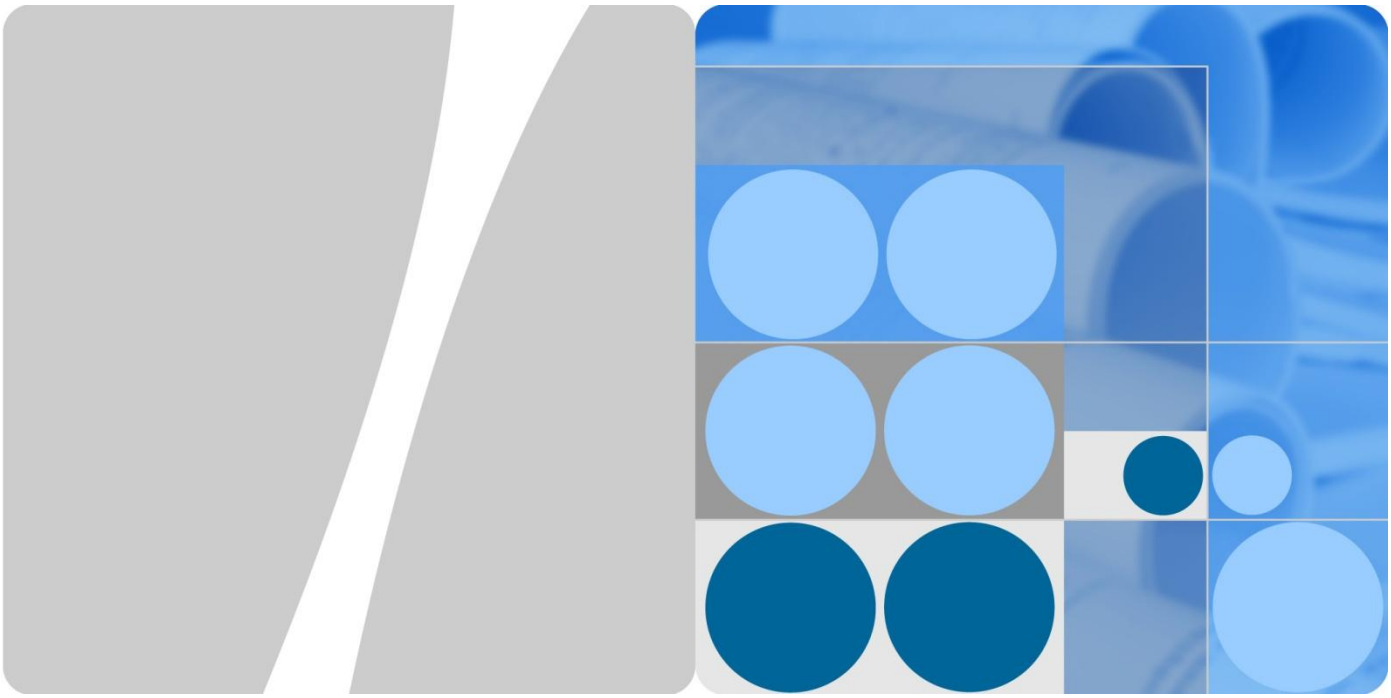
HUAWEI

华为盒式交换机

开局一本通

华为企业中国客户支持部 出品



S 系列交换机开局一本通

文档版本 01

发布日期 2015-05-17

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008229999

目 录

1 登录设备

1.1 通过串口线console口登录设备

一、功能简介：

PC端通过设备的Console口登录，实现对第一次上电的设备进行基本配置和管理。

二、配置命令和步骤：

1、准备线缆：

台式机一般有COM口，可直接使用产品随机附带的Console通信电缆，如图1-1所示：

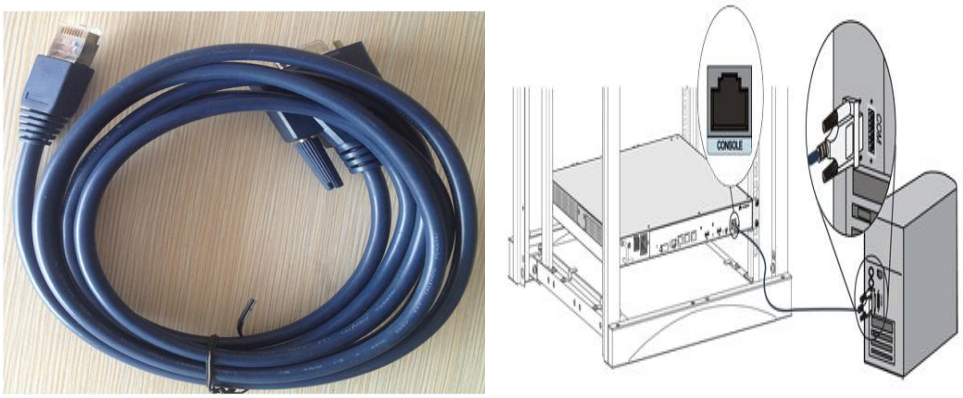


图 1-1 console线和com接口

如果是笔记本或没有COM口的电脑，需准备转接线，并安装好随线光盘的驱动：

图 1-2 USB转接线

检查设备管理器中COM口是否正常：

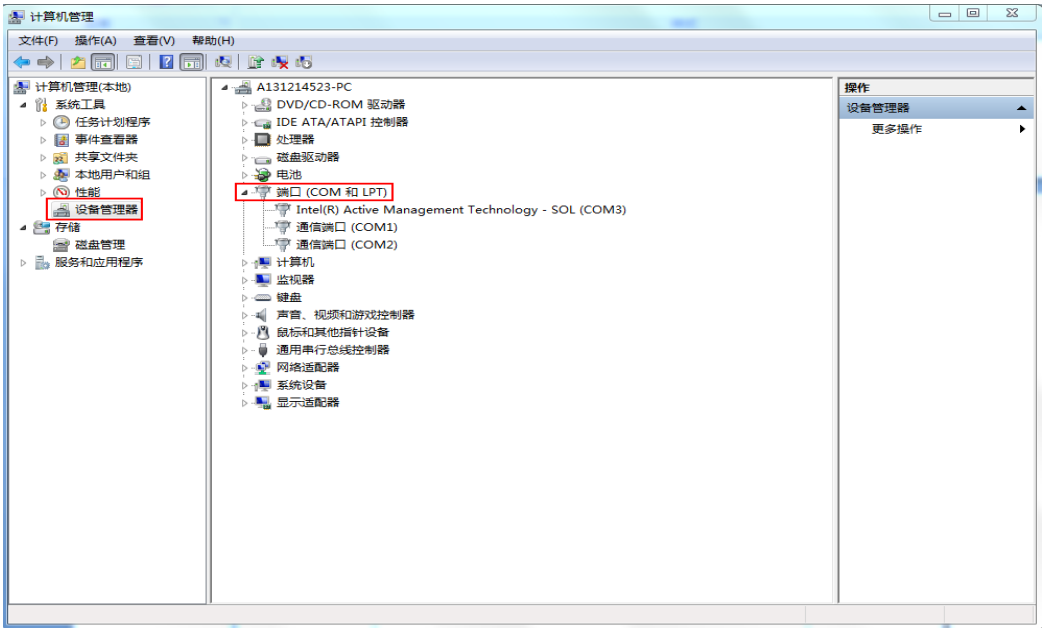


图1-3　查看终端的com接口编号

2、配置COM口参数并连接设备：

通信参数设置参考表	
参数	缺省值
传输速率	9600bit/s
流控方式	不进行流控
校验方式	不进行校验
停止位	1
数据位	8

①、超级终端（XP自带）：

鼠标依次单击"开始"->附件->通讯->超级终端

图 1-4 xp系统打开超级终端

单击进入"超级终端"后如下图所示，给超级终端命名

图1-5 超级终端设置

进入"连接到"视窗后，"连接时使用"中则需要选用相应的COM口，在此我们选择COM1口（COM口编号的选择请见上面的检查步骤），如下图所示

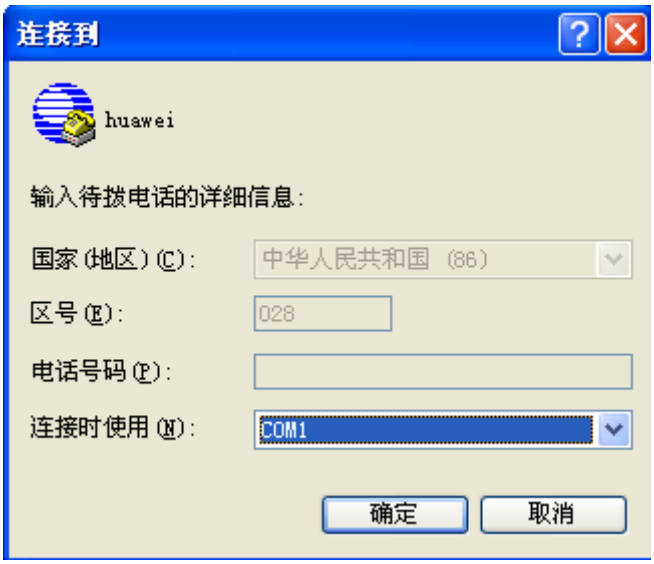


图1-6 com接口选择

在"COM1属性"视窗中，我们只需单击"还原为默认值"按钮，即可使其中各项参数自动恢复为符合本此连接属性的数值，也可手动进行设置

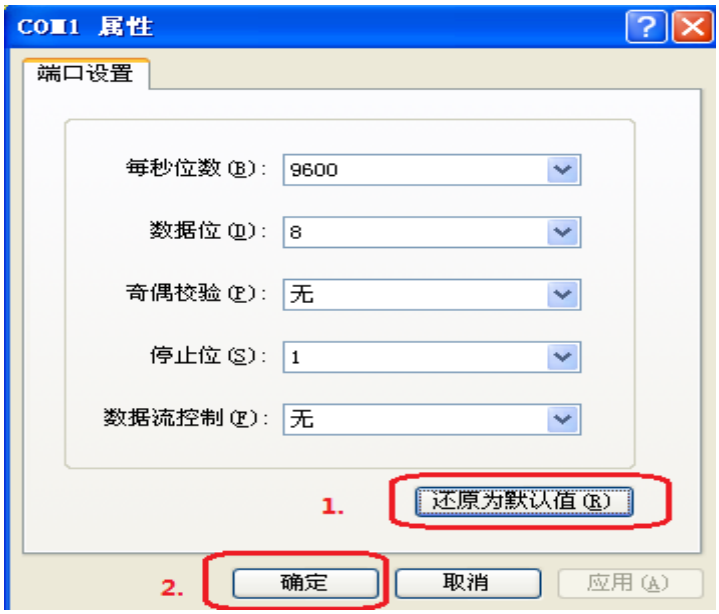


图1-7 com接口参数设置

在上一视图中各项参数设置完毕后单击"确定"进入本次超级终端连接的命令行操作视窗，表示超级终端连接已经建立，按回车开始操作，如图1-8所示

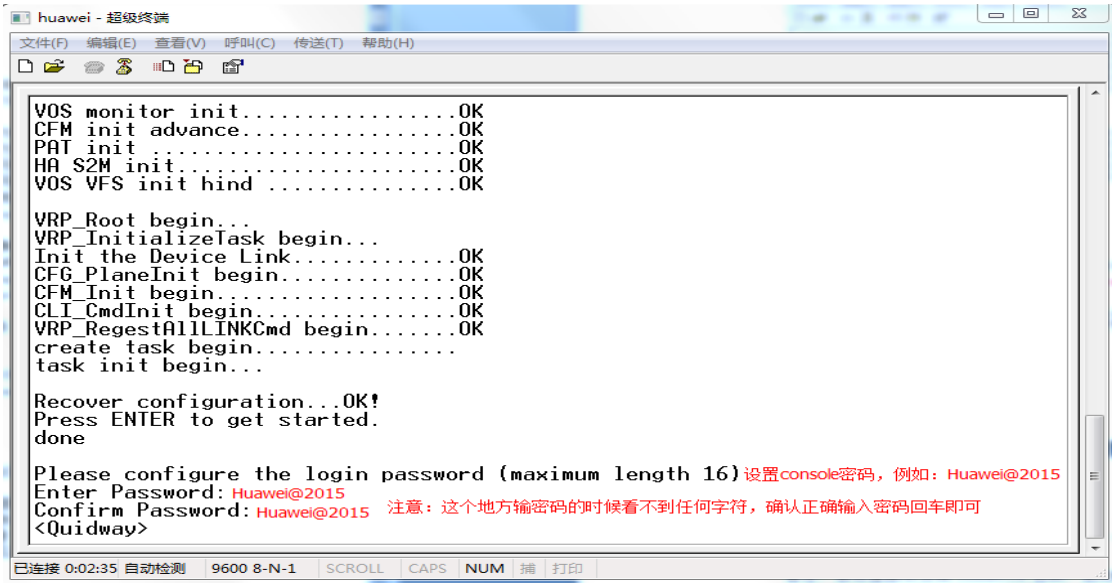


图1-8 console密码设置

②、使用 SecureCRT 软件登录：

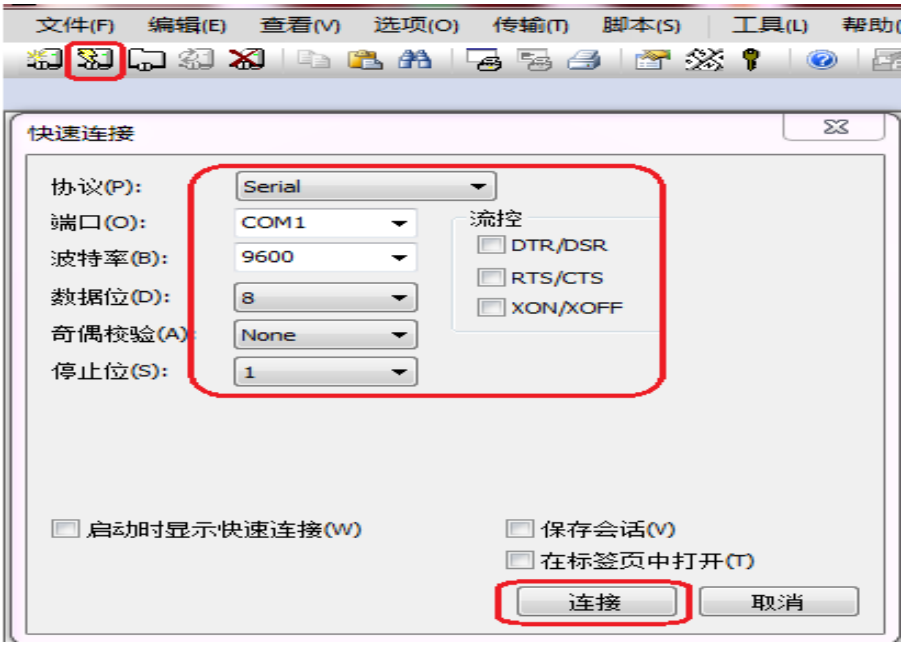


图1-9 scrt软件参数设置

1.2 交换机IP地址配置

一、功能简介

通过配置 IP 地址，实现设备与网络上其他设备进行通信。

二、配置命令和步骤

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
3. 执行命令 **ip address** *ip-address* { *mask* | *mask-length* }，配置主 IP 地址。
4. 执行命令 **ip address** *ip-address* { *mask* | *mask-length* } **sub**，配置从 IP 地址。

三、应用场景

配置接口的IP地址示例

组网需求

如图 1-10 所示，Switch 上只有一个空闲以太网接口 GE0/0/1，但该局域网中的计算机分别属于 2 个不同的网段 172.16.1.0/24 和 172.16.2.0/24，要求通过 Switch 可以实现一个接口接入两个不同的网段。

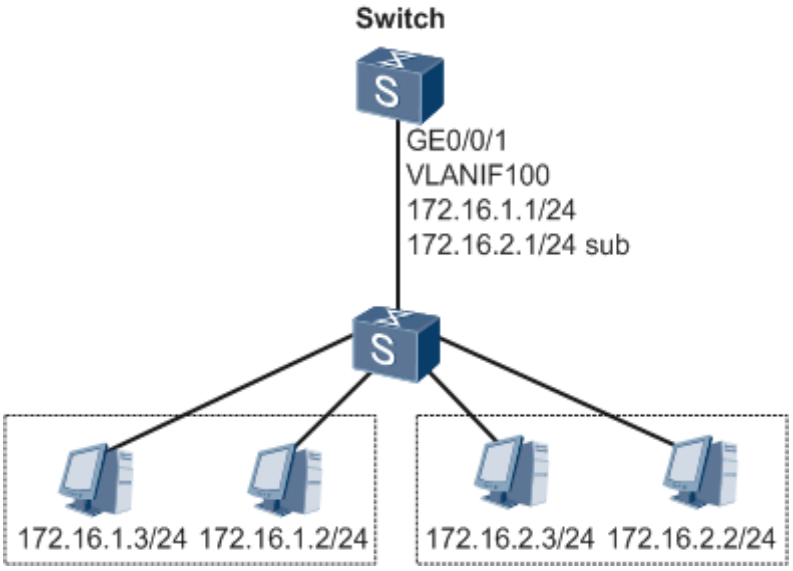


图1-10 配置IP地址示例

配置思路

配置主从 IP 地址的思路如下：

配置主从 IP 地址，实现一个接口可以接入两个不同网段。

详细配置步骤

配置 Switch 的 GE0/0/1 接口所属 VLANIF100 接口的 IP 地址

```
<HUAWEI> system-view                                    //进入系统模式
[HUAWEI] sysname Switch                                 //交换机重命名
[Switch] vlan 100                                       //创建 vlan
[Switch-vlan100] quit                                   //退出 vlan 模式
[Switch] interface gigabitethernet 0/0/1                //进入接口
[Switch-GigabitEthernet0/0/1] port link-type access
[Switch-GigabitEthernet0/0/1] port default vlan 100
 [Switch-GigabitEthernet0/0/1] quit
[Switch] interface vlanif 100                           //进入三层 vlanif 接口
[Switch-Vlanif100] ip address 172.16.1.1 24             //配置主 IP 地址
[Switch-Vlanif100] ip address 172.16.2.1 24 sub         //配置从 IP 地址
[Switch-Vlanif100] quit
[Switch] quit
```

1.3 Telnet远程登录设备

一、功能简介：

在设备上使能并配置 Telnet 功能后，用户可直接远程登录设备，无需再通过 console 口登录设备（在配置用户通过 Telnet 登录设备之前，需完成以下任务：终端与设备之间路由可达）。

二、配置命令和步骤：

1.系统视图下，执行命令 **telnet server enable** ，使能设备的 Telnet 功能；

2.执行命令 **user-interface vty** first-ui-number [last-ui-number]，进入 VTY 用户界面视图；

3.VTY 用户界面视图下，执行命令 **authentication-mode** { password | aaa | none }，配置用户验证方式为密码验证/AAA 验证/不验证；

（可选）当使用 AAA 认证模式时，需要配置登录用户的相关信息：

[HUAWEI] **aaa** //进入 AAA 模板

[HUAWEI-aaa] **local-user** user-name **password** password//配置用户名和密码

[HUAWEI-aaa] **local-user** user-name **service-type telnet** //配置协议

[HUAWEI-aaa] **local-user** user-name **privilege level 3** //用户优先级

[HUAWEI-aaa] **quit**

4.执行命令**protocol inbound { all | telnet }**，配置 VTY 用户界面支持所有协议/ssh 协议/Telnet 协议：

5.从终端通过 Telnet 登录设备，以 Windows 命令行提示符为例：

单击左下角菜单→在搜索栏中输入 cmd 并回车，进入 Windows 命令行界面，执行命令"telnet IP-address"远程登录设备(此 IP 地址为设备管理 IP 地址,需要事先配置完成并与终端之间路由可达，即 可 ping 通)。

三、应用场景：

配置用户通过Telnet登录设备示例

组网需求

如图 1-11 所示，PC 与设备之间路由可达，用户希望简单方便的配置和管理远程设备，可以在服务器端配置 Telnet 用户使用 AAA 验证登录，并配置安全策略，保证只有用户使用的 PC 才能登录设备。

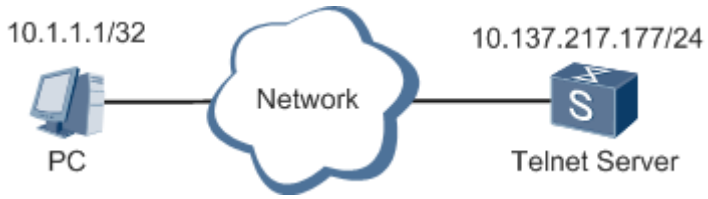


图1-11 交换机配置telnet组网

配置思路

采用如下的思路配置通过 Telnet 登录设备：

1． 配置 Telnet 方式登录设备，以实现远程维护网络设备。

2． 配置管理员的用户名和密码，并配置 AAA 认证策略，保证只有用户才能登录设备。

3． 配置安全策略，保证只有当前管理员使用的 PC 才能登录设备。

详细配置步骤

1.使能服务器功能

```
<HUAWEI> system-view
[HUAWEI] telnet server enable
```

2.配置 VTY 用户界面的相关参数

进入 VTY 用户界面视图，配置支持协议。

```
[HUAWEI] user-interface vty 0 4
[HUAWEI-ui-vty0-4] protocol inbound telnet
```

配置 VTY 用户界面的用户验证方式。

```
[HUAWEI-ui-vty0-4] authentication-mode aaa
[HUAWEI-ui-vty0-4] quit
```

3.配置登录用户的相关信息

配置登录验证方式。

```
[HUAWEI] aaa
[HUAWEI-aaa] local-user admin1234 password admin1234
[HUAWEI-aaa] local-user admin1234 service-type telnet
[HUAWEI-aaa] local-user admin1234 privilege level 15
[HUAWEI-aaa] quit
```

4.客户端登录

进入管理员 PC 的 Windows 的命令行提示符，执行相关命令，通过 Telnet 方式登录设备。

```
C:\Documents and Settings\Administrator> telnet 10.137.217.177
```

输入 Enter 键后，在登录窗口输入 AAA 验证方式配置的登录用户名和密码，验证通过后，出现用户视图的命令行提示符，至此用户成功登录设备。

```
Login authentication
Username:admin1234
Password:
Info: The max number of VTY users is 8, and the number
     of current VTY users on line is 2.
     The current login time is 2012-08-06 18:33:18+00:00.
<Telnet Server>
```

1.4 盒式交换机web使用指导

盒式交换机 web 文件配置情况一览表

⊗	设置在出厂时，存储器中无web网页文件
+	设备在出厂时，存储器中已经保存了web网页文件，未完成加载
✓	设备在出厂时，存储器中已经保存了Web网页文件，并已完成加载
☑	设备在出厂时，系统软件中集成了Web网页文件，并已完成了加载
—	设备当前无此版本

版本 设备	V100 R005	V100 R006	V200 R001	V200 R002	V200 R003	V200 R005	V200 R006	V200 R007
S2300	⊗	⊗	—	—	—	—	—	—
S2700	⊗	+	—	—	—	—	—	—
S2720							✓	
S2750					✓	✓		☑
S3300	⊗	⊗	⊗					
S3700	⊗	+	+					
S5300	⊗	⊗	⊗					
S5700	⊗	⊗	+	+	✓	✓	☑	☑
S6300	—	⊗	⊗	—	—	—	—	—
S6700	—	⊗	+	+	✓	✓	—	—
S7700	—	⊗	+	⊗	✓	☑	☑	☑
S9300	—	⊗	⊗	⊗	⊗	☑		☑
S9700	—	—	+	⊗	✓	☑	☑	☑

一. 功能介绍

通过配置 WEB 登录功能实现图形化界面配置功能。

二. 配置命令和步骤

1.获取 web 网页文件

请先登录华为公司技术支持（http://support.huawei.com/enterprise），登录后，在“软件下载 >企业网络 > 交换机 > 园区交换机 > S23&27&33&37&53&57 系列”路径下，根据版本名称，下载对应的版本软件。版本软件中包含 Web 网页文件，名称为“产品+软件版本号.web.zip”或“产品-软件版本号.WEB 网管文件版本号.web.7z”。

2.设置 S 交换机的管理 IP 地址

执行命令 **system-view**，进入系统视图。

执行命令 **interface vlanif** *interface-number*，进入管理 VLAN 接口视图。

执行命令 **ip address** *ip-address* { *mask* | *mask-length* } ，配置接口的 IP 地址。

3.上传 web 网页文件

执行命令 **ftp server enable**，系统视图下使能 FTP 服务。

执行命令 **aaa**，进入 AAA 视图

执行命令 **local-user** user-name **password { simple | cipher }** password，配置 FTP 用户名和密码。

执行命令 **local-user** user-name **ftp-directory** directory，配置 FTP 用户的访问路径。

执行命令 **local-user** user-name **service-type ftp**，配置 FTP 登录用户的服务类型。

在 PC 的 cmd 视图下执行命令 **ftp** ip-address，输入用户名和密码，登录 S 系列交换机。

在 FTP 视图下执行 **put** local-filename 命令，将 PC 上的 Web 网页文件（例如：web.zip）上传至 S 系列交换机。

4．加载 web 网页文件

执行命令 **http server load** file-name，系统视图下加载 Web 网页文件。

5．创建 web 网管账号

执行命令 **http server enable**，系统视图下使能 HTTP 服务，如果使能不成功则先执行命令 **http secure-server enable**，再敲此命令。

执行命令 **aaa**，进入 AAA 视图。

执行命令 **local-user** user-name **password { simple | cipher }** password，配置 HTTP 用户名和密码。

执行命令 **local-user** user-name **service-type http**，配置用户 admin 的访问类型为 HTTP。

6．登录 web 网管

1． 在 PC 上打开 Web 浏览器，在地址栏中输入 S 交换机的管理 IP 地址（PC 和 S 交换机之间要有可达的路由），按回车键后将显示登录对话框。如图 1-12 所示，输入之前设置的 Web 网管帐号和密码，输入验证码，并选择 Web 网管系统的语言。

图1-12 web登录界面

2． 单击“登录”或直接按回车键即可进入 Web 网管系统主页面。

登录到 Web 网管后，可以对交换机进行配置。

三． 应用场景

配置用户通过Web网管登录设备示例

组网需求

1． 如图 1-13 所示，从 PC 上通过 Web 网管登录设备，将设备作为 Web 网管服务器，实现图形化界面管理和维护设备。

图1-13 配置通过Web网管登录设备组网图

配置思路

采用如下的思路配置用户通过 Web 网管登录设备：

1． 上传 Web 网页文件。

2． 加载 Web 网页文件。

3． 配置 HTTP 服务功能及 HTTP 用户。

4． 登录 Web 网管。

详细配置步骤

1、配置管理 IP 地址

```
<huawei> system-view                                    //进入系统模式
[huawei] interface Vlanif 1                             //进入三层 vlanif 接口
[huawei-Vlanif1] ip address 192.168.0.1 24              //配置管理 IP 地址
```

2、（可选）上传 web 文件（参考 web 文件附录表选择是否执行此步骤）

```
[huawei] ftp server enable                              //系统视图下使能 FTP 功能
[huawei] aaa                                            //系统系统下进入 aaa 模式
[huawei-aaa] local-user admin password cipher Admin@123//配置 FTP 用户名、密码
[huawei-aaa] local-user admin ftp-directory flash:      //配置 FTP 用户的访问路径
[huawei-aaa] local-user admin service-type ftp          //开启 FTP 服务类型
[huawei-aaa] quit                                       //退出 aaa 模式
```

将 PC 电脑上的 web 文件上传至交换机

```
C:\>ftp 192.168.0.1                                     //PC 电脑的 cmd 下登录 FTP
Connected to 192.168.0.1
220 FTP service ready.
User (10.1.1.132:(none)): admin                         //输入 FTP 的用户名
331 Password required for client.
Password: Admin@123                                     //输入 FTP 的密码
230 User logged in.
ftp>
ftp> put web.zip                                        //将 PC 上的 web 文件上传
```

```
200 Port command okay.
150 Opening ASCII mode data connection for web.zip.
226 Transfer complete.
ftp: 发送 251047 字节，用时 3.36Seconds 74.74Kbytes/sec.
ftp>
```

3、（可选）加载 web 网页文件（参考 web 文件附录表选择是否执行此步骤）

```
[huawei] http server load s5700-28c-ei-v200r005c00spc300.web.zip  //系统系统下加载
```

4、创建 web 管理账号

```
[huawei] http server enable                                    //系统视图下使能 http 功能
[huawei] aaa                                                   //系统视图下进入 aaa 模式
[huawei-aaa] local-user admin password cipher Admin@123   //创建 HTTP 登录用户名、密码
[huawei-aaa] local-user admin privilege level 15          //配置 http 登录名权限
[huawei-aaa] local-user admin service-type http           //开启 http 登录服务
[huawei-aaa] quit                                         //退出 aaa
```

5、通过 web 登录

2． 在 PC 上打开 Web 浏览器，在地址栏中直接输入“http://192.168.0.1”，按回车键后，将显示登录对话框，如图 1-14 所示。

图 1-14 web 登录界面示意图

3． 请正确输入 HTTP 用户名、验证码和密码，单击登录或直接按回车键即可进入 Web 网管系统主页面。

2 VLAN配置

一． 功能简介

将设备中的某些接口定义为一个单独的区域，将指定接口加入到指定 VLAN 中之后，接口就可以转发指定 VLAN 报文。从而实现 VLAN 内的主机可以直接通信，而 VLAN 间的主机不能直接互通，将广播报文限制在一个 VLAN 内。

要实现 VLAN 间互通，就要建立 VLAN 间路由，用户直连在三层交换机上，只需直连路由即可。而 VLANIF 接口是一个三层的逻辑接口，在其上配置 IP 地址为用户的网关地址后，它就在三层交换机上生成直连路由，同时，可作为用户的网关。这样，发往各 VLAN 网段的报文，就可在路由表中分别找到其出接口---VLANIF 接口，从而实现三层转发。

二． 配置命令和步骤

在系统视图下先创建 VLAN、配置接口的类型，然后将 VLAN 和接口关联。

1.在系统视图下创建 vlan

执行命令 **vlan** *vlan-id*，创建 VLAN 并进入 VLAN 视图；

或

执行命令 **vlan batch** { vlan-id1 [to vlan-id2] } &<1-10>批量创建 vlan。

2.配置以太网接口属性关联接口和 vlan。

执行命令 **port link-type access** ，接口直接与终端连接；

执行命令 **port default vlan** vlan-id，将接口加入到指定的 VLAN 中。

或

执行命令 **port link-type** trunk ，接口与另一台交换机设备的接口连接；

执行命令 **port trunk allow-pass vlan** vlan-id，将接口加入到指定的 VLAN 中。

3.配置 vlanif 三层逻辑接口作为网关。

执行命令 **interfere vlanif** vlan-id，创建并进入 vlanif 接口视图；

执行命令 **ip address** ip-address mask-address

三． 应用场景

2.1 终端直连三层网关设备进行通信

组网需求：

如下图所示，PC1 和 PC2 分属研发部和质量部，两部门通过一台三层交换机互联，两部门有业务往来，需要二层隔离，三层通信。

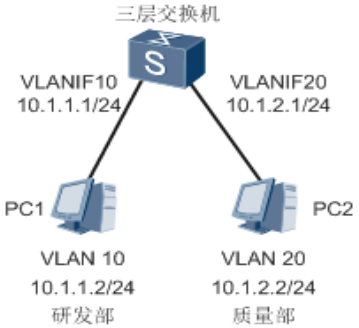


图2-1 终端直连三层网关设备组网图

配置思路 ：

此场景配置简单，只需将连接 PC 的接口加入 VLAN，然后创建 VLANIF，并配置 IP 地址为对应用户的网关即可。

详细操作步骤：

1.创建 vlan

```
<SW1> system-view                                          //进入系统模式
[SW1] vlan batch 10 20                                     //批量新建 vlan 10 和 20
```

2.创建 vlanif 三层接口作为 PC 电脑的网关 IP 地址

```
[SW1] interface Vlanif 10                                  //进入三层 vlanif10 接口
[SW1-Vlanif10] ip address 10.1.1.1 255.255.255.0 //此 IP 地址为 PC1 对应网关地址
[SW1-Vlanif10] quit                                        //退出 vlanif2 接口
[SW1] interface Vlanif 20
[SW1-Vlanif20] ip address 10.1.2.1 255.255.255.0 //此 IP 地址为 PC2 对应网关地址
[SW1-Vlanif20] quit
```

3.接口加入相应 vlan

```
[SW1] interface GigabitEthernet 0/0/1
[SW1-GigabitEthernet0/0/1] port link-type access     //链路类型为 access
[SW1-GigabitEthernet0/0/1] port default vlan 10      //将 PC1 划分到 VLAN 10 中
[SW1-GigabitEthernet0/0/1] quit
[SW1] interface GigabitEthernet 0/0/2
[SW1-GigabitEthernet0/0/2] port link-type access     //链路类型为 access
[SW1-GigabitEthernet0/0/2] port default vlan 20      //将 PC2 划分到 VLAN 10 中
[SW1-GigabitEthernet0/0/2] quit
```

2.2 终端跨二层交换机连接三层网关设备进行通信

组网需求：

如图 2-2 所示，HOSTA 和 HOSTB、HOSTC 和 HOSTD 分属研发部和质量部，两部门通过一台二层交换机互联，两部门有业务往来，需要二层隔离，三层通信。

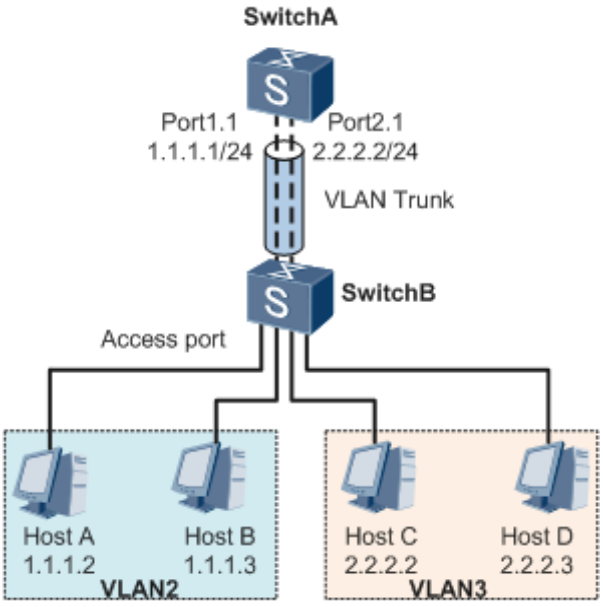


图2-2 终端跨二层交换机连接三层网关设备进行通信组网图

配置思路 ：

1.将 SwitchB 连接终端 HOST 的接口加入 vlan，链路类型为 access；

2.将 SwitchA 和 SwitchB 互联的接口加入 vlan，链路类型为 trunk；

3.创建 VLANIF 并配置 IP 地址为对应用户的网关；

详细操作步骤：

SwitchA 配置：

1.创建 vlan

```
<SWITCHA>system-view                                    //进入系统模式
[SWITCHA]vlan batch 2 3                                 //批量新建 vlan 2 和 3
```

2.创建 vlanif 三层接口作为 PC 电脑的网关 IP 地址

```
[SWITCHA] interface Vlanif 2                            //进入三层 vlanif10 接口
[SWITCHA-Vlanif2] ip address 1.1.1.1 255.255.255.0 //此 IP 地址为 HOSTA/B 对应网关地址
[SWITCHA-Vlanif2] quit                                  //退出 vlanif2 接口
[SWITCHA] interface Vlanif 3
[SWITCHA-Vlanif3] ip address 2.2.2.1 255.255.255.0  //此 IP 地址为 HOSTC/D 对应网关地址
[SWITCHA-Vlanif3] quit
```

3.接口加入相应 vlan，SwitchA-----trunk------SwitchB

```
[SWITCHA] interface GigabitEthernet 0/0/1
[SWITCHA-GigabitEthernet0/0/1] port link-type trunk          //链路类型为 trunk
[SWITCHA-GigabitEthernet0/0/1] port trunk allow-pass 2 to 3 //将接口划分到 VLAN
```

```
2 和 vlan3 中
    [SWITCHA-GigabitEthernet0/0/1] quit
```

SwitchB 配置：

1.创建 vlan

```
    <SWITCHB> system-view                                    //进入系统模式
    [SWITCHB] vlan batch 2 3                                 //批量新建 vlan 2 和 3
```

2.接口加入相应 vlan，SwitchB-----trunk------SwitchA

```
    [SWITCHB] interface GigabitEthernet 0/0/1
    [SWITCHB-GigabitEthernet0/0/1]  port link-type trunk        //链路类型为 trunk
    [SWITCHB-GigabitEthernet0/0/1] port trunk allow-pass 2 to 3  //将接口划分到
VLAN 2 和 vlan3 中
    [SWITCHB-GigabitEthernet0/0/1] quit
```

接口加入相应 vlan，SwitchB---access---HOST，HOSTA 和 HOSTB 配置一样，C 和 D 配置一样

```
    [SWITCHB] interface GigabitEthernet 0/0/2
    [SWITCHB-GigabitEthernet0/0/2] port link-type access       //链路类型为 access
    [SWITCHB-GigabitEthernet0/0/2] port default vlan 2  //将 HOSTA 划分到 vlan2 中
    [SWITCHB-GigabitEthernet0/0/2] quit
    [SWITCHB] interface GigabitEthernet 0/0/4
    [SWITCHB-GigabitEthernet0/0/4] port link-type access       //链路类型为 access
    [SWITCHB-GigabitEthernet0/0/4] port default vlan 3  //将 HOSTC 划分到 vlan3 中
    [SWITCHB-GigabitEthernet0/0/3] quit
```

2.3 不同网段之间通过静态路由进行通信

组网需求：

如下图所示，为安全及便于管理，企业为服务器专门划分 VLAN，用户属于 VLAN10，服务器属于 VLAN20，用户与服务器间跨接入、汇聚和核心交换机，其中，接入是二层交换机，汇聚、核心是三层交换机。由于业务需要，用户与服务器间需要互通。

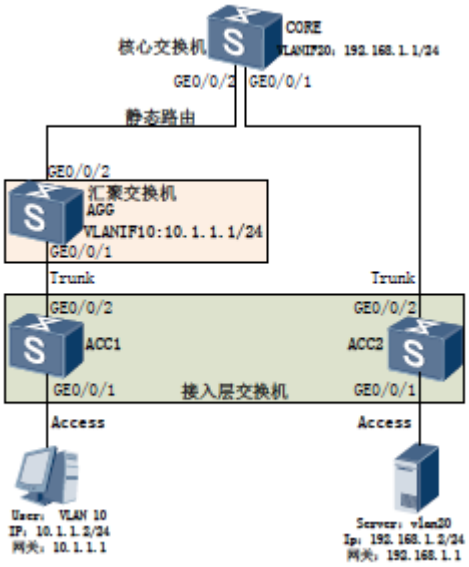


图2-3 不同网段之间通过静态路由进行通信

配置思路：

此场景用户与服务器间跨越多台二层、三层交换机，可以配置 VLANIF，将汇聚交换机 AGG 作为用户 PC 的网关，核心交换机作为服务器 Server 的网关。但 VLANIF 只生成直连路由，只能使得相邻设备互通，要使 User 与服务器互通，还需要配置从 AGG 到 VLAN20 网段以及从 CORE 到 VLAN10 网段的路由，可以使用静态路由，也可以使用动态路由，本示例采用静态路由。

详细配置步骤：

ACC1（二层接入交换机）的配置如下：

1.创建 vlan

```
<ACC1> system-view                                    //进入系统模式
[ACC1] vlan batch 10                                   //批量新建 vlan 10
```

2.接口加入相应 vlan

接口加入相应 vlan

```
[ACC1] interface GigabitEthernet 0/0/1
[ACC1-GigabitEthernet0/0/1] port link-type access          //链路类型为 access
[ACC1-GigabitEthernet0/0/1] port default vlan 10      //将 User 划分到 vlan10 中
[ACC1-GigabitEthernet0/0/1] quit
[ACC1] interface GigabitEthernet 0/0/2
[ACC1-GigabitEthernet0/0/2] port link-type trunk           //链路类型为 trunk
[ACC1-GigabitEthernet0/0/2] port trunk allow-pass 10      //透传 vlan10 到 AGG
[ACC1-GigabitEthernet0/0/2] quit
```

ACC2 的配置与 ACC1 的配置类似，只不过接口加入、透传的 vlan 是 vlan20.

AGG 的配置如下：

1.创建 vlan

```
<AGG> system-view                                    //进入系统模式
[AGG] vlan batch 10 30                               //批量新建 vlan 10 30
```

2.接口加入相应 vlan

接口加入相应 vlan

```
[AGG] interface GigabitEthernet 0/0/1
[AGG-GigabitEthernet0/0/1] port link-type trunk          //链路类型为 trunk
[AGG-GigabitEthernet0/0/1] port trunk allow-pass 10  //透传 vlan10，以转发 User 报文
[AGG-GigabitEthernet0/0/1] quit
[AGG] interface GigabitEthernet 0/0/2
[AGG-GigabitEthernet0/0/2] port link-type trunk      //链路类型为 trunk
[AGG-GigabitEthernet0/0/2] port trunk allow-pass 30   //透传互联 vlan30，以转发互联报文
[AGG-GigabitEthernet0/0/2] quit
```

3.配置 VLANIF10 和 IP 地址，作为用户的网关

```
[AGG] interface Vlanif 10                            //进入三层 vlanif10 接口
[AGG-Vlanif10] ip address 10.1.1.1 255.255.255.0//此 IP 地址为 User 对应网关地址
[AGG-Vlanif10] quit                                  //退出 vlanif2 接口
[AGG] interface Vlanif 30
[AGG-Vlanif30] ip address 10.10.30.1 255.255.255.0//互联 IP 地址，不能与 User、Server 的 IP 网段冲突
[AGG-Vlanif30] quit
```

4.配置静态路由，实现 User 和 Server 之间互通

```
[AGG] ip route-static 192.168.1.0 255.255.255.0 10.10.30.1
```

CORE 的配置如下：

1.创建 vlan

```
<CORE> system-view                                   //进入系统模式
[CORE] vlan batch 20 30                              //批量新建 vlan 20 30
```

2.接口加入相应 vlan

接口加入相应 vlan

```
[CORE] interface GigabitEthernet 0/0/1
[CORE-GigabitEthernet0/0/1] port link-type trunk         //链路类型为 trunk
[CORE-GigabitEthernet0/0/1] port trunk allow-pass 20     //透传 vlan20
```

```
[CORE-GigabitEthernet0/0/1] quit
[CORE] interface GigabitEthernet 0/0/2
[CORE-GigabitEthernet0/0/2] port link-type trunk          //链路类型为 trunk
[CORE-GigabitEthernet0/0/2] port trunk allow-pass 30      //透传互联 vlan30，
以转发互联报文
[CORE-GigabitEthernet0/0/2] quit
```

3.配置 VLANIF10 和 IP 地址，作为用户的网关

```
[CORE] interface Vlanif 20                                //进入三层 vlanif20 接口
[CORE-Vlanif20] ip address 192.168.1.1 255.255.255.0 //此 IP 地址为 User 对应网
关地址
[CORE-Vlanif20] quit                                      //退出 vlanif20 接口
[CORE] interface Vlanif 30
[CORE-Vlanif30] ip address 10.10.30.2 255.255.255.0  //互联 IP 地址
[CORE-Vlanif30] quit
```

4.配置静态路由，实现 User 和 Server 之间互通

```
[CORE] ip route-static 10.1.1.0 255.255.255.0 10.10.30.1
```

2.4 配置基于接口划分vlan示例一（汇聚层设备作为网关）

组网需求：

如图 2-4 所示，SW1 做为 PC 电脑的网关，PC1 直连 SW2 属于 vlan 2，网关为 vlanif 2 接口地址 192.168.2.1/24;PC2 直连 SW2 属于 vlan 3，网关为 vlanif 3 接口地址 192.168.3.1/24；PC3 直连 HUB 交换机 SW3 属于 vlan 4，网关为 vlanif 4 接口地址 192.168.4.1/24；通过配置实现各 PC 电脑之间的互访通信；

注：S3 接入层交换机作为 HUB 使用不做任何配置，插上即用；

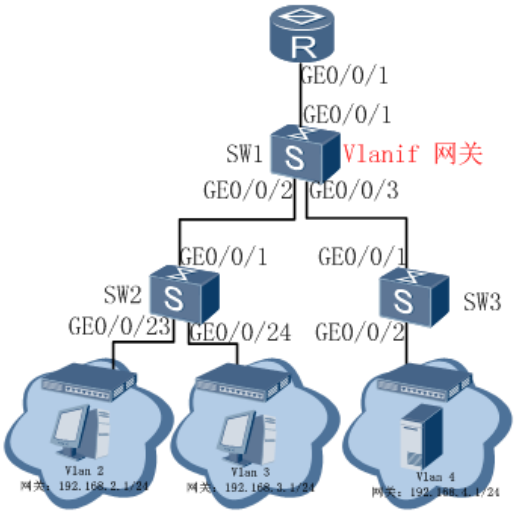


图2-4 汇聚层交换机做网关基于接口划分vlan组网

配置思路：

采用如下的思路配置 VLAN 间互通：

1.创建 VLAN 并将连接用户的接口加入 VLAN，实现不同业务用户之间的二层流量隔离。

2.配置各 PC 电脑的网关 IP 地址，实现不同业务用户之间三层互通

详细配置步骤：

汇聚层交换机 SW1 配置入：

1.创建 vlan

```
<SW1> system-view                                          //进入系统模式
[SW1] vlan batch 2 to 5                                    //批量新建 vlan 2 到 5
```

2.接口加入相应 vlan

SW1----SW2---PC，接口配置成 trunk 模式

```
[SW1] interface GigabitEthernet 0/0/2
[SW1-GigabitEthernet0/0/2] port link-type trunk     //链路类型为 trunk 模式
[SW1-GigabitEthernet0/0/2] port trunk allow-pass vlan 2 to 3
[SW1-GigabitEthernet0/0/2] quit
```

SW1---HUB 交换机---PC，接口配置成 access 模式

```
[SW1] interface GigabitEthernet 0/0/3
[SW1-GigabitEthernet0/0/3] port link-type access   //链路类型为 access
[SW1-GigabitEthernet0/0/3] port default vlan 4
[SW1-GigabitEthernet0/0/3] quit
```

SW1---R 路由器，可以配置成 access 模式

```
[SW1] interface GigabitEthernet 0/0/1
[SW1-GigabitEthernet0/0/1] port link-type access        //链路类型为 access
[SW1-GigabitEthernet0/0/1] port default vlan 5
```

3.配置 IP 地址做为 PC 电脑的网关

```
[SW1] interface Vlanif 2                                   //进入三层 vlanif2 接口
[SW1-Vlanif2] ip address 192.168.2.1 255.255.255.0    //配置 ip 地址
[SW1-Vlanif2] quit                                         //退出 vlanif2 接口
[SW1] interface Vlanif 3
[SW1-Vlanif3] ip address 192.168.3.1 255.255.255.0
[SW1-Vlanif3] quit
[SW1] interface Vlanif 4
[SW1-Vlanif4] ip address 192.168.4.1 255.255.255.0
```

4.配置 ip 地址实现和 R 路由器互联

```
[SW1] interface Vlanif 5
[SW1-Vlanif5] ip address 192.168.5.1 24            //对接 R 路由器的互联 IP 地址
```

5.配置完成后保存配置

```
<SW1> save
```

接入层交换机 SW2 配置：

1.创建 vlan

```
<Huawei> system-view                    //进入系统模式
[Huawei] sysname SW2                    //修改系统名从 Huawei 修改为 SW2（可选）
[SW2] vlan 2                            //新建 vlan 2
[SW2-vlan2] quit                        //退出 vlan 2
[SW2] vlan 3
[SW2-vlan3] quit
```

2.接口透传 vlan

SW2----SW1，接口配置成 trunk 模式

```
[SW2] interface GigabitEthernet 0/0/1
[SW2-GigabitEthernet0/0/1] port link-type trunk     //配置链路类型为 trunk
[SW2-GigabitEthernet0/0/1] port trunk allow-pass vlan 2 to 3
[SW2-GigabitEthernet0/0/1] quit
```

SW2---PC，接口需要配置成 access 模式

```
[SW2] interface GigabitEthernet 0/0/23              //对接 PC1
[SW2-GigabitEthernet0/0/23] port link-type access   //链路类型为 access
[SW2-GigabitEthernet0/0/23] port default vlan 2
[SW2-GigabitEthernet0/0/23] quit
[SW2] interface GigabitEthernet 0/0/24              //对接 PC2
[SW2-GigabitEthernet0/0/24] port link-type access
[SW2-GigabitEthernet0/0/24] port default vlan 3
[SW2-GigabitEthernet0/0/24] quit
```

3.配置完成后保存配置

```
<SW2> save
```

2.5 配置基于接口划分vlan示例二（接入层设备作为网关）

组网需求

如图 2-5 所示，S1 作为汇聚层交换机，S2、S3 作为 PC 电脑的网关设备下连 PC 电脑或 HUB 交换机；PC1 属于 vlan2 直连 SW2，网关为 vlanif 2 接口地址 192.168.2.1/24；PC2 属于 vlan 3 通过 hub 接入到 SW2，网关为 vlanif3 接口地址 192.168.3.1/24；PC3 和 PC4 属于 vlan 4 直连 S3，网关为

vlanif 4 接口地址 192.168.4.1/24；通过配置实现各 PC 电脑之间互访；

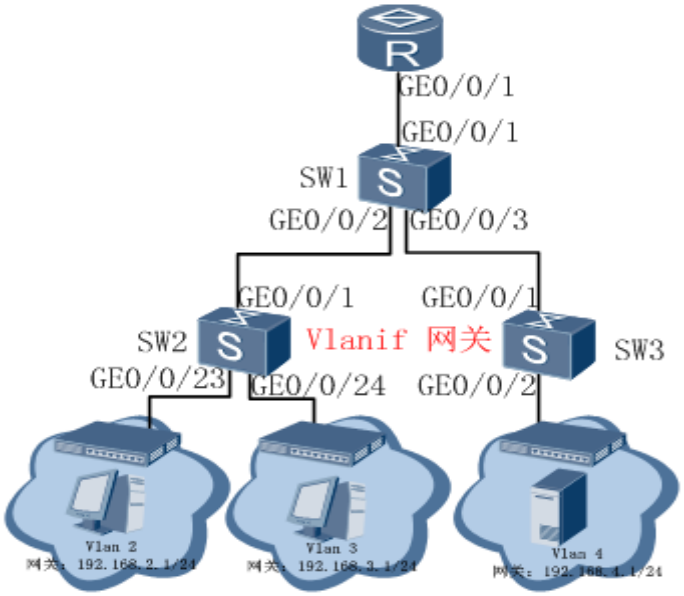


图 2-5　接入层做网关基于接口划分 vlan 组网

配置思路：

采用如下的思路配置 VLAN 间互通：

1． 创建 VLAN 并将连接用户的接口加入 VLAN，实现不同业务用户之间的二层流量隔离。

2． 配置各 PC 电脑的网关 IP 地址，实现相同业务用户之间三层互通

3． 配置静态路由实现不同业务用户之间三层互通

详细配置步骤：

SW2 配置如下：

1．创建 vlan

```
<SW2> system-view                                    //进入系统模式
[SW2] vlan batch 2 to 3                              //批量创建 vlan 2 和 3
[SW2] vlan 5                                         //新建 vlan 5
[SW2-vlan5] quit                                     //退出 vlan 5
```

2.接口加入到相应 vlan

```
# SW2-----PC
[SW2] interface GigabitEthernet 0/0/3                //对接 PC1
[SW2-GigabitEthernet0/0/3] port link-type access     //链路类型为 access
[SW2-GigabitEthernet0/0/3] port default vlan 2
[SW2-GigabitEthernet0/0/3] quit
[SW2] interface GigabitEthernet 0/0/2                //对接 PC2
[SW2-GigabitEthernet0/0/2] port link-type access
[SW2-GigabitEthernet0/0/2] port default vlan 3
```

```
[SW2-GigabitEthernet0/0/2] quit
```

SW2---SW1

```
[SW2] interface GigabitEthernet 0/0/1                //对接 SW1
[SW2-GigabitEthernet0/0/1] port link-type access
[SW2-GigabitEthernet0/0/1] port default vlan 5
[SW2-GigabitEthernet0/0/1] quit
```

3.配置 ip 地址作为 PC 电脑的网关 IP 地址

```
[SW2] interface Vlanif 2                             //系统视图下进入三层 vlanif 2 接口
[SW2-Vlanif2] ip address 192.168.2.1 255.255.255.0     //配置 PC1 的网关地址
[SW2-Vlanif2] quit                                   //退出 vlanif 接口视图
[SW2] interface Vlanif 3
[SW2-Vlanif3] ip add 192.168.3.1 24
[SW2-Vlanif3] quit
```

4.配置 ip 地址实现 SW2 和 SW1 互联

```
[SW2] interface Vlanif 5
[SW2-Vlanif5] ip address 192.168.5.2 24              //互联接口 IP 地址
[SW2-Vlanif5] quit
```

5.配置静态路由，为 SW2 下 PC 网段出去指路

```
[SW2] ip route-static 0.0.0.0 0.0.0.0 192.168.5.1 //配置默认路由出去，下一跳为对端 SW1 的接口地址 192.168.5.1
```

6.配置完成后保存配置

```
<SW2> save
```

SW3 配置如下：

1.创建 vlan

```
<SW3> system-view                                    //进入系统模式
[SW3] vlan 4                                         //新建 vlan 4
[SW3-vlan4] quit                                     // 退出 vlan 4
[SW3] vlan 5
[SW3-vlan5] quit
```

2.接口加入到相应 vlan

SW2-----PC

```
[SW3] interface Ethernet 0/0/1                       //接 PC 电脑
[SW3-Ethernet0/0/1] port link-type access            //链路类型为 access
```

```
[SW3-Ethernet0/0/1] port default vlan 4
[SW3-Ethernet0/0/1] quit
```

SW3---SW1

```
[SW3] interface GigabitEthernet 0/0/1                    //对接 SW1
[SW3-GigabitEthernet0/0/1] port link-type access         //链路类型为 access
[SW3-GigabitEthernet0/0/1] port default vlan 5
[SW3-GigabitEthernet0/0/1] quit
```

3.配置 IP 地址作为 PC 电脑的网关 IP 地址

```
[SW3] interface Vlanif 4                              //系统视图进入 vlanif4 三层接口
[SW3-Vlanif4] ip address 192.168.4.1 24               //配置 PC3 和 PC4 的网关地址
[SW3-Vlanif4] quit
```

4.配置 ip 地址实现 SW3 和 SW1 互联

```
[SW3] interface Vlanif 5
[SW3-Vlanif5] ip address 192.168.5.3 24                  //互联接口 IP 地址
[SW3-Vlanif5] quit
```

5.配置静态路由，为 SW3 下 PC 网段出去指路

```
[SW3] ip route-static 0.0.0.0 0.0.0.0 192.168.5.1    //配置默认路由出去，下一跳为对端 SW1 的接口地址 192.168.5.1
```

6.配置完成后保存配置

```
<SW3> save
```

SW1 配置：

1.创建 vlan

```
<SW1> system-view                                        //进入系统模式
[SW1] vlan 5                                             //新建 vlan 5
[SW1-vlan5] quit                                         //退出 vlan5 模式
```

2.接口加入到相应 vlan 配置

```
[SW1] interface GigabitEthernet 0/0/2                    //对接 SW2
[SW1-GigabitEthernet0/0/2] port link-type access         //链路类型为 access
[SW1-GigabitEthernet0/0/2] port default vlan 5           //透传 vlan5
[SW1-GigabitEthernet0/0/2] quit                          //退出接口 GE0/0/5
[SW1] interface GigabitEthernet 0/0/24                   //对接 SW3
[SW1-GigabitEthernet0/0/24] port link-type access
[SW1-GigabitEthernet0/0/24] port default vlan 5
[SW1-GigabitEthernet0/0/24] quit
```

```
[SW1] interface  GigabitEthernet 0/0/1                    //对接 R 路由器
[SW1-GigabitEthernet0/0/1] port link-type access
[SW1-GigabitEthernet0/0/1] port default vlan 5
[SW1-GigabitEthernet0/0/1] quit
```

3．配 IP 地址，作为对接 SW2、SW3 及 R 路由器的互联接口地址

```
[SW1] interface Vlanif 5                                  //进入三层接口 vlanif5
[SW1-Vlanif5] ip address 192.168.5.1 24                   //配置 ip 地址
[SW1-Vlanif5] quit                                        //退出 vlanif 5
```

4.配置静态路由

配置回程明细路由，实现内网网段之间互访

```
[SW1] ip route-static 192.168.2.0 255.255.255.0 192.168.5.2
[SW1] ip route-static 192.168.3.0 255.255.255.0 192.168.5.2
[SW1] ip route-static 192.168.4.0 255.255.255.0 192.168.5.3
```

配置默认路由实现内网网段到 R 实现上网，假设对端接口地址为 192.168.5.4

```
[SW1] ip route-static 0.0.0.0 0.0.0.0 192.168.5.4
```

5.配置完成后保存配置

```
<SW1> save
```

2.6 同一VLAN相同网段之间限制互访之端口隔离

组网需求：

某企业研发办公室员工分为本公司员工、A合作方公司员工和B合作方公司员工。如下图2-6所示，PC1和PC2分别代表A、B合作方员工，PC3代表本公司研发员工，公司希望在节省VLAN资源的前提下，实现本公司员工和A、B两个合作方公司之间可以相互通信，但是A、B两个合作方公司员工之间无法通信。

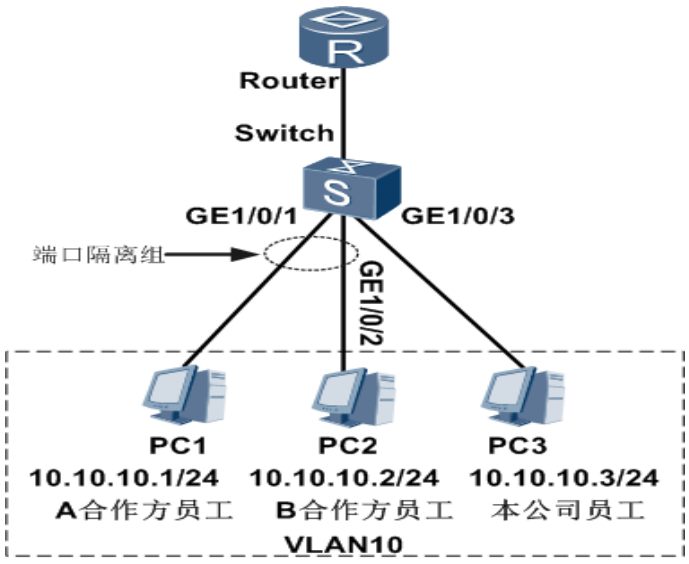


图2-6 配置端口隔离示例组网图

配置思路

采用如下的思路配置端口隔离：

1． 配置接口加入 VLAN。

2． 设备缺省端口隔离为二层隔离三层互通，只需要将接口加入到隔离组中，就可以实现隔离组内接口之间二层数据的隔离。

详细配置步骤：

1． 配置端口隔离功能

配置 GE0/0/1 的端口隔离功能。

```
<HUAWEI> system-view
[HUAWEI] vlan 10
[HUAWEI-vlan10] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type access
[HUAWEI-GigabitEthernet0/0/1] port default vlan 10
[HUAWEI-GigabitEthernet0/0/1] port-isolate enable          //配置端口隔离功能
[HUAWEI-GigabitEthernet0/0/1] quit
```

配置 GE0/0/2 的端口隔离功能。

```
[HUAWEI] interface gigabitethernet 0/0/2
[HUAWEI-GigabitEthernet0/0/2] port link-type access
[HUAWEI-GigabitEthernet0/0/2] port default vlan 10
[HUAWEI-GigabitEthernet0/0/2] port-isolate enable              //配置端口隔离功能
[HUAWEI-GigabitEthernet0/0/2] quit
```

配置 GE0/0/3 加入 VLAN10。

```
[HUAWEI] interface gigabitethernet 0/0/3
[HUAWEI-GigabitEthernet0/0/3] port link-type access
[HUAWEI-GigabitEthernet0/0/3] port default vlan 10
[HUAWEI-GigabitEthernet0/0/3] quit
```

2.7 配置VLAN聚合示例

组网需求：

某公司拥有多个部门且位于同一网段，为了提升业务安全性，将不同部门的用户划分到不同 VLAN 中。现由于业务需要，不同部门间的用户需要互通。如图 2-7 所示，VLAN2 和 VLAN3 为不同部门，现需要实现不同 VLAN 间的用户可以互相访问。可以在 Switch 上部署 VLAN 聚合，实现 VLAN2 和 VLAN3 二层隔离、三层互通，同时 VLAN2 和 VLAN3 采用同一个子网网段，节省了 IP 地址。

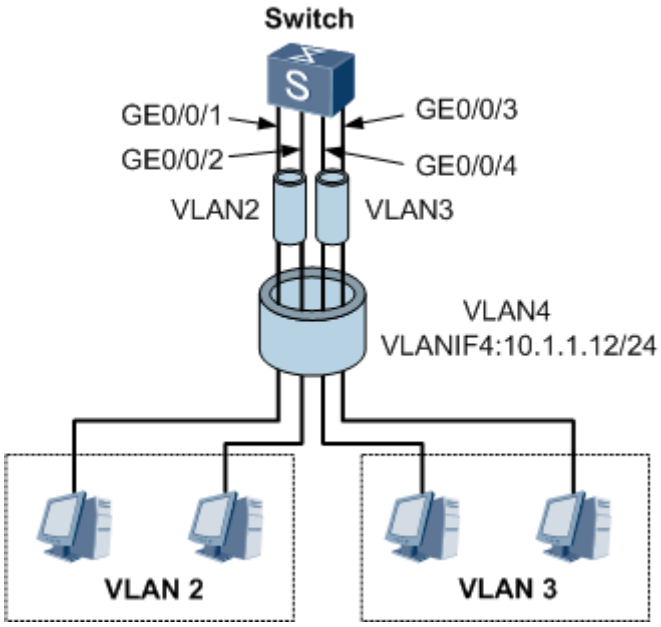


图2-7 配置VLAN聚合组网图

配置思路：

采用如下思路配置 VLAN 聚合：

1． 把 Switch 接口加入到相应的 sub-VLAN 中，实现不同 sub-VLAN 间的二层隔离。

2． 把 sub-VLAN 聚合为 super-VLAN。

3． 配置 VLANIF 接口的 IP 地址。

4． 配置 super-VLAN 的 Proxy ARP，实现 sub-VLAN 间的三层互通。

详细操作步骤：

1． 配置接口类型

配置接口 GE0/0/1 为 Access 类型。接口 GE0/0/2、GE0/0/3、GE0/0/4 配置与 GE0/0/1 相同，不再赘述。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] interface gigabitethernet 0/0/1
[Switch-GigabitEthernet0/0/1] port link-type access
[Switch-GigabitEthernet0/0/1] quit
```

2． 创建 sub-vlan

创建 VLAN2 并向 VLAN2 中加入 GE0/0/1 和 GE0/0/2。

```
[Switch] vlan 2                                          //创建 sub-vlan 2
[Switch-vlan2] port gigabitethernet 0/0/1 0/0/2     //将接口加入到 vlan 中
[Switch-vlan2] quit
```

创建 VLAN3 并向 VLAN3 中加入 GE0/0/3 和 GE0/0/4。

```
[Switch] vlan 3                                          //创建 sub-vlan 3
[Switch-vlan3] port gigabitethernet 0/0/3 0/0/4          //将接口加入到 vlan 中
[Switch-vlan3] quit
```

3. 配置 super-vlan，把 sub-vlan 加入到 super-vlan

```
 [Switch] vlan 4
[Switch-vlan4] aggregate-vlan                            //配置 vlan4 为 super vlan
[Switch-vlan4] access-vlan 2 to 3                        //将 Sub-VLAN 加入 Super-VLAN
[Switch-vlan4] quit
```

配置 super-vlan 的 VLANIF 接口地址，所有 sub-vlan 共有 super-vlan 的接口地址

```
[Switch] interface vlanif 4
[Switch-Vlanif4] ip address 10.1.1.12 255.255.255.0//配置 IP 地址作为 PC 的网关
[Switch-Vlanif4] quit
```

4. 配置 Proxy ARP ，必须配置此步骤 vlan2 和 vlan3 之间才能互访

```
[Switch] interface vlanif 4
[Switch-Vlanif4] arp-proxy inter-sub-vlan-proxy enable    //配置 ARP 代理
[Switch-Vlanif4] quit
```

2.8 部分VLAN间互通、部分VLAN间隔离、VLAN内用户隔离

组网需求

在企业网络中，企业所有员工都可以访问企业的服务器。但对于企业来说，希望企业内部部分员工之间可以互相交流，而部分员工之间是隔离的，不能够互相访问。

要求所有 HOST 都可以访问服务器（Server），即 VLAN3 和 VLAN4 可以访问 VLAN2。

HOSTB 和 HOSTC 之间可以互访，和 HOSTC、HOSTE 不能互访，即 VLAN3 和 VLAN4 不能互访。

HOSTC 和 HOSTE 之间隔离，不能互访，即 VLAN4 内用户不能互访。

如图 2-8 所示，为了解决上述问题，可在连接终端的交换机上部署 MUX VLAN 特性。MUX VLAN 不但能够实现企业需求，同时也解决了 VLAN ID 紧缺问题，也便于网络管理者维护。

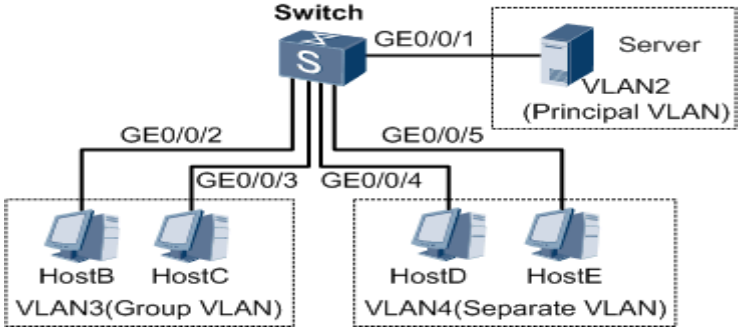


图2-8 配置MUX-VLAN组网图

配置思路

采用如下思路配置 MUX-VLAN 功能：

1． 配置主 VLAN 的 MUX-VLAN 功能。

2． 配置 Group-VLAN 功能,，Group VLAN 可以和 Principal VLAN 和本 VLAN 内互通。

3． 配置 Separate-VLAN 功能,，Separate VLAN 只能和 Principal VLAN 互通，本 VLAN 内不能互通。

4． 配置接口加入 VLAN 并使能 MUX-VLAN 功能。

操作步骤

1． 配置 MUX VLAN

创建 VLAN2、VLAN3 和 VLAN4。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] vlan batch 2 3 4
```

配置 MUX VLAN 中的 Group VLAN 和 Separate VLAN。

```
[Switch] vlan 2
[Switch-vlan2] mux-vlan                  //配置该 VLAN 为 MUX VLAN,即 Principal VLAN
[Switch-vlan2] subordinate group 3    //配置/Group VLAN
[Switch-vlan2] subordinate separate 4    //配置 Separate VLAN
[Switch-vlan2] quit
```

配置接口加入 VLAN 并使能 MUX VLAN 功能。

```
[Switch] interface gigabitethernet 0/0/1
[Switch-GigabitEthernet0/0/1] port link-type access
[Switch-GigabitEthernet0/0/1] port default vlan 2 //Principal VLAN 可以和所有 VLAN 互通
[Switch-GigabitEthernet0/0/1] port mux-vlan enable vlan 2  //接口使能 mux-vlan
[Switch-GigabitEthernet0/0/1] quit
[Switch] interface gigabitethernet 0/0/2
[Switch-GigabitEthernet0/0/2] port link-type access
[Switch-GigabitEthernet0/0/2] port default vlan 3
[Switch-GigabitEthernet0/0/2] port mux-vlan enable vlan 3  //接口使能 mux-vlan
[Switch-GigabitEthernet0/0/2] quit
[Switch] interface gigabitethernet 0/0/3
[Switch-GigabitEthernet0/0/3] port link-type access
[Switch-GigabitEthernet0/0/3] port default vlan 3
```

```
[Switch-GigabitEthernet0/0/3] port mux-vlan enable vlan 3  //接口使能 mux-vlan
[Switch-GigabitEthernet0/0/3] quit
[Switch] interface gigabitethernet 0/0/4
[Switch-GigabitEthernet0/0/4] port link-type access
[Switch-GigabitEthernet0/0/4] port default vlan 4
[Switch-GigabitEthernet0/0/4] port mux-vlan enable vlan 4  //接口使能 mux-vlan
[Switch-GigabitEthernet0/0/4] quit
[Switch] interface gigabitethernet 0/0/5
[Switch-GigabitEthernet0/0/5] port link-type access
[Switch-GigabitEthernet0/0/5] port default vlan 4
[Switch-GigabitEthernet0/0/5] port mux-vlan enable vlan 4  //接口使能 mux-vlan
[Switch-GigabitEthernet0/0/5] quit
```

2.9 限制内网网段间互访

组网需求

如图 2-9 所示，公司企业网通过 Switch 实现各部门之间的互连，不同部门在不同的 vlan 及网段下。要求正确配置 ACL，禁止研发部门和市场部门在上班时间（8:00 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。

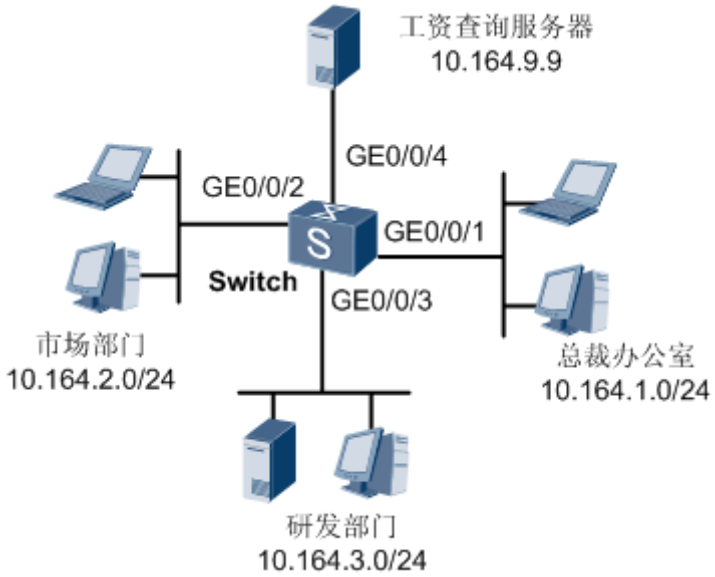


图2-9 应用高级ACL配置流分类组网图

配置思路

采用如下的思路配置 ACL：

1. 配置接口 IP 地址。
2. 配置时间段。

3． 配置 ACL。

4． 配置流分类。

5． 配置流行为。

6． 配置流策略。

7． 在接口上应用流策略。

详细配置步骤

1． 配置接口 IP 地址

配置接口加入 VLAN，并配置 VLANIF 接口的 IP 地址。

规划 GE0/0/1～GE0/0/3 分别加入 VLAN10、20、30，GE0/0/4 加入 VLAN100。VLANIF 接口的地址取所在网段的第一个 IP 地址。下面配置以 GE0/0/1 接口为例，其他接口的配置与此类似，不再赘述。

```
<HUAWEI> system-view
[HUAWEI] vlan batch 10 20 30 100                        //批量创建 vlan
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type access    //连终端接口类型为 access
[HUAWEI-GigabitEthernet0/0/1] port default vlan 10
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] interface vlanif 10                             //进入三层 vlanif 接口
[HUAWEI-Vlanif10] ip address 10.164.1.1 255.255.255.0//配置 vlan 下网段 IP 地址
[HUAWEI-Vlanif10] quit
```

2． 配置时间段

配置 8:00 至 17:30 的周期时间段。

```
[HUAWEI] time-range satime 8:00 to 17:30 working-day
```

3． 配置 ACL

配置市场部门到工资查询服务器的访问规则。

```
[HUAWEI] acl 3002
[HUAWEI-acl-adv-3002] rule deny ip source 10.164.2.0 0.0.0.255 destination
10.164.9.9 0.0.0.0 time-range satime                    //acl 访问规则调用时间段
[HUAWEI-acl-adv-3002] quit
```

配置研发部门到工资查询服务器的访问规则。

```
[HUAWEI] acl 3003
[HUAWEI-acl-adv-3003] rule deny ip source 10.164.3.0 0.0.0.255 destination
10.164.9.9 0.0.0.0 time-range satime                    //acl 访问规则调用时间段
[HUAWEI-acl-adv-3003] quit
```

4． 配置基于 ACL 的流分类

配置流分类 c_market，对匹配 ACL 3002 的报文进行分类。

```
[HUAWEI] traffic classifier c_market                    //市场部门流分类
[HUAWEI-classifier-c_market] if-match acl 3002          //匹配市场部门 acl 3002
[HUAWEI-classifier-c_market] quit
```

配置流分类 c_rd，对匹配 ACL 3003 的报文进行分类。

```
[HUAWEI] traffic classifier c_rd                        //研发部门流分类
[HUAWEI-classifier-c_rd] if-match acl 3003              //匹配研发部门 acl 3003
[HUAWEI-classifier-c_rd] quit
```

5． 配置流行为

配置流行为 b_market，动作为拒绝报文通过。

```
[HUAWEI] traffic behavior b_market                      //市场部门流行为
[HUAWEI-behavior-b_market] deny                         //动作为 deny 拒绝
[HUAWEI-behavior-b_market] quit
```

配置流行为 b_rd，动作为拒绝报文通过。

```
[HUAWEI] traffic behavior b_rd                          //研发部门流行为
[HUAWEI-behavior-b_rd] deny                             //动作为 deny 拒绝
[HUAWEI-behavior-b_rd] quit
```

6． 配置流策略

配置流策略 p_market，将流分类 c_market 与流行为 b_market 关联。

```
[HUAWEI] traffic policy p_market                                    //市场部门流策
略
[HUAWEI-trafficpolicy-p_market] classifier c_market behavior b_market //分
类关联行为
[HUAWEI-trafficpolicy-p_market] quit
```

配置流策略 p_rd，将流分类 c_rd 与流行为 b_rd 关联。

```
[HUAWEI] traffic policy p_rd                                        //研发部门流策略
[HUAWEI-trafficpolicy-p_rd] classifier c_rd behavior b_rd    //分类关联行为
[HUAWEI-trafficpolicy-p_rd] quit
```

7． 应用流策略

将流策略 p_market 应用到 GE0/0/2 接口。

```
[HUAWEI] interface gigabitethernet 0/0/2
[HUAWEI-GigabitEthernet0/0/2] traffic-policy p_market inbound   //调用市场部
门流策略
[HUAWEI-GigabitEthernet0/0/2] quit
```

将流策略 p_rd 应用到 GE0/0/3 接口。

```
[HUAWEI] interface gigabitethernet 0/0/3
[HUAWEI-GigabitEthernet0/0/3] traffic-policy p_rd inbound//调用研发部门流策略
[HUAWEI-GigabitEthernet0/0/3] quit
```

3 DHCP配置

一、功能简介

为了实现网络可以动态合理地分配 IP 地址给主机使用，需要用到动态主机配置协议 DHCP（Dynamic Host Configuration Protocol）。DHCP 技术实现了计算机快速、动态地获取 IP 地址功能，提高了 IP 地址的使用效率。根据客户端的实际需要，IP 地址分配方式可以选择动态分配或静态绑定方式。

- 动态分配方式：DHCP 服务器从地址池中选择一个可用的 IP 地址分配给客户端。这种方式一般适用于对 IP 地址没有特殊要求的客户端，通常也称这类客户端为动态客户端。
- 静态绑定方式：DHCP 服务器分配某固定 IP 地址给固定客户端，通过在地址池中配置客户端的 MAC 地址与 IP 地址的绑定来实现。这种方式一般适用于对 IP 地址有特殊要求的客户端，通常也称这类客户端为静态客户端。

二、 配置命令和步骤

配置全局地址池及网络参数：

1. 执行命令 **ip pool** *ip-pool-name*，系统视图下创建全局地址池，同时进入全局地址池视图。
2. 执行命令 **network** *ip-address* [**mask** { *mask* | *mask-length* }]，配置全局地址池可动态分配的 IP 地址范围。
3. 执行命令 **gateway-list** *ip-address* &<1-8>，配置 DHCP 客户端的出口网关地址。
4. 执行命令 **dns-list** *ip-address* &<1-8>，配置 DHCP 客户端使用的 DNS 服务器的 IP 地址
5. 执行命令 **static-bind ip-address** *ip-address* **mac-address** *mac-address*，采用静态地址绑定方式将全局地址池中的 IP 地址与 DHCP 客户端的 MAC 地址绑定。
6. 执行命令 **lease** { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** }，配置 IP 地址租期，缺省情况下，IP 地址的租期为 1 天。
7. 执行命令 **excluded-ip-address** *start-ip-address* [*end-ip-address*]，配置地址池中不参与自动分配的 IP 地址保留以分配给其他的服务。
8. 执行命令 **lock**，锁定 IP 地址池。

配置接口工作在全局地址池模式：

9. 执行命令 **dhcp enable**，系统视图下使能 DHCP 服务。
10. 执行命令 **dhcp select global**，接口视图下使能接口采用全局地址池的 DHCP 服务器功能。

配置接口地址池操作步骤

1. 执行命令 **dhcp enable**，系统视图下使能 DHCP 服务。

2. 执行命令 **dhcp select interface**，接口视图下使能接口采用接口地址池的 DHCP 服务器功能。
3. 执行命令 **dhcp server lease** { day day [hour hour [minute minute]] | unlimited }，配置 IP 地址租期，缺省情况下，IP 地址的租期为 1 天。
4. 执行命令 **dhcp server excluded-ip-address** start-ip-address [end-ip-address]，配置地址池中不参与自动分配的 IP 地址保留以分配给其他的服务。
5. 执行命令 **dhcp server static-bind ip-address** ip-address **mac-address** mac-address，采用静态地址绑定方式将接口地址池中的 IP 地址与 MAC 地址绑定。
6. 执行命令 **dhcp server dns-list** ip-address &<1-8>，为 DHCP 客户端指定 DNS 服务器的 IP 地址。

三.应用场景

3.1 同网段内配置基于VLANIF接口地址池的DHCP服务器示例

组网需求

如图一所属，某企业有两个处于同一网络内的办公室，为了节省资源，两个办公室内的主机由 Switch1 作为 DHCP 服务器统一分配 IP 地址。楼层一所属的网段为 192.168.2.0/24，主机都加入 vlan 2，（可选：地址租期为 30 天）；楼层二所属的网段为 192.168.3.0/24，主机都加入 vlan 3，（可选：地址租期为 20 天）；DNS 为 183.221.253.100（运营商 DNS）；

注：楼层交换机 SW2 和 SW3 都作为 HUB 交换机使用，无需任何配置，即插即用；

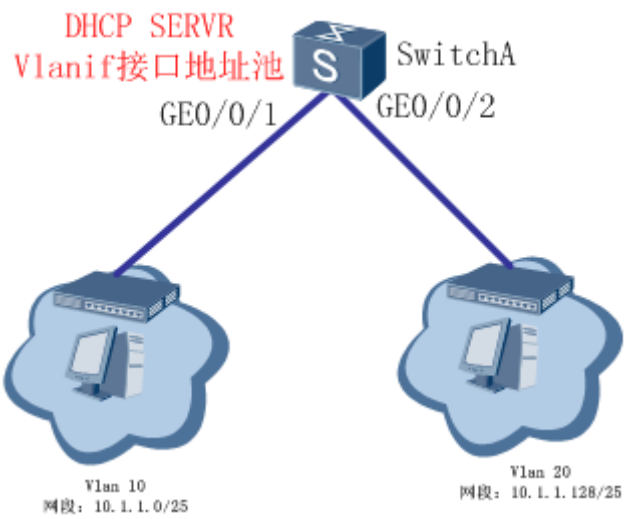


图3-1配置基于VLANIF接口地址池的DHCP服务器组网图

配置思路

基于 VLANIF 接口地址池的 DHCP 服务器的配置思路如下：

1. 在 Switch1 上创建两个接口地址池并配置地址池相关属性，实现 DHCP 服务器可以根据不同需求，从不同的接口地址池中选择合适的 IP 地址及其配置参数分配给办公室主机。

2． 在 Switch1 上配置 VLANIF 接口基于接口地址池的地址分配方式，实现 DHCP 服务器从基于接口的地址池中选择 IP 地址分配给办公室主机。

详细配置步骤步骤

SW1 配置如下：

1、创建 vlan

```
<SW1> system-view                                    //进入系统模式
[SW1] vlan batch 2 to 3                              //新建 vlan
```

2、使能 dhcp 服务

```
[SW1] dhcp enable                                    //系统视图下使能 dhcp 服务
```

3、 配置 vlanif 接口地址作为 dhcp 地址池给 PC 电脑分配 IP 地址

```
[SW1] interface Vlanif 2                             //系统视图进入 vlanif2 接口
[SW1-Vlanif2] ip address 192.168.2.1 24              //配置 PC 电脑的网关地址
[SW1-Vlanif2] dhcp select  interface                 //使能接口地址池 dhcp 服务功能
[SW1-Vlanif2] dhcp server dns-list 183.221.253.100       //配置 DNS
[SW1-Vlanif2] dhcp server lease day 30               //配置 dhcp 地址的租期为 30 天
[SW1] interface Vlanif 3
[SW1-Vlanif3] ip address 192.168.3.1 24
[SW1-Vlanif3] dhcp select interface
[SW1-Vlanif3] dhcp server dns-list 183.221.253.100
[SW1-Vlanif3] dhcp server lease day 20
```

4、SW1----SW2，SW1----SW3，接口加入相应 vlan

```
[SW1] interface GigabitEthernet 0/0/2                //对接 SW2 交换机
[SW1-GigabitEthernet0/0/2] port link-type access
[SW1-GigabitEthernet0/0/2] port default vlan 2
[SW1] interface GigabitEthernet 0/0/3                //对接 SW3 交换机
[SW1-GigabitEthernet0/0/3] port link-type access
[SW1-GigabitEthernet0/0/3] port default vlan 3
```

5、SW2、SW3 为接入 HUB 交换机可以不用配置，即插即用

3.2 同网段内配置基于全局地址池的DHCP服务器示例一

组网需求

如图 3-2 所示，某企业有两个处于同一网络内的办公室，为了节省资源，两个办公室内的主机由 SwitchA 作为 DHCP 服务器统一分配 IP 地址。

办公室 1 所属的网段为 10.1.1.0/25，主机都加入 VLAN10，地址租期为 10 天；办公室 2 所属的网段为 10.1.1.128/25，主机都加入 VLAN20，地址租期为 2 天。

在 SwitchA 上配置全局地址池，并采取动态地址分配方式为两个办公室的主机分配 IP 地址。

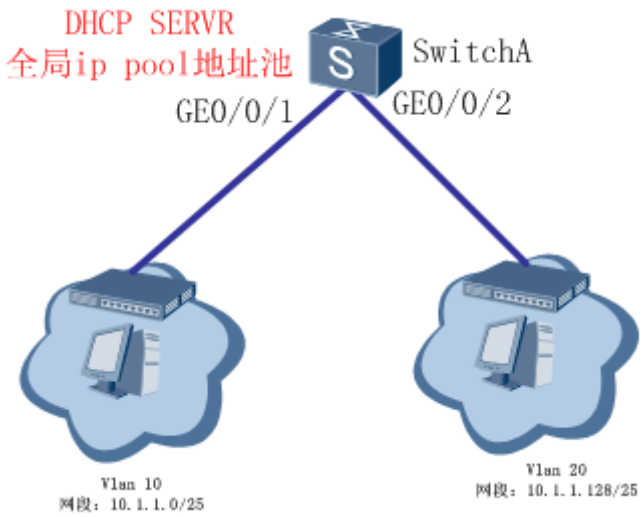


图3-2 配置基于全局地址池的DHCP服务器组网图

配置思路：

基于 VLANIF 接口地址池的 DHCP 服务器的配置思路如下：

1． 在 SwitchA 上创建两个接口地址池并配置地址池相关属性，实现 DHCP 服务器可以根据不同需求，从不同的接口地址池中选择合适的 IP 地址及其配置参数分配给办公室主机。

2． 在 SwitchA 上配置 VLANIF 接口基于接口地址池的地址分配方式，实现 DHCP 服务器从基于接口的地址池中选择 IP 地址分配给办公室主机。

详细配置步骤：

1、启动 dhcp 服务

```
<SwitchA> system-view                                    //进入系统模式
[SwitchA] dhcp enable                                    //使能 dhcp 服务器
```

2、创建地址池并配置相关属性

配置 IP 地址池 1 的属性（地址池范围、DNS 地址、出口网关、不参与分配的地址和地址池租期），IP 地址池 1 给办公室 1 的 PC 电脑分配 IP 地址

```
[SwitchA] ip pool 1                                      //系统视图下创建 IP pool
[SwitchA-ip-pool-1] network 10.1.1.0 mask 255.255.255.128  //地址池范围
[SwitchA-ip-pool-1] dns-list 10.1.1.1                    //配置 DNS
[SwitchA-ip-pool-1] gateway-list 10.1.1.1                //配置 PC 电脑网关
[SwitchA-ip-pool-1] excluded-ip-address 10.1.1.2         //保留 IP 地址
[SwitchA-ip-pool-1] excluded-ip-address 10.1.1.4         //保留 IP 地址
[SwitchA-ip-pool-1] lease lease day 10                   // 租期
[SwitchA-ip-pool-1] quit
```

配置 IP 地址池 2 的属性（地址池范围、DNS 地址、出口网关、不参与分配的地址和地址池租期），IP 地址池 2 给办公室 1 的 PC 电脑分配 IP 地址

```
[SwitchA] ip pool 2
[SwitchA-ip-pool-2] network 10.1.1.128 mask 255.255.255.128
[SwitchA-ip-pool-2] dns-list 10.1.1.129
[SwitchA-ip-pool-2] gateway-list 10.1.1.129
[SwitchA-ip-pool-2] lease day 2
[SwitchA-ip-pool-2] quit
```

3、配置 VLANIF 接口下地址分配方式

配置接口 GigabitEthernet0/0/1 和 GigabitEthernet0/0/2 分别加入相应的 VLAN。SW---HUB—PC,SW---PC，配成 access 模式

```
[SwitchA] vlan batch 10 20
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port link-type access
[SwitchA-GigabitEthernet0/0/1] port default vlan 10
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface GigabitEthernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] port link-type access
[SwitchA-GigabitEthernet0/0/2] port default vlan 20
[SwitchA-GigabitEthernet0/0/2] quit
```

配置 VLANIF10 接口下的客户端从全局地址池 ip pool 1 中获取 IP 地址。

```
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] ip address 10.1.1.1 255.255.255.128
[SwitchA-Vlanif10] dhcp select global                    //全局 dhcp 服务器
[SwitchA-Vlanif10] quit
```

配置 VLANIF20 接口下的客户端从全局地址池 ip pool 2 中获取 IP 地址。

```
[SwitchA] interface vlanif 20
[SwitchA-Vlanif20] ip address 10.1.1.129 255.255.255.128
[SwitchA-Vlanif20] dhcp select global                    //全局 dhcp 服务器
[SwitchA-Vlanif20] quit
```

3.3 同网段内配置基于全局地址池的DHCP服务器示例二

组网需求

如图 3-3 所示，IP Phone 和 PC 为某办公区办公设备。为了方便统一管理，降低手工配置成本，管理员希望网络主机通过 DHCP 协议动态获取 IP 地址。其中，PC 为值班室固定终端，需要永久在线，且需

要通过域名访问网络设备，因此，除了动态获取 IP 地址，还需要地址的租期为无限长，且需要获取 DNS 服务器信息；IP Phone 使用固定 IP 地址 10.1.1.4/24，MAC 地址为 dcd2-fc96-e4c0。PC 和 IP Phone 的网关地址为 10.1.1.1/24。

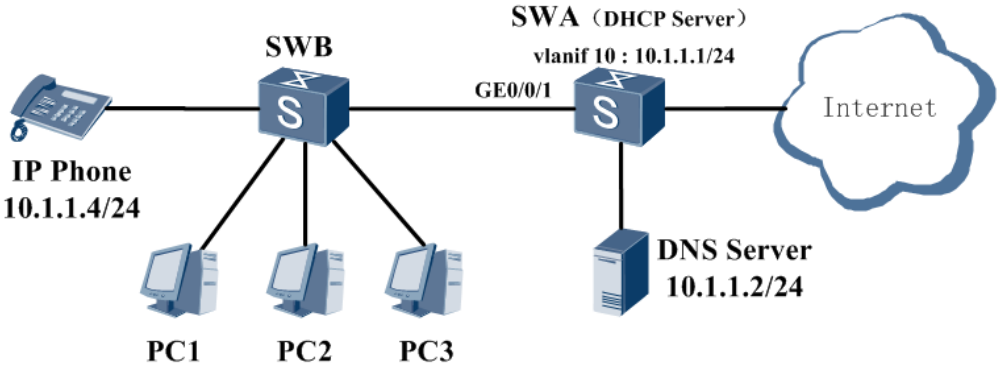


图 3-3　配置基于全局地址池的 DHCP 服务器组网图

配置思路

1．在 SwitchA 上创建 DHCP Option 模板，并在 DHCP Option 模板视图下为静态客户端 IP Phone 配置启动配置文件和获取启动配置文件的网络服务器的地址。

2．在 SwitchA 上创建全局地址池，并在全局地址池视图下为动态客户端 PC 配置租期和 DNS 服务器信息；为静态客户端 IP Phone 配置 IP 地址与 MAC 地址的绑定并绑定 DHCP Option 模板，从而实现为动态客户端和静态客户端分配不同的网络参数。

详细配置步骤

1．　配置接口相应 vlan，SW---HUB---PC，接口配置成 access 模式

```
<SwitchA> system-view
[SwitchA] vlan 10
[SwitchA-vlan10] quit
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet0/0/1] port link-type access
[SwitchA-GigabitEthernet1/0/1] port default vlan 10
[SwitchA-GigabitEthernet1/0/1] quit
```

2．　使能 DHCP 服务。

```
[SwitchA] dhcp enable                                    //全局下使能 DHCP 服务
```

3．　创建地址池并在地址池视图下为 PC 配置网关地址、租期和 DNS 服务器地址；为 IP Phone 配置分配固定 IP 地址。

```
[SwitchA] ip pool pool1                                  //全局模式配置地址池
[SwitchA-ip-pool-pool1] network 10.1.1.0 mask 255.255.255.0  //配置可分配网段
```

```
[SwitchA-ip-pool-pool1] dns-list 10.1.1.2                    //配置内网 DNS 地址
[SwitchA-ip-pool-pool1] gateway-list 10.1.1.1                //配置终端网关
[SwitchA-ip-pool-pool1] excluded-ip-address 10.1.1.2 10.1.1.3  //保留 IP 地址
[SwitchA-ip-pool-pool1] lease unlimited                  //配置 dhcp 租期为永不过期
[SwitchA-ip-pool-pool1]  static-bind  ip-address  10.1.1.4  mac-address
dcd2-fc96-e4c0              //iPhone ip 地址和 mac 地址绑定实现 IPpone 获取固定 IP 地址
[SwitchA-ip-pool-pool1] quit
```

4． 在接口下使能 dhcp 服务。

```
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] ip address 10.1.1.1 255.255.255.0        //配置接口 IP 地址
[SwitchA-Vlanif10] dhcp select global            //使能 dhcp 服务为全局地址池形式
[SwitchA-Vlanif10] quit
```

3.4 基于不同网段内配置DHCP服务器和DHCP中继示例

组网需求

如图 3-4 所示，某公司拥有多个办公地点且位于不同的商务楼宇中，在不同楼宇内的办公室主机在不同的 VLAN 内，公司希望不同办公地点的主机由共同的 DHCP 服务器 SwitchB 分配 IP 地址。公司的办公地点 A 的主机所在的网段为 20.20.20.0/24，而 DHCP 服务器所在的网段为 10.10.10.0/24。通过带 DHCP 中继功能的 SwitchA 转发 DHCP 报文，使得 DHCP 客户端可以从 DHCP 服务器上申请到 IP 地址等相关配置信息。其中 SwitchA 上接口 VLANIF10 的接口地址为 10.10.10.2/24,对端 SwitchB 上接口 VLANIF10 的接口地址为 10.10.10.1/24。

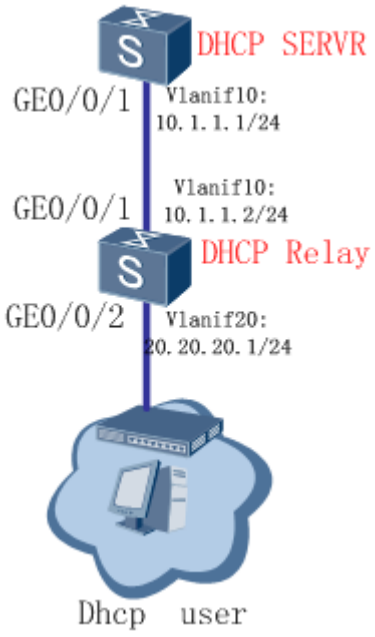


图4 配置DHCP中继组网图

配置思路

1． 在 SwitchA 上配置 DHCP 中继功能，实现 SwitchA 转发不同网段的 DHCP 报文功能。

2． 在 SwitchB 上配置一个 IP 地址范围为 20.20.20.0/24 的全局地址池，实现 DHCP 服务器为不同网段的客户端分配 IP 地址。

详细配置步骤

在 switchA 上配置 dhcp 中继功能

1． 创建 dhcp 服务器组并为服务器组添加 dhcp 服务器。

```
<SwitchA> system-view                                    //进入系统视图
[SwitchA] dhcp server group dhcpgroup1                   //创建 dhcp 服务器组 dhcpgroup1
[SwitchA-dhcp-server-group-dhcpgroup1] dhcp-server 10.10.10.1  //为 dhcp 服务器组 dhcpgroup1 添加 dhcp 服务器 10.10.10.1
[SwitchA-dhcp-server-group-dhcpgroup1] quit
```

2． 在接口下使能 dhcp 中继功能， SWA—PC，链路类型为 access

```
[SwitchA] vlan batch 10 20                               //创建 vlan 10 和 vlan 20
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] port link-type access     //链路类型为access
[SwitchA-GigabitEthernet0/0/2] port default vlan 20
[SwitchA-GigabitEthernet0/0/2] quit
```

3． 在对接 PC 电脑的接口 GE0/0/1 下使能 dhcp 中继功能、绑定 dhcp 服务器组

```
[SwitchA] dhcp enable                                    //全局下使能 dhcp 服务
[SwitchA] interface vlanif 20
[SwitchA-Vlanif20] ip address 20.20.20.1 24              //配置接口 IP 地址
[SwitchA-Vlanif20] dhcp select relay                     //使能 dhcp 中继功能
[SwitchA-Vlanif20] dhcp relay server-select dhcpgroup1   //绑定 dhcp 服务器组 dhcpgroup1
[SwitchA-Vlanif20] quit
```

4． 在 SwitchA 上配置缺省路由下一跳为 SwitchB 的接口地址 10.10.10.1。

```
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] ip address 10.10.10.2 24
[SwitchA-Vlanif10] quit
[SwitchA] ip route-static 0.0.0.0 0.0.0.0 10.10.10.1
```

DHCP Server SWB 配置步骤如下：

1． 接口下相应 vlan 配置

```
<SwitchB> system-view                                    //进入系统视图
[SwitchB] vlan 10
```

```
[SwitchB-vlan10] quit
[SwitchB] interface gigabitethernet 0/0/1
[SwitchB-GigabitEthernet0/0/1] port link-type access        //链路类型为access
[SwitchB-GigabitEthernet0/0/1] port default vlan 10
[SwitchB-GigabitEthernet0/0/1] quit
```

2. 使能 dhcp 功能

```
[SwitchB] dhcp enable                                       //全局下使能 dhcp 服务
[SwitchB] vlan 10
[SwitchB-vlan10] quit
[SwitchB] interface vlanif 10
[SwitchB-Vlanif10] ip address 10.10.10.1 24
[SwitchB-Vlanif10] dhcp select global                       //全局地址池 dhcp 功能
[SwitchB-Vlanif10] quit
```

3. 创建地址池并配置相关属性

```
[SwitchB] ip pool pool1
[SwitchB-ip-pool-pool1] network 20.20.20.0 mask 24
[SwitchB-ip-pool-pool1] gateway-list 20.20.20.1
[SwitchB-ip-pool-pool1] quit
```

4. 在 SwitchB 上配置明细回程路由，下一跳为 SwitchA 的接口地址 10.10.10.2

```
[SwitchB] ip route-static 0.0.0.0 0.0.0.0 10.10.10.2
```

3.5 VRRP组网下同网段内配置基于全局地址池的DHCP服务器示例

组网需求

如图 3-5 所示，某企业内的一台主机通过 Switch 双归属到 SwitchA 和 SwitchB，SwitchA 为主设备，作为 DHCP 服务器为客户端分配 IP 地址。现用户希望当主设备故障时，客户端能够通过备设备重新获取 IP 地址。

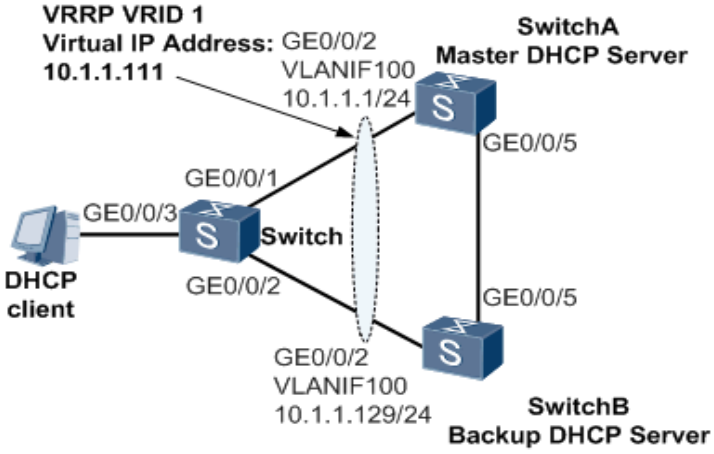


图3-5 VRRP组网下同网段内配置基于全局地址池的DHCP服务器组网图

配置思路

VRRP 组网下同网段内配置基于全局地址池的 DHCP 服务器，配置思路如下：

1、配置 SwitchA 和 SwitchB 设备上接口 IP 地址，使各设备间网络层连通；同时配置 Switch 上的二层透传功能。

2、在 SwitchA 和 SwitchB 上配置 VRRP 备份组。其中，SwitchA 上配置较高优先级，作为 Master 设备为客户端分配 IP 地址；SwitchB 上配置较低优先级，作为备用交换机。

3、在 SwitchA 和 SwitchB 上创建全局地址池，并配置地址池相关属性。

4、在 SwitchA、SwitchB 和 Switch 上配置破环协议，防止环路的产生（此处以配置 STP 为例）。

详细配置步骤

1、配置设备间的网络互连

配置设备各接口的 IP 地址，以 SwitchA 为例。SwitchB 的配置与之类似。

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchA
[SwitchA] vlan batch 100
[SwitchA] interface gigabitethernet 0/0/2                    //下连 Switch 的接口
[SwitchA-GigabitEthernet0/0/2] port link-type access
[SwitchA-GigabitEthernet0/0/2] port default vlan 100
[SwitchA-GigabitEthernet0/0/2] quit
[SwitchA] interface gigabitethernet 0/0/5                    //互联接口
[SwitchA-GigabitEthernet0/0/5] port link-type access
[SwitchA-GigabitEthernet0/0/5] port default vlan 100
[SwitchA-GigabitEthernet0/0/5] quit
[SwitchA] interface vlanif 100
[SwitchA-Vlanif100] ip address 10.1.1.1 24
[SwitchA-Vlanif100] quit
```

配置 Switch 的二层透传功能。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] interface gigabitethernet 0/0/1                     //上连 SwitchA
[Switch-GigabitEthernet0/0/1] port link-type access
[Switch-GigabitEthernet0/0/1] port default vlan 100
[Switch-GigabitEthernet0/0/1] quit
```

```
[Switch] interface gigabitethernet 0/0/2                    //上连 SwitchB
[Switch-GigabitEthernet0/0/2] port link-type access
[Switch-GigabitEthernet0/0/2] portdefault vlan 100
[Switch-GigabitEthernet0/0/2] quit
```

2、创建地址池并配置相关属性

在 SwitchA 上启动 DHCP 服务。

```
[SwitchA] dhcp enable
```

在 SwitchA 上创建地址池，配置地址池范围是 10.1.1.2～10.1.1.128，和 SwitchB 上配置的地址池地址互相排除。

说明： 由于交换机主设备上的地址池信息不能实时备份到备设备上，为防止主备切换后出现 IP 地址分配冲突，主设备和备设备上配置的地址池必须要互相排除。

```
[SwitchA] ip pool 1
[SwitchA-ip-pool-1] network 10.1.1.0 mask 255.255.255.0
[SwitchA-ip-pool-1] gateway-list 10.1.1.111
[SwitchA-ip-pool-1] excluded-ip-address 10.1.1.1
[SwitchA-ip-pool-1] excluded-ip-address 10.1.1.129 10.1.1.254
[SwitchA-ip-pool-1] lease day 10
[SwitchA-ip-pool-1] quit
```

在 SwitchB 上启动 DHCP 服务。

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchB
[SwitchB] dhcp enable
```

在 SwitchB 上创建地址池，配置地址池范围是 10.1.1.130～10.1.1.254，和 SwitchA 上配置的地址池地址互相排除。

```
[SwitchB] ip pool 1
[SwitchB-ip-pool-1] network 10.1.1.0 mask 255.255.255.0
[SwitchB-ip-pool-1] gateway-list 10.1.1.111
[SwitchB-ip-pool-1] excluded-ip-address 10.1.1.1 10.1.1.110
[SwitchB-ip-pool-1] excluded-ip-address 10.1.1.112 10.1.1.129
[SwitchB-ip-pool-1] lease day 10
[SwitchB-ip-pool-1] quit
```

3、配置 VRRP 备份组

在 SwitchA 上创建 VRRP 备份组 1，配置 SwitchA 在该备份组中的优先级为 120，并配置客户端从全局地址池中获取 IP 地址。

```
[SwitchA] interface vlanif 100
[SwitchA-Vlanif100] vrrp vrid 1 virtual-ip 10.1.1.111
[SwitchA-Vlanif100] vrrp vrid 1 priority 120
[SwitchA-Vlanif100] dhcp select global
[SwitchA-Vlanif100] quit
```

在 SwitchB 上创建 VRRP 备份组 1，其在该备份组中的优先级为缺省值 100，并配置客户端从全局地址池中获取 IP 地址。

```
[SwitchB] interface vlanif 100
[SwitchB-Vlanif100] vrrp vrid 1 virtual-ip 10.1.1.111
[SwitchB-Vlanif100] dhcp select global
[SwitchB-Vlanif100] quit
```

4、配置 STP 协议，实现破除环路

在 Switch 上全局使能 STP 功能，SwitchA 和 SwitchB 的配置与之类似。

```
[Switch] stp enable
```

在 Switch 的 GE0/0/3 接口上去使能 STP 并将端口 GE0/0/1 的路径开销值配置为 20000。

```
[Switch] interface gigabitethernet 0/0/3
[Switch-GigabitEthernet0/0/3]port link-type access
[Switch-GigabitEthernet0/0/3]port default vlan 100
[Switch-GigabitEthernet0/0/3] stp disable
[Switch-GigabitEthernet0/0/3] quit
[Switch] interface gigabitethernet 0/0/1
[Switch-GigabitEthernet0/0/1] stp cost 20000
[Switch-GigabitEthernet0/0/1] quit
```

3.6 配置DHCP客户端实例

组网需求

如图 3-6 所示，SwitchA 作为 DHCP 客户端，要求从作为 DHCP 服务器的 SwitchB 中获取动态绑定的 IP 地址、DNS 服务器、网关地址等信息。

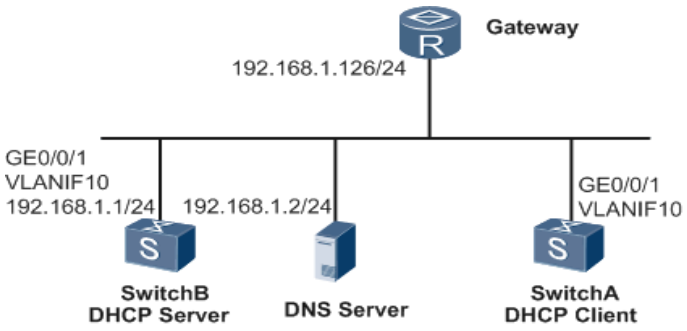


图3-6 配置DHCP客户端组网图

配置思路

DHCP 客户端示例的配置思路如下：

1、在 SwitchA 上使能 DHCP 客户端功能，实现 SwitchA 可以从 DHCP 服务器动态获取 IP 地址。

2、在 SwitchB 上创建 DHCP 服务器的全局地址池并配置相关属性。

详细配置步骤

SwitchA 上配置 DHCP 客户端功能

1、创建 VLAN10 并将 GE0/0/1 接口加入到 VLAN10 中。

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchA
[SwitchA] vlan 10
[SwitchA-vlan10] quit
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port link-type trunk
[SwitchA-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[SwitchA-GigabitEthernet0/0/1] quit
```

2、在 VLANIF10 接口上使能 DHCP 客户端功能。

```
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] ip address dhcp-alloc              //通过 HDCP 自动获取接口 IP 地址
```

在 SwitchB 上创建 DHCP 服务器的全局地址池并配置相关属性

1、使能 DHCP 服务。

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchB
[SwitchB] dhcp enable
```

2、创建 VLAN10 并将 GE0/0/1 接口加入到 VLAN10 中。

```
[SwitchB] vlan 10
[SwitchB-vlan10] quit
[SwitchB] interface gigabitethernet 0/0/1
[SwitchB-GigabitEthernet0/0/1] port link-type trunk
[SwitchB-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[SwitchB-GigabitEthernet0/0/1] quit
```

3、配置 VLANIF10 接口工作在全局地址池模式。

```
[SwitchB] interface vlanif 10
[SwitchB-Vlanif10] ip address 192.168.1.1 24
```

```
[SwitchB-Vlanif10] dhcp select global                    //全局地址池获取 IP 地址
[SwitchB-Vlanif10] quit
```

创建地址池并配置相关属性。

```
[SwitchB] ip pool pool1
[SwitchB-ip-pool-pool1] network 192.168.1.0 mask 24
[SwitchB-ip-pool-pool1] gateway-list 192.168.1.126
[SwitchB-ip-pool-pool1] dns-list 192.168.1.2
[SwitchB-ip-pool-pool1] quit
```

4 DHCP Snooping（网关防假冒）配置

一、功能简介

目前 DHCP 协议在应用的过程中遇到很多安全方面的问题,网络中存在各种针对 DHCP 的攻击,如 DHCP Server 仿冒者攻击、DHCP Server 的拒绝服务攻击、仿冒 DHCP 报文攻击等。

为了保证网络通信业务的安全性，引入了 DHCP Snooping 技术。DHCP Snooping 是 DHCP 的一种安全特性,用于保证 DHCP 客户端从合法的 DHCP 服务器获取 IP 地址,并记录 DHCP 客户端 IP 地址与 MAC 地址等参数的对应关系，防止网络上针对 DHCP 攻击。

二、 配置命令和步骤

1.在系统视图执行命令 **dhcp enable** 开启 DHCP 服务；

2.在系统视图执行命令 **dhcp snooping enable** 开启 DHCP Snooping 功能；

3.在接口或者 VLAN 视图执行命令 **dhcp snooping enable** 开启接口或 VLAN 的 dhcp snooping 功能；

4.把连接合法 DHCP 服务器的接口配置为信任接口，在接口下执行命令 **dhcp snooping trusted** 把接口配置为信任接口，在 VLAN 视图下面执行 **dhcp snooping trusted interface** interface-type interface-number 配置接口为信任接口。

三、应用场景

4.1 配置DHCP Snooping确保终端动态获取的IP地址等信息是合法DHCP服务器分配的

组网需求

如图4-1所示，公司内网(VLAN10)都是通过路由器动态分配地址上网的，在路由器上只做了对内网的192.168.1.0/24网段做地址转换，保证只有这个网段能正常上网；但是由于公司的员工在交换机下面私自接小路由器并开启小路由器的DHCP功能，导致内网其他用户无法正常上网；为了制止这种情况，只有在交换机上面配置DHCP仿冒功能，确保下面用户只从合法的DHCP服务器获取地址。

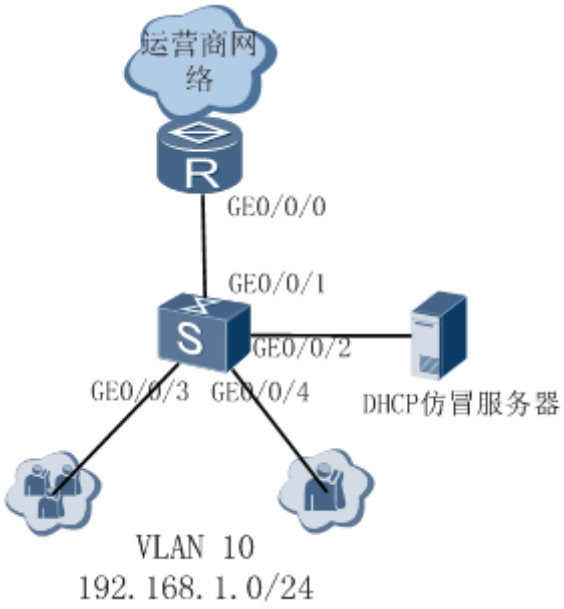


图4-1 防止DHCP仿冒组网图

配置思路

1． 交换机接口和 VLAN 配置

2． 开启交换机的 DHCP Snooping 功能；

3． 把连接合法 DHCP 服务器的接口配置为信任接口；

详细配置步骤

1． 交换机接口和 VLAN 配置

#创建 VLAN10，并把接口 GE0/0/3 和 GE0/0/4 加入到 VLAN10

```
<Huawei> system-view
[Huawei] vlan batch 10
[Huawei] interface GigabitEthernet 0/0/3
[Huawei-GigabitEthernet0/0/3] port link-type access
[Huawei-GigabitEthernet0/0/3] port default vlan 10
[Huawei] interface GigabitEthernet 0/0/4
[Huawei-GigabitEthernet0/0/4] port link-type access
[Huawei-GigabitEthernet0/0/4] port default vlan 10
```

#配置连接路由器的接口为trunk，并透传VLAN10

```
[Huawei] interface GigabitEthernet 0/0/1
[Huawei-GigabitEthernet0/0/1] port link-type access
[Huawei-GigabitEthernet0/0/1] port default vlan 10
```

2． 开启交换机的 DHCP Snooping 功能

```
<Huawei> system-view
```

```
[Huawei] dhcp enable
[Huawei] dhcp snooping enable
```

#开启交换机用户侧接口的 dhcp snooping 功能

```
[Huawei] interface GigabitEthernet 0/0/3
[Huawei-GigabitEthernet0/0/3] dhcp snooping enable
[Huawei] interface GigabitEthernet 0/0/4
[Huawei-GigabitEthernet0/0/4] dhcp snooping enable
```

3． 配置交换机连接合法 DHCP 服务器的接口为信任接口，其他的接口默认为非信任接口

```
[Huawei] interface GigabitEthernet 0/0/1
[Huawei-GigabitEthernet0/0/1] dhcp snooping trusted
[Huawei-GigabitEthernet0/0/1] quit
```

4． 配置完之后需要保存配置

```
<Huawei> save
```

5 IPSG(IP+MAC绑定)配置

一、功能简介

1.IPSG 功能简介

IPSG 功能是基于绑定表（DHCP 动态和静态绑定表）对 IP 报文进行匹配检查。当设备在转发 IP 报文时，将此 IP 报文中的源 IP、源 MAC、接口、VLAN 信息和绑定表的信息进行比较，如果信息匹配，表明是合法用户，则允许此报文正常转发，否则认为是攻击报文，并丢弃该 IP 报文。

2.DHCP Snooping 功能简介

DHCP Snooping 是 DHCP 的一种安全特性，用于保证 DHCP 客户端从合法的 DHCP 服务器获取 IP 地址，并记录 DHCP 客户端 IP 地址与 MAC 地址等参数的对应关系，防止网络上针对 DHCP 攻击，这里主要介绍终端主机通过 DHCP 获取地址，怎么实现 IP 地址、MAC 地址、VLAN 和接口等信息进行动态绑定，以防终端私自修改 IP 地址等信息获取网络访问权限。

二、配置命令和步骤

1.静态绑定表配置（客户端非 DHCP 获取地址）

1）.配置静态用户绑定表项，执行命令 **user-bind static ip-address** ip-address mac-address **mac-address interface** interface-type-number **vlan** vlan-id，四个参数 ip-address、mac-address、interface-type-number 和 vlan-id 四者任意组合；

2）.执行命令 **ip source check user-bind enable**，在接口或者 VLAN 视图下，使能接口或 VLAN 的 IP 报文检查功能。

2.动态绑定表配置（客户端通过 DHCP 获取地址）

1）.执行命令 **dhcp enable**，全局使能 DHCP 功能（在配置 DHCP Snooping 各安全功能之前需首先使能 DHCP Snooping 功能）；

2）.执行命令**dhcp snooping enable**，全局使能 DHCP Snooping 功能；

3）.执行命令 **dhcp snooping enable,** 在接口或 VLAN 下使能 DHCP Snooping 功能；

4）.执行命令**dhcp snooping trusted,** 在接口或者 VLAN 下配置连接 DHCP Server 的接口为信任接口；使能 DHCP Snooping 功能后，接口默认为非信任状态。

5）. 执行命令**ip source check user-bind enable,** 在接口或 VLAN 视图下使能 IP 报文检查功能。

三、应用场景

5.1 配置IPSG防止主机私自更改IP地址示例（静态绑定）

组网需求

如图 5-1 所示，Host 通过 Switch 接入网络，Gateway 为企业出口网关，各 Host 均使用静态配置的 IP 地址。管理员希望 Host 使用管理员分配的固定 IP 地址上网，不允许私自更改 IP 地址非法获取网络访问权限。

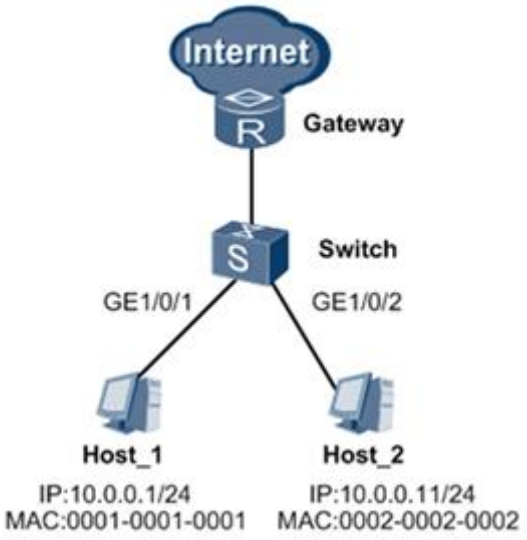


图5-1 配置IPSG防止主机私自更改IP地址（静态绑定）组网图

配置思路

采用如下的思路在 Switch 上配置 IPSG 功能，实现上述需求。

1． 在 Switch 上配置 Host_1 和 Host_2 的静态绑定表，固定 IP 和 MAC 的绑定关系。

2． 在 Switch 连接用户主机的接口使能 IPSG，实现 Host 只能使用管理员分配的固定 IP 地址上网。

详细配置步骤

1.创建 Host_1 和 Host_2 的静态绑定表项

```
<Switch> system-view
[Switch] user-bind static ip-address 10.0.0.1 mac-address 0001-0001-0001
[Switch] user-bind static ip-address 10.0.0.11 mac-address 0002-0002-0002
```

2.在接口使能 IPSG 功能

在连接 Host_1 的 GE1/0/1 接口使能 IP 报文检查功能：

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] ip source check user-bind enable
[Switch-GigabitEthernet1/0/1] quit
```

在连接 Host_2 的 GE1/0/2 接口使能 IP 报文检查功能：

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] ip source check user-bind enable
[Switch-GigabitEthernet1/0/2] quit
```

5.2 配置IPSG防止主机私自更改IP地址示例（DHCP Snooping动态绑定）

组网需求

如图 5-2 所示，Host 通过 Switch_1 接入网络，Switch_2 作为 DHCP Server 为 Host 动态分配 IP 地址，Gateway 为企业出口网关。管理员希望 Host 使用动态分配的地址，不允许私自配置静态 IP 地址，如果私自指定 IP 地址将无法访问网络。

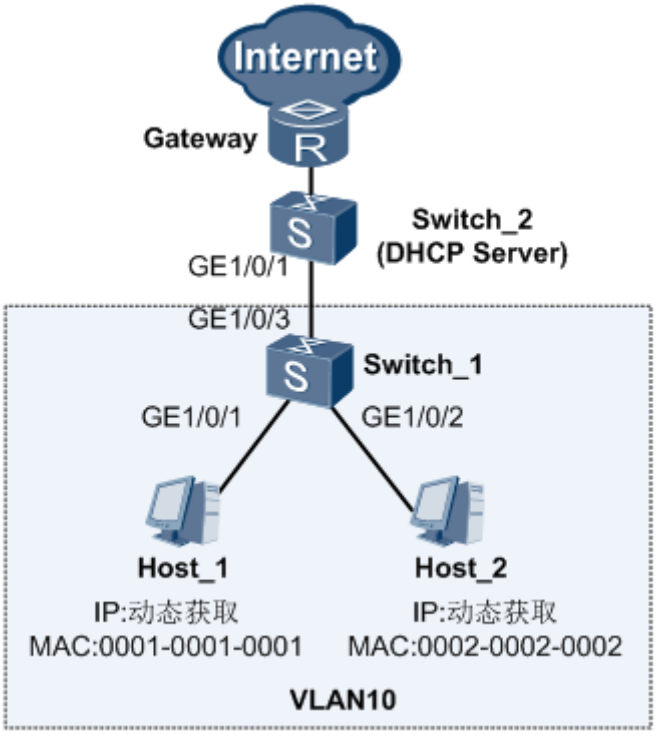


图 5-2 配置 IPSG 防止主机私自更改 IP 地址（DHCP Snooping 动态绑定）组网图

配置思路

采用如下的思路配置 IPSG 功能，实现上述需求。

1. 在 Switch_2 上配置 DHCP Server 功能（假设地址池为 10.1.1.0/24），为 Host 动态分配 IP 地址。

2． 在 Switch_1 上配置 DHCP Snooping 功能，保证 Host 从合法的 DHCP Server 获取 IP 地址，同时生成 DHCP Snooping 动态绑定表，记录 Host 的 IP 地址、MAC 地址、VLAN、接口的绑定关系。

3． 在 Switch_1 连接 Host 的 VLAN 上使能 IPSG 功能，防止 Host 通过私自配置 IP 地址的方式访问网络。

详细配置步骤

1.在 Switch_2 上配置 DHCP Server 功能

```
<HUAWEI> system-view
[HUAWEI] sysname Switch_2      //配置交换机名字（可选配置）
[Switch_2] vlan batch 10       //创建 vlan10
[Switch_2] interface gigabitethernet 1/0/1 //配置接口 1/0/1 为 trunk 类型，并允许 vlan10 通过
[Switch_2-GigabitEthernet1/0/1] port link-type trunk
[Switch_2-GigabitEthernet1/0/1] port trunk allow-pass vlan 10
[Switch_2-GigabitEthernet1/0/1] quit
[Switch_2] dhcp enable//开启 DHCP 功能
[Switch_2] ip pool 10 //配置地址池方式的 DHCP Server
[Switch_2-ip-pool-10] network 10.1.1.0 mask 24
[Switch_2-ip-pool-10] gateway-list 10.1.1.1
[Switch_2-ip-pool-10] quit
[Switch_2] interface vlanif 10 //配置 VLAN10 的网关地址
[Switch_2-Vlanif10] ip address 10.1.1.1 255.255.255.0
[Switch_2-Vlanif10] dhcp select global //配置 DHCP 服务器基于全局的地址池下发 IP 地址等信息
[Switch_2-Vlanif10] quit
```

2.在 Switch_1 上配置 DHCP Snooping 功能

配置各接口所属 VLAN。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch_1      //设置交换机的名字（可选配置）
[Switch_1] vlan batch 10
[Switch_1] interface gigabitethernet 1/0/1      //配置接口 1/0/1 为 access 模式，并把接口加入到 VLAN10
[Switch_1-GigabitEthernet1/0/1] port link-type access
[Switch_1-GigabitEthernet1/0/1] port default vlan 10
[Switch_1-GigabitEthernet1/0/1] quit
```

```
[Switch_1] interface gigabitethernet 1/0/2
[Switch_1-GigabitEthernet1/0/2] port link-type access
[Switch_1-GigabitEthernet1/0/2] port default vlan 10
[Switch_1-GigabitEthernet1/0/2] quit
[Switch_1] interface gigabitethernet 1/0/3      //配置接口 1/0/3 为 trunk 模式，并允许 VLAN10 通过
[Switch_1-GigabitEthernet1/0/3] port link-type trunk
[Switch_1-GigabitEthernet1/0/3] port trunk allow-pass vlan 10
[Switch_1-GigabitEthernet1/0/3] quit
```

使能 DHCP Snooping 功能，并将连接 DHCP Server 的 GE1/0/3 接口配置为信任接口。

```
[Switch_1] dhcp enable//使能 DHCP 功能
[Switch_1] dhcp snooping enable          //使能 DHCP Snooping 功能
[Switch_1] vlan 10     //开启 vlan 去的 dhcp snooping 功能，并把接口 g1/0/3 配置为信任接口
[Switch_1-vlan10] dhcp snooping enable
[Switch_1-vlan10] dhcp snooping trusted interface gigabitethernet 1/0/3
```

3.在 Switch_1 的 VLAN10 上使能 IPSG 报文检查功能

```
[Switch_1-vlan10] ip source check user-bind enable       [Switch_1-vlan10] quit
```

5.3 配置IPSG限制非法主机访问内网示例（静态绑定）

组网需求

如图 5-3 所示，Host 通过 Switch 接入网络，Gateway 为企业出口网关，各 Host 均使用静态配置的 IP 地址。管理员在 Switch 上做了接口限速，希望 Host 使用管理员分配的固定 IP 地址、从固定的接口上线。同时为了安全考虑，不允许外来人员的电脑随意接入内网。

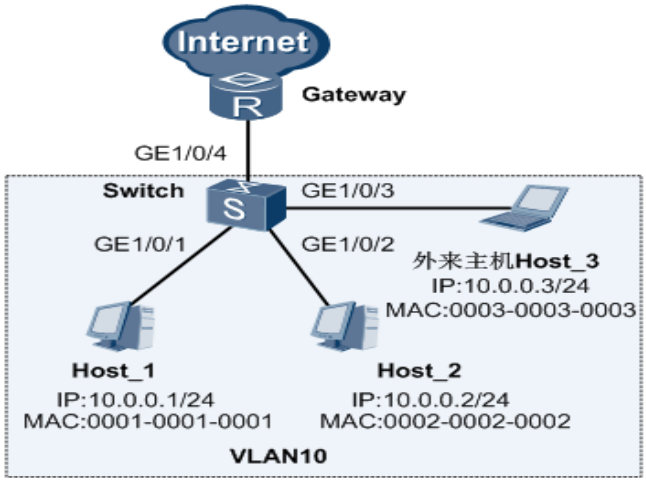


图 5-3 配置 IPSG 限制非法主机访问内网（静态绑定）组网图

配置思路

采用如下的思路在 Switch 上配置 IPSG 功能，实现上述需求。

1． 在 Switch 上配置各接口所属 VLAN。

2． 在 Switch 上创建 Host_1 和 Host_2 的静态绑定表项，固定 IP 地址、MAC 地址、接口的绑定关系。

3． 在 Switch 上配置 GE1/0/4 为信任接口，从该接口收到的报文不执行 IPSG 检查，防止从 Gateway 回程报文被丢弃。

4． 在 Switch 连接用户主机的 VLAN 上使能 IPSG 功能，实现 Host_1、Host_2 使用固定的 IP 地址、从固定的接口上线，并且外来主机 Host_3 无法随意接入内网。

详细配置步骤

1． 配置各接口所属 VLAN

```
<Switch> system-view
[Switch] vlan batch 10
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type access
[Switch-GigabitEthernet1/0/1] port default vlan 10
[Switch-GigabitEthernet1/0/1] quit
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type access
[Switch-GigabitEthernet1/0/2] port default vlan 10
[Switch-GigabitEthernet1/0/2] quit
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] port link-type access
[Switch-GigabitEthernet1/0/3] port default vlan 10
[Switch-GigabitEthernet1/0/3] quit
[Switch] interface gigabitethernet 1/0/4
[Switch-GigabitEthernet1/0/4] port link-type trunk
[Switch-GigabitEthernet1/0/4] port trunk allow-pass vlan 10
[Switch-GigabitEthernet1/0/4] quit
```

2． 创建 Host_1 和 Host_2 的静态绑定表项

```
[Switch] user-bind static ip-address 10.0.0.1 mac-address 0001-0001-0001
interface gigabitethernet 1/0/1
[Switch] user-bind static ip-address 10.0.0.2 mac-address 0002-0002-0002
interface gigabitethernet 1/0/2
```

3． 配置上行口 GE1/0/4 为信任接口

```
[Switch] dhcp enable
[Switch] dhcp snooping enable
[Switch] interface gigabitethernet 1/0/4
[Switch-GigabitEthernet1/0/4] dhcp snooping trusted
[Switch-GigabitEthernet1/0/4] quit
```

4． 在连接 Host 的 VLAN10 上使能 IPSG 功能

```
[Switch] vlan 10
[Switch-vlan10] ip source check user-bind enable
[Switch-vlan10] quit
```

6 POE配置

一、功能简介

PoE 供电就是通过以太网供电，这种方式仅凭借那根连接通信终端的网线就可完成为它们供电。PoE 提供的是-53V～0V 的直流电，供电距离最长可达 100m。PoE 款型的交换机的软件大包天然支持 PoE，无需 license，通过执行 poe-enable 命令使能 PoE 功能。

1、仅 S7700 中的 PoE 机框支持 PoE 功能,S9700、S12700 系列交换机不支持 PoE 功能。

2、盒式交换机中，面板上型号名称有 **PWR** 字样就支持 PoE 功能，无则不支持。

3、S2750 系列和 S5700-LI 系列的 PoE 交换机使用的就是内置电源，不支持可插拔电源模块。

4、可插拔电源模块的 PoE 交换机都支持 2 个电源模块槽位，至少插 1 个 PoE 电源模块，最多能插两个，且两个 PoE 电源模块款型必须相同。

表 1 POE 接口输出电压和功率			
标准	设备	最大输出功率	电压
802.3af		15.4W	-53V～0V DC
802.3at	盒式交换机	30W	
	框式交换机	37W	
PoE 接口会根据 PD 的最大功耗来选择工作在哪种标准			

S交换机POE电源匹配表.xlsx

二、配置命令和步骤

说明：POE 设备出厂状态下 POE 功能已开启，终端设备插上即可用，无需做任何配置，但是根据客户需求可用做如下配置：

使能 PoE 功能

执行命令**poe enable**，接口视图，使能接口 PoE 功能。 缺省情况下，接口 PoE 供电功能处于使能状态。

配置 PoE 电源备份模式

执行命令**poe-power backup-mode** *backup-mode*，系统视图，配置设备的 PoE 电源备份模式。缺省情况下，设备无 PoE 电源备份。

配置设备单板的最大对外输出功率

执行命令**poe max-power** max-power **slot** *slot-id*，系统视图，配置单板最大供电功率。缺省情况下，单板的最大供电功率为设备最大功率在每块单板上的平均分配。

配置接口最大供电功率

执行命令**poe power port-max-power**，接口视图，配置接口的最大供电功率。

配置 PoE 电源预留功率比例

执行命令**poe power-reserved** power-reserved，系统视图，配置 PoE 电源预留功率占最大输出功率的比例。 缺省情况下，预留功率比例为 20%。

配置 PoE 电源的告警阈值功率百分比

执行命令 **poe-power utilization-threshold** t*hreshold-value*，配置 PoE 电源的告警阈值功率百分比。 缺省情况下，告警阈值功率百分比为 90%，即当消耗的功率为电源总功率的 90%时，产生告警。

配置设备供电管理方式

执行命令**poe power-management auto slot** slot-id，系统视图，配置为自动模式（默认模式）

执行命令**interface interface-type** interface-number，进入接口视图。

执行命令**poe priority** { **critical** | **high** | **low** }，配置该接口的供电的优先级，默认为 LOW。

或

执行命令**poe power-management manual slot** slot-id，系统视图，配置为手动模式

执行命令**poe { power-on | power-off } interface** *interface-type interface-number*，手动给某个接口上的 PD 设备上下电。

三、应用场景

6.1 POE功能配置示例

组网需求

如 6-1 所示，现网环境中，交换机作为网络接入层设备。设备下接的 IP 电话放置在室外，AP 位于办公室外墙上，位置偏僻，都不方便接入电源，用户希望通过交换机设备直接供电，以节约设备部署成本。

AP1 为某银行的办公网络，设备不能断电，需要最高的供电优先级。同时 IP Phone1 业务量比较大，希望得到较高供电保证，非特殊情况不能掉电。

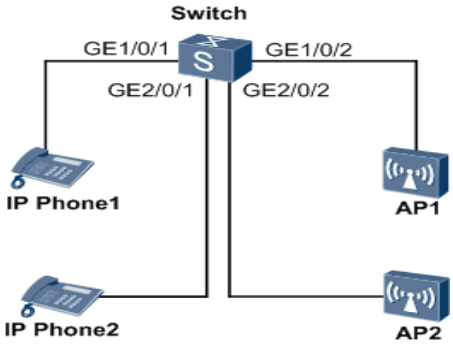


图6-1 PoE应用组网图

配置思路

要求采用支持 PoE 功能的交换机设备，并插有 PoE 电源。

采用如下的思路配置基本 PoE 功能：

1、配置设备的供电管理模式为自动模式，以便实现灵活管理接入的 PD 设备。

2、配置 1 号单板的最大对外输出功率，保证 1 号单板获得需要的功率。

3、配置 GigabitEthernet1/0/2 和 GigabitEthernet1/0/1 接口的供电优先级，优先保证 AP1 和 IP Phone1 的供电。

4、已知 IP Phone 和 AP1 的使用功率，配置 GigabitEthernet1/0/1、GigabitEthernet2/0/1 和 GigabitEthernet1/0/2 接口的最大对外输出功率，以限制对应接口的功率，保护设备安全。

详细配置步骤

1、配置设备的供电管理模式为自动模式。

```
<Quidway> system-view
[Quidway] poe power-management auto slot 1
[Quidway] poe power-management auto slot 2
```

2、配置 1 号单板的最大对外输出功率为 200W。

```
[Quidway] poe max-power 200000 slot 1
Warning: This operation may power off some PD. Continue?[Y/N]:y
```

3、分别配置 GigabitEthernet1/0/1、GigabitEthernet2/0/1 和 GigabitEthernet1/0/2 接口的最大对外输出功率为 15W、15W、20W。 （设备上功率的设置都以毫瓦（mW）为单位）

```
[Quidway] interface gigabitethernet 1/0/1
[Quidway-GigabitEthernet1/0/1] poe power 15000
Warning: This operation may power off some PD. Continue?[Y/N]:y
[Quidway-GigabitEthernet1/0/1] quit
[Quidway] interface gigabitethernet 2/0/1
[Quidway-GigabitEthernet2/0/1] poe power 15000
Warning: This operation may power off some PD. Continue?[Y/N]:y
```

```
[Quidway-GigabitEthernet2/0/1] quit
[Quidway] interface gigabitethernet 1/0/2
[Quidway-GigabitEthernet1/0/2] poe power 20000
Warning: This operation may power off some PD. Continue?[Y/N]:y
[Quidway-GigabitEthernet1/0/2] quit
```

4、配置 GigabitEthernet1/0/2 接口的供电优先级为 Critical。

```
[Quidway] interface gigabitethernet 1/0/2
[Quidway-GigabitEthernet1/0/2] poe priority critical
Warning: This operation may power off some PD with lower priority.
Continue?[Y/N]:y
[Quidway-GigabitEthernet1/0/2] quit
```

5、配置 GigabitEthernet1/0/1 接口的供电优先级为 High。

```
[Quidway] interface gigabitethernet 1/0/1
[Quidway-GigabitEthernet1/0/1] poe priority high
Warning: This operation may power off some PD with lower priority.
Continue?[Y/N]:y
[Quidway-GigabitEthernet1/0/1] quit
```

7 ACL配置

一、 功能简介

访问控制列表 ACL 是由一系列规则组成的集合，ACL 通过这些规则对数据包进行分类，从而设备可以对不同类报文进行不同的处理。

ACL 的规则匹配：报文到达设备时，查找引擎从报文中取出信息组成查找键值，键值与 ACL 中的规则进行匹配，只要有一条规则和报文匹配，就停止查找，称为命中规则。查找完所有规则，如果没有符合条件的规则，称为未命中规则，故 ACL 的规则分为“permit”（允许）规则或者“deny”（拒绝）规则和未命中规则。

常用 ACL 的功能分类如下表所示：

分类	对应编号范围	适用的IP版本	场景应用场景
基本ACL	2000-2999	IPv4	使用报文的源IP地址和时间段信息来定义规则
高级ACL	3000-3999	IPv4	除了基本ACL的应用场景外，还支持基于目的地址、IP优先级、报文类型、源目端口号来定义规则
二层ACL	4000-4999	IPv4&IPv6	根据源目MAC地址、以太网帧协议类型等定义规则

二、 配置命令和步骤

1．（可选）配置ACL生效的时间段，执行命令**time-range**配置acl生效的时间段；

2．配置ACL编号，执行命令**acl** number配置一条acl（number不同，acl可以匹配的参数也不同，具体的acl编号请参考上表）

3．配置ACL规则，执行命令**rule permit|deny**配置ACL的具体规则；

4．应用ACL，ACL可以在很多特性中被应用，但是单独的ACL是无法应用的，需要借助其他的特性，例如：流策略里面对acl匹配的数据流执行相应的动作、登陆设备的时候调用ACL对登陆设备的用户做限制等。

三、 应用场景

7.1 使用基本ACL配置交换机telnet访问的权限

组网需求

如图7-1所示，为了便于远程管理交换机，开启了telnet的服务，公司的所有网络管理员都可以登录到交换机进行管理，但是为了安全考虑，要求在上班期间交换机的管理只能由网络管理部门技术比较好的管理员小王来管理设备，其他管理员只有下班之后才可以登录交换机管理设备；

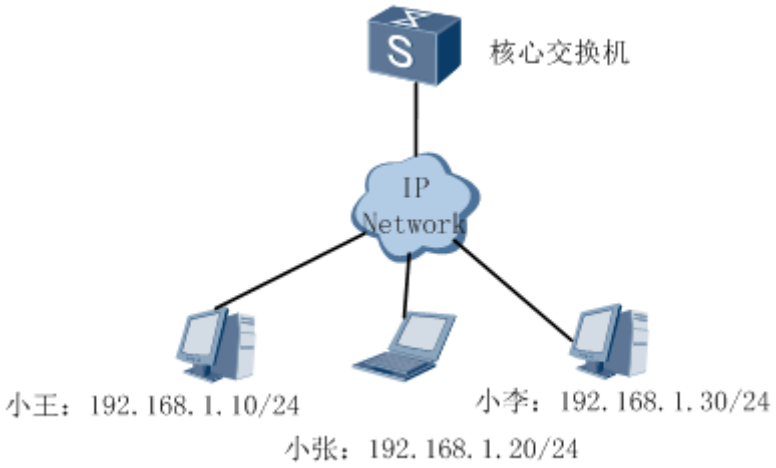


图7-1 使用基本ACL配置交换机telnet访问的权限组网图

配置思路

1． 开启交换机的 telent 服务

2． 配置时间段

3． 配置基本 ACL

4． 应用基本 ACL

详细配置步骤

1． 开启交换机的 telent 服务

```
<Huawei> system-view
[Huawei] telnet server enable    #开启交换机的telnet服务
```

```
[Huawei] user-interface vty 0 4 #配置telnet的登陆验证方式为用户名加密码
[Huawei-ui-vty0-4] authentication-mode aaa
[Huawei-ui-vty0-4] protocol inbound all     #允许通过telent和ssh登陆交换机
[Huawei-ui-vty0-4] quit
[Huawei] aaa     #创建telnet登陆交换机的用户名和密码
[Huawei-aaa] local-user huawei privilege level 15 password cipher huawei@2015
[Huawei-aaa] local-user huawei service-type telnet #给huawei用户赋予telent
的权限
```

2． 配置时间段，周一到周五早上 8:30 到下午 18:00

```
[Huawei] time-range workday 8:30 to 18:00 working-day
```

3． 配置基本 ACL

```
[Huawei] acl 2000
[Huawei-acl-basic-2000] rule permit source 192.168.1.10 0 time-range workday
 #只允许192.168.1.10这一个用户可以telnet交换机
[Huawei-acl-basic-2000] rule deny   #这个地方rule deny可以不用写，acl在这种场景
下最后隐含有一条deny any的语句；
```

4． 应用基本 ACL

```
[Huawei] user-interface vty 0 4
[Huawei-ui-vty0-4] acl 2000 inbound #在vty下面应用acl，只允许匹配acl数据流的的用
户telent登陆交换机，没有被permit的全部被deny了。
```

7.2 使用高级ACL配置流分类实现限制互访某一台服务器

组网需求

如图7-2所示，公司企业网通过Switch实现各部门之间的互连。要求正确配置ACL，禁止研发部门和市场部门在上班时间（8:30至18:00）访问工资查询服务器（IP地址为192.168.100.10），而总裁办公室不受限制，可以随时访问。

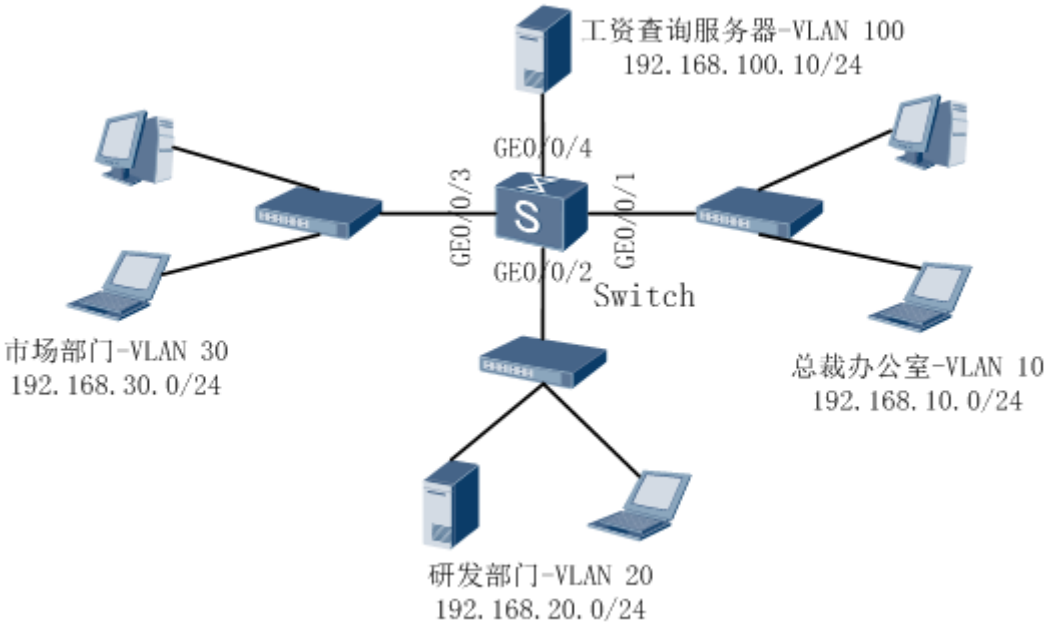


图7-2 使用高级ACL配置流分类示例

配置思路

1. 配置接口、VLAN 和网关地址；
2. 配置时间段；
3. 配置高级 ACL；
4. 配置流分类；
5. 配置流行为；
6. 配置流策略；
7. 在接口上应用流策略。

详细配置步骤

1. 配置接口、VLAN 和网关地址；

```
<Huawei> system-view
[Huawei] sysname Switch
[Switch] vlan batch 10 20 30 100    #批量创建VLAN
```

#把GE0/0/1-GE0/0/4加入到对应的VLAN

```
[Switch] interface GigabitEthernet 0/0/1
[Switch-GigabitEthernet0/0/1] port link-type access
[Switch-GigabitEthernet0/0/1] port default vlan 10
[Switch] interface GigabitEthernet 0/0/2
[Switch-GigabitEthernet0/0/2] port link-type access
[Switch-GigabitEthernet0/0/2] port default vlan 20
```

```
[Switch] interface GigabitEthernet 0/0/3
[Switch-GigabitEthernet0/0/3] port link-type access
[Switch-GigabitEthernet0/0/3] port default vlan 30
[Switch] interface GigabitEthernet 0/0/4
[Switch-GigabitEthernet0/0/4] port link-type access
[Switch-GigabitEthernet0/0/4] port default vlan 100
```

#配置四个VLAN的网关地址

```
[Switch] interface Vlanif 10
[Switch-Vlanif10] ip address 192.168.10.1 24
[Switch] interface Vlanif 20
[Switch-Vlanif20] ip address 192.168.20.1 24
[Switch] interface Vlanif 30
[Switch-Vlanif30] ip address 192.168.30.1 24
[Switch] interface Vlanif 100
[Switch-Vlanif100] ip address 192.168.100.1 24
```

上述配置基本配置完成之后，所有的部门之间都是可以互访的。

2． 配置时间段；（周一到周五早上 8:30 到下午 19:00）

```
[Huawei] time-range workday 8:30 to 18:00 working-day
```

3． 配置 ACL；

配置市场部门到工资查询服务器的访问规则。

```
[Switch] acl 3002
[Switch-acl-adv-3002] rule deny ip source 192.168.30.0 0.0.0.255 destination
192.168.100.10 0.0.0.0 time-range workday
[Switch-acl-adv-3002] quit
```

配置研发部门到工资查询服务器的访问规则。

```
[Switch] acl 3003
[Switch-acl-adv-3003] rule deny ip source 192.168.20.0 0.0.0.255 destination
192.168.100.10 0.0.0.0 time-range workday
[Switch-acl-adv-3003] quit
```

4． 配置流分类；

配置流分类 c_market，对匹配 ACL 3002 的报文进行分类。

```
[Switch] traffic classifier c_market
[Switch-classifier-c_market] if-match acl 3002
[Switch-classifier-c_market] quit
```

配置流分类 c_rd，对匹配 ACL 3003 的报文进行分类。

```
[Switch] traffic classifier c_rd
[Switch-classifier-c_rd] if-match acl 3003
[Switch-classifier-c_rd] quit
```

5. 配置流行为；

配置流行为b_market，动作为拒绝报文通过。

```
[Switch] traffic behavior b_market
[Switch-behavior-b_market] deny
[Switch-behavior-b_market] quit
```

配置流行为b_rd，动作为拒绝报文通过。

```
[Switch] traffic behavior b_rd
[Switch-behavior-b_rd] deny
[Switch-behavior-b_rd] quit
```

6. 配置流策略；

配置流策略 p_market，将流分类 c_market 与流行为 b_market 关联。

```
[Switch] traffic policy p_market
[Switch-trafficpolicy-p_market] classifier c_market behavior b_market
[Switch-trafficpolicy-p_market] quit
```

配置流策略 p_rd，将流分类 c_rd 与流行为 b_rd 关联。

```
[Switch] traffic policy p_rd
[Switch-trafficpolicy-p_rd] classifier c_rd behavior b_rd
[Switch-trafficpolicy-p_rd] quit
```

7. 在接口上应用流策略。

将流策略p_market应用到GE0/0/2接口。

```
[Switch] interface gigabitethernet 0/0/2
[Switch-GigabitEthernet0/0/2] traffic-policy p_market inbound
[Switch-GigabitEthernet0/0/2] quit
# 将流策略p_rd应用到GE0/0/3接口。
[Switch] interface gigabitethernet 0/0/3
[Switch-GigabitEthernet0/0/3] traffic-policy p_rd inbound
[Switch-GigabitEthernet0/0/3] quit
```

7.3 使用二层ACL配置流分类拒绝指定报文通过

组网需求

如图7-3所示，Switch作为网关设备，下挂用户PC。要求配置ACL，禁止源MAC地址为

00e0-f201-0101、目的MAC地址为0260-e207-0002的报文通过。

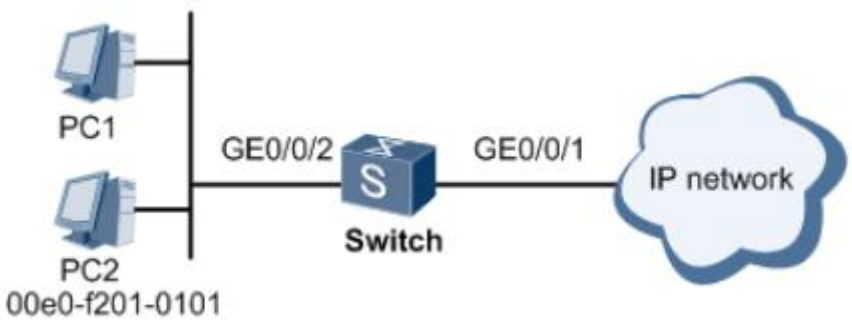


图7-3 应用二层ACL配置流分类组网图

配置思路

1. 配置 ACL。
2. 配置流分类。
3. 配置流行为。
4. 配置流策略。
5. 接口上应用流策略。

详细配置步骤

1. 配置 ACL

配置符合要求的二层ACL。

```
<Switch> system-view
[Switch] acl 4000
[Switch-acl-L2-4000] rule deny source-mac 00e0-f201-0101 ffff-ffff-ffff
destination-mac 0260-e207-0002 ffff-ffff-ffff
[Switch-acl-L2-4000] quit
```

2. 配置基于 ACL 的流分类

配置流分类tc1，对匹配ACL 4000的报文进行分类。

```
[Switch] traffic classifier tc1
[Switch-classifier-tc1] if-match acl 4000
[Switch-classifier-tc1] quit
```

3. 配置流行为

配置流行为tb1，动作为拒绝报文通过。

```
[Switch] traffic behavior tb1
[Switch-behavior-tb1] deny
[Switch-behavior-tb1] quit
```

4. 配置流策略

配置流策略tp1，将流分类tc1与流行为tb1关联。

```
[Switch] traffic policy tp1
[Switch-trafficpolicy-tp1] classifier tc1 behavior tb1
[Switch-trafficpolicy-tp1] quit
```

5． 应用流策略

将流策略tp1应用到GE0/0/2接口。

```
[Switch] interface gigabitethernet 0/0/2
[Switch-GigabitEthernet0/0/2] traffic-policy tp1 inbound
[Switch-GigabitEthernet0/0/2] quit
```

8 QoS基础配置

一、 功能简介

模块化 QoS 命令行 MQC 是指通过将具有某类共同特征的报文划分为一类，并为同一类报文提供相同的服务，也可以对不同类的报文提供不同的服务。

随着网络中 QoS 业务的不断丰富，在网络规划时若要实现对不同流量（如不同业务或不同用户）的差分服务，会使部署比较复杂。MQC 的出现，使用户能对网络中的流量进行精细化处理，用户可以更加便捷的针对自己的需求对网络中的流量提供不同的服务，完善了网络的服务能力。

MQC 包含三个要素：流分类（traffic classifier）、流行为（traffic behavior）和流策略（traffic policy）。

二、配置命令和步骤

配置流策略的步骤

1． 配置流分类，定义流分类中的匹配规则；匹配创建的 ACL 规则或者直接匹配报文优先级等参数；

2． 配置流行为，根据实际情况定义流行为中的动作；配置报文过滤、重标记优先级、重定向、流量监管、流量统计等动作；

3． 配置流策略，在流策略中为指定的流分类配置所需流行为，即绑定流分类和流行为；

4． 应用流策略，在接口、VLAN 或者全局应用流策略；

流策略具体的配置命令

1．执行命令 **traffic classifier** classifier-name，创建一个流分类并进入流分类视图，或进入已存在的流分类视图；

请根据实际情况定义流分类中的匹配规则，**if-match vlan-id** 、**if-match acl acl-number**、**if-match 8021p 8021p-value**、**if-match dscp dscp-value** 等；

2.执行命令 **traffic behavior** behavior-name，创建一个流行为并进入流行为视图，或进入已存在的流行为视图。

请根据实际情况定义流行为中的动作，只要各动作不冲突，都可以在同一流行为中配置，动作包括允许、拒绝、重定向、限速等等；

3.执行命令 **traffic policy** policy-name，创建一个流策略并进入流策略视图，或进入已存在的流策略视图；

执行命令 **classifier** classifier-name **behavior** behavior-name，在流策略中为指定的流分类配置所需流行为，即绑定流分类和流行为；

4．执行命令 **traffic-policy** policy-name { **inbound | outbound** }，在接口、VLAN 或者系统视图下应用流策略；

三、应用场景

8.1 通过流策略实现策略路由（重定向到不同的下一跳）

如图 8-1 所示，公司用户通过 Switch 双归属到外部网络设备。其中，一条是低速链路，网关为 10.1.20.1/24；另外一条是高速链路，网关为 10.1.30.1/24。

公司内网有两个网段 192.168.1.0/24 和 192.168.2.0/24，192.168.1.0 网段主要是服务器区，对链路带宽要求比较高，所以网管决定该网段走高速链路出去，剩余的 192.168.2.0 网段主要用作公司员工上网，上网的话只能走低速链路。

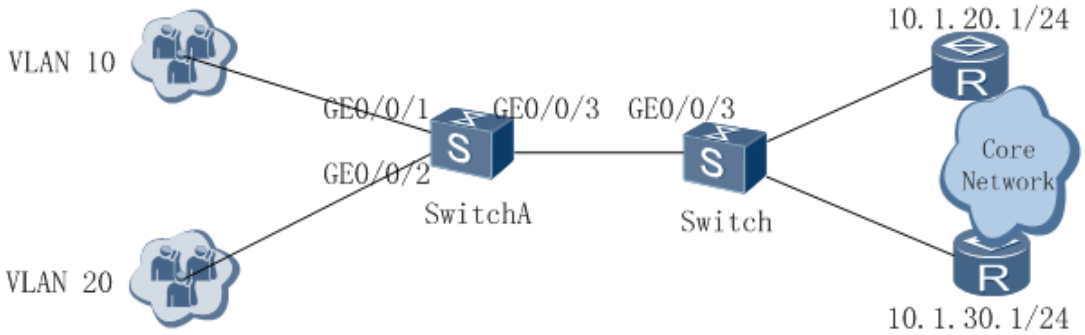


图8-1　配置策略路由组网图

配置思路：

1．　创建 VLAN 并配置各接口，配置路由实现公司和外部网络互通；

2．　配置 ACL 规则，分别匹配 192.168.1.0 和 192.168.2.0 网段的数据流；

3．　配置流分类，匹配规则为上述创建的 ACL 规则，使设备对报文可以区分；

4．　配置流行为，使满足不同 ACL 规则的数据流走不同的链路，需要先把内网互访的数据流放行；

5．　配置流策略，绑定上述流分类和流行为，并应用到 Switch 设备的 GE0/0/3 接口的入方向，实现策略路由；

配置步骤：

1．　创建 VLAN 并配置各接口

#在 SwitchA 上面创建 vlan10 和 vlan20

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchA
[SwitchA] vlan batch 100 200
```

#配置 SwitchA 交换机，连接终端 PC 的接口为 Access 类型，GE0/0/1 加到 vlan10，GE0/0/2 加入到 vlan20，上联 Switch 的接口 GE0/0/3 配置为 trunk 类型，并允许 vlan10 和 vlan20 通过

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port link-type access
[SwitchA-GigabitEthernet0/0/1] port default vlan 10
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] port link-type access
[SwitchA-GigabitEthernet0/0/2] port default vlan 20
[SwitchA-GigabitEthernet0/0/2] quit
[SwitchA] interface gigabitethernet 0/0/3
[SwitchA-GigabitEthernet0/0/3] port link-type trunk
[SwitchA-GigabitEthernet0/0/3] port trunk allow-pass vlan 10 20
[SwitchA-GigabitEthernet0/0/3] quit
```

#在 Switch 上面配置 VLAN10 和 VLAN20，并配置 Switch 连接 SwitchA 的 GE0/0/3 接口类型为 trunk，并允许 VLAN10 和 VLAN20 通过

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] vlan batch 100 200
[SwitchA] interface gigabitethernet 0/0/3
[SwitchA-GigabitEthernet0/0/3] port link-type trunk
[SwitchA-GigabitEthernet0/0/3] port trunk allow-pass vlan 10 20
[SwitchA-GigabitEthernet0/0/3] quit
```

#配置 VLAN10 和 VLAN20 的网关 VLANIF10 和 VLANIF20 地址分别为 192.168.1.1/24 和 192.168.2.1/24

```
[Switch] interface vlanif 10
[Switch-Vlanif10] ip address 192.168.1.1 24
[Switch-Vlanif10] quit
[Switch] interface vlanif 20
[Switch-Vlanif20] ip address 192.168.2.1 24
[Switch-Vlanif20] quit
```

在 Switch 分别配置两台静态路由指向外网实现互通

```
[Switch] ip route-static 0.0.0.0 0 10.1.20.1
[Switch] ip route-static 0.0.0.0 0 10.1.30.1
```

经以上调试之后，内网访问外网没问题了，但是不能保证 VLAN10 的数据走高速链路，VLAN20 的数据走低速链路；

2． 创建 ACL 规则

#在 Switch 上创建编号为 3000、3001 和 3002 的 ACL，分别匹配内网 192.168.1.0 和 192.168.2.0 之间的互访、192.168.1.0、192.168.2.0 的数据；

```
[Switch] acl 3000        //主要作用是匹配内网两个网段之间互访的数据流，不需要做重定向，否则内网之间无法互访；
[Switch-acl-adv-3000] rule permit ip source 192.168.1.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
[Switch-acl-adv-3000] rule permit ip source 192.168.2.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
[Switch-acl-adv-3000] quit
[Switch] acl 3001        //匹配内网 VLAN10 服务器的数据流
[Switch-acl-adv-3001] rule permit ip source 192.168.1.0 0.0.0.255
[Switch-acl-adv-3001] quit
[Switch] acl 3002        //匹配内网 VLAN20 上网用户的数据流
[Switch-acl-adv-3002] rule permit ip source 192.168.2.0 0.0.0.255
[Switch-acl-adv-3002] quit
```

3． 配置流分类

#在 Switch 上创建流分类 c0、c1、c2，分别匹配 ACL3000、ACL3001 和 ACL3002

```
[Switch] traffic classifier c0
[Switch-classifier-c0] if-match acl 3000
[Switch-classifier-c0] quit
[Switch] traffic classifier c1
[Switch-classifier-c1] if-match acl 3001
[Switch-classifier-c1] quit
[Switch] traffic classifier c2
[Switch-classifier-c2] if-match acl 3002
[Switch-classifier-c2] quit
```

4． 配置流行为

在 Switch 上创建流行为 b0、b1、b2，对 b0 只配置 permit 的工作，b1 和 b2 分别指定重定向到网段 10.1.20.1/24 和 10.1.30.1/24 的动作。

```
[Switch] traffic behavior b0
[Switch-behavior-b1] permit
```

```
[Switch] traffic behavior b1
[Switch-behavior-b1] redirect ip-nexthop 10.1.20.1
[Switch-behavior-b1] quit
[Switch] traffic behavior b2
[Switch-behavior-b2] redirect ip-nexthop 10.1.30.1
[Switch-behavior-b2] quit
```

5． 配置流策略并应用到接口

在 Switch 上创建流策略 p1，将流分类和对应的流行为进行绑定。

```
[Switch] traffic policy p1
[Switch-trafficpolicy-p1] classifier c0 behavior b0
[Switch-trafficpolicy-p1] classifier c1 behavior b1
[Switch-trafficpolicy-p1] classifier c2 behavior b2
[Switch-trafficpolicy-p1] quit
```

将流策略 p1 应用到接口 GE0/0/3 的入方向上。

```
[Switch] interface gigabitethernet 0/0/3
[Switch-GigabitEthernet0/0/3] traffic-policy p1 inbound
[Switch-GigabitEthernet0/0/3] quit
```

8.2 通过流策略实现不同网段间限制互访

如图 8-2 所示，公司内部有三个部门，分别属于 VLAN10、VLAN20 和 VLAN30，为了安全考虑，VLAN10 的用户只能访问 VLAN20 但是不能访问 VLAN30，要求三个部门都能正常上网，其他的没有特殊限制；

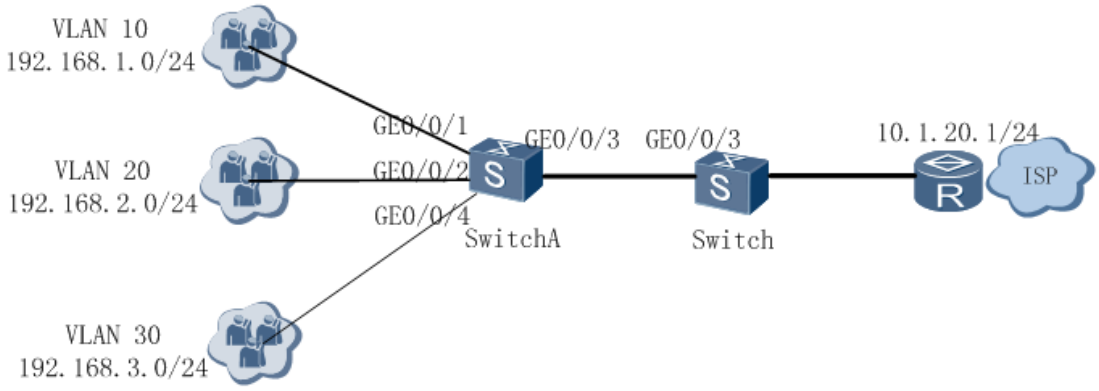


图 8-2 配置流策略实现网段限制互访组网图

配置思路：

1． 创建 VLAN 并配置各接口，配置路由实现公司和外部网络互通；

2． 配置 ACL 规则，分别匹配需要允许和拒绝访问的数据流；

3． 配置流分类，匹配规则为上述创建的 ACL 规则，使设备对报文可以区分；

4． 配置流行为，动作为 permit，允许访问（拒绝访问的数据流在 acl 里面做控制）；

5． 配置流策略，绑定上述流分类和流行为，并应用到 Switch 设备的 GE0/0/3 接口的入方向，实现不同网段限制互访的要求；

配置步骤：

1． 创建 VLAN 并配置各接口

#在 SwitchA 上面创建 vlan10、vlan20 和 vlan30

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchA
[SwitchA] vlan batch 10 20 30
```

#配置 SwitchA 交换机，连接终端 PC 的接口为 Access 类型，GE0/0/1 加到 vlan10，GE0/0/2 加入到 vlan20，GE0/0/4 加入到 vlan30，上联 Switch 的接口 GE0/0/3 配置为 trunk 类型，并允许 vlan10 和 vlan20 通过

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port link-type access
[SwitchA-GigabitEthernet0/0/1] port default vlan 10
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] port link-type access
[SwitchA-GigabitEthernet0/0/2] port default vlan 20
[SwitchA-GigabitEthernet0/0/2] quit
[SwitchA] interface gigabitethernet 0/0/3
[SwitchA-GigabitEthernet0/0/3] port link-type trunk
[SwitchA-GigabitEthernet0/0/3] port trunk allow-pass vlan 10 20
[SwitchA-GigabitEthernet0/0/3] quit
[SwitchA] interface gigabitethernet 0/0/4
[SwitchA-GigabitEthernet0/0/4] port link-type access
[SwitchA-GigabitEthernet0/0/4] port default vlan 30
[SwitchA-GigabitEthernet0/0/4] quit
```

#在 Switch 上面配置 VLAN10、VLAN20 和 VLAN30，并配置 Switch 连接 SwitchA 的 GE0/0/3 接口类型为 trunk，并允许 VLAN10、VLAN20 和 VLAN30 通过

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] vlan batch 10 20 30
[SwitchA] interface gigabitethernet 0/0/3
```

```
[SwitchA-GigabitEthernet0/0/3] port link-type trunk
[SwitchA-GigabitEthernet0/0/3] port trunk allow-pass vlan 10 20 30
[SwitchA-GigabitEthernet0/0/3] quit
```

#配置 VLAN10、VLAN20 和 VLAN30 的网关 VLANIF10、VLANIF20 和 VLANIF30 地址分别为 192.168.1.1/24、192.168.2.1/24 和 192.168.3.1/24

```
[Switch] interface vlanif 10
[Switch-Vlanif10] ip address 192.168.1.1 24
[Switch-Vlanif10] quit
[Switch] interface vlanif 20
[Switch-Vlanif20] ip address 192.168.2.1 24
[Switch-Vlanif20] quit
[Switch] interface vlanif 30
[Switch-Vlanif30] ip address 192.168.3.1 24
[Switch-Vlanif30] quit
```

在 Switch 分别配置静态路由指向外网实现互通

```
[Switch] ip route-static 0.0.0.0 0 10.1.20.1
```

2． 创建 ACL 规则

#在 Switch 上创建编号为 3000 的 ACL，配置允许 vlan10 可以访问 vlan20，拒绝 vlan10 访问 vlan30 的数据流；

```
[Switch] acl 3000
[Switch-acl-adv-3000] rule deny ip source 192.168.1.0 0.0.0.255 destination 192.168.3.0 0.0.0.255
[Switch-acl-adv-3000] rule permit ip source 192.168.1.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
[Switch-acl-adv-3000] rule permit ip source any #如果内网的网段比较多，把不做限制互访的流量放行；
 [Switch-acl-adv-3000] quit
```

3． 配置流分类

#在 Switch 上创建流分类 c1，匹配 ACL3000

```
[Switch] traffic classifier c1
[Switch-classifier-c1] if-match acl 3000
[Switch-classifier-c1] quit
```

4． 配置流行为

在 Switch 上创建流行为 b1，动作为 permit

```
[Switch] traffic behavior b1
[Switch-behavior-b1] permit
[Switch-behavior-b1] quit
```

5． 配置流策略并应用到接口

在 Switch 上创建流策略 p1，将流分类和对应的流行为进行绑定。

```
[Switch] traffic policy p1
[Switch-trafficpolicy-p1] classifier c1 behavior b1
[Switch-trafficpolicy-p1] quit
```

将流策略 p1 应用到接口 GE0/0/3 的入方向上。

```
[Switch] interface gigabitethernet 0/0/3
[Switch-GigabitEthernet0/0/3] traffic-policy p1 inbound
[Switch-GigabitEthernet0/0/3] quit
```

8.3 通过流策略实现限速功能

如图 8-3 所示，公司内部有两个部门，分别属于 VLAN10 和 VLAN20，VLAN10 主要是一些服务器对带宽要求比较高，VLAN20 只有公司员工上网对带宽要求不是很高，公司从运营商购买的是 10M 的专线，要求 VLAN20 员工上网的网速最低需要 2M 不能超过 4M，超过 4M 的流量全部丢弃以免影响服务器对外提供服务；对 VLAN10 的网速不做限制；

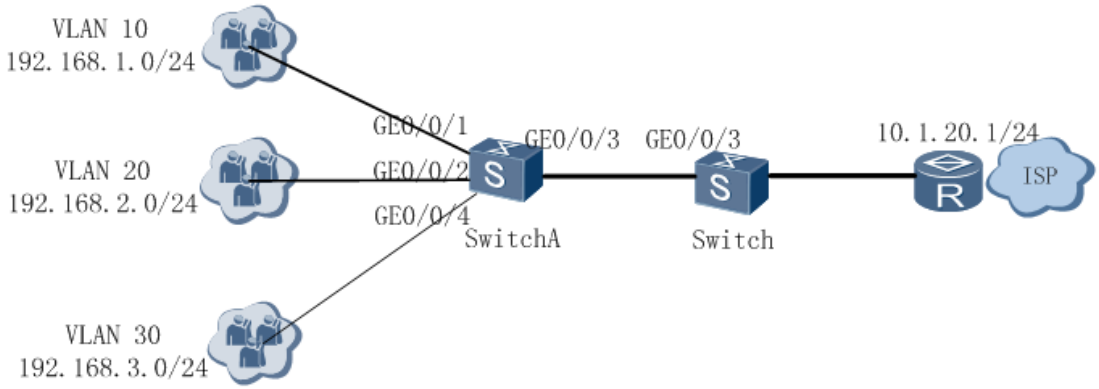


图 8-3 配置流策略实现网段限制互访组网图

配置思路：

1． 创建 VLAN 并配置各接口，配置路由实现公司和外部网络互通；

2． 配置 ACL 规则，匹配 192.168.2.0 网段的数据流；

3． 配置流分类，匹配规则为上述创建的 ACL 规则，使设备对报文可以区分；

4． 配置流行为，动作为流量监管，承诺信息速率为 2M；

5． 配置流策略，绑定上述流分类和流行为，并应用到 Switch 设备的 GE0/0/3 接口的入方向，实现对该网段的数据流做限速；

配置步骤：

1． 创建 VLAN 并配置各接口

#在 SwitchA 上面创建 vlan10 和 vlan20

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchA
[SwitchA] vlan batch 100 200
```

#配置 SwitchA 交换机，连接终端 PC 的接口为 Access 类型，GE0/0/1 加到 vlan10，GE0/0/2 加入到 vlan20，上联 Switch 的接口 GE0/0/3 配置为 trunk 类型，并允许 vlan10 和 vlan20 通过

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port link-type access
[SwitchA-GigabitEthernet0/0/1] port default vlan 10
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] port link-type access
[SwitchA-GigabitEthernet0/0/2] port default vlan 20
[SwitchA-GigabitEthernet0/0/2] quit
[SwitchA] interface gigabitethernet 0/0/3
[SwitchA-GigabitEthernet0/0/3] port link-type trunk
[SwitchA-GigabitEthernet0/0/3] port trunk allow-pass vlan 10 20
[SwitchA-GigabitEthernet0/0/3] quit
```

#在 Switch 上面配置 VLAN10 和 VLAN20，并配置 Switch 连接 SwitchA 的 GE0/0/3 接口类型为 trunk，并允许 VLAN10 和 VLAN20 通过

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] vlan batch 100 200
[SwitchA] interface gigabitethernet 0/0/3
[SwitchA-GigabitEthernet0/0/3] port link-type trunk
[SwitchA-GigabitEthernet0/0/3] port trunk allow-pass vlan 10 20
[SwitchA-GigabitEthernet0/0/3] quit
```

#配置 VLAN10 和 VLAN20 的网关 VLANIF10 和 VLANIF20 地址分别为 192.168.1.1/24 和 192.168.2.1/24

```
[Switch] interface vlanif 10
[Switch-Vlanif10] ip address 192.168.1.1 24
[Switch-Vlanif10] quit
[Switch] interface vlanif 20
```

```
[Switch-Vlanif20] ip address 192.168.2.1 24
[Switch-Vlanif20] quit
```

在 Switch 分别配置两台静态路由指向外网实现互通

```
[Switch]ip route-static 0.0.0.0 0 10.1.20.1
[Switch]ip route-static 0.0.0.0 0 10.1.30.1
```

经以上调试之后，内网访问外网没问题了，但是不能保证 VLAN10 的数据走高速链路，VLAN20 的数据走低速链路；

2． 创建 ACL 规则

#在 Switch 上创建编号为 3000 的 ACL，匹配内网 192.168.2.0 数据流；

```
[Switch] acl 3000
[Switch-acl-adv-3000] rule permit ip source 192.168.1.0 0.0.0.255
[Switch-acl-adv-3000] quit
```

3． 配置流分类

#在 Switch 上创建流分类 c1，匹配 ACL3000

```
[Switch] traffic classifier c1
[Switch-classifier-c1] if-match acl 3000
[Switch-classifier-c1] quit
```

4． 配置流行为

在 Switch 上创建流行为 b1，动作为流量监管，承诺信息速率为 2M，峰值速率不能超过 4M；

```
[Switch] traffic behavior b1
[Switch-behavior-b1] car cir 2048 pir 4096 green pass yellow discard red discard //只承诺 2M 的带宽，可以突发到 4M，超过 4M 的全部丢弃
 [Switch-behavior-b1] quit
```

5． 配置流策略并应用到接口

在 Switch 上创建流策略 p1，将流分类和对应的流行为进行绑定。

```
[Switch] traffic policy p1
[Switch-trafficpolicy-p1] classifier c1 behavior b1
[Switch-trafficpolicy-p1] quit
```

将流策略 p1 应用到接口 GE0/0/3 的入方向上。

```
[Switch] interface gigabitethernet 0/0/3
[Switch-GigabitEthernet0/0/3] traffic-policy p1 inbound
[Switch-GigabitEthernet0/0/3] quit
```

说明：

交换机可以配置基于每个 IP 地址限速，但是如果 IP 地址太多的话会浪费掉大量的 ACL 资源，并且

在配置的时候也是比较繁琐的，每 IP 限速不建议做在交换机侧，可以做在出口路由器或者防火墙上面。

8.4 通过流策略实现流量统计

如图 8-4 所示，公司内部有两个部门，分别属于 VLAN10 和 VLAN20，限制网络管理员想知道 VLAN20 里面的 192.168.1.200 这台主机是否有访问 VLAN10 内的服务器 192.168.1.100 的流量，可以通过流策略来实现流量统计功能；此外在处理网络故障的是可以通过流量统计来排查是否是网络设备丢了数据流；

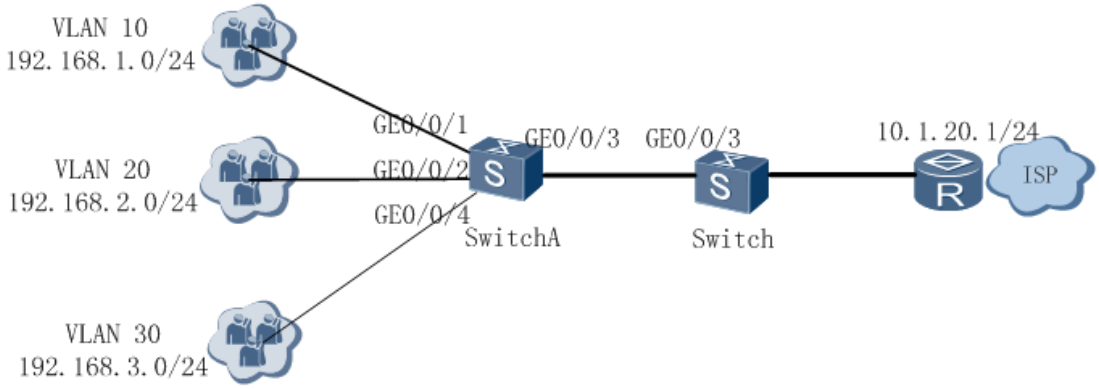


图 8-4　配置流策略实现流量统计组网图

配置思路：

1．　创建 VLAN 并配置各接口，配置路由实现公司和外部网络互通；

2．　配置 ACL 规则，匹配源 192.168.2.100 到目的 192.168.1.100 的数据流；

3．　配置流分类，匹配规则为上述创建的 ACL 规则，使设备对报文可以区分；

4．　配置流行为，动作为开启流量统计；

5．　配置流策略，绑定上述流分类和流行为，并应用到 Switch 设备的 GE0/0/3 接口的入方向，实例流量统计的功能；

配置步骤：

1．　创建 VLAN 并配置各接口

#在 SwitchA 上面创建 vlan10 和 vlan20

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchA
[SwitchA] vlan batch 100 200
```

#配置 SwitchA 交换机，连接终端 PC 的接口为 Access 类型，GE0/0/1 加到 vlan10，GE0/0/2 加入到 vlan20，上联 Switch 的接口 GE0/0/3 配置为 trunk 类型，并允许 vlan10 和 vlan20 通过

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port link-type access
[SwitchA-GigabitEthernet0/0/1] port default vlan 10
[SwitchA-GigabitEthernet0/0/1] quit
```

```
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] port link-type access
[SwitchA-GigabitEthernet0/0/2] port default vlan 20
[SwitchA-GigabitEthernet0/0/2] quit
[SwitchA] interface gigabitethernet 0/0/3
[SwitchA-GigabitEthernet0/0/3] port link-type trunk
[SwitchA-GigabitEthernet0/0/3] port trunk allow-pass vlan 10 20
[SwitchA-GigabitEthernet0/0/3] quit
```

#在 Switch 上面配置 VLAN10 和 VLAN20，并配置 Switch 连接 SwitchA 的 GE0/0/3 接口类型为 trunk，并允许 VLAN10 和 VLAN20 通过

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] vlan batch 100 200
[SwitchA] interface gigabitethernet 0/0/3
[SwitchA-GigabitEthernet0/0/3] port link-type trunk
[SwitchA-GigabitEthernet0/0/3] port trunk allow-pass vlan 10 20
[SwitchA-GigabitEthernet0/0/3] quit
```

#配置 VLAN10 和 VLAN20 的网关 VLANIF10 和 VLANIF20 地址分别为 192.168.1.1/24 和 192.168.2.1/24

```
[Switch] interface vlanif 10
[Switch-Vlanif10] ip address 192.168.1.1 24
[Switch-Vlanif10] quit
[Switch] interface vlanif 20
[Switch-Vlanif20] ip address 192.168.2.1 24
[Switch-Vlanif20] quit
```

在 Switch 配置静态路由指向外网实现互通

```
[Switch] ip route-static 0.0.0.0 0 10.1.20.1
```

2． 创建 ACL 规则

#在 Switch 上创建编号为 3000 的 ACL，匹配 192.168.2.100 到 192.168.1.100 之间的数据流；

```
[Switch] acl 3000          //匹配 192.168.2.100 到 192.168.1.100 数据流
[Switch-acl-adv-3000] rule permit ip source 192.168.2.100 0.0.0.0 destination
192.168.1.100 0.0.0.0
[Switch-acl-adv-3000] quit
```

3． 配置流分类

#在 Switch 上创建流分类 c1，匹配 ACL3000

```
[Switch] traffic classifier c1
[Switch-classifier-c1] if-match acl 3000
[Switch-classifier-c1] quit
```

4． 配置流行为

在 Switch 上创建流行为 b1，开启流量统计

```
[Switch] traffic behavior b1
[Switch-behavior-b1] statistic enable
[Switch-behavior-b1] quit
```

5． 配置流策略并应用到接口

在 Switch 上创建流策略 p1，将流分类和对应的流行为进行绑定。

```
[Switch] traffic policy p1
[Switch-trafficpolicy-p1] classifier c1 behavior b1
[Switch-trafficpolicy-p1] quit
```

将流策略 p1 应用到接口 GE0/0/3 的入方向上。

```
[Switch] interface gigabitethernet 0/0/3
[Switch-GigabitEthernet0/0/3] traffic-policy p1 inbound
[Switch-GigabitEthernet0/0/3] quit
```

6． 查看流量统计的结果

```
[Switch] display traffic policy statistics interface gigabitethernet 0/0/3
inbound
```

8.5 通过流策略配置PING报文的流量统计

在处理网络故障的时候会出现 ping 不通的情况，这个时候可以通过配置流量统计来看哪个设备在哪把流量丢了；

如图 8-5，客户有一台 PC1 无法访问 Server，这个时候可以在数据流经过的设备做流量统计来看到底在哪把报文丢弃了。

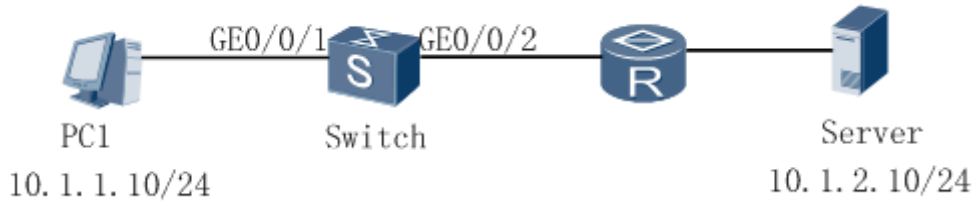


图8-5 流量统计示例图

配置思路

1． 配置 ACL，匹配协议为 ICMP、源目地址分别为 PC1 和 Server 的地址；

2． 配置流分类，

3． 配置流行为，动作为开启流量统计；

4． 配置流策略，把上面配置的流分类和流行为绑定在一起；

5． 应用流策略，在 Swithc 的接口 GE0/0/1 应用流策略；

配置步骤

1． 配置 ACL

#匹配协议为 ICMP，源目地址分别为 10.1.1.10 和 10.1.2.10 的数据流

```
<Huawei> system-view
[Huawei] sysname Switch
[Switch] acl number 3333
[Switch-acl-adv-3333] rule permit icmp source 10.1.1.10 0 destination 10.1.2.10 0
[Switch-acl-adv-3333] rule permit icmp source 10.1.2.10 0 destination 10.1.1.10 0
```

2． 配置流分类

#配置流分类 c1，匹配上述创建的 acl 3333

```
[Switch] traffic classifier c1
[Switch-classifier-c1] if-match acl 3333
```

3． 配置流行为

#配置流行为 b1，动作为开启流量统计

```
[Switch] traffic behavior b1
[Switch-behavior-b1] statistic enable
```

4． 配置流策略

#将配置流策略 p1，将上面配置的流分类和流行为绑定在一起

```
[Switch] traffic policy p1
[Switch-trafficpolicy-p1] classifier c1 behavior b1
```

5． 应用流策略

#在交换机 Switch 连接 PC1 的接口出入方向调用流策略 p1

```
[Switch] interface GigabitEthernet 0/0/1
[Switch-GigabitEthernet0/0/1] traffic-policy p1 inbound
[Switch-GigabitEthernet0/0/1] traffic-policy p1 outbound
[Switch-GigabitEthernet0/0/1] quit
```

6． 检测配置结果接流量统计结果

#首先确认流量统计配置是否正确

```
<Switch> display traffic policy user-defined p1
  User Defined Traffic Policy Information:
  Policy: p1
   Classifier: c1
    Operator: AND
     Behavior: b1
      Statistic: enable
```

#在 PC1 上进行 ping Server 的操作

#在交换机查看流量统计的结果

```
<Switch> display traffic policy statistics interface g0/0/1 inbound
 #查看入接口方向的流量统计结果
<Switch> display traffic policy statistics interface g0/0/1 outbound
#查看出接口方向的流量统计结果
```

如果两者相同表示是正常的，如果入方向为 0 表示 PC1 发的数据包没有到交换机，如果入方向不为 0，但是出方向为 0，表示数据到交换机了，但是对端没有回应过来，可以继续在其他设备做流量统计；

8.6 交换机通过流策略限制部分用户在特定时间无法上网

如图 8-6 所示，公司内部有两个部门，分别属于 VLAN10 和 VLAN20，VLAN10 主要是服务器区为内网和外网用户提供服务，VLAN20 内的都是公司员工办公的，现在有个需求就是在上班期间（8:00-18:00）限制 VLAN20 内网的用户访问公网影响办公，只能访问内网 VLAN10 里面的服务器提供的服务；

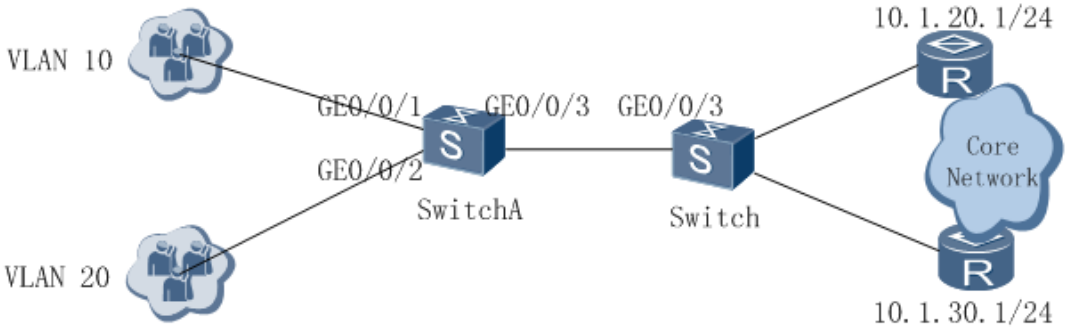


图 8-6　交换机通过流策略限制部分用户特定时间无法上网组网图

配置思路：

1．　创建 VLAN 并配置各接口，配置路由实现公司和外部网络互通；

2．　配置时间段，定义时间段为周一到周五 8:00-18:00，使设备可以根据时间段对报文做控制；

3．　配置 ACL 规则并结合上面配置的时间段，分别匹配 VLAN20 访问 VLAN10 的流量和 VLAN20 的用户访问公网的数据流；

4．　配置流分类，匹配规则为上述创建的 ACL 规则，使设备对报文可以区分；

5．　配置流行为，动作为允许数据流通过；

6． 配置流策略，绑定上述流分类和流行为，并应用到 Switch 设备的 GE0/0/3 接口的入方向，实现 VLAN20 的用户无法在上班期间上网但是下班时间可以正常上网的需求；

配置步骤：

1． 创建 VLAN 并配置各接口

#在 SwitchA 上面创建 vlan10 和 vlan20

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchA
[SwitchA] vlan batch 100 200
```

#配置 SwitchA 交换机，连接终端 PC 的接口为 Access 类型，GE0/0/1 加到 vlan10，GE0/0/2 加入到 vlan20，上联 Switch 的接口 GE0/0/3 配置为 trunk 类型，并允许 vlan10 和 vlan20 通过

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port link-type access
[SwitchA-GigabitEthernet0/0/1] port default vlan 10
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] port link-type access
[SwitchA-GigabitEthernet0/0/2] port default vlan 20
[SwitchA-GigabitEthernet0/0/2] quit
[SwitchA] interface gigabitethernet 0/0/3
[SwitchA-GigabitEthernet0/0/3] port link-type trunk
[SwitchA-GigabitEthernet0/0/3] port trunk allow-pass vlan 10 20
[SwitchA-GigabitEthernet0/0/3] quit
```

#在 Switch 上面配置 VLAN10 和 VLAN20，并配置 Switch 连接 SwitchA 的 GE0/0/3 接口类型为 trunk，并允许 VLAN10 和 VLAN20 通过

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] vlan batch 100 200
[SwitchA] interface gigabitethernet 0/0/3
[SwitchA-GigabitEthernet0/0/3] port link-type trunk
[SwitchA-GigabitEthernet0/0/3] port trunk allow-pass vlan 10 20
[SwitchA-GigabitEthernet0/0/3] quit
```

#配置 VLAN10 和 VLAN20 的网关 VLANIF10 和 VLANIF20 地址分别为 192.168.1.1/24 和 192.168.2.1/24

```
[Switch] interface vlanif 10
```

```
[Switch-Vlanif10] ip address 192.168.1.1 24
[Switch-Vlanif10] quit
[Switch] interface vlanif 20
[Switch-Vlanif20] ip address 192.168.2.1 24
[Switch-Vlanif20] quit
```

在 Switch 配置静态路由指向外网实现互通

```
[Switch] ip route-static 0.0.0.0 0 10.1.20.1
```

2. 创建时间段

#创建时间段 worktime，规定 worktime 的时间为周一至周五 8:00-18:00

```
[Switch] time-range worktime 8:00 to 18:00 working-day
```

3. 创建 ACL 规则

#在 Switch 上创建编号为 3000 的 ACL，第一条规则匹配 VLAN20 访问 VLAN10 的数据流并结合时间段 worktime，第二条规则匹配 VLAN20 访问公网的数据流并结合时间 worktime

```
[Switch] acl 3000
[Switch-acl-adv-3000] rule permit ip source 192.168.2.0 0.0.0.255 destination 192.168.1.0 0.0.0.255 time-range worktime
[Switch-acl-adv-3000] rule deny ip source 192.168.2.0 0.0.0.255 time-range worktime
[Switch-acl-adv-3000] quit
```

4. 配置流分类

#在 Switch 上创建流分类 c1，匹配 ACL3000

```
[Switch] traffic classifier c1
[Switch-classifier-c1] if-match acl 3000
[Switch-classifier-c1] quit
```

5. 配置流行为

在 Switch 上创建流行为 b1，动作为 permit 允许数据流通过

```
[Switch] traffic behavior b1
[Switch-behavior-b1] permit
[Switch-behavior-b1] quit
```

6. 配置流策略并应用到接口

在 Switch 上创建流策略 p1，将流分类和对应的流行为进行绑定。

```
[Switch] traffic policy p1
[Switch-trafficpolicy-p1] classifier c1 behavior b1
[Switch-trafficpolicy-p1] quit
```

将流策略 p1 应用到接口 GE0/0/3 的入方向上。

```
[Switch] interface gigabitethernet 0/0/3
[Switch-GigabitEthernet0/0/3] traffic-policy p1 inbound
[Switch-GigabitEthernet0/0/3] quit
```

7. 查看流量统计的结果

```
[Switch] display traffic policy statistics interface gigabitethernet 0/0/3 inbound
```

8.7 交换机配置接口限速示例

组网需求

如图 8-7 所示，Switch 通过接口 GE0/0/3 与路由器互连，企业部门 1 和企业部门 2 通过接口 GE0/0/1 和 GE0/0/2 接入 Switch，经由 Switch 和路由器访问网络。

由于业务较单一，不需要对业务进行区分，但是网络带宽有限，因此需要对企业各个部门的接入带宽进行整体限制。要求企业部门 1 入方向保证带宽为 8Mbit/s，最高不超过 10Mbit/s；企业部门 2 入方向保证带宽为 5Mbit/s，最高不超过 8Mbit/s。

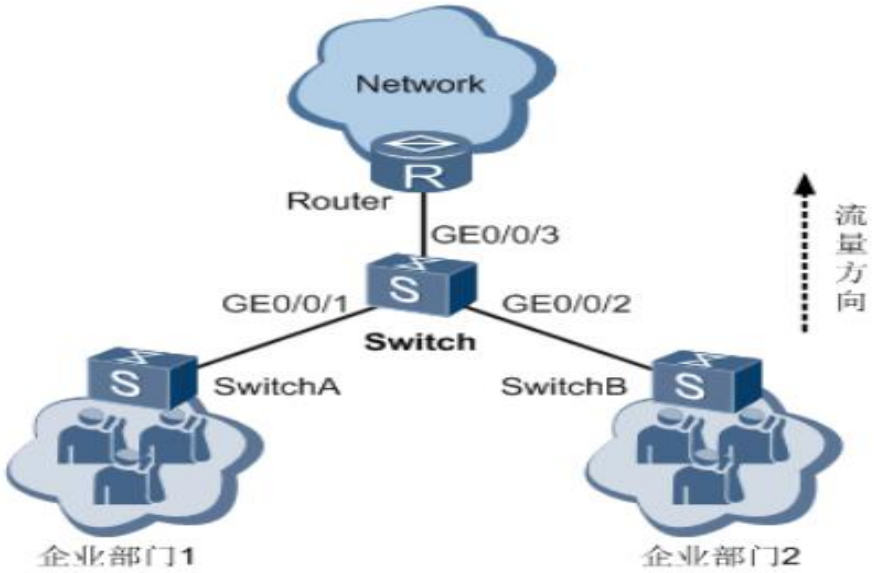


图 8-7 接口限速配置组网图

配置思路

采用如下的思路配置接口限速：

1. 配置 Switch 的各接口，使用户能够访问网络。
2. 在 Switch 接口 GE0/0/1 和 GE0/0/2 的入方向配置接口限速。

配置步骤

1. 创建 VLAN 并配置 Switch 各接口

创建 VLAN100、VLAN200 和 VLAN300。

```
<HUAWEI> system-view
```

```
[HUAWEI] sysname Switch
[Switch] vlan batch 100 200 300
```

将接口 GE0/0/1、GE0/0/2 和 GE0/0/3 的接入类型均配置为 trunk，并配置 GE0/0/1 允许 VLAN100 通过，配置 GE0/0/2 允许 VLAN200 通过，配置 GE0/0/3 允许 VLAN100、VLAN200 和 VLAN300 通过。

```
[Switch] interface gigabitethernet 0/0/1
[Switch-GigabitEthernet0/0/1] port link-type trunk
[Switch-GigabitEthernet0/0/1] port trunk allow-pass vlan 100
[Switch-GigabitEthernet0/0/1] quit
[Switch] interface gigabitethernet 0/0/2
[Switch-GigabitEthernet0/0/2] port link-type trunk
[Switch-GigabitEthernet0/0/2] port trunk allow-pass vlan 200
[Switch-GigabitEthernet0/0/2] quit
[Switch] interface gigabitethernet 0/0/3
[Switch-GigabitEthernet0/0/3] port link-type trunk
[Switch-GigabitEthernet0/0/3] port trunk allow-pass vlan 100 200 300
[Switch-GigabitEthernet0/0/3] quit
```

创建 VLANIF300，并配置网段地址 192.168.1.1/24。

```
[Switch] interface vlanif 300
[Switch-Vlanif300] ip address 192.168.1.1 24
[Switch-Vlanif300] quit
```

请在 Router 上的与 Switch 对接的接口上配置 IP 地址 192.168.1.2/24。

2. 配置接口限速

在接口 GE0/0/1 的入方向上配置接口限速，保证带宽为 8192kbit/s。

```
[Switch] interface gigabitethernet 0/0/1
[Switch-GigabitEthernet0/0/1] qos lr inbound cir 8192
[Switch-GigabitEthernet0/0/1] quit
```

在接口 GE0/0/2 的入方向上配置接口限速，保证带宽为 5120kbit/s。

```
[Switch] interface gigabitethernet 0/0/2
[Switch-GigabitEthernet0/0/2] qos lr inbound cir 5120
[Switch-GigabitEthernet0/0/2] quit
```

3. 验证配置结果

查看接口限速的配置信息。

```
[Switch] display qos lr inbound interface gigabitethernet 0/0/1
```

```
 GigabitEthernet0/0/1 lr inbound:
  cir: 8192 Kbps, cbs: 1024000 Byte
[Switch] display qos lr inbound interface gigabitethernet 0/0/2
 GigabitEthernet0/0/2 lr inbound:
  cir: 5120 Kbps, cbs: 640000 Byte
```

9 SNMP配置

一、 功能简介

1.在大型网络中，设备发生故障时，由于设备无法主动上报故障，导致网络管理员无法及时感知、及时定位和排除故障，从而导致网络的维护效率降低，维护工作量大大增加。为了解决这个问题，设备制造商在一些设备中提供网络管理的功能，网络管理员可以通过网管系统远程查询设备的状态，同样设备能够在特定类型的事件发生时向网络管理工作站发出警告。

2.SNMP 就是规定网络管理系统 NMS 和被管理设备之间如何传递管理信息的应用层协议。SNMP 定义了网管管理设备的几种操作，以及设备发生故障时能向网管主动发送告警。

3.交换机支持的 SNMP 协议有三个版本：SNMPv1、SNMPv2c 和 SNMPv3，SNMP 各版本支持的特性如表所示；

特性	SNMPv1	SNMPv2c	SNMPv3
访问控制	基于团体名和 MIB View 进行访问控制	基于团体名和 MIB View 进行访问控制	基于用户、用户组和 MIB View 进行访问控制
认证加密	基于团体名的认证	基于团体名的认证	支持认证和加密，认证和加密的方式如下： 认证：MD5、SHA 加密：DES56、AES128、AES256、3DES
错误码	支持 6 个错误码	支持 16 个错误码	支持 16 个错误码
Trap 告警	支持	支持	支持
Inform 告警	不支持	支持	不支持
GetBulk	不支持	支持	支持

二、 配置命令和步骤

1.SNMPv1 和 SNMPv2c 配置：

A. 执行命令 **snmp-agent sys-info version v1/v2**，配置 SNMP 的协议版本为 SNMPv1 或者 SNMPv2c；

B.执行命令 **snmp-agent community { read | write }** { community-name | cipher community-name }，配置设备的读写团体名。

团体名将以密文形式保存在配置文件中。

C. 配置设备发送告警和错误码的目的 IP 地址：**snmp-agent target-host trap address udp-domain**

2.SNMPv3 配置：

A.执行命令 **snmp-agent sys-info version v3**，配置 SNMP 的协议版本。

B.执行命令 **snmp-agent group v3** group-name，配置 SNMPv3 用户组。

C.执行命令 **snmp-agent usm-user v3** user-name 配置 SNMPv3 用户。

D.执行命令 **snmp-agent usm-user v3** user-name **authentication-mode** { md5 | sha } [cipher password]，配置 SNMPv3 用户认证密码。

E.执行命令 **snmp-agent usm-user v3** user-name **privacy-mode** { des56 | aes128 |aes192 | aes256 | 3des } [cipher password]，配置 SNMPv3 用户加密密码。

F. 配置设备发送告警和错误码的目的 IP 地址：**snmp-agent target-host trap address udp-domain**

三、应用场景

9.1 配置设备使用SNMPv1与网管通信示例

组网需求

如图 9-1 所示，现有网络中网管服务器对网络中的设备进行监管。由于网络规模较小，安全性较高等因素，在规划时配置设备使用 SNMPv1 版本与网管进行通信，用户希望通过利用现有的网络资源对交换机进行监管，并且对发生故障能够快速对故障定位和排除。

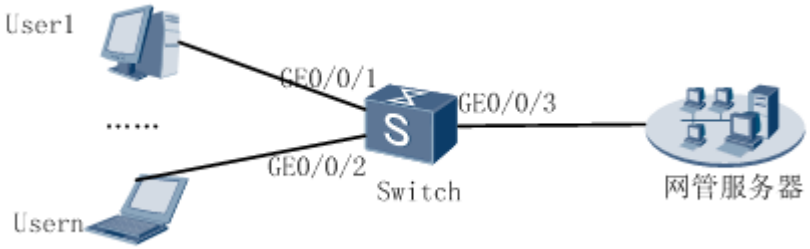


图9-1 配置设备使用SNMPv1与网管通信示例

配置思路

1.配置交换机的 SNMP 版本为 SNMPv1。

2.配置团体名为 huawei 且具有读写属性。

3.配置交换机的 Trap 功能，使交换机产生的告警能够发送至网服务器。为了方便对告警信息进行定位，避免过多的无用告警对处理问题造成干扰，仅允许缺省打开的模块可以发送告警。

4.配置网管服务器。

详细配置步骤

1.配置交换机的接口 IP 地址

按图 1 所示，配置交换机的接口 IP 地址。

```
<HUAWEI> system-view
```

```
[HUAWEI] vlan 100
[HUAWEI-vlan100] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type access
[HUAWEI-GigabitEthernet0/0/1] port default vlan 100
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 1.1.1.1 24
[HUAWEI-Vlanif100] quit
```

2.配置交换机的 SNMP 版本为 SNMPv1

```
[HUAWEI] snmp-agent sys-info version v1
```

3.配置团体名和读写属性

```
[HUAWEI] snmp-agent community write huawei
```

注意：如果这个地方配置简单的团体名无法配置的话，关闭团体名复杂度检查 **snmp-agent community complexity-check disable**（具体请参考自己版本对应的手册）

#配置告警功能

```
[HUAWEI] snmp-agent target-host trap address udp-domain 1.1.1.2 params securityname huawei
```

4.配置网管服务器（略）

在使用 SNMPv1 版本的网关服务器上需要设置"读/写团体名"。网管的配置请根据采用的网管产品参考对应的网管配置手册。

9.2 配置设备使用SNMPv2与网管通信示例

最基本的配置和上面配置 SNMPv1 的一样，只是选择版本的时候是 v2c，下面列出一些更多的配置；

组网需求

如图 9-2 所示，现有网络中网管 NMS1 和 MNS2 对网络中的设备进行监管。由于网络规模较大，安全性较高，但运行的业务较为繁忙，在规划时配置设备使用 SNMPv2c 版本与网管进行通信。现在由于扩容需要，新增一台交换机，并由网管对其进行监管。

用户希望通过利用现有的网络资源对交换机进行监管，并且对发生故障能够快速对故障定位和排除。根据用户业务需要，网管站需要对交换机的除 ISIS 的之外的节点管理。

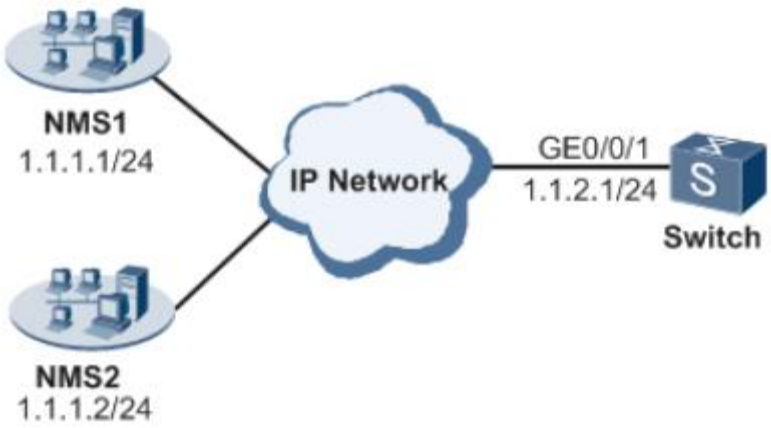


图9-2 配置使用SNMPv2c与网管通信组网图

配置思路

考虑到用户所在网络规模较大，安全性较高，业务较繁忙等因素，因此新增设备依然使用 SNMPv2c 版本。为减轻网管站的负担，选取 NMS2 来监管交换机，NMS1 不监管交换机。

采用如下的配置思路：

1.组网基础配置，包括接口和 VLAN 信息。

2.配置交换机的 SNMP 版本为 SNMPv2c。

3.配置用户访问权限，使 NMS2 可以管理交换机上 ISIS 之外的节点。

4.配置交换机的 Inform 告警功能，使交换机产生的告警能够发送至 NMS2。为了方便对告警信息进行定位，避免过多的无用告警对处理问题造成干扰，仅允许缺省打开的模块可以发送告警。

5.配置网管站（仅 NMS2）。

详细配置步骤

1.配置交换机的接口 IP 地址

按图 2 所示，配置交换机的接口 IP 地址。

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type access
[HUAWEI-GigabitEthernet0/0/1] port default vlan 100
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 1.1.2.1 24
[HUAWEI-Vlanif100] quit
```

配置交换机和网管站之间路由可达

```
[HUAWEI] ospf
```

```
[HUAWEI-ospf-1] area 0
[HUAWEI-ospf-1-area-0.0.0.0] network 1.1.2.0 0.0.0.255
[HUAWEI-ospf-1-area-0.0.0.0] quit
[HUAWEI-ospf-1] quit
```

2.配置交换机的 SNMP 版本为 SNMPv2c

```
[HUAWEI] snmp-agent sys-info version v2c
```

3.配置网管站的访问权限

配置 ACL，使 NMS2 可以管理交换机，NMS1 不允许管理交换机。

```
[HUAWEI] acl 2001
[HUAWEI-acl-basic-2001] rule 5 permit source 1.1.1.2 0.0.0.0
[HUAWEI-acl-basic-2001] rule 6 deny source 1.1.1.1 0.0.0.0
[HUAWEI-acl-basic-2001] quit
```

配置 MIB 视图，限制 NMS2 可以管理交换机上除 ISIS 之外的节点。

```
[HUAWEI] snmp-agent mib-view excluded allextisis 1.3.6.1.3.37
```

配置团体名并引用 ACL 和 MIB 视图。

```
[HUAWEI] snmp-agent community write adminnms2 mib-view allextisis acl 2001
```

4.配置告警功能

```
[HUAWEI] snmp-agent target-host inform address udp-domain 1.1.1.2 params
securityname adminnms2 v2c
```

5.配置网管站（NMS2）

在使用 SNMPv2c 版本的 NMS 上需要设置“读/写团体名”。网管的配置请根据采用的网管产品参考对应的网管配置手册。

9.3 配置设备使用SNMPv3与网管通信示例

组网需求

如图 9-3 所示，现有网络中网管 NMS1 和 MNS2 对网络中的设备进行监管。由于网络规模较大，安全性较低，在规划时配置设备使用 SNMPv3 版本与网管进行通信，并配置认证加密功能保证安全性。用户希望通过利用现有的网络资源对交换机进行监管，并且对发生故障能够快速对故障定位和排除。

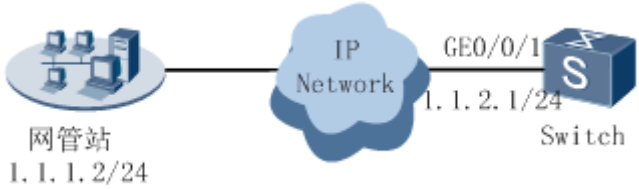


图3 配置使用SNMPv3与网管通信组网图

配置思路

考虑到用户所在网络规模较大，安全性较低，因此新增设备依然使用 SNMPv3 版本。

1.组网基础配置，包括接口、VLAN 等信息。

2.配置交换机的 SNMP 版本为 SNMPv3。

3.配置 MIB 视图，使 NMS 可以管理 ISO 节点。

4.配置交换机的 Trap 功能，使交换机产生的告警能够发送至 NMS。为了方便对告警信息进行定位，避免过多的无用告警对处理问题造成干扰，仅允许缺省打开的模块可以发送告警。

5.配置网管站。

详细配置步骤

1.组网基础配置

按图 3 所示，配置交换机的接口、IP 地址。

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type access
[HUAWEI-GigabitEthernet0/0/1] port default vlan 100
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 1.1.2.1 24
[HUAWEI-Vlanif100] quit
```

配置交换机和网管站之间路由可达

```
[HUAWEI] ospf
[HUAWEI-ospf-1] area 0
[HUAWEI-ospf-1-area-0.0.0.0] network 1.1.2.0 0.0.0.255
[HUAWEI-ospf-1-area-0.0.0.0] quit
[HUAWEI-ospf-1] quit
```

2.配置交换机的 SNMP 版本为 SNMPv3。

```
[HUAWEI] snmp-agent sys-info version v3
```

3.# 配置 MIB 视图。

```
[HUAWEI] snmp-agent mib-view included isoview iso
```

配置用户组和用户，对用户的数据进行认证和加密。

```
[HUAWEI] snmp-agent usm-user v3 nms-admin group admin
[HUAWEI] snmp-agent usm-user v3 nms-admin authentication-mode md5
Please configure the authentication password (8-64)
```

```
Enter Password:
Confirm Password:
[HUAWEI] snmp-agent usm-user v3 nms-admin privacy-mode aes128
Please configure the privacy password (8-64)
Enter Password:
Confirm Password:
[HUAWEI] snmp-agent group v3 admin privacy write-view isoview
```

4.配置告警功能。

```
[HUAWEI] snmp-agent target-host trap address udp-domain 1.1.1.2 params
securityname nms-admin v3 privacy
```

5.配置网管站。

在使用 SNMPv3 版本的 NMS 上需要设置用户名，选择安全级别。根据不同的安全级别，需要分别设置认证方式、认证密码、加密方式、加密密码等。网管的配置请根据采用的网管产品参考对应的网管配置手册。

10 VRRP配置

一. 功能简介

虚拟路由冗余协议 VRRP（Virtual Router Redundancy Protocol）通过把几台路由设备联合组成一台虚拟的路由设备，将虚拟网关设备的 IP 地址作为用户的默认网关实现与外部网络通信。当网关设备发生故障时，VRRP 机制能够选举新的网关设备承担数据流量，从而保障网络的可靠通信。

二. 配置命令和步骤

1.执行命令 **vrrp vrid** *virtual-router-id* **virtual-ip** *virtual-address*，接口视图创建 VRRP 备份组并给备份组配置虚拟 IP 地址。

2.执行命令 **vrrp vrid** *virtual-router-id* **priority** *priority-value*，配置交换机在备份组中的优先级。 缺省情况下，优先级的取值是100。数值越大，优先级越高，优先级越高，越可能成为 master 设备。

3.执行命令 **vrrp vrid** *virtual-router-id* **preempt-mode timer delay** *delay-value*，配置备份组中交换机的抢占延迟时间。

4.执行命令 **vrrp vrid** *virtual-router-id* **track bfd-session** { bfd-session-id | session-name bfd-configure-name } [increased value-increased | reduced value-reduced]，备设备 Backup 接口视图下，配置 VRRP 与 BFD 联动。

5.执行命令 **vrrp vrid** *virtual-router-id* **track interface** *interface-type interface-number* [increased value-increased | reduced value-reduced]，配置 VRRP 与接口状态联动监视上行接口。

三. 应用场景

10.1 配置VRRP主备备份示例

组网需求

如图10-1所示，HostA 通过 Switch 双归属到 SwitchA 和 SwitchB。

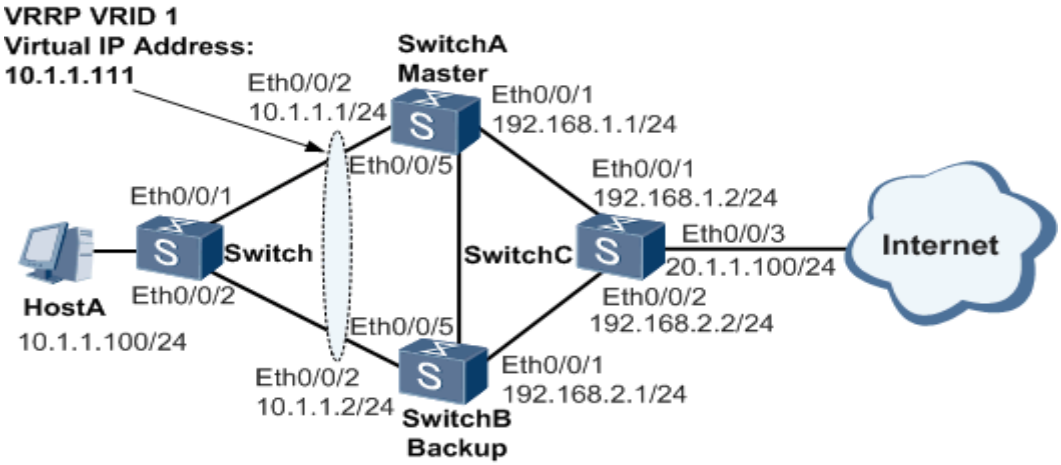


图10-1 配置VRRP主备备份组网图

用户希望实现：

- 正常情况下，主机以 SwitchA 为默认网关接入 Internet，当 SwitchA 故障时，SwitchB 接替作为网关继续进行工作，实现网关的冗余备份。
- SwitchA 故障恢复后，可以在20秒内重新成为网关。

设备	接口	对应的 Vlanif	IP 地址
SwitchA	Eth0/0/1	VLANIF300	192.168.1.1/24
	Eth0/0/2	VLANIF100	10.1.1.1/24
	Eth0/0/5	VLANIF100	10.1.1.1/24
SwitchB	Eth0/0/1	VLANIF200	192.168.2.1/24
	Eth0/0/2	VLANIF100	10.1.1.2/24
	Eth0/0/5	VLANIF100	10.1.1.2/24
SwitchC	Eth0/0/1	VLANIF300	192.168.1.2/24
	Eth0/0/2	VLANIF200	192.168.2.2/24
	Eth0/0/3	VLANIF400	20.1.1.100/24

配置思路

采用 VRRP 主备备份实现网关冗余备份，配置思路如下：

1． 配置各设备接口 IP 地址及路由协议，使各设备间网络层连通。

2． 在 SwitchA 和 SwitchB 上配置 VRRP 备份组。其中，SwitchA 上配置较高优先级和20秒抢占延时，作为 Master 设备承担流量转发；SwitchB 上配置较低优先级，作为备用交换机，实现网关冗余备份。

3． 在 SwitchA、SwitchB 和 Switch 上配置破环协议，防止环路的产生（此处以配置 STP 为例）。

详细配置步骤

SwitchA 设备配置如下：

1、配置设备间的网络互连

配置 SwitchA 设备各接口的 IP 地址。

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] vlan batch 100 300
[SwitchA] interface ethernet 0/0/1
[SwitchA-Ethernet0/0/1] port link-type access
[SwitchA-Ethernet0/0/1] port default vlan 300
[SwitchA-Ethernet0/0/1] quit
[SwitchA] interface ethernet 0/0/2
[SwitchA-Ethernet0/0/2] port link-type access
[SwitchA-Ethernet0/0/2] port default vlan 100
[SwitchA-Ethernet0/0/2] quit
[SwitchA] interface ethernet 0/0/5
[SwitchA-Ethernet0/0/5] port link-type access
[SwitchA-Ethernet0/0/5] port hybrid untagged vlan 100
[SwitchA-Ethernet0/0/5] quit
[SwitchA] interface vlanif 100
[SwitchA-Vlanif100] ip address 10.1.1.1 24
[SwitchA-Vlanif100] quit
[SwitchA] interface vlanif 300
[SwitchA-Vlanif300] ip address 192.168.1.1 24
[SwitchA-Vlanif300] quit
```

2、配置 VRRP 备份组

在 SwitchA 上创建 VRRP 备份组1，配置 SwitchA 在该备份组中的优先级为120，并配置抢占时间为20秒。

```
[SwitchA] interface vlanif 100
```

```
[SwitchA-Vlanif100] vrrp vrid 1 virtual-ip 10.1.1.111
[SwitchA-Vlanif100] vrrp vrid 1 priority 120
[SwitchA-Vlanif100] vrrp vrid 1 preempt-mode timer delay 20
[SwitchA-Vlanif100] quit
```

3、配置 SwitchA 和 SwitchC 间采用静态路由协议进行互连。

```
[SwitchA]ip route-static 0.0.0.0 0.0.0.0 192.168.1.2
```

4、配置 STP 协议

在 SwitchA 上全局使能 STP。

```
[SwitchA]stp enable
```

SwitchB 设备配置如下：

1、配置设备间的网络互连

配置 SwitchB 设备各接口的 IP 地址。

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] vlan batch 100 200
[SwitchB] interface ethernet 0/0/1
[SwitchB-Ethernet0/0/1] port link-type access
[SwitchB-Ethernet0/0/1] port default vlan 200
[SwitchB-Ethernet0/0/1] quit
[SwitchB] interface ethernet 0/0/2
[SwitchB-Ethernet0/0/2] port link-type access
[SwitchB-Ethernet0/0/2] port default vlan 100
[SwitchB-Ethernet0/0/2] quit
[SwitchB] interface ethernet 0/0/5
[SwitchB-Ethernet0/0/5] port link-type access
[SwitchB-Ethernet0/0/5] port hybrid untagged vlan 100
[SwitchB-Ethernet0/0/5] quit
[SwitchB] interface vlanif 100
[SwitchB-Vlanif100] ip address 10.1.1.2 24
[SwitchB-Vlanif100] quit
[SwitchB] interface vlanif 300
[SwitchB-Vlanif300] ip address 192.168.2.1 24
[SwitchB-Vlanif300] quit
```

1、配置 VRRP 备份组

在 SwitchB 上创建 VRRP 备份组1，其在该备份组中的优先级为缺省值100。

```
[SwitchB] interface vlanif 100
[SwitchB-Vlanif100] vrrp vrid 1 virtual-ip 10.1.1.111
[SwitchB-Vlanif100] quit
```

2、配置 SwitchB 和 SwitchC 间采用静态路由协议进行互连。

```
[SwitchA]ip route-static 0.0.0.0 0.0.0.0 192.168.2.2
```

3、配置 STP 协议

在 SwitchB 上全局使能 STP。

```
[SwitchB]stp enable
```

SwitchC 设备配置如下：

1、配置设备间的网络互连

配置 SwitchC 设备各接口的 IP 地址。

```
<Quidway> system-view
[Quidway] sysname SwitchC
[SwitchC] vlan batch 200 300 400
[SwitchC] interface ethernet 0/0/1
[SwitchC-Ethernet0/0/1] port link-type access
[SwitchC-Ethernet0/0/1] port default vlan 300
[SwitchC-Ethernet0/0/1] quit
[SwitchC] interface ethernet 0/0/2
[SwitchC-Ethernet0/0/2] port link-type access
[SwitchC-Ethernet0/0/2] port default vlan 200
[SwitchC-Ethernet0/0/2] quit
[SwitchC] interface ethernet 0/0/3
[SwitchC-Ethernet0/0/5] port link-type access
[SwitchC-Ethernet0/0/5] port hybrid untagged vlan 400
[SwitchC-Ethernet0/0/5] quit
[SwitchC] interface vlanif 200
[SwitchC-Vlanif100] ip address 192.168.2.2 24
[SwitchC-Vlanif100] quit
[SwitchC] interface vlanif 300
[SwitchC-Vlanif300] ip address 192.168.1.2 24
[SwitchC-Vlanif300] quit
[SwitchC] interface vlanif 400
```

```
[SwitchC-Vlanif300] ip address 20.1.1.100 24
[SwitchC-Vlanif300] quit
```

2、配置 SwitchC 和 Switch A 、SwitchB 间采用静态路由协议进行互连。

```
[SwitchC]ip route-static 10.1.1.0 255.255.255.0 192.168.1.1
[SwitchC]ip route-static 10.1.1.0 255.255.255.0 192.168.2.1
```

Switch 设备配置如下：

1、配置 Switch 的二层透传功能。

```
<Quidway> system-view
[Quidway] sysname Switch
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] interface ethernet 0/0/1
[Switch-Ethernet0/0/1] port link-type access
[Switch-Ethernet0/0/1] port default vlan 100
[Switch-Ethernet0/0/1] quit
[Switch] interface ethernet 0/0/2
[Switch-Ethernet0/0/2] port link-type access
[Switch-Ethernet0/0/2] port default vlan 100
[Switch-Ethernet0/0/2] quit
```

2、配置 STP 协议

在 SwitchC 上全局使能 STP。

```
[SwitchC]stp enable
```

10.2 配置VRRP负载分担示例

组网需求

如图10-2所示，HostA 和 HostC 通过 Switch 双归属到 SwitchA 和 SwitchB。为减轻 SwitchA 上数据流量的承载压力，HostA 以 SwitchA 为默认网关接入 Internet，SwitchB 作为备份网关；HostC 以 SwitchB 为默认网关接入 Internet，SwitchA 作为备份网关，以实现流量的负载均衡。

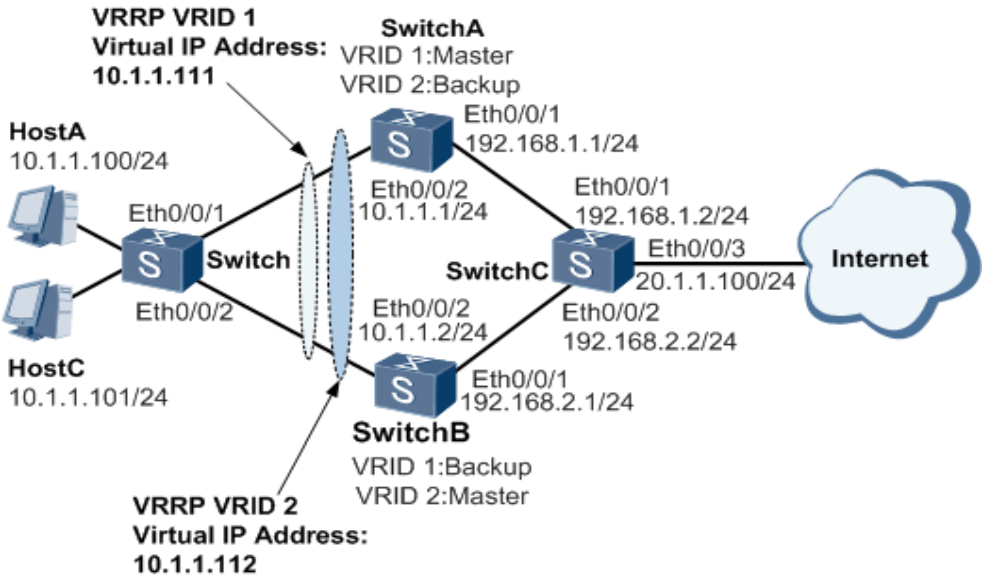


图10-2 配置VRRP负载分担组网图

设备	接口	对应的 Vlanif	IP 地址
SwitchA	Eth0/0/1	VLANIF300	192.168.1.1/24
	Eth0/0/2	VLANIF100	10.1.1.1/24
SwitchB	Eth0/0/1	VLANIF200	192.168.2.1/24
	Eth0/0/2	VLANIF100	10.1.1.2/24
SwitchC	Eth0/0/1	VLANIF300	192.168.1.2/24
	Eth0/0/2	VLANIF200	192.168.2.2/24
	Eth0/0/3	VLANIF400	20.1.1.100/24

配置思路

采用 VRRP 负载分担实现流量的负载均衡，配置思路如下：

1． 配置各设备接口 IP 地址及路由协议，使各设备间网络层连通。

2． 在 SwitchA 和 SwitchB 上创建 VRRP 备份组1和 VRRP 备份组2，在备份组1中，配置 SwitchA 为 Master 设备，SwitchB 为 Backup 设备；在备份组2中，配置 SwitchB 为 Master 设备，SwitchA 为 Backup 设备，实现流量的负载均衡。

详细配置步骤

SwitchA 设备配置如下：

1． 配置设备间的网络互连

配置 SwitchA 设备各接口的 IP 地址。

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] vlan batch 100 300
[SwitchA] interface ethernet 0/0/1
[SwitchA-Ethernet0/0/1] port link-type access
[SwitchA-Ethernet0/0/1] port default vlan 300
[SwitchA-Ethernet0/0/1] quit
[SwitchA] interface ethernet 0/0/2
[SwitchA-Ethernet0/0/2] port link-type access
[SwitchA-Ethernet0/0/2] port default vlan 100
[SwitchA-Ethernet0/0/2] quit
[SwitchA] interface vlanif 100
[SwitchA-Vlanif100] ip address 10.1.1.1 24
[SwitchA-Vlanif100] quit
[SwitchA] interface vlanif 300
[SwitchA-Vlanif300] ip address 192.168.1.1 24
[SwitchA-Vlanif300] quit
```

2．配置 VRRP 备份组

在 SwitchA 上创建 VRRP 备份组1，配置 SwitchA 在该备份组中的优先级为120，抢占延时为20秒，作为 Master 设备；

```
[SwitchA] interface vlanif 100
[SwitchA-Vlanif100] vrrp vrid 1 virtual-ip 10.1.1.111
[SwitchA-Vlanif100] vrrp vrid 1 priority 120
[SwitchA-Vlanif100] vrrp vrid 1 preempt-mode timer delay 20
[SwitchA-Vlanif100] quit
```

在 SwitchA 上创建 VRRP 备份组2，SwitchA 在该备份组中的优先级为缺省值，作为 Backup 设备。

```
[SwitchA] interface vlanif 100
[SwitchA-Vlanif100] vrrp vrid 2 virtual-ip 10.1.1.112
[SwitchA-Vlanif100] quit
```

3．配置 SwitchA 和 SwitchC 间采用静态路由协议进行互连。

```
[SwitchA]ip route-static 0.0.0.0 0.0.0.0 192.168.1.2
```

SwitchB 设备配置如下：

1．配置设备间的网络互连

配置 SwitchB 设备各接口的 IP 地址。

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] vlan batch 100 200
[SwitchB] interface ethernet 0/0/1
[SwitchB-Ethernet0/0/1] port link-type access
[SwitchB-Ethernet0/0/1] port default vlan 200
[SwitchB-Ethernet0/0/1] quit
[SwitchB] interface ethernet 0/0/2
[SwitchB-Ethernet0/0/2] port link-type access
[SwitchB-Ethernet0/0/2] port default vlan 100
[SwitchB-Ethernet0/0/2] quit
[SwitchB] interface vlanif 100
[SwitchB-Vlanif100] ip address 10.1.1.2 24
[SwitchB-Vlanif100] quit
[SwitchB] interface vlanif 200
[SwitchB-Vlanif300] ip address 192.168.2.1 24
[SwitchB-Vlanif300] quit
```

2． 配置 VRRP 备份组

在 SwitchB 上创建 VRRP 备份组2，配置 SwitchB 在该备份组中的优先级为120，抢占延时为20秒，作为 Master 设备；

```
[SwitchB] interface vlanif 100
[SwitchB-Vlanif100] vrrp vrid 2 virtual-ip 10.1.1.112
[SwitchB-Vlanif100] vrrp vrid 2 priority 120
[SwitchB-Vlanif100] vrrp vrid 2 preempt-mode timer delay 20
[SwitchB-Vlanif100] quit
```

在 SwitchB 上创建 VRRP 备份组1，SwitchB 在该备份组中的优先级为缺省值，作为 Backup 设备。

```
[SwitchB] interface vlanif 100
[SwitchB-Vlanif100] vrrp vrid 1 virtual-ip 10.1.1.111
[SwitchB-Vlanif100] quit
```

3． 配置 SwitchB 和 SwitchC 间采用静态路由协议进行互连。

```
[SwitchB]ip route-static 0.0.0.0 0.0.0.0 192.168.1.2
```

SwitchC 设备配置如下：

1． 配置设备间的网络互连

配置 SwitchC 设备各接口的 IP 地址。

```
<Quidway> system-view
[Quidway] sysname SwitchC
[SwitchC] vlan batch 200 300 400
[SwitchC] interface ethernet 0/0/1
[SwitchC-Ethernet0/0/1] port link-type access
[SwitchC-Ethernet0/0/1] port default vlan 300
[SwitchC-Ethernet0/0/1] quit
[SwitchC] interface ethernet 0/0/2
[SwitchC-Ethernet0/0/2] port link-type access
[SwitchC-Ethernet0/0/2] port default vlan 200
[SwitchC-Ethernet0/0/2] quit
[SwitchC] interface ethernet 0/0/3
[SwitchC-Ethernet0/0/5] port link-type access
[SwitchC-Ethernet0/0/5] port hybrid untagged vlan 400
[SwitchC-Ethernet0/0/5] quit
[SwitchC] interface vlanif 200
[SwitchC-Vlanif100] ip address 192.168.2.2 24
[SwitchC-Vlanif100] quit
[SwitchC] interface vlanif 300
[SwitchC-Vlanif300] ip address 192.168.1.2 24
[SwitchC-Vlanif300] quit
[SwitchC] interface vlanif 400
[SwitchC-Vlanif300] ip address 20.1.1.100 24
[SwitchC-Vlanif300] quit
```

2． 配置 SwitchC 和 Switch A 、SwitchB 间采用静态路由协议进行互连。

```
[SwitchC]ip route-static 10.1.1.0 255.255.255.0 192.168.1.1
[SwitchC]ip route-static 10.1.1.0 255.255.255.0 192.168.2.1
```

Switch 设备配置如下：

1． 配置 Switch 的二层透传功能。

```
<Quidway> system-view
[Quidway] sysname Switch
[Switch] vlan 100
```

```
[Switch-vlan100] quit
[Switch] interface ethernet 0/0/1
[Switch-Ethernet0/0/1] port link-type access
[Switch-Ethernet0/0/1] port default vlan 100
[Switch-Ethernet0/0/1] quit
[Switch] interface ethernet 0/0/2
[Switch-Ethernet0/0/2] port link-type access
[Switch-Ethernet0/0/2] port default vlan 100
[Switch-Ethernet0/0/2] quit
```

10.3 配置VRRP域BFD联动实现快速切换示例

组网需求

如图10-3所示，局域网内的主机通过 Switch 双归属到部署了 VRRP 备份组的 SwitchA 和 SwitchB，其中 SwitchA 为 Master。

当 SwitchA 或 SwitchA 到 SwitchB 间链路出现故障时，VRRP 报文协商需要一定的协商周期。为了实现链路故障时快速切换，可以在链路中部署 BFD 链路检测机制，并配置 VRRP 监视 BFD 会话，实现当主用接口或者链路出现 Down 时，备用设备迅速切换为 Master，承担网络流量，以减少故障对业务传输的影响。

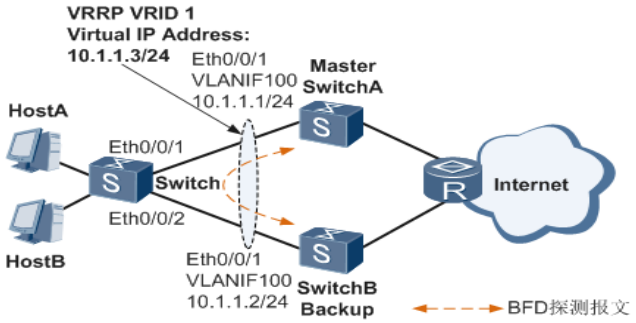


图10-3 配置VRRP与BFD联动实现快速切换组网图

配置思路

采用 VRRP 与 BFD 联动实现主备网关间的快速切换，配置思路如下：

1. 配置各设备接口 IP 地址及路由协议，使网络层路由可达。

2. 在 SwitchA 和 SwitchB 上配置 VRRP 备份组，其中 SwitchA 的优先级为120，抢占延时为20秒，作为 Master 设备；SwitchB 的优先级为缺省值，作为 Backup 设备，实现网关的主备备份。

3. 在 SwitchA 和 SwitchB 上配置静态 BFD 会话，监测备份组之间的链路。

4. 在 SwitchB 上配置 VRRP 与 BFD 联动，实现链路故障时 VRRP 备份组快速切换。

详细配置步骤

SwitchA 设备配置如下：

1. 配置设备间的网络互连

配置 SwitchA 设备各接口的 IP 地址。

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] vlan batch 100
[SwitchA] interface ethernet 0/0/1
[SwitchA-Ethernet0/0/1] port link-type access
[SwitchA-Ethernet0/0/1] port default vlan 100
[SwitchA-Ethernet0/0/1] quit
[SwitchA] interface vlanif 100
[SwitchA-Vlanif100] ip address 10.1.1.1 24
[SwitchA-Vlanif100] quit
```

2. 配置 VRRP 备份组

在 SwitchA 上创建 VRRP 备份组1，配置 SwitchA 在该备份组中的优先级为120，抢占延时为20秒，作为 Master 设备；

```
[SwitchA] interface vlanif 100
[SwitchA-Vlanif100] vrrp vrid 1 virtual-ip 10.1.1.3
[SwitchA-Vlanif100] vrrp vrid 1 priority 120
[SwitchA-Vlanif100] vrrp vrid 1 preempt-mode timer delay 20
[SwitchA-Vlanif100] quit
```

3. 配置静态 BFD 会话

在 SwitchA 上配置 BFD 会话。

```
[SwitchA] bfd
[SwitchA-bfd] quit
[SwitchA] bfd atob bind peer-ip 10.1.1.2 interface vlanif 100
[SwitchA-bfd-session-atob] discriminator local 1
[SwitchA-bfd-session-atob] discriminator remote 2
[SwitchA-bfd-session-atob] min-rx-interval 100
[SwitchA-bfd-session-atob] min-tx-interval 100
[SwitchB-bfd-session-atob] commit
[SwitchA-bfd-session-atob] quit
```

SwitchB 设备配置如下：

1. 配置设备间的网络互连

配置 SwitchB 设备各接口的 IP 地址。

```
<Quidway> system-view
```

```
[Quidway] sysname SwitchB
[SwitchB] vlan batch 100
[SwitchB] interface ethernet 0/0/1
[SwitchB-Ethernet0/0/1] port link-type access
[SwitchB-Ethernet0/0/1] port default vlan 100
[SwitchB-Ethernet0/0/1] quit
[SwitchB] interface vlanif 100
[SwitchB-Vlanif100] ip address 10.1.1.2 24
[SwitchB-Vlanif100] quit
```

2. 配置 VRRP 备份组

在 SwitchB 上创建 VRRP 备份组1，优先级为默认值100，作为 Slave 设备；

```
[SwitchB] interface vlanif 100
[SwitchB-Vlanif100] vrrp vrid 1 virtual-ip 10.1.1.3
```

3. 配置静态 BFD 会话

在 SwitchB 上配置 BFD 会话。

```
[SwitchB] bfd
[SwitchB-bfd] quit
[SwitchB] bfd atob bind peer-ip 10.1.1.1 interface vlanif 100
[SwitchB-bfd-session-atob] discriminator local 2
[SwitchB-bfd-session-atob] discriminator remote 1
[SwitchB-bfd-session-atob] min-rx-interval 100
[SwitchB-bfd-session-atob] min-tx-interval 100
[SwitchB-bfd-session-atob] commit
[SwitchB-bfd-session-atob] quit
```

4. 配置 VRRP 与 BFD 联动功能

在 SwitchB 上配置 VRRP 与 BFD 联动，当 BFD 会话状态 Down 时，SwitchB 的优先级增加40。

```
[SwitchB] interface vlanif 100
[SwitchB-Vlanif100] vrrp vrid 1 track bfd-session 2 increased 40 //bfd-session
的取值和 local 的取值一样
[SwitchB-Vlanif100] quit
```

Switch 设备配置如下：

配置 Switch 的二层透传能力

```
<Quidway> system-view
[Quidway] sysname Switch
```

```
[Switch] vlan 100
[Switch-vlan100] quit
[Switch] interface ethernet 0/0/1
[Switch-Ethernet0/0/1] port hybrid pvid vlan 100
[Switch-Ethernet0/0/1] port hybrid untagged vlan 100
[Switch-Ethernet0/0/1] quit
[Switch] interface ethernet 0/0/2
[Switch-Ethernet0/0/2] port hybrid pvid vlan 100
[Switch-Ethernet0/0/2] port hybrid untagged vlan 100
[Switch-Ethernet0/0/2] quit
```

11 链路聚合配置

一、功能简介

链路聚合（Link Aggregation）是将多条物理链路捆绑在一起成为一条逻辑链路，从而增加链路带宽的技术。

二、配置命令和步骤

1、执行命令 **interface eth-trunk** *trunk-id*，系统视图创建 Eth-Trunk 并进入 Eth-Trunk 接口视图。

2、执行命令 **mode**{ **manual load-balance** | **lacp-static** }，配置 Eth-Trunk 的工作模式，缺省情况下，Eth-Trunk 的工作模式为手工负载分担模式。

3、执行命令 **eth-trunk** trunk-id，接口视图下将当前接口加入 Eth-Trunk。

注：

1、 配置时需要保证本端和对端的聚合模式一致。即如果本端配置为手工负载分担模式，那么对端设备也必须要配置为手工负载分担模式；如果本端配置为 lacp 模式，那么对端设备也必须配置为 lacp 模式。

2、 Eth-Trunk 链路两端相连的物理接口的数量、速率、双工方式、jumbo、流控配置必须一致。

3、 如果本地设备使用了 Eth-Trunk，与成员接口直连的对端接口也必须捆绑为 Eth-Trunk 接口，两端才能正常通信。

4、 接口缺省都加入了 VLAN1，因此加入 Eth-Trunk 前建议先将接口从 VLAN1中退出或将接口 Shutdown，避免出现广播风暴。

表11-1 HUAWEI 与 H3C 厂商链路聚合对接情况

H3C 配置的链路聚合模式	HUAWEI 对接的链路聚合模式	命令行	
		H3C 命令行	HUAWEI 命令行
手工负载分担模式	手工负载分担模式	默认为手工负载分担模式	**mode manual load-balance**

动态 LACP 模式	静态 LACP 模式	**link-aggregation mode dynamic**	V100R006C00、V200R001版本：**mode lacp-static**
			V200R001之后版本：**mode lacp**

表11-2 HUAWEI 与思科厂商链路聚合对接情况			
思科配置的链路聚合模式	HUAWEI 对接的链路聚合模式	命令行	
		思科命令行	HUAWEI 命令行
手工负载分担模式	手工负载分担模式	**channel-group** *channel-number* **mod on**	**mode manual load-balance**
静态 LACP 模式	静态 LACP 模式	**channel-group** *channel-number* **mod active**	V100R006C00、V200R001版本：**mode lacp-static**
		channel-group *channel-number* **mod passive**	V200R001之后版本：**mode lacp**

交换机与 Linux 服务器多网卡对接采取的模式如下表：

表11-3 交换机与 Linux 服务器多网卡对接采取的模式		
服务器模式	交换机对接模式	说明
Round-robin	手工负载分担模式	所绑定的网卡的 IP 都被修改成相同的 MAC 地址，需要通过聚合口对接。
active-backup	划分同一个 VLAN	一个端口处于主状态 ，一个处于从状态，所有流量都在主链路上处理，建议交换机划在同一个 VLAN 中。
load balancing	手工负载分担模式	手工负载分担模式是通过源 MAC 和目的 MAC 做 HASH，交换机配置聚合口。
broadcast	2台交换机对接，配置不同 VLAN	同一个报文服务器会复制两份分别往两条线路发送，建议用2台交换机对接，配置不同 VLAN。
Lacp	LACP	链路聚合，交换机配置 LACP 静态聚合方式。
transmit load balancing	2台交换机对接	不需要对交换机配置
adaptive load balancing	手工负载分担（聚合）	针对 IPV4流量的接收负载均衡，交换机配置手动负载均衡

交换机与 Windows 服务器多网卡对接采取的模式如下表：

表11-4 交换机与 Windows 服务器多网卡对接采取的模式		
服务器模式	交换机对接模式	说明
适配器容错（AFT）	划分同一个 VLAN	适配器容错,不需要配置交换机，建议交换机划在同一个 VLAN 中。
适应性负载平衡（ALB）	划分同一个 VLAN	适应性负载平衡，不需要配置交换机，建议交换机划在同一个 VLAN 中。
静态链接聚合（SLA）	手工负载分担模式	服务器接聚合（SLA）聚合无协议交互，交换机配置手工负载分担模式聚合方式。
IEEE 802.3ad 动态聚合	静态 LACP 模式	要求交换机完全支持802.3ad 标准。
交换器容错 (SFT)	2台交换机对接	交换器容错模式，用2台交换机对接。

三、应用场景

11.1 配置手工负载分担模式链路聚合示例

组网需求

如图1所示，SwitchA 和 SwitchB 通过以太链路分别都连接 VLAN10和 VLAN20的网络，且 SwitchA 和 SwitchB 之间有较大的数据流量。

用户希望 SwitchA 和 SwitchB 之间能够提供较大的链路带宽来使相同 VLAN 间互相通信。同时用户也希望能够提供一定的冗余度，保证数据传输和链路的可靠性。

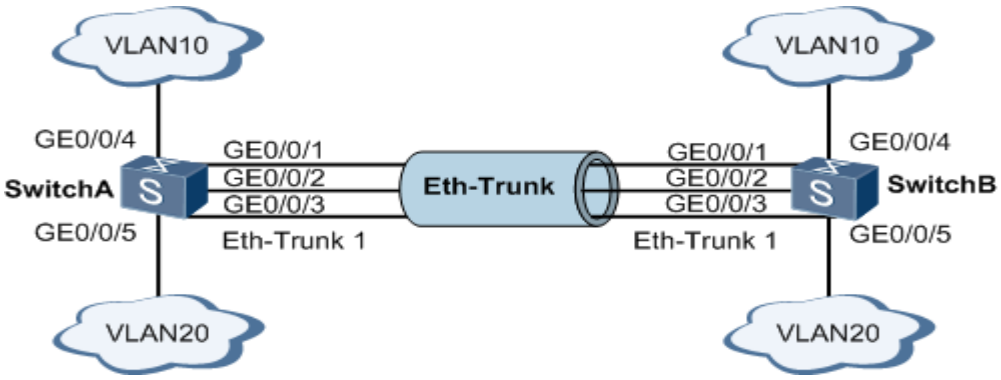


图11-1 配置手工负载分担模式链路聚合组网图

配置思路

采用如下的思路配置负载分担链路聚合：

1． 创建 Eth-Trunk 接口并加入成员接口，实现增加链路带宽。

说明： 接口缺省都加入了 VLAN1，因此加入 Eth-Trunk 前建议先将接口从 VLAN1中退出或将接口 Shutdown，避免出现广播风暴。

2． 创建 VLAN 并将接口加入 VLAN。

3． 配置负载分担方式，实现流量在 Eth-Trunk 各成员接口间的负载分担，增加可靠性。

详细配置步骤

1． 在 SwitchA 创建 Eth-Trunk 接口并加入成员接口；SwitchB 配置与 SwitchA 类似，不再赘述。

```
< SwitchA > system-view                                    //进入系统视图
[SwitchA] interface eth-trunk 1                            //创建并进入 eth-trunk 接口
[SwitchA-Eth-Trunk1] trunkport gigabitethernet 0/0/1 to 0/0/3 //增加成员接口到 eth-trunk 接口
[SwitchA-Eth-Trunk1] quit
```

2． 创建 VLAN 并将接口加入 VLAN。SwitchB 配置与 SwitchA 类似，不再赘述。

创建 VLAN10和 VLAN20并分别加入接口。

```
[SwitchA] vlan batch 10 20                                 //创建 vlan
[SwitchA] interface gigabitethernet 0/0/4
[SwitchA-GigabitEthernet0/0/4] port link-type trunk        //对接 SW 为 trunk 模式
```

```
[SwitchA-GigabitEthernet0/0/4] port trunk allow-pass vlan 10
[SwitchA-GigabitEthernet0/0/4] quit
[SwitchA] interface gigabitethernet 0/0/5
[SwitchA-GigabitEthernet0/0/5] port link-type trunk
[SwitchA-GigabitEthernet0/0/5] port trunk allow-pass vlan 20
[SwitchA-GigabitEthernet0/0/5] quit
```

配置Eth-Trunk1接口允许VLAN10和VLAN20通过。

```
[SwitchA] interface eth-trunk 1
[SwitchA-Eth-Trunk1] port link-type trunk          //允许多个vlan用trunk模式
[SwitchA-Eth-Trunk1] port trunk allow-pass vlan 10 20
```

3． 配置Eth-Trunk1的负载分担方式。SwitchB配置与SwitchA类似，不再赘述。

```
[SwitchA-Eth-Trunk1] load-balance src-dst-mac//负载分担方式基于源-目的mac地址
[SwitchA-Eth-Trunk1] quit
```

11.2 配置LACP模式的链路聚合示例

组网需求

如图11-2所示，在两台Switch设备上配置LACP模式链路聚合组，提高两设备之间的带宽与可靠性，具体要求如下：

- 两条活动链路具有负载分担的能力。
- 两设备间的链路具有1条冗余备份链路，当活动链路出现故障链路时，备份链路替代故障链路，保持数据传输的可靠性。

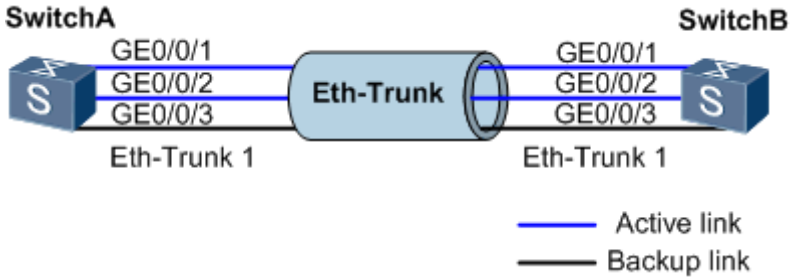


图11-2 配置LACP模式链路聚合组网图

配置思路

采用如下的思路配置LACP模式链路聚合：

1． 创建Eth-Trunk，配置Eth-Trunk为LACP模式，实现链路聚合功能。

2． 将成员接口加入Eth-Trunk。

3． 配置系统优先级，确定主动端，按照主动端设备的接口选择活动接口。

4． 配置活动接口上限阈值，实现保证带宽的情况下提高网络的可靠性。

5． 配置接口优先级，确定活动链路接口，优先级高的接口将被选作活动接口。

详细配置步骤

1． 在 SwitchA 上创建 Eth-Trunk1并配置为 LACP 模式。SwitchB 配置过程与 SwitchA 类似，不再赘述

```
< SwitchA > system-view
[SwitchA] interface eth-trunk 1
[SwitchA-Eth-Trunk1] mode lacp                    //配置模式为 lacp 模式
[SwitchA-Eth-Trunk1] quit
```

2． 配置 SwitchA 上的成员接口加入 Eth-Trunk。SwitchB 配置过程与 SwitchA 类似，不再赘述

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] eth-trunk 1
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] eth-trunk 1
[SwitchA-GigabitEthernet0/0/2] quit
[SwitchA] interface gigabitethernet 0/0/3
[SwitchA-GigabitEthernet0/0/3] eth-trunk 1
[SwitchA-GigabitEthernet0/0/3] quit
```

3． 在 SwitchA 上配置系统优先级为100，使其成为 LACP 主动端

```
[SwitchA] lacp priority 100                  //配置 switchA 的 lacp 优先级为100
```

4． 在 SwitchA 上配置活动接口上限阈值为2

```
[SwitchA] interface eth-trunk 1
[SwitchA-Eth-Trunk1] max active-linknumber 2    //配置最大活动接口数为2
[SwitchA-Eth-Trunk1] quit
```

5． 在 SwitchA 上配置接口优先级确定活动链路

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] lacp priority 100    //配置接口 lacp 优先级为100
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] lacp priority 100
[SwitchA-GigabitEthernet0/0/2] quit
```

11.3 HUAWEI设备与C厂商设备对接案例

组网需求

如图11-3所示，HUAWEI 设备和 C 厂商设备采用静态 LACP 模式对接。

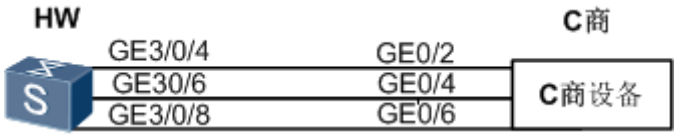


图11-3 HUAWEI 与 C 厂商对接组网图

配置思路

创建聚合链路、配置链路聚合模式

详细配置步骤

1、创建聚合链路，并将接口加入链路聚合

HUAWEI 配置：

```
<HW> system-view
[HW] interface Eth-Trunk 1
[HW-Eth-Trunk1] quit
[HW] interface GigabitEthernet3/0/4
[HW-GigabitEthernet3/0/4] eth-trunk 1
[HW-GigabitEthernet3/0/4] quit
[HW] interface GigabitEthernet3/0/6
[HW-GigabitEthernet3/0/6] eth-trunk 1
[HW-GigabitEthernet3/0/6] quit
[HW] interface GigabitEthernet3/0/8
[HW-GigabitEthernet3/0/8] eth-trunk 1
[HW-GigabitEthernet3/0/8] quit
```

C 设备配置：

```
Switch#configure terminal
Switch(config)#interface port-channel 1
```

2、配置链路聚合模式

```
[HW] interface Eth-Trunk 1
[HW-Eth-Trunk1] mode lacp                    //配置链路聚合模式为 LACP
```

C 设备配置

```
Switch(config)#interface range Gi0/2,Gi0/4,Gi0/6
Switch(config-if-range)#channel-protocol lacp
Switch(config-if-range)#channel-group 1 mode active        //配置主动 LACP 模式
```

3、配置链路聚合负载模式

```
[HW-Eth-Trunk1] load-balance src-mac                    //源 MAC 地址负载分担
```

C 设备配置

```
Switch(config)#port-channel load-balance src-mac
```

4、配置系统 LACP 优先级

```
[HW] lacp priority 0
```

C 设备配置：

```
Switch(config)#lacp system-priority 1
```

5、配置接口 LACP 优先级

```
[HW] interface GigabitEthernet 3/0/4
[HW-GigabitEthernet3/0/4] lacp priority 1
```

C 设备配置：

```
Switch(config)#interface gi0/2
Switch(config-if)#lacp port-priority 1
```

12 盒式交换机堆叠配置及注意事项

一、 功能介绍

堆叠 iStack，是指将多台支持堆叠特性的交换机设备组合在一起，从逻辑上组合成一台交换设备。如图所示，SwitchA 与 SwitchB 通过堆叠线缆连接后组成堆叠 iStack，对于上游和下游设备来说，它们就相当于一台交换机 Switch。

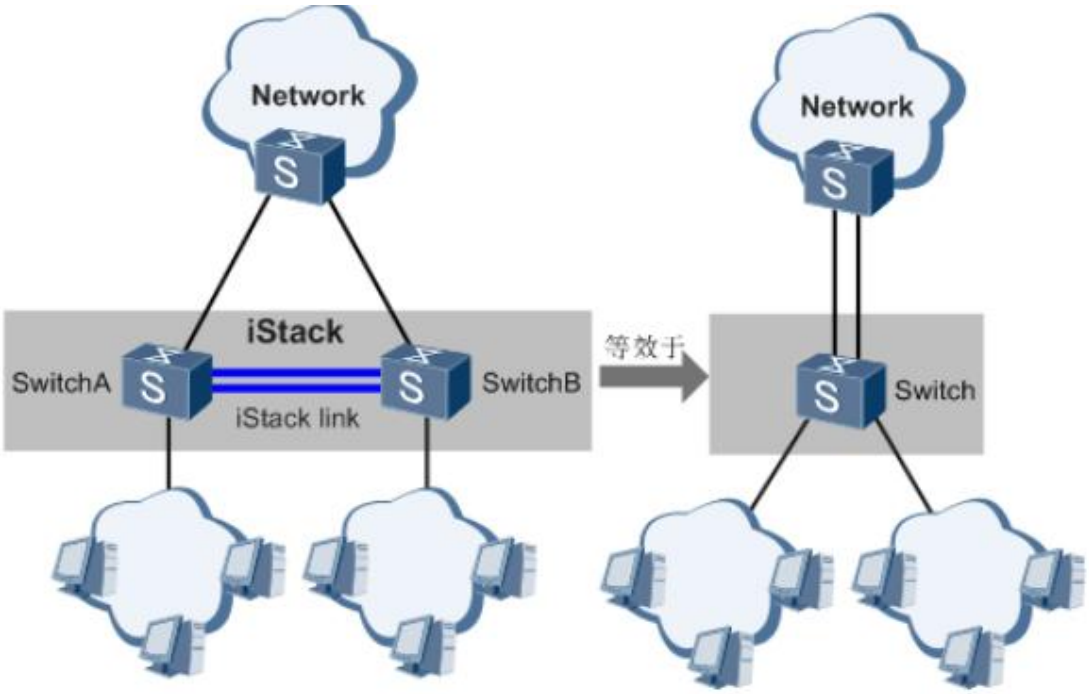


图 12-1 堆叠示例图

S2700和 S3700系列交换机堆叠支持情况：

支持堆叠的设备型号有:S3700EI、S3700SI、S2700－52P-EI、S2700－52P-PWR-EI 和 S2710SI，不同形态不能混堆叠。

除 S2700 - 52P-EI 和 S2700 - 52P-PWR-EI 以外的 S2700EI 不支持通过专用堆叠线缆堆叠。

S3752EI、S3752SI 最多支持8台设备堆叠，其他型号产品最多支持9台设备堆叠。需要特别说明的是：S3752EI 不能与 S3728EI 组成堆叠；S3752SI 不能与 S3728SI 组成堆叠。

堆叠设备之间通过上行的复用堆叠口和专用的堆叠线缆连接而成。

S2750、S5700和 S6700系列交换机通过堆叠卡堆叠支持情况：

为防止成员交换机之间软件版本不兼容，导致组建堆叠不成功。建议用户在组建堆叠之前，将所有成员交换机升级到相同的软件版本；

堆叠卡堆叠必须配套使用 ES5D00ETPC00堆叠后插卡和 PCIe 线缆，支持堆叠卡堆叠的设备系列和对应的软硬件要求如表1所示。

S2750、S5700-HI 和 S6700都不支持堆叠卡堆叠，仅有下面列出的几款是支持堆叠卡堆叠的，堆叠的接口均为堆叠卡的两个堆叠端口，最多只支持9台设备进行堆叠；堆叠时单端口的工作速率均为 12Gbit/s；

表 12-1　堆叠卡堆叠软硬件要求说明表

设备系列	支持的版本	堆叠线缆	备注
S5700-SI	V1R5 及以后版本	1m 的 PCIe 电缆； 3m 的 PCIe 电缆（V2R3 及以后版本支持）	支持 S5700-SI 的所有款型之间混堆； 说明： S5700-26X-SI-12S-AC 不支持堆叠
S5710-LI	仅 V2R1 的版本	1m 的 PCIe 电缆	支持 5710-LI 的所有款型之间混堆
S5700-EI	V1R5 及以后版本	1m 的 PCIe 电缆； 3m 的 PCIe 电缆（V200R002 版本开始支持，V200R002 版本仅 S5700-52C-EI 和 S5700-28C-EI-24S 支持，V200R003 版本及以后版本所有 S5700-EI 都支持）	支持 S5700-EI 的所有款型之间混堆。

S2750、S5700 和 S6700 交换机业务口堆叠支持情况及注意事项：

下面可以通过业务口堆叠的最多支持 9 台设备进行堆叠；

表 12-2　业务口堆叠软硬件要求说明表

设备系列	支持的软件版本	支持的堆叠接口	堆叠线缆	备注
S2750	V200R003 及以后版本	设备的 2 个 SFP 光接口（非 combo 口） 说明： S2750 只有最后倒数第三、第四个业务口可以配置为堆叠物理成员端口。	1m 无源 SFP+电缆； 3m 无源 SFP+电缆； 10m 有源 SFP+电缆；	支持所有 S2750 款型混堆。

			3m、10m AOC 线缆； 6GE 堆叠光模块（SFP-6GE-LR）和光纤；	
S5700-P-LI（GE 上行款型）	V200R001 及以后版本	V200R001 版本：设备最后的 2 个 SFP 光接口； V200R002 及以后版本：设备最后的 4 个 SFP 光接口；	1m 无源 SFP+电缆； 10m 有源 SFP+电缆； 3m、10m AOC 线缆（V200R003C00 版本及以后版本支持）；	V200R001 版本：单设备最多支持 2 个逻辑堆叠口，每个逻辑堆叠口最多包含 1 个物理成员口，单设备最大支持 2 个物理成员口。 V200R002 及以后版本：单设备最多支持 2 个逻辑堆叠口，每个逻辑堆叠口最多包含 2 个物理成员口，单设备最大支持 4 个物理成员口。 支持 S5700-P-LI 款型之间混堆，不支持 S5700-P-LI 款型与 S5700-X-LI 款型之间混堆。 说明： S5700-10P-LI-AC、S5700-28P-LI-BAT、S5700-28P-LI-24S-BAT 和 S5700-10P-PWR-LI-AC 不支持堆叠。 V200R002 及以后版本，设备最后的 4 个 SFP 光接口支持作堆叠接口。当 1 个逻辑堆叠口包含 2 个物理成员口时，只能包含堆叠接口 1 和 2 或者堆叠接口 3 和 4。
S5700-X-LI（10GE 上行款型）	V200R002 及以后版本	设备的 4 个 SFP+光接口	1m 无源 SFP+电缆； 3m 无源 SFP+电缆； 10m 有源 SFP+	单设备最多支持 2 个逻辑堆叠口，每个逻辑堆叠口最多包含 2 个物理成员口，单设备最大支持 4 个物理成员口。

			电缆； 3m、10m AOC 线缆（V200R003C00 版本及以后版本支持）； 10GE SFP+光模块和光纤	支持 S5700-X-LI 款型之间混堆，不支持 S5700-P-LI 款型与 S5700-X-LI 款型之间混堆。 说明： 设备的 4 个 SFP+光接口支持作堆叠接口，当 1 个逻辑堆叠口包含 2 个物理成员口时，只能包含堆叠接口 1 和 2 或者堆叠接口 3 和 4。
S5710-EI	V200R001 及以后版本	设备上任意 10GE 接口：包括设备正面固定的 4 个 10GE SFP+ 接口和背面 ES5D21X02S00 插卡上的接口（最多支持 2 个插卡，每个插卡支持 2 个 10GE SFP+接口） 说明： 每个逻辑堆叠端口最多可添加 4 个堆叠物理成员端口。支持不同子卡上的接口加入同一个逻辑堆叠端口，不支持子卡上的接口和设备面板上的接口混合加入同一个逻辑堆叠端口。	1m 无源 SFP+电缆； 3m 无源 SFP+电缆； 10m 有源 SFP+电缆； 3m、10m AOC 线缆（V200R003C00 版本及以后版本支持）； 10GE SFP+光模块和光纤	V200R001 版本：单设备最多支持 2 个逻辑堆叠口，每个逻辑堆叠口最多包含 3 个物理成员口，单设备最大支持 4 个物理成员口。所有堆叠口的物理成员口分布必须全部位于前面板或全部位于后面的插卡上。 V200R002 及以后版本：单设备最多支持 2 个逻辑堆叠口，每个逻辑堆叠口最多包含 4 个物理成员口，单设备最大支持 8 个物理成员口。 支持 S5710-EI 的所有款型混堆。
S5700-HI	V200R003 及以后版本	前插卡上的 10GE 接口：支持 ES5D00X2SA00/ES5D00X4SA00 两种前插卡，分别提供 2/4 个 10GE SFP+接口 说明： 设备更换插卡后，堆叠相关的配置将失效，需重新配置。	1m 无源 SFP+电缆； 3m 无源 SFP+电缆； 10m 有源 SFP+电缆； 3m、10m AOC 线缆； 10GE SFP+光模块和光纤	支持 S5700-HI 的所有款型混堆。
S6700	V100R006 及以后版本	设备上任意 10GE 接口 说明： 最多支持 8 个业务口配置为	1m 无源 SFP+电缆； 3m 无源 SFP+	支持 S6700 的所有款型之间混堆，接口工作在 GE 模式时不支持堆

		物理成员端口。每 4 个为 1 组（例如，1～4 为 1 组、5～8 为 1 组，2～5 不能作为 1 组），每组的业务口同时被配置成物理成员端口。	电缆： 10m 有源 SFP+电缆（V200R001 版本及以后版本支持）； 3m、10m AOC 线缆（V200R003C00 版本及以后版本支持）； 10GE SFP+光模块和光纤	叠。
S5700S-LI S5710-HI	不支持堆叠			

通过堆叠线缆堆叠连线情况如下：

堆叠卡堆叠的连接拓扑包括链形连接和环形连接，如图2和图3所示。两种连接拓扑的对比可参见堆叠建立。

说明：

1.堆叠线缆连接前请将交换机下电。

2.堆叠线缆连接时一台交换机的 STACK 1端口只能与另一台交换机的 STACK 2端口相连接。

图12-2 链形连接示意图

图12-3 环形连接示意图

通过业务口堆叠堆叠线路连接情况如下：

业务口堆叠的连接拓扑包括链形连接和环形连接。以3台 S5700-28X-LI-AC 设备进行环形连接和链形连接举例，将每台设备的前两个10GE 光口配置成逻辑端口1，后两个10GE 光口配置成逻辑端口2，线缆连接方式如图1和图2所示。

注意事项：

1.堆叠线缆连接前请将交换机下电。

2.堆叠成员设备之间，本端设备的逻辑堆叠端口 stack-port n/1必须与对端设备的逻辑堆叠端口 stack-port n/2相连。

3.一个逻辑堆叠端口可以绑定多个物理成员端口，用来提高堆叠的可靠性和堆叠带宽；只要其中一条物理链路保持连接堆叠就不会分裂，但堆叠带宽会相应降低。

4.如果两端设备对应的逻辑堆叠端口（本端的 stack-port n/1与对端的 stack-port n/2）内包含多个物理成员端口，对物理成员端口的连接无对应端口号的要求。

5.3台或者3台以上成员交换机组建堆叠时，为增加可靠性，建议采用环形组网，此时堆叠系统的带宽取所有堆叠端口带宽的最小值。

6.2台成员交换机组建堆叠时，只能是链形组网，也称为背靠背组网堆叠。这种场景下，建议每台成员交换机只创建一个逻辑堆叠端口，逻辑堆叠端口包含多个物理成员端口。

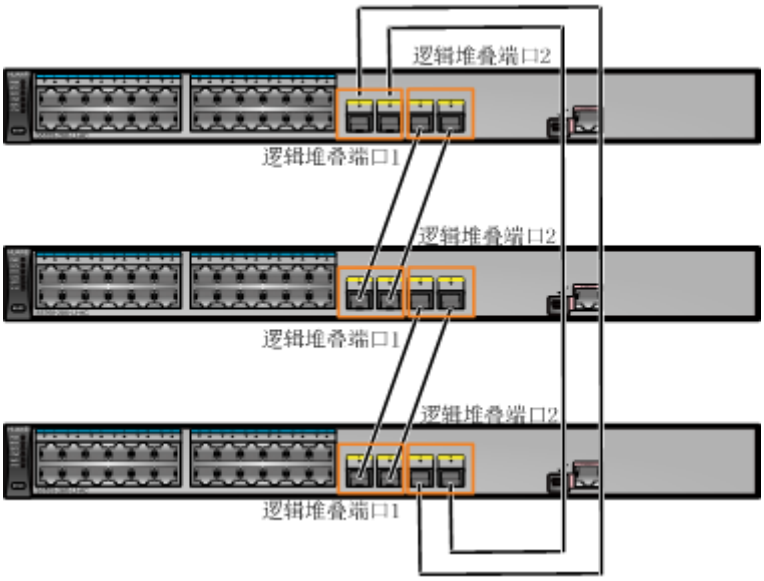


图12-4 业务口堆叠环形连接示意图

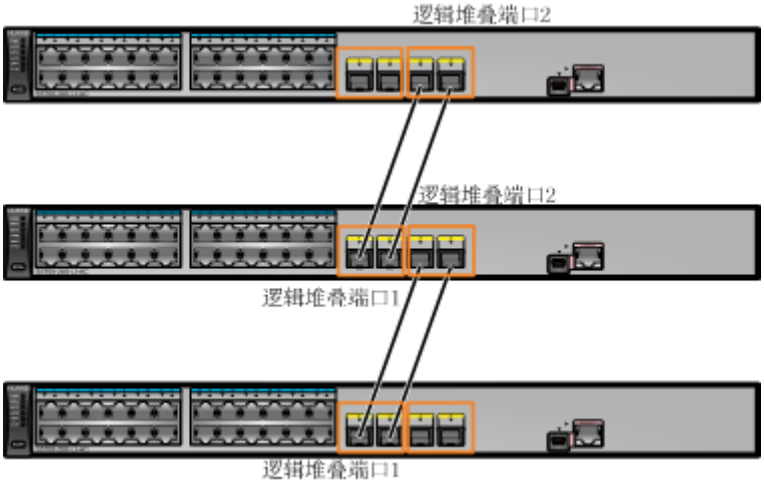


图12-5 业务口堆叠链形连接示意图

二、 配置命令和步骤

堆叠卡堆叠配置命令：

1.执行命令 **stack enable**，使能设备堆叠功能；缺省情况下，设备堆叠功能处于使能状态；

2.（可选）执行命令 **stack slot** slot-id **renumber** new-slot-id ，配置设备的堆叠 ID。缺省情况下，设备堆叠 ID 为0；

3.（可选）执行命令 **stack slot** slot-id **priority** priority，配置设备的堆叠优先级。缺省情况下，设备的堆叠优先级为100，优先级取值范围为1-255；

业务口堆叠配置命令：

1.命令 **interface stack-port** member-id/port-id 命令，创建并进入逻辑堆叠端口视图。

2.命令 **port interface** { interface-type interface-number1 [to interface-type interface-number2] } &<1-10> **enable**，配置业务口为物理成员端口并将其加入到逻辑堆叠端口中。

3.（可选）执行命令 **stack slot** slot-id **renumber** new-slot-id ，配置设备的堆叠 ID。缺省情况下，设备堆叠 ID 为0；

4.（可选）执行命令 **stack slot** slot-id **priority** priority，配置设备的堆叠优先级。缺省情况下，设备的堆叠优先级为100，优先级取值范围为1-255；

设备配置堆叠相关属性后，如堆叠 ID 和使能堆叠功能，需要重新启动设备后配置才能生效。为了成功组建堆叠，完成上述配置后，建议用户先为所有成员交换机下电，使用专用的堆叠线缆进行连接后再依次上电。

应用场景

12.1 配置环型拓扑堆叠示例（S2700和S3700系列）

组网需求

如图12-6所示，SwitchA、SwitchB、SwitchC 和 SwitchD 四台交换机组成环型堆叠系统，四台设备的堆叠优先级依次为：200、150、100、100，槽位号分别为0、1、2、3；当前主备倒换后系统 MAC 地址会立即切换，为避免系统 MAC 地址的频繁刷新浪费系统资源，现在需要将主备倒换后系统 MAC 地址切换时间配置为1分钟。

缺省情况下，堆叠功能处于使能状态，正确连接堆叠线缆后，堆叠系统即建立，无需配置；但是为了便于管理和精确指定主备交换机，建议还是配置交换机的堆叠优先级和槽位号；

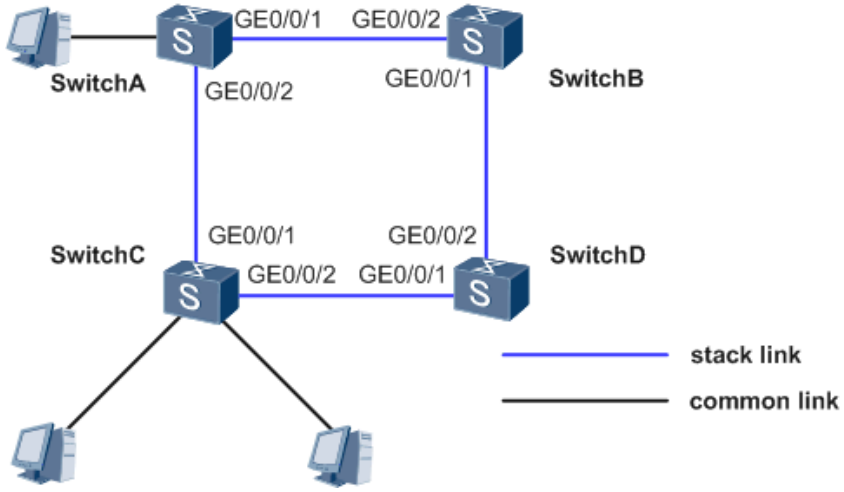


图12-6 基于环型拓扑堆叠组网图

配置思路

- 采用如下的思路配置：

1. 确认四台交换机的堆叠功能是否已使能；

2. 缺省情况下，交换机的堆叠功能处于使能状态，使用专用的堆叠线缆按上图所示连接堆叠口，如果没有使能的话手动使能堆叠功能；

3. 配置堆叠设备的优先级 SwitchA、SwitchB、SwitchC 和 SwitchD 依次为200、150、100、100；

配置四台设备 witchA、SwitchB、SwitchC 和 SwitchD 的堆叠 ID 依次为0、1、2、3；

4． 正确连接堆叠线缆后，堆叠建立，配置堆叠系统 MAC 地址切换时间。

详细配置步骤

1． 分别使能四台设备的堆叠功能；

使能 SwitchA 的堆叠功能。

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchA
[SwitchA] stack enable
Warning: All the configurations related to the slot ID will be lost after the stack function is enabled. Continue?[Y/N]: y
Info: Stack configuration has been changed, need reboot to take effect.
```

使能 SwitchB 的堆叠功能。

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchB
[SwitchB] stack enable
Warning: All the configurations related to the slot ID will be lost after the stack function is enabled. Continue?[Y/N]: y
Info: Stack configuration has been changed, need reboot to take effect.
```

使能 SwitchC 的堆叠功能。

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchC
[SwitchC] stack enable
Warning: All the configurations related to the slot ID will be lost after the stack function is enabled. Continue?[Y/N]: y
Info: Stack configuration has been changed, need reboot to take effect.
```

使能 SwitchD 的堆叠功能。

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchD
[SwitchD] stack enable
Warning: All the configurations related to the slot ID will be lost after the stack function is enabled. Continue?[Y/N]: y
Info: Stack configuration has been changed, need reboot to take effect.
```

2． 配置堆叠 ID 和堆叠优先级

配置 SwitchA 的堆叠优先级为200。

```
[SwitchA] stack slot 0 priority 200
```

```
    Warning:Please do not frequently modify Priority, it will make the stack split!
continue?[Y/N]:y
```

#配置 SwitchB 的优先级为150

```
     [SwitchA] stack slot 0 priority 150
    Warning:Please do not frequently modify Priority, it will make the stack split!
continue?[Y/N]:y
```

配置 SwitchB 的堆叠 ID 为1。

```
     [SwitchB] stack slot 0 renumber 1
     Warning: All the configurations related to the slot ID will be lost after
the slot ID is modified.
     Please do not frequently modify slot ID, it will make the stack split.
Continue?[Y/N]:y
     Info: Stack configuration has been changed, need reboot to take effect.
```

配置 SwitchC 的堆叠 ID 为2。

```
     [SwitchC] stack slot 0 renumber 2
     Warning: All the configurations related to the slot ID will be lost after
the slot ID is modified.
     Please do not frequently modify slot ID, it will make the stack split.
Continue?[Y/N]:y
     Info: Stack configuration has been changed, need reboot to take effect.
```

配置 SwitchD 的堆叠 ID 为3。

```
     [SwitchC] stack slot 0 renumber 3
     Warning: All the configurations related to the slot ID will be lost after
the slot ID is modified.
     Please do not frequently modify slot ID, it will make the stack split.
Continue?[Y/N]:y
     Info: Stack configuration has been changed, need reboot to take effect.
```

3． # 登录堆叠系统，配置系统 MAC 地址切换时间。

```
    <Quidway> system-view
    [Quidway] stack timer mac-address switch-delay 1
```

4． 配置完之后 save 保存配置，所有成员交换机都下电，使用专用的堆叠线缆进行连接后再依次上电,建议先给主设备上电，再给备设备和从设备上电；

在 SwitchA 上使用 **display stack** 命令查看堆叠的基本信息。

```
     <Quidway> display stack
```

```
Stack topology type: Ring
Stack system MAC: 0018-82d2-2e85
MAC switch delay time: 1 min
Stack reserved vlanid : 4093
Slot#    Role       Mac address     Priority   Device type
--------------------------------------------------------------
   0     Master     0018-82d2-2e85   200       S3728TP-EI
   1     Standby    0018-82c6-1f44   150       S3728TP-EI
   2     Slave      0018-82c6-1f4c   100       S3728TP-EI
   3     Slave      0018-82b1-6eb8   100       S3728TP-EI
```

12.2 设备组建堆叠示例（通过堆叠卡S2750及以上型号）

组网需求

如图1所示，根据用户需求，SwitchA、SwitchB 和 SwitchC 三台接入交换机采用环形堆叠组网，其中，SwitchA、SwitchB 和 SwitchC 的角色分别为主、备、从，堆叠 ID 分别为0、1、2，优先级分别为200、100、100。由于组成堆叠的成员交换机在逻辑上是一个整体，所以整个网络在扩展了端口数量的同时也方便了用户对网络的管理和维护。

现网设备以 S5700-EI 交换机为例，S5700-EI 交换机支持通过堆叠卡连接方式组建堆叠。

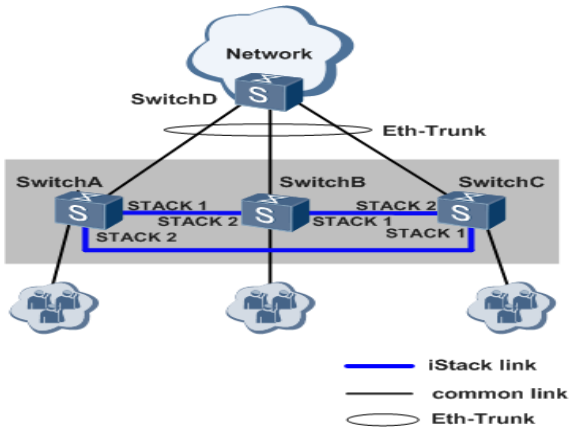


图12-7 堆叠组建后的组网

配置思路

采用如下的思路配置：

1． 设备先下电，安装 ES5D00ETPC00堆叠后插卡后，再将设备上电。

注意：

1.ES5D00ETPC00堆叠后插卡不支持热插拔，如果设备处于上电状态，安装前需要先将设备下电。

2.堆叠卡安装完成之后，才能进行相关软件配置。

2． 使能堆叠功能。

3． 为方便用户管理，配置成员交换机的堆叠 ID 和优先级。

4． SwitchA、SwitchB、SwitchC 下电。按照图1所示，使用 PCIe 线缆连接各堆叠端口并上电。

5． 为提高可靠性、增加上行链路带宽，配置跨设备 Eth-Trunk。

详细配置步骤

1． 安装 ES5D00ETPC00堆叠后插卡,分别为 SwitchA、SwitchB、SwitchC 安装 ES5D00ETPC00 堆叠后插卡；

2． 使能堆叠功能

使能 SwitchA 的堆叠功能。

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchA
[SwitchA] stack enable
Warning: All the configurations related to the slot ID will be lost after the stack function is enabled. Continue?[Y/N]: y
Info: Stack configuration has been changed, need reboot to take effect.
```

使能 SwitchB 的堆叠功能。

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchB
[SwitchB] stack enable
Warning: All the configurations related to the slot ID will be lost after the stack function is enabled. Continue?[Y/N]: y
Info: Stack configuration has been changed, need reboot to take effect.
```

使能 SwitchC 的堆叠功能。

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchC
[SwitchC] stack enable
Warning: All the configurations related to the slot ID will be lost after the stack function is enabled. Continue?[Y/N]: y
Info: Stack configuration has been changed, need reboot to take effect.
```

3． 配置堆叠 ID 和堆叠优先级

配置 SwitchA 的堆叠优先级为200。

```
[SwitchA] stack slot 0 priority 200
Warning:Please do not frequently modify Priority, it will make the stack split! continue?[Y/N]:y
```

配置 SwitchB 的堆叠 ID 为1。

```
[SwitchB] stack slot 0 renumber 1
```

```
    Warning: All the configurations related to the slot ID will be lost after the
slot ID is modified.
   Please do not frequently modify slot ID, it will make the stack split.
Continue?[Y/N]:y
    Info: Stack configuration has been changed, need reboot to take effect.
```

配置 SwitchC 的堆叠 ID 为2。

```
    [SwitchC] stack slot 0 renumber 2
    Warning: All the configurations related to the slot ID will be lost after the
slot ID is modified.
   Please do not frequently modify slot ID, it will make the stack split.
Continue?[Y/N]:y
    Info: Stack configuration has been changed, need reboot to take effect.
```

4． SwitchA、SwitchB、SwitchC 下电，使用 PCIe 线缆连接各堆叠端口并上电。

注意事项：

1.下电前，建议通过命令 save 保存配置。

2.一台交换机的 STACK 1端口只能与另一台交换机的 STACK 2端口相连接，否则堆叠组建不成功。

3.为保证堆叠组建成功，建议按照以下顺序进行连线上电（如果用户希望某台交换机为主交换机可以先为其上电。例如，按以下顺序连线上电后，SwitchA 为主交换机）：

a． 为 SwitchA～SwitchC 下电；

b． 连接 SwitchA 与 SwitchB 之间的堆叠线缆；

c． 先为 SwitchA 上电，SwitchA 启动后，再为 SwitchB 上电；

d． 与上一步类似:连接 SwitchC 与 SwitchB 和 SwitchA 之间的堆叠线缆,再为 SwitchC 上电；

e． 检查 SwitchA、SwitchB、SwitchC 的堆叠组建是否成功

12.3 设备组建堆叠示例（通过业务口S2750及以上型号）

组网需求

在一个新建的企业网络中，要求接入设备具有充足的端口数目，并且希望网络结构简单，易于配置和管理。

如图12-8所示，根据用户需求，SwitchA、SwitchB 和 SwitchC 三台接入交换机采用环形堆叠组网，并通过跨设备 Eth-Trunk 连接上层设备 SwitchD。其中，SwitchA、SwitchB 和 SwitchC 的角色分别为主、备、从，堆叠 ID 分别为0、1、2，优先级分别为200、100、100。由于组成堆叠的成员交换机在逻辑上是一个整体，所以整个网络在扩展了端口数量的同时也方便了用户对网络的管理和维护。

现网设备以 S5700-LI 交换机为例，S5700-LI 交换机支持通过业务口连接方式组建堆叠。

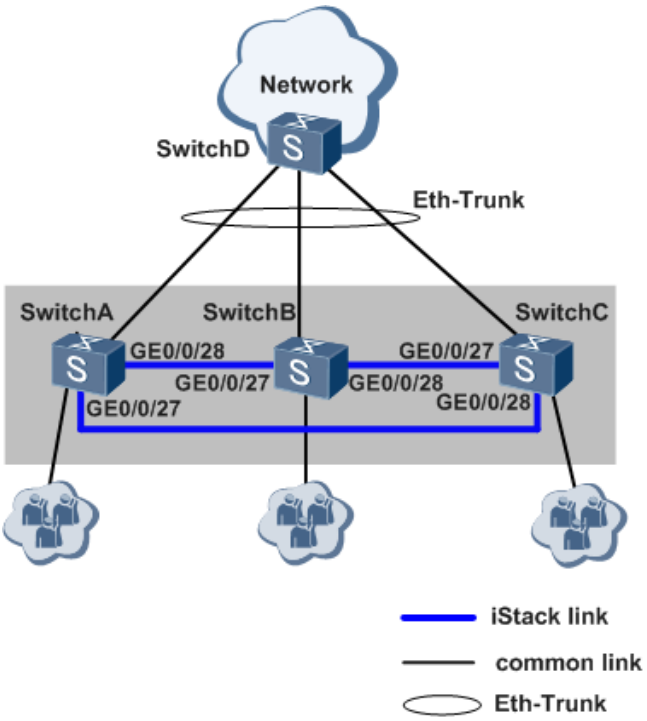


图12-8 堆叠组建后的组网

配置思路

采用如下的思路配置：

1． 通过业务口连接方式组建堆叠时，为了能够在堆叠的成员交换机之间转发数据报文，需要配置逻辑堆叠端口，并加入物理成员端口。

2． 为方便用户管理，配置成员交换机的堆叠 ID 和优先级。

3． SwitchA、SwitchB、SwitchC 下电。按照图1所示，使用 SFP+堆叠电缆连接各物理成员端口后再上电。

4． 为提高可靠性、增加上行链路带宽，配置跨设备 Eth-Trunk。

详细配置步骤

1． 配置逻辑堆叠端口并加入物理成员端口

配置 SwitchA 的业务口 GigabitEthernet0/0/27、GigabitEthernet0/0/28为物理成员端口，并加入到相应的逻辑堆叠端口。

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchA
[SwitchA] interface stack-port 0/1
[SwitchA-stack-port0/1] port interface gigabitethernet 0/0/27 enable
Warning: Enabling stack port cause configuration loss on the interface,
continue?[Y/N]:y
Info: This operation may take a few seconds. Please wait for a moment.....
```

```
[SwitchA-stack-port0/1] quit
[SwitchA] interface stack-port 0/2
[SwitchA-stack-port0/2] port interface gigabitethernet 0/0/28 enable
Warning: Enabling stack port cause configuration loss on the interface,
continue?[Y/N]:y
Info: This operation may take a few seconds. Please wait for a moment.......
[SwitchA-stack-port0/2] quit
```

- # 配置 SwitchB 的业务口 GigabitEthernet0/0/27、GigabitEthernet0/0/28为物理成员端口，并加入到相应的逻辑堆叠端口。

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchB
[SwitchB] interface stack-port 0/1
[SwitchB-stack-port0/1] port interface gigabitethernet 0/0/27 enable
Warning: Enabling stack port cause configuration loss on the interface,
continue?[Y/N]:y
Info: This operation may take a few seconds. Please wait for a moment.......
[SwitchB-stack-port0/1] quit
[SwitchB] interface stack-port 0/2
[SwitchB-stack-port0/2] port interface gigabitethernet 0/0/28 enable
Warning: Enabling stack port cause configuration loss on the interface,
continue?[Y/N]:y
Info: This operation may take a few seconds. Please wait for a moment.......
[SwitchB-stack-port0/2] quit
```

- # 配置 SwitchC 的业务口 GigabitEthernet0/0/27、GigabitEthernet0/0/28为物理成员端口，并加入到相应的逻辑堆叠端口。

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchC
[SwitchC] interface stack-port 0/1
[SwitchC-stack-port0/1] port interface gigabitethernet 0/0/27 enable
Warning: Enabling stack port cause configuration loss on the interface,
continue?[Y/N]:y
Info: This operation may take a few seconds. Please wait for a moment.......
[SwitchC-stack-port0/1] quit
[SwitchC] interface stack-port 0/2
```

```
[SwitchC-stack-port0/2] port interface gigabitethernet 0/0/28 enable
Warning: Enabling stack port cause configuration loss on the interface,
continue?[Y/N]:y
Info: This operation may take a few seconds. Please wait for a moment.....
```

2． 配置堆叠 ID 和堆叠优先级

配置 SwitchA 的堆叠优先级为200。

```
[SwitchA] stack slot 0 priority 200
Warning:Please do not frequently modify Priority, it will make the stack split!
continue?[Y/N]:y
```

- # 配置 SwitchB 的堆叠 ID 为1。

```
[SwitchB] stack slot 0 renumber 1
Warning: All the configurations related to the slot ID will be lost after the
slot ID is modified.
Please do not frequently modify slot ID, it will make the stack split.
Continue?[Y/N]:y
Info: Stack configuration has been changed, need reboot to take effect.
```

- # 配置 SwitchC 的堆叠 ID 为2。

```
[SwitchC] stack slot 0 renumber 2
Warning: All the configurations related to the slot ID will be lost after the
slot ID is modified.
Please do not frequently modify slot ID, it will make the stack split.
Continue?[Y/N]:y
Info: Stack configuration has been changed, need reboot to take effect.
```

3． SwitchA、SwitchB、SwitchC 下电，使用 SFP+电缆连接后再上电。

注意事项：

1.下电前，建议通过命令 save 保存配置。

2.本设备的 stack-port 0/1必须连接邻设备的 stack-port 0/2，否则堆叠组建不成功。

3.为保证堆叠组建成功，建议按照以下顺序进行连线上电（如果用户希望某台交换机为主交换机可以先为其上电。例如，按以下顺序连线上电后，SwitchA 为主交换机）：

a． 为 SwitchA～SwitchC 下电；

b． 连接 SwitchA 与 SwitchB 之间的堆叠线缆；

c． 先为 SwitchA 上电，SwitchA 启动后，再为 SwitchB 上电；

d． 与上一步类似:连接 SwitchC 与 SwitchB 和 SwitchA 之间的堆叠线缆,再为 SwitchC 上电；

13 静态路由配置

一、 功能简介

路由器根据路由转发数据包，路由可通过手动配置和使用动态路由算法计算产生，其中手动配置产生的路由就是静态路由。

静态路由比动态路由使用更少的带宽，并且不占用 CPU 资源来计算和分析路由更新。但是当网络发生故障或者拓扑发生变化后，静态路由不会自动更新，必须手动重新配置，因此静态路由适用于网络规模较小、网络拓扑明确的组网。静态路由有 5 个主要的参数：目的地址和掩码、出接口和下一跳、优先级。

与动态路由协议不同，静态路由自身没有检测机制，当网络发生故障的时候，需要管理员介入。

二、 配置命令和步骤

1.系统视图执行命令**ip route-static** destination-network mask nexthop-address |out-interface，配置到目的网络的静态路由

2. 通过配置优先级实现静态路由主备备份和负载分担，在系统视图执行命令**ip route-static** destination-network mask nexthop-address |out-interface **preference** preference，如果两条到达同一网络的静态路由优先级相同，则实现路由负载分担；如果两条静态路由优先级不同，则实现路由主备备份。

注意：在配置静态路由的时候可以同时指定出接口和下一跳地址，对于不同的出接口类型，可以指定出接口也可以指定下一跳地址；

A． 对于点对点类型的出接口，只需指定出接口；

B． 对于 NBMA 类型的接口，只需指定下一跳地址；

C． 对于广播类型的接口，必须指定下一跳地址；

三、 应用场景

13.1 不同网段通过静态路由实现互通

组网需求

如图 13-1 所示，属于不同网段的主机通过几台 Switch 相连，要求不配置动态路由协议，使不同网段的任意两台主机之间能够互通。

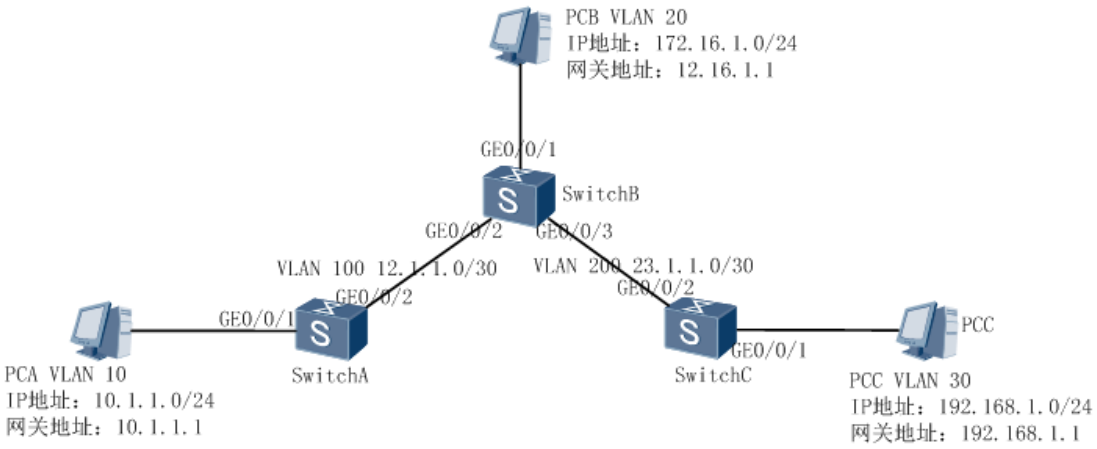


图 13-1 配置静态路由组网图

组网数据如下表所示：

设备名称	接口名称	所属的VLAN	VLANIF地址
SwitchA	GE0/0/1	VLAN 10	10.1.1.1/24
	GE0/0/2	VLAN 100	12.1.1.1/30
SwitchB	GE0/0/1	VLAN 20	172.16.1.1/24
	GE0/0/2	VLAN 100	12.1.1.2/30
	GE0/0/3	VLAN 300	23.1.1.1/30
SwitchC	GE0/0/1	VLAN 30	192.168.1.1/24
	GE0/0/2	VLAN 200	23.1.1.2/30

配置思路：

1． 创建 VLAN 并配置各接口所属 VLAN；

2． 配置各 VLANIF 接口的 IP 地址，实现相邻设备网络互通；

3． 在各主机上配置 IP 缺省网关，在各台 Switch 上配置 IPv4 静态路由或者静态缺省路由，实现不配置动态路由协议，使不同网段的任意两台主机之间能够互通。

详细配置步骤

1.配置各接口及所属的 VLAN

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchA
[SwitchA] vlan batch 10 100
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port link-type access
[SwitchA-GigabitEthernet0/0/1] port default vlan 10
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] port link-type access
[SwitchA-GigabitEthernet0/0/2] port default vlan 100
[SwitchA-GigabitEthernet0/0/2] quit
```

2.配置各 VLANIF 接口的 IP 地址

```
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] ip address 10.1.1.1 24
[SwitchA-Vlanif10] quit
[SwitchA] interface vlanif 100
[SwitchA-Vlanif100] ip address 12.1.1.1 30
```

```
[SwitchA-Vlanif100] quit
```

SwitchB 和 SwitchC 的配置跟 SwitchA 是一样的，只是修改下各个参数；

3.配置静态路由

#配置 SwitchA 的静态路由（配置静态缺省路由）

```
[SwitchA] ip route-static 0.0.0.0 0 12.1.1.2
```

#配置 SwitchB 的静态路由（明细路由）

```
[SwitchB] ip route-static 10.1.1.0 24 12.1.1.1 #配置到10.1.1.0网段的静态路由
[SwitchB] ip route-static 192.168.1.0 24 23.1.1.2 #配置到192.168.1.0网段的静态路由
```

#配置 SwitchC 的静态路由（明细路由）

```
[SwitchC] ip route-static 12.1.1.0 30 23.1.1.1
[SwitchC] ip route-static 10.1.1.0 24 23.1.1.1
[SwitchC] ip route-static 172.16.1.0 24 23.1.1.1
```

4.配置主机的 ip 地址和网关，VLAN10 的主机网关为 10.1.1.1，VLAN20 的主机网关为：172.16.1.1，VLAN30 的主机网关地址为 192.168.1.1.

5.验证配置结果

在 PCA 上面 ping PCB 或者 PCC 都是通的。

13.2 静态路由实现路由负载分担

组网需求

如图 13-2 所示，属于不同网段的主机通过几台 Switch 相连，要求不配置动态路由协议，使不同网段的任意两台主机之间能够互通，从拓扑图中可以看出，从 PCA 到 PCC 有两条路径可以过去，分别是 PCA-SwitchA-SwitchB-SwitchC-PCC 和 PCA-SwitchA-SwitchD-SwitchC-PCC，为了有效利用链路，要求从 VLAN10 到 VLAN30 的数据流分配到两条链路上，而且当一条链路故障之后所有的数据流走到另一条链路上去。

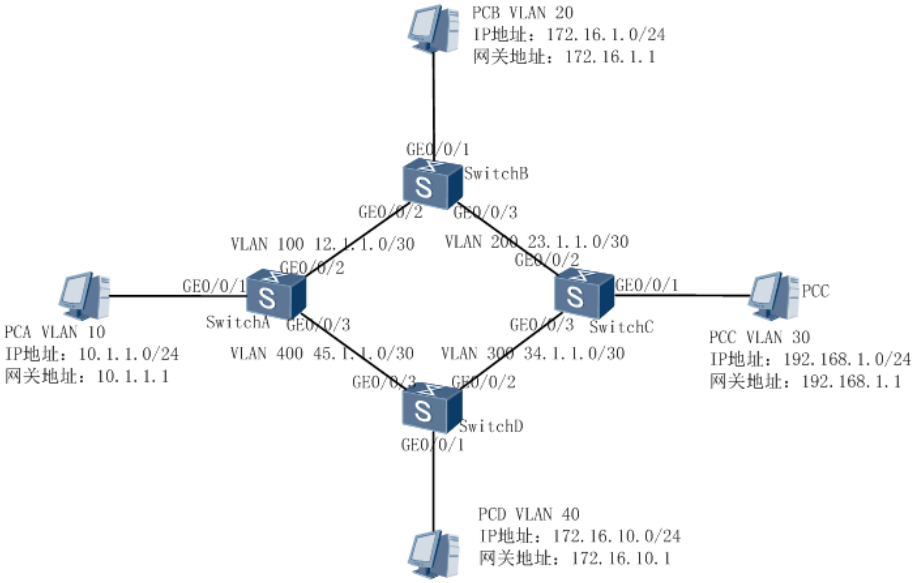


图13-2 静态路由实现路由负载分担

组网数据如下表所示：

设备名称	接口名称	所属的VLAN	VLANIF地址
SwitchA	GE0/0/1	VLAN 10	10.1.1.1/24
	GE0/0/2	VLAN 100	12.1.1.1/30
	GE0/0/3	VLAN 400	45.1.1.2/30
SwitchB	GE0/0/1	VLAN 100	12.1.1.2/30
	GE0/0/2	VLAN 200	23.1.1.1/30
SwitchC	GE0/0/1	VLAN 30	192.168.1.1/24
	GE0/0/2	VLAN 200	23.1.1.2/30
	GE0/0/3	VLAN 300	34.1.1.1/30
SwitchD	GE0/0/1	VLAN 400	45.1.1.1/30
	GE0/0/2	VLAN 300	34.1.1.2/30

配置思路

1． 配置接口所属的 VLAN；

2． 配置 VLANIF 接口地址；

3． 配置静态路由实现不同网络之间的互通

详细配置步骤

1.配置各接口及所属的VLAN

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchA
[SwitchA] vlan batch 10 100 400
```

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port link-type access
[SwitchA-GigabitEthernet0/0/1] port default vlan 10
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] port link-type access
[SwitchA-GigabitEthernet0/0/2] port default vlan 100
[SwitchA-GigabitEthernet0/0/2] quit
[SwitchA] interface gigabitethernet 0/0/3
[SwitchA-GigabitEthernet0/0/3] port link-type access
[SwitchA-GigabitEthernet0/0/3] port default vlan 400
[SwitchA-GigabitEthernet0/0/3] quit
```

2.配置各VLANIF接口的IP地址

```
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] ip address 10.1.1.1 24
[SwitchA-Vlanif10] quit
[SwitchA] interface vlanif 100
[SwitchA-Vlanif100] ip address 12.1.1.1 30
[SwitchA-Vlanif100] quit
[SwitchA] interface vlanif 400
[SwitchA-Vlanif400] ip address 45.1.1.2 30
[SwitchA-Vlanif400] quit
```

SwitchB、SwitchC和SwitchD的配置跟SwitchA是一样的，只是修改下各个参数；

3.配置静态路由实现网络互通

#配置 SwitchA 的静态路由，配置两条静态缺省路由，优先级都是 60，指向不同的下一跳地址

```
[SwitchA] ip route-static 0.0.0.0 0 12.1.1.2
[SwitchA] ip route-static 0.0.0.0 0 45.1.1.1
```

#配置 SwitchB 的静态路由（明细路由）

```
[SwitchB] ip route-static 10.1.1.0 24 12.1.1.1 #配置到10.1.1.0网段的静态路由
[SwitchB] ip route-static 192.168.1.0 24 23.1.1.2 #配置到192.168.1.0网段的静态路由
```

#配置 SwitchC 的静态路由（明细路由）

```
[SwitchC] ip route-static 10.1.1.0 24 23.1.1.1 #分别配置两条到10.1.1.0网段的等价静态路由
```

```
[SwitchC] ip route-static 10.1.1.0 24 34.1.1.2
[SwitchC] ip route-static 12.1.1.0 30 23.1.1.1 #配置到12.1.1.0网段的静态路由
[SwitchC] ip route-static 45.1.1.0 30 34.1.1.2 #配置到45.1.1.0网段的静态路由
```

#配置SwitchD的静态路由（明细路由）

```
[SwitchD] ip route-static 10.1.1.0 24 45.1.1.2 #配置到10.1.1.0网段的静态路由
[SwitchD] ip route-static 192.168.1.0 24 34.1.1.1 #配置到192.168.1.0网段的静态路由
```

4.配置结果验证

在PCA上面ping PCC是通的；

把SwitchB的任意一个接口down了之后，PCA ping PCC还是通的；

13.3 静态路由实现主备备份

组网需求

如图 13-3 所示，属于不同网段的主机通过几台 Switch 相连，要求不配置动态路由协议，使不同网段的任意两台主机之间能够互通，从拓扑图中可以看出，从 PCA 到 PCC 有两条路径可以过去，分别是 PCA-SwitchA-SwitchB-SwitchC-PCC 和 PCA-SwitchA-SwitchD-SwitchC-PCC，由于数据流不是很大，要求从 VLAN10 到 VLAN30 的数据流正常情况走上面一条链路，出故障之后切换到下面一条链路。

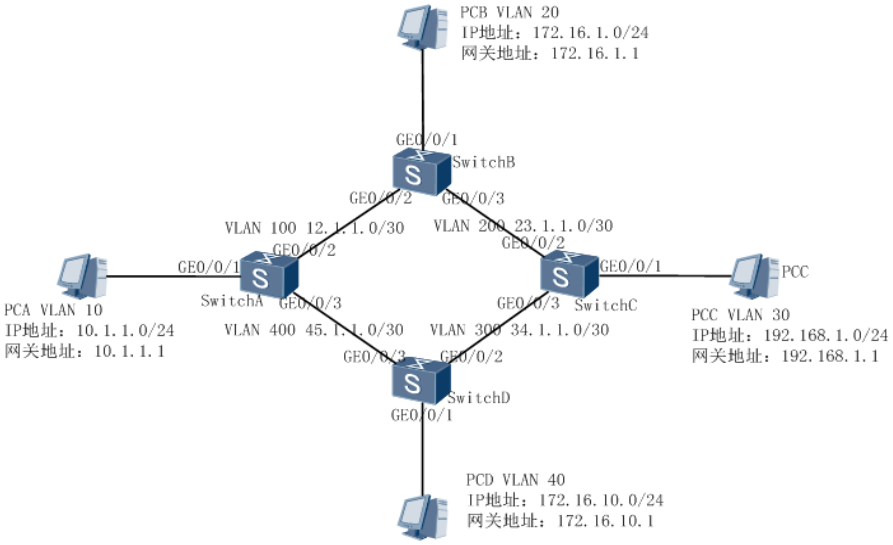


图13-3静态路由实现主备备份

配置思路

1.配置接口所属的VLAN；

2.配置VLANIF接口地址；

3.配置静态路由实现不同网络之间的互通

详细配置步骤

1.配置各接口及所属的VLAN

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchA
[SwitchA] vlan batch 10 100 400
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port link-type access
[SwitchA-GigabitEthernet0/0/1] port default vlan 10
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] port link-type access
[SwitchA-GigabitEthernet0/0/2] port default vlan 100
[SwitchA-GigabitEthernet0/0/2] quit
[SwitchA] interface gigabitethernet 0/0/3
[SwitchA-GigabitEthernet0/0/3] port link-type access
[SwitchA-GigabitEthernet0/0/3] port default vlan 400
[SwitchA-GigabitEthernet0/0/3] quit
```

2.配置各VLANIF接口的IP地址

```
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] ip address 10.1.1.1 24
[SwitchA-Vlanif10] quit
[SwitchA] interface vlanif 100
[SwitchA-Vlanif100] ip address 12.1.1.1 30
[SwitchA-Vlanif100] quit
[SwitchA] interface vlanif 400
[SwitchA-Vlanif400] ip address 45.1.1.2 30
[SwitchA-Vlanif400] quit
```

SwitchB、SwitchC和SwitchD的配置跟SwitchA是一样的，只是修改下各个参数；

3.配置静态路由实现网络互通

#配置 SwitchA 的静态缺省路由，一条优先级为默认的 60，另外一条优先级为 70，正常情况数据流走优先级为 60 的路由，只有当优先级为 60 的路由出故障之后才走优先级为 70 的路由；

```
[SwitchA] ip route-static 0.0.0.0 0 12.1.1.2
[SwitchA] ip route-static 0.0.0.0 0 45.1.1.1 preference 70
```

#配置 SwitchB 的静态路由（明细路由）

```
[SwitchB] ip route-static 10.1.1.0 24 12.1.1.1  #配置到10.1.1.0网段的静态路由
[SwitchB] ip route-static 192.168.1.0 24 23.1.1.2  #配置到192.168.1.0网段的
```

静态路由

#配置 SwitchC 的静态路由（明细路由）

```
[SwitchC] ip route-static 10.1.1.0 24 23.1.1.1 #配置两条到10.1.1.0网段的主备备份静态路由
[SwitchC] ip route-static 10.1.1.0 24 34.1.1.2 preference 70
[SwitchC] ip route-static 12.1.1.0 30 23.1.1.1 #配置到12.1.1.0网段的静态路由
[SwitchC] ip route-static 45.1.1.0 30 34.1.1.2 #配置到45.1.1.0网段的静态路由
```

#配置SwitchD的静态路由（明细路由）

```
[SwitchD] ip route-static 10.1.1.0 24 45.1.1.2 #配置到10.1.1.0网段的静态路由
[SwitchD] ip route-static 192.168.1.0 24 34.1.1.1  #配置到192.168.1.0网段的静态路由
```

4.配置结果验证

在PCA上面ping PCC是通的；

把SwitchB的任意一个接口down了之后，PCA ping PCC还是通的；

14 OSPF基础配置

一、功能简介

开放式最短路径优先OSPF（Open Shortest Path First）是IETF组织开发的一个基于链路状态的内部网关协议，OSPF路由协议是一种典型的链路状态（Link-state）的路由协议，一般用于同一个路由域内。在这里，路由域是指一个自治系统（Autonomous System），即AS，它是指一组通过统一的路由政策或路由协议互相交换路由信息的网络。在这个AS中，所有的OSPF路由器都维护一个相同的描述这个AS结构的数据库，该数据库中存放的是路由域中相应链路的状态信息，OSPF路由器正是通过这个数据库计算出其OSPF路由表的。

作为一种链路状态的路由协议，OSPF将链路状态组播数据LSA（Link State Advertisement）传送给在某一区域内的所有路由器，这一点与距离矢量路由协议不同。运行距离矢量路由协议的路由器是将部分或全部的路由表传递给与其相邻的路由器。

二、配置步骤和命令

1.在系统视图执行命令**OSPF** process-id **router-id** router-id，创建OSPF进程，并进入OSPF视图；

2.在OSPF视图下执行命令**area** area-id，创建OSPF区域；

3.在OSPF的area区域中使能OSPF，执行命令**network** ip-address wildcard-mask，配置区域所包含的网段；

三、应用场景

14.1 配置OSPF基本功能

组网需求

如图14-1所示，局域网中四个部门分别属于VLAN10、VLAN20、VLAN30和VLAN40，现在需要实现四个部门之间网络互通，考虑到配置静态路由配置繁琐以后网络出故障还得管理员手动去修改静态路由的配置，所以配置OSPF动态路由实现网络互通。

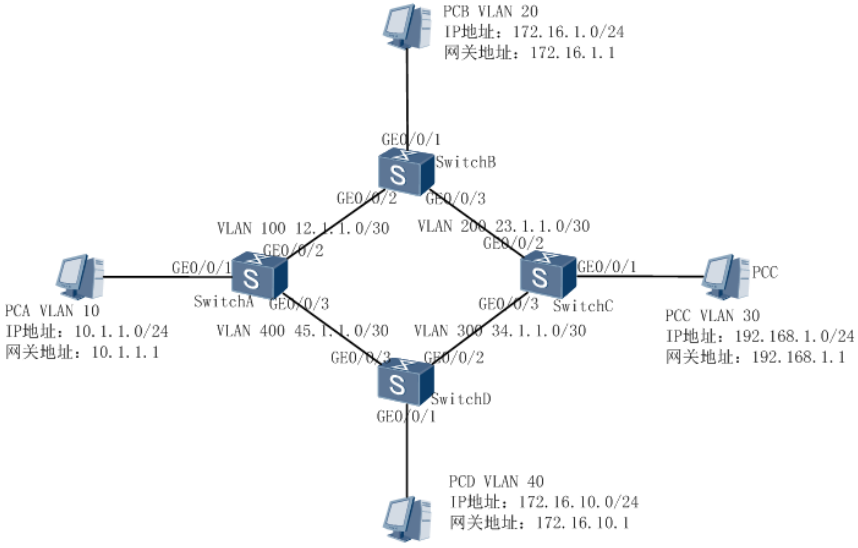


图14-1 配置OSPF基本功能组网图

组网数据如下表所示：

设备名称	接口名称	所属的VLAN	VLANIF地址
SwitchA	GE0/0/1	VLAN 10	10.1.1.1/24
	GE0/0/2	VLAN 100	12.1.1.1/30
	GE0/0/3	VLAN 400	45.1.1.2/30
SwitchB	GE0/0/1	VLAN 20	172.16.1.1/24
	GE0/0/2	VLAN 100	12.1.1.2/30
	GE0/0/3	VLAN 200	23.1.1.1/30
SwitchC	GE0/0/1	VLAN 30	192.168.1.1/24
	GE0/0/2	VLAN 200	23.1.1.2/30
	GE0/0/3	VLAN 300	34.1.1.1/30
SwitchD	GE0/0/1	VLAN 40	172.16.10.1/24
	GE0/0/2	VLAN 300	34.1.1.2/30
	GE0/0/3	VLAN 400	45.1.1.1/30

配置思路

1. 配置各接口和所属的 VLAN；
2. 配置 VLANIF 接口地址；
3. 配置 OSPF 功能；

详细配置步骤

1． 配置各接口和所属的 VLAN；

```
<HUAWEI> system-view
[HUAWEI] sysname SwitchA
[SwitchA] vlan batch 10 100 400
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port link-type access
[SwitchA-GigabitEthernet0/0/1] port default vlan 10
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] port link-type access
[SwitchA-GigabitEthernet0/0/2] port default vlan 100
[SwitchA-GigabitEthernet0/0/2] quit
[SwitchA] interface gigabitethernet 0/0/3
[SwitchA-GigabitEthernet0/0/3] port link-type access
[SwitchA-GigabitEthernet0/0/3] port default vlan 400
[SwitchA-GigabitEthernet0/0/3] quit
```

2． 配置 VLANIF 接口地址；

```
[SwitchA] interface vlanif 10
[SwitchA-Vlanif10] ip address 10.1.1.1 24
[SwitchA-Vlanif10] quit
[SwitchA] interface vlanif 100
[SwitchA-Vlanif100] ip address 12.1.1.1 30
[SwitchA-Vlanif100] quit
[SwitchA] interface vlanif 400
[SwitchA-Vlanif400] ip address 45.1.1.2 30
[SwitchA-Vlanif400] quit
```

上面基础配置只列出了SwitchA的，剩余的几台配置方式跟SwitchA是一样的，只是修改下相应的参数。

3． 配置 OSPF 功能；

#配置SwitchA的OSPF功能

```
[SwitchA] ospf 100 router-id 1.1.1.1    #配置OSPF进程为100，router-id为
1.1.1.1
[SwitchA-ospf-100] area 0   #配置OSPF的区域为area 0
[SwitchA-ospf-100-area-0.0.0.0] network 10.1.1.0 0.0.0.255 #把直连的网络宣告
```

```
进OSPF
    [SwitchA-ospf-100-area-0.0.0.0] network 12.1.1.0 0.0.0.3
    [SwitchA-ospf-100-area-0.0.0.0] network 45.1.1.0 0.0.0.3
```

#配置SwitchB的OSPF功能

```
    [SwitchB] ospf 100 router-id 2.2.2.2    #配置OSPF进程为100，router-id为
2.2.2.2
    [SwitchB-ospf-100] area 0   #配置OSPF的区域为area 0
    [SwitchB-ospf-100-area-0.0.0.0] network 172.16.1.0 0.0.0.255   #把直连的网
络宣告进OSPF
    [SwitchB-ospf-100-area-0.0.0.0] network 12.1.1.0 0.0.0.3
    [SwitchB-ospf-100-area-0.0.0.0] network 23.1.1.0 0.0.0.3
```

#配置SwitchC的OSPF功能

```
    [SwitchC]  ospf 100 router-id 3.3.3.3   #配置OSPF进程为100，router-id为
3.3.3.3
    [SwitchC-ospf-100] area 0   #配置OSPF的区域为area 0
    [SwitchC-ospf-100-area-0.0.0.0] network 192.168.1.0 0.0.0.255  #把直连的网
络宣告进OSPF
    [SwitchC-ospf-100-area-0.0.0.0] network 34.1.1.0 0.0.0.3
    [SwitchC-ospf-100-area-0.0.0.0] network 23.1.1.0 0.0.0.3
```

#配置SwitchD的OSPF功能

```
    [SwitchD] ospf 100 router-id 4.4.4.4    配置OSPF进程为100，router-id为4.4.4.4
    [SwitchD-ospf-100] area 0   #配置OSPF的区域为area 0
    [SwitchD-ospf-100-area-0.0.0.0] network 172.16.10.0 0.0.0.255  #把直连的网
络宣告进OSPF
    [SwitchD-ospf-100-area-0.0.0.0] network 34.1.1.0 0.0.0.3
    [SwitchD-ospf-100-area-0.0.0.0] network 45.1.1.0 0.0.0.3
```

4． 结果验证

在PCA上面去ping PCB、PCC、PCD的地址都是通的，证明OSPF配置是正确的。