H3C交换机最详细配置实例手册

资料整理 :hupoboy

目录

1.登录交换机典型配置指导

1.1 通过 Console 口配置 Telnet 登录方式典型配置指导

通过交换机 Console 口进行本地登录是登录交换机的最基本的方式也是配置通过其他方式登录交换机的基础。

1.1.1 组网图

通过 Console 口配置 Telnet 登录方式的组网图

1.1.2 应用要求

如上组网中，建立本地配置环境，只需将PC 机（或终端）的串口通过配置电缆与以太网交换机的 Console 口连接。当前用户通过 Console 口（AUX 用户界面）登录到交换机对 Telnet登录方式进行配置，且用户级别为管理级 3（ 级）。

1.1.3 配置过程和解释

配置 Telnet登录方式的公共属性

进入系统视图，启动 Telnet服务

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

配置从 VTY 用户界面登录后可以访问的命令级别为 2 级

```
[Sysname] user-interface vty 0
[Sysname-ui-vty0] user privilege level 2
```

设置 VTY0 用户界面支持 Telnet协议

```
[Sysname-ui-vty0] protocol inbound telnet
```

设置 VTY0 用户的终端屏幕的一屏显示 30 行命令

```
[Sysname-ui-vty0] screen-length 30
```

设置 VTY0 用户历史命令缓冲区可存放 20 条命令

```
[Sysname-ui-vty0] history-command max-size 20
```

设置 VTY0 用户界面的超时时间为 6 分钟

```
[Sysname-ui-vty0] idle-timeout 6
```

通过 Telnet登录用户的认证方式

Telnet登录有以下几种认证方式：

认证方式为None，认证方式为Password，认证方式为Scheme。下面我们分别描述这几种认证方式的配置：

设置通过 VTY0 用户界面登录交换机的 Telnet用户不需要进行认证

```
[Sysname] user-interface vty 0
```

```
[Sysname-ui-vty0] authentication-mode none
```

设置通过 VTY0 口登录交换机的 Telnet 用户进行 Password 认证，并设置用户的认证口令为明文方式，口令为123456

```
[Sysname] user-interface vty 0
[Sysname-ui-vty0] authentication-mode password
[Sysname-ui-vty0] set authentication password simple 123456
```

设置登录用户的认证方式为 Scheme，采用本地认证的方式

创建本地用户 guest，并进入本地用户视图

```
[Sysname] local-user guest
```

设置本地用户的认证口令为明文方式，口令为123456

```
[Sysname-luser-guest] password simple 123456
```

设置 VTY 用户的服务类型为 Telnet 且用户级别为 2

```
[Sysname-luser-guest] service-type telnet level 2
[Sysname-luser-guest] quit
```

进入 VTY 用户界面视图

```
[Sysname] user-interface vty 0
```

设置通过 VTY0 口登录交换机的 Telnet 用户进行 Scheme 认证

```
[Sysname-ui-vty0] authentication-mode scheme
[Sysname-ui-vty0] quit
```

指定 system 域为缺省域，并设置该域 Scheme 认证方式 local

```
[Sysname] domain default enable system
[Sysname] domain system
[Sysname-isp-system] authentication default local
```

1.1.4 完整配置

认证方式为 None 时 Telnet 登录方式的配置

```
#
 telnet server enable
#
user-interface vty 0
 authentication-mode none
 user privilege level 2
 history-command max-size 20
 idle-timeout 6 0
 screen-length 30
 protocol inbound telnet
```

认证方式为 Password 时 Telnet 登录方式的配置

```
#
 telnet server enable
#
user-interface vty 0
 authentication-mode none
 user privilege level 2
 set authentication password simple 123456
 history-command max-size 20
 idle-timeout 6 0
 screen-length 30
 protocol inbound telnet
```

认证方式为 Scheme 时 Telnet 登录方式的配置

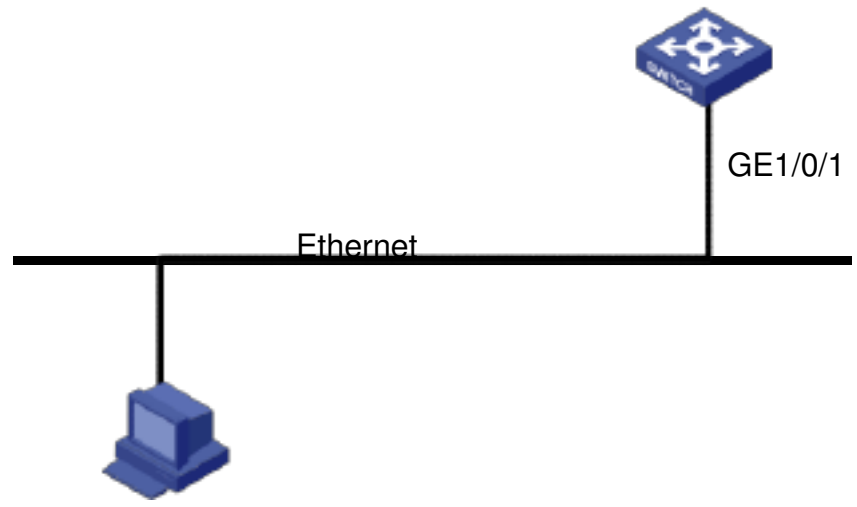
```
#
domain system
 authentication default local
#
 telnet server enable
#
local-user guest
 service-type telnet
 level 2
 password simple 123456
```

```
#
user-interface vty 0
 authentication-mode scheme
 user privilege level 2
 history-command max-size 20
 idle-timeout 6 0
 screen-length 30
 protocol inbound telnet
```

1.2 通过 Telnet 配置 Console 口登录方式典型配置指导

交换机支持 Telnet功能，用户可以通过 Telnet方式对交换机进行远程管理和维护。

1.2.1 组网图



通过 Telnet 配置 Console 口登录方式的组网图

1.2.2 应用要求

如上组网中，当前用户通过Telnet方式登录到交换机对 Console 口登录方式进行配置，且用户级别为管理级（3 级）。

1.2.3 配置过程和解释

配置 Console 口登录方式的公共属性

配置从 AUX 用户界面登录后可以访问的命令级别为 2 级。

```
[Sysname] user-interface aux 0
[Sysname-ui-aux0] user privilege level 2
```

配置 Console 口使用的波特率为 19200bit/s

```
[Sysname-ui-aux0] speed 19200
```

配置终端屏幕的一屏显示 30 行命令

```
[Sysname-ui-aux0] screen-length 30
```

配置历史命令缓冲区可存放 20 条命令

```
[Sysname-ui-aux0] history-command max-size 20
```

配置 AUX 用户界面的超时时间为 6 分钟

```
[Sysname-ui-aux0] idle-timeout 6
```

配置 Console 口登录用户的认证方式

Console 口登录有以下几种认证方式：

认证方式为None，认证方式为Password，认证方式为Scheme。下面我们分别描述这几种认证方式的配置：

设置登录用户的认证方式为None

```
[Sysname] user-interface aux 0
[Sysname-ui-aux0] authentication-mode none
```

设置登录用户的认证方式为 Password，并设置用户的认证口令为明文方式，口令为 123456

```
[Sysname] user-interface aux 0
[Sysname-ui-aux0] authentication-mode password
[Sysname-ui-aux0] set authentication password simple 123456
```

设置登录用户的认证方式为 Scheme，采用本地认证的方式

创建本地用户 guest，并进入本地用户视图

```
[Sysname] local-user guest
```

设置本地用户的认证口令为明文方式，口令为123456

```
[Sysname-luser-guest] password simple 123456
```

设置本地用户的服务类型为Terminal且用户级别为 2

```
[Sysname-luser-guest] service-type terminal level 2
[Sysname-luser-guest] quit
```

进入 AUX 用户界面视图

```
[Sysname] user-interface aux 0
```

设置通过 Console 口登录交换机的用户进行 Scheme 认证

```
[Sysname-ui-aux0] authentication-mode scheme
```

1.2.4 完整配置

认证方式为 None 时 Console 口登录方式的配置

```
#
user-interface aux 0
 authentication-mode none
 user privilege level 2
 history-command max-size 20
 idle-timeout 6 0
 speed 19200
 screen-length 30
```

认证方式为 Password 时 Console 口登录方式的配置

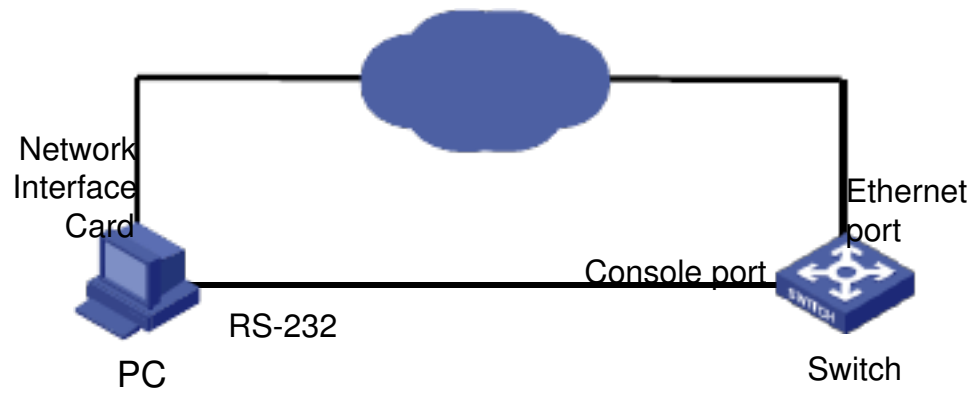
```
#
user-interface aux 0
 authentication-mode password
 user privilege level 2
 set authentication password simple 123456
 history-command max-size 20
 idle-timeout 6 0
 speed 19200
 screen-length 30
```

认证方式为 Scheme 时 Console 口登录方式的配置

```
#
local-user guest
 password simple 123456
 service-type terminal
  level 2
#
user-interface aux 0
 authentication-mode scheme
 user privilege level 2
 history-command max-size 20
 idle-timeout 6 0
 speed 19200
 screen-length 30
```

1.3 通过 WEB 网管登录交换机典型配置指导

1.3.1 组网图



通过 WEB 网管登录交换机示意图

1.3.2 应用要求

如上组网图所示，PC通过WEB网管登录交换机，实现对交换机的远程管理。

1.3.4 配置过程和解释

通过 Console 口正确配置以太网交换机 VLAN 1 接口的 IP 地址（VLAN 1 为交换机的缺省 VLAN）为10.153.17.82，子网掩码为255.255.255.0。

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-VLAN-interface1] ip address 10.153.17.82 255.255.255.0
[Sysname-VLAN-interface1] quit
```

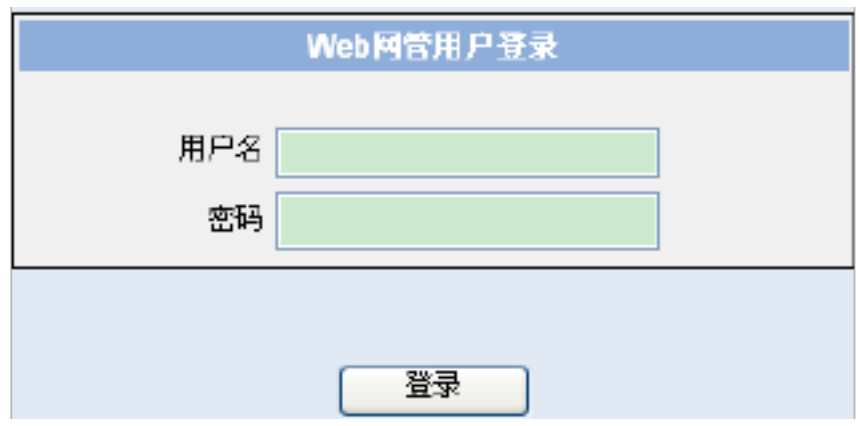
配置 WEB 网管用户名为 admin，认证口令为 admin，用户级别为 3 级。

```
[Sysname] local-user admin
[Sysname-luser-admin] service-type telnet level 3
[Sysname-luser-admin] password simple admin
[Sysname-luser-admin] quit
```

开启交换机的 WEB Server 功能。

```
[Sysname] ip http enable
```

通过浏览器登录交换机：在 WEB 网管终端(PC)的浏览器地址栏内输入 （WEB 网管终端和以太网交换机之间要路由可达），浏览器会显示 WEB 网管的登录页面，如 WEB 网管 登录页面所示。



WEB 网管登录页面

输入在交换机上添加的用户名和密码，点击<登录>按钮后即可登录，显示 WEB 网管初始页面。

1.3.5 完整配置

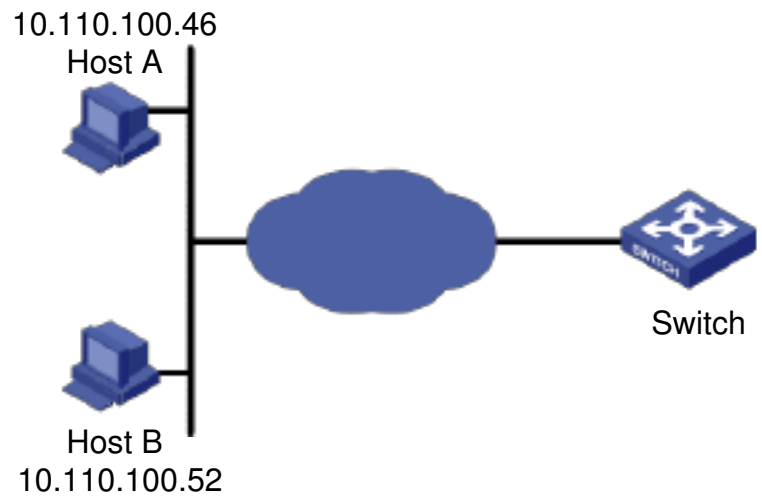
```
#
local-user admin
 password simple admin
 service-type telnet
  level 3
#
interface Vlan-interface1
 ip address 10.153.17.82 255.255.255.0
```

1.3.6 配置注意事项

缺省情况下，WEB　网管功能处于开启状态。

1.4 对登录用户的控制典型配置指导

1.4.1 组网图



对登录用户的控制典型配置示意图

1.4.2 应用要求

如上组网中，仅允许来自 10.110.100.52 和 10.110.100.46 的 Telnet/SNMP/WEB用户访问交换机。

1.4.3 配置过程和解释

创建并进入基本 ACL 视图 2000

```
[Sysname] acl number 2000 match-order config
[Sysname-acl-basic-2000]
```

定义子规则，仅允许来自 10.110.100.52 和 10.110.100.46 的 Telnet/SNMP/WEB用户访问交换机

```
[Sysname-acl-basic-2000] rule 1 permit source 10.110.100.52 0
[Sysname-acl-basic-2000] rule 2 permit source 10.110.100.46 0
[Sysname-acl-basic-2000] rule 3 deny source any
[Sysname-acl-basic-2000] quit
```

引用访问控制列表 2000，通过源 IP 对 Telnet用户进行控制

```
[Sysname] user-interface vty 0 4
[Sysname-ui-vty0-4] acl 2000 inbound
```

引用访问控制列表 2000，通过源 IP 对网管用户进行控制

```
[Sysname] snmp-agent community read aaa acl 2000
[Sysname] snmp-agent group v2c groupa acl 2000
[Sysname] snmp-agent usm-user v2c usera groupa acl 2000
```

引用访问控制列表2000，通过源IP对WEB用户进行控制

```
[Sysname] ip http acl 2000
```

1.4.4 完整配置

对Telnet用户进行控制

```
#
acl number 2000
 rule 1 permit source 10.110.100.52 0
 rule 2 permit source 10.110.100.46 0
 rule 3 deny
#
user-interface vty 0 4
 acl 2000 inbound
```

通过源IP对网管用户进行控制

```
#
acl number 2000
 rule 1 permit source 10.110.100.52 0
 rule 2 permit source 10.110.100.46 0
 rule 3 deny
#
 snmp-agent community read aaa acl 2000
 snmp-agent group v2c groupa acl 2000
 snmp-agent usm-user v2c usera groupa  acl 2000
```

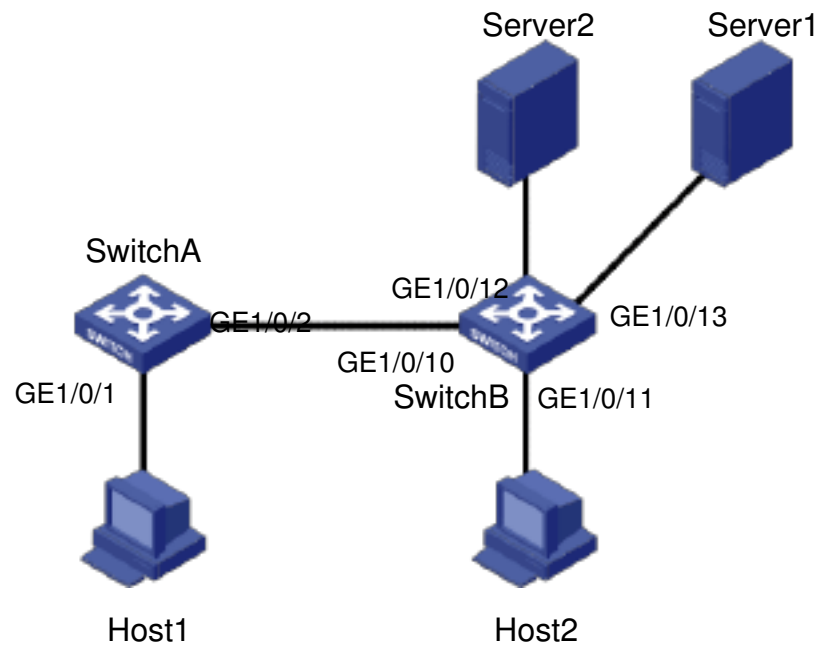
通过源IP对WEB用户进行控制

```
#
 ip http acl 2000
#
 acl number 2000
 rule 1 permit source 10.110.100.52 0
 rule 2 permit source 10.110.100.46 0
 rule 3 deny
```

2. VLAN 典型配置指导

2.1 基于端口的 VLAN 典型配置指导

2.1.1 组网图



基于端口的 VLAN 组网示意图

2.1.2 应用要求

如基于端口的 VLAN 组网示意图所示，Switch A 和 Switch B 分别连接了不同部门使用的 Host1/Host2 和 Server1/Server2。

为保证部门间数据的二层隔离，现要求将 Host1 和 Server1 划分到 VLAN100 中，Host2 和 Server2 划分到 VLAN200 中。并分别为两个 VLAN 设置描述字符为“Dept1”和“Dept2”。

在 SwitchA 上配置 VLAN 接口，对 Host1 发往 Server2 的数据进行三层转发。

2.1.3 配置过程和解释

配置 Switch A

创建 VLAN100，并配置 VLAN100 的描述字符串为“Dept1”，将端口 GigabitEthernet1/0/1 加入到 VLAN100。

```
<SwitchA> system-view
[SwitchA] vlan 100
[SwitchA-vlan100] description Dept1
[SwitchA-vlan100] port GigabitEthernet 1/0/1
[SwitchA-vlan100] quit
```

创建 VLAN200，并配置 VLAN200 的描述字符串为“Dept2”。

```
[SwitchA] vlan 200
[SwitchA-vlan200] description Dept2
[SwitchA-vlan200] quit
```

创建 VLAN100 和 VLAN200 的接口，IP 地址分别配置为 192.168.1.1 和 192.168.2.1，用来对 Host1

发往 Server2 的报文进行三层转发。

```
[SwitchA] interface Vlan-interface 100
[SwitchA-Vlan-interface100] ip address 192.168.1.1 24
[SwitchA-Vlan-interface100] quit
[SwitchA] interface Vlan-interface 200
[SwitchA-Vlan-interface200] ip address 192.168.2.1 24
```

配置 Switch B

创建 VLAN100，并配置 VLAN100 的描述字符串为“Dept1”，将端口 GigabitEthernet1/0/13 加入到 VLAN100。

```
<SwitchB> system-view
[SwitchB] vlan 100
[SwitchB-vlan100] description Dept1
[SwitchB-vlan100] port GigabitEthernet 1/0/13
[SwitchB-vlan100] quit
```

创建 VLAN200，并配置 VLAN200 的描述字符串为“Dept2”，将端口 GigabitEthernet1/0/11 和 GigabitEthernet1/0/12 加入到 VLAN200。

```
[SwitchB] vlan 200
[SwitchB-vlan200] description Dept2
[SwotchB-vlan200] port GigabitEthernet1/0/11 GigabitEthernet 1/0/12
[SwitchB-vlan200] quit
```

配置 Switch A 和 Switch B 之间的链路

由于 Switch A 和 Switch B 之间的链路需要同时传输 VLAN100 和 VLAN200 的数据，所以可以配置两端的端口为 Trunk 端口，且允许这两个 VLAN 的报文通过。

配置 Switch A 的 GigabitEthernet1/0/2 端口。

```
[SwitchA] interface GigabitEthernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-type trunk
[SwitchA-GigabitEthernet1/0/2] port trunk permit vlan 100 200
```

配置 Switch B 的 GigabitEthernet1/0/10 端口。

```
[SwitchB] interface GigabitEthernet 1/0/10
[SwitchB-GigabitEthernet1/0/10] port link-type trunk
[SwitchB-GigabitEthernet1/0/10] port trunk permit vlan 100 200
```

2.1.4 完整配置

SwitchA 上的配置

```
#
vlan 100
 description dept1
#
vlan 200
 description dept2
#
interface Vlan-interface 100
 ip address 192.168.1.1 255.255.255.0
#
interface Vlan-interface 200
 ip address 192.168.2.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 100 200
```

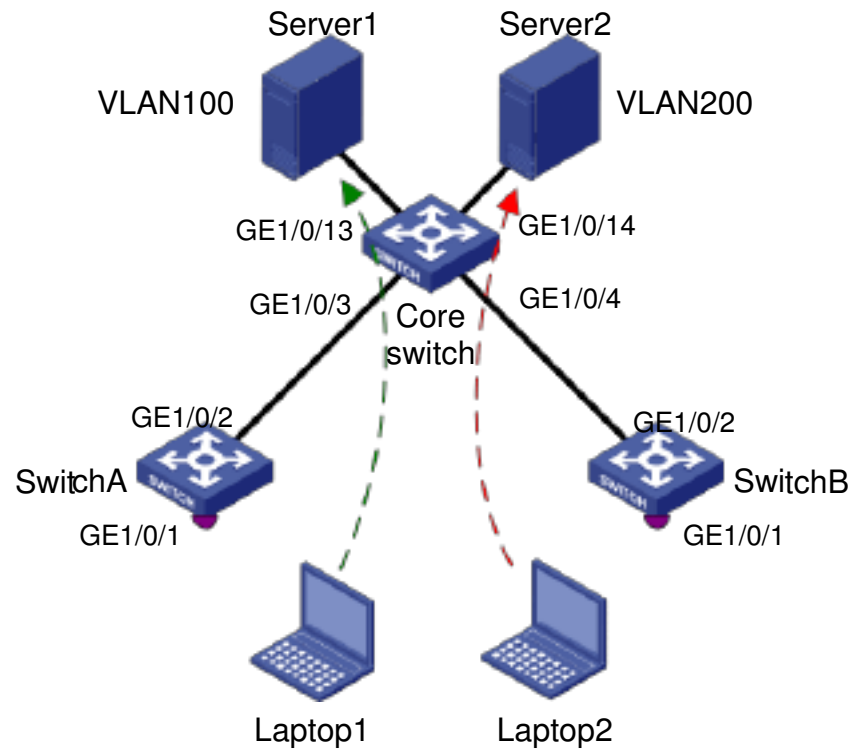
SwitchB 上的配置

```
#
vlan 100
 description dept1
#
vlan 200
```

```
 description dept2
#
 interface GigabitEthernet1/0/10
 port link-type trunk
  port trunk permit vlan 1 100 200
 #
 interface GigabitEthernet1/0/11
  port access vlan 100
 #
 interface GigabitEthernet1/0/12
  port access vlan 200
#
interface GigabitEthernet1/0/13
 port access vlan 100
```

2.2 基于 MAC 的 VLAN 典型配置指导

2.2.1 组网图



基于 MAC 的 VLAN 组网示意图

2.2.2 应用要求

如基于 MAC 的 VLAN 组网示意图所示，SwitchA 和 SwitchB 的 GigabitEthernet1/0/1 端口分别连接到两个会议室，Laptop1 和 Laptop2 是会议用笔记本电脑，会在两个会议室间移动使用。

Laptop1 和 Laptop2 分别属于两个部门，两个部门间使用 VLAN100 和 VLAN200 进行隔离。现要求这两台笔记本电脑无论在哪个会议室使用，均只能访问自己部的服务器，即 Server1 和 Server2。

Laptop1 和 Laptop2 的 MAC 地址分别为 000d-88f8-4e71、0014-222c-aa69。

2.2.3 配置过程和解释

SwitchA 的配置

创建 VLAN100 和 VLAN200，并将 GigabitEthernet1/0/2 配置为 Trunk 端口，允许 VLAN100 和 VLAN200 的报文通过。

```
<SwitchA> system-view
[SwitchA] vlan 100
[SwitchA-vlan100] quit
[SwitchA] vlan 200
[SwitchA-vlan200] quit
[SwitchA] interface GigabitEthernet1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-type trunk
[SwitchA-GigabitEthernet1/0/2] port trunk permit vlan 100 200
[SwitchA-GigabitEthernet1/0/2] quit
```

将 GigabitEthernet1/0/1 配置为 Hybrid 端口，并使其在发送 VLAN100 和 VLAN200 的报文时去掉 VLAN Tag。

```
[SwitchA] interface GigabitEthernet1/0/1
[SwitchA-GigabitEthernet1/0/1] port link-type hybrid
[SwitchA-GigabitEthernet1/0/1] port hybrid vlan 100 200 untagged
[SwitchA-GigabitEthernet1/0/1] quit
```

创建 Laptop1 的 MAC 地址与 VLAN100 的关联，创建 Laptop2 的 MAC 地址与 VLAN200 的关联，开启 GigabitEthernet1/0/1 端口的 MAC-VLAN 功能。

```
[SwitchA] mac-vlan mac-address 000d-88f8-4e71 vlan 100
[SwitchA] mac-vlan mac-address 0014-222c-aa69 vlan 200
[SwitchA] interface GigabitEthernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] mac-vlan enable
```

SwitchB 的配置

SwitchB 的配置与 SwitchA 完全一致，这里不再赘述。

Core Switch 的配置

创建 VLAN100 和 VLAN200，并将 GigabitEthernet1/0/13 和 GigabitVLANEthernet 1/0/14端口分别加入这两个 VLAN。

```
<CoreSwitch> system-view
[CoreSwitch] vlan 100
[CoreSwitch-vlan100] port gigabitethernet 1/0/13
[CoreSwitch-vlan100] quit
[CoreSwitch] vlan 200
[CoreSwitch-vlan200] port gigabitethernet 1/0/14
[CoreSwitch-vlan200] quit
```

配置 GigabitEthernet1/0/3 和 GigabitEthernet1/0/4 端口为 Trunk端口，均允许 VLAN100 和 VLAN200 的报文通过。

```
[CoreSwitch] interface GigabitEthernet1/0/3
[CoreSwitch-GigabitEthernet1/0/3] port link-type trunk
[CoreSwitch-GigabitEthernet1/0/3] port trunk permit vlan 100 200
[CoreSwitch-GigabitEthernet1/0/3] quit
[CoreSwitch] interface GigabitEthernet1/0/4
[CoreSwitch-GigabitEthernet1/0/4] port link-type trunk
[CoreSwitch-GigabitEthernet1/0/4] port trunk permit vlan 100 200
[CoreSwitch-GigabitEthernet1/0/4] quit
```

2.2.4 完整配置

SwitchA 的配置

```
#
 mac-vlan mac-address 000d-88f8-4e71 vlan 100 priority 0
 mac-vlan mac-address 0014-222c-aa69 vlan 200 priority 0
#
vlan 100
#
vlan 200
#
#
interface GigabitEthernet1/0/1
```

```
 port link-type hybrid
 port hybrid vlan 1 100 200 untagged
 mac-vlan enable
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 100 200
```

SwitchB 的配置与 SwitchA 完全一致，这里不再赘述。

Core Switch 的配置

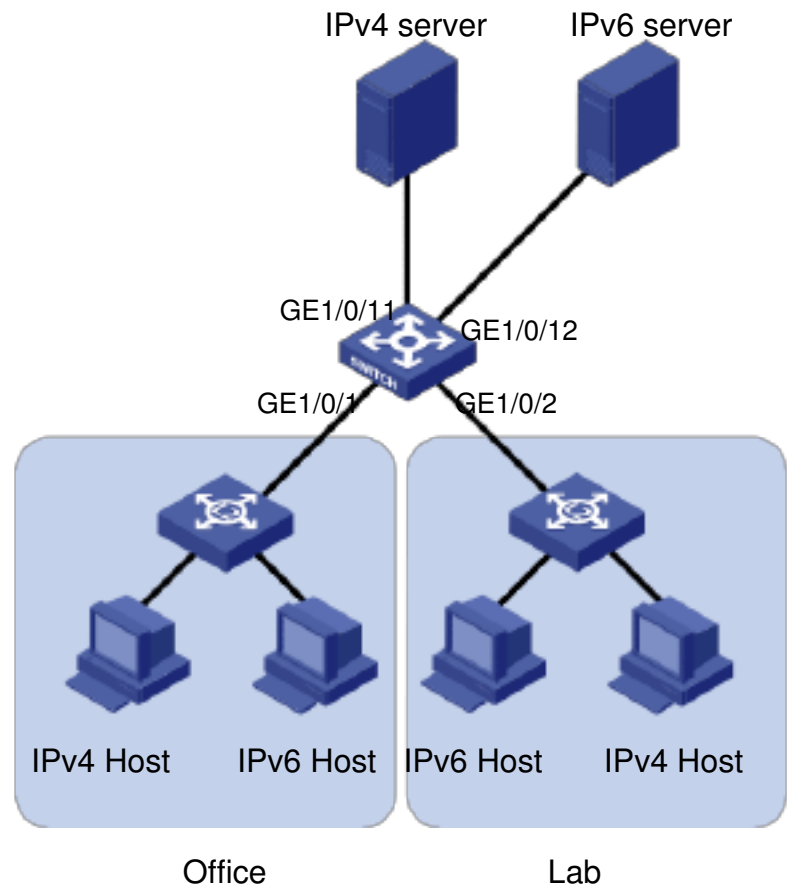
```
#
vlan 100
#
vlan 200
#
interface GigabitEthernet1/0/3
 port link-type trunk
 port trunk permit vlan 1 100 200
#
interface GigabitEthernet1/0/4
 port link-type trunk
 port trunk permit vlan 1 100 200
#
interface GigabitEthernet1/0/13
 port access vlan 100
#
interface GigabitEthernet1/0/14
 port access vlan 200
```

2.2.5 配置注意事项

基于 MAC 的 VLAN 只能在 Hybrid 端口上配置。

2.3 基于协议的 VLAN 典型配置指导

2.3.1 组网图



基于协议的 VLAN 组网示意图

2.3.2 应用要求

如基于协议的 VLAN 组网示意图所示，通过配置交换机的协议 VLAN 功能，使办公区和实验室中基于 IPv4 网络和基于 IPv6 网络的主机能分别与处在不同 VLAN 内的对应服务器进行通信，且两种网络协议的报文能够通过 VLAN 进行隔离，其中 IPv4 网络使用 VLAN100，IPv6 网络使用 VLAN200。

2.3.3 配置过程和解释

上行端口的配置

创建 VLAN100，将端口 GigabitEthernet1/0/11 加入 VLAN100

```
<Sysname> system-view
[Sysname] vlan 100
[Sysname-vlan100] port GigabitEthernet 1/0/11
```

创建 VLAN200，将端口 GigabitEthernet1/0/12 加入 VLAN200

```
[Sysname-vlan100] quit
[Sysname] vlan 200
[Sysname-vlan200] port GigabitEthernet 1/0/12
```

配置协议模板并与下行端口绑定

创建 VLAN200 和 VLAN100 的协议模板，分别匹配 IPv4 和 IPv6 协议。

```
[Sysname-vlan200] protocol-vlan ipv6
[Sysname-vlan200] quit
[Sysname-vlan100]
[Sysname-vlan100] protocol-vlan ipv4
[Sysname-vlan100] quit
```

配置端口 GigabitEthernet1/0/1 为 Hybrid 端口，并在转发 VLAN100 和 VLAN200 的报文时去掉 VLAN Tag。

```
 [Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type hybrid
[Sysname-GigabitEthernet1/0/1] port hybrid vlan 100 200 untagged
```

配置端口 GigabitEthernet1/0/1 分别与 VLAN100 的协议模板 0，VLAN200 的协议模板 0 进行绑定。

```
[Sysname-GigabitEthernet1/0/1] port hybrid protocol-vlan vlan 100 0
[Sysname-GigabitEthernet1/0/1] port hybrid protocol-vlan vlan 200 0
```

同理配置端口 GigabitEthernet1/0/2 为 Hybrid 端口，在转发 VLAN100 和 VLAN200 的报文时去掉 VLAN Tag，并与 VLAN100 和 VLAN200 的协议模板 0 进行绑定

```
[Sysname] interface GigabitEthernet 1/0/2
[Sysname-GigabitEthernet1/0/2] port link-type hybrid
[Sysname-GigabitEthernet1/0/2] port hybrid vlan 100 200 untagged
[Sysname-GigabitEthernet1/0/2] port hybrid protocol-vlan vlan 100 0
[Sysname-GigabitEthernet1/0/2] port hybrid protocol-vlan vlan 200 0
```

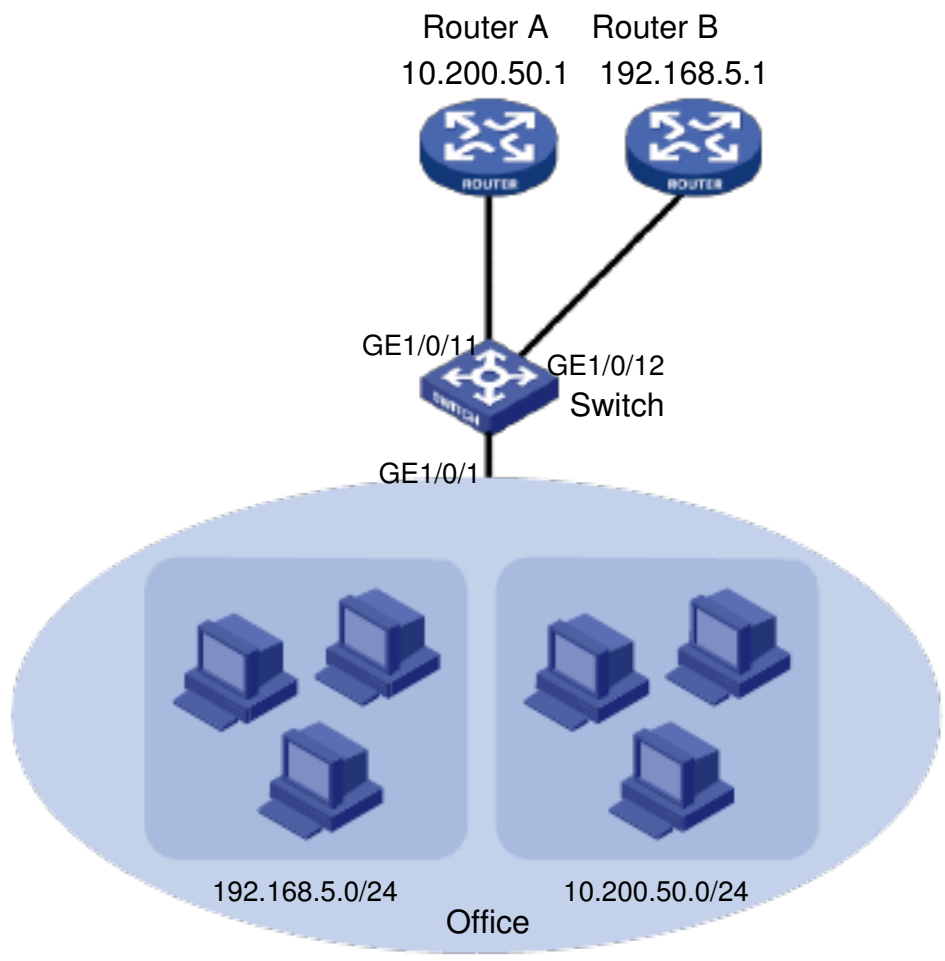
2.3.4 完整配置

```
#
vlan 100
 protocol-vlan 0 ipv4
#
vlan 200
 protocol-vlan 0 ipv6
#
interface GigabitEthernet1/0/1
 port link-type hybrid
 port hybrid vlan 1 100 200 untagged


 port hybrid protocol-vlan vlan 100 0
 port hybrid protocol-vlan vlan 200 0
#
```

```
interface GigabitEthernet1/0/2
 port link-type hybrid
 port hybrid vlan 1 100 200 untagged
 port hybrid protocol-vlan vlan 100 0
 port hybrid protocol-vlan vlan 200 0
#
interface Ethernet1/0/11
 port access vlan 100
#
interface Ethernet1/0/12
 port access vlan 200
```

2.4 基于 IP 子网的 VLAN 典型配置指导

2.4.1 组网图



基于 IP 子网的 VLAN 组网示意图

2.4.2 应用要求

如基于 IP 子网的 VLAN 组网示意图所示，办公区内的主机被配置到两个不同的网段（192.168.5.0/24 和 10.200.50.0/24）中，要求通过配置 IP 子网 VLAN 功能，使交换机能够将从 GigabitEthernet1/0/1 端口收到的报文根据源主机所属网段的不同，分别在不同的 VLAN 内传输，并到达指定的网关（RouterA 和 RouterB）。

其中 192.168.5.0/24 网段的报文分发到 VLAN100 中传输，10.200.50.0/24 网段的报文分发到 VLAN200 中传输。

2.4.3 配置过程和解释

上行端口的配置

创建 VLAN100，将端口 GigabitEthernet1/0/12 加入 VLAN100

```
[Sysname] vlan 100
[Sysname-vlan100] port GigabitEthernet 1/0/12
```

创建 VLAN200，将端口 GigabitEthernet1/0/11 加入 VLAN200

```
[Sysname-vlan100] quit
[Sysname] vlan 200
[Sysname-vlan200] port GigabitEthernet 1/0/11
```

配置 IP 子网 VLAN 并与下行端口绑定

将 10.200.50.0/24 网段与 VLAN200 进行关联，将 192.168.5.0/24 网段与 VLAN100 进行关联

```
[Sysname-vlan200] ip-subnet-vlan ip 10.200.50.0 255.255.255.0
[Sysname-vlan200] quit
[Sysname] vlan100
[Sysname-vlan100] ip-subnet-vlan ip 192.168.5.0 255.255.255.0
```

配置端口GigabitEthernet1/0/1 为Hybrid 端口，并在转发VLAN100 和VLAN200 的报文时去掉VLAN Tag。

```
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port link-type hybrid
[Sysname-GigabitEthernet1/0/1] port hybrid vlan 100 200 untagged
```

配置端口 GigabitEthernet1/0/1 分别与 VLAN100 和 VLAN200 的子网进行关联。

```
[Sysname-GigabitEthernet1/0/1] port hybrid ip-subnet-vlan vlan 100
[Sysname-GigabitEthernet1/0/1] port hybrid ip-subnet-vlan vlan 200
```

2.4.5 完整配置

```
#
vlan 100
 ip-subnet-vlan 0 ip 192.168.5.0 255.255.255.0
#
vlan 200
 ip-subnet-vlan 0 ip 10.200.50.0 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type hybrid
  port hybrid vlan 1 100 200 untagged
  port hybrid ip-subnet-vlan vlan 100
  port hybrid ip-subnet-vlan vlan 200
  #
  interface Ethernet1/0/11
   port access vlan 200
#
interface Ethernet1/0/12
 port access vlan 100
```

2.5 Isolate-user-vlan 典型配置指导

2.5.1 组网图

Isolate-user-vlan 组网示意图

2.5.2 应用要求

DeviceB 和 DeviceC 在初始状态下分别位于两个独立的网络中，并根据自身情况创建了相应的 VLAN；由于网络规划的变更，现要求使用 DeviceA 将 DeviceB 和 DeviceC 连通。

出于安全性的考虑，要求 DeviceB 和 DeviceC 所连接的设备间不能直接通信，如 Isolate-user-vlan 组网示意图所示，由于这两台设备本地创建的 VLAN 编号有重复，HostA 和 HostC 处在同一个 VLAN 中，存在一定安全隐患。因此需要使用 Isolate-user-vlan 功能，使 DeviceB 和 DeviceC 上配置的 VLAN2/VLAN3 和 VLAN3/VLAN4 仅在本地有效，DeviceA 使用 VLAN5 和 VLAN6 对这两个网络进行划分，而无需考虑这两个网络内部 VLAN 的配置。

DeviceA 使用 VLAN 接口对两个网络间的报文进行三层转发。

2.5.3 配置过程和解释

配置 DeviceB

配置 Isolate-user-vlan。

```
<DeviceB> system-view
[DeviceB] vlan 5
[DeviceB-vlan5] isolate-user-vlan enable
[DeviceB-vlan5] port GigabitEthernet 2/0/5
[DeviceB-vlan5] quit
```

配置 Secondary VLAN。

```
[DeviceB] vlan 3
[DeviceB-vlan3] port GigabitEthernet 2/0/1
[DeviceB-vlan3] quit
[DeviceB] vlan 2
[DeviceB-vlan2] port GigabitEthernet 2/0/2
```

```
[DeviceB-vlan2] quit
```

配置 Isolate-user-vlan 和 Secondary VLAN 间的映射关系。

```
[DeviceB] isolate-user-vlan 5 secondary 2 to 3
```

配置 DeviceC

配置 Isolate-user-vlan。

```
<DeviceC> system-view
[DeviceC] vlan 6
[DeviceC-vlan6] isolate-user-vlan enable
[DeviceC-vlan6] port GigabitEthernet 2/0/5
[DeviceC-vlan6] quit
```

配置 Secondary VLAN。

```
[DeviceC] vlan 3
[DeviceC-vlan3] port GigabitEthernet 2/0/3
[DeviceC-vlan3] quit
[DeviceC] vlan 4
[DeviceC-vlan4] port GigabitEthernet 2/0/4
```

配置 Isolate-user-vlan 和 Secondary VLAN 间的映射关系。

```
[DeviceC-vlan4] quit
[DeviceC] isolate-user-vlan 6 secondary 3 to 4
```

配置 DeviceA

创建 VLAN5 和 VLAN6，并将 GigabitEthernet2/0/1 和 GigabitEthernet2/0/2 端口分别加入 VLAN5 和 VLAN6，本例中以这两个端口为 Access 端口为例进行配置。

```
[DeviceA] vlan 5
[DeviceA-vlan5] port GigabitEthernet 2/0/1
[DeviceA-vlan5] quit
[DeviceA] vlan 6
[DeviceA-vlan6] port GigabitEthernet 2/0/2
[DeviceA-vlan6] quit
```

创建 VLAN5 和 VLAN6 的接口，使两个网络间的数据可以通过 Device A 进行三层转发，IP 地址分别为 192.168.0.1 和 192.168.1.1。

```
[DeviceA] interface Vlan-interface 5
[DeviceA-Vlan-interface5] ip address 192.168.0.1 24
[DeviceA-Vlan-interface5] quit
[DeviceA] interface Vlan-interface 6
[DeviceA-Vlan-interface6] ip address 192.168.1.1 24
```

用户也可以将 GigabitEthernet2/0/1 和 GigabitEthernet2/0/2 端口配置为 Trunk 端口或 Hybrid 端口，只需要保证这两个端口分别在发送 VLAN5 和 VLAN6 的报文时去掉 VLAN Tag 即可。

2.5.6 完整配置

DeviceB 的完整配置

```
#
 vlan 2 to 3
#
 vlan 5
  isolate-user-vlan enable
#
interface GigabitEthernet2/0/1
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 3 5 untagged
  port hybrid pvid vlan 3
#
interface GigabitEthernet2/0/2
port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 2 5 untagged

  port hybrid pvid vlan 2
 #
 interface GigabitEthernet2/0/5
```

```
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 2 3 5 untagged
 port hybrid pvid vlan 5
#
isolate-user-vlan 5 secondary 2 3
```

DeviceC的完整配置

```
#
vlan 3 to 4
#
vlan 6
 isolate-user-vlan enable
#
interface GigabitEthernet2/0/3
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 3 6 untagged
 port hybrid pvid vlan 3
#
interface GigabitEthernet2/0/4
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 4 6 untagged
 port hybrid pvid vlan 4
#
interface GigabitEthernet2/0/5
port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 3 4 6 untagged
 port hybrid pvid vlan 6
#
isolate-user-vlan 50 secondary 2 3
```

DeviceA的完整配置

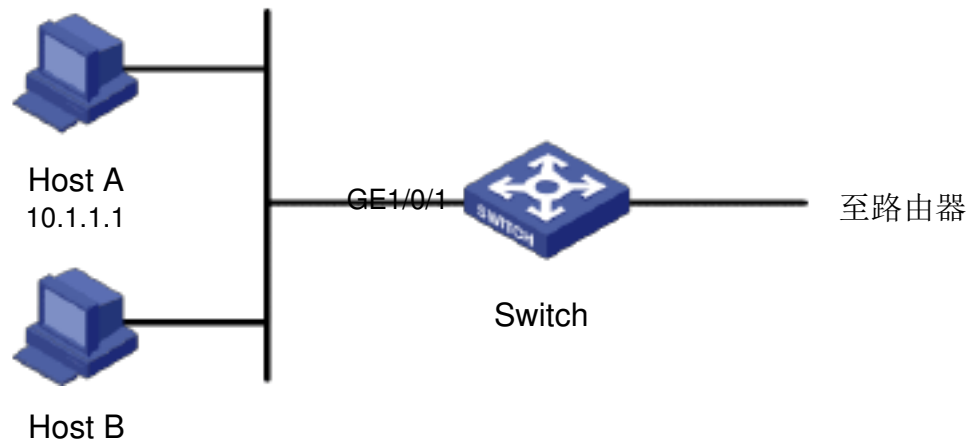
```
#
vlan 5 to 6
#
interface Vlan-interface 5
 ip address 192.168.0.1 255.255.255.0
#
interface Vlan-interface 6
 ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet2/0/1
 port access vlan 5
#
interface GigabitEthernet2/0/2
 port access vlan 6
```

3. IPv4 ACL 典型配置指导

3.1 基本 IPv4 ACL 典型配置指导

基本 IPv4 ACL 只根据源 IP 地址信息制定匹配规则，对报文进行相应的分析处理。 基本 IPv4 ACL 的序号取值范围为 2000～2999。

3.1.1 组网图



配置基本 IPv4 ACL 组网图

3.1.2 应用要求

Host A 和 Host B 通过端口 GigabitEthernet 1/0/1 接入交换机（以 S5500-EI 为例），Host A 的 IP 地址为 10.1.1.1。要求配置基本 IPv4 ACL，实现在每天 8:00～18:00 的时间段内，只允许 Host A 发出的 IP 报文通过，拒绝其它的 IP 报文通过。

3.1.3 配置过程和解释

定义周期时间段 trname，时间范围为每天的 8:00～18:00。

```
<Switch> system-view
[Switch] time-range trname 8:00 to 18:00 daily
```

定义基本 IPv4 ACL 2000，配置源 IP 地址为 10.1.1.1 的访问规则。

```
[Switch] acl number 2000
[Switch-acl-basic-2000] rule permit source 10.1.1.1 0 time-range trname
[Switch-acl-basic-2000] quit
```

定义基本 IPv4 ACL 2001，配置源 IP 地址为任意地址的访问规则。

```
[Switch] acl number 2001
[Switch-acl-basic-2001] rule deny time-range trname
[Switch-acl-basic-2001] quit
```

定义类 classifier_hostA，对匹配基本 IPv4 ACL 2000 的报文进行分类。

```
[Switch] traffic classifier classifier_hostA
[Switch-classifier-classifier_hostA] if-match acl 2000
[Switch-classifier-classifier_hostA] quit
```

定义流行为 behavior_hostA，动作为允许报文通过。

```
[Switch] traffic behavior behavior_hostA
[Switch-behavior-behavior_hostA] filter permit
[Switch-behavior-behavior_hostA] quit
```

定义类 classifier_hostB，对匹配基本 IPv4 ACL 2001 的报文进行分类。

```
[Switch] traffic classifier classifier_hostB
[Switch-classifier-classifier_hostB] if-match acl 2001
[Switch-classifier-classifier_hostB] quit
```

定义流行为 behavior_hostB，动作为拒绝报文通过。

```
[Switch] traffic behavior behavior_hostB
[Switch-behavior-behavior_hostB] filter deny
[Switch-behavior-behavior_hostB] quit
```

定义策略 policy_host，为类 classifier_hostA 指定流行为 behavior_hostA，为类 classifier_hostB 指定流行为 behavior_hostB 。其中 **filter permit** 和 **filter deny** 动作必须配置到不同的 **classifier-behavior** 中，并且在配置过程中需要注意两者的先后顺序，以保证应用策略后实际的运行结果与用户的配置意图一致。

```
[Switch] qos policy policy_host
[Switch-qospolicy-policy_host]    classifier    classifier_hostA    behavior
behavior_hostA
[Switch-qospolicy-policy_host]    classifier    classifier_hostB    behavior
behavior_hostB
[Switch-qospolicy-policy_host] quit
```

将策略 policy_host 应用到端口 GigabitEthernet 1/0/1

```
[Switch] interface GigabitEthernet 1/0/1
[Switch-GigabitEthernet1/0/1] qos apply policy policy_host inbound
```

3.1.4 完整配置

```
#
traffic classifier classifier_hostB operator and
 if-match acl 2001
traffic classifier classifier_hostA operator and
 if-match acl 2000
#
traffic behavior behavior_hostB
 filter deny
traffic behavior behavior_hostA
 filter permit
#
qos policy policy_host
 classifier classifier_hostA behavior behavior_hostA
 classifier classifier_hostB behavior behavior_hostB
#
time-range trname 08:00 to 18:00 daily
#
acl number 2000
rule 0 permit source 10.1.1.1 0 time-range trname
acl number 2001
 rule 0 deny time-range trname
#
interface GigabitEthernet1/0/1
 qos apply policy policy_host inbound
#
```

3.1.5 配置注意事项

需要注意的是：

- 当基本 IPv4 ACL 的匹配顺序为 **config** 时，用户可以修改该 ACL 中的任何一条已经存在的规则，在修改 ACL 中的某条规则时，该规则中没有修改到的部分仍旧保持原来的状态；当 ACL 的匹配顺序为 **auto** 时，用户不能修改该 ACL 中的任何一条已经存在的规则，否则系统会提示错误信息。
- 新创建或修改后的规则不能和已经存在的规则相同，否则会导致创建或修改不成功，系统会提示该规则已经存在。

当基本 IPv4 ACL的匹配顺序为 **auto** 时，新创建的规则将按照“深度优先”的原则插入到已有的规则中，但是所有规则对应的编号不会改变。

当基本 IPv4 ACL 被 QoS 策略引用对报文进行流分类时，ACL 规则中定义的动作（**deny** 或 **permit**）不起作用，交换机对匹配此 ACL 的报文采取的动作由 QoS 策略中流行为定义的动作决定。

当基本 IPv4 ACL被 QoS 策略引用对报文进行流分类时，各产品的限制情况如下表所示。

各产品的限制情况

产品	说明
S3610 系列以太网交换机	不支持配置 **logging** 参数
S5510 系列以太网交换机	不支持配置 **logging** 参数
S5500-SI 系列以太网交换机	不支持配置 **logging** 参数
S5500-EI 系列以太网交换机	不支持配置 **logging** 参数
S7500E 系列以太网交换机	不支持配置 **logging** 和 **vpn-instance** 参数

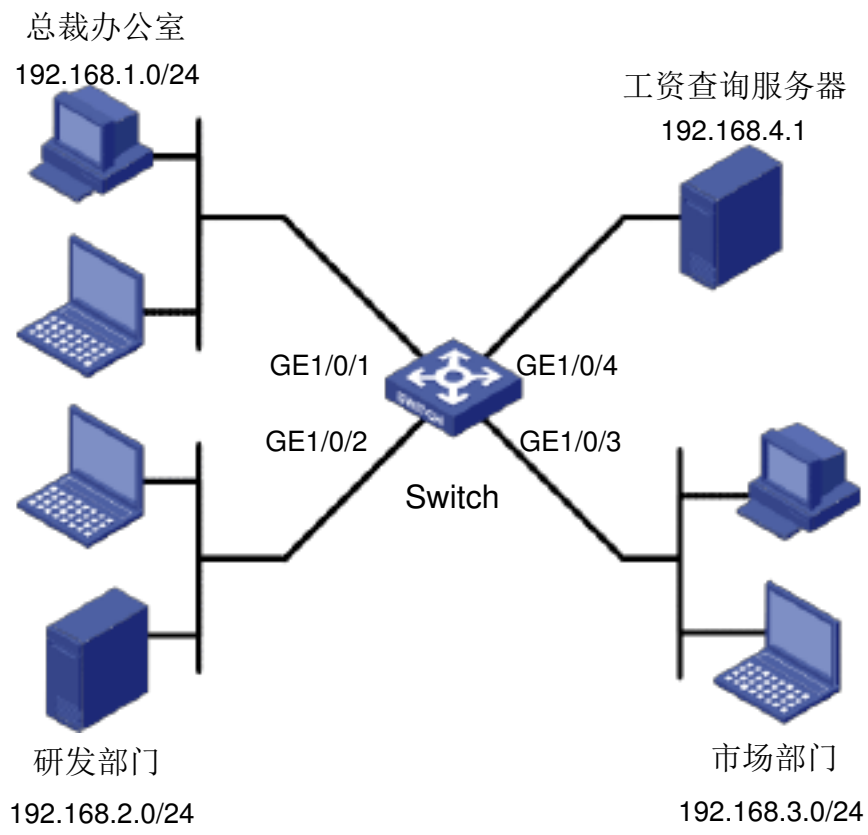
3.2 高级 IPv4 ACL 典型配置指导

高级 IPv4 ACL 可以使用报文的源 IP 地址信息、目的 IP 地址信息、IP 承载的协议类型、协议的特性（例如 TCP 或 UDP 的源端口、目的端口，ICMP 协议的消息类型、消息码等）等信息来制定匹配规则。

高级 IPv4 ACL支持对三种报文优先级的分析处理： ToS（Type of Service 服务类型）优先级 IP 优先级

DSCP（DifferentiatedServicesCodePoint，差分服务编码点）优先级 用户可以利用高级 IPv4 ACL定义比基本 IPv4 ACL更准确、更丰富、更灵活的匹配规则。 高级 IPv4 ACL 的序号取值范围为 3000～3999。

3.2.1 组网图



配置高级 IPv4 ACL 组网图

3.2.2 应用要求

公司企业网通过交换机（以S5500-EI 为例）实现各部门之间的互连。要求配置高级IPv4 ACL，禁止研发部门和市场部门在上班时间（8:00 至 18:00）访问工资查询服务器（IP 地址为 192.168.4.1），而总裁办公室不受限制，可以随时访问。

3.2.3 配置过程和解释

定义工作时间段

定义 8:00 至 18:00 的周期时间段。

```
<Switch> system-view
[Switch] time-range trname 8:00 to 18:00 working-day
```

定义到工资查询服务器的访问规则

定义研发部门到工资查询服务器的访问规则。

```
[Switch] acl number 3000
[Switch-acl-adv-3000] rule deny ip source 192.168.2.0 0.0.0.255 destination
192.168.4.1 0 time-range trname
[Switch-acl-adv-3000] quit
```

定义市场部门到工资查询服务器的访问规则。

```
[Switch] acl number 3001
[Switch-acl-adv-3001] rule deny ip source 192.168.3.0 0.0.0.255 destination
192.168.4.1 0 time-range trname
[Switch-acl-adv-3001] quit
```

应用访问规则

定义类 classifier_rd，对匹配高级 IPv4 ACL 3000 的报文进行分类。

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

定义流行为 behavior_rd，动作为拒绝报文通过。

```
[Switch] traffic behavior behavior_rd
```

```
[Switch-behavior-behavior_rd] filter deny
[Switch-behavior-behavior_rd] quit
```

定义类 classifier_market，对匹配高级 IPv4 ACL 3001 的报文进行分类。

```
[Switch] traffic classifier classifier_market
[Switch-classifier-classifier_market] if-match acl 3001
[Switch-classifier-classifier_market] quit
```

定义流行为 behavior_market，动作为拒绝报文通过。

```
[Switch] traffic behavior behavior_market
[Switch-behavior-behavior_market] filter deny
[Switch-behavior-behavior_market] quit
```

定义策略 policy_rd，为类 classifier_rd 指定流行为 behavior_rd。

```
[Switch] qos policy policy_rd
[Switch-qospolicy-policy_rd] classifier classifier_rd behavior behavior_rd
[Switch-qospolicy-policy_rd] quit
```

定义策略 policy_market，为类 classifier_market 指定流行为 behavior_market。

```
[Switch] qos policy policy_market
[Switch-qospolicy-policy_market] classifier classifier_market behavior
behavior_market
[Switch-qospolicy-policy_market] quit
```

将策略 policy_rd 应用到端口 GigabitEthernet 1/0/2

```
[Switch] interface GigabitEthernet 1/0/2
[Switch-GigabitEthernet1/0/2] qos apply policy policy_rd inbound
[Switch-GigabitEthernet1/0/2] quit
```

将策略 policy_market 应用到端口 GigabitEthernet 1/0/3

```
[Switch] interface GigabitEthernet 1/0/3
[Switch-GigabitEthernet1/0/3] qos apply policy policy_market inbound
```

3.2.4 完整配置

```
#
traffic classifier classifier_market operator and
 if-match acl 3001
traffic classifier classifier_rd operator and
 if-match acl 3000
#
traffic behavior behavior_market
 filter deny
traffic behavior behavior_rd
 filter deny
#
qos policy policy_market
 classifier classifier_market behavior behavior_market
qos policy policy_rd
 classifier classifier_rd behavior behavior_rd
#
 time-range trname 08:00 to 18:00 working-day
#
 acl number 3000
rule 0 deny ip source 192.168.2.0 0.0.0.255 destination 192.168.4.1 0
time-range trname
acl number 3001
rule 0 deny ip source 192.168.3.0 0.0.0.255 destination 192.168.4.1 0
time-range trname
#
interface GigabitEthernet1/0/2
 qos apply policy policy_rd inbound
#
interface GigabitEthernet1/0/3
 qos apply policy policy_market inbound
#
```

3.2.5 配置注意事项

需要注意的是：

当 ACL 的匹配顺序为 **config** 时，用户可以修改该 ACL 中的任何一条已经存在的规则，在修改 ACL 中的某条规则时，该规则中没有修改到的部分仍旧保持原来的状态；当 ACL 的匹配顺序为 **auto** 时，用户不能修改该 ACL 中的任何一条已经存在的规则，否则系统会提示错误信息。

新创建或修改后的规则不能和已经存在的规则相同，否则会导致创建或修改不成功，系统会提示该规则已经存在。

当 ACL 的匹配顺序为 **auto** 时，新创建的规则将按照“深度优先”的原则插入到已有的规则中，但是所有规则对应的编号不会改变。

当高级 IPv4 ACL 被 QoS 策略引用对报文进行流分类时，ACL 规则中定义的动作（**deny** 或 **permit**）不起作用，交换机对匹配此 ACL 的报文采取的动作由 QoS 策略中流行为定义的动作决定。

当高级 IPv4 ACL 被 QoS 策略引用对报文进行流分类时，各产品的限制情况如下表所示。

各产品的限制情况

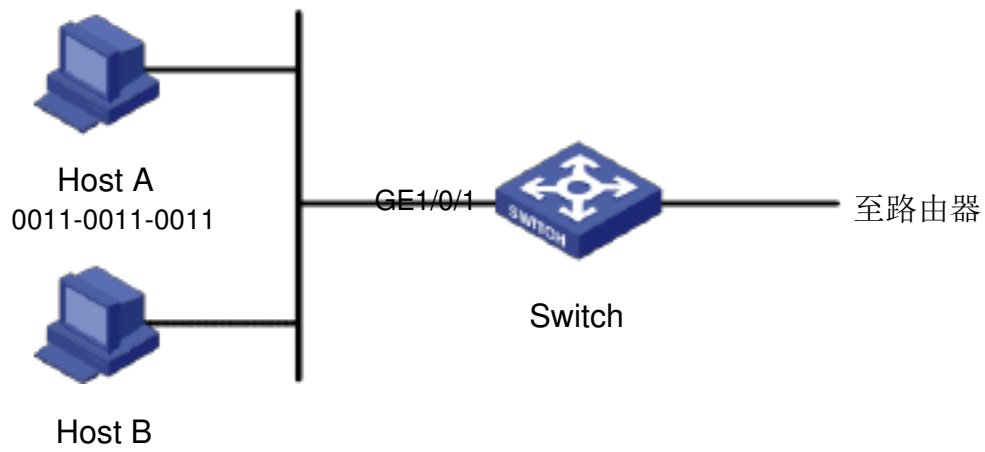
产品	说明
S3610 系列以太网交换机	不支持配置 **logging**、**reflective** 和 **established** 参数
S5510 系列以太网交换机	不支持配置 **logging**、**reflective** 和 **established** 参数
S5500-SI 系列以太网交换机	不支持配置 **logging**、**reflective** 和 **established** 参数 不支持配置操作符 *operator* 取值为 **neq**
S5500-EI 系列以太网交换机	当 QoS 策略应用于入方向（**inbound**）时，不支持配置 **logging** 和 **reflective** 参数；不支持配置操作符 *operator* 取值为 **neq** 当 QoS 策略应用于出方向（**outbound**）时，不支持配置 **logging** 和 **reflective** 参数；不支持配置操作符 *operator* 取值为 **gt**、**lt**、**neq** 和 **range**
S7500E 系列以太网交换机	当 QoS 策略应用于入方向（**inbound**）时，不支持配置 **logging**、**reflective** 和 **vpn-instance** 参数；不支持配置操作符 *operator* 取值为 **neq** 当 QoS 策略应用于出方向（**outbound**）时，不支持配置 **logging**、**reflective** 和 **vpn-instance** 参数；不支持配置操作符 *operator* 取值为 **gt**、**lt**、**neq** 和 **range**

3.3 二层 ACL 典型配置指导

二层 ACL 根据报文的源 MAC 地址、目的 MAC 地址、802.1p 优先级、二层协议类型等二层信息制定匹配规则，对报文进行相应的分析处理。

二层 ACL 的序号取值范围为 4000～4999。

3.3.1 组网图



配置二层 ACL 组网图

3.3.2 应用要求

Host A 和 Host B 通过端口 GigabitEthernet 1/0/1 接入交换机（以 S5500-EI 为例），Host A 的 MAC 地址为 0011-0011-0011。要求配置二层 ACL，实现在每天 8:00～18:00 的时间段内，对 Host A 发出的目的 MAC 为 0011-0011-0012 的报文进行过滤。

3.3.3 配置过程和解释

定义周期时间段 trname，时间范围为每天的 8:00～18:00。

```
<Switch> system-view
[Switch] time-range trname 8:00 to 18:00 daily
```

定义二层 ACL 4000，配置源 MAC 地址为 0011-0011-0011，目的 MAC 地址为 0011-0011-012 的报文的访问规则。

```
[Switch] acl number 4000
[Switch-acl-basic-4000] rule deny source-mac 0011-0011-0011 ffff-ffff-ffff
dest-mac 0011-0011-0012 ffff-ffff-ffff time-range trname
[Switch-acl-basic-4000] quit
```

定义类 classifier_hostA，对匹配二层 ACL 4000 的报文进行分类。

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

定义流行为 behavior_hostA，动作为拒绝报文通过。

```
[Switch] traffic behavior behavior_hostA
[Switch-behavior-behavior_hostA] filter deny
[Switch-behavior-behavior_hostA] quit
```

定义策略 policy_hostA，为类 classifier_hostA 指定流行为 behavior_hostA。

```
[Switch] qos policy policy_hostA
[Switch-qospolicy-policy_hostA]   classifier   classifier_hostA   behavior
behavior_hostA
[Switch-qospolicy-policy_hostA] quit
```

将策略 policy_hostA 应用到端口 GigabitEthernet 1/0/1

```
[Switch] interface GigabitEthernet 1/0/1
[Switch-GigabitEthernet1/0/1] qos apply policy policy_hostA inbound
```

3.3.4 完整配置

```
#
traffic classifier classifier_hostA operator and
 if-match acl 4000
#
```

```
traffic behavior behavior_hostA
 filter deny
#
qos policy policy_hostA
 classifier classifier_hostA behavior behavior_hostA
#
time-range trname 08:00 to 18:00 daily
#
acl number 4000
rule 0 deny source-mac 0011-0011-0011 ffff-ffff-ffff dest-mac 0011-0011-0012
ffff-ffff-ffff time-range trname
#
interface GigabitEthernet1/0/1
 qos apply policy policy_hostA inbound
#
```

3.3.5 配置注意事项

需要注意的是：

当 ACL 的匹配顺序为 **config** 时，用户可以修改该 ACL 中的任何一条已经存在的规则，在修改 ACL 中的某条规则时，该规则中没有修改到的部分仍旧保持原来的状态；当 ACL 的匹配顺序为 **auto** 时，用户不能修改该 ACL 中的任何一条已经存在的规则，否则系统会提示错误信息。

新创建或修改后的规则不能和已经存在的规则相同，否则会导致创建或修改不成功，系统会提示该规则已经存在。

当 ACL 的匹配顺序为 **auto** 时，新创建的规则将按照“深度优先”的原则插入到已有的规则中，但是所有规则对应的编号不会改变。

当二层 ACL 被 QoS 策略引用对报文进行流分类时，ACL 规则中定义的动作（**deny** 或 **permit**）不起作用，交换机对匹配此 ACL 的报文采取的动作由 QoS 策略中流行为定义的动作决定。

当二层 ACL 被 QoS 策略引用对报文进行流分类时，各产品的限制情况如下表所示。

各产品的限制情况

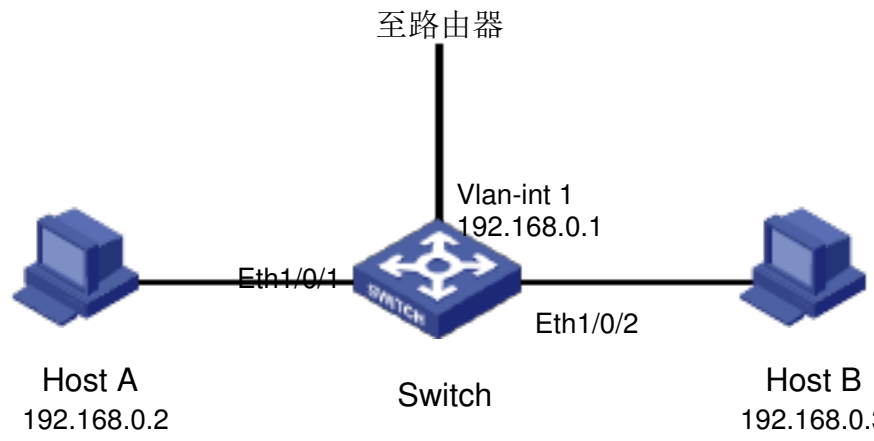
产品	说明
S3610 系列以太网交换机	不支持配置 **lsap** 参数
S5510 系列以太网交换机	不支持配置 **lsap** 参数
S5500-SI 系列以太网交换机	不支持配置 **lsap** 参数
S5500-EI 系列以太网交换机	不支持配置 **lsap** 参数
S7500E 系列以太网交换机	不支持配置 **lsap** 参数

3.4 用户自定义 ACL 和流模板典型配置指导

用户自定义 ACL 可以以报文的二层报文头、IP 报文头等为基准，指定从第几个字节开始与掩码进行“与”操作，将从报文提取出来的字符串和用户定义的字符串进行比较，找到匹配的报文，后然进行相应的处理。

用户自定义ACL的序号取值范围为5000～5999。
流模板的主要功能是对硬件下发的 ACL 规则中所能包含的信息进行限制。在以太网端口下发的 ACL 规则中包含的信息必须是该端口下发流模板中定义信息的子集。比如，流模板定义了源 IP 地址、目的 IP 地址、源 TCP 端口、目的 TCP 端口等限制，只有在上述范围内的ACL 规则可以正确下发到硬件中，用于 QoS 等功能；否则 ACL 规则将不能下发到硬件中，导致 QoS 功能不能引用此 ACL 规则。

3.4.1 组网图



配置用户自定义 ACL 和流模板组网图

3.4.2 应用要求

公司企业网通过交换机（以S3610为例）实现互连，网络环境描述如下：

Host A的 IP 地址为 192.168.0.2，通过端口 Ethernet 1/0/1 接入交换机；Host B 的 IP 地址为 192.168.0.3，通过端口 Ethernet 1/0/2接入交换机。

Host A和 Host B 属于 VLAN 1，二者的网关都设置为 192.168.0.1（交换机 VLAN 1 接口的 IP 地址），通过交换机访问 Internet。

要求配置用户自定义ACL，对 Host A 发出的仿冒网关 IP 地址的 ARP 报文进行过滤。

3.4.3 配置过程和解释

定义用户自定义 ACL 5000，配置源 IP 地址为 192.168.0.1 的 ARP 报文的访问规则。其中L2 表示从报文的二层头开始计算，0806 为 ARP 协议号，ffff 为掩码，12 为以太网报文中协议类型字段的偏移量，start 表示从报文的报文头开始计算，c0a80001 为192.168.0.1 的十六进制形式，28 为 ARP 报文中源 IP 地址字段的偏移量。

```
<Switch> system-view
[Switch] acl number 5000
[Switch-acl-user-5000] rule deny L2 0806 ffff 12 start c0a80001 ffffffff 28
```

定义扩展型流模板 ftemplate_hostA。

```
[Switch] flow-template ftemplate_hostA extend L2 12 2 start 28 4
```

在端口 Ethernet 1/0/1上应用流模板 ftemplate_hostA。

```
[Switch] interface Ethernet 1/0/1
[Switch-Ethernet1/0/1] flow-template ftemplate_hostA
[Switch-Ethernet1/0/1] quit
```

定义类 classifier_hostA，对匹配用户自定义 ACL 5000 的报文进行分类。

```
[Switch] traffic classifier classifier_hostA
[Switch-classifier-classifier_hostA] if-match acl 5000
[Switch-classifier-classifier_hostA] quit
```

定义流行为 behavior_hostA，动作为拒绝报文通过。

```
[Switch] traffic behavior behavior_hostA
[Switch-behavior-behavior_hostA] filter deny
[Switch-behavior-behavior_hostA] quit
```

定义策略 policy_hostA，为类 classifier_hostA 指定流行为 behavior_hostA。

```
[Switch] qos policy policy_hostA
[Switch-qospolicy-policy_hostA]   classifier   classifier_hostA   behavior
behavior_hostA
[Switch-qospolicy-policy_hostA] quit
```

将策略 policy_hostA 应用到端口 Ethernet 1/0/1。

```
[Switch] interface Ethernet 1/0/1
[Switch-Ethernet1/0/1] qos apply policy policy_hostA inbound
```

3.4.4 完整配置

```
#
 flow-template ftemplate_hostA extend start 28 4 l2 12 2
#
 traffic classifier classifier_hostA operator and
  if-match acl 5000
 #
 traffic behavior behavior_hostA
  filter deny
 #
 qos policy policy_hostA
  classifier classifier_hostA behavior behavior_hostA
 #
 acl number 5000
  rule 0 deny start c0a80001 ffffffff 28 l2 0806 ffff 12
#
interface Ethernet1/0/1
 flow-template ftemplate_hostA
  qos apply policy policy_hostA inbound
 #
```

3.4.5 配置注意事项

在配置用户自定义 ACL 时需要注意：

和其他类型的 IPv4 ACL 不同，用户自定义 ACL 中包含的规则不支持修改，只能进行覆盖性配置。

新创建的规则不能和已经存在的规则相同，否则会导致创建不成功用户自定义 ACL 的匹配顺序为配置顺序。

用户自定义 ACL 需要和扩展型用户自定义流模板配合使用，用户自定义 ACL 中设置的偏移范围必须包含在扩展型用户自定义流模板中设置的偏移范围之内，则用户自定义 ACL 不能成功应用。

当用户自定义 ACL 被 QoS 策略引用对报文进行流分类时，ACL 规则中定义的动作（**deny** 或 **permit**）不起作用，交换机对匹配此 ACL 的报文采取的动作由 QoS 策略中流行为定义的动作决定。在配置流模板时需要注意：

S3610&S5510 系列以太网交换机支持的流模板包括缺省流模板和用户自定义流模板。其中，用户自定义流模板又可分为标准型和扩展型。

标准型用户自定义流模板包含了若干元素，与报文的各个字段相对应；扩展型用户自定义流模板必须和用户自定义 ACL 配合使用，用户可以使用扩展型用户自定义流模板和用户自定义ACL对报文的指定字段进行匹配。

流模板只对基于硬件处理的ACL有效，对基于软件处理的 ACL不生效。 在端口上应用用户自定义流模板之前，必须先配置一个用户自定义流模板；一个端口上只能应用一个流模板。

在端口上应用流模板时，请关闭如下功能：802.1x 功能、集群功能（NDP、NTDP、HABP、Cluster）、DHCP Snooping、端口隔离、 MAC+IP+端口绑定、灵活QinQ、Voice VLAN，否则流模板将不能成功应用。同时建议用户不要在端口上应用流模版后开启这些功能。

当用户在某一端口应用了扩展型流模板后，不能在此端口上应用包含基本或高级 ACL 的 QoS 策略。

S3610&S5510 系列以太网交换机最多支持配置两个用户自定义流模板。在配置标准型用户自定义流模板时，每个模板中所有的元素所占字节之和必须小于等于 16 个字节。各个元素所占的字节数如下表所示。

各个元素所占字节数

名称	描述	流模板中占用的字节数
customer-cos	用户网络 802.1p 优先级域	1 字节
customer-vlan-id	用户网络 VLAN ID 域	6 字节
dip	IP 报文头部的目的 IP 地址域	不占用字节
dipv6	IPv6 报文头部的目的 IPv6 地址域	10 字节
dmac	以太网报文头部的目的 MAC 地址域	6 字节
dport	目的端口域	2 字节
ethernet-protocol	以太网报文头部的协议类型域	4 字节
dscp	IP 报文头部的 DSCP 域	1 字节
ip-precedence	IP 报文头部的 IP 优先级域	
tos	IP 报文头部的 ToS域	
fragments	IP 报文的分片标志位域	不占用字节
icmp-code	ICMP 代码域	2 字节
icmp-type	ICMP 类型域	2 字节
icmpv6-code	ICMPv6 代码域	2 字节
icmpv6-type	ICMPv6 类型域	2 字节
ip-protocol	IP 报文头部的协议类型域	不占用字节
ipv6-dscp	IPv6 报文头部的 DSCP 域	1 字节
ipv6-fragment	IPv6 分片标志域	不占用字节

名称	描述	流模板中占用的字节数
ipv6-protocol	IPv6 报文头部的协议类型域	不占用字节
service-cos	运营商网络 802.1p 优先级域	不占用字节
service-vlan-id	运营商网络 VLAN ID 域	不占用字节
sip	IP 报文头部的源 IP 地址域	不占用字节
sipv6	IPv6 报文头部的源 IPv6 地址域	不占用字节
smac	以太网报文头部的源 MAC 地址域	6 字节
sport	源端口域	2 字节
tcp-flag	TCP 报文头部的标志域	1 字节

说明：

dscp、**ip-precedence** **tos**　　三个元素占用同一个字节。同时配置这三个元素，或者同时配置这三个元素中的任意两个，它们在流模板中都只占用1个字节。

同时配置 **icmp-code** 和 **icmp-type** 元素，两者所占字节数仍然为2个字节。

同时配置 **icmpv6-code** 和 **icmpv6-type** 元素，两者所占字节数仍然为2个字节。

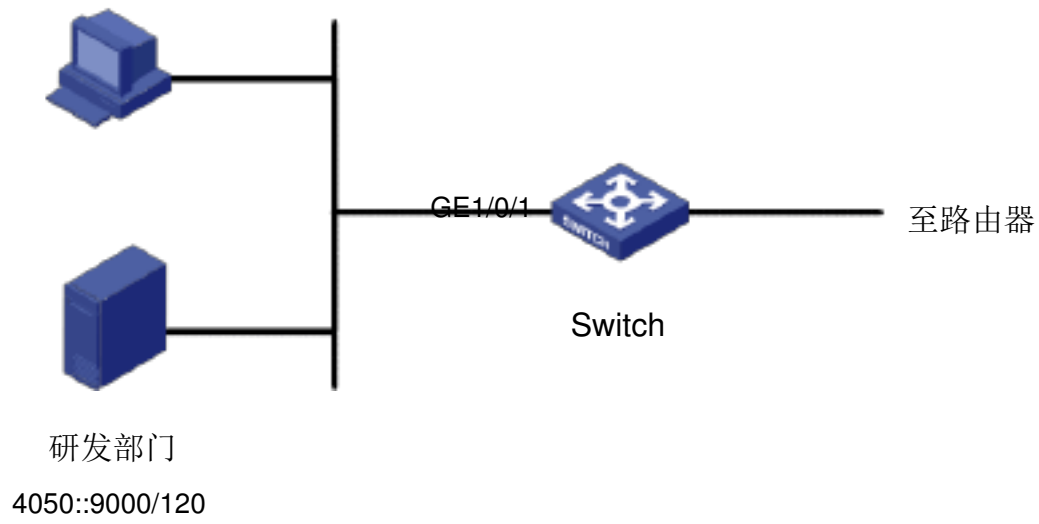
同时配置 **icmp-code** 或 **icmp-type** 与 **sport** 元素，只占用 2 个字节；同时配置 **icmpv6-code** 或 **icmpv6-type** 与 **sport** 元素，只占用 2 个字节。

4. IPv6 ACL 典型配置指导

4.1 基本 IPv6 ACL 典型配置指导

基本 IPv6 ACL 只根据源 IPv6 地址信息制定匹配规则，对报文进行相应的分析处理。 基本 IPv6 ACL 的序号取值范围为 2000～2999。

4.1.1 组网图



配置基本 IPv6 ACL 组网图

4.1.2 应用要求

公司企业网通过交换机（以S5500-EI为例）实现各部门之间的互连。 要求配置基本 IPv6 ACL，禁止研发部门（IPv6 地址为 4050::9000/120）访问网络。

4.1.3 配置过程和解释

定义基本 IPv6 ACL 2000，配置研发部门的访问规则。

```
<Switch> system-view
[Switch] acl ipv6 number 2000
[Switch-acl6-basic-2000] rule deny source 4050::9000/120
[Switch-acl6-basic-2000] quit
```

定义类 classifier_rd，对匹配 IPv6 ACL 2000 的报文进行分类。

```
[Switch] traffic classifier classifier_rd
[Switch-classifier-classifier_rd] if-match acl ipv6 2000
[Switch-classifier-classifier_rd] quit
```

定义流行为 behavior_rd，动作为拒绝报文通过。

```
[Switch] traffic behavior behavior_rd
[Switch-behavior-behavior_rd] filter deny
[Switch-behavior-behavior_rd] quit
```

定义策略 policy_rd，为类 classifier_rd 指定流行为 behavior_rd。

```
[Switch] qos policy policy_rd
[Switch-qospolicy-policy_rd]    classifier    classifier_rd    behavior
behavior_rd
[Switch-qospolicy-policy_rd] quit
```

将策略 policy_rd 应用到端口 GigabitEthernet 1/0/1

```
[Switch] interface GigabitEthernet 1/0/1
[Switch-GigabitEthernet1/0/1] qos apply policy policy_rd inbound
```

4.1.4 完整配置

```
#
traffic classifier classifier_rd operator and
 if-match acl ipv6 2000
#
traffic behavior behavior_rd
 filter deny
#
qos policy policy_rd
 classifier classifier_rd behavior behavior_rd
#
acl ipv6 number 2000
 rule 0 deny source 4050::9000/120
#
interface GigabitEthernet1/0/1
 qos apply policy policy_rd inbound
#
```

4.1.5 配置注意事项

需要注意的是：

当 ACL 的匹配顺序为 **config** 时，用户可以修改该 ACL 中的任何一条已经存在的规则，在修改 ACL 中的某条规则时，该规则中没有修改到的部分仍旧保持原来的状态；当 ACL 的匹配顺序为 **auto** 时，用户不能修改该 ACL 中的任何一条已经存在的规则，否则系统会提示错误信息。

新创建或修改后的规则不能和已经存在的规则相同，否则会导致创建或修改成功，系统会提示该规则已经存在。

当 ACL 的匹配顺序为 **auto** 时，新创建的规则将按照“深度优先”的原则插入到已有的规则中，但是所有规则对应的编号不会改变。

当基本 IPv6 ACL 被 QoS 策略引用对报文进行流分类时，ACL 规则中定义的动作（**deny** 或 **permit**）不起作用，交换机对匹配此 ACL 的报文采取的动作由 QoS 策略中流行为定义的动作决定。

当基本 IPv6 ACL 被 QoS 策略引用对报文进行流分类时，各产品的限制情况如下表所示。

各产品的限制情况

产品	说明
S3610 系列以太网交换机	不支持配置 **logging** 参数
S5510 系列以太网交换机	不支持配置 **logging** 参数
S5500-SI 系列以太网交换机	不支持配置 **logging** 和 **fragment** 参数
S5500-EI 系列以太网交换机	不支持配置 **logging** 和 **fragment** 参数
S7500E 系列以太网交换机	不支持配置 **logging** 和 **fragment** 参数

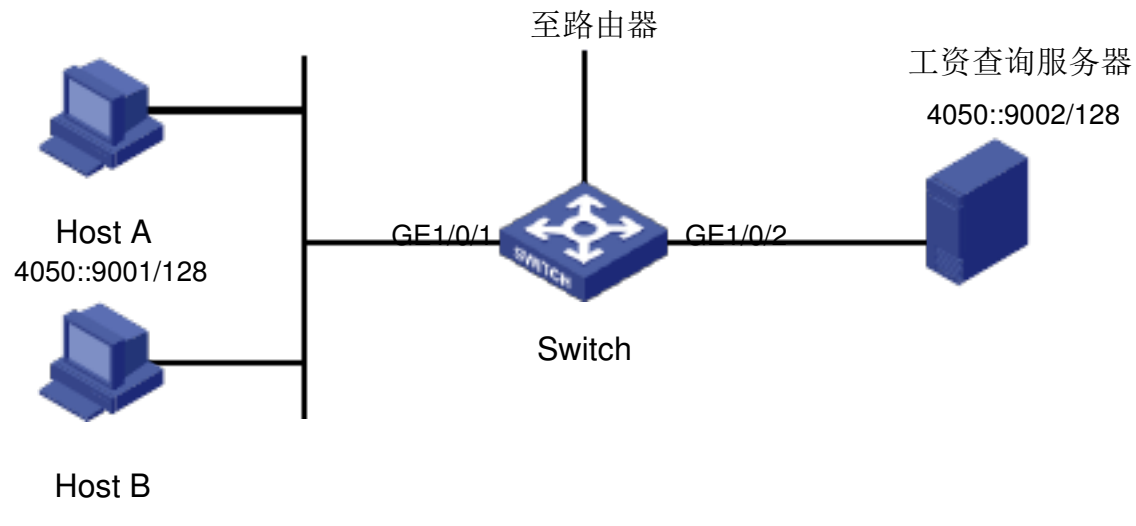
4.2 高级 IPv6 ACL 典型配置指导

高级 IPv6 ACL 可以使用报文的源 IPv6 地址信息、目的 IPv6 地址信息、IPv6 承载的协议类型、

协议的特性（例如TCP或UDP的源端口、目的端口，ICMP协议的消息类型、消息码等）等信息来制定匹配规则。

用户可以利用高级IPv6 ACL定义比基本IPv6 ACL更准确、更丰富、更灵活的规则。 高级IPv6 ACL的序号取值范围3000～3999。

4.2.1 组网图



配置高级IPv6 ACL组网图

4.2.2 应用要求

公司企业网通过交换机（以S5500-EI为例）实现各部门之间的互连。Host A和Host B通过端口GigabitEthernet 1/0/1接入交换机，Host A的IPv6地址为4050::9001，工资查询服务器的IPv6地址为4050::9002。

要求配置高级IPv6 ACL，禁止Host A访问工资查询服务器。

4.2.3 配置过程和解释

定义高级IPv6 ACL 3000，配置Host A的访问规则。

```
<Switch> system-view
[Switch] acl ipv6 number 3000
[Switch-acl6-adv-3000] rule deny ipv6 source 4050::9001 128 destination
4050::9002 128
[Switch-acl6-adv-3000] quit
```

定义类classifier_hostA，对匹配IPv6 ACL 3000的报文进行分类。

```
[Switch] traffic classifier classifier_hostA
[Switch-classifier-classifier_hostA] if-match acl ipv6 3000
[Switch-classifier-classifier_hostA] quit
```

定义流行为behavior_hostA，动作为拒绝报文通过。

```
[Switch] traffic behavior behavior_hostA
[Switch-behavior-behavior_hostA] filter deny
[Switch-behavior-behavior_hostA] quit
```

定义策略policy_hostA，为类classifier_hostA指定流行为behavior_hostA。

```
[Switch] qos policy policy_hostA
[Switch-qospolicy-policy_hostA] classifier classifier_hostA behavior
behavior_hostA
[Switch-qospolicy-policy_hostA] quit
```

将策略policy_hostA应用到端口GigabitEthernet 1/0/1

```
[Switch] interface GigabitEthernet 1/0/1
[Switch-GigabitEthernet1/0/1] qos apply policy policy_hostA inbound
```

4.2.4 完整配置

```
#
traffic classifier classifier_hostA operator and
 if-match acl ipv6 3000
#
traffic behavior behavior_hostA
 filter deny
#
qos policy policy_hostA
 classifier classifier_hostA behavior behavior_hostA
#
acl ipv6 number 3000
 rule 0 deny ipv6 source 4050::9001/128 destination 4050::9002/128
#
interface GigabitEthernet1/0/1
 qos apply policy policy_hostA inbound
#
```

4.2.5 配置注意事项

需要注意的是：

当 ACL 的匹配顺序为 **config** 时，用户可以修改该 ACL 中的任何一条已经存在的规则，在修改 ACL 中的某条规则时，该规则中没有修改到的部分仍旧保持原来的状态；当 ACL 的匹配顺序为 **auto** 时，用户不能修改该 ACL 中的任何一条已经存在的规则，否则系统会提示错误信息。

新创建或修改后的规则不能和已经存在的规则相同，否则会导致创建或修改成功，系统会提示该规则已经存在。

当 ACL 的匹配顺序为 **auto** 时，新创建的规则将按照“深度优先”的原则插入到已有的规则中，但是所有规则对应的编号不会改变。

当高级 IPv6 ACL 被 QoS 策略引用对报文进行流分类时，ACL 规则中定义的动作（**deny** 或 **permit**）不起作用，交换机对匹配此 ACL 的报文采取的动作由 QoS 策略中流行为定义的动作决定。

当高级 IPv6 ACL 被 QoS 策略引用对报文进行流分类时，各产品的限制情况如下表所示。

各产品的限制情况

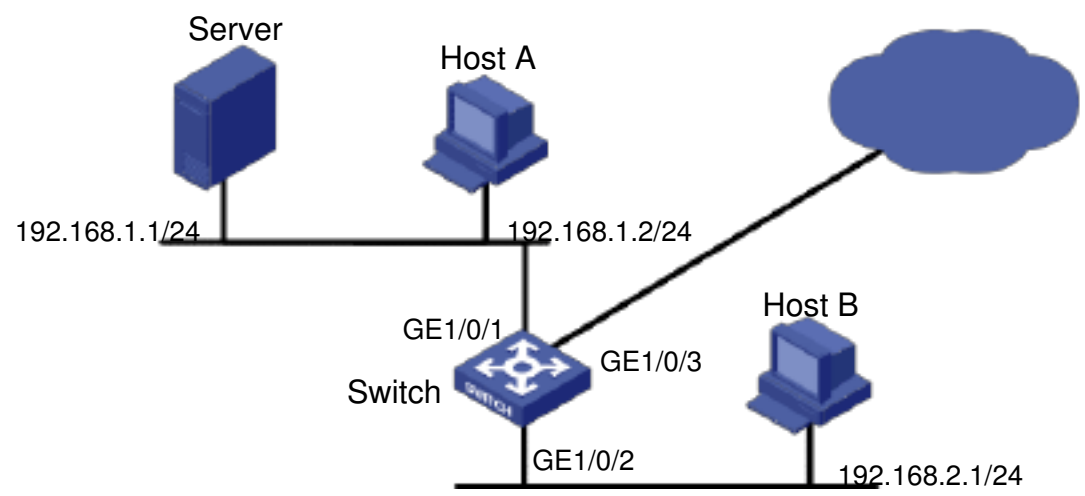
产品	说明
S3610 系列以太网交换机	不支持配置 **logging** 参数 当 *protocol* 为除 **ipv6** 之外的其他协议类型时，不支持配置 **fragment** 参数
S5510 系列以太网交换机	不支持配置 **logging** 参数 当 *protocol* 为除 **ipv6** 之外的其他协议类型时，不支持配置 **fragment** 参数
S5500-SI 系列以太网交换机	不支持配置 **dscp**、**fragment** 和 **logging** 参数 不支持配置操作符 *operator* 取值为 **gt**、**lt**、**neq** 和 **range**
S5500-EI 系列以太网交换机	当 QoS 策略应用于入方向（ **inbound** ）时，不支持配置 **logging** 和 **reflective** 参数；不支持配置操作符 *operator* 取值为 **neq** 当 QoS 策略应用于出方向（ **outbound** ）时，不支持配置 **logging** 和 **reflective** 参数；不支持配置操作符 *operator* 取值为 **gt**、**lt**、**neq** 和 **range**

产品	说明
S7500E 系列以太网交换机	当 QoS 策略应用于入方向（ **inbound** ）时，不支持配置 **logging** 和 **reflective** 参数；不支持配置操作符 *operator* 取值为 **neq** 当 QoS 策略应用于出方向（ **outbound** ）时，不支持配置 **logging** 和 **reflective** 参数；不支持配置操作符 *operator* 取值为 **gt**、**lt**、**neq** 和 **range**

5. QoS 典型配置指导

5.1 端口限速和流量监管典型配置指导

5.1.1 组网图



配置端口限速和流量监管组网图

5.1.2 应用要求

公司企业网通过交换机（以S5500-E为例）实现互连。网络环境描述如下：

Host A的 IP 地址为 192.168.1.2，Server 的 IP 地址为 192.168.1.1，两者通过 端口 GigabitEthernet 1/0/1接入交换机；

Host B的 IP 地址为 192.168.2.1，通过端口 GigabitEthernet 1/0/2 接入交换机。 配置端口限速和流量监管，实现如下需求：

限制 Switch 向 Internet 发送的流量为 640kbps，丢弃超出限制的报文；

限制 Host A向外发出的流量为 320kbps，丢弃超出限制的报文； 限制 Host B 与 Server 之间的流量为 64kbps，丢弃超出限制的报文。

5.1.3 配置过程和解释

针对 Switch 配置端口限速

在端口 GigabitEthernet 1/0/3上配置端口限速，限制端口发送报文的速率为 640kbps。

```
<Switch> system-view
[Switch] interface GigabitEthernet 1/0/3
[Switch-GigabitEthernet1/0/3] qos lr outbound cir 640
[Switch-GigabitEthernet1/0/3] quit
```

针对 Host A配置流量监管

定义基本 ACL 2000，对源 IP 地址为 192.168.1.2 的报文进行分类。

```
[Switch] acl number 2000
[Switch-acl-basic-2000] rule permit source 192.168.1.2 0
[Switch-acl-basic-2000] quit
```

定义类 classifier_hostA，匹配基本 ACL 2000。

```
[Switch] traffic classifier classifier_hostA
[Switch-classifier-classifier_hostA] if-match acl 2000
[Switch-classifier-classifier_hostA] quit
```

定义流行为 behavior_hostA，动作为限制报文的流量为320kbps。

```
[Switch] traffic behavior behavior_hostA
[Switch-behavior-behavior_hostA] car cir 320
[Switch-behavior-behavior_hostA] quit
```

定义策略 policy_hostA，为类 classifier_hostA 指定流行为 behavior_hostA。

```
[Switch] qos policy policy_hostA
[Switch-qospolicy-policy_hostA] classifier classifier_hostA behavior
behavior_hostA
[Switch-qospolicy-policy_hostA] quit
```

将策略 policy_hostA 应用到端口 GigabitEthernet 1/0/1上。

```
[Switch] interface GigabitEthernet 1/0/1
[Switch-GigabitEthernet1/0/1] qos apply policy policy_hostA inbound
[Switch-GigabitEthernet1/0/1] quit
```

针对 Host B 和 Server 配置流量监管

定义基本 ACL 3001，对源 IP 地址为 192.168.2.1，目的地址为 192.168.1.1 的报文进行分类。

```
[Switch] acl number 3001
[Switch-acl-adv-3001] rule permit ip source 192.168.2.1 0 destination
192.168.1.1 0
[Switch-acl-adv-3001] quit
```

定义基本 ACL 3002，对源 IP 地址为 192.168.1.1，目的地址为 192.168.2.1 的报文进行分类。

```
[Switch] acl number 3002
[Switch-acl-adv-3002] rule permit ip source 192.168.1.1 0 destination
192.168.2.1 0
[Switch-acl-adv-3002] quit
```

定义类 classifier_hostB，匹配基本 ACL 3001。

```
[Switch] traffic classifier classifier_hostB
[Switch-classifier-classifier_hostB] if-match acl 3001
[Switch-classifier-classifier_hostB] quit
```

定义类 classifier_Server，匹配基本 ACL 3002。

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

定义流行为 behavior_hostB，动作为限制报文的流量为64kbps。

```
[Switch] traffic behavior behavior_hostB
[Switch-behavior-behavior_hostB] car cir 64
[Switch-behavior-behavior_hostB] quit
```

定义流行为 behavior_Server，动作为限制报文的流量为64kbps。

```
[Switch] traffic behavior behavior_Server
[Switch-behavior-behavior_Server] car cir 64
[Switch-behavior-behavior_Server] quit
```

定义策略 policy_hostB，为类 classifier_hostB 指定流行为 behavior_hostB。

```
[Switch] qos policy policy_hostB
[Switch-qospolicy-policy_hostB] classifier classifier_hostB behavior
behavior_hostB
```

```
[Switch-qospolicy-policy_hostB] quit
```

定义策略 policy_Server，为类 classifier_Server 指定流行为 behavior_Server。

```
[Switch] qos policy policy_Server
[Switch-qospolicy-policy_Server] classifier classifier_Server behavior
behavior_Server
[Switch-qospolicy-policy_Server] quit
```

将策略 policy_hostB 和 policy_Server 分别应用到端口 GigabitEthernet 1/0/2 的入方向和出方向上。

```
[Switch] interface GigabitEthernet 1/0/2
[Switch-GigabitEthernet1/0/2] qos apply policy policy_hostB inbound
[Switch-GigabitEthernet1/0/2] qos apply policy policy_Server outbound
```

5.1.4 完整配置

```
#
traffic classifier classifier_hostA operator and
 if-match acl 2000
traffic classifier classifier_hostB operator and
 if-match acl 3001
traffic classifier classifier_Server operator and
 if-match acl 3002
#
traffic behavior behavior_Server
 car cir 64 cbs 4000 ebs 4000 green pass red discard yellow pass
traffic behavior behavior_hostA
 car cir 320 cbs 4000 ebs 4000 green pass red discard yellow pass
traffic behavior behavior_hostB
# car cir 64 cbs 4000 ebs 4000 green pass red discard yellow pass
qos policy policy_hostA
 classifier classifier_hostA behavior behavior_hostA
qos policy policy_hostB
 classifier classifier_hostB behavior behavior_hostB
qos policy policy_Server
 classifier classifier_Server behavior behavior_Server
 #
acl number 2000
# rule 0 permit source 192.168.1.2 0
acl number 3001
 rule 0 permit ip source 192.168.2.1 0 destination 192.168.1.1 0
acl number 3002
 rule 0 permit ip source 192.168.1.1 0 destination 192.168.2.1 0
 #
interface GigabitEthernet1/0/1
 qos apply policy policy_hostA inbound
#
interface GigabitEthernet1/0/2
 qos apply policy policy_hostB inbound
 qos apply policy policy_Server outbound
 #
interface GigabitEthernet1/0/3 qos
 lr outbound cir 640 cbs 40000
 #
```

5.1.5 配置注意事项

需要注意的是：

一个策略可以应用到多个端口上，端口的每个方向（**inbound**/**outbound**）只能应用一个策略。

S3610&S5510 系列以太网交换机不支持配置端口限速，用户可以使用 **qos gts** 命令配置流量整形，达到相同的效果。

S3610&S5510 系列以太网交换机支持在端口或端口组上直接配置流量监管， 用户可以使用 **qos car** 命令实现上述功能。

在 S5500-EI 系列以太网交换机上应用策略时，**inbound** 和 **outbound** 方向的 支持情况和流行为中定义的动作有关，详细情况如下表所示。

inbound 和 outbound 方向的支持情况

动作	**inbound** 方向	**outbound** 方向
流量统计	支持	支持
流量监管	支持	支持
流量过滤	支持	支持
流镜像	支持	支持
外层 VLAN 标签	支持	不支持
重定向	支持	不支持
标记报文的用户网络 VLAN ID	不支持	支持
标记报文的 802.1p 优先级	支持	支持
标记报文的丢弃优先级	支持	不支持
标记报文的 DSCP 优先级	支持	支持
标记报文的 IP 优先级	支持	支持
标记报文的本地优先级	支持	不支持
标记报文的运营商网络 VLAN ID	支持	支持

注意：

在 S5500-EI 系列以太网交换机上定义流行为时请遵循如下约束，否则策略将不能成功应 用：

nest 动作与除 **filter**、**remark dot1p** 以外的其他动作不能同时配置，并且将 **nest** 动作应用 到端口/端口组之前必须在端口/端口组上开启基本 QinQ 功能。

remark service-vlan-id 动作应用于入方向（**inbound**）时，与除 **filter**、**remark dot1p** 以外的其他动作不能同时配置。

mirror-to 动作应用于出方向（**outbound**）时，不能与其他动作同时配置。

在 S7500E 系列以太网交换机支持将策略应用于端口/端口组、VLAN 和全局。应用策略时，**inbound** 和 **outbound** 方向的支持情况和流行为中定义的动作以及单板的类型有关，详细情况如下表所示。关于单板类型的详细介绍请参见安装手册。

inbound 和 outbound 方向的支持情况

单板类型 / 动作	SC 单板		SA 单板		EA 单板	
	inbound 方向	**outbound** 方向	**inbound** 方向	**outbound** 方向	**inbound** 方向	**outbound** 方向

单板类型 动作	SC 单板		SA 单板		EA 单板	
	inbound 方向	**outbound** 方向	**inbound** 方向	**outbound** 方向	**inbound** 方向	**outbound** 方向
流量统计	支持	支持	支持	不支持	支持	不支持
流量监管	支持	支持	支持	不支持	支持	不支持
流量过滤	支持	支持	支持	不支持	支持	不支持
流镜像	支持	支持	支持	不支持	支持	不支持
外层 VLAN 标签	支持	不支持	支持	不支持	支持	不支持
重定向	支持	不支持	支持	不支持	支持	不支持
标记报文的用户网络 VLAN ID	不支持	支持	不支持	不支持	不支持	不支持
标记报文的 802.1p 优先级	支持	支持	支持	不支持	支持	不支持
标记报文的丢弃优先级	支持	不支持	支持	不支持	支持	不支持
标记报文的 DSCP 优先级	支持	支持	支持	不支持	支持	不支持
标记报文的 IP 优先级	支持	支持	支持	不支持	支持	不支持
标记报文的本地优先级	支持	不支持	支持	不支持	支持	不支持
标记报文的运营商网络 VLAN ID	支持	支持	支持	不支持	支持	不支持

注意：

在S7500E系列以太网交换机上应用策略时需要注意：

包含**nest**、**remark customer-vlan-id**和**remark service-vlan-id**动作的策略不能应用于VLAN或全局。

nest动作与除**filter**、**remark dot1p**以外的其他动作不能同时配置，并且将**nest**动作应用到端口/端口组上时必须在端口/端口组上开启基本 QinQ 功能，否则策略将不能成功应用。

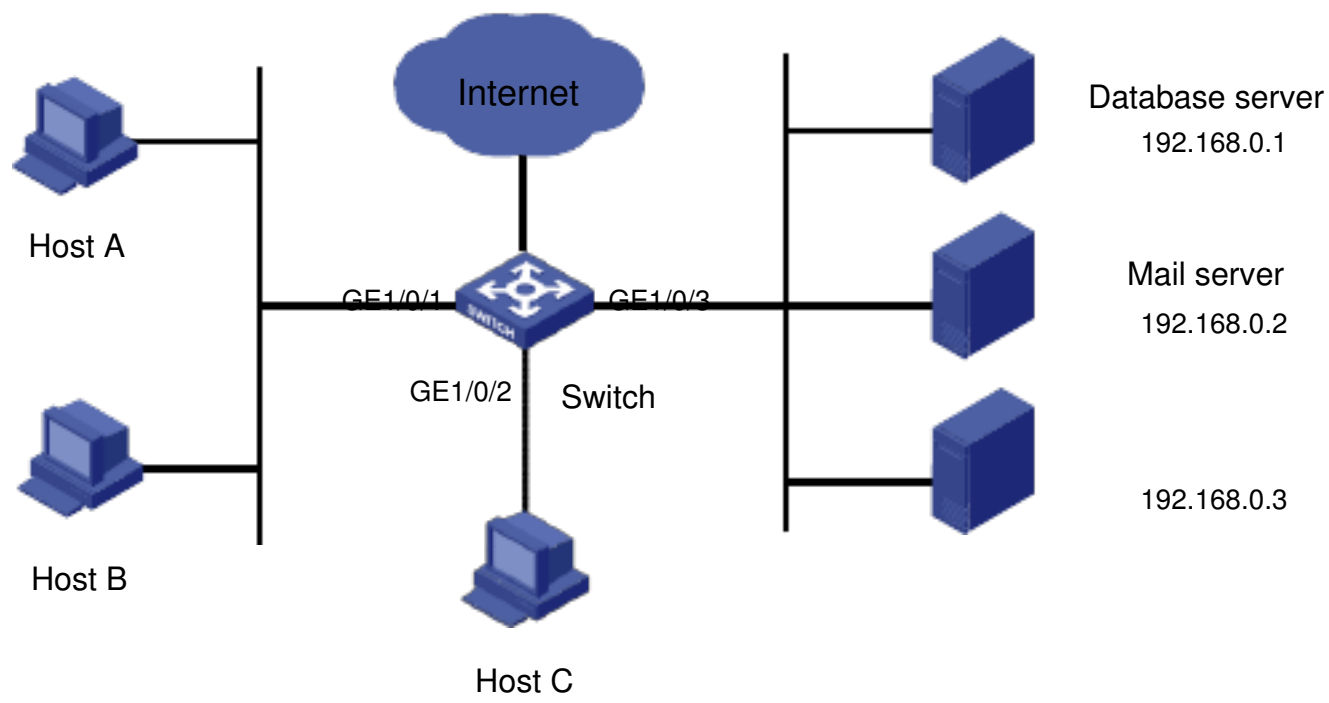
remark service-vlan-id动作应用于入方向（**inbound**）时，与除**filter**、**remark dot1p**以外的其他动作不能同时配置，否则策略将不能成功应用。

mirror-to 动作应用于出方向（**outbound**）时，不能与其他动作同时配置，否则策略将不能成功应用。

当某个策略包含的类中定义的分类规则只有**if-match service-vlan-id**时，并且流行为中定义的动作只有**remark customer-vlan-id**（或只有**remark customer-vlan-id**和**remark dot1p**）时，用户可以在 SA 单板和 EA 单板上开启了基本 QinQ 功能的端口的出方向（**outbound**）应用此策略，用来实现1:1 VLAN Mapping功能。

5.2 优先级重标记和队列调度典型配置指导

5.2.1 组网图



配置优先级重标记和队列调度组网图

5.2.2 应用要求

公司企业网通过交换机（以S5500-EI为例）实现互连。网络环境描述如下：

Host A 和 Host B 通过端口 GigabitEthernet 1/0/1 接入交换机；

Host C通过端口 GigabitEthernet 1/0/2接入交换机；

数据库服务器、邮件服务器和文件服务器通过端口GigabitEthernet 1/0/3接入交换机。

配置优先级重标记和队列调度，实现如下需求：

当 Host A 和 Host B 访问服务器时，交换机优先处理 Host A 和 Host B 访问数据库服务器的报文，其次处理 Host A 和 Host B 访问邮件服务器的报文，最后处理 Host A 和 Host B 访问文件服务器的报文；

无论 Host C 访问 Internet 或访问服务器，交换机都优先处理 Host C 发出的报文。

5.2.3 配置过程和解释

针对 Host A 和 Host B 的配置

定义高级 ACL 3000，对目的 IP 地址为 192.168.0.1 的报文进行分类。

```
<Switch> system-view
[Switch] acl number 3000
[Switch-acl-adv-3000] rule permit ip destination 192.168.0.1 0
[Switch-acl-adv-3000] quit
```

定义高级 ACL 3001，对目的 IP 地址为 192.168.0.2 的报文进行分类。

```
<Switch> system-view
[Switch] acl number 3001
[Switch-acl-adv-3001] rule permit ip destination 192.168.0.2 0
[Switch-acl-adv-3001] quit
```

定义高级 ACL 3002，对目的 IP 地址为 192.168.0.3 的报文进行分类。

```
<Switch> system-view
[Switch] acl number 3002
[Switch-acl-adv-3002] rule permit ip destination 192.168.0.3 0
[Switch-acl-adv-3002] quit
```

定义类 classifier_dbserver，匹配高级 ACL 3000。

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

定义类 classifier_mserver，匹配高级 ACL 3001。

```
[Switch] traffic classifier classifier_mserver
[Switch-classifier-classifier_mserver] if-match acl 3001
[Switch-classifier-classifier_mserver] quit
```

定义类 classifier_fserver，匹配高级 ACL 3002。

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

定义流行为 behavior_dbserver，动作为重标记报文的本地优先级为 4。

```
[Switch] traffic behavior behavior_dbserver
[Switch-behavior-behavior_dbserver] remark local-precedence 4
[Switch-behavior-behavior_dbserver] quit
```

定义流行为 behavior_mserver，动作为重标记报文的本地优先级为 3。

```
[Switch] traffic behavior behavior_mserver
[Switch-behavior-behavior_mserver] remark local-precedence 3
[Switch-behavior-behavior_mserver] quit
```

定义流行为 behavior_fserver，动作为重标记报文的本地优先级为 2。

```
[Switch] traffic behavior behavior_fserver
[Switch-behavior-behavior_fserver] remark local-precedence 2
[Switch-behavior-behavior_fserver] quit
```

定义策略 policy_server，为类指定流行为。

```
[Switch] qos policy policy_server
[Switch-qospolicy-policy_server]classifier classifier_dbserver behavior
behavior_dbserver
[Switch-qospolicy-policy_server] classifier classifier_mserver behavior
behavior_mserver
[Switch-qospolicy-policy_server] classifier classifier_fserver behavior
behavior_fserver
[Switch-qospolicy-policy_server] quit
```

将策略 policy_server 应用到端口 GigabitEthernet 1/0/1上。

```
[Switch] interface GigabitEthernet 1/0/1
[Switch-GigabitEthernet1/0/1] qos apply policy policy_server inbound
[Switch-GigabitEthernet1/0/1] quit
```

配置端口 GigabitEthernet 1/0/3 的队列调度方式为 SP（Strict-Priority，严格优先级）。

```
[Switch] interface GigabitEthernet 1/0/3
[Switch-GigabitEthernet1/0/3] qos sp
[Switch-GigabitEthernet1/0/3] quit
```

针对 Host C 的配置

配置端口 GigabitEthernet 1/0/2 的优先级信任模式为信任端口的优先级（缺省情况下即为信任端口的优先级，用户无需配置）并且设置端口的优先级为 5。

```
[Switch] interface GigabitEthernet 1/0/2
[Switch-GigabitEthernet1/0/2] qos priority 5
```

5.2.4 完整配置

```
#
traffic classifier classifier_fserver operator and
 if-match acl 3002
traffic classifier classifier_dbserver operator and
 if-match acl 3000
traffic classifier classifier_mserver operator and
 if-match acl 3001
#
traffic behavior behavior_fserver
 remark local-precedence 2
traffic behavior behavior_dbserver
 remark local-precedence 4
traffic behavior behavior_mserver
# remark local-precedence 3
qos policy policy_server
 classifier classifier_dbserver behavior behavior_dbserver
 classifier classifier_mserver behavior behavior_mserver
# classifier classifier_fserver behavior behavior_fserver
acl number 3000
 rule 0 permit ip destination 192.168.0.1 0
acl number 3001
 rule 0 permit ip destination 192.168.0.2 0
acl number 3002
 rule 0 permit ip destination 192.168.0.3 0
#
interface GigabitEthernet1/0/1
 qos apply policy policy_server inbound
#
interface GigabitEthernet1/0/2
 qos priority 5
#
interface GigabitEthernet1/0/3
 qos sp
#
```

5.2.5 配置注意事项

需要注意的是：

在 S5500-EI 系列以太网交换机上应用策略时，**inbound** 和 **outbound** 方向的支持情况请参见 inbound 和 outbound 方向的支持情况。

在 S7500E 系列以太网交换机上应用策略时，**inbound** 和 **outbound** 方向的支持情况请参见 inbound 和 outbound 方向的支持情况。

在 S5500-EI/7500E 系列以太网交换机上应用策略后，如果报文同时匹配了 **inbound** 和 **outbound** 方向上的策略，当动作冲突时，**outbound** 方向上

执行的动作会覆盖 **inbound** 方向上执行的动作，结果将会以 **outbound** 方向上执行的动作为准。例如，报文在进入交换机时匹配到 **inbound** 方向上的策略，动作为 **remark dscp 10**，在离开交换机时匹配到 **outbound** 方向上的策略，动作为 **remark dscp 40**，最终报文的 DSCP 优先级为 40。

S5500-SI/S5500-EI/S7500E 系列以太网交换机的端口支持 8 个输出队列，用户可以根据需要配置端口上的部分队列使用 SP（Strict-Priority，严格优先级）调度算法，部分队列使用W RR（Weighted Round Robin，加权轮询）调度算法。通过将端口上的队列分别加入SP 调度组和WRR 调度组（即 group 1），实现SP+WRR 的调度功能。在队列调度时，系统会优先 保证 SP 调度组内的队列调度，当 SP 调度组内的队列中没有报文发送时， 才会调度 WRR 调度组内的队列。SP 调度组内各个队列执行严格优先级 调度方式，W RR 调度组内各个队列执行加权轮询调度方式。

S3610&S5510 系列以太网交换机的端口支持 8 个输出队列，用户可以根据需 要配置端口上的部分队列使用 SP 调度算法，部分队列使用 WRR 调度算 法。通过将端口上的队列分别加入 SP 调度组和 WRR 调度组，实现 SP+WRR 的调度功能。进行队列调度时，各个组之间的调度方式为SP， 即比较各组中包含的最大队列编号，优先调度最大队列编号所在的组。例 如，将队列 5、6、7 划分到 SP 调度组，将队列2、3、4 划分到 WRR 调 度组 1，将队列 0、1 划分到WRR 调度组 2。经过比较，SP 调度组包含 的最大队列编号为 7，WRR 调度组 1 包含的最大队列编号为 4，WRR 调 度组 2 包含的最大队列编号为 1，因此交换机首先对 SP 组进行严格优先 级调度；SP 组中的队列没有报文发送时，才在 WRR 组 1 中进行轮询调 度；最后才会在W RR 组 2 中进行轮询调度。

在 S3610&S5510 系列以太网交换机上配置使用 WRR 或 SP+WRR 队列调度算 法时，必须将连续的队列划分到同一个调度组内。

缺省情况下，S5500-SI/S5500-EI 系列以太网交换机的所有端口采用 WRR 调 度算法，队列 0～7 的权重分别为 1、2、3、4、5、9、13、15。

缺省情况下，S3610&S5510/S7500E 系列以太网交换机的所有端口采用 SP 调 度算法。

S3610&S5510 系列以太网交换机支持在端口或端口组上配置拥塞避免（WRED）功能，用户可以使用**qos wred enable**命令实现上述功能。

配置 **remark** 动作时，各产品支持的可重标记的优先级类型有所不同，具体情况如下表所示。

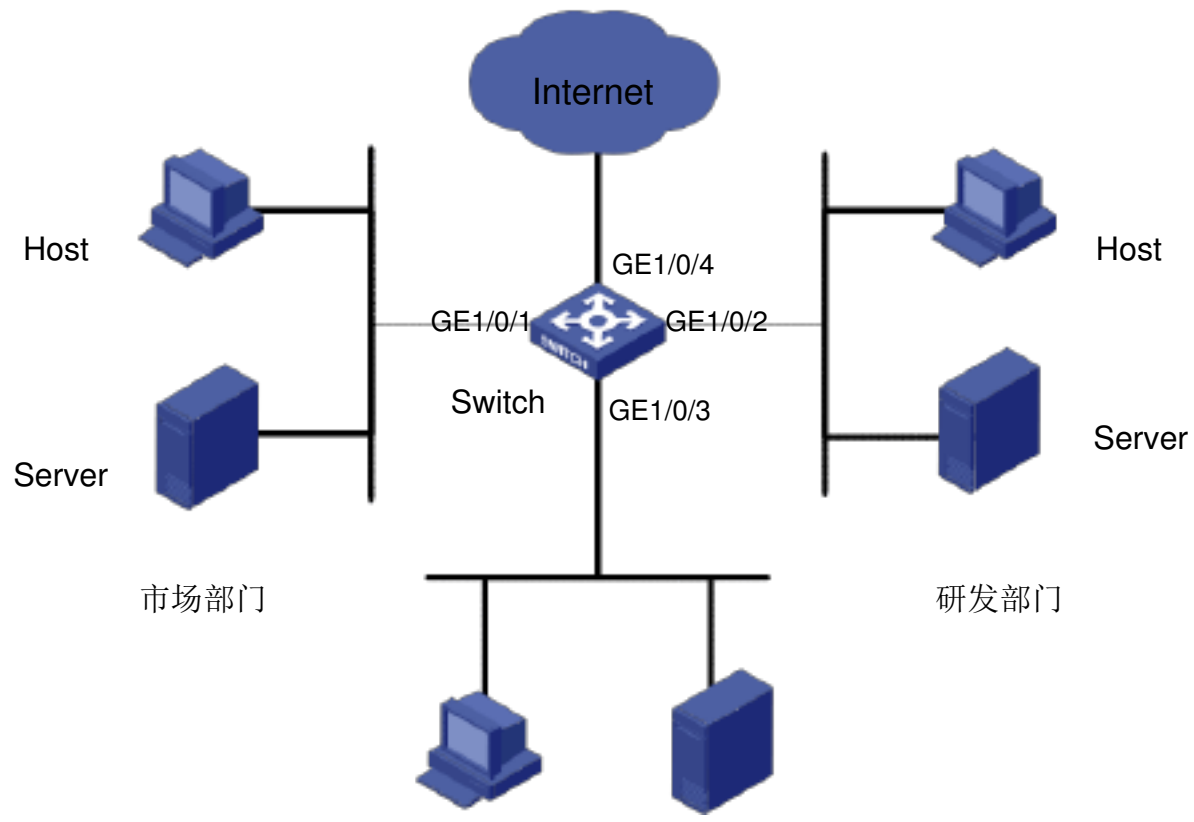
各产品对 remark 动作的支持情况

产品	说明
S3610 系列以太网交换机	支持重标记报文的 802.1p 优先级（**dot1p**）、丢弃优先级（**drop-precedence**）、DSCP 优先级（**dscp**）、IP 优先级（**ip-precedence**）、本地优先级（**local-precedence**）和运营商网络 VLAN ID（**service-vlan-id**）

产品	说明
S5510 系列以太网交换机	支持重标记报文的 802.1p 优先级（**dot1p**）、丢弃优先级（**drop-precedence**）、DSCP 优先级（**dscp**）、IP 优先级（**ip-precedence**）、本地优先级（**local-precedence**）和运营商网络 VLAN ID（**service-vlan-id**）
S5500-SI 系列以太网交换机	支持重标记报文的 802.1p 优先级（**dot1p**）、DSCP 优先级（**dscp**）、IP 优先级（**ip-precedence**）和本地优先级（**local-precedence**）
S5500-EI 系列以太网交换机	支持重标记报文的用户网络 VLAN ID（**customer-vlan-id**）、802.1p 优先级（**dot1p**）、丢弃优先级（**drop-precedence**）、DSCP 优先级（**dscp**）、IP 优先级（**ip-precedence**）、本地优先级（**local-precedence**）和运营商网络 VLAN ID（**service-vlan-id**）
S7500E 系列以太网交换机	支持重标记报文的用户网络 VLAN ID（**customer-vlan-id**）、802.1p 优先级（**dot1p**）、丢弃优先级（**drop-precedence**）、DSCP 优先级（**dscp**）、IP 优先级（**ip-precedence**）、本地优先级（**local-precedence**）和运营商网络 VLAN ID（**service-vlan-id**）

5.3 优先级映射和队列调度典型配置指导

5.3.1 组网图



配置优先级映射和队列调度组网图

5.3.2 应用要求

公司企业网通过交换机（以 S5500-EI 为例）实现各部门之间的互连。网络环境描述如下:市场部门通过端口 GigabitEthernet 1/0/1接入交换机；
研发部门通过端口 GigabitEthernet 1/0/2接入交换机；
管理部门通过端口 GigabitEthernet 1/0/3接入交换机；

市场部门、研发部门和管理部门内的设备发出的报文都不带有802.1Q标签头（VLAN Tag)。要求配置优先级映射和队列调度，实

现如下需求：

标记市场部门发出的报文的802.1p优先级为3，通过优先级映射，将此类报文放入队列4中；

标记研发部门发出的报文的802.1p优先级为4，通过优先级映射，将此类报文放入队列3中；

标记管理部门发出的报文的802.1p优先级为5，通过优先级映射，将此类报文放入队列6中；

在端口GigabitEthernet 1/0/4上配置调度算法为WRR，队列3、4和6所占的权重分别为5、10和15。

5.3.3 配置过程和解释

配置端口的端口优先级

配置端口GigabitEthernet 1/0/1的端口优先级为3。

```
<Switch> system-view
[Switch] interface GigabitEthernet 1/0/1
[Switch-GigabitEthernet1/0/1] qos priority 3
[Switch-GigabitEthernet1/0/1] quit
```

配置端口GigabitEthernet 1/0/2的端口优先级为4。

```
[Switch] interface GigabitEthernet 1/0/2
[Switch-GigabitEthernet1/0/2] qos priority 4
[Switch-GigabitEthernet1/0/2] quit
```

配置端口GigabitEthernet 1/0/3的端口优先级为5。

```
[Switch] interface GigabitEthernet 1/0/3
[Switch-GigabitEthernet1/0/3] qos priority 5
[Switch-GigabitEthernet1/0/3] quit
```

配置优先级映射表

配置802.1p优先级到本地优先级映射表，将802.1p优先级3、4、5对应的本地优先级配置为4、3、6。

```
[Switch] qos map-table dot1p-lp
[Switch-maptbl-dot1p-lp] import 3 export 4
[Switch-maptbl-dot1p-lp] import 4 export 3
[Switch-maptbl-dot1p-lp] import 5 export 6
[Switch-maptbl-dot1p-lp] quit
```

配置队列调度

配置端口GigabitEthernet 1/0/4的队列调度算法为WRR，队列3、4和6所占的权重分别为5、10和15。

```
[Switch] interface GigabitEthernet 1/0/4
[Switch-GigabitEthernet1/0/4] qos wrr 3 group 1 weight 5
[Switch-GigabitEthernet1/0/4] qos wrr 4 group 1 weight 10
[Switch-GigabitEthernet1/0/4] qos wrr 6 group 1 weight 15
```

5.3.4 完整配置

```
#
qos map-table dot1p-lp
 import 3 export 4
 import 4 export 3
 import 5 export 6
#
interface GigabitEthernet1/0/1
```

```
 qos priority 3
#
interface GigabitEthernet1/0/2
 qos priority 4
#
interface GigabitEthernet1/0/3
 qos priority 5
#
interface GigabitEthernet1/0/4
 qos wrr 3 group 1 weight 5
 qos wrr 4 group 1 weight 10
 qos wrr 6 group 1 weight 15
#
```

5.3.5 配置注意事项

关于各产品支持的队列调度算法的具体情况，请参见5.2.5 配置注意事项中的说明。

在S3610/S5510系列以太网交换机上配置优先级映射时需要注意：

对于不带有 802.1Q 标签头的报文，交换机将使用端口的优先级作为该端口接收的报文的本地优先级。

对于带有 802.1Q 标签头的报文，交换机提供两种优先级信任模式：信任报文 的优先级（根据报文的802.1p 优先级，查找802.1p 优先级到本地优先级/丢弃优先级映射表，然后为报文标记本地优先级和丢弃优先级）和信任端口的优先级（使用接收端口的端口优先级作为本地优先级）。

S3610/S5510 系列以太网交换机提供的802.1p 优先级到本地优先级/丢弃优先 级的映射关系缺省取值如下表所示。

dot1p-lp,dot1p-dp 缺省映射关系

映射输入索引	dot1p-lp 映射	dot1p-dp 映射
802.1p 优先级(dot1p)	本地优先级（lp）	丢弃优先级(dp)
0	2	0
1	0	0
2	1	0
3	3	0
4	4	0
5	5	0
6	6	0
7	7	0

S3610/S5510 系列以太网交换机还提供了 DSCP 优先级到本地优先级/丢弃优先级/802.1p 优先级/DSCP 优先级的映射表，分别对应相应的优先级映射关系，各个映射表的缺省关系取值如下表所示。

dscp-lp，dscp-dp，dscp-dot1p，dscp-dscp 缺省映射关系

映射输入索引	dscp-lp 映射	dscp-dp 映射	dscp-dot1p 映射	dscp-dscp 映射
DSCP 优先级	本地优先级(lp)	丢弃优先级(dp)	802.1p 优先级(dot1p)	DSCP 优先级

映射输入索引	dscp-lp 映射	dscp-dp 映射	dscp-dot1p 映射	dscp-dscp 映射
0～7	0	0	0	0
8～15	1	0	1	8
16～23	2	0	2	16
24～31	3	0	3	24
32～39	4	0	4	32
40～47	5	0	5	40
48～55	6	0	6	48
56～63	7	0	7	56

注意：

802.1p 优先级到本地优先级/丢弃优先级映射表和端口上的优先级信任模式相关联。配置端口上的信任模式为信任报文的802.1p优先级后，这些映射表才能起作用。

DSCP 优先级映到本地优先级/丢弃优先级/802.1p 优先级/DSCP 优先级映射表和流行为中**primap**动作相关联。在流行为中配置了**primap**动作后，这些映射表才能起作用。

在S5500-SI系列以太网交换机上配置优先级映射时需要注意：

对于不带有 802.1Q 标签头的报文，交换机将使用端口的优先级作为该端口接收的报文的802.1p 优先级，然后根据此优先级查找802.1p 优先级到本地优先级映射表，然后为报文标记本地优先级。

对于带有 802.1Q 标签头的报文，交换机将根据报文的 802.1p 优先级，查找 802.1p 优先级到本地优先级映射表，然后为报文标记本地优先级。

S5500-SI 系列以太网交换机提供的 802.1p 优先级到本地优先级的映射关系缺省取值如下表所示。

dot1p-lp 缺省映射关系

802.1p 优先级(dot1p)	本地优先级（lp）
0	2
1	0
2	1
3	3
4	4
5	5
6	6
7	7

注意：

S5500-SI系列以太网交换机不支持编辑802.1p优先级到本地优先级（dot1p-lp）映射表。

在S5500-EI/S7500E系列以太网交换机上配置优先级映射时需要注意：

S5500-EI/S7500E 系列以太网交换机提供两种优先级信任模式：信任报文的DSCP优先级和信任报文的802.1p 优先级。

信任报文的 DSCP 优先级：根据报文的 DSCP 优先级，查找 DSCP 优先级到802.1p 优先级/丢弃优先级/DSCP 优先级映射表，为报文标记 802.1p 优先级、丢弃优先级和新的DSCP 优先级。然后再根据802.1p 优先级查找802.1p 优先级到本地优先级映射表，为报文标记本地优先级。

信任报文的802.1p 优先级：对于不带有802.1Q 标签头的报文，交换机将使用端口的优先级作为该端口接收的报文的 802.1p 优先级，然后根据此优先级查找802.1p 优先级到本地优先级/丢弃优先级映射表，然后为报文标记本地优先级和丢弃优先级；对于带有802.1Q 标签头的报文，根据报文的802.1p 优先级，查找 802.1p 优先级到本地优先级/丢弃优先级映射表，然后为报文标记本地优先级和丢弃优先级。

S5500-EI/S7500E 系列以太网交换机提供的 802.1p 优先级到本地优先级/丢弃优先级、DSCP 优先级到 802.1p 优先级/丢弃优先级/DSCP 优先级的映射关系缺省取值如下表所示。

dot1p-lp,dot1p-dp 缺省映射关系

映射输入索引	dot1p-lp 映射	dot1p-dp 映射
802.1p 优先级(dot1p)	本地优先级（lp）	丢弃优先级(dp)
0	2	0
1	0	0
2	1	0
3	3	0
4	4	0
5	5	0
6	6	0
7	7	0

dscp-dp，dscp-dot1p，dscp-dscp 缺省映射关系

映射输入索引	dscp-dp 映射	dscp-dot1p 映射	dscp-dscp 映射
DSCP 优先级	丢弃优先级(dp)	802.1p 优先级(dot1p)	DSCP 优先级
0～7	0	0	0
8～15	0	1	8
16～23	0	2	16

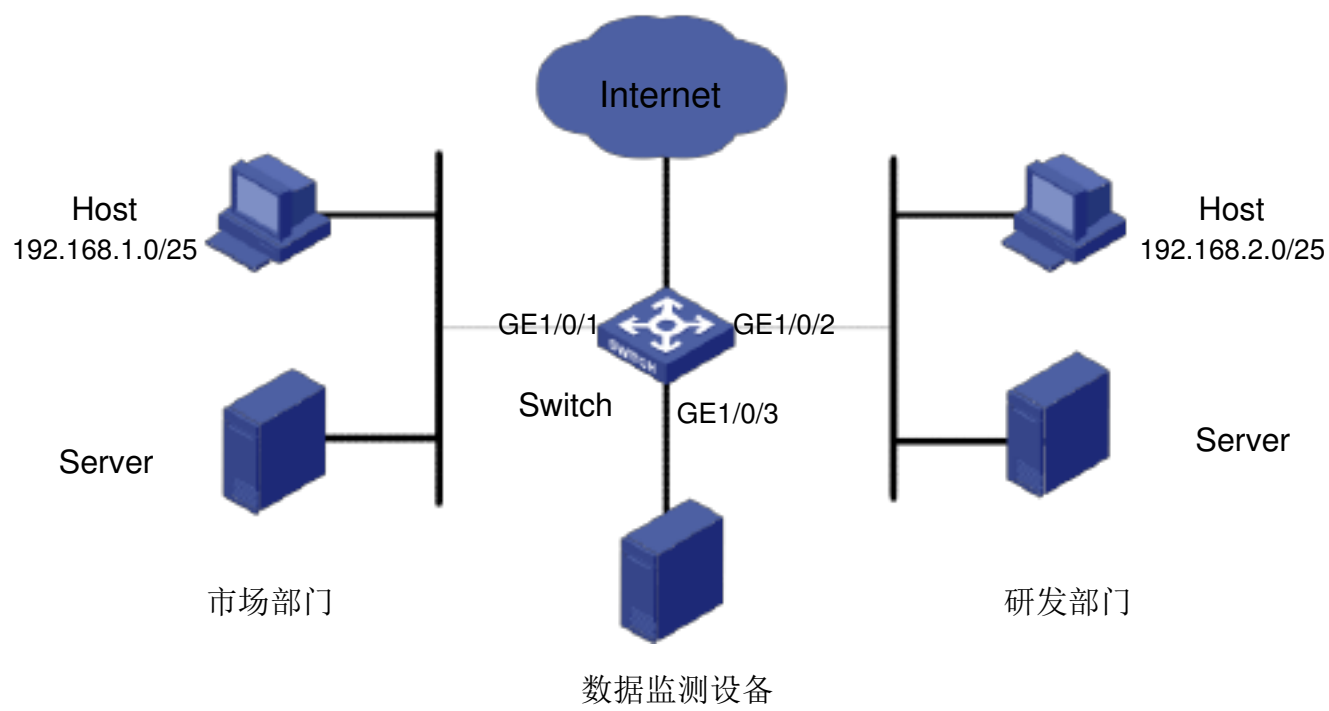
映射输入索引	dscp-dp 映射	dscp-dot1p 映射	dscp-dscp 映射
24～31	0	3	24
32～39	0	4	32
40～47	0	5	40
48～55	0	6	48
56～63	0	7	56

注意：

在S5500-EI/S7500E系列以太网交换机上配置DSCP优先级与丢弃优先级的映射关系时， 不支持将 DSCP 优先级映射为丢弃优先级 1。

5.4 流镜像和重定向至端口典型配置指导

5.4.1 组网图



配置流镜像和重定向组网图

5.4.2 应用要求

公司企业网通过交换机（以 S5500-EI 为例）实现各部门之间的互连。网络环境描述如下:市场部门通过端口 GigabitEthernet 1/0/1 接入交换机，其中 Host 的 IP 地址为 192.168.1.0/25 通过交换机访问 Internet;研发部门通过端口 GigabitEthernet 1/0/2 接入交换机，其中 Host 的 IP 地址为 192.168.2.0/25 通过交换机访问 Internet; 数据监测设备通过端口 GigabitEthernet 1/0/3接入交换机。

配置流镜像和重定向，实现如下需求：

在工作时间段（8:00 至 18:00）内，将市场部门内Host 访问 Internet 的流量镜像到数据监测设备；

在工作时间段（8:00 至 18:00）内，将研发部门内Host 访问 Internet的流量重定向到数据监测设备。

网络管理员可以使用数据监测设备对各部门访问Internet的流量进行分析。

5.4.3 配置过程和解释

定义工作时间段

定义 8:00 至 18:00 的周期时间段。

```
<Switch> system-view
[Switch] time-range trname 8:00 to 18:00 working-day
```

定义针对市场部门的策略

定义基本 ACL 2000，对市场部门内的 Host 进行分类。

```
[Switch] acl number 2000
[Switch-acl-basic-2000] rule permit source 192.168.1.0 0.0.0.127
time-range trname
[Switch-acl-basic-2000] quit
```

定义类 classifier_market，匹配基本 ACL 2000。

```
[Switch] traffic classifier classifier_market
[Switch-classifier-classifier_market] if-match acl 2000
[Switch-classifier-classifier_market] quit
```

定义流行为 behavior_market，动作为流镜像至端口 GigabitEthernet 1/0/3

```
[Switch] traffic behavior behavior_market
[Switch-behavior-behavior_market] mirror-to interface GigabitEthernet
1/0/3
[Switch-behavior-behavior_market] quit
```

定义策略 policy_market，为类 classifier_market 指定流行为 behavior_market。

```
[Switch] qos policy policy_market
[Switch-qospolicy-policy_market] classifier classifier_market behavior
behavior_market
[Switch-qospolicy-policy_market] quit
```

定义针对研发部门的策略

定义基本 ACL 2001，对研发部门内的 Host 进行分类。

```
[Switch] acl number 2001
[Switch-acl-basic-2001] rule permit source 192.168.2.0 0.0.0.127
time-range trname
[Switch-acl-basic-2001] quit
```

定义类 classifier_rd，匹配基本 ACL 2001。

```
[Switch] traffic classifier classifier_rd
[Switch-classifier-classifier_rd] if-match acl 2001
[Switch-classifier-classifier_rd] quit
```

定义流行为 behavior_rd，动作为重定向至端口 GigabitEthernet 1/0/3

```
[Switch] traffic behavior behavior_rd
[Switch-behavior-behavior_rd] redirect interface GigabitEthernet 1/0/3
[Switch-behavior-behavior_rd] quit
```

定义策略 policy_rd，为类 classifier_rd 指定流行为 behavior_rd。

```
[Switch] qos policy policy_rd
[Switch-qospolicy-policy_rd] classifier classifier_rd behavior
behavior_rd
[Switch-qospolicy-policy_rd] quit
```

应用策略

将策略 policy_market 应用到端口 GigabitEthernet 1/0/1上。

```
[Switch] interface GigabitEthernet 1/0/1
[Switch-GigabitEthernet1/0/1] qos apply policy policy_market inbound
[Switch-GigabitEthernet1/0/1] quit
```

将策略 policy_rd 应用到端口 GigabitEthernet 1/0/2上。

```
[Switch] interface GigabitEthernet 1/0/2
[Switch-GigabitEthernet1/0/2] qos a policy policy_rd inbound
```

5.4.4 完整配置

```
#
traffic classifier classifier_market operator and
 if-match acl 2000
traffic classifier classifier_rd operator and
 if-match acl 2001
#
traffic behavior behavior_market
 mirror-to interface GigabitEthernet1/0/3
traffic behavior behavior_rd
 redirect interface GigabitEthernet1/0/3
#
qos policy policy_market
 classifier classifier_market behavior behavior_market
qos policy policy_rd
 classifier classifier_rd behavior behavior_rd
#
time-range trname 08:00 to 18:00 working-day
#
acl number 2000
rule 0 permit source 192.168.1.0 0.0.0.127 time-range trname
acl number 2001
rule 0 permit source 192.168.2.0 0.0.0.127 time-range trname
#
interface GigabitEthernet1/0/1
 qos apply policy policy_market inbound
#
interface GigabitEthernet1/0/2
 qos apply policy policy_rd inbound
#
```

5.4.5 配置注意事项

需要注意的是：

在 S5500-EI 系列以太网交换机上应用策略时，**inbound** 和 **outbound** 方向的支持情况请参见 inbound 和 outbound 方向的支持情况。

在 S7500E 系列以太网交换机上应用策略时，**inbound** 和 **outbound** 方向的支持情况请参见 inbound 和 outbound 方向的支持情况。

在 S5500-EI/S7500E 系列以太网交换机上配置 **mirror-to** 动作应用于出方向（**outbound**）时，不能与其他动作同时配置，否则策略将不能成功应用在

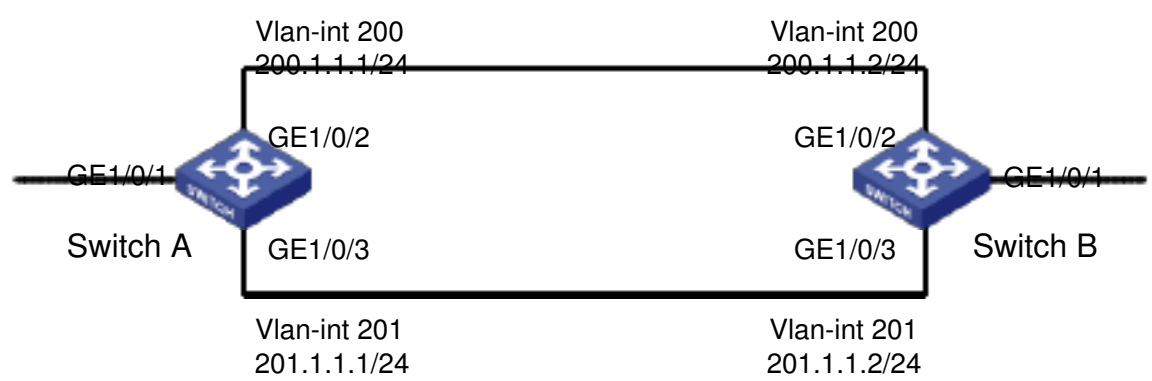
S3610&S5510 系列以太网交换机上，流镜像的目的端口不能为聚合组成员端口。

在 S3610&S5510 系列以太网交换机上同时配置本地端口镜像和流镜像时，本地端口镜像的目的端口和流镜像的目的端口必须为同一个端口。

S3610&S5510 系列以太网交换机只支持配置一个流镜像目的端口，S5500-SI/S5500-EI/S7500E 系列以太网交换机支持配置多个流镜像目的端口。

5.5 重定向至下一跳典型配置指导

5.5.1 组网图



配置重定向至下一跳组网图

5.5.2 应用要求

某网络环境描述如下：

交换机 Switch A 通过两条链路与 Switch B 连接，同时 Switch A 和 Switch B 各自连接其他的设备；

Switch A 上的端口 GigabitEthernet 1/0/2和 Switch B 上的端口 GigabitEthernet 1/0/2 属于 VLAN 200；

Switch A 上的端口 GigabitEthernet 1/0/3和 Switch B 上的端口 GigabitEthernet 1/0/3 属于 VLAN 201；

Switch A 上 VLAN 200 虚接口的 IP 地址为 200.1.1.1，VLAN 201 虚接口的 IP 地址为 201.1.1.1；Switch B 上 VLAN 200 虚接口的 IP 地址为 200.1.1.2，VLAN 201 虚接口的 IP 地址为 201.1.1.2。

配置重定向至下一跳，实现策略路由功能，满足如下需求：

将 Switch A 的端口 GigabitEthernet 1/0/1 接收到的源 IP 地址为 2.1.1.1 的报文转发至 200.1.1.2；

将 Switch A 的端口 GigabitEthernet 1/0/1 接收到的源 IP 地址为 2.1.1.2 的报文转发至 201.1.1.2；

对于 Switch A 的端口 GigabitEthernet 1/0/1 接收到的其它报文，按照查找路由表的方式进行转发。

5.5.3 配置过程和解释

配置 Switch A

定义基本 ACL 2000，对源 IP 地址为 2.1.1.1 的报文进行分类。

```
<Switch> system-view
[Switch] acl number 2000
[Switch-acl-basic-2000] rule permit source 2.1.1.1 0
[Switch-acl-basic-2000] quit
```

定义基本 ACL 2001，对源 IP 地址为 2.1.1.2 的报文进行分类。

```
[Switch] acl number 2001
[Switch-acl-basic-2001] rule permit source 2.1.1.2 0
[Switch-acl-basic-2001] quit
```

定义类 classifier_1，匹配基本 ACL 2000。

```
[Switch] traffic classifier classifier_1
[Switch-classifier-classifier_1] if-match acl 2000
[Switch-classifier-classifier_1] quit
```

定义流行为 behavior_1，动作为重定向至 200.1.1.2。

```
[Switch] traffic behavior behavior_1
[Switch-behavior-behavior_1] redirect next-hop 200.1.1.2
[Switch-behavior-behavior_1] quit
```

定义类 classifier_2，匹配基本 ACL 2001。

```
[Switch] traffic classifier classifier_2
[Switch-classifier-classifier_2] if-match acl 2001
[Switch-classifier-classifier_2] quit
```

定义流行为 behavior_2，动作为重定向至 201.1.1.2。

```
[Switch] traffic behavior behavior_2
[Switch-behavior-behavior_2] redirect next-hop 201.1.1.2
[Switch-behavior-behavior_2] quit
```

定义策略 policy，为类 classifier_1 指定流行为 behavior_1，为类 classifier_2 指定流行为 behavior_2。

```
[Switch] qos policy policy
[Switch-qospolicy-policy] classifier classifier_1 behavior behavior_1
[Switch-qospolicy-policy] classifier classifier_2 behavior behavior_2
[Switch-qospolicy-policy] quit
```

将策略 policy 应用到端口 GigabitEthernet 1/0/1的入方向上。

```
[Switch] interface GigabitEthernet 1/0/1
[Switch-GigabitEthernet1/0/1] qos apply policy policy inbound
```

5.5.4 完整配置

```
#
traffic classifier classifier_1 operator and
 if-match acl 2000
traffic classifier classifier_2 operator and
 if-match acl 2001
#
traffic behavior behavior_1
 redirect next-hop 200.1.1.2
traffic behavior behavior_2
 redirect next-hop 201.1.1.2
#
qos policy policy
 classifier classifier_1 behavior behavior_1
 classifier classifier_2 behavior behavior_2
#
acl number 2000
 rule 0 permit source 2.1.1.1 0
acl number 2001
 rule 0 permit source 2.1.1.2 0
#
interface GigabitEthernet1/0/1
 qos apply policy policy inbound
#
```

5.5.5 配置注意事项

需要注意的是：

在 S5500-EI 系列以太网交换机上应用策略时，**inbound** 和 **outbound** 方向的支持情况请参见 inbound 和 outbound 方向的支持情况。

在 S7500E 系列以太网交换机上应用策略时，**inbound** 和 **outbound** 方向的支持情况请参见 inbound 和 outbound 方向的支持情况。

用户可以根据实际情况需要配置策略路由。与单纯依照 IP 报文的目的地址查找路由表进行转发不同,策略路由基于到达报文的源地址等信息灵活地进行路由选择。

策略路由的优先级要高于普通路由，即报文首先按照策略路由进行转发。如果无法匹配所有的策略路由条件，再按照普通路由进行转发。

6. 交换机端口链路类型介绍

6.1 交换机端口链路类型介绍

交换机以太网端口共有三种链路类型：Access、Trunk 和 Hybrid。

1．Access 类型的端口只能属于 1个 VLAN，一般用于连接计算机的端口；

2．Trunk类型的端口可以属于多个 VLAN，可以接收和发送多个 VLAN 的报文，一般用于交换机之间连接的端口；

3．Hybrid 类型的端口可以属于多个 VLAN，可以接收和发送多个 VLAN 的报文，可以用于交换机之间连接，也可以用于连接用户的计算机。

其中，Hybrid 端口和 Trunk 端口的相同之处在于两种链路类型的端口都可以允许多个 VLAN 的报文发送时打标签；不同之处在于 Hybrid 端口可以允许多个 VLAN 的报文发送时不打标签，而 Trunk 端口只允许缺省 VLAN 的报文发送时不打标签。

三种类型的端口可以共存在一台以太网交换机上，但 Trunk 端口和 Hybrid 端口之间不能直接切换，只能先设为 Access 端口，再设置为其他类型端口。例如：Trunk 端口不能直接被设置为 Hybrid 端口，只能先设为 Access 端口，再设置为 Hybrid 端口。

6.2 各类型端口使用注意事项

配置 Trunk 端口或 Hybrid 端口，并利用 Trunk 端口或 Hybrid 端口发送多个 VLAN 报文时一定要注意：本端端口和对端端口的缺省 VLAN ID(端口的 PVID)要保持

一致。

当在交换机上使用 isolate-user-vlan 来进行二层端口隔离时，参与此配置的端口的链路类型会自动变成 Hybrid 类型。

Hybrid 端口的应用比较灵活，主要为满足一些特殊应用需求。此类需求多为在无法下发访问控制规则的交换机上，利用 Hybrid 端口收发报文时的处理机制，来完成对同一网段的 PC 机之间的二层访问控制。

6.3 各类型端口在接收和发送报文时的处理

1．端口接收报文时的处理：

端口接收到的报文类型	报文帧结构中携带 VLAN 标记	报文帧结构中不携带 VLAN 标记
Access 端口	丢弃该报文	为该报文打上 VLAN 标记为本端口的 PVID
Trunk 端口	判断本端口是否允许携带该 VLAN 标记的报文通过。如果允许则报文携带原有 VLAN 标记进行转发，否则丢弃该报文	同上
Hybrid 端口	同上	同上

2．端口发送报文时的处理：

Access 端口	剥掉报文所携带的 VLAN 标记，进行转发
Trunk 端口	首先判断报文所携带的 VLAN 标记是否和端口的 PVID 相等。如果相等，则剥掉报文所携带的 VLAN 标记，进行转发；否则报文将携带原有的 VLAN 标记进行转发
Hybrid 端口	首先判断报文所携带的 VLAN 标记在本端口需要做怎样的处理。如果是 untagged 方式转发，则处理方式同 Access 端口； 如果是 tagged 方式转发，则处理方式同 Trunk 端口

6.4 交换机 Trunk 端口配置

6.4.1 组网需求：

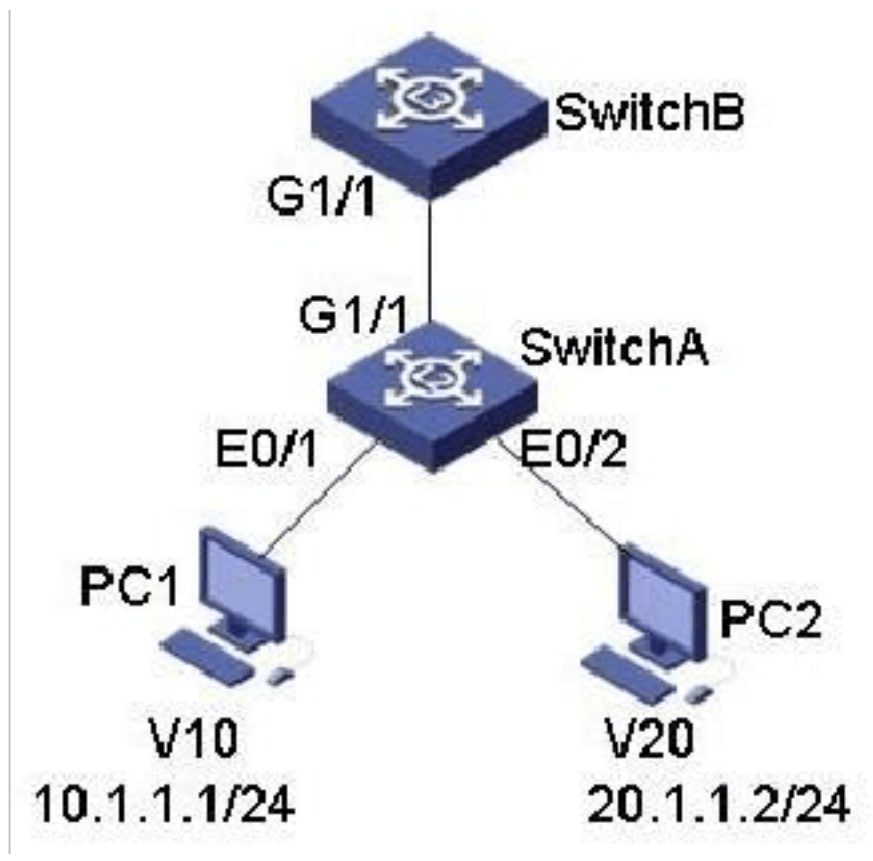
1．SwitchA 与 SwitchB 用 trunk 互连，相同 VLAN 的 PC 之间可以互访，不同 VLAN 的 PC 之间禁止互访；

2．PC1 与 PC2 之间在不同 VLAN，通过设置上层三层交换机 SwitchB 的 VLAN 接口 10 的 IP 地址为 10.1.1.254/24，VLAN 接口 20 的 IP 地址为 20.1.1.254/24 可以实现 VLAN 间的互访。

6.4.2 组网图：

1．VLAN 内互访， VLAN 间禁访

2．通过三层交换机实现 VLAN 间互访



6.4.3 配置步骤：

实现 VLAN 内互访 VLAN 间禁访配置过程

SwitchA 相关配置：

1．创建（进入） VLAN10，将 E0/1 加入到 VLAN10

[SwitchA]vlan 10

[SwitchA-vlan10]port Ethernet 0/1 2．创建（进入）
VLAN20，将 E0/2 加入到 VLAN20

[SwitchA]vlan 20

[SwitchA-vlan20]port Ethernet 0/2

3．将端口 G1/1 配置为 Trunk 端口，并允许 VLAN10 和 VLAN20 通过

[SwitchA]interface GigabitEthernet 1/1

[SwitchA-GigabitEthernet1/1]port link-type trunk

[SwitchA-GigabitEthernet1/1]port trunk permit vlan 10 20

SwitchB 相关配置：

1．创建（进入） VLAN10，将 E0/10 加入到 VLAN10

[SwitchB]vlan 10

[SwitchB-vlan10]port Ethernet 0/10 2．创建（进入）
VLAN20，将 E0/20 加入到 VLAN20

[SwitchB]vlan 20

[SwitchB-vlan20]port Ethernet 0/20

3．将端口 G1/1 配置为 Trunk 端口，并允许 VLAN10 和 VLAN20 通过

[SwitchB]interface GigabitEthernet 1/1

[SwitchB-GigabitEthernet1/1]port link-type trunk

[SwitchB-GigabitEthernet1/1]port trunk permit vlan 10 20

通过三层交换机实现 VLAN 间互访的配置

SwitchA 相关配置：

1．创建（进入） VLAN10，将 E0/1 加入到 VLAN10

[SwitchA]vlan 10

[SwitchA-vlan10]port Ethernet 0/1 2．创建（进入）

VLAN20，将 E0/2 加入到 VLAN20 [SwitchA]vlan 20

[SwitchA-vlan20]port Ethernet 0/2

3．将端口 G1/1 配置为 Trunk 端口，并允许 VLAN10 和 VLAN20 通过

[SwitchA]interface GigabitEthernet 1/1

[SwitchA-GigabitEthernet1/1]port link-type trunk

[SwitchA-GigabitEthernet1/1]port trunk permit vlan 10 20

SwitchB 相关配置:

1．创建 VLAN10

[SwitchB]vlan 10

2．设置 VLAN10 的虚接口地址

[SwitchB]interface vlan 10

[SwitchB-int-vlan10]ip address 10.1.1.254 255.255.255.0

3．创建 VLAN20

[SwitchB]vlan 20

4．设置 VLAN20 的虚接口地址

[SwitchB]interface vlan 20

[SwitchB-int-vlan20]ip address 20.1.1.254 255.255.255.0

5．将端口 G1/1 配置为 Trunk 端口，并允许 VLAN10 和 VLAN20 通过

[SwitchA]interface GigabitEthernet 1/1

[SwitchA-GigabitEthernet1/1]port link-type trunk

[SwitchA-GigabitEthernet1/1]port trunk permit vlan 10 20

6.5 交换机 Hybrid 端口配置

6.5.1 组网需求：

需求一

1.PC1、PC2 和 PC3 分别连接到二层交换机 SwitchA 的端口 E0/1 、E0/2 和 E0/3，端口分属于 VLAN10 、20 和 30，服务器连接到端口 G2/1，属于 VLAN100 。

2. PC1 的 IP 地址为 10.1.1.1/24 ， PC2 的 IP 地址为 10.1.1.2/24 ， PC3 的 IP 地

址为 10.1.1.3/24 ，服务器的 IP 地址为 10.1.1.254/24 ；

3．PC1 和 PC2 之间可以互访；

4．PC1 和 PC3 之间可以互访；

5．PC1、PC2 和 PC3 都可以访问服务器；

6．其余的 PC 间访问均禁止。　需求

二

1.PC1、PC2 和 PC3 分别连接到二层交换机 SwitchA 的端口 E0/1 、E0/2 和 E0/3，端口分属于 VLAN10 、20 和 30；PC4 和 PC5 分别连接到二层交换机 SwitchB 的端口 E0/1 和 E0/2，端口分属于 VLAN10 和 20；

2．SwitchA 通过端口 G2/1，连接到 SwitchB 的端口 G1/1；SwitchA 的端口 G2/1 和 SwitchB 的端口 G1/1 均不是 Trunk 端口；

3．PC1 的 IP 地址为 10.1.1.1/24 ，PC2 的 IP 地址为 10.1.1.2/24 ，PC3 的 IP 地址为 10.1.1.3/24 ,PC4 的 IP 地址为 10.1.1.4/24 ,PC5 的 IP 地址为 10.1.1.5/24 ；

4．PC1 和 PC3 之间可以互访；

5．PC2 和 PC3 之间可以互访；

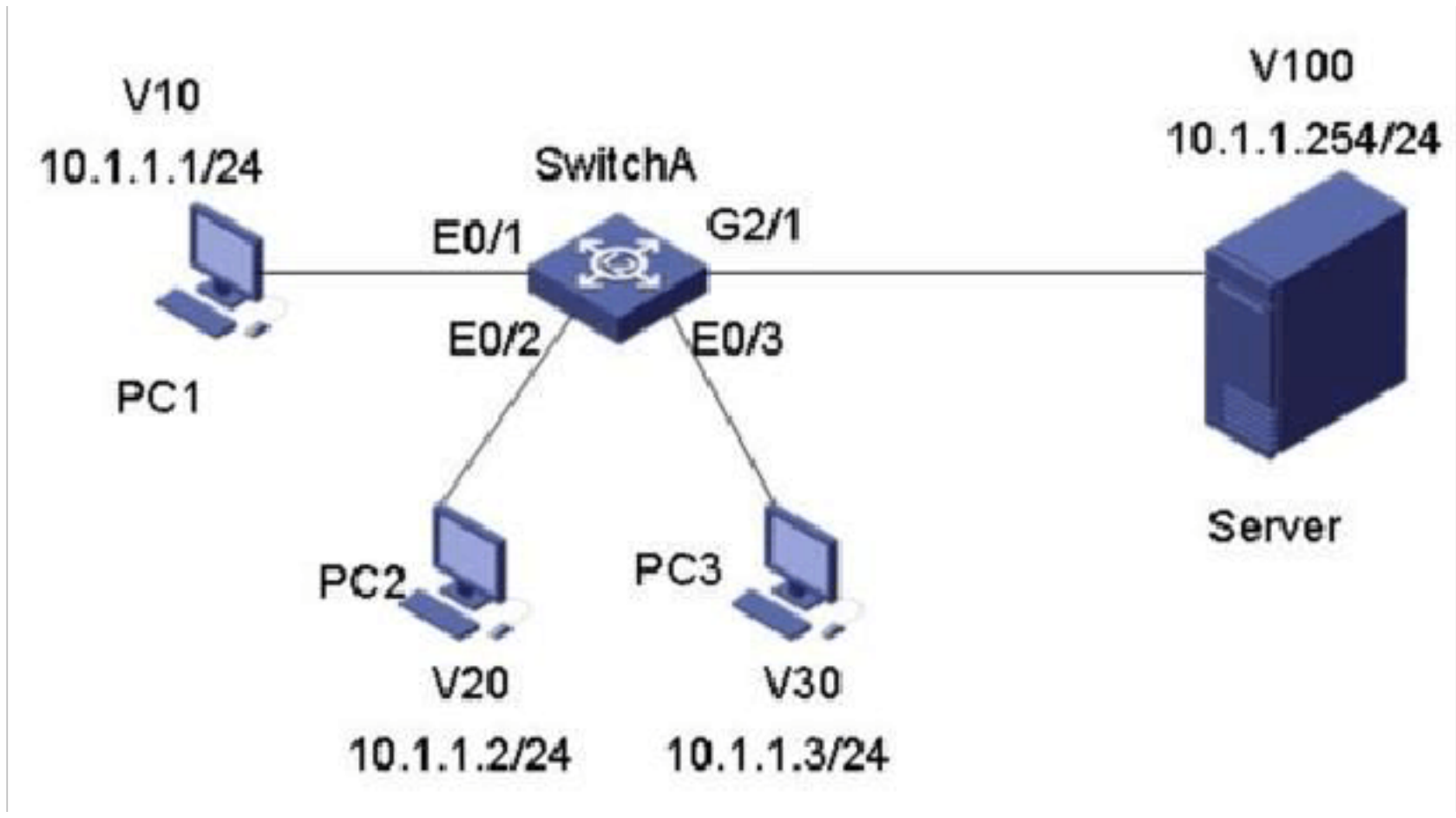
6．PC1 和 PC4 之间可以互访；

7．PC2 和 PC5 之间可以互访；

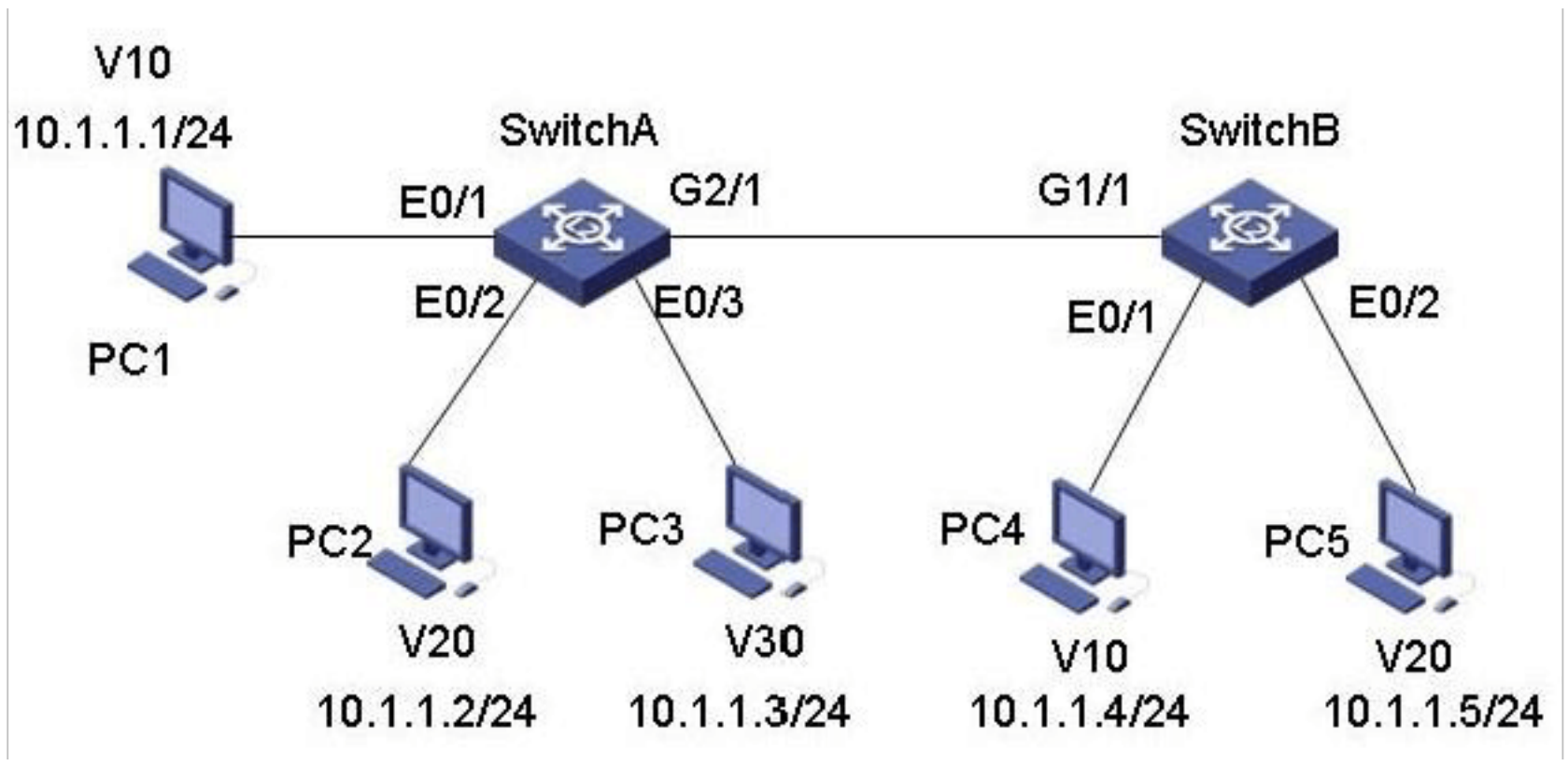
8．其余 PC 之间均禁止互相访问。

6.5.2组网图：

需求一



需求二



6.5.2 配置步骤：

需求一配置过程

SwitchA 相关配置：

1．创建（进入） VLAN10，将 E0/1 加入到 VLAN10

[SwitchA]vlan 10

[SwitchA-vlan10]port Ethernet 0/1 2. 创建（进

入）VLAN20，将 E0/2 加入到 VLAN20

[SwitchA]vlan 20

[SwitchA-vlan20]port Ethernet 0/2 3. 创建（进

入）VLAN30，将 E0/3 加入到 VLAN30

[SwitchA]vlan 30

[SwitchA-vlan30]port Ethernet 0/3 4. 创建（进入）

VLAN100，将 G2/1 加入到 VLAN100 [SwitchA]vlan 100

[SwitchA-vlan100]port GigabitEthernet 2/1

5. 配置端口 E0/1 为 Hybrid 端口，能够接收 VLAN20、30 和 100 发过来的报文

[SwitchA]interface Ethernet 0/1

[SwitchA-Ethernet0/1]port link-type hybrid

[SwitchA-Ethernet0/1]port hybrid vlan 20 30 100 untagged 6. 配置端

口 E0/2 为 Hybrid 端口，能够接收 VLAN10 和 100 发过来的报文

[SwitchA]interface Ethernet 0/2

[SwitchA-Ethernet0/2]port link-type hybrid

[SwitchA-Ethernet0/2]port hybrid vlan 10 100 untagged 7. 配置端

口 E0/3 为 Hybrid 端口，能够接收 VLAN10 和 100 发过来的报文

[SwitchA]interface Ethernet 0/3

[SwitchA-Ethernet0/3]port link-type hybrid

[SwitchA-Ethernet0/3]port hybrid vlan 10 100 untagged

8. 配置端口 G2/1 为Hybrid 端口，能够接收 VLAN10、20 和 30 发过来的报文

[SwitchA]interface GigabitEthernet 2/1

[SwitchA-GigabitEthernet2/1]port link-type hybrid

[SwitchA-GigabitEthernet2/1]port hybrid vlan 10 20 30 untagged

9. 补充说明

对于 Hybrid 端口来说，可以同时属于多个 VLAN。这些 VLAN 分别是该 Hybrid 端口的 PVID，以及手工配置的“untagged”及“tagged”方式的 VLAN。一定要注意对应端口的 VLAN 配置，保证报文能够被端口进行正常的收发处理。此应用在二层网络中，对相同网段的主机进行访问权限的控制。

需求二配置过程

SwitchA 相关配置：

1. 创建（进入） VLAN10，将 E0/1 加入到 VLAN10

[SwitchA]vlan 10

[SwitchA-vlan10]port Ethernet 0/1 2. 创建（进入）VLAN20，将 E0/2 加入到 VLAN20

[SwitchA]vlan 20

[SwitchA-vlan20]port Ethernet 0/2 3. 创建（进入）VLAN30，将 E0/3 加入到 VLAN30

[SwitchA]vlan 30

[SwitchA-vlan30]port Ethernet 0/3

4. 配置端口 E0/1 为Hybrid 端口，能够接收 VLAN30 发过来的报文

[SwitchA]interface Ethernet 0/1

[SwitchA-Ethernet0/1]port link-type hybrid

[SwitchA-Ethernet0/1]port hybrid vlan 30 untagged

5. 配置端口 E0/2 为Hybrid 端口，能够接收 VLAN30 发过来的报文

[SwitchA]interface Ethernet 0/2

[SwitchA-Ethernet0/2]port link-type hybrid

[SwitchA-Ethernet0/2]port hybrid vlan 30 untagged

6. 配置端口 E0/3 为Hybrid 端口，能够接收 VLAN10 和20 发过来的报文

[SwitchA]interface Ethernet 0/3

[SwitchA-Ethernet0/3]port link-type hybrid

[SwitchA-Ethernet0/3]port hybrid vlan 10 20 untagged

7. 配置端口 G2/1 为Hybrid 端口，能够接收并透传 VLAN10 和20 发过来的报文

[SwitchA]interface GigabitEthernet 2/1

[SwitchA-GigabitEthernet2/1]port link-type hybrid

[SwitchA-GigabitEthernet2/1]port hybrid vlan 10 20 tagged

SwitchB 相关配置：

1. 创建（进入） VLAN10，将 E0/1 加入到 VLAN10

[SwitchA]vlan 10

[SwitchA-vlan10]port Ethernet 0/1 2. 创建（进

入）VLAN20，将 E0/2 加入到 VLAN20

[SwitchA]vlan 20

[SwitchA-vlan20]port Ethernet 0/2

3. 配置端口 G1/1 为Hybrid 端口，能够接收并透传 VLAN10 和20 发过来的报文

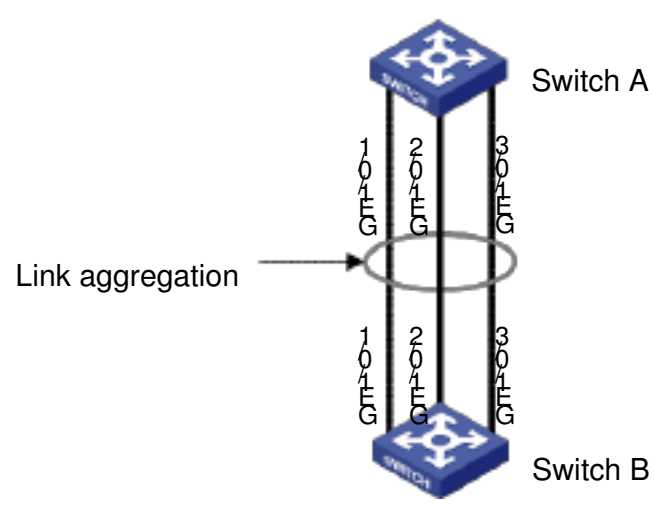
```
[SwitchA]interface GigabitEthernet 1/1

[SwitchA-GigabitEthernet2/1]port  link-type hybrid

[SwitchA-GigabitEthernet2/1]port hybrid vlan 10 20 tagged
```

7. 链路聚合典型配置指导

7.1 链路聚合典型配置指导

链路聚合是将多个物理以太网端口聚合在一起形成一个逻辑上的聚合组，使用链路聚合服务的上层实体把同一聚合组内的多条物理链路视为一条逻辑链路。 链路聚合可以实现出入负荷在聚合组中各个成员端口之间分担，以增加带宽。同时，同聚合组的各个成员端口之间彼此动态备份，提高了连接可靠性。

7.1.1 组网图



链路聚合配置示例图

7.1.2 应用要求

设备 Switch A 用 3 个端口聚合接入设备 Switch B，从而实现出/入负荷在各成员端口中分担。

Switch A 的接入端口为 GigabitEthernet1/0/1～GigabitEthernet1/0/3。

7.1.3 配置过程和解释

说明：

以下只列出对 Switch A 的配置，对 Switch B 也需要作相同的配置，才能实现链路聚合。

配置聚合组，实现端口的负载分担（下面两种方式任选其一采用手工聚合方式

创建手工聚合组 1。

```
<SwitchA> system-view
[SwitchA] link-aggregation group 1 mode manual
```

将以太网端口 GigabitEthernet1/0/1 至 GigabitEthernet1/0/3 加入聚合组 1。

```
[SwitchA] interface GigabitEthernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] port link-aggregation group 1
[SwitchA-GigabitEthernet1/0/1] interface GigabitEthernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-aggregation group 1
[SwitchA-GigabitEthernet1/0/2] interface GigabitEthernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] port link-aggregation group 1
```

采用静态 LACP 聚合方式

创建静态 LACP 聚合组 1。

```
<SwitchA> system-view
[SwitchA] link-aggregation group 1 mode static
```

将以太网端口 GigabitEthernet1/0/1 至 GigabitEthernet1/0/3 加入聚合组 1。

```
[SwitchA] interface GigabitEthernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] port link-aggregation group 1
[SwitchA-GigabitEthernet1/0/1] interface GigabitEthernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-aggregation group 1
[SwitchA-GigabitEthernet1/0/2] interface GigabitEthernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] port link-aggregation group 1
```

7.1.4 完整配置

采用手工聚合方式：

```
#
 link-aggregation group 1 mode manual
#
interface GigabitEthernet1/0/1
 port link-aggregation group 1
#
interface GigabitEthernet1/0/2
 port link-aggregation group 1
#
interface GigabitEthernet1/0/3
 port link-aggregation group 1
#
```

采用静态 LACP 聚合方式：

```
#
 link-aggregation group 1 mode static
interface GigabitEthernet1/0/1
 port link-aggregation group 1
#
interface GigabitEthernet1/0/2
 port link-aggregation group 1
#
interface GigabitEthernet1/0/3
 port link-aggregation group 1
#
```

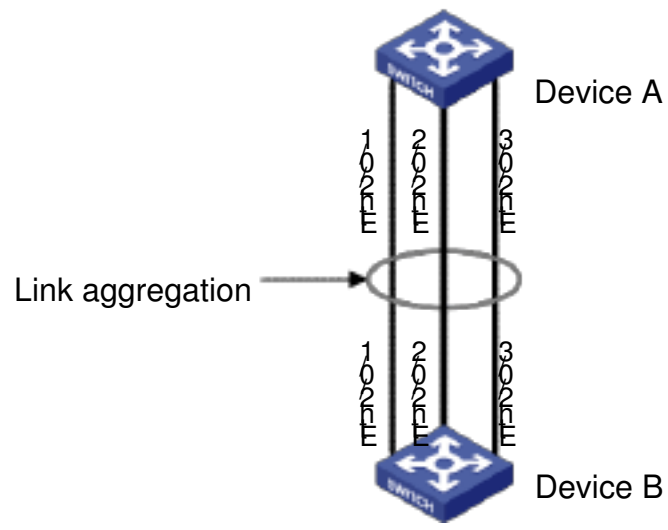
7.1.5 配置注意事项

不同平台软件对静态聚合方式的实现不同，所以不同平台软件的产品采用静态聚合方式对接时，容易产生问题。有关平台软件的版本信息可以通过 display version命令查看。

配置了 RRPP 的端口、配置了静态 MAC 地址或者黑洞 MAC 地址的端口、使能 Voice VLAN的端口以及使能 802.1x 的端口不能加入聚合组。

7.2 链路聚合典型配置指导

7.2.1 组网图



链路聚合配置示例图

7.2.2 应用要求

设备 Device A 用 3 个端口聚合接入设备 Device B，从而实现出/入负荷在各成员端口中分担。

Device A 的接入端口为 Ethernet2/0/1～Ethernet2/0/3。

7.2.3 配置过程和解释

说明：

以下只列出对 Device A的配置，对 Device B也需要作相同的配置，才能实现链路聚合。

采用静态聚合模式

创建二层聚合端口 1。

```
<DeviceA> system-view
[DeviceA] interface bridge-aggregation 1
[DeviceA-Bridge-Aggregation1] quit
```

将以太网端口 Ethernet2/0/1 至 Ethernet2/0/3 加入聚合组 1。

```
[DeviceA] interface ethernet 2/0/1
[DeviceA-Ethernet2/0/1] port link-aggregation group 1
[DeviceA-Ethernet2/0/1] interface ethernet 2/0/2
[DeviceA-Ethernet2/0/2] port link-aggregation group 1
[DeviceA-Ethernet2/0/2] interface ethernet 2/0/3
[DeviceA-Ethernet2/0/3] port link-aggregation group 1
```

采用动态聚合模式

创建二层聚合端口 1，并配置成动态聚合模式。

```
<DeviceA> system-view
[DeviceA] interface bridge-aggregation 1
```

```
[DeviceA-Bridge-Aggregation1] link-aggregation mode dynamic
[DeviceA-Bridge-Aggregation1] quit
```

将以太网端口 Ethernet2/0/1 至 Ethernet2/0/3 加入聚合组 1。

```
[DeviceA] interface ethernet 2/0/1
[DeviceA-Ethernet2/0/1] port link-aggregation group 1
[DeviceA-Ethernet2/0/1] interface ethernet 2/0/2
[DeviceA-Ethernet2/0/2] port link-aggregation group 1
[DeviceA-Ethernet2/0/2] interface ethernet 2/0/3
[DeviceA-Ethernet2/0/3] port link-aggregation group 1
```

7.2.4 配置注意事项

Bridge-Aggregation 视图下配置应与聚合组中端口下配置一致。

8、端口镜像典型配置指导

8.1 本地端口镜像典型配置指导

本地端口镜像是指将设备的一个或多个端口（源端口）的报文复制到本设备的一个监视端口（目的端口），用于报文的监视和分析。其中，源端口和目的端口必须在同一台设备上。

8.1.1 组网图

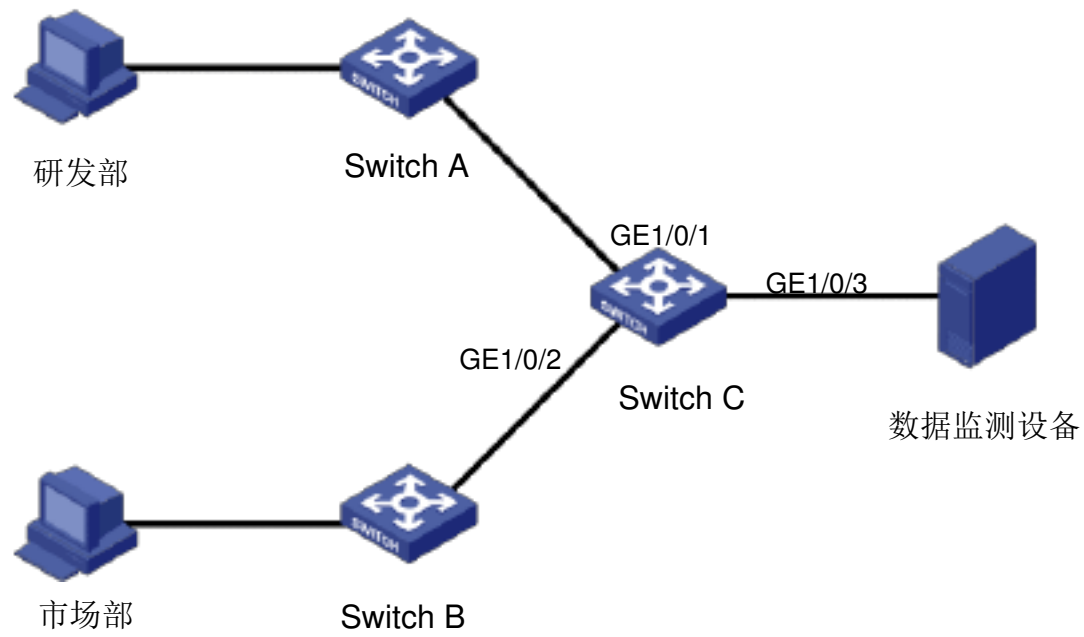


图 1-1 配置本地端口镜像组网图

8.1.2 应用要求

某公司内部通过交换机（以 S5500-EI 系列以太网交换机为例，如配置基本 IPv4 ACL组网图中 Switch C）实现各部门之间的互连，网络环境描述如下：研发部通过端口 GigabitEthernet 1/0/1 接入 Switch C；市场部通过端口 GigabitEthernet 1/0/2 接入 Switch C；数据监测设备连接在 Switch C 的 GigabitEthernet 1/0/3端口上。

网络管理员希望通过数据监测设备对研发部和市场部收发的报文进行监控使用本地端口镜像功能实现该需求，在Switch C上进行如下配置：

端口 GigabitEthernet 1/0/1和 GigabitEthernet 1/0/2为镜像源端口；

连接数据监测设备的端口GigabitEthernet 1/0/3为镜像目的端口。

8.1.3 配置过程和解释

创建本地镜像组。

```
<SwitchC> system-view
[SwitchC] mirroring-group 1 local
```

为本地镜像组配置源端口和目的端口。

```
[SwitchC]  mirroring-group  1  mirroring-port  GigabitEthernet  1/0/1
GigabitEthernet 1/0/2 both
[SwitchC] mirroring-group 1 monitor-port GigabitEthernet 1/0/3
```

显示所有镜像组的配置信息。

```
[SwitchC] display mirroring-group all
mirroring-group 1:
   type: local
   status: active
   mirroring port:
      GigabitEthernet1/0/1 both
      GigabitEthernet1/0/2 both
   monitor port: GigabitEthernet1/0/3
```

8.1.4 完整配置

```
#
 mirroring-group 1 local
#
 interface GigabitEthernet1/0/1
  mirroring-group 1 mirroring-port both
 #
 interface GigabitEthernet1/0/2
  mirroring-group 1 mirroring-port both
 #
 interface GigabitEthernet1/0/3
  mirroring-group 1 monitor-port
 #
```

8.1.5 配置注意事项

需要注意的是：

镜像后的报文是否带有 VLAN Tag，不同的产品有所不同，请以各产品的实际情况为准。

配置本地端口镜像时，必须预先创建本地镜像组。本地镜像组需要配置源端口、目的端口才能生效。其中源端口和目的端口不能是现有镜像组的成员端口，并且一个镜像组只能配置一个目的端口。

请用户不要在目的端口上开启STP、RSTP或MSTP，否则可能会影响镜像功能的正常使用。

目的端口不用做其他用途，仅用于端口镜像。

S3610&S5510 系列以太网交换机只支持配置 1 个本地镜像组，S5500-SI/S5500-EI/S7500E系列以太网交换机均支持4个本地镜像组。

在S3610&S5510系列以太网交换机上配置本地端口镜像时，目的端口不能为聚合组成员端口。

8.2 远程端口镜像典型配置指导（方式一）

远程端口镜像（方式一）通过远程源镜像组和远程目的镜像组互相配合的方式实现远程端口镜像（方式一）的应用如远程端口镜像（方式一）应用示意图所示。

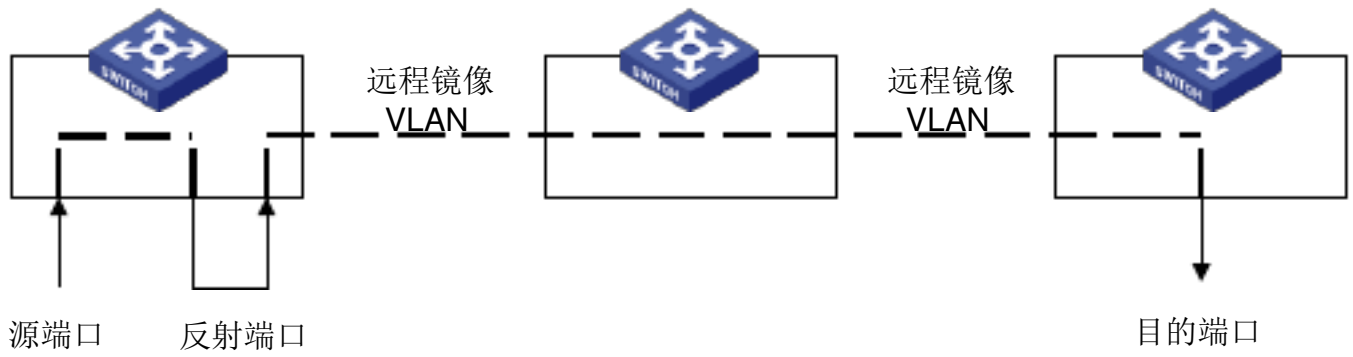


图 1-2 远程端口镜像（方式一）应用示意图

图中各设备的作用如下： 源设备：源端口所在的设备，用户需要在源设备上创建远程源镜像组。本设备

负责将源端口的报文复制一份，然后通过反射端口将报文在远程镜像

VLAN 中进行广播，传输给中间设备或目的设备。中间设备：网络中处于源设备和目的设备之间的设备。本设备负责将镜像报文

传输给下一个中间设备或目的设备如果源设备与目的设备直接相连则 不存在中间设备。用户需要确保远程镜像 VLAN 内源设备到目的设备的二层互通性。

目的设备：远程镜像目的端口所在的设备，用户需要在目的设备上创建远程目的镜像组。目的设备收到报文后，比较报文的 VLAN ID 和远程目的镜像组的远程镜像VLAN是否相同，如果相同，则将该报文通过镜像目的端口转发给监控设备。

8.2.1 组网图

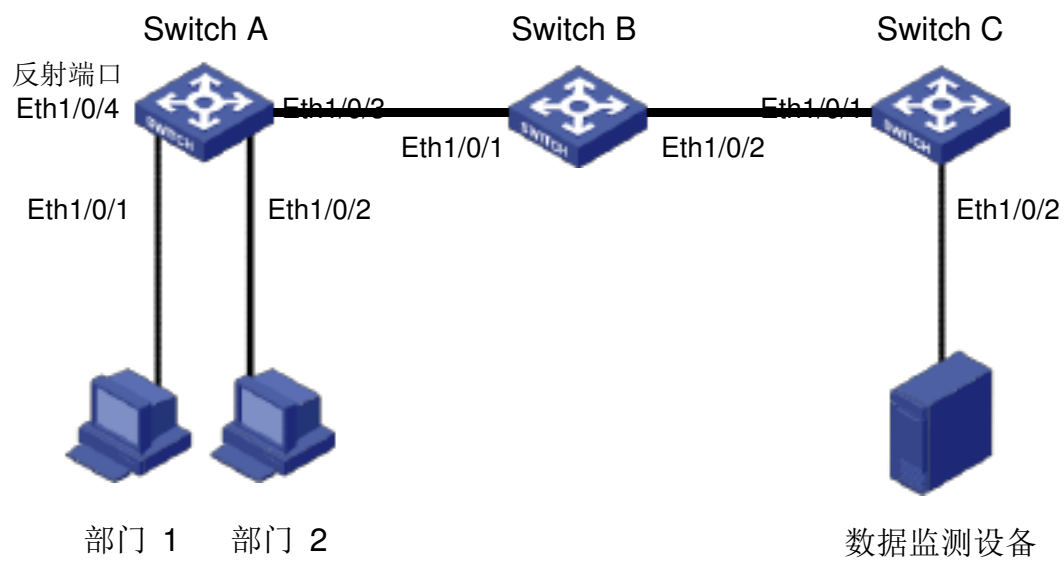


图 1-3 配置远程端口镜像（方式一）组网图

8.2.2 应用要求

某公司内部通过交换机（以 S3610 系列以太网交换机为例，如配置远程端口镜像（方式一）组网图中 Switch A、Switch B 和 Switch C）实现各部门之间的互连，网络环境描述如下：

部门 1 通过端口 Ethernet 1/0/1 接入 Switch A；

部门 2 通过端口 Ethernet 1/0/2 接入 Switch A；

Switch A 的端口 Ethernet 1/0/3 和 Switch B 的端口 Ethernet 1/0/1 相连；

Switch B 的端口 Ethernet 1/0/2 和 Switch C 的端口 Ethernet 1/0/1 相连；

数据监测设备连接在 Switch C 的 Ethernet 1/0/2 端口上。

网络管理员希望通过数据监测设备对部门 1 和部门 2 发送的报文进行监控。 使用远程端口镜像功能实现该需求，进行如下配置：

Switch A 充当源设备，Switch B 充当中间设备，Switch C 充当目的设备；

在 Switch A 上配置远程源镜像组，定义 VLAN 2 为远程镜像 VLAN，端口 Ethernet 1/0/1 和 Ethernet 1/0/2 为镜像源端口，端口 Ethernet 1/0/4 为反射端口；

配置 Switch A 的端口 Ethernet 1/0/3、Switch B 的端口 Ethernet 1/0/1 和 Ethernet 1/0/2、Switch C 的端口 Ethernet 1/0/1 的端口类型为 Trunk 端口，并且都允许 VLAN 2 的报文通过；

在 Switch C 上配置远程目的镜像组，定义 VLAN 2 为远程镜像 VLAN，连接数据监测设备的端口 Ethernet 1/0/2 为镜像目的端口。

8.2.3 配置过程和解释

(2) 配置 Switch A（源设备）

创建远程源镜像组。

```
<SwitchA> system-view
[SwitchA] mirroring-group 1 remote-source
```

创建 VLAN 2。

```
[SwitchA] vlan 2
[SwitchA-vlan2] quit
```

为远程源镜像组配置远程镜像 VLAN、源端口和反射端口。

```
[SwitchA] mirroring-group 1 remote-probe vlan 2
[SwitchA] mirroring-group 1 mirroring-port Ethernet 1/0/1 Ethernet 1/0/2
inbound
[SwitchA] mirroring-group 1 reflector-port Ethernet 1/0/4
```

配置端口 Ethernet 1/0/3的端口类型为 Trunk 端口，允许 VLAN 2 的报文通过。

```
[SwitchA] interface Ethernet 1/0/3
[SwitchA-Ethernet1/0/3] port link-type trunk
[SwitchA-Ethernet1/0/3] port trunk permit vlan 2
```

(3) 配置 Switch B（中间设备）

配置端口 Ethernet 1/0/1的端口类型为 Trunk 端口，允许 VLAN 2 的报文通过。

```
<SwitchB> system-view
[SwitchB] interface Ethernet 1/0/1
[SwitchB-Ethernet1/0/1] port link-type trunk
[SwitchB-Ethernet1/0/1] port trunk permit vlan 2
[SwitchB-Ethernet1/0/1] quit
```

配置端口 Ethernet 1/0/2的端口类型为 Trunk 端口，允许 VLAN 2 的报文通过。

```
[SwitchB] interface Ethernet 1/0/2
[SwitchB-Ethernet1/0/2] port link-type trunk
[SwitchB-Ethernet1/0/2] port trunk permit vlan 2
```

(4) 配置 Switch C（目的设备）

配置端口 Ethernet 1/0/1的端口类型为 Trunk 端口，允许 VLAN 2 的报文通过。

```
<SwitchC> system-view
[SwitchC] interface Ethernet 1/0/1
[SwitchC-Ethernet1/0/1] port link-type trunk
[SwitchC-Ethernet1/0/1] port trunk permit vlan 2
[SwitchC-Ethernet1/0/1] quit
```

创建远程目的镜像组。

```
[SwitchC] mirroring-group 1 remote-destination
```

创建 VLAN 2。

```
[SwitchC] vlan 2
[SwitchC-vlan2] quit
```

为远程目的镜像组配置远程镜像 VLAN 和目的端口。

```
[SwitchC] mirroring-group 1 remote-probe vlan 2
[SwitchC] mirroring-group 1 monitor-port Ethernet 1/0/2
[SwitchC] interface Ethernet 1/0/2
[SwitchC-Ethernet1/0/2] port access vlan 2
```

8.2.4 完整配置

Switch A 上的完整配置：

```
#
 mirroring-group 1 remote-source
 mirroring-group 1 remote-probe vlan 2
#
 vlan 2
#
interface Ethernet1/0/1
 mirroring-group 1 mirroring-port inbound
#
interface Ethernet1/0/2
 mirroring-group 1 mirroring-port inbound
#
interface Ethernet1/0/3
 port link-type trunk
  port trunk permit vlan 1 to 2
 #
 interface Ethernet1/0/4
  mirroring-group 1 reflector-port
 #
```

Switch B 上的完整配置：

```
#
interface Ethernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 to 2
```

```
#
interface Ethernet1/0/2
 port link-type trunk
  port trunk permit vlan 1 to 2
 #
```

Switch C上的完整配置：

```
#
 mirroring-group 1 remote-destination
 mirroring-group 1 remote-probe vlan 2
#
 vlan 2
#
 interface Ethernet1/0/1
 port link-type trunk
  port trunk permit vlan 1 to 2
#
interface Ethernet1/0/2
 port access vlan 2
  mirroring-group 1 monitor-port
 #
```

8.2.5 配置注意事项

配置远程端口镜像（方式一）的源设备时需要注意： 在源设备上通过配置远程源镜像组实现远程镜像功能，S3610&S5510 系列以

太网交换机只支持配置1 个远程源镜像组。 远程源镜像组的所有端口都属于同一台设备，一个远程源镜像组只能配置一个

反射端口。 反射端口不能是现有镜像组的成员端口、聚合组成员端口，不能配置 QinQ 功

能。反射口必须为Access 端口且属于缺省 VLAN。 端口的双工模式、端口速率、MDI 属性取值均为缺省值时，才能将端口配置为

反射端口；将某个端口配置为反射端口后，不能再修改此端口双工模式端口速率、MDI 属性的取值，即这些属性只能为缺省值。

请用户不要在反射端口连接网线，不要在反射端口上配置下列功能： STP、RSTP、MSTP、802.1x、IGMP Snooping、静态 ARP 和 MAC 地址学习功能，否则可能会影响镜像功能的正常使用。

配置远程镜像 VLAN 时，要求该VLAN 为静态 VLAN 并预先创建。被配置成远程镜像 VLAN 后，该 VLAN 不能直接删除，必须先删除远程镜像 VLAN 的配置才能够删除这个 VLAN。如果镜像组生效后，远程镜像 VLAN 被取消，那么该镜像组将失效。

远程镜像VLAN不用做其他用途，仅用于远程镜像。 一个远程镜像 VLAN 只能被一个远程源镜像组使用。

配置远程端口镜像（方式一）的目的设备时需要注意： 在目的设备上通过配置远程目的镜像组实现远程镜像功能。目的端口不能是现有镜像组的成员端口。

请用户不要在目的端口上开启 STP、RSTP 或 MSTP，否则可能会影响镜像功能的正常使用。

目的端口不用做其他用途，仅用于端口镜像。

配置远程镜像 VLAN 时，要求该VLAN 为静态 VLAN 并预先创建。被配置成远程镜像 VLAN 后，该 VLAN 不能直接删除，必须先删除远程镜像 VLAN

的配置才能够删除这个VLAN。如果镜像组生效后，远程镜像VLAN被取消，那么该镜像组将失效。

一个远程镜像VLAN只能被一个远程目的镜像组使用。 远程镜像VLAN不用做其他用途，仅用于远程镜像。

8.3 远程端口镜像典型配置指导（方式二）

远程端口镜像（方式二）通过远程源镜像组和远程目的镜像组互相配合的方式实现。

远程端口镜像（方式二）的应用如远程端口镜像（方式二）应用示意图所示。

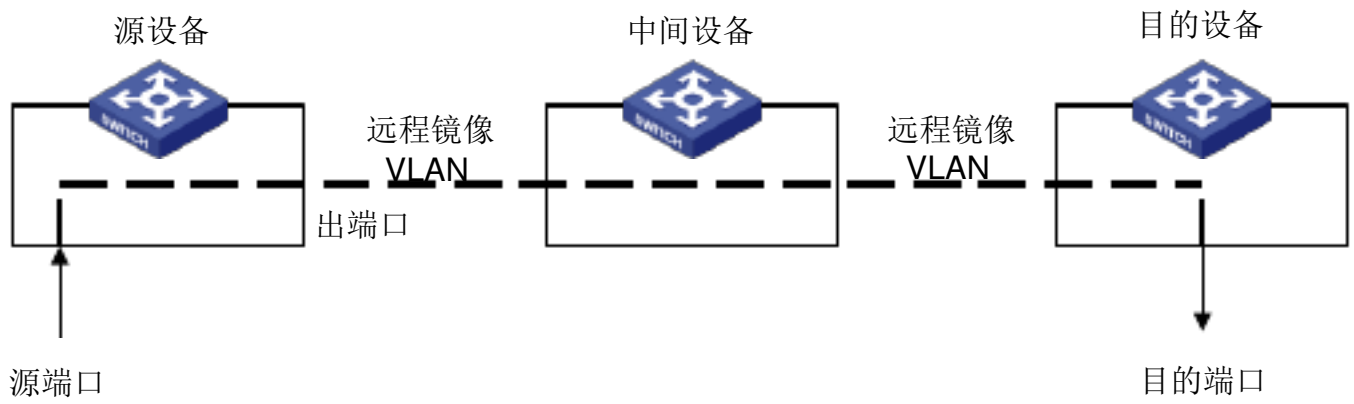


图 1-4 远程端口镜像（方式二）应用示意图

图中各设备的作用如下： 源设备：源端口所在的设备，用户需要在源设备上创建远程源镜像组。本设备

负责将源端口的报文复制一份然后通过出端口将报文在远程镜像 VLAN 中进行广播，传输给中间设备或目的设备。 中间设备：网络中处于源设备和目的设备之间的设备。本设备负责将镜像报文

传输给下一个中间设备或目的设备如果源设备与目的设备直接相连则 不存在中间设备。用户需要确保远程镜像 VLAN 内源设备到目的设备的二层互通性。

目的设备：远程镜像目的端口所在的设备，用户需要在目的设备上创建远程目的镜像组。目的设备收到报文后，比较报文的 VLAN ID 和远程目的镜像组的远程镜像VLAN是否相同，如果相同，则将该报文通过镜像目的端口转发给监控设备。

8.3.1 组网图

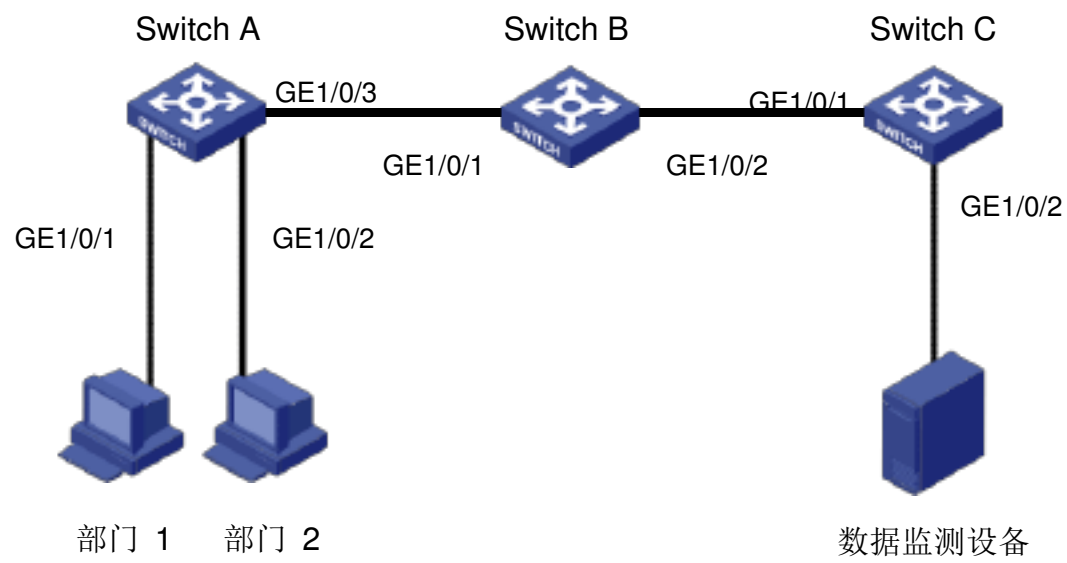


图 1-5 配置远程端口镜像（方式二）组网图

8.3.2 应用要求

某公司内部通过交换机以 S5500-EI 系列以太网交换机为例如配置远程端口镜像方式二）组网图中 Switch A、Switch B 和 Switch C）实现各部门之间的互连，网络环境描述如下：

部门 1 通过端口 GigabitEthernet 1/0/1 接入 Switch A；

部门 2 通过端口 GigabitEthernet 1/0/2 接入 Switch A；

Switch A 的端口 GigabitEthernet 1/0/3 和 Switch B 的端口 GigabitEthernet 1/0/1 相连；

Switch B 的端口 GigabitEthernet 1/0/2 和 Switch C 的端口 GigabitEthernet 1/0/1 相连；

数据监测设备连接在 Switch C 的端口 GigabitEthernet 1/0/2 上。 网络管理员希望通过数据监测设备对部门 1 和部门 2 发送的报文进行监控。 使用远程端口镜像功能实现该需求，进行如下配置：

Switch A 充当源设备，Switch B 充当中间设备，Switch C 充当目的设备；

在 Switch A 上配置远程源镜像组，定义 VLAN 2 为远程镜像 VLAN，端口 GigabitEthernet 1/0/1 和 GigabitEthernet 1/0/2 为镜像源端口，端口 GigabitEthernet 1/0/3为出端口；

配置 Switch A 的端口 GigabitEthernet 1/0/3、Switch B 的端口 GigabitEthernet 1/0/1 和 GigabitEthernet 1/0/2、Switch C 的端口 GigabitEthernet 1/0/1 的端口类型为 Trunk 端口，并且都允许 VLAN 2 的报文通过；

在 Switch C 上配置远程目的镜像组，定义 VLAN 2 为远程镜像 VLAN，连接数据监测设备的端口 GigabitEthernet 1/0/2为镜像目的端口。

8.3.3 配置过程和解释

(5) 配置 Switch A（源设备）

创建远程源镜像组。

```
<SwitchA> system-view
[SwitchA] mirroring-group 1 remote-source
```

创建 VLAN 2。

```
[SwitchA] vlan 2
[SwitchA-vlan2] quit
```

为远程源镜像组配置远程镜像VLAN、源端口和出端口。

```
[SwitchA] mirroring-group 1 remote-probe vlan 2
[SwitchA]  mirroring-group  1  mirroring-port  GigabitEthernet  1/0/1
GigabitEthernet 1/0/2 inbound
[SwitchA] mirroring-group 1 monitor-egress GigabitEthernet 1/0/3
```

配置端口 GigabitEthernet 1/0/3的端口类型为 Trunk端口，允许 VLAN 2 的报文通过。

```
[SwitchA] interface GigabitEthernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] port link-type trunk
[SwitchA-GigabitEthernet1/0/3] port trunk permit vlan 2
```

(6) 配置 Switch B（中间设备）

配置端口 GigabitEthernet 1/0/1的端口类型为 Trunk端口，允许 VLAN 2 的报文通过。

```
<SwitchB> system-view
[SwitchB] interface GigabitEthernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port link-type trunk
[SwitchB-GigabitEthernet1/0/1] port trunk permit vlan 2
[SwitchB-GigabitEthernet1/0/1] quit
```

配置端口 GigabitEthernet 1/0/2的端口类型为 Trunk端口，允许 VLAN 2 的报文通过。

```
[SwitchB] interface GigabitEthernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] port link-type trunk
[SwitchB-GigabitEthernet1/0/2] port trunk permit vlan 2
```

(7) 配置 Switch C（目的设备）

配置端口 GigabitEthernet 1/0/1的端口类型为 Trunk端口，允许 VLAN 2 的报文通过。

```
<SwitchC> system-view
[SwitchC] interface GigabitEthernet 1/0/1
[SwitchC-GigabitEthernet1/0/1] port link-type trunk
[SwitchC-GigabitEthernet1/0/1] port trunk permit vlan 2
[SwitchC-GigabitEthernet1/0/1] quit
```

创建远程目的镜像组。

```
[SwitchC] mirroring-group 1 remote-destination
```

创建 VLAN 2。

```
[SwitchC] vlan 2
[SwitchC-vlan2] quit
```

为远程目的镜像组配置远程镜像VLAN 和目的端口。

```
[SwitchC] mirroring-group 1 remote-probe vlan 2
[SwitchC] mirroring-group 1 monitor-port GigabitEthernet 1/0/2
[SwitchC] interface GigabitEthernet 1/0/2
[SwitchC-GigabitEthernet1/0/2] port access vlan 2
```

8.3.4 完整配置

Switch A上的完整配置：

```
#
 mirroring-group 1 remote-source
 mirroring-group 1 remote-probe vlan 2
#
 vlan 2
#
 interface GigabitEthernet1/0/1
  mirroring-group 1 mirroring-port inbound
 #
 interface GigabitEthernet1/0/2
  mirroring-group 1 mirroring-port inbound
#
interface GigabitEthernet1/0/3
 port link-type trunk
 port trunk permit vlan 1 to 2
  mirroring-group 1 monitor-egress
 #
```

Switch B上的完整配置：

```
#
interface GigabitEthernet1/0/1
```

```
 port link-type trunk
 port trunk permit vlan 1 to 2
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 to 2
#
```

Switch C上的完整配置：

```
#
 mirroring-group 1 remote-destination
 mirroring-group 1 remote-probe vlan 2
#
 vlan 2
#
 interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 to 2
#
interface GigabitEthernet1/0/2
 port access vlan 2
 mirroring-group 1 monitor-port
#
```

8.3.5 配置注意事项

配置远程端口镜像（方式二）的源设备时需要注意： 在源设备上通过配置远程源镜像组实现远程镜像功能。 远程源镜像组的所有端口都属于同一台设备，一个远程源镜像组只能配置一个

出端口。 出端口不能为现有镜像组的成员端口。

请用户不要在出端口上配置下列功能： STP、RSTP、MSTP、802.1x、IGMP Snooping、QinQ、静态 ARP 和 MAC 地址学习功能，否则可能会影响镜像功能的正常使用。

配置远程镜像 VLAN 时，要求该VLAN 为静态 VLAN 并预先创建。被配置成远程镜像 VLAN 后，该 VLAN 不能直接删除，必须先删除远程镜像 VLAN 的配置才能够删除这个 VLAN。如果镜像组生效后，远程镜像 VLAN 被取消，那么该镜像组将失效。

远程镜像VLAN不用做其他用途，仅用于远程镜像功能。 一个远程镜像VLAN只能被一个远程源镜像组使用。

配置远程端口镜像（方式二）的目的设备时需要注意： 在目的设备上通过配置远程目的镜像组实现远程镜像功能。目的端口不能是现有镜像组的成员端口。

请用户不要在目的端口上使能STP、RSTP 或 MSTP，否则可能会影响镜像功能的正常使用。

目的端口不用做其他用途，仅用于端口镜像。

配置远程镜像 VLAN 时，要求该VLAN 为静态 VLAN 并预先创建。被配置成远程镜像 VLAN 后，该 VLAN 不能直接删除，必须先删除远程镜像 VLAN 的配置才能够删除这个 VLAN。如果镜像组生效后，远程镜像 VLAN 被取消，那么该镜像组将失效。

远程镜像VLAN不用做其他用途，仅用于远程镜像功能。 一个远程镜像VLAN只能被一个远程目的镜像组使用。

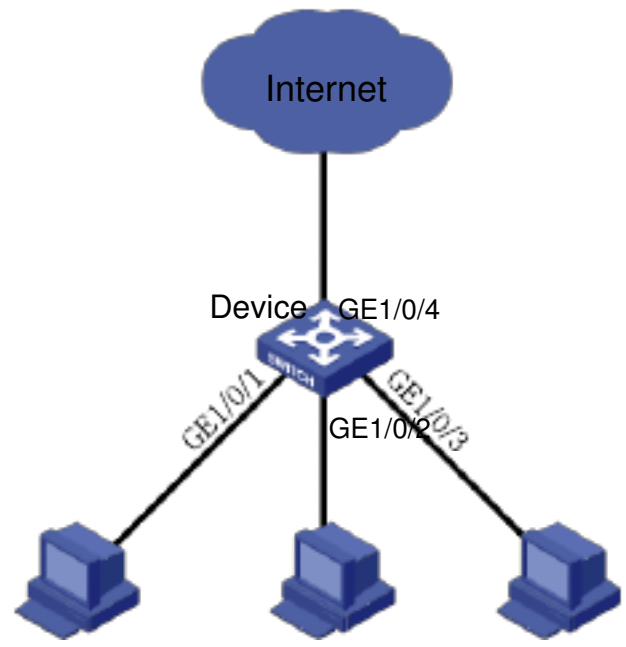
9.端口隔离典型配置指导

9.1 端口隔离概述

为了实现报文之间的二层隔离，可以将不同的端口加入不同的 VLAN，但会浪费有限的 VLAN 资源。采用端口隔离特性，可以实现同一VLAN 内端口之间的隔离。用户只需要将端口加入到隔离组中，就可以实现隔离组内端口之间二层和三层数据的隔离端口隔离功能为用户提供了更安全、更灵活的组网方案。

9.2 端口隔离配置指导（方式一）

9.2.1 组网图



端口隔离典型配置组网图

应用要求小区用户 Host A、Host B、Host C 分别与 Device 的端口 GigabitEthernet1/0/1 GigabitEthernet1/0/2 GigabitEthernet1/0/3 相连；设备通过GigabitEthernet1/0/4端口与外部网络相连；

端口 GigabitEthernet1/0/1、GigabitEthernet1/0/2、GigabitEthernet1/0/3 和 GigabitEthernet1/0/4 属于同一 VLAN；请实现小区用户 Host A、Host B 和 Host C 彼此之间二层/三层报文不能互通，但可以和外部网络通信。

9.2.2 配置过程和解释

将端口 GigabitEthernet1/0/1、GigabitEthernet1/0/2、GigabitEthernet1/0/3 加入隔离组。

```
<Device> system-view
[Device] interface GigabitEthernet1/0/1
[Device-GigabitEthernet1/0/1] port-isolate enable
[Device-GigabitEthernet1/0/1] quit
[Device] interface GigabitEthernet1/0/2
[Device-GigabitEthernet1/0/2] port-isolate enable
[Device-GigabitEthernet1/0/2] quit
[Device] interface GigabitEthernet1/0/3
[Device-GigabitEthernet1/0/3] port-isolate enable
```

显示隔离组中的信息。

```
<Device> display port-isolate group
 Port-isolate group information:
 Uplink port support: NO
 Group ID: 1
    GigabitEthernet1/0/1                    GigabitEthernet1/0/2
GigabitEthernet1/0/3
```

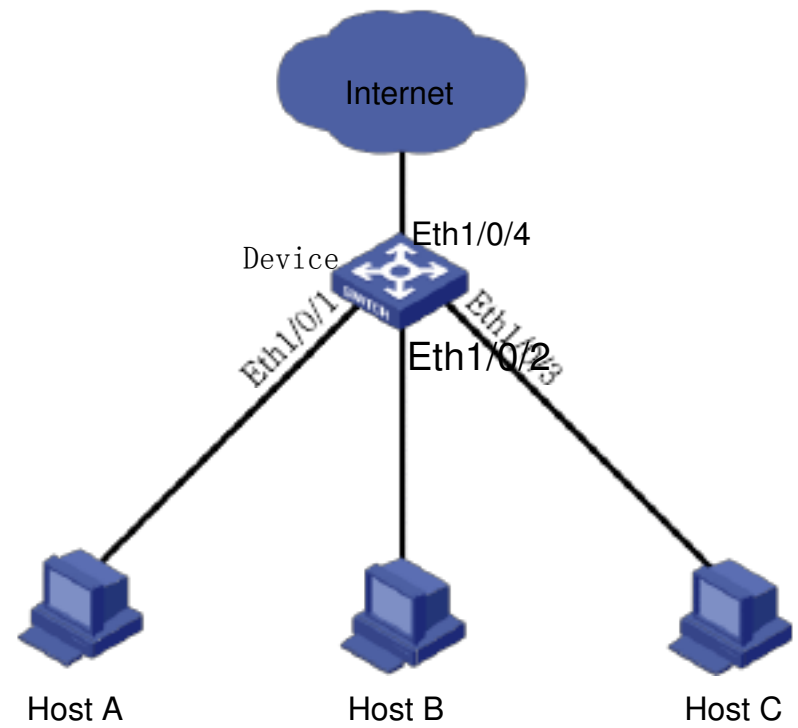
9.2.3 配置注意事项

目前，设备只支持一个隔离组，即由系统自动创建的隔离组 1，用户不可删除 该隔离组或创建其它的隔离组。

隔离组内可以加入的端口数量没有限制。 隔离组内的端口和隔离组外端口二层、三层流量双向互通，隔离组内端口之间不可互通。

9.3 端口隔离配置指导（方式二）

9.3.1 组网图



端口隔离典型配置组网图

小区用户 Host A、Host B、Host C 分别与 Device 的端口 Ethernet1/0/1、 Ethernet1/0/2、 Ethernet1/0/3 相连；

设备通过Ethernet1/0/4端口与外部网络相连；

端口 Ethernet1/0/1、Ethernet1/0/2、Ethernet1/0/3 和 Ethernet1/0/4 属于同一 VLAN；请实现小区用户 Host A、Host B 和 Host C 彼此之间二层报文不能互通，但可以和外部网络通信。

9.3.2 配置过程和解释

将端口 Ethernet1/0/1、Ethernet1/0/2、Ethernet1/0/3 加入隔离组。

```
<Device> system-view
[Device] interface ethernet 1/0/1
[Device-Ethernet1/0/1] port-isolate enable
[Device-Ethernet1/0/1] quit
[Device] interface ethernet 1/0/2
[Device-Ethernet1/0/2] port-isolate enable
[Device-Ethernet1/0/2] quit
[Device] interface ethernet 1/0/3
[Device-Ethernet1/0/3] port-isolate enable
```

配置端口 Ethernet1/0/4 为隔离组的上行端口。

```
[Device-Ethernet1/0/3] quit
[Device] interface ethernet 1/0/4
[Device-Ethernet1/0/4] port-isolate uplink-port
```

显示隔离组中的信息。

```
<Device> display port-isolate group
 Port-isolate group information:
 Uplink port support: YES
 Group ID: 1
 Uplink port: Ethernet1/0/4
    Ethernet1/0/1     Ethernet1/0/2     Ethernet1/0/3
```

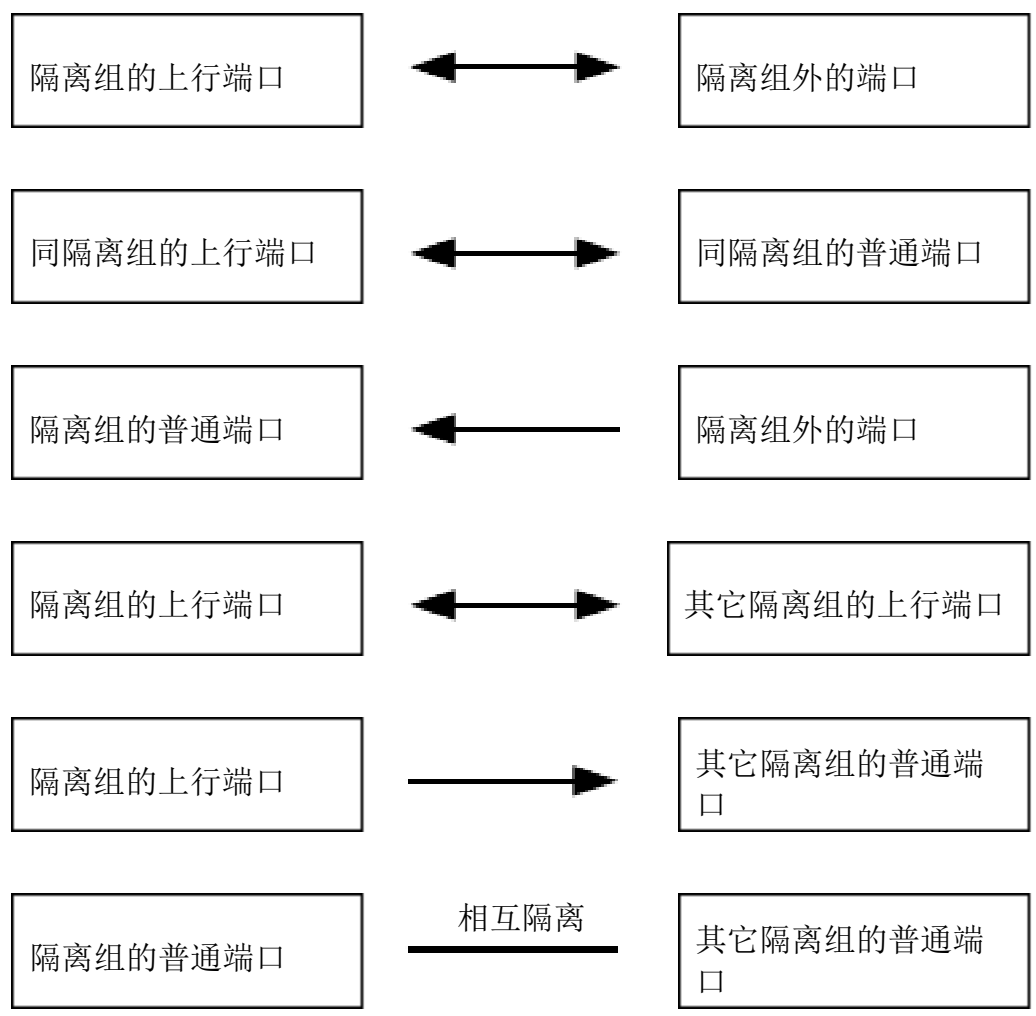
9.3.3 配置注意事项

目前，设备只支持一个隔离组，即由系统自动创建的隔离组 1，用户不可删除该隔离组或创建其它的隔离组。

隔离组内可以加入的端口数量没有限制。

对于属于不同VLAN的端口，只有同一个隔离组的普通端口到上行端口的二层报文可以单向通过，其它情况的端口二层数据是相互隔离的。

对于属于同一VLAN的端口，隔离组内、外端口的二层数据互通的情况，如图所示。图中箭头方向表示报文的发送方向。



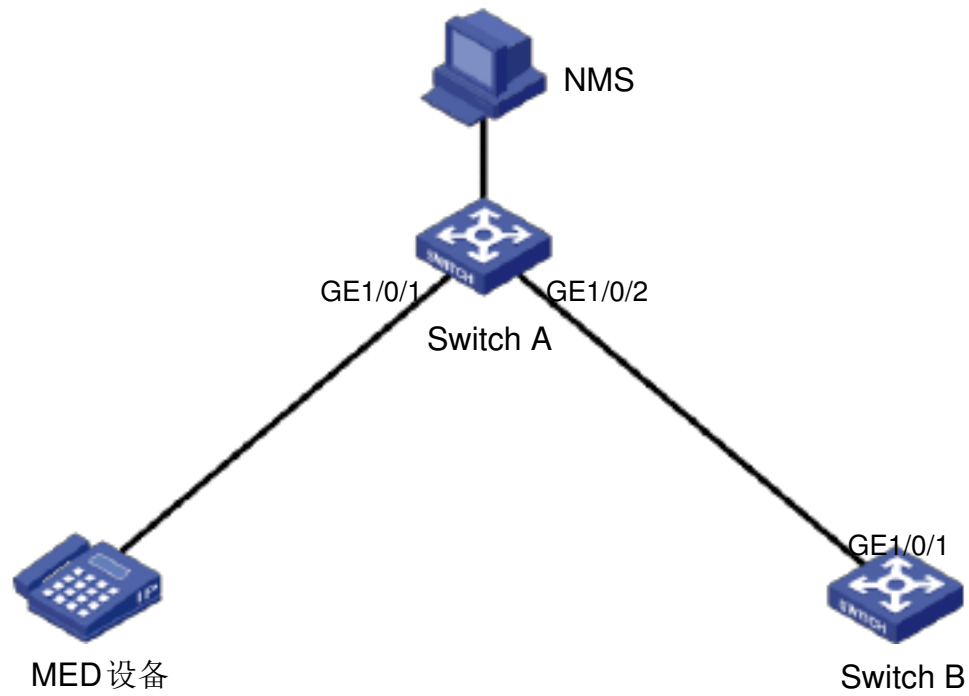
10. LLDP 典型配置指导

10.1 LLDP 简介

LLDP（Link Layer Discovery Protocol，链路层发现协议）是链路层协议，它将本地设备的信息组织成 TLV（Type/Length/Value，类型/长度/值）封装在 LLDPDU（Link Layer Discovery Protocol Data Unit，链路层发现协议数据单元）中发送给直连的邻居，同时也把从邻居接收的 LLDPDU 以标准 MIB（Management Information Base，管理信息库）的形式保存起来。通过LLDP，设备可以保存和管理自己以及直连邻居设备的信息，供网络管理系统查询和判断链路的通信状况。

10.2 LLDP 典型配置指导

10.2.1 组网图



LLDP 典型配置举例图

10.2.2 应用要求

NMS 通过以太网与 Switch A 相连，Switch A 分别通过 GigabitEthernet1/0/1、GigabitEthernet1/0/2 与 MED 设备、Switch B 相连。

在 Switch A 和 Switch B 的相应接口配置 LLDP 功能，使得 NMS 可以对 Switch A 链路的通信情况进行判断。

10.2.3 配置过程和解释

配置 Switch A

进入系统视图。

```
<SwitchA> system-view
```

全局使能 LLDP 功能。

```
[SwitchA] lldp enable
```

分别在 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 接口使能 LLDP 功能并配置其工作模式为 rx。

```
[SwitchA] interface GigabitEthernet1/0/1
[SwitchA-GigabitEthernet1/0/1] lldp enable
[SwitchA-GigabitEthernet1/0/1] lldp admin-status rx
[SwitchA-GigabitEthernet1/0/1] quit
[SwitchA] interface GigabitEthernet1/0/2
[SwitchA-GigabitEthernet1/0/2] lldp enable
[SwitchA-GigabitEthernet1/0/2] lldp admin-status rx
[SwitchA-GigabitEthernet1/0/2] quit
```

配置 Switch B

进入系统视图。

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

全局使能 LLDP 功能。

```
[SwitchB] lldp enable
```

在 GigabitEthernet1/0/1 使能 LLDP 功能并配置其工作模式为 tx。

```
[SwitchB] interface GigabitEthernet1/0/1
```

```
[SwitchB-GigabitEthernet1/0/1] lldp enable
[SwitchB-GigabitEthernet1/0/1] lldp admin-status tx
```

验证配置结果

在 Switch A 上显示全局和接口的状态信息。

```
<SwitchA> display lldp status
Global status of LLDP : Enable
The current number of neighbors : 2
Neighbor information last changed time : 0 days, 0 hours, 4 minutes, 40
seconds
Transmit interval             : 30s
Hold multiplier               : 4
Reinit delay                  : 2s
Transmit delay                : 2s
Trap interval                 : 5s
Fast start times              : 3

Port 0 [GigabitEthernet1/0/1] :
Port status of LLDP           : Enable
Admin status                  : Rx_Only
Trap flag                     : No
Roll time                     : 0s

Number of neighbors           : 1
Number of MED neighbors       : 1
Number of sent optional TLV   : 0
Number of received unknown TLV  : 0

Port 1 [GigabitEthernet1/0/2] :
Port status of LLDP           : Enable
Admin status                  : Rx_Only
Trap flag                     : No
Roll time                     : 0s

Number of neighbors           : 1
Number of MED neighbors       : 0
Number of sent optional TLV   : 0
Number of received unknown TLV  : 3
……（其他端口的显示信息略）
```

缺省情况下，Telent 终端信息中心屏幕开关处于关闭状态。欲在 NMS 端看到 LLDP 状态变化产生的日志信息，需打开屏幕开关。

```
<SwitchA> terminal monitor
```

将 Switch A 和 Switch B 上的链路断掉，Switch A 上会相继输出如下日志信息，Switch B 与此类似（此信息只有在终端屏幕开关打开的情况下才能看到）。

```
%Nov 21 11:38:42:86 2007 H3C IFNET/4/LINK UPDOWN: GigabitEthernet1/0/2:
link status is DOWN
%Nov 21 11:40:26:846 2007 H3C LLDP/2/AGEOUTREM:Port GigabitEthernet1/0/2
(IfIndex 9437201):Neighbor aged out, chassis ID: 000f-e272-8351, port ID:
GigabitEthernet1/0/1.
```

在 Switch A 上显示全局和接口的状态信息。

```
<SwitchA> display lldp status
Global status of LLDP : Enable
The current number of neighbors : 1
Neighbor information last changed time : 0 days, 0 hours, 5 minutes, 20
seconds
Transmit interval             : 30s
Hold multiplier               : 4
Reinit delay                  : 2s
Transmit delay                : 2s
Trap interval                 : 5s
Fast start times              : 3

Port 0 [GigabitEthernet1/0/1] :
Port status of LLDP           : Enable
Admin status                  : Rx_Only
Trap flag                     : No
Roll time                     : 0s
```

```
Number of neighbors             : 1
Number of MED neighbors         : 1
Number of sent optional TLV     : 0
Number of received unknown TLV  : 5

Port 1 [GigabitEthernet1/0/2] :
Port status of LLDP             : Enable
Admin status                    : Rx_Only
Trap flag                       : No
Roll time                       : 0s

Number of neighbors             : 0
Number of MED neighbors         : 0
Number of sent optional TLV     : 0
Number of received unknown TLV  : 0
……（其他端口的显示信息略）
```

10.2.4 完整配置

Switch A 上的配置

```
#
interface GigabitEthernet1/0/1
 lldp admin-status rx
#
interface GigabitEthernet1/0/2
 lldp admin-status rx
```

Switch B 上的配置

```
#
interface GigabitEthernet1/0/1
 lldp admin-status tx
```

10.2.5 配置注意事项

欲在终端屏幕上查看邻居变化产生的日志信息，需保证终端屏幕开关（通过命令 terminal monitor 打开）、日志信息开关（通过命令 terminal logging 打开）以及信息中心（通过命令 info-center enable 打开）处于打开状态。缺省情况下，S5500-EI 系列以太网交换机 telent 终端屏幕开关处于关闭状态,日志信息开关和信息中心都处于开启状态所以举例中仅对屏幕开关进行了配置，其他保持缺省情况即可。详情请参考产品操作手册“信息中心”部分。

11. DHCP 典型配置指导

11.1 DHCP 服务器静态绑定地址典型配置指导

11.1.1 组网图

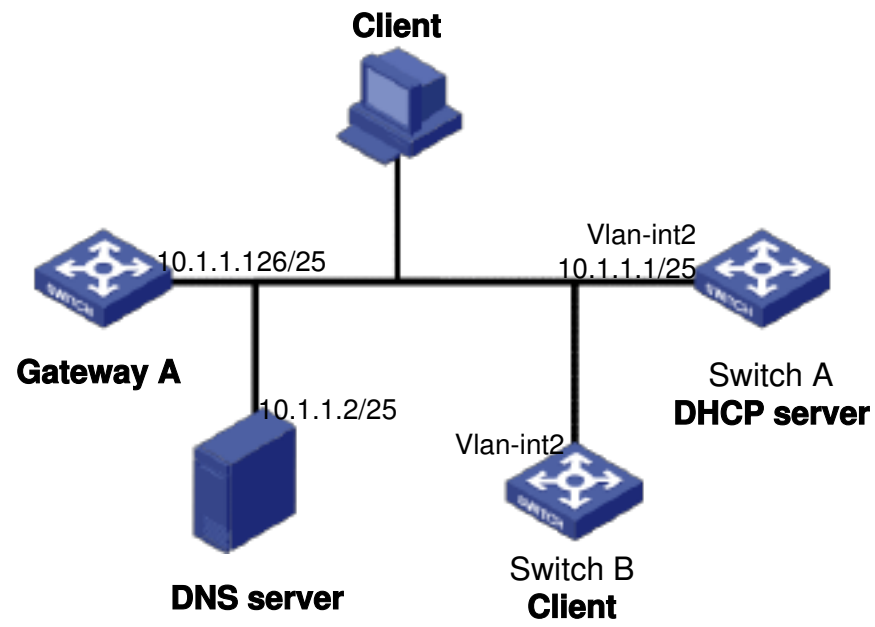


图 1-6 DHCP 服务器静态绑定地址组网图

11.1.2 应用要求

Switch B 作为 DHCP 客户端，从 DHCP 服务器 Switch A 获取静态绑定的 IP 地址、域名服务器、网关地址等信息。

11.1.3 配置过程和解释

配置接口的 IP 地址。

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 10.1.1.1 25
[SwitchA-Vlan-interface2] quit
```

使能 DHCP 服务。

```
[SwitchA] dhcp enable
```

配置 DHCP 地址池 0，采用静态绑定方式分配 IP 地址。

```
[SwitchA] dhcp server ip-pool 0
[SwitchA-dhcp-pool-0] static-bind ip-address 10.1.1.5
[SwitchA-dhcp-pool-0] static-bind mac-address 000f-e200-0002
[SwitchA-dhcp-pool-0] dns-list 10.1.1.2
[SwitchA-dhcp-pool-0] gateway-list 10.1.1.126
[SwitchA-dhcp-pool-0] quit
```

11.1.4 完整配置

```
#
dhcp server ip-pool 0
 static-bind ip-address 10.1.1.5 mask 255.0.0.0
 static-bind mac-address 000f-e200-0002
 gateway-list 10.1.1.126
  dns-list 10.1.1.2
  expired unlimited
 #
 interface Vlan-interface2
```

```
 ip address 10.1.1.1 255.255.255.128
#
 dhcp enable
#
```

11.1.5 配置注意事项

静态绑定的 IP 地址不能是 DHCP 服务器的接口 IP 地址，否则会导致 IP 地址冲突，被绑定的客户端将无法正常获取到IP地址。

目前一个 DHCP 地址池中只能配置一个静态绑定，可以是 IP 地址与 MAC 地址的绑定，也可以是 IP 地址与客户端 ID（用于唯一标识一个客户端的，4～160个字符的字符串）的绑定。

静态绑定的客户端 ID，要与在待绑定客户端通过 **display dhcp client verbose** 命令显示的客户端 ID 一致。否则，客户端无法成功获取 IP 地址。

11.2 DHCP 服务器动态分配地址典型配置指导

11.2.1 组网图

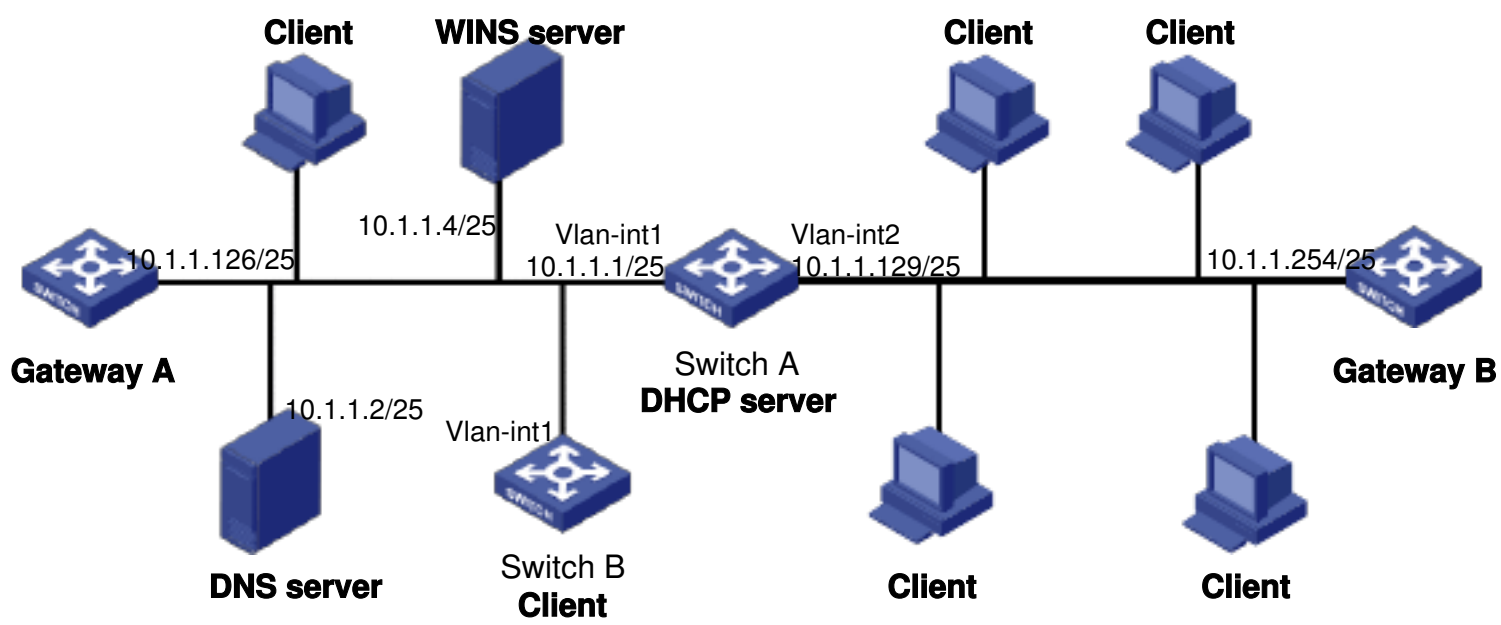


图 1-7 DHCP 服务器动态分配地址组网图

11.2.2 应用要求

作为DHCP服务器的Switch A为网段10.1.1.0/24中的客户端动态分配IP地址，该地址池网段分为两个子网网段：10.1.1.0/25和10.1.1.128/25；

Switch A 的两个 VLAN 接口，VLAN 接口 1 和 VLAN 接口 2 的地址分别为10.1.1.1/25和10.1.1.129/25；

10.1.1.0/25网段内的地址租用期限为10天12小时，域名后缀为aabbcc.com，DNS服务器地址为10.1.1.2/25，WINS服务器地址为10.1.1.4/25，网关的地址为10.1.1.126/25；

10.1.1.128/25 网段内的地址租用期限为 5 天，域名后缀为 aabbcc.com，DNS 服务器地址为 10.1.1.2/25，无 WINS 服务器地址，网关的地址为10.1.1.254/25。

10.1.1.0/25 网段与 10.1.1.128/25 网段的域名后缀、DNS 服务器地址相同，可以只配置 10.1.1.0/24 网段的域名后缀和 DNS 服务器地址，10.1.1.0/25 网段与 10.1.1.128/25 网段继承 10.1.1.0/24 网段的配置。

开启 Switch A 的伪服务器检测功能，方便管理员从系统日志中查找伪服务器信息。

11.2.3 配置过程和解释

使能 DHCP 服务。

```
[SwitchA] dhcp enable
```

配置不参与自动分配的 IP 地址（DNS 服务器、WINS 服务器和网关地址）。

```
[SwitchA] dhcp server forbidden-ip 10.1.1.2
[SwitchA] dhcp server forbidden-ip 10.1.1.4
[SwitchA] dhcp server forbidden-ip 10.1.1.126
[SwitchA] dhcp server forbidden-ip 10.1.1.254
```

配置伪服务器检测功能。

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

配置 DHCP 地址池 0 的共有属性（地址池范围、DNS 服务器地址）。

```
[SwitchA] dhcp server ip-pool 0
[SwitchA-dhcp-pool-0] network 10.1.1.0 mask 255.255.255.0
[SwitchA-dhcp-pool-0] domain-name aabbcc.com
[SwitchA-dhcp-pool-0] dns-list 10.1.1.2
[SwitchA-dhcp-pool-0] quit
```

配置 DHCP 地址池 1 的属性（地址池范围、网关、WINS 服务器地址、地址租用期限）。

```
[SwitchA] dhcp server ip-pool 1
[SwitchA-dhcp-pool-1] network 10.1.1.0 mask 255.255.255.128
[SwitchA-dhcp-pool-1] gateway-list 10.1.1.126
[SwitchA-dhcp-pool-1] expired day 10 hour 12
[SwitchA-dhcp-pool-1] nbns-list 10.1.1.4
[SwitchA-dhcp-pool-1] quit
```

配置 DHCP 地址池 2 的属性（地址池范围、地址租用期限、网关）。

```
[SwitchA] dhcp server ip-pool 2
[SwitchA-dhcp-pool-2] network 10.1.1.128 mask 255.255.255.128
[SwitchA-dhcp-pool-2] expired day 5
[SwitchA-dhcp-pool-2] gateway-list 10.1.1.254
[SwitchA-dhcp-pool-2] quit
```

开启伪服务器检测功能后，Switch A 记录所有 DHCP 服务器的信息，包括合法的 DHCP 服务器。管理员需要从系统日志中查找伪 DHCP 服务器。当 Switch A 发现网络中的其它 DHCP 服务器时，会记录如下所示的日志信息。

```
<SwitchA>
%Apr 30 08:07:51:896 2000 H3C DHCPS/4/DHCPS_LOCAL_SERVER:
 Local DHCP server information: Server IP (detected by DHCP server) =
   10.1.1.5, DHCP server interface = Vlan-interface1
 Source client information: DHCP message type = DHCPREQUEST, DHCP
   client hardware address = 000f-e200-000b
```

11.2.4 完整配置

```
#
dhcp server ip-pool 0
 network 10.1.1.0 mask 255.255.255.0
 dns-list 10.1.1.2
 domain-name aabbcc.com
#
dhcp server ip-pool 1
 network 10.1.1.0 mask 255.255.255.128
 gateway-list 10.1.1.126
 nbns-list 10.1.1.4

 expired day 10 hour 12
#
```

```
dhcp server ip-pool 2
 network 10.1.1.128 mask 255.255.255.128
 gateway-list 10.1.1.254
 expired day 5
#
 dhcp server forbidden-ip 10.1.1.2
 dhcp server forbidden-ip 10.1.1.4
 dhcp server forbidden-ip 10.1.1.126
 dhcp server forbidden-ip 10.1.1.254
 dhcp server detect
#
dhcp enable
#
```

11.2.5 配置注意事项

如果 DHCP 服务器的地址池中没有足够的可供分配的 IP 地址，则服务器无法为客户端分配地址，服务器不会将父地址池中的 IP 地址分配给客户端。故在本例中，建议从 VLAN 接口 1 申请 IP 地址的客户端数目不要超过 122 个；从 VLAN 接口 2 申请 IP 地址的客户端不要超过 124 个。

DHCP 服务器与客户端在同一网段的情况下，如果服务器的接口视图下配置了 dhcp select server global-pool subaddress命令，则当 DHCP 服务器为客户端分配 IP 地址时，从与服务器接口（与客户端相连的接口）的从 IP 地址在同一网段的地址池中选择地址分配给客户端。如果接口有多个从 IP 地址，则从第一个从 IP 地址开始依次匹配。否则，服务器从与接口主 IP 地址在同一网段的地址池中选择地址分配给客户端。

11.3 DHCP 中继典型配置指导

由于在 IP 地址动态获取过程中采用广播方式发送报文，因此 DHCP 只适用于 DHCP 客户端和服务器处于同一个子网内的情况。为进行动态主机配置，需要在所有网段上都设置一个 DHCP 服务器，这显然是很不经济的。

DHCP 中继功能的引入解决了这一难题：子网内的客户端可以通过 DHCP 中继与其他子网的 DHCP 服务器通信，最终获取到 IP 地址。这样，多个网络上的 DHCP 客户端可以使用同一个 DHCP 服务器，既节省了成本，又便于进行集中管理。

11.3.1 组网图

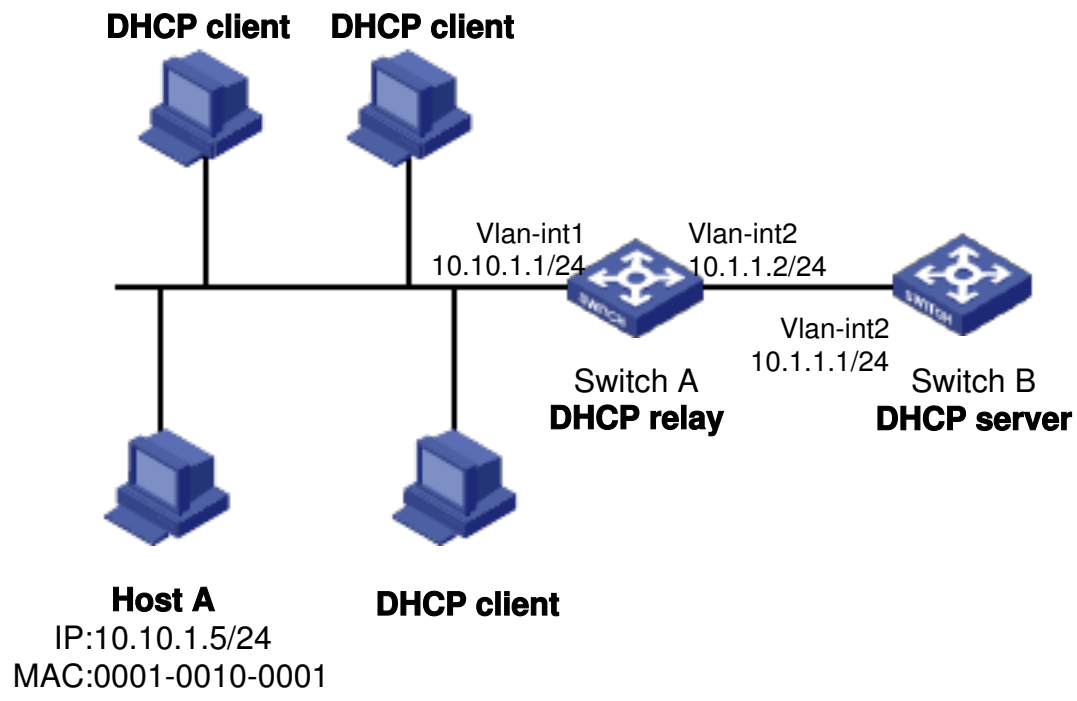


图 1-8 DHCP 中继配置示例图

11.3.2 应用要求

具有 DHCP 中继功能的 Switch A 通过端口（属于VLAN1）连接到 DHCP 客户端所在的网络，交换机 VLAN 接口 1 的 IP 地址为 10.10.1.1/24，VLAN 接口 2 的 IP 地址为 10.1.1.2/24；

DHCP 服务器的 IP 地址为 10.1.1.1/24。

Switch A 作为 DHCP 中继，负责转发 DHCP 报文，使 DHCP 客户端可以从 DHCP 服务器上申请到 10.10.1.0/24 网段的 IP 地址及相关配置信息； 客户端主机除 Host A 使用固定 IP 地址 10.10.1.5/24 外，其余主机通过 DHCP 方式动态获取 IP 地址。

开启 Switch A 上的 DHCP 中继地址表项检查功能，使合法固定 IP 地址用户和通过 DHCP 服务器获取 IP 地址的用户访问网络，防止客户端私自修改 IP 地址访问网络。

11.3.3 配置过程和解释

使能 DHCP 服务。

```
<SwitchA> system-view
[SwitchA] dhcp enable
```

配置 VLAN 接口 1 工作在 DHCP 中继模式。

```
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ip address 10.10.1.1 24
[SwitchA-Vlan-interface1] dhcp select relay
[SwitchA-Vlan-interface1] quit
```

配置 DHCP 服务器的地址，并配置 VLAN 接口 1 对应 DHCP 服务器组 1。

```
[SwitchA] dhcp relay server-group 1 ip 10.1.1.1
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] dhcp relay server-select 1
[SwitchA-Vlan-interface1] quit
```

在 DHCP 中继上为 Host A 配置一条静态用户地址表项，IP 地址为 10.10.1.5/24，MAC 地址为 0001-0010-0001。

```
[SwitchA] dhcp relay security static 10.10.1.5 0001-0010-0001
```

开启 DHCP 中继地址匹配检查功能。

```
[SwitchA] interface Vlan-interface 1
[SwitchA-Vlan-interface1] dhcp relay address-check enable
[SwitchA-Vlan-interface1] quit
```

11.3.4 完整配置

```
#
 dhcp relay server-group 1 ip 10.1.1.1
#
interface Vlan-interface1
 ip address 10.10.1.1 255.255.255.0
 dhcp select relay
 dhcp relay server-select 1
  dhcp relay address-check enable
#
 dhcp enable
#
 dhcp relay security static 10.10.1.5 0001-0010-0001
#
```

11.3.5 配置注意事项

为了使 DHCP 客户端能从 DHCP 服务器获得 IP 地址，还需要在 DHCP 服务器上进行一些配置。关于 DHCP 服务器配置，可以参考 11.2 DHCP 服务器动态分配地址典型配置指导 11.2 DHCP 服务器动态分配地址典型配置指导。

DHCP 中继与 DHCP 服务器之间必须有路由可达。

DHCP 中继的地址匹配检查功能与 DHCP 中继的其他配置无直接关系。即只要执行了 **dhcp relay address-check enable** 命令，地址匹配检查功能就可以生效，不需要配置 DHCP 中继的其他功能，如使能 DHCP、配置接口工作在 DHCP 中继模式等。

11.4 DHCP Snooping 典型配置指导

出于安全性的考虑，网络管理员可能需要记录用户上网时所用的 IP 地址，确认用户从 DHCP Server 获取的 IP 地址和用户主机的 MAC 地址的对应关系。

DHCP Snooping 通过以下两种方法来获得用户从 DHCP Server 获取的 IP 地址和用户 MAC 地址信息：

监听 DHCP-ACK 报文

监听 DHCP-REQUEST 报文

11.4.1 组网图

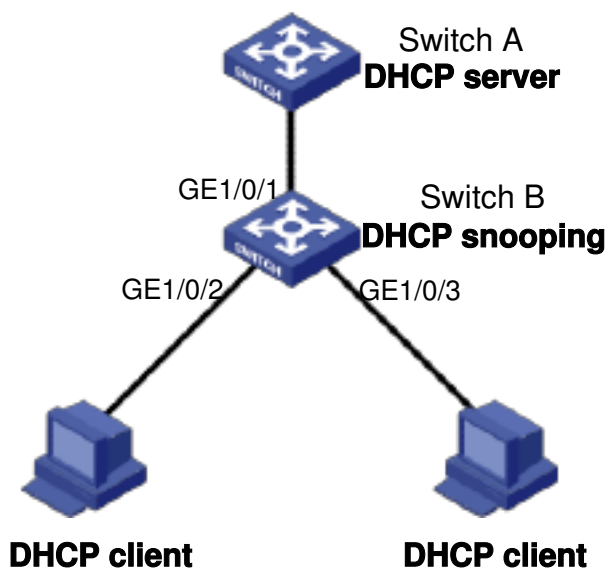


图 1-9 DHCP Snooping 组网配置示意图

11.4.2 应用要求

Switch B 通过以太网端口 GigabitEthernet1/0/1 连接到 DHCP 服务器，通过以太网端口 GigabitEthernet1/0/2、GigabitEthernet1/0/3 连接到 DHCP 客户端。要求：

与 DHCP 服务器相连的端口可以转发 DHCP 服务器的响应报文，而其他端口不转发 DHCP 服务器的响应报文。

记录 DHCP-REQUEST 和信任端口收到的 DHCP-ACK 广播报文中 DHCP 客户端 IP 地址及 MAC 地址的绑定关系。

支持 Option 82 功能。接收到客户端发送的 DHCP 请求报文后，将以 verbose 格式填充的 Option 82 添加到 DHCP 请求报文中，并转发该报文。

需要注意的是：S5500-SI 系列以太网交换机仅支持开启 DHCP Snooping，及配置信任端口功能，不支持在 DHCP Snooping 设备上应用 Option 82 功能。

11.4.3 配置过程和解释

使能 DHCP Snooping 功能。

```
<SwitchB> system-view
[SwitchB] dhcp-snooping
```

配置 GigabitEthernet1/0/1 端口为信任端口。

```
[SwitchB] interface gigabitethernet1/0/1
[SwitchB-GigabitEthernet1/0/1] dhcp-snooping trust
[SwitchB-GigabitEthernet1/0/1] quit
```

在端口 GigabitEthernet1/0/2 上配置 DHCP Snooping 支持 Option 82 功能。

```
[SwitchB] interface gigabitethernet1/0/2
[SwitchB-GigabitEthernet1/0/2] dhcp-snooping information enable
```

在端口 GigabitEthernet1/0/2 上配置 Option 82 以 verbose 格式进行填充。

```
[SwitchB-GigabitEthernet1/0/2] dhcp-snooping information format verbose
node-identifier sysname
[SwitchB-GigabitEthernet1/0/2] quit
```

在端口 GigabitEthernet1/0/3 上配置 DHCP Snooping 支持 Option 82 功能。

```
[SwitchB] interface gigabitethernet1/0/3
[SwitchB-GigabitEthernet1/0/3] dhcp-snooping information enable
```

在端口 GigabitEthernet1/0/3 上配置 Option 82 以 verbose 格式进行填充。

```
[SwitchB-GigabitEthernet1/0/3] dhcp-snooping information format verbose
node-identifier sysname
```

11.4.4 完整配置

```
#
 dhcp-snooping
#
 interface GigabitEthernet1/0/1
  dhcp-snooping trust
#
interface GigabitEthernet1/0/2
 dhcp-snooping information enable
  dhcp-snooping information format verbose node-identifier sysname
#
interface GigabitEthernet1/0/3
 dhcp-snooping information enable
  dhcp-snooping information format verbose node-identifier sysname
 #
```

11.4.5 配置注意事项

设备只有位于 DHCP 客户端与 DHCP 服务器之间，或 DHCP 客户端与 DHCP 中继之间时，DHCP Snooping 功能配置后才能正常工作；设备位于 DHCP 服务器与 DHCP 中继之间时，DHCP Snooping 功能配置后不能正常工作。

使能 DHCP Snooping 功能的设备，不能作为 DHCP 服务器和 DHCP 中继。 建议不要在同一台设备上同时配置 DHCP 客户端/BOOTP 客户端和 DHCP Snooping 功能，否则可能无法生成 DHCP Snooping 表项，DHCP 客户端/BOOTP 客户端也可能申请不到 IP 地址。

为了使 DHCP 客户端能从合法的 DHCP 服务器获取 IP 地址，必须将与合法 DHCP 服务器相连的端口设置为信任端口，设置的信任端口和与 DHCP 客户端相连的端口必须在同一个 VLAN 内。

建议不要在设备上同时配置 DHCP Snooping 功能和灵活 QinQ 功能，否则可能导致 DHCP Snooping 功能无法正常使用。

DHCP Snooping 不支持链路聚合。若以太网端口加入聚合组，则该端口上进行的 DHCP Snooping 配置不会生效；该端口退出聚合组后，之前的 DHCP Snooping 配置才会生效。

11.5 DHCP Snooping 支持 Option 82 典型配置指导

DHCP snooping 设备通过在 DHCP 请求报文中添加 Option 82，将 DHCP 客户端的位置信息告诉给 DHCP 服务器，从而使得 DHCP 服务器能够为主机分配合适的 IP 地址和其他配置信息，并实现对客户端的安全和计费等控制。

11.5.1 组网图

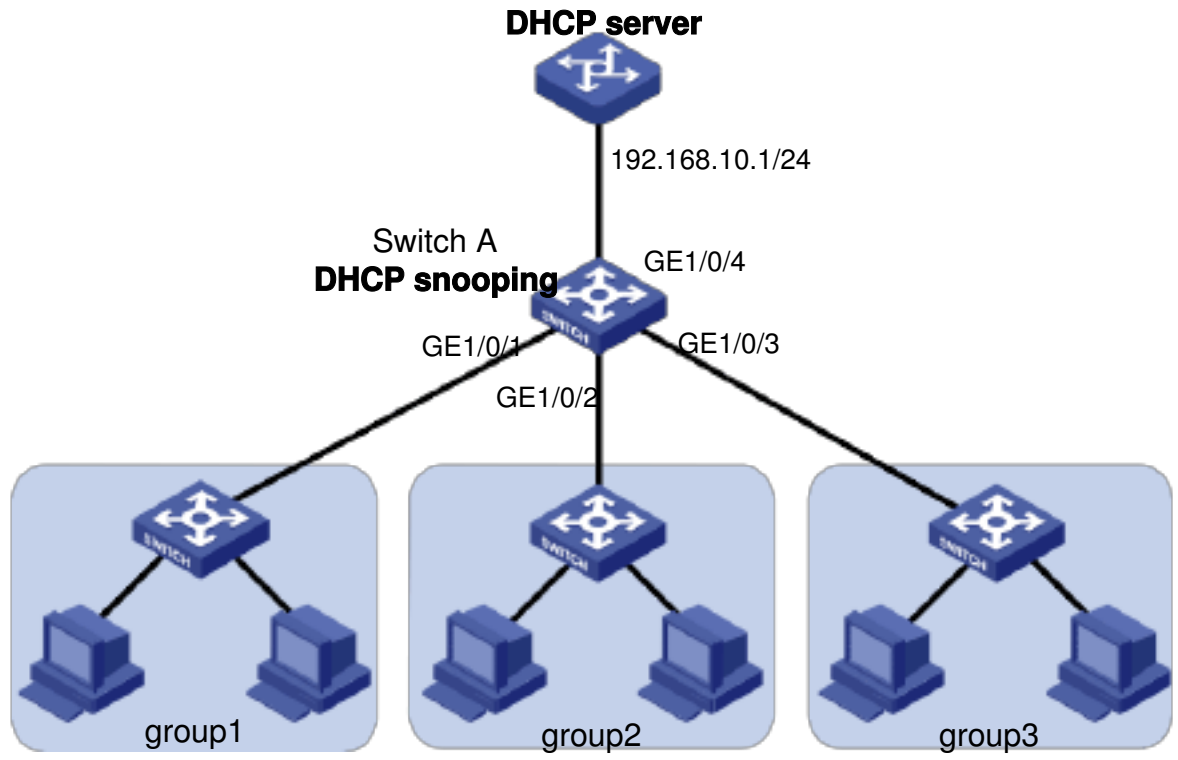


图 1-10 DHCP Snooping 组网配置示意图

11.5.2 应用要求

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

DHCP服务器为办公室设备分配192.168.10.0/24网段的地址，有效期为12小时，并指定DNS和WINS服务器地址分别为192.168.100.2和192.168.100.3。

Switch A上开启DHCP snooping功能，并配置与DHCP服务器相连的端口GigabitEthernet1/0/4为信任端口。

三个小组group1、group2和group3分别通过端口GigabitEthernet1/0/1、GigabitEthernet1/0/2和GigabitEthernet1/0/3接入DHCP snooping设备。

配置DHCP snooping支持Option 82，将用户与DHCP snooping设备相连的端口信息添加到DHCP报文的Option 82字段。

配置DHCP服务器支持Option 82，根据Option 82中携带的小组信息，为group1的用户分配192.168.10.2～192.168.10.25之间的地址；为group2的用户分配192.168.10.100～192.168.10.150之间的地址；为group3的用户分配192.168.10.151～192.168.10.200之间的地址。

11.5.3 配置过程和解释

2. Swich A上的配置

使能DHCP Snooping功能。

```
<SwitchA> system-view
[SwitchA] dhcp-snooping
```

配置GigabitEthernet1/0/4端口为信任端口。

```
[SwitchA] interface gigabitethernet1/0/4
[SwitchA-GigabitEthernet1/0/4] dhcp-snooping trust
[SwitchA-GigabitEthernet1/0/4] quit
```

在端口 GigabitEthernet1/0/1 上配置 DHCP Snooping 支持 Option 82 功能，并配置 Option 82 的填充方式为 Normal。

```
[SwitchA] interface gigabitethernet1/0/1
[SwitchA-GigabitEthernet1/0/1] dhcp-snooping information enable
[SwitchA-GigabitEthernet1/0/1] dhcp-snooping information format normal
[SwitchA-GigabitEthernet1/0/1] quit
```

在端口 GigabitEthernet1/0/2 上配置 DHCP Snooping 支持 Option 82 功能，并配置 Option 82 的填充方式为 Normal。

```
[SwitchA] interface gigabitethernet1/0/2
[SwitchA-GigabitEthernet1/0/2] dhcp-snooping information enable
[SwitchA-GigabitEthernet1/0/2] dhcp-snooping informationformat normal
[SwitchA-GigabitEthernet1/0/2] quit
```

在端口 GigabitEthernet1/0/3 上配置 DHCP Snooping 支持 Option 82 功能，并配置 Option 82 的填充方式为 Normal。

```
[SwitchA] interface gigabitethernet1/0/3
[SwitchA-GigabitEthernet1/0/3] dhcp-snooping information enable
[SwitchA-GigabitEthernet1/0/3] dhcp-snooping information format normal
[SwitchA-GigabitEthernet1/0/3] quit
```

3. DHCP 服务器的配置

说明：

DHCP server 使用的是 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。

配置接口的 IP 地址为 192.168.10.1/24。

```
Server> enable
Server# configure terminal
Server(config)# interface fastethernet 0/0
Server(config-if)# ip address 192.168.10.1 255.255.255.0
Server(config-if)# exit
```

配置 DHCP Server 功能，并配置使用 Option 82 信息进行地址分配。

```
Server(config)# service dhcp
Server(config)# ip dhcp use class
```

为从 DHCP snooping 设备 GigabitEthernet1/0/1 端口接入的 group1 用户建立 DHCP 分类，并配置匹配的 Option 82 信息为 Circuit ID 子选项中的 VLAN 编号与端口编号，无需匹配的内容可以使用通配符“*”代替。

```
Server(config)# ip dhcp class group1
Server(dhcp-class)# relay agent information
Server(dhcp-class-relayinfo)# relay-information hex 10001*
Server(dhcp-class-relayinfo)# exit
```

为从 DHCP snooping 设备 GigabitEthernet1/0/2 端口接入的 group2 用户配置分类和匹配信息，方法与上面命令相似，只是将 Option 82 信息中的端口编号由 1 改为 2。

```
Server(config)# ip dhcp class group2
Server(dhcp-class)# relay agent information
Server(dhcp-class-relayinfo)# relay-information hex 10002*
Server(dhcp-class-relayinfo)# exit
```

为从 DHCP snooping 设备 GigabitEthernet1/0/3 端口接入的 group3 用户配置分类和匹配信息，方法与上面命令相似。

```
Server(config)# ip dhcp class group3
Server(dhcp-class)# relay agent information
Server(dhcp-class-relayinfo)# relay-information hex 10003*
Server(dhcp-class-relayinfo)# exit
```

创建 DHCP 地址池 office，为 DHCP 地址池配置租约期限、网关、DNS 和 WINS 服务器地址。

```
Server(config)# ip dhcp pool office
Server(dhcp-config)# network 192.168.10.0
Server(dhcp-config)# lease 0 12
```

```
Server(dhcp-config)# default-router 192.168.10.1
Server(dhcp-config)# dns-server 192.168.100.2
Server(dhcp-config)# netbios-name-server 192.168.100.3
```

为三个 DHCP 分类分别指定地址范围。

```
Server(dhcp-config)# class group1
Server(dhcp-pool-class)# address range 192.168.10.2 192.168.10.25
Server(dhcp-pool-class)# class group2
Server(dhcp-pool-class)# address range 192.168.10.100 192.168.10.150
Server(dhcp-pool-class)# class group3
Server(dhcp-pool-class)# address range 192.168.10.151 192.168.10.200
```

11.5.4 完整配置

```
#
 dhcp-snooping
#
 interface GigabitEthernet1/0/4
  dhcp-snooping trust
#
interface GigabitEthernet1/0/1
 dhcp-snooping information enable
  dhcp-snooping information format normal
#
interface GigabitEthernet1/0/2
 dhcp-snooping information enable
  dhcp-snooping information format normal
#
interface GigabitEthernet1/0/3
 dhcp-snooping information enable
  dhcp-snooping information format normal
 #
```

11.5.6 配置注意事项

只有使能 DHCP snooping功能之后，DHCP Option 82功能才能生效。

DHCP snooping option 82 功能建议在最靠近 DHCP client 的 snooping 设备上使用，以达到精确定位用户位置的目的。

11.6 自动配置功能典型配置指导

自动配置功能是指在设备空配置启动时自动获取并执行配置文件的功能。自动配置功能简化了网络配置，便于实现对设备的集中管理。

自动配置的基本工作过程为：

(1) 交换机在空配置启动时，系统会自动将处于 up 状态的接口（如缺省 VLAN 对应的接口）配置为通过DHCP 方式获得 IP 地址及后续获取配置文件所需要的信息（例如：配置文件名、TFTP 服务器的域名、TFTP 服务器的 IP 地址、DNS 服务器 IP 地址等信息）。

(2) 如果交换机成功地从 DHCP 服务器获取到 IP 地址及配置文件名等相关信息，则发起TFTP 请求，从指定的TFTP 服务器获取配置文件。如果设备没有获取到相关信息，则在空配置文件的情况下正常启动。

11.6.1 组网图

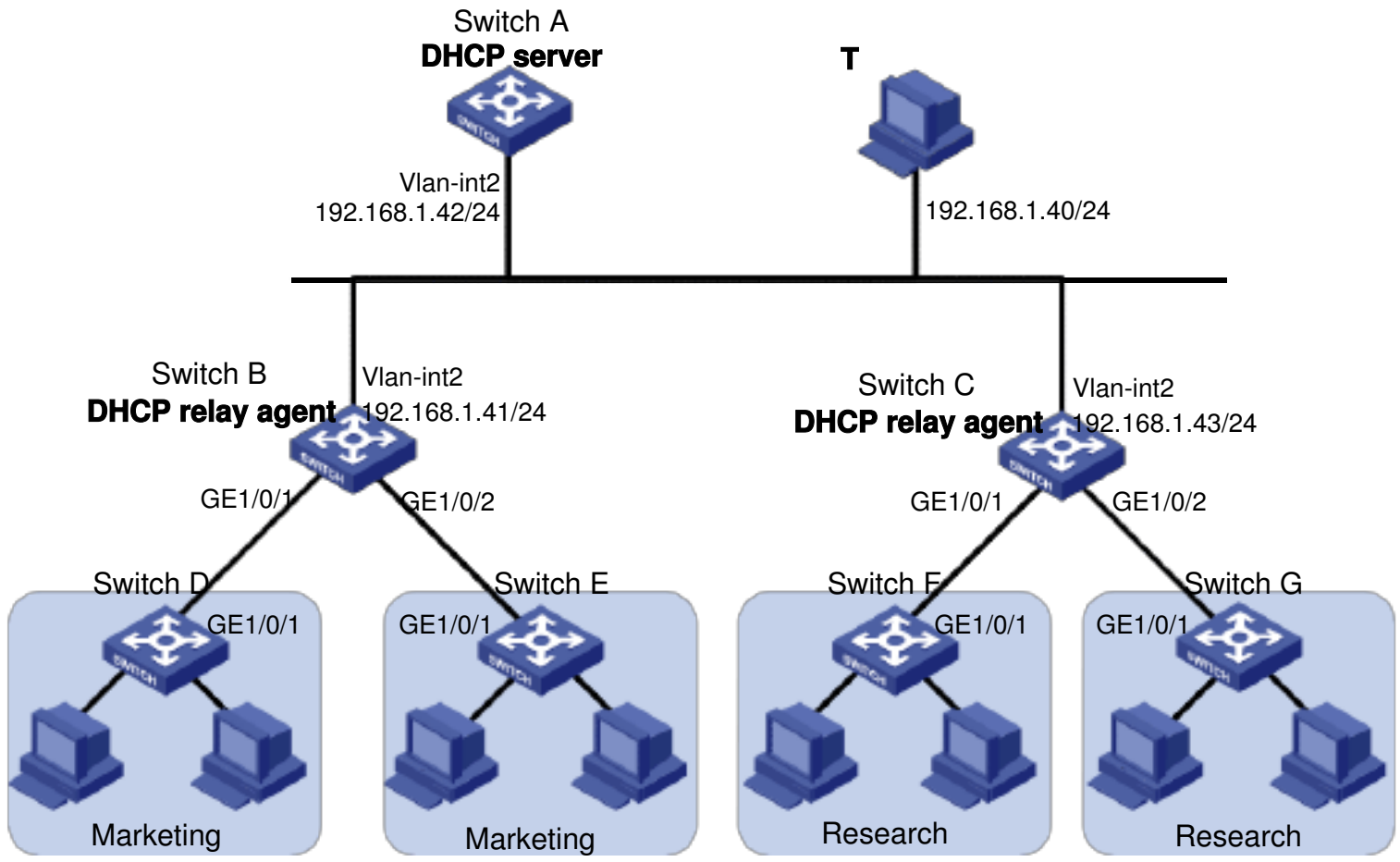


图 1-11 自动配置组网图

11.6.2 应用需求

某公司下属两个部门:市场部门和研发部门,连接终端主机的交换机分别通过不同的网关设备（同时作为DHCP中继）连入网络，如自动配置组网图所示。

Switch A 作为 DHCP server，分别为市场部和研发部的主机分配 IP 地址和其他网络配置参数；

主机上运行 T 软件，作为 T；

市场部的网关设备为 Switch B，Switch B 同时作为 DHCP 中继，通过 VLAN 接口 2 与 DHCP server、T 相连，通过 VLAN 接口 3 与连接终 端主机的 Switch D 和 Switch E 相连。VLAN 接口 3 的 IP 地址为 192.168.2.1/24。

Switch D 和 Switch E 分别通过 VLAN 接口 3 与 DHCP 中继 Switch B 连接。 研发部的网关设备为 Switch C，Switch C 同时作为 DHCP 中继，通过 VLAN 接口 2 与 DHCP server、T 相连，通过 VLAN 接口 3 与连接终 端主机的 Switch F 和 Switch G 相连。VLAN 接口 3 的 IP 地址为 192.168.3.1/24。

Switch F 和 Switch G 分别通过 VLAN 接口 3 与 DHCP 中继 Switch C 连接。 为了简化对网络中设备的管理,使网络管理员能够通过 Telnet 方式登录、控制设备，并提供 一定的安全保证，连接终端主机的交换机运行自动配置功能,使得交换机启动后自动获取配置文件。配置文件包括如下内容：

接口通过 DHCP 获取 IP 地址； 启动 Telnet服务器功能； 创建本地用户；

配置通过Telnet方式登录设备时，需要进行认证。

11.6.3 配置过程和解释

说明：

以下配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下配置不冲突。

---

4. DHCP server 设备 Switch A 的配置

配置 VLAN 接口 2 的 IP 地址

```
<SwitchA> system-view
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/1
[SwitchA-vlan2] quit
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 192.168.1.42
[SwitchA-Vlan-interface2] quit
```

使能 DHCP 服务。

```
[SwitchA] dhcp enable
```

配置 DHCP 地址池 market，为市场部动态分配 192.168.2.0/24 网段的地址，并指定 TFTP 服务器、网关地址和配置文件名。

```
[SwitchA] dhcp server ip-pool market
[SwitchA-dhcp-pool-market] network 192.168.2.0 24
[SwitchA-dhcp-pool-market] t 192.168.1.40 [SwitchA-
dhcp-pool-market] gateway-list 192.168.2.1 [SwitchA-
dhcp-pool-market] boot market.cfg [SwitchA-dhcp-pool-
market] quit
```

配置 DHCP 地址池 research，为研发部动态分配 192.168.3.0/24 网段的地址，并指定 TFTP 服务器、网关地址和配置文件名。

```
[SwitchA] dhcp server ip-pool research
[SwitchA-dhcp-pool-research] network 192.168.3.0 24
[SwitchA-dhcp-pool-research] t 192.168.1.40 [SwitchA-
dhcp-pool-research] gateway-list 192.168.3.1 [SwitchA-
dhcp-pool-research] boot research.cfg [SwitchA-dhcp-pool-
research] quit
```

配置到达 DHCP 中继的静态路由。

```
[SwitchA] ip route-static 192.168.2.0 24 192.168.1.41
[SwitchA] ip route-static 192.168.3.0 24 192.168.1.43
[SwitchA] quit
```

5. DHCP 中继设备 Switch B 的配置

配置 VLAN 接口 2 和 VLAN 接口 3 的 IP 地址

```
<SwitchB> system-view
[SwitchB] vlan 2
[SwitchB-vlan2] port gigabitethernet 1/0/3
[SwitchB-vlan2] quit
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address 192.168.1.41
[SwitchB-Vlan-interface2] quit
[SwitchB] vlan 3
[SwitchB-vlan3] port gigabitethernet 1/0/1
[SwitchB-vlan3] port gigabitethernet 1/0/2
[SwitchB-vlan3] quit
[SwitchB] interface vlan-interface 3
[SwitchB-Vlan-interface3] ip address 192.168.2.1
[SwitchB-Vlan-interface3] quit
```

使能 DHCP 服务。

```
[SwitchB] dhcp enable
```

配置 DHCP 服务器的地址

```
[SwitchB] dhcp relay server-group 1 ip 192.168.1.42
```

配置 VLAN 接口 3 工作在 DHCP 中继模式。

```
[SwitchB] interface vlan-interface 3
[SwitchB-Vlan-interface3] dhcp select relay
```

配置 VLAN 接口 3 对应 DHCP 服务器组 1。

```
[SwitchB-Vlan-interface3] dhcp relay server-select 1
```

6. DHCP 中继设备 Switch C的配置

配置接口的 IP 地址

```
<SwitchC> system-view
[SwitchC] vlan 2
[SwitchC-vlan2] port gigabitethernet 1/0/3
[SwitchC-vlan2] quit
[SwitchC] interface vlan-interface 2
[SwitchC-Vlan-interface2] ip address 192.168.1.43
[SwitchC-Vlan-interface2] quit
[SwitchC] vlan 3
[SwitchC-vlan3] port gigabitethernet 1/0/1
[SwitchC-vlan3] port gigabitethernet 1/0/2
[SwitchC-vlan3] quit
[SwitchC] interface vlan-interface 3
[SwitchC-Vlan-interface3] ip address 192.168.3.1
[SwitchC-Vlan-interface3] quit
```

使能 DHCP 服务。

```
[SwitchC] dhcp enable
```

配置 DHCP 服务器的地址

```
[SwitchC] dhcp relay server-group 1 ip 192.168.1.42
```

配置 VLAN 接口 3 工作在 DHCP 中继模式。

```
[SwitchC] interface vlan-interface 3
[SwitchC-Vlan-interface3] dhcp select relay
```

配置 VLAN 接口 3 对应 DHCP 服务器组 1。

```
[SwitchC-Vlan-interface3] dhcp relay server-select 1
```

7. 配置主机作为 T

在主机的“D:/T”目录下创建配置文件 market.cfg，文件内容如下。

```
#
 sysname Market
#
 telnet server enable
#
vlan 3
#
local-user market
 password simple market
 service-type telnet
 level 3
#
interface Vlan-interface3
 ip address dhcp-alloc
#
interface GigabitEthernet1/0/1
 port access vlan 3
#
user-interface vty 0 4
 authentication-mode scheme
 user privilege level 3
#
return
```

在主机的“D:/T”目录下创建配置文件 research.cfg，文件内容如下。

```
#
 sysname Research
#
```

```
 telnet server enable
#
vlan 3
#
local-user research
 password simple research
 service-type telnet
 level 3
#
interface Vlan-interface3
 ip address dhcp-alloc
#
interface GigabitEthernet1/0/1
 port access vlan 3
#
user-interface vty 0 4
 authentication-mode scheme
 user privilege level 3
#
return
```

运行 T 软件，点击<Settings>，如 T 配置界面所示。

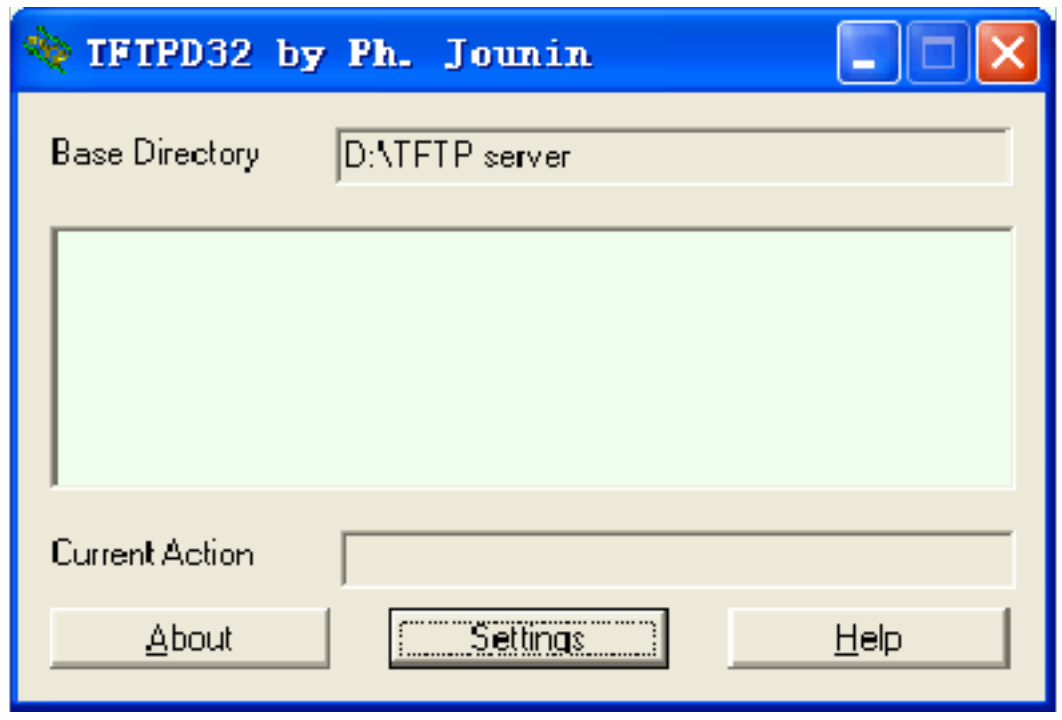


图 1-12 T 配置界面

将配置文件保存的路径设置为“Base Directory”，单击<OK>，如设置文件保存的路径所示。

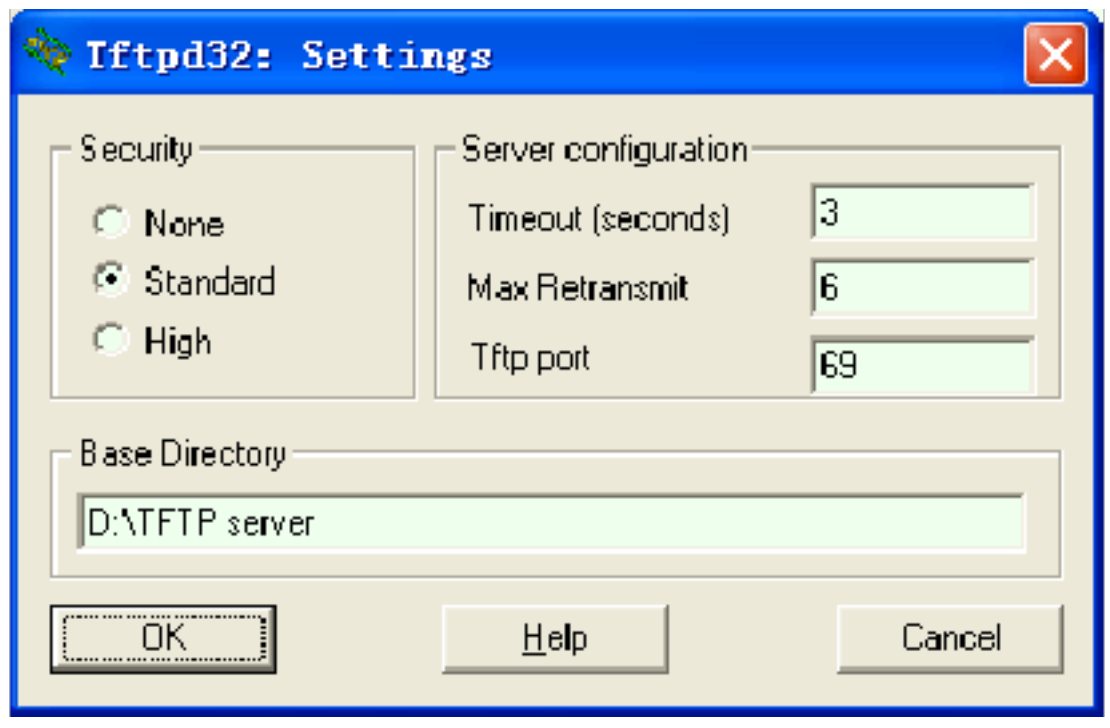


图 1-13 设置文件保存的路径

配置主机到达 192.168.2.0/24 和 192.168.3.0/24 网段的路由，即在主机上执行如下命令：

```
route add 192.168.2.0 mask 255.255.255.0 192.168.1.41
route add 192.168.3.0 mask 255.255.255.0 192.168.1.43
```

11.6.4 完整配置

Switch A 上的完整配置

```
#
vlan 1
#
vlan 2
#
dhcp server ip-pool market
 network 192.168.2.0 mask 255.255.255.0
 gateway-list 192.168.2.1
 boot market.cfg
 t ip-address 192.168.1.17
#
dhcp server ip-pool research
 network 192.168.3.0 mask 255.255.255.0
 gateway-list 192.168.3.1
 boot research.cfg
 t ip-address 192.168.1.17
#
interface Vlan-interface2
 ip address 192.168.1.42 255.255.255.0
#
interface GigabitEthernet1/0/1
 port access vlan 2
#
 ip route-static 192.168.2.0 255.255.255.0 192.168.1.41
 ip route-static 192.168.3.0 255.255.255.0 192.168.1.43
#
 dhcp enable
#
```

Switch B 上的完整配置

```
#
 dhcp relay server-group 1 ip 192.168.1.42
#
vlan 1
#
vlan 2
#
vlan 3
#
interface Vlan-interface2
 ip address 192.168.1.41 255.255.255.0
#
interface Vlan-interface3
 ip address 192.168.2.1 255.255.255.0
 dhcp select relay
 dhcp relay server-select 1
#
interface GigabitEthernet1/0/1
 port access vlan 3
#
interface GigabitEthernet1/0/2
 port access vlan 3
#
interface GigabitEthernet1/0/3
 port access vlan 2
#
dhcp enable
#
```

Switch C 上的完整配置

```
#
 dhcp relay server-group 1 ip 192.168.1.42
#
vlan 1
#
vlan 2
#
vlan 3
```

```
#
interface Vlan-interface2
 ip address 192.168.1.43 255.255.255.0
#
interface Vlan-interface3
 ip address 192.168.3.1 255.255.255.0
 dhcp select relay
  dhcp relay server-select 1
 #
 interface GigabitEthernet1/0/1
  port access vlan 3
 #
 interface GigabitEthernet1/0/2
  port access vlan 3
 #
 interface GigabitEthernet1/0/3
  port access vlan 2
 #
 dhcp enable
 #
```

11.6.7 注意事项

设备应用自动配置功能之前，需要完成 DHCP server、DHCP 中继、T 和 DNS server（可选）的配置，并将设备的配置文件保存到 TFTP 服务 器。

DHCP server 需要为客户端分配网关地址，设备才能够跨网段请求 TFTP 和 DNS 服务。 为了保证自动配置功能正常使用，建议设备启动前，只将设备的一个接口连入

网络。 设备通过自动配置功能获取配置文件后，只是执行配置文件，不会将配置文件

保存到本地。设备再次启动时，需要重新获取配置文件。