 系列数据中心交换机之前需要先配置系统的登录密码，配置密码之后每次登录交换机都要先输入

密码，系统认证通过后才允许用户登录交换机进行后续操作。对于密码验证失败的用户则无法登录成功。用户可以使用缺省的密码配置，也可以自行进行密码管理配置，自行进行密码管理的时候遵循以下步骤：

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

1.3.4.1 分配用户权限

目的

本节介绍了登录 CN12800 后，如何增加用户名及其权限和密码。

CN12800 对登录用户划分为 4 种等级，如表 1-2 所示。隶属于 Administrators 组中的用户才有权限新增用户。

表 1-2 CN12800 支持的用户类型

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

不同级别的用户登录后，只能使用等于或低于自己级别的命令。为了保密，用户在屏幕上看不到所键入的口令。

操作

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

1.3.4.2 用户权限配置举例

组网需求

一台 PC 同一台 CN12800 交换机相连。用户可采用缺省配置，也可以根据各自实际要求自行配置密码参数。

组网图

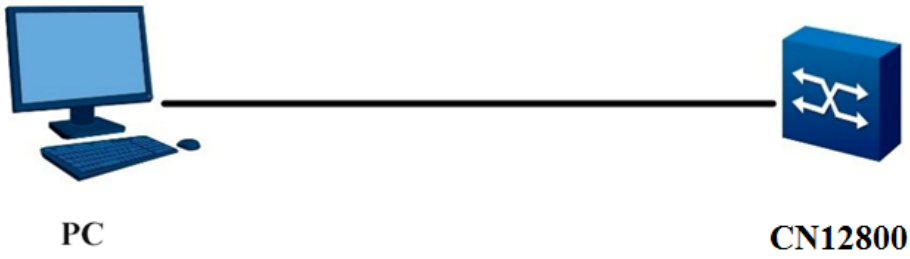


图 1-22 用户权限配置示例

配置步骤

用缺省的用户名和密码登录系统，进入全局配置视图，增加一个用户名为 123，权限为 Administrators，密码为 Admin123456 的缺省用户。

配置步骤如下：

```
CN12800#config
CN12800(config)#username 123 group Administrators password Admin123456
#退出登录
CN12800(config)#quit
CN12800#quit
#用前面配置的用户名 123，密码 Admin123456 可以登录成功
Uername：123
```

```
Password：**********
CN12800#
```

1.3.5 配置用户界面

用户界面的配置主要包括：

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

1.3.5.1 设置终端接收调试信息的功能开关

目的

本节介绍用户如何打开或者关闭命令行终端接收调试信息的功能。

过程

命令行终端接收调试信息是否打开的步骤如下所示。

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

1.3.5.2 用户进入或取消终端配置

目的

本节介绍用户如何进入或取消终端配置。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
进入终端配置模式	1. 进入全局配置视图、line 配置视图； 2. 执行命令 **line vty** *vty-number1 vty-number2*。
取消终端配置	1. 进入全局配置视图、line 配置视图； 2. 执行命令 **no line vty** *vty-number*。

1.3.5.3 进入串口终端配置视图

目的

本节介绍用户如何进入串口终端配置视图。

过程

配置进入串口终端配置视图的步骤如下所示，参数说明请参考《CN12800 系列交换机命令行手册》。

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

1.3.5.4 关闭一个虚终端

目的

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

vty 终端号包括 Telnet 和 SSH 连接终端。

设备默认存在 5 个虚拟终端，即同一时刻允许 5 个用户同时 telnet 或 ssh 登录设备。

过程

配置如何关闭一个虚终端的步骤如下所示，参数说明请参考《CN12800 系列交换机命令行手册》。

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

1.3.5.5 配置命令行终端是否区分大小写

目的

本节介绍用户如何配置命令行终端是否区分大小写。

过程

配置命令行终端是否区分大小写的步骤如下所示。

目的	步骤
配置命令行终端是否区分大小写	1. 进入全局配置视图； 2. 执行命令 **case-sensitive** { **enable** | **disable** }。

1.3.5.6 配置终端显示命令行的行数

目的

本节介绍用户如何配置终端显示行的数目。

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

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

1.3.5.7 配置终端显示的颜色

目的

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

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置终端显示的颜色	1. 进入全局配置视图； 2. 执行命令 **terminal color** { **gray** | **red** | **green** | **yellow** | **blue** | **purple** | **water** | **white** }。

1.3.5.8 配置终端显示的语言

目的

本节介绍用户如何配置终端显示的语言。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
配置终端显示的语言	1. 进入全局配置视图； 2. 执行命令 **line concole** 或 **line vty** *vty-number* 或 **line vty** *vty-number1 vty-number2*； 3. 执行命令 **language** { **chinese** | **english** }。

1.3.5.9 配置虚拟终端是否接收调试信息

目的

本节介绍用户如何配置设置调试信息是否在屏幕上打印出来。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
设置虚拟终端是否接收调试信息	1. 进入全局用户视图； 2. 执行命令 **terminal monitor**。
恢复缺省值	1. 进入全局用户视图； 2. 执行命令 **no terminal monitor**。

1.3.5.10 设置虚拟终端的超时时间

目的

本节介绍用户如何设置虚拟终端的超时时间。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
设置虚拟终端的超时时间	1. 进入全局配置视图； 2. 执行命令 **line concole** 或 **line vty**；

目的	步骤
	3. 执行命令 **timeout** *time*。
恢复缺省值	1. 进入全局配置视图； 2. 执行命令 **line concole** 或 **line vty**； 3. 执行命令 **no timeout**。

1.3.5.11 设置虚拟终端的无输入的超时时间

目的

本节介绍用户如何设置虚拟终端的无输入的超时时间。

过程

设置和恢复虚拟终端的无输入的超时时间的步骤如下所示，参数说明请参考《CN12800 系列交换机命令行手册》。

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

1.3.5.12 显示当前设备登录用户信息

目的

本节介绍用户如何显示当前设备允许多少用户登录以及已登录用户的相关信息。

过程

显示当前设备登录用户信息的步骤如下所示。

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

1.3.6 配置用户权限

本节介绍了登录 CN12800 后，如何管理和分配用户权限。

1.3.6.1 新增用户

目的

本节介绍了登录 CN12800 后，如何新增用户。

CN12800 对登录用户划分为 4 种类等级，如表 1-3 所示。隶属于 Administrators 组中的用户才有权限新增用户。

表 1-3 CN12800 支持的用户类型

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

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

过程

增加用户的步骤如下所示，参数说明请参考《CN12800 系列交换机命令行手册》。

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

1.3.6.2 删除用户

目的

本节介绍了在 CN12800 新增用户后，如果需要删除用户的操作。

隶属于 Administrators 组中的用户才有权限删除用户信息。

过程

删除用户的步骤如下所示，参数说明请参考《CN12800 系列交换机命令行手册》。

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

1.3.6.3 查看已创建的本地用户的属性

目的

本节介绍了如何查看已创建的本地用户的属性。

过程

查看已创建的本地用户的属性的步骤如下所示，参数说明请参考《CN12800 系列交换机命令行手册》。

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

1.3.6.4 配置不同的域实现管理用户的登录权限

目的

本节介绍了如何配置不同的域实现管理用户的登录权限。

过程

配置不同的域实现管理用户的登录权限的步骤如下，参数说明请参考《CN12800 系列交换机命令行手册》。

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

1.3.6.5 提升用户权限

目的

本节介绍了如何提升用户权限。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
提升用户的权限	1. 进入全局配置视图； 2. 执行命令 **enable password level** *level-value* { **cipher** | **plain** } *password* 配置权限提升密码； 3. 进入 Line 配置视图； 4. 执行命令 **enable authentication local** 使能 enable 认证功能；

目的	步骤
	5. 若用户使用低于配置的 level 权限用户登录时，进入特权用户视图； 6. 执行命令 **enable** *level-value* 后提示输入密码； 7. 输入步骤 2 中配置的密码即可实现用户权限提升。

1.3.6.6 设置用户密码复杂度

目的

本节介绍了如何设置用户密码复杂度。

过程

设置用户密码复杂度的步骤如下所示，参数说明请参考《CN12800 系列交换机命令行手册》。

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

1.3.6.7 设置指定用户或者全局用户的密码长度

目的

本节介绍了如何设置指定用户或者全局用户的密码长度。

过程

设置指定用户或者全局用户的密码长度的步骤如下所示，参数说明请参考《CN12800 系列交换机命令行手册》。

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

1.3.6.8 设置指定用户登录系统失败的最多次数

目的

本节介绍了如何设置指定用户登录系统失败的最多次数。

过程

设置指定用户登录系统失败的最多次数的步骤如下所示，参数说明请参考《CN12800 系列交换机命令行手册》。

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

1.3.6.9 设置用户重认证时间间隔

目的

本节介绍了如何设置用户重认证时间间隔。

过程

设置用户重认证时间间隔的步骤如下所示，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
设置用户重认证时间间隔	1. 进入全局配置视图； 2. 执行如下命令： ● **user reauth-interval** *reauth-interval-tim* ● **username** *word* **reauth-interval** *reauth-interval-time*。

1.3.6.10 设置用户的 FTP 路径

目的

本节介绍了如何设置用户的 FTP 路径。

过程

设置用户的 FTP 路径的步骤如下所示，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
设置用户的 FTP 路径	1. 进入全局配置视图； 2. 执行如下命令 **username** *user-name* **ftp-directory {** *dir* **| default }**设置用户的 FTP 路径。

1.3.6.11 配置 Telnet、SSH 和 FTP

目的

本节介绍了如何配置 Telnet、SSH 和 FTP。

过程

配置 Telnet、SSH 和 FTP 的步骤如下所示，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
设置 Telnet、SSH 和 FTP 用户登录系统的最大并发数	1. 进入全局配置视图； 2. 执行命令 **user** { **telnet** | **ssh** } **max-count** { *count-number* | **default** }。
打开或关闭 SSH 调试功能	1. 进入特权用户视图； 2. 执行如下命令： ● **debug ssh**； ● **no debug ssh**。
打开或关闭 SSH 文件传输协议调试功能	1. 进入特权用户视图； 2. 执行如下命令： ● **debug sftp**； ● **no debug sftp**。
使能或去使能 SSH 文件传输协议服务	1. 进入全局配置视图； 2. 执行命令 **sftp-server** { **enable** | **disable** }。
开启或关闭设备的 SSH 功能	1. 进入全局配置视图； 2. 执行如下命令： ● **sshd**； ● **no sshd**。
配置 SSHD 认证方式（包括密码认证和公钥认证）	1. 进入全局配置视图； 2. 执行如下命令： ● **sshd auth** { **password** | **pubkey** }； ● **no sshd auth** { **password** | **pubkey** }。
配置 SSHD 登录闲置时间	1. 进入全局配置视图； 2. 执行命令 **sshd login-grace-time** { *login-grace-timer* | **default** }。
配置密匙字符串	1. 进入全局配置视图； 2. 执行如下命令： ● **key** { **ssh-dss** | **ssh-rsa** } *key-string*； ● **key** *key-string*。
创建公钥	1. 进入全局配置视图； 2. 执行如下命令： ● **ssh keygen dsa**； ● **ssh keygen rsa bits** { **1024** | **2048** | **3072** }。
配置 SSH 用户密匙	1. 进入全局配置视图； 2. 执行命令 **ssh user** *user-name* **key begin**。
显示 SSH 配置信息	1. 进入普通用户视图； 2. 执行命令 **show ssh config**。

1.3.6.12 查询用户权限

目的

本节介绍如何查询用户权限。

过程

根据不同目的，执行相应步骤，具体参见下表。

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

1.3.7 带内带外网管配置

1.3.7.1 带内网管配置

目的

本节介绍如何配置带内网管。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

1.3.7.2 带外网管配置

目的

本节介绍如何配置带外网管。注意带外IP地址不能与带内IP为同网段IP。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

1.4 系统配置文件操作

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

根据操作对象的不同，可以把文件系统操作分为以下几类：

- 目录操作
- 文件操作

1.4.1 目录操作

目的

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

过程

目录操作的步骤如下所示，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
创建目录	在特权用户视图或全局配置视图下执行命令 **mkdir** *directory*。
删除目录	在特权用户视图或全局配置视图下执行命令 **rmdir** *directory*。
显示当前的工作目录	在特权用户视图或全局配置视图下执行命令 **pwd**。
改变当前目录	在特权用户视图或全局配置视图下执行命令 **cd** *directory*。
列出一个目录或其子目录内容	在特权用户视图或全局配置视图下执行命令 **ls tree** *directory* 在特权用户视图或全局配置视图下或者执行 **ls tree** *directory* **subtree**。

1.4.2 文件操作

目的

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

过程

文件操作的步骤如下所示，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
删除文件	在特权用户视图下执行命令 **del** *file-name*。
永久删除文件	在特权用户视图下执行命令 **remove** *filename*。
重新命名文件	在特权用户视图下执行命令 **rename** *old -filename new-filename*。
拷贝文件夹	在特权用户视图下执行命令 **xcopy** *srcfile destfile*。
拷贝文件	在特权用户视图下执行命令 **copy** *srcfile destfile*。
显示指定二进制 text 文件的内容	在特权用户视图下执行命令 **type** *filename* { **binary** | **text** }。
清空指定文件的内容	在特权用户视图下执行命令 **zero** *filename*。
检验打包文件合法性	在全局配置视图下执行命令 **check software file-name** *filename*。
导出指定进程或所有进程的堆栈信息到本地	在普通用户视图下执行命令 **export process** { *taskname* | **all** } **stack to** *localfile* [**slot** { *slot-id* | **all** }]。

1.4.3 系统配置文件

本节主要介绍设备的系统配置文件的相关操作。

1.4.3.1 切换本地认证模式

目的

本节介绍如何配置由其他的认证模式切换到本地认证模式。

过程

切换本地认证模式的步骤如下所示。

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

1.4.3.2 保存配置文件

目的

本节介绍如何把当前系统的配置写到启动配置文件中。

过程

保存配置文件的步骤如下。

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

1.4.3.3 引导加载设备操作系统

目的

本节介绍如何从主镜像文件或备份镜像文件引导加载设备操作系统。

过程

步骤如下：

1. 进入全局配置视图；
2. 执行命令 **boot os** { **main** | **backup** }。

1.4.3.4 升级系统文件及查看

目的

本节介绍如何升级及查看系统文件。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
更新系统或配置文件	在全局配置视图下执行命令 **upgrade** { **os** | **config** | **backup-os** } [*local-file-name*]。
升级 CMU 文件	在全局配置视图下执行命令 **upgrade cmu**。
整包升级系统文件	在全局配置视图下执行命令 **upgrade os slot** { *slot-id* | **group** *slotlist* | **self** } **whole-packet**。
打包数字签名、升级文件和公钥	在全局配置视图下执行命令 **packet-file sign-file** *sign-file* **simple-file** *simple-file* **certificate** *certificate* **output** *pktfile*。
查看单盘升级信息	在普通用户视图下执行命令 **show upgrade card-packet info**。
查看整包升级信息	在普通用户视图下执行命令 **show upgrade whole-packet info**。

1.4.3.5 查看和删除 OS 文件

目的

本节介绍如何查看或删除交换机内存里存储的 OS 文件。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

1.5 设备文件上传及下载

1.5.1 FTP 配置

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

交换机提供的 FTP 服务包括：

- FTP Server 服务，用户可以运行 FTP 客户端程序登录到服务器上（接受用户登录前，网络管理员需要事先配置好 FTP Server 的 IP 地址），访问服务器上的文件。
- FTP Client 服务，用户在微机上通过终端仿真程序或 Telnet 程序建立与交换机（FTP Client）的连接后，输入 ftp X.X.X.X（X.X.X.X 代表远程 FTP Server 的 IP 地址）命令，建立交换机与远程 FTP Server 的连接，访问远程 FTP Server 上的文件。

本设备支持 IPv4 网络地址下的 FTP 功能。

1.5.1.1 启动/关闭 FTP 服务器

目的

本节介绍如何启动和关闭 FTP 服务器。

过程

启动/关闭 FTP 服务器的步骤如下所示。

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

1.5.1.2 FTP 客户端介绍

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

1.5.1.3 FTP Server 配置举例

目的

交换机作为 FTP Server 实现配置文件的备份和软件升级配置举例。

设备	配置
Switch	启动 FTP Server，并做了用户名、密码等相关配置。
PC	使用 FTP 客户端程序登录交换机。

组网需求

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

组网图

图 1-23 FTP 配置示意图

配置步骤

交换机上的配置：

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

```
CN12800#config
CN12800(config)#ftpd
```

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

```
C:\ftp 1.1.1.1
    220 FHN(1.0)FTP Server ready
User (1.1.1.1 none): admin
331 Password required
Password:
230 User logged in
ftp>bin
200 Type set to I, binary mode
ftp> put switch.z
200 Port set okay
150 Opening BINARY mode data connection
226 Transfer complete
ftp: 发送 3069212 字节，用时 1.42Seconds 2158.38Kbytes/sec.
```

#获取交换机配置文件。

```
ftp>ascii
200 Type is ASCII
ftp>get startcfg
150 Opening ASCII mode data connection
```

```
226 Transfer complete
ftp: 收到 14251 字节，用时 0.22Seconds 65.07Kbytes/sec.
```

注意：

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

3) 在上载完毕后，用户在交换机上进行升级操作。

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

```
CN12800#config
CN12800(config)#upgrade os
CN12800(config)#quit
CN12800#reboot
```

1.5.1.4 FTP Client 配置举例

目的

交换机作为 FTP Client 实现配置文件的备份和软件升级配置举例。

设备	配置	配置说明
Switch	可以直接使用 ftp 命令登录远端的 FTP Server。	用户首先获取 FTP 用户命令和密码，然后登录远端的 FTP Server ，这样才能取得相应目录和文件。 ● **ftp get** *ipv4-address user password remotefile* [*port-id*] ● **ftp get** *ipv4-address user password remotefile* **localfile** *filename* [*port-id*] ● **ftp put** *ipv4-address user password remotefile* **config** ● **ftp put** *ipv4-address user password remotefile* **localfile** *filename* [*port-id*] ● **ftp put** *ipv4-address user password remotefile* **running-config** [*port-id*]。
PC	启动 FTP Server，并作了用户名、密码、用户的权限等相关的配置。	

组网要求

交换机作为 FTP Client，远端的 PC 作为 FTP Server，在 FTP Server 上作了如下配置：配置了一个 FTP 用户名为 123，密码为 123。配置 PC 的 IP 地址为 10.18.1.2。用户可以通过 Telnet 远程登录到 CN12800 交换机上，从 FTP Server 上下载交换机的应用程序到交换机的 Flash，通过命令行实现交换机的远程升级。

组网图

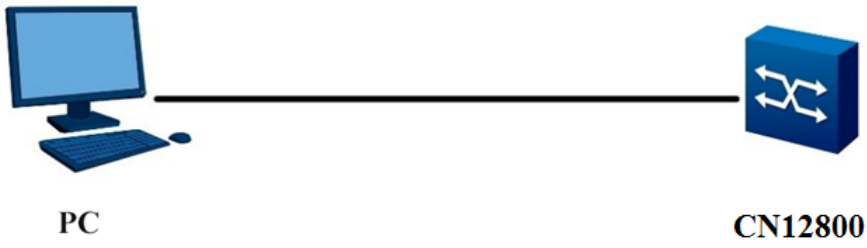


图 1-24 交换机作为 FTP client 配置组网图

配置步骤

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

```
CN12800#config
CN12800(config)#ftp get 10.18.1.2 123 123 d:\upgrade.z
    Local path is “Ram:/flash/download”.
    Getting data...
  3069212 bytes downloaded
```

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

```
CN12800(config)#upgrade os

WARNING:System will upgrade! Continue?[y/n]
   System now is upgrading,please wait.
   %Local path is “Ram:/flash/download”.
CN12800(config)#reboot
```

注意：

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

1.5.2 TFTP 配置

TFTP（Trivial File Transfer Protocol，简单文件传输协议），最初打算引导无盘系统（通常是工作站或 X 终端），相对于另一种文件传输协议 FTP，TFTP 不具有复杂的交互存取

接口和认证控制，适用于客户端和服务器之间不需要复杂交互的环境。TFTP 协议一般在 UDP 的基础上实现。

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

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

本设备支持 IPv4 网络地址下的 TFTP 功能。

图 1-25 TFTP 配置示意图

1.5.2.1 配置 TFTP Server 开关

目的

本节介绍了如何打开或者关闭设备的 TFTP Server 开关功能。

过程

根据不同目的，执行相应步骤，具体参见下表。

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

1.5.2.2 用 TFTP 下载文件

 **注意：**

建议用户在技术人员的指导下进行该命令的操作。

目的

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

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
通过 TFTP 下载远程文件并存储在本地（适用于 IPv4）	1. 进入全局配置视图； 2. 执行如下命令： ● **tftp get** { *ipv4-address* | *mac-address* } *remotefile* [*port-id*] ● **tftp get** { *ipv4-address* | *mac-address* } *remotefile* **localfile** *filename* [*port-id*] ● **tftp get** *ipv4-address* **vpn-instance** *name remotefile* [*port-id*] ● **tftp get** *ipv4-address* **vpn-instance** *name remotefile* **localfile** *filename* [*port-id*]。
使用 TFTP 协议一键导出文件	1. 进入全局配置视图； 2. 执行命令 **file export tftp** *ipv4-address remotedir localdir*。

1.5.2.3 用 TFTP 上传文件

 **注意：**

建议用户在技术人员的指导下进行该命令的操作。

目的

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

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
将本地文件上传到远程 TFTP Server（适用于 IPv4）	1. 进入全局配置视图； 2. 执行如下命令： ● **tftp put** *ipv4-address remotefile* **running-config** [*port-id*] ● **tftp put** { *ipv4-address* | *mac-address* } *remotefile* **config** ● **tftp put** { *ipv4-address* | *mac-address* } *remotefile* **localfile** *filename* [*port-id*] ● **tftp put** *ipv4-address* **vpn-instance** *name remotefile* **config** ● **tftp put** *ipv4-address* **vpn-instance** *name remotefile* **localfile** *filename* [*port-id*]。
开启设备的 IPv4 Telnet 服务功能	1. 进入全局配置视图； 2. 执行命令 **telnetd** 开启设备的 IPv4 Telnet 服务功能。
关闭设备的 IPv4 Telnet 服务功能	1. 进入全局配置视图； 2. 执行命令 **no telnetd** 关闭设备的 IPv4 Telnet 服务功能。
使能 IPv4 版本的 Telnet 服务器	1. 进入全局配置视图； 2. 执行命令 **telnetd port** [*port-number* | **default**]使能 IPv4 版本的 Telnet 服务器。
使能 IPv6 版本的 Telnet 服务器	1. 进入全局配置视图； 2. 执行命令 **telnet6d port** [*port-number* | **default**]使能 IPv6 版本的 Telnet 服务器。
使用 TFTP 协议将设备默认文件夹的内容导出到 PC 中	1. 进入全局配置视图； 2. 执行命令 **file export tftp** *ipv4-address remotedir localdir*。

1.5.2.4 TFTP Client 配置实例

 **注意：**

建议用户在技术人员的指导下进行该命令的操作。

目的

交换机作为 TFTP Client 实现配置文件的备份和和软件升级配置举例。

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

组网需求

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

组网图

图 1-26 TFTP 配置示意图

配置步骤

1) 在 PC 上启动了 TFTP Server，配置 TFTP Server 的工作目录；

2) 在交换机上配置。

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

```
CN12800#config
CN12800(config)#tftp get 1.1.1.2  switch.z
CN12800(config)#tftp put 1.1.1.2  vrpcfg.txt config
```

第2章 二层以太网配置

本章介绍了 CN12800 系列数据中心交换机二层以太基本功能配置。

2.1 以太网接口配置

介绍如何配置以太网接口。

2.1.1 以太网接口基本属性配置

2.1.1.1 进入以太网接口视图

背景信息

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

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
进入以太网接口视图	1. 进入全局配置视图； 2. 执行如下命令： ● **interface** { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number*； ● **interface eth-trunk** *trunk-number*。
退出以太网接口视图	1. 进入接口配置视图； 2. 执行命令 **quit**。
进入批量接口配置视图	1. 进入全局配置视图； 2. 执行命令 **interface** { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* **to** { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number*。
进入接口组配置视图	1. 进入全局配置视图； 2. 执行命令 **interface group** *port-list*。

2.1.1.2 打开/关闭以太网端口

背景信息

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

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
关闭以太网端口 当接口闲置时，即没有连接线缆进行工作时，请使用 shutdown 命令关闭该接口，以防止由于干扰导致接口异常情况的发生	1. 进入全局配置视图； 2. 进入接口配置视图（以太网、Trunk）、接口组配置视图、批量接口配置视图、VLANIF 配置视图； 3. 执行命令 **shutdown** 关闭当前以太网。
打开以太网端口 当修改了接口的属性参数，而新配置未能立即生效，可使用 shutdown 和 no shutdown 命令关闭和重启接口，使新配置生效	1. 进入全局配置视图； 2. 进入接口配置视图（以太网、Trunk）、接口组配置视图、批量接口配置视图、VLANIF 配置视图； 3. 执行命令 **no shutdown** 开启当前以太网。

2.1.1.3 设置以太网端口速率

背景信息

可以使用如下命令对以太网端口的速率进行设置。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
配置以太网接口速率	1. 进入全局配置视图； 2. 执行命令 **port mode** { **10gi** | **25gi** } **interface** { **10gigaethernet** | **25gigaethernet** } *interface-number* 设置端口的不同速率，25G 端口可修改为 10G。

2.1.1.4 设置以太网端口流量控制

背景信息

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

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

2.1.1.5 设置以太网端口的广播/组播报文的抑制功能

目的

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

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
配置以太网接口对广播、组播或未知单播报文进行风暴控制	1. 进入全局配置视图； 2. 进入接口配置视图（以太网接口、Trunk 接口）、接口组配置视图和批量接口配置视图； 3. 执行如下命令： ● **storm-control** { **broadcast** | **multicast** | **dlf** } **cir** { **gbps** | **kbps** | **mbps** } *cir-value* **cbs** { **bytes** | **kbytes** | **mbytes** } *cbs-value* ● **storm-control** { **broadcast** | **multicast** | **dlf** } **percent** *value*（只支持以太网接口配置视图） ● **storm-control** { **broadcast** | **multicast** | **dlf** } **pps** *pps-value*。
取消风暴控制功能	1. 进入全局配置视图； 2. 进入接口配置视图（以太网接口、Trunk 接口）、接口组配置视图和批量接口配置视图；

目的	步骤
	3. 执行命令 **no storm-control** { **broadcast** | **multicast** | **dlf** }。

2.1.1.6 设置以太网端口速率抑制功能

背景信息

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

步骤

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

2.1.1.7 设置以太网端口的最大传输单元

背景信息

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

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

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

2.1.1.8 清除当前接口的统计信息

目的

本操作适用于当一个接口配置视图下存在大量信息需要清除时。

步骤

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

2.1.1.9 清除指定接口的统计信息

目的

本操作适用于清除指定接口统计信息。

步骤

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
清除指定接口统计信息	1. 进入全局配置视图； 2. 执行如下命令清除指定接口统计信息： ● **reset counter interface eth-trunk** *trunk-number*； ● **reset counter interface eth-trunk** *trunk-number.sub-trunk-number*； ● **reset counter interface nve** *nve-id*； ● **reset counter interface bridge-domain** *bd-id*； ● **reset counter interface { ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number*；

目的	步骤
	● **reset counter interface all**。

2.1.1.10 描述以太网端口

目的

使用如下命令设置端口的描述字符串，以区分各个端口。

步骤

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

2.1.2 以太网接口高级属性配置

2.1.2.1 配置端口 CRC 检测

目的

使用以下的配置任务可以开启 CRC 错误报文超过阈值时，端口 error down 后自动恢复。

步骤

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
使能或去使能 CRC 错误报文超过阈值时，端口 error down	1. 进入以太网桥接接口配置视图、以太网路由接口配置视图、grp 桥接接口配置视图、grp 路由接口配置视图； 2. 执行命令 **port crc-error error-down** { **enable** | **disable** }。
配置 CRC 错误报文告警时间间隔	1. 进入全局配置视图 2. 执行命令 **crc-error protection interval** *interval*。
配置端口 CRC 错误报文告警阈值	1. 进入以太网桥接接口配置视图、以太网路由接口配置视图、grp 桥接接口配置视图、grp 路由接口配置视图； 2. 执行命令 **port crc-error threshold** *threshold*。

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

2.1.2.2 显示以太网端口状态

背景信息

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

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
显示以太网端口状态及相关信息	1. 进入特权用户视图、全局配置视图、普通用户视图、接口配置视图（以太网接口、trunk 接口）、接口组配置视图； 2. 执行如下命令： ● **show interface** ● **show interface** { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* ● **show interface** { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* **config** ● **show interface eth-trunk** *trunk-number* ● **show interface eth-trunk** *trunk-number* **config**。

目的	步骤
显示当前设备所有以太网接口及 trunk 接口（若已配置 trunk）的基本信息	1. 进入特权用户视图、全局配置视图、普通用户视图、接口配置视图（以太网接口、trunk 接口）、接口组配置视图； 2. 执行如下命令： ● **show interface eth-trunk** *trunk-number* **verbose** ● **show interface eth-trunk verbose** ● **show interface verbose**。
显示以太网接口及子接口的引用计数	1. 进入普通用户视图； 2. 执行如下命令： ● **show l3int ethernet** *interface-number* ● **show l3int ethernet** *interface-number.subinterface-number*。

2.1.2.3 切换不同以太网接口配置视图

目的

当配置完当前接口属性后需要配置其他接口属性可以使用本功能。

步骤

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
切换当前以太网接口配置视图到新的以太网接口视图	1. 进入全局配置视图； 2. 进入接口配置视图（以太网接口）； 3. 执行命令 **switch** { **ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number*。

2.1.3 维护及调试

目的

当以太网接口相关功能不正常，需要进行查看、定位问题时，可以使用本小节操作。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
查看硬件三层 BD 接口信息	1. 进入普通用户视图； 2. 执行命令 **show hwbd l3int** [*bd-id*] **slot** *slot-id*。

目的	步骤
查看指定槽位上三层主接口的接口信息	1. 进入普通用户视图； 2. 执行命令 **show hweth l3int** { **ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* **slot** *slot-id*。
查看指定槽位上三层子接口的接口信息	1. 进入普通用户视图； 2. 执行命令 **show hwsubeth l3int** { **ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* **slot** *slot-id*。
查看以太网接口的硬件状态	1. 进入普通用户视图； 2. 执行如下命令： ● **show hwport dcp interface status slot** *slot-id* ● **show hwport dcp interface status slot** *slot-id* **interface** { **ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number*。
查看备用主控上端口的管理状态、链路状态、双工速率、MTU、VLAN 信息	1. 进入普通用户视图； 2. 执行如下命令： ● **show hwport ha interface status slot** *slot-id* ● **show hwport ha interface status slot** *slot-id* **interface** { **ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number*。
查看指定槽位的聚合端口信息，包括 BD 信息、VLAN List 信息以及物理成员口信息	1. 进入普通用户视图； 2. 执行如下命令： ● **show hwtrunk** *trunk-number* **slot** *slot-id* **bd** ● **show hwtrunk** *trunk-number* **slot** *slot-id* **vlan** ● **show hwtrunk** *trunk-number* **verbose slot** *slot-id*。
查看指定槽位上所有 VLANIF 接口的三层接口信息	1. 进入普通用户视图； 2. 执行命令 **show hwvlan l3int slot** *slot-id*。
查看指定槽位上所有指定 VLAN 接口的三层接口信息	1. 进入普通用户视图； 2. 执行命令 **show hwvlan l3int** *vlan-id* **slot** *slot-id*。
查看协议栈指定 VLAN 接口的收发包统计信息	1. 进入普通用户视图； 2. 执行如下命令： ● **show l3int packet statistic interface vlan** *vlan-id* { **dot1x | test | dot3ah | lacp | stp-c | stp-p | gvrp | gmrp | udld | alb | rlink | g8031 | g8032 | rer | esr | pppoe+ | bpdu-tunnel | flush | bfd2 | iss | sgm | mpls | mlag | dcp | sync | ha | vlp | lldp-p | rip | ospf | bgp | pim | isis | vrrp | dhcp-server | bfd | ldp | ntp | igmp | arp | http | mlink | mad | dhcp-client | fip-snooping | rip6 | ospf6 | pim6 | dhcp6-server | bfd6 | ntp6 | mld | nd | http6 | arpmiss | vxlan | dhcp6client | syslog | smtp | telnet**

目的	步骤
	| ssh | telnet6 | ssh6 | snmp | snmp6 | icmp | icmp6 | ftp | tftp | trill | fcoe | y1731 | https | https6 | ftp6 | tftp6 | ip | ipv6 | udp | udp6 | tcp | tcp6 | fib-hit | fib-hit6 | ttl | nd-miss | ip2 | icmp2 | tftp2 | ftp2 | telnet2 | snmp2 } ● **show l3int packet statistic interface vlan** *vlan-id*。
重置协议栈指定 VLAN 接口的收发包统计信息	1. 进入 VLANIF 配置视图； 2. 执行如下命令： ● **reset l3int packet statistic** { **dot1x | test | dot3ah | lacp | stp-c | stp-p | gvrp | gmrp | udld | alb | rlink | g8031 | g8032 | rer | esr | pppoe+ | bpdu-tunnel | flush | bfd2 | iss | sgm | mpls | mlag | dcp | sync | ha | vlp | lldp-p | rip | ospf | bgp | pim | isis | vrrp | dhcp-server | bfd | ldp | ntp | igmp | arp | http | mlink | mad | dhcp-client | fip-snooping | rip6 | ospf6 | pim6 | dhcp6-server | bfd6 | ntp6 | mld | nd | http6 | arpmiss | vxlan | dhcp6client | syslog | smtp | telnet | ssh | telnet6 | ssh6 | snmp | snmp6 | icmp | icmp6 | ftp | tftp | trill | fcoe | y1731 | https | https6 | ftp6 | tftp6 | ip | ipv6 | udp | udp6 | tcp | tcp6 | fib-hit | fib-hit6 | ttl | nd-miss | ip2 | icmp2 | tftp2 | ftp2 | telnet2 | snmp2** } ● **reset l3int packet statistic all**。
导出指定槽位下的 BD 信息到文件	1. 进入普通用户视图； 2. 执行如下命令： ● **dump hwport bd slot** *slot-id* ● **dump hwport bd slot** *slot-id* **interface** { **ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number*。

2.2 MAC 表配置

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

对于目的 MAC 地址能够在 MAC 地址表中找到的报文，系统会直接使用硬件转发；对于目的 MAC 地址不能在地址表中查到的报文，系统对报文采用广播方式进行转发。如

果广播后，报文到达了目的 MAC 地址对应的网络设备，目的网络设备将应答此广播报文，应答报文中包含了此设备的 MAC 地址，交换机通过地址学习将新的 MAC 地址加入到 MAC 地址转发表中。去往同一目的 MAC 地址的后续报文，就可以利用该新增的 MAC 地址表项直接进行转发了。

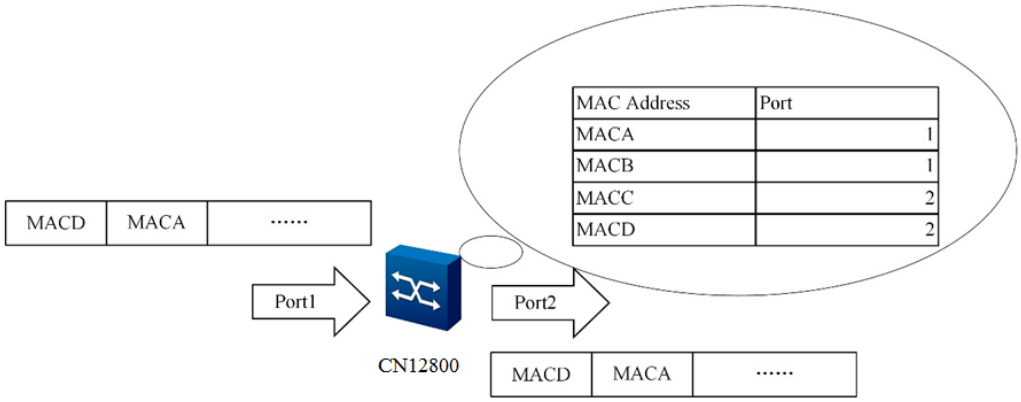


图 2-1 交换机利用转发表转发报文

2.2.1 设置 MAC 地址表项

目的

管理员根据实际情况可以手动添加、修改或删除 MAC 地址表中的表项。

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

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
添加黑洞 MAC 地址表项	1. 进入全局配置视图； 2. 执行命令 **mac-address blackhole** *vlan-id mac-address*。
删除黑洞 MAC 地址表项	1. 进入全局配置视图； 2. 执行如下命令： ● **no mac-address blackhole** ● **no mac-address blackhole** *mac-address* ● **no mac-address blackhole vlan** *vlan-id* ● **no mac-address blackhole vlan** *vlan-id mac-address*。
配置系统最大 MAC 地址学习限制	1. 进入接口配置视图（以太网接口）、接口组配置视图、VLAN 配置视图；

目的	步骤
	2. 执行如下命令： ● **mac-limit** { *limit-value* | **default** }； ● **mac-limit** { *limit-value* | **default** } **action { forward | drop }**。
添加设备静态 MAC 地址表项	1. 进入全局配置视图； 2. 执行如下命令： ● **mac-address static** *vlan-id mac-address* { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* ● **mac-address static** *vlan-id mac-address* **eth-trunk** *trunk-number*。
删除设备上静态 MAC 地址表项	1. 进入全局配置视图（第一条命令也可进入槽位节点视图执行）； 2. 执行如下命令： ● **no mac-address static** ● **no mac-address static vlan** *vlan-id* ● **no mac-address static** *mac-address* ● **no mac-address static vlan** *vlan-id mac-address* ● **no mac-address static { ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* ● **no mac-address static eth-trunk** *trunk-number*。
删除全局所有 MAC 地址表项，或根据 VLAN、VLAN+MAC 以及端口的方式来删除指定接口下的所有 MAC 地址表项	1. 进入以太网桥接接口配置视图、Trunk 接口配置视图； 2. 执行如下命令： ● **no mac-address** ● **no mac-address** { **dynamic** | **static** | **security** | **sticky** } ● **no mac-address** { **dynamic** | **static** | **security** | **sticky** } **vlan** *vlan-id* ● **no mac-address** { **dynamic** | **static** | **security** | **sticky** } **vlan** *vlan-id mac-address*。 或 1. 进入 Slot 配置视图； 2. 执行如下命令： ● **no mac-address all** ● **no mac-address** { **dynamic** | **static** }。

2.2.2 设置动态 MAC 地址老化时间

背景信息

设置合适的老化时间可以有效的实现 MAC 地址老化的功能。用户设置的老化时间过长或者过短，都可能导致交换机广播大量找不到目的 MAC 地址的数据报文，影响交换机的运行性能。如果用户设置的老化时间过长，交换机可能会保存许多过时的 MAC 地址

表项，从而耗尽 MAC 地址表资源，导致交换机无法根据网络的变化更新 MAC 地址表。如果用户设置的老化时间太短，交换机可能会删除有效的 MAC 地址表项。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

说明：

系统复位后，动态表项会丢失，而保存的静态表项和黑洞表项不会老化丢失。

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

2.2.3 配置 MAC 地址漂移检测

目的

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

背景信息

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

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

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

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

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

2.2.4 配置 MAC 地址学习或老化的告警功能

目的

本节介绍如何配置 MAC 地址学习或老化的告警功能。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

2.2.5 显示二层 MAC 地址表项

目的

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

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
显示指定项目的 MAC 地址的表项信息	1. 进入特权用户视图、全局配置视图、接口配置视图（以太网接口、trunk 接口）、普通用户视图、接口组配置视图； 2. 执行如下命令： ● **show mac-address vlan** *vlan-id* ● **show mac-address vsi** *vsi-name* ● **show mac-address [** *mac-address*] ● **show mac-address** *mac-address* **vlan** *vlan-id* ● **show mac-address { ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* ● **show mac-address eth-trunk** *trunk-number* ● **show mac-address** { **static** | **security** | **sticky** }。
显示基于接口、基于 VLAN 或基于槽位的 MAC 地址数量信息	1. 进入特权用户视图、全局配置视图、普通用户视图、接口配置视图（以太网接口、trunk 接口）、接口组配置视图； 2. 执行如下命令： ● **show mac-address total-number** ● **show mac-address total-number { ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* ● **show mac-address total-number eth-trunk** *trunk-number* ● **show mac-address total-number vlan** *vlan-id*。
显示基于接口、基于 VLAN 的动态 MAC 地址表项信息	1. 进入特权用户视图、全局配置视图、普通用户视图、接口配置视图（以太网接口、trunk 接口）、接口组配置视图； 2. 执行如下命令： ● **show mac-address dynamic { ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* ● **show mac-address dynamic eth-trunk** *trunk-number* ● **show mac-address dynamic vlan** *vlan-id*。
显示已配置的 MAC 地址学习限制规则	1. 进入特权用户视图、全局配置视图、普通用户视图、接口配置视图（以太网接口、trunk 接口）、VLAN 配置视图、接口组配置视图； 2. 执行如下命令： ● **show mac-limit** ● **show mac-limit interface** ● **show mac-limit interface { ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* ● **show mac-limit interface eth-trunk** *trunk-number* ● **show mac-limit config** ● **show mac-limit vlan** [*vlan-id*]

目的	步骤
	● **show mac-limit bridge-domain** [*bd-id*]。

2.2.6 维护及调试

目的

当 MAC 相关功能不正常，需要进行查看、定位问题时，可以使用本小节操作。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
打开或关闭 MAM 模块调试开关	1. 进入特权用户视图； 2. 执行命令 **debug mam** { **error** | **mac** | **flush** | **mac-limit** | **sync** | **hw** | **nm** | **event** | **if** | **history** | **aging** | **all** }或 **no debug mam** { **error** | **mac** | **flush** | **mac-limit** | **sync** | **hw** | **nm** | **event** | **if** | **history** | **aging** | **all** }。
查看 MAC 地址基本信息	1. 进入普通用户视图； 2. 执行命令 **show mac info**。
查看 MAC 地址管理模块的各种错误统计信息	1. 进入普通用户视图； 2. 执行命令 **show mam error**。
查看硬件 MAC 地址信息	1. 进入普通用户视图； 2. 执行如下命令： ● **show hwmac slot** ● **show hwmac slot** *slot-id* [**age**] ● **show hwmac slot** *slot-id* **{ ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* **bridge-domain** *bd-id* ● **show hwmac slot** *slot-id* **{ ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* **vlan** *vlan-id* ● **show hwmac slot** *slot-id mac-address* **bridge-domain** *bd-id* ● **show hwmac slot** *slot-id mac-address* **vlan** *vlan-id* ● **show hwmac slot** *slot-id* **bridge-domain** *bd-id* ● **show hwmac slot** *slot-id* **error** ● **show hwmac slot** *slot-id* **vlan** *vlan-id*。
导出指定槽位硬件 MAC 地址表信息到文件	1. 进入普通用户视图； 2. 执行命令 **dump hwmac slot** *slot-id*。

目的	步骤
导出 MAC 管理模块记录的 MAC 表、接口表信息	1. 进入普通用户视图； 2. 执行命令 **dump ha mac-table** { **mac** | **if** | **all** }导出 MAC 管理模块记录的 MAC 表、接口表信息。根据导出的信息判断设备两块主控卡上表项是否一致。

2.3 ARP 配置

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

2.3.1 手工添加/删除静态 ARP 映射项

目的

本节介绍如何手工添加/删除静态 ARP 映射项。

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

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
添加静态 ARP 映射表项	1. 进入全局配置视图； 2. 执行如下命令： ● **ip arp** *ip-address mac-address* { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* ● **ip arp** *ip-address mac-address* { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* **vpn-instance** *name* ● **ip arp** *ip-address mac-address* **eth-trunk** *trunk-number* ● **ip arp** *ip-address mac-address* **eth-trunk** *trunk-number* **vpn-instance** *name* ● **ip arp** *ip-address mac-address* **vlan** *vlan-id* ● **ip arp** *ip-address mac-address* **vlan** *vlan-id* **vpn-instance** *name* ● **ip arp** *ip-address mac-address* **vlan** *vlan-id* **inner-vlan** *inner-vid*

目的	步骤
	● **ip arp** *ip-address mac-address* **vlan** *vlan-id* **inner-vlan** *inner-vid* **vpn-instance** *name* ● **ip arp** *ip-address mac-address* ● **ip arp** *ip-address mac-address* **vpn-instance** *name*。
删除静态 ARP 映射表项	1. 进入全局视图； 2. 执行如下命令： ● **no ip arp** *ip-address* ● **no ip arp** *ip-address* **vpn-instance** *name*。

2.3.2 清除动态 ARP 表项

目的

本节介绍如何清除动态 ARP 映射表项。

本节帮助用户可以在需要的时候手动删除设备的所有动态 ARP 映射表项。

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

过程

根据不同目的，执行相应步骤，具体参见下表。

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

2.3.3 查看 ARP 的信息

目的

本节介绍如何查看 ARP 相关信息。本节帮助用户通过查看局域网的 ARP 映射表后，来进行局域网的故障检测。ARP 在网络地址和本地网硬件地址之间建立了对应关系。每一个对应项记录在缓存中保持一段时间，在一段时间后没有收到更新报文，则老化这种对应关系。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤

显示当前所有 VLAN 的 ARP 学习模式	1. 进入普通用户视图； 2. 执行命令 **show arp learning strict**。
显示 ARP 相关信息，包括 ARP 动态地址统计、ARP 映射表项的老化时间等。同时也支持多实例 VPN 情况下配置	1. 进入普通用户视图； 2. 执行如下命令： ● **show ip arp** ● **show ip arp** *ip-address* ● **show ip arp dynamic** ● **show ip arp static** ● **show ip arp error statistic** ● **show ip arp { ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* ● **show ip arp eth-trunk** *trunk-number* ● **show ip arp vpn-instance** *name*。
显示各接口下可以学习的最大动态 ARP 映射表项数目	1. 进入普通用户视图； 2. 执行如下命令： ● **show arp-limit maxnum vlan** *vlan-id* ● **show arp-limit maxnum { ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* ● **show arp-limit maxnum eth-trunk** *turnk-number* ● **show arp-limit maxnum**。

2.3.4 配置动态 ARP 映射表项老化时间

目的

本节介绍如何配置动态 ARP 映射表项的老化时间。

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

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

2.3.5 配置 ARP 学习功能

目的

本节介绍如何配置 ARP 学习功能。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置 ARP 严格学习功能	方法一： 1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **arp learning strict** { **enable** | **disable** }。 方法二： 1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图； 3. 执行命令 **arp learning strict** { **force-enable** | **force-disable** | **trust**}。

2.3.6 维护及调试

目的

当 ARP 功能不正常，需要进行查看、定位问题时，可以使用本小节操作。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
重置协议栈 ARP 错误统计信息	1. 进入全局配置视图； 2. 执行命令 **reset ip arp error statistic**。
查看硬件 ARP 下发错误统计信息	1. 进入普通用户视图； 2. 执行命令 **show hw arp error statistic slot** *slot-id*。
将协议栈当前的 ARP 表项信息写入文件	1. 进入普通用户视图； 2. 执行命令 **dump ha arp-table**。

2.4 链路聚合配置

2.4.1 端口汇聚简介

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

目前 CN12800 只支持手工汇聚和静态 LACP 汇聚功能。

2.4.2 配置汇聚组功能

 注意：

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

或在 Trunk 视图下执行命令 **remove** { **ethernet** | **gigaethernet** | **xgigaethernet**| **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number*。

目的

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

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
创建 eth-trunk 并进入其配置视图	1. 进入全局配置视图； 2. 执行命令 **interface eth-trunk** *trunk-number* 创建汇聚组并进入其配置视图，若待创建的组已存在，则直接进入其配置视图。
配置 eth-trunk 的工作模式	1. 进入全局配置视图； 2. 进入 Trunk 接口配置视图； 3. 执行命令 **mode** { **manual** | **lacp-static** }配置 eth-trunk 的工作模式。
向 eth-trunk 中加入成员接口	方法一： 1. 进入全局配置视图； 2. 进入 Trunk 接口配置视图； 3. 执行命令 **add** { **ethernet** | **gigaethernet** | **xgigaethernet**| **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number* 增加成员接口。 方法二： 1. 进入全局配置视图； 2. 进入接口配置视图、接口组配置视图； 3. 执行命令 **join eth-trunk** *trunk-number*，将当前接口加入 eth-trunk。
（可选）配置活动接口数阈值	配置活动接口数上限阈值： 1. 进入全局配置视图；

目的	步骤
	2. 进入 Trunk 接口配置视图； 3. 执行命令 **active-linknumber max** { *max-number* | **default** } ，配置链路聚合活动接口数上限阈值。 配置活动接口数下限阈值： 1. 进入全局配置视图； 2. 进入 Trunk 接口配置视图； 3. 执行命令 **active-linknumber min** { *min-number* | **default** }，配置链路聚合活动接口数下限阈值。
（可选）配置系统 LACP 优先级	1. 进入全局配置视图； 2. 执行命令 **lacp system-priority** { *priority* | **default** }，配置当前设备的系统 LACP 优先级。
移除 Trunk 接口配置视图下的成员接口	1. 进入全局配置视图； 2. 进入 Trunk 接口配置视图； 3. 执行如下命令： ● **remove** { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* ● **remove** { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* **to** { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number*。
配置 LACP 模式下 Eth-Trunk 接口接收 LACP 协议报文的超时时间	1. 进入全局配置视图； 2. 进入 Trunk 接口配置视图； 3. 执行命令 **lacp timeout** *timeout-value* 配置 LACP 模式下 Eth-Trunk 接口接收 LACP 协议报文的超时时间。
配置当前 LACP 聚合组端口号整体偏移量	1. 进入 Trunk 接口配置视图； 2. 执行命令 **lacp port-id extension** { *ex-value* | **default** }。
配置 trunk 接口的 LACP 系统 ID	1. 进入 Trunk 接口配置视图； 2. 执行命令 **lacp system-id** *system-id-address*。

2.4.3 配置增强负载分担

目的

使用本节操作配置增强负载分担功能。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

2.4.4 维护及调试

目的

当 LACP 功能不正常，需要进行查看、定位问题时，可以使用本小节操作。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
查看 LACP 配置文件信息	1. 进入普通用户视图； 2. 执行命令 **show lacp config** 显示 LACP 汇聚配置文件的信息。
查看 LACP 全部或指定组信息	1. 进入普通用户视图； 2. 执行命令 **show lacp eth-trunk** [*trunk-number*] 显示指定的 LACP 汇聚组或全部 LACP 汇聚组的状态信息。

目的	步骤
查看 LACP 协议相关配置信息	1. 进入普通用户视图； 2. 执行命令 **show lacp system** 显示 LACP 协议相关配置信息。
查看所有 LACP 成员口收发包统计信息	1. 进入普通用户视图； 2. 执行命令 **show lacp statistic** 查看所有 LACP 成员口收发包统计信息。
查看 LACP 模式下的 LACP 报文收发统计信息	1. 进入普通用户视图； 2. 执行命令 **show lacp statistic interface eth-trunk** *trunk-number* 查看 LACP 模式下的 LACP 报文收发统计信息。
查看接口的属性配置情况及相关信息	1. 进入普通用户视图； 2. 执行如下命令： ● **show interface eth-trunk** *trunk-number* ● **show interface eth-trunk** *trunk-number* **config**。
查看 trunk 接口的相关配置信息	1. 进入普通用户视图； 2. 执行如下命令： ● **show interface eth-trunk** *trunk-number* **verbose** ● **show interface eth-trunk verbose** ● **show interface eth-trunk** *trunk-number* ● **show interface eth-trunk** *trunk-number* **config**。
查看接口的统计信息	1. 进入普通用户视图； 2. 执行如下命令： ● **show interface statistic brief eth-trunk** *trunk-number* ● **show interface statistic eth-trunk** *trunk-number*。
查看 trunk 接口的引用计数	1. 进入普通用户视图； 2. 执行命令 **show l3int eth-trunk** *trunk-number*。
打开或关闭负载分担模板调试信息	1. 进入特权用户视图； 2. 执行如下命令： ● **debug schedule-profile** { **config** | **event** | **all** } ● **no debug schedule-profile** { **config** | **event** | **all** }。
查看增强负载分担模板的详细信息	1. 进入普通用户视图； 2. 执行如下命令： ● **show schedule-profile** ● **show schedule-profile** *profile-name*。
打开或关闭 LACP 模块的相关调试开关	1. 进入特权用户视图； 2. 执行如下命令： ● **debug lacp** { **timer** | **event** | **churn** | **mux** | **rx** | **tx** | **config** | **logic** | **sync** | **all** } ● **no debug lacp** { **timer** | **event** | **churn** | **mux** | **rx** | **tx** | **config** | **logic** | **sync** | **all** }。

目的	步骤
清除所有接口统计的 lacp（链路汇聚协议信息）	1. 进入全局配置视图； 2. 执行如下命令 **reset lacp statistic** 清除所有接口统计的 lacp（链路汇聚协议信息）。
清除接口统计的链路汇聚协议信息	1. 进入全局配置视图； 2. 执行如下命令 **reset lacp statistic interface** { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* 清除接口统计的链路汇聚协议信息。
清除 trunk 接口统计的链路汇聚协议信息	1. 进入全局配置视图； 2. 执行如下命令 **reset lacp statistic interface eth-trunk** *trunk-number* 清除 trunk 接口统计的链路汇聚协议信息。

2.4.5 链路聚合典型举例

组网要求

在两台直接相连 CN12800 设备上配置链路聚合组，提高两设备之间的带宽与可靠性，具体要求如下：

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

组网图

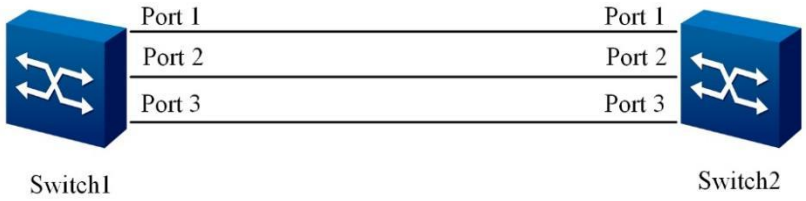


图 2-2 链路聚合配置拓扑图

配置步骤

注：两端配置一致，这里仅列出一端配置。

```
1．创建链路聚合组
CN12800(config)#interface eth-trunk 1
CN12800(config-eth-trunk-1)#no shutdown
CN12800(config-eth-trunk-1)#mode lacp-static
2．接口 1-3 加入汇聚组
```

```
CN12800(config)#interface 10gigaethernet 1/0/1 to 10gigaethernet 1/0/3
CN12800(config-10ge1/0/1->xge1/0/3)#no shutdown
CN12800(config-10ge1/0/1->xge1/0/3)#join eth-trunk 1
```

3. 配置结束，查看汇聚组的信息

```
CN12800#show lacp eth-trunk 1
eth-trunk 1:
        LACP Status: master        Port number: 3

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

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

gigaethernet-1/0/3
 Port Status: Up and bind
 Flag: S – Device is sending Slow LACPDUs
       F – Device is sending fast LACPDUs
 Local information:
        Mode      Flags    Priority   AdminKey   OperKey    PortId   State
        active    F        32768      0x19       0x19       0x3      0xa9d7f8
```

```
Partner's information:
        Port                Flags   SysPri   PortPri   AdminKey   OperKey   OperPort
OperState DevID
        3                   F       32768    32768     0x0        0x19      0x3
0x9dfb6c    0x00046798185d
```

2.5 VLAN 配置

2.5.1 VLAN 概述

VLAN 的含义

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

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

VLAN 的功能

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

2.5.2 创建 VLAN

目的

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

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
创建 VLAN 并进入 VLAN 视图	1. 进入全局配置视图； 2. 执行命令 **vlan** *vlan-id1* [*vlan-id2*] 创建一个或多个 VLAN 并进入 VLAN 视图。
创建并进入 VLANIF 接口配置视图	1. 进入全局配置视图； 2. 执行命令 **interface vlan** *vlan-id* 创建并进入 VLANIF 接口配置视图。

目的	步骤
创建 VLAN 并进入 VLAN 视图	1. 进入全局配置视图； 2. 执行命令 **vlan** *vlan-id1* [*vlan-id2*] 创建一个或多个 VLAN 并进入 VLAN 视图。
删除已创建的 VLANIF	1. 进入全局配置视图； 2. 执行命令 **no vlan** *vlan-id* 删除指定 VLANIF 接口配置视图。
删除一个或者批量删除多个 VLAN	1. 进入全局配置视图； 2. 执行命令 **no vlan** *vlan-id1* [*vlan-id2*]用来删除一个或者批量删除多个 VLAN。
切换 VLAN 配置视图	1. 进入全局配置视图； 2. 执行命令 **vlan** *vlan-id1* [*vlan-id2*] 创建一个或多个 VLAN 并进入 VLAN 视图； 3. 执行命令 **switch vlan** *vlan-id* 在 VLAN 配置视图下创建其他 VLAN，并进入所创建的 VLAN 配置视图。

2.5.3 配置基于接口的 VLAN

目的

使用本节操作配置基于接口的 VLAN。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
配置接口的缺省 VLAN 并同时加入此 VLAN	1. 进入全局配置视图； 2. 进入接口组配置视图（以太网接口、trunk 接口）； 3. 执行命令 **port link-type** *type* 将 link-type 配置为 access 或 dot1q-tunnnel 类型； 4. 执行命令 **port default vlan** *vlan-id* 配置接口的缺省 VLAN 并同时加入此 VLAN。
配置 Hybrid 类型接口所属 VLAN	1. 进入全局配置视图； 2.进入接口组配置视图（以太网接口、trunk 接口）； 3. 执行命令 **port hybrid vlan** *vlan-list* { **tagged** | **untagged** }配置 Hybrid 类型接口所属 VLAN。
配置 Hybrid 类型接口的缺省 VLAN	1. 进入全局配置视图； 2. 进入接口组配置视图（以太网接口、trunk 接口）； 3. 执行命令 **port hybrid pvid** { *vlan-id* | **default** }配置 Hybrid 类型接口的缺省 VLAN。

目的	步骤
配置接口的链路类型，也即接口类型	1. 进入全局配置视图； 2. 进入接口组配置视图（以太网接口、trunk 接口）； 3. 执行命令 **port link-type** { **access** | **trunk** | **hybrid** | **default** }配置接口的链路类型。
配置 Trunk 类型接口的缺省 VLAN	1. 进入全局配置视图； 2. 进入接口组配置视图（以太网接口、trunk 接口）； 3. 执行命令 **port trunk pvid** { *vlan-id* | **default** }配置 Trunk 类型接口的缺省 VLAN。
配置 Trunk 类型接口加入 VLAN	1. 进入全局配置视图； 2. 进入接口组配置视图（以太网接口、trunk 接口）； 3. 执行命令 **port trunk allow-pass vlan all** 配置 Trunk 类型接口加入 VLAN。

2.5.4 配置 VLAN 其他参数

目的

使用本节操作配置 VLAN 相关的其他参数，用户根据实际情况选配。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
配置 VLANIF 接口的描述信息	1. 进入全局配置视图； 2. 执行命令 **interface vlan** *vlan-id* 创建并进入 VLANIF 接口配置视图； 3. 执行命令 **alias** *description* 配置 VLANIF 接口的描述信息。
配置 VLAN 的描述信息	1. 进入全局配置视图； 2. 执行命令 **vlan** *vlan-id1* [*vlan-id2*]创建一个或多个 VLAN 并进入 VLAN 视图； 3. 执行命令 **alias** *description* 配置 VLAN 的描述信息。
配置在 VLAN 转发过程中对未知单播包的处理	1. 进入全局配置视图； 2. 执行命令 **vlan** *vlan-id1* [*vlan-id2*]创建一个或多个 VLAN 并进入 VLAN 视图； 3. 执行命令 **unknown-unicast** { **forward** | **drop** }用来配置在 VLAN 转发过程中对未知单播包的处理。
配置在 VLAN 转发过程中对未知单播包的处理	1. 进入全局配置视图； 2. 执行如下命令配置在 VLAN 转发过程中对未知单播包的处理： ● **unknown-unicast vlan** *vlan-list* { **forward** | **drop** } ● **vlan** *vlan-id* **unknown-unicast** { **forward** | **drop** }。

目的	步骤
配置三层接口延时 UP 的时间	1. 进入以太网路由接口配置视图、VLAN 接口配置视图、BD 接口配置视图； 2. 执行命令 **protocol up-delay-time** { *time* | **default** }。

2.5.5 维护及调试

目的

当 VLAN 功能不正常，需要进行查看、定位问题时，可以使用本小节操作。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
查看 VLAN 接口配置信息	1. 进入普通用户视图； 2. 执行 **show interface vlan config** 命令查看 VLAN 接口配置信息。
查看 VLAN 的相关信息	1. 进入普通用户视图； 2. 执行如下命令查看 VLAN 的相关信息： ● **show vlan** ● **show vlan all** ● **show vlan all** *vlan-list* ● **show vlan property** ● **show vlan property** *vlan-list* ● **show vlan verbose** ● **show vlan** *vlan-id* **verbose**。
查看槽位上各端口的 VLAN 信息	1. 进入普通用户视图； 2. 执行命令 **show hwport ha vlan mpu slot** { *slot-id* | **all** }。
查看物理端口的 VLAN List 信息	1. 进入普通用户视图； 2. 执行如下命令： ● **show hwport vlan slot** *slot-id* ● **show hwport vlan slot** *slot-id* **interface** { **ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* ● **show hwport vlan slot all**。

2.5.6 配置举例

组网要求

某企业用户，研发部和市场的员工电脑和部门服务器分别使用交换机 CN12800-1 和 CN12800-2 互连。现要求研发部的员工电脑能访问部门服务器 Server1，市场部的员工电脑能访问部门服务器 Server2，两个部门间不允许相互通信。

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

组网图

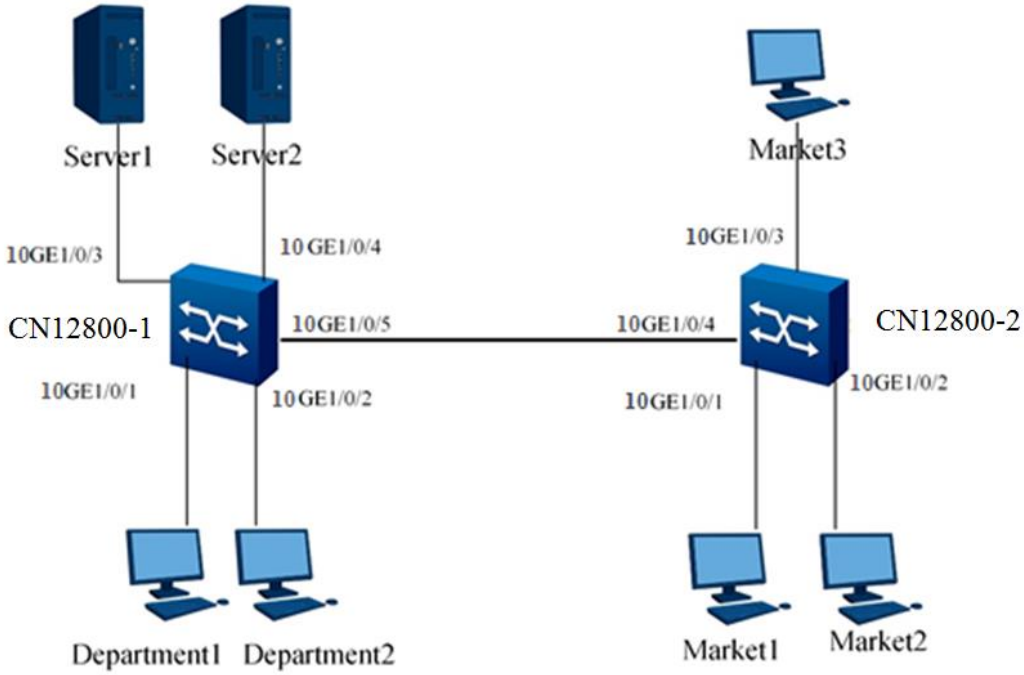


图 2-3 VLAN 配置拓扑图

配置步骤

1、配置 CN12800-1。

CN12800-1#configure

%Enter configuration commands.End with Ctrl+Z or command “quit” & “end”

#创建 VLAN100 并进入其配置视图。

CN12800-1(config)#interface vlan 100

CN12800-1(config-vlan-100)#

#配置 VLAN100 描述信息为 Development100。

CN12800-1(config-vlan-100)#description Development100

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

CN12800-1(config-vlan-100)#quit

CN12800-1(config)#

CN12800-1(config)#interface 10gigaethernet 1/0/1

CN12800-1(config-10ge1/0/1)#port hybrid vlan 100 untagged

CN12800-1(config-10ge1/0/1)#port hybrid pvid 100

CN12800-1(config-10ge1/0/1)#quit

CN12800-1(config)#interface 10gigaethernet 1/0/2

CN12800-1(config-10ge1/0/2)#port hybrid vlan 100 untagged

CN12800-1(config-10ge1/0/2)#port hybrid pvid 100

CN12800-1(config-10ge1/0/2)#quit

CN12800-1(config)#interface 10gigaethernet 1/0/3

CN12800-1(config-10ge1/0/3)#port hybrid vlan 100 untagged

CN12800-1(config-10ge1/0/3)#port hybrid pvid 100

CN12800-1(config-10ge1/0/3)#quit

CN12800-1(config)#

#创建 VLAN200 并进入其视图。

CN12800-1(config)#interface vlan 200

CN12800-1(config-vlan-200)#

#配置 VLAN200 描述信息为 Market200。

CN12800-1(config-vlan-200)#description Market200

#向 VLAN200 中加入端口 10gigaethernet1/0/4、10gigaethernet1/0/5，并设置 VLAN200 为端口 10gigaethernet1/0/4、10gigaethernet1/0/5 的 PVID 值。

CN12800-1(config-vlan-100)#quit

CN12800-1(config)#

CN12800-1(config)#interface 10gigaethernet 1/0/4

CN12800-1(config-10ge1/0/4)#port hybrid vlan 200 untagged

CN12800-1(config-10ge1/0/4#port hybrid pvid 200

CN12800-1(config-10ge1/0/4)#quit

CN12800-1(config)#interface 10gigaethernet 1/0/5

CN12800-1(config-10ge1/0/5)#port hybrid vlan 200 tagged

CN12800-1(config-10ge1/0/5)#port hybrid pvid 200

CN12800-1(config-10ge1/0/5)#quit

2、配置 CN12800-2。

#创建 VLAN200 并进入其配置视图。

CN12800-2#configure

%Enter configuration commands.End with Ctrl+Z or command “quit” & “end”

CN12800-2(config)#interface vlan 200

#配置 VLAN200 描述信息为 Market200。

CN12800-2(config-vlan-200)#description Market200

#向 VLAN200 中加入端口 10gigaethernet1/0/1、10gigaethernet1/0/2、10gigaethernet1/0/3 和 10gigaethernet1/0/4，并设置 VLAN200 为端口 10gigaethernet1/0/1、10gigaethernet1/0/2 和 10gigaethernet1/0/3 的 PVID 值。

CN12800-2(config-vlan-200)#quit

CN12800-2(config)#

CN12800-2(config)#interface 10gigaethernet 1/0/1

CN12800-2(config-10ge1/0/1)#port hybrid vlan 200 untagged

CN12800-2(config-10ge1/0/1)#port hybrid pvid 200

CN12800-2(config-10ge1/0/1)#quit

CN12800-2(config)#interface 10gigaethernet 1/0/2

CN12800-2(config-10ge1/0/2)#port hybrid vlan 200 untagged

CN12800-2(config-10ge1/0/2)#port hybrid pvid 200

CN12800-2(config-10ge1/0/2)#quit

CN12800-2(config)#interface 10gigaethernet 1/0/3

CN12800-2(config-10ge1/0/3)#port hybrid vlan 200 untagged

CN12800-2(config-10ge1/0/3)#port hybrid pvid 200

CN12800-2(config-10ge1/0/3)#quit

CN12800-2(config)#interface 10gigaethernet 1/0/4

CN12800-2(config-10ge1/0/4)#port hybrid vlan 200 tagged

CN12800-2(config-10ge1/0/4)#quit

CN12800-2(config)#

2.6 VLAN Mapping 配置

2.6.1 VLAN Mapping 简介

VLAN Mapping 即 VLAN 映射，它通过替换数据帧中的内外层 VLAN Tag 来实现用户 VLAN 与运营商 VLAN 的相互映射。通过替换 VLAN Tag 实现 VLAN 汇聚功能，使用户业务按照运营商的网络规划进行传输。

VlanMapping 功能是直接配置在端口上，这一点与旧的 Vlan 翻译模块先要创建 Vlan 翻译条目后，再将该条目与端口绑定不同。VlanMapping 只能修改 Vlan 标签，不能添加或者删除 Vlan 标签。

VlanMapping 协议具体支持的基本功能如下：

- 匹配外层 VID 修改外层 Tag
- 匹配外层 VID 范围修改外层 Tag
- 匹配外层 VID 和内层 VID 修改内外层 Tag
- 匹配外层 VID 和内层 VID 修改外层 Tag
- 匹配外层优先级修改外层 Tag
- 匹配外层 VID 和外层优先级修改外层 Tag
- 匹配外层 VID 范围和外层优先级修改外层 Tag
- 匹配内层 VID 修改内层 Tag

2.6.2 配置 VLAN Mapping

目的

使用本节操作配置 VLAN Mapping。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置 1：1 的 VLAN 转换条目，并且可以匹配数据包中外层 VLANID 来修改转发数据包的外层 VLANID 和优先级	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface** { **gigaethernet** | **xgigaethernet** } *interface-number* 或 **interface eth-trunk** *trunk-number* 进入接口配置视图或者进入接口组配置视图 3. 执行 **vlan-mapping enable** 命令，使能 vlan-map；

目的	步骤
	4. 执行如下命令： ● **vlan-mapping vlan** *outside-vlan-id* **map-vlan** outside-mapping-vlan-id ● **vlan-mapping vlan** *outside-vlan-id* **map-vlan** *outside-mapping-vlan-id* **remark-8021p** priority。
配置 N:1 的 VLAN 转换条目，其中 N:1 的方式是将指定范围的多个用户侧 VLANID 标签映射到一个网络侧 VLANID 标签，并且可以匹配数据包中外层 VLANID 来修改转发数据包的外层 VLANID 和优先级	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface** { **gigaethernet** | **xgigaethernet** } *interface-number* 或 **interface eth-trunk** *trunk-number* 进入接口配置视图或者进入接口组配置视图； 3. 执行 **vlan-mapping enable** 命令，使能 vlan-map； 4. 执行如下命令： ● **vlan-mapping vlan** *outside-vlan-id1* **to** *outside-vlan-id2* **map-vlan** *outside-mapping-vlan-id* ● **vlan-mapping vlan** *outside-vlan-id1* **to** outside-vlan-id2 **map-vlan** *outside-mapping-vlan-id* **remark-8021p** *priority*。
对经过端口的单个 vlan 数据帧配置该端口所属 VLAN 的二层标签，形成双层标签，即为转发数据包添加外层 VLANID 或外层 VLANID 和优先级	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface** { **gigaethernet** | **xgigaethernet** } *interface-number* 或 **interface eth-trunk** *trunk-number* 进入接口配置视图或者进入接口组配置视图； 3. 执行 **vlan-stacking enable** 命令，使能 vlan 堆叠功能； 4. 执行如下命令： ● **vlan-stacking vlan** *stacking-vlan-id* **stack-vlan** *stacking-mapping-vlan-id* ● **vlan-stacking vlan** *stacking-vlan-id* **8021p** *priority* **stack-vlan** *stacking-mapping-vlan-id*。
对经过端口的 N:1 的 vlan 数据帧配置该端口所属 vlan 的二层标签，其中 N:1 的方式是将多个 vlan 数据标签映射到该端口所属 vlan 的外层标签，形成双层标签，即为转发数据包添加外层 VLANID 或外层 VLANID 和优先级	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface** { **gigaethernet** | **xgigaethernet** } *interface-number* 或 **interface eth-trunk** *trunk-number* 进入接口配置视图或者进入接口组配置视图； 3. 执行 **vlan-stacking enable** 命令，使能 vlan 堆叠功能； 4. 执行如下命令： ● **vlan-stacking vlan** *stacking-vlan-id1* **to** *stacking-vlan-id2* **stack-vlan** *stacking-mapping-vlan-id* ● **vlan-stacking vlan** *stacking-vlan-id1* **8021p** *priority* **to** *priority* **stack-vlan** *stacking-mapping-vlan-id*。
匹配数据包中外层 VLANID 和内层 VLANID 来修改转发数据包的外层 VLANID 和优先级，并且可以匹配数据包中外层 VLANID 来修改转发	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface** { **gigaethernet** | **xgigaethernet** } *interface-number* 或 **interface eth-trunk** *trunk-number* 进入接口配置视图或者进入接口组配置视图； 3. 执行 **vlan-mapping enable** 命令，使能 vlan-map；

目的	步骤
数据包的外层 VLANID 和优先级	4. 执行如下命令： ● **vlan-mapping vlan** *outside-vlan-id* **inner-vlan** *inner-vlan-id* **map-vlan** *outside-mapping-vlan-id* ● **vlan-mapping vlan** *outside-vlan-id* **inner-vlan** *inner-vlan-id* **map-vlan** *outside-mapping-vlan-id* **map-inner-vlan** *outside-mapping-vlan-id* ● **vlan-mapping vlan** *outside-vlan-id* **inner-vlan** *inner-vlan-id* **map-vlan** *outside-mapping-vlan-id* **remark-8021p** *priority* ● **vlan-mapping vlan** *outside-vlan-id* **inner-vlan** *inner-vlan-id* **map-vlan** *outside-mapping-vlan-id* **map-inner-vlan** *outside-mapping-vlan-id* **remark-8021p** *priority*。
匹配数据包中外层 VLANID 和 N:1 的内层 VLANID 来修改转发数据包的外层 VLANID 和优先级，其中 N:1 的方式是将多个内层 VLANID 映射到该端口所属 vlan 的外层标签，并且可以匹配数据包中内外层 VLANID 来修改转发数据包的外层 VLANID 和优先级	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface** { **gigaethernet** | **xgigaethernet** } *interface-number* 或 **interface eth-trunk** *trunk-number* 进入接口配置视图或者进入接口组配置视图； 3. 执行 **vlan-mapping enable** 命令，使能 vlan-map； 4. 执行如下命令： ● **vlan-mapping vlan** *outside-vlan-id* **inner-vlan** *inner-vlan-id1* **to** *inner-vlan-id 2* **map-vlan** *outside-mapping-vlan-id* ● **vlan-mapping vlan** *outside-vlan-id* **inner-vlan** *inner-vlan-id1* **to** *inner-vlan-id 2* **map-vlan** *outside-mapping-vlan-id* **remark-8021p** *priority*。
删除所有配置的 VLAN 转换条目	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface** { **gigaethernet** | **xgigaethernet** } *interface-number* 或 **interface eth-trunk** *trunk-number* 进入接口配置视图或者进入接口组配置视图； 3. 执行命令 **no vlan-mapping all**。
删除指定的 VLAN 转换条目	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface** { **gigaethernet** | **xgigaethernet** } *interface-number* 或 **interface eth-trunk** *trunk-number* 进入接口配置视图或者进入接口组配置视图； 3. 执行如下命令： ● **no vlan-mapping vlan** *outside-vlan-id* **inner-vlan** *inner-mapping-vlan-id* ● **no vlan-mapping vlan** *outside-vlan-id* **inner-vlan** *inner--mapping-vlan-id1* **to** *inner--mapping-vlan-id2* ● **no vlan-mapping vlan** *outside-vlan-id* **to** *outside-mapping-vlan-id*。
在流行为中配置替换报文的 VLAN ID 的动作	1. 执行命令 **configure** 进入全局配置视图；

目的	步骤
	2. 执行命令 **interface** { **gigaethernet** | **xgigaethernet** } *interface-number* 或 **interface eth-trunk** *trunk-number* 进入接口配置视图或者进入接口组配置视图； 3. 执行 **vlan-mapping enable** 命令，使能 vlan-map； 4. 执行如下命令： ● **vlan-mapping inner-vlan** *outside-vlan-id* **map-inner-vlan** *outside-mapping-vlan-id* ● **vlan-mapping inner-vlan** *outside-vlan-id* **map-inner-vlan** *outside-mapping-vlan-id* **remark-8021p** *priority* ● **vlan-mapping inner-vlan** *outside-vlan-id1* **to** *outside-vlan-id2* **map-inner-vlan** *inner-mapping-vlan-id* ● **vlan-mapping inner-vlan** *outside-vlan-id1* **to** *outside-vlan-id2* **map-inner-vlan** *inner-mapping-vlan-id* **remark-8021p** *priority* ● **vlan-mapping inner-vlan** *outside-vlan-id1* **to** *outside-vlan-id2* **map-vlan** *mapping-vlan-id*。
匹配内外层 VID，修改转发数据包内外层 Tag 和优先级	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface** { **gigaethernet** | **xgigaethernet** } *interface-number* 或 **interface eth-trunk** *trunk-number* 进入接口配置视图或者进入接口组配置视图； 3. 执行如下命令： ● **vlan-mapping vlan** *outside-vlan-id* **inner-vlan** *inner-vlan-id* **map-vlan** *outside-mapping-vlan-id* **map-inner-vlan** *inner-mapping-vlan-id* ● **vlan-mapping vlan** *outside-vlan-id* **inner-vlan** *inner-vlan-id* **map-vlan** *outside-mapping-vlan-id* **map-inner-vlan** *inner-mapping-vlan-id* **remark-8021p priority**。

2.6.3 维护及调试

目的

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

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
打开 VLAN 转换调试功能	1. 不执行任何命令保持当前特权用户视图； 2. 执行命令 **debug vlan-mapping**。

目的	步骤
关闭 VLAN 转换调试功能	1. 不执行任何命令保持当前特权用户视图； 2. 执行命令 **no debug vlan-mapping**。
显示 VLAN 转换的信息，包括：配置信息，接口信息	1. 执行任何命令进入普通用户视图、特权用户视图、全局配置视图、接口配置视图（以太网接口）； 2. 执行如下命令； ● **show vlan-mapping** ● **show vlan-mapping config** ● **show vlan-mapping interface** { **ethernet** | **gigaethernet** | **xgigaethernet**| **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number* ● **show vlan-mapping interface eth-trunk** *trunk-number*。

2.6.4 配置举例

组网图

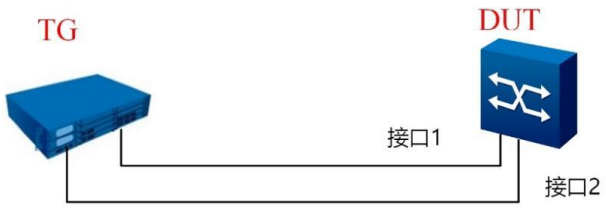


图 2-4 VLAN Mapping 配置拓扑图

配置步骤

配置过程示例如下：

1.将接口 1 和接口 2 以 tag 方式加入 vlan 100，vlan 200。

2.在接口 1 上配置 QinQ 条目。

3.在接口上上抓包查看 Vlan 翻译结果以确定条目是否生效。

2.7 QinQ 配置

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

QinQ 主要可以解决如下几个问题：

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

2.7.1 QinQ 简介

QinQ（802.1Q-in-802.1Q）协议是基于 IEEE 802.1Q 技术的一种二层隧道协议。由于在公网中传递的帧有两层 802.1Q Tag（一个公网 Tag，一个私网 Tag），所以称之为 QinQ 协议。

QinQ 的核心思想是将用户私网 VLAN Tag 封装在公网 VLAN Tag 中，报文带着两层 Tag 穿越网络运营商的骨干网络，从而为用户提供一种较为简单的二层 VPN 隧道。

QinQ 功能是直接配置在端口上，这一点与旧的 Vlan 翻译模块先要创建 Vlan 翻译条目后，再将该条目与端口绑定不同。QinQ 只能添加 Vlan 标签，不能修改或者删除 Vlan 标签。

2.7.2 配置单个 VLAN 或者配置批量 VLAN 的灵活 QinQ 功能

目的

本节介绍如何配置单个 VLAN 或者配置批量 VLAN 的灵活 QinQ 功能。

当用户 VLAN 内的报文需要穿越运营商网络时，可以通过使用该命令在用户 VLAN 的数据帧上再加上一个 VLAN Tag，实现双层 VLAN。

配置灵活 QinQ 功能时，需要注意以下几点：

- 配置灵活 QinQ 功能的当前接口类型必须为 Hybrid，且只在入方向生效。

叠加后的外层 VLAN 必须存在，且当前接口必须以 Untagged 方式加入叠加后的 **stack-vlan** 中。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置单个 VLAN 或者配置批量 VLAN 的灵活 QinQ 功能	1. 执行命令 **configure**，进入全局视图。 2. 执行命令 **interface** *interface-type interface-number* 进入接口配置视图（以太网、Trunk）。 3. 执行如下命令： ● **vlan-stacking vlan** *vlan-id1* **stack-vlan** *vlan-id2* ● **vlan-stacking vlan** *vlan-id3* **to** *vlan-id4* **stack-vlan** *vlan-id2* ● **vlan-stacking vlan** *vlan-id1* **8021p** *priority* **stack-vlan** *vlan-id2* ● **vlan-stacking vlan** *vlan-id3* **to** *vlan-id4* **8021p** *priority* **stack-vlan** *vlan-id2*。
删除配置的灵活 QinQ 功能	1. 执行命令 **configure**，进入全局视图。 2. 执行命令 **interface** *interface-type interface-number* 进入接口配置视图（以太网、Trunk）。 3. 执行如下命令： ● **no vlan-stacking all** ● **no vlan-stacking vlan** *vlan-id1* ● **no vlan-stacking vlan** *vlan-id1* **to** *vlan-id2* ● **no vlan-stacking vlan** *vlan-id1* **8021p** *priority* ● **no vlan-stacking vlan** *vlan-id3* **to** *vlan-id4* **8021p** *priority*。

2.7.3 维护及调试

目的

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

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
打开灵活 QinQ 模块的调试功能	1. 不执行任何命令保持当前特权用户视图； 2. 执行命令 **debug vlan-stacking**。
关闭灵活 QinQ 模块的调试功能	1. 不执行任何命令保持当前特权用户视图； 2. 执行命令 **no debug vlan-stacking**。
显示灵活 QinQ 信息	1.执行任何命令进入普通用户视图、特权用户视图、全局配置视图、接口配置视图（以太网接口、trunk 接口）； 2. 执行如下命令： ● **show vlan-stacking** ● **show vlan-stacking config** ● **show vlan-stacking config interface eth-trunk** *trunk-number*

目的	步骤
	● **show vlan-stacking config interface** { **ethernet	gigaethernet	xgigaethernet| 10gigaethernet	25gigaethernet	40gigaethernet	100gigaethernet** } *interface-number* ● **show vlan-stacking interface** ● **show vlan-stacking interface eth-trunk** *trunk-number* ● **show vlan-stacking interface** { **ethernet	gigaethernet	xgigaethernet| 10gigaethernet	25gigaethernet	40gigaethernet	100gigaethernet** } *interface-number*。

2.7.4 配置举例

组网图

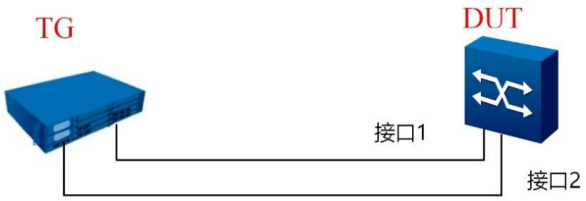


图 2-5 QinQ 配置拓扑图

配置步骤

配置过程示例如下：

1.将接口 1 和接口 2 以 tag 方式加入 vlan 100，vlan 200。

2.在接口 1 上配置 QinQ 条目。

3.在接口上上抓包查看 Vlan 翻译结果以确定条目是否生效。

2.8 ARP 代理配置

2.8.1 ARP 代理介绍

ARP 代理技术主要包括路由式 ARP 代理，VLAN 内 ARP 代理，VLAN 间 ARP 代理和协议需要使用的 ARP 代理绑定等功能。

路由式 ARP 代理

路由式 ARP 代理就是使那些在同一网段却不在同一物理网络上的计算机或交换机能够相互通信的一种功能。在实际应用中，如果连接交换机的当前主机上没有配置缺省网关地址（即不知道如何到达本网络的中介系统），此时将无法进行数据转发。路由式 Proxy ARP 可以解决这个问题，主机发送一个 ARP 请求（请求目的主机的 MAC 地址），使能 Proxy ARP 功能的交换机收到这样的请求后，会使用自己的 MAC 地址作为该 ARP 请求的回应，以此来欺骗主机进行数据转发。使能 Proxy ARP 功能的交换机还可隐藏物理网络的细节，使得处于不同物理网络但网段相同的 Ethernet A 和 Ethernet B 的内部主机之间可以正常的相互通信。

VLAN 内 ARP 代理

如果两个用户属于相同的 VLAN，但 VLAN 内配置了用户隔离。用户间要互通，需要在关联了 VLAN 的接口上启动 VLAN 内 ARP 代理功能。若交换机的接口使能了 VLAN 内 ARP 代理功能，接口在接收到目的地址不是自己的 ARP 请求报文后，交换机并不立即丢弃该报文，而是查找该接口的 ARP 表项。如果满足代理条件，则将交换机的 MAC 地址发送给 ARP 请求方。VLAN 内 ARP 代理主要用于配置了用户隔离的 VLAN 内的用户间互通。

VLAN 间 ARP 代理

如果两个用户属于同一 Super VLAN 的不同 Sub VLAN，用户间要进行互通，需要在关联了 VLAN 的接口上启动 VLAN 间 ARP 代理功能。若交换机的接口使能了 VLAN 间 ARP 代理功能，接口在接收到目的地址不是自己的 ARP 请求报文后，交换机并不立即丢弃该报文，而是查找该接口的 ARP 表项。如果满足代理条件，则将交换机的 MAC 地址发送给 ARP 请求方。

VLAN 间 Proxy ARP 主要用于：在 Super VLAN 对应的 VLANIF 接口上启动 VLAN 间 Proxy ARP 功能，实现 Sub VLAN 间用户互通。

协议需要使用的 Proxy ARP

代理 ARP 模块，提供一个协议绑定结构数组，需要进行代理的协议将代理的 IP 与 MAC 地址信息加入到该数组，ARP 模块收到本机的 ARP 请求时，调用 ARP 代理注册的回调函数，查找协议绑定数组，如果存在对应的表项，则将表项中对应的 MAC 地址作为 ARP 回应的源 MAC。

2.8.2 配置 ARP 代理

目的

本节介绍如何配置 ARP 代理。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
使能或者去使能 VLANIF 接口的路由式 Proxy ARP 功能	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图； 3. 执行命令 **arp-proxy** { **enable** | **disable** }。

2.8.3 维护及调试

目的

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

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
显示 ARP 代理的接口信息	1. 执行命令 **disable** 退出到普通用户视图，或执行命令 **configure** 进入全局配置视图，或执行命令 **interface** { **gigaethernet** | **xgigaethernet** } *interface-number* 或 **interface eth-trunk** *trunk-number* 进入接口配置视图，或不执行任何命令保持当前特权用户视图或者进入 VLANIF 配置视或者进入子接口配置视图； 2. 执行命令 **show arp-proxy interface**。
显示 ARP 代理的 VLAN 信息	1. 执行命令 **disable** 退出到普通用户视图，或执行命令 **configure** 进入全局配置视图，或执行命令 **interface** { **gigaethernet** | **xgigaethernet** } *interface-number* 或 **interface eth-trunk** *trunk-number* 进入接口配置视图，或不执行任何命令保持当前特权用户视图或者进入 VLANIF 配置视图或者进入子接口配置视图； 2. 执行命令 **show arp-proxy vlan**。
打开（关闭）Proxy ARP 同步调试功能	1. 执行命令 **disable** 退出到普通用户视图，或执行命令 **configure** 进入全局配置视图，或执行命令 **interface** { **gigaethernet** | **xgigaethernet** } *interface-number* 或 **interface eth-trunk** *trunk-number* 进入接口配置视图，或不执行任何命令保持当前特权用户视图或者进入 VLANIF 配置视图或者进入子接口配置视图； 2. 执行命令 **debug arp-proxy** 或者 **no debug arp-proxy**。

2.8.4 配置举例

组网需求

配置路由式 ARP 代理，如图 2-6 所示。交换机 CN12800 的两个以太网接口 10GE 1/1 和 10GE 1/2 分别连接一台主机，两台主机的网段均为 172.16.0.0/16。两台计算机 Host A 和 Host B 没有配置默认网关，要求在交换机上配置路由式 ARP 代理，使分处在两个物理网络的主机能互通。

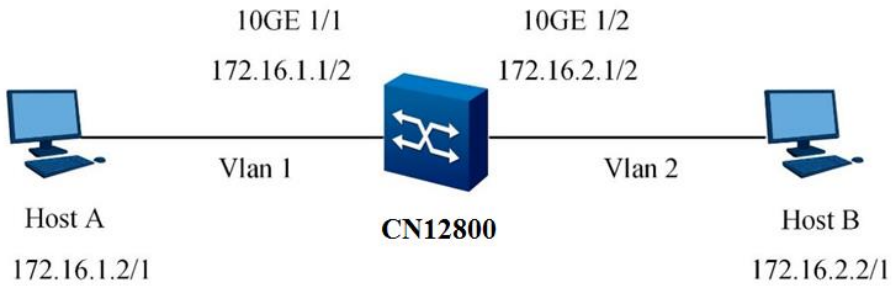


图 2-6 配置路由式 ARP 代理组网图

配置思路

路由式 ARP 代理的配置思路如下：

(1) 配置接口的 IP 地址；

(2) 在接口使能路由式 ARP 代理功能；

数据准备

完成该配置举例，需要准备如下数据：

- 相关 vlan 接口的 IP 地址
- 主机的 IP 地址

配置步骤

(1) 创建 vlan 1 并配置 IP 地址，将 10GE 1/0/1 加入到 vlan 1 中

```
CN12800(config)#interface vlan 1
CN12800(config-vlan-1)#ip address 172.16.1.1/24
CN12800(config-vlan-1)#no shutdown
CN12800(config)#interface xgigaethernet 1/0/1
CN12800(config-10ge1/0/1)#join vlan 1 untagged
```

CN12800(config-10ge1/0/1)#pvid 1

CN12800(config-10ge1/0/1)#no shutdown

CN12800(config-10ge1/0/1)#quit

(2) 在 vlan 1 上使能路由式 ARP 代理功能

CN12800(config)#interface vlan 1

CN12800(config-vlan-1)#arp-proxy enable

CN12800(config-vlan-1)# quit

(3)创建 vlan 2 并配置 IP 地址，将 10GE 1/0/2 加入到 vlan 2 中

CN12800(config)#interface vlan 2

CN12800(config-vlan-2)#ip address 172.16.2.1/24

CN12800(config-vlan-2)#no shutdown

CN12800(config)#interface 10gigaethernet 1/0/2

CN12800(config-10ge1/0/2)#join vlan 2 untagged

CN12800(config-10ge1/0/2)#pvid 2

CN12800(config-10ge1/0/2)#no shutdown

CN12800(config-10ge1/0/2)#quit

(4) 在 vlan 2 上使能路由式 ARP 代理功能

CN12800(config)#interface vlan 2

CN12800(config-vlan-2)#arp-proxy enable

CN12800(config-vlan-2)# quit

（5）配置主机

配置主机 Host A 的 IP 地址为 172.16.1.2/16。

配置主机 Host B 的 IP 地址为 172.16.2.2/16。

（6）验证配置结果

主机 Host A 上 ping 主机 Host B，可以通。

查看 Host A 的 ARP 表，可以看到 Host B 所对应的 MAC 地址是交换机的接口 10GE 1/0/1 的 MAC 地址。

2.9 端口安全配置

2.9.1.1 使能或去使能接口安全功能

目的

本节介绍使能或去使能接口安全功能。使能接口安全功能后，接口学习到的 MAC 地址为安全动态 MAC 地址，安全动态 MAC 地址不会被老化，设备重启后安全动态 MAC 地址会丢失，需要重新学习。

接口安全的其他配置需要使能接口安全后才可以配置，如安全保护动作、安全 MAC 学习限制数量、Sticky MAC 等。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
使能或去使能接口安全功能	1. 执行命令 **configure**，进入全局视图。 2. 执行命令 **interface** *interface-type interface-number* 进入指定某一接口的配置视图或者进入接口组配置视图。 3. 执行命令 **port-security** { **enable** | **disable** }。

2.9.1.2 使能或去使能接口 sticky-mac 功能

目的

本节介绍使能或去使能接口 sticky-mac 功能。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
使能或去使能接口 sticky-mac 功能	1. 执行命令 **configure**，进入全局视图。 2. 执行命令 **interface** *interface-type interface-number* 进入指定某一接口的配置视图或者进入接口组配置视图。 3. 执行命令 **port-security enable**。 4. 执行命令 **port-security mac-address sticky** { **enable** | **disable** }。

2.9.1.3 手动添加安全 MAC

目的

本节介绍手动添加或者删除安全 MAC。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
手动添加安全 MAC	1. 执行命令 **configure**，进入全局视图。 2. 执行命令 **interface** *interface-type interface-number* 进入指定某一接口的配置视图或者进入接口组配置视图。 3. 执行命令 **port-security mac-address sticky enable**，使能 sticky-mac 功能。 4. 执行命令 **port-security mac-address sticky** *vlan-id mac-address*。
手动删除安全 MAC	1. 执行命令 **configure**，进入全局视图。 2. 执行命令 **interface** *interface-type interface-number* 进入指定某一接口的配置视图或者进入接口组配置视图。 3. 执行如下命令： ● **no port-security mac-address sticky** ● **no port-security mac-address sticky vlan** *vlan-id* ● **no port-security mac-address sticky vlan** *vlan-id mac-address*

2.9.1.4 配置接口 MAC 地址学习限制数

目的

本节介绍配置接口 MAC 地址学习限制数。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置接口 MAC 地址学习限制数	1. 执行命令 **configure**，进入全局视图。 2. 执行命令 **interface** *interface-type interface-number* 进入指定某一接口的配置视图或者进入接口组配置视图。 3. 执行命令 **port-security enable**，使能端口安全的功能。 4. 执行命令 **port-security maximum** { *max-value* | **default** }。

2.9.1.5 配置接口安全功能的保护动作

目的

本节介绍配置接口安全功能的保护动作。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置接口安全功能的保护动作	1. 执行命令 **configure**，进入全局视图。 2. 执行命令 **interface** *interface-type interface-number* 进入指定某一接口的配置视图或者进入接口组配置视图。 3. 执行命令 **port-security enable**，使能端口安全的功能。 4. 执行命令 **port-security protect-action** { **protect** | **restrict** | **shutdown** }。

2.10 端口隔离配置

2.10.1 端口隔离概述

为了实现报文之间的二层隔离，用户可以将不同的端口加入不同的 VLAN，但这样会浪费有限的 VLAN 资源。采用端口隔离功能，可以实现同一 VLAN 内端口之间的隔离。用户只需要将端口加入到隔离组中，就可以实现隔离组内端口之间二层数据的隔离。端口隔离功能为用户提供了更安全、更灵活的组网方案。

2.10.2 配置端口隔离

目的

端口隔离可实现同一 VLAN 内端口之间的隔离，为用户提供更安全、更灵活的组网方案。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
配置二层、三层的端口隔离	1. 进入全局配置视图； 2. 执行命令 **port-isolate mode** { **l2** | **all** }配置二层、三层的端口隔离。
创建端口隔离组	1. 进入全局配置视图； 2. 执行命令 **port-isolate group** *group-number*。
把接口添加到隔离组	1. 进入全局配置视图； 2. 进入接口配置视图、接口组配置视图；

目的	步骤
	3. 执行如下命令把接口添加到隔离组： **join port-isolate group** *group-id*。
把接口从隔离组删除接口	1. 进入全局配置视图； 2. 进入接口配置视图、接口组配置视图； 3. 执行如下命令把接口从隔离组删除接口： ● **no join port-isolate group** *group-id* ● **no join port-isolate group all**。
将端口加入隔离组	1. 进入全局配置视图； 2. 执行命令 **port-isolate group** *group-number*； 3. 执行命令将端口加入隔离组： ● **add interface** { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* ● **add interface eth-trunk** *trunk-number*。
将端口从隔离组中删除	1. 进入全局配置视图； 2. 执行命令 **port-isolate group** *group-number*； 3. 执行命令将端口从隔离组中删除： ● **no interface** { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* ● **no interface eth-trunk** *trunk-number*。

2.10.3 维护端口隔离

目的

当端口隔离功能不正常，需要进行查看、定位问题时，可以使用本小节操作。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
查看全部或者指定端口隔离组信息	1. 进入特权用户视图、全局配置视图、普通用户视图、接口配置视图（以太网接口、trunk 接口）、接口组配置视图； 2. 执行如下命令查看全部或者指定端口隔离组信息： ● **show port-isolate group** ● **show port-isolate group** *group-number*。
查看全部端口隔离组信息	1. 进入特权用户视图、全局配置视图、普通用户视图、接口配置视图（以太网接口、trunk 接口）、接口组配置视图； 2. 执行命令 **show port-isolate information** 查看全部端口隔离组信息。

目的	步骤
以配置文件形式查看隔离组的配置信息	1. 进入特权用户视图、全局配置视图、普通用户视图、接口配置视图（以太网接口、trunk 接口）、接口组配置视图； 2. 执行命令 **show port-isolate config** 以配置文件形式查看隔离组的配置信息。

2.11 风暴控制配置

2.11.1 配置风暴控制功能

目的

使用本节操作配置风暴控制功能。

过程

根据不同目的，执行相应步骤，具体参见下表。

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

2.11.2 维护及调试

目的

当风暴控制功能不正常，需要进行查看、调试或定位问题时，可以使用本小节操作。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
打开风暴控制信息调试功能	1. 不执行任何命令保持当前特权用户视图； 2. 执行命令 **debug storm-control** { **nm** | **if** | **vlan** | **vsi** | **event** | **all** }打开风暴控制信息调试功能。

目的	步骤
关闭风暴控制信息调试功能	1. 不执行任何命令保持当前特权用户视图； 2. 执行命令 **no debug storm-control** { **nm** | **if** | **vlan** | **vsi** | **event** | **all** }关闭风暴控制信息调试功能。
查看接口的风暴控制信息	1. 执行命令 **disable** 退出到普通用户视图或不执行任何命令保持当前特权用户视图或执行命令 **configure** 进入全局视图； 2. 执行如下命令： ● **show storm-control interface** ● **show storm-control interface** { **ethernet** | **gigaethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number*。
查看 VLAN 接口的风暴控制信息	1. 执行命令 **disable** 退出到普通用户视图或不执行任何命令保持当前特权用户视图或执行命令 **configure** 进入全局视图； 2. 执行命令 **show storm-control vlan** [*vlan-id*]。
查看 VSI 接口的风暴控制信息	1. 执行命令 **disable** 退出到普通用户视图或不执行任何命令保持当前特权用户视图或执行命令 **configure** 进入全局视图； 2. 执行命令 **show storm-control vsi** [*vsi-name*]。
查看风暴控制配置信息	1. 执行命令 **disable** 退出到普通用户视图或不执行任何命令保持当前特权用户视图或执行命令 **configure** 进入全局视图； 2. 执行命令 **show storm-control config**。

2.12 Link Flap 配置

2.12.1 Link Flap 简介

Link Flap（链路震荡保护）功能可以将频繁 Up/Down 的接口关闭，从而避免网络拓扑结构频繁变化，影响通信业务。

2.12.2 配置链路震荡保护功能

目的

本节介绍如何配置接口的链路震荡保护功能。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
批量打开或关闭所有接口的链路震荡保护功能	1. 执行命令 **configure**，进入全局视图。 2. 执行命令 **link-flap protection** {**start** | **stop**}。

目的	步骤
单独开启或关闭接口的链路震荡保护功能	1. 执行命令 **configure**，进入全局视图。 2. 执行命令 **interface** *interface-type interface-number* 进入接口配置视图（以太网）。 3. 执行命令 **port link-flap protection** {**enable** | **disable**}。
配置接口由于链路震荡被 error-down 之后的恢复等待时间	1. 执行命令 **configure**，进入全局视图。 2. 执行命令 **error-down auto-recovery cause link-flap interval** *interval*。
配置接口由于链路震荡被 error-down 保护之后不再恢复	1. 执行命令 **configure**，进入全局视图。 2. 执行命令 **no error-down auto-recovery cause link-flap**。
配置接口链路震荡保护的检测时长，即从第一次链路状态变化开始的指定时间内检测是否达到链路震荡保护的阈值	1. 执行命令 **configure**，进入全局视图。 2. 执行命令 **interface** *interface-type interface-number* 进入接口配置视图（以太网）。 3. 执行命令 **port link-flap interval** { *interval* | **default**}。
配置接口链路震荡保护的震荡阈值，即从第一次链路状态变化开始的指定时间内检测是否达到链路震荡保护的阈值	1. 执行命令 **configure**，进入全局视图。 2. 执行命令 **interface** *interface-type interface-number* 进入接口配置视图（以太网）。 3. 执行命令 **port link-flap threshold** { *threshold* | **default**}。

2.12.3 维护及调试

目的

当链路震荡保护功能不正常，需要进行查看、调试或定位问题时，可以使用本小节操作。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
打开链路震荡保护模块的调试功能	1. 不执行任何命令保持当前特权用户视图。 2. 执行命令 **debug linkflap**。
关闭链路震荡保护模块的调试功能	1. 不执行任何命令保持当前特权用户视图。 2. 执行命令 **no debug linkflap**。
查看链路震荡保护相关配置	1. 不执行任何命令保持当前特权用户视图。 2. 执行命令 **show linkflap config**。

2.12.4 配置举例

组网图

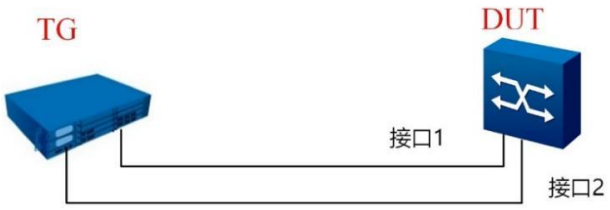


图 2-7 链路震荡保护配置拓扑图

配置步骤

配置过程示例如下：

1.在接口 1 上配置链路震荡保护。

2.在接口 1 的对端 TG 上反复开启关闭接口。

3.在 DUT 上查看接口 1 是否被 error-down 保护了。

2.13 ARP MISS 配置

2.13.1 介绍

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

根据源 IP 地址进行 ARP MISS 消息限速

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

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

针对全局、VLAN 和接口的 ARP MISS 消息限速

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

针对全局的 ARP MISS 消息限速：在设备出现目标 IP 地址不能解析的 IP 报文攻击时，限制全局处理的 ARP MISS 消息数量。

针对 VLAN 的 ARP MISS 消息限速：在某个 VLAN 内的所有接口出现目标 IP 地址不能解析的 IP 报文攻击时，限制处理该 VLAN 内报文触发的 ARP MISS 消息数量，配置本功能可以保证不影响其他 VLAN 内所有接口的 IP 报文转发。

针对接口的 ARP MISS 消息限速：在某个接口出现目标 IP 地址不能解析的 IP 报文攻击时，限制处理该接口收到的报文触发的 ARP MISS 消息数量，配置本功能可以保证不影响其他接口的 IP 报文转发。

2.13.2 配置 ARP MISS

目的

本节介绍如何配置 ARP MISS 消息限速。

过程

根据不同目的，执行相应步骤，具体参见下表。

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

目的	步骤
	2. 执行命令 **arp-miss anti-attack rate-limit source-ip** *ip-address* [*mask-address*] **maximum** { *maximum* | **default** } [**non-block** | **block timer** *timer*]。
删除源 IP 限速配置	1. 执行命令 **configure**，进入全局视图； 2. 执行命令 **no arp-miss anti-attack rate-limit source-ip** *ip-address*。
重置 ARP MISS 协议统计信息	1. 执行命令 **configure**，进入全局视图； 2. 执行命令 **arp-miss reset statistics**。

2.13.3 维护及调试

目的

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

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
显示 ARP MISS 限速的配置信息	1. 进入普通用户视图、全局配置视图、以太网接口配置视图、Trunk 接口配置视图、VLANIF 配置视图或特权用户视图； 2. 执行命令 **show arp-miss config**。
显示 ARP MISS 模块的总体信息	1. 进入普通用户视图、全局配置视图、以太网接口配置视图、Trunk 接口配置视图、VLANIF 配置视图或特权用户视图； 2. 执行命令 **show arp-miss info**。
显示 ARP MISS 的限速的统计信息	1. 进入普通用户视图、全局配置视图、以太网接口配置视图、Trunk 接口配置视图、VLANIF 配置视图或特权用户视图； 2. 执行如下命令： ● **show arp-miss statistic** ● **show arp-miss statistic all** ● **show arp-miss statistic interface** { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* ● **show arp-miss statistic srcip**。
显示 ARP MISS 协议反攻击速率信息	1. 进入普通用户视图、全局配置视图、以太网接口配置视图、Trunk 接口配置视图、VLANIF 配置视图或特权用户视图； 2. 执行命令 **show arp-miss anti-attack rate-limit**。
显示 ARP MISS 协议反攻击记录信息	1. 进入普通用户视图、全局配置视图、以太网接口配置视图、Trunk 接口配置视图、VLANIF 配置视图或特权用户视图； 2. 执行命令 **show arp-miss anti-attack record**。

目的	步骤
清除 ARP MISS 协议防攻击记录信息	1. 进入全局配置视图； 2. 执行命令 **clear arp-miss anti-attack record**。
打开（关闭）ARP MISS 同步调试功能	1. 进入特权用户视图； 2. 执行命令 **debug arp-miss** 或者 **no debug arp-miss**。

2.13.4 配置举例

配置步骤

(1) 执行命令 configure，进入全局视图，配置全局限速。

CN12800(config)# arp-miss anti-attack rate-limit global pkt-num 100

(2) 在 vlan 1 上配置 arpmiss 限速

CN12800(config)#interface vlan 1

CN12800(config-vlan-1)#arp-miss anti-attack rate-limit pkt-num 200

(3) 在接口 1/0/1 上配置 arpmiss 限速

CN12800(config)#interface gigaethernet 1/0/1

CN12800(config-ge1/0/1)#arp-miss anti-attack rate-limit pkt-num 300

CN12800(config-ge1/0/1)#no shutdown

(4) 配置动态源 IP 限速

CN12800(config)#arp-miss anti-attack rate-limit source-ip maximum 100 block timer 20

(5) 配置指定源 IP 限速

CN12800(config)#arp-miss anti-attack rate-limit source-ip 10.0.0.1 maximum 100 block timer 20

(6) 验证配置结果

CN12800(config)#show arp-miss config

2.14 MLAG 配置

2.14.1 MLAG 简介

在数据中心应用场景中，为了提供冗余，每个机顶交换机都连接到两台聚合的交换机。为了避免成环，一半的上联链路都会被生成树阻塞掉，因此减少了汇聚层和机架之间的 50%的可用带宽。

数据中心网络存在带宽浪费的情形，企业网络容忍这种带宽浪费是因为其中的应用对带宽不敏感。但随着技术的发展，比如富媒体应用、廉价的电脑服务器、日益增长的带宽需求，数据中心网络带宽不足的问题暴露无遗。MLAG 特性可以解决这个带宽上的瓶颈，并能够充分的利用网络中的带宽。

数据中心和高性能的云计算网络在网络可靠性方向有较高的要求。MLAG 逻辑上把两个交换机的端口聚合在一起，相对于把链路聚合扩展到一对数据中心交换机上，其提供系统级别的冗余和网络级别的弹性。

MLAG 的主要优点：

- 允许用户设计一个没有阻塞链路的网络
- 更加高效的带宽使用
- 提供网络的弹性设计和系统级别的冗余
- 连接到 MLAG 交换机，不需要额外的私有协议支持，仅需要支持 IEEE 802.3ad LACP

2.14.2 配置 MLAG 组及系统参数

目的

使能 MLAG 组功能，并配置 MLAG 系统参数。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
创建 MLAG 组或删除 MLAG 组	1. 进入全局配置视图； 2. 执行命令 **mlag-group** *mlag-group* 创建 MLAG 组或执行 **no mlag-group** *mlag-group* 删除 MLAG 组。

目的	步骤
配置 LACP MLAG 的系统 ID	1. 进入全局配置视图； 2. 执行命令 **lacp mlag system-id** *mac-address* 配置 LACP MLAG 的系统 ID。
配置 LACP MLAG 的系统优先级	1. 进入全局配置视图； 2. 执行命令 **lacp mlag priority** { *priority-value* | **default** }配置 LACP MLAG 的系统优先级。
配置 MLAG 双主检测发现冲突时需要保留的接口	1. 进入全局配置视图； 2. 执行以下命令配置 MLAG 双主检测发现冲突时需要保留的接口： ● **mlag exclude interface** { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number* ● **mlag exclude interface eth-trunk** *trunk-number*。
删除配置的 MLAG 双主检测发现冲突时需要保留的接口	1. 进入全局配置视图； 2. 执行以下命令删除配置的 MLAG 双主检测发现冲突时需要保留的接口： ● **no mlag exclude interface** { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number* ● **no mlag exclude interface eth-trunk** *trunk-number*。

2.14.3 配置 MLAG 视图参数

目的

配置 MLAG 组视图参数。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
配置 MLAG 成员聚合组的 Eth-trunk 接口	1. 进入全局配置视图； 2. 执行命令 **mlag-group** *mlag-group* 进入 MLAG 配置视图； 3. 执行命令 **mlag** *mlag-member* **interface eth-trunk** *trunk-number* 配置 MLAG 成员聚合组的 Eth-trunk 接口。
删除配置的 MLAG 成员聚合组	1. 进入全局配置视图； 2. 执行命令 **mlag-group** *mlag-group* 进入 MLAG 配置视图； 3. 执行命令 **no mlag** *mlag-member* 删除配置的 MLAG 成员聚合组。
配置 Eth-trunk 接口为 peer-link 接口	1. 进入全局配置视图； 2. 执行命令 **mlag-group** *mlag-group* 进入 MLAG 配置视图；

目的	步骤
	3. 执行命令 **peerlink interface eth-trunk** *trunk-number* 配置 Eth-trunk 接口为 peer-link 接口。
取消配置的指定接口为 peer-link 接口	1. 进入全局配置视图； 2. 执行命令 **mlag-group** *mlag-group* 进入 MLAG 配置视图； 3. 执行命令 **no peerlink interface** 取消配置的指定接口为 peer-link 接口。
配置 MLAG 互联链路不允许通过的 VLAN 列表	1. 进入全局配置视图； 2. 执行命令 **mlag-group** *mlag-group* 进入 MLAG 配置视图； 3. 执行命令 **peerlink exclude vlan** *vlan-list* 配置 MLAG 互联链路不允许通过的 VLAN 列表。
删除 MLAG 互联链路不允许通过的 VLAN 列表	1. 进入全局配置视图； 2. 执行命令 **mlag-group** *mlag-group* 进入 MLAG 配置视图； 3. 执行命令 **no peerlink exclude vlan** *vlan-list* 删除 MLAG 互联链路不允许通过的 VLAN 列表。
配置 MLAG 优先级	1. 进入全局配置视图； 2. 执行命令 **mlag-group** *mlag-group* 进入 MLAG 配置视图； 3. 执行命令 **priority** { *priority-value* | **default** }配置 MLAG 优先级。
配置或删除安全密码	1. 进入全局配置视图； 2. 执行命令 **mlag-group** *mlag-group* 进入 MLAG 配置视图； 3. 执行命令 **security-key** { **simple** | **md5** } { **plain** | **cipher** } *key* 配置安全密码或 **no security-key** 删除安全密码。
配置双主检测本地 IPv4 地址或 IPv6 地址和 VPN 实例	1. 进入全局配置视图； 2. 执行命令 **mlag-group** *mlag-group* 进入 MLAG 配置视图； 3. 执行命令以下命令配置双主检测本地 IPv4 地址或 IPv6 地址和 VPN 实例： ● **source-address** *ipv4-address* ● **source-address** ipv4-address **peer-address** peer-ipv4-address ● **source-address** *ipv4-address* **vpn-instance** *name* ● **source-address** *ipv4-address* **vpn-instance** *name* **peer-address** *peer-ipv4-address* ● **source-address** *ipv6-address* ● **source-address** ipv6-address **peer-address** *peer-ipv6-address* ● **source-address** *ipv6-address* **vpn-instance** *name* ● **source-address** *ipv6-address* **vpn-instance** *name* **peer-address** *peer-ipv6-address* ● **no source-address**。
配置 Hello 报文发送间隔定时器	1. 进入全局配置视图； 2. 执行命令 **mlag-group** *mlag-group* 进入 MLAG 配置视图； 3. 执行命令 **timer hello** { *hello-interval* | **default** }配置 Hello 报文发送间隔定时器。

目的	步骤
配置 Hello 时间间隔的倍数定时器	1. 进入全局配置视图； 2. 执行命令 **mlag-group** *mlag-group* 进入 MLAG 配置视图； 3. 执行命令 **timer hold-on-failure multiplier** { *value* | **default** }配置 Hello 时间间隔的倍数定时器。
配置 M-LAG 成员接口上报 UP 状态的延时时间	1. 进入全局配置视图； 2. 执行命令 **mlag-group** *mlag-group* 进入 MLAG 配置视图； 3. 执行命令 **up-delay** { *delay-value* | **default** } [**auto-recovery interval** { *interval-value* | **default** }]配置 M-LAG 成员接口上报 UP 状态的延时时间。
使能或去使能 MLAG 场景下二测故障增强功能	1. 进入全局配置视图； 2. 执行命令 **mlag-group** *mlag-group* 进入 MLAG 配置视图； 3. 执行命令 **dad enhance** { **enable | disable** }使能或去使能 MLAG 场景下二测故障增强功能。

2.14.4 维护及调试

目的

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

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
打开 MLAG 调试功能	1. 不执行任何命令保持当前特权用户视图； 2. 执行命令 **debug mlag** { **in** | **out** | **timer** | **notify** | **global** | **if** | **packet** | **error** | **all** }打开 MLAG 调试功能。
关闭 MLAG 调试功能	1. 不执行任何命令保持当前特权用户视图； 2. 执行命令 **no debug mlag** { **in** | **out** | **timer** | **notify** | **global** | **if** | **packet** | **error** | **all** }关闭 MLAG 调试功能。
清除 MLAG 统计计数	1. 进入全局配置视图； 2. 执行命令 **mlag-group** *mlag-group* 进入 MLAG 配置视图； 3. 执行命令 **reset counter** 清除 MLAG 统计计数。
查看 MLAG 系统信息	1. 执行命令 **disable** 退出到普通用户视图； 2. 执行命令 **show mlag** 查看 MLAG 系统信息。
查看 MLAG 配置文件信息	1. 执行命令 **disable** 退出到普通用户视图； 2. 执行命令 **show mlag config** 查看 MLAG 配置文件信息。
查看 M-LAG 配置一致性信息	1. 执行命令 **disable** 退出到普通用户视图； 2. 执行命令 **show mlag consistency** 查看 M-LAG 配置一致性信息。

目的	步骤
查看跨设备链路聚合预留接口信息	1. 执行命令 **disable** 退出到普通用户视图； 2. 执行命令 **show mlag exclude interface** 查看跨设备链路聚合预留接口信息。
查看跨设备链路聚合组信息	1. 执行命令 **disable** 退出到普通用户视图； 2. 执行命令 **show mlag-group** *mlag-group* 查看跨设备链路聚合组信息。

2.14.5 配置举例

2.14.5.1 二层 MLAG 典型案例

组网需求

sw1、2 为下联交换机，master 和 slave 交换机为 MLAG 域成员，运行 MLAG。链路两端的数字表示端口号，配置 master 和 slave 交换机的 peer address 分别为 192.168.1.1 和 192.168.1.2，管理员保证这些地址路由可达。

组网图

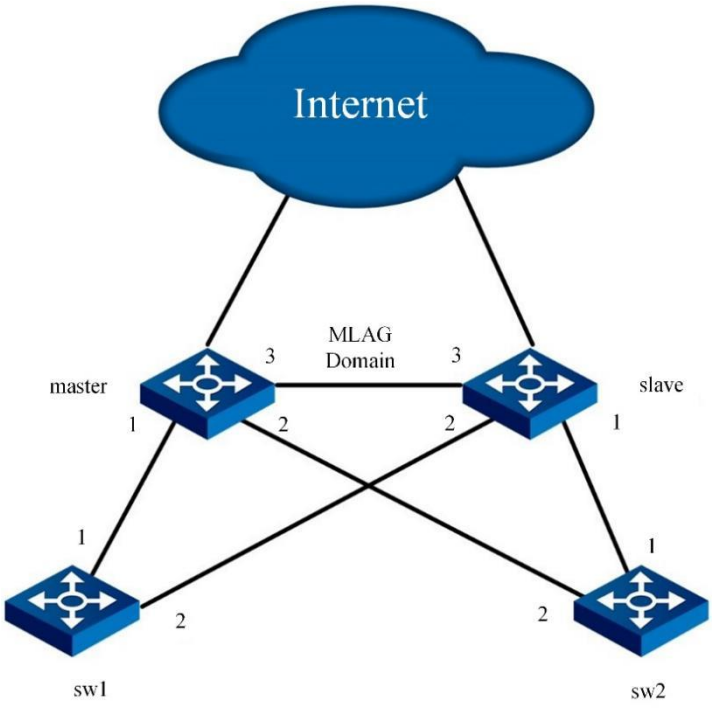


图 2-8 二层 MLAG 典型组网图

配置步骤

1、SW1、SW2 交换机

Switch(config)#interface eth-trunk 1

Switch(config-eth-trunk1)#mode lacp-static

Switch(config-eth-trunk1)#add 10gigaethernet 1/0/1

Switch(config-eth-trunk1)#add 10gigaethernet 1/0/2

2、Master 交换机

Switch(config)#interface eth-trunk 1

Switch(config-eth-trunk1)#mode lacp-static

Switch(config-eth-trunk1)#add 10gigaethernet 1/0/1

Switch(config-eth-trunk1)#exit

Switch(config)#interface eth-trunk 2

Switch(config-eth-trunk2)#mode lacp-static

Switch(config-eth-trunk2)#add 10gigaethernet 1/0/2

Switch(config-eth-trunk2)#exit

Switch(config)#interface eth-trunk 3

Switch(config-eth-trunk3)#mode lacp-static

Switch(config-eth-trunk3)#add 10gigaethernet 1/0/3

Switch(config-eth-trunk3)#exit

Switch(config)#mlag-group 1

Switch(config-mlag-1)#priority 100

Switch(config-mlag-1)#peerlink interface eth-trunk 3

Switch(config-mlag-1)#mlag 1 interface eth-trunk 1

Switch(config-mlag-1)#mlag 2 interface eth-trunk 2

Switch(config-mlag-1)#source-address 192.168.1.1 peer-address 192.168.1.2

Switch(config-mlag-1)#dad enhance enable

Switch(config-mlag-1)#up-delay 240 auto-recovery interval 60

3、Slave 交换机

Switch(config)#interface eth-trunk 1

Switch(config-eth-trunk1)#mode lacp-static

Switch(config-eth-trunk1)#add 10gigaethernet 1/0/2

Switch(config-eth-trunk1)#exit

Switch(config)#interface eth-trunk 2

Switch(config-eth-trunk2)#mode lacp-static

Switch(config-eth-trunk2)#add 10gigaethernet 1/0/1

Switch(config-eth-trunk2)#exit

Switch(config)#interface eth-trunk 3

Switch(config-eth-trunk3)#mode lacp-static

Switch(config-eth-trunk3)#add 10gigaethernet 1/0/3

Switch(config-eth-trunk3)#exit

Switch(config)#mlag-group 1

Switch(config-mlag-1)#priority 200

Switch(config-mlag-1)#peerlink interface eth-trunk 3

Switch(config-mlag-1)#mlag 1 interface eth-trunk 1

Switch(config-mlag-1)#mlag 2 interface eth-trunk 2

Switch(config-mlag-1)#source-address 192.168.1.2 peer-address 192.168.1.1

Switch(config-mlag-1)#dad enhance enable

Switch(config-mlag-1)#up-delay 240 auto-recovery interval 60

Switch(config)#lacp mlag system-id 00:00:00:01:02:03（在备设备上配置主设备的 mac 地址）

2.14.5.2 三层 MLAG 典型案例

组网需求

sw1、2 为下联交换机，master 和 slave 交换机为 MLAG 域成员，运行 MLAG。链路两端的数字表示端口号，配置 master 和 slave 交换机的 peer address 分别为 192.168.1.1 和 192.168.1.2，管理员保证这些地址路由可达。

其中 MLAG 交换机是下联设备 10.0.0.100 和 10.0.1.100 的网关，网关地址分别为 100.0.0.1 和 100.0.1.1。

组网图

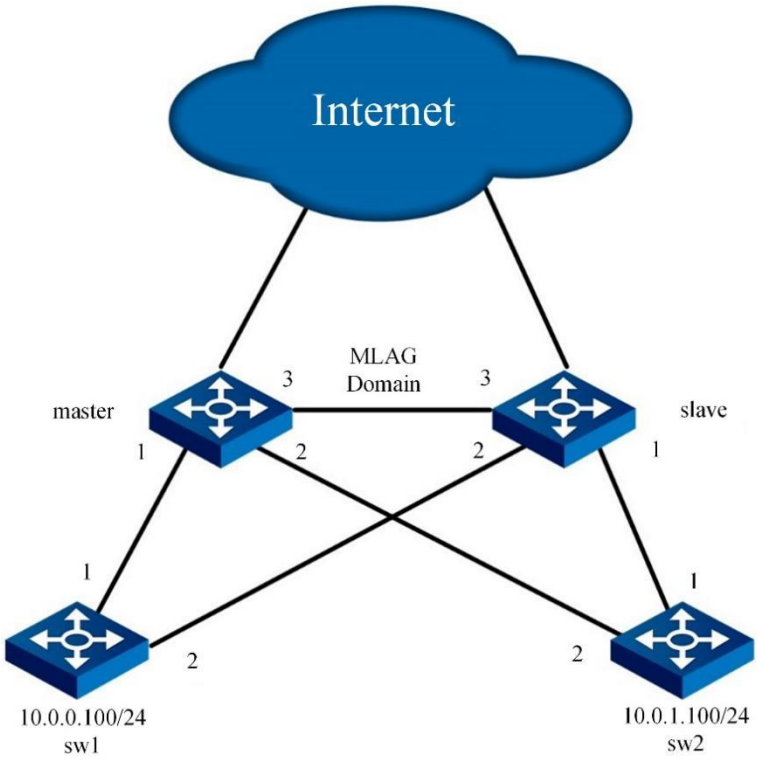


图 2-9 三层 MLAG 典型组网图

配置步骤

1、SW1、SW2 交换机

Switch(config)#interface eth-trunk 1

Switch(config-eth-trunk1)#mode lacp-static

Switch(config-eth-trunk1)#add 10gigaethernet 1/0/1

Switch(config-eth-trunk1)#add 10gigaethernet 1/0/2

2、Master 交换机

```
Switch(config)#vlan 10,20
Switch(config)#interface vlan 10
Switch(config-vlanif-10)#ip address 100.0.0.1
Switch(config-vlanif-10)#exit
Switch(config)#interface vlan 20
Switch(config-vlanif-10)#ip address 100.0.1.1
Switch(config-vlanif-10)#exit
Switch(config)#interface eth-trunk 1
Switch(config-eth-trunk1)#mode lacp-static
Switch(config-eth-trunk1)#add 10gigaethernet 1/0/1
Switch(config-eth-trunk1)#port link-type access
Switch(config-eth-trunk1)#port default vlan 10
Switch(config-eth-trunk1)#exit
Switch(config)#interface eth-trunk 2
Switch(config-eth-trunk2)#mode lacp-static
Switch(config-eth-trunk2)#add 10gigaethernet 1/0/2
Switch(config-eth-trunk2)#port link-type access
Switch(config-eth-trunk2)#port default vlan 20
Switch(config-eth-trunk2)#exit
Switch(config)#interface eth-trunk 3
Switch(config-eth-trunk3)#mode lacp-static
Switch(config-eth-trunk3)#add 10gigaethernet 1/0/3
Switch(config-eth-trunk3)#exit
Switch(config)#mlag-group 1
Switch(config-mlag-1)#priority 100
Switch(config-mlag-1)#peerlink interface eth-trunk 3
```

Switch(config-mlag-1)#mlag 1 interface eth-trunk 1

Switch(config-mlag-1)#mlag 2 interface eth-trunk 2

Switch(config-mlag-1)#source-address 192.168.1.1 peer-address 192.168.1.2

Switch(config-mlag-1)#dad enhance enable

Switch(config-mlag-1)#up-delay 240 auto-recovery interval 60

3、Slaver 交换机

Switch(config)#vlan 10,20

Switch(config)#interface vlan 10

Switch(config-vlanif-10)#ip address 100.0.0.1

Switch(config-vlanif-10)#exit

Switch(config)#interface vlan 20

Switch(config-vlanif-10)#ip address 100.0.1.1

Switch(config-vlanif-10)#exit

Switch(config)#interface eth-trunk 1

Switch(config-eth-trunk1)#mode lacp-static

Switch(config-eth-trunk1)#add 10gigaethernet 1/0/1

Switch(config-eth-trunk1)#port link-type access

Switch(config-eth-trunk1)#port default vlan 10

Switch(config-eth-trunk1)#exit

Switch(config)#interface eth-trunk 2

Switch(config-eth-trunk2)#mode lacp-static

Switch(config-eth-trunk2)#add 10gigaethernet 1/0/2

Switch(config-eth-trunk2)#port link-type access

Switch(config-eth-trunk2)#port default vlan 20

Switch(config-eth-trunk2)#exit

Switch(config)#interface eth-trunk 3

Switch(config-eth-trunk3)#mode lacp-static

Switch(config-eth-trunk3)#add 10gigaethernet 1/0/3

Switch(config-eth-trunk3)#exit

Switch(config)#mlag-group 1

Switch(config-mlag-1)#priority 200

Switch(config-mlag-1)#peerlink interface eth-trunk 3

Switch(config-mlag-1)#mlag 1 interface eth-trunk 1

Switch(config-mlag-1)#mlag 2 interface eth-trunk 2

Switch(config-mlag-1)#source-address 192.168.1.2 peer-address 192.168.1.1

Switch(config-mlag-1)#dad enhance enable

Switch(config-mlag-1)#up-delay 240 auto-recovery interval 60

Switch(config)#lacp mlag system-id 00:00:00:01:02:03（在备设备上配置主设备的 mac 地址）

第3章 IP 业务配置

本章介绍了 CN12800 系列数据中心交换机的 IP 业务。

3.1 IPv4 配置

3.1.1 配置带内/带外/环回 IP 地址

目的

本节介绍如何配置设备的带内/带外/环回 IP 地址。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
配置设备的带内/带外/环回 IP 地址	配置带内 IP 地址： 1. 进入全局配置视图； 2. 进入 VLANIF 配置视图； 3. 执行如下命令配置带内 IP 地址： ● **ip address** *ip-address/mask-length* ● **ip address** *ip-address mask-address*。 配置带外 IP 地址： 1. 进入全局配置视图； 2. 进入带外口配置视图； 3. 执行如下命令配置带外 IP 地址： ● **ip address** *ip-address/mask-length* ● **ip address** *ip-address mask-address*。 配置环回 IP 地址： 1. 进入全局配置视图； 2. 进入 Loopback 接口配置视图； 3. 执行如下命令配置环回 IP 地址： ● **ip address** *ip-address/mask-length* ● **ip address** *ip-address mask-address*。
删除设备的带内/带外/环回 IP 地址	1. 进入全局配置视图； 2. 进入 VLANIF 配置视图、带外口配置视图、Loopback 接口配置视图； 3. 执行命令 **no ip address** *ip-address*。

3.1.2 接口 IP 地址的相关配置

目的

本节介绍了各接口 IP 地址的相关配置。

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

设备上各接口配置的所有 IP 地址不能位于相同的子网。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
配置 VLANIF 接口的 IP 地址	1. 进入全局配置视图； 2. 进入 VLANIF 配置视图、带外口配置视图、Loopback 接口配置视图、bd 接口配置视图、以太网路由接口配置视图、以太网子接口配置视图或 grp 路由接口配置视图； 3. 执行如下命令： ● **ip address** *ip-address/mask-length* ● **ip address** *ip-address mask-address*。
删除 VLANIF 接口的所有 IP 地址或指定 IP 地址	1. 进入全局配置视图； 2. 进入 VLANIF 配置视图、带外口配置视图、Loopback 接口配置视图、bd 接口配置视图、以太网路由接口配置视图、以太网子接口配置视图或 grp 路由接口配置视图； 3. 执行如下命令： ● **no ip address** *ip-address* ● **no ip address**。
配置 IPv4 接口的 MTU 值	1. 进入全局配置视图； 2. 进入接口配置视图（以太网接口、Trunk 接口）； 3. 执行命令 **mtu** { *mtu-value* | **default** }。
配置三层 IP 严格转发	1. 进入全局配置视图； 2. 执行命令 **ip forward-strict** { **enable** | **disable** }。

目的	步骤
配置 IPv4 的前缀列表表项	1. 进入全局配置视图； 2. 执行如下命令： ● **ip prefix-list** *listname* { **deny | permit** } *ipv4-address/mask-length* ● **ip prefix-list** *listname* { **deny | permit** } *ipv4-address/mask-length* { **greater-equal | less-equal** } *prefix-length* ● **ip prefix-list** *listname* { **deny | permit** } *ipv4-address/mask-length* **greater-equal** *prefix-length* **less-equal** *prefix length* ● **ip prefix-list** listname **index** index-number { **deny | permit** } ipv4-address/mask-length ● **ip prefix-list** *listname* **index** *index-number* { **deny | permit** } *ipv4-address/mask-length* { **greater-equal | less-equal** } *prefix-length* ● **ip prefix-list** *listname* **index** *index-number* { **deny | permit** } *ipv4-address/mask-length* **greater-equal** *prefix-length* **less-equal** *prefix-length*。
取消配置 IPv4 的前缀列表表项	1. 进入全局配置视图； 2. 执行如下命令： ● **no ip prefix-list** *listname* ● **no ip prefix-list** *listname* **index** *index-number*。
配置最大 TCP 连接数目	1. 进入全局配置视图； 2. 执行命令 **ip tcp max-conncect** *maxnum*。
使能或者去使能把 TTL 错误的 IP 包送 CPU	1. 进入全局配置视图； 2. 执行命令 **ip ttl-err to-cpu** { **enable | disable** }。
使能或者去使能 ICMP 重定向报文的发送功能	1. 进入全局配置视图； 2. 执行命令进入 VLANIF 配置视图； 3. 执行命令 **icmp redirect send** { **enable | disable** }。
使能或去使能 ICMP 报文上送 CPU 时带时间戳	1. 进入全局配置视图； 2. 执行命令 **icmp timestamp to-cpu** { **enable | disable** }。
设置协议栈指定发送 ICMP Reply 的速率	1. 进入全局配置视图； 2. 执行命令 **icmp send-reply limit** *reply-limit*。
打开目的 IPv4 地址的 ARP 包收发包调试功能	1. 进入特权用户视图； 2. 执行命令 **debug arp** { **rxdst | txdst** } *ipv4-address*。
关闭目的 IPv4 地址的 ARP 包收发包调试功能	1. 进入特权用户视图； 2. 执行命令 **no debug arp** { **rxdst | txdst** }。
打开源 IPv4 地址的 ARP 包收发包调试功能	1. 进入特权用户视图； 2. 执行命令 **debug arp** { **rxsrc | txsrc** } *ipv4-address*。

目的	步骤
关闭源 IPv4 地址的 ARP 包收发包调试功能	1. 进入特权用户视图； 2. 执行命令 **no debug arp** { **rxsrc** | **txsrc** }。
打开目的 IPv4 地址的 IPv4 包收发包调试功能	1. 进入特权用户视图； 2. 执行命令 **debug ipv4** { **rxdst** | **txdst** } *ipv4-address*。
关闭目的 IPv4 地址的 IPv4 包收发包调试功能	1. 进入特权用户视图； 2. 执行命令 **no debug ipv4** { **rxdst** | **txdst** }。
打开源 IPv4 地址的 IPv4 包收发包调试功能	1. 进入特权用户视图； 2. 执行命令 **debug ipv4** { **rxsrc** | **txsrc** } *ipv4-address*。
关闭源 IPv4 地址的 IPv4 包收发包调试功能	1. 进入特权用户视图； 2. 执行命令 **no debug ipv4** { **rxsrc** | **txsrc** }。

3.1.3 查看 VLAN 接口配置信息

目的

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

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

3.1.4 查看 TCP/UDP 的连接状态

目的

本节介绍如何查看当前 TCP/UDP 的连接状态表项。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
查看当前 TCP/UDP 的连接状态表项	1. 进入普通用户视图、全局配置视图或者特权用户视图； 2. 执行命令 **show ip connect-table**。

目的	步骤
查看设备当前已经建立的传输层协议类型为 IPv4 的 TCP 连接状态	1. 进入普通用户视图、全局配置视图或者特权用户视图； 2. 执行命令 **show tcp ipv4 status**。
查看设备当前已经建立的传输层协议类型为 IPv4 的 TCP 相关统计信息	1. 进入普通用户视图、全局配置视图或者特权用户视图； 2. 执行命令 **show tcp ip statistic verbose**。
查看设备当前已经建立的传输层协议类型为 IPv4 的 UDP 连接状态	1. 进入普通用户视图、全局配置视图或者特权用户视图； 2. 执行命令 **show udp ipv4 status**。

3.1.5 查看 IP 相关的统计信息

目的

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

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
查看 IP 相关的统计信息	1. 进入特权用户视图、全局配置视图、普通用户视图； 2. 执行如下命令： ● **show ip statistic** ● **show ip tcp statistic** ● **show ip udp statistic** ● **show ip icmp statistic**。

3.1.6 查看系统 IP 接口的信息

目的

本节介绍如何查看系统 IP 接口的信息。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

3.1.7 配置举例

组网要求

交换机 CN12800 通过以太网接口 10gigaethernet1/0/1 连接到局域网，该局域网中的计算机分别属于两个不同网段，10.18.11.0/24 和 10.18.12.0/24。 现要求通过交换机 CN12800 能分别访问这两个网络，但这两个网段内的计算机不能互通。

组网图

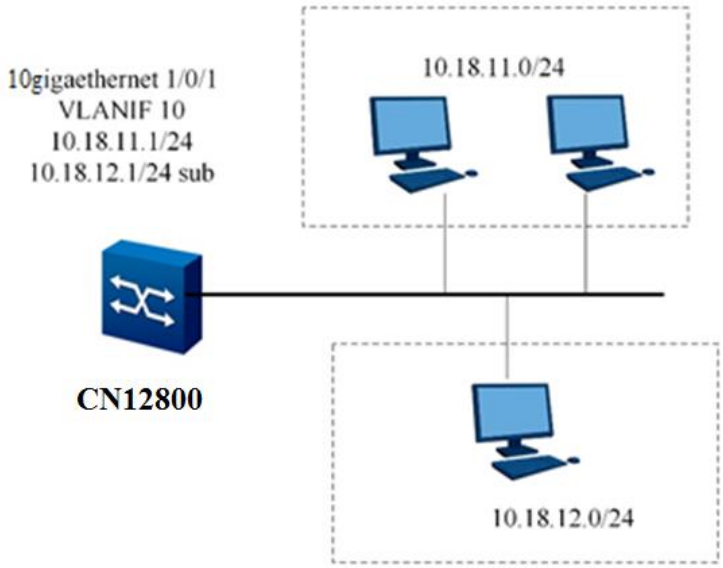


图 3-1 IPv4 地址配置拓扑图

配置步骤

配置 CN12800 的 VLAN10 接口的 IP 地址。

CN12800#configure

CN12800(config)#interface vlan 10

CN12800(config-vlan-10)#ip address 10.18.11.1/24

CN12800(config-vlan-10)#ip address 10.18.12.1/24 sub

```
CN12800(config-vlan-10)#quit
CN12800(config)#
CN12800(config)#interface 10gigaethernet 1/0/1
CN12800(config-10ge1/0/1)#port hybrid vlan 10 untagged
CN12800(config-10ge1/0/1)#port hybrid pvid 10
CN12800(config-10ge1/0/1)#quit
```

3.2 IPv6 配置

3.2.1 配置 IPv6 基本功能

3.2.1.1 配置 IPv6 地址

目的

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

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
手工设置接口的 IPv6 地址和前缀长度	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 在全局配置视图下执行命令进入 VLANIF 配置视图、带外口配置视图、BD 接口配置视图、以太网路由接口配置视图或 Loopback 接口配置视图； 3. 执行如下命令： ● **ipv6 address** *ipv6-address/prefix-length* ● **ipv6 address** *ipv6-address/prefix-length* **eui-64** ● **ipv6 address** *ipv6-address/mask-length* **sub** ● **ipv6 address** *ipv6-address/prefix-length* **eui-64 sub**。
删除接口手工设置的 IPv6 地址及其前缀	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 在全局配置视图下执行命令进入 VLANIF 配置视图、带外口配置视图、BD 接口配置视图、以太网路由接口配置视图或 Loopback 接口配置视图； 3. 执行如下命令删除接口上所有的地址或指定地址： ● **no ipv6 address** ● **no ipv6 address** *ipv6-address*。
删除已配置的接口 IPv6 单播地址	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 在全局配置视图下执行命令 **interface vlan** *vlan-id* 进入 VLAN IF 配置视图；

目的	步骤
	3. 执行命令 **no ipv6 address** *ipv6-address* **eui-64**。
使能或者去使能接口 IPv6 功能	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 在全局配置视图下执行命令进入 VLANIF 配置视图、带外口配置视图、BD 接口配置视图、以太网路由接口配置视图或 Loopback 接口配置视图； 3. 执行命令 **ipv6** { **enable** | **disable** }。
使能或去使能 IPv6 邻居转主机路由功能	1. 进入 VLANIF 配置视图、bd 接口配置视图； 2. 执行命令 **ipv6 nd direct-route { enable | disable }**。

3.2.1.2 配置 IPv6 静态路由条目

目的

本节介绍如何添加或删除一条静态 IPv6 路由条目。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
添加一条静态 IPv6 路由条目，同时也支持多实例 VPN 情况下配置	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行如下命令： ● **ipv6 route-static** *ipv6-address Prefix-len ipv6- nexthop-address* ● **ipv6 route-static** *ipv6-address Prefix-len ipv6- nexthop-address* **preference** *preference-value* ● **ipv6 route-static vpn-instance** *name ipv6-address Prefix-len ipv6-nexthop-address* [**preference** *preference-value*] ● **ipv6 route-static** *ipv6-address Prefix-len* **vpn-instance** *name ipv6-nexthop-address* **preference** *preference-value*。
删除一条静态 IPv6 路由条目	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **no ipv6 route-static** { *ipv6-address prefix-len* | **all** }。

3.2.1.3 配置 IPv6 单播路由转发功能

目的

本节介绍如何使能或去使能 IPv6 单播路由转发功能。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
使能 IPv6 单播路由转发功能	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **ipv6 unicast-forwarding enable**。
去使能 IPv6 单播路由转发功能	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **ipv6 unicast-forwarding disable**。

3.2.1.4 配置接口上发送 IPv6 报文的 MTU 值

目的

本节介绍如何配置接口 MTU。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
设置接口 MTU	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 在全局配置视图下执行命令 **interface vlan** *vlan-id* 进入 VLAN IF 配置视图； 3. 执行命令 **ipv6 mtu** *mtu-value*。
恢复接口 MTU 为默认值	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 在全局配置视图下执行命令 **interface vlan** *vlan-id* 进入 VLAN IF 配置视图； 3. 执行命令 **ipv6 mtu default**。

3.2.2 配置 IPv6 其他功能

3.2.2.1 测试 IPv6 网络连通性及主机可达性

目的

本节介绍如何检测 IPv6 网络连接是否出现故障或者监察网络线路质量。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
测试 IPv6 网络连通性及主机可达性检查主机是否可达。发送 ICMPv6	1. 进入特权用户视图； 2. 执行如下命令： ● **ping6** *ipv6-address* ● **ping6** *ipv6-address* { **-n** | **-l** | **-w** } *value* ● **ping6** *ipv6-address* { **-n** | **-l** | **-w** } *value* { **-n** | **-l** | **-w** } *value* ● **ping6** *ipv6-address* { **-n** | **-l** | **-w** } *value* { **-n** | **-l** | **-w** } *value* { **-n** | **-l** | **-w** } *value*

目的	步骤
回应请求报文后，等待接收目的主机发回的回应响应报文。同时也支持多实例 VPN 情况下配置	● **ping6** *ipv6-address* { **-n** | **-l** | **-w** } *value* { **-n** | **-l** | **-w** } *value* { **-n** | **-l** | **-w** } *value* **-s** *ipv6-source-address* ● **ping6** *ipv6-address* { **-n** | **-l** | **-w** } *value* { **-n** | **-l** | **-w** } *value* { **-n** | **-l** | **-w** } *value* **-vpn-instance** *name* ● **ping6** *ipv6-address* { **-n** | **-l** | **-w** } *value* { **-n** | **-l** | **-w** } *value* { **-n** | **-l** | **-w** } *value* **-vpn-instance** *name* **-s** *ipv6-source-address* ● **ping6** *ipv6-address* { **-n** | **-l** | **-w** } value { **-n** | **-l** | **-w** } *value* **-s** *ipv6-source-address* ● **ping6** *ipv6-address* { **-n** | **-l** | **-w** } *value* { **-n** | **-l** | **-w** } *value* **-s** *ipv6-source-address* **-t** ● **ping6** *ipv6-address* { **-n** | **-l** | **-w** } *value* { **-n** | **-l** | **-w** } *value* **-t** ● **ping6** *ipv6-address* { **-n** | **-l** | **-w** } *value* { **-n** | **-l** | **-w** } *value* **-vpn-instance** *name* ● **ping6** *ipv6-address* { **-n** | **-l** | **-w** } *value* { **-n** | **-l** | **-w** } *value* **-vpn-instance** *name* **-s** *ipv6-source-address* ● **ping6** *ipv6-address* { **-n** | **-l** | **-w** } *value* { **-n** | **-l** | **-w** } *value* **-vpn-instance** *name* **-s** *ipv6-source-address* **-t** ● **ping6** *ipv6-address* { **-n** | **-l** | **-w** } *value* { **-n** | **-l** | **-w** } *value* **-vpn-instance** *name* **-t** ● **ping6** *ipv6-address* { **-n** | **-l** | **-w** } *value* **-s** *ipv6-source-address* ● **ping6** *ipv6-address* { **-n** | **-l** | **-w** } *value* **-s** *ipv6-source-address* **-t** ● **ping6** *ipv6-address* { **-n** | **-l** | **-w** } *value* **-t** ● **ping6** *ipv6-address* { **-n** | **-l** | **-w** } *value* **-vpn-instance** *name* ● **ping6** *ipv6-address* { **-n** | **-l** | **-w** } *value* **-vpn-instance** *name* **-s** *ipv6-source-address* ● **ping6** *ipv6-address* { **-n** | **-l** | **-w** } *value* **-vpn-instance** *name* **-s** *ipv6-source-address* **-t** ● **ping6** *ipv6-address* { **-n** | **-l** | **-w** } *value* **-vpn-instance** *name* **-t**。
测试发送的 ICMP 包长	1. 进入特权用户视图； 2. 执行如下命令： ● **ping6** *ipv6-address* **-i vlan** *vlan-id* ● **ping6** *ipv6-address* **-i vlan** *vlan-id* **-vpn-instance** *name*。
检查 IPv6 网络是否能够连通，并且 ping 指定主机直至被手工中断。同时也支持多实例 VPN 情况下配置	1. 进入特权用户视图； 2. 执行如下命令： ● **ping6** *ipv6-address* **-s** *ipv6-source-address* ● **ping6** *ipv6-address* **-s** *ipv6-source-address* **-t** ● **ping6** *ipv6-address* **-t** ● **ping6** *ipv6-address* **-vpn-instance** *name* ● **ping6** ipv6-address **-vpn-instance** *name* **-s** ipv6-source-address ● **ping6** ipv6-address **-vpn-instance** *name* **-s** ipv6-source-address **-t** ● **ping6** *ipv6-address* **-vpn-instance** *name* **-t**。

目的	步骤
配置 EUI-64 格式的全球单播地址命令	1. 进入 VLANIF 配置视图、带外口配置视图、BD 接口配置视图、以太网路由接口配置视图或 Loopback 接口配置视图； 2. 执行如下命令： ● **ipv6 address** *ipv6-address/mask-length* **eui-64** ● **ipv6 address** *ipv6-address/mask-length* **eui-64 sub**。
删除指定 EUI-64 格式的全球单播地址命令	1. 进入 VLANIF 配置视图、带外口配置视图、BD 接口配置视图、以太网路由接口配置视图或 Loopback 接口配置视图； 2. 执行命令 **no ipv6 address** *ipv6-address* **eui-64**。
配置链路本地 IPv6 地址	1. 进入 VLANIF 配置视图、带外口配置视图、BD 接口配置视图、以太网路由接口配置视图或 Loopback 接口配置视图； 2. 执行命令 **ipv6 address** *ipv6-address* **link-local**。
删除链路本地 IPv6 地址	1. 进入 VLANIF 配置视图、带外口配置视图、BD 接口配置视图、以太网路由接口配置视图或 Loopback 接口配置视图； 2. 执行命令 **no ipv6 address link-local**。
配置自动生成的链路本地地址	1. 进入 VLANIF 配置视图、带外口配置视图、BD 接口配置视图、以太网路由接口配置视图或 Loopback 接口配置视图； 2. 执行命令 **ipv6 address auto link-local**。
删除自动生成的链路本地地址	1. 进入 VLANIF 配置视图、带外口配置视图、BD 接口配置视图、以太网路由接口配置视图或 Loopback 接口配置视图； 2. 执行命令 **no ipv6 address auto link-local**。

3.2.3 配置 IPv6 邻居发现功能

3.2.3.1 配置 IPv6 邻居请求消息发送的最大时间

目的

本节介绍如何配置 IPv6 邻居请求消息发送的最长时间。

过程

根据不同目的，执行相应步骤，具体参见下表。

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

目的	步骤
配置 IPv6 邻居发现的生命周期	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 在全局配置视图下执行命令 **ipv6 nd lifetime** { *life-time* | **default** }

3.2.3.2 配置 IPv6 静态邻居条目

目的

本节介绍如何配置 IPv6 静态邻居条目。

背景信息

目前设备最多可以支持 128 条静态邻居条目。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
添加一条 IPv6 静态邻居条目	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图； 3. 执行如下命令： ● **ipv6 neighbor** *ipv6-address mac-address* { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* [**vpn-instance** *name*] ● **ipv6 neighbor** *ipv6-address mac-address* **eth-trunk** *trunk-number* [**vpn-instance** *name*]。 或 1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 进入以太网路由接口配置视图； 3. 执行命令 **ipv6 neighbor** *ipv6-address mac-address*。
删除一条 IPv6 静态邻居条目	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 进入 VLANIF 配置视图、BD 接口配置视图、以太网路由接口配置视图、Loopback 接口配置视图； 3. 执行命令 **no ipv6 neighbor** *ipv6-address*。

3.2.4 配置 IPv6 调试和维护功能

目的

本节介绍 IPv6 收发包、邻居发现、路由等调试功能以及 IPv6 邻居错误统计信息重置功能。本操作用于维护及调试设备 IPv6 协议栈。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
打开 IPv6 收发包调试功能	1. 进入特权用户视图； 2. 执行命令 **debug ipv6** { **in** | **out** | **error** | **all** }打开该调试功能。
关闭 IPv6 收发包调试功能	1. 进入特权用户视图； 2. 执行命令 **no debug ipv6** { **in** | **out** | **error** | **all** }关闭该调试功能。
打开 RAW IPv6 收发包调试功能	1. 进入特权用户视图； 2. 执行命令 **debug rawip6** { **in** | **out** | **error** | **all** }打开该调试功能。
关闭 RAW IPv6 收发包调试功能	1. 进入特权用户视图； 2. 执行命令 **no debug rawip6** { **in** | **out** | **error** | **all** }关闭该调试功能。
打开 IPv6 ICMP 调试功能	1. 进入特权用户视图； 2. 执行命令 **debug icmp6 all** 打开该调试功能。
关闭 IPv6 ICMP 调试功能	1. 进入特权用户视图； 2. 执行命令 **no debug icmp6 all** 关闭该调试功能。
打开 IPv6 的 TCP 收发包调试功能	1. 进入特权用户视图； 2. 执行命令 **debug tcp6** { **in** | **out** | **error** | **event** | **all** }打开该调试功能。
关闭 IPv6 的 TCP 收发包调试功能	1. 进入特权用户视图； 2. 执行命令 **no debug tcp6** { **in** | **out** | **error** | **event** | **all** }关闭该调试功能。
打开 IPv6 的 UDP 收发包调试功能	1. 进入特权用户视图； 2. 执行命令 **debug udp6** { **in** | **out** | **error** | **all** }。
关闭 IPv6 的 UDP 收发包调试功能	1. 进入特权用户视图； 2. 执行命令 **no debug udp6** { **in** | **out** | **error** | **all** }。
打开目的 IPv6 地址的 ND 包收发包调试功能	1. 进入特权用户视图； 2. 执行命令 **debug nd** { **rxdst** | **txdst** } *ipv6-address*。
关闭目的 IPv6 地址的 ND 包收发包调试功能	1. 进入特权用户视图； 2. 执行命令 **no debug nd** { **rxdst** | **txdst** }。
打开源 IPv6 地址的 ND 包收发包调试功能	1. 进入特权用户视图； 2. 执行命令 **debug nd** { **rxsrc** | **txsrc** } *ipv6-address*。
关闭源 IPv6 地址的 ND 包收发包调试功能	1. 进入特权用户视图； 2. 执行命令 **no debug nd** { **rxsrc** | **txsrc** }。
打开目的 IPv6 地址的 IPv6 包收发包调试功能	1. 进入特权用户视图； 2. 执行命令 **debug ipv6** { **rxdst** | **txdst** } *ipv6-address*。
关闭目的 IPv6 地址的 IPv6 包收发包调试功能	1. 进入特权用户视图； 2. 执行命令 **no debug ipv6** { **rxdst** | **txdst** }。

目的	步骤
打开源 IPv6 地址的 IPv6 包收发包调试功能	1. 进入特权用户视图； 2. 执行命令 **debug ipv6** { **rxsrc** | **txsrc** } *ipv6-address*。
关闭源 IPv6 地址的 IPv6 包收发包调试功能	1. 进入特权用户视图； 2. 执行命令 **no debug ipv6** { **rxsrc** | **txsrc** }。
重置 IPv6 邻居错误统计信息	1. 进入全局配置视图； 2. 执行命令 **reset ipv6 neighbor error statistic**。

3.2.5 查看 IPv6 配置信息

目的

本节介绍如何查询 IPv6 配置信息。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
查看接口 IPv6 基本信息	1. 进入普通用户视图、特权用户视图、全局配置视图或 VLANIF 配置视图； 2. 执行如下命令： ● **show ipv6 interface** ● **show ipv6 interface** { **ethernet** | **gigaethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number* ● **show ipv6 interface vpn-instance** *name* ● **show ipv6 interface vlan** *vlan-id* ● **show ipv6 interface loopback** *loopback-number*。
查看设备上所有 IPv6 邻居节点信息，同时也支持显示多实例 VPN 情况下的信息。	1. 进入普通用户视图、特权用户视图、全局配置视图、OSPFv2 路由配置视图、VLANIF 配置视图或 Loopback 接口配置视图； 2. 执行如下命令： ● **show ipv6 neighbor** ● **show ipv6 neighbor** { **ethernet** | **gigaethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number* ● **show ipv6 neighbor bridge-domain** *bd-id* ● **show ipv6 neighbor** { **dynamic** | **static** | **vxlan** } ● **show ipv6 neighbor error statistic** ● **show ipv6 neighbor eth-trunk** *trunk-number* ● **show ipv6 neighbor** *ipv6-address* ● **show ipv6 neighbor vpn-instance** *name*

目的	步骤
	● **show ipv6 neighbor summary**。
查看设备 IPv6 路由条目信息	1. 进入普通用户视图、特权用户视图、全局配置视图、OSPFv2 路由配置视图、VLANIF 配置视图或 Loopback 接口配置视图； 2. 执行命令 **show ipv6 route**。
显示 IPv6 汇总路由信息	1. 进入普通用户视图、特权用户视图、全局配置视图或 VLANIF 配置视图； 2. 执行命令 **show ipv6 route summary**。
显示 IPv6 相关的统计信息	1. 进入普通用户视图、特权用户视图、全局配置视图或 VLANIF 配置视图； 2. 执行如下命令： ● **show ipv6 statistic** ● **show ipv6 statistic interface vlan** *vlan-id* ● **show ipv6 statistic interface** { **ethernet** | **gigaethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number*。
显示 IPv6 的 loopback 接口信息	1. 进入普通用户视图、特权用户视图、全局配置视图或 VLANIF 配置视图； 2. 执行命令 **show ipv6 interface loopback** *loopback-number*。
显示 IPv6 的 VLAN 接口信息	1. 进入普通用户视图、特权用户视图、全局配置视图或 VLANIF 配置视图； 2. 执行命令 **show ipv6 interface vlan** *vlan-id*。
显示 IPv6 地址前缀列表的表项信息	1.进入普通用户视图、特权用户视图或者全局配置视图。 2. 执行如下命令： ● **show ipv6 prefix-list** ● **show ipv6 prefix-list** *list-name*。
通过具体的 VLAN 显示 IPv6 的统计信息	1. 进入普通用户视图、特权用户视图、全局配置视图或 VLANIF 配置视图； 2. 执行如下命令： ● **show ipv6 statistic interface vlan** *vlan-id* ● **show ipv6 statistic interface** { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* ● **show ipv6 statistic interface** { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number.subinterface*。

3.2.6 查看 TCP/UDP 的连接状态

目的

本节介绍如何查看 TCP/UDP 的连接状态。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
查看设备当前已经建立的传输层协议类型为 IPv6 的 TCP 连接状态	1. 进入普通用户视图、全局配置视图或者特权用户视图； 2. 执行命令 **show tcp ipv6 status**。
查看设备当前已经建立的传输层协议类型为 IPv6 的 TCP 相关统计信息	1. 进入普通用户视图、全局配置视图或者特权用户视图； 2. 执行命令 **show tcp ipv6 statistic verbose**。
查看设备当前已经建立的传输层协议类型为 IPv6 的 UDP 连接状态	1. 进入普通用户视图、全局配置视图或者特权用户视图； 2. 执行命令 **show udp ipv6 status**。

3.2.7 配置举例

组网要求

两台 CN12800 设备通过 gigaethenet1/0/1 相连，该接口分别加入 VLANIF10，现在为 VLANIF10 配置 IPv6 全球单播地址，使其互通。

组网图

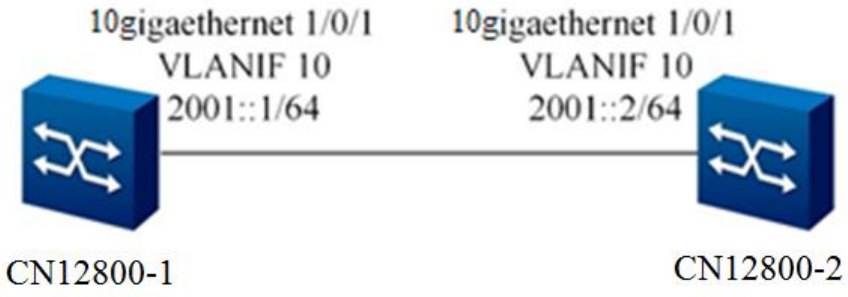


图 3-2 IPv6 地址配置拓扑图

配置步骤

1、配置 CN12800-1 的 VLAN10 接口的 IP 地址。

CN12800-1#configure

CN12800-1(config)#interface vlan 10

#使能接口 IPv6 功能。

```
CN12800-1(config-vlan-10)#ipv6 enable
CN12800-1(config-vlan-10)#ipv6 address 2001::1/64
CN12800-1(config-vlan-10)#quit
CN12800-1(config)#
CN12800-1(config)#interface 10gigaethernet 1/0/1
CN12800-1(config-10ge1/0/1)#port hybrid vlan 10 untagged
CN12800-1(config-10ge1/0/1)#port hybrid pvid 10
CN12800-1(config-10ge1/0/1)#quit
```

2、配置 CN12800-2 的 VLAN10 接口的 IP 地址。

```
CN12800-2#configure
CN12800-2(config)#interface vlan 10
#使能接口 IPv6 功能。
CN12800-2(config-vlan-10)#ipv6 enable
CN12800-2(config-vlan-10)#ipv6 address 2001::2/64
CN12800-2(config-vlan-10)#quit
CN12800-2(config)#
CN12800-2(config)#interface 10gigaethernet 1/0/1
CN12800-2(config-10ge1/0/1)#port hybrid vlan 10 untagged
CN12800-2(config-10ge1/0/1)#port hybrid pvid 10
CN12800-2(config-10ge1/0/1)#quit
```

3.3 DHCP 配置

3.3.1 DHCP 协议简介

DHCP 产生背景

连接到 Internet 的计算机需要在发送或接收数据报前知道其 IP 地址和其他信息，如网关地址、使用的子网掩码和域名服务器的地址。计算机可以通过 BOOTP 协议获取这些信息。 BOOTP 协议（Bootstrap Protocol）是一种较早出现的远程启动的协议，通过与远程服务器通信以获取通信所需的必要信息，主要用于无磁盘的客户端从服务器得到自己的 IP 地址、服务器的 IP 地址、启动映像文件名、网关 IP 地址等等。

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

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

DHCP 相关术语

- DHCP 服务器

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

- DHCP 客户端

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

- DHCP 中继

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

- DHCP Snooping

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

DHCP 常用选项

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

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

常见的 DHCP 选项有：

- Option 3：路由器选项，用来指定为客户端分配的网关地址。
- Option 6：DNS 服务器选项，用来指定为客户端分配的 DNS 服务器地址。
- Option 51：IP 地址租约选项。

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

更多 DHCP 选项的介绍，请参见 RFC 2132。

DHCP 优缺点

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

针对客户端的不同需求，DHCP 提供三种 IP 地址分配策略。管理员可以选择 DHCP 采用哪种策略响应每个网络或每台主机。

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

DHCP 从两个方面扩充了 BOOTP：

- DHCP 允许计算机快速、动态的获取 IP 地址。为使用 DHCP 的动态地址分配机制，管理员必须配置 DHCP 服务器，使其能提供一组 IP 地址，称之为地址池。任何时候一旦有新的计算机连接到网络上，该计算机就与服务器联系，并申请一个 IP 地址。服务器从配置的地址池中选择一个地址，并将它分配给该计算机。

- 与 BOOTP 相比，DHCP 可以为客户端提供更加丰富的网络配置信息。

DHCP 具有如下缺点：

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

 **注意：**

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

3.3.2 DHCP 服务器简介

DHCP Server 应用环境

在以下场合通常利用 DHCP 服务器来完成 IP 地址分配：

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

DHCP Server 地址管理

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

DHCP Server 安全功能

- 伪服务器检测功能

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

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

- IP 地址重复检测功能

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

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

- 地址匹配检测功能（防静态 IP 用户功能）

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

3.3.3 DHCP 中继简介

DHCP Relay 应用环境

原始的 DHCP 协议要求客户端和服务器只能在同一个子网内，不可以跨网段工作。因此，为进行动态主机配置需要在所有网段上都设置一个 DHCP 服务器，这显然是不经济的。DHCP 中继（DHCP Relay）的引入解决了这一问题，它在处于不同网段间的 DHCP 客户端和服务器之间承担中继服务，将 DHCP 协议报文跨网段中继到目的 DHCP 服务器，于是不同网络上的 DHCP 客户端可以共同使用一个 DHCP 服务器，既节省了成本，又便于进行集中管理。

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

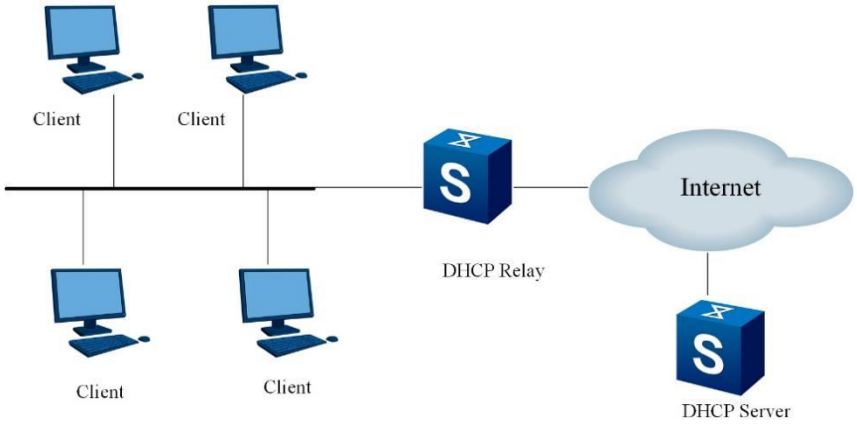


图 3-3 DHCP 应用环境示意图

DHCP Relay 支持的 Option82 选项

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

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

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

DHCP Relay 安全功能

- 地址匹配检测功能

  当客户端通过 DHCP 中继从 DHCP 服务器获取到 IP 地址时，DHCP 中继会记录 IP 地址与 MAC 地址的绑定关系。用户也可以手工配置用户地址表项，即 IP 地址与

MAC 地址的静态绑定。为了防止非法用户静态配置一个 IP 地址，并访问其他网络，设备支持 DHCP 中继的地址匹配检查功能。当设备上使能了该功能后，如果用户配置的 IP 地址与用户的 MAC 地址的对应关系没有在 DHCP 中继的用户地址表中（包括 DHCP 中继动态记录的表项以及手工配置的用户地址表项），则 DHCP 中继将不允许该用户访问外部网络。

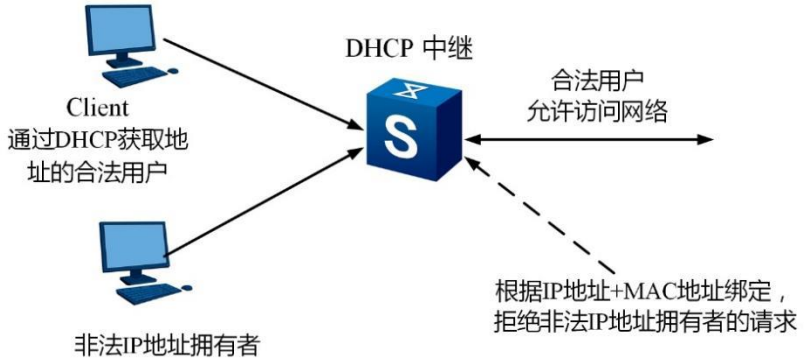


图 3-4 DHCP 安全示意图

- 用户表项定时刷新功能

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

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

  如果 DHCP 服务器响应 DHCP-ACK 报文，则表明这个 IP 地址已经可以进行分配，DHCP 中继会将动态用户地址表中对应的表项老化掉；

  如果 DHCP 服务器响应 DHCP-NAK 报文，则表示该 IP 地址的租约仍然存在，DHCP 中继不会老化该 IP 地址对应的表项。

- 伪服务器检测功能

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

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

3.3.4 配置 DHCP 服务器

前提条件

保证 DHCP Client 和 CN12800 之间能正常通信。

目的

配置 DHCP 服务器完成 IP 地址的分配。

过程

根据不同目的，执行相应步骤，具体参见下表。

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

3.3.5 配置 DHCP 服务器安全功能

前提条件

已配置 DHCP 服务器。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置 DHCP 伪服务器检测功能	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **dhcp start** 开启 DHCP 功能； 3. 执行命令 **dhcp server detect** { **enable** | **disable** }配置 DHCP 伪服务器检测功能。

3.3.6 配置 DHCP 中继

目的

配置 DHCP 中继跨网段实现 DHCP 服务器分配 IP 地址给用户。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
全局开启设备的 DHCP 功能	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **dhcp start** 全局开启 DHCP 功能。
配置 DHCP 接口工作模式为 Relay	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图； 3. 执行命令 **ip dhcp relay** 接口 DHCP 工作模式为 Relay。
配置 DHCP 中继所代理的 DHCP 服务器的 IP 地址	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图； 3. 执行命令 **dhcp relay server-ip** *ip-address* 配置 DHCP 中继所代理的 DHCP 服务器的 IP 地址。
使能或去使能 DHCP 中继支持 Option82 功能	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图； 3. 执行命令 **dhcp option82** { **enable** | **disable** }用来使能或去使能 DHCP 中继支持 Option82 功能。
配置 DHCP 中继对 DHCP 客户端发送携带了 Option82 的请求报文的处理策略	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图； 3. 执行命令 **dhcp option82** { **drop** | **keep** | **replace** }用来配置 DHCP 中继对 DHCP 客户端发送携带了 Option82 的请求报文的处理策略。
配置 DHCP Option82 选项子选项 Circuit ID 即电路 ID 的内容	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图； 3. 执行命令 **dhcp option82 circuit-id** *circuitid* 用来配置 DHCP Option82 选项子选项 Circuit ID 即电路 ID 的内容。
配置 DHCP Option82 选项子选项 Remote ID 即远程 ID 的内容	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图； 3. 执行命令 **dhcp option82 remote-id** *remoteid* 用来配置 DHCP Option82 选项子选项 Remote ID 即远程 ID 的内容。
配置 DHCP 中继的用户表项定时刷新的周期	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **dhcp relay user refresh-interval** { *interval* | **default** }配置 DHCP 中继的用户表项定时刷新的周期。

3.3.7 维护及调试

目的

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

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
打开 DHCP Relay 调试功能	1. 不执行任何命令保持当前特权用户视图； 2. 执行命令 **debug dhcp relay** { **event** | **packet** | **info** | **error** | **all** }打开 DHCP Relay 调试功能。
打开 DHCP server 调试功能	1. 不执行任何命令保持当前特权用户视图； 2. 执行命令 **debug dhcp server** { **event** | **packet** | **info** | **error** | **all** }打开 DHCP server 调试功能。
清除 DHCP 中继的统计信息	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **reset dhcp relay statistic** 清除 DHCP 中继的统计信息。
查看设备 DHCP 相关功能参数配置的状态信息	1. 进入普通用户视图、特权用户视图、全局配置视图或 VLANIF 配置视图； 2. 执行命令 **show dhcp** 用来显示设备 DHCP 相关功能参数配置的状态信息。
查看设备 DHCP 配置信息	1. 进入普通用户视图、特权用户视图、全局配置视图或 VLANIF 配置视图； 2. 执行命令 **show dhcp config** 用来显示设备 DHCP 配置信息。
查看 DHCP 中继服务器的配置信息	1. 进入普通用户视图、特权用户视图、全局配置视图或 VLANIF 配置视图； 2. 执行命令 **show dhcp relay** 用来显示 DHCP 中继服务器的配置信息。
查看 DHCP 中继的统计信息	1. 进入普通用户视图、特权用户视图、全局配置视图或 VLANIF 配置视图； 2. 执行命令 **show dhcp relay statistic** 用来显示 DHCP 中继的统计信息。
查看某个具体 VLAN 接口下 DHCP 相关的配置信息	1. 进入普通用户视图、特权用户视图、全局配置视图或 VLANIF 配置视图； 2. 执行命令 **show dhcp vlan** *vlan-id* **config** 用来显示某个具体 VLAN 接口下 DHCP 相关的配置信息。
供管理员查看网络上的 server 的信息	1. 进入普通用户视图、特权用户视图、全局配置视图或 VLANIF 配置视图； 2. 执行命令 **show dhcp fake-server**。

3.3.8 配置举例

组网要求

DHCP 服务器为处于不同网段中的客户端动态分配 IP 地址，用户所在的网段分别为 10.1.1.0/24 和 10.1.2.1/24。

具体需求如下：

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

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

组网图

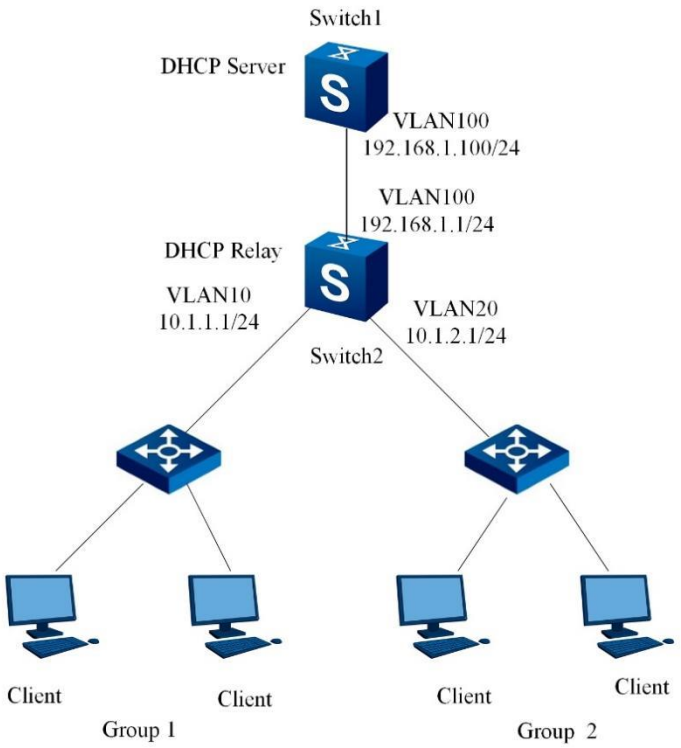


图 3-5 DHCP 配置拓扑图

配置步骤

1、配置 DHCP Server。

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

Switch#configure

Switch(config)#dhcp start

Switch(config)#interface vlan 100

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

2、配置 DHCP Relay。

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

Switch#configure

Switch(config)#dhcp start

Switch(config)#interface vlan 10

Switch(config-vlan-10)#ip address10.1.1.1/24

Switch(config-vlan-10)#ip dhcp relay

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

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

Switch#configure

Switch(config)#interface vlan 20

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

Switch(config-vlan-20)#ip dhcp relay

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

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

Switch#configure

Switch(config)#interface vlan 100

Switch(config-vlan-100)#ip address 192.168.1.1/24

Switch(config-vlan-100)#ip dhcp relay

3.4 DHCPv6 配置

3.4.1 配置 DHCPv6 基本功能

目的

本节介绍如何开启或关闭设备的 DHCPv6 功能以及如何配置 DHCPv6 中继。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
全局开启设备的 DHCPv6 功能	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **dhcpv6 start** 全局开启 DHCPv6 功能。
配置接口的 DHCPv6 工作模式为 Relay	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图； 3. 执行命令 **ipv6 enable** 开启 IPv6 功能； 4. 执行命令 **dhcpv6 relay** 配置接口 DHCPv6 工作模式为 Relay。
配置 DHCPv6 中继源 IP 地址	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图； 3. 执行命令 **dhcpv6 relay source-ip-address** *ipv6-address* 配置 DHCPv6 中继源 IP 地址。

目的	步骤
配置 DHCPv6 服务器或下一跳中继代理的 IPv6 地址	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图； 3. 执行如下命令： ● **dhcpv6 relay destination** *ipv6-address* ● **dhcpv6 relay destination** *ipv6-address* **vlan** *vlan-id*。
删除配置的 DHCPv6 服务器或下一跳中继代理的 IPv6 地址	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图； 3. 执行命令 **no dhcpv6 relay destination** *ipv6-address* 删除配置的 DHCPv6 服务器或下一跳中继代理的 IPv6 地址。
开启或关闭 Relay 接口的 remote-id 选项功能	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图； 3. 执行命令 **dhcpv6 relay remote-id** { **enable** | **disable** }用来开启或关闭 Relay 接口的 remote-id 选项功能。
配置 DHCPv6 报文中 remote-id 选项的格式	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **dhcpv6 remote-id format**{ **default** | **user-defined** *user-defined* }配置 DHCPv6 报文中 remote-id 选项的格式。

3.4.2 维护及调试

目的

当 DHCPv6 功能不正常，需要进行查看、调试或定位问题时，可以使用本小节操作。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
打开 DHCPv6 调试功能	1. 不执行任何命令保持当前特权用户视图； 2. 执行命令 **debug dhcpv6** { **global** | **server** | **relay** | **client** | **pkt** | **all** }打开 DHCPv6 调试功能。
清除 DHCPv6 的统计信息	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **reset dhcpv6 statistic** 清除 DHCPv6 的统计信息。
查看设备 DHCPv6 的全局信息以及各种资源的数目	1. 进入普通用户视图、全局配置视图、VLANIF 配置视图或特权用户视图； 2. 执行命令 **show dhcpv6** 用来显示设备 DHCPv6 的全局信息以及各种资源的数目。
查看设备 DHCPv6 的所有配置信息	1. 进入普通用户视图、全局配置视图、VLANIF 配置视图或特权用户视图； 2. 执行命令 **show dhcpv6 config** 用来显示设备 DHCPv6 的所有配置信息。

目的	步骤
查看 DHCPv6 中继服务器的配置信息	1. 进入普通用户视图、全局配置视图、VLANIF 配置视图或特权用户视图； 2. 执行如下命令： ● **show dhcpv6 relay** ● **show dhcpv6 relay interface** ● **show dhcpv6 relay interface vlan** *vlan-id* ● **show dhcpv6 relay interface** { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* ● **show dhcpv6 relay interface** { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number.subinterface*。
查看 DHCPv6 相关的统计信息	1. 进入普通用户视图、全局配置视图、VLANIF 配置视图或特权用户视图； 2. 执行如下命令： ● **show dhcpv6 statistic** ● **show dhcpv6 statistic interface vlan** *vlan-id* ● **show dhcpv6 statistic interface** { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* ● **show dhcpv6 statistic interface** { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number.subinterface*。
查看 DHCPv6 接口信息	1. 进入普通用户视图、全局配置视图、VLANIF 配置视图或特权用户视图； 2. 执行如下命令： ● **show dhcpv6 interface** ● **show dhcpv6 interface vlan** *vlan-id* ● **show dhcpv6 interface** { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* ● **show dhcpv6 interface** { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number.subinterface*。

3.5 DHCP Client 配置

3.5.1 DHCP Client 简介

DHCP Client 工作机制

DHCP 采用客户端/服务器通信模式，由客户端向服务器提出配置申请，服务器返回 IP 地址等相应的配置信息，以实现 IP 地址等信息的动态配置。

DHCP Client 为了获取到一个合法的动态 IP 地址，在不同的阶段，DHCP Client 需要与 Server 之间要交互不同的信息。

DHCP Client 的工作过程：

- 发现阶段：DHCP Client 通过发送 DISCOVER 报文来寻找 DHCP Server，由于 Server 对于 client 来说时未知的，所以会以广播的方式发送。
- 选择阶段：如果有多台 DHCP Server 向 DHCP Client 回应 offer 报文，则 DHCP Client 只接收第一个送到的 offer 报文，然后以广播的方式发送 REQUEST 报文。以广播的方式主要是为了通告其它未被选中的 Server 可以重新使用曾提供的 IP 地址。
- 对 Server 分配的地址进行有效的检测：client 在收到 server 返回的 ACK 后，会发送免费的 ARP 检测该 IP 是否可用，如果不可用，则会广播一个 DECLINE，重新开始申请 IP 地址。
- 更新租约：DHCP Server 分配给 DHCP Client 的 IP 地址一般都有一个租约期限，期满后，如果 DHCP Client 要延长其 IP 租约，则必须更新其的 IP 租约。

  1：IP 租约期限达到一半（T1）时，DHCP Client 会自动以单播的方式，

  向 Server 发送 REQUEST 报文，请求更新 IP 租约，如果收到 ACK 报文，则租约更新成功；如果收到 NAK 报文，则重新发起申请过程。

  2：到达租约期限的 87.5％(T2)时，如果仍未收到 DHCP Server 的应答，DHCP Client 会自动向 DHCP Server 发送更新其 IP 的广播报文，如果收到 ACK 报文，则租约更新成功；如果收到 NAK 报文，则重新发起申请过程。
- DHCP Client 主动释放 IP 地址：DHCP Client 不再使用分配的 IP 地址会主动向服务器发送 RELEASE 报文，通知 server 释放 IP 地址租约。

3.5.2 配置 DHCP Client 基本功能

前提条件

网络上已配置好 DHCP Server。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
使能或去使能 DHCP Client 自动获取 IP 地址的功能	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图； 3. 执行命令 **ip address dhcp** { **enable** | **disable** }使能或去使能 DHCP client 自动获取 IP 地址的功能。
更新 DHCP Client 获取的 IP 地址	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图； 3. 执行命令 **ip address dhcp renew** 更新 DHCP Client 获取的 IP 地址。
释放 DHCP Client 获取的 IP 地址	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图； 3. 执行命令 **ip address dhcp release** 释放 DHCP Client 获取的 IP 地址。

3.5.3 配置 Auto-config 模式及自定义模式下的选项信息

前提条件

网络上已配置好 DHCP Server。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置 Auto-config 模式	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **dhcp client auto-config mode** { **compatible** | **user-define** | **default** }配置 Auto-config 模式为兼容华为模式，用户自定义模式或默认浪潮网络模式。
配置 ftp-name 选项和子选项配置信息	1. 执行命令 **configure** 进入全局配置视图； 2. 执行如下命令： ● **dhcp client ftp-name option** *name-value* ● **dhcp client ftp-name option** *name-value* **sub-option** *sub-name-value*。
配置 ftp-password 选项和子选项配置信息	1. 执行命令 **configure** 进入全局配置视图； 2. 执行如下命令： ● **dhcp client ftp-password option** *password-value* ● **dhcp client ftp-password option** *password-value* **sub-option** *sub-password-value*。
配置 ftp-server-ip 选项和子选项配置信息	1. 执行命令 **configure** 进入全局配置视图； 2. 执行如下命令： ● **dhcp client ftp-server-ip option** *serverip-value* ● **dhcp client ftp-server-ip option** *serverip-value* **sub-option** *sub-serverip-value*。

目的	步骤
配置 image-file 选项和子选项配置信息	1. 执行命令 **configure** 进入全局配置视图； 2. 执行如下命令； ● **dhcp client image-file option** *imagefile-value* ● **dhcp client image-file option** *imagefile-value* **sub-option** *sub-imagefile-value*。
配置 reboot-time 选项和子选项配置信息	1. 执行命令 **configure** 进入全局配置视图； 2. 执行如下命令： ● **dhcp client reboot-time option** *reboottime-value* ● **dhcp client reboot-time option** *reboottime-value* **sub-option** *sub-reboottime-value*。
配置 auth-message 选项和子选项配置信息	1. 执行命令 **configure** 进入全局配置视图； 2. 执行如下命令： ● **dhcp client auth-message option** *authmessage-value* ● **dhcp client auth-message option** *authmessage-value* **sub-option** *sub-authmessage-value*。
配置 image-file 选项和子选项配置信息	1. 执行命令 **configure** 进入全局配置视图； 2. 执行如下命令： ● **dhcp client image-file option** *imagefile-value* ● **dhcp client image-file option** *imagefile-value* **sub-option** *sub-imagelistfile-value*。

3.5.4 维护及调试

目的

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

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
打开 DHCP Client 调试功能	1. 执行命令 **configure** 进入全局配置视图或不执行任何命令保持当前特权用户视图； 2. 执行命令 **debug dhcp client** { **state** | **in** | **out** | **packet** | **all** }打开 DHCP Client 调试功能。
查看全部或者单个 VLAN 接口的 DHCP 客户端状态信息	1. 进入普通用户视图、特权用户视图、全局配置视图或 VLANIF 配置视图； 2. 执行如下命令； ● **show dhcp client** ● **show dhcp client vlan** *vlan-id*。

目的	步骤
查看 auto-config 在 VLAN 接口下的全部配置信息	1. 进入普通用户视图、特权用户视图、全局配置视图或 VLANIF 配置视图； 2. 执行命令 **show dhcp client auto-config vlan** *vlan-id* 用来显示 auto-config 在 VLAN 接口下的全部配置信息。
查看全部或者单个 VLAN 接口的 DHCP 客户端收发包信息	1. 进入普通用户视图、特权用户视图、全局配置视图或 VLANIF 配置视图； 2. 执行如下命令； ● **show dhcp client statistic** ● **show dhcp client statistic vlan** *vlan-id*。

3.5.5 配置举例

组网要求

DHCP 协议是典型的工作在 server-client 模式下的协议，下图是 DHCP Client 和 Server 都在同一个子网内，直接进行 DHCP 协议的交互。

组网图

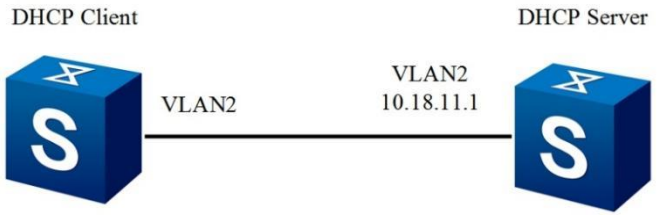


图 3-6 DHCP Client 配置拓扑图

配置步骤

1、在 DHCP Client 交换机上为接口配置 VLAN。

Switch#configure

Switch(config)#vlan 2

Switch(vlan-2)#quit

Switch(config)#interface xge1/0/2

Switch(config-10ge1/0/2)#no shutdown

Switch(config-10ge1/0/2)#port hybrid vlan 2 untagged

Switch(config-10ge1/0/2)#port hybrid pvid 2

Switch(config-10ge1/0/2)#quit

2、使能 DHCP Client 动态获取 IP 地址功能。

Switch(config)#interface vlan 2

Switch(config-vlan-2)#ip address dhcp enable

3、验证获取到的配置结果。

Switch#show dhcp client

DHCP client information:

Interface:vlan-2

Current state…..: Bound

Allocated IP……: 10.18.11.2

Subnet Mask…..:255.255.255.0

Server IP……..:10.18.11.1

Allocated lease..:86400 seconds

Lease T1 time…:43200 seconds

Lease T2 time…:75600 seconds

Lease Obtained.:2100/06/28 Mon 05:23:36

Lease timeout…:2100/06/29 Tue 05:23:36

Transaction ID….:0x7f43

Client ID…….:01 00 04 67 99 9e 6c

DHS……...:

Gateway……:10.18.11.1

Domain……..:

Lease time will time out in 0 days 23 hours 59 minutes 50 seconds.

4、更新 DHCP Client 接口上的租约信息。

Switch(config)#int vlan 2

Switch(config-vlan-2)#ip address dhcp renew

5、验证更新租约信息后的配置结果，可以看出从 23:59:50 更新到 23:59:56。

Switch(config)#show dhcp client

DHCP client information:

Interface:vlan-2

Current state…..: Bound

Allocated IP……: 10.18.11.2

Subnet Mask…..:255.255.255.0

Server IP……..:10.18.11.1

Allocated lease..:86400 seconds

Lease T1 time…:43200 seconds

Lease T2 time…:75600 seconds

Lease Obtained.:2100/06/28 Mon 05:24:55

Lease timeout…:2100/06/29 Tue 05:24:55

Transaction ID….:0x7f43

Client ID……:01 00 04 67 99 9e 6c

DHS……...:

Gateway……:10.18.11.1

Domain……..:

Lease time will time out in 0 days 23 hours 59 minutes 56 seconds.

6、释放 DHCP Client 接口上的 IP 地址。

Switch(config)#int vlan 2

Switch(config-vlan-2)#ip address dhcp release

7、验证更新租约信息后的配置结果。

Switch(config-vlan-2)#ip address dhcp release

Switch(config-vlan-2)#show dhcp client vlan 2

Current state…..: Release

Allocated IP……: 0.0.0.0

Subnet Mask…...:0.0.0.0

Server IP……..:0.0.0.0

第4章 三层 IP 路由配置

本章介绍了 CN12800 系列数据中心交换机路由相关的基本内容、配置过程和配置举例。

4.1 静态路由配置

4.1.1 IPv4 静态路由配置

目的

本节介绍如何增加或者删除一条 IPv4 静态路由。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
增加一条 IPv4 静态路由	1. 进入全局配置视图； 2. 执行如下命令： ● **ip route-static** *ip-address mask-address nexthop-address* ● **ip route-static preference** { *preference-value* | **default** } ● **ip route-static** *ip-address mask-address nexthop-address* **preference** *preference-value* ● **ip route-static** *ip-address mask-address nexthop-address* **track bfd** *track-number* ● **ip route-static** *ip-address mask-address* **interface null** *null-number* ● **ip route-static** *ip-address mask-address* **interface tunnel** *tunnel-number*。
删除某条或者全部 IPv4 静态路由	1. 进入全局配置视图； 2. 执行如下命令： ● **no ip route-static** *ip-address mask-address nexthop-address* **track bfd** ● **no ip route-static** *ip-address mask-address* ● **no ip route-static** *ip-address mask-address nexthop-address*。
删除某条 IPv4 静态路由对应的特定 VPN 实例	1. 进入全局配置视图； 2. 执行命令 **no ip route-static all**。
配置经过 NULL 接口的 IP 路由	1. 进入全局配置视图； 2. 执行命令 **ip route-static** *ip-address mask-address* **interface null** *null-number*。

4.1.2 维护及调试

目的

当静态路由配置功能不正常，需要进行查看、定位问题时，用户可以使用本小节操作。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
查看特定的一条或多条路由信息	1. 进入特权用户视图、全局配置视图、普通用户视图； 2. 执行如下命令： ● **show ip route** ● **show ip route** *ip-address*。
查看 IPv4 路由表的综合路由统计信息	1. 进入特权用户视图、全局配置视图、普通用户视图； 2. 执行命令 **show ip route statistic**。
查看汇总路由信息	1. 进入特权用户视图、全局配置视图、普通用户视图； 2. 执行命令 **show ip route summary**。
查看设备从上电或上次清除统计以来记录的IPv4或IPv6路由错误统计信息	1. 进入特权用户视图、全局配置视图、普通用户视图； 2. 执行命令 **show** { **ip** | **ipv6** } **route error statistic**。
清除设备记录的IPv4或IPv6路由错误统计信息	1. 进入特权用户视图、全局配置视图、普通用户视图； 2. 执行命令 **reset** { **ip** | **ipv6** } **route error statistic**。

4.2 DID 配置

目的

本节介绍如何配置 DID（Destination IP Detect，目的 IP 检测）功能。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
调试 DID	1. 保持特权用户视图； 2. 执行命令 **debug did** { **event** | **detect** | **cmd** | **off** | **all** }。
查看 DID 资源信息	1. 在普通视图或特权用户视图下； 2. 执行命令 **show did resource**。

查看 DID 对端信息	1. 在普通视图或特权用户视图下； 2. 执行命令 **show did peer**。

4.3 OSPF 配置

4.3.1 OSPF 简介

4.3.1.1 产生背景

OSPF（Open Shortest Path First，开发最短路径优先）协议是由 Internet Engineering Task Force 的 OSPF 工作组所开发的，特别为 TCP/IP 网络而设计，包括明确的支持 CIDR 和标记来源于外部的路由信息。OSPF 也提供了对路由更新的验证，并在发送/接收更新时使用 IP 多播。此外，还作了很多的工作使得协议仅用很少的路由流量就可以快速地响应拓扑改变。

OSPF 仅通过在 IP 包头中的目标地址来转发 IP 包。IP 包在 AS 中被转发，而没有被其他协议再次封装。OSPF 是一种动态路由协议，它可以快速地探知 AS 中拓扑的改变（例如路由器接口的失效），并在一段时间的收敛后计算出无环路的新路径。收敛的时间很短且只使用很小的路由流量。

在连接状态路由协议中，每台路由器都维持着一个数据库以描述 AS 的拓扑结构。这个数据库被称为连接状态数据库，所有参与的路由器都有着同样的数据库。数据库中的各项说明了特定路由器自身的状态（如该路由器的可用接口和可以到达的邻居）。该路由器通过洪泛/flooding 将其自身的状态传送到整个 AS 中。

所有的路由器同步地运行完全相同的算法。根据连接状态数据库，每台路由器构建出一棵以其自身为树根的最短路径树。最短路径树给出了到达 AS 中各个目标的路径，路由信息的起源在树中表现为树叶。当有多条等值的路径到达同一目标时，数据流量将在这些路径上平均分摊。路径的距离值表现为一个无量纲数。

OSPF 允许将一些网络组合到一起。这样的组被称为区域/area。区域对 AS 中的其他部分隐藏其内部的拓扑结构，信息的隐藏极大地减少了路由流量。同时，区域内的路由仅由区域自身的拓扑来决定，这可使区域抵御错误的路由信息。区域通常是一个子网化了的 IP 网络。OSPF 允许灵活的配置 IP 子网。由 OSPF 发布的每条路径都包含目标和掩码。同一个 IP 网络的两个子网可以有不同的大小（即不同的掩码），这常被称为变长子网/variable length subnetting。数据包按照最佳匹配（最长匹配）来转发。主机路径被看作掩码为“全 1”（0xffffffff）的子网来处理。

OSPF 协议中所有的信息交换都支持验证。这意味着，在 AS 中只有被信任的路由器才能参与路由。有多种验证方法可以被选择。事实上，可以为每个 IP 子网选用不同的验证方法。来源于外部的路由信息（如路由器从诸如 BGP［引用 23］的外部网关协议中得到的路径）向整个 AS 内部宣告。外部数据与 OSPF 协议的连接状态数据相对独立。每条外部路径可以由所宣告的路由器作出标记，由自治系统边界路由器（ASBR）向自治系统内传递额外的信息。

4.3.1.2 协议特点

- 适应范围广：支持各种规模的网络，最多可支持几百台路由器；
- 快速收敛：在网络的拓扑结构发生变化后立即发送更新报文，使得自治系统中的其他节点能够快速同步这一变化；
- 无环路：OSPF 根据收集到的链路状态，用最短路径树算法计算路由，该算法保证了 OSPF 不会生成自环路由；
- 区域划分：允许自治系统的网络被划分成区域来管理，区域间传送的路由信息被进一步抽象，减少了占用的网络带宽和系统资源；
- 等价路由：支持到同一目的地址的多条等价路由；
- 路由分级：使用 4 类不同的路由。按优先顺序分别是：区域内路由、区域间路由、第一类外部路由、第二类外部路由；
- 支持验证：支持基于接口的报文验证，保证报文交互的安全性；
- 组播发送：在能够发送组播的链路上，以组播地址发送协议报文，减少对其他设备的干扰。

4.3.1.3 基本概念

OSPF 路由的计算过程

OSPF 路由的计算过程可简单描述如下：

1. 每台 OSPF 路由器根据自己周围的网络拓扑结构生成链路状态通告 LSA（Link State Advertisement），并通过更新报文将 LSA 发送给网络中的其它 OSPF 路由器。
2. 每台 OSPF 路由器都会收集其它路由器发来的 LSA，所有的 LSA 形成链路状态数据库 LSDB（Link State Database），LSDB 是对整个自治系统的网络拓扑结构的描述。

3. OSPF 路由器将 LSDB 转换成一张带权的有向图，这张图是对整个网络拓扑结构的真实反映。各 OSPF 路由器得到的有向图是完全相同的。

4. 每台 OSPF 路由器根据有向图，使用 SPF 算法计算出一棵以自己为根的最短路径树，这棵树给出了到自治系统中各节点的路由。

路由器 ID 号

一台路由器如果要运行 OSPF 协议，必须存在路由器 ID。路由器 ID 是一个 32 比特无符号整数，是一台路由器在自治系统中的唯一标识。

路由器的 ID 可以手工配置，也可以由系统自动产生。如果是自动产生则遵循如下规则：

1. 最大的静态环回地址；

2. 最大的静态主地址；

3. 最大的静态次地址；

4. 最大的静态 linklocal 地址；

5. 最大的 DHCP 分配的地址；

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

同时可以使用这个命令来手工配置 ID，输入的 ID 不限于本地 IP 地址。为增强网络的稳定性，OSPF 的 ID 不随 IP 地址变化而变化，即使 ID 对应的 IP 地址被删除，也不会自动改变 OSPF 的 ID。修改 OSPF 的 ID 后，OSPF 的邻居，数据库等信息会全部重新刷新，一段时间内会产生大量的协议流量，对网络造成冲击，因此不建议频繁使用本命令。

OSPF 的协议报文

OSPF 有以下五种类型的协议报文：

1. Hello 报文：周期性发送，用于发现和维持 OSPF 邻居关系。

2. DD（Database Description Packet）报文：描述本地 LSDB 的摘要信息，用于两台路由器开始建立邻接时进行数据库同步。

3. LSR 报文（Link State Request Packet）：向对方请求所需的 LSA。

4. LSU 报文（Link State Update Packet）：向对方发送其所需要的 LSA。

5. LSAck 报文（Link State Acknowledgment Packet）：用来对收到的 LSA 进行确认。

LSA 的类型

OSPF 中对路由信息的描述都是封装在 LSA 中发布出去，常用的 LSA 有以下类型：

1. Router LSA（Type1）：每个路由器都会产生，描述了路由器的链路状态和开销，在所属的区域内传播。
2. Network LSA（Type2）：由 DR 产生，描述本网段的链路状态，在所属的区域内传播。
3. Network Sumary LSA（Type3）：由 ABR（Area Border Router）产生，描述区域内某个网段的路由，并通告给其他区域。
4. ASBR Summary LSA（Type4）：由 ABR 产生，描述到 ASBR（Autonomous System Boundary Router）的路由，通告给相关区域。
5. AS External LSA（Type5）：由 ASBR 产生，描述到 AS 外部的路由，通告到所有的区域（除了 Stub 区域和 NSSA（Not-So-Stubby Area）区域）。
6. NSSA LSA（Type7）：由 ASBR 产生，描述到 AS 外部的路由，仅在 NSSA 区域内传播。

邻居和邻接

在 OSPF 中，邻居（Neighbors）和邻接（Adjacencies）是两个不同的概念。

1. 邻居关系：SPF 路由器启动后，会通过 OSPF 接口向外发送 Hello 报文。收到 Hello 报文的 OSPF 路由器会检查报文中所定义的一些参数，如果双方一致就会形成邻居关系。
2. 邻接关系：形成邻居关系的双方不一定都能形成邻接关系，这要根据网络类型而定。只有当双方成功交换 DD 报文，并能交换 LSA 之后，才形成真正意义上的邻接关系。

4.3.1.4 OSPF 区域与路由聚合

划分区域

由于网络规模增大，运行 OSPF 路由协议的路由器数量增多，网络和路由器会产生以下的变化。

1. 网络方面的变化

拓扑结构发生变化的概率增大，网络会经常处于“动荡”之中，造成网络中大量的 OSPF 协议报文传递，降低了网络的带宽利用率。每一次拓扑结构发生变化都会导致网络中所有的路由器重新进行路由计算。

2. 路由器方面的变化

(1) LSDB 增大；

(2) 占用存储空间增加；

(3) SPF 算法变复杂；

(4) CPU 负担变重。

3. 划分区域

为了解决上述问题，OSPF 协议将自治系统划分成不同的区域（Area）。区域是从逻辑上将路由器划分为不同的组，每个组用区域号（Area ID）来标识。区域的边界是路由器，而不是链路。一个网段（链路）只能属于一个区域，或者说每个运行 OSPF 的接口必须指明属于哪一个区域，如图 4-1 所示。

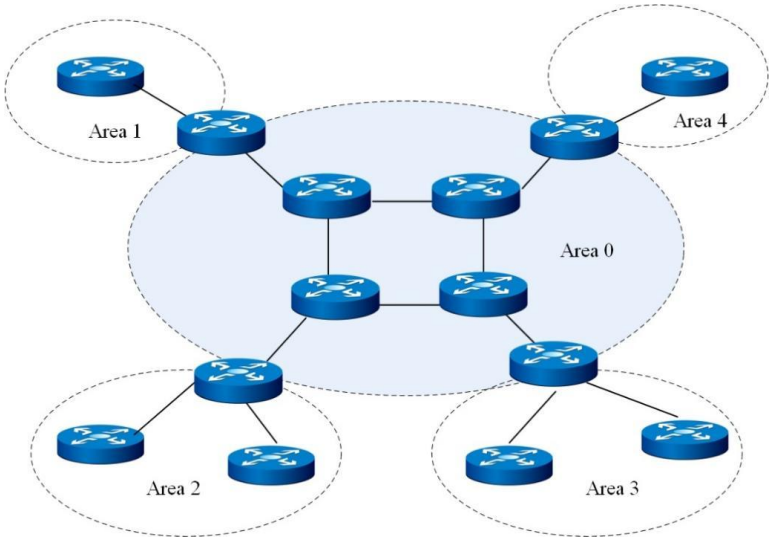


图 4-1 区域划分

划分区域后，可以在区域边界路由器上进行路由聚合，减少通告到其他区域的 LSA 数量。另外，划分区域还可以使网络拓扑变化造成的影响最小化。

路由器的类型

如图 4-2 所示，OSPF 路由器根据在 AS 中的不同位置，可以分为以下四种类型：

1. 区域内路由器（Internal Routers）

路由器的所有接口都属于同一个 OSPF 区域。

2. 区域边界路由器 ABR（Area Border Routers）

路由器可以同时属于两个以上的区域，但其中一个必须是骨干区域。ABR 用来连接骨干区域和非骨干区域，它与骨干区域之间既可以是物理连接，也可以是逻辑上的连接。

3. 骨干路由器（Backbone Routers）

路由器至少有一个接口属于骨干区域，因此，所有的 ABR 和位于 Area0 的内部路由器都是骨干路由器。

4. 自治系统边界路由器 ASBR（AS boundary Routers）

与其他 AS 交换路由信息的路由器称为 ASBR。ASBR 并不一定位于 AS 的边界，它有可能是区域内路由器，也有可能是 ABR。只要一台 OSPF 路由器引入了外部路由的信息，它就成为 ASBR。

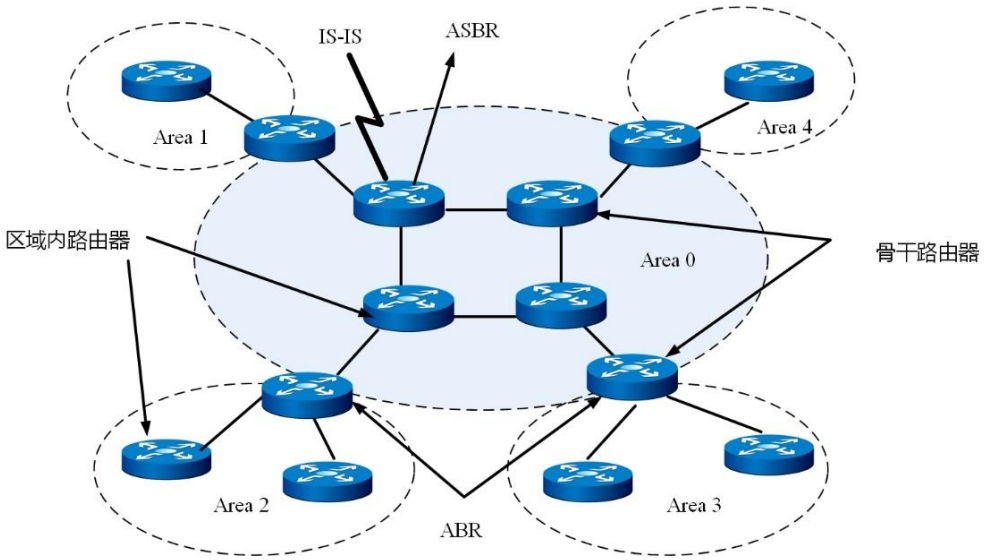


图 4-2 OSPF 路由器的类型

骨干区域

OSPF 划分区域之后，并非所有的区域都是平等的关系。其中有一个区域与众不同，通常被称为骨干区域，它的区域号（Area ID）是 0。

骨干区域负责区域之间的路由，非骨干区域之间的路由信息必须通过骨干区域来转发。对此，OSPF 有以下规定：

所有非骨干区域必须与骨干区域保持连通。骨干区域自身也必须保持连通。但在实际应用中，可能会因为网络拓扑等限制，无法满足以上要求；这时可以通过配置 OSPF 虚连接满足要求。

虚连接

虚连接指在两台 ABR 之间通过一个非骨干区域而建立的一条逻辑上的连接通道。虚连接相当于在两个 ABR 之间形成了一个点到点的连接。为虚连接两端提供一条非骨干区域内部路由的区域称为中转区域（Transit Area）。

虚连接有如下特点：

1. 虚连接的两端必须是 ABR。
2. 必须在两端同时配置虚连接，虚连接方能生效。
3. 虚连接和物理接口一样可以配置接口参数，如发送 HELLO 报文间隔等。
4. 两台 ABR 之间直接传递 OSPF 报文信息时，他们之间的 OSPF 路由器只起到转发报文的作用。由于协议报文的目的地址不是这些路由器，所以这些报文对于他们而言是透明的，只是当作普通的 IP 报文来转发。

Stub 区域

1. Stub 区域的特点

Stub 区域的 ABR 不传播它们接收到的自治系统外部路由，在这些区域中路由器的路由表规模以及路由信息传递的数量会大大减少。

Stub 区域是一种可选的配置属性，并不是每个区域都符合配置的条件。通常来说，Stub 区域是位于自治系统边界，只有一个 ABR 的非骨干区域。

为保证到自治系统外的路由依旧可达，Stub 区域的 ABR 将生成一条缺省路由，并发布给 Stub 区域中的其他非 ABR 路由器。

2. 配置 Stub 区域的注意事项

骨干区域不能配置成 Stub 区域。

如果要将一个区域配置成 Stub 区域，则该区域中的所有路由器必须都要配置 Stub 区域。

Stub 区域内不能存在 ASBR，即自治系统外部的路由不能在本区域内传播。虚连接不能穿过 Stub 区域。

NSSA 区域

在 RFC1587 NSSA Option 中增加一类新的区域：NSSA 区域；同时增加一类新的 LSA：NSSA LSA（或称为 Type7 LSA）。

NSSA 区域其实是 Stub 区域的一个变形，它和 Stub 区域有许多相似的地方。

1. NSSA 区域的特点

与 Stub 区域类似，NSSA 区域也不能配置虚连接。

与 Stub 区域类似，NSSA 区域也不允许 AS-External-LSA 即 Type5 LSA 注入，但可以允许 Type7 LSA 注入。

Type7 LSA 由 NSSA 区域的 ASBR 产生，在 NSSA 区域内传播。

当 Type7 LSA 到达 NSSA 的 ABR 时，由 ABR 将 Type7 LSA 转换成 AS-External LSA，传播到其他区域

2. NSSA 区域举例

如图 4-3 所示，运行 OSPF 协议的自治系统包括 3 个区域：区域 1、区域 2 和区域 0，区域 1 被定义为 NSSA 区域。与区域 1、区域 2 相连的非 OSPF 网络运行 RIP 协议。

区域 1 从 RIP 网络接收的 RIP 路由传播到 NSSA ASBR 后，由 NSSA ASB 产生 Type7 LSA 在区域 1 内传播；当 Type7 LSA 到达 NSSA ABR 后，转换成 Type5 LSA 传播到区域 0 和区域 2。

另一方面，区域 2 从 RIP 网络中接收的 RIP 路由通过区域 2 的 ASBR 产生 Type-5LSA 在 OSPF 自治系统中传播。但由于区域 1 是 NSSA 区域，所以 Type-5 LSA 不会到达区域 1。

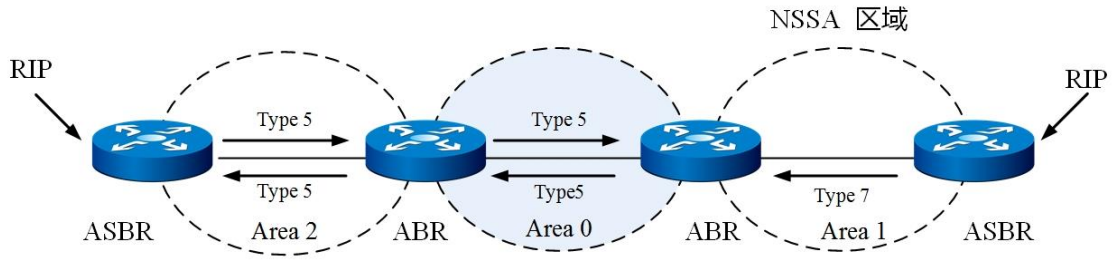


图 4-3 NSSA 区域

路由聚合

路由聚合是指：ABR 将具有相同前缀的路由信息聚合在一起后，形成一条路由发布到其它区域。

AS 被划分成不同的区域后，区域间可以通过路由聚合来减少路由信息，减小路由表的规模，提高路由器的运算速度。

例如，区域 1 内有三条区域内路由 19.1.1.0/24，19.1.2.0/24，19.1.3.0/24，如果此时在 ABR 上配置了路由聚合，将三条路由聚合成一条 19.1.0.0/16，则 ABR 就只生成一条聚合后的 LSA，并发布给其他区域的路由器。

路由类型

OSPF 将路由分为 4 级，按优先顺序分别是：

区域内路由（Intra Area）；

区域间路由（Inter Area）；

第一类外部路由（Type1 External）；

第二类外部路由（Type2 External）。

1. AS 内部路由

AS 区域内和区域间路由描述的是 AS 内部的网络结构。缺省情况下，这两种路由的协议优先级为 10。

2. AS 外部路由

外部路由则描述了应该如何选择到 AS 以外目的地址的路由。OSPF 将引入的 AS 外部路由分为两类：Type1 和 Type2。缺省情况下，这两种路由的协议优先级为 150。

第一类外部路由：指接收的是 IGP 路由（例如静态路由和 RIP 路由）。由于这类路由的可信程度比较高，所以计算出的外部路由的开销与自治系统内部的路由开销是相同的，并且和 OSPF 自身路由的开销具有可比性；即到第一类外部路由的开销等于本路由器到相应的 ASBR 的开销+ASBR 到该路由目的地址的开销。

第二类外部路由：指接收的是 EGP 路由。由于这类路由的可信度比较低，所以 OSPF 协议认为从 ASBR 到自治系统之外的开销远远大于在自治系统之内到达 ASBR 的开销；所以计算路由开销时将主要考虑前者，即到第二类外部路由的开销=ASBR 到该路由目的地址的开销。如果两条路由计算出的开销值相等，再考虑本路由器到相应的 ASBR 的开销。

4.3.1.5 OSPF 网络

OSPF 网络类型

根据链路层协议类型将网络分为下列四种类型：

1. 广播（Broadcast）类型

当链路层协议是 Ethernet、FDDI（Fiber Distributed Digital Interface）时，OSPF 缺省认为网络类型是 Broadcast。在该类型的网络中，通常以组播形式（224.0.0.5 和 224.0.0.6）发送协议报文。

2. NBMA（Non-Broadcast Multi-Access）类型

当链路层协议是帧中继、ATM 或 X.25 时，OSPF 缺省认为网络类型是 NBMA。在该类型的网络中，以单播形式发送协议报文。

3. 点到多点 P2MP（point-to-multipoint）类型

没有一种链路层协议会被缺省的认为是 Point-to-Multipoint 类型。点到多点必须是由其他的网络类型强制更改的。常用做法是将非全连通的 NBMA 改为点到多点的网络。在该类型的网络中，以组播形式（224.0.0.5）发送协议报文。

4. 点到点 P2P（point-to-point）类型

当链路层协议是 PPP、HDLC 和 LAPB 时，OSPF 缺省认为网络类型是 P2P。在该类型的网络中，以组播形式（224.0.0.5）发送协议报文。

DR 和 BDR

在广播网和 NBMA 网络中，任意两台路由器之间都要传递路由信息。如果网络中有 n 台路由器，则需要建立 nx(n-1)/2 个邻接关系。这使得任何一台路由器的路由变化都会导致多次传递，浪费了带宽资源。

为解决这一问题，OSPF 协议定义了 DR（Designated Router）、BDR（Backup Designated Router）和除 DR 和 BDR 之外的路由器（DR Other）。

1. DR

所有路由器都只将信息发送给 DR，由 DR 将网络链路状态广播出去。

2. BDR

如果 DR 由于某种故障而失效，则网络中的路由器必须重新选举 DR，并与新的 DR 同步。这需要较长的时间，在这段时间内，路由的计算是不正确的。为了能够缩短这个过程，OSPF 提出了 BDR（Backup Designated Router）的概念。BDR 实际上是对 DR 的

一个备份，在选举 DR 的同时也选举出 BDR，BDR 也和本网段内的所有路由器建立邻接关系并交换路由信息。当 DR 失效后，BDR 会立即成为 DR。由于不需要重新选举，并且邻接关系事先已建立，所以这个过程是非常短暂的。当然这时还需要再重新选举出一个新的 BDR，虽然一样需要较长的时间，但并不会影响路由的计算。

3. DR Other

除 DR 和 BDR 之外的路由器（DR Other）之间将不再建立邻接关系，也不再交换任何路由信息。这样就减少了广播网和 NBMA 网络上各路由器之间邻接关系的数量。

DR/BDR 选举

1. DR/BDR 选举过程

DR 和 BDR 不是人为指定的，而是由本网段中所有的路由器共同选举出来的。路由器接口的 DR 优先级决定了该接口在选举 DR、BDR 时所具有的资格。本网段内 DR 优先级大于 0 的路由器都可作为“候选人”。选举中使用的“选票”就是 Hello 报文。选举过程如下：

每台路由器将自己选出的 DR 写入 Hello 报文中，发给网段上的每台路由器。

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

2. DR/BDR 选举特点

只有在广播或 NBMA 类型接口时才会选举 DR，在点到点或点到多点类型的接口上不需要选举 DR。

DR 是指某个网段中概念，是针对路由器的接口而言的。某台路由器在一个接口上可能是 DR，在另一个接口上有可能是 BDR，或者是 DR Other。

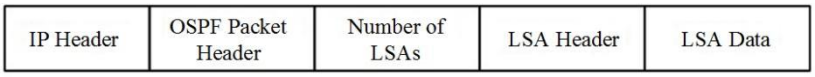
若 DR、BDR 已经选择完毕，当一台新路由器加入后，即使它的 DR 优先级值最大，也不会立即成为该网段中的 DR。

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

4.3.1.6 OSPF 报文格式

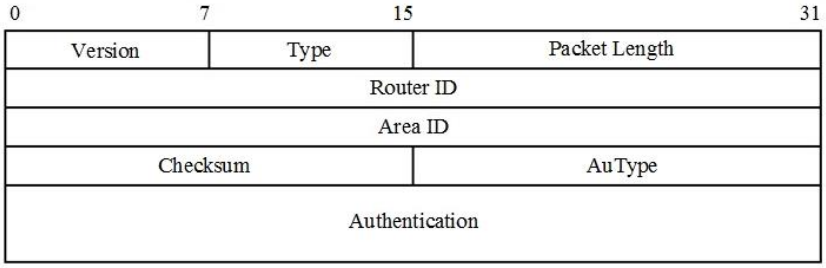
OSPF 报文结构

OSPF 用 IP 报文直接封装协议报文，协议号为 89。一个比较完整的 OSPF 报文（以 LSU 报文为例）结构如下图所示。



OSPF 报文头

OSPF 有五种报文类型，他们有相同的报文头。如下图所示：



主要字段的解释如下：

Version：OSPF 的版本号，对于 OSPFv2，其值为 2。

Type：OSPF 报文的类型，数值从 1 到 5，分别对应 Hello 报文、DD 报文、LSR 报文、LSU 报文和 LSAck 报文。

Packet length：OSPF 报文的总长度，包括报文头在内，单位为字节。

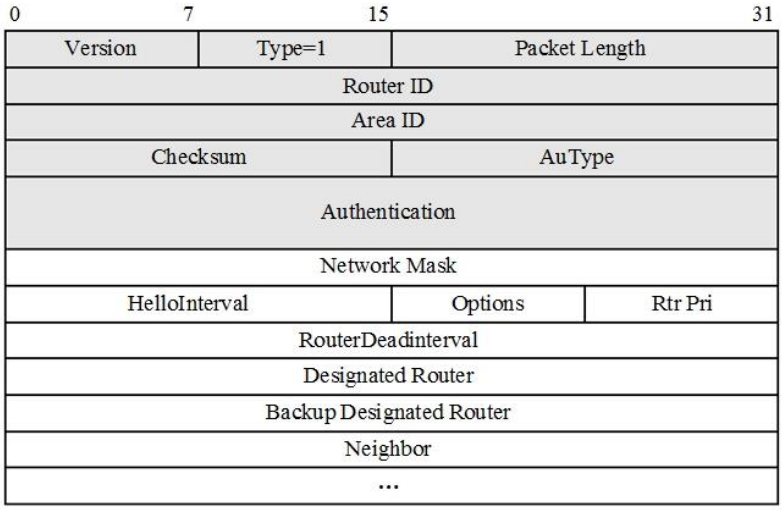
AuType：验证类型。可分为不验证、简单验证和 MD5 验证，其值分别为 0、1、2。

Authentication：其数值根据验证类型而定。当验证类型为 0 时未作定义，为 1 时此字段为密码信息，类型为 2 时此字段包括 Key ID、MD5 验证数据长度和序列号的信息。

MD5 验证数据添加在 OSPF 报文后面，不包含在 Authenticaiton 字段中。

Hello 报文

最常用的一种报文，周期性的发送给本路由器的邻居。内容包括一些定时器的数值、DR、BDR 以及自己已知的邻居。Hello 报文格式如下图所示。



主要字段解释如下：

Network Mask：发送 Hello 报文的接口所在网络的掩码。

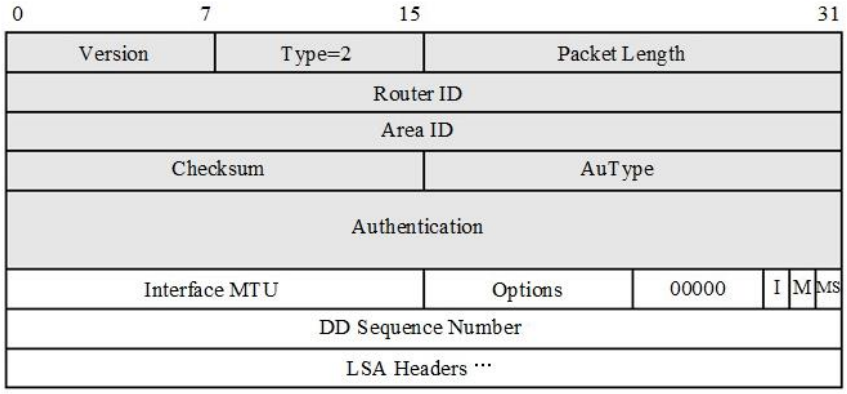
HelloInterval：发送 Hello 报文的时间间隔。如果相邻两台路由器的 Hello 间隔时间不同，则不能建立邻居关系。

Rtr Pri：DR 优先级。如果设置为 0，则路由器不能成为 DR/BDR。

RouterDeadInterval：失效时间。如果在此时间内未收到邻居发来的 Hello 报文，则认为邻居失效。如果相邻两台路由器的失效时间不同，则不能建立邻居关系。

DD 报文

两台路由器进行数据库同步时，用 DD 报文来描述自己的 LSDB，内容包括 LSDB 中每一条 LSA 的 Header（LSA 的 Header 可以唯一标识一条 LSA）。LSA Header 只占一条 LSA 的整个数据量的一小部分，这样可以减少路由器之间的协议报文流量，对端路由器根据 LSA Header 就可以判断出是否已有这条 LSA。DD 报文格式如下图所示。



主要字段的解释如下：

Interface MTU：在不分片的情况下，此接口最大可发出的 IP 报文长度。

I（Initial）：当发送连续多个 DD 报文时，如果这是第一个 DD 报文，则置为 1，否则置为 0。

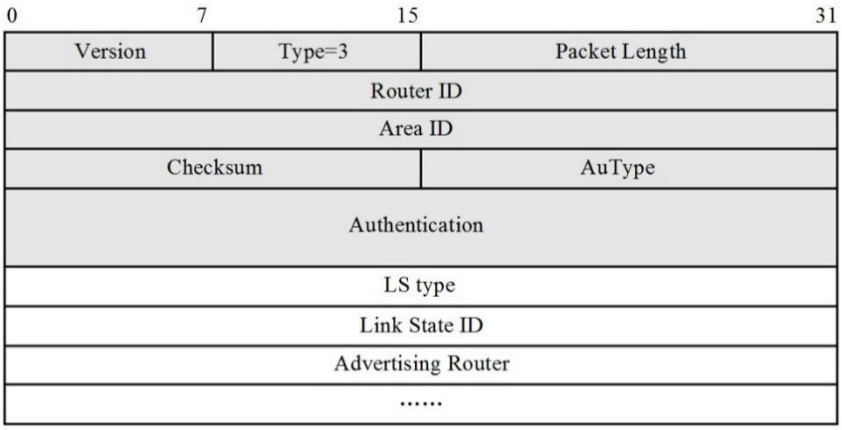
M（More）：当发送连续多个 DD 报文时，如果这是最后一个 DD 报文，则置为 0，否则置为 1；表示后面还有其他的 DD 报文。

MS（Master/Slave）：当两台 OSPF 路由器交换 DD 报文时，首先需要确定双方的主从关系，Router ID 大的一方会成为 Master。当值为 1 时表示发送方为 Master。

DD Sequence Number：DD 报文序列号，由 Master 方规定起始序列号，每发送一个 DD 报文序列号加 1，Slave 方使用 Master 的序列号作为确认。主从双方利用序列号来保证 DD 报文传输的可靠性和完整性。

LSR 报文

两台路由器互相交换过 DD 报文之后，知道对端的路由器有哪些 LSA 是本地的 LSDB 所缺少的，这时需要发送 LSR 报文向对方请求所需的 LSA。内容包括所需要的 LSA 的摘要。LSR 报文格式如下图所示。



主要字段解释如下：

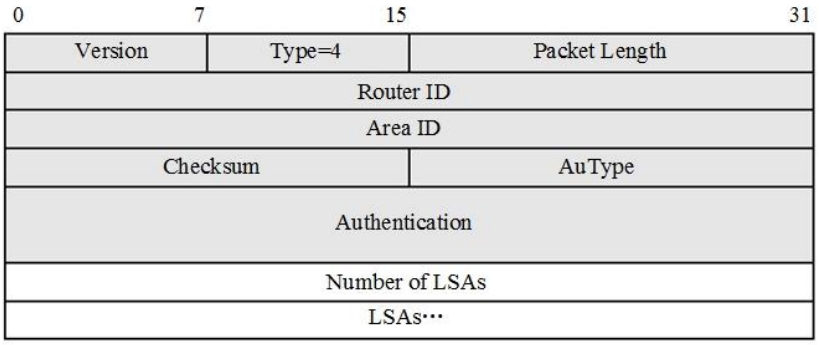
LS type：LSA 的类型号。例如 Type1 表示 Router LSA。

Link State ID：即 LSA 头格式中的字段，根据 LSA 的类型而定。

Advertising Router：产生此 LSA 的路由器的 Router ID。

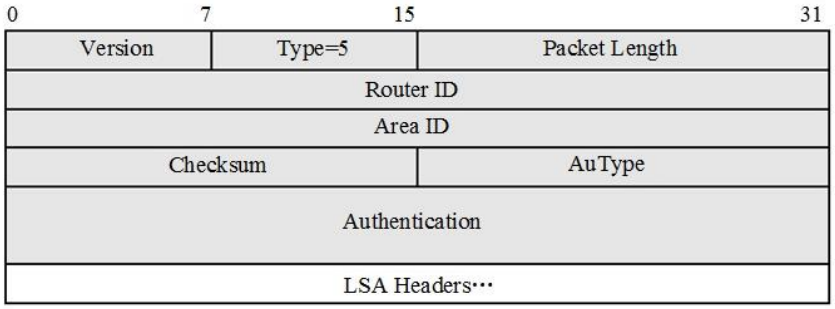
LSU 报文

用来向对端路由器发送所需要的 LSA，内容是多条 LSA（全部内容）的集合。LSU 报文格式如图所示。



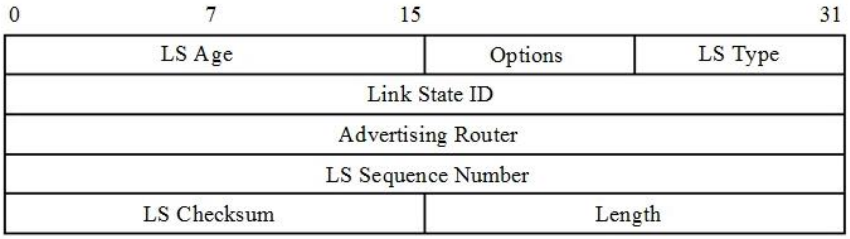
LSAck 报文

用来对接收到的 LSU 报文进行确认。内容是需要确认的 LSA 的 Header（一个 LSAck 报文可对多个 LSA 进行确认）。报文格式如图所示。



LSA 头格式

所有的 LSA 都有相同的报文头，其格式如图所示。



主要字段的解释如下：

LS age：LSA 产生后所经过的时间，以秒为单位。无论 LSA 是在链路上传送，还是保存在 LSDB 中，其值都会在不停的增长。

LS type：LSA 的类型。

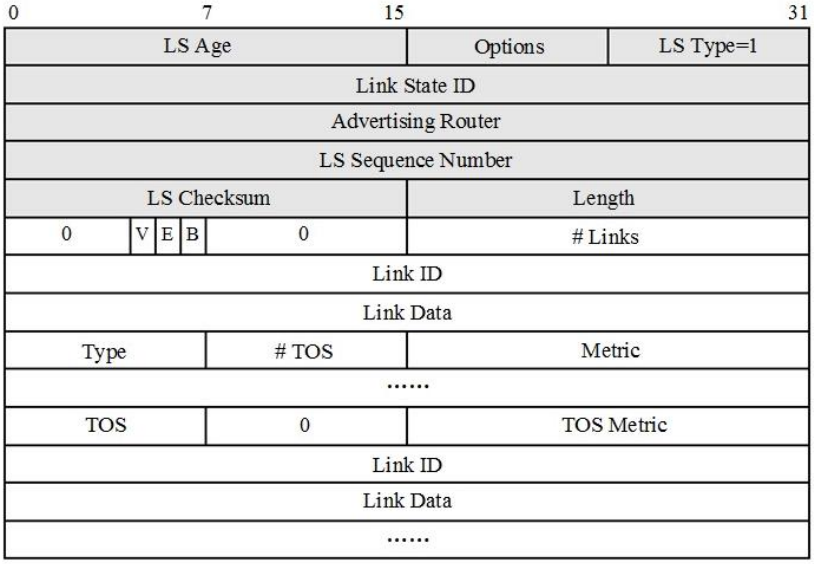
Link State ID：具体数值根据 LSA 的类型而定。

LS sequence number：LSA 的序列号，其他路由器根据这个值可以判断哪个 LSA 是最新的。

length：LSA 的总长度，包括 LSA Header，以字节为单位。

Router LSA

Router LSA 格式如图所示。



主要字段的解释如下：

Link State ID：最初产生此 LSA 的路由器的 Router ID。

V（Virtual Link）：如果产生此 LSA 的路由器是虚连接的端点，则置为 1。

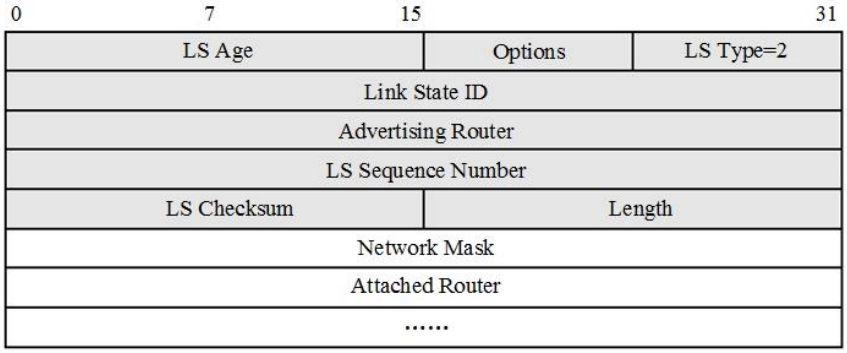
E（External）：如果产生此 LSA 的路由器是 ASBR，则置为 1。

B（Border）：如果产生此 LSA 的路由器是 ABR，则置为 1。

 # links：LSA 中所描述的链路信息的数量，包括路由器上处于某区域中的所有链路和接口。

Network LSA

Network LSA 由广播网或 NBMA 网络中的 DR 发出，LSA 中记录了这一网络上所有路由器的 Router ID。如下图所示。



主要字段的解释如下：

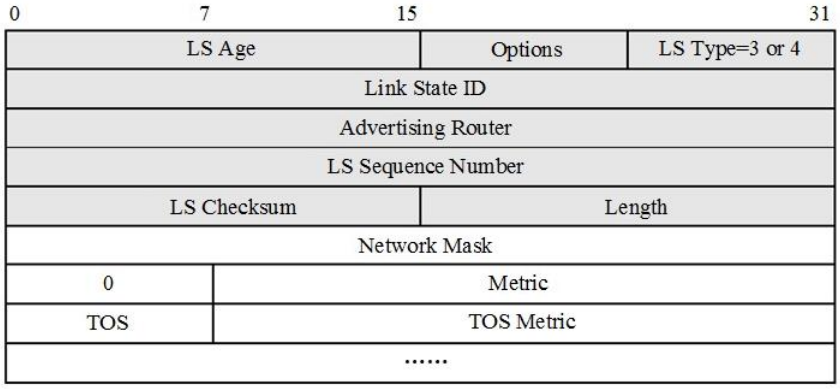
Link State ID：DR 路由器的接口地址。

Network Mask：广播网或 NBMA 网络地址的掩码。

Attached Router：连接在同一个网络上的所有路由器的 Router ID，也包括 DR 的 Router ID。

Summary LSA

Type3 和 Type4 的 LSA 有相同的格式，它们都是由 ABR 产生。如图所示。



主要字段的解释如下：

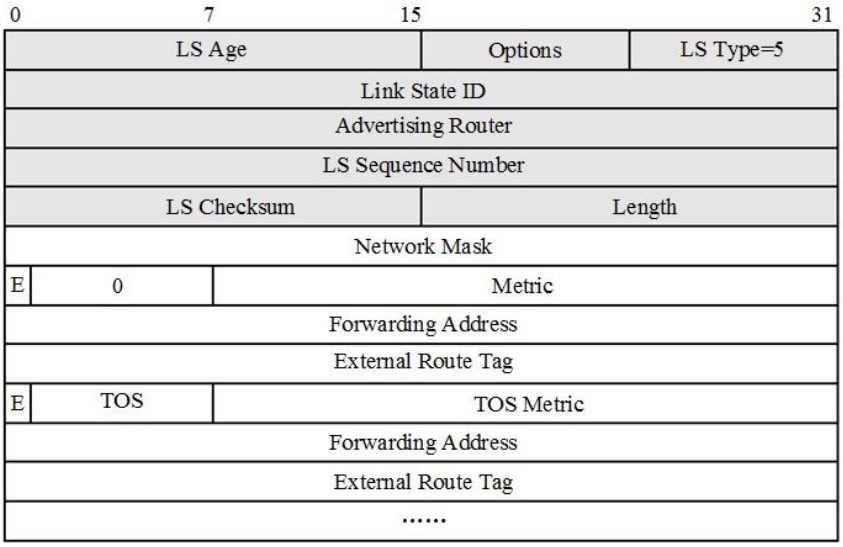
Link State ID：对于 Type3 LSA 来说，它是所通告的网络地址；对于 Type4 来说，它是 ASBR 的 Router ID。

Network Mask：Type3 LSA 的网络地址掩码。对于 Type4 LSA 来说没有意义，设置为 0.0.0.0。

metric：到目的地址的路由开销。

AS-External LSA

由 ASBR 产生，描述到 AS 外部去的路由信息。如图所示。



主要字段的解释如下：

Link State ID：所要通告的其他外部 AS 的目的地址。

Network Mask：所通告的目的地址的掩码。

E（External Metric）：外部度量值的类型。如果是第 2 类外部路由就设置为 1，如果是第 1 类外部路由则设置为 0。

metirc：路由开销。

Forwarding Address：到所通告的目的地址的报文将被转发到这个地址。通常为 0，表明以通告路由器为下一跳。

External Route Tag：添加到外部路由上的标记。OSPF 本身并不使用这个字段，它可以用来对外部路由进行管理。

NSSA External LSA

由 ASBR 产生，且只能在 NSSA 区域内传播。其格式与 AS-External LSA 相同。

4.3.2 OSPF 配置

4.3.2.1 配置全局 OSPF

4.3.2.1.1 使能 OSPF 进程

目的

本节介绍如何启动和关闭 OSPF 进程。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

4.3.2.1.2 复位 OSPF 进程

目的

本节介绍如何复位 OSPF 进程。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

4.3.2.1.3 清除 OSPF 统计信息

目的

本节介绍如何清除 OSPF 统计信息。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

4.3.2.2 配置 OSPF 节点

4.3.2.2.1 配置 Router-id 或路由器 ID

目的

本节介绍如何配置 Router-id 或路由器 ID。

背景信息

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

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

4.3.2.2.2 配置 OSPF 接口

目的

本节介绍如何配置 OSPF 接口。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
配置 OSPF 接口和区域	1. 进入全局配置视图； 2. 进入 OSPFv2 配置视图； 3. 执行命令 **network** *network-address network-mask* **area** *area-id*。
删除 OSPF 接口	1. 进入全局配置视图； 2. 进入 OSPFv2 配置视图； 3. 执行命令 **no network** *network-address network-mask* **area** *area-id*。

4.3.2.2.3 配置 Stub 区域

目的

本节介绍如何配置 Stub 区域。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

目的	步骤
删除 Stub 路由器	1. 进入全局配置视图； 2. 进入 OSPFv2 配置视图； 3. 执行命令 **no stub-router**。

4.3.2.2.4 配置 NSSA 区域

目的

本节介绍如何配置 NSSA 区域。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
配置 NSSA 区域	1. 进入全局配置视图； 2. 进入 OSPFv2 配置视图； 3. 执行命令 **area** *area-id* **nssa**。
配置 NSSA 默认 LSA 开销	1. 进入全局配置视图； 2. 进入 OSPFv2 配置视图； 3. 执行命令 **area** *area-id* **nssa default-cost** { *cost-value* | **default** }。
配置 no summary NSSA 区域	1. 进入全局配置视图； 2. 进入 OSPFv2 配置视图； 3. 执行命令 **area** *area-id* **nssa no-summary**。
配置 NSSA 区域聚合通告/不通告	1. 进入全局配置视图； 2. 进入 OSPFv2 配置视图； 3. 执行命令 **area** *area-id* **nssa range** *dst-network dst-mask* { **advertise** | **not-advertise** }。
配置 NSSA 指定转换路由器或者候选转换路由器	1. 进入全局配置视图； 2. 进入 OSPF v2 配置视图； 3. 执行命令 **area** *area-id* **nssa translator** { **always** | **candidate** }。
删除 NSSA 区域	1. 进入全局配置视图； 2. 进入 OSPF v2 配置视图； 3. 执行命令 **no area** *area-id* **nssa**。
删除 NSSA 区域聚合	1. 进入全局配置视图； 2. 进入 OSPF v2 配置视图； 3. 执行命令 **no area** *area-id* **nssa range** *dst-address/dst-mask*。

4.3.2.2.5 配置区域聚合

目的

本节介绍如何配置区域聚合。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
区域聚合	1. 进入全局配置视图； 2. 进入 OSPF v2 配置视图； 3. 执行命令 **area** *area-id* **range** *dst-address dst-mask* { **advertise** | **not-advertise** }。
删除区域聚合	1. 进入全局配置视图； 2. 进入 OSPF v2 配置视图； 3. 执行命令 **no area** *area-id* **range** *dst-address dst-mask*。

4.3.2.2.6 配置路由协议过滤策略

目的

本节介绍如何配置路由协议过滤策略。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
配置路由协议的过滤策略	1. 进入全局配置视图； 2. 进入 OSPF v2 配置视图； 3. 执行命令 **filter route-policy** *route-policy-name*。
取消路由协议的过滤策略	1. 进入全局配置视图； 2. 进入 OSPF v2 配置视图； 3. 执行命令 **no filter route-policy** *route-policy-name*。

4.3.2.2.7 配置 GR 重启

目的

本节介绍如何配置 GR（Graceful Restart）重启。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
使能 GR	1. 进入全局配置视图； 2. 进入 OSPF v2 配置视图； 3. 执行 **opaque enable** 命令，开启 opaque 支持功能。 4. 执行命令 **graceful-restart**。
配置 GR 周期	1. 进入全局配置视图； 2. 进入 OSPF v2 配置视图； 3. 执行 **opaque enable** 命令，开启 opaque 支持功能。 4. 执行命令 **graceful-restart period** *restart-time*。
使能 GR helper	1. 进入全局配置视图； 2. 进入 OSPF v2 配置视图； 3. 执行命令 **graceful-restart helper**。
去使能 GR 重启	1. 进入全局配置视图； 2. 进入 OSPF v2 配置视图； 3. 执行命令 **no graceful-restart**。
去使能 GR helper	1. 进入全局配置视图； 2. 进入 OSPF v2 配置视图； 3. 执行命令 **no graceful-restart helper**。
执行 GR 重启	1. 进入全局配置视图； 2. 进入 OSPF v2 配置视图； 3. 执行命令 **graceful-restart begin**。

4.3.2.2.8 使能 opaque 功能

目的

本节介绍如何使能 opaque 功能。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

4.3.2.2.9 配置路由计算间隔

目的

本节介绍如何配置路由计算间隔。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

4.3.2.2.10 配置 OSPF TTL

目的

本节介绍如何配置 OSPF TTL。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

4.3.2.2.11 配置 OSPF 重分配

目的

本节介绍如何配置 OSPF 重分配。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
配置 OSPF 重分配	1. 进入全局配置视图； 2. 进入 OSPFv2 配置视图； 3. 执行命令 **redistribute { static | connect | bgp}**。
删除 OSPF 重分配	1. 进入全局配置视图； 2. 进入 OSPFv2 配置视图； 3. 执行命令 **no redistribute { static | connect | bgp** }。

目的	步骤
删除指定网络的重分配	1. 进入全局配置视图； 2. 进入 OSPFv2 配置视图； 3. 执行如下命令： ● **no redistribute { static | connect | bgp }** *dst-address dst-mask* ● **no redistribute { rip | ospf | isis }** *process-id dst-address dst-mask*。
配置重分配路由策略	1. 进入全局配置视图； 2. 进入 OSPFv2 配置视图； 3. 执行命令 **redistribute { static | connect | rip | bgp | isis | ospf } route-policy** *policy-name*。
删除重分配路由策略	1. 进入全局配置视图； 2. 进入 OSPFv2 配置视图； 3. 执行命令 **no redistribute { static |connect | rip | bgp | isis | ospf } route-policy** *policy-name*。
配置重分配开销	1. 进入全局配置视图； 2. 进入 OSPFv2 配置视图； 3. 执行如下命令： ● **redistribute { connect | static | bgp } metric** *router-cost* **type** *cost-type* ● **redistribute { rip | ospf | isis }** *process-id* **metric** *router-cost* **type** *cost-type*。
配置重分配指定网络的开销	1. 进入全局配置视图； 2. 进入 OSPFv2 配置视图； 3. 执行如下命令： ● **redistribute** { **connect** | **static** | **bgp** } *dst-network network-mask* **metric** *router-cost* **type** *cost-type* ● **redistribute** { **rip** | **ospf** | **isis** } *process-id dst-network network-mask* **metric** *router-cost* **type** *cost-type*。
配置重分配的 translate 位	1. 进入全局配置视图； 2. 进入 OSPFv2 配置视图； 3. 执行如下命令： ● **redistribute { connect | static | bgp }** *dst-network network-mask* { **translate | no-translate** } ● **redistribute { connect | static | bgp }** { **translate | no-translate** } ● **redistribute { rip | ospf | isis }** *process-id dst-network network-mask* { **translate | no-translate** }。
配置拒绝特定的外部路由	1. 进入全局配置视图； 2. 进入 OSPFv2 配置视图； 3. 执行如下命令： ● **redistribute { connect | static | bgp }** *dst-network network-mask* { **not-advertise | advertise** }

目的	步骤
	● **redistribute { rip | ospf | isis }** *process-id dst-network network-mask* { **not-advertise | advertise** }。
配置重分配路由	1. 进入全局配置视图； 2. 进入 OSPFv2 配置视图； 3. 执行命令 **redistribute { rip | isis | ospf }** *process-id*。
取消重分配路由	1. 进入全局配置视图； 2. 进入 OSPFv2 配置视图； 3. 执行命令 **no redistribute { rip | isis | ospf }** *process-id*。
配置重分配聚合路由条目	1. 进入全局配置视图； 2. 进入 OSPFv2 配置视图； 3. 执行命令 **redistribute { static | connect | rip | bgp | isis | ospf } range** *range-address/M*。
删除重分配聚合路由条目	1. 进入全局配置视图； 2. 进入 OSPFv2 配置视图； 3. 执行命令 **no redistribute { static |connect | rip | bgp | isis | ospf } range** *range-address/M*。

4.3.2.2.12 使能 OSPF 上报 trap

目的

本节介绍如何使能 OSPF 上报 trap。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

目的	步骤
	ospfvirtifrxbadpacket | ospfvirtifstatechange | ospfvirtiftxretransmit | ospfvirtnbrrestarthelperstatuschange | ospfvirtnbrstatechange }。

4.3.2.2.13 配置 OSPF 开销参考带宽

目的

本节介绍如何配置 OSPF 开销参考带宽。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

4.3.2.2.14 配置兼容 RFC1583

目的

本节介绍如何配置兼容 RFC1583。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

4.3.2.2.15 配置缺省路由通告

目的

本节介绍如何配置缺省路由通告。

过程

根据不同目的，执行相应步骤，具体参见下表。

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

4.3.2.3 配置 OSPF 端口

4.3.2.3.1 配置 OSPF 接口参数

目的

本节介绍如何配置 OSPF 接口参数。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
配置 OSPF 接口类型	1. 进入全局配置视图； 2. 进入 VLANIF 配置视图、Loopback 接口配置视图； 3. 执行命令 **ip ospf if-type { broadcast | p2p | nbma | p2multip }**。
配置 OSPF 接口优先级	1. 进入全局配置视图； 2. 进入 VLANIF 配置视图； 3. 执行命令 **ip ospf priority** { *priority* | **default** }。
配置 OSPF 接口开销	1. 进入全局配置视图； 2. 进入 VLANIF 配置视图、Loopback 接口配置视图； 3. 执行命令 **ip ospf cost** { *cost* | **default** }。
配置 OSPF 接口 Hello 间隔时间	1. 进入全局配置视图； 2. 进入 VLANIF 配置视图、Loopback 接口配置视图； 3. 执行如下命令： ● **ip ospf hello-interval** *hello-interval* ● **ip ospf hello-interval default**。
配置 OSPF 接口的 wait 定时器的间隔时间	1. 进入全局配置视图； 2. 进入 VLANIF 配置视图； 3. 执行命令 **ip ospf wait-interval** { *wait-interval* | **default** }。
配置 OSPF 接口邻居超时时间	1. 进入全局配置视图； 2. 进入 VLANIF 配置视图、Loopback 接口配置视图； 3. 执行如下命令：

目的	步骤
	● **ip ospf dead-interval** *interval* ● **ip ospf dead-interval default**。
配置 OSPF 接口重传间隔	1. 进入全局配置视图； 2. 进入 VLANIF 配置视图、Loopback 接口配置视图； 3. 执行命令 **ip ospf retransmit-interval** { *retransmit-interval-time* | **default** }。
配置 OSPF 接口传输时延	1. 进入全局配置视图； 2. 进入 VLANIF 配置视图、Loopback 接口配置视图； 3. 执行命令 **ip ospf transmit-delay** { *transmit-delay-time* | **default** }。
配置发送轮询报文的时间间隔	1. 进入全局配置视图； 2. 进入 VLANIF 配置视图、Loopback 接口配置视图； 3. 执行命令 **ip ospf poll-interval** { *poll-interval-time* | **default** }。
配置接口简单密码认证	1. 进入全局配置视图； 2. 进入 VLANIF 配置视图、Loopback 接口配置视图； 3. 执行命令 **ip ospf authentication simple-password** *key-value*。
配置接口 MD5 认证	1. 进入全局配置视图； 2. 进入 VLANIF 配置视图、Loopback 接口配置视图； 3. 执行命令 **ip ospf authentication md5** *key-id md5-key*。
清除接口认证	1. 进入全局配置视图； 2. 进入 VLANIF 配置视图、Loopback 接口配置视图； 3. 执行命令 **no ip ospf authentication**。
指定从 IPv4 地址为源 IPv4 地址	1. 进入 VLANIF 配置视图、以太网子接口配置视图、Trunk 子接口配置视图、Loopback 接口配置视图、bd 接口配置视图、以太网路由接口配置视图、grp 路由接口配置视图； 2. 执行命令 **ip ospf source sub-address** *ipv4-address*。
删除指定从 IPv4 地址为源 IPv4 地址	1. 进入 VLANIF 配置视图、以太网子接口配置视图、Trunk 子接口配置视图、Loopback 接口配置视图、bd 接口配置视图、以太网路由接口配置视图、grp 路由接口配置视图； 2. 执行命令 **no ip ospf source sub-address**。

4.3.2.3.2 配置 BFD

目的

本节介绍如何配置 BFD。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
配置 BFD	1. 进入全局配置视图； 2. 进入 VLANIF 配置视图、Loopback 接口配置视图； 3. 执行命令 **ip ospf bfd { enable | disable }**。

4.3.2.3.3 配置 OSPF 接口 MTU

目的

本节介绍如何配置 OSPF 接口 MTU。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

4.3.2.3.4 配置 passive 接口

目的

本节介绍如何配置 passive 接口。

背景信息

被动接口是指不收发协议消息的 OSPF 接口，在此接口上不建立任何邻居，但是接口路由将包含在 RouterLSA 中作为内部路由传播。可用于 Stub 路由。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

4.3.2.4 维护及调试

目的

当 OSPF 相关功能不正常，需要进行查看、定位或调试问题时，可以使用本小节操作。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
显示 OSPF 简要信息	1. 进入普通用户视图、特权用户视图、全局配置视图、OSPFv2 路由配置视图、VLANIF 配置视图、Loopback 接口配置视图； 2. 执行如下命令： ● **show ip ospf brief** ● **show ip ospf brief process** *process*。
显示 OSPF 配置信息	1. 进入普通用户视图、特权用户视图、全局配置视图、OSPFv2 路由配置视图、VLANIF 配置视图、Loopback 接口配置视图； 2. 执行命令 **show ip ospf config**。
显示 OSPF 接口信息	1. 进入普通用户视图、特权用户视图、全局配置视图、OSPFv2 路由配置视图、VLANIF 配置视图、Loopback 接口配置视图； 2. 执行如下命令： ● **show ip ospf interface** ● **show ip ospf interface error** ● **show ip ospf interface** *ip-address* ● **show ip ospf interface count** ● **show ip ospf interface process** *process*。
显示 OSPF 邻居信息	1. 进入普通用户视图、特权用户视图、全局配置视图、OSPFv2 路由配置视图、VLANIF 配置视图、Loopback 接口配置视图； 2. 执行如下命令： ● **show ip ospf neighbor** ● **show ip ospf neighbor** *ip-address* ● **show ip ospf neighbor process** *process* ● **show ip ospf neighbor state statistic** ● **show ip ospf neighbor state count**。
显示 OSPF 区域信息	1. 进入普通用户视图、特权用户视图、全局配置视图、OSPFv2 路由配置视图、VLANIF 配置视图、Loopback 接口配置视图； 2. 执行如下命令： ● **show ip ospf area** ● **show ip ospf area** *area-id* ● **show ip ospf area process** *process*。

目的	步骤
显示 OSPF 数据库信息	1. 进入普通用户视图、特权用户视图、全局配置视图、OSPFv2 路由配置视图、VLANIF 配置视图、Loopback 接口配置视图； 2. 执行如下命令： ● **show ip ospf database** ● **show ip ospf database area** *area-id* ● **show ip ospf database area** *area-id* **process** *process* ● **show ip ospf database { as-external-lsa | type9 | type11 }** *Ls-id adverrouter-id* ● **show ip ospf database { as-external-lsa | type9 | type11 }** *Ls-id adverrouter-id process* ● **show ip ospf database { router | network | summary-network | summary-asbr | as-external-lsa | nssa-lsa | type9 | type10 | type11 }** ● **show ip ospf database { router | network | summary-network | summary-asbr | as-external-lsa | nssa-lsa | type9 | type10 | type11 } process** *process* ● **show ip ospf database { router | network | summary-network | summary-asbr | nssa-lsa | type10 }** *LS-id adverrouter-id area-id* ● **show ip ospf database { router | network | summary-network | summary-asbr | nssa-lsa | type10 }** *LS-id adverrouter-id area-id process* ● **show ip ospf database age** *min-age max-age* ● **show ip ospf database age** *min-age max-age* **count** ● **show ip ospf database count** ● **show ip ospf database count process** *process* ● **show ip ospf database expire** ● **show ip ospf database expire count** ● **show ip ospf database expire process** *process* ● **show ip ospf database process** *process* ● **show ip ospf database total count**。
显示 OSPF 路由信息	1. 进入普通用户视图、特权用户视图、全局配置视图、OSPFv2 路由配置视图、VLANIF 配置视图、Loopback 接口配置视图； 2. 执行如下命令： ● **show ip ospf route** ● **show ip ospf route count** ● **show ip ospf route count process** *process* ● **show ip ospf route process** *process* ● **show ip ospf route total count**。
显示 OSPF BFD 信息	1. 进入普通用户视图、特权用户视图、全局配置视图、OSPFv2 路由配置视图、VLANIF 配置视图、Loopback 接口配置视图； 2. 执行命令 **show ip ospf bfd session**。

目的	步骤
显示 OSPF trap 信息	1. 进入特权用户视图、全局配置视图、普通用户视图、OSPFv2 路由配置视图、VLANIF 配置视图、Loopbck 接口配置视图； 2. 执行命令 **show ip ospf trap**。
显示 OSPFv2 的错误信息	1. 进入特权用户视图、全局配置视图、普通用户视图、OSPFv2 路由配置视图、VLANIF 配置视图、Loopbck 接口配置视图； 2. 执行命令 **show ip ospf error**。
导出 OSPFv2 模块记录的数据库信息或所有表项信息	1. 进入普通用户视图； 2. 执行命令 **dump ha ospfv2** { **database** | **diag-all** }导出 OSPFv2 模块记录的数据库信息或所有表项信息，用来判断设备两块主控卡上表项是否一致。

4.3.3 OSPF 配置举例

4.3.3.1 配置 OSPF 基本功能

组网要求

如图 4-4 所示，所有的设备都运行 OSPF，并将整个自治系统划分为 3 个区域，其中 CN12800_1 和 CN12800_2 为 ABR 来转发区域之间的路由。

配置完成后，每台 router 都应学到自治系统内的到所有网段的路由。

组网图

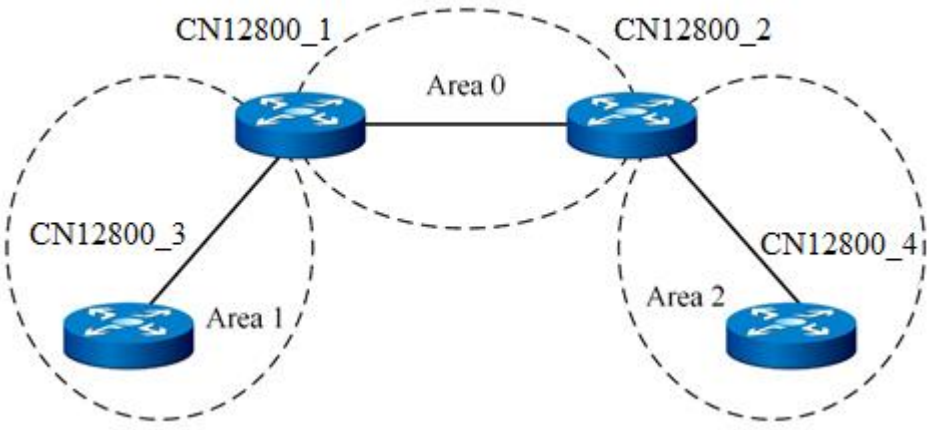


图 4-4 OSPF 基本配置组网图

配置数据

CN12800_1 的两个接口地址：1.1.1.1/24 和 3.1.1.1/24

CN12800_2 的两个接口地址：1.1.1.2/24 和 4.1.1.2/24

CN12800_3 的接口地址：3.1.1.3/24

CN12800_4 的接口地址：4.1.1.4/24

配置步骤

CN12800_1:

CN12800_1(config)#router ospf

CN12800_1(config-ospf-1)#router-id 1.1.1.1

CN12800_1(config-ospf-1)#network 1.1.1.0 255.255.255.0 area 0

CN12800_1(config-ospf-1)#network 3.1.1.0 255.255.255.0 area 1

CN12800_1(config)#

CN12800_2:

CN12800_2(config)#router ospf

CN12800_2(config-ospf-1)#router-id 1.1.1.2

CN12800_2(config-ospf-1)#network 1.1.1.0 255.255.255.0 area 0

CN12800_2(config-ospf-1)#network 4.1.1.0 255.255.255.0 area 2

CN12800_2(config)#

CN12800_3:

CN12800_3(config)#router ospf

CN12800_3(config-ospf-1)#router-id 3.1.1.3

CN12800_3(config-ospf-1)#network 3.1.1.0 255.255.255.0 area 1

CN12800_3(config)#

CN12800_4:

CN12800_4(config)#router ospf

CN12800_4(config-ospf-1)#router-id 4.1.1.4

CN12800_4(config-ospf-1)#network 4.1.1.0 255.255.255.0 area 2

CN12800_4(config)#

验证配置结果

使用 show ip ospf neighbor 命令可看到 OSPF 的信息如下:

OSPF Process 1

IpAddress	NeighborID	Option	Priority	State	Event	Aging
1.1.1.2	1.1.1.2	2	1	full	6	39
3.1.1.3	3.1.1.3	2	1	full	6	30

使用 show ip ospf database 命令可看到 OSPF 的信息如下:

Database of OSPF Process 1

Router LSA (area 0)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
1.1.1.1	1.1.1.1	146	0x80000003	0xdbff	36
1.1.1.2	1.1.1.2	147	0x80000003	0xd9fe	36

Network LSA (area 0)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
1.1.1.2	1.1.1.2	147	0x80000001	0x83c3	32

SummaryNetwork LSA (area 0)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
3.1.1.0	1.1.1.1	146	0x80000002	0xf8f5	28
4.1.1.0	1.1.1.2	138	0x80000001	0xe706	28

Router LSA (area 1)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
1.1.1.1	1.1.1.1	147	0x80000002	0xccb	36
3.1.1.3	3.1.1.3	139	0x80000004	0xd66c	48

Network LSA (area 1)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
3.1.1.3	3.1.1.3	147	0x80000001	0x5fde	32

SummaryNetwork LSA (area 1)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
1.1.1.0	1.1.1.1	187	0x80000001	0x15dc	28
4.1.1.0	1.1.1.1	136	0x80000002	0xd7b1	28

使用 show ip ospf route 命令可看到 OSPF 的信息如下:

OSPF Instance 1

Dest	Mask	Nexthop	Type	PathType	Areaid
1.1.1.2	255.255.255.255	1.1.1.2	ABR	INTRA	0
1.1.1.0	255.255.255.0	1.1.1.1	Network	INTRA	
3.1.1.0	255.255.255.0	3.1.1.1	Network	INTRA	
4.1.1.0	255.255.255.0	1.1.1.2	Network	INTER	

4.3.3.2 配置 OSPF 的 Stub 区域

组网要求

如图 4-5 所示，所有的设备都运行 OSPF，并将整个自治系统划分为 3 个区域，其中 CN12800_1 和 CN12800_2 为 ABR 来转发区域之间的路由。

配置完成后，每台设备都应学到自治系统内的到所有网段的路由。

组网图

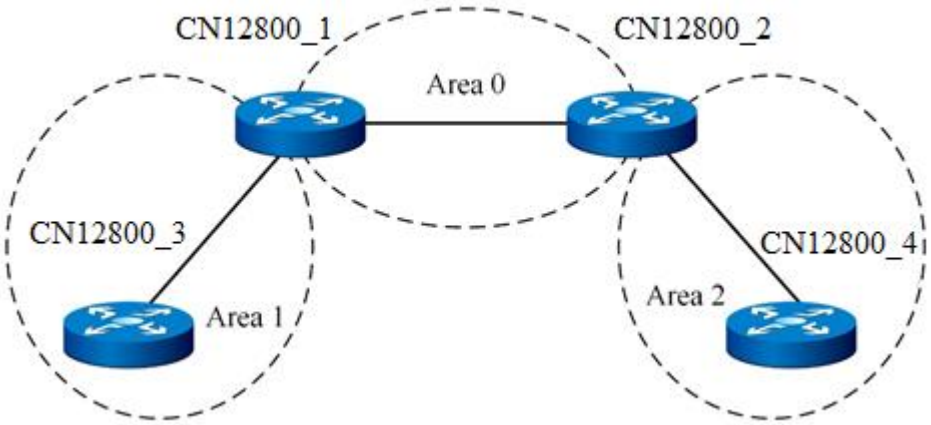


图 4-5 OSPF Stub 区域组网图

配置步骤

基本配置和拓扑同 4.3.3.1 配置 OSPF 基本功能。

配置 area 1 为 stub：

CN12800_1:

CN12800_1(config)#router ospf

CN12800_1(config-ospf-1)#area 1 stub

CN12800_1(config)#

CN12800_3:

CN12800_3(config)#router ospf

CN12800_3(config-ospf-1)# area 1 stub

CN12800_3(config)#

在 CN12800_4 引入 100.1.1.1 的 5 类 LSA

验证配置结果

1. 当 CN12800_3 所在区域为普通区域时，可以看到路由表中存在 AS 外部的路由。变成 stub 区域后，比正常区域多一个缺省的 3 类 LSA，看不到 AS 外部的 LSA。

CN12800_3# show ip ospf route

OSPF Instance 0

Dest	Mask	Nexthop	Type	PathType	Areaid
1.1.1.1	255.255.255.255	3.1.1.1	ABR	INTRA	1
1.1.1.0	255.255.255.0	3.1.1.1	Network	INTER	
3.1.1.0	255.255.255.0	3.1.1.3	Network	INTRA	
4.1.1.0	255.255.255.0	3.1.1.1	Network	INTER	
100.1.1.0	255.255.255.0	1.1.1.2	Network	ASE	

2. 当 CN12800_3 所在区域配置为 Stub 区域时，已经看不到 AS 外部的路由，取而代之的是一条通往区域外部的缺省路由。

CN12800_3# show ip ospf route

OSPF Instance 0

Dest	Mask	Nexthop	Type	PathType	Areaid
1.1.1.1	255.255.255.255	3.1.1.1	ABR	INTRA	1
0.0.0.0	0.0.0.0	3.1.1.1	Network	INTER	
1.1.1.0	255.255.255.0	3.1.1.1	Network	INTER	
3.1.1.0	255.255.255.0	3.1.1.3	Network	INTRA	
4.1.1.0	255.255.255.0	3.1.1.1	Network	INTER	

4.3.3.3 配置 OSPF 的 NSSA 区域

组网要求

如图 4-6 所示，所有的设备都运行 OSPF，并将整个自治系统划分为 3 个区域，其中 CN12800_1 和 CN12800_2 为 ABR 来转发区域之间的路由。

配置完成后，每台设备都应学到自治系统内的到所有网段的路由。

组网图

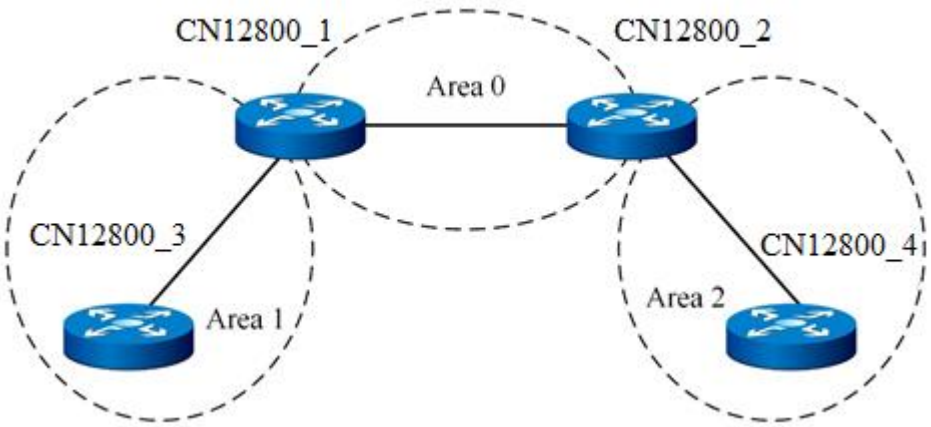


图 4-6 OSPF nssa 区域组网图

配置步骤

基本配置和拓扑同 4.3.3.1 配置 OSPF 基本功能。

配置 area 1 为 nssa：

CN12800_1:

CN12800_1(config)#router ospf

CN12800_1(config-ospf-1)#area 1 nssa

CN12800_1(config)#

CN12800_3:

CN12800_3(config)#router ospf

CN12800_3(config-ospf-1)# area 1 nssa

CN12800_3(config)#

验证配置结果

1. nssa 区域的数据库比正常区域的数据库多一个缺省 NSSA 类型 LSA

CN12800_3(config-ospf-1)#show ip ospf database

Database of OSPF Process 1

Router LSA (area 1)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
1.1.1.1	1.1.1.1	134	0x80000002	0x9934	36
3.1.1.3	3.1.1.3	133	0x80000002	0x6066	36

Network LSA (area 1)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
3.1.1.3	3.1.1.3	133	0x80000001	0xe64f	32

SummaryNetwork LSA (area 1)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
1.1.1.0	1.1.1.1	178	0x80000001	0x9c4d	28
4.1.1.0	1.1.1.1	178	0x80000001	0x6121	28

NSSA LSA (area 1)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
0.0.0.0	1.1.1.1	178	0x80000001	0xc608	36

2. 在 CN12800_3 引入 100.1.1.1 的静态路由 ip route-static 100.1.1.0 255.255.255.0 3.1.1.1，重分配静态路由，

数据库：

NSSA LSA (area 1)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
0.0.0.0	1.1.1.1	374	0x80000001	0x7550	36
100.1.1.0	3.1.1.3	0	0x80000001	0x70c4	36

ASExternal LSA

LinkId	ADV Router	Age	Seq#	CheckSum	Len
100.1.1.0	3.1.1.3	1	0x80000001	0xe656	36

路由：

CN12800_3# show ip ospf route

OSPF Instance 0

Dest	Mask	Nexthop	Type	PathType	Areaid
1.1.1.1	255.255.255.255	3.1.1.1	ABR	INTRA	1
1.1.1.1	255.255.255.255	3.1.1.1	ASBR	INTRA	1
0.0.0.0	0.0.0.0	3.1.1.1	Network	ASE2	
1.1.1.0	255.255.255.0	3.1.1.1	Network	INTER	
3.1.1.0	255.255.255.0	3.1.1.3	Network	INTRA	
4.1.1.0	255.255.255.0	3.1.1.1	Network	INTER	

在 CN12800_4 上查看

数据库：

CN12800_4#

ASExternal LSA

LinkId	ADV Router	Age	Seq#	CheckSum	Len
100.1.1.0	1.1.1.1	412	0x80000001	0x4701	36

路由：

CN12800_4# show ip ospf route

OSPF Instance 0

Dest	Mask	Nexthop	Type	PathType	Areaid
1.1.1.2	255.255.255.255	4.1.1.2	ABR	INTRA	2
1.1.1.0	255.255.255.0	4.1.1.2	Network	INTER	
3.1.1.0	255.255.255.0	4.1.1.2	Network	INTER	
4.1.1.0	255.255.255.0	4.1.1.4	Network	INTRA	
100.1.1.0	255.255.255.0	4.1.1.2	Network	ASE	

3. 在 CN12800_4 引入 200.1.1.1 的静态路由，查看 CN12800_3 是否拥有外部路由

在 CN12800_4 查看数据库

ASExternal LSA

LinkId	ADV Router	Age	Seq#	CheckSum	Len
100.1.1.0	1.1.1.1	823	0x80000001	0x4701	36
200.1.1.0	4.1.1.4	4	0x80000001	0xb933	36

在 CN12800_3 查看数据库

CN12800_3

ASExternal LSA

LinkId	ADV Router	Age	Seq#	CheckSum	Len
100.1.1.0	3.1.1.3	836	0x80000001	0xe656	36

没有 200.1.1.0 的外部路由

4.3.3.4 配置重分配

组网要求

如图 4-7 所示，2 个设备都运行 OSPF，并将所有都配置为区域 0。假定 CN12800_1 需要向 OSPF 导入外部路由，但是对外部路由有如下要求：

1 接受所有直连路由，并采用默认配置；

2 接收所有静态路由，并为路由配置开销 2000，类型 2；10.1.1.0/24 的静态路由开销为 100；

3 拒绝 20.1.1.0/24 的 RIP 路由，并对属于 30.1.0.0/16 的 RIP 路由进行聚合；

配置完成后，每台设备都应学到自治系统内的到所有网段的路由。

组网图

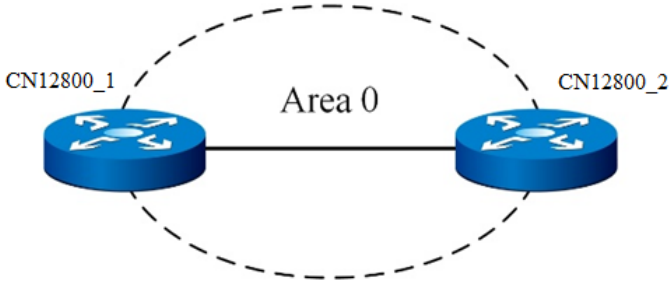


图 4-7 OSPF 重分配组网图

配置步骤

1. 基本配置

CN12800_1:

CN12800_1(config)#router ospf

CN12800_1(config-ospf-1)#router-id 1.1.1.1

CN12800_1(config-ospf-1)#network 1.1.1.0 255.255.255.0 area 0

CN12800_1(config-ospf-1)#network 3.1.1.0 255.255.255.0 area 1

CN12800_1(config)#

CN12800_2:

CN12800_2(config)#router ospf

CN12800_2(config-ospf-1)#router-id 1.1.1.2

CN12800_2(config-ospf-1)#network 1.1.1.0 255.255.255.0 area 0

CN12800_2(config-ospf-1)#network 4.1.1.0 255.255.255.0 area 2

CN12800_2(config)#

2. 重分配配置

CN12800_2(config-ospf-1)#redistribute connected

CN12800_2(config-ospf-1)#redistribute static metric 2000 type 2

CN12800_2(config-ospf-1)#redistribute static 10.1.1.0 255.255.255.0 metric 100 type 2

CN12800_2(config-ospf-1)#redistribute static

CN12800_2(config-ospf-1)#redistribute rip 20.1.1.0 255.255.255.0 not-advertise

CN12800_2(config-ospf-1)#redistribute rip

验证配置结果

执行上述配置后，可以观察 A 的数据库，检查导入的外部 LSA 是否满足要求。

4.3.3.5 配置聚合

组网要求

如图 4-8，网络要求：

- 区域 1 中存在 10.1.1.0/24、10.1.2.0/24、20.1.1.0/24、20.1.2.0/24 的区域内路由，希望将 10.1.1.0/24 和 10.1.2.0/24 聚合为 10.1.0.0/16 通告，而 20.1.1.0/24 和 20.1.2.0/24 不导入其他区域。
- 区域 2 的设备能力较差，不能接受大量外部路由，但是具有 30.1.1.0/24 的外部路由，希望将此路由通告给其他区域。
- 区域 3 与区域 2 相似，但是没有需要通告的外部路由

根据上述要求，我们可以为区域 1 配置聚合条目和过滤条目，为区域 2 配置 NSSA 属性，为区域 3 配置 Stub 属性。

组网图

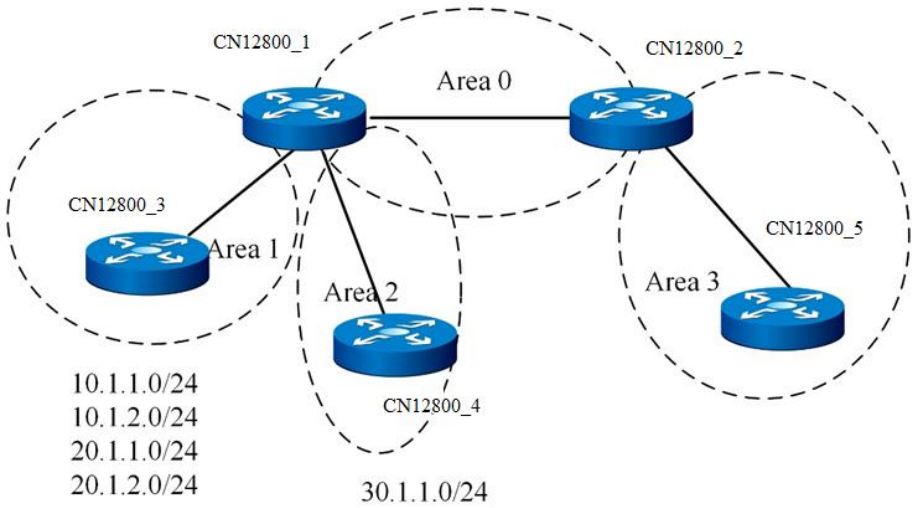


图 4-8 OSPF 聚合组网图

配置步骤

OSPF 基本配置见 4.3.3.1 配置 OSPF 基本功能节。

CN12800_1：

CN12800_1(config-ospf-1)#area 1 range 10.1.0.0 255.255.0.0 advertise

CN12800_1(config-ospf-1)#area 1 range 20.1.0.0 255.255.0.0 no-advertise

CN12800_1(config-ospf-1)#area 2 nssa

#区域 2 的路由器均需要此配置

CN12800_2：

CN12800_2(config-ospf-1)#area 3 stub

或

CN12800_2(config-ospf-1)#area 3 stub no-summary

验证配置结果

以上配置完成后，可检查数据库来判断：

1 区域 0 中包含 10.1.0.0/16 的 SummaryLSA

2 区域 0 中不包含 10.1.1.0、10.1.2.0、20.1.1.0、20.1.2.0 的 SummaryLSA

3 区域 0 中包含 30.1.1.0/16 的 5 类 LSA

4 区域 2 中包含 30.1.1.0/16 的 7 类 LSA

5 区域 2 中包含 0.0.0.0/0 的 LSA

6 区域 3 中包含 0.0.0.0/0 的 Summary LSA

7 如果区域 3 不指定 nosummary，则区域 3 中包含 10.1.0.0/16 的 SummaryLSA，否则不包含。

4.3.3.6 配置认证模式

组网要求

如图 4-9，配置要求：

1 CN12800_1 与 CN12800_2 间采用简单密码认证，密码为 test

2 CN12800_1 与 CN12800_4 建立虚链路，采用 MD5 认证，密码为 aaa，ID 为 100

3 CN12800_2 与 CN12800_3 采用 MD5 认证，密码为 ccc，ID 为 110

组网图

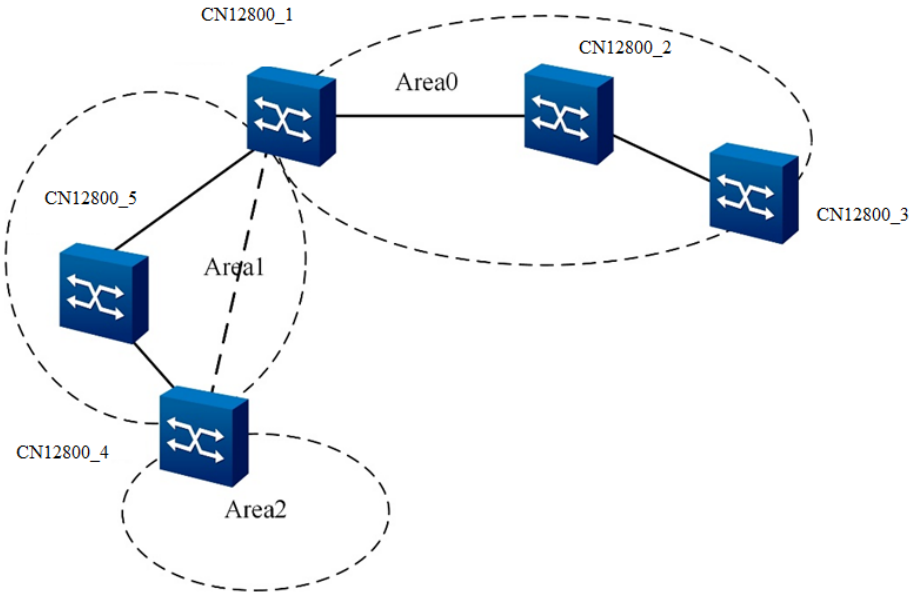


图 4-9 OSPF 认证模式组网图

配置步骤

OSPF 基本配置见 4.3.3.1 配置 OSPF 基本功能节。

CN12800_1：

CN12800_1(config)#interface vlan 1

CN12800_1(config-vlan-1)#ip ospf authentication simple-password test

CN12800_1(config-vlan-1)#exit

CN12800_1(config)#router ospf

CN12800_1(config-ospf-1)#area 1 virtual-link 1.1.1.2 authentication md5 aaa 100

CN12800_2：

CN12800_2(config)#interface vlan 1

CN12800_2(config-vlan-1)#ip ospf authentication simple-password test

CN12800_2(config-vlan-1)#exit

CN12800_2(config)#interface vlan 2

CN12800_2(config-vlan-1)#ip ospf authentication md5 110 ccc

CN12800_2(config-vlan-1)#exit

CN12800_3：

CN12800_3(config-vlan-1)#router ospf

CN12800_3(config-ospf-1)#area 0 authentication md5 110 ccc

CN12800_4：

CN12800_4(config)#router ospf

CN12800_4(config-ospf-1)#area 1 virtual-link 1.1.1.1 authentication md5 aaa 100

验证配置结果

配置之后，检查邻居关系正常。

4.3.3.7 配置 BFD

组网要求

如图 4-10 所示，2 个设备都运行 OSPF，并将所有都配置为区域 0。

组网图

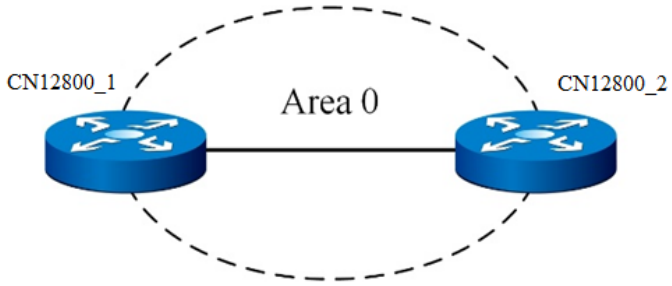


图 4-10 OSPF BFD 组网图

配置步骤

1. OSPF 基本配置见 4.3.3.1 配置 OSPF 基本功能节。
2. BFD 配置

CN12800_1：

CN12800_1(config)#interface vlan 4

CN12800_1(config-vlan-4)#bfd enable

CN12800_1(config-vlan-4)#ip ospf bfd enable

CN12800_2：

CN12800_2(config)#interface vlan 4

CN12800_2(config-vlan-4)#bfd enable

CN12800_2(config-vlan-4)#ip ospf bfd enable

验证配置结果

CN12800_1(config-vlan-4)#show ip ospf bfd session

OSPF Process 1

NeighborAddress	NeighborID	BFDState
1.1.1.2	1.1.1.2	UP

CN12800_2(config-vlan-4)#show ip ospf bfd session

OSPF Process 1

NeighborAddress	NeighborID	BFDState
1.1.1.1	1.1.1.1	UP

4.3.3.8 配置 GR

组网要求

如图 4-11 所示，2 个设备都运行 OSPF，并将两个都配置为区域 0。

测试 GR 重启需要 2 台设备，一台为 GR 重启者，一台为 GR 帮助者。GR 测试重启者采用双主控，拔插卡的方式测试。帮助者无限制。

组网图

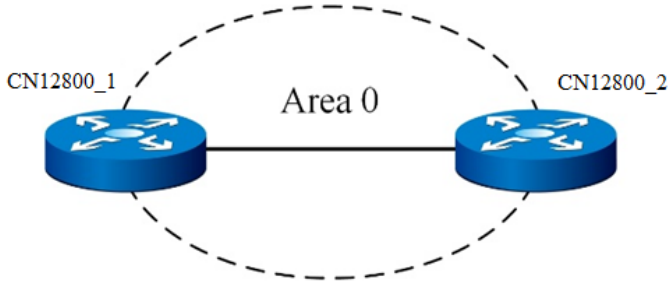


图 4-11 OSPF GR 组网图

配置步骤

1. OSPF 基本配置见 4.3.3.1 配置 OSPF 基本功能。

2. GR 配置

CN12800_1:

CN12800_1(config)#router ospf

CN12800_1(config-ospf-1)# graceful-restart

CN12800_1(config-ospf-1)# graceful-restart period 60

CN12800_2:

CN12800_2(config)#router ospf

CN12800_2(config-ospf-1)# graceful-restart helper

验证配置结果

采用插拔卡进行测试，GR 重启者和 GR 帮助者上的配置以后，将 GR 重启者的主用主控拔掉，这时设备间原有的流量应不发生中断。

4.4 OSPFv3 配置

4.4.1 OSPFv3 简介

4.4.1.1 OSPFv3 基本概念

OSPFv3 协议在一个自治系统内部运行。为了减小路由信息的数量，在 OSPFv3 中，将一个 AS 划分为不同的区域（Area），每一个区域由一个区域 ID（Area-ID）进行标识，在这里，我们规定区域 ID 采用 IPv4 地址格式。图 4-12 给出了一个区域划分的例子。

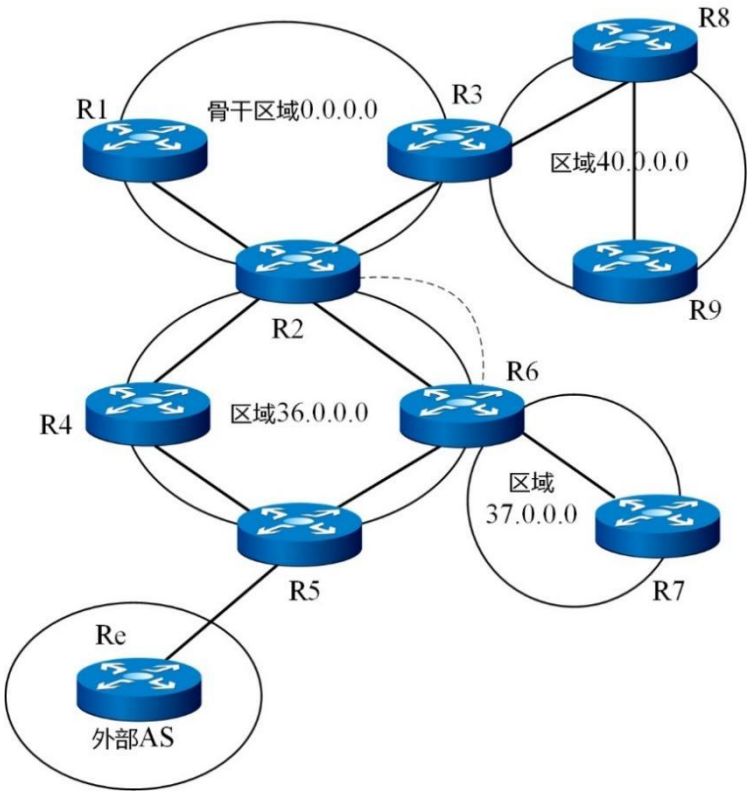


图 4-12 OSPFv3 区域划分

在图 4-12 中，一个 AS 被划分为 4 个区域，R1，R2 和 R3 的部分接口属于骨干区域 0.0.0.0，R2，R4，R5，R6 的部分接口属于区域 36.0.0.0，R6 和 R7 部分接口属于区域 37.0.0.0，而 R3，R8 和 R9 则组成了区域 40.0.0.0。

在 OSPFv3 中，区域 0.0.0.0（即区域 ID 为 0.0.0.0 的区域，以下同）是一个很特殊的区域，被称为骨干区域（Backbone Area）。为了 OSPFv3 协议正常工作，骨干区域必须是连续的，一旦骨干区域被隔离（如骨干区域中的某些链路故障导致不连续），则路由计算不能正常进行。其他的区域必须和骨干区域相连。如图 4-12 中的区域 36.0.0.0 和区域 40.0.0.0，分别通过 R2 和 R3 与骨干区域连接。这样，我们看到，R2 和 R3 都分别连接了两个区域，在 OSPFv3 中，连接两个或者更多区域的路由器被称为区域边界路由器（ABR）。图 4-12 中我们还可以看到，路由器 R6 连接了区域 36.0.0.0 和区域 37.0.0.0，因此它也是一个区域边界路由器，但是此时区域 37.0.0.0 并没有和骨干区域连接，这样会造成路由的丢失。为解决这个问题，OSPFv3 提出了虚链路的概念（virtual link），虚链路在两个路由器之间指定，它属于骨干区域。图 4-12 中，可以看到，在 R2 和 R6 之间建立了一条虚链路，这样，R6 实际上连接了三个区域，即区域 36.0.0.0，区域 37.0.0.0，

骨干区域，这样，区域 37.0.0.0 和骨干区域就建立了连接。因为这一条虚链路是通过区域 36.0.0.0 建立的，此时将区域 36.0.0.0 称为虚链路的透传区域（transit area）。

图 4-12 中我们还可以看到，区域 37.0.0.0 与骨干区域的连接只有一条链路，而区域 36.0.0.0 则有两条。在 OSPFv3 中，与骨干区域只有一条连接的区域可以被配置为残桩区域（stub area），配置残桩区域的目的是减少路由信息的数量。但是还需要注意的是，即使区域 36.0.0.0 与骨干区域只有一条链路连接，它也不能被配置为残桩区域，因为此时区域 36.0.0.0 已经作为一条虚链路的透传区域，而残桩区域是不能够作为透传区域的。

由于 OSPFv3 运行在一个自治系统内部，因此涉及到与其他 AS 的路由交换。图 4-12 中，R5 与其他 AS 的路由器有连接，此时，R5 被称为自治系统边界路由器（ASBR）。与其他自治系统的路由交互大部分情况是通过 BGP 进行的。

OSPFv3 中的每一个路由器都具有一个路由器 ID（Router ID），这个路由器 ID 唯一标识这个路由器。路由器 ID 是 IPv4 地址格式的，由用户自行指定，0.0.0.0 作为预留，不能使用。

在 OSPFv3 中，存在邻居（Neighbor）和邻接（Adjency）的概念。邻居是指路由器通过某一个接口可以直接到达的路由器，而邻接则是 OSPFv3 协议中能够交换协议消息的逻辑实体。对于点到点链路（包括虚链路）而言，链路的另一端只有一个邻居，因此也只有一个邻接。但是对于以太网这样的广播链路而言，情况不是这样，一条链路上可能连接多个路由器，为了减少路由信息，OSPFv3 定义了指定路由器（DR）和备份指定路由器（BDR），所有路由器只能够与 DR 和 BDR 建立邻接关系，而网络的路由信息则由 DR 负责通告，BDR 用于 DR 失效的情况下取代原有的 DR。图 4-13 给出了一个例子，图中，4 个路由器在以太网链路上形成邻居，其中 R1 为 DR，R2 为 BDR，图中的虚线表示实际形成的邻接关系，可以看到，R3 和 R4 之间并没有形成邻接关系。OSPFv3 中的 DR 和 BDR 由协议过程自动选择，作为操作者，如果希望某一个接口成为 DR，则可以人为规定此接口的 DR 优先级。

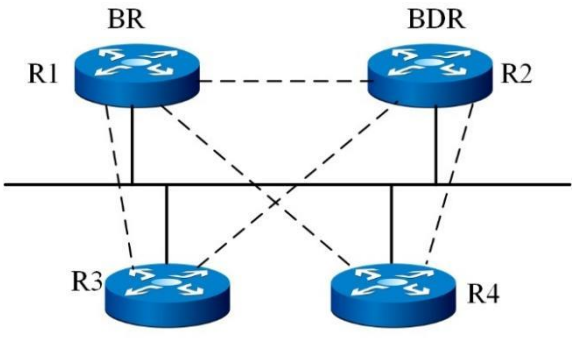


图 4-13 以太网链路上的邻接关系

4.4.1.2 路由信息扩散

OSPFv3 的工作基本上划分为邻接建立过程和随后的触发更新过程。OSPFv3 使用 5 种类型的协议消息来完成协议功能。这些消息是：Hello 消息，DDP 消息，LSR 消息，LACK 消息和 LSU 消息。Hello 消息的作用是检测邻居的状态，以及协商邻接建立参数，以及 DR 和 BDR 的选择。DDP 消息用于 OSPFv3 邻接建立过程中，路由器将自己维护的路由信息的摘要信息置于 DDP 消息中发送给邻居，邻居比较 DDP 消息中的路由信息和自己维护的路由信息，以决定需要向邻居请求哪些路由信息。一旦邻居做了这样的决定，邻居就可以发送 LSR 消息来请求相应的路由信息，收到这样的请求，路由器将发送 LSU 消息通告详细的路由信息。LACK 消息则用于 LSU 消息的确认，因为路由协议基于 IP 这个不保证到达的协议，因此确认是必要的。LSU 消息和 LACK 消息还出现在邻接建立之后的路由变化通告当中。图 4-14 显示了以上所述过程。

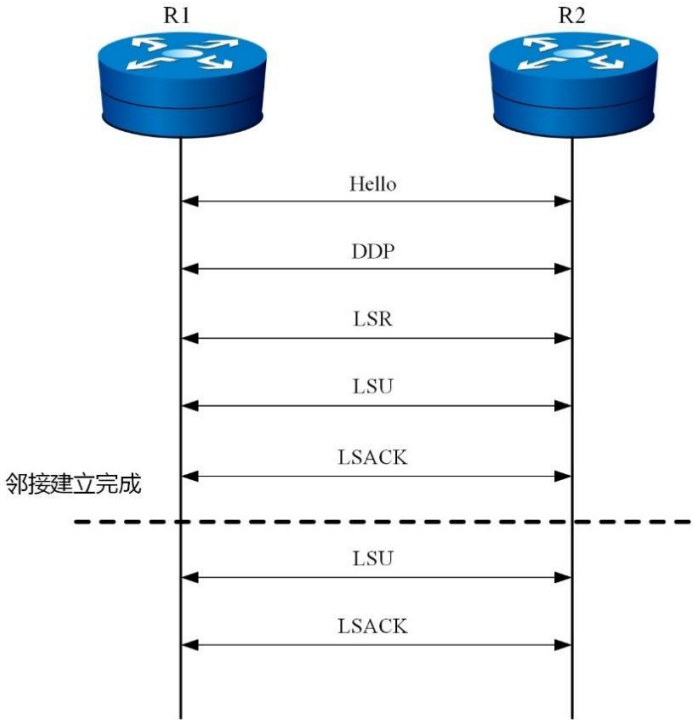


图 4-14 OSPFv3 协议工作过程

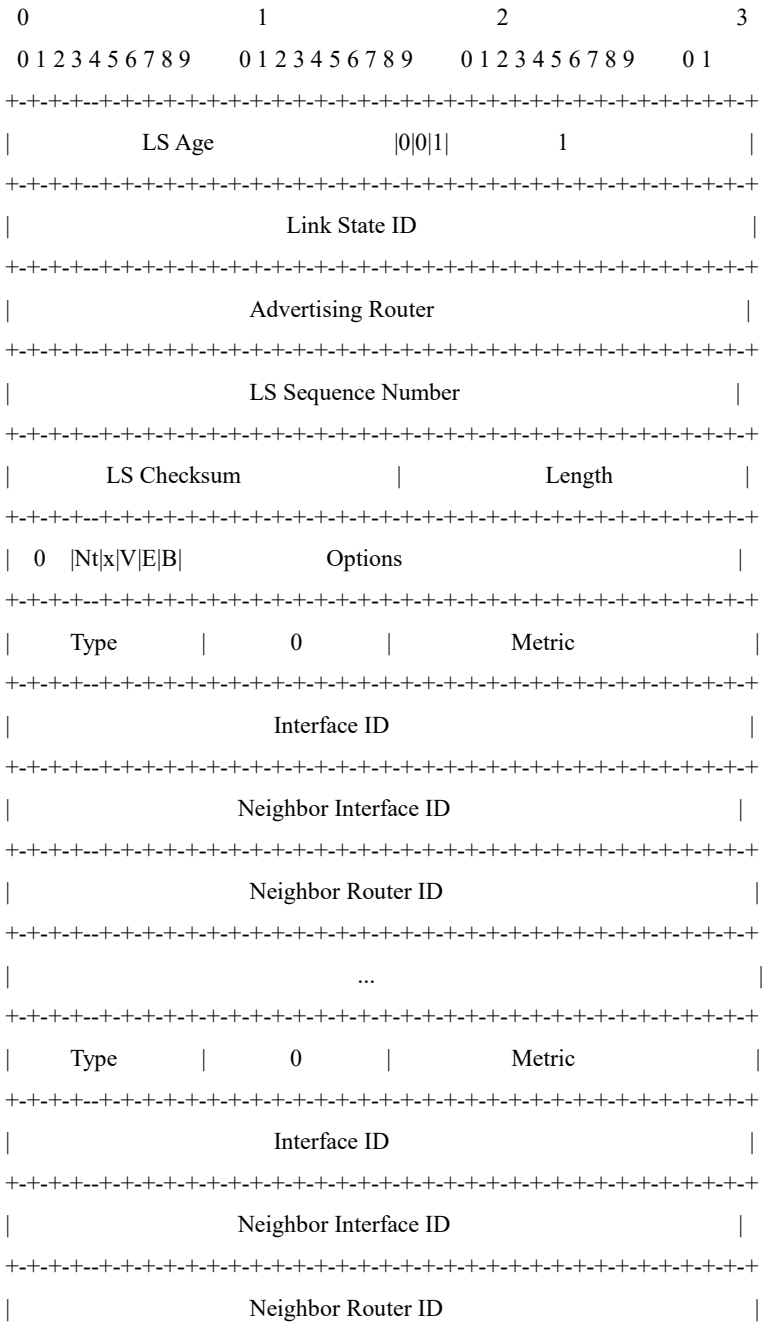
除了 Hello 消息之外，其余的 OSPFv3 消息都和路由信息有关，在 OSPFv3 中，承载路由信息的信息单元称为链路状态通告（LSA）。基本的 LSA 有 7 类，即路由器 LSA，网络 LSA，域内前缀 LSA、域内路由器 LSA、外部 LSA、链路状态 LSA、域间前缀 LSA。这些 LSA 具有不同的涵义，从而可以灵活地进行路由计算。这些 LSA 中，外部 LSA

是针对整个自治系统而言的，它不属于任何区域，而其他的 LSA 则都属于特定的区域。一旦 LSA 的扩散过程完成，则路由器可以进行路由计算，从而最终形成路由转发表中的条目。

4.4.1.3 OSPFv3 LSA 类型

Router-LSAs

Router-LSA 帧格式如图 4-15 所示：



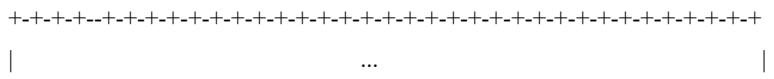


图 4-15 Router-LSA 帧格式

与 OSPFv2 不同的地方在于：

1. LSID 字段的意义。ospfV3 中考虑了分片的处理，路由器可以为一个区域生成一个或多个 RouterLSA，LSID 用来区分生成的多个 router-LSA。这样可以避免 ospfv2 中由于区域中的接口太多而产生大包，导致底层 ip 分片；

   一个 routerLSA 可以包含的链路个数可以设计为（接口 MTU－IP 头部长度 40－LSA 头部长度 16－routerLSA 头部长度 24）/每个 LINK 长度 16＝（1500－40－20－24）/16=88 个；

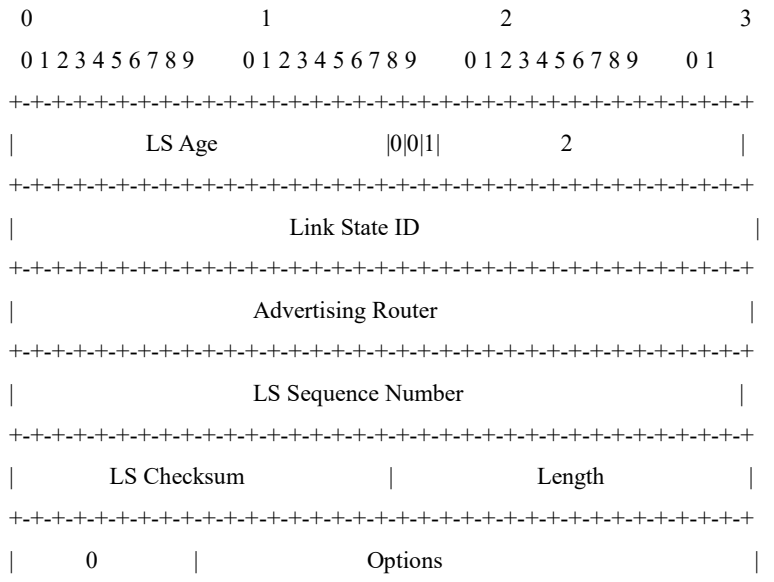
   这里假定接口 MTU 为 1500；

2. 处于 DOWN，Loopback 状态的接口不包含在 RouterLSA 中，没有 FULL 邻接的接口也不包含在 RouterLSA 中。OSPFv3 要求只有 FULL 邻接的接口才能包含在 Router LSA 中，ospfv2 没有此限制；

3. 对于广播和 NBMA 类型的链路，增加 transit 类型的 link 到 router LSA 时，LINK 中的字段：邻居接口 ID 设置为 DR 的的接口 ID，邻居 RouterID 设置为 DR 的路由器 ID。

Network-LSAs

Network-LSA 帧格式如图 4-16 所示（通告的开销为 0）：



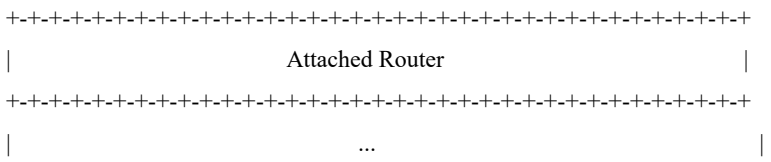


图 4-16 Network-LSA 帧格式

Network LSA 生成与 OSPFv2 相同，有以下改变：

1. LSID 设置为 DR 的接口 ID。ospfv2 中 LSID 设置为 DR 路由器的接口地址；
2. 不包含掩码信息，少了 Net MASK 字段；
3. 选项字段是链路上 FULL 邻居通告的 LINKLSA 中选项的逻辑 OR。

Inter-Area-Prefix-LSAs

Inter-Area-Prefix-LSA 帧格式如图 4-17 所示：

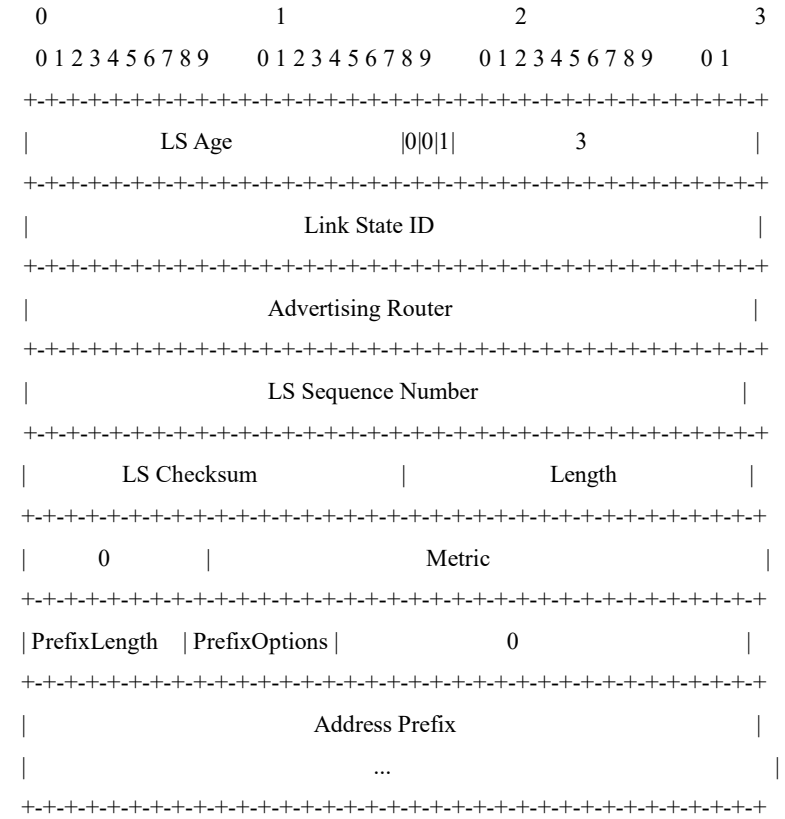


图 4-17 Inter-Area-Prefix -LSA 帧格式

此 LSA 等效于 OSPFv2 中的 3 类 LSA。生成前缀的过程和 OSPFv2 基本一致，主要有以下不同：

LSID 不具有地址意义，只是区分不同的 LSA。因此，设计时可以在目标区域设置一个 InterPrefixID 参数，初始化为 1；

如果是新增加的路由，则递增序号；

如果是已有的路由，则使用前缀进行搜索。

Inter-Area-Router-LSAs

Inter-Area-Router-LSA 帧格式如图 4-18 所示：

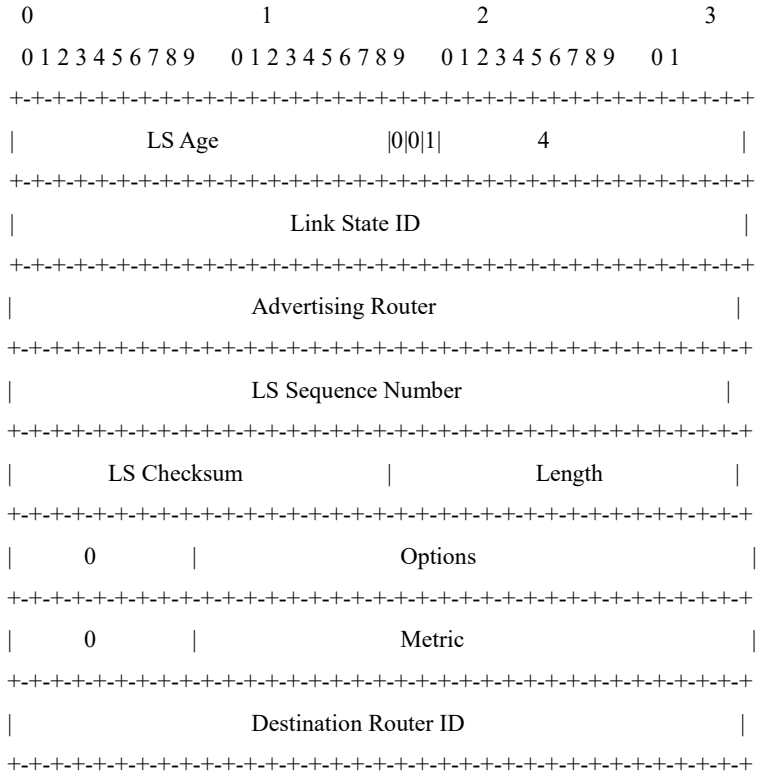


图 4-18 Inter-Area-Router -LSA 帧格式

生成过程和 OSPFv2 基本一致，有以下不同：

1. LSID 不再描述路由器的 ID，而只是用于区分不同的 LSA。设计时可以同域间前缀 LSA；
2. 目的路由器 ID 用 LSA 内容中 Destination Router ID 来标识；
3. 比 OSPFv2 多了选项字段，设置为目的路由器 RouterLSA 中的选项。

AS-External-LSAs

AS-External-LSA 帧格式如图 4-19 所示：

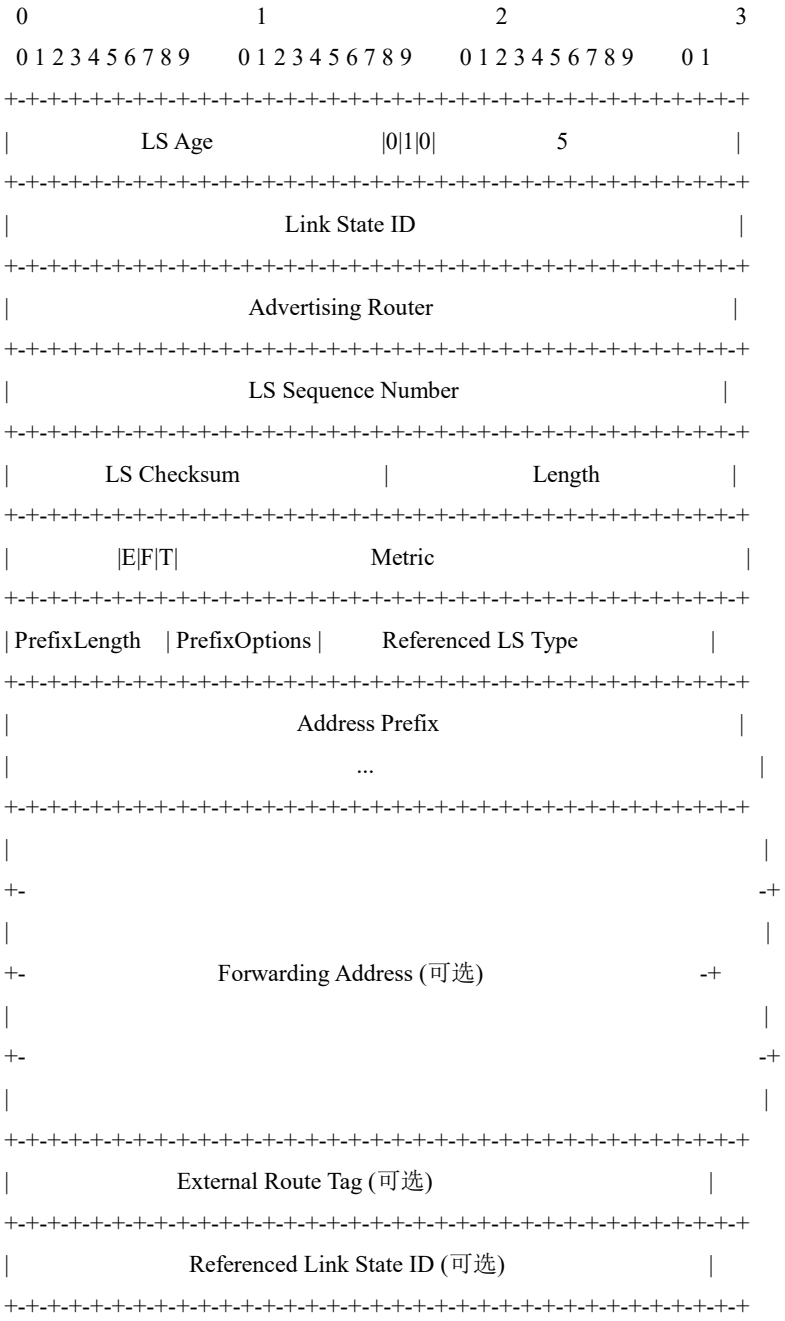


图 4-19 AS-External-LSA 帧格式

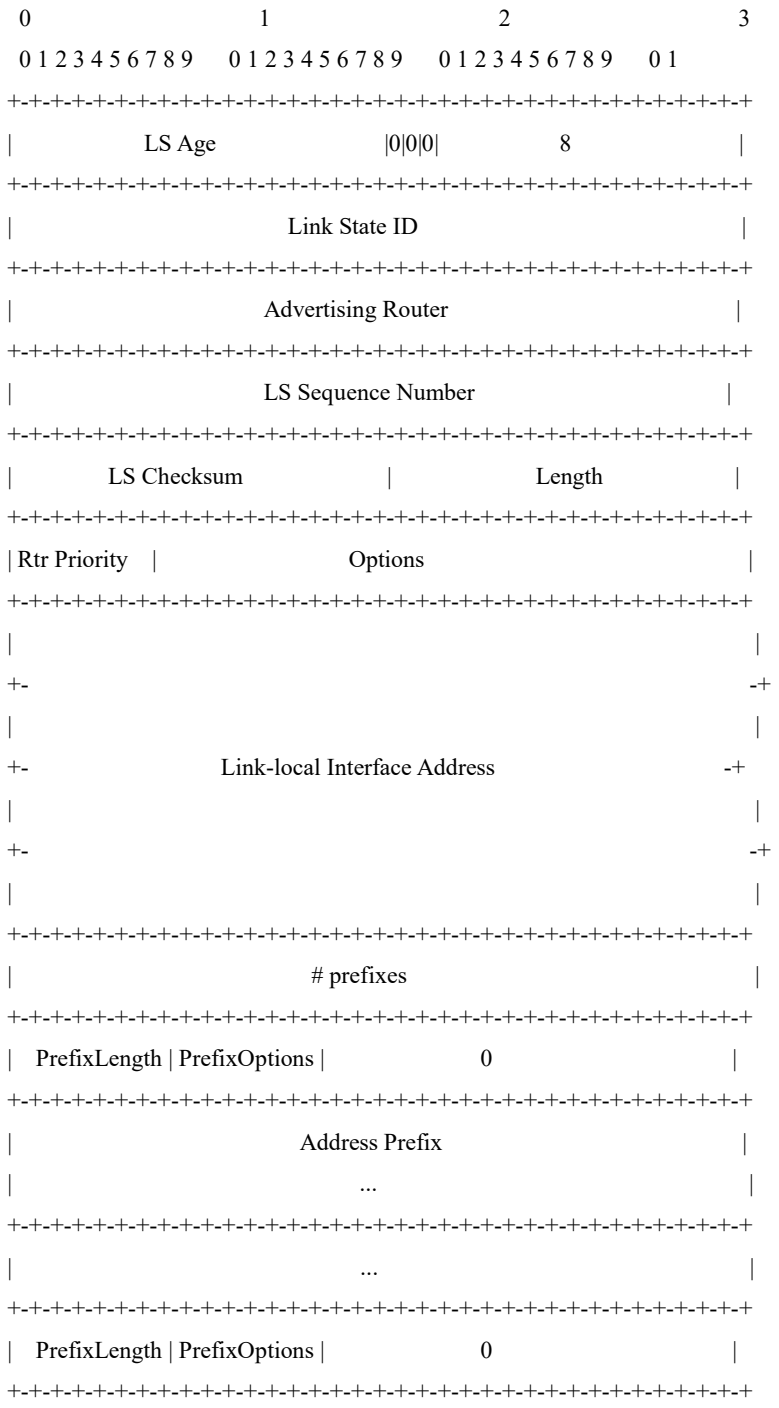
LSID 不再描述路由器的 ID，而只是用于区分不同的 LSA。目的 ID 用 LSAbody 中的地址前缀来标识。

NSSA-LSAs

格式同 5 类，与 OSPFv2 生成方式相同。

Link-LSAs

Link-LSA 帧格式如图 4-20 所示：



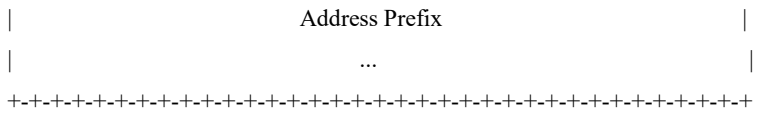


图 4-20 Link-LSA 帧格式

Link-LSA 是 OSPFv2 所没有的。

路由器为每一链路生成 LinkLSA，故设备启动后只要接口 IP，就应该有 LINK-LSA 生成。虚链路不应生成 LINKLSA。LSID 为路由器的接口 ID。

LINKLSA 有 3 个目的：

1. 提供链路本地地址，以 fe80 开始的地址；
2. 提供本地连接的 Ipv6 前缀；
3. 提供选项。

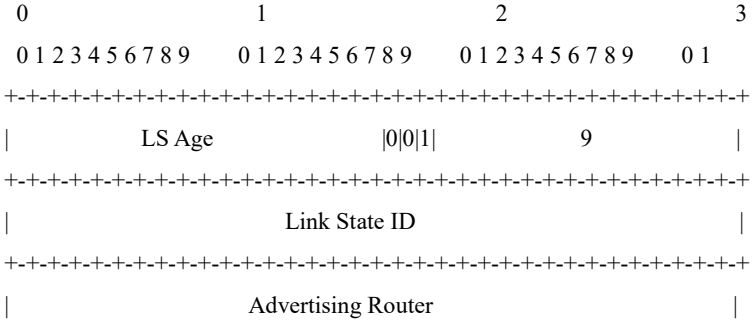
为链路 L 构造 LinkLSA 的过程如下：

- LSID 设置为路由器为 L 设置的接口 ID
- LinkLSA 包含 L 的优先级
- 选项设置为路由器的能力。在广播接口上，DR 生成 NetworkLSA 时，将对所有 FULL 状态邻居的选项进行逻辑或操作。
- 路由器在 LinkLSA 中包含 L 的链路本地地址。此信息用于下一跳计算。
- 包含 L 上配置的所有 Ipv6 地址前缀，指定前缀长度，选项，前缀。

构造之后，将 LSA 加载到链路数据库中，并在链路上扩散。链路上其他节点收到 LSA 后，进行存储，但是不会再次洪泛。

Intra-Area-Prefix-LSAs

Intra-Area-Prefix-LSA 帧格式如图 4-21 所示（LSID 没有地址含义）：



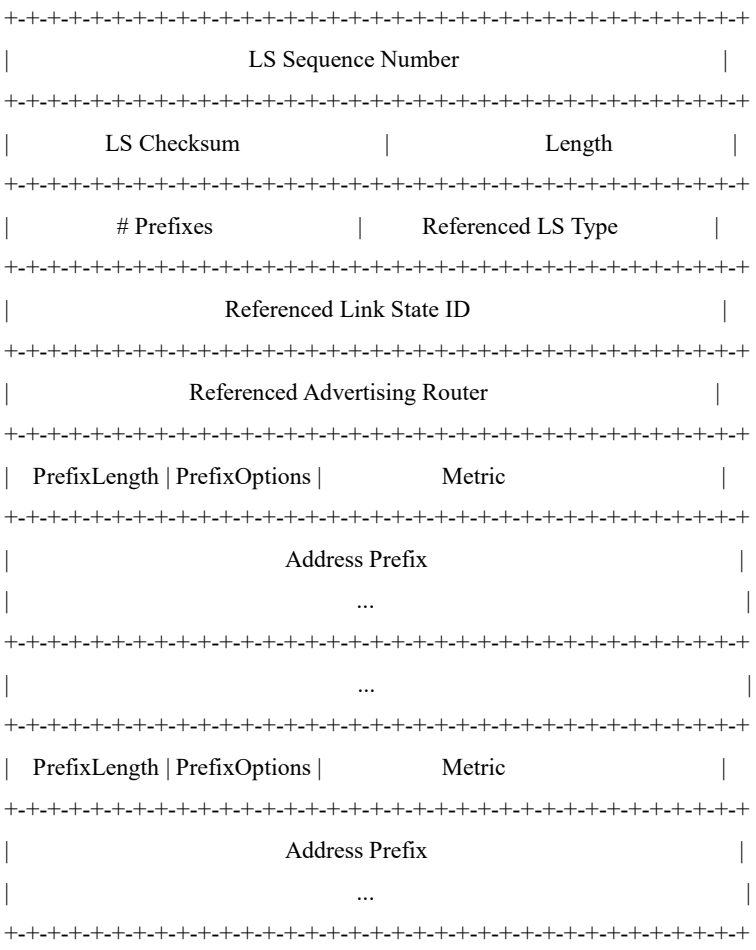


图 4-21 Intra-Area-Prefix-LSA 帧格式

Intra-area-prefix-LSA 与 ospfv2 中的 9 类 LSA 意思完全不一样，ospfv2 中的 9 类 LSA 用于 graceful restart，是接口洪泛范围。intra-area-prefix-LSA 类型描述一个网络上的前缀，或者一个路由器上的前缀，具有区域洪泛范围。LSID 也是用来区分不同的 LSA：

1. 描述一个网络的前缀

Stub 接口——-引用的是当前的 RouterLSA。引用 LSID 为 0，引用路由器 ID 为路由器自己的 ID。

2. 描述一个路由器上的前缀

具有 FULL 邻居的 BCAST 接口——引用的是 NetworkLSA。引用 LSID 为 DR 在 L 上的接口 ID，引用路由器 ID 设置为 DR 的 ID。当路由器是 DR 且有 FULL 邻居时，才生成。

链路的 DR 向区域生成一个或多个 LSA，用于通告链路上的前缀。对链路 L，L 上的 DR 按照以下过程构造 LSA：

- 为表明前缀与 L 对应，引用 LS 类型，引用 LSID 和引用路由器 ID 设置为 L 的 NetworkLSA 上的相应字段。即引用 LS 类型为 0x2002，引用 LSID 为 DR 在 L 上的接口 ID，引用路由器 ID 设置为 DR 的 ID。
- 检查 L 上的每一个 LinkLSA。如果 LinkLSA 的通告路由器与 DR 建立了 FULL 邻居，并且 LSID 与邻居的接口 ID 相同，则拷贝 LINKLSA 中的前缀到新 LSA 中。如果前缀设置了 NU 比特或者 LA 比特选项，则不应拷贝，另外链路本地地址也不应拷贝。如果出现相同的前缀（前缀长度，前缀相同），则将其选项进行逻辑或操作，得到最后的前缀选项。

  所有前缀的开销均为 0。
- “# prefixes”字段设置为 LSA 中的前缀数目。如果有必要，可以将前缀分布到多个 LSA 中以减少 LSA 的大小。

路由器为其 Stub 链路上的前缀构造 intra-area-prefix-LSA。路由器按照以下方法构造 LSA：

- 引用 LS 类型为 0x2001，引用 LSID 为 0，引用路由器 ID 为路由器自己的 ID。
- 检查自己的区域的接口。如果接口状态为 DOWN，不包含接口的前缀；

  如果接口包含在 2 类链路中，则前缀将包含在接口 DR 通告的 LSA 中，跳过接口；

  如果前缀设置了 LA 比特，则需要包含此前缀；

  前缀的开销设置为对应接口的开销。
- LSA 中包含直连的主机（可选）。
- 如果具有经过此区域的一个或多个虚链路，则包含一个全球 IPv6 接口地址（如果没有配置的话），选项中设置 LA 比特，前缀长度为 128，开销为 0。此信息可用于虚链路两端相互学习地址。
- “# prefixes”设置为前缀数目。

4.4.2 OSPFv3 配置

4.4.2.1 配置全局 OSPFv3

4.4.2.1.1 使能 OSPFv3 进程

目的

本节介绍如何启动和关闭（使能/去使能）OSPFv3 进程。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
启动默认 OSPFv3 进程	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **router ipv6 ospf**。
启动指定 OSPFv3 进程	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **router ipv6 ospf** *process-id*。
关闭默认 OSPFv3 进程	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **no router ipv6 ospf**。
关闭指定 OSPFv3 进程	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **no router ipv6 ospf** *process-id*。

4.4.2.1.2 使能 OSPFv3 进程指定 VPN 实例

目的

本节介绍如何启动（使能）OSPFv3 进程指定的 VPN 实例。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
启动指定 OSPFv3 进程指定 VPN 实例	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **router ipv6 ospf** *process-id* **vpn-instance** *name*。
启动默认 OSPFv3 进程指定 VPN 实例	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **router ipv6 ospf vpn-instance** *name*。

4.4.2.1.3 复位 OSPFv3 进程

目的

本节介绍如何复位 OSPFv3 进程。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
复位 OSPFv3 进程	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **reset ipv6 ospf**。

目的	步骤
复位指定 OSPFv3 进程	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **reset ipv6 ospf** *process-id*。

4.4.2.1.4 清除 OSPFv3 统计信息

目的

本节介绍如何清除 OSPFv3 统计信息。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
清除 OSPFv3 统计信息	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **reset ipv6 ospf counters**。

4.4.2.2 配置 OSPFv3 节点

4.4.2.2.1 配置路由器 ID

目的

本节介绍如何配置路由器 ID。

背景信息

配置的路由器 ID 必须为本地 IP 地址之一。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置路由器 ID	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **router ipv6 ospf**，进入 OSPFv3 配置视图； 3. 执行命令 **router-id** *router-id*。

4.4.2.2.2 配置 Stub 区域

目的

本节介绍如何配置 Stub 区域。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置普通 Stub 区域	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **router ipv6 ospf**，进入 OSPFv3 配置视图； 3. 执行命令 **area** *area-id* **stub**。
配置 totalStub 区域	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **router ipv6 ospf**，进入 OSPFv3 配置视图； 3. 执行命令 **area** *area-id* **stub no-summary**。
删除 Stub 区域	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **router ipv6 ospf**，进入 OSPFv3 配置视图； 3. 执行命令 **no area** *area-id* **stub**。
配置 Stub 路由器	1. 进入全局配置视图； 2. 进入 OSPFv3 配置视图； 3. 执行命令 **stub-router**。
配置 Stub 路由器，并设置设备在发生重启或故障时保持为 Stub 路由器的时间间隔	1. 进入全局配置视图； 2. 进入 OSPFv3 配置视图； 3. 执行命令 **stub-router on-startup** [*on-startup-time* | **default**]。
删除 Stub 路由器	1. 进入全局配置视图； 2. 进入 OSPFv3 配置视图； 3. 执行命令 **no stub-router**。

4.4.2.2.3 配置 NSSA 区域

目的

本节介绍如何配置 NSSA 区域。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置 NSSA 区域	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **router ipv6 ospf**，进入 OSPFv3 配置视图； 3. 执行命令 **area** *area-id* **nssa**。
配置 no summary NSSA 区域	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **router ipv6 ospf**，进入 OSPFv3 配置视图； 3. 执行命令 **area** *area-id* **nssa no-summary**。
配置 NSSA 区域聚合通告/不通告	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **router ipv6 ospf**，进入 OSPFv3 配置视图； 3. 执行命令 **area** *area-id* **nssa range** *dst-address dst-mask* { **advertise** | **not-advertise** }。

目的	步骤
配置 NSSA 指定转换路由器或者候选转换路由器	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **router ipv6 ospf**，进入 OSPFv3 配置视图； 3. 执行命令 **area** *area-id* **nssa translator** { **always** | **candidate** }。
删除 NSSA 区域	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **router ipv6 ospf**，进入 OSPFv3 配置视图； 3. 执行命令 **no area** *area-id* **nssa**。
删除 NSSA 区域聚合	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **router ipv6 ospf**，进入 OSPFv3 配置视图； 3. 执行命令 **no area** *area-id* **nssa range** *dst-address dst-mask*。

4.4.2.2.4 配置区域聚合

目的

本节介绍如何配置区域聚合。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
区域聚合	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **router ipv6 ospf**，进入 OSPFv3 配置视图； 3. 执行命令 **area** *area-id* **range** *dst-address dst-mask* { **advertise** | **not-advertise** }。
删除区域聚合	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **router ipv6 ospf**，进入 OSPFv3 配置视图； 3. 执行命令 **no area** *area-id* **range** *dst-address dst-mask*。

4.4.2.2.5 配置 GR 重启

目的

本节介绍如何配置 GR（Graceful Restart）重启。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
使能 GR	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **router ipv6 ospf**，进入 OSPFv3 配置视图； 3. 执行命令 **graceful-restart**。

目的	步骤
配置 GR 周期	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **router ipv6 ospf**，进入 OSPFv3 配置视图； 3. 执行命令 **graceful-restart period** *restart-time*。
使能 GR helper	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **router ipv6 ospf**，进入 OSPFv3 配置视图； 3. 执行命令 **graceful-restart helper**。
去使能 GR 重启	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **router ipv6 ospf**，进入 OSPFv3 配置视图； 3. 执行命令 **no graceful-restart**。
去使能 GR helper	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **router ipv6 ospf**，进入 OSPFv3 配置视图； 3. 执行命令 **no graceful-restart helper**。
执行 GR 重启	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **router ipv6 ospf**，进入 OSPFv3 配置视图； 3. 执行命令 **graceful-restart begin**。

4.4.2.2.6 配置路由计算间隔

目的

本节介绍如何配置路由计算间隔。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置路由计算间隔	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **router ipv6 ospf**，进入 OSPFv3 配置视图； 3. 执行如下命令： ● **spf-running-interval** *interval* ● **spf-running-interval default**。

4.4.2.2.7 配置 OSPFv3 重分配

目的

本节介绍如何配置 OSPFv3 重分配。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置 OSPFv3 重分配	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **router ipv6 ospf**，进入 OSPFv3 配置视图； 3. 执行命令 **redistribute** { **connect** | **static** | **rip** | **bgp** | **isis** | **ospf** }。
删除 OSPFv3 重分配	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **router ipv6 ospf**，进入 OSPFv3 配置视图； 3. 执行命令 **no redistribute** { **connect** | **static** | **rip** | **bgp** | **isis** | **ospf** }。
配置重分配路由策略	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **router ipv6 ospf**，进入 OSPFv3 配置视图； 3. 执行命令 **redistribute** { **connect** | **static** | **rip** | **bgp** | **isis** | **ospf** } **route-policy** *policy-name*。
删除重分配路由策略	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **router ipv6 ospf**，进入 OSPFv3 配置视图； 3. 执行命令 **no redistribute** { **connect** | **static** | **rip** | **bgp** | **isis** | **ospf** } **route-policy** *policy-name*。

4.4.2.2.8 使能 OSPFv3 上报 trap

目的

本节介绍如何使能 OSPFv3 上报 trap。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
使能/去使能 OSPFv3 上报 trap 功能	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **router ipv6 ospf**，进入 OSPFv3 配置视图； 3. 执行命令 **snmp-trap** { **enable** | **disable** }。
使能/去使能 OSPFv3 上报 trap 具体功能	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **router ipv6 ospf**，进入 OSPFv3 配置视图； 3. 执行命令 **snmp-trap** { **enable** | **disable** } **trap-name** { **ifconfigerror** | **ifrxbadpacket** | **ifstatechange** | **nbrrestarthelperstatuschange** | **nbrstatechange** | **nssatranslatorstatuschange** | **restartstatuschange** | **virtifconfigerror** | **virtifrxbadpacket** | **virtifstatechange** | **virtnbrrestarthelperstatuschange** | **virtnbrstatechange** }。

4.4.2.3 配置 OSPFv3 端口

4.4.2.3.1 配置 OSPFv3 接口参数

目的

本节介绍如何配置 OSPFv3 接口参数。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
将接口加入到指定的区域中	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *N*，进入 VLAN IF 配置视图； 3. 执行命令 **ipv6 ospf area** *area-id*。
将接口加入到指定的进程中	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *N*，进入 VLAN IF 配置视图； 3. 执行如下命令： ● **ipv6 ospf area** *area-id* **process** *process-id* ● **ipv6 ospf area** *area-id* **process** *process-id* **instance** *instance-id*。
配置 OSPFv3 接口类型	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *N*，进入 VLAN IF 配置视图； 3. 执行命令 **ipv6 ospf if-type** { **broadcast** | **p2p** }。
配置 OSPFv3 接口优先级	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *N*，进入 VLAN IF 配置视图； 3. 执行如下命令： ● **ipv6 ospf priority** *priority* ● **ipv6 ospf priority default**。
配置 OSPFv3 接口开销	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *N*，进入 VLAN IF 配置视图； 3. 执行如下命令： ● **ipv6 ospf cost** *cost* ● **ipv6 ospf cost default**。
配置 OSPFv3 接口 Hello 间隔时间	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *N*，进入 VLAN IF 配置视图； 3. 执行如下命令： ● **ipv6 ospf hello-interval** *hello-interval* ● **ipv6 ospf hello-interval default**。
配置 OSPFv3 接口的 wait 定时器的间隔时间	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *N*，进入 VLAN IF 配置视图； 3. 执行如下命令： ● **ipv6 ospf wait-interval** { *wait-interval* | **default** } ● **ipv6 ospf wait-interval** { *wait-interval* | **default** } **process** *process-id*。
配置 OSPFv3 接口邻居超时时间	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *N*，进入 VLAN IF 配置视图； 3. 执行如下命令：

目的	步骤
	● **ipv6 ospf dead-interval** *dead-interval* ● **ipv6 ospf dead-interval default**。
配置 OSPFv3 接口重传间隔	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *N*，进入 VLAN IF 配置视图； 3. 执行如下命令： ● **ipv6 ospf retransmit-interval** *retransmit-interval* ● **ipv6 ospf retransmit-interval default**。
配置 OSPFv3 接口传输时延	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *N*，进入 VLAN IF 配置视图； 3. 执行如下命令： ● **ipv6 ospf transmit-delay** *transmit-delay* ● **ipv6 ospf transmit-delay default**。

4.4.2.3.2 配置 BFD

目的

本节介绍如何配置 BFD。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置 BFD	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *N*，进入 VLAN IF 配置视图； 3. 执行命令 **ipv6 ospf bfd** { **enable** | **disable** }。

4.4.2.3.3 配置 OSPFv3 接口 MTU

目的

本节介绍如何配置 OSPFv3 接口 MTU。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置 OSPFv3 接口 MTU	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *N*，进入 VLAN IF 配置视图； 3. 执行命令 **ipv6 ospf mtu** *mtu* 或 **ip ospf mtu default**。
配置 MTU 检测	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *N*，进入 VLAN IF 配置视图；

目的	步骤
	3. 执行命令 **ipv6 ospf mtu-ignore** { **enable** | **disable** }。

4.4.2.3.4 配置 passive 接口

目的

本节介绍如何配置 passive 接口。

背景信息

被动接口是指不收发协议消息的 OSPFv3 接口，在此接口上不建立任何邻居，但是接口路由将包含在 RouterLSA 中作为内部路由传播。可用于 Stub 路由。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置 passive 接口	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *N*，进入 VLAN IF 配置视图； 3. 执行命令 **ipv6 ospf passive-interface**。
删除 passive 接口配置	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *N*，进入 VLAN IF 配置视图； 3. 执行命令 **no ipv6 ospf passive-interface**。

4.4.2.4 配置 OSPFv3 调试功能

目的

本节介绍如何配置 OSPFv3 调试功能。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
开启全局 debug 信息	1. 进入特权用户视图； 2. 执行命令 **debug ospf6** { **global** | **all** | **lsa** | **hello** | **packet** | **neighbor** | **interface** | **ip-route** | **rtm** | **spf** | **syn** | **graceful-restart** | **nbrchange** | **frr** | **error** }。
开启具体实例 debug 信息	1. 进入特权用户视图； 2. 执行命令 **debug ospf6** { **global** | **all** | **lsa** | **hello** | **packet** | **neighbor** | **interface** | **ip-route** | **rtm** | **spf** | **syn** | **graceful-restart** | **nbrchange** | **frr** | **error** } **process** *process-id*。

目的	步骤
开启所有实例 debug 信息	1. 进入特权用户视图； 2. 执行命令 **debug ospf6** { **global** | **all** | **lsa** | **hello** | **packet** | **neighbor** | **interface** | **ip-route** | **rtm** | **spf** | **syn** | **graceful-restart** | **nbrchange** | **frr** | **error** } **process all**。
关闭全局 debug 信息	1. 进入特权用户视图； 2. 执行命令 **no debug ospf6** { **global** | **all** | **lsa** | **hello** | **packet** | **neighbor** | **interface** | **ip-route** | **rtm** | **spf** | **syn** | **graceful-restart** | **nbrchange** | **frr** | **error** }。
关闭具体实例 debug 信息	1. 进入特权用户视图； 2. 执行命令 **no debug ospf6** { **global** | **all** | **lsa** | **hello** | **packet** | **neighbor** | **interface** | **ip-route** | **rtm** | **spf** | **syn** | **graceful-restart** | **nbrchange** | **frr** | **error** } **process** *process-id*。
关闭所有实例 debug 信息	1. 进入特权用户视图； 2. 执行命令 **no debug ospf6** { **global** | **all** | **lsa** | **hello** | **packet** | **neighbor** | **interface** | **ip-route** | **rtm** | **spf** | **syn** | **graceful-restart** | **nbrchange** | **frr** | **error** } **process all**。

4.4.2.5 维护及调试

目的

当 OSPFv3 功能不正常，需要进行查看、定位或调试问题时，可以使用本小节操作。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
显示 OSPFv3 简要信息	1. 进入普通用户视图； 2. 执行如下命令： ● **show ipv6 ospf brief** ● **show ipv6 ospf brief process** *process-id*。
显示 OSPFv3 配置信息	1. 进入普通用户视图； 2. 执行命令 **show ipv6 ospf config**。
显示 OSPFv3 错误信息	1. 进入普通用户视图； 2. 执行命令 **show ipv6 ospf error**。
显示 OSPFv3 接口信息	1. 进入普通用户视图； 2. 执行如下命令： ● **show ipv6 ospf interface** ● **show ipv6 ospf interface vlan** *vlan-id* ● **show ipv6 ospf interface loopback** *loopback-id*

目的	步骤
	● **show ipv6 ospf interface** { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* ● **show ipv6 ospf interface** { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number.subinterface* ● **show ipv6 ospf interface count** ● **show ipv6 ospf interface error** ● **show ipv6 ospf interface process** *process-id*。
显示 OSPFv3 邻居信息	1. 进入普通用户视图； 2. 执行如下命令： ● **show ipv6 ospf neighbor** ● **show ipv6 ospf neighbor process** *process-id* ● **show ipv6 ospf neighbor** *ip-address* ● **show ipv6 ospf neighbor state statistic**。
显示 OSPFv3 区域信息	1. 进入普通用户视图； 2. 执行如下命令： ● **show ipv6 ospf area** ● **show ipv6 ospf area** *area-id* ● **show ipv6 ospf area process** *process-id*。
显示 OSPFv3 数据库信息	1. 进入普通用户视图； 2. 执行如下命令： ● **show ipv6 ospf database** ● **show ipv6 ospf database process** *process-id* ● **show ipv6 ospf database area** *area-id* ● **show ipv6 ospf database area** *area-id* **process** *process-id* ● **show ipv6 ospf database count** ● **show ipv6 ospf database count process** *process-id* ● **show ipv6 ospf database total count** ● **show ipv6 ospf database** { **router** | **network** | **inter-prefix** | **inter-router** | **external** | **link** | **intra-prefix** | **nssa** | **te** } ● **show ipv6 ospf database** { **router** | **network** | **inter-prefix** | **inter-router** | **intra-prefix** | **nssa** | **te** } *LS-id advertise-router-id area-id* ● **show ipv6 ospf database age** *min-age max-age* ● **show ipv6 ospf database area** *area-id* ● **show ipv6 ospf database area** *area-id* **process** *process-id* ● **show ipv6 ospf database external** *LS-id advertise-router-id* ● **show ipv6 ospf database link** *LS-id advertise-router-id* **interface vlan** *vlan-id*

目的	步骤
	● **show ipv6 ospf database link** *LS-id advertise-router-id* **interface loopback** *loopback-id* ● **show ipv6 ospf database link** *LS-id advertise-router-id* **interface** { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* ● **show ipv6 ospf database link** *LS-id advertise-router-id* **interface** { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number*.subinterface。
显示 OSPFv3 路由信息	1. 进入普通用户视图； 2. 执行如下命令： ● **show ipv6 ospf route** ● **show ipv6 ospf route process** *process-id* ● **show ipv6 ospf route total count**。
显示 OSPFv3 BFD 信息	1. 进入普通用户视图； 2. 执行命令 **show ipv6 ospf bfd session**。
显示 OSPFv3 trap 信息	1. 进入普通用户视图； 2. 执行命令 **show ipv6 ospf trap**。
导出 OSPFv3 模块记录的数据库信息或所有表项信息	1. 进入普通用户视图； 2. 执行命令 **dump ha ospfv3** { **database** | **diag-all** }导出 OSPFv3 模块记录的数据库信息或所有表项信息，用来判断设备两块主控卡上表项是否一致。

4.4.3 OSPFv3 配置举例

4.4.3.1 配置 OSPFv3 基本功能

组网要求

本案例的任务是完成 OSPFv3 最基本的配置，通过该配置熟悉 OSPFv3 的配置过程，拓扑图如图 4-22 所示。

组网图

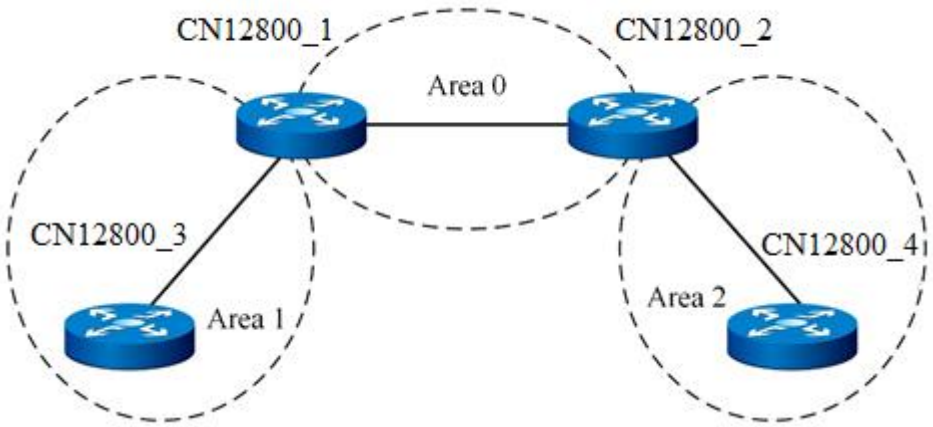


图 4-22 OSPFv3 基本配置拓扑图

配置思路

所有的设备都运行 OSPFv3，并将整个自治系统划分为 3 个区域，其中，CN12800_1 和 CN12800_2 为 ABR 来转发区域之间的路由。

配置完成后，每台设备都应学到自治系统内的到所有网段的路由。

数据准备

CN12800_1 的两个接口地址：2001::1/64 和 2003::1/64

CN12800_2 的两个接口地址：2001::2/64 和 2004::2/64

CN12800_3 的接口地址：2003::3/64

CN12800_4 的接口地址：2004::4/64。

配置步骤

CN12800_1:

CN12800_1(config)#router ipv6 ospf

CN12800_1(config-ospfv3-1)#router-id 1.1.1.1

CN12800_1(config-ospfv3-1)#quit

CN12800_1(config)#interface vlan 10

CN12800_1(config-if-vlan10)#ipv6 ospf area 0

CN12800_1(config-if-vlan10)#quit

CN12800_1(config)#

CN12800_1(config)#interface vlan 30

CN12800_1(config-if-vlan 30)#ipv6 ospf area 0

CN12800_2:

CN12800_2(config)#router ipv6 ospf

CN12800_2(config-ospfv3-1)#router-id 2.1.1.2

CN12800_2(config-ospfv3-1)#quit

CN12800_2(config)#interface vlan 10

CN12800_2(config-if-vlan10)#ipv6 ospf area 0

CN12800_1(config-if-vlan10)#quit

CN12800_1(config)#

CN12800_1(config)#interface vlan 40

CN12800_1(config-if-vlan 40)#ipv6 ospf area 0

CN12800_3:

CN12800_3(config)#router ipv6 ospf

CN12800_3(config-ospfv3-1)#router-id 3.1.1.3

CN12800_3(config-ospfv3-1)#quit

CN12800_3(config)#interface vlan 30

CN12800_3(config-if-vlan30)#ipv6 ospf area 0

CN12800_4:

CN12800_4(config)#router ipv6 ospf

CN12800_4(config-ospfv3-1)#router-id 4.1.1.4

CN12800_4(config-ospfv3-1)#quit

CN12800_4(config)#interface vlan 40

CN12800_4(config-if-vlan40)#ipv6 ospf area 0

验证配置结果

使用 show ipv6 ospf neighbor 命令可看到 OSPFv3 的信息如下：

Ospfv3 过程 1

NeighborId	Priority	State	Interface	Instance	Aging UpTime	IpAddress
1.1.1.2	1	Full	vlan10	0	32 0:01:38	fe80::b8:1

使用 show ip ospf database 命令可看到 OSPFv3 的信息如下：

Database of OSPFv3 过程 1

Router Link State (Area 0.0.0.1)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
0.0.0.0	1.1.1.1	196	0x80000002	0x49f7	40
0.0.0.0	3.1.1.3	197	0x80000002	0x43fc	40

Network Link State (Area 0.0.0.1)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
0.0.39.17	3.1.13	197	0x80000001	0x11d1	32

Intra Area Prefix Link State (Area 0.0.0.1)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
0.0.3.232	3.1.1.3	197	0x80000001	0x1a6c	44

Link(Type-8) State(interface vlan1 Area 0.0.0.1)

LinkId	ADV Router	Age	Seq#	CheckSum	Len
0.0.39.17	1.1.1.1	236	0x80000001	0xf91	76
0.0.39.17	3.1.1.3	237	0x80000001	0x6155	76

4.4.3.2 配置 Stub 区域

组网要求

本案例的任务是完成 OSPFv3 Stub 区域的配置，通过该配置熟悉 OSPFv3 Stub 区域的配置过程，拓扑图如图 4-23 所示。

组网图

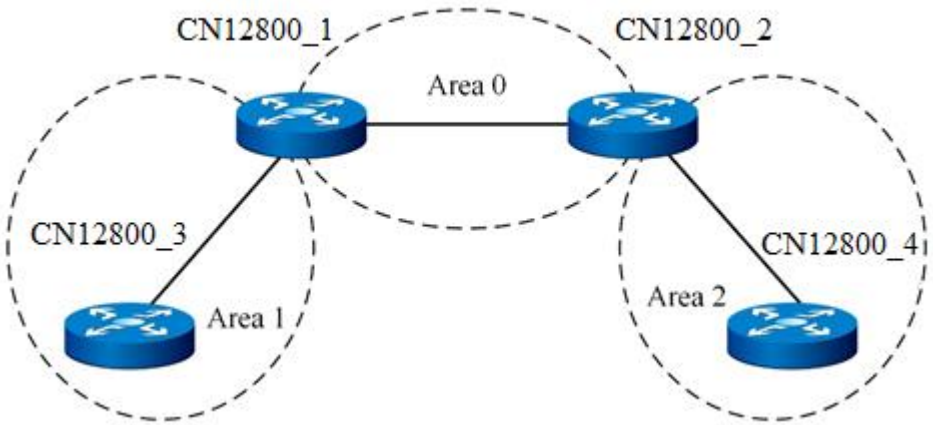


图 4-23 Stub 区域拓扑图

配置思路

所有的设备都运行 OSPFv3，并将整个自治系统划分为 3 个区域，其中 CN12800_1 和 CN12800_2 为 ABR 来转发区域之间的路由。

配置完成后，每台设备都应学到自治系统内的到所有网段的路由。

数据准备

CN12800_1 的两个接口地址：2001::1/64 和 2003::1/64

CN12800_2 的两个接口地址：2001::2/64 和 2004::2/64

CN12800_3 的接口地址：2003::3/64

CN12800_4 的接口地址：2004::4/64。

配置步骤

基本配置和拓扑同 4.4.3.1 配置 OSPFv3 基本功能。

配置 area 1 为 stub：

CN12800_1:

CN12800_1(config)#router ipv6 ospf

CN12800_1(config-ospfv3-1)#area 1 stub

CN12800_1(config)#

CN12800_3:

CN12800_3(config)#router ipv6 ospf

CN12800_3(config-ospfv3-1)# area 1 stub

CN12800_3(config)#

在 CN12800_4 引入 2013:0122::1/64 的 5 类 LSA

CN12800_4:

CN12800_4(config-ospfv3-1)#redistribute static

验证配置结果

1) 当 CN12800_3 所在区域为普通区域时，可以看到路由表中存在 AS 外部的路由。变成 stub 区域后，比正常区域多一个缺省的 3 类 Inter-Area-Prefix-LSAs，看不到 AS 外部的 LSA。

2) 当 CN12800_3 所在区域配置为 Stub 区域时，已经看不到 AS 外部的路由，取而代之的是一条通往区域外部的缺省路由。

4.4.3.3 配置 NSSA 区域

组网要求

本案例的任务是完成 OSPFv3 NSSA 区域的配置，通过该配置熟悉 OSPFv3 NSSA 区域的配置过程，拓扑图如图 4-24 所示。

组网图

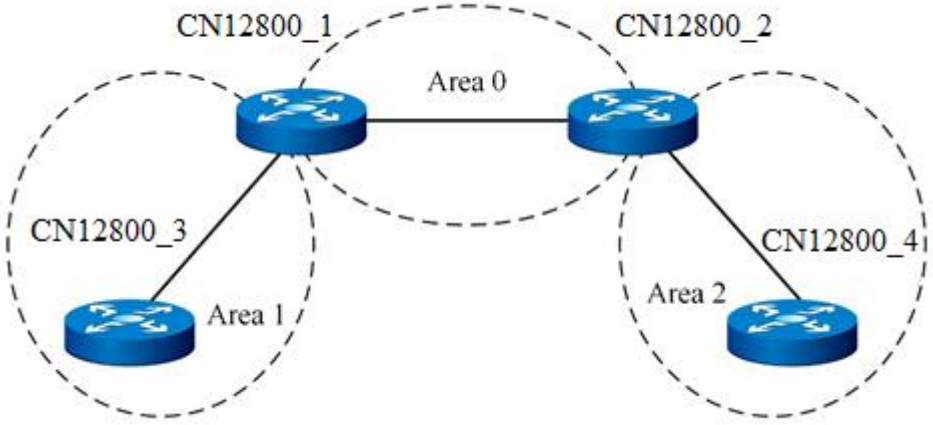


图 4-24 NSSA 区域拓扑图

配置思路

所有的设备都运行 OSPFv3，并将整个自治系统划分为 3 个区域，其中 CN12800_1 和 CN12800_2 为 ABR 来转发区域之间的路由。

配置完成后，每台设备都应学到自治系统内的到所有网段的路由。

数据准备

CN12800_1 的两个接口地址：2001::1/64 和 2003::1/64

CN12800_2 的两个接口地址：2001::2/64 和 2004::2/64

CN12800_3 的接口地址：2003::3/64

CN12800_4 的接口地址：2004::4/64。

配置步骤

基本配置和拓扑同 4.4.3.1 配置 OSPFv3 基本功能。

配置 area 1 为 nssa：

CN12800_1:

CN12800_1(config)#router ipv6 ospf

CN12800_1(config-ospfv3-1)#area 1 nssa

CN12800_1(config)#

CN12800_3:

CN12800_3(config)#router ipv6 ospf

CN12800_3(config-ospfv3-1)# area 1 nssa

CN12800_3(config)#

验证配置结果

1) nssa 区域的数据库比正常区域的数据库多一个缺省 NSSA 类型 LSA

2) 在 CN12800_3 引入 1111:1011::1/64 的静态路由，重分配静态路由。

3) 在 CN12800_4 引入 2222:1011::1/64 的静态路由，查看 CN12800_3 是否拥有外部路由。

4.4.3.4 配置 BFD 功能

组网要求

本案例的任务是完成 OSPFv3 BFD 功能的配置，通过该配置熟悉 OSPFv3 BFD 功能的配置过程，拓扑图如图 4-25 所示。

组网图

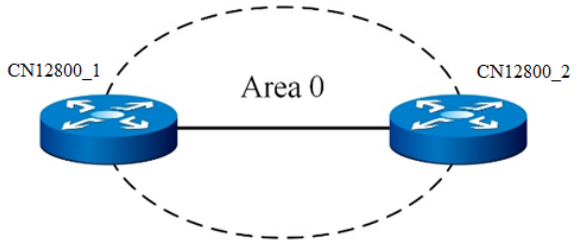


图 4-25 BFD 功能案例拓扑图

配置思路

2 个设备都运行 OSPFv3，并将有个都配置为区域 0。

数据准备

CN12800_1 的两个接口地址：2001::1/64 和 2003::1/64

CN12800_2 的两个接口地址：2001::2/64 和 2004::2/64

CN12800_3 的接口地址：2003::3/64

CN12800_4 的接口地址：2004::4/64。

配置步骤

1) 基本配置：

CN12800_1:

CN12800_1(config)#router ipv6 ospf

CN12800_1(config-ospfv3-1)#router-id 1.1.1.1

CN12800_1(config-ospfv3-1)#quit

CN12800_1(config)#interface vlan 10

CN12800_1(config-if-vlan10)#ipv6 ospf area 0

CN12800_1(config-if-vlan10)#quit

CN12800_2:

CN12800_2(config)#router ipv6 ospf

CN12800_2(config-ospfv3-1)#router-id 2.1.1.2

CN12800_2(config-ospfv3-1)#quit

CN12800_2(config)#interface vlan 10

CN12800_2(config-if-vlan10)#ipv6 ospf area 0

CN12800_2(config-if-vlan10)#quit

2) BFD 配置：

CN12800_1：

CN12800_1(config)#interface vlan 4

CN12800_1(config-vlan-10)#bfd enable

CN12800_1(config-vlan-10)#ipv6 ospf bfd enable

CN12800_2：

CN12800_2(config)#interface vlan 4

CN12800_2(config-vlan-10)#bfd enable

CN12800_2(config-vlan-10)#ipv6 ospf bfd enable

验证配置结果

CN12800_1#sho ipv6 ospf bfd session

OSPF 过程 1

NeighborAddress	NeighborID	BFDState
fe80::b8:2	2.1.1.2	UP

CN12800_2#sho ipv6 ospf bfd session

OSPF 过程 1

NeighborAddress	NeighborID	BFDState
fe80::b8:1	1.1.1.1	UP

4.4.3.5 配置 GR 功能

组网要求

本案例的任务是完成 OSPFv3 GR 功能的配置，通过该配置熟悉 OSPFv3 GR 功能的配置过程，拓扑图如图 4-26 所示。

组网图

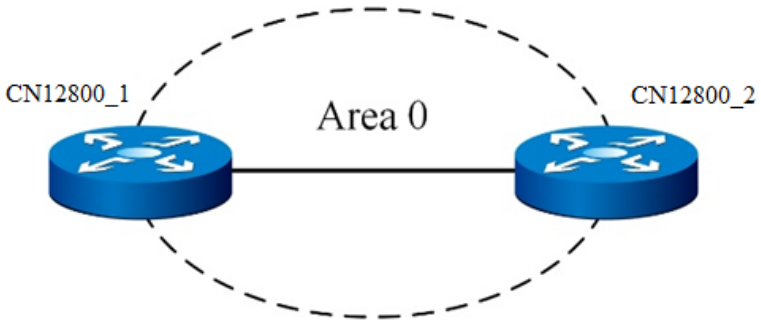


图 4-26 GR 功能案例拓扑图

配置思路

2 个设备都运行 OSPFv3，并将有个都配置为区域 0。

测试 GR 重启需要 2 台设备，一台为 GR 重启者，一台为 GR 帮助者。GR 测试重启者采用双主控，拔插卡的方式测试。帮助者无限制。

数据准备

CN12800_1 的两个接口地址：2001::1/64 和 2003::1/64

CN12800_2 的两个接口地址：2001::2/64 和 2004::2/64

CN12800_3 的接口地址：2003::3/64

CN12800_4 的接口地址：2004::4/64。

配置步骤

1) 拓扑同图 4-26，基本配置同 4.4.3.1 配置 OSPFv3 基本功能。

2) GR 配置

CN12800_1:

CN12800_1(config)#router ipv6 ospf

CN12800_1(config-ospfv3-1)# graceful-restart

CN12800_1(config-ospfv3-1)# graceful-restart period 60

CN12800_2:

CN12800_2(config)#router ipv6 ospf

CN12800_2(config-ospfv3-1)# graceful-restart helper

验证配置结果

采用插拔卡进行测试，GR 重启者和 GR 帮助者上的配置以后，将 GR 重启者的主用主控拔掉，这时设备间原有的流量应不发生中断。

4.5 BGP 配置

4.5.1 BGP 简介

4.5.1.1 产生背景

BGP 协议主要用于控制路由的传播和选择最佳路由。

BGP（Border Gateway Protocol，边界网关协议）是一种用于自治系统 AS（Autonomous System）之间的动态路由协议。早期发布的三个版本分别是 BGP-1（RFC1105）、BGP-2（RFC1163）和 BGP-3（RFC1267），当前使用的版本是 BGP-4（RFC4271）。

BGP-4 作为事实上的 Internet 外部路由协议标准，被广泛应用于 ISP（Internet Service Provider）之间。

4.5.1.2 协议特点

BGP 特性描述如下：

- BGP 是一种外部网关协议（EGP），与 OSPF、RIP 等内部网关协议（IGP）不同，其着眼点不在于发现和计算路由，而在于控制路由的传播和选择最佳路由。
- BGP 使用 TCP 作为其传输层协议（端口号 179），提高了协议的可靠性。
- BGP 支持无类别域间路由 CIDR（Classless Inter-Domain Routing）。
- 路由更新时，BGP 只发送更新的路由，大大减少了 BGP 传播路由所占用的带宽，适用于在 Internet 上传播大量的路由信息。
- BGP 路由通过携带 AS 路径信息彻底解决路由环路问题。
- BGP 提供了丰富的路由策略，能够对路由实现灵活的过滤和选择。
- BGP 易于扩展，能够适应网络新的发展。

BGP 在交换机上以下列两种方式运行：

- IBGP（Internal BGP）
- EBGP（External BGP）

当 BGP 运行于同一自治系统内部时，被称为 IBGP；当 BGP 运行于不同自治系统之间时，称为 EBGP。

4.5.1.3 基本概念

BGP-4 提供了一套新的机制支持无类域间路由。这些机制包括支持网络前缀的广播、取消 BGP 网络中“类”的概念。BGP-4 也引入机制支持路由聚合，包括 AS 路径的聚合。这些改变为建议的超网方案提供了支持。

几种主要的路由属性

- 源（Origin）属性
- AS 路径（AS_Path）属性
- 下一跳（Next_Hop）属性
- MED（Multi-Exit-Discriminator）
- 本地优先（Local_Pref）属性
- 团体（Community）属性

4.5.1.4 BGP4 技术介绍

4.5.1.4.1 BGP4 邻居

BGP 邻居又称为对等体，分为两种。如果两个交换 BGP 报文的对等体属于不同的自治系统，那么这两个对等体就是 EBGP 对等体（External BGP）。如果两个交换 BGP 报文的对等体属于同一个自治系统，那么这两个对等体就是 IBGP 对等体（Internal BGP）。一个 AS 内的不同边界路由器之间也要建立 BGP 连接，只有这样才能实现路由信息在整个 AS 内的传递。

IBGP 对等体之间不一定是物理上的直连，但必须保证逻辑上全连接。EBGP 对等体之间在绝大多数情况下是有物理上的直连链路的，但是如果实在无法实现也可以配置逻辑链接。图 4-27 显示了 BGP 邻居的例子，图中，AS100 内的 R1 和 R3 构成 IBGP 邻居，R2 和 R3 也构成 IBGP 邻居，而 AS100 的 R3 和 AS200 的 R4 构成 EBGP 邻居。

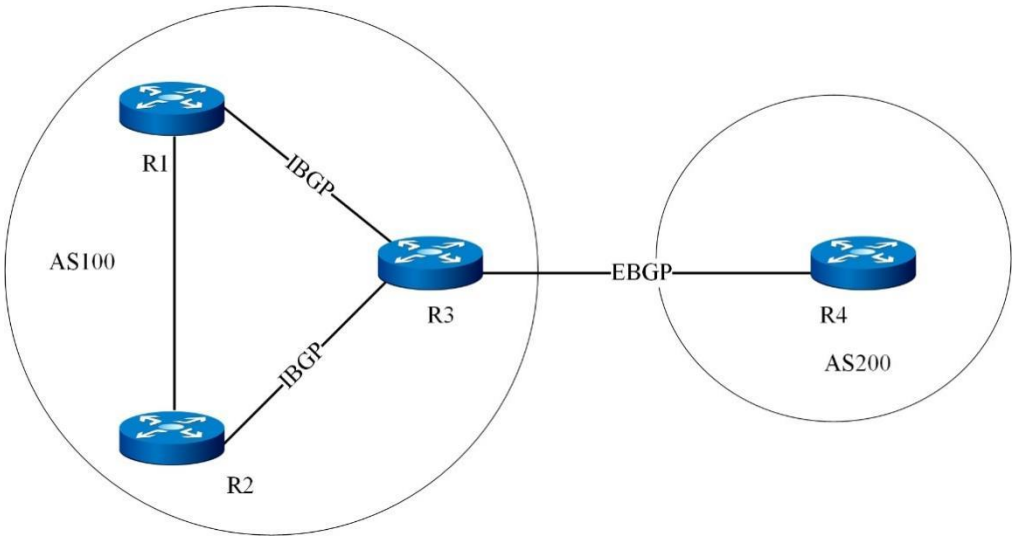


图 4-27 BGP 邻居

BGP 把从 EBGP 获得的路由向它所有的 BGP 对等体通告，包括 IBGP 和 EBGP，而把从 IBGP 获得的路由不向它的 IBGP 对等体通告，向 EBGP 通告时要保证 IGP 同 BGP 同步。同步是指 BGP 一直要等到 IGP 在本 AS 中传播了同一条路由后，再给其它各 AS 通告这条路由。也就是说在通告给其它 AS 一条路由时先要保证本 AS 内部的路由器要知道该路由。

4.5.1.4.2 BGP4 路由通告

一条路由在一般情况下是从 AS 内部产生的，它由某种内部路由协议发现和计算传递到自治系统的边界，由自治系统边界路由器器（ASBR）通过 EBGP 连接传播到其它自治系统中。

路由在传播过程中可能会经过若干个自治系统，这些自治系统称为过渡自治系统。若这个自治系统有多个边界路由器，这些路由器之间运行 IBGP 来交换路由信息。这时内部的路由器并不需要知道这些外部路由，它们只需要在边界路由器之间维护 IP 连通性。路由到达自治系统边界后，若内部路由器需要知道这些外部路由，ASBR 可以将路由引入内部路由协议。外部路由的数量是很大的，通常会超出内部路由器的处理能力，因此引入外部路由时一般需要过滤或聚合以减少路由的数量，极端的情况是使用默认路由。

图 4-28 显示了 BGP 选路时的步骤，我们看到 BGP 并没有计算路由，而是根据特定的策略选择路由。

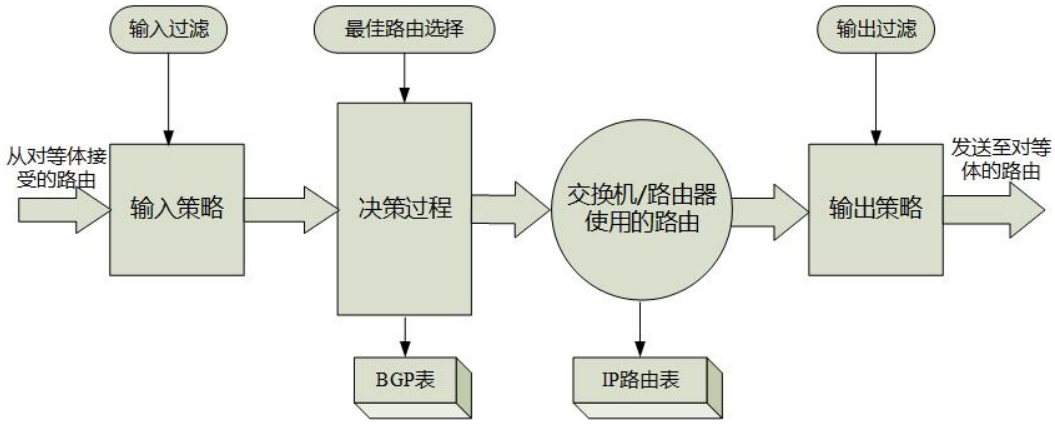


图 4-28 BGP 路由选择过程

4.5.1.4.3 BGP4 消息

BGP 协议包含以下消息：Open 消息，KeepAlive 消息，Update 消息，Notification 消息。所有消息均使用 TCP 作为传输协议。

1. Open 消息

   Open 消息是 BGP 邻居使用的 TCP 连接建立之后的第一个消息，其内容包括当前的协议版本，自治系统，路由器标识符，以及一些可选参数。如果对方对消息中的某些参数不能达成一致，则无法建立 BGP 邻居。

2. KeepAlive 消息

一旦双方对 Open 消息的内容达成一致，则开始周期性发送 KeepAlive 消息，此消息用于检测邻居的状态，一定时间内没有收到邻居发送的 KeepAlive 消息，则认为邻居发生故障。

3. Update 消息

Update 消息用于承载路由信息，包括路由的各种属性，BGP 使用这个消息向邻居通告路由信息。

4. Notification 消息

一旦 BGP 运行过程中发生了差错，就会发送 Notification 消息，消息中指明了差错的原因。

4.5.1.4.4 BGP4 属性

BGP 为路由定义了大量的属性以更详细地描述路由，在选路的过程中，BGP 需要对路由的属性作出判断，以选择符合特定策略要求的路由。

1. ORIGIN

ORIGIN 属性规定了路径信息的起源。可以取以下的值：

IGP–网络可达信息在原始自治系统的内部

EGP—通过 EGP 得到网络可达信息

INCOMLETE—通过其他方式获得网络可达信息

2. AS-PATH

AS-PATH 由自治系统路径分片组成。每个自治系统路径分片由〈路径分片类型，路径分片长度，路径分片值〉的组合体组成。路径分片类型是个 1 字节长的域，具有以下规定的值：

(1) AS-SET：路由经过的一系列无序的自治系统。

(2) AS-SEQUENCE：路由经过的一系列有序的自治系统。

路径分片长度是个 1 字节长的域，包含路径分片值域中的自治系统数目。路径分片值域包含一个或更多的自治系统号，每个都封装在 2 字节长的域中。

3. NEXT-HOP

NEXT-HOP 规定了边界路由器的 IP 地址，该地址被用做寻路时下一跳的 IP 地址。

4. MULTI-EXIT-DISC

一个四比特的非 0 整数。BGP 发起者执行决策处理来区别到邻居自治系统的多路径时用到该特性的值。

5. LOCAL-PREF

   一个四比特非 0 整数。BGP 参与者用它来通知自治系统中的其它 BGP 参与者。

6. ATOMIC-AGGREGATE

   BGP 参与者用它通知其它 BGP 参与者本地系统选择了一个相对不明确的路由而不是比较明确的路由。

7. AGGREGATOR

   包含形成聚合路由的最后一个自治系统号（用两字节封装），跟在后面的是形成聚合路由的 BGP 参与者的 IP 地址。（用四字节封装）。

4.5.1.4.5 BGP4 选择路由策略

1. 优选本地优先级（Local_Pref）最高的路由；
2. 优选聚合路由（聚合路由优先级高于非聚合路由）；
3. 优选 AS 路径（AS_Path）最短的路由；
4. 比较 Origin 属性，依次选择 Origin 类型为 IGP、EGP、Incomplete 的路由；
5. 优选 MED 值最低的路由；
6. 优选从 EBGP 学来的路由（EBGP 路由优先级高于 IBGP 路由）；
7. 优选 AS 内部 IGP 的 Metric 最低的路由；
8. 优选 Router ID 最小的交换机发布的路由；
9. 比较对等体的 IP Address，优选从具有较小 IP Address 的对等体学来的路由。

4.5.1.4.6 BGP4 发布路由策略

1. 存在多条活跃路由时，BGP 发言者（BGP Speaker）只将最优路由发布给对等体；
2. BGP 发言者只把自己使用的路由发布给对等体；
3. BGP 发言者从 EBGP 获得的路由会向它所有 BGP 对等体发布，但不会向通告该路由的对等体发布（包括 EBGP 对等体和 IBGP 对等体）；
4. BGP 发言者从 IBGP 获得的路由不向它的 IBGP 对等体发布；

5. BGP 发言者从 IBGP 获得的路由发布给它的 EBGP 对等体（在不使能 BGP 与 IGP 同步特性的情况下）；

6. 连接一旦建立，BGP 发言者将把自己所有 BGP 路由发布给新对等体。

4.5.1.4.7 BGP4 路由聚合

在大规模的网络中，BGP 路由表十分庞大，使用路由聚合（Routes Aggregation）可以大大减小路由表的规模。

路由聚合实际上是将多条路由合并的过程。这样 BGP 在向对等体通告路由时，可以只通告聚合后的路由，而不是将所有的具体路由都通告出去。

4.5.1.4.8 BGP4 的 IBGP 和 IGP 同步

同步是指 IBGP 和 IGP 之间的同步，其目的是为了避免出现误导外部 AS 路由器的现象。

如果设置了同步特性，在 IBGP 路由加入路由表并发布给 EBGP 对等体之前，会先检查 IGP 路由表。只有在 IGP 也知道这条 IBGP 路由时，它才会被加入到路由表，并发布给 EBGP 对等体。

在下面的情况中，可以安全地关闭同步特性。

- 本 AS 不是过渡 AS
- 本 AS 内所有交换机建立 IBGP 全连接

4.5.1.4.9 BGP4 团体

对等体组可以使一组对等体共享相同的策略，而利用团体可以使多个 AS 中的一组 BGP 路由器共享相同的策略。团体是一个路由属性，在 BGP 对等体之间传播，它并不受到 AS 范围的限制。

BGP 路由器在将带有团体属性的路由发布给其它对等体之前，可以改变此路由原有的团体属性。

除了使用公认的团体属性外，用户还可以使用团体属性过滤器过滤自定义扩展团体属性，以便更为灵活的控制路由策略。

4.5.1.4.10 BGP4 路由反射器

为保证 IBGP 对等体之间的连通性，需要在 IBGP 对等体之间建立全连接关系。假设在一个 AS 内部有 n 台交换机，那么应该建立的 IBGP 连接数就为 n(n-1)/2。当 IBGP 对等体数目很多时，对网络资源和 CPU 资源的消耗都很大。

利用路由反射可以解决这一问题。在一个 AS 内，其中一台交换机作为路由反射器 RR（Route Reflector），其它交换机作为客户机（Client）与路由反射器之间建立 IBGP 连接。路由反射器在客户机之间传递（反射）路由信息，而客户机之间不需要建立 BGP 连接。

既不是反射器也不是客户机的 BGP 路由器被称为非客户机（Non-Client）。非客户机与路由反射器之间，以及所有的非客户机之间仍然必须建立全连接关系。

4.5.1.4.11 BGP4 联盟

联盟（Confederation）是处理 AS 内部的 IBGP 网络连接激增的另一种方法，它将一个自治系统划分为若干个子自治系统，每个子自治系统内部的 IBGP 对等体建立全连接关系，子自治系统之间建立 EBGP 连接关系。

在不属于联盟的 BGP 发言者看来，属于同一个联盟的多个子自治系统是一个整体，外界不需要了解内部的子自治系统情况，联盟 ID 就是标识联盟这一整体的自治系统号。

联盟的缺陷是：从非联盟向联盟方案转变时，要求交换机重新进行配置，逻辑拓扑也要改变。

在大型 BGP 网络中，路由反射器和联盟可以被同时使用。

4.5.1.4.12 BGP4 的 MP-BGP

传统的 BGP-4 只能管理 IPv4 的路由信息，对于使用其它网络层协议的应用，在跨自治系统传播时就受到一定限制。

为了提供对多种网络层协议的支持，IETF 对 BGP-4 进行了扩展，形成 MP-BGP，目前的 MP-BGP 标准是 RFC2858（Multiprotocol Extensions for BGP-4，BGP-4 的多协议扩展）。

MP-BGP 前向兼容，即支持 BGP 扩展的交换机与不支持 BGP 扩展的交换机可以互通。

1. MP-BGP 的扩展属性

   BGP-4 使用的报文中，与 IPv4 相关的三条信息都由 Update 报文携带，这三条信息分别是：NLRI、路径属性中的 Next_Hop、路径属性中的 Aggregator（该属性中包含形成聚合路由的 BGP 发言者的 IP 地址）。

   为实现对多种网络层协议的支持，BGP-4 需要将网络层协议的信息反映到 NLRI 及 Next_Hop。MP-BGP 中引入了两个新的路径属性：

   MP_REACH_NLRI：Multiprotocol Reachable NLRI，多协议可达 NLRI。用于发布可达路由及下一跳信息。

MP_UNREACH_NLRI：Multiprotocol Unreachable NLRI，多协议不可达 NLRI。用于撤销不可达路由。

这两种属性都是可选非过渡（Optional non-transitive）的，因此，不提供多协议能力的 BGP 发言者将忽略这两个属性的信息，不把它们传递给其它邻居。

2. 地址族

BGP 采用地址族（Address Family）来区分不同的网络层协议，关于地址族的一些取值可以参考 RFC1700（Assigned Numbers）。MP-BGP 扩展应用，包括对 VPN 的扩展，不同的扩展应在各自的地址族视图下配置。

4.5.1.4.13 BFD for BGP 特性

在 IPv4 中使用 BFD（Bidirectional Forwarding Detection）为 BGP 协议提供更快速的链路故障检测。

BFD 能够快速检测到 BGP 对等体间的链路故障，并报告给 BGP 协议，从而实现 BGP 路由的快速收敛。

4.5.1.4.14 BGP GR

当 BGP 协议重启时会导致对等体关系重新建立和转发中断，使能平滑重启 GR（Graceful Restart）功能后可以避免流量中断。

4.5.2 BGP 配置

4.5.2.1 配置 BGP4 的基本功能

目的

本节介绍如何配置 BGP4 的基本功能。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
进入或创建 BGP 节点	1. 进入全局配置视图； 2. 执行命令 **router bgp** *as-value*，进入 BGP 配置视图。
指定 BGP 的 router id	1. 进入全局配置视图； 2. 进入 BGP 配置视图； 3. 执行命令 **router-id** *router-id*。

目的	步骤
恢复 BGP 的 router id 为默认值	1. 进入全局配置视图； 2. 进入 BGP 配置视图； 3. 执行命令 **no router-id**。
创建 BGP 邻居	1. 进入全局配置视图； 2. 进入 BGP 配置视图、BGP-VPN IPv4 地址族配置视图； 3. 执行命令 **neighbor** *ipv4-address* **remote-as** *AS-value*。
删除 BGP 邻居	1. 进入全局配置视图； 2.进入 BGP 配置视图、BGP-VPN IPv4 地址族配置视图； 3. 执行命令 **no neighbor** *ipv4-address*。
关闭 BGP 邻居	1. 进入全局配置视图； 2. 执行命令 **router bgp** *as-value*，进入 BGP 配置视图、BGP-VPN IPv4 地址族配置视图； 3. 执行命令 **neighbor** *ipv4-address* **shutdown**。
删除关闭 BGP 邻居	1. 进入全局配置视图； 2. 进入 BGP 配置视图、BGP-VPN IPv4 地址族配置视图； 3. 执行命令 **no neighbor** *ipv4-address* **shutdown**。
配置邻居的 MD5 验证	1. 进入全局配置视图； 2. 进入 BGP 配置视图、BGP-VPN IPv4 地址族配置视图； 3. 执行命令 **neighbor** *ipv4-address* **password** *password*。
删除邻居的 MD5 验证	1. 进入全局配置视图； 2. 进入 BGP 配置视图、BGP-VPN IPv4 地址族配置视图； 3. 执行命令 **no neighbor** *ipv4-address* **password**。
配置邻居的最大保持时间和向邻居发送 keeplive 的间隔	1. 进入全局配置视图； 2. 进入 BGP 配置视图、BGP-VPN IPv4 地址族配置视图； 3. 执行命令 **neighbor** *ipv4-address* **keeplive-timer** { *keeplive-timer* | **default** } **hold-timer** { *hold-timer* | **default** }。
指定邻居的更新源地址	1. 进入全局配置视图； 2. 进入 BGP 配置视图、BGP-VPN 地址族视图； 3. 执行命令 **neighbor** *ip-address1* **update-source** *ip-address2*。
删除邻居的更新源地址	1. 进入全局配置视图； 2. 进入 BGP 配置视图、BGP-VPN 地址族视图； 3. 执行命令 **no neighbor** *ip-address1* **update-source**。
检测邻居的有效 ttl 跳数	1. 进入全局配置视图； 2. 进入 BGP 配置视图、BGP-VPN IPv4 地址族配置视图； 3. 执行命令 **neighbor** *ipv4-address* **valid-ttl-hops** { *hops-value* | **default** }。

4.5.2.2 配置 BGP4 的路由的发布

目的

本节介绍如何配置 BGP4 的路由的发布。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
配置路由聚合，并指定是只发送聚合后的路由或是聚合后的和未聚合的都发送	1. 进入全局配置视图； 2. 进入 BGP 配置视图、BGP-VPN IPv4 地址族配置视图； 3. 执行命令 **aggregate** *ipv4-address ipv4mask-length* { **summaryonly** | **all** }。
配置管理路由聚合的状态，使能或关闭	1. 进入全局配置视图； 2. 进入 BGP 配置视图； 3. 执行命令 **aggregate** *ipv4-address ipv4mask-length* **adminstatus** { **up** | **down** }。
删除路由聚合	1. 进入全局配置视图； 2. 进入 BGP 配置视图、BGP-VPN IPv4 地址族配置视图； 3. 执行命令 **no aggregate** *ipv4-address ipv4mask-length*。
将发送给邻居路由的下一跳更改为本地地址	1. 进入全局配置视图； 2. 进入 BGP 配置视图、BGP-VPN IPv4 地址族配置视图； 3. 执行命令 **neighbor** *ipv4-address* **next-hop-local**。
删除将发送给邻居路由的下一跳更改为本地地址的配置	1. 进入全局配置视图； 2. 进入 BGP 配置视图、BGP-VPN IPv4 地址族配置视图； 3. 执行命令 **no neighbor** *ipv4-address* **next-hop-local**。
配置邻居的路由刷新能力	1. 进入全局配置视图； 2. 进入 BGP 配置视图、BGP-VPN IPv4 地址族配置视图； 3. 执行命令 **neighbor** *ipv4-address* **route-refresh**。
删除邻居的路由刷新能力	1. 进入全局配置视图； 2. 进入 BGP 配置视图、BGP-VPN IPv4 地址族配置视图； 3. 执行命令 **no neighbor** *ipv4-address* **route-refresh**。
发布指定的路由	1. 进入全局配置视图； 2. 进入 BGP 配置视图、BGP-VPN IPv4 地址族配置视图； 3. 执行命令 **network** *network-address network-mask*。
删除发布的指定路由	1. 进入全局配置视图； 2. 进入 BGP 配置视图、BGP-VPN IPv4 地址族配置视图； 3. 执行命令 **no network** *network-address network-mask*。
向 BGP 引入静态或直连路由	1. 进入全局配置视图； 2. 进入 BGP 配置视图；

目的	步骤
	3. 执行命令 **redistribute** { **static** | **connected** | **ospf** | **isis** }。
根据策略向 BGP 引入静态或直连路由	1. 进入全局配置视图； 2. 进入 BGP 配置视图； 3. 执行命令 **redistribute** { **static** | **connected** | **ospf** | **isis** } **route-policy** *route-policy-name*。
修改向 BGP 引入静态或直连路由的 med 值	1. 进入全局配置视图； 2. 进入 BGP 配置视图； 3. 执行命令 **redistribute** { **static** | **connected** | **ospf** | **isis** } **med** *med-value*。
删除向 BGP 引入路由	1. 进入全局配置视图； 2. 进入 BGP 配置视图； 3. 执行命令 **no redistribute** { **static** | **connected** | **ospf** | **isis** }。
删除根据策略向 BGP 引入路由	1. 进入全局配置视图； 2. 进入 BGP 配置视图； 3. 执行命令 **no redistribute** { **static** | **connected** | **ospf** | **isis** } **route-policy** *route-policy-name*。
使能或去使能 IGP 同步功能	1. 进入全局配置视图； 2. 进入 BGP 配置视图； 3. 执行命令 **synchronization** { **enable** | **disable** }。

4.5.2.3 配置 BGP4 的路径属性

目的

本节介绍如何配置 BGP4 的路径属性。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
配置默认 med 值	1. 进入全局配置视图； 2. 进入 BGP 配置视图； 3. 执行命令 **default local-med** { *local-med* | **default** }。
配置默认 local-preference 值	1. 进入全局配置视图； 2. 进入 BGP 配置视图； 3. 执行命令 **default local-preference** { *local-preference-value* | **default** }。
配置 BGP 的团体属性	1. 进入全局配置视图； 2. 进入 BGP 配置视图；

目的	步骤
	3. 执行命令 **community** { *community-value* | **noadvertise** | **noexport** } { **additive** | **replace** | **none** }。
删除 BGP 的团体属性	1. 进入全局配置视图； 2. 进入 BGP 配置视图； 3. 执行命令 **no community**。
向邻居发送团体属性	1. 进入全局配置视图； 2. 进入 BGP 配置视图； 3. 执行命令 **neighbor** *ipv4-address* **send-community**。
不向邻居发送团体属性	1. 进入全局配置视图； 2. 进入 BGP 配置视图； 3. 执行命令 **no neighbor** *ipv4-address* **send-community**。
允许本地 AS 编号重复出现次数	1. 进入全局配置视图； 2. 进入 BGP 配置视图、BGP-VPN IPv4 地址族配置视图； 3. 执行命令 **neighbor** *ipv4-address* **allow-as-loop** { *time-value* | **default** }。
BGP 更新报文时不携带私有自治系统号，仅携带公有 AS 号	1. 进入全局配置视图； 2. 进入 BGP 配置视图； 3. 执行命令 **neighbor** *ipv4-address* **public-as-only**。

4.5.2.4 配置 BGP4 的路由策略

目的

本节介绍如何配置 BGP4 的路由策略。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
配置 BGP 全局入或出过滤策略	1. 进入全局配置视图； 2. 进入 BGP 配置视图、BGP-VPN IPv4 地址族配置视图； 3. 执行命令 **filter-policy** { **export** | **import** } **route-policy** *route-policy-name*。
根据协议类型指定 BGP 全局出过滤策略	1. 进入全局配置视图； 2. 进入 BGP 配置视图、BGP-VPN IPv4 地址族配置视图； 3. 执行命令 **filter-policy export** { **static** | **connected** | **rip** | **ospf** | **isis** } **route-policy** *route-policy-name*。
删除 BGP 全局入或出过滤策略	1. 进入全局配置视图； 2. 进入 BGP 配置视图、BGP-VPN IPv4 地址族配置视图； 3. 执行命令 **no filter-policy** { **export** | **import** } **route-policy** *route-policy-name*。

目的	步骤
删除根据协议类型指定的 BGP 全局出过滤策略	1. 进入全局配置视图； 2. 进入 BGP 配置视图、BGP-VPN IPv4 地址族配置视图； 3. 执行命令 **no filter-policy export** { **static** | **connected** | **rip** | **ospf** | **isis** } **route-policy** *route-policy-name*。
针对指定邻居配置入或出路由策略	1. 进入全局配置视图； 2. 进入 BGP 配置视图； 3. 执行命令 **neighbor** *ipv4-address* **route-policy** *route-policy-name* { **export** | **import** }。
删除针对指定邻居的入或出路由策略	1. 进入全局配置视图； 2. 进入 BGP 配置视图； 3. 执行命令 **no neighbor** *ipv4-address* **route-policy** *route-policy-name* { **export** | **import** }。

4.5.2.5 配置 BFD for BGP

目的

本节介绍如何配置 BFD for BGP。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
针对邻居使能或去使能 BFD 功能	1. 进入全局配置视图； 2. 进入 BGP 配置视图、BGP-VPN IPv4 地址族配置视图； 3. 执行命令 **neighbor** *ipv4-address* **bfd** { **enable** | **disable** }。

4.5.2.6 配置 BGP4 路由反射器

目的

本节介绍如何配置 BGP4 路由反射器。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
配置路由反射器的簇 id	1. 进入全局配置视图； 2. 进入 BGP-ipv4 地址族配置视图、BGP 配置视图、BGP-EVPN 地址族配置视图、BGP-VPN IPv4 地址族配置视图、BGP-VPN IPv6 地址族配置视图；

目的	步骤
	3. 执行命令 **cluster-id** *router-id*。
指定邻居作为反射器的客户端	1. 进入全局配置视图； 2. 进入 BGP 配置视图、BGP-VPN IPv4 地址族配置视图； 3. 执行命令 **neighbor** *ipv4-address* **route-reflector-client**。
删除路由反射器的簇 id	1. 进入全局配置视图； 2. 进入 BGP-ipv4 地址族配置视图、BGP 配置视图、BGP-EVPN 地址族配置视图、BGP-VPN IPv4 地址族配置视图、BGP-VPN IPv6 地址族配置视图； 3. 执行命令 **no cluster-id**。
删除邻居作为反射器的客户端	1. 进入全局配置视图； 2. 进入 BGP 配置视图、BGP-VPN IPv4 地址族配置视图； 3. 执行命令 **no neighbor** *ipv4-address* **route-reflector-client**。

4.5.2.7 配置 BGP4 联盟

目的

本节介绍如何配置 BGP4 联盟。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
配置联盟的 AS 号	1. 进入全局配置视图； 2. 进入 BGP 配置视图； 3. 执行命令 **confederation identifier** { *autonomy-system-number* | *string* }。
指定联盟成员	1. 进入全局配置视图； 2. 进入 BGP 配置视图 3. 执行命令 **confederation peer-as** *autonomy-system-number*。
删除联盟的 AS 号	1. 进入全局配置视图； 2. 进入 BGP 配置视图； 3. 执行命令 **no confederation identifier**。
删除指定联盟成员	1. 进入全局配置视图； 2. 进入 BGP 配置视图； 3. 执行命令 **no confederation peer-as** *autonomy-system-number*。

4.5.2.8 配置 BGP4 GR

目的

本节介绍如何配置 BGP4 GR。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

4.5.2.9 配置 BGP 的地址族

目的

本节介绍如何配置 BGP 的地址族。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
进入 ipv4 单播地址族视图	1. 进入全局配置视图； 2. 进入 BGP 配置视图； 3. 执行命令 **ipv4-family unicast**。
将指定的 VPN 实例与 IPv4 地址族进行关联，进入 BGP-VPN 实例视图	1. 进入全局配置视图； 2. 进入 BGP 配置视图； 3. 执行命令 **ipv4-family vpn-instance** *name*。
地址族节点下使能或去使能地址组	1. 进入全局配置视图； 2. 进入 BGP 配置视图； 3. 进入地址族视图； 4. 执行命令 **neighbor** *ipv4-address* { **enable** | **disable** }。

4.5.2.10 查看 BGP4 配置信息

目的

本节介绍如何查看 BGP4 配置信息。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
显示 BGP 的聚合表	1. 进入普通用户视图、BGP 配置视图、特权用户视图、全局配置视图、BGP 地址族配置视图、BGP-VPN IPv4 地址族配置视图； 2. 执行命令 **show ip bgp aggregate**。
显示 BGP 的基本配置	1. 进入普通用户视图、BGP 配置视图、特权用户视图、全局配置视图、BGP 地址族配置视图、BGP-VPN IPv4 地址族配置视图； 2. 执行命令 **show ip bgp config**。
显示 BGP 的所有对等体	1. 进入普通用户视图、BGP 配置视图、特权用户视图、全局配置视图、BGP 地址族配置视图、BGP-VPN IPv4 地址族配置视图； 2. 执行命令 **show ip bgp neighbor**。
显示 BGP 指定对等体的状态	1. 进入普通用户视图、BGP 配置视图、特权用户视图、全局配置视图、BGP 地址族配置视图、BGP-VPN IPv4 地址族配置视图； 2. 执行如下命令： ● **show ip bgp neighbor** *ipv4-address* ● **show ip bgp neighbor orf state** ● **show ip bgp neighbor** *ipv4-address* **error-statistic**。
显示 BGP 的资源统计信息	1. 进入普通用户视图、BGP 配置视图、特权用户视图、全局配置视图、BGP 地址族配置视图、BGP-VPN IPv4 地址族配置视图； 2. 执行命令 **show ip bgp resource**。
显示 BGP 的路由表	1. 进入普通用户视图、BGP 配置视图、特权用户视图、全局配置视图、BGP 地址族配置视图、BGP-VPN IPv4 地址族配置视图； 2. 执行命令 **show ip bgp route**。
显示 BGP 的路由统计信息	1. 进入普通用户视图、BGP 配置视图、特权用户视图、全局配置视图、BGP 地址族配置视图、BGP-VPN IPv4 地址族配置视图； 2. 执行命令 **show ip bgp summary**。
显示 BGP 的 VPN 实例的对等体	1. 进入普通用户视图或特权用户视图； 2. 执行命令 **show ip bgp vpn-instance** *name* **neighbor**。
显示在 BGP 进程中产生的各	1. 进入全局配置视图； 2. 执行命令 **show ip bgp error-statistic**。

目的	步骤
项错误次数统计结果	

4.5.2.11 查看 BGP6 配置信息

目的

本节介绍如何查看 BGP6 配置信息。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
显示 IPv6 BGP 邻居的错误统计信息	1. 进入普通用户视图； 2. 执行命令 **show ipv6 bgp neighbor** *ipv6-address* **error-statistic**。
显示 IPv6 BGP 的路由信息	1. 进入普通用户视图； 2. 执行命令 **show ipv6 bgp route**。

4.5.2.12 维护及调试

目的

当 BGP 功能不正常，需要进行查看、定位问题时，可以使用本小节操作。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

4.5.3 BGP 配置举例

4.5.3.1 配置基本 BGP4

组网要求

如图 4-29 所示，所有 CN12800 均运行 BGP 协议，R1、R2 之间建立 EBGP 连接，R2、R3 和 R4 之间建立 IBGP 全连接。

组网图

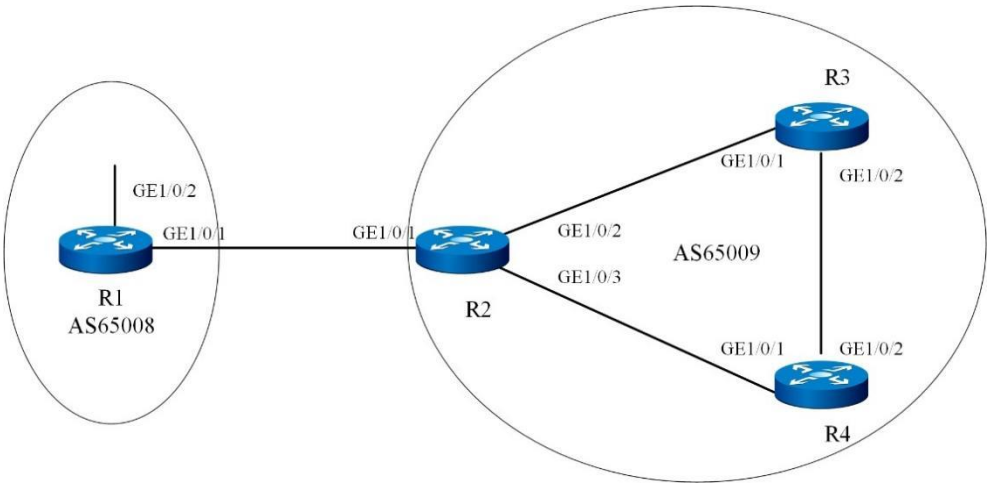


图 4-29 配置 BGP 基本组网图

Switch	接口	对应的 VLAN	IP 地址
R1	Gigaethernet1/0/1	VLAN 10	192.1.1.2/24
R1	Gigaethernet1/0/2	VLAN 50	20.1.1.1/8
R2	Gigaethernet1/0/1	VLAN 10	192.1.1.1/24
R2	Gigaethernet1/0/2	VLAN 20	10.1.3.1/24
R2	Gigaethernet1/0/3	VLAN 30	10.1.1.1/24
R3	Gigaethernet1/0/1	VLAN 20	10.1.3.2/24
R3	Gigaethernet1/0/2	VLAN 40	10.1.2.1/24
R4	Gigaethernet1/0/1	VLAN 30	10.1.1.2/24
R4	Gigaethernet1/0/2	VLAN 40	10.1.2.2/24

配置思路

采用如下的思路配置 BGP 的基本功能：

1. 在 R2、R3 和 R4 间配置 IBGP 连接。

2. 在 R1 和 R2 之间配置 EBGP 连接。

3. 在 R1 通过 network 命令发布路由，查看 R1、R2 和 R3 路由表信息。

4. 在 R2 配置 BGP 引入直连路由，查看 R1 和 R3 路由表信息。

数据准备

为完成此配置例，需准备如下的数据：

各接口所属的 VLAN ID，具体数据如图 4-29 所示。

各 VLAN 接口的 IP 地址，具体数据如图 4-29 所示。

R1 的 Router ID 1.1.1.1，所在的 AS 号 65008。

R2、R3 和 R4 的 router id 分别为 2.2.2.2、3.3.3.3、4.4.4.4，所在的 AS 号 65009。

配置步骤

步骤 1 配置 IBGP 连接

配置 R2。

R2(config)#router bgp 65009

R2(config-bgp)#router-id 2.2.2.2

R2(config-bgp)#neighbor 10.1.1.2 remote-as 65009

R2(config-bgp)#neighbor 10.1.3.2 remote-as 65009

配置 R3。

R3(config)#router bgp 65009

R3(config-bgp)#router-id 3.3.3.3

R3(config-bgp)#neighbor 10.1.3.1 remote-as 65009

R3(config-bgp)#neighbor 10.1.2.2 remote-as 65009

R3(config-bgp)#quit

配置 R4。

R4(config)#router bgp 65009

R4(config-bgp)#router-id 4.4.4.4

R4(config-bgp)#neighbor 10.1.1.1 remote-as 65009

R4(config-bgp)#neighbor 10.1.2.1 remote-as 65009

R4(config-bgp)#quit

步骤 2 配置 EBGP

配置 R1。

R1(config)# router bgp 65008

R1(config-bgp)#router-id 1.1.1.1

R1(config-bgp)#neighbor 192.1.1.1 remote-as 65009

配置 R2。

R2(config-bgp)#neighbor 192.1.1.2 remote-as 65008

R2(config-bgp)#quit

查看 BGP 对等体的连接状态。

R1(config)#show ip bgp neighbor

步骤 3 配置 R1 发布路由 20.0.0.0/8

配置 R1 发布路由。

R1(config-bgp)#network 20.0.0.0 255.0.0.0

R1(config-bgp)#quit

查看 R1 路由表信息。

R1(config)#show ip bgp route

查看 R2 的路由表。

R2(config)#show ip bgp route

查看 R3 的路由表。

R1(config)#show ip bgp route

从路由表可以看出，R3 然学到了 AS65008 中的 20.0.0.0 的路由，但因为下一跳 192.1.1.2 不可达，所以也不是有效路由。

步骤 4 配置 BGP 引入直连路由

配置 R2。

R2(config)#router bgp 65009

R2(config-bgp)#redistribute connect

R2(config-bgp)#quit

查看 R1 的 BGP 路由表。

R1(config)#show ip bgp route

查看 R3 的路由表。

R3(config)#show ip bgp route

可以看出，到 20.0.0.0 的路由变为有效路由，下一跳为 R1 的地址。

4.5.3.2 配置 BGP4 与 IGP 交互

组网要求

如图 4-30 所示，在 AS65009 内使用 OSPF 作为 IGP 协议，R1 和 R2 建立 EBGP 连接，R3 运行 OSPF 而不运行 BGP。

组网图

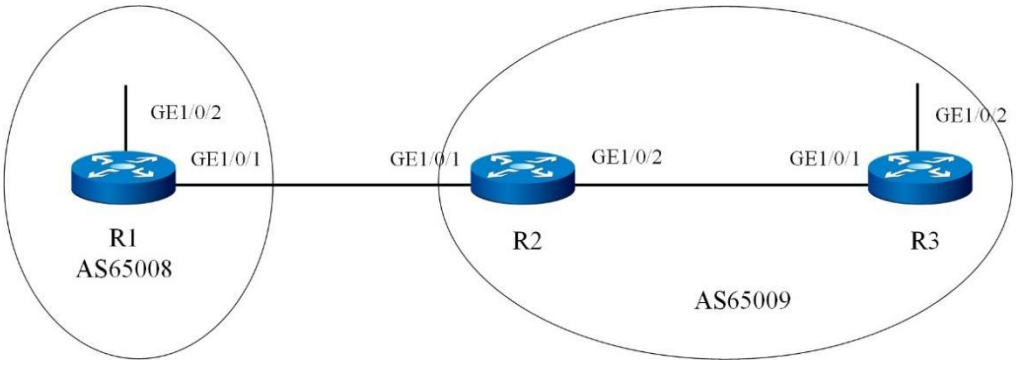


图 4-30 BGP 与 IGP 交互配置组网图

Switch	接口	对应的 VLAN	IP 地址
R1	Gigaethernet1/0/1	VLAN 10	30.1.1.2/24
R1	Gigaethernet1/0/2	VLAN 30	20.1.1.1/24
R2	Gigaethernet1/0/1	VLAN 10	30.1.1.1/24

R2	Gigaethernet1/0/2	VLAN 20	10.1.1.1/24
R3	Gigaethernet1/0/1	VLAN 20	10.1.1.2/24
R3	Gigaethernet1/0/2	VLAN 40	10.1.2.1/24

配置思路

采用如下的思路配置 BGP 与 IGP 交互：

1. 在 R2 和 R3 上配置 OSPF 协议。

2. 在 R1 和 R2 上配置 EBGP 连接。

3. 在 R2 配置 BGP 与 OSPF 互相引入，查看路由信息。

4. 在 R2 配置 BGP 路由聚合，简化 BGP 路由表。

数据准备

为完成此配置例，需准备如下的数据：

各接口所属的 VLAN ID，具体数据如图 4-30 所示。

各 VLAN 接口的 IP 地址，具体数据如图 4-30 所示。

R1 的 Router ID 1.1.1.1，所在 AS 号 65008。

R2、R3 的 Router ID 分别为 2.2.2.2、3.3.3.3，所在 AS 号 65009。

配置步骤

步骤 1 配置 OSPF

配置 R1。

```
R1(config)#router ospf
R1(config-ospf-1)#network 9.1.1.0 255.255.255.0 area 0
R1(config-ospf-1)#quit
```

配置 R2。

```
R1(config)#router ospf
R1(config-ospf-1)#network 9.1.1.0 255.255.255.0 area 0
R1(config-ospf-1)#network 9.1.2.0 255.255.255.0 area 0
R1(config-ospf-1)#quit
```

步骤 2 配置 EBGP 连接

配置 R1。

R1(config)#router bgp 65008

R1(config-bgp)#router-id 1.1.1.1

R1(config-bgp)#neighbor 3.1.1.1 remote-as 65009

R1(config-bgp)#network 8.1.1.0 255.255.255.0

R1(config-bgp)#quit

配置 R2。

R2(config)#router bgp 65009

R2(config-bgp)#router-id 2.2.2.2

R2(config-bgp)#neighbor 3.1.1.2 remote-as 65008

步骤 3 配置 BGP 与 IGP 交互

在 R2 配置 BGP 引入 OSPF 路由。

R2(config-bgp)#redistribute ospf

R2(config-bgp)#quit

查看 R1 的路由表。

R1(config)#show ip bgp route

在 R2 配置 OSPF 引入 BGP 路由。

R2(config)#router ospf

R2(config-ospf-1)#redistribute bgp

R2(config-ospf-1)#quit

查看 R3 的路由表。

R3(config)#show ip route

步骤 4 配置路由聚合

配置 R2。

R2(config)#router bgp 65009

R2(config-bgp)#aggregate 9.0.0.0 8 summaryonly

R2(config-bgp)#aggregate 9.0.0.0 8 adminstatus up

R2(config-bgp)#quit

查看 R1 的 BGP 路由表。

R1(config)#show ip bgp route

4.5.3.3 配置 BGP4 路由反射器

组网要求

如图 4-31 所示，R1 为非客户机，R2 是 Cluster1 的路由反射器，R4 和 R5 是它的两个客户机。由于他们两者之间建立了 IBGP 连接，所以不需要在客户机之间反射路由。R3 为 Cluster2 的路由反射器，R6、R7 和 R8 是它的客户机。要求使用对等体组来简化配置和管理。

组网图

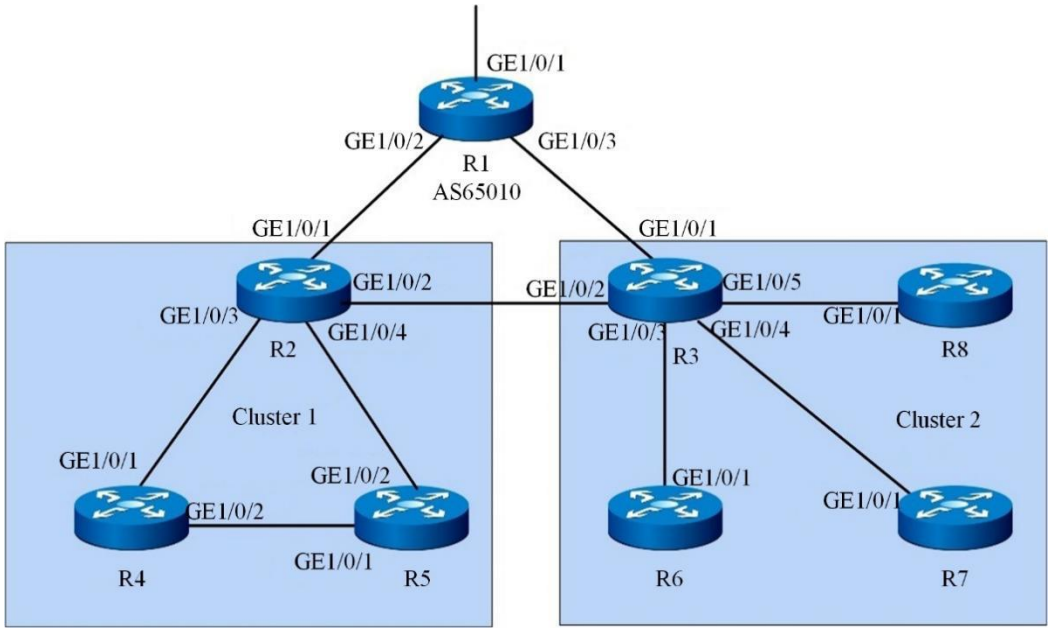


图 4-31 配置 BGP 路由反射器组网图

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

配置思路

采用如下的思路配置 BGP 路由反射器：

1. 配置客户机与路由反射器之间，非客户机与路由反射器之间建立 IBGP 连接。

2. 在 R2 和 R3 上配置路由反射器功能，指定客户机，查看路由信息。

数据准备

为完成此配置例，需准备如下的数据：

各接口所属的 VLAN ID，具体数据如图 4-31 所示。

各 VLANIF 接口的 IP 地址，具体数据如图 4-31 所示。

所有交换机的自治系统号为 AS10。

R1、R2、R3、R4、R5、R6、R7、R8 的 Router ID 分别为 1.1.1.1、2.2.2.2、3.3.3.3、4.4.4.4、5.5.5.5、6.6.6.6、7.7.7.7、8.8.8.8。

R2 所在集群的 Cluster-id 为 1，R3 在集群的 Cluster-id 为 2。

配置步骤

步骤 1 配置客户机、非客户机与路由反射器之间的 IBGP 连接（略）。

步骤 2 配置 R1 发布的本地网络路由 9.1.1.0/24（略）。

步骤 3 配置路由反射器。

配置 R2。

R2(config)#router bgp 65010

R2(config-bgp)#router-id 2.2.2.2

R2(config-bgp)#neighbor 10.1.4.2 route-reflector-client

R2(config-bgp)#neighbor 10.1.5.2 route-reflector-client

R2(config-bgp)#cluster-id 10.10.10.10

R2(config-bgp)#quit

配置 R3。

R3(config)#router bgp 65010

R3(config-bgp)#router-id 3.3.3.3

R3(config-bgp)#neighbor 10.1.7.2 route-reflector-client

R3(config-bgp)#neighbor 10.1.8.2 route-reflector-client

R3(config-bgp)#neighbor 10.1.9.2 route-reflector-client

R3(config-bgp)#cluster-id 20.20.20.20

R3(config-bgp)#quit

查看 R4 的路由表。

R4(config)#show ip bgp route

4.5.3.4 配置 BGP4 联盟

组网要求

如图 4-32 所示，网络中中有多台设备运行 BGP，为了减少 IBGP 的连接数，现将他们划分为 3 个子自治系：AS65001、AS65002 和 AS65003。其中 AS65001 内的三台设备建立 IBGP 全连接。

组网图

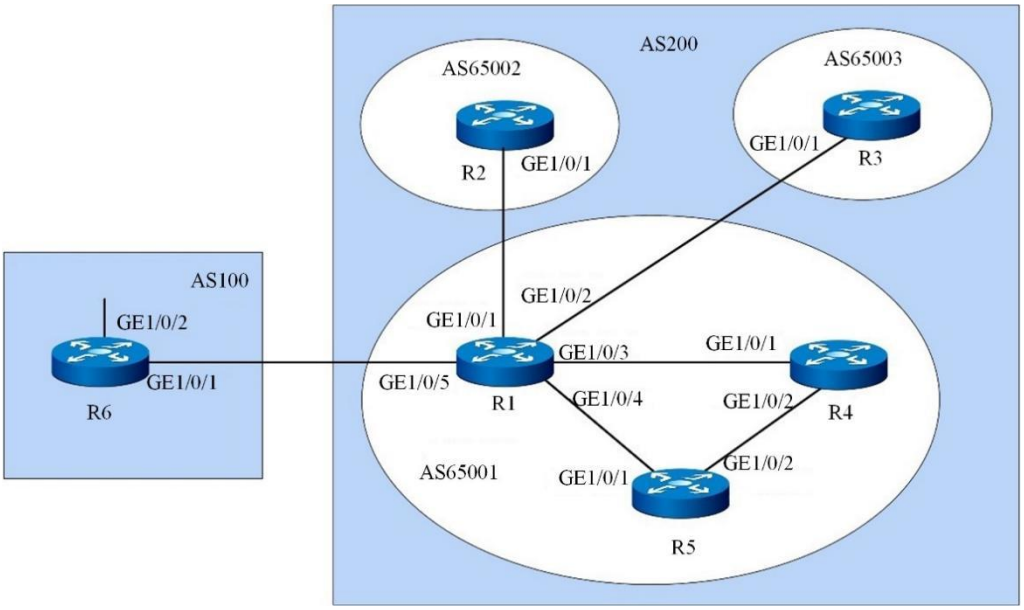


图 4-32 配置联盟组网图

Switch	接口	对应的 VLAN	IP 地址
R1	Gigaethernet 1/0/1	VLAN 10	10.1.1.1/24
R1	Gigaethernet 1/0/2	VLAN 20	10.1.2.1/24
R1	Gigaethernet 1/0/3	VLAN 30	10.1.3.1/24
R1	Gigaethernet 1/0/4	VLAN 40	10.1.4.1/24
R1	Gigaethernet 1/0/5	VLAN 60	200.1.1.1/24
R2	Gigaethernet 1/0/1	VLAN 10	10.1.1.2/24
R3	Gigaethernet 1/0/1	VLAN 20	10.1.2.2/24

R4	Gigaethernet 1/0/1	VLAN 30	10.1.3.2/24
R4	Gigaethernet 1/0/2	VLAN 50	10.1.5.1/24
R5	Gigaethernet 1/0/1	VLAN 40	10.1.4.2/24
R5	Gigaethernet 1/0/2	VLAN 50	10.1.5.2/24
R6	Gigaethernet 1/0/1	VLAN 60	200.1.1.2/24
R6	Gigaethernet 1/0/2	VLAN 70	9.1.1.1/24

配置思路

采用如下的思路配置 BGP 联盟：

1. 在 AS200 中的各 Switch 上配置 BGP 联盟。

2. 在 AS65001 中配置 IBGP 连接。

3. 在 AS100 和 AS200 之间配置 EBGP 连接，查看路由信息。

数据准备

为完成此配置例，需准备如下的数据：

各接口所属的 VLAN ID，具体数据如图 4-32 所示。

各 VLANIF 接口的 IP 地址，具体数据如图 4-32 所示。

R1、R2、R3、R4、R5、R6 的 router id 分别为 1.1.1.1、2.2.2.2、3.3.3.3、4.4.4.4、5.5.5.5、6.6.6.6。

自治系统号 AS100，自治系统号 AS200，AS200 中的 3 个子自治系统号 AS65001，AS65002，AS65003。

配置步骤

步骤 1 配置 BGP 联盟。

配置 R1。

R1(config)#router bgp 65001

R1(config-bgp)#router-id 1.1.1.1

R1(config-bgp)#confederation identifier 200

R1(config-bgp)#confederation peer-as 65002

R1(config-bgp)#confederation peer-as 65003

R1(config-bgp)#neighbor 10.1.1.2 remote-as 65002

R1(config-bgp)#neighbor 10.1.2.2 remote-as 65003

R1(config-bgp)#neighbor 10.1.1.2 next-hop-local

R1(config-bgp)#neighbor 10.1.2.2 next-hop-local

R1(config-bgp)#quit

配置 R2。

R2(config)#router bgp 65002

R2(config-bgp)#router-id 2.2.2.2

R2(config-bgp)#confederation identifier 200

R2(config-bgp)#confederation peer-as 65001

R2(config-bgp)#confederation peer-as 65003

R2(config-bgp)#neighbor 10.1.1.1 remote-as 65001

R2(config-bgp)#quit

配置 R3。

R3(config)#router bgp 65003

R3(config-bgp)#router-id 3.3.3.3

R3(config-bgp)#confederation identifier 200

R3(config-bgp)#confederation peer-as 65001

R3(config-bgp)#confederation peer-as 65002

R3(config-bgp)#neighbor 10.1.2.1 remote-as 65001

R3(config-bgp)#quit

步骤 2 配置 AS65001 内的 IBGP 连接。

配置 R1。

R1(config)#router bgp 65001

R1(config-bgp)#neighbor 10.1.3.2 remote-as 65001

R1(config-bgp)#neighbor 10.1.4.2 remote-as 65001

R1(config-bgp)#neighbor 10.1.3.2 next-hop-local

R1(config-bgp)#neighbor 10.1.4.2 next-hop-local

R1(config-bgp)#quit

配置 R4。

R4(config)#router bgp 65001

R4(config-bgp)#router-id 4.4.4.4

R4(config-bgp)#neighbor 10.1.3.1 remote-as 65001

R4(config-bgp)#neighbor 10.1.5.2 remote-as 65001

R4(config-bgp)#quit

配置 R5。

R5(config)#router bgp 65001

R5(config-bgp)#router-id 5.5.5.5

R5(config-bgp)#neighbor 10.1.4.1 remote-as 65001

R5(config-bgp)#neighbor 10.1.5.1 remote-as 65001

R5(config-bgp)#quit

步骤 3 配置 AS100 和 AS200 之间的 EBGP 连接。

配置 R1。

R1(config)#router bgp 65001

R1(config-bgp)#neighbor 200.1.1.2 remote-as 100

R1(config-bgp)#quit

配置 R6。

R6(config)#router bgp 100

R6(config-bgp)#router-id 6.6.6.6

R6(config-bgp)#neighbor 200.1.1.1 remote-as 200

R6(config-bgp)#network 9.1.1.0 255.255.255.0

R6(config-bgp)#quit

步骤 4 查看配置结果。

查看 R2 的 BGP 路由表。

R2(config)#show ip bgp route

查看 R4 的 BGP 路由表。

R4(config)#show ip bgp route

4.5.3.5 配置 BFD for BGP

组网要求

如图 4-33，R1 属于 AS100，R2 和 R3 属于 AS200，R1 和 R2，R1 和 R3 建立 EBGP 连接。业务流量在主链路 R1→R2 上传送，链路 R1→R3→R2 作为备份链路。使用 BFD 检测 R1 和 R2 之间的 BGP 邻居关系，当 R1 和 R2 之间的链路发生故障时，BFD 能够快速检测到故障并通告给 BGP 协议，使业务流量使用备份链路传送。

组网图

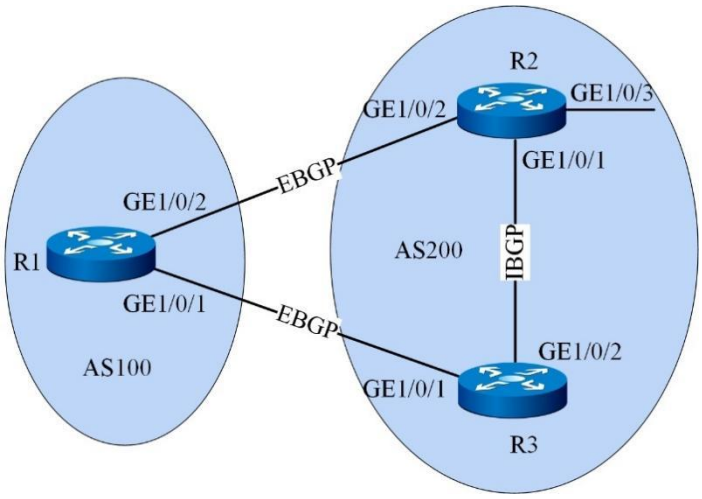


图 4-33 配置 BFD for BGP 组网图

Switch	接口	对应的 VLAN	IP 地址
R1	Gigaethernet 1/0/1	VLAN 10	200.1.2.1/24

R1	Gigaethernet 1/0/2	VLAN 20	200.1.1.1/24
R2	Gigaethernet 1/0/1	VLAN 30	9.1.1.1/24
R2	Gigaethernet 1/0/2	VLAN 20	200.1.1.2/24
R2	Gigaethernet 1/0/3	VLAN 40	192.1.1.1/24
R3	Gigaethernet 1/0/1	VLAN 10	200.1.2.2/24
R3	Gigaethernet 1/0/2	VLAN 30	9.1.1.2/24

配置思路

采用如下思路配置 BFD for BGP 功能：

1. 在各 Switch 上配置 BGP 基本功能。

2. 配置 MED 属性控制路由的选路功能。

3. 在 R1 和 R2 上使能 BFD 检测机制。

数据准备

为完成此配置例，需准备如下的数据：

R1、R2 和 R3 的 Router ID 和所在 AS 号。

BFD 检测的对端 IP 地址。

BFD 控制报文的最小发送间隔、最小接收间隔、本地检测倍数。

配置步骤

步骤 1 配置 BGP 基本功能，在 R1 和 R2，R1 和 R3 之间建立 EBGP 连接， R2 和 R3 间建立 IBGP 连接。

配置 R1。

R1(config)#router bgp 100

R1(config-bgp)#router-id 1.1.1.1

R1(config-bgp)#neighbor 200.1.1.2 remote-as 200

R1(config-bgp)#neighbor 200.1.2.2 remote-as 200

R1(config-bgp)#quit

配置 R2。

R2(config)#router bgp 200

R2(config-bgp)#router-id 2.2.2.2

R2(config-bgp)#neighbor 200.1.1.1 remote-as 100

R2(config-bgp)#neighbor 9.1.1.2 remote-as 200

R2(config-bgp)#network 9.1.1.0 255.255.255.0

R2(config-bgp)#quit

配置 R3。

R3(config)#router bgp 200

R3(config-bgp)#router-id 3.3.3.3

R3(config-bgp)#neighbor 200.1.2.1 remote-as 100

R3(config-bgp)#neighbor 9.1.1.1 remote-as 200

R3(config-bgp)#network 9.1.1.0 255.255.255.0

R3(config-bgp)#network 192.1.1.0 255.255.255.0

R3(config-bgp)#quit

在 R1 查看，BGP 邻居已经建立（Established）。

R1(config-bgp)#show ip bgp neighbor

步骤 2 配置 MED 属性。

通过策略配置 R2 和 R3 送给 R1 的 MED 值。

配置 R2。

R2(config)#route-policy 10 permit node 10

R2(config-route-policy)#apply cost 100

R2(config-route-policy)#quit

R2(config)#router bgp 200

R2(config-bgp)#neighbor 200.1.1.2 route-policy 10 export

配置 R3。

R3(config)#route-policy 10 permit node 10

R3(config-route-policy)#apply cost 150

R3(config-route-policy)#quit

R3(config)#router bgp 200

R3(config-bgp)#neighbor 200.1.2.2 route-policy 10 export

查看 R1 上 BGP 的所有路由信息。

R1(config-bgp)#show ip bgp route

从 BGP 路由表可以看出，去往 192.1.1.0/24 的路由下一跳地址为 200.1.1.2，流量在主链路 R1R2 上传输。

步骤 3 配置 BFD 检测功能、发送和接收间隔、本地检测时间倍数。

在 R1 使能 BFD 功能。

R1(config)#bfd enable

R1(config)#router bgp 100

R1(config-bgp)#neighbor 200.1.1.2 bfd enable

在 R2 使能 BFD 功能。

R2(config)#bfd enable

R2(config)#router bgp 200

R2(config-bgp)#neighbor 200.1.1.1 bfd enable

在 R1 显示 BGP 建立的所有 BFD 会话。

R1(config)#show ip bfd session

步骤 4 查看配置结果。

对 R2 的 VLAN20 接口执行 shutdown 命令，模拟主链路故障。

R2(config)#interface vlan 20

R2(config-vlan-20)#shutdown

在交换机 R1 上，查看 bgp 路由表。

R1(config)#show ip bgp route

从 BGP 路由表可以看出，在主链路失效后，备份链路 R1→R3→R2 生效，去往 192.1.1.0/24 的路由下一跳地址为 200.1.2.2。

4.6 ISIS 配置

4.6.1 ISIS 简介

4.6.1.1 产生背景

随着 Internet 的飞速发展，Internet 正在被越来越多的具有不同需求的用户使用，成千上万的网络终端使用 Internet 保持联系。所以在网络的中间设备（路由器，三层交换机）上需要动态路由协议来指导报文转发，为报文的转发提供准确有效的路由信息，IS-IS 路由协议结合自身具有良好的扩展性的特点，实现了对 IP 网络层协议的支持。

IS-IS（Intermediate System-to-Intermediate System intra-domain routing information exchange protocol，中间系统到中间系统的域内路由信息交换协议）最初是国际标准化组织（the International Organization for Standardization，ISO）为它的无连接网络协议（Connectionless Network Protocol，CLNP）设计的一种动态路由协议。为了提供对 IP 的路由支持，IETF 在 RFC 1195 中对 IS-IS 进行了扩充和修改，使它能够同时应用在 TCP/IP 和 OSI 环境中，称为集成化 IS-IS（Integrated IS-IS 或 Dual IS-IS）。

4.6.1.2 协议介绍

IS-IS 属于内部网关协议（Interior Gateway Protocol，IGP），用于自治系统内部。IS-IS 是一种链路状态协议，使用最短路径优先（Shortest Path First，SPF）算法进行路由计算。IS-IS 路由协议的基本术语包括：

1. IS（Intermediate System），中间系统。相当于 TCP/IP 中的路由器，是 IS-IS 协议中生成路由和传播路由信息的基本单元。在下文中 IS 和路由器具有相同的含义。
2. RD（Routing Domain），路由域。在一个路由域中一群 IS 通过相同的路由协议来交换路由信息。
3. Area，区域，路由域的细分单元，IS-IS 允许将整个路由域分为多个区域。
4. LSDB（Link State Database），链路状态数据库。所有的网络内连接状态组成了链路状态数据库，在每一个 IS 中都至少有一个 LSDB。IS 使用 SPF 算法，利用 LSDB 来生成自己的路由。

5. LSP（Link State Protocol Data Unit），链路状态报文。在 IS-IS 中，每一个 IS 都会生成至少一个 LSP，这些 LSP 包含了本 IS 的所有链路状态信息。每个 IS 收集本区域内所有的 LSP 与自己本地生成的 LSP 构成自己的 LSDB。

4.6.1.3 功能特性

IS-IS 直接运行于链路层之上。其工作过程包括：邻居关系建立；链路状态数据库的同步；路由计算三个方面。

邻居关系的形成过程因网络类型不同而不同，建立邻接的条件：

- 只有同一层的相邻路由器才能成为邻居路由器；
- 对于 level-1 路由器来说要求 area 地址一致；
- 同一网段检查；

链路状态数据库的同步通过 LSP、CSNP 和 PSNP 三种协议报文来完成。在一个 LAN 中必须有一台路由器被选举为 DIS，由 DIS 来负责在广播网络中创建和更新伪节点，维护一个 LAN 中的链路状态数据库。

对于 level-1-2 设备同时维护 level-1 和 level-2 两个数据库，level-1 和 level-2 运行相同 SPF 算法。IS-IS 在链路状态数据库的基础上，使用 SPF（最短路径优先）算法计算出到达网络拓扑中其他设备的最短路径，根据最短路径树可以建立路由表。

4.6.1.4 协议描述

IS-IS 可以运行在点到点链路（Point to Point Links），如 PPP、HDLC 等；也可以运行在广播链路（Broadcast Links），如 Ethernet、Token-Ring 等；对于 NBMA（Non-Broadcast Multi-Access）网络，如 ATM，也被当作 P2P 链路进行处理，对于这种链路，用户只能通过 CLNS MAP 命令配置一条 PVC；IS-IS 不能在点到多点链路（Point to MultiPoint Links）上运行。

为了支持大规模的路由网络，IS-IS 在路由域内采用两级的分层结构。一个大的路由域被分成一个或多个区域（Areas）。区域内的路由通过 Level-1 路由器管理，区域间的路由通过 Level-2 路由器管理。

1. Level-1 路由器：Level-1 路由器负责区域内的路由，它只与同一区域的 Level-1 路由器形成邻接关系，维护一个 Level-1 的 LSDB，该 LSDB 包含本区域的路由信息，到区域外的报文转发给最近的 Level-1-2 路由器。
2. Level-2 路由器：Level-2 路由器负责区域间的路由，可以与其它区域的 Level-2 路由器形成邻接关系，维护一个 Level-2 的 LSDB，该 LSDB 包含区域间的路由信息。

所有 Level-2 路由器和 Level-1-2 路由器组成路由域的骨干网，负责在不同区域间通信，路由域中的 Level-2 路由器必须是物理连续的，以保证骨干网的连续性。

3. Level-1-2 路由器：同时属于 Level-1 和 Level-2 的路由器称为 Level-1-2 路由器，每个区域至少有一个 Level-1-2 路由器，以将区域连在骨干网上。它维护两个 LSDB，Level-1 的 LSDB 用于区域内路由，Level-2 的 LSDB 用于区域间路由。

图 4-34 所示为一个运行 IS-IS 协议的经典网络拓扑，其中 Area5 是骨干区域，该区域中的所有路由器均是 Level-2 路由器。另外 4 个区域为非骨干区域，它们都通过 Level-1-2 路由器与骨干路由器相连。

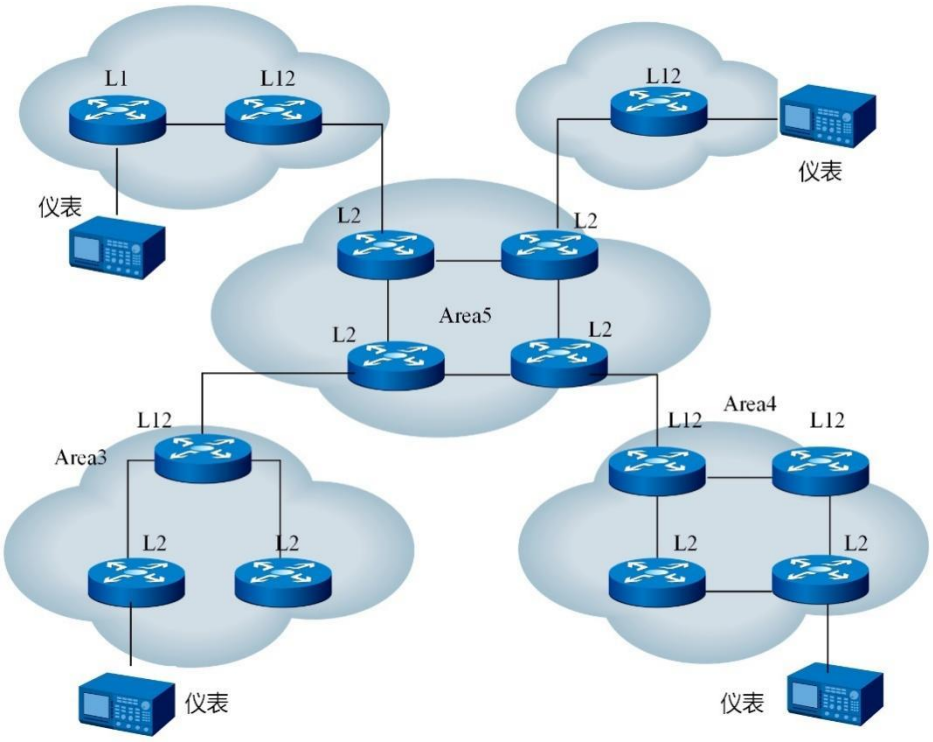


图 4-34 IS-IS 经典网络拓扑图

IS-IS 报文直接封装在数据链路帧中，主要分 3 类：

1. Hello 报文：用于建立和维持邻接关系，也称为 IIH（IS-to-IS Hello PDUs）。其中，广播网中的 Level-1 路由器使用 Level-1 LAN IIH，广播网中的 Level-2 路由器使用 Level-2 LAN IIH，点到点网络中的路由器则使用 P2P IIH。

2. LSP（Link State PDUs，链路状态报文）：用于交换链路状态信息。LSP 分为两种：Level-1 LSP 和 Level-2 LSP。Level-1 路由器传送 Level-1 LSP，Level-2 路由器传送 Level-2 LSP，Level-1-2 路由器则可传送以上两种 LSP。

3. SNP（Sequence Number PDUs，时序报文）：用于确认邻居之间最新接收的 LSP，作用类似于确认（Acknowledge）报文，但更有效。SNP 包括 CSNP（Complete SNP，全时序报文）和 PSNP（Partial SNP，部分时序报文），进一步又可分为 Level-1 CSNP、Level-2 CSNP、Level-1 PSNP 和 Level-2 PSNP。CSNP 包括 LSDB 中所有 LSP 的摘要信息，从而可以在相邻路由器间保持 LSDB 的同步。在广播网络上，CSNP 由 DIS 定期发送（缺省的发送周期为 10 秒）；在点到点链路上，CSNP 只在第一次建立邻接关系时发送。PSNP 只列举最近收到的一个或多个 LSP 的序号，它能够一次对多个 LSP 进行确认。当发现 LSDB 不同步时，也用 PSNP 来请求邻居发送新的 LSP。

根据 RFC1195，集成 IS-IS 协议实现在 OSI 和 IP 的双环境下同时运行，它不仅仅可以动态发现和生成 IP 路由，同时也可以发现和生成 CLNS 路由。ISISv6 则可以在 IPv4 环境下同时运行，它可以动态发现和生成 IPv4 路由。

IS-IS 使用 Hello 报文来发现同一条链路上的邻居路由器并建立邻接关系，使能 ISIS 功能的路由器周期性从每个使能 ISIS 功能的接口发送 Hello 报文，如果从同一条链路上的路由器收到了 IS-IS Hello 报文，且对端路由器发送的 Hello 报文通过了支持协议检查和接口地址检查，将与对方建立起邻接关系。图 4-35 和图 4-36 分别显示了 LAN 接口和点到点接口建立邻居的过程。 建立邻接关系完毕后，将继续周期性的发送 Hello 报文来维持邻接关系。 IS 之间可以建立 IPv4 邻接关系：

1. 如果 IS 之间需要建立 IPv4 邻接关系（IPv4-only），则需要双方接口都配置了合法的 IPv4 地址并且在同一网段（当网络类型为 P2P 时，如果设置了在 PPP 协议接口上接收 Hello 报文时不检查对端 IP 地址的功能，两端路由器的 IP 地址可以不在同一个网段）并且都使能了 IS-IS 功能。

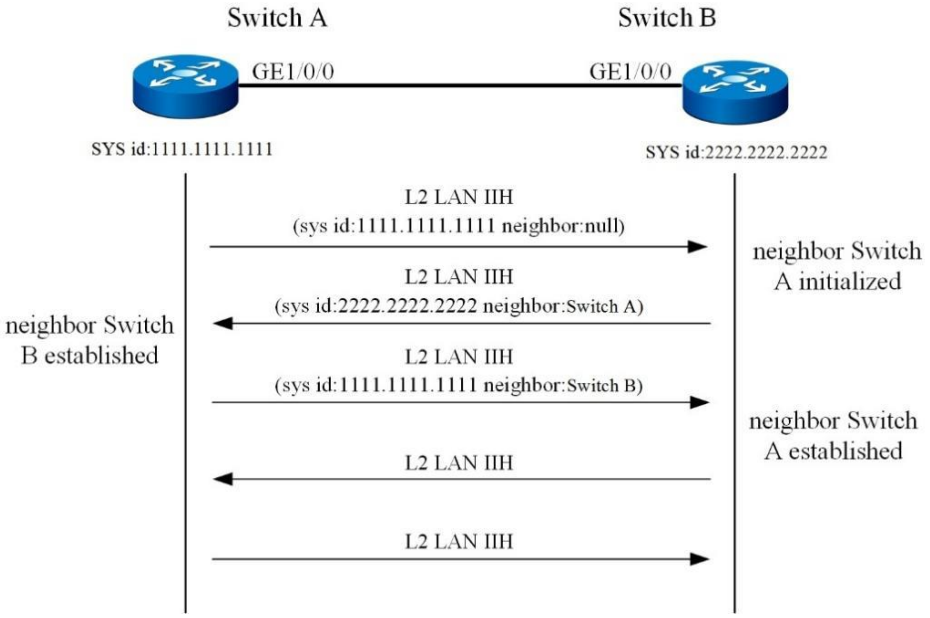


图 4-35 广播链路上的建邻过程

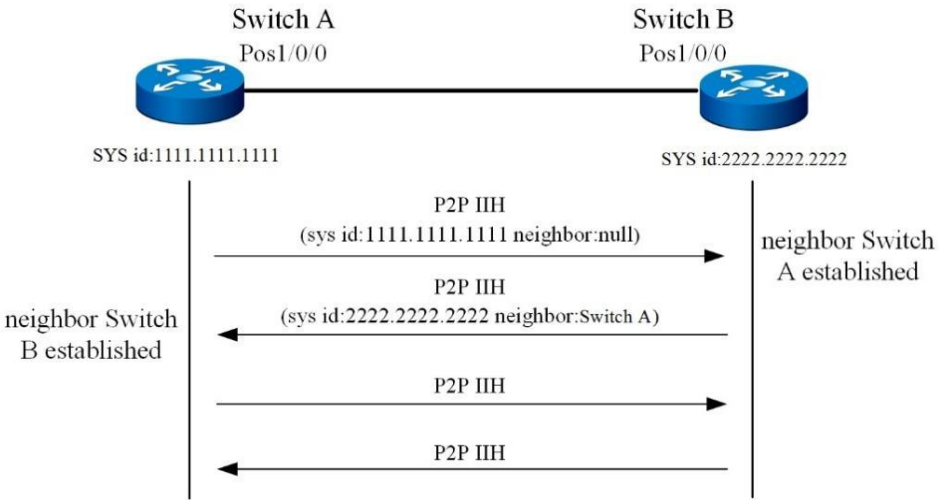


图 4-36 点到点链路上的建邻过程

ISIS 建立邻居后，对于广播链路会选出 DIS，由 DIS 负责维护数据库更新，并使用 LSP 泛洪和 SNP 报文进行数据库同步，点到点链路则直接使用 CSNP 和 PSNP 进行数据库同步。LSP 报文的“泛洪”指当一个路由器向相邻路由器报告自己的 LSP 后，相邻路由器再将同样的 LSP 报文传送到除发送该 LSP 的路由器外的其它邻居，并这样逐级将 LSP 传送到整个层次内的一种方式。通过这种“泛洪”，整个层次内的每一个路由器就

都可以拥有相同的 LSP 信息，并保持 LSDB 的同步。图 4-37 和图 4-38 分别显示了 ISIS 在广播链路和点到点链路上的数据库同步过程：

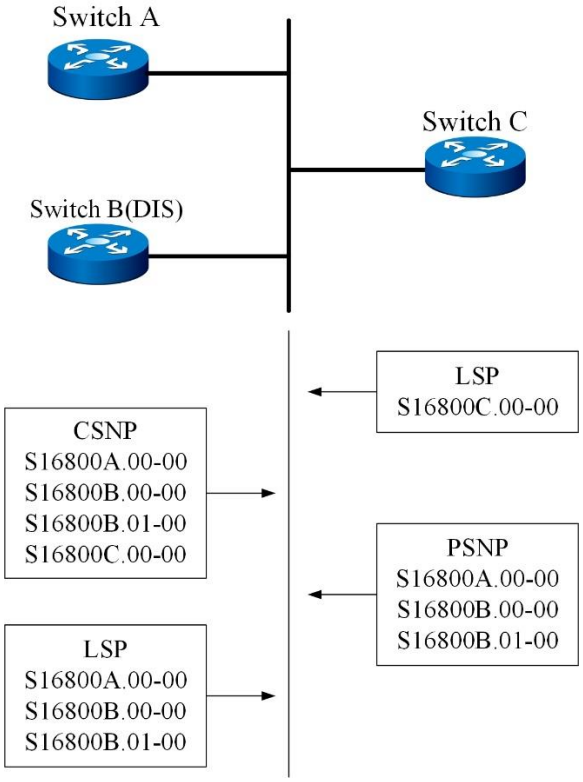


图 4-37 广播链路数据库同步过程

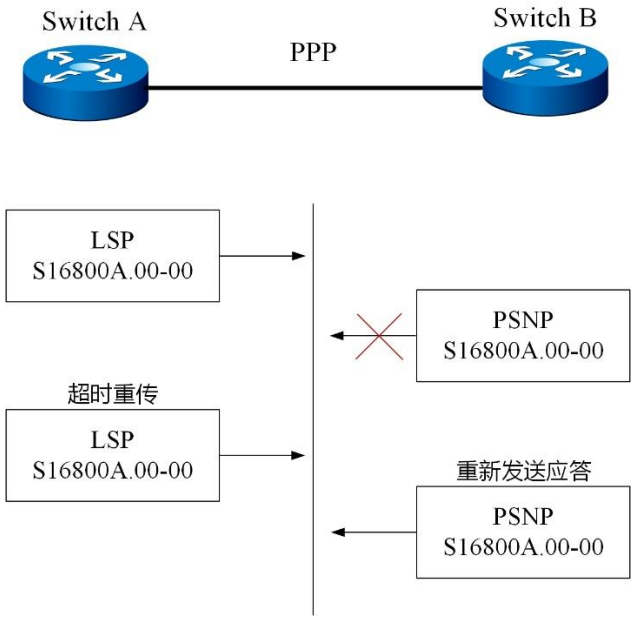


图 4-38 点到点链路数据库同步过程

IS-IS 完成数据库同步后，根据数据库中链路状态信息，使用 SPF 算法计算出无环最短路径优先树，并根据与邻居建立的邻接关系类型对路由计算类型作出限制：

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

4.6.2 ISIS 配置

4.6.2.1 ISIS 基本配置

目的

本节介绍 ISIS 基本配置，包括全局启动 ISIS 实例，接口使能 ISIS 功能并启动 ISIS 进程，配置网络实体标题，以及全局设置 ISIS 过载位。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
启动 ISIS 实例	1. 进入全局配置视图； 2. 执行命令 **router isis** 进入 ISIS 配置视图 3. 执行命令 **router isis** *isis-instance-id* 启动特定实例号的 ISIS 实例。
关闭 ISIS 实例	1. 进入全局配置视图； 2. 执行命令 **no router isis** *isis-instance-id* 关闭特定实例号的 ISIS 实例。
在接口上使能接口的 IS-IS 能力并指定要关联的 IS-IS 进程号	1. 进入全局配置视图； 2. 进入 VLANIF 配置视图、Loopback 接口配置视图； 3. 执行命令 **ip router isis** [*instance-id*]。
在接口上取消接口的 IS-IS 能力并指定要关联的 IS-IS 进程号	1. 进入全局配置视图； 2. 进入 VLANIF 配置视图、Loopback 接口配置视图； 3. 执行命令 **no ip router isis**。
配置 ISIS 网络实体标题	1. 进入全局配置视图； 2. 进入 ISIS 配置视图； 3. 执行命令 **net** *network-entity-title*。
取消 ISIS 网络实体标题	1. 进入全局配置视图； 2. 进入 ISIS 配置视图； 3. 执行命令 **no net** *network-entity-title*。
设置 ISIS 全局的过载位	1. 进入全局配置视图； 2. 进入 ISIS 配置视图； 3. 执行命令 **set-overload-bit**。

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

4.6.2.2 配置 ISIS 基本参数

目的

本节介绍 ISIS 基本参数的配置，包括配置接口状态、接口优先级、报文时间间隔等。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
配置/取消 ISIS 在广播网络上发送 csnp 报文的时间间隔	1. 进入全局配置视图； 2. 进入 VLANIF 配置视图、Loopback 接口配置视图； 3. 执行如下命令： ● **isis csnp-interval** { **level-1** | **level-2** | **ppp** } *interval-value* ● **no isis csnp-interval** { **level-1** | **level-2** | **ppp** }。
使能/关闭 ISIS 接口的被动状态，即抑制该接口发送 IS-IS 报文	1. 进入全局配置视图； 2. 进入 VLANIF 配置视图、Loopback 接口配置视图、接口组配置视图； 3. 执行命令 **isis passive-interface** 或 **no isis passive-interface**。
配置/取消 ISIS 接口下发送 hello 报文的时间间隔	1. 在特权用户视图下执行命令 **configure** 进入全局配置视图； 2. 进入 VLANIF 配置视图、接口组配置视图、Loopback 接口配置视图； 3. 执行如下命令： ● **isis hello-interval** { **level-1** | **level-2** | **ppp** } *hello-interval-time* ● **no isis hello-interval** { **level-1** | **level-2** | **ppp** }。
配置/取消 ISIS 通告邻居超时前没有收到的 hello 报文个数	1. 进入全局配置视图； 2. 进入 VLANIF 配置视图、接口组配置视图； 3. 执行如下命令： ● **isis hello-multiplier** { **level-1** | **level-2** | **ppp** } *multiple-value* ● **no isis hello-multiplier** { **level-1** | **level-2** | **ppp** }。
配置/取消 ISIS 接口下的链路开销	1. 进入全局配置视图； 2. 进入 VLANIF 配置视图、接口组配置视图； 3. 执行如下命令： ● **isis default-metric** { **level-1** | **level-2** | **ppp** } *default-metric* ● **no isis default-metric** { **level-1** | **level-2** | **ppp** }。

目的	步骤
配置/取消接口下的宽开销值	1. 进入全局配置视图； 2. 进入 VLANIF 配置视图、Loopback 接口配置视图； 3. 执行如下命令： ● **isis wide-metric** { **level-1** | **level-2** | **ppp** } *metric* ● **no isis wide-metric** { **level-1** | **level-2** | **ppp** }。
使能/去使能 IPv6 多拓扑功能	1. 进入全局配置视图； 2. 执行命令 **router isis** *isis-instance-id* 进入 ISIS 配置视图； 3. 执行命令 **ipv6-mt** { **enable | disable | enable transition }**。
配置/取消接口 IPv6 的开销值	1. 进入全局配置视图； 2. 执行命令 **router isis** *isis-instance-id* 进入 ISIS 配置视图； 3. 执行命令 **ipv6-mt enable** 使能 IPv6 多拓扑标准模式； 4. 进入 VLANIF 配置视图、Loopback 接口配置视图、以太网子接口配置视图、Trunk 子接口配置视图、以太网路由接口配置视图或 grp 路由接口配置视图； 5. 执行如下命令： ● **isis ipv6-metric** { **level-1** | **level-2** | **ppp** } { *metric* | **default** } ● **no isis ipv6-metric** { **level-1** | **level-2** | **ppp** }。
配置/取消 ISIS 接口优先级，用于 DIS 选举	1. 进入全局配置视图； 2. 进入 VLANIF 配置视图、Loopback 接口配置视图； 3. 执行如下命令： ● **isis priority** { **level-1** | **level-2** } *priority-value* ● **no isis priority** { **level-1** | **level-2** }。
使能/取消 ISIS 接口下的三次握手功能，只针对 p2p 接口	1. 进入全局配置视图； 2. 进入 VLANIF 配置视图、Loopback 接口配置视图； 3. 执行如下命令： ● **isis three-way-handshake** ● **no isis three-way-handshake**。
配置/取消 ISIS 接口下 psnp 报文发送间隔	1. 进入全局配置视图； 2. 进入 VLANIF 配置视图、Loopback 接口配置视图； 3. 执行如下命令： ● **isis psnp-interval** { **level-1** | **level-2** | **ppp** } *interval-value* ● **no isis psnp-interval** { **level-1** | **level-2** | **ppp** }。
配置一个 ISIS 接口的电路类型	1. 进入全局配置视图； 2. 进入 VLANIF 配置视图、Loopback 接口配置视图、接口组配置视图； 3. 执行命令 **isis circuit-type** { **broadcast** | **ppp** }。
使能/取消 ISIS 接口下发送 hello 报文的自动填充功能	1. 进入全局配置视图； 2. 进入 VLANIF 配置视图、Loopback 接口配置视图、接口组配置视图； 3. 执行如下命令 ● **isis hello padding**

目的	步骤
	● **no isis hello padding**。
配置/取消 ISIS 接口加入指定的 mesh-group	1. 进入全局配置视图； 2. 进入 VLANIF 配置视图、Loopback 接口配置视图、接口组配置视图； 3. 执行如下命令： ● **isis mesh-group** *group-value* ● **no isis mesh-group**。
使能 ISIS 接口下的 mesh-group 阻塞功能	1. 进入全局配置视图； 2. 进入 VLANIF 配置视图、Loopback 接口配置视图、接口组配置视图； 3. 执行命令 **isis mesh-group blocked**。
重置所有或单个 ISIS 实例计数信息	1. 进入全局配置视图或特权用户视图； 2. 执行命令 **reset isis** [*isis-instance*] **counter**。

4.6.2.3 配置 ISIS 层级

目的

本节介绍 ISIS 层级配置，包括配置全局系统层级、接口层级以及层级出入开销类型等。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

4.6.2.4 配置 ISIS LSP

目的

本节介绍 ISIS 的 LSP 配置，包括配置 LSP 刷新时间间隔、最大生存时间、全局接收 LSP 报文检查校验、以及全局接收 LSP 报文 MTU 等。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

4.6.2.5 配置 ISIS 重分配

目的

本节介绍 ISIS 的重分配配置，包括使能/取消路由重分配以及使能/取消 ISIS 的 level-2 到 level-1 的路由渗透功能等。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

4.6.2.6 配置 ISIS 路由汇总

目的

本节介绍 ISIS 的路由汇总配置，包括配置/取消一个 ISIS 汇总路由。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
配置/取消一个 ISIS 汇总路由	1. 进入全局配置视图； 2. 进入 ISIS 配置视图； 3. 执行如下命令： ● **summary-address** *ip-address mask-address* { **level-1** | **level-2** } ● **no summary-address** *ip-address mask-address* { **level-1** | **level-2** }。

4.6.2.7 配置 ISIS 认证

目的

本节介绍 ISIS 的认证配置，包括配置/取消 ISIS 全局下的区域认证、配置/取消 ISIS 全局下的域间认证、配置/取消 ISIS 接口以指定的方式和密码验证 Hello 报文等。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

目的	步骤
	● **no isis password** { **level-1** | **level-2** | **ppp** }。

4.6.2.8 配置 ISIS BFD

目的

本节介绍 ISIS 的 BFD 配置，包括使能/关闭 ISIS 接口下的 bfd 功能。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
使能/关闭 ISIS 接口下的 bfd 功能	1. 进入全局配置视图； 2. 进入 VLANIF 配置视图、Loopback 接口配置视图； 3. 执行命令 **isis bfd** { **enable** | **disable** }。

4.6.2.9 配置 ISIS GR

目的

本节介绍 ISIS 的 GR 重启配置，包括使能/取消 ISIS 全局下的 GR 功能。

过程

根据不同目的，执行相应步骤，具体参见下表。

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

4.6.2.10 使能 ISIS 其他功能模块

目的

本节介绍 ISIS 的其他功能模块使能/去使能配置，包括使能/去使能全局 TE、FRR 以及 SNMP 告警功能。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
使能/取消 ISIS 全局下的 TE 功能	1. 进入全局配置视图； 2. 进入 ISIS 配置视图； 3. 执行命令 **traffic-engineer** { **enable** | **disable** } { **level-1** | **level-2** }。
使能/取消 ISIS 全局下的 SNMP 告警功能	1. 进入全局配置视图； 2. 进入 ISIS 配置视图； 3. 执行如下命令： ● **snmp-trap enable** ● **snmp-trap disable**。
配置/取消 ISIS 识别 LSP 报文中主机名称的能力，同时为本地交换机上 IS-IS 系统配置动态主机名，并以 LSP 报文的方式发布出去	1. 进入全局配置视图； 2. 进入 ISIS 配置视图； 3. 执行如下命令： ● **hostname** *host-name* ● **no hostname**。

4.6.2.11 维护及调试

目的

当 ISIS 不正常，需要进行查看、调试或定位问题时，可以使用本小节操作。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
显示指定 level 的 isis database 信息	1. 进入普通用户视图、特权用户视图、全局配置视图、VLANIF 配置视图、Loopback 接口配置视图、ISIS 配置视图； 2. 执行命令 **show ip isis database** { **level-1** | **level-2** } *instance-id*。
显示链路状态数据库信息	1. 进入普通用户视图、特权用户视图、全局配置视图、VLANIF 配置视图、Loopback 接口配置视图、ISIS 配置视图； 2. 执行如下命令： ● **show ip isis database** ● **show ip isis database verbose** ● **show ip isis database verbose** *lsp-index*。
显示 ISIS 数据库统计信息	1. 进入普通用户视图、特权用户视图、全局配置视图、VLANIF 配置视图、Loopback 接口配置视图、ISIS 配置视图；

目的	步骤
	2. 执行命令 **show ip isis database count**。
显示 ISIS 邻居的详细信息	1. 进入普通用户视图、特权用户视图、全局配置视图、VLANIF 配置视图、Loopback 接口配置视图、ISIS 配置视图； 2. 执行命令 **show ip isis neighbor verbose**。
显示 ISIS 的邻居信息	1. 进入普通用户视图、特权用户视图、全局配置视图、VLANIF 配置视图、Loopback 接口配置视图、ISIS 配置视图； 2. 执行命令 **show ip isis neighbor**。
显示 ISIS 的基本配置信息	1. 进入普通用户视图、特权用户视图、全局配置视图、VLANIF 配置视图、Loopback 接口配置视图、ISIS 配置视图； 2. 执行命令 **show ip isis config**。
显示 ISIS 动态主机映射	1. 进入普通用户视图、特权用户视图、全局配置视图、VLANIF 配置视图、Loopback 接口配置视图、ISIS 配置视图； 2. 执行命令 **show ip isis hostname**。
显示 ISIS 接口信息	1. 进入普通用户视图、特权用户视图、全局配置视图、VLANIF 配置视图、Loopback 接口配置视图、ISIS 配置视图； 2. 执行命令 **show ip isis interface**。
显示 ISIS 的错误统计信息	1. 进入普通用户视图、特权用户视图、全局配置视图、VLANIF 配置视图、Loopback 接口配置视图、ISIS 配置视图； 2. 执行命令 **show ip isis error**。
显示 ISIS 的接口错误统计信息	1. 进入普通用户视图、特权用户视图、全局配置视图、VLANIF 配置视图、Loopback 接口配置视图、ISIS 配置视图； 2. 执行命令 **show ip isis error interface**。
显示 ISIS 接口详细信息	1. 进入普通用户视图、特权用户视图、全局配置视图、VLANIF 配置视图、Loopback 接口配置视图、ISIS 配置视图； 2. 执行命令 **show ip isis interface verbose**。
显示 ISIS 实例信息	1. 进入普通用户视图、特权用户视图、全局配置视图、VLANIF 配置视图、Loopback 接口配置视图、ISIS 配置视图； 2. 执行命令 **show ip isis** *instance-id*。
显示 ISIS 学到的路由信息	1. 进入普通用户视图、特权用户视图、全局配置视图、VLANIF 配置视图、Loopback 接口配置视图、ISIS 配置视图； 2. 执行如下命令： ● **show ip isis route** ● **show ip isis route** { **level-1** | **level-2** } ● **show ip isis route** *dst-ip-address* ● **show ip isis route all**。
导出主备盘上的 ISIS 数据到	1. 进入普通用户视图； 2. 执行命令 **dump ha isis table**。

目的	步骤
uspisis_diagnose_isis 文件	

4.6.3 ISIS 配置举例

4.6.3.1 ISIS 基本功能配置

组网要求

本案例的任务是完成 ISIS 最基本的配置，通过该配置熟悉 ISIS 的配置过程，了解 ISIS 配置中 AREA、LEVEL、SYSID 等参数的作用，拓扑图如图 4-39 所示。

组网图

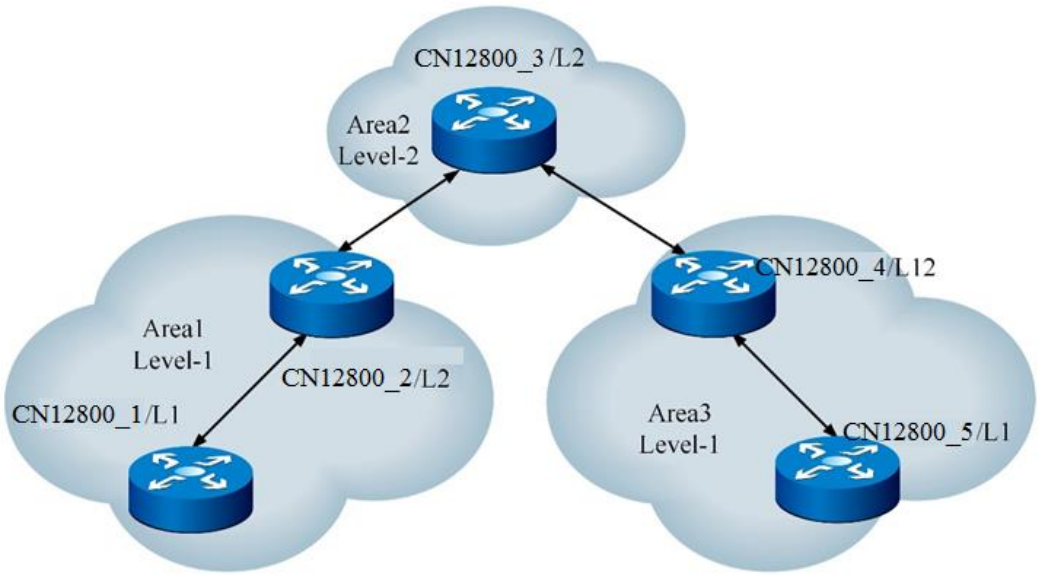


图 4-39 ISIS 基本配置拓扑图

配置思路

所有的设备都运行 ISIS，并将整个自治系统划分为 3 个区域，其中 CN12800_2 和 CN12800_4 为 DIS 来转发区域之间的路由。

配置完成后，每台 Level-1 类型设备都应只学到本区域内全部路由，Level-1-2 和 Level-2 类型设备都能学到自治系统内到所有网段的路由。

数据准备

Area1 和 Area3 为 Level-1 区域，Area2 为 Level-2 区域。

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

CN12800_1 NET 为 10.0001.0001.0001.00，接口地址：1.1.1.1/24。

CN12800_2 NET 为 10.0002.0002.0002.00，两个接口地址：1.1.1.2/24 和 2.1.1.2/24。

CN12800_3 NET 为 20.0003.0003.0003.00，两个接口地址：2.1.1.1/24 和 3.1.1.1/24。

CN12800_4 NET 为 30.0004.0004.0004.00，两个接口地址：3.1.1.2/24 和 4.1.1.2/24。

CN12800_5 NET 为 30.0005.0005.0005.00，接口地址：4.1.1.1/24。

配置步骤

CN12800_1:

CN12800_1(config)#router isis

CN12800_1(config-isis-1)#net 10.0001.0001.0001.00

CN12800_1(config-isis-1)#is-type level-1

CN12800_1(config-isis-1)#exit

CN12800_1(config)#interface vlan 1

CN12800_1(config-vlan-1)#ip router isis

CN12800_2:

CN12800_2 (config)#router isis

CN12800_2 (config-isis-1)#net 10.0002.0002.0002.00

CN12800_2 (config-isis-1)#is-type level-1-2

CN12800_2 (config-isis-1)#exit

CN12800_2 (config)#int vlan 1

CN12800_2 (config-vlan-1)#ip router isis

CN12800_2 (config-vlan-1)#exit

CN12800_2 (config)#int vlan 2

CN12800_2 (config-vlan-2)#ip router isis

CN12800_3:

CN12800_3 (config)#router isis

CN12800_3 (config-isis-2)#net 20.0003.0003.0003.00

CN12800_3 (config-isis-2)#is-type level-2

CN12800_3 (config-isis-2)#exit

CN12800_3 (config)#int vlan 2

CN12800_3 (config-vlan-2)#ip router isis

CN12800_3 (config-vlan-2)#exit

CN12800_3 (config)#int vlan 3

CN12800_3 (config-vlan-3)#ip router isis

CN12800_4:

CN12800_4 (config)#router isis

CN12800_4 (config-isis-2)#net 30.0004.0004.0004.00

CN12800_4 (config-isis-2)#is-type level-1-2

CN12800_4 (config-isis-2)#exit

CN12800_4 (config)#int vlan 3

CN12800_4 (config-vlan-3)#ip router isis

CN12800_4 (config-vlan-1)#exit

CN12800_4 (config)#int vlan 4

CN12800_4 (config-vlan-4)#ip router isis

CN12800_5:

CN12800_5 (config)#router isis

CN12800_5 (config-isis-1)#net 30.0005.0005.0005.00

CN12800_5 (config-isis-1)#is-type level-1

CN12800_5 (config-isis-1)#exit

CN12800_5 (config)#int vlan 4

CN12800_5 (config-vlan-4)#ip router isis

验证配置结果

用 show ip isis neighbor、show ip isis database、show ip isis route 命令验证运行结果。

4.6.3.2 配置 ISIS 重分配

组网要求

本案例的任务是完成 ISIS 重分配的配置，通过该配置熟悉 ISIS 重分配的配置过程，拓扑图如图 4-40 所示。

组网图

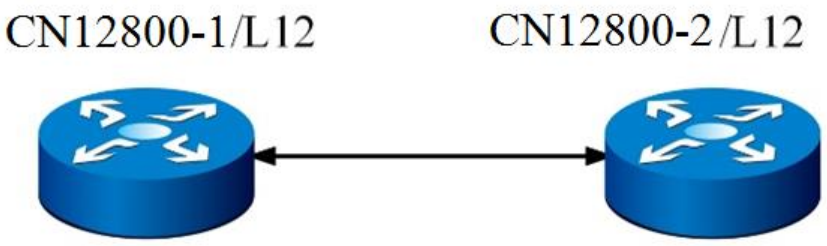


图 4-40 ISIS 重分配拓扑图

配置思路

2 个设备都运行 ISIS，并将两个都配置为同一区域。假定 CN12800_1 上有通过其他路由协议学习到的外部路由并需要向 ISIS 导入，但是对外部路由有如下要求：

1) 接受所有直连路由，并重分配到 level-1；

2) 接收所有 RIP 路由，并重分配到 level-2。

配置完成后，每台设备都应学到自治系统内的到所有网段的路由。

配置步骤

参照 ISIS 基本配置，另外在 CN12800_1 上配置重分配：

CN12800_1(config-isis-1)#redistribute connect level-1

CN12800_1(config-isis-1)#redistribute rip level-2

验证配置结果

用 show ip isis database、show ip isis route 命令验证运行结果。

4.6.3.3 配置 ISIS 路由汇总

组网要求

本案例的任务是完成 ISIS 路由汇总的配置，通过该配置熟悉 ISIS 路由汇总的配置过程，拓扑图如图 4-41 所示。

组网图

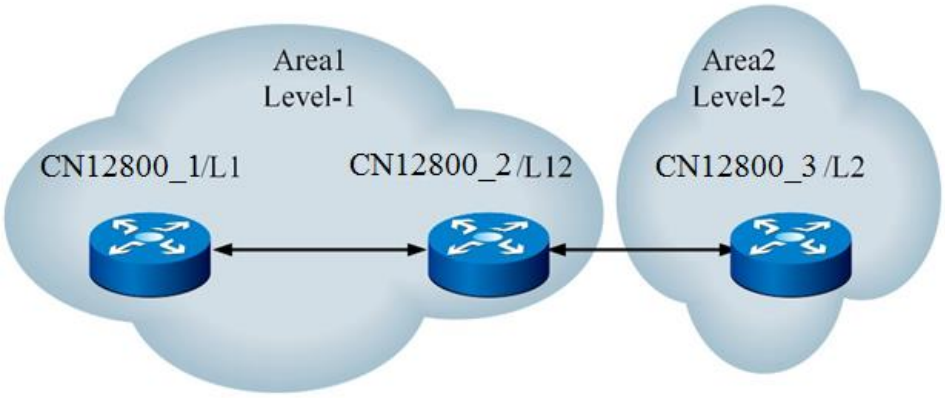


图 4-41 ISIS 路由汇总拓扑图

配置思路

CN12800_1 上有 10.1.1.0/24~10.1.10.0/24 这 10 条路由，希望减小 CN12800_3 的路由表容量，让 CN12800_2 在向 Area2 通告 Area1 路由时汇总为 10.1.0.0/16 一条，因此可以在 CN12800_2 上配置路由汇总命令，配置完后 CN12800_3 仅从 Area1 学习到 10.1.0.0/16 一条路由。

配置步骤

参照 ISIS 基本配置，另外在 CN12800_2 上配置路由汇总：

CN12800_2(config)# router isis

CN12800_2(config-isis-1)#summary-address 10.1.0.0 16

验证配置结果

用 show ip isis database、show ip isis route 命令验证运行结果。

4.6.3.4 配置 ISIS 认证

组网要求

本案例的任务是完成 ISIS 认证的配置，通过该配置熟悉 ISIS 中 level-1/level-2 类型的 Hello 和 Lsp 认证的配置过程，拓扑图如图 4-42 所示。

组网图

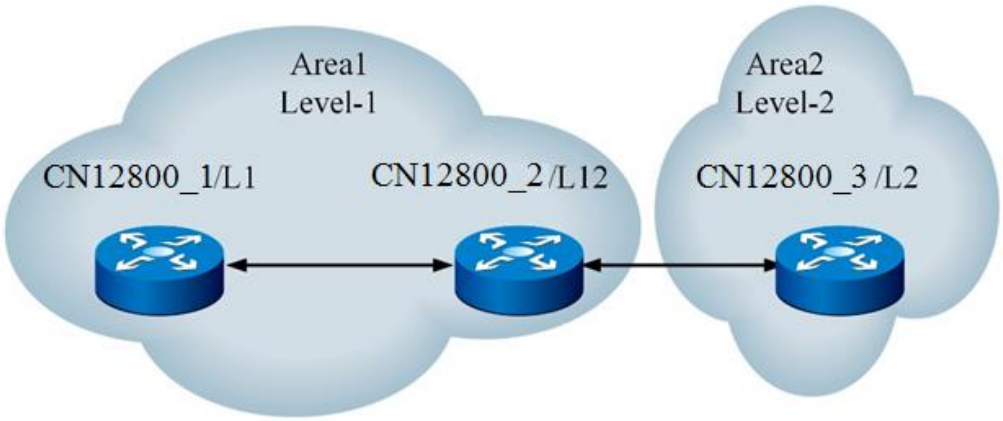


图 4-42 ISIS 认证拓扑图

配置思路

要求 CN12800_1 和 CN12800_2 之间：

level-1 hello 采用简单密码认证，密码为 123456；

level-2 hello 采用 MD5 认证，密码为 fhn；

level-1 Lsp 采用简单密码认证，密码为 12345；

level-2 Lsp 采用 MD5 认证，密码为 cmcc。

配置完成后要求 CN12800_1 和 CN12800_2 之间正常建立 level-1 和 level-2 邻居，正常通告 level-1 路由和 level-2 路由。

配置步骤

参照 ISIS 基本配置，另外再增加认证配置：

CN12800_1：

CN12800_1(config)#router isis

CN12800_1(config-isis-1)#area-password simple 12345

CN12800_1(config-isis-1)#domain-password md5 cmcc

CN12800_1(config-isis-1)#quit

CN12800_1(config)#interface vlan 1

CN12800_1(config- vlan-1)#isis password simple 123456 level-1

CN12800_1(config- vlan-1)#isis password md5 fhn level-2

CN12800_2：

CN12800_2(config)# router isis

CN12800_2(config-isis-1)#area-password simple 12345

CN12800_2(config-isis-1)#domain-password md5 cmcc

CN12800_2(config-isis-1)#quit

CN12800_2(config)#interface vlan 1

CN12800_2(config- vlan-1)#isis password simple 123456 level-1

CN12800_2(config- vlan-1)#isis password md5 fhn level-2

验证配置结果

用 show ip isis neighbor、show ip isis database、show ip isis route 命令验证运行结果。

4.6.3.5 配置 ISIS BFD

组网要求

本案例的任务是完成 ISIS BFD 的配置，通过该配置熟悉 ISIS 中 BFD 的配置过程，拓扑图如图 4-43 所示。

组网图

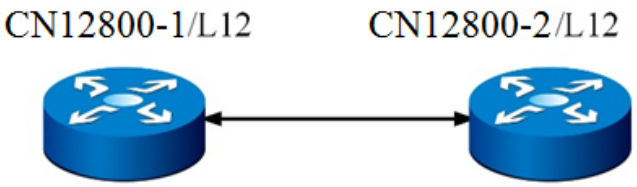


图 4-43 ISIS BFD 拓扑图

配置思路

2 个设备都运行 ISIS，并使能全局 BFD 功能，然后在 ISIS 接口下使能 BFD 功能，配置完成后，邻居和 BFD 绑定，并且连接断开后邻居迅速超时。

配置步骤

参照 ISIS 基本配置，另外再增加 BFD 配置：

CN12800_1：

CN12800_1(config)#interface vlan 2

CN12800_1(config-vlan-2)#bfd enable

CN12800_1(config-vlan-2)# isis bfd enable

CN12800_2：

CN12800_2(config)#interface vlan 2

CN12800_2(config-vlan-2)#bfd enable

CN12800_2(config-vlan-2)#isis bfd enable

验证配置结果

用 show ip isis neighbor、show ip isis database、show ip isis route、show ip isis bfd session 命令验证运行结果。

4.6.3.6 配置 ISIS GR

组网要求

本案例的任务是完成 ISIS GR 的配置，通过该配置熟悉 ISIS 中 GR 的配置过程，拓扑图如图 4-44 所示。

组网图

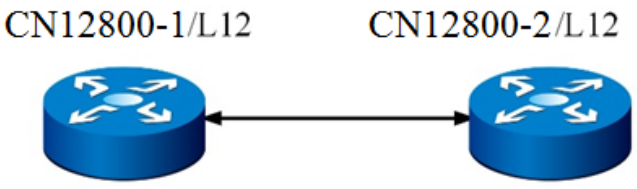


图 4-44 ISIS GR 拓扑图

配置思路

2 个设备都运行 ISIS，并将有个都配置同一 Area，CN12800_1 和 CN12800_2 都需要使能 GR 功能，互相之间发双向流量，待数据库和流量稳定后开始测 GR。

测试 GR 重启需要 2 台设备，一台为 GR 重启者，一台为 GR 帮助者。GR 测试重启者采用双主控，拔插卡的方式测试。帮助者无限制。

配置步骤

参照 ISIS 基本配置，另外再增加 GR 配置：

CN12800_1:

CN12800_1(config)#router isis

CN12800_1(config-isis-1)#graceful-restart enable

CN12800_2:

CN12800_2(config)#router isis

CN12800_2(config-isis-1)#graceful-restart enable

验证配置结果

采用插拔卡进行测试，GR 重启者和 GR 帮助者都配置完成以后，将 GR 重启者的主用主控拔掉，这时起到新的备用主控重启完成后期间，设备间原有的流量应不发生中断。

4.7 路由策略配置

4.7.1 路由策略概述

路由策略

路由策略是为了改变网络流量所经过的途径而对路由信息采用的方法。

为了实现路由策略，通过定义一组匹配规则和设置规则，然后将他们应用到路由的发布、接收和引入等过程的路由策略中。

CN12800 支持的路由策略方式

配置路由策略时，可选择使用的过滤器：地址前缀列表。

地址前缀列表的作用类似于 ACL，但在路由方面比它更为灵活，且更易于用户理解。使用地址前缀列表过滤路由信息时，其匹配对象为路由信息的目的地址信息；另外，用户可以指定路由器选项，指明只接收某些路由器发布的路由信息。

4.7.2 配置地址前缀列表

目的

使用本节操作配置地址前缀列表，实现路由信息的过滤，其匹配对象为路由信息目的地址域。

过程

 **注意：**

- 根据参数 *list-name* 及 IP 类型区分不同表。
- 任意规则匹配后直接返回。
- 匹配操作按照 index 增序进行，不设置 index 时自动取 index 值为表中最大 index – index%10 + 10 值。
- 对表中表项关系逻辑矛盾不检测，配置时需要操作人员自行安排。
- 配置已有 index 上规则时将覆盖原来位置上规则。

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
创建一条过滤规则，完全匹配前 MASKLEN 长度的网段地址	1. 进入全局配置视图； 2. 执行命令 **ip prefix-list** *listname* [**index** *index-number*] { **permit** | **deny** } *ipv4-address mask-length*。
创建一条过滤规则，路由地址掩码长度大于等于指定的最小值且完全匹配前缀掩码长度的网段地址	1. 进入全局配置视图； 2. 执行命令 **ip prefix-list** *listname* [**index** *index-number*] { **permit** | **deny** } *ipv4-address/mask-length* **greater-equal** *prefix-length*。
创建一条过滤规则，路由地址掩码长度小于等于指定的最大值且完全匹配前缀掩码长度的网段地址	1. 进入全局配置视图； 2. 执行命令 **ip prefix-list** *listname* [**index** *index-number*] { **permit** | **deny** } *ipv4-address/mask-length* **less-equal** *prefix-length*。
创建一条过滤规则，路由地址掩码长度小于等于指定的最小值与最大值范围内且完全匹配前缀掩码长度的网段地址	1. 进入全局配置视图； 2. 执行命令 **ip prefix-list** *listname* [**index** *index-number*] { **permit** | **deny** } *ipv4-address/mask-length* **greater-equal** *prefix-length* **less-equal** *prefix-length*。

4.7.3 配置 Route-Policy

前提条件

配置 Route-Policy 之前，还需要配置 ACL 的 filter 规则，请参考本手册 7.3.3 配置三层 ACL 的配置。

目的

使用本节操作配置 Route-Policy 用来匹配给定的路由信息或者路由信息的某些属性，并在条件满足时改变这些路由信息的属性。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
创建路由策略并进入该路由策略 route-policy 配置视图	1. 进入全局配置视图； 2. 执行命令 **route-policy** *policy-name* { **permit** | **deny** } **node** *node-number* 创建路由策略并进入该路由策略配置视图。
（用户可以根据需要）配置相应 match 子句	1. 进入全局配置视图； 2. 进入路由策略配置视图； 3. 选择执行如下命令配置 Router Policy 中的 match 子句： ● **match cost** *cost-value* ● **match ip filter-list** *ipv4-filter-list-number* ● **match community-filter** *community-filter* ● **match extcommunity-filter rt** *extcommunity-filter* ● **match ip** { **next-hop** | **route-source** } **filter-list** *ipv4-filter-list-number* ● **match ip-prefix** *prefix-name* ● **match ip** { **next-hop** | **route-source** } **ip-prefix** *prefix-name* ● **match route-type** { **internal** | **external-type1** | **external-type2** | **external-type1or2** | **nssa-external-type1** | **nssa-external-type2** | **nssa-external-type1or2** } ● **match tag** *tag-value*。
（用户可以根据需要）配置相应 apply 子句	1. 进入全局配置视图； 2. 进入路由策略配置视图； 3. 选择执行如下命令配置 Router Policy 中的 apply 子句： ● **apply cost** *cost-value* ● **apply cost** { **plus** | **minus** } *cost-value* ● **apply cost-type** { **type-1** | **type-2** } ● **apply community none** ● **apply community** *community* [**additive**]

目的	步骤
	● **apply extcommunity rt** *extcommunity* [**additive**] ● **apply local-preference** *local-priority* ● **apply origin** { **igp** | **incomplete** } ● **apply isis** { **level-1** | **level-2** | **level-1-2** } ● **apply origin egp** *as-number* ● **apply ospf** { **translate** | **not-translate** } ● **apply preferred-value** *preferred-value* ● **apply tag** *tag-value*。
（用户可以根据需要）配置相应 ip 子句	1. 进入全局配置视图； 2. 进入路由策略配置视图； 3. 选择执行如下命令配置 Router Policy 中的 ip 子句： ● **ip community-filter** *community* [**index** *interval*] { **permit** | **deny** } { *community-num* | *communitystr* **| internet | no-advertise | no-export | no-export-subconfed** } ● **no ip community-filter** *community* [**index** *interval*] ● **ip extcommunity-filter** *extcommunity* [**index** *interval*] { **permit** | **deny** } *extcommunitystr* ● **no ip extcommunity -filter** *extcommunity* [**index** *interval*]。

4.7.4 对 OSPF 路由协议应用路由策略

目的

使用本节操作配置 OSPF 协议中的路由策略命令引用 ACL 或地址前缀列表，对接收的路由进行过滤，仅接收满足条件的部分路由。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
对 OSPF 发布的路由应用路由策略	1. 进入全局配置视图； 2. 进入 OSPFv2 配置视图； 3. 执行命令 **filter route-policy** *route-policy-name* 用来配置路由协议的过滤策略，只有通过过滤的路由才能被加入更新报文中发布出去。
对 OSPF 引入外部路由时应用路由策略	1. 进入全局配置视图； 2. 进入 OSPFv2 配置视图； 3. 执行命令 **redistribute** { **static** | **connect** | **rip** | **bgp** | **isis** | **ospf** } **route-policy** *policy-name* 用来配置引入不同的路由策略。

4.7.5 对 BGP 路由协议应用路由策略

目的

使用本节操作配置 BGP 协议中的路由策略命令引用 ACL 或地址前缀列表，对接收的路由进行过滤，仅接收满足条件的部分路由。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
对 BGP 邻居接收的路由应用路由策略	1. 进入全局配置视图； 2. 进入 BGP 配置视图； 3. 执行命令 **neighbor** *ipv4-address* **route-policy** *route-policy-name* **import**。
对 BGP 发布的路由应用路由策略	1. 进入全局配置视图； 2. 进入 BGP 配置视图； 【步骤 3 和步骤 4，用户根据实际情况任选】 3. 执行命令 **filter-policy export route-policy** *policy-name* 用来配置路由过滤策略命令； 4. 执行命令 **filter-policy export** { **static** | **connected** | **rip** | **ospf** | **isis** } **route-policy** *route-policy-name* 用来配置路由过滤策略命令。
对 BGP 邻居发布的路由应用路由策略	1. 进入全局配置视图； 2. 进入 BGP 配置视图； 3. 执行命令 **neighbor** *ipv4-address* **route-policy** *route-policy-name* **export** 用来配置路由过滤策略命令。
对 BGP 引入外部路由时应用路由策略	1. 进入全局配置视图； 2. 进入 BGP 配置视图； 3. 执行命令 **redistribute** { **static** | **connected** | **rip** | **ospf** | **isis** } **route-policy** *route-policy-name* 用来配置引入不同的路由策略。

4.7.6 对 ISIS 协议应用路由策略

目的

使用本节操作配置 ISIS 协议中的路由策略命令引用 ACL 或地址前缀列表，对接收的路由进行过滤，仅接收满足条件的部分路由。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
对 ISIS 引入外部路由时应用路由策略	1. 进入全局配置视图； 2. 进入 ISIS 配置视图； 3. 执行命令 **redistribute** { **connect** | **static** | **rip** | **bgp** | **ospf** | **isis** } **route-policy** *policy-name*。
配置 ISIS 路由加入 IP 路由表时的过滤策略	1. 进入全局配置视图； 2. 进入 ISIS 配置视图； 3. 执行命令 **filter-policy import route-policy** *route-policy-name*。

4.7.7 维护及调试

目的

当路由策略功能不正常，需要进行查看、定位问题时，可以使用本小节操作。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
查看路由策略的全局信息	1. 进入特权用户视图、全局配置视图、路由策略配置视图； 2. 执行命令 **show route-policy information** 用来显示路由策略的全局信息。
查看配置的路由策略信息	1. 进入特权用户视图、全局配置视图、路由策略配置视图； 2. 执行如下命令显示配置的路由策略信息： ● **show route-policy config** ● **show route-policy** *policy-name* ● **show route-policy** *policy-name* **node** *node-number*。

4.7.8 配置举例

4.7.8.1 配置 BGP4 ECMP 和路由策略示例

组网要求

所有交换机都配置 BGP，R1 在 AS65008 中，R2 和 R3 在 AS65009 中。R1 与 R2、R3 之间运行 EBGP，R2 和 R3 之间运行 IBGP。

组网图

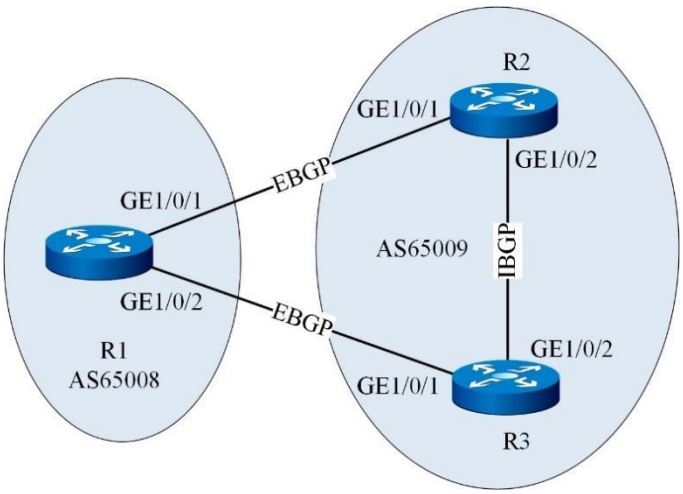


图 4-45 配置 BGP 路径选择的组网图

Switch	接口	对应的 VLAN	IP 地址
R1	Gigaethernet1/0/1	VLAN 10	200.1.1.2/24
R1	Gigaethernet1/0/2	VLAN 20	200.1.2.2/24
R2	Gigaethernet1/0/1	VLAN 10	200.1.1.1/24
R2	Gigaethernet1/0/2	VLAN 30	10.1.1.1/24
R3	Gigaethernet1/0/1	VLAN 20	200.1.2.1/24
R3	Gigaethernet1/0/2	VLAN 30	10.1.1.2/24

配置思路

采用如下的思路配置 BGP 负载分担和运用路由策略更改 MED 属性：

1. 在 R1 和 R2、R1 和 R3 之间配置 EBGP 连接；在 R2 和 R3 之间配置 IBGP 连接。

2. 在 R1 运用路由策略更改 MED 值，查看路由信息。

数据准备

为完成此配置例，需准备如下的数据：

各接口所属的 VLAN ID，具体数据如图 4-45 所示。

各 VLANIF 接口的 IP 地址，具体数据如图 4-45 所示。

R1 的 Router ID 为 1.1.1.1，所在 AS 号 65008，负载分担条数 2。

R2、R3 的 Router ID 分别为 2.2.2.2、3.3.3.3，所在 AS 号 65009，R2 缺省 MED 值 100。

配置步骤

1、 配置 BGP 连接。

#配置 R1。

R1(config)#router bgp 65008

R1(config-bgp)#router-id 1.1.1.1

R1(config-bgp)#neighbor 200.1.1.1 remote-as 65009

R1(config-bgp)#neighbor 200.1.2.1 remote-as 65009

R1(config-bgp)#quit

#配置 R2。

R2(config)#router bgp 65009

R2(config-bgp)#router-id 2.2.2.2

R2(config-bgp)#neighbor 200.1.1.2 remote-as 65008

R2(config-bgp)#neighbor 10.1.1.2 remote-as 65009

R2(config-bgp)#network 10.1.1.0 255.255.255.0

R2(config-bgp)#quit

#配置 R3。

R3(config)#router bgp 65009

R3(config-bgp)#router-id 3.3.3.3

R3(config-bgp)#neighbor 200.1.2.2 remote-as 65008

R3(config-bgp)#neighbor 10.1.1.1 remote-as 65009

R3(config-bgp)#network 10.1.1.0 255.255.255.0

R3(config-bgp)#quit

#查看 R1 的路由表。从路由表中可以看到，BGP 路由 10.1.1.0/24 存在两个下一跳，分别是 200.1.1.1 和 200.1.2.1，且都是最优路由。

R1(config)#show ip bgp route

2 、配置 MED 属性。

#通过策略配置 R2 发送给 R1 的 MED 值。

R2(config)#route-policy 10 permit node 10

R2(config-route-policy)#apply cost 100

R2(config-route-policy)#quit

R2(config)#router bgp 65009

R2(config-bgp)#neighbor 200.1.1.2 route-policy 10 export

#查看 R1 的路由表。从路由表中可以看出，由于下一跳为 200.1.1.1（R2 的路由 MED 值为 100，而下一跳为 200.1.2.1 的 MED 值为 0，所以 BGP 优先选择 MED 值较小的路由。

R1(config)#show ip bgp route

4.7.8.2 配置 OSPF 路由策略示例

组网要求

所有交换机都配置 OSPF，并将所有接口都配置为区域 0。CN12800_1 和 CN12800_2 为 ABR 来转发区域之间的路由。要求对 OSPF 协议通过 LSDB 计算路由后将路由下发本地路由表时引用路由策略。

组网图

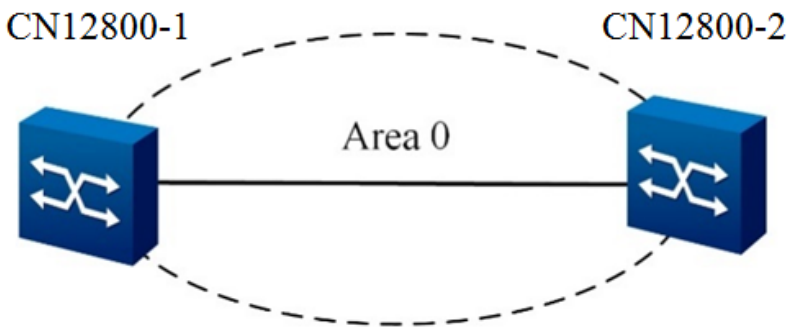


图 4-46 配置 OSPF 路由策略组网图

CN12800_1 的两个接口地址：1.1.1.1/24 和 3.1.1.1/24

CN12800_2 的两个接口地址：1.1.1.2/24 和 4.1.1.2/24

配置步骤

1、配置 CN12800_1。

CN12800_1(config)#router ospf

CN12800_1(config-ospf-1)#router-id 1.1.1.1

CN12800_1(config-ospf-1)#network 1.1.1.0 255.255.255.0 area 0

CN12800_1(config-ospf-1)#network 3.1.1.0 255.255.255.0 area 1

CN12800_1(config)#

2、配置 CN12800_2。

CN12800_2(config)#router ospf

CN12800_2(config-ospf-1)#router-id 1.1.1.2

CN12800_2(config-ospf-1)#network 1.1.1.0 255.255.255.0 area 0

CN12800_2(config-ospf-1)#network 4.1.1.0 255.255.255.0 area 2

CN12800_2(config)#

3、配置路由策略。

CN12800_1(config)#filter-list 1001

CN12800_1(configure-filter-ipv4-1001)#filter 1 ip 18.1.1.0/24 any

CN12800_1(configure-filter-ipv4-1001)#filter 1 action permit

CN12800_1(configure-filter-ipv4-1001)#quit

CN12800_1(config)#route-policy fhn deny node 1

CN12800_1(configure-route-policy)#match ip filter-list 1001

CN12800_1(configure-route-policy)#quit

CN12800_1(config)#route-policy fhn permit node 2

CN12800_1(configure-route-policy)#quit

4、OSPF 里应用路由策略。

CN12800_1(config)#router ospf

CN12800_1(config-ospf-1)#filter route-policy fhn

4.8 策略路由配置

4.8.1 策略路由概述

Policy Route（策略路由）协议概述

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

所谓策略路由，顾名思义，即是根据一定的策略进行报文转发，因此策略路由是一种比目的路由更灵活的路由机制。在路由器转发一个数据报文时，首先根据配置的规则对报

文进行过滤，匹配成功则按照一定的转发策略进行报文转发。这种规则可以是基于标准和扩展访问控制列表，也可以基于报文的长度；而转发策略则是控制报文按照指定的策略路由表进行转发，也可以修改报文的 IP 优先字段。因此，策略路由是对传统 IP 路由机制的有效增强。

Policy Route（策略路由）协议介绍

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

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

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

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

4.8.2 配置策略路由功能

目的

本节介绍配置策略路由的功能的相关操作。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
创建或修改策略路由和策略点，并进入策略路由配置视图	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **policy-based-route** *name* { **permit** | **deny** } **node** *node-id*。
删除策略路由	1. 执行命令 **configure** 进入全局配置视图；

目的	步骤
	2. 执行如下命令： ● **no policy-based-route** *name* ● **no policy-based-route** *name* **node** *node-id*。
配置策略路由应用的 IP 报文优先级	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **policy-based-route** *name* { **permit | deny** } **node** *node-id* 创建或修改策略路由和策略点，并进入策略路由配置视图； 3. 执行命令 **apply ip-precedence** *value*。
取消策略路由应用的 IP 报文优先级	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **policy-based-route** *name* { **permit | deny** } **node** *node-id* 创建或修改策略路由和策略点，并进入策略路由配置视图； 3. 执行命令 **no apply ip-precedence**。
配置策略路由应用的报文下一跳 IP 地址	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **policy-based-route** *name* { **permit | deny** } **node** *node-id* 创建或修改策略路由和策略点，并进入策略路由配置视图； 3. 执行如下命令： ● **apply ip-address next-hop** *ip-address1* ● **apply ip-address next-hop** *ip-address1 ip-address2*。
取消策略路由应用的报文下一跳 IP 地址	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **policy-based-route** *name* { **permit | deny** } **node** *node-id* 创建或修改策略路由和策略点，并进入策略路由配置视图； 3. 执行命令 **no apply ip-address next-hop**。
配置重定向的下一跳 IP 地址	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **policy-based-route** *name* { **permit | deny** } **node** *node-id* 创建或修改策略路由和策略点，并进入策略路由配置视图； 3. 执行命令 **apply load-balance ip-address next-hop** *next-hop-address*。
配置基于访问列表策略路由的 ACL 匹配条件	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **policy-based-route** *name* { **permit | deny** } **node** *node-id* 创建或修改策略路由和策略点，并进入策略路由配置视图； 3. 执行命令 **if-match acl** acl-number。
取消基于访问列表策略路由的 ACL 匹配条件	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **policy-based-route** *name* { **permit | deny** } **node** *node-id* 创建或修改策略路由和策略点，并进入策略路由配置视图； 3. 执行命令 **no if-match acl**。
删除接口应用的策略路由	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令进入接口配置视图（包括 trunk 接口、以太网子接口）； 3. 执行命令 **no ip policy-based-route** *policyname*。

目的	步骤
在策略路由的 NODE 节点下绑定 Time Range	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **policy-based-route** *name* { **permit | deny** } **node** *node-id* 创建或修改策略路由和策略点，并进入策略路由配置视图； 3. 执行命令 **bind time-range list** *list-number*。

4.8.3 维护及调试

目的

当策略路由功能不正常，需要进行查看、调试或定位问题时，可以使用本小节操作。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
显示策略路由信息	1. 进入以下任意一个视图： ● 不执行任何命令保持当前特权用户视图 ● 执行命令 **configure** 进入全局配置视图 ● 执行命令 **disable** 退出到普通用户视图 ● 执行命令 **policy-based-route** *name* { **permit | deny** } **node** *node-id* 创建或修改策略路由和策略点，并进入策略路由配置视图； 2. 执行如下命令： ● **show ip policy-based-route** ● **show ip policy-based-route** *policy-name*。
显示策略路由配置信息	1. 进入以下任意一个视图： ● 不执行任何命令保持当前特权用户视图 ● 执行命令 **configure** 进入全局配置视图 ● 执行命令 **disable** 退出到普通用户视图 ● 执行命令 **policy-based-route** *name* { **permit | deny** } **node** *node-id* 创建或修改策略路由和策略点，并进入策略路由配置视图； 2. 执行命令 **show ip policy-based-route config** 显示策略路由配置信息。

4.8.4 配置举例

4.8.4.1 配置基于 ACL 的策略路由

组网需求

如图 4-47 所示，定义一条名为 aaa 的策略路由，所有从以太网接口 10GE1/1/2 接收的 IP 报文通过接口 10GE1/1/3 发送，下一跳 IP 是 1.1.2.2，其它报文仍然按照查找路由表的方式转发。

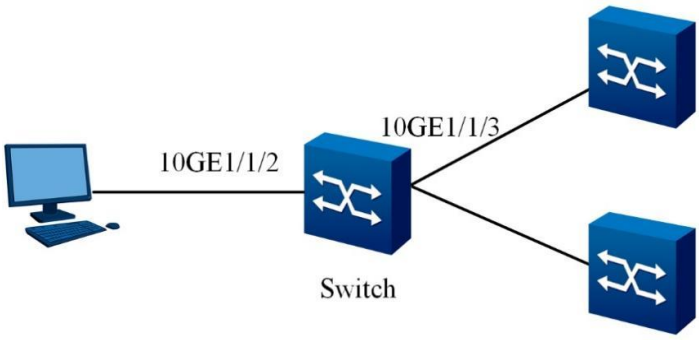


图 4-47 基于 ACL 的策略路由

配置思路

基于 ACL 的策略路由配置思路如下：

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

数据准备

完成该配置举例，需要准备如下数据：

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

配置步骤

1、配置 ACL，定义访问控制列表，ACL filter 1 匹配 IP 报文。

```
CN12800(config)#filter-list 1001
CN12800(configure-filter-ipv4-1001)#filter 1 ip any any
CN12800(configure-filter-ipv4-1001)#filter 1 action permit
```

2、定义策略的规则和动作。

```
CN12800(config) policy-based-route aaa permit node 5
CN12800(config -policy-based-route-aaa-5) if-match acl 1001
CN12800(config -policy-based-route-aaa-5) apply ip-address next-hop 1.1.2.2
CN12800(config -policy-based-route-aaa-5) quit
```

3、在接口上使能策略。

```
CN12800(config) interface 10gigaethernet 1/1/2
CN12800(config-10ge1/1/2) ip policy-based-route aaa
```

4.9 Hwroute 配置

4.9.1 Hwroute 概述

Hwroute 模块仅用于用户进行命令诊断调试所用。

4.9.2 维护及调试

目的

当路由表项不正常，需要进行查看、调试或定位问题时，可以使用本小节操作。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
打开或关闭路由下硬件的调试功能	1. 不执行任何命令保持当前特权用户视图； 2. 执行如下命令： ● **debug hwroute { arp | route | tunnel | ilm | l2vpn | evpn | l3vpn | rtm | all }** ● **no debug hwroute { arp | route | tunnel | ilm | l2vpn | evpn | l3vpn | rtm | all }**。
导出硬件路由表项信息以及路由关联的出口信息	1. 执行命令 **disable** 退出到普通用户视图； 2. 执行如下命令： ● **dump hwroute { arp | nd | ip | ipv6 } slot** *slot-id* ● **dump hwroute { arp | nd | ip | ipv6 } slot** *slot-id* **verbose**。
查看硬件路由下发错误统计信息	1. 执行命令 **disable** 退出到普通用户视图； 2. 执行命令 **show hw route error statistic slot** *slot-id*
查看 IPv4 路由表项	1. 执行命令 **disable** 退出到普通用户视图； 2. 执行如下命令： ● **show hwroute hardware route4** ● **show hwroute hardware arp** ● **show hwroute hardware ilm**。
查看 IPv6 路由表项	1. 执行命令 **disable** 退出到普通用户视图； 2. 执行如下命令： ● **show hwroute hardware route6**

目的	步骤
	● **show hwroute hardware nd**。
查看因为下一跳不可达 IPv4 路由表项	1. 执行命令 **disable** 退出到普通用户视图； 2. 执行命令 **show hwroute hardware route4 pend** 查看因为下一跳不可达 IPv4 路由表项。
查看因为下一跳不可达 IPv6 路由表项	1. 执行命令 **disable** 退出到普通用户视图； 2. 执行命令 **show hwroute hardware route6 pend** 查看因为下一跳不可达 IPv6 路由表项。
查看 IPv4 或 IPv6 ECMP 路由组信息	1. 执行命令 **disable** 退出到普通用户视图； 2. 执行如下命令： ● **show hwroute ecmp-group** ● **show hwroute ecmp-group6**。
查看 IPv4 或 IPv6 下一跳 ID 对应的信息	1. 执行命令 **disable** 退出到普通用户视图； 2. 执行如下命令 ● **show hwroute nexthop** *route-id* ● **show hwroute nexthop6** *route-id*。
查看 HwRoute 模块接收路由消息统计信息	1. 执行命令 **disable** 退出到普通用户视图； 2. 执行命令 **show hwroute statistic rtm** 查看 HwRoute 模块接收路由消息统计信息。
查看 HwRoute 模块路由消息统计信息	1. 执行命令 **disable** 退出到普通用户视图 2. 执行命令 **show hwroute statistic route { v4 | v6 | all }**查看 HwRoute 模块路由消息统计信息。
查看设备从上电以来记录的 HWRT 错误统计信息	1. 执行命令 **disable** 退出到普通用户视图； 2. 执行命令 **show hwrt error statistic** 查看设备从上电以来记录的 HWRT 路由错误统计信息。
将所有 HWRT 的路由和 ND 表项信息写入文件	1. 执行命令 **disable** 退出到普通用户视图； 2. 执行命令 **dump ha hwroute table** 将所有 HWRT 的路由和 ND 表项信息写入文件。

第5章 QoS 配置

本章介绍了 CN12800 系列数据中心交换机 QoS 的基本内容、配置过程和配置举例。

5.1 Diffserv 配置

5.1.1 Diffserv 简介

在传统的 IP 网络中，所有的报文都被无区别的等同对待，每个路由器对所有的报文均采用先入先出（FIFO）的策略进行处理，它尽最大的努力（Best-Effort）将报文送到目的地，但对报文传送的可靠性、传送延迟等性能不提供任何保证。

网络发展日新月异，随着 IP 网络上新应用的不断出现，对 IP 网络的服务质量也提出了新的要求，例如 VoIP（Voice over IP，IP 语音）等实时业务就对报文的传输延迟提出了较高要求，如果报文传送延迟太长，将是用户所不能接受的（相对而言，E-Mail 和 FTP 业务对时间延迟并不敏感）。为了支持具有不同服务需求的语音、视频以及数据等业务，要求网络能够区分出不同的通信，进而为之提供相应的服务。传统 IP 网络的尽力服务不可能识别和区分出网络中的各种通信类别，而具备通信类别的区分能力正式为不同的通信提供不同服务的前提，所以说传统网络的尽力服务模式已不能满足应用的需要。QoS（Quality of Service，服务质量）技术的出现便致力于解决这个问题。

一般来讲，在提供 IP 网络的 QoS 时，为了实现规模适应性，在 IP 骨干网往往需要采用 Diffserv（Differentiated Service，区分服务）体系结构，在 IP 边缘网可以有两种选择：采用 Diffserv 体系结构或采用 Intserv 体系结构。目前在 IP 边缘网络采用哪一种 QoS 体系结构还没有定论，也许这两种会同时并存于 IP 边缘网中。在 IP 边缘网采用 Diffserv 体系结构的情况下，IP 骨干网与 IP 边缘网之间的互通没有问题。在 IP 边缘网采用 Interserv 体系结构的情况下，需要解决 Interserv 与 Diffserv 之间的互通问题，包括 Intserv 支持的业务与 Diffserv 支持的 PHB（Per-Hop Behavior，单中继段行为）之间的映射。

在 CN12800 中，用户可以根据 DiffServ（Differentiated Services）域中定义的报文优先级与 PHB（Per-Hop Behavior）行为之间的映射关系对报文进行简单流分类。对于来自上游设备的报文，在报文的入接口上绑定 DiffServ 域，在 DiffServ 域中将报文携带的优先级信息映射到相应的 PHB 行为、颜色，在设备内部，根据报文的 PHB 行为进行拥塞管理，根据报文的颜色进行拥塞避免；对于流向下游设备的报文，在报文的出接口上绑定 DiffServ 域，在 DiffServ 域中将报文的 PHB 行为、颜色映射为相应的优先级，下游设备根据报文的优先级提供相应的 QoS 服务。

简单流分类的分类依据有：

- VLAN 报文中的 802.1p 优先级
- IP 报文中的 DSCP 优先级
- MPLS 报文中的 EXP 优先级

5.1.2 Diffserv 配置

5.1.2.1 建立配置任务

目的

使用本节操作建立配置任务，进行 Diffserv 相关配置。对于来自上游设备的报文，用户可以根据报文携带的优先级进行分类，分类依据可以是 802.1p 优先级、DSCP 优先级。在 DiffServ 域中定义优先级到 PHB 行为、颜色的映射关系，作为分类依据。将 DiffServ 域绑定到报文的入接口后，QoS 将能够在报文的出接口上根据报文的 PHB 行为和颜色进行拥塞管理和拥塞避免。

对于流向下游设备的报文，用户可以根据报文的 PHB 行为、颜色进行分类。在 DiffServ 域中定义 PHB 行为、颜色到优先级的映射关系，作为分类依据。将 DiffServ 域绑定到报文的出接口后，下游设备将能够根据报文的优先级提供相应的 QoS 服务。

5.1.2.2 创建 DiffServ 域并配置优先级映射关系

目的

本节介绍如何创建 DiffServ 域并配置优先级映射关系。DiffServ 域由一组相连的 DiffServ 节点组成，这些相连的 DiffServ 节点采用相同的服务提供策略并实现相同 PHB 组集合。

当 CN12800 作为 DiffServ 域和其他网络的边界节点时，需要配置内部优先级（以 DiffServ 服务等级和颜色表示）和外部优先级（如 802.1p、DSCP）的相互映射关系。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
创建 Diffserv 域	1. 进入全局配置视图； 2. 执行命令 **diffserv domain** *name* 创建 DiffServ 域并进入 DiffServ 域视图。
删除 Diffserv 域	1. 进入全局配置视图； 2. 执行命令 **no diffserv domain** *name* 删除 Diffserv 域。

目的	步骤
在报文的入接口，将 VLAN 报文的 802.1p 优先级映射为 PHB 行为，并为报文着色	1. 进入全局配置视图； 2. 执行命令 **diffserv domain** *name* 创建 DiffServ 域并进入 DiffServ 域视图； 3. 执行命令 **8021p-inbound** *8021p-priority-range* **default phb** { **be** | **af1** | **af2** | **af3** | **af4** | **ef** | **cs6** | **cs7** } { **green** | **yellow** | **red** }。
在报文的出接口，将 PHB 行为、颜色映射为 VLAN 报文的 802.1p 优先级	1. 进入全局配置视图； 2. 执行命令 **diffserv domain** *name* 创建 DiffServ 域并进入 DiffServ 域视图； 3. 执行如下命令： ● **8021p-outbound { be | af1 | af2 | af3 | af4 | ef | cs6 | cs7 } { green | yellow | red } map** *8021p-priority-range* ● **8021p-outbound { be | af1 | af2 | af3 | af4 | ef | cs6 | cs7 } { green | yellow | red } default**。
在报文的入接口，将 IP 报文的 DSCP 优先级映射为 PHB 行为，并为报文着色	1. 进入全局配置视图； 2. 执行命令 **diffserv domain** *name* 创建 DiffServ 域并进入 DiffServ 域视图； 3. 执行命令 **ip-dscp-inbound** *dscp-priority* **default phb { be | af1 | af2 | af3 | af4 | ef | cs6 | cs7 } { green | yellow | red** }。
在报文的出接口，将 PHB 行为、颜色映射为 IP 报文的 DSCP 优先级	1. 进入全局配置视图； 2. 执行命令 **diffserv domain** *name* 创建 DiffServ 域并进入 DiffServ 域视图； 3. 执行如下命令： ● **ip-dscp-outbound { be | af1 | af2 | af3 | af4 | ef | cs6 | cs7 } { green | yellow | red } map** *dscp priority* ● **ip-dscp-outbound { be | af1 | af2 | af3 | af4 | ef | cs6 | cs7 } { green | yellow | red } default**。

5.1.2.3 配置端口信任的报文优先级

目的

本节介绍如何配置端口信任的报文优先级。

CN12800 提供两种优先级信任模式：

1. 信任报文的 802.1p 优先级。

对于带 VLAN Tag 的报文，根据报文的 802.1p 优先级，查找 802.1p 优先级到内部优先级映射表，然后报文标记内部优先级，对于不带 VLAN Tag 的报文，CN12800 将使用端口的缺省 802.1p 优先级，根据此优先级查找 802.1p 优先级到内部优先级映射表，然后为报文标记内部优先级。

2. 信任报文的 DSCP 优先级。

根据报文的 DSCP 优先级，查找 DSCP 优先级到内部优先级映射表，为报文标记内部优先级。

说明：内部优先级以 DiffServ 模型的服务等级和颜色表示。

如果多个接口需要配置相同的信任报文优先级，可通过端口组进行配置，以减少重复配置工作。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
配置端口信任的报文优先级	1. 进入全局配置视图； 2. 进入接口配置视图（以太网接口、trunk 接口）、接口组配置视图； 3. 执行命令 **trust { 8021p | diffserv | dscp | none } { inner | outer }**。

5.1.2.4 应用 DiffServ 域

目的

本节介绍如何应用 DiffServ 域。

当需要根据 DiffServ 域中定义的映射关系，对来自上游设备的报文进行优先级到 PHB 行为和颜色之间的映射操作时，可以将 DiffServ 域绑定到报文的入接口，系统会根据 DiffServ 域中的映射关系将报文的优先级映射为相应的 PHB 行为和颜色。

当需要根据 DiffServ 域中定义的映射关系，对流向下游设备的报文进行 PHB 行为到优先级之间的映射操作时，可以将 DiffServ 域绑定到报文的出接口，系统会根据 DiffServ 域中的映射关系将报文的 PHB 行为和颜色映射为优先级。

如果接口上配置了 trust diffServ domain recover 命令，系统对出|入该接口的报文恢复默认优先级映射。缺省情况下，端口上不绑定 DiffServ 域，系统采用缺省的优先级映射关系对出入接口的 报文进行优先级映射。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
在接口上绑定 DiffServ 域	1. 进入全局配置视图； 2. 进入接口配置视图（以太网接口、trunk 接口）、接口组配置视图；

目的	步骤
	3. 执行命令 **trust diffserv domain** { *name* | **default** }。
取消对报文按照某类优先级进行的映射	1. 进入全局配置视图； 2. 进入接口配置视图（以太网接口、trunk 接口）、接口组配置视图； 3. 执行命令 **trust none**。

5.1.2.5 检查配置结果

目的

本节介绍如何检查配置结果。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
检查配置结果	1. 进入普通用户视图、特权用户视图、全局配置视图、Diffserv 配置视图、接口配置视图（以太网接口、trunk 接口）、接口组配置视图； 2. 执行如下命令： ● **show diffserv domain** ● **show diffserv domain config** ● **show diffserv domain interface** ● **show diffserv domain interface { ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* ● **show diffserv domain interface eth-trunk** *trunk-number* ● **show diffserv domain** *name*。

5.1.3 配置举例

组网要求

CN12800 通过接口 10GE1/0/1 与路由器互连，企业用户和住宅用户可经由 CN12800 和路由器访问网络。企业用户和住宅用户的 VLAN ID 分别为 100、200。由于企业用户需要得到更好的 QoS 保证，因此将来自企业用户的数据报文优先级映射为 4，将来自住宅用户的数据报文优先级映射为 2，以提供差分服务。

组网图

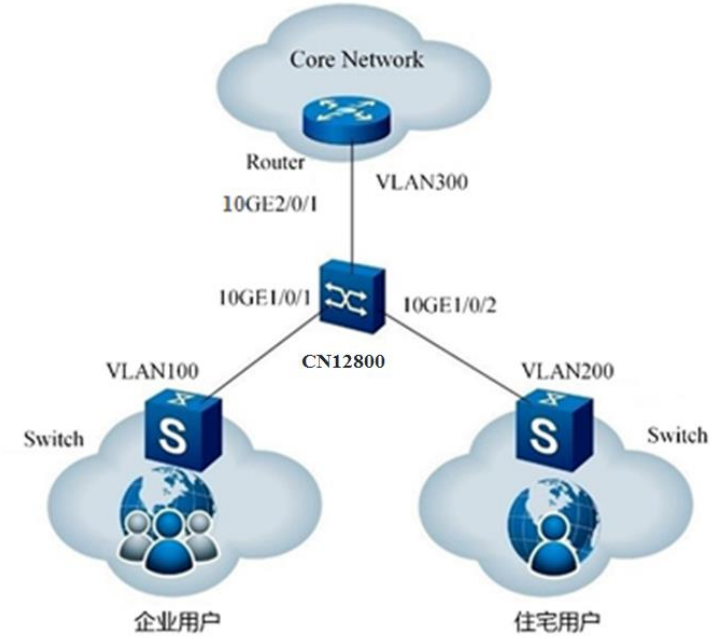


图 5-1 配置 Diffserv 的组网图

配置思路

采用如下的思路配置基于简单流分类的优先级映射：

1. 创建 VLAN，并配置各接口，使企业用户和住宅用户都能够通过 CN12800 访问网络。
2. 创建 DiffServ 域，将 802.1p 优先级映射为 PHB 行为和颜色。
3. 在 CN12800 入接口 10GE1/0/1 和 10GE1/0/2 上配置信任报文优先级。
4. 在 CN12800 入接口 10GE1/0/1 和 10GE1/0/2 上绑定 DiffServ 域。

数据准备

为完成此配置例，需要准备如下的数据：

- DiffServ 域的名称。
- 企业用户和住宅用户的报文的 802.1p 优先级。
- 企业用户和住宅用户的服务等级。

配置步骤

1、创建 VLAN 并配置各接口。

2、创建并配置 DiffServ 域。在 CN12800 上创建 DiffServ 域 ds1、ds2，并配置将企业用户和住宅用户的 802.1p 优先级映射到服务等级。

CN12800(config)#diffserv domain ds1

CN12800(config-dsdomain-ds1)#8021p-inbound 0 phb af4 green

CN12800(config-dsdomain-ds1)#quit

CN12800(config)#diffserv domain ds2

CN12800(config-dsdomain-ds2)#8021p-inbound 0 phb af2 green

CN12800(config-dsdomain-ds2)#quit

3、将 DiffServ 域绑定到接口

将 DiffServ 域 ds1 和 ds2 分别绑定到接口 10GE1/0/1、10GE1/0/2。

CN12800(config)#interface 10gigaethernet 1/0/1

CN12800(config-10ge1/0/1)#trust diffServ domain ds1

CN12800(config-10ge1/0/1)#quit

CN12800(config)#interface 10gigaethernet 1/0/2

CN12800(config-10ge1/0/2)#trust diffServ domain ds2

CN12800(config-10ge1/0/2)#quit

4、配置端口信任的报文优先级

CN12800(config)#interface 10gigaethernet 1/0/1

CN12800(config-10ge1/0/1)#trust 8021p outer

CN12800(config-10ge1/0/1)#quit

CN12800(config)#interface 10gigaethernet 1/0/2

CN12800(config-10ge1/0/2)#trust 8021p outer

CN12800(config-10ge1/0/2)#quit

说明

缺省情况下，DiffServ 域中接口入方向上 VLAN 报文的 802.1p 优先级和 PHB 行为、颜色之间的映射关系：

802.1p 优先级	PHB 行为	Color
0	BE	green
1	AF1	green
2	AF2	green
3	AF3	green
4	AF4	green
5	EF	green
6	CS6	green
7	CS7	green

缺省情况下，DiffServ 域中接口出方向上 VLAN 报文的 PHB 行为、颜色和 802.1p 优先级之间的映射关系：

PHB 行为	Color	802.1p 优先级
BE	green	0
BE	yellow	0
BE	red	0
AF1	green	1
AF1	yellow	1
AF1	red	1
AF2	green	2
AF2	yellow	2
AF2	red	2
AF3	green	3
AF3	yellow	3
AF3	red	3
AF4	green	4
AF4	yellow	4
AF4	red	4
EF	green	5
EF	yellow	5
EF	red	5
CS6	green	6
CS6	yellow	6
CS6	red	6
CS7	green	7
CS7	yellow	7
CS7	red	7

缺省情况下，DiffServ 域中接口入方向上 IP 报文的 DSCP 优先级和 PHB 行为、颜色之间的映射关系：

DSCP	PHB 行为	Color	DSCP	PHB 行为	Color
0	BE	green	32	AF4	green
1	BE	green	33	BE	green
2	BE	green	34	AF4	green
3	BE	green	35	BE	green
4	BE	green	36	AF4	yellow
5	BE	green	37	BE	green
6	BE	green	38	AF4	red
7	BE	green	39	BE	green
8	AF1	green	40	EF	green
9	BE	green	41	BE	green
10	AF1	green	42	BE	green
11	BE	green	43	BE	green
12	AF1	yellow	44	BE	green
13	BE	green	45	BE	green
14	AF1	red	46	EF	green
15	BE	green	47	BE	green
16	AF2	green	48	CS6	green
17	BE	green	49	BE	green
18	AF2	green	50	BE	green
19	BE	green	51	BE	green
20	AF2	yellow	52	BE	green
21	BE	green	53	BE	green
22	AF2	red	54	BE	green
23	BE	green	55	BE	green
24	AF3	green	56	CS7	green
25	BE	green	57	BE	green
26	AF3	green	58	BE	green
27	BE	green	59	BE	green
28	AF3	yellow	60	BE	green
29	BE	green	61	BE	green
30	AF3	red	62	BE	green
31	BE	green	63	BE	green

缺省情况下，DiffServ 域中接口出方向上 IP 报文的 PHB 行为、颜色和 DSCP 优先级之间的映射关系：

PHB 行为	Color	DSCP
BE	green	0
BE	yellow	0
BE	red	0
AF1	green	10
AF1	yellow	12
AF1	red	14
AF2	green	18
AF2	yellow	20
AF2	red	22
AF3	green	26
AF3	yellow	28
AF3	red	30
AF4	green	34
AF4	yellow	36
AF4	red	38
EF	green	46
EF	yellow	46
EF	red	46
CS6	green	48
CS6	yellow	48
CS6	red	48
CS7	green	56
CS7	yellow	56
CS7	red	56

5.2 流量监管和流量整形配置

目的

基于流的流量监管是指在设备上经过流分类后，对符合流分类的流量进行速率限制。通过监督进入设备的该类流量速率，丢弃超出速率限制的部分，使进入设备的该类流量被限制在一个合理的范围之内，从而保护网络资源和运营商的利益。基于流的流量监管采用双令牌桶技术。

通过 Meter 指定限速规则，包括 CIR、CBS、PIR 和 PBS，然后通过 ACL 指定流类型，并与 Meter 进行关联，ACL 即可以在物理接口（包括 Trunk）上使能，也可以在 VLAN 接口上使能。

CN12800 支持端口整形、端口队列整形两种流量整形，可根据需要选择配置。两种流量整形共存时，需要保证端口整形承诺信息速率（CIR）大于等于端口队列整形 CIR 之和；否则，流量整形会出现异常现象（如低优先级队列抢占高优先级队列的带宽）。

该命令用来配置 QOS CAR 模板（CIR、CBS、PIR、PBS），并应用于端口出方向和入方向。QoS CAR 应用在物理接口或 Eth-Trunk 接口上后，系统对该物理接口或 Eth-Trunk 接口上的所有上行报文进行限流。

接口上 QoS CAR 的优先级高于 VLAN 下的 QoS CAR，因此，如果接口上和 VLAN 下同时应用了 QoS CAR，系统优先选择接口上的 QoS CAR。

cir-value：指定承诺信息速率，即保证能够通过的平均速率。整数形式，取值范围是 64～4294967295，单位为 kbit/s。

cbs-value：指定承诺突发尺寸，即瞬间能够通过的承诺突发流量。整数形式，取值范围是 10000～4294967295，单位是 byte

pir-value：指定峰值信息速率。整数形式，取值范围是 64～4294967295，单位为 kbit/s。pir-value 必须大于等于 cir-value。pir-value 必须大于等于 cir-value，缺省等于 cir-value。如果指定的 pir-value 等于 cir-value，pbs-value 缺省为 0byte；否则，pbs-value 缺省为 pir-value 的 125 倍。

pbs-value：指定峰值突发尺寸。整数形式，取值范围是 10000～4294967295，单位为 byte。pbs-value 必须大于等于 cbs-value。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
配置对某个 meter 进行绑定	1. 进入全局配置视图； 2. 进入 filter 配置视图； 3. 执行命令 **filter** *rule-number* **meter** *meter-number*。
取消 filter 与某个 meter 的绑定关系	1. 进入全局配置视图； 2. 进入 filter 配置视图； 3. 执行命令 **no filter** *rule-number* **meter**。

目的	步骤
配置与 meter 绑定的 filter 条目的外部处理动作	1. 进入全局配置视图； 2. 进入 filter 配置视图； 3. 执行如下命令： ● **filter** *rule-number* **outaction** { **red** | **yellow** } **drop** ● **filter** *rule-number* **outaction** { **red** | **yellow** } **remark-dot1p** *dot1p-value* ● **filter** *rule-number* **outaction** { **red** | **yellow** } **remark-dscp** { *dscp-value* | **af11** | **af12** | **af 13** | **af21** | **af22** | **af23** | **af31** | **af32** | **af33** | **af41** | **af42** | **af43** | **cs1** | **cs2** | **cs3** | **cs4** | **cs5** | **cs6** | **cs7** | **default** | **ef** }。
取消与 meter 绑定的 filter 条目的外部处理动作	1. 进入全局配置视图； 2. 进入 filter 配置视图； 3. 执行命令 **no filter** *rule-number* **outaction**。
配置通过 meter 对包括 CIR、CBS、PIR、EBS 和 PBS 的限速规则的指定	1. 进入全局配置视图； 2. 执行如下命令： ● **meter** *meter-number* **cir** *cir-number* **cbs** *cbs-number* **ebs** *ebs-number* ● **meter** *meter-number* **cir** *cir-number* **cbs** *cbs-number* **ebs** *ebs-number* { **aware | blind** } ● **meter** *meter-number* **cir** *cir-number* **cbs** *cbs-number* **pbs** *pbs-number* **pir** *pir-number* ● **meter** *meter-number* **cir** *cir-number* **cbs** *cbs-number* **pbs** *pbs-number* **pir** *pir-number* { **aware| blind** } ● **no meter** *meter-number*。

5.3 队列调度和拥塞控制配置

5.3.1 队列调度和拥塞控制概述

拥塞影响

所谓拥塞，是指由于供给资源的相对不足而造成转发速率下降、引入额外的延迟的一种现象。

链路带宽的瓶颈会导致拥塞，任何用以正常转发处理的资源的不足，如可分配的处理器时间、缓冲区、内存资源的不足，都会造成拥塞。在目前多业务应用的复杂网络环境下，拥塞极为常见。

拥塞有可能会引发一系列的负面影响：

- 拥塞增加了报文传输的延迟和抖动，过高的延迟会引起报文重传。
- 拥塞使网络的有效吞吐率降低，造成网络资源的利用率降低。

- 拥塞加剧会耗费大量的网络资源（特别是存储资源），不合理的资源分配甚至可能导致系统陷入资源死锁而崩溃。

队列技术

拥塞管理的中心内容：当拥塞发生时如何制定一个资源的调度策略，决定报文转发的处理次序。对于拥塞管理，一般采用队列技术，使用一个队列算法对流量进行分类，之后用某种优先级算法将这些流量发送出去。每种队列算法都是用以解决特定的网络流量问题，并对带宽资源的分配、延迟、抖动等有着十分重要的影响。

5.3.2 配置队列调度及拥塞控制

目的

使用本节操作配置队列调度及拥塞控制。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
配置端口队列的调度模式	1. 进入全局配置视图； 2. 执行 **schedule-profile default** 命令进入 Schedule-profile 配置视图； 3. 执行 **cos schedule-profile** *schedule-profile-name* 命令进入 Cos Schedule-profile 配置视图； 4. 执行如下命令配置端口队列的调度模式： ● **cos scheduling { sp | rr | wrr | drr | wfq }** ● **cos scheduling { sp+rr | sp+wrr | sp+drr | sp+wfq }** *queue-list*。
（可选）配置端口队列的权重	1. 进入全局配置视图； 2. 执行 **schedule-profile default** 命令进入 Schedule-profile 配置视图； 3. 执行 **cos schedule-profile** *schedule-profile-name* 命令进入 Cos Schedule-profile 配置视图； 4. 执行命令 **cos queue** *queue-list* **weight** *weight* 配置端口队列的权重。
配置 TM 调度模型模式版本	1. 进入全局配置视图； 2. 执行命令 **assign cos mode** *mode* **slot** { *slot-list* | **all** }配置 TM 调度模型模式版本。
配置 TM 缓存值	1. 进入全局配置视图； 2. 执行 **slot** *slot-id* 命令进入 Slot 配置视图； 3. 执行命令 **cos buffer-size** { *size-value* | **default** }配置 TM 缓存值。

5.3.3 维护及调试

目的

当队列调度及拥塞控制功能不正常，需要进行查看、调试或定位问题时，可以使用本小节操作。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
查看 cos 接口的调度模板信息	1. 进入普通用户视图； 2. 执行命令 **show cos interface schedule-profile** 查看 cos 接口的调度模板信息。
查看 cos 配置信息	1. 进入普通用户视图； 2. 执行命令 **show cos config** 查看 cos 配置信息。
重置 cos 统计信息	1. 进入全局配置视图； 2. 执行命令 **reset cos statistics all** 或 **reset cos statistics interface** { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* 重置 cos 统计信息。
查看 cos 统计信息	1. 进入普通用户视图； 2. 执行如下命令查看 cos 统计信息： ● **show cos statistics all** ● **show cos statistics interface** { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number*
查看指定槽位线卡的 TM 调度模型模式版本	1. 进入普通用户视图； 2. 执行命令 **show cos mode slot {** *slot-id* **| all }**查看指定槽位线卡的 TM 调度模型模式版本。

5.3.4 配置举例

5.3.4.1 SP 调度配置示例

组网要求

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

组网图

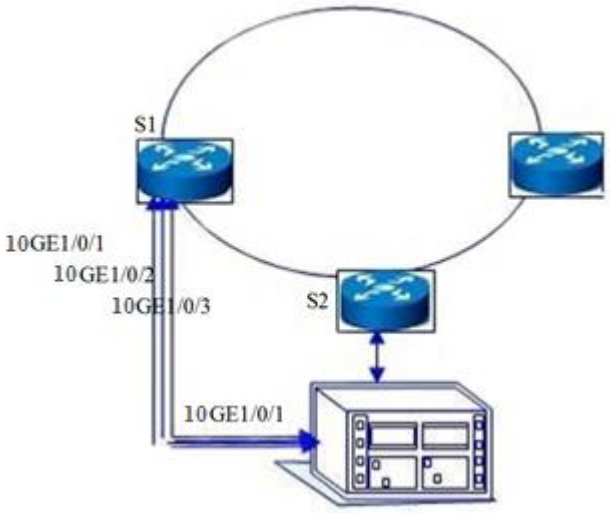


图 5-2 配置端口队列优先级调度组网图

配置步骤

1、站点 1 的配置。

#端口 10GE1/0/1 的配置

S1#configure

S1(config)#interface 10gigaethernet 1/0/1

S1(config-10ge1/0/1)#priority 1

S1(config-10ge1/0/1)#quit

退出端口 10GE1/0/1 的配置

#端口 10GE1/0/2 的配置

S1#configure

S1(config)#interface 10gigaethernet 1/0/2

S1(config-10ge1/0/2)#priority 2

S1(config-10ge1/0/2)#quit

退出端口 10GE1/0/2 的配置

#端口 10GE1/0/3 的配置

S1#configure

S1(config)#interface 10gigaethernet 1/0/3

S1(config-10ge1/0/3)#priority 3

S1(config-10ge1/0/3)#quit

退出端口 10GE1/0/3 的配置

2、站点 2 的配置。

#配置 ACL 规则

S2#configure

S2(config)#filter-list 1001

S2(configure-filter-ipv4-1001)#filter 1 ip 10.164.1.0/24 10.164.9.9/32

S2(config-filter1)#filter 1 action cos 7

#配置端口 10GE1/0/1

S2#configure

S2(config)#interface 10gigaethernet 1/0/1

S2(config-10ge1/0/1)#cos schedule sp

S2(config-10ge1/0/1)#filter-list in 1001

第6章 组播配置

本章介绍了 CN12800 系列数据中心交换机组播配置操作。

6.1 IGMP Snooping 配置

6.1.1 IGMP Snooping 简介

IGMP Snooping 基本原理

IGMP Snooping 是 Internet Group Management Protocol Snooping（互联网组管理协议窥探）的简称。它是运行在二层设备上的组播约束机制。该协议通过侦听网络上用户主机和路由器间传递的 IGMP 报文，通过对收到的 IGMP 报文进行分析，为端口和 MAC 组播地址建立起映射关系，并根据这样的映射关系转发组播数据，从而管理和控制组播组。

当二层设备没有运行 IGMP Snooping 时，组播数据在二层被广播；当二层设备运行了 IGMP Snooping 后，已知组播组的组播数据不会在二层被广播，而在二层被组播给指定的接收者。

IGMP Snooping 优点

IGMP Snooping 具有优点：

- 增强了组播信息的安全性；
- 减少了二层网络中的广播报文，节约了带宽；
- 为实现每台用户主机的单独计费提供了方便。

CN12800 支持的 IGMP Snooping 特性

- 支持静态二层组播

  以太网在传输组播报文时，报文的目的地不是一个具体的接收者，而是一个成员不确定的组。因此当组播报文由网络层转发到链路层时，无法生成组播转发表项，从而导致组播报文在链路层采用广播方式。当设备部署在路由器和用户主机之间，应用二层转发特性时，配置静态二层组播（即手工配置转发表项），可以把组播数据转发给需要长期接收该数据的用户。

  静态二层组播的特点：

  配置接口静态加入组播组，可以避免协议报文的攻击。

采用直接查找组播报文转发表转发报文的机制，可以减少网络的延时。

避免未注册用户收到组播报文，提供有偿服务。

- 支持组播 VLAN 复制

  在传统组播转发方式下，属于不同 VLAN 的用户分别点播统一组播源时，需要交换机为每个 VLAN 都复制一份组播数据，再分别传送给每个 VLAN。配置了组播 VLAN 复制功能后，属于不同 VLAN 的用户分别点播同一组播源时，设备将这些 VLAN 都配置对应一个组播 VLAN。这样，上层路由器只需把一份组播数据传送给该组播 VLAN 即可，而不必再为每个 VLAN 都复制一份组播数据。

  应用组播 VLAN 复制功能便于对组播源和组播组成员进行管理和控制，同时也可以减少带宽的浪费，减小网络的额外负担。

- 支持基于 VLAN 的 IGMP Snooping
  - IGMP 版本可以配置 V1/V2/V3
  - 组播转发模式可配
  - 支持静态路由接口
  - 支持 IGMP 查询功能
  - 支持 IGMP 报文抑制
  - 支持接口快速离开
  - 路由接口老化时间可配
  - 组成员最大响应时间可配
  - 组播策略可配
  - Router Alert 选项可配
  - 发送 IGMP 报文的源 IP 地址可配
  - 支持 IGMP Proxy 功能

6.1.2 配置静态二层组播

背景信息

在城域以太网中，当用户主机需要长期接收某个组播组的组播数据流时，可以配置接口静态加入组播组。

目的

配置该功能后，用户能够长期、稳定、及时的收到已注册的组播数据流。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

6.1.3 配置组播 VLAN 复制

背景信息

通过组播 VLAN 复制功能，可以对组播源和组播组成员进行管理和控制，实现不同 VLAN 内的用户接收相同的组播流，同时也可以减少带宽浪费。

组播 VLAN 复制功能中的 VLAN 分为组播 VLAN 和用户 VLAN。组播 VLAN 是交换机与组播源相连的接口所属的 VLAN，用于实现组播流的汇聚；用户 VLAN 是与组播组成员主机相连的接口所属的 VLAN，用于接收组播 VLAN 的数据流。

目的

通过配置各参数，以满足在不同应用环境中的需求。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
全局使能 IGMP Snooping	1. 进入全局配置视图； 2. 执行命令 **igmp-snooping start** 全局使能组播监听功能。
创建组播 VLAN	1. 进入全局配置视图； 2. 执行命令 **vlan** *vlan-list* 创建需要使能 IGMP Snooping 的 VLAN； 3. 执行命令 **igmp-snooping mvlan** *vlan-id* 创建相应组播 VLAN 并进入组播 VLAN 配置视图。
使能组播 VLAN 的组播复制功能	1. 进入全局配置视图； 2. 进入组播 VLAN 配置视图 ； 3. 执行命令 **igmp-snooping multicast-vlan enable** 使能组播 VLAN 复制功能。
配置组播监听上联口	1. 进入全局配置视图； 2. 进入组播 VLAN 配置视图 ； 3. 执行命令 **igmp-snooping uplink-port** { **ethernet** | **gigaethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number* 或 **igmp-snooping uplink-port eth-trunk** *trunk-number* 配置组播监听上联口。
配置组播复制用户 VLAN	1. 进入全局配置视图； 2. 进入组播 VLAN 配置视图 ； 3. 执行命令 **igmp-snooping multicast user-vlan** *vlan-list* 配置组播复制用户 VLAN。
配置接口加入 VLAN 并在接口上使能 IGMP Snooping 协议	1. 进入全局配置视图； 2. 进入接口组配置视图（以太网接口、trunk 接口）； 3. 执行命令 **port hybrid vlan** *vlan-list* { **tagged** | **untagged** }配置 Hybrid 类型接口所属 VLAN； 4. 执行命令 **igmp-snooping enable** 配置在接口上使能组播监听。

6.1.4 配置 IGMP Snooping

背景信息

基于 VLAN 的 IGMP Snooping 运行在位于路由器和用户主机之间的交换机上，通过侦听上层路由器和主机之间发送的组播协议报文来维护组播报文的转发表项，从而管理和控制组播数据报文的转发，实现二层组播。

目的

通过配置各参数，以满足在不同应用环境中的需求。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
全局使能 IGMP Snooping	1. 进入全局配置视图； 2. 执行命令 **igmp-snooping start** 全局使能组播监听功能。
创建组播 VLAN	1. 进入全局配置视图； 2. 执行命令 **vlan** *vlan-list* 创建需要使能 IGMP Snooping 的 VLAN； 3. 执行命令 **igmp-snooping mvlan** *vlan-id* 创建相应组播 VLAN 并进入组播 VLAN 配置视图。
使能或去使能组播目的 MAC 地址和目的 IP 的一致性检查	1. 进入全局配置视图； 2. 执行命令 **hwmc mac-ip-check** { **enable** | **disable** }。
（可选）配置 IGMP 版本	1. 进入全局配置视图； 2. 进入组播 VLAN 配置视图； 3. 执行命令 **igmp-snooping version { v1 | v2 | v3 }**配置 IGMP 版本。
（可选）配置静态路由器接口	1. 进入全局配置视图； 2. 进入组播 VLAN 配置视图； 3. 执行命令 **igmp-snooping uplink-port { ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* 配置静态路由器接口。
配置特定组查询的查询间隔	1. 进入全局配置视图； 2. 进入 IGMP Snooping MVLAN 配置视图； 3. 执行命令 **igmp-snooping lastmember-queryinterval** { *query-interval* | **default** }配置特定组查询的查询间隔。
配置特定查询的次数	1. 进入全局配置视图； 2. 进入 IGMP Snooping MVLAN 配置视图； 3. 执行命令 **igmp-snooping lastmember-querynumber** { *query-number* | **default** }配置特定查询的次数。
（可选）配置查询器	1. 进入全局配置视图； 2. 执行命令 **igmp-snooping query-interval** { *query-interval* | **default** }配置查询器发送查询报文间隔（各组播 VLAN 共用此参数）； 3. 执行命令 **igmp-snooping robust-count** { *robust-count* | **default** }配置查询器的 IGMP 健壮系数（各组播 VLAN 共用此参数）； 4. 进入组播 VLAN 配置视图； 5. 执行命令 **igmp-snooping querier** { **enable** | **disable** }配置 IGMP snooping 查询器的使能状态；

目的	步骤
	6. 执行命令 **igmp-snooping max-response-time** { *max-response-time* | **default** }配置通用查询报文中最大响应时间字段值。
（可选）配置组播策略	1. 进入全局配置视图； 2. 进入组播 VLAN 配置视图； 3. 执行命令 **igmp-snooping group-policy filter-list** *acl-number* **version** *version-list* 配置组播策略。
（可选）配置协议报文抑制	1. 进入全局配置视图； 2. 进入组播 VLAN 配置视图； 3. 执行命令 **igmp-snooping report-suppress { enable | disable }**配置 VLAN 内报文抑制使能状态。
（可选）配置组播代理地址	1. 进入全局配置视图； 2. 进入组播 VLAN 配置视图 ； 3. 执行命令 **igmp-snooping proxy-ip** *ip-address* 配置查询报文中的源 IP，此配置只要在开启了报文抑制，或者工作在 proxy 时才生效。
（可选）配置组播 VLAN 的 Router-Alert 检查功能	1. 进入全局配置视图； 2. 进入组播 VLAN 配置视图 ； 3. 执行命令 **igmp-snooping require-router-alert** { **enable** | **disable** } 配置 router-alert 需求，此配置使能后只处理携带 router-alert 选项的 IGMP 协议报文。
（可选）配置组播监听工作模式	1. 进入全局配置视图； 2. 进入组播 VLAN 配置视图 ； 3. 执行命令 **igmp-snooping workmode { igmp-snooping | igmp-proxy }**配置组播监听工作模式为 snooping 模式或者 proxy 模式。
使能或去使能当 stp 环拓扑发生变化进行快速切换	1. 进入全局配置视图； 2. 进入组播 VLAN 配置视图； 3. 执行命令 **igmp-snooping fast-switch** { **enable** | **disable** }。
使能或去使能当 stp 环拓扑发生变化进行快速切换时，发送通用查询功能	1. 进入全局配置视图； 2. 进入组播 VLAN 配置视图； 3. 执行命令 **igmp-snooping fast-switch query { enable | disable }。**
使能或去使能禁止向接口发送IGMP查询报文	1. 进入全局配置视图； 2. 进入组播 VLAN 配置视图； 3. 执行命令 **igmp-snooping proxy-uplink-port** { **enable** | **disable** }。
配置 snooping 模式下的查询报文源 IP 地址	1. 进入全局配置视图； 2. 进入组播 VLAN 配置视图； 3. 执行如下命令： ● **igmp-snooping send-query source-address** *src-address* ● **igmp-snooping send-query source-address default。**

目的	步骤
使能或去使能禁止在上联口学习组播表项	1. 进入全局配置视图； 2. 进入组播 VLAN 配置视图； 3. 执行命令 **igmp-snooping uplink-port drop-report { enable | disable }**。
配置上联口的数量限制	1. 进入全局配置视图； 2. 进入组播 VLAN 配置视图； 3. 执行命令 **igmp-snooping uplink-port-limit** { *uplink-port-limit* | **default** }。
配置IGMP snooping协议报文的802.1优先级	1. 进入全局配置视图； 2. 进入组播 VLAN 配置视图； 3. 执行命令 **igmp-snooping 8021p priority** { *value* | **default** }
（可选）配置接口快速离开	1. 进入全局配置视图； 2. 进入接口配置视图（以太网接口、trunk 接口）、接口组配置视图； 3. 执行命令 **igmp-snooping fast-leave { enable | disable }**配置接口快速离开功能。
配置接口上可控组播	1. 进入全局配置视图； 2. 进入接口配置视图（以太网接口、trunk 接口）、接口组配置视图； 3. 执行命令 **igmp-snooping ctrlmode { enable | disable }**配置使能或者去使能接口上可控组播。
配置全局路由器端口老化时间	1. 进入全局配置视图； 2. 执行命令 **igmp-snooping router-aging-time** { *router-aging-time* | **default** }配置全局路由器端口老化时间。
在组播复制使能时配置用户的静态 VLAN	1. 进入全局配置视图； 2. 进入接口配置视图（以太网接口、trunk 接口）、接口组配置视图； 3. 执行命令 i**gmp-snooping static-group group-address** *group-address* **mvlan** *vlan-id* **user-vlan** *vlan-list* 在组播复制使能时配置用户的静态 VLAN。
删除静态组播中的指定用户 VLAN 或所有用户 VLAN	1. 进入全局配置视图； 2. 进入接口配置视图（以太网接口、trunk 接口）、接口组配置视图； 3. 执行如下命令删除静态组播中的指定用户 VLAN 或所有用户 VLAN： ● **no igmp-snooping static-group** ● **no igmp-snooping static-group group-address** *group-address* **mvlan** *vlan-id* **user-vlan** *vlan-list* ● **no igmp-snooping static-group group-address** *group-address* **mvlan** *vlan-id* **user-vlan all** ● **no igmp-snooping static-group mvlan** *vlan-id*。
创建组播 VLAN 的上行接口	1. 进入全局配置视图； 2. 进入接口配置视图（以太网、trunk）、接口组配置视图； 3. 执行命令 **igmp-snooping mvlan** *vlan-id* **uplink-port** 创建组播 VLAN 的上行接口。

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

6.1.5 维护及调试

目的

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

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
查看 IGMP Snooping 配置文件信息	1. 进入普通用户视图、特权用户视图、全局配置视图、接口配置视图（以太网、trunk）、IGMP Snooping MVLAN 配置视图、接口组配置视图； 2. 执行命令 **show igmp-snooping config** 显示 IGMP Snooping 配置文件信息。
查看 IGMP Snooping 接口配置文件信息	1. 进入普通用户视图、特权用户视图、全局配置视图、接口配置视图（以太网、trunk）、IGMP Snooping MVLAN 配置视图、接口组配置视图； 2. 执行命令 **show igmp-snooping interface** 显示 IGMP-snooping 配置模式下组播接口的配置信息。
查看 IGMP-snooping 配置模式下组播 VLAN 的配置信息	1. 进入普通用户视图、特权用户视图、全局配置视图、接口配置视图（以太网、trunk）、IGMP Snooping MVLAN 配置视图、接口组配置视图； 2. 执行命令 **show igmp-snooping mvlan** 显示 IGMP-snooping 配置模式下组播 VLAN 的配置信息。
查看 IGMP-snooping 配置模式下组播上联口的配置信息	1. 进入普通用户视图、特权用户视图、全局配置视图、接口配置视图（以太网、trunk）、IGMP Snooping MVLAN 配置视图、接口组配置视图； 2. 执行命令 **show igmp-snooping uplinkport** 显示 IGMP-snooping 配置模式下组播上联口的配置信息。

目的	步骤
查看 IGMP Snooping 全部、指定接口或指定 VLAN 出端口表项信息	1. 进入普通用户视图、特权用户视图、全局配置视图、接口配置视图（以太网、trunk）、IGMP Snooping MVLAN 配置视图、接口组配置视图； 2. 执行如下命令显示 IGMP Snooping 出端口表项信息： ● **show igmp-snooping egress-port** ● **show igmp-snooping egress-port mvlan** *mvlan-id* ● **show igmp-snooping egress-port interface { ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* ● **show igmp-snooping egress-port interface eth-trunk** *trunk-number*。
查看 IGMP Snooping 组播组表项信息	1. 进入普通用户视图、特权用户视图、全局配置视图、接口配置视图（以太网、trunk）、IGMP Snooping MVLAN 配置视图、接口组配置视图； 2. 执行命令 **show igmp-snooping group** 显示 IGMP Snooping 组播组表项信息。
查看 IGMP Snooping 组播源表项信息（version 3 时有效）	1. 进入普通用户视图、特权用户视图、全局配置视图、接口配置视图（以太网、trunk）、IGMP Snooping MVLAN 配置视图、接口组配置视图； 2. 执行命令 s**how igmp-snooping source-address** 显示 IGMP-snooping 配置模式下组播源地址的配置信息。
清除 igmp-snooping 动态的组播组表信息	1. 进入全局配置视图、接口配置视图（以太网、trunk）、IGMP Snooping MVLAN 配置视图、接口组配置视图； 2. 执行命令 **reset igmp-snooping group** 清除动态的组播组表（group、egress-port 等）。
显示和查看全局配置信息	1. 进入普通用户视图、特权用户视图、全局配置视图、接口配置视图（以太网、trunk）、IGMP Snooping MVLAN 配置视图、接口组配置视图； 2. 执行命令 **show igmp-snooping** 显示和查看全局配置信息。
显示和查看 IGMP snooping 统计信息	1. 进入普通用户视图、特权用户视图、全局配置视图、接口配置视图（以太网、trunk）、IGMP Snooping MVLAN 配置视图、接口组配置视图； 2. 执行如下命令： ● **show igmp-snooping statistic** ● **show igmp-snooping statistic interface** ● **show igmp-snooping statistic interface { ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* ● **show igmp-snooping statistic interface eth-trunk** *trunk-number*。

目的	步骤
清空 IGMP snooping 统计信息	1. 进入全局配置视图、接口配置视图（以太网、trunk）、IGMP Snooping MVLAN 配置视图、接口组配置视图； 2. 执行命令 **reset igmp-snooping statistic**。

6.1.6 配置举例

6.1.6.1 配置静态二层组播举例

组网要求

交换机接口 10GE1/0/1 连接组播源测路由器，接口 10GE1/0/2 连接用户主机，要求通过配置静态二层组播功能实现 VLAN 100 内的所有主机能长期接收组地址为 225.1.1.1 的组播数据，如图 6-1 所示。

组网图

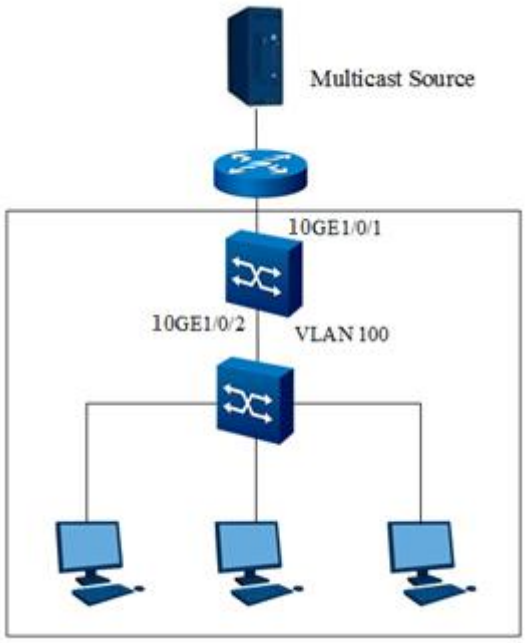


图 6-1 静态二层组播组网图

配置步骤

1、全局使能 IGMP snooping 协议。

CN12800#configure

CN12800(config)#igmp-snooping start

CN12800(config)#

2、创建 VLAN 和相应的组播 VLAN，配置接口加入 VLAN。

CN12800(config)#vlan 100

CN12800(vlan-100)#quit

CN12800(config)#interface 10gigaethernet 1/0/1

CN12800(config-10ge1/0/1)#port hybrid vlan 100 tagged

CN12800(config-10ge1/0/1)#quit

CN12800(config)#interface 10gigaethernet 1/0/2

CN12800(config-10ge1/0/2)#port hybrid vlan 100 tagged

CN12800(config-10ge1/0/2)#quit

CN12800(config)# igmp-snooping mvlan 100

CN12800(config-igmpsnoop-mvlan100)#quit

CN12800(config)#

3、在接口下使能 IGMP Snooping 协议。

CN12800(config)#interface 10gigaethernet 1/0/1

CN12800(config-10ge1/0/1)#igmp-snooping enable

CN12800(config-10ge1/0/1)#quit

CN12800(config)#interface 10gigaethernet 1/0/2

CN12800(config-10ge1/0/2)#igmp-snooping enable

CN12800(config-10ge1/0/2)#quit

CN12800(config)#

4、配置 10GE1/0/1 为静态路由器接口。

CN12800(config)#igmp-snooping mvlan 100

CN12800(config-igmpsnoop-mvlan100)#igmp-snooping uplink-port 10gigaethernet 1/0/1

CN12800(config-igmpsnoop-mvlan100)#quit

CN12800(config)#

5、配置静态组播组。

CN12800(config)#interface 10gigaethernet 1/0/2

CN12800(config-10ge1/0/2)#igmp-snooping static-group group-address 225.1.1.1 mvlan 100

CN12800(config-10ge1/0/2)#quit

CN12800(config)#

6、配置结束，检查组播组表和出端口表信息。

CN12800#show igmp-snooping group

Total Entry(s) : 1

Group Address MVlan Pre-join MemNum V3FilterMode

225.1.1.1 100 disable 1 invalid

CN12800#show igmp-snooping egress-port

Total Entry(s) : 1

Group Address : 225.1.1.1

MVlan : 100

Source Address : *

Interface : xge-1/0/2

Type : static

Expires : ---

OutVlan : 100

V3 Mode : invalid

6.1.6.2 配置 IGMP Snooping 举例

组网要求

交换机接口 10GE1/0/1 连接组播源测路由器，接口 10GE1/0/2 连接用户主机，要求通过配置 IGMP Snooping 功能实现 VLAN100 内的三台主机能长期接收组地址为 225.1.1.1~225.1.1.2 的组播数据，如图 6-2 所示。

组网图

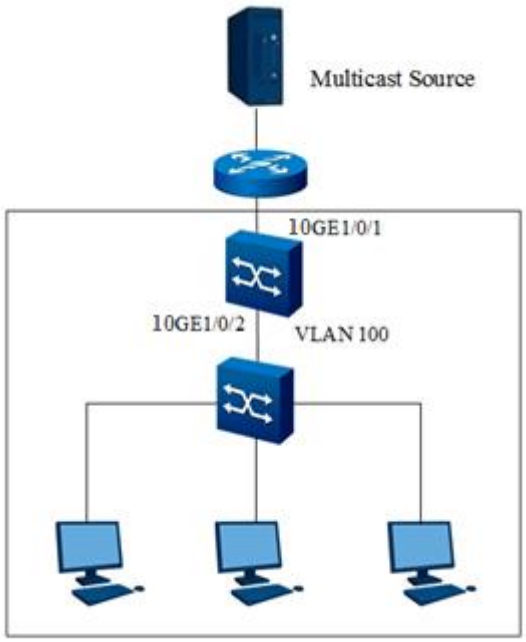


图 6-2 igmp-snooping 配置组网图

配置步骤

1、全局使能 IGMP snooping 协议。

CN12800#configure

CN12800(config)#igmp-snooping start

CN12800(config)#

2、创建 VLAN 和相应的组播 VLAN，配置接口加入 VLAN。

CN12800(config)#vlan 100

CN12800(vlan-100)#quit

CN12800(config)#interface 10gigaethernet 1/0/1

CN12800(config-10ge1/0/1)#port hybrid vlan 100 tagged

CN12800(config-10ge1/0/1)#quit

CN12800(config)#interface 10gigaethernet 1/0/2

CN12800(config-10ge1/0/2)#port hybrid vlan 100 tagged

CN12800(config-10ge1/0/2)#quit

CN12800(config)# igmp-snooping mvlan 100

CN12800(config-igmpsnoop-mvlan100)#quit

CN12800(config)#

3、在接口下使能 IGMP Snooping 协议。

CN12800(config)#interface 10gigaethernet 1/0/1

CN12800(config-10ge1/0/1)#igmp-snooping enable

CN12800(config-10ge1/0/1)#quit

CN12800(config)#interface 10gigaethernet 1/0/2

CN12800(config-10ge1/0/2)#igmp-snooping enable

CN12800(config-10ge1/0/2)#quit

CN12800(config)#

4、配置 10GE1/0/1 为静态路由器接口。

CN12800(config)#igmp-snooping mvlan 100

CN12800(config-igmpsnoop-mvlan100)#igmp-snooping uplink-port 10gigaethernet 1/0/1

CN12800(config-igmpsnoop-mvlan100)#quit

CN12800(config)#

5、配置静态组播组。

CN12800(config)#interface 10gigaethernet 1/0/2

CN12800(config-10ge1/0/2)#igmp-snooping static-group group-address 225.1.1.1 mvlan 100

CN12800(config-10ge1/0/2)#igmp-snooping static-group group-address 225.1.1.2 mvlan 100

CN12800(config-10ge1/0/2)#quit

CN12800(config)#

6、配置结束，检查组播组表和出端口表信息。

CN12800#show igmp-snooping group

Total Entry(s) : 2

Group Address	MVlan	Pre-join	MemNum	V3FilterMode
225.1.1.1	100	disable	1	invalid
225.1.1.2	100	disable	1	invalid

CN12800#show igmp-snooping egress-port

Total Entry(s) : 2

Group Address : 225.1.1.1

MVlan : 100

Source Address : *

Interface : xge-1/0/2

Type : static

Expires : ---

OutVlan : 100

V3 Mode : invalid

Group Address : 225.1.1.2

MVlan : 100

Source Address : *

Interface : xge-1/0/2

Type : static

Expires : ---

OutVlan : 100

V3 Mode : invalid

6.1.6.3 配置组播 VLAN 复制举例

组网要求

交换机接口 10GE1/0/1 连接组播源测路由器属于 VLAN 100，接口 10GE1/0/2 和 10GE10/3 连接用户主机，分别属于 VLAN2 和 VLAN3，要求连接在交换机下的 4 台主机能接收组地址为 225.0.0.1~225.0.0.3 的组播数据。其中 VLAN 100 为组播 VLAN，VLAN2 和 VLAN3 为用户 VLAN，如图 6-3 所示。

组网图

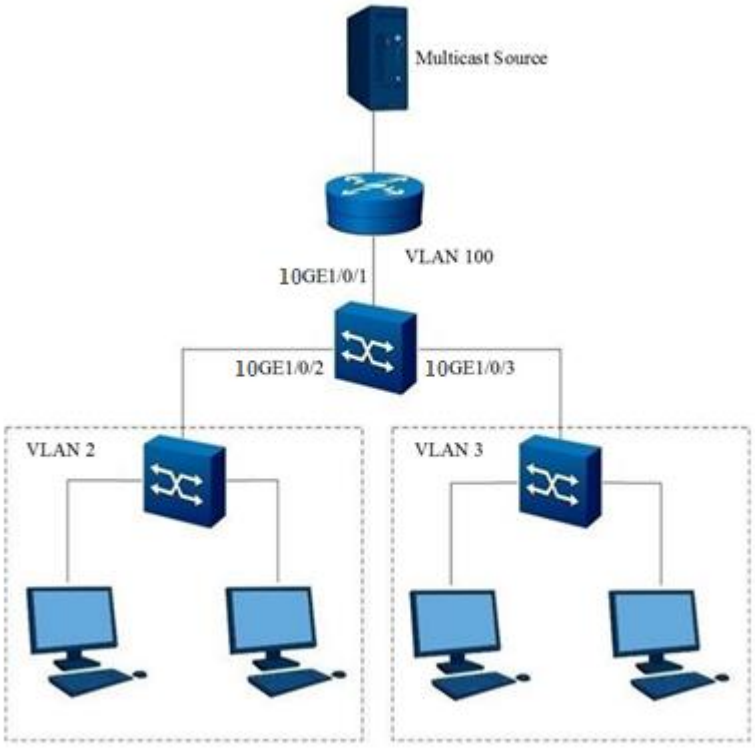


图 6-3 组播复制拓扑图

配置步骤

1、全局使能 IGMP snooping 协议。

CN12800#configure

CN12800(config)#igmp-snooping start

CN12800(config)#

2、创建 VLAN 和相应的组播 VLAN，配置接口加入 VLAN。

CN12800(config)#vlan 2,3,100

CN12800(config)#interface 10gigaethernet 1/0/1

CN12800(config-10ge1/0/1)#port hybrid vlan 100 tagged

CN12800(config-10ge1/0/1)#quit

CN12800(config)#interface 10gigaethernet 1/0/2

CN12800(config-10ge1/0/2)#port hybrid vlan 2 tagged

CN12800(config-10ge1/0/2)#quit

CN12800(config)#interface 10gigaethernet 1/0/3

CN12800(config-10ge1/0/3)#port hybrid vlan 3 tagged

CN12800(config-10ge1/0/3)#quit

CN12800(config)#igmp-snooping mvlan 100

CN12800(config-igmpsnoop-mvlan100)#quit

CN12800(config)#

3、在接口下使能 IGMP Snooping 协议。

CN12800(config)#interface 10gigaethernet 1/0/1

CN12800(config-10ge1/0/1)#igmp-snooping enable

CN12800(config-10ge1/0/1)#quit

CN12800(config)#interface 10gigaethernet 1/0/2

CN12800(config-10ge1/0/2)#igmp-snooping enable

CN12800(config-10ge1/0/2)#quit

CN12800(config)#interface 10gigaethernet 1/0/3

CN12800(config-10ge1/0/3)#igmp-snooping enable

CN12800(config-10ge1/0/3)#quit

CN12800(config)#

4、在组播 VLAN 下使能组播复制功能，并配置用户 VLAN。

CN12800(config)#igmp-snooping mvlan 100

CN12800(config-igmpsnoop-mvlan100)#igmp-snooping multicast-vlan enable

CN12800(config-igmpsnoop-mvlan100)#igmp-snooping multicast user-vlan 2,3

CN12800(config-igmpsnoop-mvlan100)#quit

CN12800(config)#

5、配置 10GE1/0/1 为静态路由器接口。

CN12800(config)#igmp-snooping mvlan 100

CN12800(config-igmpsnoop-mvlan100)#igmp-snooping uplink-port xgigaethernet 1/0/1

CN12800(config-igmpsnoop-mvlan100)#quit

CN12800(config)#

6、配置静态组播组。

CN12800(config)#interface 10gigaethernet 1/0/2

CN12800(config-10ge1/0/2)#igmp-snooping static-group group-address 225.0.0.1 mvlan 100 user-vlan 2

CN12800(config-10ge1/0/2)#igmp-snooping static-group group-address 225.0.0.2 mvlan 100 user-vlan 2

CN12800(config-10ge1/0/2)#igmp-snooping static-group group-address 225.0.0.3 mvlan 100 user-vlan 2

CN12800(config-10ge1/0/2)#quit

CN12800(config)#interface 10gigaethernet 1/0/3

CN12800(config-10ge1/0/3)#igmp-snooping static-group group-address 225.0.0.1 mvlan 100 user-vlan 3

CN12800(config-10ge1/0/3)#igmp-snooping static-group group-address 225.0.0.2 mvlan 100 user-vlan 3

CN12800(config-10ge1/0/3)#igmp-snooping static-group group-address 225.0.0.3 mvlan 100 user-vlan 3

CN12800(config-10ge1/0/3)#quit

7、配置完成，检查组播组表和出端口表信息。

CN12800#show igmp-snooping group

Total Entry(s) : 3

Group Address	MVlan	Pre-join	MemNum	V3FilterMode
225.0.0.1	100	disable	2	invalid
225.0.0.2	100	disable	2	invalid
225.0.0.3	100	disable	2	invalid

CN12800#show igmp-snooping egress-port

Total Entry(s) : 6

Group Address : 225.0.0.1

MVlan : 100

Source Address : *

Interface : xge-1/0/2

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

MVlan : 100

Source Address : *

Interface : xge-1/0/2

Type : static

Expires : ---

OutVlan : 2

V3 Mode : invalid

Group Address : 225.0.0.3

MVlan : 100

Source Address : *

Interface : xge-1/0/3

Type : static

Expires : ---

OutVlan : 3

V3 Mode : invalid

6.2 MLD Snooping 配置

6.2.1 MLD Snooping 简介

MLD Snooping 协议具有以下特点：

1. 静态二层组播：配置接口静态加入组播组，可以避免协议报文的攻击；采用直接查找组播报文转发表转发报文的机制，可以减少网络的延时。

2. 组播 vlan 复制：通过组播 VLAN 复制功能，可以实现组播数据在不同的 VLAN 内传送，便于对组播源和组播组成员的管理和控制，同时也可以减少带宽浪费。

3. MLD snooping：支持基于 vlan 的 MLD snooping 功能。

1）MLD 版本可配置 v1/v2；

2）组播转发模式可配置；

3）支持静态路由接口；

4）支持 MLD 查询功能；

5）支持 MLD 报文抑制；

6）支持接口快速离开；

7）路由接口老化时间可配置；

8）组成员最大响应世家可配置；

9）组播策略可配置；

10）Router Alert 选项可配置；

11）发送 MLD 报文的源 IP 地址可配置；

12）支持 MLD Proxy 功能。

6.2.2 配置 MLD Snooping

目的

配置 MLD Snooping 通过侦听路由器和主机之间发送的组播协议报文来维护组播报文的接口信息，从而管理和控制组播数据报文的转发，实现二层组播。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
全局使能/去使能组播功能，全局去使能组播协议后，会清除掉所有组播配置	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **mld-snooping** { **start** | **stop** }全局使能/去使能组播功能。
配置特定查询间隔，单位为秒	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **mld-snooping lastmember-queryinterval** { *queryinterval-value* | **default** }。
配置通用查询间隔，单位为秒	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **mld-snooping query-interval** { *queryinterval-value* | **default** }。
配置出端口表项健壮系数	1. 执行命令 **configure** 进入全局配置视图； 3. 执行命令 **mld-snooping robust-count** { *robust-count-num* | **default** }。
配置路由器端口老化时间，单位为秒	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **mld-snooping router-aging-time** { *router-aging-time* | **default** }。
创建组播 vlan，进入组播 vlan 配置视图	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **mld-snooping mvlan** *vlan-id*。

目的	步骤
配置组播 vlan 内的组播策略	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **mld-snooping mvlan** *vlan-id* 进入组播 VLAN 配置视图； 3. 执行命令 **mld-snooping group-policy filter-list** *acl-number*。
配置组播 vlan 内的通用查询最大响应时间，单位为秒	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **mld-snooping mvlan** *vlan-id* 进入组播 VLAN 配置视图； 3. 执行命令 **mld-snooping max-response-time** { *responsetime-value* | **default** }。
配置组播 vlan 内的组播复制功能使能/去使能	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **mld-snooping mvlan** *vlan-id* 进入组播 VLAN 配置视图； 3. 执行命令 **mld-snooping multicast-vlan** { **enable** | **disable** }。
配置组播复制用户 VLAN	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **mld-snooping mvlan** *vlan-id* 进入组播 VLAN 配置视图； 3. 执行命令 **mld-snooping multicast user-vlan** *vlan-list*。
删除配置组播复制用户 VLAN	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **mld-snooping mvlan** *vlan-id* 进入组播 VLAN 配置视图； 3. 执行命令 **no mld-snooping multicast user-vlan**。
配置组播 VLAN 内的报文抑制功能	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **mld-snooping mvlan** *vlan-id* 进入组播 VLAN 配置视图； 3. 执行命令 **mld-snooping report-suppress** { **enable** | **disable** }。
配置组播 VLAN 的查询器使能和去使能	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **mld-snooping mvlan** *vlan-id* 进入组播 VLAN 配置视图； 3. 执行命令 **mld-snooping querier** { **enable** | **disable** }。
配置组播 VLAN 的 router-alert 检查功能	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **mld-snooping mvlan** *vlan-id* 进入组播 VLAN 配置视图； 3. 执行命令 **mld-snooping require-router-alert** { **enable** | **disable** }。
配置组播 VLAN 的上联端口（路由器端口）	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **mld-snooping mvlan** *vlan-id* 进入组播 VLAN 配置视图； 3. 执行命令 **mld-snooping uplink-port** { **ethernet | gigaethernet | xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number*。
配置当前接口为指定组播 VLAN 的静态上联口	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **mld-snooping mvlan** *vlan-id* 进入组播 VLAN 配置视图； 3. 执行命令 **interface gigaethernet** *interface-number* 进入以太网桥接接口配置视图； 4. 执行命令 **mld-snooping enable** 使能 MLD Snooping 功能； 3. 执行命令 **mld-snooping mvlan** *vlan-id* **uplink-port** 或 **no mld-snooping mvlan** *vlan-id* **uplink-port**。

目的	步骤
配置组播 VLAN 的协议版本	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **mld-snooping mvlan** *vlan-id* 进入组播 VLAN 配置视图； 3. 执行命令 **mld-snooping version** { **v1** | **v2** }。
配置组播 VLAN 的协议工作模式	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **mld-snooping mvlan** *vlan-id* 进入组播 VLAN 配置视图； 3. 执行命令 **mld-snooping workmode** { **mld-snooping** | **mld-proxy** }。
配置组播 VLAN 的代理 IP	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **mld-snooping mvlan** *vlan-id* 进入组播 VLAN 配置视图； 3. 执行命令 **mld-snooping proxy-ip** *ipv6-address*。
使能或去使能 STP 拓扑变化时快速倒换	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **mld-snooping mvlan** *vlan-id* 进入组播 VLAN 配置视图； 3. 执行命令 **mld-snooping fast-switch** { **enable** | **disable** }。
使能或去使能 STP 拓扑变化时快速倒换发送查询	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **mld-snooping mvlan** *vlan-id* 进入组播 VLAN 配置视图； 3. 执行命令 **mld-snooping fast-switch query** { **enable** | **disable** }。
在端口上使能组播协议	1. 执行命令 **configure** 进入全局配置视图； 2.执行命令 **interface** { **ethernet | gigaethernet | xgigaethernet**| **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number* 进入指定某一接口的配置视图； 3. 执行命令 **mld-snooping** { **enable** | **disable** }。
在端口上使能快速离开	1. 执行命令 **configure** 进入全局配置视图； 2.执行命令 **interface** { **ethernet | gigaethernet | xgigaethernet**| **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number* 进入指定某一接口的配置视图； 3. 执行命令 **mld-snooping fast-leave** { **enable** | **disable** }。
在端口上配置静态组播组	1. 执行命令 **configure** 进入全局配置视图； 2.执行命令 **interface** { **ethernet | gigaethernet | xgigaethernet**| **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number* 进入指定某一接口的配置视图； 3. 执行命令 **mld-snooping static-group group-address** *group-ipv6-address* **mvlan** *vlan-id* **user-vlan** *vlan-list*。

6.2.3 维护及调试

目的

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

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
打开 MLDSnoop 协议调试功能	1. 进入特权用户视图或全局配置视图； 2. 执行命令 **debug mldsnoop** { **rx** | **tx** | **report** | **query** | **leave** | **group** | **uplink** | **mvlan** | **interface** | **message** | **sync** | **hw** | **error** | **control** | **all** }。
关闭 MLDSnoop 协议调试功能	1. 进入特权用户视图或全局配置视图； 2. 执行命令 **no debug mldsnoop** { **rx** | **tx** | **report** | **query** | **leave** | **group** | **uplink** | **mvlan** | **interface** | **message** | **sync** | **hw** | **error** | **control** | **all** }。
显示组播配置信息	1. 执行命令 **disable** 退出到普通用户视图或执行命令 **configure** 进入全局配置视图或执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图或不执行任何命令保持当前特权用户视图； 2. 执行命令 **show mld-snooping config**。
显示组播出端口表信息	1. 执行命令 **disable** 退出到普通用户视图或执行命令 **configure** 进入全局配置视图或执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图或不执行任何命令保持当前特权用户视图； 2. 执行命令 **show mld-snooping egress-port**。
显示组播组表信息	1. 执行命令 **disable** 退出到普通用户视图或执行命令 **configure** 进入全局配置视图或执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图或不执行任何命令保持当前特权用户视图； 2. 执行命令 **show mld-snooping group**。
显示组播接口表信息	1. 执行命令 **disable** 退出到普通用户视图或执行命令 **configure** 进入全局配置视图或执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图或不执行任何命令保持当前特权用户视图； 2. 执行命令 **show mld-snooping interface**。
显示组播 vlan 表信息	1. 执行命令 **disable** 退出到普通用户视图或执行命令 **configure** 进入全局配置视图或执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图或不执行任何命令保持当前特权用户视图； 2. 执行命令 **show mld-snooping mvlan**。
显示组播源表信息	1. 执行命令 **disable** 退出到普通用户视图或执行命令 **configure** 进入全局配置视图或执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图或不执行任何命令保持当前特权用户视图； 2. 执行命令 **show mld-snooping source-address**。
显示组播上联口表信息	1. 执行命令 **disable** 退出到普通用户视图或执行命令 **configure** 进入全局配置视图或执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图或不执行任何命令保持当前特权用户视图； 2. 执行命令 **show mld-snooping uplinkport**。
显示 MLD Snooping 当前基本参数配置信息	1. 执行命令 **disable** 退出到普通用户视图； 2. 执行命令 **show mld-snooping**。

目的	步骤
清除 MLD Snooping 组播组信息	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **reset mld-snooping group**。

6.2.4 配置举例

6.2.4.1 配置 MLD Snooping

组网要求

如图 6-4 所示，交换机接口 10GE1/0/1 连接组播源测路由器，接口 10GE1/0/2 连接用户主机，要求通过配置 MLD Snooping 功能实现 VLAN 100 内的三台主机能长期接收组地址为 FF1E::1～FF1E::2 的组播数据

组网图

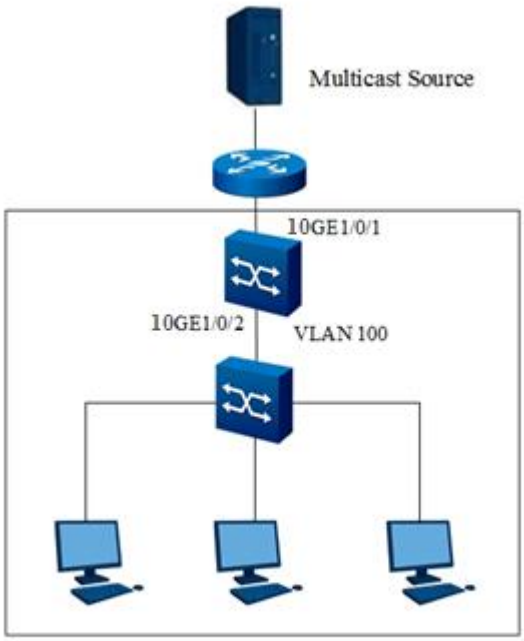


图 6-4 MLD Snooping 配置组网图

配置步骤

1. 全局使能 MLD snooping 协议

CN12800#configure

CN12800(config)# mld-snooping start；

CN12800(config)#

2. 创建 vlan 和相应的组播 vlan，配置接口加入 vlan

CN12800(config)#vlan 100

CN12800(vlan-100)#quit

CN12800(config)#interface xge1/0/1

CN12800(config-10ge1/0/1)#port hybrid vlan 100 tagged

CN12800(config-10ge1/0/1)#quit

CN12800(config)#interface xge1/0/2

CN12800(config-10ge1/0/2)#port hybrid vlan 100 tagged

CN12800(config-10ge1/0/2)#quit

CN12800(config)# mld-snooping mvlan 100

CN12800(config-mldsnoop-mvlan100)#quit

CN12800(config)#

3. 在接口下使能 MLD Snooping 协议

CN12800(config)#interface xge1/0/1

CN12800(config-10ge1/0/1)#mld-snooping enable

CN12800(config-10ge1/0/1)#quit

CN12800(config)#interface xge1/0/2

CN12800(config-10ge1/0/2)#mld-snooping enable

CN12800(config-10ge1/0/2)#quit

CN12800(config)#

4. 配置 10GE1/0/1 为静态路由器接口

CN12800(config)#mld-snooping mvlan 100

CN12800(config-mldsnoop-mvlan100)#mld-snooping uplink-port xge1/0/1

CN12800(config-mldsnoop-mvlan100)#quit

CN12800(config)#

5. 配置静态组播组

CN12800(config)#interface xge1/0/2

CN12800(config-10ge1/0/2)#mld-snooping static-group group-address FF1E::1 mvlan 100

CN12800(config-10ge1/0/2)#mld-snooping static-group group-address FF1E::2 mvlan 100

CN12800(config-10ge1/0/2)#quit

CN12800(config)#

6. 配置结束，检查组播组表和出端口表信息

Total Entry(s) : 1

Group Address MVlan Pre-join MemNum V2FilterMode

ff1e::1 100 disable 1 invalid

ff1e::2 100 disable 1 invalid

CN12800#show mld-snooping egress-port

Total Entry(s) : 2

Group Address : ff1e::1

MVlan : 100

Source Address : *

Interface : xge-1/0/2

Type : static

Expires : ---

OutVlan : 100

V2 Mode : invalid

Group Address : ff1e::2

MVlan : 100

Source Address : *

Interface : xge-1/0/2

Type : static

Expires : ---

OutVlan : 100

V2 Mode : invalid

6.2.4.2 配置静态二层组播

组网要求

如图 6-5 所示，交换机接口 10GE1/0/1 连接组播源测路由器，接口 10GE1/0/2 连接用户主机，要求通过配置静态二层组播实现 VLAN 100 内的所有主机能长期接收组地址为 FF1E::1 的组播数据。

组网图

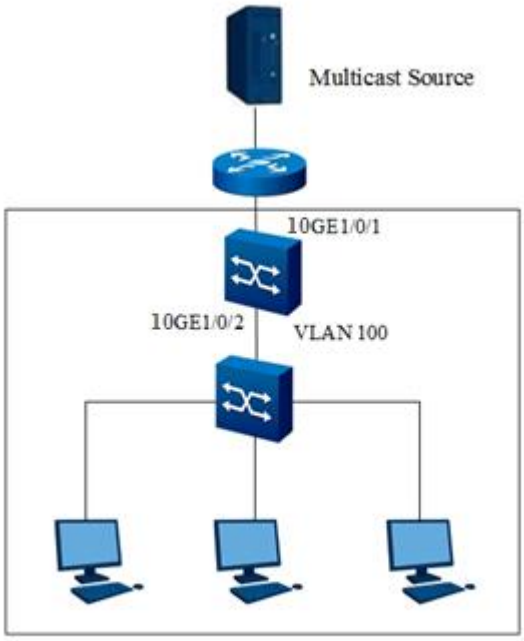


图 6-5 静态二层组播组网图

配置步骤

1. 全局使能 MLD snooping 协议

CN12800#configure

CN12800(config)# mld-snooping start；

CN12800(config)#

2. 创建 vlan 和相应的组播 vlan，配置接口加入 vlan

CN12800(config)#vlan 100

CN12800(vlan-100)#quit

CN12800(config)#interface xge1/0/1

CN12800(config-10ge1/0/1)#port hybrid vlan 100 tagged

CN12800(config-10ge1/0/1)#quit

CN12800(config)#interface xge1/0/2

CN12800(config-10ge1/0/2)#port hybrid vlan 100 tagged

CN12800(config-10ge1/0/2)#quit

CN12800(config)# mld-snooping mvlan 100

CN12800(config-mldsnoop-mvlan100)#quit

CN12800(config)#

3. 在接口下使能 MLD Snooping 协议

CN12800(config)#interface xge1/0/1

CN12800(config-10ge1/0/1)#mld-snooping enable

CN12800(config-10ge1/0/1)#quit

CN12800(config)#interface xge1/0/2

CN12800(config-10ge1/0/2)#mld-snooping enable

CN12800(config-10ge1/0/2)#quit

CN12800(config)#

4. 配置 10GE1/0/1 为静态路由器接口

CN12800(config)#mld-snooping mvlan 100

CN12800(config-mldsnoop-mvlan100)#mld-snooping uplink-port xge1/0/1

CN12800(config-mldsnoop-mvlan100)#quit

CN12800(config)#

5. 配置静态组播组

CN12800(config)#interface xge1/0/2

CN12800(config-10ge1/0/2)#mld-snooping static-group group-address FF1E::1 mvlan 100

CN12800(config-10ge1/0/2)#quit

CN12800(config)#

6. 配置结束，检查组播组表和出端口表信息

CN12800#show mld-snooping group

Total Entry(s) : 1

Group Address MVlan Pre-join MemNum V2FilterMode

ff1e::1 100 disable 1 invalid

CN12800#show mld-snooping egress-port

Total Entry(s) : 1

Group Address : ff1e::1

MVlan : 100

Source Address : *

Interface : xge-1/0/2

Type : static

Expires : ---

OutVlan : 100

V2 Mode : invalid

6.2.4.3 配置组播 VLAN 复制

组网要求

如图 6-6 所示，交换机接口 10GE1/0/1 连接组播源测路由器属于 vlan 100，接口 10GE1/0/2 和 10GE1/0/3 连接用户主机，分别属于 vlan2 和 vlan3，要求连接在交换机下的 4 台主机能接收组地址为 FF1E::1~FF1E::3 的组播数据。其中 vlan 100 为组播 vlan ，vlan2 和 vlan 3 为用户 vlan。

组网图

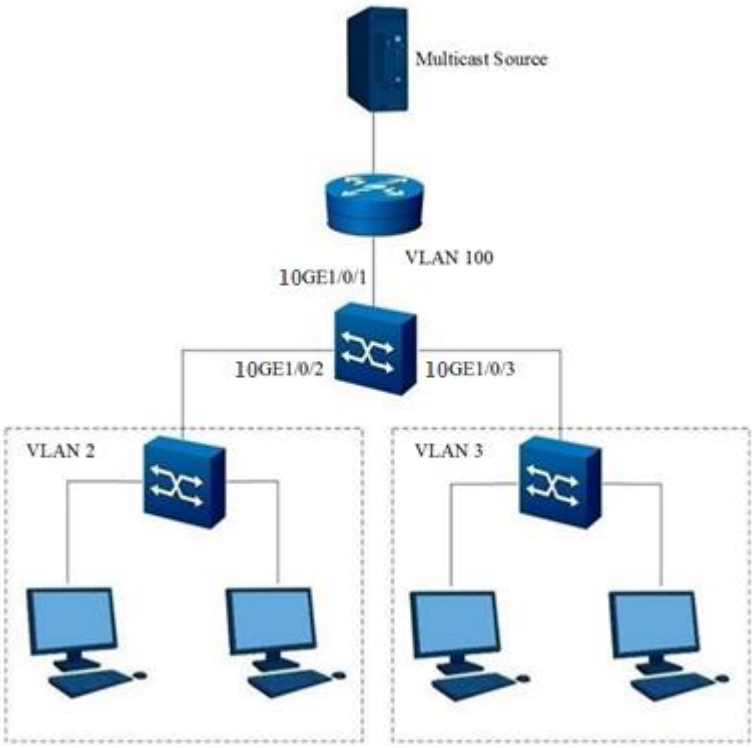


图 6-6 组播复制拓扑图

配置步骤

1. 全局使能 MLD snooping 协议；

CN12800#configure

CN12800(config)# mld-snooping start；

CN12800(config)#

2. 创建 vlan 和相应的组播 vlan，配置接口加入 vlan；

CN12800(config)#vlan 2,3,100

CN12800(config)#interface xgigaethernet 1/0/1

CN12800(config-10ge1/0/1)#port hybrid vlan 100 tagged

CN12800(config-10ge1/0/1)#quit

CN12800(config)#interface xgigaethernet 1/0/2

CN12800(config-10ge1/0/2)#port hybrid vlan 2 tagged

CN12800(config-10ge1/0/2)#quit

CN12800(config)#interface xgigaethernet 1/0/3

CN12800(config-10ge1/0/3)#port hybrid vlan 3 tagged

CN12800(config-10ge1/0/3)#quit

CN12800(config)# mld-snooping mvlan 100

CN12800(config-mldsnoop-mvlan100)#quit

CN12800(config)#

3. 在接口下使能 MLD Snooping 协议

CN12800(config)#interface xgigaethernet 1/0/1

CN12800(config-10ge1/0/1)#mld-snooping enable

CN12800(config-10ge1/0/1)#quit

CN12800(config)#interface xgigaethernet 1/0/2

CN12800(config-10ge1/0/2)#mld-snooping enable

CN12800(config-10ge1/0/2)#quit

CN12800(config)#interface xgigaethernet 1/0/3

CN12800(config-10ge1/0/3)#mld-snooping enable

CN12800(config-10ge1/0/3)#quit

CN12800(config)#

4. 在组播 vlan 下使能组播复制功能，并配置用户 vlan

CN12800(config)#mld-snooping mvlan 100

CN12800(config-mldsnoop-mvlan100)#mld-snooping multicast-vlan enable

CN12800(config-mldsnoop-mvlan100)#mld-snooping multicast user-vlan 2,3

CN12800(config-mldsnoop-mvlan100)#quit

CN12800(config)#

5. 配置 10GE1/0/1 为静态路由器接口

CN12800(config)#mld-snooping mvlan 100

CN12800(config-mldsnoop-mvlan100)#mld-snooping uplink-port xge1/0/1

CN12800(config-mldsnoop-mvlan100)#quit

CN12800(config)#

6. 配置静态组播组

CN12800(config)#interface xgigaethernet 1/0/2

CN12800(config-10ge1/0/2)#mld-snooping static-group group-address FF1E::1 mvlan 100 user-vlan 2

CN12800(config-10ge1/0/2)#mld-snooping static-group group-address FF1E::2 mvlan 100 user-vlan 2

CN12800(config-10ge1/0/2)#mld-snooping static-group group-address FF1E::3 mvlan 100 user-vlan 2

CN12800(config-10ge1/0/2)#quit

CN12800(config)#interface xgigaethernet 1/0/3

CN12800(config-10ge1/0/3)#mld-snooping static-group group-address FF1E::1 mvlan 100 user-vlan 3

CN12800(config-10ge1/0/3)#mld-snooping static-group group-address FF1E::2 mvlan 100 user-vlan 3

CN12800(config-10ge1/0/3)#mld-snooping static-group group-address FF1E::3 mvlan 100 user-vlan 3

CN12800(config-10ge1/0/2)#quit

7.配置完成，检查组播组表和出端口表信息

```
CN12800#show mld-snooping group
 Total Entry(s) : 3
 Group Address          MVlan     Pre-join MemNum V2FilterMode
 ff1e::1                100       disable  2      invalid
 ff1e::2                100       disable  2      invalid
 ff1e::3                100       disable  2      invalid

CN12800#show mld-snooping egress-port
Total Entry(s) : 6

Group Address : ff1e::1
MVlan : 100
Source Address : *
Interface : ge-1/0/2
   Type : static
   Expires : ---
   OutVlan :   100
   V2 Mode : invalid
Group Address : ff1e::1
MVlan : 100
Source Address : *
Interface : ge-1/0/3
   Type : static
   Expires : ---
   OutVlan :   100
   V2 Mode : invalid
```

Group Address : ff1e::2

MVlan : 100

Source Address : *

Interface : ge-1/0/2

Type : static

Expires : ---

OutVlan : 100

V2 Mode : invalid

Group Address : ff1e::2

MVlan : 100

Source Address : *

Interface : 10ge-1/0/3

Type : static

Expires : ---

OutVlan : 100

V2 Mode : invalid

Group Address : ff1e::3

MVlan : 100

Source Address : *

Interface : 10ge-1/0/2

Type : static

Expires : ---

OutVlan : 100

V2 Mode : invalid

Group Address : ff1e::3

MVlan : 100

Source Address : *

Interface : 10ge-1/0/3

Type : static

Expires : ---

OutVlan : 100

V2 Mode : invalid

第7章 安全配置

本章介绍了 CN12800 系列数据中心交换机安全性相关的基本内容、配置过程和配置举例。

7.1 Time-range 配置

7.1.1 Time-range 概述

背景信息

Time-range 模块是一个定时模块，可以配合 ACL 等功能使用，限制命令起作用的时间范围。

7.1.2 进入 Time-range 模块及配置其名称

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
进入某条 time-range 模块	1. 进入全局配置视图； 2. 执行命令 **time-range list** *list-number* 用来进入某条 time-range 模块。
定义某条特定 time-range 模块的描述性名称	1. 进入全局配置视图； 2. 执行命令 **time-range list** *list-number* 用来进入某条 time-range 模块； 3. 执行命令 **name** *name* 用来定义某条特定 time-range 模块的描述性名称。
删除特定 time-range 模块里的 range 配置信息	1. 进入全局配置视图； 2. 执行命令 **time-range list** *list-number* 用来进入某条 time-range 模块； 3. 执行命令 **no time-range** *range-number* 用来删除特定 time-range 模块里的 range 配置信息。

7.1.3 配置 Time-range 模块起始时间范围

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
配置 time-range 模块起始结束的绝对时间	1. 进入全局配置视图； 2. 执行命令 **time-range list** *list-number* 用来进入某条 time-range 模块； 3. 执行命令 **time-range** *range-number* **absolute** { **from** | **to** } hh:mm:ss YY/MM/DD 或 **time-range** *range-number* **absolute from** hh:mm:ss YY/MM/DD **to** hh:mm:ss YY/MM/DD 用来配置 time-range 模块起始结束的绝对时间。
配置 time-range 模块每日时间范围	1. 进入全局配置视图； 2. 执行命令 **time-range list** *list-number* 用来进入某条 time-range 模块； 3. 执行命令 **time-range** *range-number* **everyday** *hh:mm:ss* **to** *hh:mm:ss* 用来配置 time-range 模块每日时间范围。
配置 time-range 模块每小时时间范围	1. 进入全局配置视图； 2. 执行命令 **time-range list** *list-number* 用来进入某条 time-range 模块； 3. 执行命令 **time-range** *range-number* **everyhour** *mm:ss* **to** *mm:ss* 用来配置 time-range 模块每小时时间范围。
配置 time-range 模块每月时间范围	1. 进入全局配置视图； 2. 执行命令 **time-range list** *list-number* 用来进入某条 time-range 模块； 3. 执行命令 **time-range** *range-number* **everymonth** *hh:mm:ss mm* **to** *hh:mm:ss mm* 用来配置 time-range 模块每月时间范围。
配置 time-range 模块每周时间范围	1. 进入全局配置视图； 2. 执行命令 **time-range list** *list-number* 用来进入某条 time-range 模块； 3. 执行命令 **time-range** *range-number* **everyweek** *hh:mm:ss* { **mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun** } **to** *hh:mm:ss* { **mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun** }用来配置 time-range 模块每周时间范围。
配置 time-range 模块每周除周末以外的时间范围	1. 进入全局配置视图； 2. 执行命令 **time-range list** *list-number* 用来进入某条 time-range 模块； 3. 执行命令 **time-range** *range-number* **everyweekday** *hh:mm:ss* **to** *hh:mm:ss* 用来配置 time-range 模块每周除周末以外的时间范围。
配置 time-range 模块每周末的时间范围	1. 进入全局配置视图； 2. 执行命令 **time-range list** *list-number* 用来进入某条 time-range 模块； 3. 执行命令 **time-range** *range-number* **everyweekend** *hh:mm:ss* **to** *hh:mm:ss* 用来配置 time-range 模块每周末的时间范围。
配置 time-range 模块每年的时间范围	1. 进入全局配置视图； 2. 执行命令 **time-range list** *list-number* 用来进入某条 time-range 模块； 3. 执行命令 **time-range** *range-number* **everyyear** *hh:mm:ss mm/dd* **to** *hh:mm:ss mm/dd* 用来配置 time-range 模块每年的时间范围。

7.1.4 维护及调试

目的

当 Time-range 功能不正常，需要进行查看、定位问题时，可以使用本小节操作。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
打开或关闭 time-range 的调试功能	1. 进入特权用户视图； 2. 执行命令 **debug time-range** 或 **no debug time-range** 打开或关闭 time-range 的调试功能。
查看当前所有 time-range 模块的配置信息	1. 进入特权用户视图、全局配置视图或执行命令 **time-range list** *list-number* 用来进入某条 time-range 模块； 2. 执行命令 **show time-range config** 用来显示当前所有 time-range 模块的配置信息。
查看当前所有或指定的 time-range 模块的列表信息	1. 进入特权用户视图、全局配置视图，或执行命令 **time-range list** *list-number* 用来进入某条 time-range 模块； 2. 执行命令 **show time-range list** 或 **show time-range list** *list-number* 用来显示当前所有或指定的 time-range 模块的列表信息。

7.2 IP 地址前缀过滤配置

7.2.1 地址前缀过滤表概述

为实现选择性使用不同路径获得的 IP 路由项，地址前缀列表基于路由地址域（IP 地址、地址前缀长度范围、应用规则）提供有序的过滤规则集。不同协议匹配路由项目的地址域，达到路由过滤的目的。

在 IPv4 使用范围内，同一地址类型前提下，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 index 的配置有自动分配和手动分配两种方式，索引号指明了进行匹配检查的顺序。

在匹配的过程中，按升序依次检查由 index 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，不再进行下一个表项的匹配。

 **注意：**

地址前缀列表的多个表项上的配置先后逻辑顺序错误会导致匹配异常，需要操作人员配置时保证正确性。

7.2.2 配置地址前缀过滤表

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
创建一条过滤规则，完全匹配前 MASKLEN 长度的网段地址	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **ip prefix-list** *list-name* [**index** *index-number*] { **deny** | **permit** } *ip-address/mask-length* 用来创建一条过滤规则，完全匹配前 MASKLEN 长度的网段地址。
创建一条过滤规则，路由地址掩码长度大于等于指定的最小值且完全匹配前缀掩码长度的网段地址	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **ip prefix-list** *list-name* [**index** *index-number*] { **deny** | **permit** } *ip-address/mask-length* **greater-equal** *min-range* 用来创建一条过滤规则，路由地址掩码长度大于等于指定的最小值且完全匹配前缀掩码长度的网段地址。
创建一条过滤规则，路由地址掩码长度小于等于指定的最大值且完全匹配前缀掩码长度的网段地址	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **ip prefix-list** *list-name* [**index** *index-number*] { **deny** | **permit** } *ip-address/mask-length* **less-equal** *max-range* 用来创建一条过滤规则，路由地址掩码长度小于等于指定的最大值且完全匹配前缀掩码长度的网段地址。
创建一条过滤规则，路由地址掩码长度小于等于指定的最小值与最大值范围内且完全匹配前缀掩码长度的网段地址	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **ip prefix-list** *list-name* [**index** *index-number*] { **deny** | **permit** } *ip-address/mask-length* **greater-equal** *min-range* **less-equal** *max-range* 用来创建一条过滤规则，路由地址掩码长度小于等于指定的最小值与最大值范围内且完全匹配前缀掩码长度的网段地址。

7.2.3 维护及调试

目的

当地址前缀过滤表功能不正常，需要进行查看、调试或定位问题时，可以使用本小节操作。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
打开 IP 地址前缀过滤表的调试功能	1. 不执行任何命令保持当前特权用户视图； 2. 执行命令 **debug prefix-list** { **config** | **match** | **error** | **all** }打开 IP 地址前缀过滤表的调试功能。
关闭 IP 地址前缀过滤表的调试功能	1. 不执行任何命令保持当前特权用户视图； 2. 执行命令 **no debug prefix-list** { **config** | **match** | **error** | **all** }关闭 IP 地址前缀过滤表的调试功能。
删除已创建的一条过滤规则	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **no ip prefix-list** *list-name* [**index** *index-number*]用来删除已创建的一条过滤规则。
查看规则表中的规则	1. 执行命令 **disable** 退出到普通用户视图或执行命令 **configure** 进入全局配置视图或不执行任何命令保持当前特权用户视图； 2. 执行命令 **show** { **ip** | **ipv6** } **prefix-list** [*list-name*]用来显示规则表中的规则。
查看 IP 地址前缀规则信息	1. 执行命令 **disable** 退出到普通用户视图或执行命令 **configure** 进入全局配置视图或不执行任何命令保持当前特权用户视图； 2. 执行命令 **show ip prefix-list information** 用来显示 IP 地址前缀规则信息。

7.3 ACL 配置

说明：

本小节中，ACL 指用于过滤 IPv4 报文的访问控制列表。

7.3.1 ACL 概述

ACL 功能

CN12800 通过配置访问控制列表 ACL（Access Control List）的规则和动作来决定什么样的数据包能够通过，什么样的数据包要拒绝等，从而实现控制数据的传输、提高网络性能、保障业务安全。

ACL 是由二层 MAC，三层 IP 组成的一系列有顺序的规则和动作，这些规则根据数据包的源地址、目的地址、端口号等来对数据包进行过滤。ACL 通过这些规则对数据包进行

分类，这些规则应用到 CN12800 上，CN12800 根据这些规则判断哪些数据包可以接收，哪些数据包需要拒绝以及其他动作。

CN12800 支持的 ACL 分类

CN12800 支持二层 ACL，三层 ACL，混合 ACL。

- 二层 ACL：主要基于源 MAC 地址，目的 MAC 地址，VLAN，优先级，协议类型、限速模板、时间段模板等信息对数据包进行分类定义。
- 三层 ACL：主要基于源 IP 地址，目的 IP 地址，源端口号、目的端口号、协议类型、优先级、分片、生存时间、限速模板、时间段模板等信息对数据包进行更为细致的分类定义。
- 混合 ACL：主要基于源 MAC 地址，目的 MAC 地址，源 IP 地址，目的 IP 地址，源端口号，目的端口号，协议类型，优先级，VLAN、限速模板、时间段模板等信息对数据包进行分类定义。

7.3.2 配置二层 ACL

背景信息

一条 ACL 是由若干规则和动作组成的一系列的列表，若干个规则列表构成一条 ACL。

配置二层 ACL 的规则之前，首先需要创建一条二层 ACL 并指定 ACL 种类标示编号为 1~1000。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
创建一条二层 ACL	1. 进入全局配置视图； 2. 执行命令 **filter-list** *acl-number* [**name** *filter-name*]使用编号创建一条二层 ACL（访问控制列表），并进入二层 ACL 配置视图。
配置二层 ACL 规则	1. 进入全局配置视图； 2. 进入二层 ACL 配置视图； 3. 执行如下命令用来配置 MAC 条目匹配的 ACL 规则（用户根据需要自行从如下命令中选择配置）； ● **filter** *rule-number* **mac {** *src-mac-address/M* **| any } {** *dst-mac-address/M* **| any }** ● filter *rule-number* **mac** { *src-mac-address/M* | **any** } { *dst-mac-address/M* | **any** } { **customer | provider }** { **any** | *vlan-id* | *vlan-id1/vlan-id2* } { **any** | *priority* }

目的	步骤
	● **filter** *rule-number* **src-mac** *src-mac-address* **src-mask** *src-mac-mask* **dst-mac** *dst-mac-address* **dst-mask** *dst-mac-mask* **{ customer | provider } { any |** *vlan-id* **|** *vlan-id1/vlan-id2* **} { any |** *priority* **}** ● **filter** *rule-number* **mac** { *src-mac-address/M* | **any** } { *dst-mac-address/M* | **any** } **eth-type** { **ip** | **arp** | *digitial-protocol-value* } ● **filter** *rule-number* **mac** { *src-mac-address/M* | **any** } { *dst-mac-address/M* | **any** } **provider** { **any** | *vlan-id* } { **any** | *priority* } **customer** { **any** | *vlan-id* } { **any** | *priority* } ● **filter** *rule-number* **mac { src-mac-address/M | any } { dst-mac-address/M | any } provider { vlan-id1/vlan-id2 } { any |** *priority* **} customer { any |** *vlan-id* **} { any |** *priority* **}** ● **filter** *rule-number* **mac** { *src-mac-address/M* | **any**) { *dst-mac-address/M* | **any**) **provider** { **any** | *vlan-id* } { **any** | *priority* } **customer** { *vlan-id1/vlan-id2* } { **any** | *priority* } ● **filter** *rule-number* **src-mac** { *src-mac-address/M* | **any** } **src-mask** *src-mac-mask* **dst-mac** *dst-mac-address* **dst-mask** *dst-mac-mask* **provider** { **any** | *vlan-id* } { **any** | *priority* } **customer** { **any** | *vlan-id*) { **any** | *priority* } ● **filter** *rule-number* **src-mac** { *src-mac-address/M* | **any** } **src-mask** *src-mac-mask* **dst-mac** *dst-mac-address* **dst-mask** *dst-mac-mask* **provider** { *vlan-id1/vlan-id2* } { **any** | *priority* } **customer** { **any** | *vlan-id* } { **any** | *priority* } ● **filter** *rule-number* **src-mac { src-mac-address/M | any } src-mask** *src-mac-mask* **dst-mac** *dst-mac-address* **dst-mask** *dst-mac-mask* **provider { any |** *vlan-id* **} { any |** *priority* **} customer {** *vlan-id1/vlan-id2***) { any |** *priority* **}**。
配置二层 ACL 动作	1. 进入全局配置视图； 2. 进入二层 ACL 配置视图； 3. 执行如下命令配置 ACL 处理动作： ● **filter** *rule-number* **action** { **permit | deny** } ● **filter** *rule-number* **action redirect cpu** ● **filter** *rule-number* **action cpu** ● **filter** *rule-number* **action cpu queue** *queue-index* ● **filter** *rule-number* **action mac-no-learning** ● **filter** *rule-number* **action mirror group** *group-number* ● **filter** *rule-number* **action redirect { ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* ● **filter** *rule-number* **action redirect eth-trunk** *trunk-number* ● **filter** *rule-number* **action** { **cos | precedence | priority** } *priority-value* ● **filter** *rule-number* **action dscp** *dscp*。

目的	步骤
删除 ACL 动作	1. 进入全局配置视图； 2. 进入 ACL 配置视图； 3. 执行命令 **no filter** *rule-number* **action** 用来删除 ACL 规则对应的处理动作。
删除 ACL 规则	1. 进入全局配置视图； 2. 进入 ACL 配置视图； 3. 执行命令 **no filter** *rule-number* 用来删除 ACL 规则。
删除 ACL 访问控制列表	1. 进入全局配置视图； 2. 进入 ACL 配置视图； 3. 执行命令 **no filter-list** *acl-number* 用来删除 ACL 访问控制列表。
绑定二层 ACL	1. 进入全局配置视图； 2. 进入以太网接口配置视图或二层 ACL 配置视图，执行以下命令用来将 ACL 应用到物理端口，trunk 接口或者 VLAN 端口； ● **filter-list-l2** { **in** | **out** } *acl-number* ● **filter-list-l2** { **in** | **out** } **name** *acl-name*。 或 1. 进入全局配置视图； 2. 执行命令 **filter-list-l2 global** { **in** | **out** } *acl-number* 全局绑定 ACL。

7.3.3 配置三层 ACL

背景信息

一条 ACL 是由若干规则和动作组成的一系列的列表，若干个规则列表构成一条 ACL。

配置三层 ACL 的规则之前，首先需要创建一条三层 ACL 并指定 ACL 种类标示编号为 1001~2000。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
创建一条三层 ACL	1. 进入全局配置视图； 2. 执行命令 **filter-list** *acl-number* [**name** *filter-name*]使用编号创建一条三层 ACL（访问控制列表），并进入三层 ACL 配置视图。
配置三层 ACL 规则	1. 进入全局配置视图； 2. 进入三层 ACL 配置视图； 【用户可以从步骤 3~步骤 8 中根据需要任选配置】 3. （可选）执行如下命令用来配置 IP 匹配的 ACL 规则（用户根据需要自行从如下命令中选择配置）；

目的	步骤
	● **filter** *rule-number* **ip** { *src-ip-address/M* | **any** } { *dst-ip-address/M* | **any** } ● **filter** *rule-number* **src-ip** { *src-ip-address* | **any** } **src-mask** { *src-ip-mask* | **any** } **dst-ip** { *dst-ip-address* | **any** } **dst-mask** { *dst-ip-mask* | **any** } [**fragment**] ● **filter** *rule-number* **ip** { *src-ip-address/M* | **any**} { *dst-ip-address/M* | **any** } **precedence** *ip-precedence* [**fragment**] ● **filter** *rule-number* **src-ip** { *src-ip-address* | **any** } **src-mask {** *src-ip-mask* | **any** } **dst-ip** { *dst-ip-address* | **any** } **dst-mask {***dst-ip-mask* | **any** } **precedence** *ip-precedence* [**fragment**] ● **filter** *rule-number* **ip** { *src-ip-address/M* | **any** } { *dst-ip-address/M* | **any** } **dscp** *dscp* [**fragment**] ● **filter** *rule-number* **src-ip** { *src-ip-address* | **any** } **src-mask {***src-ip-mask* | **any**} **dst-ip {***dst-ip-address* | **any** } **dst-mask {** *dst-ip-mask* | **any** } **dscp** *dscp* [**fragment**] ● **filter** *rule-number* **ip** { *src-ip-address/M* | **any**} { *dst-ip-address/M* | **any** } **fragment** ● **filter** *rule-number* **src-ip** { *src-ip-address* | **any** } **src-mask {** *src-ip-mask* | **any**} **dst-ip {** *dst-ip-address* | **any** } **dst-mask {** *dst-ip-mask* | **any** } **fragment** ● **filter** *rule-number* **ip** { *src-ip-address/M* **| any** } { *dst-ip-address/M* **| any** } **tos** *tos-value* ● **filter** *rule-number* **ip** { *src-ip-address/M* **| any** } { *src-ip-address/M* **| any** } **proto-type** *proto-type-value* ● **filter** *rule-number* **src-ip** { *src-ip-address* | **any** } **src-mask** { *src-ip-mask* | **any** } **dst-ip** { *dst-ip-address* | **any** } **dst-mask** { *dst-ip-mask* | **any** } **proto-type** *proto-type-value* ● **filter** *rule-number* **ip** { *src-ip-address/M* | **any** } { *dst-ip-address/M* | **any** } **ttl** *ttl-value* ● **filter** *rule-number* **src-ip** { *src-ip-address* | **any** } **src-mask {** *src-ip-mask* | **any** } **dst-ip** { *dst-ip-address* | **any** } **dst-mask** { *dst-ip-mask* | **any** } **ttl** *ttl-value* ● **filter** *rule-number* **src-ip** *src-ip-address* **src-port** *src-port-id* **dst-ip** *dst-ip-address* **dst-port** *dst- port-id* 4. （可选）执行如下命令用来配置 TCP 匹配的 ACL 规则（用户根据需要自行从如下命令中选择配置）； ● **filter** *rule-number* **tcp** { *src-ip-address/M* | **any** } { *src-port-number* | **any** | *source-port-number-range* } { *dst-ip-address/M* | **any** } { *dst-port-number* | **any** | *destination-port-number-range* } ● **filter** *rule-number* **tcp** { *src-ip-address/M* | **any** } { *src-port-number* | **any** | *source-port-number-range* } { *dst-ip-address/M* | **any** } { *dst-port-number* | **any** | *destination-port-number-range* } { **syn** | **synack** | **ack** | **fin** }

目的	步骤
	● **filter** *rule-number* **tcp** { *src-ip-address/M* | **any** } { *src-port-number* | **any** | *source-port-number-range* } { *dst-ip-address/M* | **any** } { *dst-port-number* | **any** | *destination-port-number-range* } { **syn** | **synack** | **ack** | **fin** } **fragment** ● **filter** *rule-number* **tcp** { *src-ip-address/M* | **any** } { *src-port-number* | **any** | *source-port-number-range* } { *dst-ip-address/M* | **any** } { *dst-port-number* | **any** | *destination-port-number-range* } **fragment** ● **filter** *rule-number* **tcp src-ip** { *src-ip-address* | **any** } **src-mask** { *src-ip-mask* | **any** } { *src-port-number* | *source-port-number-range/destination-port-number-range* | **any** } **dst-ip** { *src-ip-mask* | **any** } **dst-mask** { *dst-ip-mask* | **any** } { *dst-port-number* | **any** | *source-port-number-range/destination-port-number-range* } [**fragment**] ● **filter** *rule-number* **tcp src-ip** { *src-ip-address* | **any** } **src-mask** { *src-ip-mask* | **any** } { *src-port-number* | *source-port-number-range/destination-port-number-range* | **any** } **dst-ip** { *src-ip-mask* | **any** } **dst-mask** { *dst-ip-mask* | **any** } { *dst-port-number* | **any** | *source-port-number-range/destination-port-number-range* } { **syn** | **synack** | **ack** | **fin** } [**fragment**] 5. （可选）执行如下命令用来配置 ICMP 匹配的 ACL 规则（用户根据需要自行从如下命令中选择配置）； ● **filter** *rule-number* **icmp** { *src-ip-address/M* | **any** } { *dst-ip-address/M* | **any** } ● **filter** *rule-number* **icmp src-ip** { *src-ip-address* | **any** } **src-mask** { *src-ip-mask* | **any** } **dst-ip** { *src-ip-mask* | **any** } **dst-mask** { *dst-ip-mask* | **any** } ● **filter** *rule-number* **icmp** { *src-ip-address/M* | **any** } { *dst-ip-address/M* | **any** } { *icmp type* | **any** } { *icmp code* | **any** } ● **filter** *rule-number* **icmp src-ip** *src-ip-address* **src-mask** { *src-ip-mask* | **any** } **dst-ip** { *src-ip-mask* | **any** } **dst-mask** { *dst-ip-mask* | **any** } { *icmp type* | **any** } { *icmp code* | **any** } ● **filter** *rule-number* **icmp** { *src-ip-address/M* | **any** } { *dst-ip-address/M* | **any** } { *icmp type* | **any** } { *icmp code* | **any** } **fragment** ● **filter** *rule-number* **icmp src-ip** *src-ip-address* **src-mask** { *src-ip-mask* | **any** } **dst-ip** { *dst-ip-mask* | **any** } **dst-mask** { *dst-ip-mask* | **any** } { *icmp type* | **any** } { *icmp code* | **any** } **fragment** 6. （可选）执行如下命令用来配置 IGMP 匹配的 ACL 规则（用户根据需要自行从如下命令中选择配置）； ● **filter** *rule-number* **igmp** { *src-ip-address/M* | **any** } { *dst-ip-address/M* | **any** } ● **filter** *rule-number* **igmp src-ip** { *src-ip-address/M* | **any** } **src-mask** { *src-ip-mask* | **any** } **dst-ip** { *src-ip-mask* | **any** } **dst-mask** { *dst-ip-mask* | **any** } ● **filter** *rule-number* **igmp** { *src-ip-address/M* | **any** } { *dst-ip-address/M* | **any** } **fragment**

目的	步骤
	● **filter** *rule-number* **igmp src-ip** { *src-ip-address/M* | **any** } **src-mask** { *src-ip-mask* | **any** } **dst-ip** { *dst-ip-address* | **any** } **dst-mask** { *dst-ip-mask* | **any** } 7. （可选）执行如下命令用来配置 UDP 匹配的 ACL 规则（用户根据需要自行从如下命令中选择配置）： ● **filter** *rule-number* **udp** { *src-ip-address/M* | **any** } { *src-port-number* | **any** | *source-port-number-range* } { *dst-ip-address/M* | **any** } { *dst-port-number* | **any** | *destination-port-number-range* } [**fragment**]。
配置三层 ACL 动作	1. 进入全局配置视图； 2. 进入三层 ACL 配置视图； 3. 执行如下命令配置 ACL 处理动作； ● **filter** *rule-number* **action** { **permit** | **deny** } ● **filter** *rule-number* **action redirect cpu** ● **filter** *rule-number* **action cpu** ● **filter** *rule-number* **action cpu queue** *queue-index* ● **filter** *rule-number* **action mac-no-learning** ● **filter** *rule-number* **action ip urpf disable** ● **filter** *rule-number* **action mirror group** *group-number* ● **filter** *rule-number* **action redirect { ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* ● filter *rule-number* **action redirect eth-trunk** *trunk-number* ● **filter** *rule-number* **action** { **cos** | **precedence** | **priority** } *priority-value* ● **filter** *rule-number* **action dscp** *dscp* ● **filter** *rule-number* **action counter** *counter number* ● **filter** *rule-number* **action tos** *tos number*。
绑定三层 ACL	1. 进入全局配置视图； 2. 进入以太网接口配置视图，执行以下命令用来将 ACL 应用到物理端口，trunk 接口或者 VLAN 端口； ● **filter-list-ipv4** { **in** | **out** } *acl-number* ● **filter-list-ipv4** { **in** | **out** } **name** *acl-name*。 或 1. 进入全局配置视图； 2. 执行 **filter-list-ipv4 global** { **in** | **out** } *acl-number* 命令全局绑定 ACL。

7.3.4 配置混合 ACL

背景信息

一条 ACL 是由若干规则和动作组成的一系列的列表，若干个规则列表构成一条 ACL。

配置混合 ACL 的规则之前，首先需要创建一条混合 ACL 并指定 ACL 种类标示编号为 2001~3000。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
创建一条混合 ACL	1. 进入全局配置视图； 2. 执行命令 **filter-list** *acl-number* [**name** *filter-name*]使用编号创建一条混合 ACL（访问控制列表），并进入混合 ACL 配置视图。
配置混合 ACL 规则	1. 进入全局配置视图； 2. 进入混合 ACL 配置视图； 3. 混合模式可以配置二层和三层的 ACL 规则，请参考本手册 7.3.2 和 7.3.3 小节 ACL 规则的配置命令。
配置混合 ACL 动作	1. 进入全局配置视图； 2. 进入混合 ACL 配置视图； 3. 执行如下命令配置 ACL 处理动作； ● **filter** *rule-number* **action { permit | deny }** ● **filter** *rule-number* **action redirect cpu** ● **filter** *rule-number* **action cpu** ● **filter** *rule-number* **action cpu queue** *queue-index* ● **filter** *rule-number* **action mac-no-learning** ● **filter** *rule-number* **action ip urpf disable** ● **filter** *rule-number* **action mirror group** *group-number* ● filter *rule-number* **action redirect { ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* ● **filter** *rule-number* **action** { **cos** | **precedence** | **priority** } *priority-value* ● **filter** *rule-number* **action dscp** *dscp* ● **filter** *rule-number* **action counter** *counter number* ● **filter** *rule-number* **action tos** *tos number*。
绑定混合 ACL	1. 进入全局配置视图； 2. 进入以太网接口配置视图，执行以下命令用来将 ACL 应用到物理端口，trunk 接口或者 VLAN 端口； ● **filter-list-hybrid** { **in** | **out** } *acl-number* ● **filter-list-hybrid** { **in** | **out** } **name** *acl-name*。 或 1. 进入全局配置视图； 2. 执行 **filter-list-hybrid global** { **in** | **out** } *acl-number* 命令全局绑定 ACL。

7.3.5 配置三层 ACL6

背景信息

一条 ACL 是由若干规则和动作组成的一系列的列表，若干个规则列表构成一条 ACL。

配置三层 ACL6 的规则之前，首先需要创建一条三层 ACL6 并指定 ACL6 种类标示编号为 3001~4000。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
创建一条三层 ACL6	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **filter-list** *acl-number* 使用编号创建一条三层 ACL6（访问控制列表），并进入三层 ACL6 配置视图。
配置三层 ACL6 规则	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **filter-list** *acl-number* 进入三层 ACL6 配置视图； 【用户可以从步骤 3~步骤 8 中根据需要任选配置】 3. （可选）执行以下命令用来配置 IP6 匹配的 ACL 规则（用户根据需要自行从以下命令中选择配置）； ● **filter** *rule-number* **ip6** { *src-ip6-address/M* | **any** } { *dst-ip6-address/M* | **any** } ● **filter** *rule-number* **ip6** { *src-ip6-address/M* | **any** } { *dst-ip6-address/M* | **any** } **next-header** *next-header-value* ● **filter** *rule-number* **ip6** { *src-ip6-address/M* | **any** } { *dst-ip6-address/M* | **any** } **hop-limit** *hop-limit-value* 4. （可选）执行以下命令用来配置 TCP6 匹配的 ACL 规则（用户根据需要自行从以下命令中选择配置）； ● **filter** *rule-number* **tcp6** { *src-ip6-address/M* | **any** } { *src-port-number* | **any** | *src-port-range* } { *dst-ip6-address/M* | **any** } { *dst-port-number* | **any** | *dst-port-range* } ● **filter** *rule-number* **tcp6** { *src-ip6-address/M* | **any** } { *src-port-number* | **any** | *src-port-range* } { *dst-ip6-address/M* | **any** } { *dst-port-number* | **any** | *dst-port-range* } **fragment** ● **filter** *rule-number* **tcp6** { *src-ip6-address/M* | **any** } { *src-port-number* | **any** | *src-port-range* } { *dst-ip6-address/M* | **any** } { *dst-port-number* | **any** | *dst-port-range* } { **syn** | **synack** | **ack** | **fin** } ● **filter** *rule-number* **tcp6** { *src-ip6-address/M* | **any** } { *src-port-number* | **any** | *src-port-range* } { *dst-ip6-address/M* | **any** } { *dst-port-number* | **any** | *dst-port-range* } { **syn** | **synack** | **ack** | **fin** } **fragment**

目的	步骤
	5. （可选）执行以下命令用来配置 ICMP6 匹配的 ACL 规则（用户根据需要自行从以下命令中选择配置）； ● **filter** *rule-number* **icmp6** { *src-ip6-address/M* | **any** } { *dst-ip6-address/M* | **any** } ● **filter** *rule-number* **icmp6** { *src-ip6-address/M* | **any** } { *dst-ip6-address/M* | **any** } { *icmp-type* | **any** } { *icmp-code* | **any** } [**fragment**] 6. （可选）执行以下命令用来配置 IGMP6 匹配的 ACL 规则（用户根据需要自行从以下命令中选择配置）； **filter** *rule-number* **igmp6** { *src-ip6-address/M* | **any** } { *dst-ip6-address/M* | **any** } [**fragment**] 7. （可选）执行以下命令用来配置 UDP6 匹配的 ACL 规则（用户根据需要自行从以下命令中选择配置）； ● **filter** *rule-number* **udp6** { *src-ip6-address/M* | **any** } { *src-port-number* | **any** | *src-port-range* } { *dst-ip6-address/M* | **any** } { *dst-port-number* | **any** | *dst-port-range* } ● **filter** *rule-number* **udp6** { *src-ip6-address/M* | **any** } { *src-port-number* | **any** | *src-port-range* } { *dst-ip6-address/M* | **any** } { *dst-port-number* | **any** | *dst-port-range* } **fragment**。
配置三层 ACL6 动作	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **filter-list** *acl-number* 进入三层 ACL6 配置视图； 3. 执行以下命令配置 ACL 处理动作； ● **filter** *rule-number* **action redirect cpu** ● **filter** *rule-number* **action cpu** ● **filter** *rule-number* **action cpu queue** *queue-index* ● **filter** *rule-number* **action mac-no-learning** ● **filter** *rule-number* **action ip urpf disable** ● **filter** *rule-number* **action mirror group** *group-number* ● **filter** *rule-number* **action redirect** { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* ● **filter** *rule-number* **action redirect eth-trunk** *trunk-number* ● **filter** *rule-number* **action dscp** *dscp-value* ● **filter** *rule-number* **action counter** *counter-number* ● **filter** *rule-number* **action tos** *tos number*。
绑定三层 ACL6	1. 进入全局配置视图； 2. 进入以太网接口配置视图，执行以下命令用来将 ACL 应用到物理端口，trunk 接口或者 VLAN 端口； ● **filter-list-ipv6** { **in** | **out** } *acl-number* ● **filter-list-ipv6** { **in** | **out** } **name** *acl-name*。

目的	步骤
	或 1. 进入全局配置视图； 2. 执行 **filter-list-ipv6 global** { **in** | **out** } *acl-number* 命令全局绑定 ACL。

7.3.6 配置 ACL 模式版本

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
配置 ACL 模式	1. 进入 L2 Filter 配置视图、Filter 配置视图（IPv4）或 filter-hybrid 配置视图； 2. 执行命令 **filter mode** { **tcam** | **mdb** }配置 ACL 模式。
配置 ACL 模式版本	1. 进入全局配置视图； 2. 执行命令 **assign filter mode** *mode* **slot** { *slot-list* | **all** }配置 ACL 模式版本。

7.3.7 配置 ACL 可选功能项

背景信息

ACL 可选功能项包括：

- 创建 ACL 生效时间段

  创建 ACL 生效时间段以后，当配置 ACL 规则时引用该时间段，该 ACL 规则才会在这个时间段内生效；如果配置规则时不指定时间段，则该规则不受时间范围限制，除非删除该 ACL。

- 创建 ACL 限速模板

  创建限速模板之后，当配置 ACL 规则时与限速模板绑定，该 ACL 规则才会根据不同的限速规则对数据包进行过滤。

- 创建 ACL 计数模板

  创建计数模板之后，当配置 ACL 规则时与计数模板绑定，该 ACL 规则才会根据不同的计数类型对数据包进行统计。

目的

根据实际应用情况，配置 ACL 可选项功能可以为用户提供丰富的数据包过滤方法。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
创建 ACL 生效时间段	1. 进入全局配置视图； 2. 执行命令 **time-range list** *LIST-NUMBER* 用来进入某条 time-range 配置视图； 3. 执行如下命令配置 time-range 模块起始结束的绝对时间： ● **time-range** *range-number* **absolute from** *hh:mm:ss YY/MM/DD* ● **time-range** *range-number* **absolute from** *hh:mm:ss YY/MM/DD* ***to*** *hh:mm:ss YY/MM/DD*； 4. 执行命令 **time-range** *range-number* **everyday** *hh:mm:ss* **to** *hh:mm:ss* 用来配置 time-range 模块每日时间范围； 5. 执行命令 **time-range** *range-number* **everyhour** *mm:ss* **to** *mm:ss* 用来配置 time-range 模块每小时时间范围； 6. 执行命令 **time-range** *range-number* **everymonth** *hh:mm:ss MM* **to** *hh:mm:ss MM* 用来配置 time-range 模块每月时间范围； 7. 执行命令 **time-range** *range-number* **everyweek** *hh:mm:ss* { **mon | tue | wed | thu | fri | sat | sun** } **to hh:mm:ss** { **mon | tue | wed | thu | fri | sat | sun** }用来配置 time-range 模块每周时间范围； 8. 执行命令 **time-range** *range-number* **everyweekday** *hh:mm:ss* **to** *hh:mm:ss* 用来配置 time-range 模块每周除周末以外的时间范围； 9. 执行命令 **time-range** *range-number* **everyweekend** *hh:mm:ss* **to** *hh:mm:ss* 用来配置 time-range 模块每周末的时间范围； 10. 执行命令 **time-range** *range-number* **everyyear** *hh:mm:ss MM/DD* **to** *hh:mm:ss MM/DD* 用来配置 time-range 模块每年的时间范围； 11. 执行命令 **quit** 退出到全局配置视图； 12. 进入 ACL 配置视图； 13. 执行命令 **time-range list** *list-number* 用来时间段模板与 ACL 绑定。
创建 ACL 限速模板	1. 进入全局配置视图； 2. 执行如下命令配置 Meter 模板： ● **meter** *meter-number* **cir** *cir-number* **cbs** *cbs-number* **ebs** *ebs-number* ● **meter** *meter-number* **cir** *cir-number* **cbs** *cbs-number* **ebs** *ebs-number* { **aware | blind** } ● **meter** *meter-number* **cir** *cir-number* **cbs** *cbs-number* **pbs** *pbs-number* **pir** *pir-number* ● **meter** *meter-number* **cir** *cir-number* **cbs** *cbs-number* **pbs** *pbs-number* **pir** *pir-number* { **aware | blind** } 3. 进入 ACL 配置视图；

目的	步骤
	4. 执行命令 **filter** *filter rule number* **meter** *meter number* 用来配置 ACL 规则和某个 meter 模板绑定； 5. 执行如下命令配置根据限速模板着色后包的处理： ● **filter** *rule-number* **outaction { red | yellow } drop** ● **filter** *rule-number* **outaction { red | yellow } remark-dscp** *dscp* ● **filter** *rule-number* **outaction { red | yellow } remark-dot1p** *priority* ● **filter** *rule-number* **car** *car-value* **outaction drop**。
创建 ACL 计数模板	1. 进入全局配置视图； 2. 执行命令 **counter** *counter-number* { **packet | byte | all } sort { green | red | greenred | greenyellow | redyellow | total** }用来配置 Counter 模板； 3. 进入 ACL 配置视图； 4. 执行命令 **filter** *rule-number* **action counter** *counter-number* 用来配置计数模板与 ACL 绑定。

7.3.8 维护及调试

目的

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

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
清除 ACL 的统计信息	1. 进入全局配置视图； 2. 执行如下命令重置 ACL（访问控制列表）的过滤器条目计数： ● **reset counter filter-list** *acl-number* **filter** *rule-number* [**slot** *slot-id*] { **in | out** } ● **reset counter filter-list** *acl-number* **filter** *rule-number* **port { ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* { **in | out** } ● **reset counter filter-list** *acl-number* **filter** *rule-number* **port eth-trunk** *trunk-number* { **in | out** } ● **reset counter filter-list** *acl-number* **filter** *rule-number* **vlan** *vlan-id* { **in | out** }。

目的	步骤
查看访问控制列表的配置信息	1. 进入普通用户视图、特权用户视图、全局配置视图、filter 配置视图、接口配置视图（以太网接口、trunk 接口）、VLANIF 配置视图、接口组配置视图或批量接口配置视图； 2. 执行如下命令显示访问控制列表的配置信息： ● **show filter-list** ● **show filter-list** *acl-number* ● **show filter-list slot**。
查看访问控制列表配置文件信息	1. 进入普通用户视图、特权用户视图、全局配置视图、filter 配置视图、接口配置视图（以太网接口、trunk 接口）、VLANIF 配置视图、接口组配置视图或批量接口配置视图； 2. 执行命令 **show filter-list config** 显示 ACL 配置文件信息。
查看访问控制列表的统计信息	1. 进入普通用户视图、特权用户视图、全局配置视图、filter 配置视图、接口配置视图（以太网接口、trunk 接口）、VLANIF 配置视图、接口组配置视图或批量接口配置视图； 2. 执行命令 **show filter-list statistic** 用来显示访问控制列表的统计信息。
查看所有应用了访问控制列表的端口信息	1. 进入普通用户视图、特权用户视图、全局配置视图、filter 配置视图、接口配置视图（以太网接口、trunk 接口）、VLANIF 配置视图、接口组配置视图或批量接口配置视图； 2. 执行命令 **show filter-list interface** 显示所有应用了访问控制列表的端口信息。
查看访问控制列表全局配置情况	1. 进入普通用户视图、特权用户视图、全局配置视图、filter 配置视图、接口配置视图（以太网接口、trunk 接口）、VLANIF 配置视图、接口组配置视图或批量接口配置视图； 2. 执行命令 **show filter-list global** 访问控制列表全局配置情况。
查看统计表信息、配置信息	1. 进入特权用户视图、全局配置视图、普通用户视图、接口组配置视图或批量接口配置视图； 2. 执行如下命令显示统计表信息、配置信息： ● **show counter config** ● **show counter** *counter-id* ● **show counter**
查看指定槽位的 ACL TCAM 资源信息	1. 进入普通用户视图； 2. 执行命令 **show acl tcam resource slot** *slot-id* 查看指定槽位的 ACL TCAM 资源信息。
查看过滤模式	1. 进入普通用户视图； 2. 执行命令 **show filter mode slot** { *slot-id* | **all** }查看过滤模式。

7.3.9 配置举例

7.3.9.1 配置二层 ACL 示例

组网要求

CN12800 作为网关设备，下挂用户 PC。要求配置 ACL，禁止源 MAC 地址为 0001-0203-0405、目的 MAC 地址为 0102-0304-0506 的报文通过，如图 7-1 所示。

组网图

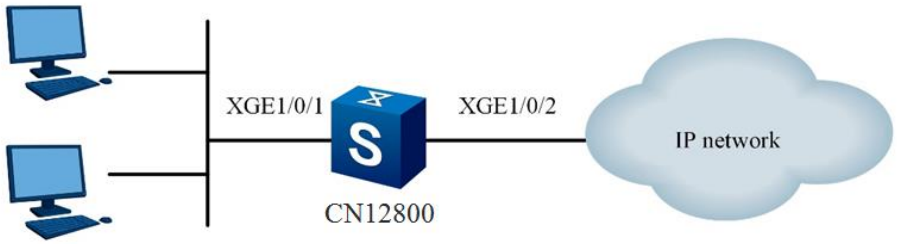


图 7-1 二层 ACL 示例图

配置步骤

1、创建二层 ACL。

CN12800#configure

CN12800(config)#filter-list 1

CN12800(configure-filter-l2-1)#

2、配置二层 ACL 规则。

CN12800(configure-filter-l2-1)#filter 1 mac 00:01:02:03:04:05/48 01:02:03:04:05:06/48

3、配置二层 ACL 动作。

CN12800(configure-filter-l2-1)#filter 1 action deny

4、端口绑定 ACL。

CN12800(configure-filter-l2-1)#quit

CN12800(config)#interface 10gigaethernet 1/0/1

CN12800(config-10ge1/0/1)#filter-list-l2 in 1

7.3.9.2 配置三层 ACL 示例

组网要求

公司企业网通过 Switch 实现各部门之间的互连。要求正确配置 IPv4 ACL，禁止研发部门、市场部门在上班时间（8:30 至 17:30）访问工资查询服务器（IP 地址为 10.164.9.9），而总裁办公室不受限制，可以随时访问，如图 7-2 所示。

组网图

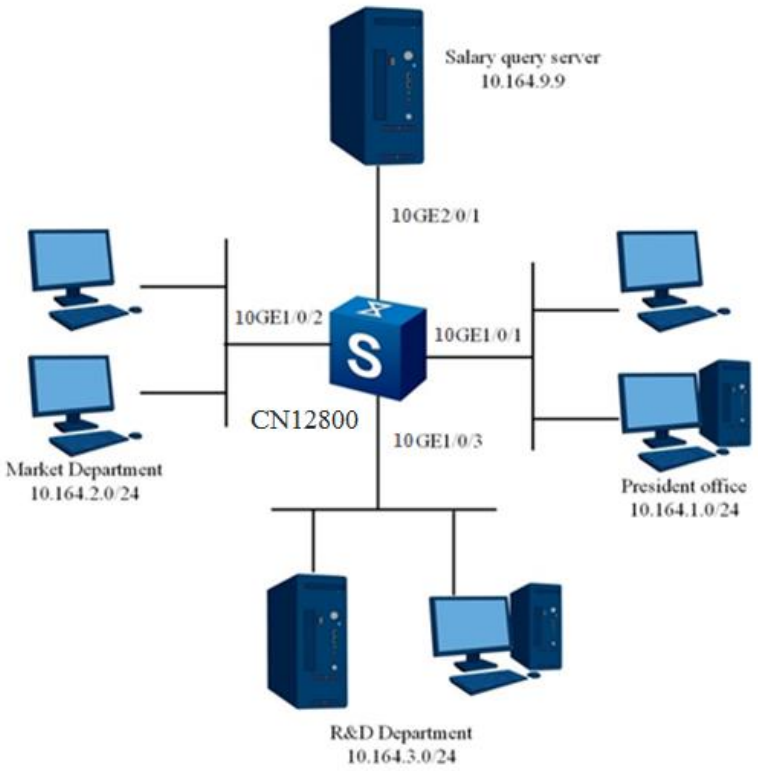


图 7-2 三层 ACL 示例图

配置步骤

1、配置 time-range。

CN12800#configure

CN12800(config)#time-range list 1

CN12800(config-timerange1)#time-range 1 everyweekday 8:30:00 to 17:30:00

CN12800(config-timerange1)#quit

2、配置总裁办公室允许访问工资查询服务器的 ACL。

CN12800(config)# filter-list 1001

CN12800(configure-filter-ipv4-1001)#filter 1 ip 10.164.1.0/24 10.164.9.9/32

CN12800(configure-filter-ipv4-1001)#filter 1 action permit

CN12800(configure-filter-ipv4-1001)#quit

3、配置市场部门在指定时间段内禁止访问工资查询服务器。

CN12800(config)#filter-list 1002

CN12800(configure-filter-ipv4-1002)#filter 1 ip 10.164.2.0/24 10.164.9.9/32

CN12800(configure-filter-ipv4-1002)#filter 1 time-range 1

CN12800(configure-filter-ipv4-1002)#filter 1 action deny

CN12800(configure-filter-ipv4-1002)#quit

4、配置研发部门在指定时间段内禁止访问工资查询服务器。

CN12800(configure)# filter-list 1003

CN12800(configure-filter-ipv4-1003)#filter 1 ip 10.164.3.0/24 10.164.9.9/32

CN12800(configure-filter-ipv4-1003)#filter 1 time-range 1

CN12800(configure-filter-ipv4-1003)#filter 1 action deny

CN12800(configure-filter-ipv4-1003)#quit

5、将 ACL 应用到端口上。

CN12800(config)#interface xgigaethernet 1/0/1

CN12800(config-10ge1/0/1)#filter-list-ipv4 in 1001

CN12800(config-10ge1/0/1)#quit

CN12800(config)#interface xgigaethernet 1/0/2

CN12800(config-10ge1/0/2)#filter-list-ipv4 in 1002

CN12800(config-10ge1/0/2)#quit

CN12800(config)#interface xgigaethernet 1/0/3

CN12800(config-10ge1/0/3)#filter-list-ipv4 in 1003

7.3.9.3 配置混合 ACL 示例

组网要求

CN12800 作为网关设备，下挂用户 PC。要求配置 ACL，将源 MAC 地址为 00:01:02:00:00:00/24 网段、源 IP 地址为 1:2:3:1/24 网段的报文送 CPU，如图 7-3 所示。

组网图

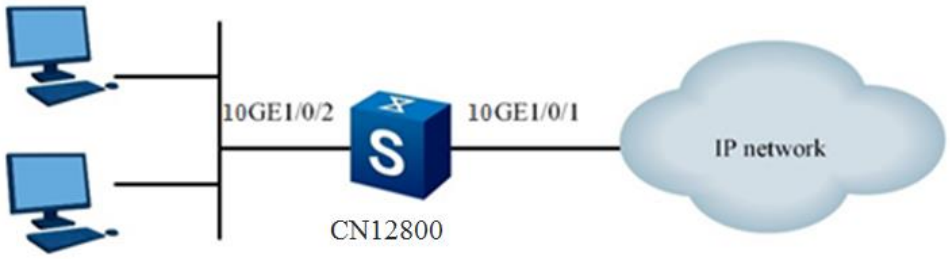


图 7-3 混合 ACL 示例图

配置步骤

1、创建混合 ACL。

CN12800#configure

CN12800(config)#filter-list 2001

CN12800(configure-filter-hybrid-2001)#

2、配置二层 ACL 规则。

CN12800(configure-filter-hybrid-2001)#filter 1 mac 00:01:02:00:00:00/24 any eth-type any provider any any customer any any ip 1.2.3.1/24 any proto-type any

3、配置二层 ACL 动作。

CN12800(configure-filter-hybrid-2001)#filter 1 action cpu

4、端口绑定 ACL。

CN12800(configure-filter-hybrid-2001)#quit

CN12800(config)#interface xgigaethernet 1/0/2

CN12800(config-10ge1/0/2)#filter-list-hybrid in 2001

7.3.9.4 配置限速模板示例

组网要求

CN12800 作为网关设备，下挂用户 PC。要求配置 ACL，对 CN12800 的 GE1/0/2 端口收到源 MAC 地址为 0001-0203-0405 的报文进行限速，黄色报文 dscp 的值修改为 AF11，如图 7-4 所示。

组网图

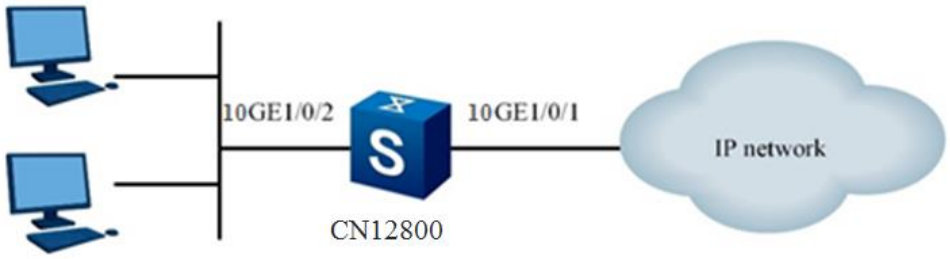


图 7-4 限速模板示例图

配置步骤

1、配置限速模板。

CN12800#configure

CN12800(config)#meter 1 cir 64 cbs 10000 pbs 10000 pir 64

2、创建 ACL。

CN12800(config)#filter-list 1

CN12800(configure-filter-l2-1)#

3、配置 ACL 规则。

CN12800(configure-filter-l2-1)#filter 1 mac 00:01:02:03:04:05/48 any

4、将限速模板与该 ACL 绑定。

CN12800(configure-filter-l2-1)#filter 1 meter 1

5、配置 ACL 动作。

CN12800(configure-filter-l2-1)#filter 1 outaction yellow remark-dscp af11

6、绑定 ACL 到端口。

CN12800(configure-filter-l2-1)#quit

CN12800(config)#interface xgigaethernet 1/0/2

CN12800(config-10ge1/0/2)#filter-list-l2 in 1

7.3.9.5 配置计数模板示例

组网要求

CN12800 作为网关设备，下挂用户 PC。要求配置 ACL，对 CN12800 的 GE1/0/2 端口收到源 IP 地址为 10.1.1.1/24 网段的报文进行计数，统计报文的个数，如图 7-5 所示。

组网图

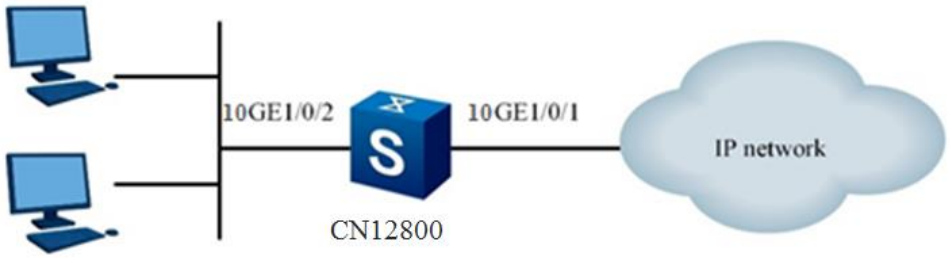


图 7-5 计数模板示例图

配置步骤

1、配置计数模板。

CN12800#configure

CN12800(config)# counter 1 packet sort total

2、创建 ACL。

CN12800(config)#filter-list 1001

CN12800(configure-filter-ipv4-1001)#

3、配置 ACL 规则。

CN12800(configure-filter-ipv4-1001)#filter 1 ip 10.1.1.1/24 any

4、将计数模板与该 ACL 绑定。

CN12800(configure-filter-ipv4-1001)#filter 1 action counter 1

5、端口绑定 ACL。

CN12800(configure-filter-ipv4-1001)#quit

CN12800(config)#interface xgigaethernet 1/0/2

CN12800(config-10ge1/0/2)#filter-list-ipv4 in 1001

7.4 本机防攻击配置

7.4.1 本机防攻击概述

本模块主要通过以下几种方式实现本机防攻击功能：

1、白名单

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

2、黑名单

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

3、用户自定义流

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

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

4、CAR

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

7.4.2 配置本机防攻击

目的

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

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
使能或去使能黑名单功能	1. 执行命令进入全局配置视图、VLANIF 配置视图、接口配置视图、接口组配置视图、VLAN 配置视图； 2. 执行命令 **cpu-defend policy** *policy-name* 进入 CPU 防攻击策略配置视图； 3. 执行命令 **blacklist** { **enable** | **disable** }。

目的	步骤
配置黑名单访问控制列表	1. 执行命令进入全局配置视图、VLANIF 配置视图、接口配置视图、接口组配置视图、VLAN 配置视图； 2. 执行命令 **cpu-defend policy** *policy-name* 进入 CPU 防攻击策略配置视图； 3. 执行命令 **blacklist enable** 使能黑名单功能。 4. 执行如下命令： ● **blacklist filter-list-l2** *acl-number1* 配置黑名单二层访问控制列表； ● **blacklist filter-list-ipv4** *acl-number2* 配置基于 IPv4 的黑名单访问控制列表； ● **blacklist filter-list-hybrid** *acl-number3* 配置黑名单混合访问控制列表； ● **blacklist filter-list-ipv6** *acl-number4* 配置基于 IPv6 的黑名单访问控制列表。
使能或去使能白名单功能	1. 执行命令进入全局配置视图、VLANIF 配置视图、接口配置视图、接口组配置视图、VLAN 配置视图； 2. 执行命令 **cpu-defend policy** *policy-name* 进入 CPU 防攻击策略配置视图； 3. 执行命令 **whitelist** { **enable** | **disable** }。
配置白名单访问控制列表	1. 执行命令进入全局配置视图、VLANIF 配置视图、接口配置视图、接口组配置视图、VLAN 配置视图； 2. 执行命令 **cpu-defend policy** *policy-name* 进入 CPU 防攻击策略配置视图； 3. 执行命令 **whitelist enable** 使能白名单功能。 4. 执行如下命令： ● **whitelist filter-list-l2** *acl-number1* 配置白名单二层访问控制列表； ● **whitelist filter-list-ipv4** *acl-number2* 配置基于 IPv4 的白名单访问控制列表； ● **whitelist filter-list-hybrid** *acl-number3* 配置白名单混合访问控制列表； ● **whitelist filter-list-ipv6** *acl-number4* 配置基于 IPv6 的白名单访问控制列表。
配置白名单访问控制列表动作	1. 执行命令进入全局配置视图、VLANIF 配置视图、接口配置视图、接口组配置视图、VLAN 配置视图； 2. 执行命令 **cpu-defend policy** *policy-name* 进入 CPU 防攻击策略配置视图； 3. 执行命令 **whitelist enable** 使能白名单功能。 4. 执行如下命令： ● **whitelist filter-list-l2 action** { **mirror-cpu** | **redirect-cpu** }配置白名单二层访问控制列表动作； ● **whitelist filter-list-ipv4 action** { **mirror-cpu** | **redirect-cpu** }配置基于 IPv4 的白名单访问控制列表动作； ● **whitelist filter-list-ipv6 action** { **mirror-cpu** | **redirect-cpu** }配置基于 IPv6 的白名单访问控制列表动作； ● **whitelist filter-list-hybrid action** { **mirror-cpu** | **redirect-cpu** }配置白名单混合访问控制列表动作。

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

7.4.3 维护及调试

目的

当本机防攻击功能不正常，需要进行查看、调试或定位问题时，可以使用本小节操作。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
显示 CPU 防攻击配置信息	1. 执行命令进入全局配置视图、特权用户视图、普通用户视图、VLANIF 配置视图、接口配置视图、接口组配置视图、VLAN 配置视图； 2. 执行命令 **show cpu-defend config**。

目的	步骤
显示防攻击所有防攻击策略列表信息或者指定防攻击策略的配置信息	1. 执行命令进入全局配置视图、特权用户视图、普通用户视图、VLANIF 配置视图、接口配置视图、接口组配置视图、VLAN 配置视图； 2. 执行如下命令： ● **show cpu-defend policy** ● **show cpu-defend policy** *policy-name*。
显示 CPU 防攻击报文峰值统计信息	1. 执行命令进入普通用户视图； 2. 执行如下命令： ● **show cpu-defend peak-statistic all** ● **show cpu-defend peak-statistic** [**slot** *slot-id*]。
清除 CPU 防攻击报文峰值统计信息	1. 执行命令进入全局配置视图； 2. 执行命令 **reset cpu-defend peak-statistic** [**slot** *slot-id*]。
清除 CPU 防攻击策略支持的具体报文峰值统计信息	1. 执行命令进入全局配置视图； 2. 执行命令 **cpu-defend policy** *policy-name* 进入 CPU 防攻击策略配置视图； 3. 执行命令 **reset cpu-defend peak-statistic packet-type** { **arp** | **bfd** | **bfd6** | **bgp** | **bpdutunnel** | **dhcp6client** | **dhcp6server** | **dhcpclient** | **dhcpserver** | **fibhit** | **ftp** | **ftp6** | **icmp** | **icmp6** | **igmp** | **isis** | **isis6** | **lacp** | **lldp** | **mldsnoop** | **nd** | **nd-miss** | **ntp** | **ntp6** | **ospf** | **ospf6** | **snmp** | **ssh** | **stp-customer** | **telnet** | **telnet6** | **tftp** | **tftp6** | **total** | **vrrp** | **vrrp6** }。
显示 CPU 防攻击统计信息	1. 执行命令进入全局配置视图、特权用户视图、普通用户视图、VLANIF 配置视图、接口配置视图、接口组配置视图、VLAN 配置视图； 2. 执行如下命令： ● **show cpu-defend statistic all** ● **show cpu-defend statistic slot** *slot-id* ● **show cpu-defend statistic packet-type** { **arp** | **bfd** | **bfd6** | **bgp** | **bpdutunnel** | **dhcpclient** | **dhcp6client** | **dhcpserver** | **dhcp6server** | **fibhit** | **ftp** | **ftp6** | **icmp** | **icmp6** | **igmpsnoop** | **isis** | **isis6** | **lacp** | **lldp** | **mldsnoop** | **nd** | **nd-miss** | **ntp** | **ntp6** | **ospf** | **ospf6** | **snmp** | **ssh** | **stp-customer** | **telnet** | **telnet6** | **tftp** | **tftp6** | **total** | **vrrp** | **vrrp6** }。

7.5 防攻击配置

7.5.1 使能 ARP 防攻击子开关 Table

目的

本节介绍如何使能 ARP 防攻击子开关。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
使能或去使能报文与 ARP 表信息匹配检查功能	1. 执行命令 **configure**； 2. 执行命令 **arp-antiattack** { **src-ip** | **src-mac** | **arp-cheat** | **gateway-cheat** | **gratuitous-arp** } { **enable** | **disable** }。
使能或去使能 ARP 老化单播探测方式	1. 执行命令进入接口配置视图（以太网、trunk）、接口组配置视图； 2. 执行命令 **arp detect-mode unicast** { **enable** | **disable** }。
配置接口能够学习到的最大 ARP 映射表项数目	1. 执行命令进入接口配置视图（以太网、trunk）、接口组配置视图； 2. 执行命令 **arp-limit vlan** *vlan-id* **maxnum** *maxnum*。
取消接口最大 ARP 映射表项数目限制	1. 执行命令进入接口配置视图（以太网、trunk）、接口组配置视图； 2. 执行命令 **no arp-limit vlan** *vlan-id*。
使能或去使能 DoS 限制防攻击功能	1. 执行命令进入全局配置视图； 2. 执行命令 **antiattack dos-limit** { **abnormal** | **fragment** | **tcp-syn** | **udp-flood** | **icmp-flood** } { **enable** | **disable** }。
配置 DoS 限制防攻击对指定报文的承诺访问速率和承诺信息速率	1. 执行命令进入全局配置视图； 2. 执行命令 **antiattack dos-limit** { **fragment** | **tcp-syn** | **icmp-flood** } **car cir** { *value* | **default** }。

7.5.2 配置 ARP 接口防攻击参数

目的

本节介绍如何配置 ARP 接口防攻击参数。.

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
使能或去使能 ARP 老化单播探测方式	1. 执行命令进入接口配置视图（以太网、trunk）、接口组配置视图； 2. 执行命令 **arp detect-mode unicast** { **enable** | **disable** }。
配置接口能够学习到的最大 ARP 映射表项数目	1. 执行命令进入接口配置视图（以太网、trunk）、接口组配置视图； 2. 执行命令 **arp-limit vlan** *vlan-id* **maxnum** *maxnum*。
取消接口最大 ARP 映射表项数目限制	1. 执行命令进入接口配置视图（以太网、trunk）、接口组配置视图； 2. 执行命令 **no arp-limit vlan** *vlan-id*。

7.5.3 防攻击模块调试

目的

本节介绍如何显示或者关闭防攻击模块的调试信息。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
显示防攻击模块的调试信息	1. 进入特权用户视图； 2. 执行命令 **debug arp-antiattack**。
关闭防攻击模块的调试信息	1. 进入特权用户视图； 2.执行命令 **no debug arp-antiattack**
清除接口下由于不匹配绑定表而造成的报文丢弃计数	1. 执行命令进入接口配置视图（以太网、trunk）、接口组配置视图； 2. 执行命令 **reset arp-antiattack statistic check user-bind**。
打开防 DOS 攻击 debug 开关	1. 进入特权用户视图； 2. 执行命令 **debug dos-antiattack** { **all** | **config** | **dev** | **info** }。
关闭防 DOS 攻击 debug 开关	1. 进入特权用户视图； 2. 执行命令 **no debug dos-antiattack** { **all** | **config** | **dev** | **info** }。
重置防攻击 DoS 限制统计值	1. 进入普通用户视图； 2. 执行命令 **reset antiattack dos-limit statistic**。
显示 DOS 防攻击模块的配置参数	1. 进入普通用户视图、特权用户视图、全局配置视图、接口配置视图（以太网、trunk）、接口组配置视图、VLAN 配置视图； 2. 执行如下命令： ● **show antiattack dos-limit config** ● **show antiattack dos-limit statistic**。
显示 ARP 报文绑定表匹配检查的项目信息	1. 进入普通用户视图、特权用户视图、全局配置视图、接口配置视图（以太网、trunk）、接口组配置视图、VLAN 配置视图； 2. 执行命令 **show arp-antiattack check user-bind**。
显示 ARP 防攻击配置信息	1. 进入普通用户视图、特权用户视图、全局配置视图、接口配置视图（以太网、trunk）、接口组配置视图； 2. 执行命令 **show arp-antiattack config**。
显示 ARP 防攻击统计信息	1. 进入普通用户视图、特权用户视图、全局配置视图、接口配置视图（以太网、trunk）、接口组配置视图； 2. 执行命令 **show arp-antiattack statistic**。

7.5.4 查看 ARP 防攻击配置

目的

本节介绍如何查看 ARP 防攻击配置。

过程

根据不同目的，执行相应步骤，具体参见下表。

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

7.6 IP Source Guard 配置

7.6.1 IP Source Guard 简介

7.6.1.1 技术背景

IP 地址的盗用方法多种多样，其常用方法主要有以下几种：

1. 静态修改 IP 地址

   对于任何一个 TCP/IP 实现来说，IP 地址都是其用户配置的必选项。如果用户在配置 TCP/IP 或修改 TCP/IP 配置时，使用的不是授权分配的 IP 地址，就形成了 IP 地址盗用。由于 IP 地址是一个逻辑地址，因此无法限制用户对于其主机 IP 地址的静态修改。

2. 成对修改 IP-MAC 地址对于静态修改 IP 地址的问题，现在很多单位都采用 IP 与 MAC 绑定技术加以解决。针对绑定技术，IP 盗用技术又有了新的发展，即成对修改 IP-MAC 地址。现在的一些兼容网卡，其 MAC 地址可以使用网卡配置程序进行修改。如果将一台计算机的 IP 地址和 MAC 地址都改为另外一台合法主机的 IP 地址和 MAC 地址，其同样可以接入网络。

   另外，对于那些 MAC 地址不能直接修改的网卡来说，用户还可以采用软件的办法来修改 MAC 地址，即通过修改底层网络软件达到欺骗上层网络软件的目的。

3. 动态修改 IP 地址某些攻击程序在网络上收发数据包，可以绕过上层网络软件，动态修改自己的 IP 地址（或 IP-MAC 地址对），以达到 IP 欺骗。

IPSG 特性是一种二层接口特性，能够提供检测机制来确保单个接口所接受到的数据包能够被各个接口所接受。如果检查成功通过，那么就将许可数据包；否则将会发生违背

策略的活动。IPSG 不仅能够确保第二层网络中终端设备的 IP 地址不被劫持，而且还能确保非授权设备不能通过自己指定 IP 地址的方式来访问网络或导致网络崩溃及瘫痪。

通过配置 IPSG，在链路 UP 的时候，只有 DHCP 数据包被许可通过。一旦 DHCP 服务器分配了 IP 地址，那么就将更新 DHCP 绑定表。IPSG 然后自动在接口加载基于端口的 ACL。上述过程能够将客户端流量限定到绑定表中所配置的源 IP 地址.对于来自源 IP 绑定之外的其他源 IP 地址的主机端口的流量，他们都将过滤.过滤能够限制主机从相邻主机夺取 IP 地址实现网络攻击的功能。

IP Source Guard 是基于 IP/MAC 的端口流量过滤技术，可以防止局域网内的 IP 地址欺骗攻击。交换机内部有一个 IP source binding table 作为每个端口接受到的数据包的检测标准，只有在两种情况下，交换机会转发数据——或者所接收到的 IP 包满足 IP source binding table 中 port/IP/MAC 的对应关系，或者是接收到的是 DHCP 数据包，其余数据包将被交换机做丢弃处理。IP source binding table 可以由用户在交换机上静态的配置，也可以由交换机从 DHCP Snooping 自动学习获得。静态配置是一种简单而固定的方式，灵活性很差，因此建议用户最好结合 DHCP Snooping 使用 IP Source Guard，由 DHCP Snooping Binding Database 生成 IP source binding table。

7.6.1.2 基本概念

IP Source Guard

IP 源防护，相当于在端口上添加了一条 ACL 表项，默认过滤该端口上所有用户发送的 IP 报文（除 DHCP 报文外）。当用户通过 DHCP 交互申请 IP 地址后，会在该端口上添加一条过滤表项，允许该用户使用该地址进行 IP 报文的通讯，其他用户依然禁止通讯。

DHCP Snooping

意为 DHCP 窥探，通过对 Client 和服务器之间的 DHCP 交互报文进行窥探，实现对用户的监控，同时 DHCP Snooping 起到一个 DHCP 报文过滤的功能，通过合理的配置实现对非法服务器的过滤。

IP Source Binding Table

IP 源绑定表可以由用户在交换机上静态添加，或者由交换机从 DHCP 监听绑定表（DHCP Snooping Binding Table）自动学习获得。 静态配置是一种简单而固定的方式，但灵活性很差，因此建议用户最好结合 DHCP Snooping 技术使用 IP Source Guard，由 DHCP 监听绑定表生成 IP 源绑定表。

ACL

访问控制列表是应用在路由器接口的指令列表，这些指令列表用来告诉路由器哪些数据包可以接收、哪些数据包需要拒绝。至于数据包是被接收还是被拒绝，可以由类似于源地址、目的地址、端口号、协议等特定指示条件来决定。

7.6.1.3 功能特性

IP Source Guard 功能特性如表 7-1 所示：

表 7-1 IP Source Guard 功能特性

序号	功能名称	功能描述
1	源 IP+PORT 过滤	根据源 IP 地址和端口对 IP 流量进行过滤，只有当流与绑定条目匹配时才允许通过。当端口创建、修改、删除新的 IP 源绑定条目的时候，IP 源地址过滤器将发生变化。为了能够反映 IP 源绑定的变更，端口 ACL 将被重新修改并重新应用到端口上。默认情况下，如果端口在没有存在 IP 源绑定条目的情况下启用了 IP 源防护功能，默认的 ACL 将拒绝端口的所有流量（实际上是除 DHCP 报文以外的所有 IP 流量）。
2	源 IP+PORT+MAC 过滤	同上
3	源 IP+PORT+VLAN 过滤	同上
4	源 IP+PORT+MAC+VLAN 过滤	同上

7.6.1.4 系统特点

IP Source Guard 系统特点如下：

- IP+PORT+MAC+VLAN 多元组合绑定来过滤 IP 流量；
- 可以结合 DHCPSNOOPING 的动态表项来配合使用，也可以单独发挥作用；
- IP SOURCE GUARD 的配置优先级高于 DHCPSNOOPING；
- IP SOURCE GUARD 和 DHCPSNOOPING 共用配置上限；
- 具有强大的 DEBUG 功能。

7.6.2 查看 IP Source Guard 配置信息

目的

本节介绍 IP Source Guard 的配置信息查看。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
查看所有绑定表项	1. 进入普通用户视图、特权用户视图、全局配置视图、接口配置视图（以太网、trunk）、接口组配置视图； 2. 执行命令 **show user-bind**。
查看静态绑定条目的配置信息	1. 进入普通用户视图或特权用户视图； 2. 执行命令 **show user-bind config**。
显示 IP 报文检查功能相关信息	1. 进入普通用户视图、特权用户视图、全局配置视图、接口配置视图（以太网）、接口组配置视图； 2. 执行命令 **show ip source check user-bind**。

7.6.3 配置检查项

目的

本节介绍配置 IP Source Guard 的检查项。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
使能接口下 IP 报文检查功能	1. 进入接口配置视图（以太网）、接口组配置视图； 2. 执行命令 **ip source check user-bind enable**。
取消接口下 IP 报文检查功能	1. 进入接口配置视图（以太网）、接口组配置视图； 2. 执行命令 **ip source check user-bind disable**。
配置 IP 报文的检查选项	1. 进入接口配置视图（以太网）、接口组配置视图； 2. 执行命令 **ip source check user-bind enable** 使能接口下 IP 报文检查功能； 3. 执行如下命令： ● **ip source check user-bind check-item** { **ip-address** | **mac-address** | **vlan** } ● **ip source check user-bind check-item ip-address mac-address** ● **ip source check user-bind check-item ip-address vlan** ● **ip source check user-bind check-item mac-address vlan**。 或 1. 进入 VLAN 配置视图； 2. 执行命令 **ip source check user-bind enable** 使能接口下 IP 报文检查功能； 3. 执行如下命令： ● **ip source check user-bind check-item** { **ip-address** | **mac-address** | **interface** }

目的	步骤
	● **ip source check user-bind check-item ip-address mac-address** ● **ip source check user-bind check-item ip-address interface** **ip source check user-bind check-item mac-address interface**。
恢复 IP 报文的检查选项为缺省选项	1. 进入接口配置视图（以太网）、接口组配置视图、VLAN 配置视图； 2. 执行命令 **no ip source check user-bind check-item**。
清除 IP Source Guard 统计信息	1. 进入接口配置视图（以太网）、接口组配置视图； 2. 执行命令 **ip source check user-bind enable** 使能接口下 IP 报文检查功能； 3. 执行命令 **reset ip source statistic check user-bind**。
使能或者去使能接口下 IP 报文告警检查功能	1. 进入接口配置视图（以太网）、接口组配置视图； 2. 执行命令 **ip source check user-bind alarm** { **enable** | **disable** }。
设置 IP 报文检查功能告警阈值	1. 进入接口配置视图（以太网）、接口组配置视图； 2. 执行命令 **ip source check user-bind alarm threshold** { *threshold* | **default** }。
使能或者去使能收到非信任 IP 报文告警功能	1. 进入全局配置视图； 2. 执行命令 **user-bind alarm untrust-user** { **enable** | **disable** }。
设置收到非信任 IP 报文告警阈值	1. 进入全局配置视图； 2. 执行命令 **user-bind alarm untrust-user threshold** { *threshold* | **default** }。
使能或者去使能 IP 报文黑名单功能	1. 进入全局配置视图； 2. 执行命令 **user-bind black-list** { **enable** | **disable** }。

7.6.4 配置静态绑定条目

目的

本节介绍 IP Source Guard 配置静态绑定条目。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
配置静态绑定条目	1. 进入全局配置视图； 2. 执行如下命令： ● **user-bind static ip** { *ipv4-address* | **any** } **mac** { *src-mac-address* | **any** } **interface** { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet |**

目的	步骤
	**25gigaethernet	40gigaethernet	100gigaethernet** } *interface-number* **vlan** { **any**	*vlan-id* } ● **user-bind static ip** { *ipv4-address*	**any** } **mac** { *src-mac-address*	**any** } **vlan** { **any**	*vlan-id* } ● **user-bind static ip6** { *ipv6-address*	**any** } **mac** { *src-mac-address*	**any** } **interface** { **ethernet	gigaethernet	xgigaethernet	10gigaethernet	25gigaethernet	40gigaethernet	100gigaethernet** } *interface-number* **vlan** { **any**	*vlan-id* } ● **user-bind static ip6** { *ipv6-address*	**any** } **mac** { *src-mac-address*	**any** } **vlan** { **any**	*vlan-id* }。
删除静态绑定条目	1. 进入全局配置视图； 2. 执行如下命令： ● **no user-bind static ip** { *ipv4-address*	**any** } **mac** { *src-mac-address*	**any** } **interface** { **ethernet	gigaethernet	xgigaethernet| 10gigaethernet	25gigaethernet	40gigaethernet	100gigaethernet** } *interface-number* **vlan** { **any**	*vlan-id* } ● **no user-bind static ip** { *ipv4-address*	**any** } **mac** { *src-mac-address*	**any** } **vlan** { **any**	*vlan-id* } ● **no user-bind static ip6** { *ipv6-address*	**any** } **mac** { *src-mac-address*	**any** } **interface** { **ethernet	gigaethernet	xgigaethernet| 10gigaethernet	25gigaethernet	40gigaethernet	100gigaethernet** } *interface-number* **vlan** { **any**	*vlan-id* } ● **no user-bind static ip6** { *ipv6-address*	**any** } **mac** { *src-mac-address*	**any** } **vlan** { **any**	*vlan-id* } ● **no user-bind static all** ● **no user-bind static interface** { **ethernet	gigaethernet	xgigaethernet| 10gigaethernet	25gigaethernet	40gigaethernet	100gigaethernet	eth-trunk** } *interface-number* ● **no user-bind static ip** *ipv4-address* ● **no user-bind static ip6** *ipv6-address* ● **no user-bind static mac** *src-mac-address* ● **no user-bind static vlan** *vlan-id*。

7.6.5 使能或去使能 IPSG 的 Trap 发送功能

目的

本节介绍如何使能或去使能 IP Source Guard 的 Trap 发送功能。

过程

目的	步骤
使能或去使能 IPSG 的 Trap 发送功能	1. 进入全局配置视图； 2. 执行命令 **ipsg trap** { **enable** | **disable** }。

7.6.6 维护及调试

目的

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

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
打开 Ip Source Guard 调试功能	1. 进入特权用户视图； 2. 执行命令 **debug ip source check**。
关闭 Ip Source Guard 调试功能	1. 进入特权用户视图； 2. 执行命令 **no debug ip source check**。

7.7 AAA/Radius 配置

7.7.1 AAA 简介

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

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

AAA 一般采用客户机/服务器结构，客户端运行于 NAS（Network Access Server，网络接入服务器）上，服务器上则集中管理用户信息。NAS 对于用户来讲是服务器端，对于服务器来说是客户端。AAA 的基本组网结构如图 7-6 所示。

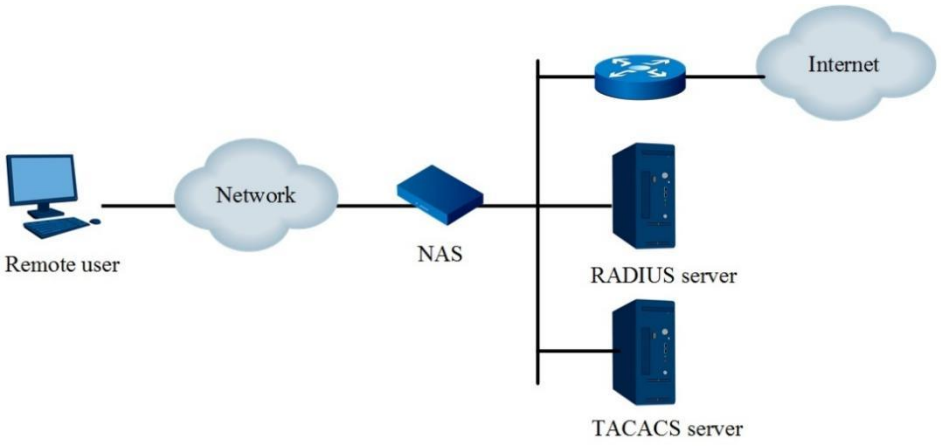


图 7-6 AAA 基本网络架构

认证功能

AAA 支持以下认证方式.

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

计费功能

AAA 支持以下计费方式：

- 不计费（**none**）：不对用户计费。
- 本地计费（**local**）：本地计费是为了支持本地用户的连接数限制管理，实现了对用户接入数的统计功能，没有实际的费用统计功能。本地的接入数管理只对本地计费有效，对本地认证和授权没有作用。
- 远端计费：支持通过 RADIUS 服务器或 TACACS 服务器进行远端计费。

AAA 一般采用客户机/服务器结构：客户端运行于被管理的资源侧，服务器上集中存放用户信息。因此，AAA 框架具有良好的可扩展性，并且容易实现用户信息的集中管理。AAA 可以通过多种协议来实现，目前设备中的 AAA 是基于 RADIUS 协议或 TACACS 协议来实现的。

授权功能

AAA 支持以下授权方式：

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

7.7.2 进入 AAA 配置视图

目的

本节介绍如何进入 AAA 配置视图。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
进入 AAA 配置视图	1. 进入全局配置视图； 2. 执行命令 **aaa**。

7.7.3 配置 AAA 认证方法

目的

本节介绍如何创建 AAA 认证方法。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
创建 AAA 认证方法	1. 进入全局配置视图； 2. 进入 AAA 配置视图； 3. 执行如下命令： ● **aaa authentication** { **dot1x** | **login** | **enable** } **method** *name* **server-group** *groupname*

目的	步骤
	● **aaa authentication** { **dot1x** | **login** | **enable** } **method** *name* **server-group** *groupname* { **local** | **none** } ● **aaa authentication** { **dot1x** | **login** | **enable** } **method** *name* **server-group** *groupname* **local none** ● **aaa authentication** { **dot1x** | **login** | **enable** } **method** *name* **server-group** *groupname groupname* ● **aaa authentication** { **dot1x** | **login** | **enable** } **method** *name* **server-group** *groupname groupname* { **local** | **none** } ● **aaa authentication** { **dot1x** | **login** | **enable** } **method** *name* **server-group** *groupname groupname* **local none**。
配置本地 AAA 认证方法名	1. 进入全局配置视图； 2. 进入 AAA 配置视图； 3. 执行命令 **aaa authentication** { **dot1x** | **login** | **enable** } **method** *name* **local**。
配置 RADIUS 服务器认证端口	1. 进入全局配置视图； 2. 进入 AAA 配置视图； 3. 执行命令 **radius-server** *name* **auth-port** { *auth-port* | **default** }。
删除已创建的 AAA 方法服务器组	1. 进入全局配置视图； 2. 进入 AAA 配置视图； 3. 执行命令 **no aaa method** *name* **server-group** *group-name*。
删除已创建的 AAA 方法	1. 进入全局配置视图； 2. 进入 AAA 配置视图； 3. 执行命令 **no aaa method** *name*。

7.7.4 配置 AAA 授权方法

目的

本节介绍如何创建 AAA 授权方法。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
创建 AAA 授权方法	1. 进入全局配置视图； 2. 进入 AAA 配置视图； 3. 执行如下命令： ● **aaa authorization method** *name* **server-group** *groupname*

目的	步骤
	● **aaa authorization method** *name* **server-group** *groupname* { **local** | **none** } ● **aaa authorization method** *name* **server-group** *groupname groupname* ● **aaa authorization method** *name* **server-group** *groupname groupname* { **local** | **none** }。
删除已创建的 AAA 方法服务器组	1. 进入全局配置视图； 2. 进入 AAA 配置视图； 3. 执行命令 **no aaa method** *name* **server-group** *group-name*。
删除已创建的 AAA 方法	1. 进入全局配置视图； 2. 进入 AAA 配置视图； 3. 执行命令 **no aaa method** *name*。
使能 console 使用 AAA 授权方法	1. 进入全局配置视图； 2. 执行命令 **aaa authorization console**。
去使能 console 使用 AAA 授权方法	1. 进入全局配置视图； 2. 执行命令 **no aaa authorization console**。

7.7.5 配置 AAA 计费方法

目的

本节介绍如何创建 AAA 计费方法。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
配置远程 AAA 认证参数	1. 进入全局配置视图； 2. 进入 AAA 配置视图； 3. 执行如下命令： ● **aaa accounting** { **dot1x** | **login** } **method** *name* **server-group** *group-name* ● **aaa accounting** { **dot1x** | **login** } **method** *name* **server-group** *group-name* { **local** | **none** } ● **aaa accounting** { **dot1x** | **login** } **method** *name* **server-group** *group-name group-name* ● **aaa accounting** { **dot1x** | **login** } **method** *name* **server-group** *group-name group-name* { **local** | **none** }

目的	步骤
	● **aaa accounting** { **dot1x** | **login** } **method** *name* **server-group** *group-name* **local none**。
配置 RADIUS 服务器计费端口	1. 进入全局配置视图； 2. 进入 AAA 配置视图； 3. 执行命令 **radius-server** *name* **acct-port** { *acct-port* | **default** }。
配置 AAA 服务器实时计费失效时间	1. 进入全局配置视图； 2. 进入 AAA 配置视图； 3. 执行命令 **accounting realtime** { *realtime* | **default** }。
删除已创建的 AAA 方法服务器组	1. 进入全局配置视图； 2. 进入 AAA 配置视图； 3. 执行命令 **no aaa method** *name* **server-group** *groupname*。
删除已创建的 AAA 方法	1. 进入全局配置视图； 2. 进入 AAA 配置视图； 3. 执行命令 **no aaa method** *name*。

7.7.6 创建和删除服务器组

目的

本节介绍如何创建和删除服务器组。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
创建服务器组包括服务器组协议类型定义并添加服务器	1. 进入全局配置视图； 2. 进入 AAA 配置视图； 3. 执行如下命令： ● **server-group** *name* **radius-server** *servername* ● **server-group** *name* **tacacs-server** *servername*。
在服务器组中删除服务器	1. 进入全局配置视图； 2. 进入 AAA 配置视图； 3. 执行如下命令： ● **no server-group** *name* **radius-server** *servername* ● **no server-group** *name* **tacacs-server** *servername*。

目的	步骤
删除服务器组	1. 进入全局配置视图； 2. 进入 AAA 配置视图； 3. 执行命令 **no server-group** *name*。

7.7.7 配置 RADIUS 服务器

目的

本节介绍如何配置 Radius 服务器。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
创建 Radius 服务器	1. 进入全局配置视图； 2. 进入 AAA 配置视图； 3. 执行命令 **radius-server** *name* **ip-address** *ipv4-address* **key** *key*。
创建基于 IPv4 地址的 Radius 服务器	1. 进入全局配置视图； 2. 进入 AAA 配置视图； 3. 执行命令 **radius-server** *name* **ip-address** *ipv4-address* **key** *key* **auth-port** { *auth-port* | **default** } **acct-port** { *acct-port* | **default** }。
配置 RADIUS 服务器失效时间	1. 进入全局配置视图； 2. 进入 AAA 配置视图； 3. 执行如下命令： ● **radius-server deadtime** { *deadtime* | **default** } ● **radius-server** *name* **deadtime** { *deadtime* | **default** }。
配置 RADIUS 服务器重传次数	1. 进入全局配置视图； 2. 进入 AAA 配置视图； 3. 执行如下命令： ● **radius-server max-retransmit** { *max-retransmit* | **default** } ● **radius-server** *name* **max-retransmit** { *max-retransmit* | **default** }。
配置 RADIUS 服务器重传时间间隔	1. 进入全局配置视图； 2. 进入 AAA 配置视图； 3. 执行如下命令： ● **radius-server retransmit-interval** { *retransmit-interval* | **default** } ● **radius-server** *name* **retransmit-interval** { *retransmit-interval* | **default** }。

目的	步骤
指定 AAA Radius 服务器的 srcip（IPv4）	1. 进入全局配置视图； 2. 进入 AAA 配置视图； 3. 执行命令 **radius-server** *name* **src-ip** *ip-address*。
删除指定 AAA Radius 服务器的 srcip（IPv4）	1. 进入全局配置视图； 2. 进入 AAA 配置视图； 3. 执行命令 **no radius-server** *name* **src-ip**。
配置 RADIUS 服务器认证端口	1. 进入全局配置视图； 2. 进入 AAA 配置视图； 3. 执行命令 **radius-server** *name* **auth-port** { *auth-port* | **default** }。
删除 Radius 服务器	1. 进入全局配置视图 2. 进入 AAA 配置视图 3. 执行命令 **no radius-server** *name*。

7.7.8 配置 TACACS 服务器

目的

本节介绍如何配置 TACACS 服务器。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
创建 TACACS 服务器	1. 进入全局配置视图； 2. 进入 AAA 配置视图； 3. 执行命令 **tacacs-server** *name* **ip-address** *ip-address* **key** *key*。
创建基于 IPv4 地址的 TACACS 服务器	1. 进入全局配置视图； 2. 进入 AAA 配置视图； 3. 执行命令 **tacacs-server** *name* **ip-address** *ip-address* **key** *key* **port** { *port-num* | **default** } **single-connection** { **enable** | **disable** }。
配置 TACACS 服务器超时时间	1. 进入全局配置视图； 2. 进入 AAA 配置视图； 3. 执行如下命令： ● **tacacs-server timeout** { *timeout* | **default** } ● **tacacs-server** *name* **timeout** { *timeout* | **default** }。
配置的 TACACS 服务	1. 进入全局配置视图； 2. 进入 AAA 配置视图；

器的全局失效时间	3. 执行如下命令： ● **tacacs-server deadtime** { *deadtime* | **default** } ● **tacacs-server** *name* **deadtime** { *deadtime* | **default** }。
配置 TACACS 服务器端口	1. 进入全局配置视图； 2. 进入 AAA 配置视图； 3. 执行命令 **tacacs-server** *name* **port** { *port-number* | **default** }。
配置 Tacacs 服务器单连接功能	1. 进入全局配置视图； 2. 进入 AAA 配置视图； 3. 执行命令 **tacacs-server** *name* **single-connection** { **enable** | **disable** }。
配置向 Tacacs Server 发送请求报文的源 IP	1. 进入全局配置视图； 2. 进入 AAA 配置视图； 3. 执行如下命令： ● **tacacs-server** *name* **src-ip** *ip-address* ● **no tacacs-server** *name* **src-ip**。
删除 tacacs 服务器	1. 进入全局配置视图； 2. 进入 AAA 配置视图； 3. 执行命令 **no tacacs-server** *name*。

7.7.9 配置 AAA 终端

目的

本节介绍如何配置 AAA 终端。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
配置终端 telnet/console 的 login aaa 认证类型	1. 进入全局配置视图； 2. 进入 Line 配置视图； 3. 执行如下命令配置终端 telnet/console 的 login aaa 认证类型： ● **login authentication aaa method** *name* **auth-type** { **pap** | **chap** | **ascii** } ● **login authentication local**。
配置终端 login 授权方法	1. 进入全局配置视图； 2. 进入 Line 配置视图； 3. 执行命令 **login authorization aaa method** *name* 配置终端 login 授权方法。
删除终端下已配置的 login 授权方法。	1. 进入全局配置视图； 2. 进入 Line 配置视图； 3. 执行命令 **no login authorization aaa method** 删除终端下已配置的 login 授权方法。

目的	步骤
配置用户二次认证模式	1. 进入全局配置视图； 2. 进入 Line 配置视图； 3. 执行如下命令配置用户二次认证模式： ● **enable authentication** { **local** | **none** } ● **enable authentication aaa method** *name*。
配置指定用户特权级别密码检查所用的 AAA 授权方法	1. 进入全局配置视图； 2. 进入 Line 配置视图； 3. 执行命令 **command authorization** *level-value* **aaa method** *name* 配置指定用户特权级别密码检查所用的 AAA 授权方法。
配置使用全局下的命令使能命令授权	1. 进入全局配置视图； 2. 进入 Line 配置视图； 3. 执行命令 **command authorization config-command** 配置使用全局下的命令使能命令授权。
配置本地二次认证对应级别的密码	1. 进入 Line 配置视图； 2. 执行如下命令配置本地二次认证对应级别的密码： ● **enable password level** *level-value* { **cipher** | **plain** } *password* ● **enable password** { **cipher** | **plain** } *password*。
删除配置本地二次认证对应级别的密码	1. 进入 Line 配置视图； 2. 执行如下命令： ● **no enable password level** *level-value* ● **no enable password**。
提升或降低用户权限	1. 进入特权用户视图、普通用户视图； 2. 执行命令 **enable | disable** [*level-value*]提升或降低用户权限。

7.7.10 显示 AAA 配置信息

目的

本节介绍如何显示 AAA 配置信息。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
显示远程用户配置信息	1. 进入普通用户视图、特权用户视图、全局配置视图、AAA 配置视图、接口配置视图（以太网、trunk）、接口组配置视图； 2. 执行命令 **show aaa**。

目的	步骤
显示全局配置信息	1. 进入特权用户视图、全局配置视图、AAA 配置视图； 2. 执行命令 **show aaa config**。
显示 AAA 方法信息	1. 进入特权用户视图、全局配置视图、AAA 配置视图； 2. 执行如下命令： ● **show aaa method** ● **show aaa method** *name*。
显示 AAA 服务器名称	1. 进入普通用户视图、特权用户视图、全局配置视图、AAA 配置视图； 2. 执行如下命令： ● **show aaa server** ● **show aaa server** *name*。
显示 AAA 服务器组信息	1. 进入特权用户视图、全局配置视图、AAA 配置视图； 2. 执行如下命令： ● **show aaa server-group** ● **show aaa server-group** *group-name*。
显示所有客户端信息	1. 进入普通用户视图、特权用户视图、全局配置视图、AAA 配置视图； 2. 执行命令 **show radius client**。
显示 tacacs 服务器相关统计数据	1. 进入特权用户视图、全局配置视图、AAA 配置视图； 2. 执行如下命令： ● **show aaa tacacs-server** *name* **statistic** ● **show aaa tacacs-server statistic**。

7.7.11 AAA 调试

目的

本节介绍如何打开或者关闭调试 AAA 开关。

过程

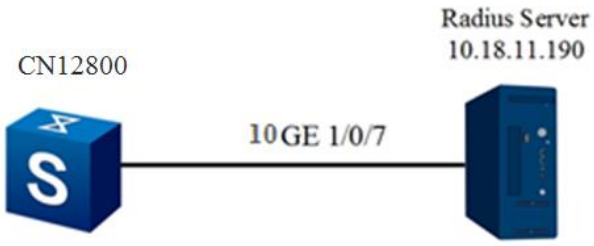
根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
打开或关闭 AAA 调试功能	1. 进入特权用户视图； 2. 执行如下命令： ● **debug aaa { auth | author | acct | sys | method | server | session | radius | tacacs | all }** ● **no debug aaa { auth | author | acct | sys | method | server | session | radius | tacacs | all }**

7.7.12 配置举例

7.7.12.1 LOGIN AAA RADIUS 认证

组网图



配置步骤

LOGIN 认证用于在用户通过串口登录设备时通过 AAA 进行认证，配置步骤如下：

首先进入 aaa 配置节点，配置 radius server，并创建 aaa 服务器组和 aaa 方法。

CN12800(config-aaa)#radius-server server1 ip-address 10.18.11.190 key wri

CN12800(config-aaa)#server-group grp1 radius-server server1

CN12800(config-aaa)#aaa authentication login method radius server-group grp1

AAA 配置完成后，进行终端 login aaa 配置。

CN12800(config)#line console 1

CN12800(config-line)#login authentication aaa method me auth-type chap

第8章 可靠性配置

本章介绍了 CN12800 系列数据中心交换机可靠性管理的基本内容、配置过程和配置举例。

8.1 MSTP 配置

8.1.1 STP 简介

STP 产生的原因

在二层交换网络中，一旦存在环路就会造成报文在环路内不断循环和增生，产生广播风暴，从而占用所有的有效带宽，使网络变得不可用。

这种环境下 STP 协议应运而生，IEEE 于 1998 年发布的 802.1D 标准定义了 STP（Spanning Tree Protocol）。

STP 工作过程

首先进行根桥的选举。选举的依据是网桥优先级和网桥 MAC 地址组合成的桥 ID，桥 ID 最小的网桥将成为网络中的根桥，它的所有端口都连接到下游桥，所以端口角色都成为指定端口。接下来，连接根桥的下游网桥将各自选择一条“最粗壮”的树枝作为到根桥的路径，相应端口的角色就成为根端口。循环这个过程到网络的边缘，指定端口和根端口确定之后一棵树就生成了。生成树经过一段时间（默认值是 30 秒左右）稳定之后，指定端口和根端口进入转发状态，其他端口进入阻塞状态。STP BPDU 会定时从各个网桥的指定端口发出，以维护链路的状态。如果网络拓扑发生变化，生成树就会重新计算，端口状态也会随之改变。这就是生成树的基本原理。

STP 的缺点

随着应用的深入和网络技术的发展，STP 的缺点在应用中也被暴露了出来。STP 协议的缺陷主要表现在收敛速度上。

当拓扑发生变化，新的配置消息要经过一定的时延才能传播到整个网络，这个时延称为 Forward Delay，协议默认值是 15 秒。在所有网桥收到这个变化的消息之前，若旧拓扑结构中处于转发的端口还没有发现自己应该在新的拓扑中停止转发，则可能存在临时环路。为了解决临时环路的问题，STP 使用了一种定时器策略，即在端口从阻塞状态到转发状态中间加上一个只学习 MAC 地址但不参与转发的中间状态，两次状态切换的时间长度都是 Forward Delay，这样就可以保证在拓扑变化的时候不会产生临时环路。但是，

这个看似良好的解决方案实际上带来的却是至少两倍 Forward Delay 的收敛时间，这在某些实时业务（如语音视频）中是不能接受的。

8.1.2 RSTP 简介

RSTP 的优点

为了解决 STP 协议的收敛速度缺陷，2001 年 IEEE 定义了基于 IEEE 802.1w 标准的快速生成树协议 RSTP（Rapid Spanning Tree Protocol，快速生成树协议）。RSTP 协议在 STP 协议基础上做了三点重要改进，加快了收敛速度（最快可在 1 秒以内）：

- 为根端口和指定端口设置了快速切换用的替换端口（Alternate Port）和备份端口（Backup Port）两种角色。当根端口失效的情况下，替换端口就会快速转换为新的根端口并无时延地进入转发状态；当指定端口失效的情况下，备份端口就会快速转换为新的指定端口并无时延地进入转发状态。
- 在只连接了两个交换端口的点对点链路中，指定端口只需与下游网桥进行一次握手就可以无时延地进入转发状态。如果是连接了三个以上网桥的共享链路，下游网桥是不会响应上游指定端口发出的握手请求的，只能等待两倍 Forward Delay 时间进入转发状态。
- 直接与终端相连而不与其他网桥相连的端口定义为边缘端口（Edge Port）。边缘端口可以直接进入转发状态，不需要任何延时。由于网桥无法知道端口是否是直接与终端相连，所以需要人工配置。

RSTP 的缺点

RSTP 协议相对于 STP 协议的确有很多改进，并且向下兼容 STP 协议，可以混合组网。但是，RSTP 和 STP 一样同属于单生成树 SST（Single Spanning Tree），有它自身的诸多缺陷，主要表现在三个方面：

- 由于整个交换网络只有一棵生成树，在网络规模比较大的时候会导致较长的收敛时间。
- 因为 RSTP 是单生成树协议，所有 VLAN 共享一棵生成树，为了保证 VLAN 内部可以正常通信，网络内每个 VLAN 都必须沿着生成树的路径方向连续分布，否则将会出现有的 VLAN 由于内部链路被阻塞而被分隔开，从而导致 VLAN 内部无法通信的问题。
- 当某条链路被阻塞后将不承载任何流量，无法实现负载均衡，造成了带宽的极大浪费。

这些缺陷都是单生成树无法克服的，于是支持 VLAN 的多生成树协议 MSTP 出现了。

8.1.3 MSTP 简介

MSTP 的优点

MSTP（Multiple Spanning Algorithm and Protocol，多生成树协议）是 IEEE 于 2002 年发布的 802.1s 标准中定义的一种新型生成树协议，相对于 STP 和 RSTP，优势非常明显。MSTP 的特点如下：

- MSTP 引入“域”的概念，把一个交换网络划分成多个域。每个域内形成多棵生成树，生成树之间彼此独立；在域间，MSTP 利用 CIST 保证全网络拓扑结构的无环路存在。
- MSTP 引入“实例（Instance）”的概念，将多个 VLAN 映射到一个实例中，以节省通信开销和资源占用率。MSTP 各个实例拓扑的计算是独立的（每个实例对应一棵单独的生成树），在这些实例上就可以实现 VLAN 数据的负载分担。
- MSTP 可以实现类似 RSTP 的端口状态快速迁移机制。
- MSTP 兼容 STP 和 RSTP。

MSTP 的算法实现

1. 初始状态

   各台设备的各个端口在初始时会生成以自己为根桥的配置消息，总根和域根都是本桥 ID，外部根路径开销和内部根路径开销全为 0，指定桥 ID 为本桥 ID，指定端口为本端口，接收 BPDU 报文的端口为 0。

2. 端口角色的选择原则

   端口角色的选择原则如表 8-1 所示。

表 8-1 端口角色的选择原则

端口角色	选择原则
根端口	端口的端口优先级向量优于其指定优先级向量，且设备的根优先级向量取自该端口的根路径优先级向量。
指定端口	端口的指定优先级向量优于其端口优先级向量。
Master 端口	域边界根端口在 MSTI 实例上的角色就是 Master 端口。
Alternate 端口	端口的端口优先级向量优于其指定优先级向量，但设备的根优先级向量不是取自该端口的根路径优先级向量。

端口角色	选择原则
Backup 端口	端口的端口优先级向量优于其指定优先级向量，但端口优先级向量中的指定桥 ID 为本设备的桥 ID。

3. 优先级向量计算

所有网桥的 MSTP 角色都是通过报文中携带的信息计算出来的，其中报文中携带的最重要的信息就是生成树的优先级向量。下面将分别介绍一下 CIST 优先级向量和 MSTI 优先级向量的计算方法。

a) CIST 优先级向量计算

在 CIST 中优先级向量由总根、外部根路径开销、域根、内部根路径开销、指定桥 ID、指定端口 ID 和接收 BPDU 报文的端口 ID 组成。

为了方便后续描述，现做如下假设：

- 初始情况下，网桥 B 的端口 PB 对外发送报文中携带的信息如下：总根为 RB，外部根路径开销为 ERCB，域根为 RRB，内部根路径开销为 IRCB，指定桥 ID 为 B，指定端口 ID 为 PB，接收 BPDU 报文的端口 ID 为 PB；
- 网桥 B 的端口 PB 收到网桥 D 的端口 PD 发送过来的报文中携带的信息如下：总根为 RD，外部根路径开销为 ERCD，域根为 RRD，内部根路径开销为 IRCD，指定桥 ID 为 D，指定端口 ID 为 PD，接收 BPDU 报文的端口 ID 为 PB；
- 网桥 B 的端口 PB 收到的网桥 D 的端口 PD 发送过来的报文的优先级较高。

根据上述假设，下面将逐一介绍各优先级向量的计算方法。

(1) 消息优先级向量

消息优先级向量是 MSTP 协议报文中所携带的优先级向量。根据假设，网桥 B 的端口 PB 收到的消息优先级向量即为：{RD : ERCD : RRD : IRCD : D : PD : PB}。如果网桥 B 和网桥 D 不在同一个域，那么内部根路径开销对网桥 B 而言是毫无意义的，它会被赋值为 0。

(2) 端口优先级向量

在初始情况下，端口优先级向量的信息是以自己为根。端口 PB 的端口优先级向量为：{RB : ERCB : RRB : IRCB : B : PB : PB}。

端口优先级向量是随端口收到的消息优先级向量更新的：如果端口收到的消息优先级向量优于端口优先级向量，则将端口优先级向量更新为消息优先级向量；否则，端口优先

级向量保持不变。由于端口 PB 收到的消息优先级向量优于端口优先级向量，所以端口优先级向量更新为：{RD ： ERCD ： RRD ： IRCD ： D ： PD ： PB}。

(3) 根路径优先级向量

根路径优先级向量由端口优先级向量计算所得：

- 如果端口的优先级向量来自不同域的网桥，根路径优先级向量的外部根路径开销为端口的路径开销和端口优先级向量的外部根路径开销之和，根路径优先级向量的域根为本桥的域根，内部根路径开销为 0。假设网桥 B 的端口 PB 的路径开销为 PCPB，则端口 PB 的根路径优先级向量为：{RD ： ERCD+ PCPB： B ： 0 ： D ： PD ： PB}；
- 如果端口优先级向量来自同一域的网桥，根路径优先级向量的内部路径开销为端口优先级向量的内部根路径开销和端口路径开销之和，计算后端口 PB 的根路径优先级向量为：{RD ： ERCD: RRD ： IRCD + PCPB ： D ： PD ： PB}。

(4) 桥优先级向量

桥优先级向量中总根 ID、域根 ID 以及指定桥 ID 都是本桥 ID，外部根路径开销和内部根路径开销为 0，指定端口 ID 和接收端口 ID 也全为 0。网桥 B 的桥优先级向量为：{B： 0： B： 0： B： 0： 0}。

(5) 根优先级向量

根优先级向量是桥优先级向量和所有指定桥 ID 和本桥 ID 值不相同的根路径优先级向量的最优值，如果本桥优先级向量比较优，那么本桥就为 CIST 总根。假设网桥 B 的桥优先级向量最优，则网桥 B 的根优先级向量为：{B： 0： B： 0： B： 0： 0}。

(6) 指定优先级向量

端口的指定优先级向量由根优先级向量计算所得，将根优先级向量的指定桥 ID 替换为本桥 ID，指定端口 ID 替换为自己的端口 ID。网桥 B 的端口 PB 的指定优先级向量为：{B： 0： B： 0： B： PB： 0}。

b) MSTI 优先级向量计算

MSTI 的各优先级向量计算的规则和 CIST 优先级向量计算规则是基本一致的，存在两点区别：

- MSTI 优先级向量中没有总根和外部根路径开销，仅由域根、内部根路径开销、指定桥 ID、指定端口 ID 和接收 BPDU 报文的端口 ID 组成。
- MSTI 只处理来自同一域的消息优先级向量。

4. 角色选择过程

下面结合图 8-1 的组网对 CIST 实例的计算过程进行简要说明。假设，网桥的优先级为 CN12800_1 优于 CN12800_2，CN12800_2 优于 CN12800_3，4、5、10 分别为链路的路径开销。CN12800_1 和 CN12800_2 属于同一域，CN12800_3 单独一个域。

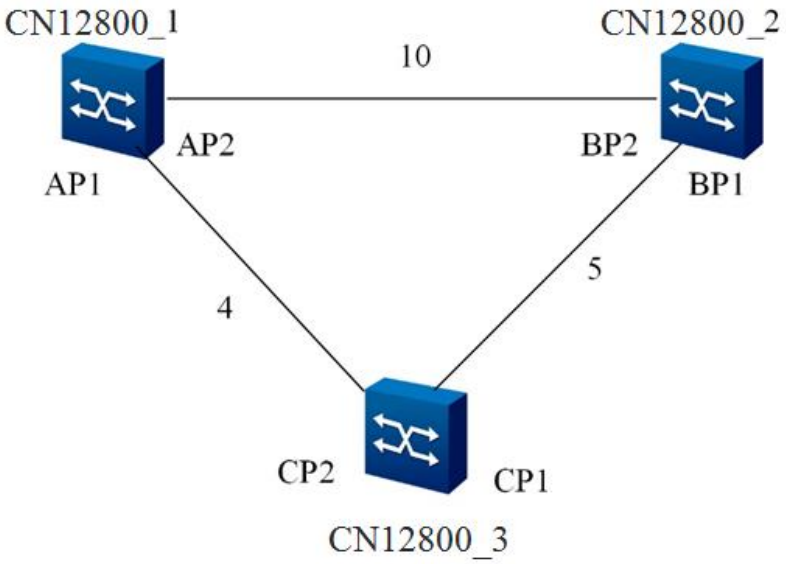


图 8-1 MSTP 算法计算过程组网图

图 8-1 中各设备的初始情况下对外发送的报文中携带的消息优先级向量如表 8-2 所示。

表 8-2 各台设备的初始状态

设备	端口	报文中的消息优先级向量
CN12800_1	AP1	{A:0:A:0:A:AP1:0}
	AP2	{A:0:A:0:A:AP2:0}
CN12800_2	BP1	{B:0:B:0:B:BP1:0}
	BP2	{B:0:B:0:B:BP2:0}
CN12800_3	CP1	{C:0:C:0:C:CP2:0}
	CP2	{C:0:C:0:C:CP2:0}

设备各端口的端口优先级向量与消息优先级向量在初始情况下是保持一致的。

在初始情况下各设备的端口都会被计算为指定端口且对外发送以自己为根桥的消息优先级向量。

a) CN12800_1 的角色选择过程

CN12800_1 的端口 AP1 和端口 AP2 会分别收到来自 CN12800_2 和 CN12800_3 的报文，CN12800_1 会将端口 AP1 以及 AP2 的端口优先级向量和收到的来自其它交换机的消息优先级向量进行比较，由于 AP1 和 AP2 的端口优先级向量优于报文中携带的消息优先级向量，端口 AP1 和 AP2 端口角色不变仍为指定端口，设备 CN12800_1 为总根且为 CN12800_1 和 CN12800_2 所在域的域根。此后端口定时对外传播以自己为根的消息。

b) CN12800_2 的角色选择过程

CN12800_2 的端口 BP1 收到来自 CN12800_3 的端口 CP1 的报文后，将消息优先级向量和端口优先级向量比较，由于端口优先级向量优于消息优先级向量，端口角色不更新。

CN12800_2 的端口 BP2 收到来自 CN12800_1 的端口 AP2 的报文后，处理过程如下：

(1) 将端口的消息优先级向量和端口优先级向量进行比较。由于端口的消息优先级向量优于端口优先级向量，将端口的端口优先级向量更新为消息优先级向量{A:0:A:0:A:AP2:BP2}；

(2) 计算端口的根路径优先级向量。CN12800_1 和 CN12800_2 在同一域内，端口的根路径优先级向量为{A:0:A:10:A:AP2:BP2}；

(3) 计算 CN12800_2 的根优先级向量。只有端口 BP2 的根路径优先级向量是来自其它设备，由于端口 BP2 的根路径优先级向量优于 CN12800_2 的桥优先级向量，CN12800_2 的根优先级向量为{A:0:A:10:A:AP2:BP2}；

(4) 指定优先级向量计算。端口 BP1 的指定优先级向量为{A:0:A:10:B:BP1:BP2}，端口 BP2 的指定优先级向量为{A:0:A:10:B:BP2:BP2}。

端口角色的确定：将端口 BP1 和 BP2 的指定优先级向量和端口优先级向量进行比较，由于 BP1 的指定优先级向量优于端口优先级向量，则 BP1 角色为指定端口，定时对外发送以 CN12800_1 为总根和域根的指定优先级向量{A:0:A:10:B:BP1:BP2}；由于 BP2 的端口优先级向量优于指定优先级向量、且根优先级向量取自端口 BP2 的根路径优先级向量，则 BP2 角色为根端口。

c) CN12800_3 的角色选择过程

CN12800_3 的端口 CP1 收到来自 CN12800_2 未更新前的消息优先级向量{B:0:B:0:B:BP1:CP1}，端口 CP2 收到来自 CN12800_1 的消息优先级向量{A:0:A:0:A:AP1:CP2}，经过分别比较，CP1 和 CP2 的消息优先级向量均优于端口优先级向量，因此分别更新 CP1 和 CP2 的端口优先级向量为{B:0:B:0:B:BP1:CP1}和{A:0:A:0:A:AP1:CP2}。由于 CN12800_3 与 CN12800_1 和 CN12800_2 不在同一域，端口 CP1 的根路径优先级向量为{B:5:C:0:B:BP1:CP1}，端口 CP2 的根路径优先级向量为

{A:4:C:0:A:AP1:CP2}，CP2 的根路径优先级向量优于 CP1 的根路径优先级向量，则根优先级向量为{A:4:C:0:A:AP1:CP2}。端口 CP1 和 CP2 的指定优先级向量分别为{A:4:C:0:C:CP1:CP2}和{A:4:C:0:C:CP2:CP2}，端口 CP1 被计算为指定端口，CP2 被计算为根端口。

CN12800_3 的端口 CP1 收到来自 BP1 更新后的消息优先级向量{A:0:A:10:B:BP1:CP1}后，经过比较 CP1 的消息优先级向量优于端口优先级向量，更新端口优先级向量为{A:0:A:10:B:BP1:CP1}，端口 CP1 计算后的根路径优先级向量为{A:5:C:0:B:BP1:CP1}。由于端口 CP2 收到的消息优先级向量没有变化，根据前面的计算，端口 CP2 的根路径优先级向量保持为{A:4:C:0:A:AP1:CP2}，CP2 的根路径优先级向量优于 CP1 的根路径优先级向量，则根优先级向量为{A:4:C:0:A:AP1:CP2}。端口 CP1 和 CP2 的指定优先级向量分别为{A:4:C:0:C:CP1:CP2}和{A:4:C:0:C:CP2:CP2}。CP1 的端口优先级向量优于其指定优先级向量、但根优先级向量不是取自端口 CP1 的根路径优先级向量，故 CP1 角色为 Alternate 端口。CP2 仍为根端口。

5. 计算结果

设备和端口的角色确定之后，整个树形拓扑就建立完毕了。经过上述计算后的流量转发线路如图 8-2 所示。

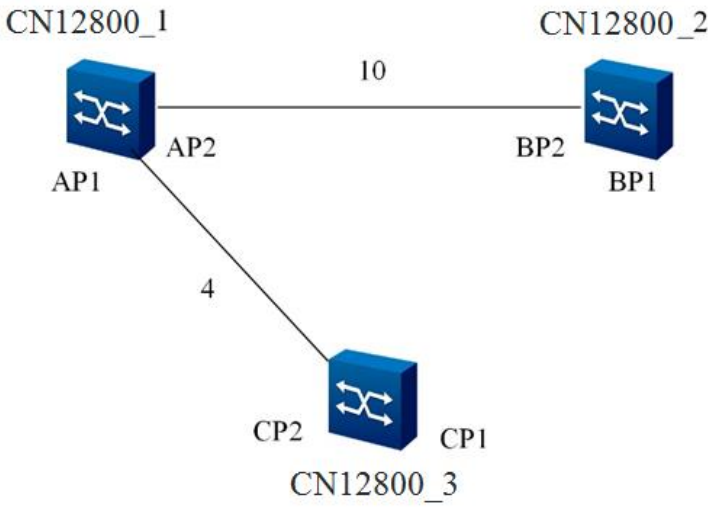


图 8-2 计算后流量转发线路

8.1.4 配置设备加入指定的 MST 域

背景信息

只要以下配置相同，两台交换机就属于同一个域：

- MST 域名
- MSTI 和 VLAN 的映射关系
- MST 域的修订级别

在配置交换机加入指定 MST 域之前，需完成端口物理特性及端口 VLAN 特性的配置。

目的

本节介绍交换机加入 MST 域的配置方法。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
配置交换机生成树的工作模式	1. 进入全局配置视图； 2. 进入 STP 配置视图； 3. 执行命令 **stp mode** { **stp** | **rstp** | **mstp** | **default** }用来设置交换机生成树的工作模式。
配置 MST 域（需要先配置交换机生成树的工作模式为 mstp 模式或 default 模式）	1. 进入全局配置视图； 2. 进入 STP 配置视图； 3. 执行命令 **stp config-name** *string* 用来设置生成树域名；缺省情况下，CN12800 生成树域名为 F-engine； 4. 执行命令 **stp instance** *instance-id* **vlan** *vlan-list* 用来设置 MSTI 应用的 VLAN； 5. 执行命令 **stp revision-level** { *range* | **default** }用来设置设备 MSTP 修订级别。
配置是否使能端口生成树功能（需要先配置交换机生成树的工作模式为 mstp 模式或 default 模式）	1. 进入全局配置视图； 2. 进入接口配置视图（以太网、trunk）、接口组配置视图、批量接口配置视图； 3. 执行命令 **stp** { **enable** | **disable** }用来使能或去使能端口生成树功能。
（可选）配置交换机在指定 MSTI 中的优先级	1. 进入全局配置视图； 2. 进入 STP 配置视图； 3. 执行命令 **stp instance** *instance-id* **priority** { *priority* | **default** }用来设置交换机在指定 MSTI 中的优先级。
（可选）配置 CIST 实例 0 的优先级	1. 进入全局配置视图； 2. 进入 STP 配置视图；

目的	步骤
	3. 执行命令 **stp priority** { *priority* | **default** }用来设置 CIST 实例 0 的优先级。
（可选）配置端口优先级	1. 进入全局配置视图； 2. 进入接口配置视图（以太网、trunk）、PeerLink 配置视图； 3. 执行如下命令： ● **stp priority** { *priority* | **default** } ● **stp process** *process-id* **priority** { *priority* | **default** }。
（可选）配置当前接口在指定 MSTI（MST 实例）上的管理路径开销	1. 进入全局配置视图； 2. 进入接口配置视图（以太网、trunk）、接口组配置视图； 3. 执行命令 **stp instance** *instance-id* **path-cost** { *path-cost* | **default** }配置当前接口在指定 MSTI（MST 实例）上的管理路径开销。
（可选）配置当前接口在指定 MSTI 上的优先级	1. 进入全局配置视图； 2. 进入接口配置视图（以太网、trunk）、接口组配置视图； 3. 执行命令 **stp instance** *instance-id* **priority** { *priority* | **default** }配置当前接口在指定 MSTI 上的优先级。

8.1.5 配置 MSTP 参数

背景信息

在调整交换机的 MSTP 参数前，需要完成以下配置任务：

- 配置端口的物理特性
- 配置端口加入的 VLAN
- 配置交换机加入指定 MST 域

目的

本节介绍调整部分 MSTP 参数的配置方法。

在一些特定的网络环境里，可以通过调整部分交换机的 MSTP 参数以达到最佳效果。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
配置生成树转发时延	1. 进入全局配置视图； 2. 进入 STP 配置视图； 3. 执行命令 **stp forward-delay** { *forward-delay* | **default** }用来设置生成树转发时延。

目的	步骤
配置协议发送 hello 报文间隔时间	1. 进入全局配置视图； 2. 进入 STP 配置视图； 3. 执行命令 **stp hello-time** { *hello-interval* | **default** }用来设置协议发送 hello 报文间隔时间。
配置交换机生成树的最大老化时间	1. 进入全局配置视图； 2. 进入 STP 配置视图； 3. 执行命令 **stp max-age** { *max-age* | **default** }用来设置交换机生成树的最大老化时间。
配置 MST 域内生成树最大跳数	1. 进入全局配置视图； 2. 进入 STP 配置视图； 3. 执行命令 **stp max-hops** { *max-hop* | **default** }设置 MST 域内生成树最大跳数。
配置是否为边缘端口	1. 进入全局配置视图； 2. 进入接口配置视图（以太网、trunk）、接口组配置视图、批量接口配置视图； 3. 执行命令 **stp** { **enable** | **disable** }使能或去使能端口生成树功能； 4. 执行命令 **stp edge-port** { **enable** | **disable** }使能或去使能接口为边缘端口。
配置接口是否点到点管理	1. 进入全局配置视图； 2.进入接口配置视图（以太网、trunk）、接口组配置视图、批量接口配置视图； 3. 执行命令 **stp** { **enable** | **disable** }使能或去使能端口生成树功能； 4. 执行命令 **stp point-to-point** { **force-true** | **force-false** | **auto** }设置接口链路类型。
配置当前接口在指定 MSTI 上的优先级	1. 进入全局配置视图； 2. 进入接口配置视图（以太网、trunk）、接口组配置视图、批量接口配置视图； 3. 执行命令 **stp** { **enable** | **disable** }使能或去使能端口生成树功能； 4. 执行命令 **stp instance** *instance-id* **priority** { *priority* | **default** }设置当前接口在指定 MSTI 上的优先级。
配置当前接口在指定 MSTI（MST 实例）上的管理路径开销	1. 进入全局配置视图； 2. 进入接口配置视图（以太网、trunk）、接口组配置视图、批量接口配置视图； 3. 执行命令 **stp** { **enable** | **disable** }使能或去使能端口生成树功能； 4. 执行命令 **stp instance** *instance-id* **path-cost** { *path-cost* | **default** }设置当前接口在指定 MSTI（MST 实例）上的管理路径开销。
配置生成树 Hello Time 周期内发包	1. 进入全局配置视图； 2. 进入 STP 配置视图；

目的	步骤
次数（即发送的 BPDU 的个数）	3. 执行命令 **stp transmit-limit** { *transmit-limit* | **default** }用来设置生成树 Hello Time 周期内发包次数。
配置接口在实例 0 上的管理路径开销值	1. 进入全局配置视图； 2. 进入接口配置视图（以太网、trunk）、接口组配置视图、批量接口配置视图； 3. 执行命令 **stp** { **enable** | **disable** }使能或去使能端口生成树功能； 4. 执行命令 **stp path-cost** { *cost* | **default** }或 **stp process** *process-id* **path-cost** { *cost* | **default** }设置接口在实例 0 上的管理路径开销值。
配置 STP 端口路径开销计算的标准	1. 进入全局配置视图； 2. 进入 STP 配置视图； 3. 执行命令 **stp pathcost-standard** { **dot1t** | **dot1d-1998** }设置 STP 端口路径开销计算的标准。
配置当前接口执行模式检查操作	1. 进入全局配置视图； 2. 进入接口配置视图（以太网、trunk）、接口组配置视图、批量接口配置视图； 3. 执行命令 **stp** { **enable** | **disable** }使能或去使能端口生成树功能； 4. 执行命令 **stp mcheck** 设置当前接口执行模式检查操作。
配置生成树协议转换周期	1. 进入全局配置视图； 2. 进入 STP 配置视图； 3. 执行命令 **stp migration-time** { *migration-time* | **default** }设置生成树协议转换周期。
配置是否使能生成树 Trap 告警功能	1. 进入全局配置视图； 2. 进入 STP 配置视图； 3. 执行命令 **stp trap** { **enable** | **disable** }使能或去使能生成树 Trap 告警功能。
配置 TC 防攻击包阈值	1. 进入全局配置视图； 2. 进入 STP 配置视图； 3. 执行命令 **stp tc-protection threshold** { *threshold-value* | **default** }配置 TC 防攻击包阈值。
删除生成树实例	1. 进入全局配置视图； 2. 进入 STP 配置视图； 3. 执行命令 **no stp instance** *instance-id* 删除生成树实例。
配置生成树的超时时间	1. 进入全局配置视图； 2. 进入 STP 配置视图； 3. 执行命令 **stp timer-factor** { *timer-value* | **default** }配置生成树的超时时间。
使能或去使能 BPDU filter 功能	1. 执行命令 **configure** 进入全局配置视图；

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

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

8.1.6 配置 MSTP 保护功能

背景信息

- BPDU 保护

对于接入层设备，接入端口一般直接与用户终端（如 PC 机）或文件服务器相连，此时可以设置接入端口为边缘端口以实现这些端口的快速迁移。正常情况下，边缘端口不会收到生成树协议的配置消息（BPDU 报文），但是，如果有人伪造配置消息，恶意攻击交换机，当边缘端口接收到配置消息时，系统会自动将这些端口设置为非边缘端口，重新进行生成树的计算，这将引起网络拓扑的震荡。BPDU 保护功能可以防止这种网络攻击。

- 环路保护

在交换机上，根端口和其他阻塞端口状态是依靠不断接收来自上游交换机的 BPDU 来维持的。当由于链路拥塞或者单向链路故障导致这些端口收不到来自上游交换机的 BPDU 时，此时交换机会重新选择根端口。原先的根端口会转变为指定端口，而原先的阻塞端口会迁移到转发状态，从而造成交换网络中可能产生环路。

环路保护功能会抑制这种环路的产生。在启动了环路保护功能后，如果根端口收不到来自上游的 BPDU 时，根端口会被设置进入阻塞状态；而阻塞端口则会一直保持在阻塞状态，不转发报文，从而不会在网络中形成环路。

- Root 保护

根节点保护功能可以用来防止来历不明的 BPDU 使网络拓扑变化。

由于维护人员的错误配置或网络中的恶意攻击，网络中的合法根桥有可能会收到优先级更高的配置消息，这样当前根桥会失去根桥的地位，引起网络拓扑结构的错误变动。假设原来的流量是经过高速链路转发的，这种不合法的变动，会导致原来通过高速链路的流量被牵引到低速链路上，导致网络拥塞。Root 保护功能可以防止这种情况的发生。

对于设置了 Root 保护功能的端口，端口角色只能保持为指定端口。一旦这种端口上收到了优先级高的配置消息，这些端口的状态将被设置为侦听状态，不再转发报文（相当于将此端口相连的链路断开）。当在足够长的时间内没有收到更优的配置消息时，端口会恢复原来的状态。

- TC 保护

交换机在接收到 TC-BPDU 报文后，会执行 MAC 地址表项和 ARP 表项的删除操作。如果有人伪造 TC-BPDU 报文恶意攻击交换机时，交换机短时间内会收到很多 TC-BPDU 报文，频繁的删除操作会给设备造成很大的负担，给网络的稳定带来很大隐患。

启用防 TC-BPDU 报文攻击功能后，在单位时间内，MSTP 进程处理 TC 类型 BPDU 报文的次数可配置。如果在单位时间内，MSTP 进程在收到 TC 类型 BPDU 报文数量大于配置的阈值，那么 MSTP 进程只会处理阈值指定的次数。对于其他超出阈值的 TC 类型 BPDU 报文，定时器到期后，MSTP 进程只对其统一处理一次。这样可以避免频繁的删除 MAC 地址表项和 ARP 表项，从而达到保护交换机的目的。

目的

当用户需要配置 MSTP 保护功能时，可以使用本节操作。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
配置交换机 BPDU 保护功能	1. 进入全局配置视图； 2. 进入 STP 配置视图； 3. 执行命令 **stp bpdu-guard** { **enable** | **disable** }设置交换机 BPDU 保护功能。
配置交换机的 root 保护功能	1. 进入全局配置视图； 2. 进入接口配置视图（以太网、trunk）、接口组配置视图； 3. 执行命令 **stp root-guard** { **enable** | **disable** }设置交换机环路保护功能。
配置交换机 TC 保护功能	1. 进入全局配置视图； 2. 进入 STP 配置视图； 3. 执行命令 **stp tc-protection** { **enable** | **disable** }设置交换机 TC 保护功能； 4. 执行命令 **stp tc-hold-off** { *time* | **default** }设置拓扑改变延迟/抑制时间。
使能或去使能对 tc-flush-arp 报文的保护功能	1. 进入全局配置视图； 2. 进入 STP 配置视图； 3. 执行命令 **stp tc-flush-arp** { **enable** | **disable** }使能或去使能对 TC-BPDU 报文的保护功能。

目的	步骤
使能或去使能对 TC-BPDU 报文的保护功能	1. 进入全局配置视图； 2. 进入 STP 配置视图； 3. 执行命令 **stp tc-protection** { **enable** | **disable** }使能或去使能对 TC-BPDU 报文的保护功能。
使能或去使能端口生成树环路保护功能	1. 进入全局配置视图； 2. 进入接口配置视图（以太网、trunk）、接口组配置视图； 3. 执行命令 **stp loop-guard** { **enable** | **disable** }使能或去使能端口生成树环路保护功能。
配置接口参与多个 MSTP 进程的状态计算	1. 进入全局配置视图； 2. 进入接口配置视图（以太网、trunk）、接口组配置视图； 3. 执行命令 **stp link-share binding process** *process-list* 配置接口参与多个 MSTP 进程的状态计算。
将当前端口加入指定 ID 的生成树进程中	1. 进入全局配置视图； 2. 进入接口配置视图（以太网、trunk）、接口组配置视图； 3. 执行命令 **stp binding process** *process-id* 将当前端口加入指定 ID 的生成树进程中。
将当前端口退出指定 ID 的生成树进程中	1. 进入全局配置视图； 2. 进入接口配置视图（以太网、trunk）、接口组配置视图； 3. 执行命令 **no stp binding process** *process-list* 将当前端口退出指定 ID 的生成树进程中。
使能或去使能点到点链路检测开关	1. 进入全局配置视图； 2. 进入 STP 配置视图； 3. 执行命令 **stp link-detection** { **enable** | **disable** }使能或去使能点到点链路检测开关。

8.1.7 维护及调试

目的

当 MSTP 功能不正常，需要进行查看、定位问题时，可以使用本小节操作。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
查看交换机生成树协议的配置信息	1. 进入普通用户视图； 2. 执行命令 **show stp** 显示交换机生成树协议的配置信息。

目的	步骤
查看交换机生成树协议的配置文件信息	1. 进入普通用户视图； 2. 执行命令 **show stp config** 显示交换机生成树协议的配置文件信息。
查看交换机生成树协议的相关信息	1. 进入普通用户视图； 2. 执行命令 **show stp information** 显示交换机生成树协议的相关信息。
查看交换机生成树协议实例在全部接口或指定接口的配置信息	1. 进入普通用户视图； 2. 执行命令 **show stp instance** *instance-id* **interface** 显示交换机生成树协议实例在全部接口的配置信息。 3. 执行如下命令显示交换机生成树协议实例指定接口的配置信息： ● **show stp instance** *instance-id* **interface** { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* ● **show stp instance** *instance-id* **interface eth-trunk** *trunk-number*。
查看交换机全部接口生成树协议的配置信息	1. 进入普通用户视图； 2. 执行命令 **show stp interface** 显示交换机全部接口生成树协议的配置信息。
查看交换机指定接口的生成树协议的相关配置信息	1. 进入普通用户视图； 2. 执行如下命令显示交换机指定接口的生成树协议的相关配置信息： ● **show stp interface** { **ethernet** | **gigaethernet** | **xgigaethernet** | **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet**} *interface-number* ● **show stp interface eth-trunk** *trunk-number*。
查看 link up 接口以及保护状态接口的生成树状态信息	1. 进入普通用户视图； 2. 执行命令 **show stp brief** 查看 link up 接口以及保护状态接口的生成树状态信息。
查看生成树多进程当前工作接口的生成树状态	1. 进入普通用户视图； 2. 执行命令 **show stp process** *process-id* **brief** 查看生成树多进程当前工作接口的生成树状态。
查看生成树多进程当前接口的具体信息	1. 进入普通用户视图； 2. 执行如下命令查看生成树多进程当前接口的具体信息： ● **show stp process** *process-id* **interface** { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* ● **show stp process** *process-id* **interface eth-trunk** *trunk-number* ● **show stp processes interface**。
查看端口 TC/TCN 报文收发计数	1. 进入普通用户视图； 2. 执行命令 **show stp tc-bpdu statistic** 查看端口 TC/TCN 报文收发计数。
查看拓扑变化相关的统计信息	1. 进入普通用户视图； 2. 执行命令 **show stp topology-change** 查看拓扑变化相关的统计信息。

目的	步骤
打开或关闭生成树调试功能	1. 进入特权用户视图； 2. 执行如下命令打开或关闭生成树调试功能： ● **debug stp** { **error** | **statemachine** | **protection** | **timer** | **in** | **out** | **packet** | **protocol** | **event** | **sync** | **ptx** | **prx** | **ppm** | **bdm** | **pim** | **prs** | **prt** | **pst** | **tcm** | **all** } **interface** { **ethernet** | **gigaethernet** | **xgigaethernet**| **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number* ● **debug stp** { **error** | **statemachine** | **protection** | **timer** | **in** | **out** | **packet** | **protocol** | **event** | **sync** | **ptx** | **prx** | **ppm** | **bdm** | **pim** | **prs** | **prt** | **pst** | **tcm** | **all** } **interface eth-trunk** *trunk-number* ● **no debug stp** { **error** | **statemachine** | **protection** | **timer** | **in** | **out** | **packet** | **protocol** | **event** | **sync** | **ptx** | **prx** | **ppm** | **bdm** | **pim** | **prs** | **prt** | **pst** | **tcm** | **all** } **interface** { **ethernet** | **gigaethernet** | **xgigaethernet**| **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number* ● **no debug stp** { **error** | **statemachine** | **protection** | **timer** | **in** | **out** | **packet** | **protocol** | **event** | **sync** | **ptx** | **prx** | **ppm** | **bdm** | **pim** | **prs** | **prt** | **pst** | **tcm** | **all** } **interface eth-trunk** *trunk-number* ● **no debug stp all**。

8.1.8 配置举例

组网要求

现有四台支持 MSTP 协议的 CN12800 系列交换机，分别为 CN12800_1、CN12800_2、CN12800_3、CN12800_4。按照如下组网示意图连接，配置 MSTP 基本功能：

- CN12800_1 和 CN12800_3 划分在同一个域内，域名为 Domain1 并创建实例 1。
- CN12800_2 和 CN12800_4 划分在另一个域内，域名为 Domain2 并创建实例 1。
- CN12800_1 为 CIST 总根。
- Domain1 内，CN12800_1 为 CIST 域根，为实例 1 的域根。且在 CN12800_1 的 10GE1/0/1 和 10GE1/0/2 端口上配置根保护功能。
- Domain2 内，CN12800_2 为 CIST 域根，CN12800_4 为实例 1 的域根。
- CN12800_3 和 CN12800_4 的 10GE1/0/1 端口配置为边缘端口，同时应用 BPDU 保护功能。

组网图

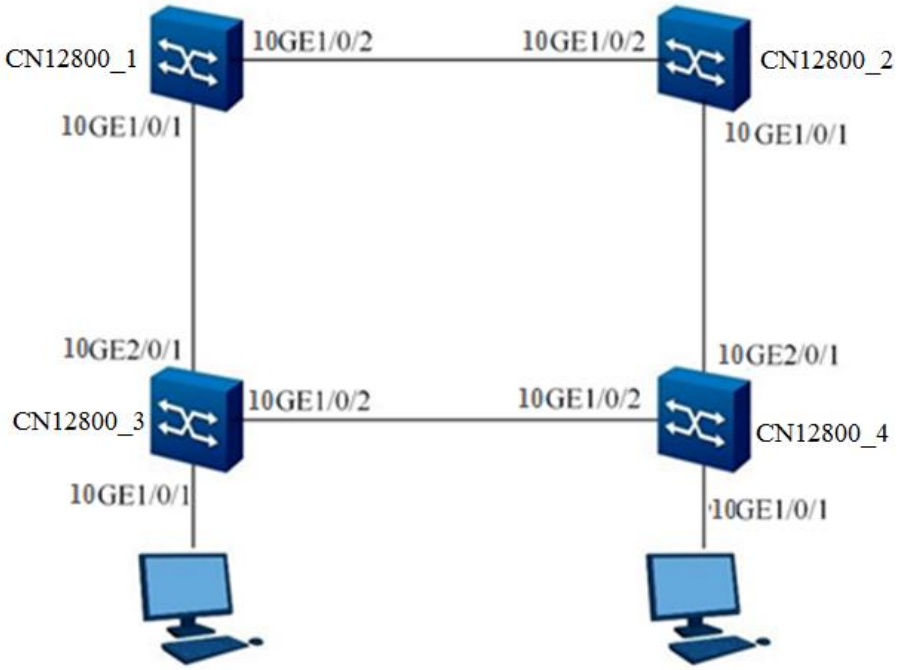


图 8-3 MSTP 组网示意图

配置步骤

1、配置 CN12800_1。

配置 CN12800_1 加入域 Domain1。

CN12800_1#configure

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

CN12800_1(config)#stp

CN12800_1(config-stp)#stp mode mstp

CN12800_1(config-stp)#stp config-name Domain1

CN12800_1(config-stp)#stp instance 1 vlan 1-10

CN12800_1(config-stp)#stp revision-level 1

配置 CN12800_1 在实例 0 中的优先级为 0 以保证 CN12800_1 作为 CIST 的总根。

CN12800_1(config-stp)#stp priority 0

配置 CN12800_1 在实例 1 中的优先级为 0，保证 CN12800_1 作为实例 1 的域根。

CN12800_1(config-stp)#stp instance 1 priority 0

创建 VLAN 2 到 20，并将 CN12800_1 的端口 10GE1/0/1 和 10GE1/0/2 分别加入 1 到 20，使能端口生成树功能，启动端口根保护功能。

CN12800_1(config)#vlan 2-20

CN12800_1(config)#interface 10gigaethernet1/0/1

CN12800_1(config-10ge1/0/1)#port link-type trunk

CN12800_1(config-10ge1/0/1)#port trunk allow-pass vlan 1-20

CN12800_1(config-10ge1/0/1)#stp enable

CN12800_1(config-10ge1/0/1)#stp root-guard enable

CN12800_1(config-10ge1/0/1)#quit

CN12800_1(config)#interface 10gigaethernet1/0/2

CN12800_1(config-10ge1/0/2)#port link-type trunk

CN12800_1(config-10ge1/0/2)#port trunk allow-pass vlan 1-20

CN12800_1(config-10ge1/0/2)#stp enable

CN12800_1(config-10ge1/0/2)# stp root-guard enable

CN12800_1(config-10ge1/0/2)#quit

CN12800_1(config)#

2、配置 CN12800_2。

配置 CN12800_2 加入域 Domain2。

CN12800_2#configure

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

CN12800_2(config)#stp

CN12800_2(config-stp)#stp mode mstp

CN12800_2(config-stp)#stp config-name Domain2

CN12800_2(config-stp)#stp instance 1 vlan 1-10

CN12800_2(config-stp)#stp revision-level 2

配置 CN12800_2 在实例 0 中的优先级为 4096 以保证 CN12800_2 作为 CIST 的总根。

CN12800_2(config-stp)#stp priority 4096

创建 VLAN 2 到 20，并将 CN12800_2 的端口 10GE1/0/1 和 10GE1/0/2 分别加入 1 到 20，使能端口生成树功能，启动端口根保护功能。

CN12800_2(config)#vlan 2-20

CN12800_2(config)#interface 10gigaethernet1/0/1

CN12800_2(config-10ge1/0/1)#port link-type trunk

CN12800_2(config-10ge1/0/1)#port trunk allow-pass vlan 1-20

CN12800_2(config-10ge1/0/1)#stp enable

CN12800_2(config-10ge1/0/1)#stp root-guard enable

CN12800_2(config-10ge1/0/1)#quit

CN12800_2(config)#interface 10gigaethernet1/0/2

CN12800_2(config-10ge1/0/2)#port link-type trunk

CN12800_2(config-10ge1/0/2)#port trunk allow-pass vlan 1-20

CN12800_2(config-10ge1/0/2)#stp enable

CN12800_2(config-10ge1/0/2)#stp root-guard enable

CN12800_2(config-10ge1/0/2)#quit

CN12800_2(config)#

3、配置 CN12800_3。

配置 CN12800_3 加入域 Domain1。

CN12800_3#configure

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

CN12800_3(config)#stp

CN12800_3(config-stp)#stp mode mstp

CN12800_3(config-stp)#stp config-name Domain1

CN12800_3(config-stp)#stp instance 1 vlan 1-10

CN12800_3(config-stp)#stp revision-level 1

启动 BPDU 保护功能。

CN12800_3(config-stp)#stp bpdu-gurad enable

创建 VLAN 2 到 20，并将 CN12800_3 的端口 10GE1/0/2 和 10GE2/0/1 分别加入 1 到 20，使能端口生成树功能，将端口 10GE1/0/1 配置为边缘端口。

CN12800_3(config)#vlan 2-20

CN12800_3(config)#interface 10gigaethernet2/0/1

CN12800_3(config-10ge2/0/1)#port link-type trunk

CN12800_3(config-10ge2/0/1)#port trunk allow-pass vlan 1-20

CN12800_3(config-10ge2/0/1)#stp enable

CN12800_3(config-ge2/0/1)#quit

CN12800_3(config)#interface 10gigaethernet1/0/2

CN12800_3(config-10ge1/0/2)#port link-type trunk

CN12800_3(config-10ge1/0/2)#port trunk allow-pass vlan 1-20

CN12800_3(config-10ge1/0/2)#stp enable

CN12800_3(config-10ge1/0/2)#quit

CN12800_3(config)#interface 10gigaethernet1/0/1

CN12800_3(config-10ge1/0/1)#stp enable

CN12800_3(config-10ge1/0/1)#stp edged-port enable

CN12800_3(config-10ge1/0/1)#port hybrid pvid 20

CN12800_3(config-10ge1/0/1)#port hybrid vlan 20 untagged

CN12800_3(config-10ge1/0/1)#quit

CN12800_3(config)#

4、配置 CN12800_4。

配置 CN12800_4 加入域 Domain2。

CN12800_4#configure

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

CN12800_4(config)#stp

CN12800_4(config-stp)#stp mode mstp

CN12800_4(config-stp)#stp config-name Domain2

CN12800_4(config-stp)#stp instance 1 vlan 1-10

CN12800_4(config-stp)#stp revision-level 2

配置 CN12800_4 在实例 1 中的优先级为 0，保证 CN12800_4 作为实例 1 的域根。

CN12800_4(config-stp)#stp instance 1 priority 0

启动 BPDU 保护功能。

CN12800_4(config-stp)#stp bpdu-gurad enable

创建 VLAN 2 到 20，并将 CN12800_4 的端口 10GE1/0/2 和 10GE2/0/1 分别加入 1 到 20，使能端口生成树功能，将端口 10GE1/0/1 配置为边缘端口。

CN12800_4(config)#vlan 2-20

```
CN12800_4(config)#interface 10gigaethernet2/0/1
CN12800_4(config-10ge2/0/1)#port link-type trunk
CN12800_4(config-10ge2/0/1)#port trunk allow-pass vlan 1-20
CN12800_4(config-10ge2/0/1)#stp enable
CN12800_4(config-10ge2/0/1)#quit
CN12800_4(config)#interface 10gigaethernet1/0/2
CN12800_4(config-10ge1/0/2)#port link-type trunk
CN12800_4(config-10ge1/0/2)#port trunk allow-pass vlan 1-20
CN12800_4(config-10ge1/0/2)#stp enable
CN12800_4(config-10ge1/0/2)#quit
CN12800_4(config)#interface 10gigaethernet1/0/1
CN12800_4(config-10ge1/0/1)#stp enable
CN12800_4(config-10ge1/0/1)#stp edged-port enable
CN12800_4(config-10ge1/0/1)#port hybrid pvid 10
CN12800_4(config-10ge1/0/1)#port hybrid vlan 10 untagged
CN12800_4(config-10ge1/0/1)#quit
CN12800_4(config)#
```

8.2 BFD 配置

8.2.1 BFD 概述

基本概念

BFD（Bidirectional Forwarding Detection）双向转发检测是一套全网统一的用于检测转发设备之间通信故障的检测机制。BFD 能够为相邻转发设备之间的通道故障提供轻负荷、持续时间短的检测；可以对任何介质及协议层进行实时检测。

CN12800 支持的 BFD 特性

- 多跳检测

  多跳检测是指检测两台非直连设备间任意路径的 IP 连通性。多跳检测一般用来检查两台设备之间是否存在可达路由。

- BFD for VRRP

  使用 BFD 检测、监控网络中链路或者 IP 路由转发状况，VRRP 绑定 BFD 会话，BFD 通告会话状态，触发 VRRP 快速切换并进行处理。

- BFD for OSPF

  OSPF 绑定 BFD 会话，BFD 通告会话状态，OSPF 负责处理。

- BFD for IS-IS

  IS-IS 绑定 BFD 会话，BFD 通告会话状态，IS-IS 负责处理。

- BFD for BGP

  BGP 绑定 BFD 会话，BFD 通告会话状态，BGP 负责处理。

- 动态修改 BFD 参数

  BFD 会话建立后，用户仍可以修改 BFD 相关参数的配置，如：BFD 报文期望发送间隔、最小接收间隔以及本地检测倍数。修改参数后不会影响会话当前的状态。

ECHO 功能

BFD 具有两种检测模式异步模式和按需模式，与这两个模式相关的附加功能是 ECHO 功能。

使用 ECHO 功能时，节点向邻居发送一系列 BFD ECHO 包，邻居将这些包反射回发送节点。如果一段时间内没收到回应的 ECHO（或者丢失了大量的 ECHO 包），则通告会话关闭。使用 ECHO 时，ECHO 包用于检测故障，因此可减少 BFD 控制包的速度（异步模式）或完全停止发送 BFD 控制包（按需模式）。

纯粹的异步模式相对 ECHO 有一个优势：为达到同样的检测时间，异步模式需要的 BFD 控制包数目是 ECHO 包数目的一半。如果因为某种原因不能使用 ECHO 功能，也需要使用异步模式。

ECHO 功能的优点是，他只检测邻居上的转发路径。这可以减小往返时间抖动，可以实现更快的检测时间，并可检测一些其他方法无法检测的故障。

ECHO 功能可在两个方向上单独使能。在一个特定方向上使能 ECHO 功能的前提条件是：执行反射 ECHO 操作的节点表明自己允许运行 ECHO 功能，而发送 ECHO 的节点表明自己希望执行 ECHO 功能。

8.2.2 配置 BFD 检测功能

前提条件

在配置 BFD 检测功能之前必须先配置 VLAN 接口以及 IP 地址。如果用户还需要检测网络层的连通性，则需要先配置好路由协议。

背景信息

目前 CN12800 数据中心交换机不支持 demand 模式。

若单独使用 BFD 功能、静态路由或 BFD 配合 VRRP 使用，需配置 bfd track 命令。

若 BFD 配合其他协议动态触发使用，则不需要再配置 bfd track 命令。

配置角色时，对于 BFD 会话建立过程中的初始化阶段，两端是主动角色还是被动角色是由应用来决定的，但是至少有一端为主动角色。

目的

当用户需要快速检测和监控网络中直连或设备间 IP 路由的连通状况，可以使用本节操作配置 BFD 检测功能。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
全局使能或去使能 BFD 功能	1. 进入全局配置视图； 2. 执行命令 **bfd** { **start** | **stop** }全局启动或停止 BFD 功能。
配置 BFD 会话	1. 进入全局配置视图； 2. 执行如下命令添加基于 IP 地址的静态 BFD 会话： ● **bfd track** *track-number* **subsession link-auto switch** ● **bfd track** *track-number* **remote-ip** *ipv4-address1* **local-ip** *ipv4-address2* **vlan** *vlan-id* ● **bfd track** *track-number* **remote-ip** *ipv4-address1* **local-ip** *ipv4-address2* **vlan** *vlan-id* **one-arm-echo** ● **bfd track** *track-number* **remote-ip** *ipv4-address1* { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* ● **bfd track** *track-number* **remote-ip** *ipv4-address1* **{ ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number.subinterface* ● **bfd track** *track-number* **remote-ip** *ipv4-address1* **local-ip** *ipv4-address2* { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* **one-arm-echo**

目的	步骤
	● **bfd track** *track-number* **remote-ip** *ipv4-address1* **local-ip** *ipv4-address2* **{ ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number.subinterface* **one-arm-echo** ● **bfd track** *track-number* **remote-ip** *ipv4-address1* **local-ip** *ipv4-address2* { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* ● **bfd track** *track-number* **remote-ip** *ipv4-address1* **local-ip** *ipv4-address2* ● **bfd track** *track-number* **remote-ip** *ipv4-address1* **vlan** *vlan-id* ● **bfd track** *track-number* **remote-ip** *ipv4-address1* ● **bfd track** *track-number* **remote-ip6** *ipv6-address1* **local-ip6** *ipv6-address2* **vlan** *vlan-id* ● **bfd track** *track-number* **remote-ip6** *ipv6-address1* **local-ip6** *ipv6-address2* **vlan** *vlan-id* **one-arm-echo** ● **bfd track** *track-number* **remote-ip6** *ipv6-address1* { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* ● **bfd track** *track-number* **remote-ip6** *ipv6-address1* **{ ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number.subinterface* ● **bfd track** *track-number* **remote-ip6** *ipv6-address1* **local-ip6** *ipv6-address2* { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* **one-arm-echo** ● **bfd track** *track-number* **remote-ip6** *ipv6-address1* **local-ip6** *ipv6-address2* { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* ● **bfd track** *track-number* **remote-ip6** *ipv6-address1* **local-ip6** *ipv6-address2* { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* **one-arm-echo** ● **bfd track** *track-number* **remote-ip6** *ipv6-address1* **local-ip6** *ipv6-address2* { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number.subinterface* **one-arm-echo** ● **bfd track** *track-number* **remote-ip6** *ipv6-address1* **local-ip6** *ipv6-address2* ● **bfd track** *track-number* **remote-ip6** *ipv6-address1* **vlan** *vlan-id* ● **bfd track** *track-number* **remote-ip6** *ipv6-address1*。
接口上使能或去使能 BFD 协议	1. 进入全局配置视图； 2. 进入接口配置视图、VLANIF 配置视图、Loopback 接口配置视图、Trunk 接口配置视图；

目的	步骤
	3. 执行命令 **bfd** { **enable** | **disable** }使能或去使能接口 BFD。
（可选）配置 BFD 会话状态告警功能	1. 进入全局配置视图； 2. 执行命令 **bfd trap** { **enable** | **disable** }使能或去使能 BFD 会话状态（up 或 down）告警功能。
在物理端口下删除 track 信息	1. 进入全局配置视图； 2. 执行如下命令： ● **no bfd track all** ● **no bfd track** *track-number* ● **no bfd track** *track-number* **subsession link-auto switch**。

8.2.3 配置 BFD 检测参数

目的

当在建立 BFD 会话时，可以根据网络状况和性能需求，调整设备的 BFD 报文期望发送间隔、最小接收间隔以及本地检测倍数，可以使用本小节操作。

通常情况下，使用系统的缺省配置即可。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
配置 BFD 最小发包间隔时间、最小收包间隔时间以及检测超时倍数	1. 进入全局配置视图； 2. 进入接口配置视图、VLANIF 配置视图、Loopback 接口配置视图； 3. 执行命令 **bfd min-tx** *tx-interval* **min-rx** *rx-interval* **multiplier** *timeout-multiple* 调整 BFD 最小发包间隔时间、最小收包间隔时间以及检测超时倍数。
配置BFD会话最小发包间隔时间、最小收包间隔时间以及检测超时倍数	1. 进入全局配置视图； 2. 进入VLANIF配置视图、Loopback接口配置视图、以太网桥接接口配置视图、以太网路由接口配置视图、Trunk接口配置视图； 3. 执行命令**bfd track** *track-number* **min-tx** { *tx-interval* | **default** } **min-rx** { *rx-interval* | **default** } **multiplier** { *timeout-multiple* | **default** }。

8.2.4 维护及调试

目的

当 BFD 功能不正常，需要进行查看、定位问题时，可以使用本小节操作。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
查看配置了 BFD 的接口信息	1. 进入普通用户视图、特权用户视图、全局配置视图、接口配置视图（以太网接口、trunk 接口）、VLANIF 配置视图、接口组配置视图； 2. 执行命令 **show bfd interface** 显示使能了 BFD 的接口信息。
查看动态建立的 BFD 会话信息	1. 进入普通用户视图、特权用户视图、全局配置视图、接口配置视图（以太网接口、trunk 接口）、VLANIF 配置视图、接口组配置视图； 2. 执行命令 **show bfd session** 显示动态建立的 BFD 会话信息。
查看静态 BFD 会话信息	1. 进入普通用户视图、特权用户视图、全局配置视图、接口配置视图（以太网接口、trunk 接口） 、VLANIF 配置视图、接口组配置视图； 2. 执行命令 **show bfd track** *track-number* 或 **show bfd track** 显示静态 BFD 会话信息。
查看 BFD 会话配置信息	1. 进入普通用户视图、特权用户视图、全局配置视图、接口配置视图（以太网接口、trunk 接口）、VLANIF 配置视图、接口组配置视图； 2. 执行命令 **show bfd config** 查看 BFD 会话配置信息。

8.2.5 配置举例

 注意：

在 VLAN 接口下配置 BFD 时，首先要保证两台设备相互能够 Ping 通。

8.2.5.1 多跳检测应用

组网要求

三台 CN12800 相连如下图所示，配置 BFD 多跳检测，用于检测 CN12800_1、CN12800_3 之间的多跳路径，需将接口加入 VLAN、创建接口 VLANIF 并在其上配置 IP 地址。

组网图

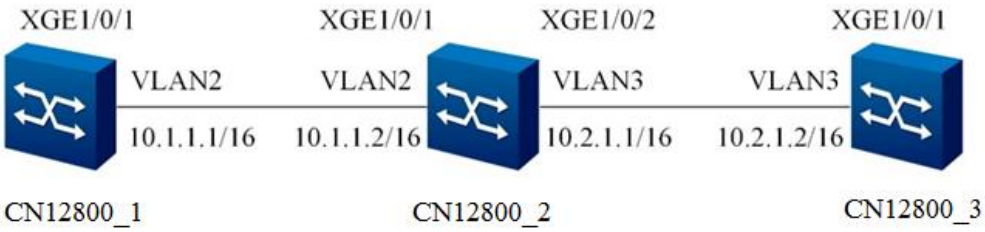


图 8-4 BFD 多跳检测组网图

配置步骤

1、配置 CN12800_1。

#将接口 xgigaethernet1/0/1 加入 VLAN2，并配置 IP 地址为 10.1.1.1/16。

CN12800_1#configure

CN12800_1(config)#interface vlan 2

CN12800_1(config-vlan-2)#ip address 10.1.1.1/16

CN12800_1(config-vlan-2)#quit

CN12800_1(config)#interface xgigaethernet 1/0/1

CN12800_1(config-10ge1/0/1)#port hybrid pvid vlan 2

CN12800_1(config-10ge1/0/1)#port hybrid vlan 2 untagged

CN12800_1(config-10ge1/0/1)#quit

CN12800_1(config)#

#配置静态路由，使 CN12800_1 与 CN12800_3 之间路由可达。

CN12800_1(config)#ip route-static 10.2.0.0 255.255.0.0 10.1.1.2

#配置 BFD 会话参数，A 端（主动）。

CN12800_1(config)#bfd start

CN12800_1(config)#interface vlan 2

CN12800_1(config-vlan-2)#bfd enable

CN12800_1(config)#bfd track 1 remote-ip 10.2.1.2 local-ip 10.1.1.1 vlan 2

#可选配置。

CN12800_1(config-vlan-2)#bfd role active

CN12800_1(config-vlan-2)#bfd min-tx 300 min-rx 300 multiplier 3

CN12800_1(config-vlan-2)#quit

CN12800_1(config)#

2、配置 CN12800_2。

#将接口 xgigaethernet1/0/1 加入 VLAN2，并配置 IP 地址为 10.1.1.2/16。

CN12800_2#configure

CN12800_2(config)#interface vlan 2

CN12800_2(config-vlan-2)#ip address 10.1.1.1/16

CN12800_2(config-vlan-2)#quit

CN12800_2(config)#interface xgigaethernet 1/0/1

CN12800_2(config-10ge1/0/1)#port hybrid pvid vlan 2

CN12800_2(config-10ge1/0/1)#port hybrid vlan 2 untagged

CN12800_2(config-10ge1/0/1)#quit

CN12800_2(config)#

#将接口 xgigaethernet1/0/2 加入 VLAN3，并配置 IP 地址为 10.2.1.1/16

CN12800_2(config)#interface vlan 3

CN12800_2(config-vlan-3)#ip address 10.2.1.1/16

CN12800_2(config-vlan-3)#quit

CN12800_2(config)#interface xgigaethernet 1/0/2

CN12800_2(config-10ge1/0/2)#port hybrid pvid vlan 3

CN12800_2(config-10ge1/0/2)#port hybrid vlan 3 untagged

CN12800_2(config-10ge1/0/2)#quit

CN12800_2(config)#

3、配置 CN12800_3。

#将接口 xgigaethernet1/0/1 加入 VLAN3，并配置 IP 地址为 10.2.1.2/16。

CN12800_3#configure

CN12800_3(config)#interface vlan 3

CN12800_3(config-vlan-3)#ip address 10.2.1.2/16

CN12800_3(config-vlan-3)#quit

CN12800_3(config)#interface xgigaethernet 1/0/1

CN12800_3(config-10ge1/0/1)#port hybrid pvid vlan 3

CN12800_3(config-10ge1/0/1)#port hybrid vlan 3 untagged

CN12800_3(config-10ge1/0/1)#quit

CN12800_3(config)#

#配置静态路由，使 CN12800_3 与 CN12800_1 之间路由可达。

CN12800_3(config)#ip route-static 10.1.0.0 16 10.2.1.1

#配置 BFD 会话参数，C 端（主动或被动）。

CN12800_3(config)#bfd start

CN12800_3(config)#interface vlan 3

CN12800_3(config-vlan-3)#bfd enable

CN12800_3(config)#bfd track 1 remote-ip 10.1.1.1 local-ip 10.2.1.2 vlan 3

可选配置。

CN12800_3(config-vlan-3)#bfd role passive （也可以是 active）

CN12800_3(config-vlan-3)#bfd min-tx 300 min-rx 300 multiplier 3

CN12800_3(config-vlan-2)#quit

CN12800_3(config)#

8.3 VRRP 配置

8.3.1 VRRP 概述

基本概念

如图 8-5 所示，通常一个网络内的所有主机都设置一条缺省路由（图中的缺省路由地址为 10.100.10.1），主机发往外部网络的报文将通过缺省路由发往三层交换机 Switch，从而实现了主机与外部网络的通信。当交换机 Switch 发生故障时，本网段内所有以 Switch 为缺省路由下一跳的主机将断掉与外部的通信。

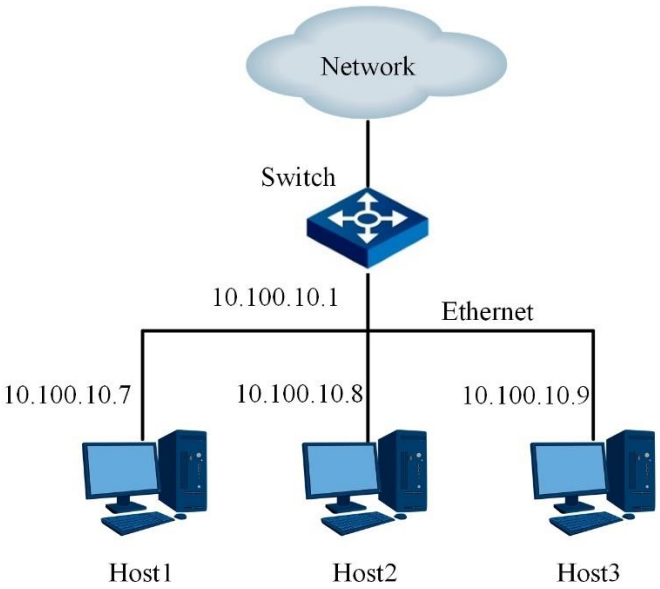


图 8-5 局域网组网方案

VRRP（Virtual Router Redundancy Protocol，虚拟路由冗余协议）是 RFC3768 定义的一种容错协议，就是为解决上述问题而提出的。

通过物理设备和逻辑设备的分离，VRRP 协议实现在多个出口网关之间的选路。VRRP 为具有多播或广播能力的局域网（如以太网）提供逻辑网关。在无需修改路由协议配置的情况下，还能够解决因某网关设备故障带来的业务中断。

VRRP 工作原理

如图 8-6 所示，VRRP 将局域网的一组交换机（包括一个 Master 即主交换机和若干个 Backup 即备份交换机）组织成一个虚拟路由器，这组交换机被称为一个备份组。虚拟的路由器拥有自己的 IP 地址 10.100.10.1（这个 IP 地址可以和备份组内的某个交换机的接口地址相同）和专用的 MAC 地址，备份组内的交换机也有自己的 IP 地址（如 Master 的 IP 地址为 10.100.10.2，Backup 的 IP 地址为 10.100.10.3）。局域网内的主机仅仅知道这个虚拟路由器的 IP 地址 10.100.10.1（通常被称为备份组的虚拟 IP 地址），而不知道具体的 Master 交换机的 IP 地址 10.100.10.2 以及 Backup 交换机的 IP 地址 10.100.10.3。局域网内的主机将自己的缺省路由下一跳设置为该虚拟路由器的 IP 地址 10.100.10.1。于是，网络内的主机就通过这个虚拟的交换机与其它网络进行通信。在正常情况下，Master 对虚拟地址 ARP 请求进行应答，当备份组内的 Master 交换机不能正常工作时，备份组内的其它 Backup 交换机将接替不能正常工作的 Master 交换机成为新的 Master 交换机，继

续向网络内的主机提供路由服务，同时保持虚拟地址的 ARP 条目不变，从而实现网络内的主机不间断地与外部网络进行通信。

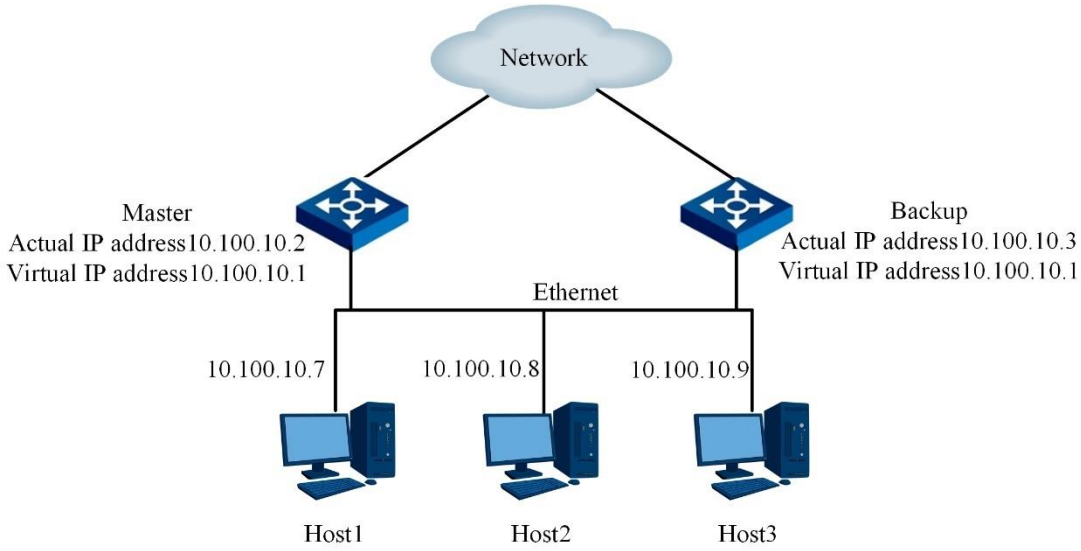


图 8-6 虚拟路由器示意图

CN12800 支持的 VRRP 特性

- VRRP 主备备份

  该功能是 VRRP 提供 IP 地址备份功能的基本方式。通过建立一个虚拟路由器，包括一个 Master 和若干 Backup 设备，由这些设备构成一个备份组。正常情况下，由 Master 转发全部业务流，当 Master 出现故障时，由 Backup 接替其工作。

- VRRP 负载分担

  负载分担方式是指建立两个或多个备份组，多台交换机同时承担通讯业务。其中允许一台交换机为多个备份组作备份，在不同备份组中有不同的优先级。通过多虚拟交换机设置可以实现负载分担。每个备份组都包括一个 Master 设备和若干 Backup 设备。各备份组的 Master 可以不同。

- VRRP 接口联动

  通过配置关联接口，在上行接口断开的情况下，下行接口上的 VRRP 主动降低优先级，使其低于对端 VRRP 的优先级，状态变为 Backup，这样从 VRRP 接口上收到的包将通过另外一个节点进行转发。

- VRRP 快速切换

通过 BFD 机制能够快速检测、监控网络中链路或者 IP 路由的连通状况。VRRP 可以通过监视 BFD 会话状态实现主备快速切换。

- VRRP 安全功能

  为增强 VRRP 的安全性，可以对 VRRP 采用认证。在一个安全的网络环境中，可以不对 VRRP 报文进行任何认证；在有可能受到安全威胁的网络环境中，VRRP 可以提供简单字符认证或 MD5 认证方式。

8.3.2 配置 VRRP 备份组

背景信息

VRRP 备份组中设备的优先级表明设备成为 Master 的优先程度。VRRP 协议首先会根据备份组中设备的优先级字段进行判断，并选择优先级最高的设备作为 Master；如果备份组中出现相同优先级的设备，则根据设备 IP 地址进行优先级排序。如果管理员认为某一设备应该作为 Master（比如接口带宽较高），则可为其设置较高的优先级，强制此设备成为 Master。

设置 VRRP 虚拟路由器的 IP 地址，此 IP 地址将作为直连主机的默认网关。


说明：

配置的虚拟 IP 地址必须和当前接口 IP 地址在同一网段。

前提条件

配置 VRRP 备份组之前，请配置以下任务：

- 配置接口物理参数及链路属性。
- 配置接口的网络层属性，使网络连通。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
创建业务 VRRP 备份组	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图； 3. 执行命令 **ip vrrp** *virtual-route-id* 创建业务备份组。

目的	步骤
配置和虚拟路由器关联的虚拟 IP 地址	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图； 3. 执行命令 **ip vrrp** *virtual-route-id* **associate-address** *ip-address* 配置和虚拟路由器关联的虚拟 IP 地址。
配置交换机在备份组中的优先级	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图； 3. 执行命令 **ip vrrp** *virtual-route-id* **priority** { *priority* | **default** }配置交换机在备份组中的优先级。
配置发送 VRRP 通告报文的时间间隔	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图； 3. 执行命令 **ip vrrp** *virtual-route-id* **advertise-interval** { *interval-time* | **default** }配置 VRRP 协议通告报文的发送时间间隔。
创建管理 VRRP 备份组	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图； 3. 执行命令 **ip vrrp** *virtual-route-id* **role admin** 创建管理 VRRP 备份组。
删除管理 VRRP 备份组	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图； 3. 执行命令 **no ip vrrp** *virtual-route-id* **role admin** 删除管理 VRRP 备份组。
配置业务 VRRP 备份组与管理 VRRP 备份组的绑定关系	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图； 3. 执行命令 **ip vrrp** *virtual-route-id* 创建业务备份组； 4. 执行命令 **ip vrrp** *virtual-route-id* **role admin** 创建管理 VRRP 备份组； 5. 进到成员 VRRP 视图下执行命令 **ip vrrp** *virtual-route-id1* **track admin-vrrp interface vlan** *vlan-id virtual-route-id2* 配置业务 VRRP 备份组与管理 VRRP 备份组的绑定关系； 注：该命令中第一个参数 virtual-route-id1 是业务 VRRP 备份组 ID；第二个参数 virtual-route-id2 是管理 VRRP 备份组 ID。
取消业务 VRRP 备份组与管理 VRRP 备份组之间的绑定关系	1. 执行命令 **no ip vrrp** *virtual-route-id1* **track admin-vrrp interface vlan** *vlan-idvirtual-route-id2* 取消业务 VRRP 备份组与管理 VRRP 备份组之间的绑定关系。

8.3.3 配置 VRRP 接口联动

背景信息

VRRP 协议只能监测下行链路的故障，而在实际的网络应用中，往往会出现上行链路出现中断的情况。若此时上层的拓扑中使用静态路由，在这种情况下，VRRP 的接口联动

功能就显得尤为重要。接口联动功能可以用来监视未配置 VRRP 协议的上行接口是否为 up，从而来更新相对应的 VRRP 状态。

前提条件

配置 VRRP 接口联动功能之前，请配置以下任务：

- 配置接口网络层属性，使网络连通。
- 配置 VRRP 备份组。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置 VRRP 与接口状态联动监视接口功能	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图； 3. 执行命令 **ip vrrp** *virtual-route-id* **track interface vlan** *vlan-id* 或 **ip vrrp** *virtual-route-id* **track interface vlan** *vlan-id* { **increased** | **reduced** } { *priority-value* | **default** }配置 VRRP 与接口状态联动监视接口功能。
取消配置 VRRP 与接口状态联动监视接口功能	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图； 3. 执行命令 **no ip vrrp** *virtual-route-id* **track interface vlan** *vlan-id* 取消配置 VRRP 与接口状态联动监视接口功能。

8.3.4 配置 VRRP 认证方式

背景信息

在安全的网路环境下，可以不需要对 VRRP 报文进行认证字的设置，CN12800 不对发送或接收的报文进行认证处理，认为都是真实的合法的 VRRP 报文。

在有可能受到安全威胁的网络环境下，VRRP 提供简单字符和 MD5 两种认证方式。

前提条件

配置 VRRP 认证方式之前，请配置以下任务：

- 配置接口物理参数及链路属性。
- 配置接口的网络层属性，使网络连通。
- 配置 VRRP 备份组。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置 VRRP 备份组的认证方式和认证字	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图； 3. 执行命令 **ip vrrp** *virtual-route-id* **authentication-mode** { **simple** | **md5** } { **cipher** | **plain** } *key* 或者 **ip vrrp** *virtual-route-id* **authentication-mode** { **simple** | **md5** } *key* 配置 VRRP 备份组的认证方式和认证字。
取消 VRRP 备份组的认证方式和认证	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图； 3. 执行命令 **no ip vrrp** *virtual-route-id* **authentication-mode** 取消 VRRP 备份组的认证方式和认证。
使能或者去使能对 VRRP 报文的 TTL 值进行检测	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图； 3. 执行命令 **ip vrrp** *vrrp-id* **check-ttl** { **enable** | **disable** }使能或者去使能对 VRRP 报文的 TTL 值进行检测。

8.3.5 配置 VRRP 参数

背景信息

通过调整 VRRP 报文的相关参数可以优化备份组功能：

- VRRP 实例的每一个接口都周期性向接口上发送 VRRP 报文。这个周期性间隔时间决定了 VRRP 主备倒换操作的速度。周期性间隔时间一般使用默认值即可，但在特定情况下，可以使用本节操作改变默认的通告间隔时间。对于此时间的设置，如果设置的时间较短，则会使 VRRP 的灵敏度很高，这样可以缩短主备之间切换的时间，减少数据的丢失；如果时间设置较长，发送通告数据包的时间间隔增大，则可以减轻网络的负担。
- 如果需要高优先级的设备能够主动成为 Master，则应将设备配置为抢占模式。


说明：

建议备份组中所有设备采用相同的通告间隔时间。

前提条件

配置 VRRP 参数之前，请配置以下任务：

- 配置接口物理参数及链路属性。

- 配置接口的网络层属性，使网络连通。
- 配置 VRRP 备份组。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置 VRRP 协议通告报文的发送间隔时间	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图； 3. 执行命令 **ip vrrp** *virtual-route-id* **advertise-interval** { *interval-time* | **default** }配置 VRRP 协议通告报文的发送间隔时间。
使能 VRRP 抢占模式	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图； 3. 执行命令 **ip vrrp** *virtual-route-id* **preempt enable** 使能 VRRP 抢占模式。
去使能 VRRP 抢占模式	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图； 3. 执行命令 **ip vrrp** *virtual-route-id* **preempt disable** 去使能 VRRP 抢占模式。
使能或者去使能 SNMP 告警功能	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **ip vrrp snmp-trap** { **enable** | **disable** }使能或者去使能 SNMP 告警功能。
使能或者去使能 VRRP 备份组中 Master 设备发送免费 ARP 报文	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图； 3. 执行命令 **ip vrrp** *vrrp-id* **gratuitous-arp** { **enable** | **disable** }使能或者去使能 VRRP 备份组中 Master 设备发送免费 ARP 报文。
配置 VRRP 备份组中的 Master 设备发送免费 ARP 报文的时间间隔	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图； 3. 执行命令 **ip vrrp** *vrrp-id* **gratuitous-arp timeout** { *time* | **default** }配置 VRRP 备份组中的 Master 设备发送免费 ARP 报文的时间间隔。
配置关联虚拟接口状态从 backup 到 master 的超时倍数	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图； 3. 执行命令 **ip vrrp** *vrrp-id* **holding-multiplier** { *time* | **default** }配置关联虚拟接口状态从 backup 到 master 的超时倍数。
配置备份组中设备的抢占延迟时间	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图； 3. 执行命令 **ip vrrp** *virtual-route-id* **preempt timer delay** { *delay-value* | **default** }配置备份组中设备的抢占延迟时间。

目的	步骤
配置管理 VRRP 所关联的 VRRP 备份组	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图； 3. 执行命令 **ip vrrp admin-vrrp** *virtual-route-id1* **associate-vrrp interface vlan** *vlan-id virtual-route-id2* 配置管理 VRRP 所关联的 VRRP 备份组。
取消管理 VRRP 所关联的 VRRP 备份组	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图； 3. 执行命令 **no ip vrrp admin-vrrp** *virtual-route-id1* **associate-vrrp interface vlan** *vlan-id virtual-route-id2* 取消管理 VRRP 所关联的 VRRP 备份组。

8.3.6 配置 VRRP 监视 BFD 会话状态

背景信息

使用 VRRP 监视 BFD 会话，当 BFD 会话状态在改变后会通知 VRRP 模块，实现 VRRP 快速切换功能。

前提条件

配置 VRRP 认证方式之前，请配置以下任务：

- 配置接口的网络层属性，使网络连通
- 配置 VRRP 备份组
- 配置 BFD 会话

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
绑定 BFD 会话与 VRRP 实例	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图； 3. 执行命令 **ip vrrp** *virtual-route-id* **track bfd-session** *bfdsession-id* 或执行命令 **ip vrrp** *virtual-route-id* **track bfd-session** *bfdsession-id* { **increased** | **reduced** } { *priority-value* | **default** }绑定 BFD 会话与 VRRP 实例。
解除 BFD 会话与 VRRP 实例的绑定关系	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图； 3. 执行命令 **no ip vrrp** *virtual-route-id* **track bfd-session** *bfdsession-id* 解除绑定关系。

8.3.7 维护及调试

目的

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

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
打开 VRRP 调试功能	1. 保持当前特权用户视图； 2. 执行命令 **debug vrrp** { **snmp** | **in** | **out** | **event** | **all** }打开 VRRP 功能调试开关。
关闭 VRRP 调试功能	1. 保持当前特权用户视图； 2. 执行命令 **no debug vrrp** { **snmp** | **in** | **out** | **event** | **all** }关闭 VRRP 能调试开关。
查看 VRRP 信息	1. 执行命令 **disable** 退出到普通用户视图，或执行命令 **configure** 进入全局配置视图，或执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图，或不执行任何命令保持当前特权用户视图； 2. 执行命令 **show ip vrrp** 查看 VRRP 信息。
查看 VRRP 相关联的接口信息	1. 执行命令 **disable** 退出到普通用户视图，或执行命令 **configure** 进入全局配置视图，或执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图，或不执行任何命令保持当前特权用户视图； 2. 执行命令 **show ip vrrp associate interface** 查看 VRRP 配置信息。
查看 VRRP 运行的配置信息	1. 执行命令 **disable** 退出到普通用户视图，或执行命令 **configure** 进入全局配置视图，或执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图，或不执行任何命令保持当前特权用户视图； 2. 执行命令 **show ip vrrp config** 查看 VRRP 配置信息。
查看 VRRP 路由器详细信息	1. 执行命令 **disable** 退出到普通用户视图，或执行命令 **configure** 进入全局配置视图，或执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图，或不执行任何命令保持当前特权用户视图； 2. 执行命令 **show ip vrrp interface vlan** *vlan-id virtual-route-id* 查看 VRRP 路由器详细信息。
重置 VRRP 全局统计信息	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **reset ip vrrp statistic** 查看 VRRP 配置信息。
查看管理 VRRP 配置信息	1. 执行命令 **disable** 退出到普通用户视图，或执行命令 **configure** 进入全局配置视图，或执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图，或不执行任何命令保持当前特权用户视图； 2. 执行命令 **show ip vrrp admin-vrrp** 查看管理 VRRP 配置信息。

目的	步骤
查看 VRRP 的绑定信息	1. 执行命令 **disable** 退出到普通用户视图，或执行命令 **configure** 进入全局配置视图，或执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图，或不执行任何命令保持当前特权用户视图； 2. 执行命令 **show ip vrrp binding** 或执行命令 **show ip vrrp binding admin-vrrp interface vlan** *vlan-id virtual-route-id* 查看 VRRP 的绑定信息。
查看 VRRP 的统计信息	1. 执行命令 **disable** 退出到普通用户视图，或执行命令 **configure** 进入全局配置视图，或执行命令 **interface vlan** *vlan-id* 进入 VLANIF 配置视图，或不执行任何命令保持当前特权用户视图； 2. 执行命令 **show ip vrrp statistic** 查看 VRRP 的统计信息。
查看 IPv4/IPv6 的 VRRP 的详细信息	1. 进入普通用户视图； 2. 执行命令 **show { ip | ipv6 } vrrp verbose** 查看 IPv4/IPv6 的 VRRP 的详细信息。

8.3.8 配置举例

8.3.8.1 配置 VRRP 主备备份

组网需求

主机 Host1、Host2、Host3 通过 SwitchA 访问外部网络。VRRP 协议根据 SwithcA 和 SwitchB 配置的优先级来确定 VRRP 备份组内哪个交换机作为 Master。当作为 Master 的交换机的状态变为 Down 时，则作为 Backup 的交换机将替换 Master 交换机使主机可以与外网通信。

组网图

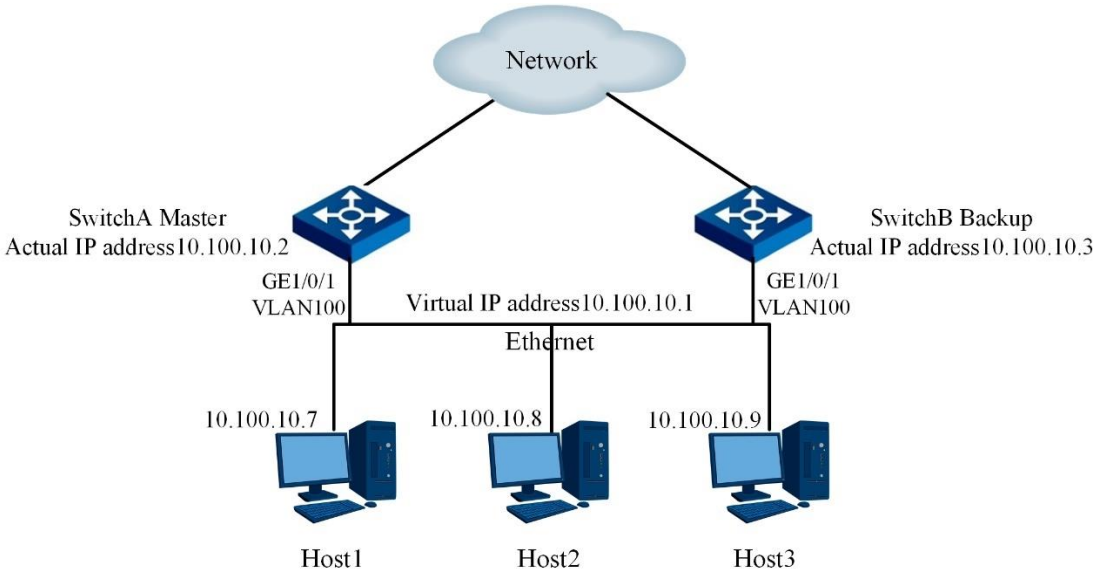


图 8-7 VRRP 主备备份组网图

配置步骤

1、配置 SwitchA。

//配置接口实际的 IP 地址。

SwitchA#configure

SwitchA(config)#interface gigaethernet 1/0/1

SwitchA(config-ge1/0/1)#port hybrid vlan 100 tagged

SwitchA(config-ge1/0/1)#quit

SwitchA(config)#interface vlan 100

SwitchA(config-vlan-100)#ip address 10.100.10.2/24

//创建 VRRP 记录表项即备份组。

SwitchA(config-vlan-100)#ip vrrp 1

//配置接口虚拟 IP 地址。

SwitchA(config-vlan-100)#ip vrrp 1 associate-address 10.100.10.1

2、配置 SwitchB。

//配置接口实际的 IP 地址。

SwitchB#configure

SwitchB(config)#interface gigaethernet 1/0/1

SwitchB(config-ge1/0/1)#port hybrid vlan 100 tagged

SwitchB(config-ge1/0/1)#quit

SwitchB(config)#interface vlan 100

SwitchB(config-vlan-100)#ip address 10.100.10.3/24

//创建 VRRP 记录表项即备份组。

SwitchB(config-vlan-100)#ip vrrp 1

//配置接口虚拟 IP 地址。

SwitchB(config-vlan-100)#ip vrrp 1 associate-address 10.100.10.1

//配置选举优先级低于 SwitchA。

SwitchB(config-vlan-100)#ip vrrp 1 priority 25

8.3.8.2 配置 VRRP 快速切换

组网需求

主机 Host1、Host2、Host3 通过 SwitchA 访问外部网络。VRRP 协议根据 SwithcA 和 SwitchB 配置的优先级来确定 VRRP 备份组内哪个交换机作为 Master。同时，在作为 Backup 的 SwitchB 上配置 VRRP 监视 BFD Session，当作为 Master 的交换机的状态变为 Down 时，则作为 Backup 的交换机将快速进行主备切换替换 Master 交换机使主机可以与外网通信。

组网图

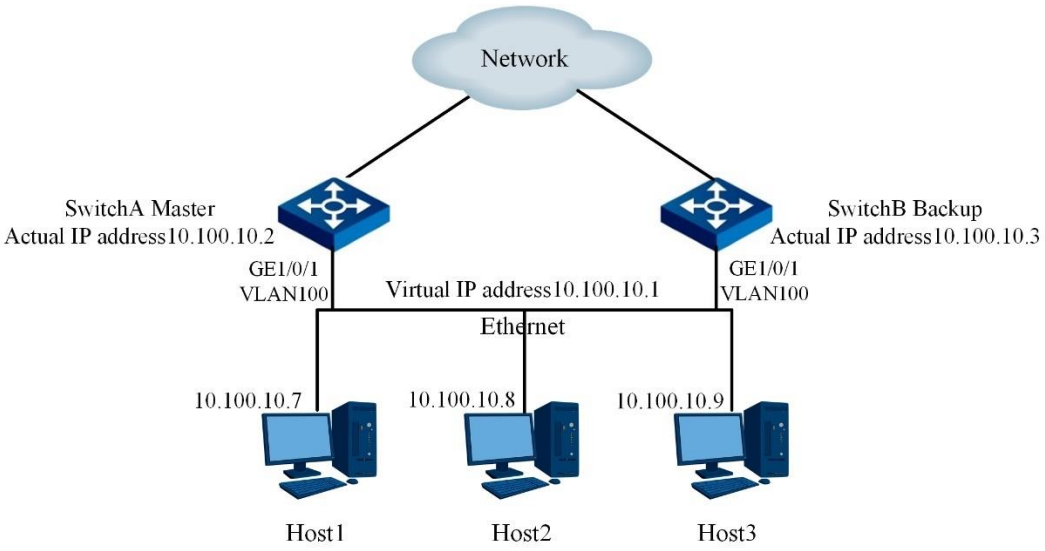


图 8-8 VRRP 快速切换组网图

配置步骤

1、配置 SwitchA。

//配置接口实际的 IP 地址。

SwitchA#configure

SwitchA(config)#interface gigaethernet 1/0/1

SwitchA(config-ge1/0/1)#port hybrid vlan 100 tagged

SwitchA(config-ge1/0/1)#quit

SwitchA(config)#interface vlan 100

SwitchA(config-vlan-100)#ip address 10.100.10.2/24

//创建 VRRP 记录表项即备份组。

SwitchA(config-vlan-100)#ip vrrp 1

//配置接口虚拟 IP 地址。

SwitchA(config-vlan-100)#ip vrrp 1 associate-address 10.100.10.1

SwitchA(config-vlan-100)#quit

SwitchA(config)#

//配置 BFD 会话。

SwitchA(config)#bfd start

SwitchA(config)#bfd track 1 vlan 100 remote-ip 10.100.10.3 local-ip 10.100.10.2

SwitchA(config)#interface vlan 100

SwitchA(config-vlan-100)#bfd enable

2、配置 SwitchB。

//配置接口实际的 IP 地址。

SwitchB#configure

SwitchB(config)#interface gigaethernet 1/0/1

SwitchB(config-ge1/0/1)#port hybrid vlan 100 tagged

SwitchB(config-ge1/0/1)#quit

SwitchB(config)#interface vlan 100

SwitchB(config-vlan-100)#ip address 10.100.10.3/24

//创建 VRRP 记录表项即备份组。

SwitchB(config-vlan-100)#ip vrrp 1

//配置接口虚拟 IP 地址。

SwitchB(config-vlan-100)#ip vrrp 1 associate-address 10.100.10.1

//配置选举优先级低于 SwitchA。

SwitchB(config-vlan-100)#ip vrrp 1 priority 25

SwitchB(config-vlan-100)#quit

SwitchB(config)#

//配置 BFD 会话。

SwitchB(config)#bfd start

SwitchB(config)#bfd track 1 vlan 100 remote-ip 10.100.10.2 local-ip 10.100.10.3

SwitchB(config)#interface vlan 100

SwitchB(config-vlan-100)#bfd enable

//配置 VRRP 监视 BFD 会话。

SwitchB(config-vlan-100)#ip vrrp 1 track bfd-session 1

8.4 MLINK 配置

8.4.1 MLink 介绍

MLink（Monitor Link）是用于监控上行链路的功能模块，通过对上行链路的监控，以达到同步上行链路和下行链路状态的目的。

用于实现上行链路监控的 MLink 联动功能，也是以 MLink 组为单位。一个 MLink 组由多个上联（Uplink）端口和多个下联（Downlink）端口组成。所有下行链路监控上行链路状态，一旦所有的上行链路出现故障，那么认为 MLink 组的状态为 DOWN，所有的下行链路都会被强制关闭。当只要有一条上行链路恢复时，认为 MLink 组的状态为 UP，所有下行链路将被重新打开，下行链路的变化不影响上行链路的状态。

值得注意的是一个接口可以同时是多个 MLink 组的 Uplink 端口，但是只能成为一个组的 Downlink 端口。一个接口也不能同时为 Uplink 和 Downlink 端口。

8.4.2 配置 MLink 保护组

目的

本节介绍如何配置 MLink。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置 MLink 保护组，并进入 MLINK 配置视图	1. 进入全局配置视图； 2. 执行命令 **mlink group** *mlink-group-number* 配置 MLink 保护组，并进入 MLINK 配置视图。
配置 MLink 保护组的端口角色	1. 进入全局配置视图； 2. 执行命令 **mlink group** *mlink-group-number* 进入 MLINK 配置视图； 3. 执行命令 **add interface** { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* **role** { **uplink** | **downlink** }配置 MLink 保护组的端口角色，添加上行或者下行链路。
配置 MLink 保护组的 hold-off 计时器	1. 进入全局配置视图； 2. 执行命令 **mlink group** *mlink-group-number* 进入 MLINK 配置视图； 3. 执行命令 **hold-off time** *time-range-value* 配置 MLink 保护组的 hold-off 计时器。计时器超时之后，链路才能恢复。

目的	步骤
将接口加入 MLink 保护组，并配置端口角色	1. 进入以太网桥接接口配置视图或 Trunk 接口配置视图； 2. 执行命令 **join mlink group** *mlink-group-number* **role** { **uplink** | **downlink** }。

8.4.3 维护及调试

目的

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

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
显示 MLink 保护组的配置信息	1. 进入普通用户视图、全局配置视图、以太网接口配置视图、Trunk 接口配置视图、VLANIF 配置视图或特权用户视图； 2 执行命令 **show mlink config**。
显示 MLink 保护组的相关信息	1. 进入普通用户视图、全局配置视图、以太网接口配置视图、Trunk 接口配置视图、VLANIF 配置视图或特权用户视图； 2. 执行命令 **show mlink group**。
显示 MLink 接口信息	1. 进入普通用户视图、全局配置视图、以太网接口配置视图、Trunk 接口配置视图、VLANIF 配置视图或特权用户视图； 2. 执行命令 **show mlink interface**。

8.4.4 配置举例

组网需求

在 switch 设备上配置 MLink，其中接口 1/1 为 uplink1 端口，接口 1/2 为 uplink2 端口，接口 1/3 为 downlink1 端口，接口 1/4 为 downlink2 端口。

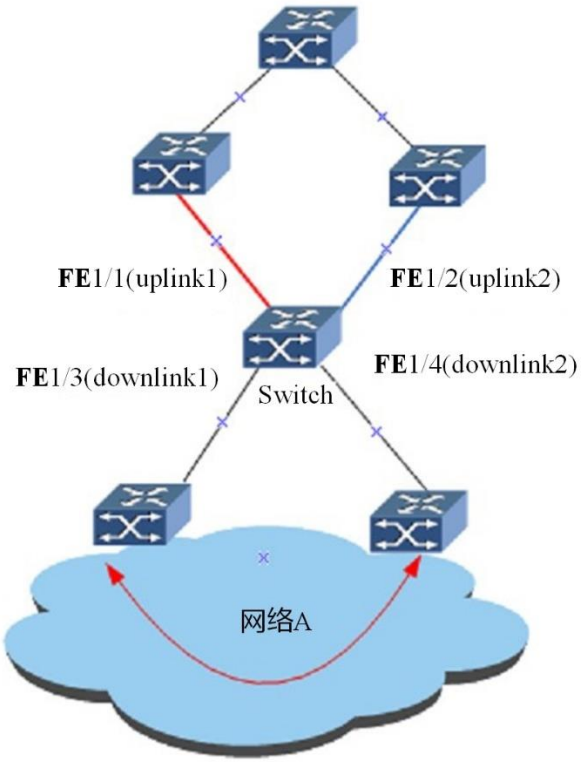


图 8-9 MLink 组网图

配置思路

MLink 的配置思路如下：

(1) 配置 MLink 保护组；

(2) 将接口配置成相应的角色加入保护组。

配置步骤

1、创建 MLink 组。

CN12800#configure

CN12800(config)#mlink group 1

CN12800(config-mlink1)#quit

CN12800(config)#

2、将接口 1/1 加入 MLink 组 1 并指定为 uplink1 端口。

CN12800(config)#interface fastethernet 1/1

CN12800(config-fe1/1)#join mlink group 1 uplink

CN12800(config-fe1/1)#mlink enable

CN12800(config-fe1/1)#quit

CN12800(config)#

3、将接口 1/2 加入 MLink 组 1 并指定为 uplink2 端口。

CN12800(config)#interface fastethernet 1/2

CN12800(config-fe1/2)#join mlink group 1 uplink

CN12800(config-fe1/2)#mlink enable

CN12800(config-fe1/2)#quit

CN12800(config)#

4、将接口 1/3 加入 MLink 组 1 并指定为 downlink1 端口。

CN12800(config)#interface fastethernet 1/3

CN12800(config-fe1/3)#join mlink group 1 downlink

CN12800(config-fe1/3)#mlink enable

CN12800(config-fe1/3)#quit

CN12800(config)#

5、将接口 1/4 加入 MLink 组 1 并指定为 downlink2 端口。

CN12800(config)#interface fastethernet 1/4

CN12800(config-fe1/4)#join mlink group 1 downlink

CN12800(config-fe1/4)#mlink enable

CN12800(config-fe1/4)#quit

CN12800(config)#

6、配置结束，查看 MLink 组配置信息。

CN12800#show mlink group

第9章 设备管理配置

本章介绍了 CN12800 系列数据中心交换机设备管理的基本内容、配置过程和配置举例。

9.1 设备硬件配置

9.1.1 硬件配置概述

CN12800 系列数据中心交换机设备的硬件配置是指硬件安装完毕后，在设备运行过程中，用户可以通过命令来对硬件资源，包括：CPU、风扇、内存、温度等硬件资源进行操作。

硬件配置便于硬件资源的利用以及提高硬件资源的可靠性。

9.1.2 配置设备 CPU

目的

用户可以通过本节操作了解 CPU 运行情况或控制 CPU 使用情况。包括：设置 CPU 监控及告警上报功能、设置 CPU 使用率的上下限阈值。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
设置 CPU 监控功能及 CPU 告警上报功能	1. 进入全局配置视图； 2. 执行命令 **cpu monitor** { **enable** | **disable** }使能或去使能 CPU 监控功能； 3. 执行命令 **cpu** { *slot-id / cpu-number* | **all** } **trap** { **enable** | **disable** }使能或去使能 CPU 上报告警功能。
设置 CPU 使用率的上限阈值和下限阈值	1. 进入全局配置视图； 2. 执行命令 **cpu** { *cpu-number* | **all** } **low-threshold** *low-threshold* **high-threshold** *high-threshold* 设置 CPU 使用率的上下限阈值。
清除设备 CPU 使用率的历史最大值	1. 进入全局配置视图； 2. 执行命令 **cpu** { *slot-id / cpu-number* | **all** } **maxusage reset** 清除设备 CPU 使用率的历史最大值。
清除设备 CPU 过载状态的历史信息	1. 进入全局配置视图； 2. 执行命令 **reset cpu** { *slot-id / cpu-number* | **all** } **monitor history** 清除设备 CPU 过载状态的历史信息。

目的	步骤
查看设备 CPU 过载状态的历史信息	1. 进入全局配置视图； 2. 执行命令 **show cpu** { *slot-id / cpu-number* | **all** } **monitor history** 查看设备 CPU 过载状态的历史信息。
查看配置结果	1. 进入普通用户视图、特权用户视图、全局配置视图； 2. 执行命令 **show cpu** 查看 CPU 使用情况和配置信息； 3. 执行命令 **show cpu config** 查看设备 CPU 当前的配置文件信息； 4. 执行命令 **show cpu statistic** 查看 CPU 占用率的统计信息。

9.1.3 配置设备风扇

目的

用户可以通过本节操作设置风扇转速阈值，并通过风扇监控及上报告警功能及时了解设备风扇当前的运转情况。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

9.1.4 配置设备内存

目的

用户可以通过本节操作设置内存使用率的上下限阈值，并通过内存监控及上报告警功能及时了解设备内存当前的使用情况。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

9.1.5 配置设备温度

目的

用户可以通过本节操作控制设备温度变化时是否上报告警以及设备温度达到多少时才上报告警。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

9.1.6 查看设备 CPU 占用率

目的

用户可以使用该命令查看设备 CPU 占用率。

过程

执行步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

9.1.7 维护及调试

目的

用户可以通过本节操作对设备硬件参数进行调试，用于定位问题。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

9.2 镜像配置

9.2.1 镜像概述

镜像是指将数据流复制到镜像目的端口。镜像技术主要用来实现数据流的监控功能，以便排除网络故障。

CN12800 支持支持 Trunk 的镜像、支持镜像到 Trunk。

CN12800 的观察端口最多可以设置为 8 个。

CN12800 支持将多个端口的报文镜像到一个观察端口。

CN12800 整台设备最多可以同时运用 3 个观察口，若同一端口既用于镜像上行流量又用于镜像下行流量则视为使用了 2 个观察端口。

CN12800 支持同一端口入方向和不同方向的流镜像到 2 个不同的观察端口，不支持对镜像报文进行再次镜像。

9.2.2 镜像分类

CN12800 系列数据中心交换机支持端口镜像和流镜像。

其中，端口镜像又分为本地镜像和远程镜像：

- 本地端口镜像：又叫 Local Switched Port Analyzer（SPAN），指镜像源和目的端口在同一台交换机上。
- 远程端口镜像：又叫 Remote SPAN（RSPAN），指镜像源和目的端口在不同的交换机上。


说明

- 源交换机：被监控端口所在的交换机，将流量镜像到 REMOTE-VLAN 中，然后二层转发给中间交换机。
- 中间交换机：网络中处于源交换机和目的交换机之间的交换机，通过 REMOTE-VLAN 把流量传输给下一个中间交换机和目的交换机。如果源交换机与目的交换机直接相连，则不存在中间交换机。
- 目的交换机：远程镜像目的端口所在的交换机，将从 REMOTE-VLAN 接收到的镜像流量通过镜像目的端口转发给监控设备。

流镜像也分为两种，分别是流镜像到 CPU 和流镜像到端口：

- 流镜像到 CPU：是指把通过配置了流镜像接口上的符合匹配要求的报文复制一份发送到 CPU，以供分析诊断。
- 流镜像到端口：是指把通过配置了流镜像接口上的符合匹配要求的报文复制一份发送到目的端口，以供分析诊断。

说明：

同端口镜像一样，流镜像也分为本地流镜像和远程流镜像。

9.2.3 配置本地端口镜像

目的

当用户需要监控或分析流经设备上某端口的报文，且镜像源端口与镜像目的端口在同一台设备上时，可以配置本地端口镜像功能。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
配置本地端口镜像	1. 进入全局配置视图； 2. 执行如下命令创建本地镜像组及其观察端口： ● **mirror group** *groupnum* { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* ● **mirror group** *groupnum* **eth-trunk** *trunk-number*； 3. 进入接口配置视图、接口组配置视图； 4. 执行命令 **mirror** { **ingress** | **egress** | **both** } **group** *groupnum* 在镜像源端口设置该接口的镜像功能。
取消端口本地镜像功能并删除本地镜像组及其观察端口	1. 进入接口配置视图、接口组配置视图； 2. 执行命令 **no mirror** { **ingress** | **egress** | **both** } **group** *groupnum* 取消端口本地镜像功能； 3. 进入全局配置视图； 4. 执行命令 **no mirror group** [*groupnum*] 删除本地镜像组及其观察端口的配置。
查看配置结果	1. 进入普通用户视图、特权用户视图、全局配置视图、接口配置视图（以太网接口、eth-trunk 接口）、VLAN 配置视图、接口组配置视图； 2. 执行命令 **show mirror config** 查看镜像功能的配置文件信息； 3. 执行命令 **show mirror group** 查看镜像组信息； 4. 执行命令 **show mirror interface** 查看镜像端口信息。

9.2.4 配置流镜像

目的

当用户需要监控或分析流经设备的且具有某些特性的报文，可以配置流镜像功能。

说明：

配置远程流镜像之前，需保证设备之间二层网络连通或三层网络可达。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
配置本地流镜像	1. 进入全局配置视图； 2. 执行如下命令创建本地镜像组及其观察端口： ● **mirror group** *groupnum* { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* ● **mirror group** *groupnum* **eth-trunk** *trunk-number*； 3. 执行命令 **filter-list** *acl-number* [**name** *filter-name*]创建一条 ACL（访问控制列表），并进入 ACL 视图； 4. 请根据实际应用情形，参考第 7.1 章 ACL 配置，选择合适的流分类规则； 5. 执行如下命令配置流镜像处理动作 **filter** *rule-number* **action mirror group** *group-number*； 6. 执行命令 **quit** 或 **exit** 退出 ACL 视图到全局配置视图； 7. 进入接口配置视图、接口组配置视图、VLAN 配置视图； 8. 执行命令 **filter-list-{ l2 | ipv4 | ipv6 | hybrid } { in | out }** *acl-name* 将 ACL 应用到该物理端口或 trunk 接口； 9. 执行命令 **mirror** { **ingress** | **egress** | **both** } **group** *group-list* 在镜像源端口设置该接口的镜像功能。
取消流镜像功能并删除本地镜像组及其观察端口	1. 进入接口配置视图、接口组配置视图； 2. 执行命令 **no filter-list-{ l2 | ipv4 | ipv6 | hybrid } { in | out }**，然后执行命令 **no mirror** { **ingress** | **egress** | **both** } *group-list* 取消端口本地镜像功能； 3. 进入全局配置视图； 4. 执行命令 **no mirror group** [*groupnum*]删除本地镜像组及其观察端口的配置。

目的	步骤
查看配置结果	1. 进入普通用户视图、特权用户视图、全局配置视图、接口配置视图（以太网接口、trunk 接口）、VLAN 配置视图、接口组配置视图； 2. 执行命令 **show mirror config** 查看镜像功能的配置文件信息； 3. 执行命令 **show mirror group** 查看镜像组信息； 4. 执行命令 **show mirror interface** 查看镜像端口信息； 5. 执行命令 **show filter-list config** 查看镜像规则。

9.2.5 配置举例

9.2.5.1 配置本地端口镜像举例

组网要求

某集团公司部门 1 和部门 2 分别通过接口 10GE1/0/1、10GE1/0/2 连接到交换机 CN12800。数据监控设备通过接口 10GE1/0/3 连接到交换机 CN12800。要求使用本地端口镜像功能来实现数据监控设备对部门 1 和部门 2 发送到交换机 CN12800 上的报文的监控，如图 9-1 所示。

组网图

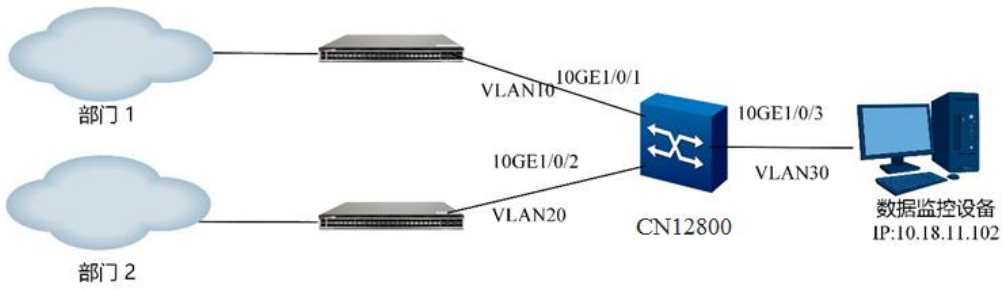


图 9-1 本地端口镜像配置组网图

配置步骤

1、配置各接口，使两个部门都能与数据监控设备互通。

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

CN12800#configure

CN12800(config)#vlan 10

CN12800(config-vlan-10)#quit

CN12800(config)#vlan 20

CN12800(config-vlan-20)#quit

CN12800(config)#vlan 30

CN12800(config-vlan-30)#quit

CN12800(config)#interface 10gigaethernet 1/0/1

CN12800(config-10ge1/0/1)#port link-type trunk

CN12800(config-10ge1/0/1)#port trunk pvid 10

CN12800(config-10ge1/0/1)#port trunk allow-pass vlan 10

CN12800(config-10ge1/0/1)#quit

CN12800(config)#interface 10gigaethernet 1/0/2

CN12800(config-10ge1/0/2)# port link-type trunk

CN12800(config-10ge1/0/2)#port trunk pvid 20

CN12800(config-10ge1/0/2)#port trunk allow-pass vlan 20

CN12800(config-10ge1/0/2)#quit

CN12800(config)#interface 10gigaethernet 1/0/3

CN12800(config-10ge1/0/3)# port link-type trunk

CN12800(config-10ge1/0/3)#port trunk allow-pass vlan 10,20,30

CN12800(config-10ge1/0/3)#quit

CN12800(config)#interface vlan 30

CN12800(config-vlan-3)#ip address 10.18.11.1/24

CN12800(config-vlan-3)#quit

CN12800(config)#

2、创建本地镜像组及其观察端口。

#在 CN12800 上创建本地镜像组 1 及配置其观察端口为 10GE1/0/3。

CN12800(config)#mirror group 1 10gigaethernet 1/0/3

3、在镜像源端口设置该端口的镜像功能。

#在 CN12800 上配置端口 10GE1/0/1 和 10GE1/0/2 为镜像源端口，以监控部门 1 和部门 2 发送的数据报文。

CN12800(config)#interface 10gigaethernet 1/0/1

CN12800(config-10ge1/0/1)#mirror ingress group 1

CN12800(config-10ge1/0/1)#quit

CN12800(config)#interface 10gigaethernet 1/0/2

CN12800(config-10ge1/0/2)#mirror ingress group 1

CN12800(config-10ge1/0/2)#quit

CN12800(config)#

4、配置结束。

9.2.5.2 配置本地流镜像举例

组网要求

某集团公司部门 1 和部门 2 分别通过接口 10GE1/0/1、10GE1/0/2 连接到交换机 CN12800。数据监控设备通过接口 10GE1/0/3 连接到交换机 CN12800。要求使用本地流镜像功能来实现数据监控设备对部门 1 和部门 2 发送到交换机 CN12800 上的源 MAC 地址为任意，目的 MAC 地址为 00:00:00:01:02:03 报文的监控，如图 9-2 所示。

组网图

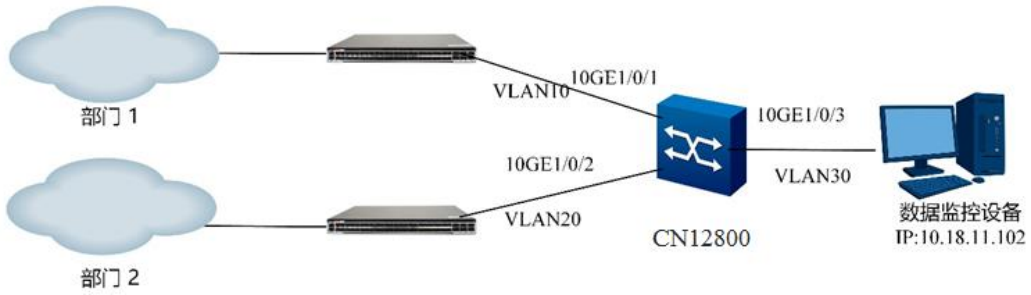


图 9-2 本地流镜像配置组网图

配置步骤

1、配置各接口，使各两个部门都能与数据监控设备互通。

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

CN12800#configure

CN12800(config)#vlan 10

CN12800(config-vlan-10)#quit

CN12800(config)#vlan 20

CN12800(config-vlan-20)#quit

CN12800(config)#vlan 30

CN12800(config-vlan-30)#quit

CN12800(config)#interface 10gigaethernet 1/0/1

CN12800(config-10ge1/0/1)#port link-type trunk

CN12800(config-10ge1/0/1)#port trunk pvid 10

CN12800(config-10ge1/0/1)#port trunk allow-pass vlan 10

CN12800(config-10ge1/0/1)#quit

CN12800(config)#interface 10gigaethernet 1/0/2

CN12800(config-10ge1/0/2)#port link-type trunk

CN12800(config-10ge1/0/2)#port trunk pvid 20

CN12800(config-10ge1/0/2)#port trunk allow-pass vlan 20

CN12800(config-10ge1/0/2)#quit

CN12800(config)#interface 10gigaethernet 1/0/3

CN12800(config-10ge1/0/3)#port link-type trunk

CN12800(config-10ge1/0/3)#port trunk allow-pass vlan 10,20,30

CN12800(config-10ge1/0/3)#quit

CN12800(config)#interface vlan 30

CN12800(config-vlan-3)#ip address 10.18.11.1/24

CN12800(config-vlan-3)#quit

CN12800(config)#

2、创建本地镜像组及其观察端口。

#在 CN12800 上创建本地镜像组 1 及配置其观察端口为 10GE1/0/3。

CN12800(config)#mirror group 1 10gigaethernet 1/0/3

3、配置流分类规则及流镜像处理动作，并将策略应用到镜像源端口。

#在 CN12800 上创建 ACL100，配置其匹配规则及处理动作，并应用到镜像源端口。

CN12800(config)#filter-list 100

CN12800(configure-filter-l2-100)#filter 1 mac any 00:00:00:01:02:03/48

CN12800(configure-filter-l2-100)#filter 1 action mirror group 1

CN12800(configure-filter-l2-100)#quit

CN12800(config)#interface 10gigaethernet 1/0/1

CN12800(config-10ge1/0/1)#filter-list-l2 in 100

CN12800(config-ge1/0/1)#quit

CN12800(config)#interface 10gigaethernet 1/0/2

CN12800(config-10ge1/0/2)#filter-list-l2 in 100

CN12800(config-10ge1/0/2)#quit

CN12800(config)#

4、配置结束。

9.3 日志管理配置

9.3.1 日志管理简介

为了跟踪系统的运行状况及当前系统的状态可以打开系统日志记录功能，使之自动记录系统的状态，从而可以掌握系统的运行状况进行相应的操作。该日志文件可以连续记录 4000 条记录，当记录超出 4000 条时，自动删除日期最久的记录。所以为了使系统不丢失记录，建议用户定期把日志文件导出。

9.3.2 配置日志管理

9.3.2.1 启动或取消日志记录功能

目的

本操作用于启动或取消交换机日志记录功能。

过程

根据不同目的，执行相应步骤，具体参见下表。

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

9.3.2.2 显示或清除日志信息

目的

本操作用于显示或清除日志的信息。

过程

根据不同目的，执行相应步骤，具体参见下表。

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

目的	步骤
	2. 执行命令 **clear logging source** { **aaa** | **acl** | **arp** | **arp-probe** | **arp-antiattack** | **bfd** | **bgp** | **cli** | **counter** | **cpu** | **cpu-defend** | **dcp** | **ddm** | **default** | **devcomm** | **device** | **dhcp** | **dhcp-client** | **dhcpv6** | **dhcp-snooping** | **did** | **diffserv** | **dos-antiattack** | **dxs** | **evpn** | **fan** | **ha** | **hwarp** | **hwroute** | **hwvp** | **hwvrf** | **hwbd** | **ipsg** | **icmp** | **icmp6** | **ifm** | **if-ref** | **igmp-snooping** | **ip** | **ipv6** | **isis** | **l3vpn** | **lacp** | **link-flap** | **lldp** | **llt** | **mam** | **memory** | **mirror** | **mlag** | **mld-snooping** | **mlink** | **ndp** | **ntp** | **ospf** | **ospf6** | **patch** | **port-isolate** | **power** | **policy-route** | **rawip** | **rawip6** | **route** | **route-policy** | **scheduleprofile** | **slot** | **snmp** | **ssh** | **stg** | **storm-control** | **stp** | **tcp** | **tcp6** | **temperature** | **time-range** | **udp** | **udp6** | **udr** | **uinetsck** | **vlan-mapping** | **vlan-stacking** | **voltage** | **vrrp** | **vxlan** }

9.3.2.3 配置 action 相关信息

目的

本操作用于配置 action 相关信息。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

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

9.3.2.4 配置 syslog 服务器

背景信息

Syslog 服务器接收来自客户端的日志信息，以此达到日志的统一管理与查看，便于对设备信息的监控。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
配置 syslog 服务器	1. 进入全局配置视图； 2. 执行命令 **syslog server** *ipv4-address* [*server-port*]。
删除 syslog 服务器	1. 进入全局配置视图； 2. 执行命令 **no syslog server** *ipv4-address*。

9.3.2.5 配置日志文件

目的

本操作用于配置日志文件的大小和数量。

过程

根据不同目的，执行相应步骤，具体参见下表。

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

目的	步骤
	snooping | **ip** | **ipv6** | **isis** | **l3vpn** | **lacp** | **link-flap** | **lldp** | **llt** | **mam** | **memory** | **mirror** | **mlag** | **mld-snooping** | **mlink** | **ndp** | **ntp** | **ospf** | **ospf6** | **patch** | **port-isolate** | **power** | **policy-route** | **rawip** | **rawip6** | **route** | **route-policy** | **scheduleprofile** | **slot** | **snmp** | **ssh** | **stg** | **storm-control** | **stp** | **tcp** | **tcp6** | **temperature** | **time-range** | **udp** | **udp6** | **udr** | **uinetsck** | **vlan-mapping** | **vlan-stacking** | **voltage** | **vrrp** | **vxlan** } **max-number** { *file_num* | **default** }

9.3.2.6 保存日志文件

目的

本操作用于配置日志文件的保存等。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

9.3.2.7 配置统一驱动平台日志功能

目的

本操作用于配置 UDR（统一驱动平台）日志功能。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
使能或去使能统一驱动平台的日志功能	1. 进入全局配置视图； 2. 执行命令 **log udr** { **error** | **poe** | **intr** | **acl** | **l3** | **mac** | **mc** | **mirror** | **misc** | **mpls** | **packet** | **port** | **route** | **system** | **trunk** | **vlan** | **card** | **oam** | **cos** | **vxlan** | **bfd** | **dpa** | **all** } { **enable** | **disable** }。
查看 UDR 日志配置信息	1. 进入普通用户视图； 2. 执行命令 **show log udr config**。
查看 UDR 日志使能状态	1. 进入普通用户视图； 2. 执行命令 **show log udr status** [**slot** *slot-id*]。

9.3.2.8 查看日志配置信息

目的

当用户配置完成日志管理功能及其相关参数后，若需要查看配置是否正确，可使用本节介绍的操作查看相关信息。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

9.4 DDM 配置

9.4.1 DDM 概述

在光链路中，定位故障的发生位置对业务的快速恢复至关重要。利用智能化的光模块 DDM（Digital Diagnostic Monitoring，数字诊断监控），网络管理单元可以实时监测收发模块的温度、供电电压、激光偏置电流以及发射和接收光功率。这些参量的测量，可以帮助管理单元找出光纤链路中发生故障的位置，简化维护工作，提高系统的可靠性。

总之，通过数字诊断功能，可以定位故障。在故障定位中，需要对 Tx_power，Rx_power，Temp，Vcc，Tx_Bias 的警告和告警状态进行综合分析。

9.4.2 配置 DDM 基本功能

目的

使用本节操作配置端口实时监测光模块温度、供电电压、激光偏置电流以及发射和接收光功率，以便快速定位光纤链路故障。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

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

9.4.3 维护及调试

目的

当 DDM 功能不正常，需要进行查看、定位问题时，可以使用本小节操作。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
查看所有视图下配置的 DDM 信息，包括电流、电压等的高低门限值	1. 进入普通用户视图； 2. 执行命令 **show ddm config**。
查看所有插入了光模块的端口的模块常规硬件信息	1. 进入普通用户视图； 2. 执行命令 **show laser hardware**。
查看所有插入了光模块的端口的模块详细硬件信息	1. 进入普通用户视图； 2. 执行命令 **show laser hardware detailed**。
查看某个具体光模块端口的模块常规硬件信息	1. 进入普通用户视图； 2. 执行命令 **show laser hardware** { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number*。
查看某个具体光模块的端口的模块详细硬件信息	1. 进入普通用户视图； 2. 执行命令 **show laser hardware** { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* **detailed**。
打开或关闭 DDM 调试功能	1. 进入特权用户视图； 2. 执行命令 **debug ddm** { **poll** | **event** | **all** }或 **no debug ddm** { **poll** | **event** | **all** }。

9.5 HA 配置

9.5.1 HA 介绍

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

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

9.5.2 配置主备倒换

目的

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

过程

根据不同目的，执行相应步骤，具体参见下表。

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

9.5.3 维护及调试

目的

当 HA 功能不正常，需要进行查看、调试或定位问题时，可以使用本小节操作。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
显示 HA 的运行状态	1. 进入普通用户视图； 2. 执行命令 **show ha global**，查看 HA 的运行状态。
显示 MAC 管理模块、路由协议模块的运行状态	1. 进入普通用户视图； 2. 执行命令 **show ha status**，查看 MAC 管理模块、路由模块的稳定状态。
将协议栈 ND 表项信息写入文件	1. 执行命令 **disable** 退出到普通用户视图； 2. 执行命令 **dump ha nd-table** 将协议栈 ND 表项信息写入文件。
将所有 IPv4/IPv6 路由表项信息写入文件	1. 执行命令 **disable** 退出到普通用户视图； 2. 执行命令 **dump ha** { **route-table** | **route6-table** }将所有 IPv4/IPv6 路由表项信息写入文件。

9.5.4 配置举例

配置思路

配置主备倒换的配置思路如下：

(1) 查看设备的运行状态；

(2) 配置主备倒换。

数据准备

要完成该配置举例，设备必须处于稳定运行状态。

配置步骤

(1) 显示 HA 的运行状态。

CN12800>show ha global

CN12800>

(2) 查看其他协议的运行状态。

CN12800>show ha status

CN12800>

(3)配置主备倒换。

CN12800#rsp switch

CN12800#

9.6 系统及指定线卡补丁配置

9.6.1 系统及指定线卡补丁概述

本设备支持系统补丁和给指定槽位的线卡打补丁。

补丁是一种与系统软件兼容的软件，用于解决系统软件的 Bug。本设备支持 3 种补丁状态：LOAD、ACTIVE、DEACTIVE。

9.6.2 加载单板补丁

背景信息

在加载补丁之前系统要对补丁包进行解析，检查补丁包中补丁文件的合法性，并获取补丁文件的属性（包括补丁类型、单板类型、版本信息）。

为单板加载补丁时，系统会根据补丁文件的属性在补丁包中查找匹配的补丁文件，查找成功，则进行加载操作。如果补丁包中没有适合某类型单板的补丁，则不加载。

补丁文件必须在主控板根目录下。

当备用主控板正在注册中且尚未注册成功时，如果进行补丁加载操作，则系统会提示：是否确认继续执行补丁操作。

目的

用户可以通过本节操作进行补丁加载配置。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

9.6.3 配置激活补丁

准备

激活补丁之前，必须先进行加载单板补丁操作，参见 9.6.2 小节。

背景信息

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

去激活补丁时，补丁必须存在且已被激活后，去激活补丁才有效。

目的

用户可以通过本节操作进行补丁激活。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
激活补丁，可以根据需要配置补	1. 进入全局配置视图；

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

9.6.4 配置去激活补丁

准备

去激活补丁之前，必须激活补丁操作，参见 9.6.3 小节。

目的

用户可以通过本节操作去激活正在运行的补丁。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

9.6.5 删除补丁

目的

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

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
直接删除补丁文件	1. 进入全局配置视图； 2. 执行命令 **patch** *patch-number* **delete** [**slot** *slot-id*]在主用/备用主控上删除补丁文件。

目的	步骤
查看配置结果	1. 进入特权用户视图； 2. 执行命令 **show patch information** 查看系统当前所有补丁信息。

9.6.6 查看补丁信息

目的

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

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

9.7 STG 配置

9.7.1 STG 概述

STG 是交换芯片 STP Group 的简称，是所有接口 VLAN 的转发控制集合。STG 协议模块是交换芯片接口 API。

9.7.2 维护及调试

目的

当 STG 不正常，需要进行查看、调试或定位问题时，可以使用本小节操作。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
打开或关闭 STG 调试功能	1. 不执行任何命令保持当前特权用户视图；

目的	步骤
	2. 执行命令 **debug stg { error | event | notification | sync | all }**或 **no debug stg { error | event | notification | sync | all }**打开或关闭 STG 调试功能。
清除所有 STG 错误统计	1. 不执行任何命令保持当前特权用户视图； 2. 执行命令 **reset stg error** 清除所有 STG 错误统计。
查看 STG 功能信息	1. 执行命令 **disable** 退出到普通用户视图； 2. 执行命令 **show stg { all | brief | error | memory }**查看 STG 功能信息。
查看 STG 的实例信息	1. 执行命令 **disable** 退出到普通用户视图； 2. 执行命令 **show stg instance** { *instance-id* | **all** }查看 STG 的实例信息。
查看 STG 的接口信息	1. 执行命令 **disable** 退出到普通用户视图； 2. 执行命令 **show stg interface { ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* 或 **show stg interface all** 查看 STG 的接口信息。
查看 STG 的协议信息	1. 执行命令 **disable** 退出到普通用户视图； 2. 执行命令 **show stg protocol { all | stp | g8032 | lacp | mlink | rlink }**查看 STG 的协议信息。
查看指定槽位上某个生成树组绑定的 VLAN List 信息	1. 执行命令 **disable** 退出到普通用户视图； 2. 执行命令 **show hwstg slot** *slot-id* **stg** *stg-id* 查看指定槽位上某个生成树组绑定的 VLAN List 信息。
查看指定端口的生成树组状态	1. 执行命令 **disable** 退出到普通用户视图； 2. 执行命令 **show hwstg slot** *slot-id* **stg** *stg-id* **interface { ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number* 查看指定端口的生成树组状态。

第10章 运维管理配置

本章介绍了 CN12800 系列数据中心交换机运维管理的基本内容、配置过程和配置举例。

10.1 NTP 配置

10.1.1 NTP 概述

Network Time Protocol（NTP）为交换机提供网络时钟同步功能，该功能包括 NTP 服务器和 NTP 客户端。通过配置 NTP，可以保持网络中设备的时钟运行一致。

NTP 协议支持的四种运行模式

- 单播模式

  在该模式下，进行如下的处理：unicast 的 client 周期性的发送 NTP 请求报文到 server，并且期望从 server 得到请求答复报文；client 在收到 server 服务器回应报文后，根据 server 和 client 的往返传播延迟计算本地时钟补偿；client 根据 server 的时间以及往返传播延迟计算的本地时钟补偿的关系进行时间计算并设置为本地时间。server 等待 client 端周期性发送的请求，根据接收到请求消息的地址构造请求消息应答报文并发送，server 不会自动的周期性的发送通告报文。

- 对等体模式

  对等体模式下，主动对等体和被动对等体可以互相同步，等级低（层数大）的对等体向等级高（层数小）的对等体同步。主动对等体向被动对等体发送同步请求报文，报文中的 Mode 字段设置为 1（主动对等体）。被动对等体收到请求报文后，自动工作在被动对等体模式，并发送应答报文，报文中的 Mode 字段设置为 2（被动对等体）。

- 组播模式

  客户端侦听来自服务器的组播消息包；当客户端接收到第一个组播消息包后，为估计网络延迟，客户端先启用一个短暂的服务器/客户端模式与远程服务器交换消息；客户端进入组播客户端模式，继续侦听组播消息包的到来，根据到来的组播消息包对本地时钟进行同步。对于 IPv4 的服务器端周期性向组播目的地址 224.0.1.1 发送时钟同步报文。

- 广播模式

客户端侦听来自服务器的广播消息包。客户端接收到第一个广播消息包后，为估计网络延迟，客户端先启用一个短暂的服务器/客户端模式与远程服务器交换消息。客户端进入广播客户模式，继续侦听广播消息包的到来，根据到来的广播消息包对本地时钟进行同步。对于 IPv4 的服务器端周期性向广播地址 255.255.255.255 或子网广播地址发送时钟同步报文。

NTP 的优点

- 支持采用单播、组播或广播方式发送协议报文。
- 支持 MD5 验证。
- 采用分层（Stratum）的方法来定义时钟的准确性，可以迅速同步网络中各台设备的时间。

10.1.2 配置 NTP 基本功能

目的

使用本节操作配置 NTP 基本功能，用户可以了解到如何配置 NTP 的工作模式。

前提配置

配置网络中设备链路层协议、网络层 IP 地址或路由协议，保证设备间 NTP 报文可达。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
指定设备为主时钟	1. 进入全局配置视图； 2. 进入 NTP 配置视图； 3. 执行命令 **master** 指定设备为主时钟。
配置 NTP 层级	1. 进入全局配置视图； 2. 进入 NTP 配置视图； 3. 执行命令 **stratum** { *layer-number* | **default** }指定 NTP 层级，服务器端（主时钟）配置的层数一定要小于客户端所在的层数，否则客户端无法同步服务器端的时钟。
配置 NTP 单播模式	配置 NTP 客户端（指定单播 NTP 服务器后，本地交换机自动工作在客户端模式。其中步骤 3 和步骤 4，用户根据实际情况选用）： 1. 进入全局配置视图； 2. 进入 NTP 配置视图； 3. 执行如下命令：

目的	步骤
	● **ntp unicast-server** *ipv4-address* ● **ntp unicast-server** *ipv4-address* **authentication-keyid** *key-id* ● **ntp unicast-server** *ipv4-address* **authentication-keyid** *key-id* **source-interface loopback** *loopback-id* ● **ntp unicast-server** *ipv4-address* **authentication-keyid** *key-id* **source-interface vlan** *vlan-id* ● **ntp unicast-server** *ipv4-address* **source-interface loopback** *loopback-id* ● **ntp unicast-server** *ipv4-address* **source-interface vlan** *vlan-id* ● **ntp unicast-server** *ipv4-address* **version** { **1** | **2** | **3** | **4** } ● **ntp unicast-server** *ipv4-address* **version** { **1** | **2** | **3** | **4** } **authentication-keyid** *key-id* [**source-ip** *src-ip*] ● **ntp unicast-server** *ipv4-address* **version** { **1** | **2** | **3** | **4** } **authentication-keyid** *key-id* **source-interface loopback** *loopback-id* ● **ntp unicast-server** *ipv4-address* **version** { **1** | **2** | **3** | **4** } **authentication-keyid** *key-id* **source-interface vlan** *vlan-id* ● **ntp unicast-server** *ipv4-address* **version { 1 | 2 | 3 | 4 }** **source-interface loopback** *loopback-id* ● **ntp unicast-server** *ipv4-address* **version { 1 | 2 | 3 | 4 } source-interface vlan** *vlan-id*。
	配置 NTP 服务器端： 服务器端除配置 NTP 主时钟外，不需要专门配置。
配置 NTP 广播模式（适用于局域网）	配置 NTP 广播客户端： 1. 进入全局配置视图； 2. 进入 VLANIF 配置视图； 3. 执行如下命令： ● **ntp broadcast-client** ● **ntp broadcast-client** *ipv4-address*。
	配置 NTP 广播服务器端： 1. 进入全局配置视图； 2. 进入 VLANIF 配置视图； 3. 执行如下命令： ● **ntp broadcast-server** ● **ntp broadcast-server** *ipv4-address* ● **ntp broadcast-server authentication-keyid** *key-id* ● **ntp broadcast-server authentication-keyid** *key-id ipv4-address* ● **ntp broadcast-server version { 1 | 2 | 3 | 4 }** ● **ntp broadcast-server version { 1 | 2 | 3 | 4 }** *ipv4-address* ● **ntp broadcast-server authentication-keyid** *key-id* version { **1** | **2** | **3** | **4** }

目的	步骤
	● **ntp broadcast-server authentication-keyid** *key-id* version { **1 | 2 | 3 | 4** } *ipv4-address*。
配置 NTP 组播模式	配置 NTP 组播客户端： 1. 进入全局配置视图； 2. 进入 VLANIF 配置视图； 3. 执行如下命令： ● **ntp multicast-client** ● **ntp multicast-client** *ipv4- address*
	配置 NTP 组播服务器端： 1. 进入全局配置视图； 2. 进入 VLANIF 配置视图； 3. 执行如下命令： ● **ntp multicast-server** ● **ntp multicast-server** *ipv4-address* ● **ntp multicast-server authentication-keyid** *key-id* ● **ntp multicast-server authentication-keyid** *key-id ipv4-address* ● **ntp multicast-server version { 1 | 2 | 3 | 4 }**； ● **ntp multicast-server version { 1 | 2 | 3 | 4 }** *ipv4-address* ● **ntp multicast-server ttl** *ttl-value* ● **ntp multicast-server ttl** *ttl-value ipv4-address* ● **ntp multicast-server version { 1 | 2 | 3 | 4 } ttl** *ttl-value* ● **ntp multicast-server version** { **1** | **2** | **3** | **4** } **ttl** *ttl-value ipv4-address* ● **ntp multicast-server authentication-keyid** *key-id* **version { 1 | 2 | 3 | 4 } ttl** *ttl-value* ● **ntp multicast-server authentication-keyid** *key-id* **version { 1 | 2 | 3 | 4 } ttl** *ttl-value ipv4-address*。
增加或者修改一条 IPv4 NTP 主动对等，也支持配置多实例 VPN	1. 进入全局配置视图； 2. 进入 NTP 配置视图； 3. 执行如下命令： ● **ntp unicast-peer** *ipv4-address* [**source-ip** *src-ip*] ● **ntp unicast-peer** *ipv4-address* **authentication-keyid** *key-id* [**source-ip** *src-ip*] ● **ntp unicast-peer** *ipv4-address* **authentication-keyid** *key-id* **source-interface loopback** *loopback-id* ● **ntp unicast-peer** *ipv4-address* **authentication-keyid** *key-id* **source-interface vlan** *vlan-id* ● **ntp unicast-peer** *ipv4-address* **source-interface loopback** *loopback-id* ● **ntp unicast-peer** *ipv4-address* **source-interface vlan** *vlan-id* ● **ntp unicast-peer** *ipv4-address* **version { 1 | 2 | 3 | 4 }**

目的	步骤
	● **ntp unicast-peer** *ipv4-address* **version { 1 | 2 | 3 | 4 } authentication-keyid** *key-id* [**source-ip** *src-ip*] ● **ntp unicast-peer** *ipv4-address* **version { 1 | 2 | 3 | 4 } authentication-keyid** *key-id* **source-interface loopback** *loopback-id* ● **ntp unicast-peer** *ipv4-address* **version { 1 | 2 | 3 | 4 } authentication-keyid** *key-id* **source-interface vlan** *vlan-id* ● **ntp unicast-peer** *ipv4-address* **version { 1 | 2 | 3 | 4 } source-interface loopback** *loopback-id* ● **ntp unicast-peer** *ipv4-address* **version { 1 | 2 | 3 | 4 } source-interface vlan** *vlan-id*。
增加或者修改一条 IPv6 NTP 主动对等，也支持配置多实例 VPN	1. 进入全局配置视图； 2. 进入 NTP 配置视图； 3. 执行如下命令： ● **ntp6 unicast-peer** *ipv6-address* [**source-ip6** *src-ip6*] ● **ntp6 unicast-peer** *ipv6-address* **authentication-keyid** *key-id* [**source-ip6** *src-ip6*] ● **ntp6 unicast-peer** *ipv6-address* **authentication-keyid** *key-id* **source-interface loopback** *loopback-id* ● **ntp6 unicast-peer** *ipv6-address* **authentication-keyid** *key-id* **source-interface vlan** *vlan-id* ● **ntp6 unicast-peer** *ipv6-address* **source-interface loopback** *loopback-id* ● **ntp6 unicast-peer** *ipv6-address* **source-interface vlan** *vlan-id* ● **ntp6 unicast-peer** *ipv6-address* **version { 1 | 2 | 3 | 4 }** ● **ntp6 unicast-peer** *ipv6-address* **version { 1 | 2 | 3 | 4 } authentication-keyid** *key-id* [**source-ip6** *src-ip6*] ● **ntp6 unicast-peer** *ipv6-address* **version { 1 | 2 | 3 | 4 } authentication-keyid** *key-id* **source-interface loopback** *loopback-id* ● **ntp6 unicast-peer** *ipv6-address* **version { 1 | 2 | 3 | 4 } authentication-keyid** *key-id* **source-interface vlan** *vlan-id* ● **ntp6 unicast-peer** *ipv6-address* **version { 1 | 2 | 3 | 4 } source-interface loopback** *loopback-id* ● **ntp6 unicast-peer** *ipv6-address* **version { 1 | 2 | 3 | 4 } source-interface vlan** *vlan-id*。
配置 NTP 客户端更新间隔	1. 进入全局配置视图； 2. 进入 NTP 配置视图； 3. 执行命令 **client update-interval** { *update-interval-time* | **default** }。
配置 NTP 服务器端的广播间隔	1. 进入全局配置视图； 2. 进入 NTP 配置视图； 3. 执行命令 **server broadcast-interval** { *interval* | **default** }。

10.1.3 配置 NTP 安全机制

目的

使用本节操作配置 NTP 安全机制，在对安全性要求比较高的网络中，可以实现可靠的时钟同步。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
全局使能或去使能 MD5 认证功能	1. 进入全局配置视图； 2. 进入 NTP 配置视图； 3. 执行命令 **authentication { enable | disable }**。
配置一条 NTP 验证密钥	1. 进入全局配置视图； 2. 进入 NTP 配置视图； 3. 执行如下命令： **authentication-keyid** *key-id* **md5 key** *key-string* **authentication-keyid** *key-id* **md5 key** { **cipher** | **plain** } *key-string*。
使能或者禁止信任一条 MD5 认证密钥	1. 进入全局配置视图； 2. 进入 NTP 配置视图； 3. 执行命令 **trusted-keyid** *trusted-keyid* { **enable** | **disable** }。
开启或关闭同步报文交互过程中的并发机制	1. 进入全局配置视图； 2. 进入 NTP 配置视图； 3. 执行命令 **oncesync { enable | disable }**。
配置 NTP 单播模式的验证	配置 NTP 客户端（指定单播 NTP 服务器后，本地交换机自动工作在客户端模式。其中步骤 3 和步骤 4，用户根据实际情况选用）： 1. 进入全局配置视图； 2. 进入 NTP 配置视图； 3. 执行如下命令： ● **ntp unicast-server** *ipv4-address* **version** { **1 | 2 | 3 | 4** } **authentication-keyid** *key-id* [**source-ip** *src-ip*] ● **ntp unicast-server** *ipv4-address* **authentication-keyid** *key-id* ● **ntp unicast-server** *ipv4-address* **version { 1 | 2 | 3 | 4 } authentication-keyid** *key-id* **vpn-instance** *vpn-instance-name* ● **ntp unicast-server** *ipv4-address* **authentication-keyid** *key-id* **vpn-instance** *vpn-instance-name*。

目的	步骤
	配置 NTP 服务器端： 服务器端除配置 NTP 主时钟外，不需要专门配置。
配置 NTP 广播模式的验证（适用于局域网）	配置 NTP 广播客户端： 1. 进入全局配置视图； 2. 进入 VLANIF 配置视图； 3. 执行如下命令： ● **ntp broadcast-client** ● **ntp broadcast-client** *ipv4-address*。
	配置 NTP 广播服务器端： 1. 进入全局配置视图； 2. 进入 VLANIF 配置视图； 3. 执行如下命令： ● **ntp broadcast-server authentication-keyid** *key-id* ● **ntp broadcast-server authentication-keyid** *key-id ipv4-address* ● **ntp broadcast-server authentication-keyid** *key-id* **version { 1 | 2 | 3 | 4** } ● **ntp broadcast-server authentication-keyid** *key-id* **version { 1 | 2 | 3 | 4** } *ipv4-address*。
配置 NTP 组播模式的验证	配置 NTP 组播客户端： 1. 进入全局配置视图； 2. 进入 VLANIF 配置视图； 3. 执行如下命令： ● **ntp multicast-client** *key-id* ● **ntp multicast-client** *key-id ipv4-address*。
	配置 NTP 组播服务器端： 1. 进入全局配置视图； 2. 进入 VLANIF 配置视图； 3. 执行如下命令： ● **ntp multicast-server authentication-keyid** *key-id* ● **ntp multicast-server authentication-keyid** *key-id ipv4-address* ● **ntp multicast-server authentication-keyid** *key-id* **version { 1 | 2 | 3 | 4 } ttl** *ttl-value* ● **ntp multicast-server authentication-keyid** *key-id* **version { 1 | 2 | 3 | 4 } ttl** *ttl-value ipv4-address*。
配置 NTP 对等体模式的验证	1. 进入全局配置视图； 2. 进入 NTP 配置视图； 3. 执行如下命令： ● **ntp unicast-peer** *ipv4-address* **version { 1 | 2 | 3 | 4 } authentication-keyid** *key-id* [**source-ip** *src-ip*] ● **ntp unicast-peer** *ipv4-address* **authentication-keyid** *key-id* [**source-ip** *src-ip*]

目的	步骤
	● **ntp unicast-peer** *ipv4-address* **version { 1 | 2 | 3 | 4 } authentication-keyid** *key-id* **vpn-instance** *vpn-instance-name* ● **ntp unicast-peer** *ipv4-address* **authentication-keyid** *key-id* **vpn-instance** *vpn-instance-name*。

10.1.4 维护及调试

目的

当 NTP 功能不正常，需要进行查看、定位问题时，可以使用本小节操作。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

10.1.5 配置举例

组网要求

NTP 协议是典型的工作在 Server-Client 模式下的协议，Client 与 Server 相连，Client 从 Server 处获得当前的时间，如图 10-1 所示。

组网图

图 10-1 NTP 配置示意图

配置步骤

步骤 1：（略）配置 NTP 服务器和客户端的 VLAN 和接口，使服务器和客户端之间能够 ping 通。

步骤 2：配置 NTP 服务器为主时钟和层数

Server(config-ntp)#master

Server(config-ntp)#stratum 2

步骤 3：配置 NTP 客户端的层数

Client(config-ntp)#stratum 9

步骤 4：配置 NTP 客户端的模式和 IP 地址（单播模式）

Client(config-ntp)#ntp unicast-server A.B.C.D（服务器的 IP 地址）

 **注意：**

其他模式类似配置步骤，不同在于多播和广播模式需要在服务器上指定模式。

10.2 RMON 配置

10.2.1 RMON 概述

简介

远程监控（RMON）是一个标准监控规范，它可以使各种网络监控器和控制台系统之间交换网络监控数据。RMON 为网络管理员选择符合特殊网络需求的控制台和网络监控探测器提供了更多的自由。

当前 RMON 有两种版本：RMON v1 和 RMONv2。RMON v1 在目前使用较为广泛的网络硬件中都能发现，它定义了 9 个 MIB 组服务于基本网络监控；RMON v2 是 RMON 的扩展，专注于 MAC 层以上更高的流量层，它主要强调 IP 流量和应用程序层流量。RMON v2 允许网络管理应用程序监控所有网络层的信息包，这与 RMONv1 不同，后者只允许监控 MAC 及其以下层的信息包。

 注意：

目前我司设备使用 RMON v1，只实现了 group 1/2/3/9（统计、历史、告警和事件）。

RMON 的实现方式

RMON 基于简单网络管理协议 SNMP 体系结构实现，与现存 SNMP 框架兼容，包括网管工作站 NMS 和运行在各网络设备上的代理 Agent 两部分。

RMON Agent 跟踪统计网络中的各种流量信息，例如，某段时间内某网段上的报文总数，或发往某台主机的正确报文总数等。它使 SNMP 更有效、更积极主动地监测远程网络设备，为监控子网的运行提供了一种高效手段。减少了网管站与代理 Agent 间的通讯流量，从而实现更简单有效地管理大型网络。

RMON 允许有多个监控者，它可用两种方法收集数据。

- 通过专用的 RMON Probe（探测仪）。NMS 直接从 RMON Probe 获取管理信息并控制网络资源，这种方式可以获取 RMON MIB 的全部信息。
- 将 RMON Agent 直接嵌入网络设备（例如交换机）中，使它们成为带 RMON Probe 功能的网络设备。NMS 是用 SNMP 基本命令与其交换数据信息，收集网络管理信息。这种方式受设备资源限制，一般无法获取 RMON MIB 的所有数据，大多数只收集四个组（告警、事件、历史和统计）的信息。

 注意：

目前我司设备采用 RMON Agent 方式。

RMON1 MIB 组

RMON1 MIB 组	功能	元素
统计量	包括探测器为该设备每个监控的接口测量的统计值。	数据包丢弃、数据包发送、广播数据包、CRC 错误、大小块、冲突以及计数器的数据包。范围从 64~128、128~256、256~512、512~1024 以及 1024~1518 字节。

历史	定期地收集统计网络值地记录并存储起来以便日后提取。	取样周期、样品数目和项目。提供有关网段流量、错误包、广播包、利用率以及碰撞次数等其他统计信息的历史数据。
告警	定期从探测器的变量选取统计例子。并与前面配的阈值相比较。	告警类型、间隔、阈值上限、阈值下限
主机	包括网络上发现的与每个主机相关的统计值。	主机地址、数据包、接收字节、传输字节、广播传送等。
HostTopN	准备描述主机的表，根据一个统计值排序列表。	统计值、主机、周期的开始和结束、速率基值、持续时间。
真值表	记录关于子网上两个主机之间流量的信息，该信息以矩阵形式存储起来。	源地址和目的地址对、数据包、字节和每一对的错误。
过滤器	允许监视器观测与一过滤器相匹配的数据包。	字节过滤器类型、过滤器表达式等。
捕获包	数据包在流过一个信道之后被捕获。	捕获所有通过过滤器的数据包或简单地记下基于这些数据包的统计。
事件	控制在此处事件的产生和报告.	事件类型、描述、事件最后一个发送的时间
令牌环	支持令牌环	不常使用

10.2.2 配置统计表

目的

使用本节操作配置 RMON，可以收集接口流量信息。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
配置 RMON 统计记录控制	1. 进入全局配置视图； 2. 进入接口配置视图； 3. 执行命令 **rmon statistics** *statistics-id* [*owner*]配置 RMON 统计记录控制。
删除已配置 RMON 统计记录控制	1. 进入全局配置视图； 2. 进入接口配置视图； 3. 执行命令 **no rmon statistics** *statistics-id* 删除已配置 RMON 统计记录控制。

10.2.3 配置历史控制表

目的

使用本节操作配置 RMON，可以定期对指定的端口进行数据采集并将采集到的信息保存到历史表中以备查看。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
配置 RMON 历史记录控制	1. 进入全局配置视图； 2. 进入接口配置视图； 3. 执行命令 **rmon history** *history-id sampling-interval sample-number* [*owner*]配置 RMON 历史记录控制。
删除已配置 RMON 历史记录控制	1. 进入全局配置视图； 2. 进入接口配置视图； 3. 执行命令 **no rmon history** *history-id* 删除已配置 RMON 历史记录控制。

10.2.4 配置告警表

目的

使用本节操作配置 RMON，可以按照指定的采样间隔对指定的告警变量（用此变量的 OID 指定）进行监视，当被监视数据的值越过定义的阈值时会产生告警事件。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
配置 RMON 告警条目	1. 进入全局配置视图； 2. 执行命令 **rmon alarm** *alarm-id object-id query-interval* { **absolute** | **delta** } *rising-threshold falling-threshold rising-event falling-event* [*owner*]配置 RMON 告警条目。
删除已配置 RMON 告警条目	1. 进入全局配置视图； 2. 执行命令 **no rmon alarm** *alarm-id* 删除已配置 RMON 告警条目。

10.2.5 配置事件表

目的

使用本节操作配置 RMON，当事件超过告警阈值时，设备可以记录日志或者产生告警，或者同时记录日志和产生告警。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
配置 RMON 事件控制条目	1. 进入全局配置视图； 2. 执行命令 **rmon event** *event-id* { **log** | **trap** | **both** } [*description*] [*owner*]配置 RMON 事件控制条目。
删除已配置 RMON 事件控制条目	1. 进入全局配置视图； 2. 执行命令 **no rmon event** *event-id* 删除已配置 RMON 事件控制条目。

10.2.6 维护及调试

目的

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

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
查看 RMON 告警控制条目的配置信息	1. 进入普通用户视图、特权用户视图、全局配置视图、接口配置视图（以太网、trunk）、接口组配置视图、批量接口配置视图； 2. 执行命令 **show rmon alarm**。
查看 RMON 事件的配置信息	1. 进入普通用户视图、特权用户视图、全局配置视图、接口配置视图（以太网、trunk）、接口组配置视图、批量接口配置视图； 2. 执行命令 **show rmon config**。
查看 RMON 事件控制条目的配置信息	1. 进入普通用户视图、特权用户视图、全局配置视图、接口配置视图（以太网、trunk）、接口组配置视图、批量接口配置视图； 2. 执行命令 **show rmon event**。
查看 RMON 历史控制条目的配置信息	1.进入普通用户视图、特权用户视图、全局配置视图、接口配置视图（以太网、trunk）、接口组配置视图、批量接口配置视图； 2. 执行命令 **show rmon history** [*history-id*]。

目的	步骤
查看 RMON 历史记录控制条目的统计信息	1.进入普通用户视图、特权用户视图、全局配置视图、接口配置视图（以太网、trunk）、接口组配置视图、批量接口配置视图； 2. 执行命令 **show rmon history statistic**。
查看 RMON 事件的日志信息	1.进入普通用户视图、特权用户视图、全局配置视图、接口配置视图（以太网、trunk）、接口组配置视图、批量接口配置视图； 2. 执行命令 **show rmon log**。
查看 RMON 统计表信息	1.进入普通用户视图、特权用户视图、全局配置视图、接口配置视图（以太网、trunk）、接口组配置视图、批量接口配置视图； 2. 执行命令 **show rmon statistic**。

10.2.7 配置举例

组网要求

现通过 CN12800 端口 10GE1/0/2 对其连接的的子网进行监控，包括：流量和各种类型包数据量的实时和历史统计信息；对此接口流量的字节数设置告警监控，超过设定值时记录日志；对超过告警设置值主动向 NMS 上报告警信息，如图 10-2 所示。

组网图

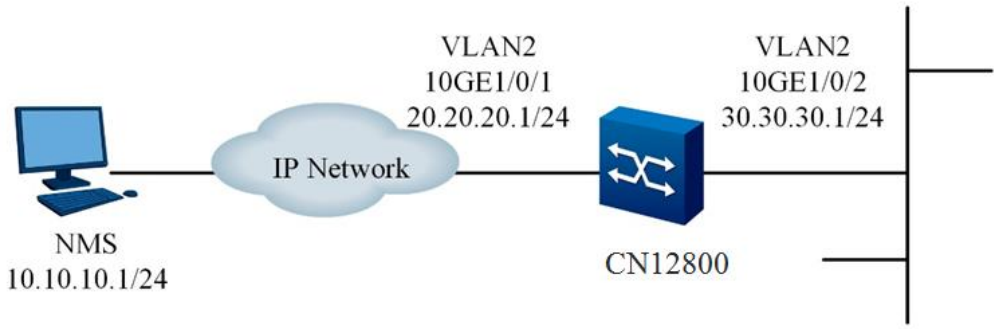


图 10-2 RMON 配置示意图

前提配置

1. 配置好 CN12800 的接口 10GE1/0/1 和 10GE1/0/2 的 IP 地址；
2. 配置好 CN12800 和 NMS 路由可达；
3. 配置好 CN12800 的 SNMP。

配置步骤

1、配置 CN12800 统计表。

CN12800#configure

CN12800(config)#interface 10gigaethernet 1/0/2

CN12800(config-10ge1/0/2)#rmon statistics 1

CN12800(config-10ge1/0/2)#

2、配置 CN12800 历史控制表。

CN12800(config-10ge1/0/2)#rmon history 1 10 30

CN12800(config-10ge1/0/2)#quit

CN12800(config)#

3、配置 CN12800 告警表。

CN12800(config)#rmon alarm 1 1.3.6.1.2.1.2.2.1.8.2 2 absolute 1 1 2 1

CN12800(config)#

4、配置 CN12800 事件表。

CN12800(config)#rmon event 1 both CLI

CN12800(config)#

10.3 SNMP 配置

10.3.1 SNMP 概述

协议介绍

SNMP（Simple Network Management Protocol，简单网络管理协议）是目前网络中用得最广泛的网络管理协议，也是被广泛接受并投入使用的工业标准，用于保证管理信息在任意两点间传送，便于网络管理员在网络上的任何节点检索信息、修改信息、寻找故障、完成故障诊断、进行容量规划和生成报告。SNMP 采用轮询机制，只提供最基本的功能集，特别适合在小型、快速和低价格的环境中使用。SNMP 的实现基于无连接的传输层协议 UDP，得到众多产品的支持。

SNMP 分为 NMS 和 Agent 两部分，NMS（Network Management Station），是运行客户端程序的工作站，目前常用的网管平台有 Sun NetManager 和 IBM NetView；Agent 是运行在网络设备上的服务器端软件。NMS 可以向 Agent 发出 GetRequest、GetNextRequest 和 SetRequest 报文，Agent 接收到 NMS 的请求报文后，根据报文类型进行 Read 或 Write

操作，生成 Response 报文，并将报文返回给 NMS。Agent 在设备发生重新启动等异常情况时，也会主动向 NMS 发送 Trap 报文，向 NMS 汇报所发生的事件。

支持的 SNMP 版本及 MIB

为了在 SNMP 报文中唯一标识设备中的管理变量，SNMP 用层次结构命名方案来识别管理对象。用层次结构命名的管理对象的集合就象一棵树，树的节点表示管理对象，如下图所示。管理对象可以用从根开始的一条路径唯一地识别。

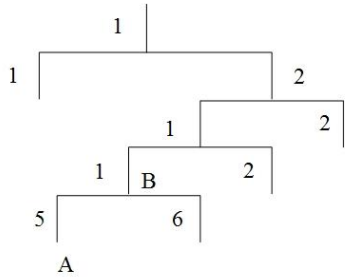


图 10-3 MIB 树结构

MIB（Management Information Base）的作用就是用来描述树的层次结构，它是所监控网络设备的标准变量定义的集合。在上图中，管理对象 B 可以用一串数字{1.2.1.1}唯一确定，这串数字是管理对象的 Object Identifier（客体标识符）。

CN12800 系列数据中心交换机中的 SNMP Agent 支持 SNMP V1、V2 和 V3，支持的常见 MIB 如下表所示。

表 10-1 交换机支持常见 MIB

MIB 属性	MIB 内容	参见资料
公有 MIB	基于 TCP/IP 网络设备的 MIB II	参见 RFC1213
	RMON MIB	参见 RFC2819
	以太网 MIB	参见 RFC2665
	IF MIB	参见 RFC1573
私有 MIB	DHCP MIB	-
	QACL MIB	
	ADBM MIB	
	RSTP MIB	
	VLAN MIB	
	设备管理	
	接口管理	

10.3.2 配置 SNMP 维护信息

目的

用户通过本节操作配置 SNMP 的维护信息，便于网管对设备的维护。

在交换机出现错误需要紧急解决时，便于联系本地的维护工程师。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

10.3.3 配置 SNMP 基本功能

目的

用户通过本节操作配置 SNMP 基本功能，实现网管站 NM Station 和 Agent 两部分的正常通信。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

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

目的	步骤
配置 SNMP 视图	1. 进入全局配置视图； 2. 执行如下命令创建不同的 MIB 视图使网管访问设备时具有不同的访问权限： ● **snmp view** *view-name oid-tree* { **included** | **excluded** } ● **snmp view** *view-name oid-tree* { **included** | **excluded** } **mask** *subtreemask*。
配置 SNMP 组信息	1. 进入全局配置视图； 2. 执行命令 **snmp group** *group-name* **read-view** *read-view* **write-view** *write-view* **notify-view** *notify-view* 配置 SNMP 组。
创建 SNMP 用户	1. 进入全局配置视图； 2. 执行如下命令创建用户信息，可以使指定组中的用户对设备进行访问： ● **snmp user** *user-name* **group** *group-name* **no-auth-no-priv** [**filter-list** *acl-number*] ● **snmp user** *user-name* **group** *group-name* **auth { md5 | sha** } *authkey* **priv no-priv** [**filter-list** *acl-number*] ● **snmp user** *user-name* **group** *group-name* **auth** { **md5** | **sha** } *authkey* **priv** { **dea** | **des** } *privkey* ● **snmp user** *user-name* **group** *group-name* **auth** { **md5** | **sha** } *authkey* **priv** { **des** | **aes** } *privkey* [**filter-list** *acl-number*]。
（可选）配置 SNMP 重认证时间	1. 进入全局配置视图； 2. 执行命令 **snmp reauth-interval** *interval* 设置 SNMP 验证失败时重新进行认证的间隔时间。
（可选）配置 SNMP 认证失败次数	1. 进入全局配置视图； 2. 执行命令 **snmp fail-count** *count* 设置 SNMP 进行认证失败的次数。
（可选）配置 SNMP 端口号	1. 进入全局配置视图； 2. 执行命令 **snmp port** { *port-number* | **default** }设置 SNMP 协议包使用的端口号。
删除 SNMP 团体名	1. 进入全局配置视图； 2. 执行命令 **no snmp community** *name* 删除已配置的 SNMP 团体名。
（可选）去使能写团体名功能	1. 进入全局配置视图； 2. 执行命令 **snmp rw-community disable** 去使能写团体名功能。
删除 SNMP 用户	1. 进入全局配置视图； 2. 执行命令 **no snmp user** *user-name* 删除已创建的 SNMP 用户。
删除 SNMP 组信息	1. 进入全局配置视图； 2. 执行命令 **no snmp group** *group-name* 删除已配置的 SNMP 组信息。
删除 SNMP 视图	1. 进入全局配置视图； 2. 执行命令 **no snmp view** *view-name* 或执行命令 **no snmp view** *view-name oid-tree* 删除已配置的 SNMP 视图。

目的	步骤
配置 SNMP Get Bulk 请求的 varbind 最大个数	1. 进入全局配置视图； 2. 执行命令 **snmp bulk max-varbind** { *varbind-number* | **default** }配置 SNMP Get Bulk 请求的 varbind 最大个数。

10.3.4 配置发送 Trap 功能

背景信息

Trap 是被管理设备未经请求而主动向 NMS 发送的消息，用于报告重要紧急的事件。被管理设备必须配置 Trap 功能后才会主动发送这些消息。

目的

用户通过本节操作配置设备主动发送 Trap 消息。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
（可选）使能认证失败后发送 Trap 消息的功能	1. 进入全局配置视图； 2. 执行命令 **snmp auth-trap enable** 使能认证 trap 后，如果认证失败则设备会发送 trap 消息。
（可选）使能 SNMP 丰富告警功能	1. 进入全局配置视图； 2. 执行命令 **snmp rich-trap enable**。
指定 SNMP 的 Trap 信息的目标主机	1. 执行命令 **configure** 进入全局配置视图； 2. （IPv4）执行如下命令： ● **snmp trap-server** *ipv4-address security-name* { **v1** | **v2** | **v3** } ● **snmp trap-server** *ipv4-address port security-name* { **v1** | **v2** | **v3** } ● **snmp trap-server** *ipv4-address security-name* **v3** { **auth** | **priv** } ● **snmp trap-server** *ipv4-address port security-name* **v3** { **auth** | **priv** }。
（可选）配置 SNMP 告警历史表的大小	1. 进入全局配置视图； 2. 执行命令 **snmp trap-history** { *history-table-size* | **default** }。
（可选）去使能认证失败后发送 Trap 消息的功能	1. 进入全局配置视图； 2. 执行命令 **snmp auth-trap disable** 去使能认证 trap 后，如果认证失败设备则不会发送 trap 消息。

目的	步骤
（可选）去使能 SNMP 丰富告警功能	1. 进入全局配置视图； 2. 执行命令 **snmp rich-trap disable**。
删除 SNMP Trap 消息的发布地址	1. 进入全局配置视图； 2. 执行命令 **no snmp trap-source**。
删除 SNMP 的 Trap 信息的目标主机	1. 进入全局配置视图； 2. （IPv4）执行如下命令： ● **no snmp trap-server** *ipv4-address* ● **no snmp trap-server** *ipv4-address security-name*。

10.3.5 维护及调试

目的

用户可以通过本节操作对 SNMP 协议进行调试，用于定位问题。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
查看设备 SNMP 的代理信息	1. 进入普通用户视图、特权用户视图、全局配置视图； 2. 执行命令 **show snmp agent** 查看设备 SNMP 的代理信息。
查看 SNMP 的团体配置信息	1. 进入普通用户视图、特权用户视图、全局配置视图； 2. 执行命令 **show snmp community** 查看 SNMP 的团体配置信息。
查看 SNMP 的配置信息	1. 进入普通用户视图、特权用户视图、全局配置视图； 2. 执行命令 **show snmp config** 查看 SNMP 的配置信息。
查看 SNMP 组信息	1. 进入普通用户视图、特权用户视图、全局配置视图； 2. 执行命令 **show snmp group** 查看 SNMP 组信息。
查看 SNMP 的报文处理统计数据信息	1. 进入普通用户视图、特权用户视图、全局配置视图； 2. 执行命令 **show snmp statistic** 查看 SNMP 的报文处理统计数据信息。
查看 SNMP 的告警描述信息	1. 进入普通用户视图、特权用户视图、全局配置视图； 2. 执行命令 **show snmp trap-description** 查看 SNMP 的告警描述信息；

目的	步骤
查看 SNMP 的告警历史信息	1. 进入普通用户视图、特权用户视图、全局配置视图； 2. 执行命令 **show snmp trap-history** 查看 SNMP 的告警历史信息。
查看显示接收 trap 信息的主机及版本类型	1.进入普通用户视图、特权用户视图、全局配置视图； 2. 执行命令 **show snmp trap-server** 查看显示接收 trap 信息的主机及版本类型。
查看 SNMP 用户信息	1. 进入普通用户视图、特权用户视图、全局配置视图； 2. 执行命令 **show snmp user** 查看 SNMP 用户信息。
查看 SNMP 视图信息	1. 进入普通用户视图、特权用户视图、全局配置视图； 2. 执行命令 **show snmp view** 查看 SNMP 视图信息。
查看网络管理协议的告警信息状态	1. 进入普通用户视图； 2. 执行命令 **show snmp trap state** 查看网络管理协议的告警信息状态。

10.3.6 配置举例

组网要求

网管工作站（NMS）与交换机通过以太网相连，网管工作站 IP 地址为 129.102.149.13，交换机的 IP 地址为 129.102.0.1。在交换机上进行如下配置：设置团体名和访问权限、允许交换机发送 Trap 消息，如图 10-4 所示。

组网图

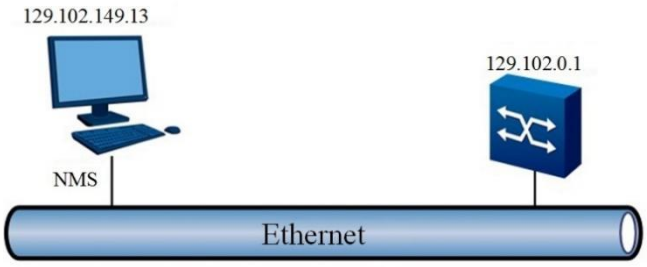


图 10-4 SNMP 配置举例组网图

配置交换机

#进入全局配置视图

CN12800#config

#设置团体、群组和用户

CN12800(config)#snmp view v3test 1.3.6 include

CN12800(config)#snmp group aaa read-view v3test write-view v3test notify-view v3test

CN12800(config)#snmp user admin group aaa no-auth-no-priv

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

CN12800(config)#snmp trap enable

CN12800(config)#snmp trap-server 129.102.149.23 name123 v3

配置 NMS

网管所在的 PC 机需要进行登录设置。对于 Mib-Browser，登录设置为：SNMPV1、V2 使用缺省的团体名登录，SNMPV3 使用用户 admin 登录。用户可利用网管系统完成对交换机的查询和配置操作，具体情况请参考网管产品的配套手册。

10.4 LLDP 配置

10.4.1 LLDP 概述

背景

目前以太网技术应用越来越广泛，随着大规模组网应用的需求以及日益繁多且配置复杂的网络设备的出现，对网络管理的能力的要求也越来越高。为了使不同厂商的设备能够在网络中相互发现并交互各自的系统及配置信息，需要有一个标准的信息交流平台。但现阶段许多网管软件最多只能分析到第三层网络拓扑结构，无法说明设备的位置以及网络操作方式等信息。LLDP（Link Layer Discovery Protocol，链路层发现协议）就是在这样的背景下产生的。

LLDP 简介

LLDP 是 IEEE 802.1ab 中定义的第二层发现协议。它提供了一种标准的链路层发现方式，可以将本端设备的的主要能力、管理地址、设备标识、接口标识等信息组织成不同的 TLV（Type/Length/Value，类型/长度/值），并封装在 LLDPDU（Link Layer Discovery Protocol Data Unit，链路层发现协议数据单元）中发布给与自己直连的邻居，邻居收到这些信息后将其以标准 MIB（Management Information Base，管理信息库）的形式保存起来，以供网络管理系统查询及判断链路的通信状况。

通过运行该协议，网络系统可以清晰得知与之相连所有设备的二层信息，这既有利于网管规模迅速扩大，同时也利于掌握更详细的网络拓扑信息及变化信息。LLDP 协议还有助于发现网络中实际存在的不合理的配置并上报给网管系统，及时消除错误配置。

LLDP 术语解释

- LLDP：Link Layer Discovery Protocol 链路层发现协议
- LLDPDU：Link Layer Discovery Protocol Data Unit 链路层发现协议数据单元
- MIB：Management Information Base (module)管理系统库
- SNAP：Subnetwork Access Protocol 子网访问协议
- TTL：time to live (value)存活时间

10.4.2 LLDP 工作机制

LLDP 端口工作模式

LLDP 端口有以下四种工作模式：

- TxRx：既发送也接收 LLDP 报文。
- Tx：只发送不接收 LLDP 报文。
- Rx：只接收不发送 LLDP 报文。
- Disable：既不发送也不接收 LLDP 报文。

说明：

当端口的 LLDP 工作模式发生变化时，端口将对协议状态机进行初始化操作。为了避免端口工作模式频繁改变而导致端口不断执行初始化操作，可配置端口初始化延迟时间，当端口工作模式改变时延迟一段时间再执行初始化操作。

10.4.3 配置 LLDP 基本功能

目的

使用本节操作配置 LLDP，以便不同厂商设备可以拓扑发现，获取对端的能力、配置等信息，同时使网络管理系统有办法发现一些影响上层应用交互的配置不一致或错误，帮助定位不一致或错误问题。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
端口下使能或去使能 LLDP 及其管理状态	1. 进入全局配置视图； 2. 进入接口组配置视图； 3. 执行命令 **lldp admin-status** { **tx-only** | **rx-only** | **rx-tx** | **disable** }使能或去使能接口 LLDP 及其管理状态。
配置 LLDP 的管理地址	1. 进入全局配置视图； 2. 进入接口配置视图、接口组配置视图； 3. 执行命令 **lldp management-address** *ip-address* { **enable** | **disable** }或 **lldp management-address** *mac-address* { **enable** | **disable** }配置 LLDP 的管理地址。

10.4.4 配置 LLDP 参数

目的

用户可以使用本节操作，根据网络负载及时调整 LLDP 报文发送、延迟时间等 LLDP 相关参数。

本节操作均可根据实际情况选配。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
（可选）配置 lldp 帧发送时间间隔	1. 进入全局配置视图、接口配置视图（以太网）、接口组配置视图； 2. 执行命令 **lldp tx-interval** { *tx-interval* | **default** }配置 LLDP 帧发送时间间隔。
（可选）配置 LLDP 帧发送间隔的倍数	1. 进入全局配置视图、接口配置视图（以太网）、接口组配置视图； 2. 执行命令 **lldp tx-hold** { *tx-hold* | **default** }配置 LLDP 帧发送间隔的倍数。
（可选）配置 LLDP 端口状态重新初始化的时延	1. 进入全局配置视图、接口配置视图（以太网）、接口组配置视图； 2. 执行命令 **lldp reinit-delay** { *reinit-delay* | **default** }配置 LLDP 端口状态重新初始化的时延。
（可选）配置设备发送 LLDP 报文的延迟时间	1. 进入全局配置视图、接口配置视图（以太网）、接口组配置视图； 2. 执行命令 **lldp tx-delay** { *tx-delay* | **default** }配置设备发送 LLDP 报文的延迟时间。
（可选）全局配置告警发送时间间隔	1. 进入全局配置视图、接口配置视图（以太网）、接口组配置视图； 2. 执行命令 **lldp notification-interval** { *notification-interval* | **default** }全局配置告警发送时间间隔。

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

目的	步骤
配置设备自身的位置信息	1. 进入全局配置视图； 2. 进入接口配置视图、接口组配置视图； 3. 执行如下命令配置设备自身的位置信息： ● **lldp location-id civic-address** *civic-address country-code ca-type ca-value* ● **lldp location-id civic-address** *civic-address country-code ca-type ca-value ca-type ca-value* ● **lldp location-id civic-address** *civic-address country-code ca-type ca-value ca-type ca-value ca-type ca-value* ● **lldp location-id civic-address** *civic-address country-code ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value* ● **lldp location-id civic-address** *civic-address country-code ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value* ● **lldp location-id civic-address** *civic-address country-code ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value* ● **lldp location-id civic-address** *civic-address country-code ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value* ● **lldp location-id civic-address** *civic-address country-code ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value* ● **lldp location-id civic-address** *civic-address country-code ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value* ● **lldp location-id civic-address** *civic-address country-code ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value ca-type ca-value* ● **lldp location-id elin-address** *number*。

10.4.5 维护及调试

目的

当 LLDP 功能不正常，需要进行查看、定位问题时，可以使用本小节操作。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列交换机命令行手册》。

目的	步骤
查看 LLDP 端口信息	1. 进入普通用户视图、特权用户视图、全局配置视图、接口配置视图； 2. 执行如下命令： ● **show lldp interface** ● **show lldp interface** { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* ● **show lldp interface verbose**。
查看 LLDP 统计信息	1. 进入普通用户视图、特权用户视图、全局配置视图、接口配置视图； 2. 执行如下命令： ● **show lldp statistic** ● **show lldp statistic interface** { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number*。
查看所有邻居或者指定邻居的设备信息	1. 进入普通用户视图、特权用户视图、全局配置视图、接口配置视图； 2. 执行如下命令： ● **show lldp remote** ● **show lldp remote verbose** ● **show lldp remote** *remote-number*。
查看 LLDP 本地信息	1. 进入普通用户视图、特权用户视图、全局配置视图、接口配置视图； 2. 执行命令 **show lldp local** 查看 LLDP 本地信息。
查看 LLDP 的配置信息	1. 进入普通用户视图、特权用户视图、全局配置视图、接口配置视图； 2. 执行命令 **show lldp config** 查看 LLDP 的配置信息。
查看指定接口邻居信息	1. 进入普通用户视图、特权用户视图、全局配置视图、接口配置视图； 2. 执行命令 **show lldp remote interface** { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* 查看指定接口邻居信息。
查看指定接口配置信息	1. 进入普通用户视图、特权用户视图、全局配置视图、接口配置视图； 2. 执行命令 **show lldp config interface** { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* 查看指定接口配置信息。
查看指定接口本地设备信息	1. 进入普通用户视图、特权用户视图、全局配置视图、接口配置视图； 2. 执行命令 **show lldp local interface** { **ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* 查看指定接口本地设备信息。
清零 LLDP 端口的统计计数	1. 进入全局配置视图； 2. 进入接口配置视图、接口组配置视图； 3. 执行命令 **reset lldp counter** 清零 LLDP 端口的统计计数。
打开或关闭 LLDP 调试开关	1. 进入特权用户视图；

目的	步骤
	2. 执行命令 **debug lldp** { **config** | **rxstate** | **txstate** | **rxpkt** | **event** | **sync** | **all** }或 **no debug lldp** { **config** | **rxstate** | **txstate** | **rxpkt** | **event** | **sync** | **all** }打开或关闭 LLDP 调试开关。

10.4.6 配置举例

组网要求

1) CN12800_1、CN12800_2、CN12800_3、CN12800_4、CN12800_5 五台交换机分别将自己的 Chassis ID、端口号 ID、TTL、管理地址以及其他的配置信息公告给其他设备。

2) 每一台设备都可以将获得的信息存储至本地 MIB 数据库中，并可通过 SNMP 访问。

3) PC 通过 SNMP 访问 CN12800_1，可得知 CN12800_2、CN12800_3 是与 CN12800_1 直连的设备，由此可得出与 CN12800_1 直连的拓扑。并通过 CN12800_2、CN12800_3 公告的消息中得知 CN12800_2、CN12800_3 的管理地址，分别为 10.1.1.2 与 10.1.1.3，进而访问 CN12800_2 与 CN12800_3。

4) 访问 CN12800_2，可知与 CN12800_2 直连的设备有 CN12800_4，由此可得出与 CN12800_2 直连的拓扑。并且可通过 CN12800_4 公告的消息中得知 CN12800_4 的管理地址，为 10.1.1.4，进而可继续访问 CN12800_4。

5) 访问 CN12800_3，可知与 CN12800_3 直连的设备有 CN12800_5，由此可得出与 CN12800_3 直连的拓扑。并且可通过 CN12800_5 公告的消息中得知 CN12800_5 的管理地址为 10.1.1.5，进而可继续访问 CN12800_5。

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

组网图

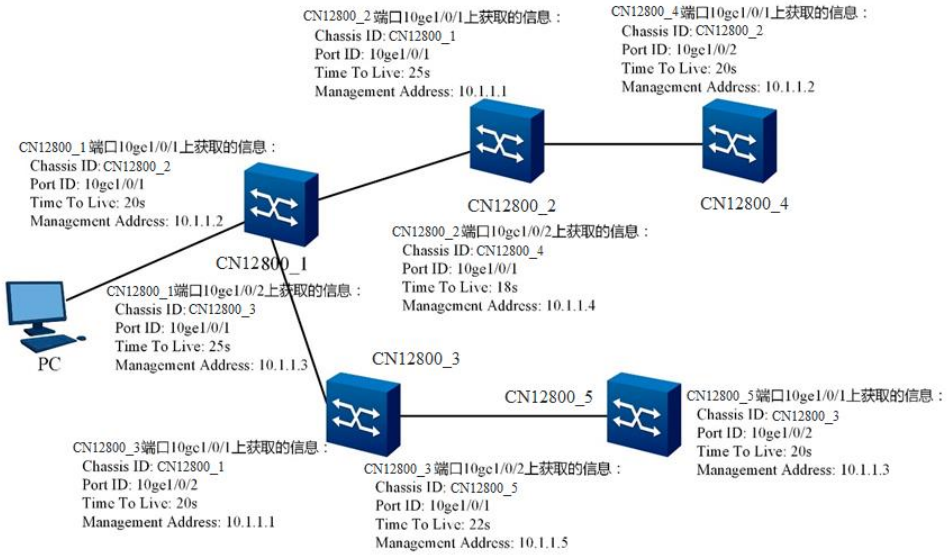


图 10-5 LLDP 配置示意图

配置思路

在 CN12800_1 设置 LLDP 工作模式为 rx-tx，并配置管理地址为 10.1.1.1。

在 CN12800_2 设置 LLDP 工作模式为 rx-tx，并配置管理地址为 10.1.1.2。

在 CN12800_3 设置 LLDP 工作模式为 rx-tx，并配置管理地址为 10.1.1.3。

在 CN12800_4 设置 LLDP 工作模式为 rx-tx，并配置管理地址为 10.1.1.4。

在 CN12800_5 设置 LLDP 工作模式为 rx-tx，并配置管理地址为 10.1.1.5。

配置步骤

1、配置 CN12800_1。

CN12800_1(config)#interface 10gigaethernet 1/0/1

CN12800_1(config-10ge1/0/1)#no shutdown

CN12800_1(config-10ge1/0/1)#lldp admin-status rx-tx

CN12800_1(config-10ge1/0/1)#lldp management-address 10.1.1.1 enable

2、配置 CN12800_2。

CN12800_2(config)#interface 10gigaethernet 1/0/1

CN12800_2(config-10ge1/0/1)#no shutdown

CN12800_2(config-10ge1/0/1)#lldp admin-status rx-tx

CN12800_2(config-10ge1/0/1)#lldp management-address 10.1.1.2 enable

3、配置 CN12800_3。

CN12800_3(config)#interface 10gigaethernet 1/0/1

CN12800_3(config-10ge1/0/1)#no shutdown

CN12800_3(config-10ge1/0/1)#lldp admin-status rx-tx

CN12800_3(config-10ge1/0/1)#lldp management-address 10.1.1.3 enable

4、配置 CN12800_4。

CN12800_4(config)#interface 10gigaethernet 1/0/1

CN12800_4(config-10ge1/0/1)#no shutdown

CN12800_4(config-10ge1/0/1)#lldp admin-status rx-tx

CN12800_4(config-10ge1/0/1)#lldp management-address 10.1.1.4 enable

5、配置 CN12800_5。

CN12800_5(config)#interface 10gigaethernet 1/0/1

CN12800_5(config-10ge1/0/1)#no shutdown

CN12800_5(config-10ge1/0/1)#lldp admin-status rx-tx

CN12800_5(config-10ge1/0/1)#lldp management-address 10.1.1.5 enable

10.5 报文捕获配置

10.5.1 CPU 报文捕获概述

用户使用设备的 CPU 调试功能，可以查看 CPU 收发包详细信息。该功能可以供用户在设备出现问题时，调试设备使用。

10.5.2 维护及调试

目的

当设备功能不正常，用户需要查看设备送往 CPU 的数据包时，可以使用本小节操作。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
显示 CPU 收发包的接口统计信息	1. 在全局配置视图下，执行命令 **disable** 退出到普通用户视图。 2. 执行以下命令： ● **show cpupkt interface** { **ethernet** | **gigaethernet** | **xgigaethernet**| **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number* ● **show cpupkt interface** { **ethernet** | **gigaethernet** | **xgigaethernet**| **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number* { **alltype** | **anydata-dcp** | **anydata-ha** | **arp** | **arpmiss** | **bfd-eth** | **bfd-ip** | **bfd-ipv6** | **bgp** | **cfm** | **dad** | **dcp** | **dhcp** | **dhcpv6** | **dot1x** | **dot3ah** | **eaps** | **g8031** | **g8032** | **ha** | **hwapi-dcp** | **hwapi-ha** | **icmp** | **icmpv6** | **icmpv6-echo-reply** | **icmpv6-echo-request** | **icmpv6-na** | **icmpv6-ns** | **icmpv6-ra** | **icmpv6-redirect** | **icmpv6-rs** | **igmp** | **ip** | **ipv6** | **isis** | **iss** | **lacp** | **loopback** | **mlag** | **ndmiss** | **ospf** | **ospfv3** | **other** | **rer** | **sgm** | **snmp** | **spanningtree** | **stack-kernel** | **stack-user** | **sw-dcp** | **sw-ha** | **swif-dcp** | **swif-ha** | **tcp** | **tcp6** | **udp** | **udp6** | **vrrpv2** | **vrrpv3** | **y1731** } { **statistic** | **change** } ● **show cpupkt interface eth-trunk** *trunk-number* { **alltype** | **anydata-dcp** | **anydata-ha** | **arp** | **arpmiss** | **bfd-eth** | **bfd-ip** | **bfd-ipv6** | **bgp** | **cfm** | **dad** | **dcp** | **dhcp** | **dhcpv6** | **dot1x** | **dot3ah** | **eaps** | **g8031** | **g8032** | **ha** | **hwapi-dcp** | **hwapi-ha** | **icmp** | **icmpv6** | **icmpv6-echo-reply** | **icmpv6-echo-request** | **icmpv6-na** | **icmpv6-ns** | **icmpv6-ra** | **icmpv6-redirect** | **icmpv6-rs** | **igmp** | **ip** | **ipv6** | **isis** | **iss** | **lacp** | **loopback** | **mlag** | **ndmiss** | **ospf** | **ospfv3** | **other** | **rer** | **sgm** | **snmp** | **spanningtree** | **stack-kernel** | **stack-user** | **sw-dcp** | **sw-ha** | **swif-dcp** | **swif-ha** | **tcp** | **tcp6** | **udp** | **udp6** | **vrrpv2** | **vrrpv3** | **y1731** } **statistic** ● **show cpupkt interface statistic** { **alltype** | **anydata-dcp** | **anydata-ha** | **arp** | **arpmiss** | **bfd-eth** | **bfd-ip** | **bfd-ipv6** | **bgp** | **cfm** | **dad** | **dcp** | **dhcp** | **dhcpv6** | **dot1x** | **dot3ah** | **eaps** | **g8031** | **g8032** | **ha** | **hwapi-dcp** | **hwapi-ha** | **icmp** | **icmpv6** | **icmpv6-echo-reply** | **icmpv6-echo-request** | **icmpv6-na** | **icmpv6-ns** | **icmpv6-ra** | **icmpv6-redirect** | **icmpv6-rs** | **igmp** | **ip** | **ipv6** | **isis** | **iss** | **lacp** | **loopback** | **mlag** | **ndmiss** | **ospf** | **ospfv3** | **other** | **rer** | **sgm** | **snmp** | **spanningtree** | **stack-kernel** | **stack-user** | **sw-dcp** | **sw-ha** | **swif-dcp** | **swif-ha** | **tcp** | **tcp6** | **udp** | **udp6** | **vrrpv2** | **vrrpv3** | **y1731** } **brief [all]** ● **show cpupkt interface statistic brief all** ● **show cpupkt interface { ha | dcp | dcp2 }** ● **show cpupkt interface outband** ● **show cpupkt interface outband** { **alltype** | **anydata-dcp** | **anydata-ha** | **arp** | **arpmiss** | **bfd-eth** | **bfd-ip** | **bfd-ipv6** | **bgp** | **cfm** | **dad** | **dcp** | **dhcp** |

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

目的	步骤
	• **reset cpupkt interface** { **ethernet** | **gigaethernet** | **xgigaethernet**| **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number* • **reset cpupkt interface** { **ha** | **dcp** | **dcp2** } • **reset cpupkt interface outband** • **reset cpupkt interface outband** { **alltype** | **anydata-dcp** | **anydata-ha** | **arp** | **arpmiss** | **bfd-eth** | **bfd-ip** | **bfd-ipv6** | **bgp** | **cfm** | **dad** | **dcp** | **dhcp** | **dhcpv6** | **dot1x** | **dot3ah** | **eaps** | **g8031** | **g8032** | **ha** | **hwapi-dcp** | **hwapi-ha** | **icmp** | **icmpv6** | **icmpv6-echo-reply** | **icmpv6-echo-request** | **icmpv6-na** | **icmpv6-ns** | **icmpv6-ra** | **icmpv6-redirect** | **icmpv6-rs** | **igmp** | **ip** | **ipv6** | **isis** | **iss** | **lacp** | **loopback** | **mlag** | **ndmiss** | **ospf** | **ospfv3** | **other** | **rer** | **sgm** | **snmp** | **spanningtree** | **stack-kernel** | **stack-user** | **sw-dcp** | **sw-ha** | **swif-dcp** | **swif-ha** | **tcp** | **tcp6** | **udp** | **udp6** | **vrrpv2** | **vrrpv3** | **y1731** } **statistic** • **reset cpupkt interface** { **ethernet** | **gigaethernet** | **xgigaethernet**| **10gigaethernet** | **25gigaethernet** | **40gigaethernet** | **100gigaethernet** } *interface-number* { **alltype** | **anydata-dcp** | **anydata-ha** | **arp** | **arpmiss** | **bfd-eth** | **bfd-ip** | **bfd-ipv6** | **bgp** | **cfm** | **dad** | **dcp** | **dhcp** | **dhcpv6** | **dot1x** | **dot3ah** | **eaps** | **g8031** | **g8032** | **ha** | **hwapi-dcp** | **hwapi-ha** | **icmp** | **icmpv6** | **icmpv6-echo-reply** | **icmpv6-echo-request** | **icmpv6-na** | **icmpv6-ns** | **icmpv6-ra** | **icmpv6-redirect** | **icmpv6-rs** | **igmp** | **ip** | **ipv6** | **isis** | **iss** | **lacp** | **loopback** | **mlag** | **ndmiss** | **ospf** | **ospfv3** | **other** | **rer** | **sgm** | **snmp** | **spanningtree** | **stack-kernel** | **stack-user** | **sw-dcp** | **sw-ha** | **swif-dcp** | **swif-ha** | **tcp** | **tcp6** | **udp** | **udp6** | **vrrpv2** | **vrrpv3** | **y1731** } **statistic** • **reset cpupkt interface eth-trunk** *trunk-number* { **alltype** | **anydata-dcp** | **anydata-ha** | **arp** | **arpmiss** | **bfd-eth** | **bfd-ip** | **bfd-ipv6** | **bgp** | **cfm** | **dad** | **dcp** | **dhcp** | **dhcpv6** | **dot1x** | **dot3ah** | **eaps** | **g8031** | **g8032** | **ha** | **hwapi-dcp** | **hwapi-ha** | **icmp** | **icmpv6** | **icmpv6-echo-reply** | **icmpv6-echo-request** | **icmpv6-na** | **icmpv6-ns** | **icmpv6-ra** | **icmpv6-redirect** | **icmpv6-rs** | **igmp** | **ip** | **ipv6** | **isis** | **iss** | **lacp** | **loopback** | **mlag** | **ndmiss** | **ospf** | **ospfv3** | **other** | **rer** | **sgm** | **snmp** | **spanningtree** | **stack-kernel** | **stack-user** | **sw-dcp** | **sw-ha** | **swif-dcp** | **swif-ha** | **tcp** | **tcp6** | **udp** | **udp6** | **vrrpv2** | **vrrpv3** | **y1731** } **statistic**。

10.6 Telemetry 配置

10.6.1 Telemetry 概述

Telemetry 是一项远程的从物理设备或虚拟设备上高速采集数据的技术。设备通过推模式（Push Mode）周期性的主动向采集器上送设备的接口流量统计、CPU 或内存数据等信息，相对传统拉模式（Pull Mode）的一问一答式交互，提供了更实时更高速的数据采集功能。

10.6.2 配置目标采集器

目的

当用户配置 Telemetry 静态订阅采样数据时，需要创建上送目标组，并指定好采样数据要上送的目标采集器。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列高端交换机命令行手册》。

目的	步骤
使能或去使能数据采集功能	1. 进入全局配置视图； 2. 执行命令 **telemetry** { **enable** | **disable** }使能或去使能数据采集功能。
配置采样数据上送目标组并进入 Destination-group 视图	1. 进入全局配置视图； 2. 执行命令 **telemetry destination-group** *name* 配置采样数据上送目标组并进入 Destination-group 视图。
创建订阅用于关联上送目标组和采样传感器组并进入 Subscription 视图	1. 进入全局配置视图； 2. 执行命令 **telemetry subscription** *name* 创建订阅用于关联上送目标组和采样传感器组并进入 Subscription 视图。
配置关联上送目标组	1. 进入全局配置视图； 2. 执行命令 **telemetry subscription** *name* 进入 Subscription 视图； 3. 执行命令 **destination-group** *name* 配置关联上送目标组。
配置上送目标采集器的 IP 地址、端口号、上送目标采集器的协议和加密方式	1. 进入全局配置视图； 2. 执行命令 **telemetry destination-group** *name* 进入 Destination-group 视图； 3. 执行命令 **ip address** *ipv4-address* **port** *port-number* **protocol grpc** 或 **ip address** *ipv4-address* **port** *port-number* **vpn-instance** *name* **protocol grpc** 配置上送目标采集器的 IP 地址、端口号、上送目标采集器的协议和加密方式。

10.6.3 配置采样数据

目的

当用户配置 Telemetry 静态订阅采样数据时，需要创建采样传感器组，并指定好采样路径和过滤条件。

过程

根据不同目的，执行相应步骤，具体参见下表，参数说明请参考《CN12800 系列高端交换机命令行手册》。

目的	步骤
使能或去使能数据采集功能	1. 进入全局配置视图； 2. 执行命令 **telemetry** { **enable** | **disable** }使能或去使能数据采集功能。
创建采样传感器组并进入 Sensor-group 视图	1. 进入全局配置视图； 2. 执行命令 **telemetry sensor-group** *name* 创建采样传感器组并进入 Sensor-group 视图。
关联采样传感器组，并可配置该采样传感器组的采样周期	1. 进入全局配置视图； 2. 执行命令 **telemetry subscription** *name* 进入 Subscription 视图； 3. 执行命令 **sensor-group** *name* **sample-interval** *interval-value* 关联采样传感器组，并可配置该采样传感器组的采样周期。
配置 Telemetry 传感器采样路径	1. 进入全局配置视图； 2. 执行命令 **telemetry sensor-group** *name* 进入 Sensor-group 视图； 3. 执行命令 **sensor-path** *name* 配置 Telemetry 传感器采样路径。

10.6.4 维护及调试

目的

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

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
查看 Telemetry 传感器配置信息	1. 执行命令 **disable** 退出到普通用户视图 2. 执行命令 **show telemetry config** 查看 Telemetry 传感器配置信息。
查看上送目标组信息	1. 执行命令 **disable** 退出到普通用户视图 2. 执行命令 **show telemetry destination config** 查看上送目标组信息。
查看采样传感器组信息	1. 执行命令 **disable** 退出到普通用户视图 2. 执行命令 **show telemetry sensor config** 查看采样传感器组信息。

目的	步骤
查看 Telemetry 传感器的订阅信息	1. 执行命令 **disable** 退出到普通用户视图 2. 执行命令 **show telemetry subscription config** 查看 Telemetry 传感器的订阅信息。

10.7 设备升级与回退

升级准备

详细描述升级所需的必备工具，设备运行状态检查，软、硬件版本检查，软件包检查等升级前的准备工作，降低升级风险。

- OS 升级包，文件名为 CN12800_OS_V370R240.squ；
- PC 安装好 FTP 软件；
- PC 安装好 7zip 软件；
- PC 安装好 winSCP 软件；
- CN12800 设备；
- 串口线，带外口线连接好相应端口。

10.7.1 远程升级方法

适用场景

所有板卡在位且正常运行，此时通过网管命令远程升级。

升级前须知

- CN12800 支持整包自动升级，即如果主用主控盘 MPU 存在整包并稳定运行，插入的所有卡都将被自动刷新成该整包中的相应分包版本。
- 在设备上已存在升级好整包版本并生效的主控盘，只需要升级新插入单盘的场景中，插入新单盘会被自动升级并自动重启生效，无需手动升级和手动重启该单盘，在该单盘自动重启上线后，检查单盘版本信息即可。

升级步骤

1. 启动 CN12800 设备，输入命令 **interface mgt-eth 0/0/0** 进入带外口配置视图后，再输入命令 **ip address 192.168.1.200/24** 配置交换机 IP 地址（此地址与 PC 网卡配置的 IP 地址属于同一网段即可）。

```
CN12800(config)#interface mgt-eth 0/0/0
CN12800(config-mgt-eth-0/0/0)#no shutdown
CN12800(config-mgt-eth-0/0/0)#ip address 192.168.1.100/24
```

2. 输入命令 **exit** 退出带外口配置视图。
3. 输入命令 **ping 192.168.1.200** 查看交换机与 PC 是否能够互通。
4. 配置 FTP 服务器，设置好文件路径，用户名（123），密码（123）。
5. 将 CN12800_OS_V370R240.squ 文件放置到 FTP 软件配置的路径下。
6. 进入全局配置视图，使用用户名 123 密码 123 登录 192.168.1.200 服务器，并从该 FTP 服务器上下载名为 CN12800_OS_V370R240.squ 的文件保存到本地设备上。

```
CN12800(config)#ftp get 192.168.1.200 123 123 CN12800_OS_V370R240.squ localfile CN12800_OS_V370R240.squ
Getting File “CN12800_OS_V370R240.squ ” from 192.168.1.200…
 643607522  bytes downloaded.
 If you want to upgrade system,use “upgrade” command!
CN12800(config)#
```

7. 输入命令 **upgrade os file CN12800_OS_V370R240.squ** 进行交换机版本升级。

```
CN12800(config)#upgrade os file CN12800_OS_V370R240.squ
  This operation will upgrade system file.Are you sure?(y/n) [y]y
  System now is upgrading,please wait...
 Putting data...
  %Transmission success.

Upgrading master...
Master upgrading with whole packet...100

 Local path is "/ram/ CN12800_OS_V370R240.squ ".
  Slot            Status
  23              Success
  21              Success
  2               Success
  5               Success
  19              Success
  20              Success
```

```
Upgrading slave...
Slave upgrading with whole packet...100
  Slot              Status
  24                Success
CN12800(config)#
```

8. 显示所有卡都升级成功后，使用 **reboot** 命令重启设备。

```
CN12800(config)#reboot
    WARNING:System will reboot! Continue?(y/n) [y]y
```

10.7.2 业务验证

1. 升级版本后，设备能正常启动。
2. 正常启动后，登录设备，使用命令 **show upgrade card-packet info** 查看版本信息是否正确，主要观察 Build time 与升级时间是否一致。

```
CN12800(config)#show upgrade card-packet info
Card packet information over local mpu :
    Card slot                :23
        Packet status            :Success
        Packet information       :
          Card type              :01000102
          Packet name            :CN12800_MPU_OS_666.squ
          Build time             :2022-06-22-09:40:50
        Card slot                :20
        Packet status            :Success
        Packet information       :
          Card type              :01000302
          Packet name            :CN12800_SFU_OS_666.squ
          Build time             :2022-06-22-09:40:50
        Card slot                :5
        Packet status            :Success
        Packet information       :
          Card type              :01000202
          Packet name            :CN12800_LPU_OS_666.squ
          Build time             :2022-06-22-09:40:50
        Card slot                :2
        Packet status            :Success
```

```
        Packet information      :
          Card type             :01000202
          Packet name           :CN12800_LPU_OS_666.squ
          Build time            :2022-06-22-09:40:50
        Card slot               :19
        Packet status           :Success
        Packet information      :
          Card type             :01000302
          Packet name           :CN12800_SFU_OS_666.squ
          Build time            :2022-06-22-09:40:50
        Card slot               :21
        Packet status           :Success
        Packet information      :
          Card type             :01000302
          Packet name           :CN12800_SFU_OS_666.squ
          Build time            :2022-06-22-09:40:50
    Card packet information over peer mpu:
        Card slot               :24
        Packet status           :Success
        Packet information      :
          Card type             :01000102
          Packet name           :CN12800_MPU_OS_666.squ
          Build time            :2022-06-22-09:
```

10.7.3 升级回退

如果要回退版本，按照上面的升级操作，通过远程升级或本地升级方法，重新升级为原始软件版本即可。

第11章 VPN 配置

本章介绍了 CN12800 中 VPN 隧道管理的基本内容、配置过程和配置举例。

11.1 L3VPN 配置

11.1.1 L3VPN 简介

协议介绍

MPLS L3VPN 是服务提供商 VPN 解决方案中一种基于 PE 的 L3VPN 技术，它使用 BGP 在服务提供商骨干网上发布 VPN 路由，使用 MPLS 在服务提供商骨干网上转发 VPN 报文。MPLS L3VPN 组网方式灵活、可扩展性好，并能够方便地支持 MPLS QoS 和 MPLS TE。

MPLS L3VPN 模块当前最新版本为 1.0。

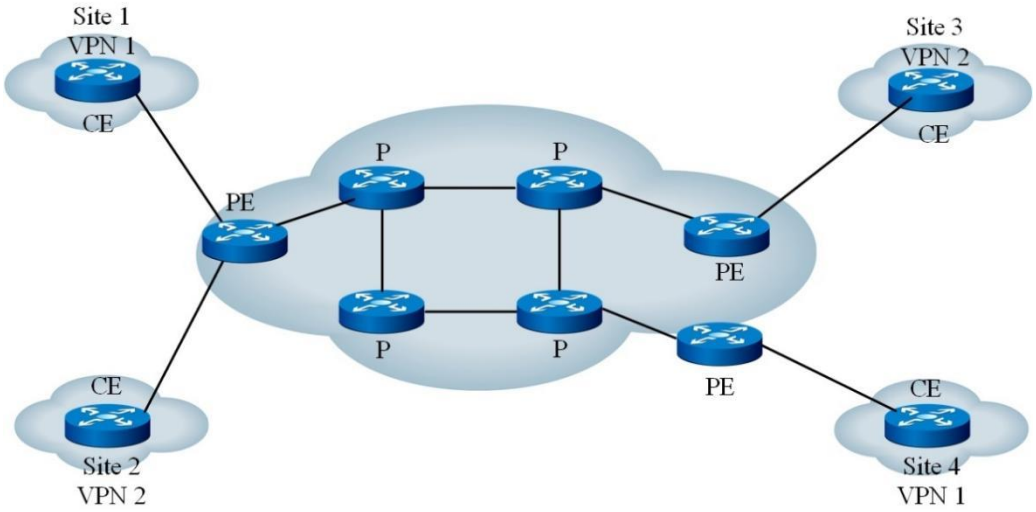


图 11-1 MPLS L3VPN 组网

MPLS L3VPN 组网方案示意图如图 11-1。MPLS L3VPN 模型由三部分组成：CE、PE 和 P。

- CE（Customer Edge）设备：用户网络边缘设备，有接口直接与 SP（Service Provider，服务提供商）相连。CE 可以是路由器或交换机，也可以是一台主机。CE“感知”不到 VPN 的存在，也不需要必须支持 MPLS。

- PE（Provider Edge）路由器：服务提供商边缘路由器，是服务提供商网络的边缘设备，与用户的 CE 直接相连。在 MPLS 网络中，对 VPN 的所有处理都发生在 PE 上。
- P（Provider）路由器：服务提供商网络中的骨干路由器，不与 CE 直接相连。P 设备只需要具备基本 MPLS 转发能力。

CE 和 PE 的划分主要是根据 SP 与用户的管理范围，CE 和 PE 是两者管理范围的边界。

CE 设备通常是一台路由器，当 CE 与直接相连的 PE 建立邻接关系后，CE 把本站点的 VPN 路由发布给 PE，并从 PE 学到远端 VPN 的路由。CE 与 PE 之间使用 BGP/IGP 交换路由信息，也可以使用静态路由。

PE 从 CE 学到 CE 本地的 VPN 路由信息后，通过 BGP 与其它 PE 交换 VPN 路由信息。PE 路由器只维护与它直接相连的 VPN 的路由信息，不维护服务提供商网络中的所有 VPN 路由。

P 路由器只维护到 PE 的路由，不需要了解任何 VPN 路由信息。

当在 MPLS 骨干网上传输 VPN 流量时，入口 PE 做为 Ingress LSR（Label Switch Router，标签交换路由器），出口 PE 做为 Egress LSR，P 路由器则做为 Transit LSR。

报文转发

在基本 MPLS L3VPN 应用中（不包括跨域的情况），VPN 报文转发采用两层标签方式：

- 第一层（外层）标签在骨干网内部进行交换，指示从 PE 到对端 PE 的一条 LSP。VPN 报文利用这层标签，可以沿 LSP 到达对端 PE；
- 第二层（内层）标签在从对端 PE 到达 CE 时使用，指示报文应被送到哪个 Site，或者更具体一些，到达哪一个 CE。这样，对端 PE 根据内层标签可以找到转发报文的接口。

特殊情况下，属于同一个 VPN 的两个 Site 连接到同一个 PE，这种情况下只需要知道如何到达对端 CE。

以图 11-2 为例，说明 VPN 报文的转发：

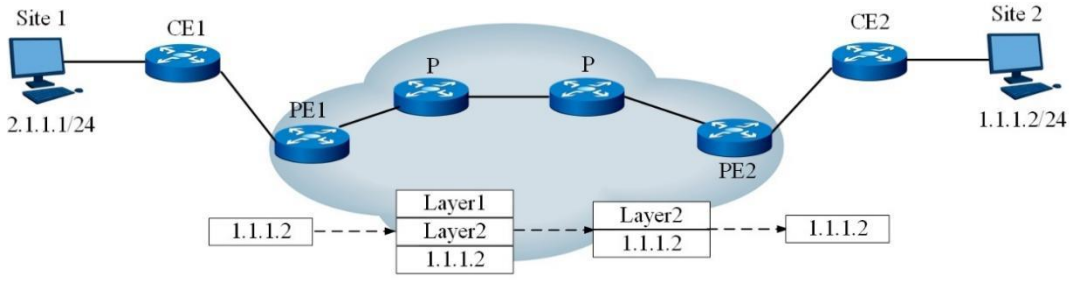


图 11-2 VPN 报文转发示意图

1) Site 1 发出一个目的地址为 1.1.1.2 的 IP 报文，由 CE 1 将报文发送至 PE 1。

2) PE 1 根据报文到达的接口及目的地址查找 VPN 实例表项，匹配后将报文转发出去，同时打上内层和外层两个标签。

3) MPLS 网络利用报文的外层标签，将报文传送到 PE 2（报文在到达 PE 2 前一跳时已经被剥离外层标签，仅含内层标签）。

4) PE 2 根据内层标签和目的地址查找 VPN 实例表项，确定报文的出接口，将报文转发至 CE 2。

5) CE 2 根据正常的 IP 转发过程将报文传送到目的地。

路由信息发布

在基本 MPLS L3VPN 组网中，VPN 路由信息的发布涉及 CE 和 PE，P 路由器只维护骨干网的路由，不需要了解任何 VPN 路由信息。PE 路由器也只维护与它直接相连的 VPN 的路由信息，不维护所有 VPN 路由。因此，MPLS L3VPN 网络具有良好的可扩展性。

VPN 路由信息的发布过程包括三部分：本地 CE 到入口 PE、入口 PE 到出口 PE、出口 PE 到远端 CE。完成这三部分后，本地 CE 与远端 CE 之间将建立可达路由，VPN 私网路由信息能够在骨干网上发布。

下面分别对这三部分进行介绍。

1) 本地 CE 到入口 PE 的路由信息交换

CE 与直接相连的 PE 建立邻接关系后，把本站点的 VPN 路由发布给 PE。

CE 与 PE 之间可以使用静态路由、RIP、OSPF、IS-IS 或 EBGP。无论使用哪种路由协议，CE 发布给 PE 的都是标准的 IPv4 路由。

2) 入口 PE 到出口 PE 的路由信息交换

PE 从 CE 学到 VPN 路由信息后，为这些标准 IPv4 路由增加 RD 和 VPN Target 属性，形成 VPN-IPv4 路由，存放到为 CE 创建的 VPN 实例中。

3) 出口 PE 到远端 CE 的路由信息交换

远端 CE 有多种方式可以从出口 PE 学习 VPN 路由，包括静态路由、RIP、OSPF、IS-IS 和 EBGP，与本地 CE 到入口 PE 的路由信息交换相同。

11.1.2 L3VPN 配置

MPLS L3VPN 由运营商经营 MPLS VPN 骨干网，通过 PE 设备提供 VPN 服务。VPN 用户通过 CE 设备与运营商的 PE 设备互连，接入 MPLS VPN 网络，实现属于用户 VPN 的不同 Site 之间的通信。MPLS L3VPN 的基本配置步骤如下：

1. 在 P 网络中配置 IGP 协议，及部署 MPLS LDP
2. 在 PE 上为 VPN 客户创建 VRF 及指定 RD，及 RT 的导入导出策略
3. 在 PE 上启用 MP-BGP，并建立 VPNV4 邻居
4. 运行 PE-CE 路由选择协议
5. 将 PE-CE 协议相互重发布

MPLS L3VPN 模块实现上述第二步骤，即 MPLS L3VPN 的 VPN 实例配置的相关内容。

11.1.2.1 创建 VPN 实例

目的

创建一条 VPN 实例并进入 VPN 实例视图。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
创建 VPN 实例	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **ip vpn-instance** *name* 创建一条 VPN 实例。
删除 VPN 实例	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **no ip vpn-instance** *name* 删除一条指定实例名的 VPN 实例。

11.1.2.2 配置 RD

目的

配置路由标识（RD，Route Distinguisher）。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置 VPN 实例的 Route Distinguisher	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **ip vpn-instance** *name* 创建一条 VPN 实例并进入 VPN 实例配置视图；

目的	步骤
（RD，路由标识）	3. 执行命令 **ipv4-family** 或 **ipv6-family** 命令进入 vpn-instance-af-ipv4 或 vpn-instance-af-ipv6 配置视图； 4. 执行命令 **route-distinguisher** *rd-string* 配置 VPN 实例的 Route Distinguisher。

 **注意：**

路由标识没有缺省值，必须在创建 VPN 实例时配置。

11.1.2.3 配置 VPN Target

目的

配置 VPN Target。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置 VPN Target	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **ip vpn-instance** *name* 创建一条 VPN 实例并进入 VPN 实例配置视图； 3. 执行命令 **ipv4-family** 或 **ipv6-family** 命令进入 vpn-instance-af-ipv4 或 vpn-instance-af-ipv6 配置视图； 4. 执行命令 **vpn-target** *target* { **both** | **export-extcommunity** | **import-extcommunity** }。
删除当前 VPN 实例关联的所有 VPN target	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **ip vpn-instance** *name* 创建一条 VPN 实例并进入 VPN 实例配置视图； 3. 执行命令 **ipv4-family** 或 **ipv6-family** 命令进入 vpn-instance-af-ipv4 或 vpn-instance-af-ipv6 配置视图； 4. 执行命令 **no vpn-target**。
删除指定的 VPN Target	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **ip vpn-instance** *name* 创建一条 VPN 实例并进入 VPN 实例配置视图； 3. 执行命令 **ipv4-family** 或 **ipv6-family** 命令进入 vpn-instance-af-ipv4 或 vpn-instance-af-ipv6 配置视图；

目的	步骤
	4. 执行命令 **no vpn-target** *target* { **both** | **export-extcommunity** | **import-extcommunity** }。

 **注意：**

VPN Target 没有缺省值，必须在创建 VPN 实例时配置。

11.1.2.4 配置 VPN 实例的描述信息

目的

配置 VPN 实例的描述信息。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置 VPN 实例的描述信息	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **ip vpn-instance** *name* 创建一条 VPN 实例并进入 VPN 实例配置视图； 3. 执行命令 **description** *description*。
删除 VPN 实例的描述信息	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **ip vpn-instance** *name* 创建一条 VPN 实例并进入 VPN 实例配置视图； 3. 执行命令 **no description**。

11.1.2.5 配置接口与指定 VPN 实例绑定

目的

配置接口与指定 VPN 实例绑定。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
配置接口与指定 VPN 实例绑定	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令进入 VLANIF 配置视图、Loopback 接口配置视图、BD 配置视图； 3. 执行命令 **ip binding vpn-instance** *name*。

目的	步骤
取消接口与 VPN 实例的绑定	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令进入 VLANIF 配置视图、Loopback 接口配置视图、BD 配置视图； 3. 执行命令 **no ip binding vpn-instance** *name*。

 **注意：**

1 执行 **ip binding vpn-instance** 命令将删除接口上已经配置的 IP 地址、路由协议等三层特性，如果需要应重新配置。

2 同一个接口不能既作为 L2VPN 的 AC 接口又作为 L3VPN 的 AC 接口。当某个接口绑定 L2VPN 后，该接口上配置的 IP 地址、路由协议等三层特性会全部变为无效。

3 配置 VPN 实例后，需要将本设备上属于该 VPN 的接口与该 VPN 实例关联，否则该接口将属于公网接口。

4 在接口上取消已建立的关联将清除该接口的 IP 地址、路由协议等三层特性，如果需要应重新配置。

11.1.3 维护及调试

目的

当 MPLS L3VPN 功能不正常，需要进行查看、调试或定位问题时，可以使用本小节操作。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
显示 VPN 实例配置情况	1. 不执行任何命令保持当前特权用户视图，或执行命令 **configure** 进入全局配置视图；或在全局配置视图下执行命令 **ip vpn-instance** *name* 进入 VPN 实例配置视图； 2. 执行命令 **show ip vpn-instance**。
显示 VPN 实例详细信息	1. 不执行任何命令保持当前特权用户视图，或执行命令 **configure** 进入全局配置视图；或在全局配置视图下执行命令 **ip vpn-instance** *name* 进入 VPN 实例配置视图； 2. 执行如下命令： ● **show ip vpn-instance verbose**； ● **show ip vpn-instance** *vpn-instance-name* **verbose**。

目的	步骤
显示 VPN 实例配置信息	1. 不执行任何命令保持当前特权用户视图，或执行命令 **configure** 进入全局配置视图；或在全局配置视图下执行命令 **ip vpn-instance** *name* 进入 VPN 实例配置视图； 2. 执行命令 **show ip vpn-instance config**。
显示具备指定入口 vpn target 属性的 VPN 实例	1. 不执行任何命令保持当前特权用户视图，或执行命令 **configure** 进入全局配置视图；或在全局配置视图下执行命令 **ip vpn-instance** *name* 进入 VPN 实例配置视图； 2. 执行命令 **show ip vpn-instance import-vt** *target*。
显示引入路由的信息	1. 执行命令进入普通用户视图； 2. 执行如下命令： ● **show import-route** { **all** | **imported** }； ● **show import-route vpn-instance** *name* { **all** | **imported** }。
打开 L3VPN 调试功能	1. 不执行任何命令保持当前特权用户视图，或执行命令 **configure** 进入全局配置视图；或在全局配置视图下执行命令 **ip vpn-instance** *name* 进入 VPN 实例配置视图； 2. 执行命令 **debug l3vpn** { **io** | **event** | **error** | **nm** | **route** | **all** }。
关闭 L3VPN 调试功能	1. 不执行任何命令保持当前特权用户视图，或执行命令 **configure** 进入全局配置视图；或在全局配置视图下执行命令 **ip vpn-instance** *name* 进入 VPN 实例配置视图； 2. 执行命令 **no debug l3vpn** { **io** | **event** | **error** | **nm** | **route** | **all** }。
在 VPN 实例内强制引入公网路由	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **router bgp** 进入 BGP 配置视图； 3. 执行命令 **ipv4-family unicast** 进入 BGP-IPv4 地址族配置视图或 **ipv6-family unicast** 进入 BGP-IPv6 地址族配置视图或 **ipv4-family vpn-instance** *name* 进入 BGP-VPN IPv4 地址族配置视图或 **ipv6-family vpn-instance** *name* 进入 BGP-VPN IPv6 地址族配置视图； 4. 执行以下命令： ● **import-rib public**； ● **import-rib public route-policy** *policy-name*； ● **no import-rib public**。
在 VPN 实例或公网实例内强制引入其他 VRF 实例路由	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **router bgp** 进入 BGP 配置视图； 3. 执行命令 **ipv4-family unicast** 进入 BGP-IPv4 地址族配置视图或 **ipv6-family unicast** 进入 BGP-IPv6 地址族配置视图或 **ipv4-family vpn-instance** *name* 进入 BGP-VPN IPv4 地址族配置视图或 **ipv6-family vpn-instance** *name* 进入 BGP-VPN IPv6 地址族配置视图； 4. 执行以下命令： ● **import-rib vpn-instance** *vpn-instance-name*； ● **import-rib vpn-instance** *vpn-instance-name* **route-policy** *policy-name*；

目的	步骤
	● **no import-rib vpn-instance** *vpn-instance-name*。
在公网下引入（静态路由、IS-IS 路由、OSPF 路由或直连路由）协议	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **ip vpn-instance** *name* 创建一条 VPN 实例并进入 VPN 实例配置视图； 3. 执行命令 **ipv4-family** 或 **ipv6-family** 命令进入 vpn-instance-af-ipv4 或 vpn-instance-af-ipv6 配置视图； 4. 执行以下命令： ● **import-rib public protocol** { **static | isis | ospf | direct** }； ● **import-rib public protocol** { **static | isis | ospf | direct** } **route-policy** *policy-name*； ● **import-rib vpn-instance** *vpn-instance-name* **protocol** { **static | isis | ospf | direct** }； ● **import-rib vpn-instance** *vpn-instance-name* **protocol** { **static | isis | ospf | direct** } **route-policy** *policy-name*； ● **no import-rib public protocol** { **static | isis | ospf | direct** }； ● **no import-rib vpn-instance** *vpn-instance-name* **protocol** { **static | isis | ospf | direct** }。
引入（静态路由、IS-IS 路由、OSPF 路由或直连路由）协议的 VPN 实例	1. 执行命令 **configure** 进入全局配置视图； 2. 执行以下命令： ● **ip import-rib vpn-instance** *vpn-instance-name* **protocol** { **static | isis | ospf | direct** }； ● **ip import-rib vpn-instance** *vpn-instance-name* **protocol** { **static | isis | ospf | direct** } **route-policy** *policy-name*； ● **ipv6 import-rib vpn-instance** *vpn-instance-name* **protocol** { **static | isis | ospf | direct** }； ● **ipv6 import-rib vpn-instance** *vpn-instance-name* **protocol** { **static | isis | ospf | direct** } **route-policy** *policy-name*； ● **no ip import-rib vpn-instance** *vpn-instance-name* **protocol** { **static | isis | ospf | direct** }； ● **no ipv6 import-rib vpn-instance** *vpn-instance-name* **protocol** { **static | isis | ospf | direct** }。
使能或去使能 L3VPN 告警功能	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **ip vpn-instance snmp-trap** { **enable** | **disable** }，使能或去使能 L3VPN 告警功能。

第12章 数据中心特性配置

本章主要介绍 VXLAN 的的基本内容、配置过程和配置举例。

12.1 VXLAN 配置

12.1.1 VXLAN 概述

传统数据中心网络的种种限制，推动了新技术的产生，在 VMware、Cisco 等全球知名厂商的共同推动下，VXLAN 登场了。

VXLAN（Virtual eXtensible Local Area Network，虚拟扩展局域网），是由 IETF 定义的 NVO3（Network Virtualization over Layer 3）标准技术之一，采用 L2 over L4（MAC-in-UDP）的报文封装模式，将二层报文用三层协议进行封装，可实现二层网络在三层范围内进行扩展，同时满足数据中心大二层虚拟迁移和多租户的需求。

12.1.1.1 VXLAN 网络模型

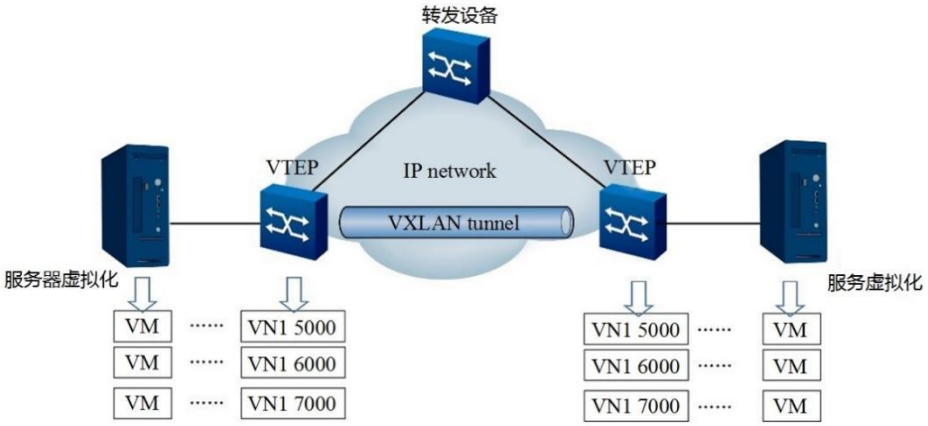


图 12-1 VXLAN 网络模型

如图 12-1 所示可以发现，VXLAN 网络中出现了以下传统数据中心网络中没有的新元素：

- VTEP（VXLAN Tunnel Endpoints，VXLAN 隧道端点）

VXLAN 网络的边缘设备，是 VXLAN 隧道的起点和终点，VXLAN 报文的相关处理均在这上面进行。VTEP 既可以是一个独立的网络设备，也可以是虚拟机所在的服务器。

- VNI（VXLAN Network Identifier，VXLAN 网络标识符）

以太网数据帧中 VLAN 只占了 12 比特的空间，这使得 VLAN 的隔离能力在数据中心网络中力不从心。而 VNI 的出现，就是专门解决这个问题的。VNI 是一种类似于 VLAN ID 的用户标示，一个 VNI 代表了一个租户，属于不同 VNI 的虚拟机之间不能直接进行二层通信。VXLAN 报文封装时，给 VNI 分配了足够的空间使其可以支持海量租户的隔离。详细的实现，我们将在后文中介绍。

- VXLAN 隧道

“隧道”是一个逻辑上的概念，它并不新鲜，比如大家熟悉的 GRE。就是将原始报文“变身”下，加以“包装”，好让它可以在承载网络（比如 IP 网络）上传输。从主机的角度看，就好像原始报文的起点和终点之间，有一条直通的链路一样。而这个看起来直通的链路，就是“隧道”。顾名思义，“VXLAN 隧道”便是用来传输经过 VXLAN 封装的报文的，它是建立在两个 VTEP 之间的一条虚拟通道。

12.1.1.2 VXLAN 数据封装格式

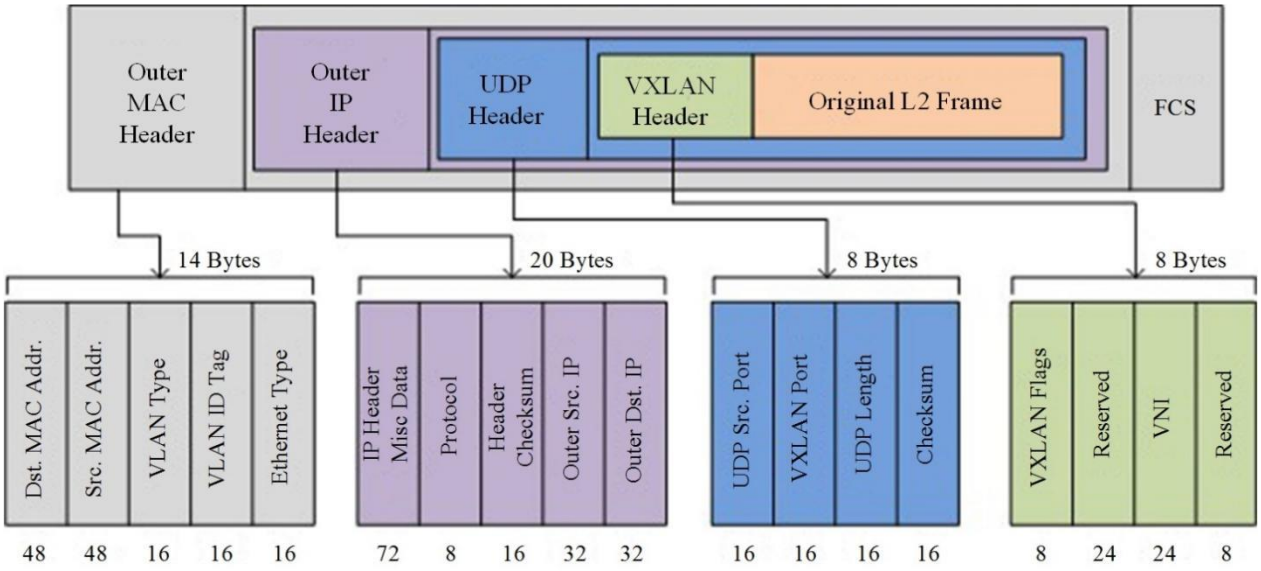


图 12-2 VXLAN 数据封装格式

如图 12-2 所示，VXLAN 是 mac in udp 的封装模式，在 VTEP 入口将原始数据报文封装好特定 VXLAN 头部后再通过 VXLAN 隧道传递到对端 VTEP，解封装（剥去头）后发送到目标机。

- VXLAN Header

增加 VXLAN 头（8 字节），其中包含 24 比特的 VNI 字段，用来定义 VXLAN 网络中不同的租户。此外，还包含 VXLAN Flags（8 比特，取值为 00001000）和两个保留字段（分别为 24 比特和 8 比特）。

- UDP Header

VXLAN 头和原始以太帧一起作为 UDP 的数据。UDP 头中，目的端口号（VXLAN Port）固定为 4789，源端口号（UDP Src. Port）是原始以太帧通过哈希算法计算后的值。

- Outer IP Header

封装外层 IP 头。其中，源 IP 地址（Outer Src. IP）为源 VM 所属 VTEP 的 IP 地址，目的 IP 地址（Outer Dst. IP）为目的 VM 所属 VTEP 的 IP 地址。

- Outer MAC Header

封装外层以太头。其中，源 MAC 地址（Src. MAC Addr.）为源 VM 所属 VTEP 的 MAC 地址，目的 MAC 地址（Dst. MAC Addr.）为到达目的 VTEP 的路径上下一跳设备的 MAC 地址。

12.1.1.3 VXLAN 报文转发机制

建立 VXLAN 隧道

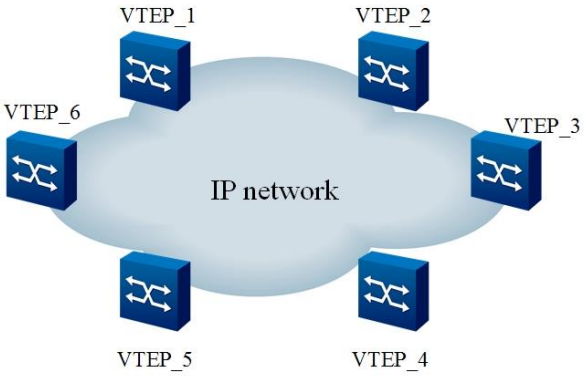


图 12-3 建立 VXLAN 隧道示意图

如图 12-3 所示，网络中存在多个 VTEP，那么这其中哪些 VTEP 间需要建立 VXLAN 隧道呢？我们知道，通过 VXLAN 隧道，“二层域”可以突破物理上的界限，实现大二层网络中 VM 之间的通信。所以，连接在不同 VTEP 上的 VM 之间如果有“大二层”互通的需求，这两个 VTEP 之间就需要建立 VXLAN 隧道。换言之，同一大二层域内的 VTEP 之间都需要建立 VXLAN 隧道。

例如，假设图 12-3 中 VTEP_1 连接的 VM、VTEP_2 连接的 VM 以及 VTEP_3 连接的 VM 之间需要“大二层”互通，那 VTEP_1、VTEP_2 和 VTEP_3 之间就需要两两建立 VXLAN 隧道，如图 12-4 所示。

“同一大二层域”，就类似于传统网络中 VLAN（虚拟局域网）的概念，只不过在 VXLAN 网络中，叫做 Bridge-Domain，简称 BD。

我们知道，不同的 VLAN 是通过 VLAN ID 来进行区分的，那不同的 BD 是如何进行区分的呢？其实前面已经提到了，就是通过 VNI 来区分的。对于数据中心交换机来说，BD 与 VNI 是 1：1 的映射关系，这种映射关系是通过在 VTEP 上配置命令行建立起来的。VTEP 会根据以上配置生成 BD 与 VNI 的映射关系表

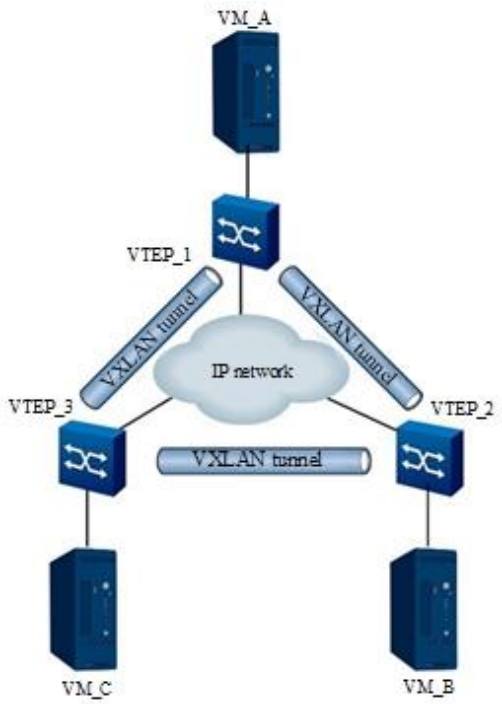


图 12-4 VXLAN 隧道建立示意图

进入 VXLAN 隧道的报文

并非所有进入到交换机的报文都会走 VXLAN 隧道（也可能报文就是走普通的二三层转发流程）。传统网络中定义了三种不同类型的接口：Access、Trunk、Hybrid。这三种类型的接口虽然应用场景不同，但他们的最终目的是一样的：一是根据配置来检查哪些报文是允许通过的；二是判断对检查通过的报文是怎样的处理。

在 VXLAN 网络中，VTEP 上的接口也承担着类似的任务，只不过在数据中心交换机中，这里的接口不是物理接口，而是一个叫做“二层子接口”的逻辑接口。二层子接口主要做两件事：一是根据配置来检查哪些报文需要进入 VXLAN 隧道；二是判断对检查通过的报文做怎样的处理。

流封装类型	允许进入 VXLAN 隧道的报文类型	报文进行封装前的处理	收到 VXLAN 报文并解封装后的处理
dot1q	只允许携带指定 VLAN Tag 的报文进入 VXLAN 隧道。（这里的“指定 VLAN Tag”是通过命令进行配置的）	先剥掉原始报文的外层 VLAN Tag。	若内层原始报文带有 VLAN Tag，则先将该 VLAN Tag 替换为指定的 VLAN Tag，再转发；若内层原始报文不带 VLAN Tag，则先将其添加指定的 VLAN Tag，再转发。
untag	只允许不携带 VLAN Tag 的报文进入 VXLAN 隧道。	不对原始报文处理，即不添加任何 VLAN Tag。	不对原始报文处理，即不添加/不替换/不剥掉任何 VLAN Tag。
default	允许所有报文进入 VXLAN 隧道，不论报文是否携带 VLAN Tag。	不对原始报文做处理，即不添加/不替换/不剥掉任何 VLAN Tag。	不对原始报做任何处理，即不添加/不替换/不剥掉任何 VLAN Tag。

只要将二层子接口加入指定的 BD，然后根据二层子接口上的配置，就可以确定报文属于哪个 BD。default 类型的子接口，一般应用在经过此接口的报文均需要走同一条 VXLAN 隧道的场景，即下挂的 VM 全部属于同一 BD。当经过同一物理接口的报文既有带 VLAN Tag 的，又有不带 VLAN Tag 的，并且他们各自要进入不同的 VXLAN 隧道，则可以在该物理接口上同时创建 dot1q 和 untag 类型的二层子接口。

12.1.2 配置 VXLAN

目的

本节介绍如何配置 VXLAN。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
创建并进入 BD（Bridge Domain）视图	1. 执行命令 **configure**； 2. 执行命令 **bridge-domain** *bd-id*。
删除 BD	1. 执行命令 **configure**；

目的	步骤
	2. 执行命令 **no bridge-domain** *bd-id*。
创建并进入三层 BD 接口配置视图	1. 执行命令 **configure**； 2. 执行命令 **interface bridge-domain** *bd-id*。
配置 BD 绑定 VNI	1. 执行命令 **configure**； 2. 执行命令 **bridge-domain** *bd-id*； 3. 执行命令 **vxlan vni** *vni-id*。
删除 BD 绑定的 VNI	1. 执行命令 **configure**； 2. 执行命令 **bridge-domain** *bd-id*； 3. 执行命令 **no vxlan vni**。
配置关联 BD 的映射 VNI，并指定该映射 VNI 所属的水平分割组	1. 执行命令 **configure**； 2. 执行命令 **bridge-domain** *bd-id*； 3. 执行命令 **vxlan vni** *vni-id* **split-group** *split-group-name*。
删除关联 BD 的映射 VNI 配置	1. 执行命令 **configure**； 2. 执行命令 **bridge-domain** *bd-id*； 3. 执行命令 **no vxlan vni** *vni-id* **split-group**。
配置子接口绑定的 BD	1. 执行命令 **configure**； 2. 执行命令 **interface { ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number.subinterface-number*； 3. 执行命令 **bridge-domain bind** *bd-id*。
删除子接口绑定的 BD	1. 执行命令 **configure**； 2. 执行命令 **interface { ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number.subinterface-number*； 3. 执行命令 **no bridge-domain bind**。
配置子接口的封装模式	1. 执行命令 **configure**； 2. 执行命令 **interface { ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number.subinterface-number*； 3. 执行命令 **encapsulation { dot1q | untag | qinq |default }**。
配置子接口 Dot1q 封装模式的 VLAN	1. 执行命令 **configure**； 2. 执行命令 **interface { ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number.subinterface-number*； 3. 执行命令 **encapsulation dot1q** *vlan-id*。
删除子接口 Dot1q 封装模式的 VLAN	1. 执行命令 **configure**；

目的	步骤
	2. 执行命令 **interface { ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number.subinterface-number*； 3. 执行命令 **no encapsulation dot1q** *vlan-id*。
配置子接口 Dot1q 封装模式的双层 VLAN	1. 执行命令 **configure**； 2. 执行命令 **interface { ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number.subinterface-number*； 3. 执行命令 **encapsulation qinq** *vlan1-id* **ce-vid** *vlan2-id*。
删除配置子接口 Dot1q 封装模式的双层 VLAN	1. 执行命令 **configure**； 2. 执行命令 **interface { ethernet | gigaethernet | xgigaethernet| 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet }** *interface-number.subinterface-number*； 3. 执行命令 **no encapsulation qinq** *vlan1-id* **ce-vid** *vlan2-id*。
创建并进入 NVE 视图	1. 执行命令 **configure**； 2. 执行命令 **interface nve** *nve-id*。
删除 NVE 视图	1. 执行命令 **configure**； 2. 执行命令 **no interface nve** *nve-id*。
配置隧道的 VNI 以及对端 IP	1. 执行命令 **configure**； 2. 执行命令 **interface nve** *nve-id*； 3. 执行命令 **vni** *id* **ucast-peer** *peer-ip-address*。
删除 NVE 接口下所有的 peer（不同 VNI 的都删除）	1. 执行命令 **configure**； 2. 执行命令 **interface nve** *nve-id*； 3. 执行命令 **no vni** *id* **peer**。
删除指定 VNI 和 IP 的隧道	1. 执行命令 **configure**； 2. 执行命令 **interface nve** *nve-id*； 3. 执行命令 **no vni** *id* **ucast-peer** *peer-ip-address*。
配置隧道的源 IP 地址	1. 执行命令 **configure**； 2. 执行命令 **interface nve** *nve-id*； 3. 执行命令 **tunnel source** *ip-address*。
删除隧道的源 IP 地址	1. 执行命令 **configure**； 2. 执行命令 **interface nve** *nve-id*； 3. 执行命令 **no tunnel source**。
配置 BD 接口下未知单播包的处理方式是转发还是丢弃	1. 执行命令 **configure**； 2. 执行命令 **bridge-domain** *bd-id*； 3. 执行命令 **unknown-ucast { forward | drop }**。

12.1.3 配置 GRPC 日志

目的

本节介绍如何配置 GRPC 日志。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
开启/关闭 GRPC 日志	1. 执行命令 **configure**； 2. 执行命令 **debug grpc** { **api** | **cares_address_sorting** | **cares_resolver** | **client_channel_call** | **client_channel_routing** | **http** | **http_keepalive** | **chttp2_refcount** | **channel** | **combiner** | **tcp** | **polling** | **fd_trace** | **fd_refcount** | **polling_api** | **executor** | **timer** | **timer_check**|**op_failure** | **pending_tags** | **cq_refcount** | **queue_pluck** | **connectivity_state** | **resource_quota** | **all** } { **on** | **off** }。
设置 GRPC 的调试等级	1. 执行命令 **configure**； 2. 执行命令 **grpc debug-level** { **debug** | **info** | **error** | **none** }。

12.1.4 维护及调试

目的

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

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
打开或者关闭 VXLAN 的调试功能	1. 不执行任何命令保持当前特权用户视图； 2. 执行命令 **debug vxlan** { **event** | **detect** | **did** | **hw** | **off** | **all** }。
显示 bd 的相关信息	1. 执行命令进入普通用户视图、特权用户视图、全局配置视图； 2. 执行如下命令： ● **show bridge-domain** 显示已配置的所有二层 BD 接口的信息，可显示 bd 接口号、绑定的 vni、未知单播配置、统计是否使能、绑定的子接口等； ● **show bridge-domain** *domain-id* 显示指定二层 BD 接口的配置信息。
显示 vni 的相关信息	1. 执行命令进入特权用户视图、全局配置视图； 2. 执行命令 **show vxlan vni**。
显示 VXLAN 资源信息	1. 执行命令进入特权用户视图、全局配置视图； 2. 执行命令 **show vxlan resourse**。

目的	步骤
显示指定槽位下 VXLAN 错误统计信息	1. 执行命令进入特权用户视图、全局配置视图； 2. 执行命令 **show vxlan error slot** *slot-id*。
显示 nve peer 信息或者详细信息	1. 执行命令进入普通用户视图、特权用户视图、全局配置视图； 2. 执行命令 **show nve peer** 或者 **show nve peer verbose**。
显示 interface nve 信息	1. 执行命令进入普通用户视图、特权用户视图、全局配置视图； 2. 执行命令 **show interface nve**。
显示 bd 接口的引用计数	1. 执行命令进入普通用户视图； 2. 执行命令 **show l3int bridge-domain** *domain-id*。
显示指定条件下的 L2vxlan 转发路径	1. 执行命令进入普通用户视图； 2. 执行命令 **show hwvxlan l2int { ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* **vlan** *vlan-id* **destmac** *mac-address* **slot** *slot-id*。
显示指定条件下的 L3vxlan 转发路径	1. 执行命令进入普通用户视图； 2. 执行如下命令： ● **show hwvxlan l3int { ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* **vlan** *vlan-id* **destip4** *ipv4-address/M* **slot** *slot-id* ● **show hwvxlan l3int { ethernet | gigaethernet | xgigaethernet | 10gigaethernet | 25gigaethernet | 40gigaethernet | 100gigaethernet** } *interface-number* **vlan** *vlan-id* **destip6** *ipv6-address/M* **slot** *slot-id*。

12.1.5 配置举例

12.1.5.1 同网段用户通过 VXLAN 隧道互通典型场景（静态隧道）

组网需求

如图 12-5 所示，PC1 和 PC3 同网段，通过 VTEP1 和 VTEP2 间的 VXLAN 隧道进行互通。

VTEP1 通过 GE1/0/1 连接 PC1、通过 10GE1/0/2 连接 VTEP2，VTEP2 通过 GE1/01 连接 PC3、10GE1/0/2 连接 VTEP1，VTEP1 和 VTEP2 通过 VLAN 10 三层互通。

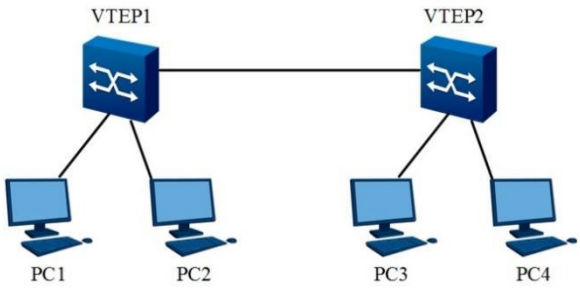


图 12-5 基本 VXLAN 二层互通组网图

配置思路

采用如下的思路配置 VXLAN 二层互通基本功能：

1. 在 VTEP1、VTEP2 间配置三层连接。

2. VTEP1 和 VTEP2 的接入侧配置子接口和 BD 接口绑定关系。

3. VTEP1 和 VTEP2 网络侧配置 NVE 接口及隧道。

数据准备

为完成此配置例，需准备如下的数据：

网络成员间互通的网络接口。

VTEP1 和 VTEP2 连接的三层 VLAN 10，互联 IP 地址 10.18.1.1/24 和 10.18.1.2/24。

VTEP1 接入侧 BD 接口 1 绑定 VNI 100；VTEP2 接入侧 BD 接口 5 绑定 VNI 100；

VTEP1 与 PC1 连接的子接口的接入方式，VLAN 5 untag，绑定 BD 1；VTEP2 与 PC3 连接的子接口接入方式，VLAN 5 untag，绑定 BD 5。

VTEP1 配置网络侧 NVE 接口和隧道 VNI 100、源及目的 IP；VTEP1 配置网络侧 NVE 接口和隧道 VNI 100、源及目的 IP

操作步骤

步骤 1 配置 VTEP1。

#配置 BD 接口。

VTEP1(config)#bridge-domain 1

VTEP1(config-bridge-domain-1)#vxlan vni 100

VTEP1(config-bridge-domain-1)#exit

#配置子接口接入方式，接入侧可根据实际情况配置 tag、untag、qinq 等接入方式。

VTEP1(config)#interface 10gigaethernet 1/0/1.1

VTEP1(config-10ge1/0/1.1)#no shutdown

VTEP1(config-10ge1/0/1.1)#encapsulation untag

VTEP1(config-10ge1/0/1.1)#bridge-domain bind 1

VTEP1(config-10ge1/0/1.1)#exit

#配置与 VTEP2 连接的网络接口。

VTEP1(config)#interface vlan 20

VTEP1(config-vlan-20)#ip address 10.18.1.1 255.255.255.0

VTEP1(config-vlan-20)#exit

VTEP1(config)#interface 10gigaethernet 1/0/2

VTEP1(config-10ge1/0/2)#no shutdown

VTEP1(config-10ge1/0/2)#port hybrid vlan 20 untagged

VTEP1(config-10ge1/0/2)#port hybrid pvid 20

VTEP1(config-10ge1/0/2)#exit

#配置 NVE 接口的 VXLAN 隧道。

VTEP1(config)#interface nve 1

VTEP1(config-nve-1)#tunnel source 10.18.1.1

VTEP1(config-nve-1)#vni 100 ucast-peer 10.18.1.2

VTEP1(config-nve-1)#exit

步骤 2 配置 VTEP2：配置基本与 VTEP1 一样（隧道的源和目的相反）。

#配置 BD 接口。

VTEP2(config)#bridge-domain 5

VTEP2(config-bridge-domain-5)#vxlan vni 100

VTEP2(config-bridge-domain-5)#exit

#配置子接口接入方式。

VTEP2(config)#interface 10gigaethernet 1/0/1.1

VTEP2(config-10ge1/0/1.1)#no shutdown

VTEP2(config-10ge1/0/1.1)#encapsulation untag

VTEP2(config-10ge1/0/1.1)#bridge-domain bind 5

VTEP2(config-10ge1/0/1.1)#exit

#配置与 VTEP1 连接的网络接口。

VTEP2(config)#interface vlan 20

VTEP2(config-vlan-20)#ip address 10.18.1.2 255.255.255.0

VTEP2(config-vlan-20)#exit

VTEP2(config)#interface 10gigaethernet 1/0/2

VTEP2(config-10ge1/0/2)#no shutdown

VTEP2(config-10ge1/0/2)#port hybrid vlan 20 untagged

VTEP2(config-10ge1/0/2)#port hybrid pvid 20

VTEP2(config-10ge1/0/2)#exit

#配置 NVE 接口的 VXLAN 隧道。

VTEP2(config)#interface nve 1

VTEP2(config-nve-1)#tunnel source 10.18.1.2

VTEP2(config-nve-1)#vni 100 ucast-peer 10.18.1.1

VTEP2(config-nve-1)#exit

步骤 3：调试 VXLAN 功能。

配置好 VTEP1 和 VTEP2 之后，从 PC1 ping PC3，看是否能 ping 通，不能 ping 通则在 VTEP1 和 VTEP2 上查看 MAC 地址表，看 VTEP1 上是否有 PC3 的带 VXLAN 隧道的 mac，VTEP2 上是否有 PC1 的 mac，如果没有则看隧道两端是否能 ping 通。

12.1.5.2 不同网段用户通过 VXLAN 隧道互通典型场景（静态隧道）

组网需求

如图 12-6 所示，PC1 和 PC3 不同网段，通过 VTEP1、L3GW、VTEP2 间的 VXLAN 隧道进行互通。

VTEP1 通过 10GE 1/0/1 连接 PC1、通过 10GE1/0/2 连接 L3GW，VTEP2 通过 10GE 1/01 连接 PC3、10GE 1/0/2 连接 L3GW，L3GW 通过 10GE1/0/2 连接 VTEP1、10GE1/0/3 连接 VTEP2。

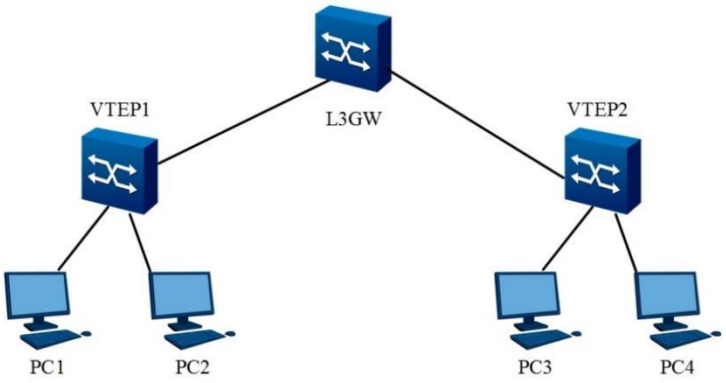


图 12-6 基本 VXLAN 三层互通组网图

配置思路

采用如下的思路配置 VXLAN 三层互通基本功能：

1. 在 VTEP1、L3GW、VTEP2 间配置三层连接，VTEP1、VTEP2 分别和三层网关设备建立 VXLAN 隧道。

2. VTEP1 和 VTEP2 的接入侧配置子接口和 BD 接口绑定关系；VTEP1 和 VTEP2 网络侧配置 NVE 接口及隧道。

L3GW 设备两侧配置 NVE 接口和隧道，配置三层 BD 接口分别作为两侧 PC 的网关。

数据准备

为完成此配置例，需准备如下的数据：

网络成员间互通的网络接口。

VTEP1 和 L3GW 连接的三层 VLAN 10，互联 IP 地址 10.18.1.1/24 和 10.18.1.2/24，VTEP2 和 L3GW 连接的三层 VLAN 20，互联 IP 地址 10.18.2.1/24 和 10.18.2.2/24。

VTEP1 接入侧 BD 接口 1 绑定 VNI 100；VTEP2 接入侧 BD 接口 5 绑定 VNI 200；

VTEP1 与 PC1 连接的子接口的接入方式，VLAN 5 untag，绑定 BD 1；VTEP2 与 PC3 连接的子接口接入方式，VLAN 50 untag，绑定 BD 5。

VTEP1 配置网络侧 NVE 接口和隧道 VNI 100、源及目的 IP；VTEP2 配置网络侧 NVE 接口和隧道 VNI 200、源及目的 IP。

L3GW 配置 NVE 接口和与 VTEP1、VTEP2 连接的隧道，配置作为 PC1 网关的三层 bd 接口 100 和做为 PC3 网关的 bd 接口 200。

操作步骤

步骤 1 配置 VTEP1。

#配置 BD 接口。

VTEP1(config)#bridge-domain 1

VTEP1(config-bridge-domain-1)#vxlan vni 100

VTEP1(config-bridge-domain-1)#exit

#配置子接口接入方式。

VTEP1(config)#interface 10gigaethernet 1/0/1.1

VTEP1(config-10ge1/0/1.1)#no shutdown

VTEP1(config-10ge1/0/1.1)#encapsulation untag

VTEP1(config-10ge1/0/1.1)#bridge-domain bind 1

VTEP1(config-10ge1/0/1.1)#exit

#配置与 L3GW 连接的网络接口。

VTEP1(config)#interface vlan 10

VTEP1(config-vlan-10)#ip address 10.18.1.1 255.255.255.0

VTEP1(config-vlan-10)#exit

VTEP1(config)#interface 10gigaethernet 1/0/2

VTEP1(config-10ge1/0/2)#no shutdown

VTEP1(config-10ge1/0/2)#port hybrid vlan 10 untagged

VTEP1(config-10ge1/0/2)#port hybrid pvid 10

VTEP1(config-10ge1/0/2)#exit

#配置 NVE 接口的 VXLAN 隧道。

VTEP1(config)#interface nve 1

VTEP1(config-nve-1)#tunnel source 10.18.1.1

VTEP1(config-nve-1)#vni 100 ucast-peer 10.18.1.2

VTEP1(config-nve-1)#exit

步骤 2 配置 VTEP2：配置基本与 VTEP1 一样。

#配置 BD 接口。

VTEP2(config)#bridge-domain 5

VTEP2(config-bridge-domain-5)#vxlan vni 200

VTEP2(config-bridge-domain-5)#exit

#配置子接口接入方式。

VTEP2(config)#interface 10gigaethernet 1/0/1.1

VTEP2(config-10ge1/0/1.1)#no shutdown

VTEP2(config-10ge1/0/1.1)#encapsulation untag

VTEP2(config-10ge1/0/1.1)#bridge-domain bind 5

VTEP2(config-10ge1/0/1.1)#exit

#配置与 VTEP1 连接的网络接口。

VTEP2(config)#interface vlan 20

VTEP2(config-vlan-20)#ip address 10.18.2.1 255.255.255.0

VTEP2(config-vlan-20)#exit

VTEP2(config)#interface 10gigaethernet 1/0/2

VTEP2(config-10ge1/0/2)#no shutdown

VTEP2(config-10ge1/0/2)#port hybrid vlan 20 untagged

VTEP2(config-10ge1/0/2)#port hybrid pvid 20

VTEP2(config-10ge1/0/2)#exit

#配置 NVE 接口的 VXLAN 隧道。

VTEP2(config)#interface nve 1

VTEP2(config-nve-1)#tunnel source 10.18.2.1

VTEP2(config-nve-1)#vni 200 ucast-peer 10.18.2.2

VTEP2(config-nve-1)#exit

步骤 3 配置 L3GW。

#配置与 VTEP1 和 VTEP2 三层互通接口。

L3GW(config)#interface vlan 10

L3GW(config-vlan-10)#ip address 10.18.1.2 255.255.255.0

L3GW(config-vlan-10)#exit

L3GW(config)#interface vlan 20

L3GW(config-vlan-20)#ip address 10.18.2.2 255.255.255.0

L3GW(config-vlan-20)#exit

L3GW(config)#interface 10gigaethernet 1/0/2

L3GW(config-10ge1/0/2)#no shutdown

L3GW(config-10ge1/0/2)#port hybrid vlan 10 untagged

L3GW(config-10ge1/0/2)#port hybrid pvid 10

L3GW(config-10ge1/0/2)#exit

L3GW(config)#interface 10gigaethernet 1/0/3

L3GW(config-10ge1/0/2)#no shutdown

L3GW(config-10ge1/0/2)#port hybrid vlan 20 untagged

L3GW(config-10ge1/0/2)#port hybrid pvid 20

L3GW(config-10ge1/0/2)#exit

#配置 NVE 接口的 VXLAN 隧道。

L3GW(config)#interface nve 1

L3GW(config-nve-1)#tunnel source 10.18.1.2

L3GW(config-nve-1)#vni 100 ucast-peer 10.18.1.1

L3GW(config-nve-1)#exit

L3GW(config)#interface nve 2

L3GW(config-nve-2)#tunnel source 10.18.2.2

```
L3GW(config-nve-2)#vni 200 ucast-peer 10.18.2.1
L3GW(config-nve-2)#exit
```

#配置三层 BD 接口。

```
L3GW(config)#bridge-domain 1
L3GW(config-bridge-domain -1)#vxlan vni 100
L3GW(config-bridge-domain-1)#exit
L3GW(config)#interface bridge-domain 1
L3GW(config-if-bridge-domain1)#ip address 10.18.3.254 255.255.255.0
L3GW(config-if-bridge-domain1)# exit
L3GW(config)#bridge-domain 2
L3GW(config-bridge-domain-2)#vxlan vni 200
L3GW(config-bridge-domain-2)#exit
L3GW(config)#interface bridge-domain 2
L3GW(config-if-bridge-domain2)#ip address 10.18.4.254 255.255.255.0
L3GW(config-if-bridge-domain2)#exit
```

步骤 4：调试 VXLAN 功能。

配置好 VTEP1 和 VTEP2、L3GW 之后，从 PC1 ping PC3，看是否能 ping 通，不能 ping 通则在 L3GW 上查看 ARP 地址表，看是否有 PC1 和 PC3 的带 VXLAN 隧道的 ARP，如果没有则看 L3GW 与 VTEP1 和 VTEP2 隧道两端是否能 ping 通。

12.2 EVPN 配置

12.2.1 EVPN 概述

EVPN（Ethernet Virtual Private Network，以太网虚拟专用网络）是一种二层 VPN 技术，控制平面采用 MP-BGP 通告 EVPN 路由信息，数据平面采用 VXLAN 封装方式转发报文。

EVPN 继承了 MP-BGP 和 VXLAN 的优势，具有如下特点：

- 配置简易：通过 MP-BGP 实现 VTEP 自动发现、VXLAN 隧道自动建立、VXLAN 隧道与 VXLAN 自动关联，用户无需手工配置，降低网络部署难度。
- 控制平面与数据平面分离：控制平面负责发布路由信息，数据平面负责转发报文，易于管理。
- 支持对称 IRB（Integrated Bridging and Routing，集成的桥接和路由）：MP-BGP 同时发布二层 MAC 地址和三层路由信息，VTEP 可以进行二层转发和三层路由。流量采用最优路径转发，减少了广播流量。

12.2.2 配置 EVPN

目的

本节介绍如何配置 EVPN。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
创建 EVPN 实例	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **bridge-domain** *bd-id* 进入 BD 配置视图； 3. 执行命令 **evpn** 创建 EVPN 实例。
删除 EVPN 实例	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **bridge-domain** *bd-id* 进入 BD 配置视图； 3. 执行命令 **no evpn** 删除 EVPN 实例。
配置 EVPN 实例的路由标识	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **bridge-domain** *bd-id* 进入 BD 配置视图； 3. 执行命令 **evpn** 进入 EVPN 实例； 4. 执行命令 **evpn route-distinguisher** *rdstring* 配置 EVPN 实例的路由标识。
配置 EVPN 实例的 target	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **bridge-domain** *bd-id* 进入 BD 配置视图； 3. 执行命令 **evpn** 进入 EVPN 实例； 4. 执行命令 **evpn vpn-target** *target* { **both** | **export-extcommunity** | **import-extcommunity** }配置 EVPN 实例的 target。
删除 EVPN 实例的 target	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **bridge-domain** *bd-id* 进入 BD 配置视图； 3. 执行命令 **evpn** 进入 EVPN 实例； 4. 执行如下命令删除 EVPN 实例的 target： ● **no evpn vpn-target**

目的	步骤
	● **no evpn vpn-target** *target* { **both** | **export-extcommunity** | **import-extcommunity** }。

12.2.3 维护及调试

目的

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

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
打开 EVPN 调试功能	1. 执行命令 **configure** 进入全局配置视图或保持特权用户视图； 2. 执行命令 **debug evpn** { **error** | **nm** | **event** | **all** }打开 EVPN 调试功能。
关闭 EVPN 调试功能	1. 执行命令 **configure** 进入全局配置视图或保持特权用户视图； 2. 执行命令 **no debug evpn** { **error** | **nm** | **event** | **all** }关闭 EVPN 调试功能。
查看 EVPN 实例信息	1. 执行命令 **configure** 进入全局配置视图或保持特权用户视图； 2. 执行命令 **show evpn** 或 **show evpn vpn-target** 查看 EVPN 实例信息。
查看 BGP EVPN 的路由信息	1. 执行命令进入特权用户视图； 2. 执行以下命令查看 EVPN 的路由信息： ● **show ip bgp evpn route**； ● **show ip bgp evpn route** { **mac-ip** | **prefix** | **tunnel** }； ● **show ip bgp evpn route arp** *ip-address*； ● **show ip bgp evpn route count**； ● **show ip bgp evpn route mac** *mac-address*； ● **show ip bgp evpn route nd** *ipv6-address*； ● **show ip bgp evpn route prefix** *ip-address*； ● **show ip bgp evpn route prefix** *ipv6-address*； ● **show ip bgp evpn route tunnel** *tunnel-source-ip-address tunnel-vni*； ● **show ip bgp evpn route tunnel** *tunnel-source-ipv6-address tunnel-vni*； ● **show ip bgp evpn route** { **arp** | **nd** } **peer** *peer-ipv4-address* **l2vni** *vni-id* **l3vni** *vni-id*； ● **show ip bgp evpn route** { **arp** | **nd** } *peer peer-ipv6-address* **l2vni** *vni-id* **l3vni** *vni-id*； ● **show ip bgp evpn route** { **arp** | **nd** | **prefix** } **peer** *peer-ipv4-address* **l3vni** *vni-id*； ● **show ip bgp evpn route** { **arp** | **nd** | **prefix** } **peer** *peer-ipv6-address* **l3vni** *vni-id*；

目的	步骤
	● **show ip bgp evpn route** { **mac** | **arp** | **nd** } **peer** *peer-ipv4-address* **l2vni** *vni-id*； ● **show ip bgp evpn route** { **mac** | **arp** | **nd** } **peer** *peer-ipv6-address* **l2vni** *vni-id*； ● **show ip bgp evpn route** { **mac** | **arp** | **nd** | **prefix** | **tunnel** } **peer** *peer-ipv4-address*； ● **show ip bgp evpn route** { **mac** | **arp** | **nd** | **prefix** | **tunnel** } **peer** *peer-ipv6-address*。

12.2.4 配置举例

组网要求

现有数据中心二层应用场景，使用 EVPN 方式进行配置，要求 S2 和 S3 能够 L2 层互通；虚拟机 VMA 和 VMG 能够互相访问。

组网图

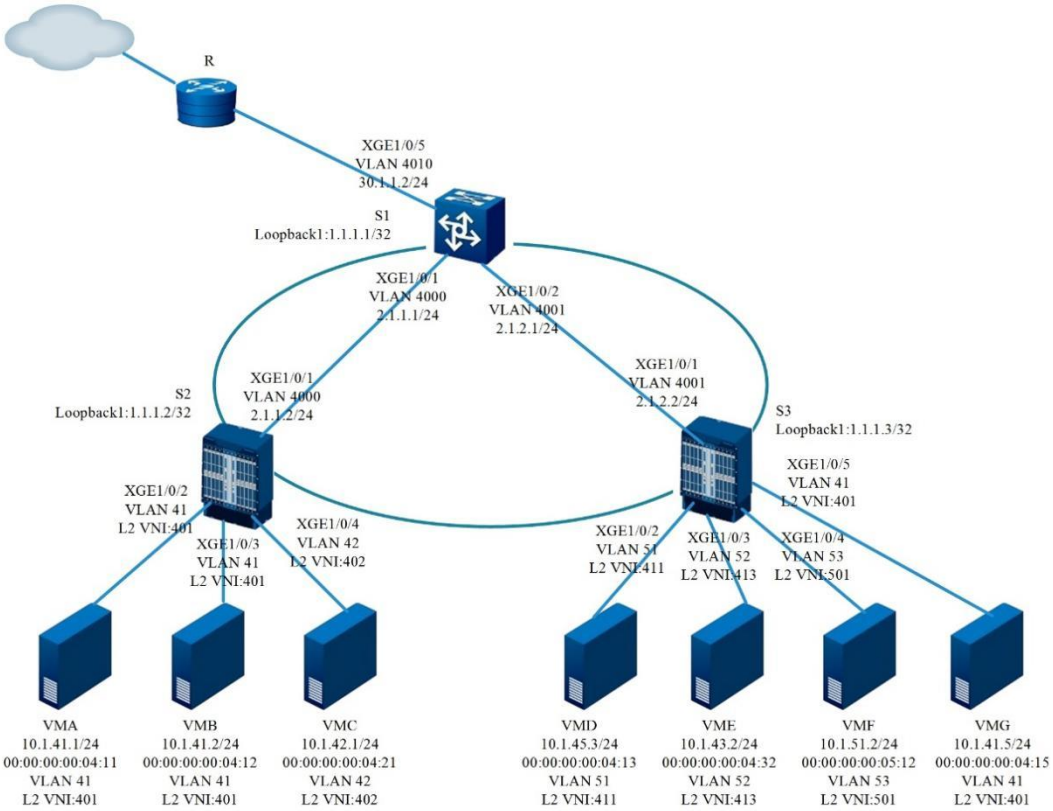


图 12-7 EVPN 组网示意图

配置步骤

1、配置 S1、S2、S3 设备名称，创建 VLAN，并端口加入 VLAN。

//设备 S1 的配置：

CN12800(config)#

CN12800(config)#hostname S1

S1(config)#vlan 4000,4001

Info: This operation may take a few seconds. Please wait for a moment....done.

S1(config)#interface xgigaethernet 1/0/1

S1(config-10ge1/0/1)#port link-type trunk

S1(config-10ge1/0/1)#port trunk allow-pass vlan 4000

S1(config-10ge1/0/1)#quit

S1(config)#interface xgigaethernet 1/0/2

S1(config-10ge1/0/2)#port link-type trunk

S1(config-10ge1/0/2)#port trunk allow-pass vlan 4001

S1(config-10ge1/0/2)#

//设备 S2 的配置：

CN12800(config)#

CN12800(config)#hostname S2

S2(config)#vlan 4000

S2(vlan-4000)#quit

S2(config)#interface xgigaethernet 1/0/1

S2(config-10ge1/0/1)#port link-type trunk

S2(config-10ge1/0/1)#port trunk allow-pass vlan 4000

S2(config-10ge1/0/1)#

//设备 S3 的配置：

CN12800(config)#

CN12800(config)#hostname S3

S3(config)#vlan 4001

S3(vlan-4001)#quit

S3(config)#interface xgigaethernet 1/0/1

S3(config-10ge1/0/1)#port link-type trunk

S3(config-10ge1/0/1)#port trunk allow-pass vlan 4001

S3(config-10ge1/0/1)#

2、配置 VLAN 接口和 Loopback 接口的 IP 地址。

//设备 S1 的配置：

S1(config)#

S1(config)#interface loopback 1

S1(config-loopback-1)#ip address 1.1.1.1/32

S1(config-loopback-1)#quit

S1(config)#interface vlan 4000

S1(config-vlan-4000)#ip address 2.1.1.1/24

S1(config-vlan-4000)#quit

S1(config)#interface vlan 4001

S1(config-vlan-4001)#ip address 2.1.2.1/24

S1(config-vlan-4001)#quit

S1(config)#

//设备 S2 的配置：

S2(config)#

S2(config)#interface loopback 1

S2(config-loopback-1)#ip address 1.1.1.2/32

S2(config-loopback-1)#quit

S2(config)#interface vlan 4000

S2(config-vlan-4000)#ip address 2.1.1.2/24

S2(config-vlan-4000)#quit

S2(config)#

//设备 S3 的配置：

S3(config)#

S3(config)#interface loopback 1

S3(config-loopback-1)#ip address 1.1.1.3/32

S3(config-loopback-1)#quit

S3(config)#interface vlan 4001

S3(config-vlan-4001)#ip address 2.1.2.2/24

S3(config-vlan-4001)#quit

S3(config)#

3、配置 S1、S2、S3 OSPF 路由协议，保证 Loopback 接口三层互通。

//设备 S1 的配置：

S1(config)#router ospf 1

S1(config-ospf-1)#network 1.1.1.1 255.255.255.255 area 0

S1(config-ospf-1)#network 2.1.1.0 255.255.255.0 area 0

S1(config-ospf-1)#network 2.1.2.0 255.255.255.0 area 0

S1(config-ospf-1)#

//设备 S2 的配置：

S2(config)#router ospf 1

S2(config-ospf-1)#network 1.1.1.2 255.255.255.255 area 0

S2(config-ospf-1)#network 2.1.1.0 255.255.255.0 area 0

S2(config-ospf-1)#

//设备 S3 的配置：

S3(config)#router ospf 1

S3(config-ospf-1)#network 1.1.1.3 255.255.255.255 area 0

S3(config-ospf-1)#network 2.1.2.0 255.255.255.0 area 0

S3(config-ospf-1)#

4、OSPF 路由配置成功之后，环回接口能够互通，以 S2 ping S3 为例。

S2(config)#ping 1.1.1.3

Pinging 1.1.1.3 with 64 bytes of data:

Reply from 1.1.1.3: bytes=64 time=10ms TTL=63 icmp_seq=1

Reply from 1.1.1.3: bytes=64 time=0ms TTL=63 icmp_seq=2

Reply from 1.1.1.3: bytes=64 time=0ms TTL=63 icmp_seq=3

Reply from 1.1.1.3: bytes=64 time=0ms TTL=63 icmp_seq=4

Reply from 1.1.1.3: bytes=64 time=0ms TTL=63 icmp_seq=5

Ping statistics for 1.1.1.3 :

Packets:Send = 5, Received = 5 , Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 10ms , Average = 2ms

S2(config)#

5、在 S2 和 S3 上配置 EVPN 实例。

//设备 S2 的配置：

S2(config)#bridge-domain 401

S2(config-bridge-domain401)#vxlan vni 401

S2(config-bridge-domain401)#evpn

S2(config-bridge-domain401)#evpn route-distinguisher 1:401

S2(config-bridge-domain401)#evpn vpn-target 1:401 both

//设备 S3 的配置：

S3(config)#bridge-domain 401

S2(config-bridge-domain401)#vxlan vni 401

S2(config-bridge-domain401)#evpn

S2(config-bridge-domain401)#evpn route-distinguisher 1:401

S2(config-bridge-domain401)#evpn vpn-target 1:401 both

6、在 S2 和 S3 上配置 NVE 邻居学习协议为 BGP。

//设备 S2 的配置：

S2(config)#interface nve 2

S2(config-nve2)#tunnel source 1.1.1.2

S2(config-nve2)#vni 401 replication-protocol bgp

//设备 S3 的配置：

S3(config)#interface nve 2

S3(config-nve2)#tunnel source 1.1.1.3

S3(config-nve2)#vni 401 replication-protocol bgp

7、S2 和 S3 配置 BGP 邻居，使能 EVPN 地址族。

//设备 S2 的配置：

S2(config)#router bgp 100

S2(config-bgp)#neighbor 1.1.1.3 remote-as 100

S2(config-bgp)#neighbor 1.1.1.3 update-source 1.1.1.2

S2(config-bgp)#evpn-family

S2(config-bgp-af-evpn)#neighbor 1.1.1.3 enable

S2(config-bgp-af-evpn)#exit

S2(config-bgp)#exit

S2(config)#

//设备 S3 的配置：

S3(config)#router bgp 100

S3(config-bgp)#neighbor 1.1.1.2 remote-as 100

S3(config-bgp)#neighbor 1.1.1.2 update-source 1.1.1.3

S3(config-bgp)#evpn-family

S3(config-bgp-af-evpn)#neighbor 1.1.1.2 enable

S3(config-bgp-af-evpn)#exit

S3(config-bgp)#exit

S3(config)#

12.3 NETCONF 配置

12.3.1 NETCONF 概述

NETCONF 协议简介

网络配置协议（Network Configuration Protocol， NETCONF）是解决网络管理中配置问题十分有效的一种方法，被认为是新一代的网络管理协议，由 RFC 6241 定义，用以替代命令行界面（command line interface, CLI）、简单网络管理协议（Simple Network Management Protocol, SNMP）以及其它专有配置机制。管理软件可以使用 NETCONF 协议将配置数据写入设备，也可从设备中检索数据。所有数据用可扩展标记语言（Extensible Markup Language, XML）编码，通过 SSL 或传输层安全这样安全、面向连接的协议，使用远程过程调用（remote procedure calls, RPCs）方式传输。

Netconf 协议采用 Client/Server 结构：

- Netconf Manager：担任网络中的 Client，运行在 NMS 上并和 Netconf Agent 相互作用来管理设备。网络管理员使用 Netconf Manager（NMS）来发送<RPC>请求给 Netconf Agent。该请求使用 XML 格式。
- Netconf Agent：担任网络中的 Server。为了配置设备，Netconf Manager 发送配置管理请求给 Netconf Agent。Netconf Agent 对该请求进行解析并在配置管理组件（NEM 的 CM 组件）的帮助下对配置进行管理。Netconf Agent 也使用 XML 格式给 Netconf Manager 发送回应。

CN12800 支持的 NETCONF 特性

- 支持 Netconf Agent 服务器端功能，主要用于和数据中心控制器互联。
- 支持基于 SSH 协议实现 Netconf 传输服务。
- 支持管理 openflow 控制器。
- 支持管理 VXLAN 二层功能。
- 支持 EVPN 相关功能模块的配置和状态获取功能。

12.3.2 配置 NETCONF

目的

本节介绍如何配置 NETCONF。

过程

根据不同目的，执行相应步骤，具体参见下表。

目的	步骤
使能或去使能 netconf 协议	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **netconf** { **enable** | **disable** }使能或去使能 netconf 协议。
配置 netconf 日志输出端	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **netconf log** { **none** | **terminal** | **file** }配置 netconf 日志输出端。
配置 netconf 日志输出级别	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **netconf debug-level** { **none** | **off** | **error** | **warn** | **info** | **debug** | **debug2** | **debug3** | **debug4** }配置 netconf 日志输出级别。
配置 netconf 单个日志文件大小	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **netconf log-per-size** *log-per-size* 配置 netconf 单个日志文件大小。
清空 netconf 候选数据库	1. 执行命令 **configure** 进入全局配置视图； 2. 执行命令 **clear netconf candidate database** 清空 netconf 候选数据库。

12.3.3 配置举例

组网要求

当用户希望通过网管统一管理网络设备，可以使用 NETCONF 保证网管与设备之间的通信。

CN12800 用作 Netconf agent 服务端设备，作为 SSH 服务器接收作为 SSH 客户端的 Netconf manager 的连接。在 Netconf manager 上部署网管系统，从而实现通过 NETCONF 管理配置文件。

组网图

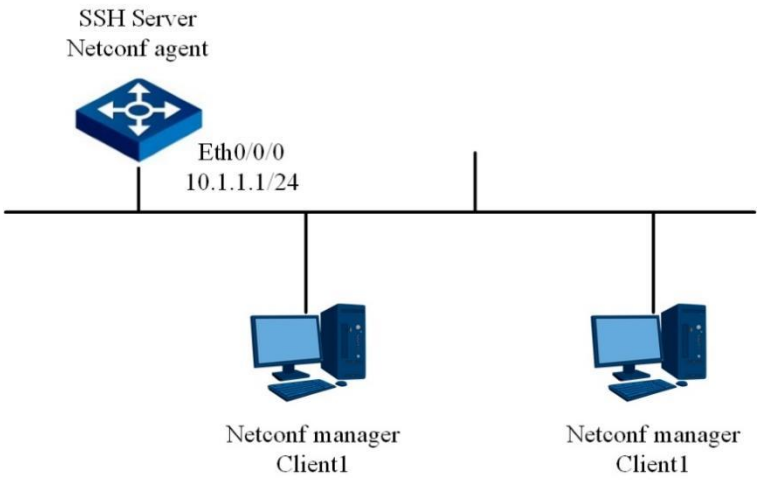


图 12-8 NETCONF 组网示意图

前提配置

已在 Netconf manager 上部署完成网管系统。

配置步骤

1、配置 CN12800 管理网口的 IP 地址。

CN12800(config)#interface ethernet 0/0/0

CN12800(config-eth0/0/0)#ip address 10.1.1.1/24

CN12800(config-eth0/0/0)#quit

CN12800(config)#

2、配置 SSH。

CN12800(config)#sshd

3、使能 NETCONF 功能。

CN12800(config)#netconf enable

4、配置 NETCONF 日志输出到串口。

CN12800(config)#netconf log terminal

5、配置 NETCONF 日志输出级别为 debug4。

CN12800(config)#netconf debug-level debug4

6、配置 NETCONF 单个日志文件大小为 10M。

CN12800(config)#netconf log-per-size 10

7、清空候选数据库的配置。

CN12800(config)#clear netconf candidate database