目 录

DHCP 典型配置举例

关键词：DHCP，Option82

摘 要：本文主要介绍以太网交换机的 DHCP 功能在具体组网中的应用配置，根据设备在网络中担当的不同角色，分别介绍 DHCP Server、DHCP Relay、DHCP Snooping 功能，以及 DHCP Option82 的功能及应用。

缩略语：DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）

第1章 DHCP 功能介绍

1.1 支持能力

1.1.1 H3C 系列产品支持的 DHCP 功能列表

表1-1 H3C 系列产品支持的 DHCP 功能列表

功能 / 产品型号	DHCP Server	DHCP Relay	DHCP Snooping
S3600-EI	●	●	●
S3600-SI	-	●	●
S5600	●	●	●
S5100	-	-	●
S3100-SI	-	-	●
S3100-52P	-	-	●
E352/E328	-	●	●
E126	-	-	●
E152	-	-	●

H3C 系列以太网交换机根据设备型号的不同，可以支持以下部分或全部 DHCP 功能。

DHCP Server：

- 支持使用全局地址池/接口地址池的 DHCP Server
- 支持配置 IP 地址租期
- 支持为 DHCP 客户端分配网关地址、DNS 服务器地址、WINS 服务器地址
- 支持对特殊地址进行静态绑定
- 支持 DHCP Server 安全功能：伪 DHCP Server 检测、IP 重复分配检测

DHCP Relay：

- 支持 DHCP Relay
- 支持 DHCP Relay 安全功能：地址匹配检查、服务器端握手功能、用户地址表项定时刷新功能
- 支持 DHCP Option82

DHCP Snooping：

- 支持 DHCP Snooping
- 支持 DHCP Snooping 安全功能：DHCP Snooping 表项更新、ARP 源检查
- 支持 DHCP Option82

📖 **说明：**

有关各款交换机支持的 DHCP 功能的详细介绍，请参见各产品的用户手册。

1.2 配置指南

📖 **说明：**

- 不同型号的设备，配置的方法会有差异，这里以 S3600 系列交换机作为举例。其它型号交换机的配置请参见产品的操作手册。
- 下文只列出了基本的配置步骤，有关各个功能的基本原理和作用，请参见各产品的操作、命令手册。

1.2.1 DHCP Server 配置

对于 DHCP Server 设备，可以使用全局地址池和接口地址池进行地址分配。这两种配置方法的适用情况是：

- 如果 DHCP Client 和 DHCP Server 在同一网段，这两种配置方法都适用；
- 如果 DHCP Client 与 DHCP Server 不在同一网段，那么只能用基于全局地址池的 DHCP Server 配置。

(1) 使用全局地址池分配地址的配置过程：

表1-2 使用全局地址池分配地址的配置过程

操作	命令	说明
进入系统视图	**system-view**	-
使能 DHCP 服务	**dhcp enable**	可选 缺省情况下，DHCP 服务处于使能状态
创建 DHCP 地址池并进入 DHCP 地址池视图	**dhcp server ip-pool** *pool-name*	必选 缺省情况下，没有创建 DHCP 全局地址池

<table>
<tr><th colspan="3">操作</th><th>命令</th><th>说明</th></tr>
<tr><td colspan="3">配置动态分配的IP地址范围</td><td>network ip-address [mask-length | mask mask]</td><td>必选
缺省情况下，没有配置动态分配的 IP 地址范围，即没有可供分配的地址</td></tr>
<tr><td colspan="3">配置动态分配的IP地址租用有效期限</td><td>expired { day day [hour hour [minute minute]] | unlimited }</td><td>可选
缺省情况下，IP 地址租用有效期限为 1 天</td></tr>
<tr><td colspan="3">配置为 DHCP 客户端分配的域名</td><td>domain-name domain-name</td><td>必选
缺省情况下，没有配置为 DHCP 客户端分配的域名</td></tr>
<tr><td colspan="3">配置为 DHCP 客户端分配的 DNS 服务器地址</td><td>dns-list ip-address&<1-8></td><td>必选
缺省情况下，没有配置 DNS 服务器地址</td></tr>
<tr><td colspan="3">配置为 DHCP 客户端分配的 WINS 服务器地址</td><td>nbns-list ip-address&<1-8></td><td>必选
缺省情况下，没有配置 WINS 服务器地址</td></tr>
<tr><td colspan="3">配置 DHCP 客户端的 NetBIOS 节点类型</td><td>netbios-type { b-node | h-node | m-node | p-node }</td><td>可选
缺省情况下，交换机不指定 DHCP 客户端的 NetBIOS 节点类型，客户端采用 h 类节点（h-node）</td></tr>
<tr><td colspan="3">配置为 DHCP 客户端分配的网关地址</td><td>gateway-list ip-address&<1-8></td><td>必选
缺省情况下，没有配置 DHCP 客户端的网关地址</td></tr>
<tr><td colspan="3">配置 DHCP 自定义选项</td><td>option code { ascii ascii-string | hex hex-string&<1-10> | ip-address ip-address&<1-8> }</td><td>必选
缺省情况下，没有配置 DHCP 自定义选项</td></tr>
<tr><td rowspan="5">配置静态绑定的 IP 地址</td><td colspan="2">退出至系统视图</td><td>quit</td><td rowspan="5">可选
缺省情况下，没有配置静态绑定的 MAC 地址或客户端 ID
需要注意的是：
● 配置绑定的 IP 地址必须与绑定的 MAC 地址或客户端 ID 二者之一共同配置才能生效
● 一个静态绑定地址池中只能配置一对 IP 地址与 MAC/客户端 ID 的绑定关系</td></tr>
<tr><td colspan="2">创建静态绑定的地址池</td><td>dhcp server ip-pool pool-name</td></tr>
<tr><td colspan="2">配置静态绑定的 IP 地址</td><td>static-bind ip-address ip-address [mask-length | mask mask]</td></tr>
<tr><td rowspan="2">配置静态绑定的 MAC 地址或客户端 ID</td><td>配置静态绑定的客户端 MAC 地址</td><td>static-bind mac-address mac-address</td></tr>
<tr><td>配置静态绑定的客户端 ID</td><td>static-bind client-identifier client-identifier</td></tr>
</table>

操作		命令	说明
退回至系统视图		**quit**	-
配置 DHCP 地址池中不参与自动分配的 IP 地址		**dhcp server forbidden-ip** *low-ip-address* [*high-ip-address*]	可选 缺省情况下，DHCP 地址池中的所有 IP 地址都参与自动分配
配置接口工作在全局地址池模式	配置当前接口	**interface** *interface-type interface-number*	可选 缺省情况下，接口工作在 DHCP 服务器全局地址池模式
		dhcp select global	
		quit	
	系统视图下同时配置多个接口	**dhcp select global** { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }	
使能伪 DHCP 服务器检测功能		**dhcp server detect**	必选 缺省情况下，禁止伪 DHCP 服务器检测功能
配置 IP 地址重复分配检测功能	配置 DHCP 服务器 ping 操作的次数	**dhcp server ping packets** *number*	可选 缺省情况下，ping 操作的次数为 2
	配置 DHCP 服务器等待响应的时间	**dhcp server ping timeout** *milliseconds*	可选 缺省情况下，等待 ping 响应的最长时间为 500 毫秒
配置 DHCP 服务器支持 Option 82 功能		**dhcp server relay information enable**	可选 缺省情况下，DHCP 服务器支持 Option 82 功能

(2) 使用接口地址池分配地址的配置过程：

表1-3 使用接口地址池分配地址的配置过程

操作	命令	说明
进入系统视图	**system-view**	-
使能 DHCP 服务	**dhcp enable**	可选 缺省情况下，DHCP 服务处于使能状态
同时配置多个 VLAN 接口工作在接口地址池模式	**dhcp select interface** { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }	可选
配置单个 VLAN 接口工作在接口地址池模式	**interface** *interface-type interface-number*	必选 缺省情况下，VLAN 接口工作在全局地址池模式
	dhcp select interface	

操作		命令	说明
配置静态绑定的 IP 地址		**dhcp server static-bind ip-address** *ip-address* { **client-identifier** *client-identifier* | **mac-address** *mac-address* }	可选 缺省情况下，没有配置静态绑定
配置动态分配的 IP 地址租用有效期限	配置当前接口	**dhcp server expired** { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** }	可选 缺省情况下，IP 地址租用有效期限为 1 天
	系统视图下配置多个接口	**quit**	
		dhcp server expired { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** } { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }	
退出至系统视图		**quit**	-
配置 DHCP 地址池中不参与自动分配的 IP 地址		**dhcp server forbidden-ip** *low-ip-address* [*high-ip-address*]	可选 缺省情况下，接口地址池中的所有 IP 地址都参与自动分配
配置为 DHCP 客户端分配的域名	配置单个接口	**interface** *interface-type interface-number*	可选 缺省情况下，没有配置为 DHCP 客户端分配的域名
		dhcp server domain-name *domain-name*	
		quit	
	配置多个接口	**dhcp server domain-name** *domain-name* { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }	
配置为 DHCP 客户端分配的 DNS 服务器地址	配置单个接口	**interface** *interface-type interface-number*	可选 缺省情况下，没有配置 DNS 服务器的地址
		dhcp server dns-list *ip-address*&<1-8>	
		quit	
	配置多个接口	**dhcp server dns-list** *ip-address*&<1-8> { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }	

操作		命令	说明
配置为 DHCP 客户端分配的 WINS 服务器地址	配置单个接口	**interface** *interface-type interface-number*	可选 缺省情况下，没有配置 WINS 服务器的 IP 地址
		dhcp server nbns-list *ip-address*&<1-8>	
		quit	
	配置多个接口	**dhcp server nbns-list** *ip-address*&<1-8> { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }	
配置 DHCP 客户端的 NetBIOS 节点类型	配置单个接口	**interface** *interface-type interface-number*	可选 缺省情况下，交换机不指定接口 DHCP 地址池的客户端 NetBIOS 节点类型，客户端采用 h 类节点（**h-node**）
		dhcp server netbios-type { **b-node** | **h-node** | **m-node** | **p-node** }	
		quit	
	配置多个接口	**dhcp server netbios-type** { **b-node** | **h-node** | **m-node** | **p-node** } { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }	
配置 DHCP 自定义选项	配置单个接口	**interface** *interface-type interface-number*	可选 缺省情况下，没有配置 DHCP 自定义选项
		dhcp server option *code* { **ascii** *ascii-string* | **hex** *hex-string*&<1-10> | **ip-address** *ip-address*&<1-8> }	
		quit	
	配置多个接口	**dhcp server option** *code* { **ascii** *ascii-string* | **hex** *hex-string*&<1-10> | **ip-address** *ip-address*&<1-8> } { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }	
配置伪 DHCP 服务器检测功能		**dhcp server detect**	可选 缺省情况下，禁止伪 DHCP 服务器检测功能
配置 IP 地址重复分配检测功能	配置 DHCP 服务器 ping 操作的次数	**dhcp server ping packets** *number*	可选 缺省情况下，ping 操作的次数为 2
	配置 DHCP 服务器等待响应的时间	**dhcp server ping timeout** *milliseconds*	可选 缺省情况下，等待 ping 响应的最长时间为 500 毫秒

操作	命令	说明
配置 DHCP 服务器支持 Option 82 功能	**dhcp server relay information enable**	可选 缺省情况下，DHCP 服务器支持 Option 82 功能

1.2.2 DHCP Relay 配置

对工作在 DHCP Relay 模式下的交换机，需要进行以下的配置。

表1-4 DHCP Relay 配置

操作	命令	说明
进入系统视图	**system-view**	-
使能 DHCP 服务	**dhcp enable**	可选 缺省情况下，DHCP 服务处于使能状态
配置 DHCP 服务器组中 DHCP 服务器的地址	**dhcp-server** *groupNo* **ip** *ip-address*&<1-8>	必选 缺省情况下，没有配置 DHCP 服务器组中的服务器的 IP 地址
配置 DHCP 用户地址表项	**dhcp-security static** *ip-address mac-address*	可选 缺省情况下，没有配置 DHCP 用户地址表项
使能 DHCP Relay 握手功能	**dhcp relay hand enable**	可选 缺省情况下，交换机上 DHCP Relay 握手功能处于使能状态
配置 DHCP 中继动态用户地址表项的定时刷新周期	**dhcp-security tracker** { *interval* | **auto** }	可选 缺省情况下，根据表项的数目自动计算握手时间间隔。
使能伪 DHCP 服务器检测功能	**dhcp-server detect**	必选 缺省情况下，禁止伪 DHCP 服务器检测功能
配置 DHCP 中继支持 option 82 功能	**dhcp relay information enable**	必选 缺省情况下，DHCP 中继不支持 option 82 功能
配置 DHCP 中继对包含 option 82 的请求报文的处理策略	**dhcp relay information strategy** { **drop** | **keep** | **replace** }	可选 缺省情况下，处理策略为 **replace**
进入 VLAN 接口视图	**interface** *interface-type interface-number*	-

操作	命令	说明
配置接口与 DHCP 服务器组的归属关系	**dhcp-server** *groupNo*	必选 缺省情况下，VLAN 接口没有与任何一个 DHCP 服务器组建立归属关系
使能 DHCP 中继的地址匹配检查功能	**address-check enable**	必选 缺省情况，禁止 DHCP 中继的地址匹配检查功能

1.2.3 DHCP Snooping 配置

对工作在 DHCP Snooping 模式下的设备，需要做以下的配置。

表1-5 DHCP Snooping 配置

操作	命令	说明
进入系统视图	**system-view**	-
开启交换机 DHCP-Snooping 功能	**dhcp-snooping**	必选 缺省情况下，以太网交换机的 DHCP-Snooping 功能处于禁止状态
进入以太网端口视图	**interface** *interface-type interface-number*	-
指定连接到 DHCP 服务器方向的端口为信任端口	**dhcp-snooping trust**	可选 缺省情况下，交换机的端口均为不信任端口

第2章 配置举例

2.1 DHCP Server 配置举例

2.1.1 组网需求

位于公司总部（HQ）的 S3600 交换机作为 DHCP Server，为总部机构及分支机构（Branch）的工作站分配 IP 地址，并作为网关转发总部设备的报文，具体需求如下：

- 为总部机构分配 10.214.10.0/24 网段的 IP 地址，有效期为 2 天，其中 DNS Server、WINS Server 和 Mail Server 的 IP 地址设置为不可分配地址。
- 使用静态绑定方式为总部的 DNS/WINS/Mail Server 分配 IP 地址。
- 为分支机构分配 10.210.10.0/24 网段的地址，有效期为 3 天，其中分支机构的文件服务器使用 IP 与 MAC 绑定的方式静态分配。
- 为总部和分支机构的工作站在分配地址时同时分配网关地址、DNS Server 地址、WINS Server 地址。
- 启用伪 DHCP Server 检测功能，避免私自架设的 DHCP Server 分配无效地址。

2.1.2 组网图

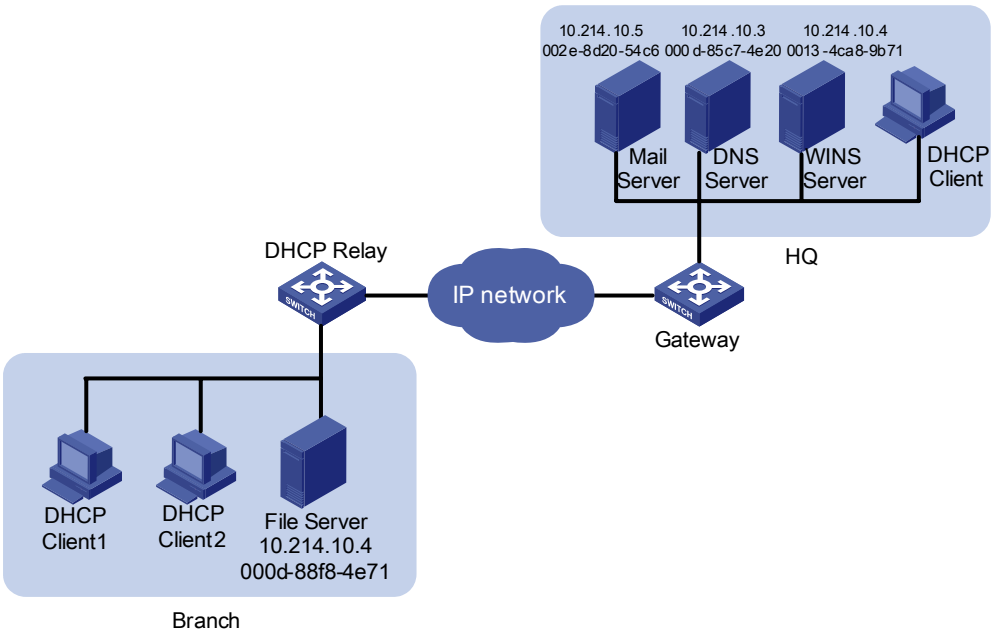


图2-1 DHCP Server 配置举例组网示例图

2.1.3 配置步骤

1. 使用的版本

本举例中使用的设备为 S3600 系列以太网交换机，软件版本为 Release 1510。

2. 配置 DHCP Server

- 配置为总部设备分配地址

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

```
<H3C> system-view
[H3C] interface Vlan-interface 10
[H3C-Vlan-interface10] ip address 10.214.10.1 24
```

配置该接口工作在接口地址池模式下，为总部设备分配 10.214.10.0/24 网段的 IP 地址。

```
[H3C-Vlan-interface10] dhcp select interface
```

配置该地址池的有效期，并配置指定的 DNS、WINS 服务器。

```
[H3C-Vlan-interface10] dhcp server expired day 2
[H3C-Vlan-interface10] dhcp server dns-list 10.214.10.3
[H3C-Vlan-interface10] dhcp server nbst-list 10.214.10.4
```

由于工作在接口地址池的接口会自动将自身作为 DHCP 客户端的网关，并把信息发送给客户端，因此无需进行客户端网关的配置操作。

使用 IP 地址与 MAC 地址绑定的方式为 DNS/WINS/Mail Server 分配 IP 地址。

```
[H3C-Vlan-interface10] dhcp server static-bind ip-address 10.214.10.3
mac-address 000d-85c7-4e20
[H3C-Vlan-interface10] dhcp server static-bind ip-address 10.214.10.4
mac-address 0013-4ca8-9b71
[H3C-Vlan-interface10] dhcp server static-bind ip-address 10.214.10.5
mac-address 002e08d20-54c6
```

配置 DNS/WINS/Mail Server 的静态 IP 地址为不可分配地址。

```
[H3C-Vlan-interface10] quit
[H3C] dhcp server forbidden-ip 10.214.10.3 10.214.10.5
```

- 配置为分支机构分配地址

为分支机构创建名为“br”的全局地址池，并指定可分配的地址范围及有效期。

```
[H3C] dhcp server ip-pool br
[H3C-dhcp-pool-br] network 10.210.10.0 mask 255.255.255.0
[H3C-dhcp-pool-br] expired day 3
```

创建静态绑定地址池名为“br-static”，将分支机构的文件服务器的 IP 地址配置为与 MAC 地址静态绑定分配方式。

```
[H3C-dhcp-pool-br] quit
[H3C] dhcp server ip-pool br-static
[H3C-dhcp-pool-br-static] static-bind ip-address 10.214.10.4 mask
255.255.255.0
[H3C-dhcp-pool-br-static] static-bind mac-address 000d-88f8-4e71
```

为分支机构工作站指定网关、DNS、WINS 服务器。

```
[H3C-dhcp-pool-br-static] quit
[H3C] dhcp server ip-pool br
[H3C-dhcp-pool-br] gateway-list 10.210.10.1
[H3C-dhcp-pool-br] dns-list 10.214.10.3
[H3C-dhcp-pool-br] nbst-list 10.214.10.4
```

配置分支机构的 Gateway 的静态 IP 为不可分配地址。

```
[H3C-dhcp-pool-br] quit
[H3C] dhcp server forbidden-ip 10.210.10.1
```

配置伪 DHCP Server 检测功能。

```
[H3C] dhcp server detect
```

配置 Vlan-interface10 接口工作在全局地址池模式。

```
[H3C] interface Vlan-interface 10
[H3C-Vlan-interface10] dhcp select global
```

需要注意的是：

在完成 DHCP 配置后，总部到分支机构必须具备可达的路由，才能够为其分配 IP 地址。

3. 配置 DHCP Relay

本节主要介绍DHCP Server的配置，对于举例中的DHCP Relay设备配置，只进行最简单的介绍，保证其可以将DHCP请求转发至DHCP Server。有关DHCP Relay的更多具体功能配置，请参见2.2 DHCP Relay/Snooping综合配置举例的介绍。

```
<H3C> system-view
[H3C] dhcp-server 1 ip 10.214.10.1
[H3C] interface Vlan-interface 5
[H3C-Vlan-interface5] dhcp-server 1
```

2.2 DHCP Relay/Snooping 综合配置举例

2.2.1 组网需求

位于总部的 Cisco Catalyst 3745 交换机作为 DHCP Server 为分支机构的办公区域工作站分配 IP 地址，分支机构采用 IRF 架构作为中心结点，并作为 DHCP Relay

转发工作站的 DHCP 请求。同时分支机构采用自己的 DHCP Server 为实验室设备分配独立 IP 网段的地址。具体需求如下：

- 总部的 DHCP Server 为办公室设备分配 192.168.10.0/24 网段的地址，有效期为 12 小时，并指定该地址池的 DNS 和 WINS 服务器分别为 192.169.100.2 和 192.168.100.3。
- 分支机构的 IRF 由四台设备构成，作为 DHCP Relay 转发办公室工作站和实验室设备的 DHCP 请求，并配置伪 DHCP Server 检测功能。
- Lab1 内有一台以太网交换机作为 Lab DHCP Server，为 Lab1 的设备分配 192.168.17.0/24 网段的地址，有效期 1 天；为 Lab2 的设备分配 192.168.19.0/24 网段的地址，有效期 2 天。Lab DHCP Server 与 IRF 架构使用 172.16.2.4/30 网段进行互连。
- 配置 DHCP Relay 的地址检查功能，使通过 DHCP Server 获得合法 IP 地址的设备才可以访问外部网络。
- 配置 DHCP Relay 表项定时刷新功能，每隔 1 分钟向 DHCP Server 进行地址表项刷新。
- 配置 DHCP Snooping 支持 DHCP Option82，将本地的端口信息添加到 DHCP 报文的 Option82 字段中。
- 配置 DHCP Relay 设备支持 DHCP Option82，Relay 在接收到携带有 DHCP Option82 选项的 DHCP 报文时，保留原有字段不作替换。
- 配置 DHCP Server 支持 DHCP Option82，为 Snooping 设备端口 Ethernet0/11 接入的客户端分配 192.168.10.2～192.168.10.25 之间的地址，为 Ethernet0/12 端口接入的客户端分配 192.168.10.100～192.168.10.150 之间的地址。

2.2.2 组网图

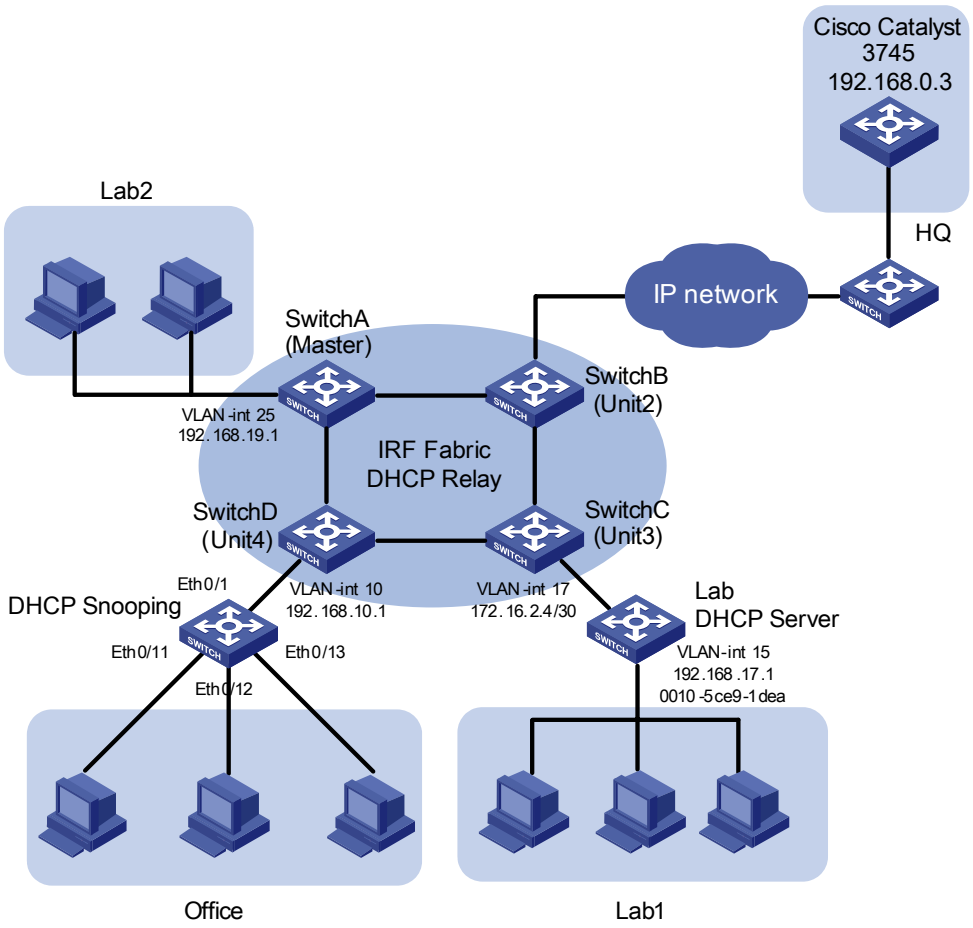


图2-2 DHCP Relay/Snooping 综合配置举例组网示意图

2.2.3 配置步骤

本举例中 IRF 架构中的设备为 S3600，软件版本为 Release 1510；DHCP Snooping 设备使用 Quidway S3552 设备，软件版本为 Release 0028；Lab DHCP Server 为 Quidway S3528 设备，软件版本为 Release 0028。

为方便阅读，下文配置中的各设备名称分别为：

- IRF 中的设备分别为 SwitchA、SwitchB、SwitchC、SwitchD
- DHCP Snooping 设备的名称为“Snooping”
- Lab DHCP Server 设备的名称为“LAB”

1. 配置 IRF

S3600 支持 IRF 特性，可以将四台设备互连成为一个 Fabric，用户可以对 Fabric 中的设备进行集中管理。详细介绍及配置过程请见 S3600 系列以太网交换机操作手册中的介绍。

2. 配置 DHCP Relay

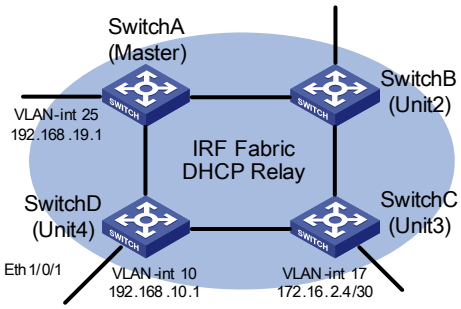


图2-3 DHCP Relay 组网

IRF 内的设备可以实现配置互相同步的功能，因此这里只在 SwitchA 上进行配置。

配置将办公室内的 DHCP 请求报文转发至 HQ 的 DHCP Server。

```
<SwitchA> system-view
[SwitchA] dhcp-server 1 ip 192.168.0.3
[SwitchA] interface Vlan-interface10
[SwitchA-Vlan-interface10] ip address 192.168.10.1 24
[SwitchA-Vlan-interface10] dhcp-server 1
```

配置将 Lab2 内的 DHCP 请求报文转发至 Lab DHCP Server。

```
[SwitchA-Vlan-interface10] quit
[SwitchA] dhcp-server 2 ip 192.168.17.1
[SwitchA] interface Vlan-interface 25
[SwitchA-Vlan-interface25] ip address 192.168.19.1 24
[SwitchA-Vlan-interface25] dhcp-server 2
```

配置 Vlan-interface17 的接口地址为 172.16.2.5/30，用于与 Lab DHCP Server 转发跨网段的 DHCP 报文。

```
[SwitchA-Vlan-interface25] quit
[SwitchA] interface Vlan-interface 17
[SwitchA-Vlan-interface17] ip add 172.16.2.5 30
```

配置 DHCP Relay 的地址检查功能，这里注意要将 DHCP Server 的 IP 地址和 MAC 地址作为静态表项配置到安全功能中。

```
[SwitchA-Vlan-interface17] quit
[SwitchA] dhcp-security static 192.168.0.3 000D-88F8-4E71
[SwitchA] dhcp-security static 192.168.17.1 0010-5ce9-1dea
[SwitchA] interface Vlan-interface 10
[SwitchA-Vlan-interface10] address-check enable
[SwitchA-Vlan-interface10] quit
[SwitchA] interface Vlan-interface 25
[SwitchA-Vlan-interface25] address-check enable
[SwitchA-Vlan-interface25] quit
```

配置 DHCP Relay 的地址表项定时刷新功能。

```
[SwitchA] dhcp relay hand enable
[SwitchA] dhcp-security tracker 60
```

配置 DHCP Relay 支持 DHCP Option82，并在收到带有 Option82 内容的 DHCP 报文时采取保留原字段的策略。

```
[SwitchA] dhcp relay information enable
[SwitchA] dhcp relay information strategy keep
```

配置 DHCP Relay 的伪 DHCP Server 检测功能

```
[SwitchA] dhcp-server detect
```

启动 UDP-Helper 功能，使 IRF 能够正常工作在 DHCP Relay 模式。

```
[SwitchA] udp-helper enable
```

为保证跨网段的 DHCP 报文能够正确转发，需要配置路由协议，并将本设备的接口网段进行发布。这里以 RIP 为例。其他路由协议的配置方法请参考产品手册的路由协议部分。

```
[SwitchA] rip
[SwitchA-rip] network 192.168.10.0
[SwitchA-rip] network 192.168.19.0
[SwitchA-rip] network 172.16.0.0
```

📖 **说明：**

在使用 IRF 构架的 DHCP Relay 与总部的 DHCP Server 之间，通过 IP 网络进行互联，也需要保证报文路由可达，这部分配置由运营商或用户进行操作，这里不进行介绍。

---

3. 配置 Lab DHCP Server

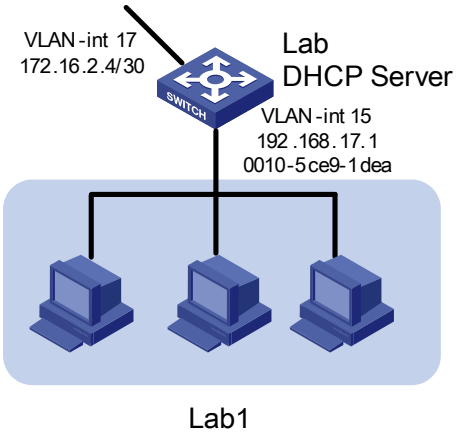


图2-4 Lab DHCP Server 组网

配置 Lab2 的地址池，并配置地址范围、有效期，网关地址。

```
<LAB> system-view
[LAB] dhcp enable
[LAB] dhcp server ip-pool lab2
[LAB-dhcp-lab2] network 192.168.19.0 255.255.255.0
[LAB-dhcp-lab2] expired day 2
[LAB-dhcp-lab2] gateway-list 192.168.19.1
```

配置 Vlan-interface17 的 IP 地址为 172.16.2.6/30，并使其工作在全局地址池模式

```
[LAB-dhcp-lab2] quit
[LAB] interface Vlan-interface 17
[LAB-Vlan-interface17] ip address 172.16.2.6 30
[LAB-Vlan-interface17] dhcp select global
```

由于 Lab1 连接到 Vlan-interface15 接口，因此，只需要配置 Vlan-interface15 接口工作在接口地址池模式，即可为 Lab1 的设备分配 192.168.17.0/24 网段的地址。

```
[LAB-Vlan-interface17] quit
[LAB] interface Vlan-interface 15
[LAB-Vlan-interface15] ip address 192.168.17.1 24
[LAB-Vlan-interface15] dhcp select interface
[LAB-Vlan-interface15] quit
```

为保证该服务器能够正常转发 DHCP 报文，需要配置路由协议，参照 Relay 的配置，这里以 RIP 为例。其他路由协议的配置方法请参考产品手册中的描述。

```
[LAB] rip
[LAB-rip] network 192.168.17.0
[LAB-rip] network 172.16.0.0
```

4. 配置 DHCP Snooping

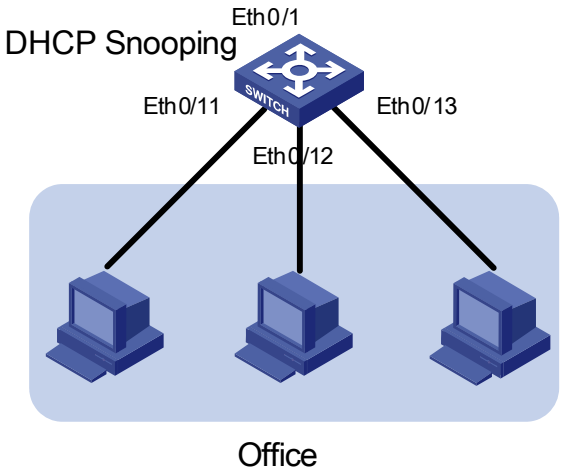


图2-5 DHCP Snooping 组网

启动 DHCP Snooping 功能，并配置 DHCP-Snooping 支持 Option 82 功能。（S3552 设备在开启 Option82 功能的同时，需要同时开启 DHCP 报文重定向功能）

```
<Snooping> system-view
[Snooping] dhcp-snooping
[Snooping] dhcp-snooping information enable
[Snooping] dhcp-packet redirect Ethernet 0/11 to 0/13
```

5. 配置 HQ DHCP Server。

H3C 系列产品在 DHCP Option82 选项中添加端口编号、VLAN 编号和 Snooping/Relay 设备 MAC 地址。一条完整的 Option82 信息由两个子选项的数值组合构成：

Circuit ID 子选项，这里主要标识客户端所在的 VLAN 和接入 DHCP-Snooping 设备的端口编号。

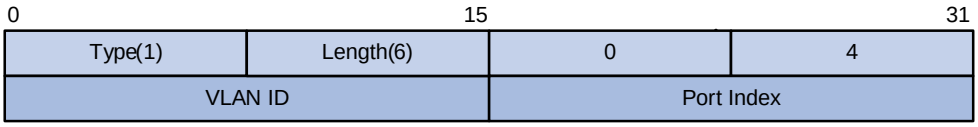


图2-6 Circuit ID 子选项报文结构

例如，由端口 Ethernet0/11 接入的客户端，增加了 Option82 信息的 DHCP 报文中 Circuit ID 子选项信息应为：0x0106000400010010，其中 01060004 为固定取值，0001 标识接入的端口所在 VLAN 为 VLAN1，0010 为端口的绝对编号，比实际端口编号小 1，即实际连接端口为 Ethernet0/11。

Remote ID 子选项，这里主要标识客户端接入的 DHCP-Snooping 设备的 MAC 地址。

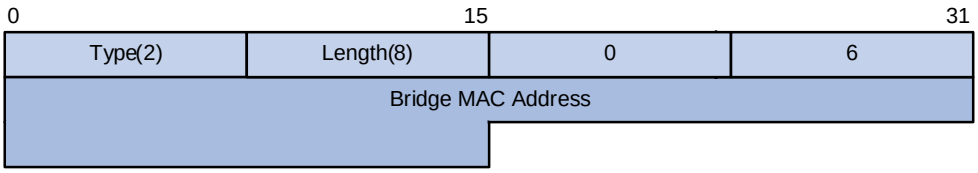


图2-7 Remote ID 子选项报文结构

例如，由 MAC 地址为 000f-e234-bc66 的 DHCP-Snooping 设备接入的 DHCP 客户端，增加了 Option82 信息的 DHCP 报文中 Remote ID 子选项信息应为：02080006000fe234bc66，其中 02080006 为固定取值，000fe234bc66 为 DHCP-Snooping 设备的 MAC 地址。

本举例中只需根据端口编号进行 IP 地址的分配，因此，在 DHCP Server 上只需对 Circuit ID 子选项中标识端口编号的字段进行匹配即可。

📖 **说明：**

下面列举的是 Cisco Catalyst 3745 设备上的配置，对应的软件版本为 IOS 12.3(11)T2 版本，如果使用其他型号或其他版本的设备，请参考随机资料中的用户手册进行操作。

配置 DHCP Server 功能，并配置使用 Option82 信息进行地址分配。

```
Switch> enable
Switch(config)# configure terminal
Enter Configuration commands, one per line. End with CNTL/Z.
Switch(config)# service dhcp
Switch(config)# ip dhcp use class
```

为从 Snooping 设备的 Ethernet0/11 端口接入的客户端建立 DHCP 分类，并配置匹配的 Option82 信息为 Circuit ID 子选中的端口编号，无需匹配的内容可以使用通配符“*”代替。

```
Switch(config)# ip dhcp class office1
Switch(dhcp-class)# relay agent information hex 0106000400010010*
Swtich(dhcp-class)# exit
```

为从 Snooping 设备的 Etherent0/12 端口接入的客户端配置分类和匹配信息，方法与上面命令相似，只将 Option82 信息中的端口标识由 10 改为 11。

```
Switch(config)# ip dhcp class office2
Switch(dhcp-class)# relay agent information hex 0106000400010011*
```

创建 Office 地址池，并为两个 DHCP 分类分别指定地址范围。

```
Switch(config)# ip dhcp pool office
Switch(dhcp-pool)# network 192.168.10.0
Switch(dhcp-pool)# class office1
Switch(dhcp-pool-class)# address range 192.168.10.2 192.168.10.25
Switch(dhcp-pool-class)# exit
Switch(dhcp-pool)# class office2
Switch(dhcp-pool-class)# address range 192.168.10.100 192.168.10.150
Switch(dhcp-pool-class)# exit
```

为 DHCP 地址池配置租约期限，网关、DNS 和 WINS 服务器地址。

```
Switch(dhcp-pool)# lease 0 12
Switch(dhcp-pool)# default-router 192.168.10.1
Switch(dhcp-pool)# dns-server 192.168.100.2
Switch(dhcp-pool)# netbios-name-server 192.168.100.3
```

经过上述配置后，DHCP 服务器即可为 Office 区域的设备自动分配 IP 地址及网关、DNS、WINS 服务器地址。

2.3 注意事项

2.3.1 DHCP Relay 与 IRF 的配合

- 在 IRF（Intelligent Resilient Framework，可扩展弹性网络）系统中，DHCP Relay 同时运行在 Fabric 系统内的所有 Unit 上，但只有运行在 Master 上的 DHCP Relay 能够收发报文，完成全部 DHCP Relay 的功能，而运行在 Slave 上的 DHCP Relay 只是作为运行在 Master 上的任务的备份。
- DHCP 协议是基于 UDP 的应用层协议,作为 Slave 的 Unit 收到 DHCP 请求报文后，UDP-Helper 会将报文重定向到 Master Unit 上，由 Master 上的 DHCP Relay 响应此请求并将需要备份的信息实时发送到各个 Slave Unit 上。这样当 Master Unit 出现故障时，由 Slave 变为 Master 的 Unit 能够马上承担起 DHCP Relay 的角色。因此，在 IRF 系统中使用 DHCP Server/Relay 时，一定要注意先使能 UDP-Helper 功能。

第3章 相关资料

3.1 相关协议和标准

- RFC2131：Dynamic Host Configuration Protocol
- RFC2132：DHCP Options and BOOTP Vendor Extensions
- RFC3046：DHCP Relay Agent Information Option

目 录

QACL 典型配置举例

关键词：ACL，QoS

摘 要：本文主要介绍以太网交换机的QACL功能在具体组网中的应用配置，根据用户不同的需求，分别介绍基于时间段的ACL、流量监管、优先级重标记、队列调度、流量统计、端口重定向、本地流镜像以及WEB Cache重定向的功能及应用。

缩略语：ACL（Access Control List，访问控制列表）、QoS（Quality of Service，服务质量）

第1章 QACL 功能介绍

1.1 支持能力

1.1.1 H3C 系列产品支持的 ACL/QoS 功能列表

表1-1 H3C 系列产品支持的 ACL/QoS 功能列表

产品型号 / 功能	S3600-EI	S3600-SI	S5600	S5100-EI	S5100-SI	S3100-SI	E352/E328	E126
基本 ACL	●	●	●	●	●	●	●	●
高级 ACL	●	●	●	●	●	●	●	●
二层 ACL	●	●	●	●	-	-	●	-
用户自定义 ACL	●	●	●	-	-	-	●	-
ACL 被上层软件引用	●	●	●	●	●	●	●	●
ACL 下发到硬件	●	●	●	●	-	-	●	-
流分类	●	●	●	●	-	-	●	-
优先级重标记	●	●	●	●	-	-	●	-
端口限速	●	●	●	-	●	●	●	●
流量监管	●	●	●	●	-	-	●	-
流量整形	-	-	-	●	-	-	-	-
端口重定向	●	●	●	●	-	-	●	-
队列调度	●	●	●	●	●	●	●	●
拥塞避免	●	●	-	-	-	-	●	-
本地流镜像	●	●	●	●	-	-	●	-
流量统计	●	●	●	●	-	-	●	-
WEB Cache 重定向	●	-	-	-	-	-	-	-

说明：

有关各款交换机支持的 ACL/QoS 功能的详细介绍，请参见各产品的操作手册。

1.2 ACL/QoS 配置指南

说明：

- 不同型号的设备，配置的方法会有差异，这里以 H3C S3600 系列以太网交换机为例。其它型号交换机的配置请参见产品的用户手册。
- 下文只列出了基本的配置步骤，有关各个功能的基本原理和作用，请参见各产品的操作、命令手册。

表1-2 系统视图下的 ACL/QoS 配置

配置	命令	说明
创建 ACL 并进入相应视图	**acl number** *acl-number* [**match-order** { **config** | **auto** }]	缺省情况下，匹配顺序为 **config** 二层 ACL 及用户自定义 ACL 不支持 **match-order** 参数
定义 ACL 规则	**rule** [*rule-id*] { **permit** | **deny** } *rule-string*	对于不同类型的 ACL，*rule-string* 的内容不同，具体请参见产品的命令手册
系统视图下配置队列调度算法	**queue-scheduler** { **strict-priority** | **wfq** *queue0-width queue1-width queue2-width queue3-width queue4-width queue5-width queue6-width queue7-width* | **wrr** *queue0-weight queue1-weight queue2-weight queue3-weight queue4-weight queue5-weight queue6-weight queue7-weight* }	• 在 WRR 或 WFQ 方式中，如果某一个或多个队列的权值或最小带宽设为 0，则对这个或这些队列实行严格优先级调度算法 • 缺省情况下，端口所有输出队列采用 WRR 队列调度方法，缺省权重为：1:2:3:4:5:9:13:15 • 在系统视图下用 **queue-scheduler** 命令定义的队列调度算法会在设备的所有端口上生效
拥塞避免配置	**wred** *queue-index qstart probability*	-

表1-3 端口视图下的 ACL/QoS 配置

配置	命令	说明
在端口上应用 ACL	**packet-filter** { **inbound** | **outbound** } *acl-rule*	-

配置	命令	说明
设置交换机信任报文的优先级	**priority trust**	用户可以通过配置实现交换机信任报文自身携带的优先级，而不使用接收端口的优先级来替换报文的优先级
基于端口的速率限制配置	**line-rate** { **inbound** | **outbound** } *target-rate*	速率限制的粒度为 64Kbps，如果用户输入的数字在 N*64～(N+1)*64 之间（N 为自然数），交换机自动将该参数取值为(N+1)*64
引用 ACL 进行流识别，为匹配的报文重新指定优先级	**traffic-priority** { **inbound** | **outbound** } *acl-rule* { { **dscp** *dscp-value* | **ip-precedence** { *pre-value* | **from-cos** } } | **cos** { *pre-value* | **from-ipprec** } | **local-precedence** *pre-value* }*	用户可以重标记报文的 IP 优先级、802.1p 优先级、DSCP 优先级和本地队列的优先级
基于流的流量监管配置	**traffic-limit inbound** *acl-rule target-rate* [**exceed** *action*]	**exceed** *action*：设定报文流量超过设定流量时设备对超过部分的报文采取的动作，有如下动作： ● **drop**：丢弃报文 ● **remark-dscp** *value*：重新设置报文的 DSCP 优先级，同时转发报文
端口视图下配置队列调度算法	**queue-scheduler** { **wfq** *queue0-width queue1-width queue2-width queue3-width queue4-width queue5-width queue6-width queue7-width* | **wrr** *queue0-weight queue1-weight queue2-weight queue3-weight queue4-weight queue5-weight queue6-weight queue7-weight* }	● 在以太网端口视图下用 **queue-scheduler** 命令定义的队列调度算法只在当前端口生效 ● 如果全局定义的 WRR(或 WFQ)队列调度算法中各队列的权值(或带宽值)不能满足某一端口的需求，用户可在此端口视图下修改其队列权值(或带宽值) ● 在此端口上，新定义的队列权值(或带宽值)会覆盖全局定义的队列权值(或带宽值) ● 在端口视图下定义的队列权值(或带宽值)不能用 **display queue-scheduler** 命令来显示
重定向配置	**traffic-redirect** { **inbound** | **outbound** } *acl-rule* { **cpu** | **interface** *interface-type interface-number* }	当报文被重定向到 CPU 后，将不能正常转发
引用 ACL 进行流识别，对匹配的报文进行流量统计	**traffic-statistic inbound** *acl-rule*	-

第2章 QACL 典型配置举例

2.1 网络环境简介

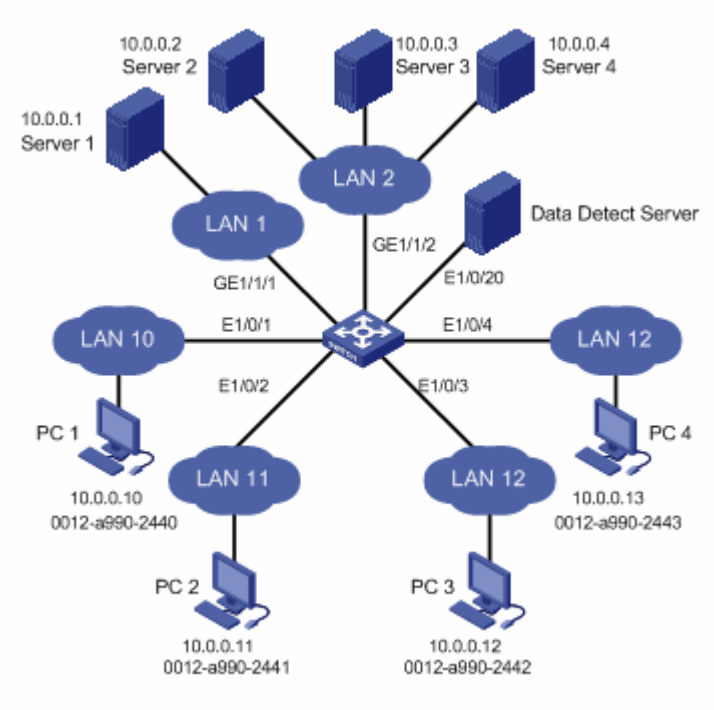


图2-1 网络拓扑图

图 2-1为某公司的网络拓扑图，具体环境如下：

- S3600 交换机作为公司的中心交换机，软件版本为 Release 1510；
- 公司内部通过服务器 Server1 访问 Internet，Server1 通过端口 GigabitEthernet1/1/1 接入交换机；
- Server2、Server3、Server4 分别为公司内部的数据服务器、邮件服务器、文件服务器，通过端口 GigabitEthernet1/1/2 接入交换机；
- Data Detect Server 为公司的数据检测设备，通过端口 Ethernet1/0/20 接入交换机；
- PC1、PC2、PC3、PC4 为公司的客户端，分别通过端口 Ethernet1/0/1、Ethernet1/0/2、Ethernet1/0/3、Ethernet1/0/4 接入交换机。

2.2 基于时间段的 ACL+端口带宽限制+流量监管配置举例

2.2.1 组网需求

公司通过服务器 Server1 访问 Internet，具体需求如下：

- 在工作日的 8:30 到 18:00 限制客户端通过 HTTP 方式访问 Internet，在其它时段可以访问，访问 Internet 的最大流量为 100M；
- 限制 PC 1 发出 IP 优先级为 7 的报文的速率为 20M，将速率超过 20M 的此类报文的 DSCP 优先级修改为 ef；
- 限制 PC 2 发出的 CoS 优先级为 5 的报文的速率为 10M，将速率超过 10M 的此类报文丢弃。

2.2.2 组网图

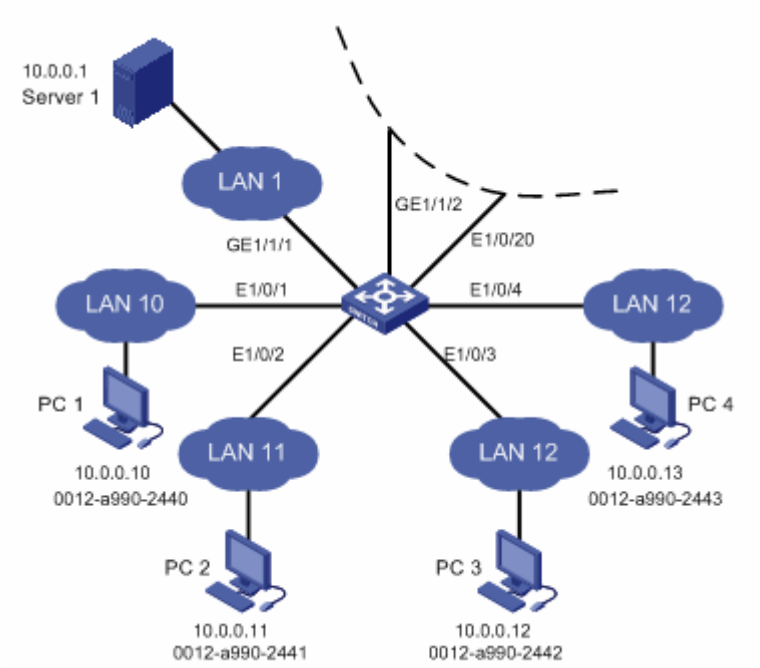


图2-2 配置基于时间段的 ACL+端口带宽限制+流量监管组网图

2.2.3 配置步骤

配置工作日时间段。

```
<H3C> system-view
System View: return to User View with Ctrl+Z.
[H3C] time-range a001 8:30 to 18:00 working-day
```

配置非工作日时间段。

```
[H3C] time-range a002 00:00 to 8:30 working-day
[H3C] time-range a002 18:00 to 24:00 working-day
[H3C] time-range a002 00:00 to 24:00 off-day
```

定义 ACL 3010，禁止客户端在工作日时间段内通过 HTTP 方式访问 Internet；对在非工作时间段内 PC 1 访问 Internet 的 IP 优先级为 7 的报文进行分类标识。

```
[H3C] acl number 3010
[H3C-acl-adv-3010] rule 0 deny tcp destination 10.0.0.1 0 destination-port eq 80 time-range a001
[H3C-acl-adv-3010] rule 1 permit ip source 10.0.0.10 0 precedence 7 time-range a002
[H3C-acl-adv-3010] quit
```

定义 ACL 4010，对在非工作时间段内 PC 2 访问 Internet 的 CoS 优先级为 5 的报文进行分类标识。

```
[H3C] acl number 4010
[H3C-acl-ethernetframe-4010] rule 0 permit cos 5 source 0012-0990-2241 ffff-ffff-ffff time-range a002
[H3C-acl-ethernetframe-4010] quit
```

在连接 Server1 的端口 GigabitEthernet1/1/1 上应用 ACL 3010 的 rule 0 规则，并且限制客户端访问 Internet 的最大流量为 100M。

```
[H3C] interface GigabitEthernet 1/1/1
[H3C-GigabitEthernet1/1/1] packet-filter outbound ip-group 3010 rule 0
[H3C-GigabitEthernet1/1/1] line-rate outbound 102400
[H3C-GigabitEthernet1/1/1] quit
```

在连接 PC 1 的端口 Ethernet1/0/1 上对 ACL 3010 的 rule 1 标识的报文进行流量监管，限制流量为 20M，并将超出流量的报文的 DSCP 优先级修改为 ef。

```
[H3C] interface Ethernet 1/0/1
[H3C-Ethernet1/0/1] traffic-limit inbound ip-group 3010 rule 1 20480 exceed remark-dscp ef
[H3C-Ethernet1/0/1] quit
```

在连接 PC 2 的端口 Ethernet1/0/2 上对 ACL 4010 的 rule 0 标识的报文进行流量监管，限制流量为 10M，并将超出流量的报文丢弃。

```
[H3C] interface Ethernet 1/0/2
[H3C-Ethernet1/0/2] traffic-limit inbound link-group 4010 rule 0 10240 exceed drop
```

需要注意的是，在使用 **traffic-limit** 命令对报文进行流量监管时，仅对 ACL 中动作为 **permit** 的规则有效。

2.3 优先级重新标记+队列调度算法+拥塞避免+报文优先级信任配置举例

2.3.1 组网需求

Server2、Server3、Server4 分别为公司内部的数据服务器、邮件服务器、文件服务器，具体需求如下：

- 要求交换机优先处理访问数据服务器的报文，其次处理访问邮件服务器的报文，最后处理访问文件服务器的报文；
- 配置端口 GigabitEthernet1/1/2 采用 WRR 队列优先级算法，各出队列的权重分别为 1:1:1:5:1:10:1:15；
- 配置端口 GigabitEthernet1/1/2 上索引值为 4 的队列使用 WRED，当该队列的长度超过 64 个报文时，对后续报文进行随机丢弃，丢弃概率为 20%；
- 配置端口 Ethernet1/0/3 信任报文自己的优先级，不使用端口的优先级替换报文的优先级。

2.3.2 组网图

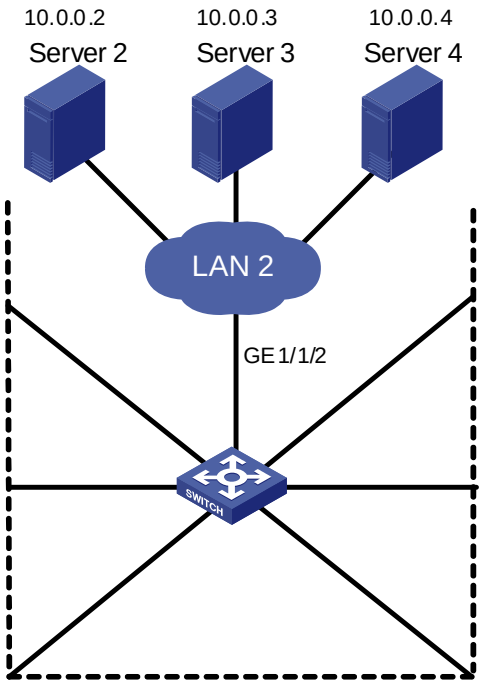


图2-3 配置优先级重新标记+队列调度算法+拥塞避免+报文优先级信任组网图

2.3.3 配置步骤

定义 ACL 3020，根据不同的目的 IP 地址对报文进行分类标识。

```
<H3C> system-view
System View: return to User View with Ctrl+Z.
[H3C] acl number 3020
[H3C-acl-adv-3020] rule 0 permit ip destination 10.0.0.2 0
[H3C-acl-adv-3020] rule 1 permit ip destination 10.0.0.3 0
[H3C-acl-adv-3020] rule 2 permit ip destination 10.0.0.4 0
[H3C-acl-adv-3020] quit
```

在端口 GigabitEthernet1/1/2 上对匹配 ACL 3020 内规则的报文进行优先级重标记。

```
[H3C] interface GigabitEthernet 1/1/2
[H3C-GigabitEthernet1/1/2] traffic-priority outbound ip-group 3020 rule 0 local-precedence 7
[H3C-GigabitEthernet1/1/2] traffic-priority outbound ip-group 3020 rule 1 local-precedence 5
[H3C-GigabitEthernet1/1/2] traffic-priority outbound ip-group 3020 rule 2 local-precedence 3
```

在端口 GigabitEthernet1/1/2 上配置 WRR 队列调度算法，出队列权重为 1:1:1:5:1:10:1:15。

```
[H3C-GigabitEthernet1/1/2] queue-scheduler wrr 1 1 1 5 1 10 1 15
```

为端口 GigabitEthernet1/1/2 上索引值为 4 的队列配置 WRED，当该队列的长度超过 64 个报文时，对后续报文进行随机丢弃，丢弃概率为 20%。

```
[H3C-GigabitEthernet1/1/2] wred 4 64 20
[H3C-GigabitEthernet1/1/2] quit
```

在连接 PC 3 的端口 Ethernet1/0/3 上配置该端口信任报文自己带有的 802.1p 优先级。

```
[H3C] interface Ethernet 1/0/3
[H3C-Ethernet1/0/3] priority trust
```

需要注意的是，在使用 **traffic-priority** 命令对报文进行优先级重标记时，仅对 ACL 中动作为 **permit** 的规则有效。

2.4 流量统计+端口重定向配置举例

2.4.1 组网需求

Data Detect Server 为数据检测设备，通过端口 Ethernet1/0/20 接入交换机，具体需求如下：

- 统计在非工作日时间段内通过端口 Ethernet1/0/1 的以 HTTP 方式访问 Internet 的流量；
- 将工作日时间段内通过端口 Ethernet1/0/1 的以 HTTP 方式访问 Internet 的流量全部重定向到端口 Ethernet1/0/20。

2.4.2 组网图

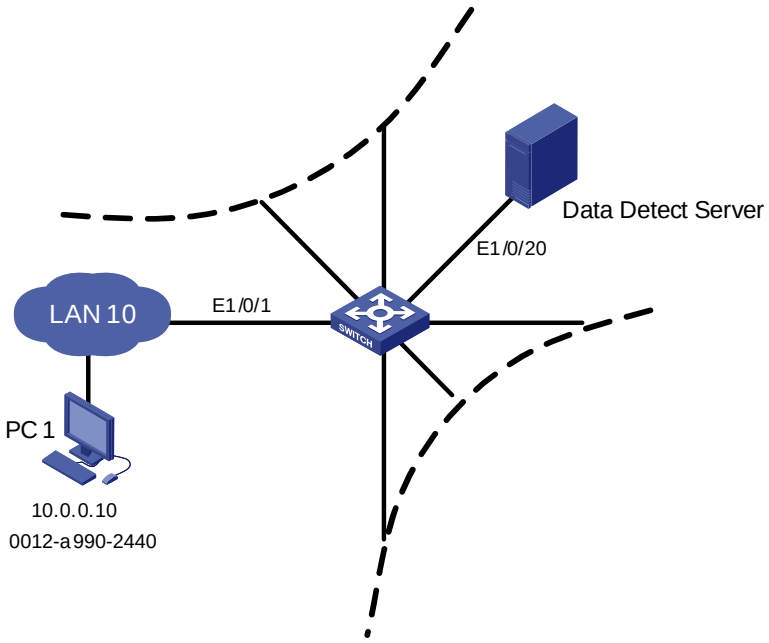


图2-4 配置流量统计+端口重定向组网图

2.4.3 配置步骤

配置工作日时间段。

```
<H3C> system-view
System View: return to User View with Ctrl+Z.
[H3C] time-range a001 8:30 to 18:00 working-day
```

配置非工作日时间段。

```
[H3C] time-range a002 00:00 to 8:30 working-day
[H3C] time-range a002 18:00 to 24:00 working-day
[H3C] time-range a002 00:00 to 24:00 off-day
```

定义 ACL 3030，根据不同的时间段对通过 HTTP 方式访问 Internet 的报文进行分类。

```
[H3C] acl number 3030
[H3C-acl-adv-3030] rule 0 permit tcp destination 10.0.0.1 0 destination-port
eq 80 time-range a001
[H3C-acl-adv-3030] rule 1 permit tcp destination 10.0.0.1 0 destination-port
```

```
eq 80 time-range a002
```

在端口 Ethernet1/0/1 上配置流量重定向，将工作时间段内通过 HTTP 方式访问 Internet 的流量全部重定向到端口 Ethernet1/0/20。

```
[H3C] interface Ethernet 1/0/1
[H3C-Ethernet1/0/1] traffic-redirect inbound ip 3030 rule 0 interface Ethernet 1/0/20
```

在端口 Ethernet1/0/1 上对非工作时间段内通过 HTTP 方式访问 Internet 的流量进行统计。

```
[H3C-Ethernet1/0/1] traffic-statistic inbound ip-group 3030 rule 1
```

需要注意的是，在使用 **traffic-redirect** 和 **traffic-statistic** 命令进行流量重定向和流量统计时，仅对 ACL 中动作为 **permit** 的规则有效。

2.5 本地流镜像配置举例

2.5.1 组网需求

Data Detect Server 为数据检测设备，通过端口 Ethernet1/0/20 接入交换机，要求将工作日时间段内通过端口 Ethernet1/0/1 与 Ethernet1/0/2 的以 HTTP 方式访问 Internet 的报文全部镜像到端口 Ethernet1/0/20，然后使用数据检测设备分析这些报文。

2.5.2 组网图

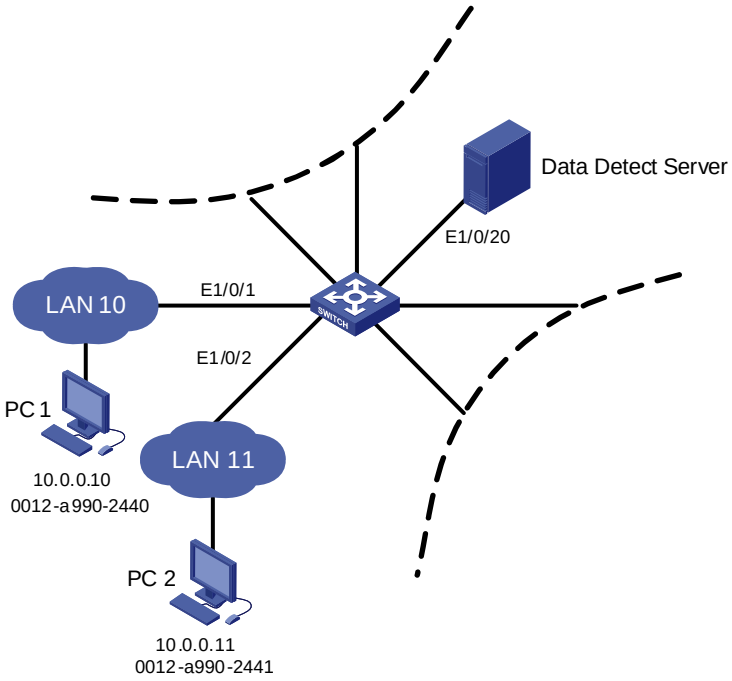


图2-5 配置流镜像组网图

2.5.3 配置步骤

配置工作日时间段。

```
<H3C> system-view
System View: return to User View with Ctrl+Z.
[H3C] time-range a001 8:30 to 18:00 working-day
```

定义 ACL 3030，对工作日时间段内通过 HTTP 方式访问 Internet 的报文进行分类。

```
[H3C] acl number 3030
[H3C-acl-adv-3030] rule 0 permit tcp destination 10.0.0.1 0 destination-port
eq 80 time-range a001
[H3C-acl-adv-3030] quit
```

将端口 Ethernet1/0/20 配置为镜像目的端口。

```
[H3C] interface Ethernet 1/0/20
[H3C-Ethernet1/0/20] monitor-port
[H3C-Ethernet1/0/20] quit
```

在端口 Ethernet1/0/1 和 Ethernet1/0/2 上配置流镜像，通过 ACL 3010 进行流识别，将匹配该 ACL 的报文镜像到目的端口 Ethernet1/0/20。

```
[H3C] interface Ethernet 1/0/1
[H3C-Ethernet1/0/1] mirrored-to inbound ip-group 3010 rule 0
monitor-interface
```

```
[H3C-Ethernet1/0/1] quit
[H3C] interface Ethernet 1/0/2
[H3C-Ethernet1/0/2] mirrored-to inbound ip-group 3010 rule 0
monitor-interface
```

需要注意的是，在使用 **mirrored-to** 命令进行流镜像时，仅对 ACL 中动作为 **permit** 的规则有效。

2.6 配置注意事项

配置中请注意如下事项：

(1) 在端口上下发 ACL 规则时，此时一条 ACL 中多个规则的匹配顺序是由交换机的硬件决定的，S3600 系列以太网交换机的匹配顺序为先下发后生效。用户即使在定义 ACL 时配置了匹配顺序，该匹配顺序也不起作用。

(2) 每个端口支持 8 个出队列，队列 7 到队列 0 优先级依次降低。当端口采用 SP+WRR 队列调度算法时，设备会按照严格优先级优先调度权值为 0 的队列，当队列中没有报文发送时，才会对剩余的队列进行 WRR 调度；当端口采用 SP+WFQ 队列调度算法时，设备会按照严格优先级优先调度带宽为 0 的队列，当队列中没有报文发送时，才会对剩余的队列进行 WFQ 调度。

(3) 设备上可以配置多个镜像源端口，但只能配置一个镜像目的端口。建议镜像目的端口只用于转发镜像流量，不要作为业务端口使用，否则可能会影响正常业务。

(4) 如下命令只能匹配动作为 **permit** 的 ACL 规则：**traffic-limit**，**traffic-priority**、**traffic-redirect**、**mirrored-to**。

(5) 对于高级 ACL 中 TCP/UDP 端口号的匹配：只支持配置操作符为 **eq**。

(6) 对于二层 ACL，不支持配置 *format-type*（包括 802.3/802.2、802.3、ether_ii、snap）参数。

(7) 重定向的报文无论出端口是否 tagged，报文都会带上 tag。

(8) 配置用户自定义 ACL 时，偏移量长度的设置需要考虑如下情况：

- 如果没有开启 VLAN-VPN 功能，交换机内部处理的报文都带有 1 层 VLAN tag，1 层 VLAN tag 占 4 个字节。
- 如果某一端口上开启了 VLAN-VPN 功能，交换机内部处理的报文都带有 2 层 VLAN tag，2 层 VLAN tag 占 8 个字节。

常用协议类型号以及偏移量如下表所示。

表2-1 常用协议类型号以及偏移量

协议类型	协议号	没有使能 VLAN VPN 功能时的偏移量	使能 VLAN VPN 功能后的偏移量
ARP	0x0806	16	20
RARP	0x8035	16	20
IP	0x0800	16	20
IPX	0x8137	16	20
AppleTalk	0x809B	16	20
ICMP	0x01	27	31
IGMP	0x02	27	31
TCP	0x06	27	31
UDP	0x17	27	31

2.7 引用 ACL 规则的其它功能

其它引用 ACL 规则的功能包括：

- Telnet/SNMP/WEB 登录用户控制，其中 Telnet 用户可引用 ACL 2000～4999，SNMP/WEB 用户可引用的 ACL 2000～2999；
- 路由策略匹配规则中引用 ACL，可以引用 ACL 2000～3999；
- 路由信息过滤中引用 ACL，可以引用 ACL 2000～3999；
- 显示匹配 ACL 规则的路由表项，可以引用 ACL 2000～3999；
- 显示匹配 ACL 规则的 FIB 表项，可以引用 ACL 2000～3999；
- TFTP 客户端连接 TFTP 服务器引用 ACL 规则，可以引用 ACL 2000～3999。

引用系统 ACL 规则的功能包括：

- 802.1x 功能 (全局及端口使能后 802.1x 下发 ACL 规则)；
- 集群功能 (缺省使能，在所有端口下发 ACL 规则)，其中 ACL 3998 与 3999 是系统为集群管理预留的编号，用户无法配置；
- DHCP Snooping (使能后在所有端口下发 ACL 规则)；
- 端口隔离 (配置且存在虚接口时下发 ACL 规则)；
- MAC + IP 端口绑定 (在端口上配置绑定策略后下发 ACL 规则)；
- 灵活 QinQ (在端口配置灵活 QinQ 后，根据用户配置的范围下发 ACL 规则)；
- Voice VLAN (在端口使能 Voice VLAN 并存在 OUIMAC 时添加 ACL 规则)。

第3章 WEB Cache 重定向典型配置举例

📖 **说明：**

目前仅 S3600-EI 系列以太网交换机支持 WEB Cache 重定向功能。

3.1 WEB Cache 重定向典型配置举例

3.1.1 组网需求

某公司的网络拓扑如图 3-1所示，具体环境如下：

- S3600 交换机作为公司的中心交换机，软件版本为 Release 1510；
- 市场部门通过端口 Ethernet1/0/1 接入交换机，属于 VLAN 10，网段为 192.168.1.1/24；
- 研发部门通过端口 Ethernet1/0/2 接入交换机，属于 VLAN 20，网段为 192.168.2.1/24；
- 管理部门通过端口 Ethernet1/0/3 接入交换机，属于 VLAN 30，网段为 192.168.3.1/24；
- WEB Cache Server 通过端口 Ethernet1/0/4 接入交换机，属于 VLAN 40，网段为 192.168.4.1/24。WEB Cache Server 的 IP 地址为 192.168.4.2，MAC 地址为 0012-0990-2250。

要求启动交换机的 WEB Cache 重定向功能，将市场部门、研发部门和管理部门的 HTTP 报文全部重定向到 WEB Cache Server，减少广域网连接链路的压力，同时提高获取因特网信息的速度。

3.1.2 组网图

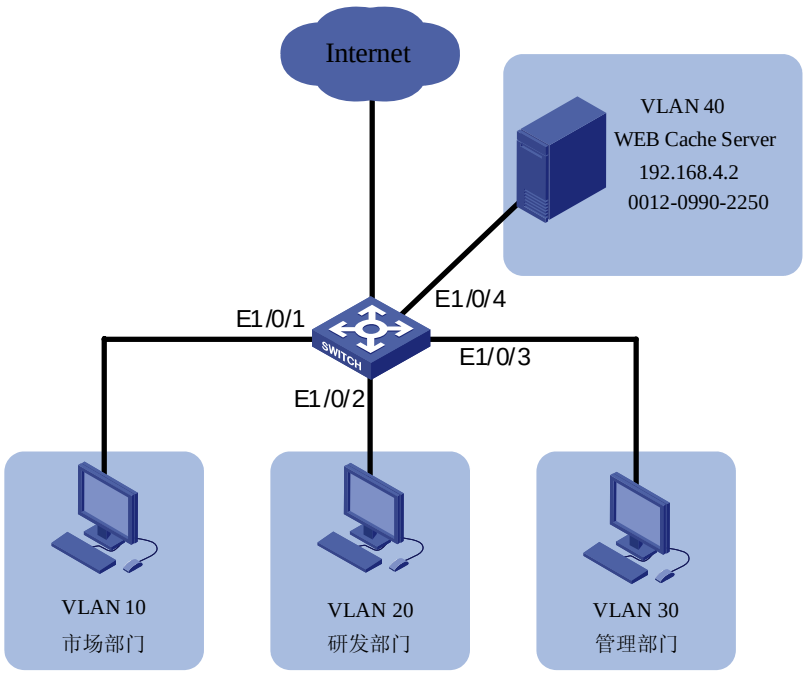


图3-1 配置 WEB Cache 重定向组网图

3.1.3 配置步骤

创建市场部门所属的 VLAN 10，配置 VLAN 10 接口的 IP 地址为 192.168.1.1。

```
<H3C> system-view
System View: return to User View with Ctrl+Z.
[H3C] vlan 10
[H3C-vlan10] port Ethernet 1/0/1
[H3C-vlan10] quit
[H3C] interface Vlan-interface 10
[H3C-Vlan-interface10] ip address 192.168.1.1 24
[H3C-Vlan-interface10] quit
```

创建研发部门所属的 VLAN 20，配置 VLAN 20 接口的 IP 地址为 192.168.2.1。

```
[H3C] vlan 20
[H3C-vlan20] port Ethernet 1/0/2
[H3C-vlan20] quit
[H3C] interface Vlan-interface 20
[H3C-Vlan-interface20] ip address 192.168.2.1 24
[H3C-Vlan-interface20] quit
```

创建管理部门所属的 VLAN 30，配置 VLAN 30 接口的 IP 地址为 192.168.3.1。

```
[H3C] vlan 30
[H3C-vlan30] port Ethernet 1/0/3
```

```
[H3C-vlan30] quit
[H3C] interface Vlan-interface 30
[H3C-Vlan-interface30] ip address 192.168.3.1 24
[H3C-Vlan-interface30] quit
```

创建 WEB Cache Server 所属的 VLAN 40，配置 VLAN 40 接口的 IP 地址为 192.168.4.1。

```
[H3C] vlan 40
[H3C-vlan40] port Ethernet 1/0/4
[H3C-vlan30] quit
[H3C] interface Vlan-interface 40
[H3C-Vlan-interface40] ip address 192.168.4.1 24
[H3C-Vlan-interface40] quit
```

配置 WEB Cache 重定向功能，将 VLAN 10、VLAN 20 和 VLAN 30 接收到的 HTTP 报文全部重定向到 WEB Cache Server。

```
[H3C] webcache address 192.168.4.2 mac 0012-0990-2250 vlan 40 port Ethernet
1/0/4
[H3C] webcache redirect-vlan 10
[H3C] webcache redirect-vlan 20
[H3C] webcache redirect-vlan 30
```

需要注意的是，本例中 WEB Cache Server 所属的 VLAN 40 的接口和参与 WEB Cache 重定向的 VLAN 10、VLAN 20 和 VLAN 30 的接口必须处于 UP 状态，否则 WEB Cache 重定向功能不会生效。

目 录

802.1x 典型配置举例

关键词：802.1x，AAA

摘　要：本文主要介绍以太网交换机的802.1x功能在具体组网中的应用配置，对所涉及到的802.1x客户端、交换机、AAA服务器等角色，分别给出了详细的配置步骤。

缩略语：AAA（Authentication，Authorization and Accounting，认证、授权和计费）

第1章 802.1x 功能介绍

📖 **说明：**

本章中的 802.1x 功能适用于 H3C S3600、H3C S5600、H3C S3100、H3C S5100、H3C S3100-52P、E352&E328、E126 和 E152 这一系列以太网交换机。

1.1 802.1x 简介

IEEE 802 协议定义的局域网不提供接入认证，一般来说，只要用户接入局域网就可以访问网络上的设备或资源。但是对于如电信接入、写字楼、局域网以及移动办公等应用场合，网络管理者希望能对用户设备的接入进行控制和配置，为此产生了基于端口或用户的网络接入控制需求。

802.1x 协议是一种基于端口的网络接入控制（Port Based Network Access Control）协议。802.1x 作为一种基于端口的用户访问控制机制，由于其低成本、良好的业务连续性和扩充性以及较高的安全性和灵活性，受到了设备制造商、各大网络运营商和最终用户的广泛支持和肯定。

1.2 产品特性支持情况

1.2.1 全局配置

- 开启全局的 802.1x 特性
- 设置时间参数
- 设置认证请求帧的最大可重复发送次数
- 打开静默定时器功能
- 打开设备重启用户再认证功能

1.2.2 端口视图下的配置

- 开启端口 dot1x
- 配置 Guest VLAN 功能
- 配置端口允许的最大用户数
- 端口接入控制方式(基于端口或基于 MAC)
- 端口接入控制模式（强制授权、非强制授权、自动）

- 客户端版本检测
- 代理检测

1.2.3 注意事项

- 只有全局开启 dot1x 特性后，dot1x 的配置才会生效。
- 在启用 dot1x 功能前，可以配置设备或以太网端口的 dot1x 相关参数，但这些配置并不生效；启用 dot1x 功能后，提前配置的 dot1x 相关参数将生效。
- 关闭 dot1x 功能后，交换机上配置的 dot1x 相关参数仍被保留；当 dot1x 功能重新启动后，以前所做的这些 dot1x 相关配置依然生效。

第2章 配置命令介绍

2.1 802.1x 相关功能配置命令

要实现 802.1x 功能，需要对接入用户、交换机、认证/授权服务器三个部分进行正确配置。

- 接入用户端：保证用户 PC 使用正确的客户端。
- 交换机：需要进行 802.1x 配置和 AAA 相关配置。
- 认证/授权服务器：需要进行正确的配置。

下面仅介绍交换机上所需的 802.1x 相关配置命令，其他配置请参见相关设备手册。

表2-1 802.1x 相关功能配置命令

功能	命令	说明
开启全局的 802.1x 特性	**dot1x**	必选 缺省情况下，全局的 802.1x 特性为关闭状态
开启端口的 802.1x 特性	系统视图下 **dot1x** [**interface** *interface-list*] 端口视图下 **dot1x**	必选 缺省情况下，端口的 802.1x 特性均为关闭状态，只有端口和全局 802.1x 特性均开启，802.1x 的相应配置才能生效
设置端口接入控制方式	**dot1x port-method** { **macbased** | **portbased** } [**interface** *interface-list*]	可选 缺省情况下，802.1x 在端口上进行接入控制方式为 **macbased**。 使用 Guest VLAN 功能时必须保持 **portbased** 的接入控制方式
开启 Guest VLAN 功能	**dot1x guest-vlan** *vlan-id* [**interface** *interface-list*]	可选 缺省情况下，Guest VLAN 功能处于关闭状态。配置为 Guest VLAN 的 *vlan-id* 必需事先已经创建

第3章 典型企业网络接入认证应用

📖 **说明：**

不同型号的设备，配置的细节或显示信息会稍有差异，这里以 H3C S3600 系列交换机（软件版本为 Release 1510）为例。

3.1 网络应用分析

某企业网的管理者希望在交换机各端口上对用户接入进行认证，以控制用户对相应资源的访问，详细网络应用需求分析如表 3-1所示。

表3-1 网络应用分析

网络需求	相关设备所需配置
接入用户受控，必须通过认证才能访问网络	启动 802.1x 特性
用户未通过认证时，只能受限访问网络 VLAN 10	启用 Guest VLAN 功能。
用户通过认证后，可以访问网络 VLAN 100	动态 VLAN 下发配置
计费方式为 50 元包月，其访问网络的带宽为 2M	在 RADIUS Server 上设置计费策略、带宽限制策略
用户上线后将 IP 与 Mac 进行绑定	MAC+IP 绑定功能设置
在线闲置 20 分钟后，服务器强制切断用户连接	启用闲置用户切断功能
设备无预警重启后，在线用户可以重新认证并成功	配置设备重启用户再认证功能

3.2 组网图

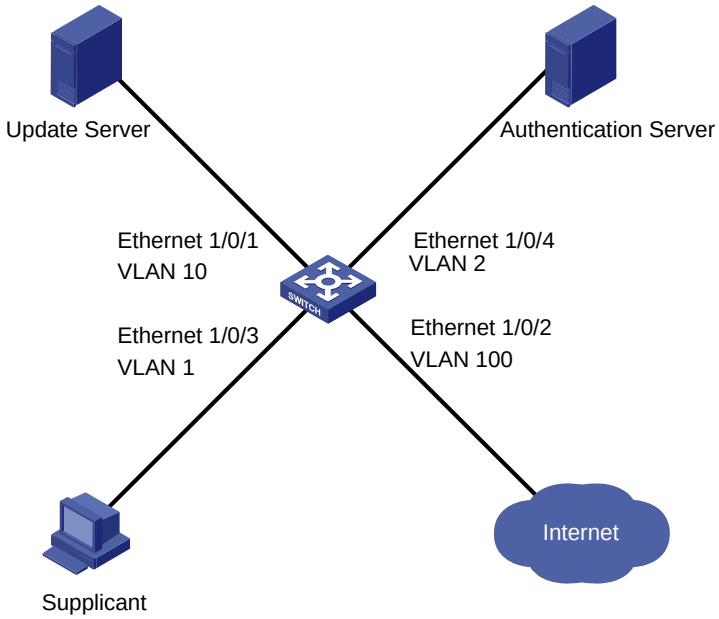


图3-1 典型企业网应用组网图

3.3 配置步骤

3.3.1 交换机上的配置

设置 RADIUS 方案 cams，设置主备服务器。

```
<H3C> system-view
[H3C] radius scheme cams
[H3C-radius-cams] primary authentication 192.168.1.19
[H3C-radius-cams] primary accounting 192.168.1.19
[H3C-radius-cams] secondary authentication 192.168.1.20
[H3C-radius-cams] secondary accounting 192.168.1.20
```

设置系统与认证 Radius 服务器交互报文时加密密码为 expert，与计费 Radius 服务器交互报文的加密密码为 expert。

```
[H3C-radius-cams] key authentication expert
[H3C-radius-cams] key accounting expert
```

#设置用户名为带域名格式。

```
[H3C-radius-cams] user-name-format with-domain
```

#服务类型为 extended。

```
[H3C-radius-cams] server-type extended
```

配置设备重启用户再认证功能。

```
[H3C-radius-cams] accounting-on enable
```

定义 ISP 域 abc，并配置认证采用 RADIUS 方案 cams。

```
[H3C] domain abc
[H3C-isp-abc] radius-scheme cams
[H3C-isp-abc] quit
```

将 ISP 域 abc 设置为缺省 ISP 域。

```
[H3C] domain default enable abc
```

动态 VLAN 下发模式

```
[H3C-isp-abc] vlan-assignment-mode integer
```

用户接入端口启用 Guest VLAN 功能

```
[H3C] vlan 10
[H3C-Ethernet1/0/3] dot1x port-method portbased
[H3C-Ehternet1/0/3] dot1x guest-vlan 10
```

启用 802.1x

```
[H3C] dot1x
```

端口视图下启用 dot1x

```
[H3C-Ethernet1/0/3] dot1x
```

使用 display 命令可以查看关于 802.1x，AAA 相关参数配置。

```
[H3C] display dot1x interface ethernet1/0/3
Global 802.1x protocol is enabled
 CHAP authentication is enabled
 DHCP-launch is disabled
 Proxy trap checker is disabled
 Proxy logoff checker is disabled

 Configuration: Transmit Period     30 s,  Handshake Period       15 s
                ReAuth Period     3600 s,  ReAuth MaxTimes        2
                Quiet Period        60 s,  Quiet Period Timer is disabled
                Supp Timeout        30 s,  Server Timeout         100 s
                Interval between version requests is 30s
                Maximal request times for version information is 3
                The maximal retransmitting times          2

 Total maximum 802.1x user resource number is 1024
 Total current used 802.1x resource number is 0

 Ethernet1/0/3  is link-up
```

```
    802.1x protocol is enabled
    Proxy trap checker is disabled
    Proxy logoff checker is disabled
    Version-Check is disabled
    The port is an authenticator
    Authentication Mode is Auto
    Port Control Type is Port-based
    ReAuthenticate is disabled
    Max number of on-line users is 256

    Authentication Success: 0, Failed: 0
    EAPOL Packets: Tx 0, Rx 0
    Sent EAP Request/Identity Packets : 0
         EAP Request/Challenge Packets: 0
    Received EAPOL Start Packets : 0
             EAPOL LogOff Packets: 0
             EAP Response/Identity Packets : 0
             EAP Response/Challenge Packets: 0
             Error Packets: 0

    Controlled User(s) amount to 0

[H3C] display radius scheme cams
SchemeName  =cams                           Index=1    Type=extended
Primary Auth IP  =192.168.1.19     Port=1812
Primary Acct IP  =192.168.1.19     Port=1813
Second  Auth IP  =192.168.1.20     Port=1812
Second  Acct IP  =192.168.1.20     Port=1813
Auth Server Encryption Key= expert
Acct Server Encryption Key= expert
Accounting method = required
Accounting-On packet enable, send times = 15 , interval = 3s
TimeOutValue(in second)=3 RetryTimes=3 RealtimeACCT(in minute)=12
Permitted send realtime PKT failed counts       =5
Retry sending times of noresponse acct-stop-PKT =500
Quiet-interval(min)                             =5
Username format                                 =with-domain
Data flow unit                                  =Byte
Packet unit                                     =1
unit 1 :
Primary Auth State=active,   Second Auth State=active
Primary Acc  State=active,   Second Acc  State=active
```

```
[H3C] display domain abc
The contents of Domain abc:
   State = Active
   RADIUS Scheme = cams
   Access-limit = Disable
   Vlan-assignment-mode = Integer
   Domain User Template:
   Idle-cut = Disable
   Self-service = Disable
   Messenger Time = Disable
```

3.3.2 RADIUS Server 上的配置（以 CAMS 1.20 标准版为例）

CAMS 认证/授权、计费服务器的配置，主要由以下四个部分组成：创建计费策略、创建服务类型、添加用户信息、接入网段及协议配置。

本文所述 CAMS 综合访问服务器的版本为 V1.20（标准版）。

1. 登陆 CAMS 服务器

(1) 在登陆页面输入正确的用户名、密码登陆 CAMS 服务器

图3-2 CAMS 登陆页面

(2) 登陆成功后页面如图所示：

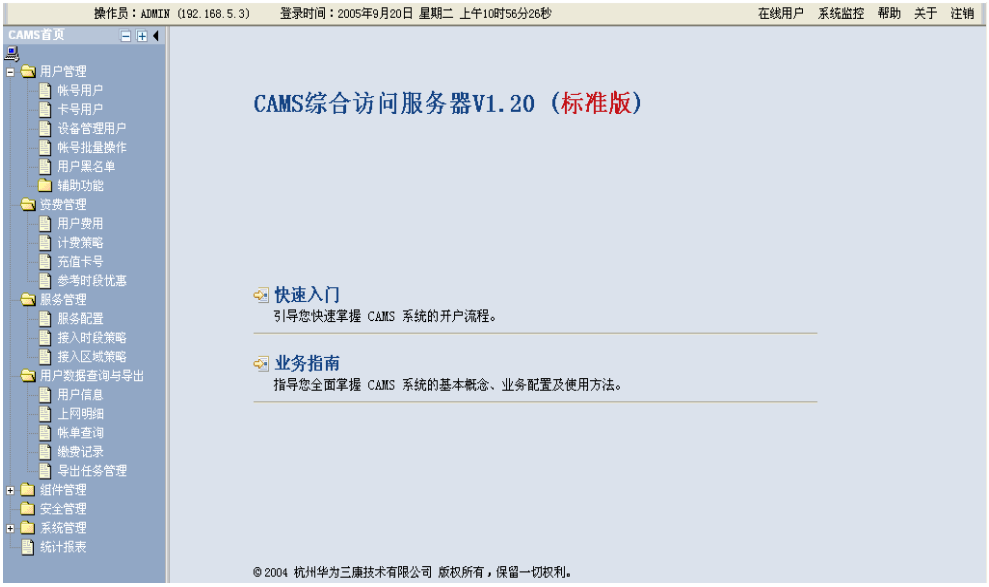


图3-3 CAMS 首页面

2. 创建计费策略

(1) 进入计费策略页面

登录 CAMS 服务器配置平台，点击左侧的“资费管理”下的“计费策略”，进入“计费策略管理”界面，如图所示。

图3-4 计费策略管理页面

从列表中可以看到已有的计费策略，可以选择对已有计费策略进行“查询”、“修改”或“维护”。

(2) 创建计费策略

点击“计费策略管理”界面上方的“增加”按钮：新建“包月计费”的计费策略。

图3-5 计费策略基本信息页面

(3) 点击下一步：选择“按时长计费”，计费周期“月为周期”，周期内固定费用“50 元每月”。

图3-6 计费属性设置页面

点击完成，成功添加新的计费策略“包月计费”。

3. 创建服务类型

(1) 进入服务配置界面

登录 CAMS 服务器配置平台，点击左侧的“服务管理”下的“服务配置”，进入“服务配置”界面，如图所示。

图3-7 服务配置页面

从列表中可以看到已有的服务类型，可以选择对已有服务类型进行“查询”、“修改”或“删除”。

(2) 创建服务类型

点击“服务配置”界面上方的“增加”按钮：新建服务名为“abc”的服务类型，服务后缀名为“abc”。计费策略为“包月计费”，上下行速率限制为 2M（2048Kbps），认证成功后下发 VLAN 100。认证绑定选择绑定用户 IP 和绑定用户 MAC 地址。

图3-8 增加服务页面

点击确定，成功添加服务类型。

4. 添加帐户用户

(1) 进入用户帐户界面

登录 CAMS 服务器配置平台，点击左侧的“用户管理”的“帐号用户”，进入“帐户管理”界面。

图3-9 用户帐户界面

从列表中可以看到已有的帐户用户，可以选择对已有帐户用户进行维护。

(2) 创建用户帐户

选择页面上方“增加”：用户为 info 密码为 info 用户姓名为 Bruce，预付费用户，预付金额 100 元。并添加 绑定的用户 IP 地址、网卡 MAC 地址，在线数量限制为 1，最大闲置时长 20 分钟。

在“服务信息”一栏，选择服务名称 abc。

图3-10 用户开户页面

点击确定完成帐户用户添加。

5. 接入设备配置

(1) 进入系统配置页面

登录 CAMS 服务器配置平台，点击左侧的“系统管理”的“系统配置”，进入“系统配置”界面。

图3-11 系统配置页面

(2) 选择修改“接入设备配置”，修改 接入设备的地址、密钥及认证、计费处理端口等信息。

图3-12 接入设备配置列表页面

6. 接入设备配置

(1) 点击页面下方的“增加”按钮，增加配置项。

图3-13 增加配置项页面

(2) 点击确定后，可以看到如下提示：

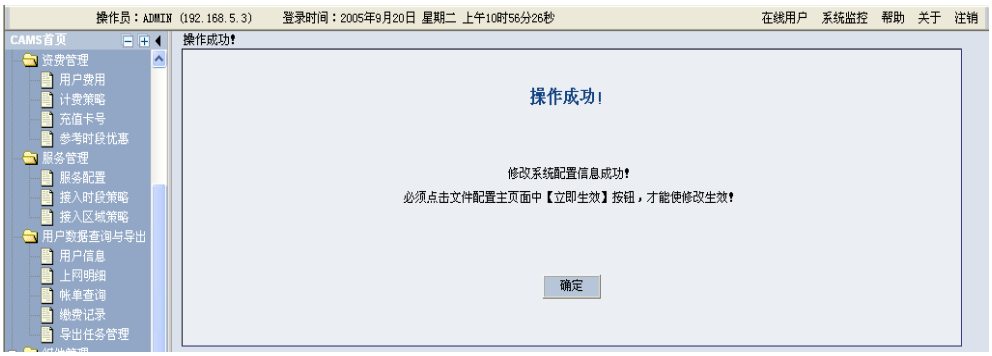


图3-14 操作成功提示

(3) 此时需要返回“系统配置”页面，点击“立即生效”。

图3-15 系统配置页面的立即生效按钮

3.3.3 接入用户 PC 上的操作

PC 上需要安装 802.1x 客户端。客户端可是选择 H3C 公司 802.1X 客户端产品，也可以是 XP 自带客户端，或者其他第三方标准客户端。以下以 H3C 公司 802.1X 客户端为例进行介绍。

1. 启动客户端

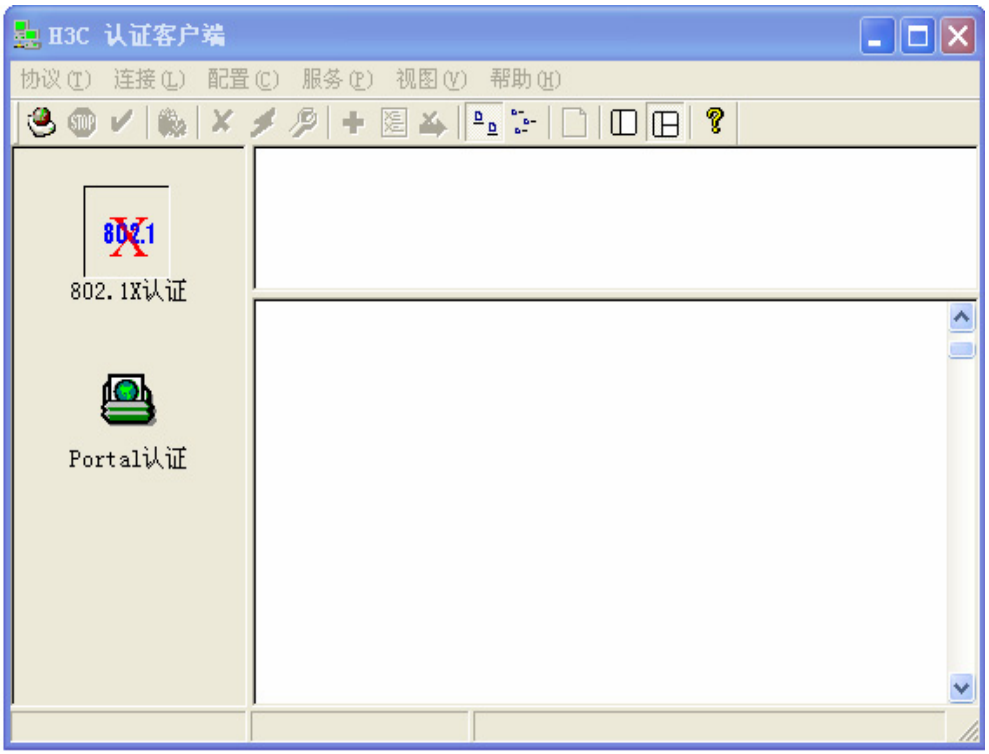


图3-16 客户端页面

2. 新建连接

在 802.1x 认证图标上点击右键：选择创建一个新的连接。

图3-17 新建 802.1x 连接

3. 设置连接属性

点击下一步：

图3-18 设置连接属性

保持默认状态，选择完成。

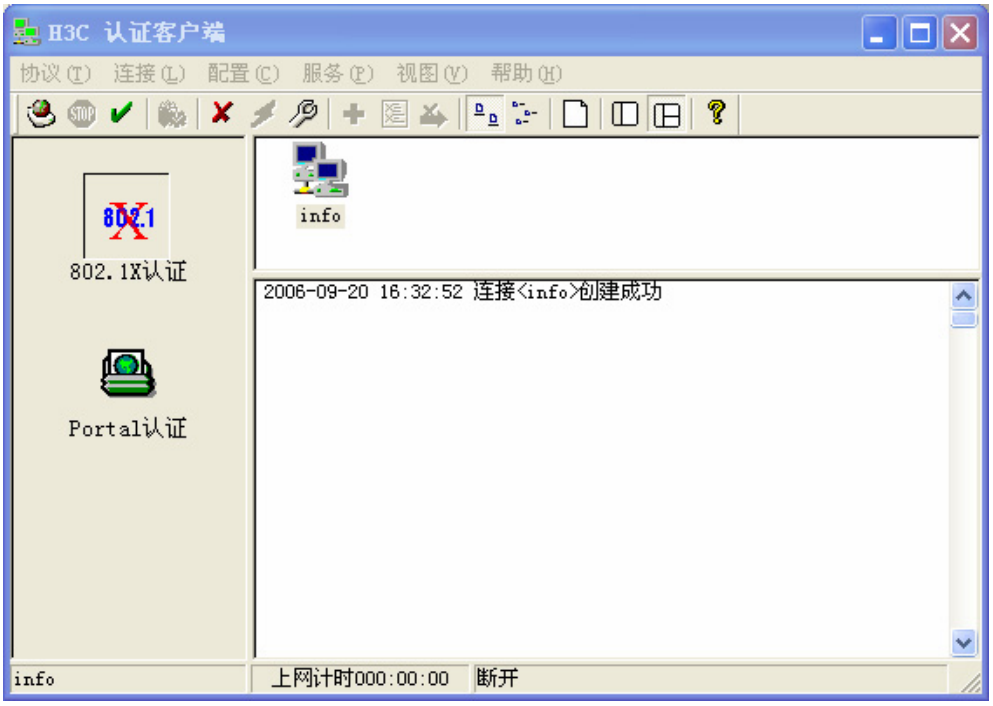


图3-19 连接创建成功

4. 启动连接

双击 info 连接：

图3-20 连接中

连接成功：

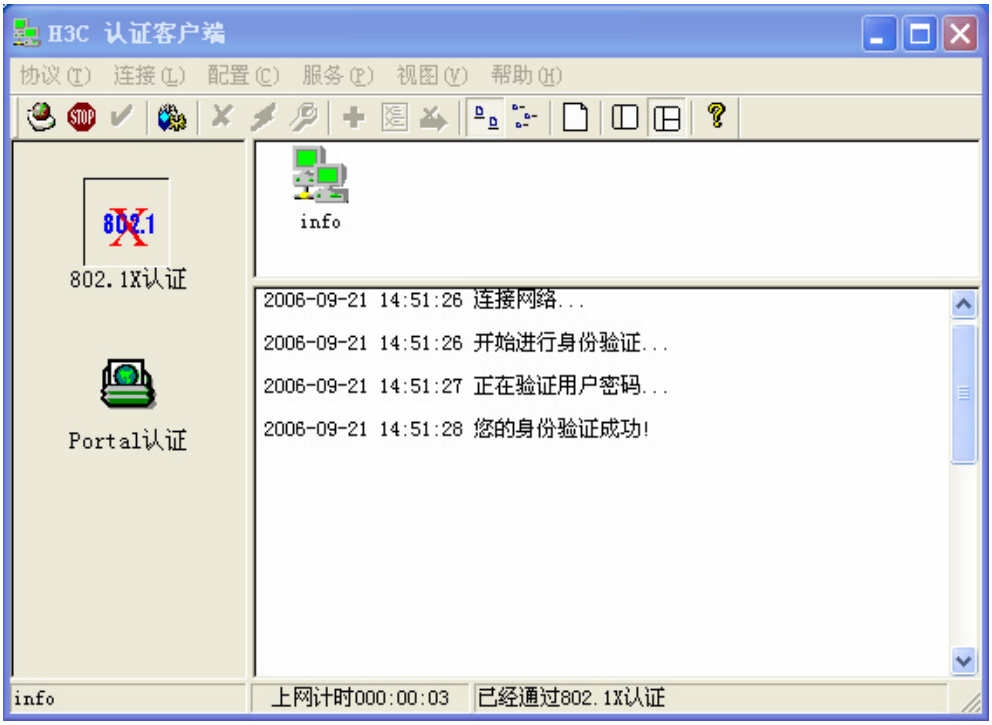


图3-21 认证通过页面

3.3.4 验证结果

可以看到，在用户没有发起认证或认证失败的情形下，可以访问 VLAN10 范围内的网络，证明 Guest VLAN 生效。

当用户使用正确的客户端认证通过时，可以访问 VLAN 100 的网络，证明动态下发的 VLAN 生效，同时与 CAMS 配合完成计费、实时监控。当设备无预警重启时，用户可以重新认证并上线。当用户使用的 IP/MAC 与 CAMS 上设置的不一致时，用户无法上线。

3.3.5 故障诊断与排错

1. 故障现象：客户端无法验证通过

- 使用 display dot1x 命令确认全局和端口上都启用了 802.1x。
- 确认客户端拨号程序设置正确的用户名和验证密码。
- 确认链路是否正常。
- 若上面检查没有问题，可以打开 802.1x 调试开关 debugging dot1x packet 查看交换机收到和发送的 EAP、EAPoL 报文是否正常。

2. 故障现象：用户无需进行 802.1X 验证就能使用网络资源

- 使用 display dot1x 确认全局和端口上都启用了 802.1x。
- 使用 display interface 确认端口是否有入包统计；802.1x 只针对入包进行认证限制，而对于出包来说，并不需要经过认证。即禁止从客户端接收帧，但允许向客户端发送帧。

目 录

SSH 典型配置举例

关键词：SSH，RSA

摘 要：本文主要介绍以太网交换机的SSH功能在具体组网中的应用配置，对所涉及到的SSH客户端、交换机等角色，分别给出了详细的配置步骤。

缩略语：SSH（Secure Shell，安全外壳）、RSA（Rivest Shamir Adleman）

第1章 SSH 功能介绍

1.1 SSH 简介

SSH（Secure Shell，安全外壳）是一个用于在非安全网络中提供安全的远程登录以及其他安全网络服务的协议。当用户通过非安全的网络环境远程登录到交换机时，每次发送数据前，SSH 都会自动对数据进行加密，当数据到达目的地时，SSH 自动对加密数据进行解密，以此提供安全的信息保障，以保护交换机不受诸如明文密码截取等攻击。除此之外，SSH 还提供强大的认证功能，以保护不受诸如“中间人”等攻击方式的攻击。SSH 采用客户端——服务器模式。SSH 服务器接受 SSH 客户端的连接并提供认证，SSH 客户端与 SSH 服务器建立 SSH 连接，从而实现通过 SSH 登录到 SSH 服务器端。

此外，SSH 还支持其他功能，比如可以对传输的数据进行压缩，从而加快传输的速度。又可以代替 Telnet，或为 FTP、Pop 甚至 PPP 提供安全的“通道”。

说明：

有关各款交换机支持的 SSH 功能的详细介绍，请参见各产品的用户手册。

1.2 支持能力

表1-1 H3C 系列低端以太网交换机产品支持的 SSH 功能列表

功能 / 产品型号	SSH Server 功能	SSH Client 功能
S3600-EI	●	●
S3600-SI	●	●
E352&E328	●	●
S5600	●	●
S5100	●	●
S3100	●	●
E126	●	●
S3100-52P	●	●
E152	●	●

1.3 SSH 配置

1.3.1 SSH 服务器端的配置

1. H3C 交换机充当 SSH 服务器时的配置

- 配置所在用户界面支持的协议
- 生成或销毁 RSA 密钥对
- 导出 RSA 密钥
- 创建 SSH 用户并指定认证方式
- 配置 SSH 用户使用的服务类型
- 配置服务器上的 SSH 管理功能
- 在服务器端配置客户端的公钥
- 为 SSH 用户分配公共密钥
- 指定业务报文源 IP 或源接口

2. 其它设备充当 SSH 服务器时的配置

当使用其它设备充当 SSH 服务器时的配置，请参见各产品的相关用户手册。

1.3.2 SSH 客户端配置

1. 采用 SSH 客户端软件的配置

SSH 客户端软件有很多，例如 PuTTY、OpenSSH 等。用户可根据自己的具体情况决定使用的 SSH 客户端软件，具体软件配置请参见软件附带的手册。

2. 采用支持 SSH2 的交换机作为客户端的配置

- 设置对 SSH 服务器是否支持首次认证
- 建立 SSH 客户端和服务器端的连接

1.3.3 注意事项

- 为确保 SSH 用户登录成功，请务必在服务器端配置登录用户界面的认证方式为 **authentication-mode scheme**（采用 AAA 认证）。
- 生成服务器端的 RSA 密钥对是完成 SSH 登录的必要操作。
- 对于新用户，必须指定其认证方式，否则将无法登录。

第2章 配置命令介绍

2.1 SSH 配置命令

要实现 SSH 特性，需要对 SSH 客户端和 SSH 服务器端进行相应的配置。

下面只是介绍交换机上需要的 SSH 相关配置命令，详细配置请参见操作手册。

2.2 H3C 交换机充当 SSH 服务器时的配置

2.2.1 H3C 交换机充当 SSH 服务器时的配置过程

表2-1 H3C 交换机充当 SSH 服务器时的配置过程

<table>
<tr><th>交换机角色</th><th>公共配置</th><th>不同认证方式</th><th colspan="2">配置公钥</th><th>说明</th></tr>
<tr><td rowspan="3">SSH Server</td><td rowspan="3">具体命令请参见2.2.2 1.</td><td>password</td><td colspan="2">-</td><td>具体命令请参见2.2.2 2.</td></tr>
<tr><td rowspan="2">RSA 认证</td><td>手工配置（将客户端公钥文件中的公钥手工写入到服务器端）</td><td rowspan="2">将 SSH 服务器端保存的客户端公钥与 SSH 客户端关联</td><td>具体命令请参见2.2.2 3.</td></tr>
<tr><td>导入配置（将客户端公钥文件中的公钥通过 SSH 服务器命令导入到服务器端）</td><td>具体命令请参见2.2.2 4.</td></tr>
</table>

1. 认证方式配置注意事项

如表 2-1，介绍的只是单独指定**password**认证或RSA认证方式的情况。实际上还可以将这两种认证方式结合使用：

- 使用 **ssh authentication-type default password-publickey** 或 **ssh user authentication-type password-publickey** 命令指定认证方式为 **password** 认证和 RSA 认证，也就是用户必须不但要通过 **password** 认证还要通过 RSA 认证，才能登录。

- 使用 **ssh authentication-type default all** 或 **ssh user authentication-type all** 命令指定该用户的认证方式可以是 **password** 认证，也可以是 RSA 认证，也就是用户只要满足其中任何一种认证方式，即可登录。

2. 公钥配置过程及注意事项

如表 2-1，在服务器端采用RSA认证方式的配置过程中，需要SSH服务器端和SSH客户端的相互配合。

(1) 手工配置 RSA 公钥过程

- 当使用交换机作为客户端时，在客户端通过命令生成 RSA 密钥对后，还需要使用 **display rsa local-key-pair public** 命令显示主机公钥数据。
- 将主机公钥数据手工配置到服务器端，从而使服务器端与该客户端具有相同的公钥，以便后续建立连接时服务器端对客户端进行认证。

(2) 注意事项

当使用某些 SSH 客户端软件（如 Putty 软件）时，在客户端生成 RSA 密钥对后。除了将公钥数据手工配置到服务器端外，还可采用导入配置公钥方式。

(3) RSA 公钥导入过程

- 当使用交换机作为服务器时，使用 SSH 客户端软件生成 RSA 密钥对后，将保存的公钥文件通过 FTP/TFTP 方式上传到服务器端。
- 再将此公钥文件中的公钥通过 SSH 服务器命令导入到服务器端。

2.2.2 SSH 服务器端配置命令

1. 公共配置

表2-2 H3C 交换机充当 SSH 服务器时的公共配置命令

功能	命令	说明
进入系统视图	**system-view**	-
进入单一或多个用户界面视图	**user-interface** [*type-keyword*] *number* [*ending-number*]	-
配置登录用户界面的认证为 scheme 方式	**authentication-mode scheme** [**command-authorization**]	必选 缺省情况下，用户界面认证为 **password** 方式
配置所在用户界面支持的协议	**protocol inbound** { **all** |**ssh** | **telnet** }	可选 缺省情况下，系统支持所有的协议，即支持 Telnet 和 SSH
退出到系统视图	**quit**	-

功能	命令	说明
生成 RSA 密钥对	**rsa local-key-pair create**	必选 缺省情况下，没有生成 RSA 密钥对
销毁 RSA 密钥对	**rsa local-key-pair destroy**	可选 该命令用来销毁已生成的 RSA 密钥对
配置用户可以使用的服务类型	**ssh user** *username* **service-type** { **stelnet** | **sftp** | **all** }	可选 缺省情况下，用户可以使用的的服务类型为 **stelnet**
设置 SSH 认证超时时间	**ssh server timeout** *seconds*	可选 缺省情况下，认证超时时间为 60 秒
设置 SSH 验证重试次数	**ssh server authentication-retries** *times*	可选 缺省情况下，SSH 验证重试次数为 3 次
设置服务器密钥的更新时间	**ssh server rekey-interval** *hours*	可选 缺省情况下，系统不更新服务器密钥
设定服务器端兼容 SSH1.x 版本的客户端	**ssh server compatible-ssh1x enable**	可选 缺省情况下，服务器端兼容 SSH1.x 版本的客户端
为 SSH 服务器端指定源 IP 地址	**ssh-server source-ip** *ip-address*	可选
为 SSH 服务器端指定源接口	**ssh-server source-interface** *interface-type interface-number*	可选

2. SSH 服务器端采用 password 认证时

表2-3 H3C 交换机充当 SSH 服务器采用 password 认证时的配置命令

功能	命令	说明
公共配置请参见“表 2-2 H3C交换机充当SSH服务器时的公共配置命令”		

功能	命令		说明
创建 SSH 用户并指定认证方式	创建 SSH 用户并指定缺省认证方式	**ssh authentication-type default password**	二者必选其一 缺省情况下，系统没有创建 SSH 用户并且没有指定认证方式 当 **ssh authentication-type default** 和 **ssh user authentication-type** 两条命令同时配置，且认证方式不同时，SSH 用户的认证方式以 **ssh user authentication-type** 命令的配置为准
		ssh user *username*	
	创建 SSH 用户并为该用户指定某一认证方式	**ssh user** *username* **authentication-type password**	

3. SSH 服务器端采用手工配置 RSA 公钥认证

表2-4 H3C 交换机充当 SSH 服务器采用手工配置 RSA 公钥认证时的配置命令

功能	命令		说明
公共配置请参见“表 2-2 H3C交换机充当SSH服务器时的公共配置命令”			
创建 SSH 用户并指定认证方式	创建 SSH 用户并指定缺省认证方式	**ssh authentication-type default rsa**	二者必选其一 缺省情况下，系统没有创建 SSH 用户并且没有指定认证方式 当 **ssh authentication-type default** 和 **ssh user authentication-type** 两条命令同时配置，且认证方式不同时，SSH 用户的认证方式以 **ssh user authentication-type** 命令的配置为准
		ssh user *username*	
	创建 SSH 用户并为该用户指定某一认证方式	**ssh user** *username* **authentication-typ rsa**	
进入公共密钥视图	**rsa peer-public-key** *keyname*		必选
进入公共密钥编辑视图	**public-key-code begin**		-
配置客户端的 RSA 公钥	直接输入 RSA 公钥内容		在输入密钥数据时，字符之间可以有空格，也可以按回车键继续输入数据，所配置的公钥必须是按公钥格式编码的十六进制字符串
退出公共密钥编辑视图，退回到公共密钥视图	**public-key-code end**		退出视图时，系统自动保存配置的公钥密钥
退出公共密钥视图，退回到系统视图	**peer-public-key end**		-

功能	命令	说明
为 SSH 用户分配公共密钥	**ssh user** *username* **assign rsa-key** *keyname*	必选 多次分配公钥时，则以最后一次分配的公钥为准

4. SSH 服务器端采用导入配置 RSA 公钥认证

表2-5 H3C 交换机充当 SSH 服务器采用导入配置 RSA 公钥认证时的配置命令

<table>
<tr><th>功能</th><th colspan="2">命令</th><th>说明</th></tr>
<tr><td colspan="4">公共配置请参见“表 2-2 H3C交换机充当SSH服务器时的公共配置命令”</td></tr>
<tr><td rowspan="3">创建 SSH 用户并指定认证方式</td><td rowspan="2">创建 SSH 用户并指定缺省认证方式</td><td>ssh authentication-type default rsa</td><td rowspan="3">二者必选其一
缺省情况下，系统没有创建 SSH 用户并且没有指定认证方式
当 ssh authentication-type default 和 ssh user authentication-type 两条命令同时配置，且认证方式不同时，SSH 用户的认证方式以 ssh user authentication-type 命令的配置为准</td></tr>
<tr><td>ssh user username</td></tr>
<tr><td>创建 SSH 用户并为该用户指定某一认证方式</td><td>ssh user username authentication-type rsa</td></tr>
<tr><td>从公钥文件中导入 SSH 用户的 RSA 公钥</td><td colspan="2">rsa peer-public-key keyname import sshkey filename</td><td>必选</td></tr>
<tr><td>为 SSH 用户分配公钥</td><td colspan="2">ssh user username assign rsa-key keyname</td><td>必选
多次分配公钥时，则以最后一次分配的公钥为准</td></tr>
</table>

2.3 H3C 交换机充当 SSH 客户端时的配置

当设备作为 SSH 客户端和服务器端连接时，可以设置 SSH 客户端对所访问的 SSH 服务器是否支持首次认证。

- 如果设置支持首次认证，则当 SSH 客户端首次访问服务器端，而客户端没有配置服务器端的主机公钥时，用户仍可以选择继续访问该服务器端，并在客户端保存该主机公钥；当用户下次访问该服务器端时，就以所保存的主机公钥来认证该服务器。
- 如果设置不支持首次认证，则当客户端没有配置服务器端的主机公钥时，客户端将拒绝访问该服务器。用户必须事先将要访问的服务器端的主机公钥配置在

本地，同时指定要访问的服务器端的主机公钥名称，以便客户端对要访问的服务器进行认证。

2.3.1 H3C 交换机充当 SSH 客户端时的配置过程

表2-6 H3C 交换机充当 SSH 客户端时的配置过程

<table>
<tr><th>交换机角色</th><th>公共配置</th><th>是否支持首次认证</th><th colspan="2">配置公钥</th><th>访问 SSH 服务器端</th><th>说明</th></tr>
<tr><td rowspan="2">SSH Client</td><td rowspan="2">请参见 2.3.2 1.</td><td>支持</td><td colspan="2">-</td><td rowspan="2">建立 SSH 客户端和服务器端的连接</td><td>请参见 2.3.2 2.</td></tr>
<tr><td>不支持</td><td>手工配置（将服务器端公钥文件中的公钥手工写入到客户端）</td><td>在客户端上指定要连接的服务器端的主机公钥</td><td>请参见 2.3.2 3.</td></tr>
</table>

如表 2-6，在客户端不支持首次认证的配置过程中，需要SSH客户端和SSH服务器端的相互配合。

采用手工配置公钥过程：

- 在服务器端使用 **display rsa local-key-pair public** 命令显示公钥数据。
- 将公钥数据手工配置到客户端，从而使客户端与该服务器端具有相同的公钥，以便后续建立连接时就以保存的服务器的主机公钥来认证该服务器。

2.3.2 SSH 客户端配置命令

1. H3C 交换机充当 SSH 客户端时的公共配置命令

表2-7 H3C 交换机充当 SSH 客户端时的公共配置命令

操作	命令	说明
进入系统视图	**system-view**	-
为 SSH 客户端指定源 IP 地址	**ssh2 source-ip** *ip-address*	可选
为 SSH 客户端指定源接口	**ssh2 source-interface** *interface-type interface-number*	可选

2. 支持首次认证时 SSH 客户端的配置

表2-8 H3C 交换机充当 SSH 客户端支持首次认证时的配置命令

操作	命令	说明
公共配置请参见“2.3.2 1. H3C交换机充当SSH客户端时的公共配置命令”		
进入系统视图	**system-view**	-

操作	命令	说明
设置 SSH 客户端支持首次认证	**ssh client first-time enable**	可选 缺省情况下，客户端支持首次认证
建立 SSH 客户端和服务器端的连接	**ssh2** { *host-ip* | *host-name* } [*port-num*] [**prefer_kex** { **dh_group1** | **dh_exchange_group** } | **prefer_ctos_cipher** { **des** | **aes128** } | **prefer_stoc_cipher** { **des** | **aes128** } | **prefer_ctos_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** } | **prefer_stoc_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }] *	必选 该配置用来启动 SSH 客户端和服务器端建立连接，并指定客户端和服务器端的首选密钥交换算法、首选加密算法和首选 HMAC 算法

3. 不支持首次认证并采用手工配置服务器端公钥时 SSH 客户端的配置

表2-9 H3C 交换机充当 SSH 客户端不支持首次认证并采用手工配置公钥时 SSH 的配置

操作	命令	说明
公共配置请参见“2.3.2 1. H3C交换机充当SSH客户端时的公共配置命令”		
进入系统视图	**system-view**	-
设置 SSH 客户端不支持首次认证	**undo ssh client first-time**	必选 缺省情况下，客户端支持首次认证
进入公共密钥视图	**rsa peer-public-key** *keyname*	必选
进入公共密钥编辑视图	**public-key-code begin**	-
配置服务器端的 RSA 公钥	直接输入 RSA 公钥内容	在输入密钥数据时，字符之间可以有空格，也可以按回车键继续输入数据，所配置的公钥必须是按公钥格式编码的十六进制字符串
退出公共密钥编辑视图，退回到公共密钥视图	**public-key-code end**	退出视图时，系统自动保存配置的公钥密钥
退出公共密钥视图，退回到系统视图	**peer-public-key end**	-
在客户端上指定要连接的服务器端的主机公钥名称	**ssh client** { *server-ip* | *server-name* } **assign rsa-key** *keyname*	可选 当客户端不支持首次认证时，必选 进行该项配置前，需要将服务器端公钥配置到客户端

操作	命令	说明
建立 SSH 客户端和服务器端的连接	**ssh2** { *host-ip* | *host-name* } [*port-num*] [**prefer_kex** { **dh_group1** | **dh_exchange_group** } | **prefer_ctos_cipher** { **des** | **aes128** } | **prefer_stoc_cipher** { **des** | **aes128** } | **prefer_ctos_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** } | **prefer_stoc_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }] *	必选 该配置用来启动 SSH 客户端和服务器端建立连接，并指定客户端和服务器端的首选密钥交换算法、首选加密算法和首选 HMAC 算法

第3章 配置举例

说明：

此典型配置举例中使用的 S3600 系列以太网交换机的版本为 Release 1510。

3.1 SSH 典型配置举例

3.1.1 S3600 交换机充当 SSH 服务器并采用 password 认证时的配置举例

1. 组网需求

当用户通过一个不能保证安全的网络远程登录到交换机时，为更大限度地保证数据信息交换的安全性，使用SSH来实现此目的，并采用password认证。如图 3-1所示，PC终端（SSH Client）上运行支持SSH2.0 的客户端软件，与交换机（SSH Server）建立本地连接。

2. 组网图

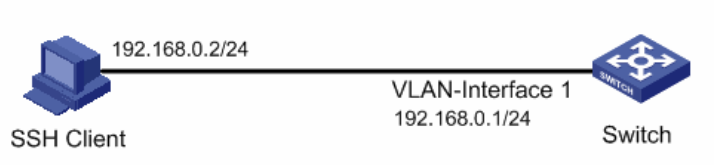


图3-1 SSH Server 采用 password 认证时的配置组网图

3. 配置步骤

- SSH 服务器端配置

在交换机上创建 VLAN 接口，并为其分配 IP 地址，作为客户端连接的 SSH 服务器地址。

```
<H3C> system-view
[H3C] interface vlan-interface 1
[H3C-Vlan-interface1] ip address 192.168.0.1 255.255.255.0
[H3C-Vlan-interface1] quit
```

生成 RSA 密钥对。

```
[H3C] rsa local-key-pair create
```

设置用户接口上的认证模式为 AAA 认证。

```
[H3C] user-interface vty 0 4
```

```
[H3C-ui-vty0-4] authentication-mode scheme
```

设置用户接口上支持 SSH 协议。

```
[H3C-ui-vty0-4] protocol inbound ssh
[H3C-ui-vty0-4] quit
```

创建用户 client001，设置其认证密码为 abc，登录协议为 SSH，能访问的命令级别为 3。

```
[H3C] local-user client001
[H3C-luser-client001] password simple abc
[H3C-luser-client001] service-type ssh level 3
[H3C-luser-client001] quit
```

指定用户 client001 的认证方式为 password 认证

```
[H3C] ssh user client001 authentication-type password
```

- SSH 客户端配置

客户端主机配置 IP 地址

客户端主机的 IP 地址必须同交换机上的 VLAN 接口的 IP 地址位于同一个网段，这里设置为“192.168.0.2”。

建立与 SSH 服务器端的连接

SSH 客户端软件的配置（以 Putty0.58 为例）

(1) 打开 PuTTY.exe 程序，出现如下客户端配置界面。

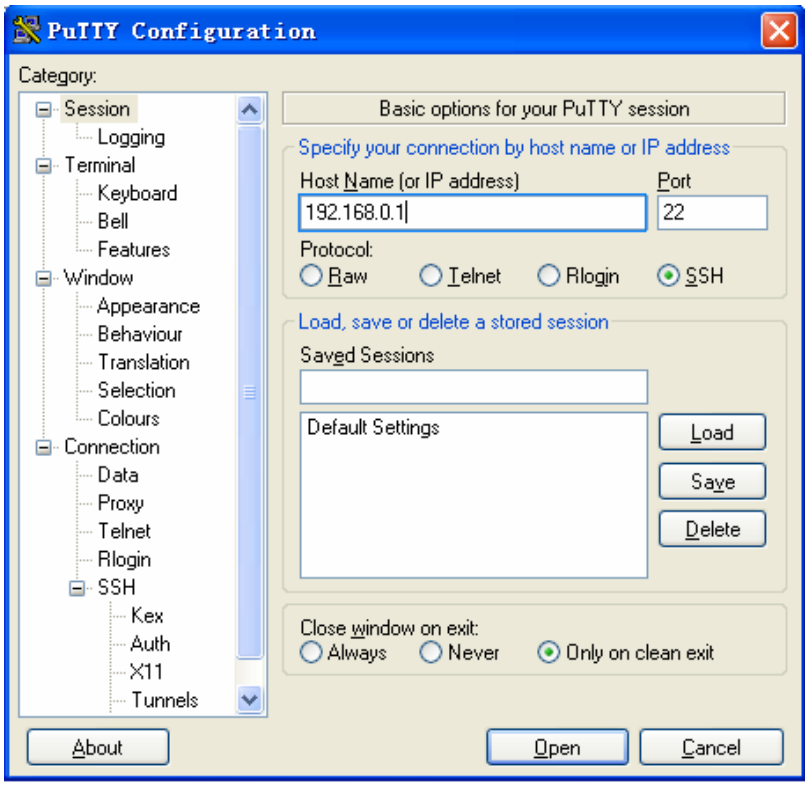


图3-2 SSH 客户端配置界面

在“Host Name（or IP address）”文本框中输入 SSH 服务器的 IP 地址。

(2) 单击SSH客户端配置界面左边目录树（“Category”）中的连接协议（“Connection”）中的“SSH”，出现如图 3-3的界面。

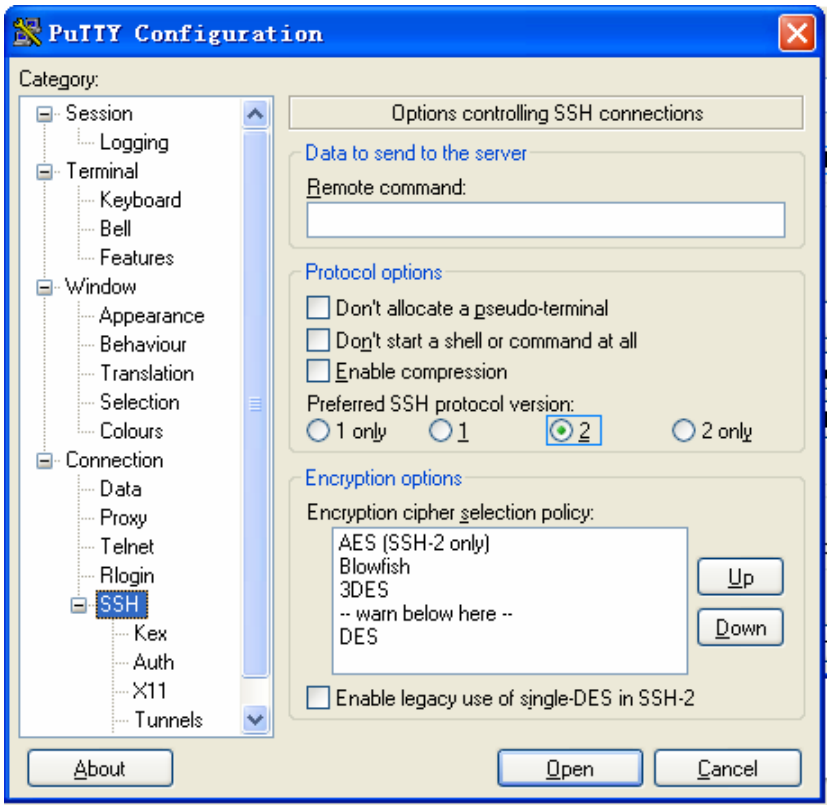


图3-3 SSH 客户端配置界面（2）

在“Protocol options”区域中，选择“Preferred SSH protocol version”参数的值为 2。

(3) 在图 3-4中，单击<Open>按钮，出现如所示的SSH客户端界面，如果连接正常则会提示用户输入用户名client001，密码abc。

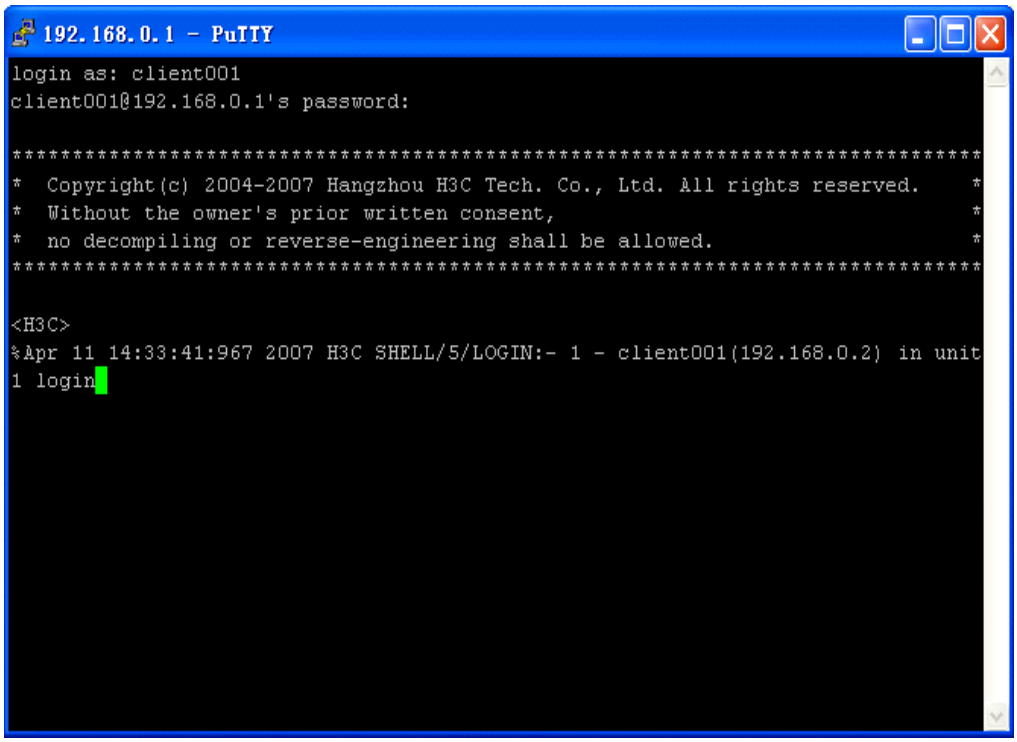


图3-4 SSH 客户端界面

3.1.2 S3600 交换机充当 SSH 服务器并采用 RSA 认证时的配置举例

1. 组网需求

当用户通过一个不能保证安全的网络远程登录到交换机时，为更大限度地保证数据信息交换的安全性，使用SSH来实现此目的，并采用RSA认证。如图 3-5所示，PC 终端（SSH Client）上运行支持SSH2.0 的客户端软件，与交换机（SSH Server）建立本地连接。

2. 组网图

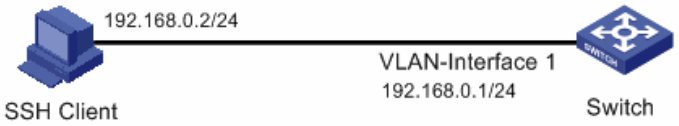


图3-5 SSH Server 采用 RSA 认证时的配置组网图

3. 配置步骤

- SSH 服务器端配置

在交换机上创建 VLAN 接口，并为其分配 IP 地址，作为客户端连接的 SSH 服务器地址。

```
<H3C> system-view
[H3C] interface vlan-interface 1
```

```
[H3C-Vlan-interface1] ip address 192.168.0.1 255.255.255.0
[H3C-Vlan-interface1] quit
```

生成 RSA 密钥对。

```
[H3C] rsa local-key-pair create
```

设置用户接口上的认证模式为 AAA 认证。

```
[H3C] user-interface vty 0 4
[H3C-ui-vty0-4] authentication-mode scheme
```

设置用户接口上支持 SSH 协议。

```
[H3C-ui-vty0-4] protocol inbound ssh
```

设置用户能访问的命令级别为 3。

```
[H3C-ui-vty0-4] user privilege level 3
[H3C-ui-vty0-4] quit
```

创建用户 client001，并指定认证方式为 RSA 认证。

```
[H3C] ssh user client001 authentication-type rsa
```

📖 **说明：**

这里需要先在 SSH 客户端使用 SSH 客户端软件生成 RSA 密钥对，并将生成的 RSA 公钥保存到指定文件中，再将此公钥文件通过 FTP/TFTP 方式上传到服务器端，文件名为 public。有关配置请参见客户端的配置。

在服务器端从文件 public 中导入客户端的公钥，公钥名为 Switch001。

```
[H3C] rsa peer-public-key Switch001 import sshkey public
```

为用户 client001 指定公钥 Switch001。

```
[H3C] ssh user client001 assign rsa-key Switch001
```

- SSH 客户端的配置

生成密钥对（以 PuTTYGen 为例）

(1) 运行 PuTTYGen.exe，选择要生成的密钥对。此处参数栏选择“SSH2(RSA)”，点击<Generate>，产生客户端密钥对。

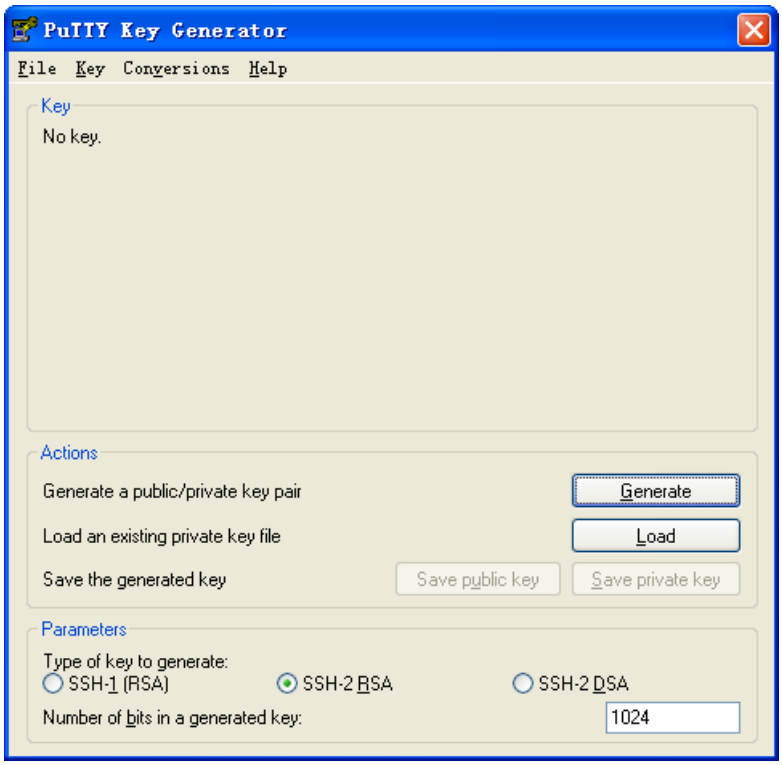


图3-6 生成客户端密钥（1）

📖 注意：

在产生密钥对的过程中需不停的移动鼠标，鼠标移动仅限于下图蓝色框中除绿色标记进程条外的地方，否则进程条的显示会不动，密钥对将停止产生，见图 3-7。

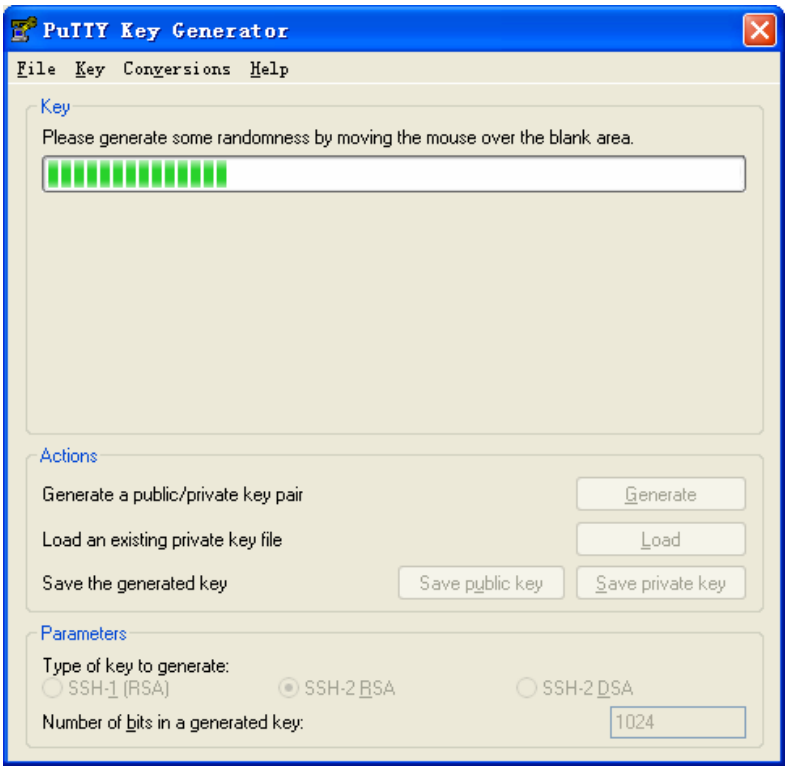


图3-7 生成客户端密钥（2）

密钥对产生后，点击<save public key>，输入存储公钥的文件名 public，点击保存。

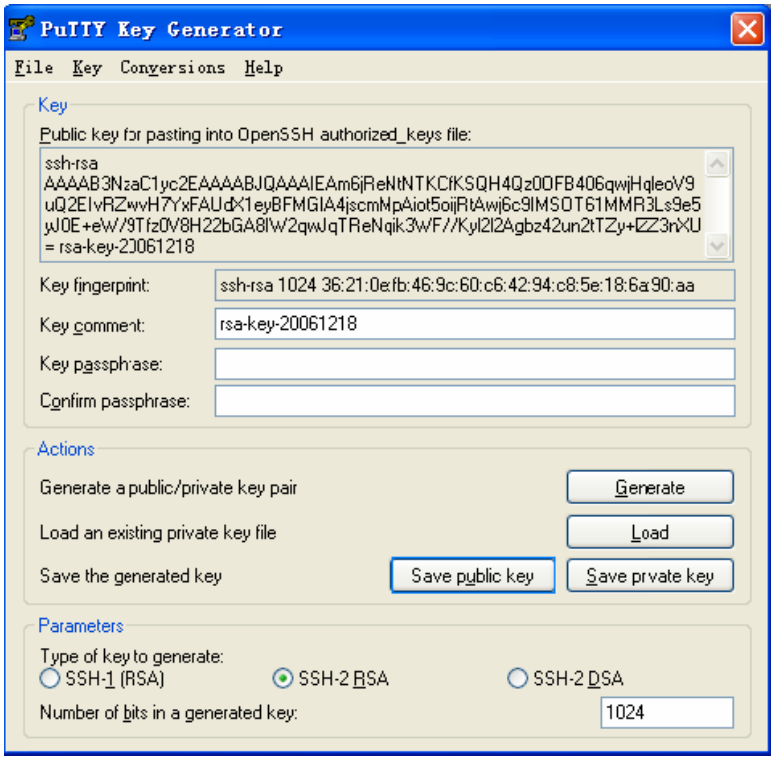


图3-8 生成客户端密钥（3）

同理，点击<save private key>存储私钥，弹出警告框，提醒是否保存没做任何保护措施的私钥，点击<Yes>，输入私钥文件名即可，此处为 private.ppk，点击保存。

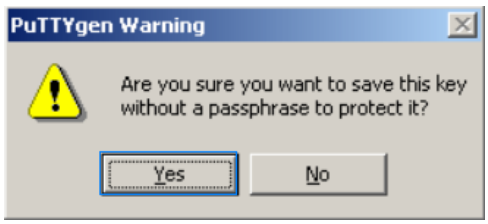


图3-9 生成客户端密钥（4）

🕮 **说明：**

客户端生成密钥对后，需要将保存的公钥文件通过 FTP/TFTP 方式上传到服务器端。这里需要在完成服务器端的配置后才可以继续客户端的配置。

建立与 SSH 服务器端的连接

SSH 客户端软件的配置（以 Putty0.58 为例）

(1) 打开PuTTY.exe程序，出现如图 3-10所示的客户端配置界面。

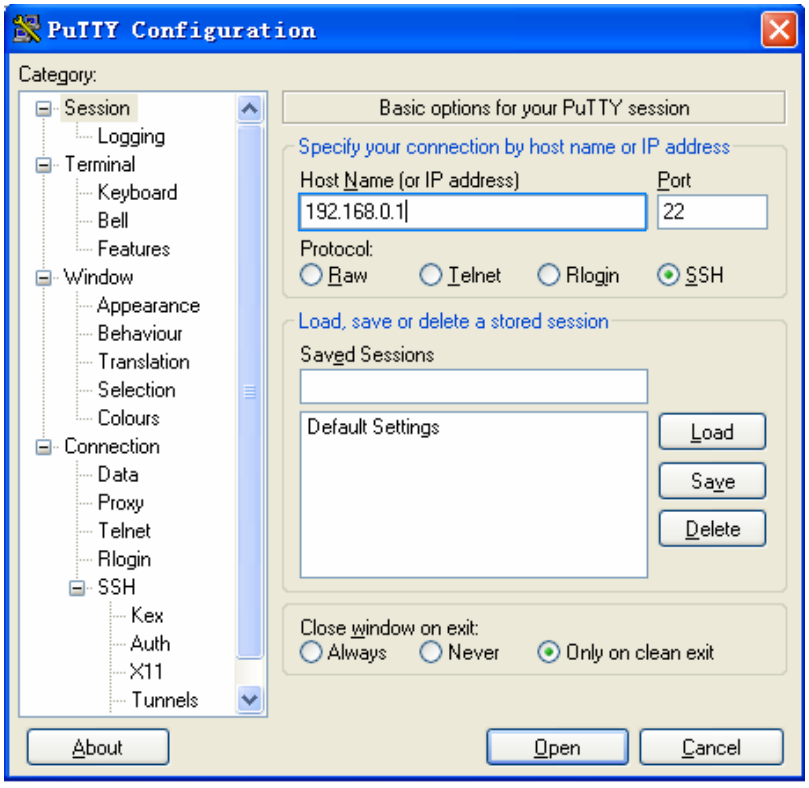


图3-10 SSH 客户端配置界面（1）

在“Host Name（or IP address）”文本框中输入 SSH 服务器的 IP 地址。

(2) 单击SSH客户端配置界面左边目录树（“Category”）中的连接协议（“Connection”）中的“SSH”，出现如图 3-11的界面。

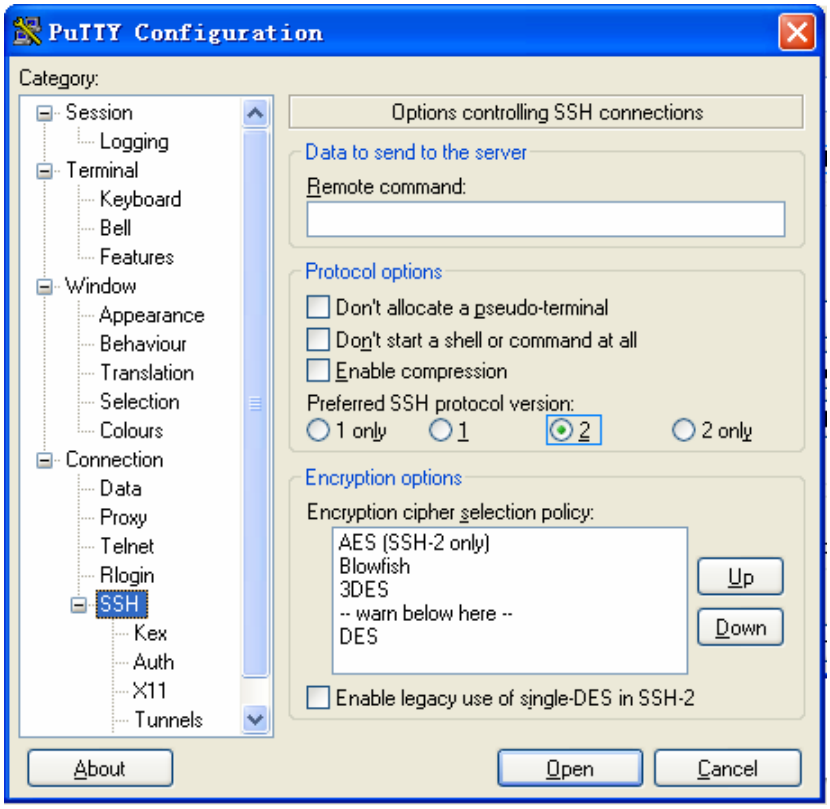


图3-11 SSH 客户端配置界面（2）

在“Protocol options”区域中，选择“Preferred SSH protocol version”参数的值为 2。

(3) 单击“SSH”下面的“Auth”（认证），出现如图 3-12的界面。

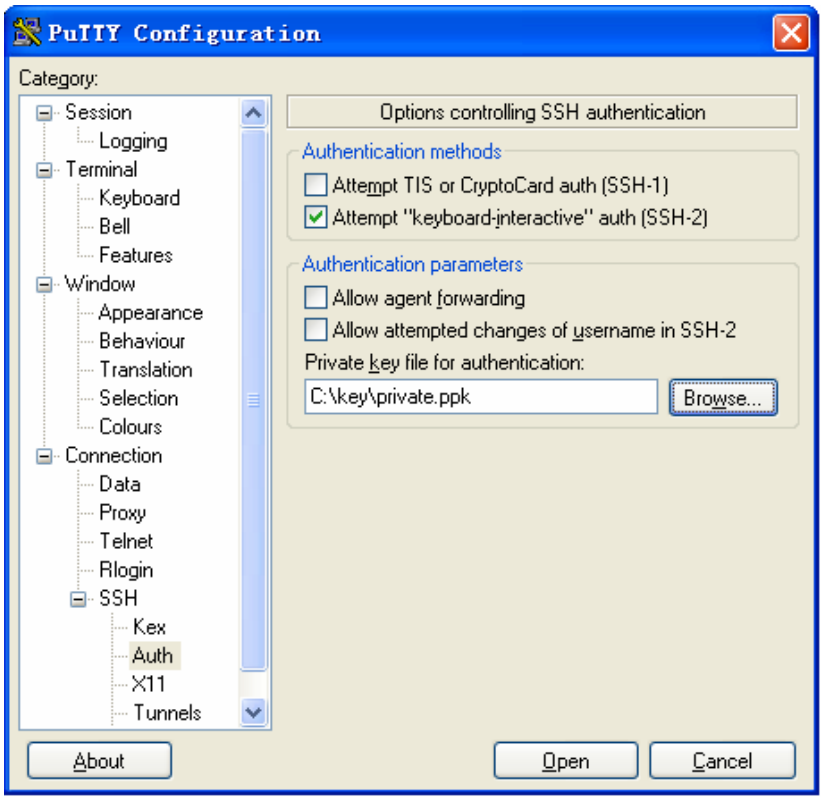


图3-12 SSH 客户端配置界面（2）

单击<Browse…>按钮，弹出文件选择窗口。选择与配置到服务器端的公钥对应的私钥文件，并确定即可。

(4) 如图 3-12，单击<Open>按钮，出现如图 3-13所示的SSH客户端界面，如果连接正常则会提示用户输入用户名client001。

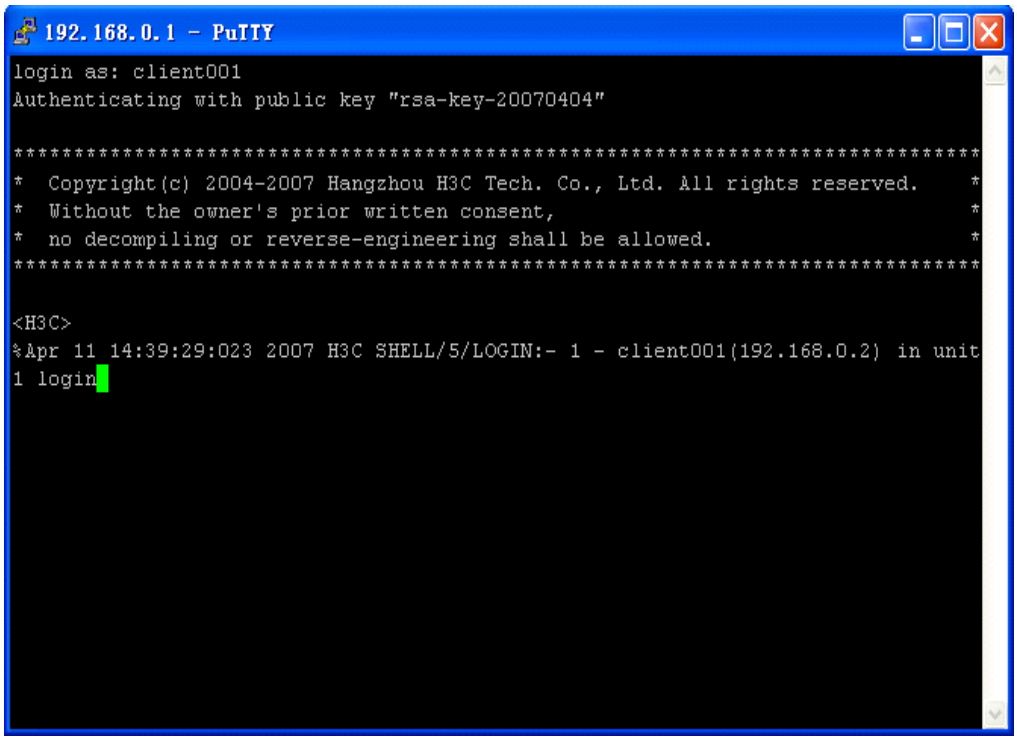


图3-13 SSH 客户端界面

3.1.3 S3600 交换机充当 SSH 客户端并采用 password 认证时的配置举例

1. 组网需求

当用户通过交换机远程登录到另一台交换机时，如果通过的网络不能保证安全,为更大限度地保证数据信息交换的安全性，使用SSH来实现此目的，并采用password认证。如图 3-14所示：

- 交换机 SwitchA 作为 SSH 客户端，用来进行 SSH 登录的用户名为 client001。
- 交换机 SwitchB 作为 SSH 服务器，IP 地址为 10.165.87.136。

2. 组网图

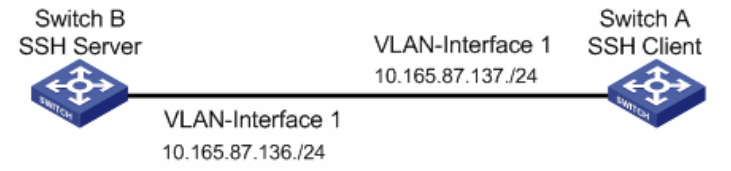


图3-14 SSH 客户端采用 password 认证时的配置组网图

3. 配置步骤

- 配置 SwitchB

在交换机上创建 VLAN 接口，并为其分配 IP 地址，作为客户端连接的 SSH 服务器地址。

```
<H3C> system-view
[H3C] interface vlan-interface 1
[H3C-Vlan-interface1] ip address 10.165.87.136 255.255.255.0
[H3C-Vlan-interface1] quit
```

生成 RSA 密钥对。

```
[H3C] rsa local-key-pair create
```

设置用户接口上的认证模式为 AAA 认证。

```
[H3C] user-interface vty 0 4
[H3C-ui-vty0-4] authentication-mode scheme
```

设置用户接口上支持 SSH 协议。

```
[H3C-ui-vty0-4] protocol inbound ssh
[H3C-ui-vty0-4] quit
```

创建用户 client001，设置其认证密码为 abc，登录协议为 SSH，能访问的命令级别为 3。

```
[H3C] local-user client001
[H3C-luser-client001] password simple abc
[H3C-luser-client001] service-type ssh level 3
[H3C-luser-client001] quit
```

指定用户 client001 的认证方式为 password。

```
[H3C] ssh user client001 authentication-type password
```

- 配置 SwitchA

在交换机上创建 VLAN 接口，并为其分配 IP 地址，作为连接 SSH 服务器端的 SSH 客户端地址。

```
<H3C> system-view
[H3C] interface vlan-interface 1
[H3C-Vlan-interface1] ip address 10.165.87.137 255.255.255.0
[H3C-Vlan-interface1] quit
```

建立到服务器 10.165.87.136 的 SSH 连接。

```
[H3C] ssh2 10.165.87.136
Username: client001
Trying 10.165.87.136 ...
Press CTRL+K to abort
Connected to 10.165.87.136 ...

The Server is not authenticated. Do you continue to access it?(Y/N):y
Do you want to save the server's public key?(Y/N):n
Enter password:
```

```
**************************************************************************
*  Copyright(c) 2004-2007 Hangzhou H3C Tech. Co., Ltd. All rights reserved.*
*  Without the owner's prior written consent,                             *
*  no decompiling or reverse-engineering shall be allowed.                *
**************************************************************************

<H3C>
```

3.1.4 S3600 交换机充当 SSH 客户端并采用 RSA 认证时的配置举例

1. 组网需求

当用户通过交换机远程登录到另一台交换机时，如果通过的网络不能保证安全,为更大限度地保证数据信息交换的安全性，使用SSH来实现此目的，并采用RSA认证。如图 3-15所示：

- 交换机 SwitchA 作为 SSH 客户端，用来进行 SSH 登录的用户名为 client001。
- 交换机 SwitchB 作为 SSH 服务器，IP 地址为 10.165.87.136。

2. 组网图

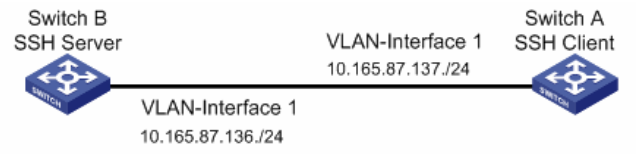


图3-15 SSH 客户端采用 RSA 认证时的配置组网图

3. 配置步骤

- 配置 SwitchB

在交换机上创建 VLAN 接口，并为其分配 IP 地址，作为客户端连接的 SSH 服务器地址。

```
<H3C> system-view
[H3C] interface vlan-interface 1
[H3C-Vlan-interface1] ip address 10.165.87.136 255.255.255.0
[H3C-Vlan-interface1] quit
```

生成 RSA 密钥对。

```
[H3C] rsa local-key-pair create
```

设置用户接口上的认证模式为 AAA 认证。

```
[H3C] user-interface vty 0 4
[H3C-ui-vty0-4] authentication-mode scheme
```

设置用户接口上支持 SSH 协议。

```
[H3C-ui-vty0-4] protocol inbound ssh
```

设置用户能访问的命令级别为 3。

```
[H3C-ui-vty0-4] user privilege level 3
[H3C-ui-vty0-4] quit
```

创建用户 client001，并指定认证方式为 RSA 认证。

```
[H3C] ssh user client001 authentication-type rsa
```

📖 **说明：**

这里需要先在 SSH 客户端生成 RSA 密钥对，并将 RSA 公钥数据手工配置到服务器端。有关配置请参见客户端的配置。

在服务器端配置客户端的公钥，指定公钥名称为 Switch001。

```
[H3C] rsa peer-public-key Switch001
RSA public key view: return to System View with "peer-public-key end".
[H3C-rsa-public-key] public-key-code begin
RSA key code view: return to last view with "public-key-code end".
[H3C-rsa-key-code] 3047
[H3C-rsa-key-code] 0240
[H3C-rsa-key-code] C8969B5A 132440F4 0BDB4E5E 40308747 804F608B
[H3C-rsa-key-code] 349EBD6A B0C75CDF 8B84DBE7 D5E2C4F8 AED72834
[H3C-rsa-key-code] 74D3404A 0B14363D D709CC63 68C8CE00 57C0EE6B
[H3C-rsa-key-code] 074C0CA9
[H3C-rsa-key-code] 0203
[H3C-rsa-key-code] 010001
[H3C-rsa-key-code] public-key-code end
[H3C-rsa-public-key] peer-public-key end
[H3C]
```

为用户 client001 指定公钥 Switch001。

```
[H3C] ssh user client001 assign rsa-key Switch001
```

- 配置 SwitchA

在交换机上创建 VLAN 接口，并为其分配 IP 地址，作为连接 SSH 服务器端的 SSH 客户端地址。

```
<H3C> system-view
[H3C] interface vlan-interface 1
[H3C-Vlan-interface1] ip address 10.165.87.137 255.255.255.0
[H3C-Vlan-interface1] quit
```

生成 RSA 密钥对。

```
[H3C] rsa local-key-pair create
```

显示 RSA 主机公钥数据（这里只显示 RSA 主机公钥数据部分）

```
<H3C> display rsa local-key-pair public

=====================================================
Time of Key pair created: 05:15:04  2006/12/08
Key name: H3C_Host
Key type: RSA encryption Key
=====================================================
Key code:
3047
  0240
    C8969B5A 132440F4 0BDB4E5E 40308747 804F608B
    349EBD6A B0C75CDF 8B84DBE7 D5E2C4F8 AED72834
    74D3404A 0B14363D D709CC63 68C8CE00 57C0EE6B
    074C0CA9
  0203
    010001
<略>
```

说明：

客户端生成密钥对后，需要将 RSA 主机公钥数据手工配置到服务器端，并完成服务器端配置后才继续客户端的配置。

建立到服务器 10.165.87.136 的 SSH 连接。

```
[H3C] ssh2 10.165.87.136
Username: client001
Trying 10.165.87.136 ...
Press CTRL+K to abort
Connected to 10.165.87.136 ...

The Server is not authenticated. Do you continue to access it?(Y/N):y
Do you want to save the server's public key?(Y/N):n

**************************************************************************
*  Copyright(c) 2004-2007 Hangzhou H3C Tech. Co., Ltd. All rights reserved.*
*  Without the owner's prior written consent,                            *
*  no decompiling or reverse-engineering shall be allowed.               *
**************************************************************************
```

```
<H3C>
```

3.1.5 S3600 交换机充当 SSH 客户端并采用不支持首次认证时的配置举例

1. 组网需求

当用户通过交换机远程登录到另一台交换机时，如果通过的网络不能保证安全,为更大限度地保证数据信息交换的安全性，使用SSH来实现此目的。如图 3-16所示：

- 交换机 SwitchA 作为 SSH 客户端，用来进行 SSH 登录的用户名为 client001。
- 交换机 SwitchB 作为 SSH 服务器，IP 地址为 10.165.87.136。
- 采用 RSA 认证方式，以提高安全性。

2. 组网图

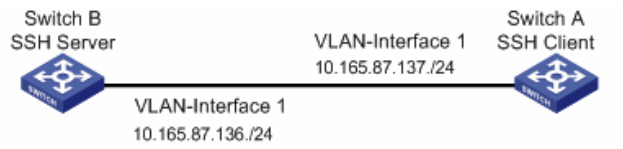


图3-16 SSH 客户端配置组网图

3. 配置步骤

- 配置 SwitchB

在交换机上创建 VLAN 接口，并为其分配 IP 地址，作为客户端连接的 SSH 服务器地址。

```
<H3C> system-view
[H3C] interface vlan-interface 1
[H3C-Vlan-interface1] ip address 10.165.87.136 255.255.255.0
[H3C-Vlan-interface1] quit
```

生成 RSA 密钥对。

```
[H3C] rsa local-key-pair create
```

设置用户接口上的认证模式为 AAA 认证。

```
[H3C] user-interface vty 0 4
[H3C-ui-vty0-4] authentication-mode scheme
```

设置用户接口上支持 SSH 协议。

```
[H3C-ui-vty0-4] protocol inbound ssh
```

设置用户能访问的命令级别为 3。

```
[H3C-ui-vty0-4] user privilege level 3
[H3C-ui-vty0-4] quit
```

创建用户 client001，并指定认证方式为 RSA 认证。

```
[H3C] ssh user client001 authentication-type rsa
```

📖 说明：

这里需要先在 SSH 客户端生成 RSA 密钥对，并将 RSA 公钥数据手工配置到服务器端。有关配置请参见客户端的配置。

在服务器端配置客户端的公钥，指定公钥名称为 Switch001。

```
[H3C] rsa peer-public-key Switch001
RSA public key view: return to System View with "peer-public-key end".
[H3C-rsa-public-key] public-key-code begin
RSA key code view: return to last view with "public-key-code end".
[H3C-rsa-key-code] 3047
[H3C-rsa-key-code] 0240
[H3C-rsa-key-code] C8969B5A 132440F4 0BDB4E5E 40308747 804F608B
[H3C-rsa-key-code] 349EBD6A B0C75CDF 8B84DBE7 D5E2C4F8 AED72834
[H3C-rsa-key-code] 74D3404A 0B14363D D709CC63 68C8CE00 57C0EE6B
[H3C-rsa-key-code] 074C0CA9
[H3C-rsa-key-code] 0203
[H3C-rsa-key-code] 010001
[H3C-rsa-key-code] public-key-code end
[H3C-rsa-public-key] peer-public-key end
[H3C]
```

为用户 client001 指定公钥 Switch001。

```
[H3C] ssh user client001 assign rsa-key Switch001
```

📖 说明：

采用不支持首次认证时，需要将服务器端的 RSA 主机公钥数据通过手工配置方式配置到客户端。

显示服务器端的 RSA 主机公钥数据（这里只显示 RSA 主机公钥数据部分）。

```
[H3C] display rsa local-key-pair public

=====================================================
Time of Key pair created: 09:04:41  2000/04/04
Key name: H3C_Host
Key type: RSA encryption Key
=====================================================
Key code:
308188
  028180
```

```
    C9330FFD 2E2A606F 3BFD5554 8DACDFB8 4D754E86
    FC2D15E8 1996422A 0F6A2A6A A94A207E 1E25F3F9
    E0EA01A2 4E0F2FF7 B1D31505 39F02333 E443EE74
    5C3615C3 E5B3DC91 D41900F0 2AE8B301 E55B1420
    024ECF2C 28A6A454 C27449E0 46EB1EAF 8A918D33
    BAF53AF3 63B1FB17 F01E4933 00BE2EEA A272CD78
    C289B7DD 2BE0F7AD
  0203
    010001
<略>
```

- 配置 SwitchA

在交换机上创建 VLAN 接口，并为其分配 IP 地址，作为连接 SSH 服务器端的 SSH 客户端地址。

```
<H3C> system-view
[H3C] interface vlan-interface 1
[H3C-Vlan-interface1] ip address 10.165.87.137 255.255.255.0
[H3C-Vlan-interface1] quit
```

生成 RSA 密钥对。

```
[H3C] rsa local-key-pair create
```

显示客户端的 RSA 主机公钥数据（这里只显示 RSA 主机公钥数据部分）

```
<H3C> display rsa local-key-pair public

=====================================================
Time of Key pair created: 05:15:04  2006/12/08
Key name: H3C_Host
Key type: RSA encryption Key
=====================================================
Key code:
3047
  0240
    C8969B5A 132440F4 0BDB4E5E 40308747 804F608B
    349EBD6A B0C75CDF 8B84DBE7 D5E2C4F8 AED72834
    74D3404A 0B14363D D709CC63 68C8CE00 57C0EE6B
    074C0CA9
  0203
    010001
<略>
```

📖 **说明：**

客户端生成密钥对后，需要将 RSA 主机公钥数据手工配置到服务器端，并完成服务器端配置后才继续客户端的配置。

设置不支持首次认证

```
[H3C] undo ssh client first-time
```

📖 **说明：**

采用不支持首次认证时，需要将 SSH 服务器端的 RSA 主机公钥数据手工配置到客户端。

在客户端配置服务器端的公钥，指定公钥名称为 Switch002。

```
[H3C] rsa peer-public-key Switch002
RSA public key view: return to System View with "peer-public-key end".
[H3C-rsa-public-key] public-key-code begin
RSA key code view: return to last view with "public-key-code end".
[H3C-rsa-key-code] 308188
[H3C-rsa-key-code] 028180
[H3C-rsa-key-code] C9330FFD 2E2A606F 3BFD5554 8DACDFB8 4D754E86
[H3C-rsa-key-code] FC2D15E8 1996422A 0F6A2A6A A94A207E 1E25F3F9
[H3C-rsa-key-code] E0EA01A2 4E0F2FF7 B1D31505 39F02333 E443EE74
[H3C-rsa-key-code] 5C3615C3 E5B3DC91 D41900F0 2AE8B301 E55B1420
[H3C-rsa-key-code] 024ECF2C 28A6A454 C27449E0 46EB1EAF 8A918D33
[H3C-rsa-key-code] BAF53AF3 63B1FB17 F01E4933 00BE2EEA A272CD78
[H3C-rsa-key-code] C289B7DD 2BE0F7AD
[H3C-rsa-key-code] 0203
[H3C-rsa-key-code] 010001
[H3C-rsa-key-code] public-key-code end
[H3C-rsa-public-key] peer-public-key end
[H3C]
```

在客户端上指定要连接的服务器端的主机公钥名称。

```
[H3C] ssh client 10.165.87.136 assign rsa-key Switch002
```

建立到服务器 10.165.87.136 的 SSH 连接。

```
[H3C] ssh2 10.165.87.136
Username: client001
Trying 10.165.87.136 ...
Press CTRL+K to abort
Connected to 10.165.87.136 ...
```

```
**************************************************************************
*  Copyright(c) 2004-2007 Hangzhou H3C Tech. Co., Ltd. All rights reserved.*
*  Without the owner's prior written consent,                             *
*  no decompiling or reverse-engineering shall be allowed.                *
**************************************************************************

<H3C>
```

目 录

第1章 路由协议简介

1.1 路由协议简介

1.1.1 静态路由和动态路由协议

1. 静态路由

无开销，配置简单，需要人工维护，适合简单、稳定的拓扑结构的网络。对于网络结构的变化需要人工干涉。

2. RIP

配置相对比较简单，对路由器的 CPU 及内存性能不是很敏感，适合中小型网络。收敛速度较慢，无法彻底解决路由环路的问题。由于路由更新原则是周期性的广播或组播模式，消耗较多的网络资源。

3. OSPF

配置比较复杂，对路由器的 CPU 及内存性能要求较高，适合大中型网络。收敛速度快，彻底根除路由环路的问题。支持区域划分，提供路由分级管理。

4. BGP

配置比较复杂，是运行在 AS 之间的路由协议。具有非常灵活和强大的路由策略控制，彻底根除路由环路问题。具有高可靠性、稳定性、可扩展性。

1.1.2 动态路由协议在交换机中的应用

表1-1 H3C 系列交换机支持动态路由协议列表

路由协议 / 产品型号	RIP	OSPF	BGP
S3600-SI	√	-	-
E352&328	√	-	-
S3600-EI	√	√	-
S5600	√	√	√

1.2 配置指南

说明：

- 该配置指南以 S5600 系列交换机为准。
- 各配置注意事项请参见具体产品操作手册和命令手册。

1.2.1 配置任务简介

表1-2 配置任务简介

配置任务	详细说明
静态路由配置	1.2.2
RIP 配置	1.2.3
OSPF 配置	1.2.4
BGP 配置	1.2.5

1.2.2 静态路由配置

表1-3 配置静态路由

操作	命令	说明
进入系统视图	**system-view**	-
配置静态路由	**ip route-static** *ip-address* { *mask* | *mask-length* } { *interface-type interface-number* | *next-hop* } [**preference** *preference-value*] [**reject** | **blackhole**] [**detect-group** *group number*] [**description** *text*]	必选 缺省情况下，系统可以获取到去往与路由器直连的子网路由

1.2.3 RIP 配置

表1-4 RIP 配置指导

配置任务		说明	详细配置
配置 RIP 的基本功能	RIP 基本配置	必选	1.2.3 1.
	配置接口的工作状态	可选	1.2.3 2.
	配置 RIP 的版本号	可选	1.2.3 3.

配置任务		说明	详细配置
控制 RIP 的路由信息	配置接口的附加度量值	可选	1.2.3 4.
	配置 RIP 的路由聚合	可选	1.2.3 5.
	禁止 RIP 接收主机路由	可选	1.2.3 6.
	配置 RIP 接收或者发布的路由进行过滤	可选	1.2.3 7.
	配置 RIP 协议优先级	可选	1.2.3 8.
	配置 RIP 在不同接口之间流量等价分担	可选	1.2.3 9.
	配置 RIP 的引入外部路由信息	可选	1.2.3 10.
调整和优化 RIP 网络	配置 RIP 定时器	可选	1.2.3 11.
	配置水平分割	可选	1.2.3 12.
	配置 RIP-1 报文的零域检查	可选	1.2.3 13.
	配置 RIP-2 报文的认证方式	可选	1.2.3 14.
	配置 RIP 邻居	可选	1.2.3 15.

1. RIP 基本配置

表1-5 启动 RIP，并在指定的网段使能 RIP

操作	命令	说明
进入系统视图	**system-view**	-
启动 RIP 并进入 RIP 视图	**rip**	必选
在指定网段接口上使能 RIP	**network** *network-address*	必选 缺省情况下，接口禁用 RIP

2. 配置接口的工作状态

表1-6 配置接口的工作状态

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
允许接口接收 RIP 更新报文	**rip input**	可选 缺省情况下，允许接口发送或接收 RIP 报文
允许接口发送 RIP 更新报文	**rip output**	
允许接口收发 RIP 报文	**rip work**	

3. 配置 RIP 的版本号

表1-7 配置 RIP 版本号

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
指定接口运行的 RIP 版本	**rip version** { **1** | **2** [**broadcast** | **multicast**] }	必选 缺省情况下，接口接收 RIP-1 和 RIP-2 的报文，只发送 RIP-1 报文。当配置接口版本为 RIP-2 时，同时可以指定报文的发送方式

4. 配置接口的附加度量值

表1-8 配置接口的附加度量值

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
设置接口在接收路由时增加的度量值	**rip metricin** *value*	可选 缺省情况下，RIP 在接收报文时给路由增加的附加路由度量值为 0
设置接口在发布路由时增加的度量值	**rip metricout** *value*	可选 缺省情况下，RIP 在发送报文时给路由增加的附加路由度量值为 1

5. 配置 RIP 的路由聚合

表1-9 配置 RIP 的路由聚合

操作	命令	说明
进入系统视图	**system-view**	-
进入 RIP 视图	**rip**	-
使能 RIP-2 自动路由聚合	**summary**	必选 缺省情况下，RIP-2 启用自动路由聚合功能

6. 禁止 RIP 接收主机路由

表1-10 禁止 RIP 接收主机路由

操作	命令	说明
进入系统视图	**system-view**	-
进入 RIP 视图	**rip**	-
禁止接收主机路由	**undo host-route**	必选 缺省情况下，允许路由器接收主机路由

7. 对接收或发布的路由信息进行过滤

表1-11 配置对接收或者发布的路由信息进行过滤

操作	命令	说明
进入系统视图	**system-view**	-
进入 RIP 视图	**rip**	-
对接收的路由信息进行过滤	**filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* [**gateway** *ip-prefix-name*] | **route-policy** *route-policy-name* } **import**	必选 缺省情况下，RIP 不对接收的路由信息进行过滤 使用 **gateway** 参数的命令用来配置对接收的指定地址发布的路由信息进行过滤
	filter-policy gateway *ip-prefix-name* **import**	
对发布的路由信息进行过滤	**filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*protocol*] [*process-id*]	必选 缺省情况下，RIP 不对发布的路由信息进行过滤
	filter-policy route-policy *route-policy-name* **export**	

8. 配置 RIP 协议优先级

表1-12 配置 RIP 协议优先级

操作	命令	说明
进入系统视图	**system-view**	-
进入 RIP 视图	**rip**	-
设置 RIP 协议的优先级	**preference** *value*	必选 缺省值为 100

9. 配置 RIP 在不同接口之间流量等价分担

表1-13 配置 RIP 在不同接口之间流量等价分担

操作	命令	说明
进入系统视图	**system-view**	-
进入 RIP 视图	**rip**	-
配置 RIP 在不同接口之间流量等价分担	**traffic-share-across-interface**	必选 缺省情况下，**traffic-share-across-interface** 处于关闭状态

10. RIP 引入外部路由信息

表1-14 配置 RIP 引入外部路由信息

操作	命令	说明
进入系统视图	**system-view**	-
进入 RIP 视图	**rip**	-
设定路由引入的缺省度量值	**default cost** *value*	可选 缺省值为 1
引入外部路由信息	**import-route** *protocol* [*process-id*] [**cost** *value* | **route-policy** *route-policy-name*]*	必选 *process-id* 参数仅在引入 ospf 路由时使用

11. 配置 RIP 定时器

表1-15 配置 RIP 定时器

操作	命令	说明
进入系统视图	**system-view**	-
进入 RIP 视图	**rip**	-
配置 RIP 定时器的值	**timers** { **update** *update-timer* | **timeout** *timeout-timer* } *	必选 缺省情况下，Update 定时器值：30 秒，Timeout 定时器值：180 秒

12. 配置水平分割

表1-16 配置水平分割

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
进入接口视图	**interface** *interface-type interface-number*	-
启动水平分割	**rip split-horizon**	必选 缺省情况下，接口发送 RIP 报文时使用水平分割

13. 配置 RIP-1 报文的零域检查

表1-17 配置 RIP-1 报文的零域检查

操作	命令	说明
进入系统视图	**system-view**	-
进入 RIP 视图	**rip**	-
对 RIP-1 报文的零域进行检查	**checkzero**	必选 缺省情况下，RIP-1 进行零域检查

14. 配置 RIP-2 报文的认证方式

表1-18 配置 RIP-2 报文的认证方式

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置RIP-2报文的认证方式	**rip authentication-mode** { **simple** *password* | **md5** { **rfc2453** *key-string* | **rfc2082** *key-string key-id* } }	必选 如果配置MD5认证，则必须配置MD5的类型： ● **rfc2453** 类型支持符合 RFC2453 规定的报文格式 ● **rfc2082** 类型支持符合 RFC2082 规定的报文格式

15. 配置 RIP 邻居

表1-19 配置 RIP 邻居

操作	命令	说明
进入系统视图	**system-view**	-
进入 RIP 视图	**rip**	-

操作	命令	说明
配置 RIP 邻居	**peer** *ip-address*	必选 如果在不支持广播或组播报文的链路上运行 RIP，则必须手工指定 RIP 的邻居 通常情况下，RIP 使用广播或组播地址发送报文

1.2.4 OSPF 配置

表1-20 OSPF 配置指导

配置任务		说明	详细配置
配置 OSPF 基本功能		必选	1.2.4 1.
配置 OSPF 的区域特性		可选	1.2.4 2.
配置 OSPF 的网络类型	配置 OSPF 接口的网络类型	可选	1.2.4 3.
	配置 NBMA 网络的邻居	可选	1.2.4 4.
	配置 OSPF 接口的 DR 优先级	可选	1.2.4 5.
配置 OSPF 的路由信息控制	配置 OSPF 路由聚合	可选	1.2.4 6.
	配置 OSPF 对接收的路由进行过滤	可选	1.2.4 7.
	配置 OSPF 的链路开销	可选	1.2.4 8.
	配置 OSPF 协议的优先级	可选	1.2.4 9.
	配置 OSPF 等价路由的条数	可选	1.2.4 10.
	配置 OSPF 引入外部路由	可选	1.2.4 11.
配置 OSPF 网络调整优化	配置 OSPF 报文定时器	可选	1.2.4 12.
	配置接口传送 LSA 的延迟时间	可选	1.2.4 13.
	配置 SPF 计算间隔	可选	1.2.4 14.
	禁止接口发送 OSPF 报文	可选	1.2.4 15.
	配置 OSPF 验证	可选	1.2.4 16.
	配置 DD 报文中的 MTU	可选	1.2.4 17.
	配置 OSPF 记录功能	可选	1.2.4 18.
	配置 OSPF 网管功能	可选	1.2.4 19.

1. 配置 OSPF 基本功能

表1-21 OSPF 基本配置

操作	命令	说明
进入系统视图	**system-view**	-
配置路由器的 ID	**router id** *router-id*	可选 当在一台路由器上运行多个 OSPF 进程时，建议使用 **ospf** 命令中的 **router-id** 为不同进程指定不同的 Router ID
启动 OSPF，进入 OSPF 视图	**ospf** [*process-id* [**router-id** *router-id*]]	必选 进入 OSPF 视图
进入 OSPF 区域视图	**area** *area-id*	必选
配置区域所包含的网段	**network** *address wildcard-mask*	必选 缺省情况下，接口不属于任何区域

2. 配置 OSPF 的区域特性

表1-22 配置 OSPF 的区域特性

操作	命令	说明
进入系统视图	**system-view**	-
进入 OSPF 视图	**ospf** [*process-id* [**router-id** *router-id*]]	-
进入 OSPF 区域视图	**area** *area-id*	-
配置当前区域为 Stub 区域	**stub** [**no-summary**]	可选 缺省情况下，没有区域被设置为 Stub 区域
配置当前区域为 NSSA 区域	**nssa** [**default-route-advertise** | **no-import-route** | **no-summary**]*	可选 缺省情况下，没有区域被设置为 NSSA 区域
配置发送到 Stub 区域或者 NSSA 区域缺省路由的开销	**default-cost** *cost*	可选 仅在 ABR 上进行配置。 缺省情况下，发送到 Stub 区域或者 NSSA 区域的缺省路由的开销为 1
创建并配置虚连接	**vlink-peer** *router-id* [**hello** *seconds* | **retransmit** *seconds* | **trans-delay** *seconds* | **dead** *seconds* | **simple** *password* | **md5** *keyid key*]*	可选 为使虚连接生效，在虚连接的两端都需配置此命令，并且两端配置的 **hello**、**dead** 等参数必须一致。

3. 配置 OSPF 接口的网络类型

表1-23 配置 OSPF 接口的网络类型

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置 OSPF 接口的网络类型	**ospf network-type** { **broadcast** | **nbma** | **p2mp** | **p2p** }	必选 缺省情况下，接口的网络类型根据物理接口而定

4. 配置 NBMA 网络的邻居

表1-24 配置 NBMA 网络的邻居

操作	命令	说明
进入系统视图	**system-view**	-
进入 OSPF 视图	**ospf** [*process-id* [**router-id** *router-id*]]	-
配置 NBMA 网络的邻居	**peer** *ip-address* [**dr-priority** *dr-priority*]	必选 缺省情况下，NBMA 接口的邻接点优先级的取值为 1

5. 配置 OSPF 接口的 DR 优先级

表1-25 配置 OSPF 接口的 DR 优先级

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
设置 OSPF 接口的 DR 优先级	**ospf dr-priority** *priority*	必选 缺省情况下，优先级为 1

6. 配置 OSPF 路由聚合

表1-26 配置 ABR 路由聚合

操作	命令	说明
进入系统视图	**system-view**	-
进入 OSPF 视图	**ospf** [*process-id* [**router-id** *router-id*]]	必选

操作	命令	说明
进入区域视图	**area** *area-id*	-
配置 OSPF 的 ABR 路由聚合	**abr-summary** *ip-address mask* [**advertise** | **not-advertise**]	必选 此命令只有在 ABR 上配置才会有效。缺省情况下，区域边界路由器不对路由聚合

表1-27 配置 ASBR 路由聚合

操作	命令	说明
进入系统视图	**system-view**	-
进入 OSPF 视图	**ospf** [*process-id* [**router-id** *router-id*]]	-
配置 OSPF 的 ASBR 路由聚合	**asbr-summary** *ip-address mask* [**not-advertise** | **tag** *value*]	必选 此命令只有在 ASBR 上配置才会有效。缺省情况下，不对引入的路由进行聚合

7. 配置 OSPF 对接收的路由进行过滤

表1-28 配置 OSPF 对接收的路由进行过滤

操作	命令	说明
进入系统视图	**system-view**	-
进入 OSPF 视图	**ospf** [*process-id* [**router-id** *router-id*]]	-
配置对接收的路由进行过滤	**filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* | **gateway** *ip-prefix-name* } **import**	必选 缺省情况下，不对接收到的路由信息进行过滤

8. 配置 OSPF 的链路开销

表1-29 配置 OSPF 接口的开销值

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-

操作	命令	说明
设置 OSPF 接口的开销值	**ospf cost** *value*	必选 缺省情况下，接口按照当前的波特率自动计算开销。对于交换机的 VLAN 接口，该值固定为 10

9. 配置 OSPF 协议的优先级

表1-30 配置 OSPF 协议的优先级

操作	命令	说明
进入系统视图	**system-view**	-
进入 OSPF 视图	**ospf** [*process-id* [**router-id** *router-id*]]	-
配置 OSPF 协议的优先级	**preference** [**ase**] *value*	必选 缺省情况下，OSPF 路由的优先级为 10，OSPF ASE 的优先级为 150

10. 配置 OSPF 等价路由的条数

表1-31 配置 OSPF 等价路由

操作	命令	说明
进入系统视图	**system-view**	-
进入 OSPF 视图	**ospf** [*process-id* [**router-id** *router-id*]]	-
配置 OSPF 等价路由的条数	**multi-path-number** *value*	必选

11. 配置 OSPF 引入外部路由

表1-32 配置 OSPF 引入外部路由

操作	命令	说明
进入系统视图	**system-view**	-
进入 OSPF 视图	**ospf** [*process-id* [**router-id** *router-id*]]	-
配置 OSPF 引入其它协议的路由	**import-route** *protocol* [*process-id*] [**cost** *value* | **type** *value* | **tag** *value* | **route-policy** *route-policy-name*]*	必选 缺省情况下，不引入其他协议的路由信息

操作	命令	说明
配置对发布的路由进行过滤	**filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*protocol*]	可选 缺省情况下，不对发布的路由信息进行过滤
配置 OSPF 引入缺省路由	**default-route-advertise** [**always** | **cost** *value* | **type** *type-value* | **route-policy** *route-policy-name*]*	可选 缺省情况下，不引入缺省路由
配置 OSPF 在接收外部路由时缺省的花费值	**default cost** *value*	可选 缺省情况下，OSPF 引入外部路由的缺省度量值为 1
配置 OSPF 在每单位时间内引入外部路由数量的缺省限制	**default limit** *routes*	可选 缺省情况下，引入路由数量的上限为 1000
配置 OSPF 引入外部路由的缺省时间间隔	**default interval** *seconds*	缺省情况下，缺省时间间隔为 1 秒
配置 OSPF 在接收外部路由时缺省的标记值	**default tag** *tag*	可选 缺省情况下，设置缺省标记值为 1
配置 OSPF 在接收外部路由时缺省的类型	**default type** { **1** | **2** }	可选 缺省情况下，引入的外部路由类型为 Type2

12. 配置 OSPF 报文定时器

表1-33 配置 OSPF 报文定时器

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置接口发送 Hello 报文的时间间隔	**ospf timer hello** *seconds*	可选 缺省情况下，**point-to-point**、**broadcast** 类型接口发送 Hello 报文的时间间隔的值为 10 秒； **point-to-multipoint**、**NBMA** 类型接口发送 Hello 报文的时间间隔的值为 30 秒
在 NBMA 接口上配置发送轮询报文的时间间隔	**ospf timer poll** *seconds*	可选 缺省情况下，发送轮询报文的时间间隔为 40 秒

操作	命令	说明
设置相邻路由器间失效时间	**ospf timer dead** *seconds*	可选 缺省情况下，**point-to-point**、**broadcast** 类型接口的 OSPF 邻居失效时间为 40 秒，**point-to-multipoint**、**NBMA** 类型接口的 OSPF 邻居失效时间为 120 秒
设置邻接路由器重传 LSA 的间隔	**ospf timer retransmit** *interval*	可选 缺省情况下，时间间隔为 5 秒

13. 配置接口传送 LSA 的延迟时间

表1-34 配置接口传送 LSA 的延迟时间

操作	命令	说明
进入系统视图	**system-view**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置接口传送 LSA 的延迟时间	**ospf trans-delay** *seconds*	必选 缺省情况下，传输延迟时间为 1 秒

14. 配置 SPF 计算间隔

表1-35 配置 SPF 计算间隔

操作	命令	说明
进入系统视图	**system-view**	-
进入 OSPF 视图	**ospf** [*process-id* [**router-id** *router-id*]]	-
设置 SPF 计算间隔	**spf-schedule-interval** *interval*	必选 缺省情况下，SPF 计算的时间间隔为 5 秒

15. 禁止接口发送 OSPF 报文

表1-36 禁止接口发送 OSPF 报文

操作	命令	说明
进入系统视图	**system-view**	-
进入 OSPF 视图	**ospf** [*process-id* [**router-id** *router-id*]]	-

操作	命令	说明
禁止接口发送 OSPF 报文	**silent-interface** *silent-nterface-type silent-interface-number*	必选 缺省情况下，允许接口发送 OSPF 报文

16. 配置 OSPF 验证

表1-37 配置 OSPF 验证

操作	命令	说明
进入系统视图	**system-view**	-
进入 OSPF 视图	**ospf** [*process-id* [**router-id** *router-id*]]	-
进入 OSPF 区域视图	**area** *area-id*	-
配置 OSPF 区域的验证模式	**authentication-mode** { **simple** | **md5** }	必选 缺省情况下，没有配置区域验证模式
退回到 OSPF 视图	**quit**	-
退回到系统视图	**quit**	-
进入接口视图	**interface** *interface-type interface-number*	-
配置 OSPF 接口的验证模式	**ospf authentication-mode** { **simple** *password* | **md5** *key-id key* }	必选 缺省情况下，接口不对 OSPF 报文进行验证

17. 配置 DD 报文中的 MTU

表1-38 配置 DD 报文中的 MTU

操作	命令	说明
进入系统视图	**system-view**	-
进入 Ethernet 接口视图	**interface** *interface-type interface-number*	-
使能接口发送 DD 报文时填 MTU 值	**ospf mtu-enable**	必选 缺省情况下，接口发送 DD 报文时 MTU 值为 0，即不填接口的实际 MTU 值

18. 配置 OSPF 记录功能

表1-39 配置 OSPF 记录信息

操作	命令	说明
进入系统视图	**system-view**	-
进入 OSPF 视图	**ospf** [*process-id* [**router-id** *router-id*]]	-
配置邻居状态记录	**log-peer-change**	必选 记录邻居状态变化信息

19. 配置 OSPF 网管功能

表1-40 配置 OSPF MIB 绑定

操作	命令	说明
进入系统视图	**system-view**	-
配置 OSPF MIB 绑定	**ospf mib-binding** *process-id*	可选 如果不配此命令，MIB 操作绑定会默认绑定第 1 个 OSPF 进程。当启动了多个 OSPF 进程时，可以配置 OSPF MIB 绑定在哪个进程上
使能 OSPF 的 TRAP 功能	**snmp-agent trap enable ospf** [*process-id*] [**ifauthfail** | **ifcfgerror** | **ifrxbadpkt** | **ifstatechange** | **iftxretransmit** | **lsdbapproachoverflow** | **lsdboverflow** | **maxagelsa** | **nbrstatechange** | **originatelsa** | **vifauthfail** | **vifcfgerror** | **virifrxbadpkt** | **virifstatechange** | **viriftxretransmit** | **virnbrstatechange**]*	可选 可以配置 OSPF 发送多种 SNMP TRAP 报文，并可以通过进程号指定某个 OSPF 进程发送 SNMP TRAP 报文

1.2.5 BGP 配置

表1-41 BGP 配置指导

配置任务	说明	详细配置
配置 BGP 的基本功能	必选	1.2.5 1.

配置任务		说明	详细配置
控制路由信息的发布与接收	配置 BGP 引入其他路由信息	可选	1.2.5 2.
	配置 BGP 路由聚合	可选	1.2.5 3.
	配置发送缺省路由	可选	1.2.5 4.
	配置 BGP 路由信息的接收策略	可选	1.2.5 5.
	配置 BGP 路由信息的发布策略	可选	1.2.5 6.
	配置 BGP 与 IGP 路由不同步	可选	1.2.5 7.
	配置 BGP 路由衰减	可选	1.2.5 8.
配置 BGP 的路由属性		可选	1.2.5 9.
调整和优化 BGP 网络		可选	1.2.5 10.
配置 BGP 大型网络	配置 BGP 对等体组	必选	1.2.5 11.
	配置 BGP 团体	必选	1.2.5 12.
	配置 BGP 路由反射器	可选	1.2.5 13.
	配置 BGP 联盟	可选	1.2.5 14.

1. BGP 基本配置

表1-42 配置 BGP 的基本功能

操作	命令	说明
进入系统视图	**system-view**	-
配置 Router ID	**router id** *router-id*	可选
启动 BGP，进入 BGP 视图	**bgp** *as-number*	必选 缺省情况下，系统不运行 BGP
指定对等体组的 AS 号	**peer** *group-name* **as-number** *as-number*	必选 缺省情况下，对等体组无 AS 号
配置对等体/对等体组的描述信息	**peer** { *group-name* | *ip-address* } **description** *description-text*	可选 缺省情况下，对等体/对等体组无描述信息
激活指定对等体	**peer** { *group-name* | *ip-address* } **enable**	可选 缺省情况下，BGP 对等体是激活的
使能 BGP 日志记录功能	**log-peer-change**	可选 缺省情况下，BGP 日志记录功能处于关闭状态

操作	命令	说明
指定路由更新报文的源接口	**peer** { *group-name* | *ip-address* } **connect-interface** *interface-type interface-number*	可选 缺省情况下，BGP 使用最佳路由更新报文的源接口
配置允许同非直接相连网络上的邻居建立 EBGP 连接	**peer** *group-name* **ebgp-max-hop** [*hop-count*]	可选 缺省情况下，不允许同非直接相连网络上的邻居建立 EBGP 连接。配置参数 *hop-count*，可以同时配置 EBGP 连接的最大路由器跳数

2. 配置 BGP 引入其他路由信息

表1-43 配置 BGP 引入其他路由信息

操作	命令	说明
进入系统视图	**system-view**	-
进入 BGP 视图	**bgp** *as-number*	-
允许将缺省路由引入到 BGP 路由表中	**default-route imported**	可选 缺省情况下，BGP 不允许将缺省路由引入到 BGP 路由表中
引入其它协议路由信息并通告	**import-route** *protocol* [*process-id*] [**med** *med-value* | **route-policy** *route-policy-name*]*	必选 缺省情况下，BGP 未引入且不通告其它协议的路由
将网段路由通告到 BGP 路由表中	**network** *network-address* [*mask*] [**route-policy** *route-policy-name*]	可选 缺省情况下，BGP 不通告任何网段路由

3. 配置 BGP 路由聚合

表1-44 配置 BGP 路由聚合

操作		命令	说明
进入系统视图		**system-view**	-
进入 BGP 视图		**bgp** *as-number*	-
配置 BGP 路由聚合	配置路由自动聚合	**summary**	必选 缺省情况下，不进行路由聚合
	配置手动路由聚合	**aggregate** *ip-address mask* [**as-set** | **attribute-policy** *route-policy-name* | **detail-suppressed** | **origin-policy** *route-policy-name* | **suppress-policy** *route-policy-name*]*	

4. 配置发送缺省路由

表1-45 配置向对等体发送缺省路由

操作	命令	说明
进入系统视图	**system-view**	-
进入 BGP 视图	**bgp** *as-number*	-
向对等体组发送缺省路由	**peer** *group-name* **default-route-advertise**	必选 缺省情况下，不向对等体组发送缺省路由

5. 配置对接收的路由信息的过滤策略

表1-46 配置对接收的路由信息的过滤策略

操作	命令	说明
进入系统视图	**system-view**	-
进入 BGP 视图	**bgp** *as-number*	-
对接收的全局路由信息进行过滤	**filter-policy** { *acl-number* | **gateway** *ip-prefix-name* **| ip-prefix** *ip-prefix-name* [**gateway** *ip-prefix-name*] } **import**	必选 缺省情况下，不对接收的路由信息进行过滤
对来自对等体/对等体组的路由指定路由策略	**peer** { *group-name* | *ip-address* } **route-policy** *policy-name* **import**	必选 缺省情况下，不指定对等体/对等体组的路由策略

操作		命令	说明
过滤从对等体/对等体组接收的路由信息	为对等体/对等体组设置基于 ACL 的过滤策略	**peer** { *group-name* | *ip-address* } **filter-policy** *acl-number* **import**	必选 缺省情况下，对等体/对等体组无基于 ACL 过滤策略，无基于 AS 路径过滤列表的路由过滤策略，无基于 IP 前缀列表的过滤策略
	为对等体/对等体组设置基于 AS 路径过滤列表的 BGP 路由过滤策略	**peer** { *group-name* | *ip-address* } **as-path-acl** *acl-number* **import**	
	为对等体/对等体组设置基于 IP 前缀列表的路由过滤策略	**peer** { *group-name* | *ip-address* } **ip-prefix** *ip-prefix-name* **import**	

6. 配置对发布的路由信息的过滤策略

表1-47 配置对发布的路由信息的过滤策略

操作		命令	说明
进入系统视图		**system-view**	-
进入 BGP 视图		**bgp** *as-number*	-
对发布的路由进行过滤		**filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*protocol* [*process-id*]]	必选 缺省情况下，不对发布的路由信息进行过滤
对向对等体组发布的路由指定路由策略		**peer** *group-name* **route-policy** *route-policy-name* **export**	必选 缺省情况下，不指定对等体组的路由策略
过滤发布给对等体的路由信息	为对等体组设置基于 ACL 的路由过滤策略	**peer** *group-name* **filter-policy** *acl-number* **export**	必选 缺省情况下，对等体组无基于 ACL 路由过滤策略，无基于 AS 路径过滤列表的路由过滤策略，无基于 IP 前缀列表的路由过滤策略
	为对等体组设置基于 AS 路径过滤列表的路由过滤策略	**peer** *group-name* **as-path-acl** *acl-number* **export**	
	为对等体组配置基于 IP 前缀列表的路由过滤策略	**peer** *group-name* **ip-prefix** *ip-prefix-name* **export**	

7. 配置 BGP 与 IGP 路由不同步

表1-48 配置 BGP 与 IGP 路由不同步

操作	命令	说明
进入系统视图	**system-view**	-
进入 BGP 视图	**bgp** *as-number*	-
取消 BGP 与 IGP 路由同步	**undo synchronization**	必选 缺省情况下，BGP 和 IGP 路由不同步

8. 配置 BGP 路由衰减

表1-49 配置 BGP 路由衰减

操作	命令	说明
进入系统视图	**system-view**	-
进入 BGP 视图	**bgp** *as-number*	-
配置 BGP 路由衰减参数	**dampening** [*half-life-reachable half-life-unreachable reuse suppress ceiling*] [**route-policy** *route-policy-name*]	必选 缺省情况下，没有配置路由衰减，*half-life-reachable* 缺省值为 15 分钟，*half-life-unreachable* 缺省值为 15 分钟，*reuse* 缺省值为 750，*suppress* 缺省值为 2000， *ceiling* 缺省值为 16000

9. 配置 BGP 的路由属性

表1-50 配置 BGP 的路由属性

操作	命令	说明
进入系统视图	**system-view**	-
进入 BGP 视图	**bgp** *as-number*	-
配置外部、内部、本地路由的管理优先级	**preference** *ebgp-value ibgp-value local-value*	可选 缺省情况下，各优先级的值分别为 256、256、130
配置本地优先级的缺省值	**default local-preference** *value*	可选 缺省情况下，本地优先级的缺省值为 100

操作		命令	说明
配置 MED 属性	配置本机的缺省 MED 值	**default med** *med-value*	可选 缺省情况下，*med-value* 为 0
	配置允许比较来自不同自治系统中的邻居的路由的 MED 值	**compare-different-as-med**	可选 缺省情况下，不允许比较来自不同 AS 邻居的路由路径的 MED 属性值。
配置发布路由时将自身地址作为下一跳		**peer** *group-name* **next-hop-local**	必选 在某些组网环境中，为保证 IBGP 邻居能够找到正确的下一跳，可以配置在向 IBGP 对等体组发布路由时，改变下一跳地址为自身地址
配置 AS_Path 属性	配置允许本地 AS 编号重复出现的次数	**peer** { *group-name* | *ip-address* } **allow-as-loop** [*number*]	可选 缺省情况下，允许的重复次数为 1
	为对等体组指定一个自治系统号	**peer** *group-name* **as-number** *as-number*	可选 缺省情况下，没有为对等体组配置本地自治系统号
	配置发送 BGP 更新报文时 AS_Path 属性中仅携带公有 AS 编号	**peer** *group-name* **public-as-only**	可选 缺省情况下，发送 BGP 更新报文时，携带私有自治系统号

10. 调整和优化 BGP 网络

表1-51 调整和优化 BGP 网络

操作		命令	说明
进入系统视图		**system-view**	-
进入 BGP 视图		**bgp** *as-number*	-
配置 BGP 定时器	配置 BGP 的存活时间与保持时间间隔	**timer keepalive** *keepalive-interval* **hold** *holdtime-interval*	可选 缺省情况下，存活时间为 60 秒，保持时间为 180 秒。使用 **timer** 命令配置的定时器比使用 **peer timer** 命令配置的定时器优先级要低
	配置指定对等体/对等体组的存活和保持时间	**peer** { *group-name* | *ip-address* } **timer keepalive** *keepalive-interval* **hold** *holdtime-interval*	

操作	命令	说明
配置对等体组的发送同一路由更新报文的时间间隔	**peer** *group-name* **route-update-interval** *seconds*	可选 缺省情况下，向 IBGP 对等体发送同一路由更新的时间间隔为 15 秒，向 EBGP 对等体发送同一路由更新的时间间隔为 30 秒
配置从 BGP 对等体/对等体组接收的路由前缀数量	**peer** { *group-name* | *ip-address* } **route-limit** *prefix-number* [{ **alert-only** | **reconnect** *reconnect-time* } | *percentage-value*] *	可选 缺省情况下，没有限制从 BGP 对等体/对等体组接收的路由前缀数量
手工对 BGP 连接进行软复位	**return**	-
	refresh bgp { **all** | *ip-address* | **group** *group-name* } [**multicast**] { **import** | **export** }	可选
	system-view	重新进入 BGP 视图
	bgp *as-number*	
配置 BGP 建立 TCP 连接时进行 MD5 认证	**peer** { *group-name* | *ip-address* } **password** { **cipher** | **simple** } *password*	可选 缺省情况下，BGP 在建立 TCP 连接时不进行 MD5 认证

11. 配置 BGP 对等体组

表1-52 配置 BGP 对等体组

操作		命令	说明
进入系统视图		**system-view**	-
进入 BGP 视图		**bgp** *as-number*	-
创建 IBGP 对等体组	创建 IBGP 对等体组	**group** *group-name* [**internal**]	可选 如果不选择 **internal** 或 **external** 参数，则创建的是 IBGP 对等体组。可向组中加入多个对等体。系统会自动在 BGP 视图下创建该对等体，并配置其 AS 编号为本地 AS 编号
	向对等体组中加入对等体	**peer** *ip-address* **group** *group-name* [**as-number** *as-number*]	

操作		命令	说明
创建 EBGP 对等体组	创建 EBGP 对等体组	**group** *group-name* **external**	可选 可向组中加入多个对等体。系统会自动在 BGP 视图下创建该对等体，并配置其 AS 编号为对等体组的 AS 编号
	配置对等体组的 AS 编号	**peer** *group-name* **as-number** *as-number*	
	向对等体组中加入对等体	**peer** *ip-address* **group** *group-name* [**as-number** *as-number*]	
创建混合 EBGP 对等体组	创建 EBGP 对等体组	**group** *group-name* **external**	可选 可向组中加入多个对等体
	向对等体组中加入对等体	**peer** *ip-address* **group** *group-name* [**as-number** *as-number*]	
结束与指定对等体/对等体组的会话		**peer** { *group-name* | *ip-address* } **shutdown**	可选

12. 配置 BGP 团体

表1-53 配置 BGP 团体

操作	命令	说明
进入系统视图	**system-view**	-
进入 BGP 视图	**bgp** *as-number*	-
配置向对等体发布团体属性	**peer** *group-name* **advertise-community**	必选 缺省情况下，不将团体属性和扩展团体属性发布给任何对等体组
对向对等体组发布的路由指定路由策略	**peer** *group-name* **route-policy** *route-policy-name* **export**	必选 缺省情况下，不指定对等体组的路由策略

13. 配置 BGP 路由反射器

表1-54 配置 BGP 路由反射器

操作	命令	说明
进入系统视图	**system-view**	-
进入 BGP 视图	**bgp** *as-number*	-

操作	命令	说明
配置将本机作为路由反射器，并将对等体组作为路由反射器的客户	**peer** *group-name* **reflect-client**	必选 缺省情况下，没有配置路由反射器及其客户
使能客户机之间的路由反射	**reflect between-clients**	可选 缺省情况下，允许客户到客户的路由反射
配置路由反射器的集群 ID	**reflector cluster-id** *cluster-id*	可选 缺省情况下，每个路由反射器是使用自己的路由 ID 作为集群 ID

14. 配置 BGP 联盟

表1-55 配置 BGP 联盟

操作		命令	说明
进入系统视图		**system-view**	-
进入 BGP 视图		**bgp** *as-number*	-
BGP 联盟的基本配置	配置联盟 ID	**confederation id** *as-number*	必选 缺省情况下，未配置联盟的 ID，未配置属于联盟的子自治系统
	指定一个联盟体中包含了哪些子自治系统	**confederation peer-as** *as-number-list*	
配置联盟的兼容性		**confederation nonstandard**	可选 缺省情况下，配置的联盟与 RFC1965 一致

1.2.6 路由策略配置

表1-56 路由策略配置指导

配置任务		说明	详细配置
配置过滤列表	配置 IPv4 地址前缀列表	可选	1.2.6 1.
	配置 AS 路径列表	可选	1.2.6 2.
	配置团体属性列表	可选	1.2.6 3.
配置路由策略	创建路由策略	必选	1.2.6 4.
	配置 if-match 子句	可选	1.2.6 5.
	配置 apply 子句	可选	1.2.6 6.

1. 配置 IPv4 地址前缀列表

表1-57 配置 IPv4 地址前缀列表

操作	命令	说明
进入系统视图	**system-view**	-
配置 IPv4 地址前缀列表	**ip ip-prefix** *ip-prefix-name* [**index** *index-number*] { **permit** | **deny** } *network len* [**greater-equal** *greater-equal* | **less-equal** *less-equal*]	必选 缺省情况下，不指定地址前缀列表。

2. 配置 AS 路径列表

表1-58 配置 AS 路径列表

操作	命令	说明
进入系统视图	**system-view**	-
配置 AS 路径列表	**ip as-path-acl** *acl-number* { **permit** | **deny** } *as-regular-expression*	必选 缺省情况下，没有定义 AS 路径列表

3. 配置团体属性列表

表1-59 配置团体属性列表

操作	命令	说明
进入系统视图	**system-view**	-
配置基本团体属性列表	**ip community-list** *basic-comm-list-number* { **permit** | **deny** } [*aa:nn* | **internet** | **no-export-subconfed** | **no-advertise** | **no-export**]*	可选 缺省情况下，未配置 BGP 团体属性列表
配置高级团体属性列表	**ip community-list** *adv-comm-list-number* { **permit** | **deny** } *comm-regular-expression*	可选 缺省情况下，未配置 BGP 团体属性列表

4. 创建路由策略

表1-60 创建路由策略

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
创建路由策略	**route-policy** *route-policy-name* { **permit** | **deny** } **node** *node-number*	必选 缺省情况下，不创建路由策略

5. 配置 if-match 子句

表1-61 配置 If-match 子句

操作	命令	说明
进入系统视图	**system-view**	-
进入路由策略视图	**route-policy** *route-policy-name* { **permit** | **deny** } **node** *node-number*	-
匹配 BGP 路由信息的 AS 路径域	**if-match as-path** *as-path-number*	可选
匹配 BGP 路由信息的团体属性	**if-match community** { *basic-community-number* [**whole-match**] | *adv-community-number* }	可选
匹配路由策略的 IP 地址范围	**if-match** { **acl** *acl-number* | **ip-prefix** *ip-prefix-name* }	可选 缺省情况下，不匹配路由策略的 IP 地址范围
匹配路由信息的路由开销	**if-match cost** *value*	可选 缺省情况下，不匹配路由信息的路由开销
匹配路由信息的出接口	**if-match interface** *interface-type interface-number*	可选 缺省情况下，不匹配路由信息的出接口
匹配路由信息下一跳	**if-match ip next-hop** { **acl** *acl-number* | **ip-prefix** *ip-prefix-name* }	可选 缺省情况下，不匹配路由信息下一跳地址
匹配 OSPF 路由信息的标记域	**if-match tag** *value*	可选 缺省情况下，不匹配 OSPF 路由信息的标记域

6. 配置 apply 子句

表1-62 配置 apply 子句

操作	命令	说明
进入系统视图	**system-view**	-

操作	命令	说明
进入路由策略视图	**route-policy** *route-policy-name* { **permit** | **deny** } **node** *node-number*	-
在 BGP 路由信息的 as-path 系列前加入指定的 AS 号	**apply as-path** *as-number-1* [*as-number-2* [*as-number-3* ...]]	可选
在 BGP 路由信息中配置团体属性	**apply community** { **none** | [*aa:nn*] [**no-export-subconfed** | **no-export** | **no-advertise**]* [**additive**] }	可选
配置路由信息的下一跳地址	**apply ip next-hop** *ip-address*	可选
配置 BGP 路由信息的本地优先级	**apply local-preference** *local-preference*	可选
配置路由信息的开销值	**apply cost** *value*	可选 缺省情况下，不配置路由信息的路由开销
配置路由信息的路由权类型	**apply cost-type** [**internal** | **external**]	可选
配置 BGP 路由信息的路由源	**apply origin** { **igp** | **egp** *as-number* | **incomplete** }	可选
配置路由信息的标记域	**apply tag** *value*	可选 缺省情况下，不配置 OSPF 路由信息的标记域

第2章 典型配置举例

说明：

典型配置举例以 S5600 系列交换机为准。

2.1 典型配置举例

2.1.1 静态路由典型配置

1. 组网需求

(1) 需求分析

某小型公司办公网络需要任意两个节点之间能够互通，网络结构简单、稳定，用户希望最大限度利用现有设备。用户现在拥有的设备不支持动态路由协议。

根据用户需求及用户网络环境，选择静态路由实现用户网络之间互通。

(2) 网络规划

根据用户需求，设计如 图 2-1所示网络拓扑图。

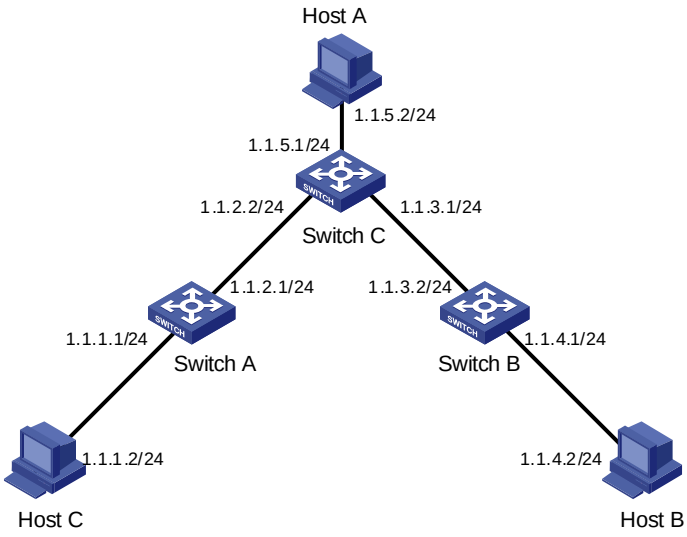


图2-1 静态路由配置举例组网图

2. 配置步骤

交换机上的配置步骤：

设置以太网交换机 Switch A 的静态路由。

```
<SwitchA> system-view
[SwitchA] ip route-static 1.1.3.0 255.255.255.0 1.1.2.2
[SwitchA] ip route-static 1.1.4.0 255.255.255.0 1.1.2.2
[SwitchA] ip route-static 1.1.5.0 255.255.255.0 1.1.2.2
```

设置以太网交换机 Switch B 的静态路由。

```
<SwitchB> system-view
[SwitchB] ip route-static 1.1.2.0 255.255.255.0 1.1.3.1
[SwitchB] ip route-static 1.1.5.0 255.255.255.0 1.1.3.1
[SwitchB] ip route-static 1.1.1.0 255.255.255.0 1.1.3.1
```

设置以太网交换机 Switch C 的静态路由。

```
<SwitchC> system-view
[SwitchC] ip route-static 1.1.1.0 255.255.255.0 1.1.2.1
[SwitchC] ip route-static 1.1.4.0 255.255.255.0 1.1.3.2
```

主机上的配置步骤：

在主机 A 上配缺省网关为 1.1.5.1，具体配置略。

在主机 B 上配缺省网关为 1.1.4.1，具体配置略。

在主机 C 上配缺省网关为 1.1.1.1，具体配置略。

至此图中所有主机或以太网交换机之间均能两两互通。

2.1.2 RIP 典型配置

1. 组网需求

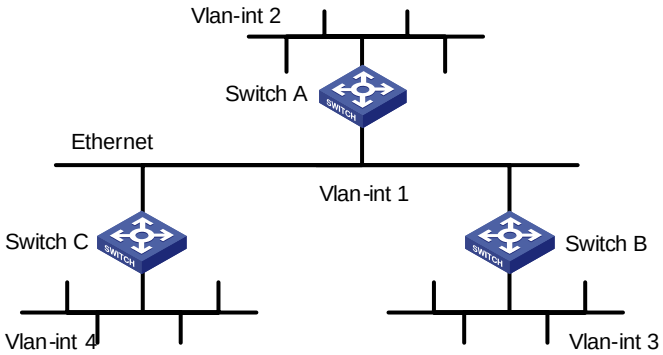
(1) 需求分析

某小型公司办公网络需要任意两个节点之间能够互通，网络规模比较小。需要设备自动适应网络拓扑变化，降低人工维护工作量。

根据用户需求及用户网络环境，选择 RIP 路由协议实现用户网络之间互通。

(2) 网络规划

根据用户需求，设计如 图 2-2所示网络拓扑图。



设备	接口	IP 地址	设备	接口	IP 地址
Switch A	Vlan-int1	110.11.2.1/24	Switch B	Vlan-int1	110.11.2.2/24
	Vlan-int2	155.10.1.1/24		Vlan-int3	196.38.165.1/24
Switch C	Vlan-int1	110.11.2.3/24			
	Vlan-int4	117.102.0.1/16			

图2-2 RIP 典型配置组网图

2. 配置步骤

📖 **说明：**

以下的配置，只列出了与 RIP 相关的操作。在进行下列配置之前，请先确保以太网链路层能够正常工作，且各 VLAN 接口 IP 地址已经配置完成。

(1) 配置 Switch A

配置 RIP。

```
<SwitchA> system-view
[SwitchA] rip
[SwitchA-rip] network 110.11.2.0
[SwitchA-rip] network 155.10.1.0
```

(2) 配置 Switch B

配置 RIP。

```
<SwitchB> system-view
[SwitchB] rip
[SwitchB-rip] network 196.38.165.0
[SwitchB-rip] network 110.11.2.0
```

(3) 配置 Switch C

配置 RIP。

```
<SwitchC> system-view
[SwitchC] rip
[SwitchC-rip] network 117.102.0.0
```

```
[SwitchC-rip] network 110.11.2.0
```

2.1.3 OSPF 的 DR 典型配置

1. 组网需求

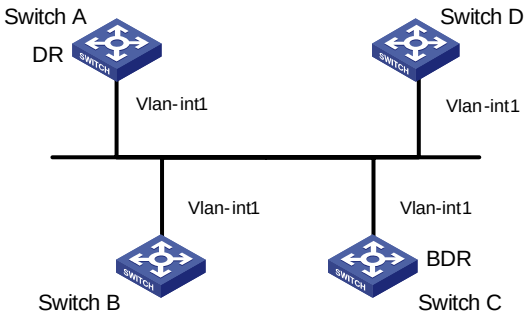
(1) 需求分析

某用户网络链路类型为广播型网络，通过 OSPF 实现网络之间互通。由于网络中设备性能有差异，希望 DR/BDR 由性能较高的设备承担，优化网络处理速度。对于网络中性能较低的设备，禁止其参加 DR/BDR 选举。

根据用户需求及其网络环境，通过修改接口优先级实现用户需求。

(2) 网络规划

根据用户需求，设计如 图 2-3所示网络拓扑图。



设备	接口	IP 地址	Router ID	接口优先级
Switch A	Vlan-int1	196.1.1.1/24	1.1.1.1	100
Switch B	Vlan-int1	196.1.1.2/24	2.2.2.2	0
Switch C	Vlan-int1	196.1.1.3/24	3.3.3.3	2
Switch D	Vlan-int1	196.1.1.4/24	4.4.4.4	1

图2-3 配置 OSPF 的 DR 选择组网图

2. 配置步骤

配置 Switch A

```
<SwitchA> system-view
[SwitchA] interface Vlan-interface 1
[SwitchA-Vlan-interface1] ip address 196.1.1.1 255.255.255.0
[SwitchA-Vlan-interface1] ospf dr-priority 100
[SwitchA-Vlan-interface1] quit
[SwitchA] router id 1.1.1.1
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 196.1.1.0 0.0.0.255
```

配置 Switch B

```
<SwitchB> system-view
```

```
[SwitchB] interface Vlan-interface 1
[SwitchB-Vlan-interface1] ip address 196.1.1.2 255.255.255.0
[SwitchB-Vlan-interface1] ospf dr-priority 0
[SwitchB-Vlan-interface1] quit
[SwitchB] router id 2.2.2.2
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 196.1.1.0 0.0.0.255
```

配置 Switch C

```
<SwitchC> system-view
[SwitchC] interface Vlan-interface 1
[SwitchC-Vlan-interface1] ip address 196.1.1.3 255.255.255.0
[SwitchC-Vlan-interface1] ospf dr-priority 2
[SwitchC-Vlan-interface1] quit
[SwitchC] router id 3.3.3.3
[SwitchC] ospf
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 196.1.1.0 0.0.0.255
```

配置 Switch D

```
<SwitchD> system-view
[SwitchD] interface Vlan-interface 1
[SwitchD-Vlan-interface1] ip address 196.1.1.4 255.255.255.0
[SwitchD-Vlan-interface1] quit
[SwitchD] router id 4.4.4.4
[SwitchD] ospf
[SwitchD-ospf-1] area 0
[SwitchD-ospf-1-area-0.0.0.0] network 196.1.1.0 0.0.0.255
```

在 Switch A 上运行 **display ospf peer** 来显示 OSPF 邻居，注意 Switch A 有三个邻居。

每个邻居的状态都是 full，这意味着 Switch A 与它的每个邻居都形成了邻接（Switch A 和 Switch C 必须与网络中的所有交换机形成邻接，才能分别充当网络的 DR 和 BDR）。Switch A 是网络中的 DR，而 Switch C 是 BDR。其它所有的邻居都是 DRother（这意味着它们既不是 DR，也不是 BDR）。

将 Switch B 的优先级改为 200

```
<SwitchB> system-view
[SwitchB] interface Vlan-interface 1
[SwitchB-Vlan-interface1] ospf dr-priority 200
```

在 Switch A 上运行 **display ospf peer** 来显示 OSPF 邻居，注意 Switch B 的优先级变为 200；但它并不是 DR。

只有当现在的 DR 不在网络上了后，DR 才会改变。关掉 Switch A，在 Switch D 上运行 **display ospf peer** 命令可显示邻居，注意本来是 BDR 的 Switch C 成为了 DR，并且 Switch B 现在成为了 BDR。

若网络中所有的交换机被移走后又重新加入，Switch B 就被选为 DR（优先级为 200），Switch A 成为了 BDR（优先级为 100）。关掉所有的交换机再重新启动，这个操作会带来一个新的 DR/BDR 选择。

2.1.4 OSPF 虚连接配置

1. 组网需求

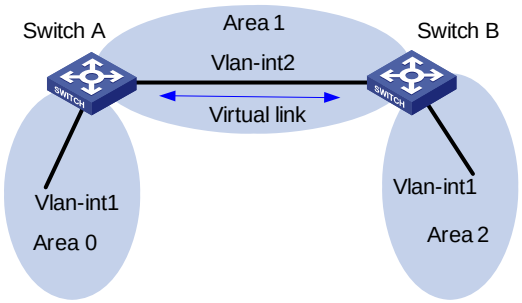
(1) 需求分析

用户网络运行 OSPF 实现网络互通。网络分为三个区域，一个骨干区域，两个普通区域（Area 1、Area 2）。其中某普通区域（Area 2）无法与骨干区域直接相连，只能通过另外一个普通区域（Area 1）接入。用户希望无法与骨干区域直接连接的普通区域（Area 2）能够与另外两个区域互通。

根据用户需求及用户网络环境，选择虚连接来实现普通区域（Area 2）与骨干区域之间的连接。

(2) 网络规划

根据用户需求，设计如 图 2-4所示网络拓扑图。



设备	接口	IP 地址	Router ID
Switch A	Vlan-int1	196.1.1.2/24	1.1.1.1
	Vlan-int2	197.1.1.2/24	-
Switch B	Vlan-int1	152.1.1.1/24	2.2.2.2
	Vlan-int2	197.1.1.1/24	-

图2-4 配置 OSPF 虚链路组网图

2. 配置步骤

(1) 配置 OSPF 基本功能

配置 Switch A。

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ip address 196.1.1.2 255.255.255.0
```

```
[SwitchA-Vlan-interface1] quit
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 197.1.1.2 255.255.255.0
[SwitchA-Vlan-interface2] quit
[SwitchA] router id 1.1.1.1
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 196.1.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[SwitchA-ospf-1] area 1
[SwitchA-ospf-1-area-0.0.0.1] network 197.1.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.1] quit
[SwitchA-ospf-1] quit
```

配置 Switch B。

```
<SwitchB> system-view
[SwitchB] interface Vlan-interface 1
[SwitchB-Vlan-interface1] ip address 152.1.1.1 255.255.255.0
[SwitchB-Vlan-interface1] quit
[SwitchB] interface Vlan-interface 2
[SwitchB-Vlan-interface2] ip address 197.1.1.1 255.255.255.0
[SwitchB-Vlan-interface2] quit
[SwitchB] router id 2.2.2.2
[SwitchB] ospf
[SwitchB-ospf-1] area 1
[SwitchB-ospf-1-area-0.0.0.1] network 197.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.1] quit
[SwitchB-ospf-1] area 2
[SwitchB-ospf-1-area-0.0.0.2] network 152.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.2] quit
```

显示 Switch A 的 OSPF 路由表。

```
[SwitchA] display ospf routing

                OSPF Process 1 with Router ID 1.1.1.1
                        Routing Tables

Routing for Network
Destination             Cost Type NextHop         AdvRouter        Area
196.1.1.0/24              10 Stub 196.1.1.2       1.1.1.1          0.0.0.0
197.1.1.0/24              10 Net  197.1.1.1       2.2.2.2          0.0.0.1

Total Nets: 2
```

```
  Intra Area: 2  Inter Area: 0  ASE: 0  NSSA: 0
```

📖 **说明：**

由于 Area2 没有与 Area0 直接相连，所以 Switch A 的路由表中没有 Area2 中的路由。

(2) 配置虚连接。

配置 Switch A。

```
[SwitchA] ospf
[SwitchA-ospf-1] area 1
[SwitchA-ospf-1-area-0.0.0.1] vlink-peer 2.2.2.2
[SwitchA-ospf-1-area-0.0.0.1] quit
[SwitchA-ospf-1] quit
```

配置 Switch B。

```
[SwitchB-ospf-1] area 1
[SwitchB-ospf-1-area-0.0.0.1] vlink-peer 1.1.1.1
[SwitchB-ospf-1-area-0.0.0.1] quit
```

显示 Switch A 的 OSPF 路由表。

```
[SwitchA]display ospf routing

                OSPF Process 1 with Router ID 1.1.1.1
                        Routing Tables

Routing for Network
Destination             Cost Type NextHop         AdvRouter        Area
196.1.1.0/24              10 Stub 196.1.1.2       1.1.1.1          0.0.0.0
197.1.1.0/24              10 Net  197.1.1.1       2.2.2.2          0.0.0.1
152.1.1.0/24              20 SNet 197.1.1.1       2.2.2.2          0.0.0.0

Total Nets: 3
  Intra Area: 2  Inter Area: 1  ASE: 0  NSSA: 0
```

可以看到，Switch A 已经学到了 Area2 的路由 152.1.1.0/24。

2.1.5 配置 BGP 联盟属性

1. 组网需求

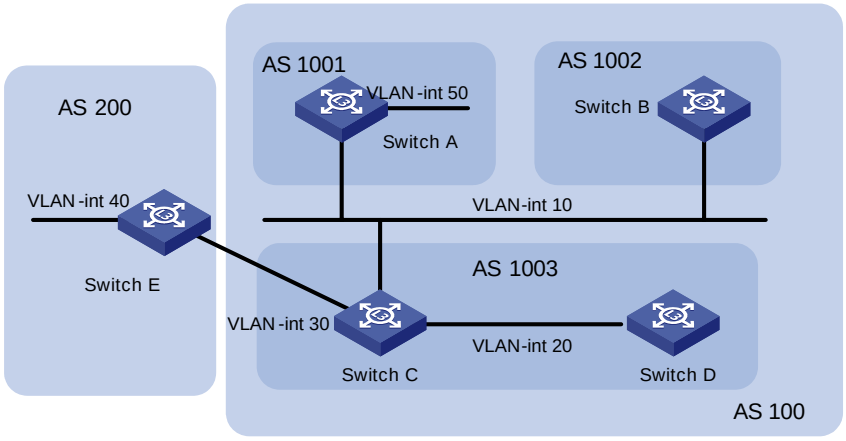
(1) 需求分析

某用户拥有一个大型 AS，AS 中运行 BGP 协议。随着 AS 规模的增长，IBGP 对等体数量激增，用于 BGP 通信的网络资源亦随之增加。用户希望不影响设备工作性能条件下，削减 IBGP 对等体数量，降低 BGP 对设备 CPU 和网络资源的消耗。

根据用户需求，选择应用 BGP 自治系统联盟属性实现用户需求。

(2) 网络规划

根据用户需求，设计如 图 2-5所示网络拓扑图。



设备	接口	IP 地址	AS
Switch A	Vlan-int 10	172.68.10.1/24	
	Vlan-int 50	10.1.1.1/24	
Switch B	Vlan-int 10	172.68.10.2/24	
Switch C	Vlan-int 10	172.68.10.3/24	100
	Vlan-int 20	172.68.1.1/24	
	Vlan-int 30	156.10.1.1/24	
Switch D	Vlan-int 20	172.68.1.2/24	
Switch E	Vlan-int 30	156.10.1.2/24	
	Vlan-int 40	8.1.1.1/24	200

图2-5 配置自治系统联盟的组网图

(3) 配置策略

- 将 AS 100 划分为三个子自治系统，分别为 AS 1001，AS 1002，AS 1003；
- AS 1001，AS 1002，AS 1003 之间运行 EBGP;
- AS 1001，AS 1002，AS 1003 内部建立全连接，运行 IBGP；
- AS 100，AS 200 之间运行 EBGP。

2. 配置步骤

配置 Switch A。

```
<SwitchA> system-view
[SwitchA] bgp 1001
[SwitchA-bgp] network 10.1.1.0 255.255.255.0
[SwitchA-bgp] confederation id 100
[SwitchA-bgp] confederation peer-as 1002 1003
[SwitchA-bgp] group confed1002 external
[SwitchA-bgp] peer 172.68.10.2 group confed1002 as-number 1002
[SwitchA-bgp] group confed1003 external
[SwitchA-bgp] peer 172.68.10.3 group confed1003 as-number 1003
[SwitchA-bgp] quit
```

配置 Switch B。

```
<SwitchB> system-view
[SwitchB] bgp 1002
[SwitchB-bgp] confederation id 100
[SwitchB-bgp] confederation peer-as 1001 1003
[SwitchB-bgp] group confed1001 external
[SwitchB-bgp] peer 172.68.10.1 group confed1001 as-number 1001
[SwitchB-bgp] group confed1003 external
[SwitchB-bgp] peer 172.68.10.3 group confed1003 as-number 1003
```

配置 Switch C。

```
<SwitchC> system-view
[SwitchC] bgp 1003
[SwitchC-bgp] confederation id 100
[SwitchC-bgp] confederation peer-as 1001 1002
[SwitchC-bgp] group confed1001 external
[SwitchC-bgp] peer 172.68.10.1 group confed1001 as-number 1001
[SwitchC-bgp] group confed1002 external
[SwitchC-bgp] peer 172.68.10.2 group confed1002 as-number 1002
[SwitchC-bgp] group ebgp200 external
[SwitchC-bgp] peer 156.10.1.2 group ebgp200 as-number 200
[SwitchC-bgp] group ibgp1003 internal
[SwitchC-bgp] peer 172.68.1.2 group ibgp1003
```

配置 Switch D。

```
<SwitchD> system-view
[SwitchD] bgp 1003
[SwitchD-bgp] confederation id 100
[SwitchD-bgp] group ibgp1003 internal
[SwitchD-bgp] peer 172.68.1.1 group ibgp1003
```

配置 Switch E。

```
<SwitchE> system-view
```

```
[SwitchE] bgp 200
[SwitchE-bgp] network 8.1.1.0 255.255.255.0
[SwitchE-bgp] group ebgp100 external
[SwitchE-bgp] peer 156.10.1.1 group ebgp100 as-number 100
[SwitchE-bgp] quit
```

显示 Switch E 的 BGP 路由表。

```
[SwitchE] display bgp routing

Flags:  # - valid       ^ - active      I - internal
        D - damped      H - history     S - aggregate suppressed

    Dest/Mask          Next-Hop        Med        Local-pref Origin Path
------------------------------------------------------------------------
--
#^  8.1.1.0/24         0.0.0.0         0          100         IGP
#^  10.1.1.0/24        156.10.1.1      0          100         IGP   100

  Routes total: 2
```

显示 Switch A 的 BGP 路由表。

```
[SwitchA] display bgp routing

Flags:  # - valid       ^ - active      I - internal
        D - damped      H - history     S - aggregate suppressed

    Dest/Mask       Next-Hop      Med      Local-pref  Origin  Path
------------------------------------------------------------------------
--
  I 8.1.1.0/24      156.10.1.2    0        100         IGP     (1003) 200
#^  10.1.1.0/24     0.0.0.0       0        100         IGP

  Routes total: 2
```

根据显示信息可以看出，子自治系统信息仅在联盟内部通告。处于联盟外部的自治系统的设备（例如 Switch E）将联盟作为一个自治系统，不能学习联盟内部的子自治系统信息。

2.1.6 配置 BGP 路由反射器

1. 组网需求

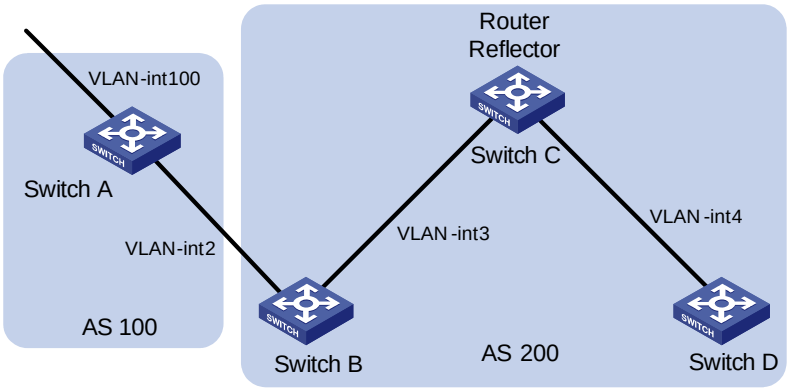
(1) 需求分析

某用户拥有一个大型 AS，AS 中运行 BGP 协议。随着 AS 规模的增长，IBGP 对等体数量激增，用于 BGP 通信的网络资源亦随之增加。用户希望不影响设备工作性能条件下，削减 IBGP 对等体数量，降低 BGP 对设备 CPU 和网络资源的消耗。另外，该 AS 中，IBGP 对等体之间连接采用部分互联。

根据用户需求和用户网络环境，选择 BGP 路由反射器方案满足用户需求。

(2) 网络规划

根据用户需求，设计如 图 2-6所示网络拓扑图。



设备	接口	IP 地址	AS
Switch A	Vlan-int 100	1.1.1.1/8	100
	Vlan-int 2	192.1.1.1/24	
Switch B	Vlan-int 2	192.1.1.2/24	
	Vlan-int 3	193.1.1.2/24	
Switch C	Vlan-int 3	193.1.1.1/24	200
	Vlan-int 4	194.1.1.1/24	
Switch D	Vlan-int 4	194.1.1.2/24	

图2-6 配置 BGP 路由反射器的组网图

(3) 配置策略

- AS 100 与 AS 200 对等体之间运行 EBGP，通告 1.0.0.0/8 网段；
- AS 200 中对等体之间运行 IBGP，AS 网络拓扑采用星型拓扑结构；中央设备作为路由反射器，其他设备作为客户机。

2. 配置步骤

(1) 配置 Switch A

```
<SwitchA> system-view
[SwitchA] interface Vlan-interface 2
[SwitchA-Vlan-interface2] ip address 192.1.1.1 255.255.255.0
```

```
[SwitchA-Vlan-interface2] interface Vlan-interface 100
[SwitchA-Vlan-interface100] ip address 1.1.1.1 255.0.0.0
[SwitchA-Vlan-interface100] quit
[SwitchA] bgp 100
[SwitchA-bgp] group ex external
[SwitchA-bgp] peer 192.1.1.2 group ex as-number 200
[SwitchA-bgp] network 1.0.0.0 255.0.0.0
```

(2) 配置 Switch B

配置 VLAN 接口的 IP 地址。

```
<SwitchB> system-view
[SwitchB] interface Vlan-interface 2
[SwitchB-Vlan-interface2] ip address 192.1.1.2 255.255.255.0
[SwitchB-Vlan-interface2] quit
[SwitchB] interface Vlan-interface 3
[SwitchB-Vlan-interface3] ip address 193.1.1.2 255.255.255.0
[SwitchB-Vlan-interface3] quit
```

配置 BGP 对等体。

```
[SwitchB] bgp 200
[SwitchB-bgp] group ex external
[SwitchB-bgp] peer 192.1.1.1 group ex as-number 100
[SwitchB-bgp] group in internal
[SwitchB-bgp] peer 193.1.1.1 group in
```

(3) 配置 Switch C

配置 VLAN 接口的 IP 地址。

```
<SwitchC> system-view
[SwitchC] interface Vlan-interface 3
[SwitchC-Vlan-interface3] ip address 193.1.1.1 255.255.255.0
[SwitchC-Vlan-interface3] quit
[SwitchC] interface vlan-Interface 4
[SwitchC-Vlan-interface4] ip address 194.1.1.1 255.255.255.0
[SwitchC-Vlan-interface4] quit
```

配置 BGP 对等体及路由反射器。

```
[SwitchC] bgp 200
[SwitchC-bgp] group rr internal
[SwitchC-bgp] peer rr reflect-client
[SwitchC-bgp] peer 193.1.1.2 group rr
[SwitchC-bgp] peer 194.1.1.2 group rr
```

(4) 配置 Switch D

配置 VLAN 接口的 IP 地址。

```
<SwitchD> system-view
[SwitchD] interface Vlan-interface 4
[SwitchD-Vlan-interface4] ip address 194.1.1.2 255.255.255.0
[SwitchD-Vlan-interface4] quit
```

配置 BGP 对等体。

```
[SwitchD] bgp 200
[SwitchD-bgp] group in internal
[SwitchD-bgp] peer 194.1.1.1 group in
```

在 Switch B 上用 **display bgp routing** 命令查看 BGP 路由表。注意：Switch B 已知道了网络 1.0.0.0 的存在。

在 Switch D 上用 **display bgp routing** 命令查看 BGP 路由表。注意：Switch D 也知道网络 1.0.0.0 的存在。

2.1.7 配置 BGP 路径选择

1. 组网需求

(1) 需求分析

某用户网络由两个 AS 组成，两个 AS 通过 BGP 实现网络互通，其中一个 AS 运行 OSPF。

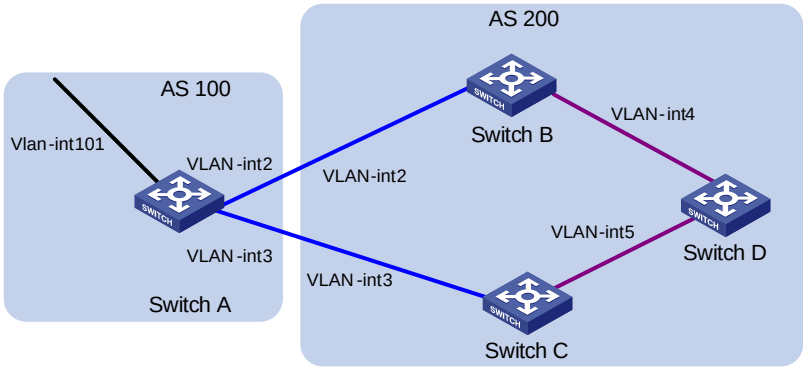
用户需求：控制从 AS 200 到 AS 100 的数据转发路径。

根据用户需求，可在如下方案中任选其一：

- 选择 BGP 的 MED 属性控制数据从 AS 200 到 AS 100 时的转发路径；
- 选择 BGP 的 LOCAL_PREF 属性控制数据从 AS 200 到 AS 100 时的转发路径。

(2) 网络规划

根据用户需求，设计如 图 2-7所示网络拓扑图。



设备	接口	IP 地址	AS
Switch A	Vlan-int 101	1.1.1.1/8	
	Vlan-int 2	192.1.1.1/24	100
	Vlan-int 3	193.1.1.1/24	
Switch B	Vlan-int 2	192.1.1.2/24	
	Vlan-int 4	194.1.1.2/24	
Switch C	Vlan-int 3	193.1.1.2/24	200
	Vlan-int 5	195.1.1.2/24	
Switch D	Vlan-int 4	194.1.1.1/24	
	Vlan-int 5	195.1.1.1/24	

图2-7 配置 BGP 路径选择的组网图

(3) 配置策略

- AS 100 与 AS 200 对等体之间运行 EBGP，通告 1.0.0.0/8 网段；
- AS 200 运行 OSPF 实现网络互通；
- Switch D 与 Switch B，Switch D 与 Switch C 对等体之间运行 IBGP；
- 在 Switch A 上应用路由策略，修改发布的路由信息 MED 属性，控制 Switch D 发出的数据进入 AS 100 时转发路径为：Switch D－Switch C－Switch A。
- 在 Switch C 上应用路由策略，修改发布路由信息的 LOCAL_PREF 属性，控制 Switch D 发出的数据进入 AS 100 时转发路径为：Switch D－Switch C－Switch A。

2. 配置步骤

(1) 配置 Switch A

配置 VLAN 接口的 IP 地址

```
<SwitchA> system-view
[SwitchA] interface Vlan-interface 2
[SwitchA-Vlan-interface2] ip address 192.1.1.1 255.255.255.0
[SwitchA-Vlan-interface2] quit
[SwitchA] interface Vlan-interface 3
[SwitchA-Vlan-interface3] ip address 193.1.1.1 255.255.255.0
[SwitchA-Vlan-interface3] quit
[SwitchA] interface Vlan-interface 101
```

```
[SwitchA-Vlan-interface101] ip address 1.1.1.1 255.0.0.0
[SwitchA-Vlan-interface101] quit
```

启动 BGP。

```
[SwitchA] bgp 100
```

通告 1.0.0.0/8 网段路由信息。

```
[SwitchA-bgp] network 1.0.0.0
```

配置对等体。

```
[SwitchA-bgp] group ex192 external
[SwitchA-bgp] peer 192.1.1.2 group ex192 as-number 200
[SwitchA-bgp] group ex193 external
[SwitchA-bgp] peer 193.1.1.2 group ex193 as-number 200
[SwitchA-bgp] quit
```

创建 ACL 2000，允许目的地址为 1.0.0.0/8 的路由信息通过。

```
[SwitchA] acl number 2000
[SwitchA-acl-basic-2000] rule permit source 1.0.0.0 0.255.255.255
[SwitchA-acl-basic-2000] rule deny source any
[SwitchA-acl-basic-2000] quit
```

创建路由策略 apply_med_50，匹配模式为允许，如果路由信息通过 ACL 2000 的过滤，则设置其 MED 值为 50。

```
[SwitchA] route-policy apply_med_50 permit node 10
[SwitchA-route-policy] if-match acl 2000
[SwitchA-route-policy] apply cost 50
[SwitchA-route-policy] quit
```

创建路由策略 apply_med_100，匹配模式为允许，如果路由信息通过 ACL 2000 的过滤，则设置其 MED 值为 100。

```
[SwitchA] route-policy apply_med_100 permit node 10
[SwitchA-route-policy] if-match acl 2000
[SwitchA-route-policy] apply cost 100
[SwitchA-route-policy] quit
```

对发布给对等体组 ex193（对等体 193.1.1.2）的路由信息应用路由策略 apply_med_50；对发布给对等体组 ex192（对等体 192.1.1.2）的路由信息应用路由策略 apply_med_100。

```
[SwitchA] bgp 100
[SwitchA-bgp] peer ex193 route-policy apply_med_50 export
[SwitchA-bgp] peer ex192 route-policy apply_med_100 export
```

(2) 配置 Switch B

配置 VLAN 接口 IP 地址。

```
<SwitchB> system-view
[SwitchB] interface vlan 2
[SwitchB-Vlan-interface2] ip address 192.1.1.2 255.255.255.0
[SwitchB-Vlan-interface2] quit
[SwitchB] interface Vlan-interface 4
[SwitchB-Vlan-interface4] ip address 194.1.1.2 255.255.255.0
[SwitchB-Vlan-interface4] quit
```

配置 OSPF。

```
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 194.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] network 192.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] quit
```

启动 BGP，创建对等体组，并向对等体组添加对等体。

```
[SwitchB] bgp 200
[SwitchB-bgp] undo synchronization
[SwitchB-bgp] group ex external
[SwitchB-bgp] peer 192.1.1.1 group ex as-number 100
[SwitchB-bgp] group in internal
[SwitchB-bgp] peer 194.1.1.1 group in
[SwitchB-bgp] peer 195.1.1.2 group in
```

(3) 配置 Switch C

配置 VLAN 接口 IP 地址。

```
<SwitchC> system-view
[SwitchC] interface Vlan-interface 3
[SwitchC-Vlan-interface3] ip address 193.1.1.2 255.255.255.0
[SwitchC-Vlan-interface3] quit
[SwitchC] interface Vlan-interface 5
[SwitchC-Vlan-interface5] ip address 195.1.1.2 255.255.255.0
[SwitchC-Vlan-interface5] quit
```

启动 OSPF。

```
[SwitchC] ospf
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 193.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] network 195.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] quit
```

```
[SwitchC-ospf-1] quit
```

启动 BGP，创建对等体组，并向对等体组添加对等体。

```
[SwitchC] bgp 200
[SwitchC-bgp] undo synchronization
[SwitchC-bgp] group ex external
[SwitchC-bgp] peer 193.1.1.1 group ex as-number 100
[SwitchC-bgp] group in internal
[SwitchC-bgp] peer 195.1.1.1 group in
[SwitchC-bgp] peer 194.1.1.2 group in
```

(4) 配置 Switch D

配置 VLAN 接口 IP 地址。

```
<SwitchD> system-view
[SwitchD] interface Vlan-interface 4
[SwitchD-Vlan-interface4] ip address 194.1.1.1 255.255.255.0
[SwitchD-Vlan-interface4] quit
[SwitchD] interface Vlan-interface 5
[SwitchD-Vlan-interface5] ip address 195.1.1.1 255.255.255.0
[SwitchD-Vlan-interface5] quit
```

启动 OSPF。

```
[SwitchD] ospf
[SwitchD-ospf-1] area 0
[SwitchD-ospf-1-area-0.0.0.0] network 194.1.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] network 195.1.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] network 4.0.0.0 0.255.255.255
[SwitchD-ospf-1-area-0.0.0.0] quit
[SwitchD-ospf-1] quit
```

启动 BGP，创建对等体组，并向对等体组添加对等体。

```
[SwitchD] bgp 200
[SwitchD-bgp] undo synchronization
[SwitchD-bgp] group in internal
[SwitchD-bgp] peer 195.1.1.2 group in
[SwitchD-bgp] peer 194.1.1.2 group in
```

为使配置生效，所有的 BGP 邻居需要运行 **reset bgp all** 命令。

- 通过上述配置后，由于 Switch C 学到的路由 1.0.0.0 的 MED 属性比 Switch B 学到的更小，Switch D 优选来自 Switch C 的路由 1.0.0.0。
- 如果在配置 Switch A 时，不配置 Switch A 的 MED 属性，而在 Switch C 上配置本地优先级如下：

创建 ACL 2000，允许目的地址为 1.0.0.0/8 的路由信息通过。

```
[SwitchC] acl number 2000
[SwitchC-acl-basic-2000] rule permit source 1.0.0.0 0.255.255.255
[SwitchC-acl-basic-2000] rule deny source any
[SwitchC-acl-basic-2000] quit
```

创建路由策略 localpref，节点序号为 10，匹配模式为允许，如果路由信息通过 ACL 2000 的过滤，则设置其本地优先级为 200。

```
[SwitchC] route-policy localpref  permit node 10
[SwitchC-route-policy] if-match acl 2000
[SwitchC-route-policy] apply local-preference 200
[SwitchC-route-policy] quit
```

创建路由策略 localpref，节点序号为 20，匹配模式为允许，设置路由信息本地优先级值为 100。

```
[SwitchC] route-policy localpref permit node 20
[SwitchC-route-policy] apply local-preference 100
[SwitchC-route-policy] quit
```

对从对等体 193.1.1.1（Switch A）接收的路由信息应用路由策略 localpref。

```
[SwitchC] bgp 200
[SwitchC-bgp] peer 193.1.1.1 route-policy localpref import
```

此时，由于 Switch C 学到的路由 1.0.0.0 的 LOCAL_PREF 属性值为 200，比 Switch B 学到的路由 1.0.0.0 的 LOCAL_PREF 属性值（Switch B 没有配置 LOCAL_PREF 属性，默认为 100）更大，Switch D 依然优选来自 Switch C 的路由 1.0.0.0。

第3章 综合配置举例

说明：

- 路由协议介绍请参见各产品操作手册;
- 配置中使用的命令请参见各产品命令手册;
- 本配置举例主要以 S3600、S5600 系列交换机为例，其他产品请参照使用。

3.1 组网需求

3.1.1 需求分析、网络规划及配置策略

1. 需求分析

某大型 ISP 运营商，拥有 4 个自治系统，分别是 AS 100、AS 200、AS 300、AS 400。AS 100 为核心层，连接 AS 200、AS 300、AS 400，转发他们之间的数据。AS 200、AS 300、AS 400 为分布层，对接入用户提供接入服务。具体需求如下：

- AS 200、AS 400 两个自治系统的网络拓扑比较复杂，网络规模较大，需要网络快速收敛。
- AS 300 自治系统网络拓扑简单，网络规模较小，网络中的设备仅支持 RIP 路由协议，而且设备的性能较低，路由表容量有限。
- AS 200 的接入用户需要高可靠性的网络。
- AS 200、AS 300、AS 400 中接入用户需要相互访问。
- AS 200 中 S200_10 下挂设备为二层设备。
- AS 300 中 S300_B 下挂设备为二层设备。
- AS 400 接入用户访问 AS 200、AS 300 时需要控制数据的转发路径。
- AS 300 接入用户只有单出口与 ISP 互连。

2. 网络规划

根据需求，设计如 图 3-1所示网络拓扑图。

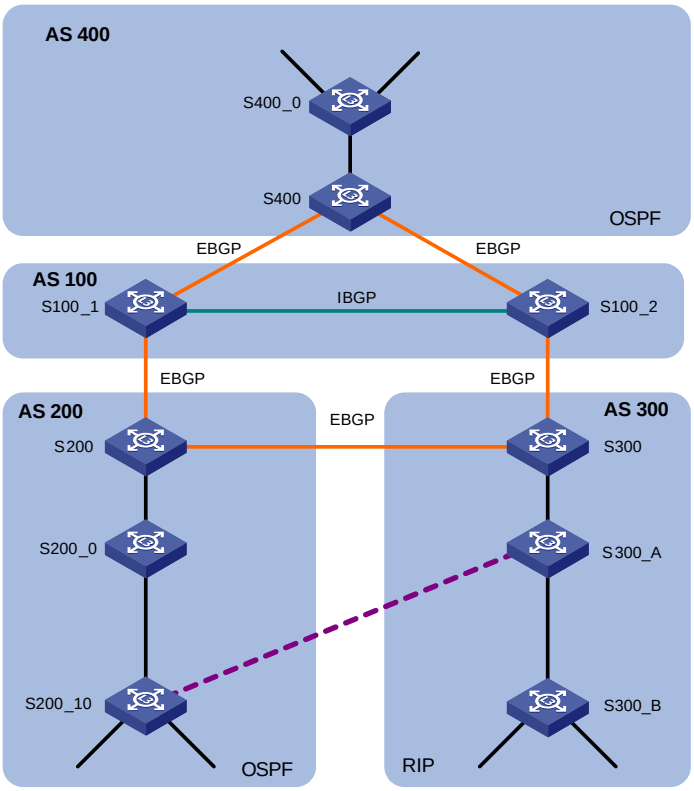


图3-1 配置组网图

3. 配置策略

- AS 100 选择 BGP，提供 AS 200、AS 300、AS 400 之间的互连。选择 BGP 的 MED 属性控制数据的转发路径。
- AS 200 选择 OSPF，AS 200 与 AS 100 互连设备同时运行 OSPF 和 BGP。选择静态路由作为备份路由，实现链路冗余，提高网络可靠性。引入 BGP 路由时应用路由策略，控制引入的路由信息。
- AS 400 选择 OSPF，AS 400 与 AS 100 互连设备同时运行 OSPF 和 BGP。引入 BGP 路由时应用路由策略，控制引入的路由信息。
- AS 300 选择 RIPv2，AS 300 与 AS 100 互连设备同时运行 RIPv2 和 BGP。引入 BGP 路由时应用路由策略，控制引入的路由信息。
- AS 300 用户使用静态路由、RIP、路由策略相结合的方式接入 ISP。
- 配置过程中涉及到了 IGP 与 BGP 的交互，由于 BGP 的缺省优先级为 256，当路由表中存在备份路由时，便于按需选择主路由，需要修改 BGP 优先级为适合的值。

3.1.2 组网中使用的产品

表3-1 产品型号与设备名称对应表

产品型号	设备名称
7500	S200/S300
5600	S100_1/S100_2/S400
3600	S200_0/S200_10/S300_A/S300_B/ S400_0

说明：

- 在本配置中，S100_1/S100_2/S400/S200/S300 既可以选择 S7500 系列以太网交换机，也可以选择 S5600 系列以太网交换机。
- S300_B 可以使用其它弱三层特性交换机替代。

3.1.3 设备运行的路由协议及相关参数

表3-2 设备与运行的路由协议对应表

设备名称	路由协议	Router ID	AS
S100_1	BGP(IBGP&EBGP)	1.1.1.1	100
S100_2	BGP(IBGP&EBGP)	1.2.1.1	
S200	BGP(EBGP)/OSPF	2.1.1.1	200
S200_0	OSPF	-	
S200_10	OSPF/STATIC		
S300	BGP(EBGP)/RIPv2	3.1.1.1	300
S300_A	RIPv2/STATIC	-	
S300_B	RIPv2		
S400	BGP(EBGP)/OSPF	4.1.1.1	400
S400_0	OSPF	-	

3.1.4 组网实现时使用的软件版本

S3600 系列使用的软件版本 Release 1510。

S5600 系列使用的软件版本 Release 1510。

S7500 系列使用的软件版本 Release 3130。

3.2 配置步骤

3.2.1 配置指南

表3-3 配置指南

配置任务	说明	详细配置
基本配置	创建 VLAN，配置 VLAN 接口 IP 地址	3.2.2
RIPv2/OSPF/BGP 基本配置	RIPv2、OSPF、BGP 基本配置	3.2.3
RIP＋静态路由＋路由策略	RIP 与路由策略结合，只发布不接收路由更新信息，通过静态路由实现对 ISP 的访问	3.2.4
IGP 与 BGP 交互	IGP 与 BGP 共享路由信息，当 IGP 引入 BGP 路由信息时，应用路由策略，按需引入路由信息	3.2.5
路由备份配置	为了提高接入用户的网络可靠性，接入的主链路运行 OSPF，备份链路选择静态路由，实现网络互连	3.2.6
BGP 的 MED 属性配置	应用路由策略，修改 BGP 的 MED 属性值，控制数据报文转发路径	3.2.7

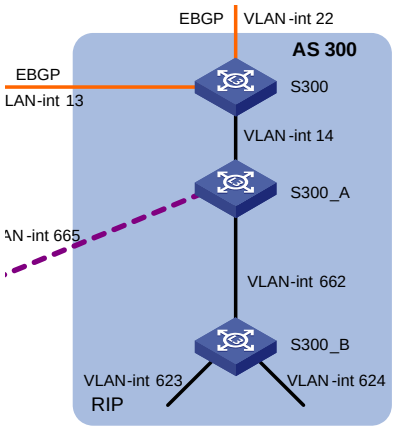
3.2.2 基本配置

创建 VLAN，配置 VLAN 接口 IP 地址，配置步骤略，请参见完整配置部分。

3.2.3 RIPv2/OSPF/BGP 基本配置

1. RIPv2 基本配置

AS 300 局部组网图如 图 3-2所示



设备	接口	IP 地址
S300	Vlan-int 14	206.1.4.2/24
S300_A	Vlan-int 14	206.1.4.1/24
	Vlan-int 662	166.1.2.1/24
	Vlan-int 665	166.1.5.2/24
S300_B	Vlan-int 662	166.1.2.2/24
	Vlan-int 623	162.1.3.1/24
	Vlan-int 624	162.1.4.1/24

图3-2 AS 300 局部组网图

- 配置 S300

配置网络地址为 206.1.4.0 的接口运行 RIP。

```
<S300> system-view
[S300] rip
[S300-rip] network 206.1.4.0
```

关闭 RIPv2 的路由聚合功能。

```
[S300-rip] undo summary
[S300-rip] quit
```

配置接口 Vlan-interface 14 运行 RIPv2。

```
[S300] interface vlan-interface 14
[S300-Vlan-interface14] rip version 2
[S300-Vlan-interface14] quit
```

- 配置 S300_A

配置网络地址为 206.1.4.0、166.1.0.0 的接口运行 RIP。

```
<S300_A> system-view
[S300_A] rip
[S300_A-rip] network 206.1.4.0
[S300_A-rip] network 166.1.0.0
```

关闭 RIPv2 的路由聚合功能。

```
[S300_A-rip] undo summary
[S300_A-rip] quit
```

配置接口 Vlan-interface 14、Vlan-interface 662 运行 RIPv2。

```
[S300_A] interface vlan-interface 14
[S300_A-Vlan-interface14] rip version 2
[S300_A-Vlan-interface14] quit
[S300_A] interface vlan-interface 662
[S300_A-Vlan-interface662] rip version 2
[S300_A-Vlan-interface662] quit
```

- 配置 S300_B

配置网络地址为 162.1.0.0、166.1.0.0 的接口运行 RIP。

```
<S300_B> system-view
[S300_B] rip
[S300_B-rip] network 162.1.0.0
[S300_B-rip] network 166.1.0.0
```

关闭 RIPv2 的路由聚合功能。

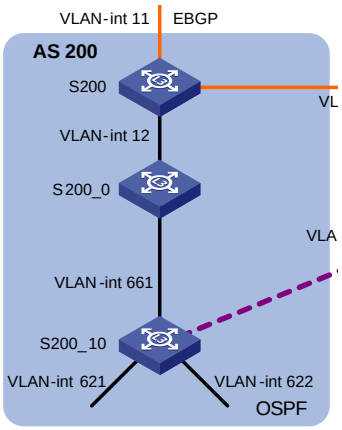
```
[S300_B-rip] undo summary
[S300_B-rip] quit
```

配置接口 Vlan-interface 623、Vlan-interface 624、Vlan-interface 662 运行 RIPv2。

```
[S300_B] interface vlan-interface 623
[S300_B-Vlan-interface623] rip version 2
[S300_B-Vlan-interface623] quit
[S300_B] interface vlan-interface 624
[S300_B-Vlan-interface624] rip version 2
[S300_B-Vlan-interface624] quit
[S300_B] interface vlan-interface 662
[S300_B-Vlan-interface662] rip version 2
[S300_B-Vlan-interface662] quit
```

2. OSPF 基本配置

AS 200 局部组网图如 图 3-3所示：



设备	接口	IP 地址	Area
S200	Vlan-int 12	206.1.2.3/24	0
S200_0	Vlan-int 12	206.1.2.1/24	0
	Vlan-int 661	166.1.1.1/24	10
S200_10	Vlan-int 661	166.1.1.2/24	10
	Vlan-int 621	162.1.1.1/24	10
	Vlan-int 622	162.1.2.1/24	10

图3-3 AS 200 局部组网图

- 配置 S200

指定运行 OSPF 协议的接口 IP 地址位于网段 206.1.2.0/24，接口所在的 OSPF 区域 ID 为 0。

```
<S200> system-view
[S200] ospf
[S200-ospf-1] area 0
[S200-ospf-1-area-0.0.0.0] network 206.1.2.0 0.0.0.255
```

- 配置 S200_0

指定运行 OSPF 协议的接口 IP 地址位于网段 206.1.2.0/24，接口所在的 OSPF 区域 ID 为 0。

```
<S200_0> system-view
[S200_0] ospf
[S200_0-ospf-1] area 0
[S200_0-ospf-1-area-0.0.0.0] network 206.1.2.0 0.0.0.255
[S200_0-ospf-1-area-0.0.0.0] quit
```

指定运行 OSPF 协议的接口 IP 地址位于网段 166.1.1.0/24，接口所在的 OSPF 区域 ID 为 10。

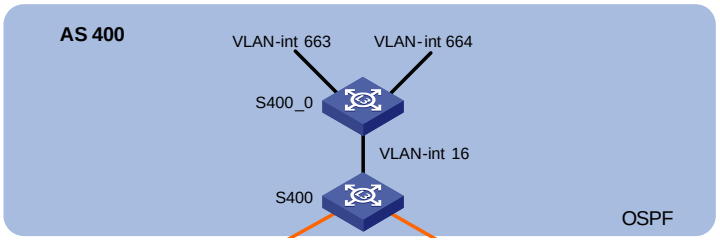
```
[S200_0-ospf-1] area 10
[S200_0-ospf-1-area-0.0.0.10] network 166.1.1.0 0.0.0.255
```

- 配置 S200_10

指定运行 OSPF 协议的接口 IP 地址位于网段 162.1.1.0/24、162.1.2.0/24、166.1.1.0/24，接口所在的 OSPF 区域 ID 为 10。

```
<S200_10> system-view
[S200_10] ospf
[S200_10-ospf-1] area 10
[S200_10-ospf-1-area-0.0.0.10] network 162.1.1.0 0.0.0.255
[S200_10-ospf-1-area-0.0.0.10] network 162.1.2.0 0.0.0.255
[S200_10-ospf-1-area-0.0.0.10] network 166.1.1.0 0.0.0.255
```

AS 400 局部组网图如 图 3-4所示：



设备	接口	IP 地址	Area
S400	Vlan-int 16	206.1.6.3/24	0
S400_0	Vlan-int 16	206.1.6.1/24	0
	Vlan-int 663	166.1.3.1/24	0.0.1.44
	Vlan-int 664	166.1.4.1/24	0.0.1.44

图3-4 AS 400 局部组网图

- 配置 S400

指定运行 OSPF 协议的接口 IP 地址位于网段 206.1.6.0/24，接口所在的 OSPF 区域 ID 为 0。

```
<S400> system-view
[S400] ospf
[S400-ospf-1] area 0
[S400-ospf-1-area-0.0.0.0] network 206.1.6.0 0.0.0.255
```

- 配置 S400_0

指定运行 OSPF 协议的接口 IP 地址位于网段 206.1.6.0/24，接口所在的 OSPF 区域 ID 为 0。

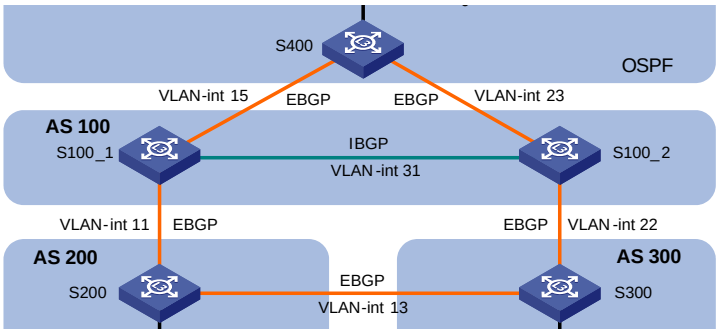
```
<S400_0> system-view
[S400_0] ospf
[S400_0-ospf-1] area 0
[S400_0-ospf-1-area-0.0.0.0] network 206.1.6.0 0.0.0.255
[S400_0-ospf-1-area-0.0.0.0] quit
```

指定运行 OSPF 协议的接口 IP 地址位于网段 166.1.3.0/24、166.1.4.0/24，接口所在的 OSPF 区域 ID 为 0.0.1.44。

```
[S400_0-ospf-1] area 0.0.1.44
[S400_0-ospf-1-area-0.0.1.44] network 166.1.3.0 0.0.0.255
[S400_0-ospf-1-area-0.0.1.44] network 166.1.4.0 0.0.0.255
```

3. BGP 基本配置

局部组网图如 图 3-5所示：



设备	接口	IP 地址	Router ID	AS
S100_1	Vlan-int 11	196.1.1.1/24	1.1.1.1	100
	Vlan-int 15	196.1.3.1/24		
	Vlan-int 31	196.3.1.1/24		
S100_2	Vlan-int 22	196.2.2.1/24	1.2.1.1	
	Vlan-int 23	196.2.3.2/24		
	Vlan-int 31	196.3.1.2/24		
S200	Vlan-int 11	196.1.1.3/24	2.1.1.1	200
	Vlan-int 13	206.1.3.3/24		
S300	Vlan-int 22	196.2.2.2/24	3.1.1.1	300
	Vlan-int 13	206.1.3.2/24		
S400	Vlan-int 15	196.1.3.3/24	4.1.1.1	400
	Vlan-int 23	196.2.3.3/24		

图3-5 局部组网图

- 配置 S100_1

配置 S100_1 的 Router ID 1.1.1.1。

```
<S100_1> system-view
[S100_1] router id 1.1.1.1
```

启动 BGP，本地 AS 号为 100。

```
[S100_1] bgp 100
```

创建 IBGP 对等体组 100；创建 EBGP 对等体组 200、400。

```
[S100_1-bgp] group 100 internal
[S100_1-bgp] group 200 external
[S100_1-bgp] group 400 external
```

将 IP 地址为 196.3.1.2 对等体加入到对等体组 100 中，AS 号为 100；IP 地址为 196.1.1.3 对等体加入到对等体组 200 中，AS 号为 200；；IP 地址为 196.1.3.3 对等体加入到对等体组 400 中，AS 号为 400。

```
[S100_1-bgp] peer 196.3.1.2 group 100
[S100_1-bgp] peer 196.1.1.3 group 200 as-number 200
[S100_1-bgp] peer 196.1.3.3 group 400 as-number 400
```

通告到达 196.1.3.0、196.3.1.0、196.1.1.0 网段的路由。

```
[S100_1-bgp] network 196.1.3.0
[S100_1-bgp] network 196.3.1.0
[S100_1-bgp] network 196.1.1.0
```

配置 EBGP、IBGP 和本地生成路由的优先级都为 200。

```
[S100_1-bgp] preference 200 200 200
```

- 配置 S100_2

配置 S100_2 的 Router ID 1.2.1.1。

```
<S100_2> system-view
[S100_2] router id 1.2.1.1
```

启动 BGP，本地 AS 号为 100。

```
[S100_2] bgp 100
```

创建 IBGP 对等体组 100；创建 EBGP 对等体组 300、400。

```
[S100_2-bgp] group 100 internal
[S100_2-bgp] group 300 external
[S100_2-bgp] group 400 external
```

将 IP 地址为 196.3.1.1 对等体加入到对等体组 100 中，AS 号为 100；IP 地址为 196.2.2.2 对等体加入到对等体组 300 中，AS 号为 300；；IP 地址为 196.2.3.3 对等体加入到对等体组 400 中，AS 号为 400。

```
[S100_2-bgp] peer 196.3.1.1 group 100
[S100_2-bgp] peer 196.2.2.2 group 300 as-number 300
[S100_2-bgp] peer 196.2.3.3 group 400 as-number 400
```

通告到达 196.2.2.0、196.2.3.0、196.3.1.0 网段的路由。

```
[S100_2-bgp] network 196.2.2.0
[S100_2-bgp] network 196.2.3.0
[S100_2-bgp] network 196.3.1.0
```

配置 EBGP、IBGP 和本地生成路由的优先级都为 200。

```
[S100_2-bgp] preference 200 200 200
```

- 配置 S200

配置 S200 的 Router ID 2.1.1.1。

```
<S200> system-view
[S200] router id 2.1.1.1
```

启动 BGP，本地 AS 号为 200。

```
[S200] bgp 200
```

创建 EBGP 对等体组 100、300。

```
[S200-bgp] group 100 external
[S200-bgp] group 300 external
```

将 IP 地址为 196.1.1.1 对等体加入到对等体组 100 中，AS 号为 100；IP 地址为 206.1.3.2 对等体加入到对等体组 300 中，AS 号为 300。

```
[S200-bgp] peer 196.1.1.1 group 100 as-number 100
[S200-bgp] peer 206.1.3.2 group 300 as-number 300
```

通告到达 192.1.1.0、206.1.3.0 网段的路由。

```
[S200-bgp] network 192.1.1.0
[S200-bgp] network 206.1.3.0
```

配置 EBGP、IBGP 和本地生成路由的优先级都为 200。

```
[S200-bgp] preference 200 200 200
```

- 配置 S300

配置 S300 的 Router ID 3.1.1.1。

```
<S300> system-view
[S300] router id 3.1.1.1
```

启动 BGP，本地 AS 号为 300。

```
[S300] bgp 300
```

创建 EBGP 对等体组 100、200。

```
[S300-bgp] group 100 external
[S300-bgp] group 200 external
```

将 IP 地址为 196.2.2.1 对等体加入到对等体组 100 中，AS 号为 100；IP 地址为 206.1.3.3 对等体加入到对等体组 200 中，AS 号为 200。

```
[S300-bgp] peer 196.2.2.1 group 100 as-number 100
[S300-bgp] peer 206.1.3.3 group 200 as-number 200
```

通告到达 206.1.3.0、196.2.2.0 网段的路由。

```
[S300-bgp] network 206.1.3.0
[S300-bgp] network 196.2.2.0
```

配置 EBGP、IBGP 和本地生成路由的优先级都为 200。

```
[S300-bgp] preference 200 200 200
```

- 配置 S400

配置 S400 的 Router ID 为 4.1.1.1。

```
<S400> system-view
[S400] router id 4.1.1.1
```

启动 BGP，本地 AS 号为 400。

```
[S400] bgp 400
```

创建 EBGP 对等体组 100_1、100_2。

```
[S400-bgp] group 100_1 external
```

```
[S400-bgp] group 100_2 external
```

将 IP 地址为 196.1.3.1 对等体加入到对等体组 100_1 中，IP 地址为 196.2.3.2 对等体加入到对等体组 100_2 中，AS 号都为 100。

```
[S400-bgp] peer 196.1.3.1 group 100_1 as-number 100
[S400-bgp] peer 196.2.3.2 group 100_2 as-number 100
```

通告到达 196.1.3.0、196.2.3.0 网段的路由。

```
[S400-bgp] network 196.1.3.0
[S400-bgp] network 196.2.3.0
```

配置 EBGP、IBGP 和本地生成路由的优先级都为 200。

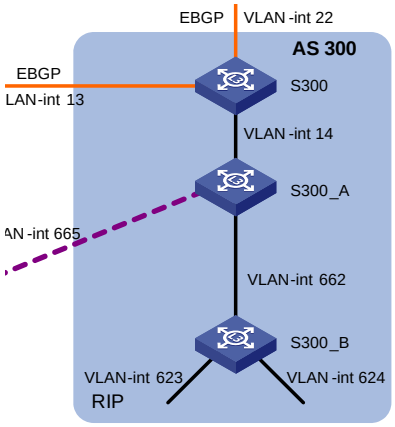
```
[S400-bgp] preference 200 200 200
```

3.2.4 RIP＋静态路由＋路由策略配置

1. 组网需求

如 图 3-6所示，S300_A/S300_B运行RIPv2。为了控制S300_B通过RIP学习到的路由数量，允许S300_B向S300_A发布路由信息，禁止S300_B接收S300_A发布的路由信息。S300_B到S300_A的报文转发通过缺省路由实现。

2. 组网图



设备	接口	IP 地址
S300_A	Vlan-int 662	166.1.2.1/24
S300_B	Vlan-int 662	166.1.2.2/24
	Vlan-int 623	162.1.3.1/24
	Vlan-int 624	162.1.4.1/24

图3-6 RIP＋静态路由＋路由策略配置组网图

3. 配置步骤

创建编号为 2000 的 ACL，拒绝所有的报文。

```
<S300_B> system-view
[S300_B]acl number 2000
```

```
[S300_B-acl-basic-2000] rule deny source any
[S300_B-acl-basic-2000] quit
```

在 RIP 进程中，对接收的路由信息应用 ACL 2000。

```
[S300_B] rip
[S300_B-rip] filter-policy 2000 import
```

配置缺省路由，下一跳 IP 地址为 166.1.2.1。

```
[S300_B] ip route-static 0.0.0.0 0.0.0.0 166.1.2.1 preference 60
```

3.2.5 IGP 与 BGP 交互配置

1. 组网需求

如 图 3-7所示，S400/S200 上运行OSPF和BGP，S300 上运行RIPv2 和BGP。为了保证各个AS的设备学习到其它AS的网络拓扑，配置IGP与BGP交互，共享路由信息。在IGP引入BGP的过程中，应用路由策略，仅引入前缀IP地址为如下的路由：162.1.1.0/24 、 162.1.2.0/24 、 162.1.3.0/24 、 162.1.4.0/24 、 166.1.3.0/24 、 166.1.4.0/24。

2. 组网图

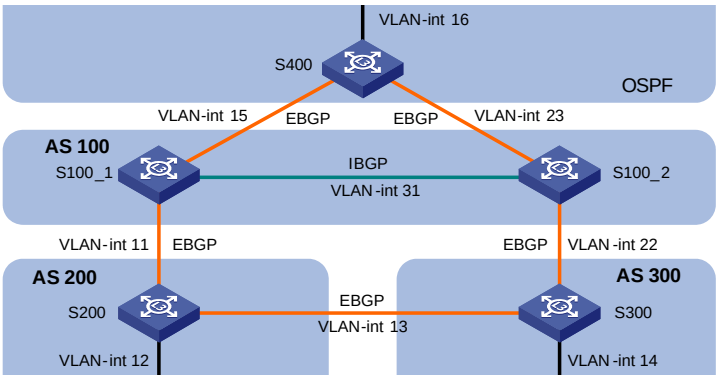


图3-7 IGP 与 BGP 交互配置组网图

3. 配置步骤

- 在 S200 上配置 IGP 与 BGP 交互

BGP 引入 OSPF

```
<S200> system-view
[S200] bgp 200
[S200-bgp] import-route ospf 1
[S200-bgp] quit
```

定义前缀列表 ospf_import，允许前缀 IP 地址为 162.1.3.0/24、162.1.4.0/24、166.1.3.0/24、166.1.4.0/24 的路由信息通过。

```
[S200] ip ip-prefix ospf_import index 10 permit 162.1.3.0 24
[S200] ip ip-prefix ospf_import index 20 permit 162.1.4.0 24
[S200] ip ip-prefix ospf_import index 30 permit 166.1.4.0 24
[S200] ip ip-prefix ospf_import index 40 permit 166.1.3.0 24
```

创建路由策略 ospf_import，匹配模式为允许，定义 if-match 子句，允许路由目的地址与前缀列表 ospf_import 匹配的路由信息通过。

```
[S200] route-policy ospf_import permit node 10
[S200-route-policy] if-match ip-prefix ospf_import
[S200-route-policy] quit
```

OSPF 引入 BGP，应用路由策略 ospf_import。

```
[S200] ospf
[S200-ospf-1] import-route bgp route-policy ospf_import
```

- 在 S300 上配置 IGP 与 BGP 交互

BGP 引入 RIP。

```
<S300> system-view
[S300] bgp 300
[S300-bgp] import-route rip
[S300-bgp] quit
```

定义前缀列表 rip_import，允许前缀 IP 地址为 162.1.1.0/24、162.1.2.0/24、166.1.3.0/24、166.1.4.0/24 的路由信息通过。

```
[S300] ip ip-prefix rip_import index 10 permit 162.1.1.0 24
[S300] ip ip-prefix rip_import index 20 permit 162.1.2.0 24
[S300] ip ip-prefix rip_import index 30 permit 166.1.3.0 24
[S300] ip ip-prefix rip_import index 40 permit 166.1.4.0 24
```

创建路由策略 rip_import，匹配模式为允许，定义 if-match 子句，允许路由目的地址与前缀列表 rip_import 匹配的路由信息通过。

```
[S300] route-policy rip_import permit node 10
[S300-route-policy] if-match ip-prefix rip_import
[S300-route-policy] quit
```

RIP 引入 BGP，应用路由策略 rip_import。

```
[S300] rip
[S300-rip] import-route bgp route-policy rip_import
```

- 在 S400 上配置 IGP 与 BGP 交互

BGP 引入 OSPF。

```
<S400> system-view
[S400] bgp 400
[S400-bgp] import-route ospf 1
```

```
[S400-bgp] quit
```

定义前缀列表 ospf_import，允许前缀 IP 地址为 162.1.1.0/24、162.1.2.0/24、162.1.3.0/24、162.1.4.0/24 的路由信息通过。

```
[S400] ip ip-prefix ospf_import index 10 permit 162.1.1.0 24
[S400] ip ip-prefix ospf_import index 20 permit 162.1.2.0 24
[S400] ip ip-prefix ospf_import index 30 permit 162.1.3.0 24
[S400] ip ip-prefix ospf_import index 40 permit 162.1.4.0 24
```

创建路由策略 ospf_import，匹配模式为允许，定义 if-match 子句，允许路由目的地址与前缀列表 ospf_import 匹配的路由信息通过。

```
[S400] route-policy ospf_import permit node 10
[S400-route-policy] if-match ip-prefix ospf_import
[S400-route-policy] quit
```

OSPF 引入 BGP，应用路由策略 ospf_import。

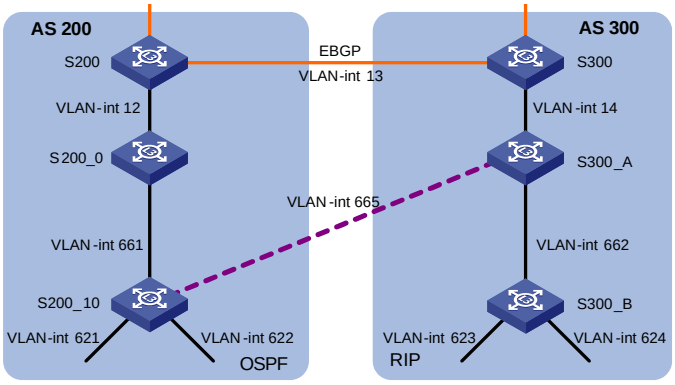
```
[S400] ospf
[S400-ospf-1] import-route bgp route-policy ospf_import
```

3.2.6 路由备份配置

1. 组网需求

如 图 3-8所示，S200_10 上实现路由备份。S200_10 与S200_0 之间运行OSPF，该路由为主路由，S200_10 与S300_A之间配置缺省路由，该路由为备份路由。当 S200_10 的主路由无法工作时，自动切换为备份路由。当主路由恢复正常时，自动从备份路由切换到主路由。配合S200_10 实现备份路由，在S300_A上配置静态路由，将该静态路由引入到RIPv2。

2. 组网图



设备	接口	IP 地址	AS
S300_A	Vlan-int 665	166.1.5.2/24	300
S200_10	Vlan-int 665	166.1.5.1/24	
	Vlan-int 621	162.1.1.1/24	200
	Vlan-int 622	162.1.2.1/24	

图3-8 路由备份配置组网图

3. 配置步骤

在 S200_10 上配置静态缺省路由，下一跳 IP 地址为 166.1.5.2，缺省优先级为 200。

```
<S200_10> system-view
[S200_10] ip route-static 0.0.0.0 0.0.0.0 166.1.5.2 preference 200
```

在 S300_A 上配置静态路由，目的地址为 162.1.1.0/24、162.1.2.0/24，下一跳 IP 地址为 166.1.5.1，缺省优先级为 200。

```
<S300_A> system-view
[S300_A] ip route-static 162.1.1.0 255.255.255.0 166.1.5.1 preference 200
[S300_A] ip route-static 162.1.2.0 255.255.255.0 166.1.5.1 preference 200
```

在 RIP 进程中引入静态路由。

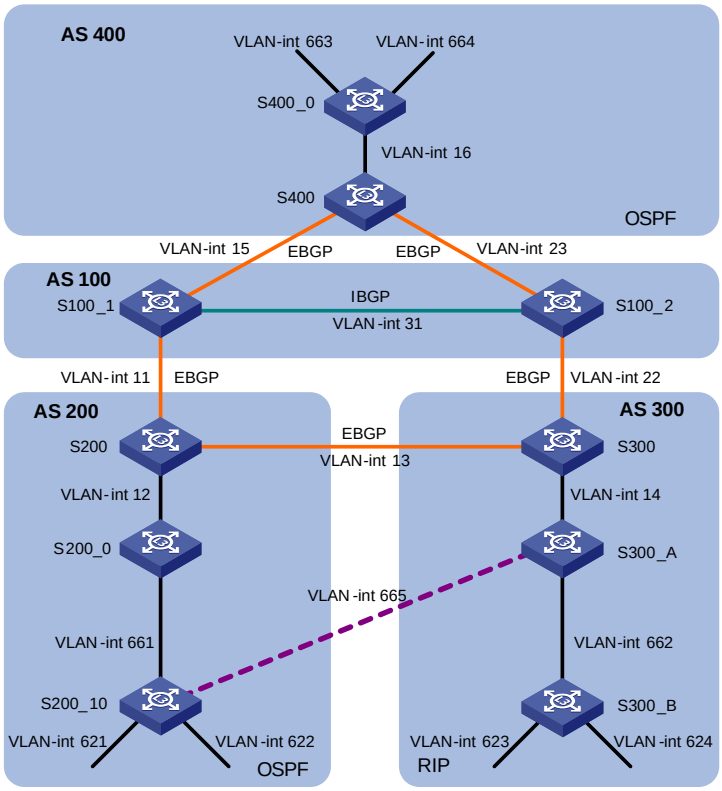
```
[S300_A] rip
[S300_A-rip] import-route static
```

3.2.7 BGP 的 MED 属性配置

1. 组网需求

如 图 3-9所示，从S400 到S200_10 的报文由S100_1 转发，从S400 到S300_B的报文由S100_2 转发，通过修改BGP属性中的MED值实现该目标。

2. 组网图



设备	接口	IP 地址	AS
S200_10	Vlan-int 621	162.1.1.1/24	200
	Vlan-int 622	162.1.2.1/24	
S300_B	Vlan-int 623	162.1.3.1/24	300
	Vlan-int 624	162.1.4.1/24	
S400_0	Vlan-int 663	166.1.3.1/24	400
	Vlan-int 664	166.1.4.1/24	

图3-9 BGP 的 MED 属性配置组网图

3. 配置步骤

- S100_1 的配置

定义前缀列表 as200_1，允许前缀 IP 地址为 162.1.1.0/24 的路由信息通过。

```
<S100_1> system-view
[S100_1] ip ip-prefix as200_1 index 10 permit 162.1.1.0 24
```

定义前缀列表 as200_2，允许前缀 IP 地址为 162.1.2.0/24 的路由信息通过。

```
[S100_1] ip ip-prefix as200_2 index 10 permit 162.1.2.0 24
```

定义前缀列表 as300_1，允许前缀 IP 地址为 162.1.3.0/24 的路由信息通过。

```
[S100_1] ip ip-prefix as300_1 index 10 permit 162.1.3.0 24
```

定义前缀列表 as300_2，允许前缀 IP 地址为 162.1.4.0/24 的路由信息通过。

```
[S100_1] ip ip-prefix as300_2 index 10 permit 162.1.4.0 24
```

定义前缀列表 other，允许所有的路由信息通过。

```
[S100_1] ip ip-prefix other index 10 permit 0.0.0.0 0 less-equal 32
```

创建路由策略 as200，节点序号为 10，匹配模式为允许。如果路由信息通过前缀列表 as200_1 过滤，则设置其 MED 值为 100。

```
[S100_1] route-policy as200 permit node 10
[S100_1-route-policy] if-match ip-prefix as200_1
[S100_1-route-policy] apply cost 100
[S100_1-route-policy] quit
```

创建路由策略 as200，节点序号为 20，匹配模式为允许。如果路由信息通过前缀列表 as200_2 过滤，则设置其 MED 值为 100。

```
[S100_1] route-policy as200 permit node 20
[S100_1-route-policy] if-match ip-prefix as200_2
[S100_1-route-policy] apply cost 100
[S100_1-route-policy] quit
```

创建路由策略 as200，节点序号为 30，匹配模式为允许。如果路由信息通过前缀列表 as300_1 过滤，则设置其 MED 值为 200。

```
[S100_1] route-policy as200 permit node 30
[S100_1-route-policy] if-match ip-prefix as300_1
[S100_1-route-policy] apply cost 200
[S100_1-route-policy] quit
```

创建路由策略 as200，节点序号为 40，匹配模式为允许。如果路由信息通过前缀列表 as300_2 过滤，则设置其 MED 值为 200。

```
[S100_1] route-policy as200 permit node 40
[S100_1-route-policy] if-match ip-prefix as300_2
[S100_1-route-policy] apply cost 200
[S100_1-route-policy] quit
```

创建路由策略 as200，节点序号为 50，匹配模式为允许，允许所有的路由信息通过。

```
[S100_1] route-policy as200 permit node 50
[S100_1-route-policy] if-match ip-prefix other
[S100_1-route-policy] quit
```

对发布给对等体组 400（实质上是发布给对等体 196.1.3.3）的路由信息应用路由策略 as200。

```
[S100_1] bgp 100
[S100_1-bgp] peer 400 route-policy as200 export
```

- S100_2 的配置

定义前缀列表 as200_1，允许前缀 IP 地址为 162.1.1.0/24 的路由信息通过。

```
<S100_2> system-view
[S100_2] ip ip-prefix as200_1 index 10 permit 162.1.1.0 24
```

定义前缀列表 as200_2，允许前缀 IP 地址为 162.1.2.0/24 的路由信息通过。

```
[S100_2] ip ip-prefix as200_2 index 10 permit 162.1.2.0 24
```

定义前缀列表 as300_1，允许前缀 IP 地址为 162.1.3.0/24 的路由信息通过。

```
[S100_2] ip ip-prefix as300_1 index 10 permit 162.1.3.0 24
```

定义前缀列表 as300_2，允许前缀 IP 地址为 162.1.4.0/24 的路由信息通过。

```
[S100_2] ip ip-prefix as300_2 index 10 permit 162.1.4.0 24
```

定义前缀列表 other，允许所有的路由信息通过。

```
[S100_2] ip ip-prefix other index 10 permit 0.0.0.0 0 less-equal 32
```

创建路由策略 as300，节点序号为 10，匹配模式为允许。如果路由信息通过前缀列表 as200_1 过滤，则设置其 MED 值为 200。

```
[S100_2] route-policy as300 permit node 10
[S100_2-route-policy] if-match ip-prefix as200_1
[S100_2-route-policy] apply cost 200
[S100_2-route-policy] quit
```

创建路由策略 as300，节点序号为 20，匹配模式为允许。如果路由信息通过前缀列表 as200_2 过滤，则设置其 MED 值为 200。

```
[S100_2] route-policy as300 permit node 20
[S100_2-route-policy] if-match ip-prefix as200_2
[S100_2-route-policy] apply cost 200
[S100_2-route-policy] quit
```

创建路由策略 as300，节点序号为 30，匹配模式为允许。如果路由信息通过前缀列表 as300_1 过滤，则设置其 MED 值为 100。

```
[S100_2] route-policy as300 permit node 30
[S100_2-route-policy] if-match ip-prefix as300_1
[S100_2-route-policy] apply cost 100
[S100_2-route-policy] quit
```

创建路由策略 as300，节点序号为 40，匹配模式为允许。如果路由信息通过前缀列表 as300_2 过滤，则设置其 MED 值为 100。

```
[S100_2] route-policy as300 permit node 40
[S100_2-route-policy] if-match ip-prefix as300_2
[S100_2-route-policy] apply cost 100
[S100_2-route-policy] quit
```

创建路由策略 as300，节点序号为 50，匹配模式为允许，允许所有的路由信息通过。

```
[S100_2] route-policy as300 permit node 50
[S100_2-route-policy] if-match ip-prefix other
[S100_2-route-policy] quit
```

对发布给对等体组 400（实质上是发布给对等体 196.2.3.3）的路由信息应用路由策略 as300。

```
[S100_2] bgp 100
[S100_2-bgp] peer 400 route-policy as300 export
```

3.3 完整配置

3.3.1 设备完整配置

1. S100_1

```
<S100_1> display current-configuration
#
 sysname S100_1
#
 router id 1.1.1.1
#
……
#
vlan 11
#
vlan 15
#
vlan 31
#
interface Vlan-interface11
 ip address 196.1.1.1 255.255.255.0
#
interface Vlan-interface15
 ip address 196.1.3.1 255.255.255.0
#
interface Vlan-interface31
 ip address 196.3.1.1 255.255.255.0
#
……
#
 undo fabric-port Cascade1/2/1 enable
 undo fabric-port Cascade1/2/2 enable
#
```

```
interface NULL0
#
bgp 100
 network 196.1.3.0
 network 196.3.1.0
 network 196.1.1.0
 undo synchronization
 group 100 internal
 peer 196.3.1.2 group 100
 group 200 external
 peer 196.1.1.3 group 200 as-number 200
 group 400 external
 peer 400 route-policy as200 export
 peer 196.1.3.3 group 400 as-number 400
 preference 200 200 200
#
route-policy as200 permit node 10
 if-match ip-prefix as200_1
 apply cost 100
route-policy as200 permit node 20
 if-match ip-prefix as200_2
 apply cost 100
route-policy as200 permit node 30
 if-match ip-prefix as300_1
 apply cost 200
route-policy as200 permit node 40
 if-match ip-prefix as300_2
 apply cost 200
route-policy as200 permit node 50
 if-match ip-prefix other
#
 ip ip-prefix as200_1 index 10 permit 162.1.1.0 24
 ip ip-prefix as200_2 index 10 permit 162.1.2.0 24
 ip ip-prefix as300_1 index 10 permit 162.1.3.0 24
 ip ip-prefix as300_2 index 10 permit 162.1.4.0 24
 ip ip-prefix other index 10 permit 0.0.0.0 0 less-equal 32
#
…
```

2. S100_2

```
<S100_2> display current-configuration
#
```

```
 sysname S100_2
#
 router id 1.2.1.1
#
……
#
vlan 22
#
vlan 23
#
vlan 31
#
interface Vlan-interface22
 ip address 196.2.2.1 255.255.255.0
#
interface Vlan-interface23
 ip address 196.2.3.2 255.255.255.0
#
interface Vlan-interface31
 ip address 196.3.1.2 255.255.255.0
#
……
#
interface Cascade1/2/1
#
interface Cascade1/2/2
#
 undo fabric-port Cascade1/2/1 enable
 undo fabric-port Cascade1/2/2 enable
#
interface NULL0
#
bgp 100
 network 196.2.2.0
 network 196.2.3.0
 network 196.3.1.0
 undo synchronization
 group 100 internal
 peer 196.3.1.1 group 100
 group 300 external
 peer 196.2.2.2 group 300 as-number 300
 group 400 external
```

```
 peer 400 route-policy as300 export
 peer 196.2.3.3 group 400 as-number 400
 preference 200 200 200
#
route-policy as300 permit node 10
 if-match ip-prefix as200_1
 apply cost 200
route-policy as300 permit node 20
 if-match ip-prefix as200_2
 apply cost 200
route-policy as300 permit node 30
 if-match ip-prefix as300_1
 apply cost 100
route-policy as300 permit node 40
 if-match ip-prefix as300_2
 apply cost 100
route-policy as300 permit node 50
 if-match ip-prefix other
#
 ip ip-prefix as200_1 index 10 permit 162.1.1.0 24
 ip ip-prefix as200_2 index 10 permit 162.1.2.0 24
 ip ip-prefix as300_1 index 10 permit 162.1.3.0 24
 ip ip-prefix as300_2 index 10 permit 162.1.4.0 24
 ip ip-prefix other index 10 permit 0.0.0.0 0 less-equal 32
#
……
```

3. S200

```
<S200> display current-configuration
#
 sysname S200
#
……
#
 router id 2.1.1.1
#
……
#
vlan 11
#
vlan 12
#
```

```
vlan 13
#
interface Vlan-interface11
 ip address 196.1.1.3 255.255.255.0
#
interface Vlan-interface12
 ip address 206.1.2.3 255.255.255.0
#
interface Vlan-interface13
 ip address 206.1.3.3 255.255.255.0
#
……
#
bgp 200
 network 192.1.1.0
 network 206.1.3.0
 import-route ospf 1
 undo synchronization
 group 100 external
 peer 196.1.1.1 group 100 as-number 100
 group 300 external
 peer 206.1.3.2 group 300 as-number 300
 preference 200 200 200
#
ospf 1
 import-route bgp route-policy ospf_import
 area 0.0.0.0
  network 206.1.2.0 0.0.0.255
#
route-policy ospf_import permit node 10
 if-match ip-prefix ospf_import
#
 ip ip-prefix ospf_import index 10 permit 162.1.3.0 24
 ip ip-prefix ospf_import index 20 permit 162.1.4.0 24
 ip ip-prefix ospf_import index 30 permit 166.1.4.0 24
 ip ip-prefix ospf_import index 40 permit 166.1.3.0 24
#
……
```

4. S200_0

```
<S200_0> display current-configuration
#
```

```
 sysname S200_0
#
……
#
vlan 12
#
vlan 661
#
interface Vlan-interface12
 ip address 206.1.2.1 255.255.255.0
#
interface Vlan-interface661
 ip address 166.1.1.1 255.255.255.0
#
……
#
ospf 1
 area 0.0.0.10
  network 166.1.1.0 0.0.0.255
 #
 area 0.0.0.0
  network 206.1.2.0 0.0.0.255
#
……
```

5. S200_10

```
<S200_10> display current-configuration
#
 sysname S200_10
#
……
#
vlan 621 to 622
#
vlan 661
#
vlan 665
#
interface Vlan-interface621
 ip address 162.1.1.1 255.255.255.0
#
interface Vlan-interface622
```

```
 ip address 162.1.2.1 255.255.255.0
#
interface Vlan-interface661
 ip address 166.1.1.2 255.255.255.0
#
interface Vlan-interface665
 ip address 166.1.5.1 255.255.255.0
#
……
#
ospf 1
 area 0.0.0.10
  network 162.1.1.0 0.0.0.255
  network 162.1.2.0 0.0.0.255
  network 166.1.1.0 0.0.0.255
#
 ip route-static 0.0.0.0 0.0.0.0 166.1.5.2 preference 200
#
……
```

6. S300

```
<S300> display current-configuration
#
 sysname S300
#
router id 3.1.1.1
#
……
#
vlan 13
#
vlan 14
#
vlan 22
#
interface Vlan-interface13
 ip address 206.1.3.2 255.255.255.0
#
interface Vlan-interface14
 ip address 206.1.4.2 255.255.255.0
 rip version 2 multicast
#
```

```
interface Vlan-interface22
 ip address 196.2.2.2 255.255.255.0
#
……
#
bgp 300
 network 206.1.3.0
 network 196.2.2.0
 import-route rip
 undo synchronization
 group 100 external
 peer 196.2.2.1 group 100 as-number 100
 group 200 external
 peer 206.1.3.3 group 200 as-number 200
 preference 200 200 200
#
rip
 undo summary
 network 206.1.4.0
 import-route bgp route-policy rip_import
#
route-policy rip_import permit node 10
 if-match ip-prefix rip_import
#
 ip ip-prefix rip_import index 10 permit 162.1.1.0 24
 ip ip-prefix rip_import index 20 permit 162.1.2.0 24
 ip ip-prefix rip_import index 30 permit 166.1.3.0 24
 ip ip-prefix rip_import index 40 permit 166.1.4.0 24
#
……
```

7. S300_A

```
<S300_A> display current-configuration
#
 sysname S300_A
#
……
#
vlan 14
#
vlan 662
#
```

```
vlan 665
#
interface Vlan-interface14
 ip address 206.1.4.1 255.255.255.0
 rip version 2 multicast
#
interface Vlan-interface662
 ip address 166.1.2.1 255.255.255.0
 rip version 2 multicast
#
interface Vlan-interface665
 ip address 166.1.5.2 255.255.255.0
#
…….
#
rip
 undo summary
 network 206.1.4.0
 network 166.1.0.0
 import-route static
#
ip route-static 162.1.1.0 255.255.255.0 166.1.5.1 preference 200
 ip route-static 162.1.2.0 255.255.255.0 166.1.5.1 preference 200
#
……
```

8. S300_B

```
<S300_B> display current-configuration
#
 sysname S300_B
#
……
#
acl number 2000
 rule 5 deny
#
……
#
vlan 623
#
vlan 624
#
```

```
vlan 662
#
interface Vlan-interface623
 ip address 162.1.3.1 255.255.255.0
 rip version 2 multicast
#
interface Vlan-interface624
 ip address 162.1.4.1 255.255.255.0
 rip version 2 multicast
#
interface Vlan-interface662
 ip address 166.1.2.2 255.255.255.0
 rip version 2 multicast
#
……
#
rip
 undo summary
 network 166.1.0.0
 network 162.1.0.0
 filter-policy 2000 import
#
 ip route-static 0.0.0.0 0.0.0.0 166.1.2.1 preference 60
#
……
```

9. S400

```
<S400> display current-configuration
#
 sysname S400
#
 router id 4.1.1.1
#
……
#
vlan 15 to 16
#
vlan 23
#
interface Vlan-interface15
 ip address 196.1.3.3 255.255.255.0
#
```

```
interface Vlan-interface16
 ip address 206.1.6.3 255.255.255.0
#
interface Vlan-interface23
 ip address 196.2.3.3 255.255.255.0
#
……
#
interface Cascade1/2/1
#
interface Cascade1/2/2
#
 undo fabric-port Cascade1/2/1 enable
 undo fabric-port Cascade1/2/2 enable
#
interface NULL0
#
bgp 400
 network 196.1.3.0
 network 196.2.3.0
 import-route ospf 1
 undo synchronization
 group 100_1 external
 peer 196.1.3.1 group 100_1 as-number 100
 group 100_2 external
 peer 196.2.3.2 group 100_2 as-number 100
 preference 200 200 200
#
ospf 1
 import-route bgp route-policy ospf_import
 area 0.0.0.0
  network 206.1.6.0 0.0.0.255
#
route-policy ospf_import permit node 10
 if-match ip-prefix ospf_import
#
 ip as-path-acl 1 permit ^100 200$
 ip as-path-acl 2 permit ^100 300$
#
 ip ip-prefix ospf_import index 10 permit 162.1.1.0 24
 ip ip-prefix ospf_import index 20 permit 162.1.2.0 24
 ip ip-prefix ospf_import index 30 permit 162.1.3.0 24
```

```
 ip ip-prefix ospf_import index 40 permit 162.1.4.0 24
#
……
```

10. S400_0

```
<S400_0> display current-configuration
#
 sysname S400_0
#
……
#
vlan 16
#
vlan 663 to 664
#
……
#
interface Vlan-interface16
 ip address 206.1.6.1 255.255.255.0
#
interface Vlan-interface663
 ip address 166.1.3.1 255.255.255.0
#
interface Vlan-interface664
 ip address 166.1.4.1 255.255.255.0
#
……
#
ospf 1
 area 0.0.1.44
  network 166.1.3.0 0.0.0.255
  network 166.1.4.0 0.0.0.255
 #
 area 0.0.0.0
  network 206.1.6.0 0.0.0.255
#
……
```

3.4 配置结果验证

3.4.1 路由策略＋静态路由配置验证

```
<S300_B> display ip routing-table
 Routing Table: public net
Destination/Mask   Protocol Pre  Cost  Nexthop     Interface
0.0.0.0/0            STATIC   60    0     166.1.2.1   Vlan-interface662
127.0.0.0/8          DIRECT   0     0     127.0.0.1   InLoopBack0
127.0.0.1/32         DIRECT   0     0      127.0.0.1   InLoopBack0
162.1.3.0/24         DIRECT   0     0     162.1.3.1   Vlan-interface623
162.1.3.1/32         DIRECT   0     0     127.0.0.1   InLoopBack0
162.1.4.0/24         DIRECT   0     0     162.1.4.1   Vlan-interface624
162.1.4.1/32         DIRECT   0     0     127.0.0.1   InLoopBack0
166.1.2.0/24         DIRECT   0     0     166.1.2.2   Vlan-interface662
166.1.2.2/32         DIRECT   0     0     127.0.0.1   InLoopBack0
<S300_B> tracert -a 162.1.3.1 166.1.4.1
 traceroute to 166.1.4.1(166.1.4.1) 30 hops max,40 bytes packet
 1 166.1.2.1 18 ms  3 ms  3 ms
 2 206.1.4.2 9 ms  4 ms  4 ms
 3 196.2.2.1 9 ms  9 ms  18 ms
 4 196.2.3.3 6 ms  3 ms  4 ms
 5 206.1.6.1 14 ms  4 ms  3 ms
```

3.4.2 IGP 与 BGP 交互配置验证

```
<S400_0> display ip routing-table
 Routing Table: public net
Destination/Mask  Protocol  Pre  Cost    Nexthop      Interface
127.0.0.0/8        DIRECT    0     0       127.0.0.1    InLoopBack0
127.0.0.1/32       DIRECT    0     0       127.0.0.1    InLoopBack0
162.1.1.0/24       O_ASE     150   1       206.1.6.3    Vlan-interface16
162.1.2.0/24       O_ASE     150   1       206.1.6.3    Vlan-interface16
162.1.3.0/24       O_ASE     150   1       206.1.6.3    Vlan-interface16
162.1.4.0/24       O_ASE     150   1       206.1.6.3    Vlan-interface16
166.1.3.0/24       DIRECT    0     0       166.1.3.1    Vlan-interface663
166.1.3.1/32       DIRECT    0     0       127.0.0.1    InLoopBack0
166.1.4.0/24       DIRECT    0     0       166.1.4.1    Vlan-interface664
166.1.4.1/32       DIRECT    0     0       127.0.0.1    InLoopBack0
192.168.0.0/24     DIRECT    0     0      192.168.0.30 Vlan-interface1
192.168.0.30/32    DIRECT    0     0      127.0.0.1    InLoopBack0
206.1.6.0/24       DIRECT     0     0      206.1.6.1    Vlan-interface16
```

```
206.1.6.1/32       DIRECT     0     0      127.0.0.1    InLoopBack0
<S300_A>display ip routing-table
 Routing Table: public net
Destination/Mask  Protocol Pre  Cost    Nexthop         Interface
127.0.0.0/8        DIRECT    0    0        127.0.0.1       InLoopBack0
127.0.0.1/32       DIRECT    0    0        127.0.0.1       InLoopBack0
162.1.1.0/24       RIP       100  1        206.1.4.2     Vlan-interface14
162.1.2.0/24       RIP       100  1        206.1.4.2     Vlan-interface14
162.1.3.0/24       RIP       100  1        166.1.2.2    Vlan-interface662
162.1.4.0/24       RIP       100  1        166.1.2.2    Vlan-interface662
166.1.2.0/24       DIRECT      0    0      166.1.2.1    Vlan-interface662
166.1.2.1/32       DIRECT  0    0      127.0.0.1       InLoopBack0
166.1.3.0/24       RIP         100  1      206.1.4.2      Vlan-interface14
166.1.4.0/24       RIP          100  1     206.1.4.2     Vlan-interface14
166.1.5.0/24       DIRECT  0    0      166.1.5.2       Vlan-interface665
166.1.5.2/32       DIRECT  0    0      127.0.0.1       InLoopBack0
206.1.4.0/24       DIRECT  0    0      206.1.4.1       Vlan-interface14
206.1.4.1/32       DIRECT   0    0         127.0.0.1       InLoopBack0
<S200_10> display ip routing-table
 Routing Table: public net
Destination/Mask  Protocol Pre  Cost   Nexthop     Interface
0.0.0.0/0          STATIC    200  0      166.1.5.2   Vlan-interface665
127.0.0.0/8        DIRECT       0    0      127.0.0.1   InLoopBack0
127.0.0.1/32       DIRECT   0    0      127.0.0.1   InLoopBack0
162.1.1.0/24       DIRECT   0    0      162.1.1.1   Vlan-interface621
162.1.1.1/32       DIRECT   0    0      127.0.0.1   InLoopBack0
162.1.2.0/24       DIRECT   0    0     162.1.2.1    Vlan-interface622
162.1.2.1/32       DIRECT    0    0      127.0.0.1   InLoopBack0
162.1.3.0/24       O_ASE     150  1      166.1.1.1   Vlan-interface661
162.1.4.0/24       O_ASE     150  1      166.1.1.1   Vlan-interface661
166.1.1.0/24       DIRECT    0    0      166.1.1.2   Vlan-interface661
166.1.1.2/32       DIRECT    0    0      127.0.0.1   InLoopBack0
166.1.3.0/24       O_ASE     150  1      166.1.1.1   Vlan-interface661
166.1.4.0/24       O_ASE     150  1      166.1.1.1   Vlan-interface661
166.1.5.0/24       DIRECT    0    0      166.1.5.1   Vlan-interface665
166.1.5.1/32       DIRECT    0    0      127.0.0.1   InLoopBack0
206.1.2.0/24       OSPF      10   20     166.1.1.1   Vlan-interface661
```

3.4.3 路由备份配置验证

1. 交换机将主路由安装到路由表中

```
<S200_10> display ip routing-table
```

```
 Routing Table: public net
Destination/Mask  Protocol Pre  Cost   Nexthop     Interface
0.0.0.0/0         STATIC    200  0      166.1.5.2   Vlan-interface665
127.0.0.0/8        DIRECT       0    0      127.0.0.1   InLoopBack0
127.0.0.1/32      DIRECT   0    0      127.0.0.1   InLoopBack0
162.1.1.0/24       DIRECT   0    0      162.1.1.1   Vlan-interface621
162.1.1.1/32       DIRECT   0    0      127.0.0.1   InLoopBack0
162.1.2.0/24       DIRECT   0    0     162.1.2.1    Vlan-interface622
162.1.2.1/32       DIRECT    0    0      127.0.0.1   InLoopBack0
162.1.3.0/24       O_ASE     150  1      166.1.1.1   Vlan-interface661
162.1.4.0/24       O_ASE     150  1      166.1.1.1   Vlan-interface661
166.1.1.0/24       DIRECT    0    0      166.1.1.2   Vlan-interface661
166.1.1.2/32       DIRECT    0    0      127.0.0.1   InLoopBack0
166.1.3.0/24       O_ASE     150  1      166.1.1.1   Vlan-interface661
166.1.4.0/24       O_ASE     150  1      166.1.1.1   Vlan-interface661
166.1.5.0/24       DIRECT    0    0      166.1.5.1   Vlan-interface665
166.1.5.1/32       DIRECT    0    0      127.0.0.1   InLoopBack0
206.1.2.0/24       OSPF      10   20     166.1.1.1   Vlan-interface661
<S200_10> tracert -a 162.1.1.1 166.1.3.1
 traceroute to  166.1.3.1(166.1.3.1) 30 hops max,40 bytes packet
 1 166.1.1.1 10 ms  3 ms  3 ms
 2 206.1.2.3 13 ms  3 ms  5 ms
 3 196.1.1.1 9 ms  3 ms  4 ms
 4 196.1.3.3 12 ms  3 ms  3 ms
 5 206.1.6.1 14 ms  5 ms  3 ms
```

2. 当主路由链路出现故障时，交换机将备份路由安装到路由表中。

```
<S200_10> display ip routing-table
 Routing Table: public net
Destination/Mask  Protocol Pre  Cost   Nexthop     Interface
0.0.0.0/0           STATIC   200  0       166.1.5.2    Vlan-interface665
127.0.0.0/8         DIRECT   0    0       127.0.0.1    InLoopBack0
127.0.0.1/32        DIRECT   0    0      127.0.0.1    InLoopBack0
162.1.1.0/24        DIRECT   0    0      162.1.1.1
Vlan-interface621
162.1.1.1/32        DIRECT   0    0      127.0.0.1        InLoopBack0
162.1.2.0/24        DIRECT   0    0      162.1.2.1
Vlan-interface622
162.1.2.1/32        DIRECT   0    0      127.0.0.1        InLoopBack0
166.1.5.0/24        DIRECT   0    0      166.1.5.1
Vlan-interface665
166.1.5.1/32        DIRECT   0    0      127.0.0.1    InLoopBack0
```

```
<S200_10> tracert -a 162.1.1.1 166.1.3.1
 traceroute to  166.1.3.1(166.1.3.1) 30 hops max,40 bytes packet
 1 166.1.5.2 11 ms  3 ms  4 ms
 2 206.1.4.2 13 ms  3 ms  4 ms
 3 196.2.2.1 13 ms  3 ms  6 ms
 4 196.2.3.3 11 ms  3 ms  4 ms
 5 206.1.6.1 12 ms  3 ms  4 ms
```

3.4.4 BGP 的 MED 属性配置验证

1. 使用缺省 MED 值时报文的转发路径

```
<S400_0> tracert -a 166.1.3.1 162.1.1.1
 traceroute to  162.1.1.1(162.1.1.1) 30 hops max,40 bytes packet
 1 206.1.6.3 11 ms  3 ms  7 ms
 2 196.1.3.1 10 ms  3 ms  8 ms
 3 196.1.1.3 8 ms  3 ms  3 ms
 4 206.1.2.1 13 ms  4 ms  3 ms
 5 166.1.1.2 13 ms  4 ms  3 ms
<S400_0> tracert -a 166.1.3.1 162.1.3.1
 traceroute to  162.1.3.1(162.1.3.1) 30 hops max,40 bytes packet
 1 206.1.6.3 11 ms  3 ms  3 ms
 2 196.1.3.1 14 ms  4 ms  5 ms
 3 196.3.1.2 10 ms  8 ms  17 ms
 4 196.2.2.2 14 ms  3 ms  3 ms
 5 206.1.4.1 13 ms  3 ms  3 ms
 6 166.1.2.2 13 ms  3 ms  4 ms
```

2. 对 MED 值进行控制时报文的转发路径

配置 AS 路径过滤列表 1，允许 AS_PATH 以 100 开始，200 结束的路由信息通过

```
[S400] ip as-path-acl 1 permit ^100 200$
```

显示匹配 AS 路径过滤列表 1 的路由

```
<S400> display bgp routing as-path-acl 1

Flags:   # - valid       ^ - active      I - internal
         D - damped      H - history     S - aggregate suppressed
    Dest/Mask         Next-Hop       Med    Local-pref    Origin       Path
--------------------------------------------------------------------------
#^  162.1.1.0/24      196.1.3.1        100    100           INC       100
200
#   162.1.1.0/24      196.2.3.2        200    100           INC       100
```

```
200
#^  162.1.2.0/24      196.1.3.1        100    100           INC       100
200
#   162.1.2.0/24      196.2.3.2        200    100           INC       100
200
#^  166.1.1.0/24      196.1.3.1       0     100          INC      100 200
#   166.1.1.0/24      196.2.3.2       0     100          INC      100 200
#^  206.1.3.0         196.1.3.1      0      100          IGP      100 200
```

配置 AS 路径过滤列表 1，允许 AS_PATH 以 100 开始，300 结束的路由信息通过

```
[S400] ip as-path-acl 2 permit ^100 300$
```

显示匹配 AS 路径过滤列表 2 的路由

```
<S400> display bgp routing as-path-acl 2

Flags:   # - valid       ^ - active      I - internal
         D - damped      H - history     S - aggregate suppressed
    Dest/Mask         Next-Hop       Med       Local-pref   Origin     Path
--------------------------------------------------------------------------
#^  162.1.3.0/24     196.2.3.2      100       100            INC      100
300
#   162.1.3.0/24     196.1.3.1      200       100            INC      100
300
#^  162.1.4.0/24     196.2.3.2      100       100            INC      100
300
#   162.1.4.0/24     196.1.3.1      200       100            INC      100
300
#^  166.1.2.0/24     196.1.3.1      0         100            INC      100
300
#   166.1.2.0/24     196.2.3.2      0         100            INC      100
300
#^  166.1.5.0/24     196.1.3.1      0         100            INC      100
300
#   166.1.5.0/24     196.2.3.2      0         100            INC      100
300
#   206.1.3.0       196.2.3.2     0         100          IGP      100 300
<S400_0> tracert -a 166.1.3.1 162.1.1.1
 traceroute to  162.1.1.1(162.1.1.1) 30 hops max,40 bytes packet
 1 206.1.6.3 9 ms  4 ms  3 ms
 2 196.1.3.1 13 ms  4 ms  3 ms
 3 196.1.1.3 14 ms  4 ms  3 ms
 4 206.1.2.1 12 ms  3 ms  3 ms
```

```
 5 166.1.1.2 13 ms  4 ms  3 ms
<S400_0> tracert -a 166.1.3.1 162.1.3.1
 traceroute to  162.1.3.1(162.1.3.1) 30 hops max,40 bytes packet
 1 206.1.6.3 10 ms  4 ms  3 ms
 2 196.2.3.2 13 ms  3 ms  5 ms
 3 196.2.2.2 12 ms  5 ms  3 ms
 4 206.1.4.1 12 ms  4 ms  3 ms
 5 166.1.2.2 14 ms  3 ms  5 ms
```

3.5 注意事项

在配置及验证的过程中，请注意以下几点：

- 对于支持 Fabric 的设备，启动 BGP 之前必须关闭 Fabric 功能；
- 为了保证配置目标的实现，建议在配置的过程中将 BGP 优先级修改为适合的值（建议修改为 200）；配置静态路由的设备，根据情况对静态路由的优先级进行相应的修改；

在 S300_A 上无法实现备份路由（静态路由）到主路由（RIP）的自动切换，需要手工干涉，方法是将备份路由手动从配置中删除，然后在添加到配置中；

由于将 BGP 引入到 IGP 时应用了路由策略，可能存在部分路由条目没有被引入的情况，所以在验证时建议使用源地址的模式进行验证：**tracert –a / ping –a**

目 录

组播协议典型配置举例

关键词：IGMP、PIM-DM、PIM-SM、MSDP、IGMP Snooping

摘 要：本文主要介绍以太网交换机的组播功能在具体组网中的应用配置，根据组网需求的不同，分别介绍了三个典型的组网应用。

第一，介绍了PIM-DM＋IGMP分别在存在和不存在IGMP Snooping两种情况下的组播应用情况，其中体现了IGMP和IGMP Snooping组播组过滤功能的应用；

第二，介绍了PIM-SM＋IGMP分别在存在和不存在IGMP Snooping两种情况下的组播应用情况，其中体现了模拟组播客户端加入组播组的应用；

第三，介绍了在只运行IGMP Snooping的情况下的应用，其中体现了未知组播报文丢弃功能的应用。

缩略语：IGMP（Internet Group Management Protocol，互联网组管理协议）；IGMP Snooping（Internet Group Management Protocol Snooping，互联网组管理协议窥探）；PIM-DM（Protocol Independent Multicast Dense Mode，密集模式协议无关组播）；PIM-SM（Protocol Independent Multicast Sparse Mode，稀疏模式协议无关组播）；MSDP（Multicast Source Discovery Protocol，组播源发现协议）。

第1章 组播协议功能简介

1.1 组播特性简介

作为一种与单播和广播并列的通信方式，组播技术能够有效地解决单点发送、多点接收的问题，从而实现了网络中点到多点的高效数据传送，能够节约大量网络带宽、降低网络负载。

利用组播技术可以方便地提供一些新的增值业务，包括在线直播、网络电视、远程教育、远程医疗、网络电台、实时视频会议等对带宽和数据交互的实时性要求较高的信息服务。

1. IGMP

IGMP 是 TCP/IP 协议族中负责 IP 组播成员管理的协议。它用来在 IP 主机和与其直接相邻的组播路由器之间建立、维护组播组成员关系。

2. PIM

PIM 是 Protocol Independent Multicast（协议无关组播）的简称，表示可以利用静态路由或者任何单播路由协议（包括 RIP、OSPF、IS-IS、BGP 等）生成的单播路由表为 IP 组播提供路由。PIM 通过使用单播路由表进行 RPF（Reverse Path Forwarding，逆向路径转发）检查，以实现对组播数据的传送。

根据转发机制的不同，PIM 分为两种模式：

- PIM-DM
- PIM-SM

PIM-DM 属于密集模式的组播路由协议，使用“推（Push）模式”传送组播数据，通常适用于组播组成员相对比较密集的小型网络。.

PIM-SM 属于稀疏模式的组播路由协议，使用“拉（Pull）模式”传送组播数据，通常适用于组播组成员分布相对分散、范围较广的大中型网络。

3. IGMP Snooping

IGMP Snooping 是运行在二层设备上的组播约束机制，用于管理和控制组播组。运行 IGMP Snooping 的二层设备通过对收到的 IGMP 报文进行分析，为端口和 MAC 组播地址建立起映射关系，并根据这样的映射关系转发组播数据。

4. MSDP

MSDP 是基于多个 PIM-SM 域的互连而开发的一种域间组播解决方案，用来发现其它 PIM-SM 域内的组播源信息。

在 PIM-SM 域中，组播源只向本地 RP（Rendezvous Point，汇集点）进行注册，因此 RP 知道本域内的所有组播源。如果能够有一种机制，使不同 PIM-SM 域的 RP 共享其组播源信息，那么就能够将其它域内活动的组播源信息传递给本域内的接收者，从而实现组播报文的跨域转发。MSDP 成功地实现了这一构想，通过在各域的 RP 之间建立 MSDP 对等体关系，使它们能够在域间相互转发组播数据，共享组播源信息。

5. IGMP Proxy

在一个大规模的网络中应用组播路由协议时（例如 PIM-DM），会存在很多末梢网络（末梢区域），对这些末梢网络进行配置和管理是一件很繁重的工作。

为了减少这些配置和管理工作，同时又不影响末梢网络的组播连接，可以在末梢网络的三层交换机上配置 IGMP Proxy，三层交换机将自己所连接的主机发出的 IGMP 主机报告报文或 IGMP 离开报文进行转发。配置了 IGMP Proxy 后，对于外部网络来说，末梢三层交换机不再是一个 PIM 邻居，而是一台主机，只有当该三层交换机有直连成员时，才会接收相应组的组播数据。

1.2 特性支持情况

H3C系列以太网交换机根据设备型号的不同，支持的组播的功能也不同，详细情况请参见相关产品的操作手册。表 1-1列出了H3C系列以太网交换机支持的组播特性支持情况。

表1-1 各产品组播特性支持情况

功能 / 产品型号	IGMP Snooping	IGMP	PIM	MSDP
S3600-EI	●	●	●	●
S3600-SI	●	-	-	-
S5600	●	●	●	●
S5100	●	-	-	-
S3100-SI	●	-	-	-
E352&E328	●	-	-	-
E126	●	-	-	-
S3152P	●	-	-	-
E152	●	-	-	-

1.3 组播配置指南

下面以 S5600 系列以太网交换机为例简要介绍一下相关特性的主要配置过程，如果需要了解更多的相关配置请参见产品操作手册。

1.3.1 配置 IGMP Snooping

表1-2 IGMP Snooping 配置过程

配置任务	说明	详细配置
启动 IGMP Snooping	必选	1.3.1 1.
配置 IGMP Snooping 定时器	可选	1.3.1 2.
配置端口从组播组中快速删除功能	可选	1.3.1 3.
配置组播组过滤功能	可选	1.3.1 4.
配置端口可以加入的组播组最大数量	可选	1.3.1 5.
配置 IGMP Snooping 查询器	可选	1.3.1 6.

1. 启动 IGMP Snooping

表1-3 配置 IGMP Snooping

操作	命令	说明
进入系统视图	**system-view**	-
启动 IGMP Snooping	**igmp-snooping enable**	必选 缺省情况下 IGMP Snooping 功能处于关闭状态
进入 VLAN 视图	**vlan** *vlan-id*	-
启动 IGMP Snooping	**igmp-snooping enable**	必选 缺省情况下，IGMP Snooping 功能处于关闭状态

2. 配置 IGMP Snooping 定时器

表1-4 配置 IGMP Snooping 定时器

操作	命令	说明
进入系统视图	**system-view**	-
配置路由器端口老化定时器	**igmp-snooping router-aging-time** *seconds*	可选 缺省情况下，路由器端口老化时间为 105 秒

操作	命令	说明
配置响应查询定时器	**igmp-snooping max-response-time** *seconds*	可选 缺省情况下，最大响应时间为 10 秒
配置组播组成员端口老化定时器	**igmp-snooping host-aging-time** *seconds*	可选 缺省情况下，组播组成员端口老化时间为 260 秒

3. 配置端口从组播组中快速删除功能

(1) 在系统视图下配置端口从组播组中快速删除功能

表1-5 在系统视图下配置端口从组播组中快速删除功能

操作	命令	说明
进入系统视图	**system-view**	-
配置端口从组播组中快速删除功能	**igmp-snooping fast-leave** [**vlan** *vlan-list*]	必选 缺省情况下，端口从组播组中快速删除功能处于关闭状态

(2) 在以太网端口视图下配置端口从组播组中快速删除功能

表1-6 在以太网端口视图下配置端口从组播组中快速删除功能

操作	命令	说明
进入系统视图	**system-view**	-
进入以太网端口	**interface** *interface-type interface-number*	-
配置端口从组播组中快速删除功能	**igmp-snooping fast-leave** [**vlan** *vlan-list*]	必选 缺省情况下，端口从组播组中快速删除功能处于关闭状态

4. 配置组播组过滤功能

(1) 在系统视图下配置组播组过滤功能

表1-7 在系统视图下配置组播组过滤功能

操作	命令	说明
进入系统视图	**system-view**	-
配置组播组过滤功能	**igmp-snooping group-policy** *acl-number* [**vlan** *vlan-list*]	必选 缺省情况下，组播组过滤功能关闭

(2) 在以太网端口视图下配置组播组过滤功能

表1-8 在以太网端口视图下配置组播组过滤功能

操作	命令	说明
进入系统视图	**system-view**	-
进入以太网端口视图	**interface** *interface-type interface-number*	-
配置组播组过滤功能	**igmp-snooping group-policy** *acl-number* [**vlan** *vlan-list*]	必选 缺省情况下，组播组过滤功能关闭

5. 配置端口可以加入的组播组最大数量

表1-9 配置端口可以加入的组播组最大数量

操作	命令	说明
进入系统视图	**system-view**	-
进入以太网端口视图	**interface** *interface-type interface-number*	-
配置端口上允许通过的组播组数量	**igmp-snooping group-limit** *limit* [**vlan** *vlan-list* [**overflow-replace**]]	必选 缺省情况下，端口上允许通过的组播组最大数量为 255 个

6. 配置 IGMP Snooping 查询器

表1-10 配置 IGMP Snooping 查询器

操作	命令	说明
进入系统视图	**system-view**	-
启动 IGMP Snooping	**igmp-snooping enable**	必选 缺省情况下，IGMP Snooping 功能处于关闭状态
进入 VLAN 视图	**vlan** *vlan-id*	-
启动 IGMP Snooping	**igmp-snooping enable**	必选 缺省情况下，IGMP Snooping 功能处于关闭状态
启动 IGMP Snooping 查询器	**igmp-snooping querier**	必选 缺省情况下，IGMP Snooping 查询器功能处于关闭状态
配置发送通用查询报文的时间间隔	**igmp-snooping query-interval** *seconds*	可选 缺省情况下，发送通用查询报文的时间间隔为 60 秒

操作	命令	说明
配置发送通用查询报文的源 IP 地址	**igmp-snooping general-query source-ip** { **current-interface** | *ip-address* }	可选 缺省情况下，发送通用查询报文的源 IP 地址为 0.0.0.0

1.3.2 配置 IGMP

表1-11 配置任务简介

配置任务	说明	详细配置
启动 IGMP	必选	1.3.2 1.
配置 IGMP 版本	可选	1.3.2 2.
配置 IGMP 查询报文的相关参数	可选	1.3.2 3.
配置接口可以通过的组播组最大数量	可选	1.3.2 4.
配置组播组过滤功能	可选	1.3.2 5.
配置 IGMP 模拟主机加入功能	可选	1.3.2 6.
配置 IGMP Proxy	可选	1.3.2 7.
删除接口上已经加入的 IGMP 组播组	可选	1.3.2 8.

1. 启动 IGMP

表1-12 启动 IGMP

操作	命令	说明
进入系统视图	**system-view**	-
启动组播路由	**multicast routing-enable**	-
进入 VLAN 接口视图	**interface Vlan-interface** *interface-number*	-
启动 IGMP	**igmp enable**	必选 缺省情况下， IGMP 处于关闭状态

⚠ 注意：

本章中以下的配置都是在启动组播路由并在接口上启动 IGMP 的情况下实现的，请用户在配置过程中注意。

2. 配置 IGMP 版本

表1-13 配置 IGMP 版本

操作	命令	说明
进入系统视图	**system-view**	-
进入 VLAN 接口视图	**interface Vlan-interface** *interface-number*	-
配置 IGMP 版本	**igmp version** { **1** | **2** }	必选 缺省情况下，IGMP 的版本为 IGMPv2

⚠ 注意：

IGMP 各版本之间不能自动转换。因此，应该配置连接到同一网段上的所有交换机的接口使用同一 IGMP 版本。

3. 配置 IGMP 查询报文的相关参数

表1-14 配置 IGMP 查询报文的相关参数

操作	命令	说明
进入系统视图	**system-view**	-
进入 VLAN 接口视图	**interface Vlan-interface** *interface-number*	-
配置查询间隔	**igmp timer query** *seconds*	可选 缺省情况下，查询时间间隔为 60 秒
配置发送 IGMP 特定组查询报文的时间间隔	**igmp lastmember-queryinterval** *seconds*	可选 缺省情况下，IGMP 特定组查询报文的时间间隔为 1 秒
配置发送 IGMP 特定组查询报文的次数	**igmp robust-count** *robust-value*	可选 缺省情况下，发送 IGMP 特定组查询报文的次数为 2 次
配置 IGMP 查询器存在时间	**igmp timer other-querier-present** *seconds*	可选 缺省情况下，IGMP 查询器存在的时间值为 120 秒，是 **igmp timer query** 命令指定的间隔的 2 倍
配置 IGMP 最大响应时间	**igmp max-response-time** *seconds*	可选 缺省情况下，IGMP 最大响应时间为 10 秒

4. 配置接口可以通过的组播组最大数量

表1-15 配置接口可以通过的组播组最大数量

操作	命令	说明
进入系统视图	**system-view**	-
进入 VLAN 接口视图	**interface Vlan-interface** *interface-number*	-
配置接口可以加入IGMP组的最大数量	**igmp group-limit** *limit*	必选 缺省情况下，接口上可以通过的组播组最大数量为 256

⚠ 注意：

- 如果用户在接口上配置的 IGMP 组的数量为 1 时，采用新加入组优先的原则。即如用户将新的组播组加入接口时，系统将自动取代原有的组播组，原组播组将会自动脱离接口。
- 在接口配置可以通过的组播组最大数量时，如果接口已有的 IGMP 组播组比要配置的值多，系统自动删除某些已有的组播组，直到接口组播组数量符合配置的数量限制。

5. 配置组播组过滤功能

(1) 在 VLAN 接口视图下配置组播组过滤功能

表1-16 配置组播组过滤功能

操作	命令	说明
进入系统视图	**system-view**	-
进入 VLAN 接口视图	**interface Vlan-interface** *interface-number*	-
配置组播组过滤功能	**igmp group-policy** *acl-number* [**1 | 2 | port** *interface-type interface-number* [**to** *interface-type interface-number*]]	可选 缺省情况下，接口允许任意组播组通过

(2) 在以太网端口视图下配置组播组过滤功能

表1-17 配置组播组过滤功能

操作	命令	说明
进入系统视图	**system-view**	-
进入以太网端口视图	**interface** *interface-type interface-number*	-

操作	命令	说明
配置组播组过滤功能	**igmp group-policy** *acl-number* **vlan** *vlan-id*	可选 缺省情况下，接口允许任意组播组通过，该端口必须属于命令所指定的 VLAN

6. 配置 IGMP 模拟主机加入功能

(1) 在 VLAN 接口视图下配置 IGMP 模拟主机加入功能

表1-18 在 VLAN 接口视图下配置 IGMP 模拟主机加入功能

操作	命令	说明
进入系统视图	**system-view**	-
进入 VLAN 接口视图	**interface Vlan-interface** *interface-number*	-
配置 IGMP 模拟主机加入功能	**igmp host-join** *group-address* **port** *interface-list*	可选 缺省情况下，模拟主机加入功能处于关闭状态

(2) 在以太网端口视图下配置 IGMP 模拟主机加入功能

表1-19 在以太网端口视图下配置 IGMP 模拟主机加入功能

操作	命令	说明
进入系统视图	**system-view**	-
进入以太网端口视图	**interface** *interface-type interface-number*	-
配置 IGMP 模拟主机加入功能	**igmp host-join** *group-address* **vlan** *vlan-id*	可选 缺省情况下，模拟主机加入功能处于关闭状态

⚠ 注意：

- 配置 IGMP 模拟主机加入功能前，应该先在 VLAN 接口视图下启动 IGMP 功能；
- 在以太网端口视图下，配置 IGMP 模拟主机加入功能的端口必须属于指定 VLAN，否则配置不会生效；

7. 配置 IGMP Proxy

表1-20 配置 IGMP Proxy

操作	命令	说明
进入系统视图	**system-view**	-
启动组播路由	**multicast routing-enable**	必选
进入 VLAN 接口视图	**interface Vlan-interface** *interface-number*	-
启动 IGMP 协议	**igmp enable**	必选
配置 IGMP Proxy	**igmp proxy Vlan-interface** *interface-number*	必选 缺省情况下，IGMP Proxy 功能处于关闭状态

⚠ 注意：

- 配置 **igmp proxy** 前需要先在接口上启动 PIM 协议，否则 IGMP Proxy 功能不能生效。
- 同一个接口不能作为两个及两个以上其它接口的 IGMP 代理接口。
- 在配置将要成为 IGMP 代理接口的 IP 地址时，要保证该接口的 IP 地址在该网段不是最小的，从而避免该接口被选举成 IGMP 查询器，而造成无法正常转发组播数据。

8. 删除接口上已加入的 IGMP 组播组

表1-21 删除接口上已加入的 IGMP 组播组

操作	命令	说明
删除接口上已加入的 IGMP 组播组	**reset igmp group** { **all** | **interface** *interface-type interface-number* { **all** | *group-address* [*group-mask*] } }	**reset** 命令可以在用户视图下执行

⚠ 注意：

删除接口上已加入的 IGMP 组后，不影响该组的再次加入。

1.3.3 配置 PIM

1. 配置 PIM-DM

表1-22 配置 PIM-DM

操作	命令	说明
进入系统视图	**system-view**	-
启动组播路由	**multicast routing-enable**	必选 缺省情况下，没有启动组播路由协议
进入 PIM 视图	**pim**	-
对接收的组播数据报文进行源（组）过滤	**source-policy** *acl-number*	可选 用户可在 ACL 中配置过滤相关的组播组 IP 地址
进入 VLAN 接口视图	**interface Vlan-interface** *interface-number*	-
启动 PIM-DM	**pim dm**	必选
设置接口的 Hello 报文发送间隔	**pim timer hello** *seconds*	可选 缺省的 Hello 报文发送间隔是 30 秒
配置接口的 PIM 邻居数量限制	**pim neighbor-limit** *limit*	可选 缺省情况下，接口的 PIM 邻居数量上限为 128
配置 PIM 邻居过滤规则	**pim neighbor-policy** *acl-number*	可选 用户可在 ACL 中配置过滤相关的组播组 IP 地址 缺省情况下，接口不启动邻居过滤规则

2. 配置 PIM-SM

表1-23 配置 PIM-SM

操作	命令	说明
进入系统视图	**system-view**	-
启动组播路由	**multicast routing-enable**	必选 缺省情况下，没有启动组播路由协议
进入 PIM 视图	**pim**	-
对接收的组播数据报文进行源（组）过滤	**source-policy** *acl-number*	可选 用户可在 ACL 中配置过滤相关的组播组 IP 地址

操作	命令	说明
配置候选 BSR	**c-bsr** *interface-type interface-number hash-mask-len* [*priority*]	可选 缺省情况下，交换机没有设置候选 BSR，优先级的缺省值为 0
配置候选 RP	**c-rp** *interface-type interface-number* [**group-policy** *acl-number* | **priority** *priority*]*	可选 缺省情况下，交换机没有设置候选 RP，优先级的缺省值为 0
配置静态 RP	**static-rp** *rp-address* [*acl-number*]	可选 缺省情况下，交换机没有设置静态 RP
限定合法 BSR 的范围	**bsr-policy** *acl-number*	可选 缺省情况下，交换机没有设置合法 BSR 的范围
限定合法 C-RP 的范围	**crp-policy** *acl-number*	可选 用户可在 ACL 中配置过滤相关的组播组 IP 地址 缺省情况下，交换机没有设置合法的 C-RP 范围
配置 RP 对 DR 发来的注册报文进行过滤	**register-policy** *acl-number*	可选 用户可在 ACL 中配置过滤相关的组播组 IP 地址 缺省情况下，交换机对 DR 发来的注册报文不进行过滤
设置从共享树永不切换到最短路径树	**spt-switch-threshold infinity** [**group-policy** *acl-number* [**order** *order-value*]]	可选 缺省情况下，设备从 RPT 收到第一个组播数据包后便立即向 SPT 切换
进入 VLAN 接口视图	**interface Vlan-interface** *interface-number*	-
启动 PIM-SM	**pim sm**	必选
配置 PIM-SM 域边界	**pim bsr-boundary**	可选 缺省情况下，交换机不设置域边界
设置接口的 Hello 报文发送间隔	**pim timer hello** *seconds*	可选 缺省的 Hello 报文发送间隔是 30 秒
配置接口的 PIM 邻居数量限制	**pim neighbor-limit** *limit*	可选 缺省情况下，接口的 PIM 邻居数量上限为 128
配置 PIM 邻居过滤规则	**pim neighbor-policy** *acl-number*	可选 用户可在 ACL 中配置过滤相关的组播组 IP 地址 缺省情况下，接口不启动邻居过滤规则

1.3.4 配置 MSDP

1. 配置 MSDP 基本功能

表1-24 配置 MSDP 基本功能

操作	命令	说明
进入系统视图	**system-view**	-
启动 MSDP 功能，并进入 MSDP 视图	**msdp**	必选
创建 MSDP 对等体连接	**peer** *peer-address* **connect-interface** *interface-type interface-number*	必选 需要在互为对等体的两端都配置参数才能建立 MSDP 对等体，对等体标识为地址对（本端路由器接口主地址、远端 MSDP 对等体地址）
配置静态 RPF 对等体	**static-rpf-peer** *peer-address* [**rp-policy** *ip-prefix-name*]	可选 对于只有一个 MSDP 对等体的区域，如果不运行 BGP 或 MBGP，则需要配置静态 RPF 对等体

2. 配置 MSDP 对等体连接

表1-25 配置任务简介

配置任务	说明	详细配置
配置 MSDP 对等体的描述信息	必选	1.3.4 2. (1)
配置 MSDP 全连接组	可选	1.3.4 2. (2)
配置 MSDP 对等体连接控制	可选	1.3.4 2. (3)

(1) 配置 MSDP 对等体描述信息

表1-26 配置 MSDP 对等体的描述信息

操作	命令	说明
进入系统视图	**system-view**	-
进入 MSDP 视图	**msdp**	-
配置 MSDP 对等体的描述信息	**peer** *peer-address* **description** *text*	可选 缺省情况下，MSDP 对等体没有描述信息

(2) 配置 MSDP 全连接组

表1-27 配置 MSDP 全连接组

操作	命令	说明
进入系统视图	**system-view**	-
进入 MSDP 视图	**msdp**	-
配置将 MSDP 对等体加入全连接组	**peer** *peer-address* **mesh-group** *name*	必选 缺省情况下，MSDP 对等体不属于任何全连接组

📖 说明：

- 配置 MSDP 全连接组之前，各路由器之间应该保持彼此两两互相连接。
- 各对等体上配置的组名称必须相同，才能够加入同一个全连接组。
- 如果将同一 MSDP 对等体加入到多个全连接组时，只有最后一个配置有效。

(3) 配置 MSDP 对等体连接控制

表1-28 配置 MSDP 对等体连接控制

操作	命令	说明
进入系统视图	**system-view**	-
进入 MSDP 视图	**msdp**	-
关闭 MSDP 对等体	**shutdown** *peer-address*	可选 缺省情况下，MSDP 对等体处于连接状态
配置 MSDP 对等体连接的重试周期	**timer retry** *seconds*	可选 缺省情况下，建立 MSDP 对等体连接的重试周期为 30 秒

3. 配置 SA 消息传递

表1-29 配置任务简介

配置任务	说明	详细配置
配置 SA 消息中的 RP 地址	可选	1.3.4 3. (1)
配置 SA 消息缓存	可选	1.3.4 3. (2)
配置 SA 请求消息的发送和过滤	可选	1.3.4 3. (3)
配置 SA 消息的组播源过滤规则	可选	1.3.4 3. (4)
配置接收和转发 SA 消息的过滤规则	可选	1.3.4 3. (5)

(1) 配置 SA 消息中的 RP 地址

表1-30 配置 Anycast RP 应用

操作	命令	说明
进入系统视图	**system-view**	-
进入 MSDP 视图	**msdp**	-
配置 SA 消息中的 RP 地址	**originating-rp** *interface-type interface-number*	可选 缺省情况下，SA 消息的 RP 地址为 PIM 配置的 RP 地址

📖 **说明：**

在 Anycast RP 应用中，C-BSR 和 C-RP 必须配置在不同设备或端口上。

(2) 配置 SA 消息缓存

表1-31 配置 SA 消息缓存

操作	命令	说明
进入系统视图	**system-view**	-
进入 MSDP 视图	**msdp**	-
启动 SA 消息缓存机制	**cache-sa-enable**	可选 缺省情况下，启动 SA 消息缓存机制
配置 SA 消息的缓存数量	**peer** *peer-address* **sa-cache-maximum** *sa-limit*	可选 缺省情况下，SA 缓存数量为最大值 2048

(3) 配置 SA 请求消息的发送和过滤

表1-32 配置 SA 请求消息的发送和过滤

操作	命令	说明
进入系统视图	**system-view**	-
进入 MSDP 视图	**msdp**	-
启动 SA 消息缓存机制	**cache-sa-enable**	可选 在缺省情况下，路由器收到 SA 消息后缓存 SA 的状态
启动 MSDP 对等体发送 SA 请求消息的功能	**peer** *peer-address* **request-sa-enable**	可选 缺省情况下，路由器在收到新的组加入消息时，不向其 MSDP 对等体发送 SA 请求消息，而是等待下一个 SA 消息的到来

操作	命令	说明
配置对 MSDP 对等体接收的 SA 请求消息进行过滤	**peer** *peer-address* **sa-request-policy** [**acl** *acl-number*]	可选 缺省情况下，路由器接收来自该 MSDP 对等体的所有 SA 请求消息

(4) 配置 SA 消息的组播源过滤规则

表1-33 配置 SA 消息的组播源过滤规则

操作	命令	说明
进入系统视图	**system-view**	-
进入 MSDP 视图	**msdp**	-
配置用 SA 消息过滤组播源	**import-source** [**acl** *acl-number*]	可选 缺省情况下，SA 消息通告域内的所有的（S, G）项

(5) 配置接收和转发 SA 消息的过滤规则

表1-34 配置接收和转发 SA 消息的过滤规则

操作	命令	说明
进入系统视图	**system-view**	-
进入 MSDP 视图	**msdp**	-
配置对接收或转发的 SA 消息进行过滤	**peer** *peer-address* **sa-policy** { **import** | **export** } [**acl** *acl-number*]	可选 缺省情况下，对接收或转发的消息不作过滤， MSDP 对等体接收或转发所有的 SA 消息
配置发送到指定 MSDP 对等体的组播数据包的最小 TTL	**peer** *peer-address* **minimum-ttl** *ttl-value*	可选 缺省情况下，TTL 阈值为 0

第2章 组播协议典型配置举例

2.1 PIM-DM+IGMP+IGMP Snooping 配置举例

2.1.1 需求分析

用户通过组播方式接收视频点播信息，根据用户需求的不同，视频信息的接收方式也不尽相同：

(1) 为了避免视频信息在二层的广播，HostA 和 HostB 通过连接到运行 IGMP Snooping 的 SwitchE 接收组播数据；

(2) 为了可靠和稳定的的接收组播数据，HostC 和 HostD 直接连接到与 SwitchB 和 SwitchC 相连的末梢网络 N1 接收组播数据，从而可以实现上行链路的备份；

(3) 各个交换机之间运行的单播路由协议是 RIP，运行的组播路由协议是 PIM-DM。

2.1.2 网络布局

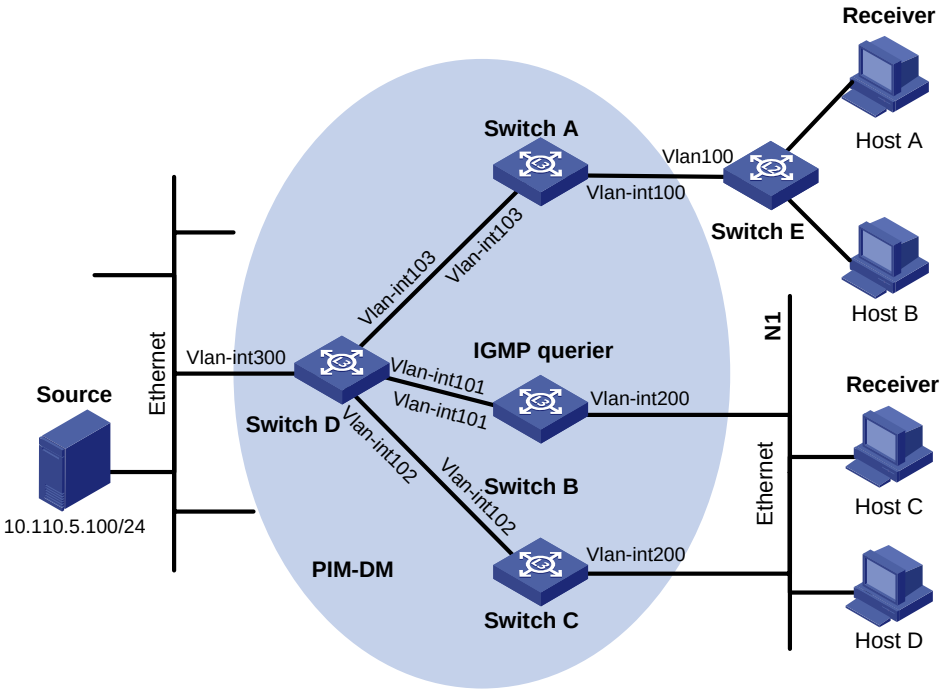
(1) SwitchD 通过 Vlan-interface300 接口与组播源 Source 所在的网络连接；

(2) SwitchA 通过 Vlan-interface100 接口连接 SwitchE，通过 Vlan-interface103 接口连接 SwitchD；

(3) SwitchB 和 SwitchC 通过各自的 Vlan-interface200 接口连接末梢网络 N1，分别通过 Vlan-interface101 和 Vlan-interface102 接口连接 SwitchD；

(4) 在 SwitchA 的 Vlan-interface100 接口上运行 IGMPV2，在 SwitchE 上全局启动 IGMP Snooping 和在 VLAN100 内启动 IGMP Snooping；SwitchB 和 SwitchC 与末梢网络 N1 之间也运行 IGMPv2，通常 SwitchB 充当查询器。

2.1.3 组网图



设备	接口	IP 地址	包含端口
Switch A	Vlan-int100	10.110.1.1/24	Ethernet1/0/1
	Vlan-int103	192.168.1.1/24	Ethernet1/0/2
Switch B	Vlan-int200	10.110.2.1/24	Ethernet1/0/1
	Vlan-int101	192.168.2.1/24	Ethernet1/0/2
Switch C	Vlan-int200	10.110.2.2/24	Ethernet1/0/1
	Vlan-int102	192.168.3.1/24	Ethernet1/0/2
Switch D	Vlan-int300	10.110.5.1/24	Ethernet1/0/1
	Vlan-int103	192.168.1.2/24	Ethernet1/0/2
	Vlan-int101	192.168.2.2/24	Ethernet1/0/3
	Vlan-int102	192.168.3.2/24	Ethernet1/0/4
Switch E	Vlan100	-	Ethernet1/0/1、Ethernet1/0/2、Ethernet1/0/3

图2-1 PIM-DM＋IGMP＋IGMP Snooping 典型配置组网图

2.1.4 配置步骤

1. 配置各交换机的 VLAN、VLAN 接口及其 IP 地址

配置 SwitchA 的 VLAN、VLAN 接口及其 IP 地址。

```
<SwitchA> system-view
System View: return to User View with Ctrl+Z.
[SwitchA] vlan 100
[SwitchA-vlan100] port Ethernet 1/0/1
[SwitchA-vlan100] quit
[SwitchA] vlan 103
```

```
[SwitchA-vlan103] port Ethernet 1/0/2
[SwitchA-vlan103] quit
[SwitchA] interface Vlan-interface 100
[SwitchA-Vlan-interface100] ip address 10.110.1.1 24
[SwitchA-Vlan-interface100] quit
[SwitchA] interface Vlan-interface 103
[SwitchA-Vlan-interface103] ip address 192.168.1.1 24
[SwitchA-Vlan-interface103] quit
```

请参照图 2-1配置其他各交换机的Vlan、Vlan接口及其IP地址，具体的配置过程略。

2. 配置单播路由协议

在 SwitchA 上启动 RIP 协议，并且在 192.168.1.0 和 10.110.1.0 两个网段启动 RIP。

```
<SwitchA> system-view
[SwitchA] rip
[SwitchA- rip] network 192.168.1.0
[SwitchA- rip] network 10.110.1.0
[SwitchA- rip] quit
```

SwitchB、SwitchC 和 SwitchD 的配置与 SwitchA 相似，配置过程略。

3. 配置组播协议

在 SwitchA 上启动 IP 组播路由，在各接口上启动 PIM-DM，并在 Vlan-interface100 接口上启动 IGMPv2。

```
<SwitchA> system-view
[SwitchA] multicast routing-enable
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] igmp enable
[SwitchA-Vlan-interface100] pim dm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 103
[SwitchA-Vlan-interface103] pim dm
[SwitchA-Vlan-interface103] quit
```

SwitchB 和 SwitchC 的配置与 SwitchA 相似，配置过程略。

在 SwitchD 上启动组播路由，并在其各接口上启动 PIM-DM。

```
<SwitchD> system-view
[SwitchD] multicast routing-enable
[SwitchD] interface vlan-interface 300
[SwitchD-Vlan-interface300] pim dm
[SwitchD-Vlan-interface300] quit
[SwitchD] interface vlan-interface 103
[SwitchD-Vlan-interface103] pim dm
```

```
[SwitchD-Vlan-interface103] quit
[SwitchD] interface vlan-interface 101
[SwitchD-Vlan-interface101] pim dm
[SwitchD-Vlan-interface101] quit
[SwitchD] interface vlan-interface 102
[SwitchD-Vlan-interface102] pim dm
[SwitchD-Vlan-interface102] quit
```

在 SwitchE 上全局启动 IGMP Snooping，并在 Vlan100 内启动 IGMP Snooping。

```
<SwitchE> system-view
[SwitchE] igmp-snooping enable
  Enable IGMP-Snooping ok.
[SwitchE] vlan 100
[SwitchE-vlan100] igmp-snooping enable
[SwitchE-vlan100] quit
```

4. 检验配置效果

现在从组播源 Source 向组播组 224.1.1.1 发送组播数据，HostA 点播组播组 224.1.1.1 的组播数据，检验各个交换机的配置效果。

(1) 通过查看命令判断 HostA 是否接收到组播数据。

查看 Switch D 上 PIM 的邻居关系信息。

```
<SwitchD> display pim neighbor
Neighbor's Address  Interface Name                Uptime    Expires
192.168.2.1         Vlan-interface101              02:45:04  00:04:46
192.168.3.1         Vlan-interface102              02:42:24  00:04:45
192.168.1.1         Vlan-interface103              02:43:44  00:05:44
```

查看 SwitchD 的组播转发表。

```
<SwitchD>display multicast forwarding-table
Multicast Forwarding Cache Table
Total 1 entries: 0 entry created by IP, 1 entries created by protocol

00001. (10.110.5.110, 224.1.1.1), iif Vlan-interface1, 1 oifs,
     Protocol Create
     List of outgoing interface:
       01: Vlan-interface101
     Matched 181 pkts(271500 bytes), Wrong If 0 pkts
     Forwarded 130 pkts(195000 bytes)

Total 1 entries Listed
```

查看 SwitchA 的组播转发表。

```
<SwitchA> display multicast forwarding-table
Multicast Forwarding Cache Table
Total 1 entry: 0 entry created by IP, 1 entry created by protocol
00001. (10.110.5.110, 224.1.1.1), iif Vlan-interface101, 1 oifs,
     Protocol Create
     List of outgoing interface:
       01: Vlan-interface100
     Matched 451 pkts(676500 bytes), Wrong If 0 pkts
     Forwarded 451 pkts(676500 bytes)

Total 1 entry Listed
Matched 1 entry
```

查看 SwitchA 含端口信息的组播组信息。

```
<SwitchA> display mpm group
  Total 1 IP Group(s).
  Total 1 MAC Group(s).

  Vlan(id):101.
    Total 0 IP Group(s).
    Total 0 MAC Group(s).
    Router port(s):Ethernet1/0/2
  Vlan(id):200.
    Total 1 IP Group(s).
    Total 1 MAC Group(s).
    Router port(s):
    IP group(s):the following ip group(s) match to one mac group.
        IP group address:224.1.1.1
        Host port(s):Ethernet1/0/15
    MAC group(s):
        MAC group address:0100-5e01-0101
        Host port(s):Ethernet1/0/15
```

查看 SwitchE 上 IGMP Snooping 侦测到的组播组信息。

```
<SwitchE> display igmp-snooping group
  Total 1 IP Group(s).
  Total 1 MAC Group(s).

  Vlan(id):100.
    Total 1 IP Group(s).
    Total 1 MAC Group(s).
    Router port(s):Ethernet1/0/2
    IP group(s):the following ip group(s) match to one mac group.
```

```
        IP group address:224.1.1.1
        Host port(s):Ethernet1/0/19
    MAC group(s):
        MAC group address:0100-5e01-0101
        Host port(s):Ethernet1/0/19
```

通过以上显示信息可以看出 SwitchD 和 SwitchA 都已正确建立组播转发表项，并且 HostA 已成功接受到组播数据。

(2) 在 SwitchE 上配置 IGMP Snooping 组播组过滤功能。

在 SwitchE 上配置对组播组 224.1.1.1 的过滤功能。

```
<SwitchE> system-view
[SwitchE-acl-basic-2000] rule deny source 224.1.1.1 0
[SwitchE-acl-basic-2000] rule permit source any
[SwitchE-acl-basic-2000] quit
[SwitchE]igmp-snooping group-policy 2000 vlan 100
```

查看 SwitchA 的组播转发表项。

```
<SwitchA> display multicast forwarding-table
Multicast Forwarding Cache Table
Total 1 entry: 0 entry created by IP, 1 entry created by protocol

00001. (10.110.5.100, 224.1.1.1), iif Vlan-interface101, 0 oifs,
     Protocol Create
     Matched 5 pkts(7500 bytes), Wrong If 0 pkts
     Forwarded 0 pkts(0 bytes)

Total 1 entry Listed
```

以上显示信息表明 SwitchA 已停止转发组播数据。

查看 SwitchE 的组播组信息。

```
<SwitchE> display igmp-snooping group
  Total 0 IP Group(s).
  Total 0 MAC Group(s).

  Vlan(id):200.
    Total 0 IP Group(s).
    Total 0 MAC Group(s).
    Router port(s):Ethernet1/0/19
```

在配置了组播组过滤功能后，相应端口不能收到 IGMP 报告报文，IP 组播组和 MAC 组在定时器超时后被删除。

(3) 在 SwitchA 上配置 IGMP 组播组过滤功能。

关闭 SwitchE 上组播组过滤功能。

```
<SwitchE> system-view
[SwitchE] undo igmp-snooping group-policy
```

📖 **说明：**

为了避免不能区分 IGMP Snooping 的组播组过滤规则与 IGMP 的组播组过滤规则是哪一个在起作用，这里先关闭 IGMP Snooping 的组播组过滤功能。

在 SwitchA 的 Vlan-interface100 上启动对组播组 224.1.1.1 的过滤功能，查看 SwitchA 的组播转发表项。

在 SwitchA 的 Vlan-interface100 上启动对组播组 224.1.1.1 的过滤功能。

```
<SwitchA> system-view
[SwitchA] acl number 2000
[SwitchA-acl-basic-2000] rule deny source  224.1.1.1 0
[SwitchA-acl-basic-2000] rule permit source any
[SwitchA-acl-basic-2000] quit
[SwitchA] interface Vlan-interface 100
[SwitchA-Vlan-interface100] igmp group-policy 2000
[SwitchA-Vlan-interface100] return
```

查看 SwitchA 的组播转发表。

```
<SwitchA> display multicast forwarding-table
Multicast Forwarding Cache Table
Total 1 entry: 0 entry created by IP, 1 entry created by protocol

00001. (10.110.5.100, 224.1.1.1), iif Vlan-interface101, 0 oifs,
     Protocol Create
     Matched 5 pkts(7500 bytes), Wrong If 0 pkts
     Forwarded 0 pkts(0 bytes)

Total 1 entry Listed
```

查看 SwitchA 组播组信息。

```
<SwitchA> display igmp group
 Total 0 IGMP groups reported on this router
```

在配置了组播组过滤功能后，相应端口不能收到 IGMP 报告报文，相应的组播组在定时器超时后被删除。

📖 **说明：**

可以看出 IGMP Snooping 的组播组过滤规则与 IGMP 的组播组过滤规则作用相同的，用户可以在不同的组网情况下进行相应的配置。

2.2 PIM-SM+IGMP+IGMP Snooping 配置举例

2.2.1 需求分析

用户通过组播方式接收视频点播信息，根据用户需求的不同，视频信息的接收方式也不尽相同：

(1) 为了避免视频信息在二层的广播，HostA 和 HostB 通过连接到运行 IGMP Snooping 的 SwitchE 接收组播数据；

(2) 为了可靠和稳定的的接收组播数据，HostC 和 HostD 直接连接到与 SwitchB 和 SwitchC 相连的末梢网络 N1 接收组播数据，从而可以实现上行链路的备份；

(3) 整个 PIM 域采用 SM 单 BSR 管理域方式，各个交换机之间运行 OSPF 协议。

2.2.2 网络布局

(1) SwitchD 通过 Vlan-interface300 接口与组播源 Source 所在网络连接；

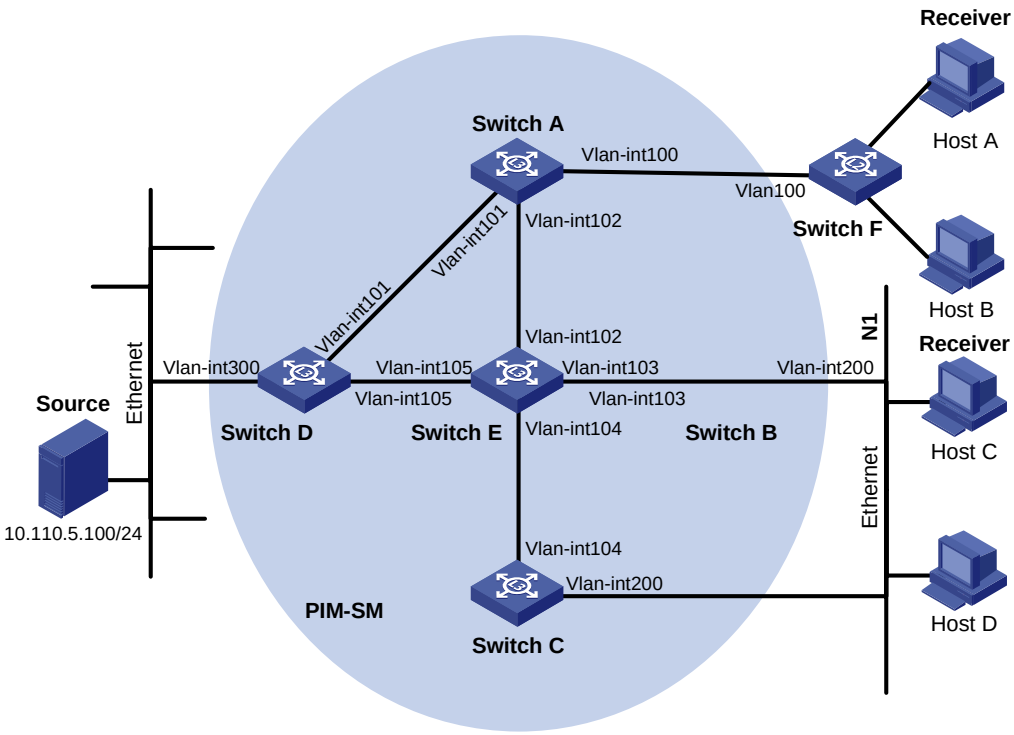
(2) SwitchA 通过 Vlan-interface100 接口连接 SwitchF，通过 Vlan-interface101 接口连接 SwitchD，通过 Vlan-interface102 接口连接 SwitchE

(3) SwitchB 和 SwitchC 通过各自的 Vlan-interface200 接口连接末梢网络 N1，分别通过 Vlan-interface103 和 Vlan-interface104 接口连接 SwitchE；

(4) 将 SwitchD 的 Vlan-interface105 接口和 SwitchE 的 Vlan-interface102 接口作为 C-BSR 和 C-RP。

(5) 在 SwitchA 的 Vlan-interface100 接口上运行 IGMPV2，在 SwitchF 上全局启动 IGMP Snooping 和在 VLAN100 内启动 IGMP Snooping；SwitchB 和 SwitchC 与末梢网络 N1 之间也运行 IGMPv2，通常 SwitchB 充当查询器。

2.2.3 组网图



设备	接口	IP 地址	包含端口
Switch A	Vlan-int100	10.110.1.1/24	Ethernet1/0/1
	Vlan-int101	192.168.1.1/24	Ethernet1/0/2
	Vlan-int102	192.168.9.1/24	Ethernet1/0/3
Switch B	Vlan-int200	10.110.2.1/24	Ethernet1/0/1
	Vlan-int103	192.168.2.1/24	Ethernet1/0/2
Switch C	Vlan-int200	10.110.2.2/24	Ethernet1/0/1
	Vlan-int104	192.168.3.1/24	Ethernet1/0/2
Switch D	Vlanint300	10.110.5.1/24	Ethernet1/0/1
	Vlanint101	192.168.1.2/24	Ethernet1/0/2
	Vlanint105	192.168.4.2/24	Ethernet1/0/3
Switch E	Vlanint104	192.168.3.2/24	Ethernet1/0/3
	Vlanint103	192.168.2.2/24	Ethernet1/0/2
	Vlanint102	192.168.9.2/24	Ethernet1/0/1
	Vlanint105	192.168.4.1/24	Ethernet1/0/4
Switch F	Vlan100	-	Ethernet1/0/1、Ethernet1/0/2、Ethernet1/0/3

图2-2 PIM-SM＋IGMP＋IGMP Snooping 典型配置组网图

2.2.4 配置步骤

1. 配置各交换机的 VLAN、VLAN 接口及其 IP 地址

配置 SwitchA 的 VLAN、VLAN 接口及其 IP 地址。

```
<SwitchA> system-view
System View: return to User View with Ctrl+Z.
[SwitchA] vlan 100
```

```
[SwitchA-vlan100] port Ethernet 1/0/1
[SwitchA-vlan100] quit
[SwitchA] vlan 101
[SwitchA-vlan101] port Ethernet 1/0/2
[SwitchA-vlan101] quit
[SwitchA] vlan 102
[SwitchA-vlan102] port Ethernet 1/0/3
[SwitchA-vlan102] quit
[SwitchA] interface Vlan-interface 100
[SwitchA-Vlan-interface100] ip address 10.110.1.1 24
[SwitchA-Vlan-interface100] quit
[SwitchA] interface Vlan-interface 101
[SwitchA-Vlan-interface101] ip address 192.168.1.1 24
[SwitchA-Vlan-interface101] quit
[SwitchA] interface Vlan-interface 102
[SwitchA-Vlan-interface102] ip address 192.168.9.1 24
[SwitchA-Vlan-interface102] quit
```

请参照图 2-2配置其他各交换机的VLAN、VLAN接口及其IP地址，具体的配置过程略。

2. 配置单播路由协议

在 SwitchA 上配置 Router ID 并配置 OSPF 协议。

```
<SwitchA> system-view.
[SwitchA]router id 1.1.1.1
[SwitchA]ospf
[SwitchA-ospf-1]area 0
[SwitchA-ospf-1-area-0.0.0.0]network 10.110.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0]network 192.168.1.0 0.0.0.255
[SwitchA-ospf-1-area-0.0.0.0]network 192.168.9.0 0.0.0.255
```

SwitchB、SwitchC、SwitchD 和 SwitchE 的配置与 SwitchA 相似，配置过程略。

3. 配置组播协议

在 SwitchA 上启动组播路由，在各接口上启动 PIM-SM，并在 Vlan-interface100 接口上启动 IGMPv2。

```
<SwitchA> system-view
[SwitchA] multicast routing-enable
[SwitchA] interface Vlan-interface 100
[SwitchA-Vlan-interface100] igmp enable
[SwitchA-Vlan-interface100] pim sm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 101
```

```
[SwitchA-Vlan-interface101] pim sm
[SwitchA-Vlan-interface101] quit
[SwitchA] interface vlan-interface 102
[SwitchA-Vlan-interface102] pim sm
```

📖 **说明：**

只有存在组播接受者的接口上才有必要启动 IGMP，并且由于缺省情况下，启动了 IGMP 的接口上运行的就是 IGMPv2，所以不需要再重复配置 IGMP 的版本。

Switch B 和 Switch C 的配置与 Switch A 相似，Switch D 和 Switch E 除了不需要在相应接口上启动 IGMP 外，其它的配置也与 Switch A 相似，配置过程略。

在 Switch D 上配置 RP 通告的服务范围，以及 C-BSR 和 C-RP 的位置。

```
<SwitchD> system-view
[SwitchD] acl number 2005
[SwitchD-acl-basic-2005] rule permit source 225.1.1.0 0.0.0.255
[SwitchD-acl-basic-2005] quit
[SwitchD] pim
[SwitchD-pim] c-bsr vlan-interface 105 24 2
[SwitchD-pim] c-rp vlan-interface 105 group-policy 2005 priority 2
[SwitchD-pim] quit
```

在 Switch E 上配置 RP 通告的服务范围，以及 C-BSR 和 C-RP 的位置。

```
<SwitchE> system-view
[SwitchE] acl number 2005
[SwitchE-acl-basic-2005] rule permit source 225.1.1.0 0.0.0.255
[SwitchE-acl-basic-2005] quit
[SwitchE] pim
[SwitchE-pim] c-bsr vlan-interface 102 24 1
[SwitchE-pim] c-rp vlan-interface 102 group-policy 2005 priority 1
[SwitchE-pim] quit
```

在 SwitchF 上全局启动 IGMP Snooping，并在 Vlan100 内启动 IGMP Snooping。

```
<SwitchF> system-view
[SwitchF] igmp-snooping enable
  Enable IGMP-Snooping ok.
[SwitchF] vlan 100
[SwitchF-vlan100] igmp-snooping enable
[SwitchF-vlan100] quit
```

4. 检验配置效果

现在从组播源 Source 向组播组 225.1.1.1 发送组播数据，HostA 和 HostC 点播组播组 225.1.1.1 的组播数据，检验各个交换机的配置效果。

(1) 通过查看命令判断 HostA 和 HostC 是否接收到组播数据。

查看 Switch E 上 PIM 的邻居关系信息。

```
<SwitchE> display pim neighbor
Neighbor's Address  Interface Name                Uptime    Expires
192.168.9.1         Vlan-interface102             02:47:04  00:01:42
192.168.2.1         Vlan-interface103             02:45:04  00:04:46
192.168.3.1         Vlan-interface104             02:42:24  00:04:45
192.168.4.2         Vlan-interface105             02:43:44  00:05:44
```

查看 Switch E 上的 BSR 信息。

```
<SwitchE> display pim bsr-info
  Current BSR Address: 192.168.4.2
             Priority: 2
          Mask Length: 24
              Expires: 00:01:39
  Local Host is C-BSR: 192.168.9.2
             Priority: 1
          Mask Length: 24
```

查看 Switch E 上的 RP 信息。

```
<SwitchE> display pim rp-info
 PIM-SM RP-SET information:
    BSR is: 192.168.4.2

    Group/MaskLen: 225.1.1.0/24
      RP 192.168.9.2
        Version: 2
        Priority: 1
        Uptime: 00:03:15
        Expires: 00:01:14
      RP 192.168.4.2
        Version: 2
        Priority: 2
        Uptime: 00:04:25
        Expires: 00:01:09
```

查看 Switch A 上 PIM 路由表信息。

```
<SwitchA> display pim routing-table
PIM-SM Routing Table
Total 1 (S,G) entries, 1 (*,G) entries, 0 (*,*,RP) entry

(*, 225.1.1.1), RP 192.168.9.2
    Protocol 0x20: PIMSM, Flag 0x2003: RPT WC NULL_IIF
```

```
    Uptime: 00:23:21, never timeout
    Upstream interface: Vlan-interface102, RPF neighbor: 192.168.9.2
    Downstream interface list:
      Vlan-interface100, Protocol 0x1: IGMP, never timeout
(10.110.5.100, 225.1.1.1)
    Protocol 0x20: PIMSM, Flag 0x80004: SPT
    Uptime: 00:03:43, Timeout in 199 sec
    Upstream interface: Vlan-interface102, RPF neighbor: 192.168.9.2
    Downstream interface list:
      Vlan-interface100, Protocol 0x1: IGMP, never timeout
Matched 1 (S,G) entries, 1 (*,G) entries, 0 (*,*,RP) entry
```

Switch B 和 Switch C 上的显示信息与 Switch A 类似。

查看 SwitchD 上 PIM 路由表信息。

```
<SwitchD> display pim routing-table
PIM-SM Routing Table
Total 1 (S,G) entry, 0 (*,G) entry, 0 (*,*,RP) entry

(10.110.5.100, 225.1.1.1)
    Protocol 0x20: PIMSM, Flag 0x4: SPT
    Uptime: 00:03:03, Timeout in 27 sec
    Upstream interface: Vlan-interface300, RPF neighbor: NULL
    Downstream interface list:
      Vlan-interface101, Protocol 0x200: SPT, timeout in 147 sec
      Vlan-interface105, Protocol 0x200: SPT, timeout in 145 sec
Matched 1 (S,G) entry, 0 (*,G) entry, 0 (*,*,RP) entry
```

查看 Switch E 上的 PIM 路由表信息。

```
<SwitchE> display pim routing-table
PIM-SM Routing Table
Total 1 (S,G) entry, 1 (*,G) entry, 0 (*,*,RP) entry

(*,225.1.1.1), RP 192.168.9.2
    Protocol 0x20: PIMSM, Flag 0x2003: RPT WC NULL_IIF
    Uptime: 00:02:34, Timeout in 176 sec
    Upstream interface: Null, RPF neighbor: 0.0.0.0
    Downstream interface list:
      Vlan-interface102, Protocol 0x100: RPT, timeout in 176 sec
      Vlan-interface103, Protocol 0x100: SPT, timeout in 135 sec

(10.110.5.100, 225.1.1.1)
    Protocol 0x20: PIMSM, Flag 0x4: SPT
    Uptime: 00:03:03, Timeout in 27 sec
```

```
    Upstream interface: Vlan-interface105, RPF neighbor: 192.168.4.2
    Downstream interface list:
      Vlan-interface102, Protocol 0x200: SPT, timeout in 147 sec
      Vlan-interface103, Protocol 0x200: SPT, timeout in 145 sec
Matched 1 (S,G) entry, 1 (*,G) entry, 0 (*,*,RP) entry
```

查看 SwitchF 上 IGMP Snooping 侦测到的组播组信息。

```
<SwitchF> display igmp-snooping group
  Total 1 IP Group(s).
  Total 1 MAC Group(s).

  Vlan(id):100.
    Total 1 IP Group(s).
    Total 1 MAC Group(s).
    Router port(s):Ethernet1/0/2
    IP group(s):the following ip group(s) match to one mac group.
        IP group address:225.1.1.1
        Host port(s):Ethernet1/0/19
    MAC group(s):
        MAC group address:0100-5e01-0101
        Host port(s):Ethernet1/0/19
```

查看 SwitchB 含端口信息的组播组信息。

```
<SwitchB> display mpm group
  Total 1 IP Group(s).
  Total 1 MAC Group(s).

  Vlan(id):200.
    Total 1 IP Group(s).
    Total 1 MAC Group(s).
    Router port(s):
    IP group(s):the following ip group(s) match to one mac group.
        IP group address:225.1.1.1
        Host port(s):Ethernet1/0/24
    MAC group(s):
        MAC group address:0100-5e01-0101
        Host port(s):Ethernet1/0/24

  Vlan(id):103.
    Total 0 IP Group(s).
    Total 0 MAC Group(s).
    Router port(s):Ethernet1/0/10
```

通过以上显示信息可以说明 hostA 和 HostC 可以接收到组播数据。

(2) 配置模拟主机加入功能。

现在在 SwitchB 上配置以太网端口加入指定组播组，以避免由于某些原因而导致的组播交换机认为该网段没有组播组的成员，从而取消相应的路径。

配置以太网端口 Ethernet1/0/21 加入组播组 225.1.1.1。

```
<SwitchB> system-view
[SwitchB] interface Vlan-interface 200
[SwitchB-Vlan-interface200] igmp host-join 225.1.1.1 port Ethernet 1/0/21
```

查看 SwitchB 含端口信息的组播组信息。

```
<SwitchB> display mpm group
  Total 1 IP Group(s).
  Total 1 MAC Group(s).

  Vlan(id):200.
    Total 1 IP Group(s).
    Total 1 MAC Group(s).
    Router port(s):
    IP group(s):the following ip group(s) match to one mac group.
        IP group address:225.1.1.1
        Host port(s):Ethernet1/0/21             Ethernet1/0/24
    MAC group(s):
        MAC group address:0100-5e01-0101
        Host port(s):Ethernet1/0/21             Ethernet1/0/24

  Vlan(id):103.
    Total 0 IP Group(s).
    Total 0 MAC Group(s).
    Router port(s):Ethernet1/0/10
```

通过以上显示信息可以看出 Ethernet 1/0/21 已成为组播组 225.1.1.1 的主机成员端口。

2.3 IGMP Snooping Only 配置举例

2.3.1 组网需求

在某些情况下，没有必要或是没有条件组建三层组播网络时，可以组建一个在所有设备上都启动 IGMP Snooping 的网络，这样也可以实现某些组播功能。

2.3.2 网络布局

(1) 如图 2-3所示，在一个没有三层设备的纯二层网络环境中，Switch C通过Ethernet1/0/3 接口连接组播源（Source），Switch B和Switch C上分别连接至少一个接收者（Receiver）；

(2) Switch A、Switch B 和 Switch C 上都运行 IGMP Snooping，并由 Switch A 充当 IGMP Snooping 查询器；

(3) 为了防止 Switch A 和 Switch B 在没有组播转发表项的情况下，将组播报文在 VLAN 内广播，在 Switch A 和 Switch B 上要启动未知组播报文丢弃功能。

2.3.3 组网图

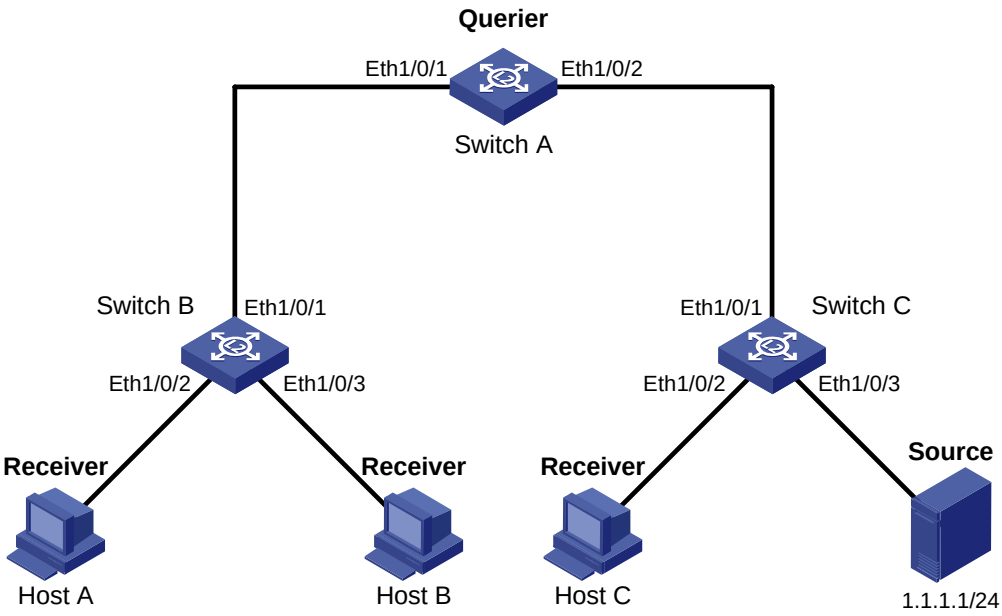


图2-3 IGMP Snooping Only 配置组网图

2.3.4 配置步骤

1. 配置 Switch A

全局启动 IGMP Snooping。

```
<SwitchA> system-view
[SwitchA] igmp-snooping enable
Enable IGMP-Snooping ok.
```

创建 VLAN 100，把端口 Ethernet1/0/1 和 Ethernet1/0/2 添加到该 VLAN 中，并在该 VLAN 内启动 IGMP Snooping。

```
[SwitchA] vlan 100
[SwitchA-vlan100] port Ethernet 1/0/1 Ethernet 1/0/2
```

```
[SwitchA-vlan100] igmp-snooping enable
```

在 VLAN 100 内启动 IGMP Snooping 查询器。

```
[SwitchA-vlan100] igmp-snooping querier
[SwitchA-vlan100] quit
```

启动未知组播报文丢弃功能

```
[SwitchA] unknown-multicast drop enable
```

2. 配置 Switch B

全局启动 IGMP Snooping。

```
<SwitchB> system-view
[SwitchB] igmp-snooping enable
Enable IGMP-Snooping ok.
```

创建 VLAN 100，把端口 Ethernet1/0/1 到 Ethernet1/0/3 添加到该 VLAN 中，并在该 VLAN 内启动 IGMP Snooping。

```
[SwitchB] vlan 100
[SwitchB-vlan100] port Ethernet 1/0/1 to Ethernet 1/0/3
[SwitchB-vlan100] igmp-snooping enable
[SwitchB-vlan100] quit
```

启动未知组播报文丢弃功能

```
[SwitchB] unknown-multicast drop enable
```

3. 配置 Switch C

全局启动 IGMP Snooping。

```
<SwitchC system-view
[SwitchC] igmp-snooping enable
Enable IGMP-Snooping ok.
```

创建 VLAN 100，把端口 Ethernet1/0/1 到 Ethernet1/0/3 添加到该 VLAN 中，并在该 VLAN 内启动 IGMP Snooping。

```
[SwitchC] vlan 100
[SwitchC-vlan100] port Ethernet 1/0/1 to Ethernet 1/0/3
[SwitchC-vlan100] igmp-snooping enable
```

⚠ 注意：

在 SwitchC 上不要启动未知组播报文丢弃功能，所以为了防止在组播报文对网络和 SwitchC 的冲击，组网规划时应尽量将查询器配置在有组播源的设备上。

4. 检验配置效果

(1) 查看 SwitchB 的相关显示信息

查看 Switch B 上收到的 IGMP 报文的统计信息。

```
<SwitchB> display igmp-snooping statistics
  Received IGMP general query packet(s) number:16.
  Received IGMP specific query packet(s) number:3.
  Received IGMP V1 report packet(s) number:0.
  Received IGMP V2 report packet(s) number:53.
  Received IGMP leave packet(s) number:1.
  Received error IGMP packet(s) number:0.
  Sent IGMP specific query packet(s) number:1.
```

Switch B 收到了查询器的 IGMP 普遍组查询报文和接收者的 IGMP 报告报文。

查看 Switch B 上的组播组信息。

```
<Switch B> display igmp-snooping group
  Total 1 IP Group(s).
  Total 1 MAC Group(s).

  Vlan(id):100.
    Total 1 IP Group(s).
    Total 1 MAC Group(s).
    Router port(s):Ethernet1/0/1
    IP group(s):the following ip group(s) match to one mac group.
        IP group address:224.1.1.1
        Host port(s):Ethernet1/0/2
    MAC group(s):
        MAC group address:0100-5e7f-fffe
        Host port(s):Ethernet1/0/2
```

以上显示信息表明，Switch B 上已经建立起以路由器端口为 Ethernet1/0/1 和主机成员端口为 Ethernet1/0/2 的组播组 224.1.1.1。

(2) 查看 SwitchA 的相关显示信息

查看 Switch A 上收到的 IGMP 报文的统计信息。

```
<SwitchA> display igmp-snooping statistics
  Received IGMP general query packet(s) number:0.
  Received IGMP specific query packet(s) number:0.
  Received IGMP V1 report packet(s) number:0.
  Received IGMP V2 report packet(s) number:53.
  Received IGMP leave packet(s) number:1.
  Received error IGMP packet(s) number:0.
```

```
  Sent IGMP specific query packet(s) number:1.
```

Switch A 收到了接收者的 IGMP 报告报文。

查看 Switch A 上的组播组信息。

```
<Switch A> display igmp-snooping group
  Total 1 IP Group(s).
  Total 1 MAC Group(s).

  Vlan(id):100.
    Total 1 IP Group(s).
    Total 1 MAC Group(s).
    Router port(s):
    IP group(s):the following ip group(s) match to one mac group.
        IP group address:224.1.1.1
        Host port(s):Ethernet1/0/1
    MAC group(s):
        MAC group address:0100-5e7f-fffe
        Host port(s):Ethernet1/0/1
```

以上显示信息表明，Switch A 上已经建立起以主机成员端口为 Ethernet1/0/1 的组播组 224.1.1.1，由于在 SwitchA 已经启动了 IGMP Snooping 查询器，所以没有路由器端口。

(3) 查看 SwitchC 的相关显示信息

查看 Switch C 上收到的 IGMP 报文的统计信息。

```
<SwitchC> display igmp-snooping statistics
  Received IGMP general query packet(s) number:10.
  Received IGMP specific query packet(s) number:0.
  Received IGMP V1 report packet(s) number:0.
  Received IGMP V2 report packet(s) number:0.
  Received IGMP leave packet(s) number:.0
  Received error IGMP packet(s) number:0.
  Sent IGMP specific query packet(s) number:0.
```

Switch C 只收到了查询器的 IGMP 普遍组查询报文。

查看 Switch C 上的组播组信息。

```
<Switch C> display igmp-snooping group
  Total 0 IP Group(s).
  Total 0 MAC Group(s).

Vlan(id):100.
    Total 0 IP Group(s).
    Total 0 MAC Group(s).
```

```
Router port(s):Ethernet1/0/1
```

以上显示信息可以看出，Switch C 上并没有建立起相关组播表项，组播源将组播数据将在所有端口广播，所以请不要在 SwitchC 上启动未知组播报文丢弃功能。

2.4 MSDP 配置举例

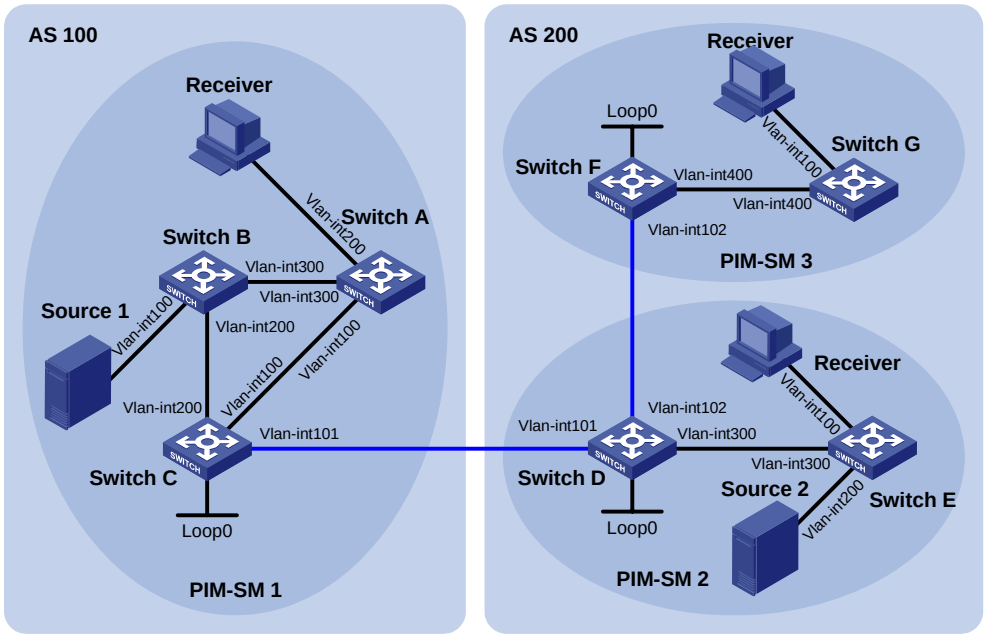
2.4.1 组网需求

现在要实现多个不同 PIM-SM 域之间的组播源和组播接收者的组播点播，所以要应用到 MSDP 使这些 PIM-SM 域的 RP 之间建立起 MSDP 对等体关系。使它们能够在域间相互转发 SA 消息，共享组播源信息。

2.4.2 网络布局

- 两个 ISP 所维护网络的自治系统分别为 AS 100 和 AS 200，各 AS 内部采用 OSPF 进行互联，AS 之间采用 BGP 交换路由信息；
- PIM-SM 1 属于 AS 100，PIM-SM 2 和 PIM-SM 3 属于 AS 200；
- 每个 PIM-SM 域分别拥有 0 或 1 个组播源以及至少一个接收者，域内运行 OSPF 协议以提供单播路由；
- 将 Switch C、Switch D 和 Switch F 各自的 Loopback0 接口分别配置为各自 PIM-SM 域的 C-BSR 和 C-RP；
- 在 Switch C 与 Switch D 之间通过 EBGP 建立 MSDP 对等体关系，在 Switch D 与 Switch F 之间通过 IBGP 建立 MSDP 对等体关系。

2.4.3 组网图



设备	接口	IP 地址	设备	接口	IP 地址
SwitchA	Vlan-int100	10.110.1.2/24	Switch D	Vlan-int300	10.110.4.1/24
	Vlan-int200	10.110.6.1/24		Vlan-int102	192.168.3.1/24
	Vlan-int300	10.110.5.1/24		Vlan-int101	192.168.1.2/24
SwitchB	Vlan-int100	10.110.7.1/24		Loop0	2.2.2.2/32
	Vlan-int200	10.110.2.2/24	Switch E	Vlan-int100	10.110.8.1/24
	Vlan-int300	10.110.5.2/24		Vlan-int200	10.110.9.1/24
Switch C	Vlan-int100	10.110.1.1/24		Vlan-int300	10.110.4.2/24
	Vlan-int200	10.110.2.1/24		Loop0	2.2.2.2/32
	Vlan-int101	192.168.1.1/24	Switch F	Vlan-int400	10.110.3.1/24
	Loop0	1.1.1.1/32		Vlan-int102	192.168.3.2/24
				Loop0	3.3.3.3/32
			SwitchG	Vlan-int100	10.110.10.1/24
				Vlan-int400	10.110.3.2/24

图2-4 MSDP 配置举例

2.4.4 配置步骤

1. 配置各交换机的接口 IP 地址和单播路由协议

请按照图 2-4配置各接口的IP地址和子网掩码，具体配置过程略。

配置各域内的交换机之间采用 OSPF 协议进行互连，确保 PIM-SM 1 域中 Switch A、Switch B 和 Switch C 之间能够在网络层互通，PIM-SM 2 域中 Switch D 和 Switch E 之间能够在网络层互通，PIM-SM 3 域中 Switch F 和 Switch G 之间能够在网络层互通，并且每个 PIM-SM 域内各交换机之间能够借助单播路由协议实现动态路由更新，具体配置过程略。

2. 配置各自治系统内的单播路由协议

在 SwitchC 上配置 OSPF 协议。

```
<SwitchC> system-view.
[SwitchC]ospf
[SwitchC-ospf-1]area 0
[SwitchC-ospf-1-area-0.0.0.0]network 10.110.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0]network 10.110.2.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0]network 1.1.1.1 0.0.0.0
```

SwitchA、SwitchB、SwitchD、SwitchE、SwitchF 和 SwitchG 的配置与 SwitchC 相似，配置过程略。

3. 配置组播路由协议

(1) 启动 IP 组播路由，在各接口上启动 PIM-SM，并在存在接收者的接口上启动 IGMP。

在 Switch A 上启动 IP 组播路由，在各接口上启动 PIM-SM，并在 Vlan-interface200 上启动 IGMP。

```
<SwitchA> system-view
[SwitchA] multicast routing-enable
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] pim sm
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 200
[SwitchA-Vlan-interface200] pim sm
[SwitchA-Vlan-interface200] igmp enable
[SwitchA-Vlan-interface200] quit
[SwitchA] interface vlan-interface 300
[SwitchA-Vlan-interface101] pim sm
```

Switch E 和 Switch G 上的配置与 Switch A 相似，配置过程略。

在 Switch C 上启动 IP 组播路由，并在各接口上启动 PIM-SM。

```
<SwitchC> system-view
[SwitchC] multicast routing-enable
[SwitchC] interface vlan-interface 100
[SwitchC-Vlan-interface100] pim sm
[SwitchC-Vlan-interface100] quit
[SwitchC] interface vlan-interface 200
[SwitchC-Vlan-interface200] pim sm
[SwitchC-Vlan-interface200] quit
[SwitchC] interface vlan-interface 101
[SwitchC-Vlan-interface101] pim sm
```

Switch B、Switch D 和 Switch F 上的配置与 Switch C 相似，配置过程略。

在 Switch C 上配置 BSR 服务边界。

```
[SwitchC-Vlan-interface101] pim bsr-boundary
[SwitchC-Vlan-interface101] quit
```

Switch D 和 Switch F 上的配置与 Switch C 相似，配置过程略。

(2) 配置 Loopback0 接口和 C-BSR、C-RP 的位置

在 Switch C 上配置 Loopback0 接口和 C-BSR、C-RP 的位置。

```
[SwitchC] interface loopback 0
[SwitchC-LoopBack0] ip address 1.1.1.1 255.255.255.255
[SwitchC-LoopBack0] pim sm
[SwitchC-LoopBack0] quit
[SwitchC] pim
[SwitchC-pim] c-bsr loopback 0 24
[SwitchC-pim] c-rp loopback 0
[SwitchC-pim] quit
```

Switch D 和 Switch F 上的配置与 Switch C 相似，配置过程略。

4. 配置自治系统间的 BGP 路由协议，将 BGP 与 OSPF 互相引入

在 Switch C 上配置 EBGP 协议，并引入 OSPF 路由。

```
[SwitchC] bgp 100
[SwitchC-bgp] group 100 external
[SwitchC-bgp] peer 192.168.1.2 group 100 as-number 200
[SwitchC-bgp] import-route ospf 1
[SwitchC-bgp] import-route direct
[SwitchC-bgp] quit
```

在 Switch D 上配置 IBGP 和 EBGP 协议，并引入 OSPF 路由。

```
[SwitchD] bgp 200
[SwitchD-bgp] group 100 external
[SwitchD-bgp] group 200
[SwitchD-bgp] peer 192.168.1.1 group 100 as-number 100
[SwitchD-bgp] peer 192.168.3.2 group 200
[SwitchD-bgp] import-route ospf 1
[SwitchD-bgp] import-route direct
[SwitchD-bgp] quit
```

在 Switch F 上配置 IBGP 协议，并引入 OSPF 路由。

```
[SwitchF] bgp 200
[SwitchF-bgp] group 200
[SwitchF-bgp] peer 192.168.3.1 group 200
```

```
[SwitchF-bgp] import-route ospf 1
[SwitchF-bgp] import-route direct
[SwitchF-bgp] quit
```

在 Switch C 的 OSPF 中引入 BGP。

```
[SwitchC] ospf 1
[SwitchC-ospf-1] import-route bgp
[SwitchC-ospf-1] quit
```

Switch D 和 Switch F 上的配置与 Switch C 相似，配置过程略。

通过使用 **display bgp peer** 命令可以查看交换机之间 BGP 对等体的关系。例如：

查看 Switch C 上 BGP 对等体关系的信息。

```
[SwitchC] display bgp peer

    Peer        AS-num Ver Queued-Tx    Msg-Rx    Msg-Tx    Up/Down  State
--------------------------------------------------------------------------
192.168.1.2      200  4         0       950       945   15:41:14 Established
```

查看 SwitchD 上 BGP 对等体关系的信息。

```
[SwitchD] display bgp peer

    Peer        AS-num Ver Queued-Tx    Msg-Rx    Msg-Tx    Up/Down  State
--------------------------------------------------------------------------
192.168.1.1      100  4         0       946       953   15:43:32 Established
192.168.3.2      200  4         0       946       954   15:41:18 Established
```

查看 SwitchF 上 BGP 对等体关系的信息。

```
[SwitchF] display bgp peer

    Peer        AS-num Ver Queued-Tx    Msg-Rx    Msg-Tx    Up/Down  State
--------------------------------------------------------------------------
192.168.3.1      200  4         0       953       948   15:42:23 Established
```

5. 配置 MSDP 对等体

在 Switch C 上配置 MSDP 对等体。

```
[SwitchC] msdp
[SwitchC-msdp] peer 192.168.1.2 connect-interface vlan-interface 101
[SwitchC-msdp] quit
```

在 SwitchD 上配置 MSDP 对等体。

```
[SwitchD] msdp
[SwitchD-msdp] peer 192.168.1.1 connect-interface vlan-interface 101
[SwitchD-msdp] peer 192.168.3.2 connect-interface vlan-interface 102
```

```
[SwitchD-msdp] quit
```

在 SwitchF 上配置 MSDP 对等体。

```
[SwitchF] msdp
[SwitchF-msdp] peer 192.168.3.1 connect-interface vlan-interface 102
[SwitchF-msdp] quit
```

当 PIM-SM 1 域内的组播源 Source1 发送组播信息时，PIM-SM 2 和 PIM-SM 3 域内的接收者能收到该组播信息。通过使用 **display msdp brief** 命令可以查看交换机之间 MSDP 对等体建立情况。例如：

查看 Switch C 上 MSDP 对等体建立情况的简要信息。

```
[SwitchC] display msdp brief
 MSDP Peer Brief Information
 Peer's Address     State     Up/Down time    AS     SA Count   Reset Count
 192.168.1.2         Up        00:12:27         200    13          0
```

查看 SwitchD 上 MSDP 对等体建立情况的简要信息。

```
[SwitchD] display msdp brief
 MSDP Peer Brief Information
 Peer's Address     State     Up/Down time    AS     SA Count   Reset Count
 192.168.3.2         Up        00:15:32         200    8           0
 192.168.1.1         UP        00:06:39         100    13          0
```

查看 SwitchF 上 MSDP 对等体建立情况的简要信息。

```
[SwitchF] display msdp brief
 MSDP Peer Brief Information
 Peer's Address     State     Up/Down time    AS     SA Count   Reset Count
 192.168.3.1         UP         01:07:08        200    8           0
```

查看 Switch C 上 MSDP 对等体的详细信息。

```
[SwitchC] display msdp peer-status
  MSDP Peer 192.168.1.2, AS 200
  Description:
  Information about connection status:
    State: Up
    Up/down time: 00:15:47
    Resets: 0
    Connection interface: Vlan-interface101 (192.168.1.1)
    Number of sent/received messages: 16/16
    Number of discarded output messages: 0
    Elapsed time since last connection or counters clear: 00:17:51
  Information about (Source, Group)-based SA filtering policy:
    Import policy: none
    Export policy: none
```

```
Information about SA-Requests:
  Policy to accept SA-Request messages: none
  Sending SA-Requests status: disable
Minimum TTL to forward SA with encapsulated data: 0
SAs learned from this peer: 0, SA-cache maximum for the peer: none
Input queue size: 0, Output queue size: 0
Counters for MSDP message:
  Count of RPF check failure: 0
  Incoming/outgoing SA messages: 0/0
  Incoming/outgoing SA requests: 0/0
  Incoming/outgoing SA responses: 0/0
  Incoming/outgoing data packets: 0/0
```