H3C 园区盒式交换机 Web 快速配置指南

目 录

1 适用产品型号

如表 1所示的 H3C 交换机系列，出厂时已经缺省启用了 HTTP 和 HTTPS 服务，并且设置有缺省的 Web 登录信息，包括：管理 IP 地址、用户名、密码、用户角色等；用户可以直接使用缺省信息登录设备的 Web 界面。

其它系列交换机，请参考基础配置指导中的“登录设备”一章，确认其支持“通过 Web 登录设备”后，用户可以先通过 Console 口登录设备，然后设置通过 Web 登录设备所需的配置，包括开启 HTTP 和 HTTPS 服务、登录 Web 所需的 IP 地址、用户名、密码、用户角色等，再登录设备的 Web 界面。

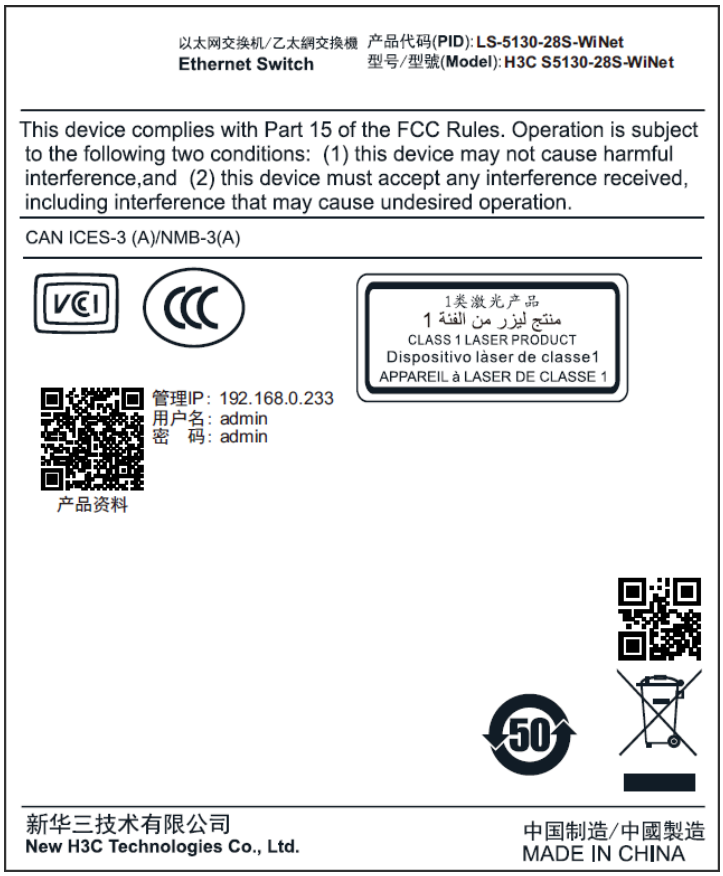
表1 缺省支持 Web 登录的交换机系列

系列	管理 IP	用户名/密码
MS4100V2-EI系列	192.168.0.233	admin/admin
S1850-X系列		
S1850V2-X系列		
S1850V2-EI系列		
S5000V3-EI系列		
S5000V5-EI系列		
S5000E-X系列		
S5000X-EI系列		
S5000-E系列		
US300系列		
US500系列		
US536-F-S		
US300S系列		
US500S系列		
US1750系列		
WAS1760系列		
WAS6000系列		
WS5810-WiNet系列		
WS5820-WiNet系列		
WS5850-WiNet系列		
NS200系列	192.168.1.1（Release 3115P03及以上版）	admin/admin
NS300系列	192.168.1.1	admin/admin
S5130-WiNet	192.168.0.233	admin/admin
S5500V2-WiNet	192.168.0.233	admin/admin

说明

缺省支持 Web 登录的交换机系列随着时间变化有更新的可能性，若您需要准确的信息，请查看设备铭牌（如 1 图 1）。铭牌上打印了“管理 IP、用户名、密码”的设备，缺省支持 Web 登录。

图1 设备铭牌信息（以 S5130-28S-WiNet 机型的铭牌为例）



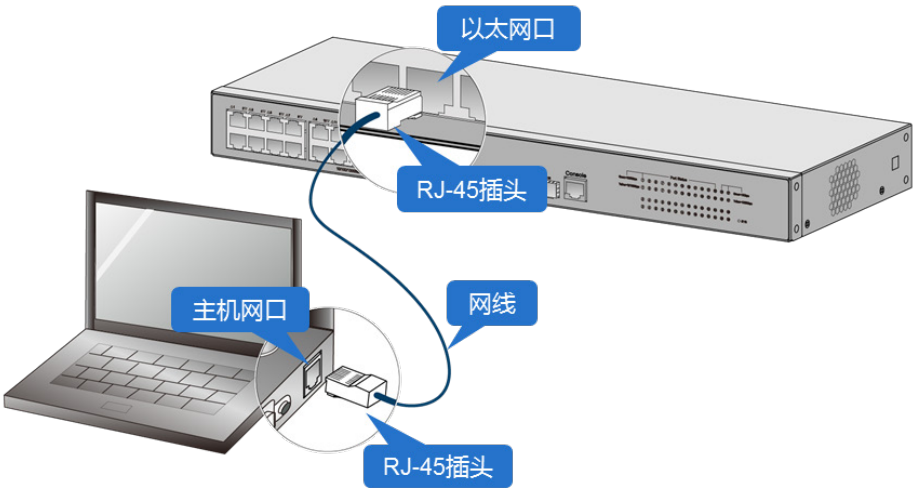
目 录

1 通过 Web 登录有缺省 IP 地址的设备

1.1 组网需求

如图 1 所示，主机通过网线与有缺省 IP 地址的交换机设备相连，要求主机可以通过浏览器访问设备的 Web 管理页面。

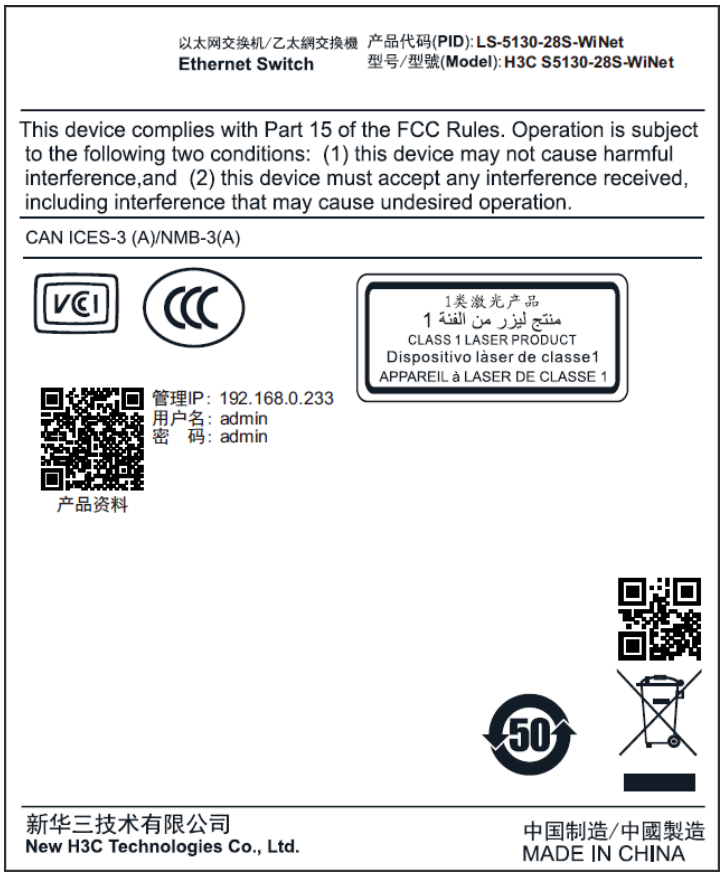
图1 通过 Web 登录设备组网图



1.2 配置准备

(1) 查看设备铭牌信息，记录设备缺省 IP 地址和用户名密码，此处以 S5130-28S-WiNet 机型的铭牌为例。

图2 设备铭牌信息



(2) 使用网线连接主机网口与设备以太网口。

1.3 配置步骤

1. 配置主机的 IP 地址

(1) 打开“网络和共享中心”，点击“本地连接”。

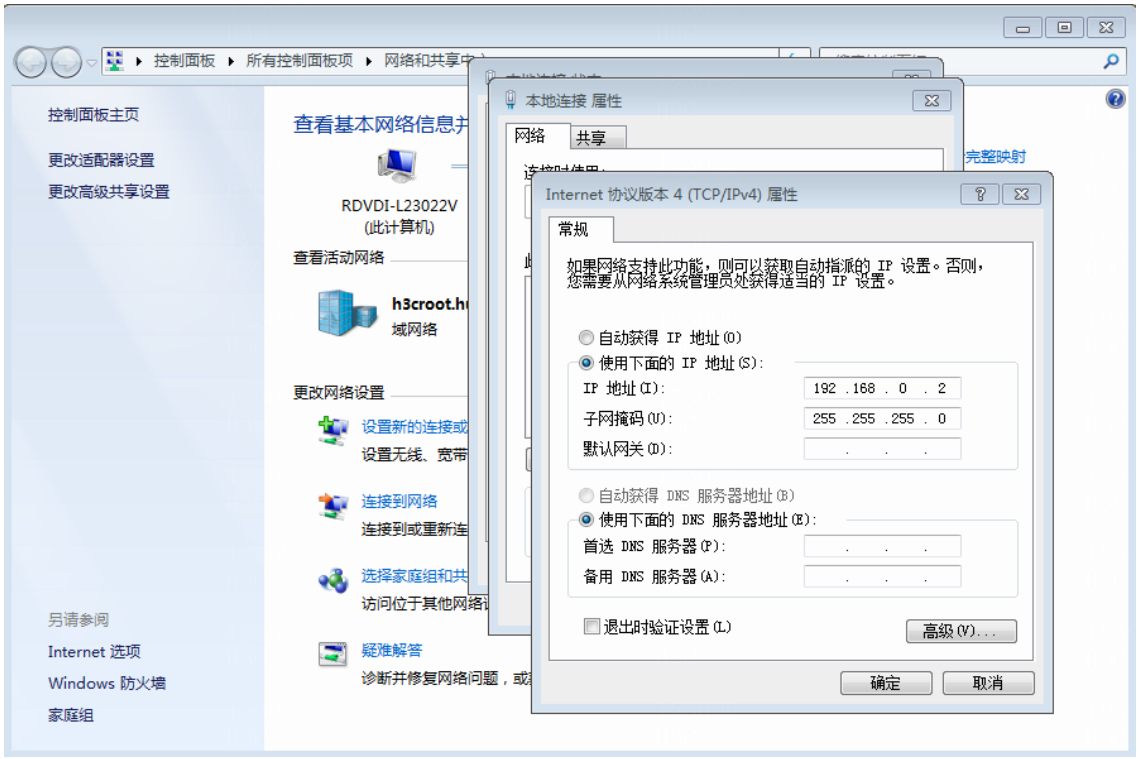
(2) 在弹出的窗口中点击“属性”，双击“Internet 协议版本 4（TCP/IPv4）”。

(3) 在弹出的窗口中进行如下配置：

- 选择“使用下面的 IP 地址（S）”。
- 配置 IP 地址，注意配置的 IP 地址需和设备的 IP 地址在同一网段，本文以 192.168.0.2 为例。
- 配置子网掩码为“255.255.255.0”。

(4) 点击<确定>按钮，完成主机 IP 地址的配置。

图3 配置主机的 IP 地址



2. 登录设备

(1) 打开主机的浏览器，在地址栏中输入设备的缺省 IP 地址“192.168.0.233”。

(2) 进入设备的 Web 登录页面，输入缺省用户名“admin”和缺省密码“admin”。

(3) 点击<登录>按钮登录设备。

图4 进入设备的 Web 登录页面

(4) （可选）部分设备支持首次登录时修改密码，可根据系统提示，修改缺省密码。

图5 修改缺省密码

(5) 登录成功，进入设备的 Web 管理页面。

图6 设备 Web 管理页面

1.4 验证配置

无。

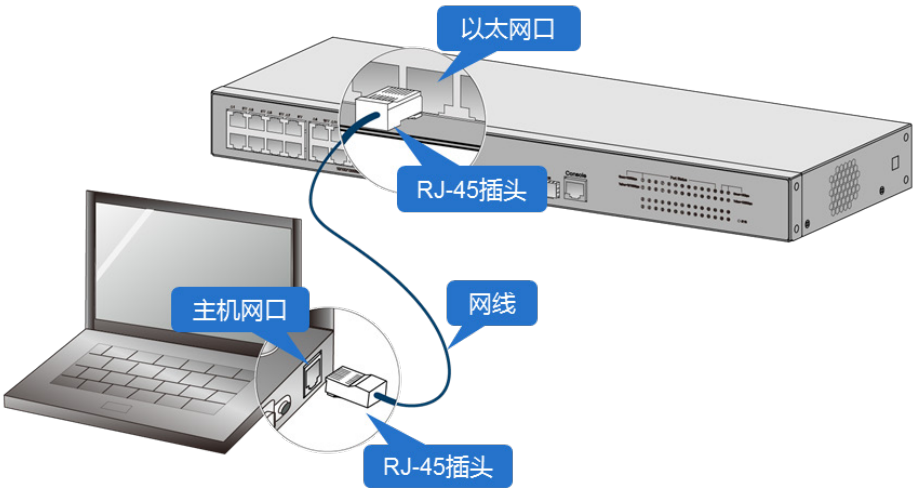
目 录

1 通过 Web 登录没有缺省 IP 地址的设备

1.1 组网需求

如图 1 所示，主机通过网线与没有缺省 IP 地址的交换机设备相连，要求主机可以通过浏览器访问设备的 Web 管理页面。

图1 通过 Web 登录设备组网图



1.2 配置准备

首先通过 Console 口登录到设备的命令行页面完成 1. 通过 Web 登录设备基础功能配置。有关如何通过 Console 口登录设备的具体描述，请参见《CLI 快速配置指南》中的“登录设备”。

然后使用网线连接主机网口与设备的以太网口完成 2. 配置主机的 IP 地址和 3. 登录设备。

1.3 配置步骤

1. 通过 Web 登录设备基础功能配置

进入系统视图

```
<Device> system-view
```

创建本地用户 admin，并设置登录密码为 hello12345，服务类型为 http 和 https，用户角色为 network-admin 管理员角色，此角色可操作系统所有功能和资源。

```
[Device] local-user admin
[Device-luser-manage-admin] password simple hello12345
[Device-luser-manage-admin] service-type http https
[Device-luser-manage-admin] authorization-attribute user-role network-admin
[Device-luser-manage-admin] quit
```

配置设备的 IP 地址为 192.168.0.1。

```
[Device] interface vlan-interface 1
```

```
[Device-VLAN-interface1] ip address 192.168.0.1 255.255.255.0
[Device-VLAN-interface1] quit
```

开启 http 和 https 服务

```
[Device] ip http enable
[Device] ip https enable
```

保存配置

```
[Device] save
```

2. 配置主机的 IP 地址

(1) 打开“网络和共享中心”，点击“本地连接”。

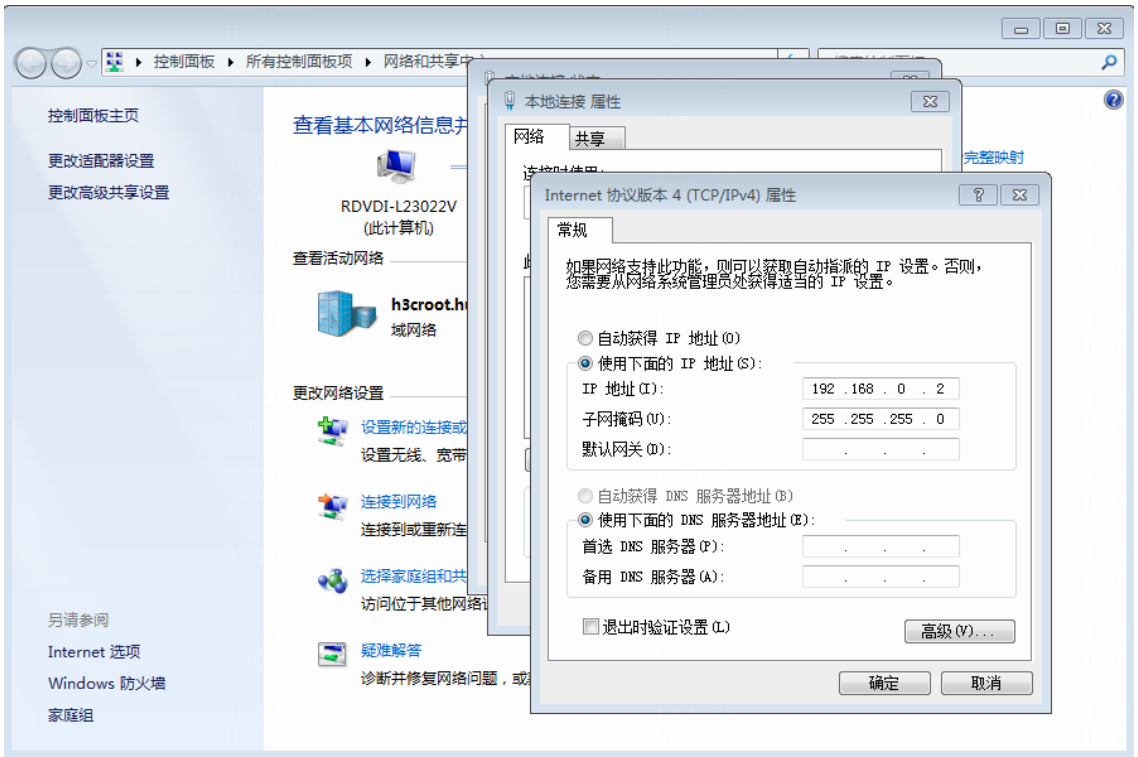
(2) 在弹出的窗口中点击“属性”，双击“Internet 协议版本 4（TCP/IPv4）”。

(3) 在弹出的窗口中进行如下配置：

- 选择“使用下面的 IP 地址（S）”。
- 配置 IP 地址，注意配置的 IP 地址需和设备的 IP 地址在同一网段，本文以 192.168.0.2 为例。
- 配置子网掩码为“255.255.255.0”。

(4) 点击<确定>按钮，完成主机 IP 地址的配置。

图2 配置主机 IP 地址



3. 登录设备

(1) 打开浏览器，在地址栏中输入设备 IP 地址“192.168.0.1”。

(2) 进入设备 Web 登录页面，输入用户名“admin”和密码“hello12345”。

(3) 击<登录>按钮登录设备。

图3 进入 Web 登录页面

(4) 登录成功，进入设备 Web 管理页面。

图4 Web 配置页面

1.4 验证配置

无。

目 录

1 接口设置快速配置指南

1.1 组网需求

无。

1.2 配置步骤

(1) 修改接口设置

选择页面左侧导航栏的[网络/接口]，进入“接口”页面。单击右侧的“  ”按钮，进入“修改接口设置”页面，进行如下配置：

- 修改描述为“GE1/0/1”。
- 配置速率为“1Gbps”。
- 修改双工模式为“全双工”。
- 若工作模式配置为“三层模式”，则可以为接口配置 IPv4 和 IPv6 地址。仅部分设备支持切换接口的工作模式，请以设备的实际情况为准。
- 单击<确定>按钮，完成操作。

图1 修改接口设置页面

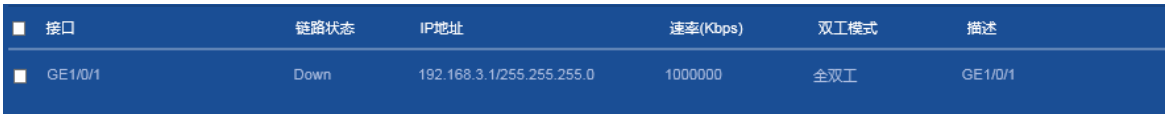
(2) 保存配置

点击页面左上方标识和辅助区内的“  ”按钮保存配置。

1.3 验证配置

选择页面左侧导航栏的[网络/接口]，进入“接口”页面，查看接口设置。

图2 查看接口配置



接口	链路状态	IP地址	速率(Kbps)	双工模式	描述
GE1/0/1	Down	192.168.3.1/255.255.255.0	1000000	全双工	GE1/0/1

目 录

1 开启 PoE 快速配置指南

1.1 组网需求

无。

1.2 配置注意事项

如果没有开启 PoE 接口的远程供电功能，系统不会给 PoE 接口下挂的 PD 供电，也不会给 PD 预留功率。

如果该 PoE 接口的加入不会导致 PSE 功率过载，则允许该 PoE 接口为下挂的 PD 供电；如果该 PoE 接口的加入会导致 PSE 功率过载，则由该 PoE 接口是否开启 PoE 接口优先级策略决定。

1.3 配置步骤

(1) 选择页面左侧导航栏的[PoE/PoE]，进入“PoE”配置页面。

图1 PoE 页面

(2) 单击需要开启 PoE 功能的接口，以 GigabitEthernet1/0/1 举例。

- 点开“PI（Power Interface，电源接口）”选项，在远程供电处勾选“开启”，并根据实际需要修改最大供电功率、供电优先级等配置。
- 单击<确定>按钮，完成配置。

图2 开启 PoE 功能

(3) 保存配置

点击页面左上方标识和辅助区内的“  ”按钮保存配置。

1.4 验证配置

配置完成后，下挂的 PD 设备被供电，能够正常工作。

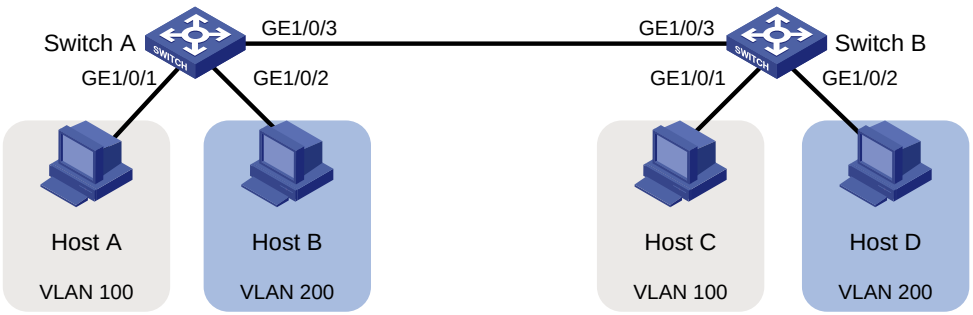
目 录

1 划分 VLAN 快速配置指南

1.1 组网需求

- HOST A 和 Host C 属于部门 A，但是通过不同的设备接入公司网络；Host B 和 Host D 属于部门 B，也通过不同的设备接入公司网络。
- 为了通信的安全性，也为了避免广播报文泛滥，公司网络使用 VLAN 技术来隔离部门间的二层流量，其中部门 A 使用 VLAN 100，部门 B 使用 VLAN 200。

图1 VLAN 配置组网图



1.2 配置步骤

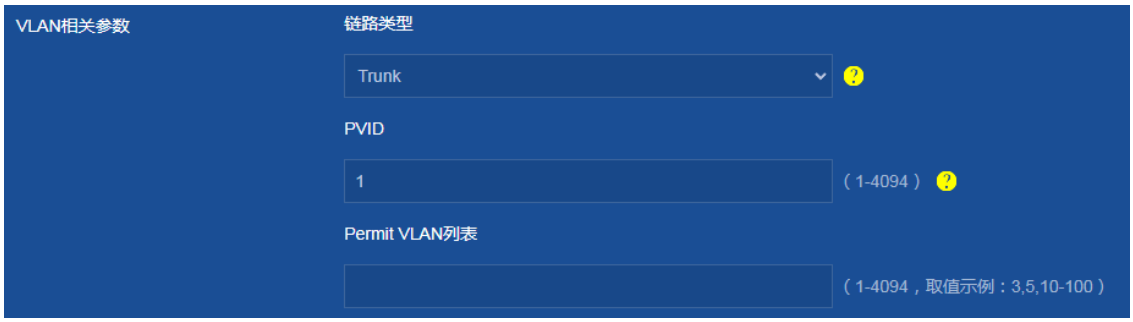
1. Switch A 的配置

(1) 配置链路类型

选择页面左侧导航栏的[网络/接口/接口]，进入“接口”配置页面，进行如下配置：

- 点击 GE1/0/3 右侧“ ”按钮，进入“修改接口设置”页面。
- 设置链路类型为“Trunk”。
- 单击<确定>按钮，提示设置成功，完成链路类型的修改。

图2 配置链路类型



(2) 创建 VLAN

选择页面左侧导航栏的[网络/链路/VLAN]，进入“VLAN”配置页面，进行如下配置：

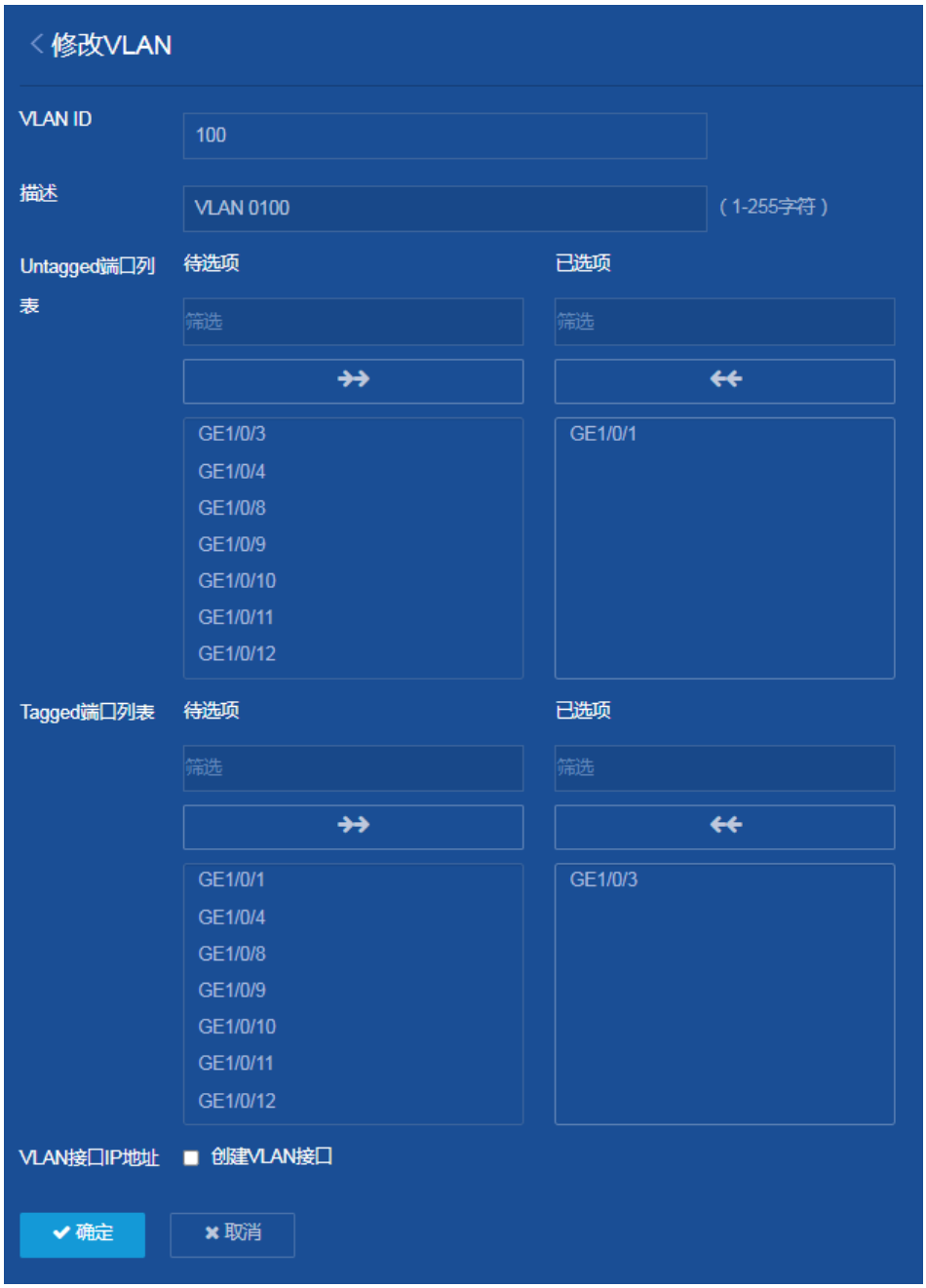
- 点击“  ”按钮，进入“创建 VLAN”对话框。
- 配置 VLAN 列表为“100,200”。
- 单击<确定>按钮，完成 VLAN 的创建。

图3 创建 VLAN

(3) 配置 VLAN 100

- 点击“  ”按钮，进入“修改 VLAN”页面。
- 配置端口 GE1/0/1 加入 VLAN 100 的 Untagged 端口列表。
- 配置端口 GE1/0/3 加入 VLAN 100 的 Tagged 端口列表。
- 单击<确定>按钮，提示设置成功，完成 VLAN 100 的配置。

图4 配置 VLAN 100



(4) 配置 VLAN 200

- 点击“  ”按钮，进入“修改 VLAN”页面。
- 配置端口 GE1/0/2 加入 VLAN 200 的 Untagged 端口列表。
- 配置端口 GE1/0/3 加入 VLAN 200 的 Tagged 端口列表。
- 单击<确定>按钮，提示设置成功，完成 VLAN 200 的配置。

(5) 保存配置

点击页面左上方标识和辅助区内的“  ”按钮保存配置。

2. Switch B 的配置

(1) 配置链路类型

选择页面左侧导航栏的[网络/链路/接口]，进入“接口”配置页面，进行如下配置：

- 点击 GE1/0/3 右侧“  ”按钮，进入“修改接口设置”页面。
- 设置链路类型为“Trunk”。
- 单击<确定>按钮，提示设置成功，完成链路类型的修改。

(2) 创建 VLAN

选择页面左侧导航栏的[网络/链路/VLAN]，进入“VLAN”配置页面，进行如下配置：

- 点击“  ”按钮，进入“创建 VLAN”对话框。
- 配置 VLAN 列表为“100,200”。
- 单击<确定>按钮，完成 VLAN 的创建。

(3) 配置 VLAN 100

- 点击“  ”按钮，进入“修改 VLAN”页面。
- 配置端口 GE1/0/1 加入 VLAN 100 的 Untagged 端口列表。
- 配置端口 GE1/0/3 加入 VLAN 100 的 Tagged 端口列表。
- 单击<确定>按钮，提示设置成功，完成 VLAN 100 的配置。

(4) 配置 VLAN 200

- 点击“  ”按钮，进入“修改 VLAN”页面。
- 配置端口 GE1/0/2 加入 VLAN 200 的 Untagged 端口列表。
- 配置端口 GE1/0/3 加入 VLAN 200 的 Tagged 端口列表。
- 单击<确定>按钮，提示设置成功，完成 VLAN 200 的配置。

(5) 保存配置

点击页面左上方标识和辅助区内的“  ”按钮保存配置。

3. Host 的配置

将 Host A 和 Host C 配置在一个网段，例如 192.168.100.0/24；将 Host B 和 Host D 配置在一个网段，比如 192.168.200.0/24。

1.3 验证配置

完成上述配置后，Host A 和 Host C 能够互相 ping 通，但是均不能 ping 通 Host B 和 Host D。Host B 和 Host D 能够互相 ping 通，但是均不能 ping 通 Host A 和 Host C。

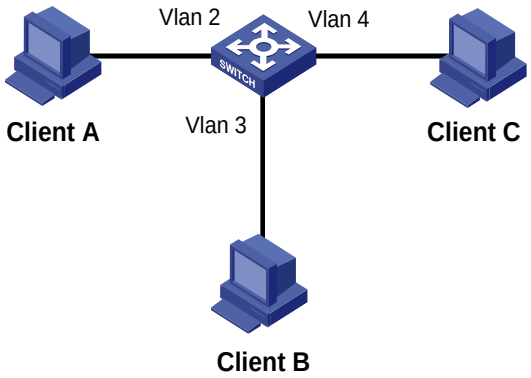
目 录

1 DHCP 服务器快速配置指南

1.1 组网需求

在公司内部网络中，需要在核心交换机上划分 3 个 VLAN 网段，部门 A、B、C 分别属于 VLAN 2、VLAN 3 和 VLAN 4。要求在交换机上开启 DHCP 功能，分别给三个部门内的主机动态分配 IP 地址。

图1 配置 DHCP 服务器组网图



1.2 配置步骤

1. 创建 DHCP 服务器

(1) 配置 VLAN

选择页面左侧导航栏的[网络/链路/VLAN]，进入“VLAN”配置页面，进行如下配置：

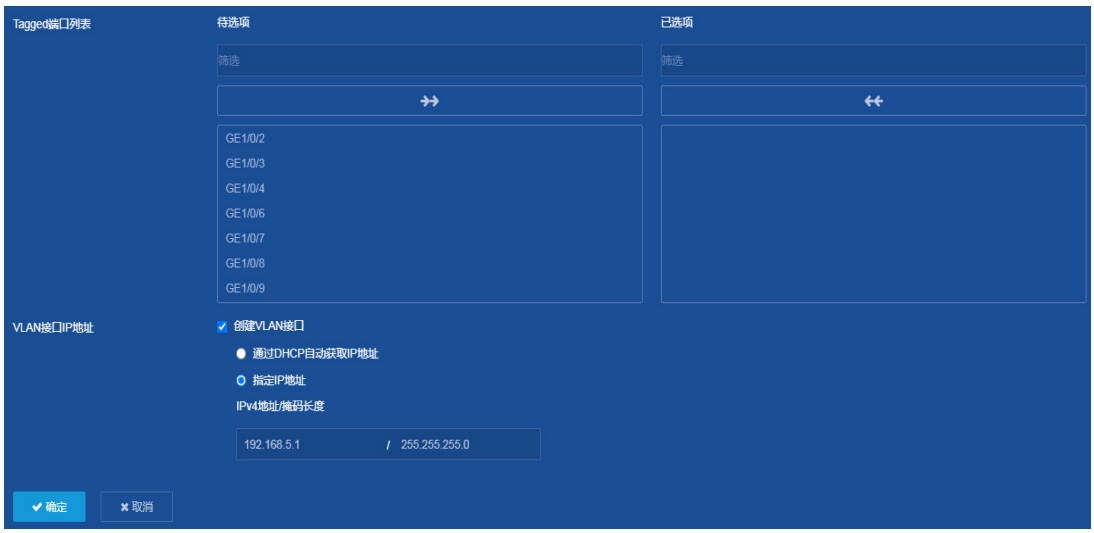
- 单击右上角“ ”按钮，添加 VLAN。
- 创建 VLAN 2。

图2 创建 VLAN 2

在 VLAN 界面中点击 VLAN 2 右侧的“ ”，进入“修改 VLAN”配置页面：

- 将 GE1/0/2 加入到 VLAN 2 的 UnTagged 端口列表;
- 在 VLAN 接口 IP 地址处勾选“创建 VLAN 接口”；
- 指定 VLAN 2 接口的 IP 地址为“192.168.5.1”，子网掩码为“255.255.255.0”。

图3 配置 VLAN 2 接口 IP 地址



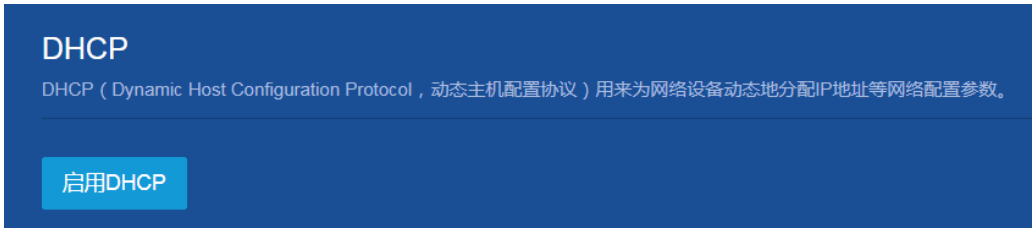
- 单击<确定>按钮，提示设置成功，完成 VLAN 2 和 VLAN 2 接口的创建。
- 参考 VLAN 2 完成 VLAN 3 和 VLAN 4 的设置，具体配置步骤略。

(2) 建立 DHCP 地址池

选择页面左侧导航栏的[网络/服务/DHCP]，进入“DHCP”配置页面，进行如下配置：

- 点击<启用 DHCP>按钮，开启 DHCP 服务。

图4 开启 DHCP 服务



- 在 DHCP 配置界面右上角点击“地址池”，然后点击“添加地址池”，创建 DHCP 地址池“1”。

图5 在 DHCP 配置里添加地址池

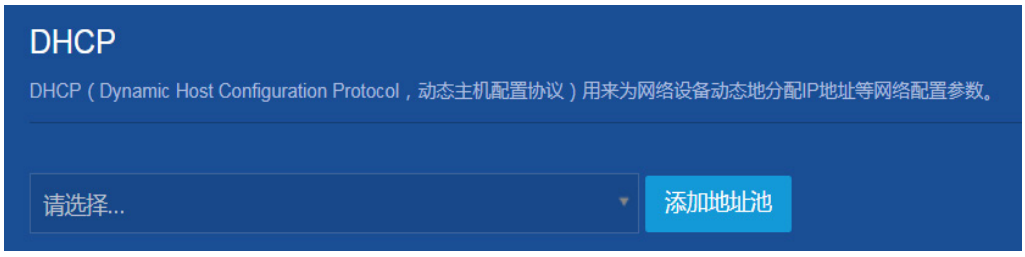


图6 创建 DHCP 地址池“1”

- 配置 DHCP 地址池“1”，动态分配的地址段 192.168.5.0，掩码 255.255.255.0。

图7 配置 DHCP 地址池动态分配的地址段

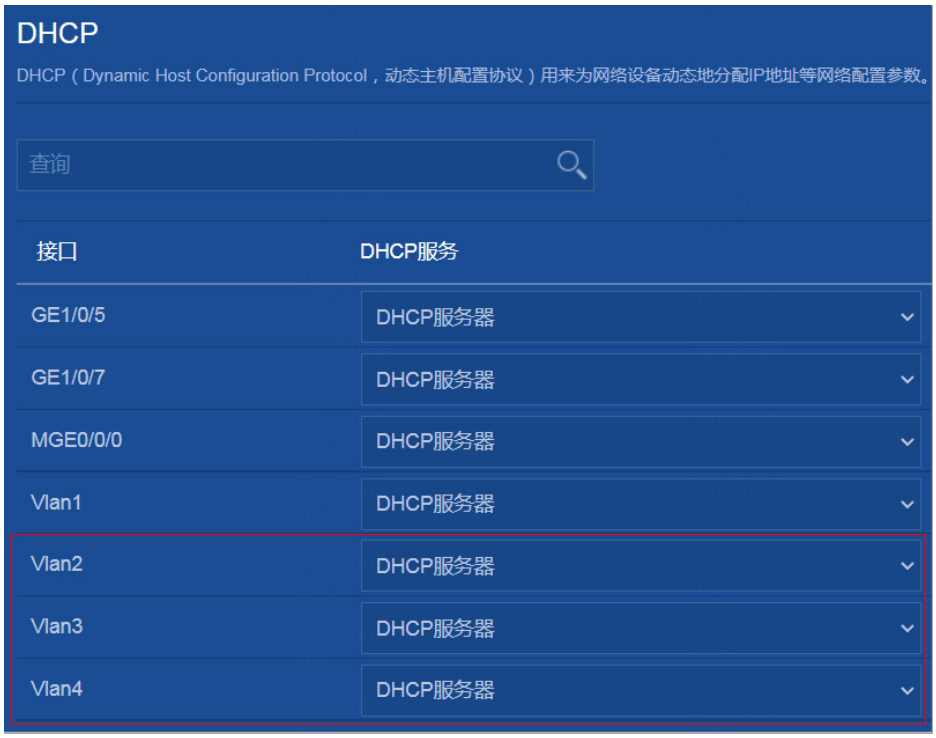
- 点击地址池选项，配置网关为“192.168.5.1”，点击“  ”按钮完成添加。

图8 配置 DHCP 地址池网关

(3) 配置接口工作在 DHCP 服务器模式

- 选择页面左侧导航栏的[网络/服务/DHCP]，进入“DHCP”配置页面。在 DHCP 界面，分别配置 Vlan 2、VLAN 3 和 VLAN 4 作为 DHCP 服务器”。缺省情况下，接口工作在 DHCP 服务器模式，无需修改。

图9 配置 DHCP 服务器



- 点击右上角“  ”按钮，进入“DHCP 高级设置”界面，配置冲突地址检查功能中的发送回显请求报文的最大数目为“1”，等待回显应答报文的超时时间为“500”毫秒。

图10 DHCP 高级设置

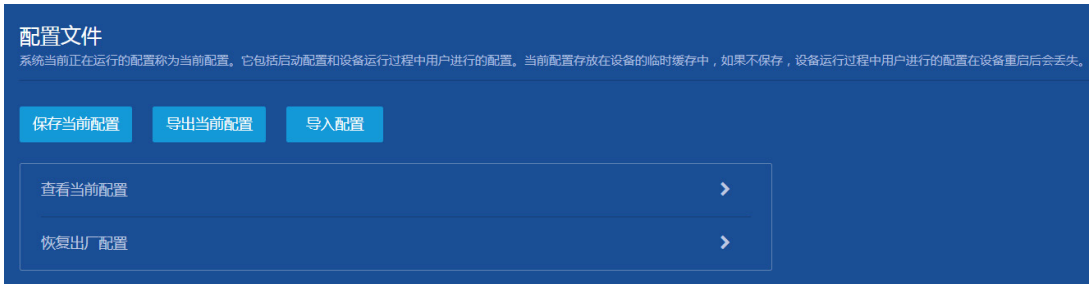
- 单击<确定>按钮，提示设置成功，完成 DHCP 高级配置。

(4) 保存配置

选择页面左侧导航栏的[设备/配置文件]，进入“配置文件”界面，进行如下配置：

- 进入配置文件界面后，点击<保存当前配置>按钮。

图11 进入“配置文件”界面



- 在弹出的“保存当前配置”对话框中，选择“保存到下次启动配置文件”，或“保存到指定配置文件”。如果选择了“保存到指定配置文件”，则指定配置文件将作为下次启动配置文件。

图12 保存当前配置

- 单击<确定>按钮，保存当前配置。

1.3 验证配置

完成上述配置后，在把 Client A、Client B 和 Client C 分别连接到交换机的 GigabitEthernet1/0/2 、GigabitEthernet1/0/3、GigabitEthernet1/0/4 接口，三台主机自动获取到了相应网段的 IP 地址。

打开交换机配置界面，选择页面左侧导航栏的[网络/服务/DHCP]，进入 DHCP 配置界面后，选择右上角“地址池”，进入“地址池”界面后选择“已分配地址”中可以查看 DHCP 服务器已分配的 IP 地址。

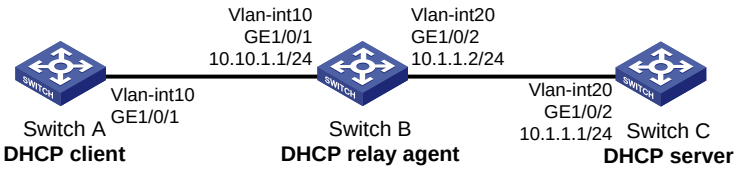
目 录

1 DHCP 中继快速配置指南

1.1 组网需求

DHCP 客户端所在网段为 10.10.1.0/24，DHCP 服务器的 IP 地址为 10.1.1.1/24。由于 DHCP 客户端和 DHCP 服务器不在同一网段，因此，需要在客户端所在网段设置 DHCP 中继设备，以便客户端可以从 DHCP 服务器申请到 10.10.1.0/24 网段的 IP 地址及相关配置信息。

图1 配置 DHCP 中继组网图



1.2 配置步骤

1. 配置 DHCP 服务器 Switch C

(1) 配置 VLAN

选择页面左侧导航栏的[网络/链路/VLAN]，进入“VLAN”页面，进行如下配置：

- 点击“ ”按钮，弹出“创建 VLAN”对话框。
- 配置 VLAN 列表为“20”。
- 单击<确定>按钮，完成 VLAN 20 的创建。

图2 创建 VLAN 20

- 点击 VLAN 20 右侧的“ ”按钮，进入“修改 VLAN”页面。
- 将端口“GE1/0/2”加入 VLAN 20 的 Tagged 端口列表。
- 勾选“创建 VLAN 接口”，配置 VLAN 接口 20 的地址为“10.1.1.1”，掩码长度为“24”
- 单击<确定>按钮，提示设置成功，完成 VLAN 20 的配置。

图3 配置 VLAN 20

(2) 配置静态路由

选择页面左侧导航栏的[网络/路由/静态路由]，进入“静态路由”页面，进行如下配置：

- 点击“IPv4 静态路由”右侧的“ ”按钮，进入 IPv4 静态路由配置页面。
- 点击页面右上角的“ ”按钮，进入“添加 IPv4 静态路由”页面。
- 配置目的 IP 地址为“10.10.1.0”、掩码长度为“24”、取消勾选“出接口”、下一跳地址为“10.1.1.2”。

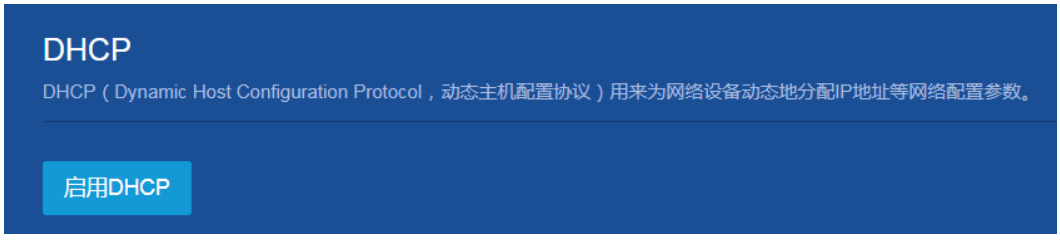
图4 添加 IPv4 静态路由

(3) 配置 DHCP 服务器

选择页面左侧导航栏的[网络/服务/DHCP]，进入“DHCP”页面，进行如下配置：

- 点击“启用 DHCP”按钮，开启 DHCP 服务，并进入“DHCP”配置页面。

图5 启用 DHCP



- 在“DHCP”页面，点击页面右上角的“服务”按钮，配置 VLAN 接口 20 工作在 DHCP 服务器模式。缺省情况下接口工作在 DHCP 服务器模式，无需修改。

图6 配置接口工作在 DHCP 服务器模式

- 点击页面右上角的“地址池”按钮，进入 DHCP 地址池配置页面。
- 点击“添加地址池”按钮，添加地址池“1”。
- 在地址池 1 的“地址分配”页面，输入动态分配的地址段地址“10.10.1.0”，掩码“255.255.255.0”。

图7 地址池 1 的地址分配配置页面

- 在地址池 1 的“地址池选项”页面，配置网关为“10.10.1.1”点击右侧的“+”按钮完成添加。
- 单击<确定>按钮，提示设置成功，完成地址池 1 配置。

图8 地址池选项配置页面

(4) 保存配置

点击页面左上方标识和辅助区内的“ ”按钮保存配置。

2. 配置 DHCP 中继 Switch B

(1) 配置 VLAN

选择页面左侧导航栏的[网络/链路/VLAN]，进入“VLAN”页面，进行如下配置：

- 点击“ ”按钮，弹出“创建 VLAN”对话框。
- 配置 VLAN 列表为“10,20”。
- 单击<确定>按钮，完成 VLAN 10 和 VLAN 20 的创建。

图9 创建 VLAN

- 点击 VLAN 10 右侧的“ ”按钮，进入“修改 VLAN”页面。
- 将端口“GE1/0/1”加入 VLAN 10 的 Tagged 端口列表。
- 勾选“创建 VLAN 接口”，配置 VLAN 接口 10 的地址为“10.10.1.1”，子网掩码为“255.255.255.0”
- 单击<确定>按钮，提示设置成功，完成 VLAN 10 的配置。

图10 配置 VLAN 10

- 点击 VLAN 20 右侧的“  ”按钮，进入“修改 VLAN”页面。
- 将端口“GE1/0/2”加入 VLAN 20 的 Tagged 端口列表。
- 勾选“创建 VLAN 接口”，配置 VLAN 接口 20 的地址为“10.1.1.2”，子网掩码为“255.255.255.0”
- 单击<确定>按钮，提示设置成功，完成 VLAN 20 的配置。

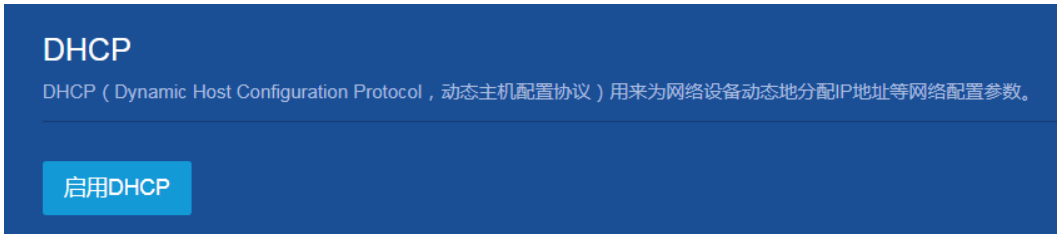
图11 配置 VLAN 20

(2) 配置 DHCP 中继

选择页面左侧导航栏的[网络/服务/DHCP]，进入“DHCP”页面，进行如下配置：

- 点击“启用 DHCP”按钮，开启 DHCP 服务，并进入“DHCP”配置页面。

图12 启用 DHCP



- 在“DHCP”页面，点击页面右上角的“服务”按钮，配置 VLAN 接口 10 工作在 DHCP 中继模式，配置中继服务器地址为 10.1.1.1
- 单击<确定>按钮，提示设置成功，完成 DHCP 中继的配置。

图13 配置接口工作在 DHCP 中继模式

- 在 DHCP 页面点击右上角的“ ”按钮，进入“DHCP 高级设置页面”。
- 开启“记录中继用户信息”功能和“开启 DHCP 中继动态用户地址表项定时刷新功能”。
- 配置刷新时间间隔为“100”秒。
- 单击<确定>按钮，提示设置成功，完成 DHCP 中继高级设置。

图14 DHCP 高级设置

(3) 保存配置

点击页面左上方标识和辅助区内的“ ”按钮保存配置。

3. 配置 DHCP 客户端 Switch A

(1) 配置 VLAN

选择页面左侧导航栏的[网络/链路/VLAN]，进入“VLAN”页面，进行如下配置：

- 点击“ ”按钮，弹出“创建 VLAN”对话框。
- 配置 VLAN 列表为“10”。
- 单击<确定>按钮，完成 VLAN 10 的创建。

图15 创建 VLAN

- 点击 VLAN 10 右侧的“ ”按钮，进入“修改 VLAN”页面。
- 将端口“GE1/0/1”加入 VLAN 10 的 Tagged 端口列表。
- 勾选“创建 VLAN 接口”，点击“通过 DHCP 自动获取 IP 地址”。
- 单击<确定>按钮，提示设置成功，完成 VLAN 10 的配置。

图16 配置 VLAN 10

(2) 配置静态路由

选择页面左侧导航栏的[网络/路由/静态路由]，进入“静态路由”页面，进行如下配置：

- 点击“IPv4 静态路由”右侧的“ ”按钮，进入 IPv4 静态路由配置页面。
- 点击页面右上角的“ ”按钮，进入“添加 IPv4 静态路由”页面。
- 配置目的 IP 地址为“10.1.1.0”、掩码长度为“24”、取消勾选“出接口”、下一跳地址为“10.10.1.1”。该路由用于 DHCP 服务器和 DHCP 客户端实现路由互通。

图17 添加 IPv4 静态路由

(3) 保存配置

点击页面左上方标识和辅助区内的“  ”按钮保存配置。

1.3 验证配置

完成上述配置后，在 DHCP 服务器的已分配地址表中可以查看到已分配的 IP 地址；在 DHCP 中继表项中可以查看到对应的 DHCP 中继表项；在 DHCP 客户端上可以查看到获取的 IP 地址信息。

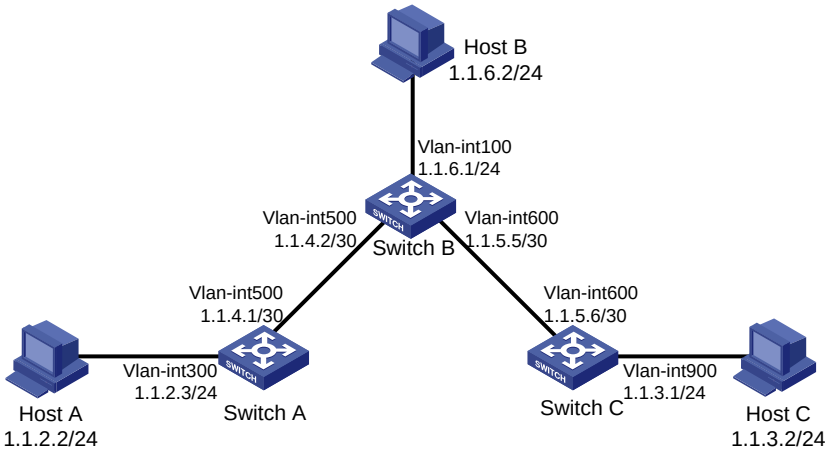
目 录

1 静态路由快速配置指南

1.1 组网需求

在 Switch A、Switch B 和 Switch C 上配置静态路由，实现主机之间的两两互通。

图1 IPv4 静态路由配置组网图



1.2 配置步骤

1. 设备 A 的配置

(1) 配置 VLAN 接口和接口 IP 地址

选择页面左侧导航栏的[网络/链路/VLAN]，进入“VLAN”配置页面，进行如下配置：

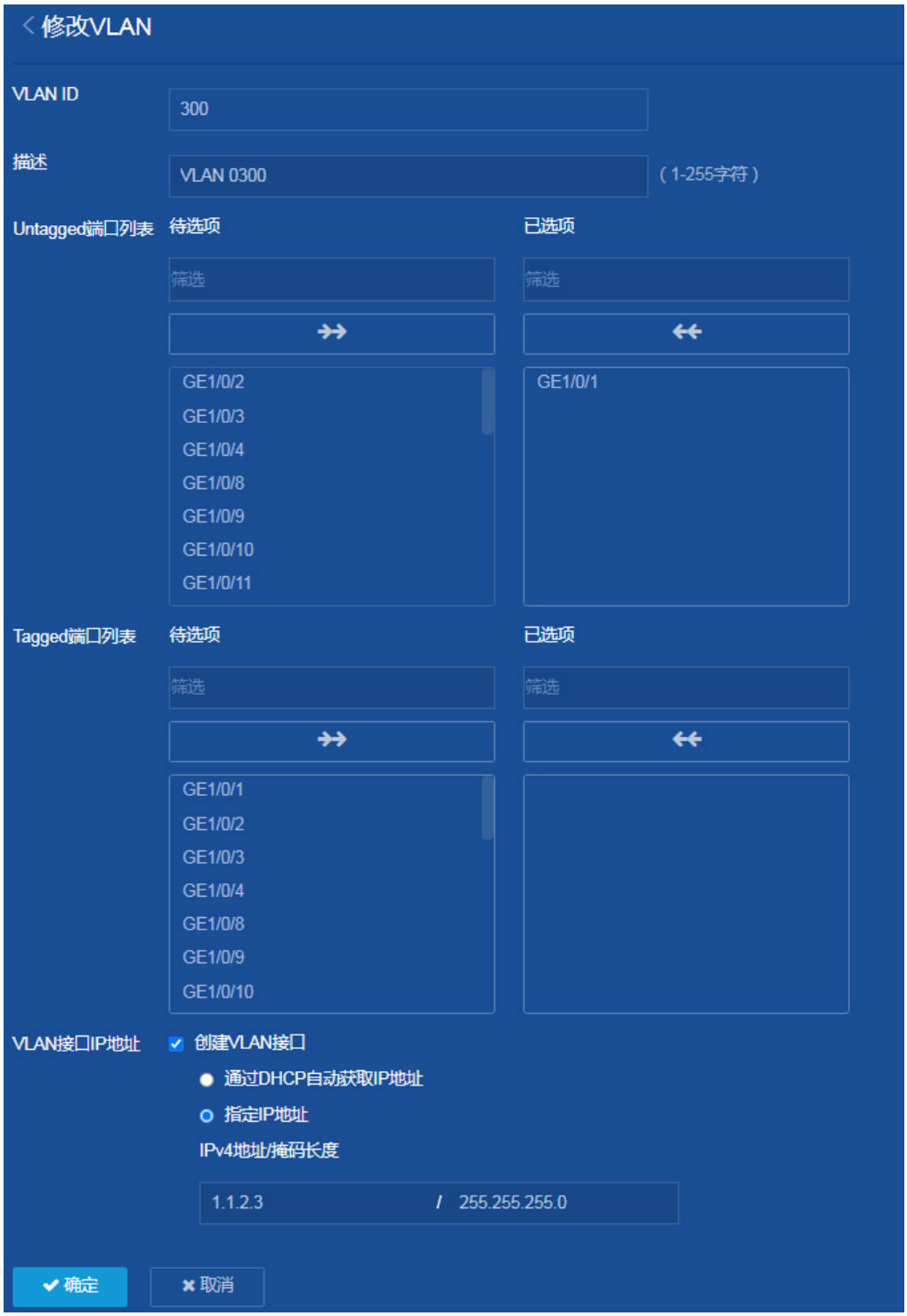
- 单击“  ”按钮，进入“创建 VLAN”页面，输入 VLAN 列表号“300”，单击<确定>按钮添加 VLAN。

  图2 创建 VLAN

- 单击在“VLAN”配置页面单击 VLAN300 右侧的“  ”按钮，进入“修改 VLAN”页面。

- 将和连接 Host A 的接口“GE1/0/1”加入到 Untagged 端口列表。
- 在“VLAN 接口 IP 地址”处勾选“创建 VLAN 接口”。
- 指定 VLAN 接口的 IP 地址为“1.1.2.3”，掩码长度为“24”.
- 单击<确定>按钮，提示设置成功，完成 VLAN 接口 300 和接口 IP 地址的配置。
- 创建 VLAN 接口 500 和接口 IP 地址，具体配置过程略。

图3 修改 VLAN



(2) 配置静态路由

选择页面左侧导航栏的[网络/路由/静态路由]，进入“IPv4 静态路由”配置页面，进行如下配置：

- 单击“⊕”按钮，添加静态路由。
- 配置目的 IP 地址为“0.0.0.0”，该路由用来匹配所有的目的 IP 地址。
- 掩码长度为“0”。
- 取消勾选“出接口”。
- 下一跳地址为“1.1.4.2”。
- 其它配置项使用缺省值。
- 单击<确定>按钮，提示设置成功，完成 IPv4 静态路由的创建。

图4 添加 IPv4 静态路由

(3) 保存配置

点击页面左上方标识和辅助区内的“💾”按钮保存配置。

2. 设备 B 的配置

(1) 配置 VLAN 接口和接口 IP 地址（略）

(2) 配置静态路由

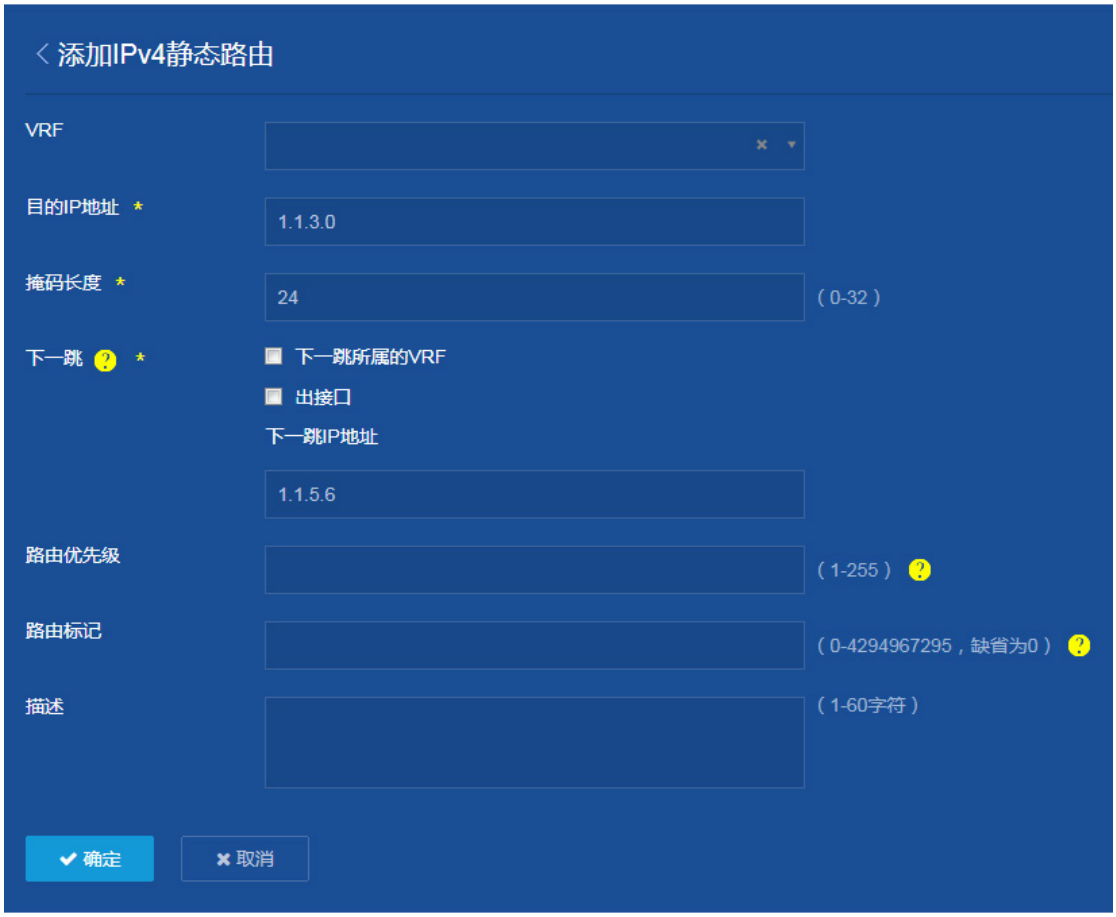
选择页面左侧导航栏的[网络/路由/静态路由]，进入“IPv4 静态路由”配置页面，进行如下配置：

- 单击“⊕”按钮，添加静态路由。
- 配置目的 IP 地址为“1.1.2.0”。
- 掩码长度为“24”。
- 取消勾选“出接口”。
- 下一跳地址为“1.1.4.1”。
- 其它配置项使用缺省值。
- 单击<确定>按钮，提示设置成功，完成到达 Host A 所在网段的静态路由的创建。

图5 添加到达 Host A 所在网段的静态路由

- 单击“⊕”按钮，添加静态路由。
- 配置目的 IP 地址为“1.1.3.0”。
- 掩码长度为“24”。
- 取消勾选“出接口”。
- 下一跳地址为“1.1.5.6”。
- 其它配置项使用缺省值。
- 单击<确定>按钮，提示设置成功，完成到达 Host C 所在网段的静态路由的创建。

图6 添加到达 Host C 所在网段的静态路由



(3) 保存配置

点击页面左上方标识和辅助区内的“ ”按钮保存配置。

3. 设备 C 的配置

(1) 配置 VLAN 接口和接口 IP 地址（略）

(2) 配置静态路由

选择页面左侧导航栏的[网络/路由/静态路由]，进入“IPv4 静态路由”配置页面，进行如下配置：

- 单击“ ”按钮，添加静态路由。
- 配置目的 IP 地址为“0.0.0.0”。
- 配置掩码长度为“0”。
- 取消勾选“出接口”。
- 配置下一跳地址为“1.1.5.5”，该路由用来匹配所有的目的 IP 地址。
- 其它配置项使用缺省值。
- 单击<确定>按钮，提示设置成功，完成 IPv4 静态路由的创建。

图7 配置 IPv4 静态路由

(3) 保存配置

点击页面左上方标识和辅助区内的“ ”按钮保存配置。

1.3 验证配置

完成上述配置后，在任意一台主机上可以 ping 通另外两台主机。

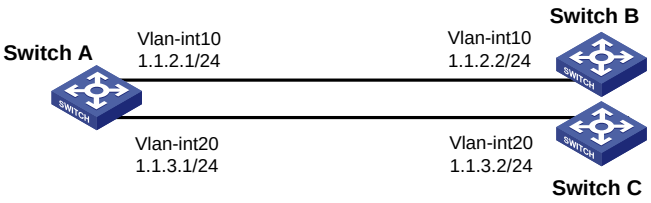
目 录

1 IPv4 本地策略路由快速配置指南

1.1 组网需求

通过策略路由控制由 Switch A 产生的 TCP 报文的下一跳为 1.1.2.2，其它类型报文仍然按照查找路由表的方式进行转发。

图1 IPv4 本地策略路由配置组网图



1.2 配置步骤

1. 设备 A 的配置

(1) 配置 VLAN 接口和接口 IP 地址

选择页面左侧导航栏的[网络/链路/VLAN]，进入“VLAN”配置页面，进行如下配置：

- 单击“  ”按钮，进入“创建 VLAN”页面，输入 VLAN 列表号“10”，单击<确定>按钮添加 VLAN。

  图2 创建 VLAN

- 单击在“VLAN”配置页面单击 VLAN10 右侧的“  ”按钮，进入“修改 VLAN”页面。
- 将和连接 Switch B 的接口“GE1/0/1”加入到 Tagged 端口列表。
- 在“VLAN 接口 IP 地址”处勾选“创建 VLAN 接口”。
- 指定 VLAN 接口的 IP 地址为“1.1.2.1”，掩码长度为“24”.
- 单击<确定>按钮，提示设置成功，完成 VLAN 接口 10 和接口 IP 地址的配置。
- 配置 VLAN 接口 20 和接口 IP 地址，具体配置过程略。

图3 修改 VLAN

(2) 配置策略路由

选择页面左侧导航栏的[网络/路由/策略路由]，进入“IPv4 策略路由”配置页面，进行如下配置：

- 单击“⊕”按钮，添加 IPv4 策略路由。

- 配置策略名称“pbr”。
- 在应用于下拉菜单中选择“本机”。
- 点击添加策略节点，在弹出的添加节点对话框中输入节点编号“5”。
- 节点匹配模式设置为“允许”。
- 在报文匹配规则处勾选“匹配 IPv4 ACL”，单击“  ”按钮，添加 IPv4 ACL。
- 在弹出的“添加 ACL”对话框中选择 IPv4 ACL，点击<确定>按钮。
- 在弹出的“添加 IPv4 ACL”对话框中，勾选类型为“高级 ACL”，ACL 编号为“3001”，点击<确定>按钮，提示设置成功，开始添加 IPv4 高级 ACL 规则。
- 在添加 IPv4 高级 ACL 规则对话框中，动作使用缺省值“允许”，在 IP 协议类型下拉菜单中选择“tcp(6)”，取消勾选“继续添加下一条规则”，点击<确定>按钮，提示设置成功。
- 在执行操作出勾选“设置报文转发的下一跳地址”，设置 IP 地址为 1.1.2.2.
- 点击确定<确定>按钮，提示设置成功，完成本地策略路由的创建和应用。

图4 添加 IPv4 策略路由

(3) 保存配置

点击页面左上方标识和辅助区内的“  ”按钮保存配置。

2. 设备 B 的配置

配置各接口的 IP 地址（略）

3. 设备 C 的配置

配置各接口的 IP 地址（略）

1.3 验证配置

由于 Telnet 使用的是 TCP 协议，ping 使用的是 ICMP 协议，完成上述配置后：

- 在 Switch B 上开启 Telnet 服务后，Switch A 可以成功通过 Telnet 方式登录 Switch B。
- 在 Switch C 上开启 Telnet 服务后，Switch A 无法通过 Telnet 方式登录 Switch C。
- 在 Switch A 上可以 ping 通 Switch C。

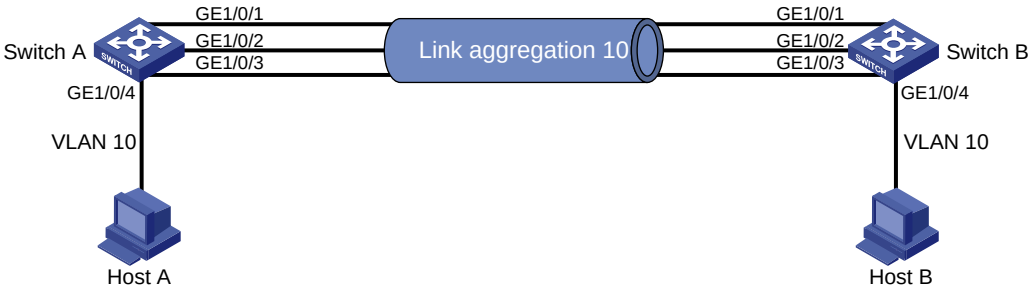
目 录

1 二层静态链路聚合快速配置指南

1.1 组网需求

为了增加链路带宽，提高网络可靠性，现要在 Switch A 与 Switch B 之间运行二层静态链路聚合。Switch A 与 Switch B 通过各自的二层以太网接口 GigabitEthernet1/0/1～GigabitEthernet1/0/3 相互连接。

图1 链路聚合配置组网图



1.2 配置注意事项

- 配置聚合组的成员端口过程中，使端口保持在缺省属性类配置状态，然后再把端口加入到新创建的聚合组内。
- 由于静态聚合组中端口选中状态不受对端端口是否在聚合组中及是否处于选中状态的影响。这样有可能导致两端设备所确定的 Selected 状态端口不一致，当两端都支持配置静态和动态聚合组的情况下，建议用户优选动态聚合组。
- 配置或使能了下列功能的端口将不能加入二层聚合组：MAC 地址认证、端口安全模式、802.1X 功能。

1.3 配置步骤

1. Switch A 的配置

(1) 创建 VLAN

选择页面左侧导航栏的[网络/链路/VLAN]，进入“VLAN”配置页面，进行如下配置：

- 点击“ ”按钮，进入“创建 VLAN”对话框。
- 配置 VLAN 列表为“10”。
- 单击<确定>按钮，完成 VLAN 的创建。

图2 创建 VLAN

(2) 配置二层静态聚合

选择页面左侧导航栏的[网络/接口/链路聚合]，进入“链路聚合”页面，进行如下配置：

- 单击“ ”按钮，添加聚合组。
- 在聚合类型下拉菜单中选择“二层聚合”。
- 聚合组编号为“1”。
- 在聚合模式下拉菜单中选择“静态聚合”。
- 在成员端口下拉菜单中选择“GE1/0/1、GE1/0/2 和 GE1/0/3”。
- 单击<确定>按钮，提示设置成功，完成二层静态聚合组的创建。

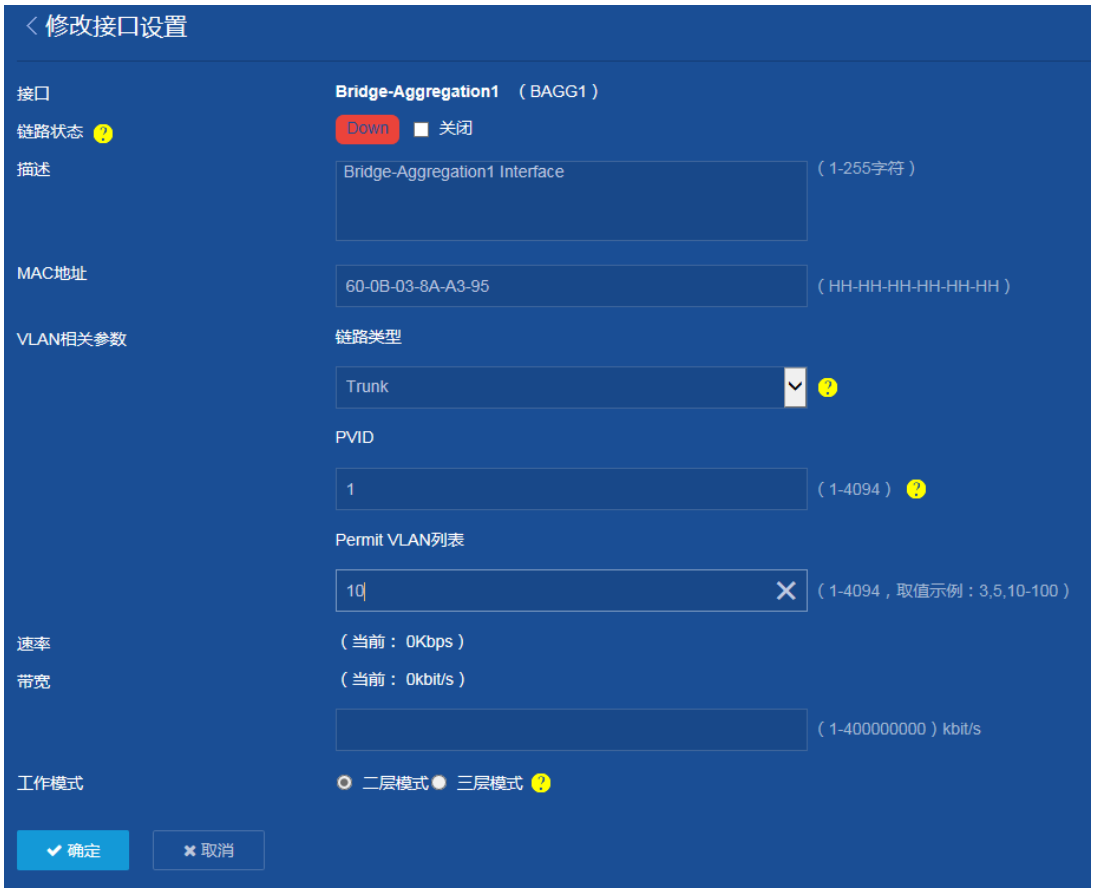
图3 配置二层静态聚合

(3) 配置二层静态聚合接口的 VLAN 属性

选择页面左侧导航栏的[网络/接口/接口]，进入“接口”页面，进行如下配置：

- 单击“ ”按钮，修改二层聚合接口 1 的接口设置。
- 在链路类型下拉菜单中选择“Trunk”。
- 配置 Permit VLAN 列表为“10”。
- 单击<确定>按钮，提示设置成功，完成二层聚合接口 1 的 VLAN 属性配置。

图4 配置二层静态聚合接口的 VLAN 属性



(4) 配置连接 Host 的接口的 VLAN 属性

选择页面左侧导航栏的[网络/接口/接口]，进入“接口”页面，进行如下配置：

- 单击“ ”按钮，修改 GE1/0/4 的接口设置。
- 在链路类型下拉菜单中选择“Access”。
- 配置 PVID 为“10”
- 单击<确定>按钮，提示设置成功，完成 GE1/0/4 的 VLAN 属性配置。

图5 配置连接 Host 的接口的 VLAN 属性

(5) 保存配置

点击页面左上方标识和辅助区内的“  ”按钮保存配置。

2. Switch B 的配置

Switch B 上的配置与 Switch A 完全相同，此处不再赘述。

1.4 验证配置

完成上述配置后，在“网络 > 接口 > 链路聚合”页面中可以看到 GigabitEthernet1/0/1～GigabitEthernet1/0/3 已经加入到二层静态聚合组 1。

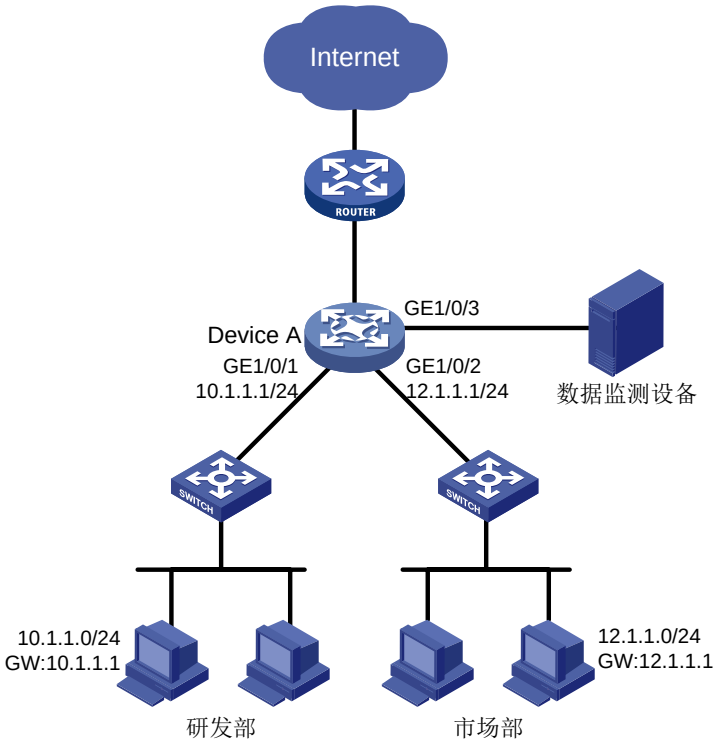
目 录

1 本地端口镜像

1.1 组网需求

某公司内部各部门使用不同网段的 IP 地址，其中研发部使用 10.1.1.0/24 网段，市场部使用 12.1.1.0/24 网段。现要求通过配置本地端口镜像功能，使用数据监测设备对研发部和市场部访问 Internet 的流量进行监控。

图1 本地端口镜像组网图



1.2 配置注意事项

- 本地镜像组需要配置源端口、目的端口才能生效，其中目的端口不能是现有镜像组的成员端口。
- 目的端口收到的报文包括复制自源端口的报文和来自其他端口的正常转发报文。为了保证数据监测设备只对源端口的报文进行分析，请将目的端口只用于端口镜像，不作其他用途。

1.3 配置步骤

1. 配置本地端口镜像组

(1) 配置各接口的 IP 地址（略）

(2) 配置本地端口镜像

选择页面左侧导航栏的[网络/镜像/端口镜像]，进入“端口镜像”配置页面，进行如下配置：

- 单击“⊕”按钮，添加端口镜像组。

- 配置镜像组编号为“1”。
- 类型为“本地镜像组”。
- 配置 DeviceA 连接研发部的接口为源端口：选择接口“GE1/0/1”，方向选择“入方向”，单击“+”按钮添加源端口。
- 配置 DeviceA 连接市场部的接口为源端口：选择接口“GE1/0/2”，方向选择“入方向”，单击“+”按钮添加源端口。
- 配置 DeviceA 连接数据监测设备的接口为目的端口：选择接口“GE1/0/3”。
- 单击<确定>按钮，提示设置成功，完成本地端口镜像的创建。

图2 配置本地端口镜像

(3) 保存配置

点击页面左上方标识和辅助区内的“”按钮保存配置。

1.4 验证配置

配置完成后，可在“网络 > 镜像 > 端口镜像”页面中，可以查看到已配置的本地端口镜像信息。

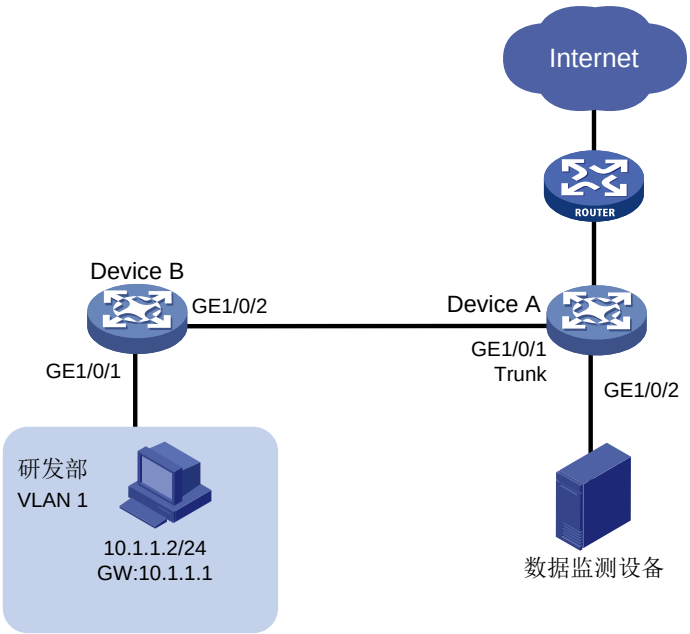
图3 本地端口镜像

2 出端口方式二层远程端口镜像

2.1 组网需求

某公司研发部通过二层网络连接到核心设备 Device A，使用 10.1.1.0/24 网段。现要求通过配置出端口方式二层远程端口镜像功能，使用数据监测设备对研发部发送的报文进行监控。

图4 出端口方式二层远程端口镜像组网图



2.2 配置注意事项

- 建议用户先配目的设备，再配源设备，以保证镜像流量的正常转发。

配置远程端口镜像的目的设备和源设备时均需要注意：

- 配置远程镜像 VLAN 时：
  - 要求该 VLAN 为静态 VLAN 并预先创建。
  - 要求该 VLAN 不用做其他用途，仅用于远程镜像功能。
  - 要求该 VLAN 只能被一个远程源镜像组使用。
- 源设备和目的设备上的远程镜像组必须使用相同的远程镜像 VLAN。

配置远程端口镜像的目的设备时需要注意：

- 目的端口不能是现有镜像组的成员端口。
- 目的端口不用做其他用途，仅用于端口镜像。

配置远程端口镜像的源设备时需要注意：

- 请不要将源端口加入到远程镜像 VLAN 中，否则会影响镜像功能的正常使用。

- 请不要在出端口上配置下列功能：生成树协议、802.1X、IGMP Snooping、静态 ARP 和 MAC 地址学习，否则会影响镜像功能的正常使用。
- 出端口不能是现有镜像组的成员端口。

2.3 配置步骤

1. 配置 Device A（目的设备）

(1) 配置各接口的 IP 地址（略）

(2) 创建远程镜像 VLAN

选择页面左侧导航栏的[网络/链路/VLAN]，进入“VLAN”配置页面，进行如下配置：

- 单击“⊕”按钮，创建远程镜像 VLAN 5。

图5 创建远程镜像 VLAN

- 将目的端口 GE1/0/2 加入远程镜像 VLAN。（略）

(3) 配置二层远程镜像组

选择页面左侧导航栏的[网络/镜像/端口镜像]，进入“端口镜像”配置页面，进行如下配置：

- 单击“⊕”按钮，添加端口镜像组。
- 配置镜像组编号为“2”。
- 类型为“远程目的镜像组”。
- 配置 DeviceB 连接数据监测设备的接口为目的端口：选择接口“GE1/0/2”。
- 远程镜像 VLAN 为“5”
- 单击<确定>按钮，提示设置成功，完成目的设备远程端口镜像组的创建。

图6 配置二层远程端口镜像组

(4) 保存配置

点击页面左上方标识和辅助区内的“ ”按钮保存配置。

2. 配置 Device B（源设备）

(1) 配置各接口的 IP 地址（略）

(2) 创建远程镜像 VLAN，同 DeviceA

(3) 配置二层远程镜像组

选择页面左侧导航栏的[网络/镜像/端口镜像]，进入“端口镜像”配置页面，进行如下配置：

- 单击“ ”按钮，添加端口镜像组。
- 配置镜像组编号为“2”。
- 类型为“远程源镜像组”。
- 配置 DeviceB 连接数据监测设备的接口为源端口：选择接口“GE1/0/1”，方向为“入方向”，单击“ ”按钮添加源端口。
- 远程镜像 VLAN 为“5”
- 配置 DeviceB 连接目的设备的接口为出端口：选择接口“GE1/0/2”。
- 单击<确定>按钮，提示设置成功，完成目的设备远程端口镜像组的创建。

图7 配置二层远程端口镜像组

(4) 保存配置

点击页面左上方标识和辅助区内的“  ”按钮保存配置。

2.4 验证配置

(1) 在 Device A 的“网络 > 镜像 > 端口镜像”页面中，可以查看到已配置的远程端口镜像信息。

图8 远程目的镜像组

(2) 在 Device B 的“网络 > 镜像 > 端口镜像”页面中，可以查看到已配置的远程端口镜像信息。

图9 远程源镜像组

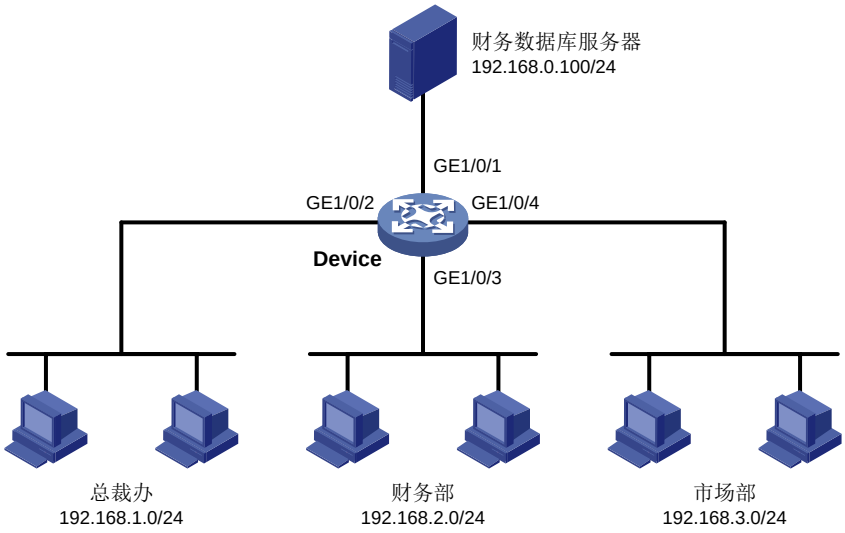
目 录

1 包过滤快速配置指南

1.1 组网需求

- 某公司内的各部门之间通过 Device 实现互连，该公司的工作时间为每周工作日的 8 点到 18 点。
- 通过配置，允许总裁办在任意时间、财务部在工作时间访问财务数据库服务器，禁止其它部门在任何时间、财务部在非工作时间访问该服务器。

表1 包过滤配置组网图



1.2 配置步骤

选择页面左侧导航栏的[安全/包过滤/包过滤]，进入“包过滤”配置页面，进行如下配置：

(1) 点击“+”按钮，进入“添加接口的包过滤策略”页面。

- 选择配置包过滤的接口为“GE1/0/1”。
- 选择“过滤出方向报文”。
- 选择包过滤规则为“IPv4 ACL”。
- 选择 ACL 规则。如果 ACL 规则已存在，则点击<确定>完成接口包过滤的配置；如果 ACL 规则不存在，继续点击右侧“+”按钮，进入添加“ACL 界面”。

图1 添加接口的包过滤策略

(2) 在“添加 ACL”界面选择 ACL 类型，本例选择 IPv4 ACL，点击<确定>按钮，进入“添加 IPv4 ACL”界面。

图2 添加 ACL

(3) 进入“添加 IPv4 ACL”界面，选择高级 ACL，输入 ACL 编号，规则匹配顺序、规则编号步长和描述可以根据需要修改，本例不做修改。默认勾选“开始添加规则”，点击<确定>按钮开始添加规则。

图3 添加 IPv4 ACL

(4) 配置总裁办访问规则

- 选择动作为“允许”。
- 选择 IP 协议类型为“ip”。
- 设置匹配条件源 IP 地址/通配符掩码为“192.168.1.0/0.0.0.255”。
- 设置目的 IP 地址/通配符掩码为“192.168.100.0/0.0.0.0”。
- 其它配置项使用缺省值。
- 点击<确定>按钮，完成总裁办访问规则配置，并继续添加规则。

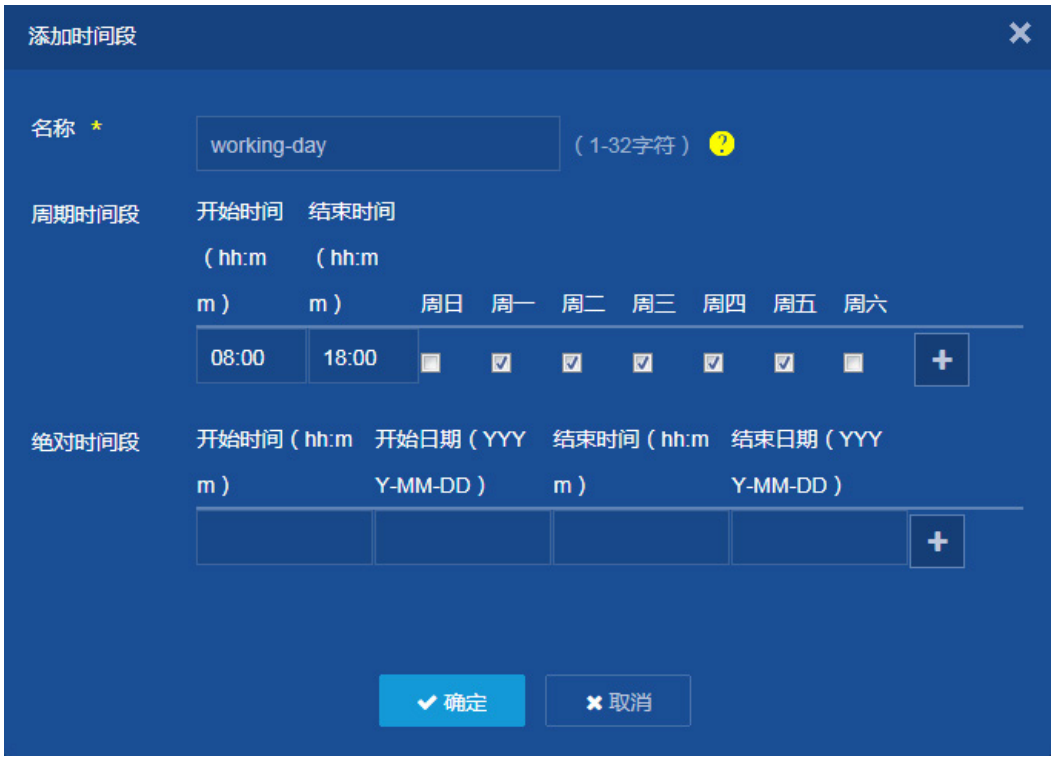
图4 配置总裁办访问规则

(5) 配置财务部生效的时间段。

在“添加 IPv4 高级 ACL 的规则”页面，点击“规则生效时间段”右侧的“+”按钮，进入“添加时间段”页面，进行如下配置。

- 输入时间段名称“working-day”。
- 配置周期时间段为工作日的 08:00-18:00，点击右侧的“+”按钮完成时间段的添加。
- 点击<确定>按钮，完成时间段的配置，继续添加财务部访问规则。

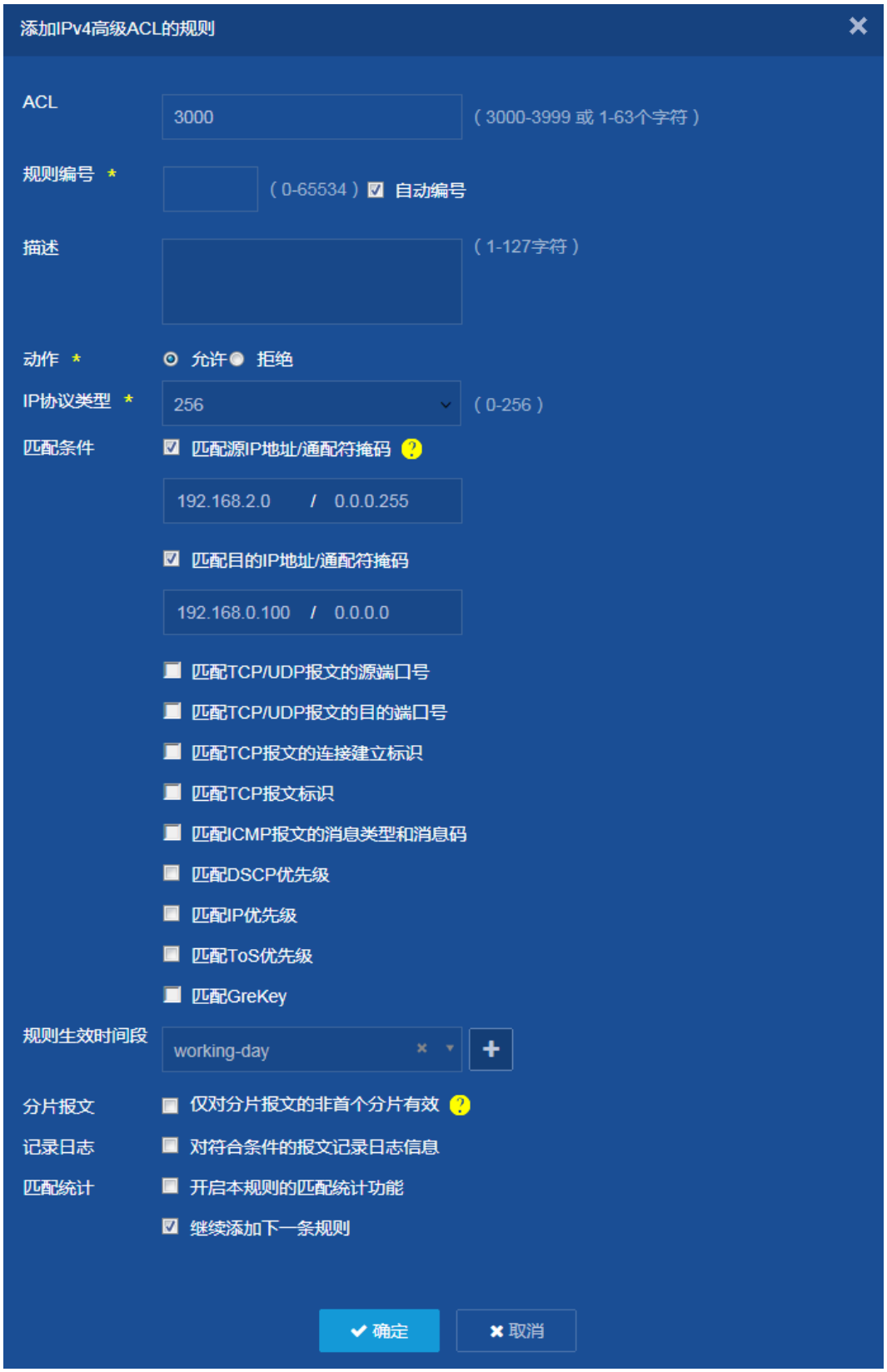
图5 配置时间段



(6) 配置财务部访问规则

- 选择动作为“允许”。
- 选择 IP 协议类型为“ip”。
- 设置匹配条件源 IP 地址/通配符掩码为“192.168.2.0/0.0.0.255”。
- 设置目的 IP 地址/通配符掩码为“192.168.100.0/0.0.0.0”。
- 选择规则生效的时间段为上一步中配置的“working-day”。
- 其它配置项使用缺省值。
- 点击<确定>按钮，完成财务部访问规则配置，并继续添加规则。

图6 配置财务部访问规则



(7) 配置其它部门访问规则。

- 选择动作为“拒绝”。
- 选择 IP 协议类型为“ip”。
- 设置匹配条件目的 IP 地址/通配符掩码为“192.168.100.0/0.0.0.0”。
- 取消勾选“继续添加下一跳规则”。
- 其它配置项使用缺省值。
- 点击<确定>按钮，完成其它部门访问规则配置。

图7 配置其它部门访问规则

(8) 点击<确定>按钮，完成接口包过滤的配置。

图8 接口包过滤策略信息

(9) 保存配置

点击页面左上方标识和辅助区内的“ ”按钮保存配置。

1.3 验证配置

配置完成后，在“安全 > 包过滤 > 包过滤”页面中，可以查看到已配置的包过滤信息。

图9 接口包过滤配置信息

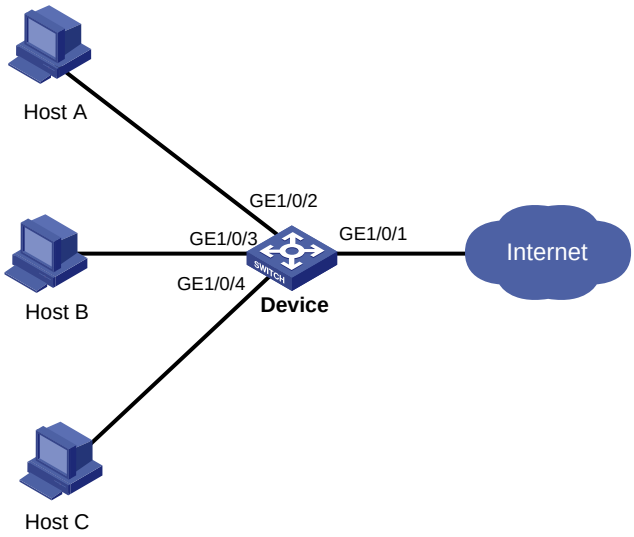
目 录

1 接口限速快速配置指南

1.1 组网需求

Device 为运营商的边缘设备，主机经该设备访问 Internet 网络时，为减少边缘设备对上层网络的冲击，建议在设备的 GE1/0/1 上配置出方向限速，限制访问 Internet 网络的总数据速率。

图1 接口限速配置组网图



1.2 配置步骤

(1) 配置接口限速

选择页面左侧导航栏的[QoS/QoS/限速]，进入“接口限速”配置页面，进行如下配置：

- 单击“ ”按钮，进入“添加接口限速”页面。
- 选择设备要进行限速的接口“GE1/0/1”。
- 选择方向为“出方向”，即对接口 GE1/0/1 发送的报文进行限速。
- 输入承诺信息速率 CIR 为“10240”。
- 承诺突发尺寸 CBS 为可选配置。当用户未配置该选项时，CBS 默认值为 62.5*CIR。本例中不配置该选项。
- 单击<确定>按钮，提示设置成功，完成限速配置。

图2 配置接口限速

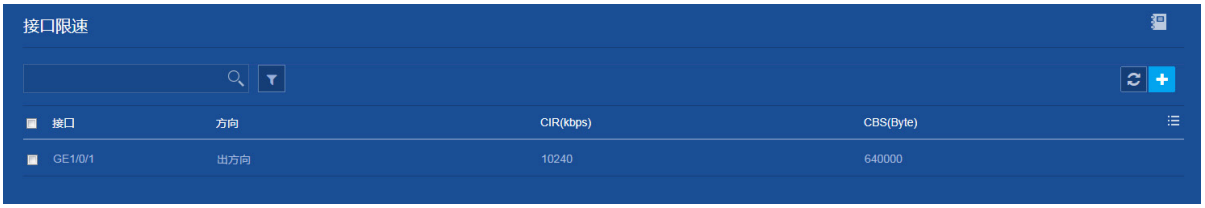
(2) 保存配置

点击页面左上方标识和辅助区内的“  ”按钮保存配置。

1.3 验证配置

配置完成后，在“QoS > QoS > 限速”页面中，可以查看到已配置的接口限速信息。

图3 接口限速配置信息



目 录

1 流量控制快速配置指南

1.1 组网需求

无。

1.2 配置注意事项

本功能不能和接口下的风暴抑制功能同时配置，以免导致抑制效果不确定。

1.3 配置步骤

(1) 选择页面左侧导航栏的[网络/接口/流量控制]，进入“流量控制”页面，如图 1 所示。

(2) 单击需要开启流量控制的接口，以 GigabitEthernet1/0/3 举例，进入“端口设置”页面。

图1 流量控制页面

(3) 在“端口设置”页面进行以下配置：

- 配置控制动作为“阻塞”。
- 配置广播流量阈值单位为“占接口最大速率的百分比”。
- 配置广播流量阈值上限为“80%”。
- 配置广播流量阈值下限为“20%”。
- 配置组播流量阈值单位为“占接口最大速率的百分比”。
- 配置组播流量阈值上限为“80%”。
- 配置组播流量阈值下限为“20%”。

- 配置未知单播流量阈值单位为“占接口最大速率的百分比”。
- 配置未知单播流量阈值上限为“80%”。
- 配置未知单播流量阈值下限为“20%”。
- 开启输出 Trap 功能。
- 开完输出日志功能。

图2 端口设置页面

(4) 保存配置

点击页面左上方标识和辅助区内的“  ”按钮保存配置。

1.4 验证配置

选择页面左侧导航栏的[网络/接口/流量控制]，选中 GigabitEthernet1/0/3 接口，单击“显示接口信息”按钮，查看流量控制配置信息。

图3 接口流量监控信息


接口流量监控信息
接口：GigabitEthernet1/0/3 描述：GigabitEthernet1/0/3 Interface
控制动作：阻塞
Trap输出：开启
日志输出：开启
广播阈值：20-80(%)
转发状态：转发
转发状态切换次数：0
组播阈值：20-80(%)
转发状态：转发
转发状态切换次数：0
未知单播阈值：20-80(%)
转发状态：转发
转发状态切换次数：0
确定

目 录

1 多生成树协议（MSTP）快速配置指南

1.1 组网需求

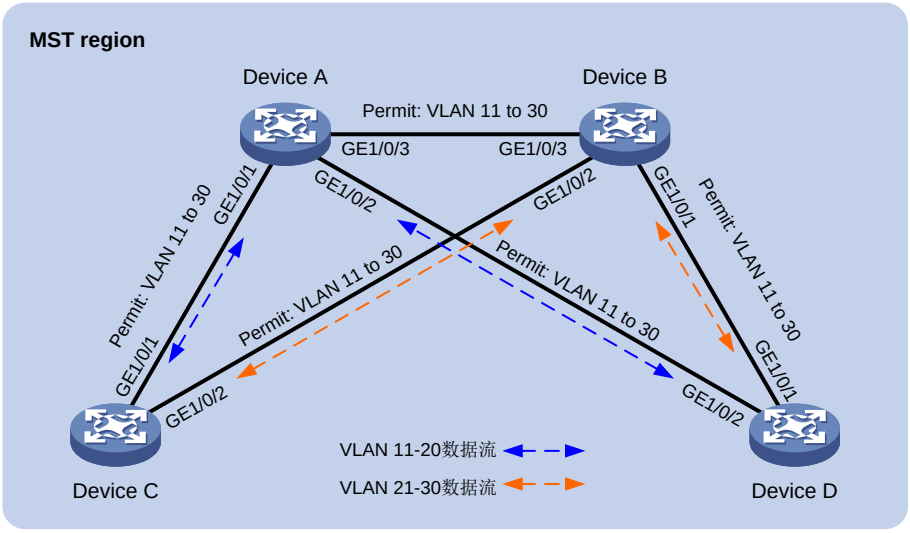
如 1.1 图 1 所示：

- 网络中所有设备都属于同一个 MST 域，设备的端口均允许 VLAN 11～30 通过。
- Device A 和 Device B 为核心层设备，Device C 和 Device D 为汇聚层设备。
- 假定所有端口路径开销相同。

要求通过配置 MSTP 功能，实现：

- 网络中无二层环路。
- Device C 和 Device D 的 VLAN 11～20 报文、VLAN 21～30 报文沿不同链路分别上行到 Device A 和 Device B，实现流量负载分担和链路备份。

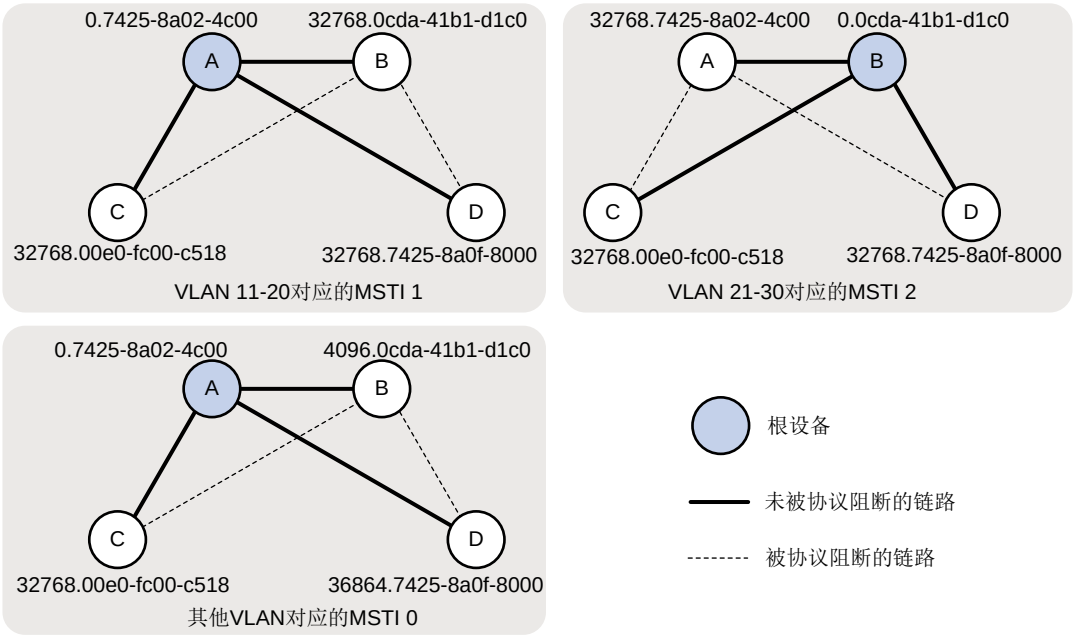
图1 MSTP 配置组网图



1.2 配置思路与数据规划

- 要使所有设备属于同一 MST 域，如下参数在所有设备上必须相同：
  - 生成树的工作模式（缺省为 MSTP 模式，无需配置）
  - 域名（本例配置为 TEST）
  - 修订级别（缺省为 0，无需配置）
  - VLAN 映射表（本例将 VLAN 11～20 映射到 MSTI 1，VLAN 21～30 映射到 MSTI 2）
- 为了使 MSTI 1 和 MSTI 2 拓扑中的上行链路不同并互相作为冗余备份，配置 Device A 为 MSTI 1 的根桥，Device B 为 MSTI 2 的根桥。另外，本例中配置 Device A、B、C、D 在 MSTI 0 的优先级依次降低，使 Device A 成为 IST 域根。形成的多个生成树实例拓扑如图 2 所示。

图2 各 VLAN 对应的生成树实例的拓扑



1.3 配置步骤

1. Device A 的配置

(1) 创建 VLAN 11～30。

选择页面左侧导航栏的[网络/链路/VLAN]，进入“VLAN”配置页面，进行如下配置：

- 点击“ ”按钮，进入“创建 VLAN”对话框。
- 配置 VLAN 列表为“11-30”。
- 单击<确定>按钮，完成 VLAN 的创建。

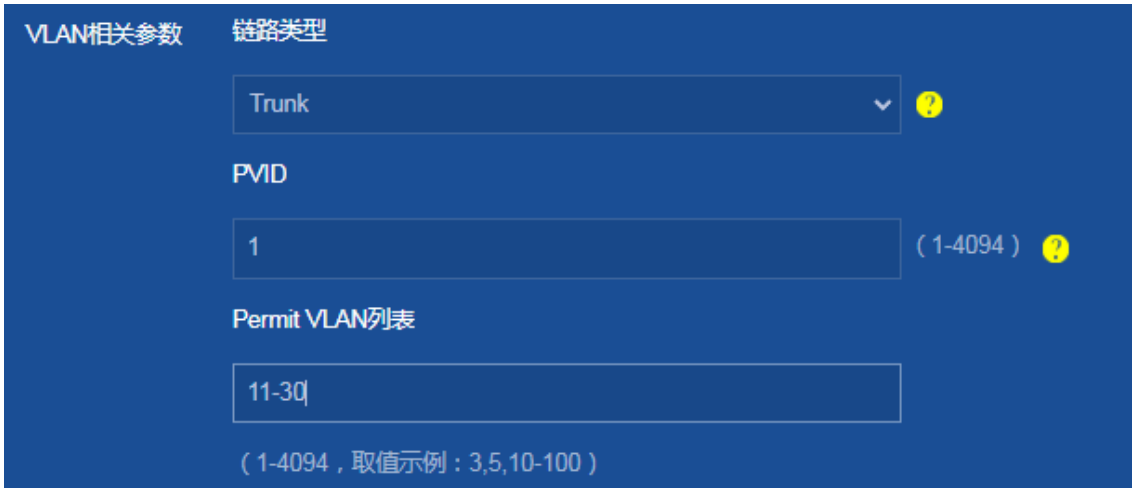
图3 创建 VLAN

(2) 配置设备的各端口为 Trunk 端口并允许 VLAN 11～30 通过。

选择页面左侧导航栏的[网络/接口/接口]，进入“接口”配置页面，进行如下配置：

- 点击 GE1/0/1 右侧“ ”按钮，进入“修改接口设置”页面。
- 设置链路类型为“Trunk”。
- 设置 Permit VLAN 列表为“11-30”。
- 单击<确定>按钮，提示设置成功，完成配置。
- 配置 GE1/0/2 和 GE1/0/3，相关参数和 GE1/0/1 相同，具体配置过程略。

图4 配置 VLAN 相关参数



(3) 开启 STP（默认 MSTP 模式）

选择页面左侧导航栏的[网络/链路/STP]，进入“STP”配置页面，进行如下配置：

- 点击<开启 STP>按钮，开启 STP。

图5 开启 STP

(4) 配置 MST 域的域名为 TEST 并配置 VLAN 与 MSTI 的映射关系

点击“域设置”右侧箭头，进入“多生成树域设置”页面，进行如下配置：

- 配置 MST 域的域名为“TEST”。
- 将 VLAN 11～20 分别映射到 MSTI 1 上。
- 将 VLAN 21～30 分别映射到 MSTI 2 上，并配置 MSTP 的修订级别为 0。
- 设置完成，返回“STP”页面。

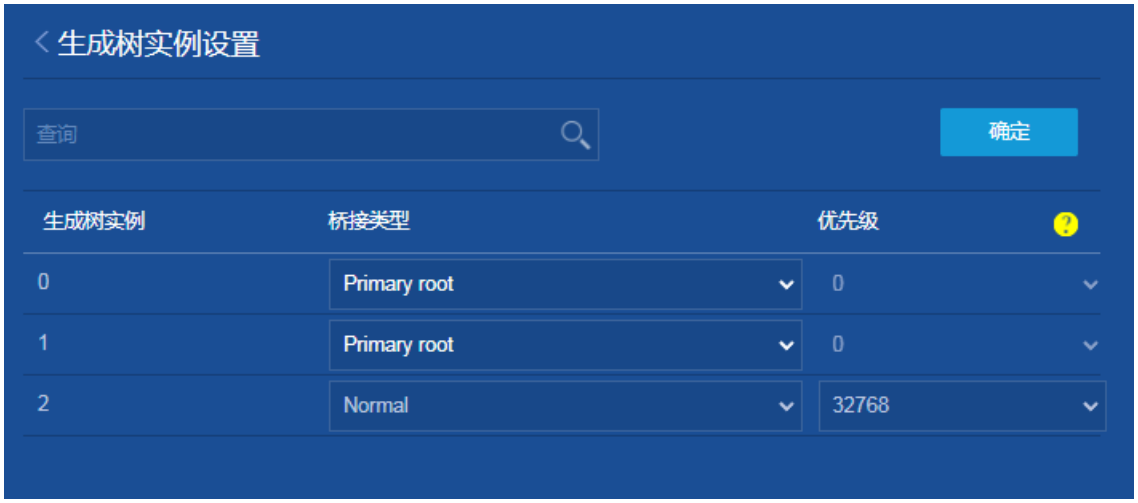
图6 多生成树域设置

(5) 配置本设备为 MSTI 0 和 MSTI 1 的根桥

点击“实例设置”右侧箭头，进入“生成树实例设置”页面，进行如下配置：

- 将 MSTI 0 的桥接类型设置为“Primary root”。
- 将 MSTI 1 的桥接类型设置为“Primary root”。
- 单击<确定>按钮，提示设置成功，完成根桥配置。

图7 生成树实例设置



(6) 保存配置

点击页面左上方标识和辅助区内的“ ”按钮保存配置。

2. Device B 的配置

(1) 创建 VLAN 11～30。

选择页面左侧导航栏的[网络/链路/VLAN]，进入“VLAN”配置页面，进行如下配置：

- 点击“ ”按钮，进入“创建 VLAN”对话框。
- 配置 VLAN 列表为“11-30”。
- 单击<确定>按钮，完成 VLAN 的创建。

(2) 配置设备的各端口为 Trunk 端口并允许 VLAN 11～30 通过。

选择页面左侧导航栏的[网络/接口/接口]，进入“接口”配置页面，进行如下配置：

- 点击 GE1/0/1 右侧“ ”按钮，进入“修改接口设置”页面。
- 设置链路类型为“Trunk”。
- 设置 Permit VLAN 列表为“11-30”。
- 单击<确定>按钮，提示设置成功，完成配置。
- 配置 GE1/0/2 和 GE1/0/3，相关参数和 GE1/0/1 相同，具体配置过程略。

(3) 开启 STP（默认 MSTP 模式）

选择页面左侧导航栏的[网络/链路/STP]，进入“STP”配置页面，进行如下配置：

- 点击<开启 STP>按钮，开启 STP。

(4) 配置 MST 域的域名为 TEST 并配置 VLAN 与 MSTI 的映射关系

点击“域设置”右侧箭头，进入“多生成树域设置”页面，进行如下配置：

- 配置 MST 域的域名为“TEST”。
- 将 VLAN 11～20 分别映射到 MSTI 1 上。

- 将 VLAN 21～30 分别映射到 MSTI 2 上，并配置 MSTP 的修订级别为 0。
- 设置完成，返回“STP”页面。

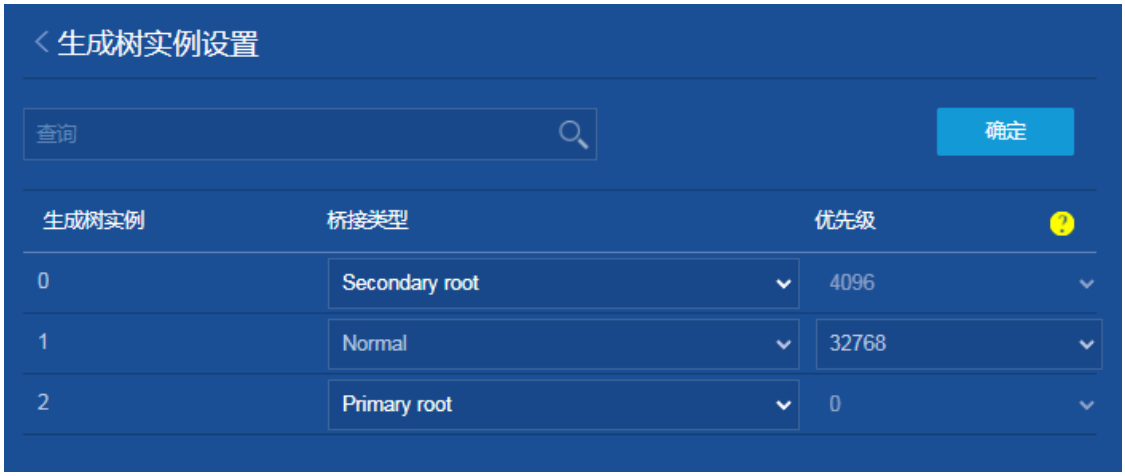
图8 多生成树域设置

(5) 配置本设备为 MSTI 2 的根桥，以及 MSTI 0 的备份根桥

点击“实例设置”右侧箭头，进入“生成树实例设置”页面，进行如下配置：

- 将 MSTI 0 的桥接类型设置为“Secondary root”。
- 将 MSTI 2 的桥接类型设置为“Primary root”。
- 单击<确定>按钮，提示设置成功，完成根桥配置。

图9 生成树实例设置



(6) 保存配置

点击页面左上方标识和辅助区内的“ ”按钮保存配置。

3. Device C 的配置

(1) 创建 VLAN 11～30。

选择页面左侧导航栏的[网络/链路/VLAN]，进入“VLAN”配置页面，进行如下配置：

- 点击“ ”按钮，进入“创建 VLAN”对话框。
- 配置 VLAN 列表为“11-30”。
- 单击<确定>按钮，完成 VLAN 的创建。

(2) 配置设备的各端口为 Trunk 端口并允许 VLAN 11～30 通过。

选择页面左侧导航栏的[网络/接口/接口]，进入“接口”配置页面，进行如下配置：

- 点击 GE1/0/1 右侧“ ”按钮，进入“修改接口设置”页面。
- 设置链路类型为“Trunk”。
- 设置 Permit VLAN 列表为“11-30”。
- 单击<确定>按钮，提示设置成功，完成配置。
- 配置 GE1/0/2，相关参数和 GE1/0/1 相同，具体配置过程略。

(3) 开启 STP（默认 MSTP 模式）

选择页面左侧导航栏的[网络/链路/STP]，进入“STP”配置页面，进行如下配置：

- 点击<开启 STP>按钮，开启 STP。

(4) 配置 MST 域的域名为 TEST 并配置 VLAN 与 MSTI 的映射关系

点击“域设置”右侧箭头，进入“多生成树域设置”页面。

- 配置 MST 域的域名为“TEST”。
- 将 VLAN 11～20 分别映射到 MSTI 1 上。

- 将 VLAN 21～30 分别映射到 MSTI 2 上，并配置 MSTP 的修订级别为 0。
- 设置完成，返回“STP”页面。

图10 多生成树域设置

(5) 保存配置

点击页面左上方标识和辅助区内的“ ”按钮保存配置。

4. Device D 的配置

(1) 创建 VLAN 11～30。

选择页面左侧导航栏的[网络/链路/VLAN]，进入“VLAN”配置页面，进行如下配置：

- 点击“ ”按钮，进入“创建 VLAN”对话框。
- 配置 VLAN 列表为“11-30”。
- 单击<确定>按钮，完成 VLAN 的创建。

(2) 配置设备的各端口为 Trunk 端口并允许 VLAN 11～30 通过。

选择页面左侧导航栏的[网络/接口/接口]，进入“接口”配置页面，进行如下配置：

- 点击 GE1/0/1 右侧“ ”按钮，进入“修改接口设置”页面。
- 设置链路类型为“Trunk”。

- 设置 Permit VLAN 列表为“11-30”。
- 单击<确定>按钮，提示设置成功，完成配置。
- 配置 GE1/0/2，相关参数和 GE1/0/1 相同，具体配置过程略。

(3) 开启 STP（默认 MSTP 模式）

选择页面左侧导航栏的[网络/链路/STP]，进入“STP”配置页面，进行如下配置：

- 点击<开启 STP>按钮，开启 STP。

(4) 配置 MST 域的域名为 TEST 并配置 VLAN 与 MSTI 的映射关系

点击“域设置”右侧箭头，进入“多生成树域设置”页面，进行如下配置：

- 配置 MST 域的域名为“TEST”。
- 将 VLAN 11～20 分别映射到 MSTI 1 上。
- 将 VLAN 21～30 分别映射到 MSTI 2 上，并配置 MSTP 的修订级别为 0。
- 设置完成，返回“STP”页面。

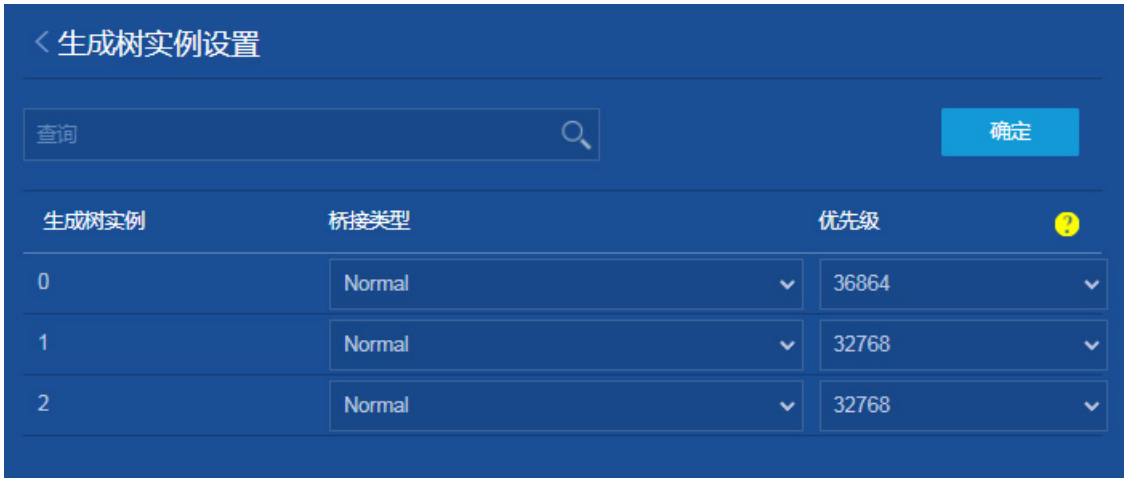
图11 多生成树域设置

(5) 配置本设备在 MSTI 0 的优先级为 36864，从而使本设备在 MSTI 0 的优先级低于 Device C（Device C 使用缺省优先级 32768）。

点击“实例设置”右侧箭头，进入“生成树实例设置”页面，进行如下配置：

- 将 MSTI 0 的优先级设置为“36864”。
- 单击<确定>按钮，提示设置成功，完成根桥配置。

图12 生成树实例设置



(6) 保存配置

点击页面左上方标识和辅助区内的“  ”按钮保存配置。

1.4 验证配置

(1) 查看生成树实例拓扑信息

完成上述配置后，在端口实例信息中可以查看各个接口的端口角色、端口状态等信息。

(2) 验证链路备份功能

关闭 Device C 的端口 GigabitEthernet1/0/1（这是 Device C 在 MSTI 0～1 中的上行链路所在端口）。在 Device C 的端口实例信息中可以看到 MSTI 0～1 中的上行链路所在端口已从原先的 GE1/0/1 切换为 GE1/0/2。

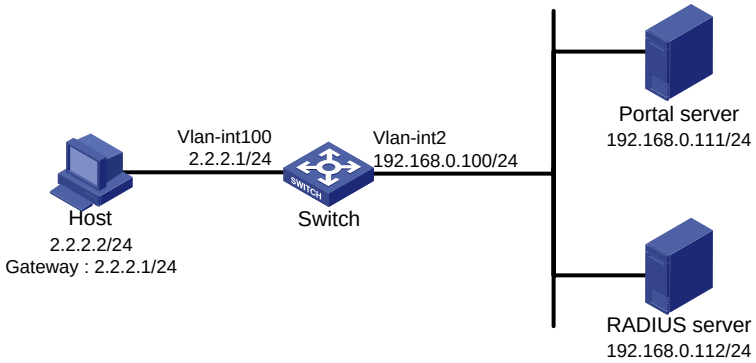
目 录

1 Portal 直接认证快速配置指南

1.1 组网需求

- 用户主机与接入设备 Switch 直接相连，采用直接方式的 Portal 认证。用户通过手工配置或 DHCP 获取的一个公网 IP 地址进行认证，在通过 Portal 认证前，只能访问 Portal Web 服务器；在通过 Portal 认证后，可以使用此 IP 地址访问非受限互联网资源。
- 采用一台 Portal 服务器承担 Portal 认证服务器和 Portal Web 服务器的职责。
- 采用 RADIUS 服务器作为认证/计费服务器。

图1 Portal 直接认证组网图



1.2 配置步骤

1. 配置 Portal server

配置 Portal server，具体配置步骤略。

2. 配置 Switch

(1) 配置 RADIUS 方案

选择页面左侧导航栏的[安全/认证/RADIUS]页面，进入“RADIUS 方案”配置页面，进行如下配置：

- 点击右上角的“ ”按钮，添加 RADIUS 方案。
- 配置方案名称为“rs1”。
- 指定主认证服务器 IP 地址为“192.168.0.112”，端口号为“1812”，共享密钥为“radius”。设置主认证服务器状态为“活动”，点击右侧的“ ”按钮完成添加。
- 指定主计费服务器 IP 地址为“192.168.0.112”，端口号为“1813”，共享密钥为“radius”。设置主计费服务器状态为“活动”，点击右侧的“ ”按钮完成添加。

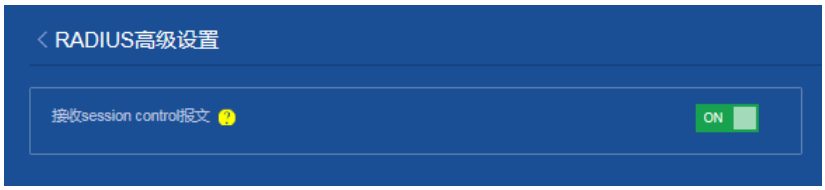
图2 添加 RADIUS 方案

- 点击“显示高级设置”。
- 指定发送给 RADIUS 服务器的用户名格式为“不携带域名”。
- 单击<确定>按钮，提示设置成功，完成 RADIUS 方案的添加。

图3 添加 RADIUS 方案

- 点击“RADIUS”配置页面右上角的“ ”按钮，进入“RADIUS 高级设置”页面，在该页面上开启接收 session-control 报文功能。

图4 RADIUS 高级设置



(2) 配置 ISP 域

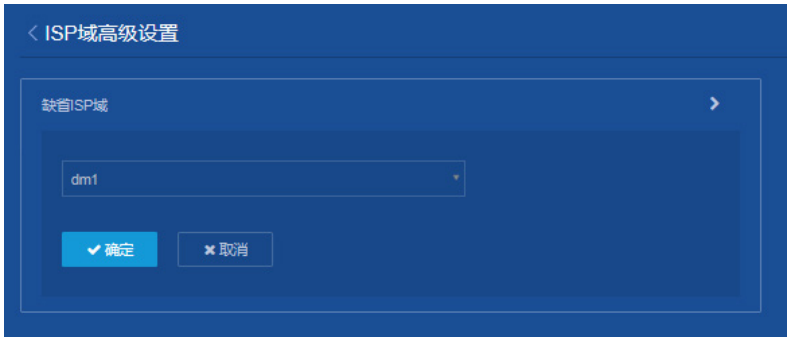
选择页面左侧导航栏的[安全/认证/ISP 域]页面，进入“ISP 域”配置页面，进行如下配置：

- 点击右上角的“ ”按钮，添加 ISP 域。
- 配置域名为“dm1”，并将该 ISP 域的状态设置为“活动”。
- 指定接入方式为“Portal”。
- 指定 Portal 接入 AAA 方案的认证、授权和计费的方法均为“RADIUS”，方案都选择“rs1”。
- 单击<确定>按钮，提示设置成功，完成 ISP 域的添加。

图5 添加 ISP 域

- 点击“ISP 域”配置页面右上角的“”按钮，进入“ISP 域高级设置”页面。在该页面上指定系统缺省的 ISP 域为“dm1”，所有接入用户共用此缺省域的认证和计费方法。若用户登录时输入的用户名未携带 ISP 域名，则使用缺省域下的认证方法。
- 单击<确定>按钮，提示设置成功，完成“ISP 域高级设置”。

图6 ISP 域高级设置



(3) 配置 VLAN 和 VLAN 接口

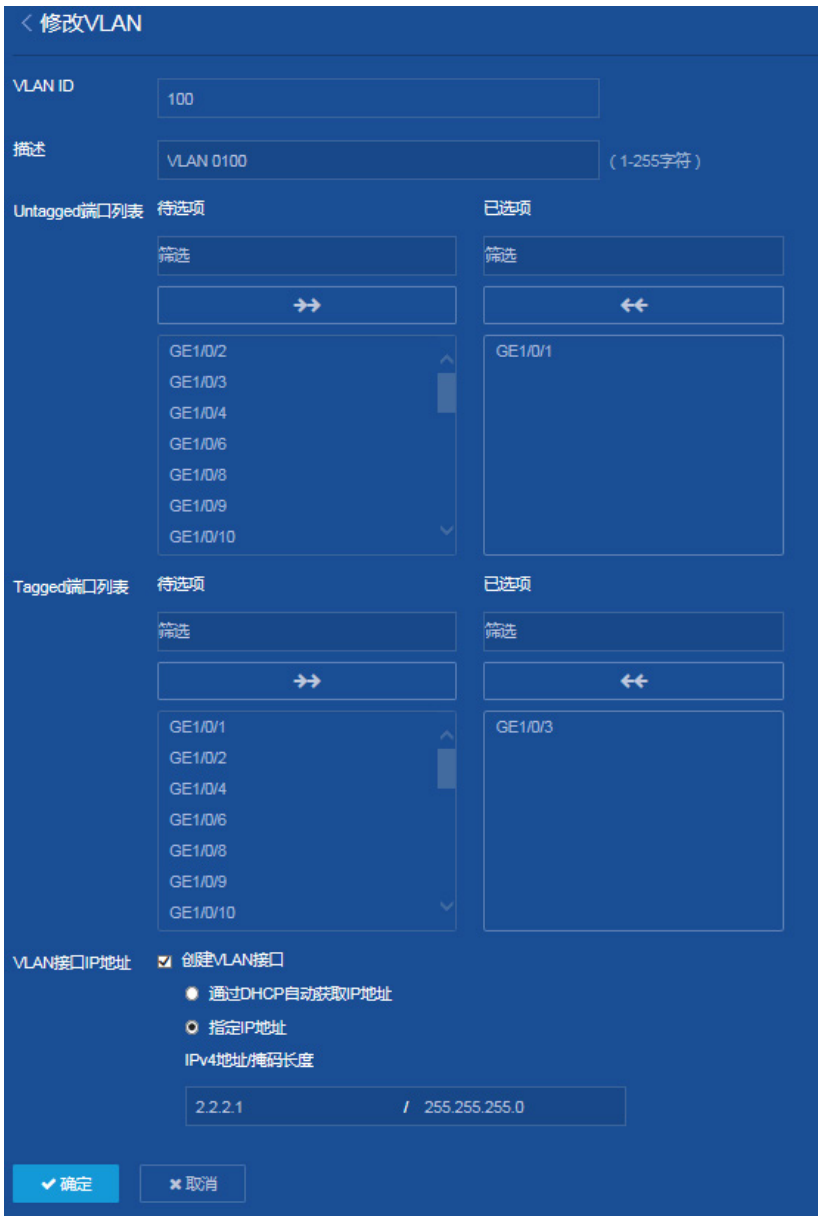
选择页面左侧导航栏的[网络/链路/VLAN]页面，进入“VLAN”配置页面，进行如下配置：

- 点击右上角的“”按钮，创建 VLAN 100，单击<确定>按钮。

图7 创建 VLAN

- 点击 VLAN 100 右侧的“ ”按钮，进入“修改 VLAN”页面。
- 将和用户主机和 Switch 相连的接口 GE1/0/1 加入 VLAN100 的 Untagged 端口列表。
- 在 VLAN 接口 IP 地址处勾选“创建 VLAN 接口”，配置 VLAN 接口的 IP 地址为“2.2.2.1”，子网掩码为 “255.255.255.0”。
- 单击<确定>按钮，提示设置成功，完成 VLAN 和 VLAN 接口的创建。

图8 配置 VLAN 和 VLAN 接口



- 完成 VLAN2 和 VLAN 接口的创建，具体配置步骤略。

(4) 配置 Portal 认证

选择页面左侧导航栏的[安全/接入/Portal]页面，进入“Portal”配置页面，进行如下配置：

- 点击“Portal 认证服务器”右侧的“ ”按钮，进入“Portal 认证服务器”配置页面。

图9 Portal

图10 Portal 认证服务器

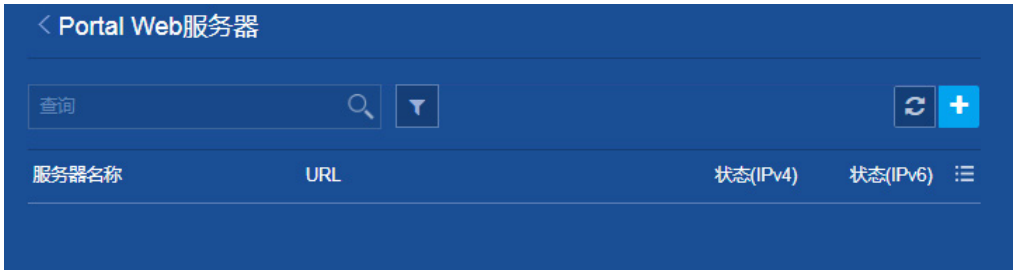
- 点击右上角的“  ”按钮，进入“创建 Portal 认证服务器”配置页面。
- 添加 Portal 认证服务器：名称为“newpt”，IP 地址为“192.168.0.111”，共享密钥为“portal”，服务器监听端口号为“50100”。
- 单击<确定>按钮，提示配置成功，完成 Portal 认证服务器的创建。

图11 创建 Portal 认证服务器

- 返回“Portal”配置页面。
- 点击“Portal Web 服务器”右侧的“ ”按钮，进入“Portal Web 服务器”配置页面。

图12 Portal

图13 Portal Web 服务器



- 点击右上角的“ ”按钮，进入“创建 Portal Web 服务器”配置页面。
- 添加 Portal Web 服务器：配置服务器名称为“newpt”、URL 为“http://192.168.0.111:8080/portal”。（Portal Web 服务器的 URL 请与实际环境中的 Portal Web 服务器配置保持一致，此处仅为示例）。
- 单击<确定>按钮，提示配置成功，完成 Portal Web 服务器的创建。

图14 创建 Portal Web 服务器

- 返回“Portal”配置页面。
- 点击“接口策略”右侧的“ ”按钮，进入“接口策略”配置页面。

图15 Portal

图16 接口策略

- 添加接口策略：选择 Vlan-interface100 接口，选择 IPv4 Portal 认证方式为“直接认证”，引用 Portal Web 服务器为“newpt”，BAS-IP 地址为“2.2.2.1”。
- 单击<确定>按钮，提示配置成功，完成接口策略的创建。

图17 创建接口策略

(5) 保存配置

点击页面左上方标识和辅助区内的“  ”按钮保存配置。

3. 配置 RADIUS 服务器

在 RADIUS 服务器上添加用户帐户，保证用户的认证/授权/计费功能正常运行。具体配置方法请参考关于 RADIUS 服务器的配置说明。

1.3 验证配置

(1) 在[安全/认证/RADIUS]页面上，可以看到已添加成功的 RADIUS 方案 rs1 的概要信息。

(2) 在[安全/认证/ISP 域]页面上，可以看到已添加成功的 ISP 域的 dm1 的概要信息。

(3) 用户 Portal 认证成功上线后，在[安全/接入/Portal]页面中，可以在“在线用户信息”中查看接口 Vlan-interface100 的当前用户数。

目 录

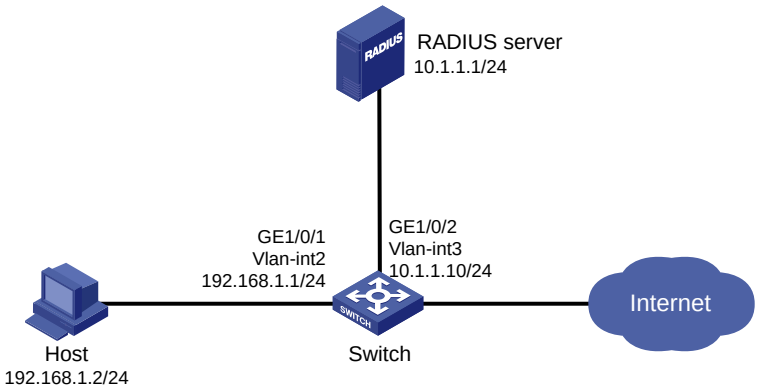
1 端口安全快速配置指南

1.1 组网需求

用户通过 Switch 的端口 GigabitEthernet1/0/1 接入网络，Switch 对该端口接入的用户进行端口安全认证以控制其访问 Internet，具体要求如下：

- RADIUS 服务器作为认证/授权/计费服务器与 Switch 相连，其 IP 地址为 10.1.1.1/24。
- 端口 GigabitEthernet1/0/1 上同时允许一个 802.1X 用户以及一个与指定 OUI 值匹配的设备接入。
- Switch 对 802.1X 用户进行认证时，采用 RADIUS 认证方式，认证 ISP 域为 portsec。
- Switch 与 RADIUS 认证/授权和计费服务器交互报文时的共享密钥均为 name，认证/授权、计费的端口号分别为 1812 和 1813，向 RADIUS 服务器发送的用户名不携带域名。
- 添加 5 个 OUI 值，分别为：1234-0100-1111、1234-0200-1111、1234-0300-1111、1234-0400-1111 和 1234-0500-1111。系统会自动取输入的前 24 位作为 OUI 值，忽略后 24 位。

图1 端口安全用户的 RADIUS 认证配置组网图



1.2 配置注意事项

OUI 值只在端口安全模式为 userLoginWithOUI 时生效。在 userLoginWithOUI 模式下，端口上除了允许一个 802.1X 认证用户接入之外，还额外允许一个特殊用户接入，该用户报文的源 MAC 地址的 OUI 与设备上配置的某个 OUI 值相符。

1.3 配置步骤

1. 配置各接口的 IP 地址（略）

2. 配置 Switch

(1) 配置 RADIUS 方案

选择页面左侧导航栏[安全/认证/RADIUS]，进入“RADIUS 方案”配置页面，进行如下配置：

- 点击右上角“ ”按钮，添加 RADIUS 方案。

- 配置方案名称为“portsec”。
- 指定主认证服务器 IP 地址为“10.1.1.1”，端口号为“1812”，共享密钥为“name”。设置主认证服务器状态为“活动”，点击右侧的“+”按钮完成添加。
- 指定主计费服务器 IP 地址为“10.1.1.1”，端口号为“1813”，共享密钥为“name”。设置主计费服务器状态为“活动”，点击右侧的“+”按钮完成添加。

图2 添加 RADIUS 方案

- 点击“显示高级设置”。
- 指定发送给 RADIUS 服务器的用户名格式为“不携带域名”。
- 单击<确定>按钮，提示设置成功，完成 RADIUS 方案的添加。

图3 添加 RADIUS 方案

(2) 在 Switch 上配置 ISP 域

选择页面左侧导航栏[安全/认证/ISP 域]，进入“ISP 域”配置页面，进行如下配置：

- 点击右上角“ ”按钮，添加 ISP 域
- 配置域名为“portsec”，并将该 ISP 域的状态设置为活动。
- 指定接入方式为“LAN 接入”。
- 指定 LAN 接入 AAA 方案的认证、授权和计费的方法均为“RADIUS”，方案都选择“portsec”。
- 单击<确定>按钮，提示设置成功，完成 ISP 域的添加。

图4 添加 ISP 域

(3) 在 Switch 上配置端口安全

选择页面左侧导航栏[安全/接入/端口安全]，进入“端口安全”配置页面，进行如下配置：

- 点击“开启端口安全”按钮，开启 Switch 的端口安全认证功能。
- 点击端口 GigabitEthernet1/0/1 右侧的“高级设置”按钮，进入“端口高级设置”配置页面，指定认证模式为“userLoginWithOUI”。
- 在端口 GigabitEthernet1/0/1 的“高级设置”配置页面上的 802.1X 标签下，指定 802.1X 用户使用的端口的强制认证 ISP 域为“portsec”。
- 单击<确定>按钮，提示设置成功，完成端口 GE1/0/1 的高级设置。

图5 端口高级设置

- 点击“端口安全”配置页面右上角的“ ”按钮，进入端口安全的“高级设置”页面，在认证 OUIMAC 中添加 5 个 OUI 值，分别为：1234-0100-1111、1234-0200-1111、1234-0300-1111、1234-0400-1111 和 1234-0500-1111。

图6 端口安全高级设置

(4) 保存配置

点击页面左上方标识和辅助区内的“ ”按钮保存配置。

3. 配置 RADIUS 服务器

在 RADIUS 服务器上添加用户帐户，保证用户的认证/授权/计费功能正常运行。具体配置方法请参考关于 RADIUS 服务器的配置说明。

1.4 验证配置

(1) 在[安全/认证/RADIUS]页面上，可以看到已添加成功的 RADIUS 方案 portsec 的概要信息。

(2) 在[安全/认证/ISP 域]页面上，可以看到已添加成功的 ISP 域的 portsec 的概要信息。

(3) 802.1X 用户上线后，在[安全/接入/端口安全]页面中，可以查看接口 GigabitEthernet1/0/1 的当前用户数为 1。

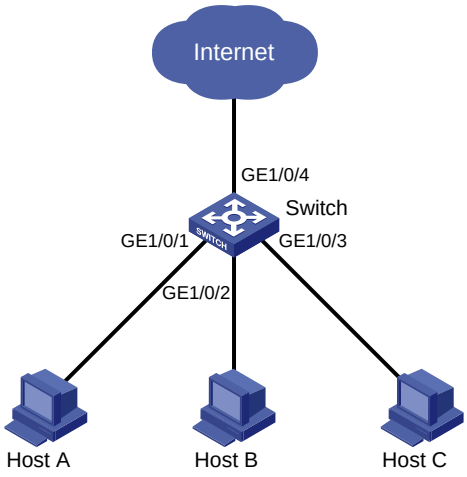
目 录

1 端口隔离快速配置指南

1.1 组网需求

小区用户 Host A、Host B、Host C 分别与 Switch 的端口 GigabitEthernet1/0/1、GigabitEthernet1/0/2、GigabitEthernet1/0/3 相连，Switch 通过 GigabitEthernet1/0/4 端口与外部网络相连。现需要实现小区用户 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。

图1 端口隔离配置组网图



1.2 配置步骤

(1) 配置端口隔离

选择页面左侧导航栏的[网络/接口/端口隔离]，进入“端口隔离”配置页面，进行如下配置：

- 点击“ ”按钮，进入“创建隔离组”页面。
- 配置隔离组 ID 为“2”。
- 接口列表添加“GE1/0/1”、“GE1/0/2”、“GE1/0/3”.
- 单击<确定>按钮，提示设置成功，完成配置。

图2 创建端口隔离组，并添加隔离端口

(2) 保存配置

点击页面左上方标识和辅助区内的“  ”按钮保存配置。

1.3 验证配置

完成上述配置后，Switch 的 GigabitEthernet1/0/1、GigabitEthernet1/0/2、GigabitEthernet1/0/3 之间实现二层隔离，Host A、Host B 和 Host C 彼此之间不能 ping 通。

目 录

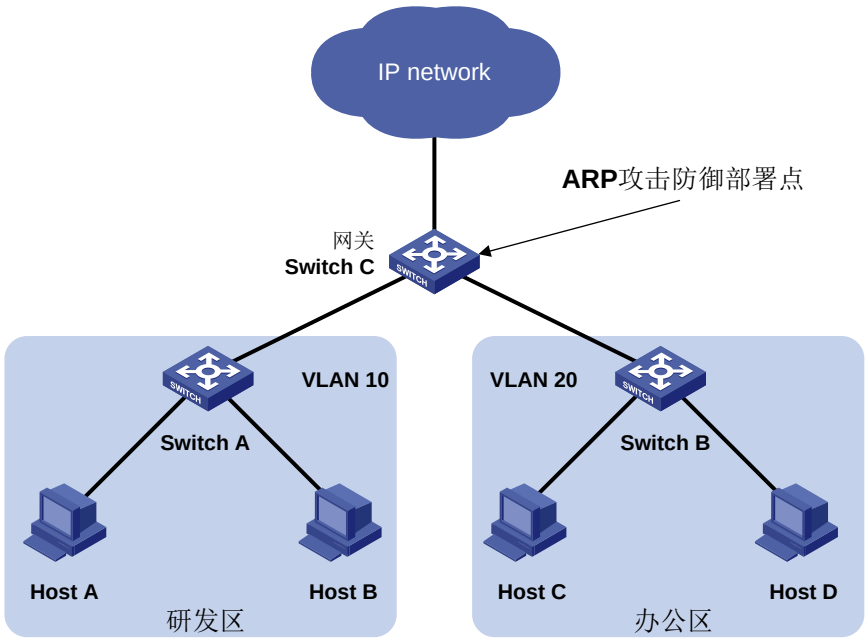
1 ARP 防 IP 报文攻击快速配置指南

1.1 组网需求

某局域网内存在两个区域：研发区和办公区，分别属于 VLAN 10 和 VLAN 20，通过接入交换机连接到网关 Device，如图 1 所示。

网络管理员在监控网络时发现办公区存在大量 ARP 请求报文，通过分析认为存在 IP 泛洪攻击，为避免这种 IP 报文攻击所带来的危害，可采用 ARP 源抑制功能和 ARP 黑洞路由功能。

图1 ARP 防止 IP 报文攻击配置组网图



1.2 配置思路

- 如果发送攻击报文的源 IP 地址是不固定的，可配置 ARP 黑洞路由功能。
- 如果发送攻击报文的源 IP 地址是固定的，可配置 ARP 源抑制功能，并配置源抑制的阈值。当固定时间内（5 秒）ARP 请求报文的流量超过阈值后，对于由此 IP 地址发出的 IP 报文，设备不允许其触发 ARP 请求，直至 5 秒后再处理。

1.3 配置步骤

(1) 开启 ARP 黑洞路由功能

进入 Switch C 配置界面，选择页面左侧导航栏的[网络/IP/ARP]，进入“ARP”配置页面，进行如下配置。

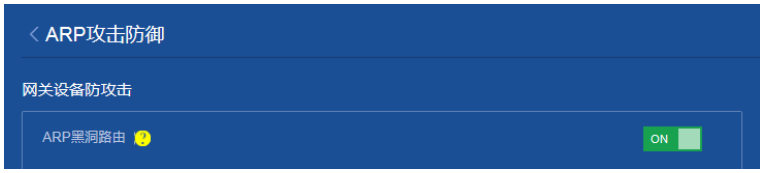
- 在右侧点击“ ”高级设置，进入“ARP 高级设置”页面。

- 在“ARP 高级设置”页面，点击“ARP 攻击防御”，进入“ARP 攻击防御”配置页面。

图2 进入 ARP 攻击防御配置页面

- 在“ARP 攻击防御”配置页面，开启“ARP 黑洞路由”功能。

图3 开启 ARP 黑洞路由功能



(2) 配置 ARP 源抑制功能

在“ARP 攻击防御”配置页面，开启“ARP 源抑制”功能，并配置源抑制的阈值为 100。

图4 开启 ARP 源抑制功能并配置 ARP 源抑制的阈值

(3) 保存配置

点击页面左上方标识和辅助区内的“  ”按钮保存配置。

1.4 验证配置

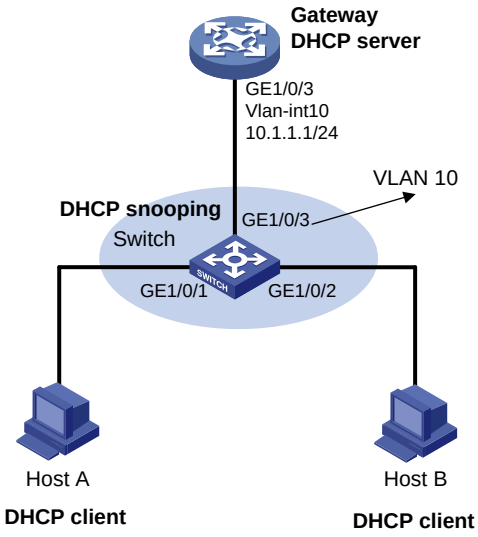
完成上述配置后，Switch C 的端口收到某 IP 地址向设备某接口发送目的 IP 地址不能解析的 IP 报文超过了设置的阈值，则设备将不再处理由此 IP 地址发出的 IP 报文直至该 5 秒结束；非固定 IP 地址发送的不能解析的 IP 报文，会产生黑洞路由，丢弃报文。

2 ARP Detection 快速配置指南

2.1 组网需求

- 网络中 Device 为一台 DHCP 服务器；Host A 和 Host B 是 DHCP 客户端。
- Switch 是 DHCP Snooping 设备，在 VLAN 10 内配置 ARP Detection 功能，对 DHCP 客户端和用户进行用户合法性检查和报文有效性检查。

图5 ARP Detection 组网图



2.2 配置步骤

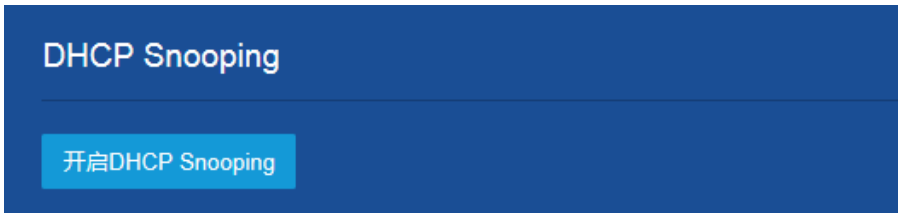
(1) 配置 DHCP 服务器和 DHCP client（略）

(2) 配置 Switch 的 DHCP snooping 功能

进入 Switch 配置界面，选择页面左侧导航栏的[网络/链路/DHCP Snooping]，进入“DHCP Snooping”配置页面，进行如下配置。

- 开启“DHCP Snooping”功能。

图6 开启 DHCP snooping 功能



- 配置连接合法 DHCP 服务器的接口 GigabitEthernet1/0/3 为信任接口。
- 配置连接 DHCP Client 的接口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 开启 DHCP Snooping 表项记录功能。

- 点击<确定>按钮，完成信任端口和 DHCP Snooping 表项记录功能的配置。

图7 配置 DHCP snooping 信任端口和表项记录功能

- 点击右上角的“ ”，进入“DHCP Snooping 高级设置”页面。
- 在高级设置页面，配置 DHCP Snooping 设备的表项备份功能：将 DHCP Snooping 表项备份到本地，并命名为“dhcp snooping binding record-001”。

图8 将 DHCP Snooping 表项备份到本地

(3) 开启 Switch 的 ARP Detection 功能

进入 Switch 配置界面，选择页面左侧导航栏的[网络/IP/ARP]，进入“ARP”配置页面，进行如下配置。

- 点击右上角的“  ”，进入“ARP 高级设置”页面。
- 点击“ARP 攻击防御”，进入“ARP 攻击防御”配置页面。

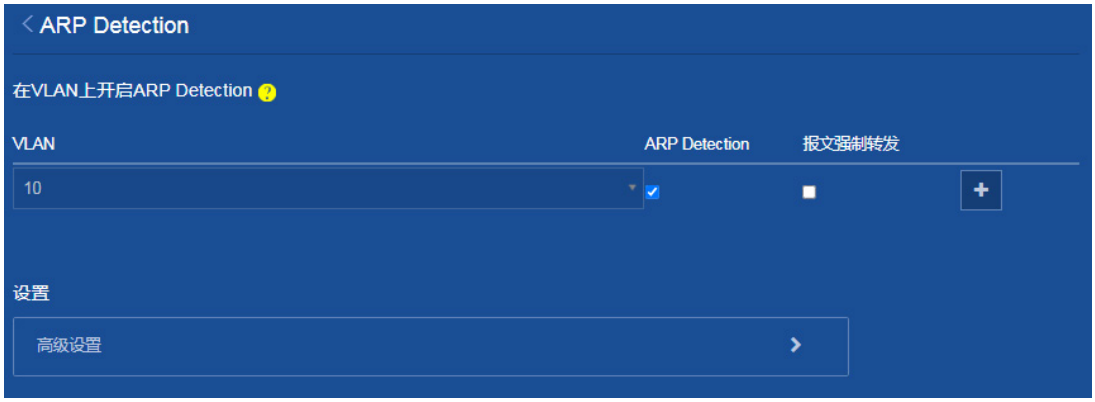
图9 进入 ARP 攻击防御配置页面

- 从“ARP 攻击防御”配置页面的接入设备防攻击区域，进入“ARP Detection”配置页面。

图10 进入 ARP Detection 配置页面

- 在“ARP Detection”配置页面，选择开启 ARP Detection 功能的 VLAN，点击右侧的“  ”按钮完成配置。

图11 在 VLAN 内开启 ARP Detection 功能



- 在“ARP Detection”配置页面，选择高级设置，进入“ARP Detection 高级设置”页面。
- 开启 ARP 报文有效性检查，选择检查模式为同时开启源 MAC 地址的检查、目的 MAC 地址的检查和 IP 地址检查。

图12 配置 ARP 报文有效性检查

- 在“ARP Detection 高级设置”页面，将连接 DHCP 服务器的接口 GigabitEthernet1/0/3 设置为 ARP Detection 信任接口，点击右侧的“ ”按钮完成配置。

图13 配置 ARP Detection 信任接口

(4) 保存配置

点击页面左上方标识和辅助区内的“ ”按钮保存配置。

2.3 验证配置

完成上述配置后，对于接口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 收到的 ARP 报文，先进行报文有效性检查，然后基于 DHCP Snooping 安全表项进行用户合法性检查。

目 录

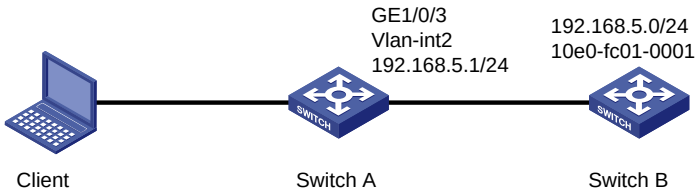
1 手工添加静态 ARP 表项快速配置指南

1.1 组网需求

为了增加Switch A与Switch B之间通信的安全性，可以在两台交换机之间配置一条静态ARP表项，从而防止攻击报文修改此表项的 IP 地址和 MAC 地址对应关系。

如图 1 所示，Switch A 通过下行口连接主机，通过接口 GigabitEthernet1/0/3 连接 Switch B，GigabitEthernet1/0/3 属于 VLAN 2，IP 地址为 192.168.5.1/24。Switch B 接口的 IP 地址为 192.168.5.0，MAC 地址为 10e0-fc01-0001。

图1 配置 ARP 静态表项组网图



1.2 配置步骤

1. 配置 Switch A

(1) 配置 VLAN

进入 Switch A 的 Web 配置界面，选择页面左侧导航栏的[网络/链路/VLAN]，进入“VLAN”配置页面，进行如下配置：

- 单击右上角“ ”按钮，添加 VLAN。

图2 创建 VLAN 2

- 在 VLAN 界面中新创建的 VLAN 2 点击“ ”，进入“修改 VLAN”界面。

- 将 GE1/0/3 接口加入到 VLAN 2 的 Tagged 端口列表里。
- 在修改 VLAN 界面下方“VLAN 接口 IP 地址”选择“指定 IP 地址”。配置 VLAN 2 接口地址为“192.168.5.1”，掩码为“255.255.255.0”。
- 单击<确定>按钮，提示设置成功，完成 VLAN 的配置。

图3 修改 VLAN

(2) 添加静态 ARP 表项

返回交换机配置主界面，选择页面左侧导航栏的[网络/IP/ARP]，进入“ARP”界面，进行如下配置：

- 点击右上角“  ”，添加静态 ARP 表项。
- 将 IP 地址设置为：192.168.5.1，MAC 地址设置为 10e0-fc01-0001，
- VLAN 接口设置为 2,接口设置为 GE1/0/3。

图4 添加静态 ARP 表项

(3) 保存配置

点击页面左上方标识和辅助区内的“  ”按钮保存配置。

2. 配置 Switch B

为 Switch B 配置 VLAN 接口和 IP 地址，具体配置过程略。

1.3 验证配置

完成上述配置后，在 Switch A Web 配置界面选择页面左侧导航栏的[网络/IP/ARP]，进入 ARP 配置界面后，就可以看见新配置的静态 ARP 表项。

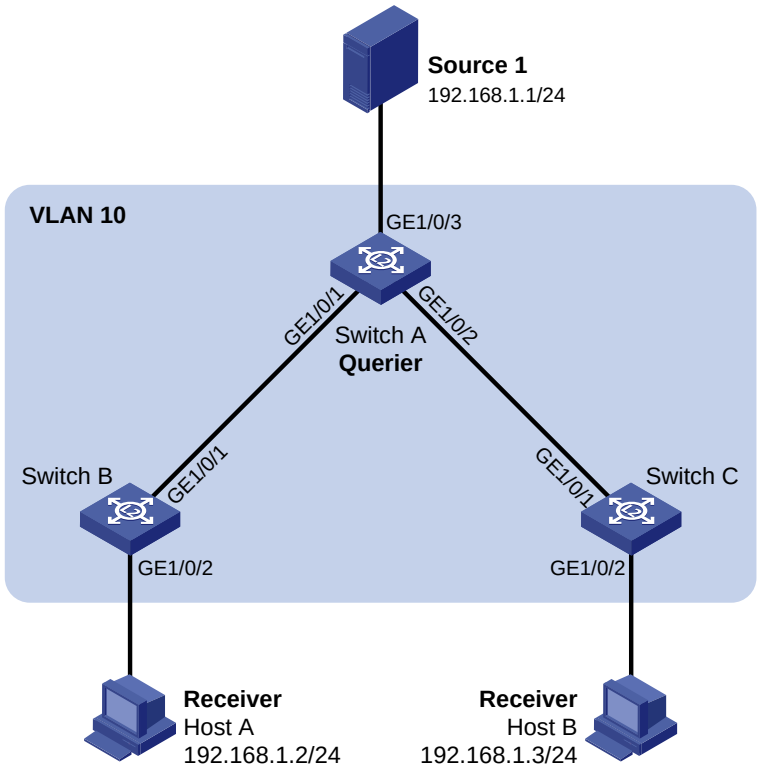
目 录

1 IGMP Snooping 快速配置指南

1.1 组网需求

- 如图 1 所示，在一个没有三层网络设备的纯二层网络中，组播源 Source 1 向组播组 224.1.1.1 发送组播数据，Host A 和 Host B 都是该组播组的接收者，且都使用 IGMPv2。
- 由于该网络中没有可运行 IGMP 的三层网络设备，因此由 Switch A 来充当 IGMP 查询器，并将其发出的 IGMP 查询报文的源 IP 地址配置为非 0.0.0.0，以免影响各交换机上 IGMP snooping 转发表项的建立从而导致组播数据无法正常转发。
- 为防止交换机在没有相应转发表项时将组播数据在 VLAN 内广播，在所有交换机上都开启丢弃未知组播数据报文功能。

图1 IGMP Snooping 配置组网图



1.2 配置步骤

1. 配置 Switch A

(1) 配置接口和 IP 地址（略）

(2) 开启 IGMP Snooping

选择页面左侧导航栏的[网络/组播/IGMP Snooping]，进入“IGMP Snooping”页面，点击“开启 IGMP Snooping”。

图2 开启 IGMP Snooping

(3) 在 VLAN 上开启 IGMP Snooping

在“IGMP Snooping”配置页面，进行如下配置：

- 单击“ ”按钮，进入“在 VLAN 上开启 IGMP Snooping”配置页面。
- 配置开启 IGMP Snooping 功能的 VLAN 编号为“10”。
- 配置 IGMP Snooping 版本为“2”。
- 勾选“对未知组播数据报文进行丢弃”。
- 勾选“充当 IGMP 查询器”。
- 配置普遍组查询报文的源 IP 地址配置为“10.1.1.1”。
- 配置特定组查询报文的源 IP 地址配置为“10.1.1.1”。
- 单击<确定>按钮，提示设置成功，完成 VLAN10 的 IGMP Snooping 配置。

图3 在 VLAN 上开启 IGMP Snooping

(4) 保存配置

点击页面左上方标识和辅助区内的“ ”按钮保存配置。

2. 配置 Switch B

(1) 配置接口和 IP 地址（略）

(2) 开启 IGMP Snooping

选择页面左侧导航栏的[网络/组播/IGMP Snooping]，进入“IGMP Snooping”页面，点击“开启 IGMP Snooping”。

图4 开启 IGMP Snooping

(3) 在 VLAN 上开启 IGMP Snooping

选择页面左侧导航栏的[网络/组播/IGMP Snooping]，进入“IGMP Snooping”配置页面，进行如下配置：

- 单击“ ”按钮，进入“在 VLAN 上开启 IGMP Snooping”配置页面。
- 配置开启 IGMP Snooping 功能的 VLAN 编号为“10”。
- 配置 IGMP Snooping 版本为“2”。
- 勾选“对未知组播数据报文进行丢弃”。
- 单击<确定>按钮，提示设置成功，完成 VLAN10 的 IGMP Snooping 配置。

图5 在 VLAN 上开启 IGMP Snooping

(4) 保存配置

点击页面左上方标识和辅助区内的“ ”按钮保存配置。

3. 配置 Switch C

Switch C 上的配置与 Switch B 完全相同，此处不再赘述。

1.3 验证配置

完成上述配置后，在 Switch A、Switch B 和 Switch C 的“网络 > 组播 > IGMP Snooping”页面中，可以查看 VLAN10 的 IGMP Snooping 配置信息。

目 录

1 IP Source Guard（端口绑定）快速配置指南

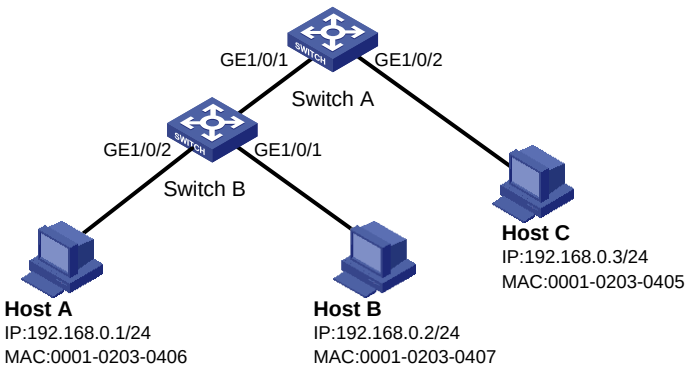
1.1 组网需求

在一个公司的小型网络中，各主机和服务器均使用静态配置的 IPv4 地址。要求在 Switch A 和 Switch B 上配置 IP Source Guard 端口静态绑定表项，并在端口下开启 IP Source Guard 功能，对 Switch A 和 Switch B 接收到的报文进行过滤，以防止非法用户报文通过。

具体需求如下：

- Switch A 的端口 GigabitEthernet1/0/2 上只允许 Host C 发送的 IP 报文通过。
- Switch A 的端口 GigabitEthernet1/0/1 上只允许 Host A 发送的 IP 报文通过。
- Switch B 的端口 GigabitEthernet1/0/2 上只允许 Host A 发送的 IP 报文通过。
- Switch B 的端口 GigabitEthernet1/0/1 上只允许 Host B 发送的 IP 报文通过。

图1 IP Source Guard 配置组网图



1.2 配置步骤

1. Switch A 的配置

(1) 配置各接口的 IP 地址（略）

(2) 新增 IP Source Guard IPv4 静态绑定表项

选择页面左侧导航栏的[安全/包过滤/IP Source Guard]，进入“IP Source Guard”配置页面，进行如下配置：

- 在“IP Source Guard”配置页面右侧点击“ ”，添加 IP Source Guard 表项信息。
- 配置接口为“GE1/0/2”。
- 配置 IP 地址为“192.168.0.3”。
- 配置 MAC 地址为“00-01-02-03-04-05”。
- 单击<确定>按钮，提示设置成功，完成 IP Source Guard 表项的添加。

图2 添加 IP Source Guard 表项

- 在“IP Source Guard”配置页面右侧点击“ ”，添加 IP Source Guard 表项信息。
- 配置接口为“GE1/0/1”。
- 配置 IP 地址为“192.168.0.1”。
- 配置 MAC 地址为“00-01-02-03-04-06”。
- 单击<确定>按钮，提示设置成功，完成 IP Source Guard 表项的添加。

(3) 保存配置

点击页面左上方标识和辅助区内的“ ”按钮保存配置。

2. Switch B 的配置

(1) 配置各接口的 IP 地址（略）

(2) 新增 IP Source Guard IPv4 静态绑定表项

选择页面左侧导航栏的[安全/包过滤/IP Source Guard]，进入“IP Source Guard”配置页面，进行如下配置：

- 在“IP Source Guard”配置页面右侧点击“ ”，添加 IP Source Guard 表项信息。
- 配置接口为“GE1/0/2”。
- 配置 IP 地址为“192.168.0.1”。
- 配置 MAC 地址为“00-01-02-03-04-06”。
- 单击<确定>按钮，提示设置成功，完成 IP Source Guard 表项的添加。
- 在“IP Source Guard”配置页面右侧点击“ ”，添加 IP Source Guard 表项信息。
- 配置接口为“GE1/0/1”。
- 配置 IP 地址为“192.168.0.2”。
- 配置 MAC 地址为“00-01-02-03-04-07”。
- 单击<确定>按钮，提示设置成功，完成 IP Source Guard 表项的添加。

(3) 保存配置

点击页面左上方标识和辅助区内的“  ”按钮保存配置。

1.3 验证配置

完成上述配置后，可分别在 Switch A 和 Switch B 的“安全 > 包过滤 > IP Source Guard”页面查看到对应的 IP Source Guard 表项。

目 录

1 软件升级快速配置指南

1.1 组网需求

无。

1.2 配置注意事项

升级之前，请您认真阅读版本说明书，确保升级软件包和设备当前软件版本之间的兼容性，了解升级对现行系统的影响以及本版本升级的注意事项。

升级过程中需要重启设备，请您避开业务高峰，选择合适时间段进行。

1.3 配置准备

获取升级软件包有如下方式：

- 如图 1所示，登录 H3C 官网 http://www.h3c.com/cn，在“首页——支持——文档与软件——软件下载”栏目下，按产品检索，找到升级软件包。
- 联系 H3C 技术支持人员获取待升级软件包。

图1 打开“软件下载”页面

1.4 配置步骤

(1) 查看当前版本。

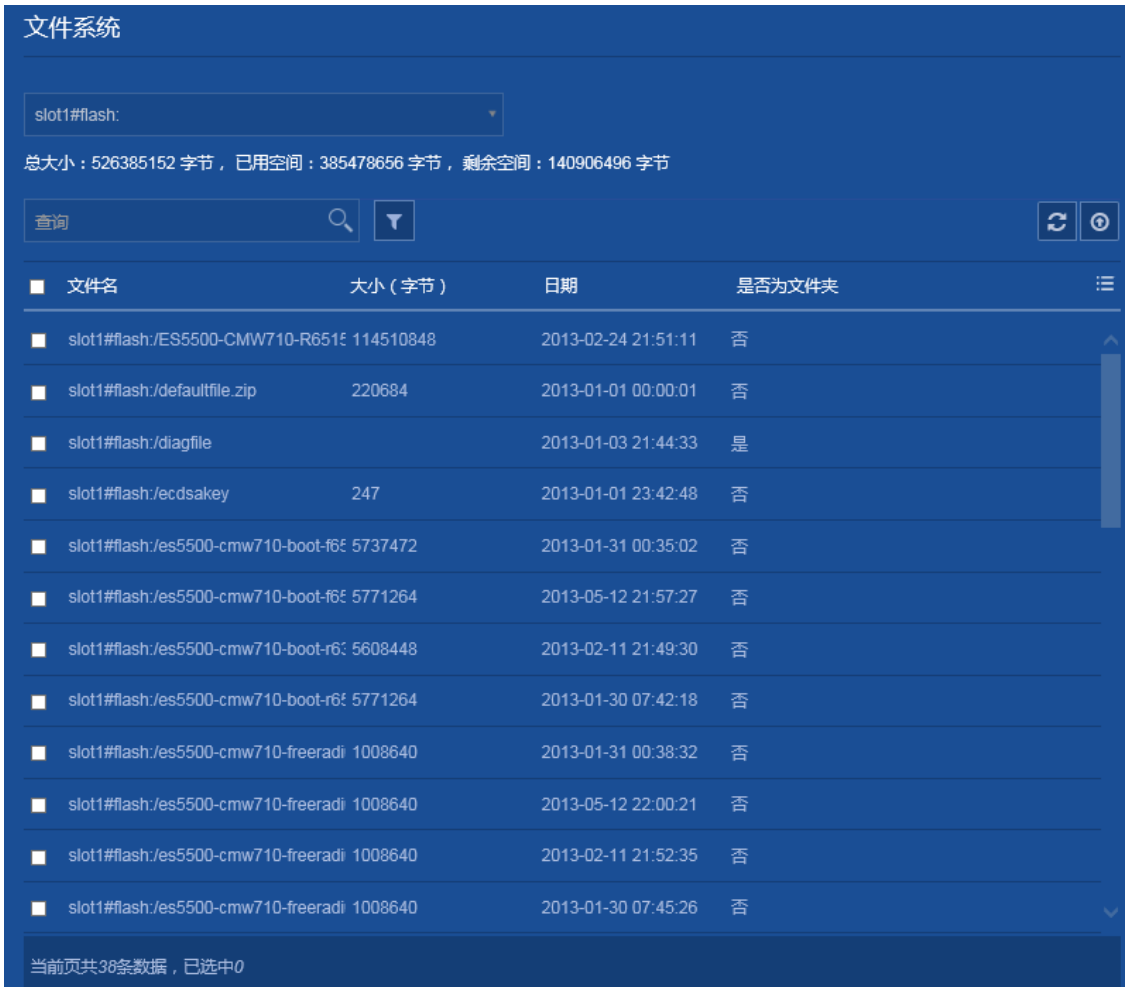
选择页面左侧导航栏的[概览]，在“系统信息”页面查看设备当前版本。

图2 查看系统信息

(2) 查看剩余空间。

选择页面左侧导航栏的[设备/文件系统]，进入“文件系统”页面，查看设备剩余存储空间，确保剩余空间足够保存新的待升级软件包（一般为软件包大小的两倍以上）。当空间不足时，可在该页面删除多余的文件。

图3 文件系统



(3) 升级系统软件。

- 选择页面左侧导航栏的[设备/软件更新]，进入“软件更新”配置页面，单击<升级系统软件>按钮，弹出“升级系统软件”对话框。
- 在“升级系统软件”对话框中，单击<浏览>按钮，选择本地的升级软件包。如果想立即升级，请勾选“立即重启设备”，如果想稍后手工重启，请取消勾选。
- 单击<确定>按钮，完成操作。对于勾选“立即重启设备”的情况，升级成功后请等待设备重启并重新登录设备。

图4 升级系统软件

1.5 验证配置

选择页面左侧导航栏的[概览]，在“系统信息”页面查看设备当前软件版本。

图5 查看系统信息

目 录

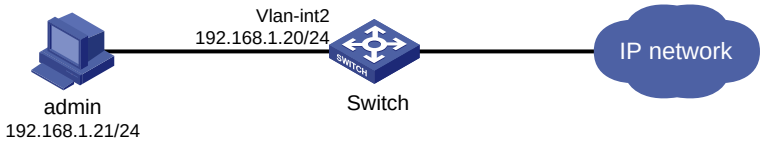
1 添加管理账户快速配置指南

1.1 组网需求

在 Switch 上配置一个管理员帐户，用于用户采用 HTTP 方式登录 Switch，具体要求如下：

- 用户使用管理员帐户登录时，Switch 对其进行本地认证。
- 管理员帐户名称为 webuser，密码为 12345。
- 通过认证之后，用户被授予角色 network-admin。

图1 配置管理员账户组网图



1.2 配置步骤

(1) 配置 VLAN 和 VLAN 接口

选择页面左侧导航栏的[网络/链路/VLAN]页面，进入“VLAN”配置页面，进行如下配置：

- 点击右侧“ ”按钮，在 VLAN 列表处输入“2”，单击<确定>按钮完成创建。

图2 创建 VLAN

- 点击 VLAN 2 右侧“ ”按钮，进入“修改 VLAN”页面。
- 将与管理员 PC 相连的接口加入 VLAN 2 的 Untagged 端口列表。
- 在 VLAN 接口 IP 地址处勾选“创建 VLAN 接口”，指定接口的 IP 地址为“192.168.1.20”，子网掩码为“255.255.255.0”。
- 单击<确定>按钮，提示设置成功，完成 VLAN 和 VLAN 接口的创建。

图3 配置 VLAN 和 VLAN 接口

(2) 配置管理员账户

选择页面左侧导航栏的[设备/维护/管理员]页面，进入“管理员”配置页面，进行如下配置：

- 点击右侧“+”按钮，添加管理员。
- 配置用户名为“webuser”。
- 密码为“12345”。

- 选择角色为“network-admin”。
- 指定可用的服务为“HTTP”。
- 单击<确定>按钮，提示设置成功，完成管理员账户的添加。

图4 添加管理员账户

(3) 开启 HTTP 和 HTTPS 服务

选择页面左侧导航栏的[网络/服务/HTTP/HTTPS]页面，进入“网络服务”配置页面，进行如下配置：

- 单击“开启 HTTP”按钮，开启 HTTP 登录服务。
- 单击“开启 HTTPS”按钮，开启 HTTPS 登录服务。
- 提示设置成功，完成 HTTP 和 HTTPS 登录服务的开启。

图5 开启 HTTP 和 HTTPS 服务

(4) 保存配置

点击页面左上方标识和辅助区内的“ ”按钮保存配置。

1.3 验证配置

(1) 完成上述配置后，在管理员页面上可以看到已成功添加的管理员帐户。

(2) 用户在 PC 的 Web 浏览器地址栏中输入 http://192.168.1.20 并回车后，浏览器将显示 Web 登录页面。用户在该登录页面中输入管理员帐户名称、密码以及验证码后，即可成功登录设备的 Web 页面进行相关配置。

目 录

1 Ping 不通故障排查快速配置指南

1.1 组网需求

无。

1.2 配置注意事项

IPv4 和 IPv6 网络的故障排查检测方法相同，本次仅以检测 IPv4 网络为例。

1.3 配置步骤

1.3.1 使用 Ping 功能测试链路通畅性

(1) 配置接口的 IP 地址（略）

(2) Ping 功能配置

选择页面左侧导航栏的[网络/探测工具/Ping]，进入“Ping”功能配置页面，进行如下配置：

- 选择“IPv4 Ping”页签。
- 配置目的 IP 地址或者主机名。
- 单击<开始>按钮，进行链路通畅性测试，在“结果”窗口会显示测试信息。

图1 Ping 功能测试链路通畅

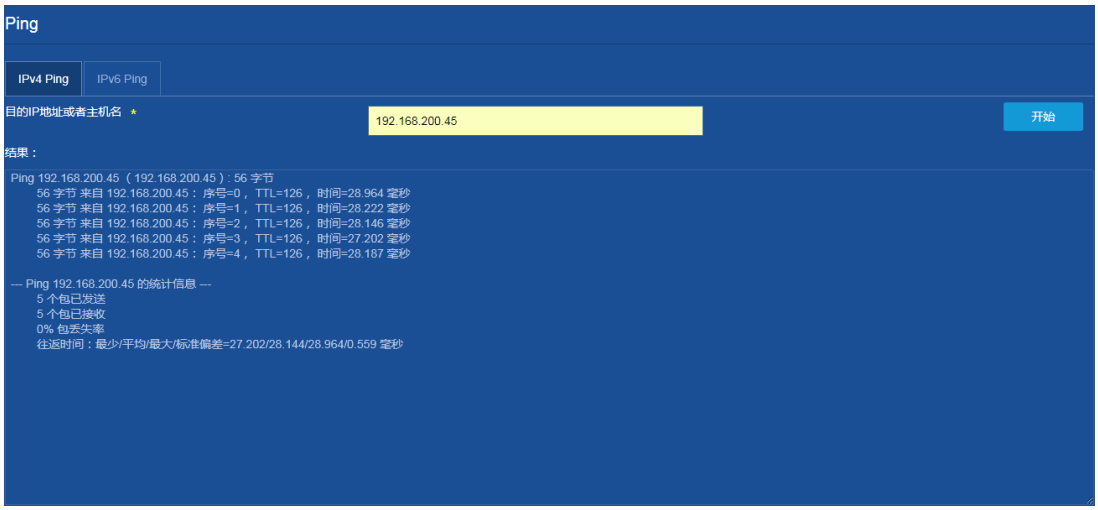


图2 Ping 功能测试链路不通畅

1.3.2 使用 Tracert 功能测试数据通信路径

(1) 配置接口的 IP 地址（略）

(2) Tracert 功能配置

选择页面左侧导航栏的[网络/探测工具/Tracert]，进入“Tracert”功能配置页面，进行如下配置：

- 选择“IPv4 Tracert”页签。
- 配置目的 IP 或者主机名。
- 单击<开始>按钮，进行数据通信路径测试，在“结果”窗口会显示测试信息。

图3 Tracert 功能测试数据通信路径可用

图4 Tracert 功能测试数据通信路径不可用

1.4 验证配置

无。

目 录

1 修改密码

1.1 组网需求

无。

1.2 配置注意事项

部分设备默认启用了密码管理功能，要求配置的密码最小长度为 10 个字符，密码元素的最少组合类型为 2 种，至少要包含每种元素的个数为 1 个。若配置的新密码不符合要求则会弹出对应提示，请按照提示配置符合要求的密码。

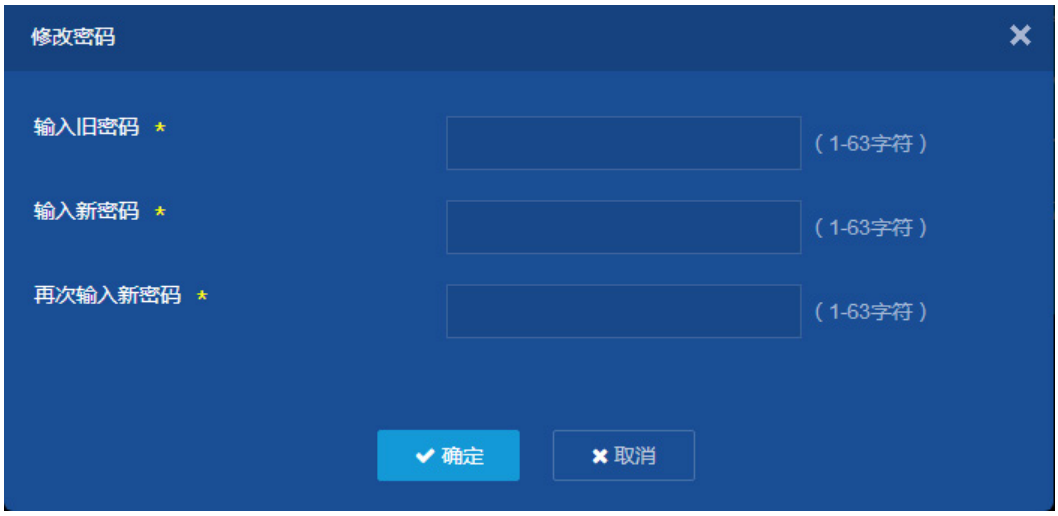
1.3 配置步骤

(1) 点击页面左侧导航栏上的用户名，在扩展菜单中点击修改密码，进入“修改密码”页面。

图1 修改密码

(2) 输入旧密码与两次新密码。点击<确定>按钮，完成密码的修改。

图2 设置新密码



1.4 验证配置

密码修改完成后不会自动退出当前 Web 页面，手动退出后即可使用新密码再次登录设备。

目 录

1 系统时间快速配置指南

1.1 组网需求

无。

1.2 配置注意事项

仅执行夏令时制的国家地区需要配置夏令时。

1.3 配置步骤

(1) 配置各接口的 IP 地址（略）

(2) 配置系统时间

选择页面左侧导航栏的[设备/维护/系统设置]，进入“系统设置”配置页面，进行如下配置：

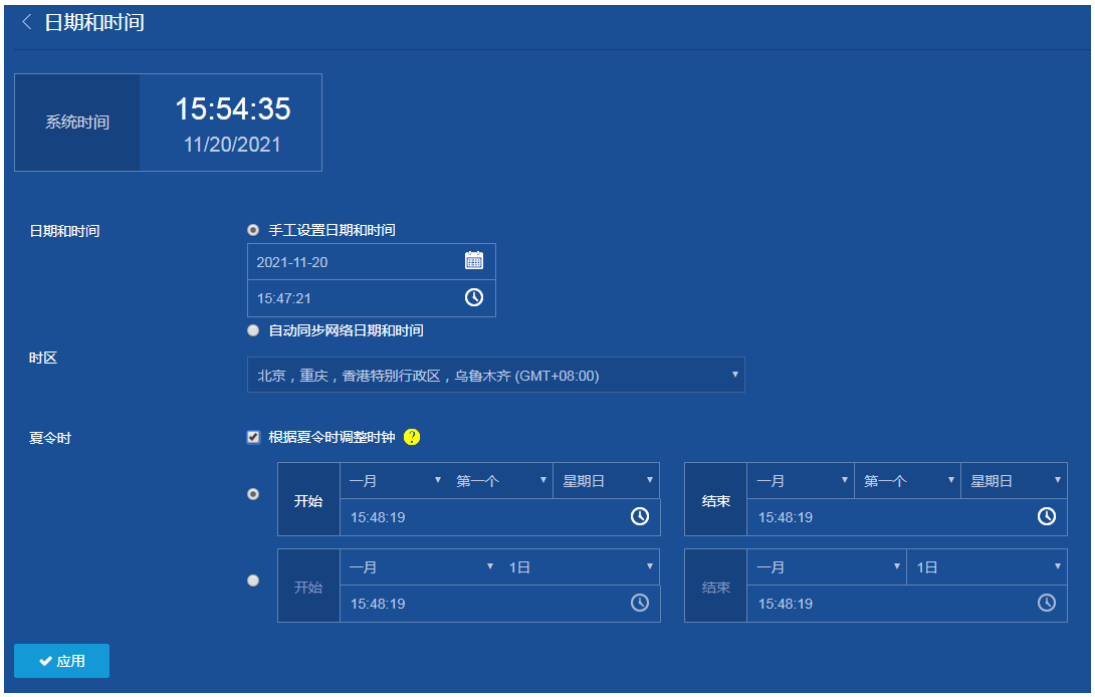
- 单击日期和时间右侧的“ ”按钮，进入“日期和时间”配置页签。
- 配置设备的日期和时间为“手工设置日期和时间”模式。
- 单击“ ”按钮，配置设备要设置的日期。
- 单击“ ”按钮，配置设备要设置的时间。

图1 手工设置日期和时间

- 在时区下拉菜单中选择“北京，重庆，香港特别行政区，乌鲁木齐（GMT+08:00）”。

- 在夏令时处勾选“根据夏令时调整时钟”，分别设置夏令时的开始时间和结束时间。

图2 根据夏令时调整时钟



- 单击<应用>按钮，提示设置成功，完成设备系统时间的配置。

1.4 验证配置

无。

目 录

1 系统日志快速配置指南

1.1 组网需求

无。

1.2 配置注意事项

系统可以向日志缓冲区（logbuffer）、日志主机（loghost）等方向发送日志信息，日志信息的各个输出方向相互独立，可在页面中分别设置。

1.3 配置步骤

(1) 配置日志主机

选择页面左侧导航栏的[日志/设置]，进入“系统日志设置”页面，配置日志主机的 IP 地址，本例为“192.168.1.1”，点击“ ”按钮，提示设置成功，完成日志主机的配置。

图1 系统日志设置页面

(2) 保存配置

点击页面左上方标识和辅助区内的“ ”按钮保存配置。

1.4 验证配置

无。

目 录

1 配置备份/导出/恢复出厂快速配置指南

1.1 组网需求

无。

1.2 配置步骤

1. 配置备份

选择页面左侧导航栏的[设备/维护/配置文件]，进入“配置文件”页面，进行如下配置：

(1) 单击<保存当前配置>按钮，弹出“保存当前配置”对话框。

(2) 在“保存当前配置”对话框中，将配置文件备份到名称为“config.cfg”的配置文件中。

(3) 单击<确定>按钮，完成操作。

图1 保存当前配置

2. 导出配置

(1) 选择页面左侧导航栏的[设备/维护/配置文件]，进入“配置文件”页面。

(2) 单击<导出当前配置>按钮，配置文件会自动下载到本地。

说明

备份的配置文件格式为.cfg，在浏览器下方可以查看。

3. 恢复出厂配置

(1) 选择页面左侧导航栏的[设备/维护/配置文件]，进入“配置文件”页面

(2) 单击“恢复出厂配置”右侧的“”按钮，进入“恢复出厂配置”页面。

(3) 单击<重置>按钮，完成操作。

图2 恢复出厂配置

目 录

1 设备重启

1.1 组网需求

无。

1.2 配置注意事项

重新启动可能会导致业务中断，请谨慎执行重启操作。

勾选“强制设备不进行任何检查直接重启”时，系统在重启时不会做任何保护性措施。重启后，可能导致文件系统损坏，建议在系统故障或无法正常重启时，再进行勾选。

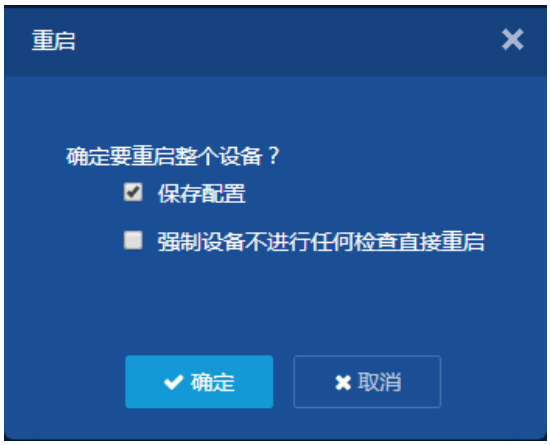
1.3 配置步骤

(1) 选择页面左侧导航栏的[设备/维护/重启]，进入“重启”配置页面。

图1 重启配置页面

(2) 点击“重启设备”，在弹出的对话框中单击<确定>按钮，开始重启设备。

图2 重启设备



(3) 等待设备重启完成后，即可再次进入 Web 配置页面。

1.4 验证配置

无。

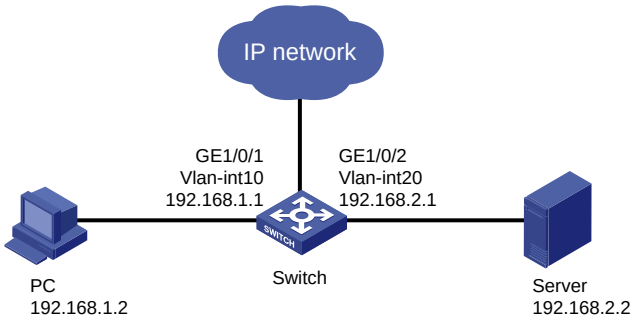
目 录

1 配置 QoS 策略禁止 VLAN 间设备互访

1.1 组网需求

如图 1 所示，PC 属于 VLAN 10，服务器属于 VLAN 20，为安全考虑，需要在交换机的 GE1/0/1 和 GE1/0/2 接口配置 QoS 策略，禁止不同 VLAN 的设备互相访问，同时不影响其他流量的转发。

图1 配置 QoS 策略禁止 VLAN 间设备互访组网图



1.2 配置思路

配置思路如下：

- 在接口 GigabitEthernet1/0/1 的入方向应用 QoS 策略，禁止访问 VLAN 接口 20 网段设备的流量通过。
- 在接口 GigabitEthernet1/0/2 的入方向应用 QoS 策略，禁止访问 VLAN 接口 10 网段设备的流量通过。

1.3 配置步骤

(1) 配置各接口的 IP 地址（略）

(2) 配置 QoS 策略

选择页面左侧导航栏的[QoS/QoS/QoS 策略]，进入“QoS 策略”配置页面，进行如下配置：

- 点击“添加用户自定义 policy”，进入“添加自定义 policy”页面。

图2 配置 QoS 策略

- 配置策略名“a3”，策略类型“普通”，点击“ + ”按钮，完成添加。

- 配置策略名“b3”，策略类型“普通”，点击“ ”按钮，完成添加。

图3 添加用户自定义 policy

(3) 应用 QoS 策略

在“添加自定义 policy”页面点击“ ”按钮，回到“QoS 策略”页面。

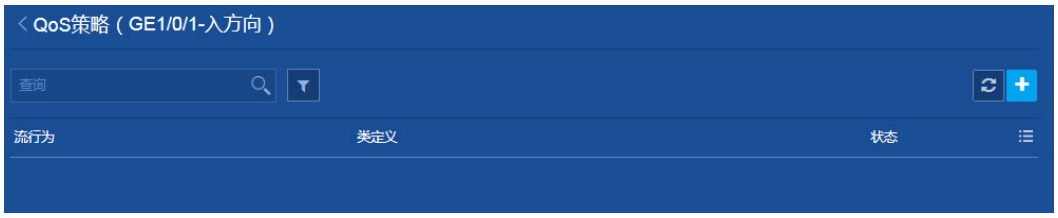
- 选择应用 QoS 策略的接口为“GE1/0/1”，策略名为“a3”，入方向应用模式为“无”，勾选“入方向”，点击“ ”按钮，完成添加。
- 选择应用 QoS 策略的接口为“GE1/0/2”，策略名为“b3”，入方向应用模式为“无”，勾选“入方向”，点击“ ”按钮，完成添加。

图4 应用 QoS 策略

(4) 配置 GE1/0/1 接口 QoS 策略的流行为和类定义

在“QoS 策略”页面，点击 GE1/0/1 接口的“修改策略”，进入“QoS 策略（GE1/0/1-入方向）”配置页面。

图5 QoS 策略（GE1/0/1-入方向）



- 点击右上角的“ ”按钮，进入“添加 QoS 策略”配置页面。

- 在“流行为”页面，勾选“丢弃数据包”。

图6 流行为

- 在“类定义”页面，勾选“匹配 IPv4 ACL”。

图7 类定义

- 点击“+”按钮，弹出“ACL”页面，开始添加 ACL。

图8 添加 ACL

- 选择 ACL 的类型为“高级 ACL”，ACL 的编号为“3000”，点击<确定>按钮，进入“添加 IPv4 高级 ACL 的规则”页面。

图9 添加 IPv4 ACL

- 选择动作为“允许”，IP 协议类型为“IP”，匹配条件为匹配源地址“192.168.1.0”，通配符“0.0.0.255”，匹配目的地址为“192.168.2.0”，通配符“0.0.0.255”。
- 取消勾选“继续添加下一条规则”，点击<确定>按钮，完成 ACL 的添加。

图10 添加 IPv4 高级 ACL 的规则

- 点击<确定>按钮，完成 GE1/0/1 接口的 QoS 策略配置。

(5) 配置 GE1/0/2 接口 QoS 策略的流行为和类定义

参考 GE1/0/1 接口的 QoS 策略配置，完成 GE1/0/2 接口的 QoS 策略配置。除以下配置，其他配置相同：GE1/0/2 接口使用的 IPv4 高级 ACL 的编号为“3001”，匹配源地址“192.168.2.0”，通配符“0.0.0.255”，匹配目的地址为“192.168.1.0”，通配符“0.0.0.255”。

1.4 验证配置

配置完成后，在“QoS 策略”页面，点击 GE1/0/1 和 GE1/0/2 接口的“修改策略”，进入“QoS 策略（GE1/0/1-入方向）”配置页面，可以查看到已配置的 QoS 策略信息。

图11 接口入方向下发 QoS 策略配置信息

在接口配置 QoS 策略前，在 PC 上 ping 服务器的 IP 地址，可以看出发出 4 个数据包，接收 4 个数据包。

```
C:\Users\user>ping 192.168.2.2
正在 Ping 192.168.2.2 具有 32 字节的数据:
来自 192.168.2.2 的回复: 字节=32 时间=3ms TTL=255
来自 192.168.2.2 的回复: 字节=32 时间=1ms TTL=255
来自 192.168.2.2 的回复: 字节=32 时间=1ms TTL=255
来自 192.168.2.2 的回复: 字节=32 时间=1ms TTL=255

192.168.2.2 的 Ping 统计信息:
    数据包: 已发送 = 4，已接收 = 4，丢失 = 0 (0% 丢失)，
往返行程的估计时间(以毫秒为单位):
    最短 = 1ms，最长 = 3ms，平均 = 1ms
```

在接口配置 QoS 策略后，在 PC 上 ping 服务器的 IP 地址，发现不能 ping 通：

```
C:\Users\user>ping 192.168.2.2

正在 Ping 192.168.2.2 具有 32 字节的数据:
来自 192.168.2.2 的回复: 无法访问目标主机。
来自 192.168.2.2 的回复: 无法访问目标主机。
来自 192.168.2.2 的回复: 无法访问目标主机。
来自 192.168.2.2 的回复: 无法访问目标主机。

192.168.2.2 的 Ping 统计信息:
    数据包: 已发送 = 4，已接收 = 0，丢失 = 4 (100% 丢失)，
```

目 录

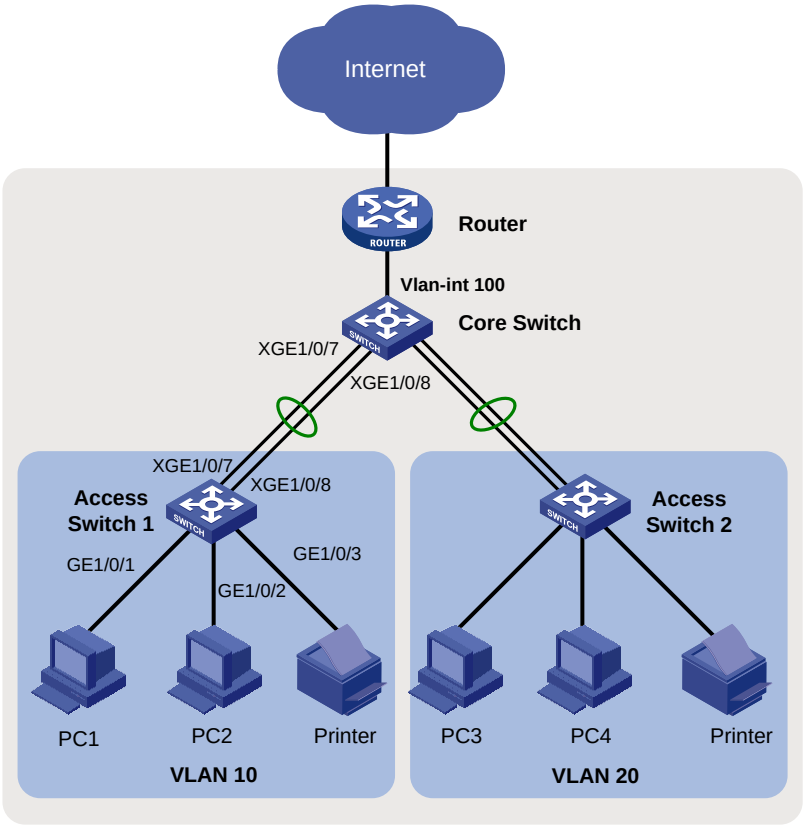
1 小型园区典型组网 Web 配置

1.1 组网需求

如图 1 所示，在小型园区中，通常采用接入及核心两层网络结构，出口路由器一般选用 MSR 系列路由器。

- 各交换机开启 STP 功能防止环路。
- 接入交换机与核心交换机通过链路聚合组网保证可靠性。
- 园区网中不同的业务部门划分到不同的 VLAN 中，部门间的业务在核心交换机上通过 VLAN 接口进行三层互通。
- 核心交换机作为 DHCP 服务器，为园区网用户动态分配 IP 地址。
- 接入交换机上开启 DHCP Snooping 功能，防止内网用户私接小路由器分配 IP 地址；同时配置 IP source guard 功能，防止内网用户私自更改 IP 地址。

图1 小型园区典型组网图



1.2 配置思路与数据规划

配置思路如下，具体数据规划请参见表 1。

(1) 通过 Web 登录设备

(2) 配置接口和 VLAN

(3) 配置核心交换机 DHCP 服务器功能

(4) 配置核心交换机路由

(5) 配置出口路由器

(6) 配置接入交换机的 DHCP Snooping 功能

(7) 配置接入交换机 IP source Guard 功能

表1 配置数据表

配置步骤	配置项	配置数据	说明
登录设备	通过Web登录	对于有缺省IP地址的设备，适用缺省信息登录；对于没有缺省IP地址的设备，需通过Console口登录设备，然后设置通过Web登录设备所需的配置	PC端通过浏览器登录设备
配置接口和VLAN	动态聚合	ACCSW1：上行聚合接口BAGG1 CORESW：下行聚合接口BAGG1	接入交换机与核心交换机间通过聚合链路连接
	端口类型	连接PC的端口一般设置为access口；连接交换机的端口建议设置为trunk口。	trunk类型端口一般用于连接交换机 access类型端口一般用于连接PC
	VLAN ID	ACCSW1：VLAN 10 ACCSW2：VLAN 20 CORESW：VLAN 100、10、20	为实现部门A和部门B二层隔离，将部门A划分到VLAN10中，部门B划分到VLAN20中。 核心交换机通过Vlan-int100连接出口路由器
核心交换机上配置DHCP服务器功能	DHCP Server	-	在园区核心交换机上部署DHCP服务器
	地址池	VLAN 10：ip pool 1 VLAN 20：ip pool 2	部门A的终端从ip pool 1中获取IP地址 部门B的终端从ip pool 2中获取IP地址
	地址分配方式	基于全局地址池	无
配置核心交换机路由	IP地址	Vlan-int10：10.10.10.1/24 Vlan-int20：10.10.20.1/24 Vlan-int100：10.10.100.1/24	Vlan-int100是核心交换机与园区出口路由器对接的IP地址，用于园区内部网络与出口路由器互通 核心交换机上需要配置一条缺省路由下一跳指向出口路由器 在核心交换机上配置Vlan-int10、Vlan-int20的IP地址后，部门A与部门B之间可以通过核心交换机互访
配置出口路由器	公网接口IP地址	GE1/0/2：202.101.100.2/30	GE1/0/2为出口路由器连接Internet的接口，一般称为公网接口
	公网网关	202.101.100.1/30	该地址是与出口路由器对接的运营商设备的IP地址，出口路由器上需要配置一条缺省路由指向该地址，用于指导内网流量转发至外网
	DNS地址	202.101.100.199	DNS服务器用于将域名解析成IP地址
	内网接口IP地址	GE1/0/1：10.10.100.2/24	GE1/0/1为出口路由器连接内网的接口

配置步骤	配置项	配置数据	说明
接入交换机上配置DHCP Snooping	信任接口	-	指定二层聚合接口BAGG1为DHCP Snooping功能的信任端口
接入交换机上配置IP Source Guard	IPSG检查	-	配置IPv4接口绑定功能，绑定源IP地址和MAC地址

1.3 配置准备

登录设备的 Web 管理页面：

- 对于有缺省 IP 地址的设备，有关如何登录 Web 页面的具体描述请参见《Web 快速配置指南》中的“通过 Web 登录有缺省 IP 地址的设备”。
- 对于没有缺省 IP 地址的设备，有关如何登录 Web 页面的具体描述请参见《Web 快速配置指南》中的“通过 Web 登录没有缺省 IP 地址的设备”。

有关设备是否支持 web 和缺省 IP 地址的详细介绍，请参见《Web 快速配置指南》中的“适用产品型号”。

1.4 配置步骤

1. 配置接入交换机

说明

接入交换机 Access Switch 1 和 Access Switch 2 的配置基本相同。本小节以配置接入交换机 Access Switch 1 为例说明配置方法。

(1) 配置 VLAN

选择页面左侧导航栏的[网络/链路/VLAN]，进入“VLAN”页面，进行如下配置：

- 点击“ ”按钮，弹出“创建 VLAN”对话框。
- 配置 VLAN 列表为“10”。
- 单击<确定>按钮，完成 VLAN 的创建。

图2 创建 VLAN

- 点击 VLAN 10 右侧的“”按钮，进入“修改 VLAN”页面。
- 将端口“GE1/0/1”、“GE1/0/2”和“GE1/0/3”加入 VLAN 10 的 Untagged 端口列表。
- 单击<确定>按钮，提示设置成功，完成 VLAN 10 的配置。

图3 配置 VLAN 10

(2) 配置上行链路聚合

选择页面左侧导航栏的[网络/接口/链路聚合]，进入“链路聚合”页面，进行如下配置：

- 单击“+”按钮，添加聚合组。
- 在聚合类型下拉菜单中选择“二层聚合”。
- 聚合组编号为“1”。
- 在聚合模式下拉菜单中选择“动态聚合”。
- 在成员端口下拉菜单中选择“XGE1/0/7 和 XGE1/0/8”。
- 单击<确定>按钮，提示设置成功，完成二层动态聚合组的创建。

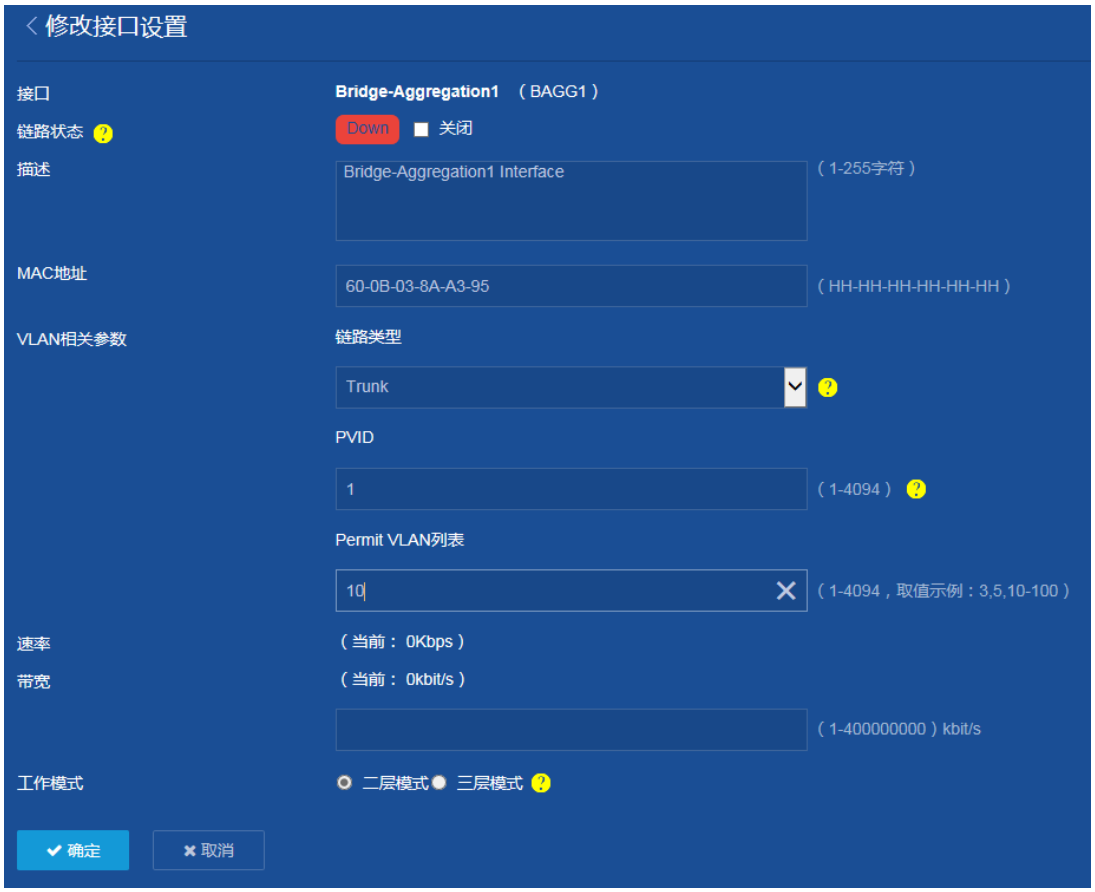
图4 配置二层链路聚合

(3) 配置二层静态聚合接口的 VLAN 属性

选择页面左侧导航栏的[网络/接口/接口]，进入“接口”页面，进行如下配置：

- 单击“ ”按钮，修改二层聚合接口 1 的接口设置。
- 在链路类型下拉菜单中选择“Trunk”。
- 配置 Permit VLAN 列表为“10”
- 单击<确定>按钮，提示设置成功，完成二层聚合接口 1 的 VLAN 属性配置。

图5 配置二层聚合接口的 VLAN 属性



(4) 生成树端口设置

选择页面左侧导航栏的[网络/链路/STP]，进入“STP”页面，进行如下配置：

- 点击“端口设置”右侧的“ ”按钮，修改生成树端口设置。
- 在端口“GE1/0/1”、“GE1/0/2”和“GE1/0/3”处勾选“边缘端口”。
- 单击<确定>按钮，提示设置成功，完成生成树端口设置。

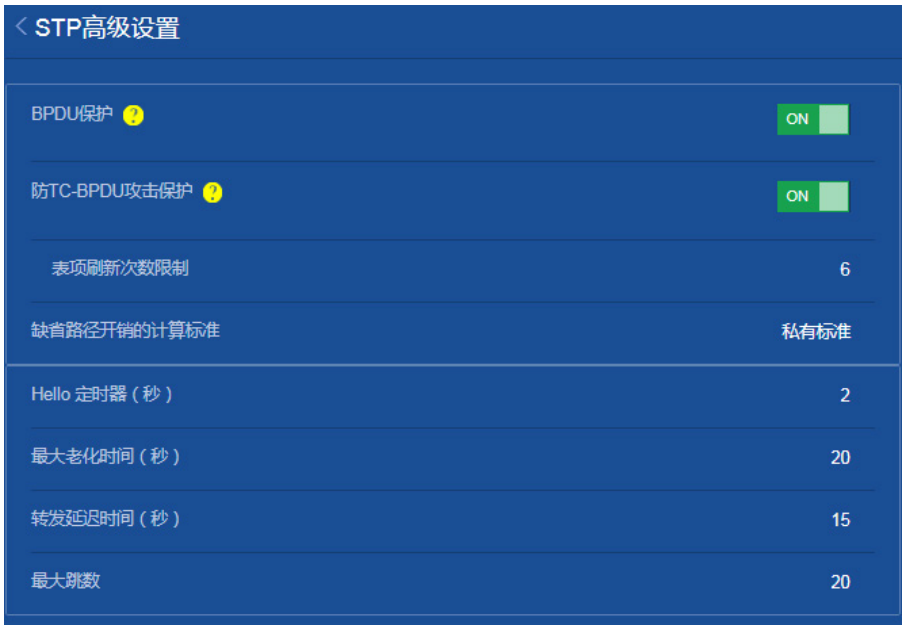
图6 生成树端口设置

(5) 配置 BPDU 保护功能

选择页面左侧导航栏的[网络/链路/STP]，进入“STP”页面，进行如下配置：

- 点击“高级设置”右侧的“ ”按钮，修改生成树高级设置。
- 将“BPDU 保护”右侧的按钮设置为 ON，提示设置成功，开启 BPDU 保护功能。

图7 开启 BPDU 保护功能



(6) 配置 DHCP snooping

选择页面左侧导航栏的[网络/链路/DHCP Snooping]，进入“DHCP Snooping”页面，进行如下配置：

- 点击“开启 DHCP Snooping”按钮，开启 DHCP Snooping 功能。

图8 开启 DHCP snooping

- 在端口“BAGG1”处勾选“信任端口”。
- 在端口“GE1/0/1”和“GE1/0/2”处勾选“表项记录功能”。
- 单击<确定>按钮，提示设置成功，完成 DHCP snooping 的设置。

图9 配置 DHCP snooping

(7) 配置 IP Source Guard IPv4 接口绑定功能

选择页面左侧导航栏的[安全/包过滤/IP Source Guard]，进入“IP Source Guard”页面，进行如下配置：

- 在“IP Source Guard”页面右上角点击源检查，进入接口绑定配置页面。
- 在 GE1/0/1 和 GE1/0/2 处勾选“IP 地址”和“MAC 地址”。
- 单击<确定>按钮，提示设置成功，完成接口绑定功能的设置。

图10 配置 IP Source Guard IPv4 接口绑定功能

(8) 保存配置

点击页面左上方标识和辅助区内的“  ”按钮保存配置。

2. 配置核心交换机

(1) 配置 VLAN

选择页面左侧导航栏的[网络/链路/VLAN]，进入“VLAN”页面，进行如下配置：

- 点击“ ”按钮，进入“创建 VLAN”对话框。
- 配置 VLAN 列表为“10,20,100”。
- 单击<确定>按钮，完成 VLAN 的创建。

图11 创建 VLAN

- 在“VLAN”页面点击 VLAN 10 右侧的“ ”按钮，进入“修改 VLAN”页面。
- 在“VLAN 接口 IP 地址”处勾选“创建 VLAN 接口”，并设置接口的 IP 地址为“10.10.10.1”，掩码长度为“24”。
- 单击<确定>按钮，提示设置成功，完成 VLAN 10 的配置。

图12 配置 VLAN

- 在“VLAN”页面，点击 VLAN 20 右侧的“ ”按钮，进入“修改 VLAN”页面。
- 在“VLAN 接口 IP 地址”处勾选“创建 VLAN 接口”，并设置接口的 IP 地址为“10.10.20.1”，掩码长度为“24”。
- 单击<确定>按钮，提示设置成功，完成 VLAN 20 的配置。
- 在“VLAN”页面，点击 VLAN 100 右侧的“ ”按钮，进入“修改 VLAN”页面。

- 在“VLAN 接口 IP 地址”处勾选“创建 VLAN 接口”，并设置接口的 IP 地址为“10.10.100.1”，掩码长度为“24”。
- 将端口 GE1/0/1 加入 VLAN 100 的 Untagged 端口列表。
- 单击<确定>按钮，提示设置成功，完成 VLAN 100 的配置。

(2) 配置下行链路聚合

选择页面左侧导航栏的[网络/接口/链路聚合]，进入“链路聚合”页面，进行如下配置：

- 单击“  ”按钮，添加聚合组。
- 在聚合类型下拉菜单中选择“二层聚合”。
- 聚合组编号为“1”。
- 在聚合模式下拉菜单中选择“动态聚合”。
- 在成员端口下拉菜单中选择“XGE1/0/7 和 XGE1/0/8”。
- 单击<确定>按钮，提示设置成功，完成二层动态聚合组的创建。

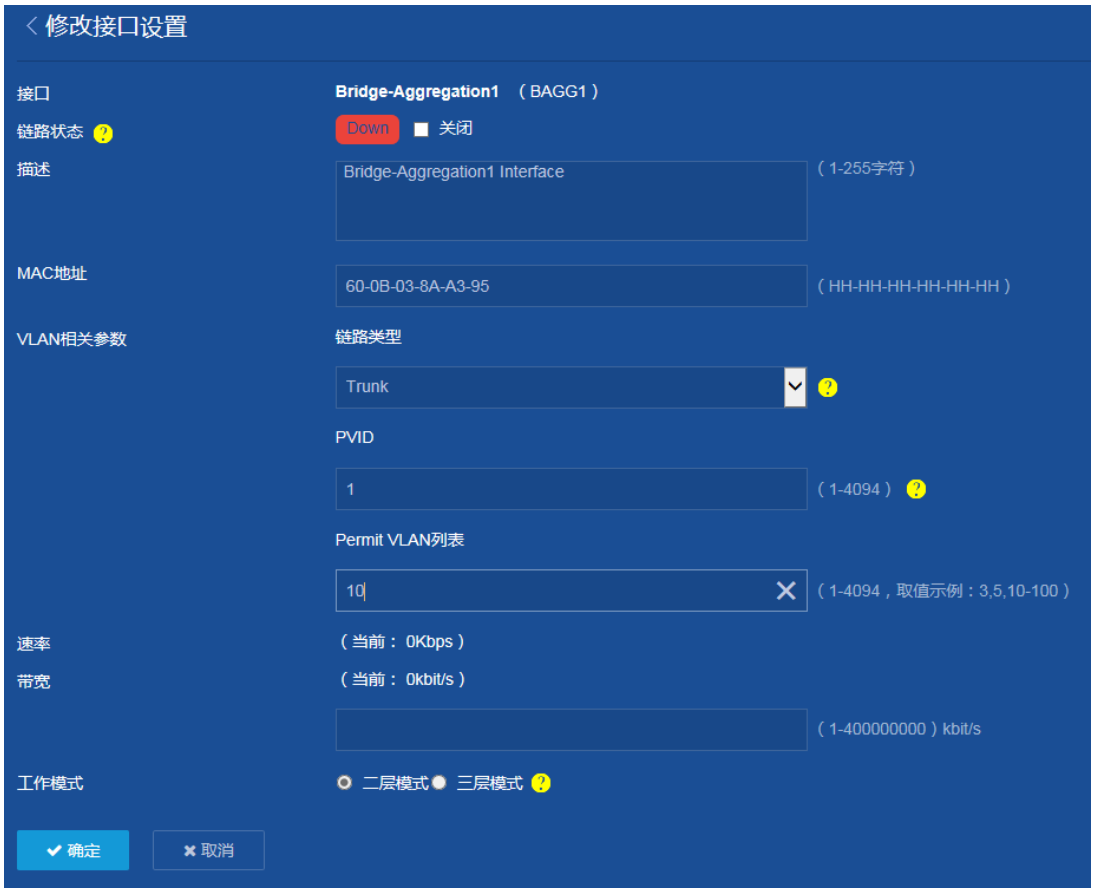
图13 配置二层链路聚合

(3) 配置二层静态聚合接口的 VLAN 属性

选择页面左侧导航栏的[网络/接口/接口]，进入“接口”页面，进行如下配置：

- 单击“  ”按钮，修改二层聚合接口 1 的接口设置。
- 在链路类型下拉菜单中选择“Trunk”。
- 配置 Permit VLAN 列表为“10”
- 单击<确定>按钮，提示设置成功，完成二层聚合接口 1 的 VLAN 属性配置。

图14 配置二层聚合接口的 VLAN 属性



(4) 配置 DHCP 服务器

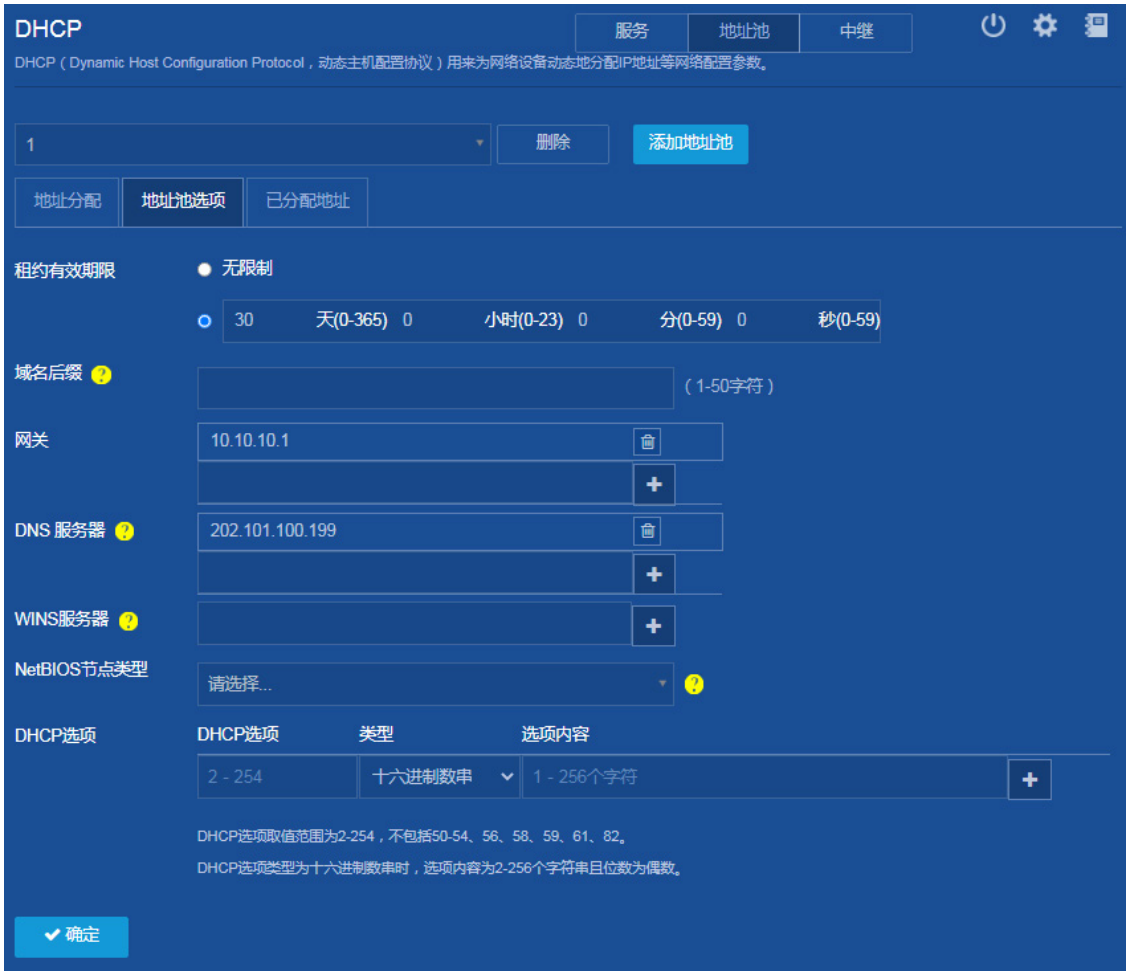
选择页面左侧导航栏的[网络/服务/DHCP]，进入“DHCP”页面，进行如下配置：

- 点击“启用 DHCP”按钮，开启 DHCP 服务，并进入 DHCP 配置页面。
- 点击页面右上角的“地址池”按钮，进入 DHCP 地址池配置页面。
- 点击“添加地址池”按钮，添加地址池“1”。
- 在地址池 1 的“地址分配”页面，进行如下配置：
  - 输入动态分配的地址段地址“10.10.10.0”，掩码“255.255.255.0”。
  - 在静态绑定的地址列表处，输入为打印机配置固定的 IP 地址“10.10.10.254”，掩码“24”，硬件地址“aabb-cccc-dd”，点击右侧的“+”按钮，完成静态绑定的地址列表的添加。

图15 地址池 1 的地址分配配置页面

- 在地址池 1 的“地址池选项”页面，进行如下配置：
  - 配置租约有效期限为“30”天。
  - 配置网关为“10.10.10.1”，点击右侧的“+”按钮，完成添加。
  - 配置 DNS 服务器为“202.101.100.199”，点击右侧的“+”按钮，完成添加。
- 单击<确定>按钮，提示设置成功，完成地址池 1 配置。

图16 地址池 1 的地址池选项配置页面

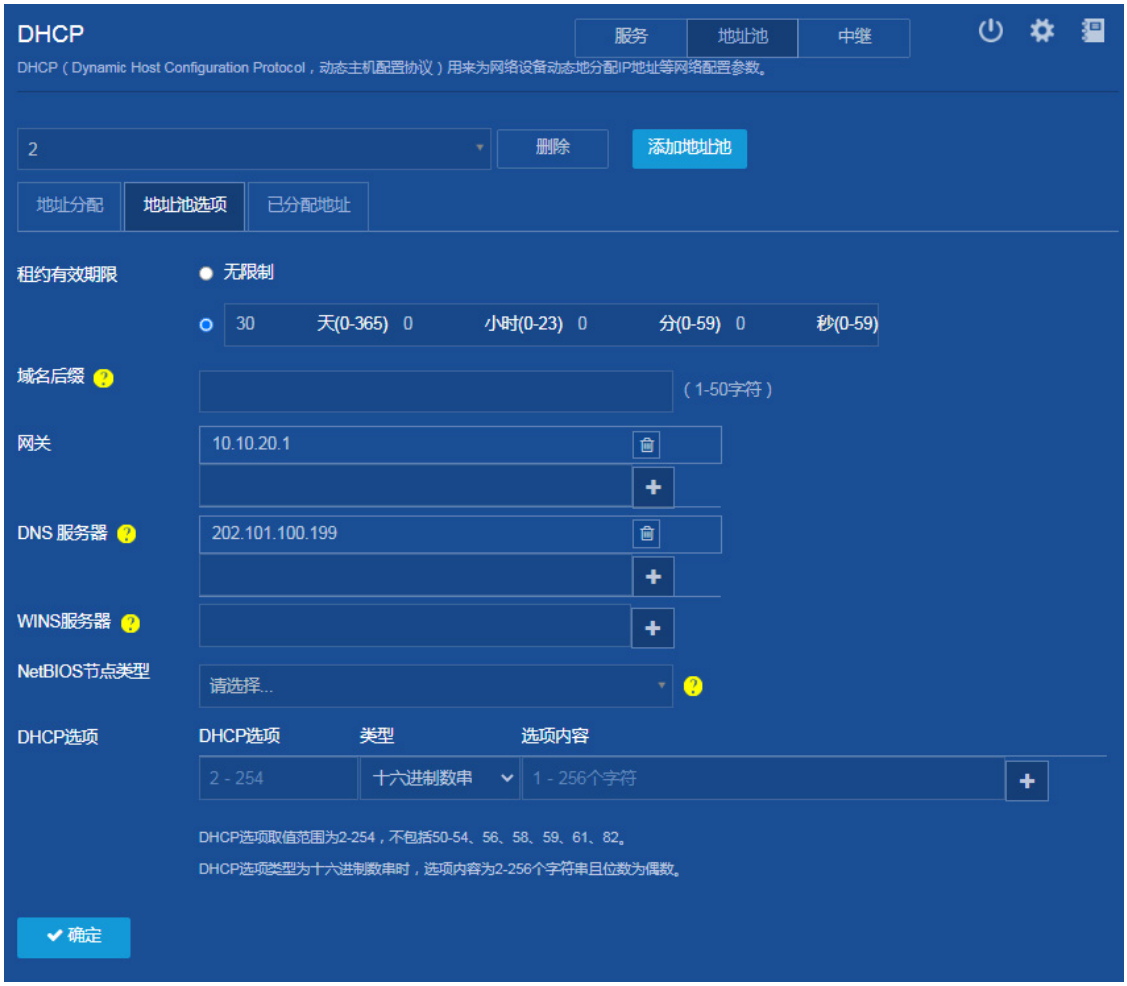


- 在“DHCP”页面，点击“添加地址池”按钮，添加地址池“2”。
- 在地址池 2 的“地址分配”页面，输入动态分配的地址段地址“10.10.20.0”，掩码“255.255.255.0”。

图17 地址池 2 的地址分配配置页面

- 在地址池 2 的“地址池选项”页面，进行如下配置：
  - 配置租约有效期限为“30”天。
  - 配置网关为“10.10.20.1”，点击右侧的“+”按钮，完成添加。
  - 配置 DNS 服务器为“202.101.100.199”，点击右侧的“+”按钮，完成添加。
- 单击<确定>按钮，提示设置成功，完成地址池 2 配置。

图18 地址池 2 的地址池选项配置页面



在“DHCP”页面，点击页面右上角的“服务”按钮，进入 DHCP 服务配置页面，缺省情况下，配置 VLAN 接口 10 和 VLAN 接口 20 均工作在 DHCP 服务器模式，无需修改。

图19 配置接口工作在 DHCP 服务器模式

(5) 配置静态路由

选择页面左侧导航栏的[网络/路由/静态路由]，进入“静态路由”页面，进行如下配置：

- 点击“IPv4 静态路由”右侧的“ ”按钮，进入 IPv4 静态路由配置页面。
- 点击页面右上角的“ ”按钮，进入“添加 IPv4 静态路由”页面。
- 配置目的 IP 地址为“0.0.0.0”、掩码长度为“0”、取消勾选“出接口”、下一跳地址为“10.10.100.2”。该下一跳指向出口路由器，使内网数据可以发到出口路由器。

图20 添加 IPv4 静态路由

(6) 保存配置

点击页面左上方标识和辅助区内的“ ”按钮保存配置。

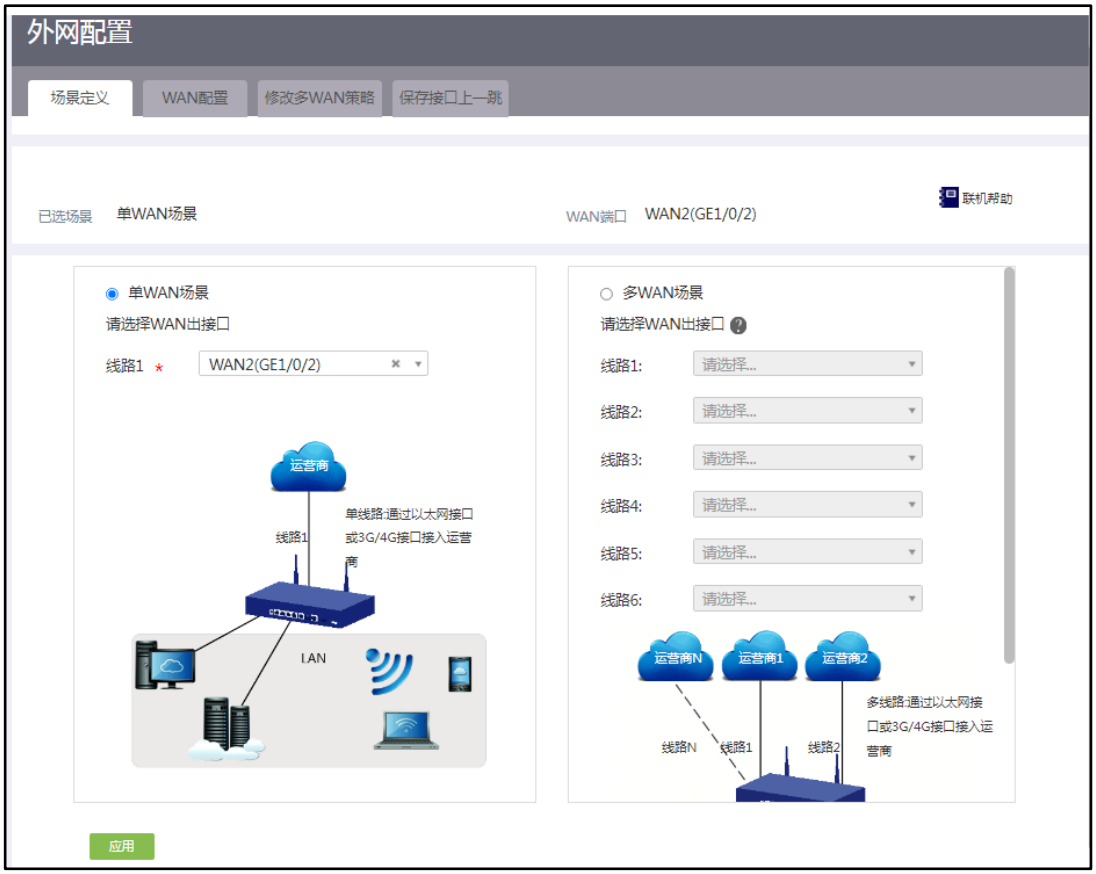
3. 配置出口路由器

(1) 配置公网接口 IP 地址

选择页面左侧导航栏的[网络设置/外网配置]，进入“外网配置”页面。

- 在“场景定义”页面，进行如下配置：
  - 配置场景为“单 WAN 场景”，
  - 选择 WAN 出接口为“WAN2（GE1/0/2）”。
  - 单击<应用>按钮，提示设置成功，完成场景定义。

图21 场景定义



- 在“WAN 配置”页面，进行如下配置：
  - 点击接口 WAN2（GE1/0/2）右侧的操作按钮“”，进入修改“WAN 配置”页面。
  - 选择连接模式为“固定地址”。
  - 配置“IP 地址”为“202.101.100.2”。
  - 配置“子网掩码”为“30”。
  - 单击<确定>按钮，提示设置成功，完成场公网接口 IP 地址的配置。

图22 配置公网接口 IP 地址

(2) 配置内网接口 IP 地址

选择页面左侧导航栏的[网络设置/LAN 配置]，进入“LAN 配置”页面，进行如下配置：

- 点击“LAN 配置”页面右上角的<添加>按钮，进入“添加 LAN”页面。
- 选择“LAN 接口类型”为“GE 接口”。
- 选择 GE 接口为“GE1/0/1”。
- 配置“接口 IP 地址”为“10.10.100.2”。
- 配置“子网掩码”为“24”。
- 单击<确定>按钮，提示设置成功，完成场内网接口 IP 地址的配置。

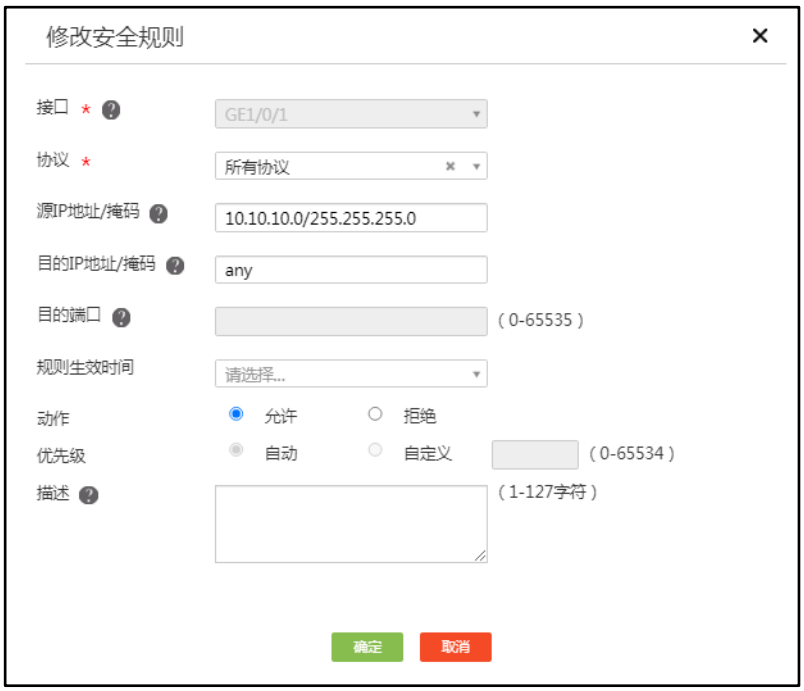
图23 配置内网接口 IP 地址

(3) 配置允许上网的 ACL

选择页面左侧导航栏的[网络安全/防火墙]，进入“防火墙”页面，进行如下配置：

- 单击<添加>按钮，进入“创建安全规则”页面。
- 选择“接口”为“GE1/0/1”。
- 选择“协议”为“所有协议”。
- 配置“源 IP 地址/掩码”为“10.10.10.0/255.255.255.0”。
- 单击<确定>按钮，提示设置成功，完成第一条安全规则的配置。

图24 配置安全规则



- 在“防火墙”页面单击<添加>按钮，进入“创建安全规则”页面。
- 选择“接口”为“GE1/0/1”。
- 选择“协议”为“所有协议”。
- 配置“源 IP 地址/掩码”为“10.10.20.0/255.255.255.0”。
- 单击<确定>按钮，提示设置成功，完成第二条安全规则的配置。
- 在“防火墙”页面单击<添加>按钮，进入“创建安全规则”页面。
- 选择“接口”为“GE1/0/1”。
- 选择“协议”为“所有协议”。
- 配置“源 IP 地址/掩码”为“10.10.100.0/255.255.255.0”。
- 单击<确定>按钮，提示设置成功，完成第三条安全规则的配置。
- 在“防火墙”页面单击<添加>按钮，进入“创建安全规则”页面。
- 选择“接口”为“GE1/0/1”。
- 选择“协议”为“所有协议”。
- 配置“源 IP 地址/掩码”为“0.0.0.0/0.0.0.0”。
- 配置“动作”为“拒绝”。
- 单击<确定>按钮，提示设置成功，完成第四条安全规则的配置。该规则用于拒绝其他源地址的流量访问外网。

配置完成后，在“防火墙”页面，选择接口“GE1/0/1”，查看为该接口配置的所有规则。

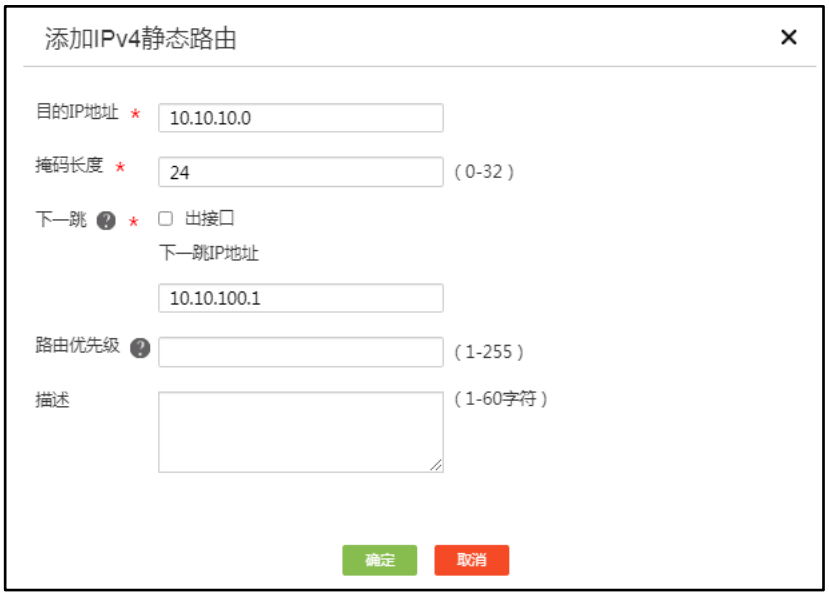
图25 查看所有规则

(4) 配置到内网和公网的路由

选择页面左侧导航栏的[高级选项/静态路由]，进入“静态路由”页面，进行如下配置：

- 点击“静态路由”页面右上角的<添加>按钮，进入“添加 IPv4 静态路由”页面。
- 配置“目的 IP 地址”为“10.10.10.0”
- 配置“掩码长度”为“24”。
- 取消勾选“出接口”。
- 配置“下一跳 IP 地址”为“10.10.100.1”。
- 单击<确定>按钮，提示设置成功，完成第一条静态路由的配置。

图26 添加 IPv4 静态路由



- 在“静态路由”页面，点击右上角的<添加>按钮，进入“添加 IPv4 静态路由”页面。
- 配置“目的 IP 地址”为“10.10.20.0”
- 配置“掩码长度”为“24”。
- 取消勾选“出接口”。
- 配置“下一跳 IP 地址”为“10.10.100.1”。

- 单击<确定>按钮，提示设置成功，完成第二条静态路由的配置。
- 在“静态路由”页面，点击右上角的<添加>按钮，进入“添加 IPv4 静态路由”页面。
- 配置“目的 IP 地址”为“0.0.0.0”
- 配置“掩码长度”为“0”。
- 取消勾选“出接口”。
- 配置“下一跳 IP 地址”为“202.101.100.1”。
- 单击<确定>按钮，提示设置成功，完成第三条静态路由的配置。

(5) 保存配置

选择页面左侧导航栏的[系统工具/配置管理]，进入“配置管理”页面，进行如下配置：

- 点击“备份恢复配置”，进入“备份恢复配置”页面。
- 点击<保存当前配置>按钮，在弹出的对话框中选择“保存到下次启动配置文件”或“保存到指定配置文件”。点击<确定>按钮，提示设置成功，完成当前配置的保存。

图27 备份恢复配置

图28 保存当前配置

1.5 验证配置

完成上述配置后，可以通过如下步骤验证配置是否成功：

(1) 同一个部门内部两台 PC 间可以 ping 通。

以 VLAN 10 所在的业务部门为例，PC1 和 PC2 是通过 ACCSW1 实现二层互通的。假设 PC2 通过 DHCP 自动获取的 IP 为 10.10.10.20，如果 PC1 和 PC2 之间能 ping 通，则说明二层互通正常。

```
<PC1> ping 10.10.10.20
Ping 10.10.10.20 (10.10.10.20): 56 data bytes, press CTRL+C to break
56 bytes from 10.10.10.20: icmp_seq=0 ttl=255 time=1.015 ms
56 bytes from 10.10.10.20: icmp_seq=1 ttl=255 time=2.338 ms
56 bytes from 10.10.10.20: icmp_seq=2 ttl=255 time=1.951 ms
56 bytes from 10.10.10.20: icmp_seq=3 ttl=255 time=1.719 ms
56 bytes from 10.10.10.20: icmp_seq=4 ttl=255 time=1.629 ms

--- Ping statistics for 10.10.10.20 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.015/1.730/2.338/0.434 ms
```

(2) 两个不同部门内的 PC 可以 ping 通。

部门间的通信是通过 CORESW1 上的 VLAN 接口实现的。假设 PC3 通过 DHCP 自动获取的 IP 为 10.10.20.10，如果 PC1 和 PC3 之间互 ping 测试正常，则说明两个部门之间通过 VLAN 接口实现三层互通正常。

```
<PC1> ping 10.10.20.10
Ping 10.10.20.10 (10.10.20.10): 56 data bytes, press CTRL+C to break
56 bytes from 10.10.20.10: icmp_seq=0 ttl=254 time=2.709 ms
56 bytes from 10.10.20.10: icmp_seq=1 ttl=254 time=0.877 ms
56 bytes from 10.10.20.10: icmp_seq=2 ttl=254 time=0.850 ms
56 bytes from 10.10.20.10: icmp_seq=3 ttl=254 time=0.805 ms
56 bytes from 10.10.20.10: icmp_seq=4 ttl=254 time=0.814 ms

--- Ping statistics for 10.10.20.10 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.805/1.211/2.709/0.749 ms
```

(3) 每个部门各选一台 PC 可以 ping 通外网。

以 VLAN 10 所在的业务部门为例，通过在 PC1 上 ping 公网网关地址（即与出口路由器对接的运营商设备的 IP 地址）来验证是否可以访问外网，如果 ping 测试正常，则说明内网用户访问外网正常。测试方法与步骤 1 类似。