设备命令行界面介绍

目 录

1 ComwareV7 常用命令行视图介绍

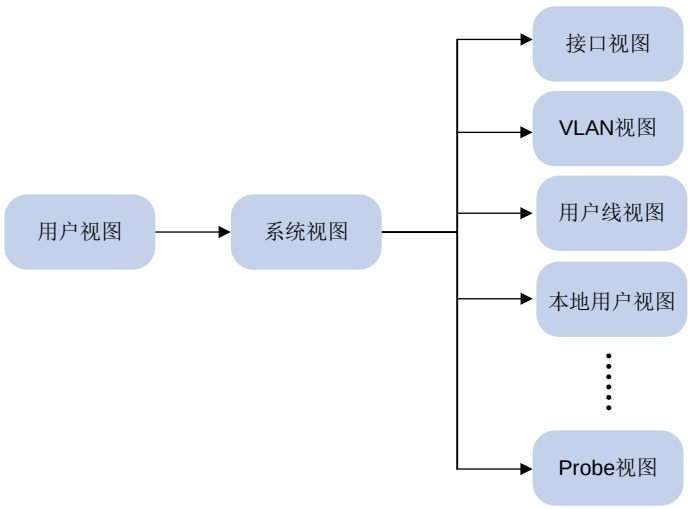
1.1 简介

本节介绍 ComwareV7 常用命令行视图。

设备提供了丰富的功能，不同的功能对应不同的配置和查询命令。为便于用户使用这些命令，设备按功能对命令进行分类组织。功能分类与命令视图对应，当要配置某功能的某条命令时，需要先进入这条命令所在的视图。每个视图都有唯一的、含义清晰的提示符，例如提示符[Sysname-vlan100]表示当前的命令视图是 VLAN 视图，VLAN 的编号是 100，在该视图下可对 VLAN 100 的属性进行配置。

命令视图采用分层结构，如图 1 所示。第一层为用户视图，第二层为系统视图，第三层为各个功能视图。

图1 命令视图示意图



- 用户登录设备后，直接进入用户视图。用户视图下可执行的操作主要包括查看操作、调试操作、文件管理操作、设置系统时间、重启设备、FTP 和 Telnet 操作等。
- 从用户视图可以进入系统视图。系统视图下能对设备运行参数以及部分功能进行配置，例如配置夏令时、配置欢迎信息、配置快捷键等。
- 在系统视图下输入特定命令，可以进入相应的功能视图，完成相应功能的配置，例如：进入接口视图配置接口参数、进入 VLAN 视图给 VLAN 添加端口、进入用户线视图配置登录用户的属性、创建本地用户并进入本地用户视图配置本地用户的属性等。功能视图下可能还包含子视图，例如 NQA 测试组视图下还包含测试类型视图，请参见各功能模块的详细描述。

想要了解某命令视图下支持哪些命令，请在该命令视图提示符后输入<?>。

1.2 进入视图

不同视图的进入方式为：

- 用户登录设备后，直接进入用户视图。

- 从用户视图执行 **system-view** 命令，可以进入系统视图。
- 在系统视图下输入特定命令，可以进入相应的功能视图。功能视图下可能还包含子视图。

1.3 退出视图

除用户视图、Tcl 配置视图、Python shell、公共密钥编辑视图和公共密钥视图外，其他视图的退出方式为：

- 在当前视图执行 **quit** 命令可返回上一级视图。
- 执行 **return** 命令返回用户视图。
- 按快捷键<Ctrl+Z>可返回用户视图，功能等同于 **return** 命令。

用户视图下执行 **quit** 命令后，会断开与设备的连接；用户视图下不能使用 **return** 命令。

Tcl 配置视图、Python shell、公共密钥编辑视图和公共密钥视图的退出方式分别为：

- Tcl 配置视图下请使用 **tclquit** 返回用户视图。
- 在 Python shell 下请通过执行 **exit()**命令，从 Python shell 退回到用户视图。
- 公共密钥编辑视图下请使用 **public-key-code end** 返回上一级视图（公共密钥视图）；公共密钥视图下请使用 **peer-public-key end** 命令返回系统视图。

1.4 用户视图

用户登录设备后，即进入用户视图，在用户视图下可执行的操作主要包括查看操作、调试操作、文件管理操作、设置系统时间、重启设备、FTP 和 Telnet 操作等。

用户视图的提示符为<系统名称>，例如，<Sysname>。用户可以自行配置系统名称。

1.5 系统视图

在用户视图下键入 **system-view** 命令，即进入系统视图。如下所示：

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname]
```

在系统视图下，能对设备运行参数以及部分功能进行配置，例如配置夏令时、配置欢迎信息、配置快捷键等。

1.6 功能视图

在系统视图下，可以分别进入各功能视图。

例如进入以太网接口视图：

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1]
```

例如进入 VLAN 视图：

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2]
```

1.7 相关资料

- 产品配套“基础配置指导”中的“CLI”。
- 产品配套“基础命令参考”中的“CLI”。

2 命令行界面配置说明

2.1 简介

本节介绍命令行界面配置说明。

2.2 使用命令行在线帮助

在命令行输入过程中，可以在命令行的任意位置输入<?>以获得详尽的在线帮助。下面给出常见的在线帮助应用场景，供参考使用。

- 在任意视图下，输入<?>即可获取该视图下可以使用的所有命令及其简单描述。例如：

```
<Sysname> ?
User view commands:
  archive             Archive configuration
  arp                 Address Resolution Protocol (ARP) module
  backup              Backup the startup configuration file to a TFTP server
  boot-loader         Software image file management
……略……
```

- 输入一条命令的关键字，后接以空格分隔的<?>。

  如果<?>位置为关键字，则列出全部关键字及其简单描述。例如：

```
<Sysname> terminal ?
  debugging  Enable to display debugging logs on the current terminal
  logging    Display logs on the current terminal
  monitor    Enable to display logs on the current terminal
```

  如果<?>位置为参数，则列出有关的参数描述。例如：

```
<Sysname> system-view
[Sysname] interface vlan-interface ?
  <1-4094>  Vlan-interface interface number
[Sysname] interface vlan-interface 1 ?
  <cr>
```

  其中，<1-4094>表示该参数的取值范围为 1～4094；<cr>表示命令行当前位置无参数，直接输入回车即可执行。

- 输入命令的不完整关键字，其后紧接<?>，显示以该字符串开头的所有命令关键字及其帮助信息。例如：

```
<Sysname> f?
  fdisk    Partition a storage medium
  fixdisk   Check and repair a storage medium
  format    Format a storage medium
  free      Release a connection
  ftp       Open an FTP connection
<Sysname> display ftp?
  ftp         FTP module
  ftp-server  FTP server information
  ftp-user    FTP user information
```

2.3 命令的undo形式

命令的 **undo** 形式一般用来恢复缺省情况、关闭某个功能或者删除某项设置。大部分配置命令都有对应的 **undo** 形式。例如，**info-center enable** 命令用来开启信息中心，**undo info-center enable** 命令用来关闭信息中心。

2.4 命令行输入

2.4.1 编辑命令行

编辑命令行时，系统支持如表 1 所示的单个按键和如 2.4.6 3. (3)表 4 所示的组合键。

用户通过键盘输入命令行后，按<Enter>键执行该命令。

表1 编辑功能表

按键	功能
普通按键	若编辑缓冲区未满，则插入到当前光标位置，并向右移动光标（命令行下发前会暂时缓存在编辑缓冲区，缓冲区的大小为511个字符，如果编辑缓冲区满，则后续输入的字符无效）
退格键<Backspace>	删除光标位置的前一个字符，光标前移
左光标键<←>	光标向左移动一个字符位置
右光标键<→>	光标向右移动一个字符位置
上光标键<↑>	访问上一条历史命令
下光标键<↓>	访问下一条历史命令
<Tab>键	输入不完整的关键字后按下<Tab>键，系统自动补全关键字： • 如果与之匹配的关键字唯一，则系统用此完整的关键字替代原输入并换行显示 • 如果与之匹配的关键字不唯一，则多次按<Tab>键，系统会循环显示所有以输入字符串开头的关键字 • 如果没有与之匹配的关键字，系统会不作任何修改，重新换行显示原输入

说明

- 在命令行末尾进行自动补全时，如果自动补全后整条命令行超过编辑缓冲区的大小（编辑缓冲区的大小为 511 个字符），则系统不再进行补全。
- 在配置文件中，存在#和 version 7.1.xxx, Release xxx 这样的特殊命令行配置信息。#用于将两段配置信息隔开；version 7.1.xxx, Release xxx 用于记录设备正在运行的软件包的版本信息。这样的命令行不支持在线帮助，但可以在任意视图下执行# xxx 或者在系统视图下执行 **version** xxx（例如执行# abc 或者 **version** abc），执行后系统不会提示错误信息，也不会修改这些行的值。这样的命令行用户没有必要使用，因此在命令手册中不再描述。

2.4.2 STRING 和 TEXT 类型参数的输入

如果命令行中的参数为 STRING 类型，则建议输入除“?”、“"”、“\”、空格之外的可见字符（可见字符对应的 ASCII 码区间为 32～126），以免设备将该参数传递给其它网络设备时，对端设备无法解析。如果 STRING 类型的参数中需要包含字符“"”、“\”，则必须使用转义字符“\”辅助输入，即实际应输入“\"”、“\\”；如需输入空格，则需要将整个字符串包含在双引号中，例如，若要配置字符串参数为“my device”，则实际应输入“"my device"”。

如果命令行中的参数为 TEXT 类型，则除了“?”外的其他字符均可输入。

各业务模块可能对参数有更多的输入限制，详情请参见命令的提示信息以及命令参考中的参数描述。

2.4.3 接口类型的输入

输入接口类型时，设备支持使用接口类型的全称和简称。使用接口类型的全称时，支持不完整的字符输入；使用接口类型简称时，必须输入完整的简称。两种方式输入的接口类型均不区分大小写。例如在输入 **`interface gigabitethernet 1/0/1`** 时，可以使用接口类型全称的不完整字符 **`interface g 1/0/1`**，也可以使用接口类型简称 **`interface ge 1/0/1`**。接口类型和接口编号之间无论输入空格与否，都可以成功进入接口视图。关于接口全名与简名的对应关系请参见下表。

表2 接口类型的全称和简称对应表

接口类型全称	接口类型简称
Bridge-Aggregation	BAGG
Ethernet	Eth
EVI-Link	EVI
FiftyGigE	50GE
FortyGigE	FGE
FourHundredGigE	400GE
GigabitEthernet	GE
HundredGigE	HGE
InLoopBack	InLoop
LoopBack	Loop
M-Ethernet	ME
M-GigabitEthernet	MGE
Multicast Tunnel	MTunnel
NULL	NULL
Pex	PEX
RPR-Bridge	RPR-B
RPR-Router	RPR-R
Register-Tunnel	REG
Route-Aggregation	RAGG
SAN-Aggregation	SAGG

接口类型全称	接口类型简称
S-Channel	S-Ch
Schannel-Aggregation	SCH-AGG
Schannel-Bundle	SCH-B
Smartrate-Ethernet	SGE
Ten-GigabitEthernet	XGE
Tunnel	Tun
Tunnel-Bundle	Tunnel-B
TwentyGigE	TGE
Twenty-FiveGigE	WGE
Vfc	Vfc
Vsi-interface	Vsi
Vlan-interface	Vlan-int

2.4.4 快速输入命令行

设备支持不完整关键字输入，即在当前视图下，当输入的字符足够匹配唯一的关键字时，可以不必输入完整的关键字。该功能提供了一种快捷的输入方式，有助于提高操作效率。

例如用户视图下以 **s** 开头的命令有 **startup saved-configuration**、**system-view** 等。

- 如果要输入 **system-view**，可以直接输入 **sy**（不能只输入 **s**，因为只输入 **s** 时，匹配到的关键字不唯一）。
- 如果要输入 **startup saved-configuration**，可以直接输入 **st s**。

可以按<Tab>键由系统自动补全关键字的全部字符，以确认系统的选择是否为所需输入的关键字。

2.4.5 配置命令字符串的别名

1. 功能简介

通过本命令用户可以为命令行指定一个或多个别名，也可以为命令行开头的一个或多个关键字配置多个别名，使其符合用户的使用习惯。例如：

- 将命令 **display ip routing-table** 的别名配置为 **shiprt** 后，就可以使用别名命令 **shiprt** 来代替执行命令 **display ip routing-table**。
- 将命令关键字 **display ip** 的别名配置为 **ship**，就可以用别名命令 **ship** 执行所有以 **display ip** 开头的命令行，如可以使用 **ship routing-table** 代替执行 **display ip routing-table**，使用 **ship interface** 代替执行 **display ip interface**。

用户成功执行的带别名的命令将以系统原始的命令形式被显示或存储。

为了方便用户使用，系统定义了部分常用的关键字作为缺省别名，如表 3 所示。

表3 系统定义的缺省别名

缺省别名	命令
access-list	**acl**
end	**return**
erase	**delete**
exit	**quit**
hostname	**sysname**
logging	**info-center**
no	**undo**
show	**display**
write	**save**

2. 配置限制和指导

使用本特性，只有当命令行第一个关键字或者 **undo** 命令的第二个关键字是别名时，才按照别名命令替换执行，否则按照非别名命令执行。例如：

用户成功执行的带别名的命令将以系统原始的命令形式被显示或存储。

配置别名时，可以使用$n 表示命令行中的参数或者关键字，这样既可以用别名替代部分关键字来简化输入，又可以根据实际需要指定不同的参数或者关键字，增加了灵活性。$n 最多可以使用 9 次，n 为 1～9 的整数，表示参数或关键字出现的顺序。如果别名命令中定义了参数，则参数必须输入完整。比如，将命令 **display ip $1 | include $2** 的别名配置为 **shinc** 后，如果需要执行 **display ip routing-table | include Static** 命令来筛选并查看路由表中的所有静态路由信息，可直接执行 **shinc routing-table Static**。

系统定义的缺省别名无法取消。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 给指定的命令字符串配置别名。

alias *alias command*

系统定义的缺省别名命令，请参见 1. 表 3。

(3) （可选）可在任意视图下执行本命令，显示命令字符串别名功能的相关配置。

display alias [*alias*]

2.4.6 修改快捷键的绑定关系

1. 功能简介

为方便用户快捷操作设备，设备支持 23 个快捷键，用户可以修改除“CTRL_]”外的 22 个快捷键的绑定关系。用户按下快捷键后，设备会立即执行对应的命令行或者功能。如果这些快捷键和用户

登录终端定义的快捷键冲突，或者不符合用户的使用习惯，用户可使用该命令重新定义快捷键，甚至取消快捷键的绑定关系。

2. 配置限制和指导

一个快捷键对应一个命令或功能，如果使用本命令多次定义同一快捷键，则最新配置生效。如果多次使用本命令将多个快捷键和同一命令、功能绑定，则这些绑定的快捷键均生效。

当用户使用终端软件与设备进行交互时，如果终端软件定义快捷键（包括用户可定义和系统保留快捷键），则快捷键会遵从终端软件的定义。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 修改快捷键的绑定关系。

hotkey *hotkey* { *command* | **function** *function* | **none** }

缺省情况下，各快捷键的绑定关系见(3)表 4。

(3) （可选）可在任意视图下执行本命令，显示系统中快捷键的分配信息。

display hotkey

表4 快捷键的缺省绑定关系

快捷键	缺省绑定的功能或命令
CTRL_A	move_the_cursor_to_the_beginning_of_the_line，表示将光标移动到当前行的开头
CTRL_B	move_the_cursor_one_character_to_the_left，表示将光标向左移动一个字符
CTRL_C	stop_the_current_command，表示停止当前正在执行的功能
CTRL_D	erase_the_character_at_the_cursor，表示删除当前光标所在位置的字符
CTRL_E	move_the_cursor_to_the_end_of_the_line，表示将光标移动到当前行的末尾
CTRL_F	move_the_cursor_one_character_to_the_right，表示将光标向右移动一个字符
CTRL_G	**display current-configuration**，表示显示当前配置
CTRL_H	erase_the_character_to_the_left_of_the_cursor，表示删除光标左侧的一个字符
CTRL_L	**display ip routing-table**，表示显示IPv4路由表信息
CTRL_N	display_the_next_command_in_the_history_buffer，表示显示历史缓冲区中的下一条命令（密码配置命令会跳过）
CTRL_O	**undo debugging all**，表示关闭所有功能项的调试开关
CTRL_P	display_the_previous_command_in_the_history_buffer，表示显示历史缓冲区中的上一条命令（密码配置命令会跳过）
CTRL_R	redisplay_the_current_line，表示重新显示当前行信息
CTRL_T	未绑定任何命令行或功能
CTRL_U	未绑定任何命令行或功能
CTRL_W	delete_the_word_to_the_left_of_the_cursor，表示删除光标左侧连续字符串内的所有字符

快捷键	缺省绑定的功能或命令
CTRL_X	delete_all_characters_from_the_beginning_of_the_line_to_the_cursor，表示删除光标左侧所有的字符
CTRL_Y	delete_all_characters_from_the_cursor_to_the_end_of_the_line，表示删除光标所在位置及其右侧所有的字符
CTRL_Z	return_to_the_User_View，表示退回到用户视图
CTRL_]	kill_incoming_connection_or_redirect_connection，表示终止当前连接
ESC_B	move_the_cursor_back_one_word，表示将光标移动到左侧连续字符串的首字符处
ESC_D	delete_all_characters_from_the_cursor_to_the_end_of_the_word，表示删除光标所在位置及其右侧连续字符串内的所有字符
ESC_F	move_the_cursor_forward_one_word，表示将光标向右移到下一个连续字符串之前

2.4.7 命令行输入回显功能

1. 功能简介

当用户在未完成输入操作却被大量的系统信息打断时，开启此功能可以回显用户已经输入而未提交执行的信息，方便用户继续完成未输入的内容。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 打开命令行输入回显功能。

info-center synchronous

缺省情况下，命令行输入回显功能处于关闭状态。

本命令的详细介绍请参见“网络管理和监控命令参考”中的“信息中心”。

2.5 解读输入错误提示信息

命令行输入完毕后，请按<Enter>键执行该命令。设备执行命令的过程中，首先会对命令行进行合法性检查。如果通过合法性检查，则正确执行；否则，输出错误信息，常见的错误信息如表 5 所示。

表5 命令行常见错误信息表

英文错误信息	错误原因
% Unrecognized command found at '^' position.	命令无法解析，符号“^”指示位置出错
% Incomplete command found at '^' position.	符号“^”指示位置的参数输入不完整
% Ambiguous command found at '^' position.	符号“^”指示位置的关键字不明确，存在二义性
% Too many parameters found at '^' position.	符号“^”指示位置的参数输入太多
% Wrong parameter found at '^' position.	在符号“^”指示位置的参数错误

2.6 使用历史命令

2.6.1 功能简介

用户在设备上成功执行的命令，会同时保存到用户独享的历史命令缓冲区和所有用户共享的历史命令缓冲区。

表6 历史命令缓冲区描述表

选项	独享历史命令缓冲区	共享历史命令缓冲区
内容	当前用户执行成功的命令	所有用户执行成功的命令
查看	支持	支持
调用	支持	不支持
保存	不保存	保存
调整大小	支持	大小固定为1024条

2.6.2 配置限制和指导

设备保存用户执行过的命令时，遵循以下原则：

- 如果用户使用了命令的不完整形式，保存的历史命令也是不完整形式。
- 如果用户使用了命令字符串的别名形式，保存的历史命令是原始命令形式。
- 如果用户连续多次执行同一条命令，设备的历史命令中只保留一次。但如果执行时输入的形式不同，将作为不同的命令对待。例如：连续多次执行 **display current-configuration** 命令，设备只保存一条历史命令；如果分别执行 **display current-configuration** 命令和它的不完整形式 **display cu**，设备将保存为两条历史命令。
- 如果当前历史命令缓冲区满且有新的命令需要缓存，则自动删除最早的记录，来保存新命令。

2.6.3 操作历史命令缓冲区

1. 查看历史命令缓冲区

- 可在任意视图下执行本命令，查看独享历史命令缓冲区。

  display history-command
- 可在任意视图下执行本命令，查看共享历史命令缓冲区。

  display history-command all

2. 调用历史命令缓冲区

使用上光标键↑并回车，调用上一条历史命令；使用下光标键↓并回车，可调用下一条历史命令。但是该操作不支持调用密码配置命令。

3. 配置命令缓冲区的大小

在用户线/用户线类视图下执行 **history-command max-size** 命令，可调整独享历史命令缓冲区大小。具体配置请参见“基础配置命令参考”中的“登录设备”。

2.6.4 重复执行历史记录命令

1. 功能简介

当需要重复执行最近的历史记录命令时，使用 **repeat** 命令可以重复多次执行多条历史命令，并且可以设置每次重复执行历史命令的时间间隔。

2. 配置限制和指导

- 重复执行历史命令时，系统将按照历史命令的下发顺序执行。例如，用户在某视图下依次执行命令 a、b 和 c 后，再执行 **repeat** 3 命令，则系统将按照 a、b 和 c 的顺序重复执行。
- 重复执行某条历史命令时，需要先进入该命令所在的视图。重复执行多条历史命令时，需要先进入第一条命令所在的视图。
- 如果用户重复执行的历史命令中存在交互式命令，需要用户手工输入交互信息来完成该命令的执行或者等待系统超时退出执行该命令，交互命令处理结束后，系统会继续执行其他历史命令。
- 如果用户重复执行的历史命令中存在密码配置命令，系统会跳过密码配置命令。

3. 配置步骤

可在任意视图下执行本命令，重复执行历史记录命令。

repeat [*number*] [**count** *times*] [**delay** *seconds*]

2.7 便捷地查看显示信息

2.7.1 控制显示信息的分屏

1. 功能简介

缺省情况下，设备支持分屏显示功能，即当显示信息超过一屏时，系统会将信息分屏显示，并在屏间显示“----more----”信息，表示这一屏信息已经显示完毕，自动暂停，方便查看显示信息。这时用户可以使用表 7 所示的按键来选择下一步操作。

表7 分屏显示功能表

按键	功能
空格键	继续显示下一屏信息
回车键	继续显示下一行信息
<Ctrl+C>	停止显示，退回到命令行编辑状态
<PageUp>	显示上一页信息
<PageDown>	显示下一页信息

如果想要一次查看全部显示信息，可以通过以下配置关闭当前登录用户的分屏显示功能。分屏显示功能处于关闭状态时，如果信息较多，则会连续刷屏，不方便查看。

2. 关闭分屏显示功能

请在用户视图下执行本命令，关闭当前用户的分屏显示功能。

screen-length disable

缺省情况下，用户登录后将遵循用户线下的 **screen-length** 设置。**screen-length** 设置的缺省情况为：允许分屏显示，下一屏显示 24 行数据。**screen-length** 命令的详细介绍请参见“基础配置命令参考”中的“登录设备”

命令的执行仅对当前用户本次登录有效，用户重新登录后将恢复到缺省情况。

2.7.2 查看带行号的显示信息

1. 功能简介

在用 **display** 命令查看显示信息时，用户可以用 **by-linenum** 参数在显示信息的同时显示信息行号，方便定位显示信息。

行号占 5 个字符，通常行号后面接“:”。当 **by-linenum** 和 **begin** 参数一起使用时，行号后面还可能接“-”，其中“:”表示该行符合匹配规则，“-”表示该行不符合匹配规则。

2. 配置步骤

按行显示 **display** 命令执行结果。

display *command* **| by-linenum**

3. 配置举例

显示 VLAN 999 信息的同时显示行号。

```
<Sysname> display vlan 999 | by-linenum
    1:  VLAN ID: 999
    2:  VLAN type: Static
    3:  Route interface: Configured
    4:  IPv4 address: 192.168.2.1
    5:  IPv4 subnet mask: 255.255.255.0
    6:  Description: For LAN Access
    7:  Name: VLAN 0999
    8:  Tagged ports:   None
    9:  Untagged ports: None
```

2.7.3 使用正则表达式过滤显示信息

1. 功能简介

在执行 **display** 命令查看显示信息时，可以使用正则表达式来过滤显示信息，以便快速的找到自己关注的信息。

在 **display** 命令中通过输入**[| [by-linenum] { begin | exclude | include }** *regular-expression* **]&<1-128>**参数的方式来过滤显示。各关键字的含义如下：

- **by-linenum**：表示带行号显示。当多次使用正则表达式对显示信息过滤时，**by-linenum** 参数只需要输入一次即可生效。不指定该参数时，表示不带行号显示。
- **begin**：显示特定行及其以后的所有行，该特定行必须包含指定正则表达式。
- **exclude**：显示不包含指定正则表达式的所有行。
- **include**：只显示包含指定正则表达式的所有行。
- **&<1-128>**：表示前面的参数最多可以输入 128 次。

正则表达式（*regular-expression*）为 1～256 个字符的字符串，区分大小写，它支持多种特殊字符，特殊字符的匹配规则如表 8 所示。

表8 正则表达式中的特殊字符描述表

特殊字符	含义	举例
^	匹配以指定字符开始的行	^u只能匹配以u开始的行，不能匹配以Au开始的行
$	匹配以指定字符结束的行	u$只能匹配以u结尾的行，不能匹配以uA结尾的行
.	通配符，可代表任何一个字符	.s可以匹配as和bs等
*	匹配星号前面的字符或字符串零次或多次	• zo*可以匹配 z 以及 zoo • (zo)*可以匹配 zo 以及 zozo
+	匹配+前面的字符或字符串一次或多次	zo+可以匹配zo以及zoo，但不能匹配z
|	匹配|左边或右边的整个字符串	def|int只能匹配包含def或者int的字符串所在的行
( )	表示字符串，一般与“+”或“*”等符号一起使用	(123A) 表示字符串 123A；408(12)+ 可以匹配 40812 或 408121212等字符串，但不能匹配408
\index	表示重复一次指定字符串，字符串是指\前用()括起来的字符串，index对应\前字符串的顺序号按从左至右的顺序从1开始编号：如果\前面只有一个字符串，则index只能为1；如果\前面有n个字符串，则index可以为1到n中的任意整数	(string)\1表示把string重复一次，匹配的字符串必须包含stringstring；(string1)(string2)\2表示把string2重复一次，匹配的字符串必须包含string1string2string2；(string1)(string2)\1\2表示先把string1重复一次，再重复一次string2，匹配的字符串必须包含string1string2string1string2
[ ]	表示字符选择范围，将以选择范围内的单个字符为条件进行匹配，只要字符串里包含该范围的某个字符就能匹配到	• [16A]表示可以匹配到的字符串只需要包含 1、6 或 A 中任意一个 • [1-36A] 表示可以匹配到的字符串只需要包含 1、2、3、6 或 A 中任意一个（-为连接符） 如果]需要作为普通字符出现在[ ]内时，必须把]写在[ ]中字符的最前面，形如[]string]，才能匹配到]。[没有这样的限制
[^]	表示选择范围外的字符，将以单个字符为条件进行匹配，只要字符串里包含该范围外的某个字符就能匹配到	[^16A]表示可匹配的字符串只需要包含1、6和A之外的任意字符，该字符串也可以包含字符1、6或A，但不能只包含这三个字符。例如[^16A]可以匹配abc、m16，不能匹配1、16、16A
{n}	n是一个非负整数，匹配n次	o{2}不能匹配Bob，但是能匹配food
{n,}	n是一个非负整数，至少匹配n次	o{2,}不能匹配Bob，但能匹配foooood
{n,m}	m和n均为非负整数，其中n小于等于m。只要字符串里包含n到m个某字符就能匹配到	o{1,3}能匹配fod、food、foood、fooood，但不能匹配fd
\<	匹配包含指定字符串的字符串，字符串前面如果有字符则不能是数字、字母和下划线	\<do匹配单词domain，还可以匹配字符串doa
\>	匹配包含指定字符串的字符串，字符串后面如果有字符则不能是数字、字母和下划线	do\>匹配单词undo，还可以匹配字符串cdo
\b	匹配一个单词边界，也就是指单词和空格间的位置	er\b可以匹配never，但不能匹配verb \ber可以匹配erase，但不能匹配verb

特殊字符	含义	举例
\B	匹配非单词边界	er\B能匹配verb，但不能匹配never
\w	\w等效于[A-Za-z0-9_]，是数字、字母或下划线	v\w能匹配vlan，v\w还能匹配service
\W	\W等效于[^A-Za-z0-9_]，是除了数字、字母和下划线之外的任意字符	\Wa可以匹配-a，但是不能匹配2a和ba等
\	转义操作符，\后紧跟本表中罗列的单个特殊字符时，将去除特殊字符的特定含义	• \\可以匹配包含\的字符串 • \^可以匹配包含^的字符串 • \\b 可以匹配包含\b 的字符串

2. 配置限制和指导

正则表达式的执行时间和正则表达式的复杂程度成正比，对于复杂的正则表达式，执行时间会比较长，如有需要，可按<CTRL+C>键终止。

3. 配置举例

查看当前生效的配置中，从包含“line”字符串的行开始到最后一行的配置信息（该显示信息与设备型号以及用户的当前配置有关）。

```
<Sysname> display current-configuration | begin line
line class aux
 user-role network-admin
#
line class vty
 user-role network-operator
#
line aux 0
 user-role network-admin
#
line vty 0 63
 authentication-mode none
 user-role network-admin
 user-role network-operator
#
……略……
```

查看设备当前处于 UP 状态的接口概要信息。

```
<Sysname> display interface brief | exclude DOWN
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Protocol: (s) - spoofing
Interface            Link Protocol Primary IP      Description
InLoop0              UP   UP(s)    --
NULL0                UP   UP(s)    --
Vlan1                UP   UP       192.168.1.83

Brief information on interfaces in bridge mode:
```

```
Link: ADM - administratively down; Stby - standby
Speed: (a) - auto
Duplex: (a)/A - auto; H - half; F - full
Type: A - access; T - trunk; H - hybrid
Interface            Link Speed    Duplex Type PVID Description
GE1/0/1              UP   1000M(a) F(a)  A    1
```

查看 SNMP 相关配置。

```
<Sysname> display current-configuration | include snmp
 snmp-agent
 snmp-agent community write private
 snmp-agent community read public
 snmp-agent sys-info version all
 snmp-agent target-host trap address udp-domain 192.168.1.26 params securityname public
```

显示日志缓冲区中包含 SHELL 字符串且包含 VTY 字符串的日志。

```
<Sysname> display logbuffer | include SHELL | include VTY
%Sep  6 10:38:12:320 2018 Sysname SHELL/5/SHELL_LOGIN: VTY logged in from 169.254.100.171.
%Sep  6 10:52:32:576 2018 Sysname SHELL/5/SHELL_LOGOUT: VTY logged out from 169.254.100.171.
%Sep  6 16:03:27:100 2018 Sysname SHELL/5/SHELL_LOGIN: VTY logged in from 169.254.100.171.
%Sep  6 16:44:18:113 2018 Sysname SHELL/5/SHELL_LOGOUT: VTY logged out from 169.254.100.171.
```

2.7.4 将显示信息保存到指定文件

1. 功能简介

display 命令显示的内容通常是统计信息、功能是否开启以及功能的相关参数配置，这些信息在设备运行过程中会随着时间或者用户的配置而改变。使用本配置可以将当前显示信息保存到指定文件，方便随时比对和查看。

有两种方式将显示信息保存到文件中：

- 将显示信息独立保存到指定文件：使用该方式时，该文件只包含该显示信息的内容。
- 将显示信息以追加方式保存到已有文件：使用该方式时，该命令的显示信息会追加在指定文件的尾部保存，该文件能包含多条显示信息的内容。

2. 配置步骤

- 请在任意视图下执行本命令，将显示信息独立保存到指定文件。

  display *command* **>** *filename*
- 请在任意视图下执行本命令，将显示信息以追加方式保存到已有文件。

  display *command* **>>** *filename*

3. 配置举例

将 **display vlan 1** 命令的显示信息保存到指定文件 vlan.txt。

```
<Sysname> display vlan 1 > vlan.txt
```

查看 vlan.txt 的内容，验证 **display >**命令的执行效果。

```
<Sysname> more vlan.txt
VLAN ID: 1
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0001
```

```
 Name: VLAN 0001
 Tagged ports:   None
 Untagged ports: None
```

将 **display vlan 999** 的显示信息以追加方式保存到指定文件 vlan.txt。

```
<Sysname> display vlan 999 >> vlan.txt
```

查看 vlan.txt 的内容，验证 **display >>**命令的执行效果。

```
<Sysname> more vlan.txt
VLAN ID: 1
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0001
 Name: VLAN 0001
 Tagged ports:   None
 Untagged ports: None
 VLAN ID: 999
 VLAN type: Static
 Route interface: Configured
 IP address: 192.168.2.1
 Subnet mask: 255.255.255.0
 Description: For LAN Access
 Name: VLAN 0999
 Tagged ports:   None
 Untagged ports: None
```

2.7.5 各种便捷查看方式的综合应用

1. 功能简介

执行 **display** 命令时，通过选择参数，可以同时实现“2.7.2 查看带行号的显示信息”、“2.7.3 使用正则表达式过滤显示信息”和“2.7.4 将显示信息保存到指定文件”。

2. 配置步骤

请在用户视图下执行本命令，以综合使用各种方式便捷地查看显示信息。

display *command* [**|** [**by-linenum**] { **begin** | **exclude** | **include** } *regular-expression*]&<1-128> [**>** *filename* | **>>** *filename*]

3. 配置举例

下面将通过举例示意如何将各种便捷查看方式综合应用。

按行号将当前配置保存到文件 test.txt。

```
<Sysname> display current-configuration | by-linenum > test.txt
```

将 SNMP 的相关配置以追加方式保存到文件 test.txt。

```
<Sysname> display current-configuration | include snmp >> test.txt
```

查看当前配置，从包含“user-group”字符串的行开始到最后一行配置信息，并同时显示行号。（行号后为“:”表示该行包含“user-group”字符串，行号后为“-”表示该行不包含“user-group”字符串。）

```
<Sysname> display current-configuration | by-linenum begin user-group
  114:  user-group system
```

```
115-  #
116-  return
```

2.8 相关资料

- 产品配套“基础配置指导”中的“CLI”。
- 产品配套“基础命令参考”中的“CLI”。

登录设备快速配置指南

目 录

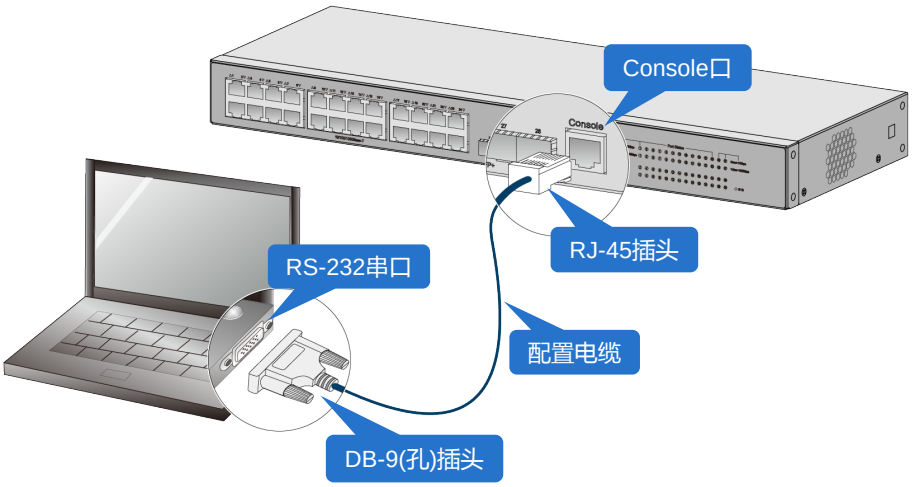
1 通过 Console 口登录设备

1.1 简介

本案例介绍如何通过 Console 口登录设备。

1.2 组网需求

图1 通过 Console 口连接设备（以使用 DB9-to-RJ45 Console 口电缆为例）



1.3 配置准备

- 终端软件：PuTTY、VTP 等软件。
- 配置电缆：H3C 设备支持的配置电缆如表 1 和表 2 所示。不同产品支持的配置电缆类型存在差异。设备标配的配置电缆和可以选配的配置电缆请参见安装手册。

说明

不同厂商提供的串行 Console 口电缆 RJ-45 连接器引脚定义可能存在差异，为避免配置终端显示异常，推荐您选配 H3C 提供的串行 Console 口电缆，具体编码参见表 2；如果您需要自备串行 Console 口电缆，请确保所选电缆 RJ-45 连接器引脚定义与表 3 一致。

表1 配置电缆类型

配置连接方式	配置电缆类型	配置终端侧连接器类型	交换机侧连接器类型
通过串行Console口电缆连接	DB9-to-RJ45 Console口电缆	DB-9孔式插头	RJ-45

配置连接方式	配置电缆类型	配置终端侧连接器类型	交换机侧连接器类型
	USB-to-RJ45 Console口电缆	USB口	RJ-45
通过Mini USB Console口电缆连接	Mini USB Console口电缆	USB口	USB mini-Type B
通过Micro USB Console口电缆连接	Micro USB Console口电缆	USB口	USB micro-Type B

表2 配置电缆图示

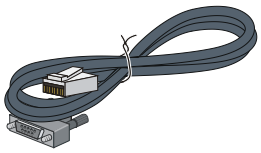
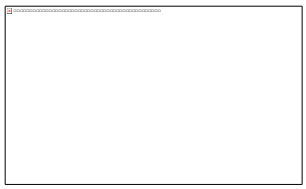
配置电缆类型	图示	H3C 编码
DB9-to-RJ45 Console口电缆		04042967
USB-to-RJ45 Console口电缆		0404A1EE
Mini USB Console口电缆		-
Micro USB Console口电缆		-

表3 DB9-to-RJ45 Console 口电缆连接关系

RJ-45	Signal	DB-9	Signal
1	RTS	8	CTS
2	DTR	6	DSR
3	TXD	2	RXD
4	SG	5	SG
5	SG	5	SG
6	RXD	3	TXD
7	DSR	4	DTR
8	CTS	7	RTS

1.4 配置步骤

(1) 如 1.2 图 1 所示，本文使用 DB9-to-RJ45 Console 口电缆连接设备为例进行介绍。使用配置电缆连接 PC 机与设备后，右击【计算机】选择【属性】--【设备管理器】--【端口】，查看确认电脑上使用的通信端口，本案例中使用 COM1，如图 2 所示。

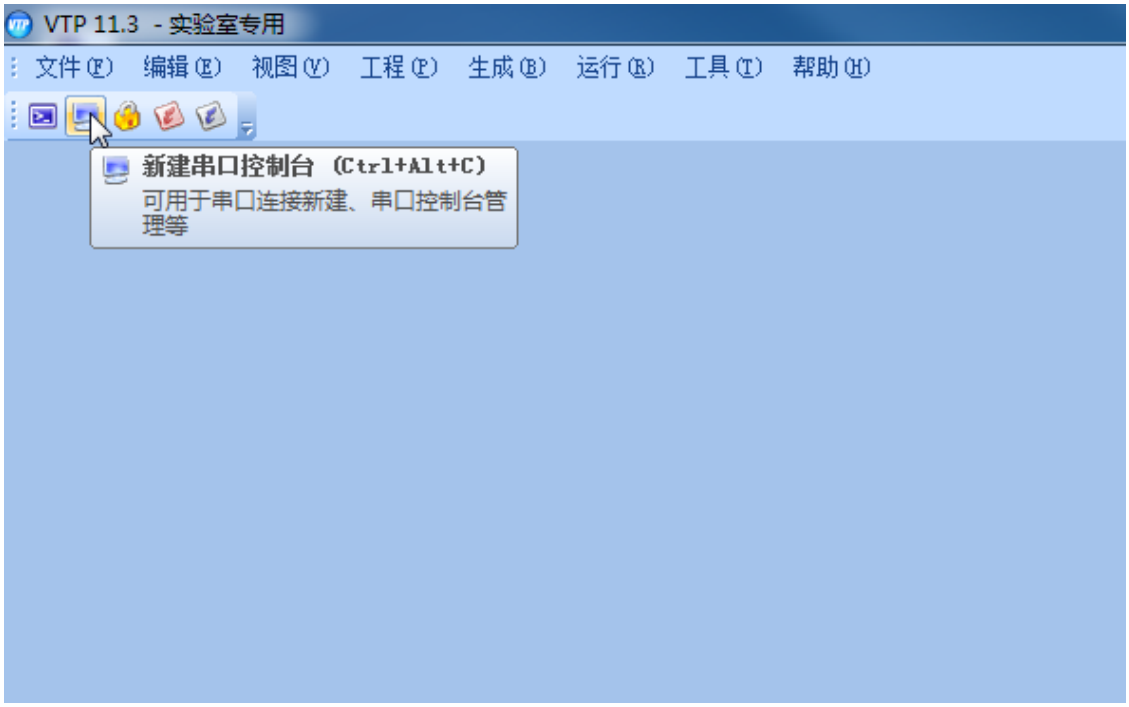
注意

若使用 USB-to-RJ45 Console 口电缆、Mini USB Console 口电缆或 Micro USB Console 口电缆连接 PC 机与设备，PC 机需安装相应驱动后才会识别到端口。驱动程序的获取和安装方式请参考产品安装手册。

图2 确认通信端口

(2) 打开 PC 机上的终端软件，本文以 VTP 软件为例。如图 3 所示，新建串口控制台。

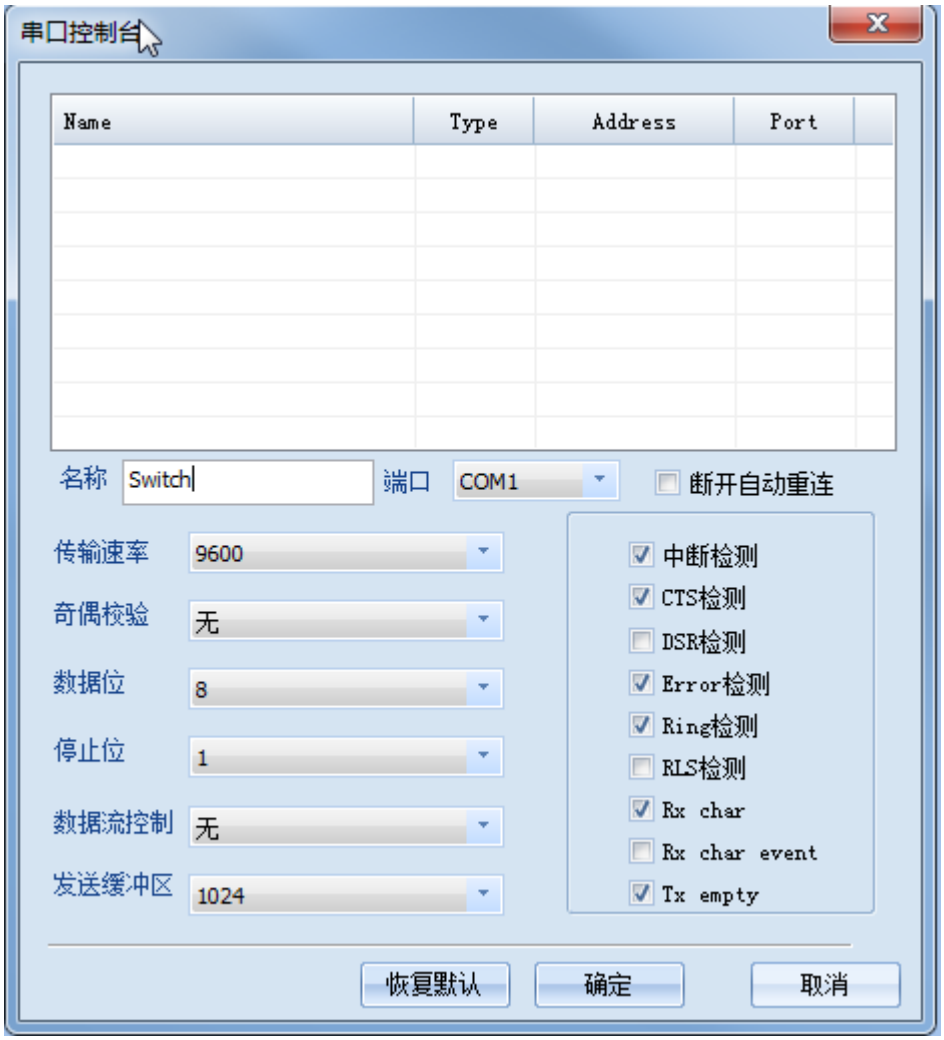
图3 新建串口工作台



(3) 如图 4 所示，输入设备名称 Switch，端口选择 COM1，配置如下终端控制参数后点击确定。

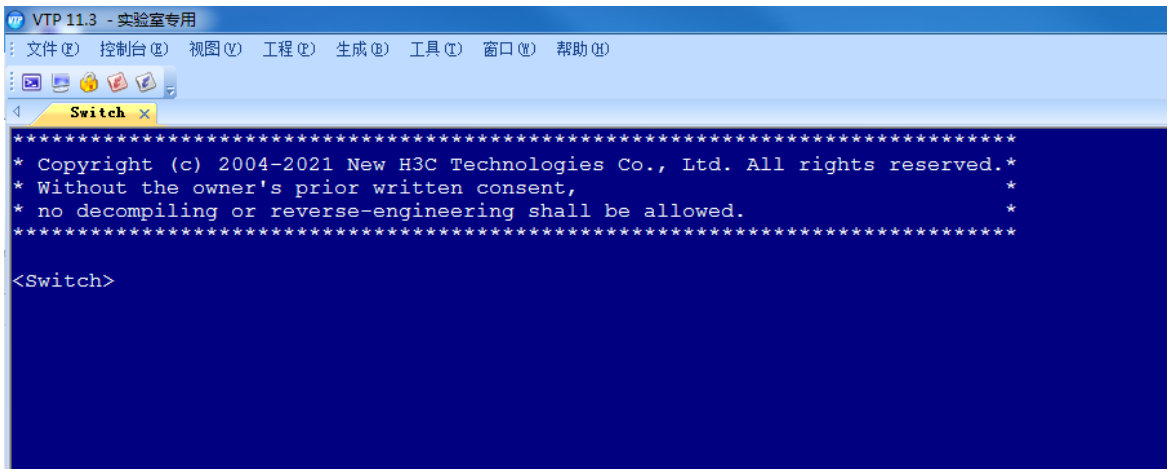
- 波特率：9600
- 数据位：8
- 停止位：1
- 奇偶校验：无
- 流量控制：无

图4 配置终端参数



(4) 进入图 5 所示命令行页面，表示 PC 机使用 Console 线连接设备成功。

图5 成功连接设备



1.5 配置文件

无

1.6 相关资料

- 产品配套“基础配置指导”中的“登录设备”。
- 产品配套“基础配置命令参考”中的“登录设备”。

2 通过 Telnet 登录设备

2.1 简介

本案例介绍通过 Telnet 登录设备的配置方法。

2.2 组网需求

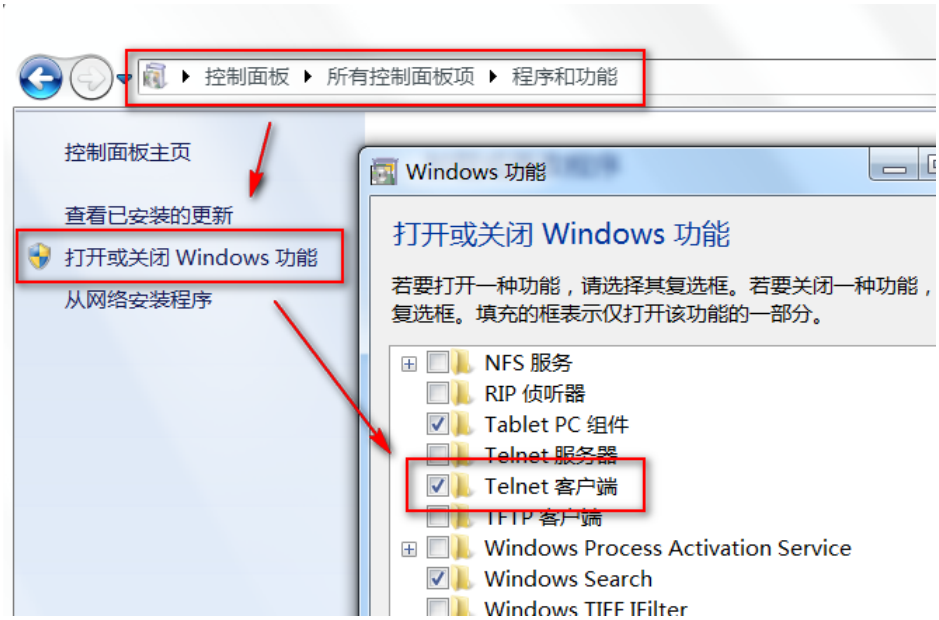
如图 6 所示，将 Host A 的网口通过网线与 Device 设备的 GigabitEthernet1/0/1 接口连接。通过在 Device 设备上进行配置，实现用户通过 Telnet 登录 Device 设备，具体要求采用 scheme 本地认证方式登录，需要输入用户名 abc 和密码 hello12345，建议将本地用户的用户角色配置为 network-admin。

图6 通过 Telnet 登录设备组网图

2.3 配置准备

- 先配置设备 IP 地址并获取 Telnet 服务器的 IP 地址。如果设备与 Telnet 服务器相连的端口不在同一子网内，请保证两台设备间路由可达。
- Windows 系统的命令提示符窗口，可以充当 Telnet 客户端。Win7 以上系统默认未开启 Telnet 客户端功能，手动开启方法如图 7 所示：控制面板—程序和功能—打开或关闭 Windows 功能—勾选 Telnet 客户端即可。

图7 开启 Telnet 客户端功能



2.4 配置步骤

通过 Console 口登录设备，进入系统视图，并开启 Telnet 服务。

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

设置通过 VTY 用户线登录设备使用 AAA 的认证方式。

```
[Sysname] line vty 0 63
[Sysname-line-vty0-63] authentication-mode scheme
[Sysname-line-vty0-63] quit
```

创建本地用户 abc，配置密码为 hello12345，授权其用户角色为 network-admin。

```
[Sysname] local-user abc
[Sysname-luser-manage-abc] password simple hello12345
[Sysname-luser-manage-abc] service-type telnet
[Sysname-luser-manage-abc] authorization-attribute user-role network-admin
[Sysname-luser-manage-abc] quit
```

2.5 验证配置

按下 Win+R 组合键，打开“运行”对话框，输入“cmd”即可打开命令提示符界面，输入命令 Telnet 设备管理 IP，回车即可打开登录界面，。

```
C:\Users\Administrator> telnet 192.168.3.1
```

先输入账号回车，再输入密码回车（注意：密码无回显），即可进入系统命令行。

```
Login: abc
Password:
******************************************************************************
* Copyright (c) 2004-2019 New H3C Technologies Co., Ltd. All rights reserved.*
```

```
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

<Sysname>
```

2.6 配置文件

```
#
 telnet server enable
#
line vty 0 63
 authentication-mode scheme
#
local-user abc
 password hash $h$6$I2Sg4Llj1qVUWQZ3$JA6KkU3zfVVRg48MM92X6cVpdiqR2JF887PKi3GQMwn
XXXcsWBuz7GIeJZeeNFMmMBaV7DPkKblnb0sGT2axvg==
 service-type telnet
 authorization-attribute user-role network-admin
#
```

2.7 相关资料

- 产品配套“基础配置指导”中的“登录设备”。
- 产品配套“基础命令参考”中的“登录设备”。

3 通过 Console 口本地认证方式登录设备

3.1 简介

本案例介绍如何通过 Console 口本地认证的方式登录设备。

3.2 配置准备

参考 1 通过 Console 口登录设备章节进入设备命令行页面。

3.3 配置步骤

本地认证分为 password 认证和 scheme 认证方式两种。

1. password 认证方式

进入系统视图。

```
<Sysname> system-view
```

配置 AUX 用户线（管理 Console 口）认证模式为 password 模式（密码认证）

```
[Sysname] line aux 0
[Sysname-line-aux0] authentication-mode password
```

设置密码为 simple 明文方式，值为 hello12345。

```
[Sysname-line-aux0] set authentication password simple hello12345
```

配置用户角色为 network-admin，可操作系统所有功能和资源。

```
[Sysname-line-aux0] user-role network-admin
```

退回系统视图。

```
[Sysname-line-aux0] quit
```

保存配置，防止配置丢失。

```
[Sysname] save
```

2. scheme 认证方式

进入系统视图。

```
<Sysname> system-view
```

配置 AUX 用户线（管理 Console 口）认证模式为 scheme 模式（用户名密码认证）。

```
[Sysname] line aux 0
[Sysname-line-aux0] authentication-mode scheme
```

退回系统视图。

```
[Sysname-line-aux0] quit
```

创建本地用户 Client，设置密码为 simple 明文方式，值为 hello12345，用户角色为 network-admin，可操作系统所有功能和资源。

```
[Sysname] local-user Client
[Sysname-luser-manage-Client] password simple hello12345
[Sysname-luser-manage-Client] authorization-attribute user-role network-admin
```

配置服务类型为 terminal，即 Console 口登陆类型。

```
[Sysname-luser-manage-Client] service-type terminal
```

退回系统视图。

```
[Sysname-luser-manage-Client] quit
```

保存配置，防止配置丢失。

```
[Sysname] save
```

3.4 验证配置

配置完成后再次通过 Console 口登录设备时：

- password 认证方式出现如下提示，在 password 处输入配置的密码 hello12345 后即可进入系统命令行（输入的密码不会打印显示）。

```
Line aux0 is available.

Press ENTER to get started.
Password:
******************************************************************************
* Copyright (c) 2004-2021 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

<Sysname>
```

- scheme 认证方式出现如下提示，在 Login 处输入配置的用户 Client，在 password 处输入配置的密码 hello12345 后即可进入系统命令行（输入的密码不会打印显示）。

```
Line aux0 is available.

Press ENTER to get started.
Login: Client
Password:
******************************************************************************
* Copyright (c) 2004-2021 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

<Sysname>
```

3.5 配置文件

- password 认证方式

```
#
line aux 0
 authentication-mode password
 user-role network-admin
 set authentication password hash $h$6$fHkW5VqkiATx1+QX$1c5xycW0hx3f9TJi2vMzCwUS
tFKCPNvM+M8KyCWPc1f1Q4nhm1SUDGp59LGlSHn+tsjjxpxEfA+00Y6yr00Ojg==
```

```
#
```

- scheme 认证方式

```
#
line aux 0
 authentication-mode scheme
#
local-user Client class manage
 password hash $h$6$nz1haYkZ7nMNDuD8$61zQWor52DYHpv2KFyCdVHX/d4W9VNRPfyEEU2zyuoB
oOZ5lIS8bLYqUFSjVlBncRIA25FIiz4Js13akTZ3SXw==
 service-type terminal
 authorization-attribute user-role network-admin
#
```

3.6 相关资料

- 产品配套“基础配置指导”中的“登录设备”。
- 产品配套“基础配置命令参考”中的“登录设备”。

4 通过云简网络远程登录设备

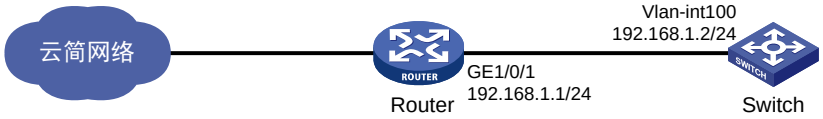
4.1 简介

本案例介绍通过云简网络远程登录设备的配置方法。

4.2 组网需求

如图 8 所示，交换机 Switch 安装在公司内部网络。现要求将 Switch 接入云简网络，使管理员可以通过云简网络远程登录该设备。

图8 通过云简网络远程登录设备配置组网图



4.3 配置注意事项

本特性的支持情况与设备型号有关，具体支持情况可以在微信公众号“新华三云简网络 > 服务 > 版本说明”中的“云简网络版本说明.pdf”查看。

执行本配置前，请先将 Switch 配置为 Telnet 服务器，以便用户能够通过 Telnet 登录到设备进行远程管理和监控。关于如何配置通过 Telnet 登录设备的详细介绍，请参见产品配套“基础配置指导”中的“登录设备”。

4.4 配置步骤

1. 配置 Switch

创建 VLAN，在 VLAN 中加入对应的端口，并配置各 VLAN 接口的 IP 地址。

```
<Switch> system-view
[Switch] vlan 100
[Switch-vlan100] port gigabitethernet 1/0/1
[Switch-vlan100] quit
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip address 192.168.1.2 24
[Switch-Vlan-interface100] quit
```

配置静态路由。

```
[Switch] ip route-static 0.0.0.0 0 192.168.1.1
```

配置域名服务器的 IPv4 地址。

```
[Switch] dns server 114.114.114.114
```

配置云简网络域名。

```
[Switch] cloud-management server domain oasis.h3c.com
```

保存配置。

```
[SwitchA] save force
```

2. 配置 Router

配置接口的 IP 地址。

```
<Router> system-view
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] ip address 192.168.1.1 24
[Router-GigabitEthernet1/0/1] quit
```

保存配置。

```
[Router] save force
```

3. 云简网络配置

在云简网络（https://oasis.h3c.com），在云简平台上需要添加手动设备，具体操作步骤请查看官网路径“首页 > 支持 > 文档与软件 > 文档中心 > 云简网络 > 云简网络 > H3C 云简网络”。

也可以直接点击链接查看手册：

https://www.h3c.com/cn/Service/Document_Software/Document_Center/Oasis/Catalog/Oasis_Platform/Oasis_Platform/

图9 将 Switch 添加到云简网络

4.5 验证配置

查看 Switch 与云简网络的连接状态，当 Cloud connection state 为 Established 状态时，表示连接已建立。

```
[Switch] display cloud-management state
Cloud connection state   : Established
Device state             : Request_success
Cloud server address     : 101.36.161.141
Cloud server domain name : oasis.h3c.com
Cloud server port        : 443
```

```
Connected at              : Tue Apr  20 15:43:17 2021
Duration                  : 00d 00h 02m 32s
Process state             : Message received
Failure reason            : N/A
```

在云简网络通过 Telnet 管理设备。

在云简网络管理页面顶部导航栏中选择“网络管理”，左侧导航栏中选择“维护 > 命令助手”，打开 telnet 模式，即可通过云简网络远程登录设备命令行界面。

图10 在云简网络通过 Telnet 管理设备

4.6 配置文件

- Switch：

```
#
 dns server 114.114.114.114
#
vlan 100
#
interface Vlan-interface100
 ip address 192.168.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
 ip route-static 0.0.0.0 0 192.168.1.1
#
 cloud-management server domain oasis.h3c.com
#
```

- Router：

```
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 192.168.1.1 255.255.255.0
#
```

4.7 相关资料

- 产品配套“网络管理和监控配置指导”中的“云平台连接”。
- 产品配套“网络管理和监控命令参考”中的“云平台连接”。

5 忘记 Console 口密码处理方法

5.1 简介

本案例介绍忘记 Console 口密码的处理方法。

方法一适用于仅忘记 Console 口密码，仍可通过 Telnet/SSH 方式登录设备时。

方法二与方法三适用于忘记所有密码，无法登录设备且需要保留设备配置文件时。

方法四适用于忘记所有密码，无法登录设备且无需保留设备配置文件时。

5.2 组网需求

无

5.3 配置步骤

说明

建议优先使用方法一恢复 console 口密码，如果忘记所有登录设备的密码，再使用其他方法。

1. 方法一：通过 Telnet/SSH 登录设备后修改 Console 口密码

通过 Telnet/SSH 方式登录设备后，参考 3.3 1. password 认证方式 3.3 2. scheme 认证方式重新配置 Console 口密码。

2. 方法二：通过 bootware 菜单选择跳过配置文件启动后手工修改 console 口密码

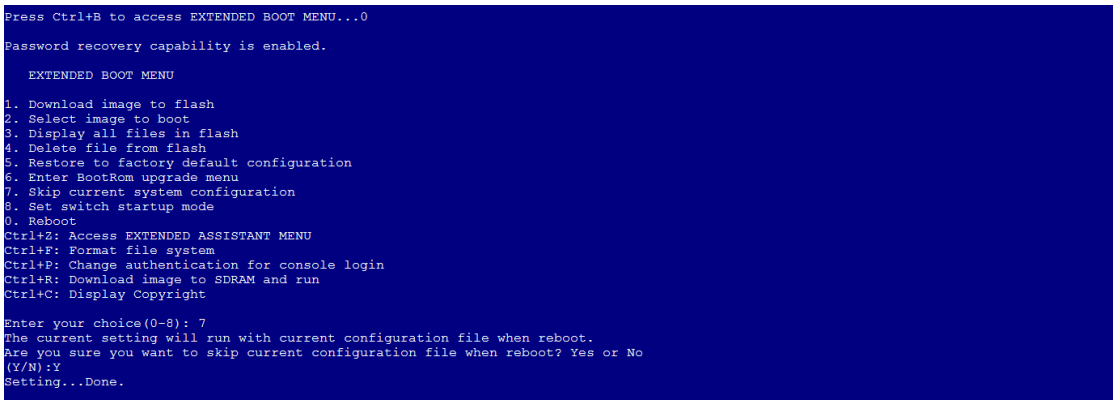
说明

不同产品的 bootware 页面可能有所不同，此处以 S5130 系列以太网交换机为例。

(1) 通过 console 口连接设备后将设备重新启动。

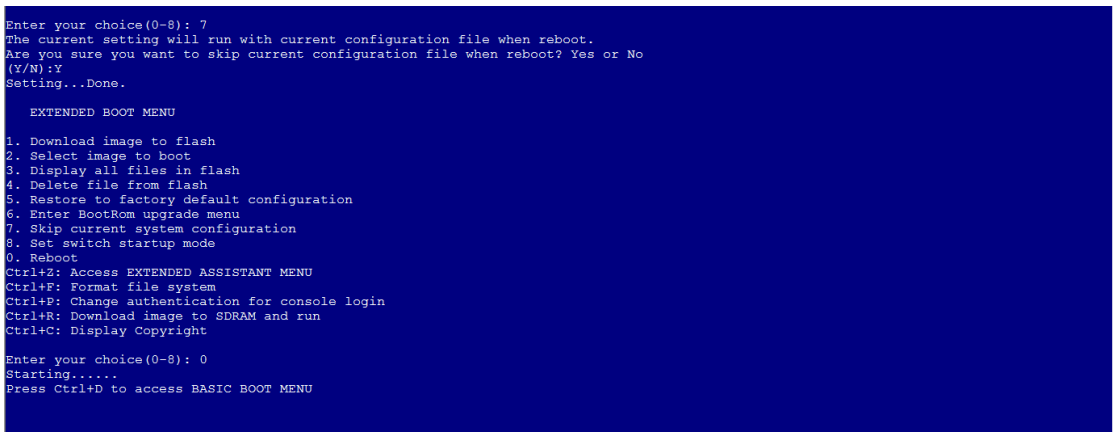
(2) 设备重启时按下 Ctrl+B 进入 bootware 菜单，选择跳过当前配置启动，如图 11 所示。

图11 进入 bootware 菜单并跳过当前配置启动



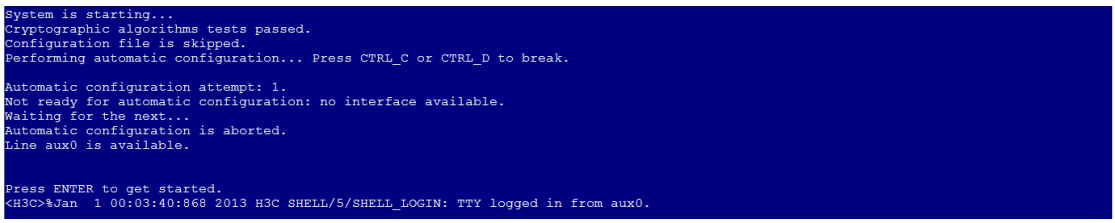
(3) 选择 Reboot 重启设备，如图 12 所示。

图12 重启设备



(4) 设备重启时按下 Ctrl+C 或 Ctrl+D 跳过自动配置，如图 13 所示。

图13 跳过自动配置



(5) 按下 Enter 键成功跳过配置文件启动，进入命令行页面。

(6) 查看配置文件内容。

```
<Sysname> more startup.cfg
```

(7) 将显示配置文件全部选中后复制粘贴到本地 txt 文件中，如图 14 与图 15 所示。

图14 导出配置文件（一）

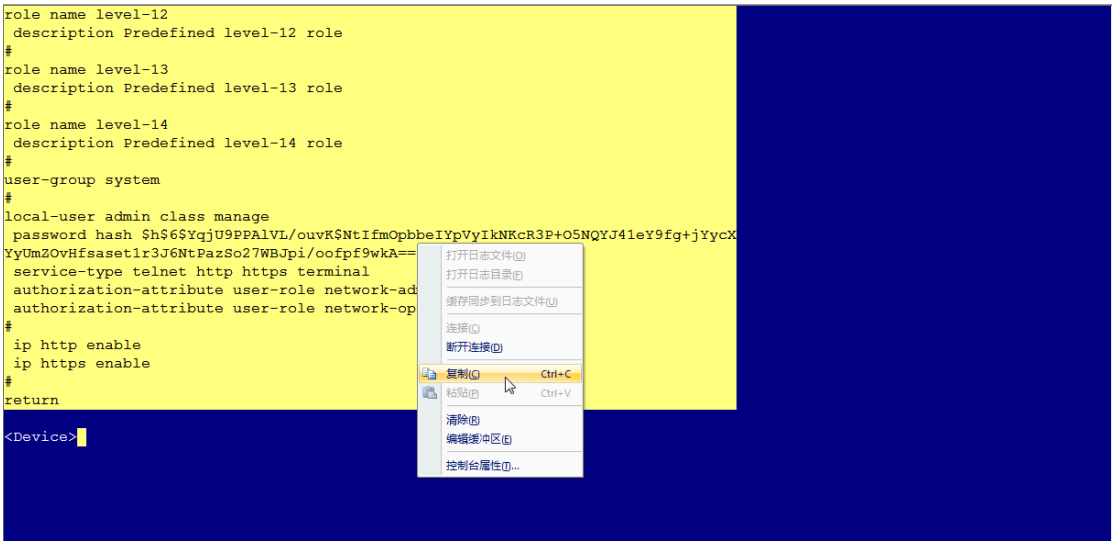
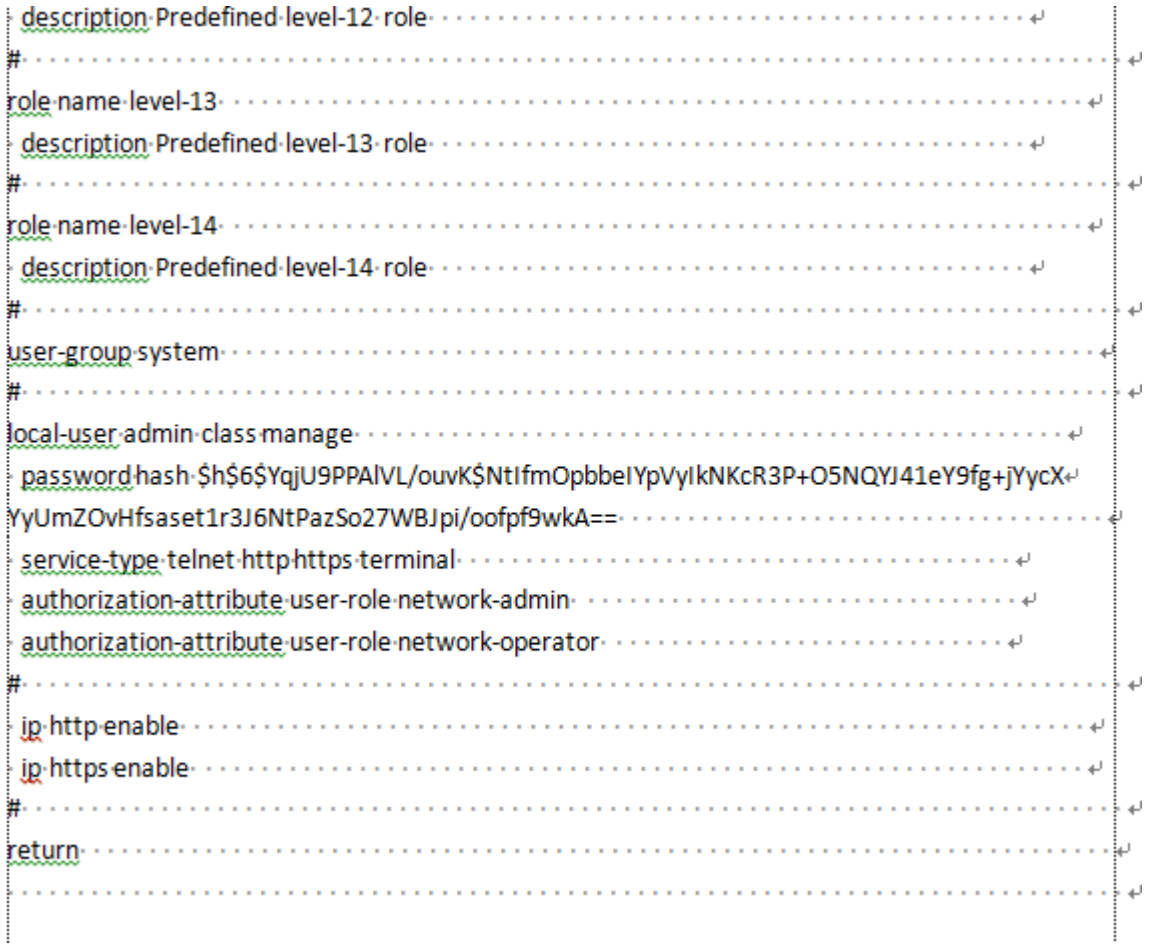


图15 导出配置文件（二）

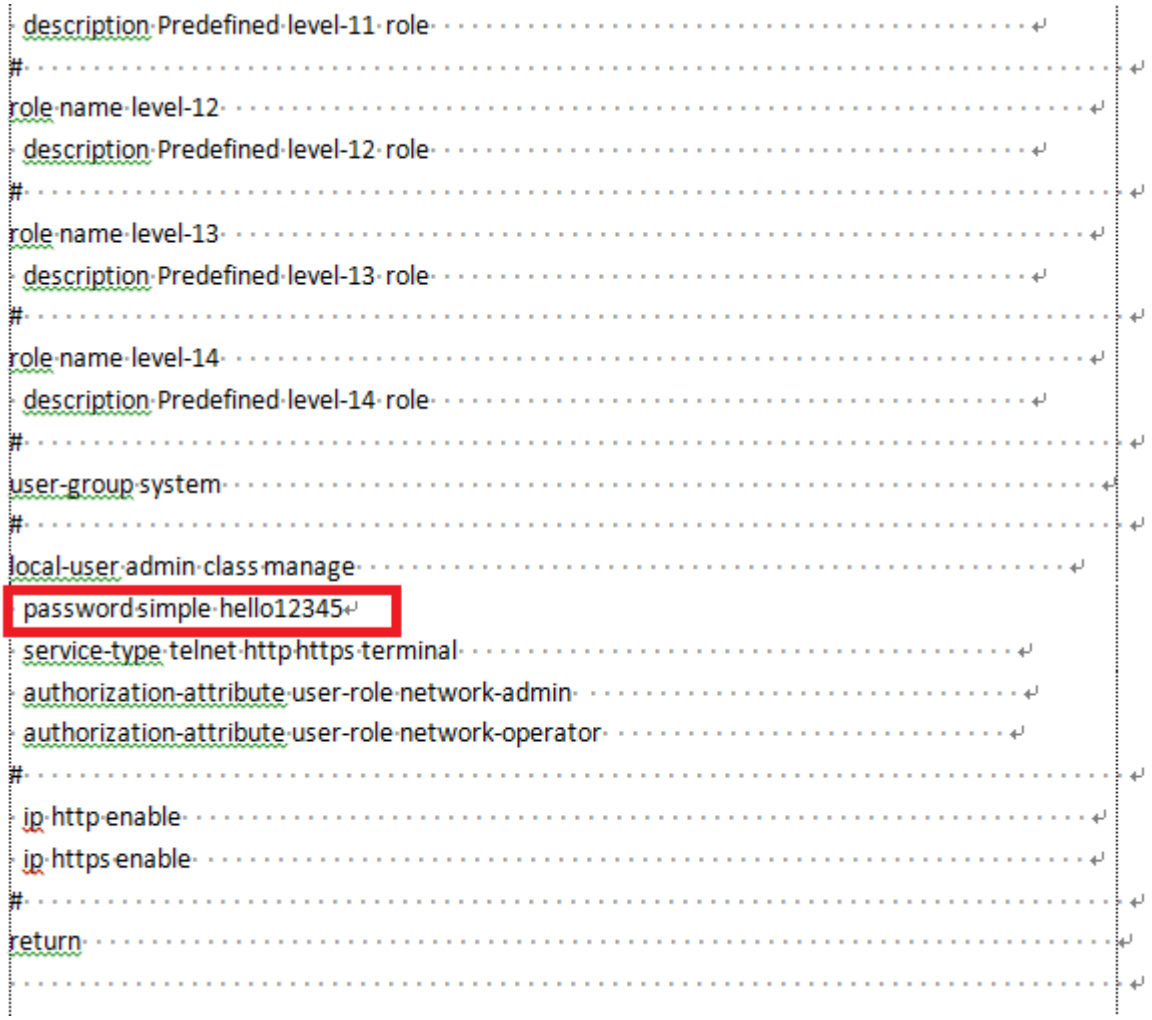


(8) 修改配置文件，删除密码或配置新密码。本文以配置新密码 hello12345 为例，如图 16 所示。

注意

password 认证方式密码配置在 AUX 口配置下，scheme 方式密码配置在 local-user 配置下，本文以修改 scheme 方式密码为例。

图16 配置新密码

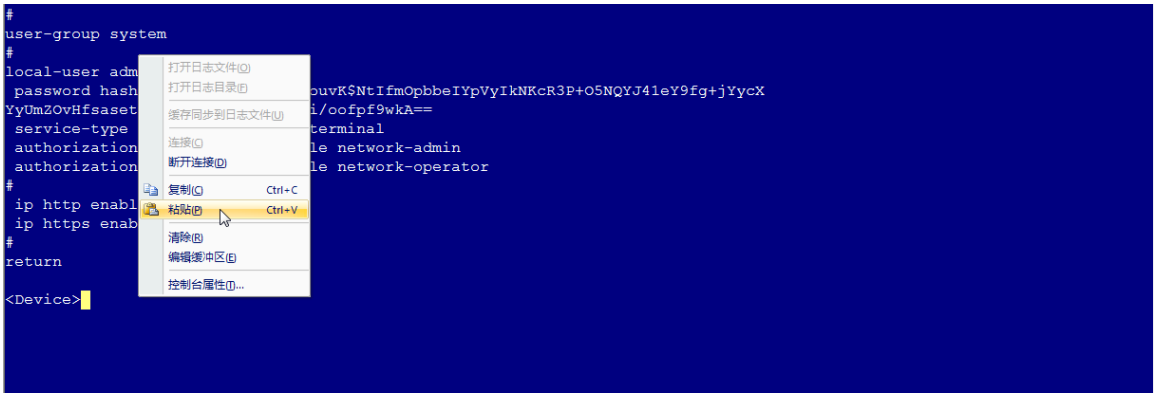


(9) 回到设备命令行页面，进入系统视图。

```
<Sysname> system-view
```

(10) 将修改后的配置文件复制粘贴到设备，如图 17 所示。

图17 导入配置文件



(11) 保存配置。

```
[Sysname] save
```

(12) 回到用户视图重启设备。

```
[Sysname] quit
<Sysname> reboot
```

3. 方法三：通过 bootware 菜单选择跳过配置文件启动后配置回滚

(1) 通过方法二跳过配置文件启动后不查看配置文件，直接进入系统视图。

```
<Sysname> system-view
```

(2) 将当前配置回滚至默认配置文件 startup.cfg 中的配置状态并输入 N 不保存当前空配置。

```
[Sysname] configuration replace file startup.cfg
Current configuration will be lost, save current configuration? [Y/N]:N
Now replacing the current configuration. Please wait...
Succeeded in replacing current configuration with the file startup.cfg.
```

(3) 参见 3.3 1. password 认证方式或 3.3 2. scheme 认证方式重新配置 Console 口密码。

4. 方法四：通过 bootware 菜单选择跳过配置文件启动后保留当前空配置

注意

此方法会清空设备所有配置，请确保当前业务不会受到影响时再进行。

(1) 通过方法二跳过配置文件启动后直接进入系统视图，并保存当前空配置。

```
<Sysname> system-view
[Sysname] save
```

(2) 参见 3.3 1. password 认证方式或 3.3 2. scheme 认证方式重新配置 Console 口密码。

5.4 配置文件

无

5.5 相关资料

- 产品配套“基础配置指导”中的“登录设备”。
- 产品配套“基础配置指导”中的“配置文件管理”。
- 产品配套“基础配置命令参考”中的“登录设备”。
- 产品配套“基础配置命令参考”中的“配置文件管理”。

6 忘记 Telnet/Web 登录密码处理方法

6.1 简介

本案例介绍忘记 Telnet/Web 登录密码处理方法。

6.2 组网需求

无

6.3 配置步骤

1. 忘记 Telnet 登录密码处理方法

通过 Console 口登录设备后，请参见 2 通过 Telnet 登录设备重新配置 Telnet 登录密码。

2. 忘记 Web 登录密码处理方法

通过 Console 口登录设备后，重新配置 Web 登录密码。

#进入系统视图。

```
<Sysname> system-view
```

进入所需 Web 用户视图（此处以 client 为例），配置认证密码为 hello12345。

```
[Sysname] local-user client
[Sysname-luser-manage-client] password simple hello12345
[Sysname-luser-manage-client] quit
```

#保存配置，防止配置丢失。

```
[Sysname] save
```

6.4 配置文件

- Telnet 方式

请参见 2 通过 Telnet 登录设备

- Web 方式

```
#
ip http enable
#
ip https enable
#
local-user client
 password hash $h$6$I2Sg4Llj1qVUWQZ3$JA6KkU3zfVVRg48MM92X6cVpdiqR2JF887PKi3GQMwn
XXXcsWBuz7GIeJZeeNFMmMBaV7DPkKblnb0sGT2axvg==
 service-type http https
 authorization-attribute user-role network-admin
#
```

6.5 相关资料

- 产品配套“基础配置指导”中的“登录设备”。
- 产品配套“基础配置命令参考”中的“登录设备”。

配置文件管理快速配置指南

目 录

1 恢复出厂配置

1.1 简介

本案例介绍使设备恢复到出厂状态的常用方法。

1.2 配置注意事项

不同设备支持恢复到出厂状态方法可能不同，具体以设备的实际情况为准。

恢复出厂配置后，设备会清除所有用户的配置信息。因此，用户需要登录设备的 Console 口进行操作，不能通过 SSH 或 Telnet 方式远程登录设备。关于 Console 登录设备的方法，请参见“通过 Console 登录设备快速配置指南”。

1.3 配置步骤

- 执行 **restore factory-default** 命令行并重启设备

  # 将设备恢复到出厂状态。

  ```
  <Sysname> restore factory-default
  This command will restore the system to the factory default configuration and clear the
  operation data. Continue [Y/N]:y
  Restoring the factory default configuration. This process might take a few minutes.
  Please
  wait.....................................................................................
  ..........................Done.
  Please reboot the system to place the factory default configuration into effect.
  ```

  # 重启设备，请不要选择保存当前配置。重启完成之后，设备将恢复到出厂状态。

  ```
  <Sysname> reboot
  Start to check configuration with next startup configuration file, please
  wait.........DONE!
  Current configuration will be lost after the reboot, save current configuration? [Y/N]:n
  This command will reboot the device. Continue? [Y/N]:y
  Now rebooting, please wait...
  ```

- 删除配置文件并重启设备

  # 显示用于本次及下次启动的配置文件的名称。

  ```
  <Sysname> display startup
  MainBoard:
   Current startup saved-configuration file: flash:/startup.cfg
   Next main startup saved-configuration file: flash:/startup.cfg
   Next backup startup saved-configuration file: NULL
  ```

  # 查看设备当前已存在的配置文件。

  ```
  <Sysname> dir
  Directory of flash:
     0 -rw-        6244 Jan 08 2013 07:26:03   startup.cfg
     1 -rw-      136628 Jan 08 2013 07:26:03   startup.mdb
     2 -rw-       58704 Jan 03 2013 07:56:22   diag_H3C_20130103-005605.tar.gz
  ```

```
...
```

删除下次启动的配置文件。

```
<Sysname> delete /unreserved startup.cfg
The file cannot be restored. Delete flash:/startup.cfg?[Y/N]:y
Deleting a file permanently will take a long time. Please wait...
%Delete file flash:/startup.cfg...Done.
```

重启设备。重启完成之后，设备将恢复到出厂状态。

```
<Sysname> reboot
Start to check configuration with next startup configuration file, please
wait.........DONE!
Current configuration will be lost after the reboot, save current configuration? [Y/N]:n
This command will reboot the device. Continue? [Y/N]:y
Now rebooting, please wait...
```

- 清除保存的配置并重启设备

说明

- 缺省情况下，本特性会将下次启动配置文件从所有的成员设备上彻底删除，请谨慎使用。如果只需从主设备上删除下次启动配置文件，请关闭配置文件同步功能。
- 重启设备时，请勿保存当前配置文件。

显示用于本次及下次启动的配置文件的名称。

```
<Sysname> display startup
MainBoard:
 Current startup saved-configuration file: flash:/startup.cfg
 Next main startup saved-configuration file: flash:/startup.cfg
 Next backup startup saved-configuration file: NULL
```

删除下次启动的主用配置文件。

```
<Sysname> reset saved-configuration
The saved configuration file will be erased. Are you sure? [Y/N]:Y
```

如果设备上存在备用配置文件，则需再执行 **reset saved-configuration backup** 命令，本例中不需要执行此命令。

重启设备。重启完成之后，设备将恢复到出厂状态。

```
<Sysname> reboot
Start to check configuration with next startup configuration file, please
wait.........DONE!
Current configuration will be lost after the reboot, save current configuration? [Y/N]:n
This command will reboot the device. Continue? [Y/N]:y
Now rebooting, please wait...
```

1.4 相关资料

- 产品配套“基础配置指导”中的“配置文件管理”。
- 产品配套“基础配置命令参考”中的“配置文件管理”。
- 产品配套“基础配置指导”中的“设备管理”。

- 产品配套“基础配置命令参考”中的“设备管理”。
- 产品配套“基础配置指导”中的“文件系统管理”。
- 产品配套“基础配置命令参考”中的“文件系统管理”。

2 备份配置文件

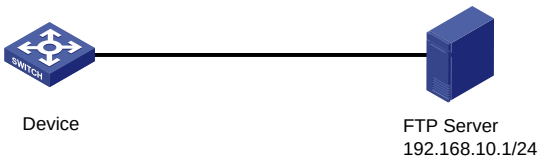
2.1 简介

本案例介绍备份配置文件方法。

2.2 组网需求

如图 1 示，备份 Device 的当前配置文件，并保存到 FTP Server 上。

图1 备份配置文件组网图



2.3 配置准备

请确保 Device 设备与 FTP Server 间路由可达。

2.4 配置步骤

保存设备配置，配置文件名采用缺省名字 startup.cfg。

```
<Sysname> save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
Validating file. Please wait...
Saved the current configuration to mainboard device successfully.
```

以上表明设备默认保存了一个名为 starup.cfg 的配置文件。

将 startup.cfg 文件上传到 FTP 服务器上。

```
<Sysname> ftp 192.168.10.1
Press CTRL+C to abort.
Connected to 192.168.10.1 (192.168.10.1).
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
User (192.168.10.1:(none)): root
331 Give me your password, please
Password:
230 Logged in successfully
Remote system type is MSDOS.
ftp> binary
200 Type is Image (Binary)
ftp> put start.cfg
ftp: No such file or directory
ftp> put startup.cfg
```

```
227 Entering Passive Mode (192,168,10,1,235,54)
150 "D:\temp\startup.cfg" file ready to receive in IMAGE / Binary mode
.
226 Transfer finished successfully.
4326 bytes sent in 0.003 seconds (1.49 Mbytes/s)
```

2.5 验证配置

查看上传的配置文件。

```
ftp> dir
227 Entering Passive Mode (192,168,10,1,252,152)
1 File Listing Follows in ASCII mode
-rwxrwxrwx   1 noone    nogroup     4326 Sep  2 14:00 startup.cfg
```

以上表明 startup.cfg 文件已上传到 FTP 服务器上。

2.6 相关资料

- 产品配套“基础配置指导”中的“配置文件管理”。
- 产品配套“基础配置命令参考”中的“配置文件管理”。
- 产品配套“基础配置指导”中的“FTP 和 TFTP”。
- 产品配套“基础配置命令参考”中的“FTP 和 TFTP”。

3 跳过自动配置

3.1 简介

自动配置功能是指设备在启动时自动获取并执行配置文件。网络管理员只需将配置文件保存在指定的存储介质上，启动设备，即可实现自动配置，从而简化了网络配置，大大降低了网络管理员的工作量，便于实现对设备的集中管理。应用场景是网络规模较大，设备位置较分散。

设备空配置启动时，首先自动检查存储介质的根目录下是否存在 autocfg.py、autocfg.tcl 或 autocfg.cfg 配置文件。如果存在，则直接执行此文件；如果不存在，则通过自动从文件服务器上获取并执行配置脚本文件或配置文件，实现自动配置功能。autocfg.py、autocfg.tcl 和 autocfg.cfg 配置文件同时只能在设备上存在一个。

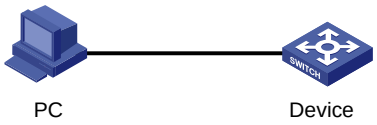
但是有的时候设备并不会应用在网络规模较大的场景中，所以就需要跳过自动配置。

本案例介绍跳过自动配置方法。

3.2 组网需求

如图 2 所示，设备空配置启动，跳过自动配置。

图2 跳过自动配置组网图



3.3 配置准备

设备空配置启动，需使用 Console 口登录设备。关于 Console 登录设备的方法，请参见“通过 Console 登录设备快速配置指南”。

3.4 配置步骤

设备开机启动。

```
Starting......
Press Ctrl+D to access BASIC BOOT MENU
Press Ctrl+T to start heavy memory test

********************************************************************************
*                                                                              *
*                 H3C S5570S-28S-HPWR-EI  BOOTROM, Version 105                 *
*                                                                              *
********************************************************************************
Copyright (c) 2004-2021 New H3C Technologies Co., Ltd.

Creation Date         : Jul  6 2021
CPU Clock Speed       : 1000MHz
```

```
Memory Type           : DDR4 SDRAM
Memory Size           : 1024MB
Memory Speed          : 800MHz
CPLD Version          : 001
PCB Version           : Ver.A
Mac Address           : b04414cd47a4


BootRom Validating...
Press Ctrl+B to access EXTENDED BOOT MENU...0
Loading the main image files...
Loading file flash:/s5570s_ei-cmw710-system-e1105p09.bin.....................
.....................................................Done.
Loading file flash:/s5570s_ei-cmw710-devkit-e1105p09.bin.....Done.
Loading file flash:/s5570s_ei-cmw710-boot-e1105p09.bin.........Done.

Image file flash:/s5570s_ei-cmw710-boot-e1105p09.bin is self-decompressing......
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
.............Done.
System is starting...
Cryptographic algorithms tests passed.

Startup configuration file doesn't exist or is invalid.
Performing automatic configuration... Press CTRL_C or CTRL_D to break.

Automatic configuration attempt: 1.
Not ready for automatic configuration: no interface available.
Waiting for the next...

Automatic configuration attempt: 2.
Not ready for automatic configuration: no interface available.
Waiting for the next...
```

可以通过按“CTRL+D”或者“Ctrl+C”中断自动配置，进入 Comware 系统。

3.5 相关资料

- 产品配套“基础配置指导”中的“自动配置”。
- 产品配套“基础配置命令参考”中的“自动配置”。

软件升级快速配置指南

目 录

1 使用命令行方式升级设备软件版本

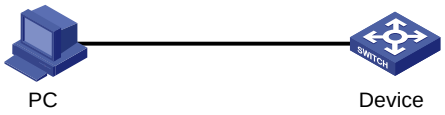
1.1 简介

本案例介绍用命令行方式升级设备软件版本的方法。

1.2 组网需求

如图 1 所示，主机和设备之间仅使用配置电缆连接。现要求：PC 作为文件服务器，并启动 TFTP 服务器功能，Device 作为 TFTP 客户端，通过 TFTP 方式将软件升级包下载到 Device，并升级软件版本。

图1 使用命令行方式升级设备软件版本组网图



1.3 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。

1.4 配置准备

1.4.1 获取升级软件包

获取升级软件包有如下方式：

- 登录 H3C 官网 http://www.h3c.com，获取待升级的启动软件包。
- 联系 H3C 技术支持人员获取待升级的启动软件包。

1.4.2 文件服务器的配置

说明

设备支持通过 FTP、TFTP、SFTP 等方式备份设备的重要文件和上传最新的软件版本，本文仅以 TFTP 协议为例进行介绍。其它文件传输方式请参见产品配置指导。

启动文件服务器上的 TFTP 服务器功能（以 3CDaemon 软件为例），设置 TFTP 服务器上传/下载路径等参数，并开启服务。

图2 配置 TFTP 服务器上传/下载路径

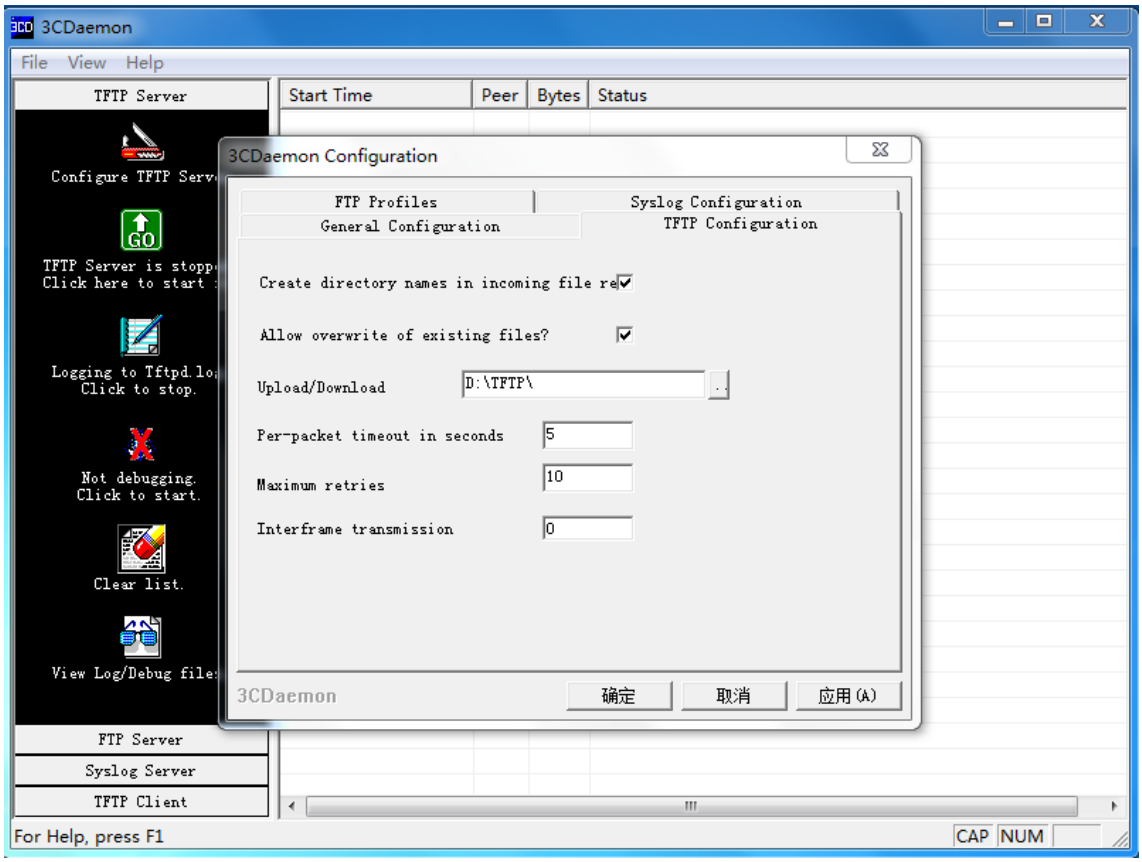
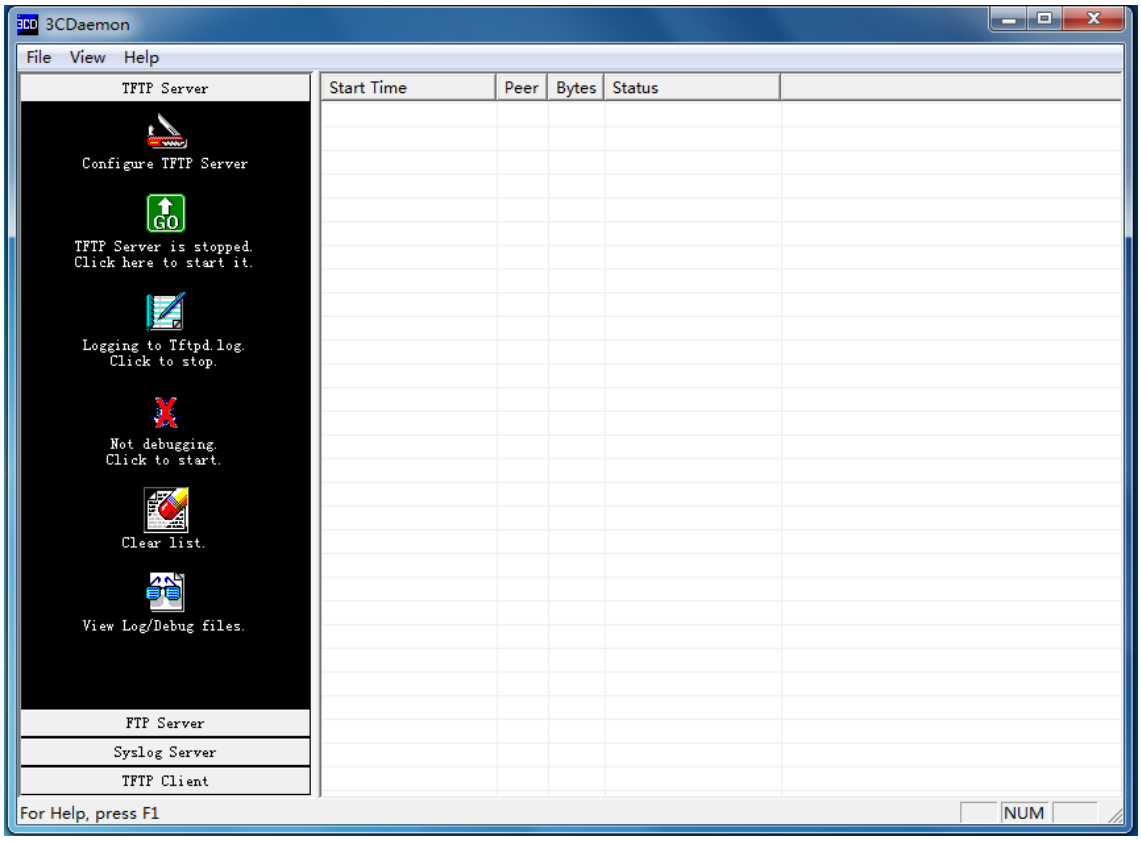
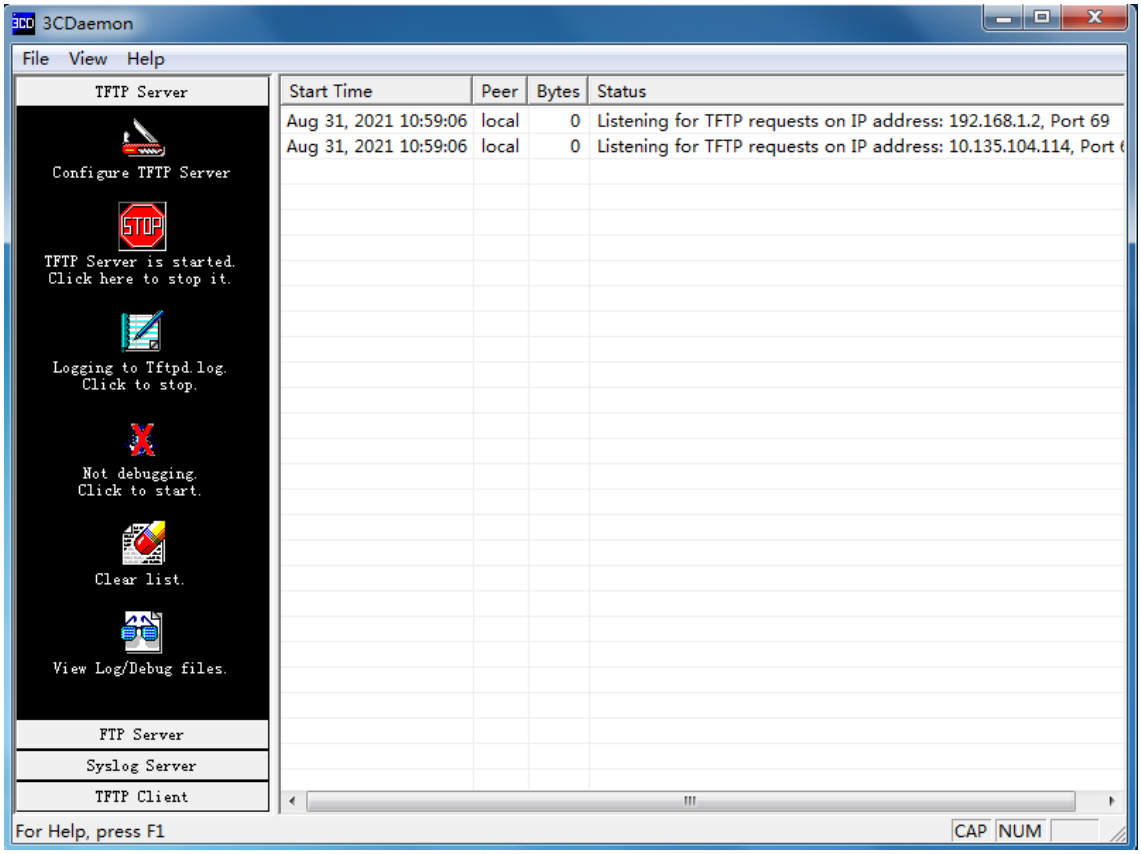


图3 开启 TFTP 服务


3CDaemon
File View Help
TFTP Server
Configure TFTP Server
TFTP Server is stopped.
Click here to start it.
Logging to Tftpd.log.
Click to stop.
Not debugging.
Click to start.
Clear list.
View Log/Debug files.
FTP Server
Syslog Server
TFTP Client
Start Time
Peer
Bytes
Status
For Help, press F1
NUM



1.5 配置步骤

1.5.1 配置设备接口 IP 地址

创建管理 VLAN 99。

```
<Switch> system-view
[Switch] vlan 99
[Switch-vlan99] quit
```

创建管理 VLAN 的接口。

```
[Switch] interface vlan-interface 99
```

配置 Vlan-interface99 接口 IP 地址为 192.168.1.1/24。

```
[Switch-Vlan-interface99] ip address 192.168.1.1 24
[Switch-Vlan-interface99] quit
```

进入设备与主机相连的以太网接口视图（请以设备实际情况为准，此处仅作示例）

```
[Switch] interface gigabitethernet 1/0/1
```

配置接口工作在二层模式。

```
[Switch-GigabitEthernet1/0/1] port link-mode bridge
```

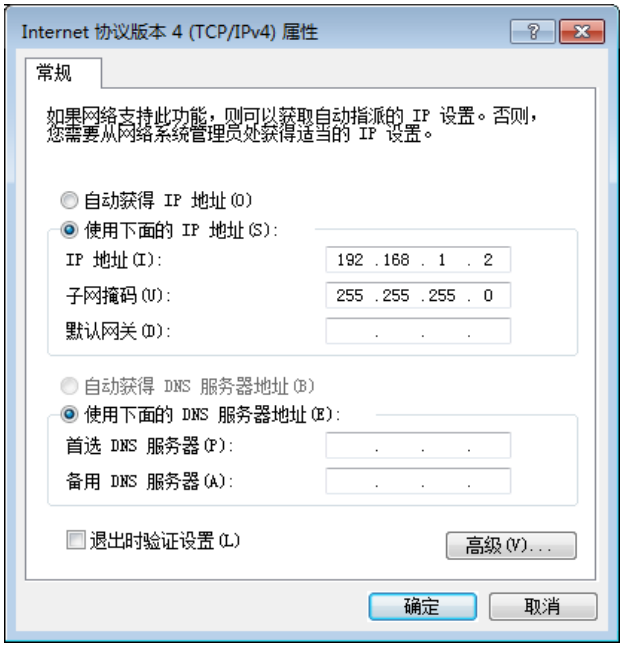
将该接口加入 VLAN 99。

```
[Switch-GigabitEthernet1/0/1] port access vlan99
[Switch-GigabitEthernet1/0/1] quit
```

1.5.2 配置主机 IP 地址

配置本地主机 IP 地址为：192.168.1.2/24。

图4 配置主机 IP 地址



使用“Win+R”快捷键打开运行窗口，输入 cmd 打开命令行终端，测试网络的连通性，确保主机与设备之间路由可达。

```
C:\ Documents and Setting\Administrato> ping 192.168.1.1

正在 Ping 192.168.1.1 具有 32 字节的数据:
来自 192.168.1.1 的回复: 字节=32 时间=31ms TTL=253
来自 192.168.1.1 的回复: 字节=32 时间=30ms TTL=253
来自 192.168.1.1 的回复: 字节=32 时间=30ms TTL=253
来自 192.168.1.1 的回复: 字节=32 时间=30ms TTL=253

192.168.1.1 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 = 30ms，最长 = 31ms，平均 = 30ms
```

在设备上 ping TFTP 服务器地址（即主机 IP 地址），能够 ping 通。

```
<Switch> ping 192.168.1.2
Ping 192.168.1.2 (192.168.1.2): 56 data bytes, press CTRL_C to break
56 bytes from 192.168.1.2: icmp_seq=0 ttl=64 time=10.701 ms
56 bytes from 192.168.1.2 icmp_seq=1 ttl=64 time=2.678 ms
56 bytes from 192.168.1.2: icmp_seq=2 ttl=64 time=2.282 ms
56 bytes from 192.168.1.2: icmp_seq=3 ttl=64 time=1.617 ms
56 bytes from 192.168.1.2: icmp_seq=4 ttl=64 time=1.701 ms

--- Ping statistics for 192.168.1.2 ---
```

```
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.617/3.796/10.701/3.474 ms
```

执行 **save** 命令保存设备当前配置信息。

```
<Switch> save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait...
Saved the current configuration to mainboard device successfully.
```

1.5.3 查看当前版本

通过 **display version** 命令查看设备当前版本号（对比升级前后的设备软件版本可以验证升级是否成功）。

```
<Switch> display version
H3C Comware Software, Version 7.1.070, Release xxxx
Copyright (c) 2004-2021 New H3C Technologies Co., Ltd. All rights reserved.
H3C Switch uptime is 0 weeks, 0 days, 0 hours, 19 minutes
Last reboot reason : User reboot
...
```

1.5.4 查看剩余空间

通过 **dir** 命令查看设备剩余存储空间，确保足够的空间（一般为软件包大小的两倍以上）保存新的待升级软件包。

```
<Switch> dir
Directory of flash:
   0 drw-      707584 Jan 29 2013 05:41:21   123.bin
   1 drw-       12639 Jan 29 2013 05:41:21   patch.bin
   2 drw-    48866304 Jan 02 2013 08:30:11   r6126p20.ipe
   3 -rw-         591 Jan 01 2013 03:31:14   serverkey
   4 -rw-        6304 Feb 02 2013 06:58:55   startup.cfg
   5 -rw-      159335 Feb 02 2013 06:58:55   startup.mdb
   6 -rw-           0 Jan 02 2013 06:19:27   topology.dba
   7 drw-           - Jan 02 2013 05:32:24   versionInfo
...

251904 KB total (25052 KB free)
```

当空间不足时，需要使用 **delete /unreserved** file 命令来彻底删除多余的文件。

```
<Switch> delete /unreserved patch.bin
The file cannot be restored. Delete flash:/patch.bin? [Y/N]:y
Deleting the file permanently will take a long time. Please wait...
Deleting file flash:/123.bin...Done.
```

说明

- .ipe 格式的启动软件包在升级过程中会先解压缩为多个.bin 文件，请确保预留足够的存储空间（一般为软件包大小的两倍以上）放置启动软件包、解压文件。
- 使用 **delete /unreserved** ***file*** 命令删除文件，被删除的文件将被彻底删除，不能再恢复。
- 使用 **delete** ***file*** 命令删除文件，被删除的文件被保存在回收站中，仍会占用存储空间。如果要彻底删除回收站中的某个废弃文件，执行 **reset recycle-bin** 命令，以释放空间。

1.5.5 升级设备

将待升级的软件包 switch.ipe 放入之前设置好的 TFTP 服务器上传/下载路径。

使用 TFTP 方式将文件服务器上的软件版本 switch.ipe 文件下载到设备上。

```
<Switch> tftp 192.168.1.2 get switch.ipe
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 58.7M  100 58.7M    0     0  1193k      0  0:00:50  0:00:50 --:--:-- 1127k
```

指定设备下次启动时所用的主用启动文件为 switch.ipe。

```
<Switch> boot-loader file flash:/switch.ipe all main
```

启动软件包解压设置完成后会提示是否删除文件，若后期升级后需切换回本软件版本，建议选择“N”。

```
<Switch> Do you want to delete flash:/switch.ipe now? [Y/N]:N
```

重启设备。

```
<Switch> reboot
```

1.6 验证配置

设备重启后，使用 **display version** 命令查看设备版本信息。

```
<Switch> display version
H3C Comware Software, Version 7.1.070, Release xxxx
Copyright (c) 2004-2021 New H3C Technologies Co., Ltd. All rights reserved.
H3C Switch uptime is 0 weeks, 0 days, 0 hours, 19 minutes
Last reboot reason : User reboot
...
```

使用 **display boot-loader** 命令查看本次启动和下次启动所采用的启动软件包的名称。

```
<Switch> display boot-loader
Software images on slot 1:
Current software images:
  flash:/boot.bin
  flash:/system.bin
Main startup software images:
  flash:/boot.bin
  flash:/system.bin
Backup startup software images:
```

None

1.7 配置文件

```
#
interface vlan-interface 99
ip address 192.168.1.1 24
#
interface gigabitethernet 1/0/1
port link-mode bridge
port access vlan 99
#
```

1.8 相关资料

- 产品配套“基础配置指导”中的“软件升级”。
- 产品配套“基础配置命令参考”中的“软件升级”。

2 使用 BootRom 菜单和 XModem 协议升级设备软件版本

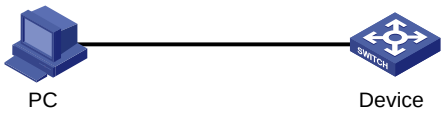
2.1 简介

本案例介绍用 BootRom 菜单和 XModem 协议方式升级设备软件版本的方法。

2.2 组网需求

如图 5 所示，主机和设备之间仅使用配置电缆连接。现要求：通过 XModem 协议方式将文件 switch.ipe 下载到 Device，并升级软件版本。

图5 通过 Console 口登录设备组网图



2.3 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包版本之间的兼容性，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。

使用 XMODE 方式传输文件较慢，一般情况下不推荐此种方式升级，建议使用网线传输文件，详见 1 使用命令行方式升级设备软件版本。

2.4 配置准备

2.4.1 获取升级软件包

获取升级软件包有如下方式：

- 登录 H3C 官网 http://www.h3c.com，获取待升级的启动软件包。
- 联系 H3C 技术支持人员获取待升级的启动软件包。

2.4.2 下载管理软件

请提前下载好管理软件，本例以超级终端为例。

2.5 配置步骤

2.5.1 查看当前版本

通过 **display version** 命令查看设备当前版本号（对比升级前后的设备软件版本可以验证升级是否成功）。

```
<Switch> display version
H3C Comware Software, Version 7.1.070, Release xxxx
```

```
Copyright (c) 2004-2021 New H3C Technologies Co., Ltd. All rights reserved.
H3C Switch uptime is 0 weeks, 0 days, 0 hours, 19 minutes
Last reboot reason : User reboot
...
```

2.5.2 进入 BootRom 菜单

#重启设备后，根据提示按住 Ctrl+B 进入设备的 BootRom 菜单

```
   EXTENDED BOOT MENU

1. Download image to flash
2. Select image to boot
3. Display all files in flash
4. Delete file from flash
5. Restore to factory default configuration
6. Enter BootRom upgrade menu
7. Skip current system configuration
8. Set switch startup mode
0. Reboot
Ctrl+Z: Access EXTENDED ASSISTANT MENU
Ctrl+F: Format file system
Ctrl+P: Change authentication for console login
Ctrl+R: Download image to SDRAM and run
Ctrl+C: Display Copyright
```

#选择 1 下载镜像文件到 flash

```
Enter your choice(0-8): 1
1. Set TFTP protocol parameters
2. Set FTP protocol parameters
3. Set XMODEM protocol parameters
0. Return to boot menu
```

#选择 3 采用 XModem 协议完成启动软件包的加载，进入下载速率设置菜单

```
Enter your choice(0-3): 3
Please select your download baudrate:
1.* 9600
2.  19200
3.  38400
4.  57600
5.  115200
0.  Return to boot menu
```

#根据实际情况，选择合适的下载速率，本例选择 5，修改下载速率为 115200bit/s

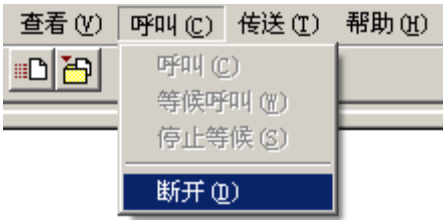
```
Enter your choice(0-5): 5
Download baudrate is 115200 bps
Please change the terminal's baudrate to 115200 bps and select XMODEM protocol
Press enter key when ready
```

2.5.3 修改终端设置的波特率

由于交换机 Console 口的波特率已经修改为 115200bps，而终端的波特率还为 9600bps，双方是无法通信的。因此，根据系统的提示，需要改变终端设置的波特率，使其与交换机选择的下载波特率一致。

(1) 单击超级终端的[呼叫/断开]菜单项，即断开了超级终端和交换机的连接。

图6 [呼叫/断开]菜单项



(2) 进入超级终端软件的[文件/属性]菜单，在弹出的对话框单击[配置]按钮（如图 7），进入 Console 口配置对话框，将“每秒位数”配置 115200 后，单击[确定]按钮(如图 8)。

图7 进入属性对话框

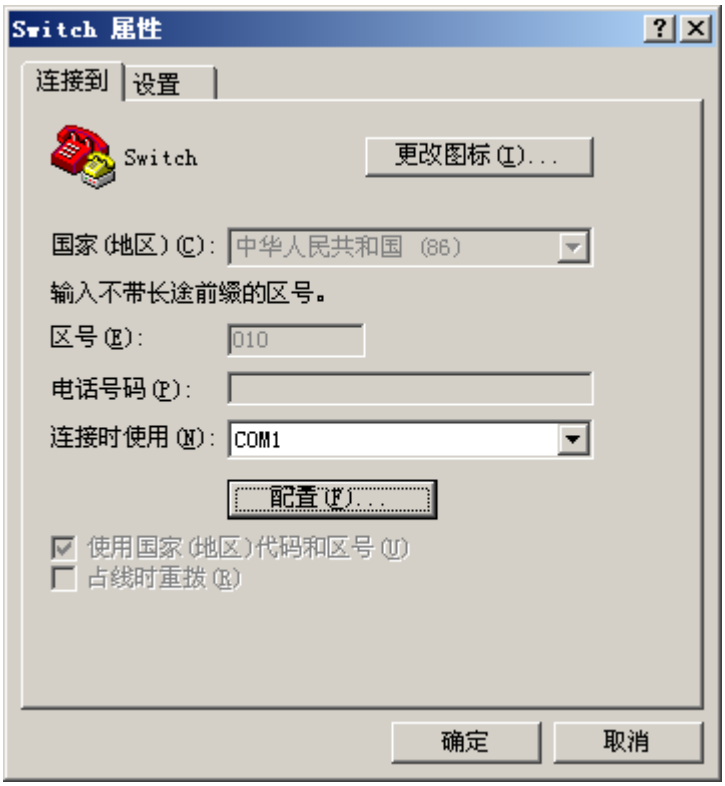
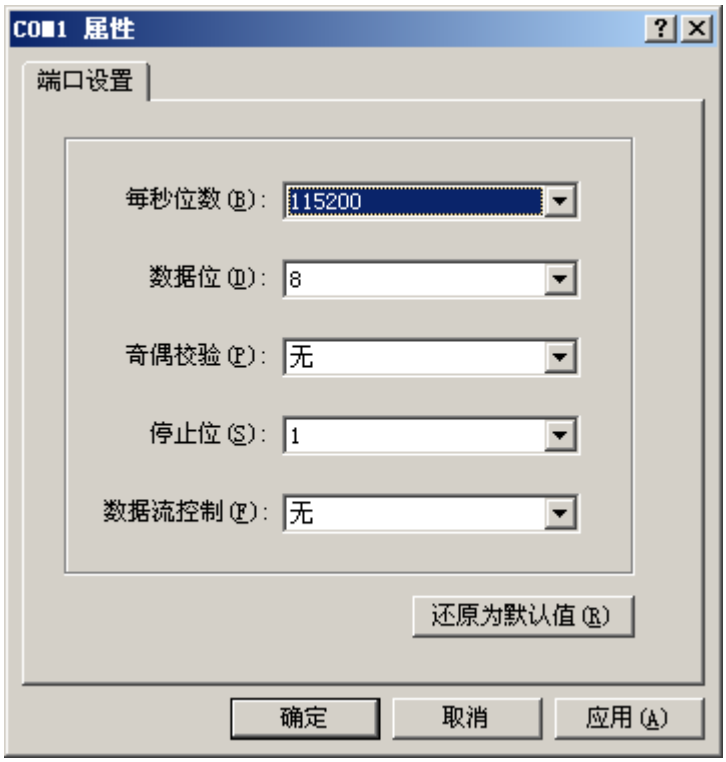


图8 串口配置对话框



(3) 设置完连接的波特率后，单击超级终端菜单栏的[呼叫/呼叫]菜单项，重新建立超级终端和交换机的连接。

图9 [呼叫/呼叫]菜单项

2.5.4 升级设备

(1) 回车后系统输出下载确认提示，键入<Y>，系统开始软件包下载；键入<N>，系统将返回BootRom 主菜单：

```
Are you sure to download file to flash? Yes or No (Y/N):Y
```

(2) 键入<Y>并回车后，系统开始软件包下载，终端显示如下信息：

```
Now please start transfer file with XMODEM protocol
If you want to exit, Press <Ctrl+X>
Loading ...CCCCCCCCCCCCCCCCCCCCCCCCC
```

说明

此时，若想退出程序下载，请键入<Ctrl+X>，否则继续进行如下操作。

(3) 从超级终端菜单栏中选择[传送/发送文件]（如图 10），在弹出的对话框中点击[浏览]按扭（如图 11），选择需要下载的软件包（此处以“update.ipe”为例），并将下载使用的协议改为XModem。

图10 [传送/发送文件]菜单项

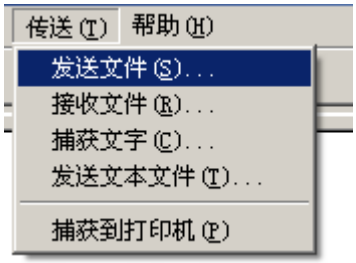
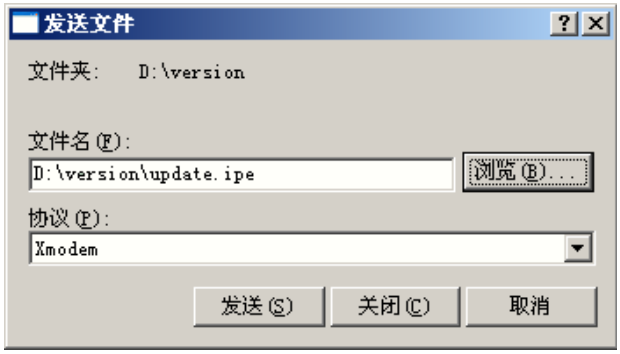


图11 [发送文件]对话框



(4) 选择完成后，点击[发送]按钮，系统弹出如下图所示的界面。

图12 正在发送文件界面

(5) 启动软件包下载完成后，系统提示用户设置该启动软件包的属性，即主用（M）、备用（B）或无属性（N）。键入<M>并回车，将所下载的软件包设置为主用启动软件包。

```
Please input the file attribute (Main/Backup/None) m
The boot.bin image is self-decompressing...
Load File name   : boot.bin          设置已下载的 Boot 软件包的名称
Free space: 470519808 bytes
Writing flash.....................................................................
.............
Done!
The system-update.bin image is self-decompressing...
Load File name   : system.bin         设置已下载的 System 软件包的名称
Free space: 461522944 bytes
Writing flash.....................................................................
.............
Done!
Your baudrate should be set to 9600 bps again!
Press enter key when ready
```

说明

如果在设置启动软件包的属性前设备中已经存在同样属性的启动软件包，则在用户的设置生效后，原有启动软件包的属性将会变为“无属性”。

(6) 参考 2.5.3 修改终端设置的波特率，重新将超级终端的波特率调整为 9600 bps。

说明

如果下载的速率选择为 9600 bps，用户不用重新调整超级终端的速率，请跳过此步骤。

(7) 回车后，系统返回 BootRom 主菜单，在 BootRom 主菜单中键入<0>并回车，重启设备后，升级后的启动软件包生效。

```
   EXTENDED BOOT MENU

EXTENDED BOOT MENU

1. Download image to flash
2. Select image to boot
3. Display all files in flash
4. Delete file from flash
5. Restore to factory default configuration
6. Enter BootRom upgrade menu
7. Skip current system configuration
8. Set switch startup mode
9. Set default boot storage medium
0. Reboot
Ctrl+F: Format file system
Ctrl+P: Change authentication for console login
Ctrl+R: Download image to SDRAM and run
Ctrl+C: Display Copyright

Enter your choice(0-9): 0
```

2.6 验证配置

设备重启后，使用 **display version** 命令查看设备版本信息。

```
<Switch> display version
H3C Comware Software, Version 7.1.070, Release xxxx
Copyright (c) 2004-2021 New H3C Technologies Co., Ltd. All rights reserved.
H3C Switch uptime is 0 weeks, 0 days, 0 hours, 19 minutes
Last reboot reason : User reboot
...
```

使用 **display boot-loader** 命令查看本次启动和下次启动所采用的启动软件包的名称。

```
<Switch> display boot-loader
Software images on slot 1:
Current software images:
  flash:/boot.bin
  flash:/system.bin
Main startup software images:
  flash:/boot.bin
  flash:/system.bin
Backup startup software images:
None
```

2.7 相关资料

- 产品配套“基础配置指导”中的“软件升级”。
- 产品配套“基础配置命令参考”中的“软件升级”。

3 使用 BootRom 菜单通过 TFTP/FTP 协议升级设备软件版本

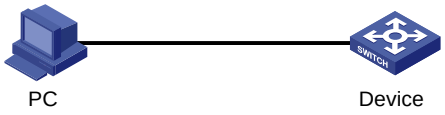
3.1 简介

本案例介绍用 BootRom 菜单通过 TFTP/FTP 协议升级设备软件版本的方法。

3.2 组网需求

如图 13 所示，主机和设备之间仅使用配置电缆连接。现要求：PC 作为文件服务器，并启动 FTP 服务器功能，Device 作为 FTP 客户端，通过 FTP 方式将软件升级包下载到 Device，并升级软件版本。

图13 通过 Console 口登录设备组网图



3.3 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包版本之间的兼容性，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。

3.4 配置准备

3.4.1 配置通过 Console 口登录设备

在通过 Console 口搭建本地配置环境时，需要通过终端仿真程序与设备建立连接。

打开终端仿真程序后，请按如下要求设置终端参数：

- 波特率：9600
- 数据位：8
- 停止位：1
- 奇偶校验：无
- 流量控制：无

设备上电，终端上显示设备自检信息，自检结束后提示用户键入回车，用户键入回车后将出现命令行提示符（如<Sysname>）。

```
******************************************************************************
* Copyright (c) 2004-2024 New H3C Technologies Co.,Ltd.All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************
Line aux0 is available.
Press ENTER to get started.
<Sysname>%Mar 30 09:52:58:243 2022 H3C SHELL/5/SHELL_LOGIN:TTY logged in from aux0.
<Sysname>
```

3.4.2 获取升级软件包

获取升级软件包有如下方式：

- 登录 H3C 官网 http://www.h3c.com，获取待升级的启动软件包。
- 联系 H3C 技术支持人员获取待升级的启动软件包。

3.4.3 下载管理软件

请提前下载好管理软件，本例以 FTP Server 为例。

3.5 配置步骤

3.5.1 查看当前版本

通过 **display version** 命令查看设备当前版本号（对比升级前后的设备软件版本可以验证升级是否成功）。

```
<Switch> display version
H3C Comware Software, Version 7.1.070, Release xxxx
Copyright (c) 2004-2024 New H3C Technologies Co., Ltd. All rights reserved.
H3C Switch uptime is 0 weeks, 0 days, 0 hours, 19 minutes
Last reboot reason : User reboot
...
```

3.5.2 通过 BootRom 菜单下载并升级 BootRom 程序

注意

- 不同设备不同版本的 BootRom 菜单不同，请以设备实际显示内容为准。
- 通过 FTP 和 TFTP 协议下载软件的操作类似，此处以 FTP 协议为例。
- 不同设备的升级过程可能存在差异，请以设备实际情况为准。

(1) 在用户 PC（假设 IP 地址为 192.168.0.23）上运行 FTP Server 程序，设置用户名和密码，以及正确的文件保存目录，并把待升级文件保存在 FTP Server 的工作目录下。

(2) 在用户 PC 上运行终端仿真程序，启动设备，键入<Ctrl+B>，进入 BootRom 扩展段主菜单。

```
   EXTENDED BOOT MENU

1. Download image to flash
2. Select image to boot
3. Display all files in flash
4. Delete file from flash
5. Restore to factory default configuration
6. Enter BootRom upgrade menu
7. Skip current system configuration
8. Set switch startup mode
9. Set The Operating Device
0. Reboot
Ctrl+Z: Access EXTENDED ASSISTANT MENU
Ctrl+F: Format file system
Ctrl+P: Change authentication for console login
Ctrl+R: Download image to SDRAM and run
Ctrl+C: Display Copyright

Enter your choice(0-9):
```

(3) 下载并升级 BootRom。

```
   EXTENDED BOOT MENU

1. Download image to flash
2. Select image to boot
3. Display all files in flash
4. Delete file from flash
5. Restore to factory default configuration
6. Enter BootRom upgrade menu
7. Skip current system configuration
8. Set switch startup mode
9. Set The Operating Device
0. Reboot
Ctrl+Z: Access EXTENDED ASSISTANT MENU
Ctrl+F: Format file system
Ctrl+P: Change authentication for console login
Ctrl+R: Download image to SDRAM and run
Ctrl+C: Display Copyright
```

键入<1>，加载应用程序到 flash。

```
1. Set TFTP protocol parameters
2. Set FTP protocol parameters
3. Set XMODEM protocol parameters
0. Return to boot menu

Enter your choice(0-3):
```

键入<2>，设置 FTP 协议参数。

说明

在设置参数时，直接输入新的参数即可；不输入参数，直接回车则不做修改，保留原有参数。

```
Load File Name         :test.ipe
                       :test.ipe
Server IP Address      :192.168.0.23
Local IP Address       :192.168.0.105
Subnet Mask            :255.255.255.0
Gateway IP Address     :0.0.0.0
FTP User Name          :xxx
FTP User Password      :***
```

表1 设置以太网口参数显示信息描述表

显示信息	说明
Load File Name	下载文件的名称，要与下载的文件名一致
Server IP Address	FTP/TFTP服务器或PC的IP地址
Local IP Address	设备的IP地址
Subnet Mask	子网掩码
Gateway IP Address	网关IP地址，如果设备与下载文件所在PC不在同一个网段中，需要配置网关IP地址
FTP User Name	FTP用户名
FTP User Password	FTP下载密码

设置完 FTP 协议相关参数后，键入<Y>，确认将应用程序下载到 flash。

```
Are you sure to download file to flash? Yes or No (Y/N):
```

键入<Main>，将应用程序设置为主用下次启动配置文件。

```
Please input the file attribute (Main/Backup/None)
```

菜单项	解释
Main	加载主用程序文件到当前存储介质 新加载的程序文件将自动被设置为M类型，原带有M类型的程序文件中的该属性将被取消
Backup	加载备用程序文件到当前存储介质 新加载的程序文件将自动被设置为B类型，原带有B类型的程序文件中的该属性将被取消
None	加载文件到当前存储介质

3.5.3 重启设备

BootRom 升级成功后，在 BootRom 主菜单中键入<0>，重启设备。

3.6 验证配置

设备重启后，使用 **display version** 命令查看设备版本信息。

```
<Switch> display version
H3C Comware Software, Version 7.1.070, Release xxxx
Copyright (c) 2004-2024 New H3C Technologies Co., Ltd. All rights reserved.
H3C Switch uptime is 0 weeks, 0 days, 0 hours, 19 minutes
Last reboot reason : User reboot
...
```

使用 **display boot-loader** 命令查看本次启动和下次启动所采用的启动软件包的名称。

```
<Switch> display boot-loader
Software images on slot 1:
Current software images:
  flash:/boot.bin
  flash:/system.bin
Main startup software images:
  flash:/boot.bin
  flash:/system.bin
Backup startup software images:
None
```

3.7 相关资料

- 产品配套“基础配置指导”中的“软件升级”。
- 产品配套“基础配置命令参考”中的“软件升级”。

设备管理快速配置指南

目 录

1 设备基础配置

1.1 简介

本案例介绍如何配置设备名称及系统时间。

设备可通过以下方式获取系统时间：

- 命令行配置。用户通过命令行指定系统时间后，设备会使用内部晶体震荡器产生的时钟信号继续计时。
- 网络时钟同步。设备周期性的同步 NTP/PTP 服务器的 UTC（Coordinated Universal Time，国际协调时间）时间，并用同步得到的 UTC 时间和设备上配置的本地时区、夏令时参数运算，得出当前的系统时间。关于 NTP 和 PTP 的详细介绍，请参见“网络管理和监控配置指导”中的“NTP”和“PTP”。

从网络时钟源获取的时间比命令行配置的时间更精准，推荐使用。

说明

PTP 的支持情况与设备型号有关，请根据实际情况进行配置。

1.2 组网需求

无。

1.3 配置步骤

1.3.1 配置设备名称

进入系统视图。

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

配置设备名称为 abcd。

```
[Device] sysname abcd
[adcd]
```

1.3.2 配置系统时间

1. 手动设置系统时间

进入系统视图。

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

配置系统时间获取方式为无。

```
[Device] clock protocol none
```

返回用户视图手动设置系统时间为 2021 年 9 月 1 日 11 时 8 分。

```
[Device] quit
```

```
<Device> clock datetime 11:8 2021/9/1
```

2. 通过 NTP 协议自动获取系统时间

进入系统视图。

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

配置系统时间获取方式为 NTP。

```
[Device] clock protocol ntp
```

3. 通过 PTP 协议自动获取系统时间

进入系统视图。

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

配置系统时间获取方式为 PTP。

```
[Device] clock protocol ptp
```

1.4 验证配置

查看设备当前系统时间。

```
[Device] display clock
11:08:00.258 UTC Wed 01/09/2021
```

显示信息中，时间的格式采用“时:分:秒.毫秒”的格式。

1.5 配置文件

- 配置设备名称

```
#
 sysname abcd
#
```

- 手工设置系统时间

```
#
 clock datetime 11:8 2021/9/1
 clock protocol none
#
```

- NTP 协议获取系统时间

```
#
 clock protocol ntp
#
```

- PTP 协议获取系统时间

```
#
 clock protocol ptp
#
```

1.6 相关资料

- 产品配套“基础配置指导”中的“设备管理”。
- 产品配套“基础配置命令参考”中的“设备管理”。

2 通过 scheduler reboot 定时重启设备

2.1 简介

本案例介绍通过 scheduler reboot 定时重启设备。

定时重启的方式有以下几种：

- 配置设备在具体的时间点重启
- 配置设备在一定时间后重启
- 配置设备在固定的时间重复执行重启操作

2.2 组网需求

无

2.3 配置步骤

2.3.1 配置设备在具体的时间和日期重启

假设系统的当前时间为 2021 年 9 月 1 日 11:00，配置设备在当天中午 12:00 重启。

```
<Device> scheduler reboot at 12:00
Reboot system at 12:00:00 01/09/2021 (in 1 hours and 0 minutes). Confirm? [Y/N]:Y
```

2.3.2 配置设备在一定时间后重启

假设系统的当前时间为 2021 年 9 月 1 日 11:00，配置设备在 88 分钟后重启。

```
<Device> scheduler reboot delay 88
Reboot system at 12:28 01/09/2021(in 1 hours and 28 minutes). Confirm? [Y/N]:Y
```

2.3.3 配置设备重复执行重启

进入系统视图。

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

创建执行重启命令的 job，命名为 reboot。

```
[Device] scheduler job reboot
[Device-job-reboot] command 1 reboot
```

退回系统视图。

```
[Device-job-reboot] quit
```

创建名称为 schedule-reboot 的 schedule，引用命名为 reboot 的 job 并配置每天 23:00 时执行。

```
[Device] scheduler schedule schedule-reboot
[Device-schedule-schedule-reboot] job reboot
[Device-schedule-schedule-reboot] time repeating at 23:00
```

退回系统视图。

```
[Device-schedule-schedule-reboot] quit
```

保存配置。

```
[Device] save
```

2.4 验证配置

显示设备重启时间。

```
<Device> display scheduler reboot
System will reboot at 12:28 01/09/2021 (in 1 hours and 28 minutes).
```

显示 Schedule。

```
[Device-schedule-schedule-reboot] display scheduler schedule
Schedule name        : schedule-reboot
Schedule type        : Run on every day at 23:00:00
Start time           : Wed Sep 01 11:00:00 2021
Last execution time  : Yet to be executed
--------------------------------------------------------------------------
Job name                                           Last execution status
reboot                                             -NA-
```

显示 Job。

```
[Device] display scheduler job
Job name: reboot
 reboot
```

2.5 配置文件

配置设备重复执行重启：

```
#
scheduler job reboot
 command 1 reboot
#
scheduler schedule schedule-reboot
 user-role network-operator
 user-role network-admin
 job reboot
 time repeating at 23:00
#
```

2.6 相关资料

- 产品配套“基础配置指导”中的“设备管理”。
- 产品配套“基础配置命令参考”中的“设备管理”。

NTP 快速配置指南

目 录

1 NTP 服务器/客户端模式典型配置

1.1 简介

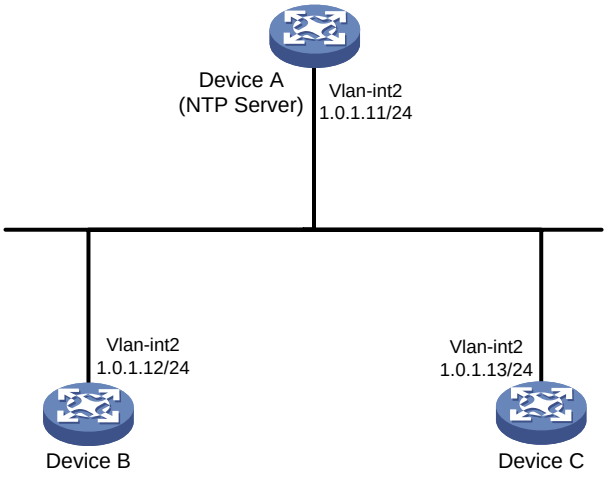
本案例介绍通过 NTP 实现服务器与客户端时间同步的配置方法。

1.2 组网需求

为了通过 NTP 实现 Device B 与 Device A 的时间同步，要求：

- 在 Device A 上设置本地时钟作为参考时钟，层数为 2；
- 配置 Device B 和 Device C 工作在客户端模式，指定 Device A 为 NTP 服务器。

图1 网络时钟 NTP 配置组网图



1.3 配置思路

(1) 配置 A、B、C 设备的 IP 地址并开启 NTP 服务

(2) 配置 A 设备的本地时钟作为参考时钟，层数为 2

(3) 配置 A 设备为 B、C 设备的 NTP 服务器

1.4 配置步骤

1. Device A 的配置

配置接口 Vlan-interface2 的 IP 地址。

```
<DeviceA> system-view
[DeviceA] interface Vlan-interface 2
[DeviceA-Vlan-interface2] ip address 1.0.1.11 24
[DeviceA-Vlan-interface2] quit
```

开启 NTP 服务。

```
[DeviceA] ntp-service enable
```

设置本地时钟作为参考时钟，层数为 2。

```
[DeviceA] ntp-service refclock-master 2
```

2. Device B 的配置

配置接口 Vlan-interface2 的 IP 地址。

```
<DeviceB> system-view
[DeviceB] interface Vlan-interface2
[DeviceB-Vlan-interface2] ip address 1.0.1.12 24
[DeviceB-Vlan-interface2] quit
```

开启 NTP 服务。

```
<DeviceB> system-view
[DeviceB] ntp-service enable
```

配置通过 NTP 协议获取时间。

```
[DeviceB] clock protocol ntp
```

设置 NTP Server 为 Device B 的 NTP 服务器。

```
[DeviceB] ntp-service unicast-server 1.0.1.11
```

3. Device C 的配置

配置接口 Vlan-interface2 的 IP 地址。

```
<DeviceC> system-view
[DeviceC] interface Vlan-interface2
[DeviceC-Vlan-interface2] ip address 1.0.1.13 24
[DeviceC-Vlan-interface2] quit
```

开启 NTP 服务。

```
<DeviceC> system-view
[DeviceC] ntp-service enable
```

配置通过 NTP 协议获取时间。

```
[DeviceC] clock protocol ntp
```

设置 NTP Server 为 Device C 的 NTP 服务器。

```
[DeviceC] ntp-service unicast-server 1.0.1.11
```

1.5 验证配置

完成上述配置后，Device B 和 Device C 向 Device A 进行时间同步。以 Device B 为例查看 NTP 状态。可以看出，Device B 已经与 Device A 同步，层数比 Device A 的层数大 1，为 3。

```
[DeviceB] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 System peer: 1.0.1.11
 Local mode: client
 Reference clock ID: 1.0.1.11
 Leap indicator: 00
 Clock jitter: 0.000977 s
 Stability: 0.000 pps
```

```
 Clock precision: 2^-10
 Root delay: 0.00383 ms
 Root dispersion: 16.26572 ms
 Reference time: d0c6033f.b9923965  Wed, Dec 29 2019 18:58:07.724
 System poll interval: 64 s
```

查看 Device B 的 NTP 服务的所有 IPv4 会话信息，可以看到 Device B 与 Device A 建立了会话。

```
[DeviceB] display ntp-service sessions
       source          reference       stra reach poll  now offset  delay disper
**************************************************************************
[12345]1.0.1.11        127.127.1.0        2   255  64   15   -4.0 0.0038 16.262
Notes: 1 source(master), 2 source(peer), 3 selected, 4 candidate, 5 configured.
     Total sessions: 1
```

1.6 配置文件

- Device A：

```
#
 interface Vlan-interface2
 ip address 1.0.1.11 24
 quit
 ntp-service enable
 ntp-service refclock-master 2
#
```

- Device B：

```
#
 interface Vlan-interface2
 ip address 1.0.1.12 24
 quit
 ntp-service enable
 clock protocol ntp
 ntp-service unicast-server 1.0.1.11
#
```

- Device C：

```
#
interface Vlan-interface2
 ip address 1.0.1.13 24
#
 ntp-service enable
 clock protocol ntp
 ntp-service unicast-server 1.0.1.11
#
```

1.7 相关资料

- 产品配套“网络管理和监控配置指导”中的“NTP”。
- 产品配套“网络管理和监控命令参考”中的“NTP”。

RBAC 快速配置指南

目 录

1 配置用户角色

1.1 简介

本案例介绍用户角色的配置方法。

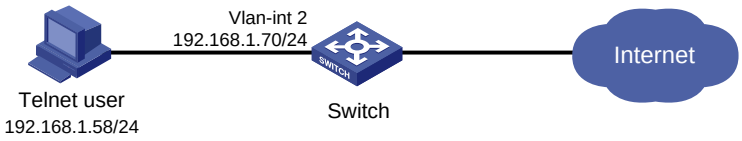
1.2 组网需求

Telnet 用户主机与 Switch 相连，需要实现 Switch 对 Telnet 用户进行本地认证并授权用户角色。Telnet 用户的登录用户名为 user1@bbb，认证通过后被授权的用户角色为 role1。

role1 具有如下用户权限：

- 允许用户执行所有特性中读类型的命令；
- 允许用户执行创建 VLAN 以及进入 VLAN 视图后的相关命令，并只具有操作 VLAN 10～VLAN 20 的权限。

图1-1 Telnet 用户本地认证/授权配置组网图



1.3 配置注意事项

- 一个 ISP 域被配置为缺省的 ISP 域后将不能够被删除，必须首先使用命令 **undo domain default enable** 将其修改为非缺省 ISP 域，然后才可以被删除。
- 一个用户角色中允许创建多条规则，各规则以创建时指定的编号为唯一标识，被授权该角色的用户可以执行的命令为这些规则定义的可执行命令的并集。若这些规则定义的权限内容有冲突，则规则编号大的有效。例如，规则 1 允许执行命令 A，规则 2 允许执行命令 B，规则 3 禁止执行命令 A，则最终规则 2 和规则 3 生效，即禁止执行命令 A，允许执行命令 B。

1.4 配置步骤

设置交换机系统名称为 Switch。

```
<H3C> system-view
[H3C] sysname Switch
```

配置 VLAN 接口 2 的 IP 地址，Telnet 用户将通过该地址连接 Switch。

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.1.70 255.255.255.0
[Switch-Vlan-interface2] quit
```

开启 Switch 的 Telnet 服务器功能。

```
[Switch] telnet server enable
```

配置 Telnet 用户登录采用 AAA 认证方式。

```
[Switch] line vty 0 63
[Switch-line-vty0-63] authentication-mode scheme
[Switch-line-vty0-63] quit
```

配置 ISP 域 bbb 的 AAA 方法为本地认证和本地授权。

```
[Switch] domain bbb
[Switch-isp-bbb] authentication login local
[Switch-isp-bbb] authorization login local
[Switch-isp-bbb] quit
```

创建用户角色 role1。

```
[Switch] role name role1
```

配置用户角色规则 1，允许用户执行所有特性中读类型的命令。

```
[Switch-role-role1] rule 1 permit read feature
```

配置用户角色规则 2，允许用户执行创建 VLAN 以及进入 VLAN 视图后的相关命令。

```
[Switch-role-role1] rule 2 permit command system-view ; vlan *
```

进入 VLAN 策略视图，允许用户具有操作 VLAN 10～VLAN 20 的权限。

```
[Switch-role-role1] vlan policy deny
[Switch-role-role1-vlanpolicy] permit vlan 10 to 20
[Switch-role-role1-vlanpolicy] quit
[Switch-role-role1] quit
```

创建设备管理类本地用户 user1。

```
[Switch] local-user user1 class manage
```

配置用户的密码是明文的 123456TESTplat&!。

```
[Switch-luser-manage-user1] password simple 123456TESTplat&!
```

指定用户的服务类型是 Telnet。

```
[Switch-luser-manage-user1] service-type telnet
```

指定用户 user1 的授权角色为 role1。

```
[Switch-luser-manage-user1] authorization-attribute user-role role1
```

为保证用户仅使用授权的用户角色 role1，删除用户 user1 具有的缺省用户角色 network-operator。

```
[Switch-luser-manage-user1] undo authorization-attribute user-role network-operator
[Switch-luser-manage-user1] quit
```

1.5 验证配置

用户向设备发起 Telnet 连接，在 Telnet 客户端按照提示输入用户名 user1@bbb 及正确的密码后，成功登录设备。

```
C:\Documents and Settings\user> telnet 192.168.1.50
login: user1@bbb
Password:
******************************************************************************
* Copyright (c) 2004-2019 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************
```

```
<Switch>
```

登录用户并被授予用户角色 role1，具有相应的命令行执行权限。可通过如下步骤验证用户的权限：

- 可操作 VLAN 10～VLAN 20。（以创建 VLAN 10 为例）

```
<Switch> system-view
[Switch] vlan 10
[Switch-vlan10] quit
```

- 不能操作其它 VLAN。（以创建 VLAN 30 为例）

```
[Switch] vlan 30
Permission denied.
```

- 可执行所有特性中读类型的命令。（以 **display clock** 为例）

```
[Switch] display clock
09:31:56.258 UTC Sat 01/01/2017
[Switch] quit
```

- 不能执行特性中写类型和执行类型的命令。

```
<Switch> debugging role all
Permission denied.
<Switch> ping 192.168.1.58
Permission denied.
```

1.6 配置文件

```
#
 sysname Switch
#
 telnet server enable
#
vlan 2
#
interface Vlan-interface2
 ip address 192.168.1.50 255.255.255.0
#
line vty 0 63
 authentication-mode scheme
#
domain bbb
 authentication login local
 authorization login local
#
role name role1
 rule 1 permit read feature
 rule 2 permit command system-view ; vlan *
 vlan policy deny
  permit vlan 10 to 20
#
local-user user1 class manage
 password hash $h$6$3nDcf1enrif2H0W6$QUWsXcld9MjeCMWGlkU6qleuV3WqFFEE8i2TTSoFRL3
ENZ2ExkhXZZrRmOl3pblfbje6fim7vV+u5FbCif+SjA==
```

```
 service-type telnet
 authorization-attribute user-role role1
 undo authorization-attribute user-role network-operator
#
```

1.7 相关资料

- 产品配套“基础配置指导”中的“RBAC”。
- 产品配套“基础命令参考”中的“RBAC”。

2 切换用户角色

2.1 简介

本案例介绍切换用户角色的配置方法。

2.2 组网需求

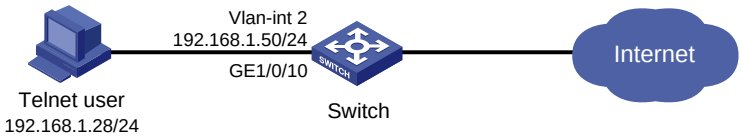
为了加强用户登录的安全性，采用本地 AAA 认证对登录设备的 Telnet 用户进行认证。登录设备的 Telnet 用户能够进行用户角色的切换，即在不下线的情况下，临时改变自身对系统的操作权限。当前 Telnet 用户被授权为用户角色 role1，用户角色 role1 具有如下权限：

- 允许执行系统预定义特性组 L3 相关的所有命令。
- 允许执行所有以 **display** 开头的命令。
- 允许执行所有以 **super** 开头的命令。
- 具有所有接口、VLAN 和 VPN 实例资源的操作权限。

现要求，Telnet 用户能够被切换到用户角色 role2 和 network-operator，其中用户角色 role2 具有如下权限：

- 允许执行系统预定义特性组 L2 相关的所有命令。
- 具有所有接口、VLAN 和 VPN 实例资源的操作权限。

图2-1 切换用户角色权限配置组网图



2.3 配置注意事项

- 一个 ISP 域被配置为缺省的 ISP 域后将不能够被删除，必须首先使用命令 **undo domain default enable** 将其修改为非缺省 ISP 域，然后才可以被删除。
- 一个用户角色中允许创建多条规则，各规则以创建时指定的编号为唯一标识，被授权该角色的用户可以执行的命令为这些规则定义的可执行命令的并集。若这些规则定义的权限内容有冲突，则规则编号大的有效。例如，规则 1 允许执行命令 A，规则 2 允许执行命令 B，规则 3 禁止执行命令 A，则最终规则 2 和规则 3 生效，即禁止执行命令 A，允许执行命令 B。
- 切换后的用户角色只对当前登录生效，用户重新登录后，又会恢复到原有用户角色。

2.4 配置步骤

设置交换机系统名称为 Switch。

```
<H3C> system-view
```

```
[H3C] sysname Switch
```
创建 VLAN 2 并将 Switch 连接 Telnet user 的端口划分到 VLAN 2 中。
```
[Switch] vlan 2
[Switch-vlan2] quit
[Switch] interface GigabitEthernet1/0/10
[Switch-GigabitEthernet1/0/10] port access vlan 2
[Switch-GigabitEthernet1/0/10] quit
```
创建 VLAN 接口 2 并配置 IP 地址。
```
[Switch] interface Vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.1.50 24
```
开启设备的 Telnet 服务器功能。
```
[Switch] telnet server enable
```
在编号为 0～63 的 VTY 用户线下，配置 Telnet 用户登录采用 AAA 认证方式。
```
[Switch] line vty 0 63
[Switch-line-vty0-63] authentication-mode scheme
[Switch-line-vty0-63] quit
```
配置 ISP 域 bbb 的 AAA 方法为本地认证和本地授权。
```
[Switch] domain bbb
[Switch-isp-bbb] authentication login local
[Switch-isp-bbb] authorization login local
[Switch-isp-bbb] quit
```
创建用户角色 role1，进入用户角色视图。
```
[Switch] role name role1
```
配置用户角色规则 1，允许用户执行预定义特性组 L3 相关的所有命令。
```
[Switch-role-role1] rule 1 permit execute read write feature-group L3
```
配置用户角色规则 2，允许用户执行所有以 **display** 开头的命令。
```
[Switch-role-role1] rule 2 permit command display *
```
配置用户角色规则 3，允许用户执行所有以 **super** 开头的命令。
```
[Switch-role-role1] rule 3 permit command super *
[Switch-role-role1] quit
```
创建用户角色 role2，进入用户角色视图。
```
[Switch] role name role2
```
配置用户角色规则 1，允许用户执行预定义特性组 L2 相关的所有命令。
```
[Switch-role-role2] rule 1 permit execute read write feature-group L2
[Switch-role-role2] quit
```
创建设备管理类本地用户 telnetuser。
```
[Switch] local-user telnetuser class manage
```
配置用户的密码是明文的 aabbcc。
```
[Switch-luser-manage-telnetuser] password simple aabbcc
```
指定用户的服务类型是 Telnet。
```
[Switch-luser-manage-telnetuser] service-type telnet
```
指定用户 telnetuser 的授权角色为 role1。
```
[Switch-luser-manage-telnetuser] authorization-attribute user-role role1
```

为保证用户仅使用授权的用户角色 role1，删除用户 telnetuser 具有的缺省用户角色 network-operator。

```
[Switch-luser-manage-telnetuser] undo authorization-attribute user-role network-operator
[Switch-luser-manage-telnetuser] quit
```

配置 Telnet 用户切换用户角色时采用 **local** 认证方式（系统缺省值为 **local**）。

```
[Switch] super authentication-mode local
```

配置 Telnet 用户将用户角色切换到 role2 时使用的密码为明文密码 123456TESTplat&!。

```
[Switch] super password role role2 simple 123456TESTplat&!
```

配置 Telnet 用户将用户角色切换到 network-operator 时使用的密码为明文密码 987654TESTplat&!。

```
[Switch] super password role network-operator simple 987654TESTplat&!
```

2.5 验证配置

(1) 查看用户角色和特性组信息

通过 **`display role`** 命令查看用户角色 role1、role2 和 network-operator 的信息。

显示用户角色 role1 的信息。

```
<Switch> display role name role1
Role: role1
  Description:
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  1       permit RWX   feature-group L3
  2       permit       command       display *
  3       permit       command       super *
  R:Read W:Write X:Execute
```

显示用户角色 role2 的信息。

```
<Switch> display role name role2
Role: role2
  Description:
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ----------------------------------------------------------------------
  1       permit RWX   feature-group L2
  R:Read W:Write X:Execute
```

显示用户角色 network-operator 的信息。

```
<Switch> display role name network-operator
Role: network-operator
  Description: Predefined network operator role has access to all read commands
```

```
on the device
  VLAN policy: permit (default)
  Interface policy: permit (default)
  VPN instance policy: permit (default)
  ------------------------------------------------------------------
  Rule    Perm   Type  Scope         Entity
  ------------------------------------------------------------------
  sys-1   permit       command       display *
  sys-2   permit       command       xml
  sys-3   permit       command       system-view ; probe ; display *
  sys-4   deny         command       display history-command all
  sys-5   deny         command       display exception *
  sys-6   deny         command       display cpu-usage configuration
                                     *
  sys-7   deny         command       display kernel exception *
  sys-8   deny         command       display kernel deadloop *
  sys-9   deny         command       display kernel starvation *
  sys-10  deny         command       display kernel reboot *
  sys-13  permit       command       system-view ; local-user *
  sys-16  permit R--   web-menu      -
  sys-17  permit RW-   web-menu      m_device/m_maintenance/m_changep
                                     assword
  sys-18  permit R--   xml-element   -
  sys-19  deny         command       display security-logfile summary
  sys-20  deny         command       display security-logfile buffer
  sys-21  deny         command       system-view ; info-center securi
                                     ty-logfile directory *
  sys-22  deny         command       security-logfile save
  sys-23  deny         command       system-view ; local-user-import
                                     *
  sys-24  deny         command       system-view ; local-user-export
                                     *
  sys-25  permit R--   oid           1
  R:Read W:Write X:Execute
```

通过 **display role feature-group** 命令查看特性组 L2 和 L3 中包括的特性信息，此处不详细介绍。

(2) 用户登录设备

用户向设备发起 Telnet 连接，在 Telnet 客户端按照提示输入用户名 telnetuser@bbb 及正确的密码后，成功登录设备。

```
C:\Documents and Settings\user> telnet 192.168.1.50
login: telnetuser@bbb
Password:
******************************************************************************
* Copyright (c) 2004-2019 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************
```

```
<Switch>
```

(3) 验证切换用户角色前的用户权限

Telnet 用户成功登录设备后，可通过如下步骤验证用户的权限：

- 可执行特性组 L3 中特性相关的所有命令。（以创建 VPN 实例 vpn1 为例）

```
<Switch> system-view
[Switch] ip vpn-instance vpn1
```

- 可执行所有以 **display** 开头的命令。（以显示系统当前日期和时间为例）

```
<Switch> display clock
13:53:24.357 test Sat 01/01/2018
Time Zone : test add 05:00:00
Summer Time : PDT 06:00:00 08/01 06:00:00 09/01 01:00:00
```

(4) 验证切换用户角色

Telnet 用户成功登录设备后，可通过如下步骤验证用户的权限：

a. 在用户视图下使用 **super** 开头的命令。（以切换到用户角色 role2 并输入相应的切换密码为例）

```
<Switch> super role2
Password:
User privilege role is role2, and only those commands that authorized to the role can be used.
<Switch>
```

b. 切换到用户角色 role2 后，可执行特性组 L2 中特性相关的所有命令。（以创建 VLAN 10 为例）

```
<Switch> system-view
[Switch] vlan 10
[Switch-vlan10] quit
[Switch] quit
```

c. 切换到用户角色 role2 后，不能执行非特性组 L2 中特性相关的命令。（以切换到用户角色 network-operator 为例）

```
<Switch> super network-operator
Permission denied.
```

d. 切换到用户角色 role2 后，不能执行以 **display** 开头的命令。（以显示系统当前日期和时间为例）

```
<Switch> display clock
Permission denied.
```

e. Telnet 用户重新登录设备后，才能执行所有以 **super** 开头的命令。（以切换到用户角色 network-operator 并输入相应的切换密码为例）

```
C:\Documents and Settings\user> telnet 192.168.1.50
login: telnetuser@bbb
Password:
******************************************************************************
* Copyright (c) 2004-2019 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
```

```
**************************************************************************

<Switch>
<Switch> super network-operator
Password:
User privilege role is network-operator, and only those commands that authorized
 to the role can be used.
<Switch>
```

通过显示信息可以确认配置生效。

2.6 配置文件

```
#
 sysname Switch
#
 telnet server enable
#
vlan 2
#
interface Vlan-interface2
 ip address 192.168.1.50 255.255.255.0
#
interface GigabitEthernet1/0/10
port access vlan 2
#
line vty 0 63
 authentication-mode scheme
 user-role network-operator
#
 super password role role2 hash $h$6$D0kjHFktkktzgR5g$e673xFnIcKytCj6EDAw+pvwgh3
/ung3WNWHnrUTnXT862B+s7PaLfKTdil8ef71RBOvuJvPAZHjiLjrMPyWHQw==
 super password role network-operator hash $h$6$3s5KMmscn9hJ6gPx$IcxbNjUc8u4yxwR
m87b/Jki8BoPAxw/s5bEcPQjQj/cbbXwTVcnQGL91WOd7ssO2rX/wKzfyzAO5VhBTn9Q4zQ==
#
domain bbb
 authentication login local
 authorization login local
#
role name role1
 rule 1 permit read write execute feature-group L3
 rule 2 permit command display *
 rule 3 permit command super *
#
role name role2
 rule 1 permit read write execute feature-group L2
#
 local-user telnetuser class manage
 password hash $h$6$kZw1rKFsAY4lhgUz$+teVLy8gmKN4Mr00VWgXQTB8ai94gKHlrys5OkytGf4
```

```
kT+nz5X1ZGASjc282CYAR6A1upH2jbmRoTcfDzZ9Gmw==
 service-type telnet
 authorization-attribute user-role role1
#
```

2.7 相关资料

- 产品配套“基础配置指导”中的“RBAC”。
- 产品配套“基础命令参考”中的“RBAC”。

IRF 快速配置指南

目 录

1 配置两台成员设备的 IRF

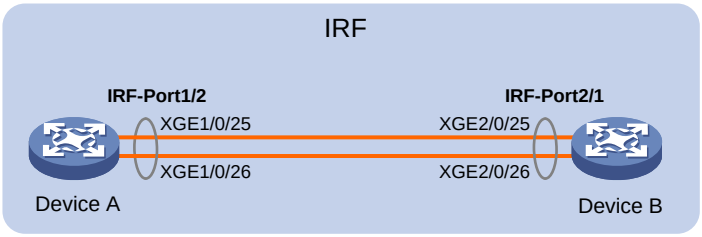
1.1 简介

本案例介绍两台成员设备的 IRF 的配置方法。

1.2 组网需求

Device A 为公司的核心设备，但由于公司网络规模日益增大，Device A 单台设备的转发能力已无法达到公司网络的需求。为了拓展核心设备的转发能力，又尽量不改变现有网络。现公司希望增加 Device B，与 Device A 组成 IRF，来满足当前网络的需求。

图1 两台成员设备的 IRF 典型配置组网图



1.3 配置思路与数据规划

配置思路如下，数据规划请参见表 1：

(1) 配置成员编号

不同成员设备需要配置不同的成员编号。修改成员编号的配置需要重启设备后生效。

(2) 配置成员优先级

在主设备选举过程中，优先级数值大的成员设备将优先被选举成为主设备。

(3) 配置 IRF 物理端口

(4) 保存配置

(5) 连接 IRF 物理链路

(6) 激活 IRF 端口配置

表1 数据规划表

设备	成员编号	成员优先级	IRF 端口及其绑定的物理端口
Device A	1（缺省）	32	IRF端口：irf-port 1/2 IRF物理接口： • Ten-GigabitEthernet 1/0/25 • Ten-GigabitEthernet 1/0/26
Device B	2	1（缺省）	IRF端口：irf-port 2/1 IRF物理接口：

设备	成员编号	成员优先级	IRF 端口及其绑定的物理端口
			• Ten-GigabitEthernet 2/0/25 • Ten-GigabitEthernet 2/0/26

1.4 配置注意事项

与IRF-Port1口绑定的IRF物理端口只能和邻居成员设备IRF-Port2口上绑定的IRF物理端口相连，本设备上与 IRF-Port2 口绑定的 IRF 物理端口只能和邻居成员设备 IRF-Port1 口上绑定的 IRF 物理端口相连。否则，不能形成 IRF。

1.5 配置步骤

1. Device A 的配置

(1) Device A 保留缺省编号为 1，不需要进行配置

(2) 创建 IRF 端口 2，并将它与物理端口 Ten-GigabitEthernet 1/0/25 和 Ten-GigabitEthernet 1/0/26 绑定

```
<DeviceA> system-view
[DeviceA] interface ten-gigabitethernet 1/0/25
[DeviceA-Ten-GigabitEthernet1/0/25] shutdown
[DeviceA-Ten-GigabitEthernet1/0/25] quit
[DeviceA] interface ten-gigabitethernet 1/0/26
[DeviceA-Ten-GigabitEthernet1/0/26] shutdown
[DeviceA-Ten-GigabitEthernet1/0/26] quit
[DeviceA] irf-port 1/2
[DeviceA-irf-port1/2] port group interface ten-gigabitethernet1/0/25
[DeviceA-irf-port1/2] port group interface ten-gigabitethernet1/0/26
[DeviceA-irf-port1/2] quit
[DeviceA] interface ten-gigabitethernet 1/0/25
[DeviceA-Ten-GigabitEthernet1/0/25] undo shutdown
[DeviceA-Ten-GigabitEthernet1/0/25] quit
[DeviceA] interface ten-gigabitethernet 1/0/26
[DeviceA-Ten-GigabitEthernet1/0/26] undo shutdown
[DeviceA-Ten-GigabitEthernet1/0/26] quit
```

(3) 配置 Device A 的成员优先级为 32，以保证其成为 IRF 中的主设备。

```
[DeviceA] irf member 1 priority 32
```

(4) 保存配置

```
[DeviceA] save force
```

2. Device B 的配置

(1) 设置 Device B 的成员编号为 2，并重启设备使配置生效。

```
<DeviceB> system-view
[DeviceB] irf member 1 renumber 2
Warning: Renumbering the switch number may result in configuration change or loss.
Continue? [Y/N]:y
[DeviceB] quit
```

```
<DeviceB> reboot
```

(2) 创建设备的 IRF 端口 1，并将它与物理端口 Ten-GigabitEthernet 2/0/25 和 Ten-GigabitEthernet 2/0/26 绑定

```
[DeviceB] interface ten-gigabitethernet 2/0/25
[DeviceB-Ten-GigabitEthernet2/0/25] shutdown
[DeviceB-Ten-GigabitEthernet2/0/25] quit
[DeviceB] interface ten-gigabitethernet 2/0/26
[DeviceB-Ten-GigabitEthernet2/0/26] shutdown
[DeviceB-Ten-GigabitEthernet2/0/26] quit
[DeviceB] irf-port 2/1
[DeviceB-irf-port2/1] port group interface ten-gigabitethernet2/0/25
[DeviceB-irf-port2/1] port group interface ten-gigabitethernet2/0/26
[DeviceB-irf-port2/1] quit
[DeviceB] interface ten-gigabitethernet 2/0/25
[DeviceB-Ten-GigabitEthernet2/0/25] undo shutdown
[DeviceB-Ten-GigabitEthernet2/0/25] quit
[DeviceB] interface ten-gigabitethernet 2/0/26
[DeviceB-Ten-GigabitEthernet2/0/26] undo shutdown
[DeviceB-Ten-GigabitEthernet2/0/26] quit
```

(3) 保存配置

```
[DeviceB] save force
```

(4) 参照 1.2 图 1 和端口连接表连接 Device A 和 Device B 之间的 IRF 端口

3. 激活配置

激活 DeviceA 的 IRF 端口配置。

```
[DeviceA] irf-port-configuration active
```

激活 DeviceB 的 IRF 端口配置。

```
[DeviceB] irf-port-configuration active
```

两台设备间将会进行 Master 竞选，竞选失败的一方将自动重启，重启完成后，IRF 形成，系统名称统一为 DeviceA。

1.6 验证配置

验证 IRF 建立成功：

```
<DeviceA> display irf
MemberID  Slot  Role    Priority  CPU-Mac         Description
 *+1      0     Master  32        0210-fc01-0000  ---
   2      0     Standby 1         0210-fc02-0000  ---
--------------------------------------------------
 * indicates the device is the master.
 + indicates the device through which the user logs in.

 The Bridge MAC of the IRF is: 3822-d60f-2800
 Auto upgrade                : yes
 Mac persistent              : always
 Domain ID                   : 0
 Auto merge                  : yes
```

从命令行的显示看，当前两台设备 IRF 成功建立。

1.7 配置文件

- Device A：

```
#
irf-port 1/2
 port group interface ten-gigabitethernet1/0/25
 port group interface ten-gigabitethernet1/0/26
#
 irf member 1 priority 32
 irf-port-configuration active
#
```

- Device B：

```
#
irf-port 2/1
 port group interface ten-gigabitethernet2/0/25
 port group interface ten-gigabitethernet2/0/26
#
 irf member 1 renumber 2
 irf-port-configuration active
#
```

1.8 相关资料

- 产品配套“虚拟化技术配置指导”中的“IRF”。
- 产品配套“虚拟化技术命令参考”中的“IRF”。

2 通过 BFD MAD 检测 IRF

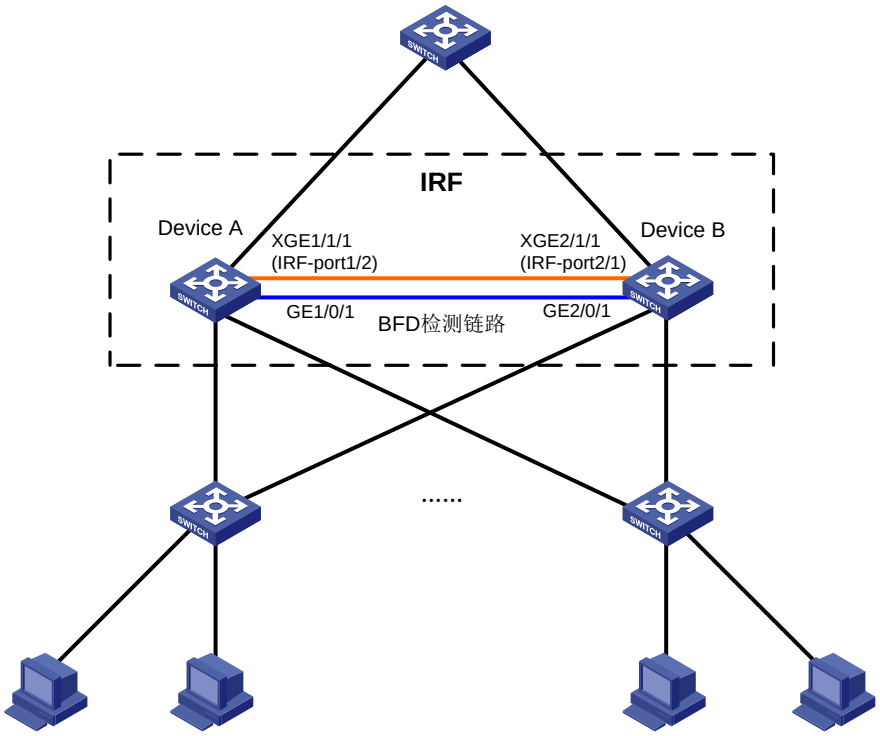
2.1 简介

本案例介绍通过 BFD MAD 检测 IRF 的配置方法。

2.2 组网需求

设备 Device A 和 Device B 配置 IRF，为了防止万一 IRF 链路故障导致 IRF 分裂、网络中存在两个配置冲突的 IRF，需要启用 MAD 检测功能，采用 BFD MAD 检测方式来监测 IRF 的状态，IRF 分裂后，通过分裂检测机制 IRF 会检测到网络中存在其它处于 Active 状态，冲突处理会让 Master 成员编号最小的 IRF 继续正常工作，其它 IRF 会迁移到 Recovery 状态（表示 IRF 处于禁用状态），并关闭 Recovery 状态 IRF 中所有成员设备上除保留端口以外的其它所有物理端口。

图2 BFD MAD 组网连接图



2.3 配置注意事项

- BFD MAD 和 STP 功能互斥，用于 BFD MAD 检测的端口不能使能 STP 功能。
- 使能 BFD MAD 检测功能的三层接口只能专用于 BFD MAD 检测，不允许运行其它业务。如果配置了其它业务，可能会影响该业务以及 BFD MAD 检测功能的运行。

2.4 配置步骤

1. 配置交换机 Device A 和 Device B 建立 IRF

具体配置可参考 1 配置两台成员设备的 IRF。

2. 配置 BFD MAD

IRF 上的配置：

创建 VLAN 3，并将 Device A 上的端口 GigabitEthernet1/0/1 和 Device B 上的端口 GigabitEthernet2/0/1 加入 VLAN3 中。

```
<IRF> system-view
[IRF] vlan 3
[IRF-vlan3] port gigabitethernet 1/0/1 gigabitethernet 2/0/1
[IRF-vlan3] quit
```

创建 VLAN 接口 3，并配置 MAD IP 地址。

```
[IRF] interface vlan-interface 3
[IRF-Vlan-interface3] mad bfd enable
[IRF-Vlan-interface3] mad ip address 192.168.2.1 24 member 1
[IRF-Vlan-interface3] mad ip address 192.168.2.2 24 member 2
[IRF-Vlan-interface3] quit
```

因为 BFD MAD 和生成树功能互斥，所以在 GigabitEthernet1/0/1 和 GigabitEthernet2/0/1 上关闭生成树协议。

```
[IRF] interface gigabitethernet 1/0/1
[IRF-gigabitethernet1/0/1] undo stp enable
[IRF-gigabitethernet1/0/1] quit
[IRF] interface gigabitethernet 2/0/1
[IRF-gigabitethernet2/0/1] undo stp enable
```

2.5 验证配置

当 IRF 分裂时，在 Device A 上执行 **display mad verbose** 命令，可以看到一台设备 Multi-active recovery state 为 No，Device A 正常工作。

```
<DeviceA> display mad
MAD ARP disabled.
MAD ND disabled.
MAD LACP disabled.
MAD BFD enabled.
<DeviceA> display mad verbose
Multi-active recovery state: No
Excluded ports (user-configured):
Excluded ports (system-configured):
Ten-GigabitEthernet1/1/1
MAD ARP disabled.
MAD ND disabled.
MAD LACP disabled.
MAD BFD enabled interface: Vlan-interface3
  MAD status                 : Faulty
```

```
  Member ID   MAD IP address       Neighbor    MAD status
  1           192.168.2.1/24       2           Faulty
```

当 Device B 为 Recovery 状态时，使用 **display interface brief down** 查看 Device B 端口时发现端口全部被关闭，状态为 mad shutdown。

```
<DeviceB> display interface brief down
Brief information on interfaces in route mode:
Link: ADM - administratively down; Stby - standby
Interface Link Cause
GE2/0/2 DOWN MAD ShutDown
GE2/0/3 DOWN MAD ShutDown
```

2.6 配置文件

```
#
vlan 3
 port gigabitethernet 1/0/1 gigabitethernet 2/0/1
#
interface vlan-interface 3
 mad bfd enable
 mad ip address 192.168.2.1 24 member 1
 mad ip address 192.168.2.2 24 member 2
#
interface gigabitethernet 1/0/1
 undo stp enable
#
interface gigabitethernet 2/0/1
 undo stp enable
#
```

2.7 相关资料

- 产品配套“虚拟化技术配置指导”中的“IRF”。
- 产品配套“虚拟化技术命令参考”中的“IRF”。

以太网接口快速配置指南

目 录

1 激活 Combo 接口中的电口或者光口

1.1 简介

本案例介绍激活 Combo 接口中的电口或者光口的配置方法。

1.2 配置需求

通过命令行先后开启 Combo 接口中的电口和光口。

1.3 配置注意事项

Combo 接口是一个逻辑接口，一个 Combo 接口在物理上对应设备面板上一个电口和一个光口。电口与其对应的光口共用一个转发接口和接口视图，所以，两者不能同时工作。当激活其中的一个接口时，另一个接口就自动处于禁用状态。

1.4 配置步骤

指定 GigabitEthernet1/0/1 端口的电口被激活，使用双绞线连接。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] combo enable copper
[Sysname-GigabitEthernet1/0/1] quit
```

指定 GigabitEthernet1/0/1 端口的光口被激活，使用光纤连接。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] combo enable fiber
[Sysname-GigabitEthernet1/0/1] quit
```

1.5 验证配置

Combo 接口上同时连接了电缆或光模块时，请通过 **display interface** 命令查看接口信息，如果显示信息中包含“Media type is twisted pair”，则表示电口处于激活状态，否则，则表示光口处于激活状态。

```
[Sysname] display interface GigabitEthernet 1/0/1
GigabitEthernet1/0/1
Current state: DOWN
Line protocol state: DOWN
IP packet frame type: Ethernet II, hardware address: 00ff-00ff-0139
Description: GigabitEthernet1/0/1 Interface
Bandwidth: 1000000 kbps
Loopback is not set
Media type is twisted pair
Port hardware type is 1000_BASE_T
Unknown-speed mode, unknown-duplex mode
```

```
Link speed type is autonegotiation, link duplex type is autonegotiation
…
```

1.6 配置文件

```
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 combo enable copper
#
```

1.7 相关资料

- 产品配套“二层技术-以太网交换配置指导”中的“以太网接口”。
- 产品配套“二层技术-以太网交换命令参考”中的“以太网接口”。

2 配置以太网接口速率和双工模式

2.1 简介

本案例介绍以太网接口速率和双工模式的配置方法。

2.2 组网需求

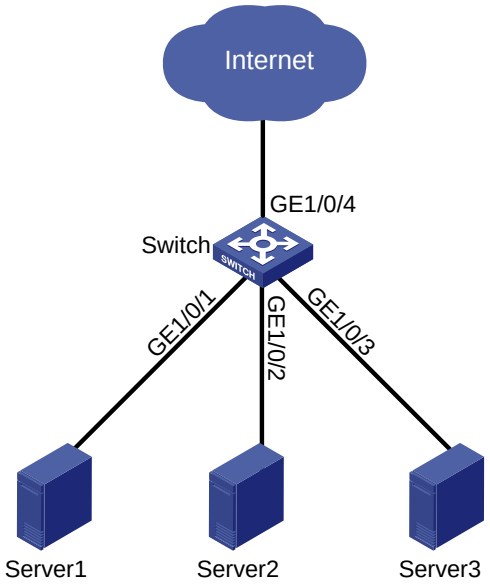
如图 1 所示，服务器群（Server1、Server2 和 Server3）分别与 Switch 的接口 GE1/0/1、GE1/0/2 和 GE1/0/3 相连，Switch 通过接口 GE1/0/4 上行接入 Internet 网络。

由于服务器网卡的特殊限制，存在以下问题：

- 接口 GE1/0/1、GE1/0/2 和 GE1/0/3 只能自协商为半双工模式，在该双工模式下，当业务数据流量较大时将会产生丢包现象。
- 接口 GE1/0/1、GE1/0/2 和 GE1/0/3 速率自协商为最大速率 1000Mbit/s，当服务器群同时以 1000Mbit/s 速率对外发送数据时，就会造成出接口 GE1/0/4 拥塞。

用户希望解决数据丢包和拥塞问题。

图1 配置非自协商模式下速率和双工模式组网图



2.3 配置思路

配置思路如下：

- 强制指定接口双工模式为全双工，避免发生数据丢包现象。
- 强制指定接口工作速率为 100Mbit/s，避免发生数据拥塞现象。

2.4 配置步骤

##将以太网接口 GigabitEthernet1/0/1～GigabitEthernet1/0/3 定义为 myEthPort，并进入批量接口视图。

```
<H3C> system-view
[H3C] sysname Switch
[Switch] interface range name myEthPort interface gigabitethernet 1/0/1 to gigabitethernet 1/0/3
[Sysname-if-range-myEthPort]
```

批量配置接口 GE1/0/1、GE1/0/2 和 GE1/0/3 工作在全双工模式、工作速率为 100Mbit/s。

```
[Sysname-if-range-myEthPort] duplex full
[Sysname-if-range-myEthPort] speed 100
[Sysname-if-range-myEthPort] quit
```

说明

在批量接口配置视图下执行配置命令后，设备会向 GE1/0/1、GE1/0/2 和 GE1/0/3 下发该配置，并打印各端口的配置信息。

2.5 验证配置

在任意视图下执行命令 **display interface**，检查接口当前工作速率及双工模式。

```
[Switch] display interface gigabitethernet 1/0/1
...
Media type is twisted pair, port hardware type is 1000_BASE_T
Port priority: 0
100Mbps-speed mode, Full-duplex mode
Link speed type is force link, link duplex type is force link
Flow-control is not enabled
Maximum frame length: 12288                                                    ...
```

由上述回显字段看出接口工作在全双工模式，工作速率为 100Mbit/s。

同理，对于 GE1/0/2 和 GE1/0/3 也可以通过执行 **display interface** 命令查看接口当前工作信息。

2.6 配置文件

Switch 的配置文件：

```
#
sysname Switch
#
interface range name myEthPort interface gigabitethernet 1/0/1 to gigabitethernet 1/0/3
#
```

2.7 相关资料

- 产品配套“二层技术-以太网交换配置指导”中的“以太网接口”。
- 产品配套“二层技术-以太网交换命令参考”中的“以太网接口”。

3 配置接口二三层切换

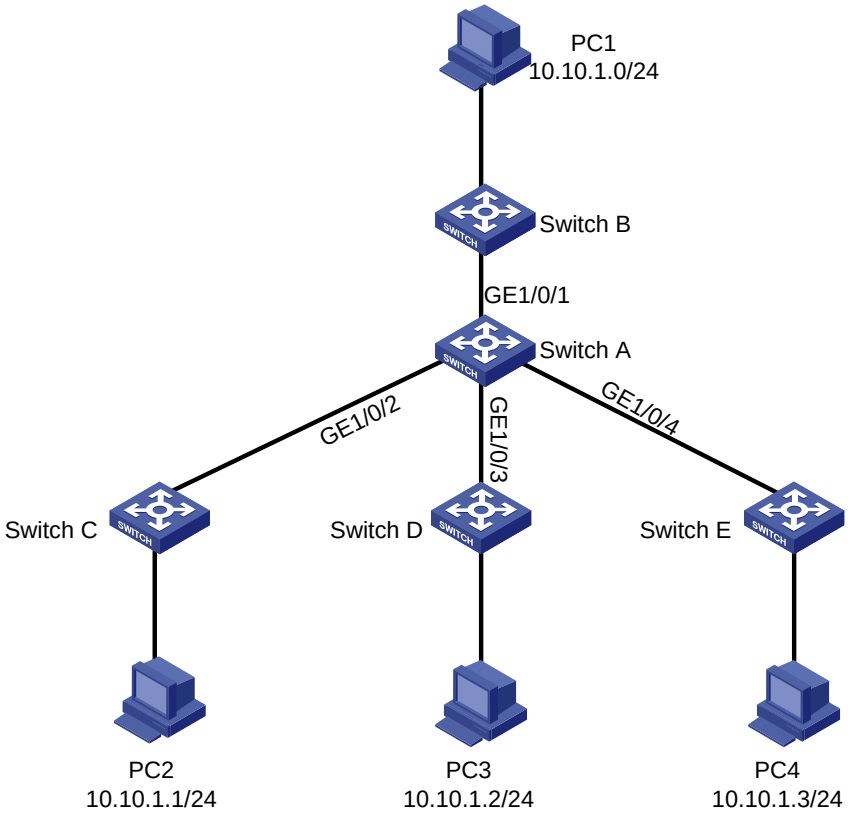
3.1 简介

本案例介绍以太网接口二三层切换的配置方法。

3.2 组网需求

如图 2 所示，PC1、PC2、PC3 和 PC4 分别属于不同网段，SwitchB、SwitchC、SwitchD、SwitchE 分别为这四个网段的接入层交换机。用户希望使用 SwitchA 上的四个以太网物理接口作为这四个网段的网关接口。

图2 以太网接口二三层切换配置组网图



3.3 配置思路

配置思路如下：

- 将接口的工作模式切换为三层模式。
- 配置三层以太网接口的 IP 地址作为网关。

3.4 配置步骤

1. 配置接口切换到三层模式

配置以太网接口 GigabitEthernet1/0/1～GigabitEthernet1/0/4 切换到三层模式。

```
<H3C> system-view
[H3C] sysname SwitchA
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] port link-mode route
[SwitchA-GigabitEthernet1/0/1] quit
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-mode route
[SwitchA-GigabitEthernet1/0/2] quit
[SwitchA] interface gigabitethernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] port link-mode route
[SwitchA-GigabitEthernet1/0/3] quit
[SwitchA] interface gigabitethernet 1/0/4
[SwitchA-GigabitEthernet1/0/4] port link-mode route
[SwitchA-GigabitEthernet1/0/4] quit
```

2. 配置三层接口的 IP 地址作为网关

以配置 GE1/0/1 接口的 IP 地址作为网关为例。

说明

GE1/0/2、GE1/0/3、GE1/0/4 的配置与 GE1/0/1 的类似，详见配置文件。

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] ip address 10.10.1.1 24
[SwitchA-GigabitEthernet1/0/1] quit
```

3.5 验证配置

在任意视图下执行命令 **display interface**，检查接口当前工作模式。

```
[SwitchA] display interface gigabitethernet 1/0/1
...
Unicast max-ratio: 100%
Internet protocol processing: Disabled
IP packet frame type: Ethernet II, hardware address: 3c8c-4002-8001
IPv6 packet frame type: Ethernet II, hardware address: 3c8c-4002-8001
Media type is not sure, port hardware type is no connector
Ethernet port mode: LAN
Port priority: 0
...
```

3.6 配置文件

SwitchA 的配置文件：

```
#
sysname SwitchA
#
interface GigabitEthernet1/0/1
port link-mode route
ip address 10.10.1.1 255.255.255.0
#
interface GigabitEthernet1/0/2
port link-mode route
ip address 10.10.2.1 255.255.255.0
#
interface GigabitEthernet1/0/3
port link-mode route
ip address 10.10.3.1 255.255.255.0
#
interface GigabitEthernet1/0/4
port link-mode route
ip address 10.10.4.1 255.255.255.0
#
```

3.7 相关资料

- 产品配套“二层技术-以太网交换配置指导”中的“以太网接口”。
- 产品配套“二层技术-以太网交换命令参考”中的“以太网接口”。

4 配置流量抑制

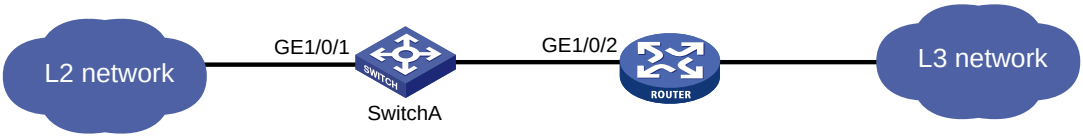
4.1 简介

本案例介绍流量抑制的配置方法。

4.2 组网需求

如图 3 所示，SwitchA 作为二层网络到三层路由器的衔接点，需要限制二层网络转发。

图3 配置流量抑制组网图



4.3 配置步骤

#进入接口视图。

```
<H3C> system-view
[H3C] sysname SwitchA
[SwitchA] interface gigabitethernet 1/0/1
```

配置广播流量阈值，上限阈值为 2000kbps、下限阈值为 1500kbps。

```
[SwitchA-gigabitethernet 1/0/1] storm-constrain broadcast kbps 2000 1500
```

配置组播流量百分比阈值，上限为 80%、下限为 15%。

```
[SwitchA-gigabitethernet 1/0/1] storm-constrain multicast ratio 80 15
```

配置未知单播流量阈值，上限阈值为 200pps、下限阈值为 150pps。

```
[SwitchA-gigabitethernet 1/0/1] storm-constrain unicast pps 200 150
```

配置当流量超过上限阈值时，采用 block 方式控制。

```
[SwitchA-GigabitEthernet1/0/1] storm-constrain control block
```

配置端口流量从小于等于上限阈值到大于上限阈值或者从超上限回落到小于下限阈值时输出 Log 信息。

```
[SwitchA-GigabitEthernet1/0/1] storm-constrain enable log
```

配置端口流量从小于等于上限阈值到大于上限阈值或者从超上限回落到小于下限阈值时输出 Trap 信息。

```
[SwitchA-GigabitEthernet1/0/1] storm-constrain enable trap
```

配置端口流量统计时间间隔为 60 秒。

```
[SwitchA-GigabitEthernet1/0/1]quit
[SwitchA] storm-constrain interval 60
```

4.4 验证配置

在 GE1/0/1 接口下执行命令 display this 查看接口的流量抑制配置情况。

```
[SwitchA-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
storm-constrain broadcast kbps 2000 1500
 storm-constrain multicast ratio 80 15
 storm-constrain unicast pps 200 150
 storm-constrain control block
#
return
```

4.5 配置文件

SwitchA 的配置文件：

```
#
sysname SwitchA
#
interface GigabitEthernet1/0/1
storm-constrain broadcast kbps 2000 1500
storm-constrain multicast ratio 80 15
storm-constrain unicast pps 200 150
storm-constrain control block
storm-constrain enable log
storm-constrain enable trap
#
storm-constrain interval 60
#
```

4.6 相关资料

- 产品配套“二层技术-以太网交换配置指导”中的“以太网接口”。
- 产品配套“二层技术-以太网交换命令参考”中的“以太网接口”。

5 配置风暴抑制

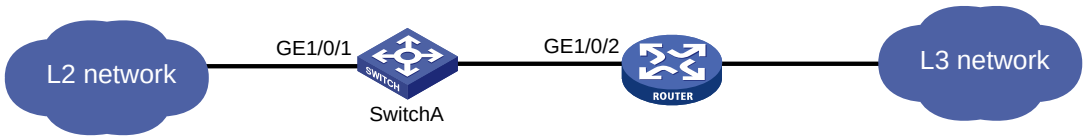
5.1 简介

本案例介绍风暴抑制的配置方法。

5.2 组网需求

如图 4 所示，SwitchA 作为二层网络到三层路由器的衔接点，需要防止二层网络转发的来自用户的广播、组播或未知单播报文而产生的广播风暴。

图4 配置风暴抑制组网图



5.3 配置步骤

进入接口视图。

```
<H3C> system-view
[H3C] sysname SwitchA
[SwitchA] interface gigabitethernet 1/0/1
```

配置广播风暴抑制。每秒最多允许10000kbps广播报文通过，对超出该范围的广播报文进行抑制。

```
[SwitchA-GigabitEthernet1/0/1] broadcast-suppression kbps 10000
```

配置组播风暴抑制。每秒最多允许10000kbps组播报文通过，对超出该范围的组播报文进行抑制。

```
[SwitchA-GigabitEthernet1/0/1] multicast-suppression kbps 10000
```

配置未知单播播风暴抑制。每秒最多允许 10000kbps 未知单播报文通过，对超出该范围的未知单播报文进行抑制。

```
[SwitchA-GigabitEthernet1/0/1] unicast-suppression kbps 10000
```

5.4 验证配置

在 GE1/0/1 接口下执行命令 display this 查看接口的风暴抑制配置情况。

```
[SwitchA-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
broadcast-suppression kbps 10000
multicast-suppression kbps 10000
unicast-suppression kbps 10000
#
return
```

5.5 配置文件

SwitchA 的配置文件：

```
#
sysname SwitchA
#
interface GigabitEthernet1/0/1
broadcast-suppression kbps 10000
multicast-suppression kbps 10000
unicast-suppression kbps 10000
#
```

5.6 相关资料

- 产品配套“二层技术-以太网交换配置指导”中的“以太网接口”。
- 产品配套“二层技术-以太网交换命令参考”中的“以太网接口”。

VLAN 快速配置指南

目 录

1 基于端口的 VLAN 快速配置指南

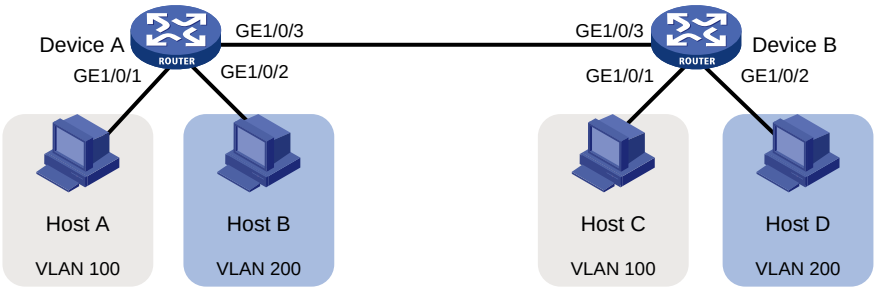
1.1 简介

本案例介绍基于端口的 VLAN 的配置方法。

1.2 组网需求

如图 1 所示，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，以及避免广播报文泛滥，公司网络中使用 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。现要求同一 VLAN 内的主机能够互通，即 Host A 和 Host C 能够互通，Host B 和 Host D 能够互通。

图1 基于端口的 VLAN 组网图



1.3 配置步骤

1. Device A 的配置

创建 VLAN 100，并将 GigabitEthernet1/0/1 加入 VLAN 100

```
<DeviceA> system-view
[DeviceA] vlan 100
[DeviceA-vlan100] port gigabitEthernet 1/0/1
[DeviceA-vlan100] quit
```

创建 VLAN 200，并将 GigabitEthernet1/0/2 加入 VLAN 200

```
[DeviceA] vlan 200
[DeviceA-vlan200] port GigabitEthernet 1/0/2
[DeviceA-vlan200] quit
```

为了使 Device A 上 VLAN 100 和 VLAN 200 的报文能发送给 Device B，将 GigabitEthernet 1/0/3 的链路类型配置为 Trunk，并允许 VLAN 100 和 VLAN 200 的报文通过。

```
[DeviceA] interface gigabitEthernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port link-type trunk
[DeviceA-GigabitEthernet1/0/3] port trunk permit vlan 100 200
[DeviceA-GigabitEthernet1/0/3] quit
```

保存配置

```
[DeviceA] save force
```

2. Device B 的配置

创建 VLAN 100，并将 GigabitEthernet1/0/1 加入 VLAN 100

```
<DeviceB> system-view
[DeviceB] vlan 100
[DeviceB-vlan100] port gigabitEthernet 1/0/1
[DeviceB-vlan100] quit
```

创建 VLAN 200，并将 GigabitEthernet1/0/2 加入 VLAN 200

```
[DeviceB] vlan 200
[DeviceB-vlan200] port gigabitEthernet 1/0/2
[DeviceB-vlan200] quit
```

为了使 Device B 上 VLAN 100 和 VLAN 200 的报文能发送给 Device A，将 GigabitEthernet 1/0/3 的链路类型配置为 Trunk，并允许 VLAN 100 和 VLAN 200 的报文通过。

```
[DeviceB] interface gigabitEthernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] port link-type trunk
[DeviceB-GigabitEthernet1/0/3] port trunk permit vlan 100 200
[DeviceB-GigabitEthernet1/0/3] quit
```

保存配置

```
[DeviceB] save force
```

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。

1.4 验证配置

显示 Device A 上 VLAN 的配置信息。

```
<DeviceA> display vlan 100
 VLAN ID: 100
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0100
 Name: VLAN 0100
 Tagged ports:
    GigabitEthernet1/0/3(D)
 Untagged ports:
    GigabitEthernet1/0/1(D)
<DeviceA> display vlan 200
 VLAN ID: 200
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0200
 Name: VLAN 0200
 Tagged ports:
    GigabitEthernet1/0/3(D)
 Untagged ports:
    GigabitEthernet1/0/2(D)
```

显示 Device B 上 VLAN 的配置信息。

```
<DeviceB> display vlan 100
 VLAN ID: 100
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0100
 Name: VLAN 0100
 Tagged ports:
    GigabitEthernet1/0/3(D)
 Untagged ports:
GigabitEthernet1/0/1(D)
<DeviceB> display vlan 200
 VLAN ID: 200
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0200
 Name: VLAN 0200
 Tagged ports:
    GigabitEthernet1/0/3(D)
 Untagged ports:
    GigabitEthernet1/0/2(D)
```

1.5 配置文件

- Device A：

```
#
vlan 100
#
vlan 200
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 200
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100 200
```

- #Device B ：

```
vlan 100
#
vlan 200
#
```

```
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 200
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100 200
```

1.6 相关资料

- 产品配套“二层技术-以太网交换配置指导”中的“VLAN”。
- 产品配套“二层技术-以太网交换命令参考”中的“VLAN”。

2 Super VLAN 快速配置指南

2.1 简介

本案例介绍 Super VLAN 的配置方法。

2.2 组网需求

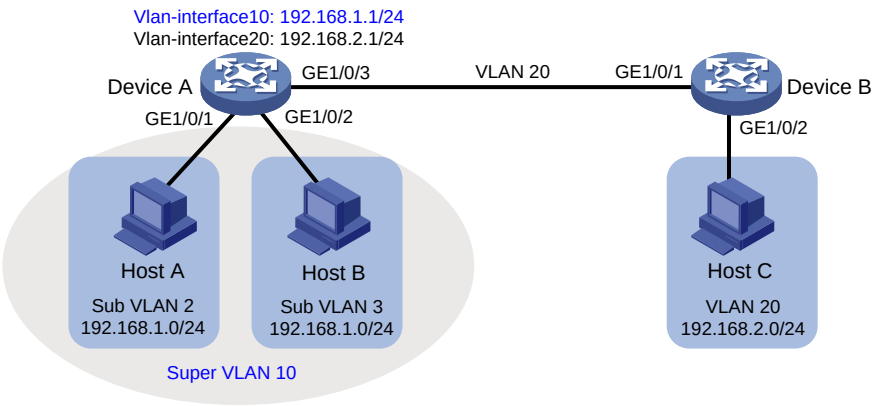
如图 2 所示：

- VLAN 2 中的用户通过 Device A 的 GigabitEthernet1/0/1 接入网络，VLAN 3 中的用户通过 Device A 的 GigabitEthernet1/0/2 接入网络。VLAN 2 中有 30 个用户，VLAN 3 中有 50 个用户。
- Device A 的 GigabitEthernet1/0/3 和 Device B 的 GigabitEthernet1/0/1 属于 VLAN 20。
- VLAN 20 中的终端用户都使用 192.168.2.0/24 网段的 IP 地址，使用 192.168.2.1 作为网关地址。

现要求通过配置 Super VLAN 功能实现以下应用需求：

- VLAN 2 和 VLAN 3 中的终端用户都使用 192.168.1.0/24 网段的 IP 地址以节省 IP 地址资源，使用 192.168.1.1 作为网关地址。
- VLAN 2、VLAN 3、VLAN 20 中的终端用户二层隔离，三层互通。

图2 Super VLAN 组网图



2.3 配置注意事项

由于 Super VLAN 中不能包含物理端口，由此若某 VLAN 中已经包含物理端口，则该 VLAN 不能被配置为 Super VLAN。

2.4 配置步骤

1. Device A 的配置

创建 Super VLAN 10。

```
<DeviceA> system-view
```

```
[DeviceA] vlan 10
[DeviceA-vlan10] supervlan
[DeviceA-vlan10] quit
```

创建 VLAN 2 并将端口 GigabitEthernet1/0/1 加入 VLAN 2。

```
[DeviceA] vlan 2
[DeviceA-vlan2] port gigabitethernet 1/0/1
[DeviceA-vlan2] quit
```

创建 VLAN 3 并将端口 GigabitEthernet1/0/2 加入 VLAN 3。

```
[DeviceA] vlan 3
[DeviceA-vlan3] port gigabitethernet 1/0/2
[DeviceA-vlan3] quit
```

将 Super VLAN 10 和 Sub VLAN 2 和 Sub VLAN 3 关联。

```
[DeviceA] vlan 10
[DeviceA-vlan10] subvlan 2 3
[DeviceA-vlan10] quit
```

配置 Super VLAN 10 对应的 VLAN 接口的 IP 地址和本地代理 ARP 功能。

```
[DeviceA] interface vlan-interface 10
[DeviceA-Vlan-interface10] ip address 192.168.1.1 24
[DeviceA-Vlan-interface10] local-proxy-arp enable
[DeviceA-Vlan-interface10] quit
```

创建 VLAN 20。

```
[DeviceA] vlan 20
[DeviceA-vlan20] quit
```

将端口 GigabitEthernet1/0/3 配置为 Trunk 端口并允许 VLAN 20 通过，取消允许 VLAN 1 通过。

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port link-type trunk
[DeviceA-GigabitEthernet1/0/3] undo port trunk permit vlan 1
[DeviceA-GigabitEthernet1/0/3] port trunk permit vlan 20
[DeviceA-GigabitEthernet1/0/3] quit
```

配置 VLAN 20 对应的 VLAN 接口的 IP 地址。

```
[DeviceA] interface Vlan-interface 20
[DeviceA-Vlan-interface20] ip address 192.168.2.1 24
[DeviceA-Vlan-interface20] quit
```

保存配置

```
[DeviceA] save force
```

2. Device B 的配置

创建 VLAN 20。

```
[DeviceB] vlan 20
[DeviceB-vlan20] quit
```

将端口 GigabitEthernet1/0/1 配置为 Trunk 端口并允许 VLAN 20 通过，取消允许 VLAN 1 通过。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 20
```

```
[DeviceB-GigabitEthernet1/0/1] quit
```

将端口 GigabitEthernet1/0/2 加入 VLAN 20。

```
[DeviceB] vlan 20
[DeviceB-vlan20] port gigabitethernet 1/0/2
[DeviceB-vlan20] quit
```

保存配置

```
[DeviceB] save force
```

2.5 验证配置

显示 Device A 上 Super VLAN 的配置信息。

```
<DeviceA> display supervlan
 Super VLAN ID: 10
 Sub-VLAN ID: 2-3

 VLAN ID: 10
 VLAN type: Static
 It is a super VLAN.
 Route interface: Configured
 IPv4 address: 192.168.1.1
 IPv4 subnet mask: 255.255.255.0
 Description: VLAN 0010
 Name: VLAN 0010
 Tagged ports:   None
 Untagged ports: None

 VLAN ID: 2
 VLAN type: Static
 It is a sub-VLAN.
 Route interface: Configured
 IPv4 address: 192.168.1.1
 IPv4 subnet mask: 255.255.255.0
 Description: VLAN 0002
 Name: VLAN 0002
 Tagged ports:   None
 Untagged ports:
    GigabitEthernet1/0/1

 VLAN ID: 3
 VLAN type: Static
 It is a sub-VLAN.
 Route interface: Configured
 IPv4 address: 192.168.1.1
 IPv4 subnet mask: 255.255.255.0
 Description: VLAN 0003
 Name: VLAN 0003
 Tagged ports:   None
```

```
 Untagged ports:
GigabitEthernet1/0/2
```

显示 Device A 上 VLAN 20 的配置信息。

```
<DeviceA> display vlan 20
 VLAN ID: 20
 VLAN type: Static
 Route interface: Configured
 IPv4 address: 192.168.2.1
 IPv4 subnet mask: 255.255.255.0
 Description: VLAN 0020
 Name: VLAN 0020
 Tagged ports:
    GigabitEthernet1/0/3
 Untagged ports: None
```

显示 Device B 上 VLAN 20 的配置信息。

```
<DeviceA> display vlan 20
 VLAN ID: 20
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0020
 Name: VLAN 0020
 Tagged ports:
    GigabitEthernet1/0/1
 Untagged ports:
    GigabitEthernet1/0/2
```

2.6 配置文件

- Device A：

```
#
vlan 2
#
vlan 3
#
vlan 10
 supervlan
 subvlan 2 3
#
vlan 20
#
interface Vlan-interface10
 ip address 192.168.1.1 255.255.255.0
 local-proxy-arp enable
#
interface Vlan-interface20
 ip address 192.168.2.1 255.255.255.0
#
```

```
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 3
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 20
```

- #Device B：

```
#
vlan 20
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 20
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 20
#
```

2.7 相关资料

- 产品配套“二层技术-以太网交换配置指导”中的“VLAN”。
- 产品配套“二层技术-以太网交换命令参考”中的“VLAN”。

3 Voice VLAN 快速配置指南

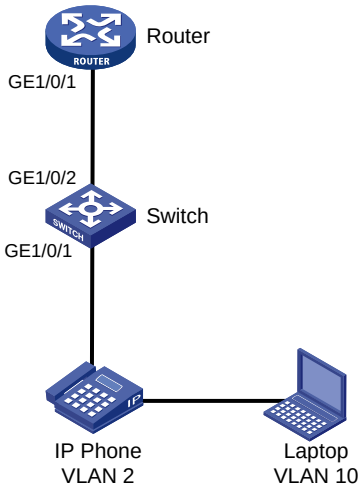
3.1 简介

本案例介绍 Voice VLAN 的配置方法。

3.2 组网需求

为了保障语音数据能够优先转发，需要将语音电话和 Laptop 地址区分开，将语音电话地址设置成 192.168.2.0 网段划分到 VLAN2，将 Laptop 地址设置成 192.168.10.0 网段划分到 VLAN10，路由器作为 DHCP 服务器给语音电话和 Laptop 下发 IP 地址。

图3 Voice VLAN 组网图



3.3 配置步骤

1. Swtich 的配置

开启 POE，为话机供电。

```
<Switch> system-view
[Switch] interface gigabitEthernet1/0/1
[Switch-GigabitEthernet1/0/1] poe enable
[Switch-GigabitEthernet1/0/1] quit
```

创建话机所属 VLAN2 以及 PC 所属 VLAN10

```
[Switch] vlan 2
[Switch-vlan2] quit
[Switch] vlan 10
[Switch-vlan10] quit
```

设置允许通过的 OUI 地址为 MAC 地址前缀为 6ca8-4900-0000，即当报文的前缀为 6ca8-4900-0000 时，设备会把它当成语音报文来处理

```
[Switch] voice-vlan mac-address 6ca8-4900-0000 mask ffff-ff00-0000 description avaya
```

将端口 GigabitEthernet1/0/1 设定为 Hybrid 端口，开启端口 Voice VLAN 功能

```
[Switch] interface gigabitEthernet 1/0/1
[Switch-GigabitEthernet1/0/1] port link-type hybrid
[Switch-GigabitEthernet1/0/1] voice-vlan 2 enable
```

设置 PC 所属 vlan 为 vlan10

```
[Switch-GigabitEthernet1/0/1] port hybrid pvid vlan 10
[Switch-GigabitEthernet1/0/1] port hybrid vlan 10 untagged
[SWITCH-GigabitEthernet1/0/1] quit
```

#设备连接 dhcp 服务器的接口 GigabitEthernet 1/0/2，允许 VLAN2、LAN10 通过

```
[Switch] interface gigabitEthernet 1/0/2
[Switch-GigabitEthernet1/0/2] port link-type trunk
[Switch-GigabitEthernet1/0/2] port trunk permit vlan 2 10
[Switch-GigabitEthernet1/0/2] quit
```

保存配置

```
[Switch] save force
```

2. Router 的配置

创建 VLAN2、VLAN10 及其对应的 VLAN 接口，为该虚接口配置 IP 地址

```
<Router> system-view
[Router] vlan 2
[Router-vlan2] quit
[Router] vlan 10
[Router-vlan10] quit
[Router] interface Vlan-interface 2
[Router-Vlan-interface2] ip address 192.168.2.1 255.255.255.0
[Router-Vlan-interface2] quit
[Router] interface Vlan-interface 10
[Router-Vlan-interface10] ip address 192.168.10.1 255.255.255.0
[Router-Vlan-interface10] quit
```

设备连接交换机的接口 GigabitEthernet 1/0/1，允许 VLAN2、VLAN10 通过

```
[Router] interface GigabitEthernet 1/0/1
[Router-GigabitEthernet1/0/1] port link-type trunk
[Router-GigabitEthernet1/0/1] port trunk permit vlan 2 10
[Router-GigabitEthernet1/0/1] quit
```

开启 DHCP 服务。

```
[Router] dhcp enable
```

设置话机 VLAN2 的 DHCP 地址池

```
[Router] dhcp server ip-pool vlan2
[Router-dhcp-pool-vlan2] network 192.168.2.0 mask 255.255.255.0
[Router-dhcp-pool-vlan2] gateway-list 192.168.2.1
[Router-dhcp-pool-vlan2] quit
```

设置 Laptop VLAN10 的 DHCP 地址池

```
[Router] dhcp server ip-pool vlan10
[Router-dhcp-pool-vlan10] network 192.168.10.0 mask 255.255.255.0
[Router-dhcp-pool-vlan10] gateway-list 192.168.10.1
[Router-dhcp-pool-vlan10] dns-list 114.114.114.114
[Router-dhcp-pool-vlan10] quit
```

保存配置

```
[Router] save force
```

3.4 验证配置

交换机上查验证结果，查看话机是否加入到 VLAN2

```
<Switch> display mac-address
MAC Address VLAN ID STATE Port/Nickname AGING
3897-d630-676b 10 Learned GE1/0/2 Y
3897-d630-676b 2 Learned GE1/0/2 Y
6ca8-4986-6d59 2 Learned GE1/0/1 Y
0068-eb95-3683 10 Learned GE1/0/1 Y
```

查看 voice vlan 配置是否生效

```
<Switch> display voice-vlan mac-address
Oui Address Mask Description
0003-6b00-0000 ffff-ff00-0000 Cisco phone
00e0-7500-0000 ffff-ff00-0000 Polycom phone
6ca8-4900-0000 ffff-ff00-0000 avaya
```

默认 voice vlan 为 auto(自动模式)

```
<Switch> display voice-vlan state
Current Voice VLANs: 1
Voice VLAN security mode: Security
Voice VLAN aging time: 1440 minutes
Voice VLAN enabled port and its mode:
PORT VLAN MODE COS DSCP
------------------------------------------------------------------------
GE1/0/1 2 AUTO 6 46
```

DHCP 服务器上查看话机和 PC 获取 IP 地址

```
%Sep 1 09:19:59:333 2021 DHCP DHCPS/5/DHCPS_ALLOCATE_IP: DHCP server information: Server IP
= 192.168.2.1, DHCP client IP = 192.168.2.2, DHCP client hardware address = 6ca8-4986-6d59,
DHCP client lease = 86400.
<Router> display dhcp server ip-in-use all
Pool utilization: 0.59%
IP address Client-identifier/ Lease expiration Type
Hardware address
192.168.2.2 6ca8-4986-6d59 Aug 31 2021 09:19:59 Auto:COMMITTED
192.168.10.4 0068-eb95-3683 Aug 31 2021 09:19:42 Auto:COMMITTED
```

3.5 配置文件

- Switch：

```
#
 voice-vlan mac-address 6ca8-4900-0000 mask ffff-ff00-0000 description avaya
#
vlan 2
#
vlan 10
```

```
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 port hybrid vlan 10 untagged
 port hybrid pvid vlan 10
 voice-vlan 2 enable
 poe enable
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 2 10
```

- Router：

```
#
vlan 2
#
vlan 10
#
dhcp server ip-pool vlan2
 gateway-list 192.168.2.1
 network 192.168.2.0 255.255.255.0
#
dhcp server ip-pool vlan10
 gateway-list 192.168.10.1
 network 192.168.10.0 255.255.255.0
 dns-list 114.114.114.114
#
interface Vlan-interface2
 ip address 192.168.2.1 255.255.255.0
#
interface Vlan-interface10
 ip address 192.168.10.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 2 10
```

3.6 相关资料

- 产品配套“二层技术-以太网交换配置指导”中的“VLAN”。
- 产品配套“二层技术-以太网交换命令参考”中的“VLAN”。

4 Private VLAN 快速配置指南

4.1 简介

本案例介绍 Private VLAN 的配置方法。

4.2 组网需求

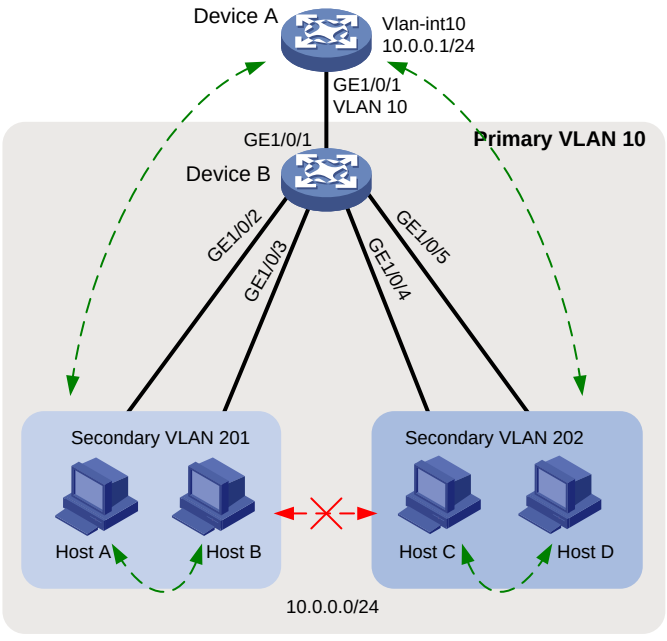
如图 4 所示：

- 汇聚层设备 Device A 为接入设备 Device B 分配了 VLAN 10，网关接口 VLAN-interface10 可以和所有用户互通，以便用户可以通过 Device A 来访问外部网络。Device B 连接的所有用户均处于同一网段 10.0.0.0/24。
- Host A 和 B 属于销售部，Host C 和 D 属于财务部。为保证安全，需要使不同部门之间二层隔离，同部门的用户之间则可以互通。

现由于 Device A 不能为 Device B 分配更多 VLAN，要求通过 Private VLAN 功能实现：

- Device A 只需识别 VLAN 10。
- Device B 在 Primary VLAN 10 下为各部门配置不同的 Secondary VLAN，使部门间二层隔离。

图4 Private VLAN 典型配置举例组网图



4.3 配置注意事项

- Private VLAN 功能只需要在接入设备 Device B 上配置。
- 系统缺省 VLAN（VLAN 1）不支持 Private VLAN 相关配置。

4.4 配置步骤

1. Dvice B 的配置

配置 VLAN 10 为 Primary VLAN。

```
<DeviceB> system-view
[DeviceB] vlan 10
[DeviceB-vlan10] private-vlan primary
[DeviceB-vlan10] quit
```

创建 Secondary VLAN 201、202。

```
[DeviceB] vlan 201 to 202
```

建立 Primary VLAN 10 和 Secondary VLAN 201、202 的映射关系。

```
[DeviceB] vlan 10
[DeviceB-vlan10] private-vlan secondary 201 to 202
[DeviceB-vlan10] quit
```

配置上行端口 GigabitEthernet1/0/1 在 VLAN 10 中工作在 promiscuous 模式。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port private-vlan 10 promiscuous
[DeviceB-GigabitEthernet1/0/1] quit
```

将下行端口 GigabitEthernet1/0/2、GigabitEthernet1/0/3 添加到 VLAN 201，GigabitEthernet1/0/4、GigabitEthernet1/0/5 添加到 VLAN 202，并配置它们工作在 host 模式。

```
[DeviceB] interface range gigabitethernet 1/0/2 to gigabitethernet 1/0/3
[DeviceB-if-range] port access vlan 201
[DeviceB-if-range] port private-vlan host
[DeviceB-if-range] quit
[DeviceB] interface range gigabitethernet 1/0/4 to gigabitethernet 1/0/5
[DeviceB-if-range] port access vlan 202
[DeviceB-if-range] port private-vlan host
[DeviceB-if-range] quit
```

保存配置

```
[DeviceB] save force
```

2. Dvice A 的配置

创建 VLAN 10。将接口 GigabitEthernet1/0/1 加入 VLAN 10。

```
<DeviceA> system-view
[DeviceA] vlan 10
[DeviceA-vlan10] quit
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port access vlan 10
[DeviceA-GigabitEthernet1/0/1] quit
```

配置网关接口 VLAN-interface10。

```
[DeviceA] interface vlan-interface 10
[DeviceA-Vlan-interface10] ip address 10.0.0.1 24
[DeviceA-Vlan-interface10] quit
```

保存配置

```
[DeviceA] save force
```

4.5 验证配置

Device A 可以 ping 通任意用户。查看 ARP 表，可以看到所有用户均属于 VLAN 10。

```
[DeviceA] display arp
  Type: S-Static   D-Dynamic   O-Openflow   R-Rule   M-Multiport  I-Invalid
IP address      MAC address    VLAN/VSI name Interface               Aging Type
10.0.0.2        0e9e-0671-0302 10            GE1/0/1                 1062  D
10.0.0.3        0e9e-09f7-0402 10            GE1/0/1                 1052  D
10.0.0.4        0e9e-0d94-0502 10            GE1/0/1                 1164  D
10.0.0.5        0e9e-1263-0602 10            GE1/0/1                 1109  D
```

显示 Device B 上的 Private VLAN 配置情况。

```
<DeviceB> display private-vlan
 Primary VLAN ID: 10
 Secondary VLAN ID: 201-202

 VLAN ID: 10
 VLAN type: Static
 Private VLAN type: Primary
 Route interface: Not configured
 Description: VLAN 0010
 Name: VLAN 0010
 Tagged ports:
    None
 Untagged ports:
    GigabitEthernet1/0/1(U)           GigabitEthernet1/0/2(U)
    GigabitEthernet1/0/3(U)           GigabitEthernet1/0/4(U)
    GigabitEthernet1/0/5(U)

 VLAN ID: 201
 VLAN type: Static
 Private VLAN type: Secondary
 Route interface: Not configured
 Description: VLAN 0201
 Name: VLAN 0201
 Tagged ports:
    None
 Untagged ports:
    GigabitEthernet1/0/1(U)           GigabitEthernet1/0/2(U)
    GigabitEthernet1/0/3(U)

 VLAN ID: 202
 VLAN type: Static
 Private VLAN type: Secondary
 Route interface: Not configured
 Description: VLAN 0202
 Name: VLAN 0202
 Tagged ports:
```

```
    None
 Untagged ports:
    GigabitEthernet1/0/1(U)            GigabitEthernet1/0/4(U)
    GigabitEthernet1/0/5(U)
```

可以看到，工作在 promiscuous 模式的端口 GigabitEthernet1/0/1 和工作在 host 模式的端口 GigabitEthernet1/0/2～GigabitEthernet1/0/5 均以 Untagged 方式允许 VLAN 报文通过。

Host A、B 之间可以互相 ping 通，Host C、D 之间可以互相 ping 通。Host A、B 与 Host C、D 之间均不能 ping 通。

4.6 配置文件

- Device A：

```
#
vlan 10
#
interface Vlan-interface10
 ip address 10.0.0.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 10
#
```

- Device B：

```
#
vlan 10
 private-vlan primary
 private-vlan secondary 201 to 202
#
vlan 201 to 202
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 10 201 to 202 untagged
 port hybrid pvid vlan 10
 port private-vlan 10 promiscuous
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 10 201 untagged
 port hybrid pvid vlan 201
 port private-vlan host
#
interface GigabitEthernet1/0/3
```

```
 port link-mode bridge
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 10 201 untagged
 port hybrid pvid vlan 201
 port private-vlan host
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 10 202 untagged
 port hybrid pvid vlan 202
 port private-vlan host
#
interface GigabitEthernet1/0/5
 port link-mode bridge
 port link-type hybrid
 undo port hybrid vlan 1
 port hybrid vlan 10 202 untagged
 port hybrid pvid vlan 202
 port private-vlan host
#
```

4.7 相关资料

- 产品配套“二层技术-以太网交换配置指导”中的“VLAN”。
- 产品配套“二层技术-以太网交换命令参考”中的“VLAN”。

端口隔离快速配置指南

目 录

1 端口隔离快速配置指南

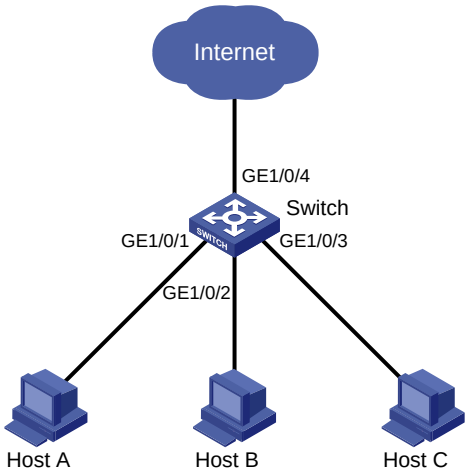
1.1 简介

本案例介绍端口隔离的配置方法。

1.2 组网需求

如图 1 所示，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，Switch 设备通过 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 配置端口隔离组网图



1.3 配置注意事项

- 在设备上将端口加入到指定的隔离组中前，必须先完成该隔离组的创建。
- 一个端口最多只能加入一个隔离组。

1.4 配置步骤

注意

单隔离组设备，只支持一个隔离组，由系统自动创建隔离组 1，用户不可删除该隔离组或创建其他的隔离组。多隔离组设备，支持多个隔离组，用户可以手工配置。

创建隔离组 1。

```
<Switch> system-view
```

```
[Switch] port-isolate group 1
```

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

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] port-isolate enable group 1
[Switch-GigabitEthernet1/0/1] quit
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] port-isolate enable group 1
[Switch-GigabitEthernet1/0/2] quit
[Switch] interface gigabitethernet 1/0/3
[Switch-GigabitEthernet1/0/3] port-isolate enable group 1
[Switch-GigabitEthernet1/0/3] quit
```

保存配置。

```
[Switch] save force
```

1.5 验证配置

显示隔离组 1 中的信息。

```
[Switch] display port-isolate group 1
 Port isolation group information:
 Group ID: 1
 Group members:
    GigabitEthernet1/0/1
    GigabitEthernet1/0/2
    GigabitEthernet1/0/3
```

以上信息显示 Device 上的端口 GigabitEthernet1/0/1、GigabitEthernet1/0/2、GigabitEthernetE1/0/3 已经加入隔离组 1，从而实现二层隔离，Host A、Host B 和 Host C 彼此之间不能 ping 通。

1.6 配置文件

```
#
 port-isolate group 1
#
interface GigabitEthernet1/0/1
port link-mode bridge
port-isolate enable group 1
#
interface GigabitEthernet1/0/2
port link-mode bridge
port-isolate enable group 1
#
interface GigabitEthernet1/0/3
port link-mode bridge
port-isolate enable group 1
#
```

1.7 相关资料

- 产品配套“二层技术-以太网交换配置指导”中的“端口隔离配置”。
- 产品配套“二层技术-以太网交换命令参考”中的“端口隔离命令”。

环路检测快速配置指南

目 录

1 环路检测快速配置指南

1.1 简介

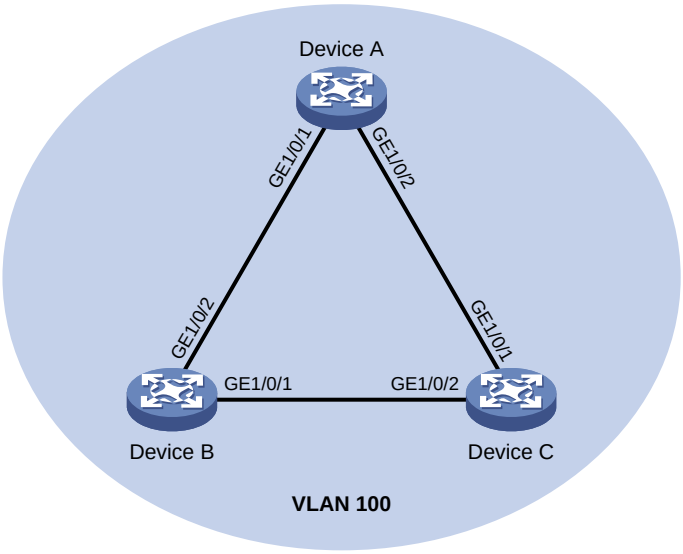
本案例介绍环路检测的配置方法。

1.2 组网需求

如图 1 所示，

- 三台设备 Device A、Device B 和 Device C 组成一个物理上的环形网络。
- 通过在 Device A 上配置环路检测功能，使系统能够自动关闭 Device A 上出现环路的端口，并通过打印日志信息来通知用户检查网络。

图1 环路检测基本功能配置组网图



1.3 配置步骤

1. Device A 的配置

创建 VLAN 100，并全局开启该 VLAN 内的环路检测功能。

```
<DeviceA> system-view
[DeviceA] vlan 100
[DeviceA-vlan100] quit
[DeviceA] loopback-detection global enable vlan 100
```

配置端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 为 Trunk 类型，并允许 VLAN 100 通过。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 100
[DeviceA-GigabitEthernet1/0/1] quit
```

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-type trunk
[DeviceA-GigabitEthernet1/0/2] port trunk permit vlan 100
[DeviceA-GigabitEthernet1/0/2] quit
```

全局配置环路检测的处理模式为 Shutdown 模式。

```
[DeviceA] loopback-detection global action shutdown
```

配置环路检测的时间间隔为 35 秒。

```
[DeviceA] loopback-detection interval-time 35
```

保存配置。

```
[DeviceA] save force
```

2. Device B 的配置

创建 VLAN 100。

```
<DeviceB> system-view
[DeviceB] vlan 100
[DeviceB–vlan100] quit
```

配置端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 为 Trunk 类型，并允许 VLAN 100 通过。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 100
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 100
[DeviceB-GigabitEthernet1/0/2] quit
```

保存配置。

```
[DeviceB] save force
```

3. Device C 的配置

创建 VLAN 100。

```
<DeviceC> system-view
[DeviceC] vlan 100
[DeviceC–vlan100] quit
```

配置端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 为 Trunk 类型，并允许 VLAN 100 通过。

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] port link-type trunk
[DeviceC-GigabitEthernet1/0/1] port trunk permit vlan 100
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] port link-type trunk
[DeviceC-GigabitEthernet1/0/2] port trunk permit vlan 100
[DeviceC-GigabitEthernet1/0/2] quit
```

保存配置。

```
[DeviceC] save force
```

1.4 验证配置

当配置完成后，系统在一个环路检测时间间隔内在 Device A 的端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 上都检测到了环路，于是将这两个端口自动关闭，并打印了如下日志信息：

```
<DeviceA> %Aug 26 19:17:29:760 2021 DeviceA IFNET/3/PHY_UPDOWN: -MDC=1; Physical state on the interface GigabitEthernet1/0/2 changed to up.
%Aug 26 19:17:29:760 2021 DeviceA IFNET/5/LINK_UPDOWN: -MDC=1; Line protocol state on the interface GigabitEthernet1/0/2 changed to up.
%Aug 26 19:17:30:356 2021 DeviceA IFNET/3/PHY_UPDOWN: -MDC=1; Physical state on the interface GigabitEthernet1/0/1 changed to up.
%Aug 26 19:17:30:356 2021 DeviceA IFNET/5/LINK_UPDOWN: -MDC=1; Line protocol state on the interface GigabitEthernet1/0/1 changed to up.
%Aug 26 19:17:33:985 2021 DeviceA LPDT/4/LPDT_LOOPED: -MDC=1; A loop was detected on GigabitEthernet1/0/1.
%Aug 26 19:17:34:005 2021 DeviceA IFNET/3/PHY_UPDOWN: -MDC=1; Physical state on the interface GigabitEthernet1/0/1 changed to down.
%Aug 26 19:17:34:006 2021 DeviceA IFNET/5/LINK_UPDOWN: -MDC=1; Line protocol state on the interface GigabitEthernet1/0/1 changed to down.
%Aug 26 19:17:34:018 2021 DeviceA LPDT/4/LPDT_VLAN_LOOPED: -MDC=1; A loop was detected on GigabitEthernet1/0/1 in VLAN 100.
%Aug 26 19:17:34:019 2021 DeviceA LPDT/4/LPDT_LOOPED: -MDC=1; A loop was detected on GigabitEthernet1/0/2.
%Aug 26 19:17:34:040 2021 DeviceA IFNET/3/PHY_UPDOWN: -MDC=1; Physical state on the interface GigabitEthernet1/0/2 changed to down.
%Aug 26 19:17:34:041 2021 DeviceA IFNET/5/LINK_UPDOWN: -MDC=1; Line protocol state on the interface GigabitEthernet1/0/2 changed to down.
%Aug 26 19:17:34:055 2021 DeviceA LPDT/4/LPDT_VLAN_LOOPED: -MDC=1; A loop was detected on GigabitEthernet1/0/2 in VLAN 100.
%Aug 26 19:17:34:055 2021 DeviceA LPDT/5/LPDT_VLAN_RECOVERED: -MDC=1; A loop was removed on GigabitEthernet1/0/1 in VLAN 100.
%Aug 26 19:17:34:055 2021 DeviceA LPDT/5/LPDT_RECOVERED: -MDC=1; All loops were removed on GigabitEthernet1/0/1.
%Aug 26 19:17:34:056 2021 DeviceA LPDT/5/LPDT_VLAN_RECOVERED: -MDC=1; A loop was removed on GigabitEthernet1/0/2 in VLAN 100.
%Aug 26 19:17:34:056 2021 DeviceA LPDT/5/LPDT_RECOVERED: -MDC=1; All loops were removed on GigabitEthernet1/0/2.
```

使用 **display loopback-detection** 命令可以查看 Device A 上环路检测的配置和运行情况：

显示 Device A 上环路检测的配置和运行情况。

```
<DeviceA> display loopback-detection
Loop detection is enabled.
Global loop detection interval is 35 second(s).
Loop is detected on following interfaces:
  Interface                     Action mode     VLANs/VSI
  GigabitEthernet1/0/1          Shutdown        100
  GigabitEthernet1/0/2          Shutdown        100
```

由此可见，Device A 上显示在端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 上检测到环路，由于环路检测功能运行在 Shutdown 模式下，端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 上出现环路后均已被自动关闭，因此设备打印的日志信息显示这两个端口上的环路已消除。此时，使

用 **display interface** 命令分别查看 Device A 上端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 的状态信息：

```
<DeviceA> display interface gigabitEthernet 1/0/1
GigabitEthernet1/0/1
Current state: DOWN (Loopback detection down)
<DeviceA>display interface gigabitEthernet 1/0/2
GigabitEthernet1/0/2
Current state: DOWN (Loopback detection down)
```

由此可见，端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 均已被环路检测模块自动关闭。

1.5 配置文件

- Device A：

```
#

 loopback-detection global enable vlan 100
 loopback-detection global action shutdown
 loopback-detection interval-time 35
#
vlan 100
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100
#
```

- Device B：

```
#
vlan 100
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100
#
```

- Device C：

```
#
```

```
vlan 100
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100
#
```

1.6 相关资料

- 产品配套“二层技术-以太网交换配置指导”中的“环路检测”。
- 产品配套“二层技术-以太网交换命令参考”中的“环路检测”。

QinQ 快速配置指南

目 录

1 配置 QinQ 基本组网

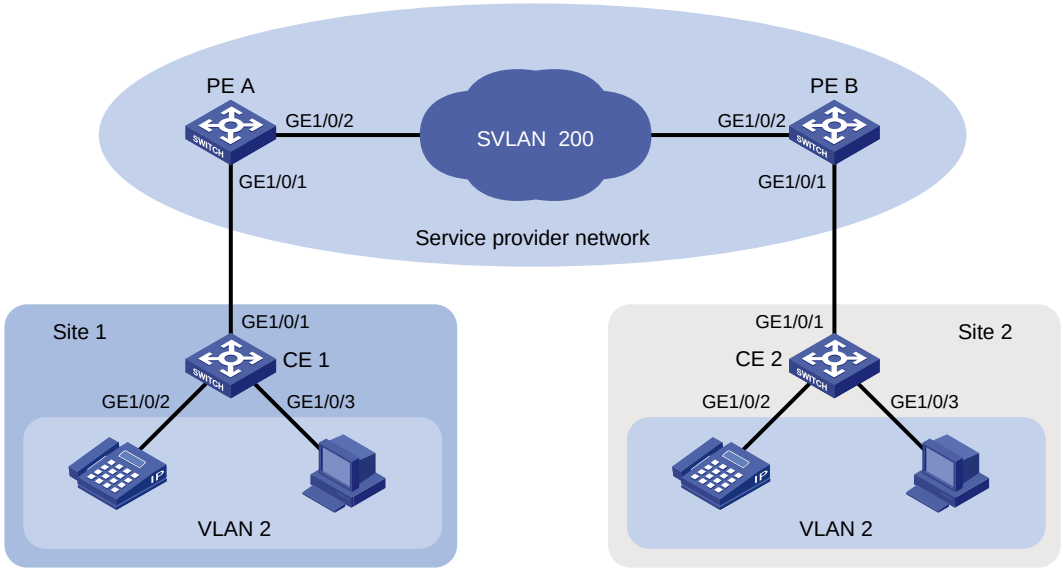
1.1 简介

本案例介绍 QinQ 的配置方法。

1.2 组网需求

如图 1-1 所示，CE 1 和 CE 2 是同一公司两个分支机构的接入交换机，PE A 和 PE B 是运营商网络的边缘设备，通过运营商网络进行通信，公司内业务使用的 VLAN 为 VLAN 2，运营商网络中可用的 VLAN 资源为 VLAN 200。通过配置 QinQ 功能，实现两个分支机构之间通过运营商网络进行通信。

图1-1 QinQ 基本组网图



1.3 配置注意事项

开启 QinQ 功能的端口，需要配置端口的缺省 VLAN 为 QinQ 封装的外层 VLAN（SVLAN）。

1.4 配置步骤

1.4.1 CE 1 的配置

创建 VLAN 2。

```
<CE 1> system-view
[CE 1] vlan 2
[CE 1-vlan2] quit
```

配置端口 GigabitEthernet 1/0/2 和 GigabitEthernet 1/0/3 为 Access 端口，允许 VLAN 2 的报文通过。

```
[CE 1] interface range gigabitethernet 1/0/2 to gigabitethernet 1/0/3
[CE 1-if-range] port access vlan 2
[CE 1-if-range] quit
```

配置端口 GigabitEthernet 1/0/1 为 Trunk 端口，允许 VLAN 2 的报文通过。

```
[CE 1] interface gigabitethernet 1/0/1
[CE 1-GigabitEthernet1/0/1] port link-type trunk
[CE 1-GigabitEthernet1/0/1] port trunk permit vlan 2
[CE 1-GigabitEthernet1/0/1] quit
```

1.4.2 CE 2 的配置

CE 2 的配置与 CE 1 相同，此处不做赘述。

1.4.3 PE A 的配置

创建 VLAN 2 和 VLAN 200。

```
<PE A> system-view
[PE A] vlan 2
[PE A-vlan2] quit
[PE A] vlan 200
[PE A-vlan200] quit
```

配置端口 GigabitEthernet 1/0/1 为 Trunk 端口，允许 VLAN 2 和 VLAN 200 的报文通过。

```
[PE A] interface gigabitethernet 1/0/1
[PE A-GigabitEthernet1/0/1] port link-type trunk
[PE A-GigabitEthernet1/0/1] port trunk permit vlan 2 200
```

配置端口 GigabitEthernet 1/0/1 的 PVID 为 VLAN 200。

```
[PE A-GigabitEthernet1/0/1] port trunk pvid vlan 200
```

开启端口 GigabitEthernet 1/0/1 的 QinQ 功能。

```
[PE A-GigabitEthernet1/0/1] qinq enable
[PE A-GigabitEthernet1/0/1] quit
```

配置端口 GigabitEthernet 1/0/2 为 Trunk 端口，允许 VLAN 200 的报文通过。

```
[PE A] interface gigabitethernet 1/0/2
[PE A-GigabitEthernet1/0/2] port link-type trunk
[PE A-GigabitEthernet1/0/2] port trunk permit vlan 200
[PE A-GigabitEthernet1/0/2] quit
```

1.4.4 PE B 的配置

PE B 的配置与 PE A 相同，此处不做赘述。

1.5 验证配置

同一公司中，分别属于两个分支机构的两台 PC 互相进行 Ping 操作，可以 Ping 通，且这两台 PC 能够互相学习到对方的 MAC 地址。可见业务 VLAN 信息能够跨越运营商网络进行透明传输。例如：

在 Site 1 分支的 PC 执行 Ping 操作，检查 Site 2 分支的 PC 是否可达。

```
C:\Users\usera>ping 192.168.1.2

正在 Ping 192.168.1.2 具有 32 字节的数据:
来自 192.168.1.2 的回复: 字节=32 时间=28ms TTL=253
来自 192.168.1.2 的回复: 字节=32 时间=27ms TTL=253
来自 192.168.1.2 的回复: 字节=32 时间=27ms TTL=253
来自 192.168.1.2 的回复: 字节=32 时间=26ms TTL=253

192.168.1.2 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 = 26ms，最长 = 28ms，平均 = 27ms
```

在 CE 1 上查看 MAC 地址表，发现学习到了 Site 2 分支设备的 MAC 地址。

```
<Sysname> display mac-address vlan 2
MAC Address      VLAN ID    State           Port/Nickname           Aging
0003-2d00-5761   2          Learned         GE1/0/1                 Y
```

1.6 配置文件

- CE 1

```
#
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
#
interface GigabitEthernet1/0/3
 port access vlan 2
```

- CE 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
#
interface GigabitEthernet1/0/3
 port access vlan 2
```

- PE A

```
#
vlan 2
#
Vlan 200
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 to 2 200
 port trunk pvid vlan 200
 qinq enable
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 200
```

- PE B

```
#
vlan 2
#
Vlan 200
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan 1 to 2 200
 port trunk pvid vlan 200
 qinq enable
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk permit vlan 1 200
#
```

1.7 相关资料

- 产品配套“二层技术-以太网交换配置指导”中的“QinQ”。
- 产品配套“二层技术-以太网交换命令参考”中的“QinQ”。

MAC 地址表快速配置指南

目 录

1 配置静态 MAC 地址表项

1.1 简介

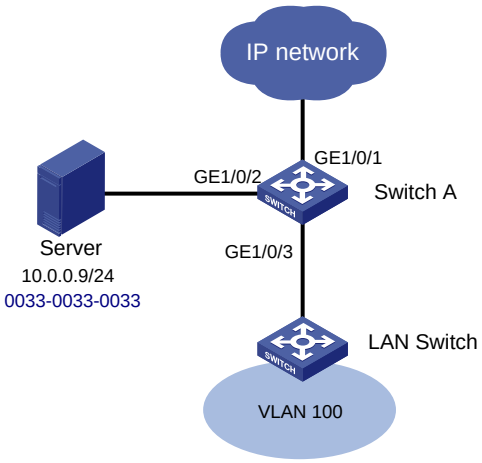
本案例介绍静态 MAC 地址表项的配置方法。

1.2 组网需求

某个企业网络如图 1 所示，企业网络内的用户通过 Switch A 与服务器或外部网络进行通信。该网络的组网需求如下：

- VLAN 100 的用户群需要访问服务器。
- 如果有非法用户从其他接口假冒服务器的 MAC 地址发送报文，则服务器的 MAC 地址将在其他接口学到，导致用户不能与服务器正常通信，还会导致一些重要用户信息被窃取。为提高服务器安全性，在 Switch A 上配置一条静态 MAC 地址表项，将服务器 MAC 地址 0033-0033-0033 与接口 GE1/0/2 绑定。

图1 静态 MAC 地址表项组网图



1.3 配置步骤

对 Switch A 进行配置：

创建 VLAN 100。

```
<Switch A> system-view
[Switch A] vlan 100
[Switch A-vlan100] quit
```

将 GigabitEthernet1/0/2 加入 VLAN 100。

```
[Switch A] interface gigabitethernet 1/0/2
[Switch A-GigabitEthernet1/0/2] port access vlan 100
[Switch A-GigabitEthernet1/0/2] quit
```

将 Switch A 连接下级交换机的端口 GigabitEthernet1/0/3 的链路类型配置为 Trunk，并允许 VLAN 100 的报文通过。

```
[Switch A] interface gigabitethernet 1/0/3
[Switch A-GigabitEthernet1/0/3] port link-type trunk
[Switch A-GigabitEthernet1/0/3] port trunk permit vlan 100
[Switch A-GigabitEthernet1/0/3] quit
```

增加一个静态 MAC 地址表项，目的地址为 0033-0033-0033，出接口为 GigabitEthernet1/0/2，且该接口属于 VLAN 100。

```
[Switch A] mac-address static 0033-0033-0033 interface gigabitethernet 1/0/2 vlan 100
```

1.4 验证配置

(1) 假设 VLAN 100 的某个用户处于 10.0.0.0/24 网段，该用户能够和 Server 互通。

VLAN 100 的某个用户执行 Ping 操作，检查 10.0.0.9 是否可达。

```
<Switch A> ping 10.0.0.9
Ping 10.0.0.9 (10.0.0.9): 56 data bytes, press CTRL+C to break
56 bytes from 10.0.0.9: icmp_seq=0 ttl=254 time=2.137 ms
56 bytes from 10.0.0.9: icmp_seq=1 ttl=254 time=2.051 ms
56 bytes from 10.0.0.9: icmp_seq=2 ttl=254 time=1.996 ms
56 bytes from 10.0.0.9: icmp_seq=3 ttl=254 time=1.963 ms
56 bytes from 10.0.0.9: icmp_seq=4 ttl=254 time=1.991 ms

--- Ping statistics for 10.0.0.9 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.963/2.028/2.137/0.062 ms
```

(2) 查看 Switch A 的 MAC 地址表项信息，验证配置是否成功。

```
[Switch A] display mac-address
MAC Address      VLAN ID    State           Port/NickName           Aging
0033-0033-0033   100        Static          GE1/0/2                 N
```

1.5 配置文件

```
#
vlan 100
#
interface GigabitEthernet1/0/2
 port access vlan 100
 mac-address static 0033-0033-0033 vlan 100
#
interface GigabitEthernet1/0/3
 port link-type trunk
 port trunk permit vlan 1 100
#
```

1.6 相关资料

- 产品配套“二层技术-以太网交换配置指导”中的“MAC 地址表”。
- 产品配套“二层技术-以太网交换命令参考”中的“MAC 地址表”。

2 配置 VLAN 的 MAC 地址数学习上限

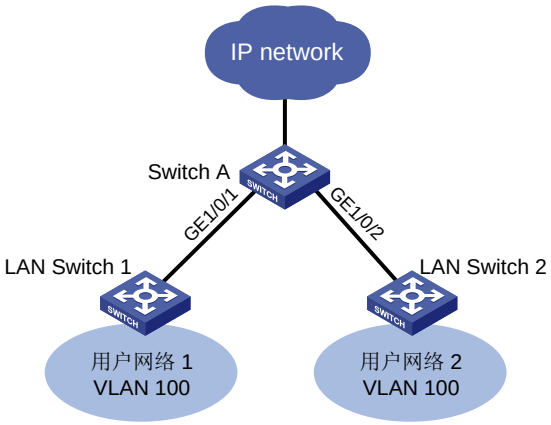
2.1 简介

本案例介绍 VLAN 的 MAC 地址数学习上限的配置方法。

2.2 组网需求

如图 2 所示，用户网络 1 和用户网络 2 均使用 VLAN 100，通过 Switch A 与外部网络进行通信。如果 MAC 地址表过于庞大，可能导致 Switch A 的转发性能下降。为保证 Switch A 的转发性能，在 Switch A 上配置 VLAN 100 的 MAC 地址数学习上限为 1024。

图2 VLAN 的 MAC 地址数学习上限组网图



2.3 配置步骤

对 Switch A 进行配置：

创建 VLAN 100。

```
<Switch A> system-view
[Switch A] vlan 100
[Switch A-vlan100] quit
```

将 GigabitEthernet1/0/1 的链路类型配置为 Trunk，并允许 VLAN 100 的报文通过。

```
[Switch A] interface gigabitethernet 1/0/1
[Switch A-GigabitEthernet1/0/1] port link-type trunk
[Switch A-GigabitEthernet1/0/1] port trunk permit vlan 100
[Switch A-GigabitEthernet1/0/1] quit
```

将 GigabitEthernet1/0/2 的链路类型配置为 Trunk，并允许 VLAN 100 的报文通过。

```
[Switch A] interface gigabitethernet 1/0/2
[Switch A-GigabitEthernet1/0/2] port link-type trunk
[Switch A-GigabitEthernet1/0/2] port trunk permit vlan 100
[Switch A-GigabitEthernet1/0/2] quit
```

配置 VLAN 100 的 MAC 地址数学习上限为 1024。

```
[Switch A] vlan 100
[Switch A-vlan100] mac-address max-mac-count 1024
[Switch A-vlan100] quit
```

2.4 验证配置

在 VLAN 100 视图下执行 **display this** 命令查看配置是否生效。

```
[Switch A] vlan 100
[Switch A-vlan100] display this
#
mac-address max-mac-count 1024
#
Return
```

2.5 配置文件

```
#
vlan 100
 mac-address max-mac-count 1024
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100
#
```

2.6 相关资料

- 产品配套“二层技术-以太网交换配置指导”中的“MAC 地址表”。
- 产品配套“二层技术-以太网交换命令参考”中的“MAC 地址表”。

3 配置接口的 MAC 地址数学习上限

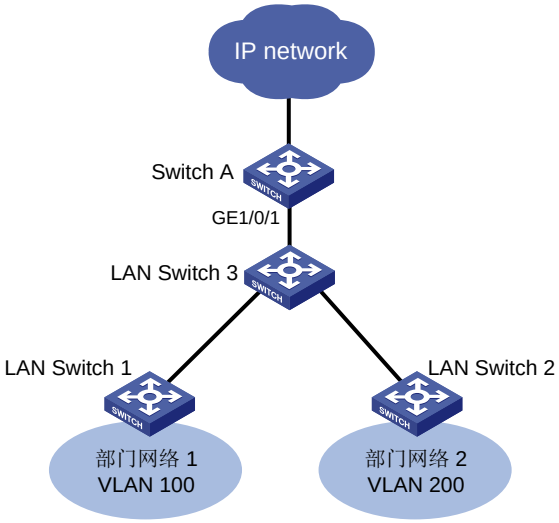
3.1 简介

本案例介绍端口的 MAC 地址数学习上限的配置方法。

3.2 组网需求

如图 3 所示，Switch A 是运营商网络的边缘设备，LAN Switch 3 是公司的接入交换机，LAN Switch 1 和 LAN Switch 2 是该公司内两个部门的接入交换机（部门网络 1 使用 VLAN 100，部门网络 2 使用 VLAN 200）。公司网络通过 LAN Switch 3 与 Switch A 相连访问外部网络。如果 MAC 地址表过于庞大，可能导致 Switch A 的转发性能下降。为保证 Switch A 的转发性能，在 Switch A 上配置端口 GE1/0/1 的 MAC 地址数学习上限为 2048。

图3 接口的 MAC 地址数学习上限组网图



3.3 配置步骤

对 Switch A 进行配置：

创建 VLAN 100、200。

```
<Switch A> system-view
[Switch A] vlan 100 200
```

将 GigabitEthernet1/0/1 的链路类型配置为 Trunk，并允许 VLAN 100、200 的报文通过。

```
[Switch A] interface gigabitethernet 1/0/1
[Switch A-GigabitEthernet1/0/1] port link-type trunk
[Switch A-GigabitEthernet1/0/1] port trunk permit vlan 100 200
[Switch A-GigabitEthernet1/0/1] quit
```

配置 VLAN 100 的 MAC 地址数学习上限为 1024。

```
[Switch A] interface gigabitethernet 1/0/1
[Switch A-GigabitEthernet1/0/1]mac-address max-mac-count 1024
```

```
[Switch A-GigabitEthernet1/0/1] quit
```

3.4 验证配置

在 VLAN 100 视图下执行 **display this** 命令查看配置是否生效。

```
[Switch A] interface gigabitethernet 1/0/1
[Switch A-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100 200
 mac-address max-mac-count 1024
#
return
```

3.5 配置文件

```
#
vlan 100
#
vlan 200
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 100 200
 mac-address max-mac-count 1024
#
```

3.6 相关资料

- 产品配套“二层技术-以太网交换配置指导”中的“MAC 地址表”。
- 产品配套“二层技术-以太网交换命令参考”中的“MAC 地址表”。

以太网链路聚合快速配置指南

目 录

1 配置二层链路聚合

1.1 简介

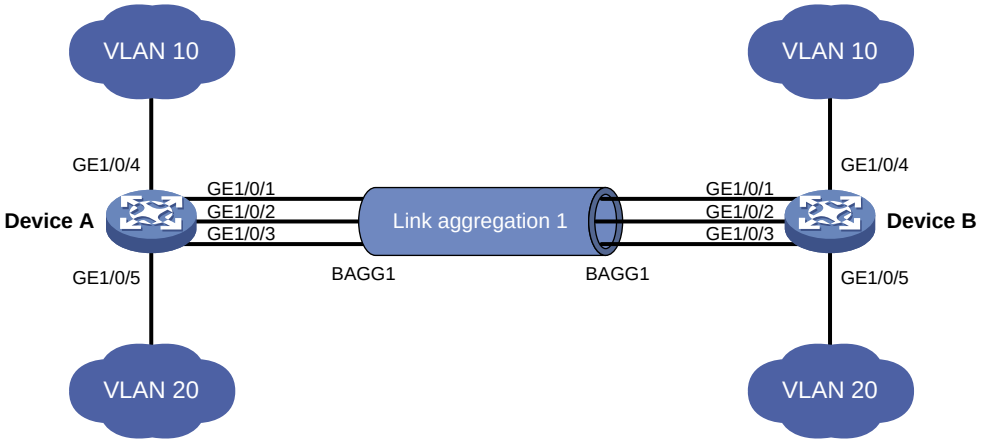
本案例介绍二层链路聚合的配置方法。

1.2 组网需求

如图 1 所示：

- Device A 与 Device B 通过各自的二层以太网接口 GigabitEthernet1/0/1～GigabitEthernet1/0/3 相互连接。
- Device A 和 DeviceB 均参与 VLAN 10、VLAN 20 的数据流量转发。现要求两设备上相同 VLAN 可以互通。为提高设备间链路带宽及可靠性，可使用二层链路聚合特性实现。

图1 二层链路聚合配置示例图



1.3 配置注意事项

- 配置聚合组的成员端口过程中，建议配置顺序：在端口视图下使用 **display this** 命令查看端口上是否存在属性类配置（包括端口隔离配置、QinQ 配置、VLAN 配置、VLAN 映射），如果有这类配置，请使用对应的 **undo** 命令删除这些配置，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。

1.4 配置步骤

1. Device A 的配置

进入系统视图，创建 VLAN 10，并将端口 GigabitEthernet1/0/4 加入到该 VLAN 10 中。

```
<DeviceA> system-view
[DeviceA] vlan 10
[DeviceA-vlan10] port gigabitethernet 1/0/4
[DeviceA-vlan10] quit
```

创建 VLAN 20，并将端口 GigabitEthernet1/0/5 加入到该 VLAN 20 中。

```
[DeviceA] vlan 20
[DeviceA-vlan20] port gigabitethernet 1/0/5
[DeviceA-vlan20] quit
```

创建二层聚合接口 1。（根据具体情况选择下面两种方式之一）

- 采用静态聚合模式：创建二层聚合接口 1

```
[DeviceA] interface bridge-aggregation 1
[DeviceA-Bridge-Aggregation1] quit
```

- 采用动态聚合模式：创建二层聚合接口 1，并配置动态聚合模式

```
[DeviceA] interface bridge-aggregation 1
[DeviceA-Bridge-Aggregation1] link-aggregation mode dynamic
[DeviceA-Bridge-Aggregation1] undo shutdown
[DeviceA-Bridge-Aggregation1] quit
```

将端口 GigabitEthernet1/0/1～GigabitEthernet1/0/3 加入到聚合组 1 中。

```
[DeviceA] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/3
[DeviceA-if-range] port link-aggregation group 1
[DeviceA-if-range] undo shutdown
[DeviceA-if-range] quit
```

配置二层聚合接口 1 为 Trunk 端口，并允许 VLAN 10 和 VLAN 20 的报文通过。

```
[DeviceA] interface bridge-aggregation 1
[DeviceA-Bridge-Aggregation1] port link-type trunk
Configuring GigabitEthernet1/0/1 done.
Configuring GigabitEthernet1/0/2 done.
Configuring GigabitEthernet1/0/3 done.
[DeviceA-Bridge-Aggregation1] port trunk permit vlan 10 20
Configuring GigabitEthernet1/0/1 done.
Configuring GigabitEthernet1/0/2 done.
Configuring GigabitEthernet1/0/3 done.
[DeviceA-Bridge-Aggregation1] quit
```

2. Device B 的配置

Device B 上的配置与 Device A 完全相同，此处不再赘述。

1.5 验证配置

通过 **display link-aggregation verbose** 命令来显示聚合组的相关信息，以验证配置是否成功。

- 采用静态聚合模式的链路聚合配置信息

```
[DeviceA] display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port, M -- Management port, R -- Reference port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregation Interface: Bridge-Aggregation1
Aggregation Mode: Static
Loadsharing Type: Shar
Management VLANs: None
  Port             Status  Priority  Oper-Key
  GE1/0/1(R)       S       32768     1
  GE1/0/2          S       32768     1
  GE1/0/3          S       32768     1
```

结果说明：本端加入到静态聚合组内的成员端口都处于 Selected 状态，与对端对应端口是否是 Selected 状态无关。

- 采用动态聚合模式的链路聚合配置信息

```
[DeviceA] display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port, M -- Management port, R -- Reference port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregation Interface: Bridge-Aggregation1
Creation Mode: Manual
Aggregation Mode: Dynamic
Loadsharing Type: Shar
Management VLANs: None
System ID: 0x8000, 000f-e234-5678
Local:
  Port               Status   Priority Index    Oper-Key               Flag
  GE1/0/1            S        32768    1        1                      {ACDEF}
  GE1/0/2            S        32768    2        1                      {ACDEF}
  GE1/0/3            S        32768    3        1                      {ACDEF}
Remote:
  Actor              Priority Index    Oper-Key SystemID               Flag
  GE1/0/1(R)         32768    1        1        0x8000, a4e5-c316-0100 {ACDEF}
  GE1/0/2            32768    2        1        0x8000, a4e5-c316-0100 {ACDEF}
  GE1/0/3            32768    3        1        0x8000, a4e5-c316-0100 {ACDEF}
```

结果说明：本端和对端设备上聚合组内的成员端口都处于 Selected 状态。原因是在动态链路聚合中通过 LACP 协议报文交互，可使两端聚合组内的成员端口选中状态达成一致，可顺利实现对用户数据的转发。

1.6 配置文件

- Device A：

```
#
vlan 10
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port access vlan 10
#
vlan 20
#
interface GigabitEthernet1/0/5
 port link-mode bridge
 port access vlan 20
```

  - 采用静态聚合模式

```
#
interface Bridge-Aggregation1
 port link-type trunk
 port trunk permit vlan 10 20
```

  - 采用动态聚合模式

```
#
interface Bridge-Aggregation1
 port link-type trunk
 port trunk permit vlan 10 20
 link-aggregation mode dynamic
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 10 20
 port link-aggregation group 1
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 10 20
 port link-aggregation group 1
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 10 20
 port link-aggregation group 1
#
```

- Device B：

Device B 上的配置文件与 Device A 相同。

1.7 相关资料

- 产品配套“二层技术-以太网交换配置指导”中的“以太网链路聚合”。
- 产品配套“二层技术-以太网交换命令参考”中的“以太网链路聚合”。

2 配置聚合负载分担采用本地转发优先

2.1 简介

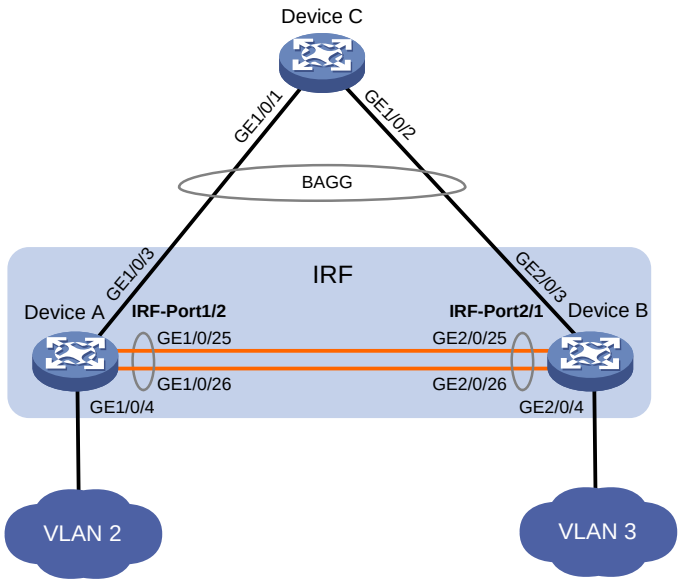
本案例介绍聚合负载分担采用本地转发优先的配置方法。

2.2 组网需求

如图 2 所示：

- Device A 与 Device B 组成 IRF，并通过 GigabitEthernet1/0/3 和 GigabitEthernet2/0/3 接口跨成员设备聚合。
- 由于聚合负载分担特性，VLAN 2 和 VLAN 3 的流量均会通过 GigabitEthernet1/0/3 和 GigabitEthernet2/0/3 接口转发至 Device C，流量转发效率较低。在带宽满足的情况下，现希望 VLAN 2 的流量通过 GigabitEthernet1/0/3 接口转发，VLAN 3 的流量通过 GigabitEthernet2/0/3 接口转发，以提升流量转发效率。

图2 二层链路聚合配置示例图



2.3 配置注意事项

- 仅 IRF 模式下支持配置本功能。
- 仅在 IRF 单台设备的带宽足以承载流量转发需求时推荐配置本功能，用于提升转发效率，缓解 IRF 集群带宽承载压力较大的问题。
- 有关如何组建 IRF，请参见“IRF 快速配置指南”或产品的配置命令手册，本例不做介绍。

2.4 配置步骤

1. Device A 的配置

进入系统视图，创建二层聚合接口 1。

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

将 GigabitEthernet1/0/3 和 GigabitEthernet2/0/3 接口加入到二层聚合口 1 中。

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port link-aggregation group 1
[DeviceA-GigabitEthernet1/0/3] quit
[DeviceA] interface gigabitethernet 2/0/3
[DeviceA-GigabitEthernet2/0/3] port link-aggregation group 1
[DeviceA-GigabitEthernet2/0/3] quit
```

配置二层聚合接口 1 类型为 Trunk，并允许通过所有 VLAN。

```
[DeviceA] interface bridge-aggregation 1
[DeviceA-Bridge-Aggregation1]port link-type trunk
[DeviceA-Bridge-Aggregation1]port trunk permit vlan all
[DeviceA-Bridge-Aggregation1]quit
```

配置聚合负载分担采用本地转发优先。

```
[DeviceA] link-aggregation load-sharing mode local-first
```

创建 VLAN 2 和 VLAN 3。

```
[DeviceA] vlan 2 to 3
```

配置 GigabitEthernet1/0/4 接口类型为 Trunk，并允许通过 VLAN 2。

```
[DeviceA] interface gigabitethernet 1/0/4
[DeviceA-GigabitEthernet1/0/4]port link-type trunk
[DeviceA-GigabitEthernet1/0/4]undo port trunk permit vlan 1
[DeviceA-GigabitEthernet1/0/4]port trunk permit vlan 2
[DeviceA-GigabitEthernet1/0/4]quit
```

配置 GigabitEthernet2/0/4 接口类型为 Trunk，并允许通过 VLAN 3。

```
[DeviceA] interface gigabitethernet 2/0/4
[DeviceA-GigabitEthernet2/0/4]port link-type trunk
[DeviceA-GigabitEthernet2/0/4]undo port trunk permit vlan 1
[DeviceA-GigabitEthernet2/0/4]port trunk permit vlan 3
[DeviceA-GigabitEthernet2/0/4]quit
```

2. Device B 的配置

Device B 上的配置与 Device A 完全相同，此处不再赘述。

3. Device C 的配置

进入系统视图，创建二层聚合接口 1。

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

将端口 GigabitEthernet1/0/1～GigabitEthernet1/0/2 加入到聚合组 1 中。

```
[DeviceC] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/2
[DeviceC-if-range] port link-aggregation group 1
[DeviceC-if-range] quit
```

配置二层聚合接口 1 类型为 Trunk，并允许通过所有 VLAN。

```
[DeviceC] interface bridge-aggregation 1
[DeviceC-Bridge-Aggregation1]port link-type trunk
[DeviceC-Bridge-Aggregation1]port trunk permit vlan all
[DeviceC-Bridge-Aggregation1]quit
```

2.5 验证配置

通过 **display link-aggregation verbose** 命令来显示聚合组的相关信息，以验证配置是否成功。

```
[DeviceA] display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port, M -- Management port, R -- Reference port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregation Interface: Bridge-Aggregation1
Aggregation Mode: Static
Loadsharing Type: Shar
Management VLANs: None
  Port             Status  Priority  Oper-Key
  GE1/0/3          S       32768     1
  GE2/0/3          S       32768     1
```

结果说明：加入到静态聚合组内的成员端口都处于 Selected 状态，VLAN 2 的流量将只通过 GigabitEthernet1/0/3 接口转发。

2.6 配置文件

- Device A：

```
#
interface Bridge-Aggregation1
 port link-type trunk
 port trunk permit vlan all
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan all
 port link-aggregation group 1
#
interface GigabitEthernet2/0/3
 port link-mode bridge
```

```
 port link-type trunk
 port trunk permit vlan all
 port link-aggregation group 1
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 2
#
interface GigabitEthernet2/0/4
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 3
#
link-aggregation load-sharing mode local-first
#
```

- Device B：

Device B 上的配置文件与 Device A 相同。

- Device C：

```
#
interface Bridge-Aggregation1
 port link-type trunk
 port trunk permit vlan all
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan all
 port link-aggregation group 1
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan all
 port link-aggregation group 1
#
```

2.7 相关资料

- 产品配套“二层技术-以太网交换配置指导”中的“以太网链路聚合”。
- 产品配套“二层技术-以太网交换命令参考”中的“以太网链路聚合”。

生成树快速配置指南

目 录

1 MSTP 快速配置指南

1.1 简介

本案例介绍 MSTP（Multiple Spanning Tree Protocol，多生成树协议）的配置方法。

1.2 组网需求

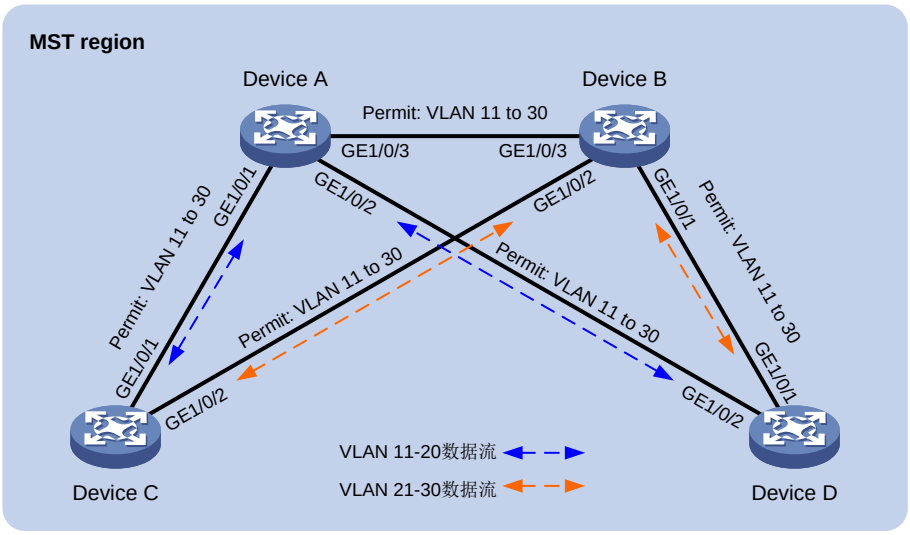
如图 1 所示：

- 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



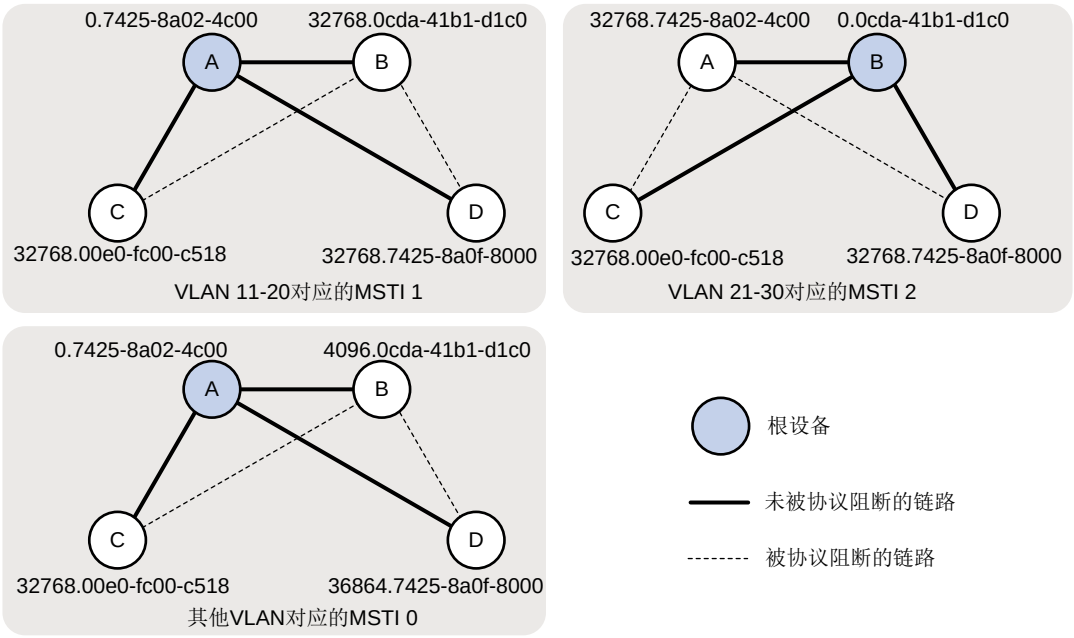
1.3 配置思路

要使所有设备属于同一 MST 域，在所有设备上配置相同的如下参数：

- 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 1.3 图 2 所示。

图2 各 VLAN 对应的生成树实例的拓扑



1.4 配置步骤

1. Device A 的配置

```
<DeviceA> system-view
[DeviceA] vlan 11 to 30
[DeviceA] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/3
[DeviceA-if-range] port link-type trunk
[DeviceA-if-range] port trunk permit vlan 11 to 30
[DeviceA-if-range] quit
```

配置 MST 域的域名为 test，将 VLAN 11～20 映射到 MSTI 1，VLAN 21～30 映射到 MSTI 2。

```
[DeviceA] stp region-configuration
[DeviceA-mst-region] region-name test
[DeviceA-mst-region] instance 1 vlan 11 to 20
[DeviceA-mst-region] instance 2 vlan 21 to 30
[DeviceA-mst-region] active region-configuration
[DeviceA-mst-region] quit
```

配置本设备为 MSTI 0 和 1 的根桥。

```
[DeviceA] stp instance 0 to 1 root primary
```

全局开启生成树协议。

```
[DeviceA] stp global enable
```

保存配置。

```
[DeviceA] save force
```

2. Device B 的配置

创建 VLAN 11～30。将设备的各端口配置为 Trunk 端口并允许 VLAN 11～30 通过。

```
<DeviceB> system-view
[DeviceB] vlan 11 to 30
[DeviceB] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/3
[DeviceB-if-range] port link-type trunk
[DeviceB-if-range] port trunk permit vlan 11 to 30
[DeviceB-if-range] quit
```

配置 MST 域的域名为 test，将 VLAN 11～20 映射到 MSTI 1，VLAN 21～30 映射到 MSTI 2。

```
[DeviceB] stp region-configuration
[DeviceB-mst-region] region-name test
[DeviceB-mst-region] instance 1 vlan 11 to 20
[DeviceB-mst-region] instance 2 vlan 21 to 30
[DeviceB-mst-region] active region-configuration
[DeviceB-mst-region] quit
```

配置本设备为 MSTI 2 的根桥，以及 MSTI 0 的备份根桥。

```
[DeviceB] stp instance 2 root primary
[DeviceB] stp instance 0 root secondary
```

全局开启生成树协议。

```
[DeviceB] stp global enable
```

保存配置。

```
[DeviceB] save force
```

3. Device C 的配置

创建 VLAN 11～30。将设备的各端口配置为 Trunk 端口并允许 VLAN 11～30 通过。

```
<DeviceC> system-view
[DeviceC] vlan 11 to 30
[DeviceC] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/2
[DeviceC-if-range] port link-type trunk
[DeviceC-if-range] port trunk permit vlan 11 to 30
[DeviceC-if-range] quit
```

配置 MST 域的域名为 test，将 VLAN 11～20 映射到 MSTI 1，VLAN 21～30 映射到 MSTI 2。

```
[DeviceC] stp region-configuration
[DeviceC-mst-region] region-name test
[DeviceC-mst-region] instance 1 vlan 11 to 20
[DeviceC-mst-region] instance 2 vlan 21 to 30
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
```

全局开启生成树协议。

```
[DeviceC] stp global enable
```

保存配置。

```
[DeviceC] save force
```

4. Device D 的配置

创建 VLAN 11～30。将设备的各端口配置为 Trunk 端口并允许 VLAN 11～30 通过。

```
<DeviceD> system-view
[DeviceD] vlan 11 to 30
[DeviceD] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/2
[DeviceD-if-range] port link-type trunk
[DeviceD-if-range] port trunk permit vlan 11 to 30
[DeviceD-if-range] quit
```

配置 MST 域的域名为 test，将 VLAN 11～20 映射到 MSTI 1，VLAN 21～30 映射到 MSTI 2。

```
[DeviceD] stp region-configuration
[DeviceD-mst-region] region-name test
[DeviceD-mst-region] instance 1 vlan 11 to 20
[DeviceD-mst-region] instance 2 vlan 21 to 30
[DeviceD-mst-region] active region-configuration
[DeviceD-mst-region] quit
```

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）。

```
[DeviceD] stp instance 0 priority 36864
```

全局开启生成树协议。

```
[DeviceD] stp global enable
```

保存配置。

```
[DeviceD] save force
```

1.5 验证配置

1. 查看生成树实例拓扑信息

查看 Device A 上生成树的简要信息。

```
[DeviceA] display stp brief
 MST ID   Port                                Role  STP State     Protection
 0        GigabitEthernet1/0/1                DESI  FORWARDING    NONE
 0        GigabitEthernet1/0/2                DESI  FORWARDING    NONE
 0        GigabitEthernet1/0/3                DESI  FORWARDING    NONE
 1        GigabitEthernet1/0/1                DESI  FORWARDING    NONE
 1        GigabitEthernet1/0/2                DESI  FORWARDING    NONE
 1        GigabitEthernet1/0/3                DESI  FORWARDING    NONE
 2        GigabitEthernet1/0/1                ALTE  FORWARDING    NONE
 2        GigabitEthernet1/0/2                DESI  FORWARDING    NONE
 2        GigabitEthernet1/0/3                ROOT  FORWARDING    NONE
```

查看 Device B 上生成树的简要信息。

```
[DeviceB] display stp brief
 MST ID   Port                                Role  STP State     Protection
 0        GigabitEthernet1/0/1                DESI  FORWARDING    NONE
 0        GigabitEthernet1/0/2                DESI  FORWARDING    NONE
 0        GigabitEthernet1/0/3                ROOT  FORWARDING    NONE
 1        GigabitEthernet1/0/1                DESI  FORWARDING    NONE
```

```
1          GigabitEthernet1/0/2                ALTE  FORWARDING  NONE
1          GigabitEthernet1/0/3                ROOT  FORWARDING  NONE
2          GigabitEthernet1/0/1                DESI  FORWARDING  NONE
2          GigabitEthernet1/0/2                DESI  FORWARDING  NONE
2          GigabitEthernet1/0/3                DESI  FORWARDING  NONE
```

查看 Device C 上生成树的简要信息。

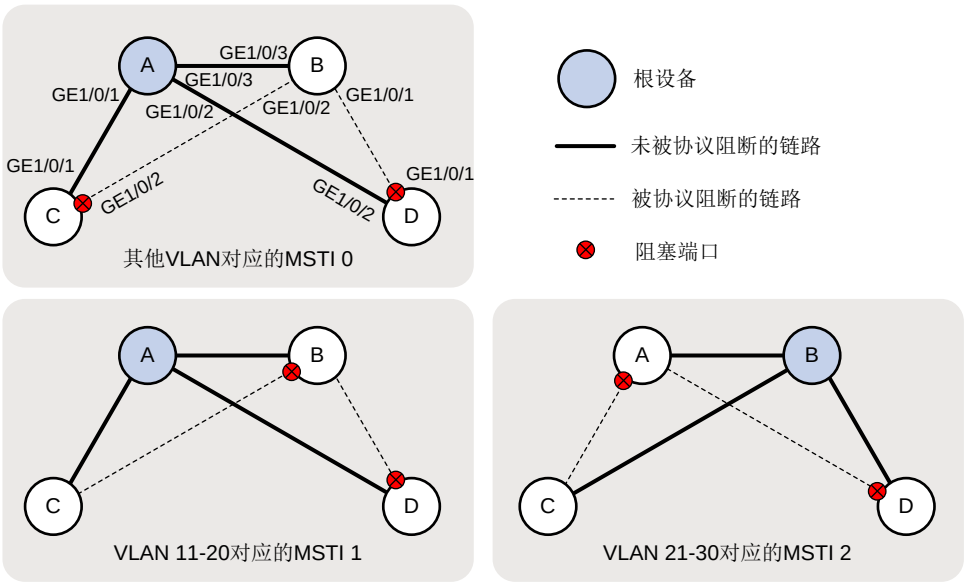
```
[DeviceC] display stp brief
 MST ID   Port                                Role  STP State   Protection
 0        GigabitEthernet1/0/1                ROOT  FORWARDING  NONE
 0        GigabitEthernet1/0/2                ALTE  DISCARDING  NONE
 1        GigabitEthernet1/0/1                ROOT  FORWARDING  NONE
 1        GigabitEthernet1/0/2                DESI  DISCARDING  NONE
 2        GigabitEthernet1/0/1                DESI  DISCARDING  NONE
 2        GigabitEthernet1/0/2                ROOT  FORWARDING  NONE
```

查看 Device D 上生成树的简要信息。

```
[DeviceD] display stp brief
 MST ID   Port                                Role  STP State   Protection
 0        GigabitEthernet1/0/1                ALTE  DISCARDING  NONE
 0        GigabitEthernet1/0/2                ROOT  FORWARDING  NONE
 1        GigabitEthernet1/0/1                ALTE  DISCARDING  NONE
 1        GigabitEthernet1/0/2                ROOT  FORWARDING  NONE
 2        GigabitEthernet1/0/1                ROOT  FORWARDING  NONE
 2        GigabitEthernet1/0/2                ALTE  DISCARDING  NONE
```

根据上述显示信息中的 Alternate 端口（阻塞端口），可以绘出各 VLAN 所对应 MSTI 的拓扑，如 1.5 1. 图 3所示。

图3 MSTI 0～2 的拓扑



可以看到，Device C 和 Device D 的 VLAN 11～20 报文和 VLAN 21～30 报文沿不同的上行链路转发；网络中无二层环路。

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）。

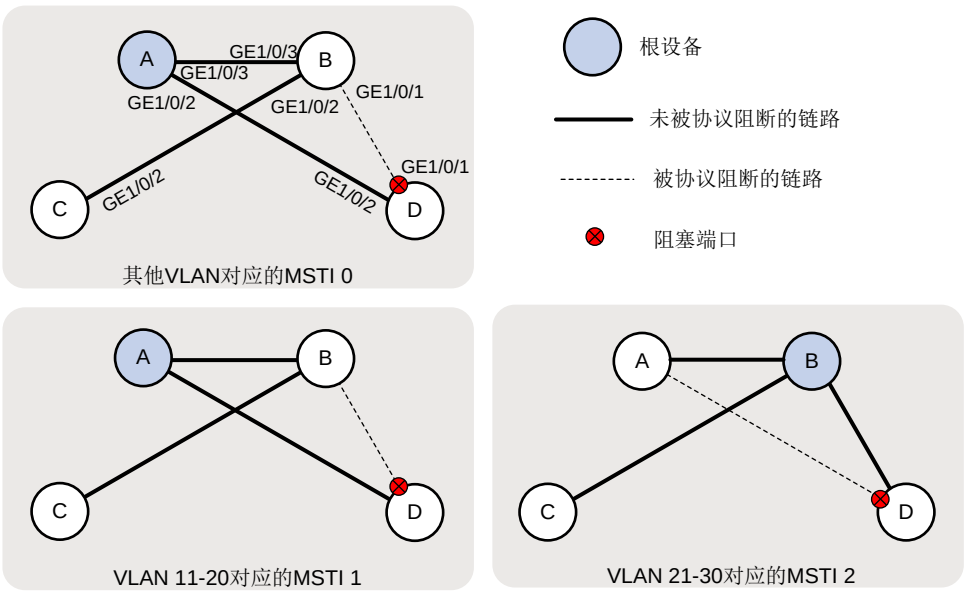
```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] shutdown
```

查看 Device A、B、C、D 上生成树的简要信息。

```
[DeviceA] display stp brief
 MST ID   Port                                Role  STP State   Protection
 0        GigabitEthernet1/0/2                DESI  FORWARDING  NONE
 0        GigabitEthernet1/0/3                DESI  FORWARDING  NONE
 1        GigabitEthernet1/0/2                DESI  FORWARDING  NONE
 1        GigabitEthernet1/0/3                DESI  FORWARDING  NONE
 2        GigabitEthernet1/0/2                DESI  FORWARDING  NONE
 2        GigabitEthernet1/0/3                ROOT  FORWARDING  NONE
[DeviceB] display stp brief
 MST ID   Port                                Role  STP State   Protection
 0        GigabitEthernet1/0/1                DESI  FORWARDING  NONE
 0        GigabitEthernet1/0/2                DESI  FORWARDING  NONE
 0        GigabitEthernet1/0/3                ROOT  FORWARDING  NONE
 1        GigabitEthernet1/0/1                DESI  FORWARDING  NONE
 1        GigabitEthernet1/0/2                DESI  FORWARDING  NONE
 1        GigabitEthernet1/0/3                ROOT  FORWARDING  NONE
 2        GigabitEthernet1/0/1                DESI  FORWARDING  NONE
 2        GigabitEthernet1/0/2                DESI  FORWARDING  NONE
 2        GigabitEthernet1/0/3                DESI  FORWARDING  NONE
[DeviceC] display stp brief
 MST ID   Port                                    Role  STP State   Protection
 0        GigabitEthernet1/0/2                ROOT  FORWARDING  NONE
 1        GigabitEthernet1/0/2                ROOT  FORWARDING  NONE
 2        GigabitEthernet1/0/2                ROOT  FORWARDING  NONE
[DeviceD] display stp brief
 MST ID   Port                                Role  STP State   Protection
 0        GigabitEthernet1/0/1                ALTE  DISCARDING  NONE
 0        GigabitEthernet1/0/2                ROOT  FORWARDING  NONE
 1        GigabitEthernet1/0/1                ALTE  DISCARDING  NONE
 1        GigabitEthernet1/0/2                ROOT  FORWARDING  NONE
 2        GigabitEthernet1/0/1                ROOT  FORWARDING  NONE
 2        GigabitEthernet1/0/2                ALTE  DISCARDING  NONE
```

根据上述显示信息中的 Alternate 端口（阻塞端口），可以绘出各 VLAN 所对应 MSTI 的拓扑，如 2. 图 4 所示。

图4 某链路断开后 MSTI 0～2 的拓扑



可以看到，Device C 在 MSTI 0～1 中的上行链路所在端口已从原先的 GigabitEthernet1/0/1 切换为 GigabitEthernet1/0/2。

1.6 配置文件

- Device A：

```
#
vlan 1
#
vlan 11 to 30
#
stp region-configuration
 region-name test
 instance 1 vlan 11 to 20
 instance 2 vlan 21 to 30
 active region-configuration
#
 stp instance 0 to 1 root primary
 stp global enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 11 to 30
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
```

```
 port trunk permit vlan 1 11 to 30
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 11 to 30
```

- Device B：

```
#
vlan 1
#
vlan 11 to 30
#
stp region-configuration
 region-name test
 instance 1 vlan 11 to 20
 instance 2 vlan 21 to 30
 active region-configuration
#
 stp instance 0 root secondary
 stp instance 2 root primary
 stp global enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 11 to 30
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 11 to 30
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 11 to 30
```

- Device C：

```
#
vlan 1
#
vlan 11 to 30
#
stp region-configuration
 region-name test
 instance 1 vlan 11 to 20
 instance 2 vlan 21 to 30
 active region-configuration
#
```

```
 stp global enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 11 to 30
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 11 to 30
```

- Device D：

```
#
vlan 1
#
vlan 11 to 30
#
stp region-configuration
 region-name test
 instance 1 vlan 11 to 20
 instance 2 vlan 21 to 30
 active region-configuration
#
 stp instance 0 priority 36864
 stp global enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 11 to 30
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 11 to 30
```

1.7 相关资料

- 产品配套“二层技术-以太网交换配置指导”中的“生成树”。
- 产品配套“二层技术-以太网交换命令参考”中的“生成树”。

DHCP 快速配置指南

目 录

1 配置 DHCP 服务器动态分配 IPv4 地址

1.1 简介

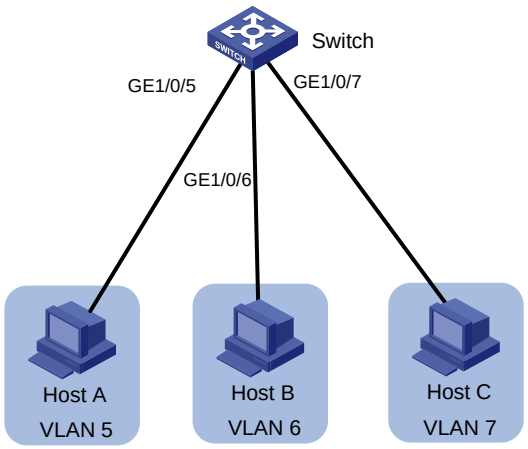
本案例介绍配置接口工作在 DHCP 服务器模式，实现动态分配 IPv4 地址的方法。

1.2 组网需求

如 1.2 图 1 所示，公司将交换机做为核心交换机，现在需要在核心交换机上划分 3 个 VLAN 网段，HostA、Host B 和 Host C 分别属于 VLAN 5、VLAN 6 和 VLAN 7，要求在交换机上配置 DHCP 服务器功能，分别给主机分配不同网段的 IP 地址。

- 作为 DHCP 服务器的 Switch 为网段 192.168.5.0/24、192.168.6.0/24 和 192.168.7.0/24 中的客户端动态分配 IP 地址；
- Switch 的三个 VLAN 接口，VLAN 接口 5、VLAN 接口 6 和 VLAN 接口 7 的地址分别为 192.168.5.254/24、192.168.6.254/24 和 192.168.7.254/24；
- 192.168.5.0/24 网段内的 DNS 服务器地址为 192.168.5.100/24，网关的地址为 192.168.5.254/24；
- 192.168.6.0/24 网段内的 DNS 服务器地址为 192.168.6.100/24，网关的地址为 192.168.6.254/24；
- 192.168.7.0/24 网段内的 DNS 服务器地址为 192.168.7.100/24，网关的地址为 192.168.7.254/24。

图1 DHCP 服务器配置组网图



1.3 配置步骤

配置端口所属 VLAN 和对应 VLAN 接口的 IP 地址，IP 地址即是对应 VLAN 的网关地址。

```
<Switch> system-view
[Switch] vlan 5
[Switch-vlan5] port gigabitEthernet 1/0/5
[Switch-vlan5] quit
```

```
[Switch]vlan 6
[Switch-vlan6] port gigabitEthernet 1/0/6
[Switch-vlan6] quit
[Switch]vlan 7
[Switch-vlan7] port gigabitEthernet 1/0/7
[Switch-vlan7] quit
[Switch] interface vlan-interface 5
[Switch-Vlan-interface5] ip address 192.168.5.254 255.255.255.0
[Switch-Vlan-interface5] quit
[Switch]interface vlan-interface 6
[Switch-Vlan-interface6] ip address 192.168.6.254 255.255.255.0
[Switch-Vlan-interface6] quit
[Switch]interface vlan-interface 7
[Switch-Vlan-interface7] ip address 192.168.7.254 255.255.255.0
[Switch-Vlan-interface7] quit
```

配置不参与自动分配的 IP 地址（DNS 服务器等，此步为选配）

```
[Switch] dhcp server forbidden-ip 192.168.5.100
[Switch] dhcp server forbidden-ip 192.168.6.100
[Switch] dhcp server forbidden-ip 192.168.7.100
```

配置 DHCP 地址池 5，用来为 192.168.5.0/24 网段内的客户端分配 IP 地址。

```
[Switch] dhcp server ip-pool 5
[Switch-dhcp-pool-5] network 192.168.5.0 mask 255.255.255.0
[Switch-dhcp-pool-5] dns-list 192.168.5.100
[Switch-dhcp-pool-5] gateway-list 192.168.5.254
[Switch-dhcp-pool-5] quit
```

配置 DHCP 地址池 6，用来为 192.168.6.0/24 网段内的客户端分配 IP 地址。

```
[Switch] dhcp server ip-pool 6
[Switch-dhcp-pool-6] network 192.168.6.0 mask 255.255.255.0
[Switch-dhcp-pool-6] dns-list 192.168.6.100
[Switch-dhcp-pool-6] gateway-list 192.168.6.254
[Switch-dhcp-pool-6] quit
```

配置 DHCP 地址池 7，用来为 192.168.7.0/24 网段内的客户端分配 IP 地址。

```
[Switch] dhcp server ip-pool 7
[Switch-dhcp-pool-7] network 192.168.7.0 mask 255.255.255.0
[Switch-dhcp-pool-7] dns-list 192.168.7.100
[Switch-dhcp-pool-7] gateway-list 192.168.7.254
[Switch-dhcp-pool-7] quit
```

开启 DHCP 服务

```
[Switch] dhcp enable
```

配置 VLAN 接口 5、6 和 7 工作在 DHCP 服务器模式。

```
[Switch] interface vlan-interface 5
[Switch-Vlan-interface5] dhcp select server
[Switch-Vlan-interface5] quit
[Switch] interface vlan-interface 6
[Switch-Vlan-interface6] dhcp select server
[Switch-Vlan-interface6] quit
```

```
[Switch] interface vlan-interface 7
[Switch-Vlan-interface7] dhcp select server
[Switch-Vlan-interface7] quit
```

1.4 验证配置

配置完成后，5、6、7 三个网段客户端可以从 DHCP 服务器申请到相应网段的 IP 地址和网络配置参数。

1. 显示 DHCP 服务器的配置

显示 DHCP 地址池的信息。

```
[Switch] display dhcp server pool
Pool name: 5
  Network: 192.168.5.0 mask 255.255.255.0
  dns-list 192.168.5.100
  expired day 1 hour 0 minute 0 second 0
  gateway-list 192.168.5.254
  IP-in-use threshold 100
Pool name: 6
  Network: 192.168.6.0 mask 255.255.255.0
  dns-list 192.168.6.100
  expired day 1 hour 0 minute 0 second 0
  gateway-list 192.168.6.254
  IP-in-use threshold 100
Pool name: 7
  Network: 192.168.7.0 mask 255.255.255.0
  dns-list 192.168.7.100
  expired day 1 hour 0 minute 0 second 0
  gateway-list 192.168.7.254
  IP-in-use threshold 100
```

2. 显示 DHCP 服务器的 IP 地址分配信息

显示 DHCP 地址绑定信息。在显示信息里可以查看 DHCP 服务器为客户端分配的 IP 地址。

```
[Switch] display dhcp server ip-in-use
IP address       Client-identifier/    Lease expiration      Type
                 Hardware address
192.168.5.1      0262-1d36-1802-00     Feb 18 10:41:21 2023  Auto(C)
                 3264-2e30-3130-322d-
                 566c-616e-3130
192.168.6.1      0262-1d3b-7403-00     Feb 18 10:41:17 2023  Auto(C)
192.168.7.2      0262-1d41-8304-00     Feb 18 10:41:41 2023  Auto(C)
```

显示 DHCP 地址池的空闲地址信息。

```
[Switch] display dhcp server free-ip
Pool name: 5
  Network: 192.168.5.0 mask 255.255.255.0
    IP ranges from 192.168.5.2 to 192.168.5.99
    IP ranges from 192.168.5.101 to 192.168.5.254
```

```
Pool name: 6
  Network: 192.168.6.0 mask 255.255.255.0
    IP ranges from 192.168.6.2 to 192.168.6.99
    IP ranges from 192.168.6.101 to 192.168.6.254

Pool name: 7
  Network: 192.168.7.0 mask 255.255.255.0
    IP ranges from 192.168.7.2 to 192.168.7.99
IP ranges from 192.168.7.101 to 192.168.7.254
```

显示租约过期的地址绑定信息。当分配的 IP 地址的租约超过有效期限后，执行本命令可以查看到租约过期的地址绑定信息（通过 **expired** 命令可以配置租约有效期，缺省有效期限为 1 天）。

```
[Switch] display dhcp server expired
IP address       Client-identifier/Hardware address   Lease expiration
192.168.7.1      0262-1d36-2703-00                    Feb 17 10:53:52 2023
```

3. 清除 DHCP 服务器的 IP 地址分配信息

清除 DHCP 的正式绑定和临时绑定信息。请在用户视图下执行本命令。

```
[Switch] quit
<Switch> reset dhcp server ip-in-use
```

显示 DHCP 地址绑定信息。此时设备上不存在相关信息。

```
<Switch> display dhcp server ip-in-use
IP address       Client-identifier/    Lease expiration      Type
                 Hardware address
```

清除租约过期的地址绑定信息。请在用户视图下执行本命令。

```
<Switch> reset dhcp server expired
```

显示租约过期的地址绑定信息。此时设备上不存在相关信息。

```
<Switch> display dhcp server ip-in-use
IP address       Client-identifier/    Lease expiration      Type
                 Hardware address
```

4. 显示和清除 DHCP 服务器的统计信息

显示 DHCP 服务器的统计信息。

```
<Switch> dis dhcp server statistics
    Pool number:                    3
    Pool utilization:               0.00%
    Bindings:
      Automatic:                    0
      Manual:                       0
      Expired:                      3
    Conflict:                       0
    Messages received:              170
      DHCPDISCOVER:                 57
      DHCPREQUEST:                  57
      DHCPDECLINE:                  0
      DHCPRELEASE:                  56
      DHCPINFORM:                   0
      BOOTPREQUEST:                 0
```

```
    Messages sent:                    114
      DHCPOFFER:                      57
      DHCPACK:                        57
      DHCPNAK:                        0
      BOOTPREPLY:                     0
    Bad Messages:                     0
```

清除 DHCP 服务器的统计信息。请在用户视图下执行本命令。

```
<Switch> reset dhcp server statistics
```

清除 DHCP 服务器的统计信息后，设备上不存在相关统计信息。

```
<Switch> dis dhcp server statistics
    Pool number:                      3
    Pool utilization:                 0.39%
    Bindings:
      Automatic:                      3
      Manual:                         0
      Expired:                        0
    Conflict:                         0
    Messages received:                0
      DHCPDISCOVER:                   0
      DHCPREQUEST:                    0
      DHCPDECLINE:                    0
      DHCPRELEASE:                    0
      DHCPINFORM:                     0
      BOOTPREQUEST:                   0
    Messages sent:                    0
      DHCPOFFER:                      0
      DHCPACK:                        0
      DHCPNAK:                        0
      BOOTPREPLY:                     0
    Bad Messages:                     0
```

1.5 配置文件

- Switch：

```
#
 dhcp enable
 dhcp server forbidden-ip 192.168.5.100
 dhcp server forbidden-ip 192.168.6.100
 dhcp server forbidden-ip 192.168.7.100
#
vlan 5 to 7
#
dhcp server ip-pool 5
 gateway-list 192.168.5.254
 network 192.168.5.0 mask 255.255.255.0
 dns-list 192.168.5.100
#
```

```
dhcp server ip-pool 6
 gateway-list 192.168.6.254
 network 192.168.6.0 mask 255.255.255.0
 dns-list 192.168.6.100
#
dhcp server ip-pool 7
 gateway-list 192.168.7.254
 network 192.168.7.0 mask 255.255.255.0
 dns-list 192.168.7.100
#
interface Vlan-interface5
 ip address 192.168.5.254 255.255.255.0
 dhcp select server
#
interface Vlan-interface6
 ip address 192.168.6.254 255.255.255.0
 dhcp select server
#
interface Vlan-interface7
 ip address 192.168.7.254 255.255.255.0
 dhcp select server
#
interface GigabitEthernet1/0/5
 port link-mode bridge
 port access vlan 5
#
interface GigabitEthernet1/0/6
 port link-mode bridge
 port access vlan 6
#
interface GigabitEthernet1/0/7
 port link-mode bridge
 port access vlan 7
#
```

1.6 相关资料

- 产品配套“三层技术-IP 业务配置指导”中的“DHCP”。
- 产品配套“三层技术-IP 业务命令参考”中的“DHCP”。

2 配置 DHCP 中继

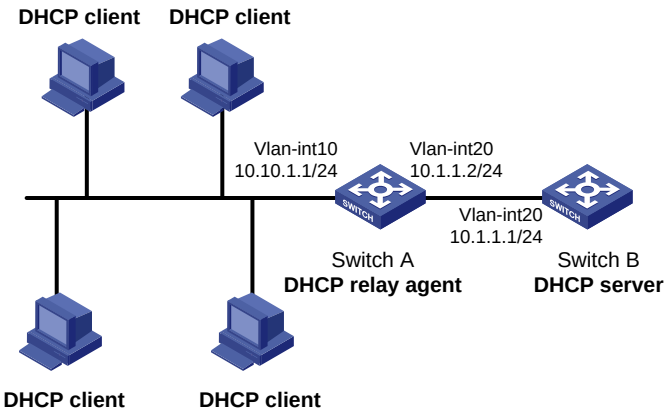
2.1 简介

本案例介绍配置接口工作在 DHCP 中继模式，当 DHCP 客户端和 DHCP 服务器处于不同物理网段时，用于实现客户端可以通过 DHCP 中继与 DHCP 服务器通信，获取 IP 地址及其他配置信息。

2.2 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；
- Switch A 作为 DHCP 中继通过端口（属于 VLAN10）连接到 DHCP 客户端所在的网络，交换机 VLAN 接口 10 的 IP 地址为 10.10.1.1/24，VLAN 接口 20 的 IP 地址为 10.1.1.2/24。

图2 DHCP 中继配置组网图



2.3 配置步骤

- 配置 DHCP 服务器 Switch B

  # 创建 VLAN 接口和 IP 地址。

```
<SwitchB> system-view
[SwitchB] vlan 20
[SwitchB-vlan20] port gigabitEthernet 1/0/1
[SwitchB-vlan20] quit
[SwitchB] interface vlan-interface 20
[SwitchB-Vlan-interface20] ip address 10.1.1.1 255.255.255.0
[SwitchB-Vlan-interface20] quit
```

  # 配置 DHCP 地址池 5，用来为 10.10.1.0/24 网段内的客户端分配 IP 地址。

```
[SwitchB] dhcp server ip-pool 5
[SwitchB-dhcp-pool-5] network 10.10.1.0 mask 255.255.255.0
```

```
[SwitchB-dhcp-pool-5] dns-list 10.10.1.100
[SwitchB-dhcp-pool-5] gateway-list 10.10.1.1
[SwitchB-dhcp-pool-5] quit
```

配置和 DHCP 客户端互通的静态路由。

```
[SwitchB] ip route-static 10.10.1.0 24 10.1.1.2
```

开启 DHCP 服务

```
[SwitchB] dhcp enable
```

配置 VLAN 接口 20 工作在 DHCP 服务器模式。

```
[SwitchB] interface vlan-interface 20
[SwitchB-Vlan-interface20] dhcp select server
[SwitchB-Vlan-interface20] quit
```

- 配置 DHCP 中继设备 Switch A

创建 VLAN 接口和 IP 地址。

```
<SwitchA> system-view
[SwitchA] vlan 10
[SwitchA-vlan10] port gigabitEthernet 1/0/1
[SwitchA-vlan10] quit
[SwitchA] vlan 20
[SwitchA-vlan20] port gigabitEthernet 1/0/2
[SwitchA-vlan20] quit
[SwitchA] interface vlan-interface 10
[SwitchA-Vlan-interface10] ip address 10.10.1.1 255.255.255.0
[SwitchA-Vlan-interface10] quit
[SwitchA] interface vlan-interface 20
[SwitchA-Vlan-interface20] ip address 10.1.1.2 255.255.255.0
[SwitchA-Vlan-interface20] quit
```

开启 DHCP 服务。

```
[SwitchA] dhcp enable
```

配置 VLAN 接口 10 工作在 DHCP 中继模式。

```
[SwitchA] interface vlan-interface 10
[SwitchA-Vlan-interface10] dhcp select relay
```

配置 DHCP 服务器的地址。

```
[SwitchA-Vlan-interface10] dhcp relay server-address 10.1.1.1
```

2.4 验证配置

配置完成后，DHCP 客户端可以通过 DHCP 中继从 DHCP 服务器获取 IP 地址及相关配置信息。

显示接口上指定的 DHCP 服务器地址信息。

```
[SwitchA] display dhcp relay server-address
Interface name      Server IP address   Public/VRF name     Class name
Vlan10              10.1.1.1            Y/--                --
```

显示 DHCP 地址绑定信息。在显示信息里可以查看 DHCP 服务器为客户端分配的 IP 地址。

```
[SwitchB] display dhcp server ip-in-use
IP address       Client-identifier/    Lease expiration      Type
```

```
                Hardware address
10.10.1.2       0036-3232-352e-3261-  Feb 18 16:14:25 2023  Auto(C)
                3264-2e30-3130-322d-
                566c-616e-3130
```

显示 DHCP 中继的相关报文统计信息。

```
[SwitchB] display dhcp relay statistics
DHCP packets dropped:                  0
   Incorrect Message type:             0
   Option Parsing failed:              0
   Mac-check failed:                   0
   Other count:                        0
DHCP packets received from clients:    2
   DHCPDISCOVER:                       1
   DHCPREQUEST:                        1
   DHCPINFORM:                         0
   DHCPRELEASE:                        0
   DHCPDECLINE:                        0
   BOOTPREQUEST:                       0
DHCP packets received from servers:    2
   DHCPOFFER:                          1
   DHCPACK:                            1
   DHCPNAK:                            0
   BOOTPREPLY:                         0
DHCP packets relayed to servers:       2
   DHCPDISCOVER:                       1
   DHCPREQUEST:                        1
   DHCPINFORM:                         0
   DHCPRELEASE:                        0
   DHCPDECLINE:                        0
   BOOTPREQUEST:                       0
DHCP packets relayed to clients:       2
   DHCPOFFER:                          1
   DHCPACK:                            1
   DHCPNAK:                            0
   BOOTPREPLY:                         0
DHCP packets sent to servers:          0
   DHCPDISCOVER:                       0
   DHCPREQUEST:                        0
   DHCPINFORM:                         0
   DHCPRELEASE:                        0
   DHCPDECLINE:                        0
   BOOTPREQUEST:                       0
DHCP packets sent to clients:          0
   DHCPOFFER:                          0
   DHCPACK:                            0
   DHCPNAK:                            0
   BOOTPREPLY:                         0
```

在用户视图下执行 **reset dhcp relay statistics** 命令，可以清除该统计信息。

```
[SwitchB] quit
<SwitchB> reset dhcp relay statistics
```
再次查看显示 DHCP 中继的相关报文统计信息。
```
[SwitchB] display dhcp relay statistics
DHCP packets dropped:                  0
   Incorrect Message type:             0
   Option Parsing failed:              0
   Mac-check failed:                   0
   Other count:                        0
DHCP packets received from clients:    0
   DHCPDISCOVER:                       0
   DHCPREQUEST:                        0
   DHCPINFORM:                         0
   DHCPRELEASE:                        0
   DHCPDECLINE:                        0
   BOOTPREQUEST:                       0
DHCP packets received from servers:    0
   DHCPOFFER:                          0
   DHCPACK:                            0
   DHCPNAK:                            0
   BOOTPREPLY:                         0
DHCP packets relayed to servers:       0
   DHCPDISCOVER:                       0
   DHCPREQUEST:                        0
   DHCPINFORM:                         0
   DHCPRELEASE:                        0
   DHCPDECLINE:                        0
   BOOTPREQUEST:                       0
DHCP packets relayed to clients:       0
   DHCPOFFER:                          0
   DHCPACK:                            0
   DHCPNAK:                            0
   BOOTPREPLY:                         0
DHCP packets sent to servers:          0
   DHCPDISCOVER:                       0
   DHCPREQUEST:                        0
   DHCPINFORM:                         0
   DHCPRELEASE:                        0
   DHCPDECLINE:                        0
   BOOTPREQUEST:                       0
DHCP packets sent to clients:          0
   DHCPOFFER:                          0
   DHCPACK:                            0
   DHCPNAK:                            0
   BOOTPREPLY:                         0
```

2.5 配置文件

- 配置 Switch B

```
#
 dhcp enable
#
vlan 20
#
dhcp server ip-pool 5
 gateway-list 10.10.1.1
 network 10.10.1.0 mask 255.255.255.0
 dns-list 10.10.1.100
#
interface Vlan-interface20
 ip address 10.1.1.1 255.255.255.0
 dhcp select server
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 20
#
 ip route-static 10.10.1.0 24 10.1.1.2
#
```

- 配置 Switch A

```
#
 dhcp enable
#
vlan 10
#
vlan 20
#
interface Vlan-interface10
 ip address 10.10.1.1 255.255.255.0
 dhcp select relay
 dhcp relay server-address 10.1.1.1
#
interface Vlan-interface20
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 10
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 20
#
```

2.6 相关资料

- 产品配套“三层技术-IP 业务配置指导”中的“DHCP”。
- 产品配套“三层技术-IP 业务命令参考”中的“DHCP”。

3 配置 DHCP Snooping

3.1 简介

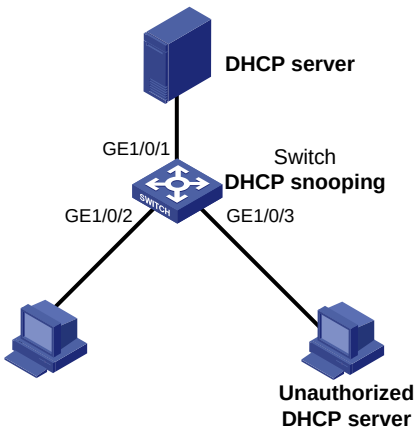
本案例介绍配置 DHCP Snooping 功能的配置方法。

3.2 组网需求

如 3.2 图 3 所示，Switch 通过以太网端口 GigabitEthernet1/0/1 连接到合法 DHCP 服务器，通过以太网端口 GigabitEthernet1/0/3 连接到非法 DHCP 服务器，通过 GigabitEthernet1/0/2 连接到 DHCP 客户端。要求：

- 与合法 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 报文和信任端口收到的 DHCP-ACK 报文中 DHCP 客户端 IP 地址及 MAC 地址的绑定信息。

图3 DHCP Snooping 配置组网图



3.3 配置步骤

全局开启 DHCP Snooping 功能。

```
<Switch> system-view
[Switch] dhcp snooping enable
```

设置 GigabitEthernet1/0/1 端口为信任端口。

```
[Switch] interface gigabitethernet 1/0/1
[Switch-GigabitEthernet1/0/1] dhcp snooping trust
[Switch-GigabitEthernet1/0/1] quit
```

在 GigabitEthernet1/0/2 上开启 DHCP Snooping 表项功能。

```
[Switch] interface gigabitethernet 1/0/2
[Switch-GigabitEthernet1/0/2] dhcp snooping binding record
[Switch-GigabitEthernet1/0/2] quit
```

3.4 验证配置

配置完成后，DHCP 客户端只能从合法 DHCP 服务器获取 IP 地址和其它配置信息，非法 DHCP 服务器无法为 DHCP 客户端分配 IP 地址和其他配置信息。且使用 **display dhcp snooping binding** 可查询到获取到的 DHCP Snooping 表项。在用户视图下执行 **reset dhcp snooping binding** 命令，可以清除 DHCP Snooping 表项。

3.5 配置文件

```
#
 dhcp snooping enable
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 dhcp snooping trust
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 dhcp snooping binding record
#
```

3.6 相关资料

- 产品配套“三层技术-IP 业务配置指导”中的“DHCP”。
- 产品配套“三层技术-IP 业务命令参考”中的“DHCP”。

4 配置 DHCPv6 服务器动态分配 IPv6 地址

4.1 简介

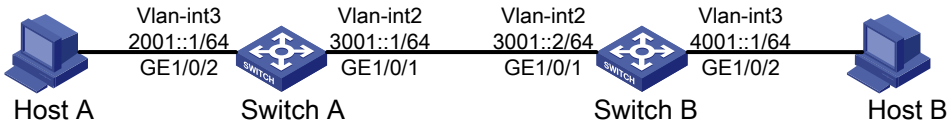
本案例介绍配置接口工作在 DHCPv6 服务器模式，实现动态分配 IPv6 地址的方法。

4.2 组网需求

如图 4 所示，交换机作为企业网络内部的网关设备。配置交换机接口工作在 DHCPv6 服务器模式，并配置地址/前缀分配方式，从而为主机 Host A 和 Host B 自动分配 IPv6 地址。不同网段的主机通过 IPv6 静态路由互相访问。

- Host A、Host B、Switch A 和 Switch B 之间通过以太网端口相连，将以太网端口分别加入相应的 VLAN 里，在 VLAN 接口上配置 IPv6 地址，验证它们之间的互通性。
- 配置 VLAN 接口工作在 DHCPv6 服务器模式，并引用地址池，从而为主机自动分配 IPv6 地址。
- 在 Switch A 和 Switch B 上配置 IPv6 静态路由，实现各网段的互通。

图4 动态分配 IPv6 地址组网图



4.3 配置步骤

1. 配置 Switch A

创建 VLAN，在 VLAN 中加入对应的端口。

```
<SwitchA> system-view
[SwitchA] vlan 3
[SwitchA-vlan3] port gigabitethernet 1/0/2
[SwitchA-vlan3] quit
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/1
[SwitchA-vlan2] quit
```

手工指定 VLAN 接口 2 的全球单播地址。

```
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ipv6 address 3001::1/64
[SwitchA-Vlan-interface2] quit
```

手工指定 VLAN 接口 3 的全球单播地址，并允许其发布 RA 消息。

```
[SwitchA] interface vlan-interface 3
[SwitchA-Vlan-interface3] ipv6 address 2001::1/64
[SwitchA-Vlan-interface3] undo ipv6 nd ra halt
```

配置 VLAN 接口 3 引用 DHCP 地址池。

```
[SwitchA-Vlan-interface3] ipv6 dhcp server apply pool 1 allow-hint rapid-commit
```

配置被管理地址的配置标志位为 1，即主机通过 DHCPv6 服务器获取 IPv6 地址。配置其他信息配置标志位为 1，即主机通过 DHCPv6 服务器获取除 IPv6 地址以外的其他信息。

```
[SwitchA-Vlan-interface3] ipv6 nd autoconfig managed-address-flag
[SwitchA-Vlan-interface3] ipv6 nd autoconfig other-flag
```

配置接口 VLAN 接口 3 工作在 DHCPv6 服务器模式。

```
[SwitchA-Vlan-interface3] ipv6 dhcp select server
[SwitchA-Vlan-interface3] quit
```

配置 DHCPv6 地址池 1。

```
[SwitchA] ipv6 dhcp pool 1
[SwitchA-dhcp6-pool-1] network 2001::/64
[SwitchA-dhcp6-pool-1] dns-server 1::1
[SwitchA-dhcp6-pool-1] quit
```

配置 IPv6 静态路由，该路由的目的地址为 4001::/64，下一跳地址为 3001::2。

```
[SwitchA] ipv6 route-static 4001:: 64 3001::2
```

保存配置。

```
[SwitchA] save force
```

2. 配置 Switch B

创建 VLAN，在 VLAN 中加入对应的端口。

```
<SwitchB> system-view
[SwitchB] vlan 2
[SwitchB-vlan2] port gigabitethernet 1/0/1
[SwitchB-vlan2] quit
[SwitchB] vlan 3
[SwitchB-vlan3] port gigabitethernet 1/0/2
[SwitchB-vlan3] quit
```

手工指定 VLAN 接口 2 的全球单播地址。

```
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ipv6 address 3001::2/64
[SwitchB-Vlan-interface2] quit
```

手工指定 VLAN 接口 3 的全球单播地址，并允许其发布 RA 消息。

```
[SwitchB] interface vlan-interface 3
[SwitchB-Vlan-interface3] ipv6 address 4001::1/64
[SwitchB-Vlan-interface3] undo ipv6 nd ra halt
```

配置 VLAN 接口 3 引用 DHCP 地址池。

```
[SwitchB-Vlan-interface3] ipv6 dhcp server apply pool 1 allow-hint rapid-commit
```

配置被管理地址的配置标志位为 1，即主机通过 DHCPv6 服务器获取 IPv6 地址。配置其他信息配置标志位为 1，即主机通过 DHCPv6 服务器获取除 IPv6 地址以外的其他信息。

```
[SwitchB-Vlan-interface3] ipv6 nd autoconfig managed-address-flag
[SwitchB-Vlan-interface3] ipv6 nd autoconfig other-flag
```

配置接口 VLAN 接口 3 工作在 DHCPv6 服务器模式。

```
[SwitchB-Vlan-interface3] ipv6 dhcp select server
[SwitchB-Vlan-interface3] quit
```

配置 DHCPv6 地址池 1。

```
[SwitchB] ipv6 dhcp pool 1
[SwitchB-dhcp6-pool-1] network 4001::/64
[SwitchB-dhcp6-pool-1] dns-server 1::1
[SwitchB-dhcp6-pool-1] quit
```

配置 IPv6 静态路由，该路由的目的地址为 2001::/64，下一跳地址为 3001::1。

```
[SwitchB] ipv6 route-static 2001:: 64 3001::1
```

保存配置。

```
[SwitchB] save force
```

3. 配置 Host A

在 Host A 上安装 IPv6，并配置自动获取 IPv6 地址。

4. 配置 Host B

在 Host B 上安装 IPv6，并配置自动获取 IPv6 地址。

4.4 验证配置

1. 显示 DHCPv6 服务器的配置

显示 DHCPv6 地址池的信息。

```
[SwitchA] display ipv6 dhcp server ip-in-use
DHCPv6 pool: 1
  Network: 2001::/64
    Preferred lifetime 604800 seconds, valid lifetime 2592000 seconds
  DNS server addresses:
    1::1
  IP-in-use threshold: 100
  PD-in-use threshold: 100
```

显示接口上的 DHCPv6 服务器信息。

```
[SwitchA] displsy ipv6 dhcp server
Interface                       Pool
Vlan-interface3                 1
```

2. 显示和清除 DHCPv6 服务器的地址绑定信息

在 Switch A 上查看 DHCPv6 服务器为客户端分配的 IPv6 地址。

```
[SwitchA] display ipv6 dhcp server ip-in-use
Pool: 1
 IPv6 address                              Type      Lease expiration
 2001::2                                   Auto(C)   Sep 30 11:45:07 2021
```

从 Switch A 上查看端口 GigabitEthernet1/0/2 的邻居信息。

```
[SwitchA] display ipv6 neighbors interface gigabitethernet 1/0/2
Type: S-Static    D-Dynamic    O-Openflow     R-Rule    IS-Invalid static
IPv6 address              MAC address    VLAN/VSI   Interface     State T  Aging
2001::2                   b025-0b54-0106 --         GE1/0/2       REACH D  29
FE80::B225:BFF:FE54:106   b025-0b54-0106 --         GE1/0/2       REACH D  18
```

通过上面的信息可以知道 Host A 上获得的 IPv6 全球单播地址为 2001::2。

显示租约过期的 DHCPv6 地址绑定信息。

```
[SwitchA] display ipv6 dhcp server expired
IPv6 address           DUID                          Lease expiration
2001::3                0262-9ead-ab03-00             Feb 17 17:09:02 2023
```

清除 DHCPv6 的正式地址绑定和临时地址绑定信息。并再次查看 DHCPv6 服务器为客户端分配的 IPv6 地址

```
[SwitchA] quit
<SwitchA> reset ipv6 dhcp server ip-in-use
<SwitchA> display ipv6 dhcp server ip-in-use
```

清除租约过期的 DHCPv6 地址绑定信息。并再次查看租约过期的 DHCPv6 地址绑定信息

```
<SwitchA> reset ipv6 dhcp server expired
<SwitchA> display ipv6 dhcp server expired
IPv6 address           DUID                          Lease expiration
```

3. 显示和清除 DHCPv6 服务器的报文统计信息

显示 DHCPv6 服务器的报文统计信息。

```
<SwitchA> display ipv6 dhcp server statistics
Bindings:
    Ip-in-use               :  0
    Pd-in-use               :  0
    Expired                 :  1
Conflict                    :  1
Packets received            :  24
    Solicit                 :  8
    Request                 :  8
    Confirm                 :  0
    Renew                   :  0
    Rebind                  :  0
    Release                 :  8
    Decline                 :  0
    Information-request     :  0
    Relay-forward           :  0
Packets dropped             :  0
Packets sent                :  24
    Advertise               :  8
    Reconfigure             :  0
    Reply                   :  16
    Relay-reply             :  0
```

在用户视图下执行 **reset ipv6 dhcp server statistics** 命令，可以清除该统计信息。

```
<SwitchA> reset ipv6 dhcp server statistics
<SwitchA> display ipv6 dhcp server statistics
Bindings:
    Ip-in-use               :  0
    Pd-in-use               :  0
    Expired                 :  1
Conflict                    :  1
Packets received            :  0
    Solicit                 :  0
```

```
    Request                  :  0
    Confirm                  :  0
    Renew                    :  0
    Rebind                   :  0
    Release                  :  0
    Decline                  :  0
    Information-request      :  0
    Relay-forward            :  0
Packets dropped              :  0
Packets sent                 :  0
    Advertise                :  0
    Reconfigure              :  0
    Reply                    :  0
    Relay-reply              :  0
```

在 Switch B 上查看 DHCPv6 服务器为客户端分配的 IPv6 地址

```
[SwitchB] display ipv6 dhcp server ip-in-use
Pool: 1
 IPv6 address                                Type      Lease expiration
 4001::2                                     Auto(C)   Sep 30 14:05:49 2021
```

从 Switch B 上查看端口 GigabitEthernet1/0/2 的邻居信息。

```
[SwitchB] display ipv6 neighbors interface gigabitethernet 1/0/2
Type: S-Static    D-Dynamic    O-Openflow     R-Rule    IS-Invalid static
IPv6 address              MAC address    VLAN/VSI   Interface     State T  Aging
4001::2                   b043-5415-0406 --         GE1/0/2       REACH D  3
FE80::B243:54FF:FE15:406  b043-5415-0406 --         GE1/0/2       REACH D  44
```

通过上面的信息可以知道 Host B 上获得的 IPv6 全球单播地址为 4001::2。

从 Host A 上也可以 ping 通 Host B，证明它们是互通的。

4.5 配置文件

- Switch A：

```
#
vlan 2 to 3
#
ipv6 dhcp pool 1
 network 2001::/64
 dns-server 1::1
#
interface Vlan-interface3
 ipv6 dhcp select server
 ipv6 dhcp server apply pool 1 allow-hint rapid-commit
 ipv6 address 2001::1/64
 ipv6 nd autoconfig managed-address-flag
 ipv6 nd autoconfig other-flag
 undo ipv6 nd ra halt
#
interface Vlan-interface2
```

```
 ipv6 address 3001::1/64
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 3
#
 ipv6 route-static 4001:: 64 3001::2
#
```

- Switch B：

```
#
vlan 2 to 3
#
ipv6 dhcp pool 1
 network 4001::/64
 dns-server 1::1
#
interface Vlan-interface2
 ipv6 address 3001::2/64
#
interface Vlan-interface3
 ipv6 dhcp select server
 ipv6 dhcp server apply pool 1 allow-hint rapid-commit
 ipv6 address 4001::1/64
 ipv6 nd autoconfig managed-address-flag
 ipv6 nd autoconfig other-flag
 undo ipv6 nd ra halt
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 3
#
 ipv6 route-static 2001:: 64 3001::1
#
```

4.6 相关资料

- 产品配套“三层技术-IP 业务配置指导”中的“DHCPv6”。
- 产品配套“三层技术-IP 业务命令参考”中的“DHCPv6”

OSPF 快速配置指南

目 录

1 配置 OSPF 引入自治系统外部路由

1.1 简介

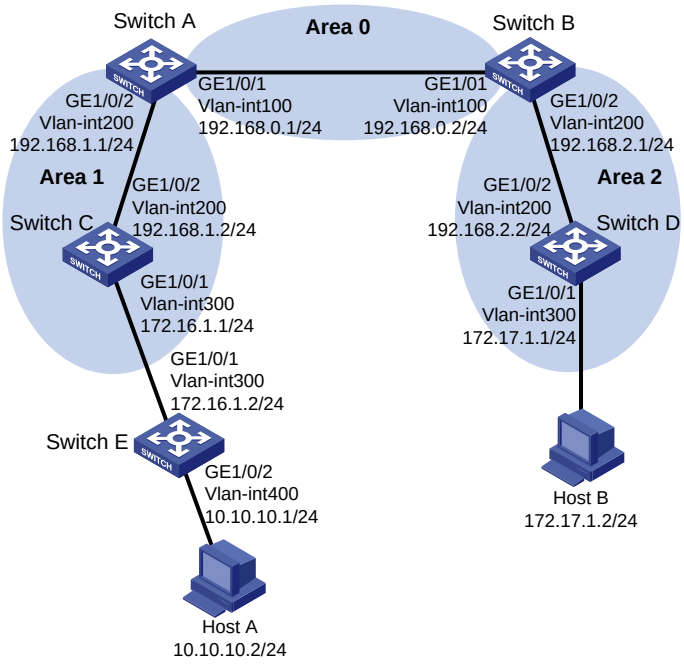
本案例介绍 OSPF 引入自治系统外部路由的配置方法。

1.2 组网需求

如图 1 所示，Switch A、Switch B、Switch C 和 Switch D 运行 OSPF；Switch C 和 Switch E 运行静态路由。整个自治系统划分为 3 个区域。具体应用需求如下：

- Switch A 和 Switch B 作为 ABR 来转发区域之间的路由。
- Switch C 作为 ASBR 引入外部路由（静态路由），要求路由信息可正确的在 AS 内传播。

图1 OSPF 引入自治系统外部路由组网图



1.3 数据规划

设备	Router ID	接口和 IP 地址	网段和区域
Switch A	1.1.1.1	物理接口：GE1/0/1 VLAN：100 IP 地址：192.168.0.1/24	网段：192.168.0.0/24 区域：area 0
		物理接口：GE1/0/2 VLAN：200 IP 地址：192.168.1.1/24	网段：192.168.1.0/24 区域：area 1

设备	Router ID	接口和 IP 地址	网段和区域
Switch B	2.2.2.2	物理接口：GE1/0/1 VLAN：100 IP 地址：192.168.0.2/24	网段：192.168.0.0/24 区域：area 0
		物理接口：GE1/0/2 VLAN：200 IP 地址：192.168.2.1/24	网段：192.168.2.0/24 区域：area 2
Switch C	3.3.3.3	物理接口：GE1/0/1 VLAN：300 IP 地址：172.16.1.1/24	网段：172.16.1.0/24 区域：area 1
		物理接口：GE1/0/2 VLAN：200 IP 地址：192.168.1.2/24	网段：192.168.1.0/24 区域：area 1
Switch D	4.4.4.4	物理接口：GE1/0/1 VLAN：300 IP 地址：172.17.1.1/24	网段：172.17.1.0/24 区域：area 2
		物理接口：GE1/0/2 VLAN：200 IP 地址：192.168.2.2/24	网段：192.168.2.0/24 区域：area 2
Switch E	-	物理接口：GE1/0/1 VLAN：300 IP 地址：172.16.1.2/24	网段：172.16.1.0/24
		物理接口：GE1/0/2 VLAN：400 IP 地址：10.10.10.1/24	网段：10.10.10.0/24
Host A	-	IP 地址：10.10.10.2/24	网段：10.10.10.0/24
Host B	-	IP 地址：172.17.1.2/24	网段：172.17.1.0/24

1.4 配置步骤

1. Switch A 的配置

创建 VLAN 100 和 VLAN 200，将接口 GE1/0/1 加入 VLAN 100、接口 GE1/0/2 加入 VLAN 200，并配置 VLAN 100 的 IP 地址为 192.168.0.1/24，VLAN 200 的 IP 地址为 192.168.1.1/24。

```
<Switch A> system-view
[Switch A] vlan 100
[Switch A-vlan100] port gigabitethernet 1/0/1
[Switch A-vlan100] quit
```

```
[Switch A] vlan 200
[Switch A-vlan200] port gigabitethernet 1/0/2
[Switch A-vlan200] quit
[Switch A] interface vlan 100
[Switch A-Vlan-interface100] ip address 192.168.0.1 255.255.255.0
[Switch A-Vlan-interface100] quit
[Switch A] interface vlan 200
[Switch A-Vlan-interface200] ip address 192.168.1.1 255.255.255.0
[Switch A-Vlan-interface200] quit
```

配置全局 Router ID 为 1.1.1.1。

```
[Switch A] router id 1.1.1.1
```

启动 OSPF 进程 1，创建区域 0，并通告 192.168.0.0/24 网段；创建区域 1，并通告 192.168.1.0/24 网段。

```
[Switch A] ospf 1
[Switch A-ospf-1] area 0
[Switch A-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[Switch A-ospf-1-area-0.0.0.0] quit
[Switch A-ospf-1] area 1
[Switch A-ospf-1-area-0.0.0.1] network 192.168.1.0 0.0.0.255
[Switch A-ospf-1] quit
```

保存配置。

```
[Switch A] save force
```

2. Switch B 的配置

创建 VLAN 100 和 VLAN 200，将接口 GE1/0/1 加入 VLAN 100、接口 GE1/0/2 加入 VLAN 200，并配置 VLAN 100 的 IP 地址为 192.168.0.2/24，VLAN 200 的 IP 地址为 192.168.2.1/24。

```
<Switch B> system-view
[Switch B] vlan 100
[Switch B-vlan100] port gigabitethernet 1/0/1
[Switch B-vlan100] quit
[Switch B] vlan 200
[Switch B-vlan200] port gigabitethernet 1/0/2
[Switch B-vlan200] quit
[Switch B] interface vlan 100
[Switch B-Vlan-interface100] ip address 192.168.0.2 255.255.255.0
[Switch B-Vlan-interface100] quit
[Switch B] interface vlan 200
[Switch B-Vlan-interface200] ip address 192.168.2.1 255.255.255.0
[Switch B-Vlan-interface200] quit
```

配置全局 Router ID 为 2.2.2.2。

```
[Switch B] router id 2.2.2.2
```

启动 OSPF 进程 1，创建区域 0，并通告 192.168.0.0/24 网段；创建区域 2，并通告 192.168.2.0/24 网段。

```
[Switch B] ospf 1
[Switch B-ospf-1] area 0
[Switch B-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
```

```
[Switch B-ospf-1-area-0.0.0.0] quit
[Switch B-ospf-1] area 2
[Switch B-ospf-1-area-0.0.0.2] network 192.168.2.0 0.0.0.255
[Switch B-ospf-1-area-0.0.0.2] quit
[Switch B-ospf-1] quit
```

保存配置。

```
[Switch B] save force
```

3. Switch C 的配置

创建 VLAN 200 和 VLAN 300，将接口 GE1/0/1 加入 VLAN 300、接口 GE1/0/2 加入 VLAN 200，并配置 VLAN 300 的 IP 地址为 172.16.1.1/24，VLAN 200 的 IP 地址为 192.168.1.2/24。

```
<Switch C> system-view
[Switch C] vlan 300
[Switch C-vlan300] port gigabitethernet 1/0/1
[Switch C-vlan300] quit
[Switch C] vlan 200
[Switch C-vlan200] port gigabitethernet 1/0/2
[Switch C-vlan200] quit
[Switch C] interface vlan 300
[Switch C-Vlan-interface300] ip address 172.16.1.1 255.255.255.0
[Switch C-Vlan-interface300] quit
[Switch C] interface vlan 200
[Switch C-Vlan-interface200] ip address 192.168.1.2 255.255.255.0
[Switch C-Vlan-interface200] quit
```

配置静态路由，其目的网段为 10.10.10.0/24，下一跳为 172.16.1.2。

```
[Switch C] ip route-static 10.10.10.0 24 172.16.1.2
```

配置全局 Router ID 为 3.3.3.3。

```
[Switch C] router id 3.3.3.3
```

启动 OSPF 进程 1，创建区域 1，并通告 192.168.1.0/24 网段和 172.16.1.0/24 网段。

```
[Switch C] ospf 1
[Switch C-ospf-1] area 1
[Switch C-ospf-1-area-0.0.0.1] network 192.168.1.0 0.0.0.255
[Switch C-ospf-1-area-0.0.0.1] network 172.16.1.0 0.0.0.255
[Switch C-ospf-1-area-0.0.0.1] quit
```

配置 OSPF 引入静态路由。

```
[Switch C-ospf-1] import-route static
[Switch C-ospf-1] quit
```

保存配置。

```
[Switch C] save force
```

4. Switch D 的配置

创建 VLAN 200 和 VLAN 300，将接口 GE1/0/1 加入 VLAN 300、接口 GE1/0/2 加入 VLAN 200，并配置 VLAN 300 的 IP 地址为 172.17.1.1/24，VLAN 200 的 IP 地址为 192.168.2.2/24。

```
<Switch D> system-view
[Switch D] vlan 300
[Switch D-vlan300] port gigabitethernet 1/0/1
```

```
[Switch D-vlan300] quit
[Switch D] vlan 200
[Switch D-vlan200] port gigabitethernet 1/0/2
[Switch D-vlan200] quit
[Switch D] interface vlan 300
[Switch D-Vlan-interface300] ip address 172.17.1.1 255.255.255.0
[Switch D-Vlan-interface300] quit
[Switch D] interface vlan 200
[Switch D-Vlan-interface200] ip address 192.168.2.2 255.255.255.0
[Switch D-Vlan-interface200] quit
```

配置全局 Router ID 为 4.4.4.4。

```
[Switch D] router id 4.4.4.4
```

启动 OSPF 进程 1，创建区域 2，并通告 192.168.2.0/24 网段和 172.17.1.0/24 网段。

```
[Switch D] ospf 1
[Switch D-ospf-1] area 2
[Switch D-ospf-1-area-0.0.0.2] network 192.168.2.0 0.0.0.255
[Switch D-ospf-1-area-0.0.0.2] network 172.17.1.0 0.0.0.255
[Switch D-ospf-1-area-0.0.0.2] quit
[Switch D-ospf-1] quit
```

保存配置。

```
[Switch D] save force
```

5. Switch E 的配置

创建 VLAN 300 和 VLAN 400，将接口 GE1/0/1 加入 VLAN 300、接口 GE1/0/2 加入 VLAN 400，并配置 VLAN 300 的 IP 地址为 172.16.1.2/24，VLAN 400 的 IP 地址为 10.10.10.1/24。

```
<Switch E> system-view
[Switch E] vlan 300
[Switch E-vlan300] port gigabitethernet 1/0/1
[Switch E-vlan300] quit
[Switch E] vlan 400
[Switch E-vlan400] port gigabitethernet 1/0/2
[Switch E-vlan400] quit
[Switch E] interface vlan 300
[Switch E-Vlan-interface300] ip address 172.16.1.2 255.255.255.0
[Switch E-Vlan-interface300] quit
[Switch E] interface vlan 400
[Switch E-Vlan-interface400] ip address 10.10.10.1 255.255.255.0
[Switch E-Vlan-interface400] quit
```

配置缺省路由，下一跳为 172.16.1.1。

```
[Switch E] ip route-static 0.0.0.0 0 172.16.1.1
```

保存配置。

```
[Switch E] save force
```

1.5 验证配置

查看 Switch A 的路由表，存在到 172.16.1.0、172.17.1.0、192.168.2.0 的路由，以及学习到的外部引入的静态路由。

```
[Switch A] display ip routing-table
Destinations : 20       Routes : 20

Destination/Mask    Proto   Pre Cost        NextHop         Interface

0.0.0.0/32          Direct  0   0           127.0.0.1       InLoop0
10.10.10.0/24       O_ASE2  150 1           192.168.1.2     Vlan200
127.0.0.0/8         Direct  0   0           127.0.0.1       InLoop0
127.0.0.0/32        Direct  0   0           127.0.0.1       InLoop0
127.0.0.1/32        Direct  0   0           127.0.0.1       InLoop0
127.255.255.255/32  Direct  0   0           127.0.0.1       InLoop0
172.16.1.0/24       O_INTRA 10  2           192.168.1.2     Vlan200
172.17.1.0/24       O_INTER 10  3           192.168.0.2     Vlan100
192.168.0.0/24      Direct  0   0           192.168.0.1     Vlan100
192.168.0.0/32      Direct  0   0           192.168.0.1     Vlan100
192.168.0.1/32      Direct  0   0           127.0.0.1       InLoop0
192.168.0.255/32    Direct  0   0           192.168.0.1     Vlan100
192.168.1.0/24      Direct  0   0           192.168.1.1     Vlan200
192.168.1.0/32      Direct  0   0           192.168.1.1     Vlan200
192.168.1.1/32      Direct  0   0           127.0.0.1       InLoop0
192.168.1.255/32    Direct  0   0           192.168.1.1     Vlan200
192.168.2.0/24      O_INTER 10  2           192.168.0.2     Vlan100
224.0.0.0/4         Direct  0   0           0.0.0.0         NULL0
224.0.0.0/24        Direct  0   0           0.0.0.0         NULL0
255.255.255.255/32  Direct  0   0           127.0.0.1       InLoop0
```

Host A 可以 ping 通 Host B。

```
C:\Users\HostA>ping 172.17.1.2
正在 Ping 172.17.1.2 具有 32 字节的数据:
来自 172.17.1.2 的回复: 字节=32 时间=3ms TTL=255
来自 172.17.1.2 的回复: 字节=32 时间=1ms TTL=255
来自 172.17.1.2 的回复: 字节=32 时间<1ms TTL=255
来自 172.17.1.2 的回复: 字节=32 时间=2ms TTL=255

172.17.1.2 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 = 0ms，最长 = 3ms，平均 = 1ms
```

1.6 配置文件

- Switch A：

```
#
 router id 1.1.1.1
```

```
#
ospf 1
 area 0.0.0.0
  network 192.168.0.0 0.0.0.255
 area 0.0.0.1
  network 192.168.1.0 0.0.0.255
#
interface Vlan-interface100
 ip address 192.168.0.1 255.255.255.0
#
interface Vlan-interface200
 ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port access vlan 200
#
```

- Switch B：

```
#
 router id 2.2.2.2
#
ospf 1
 area 0.0.0.0
  network 192.168.0.0 0.0.0.255
 area 0.0.0.2
  network 192.168.2.0 0.0.0.255
#
interface Vlan-interface100
 ip address 192.168.0.2 255.255.255.0
#
interface Vlan-interface200
 ip address 192.168.2.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port access vlan 200
#
```

- Switch C：

```
#
 router id 3.3.3.3
#
ospf 1
 area 0.0.0.1
  network 192.168.1.0 0.0.0.255
```

```
  network 172.16.1.0 0.0.0.255
#
interface Vlan-interface200
 ip address 192.168.1.2 255.255.255.0
#
interface Vlan-interface300
 ip address 172.16.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port access vlan 300
#
interface GigabitEthernet1/0/2
 port access vlan 200
#
```

- Switch D：

```
#
 router id 4.4.4.4
#
ospf 1
 area 0.0.0.2
  network 192.168.2.0 0.0.0.255
  network 172.17.1.0 0.0.0.255
#
interface Vlan-interface200
 ip address 192.168.2.2 255.255.255.0
#
interface Vlan-interface300
 ip address 172.17.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port access vlan 300
#
interface GigabitEthernet1/0/2
 port access vlan 200

#
```

- Switch E：

```
#
interface Vlan-interface200
 ip address 10.10.10.1 255.255.255.0
#
interface Vlan-interface300
 ip address 172.16.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port access vlan 300
#
interface GigabitEthernet1/0/2
```

```
 port access vlan 200
#
 ip route-static 0.0.0.0 0 172.16.1.1
#
```

1.7 相关资料

- 产品配套“三层技术-IP 路由配置指导”中的“OSPF”。
- 产品配套“三层技术-IP 路由命令参考”中的“OSPF”。

2 单区域 OSPF 基本功能配置

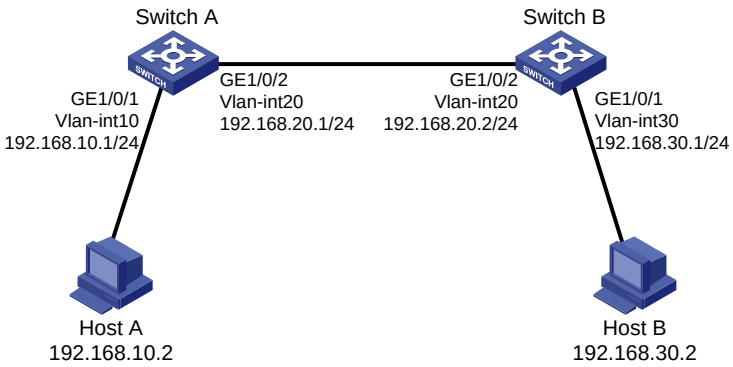
2.1 简介

本案例介绍单区域 OSPF 基本功能的配置方法。

2.2 组网需求

如图 2 所示，Switch A 和 Switch B 运行 OSPF，要求 Host A 和 Host B 通过运行 OSPF 协议的 Switch A 和 Switch B 实现互联互通。

图2 单区域 OSPF 基本功能组网图



2.3 配置步骤

1. Switch A 的配置

创建 VLAN 10 和 VLAN 20，将接口 GE1/0/1 加入 VLAN 10、接口 GE1/0/2 加入 VLAN 20，并配置 VLAN 10 的 IP 地址为 192.168.10.1/24，VLAN 20 的 IP 地址为 192.168.20.1/24。

```
<Switch A> system-view
[Switch A] vlan 10
[Switch A-vlan10] port gigabitethernet 1/0/1
[Switch A-vlan10] quit
[Switch A] vlan 20
[Switch A-vlan20] port gigabitethernet 1/0/2
[Switch A-vlan20] quit
[Switch A] interface vlan 10
[Switch A-Vlan-interface10] ip address 192.168.10.1 255.255.255.0
[Switch A-Vlan-interface10] quit
[Switch A] interface vlan 20
[Switch A-Vlan-interface20] ip address 192.168.20.1 255.255.255.0
[Switch A-Vlan-interface20] quit
```

配置全局 Router ID 为 1.1.1.1。

```
[Switch A] router id 1.1.1.1
```

启动 OSPF 进程 1，创建区域 0，并通告 192.168.10.0/24 网段和 192.168.20.0/24 网段。

```
[Switch A] ospf 1
[Switch A-ospf-1] area 0
[Switch A-ospf-1-area-0.0.0.0] network 192.168.10.0 0.0.0.255
[Switch A-ospf-1-area-0.0.0.0] network 192.168.20.0 0.0.0.255
[Switch A-ospf-1-area-0.0.0.0] quit
[Switch A-ospf-1] quit
```

保存配置。

```
[Switch A] save force
```

2. Switch B 的配置

创建 VLAN 20 和 VLAN 30，将接口 GE1/0/1 加入 VLAN 30、接口 GE1/0/2 加入 VLAN 20，并配置 VLAN 30 的 IP 地址为 192.168.30.1/24，VLAN 20 的 IP 地址为 192.168.20.2/24。

```
<Switch B> system-view
[Switch B] vlan 30
[Switch B-vlan30] port gigabitethernet 1/0/1
[Switch B-vlan30] quit
[Switch B] vlan 20
[Switch B-vlan20] port gigabitethernet 1/0/2
[Switch B-vlan20] quit
[Switch B] interface vlan 30
[Switch B-Vlan-interface30] ip address 192.168.30.1 255.255.255.0
[Switch B-Vlan-interface30] quit
[Switch B] interface vlan 20
[Switch B-Vlan-interface20] ip address 192.168.20.2 255.255.255.0
[Switch B-Vlan-interface20] quit
```

配置全局 Router ID 为 2.2.2.2。

```
[Switch B] router id 2.2.2.2
```

启动 OSPF 进程 1，创建区域 0，并通告 192.168.20.0/24 网段和 192.168.30.0/24 网段。

```
[Switch B] ospf 1
[Switch B-ospf-1] area 0
[Switch B-ospf-1-area-0.0.0.0] network 192.168.20.0 0.0.0.255
[Switch B-ospf-1-area-0.0.0.0] network 192.168.30.0 0.0.0.255
[Switch B-ospf-1-area-0.0.0.0] quit
[Switch B-ospf-1] quit
```

保存配置。

```
[Switch B] save force
```

2.4 验证配置

查看 Switch A 的 OSPF 邻居。

```
[Switch A] display ospf peer

         OSPF Process 1 with Router ID 1.1.1.1
               Neighbor Brief Information

 Area: 0.0.0.0
```

```
 Router ID       Address         Pri Dead-Time  State             Interface
 2.2.2.2         192.168.20.2    1   30         Full/DR -         Vlan20
```

查看 Switch A 的 OSPF 路由信息。

```
[Switch A] display ospf routing

         OSPF Process 1 with Router ID 1.1.1.1

                  Routing Table

                Topology base (MTID 0)

 Routing for network

 Destination        Cost     Type    NextHop         AdvRouter       Area
 192.168.10.0/24    1        Stub    0.0.0.0         192.168.20.1    0.0.0.0
 192.168.30.0/24    2        Stub    192.168.20.2    192.168.20.2    0.0.0.0
 192.168.20.0/24    1        Transit 0.0.0.0         192.168.20.1    0.0.0.0
```

查看 Switch A 的路由表信息，存在到达 192.168.30.0/24 网段的路由。

```
[Switch A] display ip routing-table

Destinations : 17       Routes : 17

Destination/Mask   Proto   Pre Cost        NextHop         Interface

0.0.0.0/32         Direct  0   0           127.0.0.1       InLoop0
127.0.0.0/8        Direct  0   0           127.0.0.1       InLoop0
127.0.0.0/32       Direct  0   0           127.0.0.1       InLoop0
127.0.0.1/32       Direct  0   0           127.0.0.1       InLoop0
127.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
192.168.10.0/24    Direct  0   0           192.168.10.1    Vlan10
192.168.10.0/32    Direct  0   0           192.168.10.1    Vlan10
192.168.10.1/32    Direct  0   0           127.0.0.1       InLoop0
192.168.10.255/32  Direct  0   0           192.168.10.1    Vlan10
192.168.20.0/24    Direct  0   0           192.168.20.1    Vlan20
192.168.20.0/32    Direct  0   0           192.168.20.1    Vlan20
192.168.20.1/32    Direct  0   0           127.0.0.1       InLoop0
192.168.20.255/32  Direct  0   0           192.168.20.1    Vlan20
192.168.30.0/24    O_INTRA 10  2           192.168.20.2    Vlan20
224.0.0.0/4        Direct  0   0           0.0.0.0         NULL0
224.0.0.0/24       Direct  0   0           0.0.0.0         NULL0
255.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
```

Host A 可以 ping 通 Host B。

```
C:\Users\HostA>ping 192.168.30.2
正在 Ping 192.168.30.2 具有 32 字节的数据:
来自 192.168.30.2 的回复: 字节=32 时间=3ms TTL=255
来自 192.168.30.2 的回复: 字节=32 时间=1ms TTL=255
来自 192.168.30.2 的回复: 字节=32 时间<1ms TTL=255
```

```
来自 192.168.30.2 的回复: 字节=32 时间=2ms TTL=255

192.168.30.2 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 = 2ms，最长 = 3ms，平均 = 2ms
```

2.5 配置文件

- Switch A：

```
#
 router id 1.1.1.1
#
ospf 1
 area 0.0.0.0
  network 192.168.10.0 0.0.0.255
  network 192.168.20.0 0.0.0.255
#
interface Vlan-interface10
 ip address 192.168.10.1 255.255.255.0
#
interface Vlan-interface20
 ip address 192.168.20.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port access vlan 10
#
interface GigabitEthernet1/0/2
 port access vlan 20
#
```

- Switch B：

```
#
 router id 2.2.2.2
#
ospf 1
 area 0.0.0.0
  network 192.168.20.0 0.0.0.255
  network 192.168.30.0 0.0.0.255
#
interface Vlan-interface20
 ip address 192.168.20.2 255.255.255.0
#
interface Vlan-interface30
 ip address 192.168.30.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port access vlan 30
#
```

```
interface GigabitEthernet1/0/2
 port access vlan 20
#
```

2.6 相关资料

- 产品配套“三层技术-IP 路由配置指导”中的“OSPF”。
- 产品配套“三层技术-IP 路由命令参考”中的“OSPF”。

3 多区域 OSPF 基本功能配置

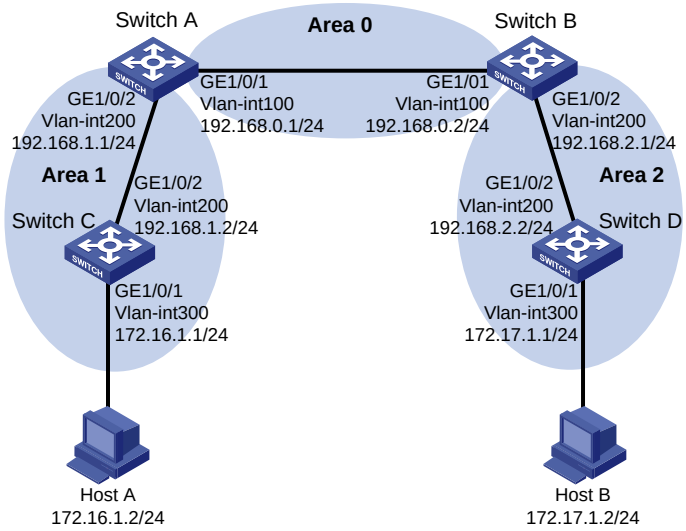
3.1 简介

本案例介绍多区域 OSPF 基本功能的配置方法。

3.2 组网需求

如图 3 所示，Switch A、Switch B、Switch C、Switch D 都运行 OSPF，并将整个自治系统划分为 3 个区域。其中 Switch A 和 Switch B 作为 ABR 来转发区域之间的路由。配置完成后，每台交换机都应学到 AS 内的到所有网段的路由。

图3 多区域 OSPF 基本功能组网图



3.3 数据规划

设备	Router ID	接口和 IP 地址	网段和区域
Switch A	1.1.1.1	物理接口：GE1/0/1 VLAN：100 IP 地址：192.168.0.1/24	网段：192.168.0.0/24 区域：area 0
		物理接口：GE1/0/2 VLAN：200 IP 地址：192.168.1.1/24	网段：192.168.1.0/24 区域：area 1
Switch B	2.2.2.2	物理接口：GE1/0/1 VLAN：100 IP 地址：192.168.0.2/24	网段：192.168.0.0/24 区域：area 0
		物理接口：GE1/0/2	网段：192.168.2.0/24

设备	Router ID	接口和 IP 地址	网段和区域
		VLAN：200 IP 地址：192.168.2.1/24	区域：area 2
Switch C	3.3.3.3	物理接口：GE1/0/1 VLAN：300 IP 地址：172.16.1.1/24	网段：172.16.1.0/24 区域：area 1
		物理接口：GE1/0/2 VLAN：200 IP 地址：192.168.1.2/24	网段：192.168.1.0/24 区域：area 1
Switch D	4.4.4.4	物理接口：GE1/0/1 VLAN：300 IP 地址：172.17.1.1/24	网段：172.17.1.0/24 区域：area 2
		物理接口：GE1/0/2 VLAN：200 IP 地址：192.168.2.2/24	网段：192.168.2.0/24 区域：area 2
Host A	-	IP 地址：172.16.1.2/24	网段：172.16.1.0/24
Host B	-	IP 地址：172.17.1.2/24	网段：172.17.1.0/24

3.4 配置步骤

1. Switch A 的配置

创建 VLAN 100 和 VLAN 200，将接口 GE1/0/1 加入 VLAN 100、接口 GE1/0/2 加入 VLAN 200，并配置 VLAN 100 的 IP 地址为 192.168.0.1/24，VLAN 200 的 IP 地址为 192.168.1.1/24。

```
<Switch A> system-view
[Switch A] vlan 100
[Switch A-vlan100] port gigabitethernet 1/0/1
[Switch A-vlan100] quit
[Switch A] vlan 200
[Switch A-vlan200] port gigabitethernet 1/0/2
[Switch A-vlan200] quit
[Switch A] interface vlan 100
[Switch A-Vlan-interface100] ip address 192.168.0.1 255.255.255.0
[Switch A-Vlan-interface100] quit
[Switch A] interface vlan 200
[Switch A-Vlan-interface200] ip address 192.168.1.1 255.255.255.0
[Switch A-Vlan-interface200] quit
```

配置全局 Router ID 为 1.1.1.1。

```
[Switch A] router id 1.1.1.1
```

启动 OSPF 进程 1，创建区域 0，并通告 192.168.0.0/24 网段；创建区域 1，并通告 192.168.1.0/24 网段。

```
[Switch A] ospf 1
[Switch A-ospf-1] area 0
[Switch A-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[Switch A-ospf-1-area-0.0.0.0] quit
[Switch A-ospf-1] area 1
[Switch A-ospf-1-area-0.0.0.1] network 192.168.1.0 0.0.0.255
[Switch A-ospf-1-area-0.0.0.1] quit
[Switch A-ospf-1] quit
```

保存配置。

```
[Switch A] save force
```

2. Switch B 的配置

创建 VLAN 100 和 VLAN 200，将接口 GE1/0/1 加入 VLAN 100、接口 GE1/0/2 加入 VLAN 200，并配置 VLAN 100 的 IP 地址为 192.168.0.2/24，VLAN 200 的 IP 地址为 192.168.2.1/24。

```
<Switch B> system-view
[Switch B] vlan 100
[Switch B-vlan100] port gigabitethernet 1/0/1
[Switch B-vlan100] quit
[Switch B] vlan 200
[Switch B-vlan200] port gigabitethernet 1/0/2
[Switch B-vlan200] quit
[Switch B] interface vlan 100
[Switch B-Vlan-interface100] ip address 192.168.0.2 255.255.255.0
[Switch B-Vlan-interface100] quit
[Switch B] interface vlan 200
[Switch B-Vlan-interface200] ip address 192.168.2.1 255.255.255.0
[Switch B-Vlan-interface200] quit
```

配置全局 Router ID 为 2.2.2.2。

```
[Switch B] router id 2.2.2.2
```

启动 OSPF 进程 1，创建区域 0，并通告 192.168.0.0/24 网段；创建区域 2，并通告 192.168.2.0/24 网段。

```
[Switch B] ospf 1
[Switch B-ospf-1] area 0
[Switch B-ospf-1-area-0.0.0.0] network 192.168.0.0 0.0.0.255
[Switch B-ospf-1-area-0.0.0.0] quit
[Switch B-ospf-1] area 2
[Switch B-ospf-1-area-0.0.0.2] network 192.168.2.0 0.0.0.255
[Switch B-ospf-1-area-0.0.0.2] quit
[Switch B-ospf-1] quit
```

保存配置。

```
[Switch B] save force
```

3. Switch C 的配置

创建 VLAN 200 和 VLAN 300，将接口 GE1/0/1 加入 VLAN 300、接口 GE1/0/2 加入 VLAN 200，并配置 VLAN 300 的 IP 地址为 172.16.1.1/24，VLAN 200 的 IP 地址为 192.168.1.2/24。

```
<Switch C> system-view
[Switch C] vlan 300
```

```
[Switch C-vlan300] port gigabitethernet 1/0/1
[Switch C-vlan300] quit
[Switch C] vlan 200
[Switch C-vlan200] port gigabitethernet 1/0/2
[Switch C-vlan200] quit
[Switch C] interface vlan 300
[Switch C-Vlan-interface300] ip address 172.16.1.1 255.255.255.0
[Switch C-Vlan-interface300] quit
[Switch C] interface vlan 200
[Switch C-Vlan-interface200] ip address 192.168.1.2 255.255.255.0
[Switch C-Vlan-interface200] quit
```

配置全局 Router ID 为 3.3.3.3。

```
[Switch C] router id 3.3.3.3
```

启动 OSPF 进程 1，创建区域 1，并通告 192.168.1.0/24 网段和 172.16.1.0/24 网段。

```
[Switch C] ospf 1
[Switch C-ospf-1] area 1
[Switch C-ospf-1-area-0.0.0.1] network 192.168.1.0 0.0.0.255
[Switch C-ospf-1-area-0.0.0.1] network 172.16.1.0 0.0.0.255
[Switch C-ospf-1-area-0.0.0.1] quit
[Switch C-ospf-1] quit
```

保存配置。

```
[Switch C] save force
```

4. Switch D 的配置

创建 VLAN 200 和 VLAN 300，将接口 GE1/0/1 加入 VLAN 300、接口 GE1/0/2 加入 VLAN 200，并配置 VLAN 300 的 IP 地址为 172.17.1.1/24，VLAN 200 的 IP 地址为 192.168.2.2/24。

```
<Switch D> system-view
[Switch D] vlan 300
[Switch D-vlan300] port gigabitethernet 1/0/1
[Switch D-vlan300] quit
[Switch D] vlan 200
[Switch D-vlan200] port gigabitethernet 1/0/2
[Switch D-vlan200] quit
[Switch D] interface vlan 300
[Switch D-Vlan-interface300] ip address 172.17.1.1 255.255.255.0
[Switch D-Vlan-interface300] quit
[Switch D] interface vlan 200
[Switch D-Vlan-interface200] ip address 192.168.2.2 255.255.255.0
[Switch D-Vlan-interface200] quit
```

配置全局 Router ID 为 4.4.4.4。

```
[Switch D] router id 4.4.4.4
```

启动 OSPF 进程 1，创建区域 2，并通告 192.168.2.0/24 网段和 172.17.1.0/24 网段。

```
[Switch D] ospf 1
[Switch D-ospf-1] area 2
[Switch D-ospf-1-area-0.0.0.2] network 192.168.2.0 0.0.0.255
[Switch D-ospf-1-area-0.0.0.2] network 172.17.1.0 0.0.0.255
```

```
[Switch D-ospf-1-area-0.0.0.2] quit
[Switch D-ospf-1] quit
```

保存配置。

```
[Switch D] save force
```

3.5 验证配置

查看 Switch A 的 OSPF 邻居。

```
[Switch A] display ospf peer

         OSPF Process 1 with Router ID 1.1.1.1
               Neighbor Brief Information

 Area: 0.0.0.0
 Router ID       Address         Pri Dead-Time  State             Interface
 2.2.2.2         192.168.0.2     1   33         Full/DR           Vlan100

 Area: 0.0.0.1
 Router ID       Address         Pri Dead-Time  State             Interface
 3.3.3.3         192.168.1.2     1   34         Full/DR           Vlan200
```

查看 Switch A 的路由表，存在到 172.16.1.0、172.17.1.0、192.168.2.0 的路由。

```
[Switch A] display ip routing-table

Destinations : 19       Routes : 19

Destination/Mask    Proto   Pre Cost        NextHop         Interface
0.0.0.0/32          Direct  0   0           127.0.0.1       InLoop0
127.0.0.0/8         Direct  0   0           127.0.0.1       InLoop0
127.0.0.0/32        Direct  0   0           127.0.0.1       InLoop0
127.0.0.1/32        Direct  0   0           127.0.0.1       InLoop0
127.255.255.255/32  Direct  0   0           127.0.0.1       InLoop0
172.16.1.0/24       O_INTRA 10  2           192.168.1.2     Vlan200
172.17.1.0/24       O_INTER 10  3           192.168.0.2     Vlan100
192.168.0.0/24      Direct  0   0           192.168.0.1     Vlan100
192.168.0.0/32      Direct  0   0           192.168.0.1     Vlan100
192.168.0.1/32      Direct  0   0           127.0.0.1       InLoop0
192.168.0.255/32    Direct  0   0           192.168.0.1     Vlan100
192.168.1.0/24      Direct  0   0           192.168.1.1     Vlan200
192.168.1.0/32      Direct  0   0           192.168.1.1     Vlan200
192.168.1.1/32      Direct  0   0           127.0.0.1       InLoop0
192.168.1.255/32    Direct  0   0           192.168.1.1     Vlan200
192.168.2.0/24      O_INTER 10  2           192.168.0.2     Vlan100
224.0.0.0/4         Direct  0   0           0.0.0.0         NULL0
224.0.0.0/24        Direct  0   0           0.0.0.0         NULL0
255.255.255.255/32  Direct  0   0           127.0.0.1       InLoop0
```

Host A 可以 ping 通 Host B。

```
C:\Users\HostA>ping 172.17.1.2
```

```
正在 Ping 192.168.30.2 具有 32 字节的数据:
来自 172.17.1.2 的回复: 字节=32 时间=3ms TTL=255
来自 172.17.1.2 的回复: 字节=32 时间=1ms TTL=255
来自 172.17.1.2 的回复: 字节=32 时间<1ms TTL=255
来自 172.17.1.2 的回复: 字节=32 时间=2ms TTL=255

172.17.1.2 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 = 2ms，最长 = 3ms，平均 = 2ms
```

3.6 配置文件

- Switch A：

```
#
 router id 1.1.1.1
#
ospf 1
 area 0.0.0.0
  network 192.168.0.0 0.0.0.255
 area 0.0.0.1
  network 192.168.1.0 0.0.0.255
#
interface Vlan-interface100
 ip address 192.168.0.1 255.255.255.0
#
interface Vlan-interface200
 ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port access vlan 200
#
```

- Switch B：

```
#
 router id 2.2.2.2
#
ospf 1
 area 0.0.0.0
  network 192.168.0.0 0.0.0.255
 area 0.0.0.2
  network 192.168.2.0 0.0.0.255
#
interface Vlan-interface100
 ip address 192.168.0.2 255.255.255.0
#
```

```
interface Vlan-interface200
 ip address 192.168.2.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port access vlan 200
#
```

- Switch C：

```
#
 router id 3.3.3.3
#
ospf 1
 area 0.0.0.1
  network 192.168.1.0 0.0.0.255
  network 172.16.1.0 0.0.0.255
#
interface Vlan-interface200
 ip address 192.168.1.2 255.255.255.0
#
interface Vlan-interface300
 ip address 172.16.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port access vlan 300
#
interface GigabitEthernet1/0/2
 port access vlan 200
#
```

- Switch D：

```
#
 router id 4.4.4.4
#
ospf 1
 area 0.0.0.2
  network 192.168.2.0 0.0.0.255
  network 172.17.1.0 0.0.0.255
#
interface Vlan-interface200
 ip address 192.168.2.2 255.255.255.0
#
interface Vlan-interface300
 ip address 172.17.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port access vlan 300
#
```

```
interface GigabitEthernet1/0/2
 port access vlan 200
#
```

3.7 相关资料

- 产品配套“三层技术-IP 路由配置指导”中的“OSPF”。
- 产品配套“三层技术-IP 路由命令参考”中的“OSPF”。

静态路由快速配置指南

目 录

1 静态路由基本功能配置

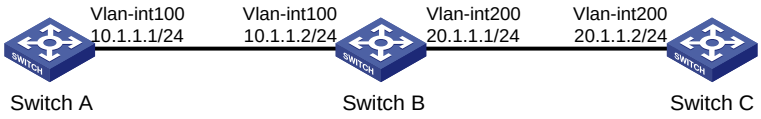
1.1 简介

本案例介绍静态路由基本功能的配置方法。

1.2 组网需求

如图 1 所示，要求配置静态路由，使 Switch A 和 Switch C 之间能够互通。

图1 静态路由基本功能配置组网图



1.3 配置步骤

1. 配置 Switch A

创建 VLAN，在 VLAN 中加入对应的端口，并配置各 VLAN 接口的 IP 地址。

```
<SwitchA> system-view
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1
[SwitchA-vlan100] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ip address 10.1.1.1 24
[SwitchA-Vlan-interface100] quit
```

配置静态路由。

```
[SwitchA] ip route-static 20.1.1.0 24 10.1.1.2
```

保存配置。

```
[SwitchA] save force
```

2. 配置 Switch B

创建 VLAN，在 VLAN 中加入对应的端口，并配置各 VLAN 接口的 IP 地址。

```
<SwitchB> system-view
[SwitchB] vlan 100
[SwitchB-vlan100] port gigabitethernet 1/0/1
[SwitchB-vlan100] quit
[SwitchB] vlan 200
[SwitchB-vlan200] port gigabitethernet 1/0/2
[SwitchB-vlan200] quit
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ip address 10.1.1.2 24
[SwitchB-Vlan-interface100] quit
[SwitchB] interface vlan-interface 200
```

```
[SwitchB-Vlan-interface200] ip address 20.1.1.1 24
[SwitchB-Vlan-interface200] quit
```

保存配置。

```
[SwitchB] save force
```

3. 配置 Switch C

创建 VLAN，在 VLAN 中加入对应的端口，并配置各 VLAN 接口的 IP 地址。

```
<SwitchC> system-view
[SwitchC] vlan 200
[SwitchC-vlan200] port gigabitethernet 1/0/1
[SwitchC-vlan200] quit
[SwitchC] interface vlan-interface 200
[SwitchC-Vlan-interface200] ip address 20.1.1.2 24
[SwitchC-Vlan-interface200] quit
```

配置静态路由。

```
[SwitchC] ip route-static 10.1.1.0 24 20.1.1.1
```

保存配置。

```
[SwitchC] save force
```

1.4 验证配置

在 Switch A 上使用 Ping 命令测试 Switch C 的互通性。

```
[SwitchA] ping 20.1.1.2
Ping 20.1.1.2 (20.1.1.2): 56 data bytes, press CTRL+C to break
56 bytes from 20.1.1.2: icmp_seq=0 ttl=255 time=2.000 ms
56 bytes from 20.1.1.2: icmp_seq=1 ttl=255 time=0.000 ms
56 bytes from 20.1.1.2: icmp_seq=2 ttl=255 time=0.000 ms
56 bytes from 20.1.1.2: icmp_seq=3 ttl=255 time=1.000 ms
56 bytes from 20.1.1.2: icmp_seq=4 ttl=255 time=0.000 ms

--- Ping statistics for 20.1.1.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/0.600/2.000/0.800 ms
```

1.5 配置文件

- Switch A：

```
#
vlan 100
#
interface Vlan-interface100
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
```

```
 ip route-static 20.1.1.0 24 10.1.1.2
#
```

- Switch B：

```
#
vlan 100
#
vlan 200
#
interface Vlan-interface100
 ip address 10.1.1.2 255.255.255.0
#
interface Vlan-interface200
 ip address 20.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 200
#
```

- Switch C：

```
#
vlan 200
#
interface Vlan-interface200
 ip address 20.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 200
#
 ip route-static 10.1.1.0 24 20.1.1.1
#
```

1.6 相关资料

- 产品配套“三层技术-IP 路由配置指导”中的“静态路由”。
- 产品配套“三层技术-IP 路由命令参考”中的“静态路由”。

2 IPv6 静态路由基本功能配置

2.1 简介

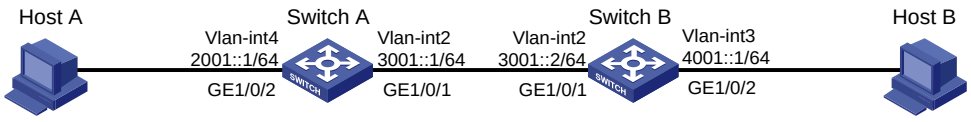
本案例介绍无状态自动配置 IPv6 地址，并配置 IPv6 静态路由基本功能实现跨网段设备互通的配置方法。

2.2 组网需求

如图 2 所示，交换机作为企业网络内部的网关设备，要实现无状态自动配置主机 Host A 和 Host B 的 IPv6 地址。不同网段的主机通过 IPv6 静态路由互相访问。

- Host A、Host B、Switch A 和 Switch B 之间通过以太网端口相连，将以太网端口分别加入相应的 VLAN 里，在 VLAN 接口上配置 IPv6 地址，验证它们之间的互通性。
- 在 Switch A 和 Switch B 上配置 IPv6 静态路由，实现各网段的互通。

图2 IPv6 静态路由基本功能配置组网图



2.3 配置步骤

1. 配置 Switch A

创建 VLAN，在 VLAN 中加入对应的端口。

```
<SwitchA> system-view
[SwitchA] vlan 4
[SwitchA-vlan4] port gigabitethernet 1/0/2
[SwitchA-vlan4] quit
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/1
[SwitchA-vlan2] quit
```

手工指定 VLAN 接口 2 的全球单播地址。

```
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ipv6 address 3001::1/64
[SwitchA-Vlan-interface2] quit
```

手工指定 VLAN 接口 4 的全球单播地址，并允许其发布 RA 消息。（缺省情况下，所有的接口不会发布 RA 消息）

```
[SwitchA] interface vlan-interface 4
[SwitchA-Vlan-4] ipv6 address 2001::1/64
[SwitchA-Vlan-4] undo ipv6 nd ra halt
[SwitchA-Vlan-4] quit
```

配置 IPv6 静态路由，该路由的目的地址为 4001::/64，下一跳地址为 3001::2。

```
[SwitchA] ipv6 route-static 4001:: 64 3001::2
```

保存配置。

```
[SwitchA] save force
```

2. 配置 Switch B

创建 VLAN，在 VLAN 中加入对应的端口。

```
<SwitchB> system-view
[SwitchB] vlan 2
[SwitchB-vlan2] port gigabitethernet 1/0/1
[SwitchB-vlan2] quit
[SwitchB] vlan 3
[SwitchB-vlan3] port gigabitethernet 1/0/2
[SwitchB-vlan3] quit
```

手工指定 VLAN 接口 2 的全球单播地址。

```
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ipv6 address 3001::2/64
[SwitchB-Vlan-interface2] quit
```

手工指定 VLAN 接口 3 的全球单播地址，并允许其发布 RA 消息。（缺省情况下，所有的接口不会发布 RA 消息）

```
[SwitchB] interface vlan-interface 3
[SwitchB-Vlan-interface3] ipv6 address 4001::1/64
[SwitchB-Vlan-interface3] undo ipv6 nd ra halt
[SwitchB-Vlan-interface3] quit
```

配置 IPv6 静态路由，该路由的目的地址为 2001::/64，下一跳地址为 3001::1。

```
[SwitchB] ipv6 route-static 2001:: 64 3001::1
```

3. 配置 Host A

在 Host A 上安装 IPv6，并配置自动获取 IPv6 地址。

4. 配置 Host B

在 Host B 上安装 IPv6，并配置自动获取 IPv6 地址。

2.4 验证配置

从 Switch A 上查看端口 GigabitEthernet1/0/2 的邻居信息。

```
[SwitchA] display ipv6 neighbors interface gigabitethernet 1/0/2
Type: S-Static    D-Dynamic    O-Openflow     R-Rule    IS-Invalid static
IPv6 address              MAC address    VLAN/VSI   Interface     State T  Aging
2001::15B:E0EA:3524:E791  0015-e9a6-7d14 4          GE1/0/2       REACH D  1248
FE80::215:E9FF:FEA6:7D14  0015-e9a6-7d14 4          GE1/0/2       REACH D  1238
```

通过上面的信息可以知道 Host A 上获得的 IPv6 全球单播地址为 2001::15B:E0EA:3524:E791。

从 Switch B 上查看端口 GigabitEthernet1/0/2 的邻居信息。

```
[SwitchB] display ipv6 neighbors interface gigabitethernet 1/0/2
Type: S-Static    D-Dynamic    O-Openflow     R-Rule    IS-Invalid static
IPv6 address              MAC address    VLAN/VSI   Interface     State T  Aging
4001::B15F:BC63:DBCE:EB57 6805-ca8b-18f3 3          GE1/0/2       REACH D  46
FE80::510B:D60F:31A7:4AFF 6805-ca8b-18f3 3          GE1/0/2       REACH D  1238
```

通过上面的信息可以知道 Host B 上获得的 IPv6 全球单播地址为 4001::B15F:BC63:DBCE:EB57。

在 Switch A 上使用 Ping 测试 Host B 的互通性。

```
[Switch A] ping ipv6 4001::B15F:BC63:DBCE:EB57
Ping6(56 data bytes) 3001::1 --> 4001::B15F:BC63:DBCE:EB57, press CTRL+C to break
56 bytes from 4001::B15F:BC63:DBCE:EB57, icmp_seq=0 hlim=64 time=1.000 ms
56 bytes from 4001::B15F:BC63:DBCE:EB57, icmp_seq=1 hlim=64 time=0.000 ms
56 bytes from 4001::B15F:BC63:DBCE:EB57, icmp_seq=2 hlim=64 time=0.000 ms
56 bytes from 4001::B15F:BC63:DBCE:EB57, icmp_seq=3 hlim=64 time=1.000 ms
56 bytes from 4001::B15F:BC63:DBCE:EB57, icmp_seq=4 hlim=64 time=0.000 ms
--- Ping6 statistics for 4001::B15F:BC63:DBCE:EB57 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/0.400/1.000/0.490 ms
```

在 Switch B 上使用 Ping 测试 Host A 的互通性。

```
[Switch B] ping ipv6 2001::15B:E0EA:3524:E791
Ping6(56 data bytes) 3001::2 --> 2001::15B:E0EA:3524:E791, press CTRL+C to break
56 bytes from 2001::15B:E0EA:3524:E791, icmp_seq=0 hlim=64 time=1.000 ms
56 bytes from 2001::15B:E0EA:3524:E791, icmp_seq=1 hlim=64 time=0.000 ms
56 bytes from 2001::15B:E0EA:3524:E791, icmp_seq=2 hlim=64 time=0.000 ms
56 bytes from 2001::15B:E0EA:3524:E791, icmp_seq=3 hlim=64 time=1.000 ms
56 bytes from 2001::15B:E0EA:3524:E791, icmp_seq=4 hlim=64 time=0.000 ms
--- Ping6 statistics for 2001::15B:E0EA:3524:E791 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/0.400/1.000/0.490 ms
```

从 Host A 上也可以 ping 通 Host B，证明它们是互通的。

2.5 配置文件

- Switch A：

```
#
vlan 1
#
vlan 2
#
interface Vlan-interface1
 ipv6 address 2001::1/64
 undo ipv6 nd ra halt
#
interface Vlan-interface2
 ipv6 address 3001::1/64
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 1
```

```
#
 ipv6 route-static 4001:: 64 3001::2
#
```

- Switch B：

```
#
vlan 2
#
vlan 3
#
interface Vlan-interface2
 ipv6 address 3001::2/64
#
interface Vlan-interface3
 ipv6 address 4001::1/64
 undo ipv6 nd ra halt
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 3
#
 ipv6 route-static 2001:: 64 3001::1
#
```

2.6 相关资料

- 产品配套“三层技术-IP 业务配置指导”中的“IPv6 基础”。
- 产品配套“三层技术-IP 业务命令参考”中的“IPv6 基础”。
- 产品配套“三层技术-IP 路由配置指导”中的“IPv6 静态路由”。
- 产品配套“三层技术-IP 路由命令参考”中的“IPv6 静态路由”。

3 配置缺省路由

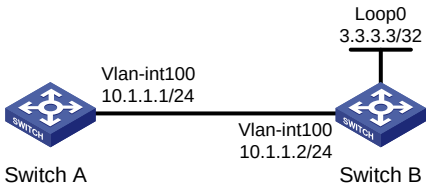
3.1 简介

本案例介绍缺省路由的配置方法。

3.2 组网需求

如图 3 所示，在 Switch A 上配置缺省路由，下一跳地址设置为 Switch B 的接口地址 10.1.1.2/24。配置完成后，Switch A 可以 ping 通 Switch B 的 Loopback 接口地址 3.3.3.3/32。

图3 缺省路由配置组网图



3.3 配置步骤

1. 配置 Switch A

创建 VLAN，在 VLAN 中加入对应的端口，并配置各 VLAN 接口的 IP 地址。

```
<SwitchA> system-view
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1
[SwitchA-vlan100] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ip address 10.1.1.1 24
[SwitchA-Vlan-interface100] quit
```

配置缺省路由。

```
[SwitchA] ip route-static 0.0.0.0 0 10.1.1.2
```

保存配置。

```
[SwitchA] save force
```

2. 配置 Switch B

创建 VLAN，在 VLAN 中加入对应的端口，并配置各 VLAN 接口的 IP 地址。

```
<SwitchB> system-view
[SwitchB] vlan 100
[SwitchB-vlan100] port gigabitethernet 1/0/1
[SwitchB-vlan100] quit
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ip address 10.1.1.2 24
[SwitchB-Vlan-interface100] quit
```

配置 Loopback 接口的 IP 地址。

```
[SwitchB] interface LoopBack 0
```

```
[SwitchB-LoopBack0] ip address 3.3.3.3 32
```

保存配置。

```
[SwitchB] save force
```

3.4 验证配置

当 Switch A 上未配置缺省路由时，无法访问 3.3.3.3。

```
[SwitchA] ping 3.3.3.3
Ping 3.3.3.3 (3.3.3.3): 56 data bytes, press CTRL+C to break
Request time out
Request time out
Request time out
Request time out
Request time out
--- Ping statistics for 3.3.3.3 ---
5 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss
```

当 Switch A 上配置了缺省路由时，可以访问 3.3.3.3。

```
[SwitchA] ping 3.3.3.3
Ping 3.3.3.3 (3.3.3.3): 56 data bytes, press CTRL+C to break
56 bytes from 3.3.3.3: icmp_seq=0 ttl=255 time=2.000 ms
56 bytes from 3.3.3.3: icmp_seq=1 ttl=255 time=0.000 ms
56 bytes from 3.3.3.3: icmp_seq=2 ttl=255 time=0.000 ms
56 bytes from 3.3.3.3: icmp_seq=3 ttl=255 time=1.000 ms
56 bytes from 3.3.3.3: icmp_seq=4 ttl=255 time=0.000 ms
--- Ping statistics for 3.3.3.3 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/0.600/2.000/0.800 ms
```

3.5 配置文件

- Switch A：

```
#
vlan 100
#
interface Vlan-interface100
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
 ip route-static 0.0.0.0 0 10.1.1.2
#
```

- Switch B ：

```
#
vlan 100
#
```

```
interface Vlan-interface100
 ip address 10.1.1.2 255.255.255.0
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
```

3.6 相关资料

- 产品配套“三层技术-IP 路由配置指导”中的“静态路由”。
- 产品配套“三层技术-IP 路由命令参考”中的“静态路由”。

4 配置浮动静态路由

4.1 简介

本案例介绍浮动静态路由的配置方法。

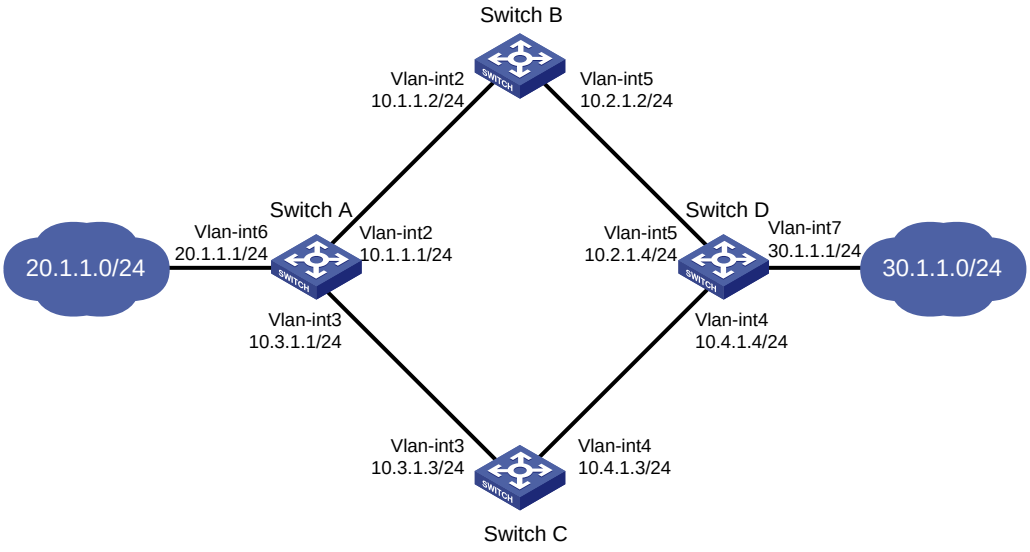
4.2 组网需求

浮动路由又被称为路由备份。如图 4 所示，Switch A、Switch B、Switch C 和 Switch D 连接了 20.1.1.0/24 和 30.1.1.0/24 两个网段，在交换机上配置静态路由以实现两个网段的互通，并配置路由备份以提高网络的可靠性。

Switch A 作为 20.1.1.0/24 网段内主机的缺省网关，在 Switch A 上存在两条到达 30.1.1.0/24 网段的静态路由，下一跳分别为 Switch B 和 Switch C。这两条静态路由形成备份，其中：

- 下一跳为 Switch B 的静态路由优先级高，作为主路由。该路由可达时，Switch A 通过 Switch B 将报文转发到 30.1.1.0/24 网段。
- 下一跳为 Switch C 的静态路作为备份路由。当主路由不可达时，备份路由生效，Switch A 通过 Switch C 将报文转发到 30.1.1.0/24 网段。
- 在主路由恢复正常后，业务流量将切换到主链路上，备份路由失效。

图4 浮动静态路由配置组网图



说明

此应用场景下，请确保生成树协议处于未使能状态。

4.3 配置步骤

1. 配置 Switch A

创建 VLAN，在 VLAN 中加入对应的端口，并配置各 VLAN 接口的 IP 地址。

```
<SwitchA> system-view
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/1
[SwitchA-vlan2] quit
[SwitchA] vlan 3
[SwitchA-vlan3] port gigabitethernet 1/0/2
[SwitchA-vlan3] quit
[SwitchA] vlan 6
[SwitchA-vlan6] port gigabitethernet 1/0/3
[SwitchA-vlan6] quit
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 10.1.1.1 24
[SwitchA-Vlan-interface2] quit
[SwitchA] interface vlan-interface 3
[SwitchA-Vlan-interface3] ip address 10.3.1.1 24
[SwitchA-Vlan-interface3] quit
[SwitchA] interface vlan-interface 6
[SwitchA-Vlan-interface6] ip address 20.1.1.1 24
[SwitchA-Vlan-interface6] quit
```

配置到达 30.1.1.0/24 网段的静态路由：下一跳地址为 10.1.1.2，优先级为缺省值 60。

```
[SwitchA] ip route-static 30.1.1.0 24 10.1.1.2
```

配置到达 10.2.1.0/24 网段的静态路由：下一跳地址为 10.1.1.2，优先级为缺省值 60。

```
[SwitchA] ip route-static 10.2.1.0 24 10.1.1.2
```

配置到达 30.1.1.0/24 网段的静态路由：下一跳地址为 10.3.1.3，优先级为 80。

```
[SwitchA] ip route-static 30.1.1.0 24 10.3.1.3 preference 80
```

配置到达 10.4.1.0/24 网段的静态路由：下一跳地址为 10.3.1.3，优先级为 80。

```
[SwitchA] ip route-static 10.4.1.0 24 10.3.1.3 preference 80
```

保存配置。

```
[SwitchA] save force
```

2. 配置 Switch B

创建 VLAN，在 VLAN 中加入对应的端口，并配置各 VLAN 接口的 IP 地址。

```
<SwitchB> system-view
[SwitchB] vlan 2
[SwitchB-vlan2] port gigabitethernet 1/0/1
[SwitchB-vlan2] quit
[SwitchB] vlan 5
[SwitchB-vlan5] port gigabitethernet 1/0/2
[SwitchB-vlan5] quit
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address 10.1.1.2 24
```

```
[SwitchB-Vlan-interface2] quit
[SwitchB] interface vlan-interface 5
[SwitchB-Vlan-interface5] ip address 10.2.1.2 24
[SwitchB-Vlan-interface5] quit
```

配置到达 30.1.1.0/24 网段的静态路由：下一跳地址为 10.2.1.4。

```
[SwitchB] ip route-static 30.1.1.0 24 10.2.1.4
```

配置到达 20.1.1.0/24 网段的静态路由：下一跳地址为 10.1.1.1。

```
[SwitchB] ip route-static 20.1.1.0 24 10.1.1.1
```

保存配置。

```
[SwitchB] save force
```

3. 配置 Switch C

创建 VLAN，在 VLAN 中加入对应的端口，并配置各 VLAN 接口的 IP 地址。

```
<SwitchC> system-view
[SwitchC] vlan 3
[SwitchC-vlan3] port gigabitethernet 1/0/1
[SwitchC-vlan3] quit
[SwitchC] vlan 4
[SwitchC-vlan4] port gigabitethernet 1/0/2
[SwitchC-vlan4] quit
[SwitchC] interface vlan-interface 3
[SwitchC-Vlan-interface3] ip address 10.3.1.3 24
[SwitchC-Vlan-interface3] quit
[SwitchC] interface vlan-interface 4
[SwitchC-Vlan-interface4] ip address 10.4.1.3 24
[SwitchC-Vlan-interface4] quit
```

配置到达 30.1.1.0/24 网段的静态路由：下一跳地址为 10.4.1.4。

```
[SwitchC] ip route-static 30.1.1.0 24 10.4.1.4
```

配置到达 20.1.1.0/24 网段的静态路由：下一跳地址为 10.3.1.1。

```
[SwitchC] ip route-static 20.1.1.0 24 10.3.1.1
```

保存配置。

```
[SwitchC] save force
```

4. 配置 Switch D

创建 VLAN，在 VLAN 中加入对应的端口，并配置各 VLAN 接口的 IP 地址。

```
<SwitchD> system-view
[SwitchD] vlan 4
[SwitchD-vlan4] port gigabitethernet 1/0/1
[SwitchD-vlan4] quit
[SwitchD] vlan 5
[SwitchD-vlan5] port gigabitethernet 1/0/2
[SwitchD-vlan5] quit
[SwitchD] vlan 7
[SwitchD-vlan7] port gigabitethernet 1/0/3
[SwitchD-vlan7] quit
[SwitchD] interface vlan-interface 4
```

```
[SwitchD-Vlan-interface6] ip address 10.4.1.4 24
[SwitchD-Vlan-interface6] quit
[SwitchD] interface vlan-interface 5
[SwitchD-Vlan-interface5] ip address 10.2.1.4 24
[SwitchD-Vlan-interface5] quit
[SwitchD] interface vlan-interface 7
[SwitchD-Vlan-interface7] ip address 30.1.1.1 24
[SwitchD-Vlan-interface7] quit
```

配置到达 20.1.1.0/24 网段的静态路由：下一跳地址为 10.2.1.2，优先级为缺省值 60。

```
[SwitchD] ip route-static 20.1.1.0 24 10.2.1.2
```

配置到达 10.1.1.0/24 网段的静态路由：下一跳地址为 10.2.1.2，优先级为缺省值 60。

```
[SwitchD] ip route-static 10.1.1.0 24 10.2.1.2
```

配置到达 20.1.1.0/24 网段的静态路由：下一跳地址为 10.4.1.3，优先级为 80。

```
[SwitchD] ip route-static 20.1.1.0 24 10.4.1.3 preference 80
```

配置到达 10.3.1.0/24 网段的静态路由：下一跳地址为 10.4.1.3，优先级为 80。

```
[SwitchD] ip route-static 10.3.1.0 24 10.4.1.3 preference 80
```

保存配置。

```
[SwitchD] save force
```

4.4 验证配置

显示 Switch A 的路由表。

```
[SwitchA] display ip routing-table

Destinations : 9       Routes : 9

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
10.1.1.0/24         Direct 0    0            10.1.1.1        Vlan2
10.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
10.3.1.0/24         Direct 0    0            10.3.1.1        Vlan3
10.3.1.1/32         Direct 0    0            127.0.0.1       InLoop0
20.1.1.0/24         Direct 0    0            20.1.1.1        Vlan6
20.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
30.1.1.0/24         Static 60   0            10.1.1.2        Vlan2
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
```

以上显示信息表示，Switch A 通过 Switch B 将报文转发到 30.1.1.0/24 网段。

在 Switch B 上关闭 VLAN 接口 2 对应的以太网接口。

```
<SwitchB> system-view
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] shutdown
```

显示 Switch A 的路由表。

```
[SwitchA] display ip routing-table

Destinations : 9       Routes : 9
```

```
Destination/Mask    Proto  Pre  Cost         NextHop         Interface
10.1.1.0/24         Direct 0    0            10.1.1.1        Vlan2
10.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
10.3.1.0/24         Direct 0    0            10.3.1.1        Vlan3
10.3.1.1/32         Direct 0    0            127.0.0.1       InLoop0
20.1.1.0/24         Direct 0    0            20.1.1.1        Vlan6
20.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
30.1.1.0/24         Static 80   0            10.3.1.3        Vlan3
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
```

以上显示信息表示，备份路由生效，Switch A 通过 Switch C 将报文转发到 30.1.1.0/24 网段。

主路由出现故障后，20.1.1.0/24 网段内的主机仍然可以与 30.1.1.0/24 网段内的主机通信。

```
[SwitchA] ping -a 20.1.1.1 30.1.1.1
Ping 30.1.1.1: 56  data bytes, press CTRL+C to break
Reply from 30.1.1.1: bytes=56 Sequence=1 ttl=254 time=2 ms
Reply from 30.1.1.1: bytes=56 Sequence=2 ttl=254 time=1 ms
Reply from 30.1.1.1: bytes=56 Sequence=3 ttl=254 time=1 ms
Reply from 30.1.1.1: bytes=56 Sequence=4 ttl=254 time=2 ms
Reply from 30.1.1.1: bytes=56 Sequence=5 ttl=254 time=1 ms

--- Ping statistics for 30.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.00% packet loss
round-trip min/avg/max/std-dev = 1/1/2/1 ms
```

Switch D 上的显示信息与 Switch A 类似。主路由出现故障后，30.1.1.0/24 网段内的主机仍然可以与 20.1.1.0/24 网段内的主机通信。

```
[SwitchD] ping -a 30.1.1.1 20.1.1.1
Ping 20.1.1.1: 56  data bytes, press CTRL+C to break
Reply from 20.1.1.1: bytes=56 Sequence=1 ttl=254 time=2 ms
Reply from 20.1.1.1: bytes=56 Sequence=2 ttl=254 time=1 ms
Reply from 20.1.1.1: bytes=56 Sequence=3 ttl=254 time=1 ms
Reply from 20.1.1.1: bytes=56 Sequence=4 ttl=254 time=1 ms
Reply from 20.1.1.1: bytes=56 Sequence=5 ttl=254 time=1 ms

--- Ping statistics for 20.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.00% packet loss
round-trip min/avg/max/std-dev = 1/1/2/1 ms
```

4.5 配置文件

- Switch A：

```
#
vlan 2
#
vlan 3
#
vlan 6
```

```
#
interface Vlan-interface2
 ip address 10.1.1.1 255.255.255.0
#
interface Vlan-interface3
 ip address 10.3.1.1 255.255.255.0
#
interface Vlan-interface6
 ip address 20.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 3
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 6
#
 ip route-static 30.1.1.0 24 10.1.1.2
 ip route-static 10.2.1.0 24 10.1.1.2
 ip route-static 30.1.1.0 24 10.3.1.3 preference 80
 ip route-static 10.4.1.0 24 10.3.1.3 preference 80
#
```

- Switch B：

```
#
vlan 2
#
vlan 5
#
interface Vlan-interface2
 ip address 10.1.1.2 255.255.255.0
#
interface Vlan-interface5
 ip address 10.2.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 5
#
 ip route-static 20.1.1.0 24 10.1.1.1
```

```
 ip route-static 30.1.1.0 24 10.2.1.4
#
```

- Switch C

```
#
vlan 3
#
vlan 4
#
interface Vlan-interface3
 ip address 10.3.1.3 255.255.255.0
#
interface Vlan-interface4
 ip address 10.4.1.3 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 3
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 4
#
 ip route-static 20.1.1.0 24 10.3.1.1
 ip route-static 30.1.1.0 24 10.4.1.4
#
```

- Switch D

```
#
vlan 4
#
vlan 5
#
vlan 7
#
interface Vlan-interface4
 ip address 10.4.1.4 255.255.255.0
#
interface Vlan-interface5
 ip address 10.2.1.4 255.255.255.0
#
interface Vlan-interface7
 ip address 30.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 4
#
interface GigabitEthernet1/0/2
 port link-mode bridge
```

```
 port access vlan 5
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 7
#
 ip route-static 20.1.1.0 24 10.2.1.2
 ip route-static 10.1.1.0 24 10.2.1.2
 ip route-static 20.1.1.0 24 10.4.1.3 preference 80
 ip route-static 10.3.1.0 24 10.4.1.3 preference 80
#
```

4.6 相关资料

- 产品配套“三层技术-IP 路由配置指导”中的“静态路由”。
- 产品配套“三层技术-IP 路由命令参考”中的“静态路由”。

5 配置静态路由实现路由负载分担

5.1 简介

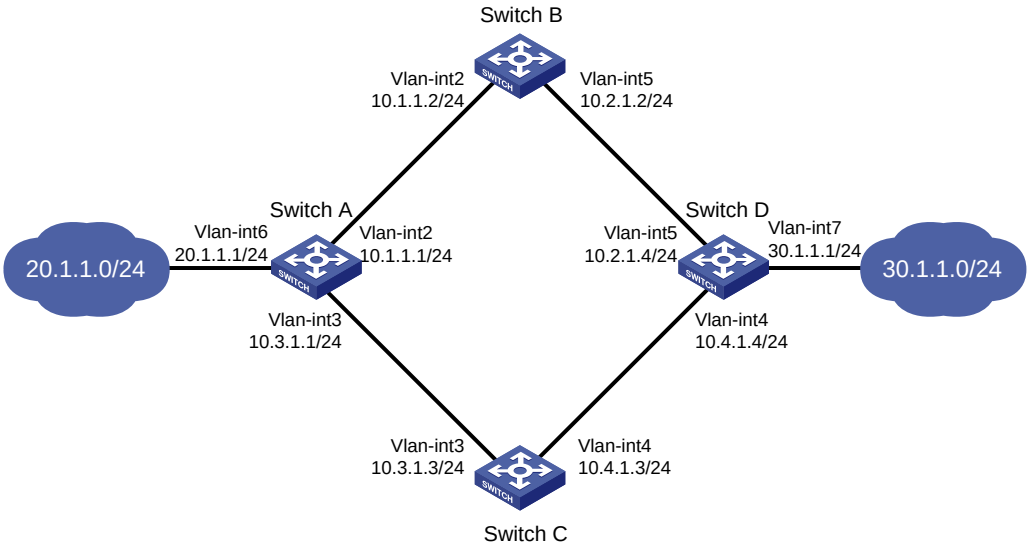
本案例介绍静态路由实现路由负载分担的配置方法。

5.2 组网需求

如图 5 所示，Switch A、Switch B、Switch C 和 Switch D 连接了 20.1.1.0/24 和 30.1.1.0/24 两个网段，在交换机上配置静态路由以实现两个网段的互通，为了提高链路利用率，要求从 20.1.1.0/24 到 30.1.1.0/24 的数据流平均分配到两条链路上，并且当其中一条链路故障后流量自动切换到另一条链路上。

Switch A 作为 20.1.1.0/24 网段内主机的缺省网关，在 Switch A 上存在两条到达 30.1.1.0/24 网段的静态路由，下一跳分别为 Switch B 和 Switch C。通过这两条静态路由形成路由负载分担。注意：需要配置数据流的去程和回程两个方向的静态路由。

图5 静态路由实现路由负载分担配置组网图



说明

此应用场景下，请确保生成树协议处于未使能状态。

5.3 配置步骤

1. 配置 Switch A

创建 VLAN，在 VLAN 中加入对应的端口，并配置各 VLAN 接口的 IP 地址。

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

```
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/1
[SwitchA-vlan2] quit
[SwitchA] vlan 3
[SwitchA-vlan3] port gigabitethernet 1/0/2
[SwitchA-vlan3] quit
[SwitchA] vlan 6
[SwitchA-vlan6] port gigabitethernet 1/0/3
[SwitchA-vlan6] quit
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 10.1.1.1 24
[SwitchA-Vlan-interface2] quit
[SwitchA] interface vlan-interface 3
[SwitchA-Vlan-interface3] ip address 10.3.1.1 24
[SwitchA-Vlan-interface3] quit
[SwitchA] interface vlan-interface 6
[SwitchA-Vlan-interface6] ip address 20.1.1.1 24
[SwitchA-Vlan-interface6] quit
```

配置到达 30.1.1.0/24 网段的静态路由：下一跳地址为 10.1.1.2。

```
[SwitchA] ip route-static 30.1.1.0 24 10.1.1.2
```

配置到达 10.2.1.0/24 网段的静态路由：下一跳地址为 10.1.1.2。

```
[SwitchA] ip route-static 10.2.1.0 24 10.1.1.2
```

配置到达 30.1.1.0/24 网段的静态路由：下一跳地址为 10.3.1.3。

```
[SwitchA] ip route-static 30.1.1.0 24 10.3.1.3
```

配置到达 10.4.1.0/24 网段的静态路由：下一跳地址为 10.3.1.3。

```
[SwitchA] ip route-static 10.4.1.0 24 10.3.1.3
```

保存配置。

```
[SwitchA] save force
```

2. 配置 Switch B

创建 VLAN，在 VLAN 中加入对应的端口，并配置各 VLAN 接口的 IP 地址。

```
<SwitchB> system-view
[SwitchB] vlan 2
[SwitchB-vlan2] port gigabitethernet 1/0/1
[SwitchB-vlan2] quit
[SwitchB] vlan 5
[SwitchB-vlan5] port gigabitethernet 1/0/2
[SwitchB-vlan5] quit
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address 10.1.1.2 24
[SwitchB-Vlan-interface2] quit
[SwitchB] interface vlan-interface 5
[SwitchB-Vlan-interface5] ip address 10.2.1.2 24
[SwitchB-Vlan-interface5] quit
```

配置到达 30.1.1.0/24 网段的静态路由：下一跳地址为 10.2.1.4。

```
[SwitchB] ip route-static 30.1.1.0 24 10.2.1.4
```

配置到达 20.1.1.0/24 网段的静态路由：下一跳地址为 10.1.1.1。

```
[SwitchB] ip route-static 20.1.1.0 24 10.1.1.1
```

保存配置。

```
[SwitchB] save force
```

3. 配置 Switch C

创建 VLAN，在 VLAN 中加入对应的端口，并配置各 VLAN 接口的 IP 地址。

```
<SwitchC> system-view
[SwitchC] vlan 3
[SwitchC-vlan3] port gigabitethernet 1/0/1
[SwitchC-vlan3] quit
[SwitchC] vlan 4
[SwitchC-vlan4] port gigabitethernet 1/0/2
[SwitchC-vlan4] quit
[SwitchC] interface vlan-interface 3
[SwitchC-Vlan-interface3] ip address 10.3.1.3 24
[SwitchC-Vlan-interface3] quit
[SwitchC] interface vlan-interface 4
[SwitchC-Vlan-interface4] ip address 10.4.1.3 24
[SwitchC-Vlan-interface4] quit
```

配置到达 30.1.1.0/24 网段的静态路由：下一跳地址为 10.4.1.4。

```
[SwitchC] ip route-static 30.1.1.0 24 10.4.1.4
```

配置到达 20.1.1.0/24 网段的静态路由：下一跳地址为 10.3.1.1。

```
[SwitchC] ip route-static 20.1.1.0 24 10.3.1.1
```

保存配置。

```
[SwitchC] save force
```

4. 配置 Switch D

创建 VLAN，在 VLAN 中加入对应的端口，并配置各 VLAN 接口的 IP 地址。

```
<SwitchD> system-view
[SwitchD] vlan 4
[SwitchD-vlan4] port gigabitethernet 1/0/1
[SwitchD-vlan4] quit
[SwitchD] vlan 5
[SwitchD-vlan5] port gigabitethernet 1/0/2
[SwitchD-vlan5] quit
[SwitchD] vlan 7
[SwitchD-vlan7] port gigabitethernet 1/0/3
[SwitchD-vlan7] quit
[SwitchD] interface vlan-interface 4
[SwitchD-Vlan-interface4] ip address 10.4.1.4 24
[SwitchD-Vlan-interface4] quit
[SwitchD] interface vlan-interface 5
[SwitchD-Vlan-interface5] ip address 10.2.1.4 24
[SwitchD-Vlan-interface5] quit
[SwitchD] interface vlan-interface 7
[SwitchD-Vlan-interface7] ip address 30.1.1.1 24
```

```
[SwitchD-Vlan-interface7] quit
```
配置到达 20.1.1.0/24 网段的静态路由：下一跳地址为 10.2.1.2。
```
[SwitchD] ip route-static 20.1.1.0 24 10.2.1.2
```
配置到达 10.1.1.0/24 网段的静态路由：下一跳地址为 10.2.1.2。
```
[SwitchD] ip route-static 10.1.1.0 24 10.2.1.2
```
配置到达 20.1.1.0/24 网段的静态路由：下一跳地址为 10.4.1.3。
```
[SwitchD] ip route-static 20.1.1.0 24 10.4.1.3
```
配置到达 10.3.1.0/24 网段的静态路由：下一跳地址为 10.4.1.3。
```
[SwitchD] ip route-static 10.3.1.0 24 10.4.1.3
```
保存配置。
```
[SwitchD] save force
```

5.4 验证配置

显示 Switch A 的路由表。
```
[SwitchA] display ip routing-table

Destinations : 9       Routes : 10

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
10.1.1.0/24         Direct 0    0            10.1.1.1        Vlan2
10.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
10.3.1.0/24         Direct 0    0            10.3.1.1        Vlan3
10.3.1.1/32         Direct 0    0            127.0.0.1       InLoop0
20.1.1.0/24         Direct 0    0            20.1.1.1        Vlan6
20.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
30.1.1.0/24         Static 60   0            10.1.1.2        Vlan2
                    Static 60   0            10.3.1.3        Vlan3
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
```
以上显示信息表示，Switch A 可以通过 Switch B 和 Switch C 将报文转发到 30.1.1.0/24 网段。

在 Switch B 上关闭 VLAN 接口 2 对应的以太网接口。
```
<SwitchB> system-view
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] shutdown
```
显示 Switch A 的路由表。
```
[SwitchA] display ip routing-table

Destinations : 9       Routes : 9

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
10.1.1.0/24         Direct 0    0            10.1.1.1        Vlan2
10.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
10.3.1.0/24         Direct 0    0            10.3.1.1        Vlan3
10.3.1.1/32         Direct 0    0            127.0.0.1       InLoop0
```

```
20.1.1.0/24         Direct 0    0           20.1.1.1        Vlan6
20.1.1.1/32         Direct 0    0           127.0.0.1       InLoop0
30.1.1.0/24         Static 60   0           10.3.1.3        Vlan3
127.0.0.0/8         Direct 0    0           127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0           127.0.0.1       InLoop0
```

以上显示信息表示，当其中一条链路故障时，Switch A 可以通过 Switch C 将报文转发到 30.1.1.0/24 网段。

#其中一条链路出现故障后，20.1.1.0/24 网段内的主机仍然可以与 30.1.1.0/24 网段内的主机通信。

```
[SwitchA] ping -a 20.1.1.1 30.1.1.1
Ping 30.1.1.1: 56  data bytes, press CTRL+C to break
Reply from 30.1.1.1: bytes=56 Sequence=1 ttl=254 time=2 ms
Reply from 30.1.1.1: bytes=56 Sequence=2 ttl=254 time=1 ms
Reply from 30.1.1.1: bytes=56 Sequence=3 ttl=254 time=1 ms
Reply from 30.1.1.1: bytes=56 Sequence=4 ttl=254 time=2 ms
Reply from 30.1.1.1: bytes=56 Sequence=5 ttl=254 time=1 ms

--- Ping statistics for 30.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.00% packet loss
round-trip min/avg/max/std-dev = 1/1/2/1 ms
```

Switch D 上的显示信息与 Switch A 类似。其中一条链路出现故障后，30.1.1.0/24 网段内的主机仍然可以与 20.1.1.0/24 网段内的主机通信。

```
[SwitchD] ping -a 30.1.1.1 20.1.1.1
Ping 20.1.1.1: 56  data bytes, press CTRL+C to break
Reply from 20.1.1.1: bytes=56 Sequence=1 ttl=254 time=2 ms
Reply from 20.1.1.1: bytes=56 Sequence=2 ttl=254 time=1 ms
Reply from 20.1.1.1: bytes=56 Sequence=3 ttl=254 time=1 ms
Reply from 20.1.1.1: bytes=56 Sequence=4 ttl=254 time=1 ms
Reply from 20.1.1.1: bytes=56 Sequence=5 ttl=254 time=1 ms

--- Ping statistics for 20.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.00% packet loss
round-trip min/avg/max/std-dev = 1/1/2/1 ms
```

5.5 配置文件

- Switch A：

```
#
vlan 2
#
vlan 3
#
vlan 6
#
interface Vlan-interface2
 ip address 10.1.1.1 255.255.255.0
#
interface Vlan-interface3
```

```
 ip address 10.3.1.1 255.255.255.0
#
interface Vlan-interface6
 ip address 20.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 3
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 6
#
 ip route-static 30.1.1.0 24 10.1.1.2
 ip route-static 10.2.1.0 24 10.1.1.2
 ip route-static 30.1.1.0 24 10.3.1.3
 ip route-static 10.4.1.0 24 10.3.1.3
#
```

- Switch B：

```
#
vlan 2
#
vlan 5
#
interface Vlan-interface2
 ip address 10.1.1.2 255.255.255.0
#
interface Vlan-interface5
 ip address 10.2.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 5
#
 ip route-static 20.1.1.0 24 10.1.1.1
 ip route-static 30.1.1.0 24 10.2.1.4
#
```

- Switch C

```
#
vlan 3
```

```
#
vlan 4
#
interface Vlan-interface3
 ip address 10.3.1.3 255.255.255.0
#
interface Vlan-interface4
 ip address 10.4.1.3 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 3
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 4
#
 ip route-static 20.1.1.0 24 10.3.1.1
 ip route-static 30.1.1.0 24 10.4.1.4
#
```

- Switch D

```
#
vlan 4
#
vlan 5
#
vlan 7
#
interface Vlan-interface4
 ip address 10.4.1.4 255.255.255.0
#
interface Vlan-interface5
 ip address 10.2.1.4 255.255.255.0
#
interface Vlan-interface7
 ip address 30.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 4
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 5
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 7
```

```
#
 ip route-static 20.1.1.0 24 10.2.1.2
 ip route-static 10.1.1.0 24 10.2.1.2
 ip route-static 20.1.1.0 24 10.4.1.3
 ip route-static 10.3.1.0 24 10.4.1.3
#
```

5.6 相关资料

- 产品配套“三层技术-IP 路由配置指导”中的“静态路由”。
- 产品配套“三层技术-IP 路由命令参考”中的“静态路由”。

6 静态路由、Track 与 NQA 联动

6.1 简介

本案例介绍静态路由、Track 与 NQA 联动的配置方法。

6.2 组网需求

如图 6 所示，Switch A、Switch B、Switch C 和 Switch D 连接了 20.1.1.0/24 和 30.1.1.0/24 两个网段，在交换机上配置静态路由以实现两个网段的互通，并配置路由备份以提高网络的可靠性。

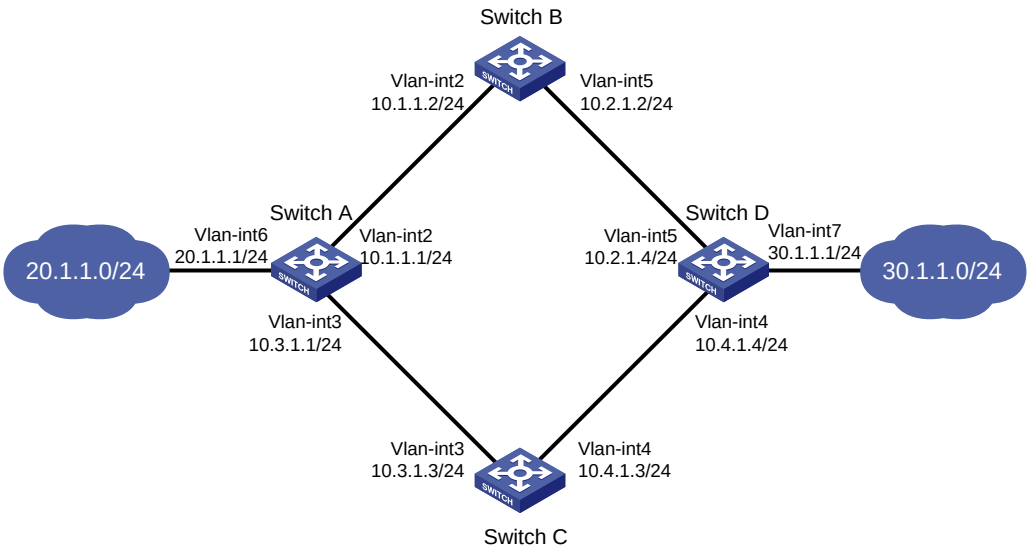
Switch A 作为 20.1.1.0/24 网段内主机的缺省网关，在 Switch A 上存在两条到达 30.1.1.0/24 网段的静态路由，下一跳分别为 Switch B 和 Switch C。这两条静态路由形成备份，其中：

- 下一跳为 Switch B 的静态路由优先级高，作为主路由。该路由可达时，Switch A 通过 Switch B 将报文转发到 30.1.1.0/24 网段。
- 下一跳为 Switch C 的静态路作为备份路由。
- 在 Switch A 上通过静态路由、Track 与 NQA 联动，实时判断主路由是否可达。当主路由不可达时，备份路由生效，Switch A 通过 Switch C 将报文转发到 30.1.1.0/24 网段。

同样地，Switch D 作为 30.1.1.0/24 网段内主机的缺省网关，在 Switch D 上存在两条到达 20.1.1.0/24 网段的静态路由，下一跳分别为 Switch B 和 Switch C。这两条静态路由形成备份，其中：

- 下一跳为 Switch B 的静态路由优先级高，作为主路由。该路由可达时，Switch D 通过 Switch B 将报文转发到 20.1.1.0/24 网段。
- 下一跳为 Switch C 的静态路作为备份路由。
- 在 Switch D 上通过静态路由、Track 与 NQA 联动，实时判断主路由是否可达。当主路由不可达时，备份路由生效，Switch D 通过 Switch C 将报文转发到 20.1.1.0/24 网段。

图6 静态路由、Track 与 NQA 联动配置组网图



说明

此应用场景下，请确保生成树协议处于未使能状态。

6.3 配置思路

配置思路如下：

(1) 配置各设备 IP 地址

(2) 配置静态路由

配置主备静态路由，其中下一跳为 Switch B 的静态路由优先级高，作为主路由，下一跳为 Switch C 的静态路作为备份路由。

(3) 配置 NQA 测试

分别在 Switch A 和 Switch D 上配置 NQA 检测 Switch A－Switch B－Switch D 这条路径的连通性。通过 Track 关联 NQA 测试组，实现静态路由、Track 与 NQA 联动。

6.4 配置步骤

1. 配置 Switch A

创建 VLAN，在 VLAN 中加入对应的端口，并配置各 VLAN 接口的 IP 地址。

```
<SwitchA> system-view
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/1
[SwitchA-vlan2] quit
[SwitchA] vlan 3
[SwitchA-vlan3] port gigabitethernet 1/0/2
[SwitchA-vlan3] quit
[SwitchA] vlan 6
[SwitchA-vlan6] port gigabitethernet 1/0/3
[SwitchA-vlan6] quit
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 10.1.1.1 24
[SwitchA-Vlan-interface2] quit
[SwitchA] interface vlan-interface 3
[SwitchA-Vlan-interface3] ip address 10.3.1.1 24
[SwitchA-Vlan-interface3] quit
[SwitchA] interface vlan-interface 6
[SwitchA-Vlan-interface6] ip address 20.1.1.1 24
[SwitchA-Vlan-interface6] quit
```

配置到达 30.1.1.0/24 网段的静态路由：下一跳地址为 10.1.1.2，优先级为缺省值 60，该路由与 Track 项 1 关联。

```
[SwitchA] ip route-static 30.1.1.0 24 10.1.1.2 track 1
```

配置到达 10.2.1.0/24 网段的静态路由：下一跳地址为 10.1.1.2，优先级为缺省值 60。

```
[SwitchA] ip route-static 10.2.1.0 24 10.1.1.2
```
配置到达 30.1.1.0/24 网段的静态路由：下一跳地址为 10.3.1.3，优先级为 80。
```
[SwitchA] ip route-static 30.1.1.0 24 10.3.1.3 preference 80
```
配置到达 10.4.1.0/24 网段的静态路由：下一跳地址为 10.3.1.3，优先级为 80。
```
[SwitchA] ip route-static 10.4.1.0 24 10.3.1.3 preference 80
```
配置到达 10.2.1.4 的静态路由：下一跳地址为 10.1.1.2。
```
[SwitchA] ip route-static 10.2.1.4 24 10.1.1.2
```
创建管理员名为 admin、操作标签为 test 的 NQA 测试组。
```
[SwitchA] nqa entry admin test
```
配置测试类型为 ICMP-echo。
```
[SwitchA-nqa-admin-test] type icmp-echo
```
配置测试的目的地址为 10.2.1.4，下一跳地址为 10.1.1.2，以便通过 NQA 检测 Switch A－Switch B－Switch D 这条路径的连通性。
```
[SwitchA-nqa-admin-test-icmp-echo] destination ip 10.2.1.4
[SwitchA-nqa-admin-test-icmp-echo] next-hop ip 10.1.1.2
```
配置测试频率为 100ms。
```
[SwitchA-nqa-admin-test-icmp-echo] frequency 100
```
配置联动项 1（连续失败 5 次触发联动）。
```
[SwitchA-nqa-admin-test-icmp-echo] reaction 1 checked-element probe-fail threshold-type
consecutive 5 action-type trigger-only
[SwitchA-nqa-admin-test-icmp-echo] quit
```
启动探测。
```
[SwitchA] nqa schedule admin test start-time now lifetime forever
```
配置 Track 项 1，并进入 Track 视图，关联 NQA 测试组（管理员为 admin，操作标签为 test）的联动项 1。
```
[SwitchA] track 1 nqa entry admin test reaction 1
[SwitchA-track-1] quit
```
保存配置。
```
[SwitchA] save force
```
2. 配置 Switch B

创建 VLAN，在 VLAN 中加入对应的端口，并配置各 VLAN 接口的 IP 地址。
```
<SwitchB> system-view
[SwitchB] vlan 2
[SwitchB-vlan2] port gigabitethernet 1/0/1
[SwitchB-vlan2] quit
[SwitchB] vlan 5
[SwitchB-vlan5] port gigabitethernet 1/0/2
[SwitchB-vlan5] quit
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address 10.1.1.2 24
[SwitchB-Vlan-interface2] quit
[SwitchB] interface vlan-interface 5
[SwitchB-Vlan-interface5] ip address 10.2.1.2 24
```

```
[SwitchB-Vlan-interface5] quit
```
配置到达 30.1.1.0/24 网段的静态路由：下一跳地址为 10.2.1.4。
```
[SwitchB] ip route-static 30.1.1.0 24 10.2.1.4
```
配置到达 20.1.1.0/24 网段的静态路由：下一跳地址为 10.1.1.1。
```
[SwitchB] ip route-static 20.1.1.0 24 10.1.1.1
```
保存配置。
```
[SwitchB] save force
```
3. 配置 Switch C
创建 VLAN，在 VLAN 中加入对应的端口，并配置各 VLAN 接口的 IP 地址。
```
<SwitchC> system-view
[SwitchC] vlan 3
[SwitchC-vlan3] port gigabitethernet 1/0/1
[SwitchC-vlan3] quit
[SwitchC] vlan 4
[SwitchC-vlan4] port gigabitethernet 1/0/2
[SwitchC-vlan4] quit
[SwitchC] interface vlan-interface 3
[SwitchC-Vlan-interface3] ip address 10.3.1.3 24
[SwitchC-Vlan-interface3] quit
[SwitchC] interface vlan-interface 4
[SwitchC-Vlan-interface4] ip address 10.4.1.3 24
[SwitchC-Vlan-interface4] quit
```
配置到达 30.1.1.0/24 网段的静态路由：下一跳地址为 10.4.1.4。
```
[SwitchC] ip route-static 30.1.1.0 24 10.4.1.4
```
配置到达 20.1.1.0/24 网段的静态路由：下一跳地址为 10.3.1.1。
```
[SwitchC] ip route-static 20.1.1.0 24 10.3.1.1
```
保存配置。
```
[SwitchC] save force
```
4. 配置 Switch D
创建 VLAN，在 VLAN 中加入对应的端口，并配置各 VLAN 接口的 IP 地址。
```
<SwitchD> system-view
[SwitchD] vlan 4
[SwitchD-vlan4] port gigabitethernet 1/0/1
[SwitchD-vlan4] quit
[SwitchD] vlan 5
[SwitchD-vlan5] port gigabitethernet 1/0/2
[SwitchD-vlan5] quit
[SwitchD] vlan 7
[SwitchD-vlan7] port gigabitethernet 1/0/3
[SwitchD-vlan7] quit
[SwitchD] interface vlan-interface 4
[SwitchD-Vlan-interface6] ip address 10.4.1.4 24
[SwitchD-Vlan-interface6] quit
[SwitchD] interface vlan-interface 5
```

```
[SwitchD-Vlan-interface5] ip address 10.2.1.4 24
[SwitchD-Vlan-interface5] quit
[SwitchD] interface vlan-interface 7
[SwitchD-Vlan-interface7] ip address 30.1.1.1 24
[SwitchD-Vlan-interface7] quit
```

配置到达 20.1.1.0/24 网段的静态路由：下一跳地址为 10.2.1.2，优先级为缺省值 60，该路由与 Track 项 1 关联。

```
[SwitchD] ip route-static 20.1.1.0 24 10.2.1.2 track 1
```

配置到达 10.1.1.0/24 网段的静态路由：下一跳地址为 10.2.1.2，优先级为缺省值 60。

```
[SwitchD] ip route-static 10.1.1.0 24 10.2.1.2
```

配置到达 20.1.1.0/24 网段的静态路由：下一跳地址为 10.4.1.3，优先级为 80。

```
[SwitchD] ip route-static 20.1.1.0 24 10.4.1.3 preference 80
```

配置到达 10.3.1.0/24 网段的静态路由：下一跳地址为 10.4.1.3，优先级为 80。

```
[SwitchD] ip route-static 10.3.1.0 24 10.4.1.3 preference 80
```

配置到达 10.1.1.1 的静态路由：下一跳地址为 10.2.1.2。

```
[SwitchD] ip route-static 10.1.1.1 24 10.2.1.2
```

创建管理员名为 admin、操作标签为 test 的 NQA 测试组。

```
[SwitchD] nqa entry admin test
```

配置测试类型为 ICMP-echo。

```
[SwitchD-nqa-admin-test] type icmp-echo
```

配置测试的目的地址为 10.1.1.1，下一跳地址为 10.2.1.2，以便通过 NQA 检测 Switch D－Switch B－Switch A 这条路径的连通性。

```
[SwitchD-nqa-admin-test-icmp-echo] destination ip 10.1.1.1
[SwitchD-nqa-admin-test-icmp-echo] next-hop ip 10.2.1.2
```

配置测试频率为 100ms。

```
[SwitchD-nqa-admin-test-icmp-echo] frequency 100
```

配置联动项 1（连续失败 5 次触发联动）。

```
[SwitchD-nqa-admin-test-icmp-echo] reaction 1 checked-element probe-fail threshold-type
consecutive 5 action-type trigger-only
[SwitchD-nqa-admin-test-icmp-echo] quit
```

启动探测。

```
[SwitchD] nqa schedule admin test start-time now lifetime forever
```

配置 Track 项 1，并进入 Track 视图，关联 NQA 测试组（管理员为 admin，操作标签为 test）的联动项 1。

```
[SwitchD] track 1 nqa entry admin test reaction 1
[SwitchD-track-1] quit
```

保存配置。

```
[SwitchD] save force
```

6.5 验证配置

显示 Switch A 上 Track 项的信息。

```
[SwitchA] display track all
```

```
Track ID: 1
  State: Positive
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Tracked object type: NQA
  Notification delay: Positive 0, Negative 0 (in seconds)
  Tracked object:
    NQA entry: admin test
    Reaction: 1
    Remote IP/URL: 10.2.1.4
    Local IP: --
    Interface: --
```

显示 Switch A 的路由表。

```
[SwitchA] display ip routing-table

Destinations : 10       Routes : 10

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
10.1.1.0/24         Direct 0    0            10.1.1.1        Vlan2
10.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
10.2.1.0/24         Static 60   0            10.1.1.2        Vlan2
10.3.1.0/24         Direct 0    0            10.3.1.1        Vlan3
10.3.1.1/32         Direct 0    0            127.0.0.1       InLoop0
20.1.1.0/24         Direct 0    0            20.1.1.1        Vlan6
20.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
30.1.1.0/24         Static 60   0            10.1.1.2        Vlan2
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
```

以上显示信息表示，NQA 测试的结果为主路由可达（Track 项状态为 Positive），Switch A 通过 Switch B 将报文转发到 30.1.1.0/24 网段。

在 Switch B 上关闭 VLAN 接口 2 对应的以太网接口。

```
<SwitchB> system-view
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-Gigabitethernet 1/0/1] shutdown
```

显示 Switch A 上 Track 项的信息。

```
[SwitchA] display track all
Track ID: 1
  State: Negative
  Duration: 0 days 0 hours 0 minutes 32 seconds
  Tracked object type: NQA
  Notification delay: Positive 0, Negative 0 (in seconds)
  Tracked object:
    NQA entry: admin test
    Reaction: 1
    Remote IP/URL: 10.2.1.4
    Local IP: --
    Interface: --
```

显示 Switch A 的路由表。

```
[SwitchA] display ip routing-table

Destinations : 10       Routes : 10

Destination/Mask    Proto  Pre  Cost         NextHop         Interface
10.1.1.0/24         Direct 0    0            10.1.1.1        Vlan2
10.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
10.2.1.0/24         Static 60   0            10.1.1.2        Vlan2
10.3.1.0/24         Direct 0    0            10.3.1.1        Vlan3
10.3.1.1/32         Direct 0    0            127.0.0.1       InLoop0
20.1.1.0/24         Direct 0    0            20.1.1.1        Vlan6
20.1.1.1/32         Direct 0    0            127.0.0.1       InLoop0
30.1.1.0/24         Static 80   0            10.3.1.3        Vlan3
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
```

以上显示信息表示，NQA 测试的结果为主路由不可达（Track 项状态为 Negative），则备份路由生效，Switch A 通过 Switch C 将报文转发到 30.1.1.0/24 网段。

主路由出现故障后，20.1.1.0/24 网段内的主机仍然可以与 30.1.1.0/24 网段内的主机通信。

```
[SwitchA] ping -a 20.1.1.1 30.1.1.1
Ping 30.1.1.1: 56  data bytes, press CTRL+C to break
Reply from 30.1.1.1: bytes=56 Sequence=1 ttl=254 time=2 ms
Reply from 30.1.1.1: bytes=56 Sequence=2 ttl=254 time=1 ms
Reply from 30.1.1.1: bytes=56 Sequence=3 ttl=254 time=1 ms
Reply from 30.1.1.1: bytes=56 Sequence=4 ttl=254 time=2 ms
Reply from 30.1.1.1: bytes=56 Sequence=5 ttl=254 time=1 ms

--- Ping statistics for 30.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.00% packet loss
round-trip min/avg/max/std-dev = 1/1/2/1 ms
```

Switch D 上的显示信息与 Switch A 类似。主路由出现故障后，30.1.1.0/24 网段内的主机仍然可以与 20.1.1.0/24 网段内的主机通信。

```
[SwitchD] ping -a 30.1.1.1 20.1.1.1
Ping 20.1.1.1: 56  data bytes, press CTRL+C to break
Reply from 20.1.1.1: bytes=56 Sequence=1 ttl=254 time=2 ms
Reply from 20.1.1.1: bytes=56 Sequence=2 ttl=254 time=1 ms
Reply from 20.1.1.1: bytes=56 Sequence=3 ttl=254 time=1 ms
Reply from 20.1.1.1: bytes=56 Sequence=4 ttl=254 time=1 ms
Reply from 20.1.1.1: bytes=56 Sequence=5 ttl=254 time=1 ms

--- Ping statistics for 20.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.00% packet loss
round-trip min/avg/max/std-dev = 1/1/2/1 ms
```

6.6 配置文件

- Switch A：

```
#
```

```
vlan 2
#
vlan 3
#
vlan 6
#
nqa entry admin test
 type icmp-echo
  destination ip 10.2.1.4
  frequency 100
  next-hop ip 10.1.1.2
  reaction 1 checked-element probe-fail threshold-type consecutive 5 action-type
trigger-only
#
 nqa schedule admin test start-time now lifetime forever
#
interface Vlan-interface2
 ip address 10.1.1.1 255.255.255.0
#
interface Vlan-interface3
 ip address 10.3.1.1 255.255.255.0
#
interface Vlan-interface6
 ip address 20.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 3
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 6
#
 ip route-static 10.2.1.0 24 10.1.1.2
 ip route-static 30.1.1.0 24 10.1.1.2 track 1
 ip route-static 10.4.1.0 24 10.3.1.3 preference 80
 ip route-static 30.1.1.0 24 10.3.1.3 preference 80
#
 track 1 nqa entry admin test reaction 1
#
```

- Switch B：

```
#
vlan 2
#
```

```
vlan 5
#
interface Vlan-interface2
 ip address 10.1.1.2 255.255.255.0
#
interface Vlan-interface5
 ip address 10.2.1.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 5
#
 ip route-static 20.1.1.0 24 10.1.1.1
 ip route-static 30.1.1.0 24 10.2.1.4
#
```

- Switch C

```
#
vlan 3
#
vlan 4
#
interface Vlan-interface3
 ip address 10.3.1.3 255.255.255.0
#
interface Vlan-interface4
 ip address 10.4.1.3 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 3
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 4
#
 ip route-static 20.1.1.0 24 10.3.1.1
 ip route-static 30.1.1.0 24 10.4.1.4
#
```

- Switch D

```
#
vlan 4
#
vlan 5
#
```

```
vlan 7
#
nqa entry admin test
 type icmp-echo
  destination ip 10.1.1.1
  frequency 100
  next-hop ip 10.2.1.2
  reaction 1 checked-element probe-fail threshold-type consecutive 5 action-type
trigger-only
#
 nqa schedule admin test start-time now lifetime forever
#
interface Vlan-interface4
 ip address 10.4.1.4 255.255.255.0
#
interface Vlan-interface5
 ip address 10.2.1.4 255.255.255.0
#
interface Vlan-interface7
 ip address 30.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 4
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 5
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 7
#
 ip route-static 10.1.1.0 24 10.2.1.2
 ip route-static 20.1.1.0 24 10.2.1.2 track 1
 ip route-static 10.3.1.0 24 10.4.1.3 preference 80
 ip route-static 20.1.1.0 24 10.4.1.3 preference 80
#
 track 1 nqa entry admin test reaction 1
#
```

6.7 相关资料

- 产品配套“三层技术-IP 路由配置指导”中的“静态路由”。
- 产品配套“三层技术-IP 路由命令参考”中的“静态路由”。
- 产品配套“可靠性配置指导”中的“Track”。
- 产品配套“可靠性命令参考”中的“Track”。

7 跨网段登录设备 Web 页面

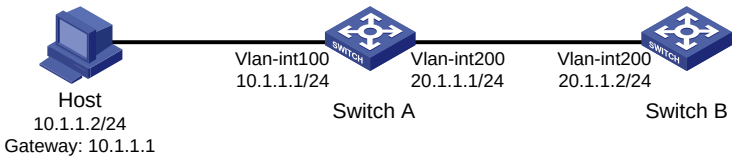
7.1 简介

本案例介绍使用 HTTP 方式跨网段登录设备 Web 页面的配置方法。

7.2 组网需求

如图 7 所示，Host 与交换机设备通过 IP 网络相连且路由可达，要求 Host 能通过 HTTP 方式跨网段登录 Switch B 的 Web 页面。

图7 跨网段登录设备 Web 页面组网图



7.3 配置步骤

1. 配置 Switch A

创建 VLAN，在 VLAN 中加入对应的端口，并配置各 VLAN 接口的 IP 地址。

```
<SwitchA> system-view
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1
[SwitchA-vlan100] quit
[SwitchA] vlan 200
[SwitchA-vlan200] port gigabitethernet 1/0/2
[SwitchA-vlan200] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ip address 10.1.1.1 24
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 200
[SwitchA-Vlan-interface200] ip address 20.1.1.1 24
[SwitchA-Vlan-interface200] quit
```

保存配置。

```
[SwitchA] save force
```

2. 配置 Switch B

创建 VLAN，在 VLAN 中加入对应的端口，并配置各 VLAN 接口的 IP 地址。

```
<SwitchB> system-view
[SwitchB] vlan 200
[SwitchB-vlan200] port gigabitethernet 1/0/1
[SwitchB-vlan200] quit
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] ip address 20.1.1.2 24
```

```
[SwitchB-Vlan-interface200] quit
```

配置Web用户名为admin，认证密码为hello12345，服务类型为http，用户角色为network-admin。

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

配置开启 HTTP 服务。

```
[SwitchB] ip http enable
```

配置静态路由。

```
[SwitchB] ip route-static 10.1.1.0 24 20.1.1.1
```

保存配置。

```
[SwitchB] save force
```

3. 配置 Host

为 Host 配置 IP 地址为 10.1.1.2，掩码为 255.255.255.0，网关地址为 10.1.1.1。

7.4 验证配置

在 Host 上使用 **ping** 命令验证 Switch B 是否可达（假定主机安装的操作系统为 Windows XP）。

```
C:\Documents and Settings\Administrator>ping 20.1.1.2

Pinging 20.1.1.2 with 32 bytes of data:

Reply from 20.1.1.2: bytes=32 time=1ms TTL=126
Reply from 20.1.1.2: bytes=32 time=1ms TTL=126
Reply from 20.1.1.2: bytes=32 time=1ms TTL=126
Reply from 20.1.1.2: bytes=32 time=1ms TTL=126

Ping statistics for 20.1.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

在 Host 的浏览器地址栏内输入 Switch B 的 IP 地址并回车，浏览器将显示 Web 登录页面。在本页面输入用户名和密码，点击<登录>按钮后即可登录。成功登录后，用户可以在配置区对设备进行相关配置。

图8 Switch B 的 Web 登录页面

7.5 配置文件

- Switch A：

```
#
vlan 100
#
vlan 200
interface Vlan-interface100
 ip address 10.1.1.1 255.255.255.0
#
interface Vlan-interface200
 ip address 20.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 200
#
```

- Switch B ：

```
#
vlan 200
#
interface Vlan-interface200
 ip address 20.1.1.2 255.255.255.0
#
```

```
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 200
#
 ip route-static 10.1.1.0 24 20.1.1.1
#
local-user admin class manage
 password hash
$h$6$BdqhpnjJwOBmHmmt$rQ/FQ6WnS9gVhEpdZY3hjvWSYxCtI+9ngtivuAwrvFdCDVE8AepcSxtprJR5XAdrYb
XQE76FumgUszLRn03a0g==
 service-type http
 authorization-attribute user-role network-admin
 authorization-attribute user-role network-operator
#
 ip http enable
#
```

7.6 相关资料

- 产品配套“三层技术-IP 路由配置指导”中的“静态路由”。
- 产品配套“三层技术-IP 路由命令参考”中的“静态路由”。
- 产品配套“基础配置指导”中的“登录设备”。
- 产品配套“基础命令参考”中的“登录设备”。

RIP 基本功能快速配置指南

目 录

1 RIP 基本功能配置

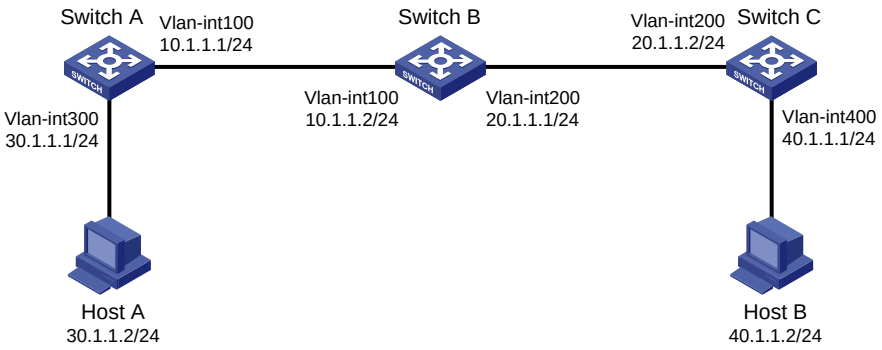
1.1 简介

本案例介绍 RIP 基本功能的配置方法。

1.2 组网需求

如图 1 所示，要求所有交换机均运行 RIP-2 协议，Host A 和 Host B 两台主机能互相通信。

图1 RIP 基本配置组网图



1.3 配置步骤

1. 配置 Host A 和 Host B

为 Host A 配置 IP 地址为 30.1.1.2，掩码为 255.255.255.0，网关地址为 30.1.1.1。

为 Host B 配置 IP 地址为 40.1.1.2，掩码为 255.255.255.0，网关地址为 40.1.1.1。

2. 配置 Switch A

创建 VLAN，在 VLAN 中加入对应的端口，并配置各 VLAN 接口的 IP 地址。

```
<SwitchA> system-view
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1
[SwitchA-vlan100] quit
[SwitchA] vlan 300
[SwitchA-vlan300] port gigabitethernet 1/0/2
[SwitchA-vlan300] quit
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ip address 10.1.1.1 24
[SwitchA-Vlan-interface100] quit
[SwitchA] interface vlan-interface 300
[SwitchA-Vlan-interface300] ip address 30.1.1.1 24
[SwitchA-Vlan-interface300] quit
```

配置 RIP-2。

```
[SwitchA] rip
[SwitchA-rip-1] network 10.1.1.0
[SwitchA-rip-1] network 30.1.1.0
[SwitchA-rip-1] version 2
[SwitchA-rip-1] undo summary
[SwitchA-rip-1] quit
```

保存配置。

```
[SwitchA] save force
```

3. 配置 Switch B

创建 VLAN，在 VLAN 中加入对应的端口，并配置各 VLAN 接口的 IP 地址。

```
<SwitchB> system-view
[SwitchB] vlan 100
[SwitchB-vlan100] port gigabitethernet 1/0/1
[SwitchB-vlan100] quit
[SwitchB] vlan 200
[SwitchB-vlan200] port gigabitethernet 1/0/2
[SwitchB-vlan200] quit
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ip address 10.1.1.2 24
[SwitchB-Vlan-interface100] quit
[SwitchB] interface vlan-interface 200
[SwitchB-Vlan-interface200] ip address 20.1.1.1 24
[SwitchB-Vlan-interface200] quit
```

配置 RIP-2。

```
[SwitchB] rip
[SwitchB-rip-1] network 10.1.1.0
[SwitchB-rip-1] network 20.1.1.0
[SwitchB-rip-1] version 2
[SwitchB-rip-1] undo summary
[SwitchB-rip-1] quit
```

保存配置。

```
[SwitchB] save force
```

4. 配置 Switch C

创建 VLAN，在 VLAN 中加入对应的端口，并配置各 VLAN 接口的 IP 地址。

```
<SwitchC> system-view
[SwitchC] vlan 200
[SwitchC-vlan200] port gigabitethernet 1/0/1
[SwitchC-vlan200] quit
[SwitchC] vlan 400
[SwitchC-vlan400] port gigabitethernet 1/0/2
[SwitchC-vlan400] quit
[SwitchC] interface vlan-interface 200
[SwitchC-Vlan-interface200] ip address 20.1.1.2 24
[SwitchC-Vlan-interface200] quit
[SwitchC] interface vlan-interface 400
[SwitchC-Vlan-interface400] ip address 40.1.1.1 24
```

```
[SwitchC-Vlan-interface400] quit
```
配置 RIP-2。
```
[SwitchC] rip
[SwitchC-rip-1] network 20.1.1.0
[SwitchC-rip-1] network 40.1.1.0
[SwitchC-rip-1] version 2
[SwitchC-rip-1] undo summary
[SwitchC-rip-1] quit
```
保存配置。
```
[SwitchC] save force
```

1.4 验证配置

查看 Switch A 的 RIP 路由表信息。
```
[SwitchA] display rip 1 route
 Route Flags: R - RIP, T - TRIP
              P - Permanent, A - Aging, S - Suppressed, G - Garbage-collect
              D - Direct, O - Optimal, F - Flush to RIB
 ------------------------------------------------------------------------------
 Peer 10.1.1.2 on Vlan-interface100
      Destination/Mask        Nexthop          Cost    Tag     Flags   Sec
      20.1.1.0/24             10.1.1.2         1       0       RAOF    27
      40.1.1.0/24             10.1.1.2         2       0       RAOF    27
 Local route
      Destination/Mask        Nexthop          Cost    Tag     Flags   Sec
      10.1.1.0/24             0.0.0.0          0       0       RDOF    -
      30.1.1.0/24             0.0.0.0          0       0       RDOF    -
```
查看 Switch B 的 RIP 路由表信息。
```
[SwitchB] display rip 1 route
 Route Flags: R - RIP, T - TRIP
              P - Permanent, A - Aging, S - Suppressed, G - Garbage-collect
              D - Direct, O - Optimal, F - Flush to RIB
 ------------------------------------------------------------------------------
 Peer 10.1.1.1 on Vlan-interface100
      Destination/Mask        Nexthop          Cost    Tag     Flags   Sec
      30.1.1.0/24             10.1.1.1         1       0       RAOF    0
 Peer 20.1.1.2 on Vlan-interface200
      Destination/Mask        Nexthop          Cost    Tag     Flags   Sec
      40.1.1.0/24             20.1.1.2         1       0       RAOF    9
 Local route
      Destination/Mask        Nexthop          Cost    Tag     Flags   Sec
      20.1.1.0/24             0.0.0.0          0       0       RDOF    -
      10.1.1.0/24             0.0.0.0          0       0       RDOF    -
```
查看 Switch C 的 RIP 路由表信息。
```
[SwitchC] display rip 1 route
 Route Flags: R - RIP, T - TRIP
              P - Permanent, A - Aging, S - Suppressed, G - Garbage-collect
```

```
              D - Direct, O - Optimal, F - Flush to RIB
 ------------------------------------------------------------------------------
 Peer 20.1.1.1 on Vlan-interface200
      Destination/Mask        Nexthop          Cost    Tag     Flags   Sec
      10.1.1.0/24             20.1.1.1         1       0       RAOF    32
      30.1.1.0/24             20.1.1.1         2       0       RAOF    32
 Local route
      Destination/Mask        Nexthop          Cost    Tag     Flags   Sec
      20.1.1.0/24             0.0.0.0          0       0       RDOF    -
      40.1.1.0/24             0.0.0.0          0       0       RDOF    -
```

在 Host A 上使用 **ping** 命令验证 Host B 是否可达（假定主机安装的操作系统为 Windows XP）。

```
C:\Documents and Settings\Administrator>ping 40.1.1.2

Pinging 40.1.1.2 with 32 bytes of data:

Reply from 40.1.1.2: bytes=32 time=1ms TTL=126
Reply from 40.1.1.2: bytes=32 time=1ms TTL=126
Reply from 40.1.1.2: bytes=32 time=1ms TTL=126
Reply from 40.1.1.2: bytes=32 time=1ms TTL=126

Ping statistics for 40.1.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

1.5 配置文件

- Switch A：

```
#
rip 1
 undo summary
 version 2
 network 10.0.0.0
 network 30.0.0.0
#
vlan 100
#
vlan 300
#
interface Vlan-interface100
 ip address 10.1.1.1 255.255.255.0
#
interface Vlan-interface300
 ip address 30.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
```

```
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 300
#
```

- Switch B：

```
#
rip 1
 undo summary
 version 2
 network 10.0.0.0
 network 20.0.0.0
#
vlan 100
#
vlan 200
#
interface Vlan-interface100
 ip address 10.1.1.2 255.255.255.0
#
interface Vlan-interface200
 ip address 20.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 200
#
```

- Switch C：

```
#
rip 1
 undo summary
 version 2
 network 20.0.0.0
 network 40.0.0.0
#
vlan 200
#
vlan 400
#
interface Vlan-interface200
 ip address 20.1.1.2 255.255.255.0
#
interface Vlan-interface400
 ip address 40.1.1.1 255.255.255.0
```

```
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 200
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 400
#
```

1.6 相关资料

- 产品配套“三层技术-IP 路由配置指导”中的“RIP”。
- 产品配套“三层技术-IP 路由命令参考”中的“RIP”。

策略路由快速配置指南

目 录

1 配置基于报文源 IPv4 地址的策略路由

1.1 简介

本案例介绍基于报文源 IPv4 地址的策略路由的配置方法。

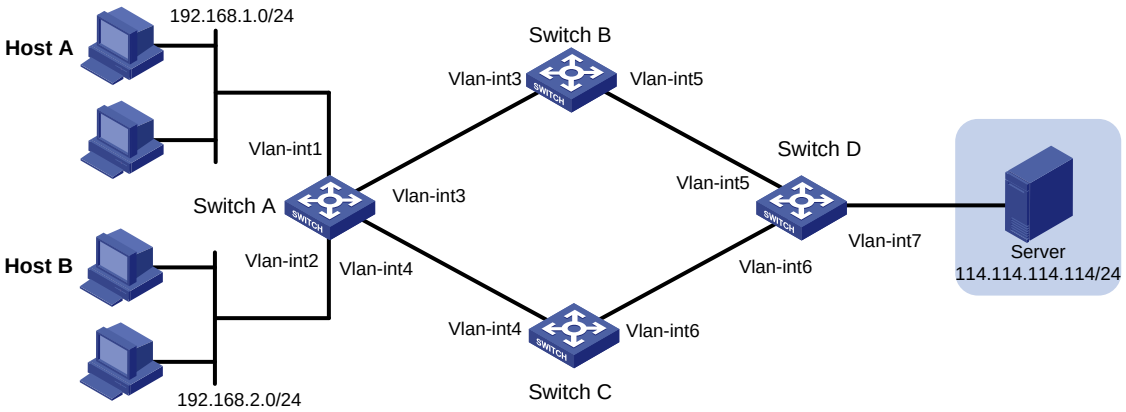
1.2 组网需求

如图 1 所示，Switch A 分别与 Switch B 和 Switch C 相连。配置静态路由，使 Switch A 收到的所有访问服务器 114.114.114.114/24 的报文都根据路由表从 Switch B 转发。

现要求在 Switch A 上配置策略路由，控制访问服务器 114.114.114.114/24 的报文：

- 匹配 Vlan-interface2 上收到的源地址为 192.168.2.0/24 报文，将该报文的下一跳重定向到 Switch C 转发；
- 其他报文仍从 Switch B 转发。

图1 基于报文源 IPv4 地址的策略路由配置组网图



设备	接口	IP地址	设备	接口	IP地址
Switch A	Vlan-int1	192.168.1.1/24	Switch C	Vlan-int4	20.20.20.2/24
	Vlan-int2	192.168.2.1/24		Vlan-int6	40.40.40.1/24
	Vlan-int3	10.10.10.1/24	Switch D	Vlan-int5	30.30.30.2/24
	Vlan-int4	20.20.20.1/24		Vlan-int6	40.40.40.2/24
Switch B	Vlan-int3	10.10.10.2/24		Vlan-int7	114.114.114.1/24
	Vlan-int5	30.30.30.1/24			

1.3 配置步骤

1. 配置 Host A 和 Host B

为 Host A 配置 IP 地址为 192.168.1.2，掩码为 255.255.255.0，网关地址为 192.168.1.1。

为 Host B 配置 IP 地址为 192.168.2.2，掩码为 255.255.255.0，网关地址为 192.168.2.1。

2. 配置 Switch A

创建 VLAN，在 VLAN 中加入对应的端口，并配置各 VLAN 接口的 IP 地址。

```
<SwitchA> system-view
[SwitchA] vlan 1
[SwitchA-vlan1] port gigabitethernet 1/0/1
[SwitchA-vlan1] quit
[SwitchA] vlan 2
[SwitchA-vlan2] port gigabitethernet 1/0/2
[SwitchA-vlan2] quit
[SwitchA] vlan 3
[SwitchA-vlan3] port gigabitethernet 1/0/3
[SwitchA-vlan3] quit
[SwitchA] vlan 4
[SwitchA-vlan4] port gigabitethernet 1/0/4
[SwitchA-vlan4] quit
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ip address 192.168.1.1 24
[SwitchA-Vlan-interface1] quit
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 192.168.2.1 24
[SwitchA-Vlan-interface2] quit
[SwitchA] interface vlan-interface 3
[SwitchA-Vlan-interface3] ip address 10.10.10.1 24
[SwitchA-Vlan-interface3] quit
[SwitchA] interface vlan-interface 4
[SwitchA-Vlan-interface4] ip address 20.20.20.1 24
[SwitchA-Vlan-interface4] quit
```

配置目的地址是 114.114.114.114/24 的静态路由。在未配置策略路由的情况下，所有访问目的地址 114.114.114.114/24 的报文均从 Switch B 转发。

```
[SwitchA] ip route-static 114.114.114.114 24 10.10.10.2
```

定义访问控制列表 ACL 3000，用来匹配源地址为 192.168.2.0/24 网段的报文。

```
[SwitchA] acl advanced 3000
[SwitchA-acl-ipv4-adv-3000] rule permit ip source 192.168.2.0 0.0.0.255
[SwitchA-acl-ipv4-adv-3000] quit
```

定义访问控制列表 ACL 3001，用来匹配源地址为 192.168.2.0/24 网段，目的地址是 192.168.1.0/24 的报文。

```
[SwitchA] acl advanced 3001
[SwitchA-acl-ipv4-adv-3001] rule permit ip source 192.168.2.0 0.0.0.255 destination
192.168.1.0 0.0.0.255
[SwitchA-acl-ipv4-adv-3001] quit
```

创建策略路由，名称为 aaa，节点为 10，匹配 ACL 3001 的数据流，不设置 apply 动作，从而避免 SwitchA 不同接口之间互相访问的流量被拦截（如果不设置动作，则匹配到的数据转发时根据路由表来进行转，且不再匹配下一节点，配置这个节点的作用是实现内网不同网段之间互访的流量不匹配策略路由，达到可以互访的目的。缺省情况下，网关在路由器上的不同网段是可以互相访问的）。

```
[SwitchA] policy-based-route aaa permit node 10
[SwitchA-pbr-aaa-10] if-match acl 3001
```

```
[SwitchA-pbr-aaa-10] quit
```
创建策略路由 aaa 的节点 20，匹配 ACL 3000 的数据流，设置 apply 动作，指定数据的下一跳为 20.20.20.2。
```
[SwitchA] policy-based-route aaa permit node 20
[SwitchA-pbr-aaa-20] if-match acl 3000
[SwitchA-pbr-aaa-20] apply next-hop 20.20.20.2
[SwitchA-pbr-aaa-20] quit
```
在 SwitchA 的 Vlan-interface2 接口上应用策略路由。
```
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip policy-based-route aaa
[SwitchA-Vlan-interface2] quit
```
开启设备的 ICMP 目的不可达报文的发送功能。
```
[SwitchA] ip unreachables enable
```
开启 ICMP 超时报文发送功能。
```
[SwitchA] ip ttl-expires enable
```
保存配置。
```
[SwitchA] save force
```
3. 配置 Switch B

创建 VLAN，在 VLAN 中加入对应的端口，并配置各 VLAN 接口的 IP 地址。
```
<SwitchB> system-view
[SwitchB] vlan 3
[SwitchB-vlan3] port gigabitethernet 1/0/1
[SwitchB-vlan3] quit
[SwitchB] vlan 5
[SwitchB-vlan5] port gigabitethernet 1/0/2
[SwitchB-vlan5] quit
[SwitchB] interface vlan-interface 3
[SwitchB-Vlan-interface3] ip address 10.10.10.2 24
[SwitchB-Vlan-interface3] quit
[SwitchB] interface vlan-interface 5
[SwitchB-Vlan-interface5] ip address 30.30.30.1 24
[SwitchB-Vlan-interface5] quit
```
配置访问 114.114.114.114/32 的静态路由。
```
[SwitchB] ip route-static 114.114.114.114 24 30.30.30.2
```
配置访问 192.168.1.0/24 的静态路由。
```
[SwitchB] ip route-static 192.168.1.0 24 10.10.10.1
```
配置访问 192.168.2.0/24 的静态路由。
```
[SwitchB] ip route-static 192.168.2.0 24 10.10.10.1
```
开启设备的 ICMP 目的不可达报文的发送功能。
```
[SwitchB] ip unreachables enable
```
开启 ICMP 超时报文发送功能。
```
[SwitchB] ip ttl-expires enable
```
保存配置。
```
[SwitchB] save force
```

4. 配置 Switch C

创建 VLAN，在 VLAN 中加入对应的端口，并配置各 VLAN 接口的 IP 地址。

```
<SwitchC> system-view
[SwitchC] vlan 4
[SwitchC-vlan4] port gigabitethernet 1/0/1
[SwitchC-vlan4] quit
[SwitchC] vlan 6
[SwitchC-vlan6] port gigabitethernet 1/0/2
[SwitchC-vlan6] quit
[SwitchC] interface vlan-interface 4
[SwitchC-Vlan-interface4] ip address 20.20.20.2 24
[SwitchC-Vlan-interface4] quit
[SwitchC] interface vlan-interface 6
[SwitchC-Vlan-interface6] ip address 40.40.40.1 24
[SwitchC-Vlan-interface6] quit
```

配置访问 114.114.114.114/32 的静态路由。

```
[SwitchC] ip route-static 114.114.114.114 24 40.40.40.2
```

配置访问 192.168.1.0/24 的静态路由。

```
[SwitchC] ip route-static 192.168.1.0 24 20.20.20.1
```

配置访问 192.168.2.0/24 的静态路由。

```
[SwitchC] ip route-static 192.168.2.0 24 20.20.20.1
```

开启设备的 ICMP 目的不可达报文的发送功能。

```
[SwitchC] ip unreachables enable
```

开启 ICMP 超时报文发送功能。

```
[SwitchC] ip ttl-expires enable
```

保存配置。

```
[SwitchC] save force
```

5. 配置 Switch D

创建 VLAN，在 VLAN 中加入对应的端口，并配置各 VLAN 接口的 IP 地址。

```
<SwitchD> system-view
[SwitchD] vlan 5
[SwitchD-vlan5] port gigabitethernet 1/0/1
[SwitchD-vlan5] quit
[SwitchD] vlan 6
[SwitchD-vlan6] port gigabitethernet 1/0/2
[SwitchD-vlan6] quit
[SwitchD] vlan 7
[SwitchD-vlan7] port gigabitethernet 1/0/3
[SwitchD-vlan7] quit
[SwitchD] interface vlan-interface 5
[SwitchD-Vlan-interface5] ip address 30.30.30.2 24
[SwitchD-Vlan-interface5] quit
[SwitchD] interface vlan-interface 6
[SwitchD-Vlan-interface6] ip address 40.40.40.2 24
[SwitchD-Vlan-interface6] quit
```

```
[SwitchD] interface vlan-interface 7
[SwitchD-Vlan-interface7] ip address 114.114.114.1 24
[SwitchD-Vlan-interface7] quit
```
配置访问 192.168.1.0/24 的静态路由。
```
[SwitchD] ip route-static 192.168.1.0 24 30.30.30.1
```
配置访问 192.168.2.0/24 的静态路由。
```
[SwitchD] ip route-static 192.168.2.0 24 40.40.40.1
```
开启设备的 ICMP 目的不可达报文的发送功能。
```
[SwitchD] ip unreachables enable
```
开启 ICMP 超时报文发送功能。
```
[SwitchD] ip ttl-expires enable
```
保存配置。
```
[SwitchD] save force
```

1.4 验证配置

在 Switch A 上通过 **display ip policy-based-route** 命令可以查看到当前策略路由配置已经配置成功。
```
[SwitchA] display ip policy-based-route interface Vlan-interface 2
Policy-based routing information for interface Vlan-interface2:
Policy name: aaa
  node 10 permit:
    if-match acl 3001
  Matches: 0, bytes: 0
  node 20 permit:
    if-match acl 3000
    apply next-hop 20.20.20.2
  Matches: 0, bytes: 0
Total matches: 0, total bytes: 0
```
在 Host A 上使用 **tracert** 命令验证服务器 114.114.114.114/24 是否可达（使用 Tracert 功能需要在中间设备上开启 ICMP 超时报文发送功能，在目的端开启 ICMP 目的不可达报文发送功能）。可以看到报文从 Switch B 转发。
```
C:\Documents and Settings\Administrator>tracert 114.114.114.114

Tracing route to 114.114.114.114 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms  192.168.1.1
  2    <1 ms    <1 ms    <1 ms  10.10.10.2
  3    <1 ms    <1 ms    <1 ms  30.30.30.2
  4     1 ms    <1 ms    <1 ms  114.114.114.114

Trace complete.
```
在 Host B 上使用 **tracert** 命令验证服务器 114.114.114.114/24 是否可达。可以看到报文从 Switch C 转发，策略路由配置成功。
```
C:\Documents and Settings\Administrator>tracert 114.114.114.114
```

```
Tracing route to 114.114.114.114 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms  192.168.2.1
  2    <1 ms    <1 ms    <1 ms  20.20.20.2
  3    <1 ms    <1 ms    <1 ms  40.40.40.2
  4     1 ms    <1 ms    <1 ms  114.114.114.114

Trace complete.
```

1.5 配置文件

- Switch A：

```
#
 ip unreachables enable
 ip ttl-expires enable
#
vlan 1
#
vlan 2 to 4
#
policy-based-route aaa permit node 10
 if-match acl 3001
#
policy-based-route aaa permit node 20
 if-match acl 3000
 apply next-hop 20.20.20.2
#
interface Vlan-interface1
 ip address 192.168.1.1 255.255.255.0
#
interface Vlan-interface2
 ip address 192.168.2.1 255.255.255.0
 ip policy-based-route aaa
#
interface Vlan-interface3
 ip address 10.10.10.1 255.255.255.0
#
interface Vlan-interface4
 ip address 20.20.20.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
interface GigabitEthernet1/0/3
```

```
 port link-mode bridge
 port access vlan 3
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port access vlan 4
#
 ip route-static 114.114.114.114 24 10.10.10.2
#
acl advanced 3000
 rule 0 permit ip source 192.168.2.0 0.0.0.255
#
acl advanced 3001
 rule 0 permit ip source 192.168.2.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
#
```

- Switch B：

```
#
 ip unreachables enable
 ip ttl-expires enable
#
vlan 3
#
vlan 5
#
interface Vlan-interface3
 ip address 10.10.10.2 255.255.255.0
#
interface Vlan-interface5
 ip address 30.30.30.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 3
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 5
#
 ip route-static 114.114.114.114 24 30.30.30.2
 ip route-static 192.168.1.0 24 10.10.10.1
 ip route-static 192.168.2.0 24 10.10.10.1
#
```

- Switch C：

```
#
 ip unreachables enable
 ip ttl-expires enable
#
vlan 4
```

```
#
vlan 6
#
interface Vlan-interface4
 ip address 20.20.20.2 255.255.255.0
#
interface Vlan-interface6
 ip address 40.40.40.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 4
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 6
#
 ip route-static 114.114.114.114 24 40.40.40.2
 ip route-static 192.168.1.0 24 20.20.20.1
 ip route-static 192.168.2.0 24 20.20.20.1
#
```

- Switch D：

```
#
 ip unreachables enable
 ip ttl-expires enable
#
vlan 5 to 7
#
interface Vlan-interface5
 ip address 30.30.30.2 255.255.255.0
#
interface Vlan-interface6
 ip address 40.40.40.2 255.255.255.0
#
interface Vlan-interface7
 ip address 114.114.114.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 5
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 6
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 7
```

```
#
 ip route-static 192.168.1.0 24 30.30.30.1
 ip route-static 192.168.2.0 24 40.40.40.1
#
```

1.6 相关资料

- 产品配套“三层技术-IP 路由配置指导”中的“策略路由”。
- 产品配套“三层技术-IP 路由命令参考”中的“策略路由”。

IGMP snooping 快速配置指南

目 录

1 IGMP snooping 快速配置指南

1.1 简介

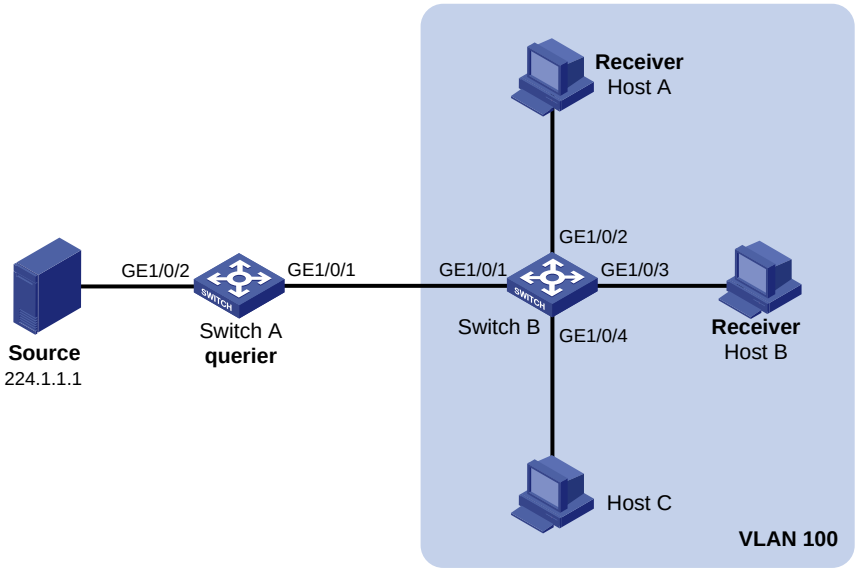
本案例介绍如何配置 IGMP snooping。

1.2 组网需求

如图 1 所示，在一个没有三层设备的纯二层网络环境中，组播源 Source 向组播组 224.1.1.1 发送组播数据，Host A 和 Host B 是组播组 224.1.1.1 的接收者（Receiver），Host C 不是组播组 224.1.1.1 的接收者。所有接收者均使用 IGMPv2，保持所有交换机上都运行版本 2 的 IGMP Snooping 不变，并选择距组播源较近的 Switch A 来充当 IGMP Snooping 查询器。

为防止组播数据在二层网络中广播，在 Switch B 上开启 IGMP snooping，使组播数据仅发送给指定接收者（Host A 和 Host B）。

图1 IGMP snooping 配置组网图



1.3 配置步骤

1. 配置 Switch A

开启设备的 IGMP Snooping 特性。

```
<SwitchA> system-view
[SwitchA] igmp-snooping
[SwitchA-igmp-snooping] quit
```

创建 VLAN 100，把端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 添加到该 VLAN 中；在该 VLAN 内使能 IGMP Snooping。

```
[SwitchA] vlan 100
[SwitchA-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/2
```

```
[SwitchA-vlan100] igmp-snooping enable
```

在 VLAN 100 内开启 IGMP Snooping 查询器。

```
[SwitchA-vlan100] igmp-snooping querier
[SwitchA-vlan100] quit
```

保存配置，防止配置丢失

```
[SwitchA] save
```

2. 配置 Switch B

开启设备的 IGMP Snooping 特性。

```
<SwitchB> system-view
[SwitchB] igmp-snooping
[SwitchB-igmp-snooping] quit
```

创建 VLAN 100，把端口 GigabitEthernet1/0/1 到 GigabitEthernet1/0/4 添加到该 VLAN 中；在该 VLAN 内使能 IGMP Snooping。

```
[SwitchB] vlan 100
[SwitchB-vlan100] port gigabitethernet 1/0/1 to gigabitethernet 1/0/4
[SwitchB-vlan100] igmp-snooping enable
[SwitchB-vlan100] quit
```

1.4 验证配置

显示 Switch B 上 IGMP Snooping 组播组的信息。

```
<SwitchB> display igmp-snooping group
Total 2 entries.

VLAN 100: Total 2 entries.
  (0.0.0.0, 224.1.1.1)
    Host ports (2 in total):
      GE1/0/2                          (00:03:23)
      GE1/0/3                          (00:03:23)
```

连接 Host C 的端口 GE1/0/4 不在 IGMP snooping 组播组信息中，组播数据将不会发送给 Host C。

1.5 配置文件

1. Switch A 的配置

```
#
igmp-snooping
#
vlan 100
 igmp-snooping enable
 igmp-snooping querier
#
interface GigabitEthernet1/0/1
 port access vlan 100
#
interface GigabitEthernet1/0/2
```

```
 port access vlan 100
#
```

2. Switch B 的配置

```
#
igmp-snooping
#
vlan 100
 igmp-snooping enable
#
interface GigabitEthernet1/0/1
 port access vlan 100
#
interface GigabitEthernet1/0/2
 port access vlan 100
#
interface GigabitEthernet1/0/3
 port access vlan 100
#
interface GigabitEthernet1/0/4
 port access vlan 100
#
```

1.6 相关资料

- 产品配套“IP 组播配置指导”中的“IGMP snooping”。
- 产品配套“IP 组播命令参考”中的“IGMP snooping”。

报文过滤配置快速配置指南

目 录

1 配置报文过滤

1.1 简介

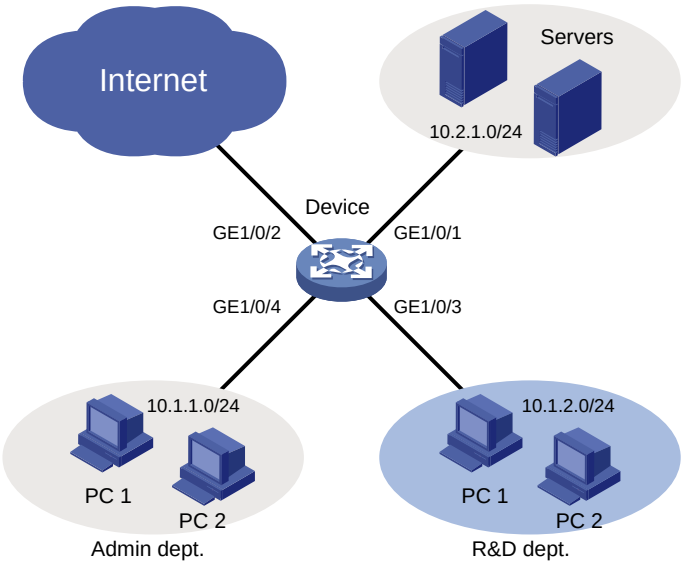
本案例介绍报文过滤的配置方法。

1.2 组网需求

如 1.2 图 1 所示，某公司的网络分成管理部、研发部和服务器三个区域，通过 Device 设备与 Internet 连接。现要求通过 ACL 实现：

- 管理部任意时间都可以访问 Internet 和服务器，但不能访问研发部；
- 研发部只能访问服务器，不能访问 Internet 和管理部。

图1 通过 IP 地址过滤流量配置组网图



1.3 配置步骤

(1) 配置管理部的网络权限

创建 IPv4 高级 ACL 3000。

```
<Device> system-view
[Device] acl advanced 3000
```

创建规则，过滤目的地址为 10.1.2.0/24 网段的报文。

```
[Device-acl-ipv4-adv-3000] rule deny ip destination 10.1.2.0 0.0.0.255
[Device-acl-ipv4-adv-3000] quit
```

配置包过滤功能，应用 IPv4 高级 ACL 3000 对端口 GigabitEthernet1/0/4 收到的 IP 报文进行过滤。

```
[Device] interface gigabitethernet 1/0/4
```

```
[Device-GigabitEthernet1/0/4] packet-filter 3000 inbound
[Device-GigabitEthernet1/0/4] quit
```

(2) 配置研发部的网络权限

创建 IPv4 高级 ACL 3001。

```
[Device] acl advanced 3001
```

创建规则，允许目的地址为 10.2.1.0/24 网段的报文通过。

```
[Device-acl-ipv4-adv-3001] rule permit ip destination 10.2.1.0 0.0.0.255
```

创建规则，不允许目的地址为其他网段的报文通过。

```
[Device-acl-ipv4-adv-3001] rule deny ip
```

配置包过滤功能，应用 IPv4 高级 ACL 3001 对端口 GigabitEthernet1/0/3 收到的 IP 报文进行过滤。

```
[Device] interface gigabitethernet 1/0/3
[Device-GigabitEthernet1/0/3] packet-filter 3001 inbound
[Device-GigabitEthernet1/0/3] quit
```

1.4 验证配置

执行 **display packet-filter** 命令查看包过滤功能的应用状态。

```
[Device] display packet-filter interface inbound
Interface: GigabitEthernet1/0/3
 Inbound policy:
  IPv4 ACL 3001
Interface: GigabitEthernet1/0/4
 Inbound policy:
  IPv4 ACL 3000
```

上述信息显示 GigabitEthernet1/0/3 和 GigabitEthernet1/0/4 端口上已经正确应用了包过滤功能。

从研发部的某台电脑上 ping Internet 上某个网站，结果无法 ping 通。

```
C:\>ping www.google.com

Pinging www.google.com [172.217.194.99] with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 173.194.127.242:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
```

从研发部的某台电脑上 ping 10.2.1.10 服务器的某台设备，可以 ping 通。

```
C:\>ping 10.2.1.10
Ping 192.168.1.60 (10.2.1.10): 56 data bytes, press CTRL+C to break
56 bytes from 10.2.1.10: icmp_seq=0 ttl=255 time=12.963 ms
56 bytes from 10.2.1.10: icmp_seq=1 ttl=255 time=4.168 ms
56 bytes from 10.2.1.10: icmp_seq=2 ttl=255 time=7.390 ms
```

```
56 bytes from 10.2.1.10: icmp_seq=3 ttl=255 time=3.363 ms
56 bytes from 10.2.1.10: icmp_seq=4 ttl=255 time=2.901 ms
C:\>
```

从管理部的某台电脑上 ping Internet 上某个网站，结果可以 ping 通。

```
C:\>ping www.google.com

Pinging www.google.com [172.217.194.99] with 32 bytes of data:

Reply from 172.217.194.99: bytes=32 time=30ms TTL=50
Reply from 172.217.194.99: bytes=32 time=30ms TTL=50
Reply from 172.217.194.99: bytes=32 time=30ms TTL=50
Reply from 172.217.194.99: bytes=32 time=30ms TTL=50

Ping statistics for 172.217.194.99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 30ms, Maximum = 30ms, Average = 30ms
C:\>
```

1.5 配置文件

```
#
interface Ten-GigabitEthernet1/0/3
 port link-mode bridge
 packet-filter 3001 inbound
#
interface Ten-GigabitEthernet1/0/4
 port link-mode bridge
 packet-filter 3000 inbound
#
acl advanced 3000
 rule 0 deny ip destination 10.1.2.0 0.0.0.255
#
acl advanced 3001
 rule 0 permit ip destination 10.2.1.0 0.0.0.255
 rule 5 deny ip
#
```

1.6 相关资料

- 产品配套“ACL 和 QoS 配置指导”中的“ACL”。
- 产品配套“ACL 和 QoS 命令参考”中的“ACL”。

QoS 快速配置指南

目 录

1 配置 IP 限速

1.1 简介

本案例介绍 IP 限速配置方法。

1.2 组网需求

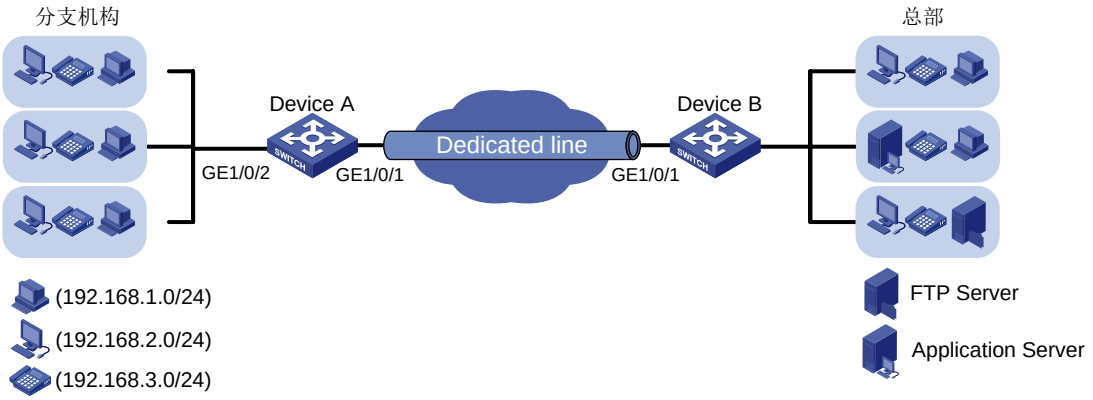
如图 1 所示，某公司通过专线连接分支机构与总部，专线中传输的流量主要有三类：FTP 流量、业务应用流量、IP 语音流量。整个专线的速率为 15Mbps，在总部的边缘设备 DeviceB 上已经配置了相应的流量监管功能：

- IP 语音流量的承诺速率为 10Mbps
- 业务应用流量的承诺速率为 3Mbps
- FTP 流量的承诺速率为 7Mbps

为配合总部的流量监管，要求在分支机构的边缘设备 DeviceA 上配置流量整形功能，对各类流量中突发的超出部分进行缓存，避免数据丢失。

由于整个专线的速率为 15Mbps，因此要求在 DeviceA 上配置接口限速功能，保证发往专线的所有数据总速率不得超过 15Mbps。

图1 流量整形与接口限速组网示意图



1.3 配置思路

- 要实现流量整形功能，首先要确认各类报文在发送时所在的队列编号。本例中没有给出各类报文的优先级，因此需要使用重标记功能将不同类型的报文手工调度到不同的队列中。
- 手工调度报文队列可以通过重标记报文的 DSCP/802.1p 优先级或者重标记本地优先级来实现，为保持原始报文内容不变，使用重标记本地优先级进行配置。

1.4 配置步骤

说明

在进行流量整形和接口限速配置前，应确保 1.2 图 1 中网络的连通性。关于在 DeviceA 和 DeviceB 上为提供网络连通性而进行的配置（如创建 VLAN 接口及为其配置 IP 地址等），此处不进行介绍。

1. 重标记功能的配置

(1) 在 Device A 上创建三个流分类，分别匹配三类报文的源 IP 网段。

创建基本 IPv4 ACL2000，匹配 IP 电话发送的流量（源地址为 192.168.3.0/24 网段）。

```
<DeviceA> system-view
[DeviceA] acl basic 2000
[DeviceA-acl-ipv4-basic-2000] rule permit source 192.168.3.0 0.0.0.255
[DeviceA-acl-ipv4-basic-2000] quit
```

创建流分类 voice，匹配规则为 IPv4 ACL 2000。

```
[DeviceA] traffic classifier voice
[DeviceA-classifier-voice] if-match acl 2000
[DeviceA-classifier-voice] quit
```

创建基本 IPv4 ACL2001，匹配业务软件终端发送的流量(源地址为 192.168.2.0/24 网段)。

```
[DeviceA] acl basic 2001
[DeviceA-acl-ipv4-basic-2001] rule permit source 192.168.2.0 0.0.0.255
[DeviceA-acl-ipv4-basic-2001] quit
```

创建流分类 service，匹配规则为 IPv4 ACL 2001。

```
[DeviceA] traffic classifier service
[DeviceA-classifier-service] if-match acl 2001
[DeviceA-classifier-service] quit
```

创建高级 IPv4 ACL 3000，匹配普通 PC 发送的 FTP 流量(源地址为 192.168.1.0/24 网段，目的端口为 20）。

```
[DeviceA] acl advanced 3000
[DeviceA-acl-ipv4-adv-3000] rule permit tcp destination-port eq 20 source 192.168.1.0
0.0.0.255
[DeviceA-acl-ipv4-adv-3000] quit
```

创建流分类 ftp，匹配规则为 IPv4 ACL 3000。

```
[DeviceA] traffic classifier ftp
[DeviceA-classifier-ftp] if-match acl 3000
[DeviceA-classifier-ftp] quit
```

(2) 创建三个流行为，动作分别为重标记本地优先级为 6、4、2。

创建流行为 voice，动作为重标记本地优先级为 6。

```
[DeviceA] traffic behavior voice
[DeviceA-behavior-voice] remark local-precedence 6
[DeviceA-behavior-voice] quit
```

创建流行为 service，动作为重标记本地优先级为 4。

```
[DeviceA] traffic behavior service
[DeviceA-behavior-service] remark local-precedence 4
```

```
[DeviceA-behavior-service] quit
```

创建流行为 ftp，动作为重标记本地优先级为 2。

```
[DeviceA] traffic behavior ftp
[DeviceA-behavior-ftp] remark local-precedence 2
[DeviceA-behavior-ftp] quit
```

(3) 创建 QoS 策略并应用

创建 QoS 策略 shaping，将上面三组流分类和流行为进行关联。

```
[DeviceA] qos policy shaping
[DeviceA-qospolicy-shaping] classifier voice behavior voice
[DeviceA-qospolicy-shaping] classifier service behavior service
[DeviceA-qospolicy-shaping] classifier ftp behavior ftp
[DeviceA-qospolicy-shaping] quit
```

将 QoS 策略应用到 GigabitEthernet1/0/2 端口的入方向。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] qos apply policy shaping inbound
[DeviceA-GigabitEthernet1/0/2] quit
```

经过上述配置，三类报文在 DeviceA 中的本地优先级已经被修改，即可以确定三类报文的输出队列分别为 6、4、2。

2. 流量整形配置

在 GigabitEthernet1/0/1 端口上配置流量整形，为语音报文（队列 6）配置承诺速率为 10Mbps。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] qos gts queue 6 cir 10240
```

在 GigabitEthernet1/0/1 端口上配置流量整形，为业务应用报文（队列 4）配置承诺速率为 3Mbps。

```
[DeviceA-GigabitEthernet1/0/1] qos gts queue 4 cir 3072
```

在 GigabitEthernet1/0/1 端口上配置流量整形，为 FTP 报文（队列 2）配置承诺速率为 7Mbps。

```
[DeviceA-GigabitEthernet1/0/1] qos gts queue 2 cir 7168
```

3. 接口限速配置

在 GigabitEthernet1/0/1 端口上配置接口限速，对出端口方向的流量配置承诺速率为 15Mbps。

```
[DeviceA-GigabitEthernet1/0/1] qos lr outbound cir 15360
```

1.5 验证配置

使用 **display qos policy interface** 命令查看重标记功能的配置。

```
<Device> display qos policy interface inbound
Interface: GigabitEthernet1/0/2
  Direction: Inbound
  Policy: shaping
   Classifier: voice
     Operator: AND
     Rule(s) :
      If-match acl 2000
     Behavior: voice
      Marking:
        Remark local-precedence 6
```

```
  Classifier: service
    Operator: AND
    Rule(s) :
     If-match acl 2001
    Behavior: service
     Marking:
       Remark local-precedence 4
  Classifier: ftp
    Operator: AND
    Rule(s) :
     If-match acl 3000
    Behavior: ftp
     Marking:
       Remark local-precedence 2
```

使用 **display qos gts interface** 命令查看流量整形的配置。

```
<Device> display qos gts interface
Interface: GigabitEthernet1/0/1
 Rule: If-match queue 6
  CIR 10240 (kbps), CBS 640000 (Bytes)
 Rule: If-match queue 4
  CIR 3072 (kbps), CBS 192000 (Bytes)
 Rule: If-match queue 2
  CIR 7168 (kbps), CBS 448000 (Bytes)
```

使用 **display qos lr interface** 命令查看接口限速的配置。

```
<Device> display qos lr interface
Interface: GigabitEthernet1/0/1
Direction: Outbound
 CIR 15360 (kbps), CBS 960000 (Bytes)
```

1.6 配置文件

```
#
acl basic 2000
 rule 0 permit source 192.168.3.0 0.0.0.255
#
acl basic 2001
 rule 0 permit source 192.168.2.0 0.0.0.255
#
acl advanced 3000
 rule 0 permit tcp source 192.168.1.0 0.0.0.255 destination-port eq ftp-data
#
traffic classifier ftp operator and
 if-match acl 3000
#
traffic classifier service operator and
 if-match acl 2001
#
traffic classifier voice operator and
```

```
 if-match acl 2000
#
traffic behavior ftp
 remark local-precedence 2
#
traffic behavior service
 remark local-precedence 4
#
traffic behavior voice
 remark local-precedence 6
#
qos policy shaping
 classifier voice behavior voice
 classifier service behavior service
 classifier ftp behavior ftp
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 qos lr outbound cir 15360 cbs 960000
 qos gts queue 6 cir 10240 cbs 640000
 qos gts queue 4 cir 3072 cbs 192000
 qos gts queue 2 cir 7168 cbs 448000
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 qos apply policy shaping inbound
#
return
```

1.7 相关资料

- 产品配套“ACL 和 QoS 配置指导”中的“ACL”。
- 产品配套“ACL 和 QoS 命令参考”中的“ACL”。

2 配置流量统计

2.1 简介

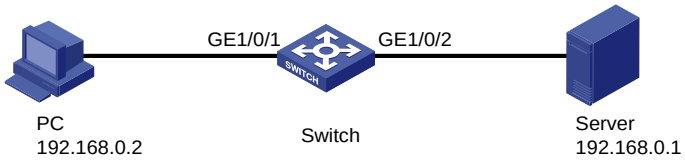
本案例介绍流量统计配置方法。

2.2 组网需求

如 2.2 图 2 所示，PC 访问服务器出现丢包现象，可以通过配置 QoS 策略做流量统计来排查报文是否丢弃在交换机上。

在交换机 GE1/0/1 和 GE1/0/2 接口配置流量统计，查看接口下的报文统计信息。

图2 流量统计配置组网图



2.3 配置步骤

创建高级规则 IPv4 ACL3001，配置 2 条规则，用于分别匹配源 IP 地址为 192.168.0.2，目的地址为 192.168.0.1 的流量和源 IP 地址为 192.168.0.1，目的地址为 192.168.0.2 流量。

```
<Sysname> system-view
[Sysname] acl advanced 3001
[Sysname-acl-ipv4-adv-3001] rule 0 permit ip source 192.168.0.2 0 destination 192.168.0.241
0
[Sysname-acl-ipv4-adv-3001] rule 5 permit ip source 192.168.0.241 0 destination 192.168.0.2
0
[Sysname-acl-ipv4-adv-3001] quit
```

创建流分类 aa，匹配规则为 IPv4 ACL 3001。

```
[Sysname] traffic classifier aa
[Sysname-classifier-1] if-match acl 3001
[Sysname-classifier-1] quit
```

创建流行为 aa，动作为记录报文。

```
[Sysname] traffic behavior aa
[Sysname-behavior-1] accounting packet
[Sysname-behavior-1] quit
```

创建 QoS 策略 aa，将上面已创建的流分类和流行为进行关联。

```
[Sysname] qos policy aa
[Sysname-qospolicy-aa] classifier aa behavior aa
[Sysname-qospolicy-aa] quit
```

将 QoS 策略应用到 GigabitEthernet1/0/1 端口和 GigabitEthernet1/0/2 的入方向和出方向。（此处可以根据现场业务情况，调用在终端访问的接口的入方向和服务器连接接口的出方向）。

```
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] qos apply policy 1 inbound
[Sysname-GigabitEthernet1/0/1] qos apply policy 1 outbound
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] qos apply policy 1 inbound
[Sysname-GigabitEthernet1/0/2] qos apply policy 1 outbound
[Sysname-GigabitEthernet1/0/2] quit
```

2.4 验证配置

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 192.168.0.1

正在 Ping 192.168.0.1 具有 32 字节的数据:
来自 192.168.0.1 的回复: 字节=32 时间=3ms TTL=255
来自 192.168.0.1 的回复: 字节=32 时间=1ms TTL=255
来自 192.168.0.1 的回复: 字节=32 时间=1ms TTL=255
来自 192.168.0.1 的回复: 字节=32 时间=1ms TTL=255

192.168.0.1 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
```

在交换机上查看接口 GE1/0/1 和 GE1/0/2 的报文统计信息，GE1/0/1 口连接 PC，入方向报文为 4 个，GE1/0/2 口连接服务器，出方向报文为 4 个，报文数相同，说明交换机将报文全部转发。

```
[Sysname] display qos policy interface
Interface: GigabitEthernet1/0/1
  Direction: Inbound
  Policy: aa
   Classifier: aa
     Operator: AND
     Rule(s) :
      If-match acl 3001
   Behavior: aa
      Accounting enable:
        4 (Packets)

Interface: GigabitEthernet1/0/1
  Direction: Outbound
  Policy: aa
   Classifier: aa
     Operator: AND
     Rule(s) :
      If-match acl 3001
     Behavior: aa
      Accounting enable:
        7 (Packets)
```

```
Interface: GigabitEthernet1/0/2
  Direction: Inbound
  Policy: aa
   Classifier: aa
     Operator: AND
     Rule(s) :
      If-match acl 3001
   Behavior: aa
      Accounting enable:
        7 (Packets)

Interface: GigabitEthernet1/0/2
  Direction: Outbound
  Policy: aa
   Classifier: aa
     Operator: AND
     Rule(s) :
      If-match acl 3001
     Behavior: aa
      Accounting enable:
        4 (Packets)
```

2.5 配置文件

```
#
traffic classifier aa operator and
 if-match acl 3001
#
traffic behavior aa
 accounting packet
#
qos policy aa
 classifier aa behavior aa
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 qos apply policy aa inbound
 qos apply policy aa outbound
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 qos apply policy aa inbound
 qos apply policy aa outbound
#
acl number 3001
rule 0 permit ip source 192.168.0.2 0 destination 192.168.0.1 0
rule 5 permit ip source 192.168.0.1 0 destination 192.168.0.2 0
#
```

2.6 相关资料

- 产品配套“ACL 和 QoS 配置指导”中的“ACL”。
- 产品配套“ACL 和 QoS 命令参考”中的“ACL”。

3 配置 QoS 策略禁止 VLAN 间设备互访

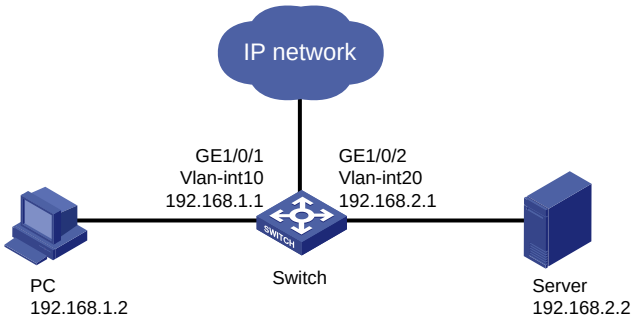
3.1 简介

本案例介绍禁止不同 VLAN 之间的流量互访的配置方法。

3.2 组网需求

如 3.2 图 3 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，同时不影响其他的流量的转发。

图3 配置 QoS 策略禁止 VLAN 间设备互访组网图



3.3 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。

3.4 配置步骤

配置 VLAN 接口和 IP 地址。

```
<Sysname> system-view
[Sysname] vlan 10
[Sysname-vlan10] port gigabitethernet 1/0/1
[Sysname-vlan10] quit
[Sysname] vlan 20
[Sysname-vlan20] port gigabitethernet 1/0/2
[Sysname-vlan20] quit
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ip address 192.168.1.1 24
[Sysname-Vlan-interface10] quit
[Sysname] interface vlan-interface 20
```

```
[Sysname-Vlan-interface20] ip address 192.168.2.1 24
[Sysname-Vlan-interface20] quit
```
创建高级规则 IPv4 ACL 3000，配置 1 条规则，匹配源 IP 地址为 192.168.1.0/24，目的地址为 192.168.2.0/24 的流量。
```
<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000] rule 0 permit ip source 192.168.1.0 0.0.0.255 destination
192.168.2.0 0.0.0.255
[Sysname-acl-ipv4-adv-3000] quit
```
创建流分类 a1，匹配规则为 IPv4 ACL 3000。
```
[Sysname] traffic classifier a1
[Sysname-classifier-a1] if-match acl 3000
[Sysname-classifier-a1] quit
```
创建流行为 a2，动作为丢弃命中规则的数据包。
```
[Sysname] traffic behavior a2
[Sysname-behavior-a2] filter deny
[Sysname-behavior-a2] quit
```
创建 QoS 策略 a3，将上面已创建的流分类和流行为进行关联。
```
[Sysname] qos policy a3
[Sysname-qospolicy-a3] classifier a1 behavior a2
[Sysname-qospolicy-a3] quit
```
将 QoS 策略 a3 应用到 GigabitEthernet1/0/1 接口的入方向。
```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos apply policy a3 inbound
[Sysname-GigabitEthernet1/0/1] quit
```
创建高级规则 IPv4 ACL 3001，配置 1 条规则，匹配源 IP 地址为 192.168.2.0/24，目的地址为 192.168.1.0/24 的流量。
```
[Sysname] acl advanced 3001
[Sysname-acl-ipv4-adv-3001] rule 0 permit ip source 192.168.2.0 0.0.0.255 destination
192.168.1.0 0.0.0.255
[Sysname-acl-ipv4-adv-3001] quit
```
创建流分类 b1，匹配规则为 IPv4 ACL 3001。
```
[Sysname] traffic classifier b1
[Sysname-classifier-b1] if-match acl 3001
[Sysname-classifier-b1] quit
```
创建流行为 b2，动作为丢弃命中规则的数据包。
```
[Sysname] traffic behavior b2
[Sysname-behavior-b2] filter deny
[Sysname-behavior-b2] quit
```
创建 QoS 策略 b3，将上面已创建的流分类和流行为进行关联。
```
[Sysname] qos policy b3
[Sysname-qospolicy-b3] classifier b1 behavior b2
[Sysname-qospolicy-b3] quit
```
将 QoS 策略 b3 应用到 GigabitEthernet1/0/2 接口的入方向。
```
[Sysname] interface gigabitethernet 1/0/2
[Sysname-GigabitEthernet1/0/2] qos apply policy b3 inbound
```

```
[Sysname-GigabitEthernet1/0/2] quit
```

3.5 验证配置

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)，
```

在交换机上查看接口的 QoS 策略应用信息：

```
[Sysname] display qos policy interface
Interface: GigabitEthernet1/0/1
  Direction: Inbound
  Policy: a3
  Classifier: a1
    Operator: AND
    Rule(s) :
     If-match acl 3000
    Behavior: a2
     Filter enable: Deny
Interface: GigabitEthernet1/0/2
  Direction: Inbound
  Policy: b3
  Classifier: b1
    Operator: AND
    Rule(s) :
     If-match acl 3001
```

```
    Behavior: b2
     Filter enable: Deny
```

3.6 配置文件

```
#
vlan 10
#
vlan 20
#
interface Vlan-interface10
 ip address 192.168.1.1 255.255.255.0
#
interface Vlan-interface20
 ip address 192.168.2.1 255.255.255.0
#
traffic classifier a1 operator and
 if-match acl 3000
#
traffic classifier b1 operator and
 if-match acl 3001
#
traffic behavior a2
 filter deny
#
traffic behavior b2
 filter deny
#
qos policy a3
 classifier a1 behavior a2
#
qos policy b3
 classifier b1 behavior b2
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 10
 qos apply policy a3 inbound
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 20
 qos apply policy b3 inbound
#
acl number 3000
rule 0 permit ip source 192.168.1.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
#
#
```

```
acl number 3001
rule 0 permit ip source 192.168.2.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
#
```

3.7 相关资料

- 产品配套“ACL 和 QoS 配置指导”中的“ACL”。
- 产品配套“ACL 和 QoS 命令参考”中的“ACL”。
- 产品配套“ACL 和 QoS 配置指导”中的“QoS”。
- 产品配套“ACL 和 QoS 命令参考”中的“QoS”。

IP Source Guard 快速配置指南

目 录

1 IP Source Guard 静态绑定快速配置指南

1.1 简介

本案例介绍静态配置绑定表项方式的 IP Source Guard 的配置方法。

1.2 使用限制

加入聚合组或加入业务环回组的端口上不能配置 IP Source Guard 功能。

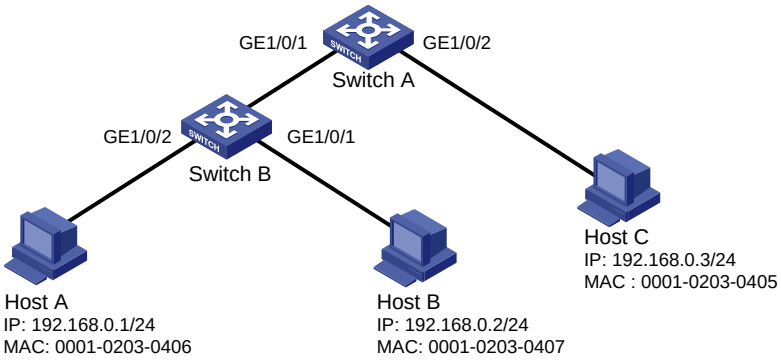
1.3 组网需求

如图所示，Host A 与 Host B 分别与 Switch B 的端口 GigabitEthernet1/0/2、GigabitEthernet1/0/1 相连；Host C 与 Switch A 的端口 GigabitEthernet1/0/2 相连。Switch B 接到 Switch A 的端口 GigabitEthernet1/0/1 上。各主机均使用静态配置的 IP 地址。

通过在 Switch A 和 Switch B 上配置 IPv4 静态绑定表项，满足以下各项应用需求：

- 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 上只允许使用 IP 地址 192.168.0.2/24 的主机发送的 IP 报文通过，即允许 Host B 更换网卡后仍然可以使用该 IP 地址与 Host A 互通。

图1 配置 IP Source Guard 静态绑定组网图



1.4 配置步骤

1. Switch A 的配置

在端口 GigabitEthernet1/0/2 上配置 IPv4 动态绑定功能，绑定源 IP 地址和 MAC 地址。

```
<SwitchA> system-view
[SwitchA] interface gigabitethernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] ip verify source ip-address mac-address
```

配置 IPv4 静态绑定表项，只允许 MAC 地址为 0001-0203-0405、IP 地址为 192.168.0.3 的 Host C 发送的 IP 报文通过端口 GigabitEthernet1/0/2。

```
[SwitchA-GigabitEthernet1/0/2] ip source binding ip-address 192.168.0.3 mac-address 0001-0203-0405
[SwitchA-GigabitEthernet1/0/2] quit
```

在端口 GigabitEthernet1/0/1 上配置 IPv4 端口绑定功能，绑定源 IP 地址和 MAC 地址。

```
[SwitchA] interface gigabitethernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] ip verify source ip-address mac-address
```

配置 IPv4 静态绑定表项，只允许 MAC 地址为 0001-0203-0406、IP 地址为 192.168.0.1 的 Host A 发送的 IP 报文通过端口 GigabitEthernet1/0/1。

```
[SwitchA-GigabitEthernet1/0/1] ip source binding ip-address 192.168.0.1 mac-address 0001-0203-0406
[SwitchA-GigabitEthernet1/0/1] quit
```

保存配置

```
[SwitchA] save
```

2. 配置 Switch B 的配置

在端口 GigabitEthernet1/0/2 上配置 IPv4 动态绑定功能，绑定源 IP 地址和 MAC 地址。

```
<SwitchB> system-view
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] ip verify source ip-address mac-address
```

配置 IPv4 静态绑定表项，只允许 MAC 地址为 0001-0203-0406、IP 地址为 192.168.0.1 的 Host A 发送的 IP 报文通过端口 GigabitEthernet1/0/2。

```
[SwitchB-GigabitEthernet1/0/2] ip source binding ip-address 192.168.0.1 mac-address 0001-0203-0406
[SwitchB-GigabitEthernet1/0/2] quit
```

在端口 GigabitEthernet1/0/1 上配置 IPv4 端口绑定功能，绑定源 IP 地址。

```
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] ip verify source ip-address
```

配置 IPv4 静态绑定表项，只允许 IP 地址为 192.168.0.2 的主机发送的 IP 报文通过端口 GigabitEthernet1/0/1。

```
[SwitchB-GigabitEthernet1/0/1] ip source binding ip-address 192.168.0.2
[SwitchB-GigabitEthernet1/0/1] quit
```

保存配置

```
[SwitchB] save
```

1.5 验证配置

在 Switch A 上显示 IPv4 静态绑定表项配置成功。

```
[SwitchA] display ip source binding static
Total entries found: 2
IP Address      MAC Address    Interface              VLAN Type
192.168.0.1     0001-0203-0406 GE1/0/1                N/A  Static
192.168.0.3     0001-0203-0405 GE1/0/2                N/A  Static
```

在 Switch B 上显示 IPv4 静态绑定表项配置成功。

```
[SwitchB] display ip source binding static
Total entries found: 2
IP Address      MAC Address    Interface               VLAN Type
192.168.0.1     0001-0203-0406 GE1/0/2                 N/A  Static
192.168.0.2     N/A            GE1/0/1                 N/A  Static
```

1.6 配置文件

- SwitchA

```
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 ip verify source ip-address mac-address
 ip source binding ip-address 192.168.0.1 mac-address 0001-0203-0406
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 ip verify source ip-address mac-address
 ip source binding ip-address 192.168.0.3 mac-address 0001-0203-0405
#
```

- SwitchB

```
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 ip verify source ip-address
 ip source binding ip-address 192.168.0.2
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 ip verify source ip-address mac-address
 ip source binding ip-address 192.168.0.1 mac-address 0001-0203-0406
#
```

1.7 相关资料

- 产品配套“安全配置指导”中的“IP Source Guard”。
- 产品配套“安全命令参考”中的“IP Source Guard”。

SSH 快速配置指南

目 录

1 配置设备作为 SSH 服务器

1.1 简介

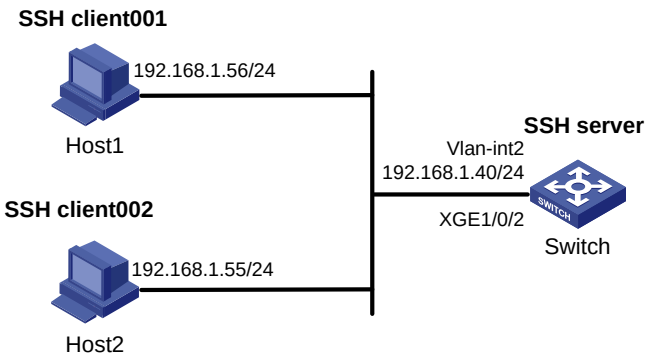
本案例介绍配置设备作为 SSH 服务器的方法。

1.2 组网需求

如图 1 所示，Switch 作为 SSH 服务器，与客户端 Host1 和 Host2 之间路由可达。Host1 和 Host2 需要通过 SSH 登录到 Switch 上对其进行相关配置。并要求：

- Switch 通过 SSH 的 password 认证方式和 publickey 认证方式分别对 Host1 和 Host2 进行认证，认证过程在 Switch 本地完成；
- Host1 的登录用户名为 client001，密码为 hello12345，登录设备后可以使用所有命令。
- Host2 的登录用户名为 client002，使用的公钥算法为 RSA，登录设备后可以使用所有命令。

图1 设备作为 SSH 服务器组网图



1.3 配置步骤

1. 配置 SSH 客户端 Host2

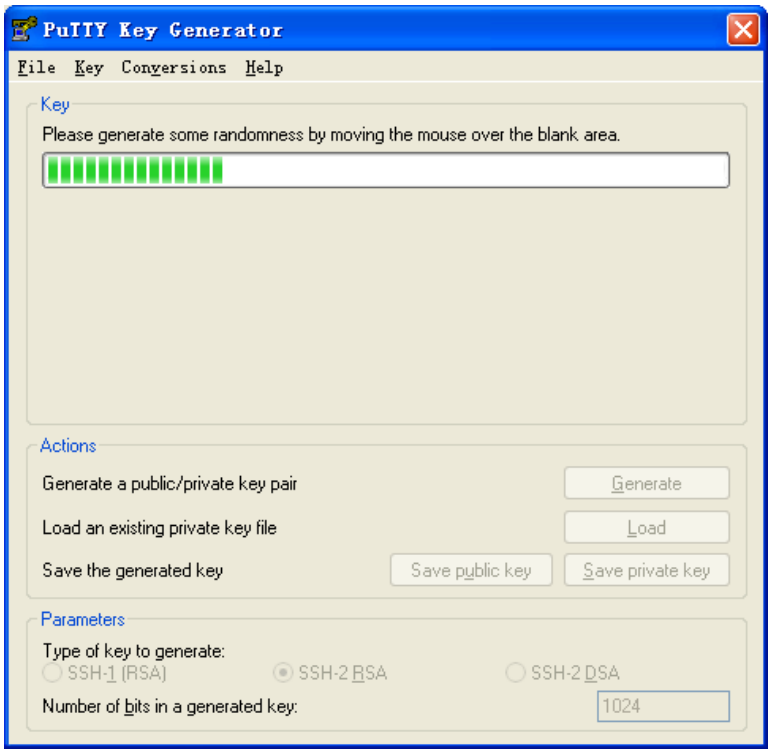
生成 RSA 密钥对。

在客户端运行 PuTTYGen.exe，在参数栏中选择“SSH-2 RSA”，点击<Generate>，产生客户端密钥对。

图2 生成客户端密钥（步骤 1）

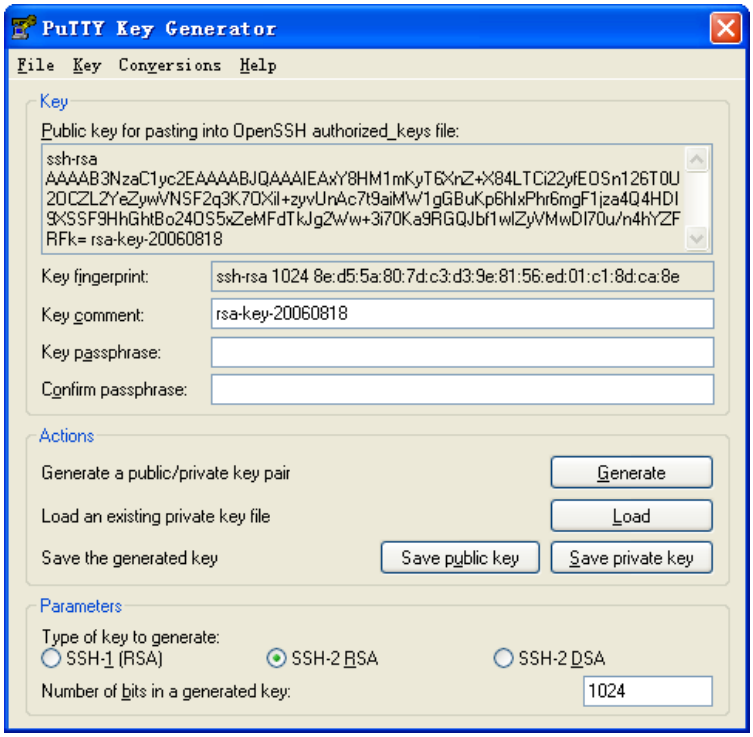
在产生密钥对的过程中需不停地移动鼠标，鼠标移动仅限于下图蓝色框中除绿色标记进程条外的地方，否则进程条的显示会不动，密钥对将停止产生，见图 3。

图3 生成客户端密钥（步骤 2）



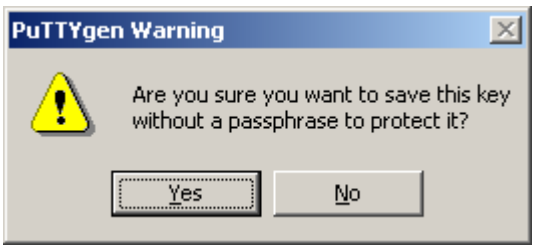
密钥对产生后，点击<Save public key>，输入存储公钥的文件名 key.pub，点击<保存>按钮。

图4 生成客户端密钥（步骤 3）



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

图5 生成客户端密钥（步骤 4）



客户端生成密钥对后，需要将保存的公钥文件 key.pub 通过 FTP/TFTP 方式上传到服务器，具体过程略。

2. 配置 SSH 服务器

配置设备生成 RSA 密钥对。

```
<Switch> system-view
[Switch] public-key local create rsa
The range of public key modulus is (512 ~ 4096).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
```

```
Generating Keys...
..
Create the key pair successfully.
```
配置设备生成 DSA 密钥对。
```
[Switch] public-key local create dsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
......
Create the key pair successfully.
```
配置设备生成 ECDSA 密钥对。
```
[Switch] public-key local create ecdsa secp256r1
Generating Keys...
.
Create the key pair successfully.
```
开启 SSH 服务器功能。
```
[Switch] ssh server enable
```
创建 VLAN 2，并将 Ten-GigabitEthernet1/0/2 加入 VLAN 2。
```
[Switch] vlan 2
[Switch-vlan2] port ten-gigabitethernet 1/0/2
[Switch-vlan2] quit
```
配置 VLAN 接口 2 的 IP 地址，客户端将通过该地址连接 SSH 服务器。
```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.1.40 255.255.255.0
[Switch-Vlan-interface2] quit
```
配置 VTY 用户线的认证方式为 scheme，SSH 客户端使用 VTY 用户线登录设备。
```
[Switch] line vty 0 63
[Switch-line-vty0-63] authentication-mode scheme
[Switch-line-vty0-63] quit
```
创建本地用户 client001，并设置用户密码为 hello12345、服务类型为 SSH、用户角色为 network-admin。
```
[Switch] local-user client001 class manage
New local user added.
[Switch-luser-manage-client001] password simple hello12345
[Switch-luser-manage-client001] service-type ssh
[Switch-luser-manage-client001] authorization-attribute user-role network-admin
[Switch-luser-manage-client001] quit
```
从文件 key.pub 中导入远端的公钥，并命名为 switchkey。
```
[Switch] public-key peer switchkey import sshkey key.pub
```
设置 SSH 用户 client002 的认证方式为 publickey，并指定公钥为 switchkey。
```
[Switch] ssh user client002 service-type stelnet authentication-type publickey assign publickey switchkey
```
创建设备管理类本地用户 client002，并设置服务类型为 SSH，用户角色为 network-admin。

```
[Switch] local-user client002 class manage
New local user added.
[Switch-luser-manage-client002] service-type ssh
[Switch-luser-manage-client002] authorization-attribute user-role network-admin
[Switch-luser-manage-client002] quit
```

1.4 验证配置

说明

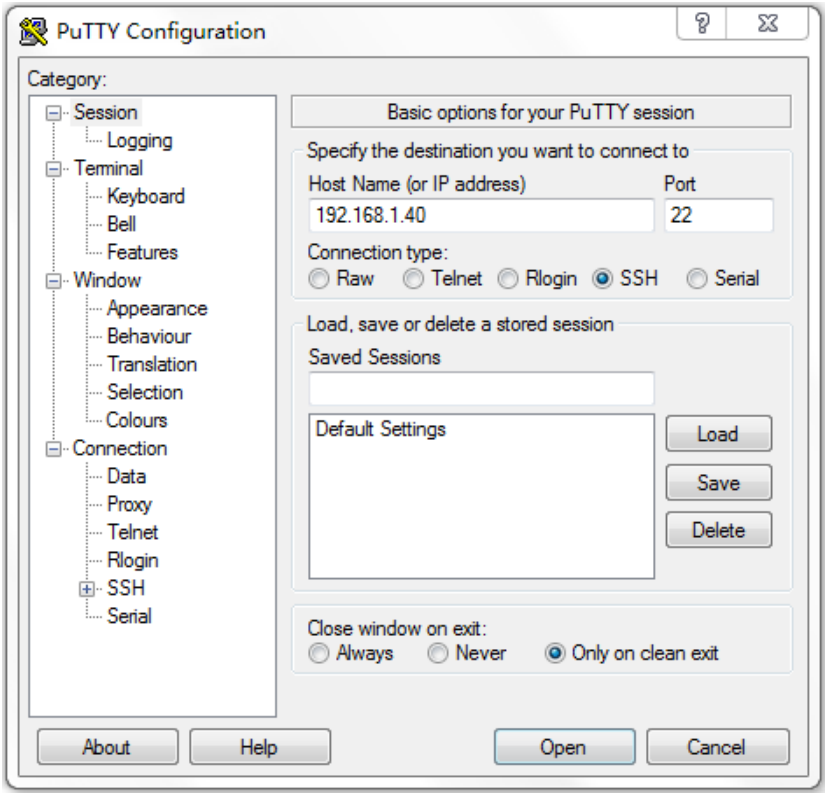
SSH 客户端软件很多，本文中以客户端软件 PuTTY0.60 为例说明 SSH 客户端的配置方法。

安装 PuTTY0.60 软件。

打开 PuTTY.exe 程序，点击“Session”功能区，出现如图 6 所示的客户端配置界面。

- 在“Host Name（or IP address）”文本框中输入 SSH 服务器的 IP 地址为 192.168.1.40。
- 在“Port”文本框中输入 SSH 协议端口号 22。
- 在“Connection type”区域选择 SSH 协议。

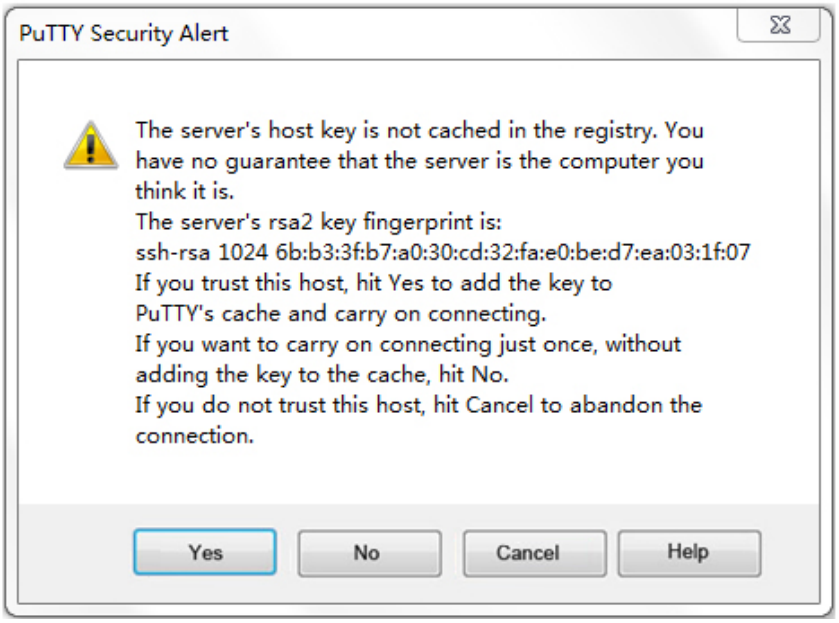
图6 SSH 客户端配置界面



1. Host1 端 client001 用 password 认证方式连接 SSH 服务器。

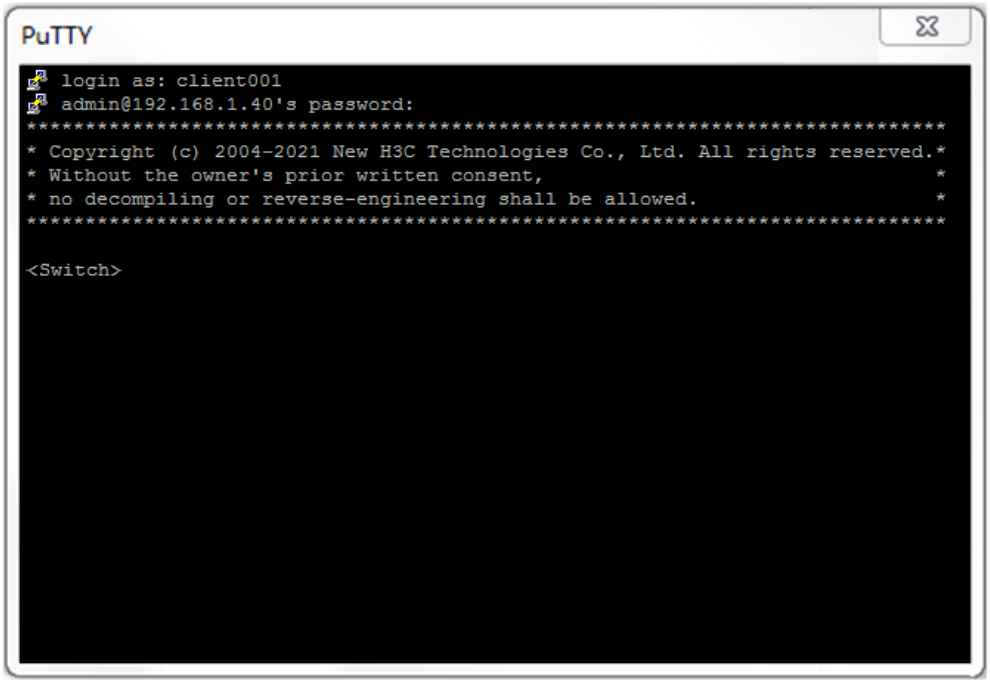
在图 6 界面中，单击<Open>按钮。弹出“PuTTY Security Alert”对话框。

图7 SSH 客户端登录界面（一）



单击“Yes”按钮，并输入用户名“client001”和密码“hello12345”（输入密码的不会显示），即可成功登录设备并使用所有命令。

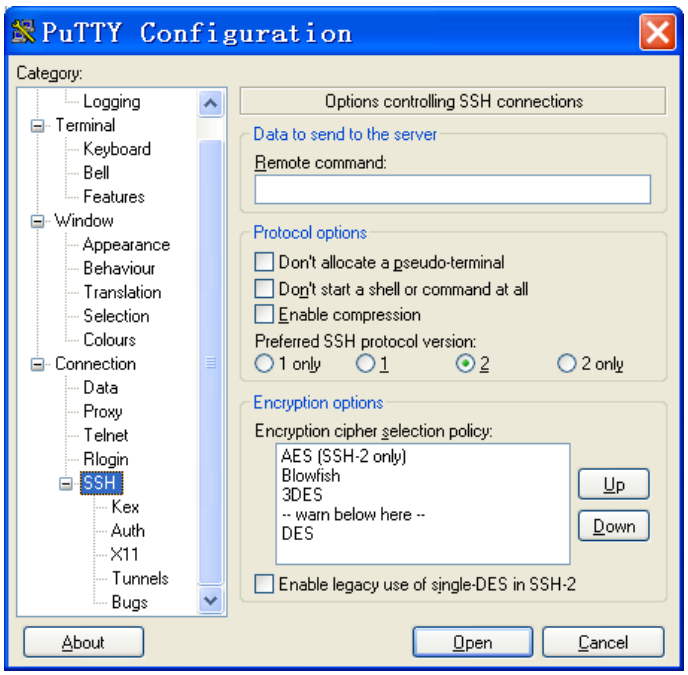
图8 SSH 客户端登录界面（二）



2. Host2 端 client002 用 RSA 认证方式连接 SSH 服务器。

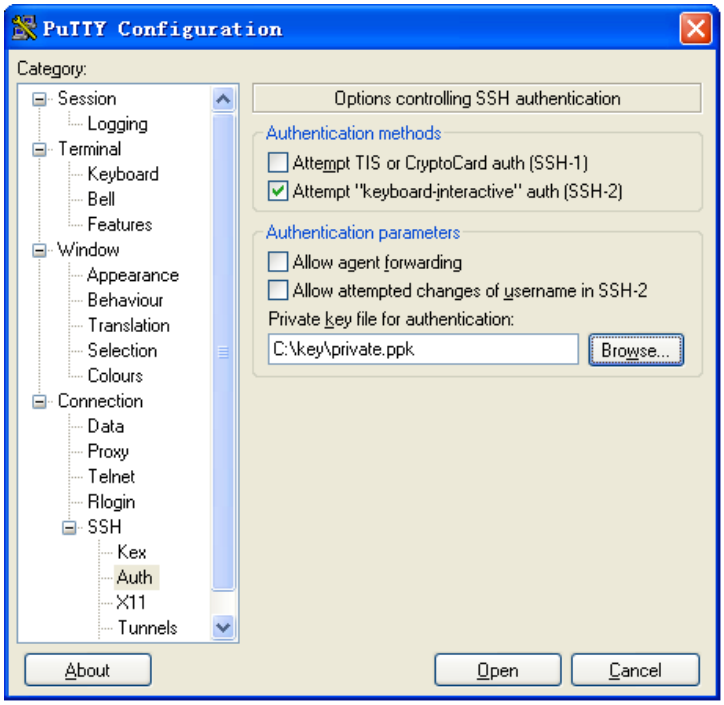
单击左侧导航栏“Connection->SSH”，出现如图 9 的界面。选择“Preferred SSH protocol version”为“2”。

图9 Stelnet 客户端配置界面



单击左侧导航栏“Connection->SSH”下面的“Auth”（认证），出现如图 10 的界面。单击<Browse…>按钮，弹出文件选择窗口。选择与配置到服务器端的公钥对应的私钥文件 private.ppk。

图10 Stelnet 客户端配置界面



单击<Open>按钮。按提示输入用户名 client002，即可进入 Switch 的配置界面。

1.5 配置文件

```
#
vlan 2
#
interface Vlan-interface2
 ip address 192.168.1.40 255.255.255.0
#
interface Ten-GigabitEthernet1/0/2
 port access vlan 2
#
line vty 0 63
 authentication-mode scheme
#
ssh server enable
#
local-user client001 class manage
 password hash $h$6$CqMnWdX6LIW/hz2Z$4+0Pumk+A98VlGVgqN3n/mEi7hJka9fEZpRZIpSNi9b
cBEXhpvIqaYTvIVBf7ZUNGnovFsqW7nYxjoToRDvYBg==
 service-type ssh
 authorization-attribute user-role network-admin
 authorization-attribute user-role network-operator
#
public-key peer clientkey import sshkey key.pub
ssh user client002 service-type stelnet authentication-type publickey assign publickey ackey
#
local-user client002 class manage
 service-type ssh
 authorization-attribute user-role network-admin
#
```

1.6 相关资料

- 产品配套“安全配置指导”中的“SSH”。
- 产品配套“安全命令参考”中的“SSH”。

2 配置设备作为 SSH 客户端

2.1 简介

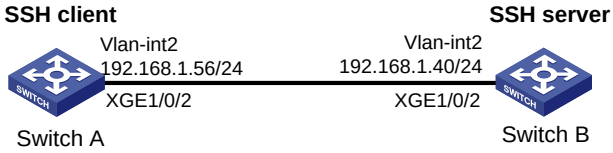
本案例介绍配置设备作为 SSH 客户端的方法。

2.2 组网需求

如图 11 所示，Switch A 作为 SSH 客户端，Switch B 作为 SSH 服务器，Switch A 采用 SSH 协议远程登录到 Switch B 上。并要求：

- Switch B 采用本地认证的方式认证用户，认证方式为 password 认证。
- 登录用户名为 client001，密码为 hello12345，登录设备后可以使用所有命令。

图11 设备作为 SSH 客户端配置组网图



2.3 配置步骤

1. 配置 Switch A

创建 VLAN 2，并将 Ten-GigabitEthernet1/0/2 加入 VLAN 2。

```
<SwitchA> system-view
[SwitchA] vlan 2
[SwitchA-vlan2] port ten-gigabitethernet 1/0/2
[SwitchA-vlan2] quit
```

配置 VLAN 接口 2 的 IP 地址。

```
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 192.168.1.56 255.255.255.0
[SwitchA-Vlan-interface2] quit
```

2. 配置 Switch B

请参见 1 配置设备作为 SSH 服务器配置 Switch B 作为 SSH 服务器。

2.4 验证配置

Switch A 建立到服务器 192.168.1.40 的 SSH 连接。输入正确的用户名后根据提示输入 Y 确认，然后输入 N 不保存公钥，最后输入密码，即可成功登录到 Switch B 上，用户角色为 network-admin。

说明

若输入 Y 保存公钥，当 Switch B 公钥变化时，需要在 Switch A 系统视图下执行 delete ssh client server-public-key 命令删除已保存的公钥才能再次建立连接。

```
<SwitchA> ssh2 192.168.1.40
Username: client001
Press CTRL+C to abort.
Connecting to 192.168.1.40 port 22.
The server is not authenticated. Continue? [Y/N]:Y
Do you want to save the server public key? [Y/N]:N
Enter password:

**************************************************************************
* Copyright (c) 2004-2021 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                             *
* no decompiling or reverse-engineering shall be allowed.                *
**************************************************************************


<SwitchB>
```

2.5 配置文件

- Switch A

```
#
vlan 2
#
interface Vlan-interface2
ip address 192.168.1.56 255.255.255.0
#
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
```

- Switch B

请参见 1.5 配置文件查看 Switch B 的配置文件。

2.6 相关资料

- 产品配套“安全配置指导”中的“SSH”。
- 产品配套“安全命令参考”中的“SSH”。

3 配置 SSH 用户的 RADIUS 认证和授权

3.1 简介

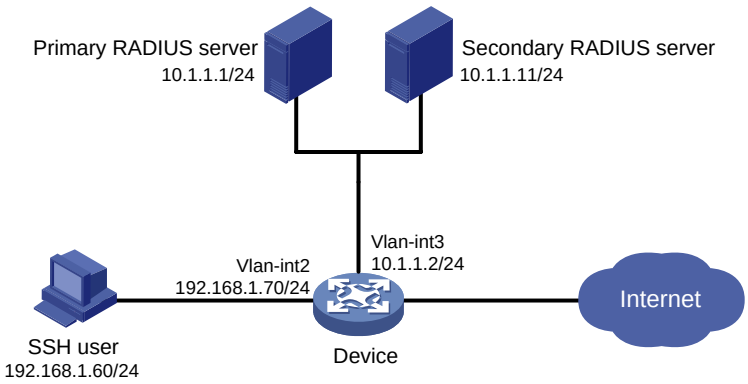
本案例介绍 SSH 用户的 RADIUS 认证和授权的配置方法。

3.2 组网需求

如图 12 所示，通过在作为 NAS 的 Device 上配置远程 RADIUS 认证、授权功能，实现 SSH 用户的安全登录。在网络架构上采用主从 RADIUS 服务器的方式来提高用户认证的稳定性。要求在 Device 上配置实现：

- 使用 RADIUS 服务器对登录 Device 的 SSH 用户进行认证和授权，登录用户名为 hello@bbb，密码为 aabbcc；
- Device 向 RADIUS 服务器发送的用户名带域名，服务器根据用户名携带的域名来区分提供给用户的服务。
- 用户通过认证后可执行系统所有功能和资源的相关 **display** 命令。

图12 SSH 用户的远端 RADIUS 认证和授权配置组网图



3.3 配置步骤

1. 配置 RADIUS 服务器

说明

- 本节以 iMC 为例（使用 iMC 版本为：iMC PLAT 7.0(E0102)、iMC EIA 7.0(E0201)），说明该例中 RADIUS 服务器的基本配置。
- 主从 RADIUS 服务器设置相同，本节以主 RADIUS 服务器设置为例。

登录进入 iMC 管理平台，选择“用户”页签，单击导航树中的[接入策略管理/接入设备管理/接入设备配置]菜单项，进入接入设备配置页面，在该页面中单击“增加”按钮，进入增加接入设备页面。

- 设置与 Device 交互报文时使用的认证和授权共享密钥为“expert”；
- 设置认证及计费的端口号分别为“1812”（RADIUS 服务器的认证端口为 UDP 端口 1812）和“1813”（RADIUS 服务器的计费端口为 UDP 端口 1813）；
- 选择业务类型为“设备管理业务”；
- 选择接入设备类型为“H3C(General)”；
- 选择或手工增加接入设备，添加 IP 地址为 10.1.1.2 的接入设备；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图13 增加接入设备

选择“用户”页签，单击导航树中的[接入用户管理视图/设备管理用户]菜单项，进入设备管理用户列表页面，在该页面中单击<增加>按钮，进入增加设备管理用户页面。

- 输入用户名“hello@bbb”和密码。
- 选择服务类型为“SSH”。
- 输入用户角色名“network-operator”
- 添加所管理设备的 IP 地址，IP 地址范围为“10.1.1.0～10.1.1.255”。
- 单击<确定>按钮完成操作。

说明

添加的所管理设备的 IP 地址范围要包含添加的接入设备的 IP 地址。

图14 增加设备管理用户

2. 配置 Device

创建 VLAN 2，并将 Ten-GigabitEthernet1/0/2 加入 VLAN 2。

```
<Device> system-view
[Device] vlan 2
[Device-vlan2] port ten-gigabitethernet 1/0/2
[Device-vlan2] quit
```

配置 VLAN 接口 2 的 IP 地址。

```
[Device] interface vlan-interface 2
[Device-Vlan-interface2] ip address 192.168.1.70 255.255.255.0
[Device-Vlan-interface2] quit
```

创建 VLAN 3，并将 Ten-GigabitEthernet1/0/1 加入 VLAN 3。

```
[Device] vlan 3
[Device-vlan3] port ten-gigabitethernet 1/0/1
[Device-vlan3] quit
```

配置 VLAN 接口 3 的 IP 地址。

```
[Device] interface vlan-interface 3
[Device-Vlan-interface3] ip address 10.1.1.2 255.255.255.0
[Device-Vlan-interface3] quit
```

生成 RSA 密钥对。

```
[Device] public-key local create rsa
```

```
The range of public key modulus is (512 ~ 4096).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
...........
Create the key pair successfully.
```

生成 DSA 密钥对。

```
[Device] public-key local create dsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.......
Create the key pair successfully.
```

生成 secp256r1 类型的 ECDSA 密钥对。

```
[Device] public-key local create ecdsa secp256r1
Generating Keys...
Create the key pair successfully.
```

生成 secp384r1 类型的 ECDSA 密钥对。

```
[Device] public-key local create ecdsa secp384r1
Generating Keys...
.
Create the key pair successfully.
```

开启 SSH 服务器功能。

```
[Device] ssh server enable
```

配置 SSH 用户登录采用 AAA 认证方式。

```
[Device] line vty 0 63
[Device-line-vty0-63] authentication-mode scheme
[Device-line-vty0-63] quit
```

创建 RADIUS 方案 rad。

```
[Device] radius scheme rad
```

配置主认证服务器的 IP 地址为 10.1.1.1，认证端口号为 1812。

```
[Device-radius-rad] primary authentication 10.1.1.1 1812
```

配置从认证服务器的 IP 地址为 10.1.1.11，认证端口号为 1812。

```
[Device-radius-rad] secondary authentication 10.1.1.11 1812
```

配置主计费服务器的 IP 地址为 10.1.1.1，计费端口号为 1813。

```
[Device-radius-rad] primary accounting 10.1.1.1 1813
```

配置从计费服务器的 IP 地址为 10.1.1.11，计费端口号为 1813。

```
[Device-radius-rad] secondary accounting 10.1.1.11 1813
```

配置与认证和计费服务器交互报文时的共享密钥为明文 expert。

```
[Device-radius-rad] key authentication simple expert
[Device-radius-rad] key accounting simple expert
```

配置向 RADIUS 服务器发送的用户名要携带域名。

```
[Device-radius-rad] user-name-format with-domain
[Device-radius-rad] quit
```

创建 ISP 域 bbb，为 login 用户配置 AAA 认证方法为 RADIUS 认证、授权和计费。

```
[Device] domain bbb
[Device-isp-bbb] authentication login radius-scheme rad
[Device-isp-bbb] authorization login radius-scheme rad
[Device-isp-bbb] accounting login radius-scheme rad
[Device-isp-bbb] quit
```

3.4 验证配置

用户向 Device 发起 SSH 连接，在 SSH 客户端按照提示输入用户名 hello@bbb 和密码 aabbcc 通过认证，并且获得用户角色 network-operator（用户通过认证后可执行系统所有功能和资源的相关 **display** 命令）。

主服务器可达时，设备与主 RADIUS 服务器进行交互。

显示主服务器可达时的 RADIUS 方案的配置信息。

```
<Sysname> display radius scheme
Total 1 RADIUS schemes

------------------------------------------------------------------------
RADIUS scheme name: rad
  Index: 0
  Primary authentication server:
    Host name: Not Configured
    IP   : 10.1.1.1                                 Port: 1812
    VPN  : Not configured
    State: Active
    Test profile: Not configured
    Weight: 0
  Primary accounting server:
    Host name: Not Configured
    IP   : 10.1.1.1                                 Port: 1813
    VPN  : Not configured
    State: Active
    Weight: 0
  Second authentication server:
    Host name: Not Configured
    IP   : 10.1.1.11                                Port: 1812
    VPN  : Not configured
    State: Active
    Test profile: Not configured
    Weight: 0
  Second accounting server:
    Host name: Not Configured
    IP   : 10.1.1.11                                Port: 1813
    VPN  : Not configured
    State: Active
```

```
    Weight: 0
  Accounting-On function                     : Disabled
    extended function                        : Disabled
    retransmission times                     : 50
    retransmission interval(seconds)         : 3
  Timeout Interval(seconds)                  : 3
  Retransmission Times                       : 3
  Retransmission Times for Accounting Update : 5
  Server Quiet Period(minutes)               : 5
  Realtime Accounting Interval(seconds)      : 720
  Stop-accounting packets buffering          : Enabled
    Retransmission times                     : 500
  NAS IP Address                             : Not configured
  VPN                                        : Not configured
  User Name Format                           : with-domain
  Data flow unit                             : Byte
  Packet unit                                : One
  Attribute 15 check-mode                    : Strict
  Attribute 25                               : Standard
  Attribute Remanent-Volume unit             : Kilo
  server-load-sharing                        : Disabled
  Attribute 31 MAC format                    : HH-HH-HH-HH-HH-HH
  Stop-accounting packets send-force         : Disabled
  Reauthentication server selection          : Inherit
```

主服务器不可达时，再查看 RADIUS 方案的配置信息，会发现主服务器的状态从 Active 变为 Block。此时，设备变成与从 RADIUS 服务器进行交互。

3.5 配置文件

```
#
vlan 2 to 3
#
interface Vlan-interface2
 ip address 192.168.1.70 255.255.255.0
#
interface Vlan-interface3
 ip address 10.1.1.2 255.255.255.0
#
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 3
#
line vty 0 63
 authentication-mode scheme
```

```
 user-role network-operator
#
 ssh server enable
#
radius scheme rad
 primary authentication 10.1.1.1
 primary accounting 10.1.1.1
 secondary authentication 10.1.1.11
 secondary accounting 10.1.1.11
 key authentication cipher $c$3$GBZ1jhslcGwSOpSejsESMnOr8Gb8SIT5ew==
 key accounting cipher $c$3$nGb/DWK8pxbHaLXQVc+xsmbUr1etIZVd7Q==
#
domain bbb
 authentication login radius-scheme rad
 authorization login radius-scheme rad
 accounting login radius-scheme rad
#
```

3.6 相关资料

- 产品配套“安全配置指导”中的“SSH”和“AAA”。
- 产品配套“安全命令参考”中的“SSH”和“AAA”。

4 SSH 用户的 HWTACACS 认证、授权、计费配置（ACS server）

4.1 简介

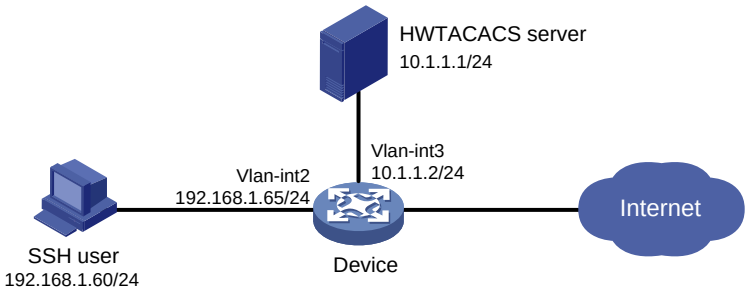
本案例介绍 SSH 用户的 HWTACACS 认证、授权、计费配置方法。

4.2 组网需求

为了提高远程访问的安全性，需要在 Device 和管理员主机之间建立 SSH 连接，具体要求如下：

- Device 使用 Cisco ACS server 作为 HWTACACS 服务器对 Stelnet 客户端进行认证和授权；
- 管理员在主机上运行 Stelnet 客户端，并采用用户名 manager@bbb 和密码 1234ab##登录 Device，且登录后享有最高配置权限。

图15 SSH 用户的 HWTACACS 认证和授权配置举例



4.3 配置思路

- 为了保证 Device 可以使用 ACS server 认证用户，需要在 ACS server 上完成添加 AAA client 以及用户的相关配置。
- 为了要求用户通过用户线登录 Device 时输入用户名和密码，需要在 Device 上配置登录用户线的认证方式为 scheme 方式。
- 未了保证 Device 能够对登录用户进行认证和授权，需要在 Device 上完成 AAA 配置，包括配置 ISP 域，以及与 HWTACACS 服务器交互的 TACACS 方案。
- 为了保证管理员可以运行采用了不同公钥算法的 Stelnet 客户端与 Device 建立 SSH 连接，需要在 Device 上生成 RSA、DSA、ECDSA 密钥对。
- 为了使 Stelnet 用户登录设备后能享有最高配置权限，指定缺省用户角色为 network-admin。

4.4 配置步骤

1. 配置 HWTACACS 服务器

说明

- 本文以 ACSv4.2 为例，说明 TACACS server 的基本配置。
- 在进行下面的配置之前，请保证设备管理员的主机与 ACS 服务器之间路由可达。

(1) 登录 ACS server

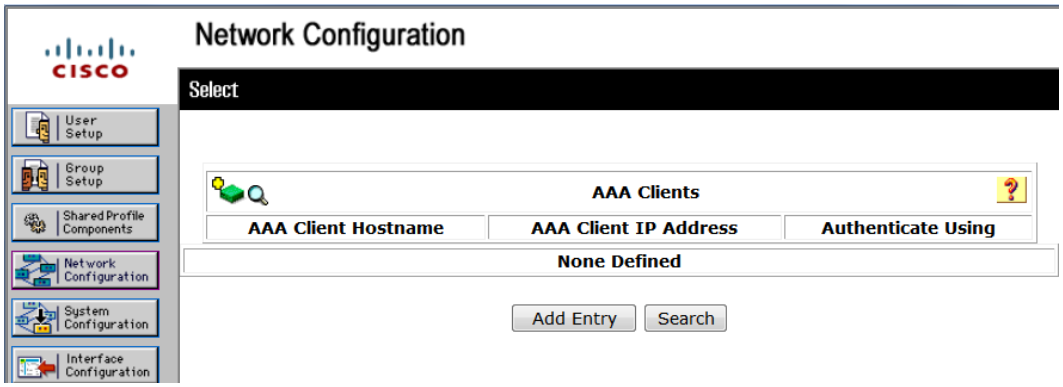
如图 16 所示的 Web 登录页面中，输入 Web 登录用户名和密码，单击“Login”按钮，即可登录 ACS server。

图16 登录 ACS server

(2) 添加接入设备

在左侧导航栏中选择[Network Configuration]，打开网络配置界面，单击<Add Entry>，进入 AAA Client 的编辑页面。

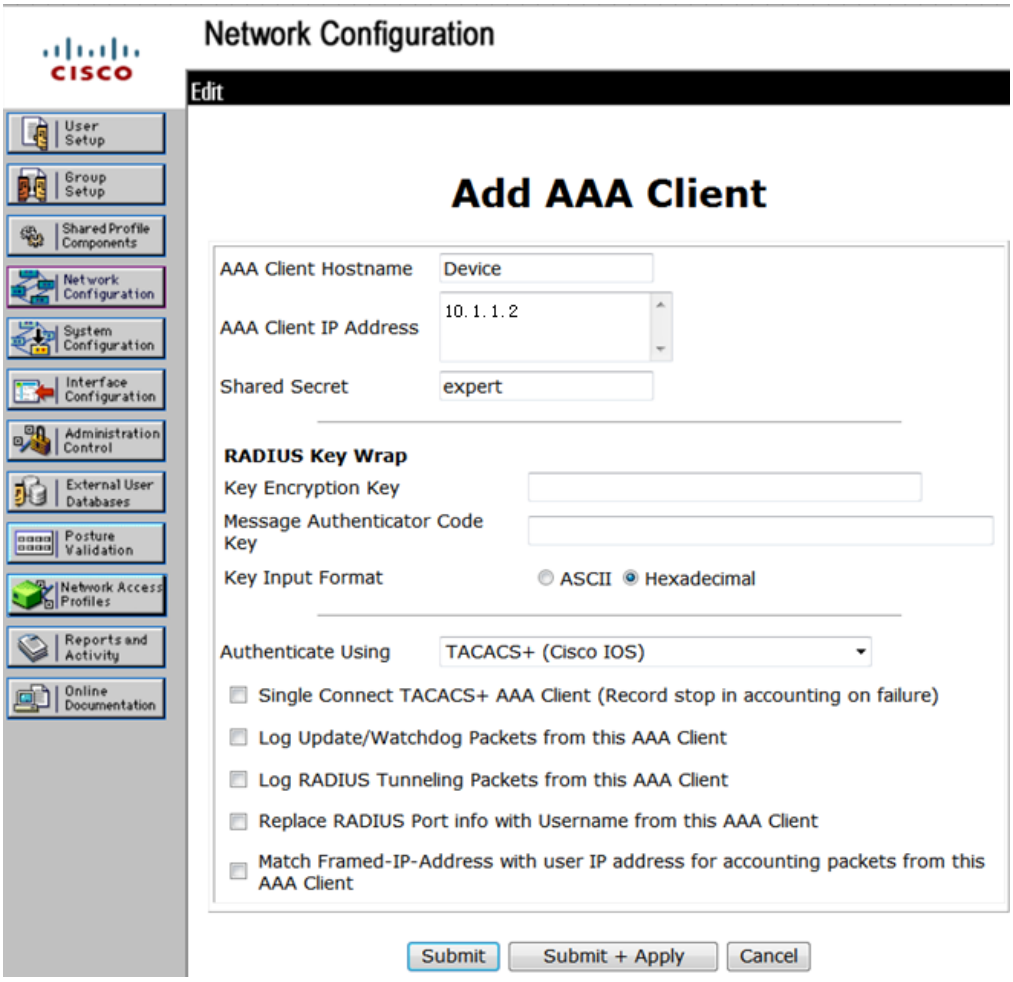
图17 添加接入设备



在 AAA Client 的编辑页面中进行如下配置：

- 输入接入设备名称、接入设备 IP 地址、交互 TACACS 报文的共享密钥；
- 选择认证协议类型为“TACACS+ (Cisco IOS)”；
- 单击“Submit + Apply”按钮完成操作。

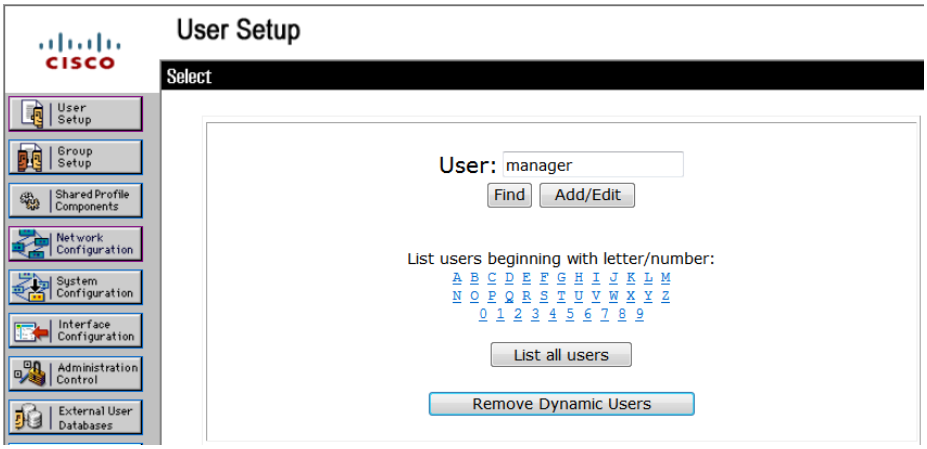
图18 配置接入设备



(3) 添加登录用户

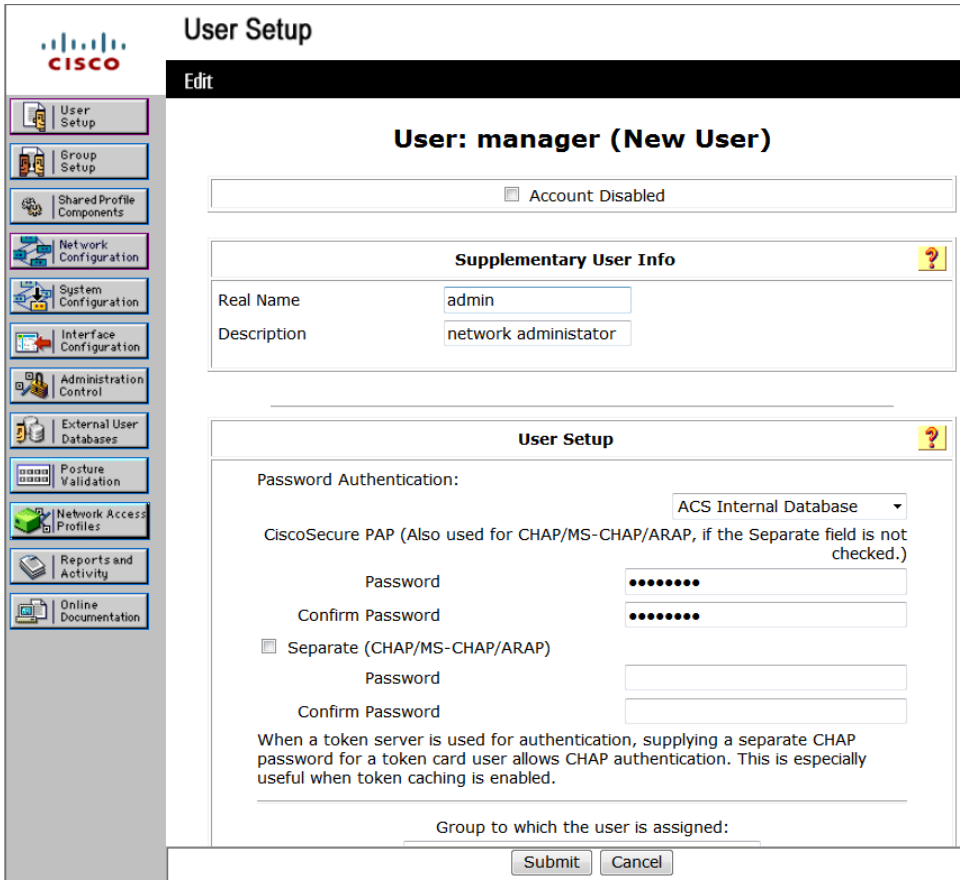
在左侧导航栏中选择[User Setup]，打开用户配置界面，在文本框中输入用户名“manager”，单击“Add/Edit”后，进入该用户的编辑页面。

图19 添加登录用户



填写用户的相关信息，配置用户登录密码，选择用户所属组（本例中使用缺省组）。

图20 配置登录用户信息



2. 配置 Device

创建 VLAN 2，并将 Ten-GigabitEthernet1/0/2 加入 VLAN 2。

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

```
[Device] vlan 2
[Device-vlan2] port ten-gigabitethernet 1/0/2
[Device-vlan2] quit
```

配置 VLAN 接口 2 的 IP 地址。

```
[Device] interface vlan-interface 2
[Device-Vlan-interface2] ip address 192.168.1.65 255.255.255.0
[Device-Vlan-interface2] quit
```

创建 VLAN 3，并将 Ten-GigabitEthernet1/0/1 加入 VLAN 3。

```
[Device] vlan 3
[Device-vlan3] port ten-gigabitethernet 1/0/1
[Device-vlan3] quit
```

配置 VLAN 接口 3 的 IP 地址。

```
[Device] interface vlan-interface 3
[Device-Vlan-interface3] ip address 10.1.1.2 255.255.255.0
[Device-Vlan-interface3] quit
```

生成 RSA 密钥对。

```
[Device] public-key local create rsa
The range of public key modulus is (512 ~ 4096).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
...
Create the key pair successfully.
```

生成 DSA 密钥对。

```
[Device] public-key local create dsa
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
........
Create the key pair successfully.
```

生成 secp256r1 类型的 ECDSA 密钥对。

```
[Device] public-key local create ecdsa secp256r1
Generating Keys...
Create the key pair successfully.
```

生成 secp384r1 类型的 ECDSA 密钥对。

```
[Device] public-key local create ecdsa secp384r1
Generating Keys...
.
Create the key pair successfully.
```

使能 SSH 服务器功能。

```
[Device] ssh server enable
```

设置 Stelnet 客户端登录用户界面的认证方式为 scheme。

```
[Device] line vty 0 63
```

```
[Device-line-vty0-63] authentication-mode scheme
[Device-line-vty0-63] quit
```
使能缺省用户角色授权功能，使得认证通过后的用户具有缺省的用户角色 network-admin。
```
[Device] role default-role enable network-admin
```
创建 TACACS 方案 rad。
```
[Device] hwtacacs scheme tac
```
配置主认证服务器的 IP 地址为 10.1.1.1，认证端口号为 49。
```
[Device-hwtacacs-tac] primary authentication 10.1.1.1 49
```
配置与认证服务器交互报文时的共享密钥为明文 expert。
```
[Device-hwtacacs-tac] key authentication simple expert
```
配置主授权服务器的 IP 地址为 10.1.1.1，授权端口号为 49。
```
[Device-hwtacacs-tac] primary authorization 10.1.1.1 49
```
配置与授权服务器交互报文时的共享密钥为明文 expert。
```
[Device-hwtacacs-tac] key authorization simple expert
```
配置向 TACACS 服务器发送的用户名不携带域名。
```
[Device-hwtacacs-tac] user-name-format without-domain
[Device-hwtacacs-tac] quit
```
创建 ISP 域 bbb，为 login 用户配置 AAA 认证方法为 TACACS 认证/授权、不计费。
```
[Device] domain bbb
[Device-isp-bbb] authentication login hwtacacs-scheme tac
[Device-isp-bbb] authorization login hwtacacs-scheme tac
[Device-isp-bbb] accounting login none
[Device-isp-bbb] quit
```

4.5 验证配置


说明

Stelnet客户端软件有很多，例如PuTTY、OpenSSH等。本文中仅以客户端软件PuTTY0.60为例，说明 Stelnet 客户端的配置方法。

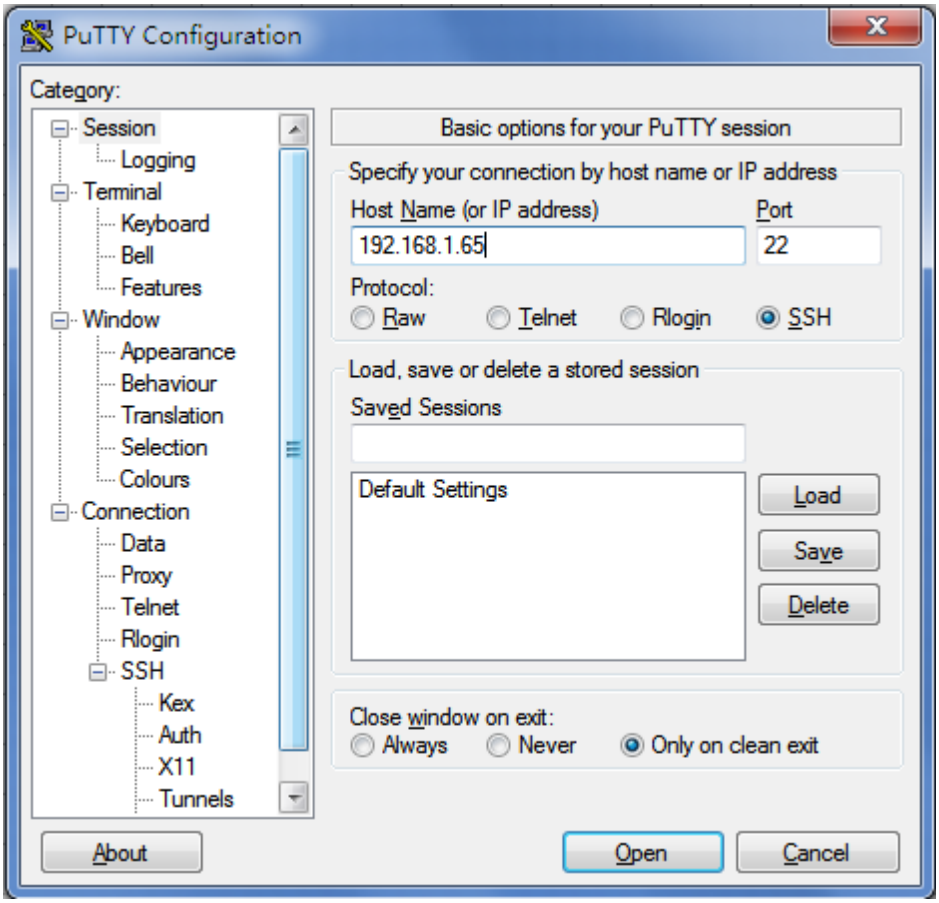
安装 PuTTY 0.60 软件。

打开 PuTTY.exe 程序，点击“Session”功能区，在图 21 所示的配置界面中进行如下配置：

- 在“Host Name（or IP address）”文本框中输入 Stelnet 服务器的 IP 地址为 192.168.1.65。
- 在“Port”文本框中输入 SSH 协议端口号 22。
- 在“Connection type”区域选择 SSH 协议。

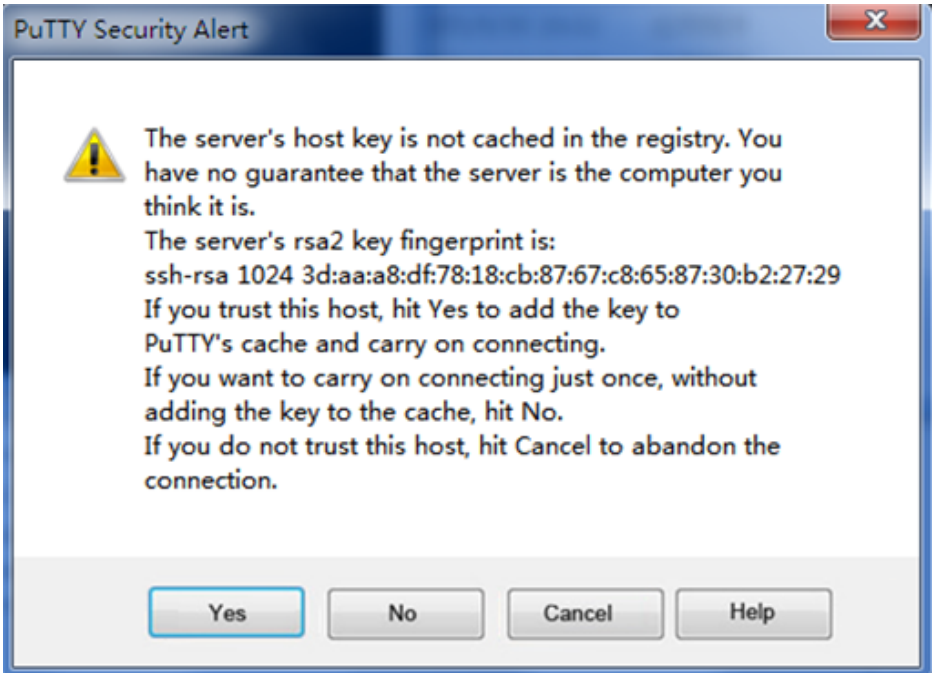
单击<Open>按钮。

图21 Stelnet 客户端配置界面



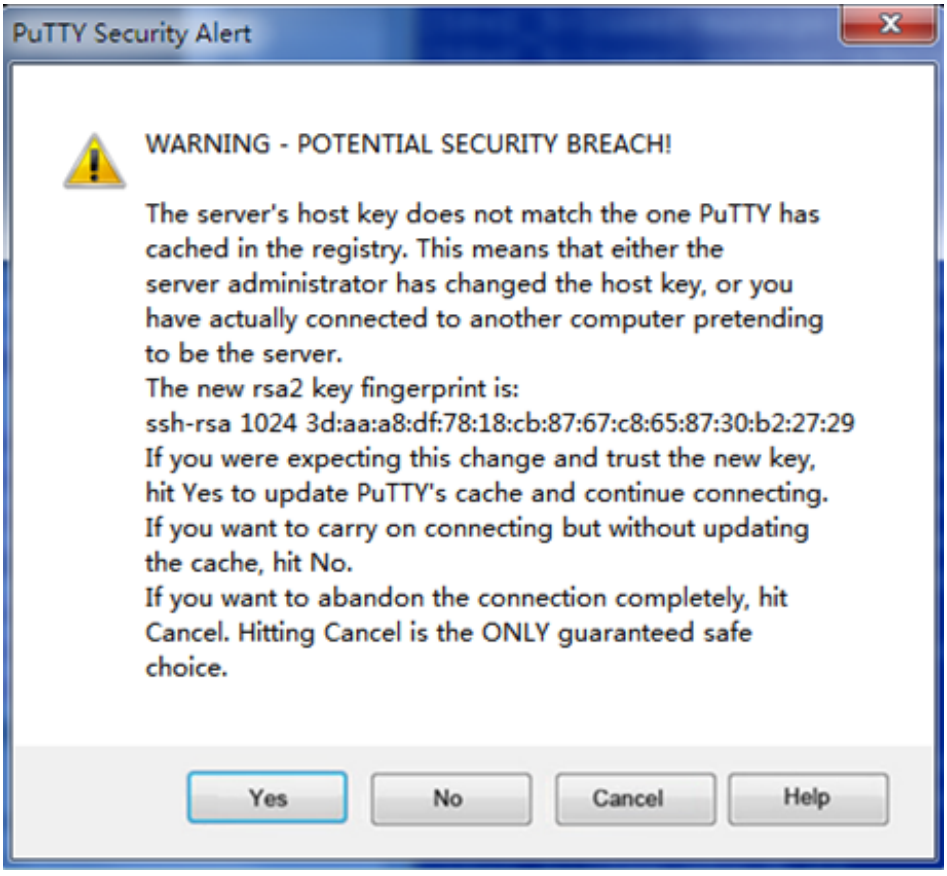
如果弹出图 22 所示“PuTTY Security Alert”对话框，请根据实际情况做出选择。本例中选择信任该服务器，则单击“Yes”按钮。

图22 Stelnet 客户端登录界面（一）



如果弹出图 23 所示“PuTTY Security Alert”对话框，请根据实际情况做出选择。本例中选择信任该主机密钥，则单击“Yes”按钮。

图23 Stelnet 客户端登录界面（二）



在如下登录界面中输入用户名 manager@bbb 和密码 1234ab##，即可成功登录设备使用所有命令。

```
login as: manager@bbb
manager@bbb@192.168.1.65's password:

******************************************************************************
* Copyright (c) 2004-2018 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

<Device>
```

4.6 配置文件

```
#
vlan 2 to 3
#
interface Vlan-interface2
 ip address 192.168.1.65 255.255.255.0
#
interface Vlan-interface3
 ip address 10.1.1.2 255.255.255.0
#
interface Ten-GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 3
#
line vty 0 63
 authentication-mode scheme
 user-role network-operator
#
ssh server enable
#
hwtacacs scheme tac
 primary authentication 10.1.1.1
 primary authorization 10.1.1.1
 key authentication cipher $c$3$/9bCuPjMxjOtUvBx8NjtN+AnAsuLT2SrNA==
 key authorization cipher $c$3$QF/fFJNv9IyKyFlsNOpeBYnDXArNhOvOdQ==
 user-name-format without-domain
#
domain bbb
 authentication login hwtacacs-scheme tac
```

```
 authorization login hwtacacs-scheme tac
 accounting login none
#
role default-role enable network-admin
#
```

4.7 相关资料

- 产品配套“安全配置指导”中的“SSH”。
- 产品配套“安全命令参考”中的“SSH”。
- 产品配套“安全配置指导”中的“AAA”。
- 产品配套“安全命令参考”中的“AAA”。

5 SSH 用户的 AAA local 认证配置

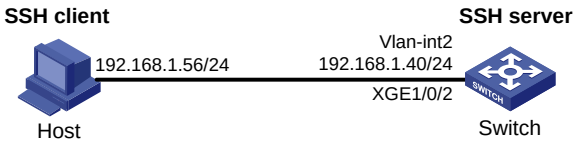
5.1 简介

本案例介绍 SSH 用户的 AAA local 认证配置方法。

5.2 组网需求

通过配置 Switch 实现 AAA local 认证。SSH 用户的用户名为 client001，密码为 hello12345，登录设备后可以使用所有命令。

图24 SSH 用户 local 认证配置组网图



5.3 配置步骤

创建 VLAN 2，并将 Ten-GigabitEthernet1/0/2 加入 VLAN 2。

```
[Switch] vlan 2
[Switch-vlan2] port ten-gigabitethernet 1/0/2
[Switch-vlan2] quit
```

配置 VLAN 接口 2 的 IP 地址，客户端将通过该地址连接 SSH 服务器。

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.1.40 255.255.255.0
[Switch-Vlan-interface2] quit
```

创建本地 RSA 及 DSA 密钥对。

```
<Switch> system-view
[Switch] public-key local create rsa
[Switch] public-key local create dsa
```

使能 SSH 服务器功能。

```
[Switch] ssh server enable
```

设置 SSH 用户登录用户线的认证方式为 AAA 认证。

```
[Switch] line vty 0 63
[Switch-line-vty0-63] authentication-mode scheme
[Switch-line-vty0-63] quit
```

创建本地用户 client001，并设置用户密码为 hello12345、服务类型为 SSH、用户角色为 network-admin。

```
[Switch] local-user client001 class manage
New local user added.
[Switch-luser-manage-client001] password simple hello12345
[Switch-luser-manage-client001] service-type ssh
```

```
[Switch-luser-manage-client001] authorization-attribute user-role network-admin
[Switch-luser-manage-client001] quit
```

创建 ISP 域 bbb，为 login 用户配置 AAA 认证方法为本地认证。

```
[Switch] domain bbb
[Switch-isp-bbb] authentication login local
[Switch-isp-bbb] quit
```

5.4 验证配置

说明

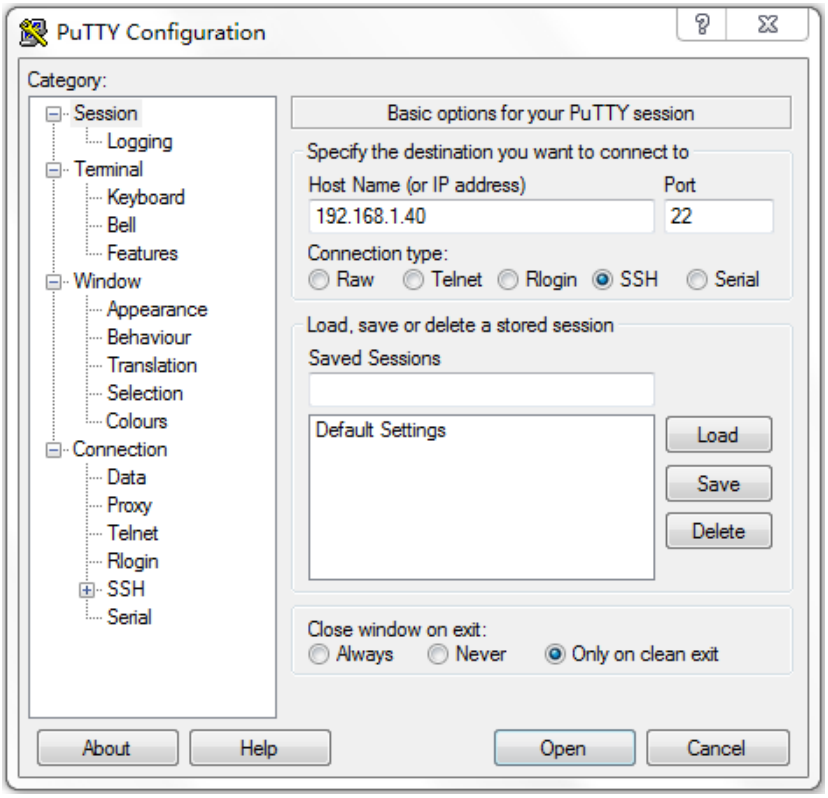
SSH 客户端软件很多，本文中以客户端软件 PuTTY0.60 为例说明 SSH 客户端的配置方法。

安装 PuTTY0.60 软件。

打开 PuTTY.exe 程序，点击“Session”功能区，出现如图 25 所示的客户端配置界面。

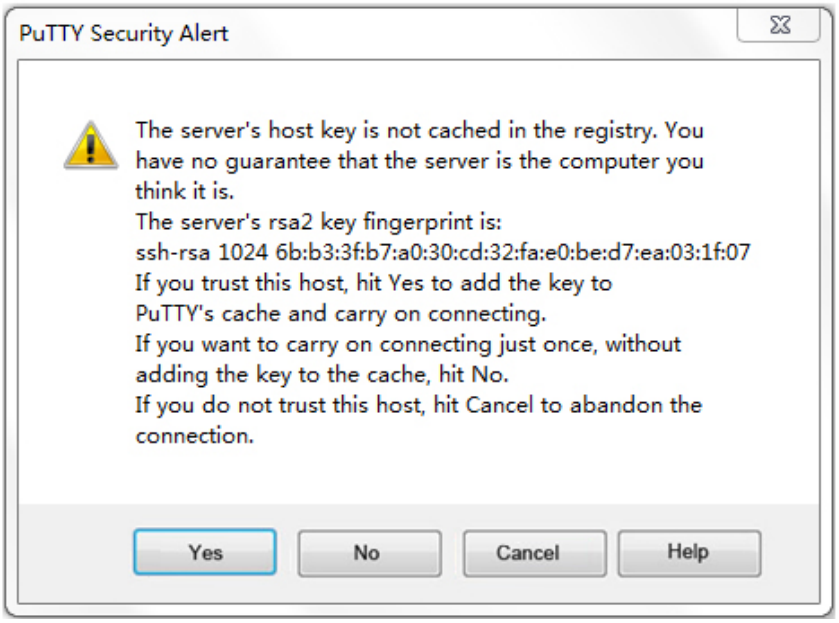
- 在“Host Name（or IP address）”文本框中输入 SSH 服务器的 IP 地址为 192.168.1.40。
- 在“Port”文本框中输入 SSH 协议端口号 22。
- 在“Connection type”区域选择 SSH 协议。

图25 SSH 客户端配置界面



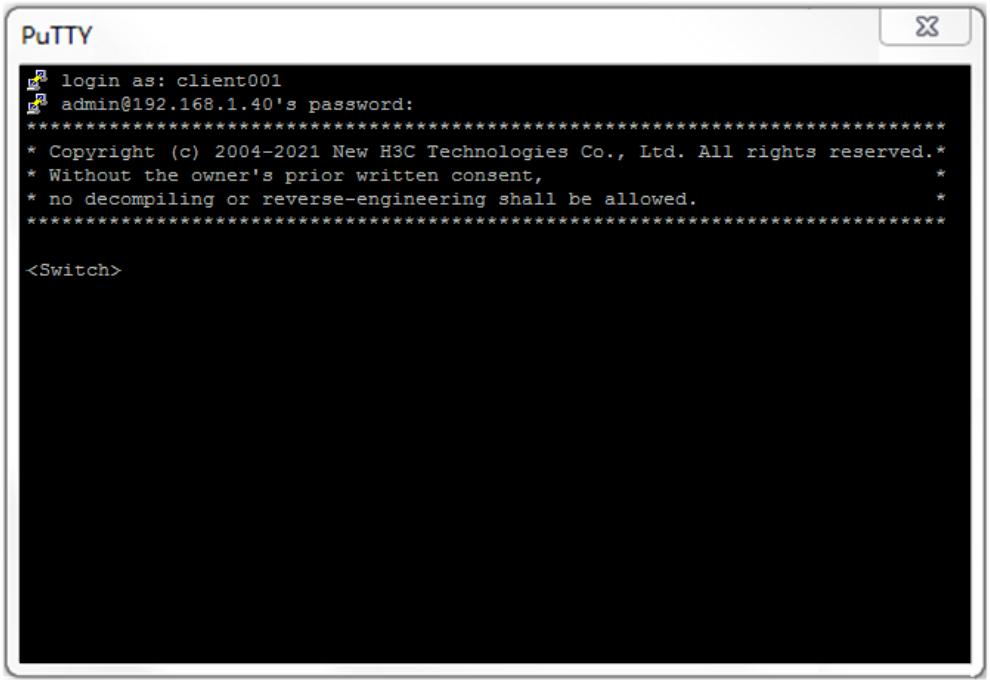
在图 25 界面中，单击<Open>按钮。弹出“PuTTY Security Alert”对话框。

图26 SSH 客户端登录界面（一）



单击“Yes”按钮，并输入用户名“client001”和密码“hello12345”（输入密码的不会显示），即可成功登录设备并使用所有命令。

图27 SSH 客户端登录界面（二）



5.5 配置文件

```
#
vlan 2
#
interface Vlan-interface2
 ip address 192.168.1.40 255.255.255.0
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 2
#
line vty 0 63
 authentication-mode scheme
 user-role network-operator
#
 ssh server enable
#
domain bbb
 authentication login local
#
local-user client001 class manage
 password hash
$h$6$rLDGxBtUHlyovI15$k8yc//6l73h6CRK89jqTVf8Hu6VicbEl5EjUPqzykYj33YSQxPdHrSr+BIMeZUZDfs
RAiy28ME9Vhb7VcVXpZw==
 service-type ssh
 authorization-attribute user-role network-admin
 authorization-attribute user-role network-operator
#
```

5.6 相关资料

- 产品配套“安全配置指导”中的“SSH”。
- 产品配套“安全命令参考”中的“SSH”。
- 产品配套“安全配置指导”中的“AAA”。
- 产品配套“安全命令参考”中的“AAA”。

端口安全快速配置指南

目 录

1 配置端口安全 autoLearn 模式

1.1 简介

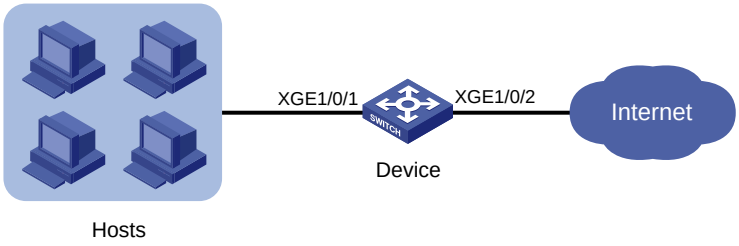
本案例介绍端口安全 autoLearn 模式的配置方法。

1.2 组网需求

如图 1 所示，用户通过 Device 连接到网络。通过配置端口安全 autolearn 模式，实现对接入用户的控制，具体需求如下：

- 最多同时允许 64 个用户直接通过交换机接入 Internet，无需进行认证；
- 当用户数量超过设定值后，新用户无法通过 Device 接入 Internet；
- 配置安全 MAC 地址并设定安全 MAC 地址老化时间，来防止交换机与用户相连端口学习到的 MAC 地址的丢失，及安全 MAC 地址不老化带来的一些问题；
- 配置入侵检测特性方式为**`disableport-temporarily`**，当再有新的 MAC 地址接入时，交换机与用户相连端口被暂时断开连接，30 秒后自动恢复端口的开启状态。

图1 端口安全 autoLearn 模式组网图



1.3 配置注意事项

当端口工作于 autoLearn 模式时，无法更改端口安全允许的最大 MAC 地址数。

1.4 配置步骤

使能端口安全。

```
<Device> system-view
[Device] port-security enable
```

设置安全 MAC 地址的老化时间为 30 分钟。

```
[Device] port-security timer autolearn aging 30
```

设置端口安全允许的最大安全 MAC 地址数为 64。

```
[Device] interface ten-gigabitethernet 1/0/1
[Device-Ten-GigabitEthernet1/0/1] port-security max-mac-count 64
```

设置端口安全模式为 autoLearn。

```
[Device-Ten-GigabitEthernet1/0/1] port-security port-mode autolearn
```

设置触发入侵检测特性后的保护动作为暂时关闭端口，关闭时间为 30 秒。

```
[Device-Ten-GigabitEthernet1/0/1] port-security intrusion-mode disableport-temporarily
[Device-Ten-GigabitEthernet1/0/1] quit
[Device] port-security timer disableport 30
```

1.5 验证配置

上述配置完成后，可以使用 **display port-security interface** 命令查看端口安全的配置情况。

```
[Device] display port-security interface ten-gigabitethernet 1/0/1
Global port security parameters:
   Port security           : Enabled
   AutoLearn aging time    : 30 min
   Disableport timeout     : 30 s
   Blockmac timeout        : 180 s
   MAC move                : Denied
   Authorization fail      : Online
   NAS-ID profile          : Not configured
   Dot1x-failure trap      : Disabled
   Dot1x-logon trap        : Disabled
   Dot1x-logoff trap       : Disabled
   Intrusion trap          : Disabled
   Address-learned trap    : Disabled
   Mac-auth-failure trap   : Disabled
   Mac-auth-logon trap     : Disabled
   Mac-auth-logoff trap    : Disabled
   Open authentication     : Disabled
   OUI value list          :

 Ten-GigabitEthernet1/0/1 is link-up
   Port mode                       : autoLearn
   NeedToKnow mode                 : Disabled
   Intrusion protection mode       : DisablePortTemporarily
   Security MAC address attribute
       Learning mode               : Sticky
       Aging type                  : Periodical
   Max secure MAC addresses        : 64
   Current secure MAC addresses    : 5
   Authorization                   : Permitted
   NAS-ID profile                  : Not configured
   Free VLANs                      : Not configured
   Open authentication             : Disabled
   MAC-move VLAN check bypass      : Disabled
```

可以看到端口安全所允许的最大安全 MAC 地址数为 64，端口模式为 autoLearn，入侵检测保护动作为 DisablePortTemporarily，入侵发生后端口被禁用时间为 30 秒。

配置生效后，端口允许地址学习，学习到的 MAC 地址数可在上述显示信息的“Current secure MAC addresses”字段查看到。

具体的 MAC 地址信息可以在二层以太网接口视图下用 **display this** 命令查看。

```
[Device] interface ten-gigabitethernet 1/0/1
[Device-Ten-GigabitEthernet1/0/1] display this
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 port-security intrusion-mode disableport-temporarily
 port-security max-mac-count 64
 port-security port-mode autolearn
 port-security mac-address security sticky 00e0-fc00-5920 vlan 1
 port-security mac-address security sticky 00e0-fc00-592a vlan 1
 port-security mac-address security sticky 00e0-fc00-592b vlan 1
 port-security mac-address security sticky 00e0-fc00-592c vlan 1
 port-security mac-address security sticky 00e0-fc00-592d vlan 1
#
```

当学习到的 MAC 地址数达到 64 后，用命令 **display port-security interface** 可以看到端口模式变为 secure，再有新的 MAC 地址到达将触发入侵保护，可以通过命令 **display interface** 看到此端口关闭。30 秒后，端口状态恢复。此时，如果手动删除几条安全 MAC 地址后，端口安全的状态重新恢复为 autoLearn，可以继续学习 MAC 地址。

1.6 配置文件

```
#
 port-security enable
 port-security timer disableport 30
 port-security timer autolearn aging 30
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 port-security intrusion-mode disableport-temporarily
 port-security max-mac-count 64
 port-security port-mode autolearn
#
```

1.7 相关资料

- 产品配套“安全配置指导”中的“端口安全”。
- 产品配套“安全命令参考”中的“端口安全”。

VRRP 快速配置指南

目 录

1 配置 IPv4 VRRP 单备份组

1.1 简介

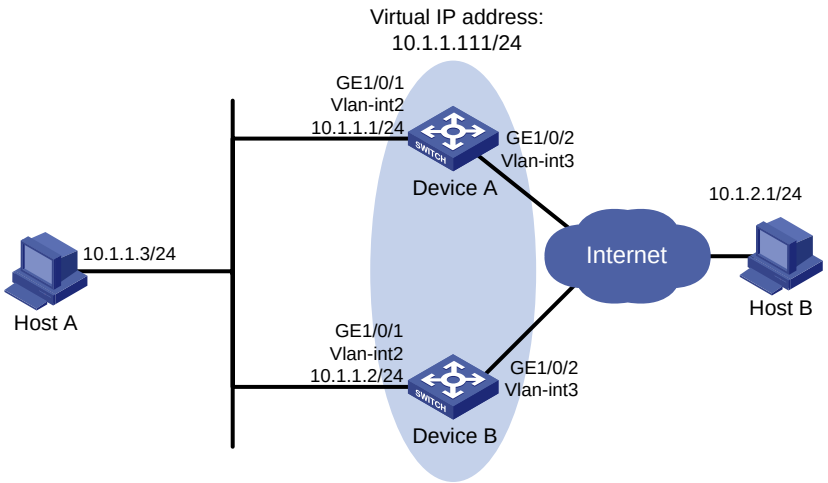
本案例介绍 IPv4 VRRP 单备份组的配置方法。

1.2 组网需求

如图 1 所示，Host A 需要访问 Internet 上的 Host B，Host A 所在网络的出口处部署了两台设备。现要求使用 VRRP 单备份组功能，将这两台设备组成一台虚拟路由器，作为 Host A 的缺省网关。具体应用需求如下：

- 在正常情况下，由 Device A 承担网关功能，转发 Host A 发送至外网的流量；
- 当 Device A 或者 Device A 的上行接口出现故障时，由 Device B 接替 Device A 承担网关功能；
- 当 Device A 或者 Device A 的上行接口故障恢复后，由 Device A 继续承担网关功能。

图1 VRRP 单备份组配置组网图



1.3 配置注意事项

- 备份组的虚拟 IP 地址不能为全零地址（0.0.0.0）、广播地址（255.255.255.255）、环回地址、非 A/B/C 类地址和其它非法 IP 地址（如 0.0.0.1）。
- IPv4 VRRP 既可以使用 VRRPv2 版本，也可以使用 VRRPv3 版本（缺省情况使用 VRRPv3）。请确保 IPv4 VRRP 备份组中的所有设备上配置的 IPv4 VRRP 版本一致，否则备份组无法正常工作。
- 建议将备份组的虚拟 IP 地址和备份组中设备下行接口的 IP 地址配置为同一网段，否则可能导致局域网内的主机无法访问外部网络。
- 对于同一个 VRRP 备份组的成员设备，必须保证虚拟路由器的 IP 地址配置完全一样。
- 用户在配置降低优先级幅度时，需要确保降低后的优先级比备份组内其他设备的优先级要低，确保备份组内有其他设备被选为 Master。

1.4 配置步骤

1. 配置 Device A

创建 VLAN 2，并将接口 GigabitEthernet1/0/1 加入到 VLAN 2 中

```
<DeviceA> system-view
[DeviceA] vlan 2
[DeviceA-vlan2] port gigabitethernet 1/0/1
[DeviceA-vlan2] quit
```

创建 VLAN 接口 2，并将接口 IP 地址配置为 10.1.1.1/24。

```
[DeviceA] interface vlan-interface 2
[DeviceA-Vlan-interface2] ip address 10.1.1.1 255.255.255.0
```

创建 VRRP 备份组 1，并配置备份组 1 的虚拟 IP 地址为 10.1.1.111。

```
[DeviceA-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.111
```

设置 Device A 在备份组 1 中的优先级为 110，高于 Device B 的优先级 100，以保证 Device A 成为 Master 负责转发流量。

```
[DeviceA-Vlan-interface2] vrrp vrid 1 priority 110
```

设置 Device A 工作在抢占方式，以保证 Device A 故障恢复后，能再次抢占成为 Master，即只要 Device A 正常工作，就由 Device A 负责转发流量。为了避免频繁地进行状态切换，配置抢占延迟时间为 5000 厘秒。

```
[DeviceA-Vlan-interface2] vrrp vrid 1 preempt-mode delay 5000
[DeviceA-Vlan-interface2] quit
```

创建和上行端口 GigabitEthernet1/0/2 关联的 Track 项 1。

```
[DeviceA] track 1 interface gigabitethernet 1/0/2
[DeviceA-track-1] quit
```

配置监视 Track 项 1，Track 项的状态为 Negative 时，Device A 在 VRRP 备份组中的优先级降低的数值为 50。

```
[DeviceA] interface vlan-interface 2
[DeviceA-Vlan-interface2] vrrp vrid 1 track 1 priority reduced 50
[DeviceA-Vlan-interface2] quit
```

2. 配置 Device B

配置 VLAN2。

```
<DeviceB> system-view
[DeviceB] vlan 2
[DeviceB-Vlan2] port gigabitethernet 1/0/1
[DeviceB-vlan2] quit
[DeviceB] interface vlan-interface 2
[DeviceB-Vlan-interface2] ip address 10.1.1.2 255.255.255.0
```

创建备份组 1，并配置备份组 1 的虚拟 IP 地址为 10.1.1.111。

```
[DeviceB-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.111
```

设置 Device B 在备份组 1 中的优先级为 100。

```
[DeviceB-Vlan-interface2] vrrp vrid 1 priority 100
```

1.5 验证配置

配置完成后，在 Host A 上可以 ping 通 Host B。

通过 **display vrrp verbose** 命令查看配置后的结果，显示 Device A 上 VRRP 备份组 1 的详细信息。

```
[DeviceA-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
 Running mode : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                  Adver Timer   : 100
     Admin Status   : Up                 State         : Master
     Config Pri     : 110                Running Pri   : 110
     Preempt Mode   : Yes                Delay Time    : 5000
     Auth Type      : Not supported
     Version          : 3
     Virtual IP       : 10.1.1.111
     Virtual MAC      : 0000-5e00-0101
     Master IP        : 10.1.1.1
   VRRP Track Information:
     Track Object   : 1                  State : Positive   Pri Reduced : 50
```

通过 **display vrrp verbose** 命令查看配置后的结果，显示 Device B 上 VRRP 备份组 1 的详细信息。

```
[DeviceB-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
 Running mode : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                  Adver Timer   : 100
     Admin Status   : Up                 State         : Backup
     Config Pri     : 100                Running Pri   : 100
     Preempt Mode   : Yes                Delay Time    : 0
     Become Master  : 401ms left
     Auth Type        : Not supported
     Version          : 3
     Virtual IP       : 10.1.1.111
     Master IP        : 10.1.1.1
```

以上显示信息表示在 VRRP 备份组 1 中 Device A 为 Master，Device B 为 Backup，Host A 发送给 Host B 的报文通过 Device A 转发。

Device A 出现故障后，在 Host A 上仍然可以 ping 通 Host B。

通过 **display vrrp verbose** 命令查看 Device B 上 VRRP 备份组的详细信息，Device A 出现故障后，显示 Device B 上 VRRP 备份组 1 的详细信息。

```
[DeviceB-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode : Standard
 Total number of virtual routers : 1
```

```
  Interface Vlan-interface2
    VRID           : 1                    Adver Timer   : 100
    Admin Status   : Up                   State         : Master
    Config Pri     : 100                  Running Pri   : 100
    Preempt Mode   : Yes                  Delay Time    : 0
    Auth Type        : Not supported
    Version          : 3
    Virtual IP       : 10.1.1.111
    Master IP        : 10.1.1.2
```

以上显示信息表示 Device A 出现故障后，Device B 成为 Master，Host A 发送给 Host B 的报文通过 Device B 转发。

Device A 故障恢复后，显示 Device A 上 VRRP 备份组 1 的详细信息。

```
[DeviceA-Vlan-interface2] display vrrp verbose
IPv4 Virtual Router Information:
 Running Mode      : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface2
     VRID           : 1                    Adver Timer   : 100
     Admin Status   : Up                   State         : Master
     Config Pri     : 110                  Running Pri   : 110
     Preempt Mode   : Yes                  Delay Time    : 5000
     Auth Type      : Not supported
     Version          : 3
     Virtual IP       : 10.1.1.111
     Virtual MAC      : 0000-5e00-0101
     Master IP        : 10.1.1.1
   VRRP Track Information:
     Track Object   : 1                  State : Positive   Pri Reduced : 50
```

以上显示信息表示 Device A 故障恢复后，Device A 会抢占成为 Master，Host A 发送给 Host B 的报文仍然通过 Device A 转发。

1.6 配置文件

- Device A：

```
#
vlan 2
#
interface Vlan-interface2
 ip address 10.1.1.1 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.111
 vrrp vrid 1 priority 110
 vrrp vrid 1 preempt-mode delay 5000
 vrrp vrid 1 track 1 priority reduced 50
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2
#
```

```
 track 1 interface Ten-GigabitEthernet1/0/2
#
```

- Device B 的配置文件：

```
#
vlan 2
#
interface Vlan-interface2
 ip address 10.1.1.2 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.111
 vrrp vrid 1 priority 100
#
interface Ten-GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2
#
```

1.7 相关资料

- 产品配套“可靠性配置指导”中的“VRRP”。
- 产品配套“可靠性命令参考”中的“VRRP”。

PoE 快速配置指南

目 录

1 PoE 基本组网配置

1.1 简介

本案例介绍设备通过 PoE 接口为 PD 设备供电的配置方法。

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。

不能通过重复执行 **apply poe-profile** 或 **apply poe-profile interface** 命令修改 PoE Profile。如需修改 PoE Profile，请先取消 PoE profile 在 PoE 接口的应用，修改 PoE Profile 后，再将 PoE profile 应用到 PoE 接口。

1.3 配置步骤

1. 开启单个 PoE 接口远程供电功能

进入系统视图。

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

开启 GigabitEthernet 1/0/1 接口的 PoE 接口远程供电功能。

```
[Device] interface GigabitEthernet 1/0/1
[Device-GigabitEthernet1/0/1] poe enable
[Device-GigabitEthernet1/0/1] quit
```

#保存配置

```
[Device] save force
```

2. 批量开启 GigabitEthernet1/0/1 到 GigabitEthernet1/0/6 接口的远程供电功能。

创建名称为 abc 的 PoE profile，指定索引为 1。

```
<Device> system-view
[Device] poe-profile abc 1
```

开启 PoE 接口远程供电功能

```
[Device-poe-profile-abc-1] poe enable
[Device-poe-profile-abc-1] return
```

将索引为 1 的 PoE profile 应用到 PoE 接口 GigabitEthernet1/0/1 至 GigabitEthernet1/0/6。

```
<Device> system-view
[Device] apply poe-profile abc index 1 interface gigabitethernet 1/0/1 to gigabitethernet
1/0/6
```

#保存配置

```
[Device] save force
```

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。

1.5 配置文件

- 开启单个 PoE 接口远程供电功能

```
#
interface GigabitEthernet 1/0/1
poe enable
#
```

- 批量开启 PoE 接口远程供电功能

```
#
 poe-profile abc 1
 poe enable
 apply poe-profile index 1
 save force
 #
```

1.6 相关资料

- 产品配套“网络管理和监控配置指导”中的“PoE”。
- 产品配套“网络管理和监控命令参考”中的“PoE”。

镜像快速配置指南

目 录

1 本地端口镜像

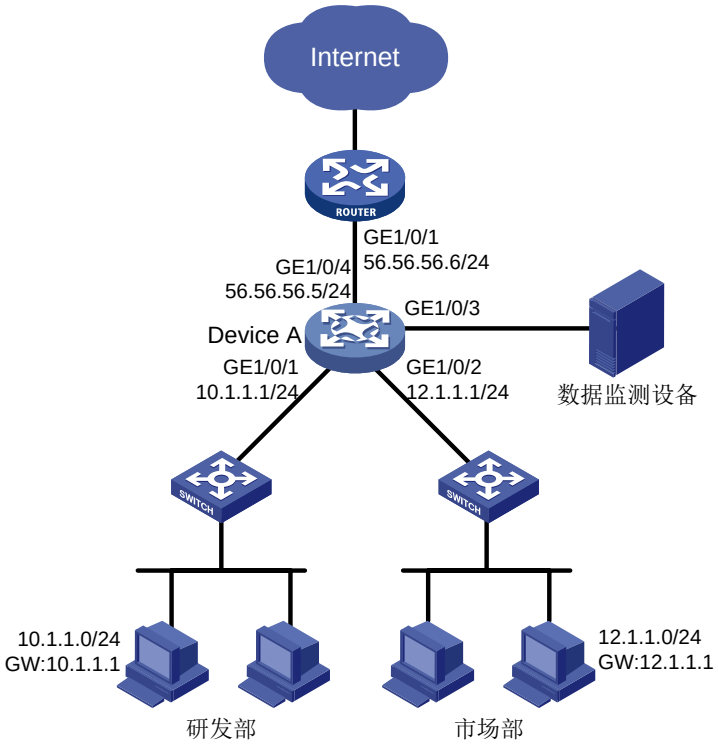
1.1 简介

本案例介绍本地端口镜像的配置方法。

1.2 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 的流量以及两个部门之间互访的流量进行监控。

图1 本地端口镜像配置组网图



1.3 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。

1.4 配置步骤

配置 GigabitEthernet1/0/1 接口 IP 地址为 10.1.1.1/24，连接研发部设备。

```
<DeviceA> system-view
```

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-mode route
[DeviceA-GigabitEthernet1/0/1] ip address 10.1.1.1 24
[DeviceA-GigabitEthernet1/0/1] quit
```

配置 GigabitEthernet1/0/2 接口 IP 地址为 12.1.1.1/24，连接市场部设备。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-mode route
[DeviceA-GigabitEthernet1/0/2] ip address 12.1.1.1 24
[DeviceA-GigabitEthernet1/0/2] quit
```

配置 GigabitEthernet1/0/4 接口 IP 地址为 56.56.56.5/24。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/4
[DeviceA-GigabitEthernet1/0/4] port link-mode route
[DeviceA-GigabitEthernet1/0/4] ip address 56.56.56.5 24
[DeviceA-GigabitEthernet1/0/4] quit
```

创建本地镜像组。

```
[DeviceA] mirroring-group 1 local
```

将 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 配置为镜像源端口，对这两个端口接收的报文进行镜像。

```
[DeviceA] mirroring-group 1 mirroring-port gigabitethernet 1/0/1 gigabitethernet 1/0/2
inbound
```

将 GigabitEthernet1/0/3 配置为镜像目的端口。

```
[DeviceA] mirroring-group 1 monitor-port gigabitethernet 1/0/3
```

关闭目的端口 GigabitEthernet1/0/3 上的生成树协议。

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] undo stp enable
[DeviceA-GigabitEthernet1/0/3] quit
```

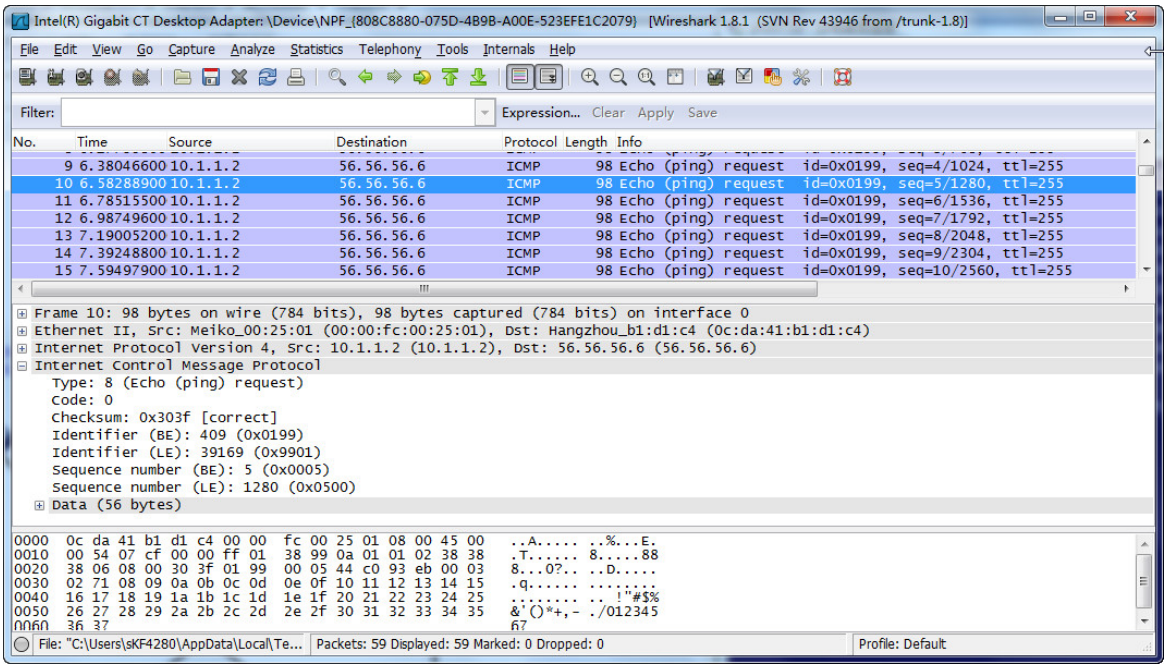
1.5 验证配置

在完成上述配置后，在 Device A 上显示镜像组 1 的配置信息。

```
[DeviceA] display mirroring-group 1
Mirroring group 1:
    Type: Local
    Status: Active
    Mirroring port:
        GigabitEthernet1/0/1  Inbound
        GigabitEthernet1/0/2  Inbound
    Monitor port: GigabitEthernet1/0/3
```

以研发部某台主机 10.1.1.2 通过 ping 方式访问 56.56.56.6 为例，进行镜像测试，数据监测设备的抓包数据如图 2 所示。本例以 Wireshark 网络封包分析软件的显示为例。

图2 Wireshark 的抓包数据



以上抓包信息表明，配置的本地镜像功能生效，数据监测设备可以成功对需要监控的流量进行监控。

1.6 配置文件

```
#
 mirroring-group 1 local
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 10.1.1.1 255.255.255.0
 mirroring-group 1 mirroring-port inbound
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 12.1.1.1 255.255.255.0
 mirroring-group 1 mirroring-port inbound
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 undo stp enable
 mirroring-group 1 monitor-port
#
interface GigabitEthernet1/0/4
 port link-mode route
 ip address 56.56.56.5 255.255.255.0
#
```

1.7 相关资料

- 产品配套“网络管理和监控配置指导”中的“镜像”。
- 产品配套“网络管理和监控命令参考”中的“镜像”。

2 本地端口镜像（1：1）快速配置指南

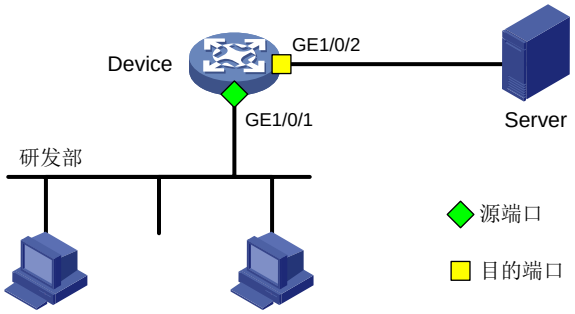
2.1 简介

本案例介绍 1:1 本地端口镜像的配置方法。1:1 镜像是指将单个镜像端口的报文复制到单个观察端口。

2.2 组网需求

研发部使用 GigabitEthernet1/0/1 端口接入 Device，现要求通过镜像功能，使数据检测设备 Server 能够对研发部发送和接收的报文进行镜像。

图3 1:1 本地端口镜像配置组网图



2.3 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。

2.4 配置步骤

创建本地镜像组 1。

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

配置本地镜像组 1 的源端口为 GigabitEthernet1/0/1，对源端口收发的报文进行镜像，目的端口为 GigabitEthernet1/0/2。

```
[Device] mirroring-group 1 mirroring-port gigabitethernet 1/0/1 both
[Device] mirroring-group 1 monitor-port gigabitethernet 1/0/2
```

在目的端口 GigabitEthernet1/0/2 上关闭生成树协议。

```
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] undo stp enable
[Device-GigabitEthernet1/0/2] quit
```

2.5 验证配置

显示所有镜像组的配置信息。

```
<Device> display mirroring-group all
Mirroring group 1:
    Type: Local
    Status: Active
    Mirroring port:
        GigabitEthernet1/0/1  Both
    Monitor port: GigabitEthernet1/0/2
```

配置完成后，用户可以通过 Server 监控所有进、出研发部的报文。

2.6 配置文件

```
#
 mirroring-group 1 local
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 mirroring-group 1 mirroring-port both
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 undo stp enable
 mirroring-group 1 monitor-port
#
```

2.7 相关资料

- 产品配套“网络管理和监控配置指导”中的“镜像”。
- 产品配套“网络管理和监控命令参考”中的“镜像”。

3 本地端口镜像（1：N）快速配置指南

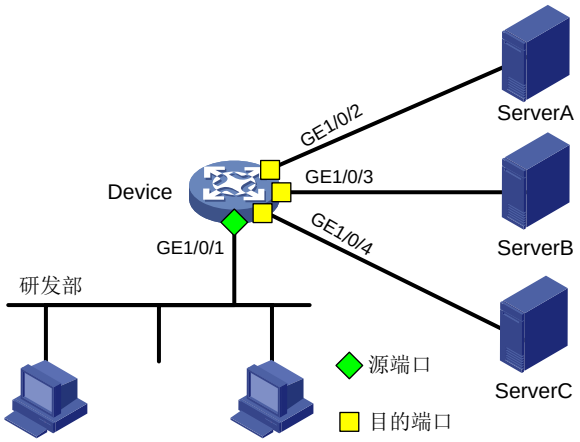
3.1 简介

本案例介绍 1:N 本地端口镜像的配置方法。1:N 镜像是指将单个镜像端口的报文复制到 N 个不同的观察端口。

3.2 组网需求

研发部使用 GigabitEthernet1/0/1 端口接入 Device，现要求通过镜像功能，使不同的数据检测设备 ServerA、ServerB、ServerC 能够对分别研发部发送和接收的报文进行监控分析。

图4 1:N 本地端口镜像配置组网图



3.3 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。

3.4 配置步骤

创建本地镜像组 1。

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

配置本地镜像组 1 的源端口为 GigabitEthernet1/0/1，对源端口收发的报文进行镜像，目的端口为 GigabitEthernet1/0/2、GigabitEthernet1/0/3、GigabitEthernet1/0/4。

```
[Device] mirroring-group 1 mirroring-port gigabitethernet 1/0/1 both
[Device] mirroring-group 1 monitor-port gigabitethernet 1/0/2 to gigabitethernet 1/0/4
```

在目的端口 GigabitEthernet1/0/2、GigabitEthernet1/0/3、GigabitEthernet1/0/4 上关闭生成树协议。

```
[Device] interface gigabitethernet 1/0/2
```

```
[Device-GigabitEthernet1/0/2] undo stp enable
[Device-GigabitEthernet1/0/2] quit
[Device] interface gigabitethernet 1/0/3
[Device-GigabitEthernet1/0/3] undo stp enable
[Device-GigabitEthernet1/0/3] quit
[Device] interface gigabitethernet 1/0/4
[Device-GigabitEthernet1/0/4] undo stp enable
[Device-GigabitEthernet1/0/4] quit
```

3.5 验证配置

显示所有镜像组的配置信息。

```
<Device> display mirroring-group all
Mirroring group 1:
    Type: Local
    Status: Active
    Mirroring port:
        GigabitEthernet1/0/1  Both
    Monitor port: GigabitEthernet1/0/2
                  GigabitEthernet1/0/3
                  GigabitEthernet1/0/4
```

配置完成后，用户可以通过 ServerA、ServerB、ServerC 分别监控所有进、出研发部的报文。

3.6 配置文件

```
#
 mirroring-group 1 local
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 mirroring-group 1 mirroring-port both
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 undo stp enable
 mirroring-group 1 monitor-port
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 undo stp enable
 mirroring-group 1 monitor-port
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 undo stp enable
 mirroring-group 1 monitor-port
#
```

3.7 相关资料

- 产品配套“网络管理和监控配置指导”中的“镜像”。
- 产品配套“网络管理和监控命令参考”中的“镜像”。

4 本地端口镜像（M：N）快速配置指南

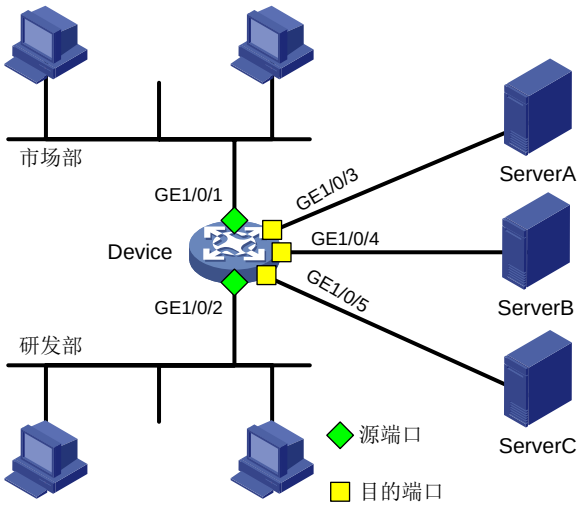
4.1 简介

本案例介绍 M:N 本地端口镜像的配置方法。M:N 镜像是指将 M 个镜像端口的报文复制到 N 个不同的观察端口。

4.2 组网需求

市场部和研发部分别使用 GigabitEthernet1/0/1、GigabitEthernet1/0/2 端口接入 Device，现要求通过镜像功能，使不同的数据检测设备 ServerA、ServerB、ServerC 能够对分别市场部、研发部发送和接收的报文进行监控分析。

图5 M:N 本地端口镜像配置组网图



4.3 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。

4.4 配置步骤

创建本地镜像组 1。

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

配置本地镜像组 1 的源端口为 GigabitEthernet1/0/1、GigabitEthernet1/0/2，对源端口收发的报文进行镜像，目的端口为 GigabitEthernet1/0/3、GigabitEthernet1/0/4、GigabitEthernet1/0/5。

```
[Device] mirroring-group 1 mirroring-port gigabitethernet 1/0/1 gigabitethernet 1/0/2 both
[Device] mirroring-group 1 monitor-port gigabitethernet 1/0/3 to gigabitethernet 1/0/5
```

在目的端口 GigabitEthernet1/0/3、GigabitEthernet1/0/4、GigabitEthernet1/0/5 上关闭生成树协议。

```
[Device] interface gigabitethernet 1/0/3
[Device-GigabitEthernet1/0/3] undo stp enable
[Device-GigabitEthernet1/0/3] quit
[Device] interface gigabitethernet 1/0/4
[Device-GigabitEthernet1/0/4] undo stp enable
[Device-GigabitEthernet1/0/4] quit
[Device] interface gigabitethernet 1/0/5
[Device-GigabitEthernet1/0/5] undo stp enable
[Device-GigabitEthernet1/0/5] quit
```

4.5 验证配置

显示所有镜像组的配置信息。

```
<Device> 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
                  GigabitEthernet1/0/4
                  GigabitEthernet1/0/5
```

配置完成后，用户可以通过 ServerA、ServerB、ServerC 分别监控所有进、出市场部和研发部的报文。

4.6 配置文件

```
#
 mirroring-group 1 local
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 mirroring-group 1 mirroring-port both
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 mirroring-group 1 mirroring-port both
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 undo stp enable
 mirroring-group 1 monitor-port
#
interface GigabitEthernet1/0/4
 port link-mode bridge
```

```
 undo stp enable
 mirroring-group 1 monitor-port
#
interface GigabitEthernet1/0/5
 port link-mode bridge
 undo stp enable
 mirroring-group 1 monitor-port
#
```

4.7 相关资料

- 产品配套“网络管理和监控配置指导”中的“镜像”。
- 产品配套“网络管理和监控命令参考”中的“镜像”。

5 利用远程镜像 VLAN 实现本地镜像支持多目的端口配置

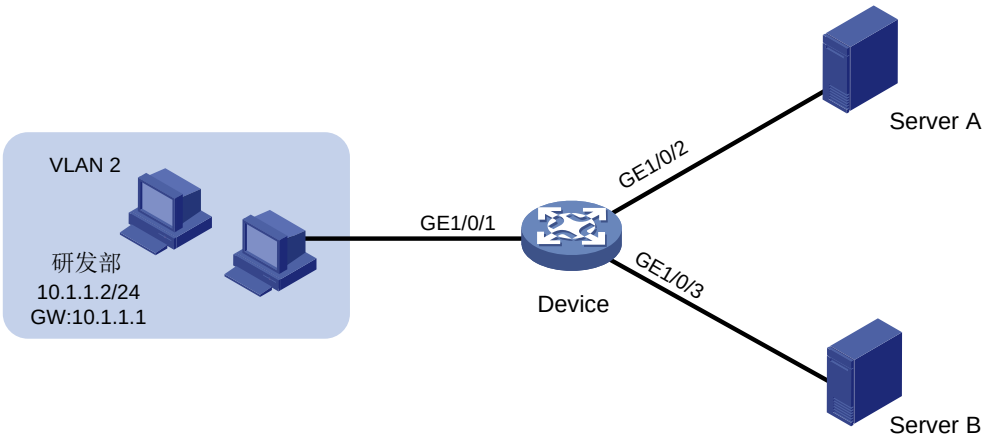
5.1 简介

本案例介绍利用远程镜像 VLAN 实现本地镜像支持多目的端口配置方法。

5.2 组网需求

研发部使用 GigabitEthernet1/0/1 端口接入 Device，现要求通过镜像功能，使数据检测设备 ServerA 和 ServerB 都能够对研发部发送和接收的报文进行镜像。

图6 利用远程镜像 VLAN 实现本地镜像支持多目的端口组网图



5.3 配置注意事项

当一个 VLAN 已被指定为远程镜像 VLAN 后，请不要将该 VLAN 再作其他用途。

只能将已存在的静态 VLAN 配置为远程镜像 VLAN，且一个 VLAN 只能配置为一个镜像组的远程镜像 VLAN。

当某 VLAN 被配置为远程镜像 VLAN 后，必须先删除远程镜像 VLAN 的配置才能删除该 VLAN。

5.4 配置步骤

创建业务 VLAN2。

```
<Device> system-view
[Device] vlan 2
[Device-vlan2] quit
```

创建 VLAN 2 接口并配置 IP 地址。

```
[Device] interface vlan-interface 2
[Device-Vlan-interface2] ip address 10.1.1.1 24
[Device-Vlan-interface2] quit
```

创建 VLAN 10 作为远程镜像 VLAN。

```
[Device] vlan 10
```

```
[Device-vlan10] quit
```
配置端口 GigabitEthernet1/0/1 的端口类型为 Trunk 端口，允许业务 VLAN 2 的报文通过。
```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] port link-type trunk
[Device-GigabitEthernet1/0/1] port trunk permit vlan 2
[Device-GigabitEthernet1/0/1] quit
```
创建远程源镜像组 1。
```
<Device> system-view
[Device] mirroring-group 1 remote-source
```
将接入研发部的端口 GigabitEthernet1/0/1 配置为远程源镜像组 1 的源端口。
```
[Device] mirroring-group 1 mirroring-port gigabitethernet1/0/1 both
```
将设备上任意未使用的端口（此处以 GigabitEthernet1/0/4 为例）配置为镜像组 1 的反射口。
```
[Device] mirroring-group 1 reflector-port gigabitethernet1/0/4
This operation may delete all settings made on the interface. Continue? [Y/N]:y
```
将接入数据检测设备的端口加入 VLAN10。
```
[Device] vlan 10
[Device-vlan10] port gigabitethernet1/0/2 to gigabitethernet1/0/3
[Device-vlan10] quit
```
配置 VLAN10 作为镜像组 1 的远程镜像 VLAN。
```
[Device] mirroring-group 1 remote-probe vlan 10
```

5.5 验证配置

在完成上述配置后，在 Device 上显示镜像组 1 的配置信息。
```
[DeviceA] display mirroring-group all
Mirroring group 1:
    Type: Remote source
    Status: Active
    Mirroring port:
        GigabitEthernet1/0/1  Both
    Reflector port: GigabitEthernet1/0/4
    Remote probe VLAN: 10
```

5.6 配置文件

```
#
 mirroring-group 1 remote-source
 mirroring-group 1 remote-probe vlan 10
#
vlan 2
#
vlan 10
#
interface Vlan-interface2
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
```

```
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 2
 mirroring-group 1 mirroring-port inbound
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 10
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 10
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port access vlan 10
 mirroring-group 1 reflector-port
#
```

5.7 相关资料

- 产品配套“网络管理和监控配置指导”中的“镜像”。
- 产品配套“网络管理和监控命令参考”中的“镜像”。

6 出端口方式二层远程端口镜像

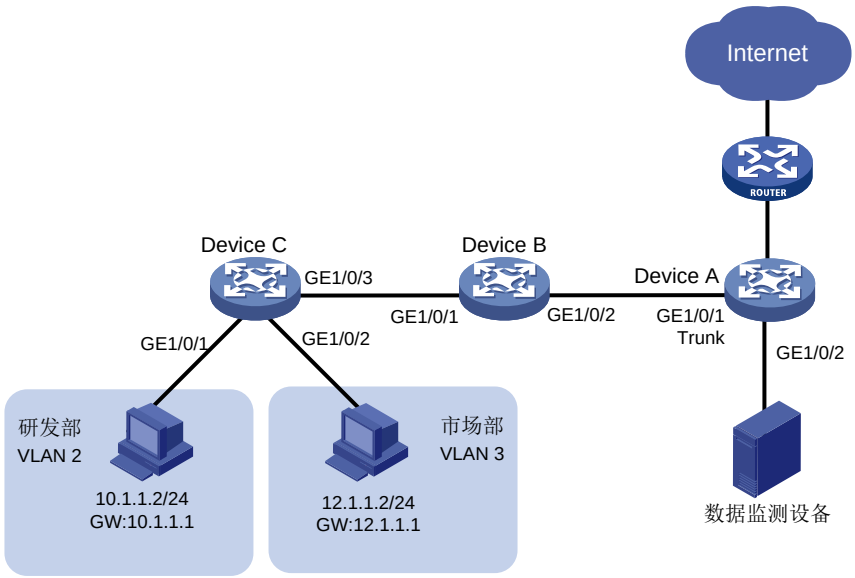
6.1 简介

本案例介绍出端口方式二层远程端口镜像的配置方法。

6.2 组网需求

某公司内部各部门通过二层网络连接到核心设备 Device A，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7 出端口方式二层远程端口镜像组网图



6.3 配置注意事项

- 为确保源设备与目的设备之间的镜像报文可以二层转发，中间设备连接到源设备和目的设备方向的端口上需允许远程镜像 VLAN 通过。
- 建议用户先配目的设备，再配中间设备，最后配源设备，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。
- 一个镜像组内只能配置一个出端口。
- 源端口为三层接口时，只能通过配置出端口方式实现二层远程镜像。

6.4 配置步骤

1. Device A 的配置（目的设备）

创建业务 VLAN 2 和 VLAN 3。

```
<DeviceA> system-view
[DeviceA] vlan 2 to 3
```

创建 VLAN 5 作为远程镜像 VLAN。

```
[DeviceA] vlan 5
[DeviceA-vlan5] quit
```

创建 VLAN 2 接口和 VLAN 3 接口并配置 IP 地址作为相应 VLAN 的网关。

```
[DeviceA] interface vlan-interface 2
[DeviceA-Vlan-interface2] ip address 10.1.1.1 24
[DeviceA-Vlan-interface2] quit
[DeviceA] interface vlan-interface 3
[DeviceA-Vlan-interface3] ip address 12.1.1.1 24
[DeviceA-Vlan-interface3] quit
```

配置端口 GigabitEthernet1/0/1 的端口类型为 Trunk 端口，允许业务 VLAN 2、VLAN 3 和镜像 VLAN 5 的报文通过。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 2 3 5
[DeviceA-GigabitEthernet1/0/1] quit
```

创建远程目的镜像组 1。

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

为远程目的镜像组 1 配置远程镜像 VLAN 为 VLAN 5，及配置连接数据监测设备的端口 GigabitEthernet1/0/2 为目的端口。

```
[DeviceA] mirroring-group 1 remote-probe vlan 5
[DeviceA] mirroring-group 1 monitor-port gigabitethernet 1/0/2
```

将镜像目的端口加入远程镜像 VLAN。将镜像数据发送给监测设备时，不需要携带远程镜像 VLAN 的 VLAN Tag，因此将该端口配置为 Access 端口。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port access vlan 5
```

关闭目的端口 GigabitEthernet1/0/2 上的生成树协议。

```
[DeviceA-GigabitEthernet1/0/2] undo stp enable
[DeviceA-GigabitEthernet1/0/2] quit
```

2. Device B 的配置（中间设备）

创建业务 VLAN 2 和 VLAN 3。

```
<DeviceB> system-view
[DeviceB] vlan 2 to 3
```

创建 VLAN 5 作为远程镜像 VLAN。

```
[DeviceB] vlan 5
[DeviceB-vlan5] quit
```

配置端口 GigabitEthernet1/0/1 的端口类型为 Trunk 端口，允许业务 VLAN 2、VLAN 3 和镜像 VLAN 5 的报文通过。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 2 3 5
[DeviceB-GigabitEthernet1/0/1] quit
```

配置端口 GigabitEthernet1/0/2 的端口类型为 Trunk 端口，允许业务 VLAN 2、VLAN 3 和镜像 VLAN 5 的报文通过。

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 2 3 5
[DeviceB-GigabitEthernet1/0/2] quit
```

3. Device C 的配置（源设备）

创建业务 VLAN 2 和 VLAN 3。

```
<DeviceC> system-view
[DeviceC] vlan 2 to 3
```

将端口 GigabitEthernet1/0/1 加入 VLAN 2。

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] port access vlan 2
[DeviceC-GigabitEthernet1/0/1] quit
```

将端口 GigabitEthernet1/0/2 加入 VLAN 3。

```
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] port access vlan 3
[DeviceC-GigabitEthernet1/0/2] quit
```

创建远程源镜像组 1。

```
[DeviceC] mirroring-group 1 remote-source
```

创建 VLAN 5 作为远程镜像 VLAN。

```
[DeviceC] vlan 5
[DeviceC-vlan5] quit
```

配置远程源镜像组 1 的远程镜像 VLAN 为 VLAN 5，源端口为 GigabitEthernet1/0/1，出端口为 GigabitEthernet1/0/3。

```
[DeviceC] mirroring-group 1 remote-probe vlan 5
[DeviceC] mirroring-group 1 mirroring-port gigabitethernet 1/0/1 inbound
[DeviceC] mirroring-group 1 monitor-egress gigabitethernet 1/0/3
```

配置端口 GigabitEthernet1/0/3 的端口类型为 Trunk 端口，允许业务 VLAN 2、VLAN 3 和镜像 VLAN 5 的报文通过。

```
[DeviceC] interface gigabitethernet 1/0/3
```

```
[DeviceC-GigabitEthernet1/0/3] port link-type trunk
[DeviceC-GigabitEthernet1/0/3] port trunk permit vlan 2 3 5
[DeviceC-GigabitEthernet1/0/3] quit
```

关闭出端口 GigabitEthernet1/0/3 上的生成树协议。

```
[DeviceC-GigabitEthernet1/0/3] undo stp enable
[DeviceC-GigabitEthernet1/0/3] quit
```

6.5 验证配置

在完成上述配置后，在 DeviceC 上显示镜像组 1 的配置信息。

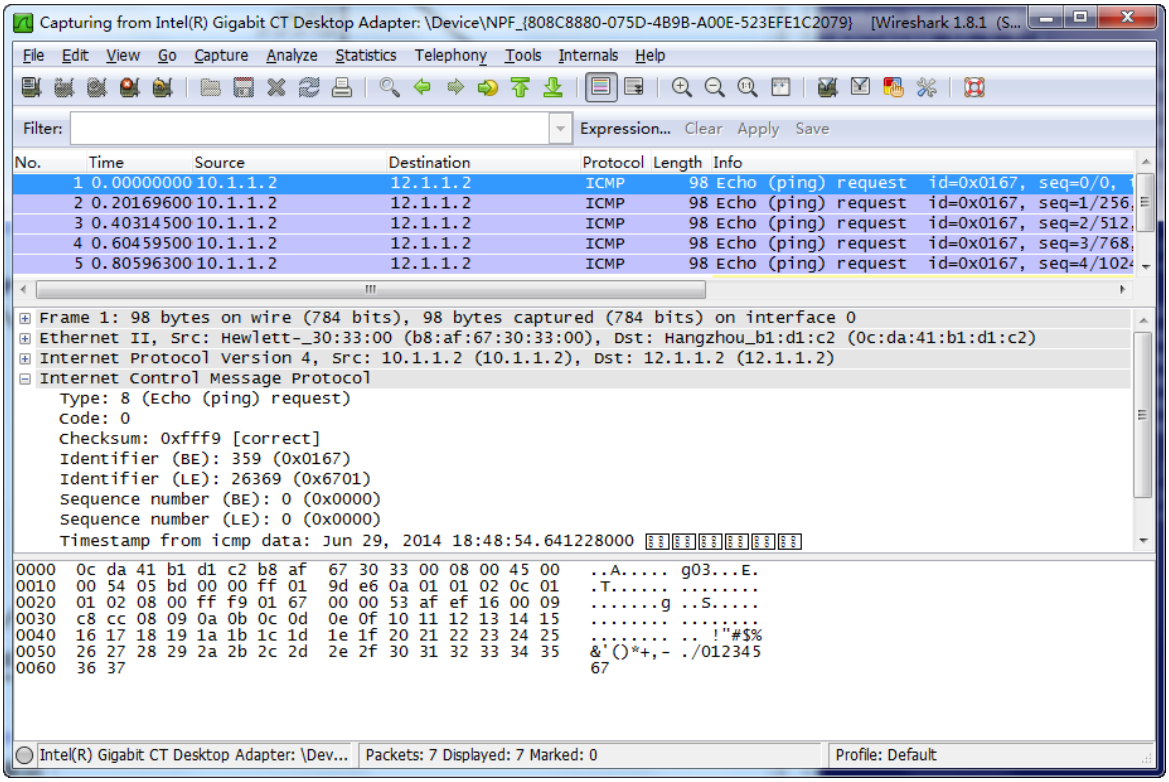
```
[DeviceC] display mirroring-group 1
Mirroring group 1:
    Type: Remote source
    Status: Active
    Mirroring port:
        GigabitEthernet1/0/1  Inbound
    Monitor egress port: GigabitEthernet1/0/3
        Remote probe VLAN: 5
```

在 DeviceA 上显示镜像组 1 的配置信息。

```
[DeviceA] display mirroring-group 1
Mirroring group 1:
    Type: Remote destination
    Status: Active
    Monitor port: GigabitEthernet1/0/2
    Remote probe VLAN: 5
```

以研发部某台主机 10.1.1.2 通过 ping 方式访问市场部某台主机 12.1.1.2 为例，进行镜像测试，数据监测设备的抓包数据如图 8 所示。本例以 Wireshark 网络封包分析软件的显示为例。

图8 Wireshark 的抓包数据



以上抓包信息表明，配置的二层远程端口镜像功能生效，数据监测设备可以成功对对研发部发送的报文进行监控。

6.6 配置文件

- 设备 Device A：

```
#
 mirroring-group 1 remote-destination
 mirroring-group 1 remote-probe vlan 5
#
vlan 2 to 3
#
vlan 5
#
interface Vlan-interface2
 ip address 10.1.1.1 255.255.255.0
#
interface Vlan-interface3
 ip address 12.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 3 5
```

```
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 5
 undo stp enable
 mirroring-group 1 monitor-port
#
```

- 设备 Device B：

```
#
vlan 2 to 3
#
vlan 5
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 3 5
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 3 5
#
```

- 设备 Device C：

```
#
 mirroring-group 1 remote-source
 mirroring-group 1 remote-probe vlan 5
#
vlan 2 to 3
#
vlan 5
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2
 mirroring-group 1 mirroring-port inbound
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 3
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 3 5
 mirroring-group 1 monitor-egress
#
```

6.7 相关资料

- 产品配套“网络管理和监控配置指导”中的“镜像”。
- 产品配套“网络管理和监控命令参考”中的“镜像”。

7 反射端口方式二层远程端口镜像

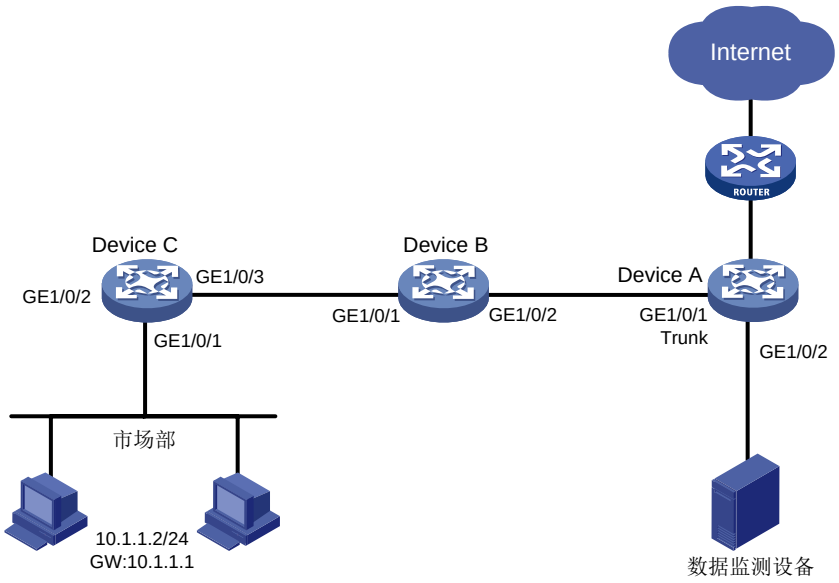
7.1 简介

本案例介绍反射端口方式二层远程端口镜像的配置方法。

7.2 组网需求

某公司市场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。现要求通过配置反射端口方式二层远程端口镜像功能，使用数据监测设备对市场部发送的报文进行监控。

图9 反射端口方式二层远程端口镜像组网图



7.3 配置注意事项

- 为确保源设备与目的设备之间的镜像报文可以二层转发，中间设备连接到源设备和目的设备方向的端口上需允许远程镜像 VLAN 通过。
- 建议用户先配目的设备，再配中间设备，最后配源设备，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。
- 建议选择设备上未被使用的端口作为反射端口，并不要在该端口上连接网线，否则会影响镜像功能的正常使用。
- 在将端口配置为反射端口时，该端口上已存在的所有配置都将被清除；在配置为反射端口后，该端口上不能再配置其他业务。
- 当 IRF 端口只绑定了一个物理端口时，请勿将该物理端口配置为反射端口，以免 IRF 分裂。

7.4 配置步骤

1. Device A 的配置（目的设备）

创建业务 VLAN 2。

```
<DeviceA> system-view
[DeviceA] vlan 2
```

创建 VLAN 5 作为远程镜像 VLAN。

```
[DeviceA] vlan 5
[DeviceA-vlan5] quit
```

创建 VLAN 2 接口并配置 IP 地址作为相应 VLAN 的网关。

```
[DeviceA] interface vlan-interface 2
[DeviceA-Vlan-interface2] ip address 10.1.1.1 24
[DeviceA-Vlan-interface2] quit
```

配置端口 GigabitEthernet1/0/1 的端口类型为 Trunk 端口，允许业务 VLAN 2 和镜像 VLAN 5 的报文通过。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-type trunk
[DeviceA-GigabitEthernet1/0/1] port trunk permit vlan 2 5
[DeviceA-GigabitEthernet1/0/1] quit
```

创建远程目的镜像组 1。

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

为远程目的镜像组 1 配置远程镜像 VLAN 为 VLAN 5，及配置连接数据监测设备的端口 GigabitEthernet1/0/2 为目的端口。

```
[DeviceA] mirroring-group 1 remote-probe vlan 5
[DeviceA] mirroring-group 1 monitor-port gigabitethernet 1/0/2
```

将镜像目的端口加入远程镜像 VLAN。将镜像数据发送给监测设备时，不需要携带远程镜像 VLAN 的 VLAN Tag，因此将该端口配置为 Access 端口。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port access vlan 5
```

关闭目的端口 GigabitEthernet1/0/2 上的生成树协议。

```
[DeviceA-GigabitEthernet1/0/2] undo stp enable
[DeviceA-GigabitEthernet1/0/2] quit
```

2. Device B 的配置（中间设备）

创建业务 VLAN 2。

```
<DeviceB> system-view
[DeviceB] vlan 2
```
创建 VLAN 5 作为远程镜像 VLAN。
```
[DeviceB] vlan 5
[DeviceB-vlan5] quit
```
配置端口 GigabitEthernet1/0/1 的端口类型为 Trunk 端口，允许业务 VLAN 2 和镜像 VLAN 5 的报文通过。
```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type trunk
[DeviceB-GigabitEthernet1/0/1] port trunk permit vlan 2 5
[DeviceB-GigabitEthernet1/0/1] quit
```
配置端口 GigabitEthernet1/0/2 的端口类型为 Trunk 端口，允许业务 VLAN 2 和镜像 VLAN 5 的报文通过。
```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type trunk
[DeviceB-GigabitEthernet1/0/2] port trunk permit vlan 2 5
[DeviceB-GigabitEthernet1/0/2] quit
```
3. Device C 的配置（源设备）
创建业务 VLAN 2。
```
<DeviceC> system-view
[DeviceC] vlan 2
```
将端口 GigabitEthernet1/0/1 加入 VLAN 2。
```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] port access vlan 2
[DeviceC-GigabitEthernet1/0/1] quit
```
创建远程源镜像组 1。
```
[DeviceC] mirroring-group 1 remote-source
```
创建 VLAN 5 作为远程镜像 VLAN。
```
[DeviceC] vlan 5
[DeviceC-vlan5] quit
```
配置远程源镜像组 1 的远程镜像 VLAN 为 VLAN 5，源端口为 GigabitEthernet1/0/1，反射端口为 GigabitEthernet1/0/2。
```
[DeviceC] mirroring-group 1 remote-probe vlan 5
[DeviceC] mirroring-group 1 mirroring-port gigabitethernet 1/0/1 inbound
[DeviceC] mirroring-group 1 reflector-port gigabitethernet 1/0/2
```
配置端口 GigabitEthernet1/0/3 为 Trunk 口，并允许业务 VLAN 2 和镜像 VLAN 5 的报文通过。
```
[DeviceC] interface gigabitethernet 1/0/3
[DeviceC-GigabitEthernet1/0/3] port link-type trunk
[DeviceC-GigabitEthernet1/0/3] port trunk permit vlan 2
[DeviceC-GigabitEthernet1/0/3] quit
```
7.5 验证配置
显示 Device A 上所有镜像组的配置信息。
```
[DeviceA] display mirroring-group all
```

```
Mirroring group 1:
    Type: Remote destination
    Status: Active
    Monitor port: GigabitEthernet1/0/2
    Remote probe VLAN: 5
```

显示 Device C 上所有镜像组的配置信息。

```
[DeviceC] display mirroring-group all
Mirroring group 1:
    Type: Remote source
    Status: Active
    Mirroring port:
        GigabitEthernet1/0/1  inbound
    Reflector port: GigabitEthernet1/0/2
    Remote probe VLAN: 5
```

7.6 配置文件

- 设备 Device A：

```
#
 mirroring-group 1 remote-destination
 mirroring-group 1 remote-probe vlan 5
#
vlan 2
#
vlan 5
#
interface Vlan-interface2
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 2 5
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 5
 undo stp enable
 mirroring-group 1 monitor-port
#
```

- 设备 Device B：

```
#
vlan 2
#
vlan 5
#
interface GigabitEthernet1/0/1
```

```
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 2 5
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 1 to 2 5
#
```

- 设备 Device C：

```
#
 mirroring-group 1 remote-source
 mirroring-group 1 remote-probe vlan 5
#
vlan 2
#
vlan 5
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 2
 mirroring-group 1 mirroring-port inbound
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 mirroring-group 1 reflector-port
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 2 5
#
```

7.7 相关资料

- 产品配套“网络管理和监控配置指导”中的“镜像”。
- 产品配套“网络管理和监控命令参考”中的“镜像”。

8 配置封装参数方式三层远程端口镜像

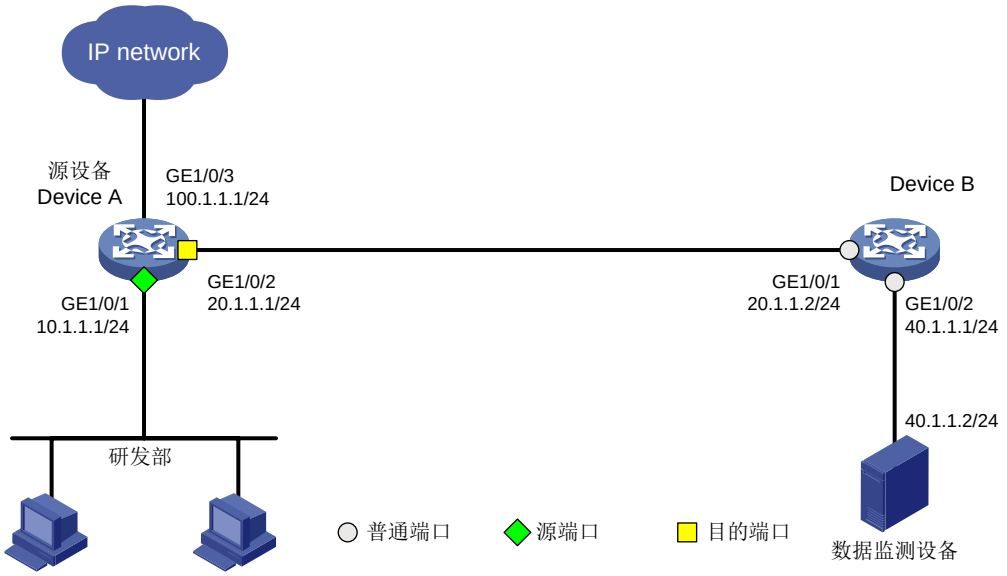
8.1 简介

本案例介绍配置封装参数方式三层远程端口镜像的配置方法。

8.2 组网需求

某公司研发部使用 10.1.1.1/24 网段。现要求通过配置三层远程端口镜像功能，使用数据监测设备对研发部访问 Internet 的报文进行监控。

图10 三层远程端口镜像组网图



8.3 配置注意事项

如果源设备和目的设备之间存在中间设备，则需要在中间设备上配置单播路由协议，以确保源设备与目的设备之间的三层网络畅通。

8.4 配置步骤

1. Device A 的配置

配置接口 GigabitEthernet1/0/1 的 IP 地址为 10.1.1.1。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-mode route
[DeviceA-GigabitEthernet1/0/1] ip address 10.1.1.1 24
[DeviceA-GigabitEthernet1/0/1] quit
```

配置接口 GigabitEthernet1/0/2 的 IP 地址为 20.1.1.1。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-mode route
[DeviceA-GigabitEthernet1/0/2] ip address 20.1.1.1 24
[DeviceA-GigabitEthernet1/0/2] quit
```

配置接口 GigabitEthernet1/0/3 的 IP 地址为 100.1.1.1。

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port link-mode route
[DeviceA-GigabitEthernet1/0/3] ip address 100.1.1.1 24
[DeviceA-GigabitEthernet1/0/3] quit
```

配置 OSPF 协议。

```
<DeviceB> system-view
[DeviceB] ospf 1
[DeviceB-ospf-1] area 0
[DeviceB-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.0] quit
[DeviceB-ospf-1] quit
```

创建本地镜像组 1。

```
[DeviceA] mirroring-group 1 local
```

为本地镜像组 1 配置源端口。

```
[DeviceA] mirroring-group 1 mirroring-port gigabitethernet 1/0/1 inbound
```

为本地镜像组 1 配置目的端口及镜像报文的封装参数。

```
[DeviceA] mirroring-group 1 monitor-port gigabitethernet 1/0/2 destination-ip 40.1.1.2
source-ip 20.1.1.1
```

2. Device B 的配置

配置接口 GigabitEthernet1/0/1 的 IP 地址为 20.1.1.2。

```
<DeviceA> system-view
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-mode route
[DeviceA-GigabitEthernet1/0/1] ip address 20.1.1.2 24
[DeviceA-GigabitEthernet1/0/1] quit
```

配置接口 GigabitEthernet1/0/2 的 IP 地址为 40.1.1.1。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-mode route
[DeviceA-GigabitEthernet1/0/2] ip address 40.1.1.1 24
[DeviceA-GigabitEthernet1/0/2] quit
```

配置 OSPF 协议。

```
<DeviceB> system-view
[DeviceB] ospf 1
[DeviceB-ospf-1] area 0
[DeviceB-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.0] network 40.1.1.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.0] quit
[DeviceB-ospf-1] quit
```

8.5 验证配置

在完成上述配置后，在 DeviceA 上显示镜像组 1 的配置信息。

```
[DeviceA] display mirroring-group 1
Mirroring group 1:
    Type: Local
    Status: Active
    Mirroring port:
        GigabitEthernet1/0/1  Inbound
    Monitor port: GigabitEthernet1/0/2
                  Encapsulation: Destination IP address 40.1.1.2
                                 Source IP address 20.1.1.1
                                 Destination MAC address 1025-4125-412b
```

8.6 配置文件

- 设备 Device A：

```
#
ospf 1
 area 0.0.0.0
  network 10.1.1.0 0.0.0.255
  network 20.1.1.0 0.0.0.255
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 10.1.1.1 255.255.255.0
 mirroring-group 1 mirroring-port inbound
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 20.1.1.1 255.255.255.0
 mirroring-group 1 monitor-port  destination-ip 40.1.1.2 source-ip 20.1.1.1
#
interface GigabitEthernet1/0/3
 port link-mode route
 ip address 100.1.1.1 255.255.255.0
#
```

- 设备 Device B：

```
#
ospf 1
 area 0.0.0.0
  network 20.1.1.0 0.0.0.255
  network 40.1.1.0 0.0.0.255
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 20.1.1.2 255.255.255.0
```

```
#
interface GigabitEthernet1/0/2
 port link-mode route
 ip address 40.1.1.1 255.255.255.0
#
```

8.7 相关资料

- 产品配套“网络管理和监控配置指导”中的“镜像”。
- 产品配套“网络管理和监控命令参考”中的“镜像”。

9 本地流镜像快速配置指南

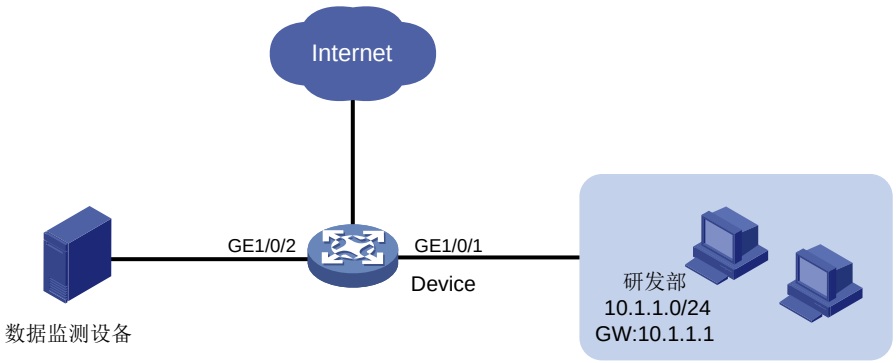
9.1 简介

本案例介绍本地流镜像的配置方法。

9.2 组网需求

某公司研发部使用 10.1.1.0/24 网段,现要求通过配置本地流镜像功能，使用数据监测设备对研发部主机访问互联网的 WWW 流量进行监控。

图11 本地流镜像组网示意图



9.3 配置步骤

配置 GigabitEthernet1/0/1 接口 IP 地址为 10.1.1.0/24，连接研发部设备。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] port link-mode route
[Device-GigabitEthernet1/0/1] ip address 10.1.1.0 24
[Device-GigabitEthernet1/0/1] quit
```

#定义对研发部上网流量进行镜像的 QoS 策略，创建 ACL 3000，匹配研发部的上网流量。

```
[Device] acl number 3000
[Device-acl-adv-3000] rule permit tcp destination-port eq www source 10.1.1.0 0.0.0.255
[Device-acl-adv-3000] quit
```

创建流分类 classifier_research，匹配 ACL 3000。

```
[Device] traffic classifier classifier_research
[Device-classifier-classifier_research] if-match acl 3000
[Device-classifier-classifier_research] quit
```

定义流行为 behavior_research，动作为镜像至端口 GigabitEthernet1/0/2。

```
[Device] traffic behavior behavior_research
[Device-behavior-behavior_research] mirror-to interface gigabitethernet 1/0/2
[Device-behavior-behavior_research] quit
```

定义策略 policy_research，为类 classifier_research 指定流行为 behavior_research。

```
[Device] qos policy policy_research
```

```
[Device-qospolicy-policy_research] classifier classifier_research behavior
behavior_research
[Device-qospolicy-policy_research] quit
```

将 policy_research 策略应用到 GigabitEthernet1/0/1 端口的入方向。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] qos apply policy policy_research inbound
[Device-GigabitEthernet1/0/1] quit
```

9.4 验证配置

在完成上述配置后，在 Device 上验证流镜像的配置信息。

```
[Device] display qos policy interface
  Interface: GigabitEthernet1/0/1
  Direction: Inbound
  Policy: policy_research
   Classifier: classifier_research
     Operator: AND
     Rule(s) :
      If-match acl 3000
     Behavior: behavior_research
      Mirroring:
        Mirror to the interface: GigabitEthernet1/0/2
```

9.5 配置文件

```
#
acl number 3000
 rule 0 permit tcp source 10.1.1.0 0.0.0.255 destination-port eq www
#
traffic classifier classifier_research operator and
 if-match acl 3000
#
traffic behavior behavior_research
 mirror-to interface GigabitEthernet1/0/2
#
qos policy policy_research
 classifier classifier_research behavior behavior_research
#
interface GigabitEthernet1/0/1
 port link-mode route
 ip address 10.1.1.0 0.0.0.255
 qos apply policy policy_research inbound
#
```

9.6 相关资料

- 产品配套“网络管理和监控配置指导”中的“镜像”。
- 产品配套“网络管理和监控命令参考”中的“镜像”。

信息中心快速配置指南

目 录

1 配置设备发送日志到服务器

1.1 简介

本案例介绍设备发送日志到服务器的配置方法。

1.2 组网需求

- 将系统的日志信息发送到日志主机；
- 将日志信息等级为 0～7 的日志信息发送到日志主机的服务器上。

图1 日志信息发送到日志主机配置组网图

1.3 配置准备

- 配置前请配置 IP 地址和路由，确保 Device 和 PC 之间路由可达。（具体配置步骤略）
- 在 PC 上安装 3CDaemon 软件作为日志服务器。

1.4 配置步骤

1. Device 上的配置

开启信息中心功能。

```
<Device> system-view
[Device] info-center enable
```

配置发送日志信息到 IP 地址为 1.2.0.1/16 的日志主机，日志主机记录工具为 local7，表示等级 0～7 的信息均会被输出。

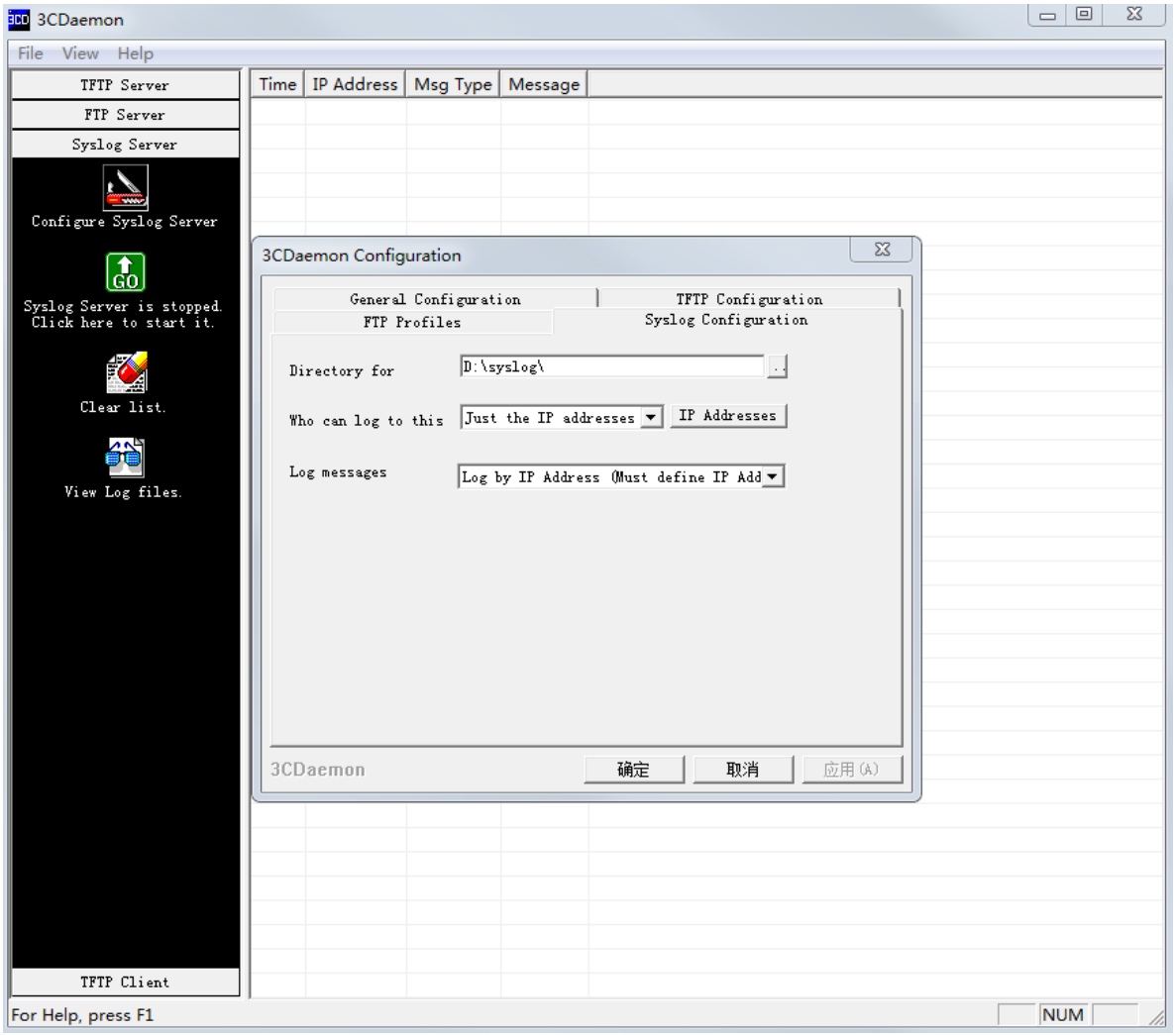
```
[Device] info-center loghost 1.2.0.1 facility local7
```

2. 日志主机上的配置

本案例通过 3CDaemon 作为日志服务器来接收交换机发过来的日志信息，不同厂商软件配置可能不同，以下步骤仅作为参考。

(1) 打开 3Cdaemon，并配置对应信息。

图2 配置 3CDaemon 作为日志服务器

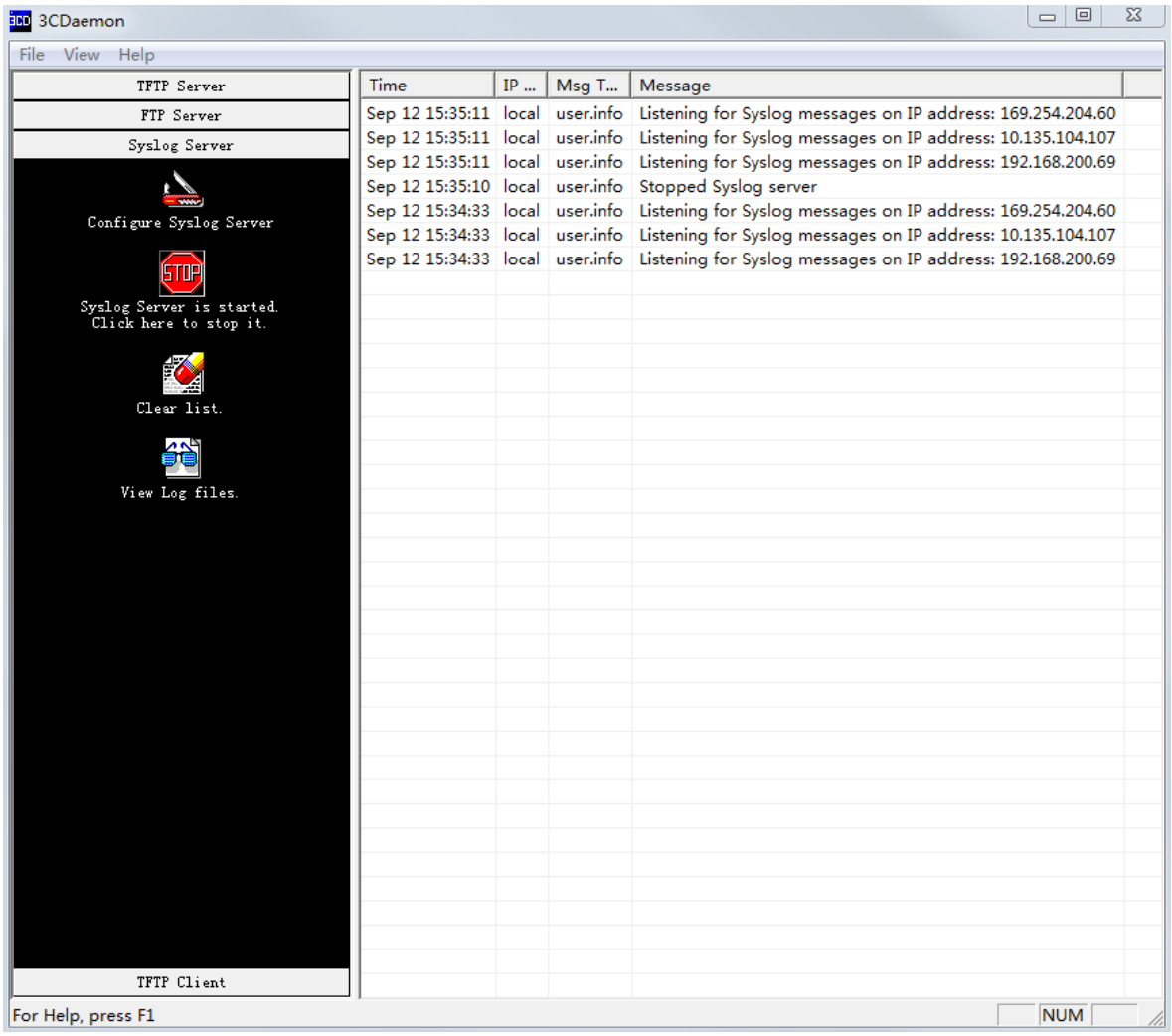


(2) 启动 3CDaemo 日志服务器。

1.5 验证配置

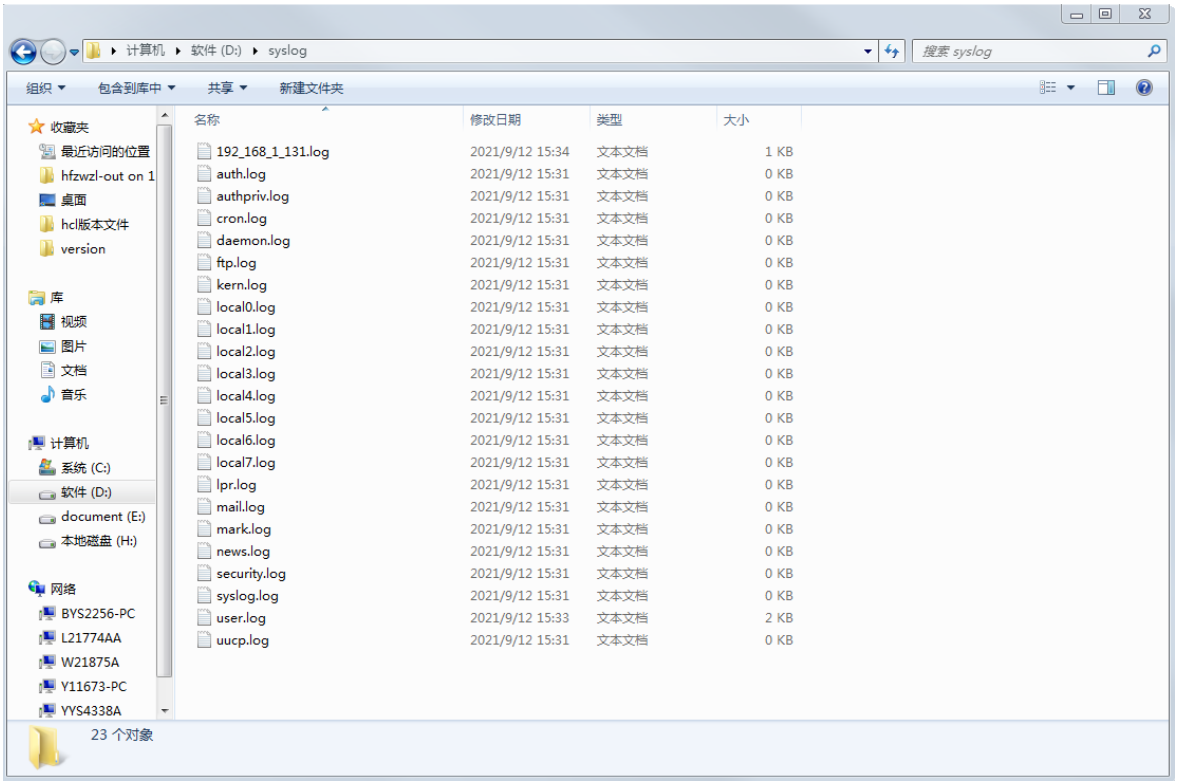
在日志服务器上可以看到交换机发过来的日志信息。

图3 查看日志信息



打开保存日志文件的目录查看日志信息。

图4 查看日志文件目录



1.6 配置文件

```
#
 info-center enable
 info-center loghost 1.2.0.1 facility local7
#
```

1.7 相关资料

- 产品配套“网络管理和监控配置指导”中的“信息中心”。
- 产品配套“网络管理和监控命令参考”中的“信息中心”。

2 配置设备保存日志到 Flash 指定文件夹

2.1 简介

本案例介绍将设备日志信息保存到 FLASH 指定文件夹的配置方法。

2.2 配置需求

- 将交换机的日志级别为 0-7 的日志保存到 FLASH，并且配置一个日志文件的最大为 1M。
- 设置日志缓存区容量最多可记录 500 条日志信息，设备自动保存日志文件的频率为 60000 秒。
- 记录用户登入信息及用户登入后所操作的命令。
- 配置日志信息时间戳输出格式为 boot 格式。

2.3 配置注意事项

日志在保存到日志文件前，先保存在日志文件缓冲区。系统会按照指定的频率将日志文件缓冲区的内容写入日志文件，用户也可以手工触发立即保存。成功保存后，保存前的日志文件缓冲区里的内容会被清空。

2.4 配置步骤

进入系统视图。

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

配置 0～7 级别的日志信息发送到日志缓冲区时的输出规则。

```
[Device] info-center source default logbuffer level debugging
```

允许日志信息输出到日志缓冲区。

```
[Device] info-center logbuffer
```

配置日志缓冲区可存储的信息最多为 500 条。

```
[Device] info-center logbuffer size 500
```

配置 0～7 级别的日志信息输出到日志文件。

```
[Device] info-center source default logfile level debugging
```

开启日志文件功能。

```
[Device] info-center logfile enable
```

配置单个日志文件最大能占用的存储空间为 1MB。

```
[Device] info-center logfile size-quota 1
```

配置设备保存日志文件到 FLASH 的 test 文件夹。

```
[Device] info-center logfile directory flash:/test
```

配置设备自动保存日志文件的频率为 60000 秒。

```
[Device] info-center logfile frequency 60000
```

配置日志信息时间戳输出格式为 boot 格式。

```
[Device] info-center timestamp boot
```

2.5 验证配置

查看显示系统日志文件的概要信息，可以看到日志文件功能已开启、单个日志文件最大能占用的存储空间为 1MB、设备保存日志文件到 FLASH 的 test 文件夹、保存日志文件的频率为 60000 秒。

```
[Device] display logfile summary
  Log file: Enabled
  Log file size quota: 1 MB
  Log file directory: flash:/test
  Writing frequency: 16 hour 40 min 0 sec
```

查看日志缓冲区的状态和日志缓冲区记录的日志信息，可以看到允许日志信息输出到日志缓冲区、单个日志文件最大能占用的存储空间为 1MB、可存储的信息最多为 500 条。

```
[Device] display logbuffer
Log buffer: Enabled
Max buffer size: 1024
Actual buffer size: 500
Dropped messages: 0
Overwritten messages: 402788
Current messages: 500
---- More ----
```

查看设备发送到 FLASH 的 test 文件夹的日志信息。

```
[Device] more test/logfile.log
%@3049495%0.2409505789 H3C ARP/6/ARP_TARGET_IP_INVALID: Target IP 192.168.1.60 w
as not the IP of the receiving interface M-GigabitEthernet0/0/0.
%@3049496%0.2409506971 H3C ARP/6/ARP_TARGET_IP_INVALID: Target IP 10.1.1.2 was n
ot the IP of the receiving interface M-GigabitEthernet0/0/0.
%@3049497%0.2409510823 H3C ARP/6/ARP_TARGET_IP_INVALID: Target IP 10.1.1.2 was n
ot the IP of the receiving interface M-GigabitEthernet0/0/0. This message repeat
ed 2 times in last 3 seconds.
%@3049498%0.2409510789 H3C ARP/6/ARP_TARGET_IP_INVALID: Target IP 192.168.1.60 w
as not the IP of the receiving interface M-GigabitEthernet0/0/0.
%@3049499%0.2409520259 H3C ARP/6/ARP_TARGET_IP_INVALID: Target IP 192.168.1.60 w
as not the IP of the receiving interface M-GigabitEthernet0/0/0. This message re
peated 1 times in last 10 seconds.
---- More ----
```

2.6 配置文件

```
#
 info-center timestamp boot
 info-center logfile frequency 6000
 info-center logfile size-quota 1
 info-center source default monitor deny
 info-center source default logbuffer level debugging
 info-center source default logfile level debugging
#
```

2.7 相关资料

- 产品配套“网络管理和监控配置指导”中的“信息中心”。
- 产品配套“网络管理和监控命令参考”中的“信息中心”。

SNMP 快速配置指南

目 录

1 SNMPv1/v2c 配置

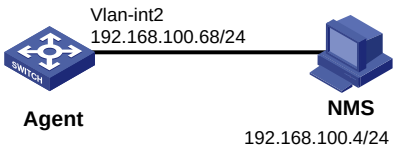
1.1 简介

本案例介绍 SNMPv1/v2c 的配置方法。

1.2 组网需求

如图 1 所示，iMC 服务器作为 NMS 通过 SNMPv1/SNMPv2c 协议对设备（Agent）进行监控管理，只读团体名为 readtest，读写团体名为 writetest，并且当设备出现故障时能够主动向 NMS 发送告警信息。

图1 SNMPv1/v2c 功能配置组网图



1.3 配置注意事项

- SNMPv2c 与 SNMPv1 配置方法完全一致，本举例中以配置 SNMPv2c 为例进行介绍。
- 用户在设备和 NMS 上配置的 SNMP 版本号和团体字必须一致，否则，NMS 无法对设备进行管理和维护。
- 不同厂商的 NMS 软件配置方法不同，关于 NMS 的详细配置，具体请参考 NMS 的相关手册。本配置举例中，以 iMC PLAT 7.0 (E0202)为例进行介绍。

1.4 配置步骤

1. Agent 的配置

配置接口 Vlan-interface2 的 IP 地址。

```
<Agent> system-view
[Agent] interface Vlan-interface 2
[Agent-Vlan-interface 2] ip address 192.168.100.68 24
[Agent-Vlan-interface 2] quit
```

设置 Agent 使用的 SNMP 版本为 v2c、只读团体名为 readtest，读写团体名为 writetest。

```
[Agent] snmp-agent sys-info version v2c
[Agent] snmp-agent community read readtest
[Agent] snmp-agent community write writetest
```

设置设备的联系人和位置信息，以方便维护。

```
[Agent] snmp-agent sys-info contact Mr.Wang-Tel:3306
[Agent] snmp-agent sys-info location telephone-closet,3rd-floor
```

设置允许向 NMS 发送告警信息，使用的团体名为 readtest。

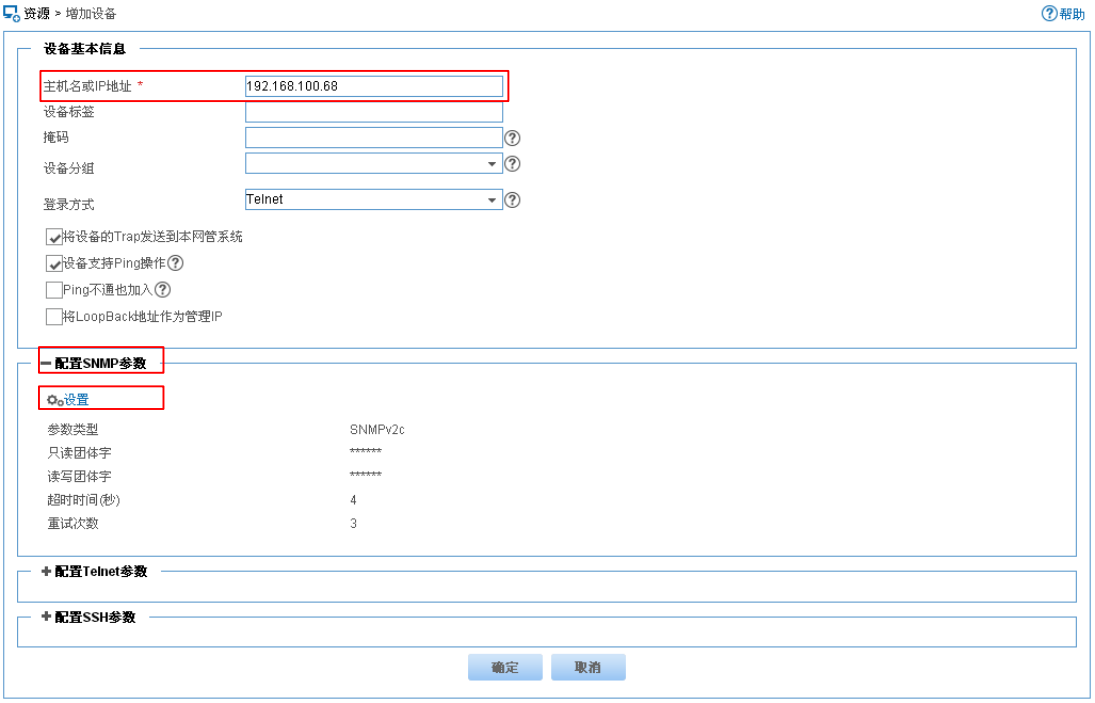
```
[Agent] snmp-agent trap enable
```

```
[Agent] snmp-agent target-host trap address udp-domain 192.168.100.4 params securityname
readtest v2c
```

2. NMS 的配置

(1) 登录进入 iMC 管理平台，选择“资源”页签，单击导航树中的[增加设备]菜单项，进入增加设备配置页面。在该页面中输入设备的主机名或 IP 地址，并点击<配置 SNMP 参数/设置>链接。

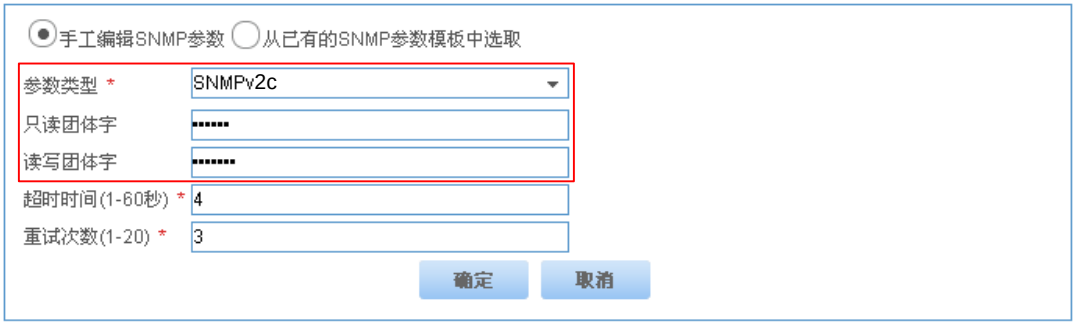
图2 增加设备配置页面



(2) 进入 SNMP 参数设置页面配置 SNMP 参数。

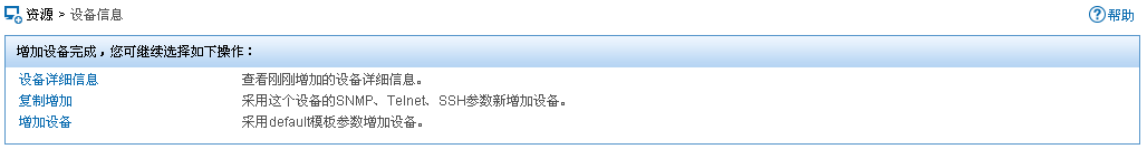
- 设置参数类型为“SNMPv2c”；
- 设置只读团体字为“readtest”；
- 设置读写团体字为“writetest”；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图3 SNMP 参数设置页面



(3) 在增加设备配置页面单击<确定>按钮，iMC 返回增加设备成功信息。增加设备成功后，用户即可通过 iMC 对设备进行配置、管理和维护。

图4 增加设备成功页面



1.5 验证配置

完成以上配置之后，在设备上的某个空闲接口执行 **shutdown** 或 **undo shutdown** 操作，设备会向 NMS 发送接口状态改变的 Trap。

在 iMC 的“告警>告警浏览>全部告警”页面中会显示上述接口状态改变的 Trap 信息。

1.6 配置文件

```
#
 snmp-agent
 snmp-agent community write writetest
 snmp-agent community read readtest
 snmp-agent sys-info contact Mr.Wang-Tel:3306
 snmp-agent sys-info location telephone-closet,3rd-floor
 snmp-agent sys-info version v2c
 snmp-agent trap enable arp
 snmp-agent trap enable syslog
 snmp-agent target-host trap address udp-domain 192.168.100.4 params securityname readtest
v2c
#
```

1.7 相关资料

- 产品配套“网络管理和监控配置指导”中的“SNMP”。
- 产品配套“网络管理和监控命令参考”中的“SNMP”。

2 SNMPv3 配置

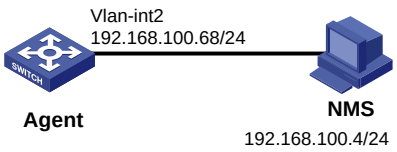
2.1 简介

本案例介绍 SNMPv3 的配置方法。

2.2 组网需求

- NMS 通过 SNMPv3 只能对 Agent 的 SNMP 报文的相关信息进行监控管理，Agent 在出现故障时能够主动向 NMS 发送告警信息，NMS 上接收 SNMP 告警信息的默认 UDP 端口号为 162。
- NMS 与 Agent 建立 SNMP 连接时，需要认证，使用的认证算法为 SHA-1，认证密码为 123456TESTauth&!。NMS 与 Agent 之间传输的 SNMP 报文需要加密，使用的加密协议为 AES，加密密码为 123456TESTencr&!。

图2 SNMPv3 功能典型配置组网图



2.3 配置注意事项

- SNMPv3 支持基于 RBAC（Role Based Access Control，基于角色的访问控制）和基于 VACM（View-based Access Control Model，基于视图的访问控制模型）两种访问控制方式。本配置举例中，针对同一需求分别给出了两种方式的配置示例，请选择一种作为参考即可。
- 用户在设备和 NMS 上配置的 SNMP 版本号和团体字必须一致，否则，NMS 无法对设备进行管理和维护。
- 不同厂商的 NMS 软件配置方法不同，关于 NMS 的详细配置，具体请参考 NMS 的相关手册。本配置举例中，以 iMC PLAT 7.0 (E0202)为例进行介绍。
- SNMPv3 接收 Trap 报文的目的主机的安全参数要使用设备已配置的 v3 用户，且安全模型要一致。
- SNMPv3 的认证密码和加密密码以密文形式保存在配置文件中，密文密码由明文密码和本设备的引擎 ID 计算后生成。如果要将两台设备的认证密码和加密密码配置为相同值，建议使用明文密码在两台设备上分别手工配置，不要直接拷贝配置文件中的相关配置。因为两台设备的引擎 ID 不同，会导致密文密码相同，而对应的明文密码不同。

2.4 配置步骤

1. 基于 RBAC 的 SNMPv3 配置

配置接口 Vlan-interface2 的 IP 地址。

<Agent> system-view

```
[Agent] interface Vlan-interface2
```

```
[Agent-Vlan-interface2] ip address 192.168.100.68 24
[Agent-Vlan-interface2] quit
```
设置 Agent 使用的 SNMP 版本为 v3。
```
[Agent] snmp-agent sys-info version v3
```
创建用户角色 test，允许他读写 internet 子树（OID 为“1.3.6.1”）下的所有对象。
```
[Agent] role name test
[Agent-role-test] rule 1 permit read write oid 1.3.6.1
[Agent-role-test] quit
```
创建 SNMPv3 用户 managev3user，为其绑定用户角色 test，认证算法为 SHA-1，明文认证密码为 123456TESTauth&!，加密算法为 AES，明文加密密码是 123456TESTencr&!。
```
[Agent] snmp-agent usm-user v3 managev3user user-role test simple authentication-mode sha 123456TESTauth&! privacy-mode aes128 123456TESTencr&!
```
配置设备的联系人和位置信息，以方便维护。
```
[Agent] snmp-agent sys-info contact Mr.Wang-Tel:3306
[Agent] snmp-agent sys-info location telephone-closet,3rd-floor
```
开启 SNMP 告警功能。
```
[Agent] snmp-agent trap enable
```
设置接收 SNMP 告警信息的目的主机 IP 地址，即 NMS 的 IP 地址，配置安全认证参数为 managev3user。
```
[Agent] snmp-agent target-host trap address udp-domain 192.168.100.4 params securityname managev3user v3 privacy
```
2. 基于 VACM 的 SNMPv3 配置

配置接口 Vlan-interface2 的 IP 地址。
```
<Agent> system-view
[Agent] interface Vlan-interface2
[Agent-Vlan-interface2] ip address 192.168.100.68 24
[Agent-Vlan-interface2] quit
```
设置 Agent 使用的 SNMP 版本为 v3。
```
<Agent> system-view
[Agent] snmp-agent sys-info version v3
```
创建 MIB 视图，名字为 mibtest，包含 internet 子树（OID 为“1.3.6.1”）下的所有对象。
```
[Agent] snmp-agent mib-view included mibtest 1.3.6.1
```
创建 SNMPv3 组 managev3group，并配置与该组绑定的 SNMPv3 用户与 NMS 建立连接时，均进行认证和加密，NMS 可以对设备进行读写的视图均为 mibtest。
```
[Agent] snmp-agent group v3 managev3group privacy read-view mibtest write-view mibtest notify-view mibtest
```
创建 SNMPv3 用户 managev3user，认证算法为 SHA-1，明文认证密码为 123456TESTauth&!，加密算法为 AES，明文加密密码是 123456TESTencr&!。
```
[Agent] snmp-agent usm-user v3 managev3user managev3group simple authentication-mode sha 123456TESTauth&! privacy-mode aes128 123456TESTencr&!
```
配置设备的联系人和位置信息，以方便维护。
```
[Agent] snmp-agent sys-info contact Mr.Wang-Tel:3306
[Agent] snmp-agent sys-info location telephone-closet,3rd-floor
```
开启 SNMP 告警功能。
```
[Agent] snmp-agent trap enable
```

设置接收 SNMP 告警信息的目的主机 IP 地址，即 NMS 的 IP 地址，配置安全认证参数为 managev3user。

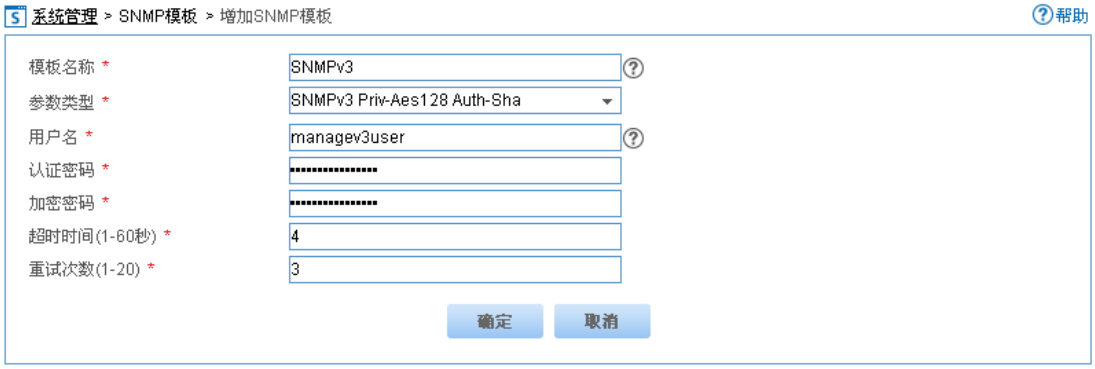
```
[Agent] snmp-agent target-host trap address udp-domain 192.168.100.4 params securityname managev3user v3 privacy
```

3. NMS 的配置

配置 SNMP 模板。

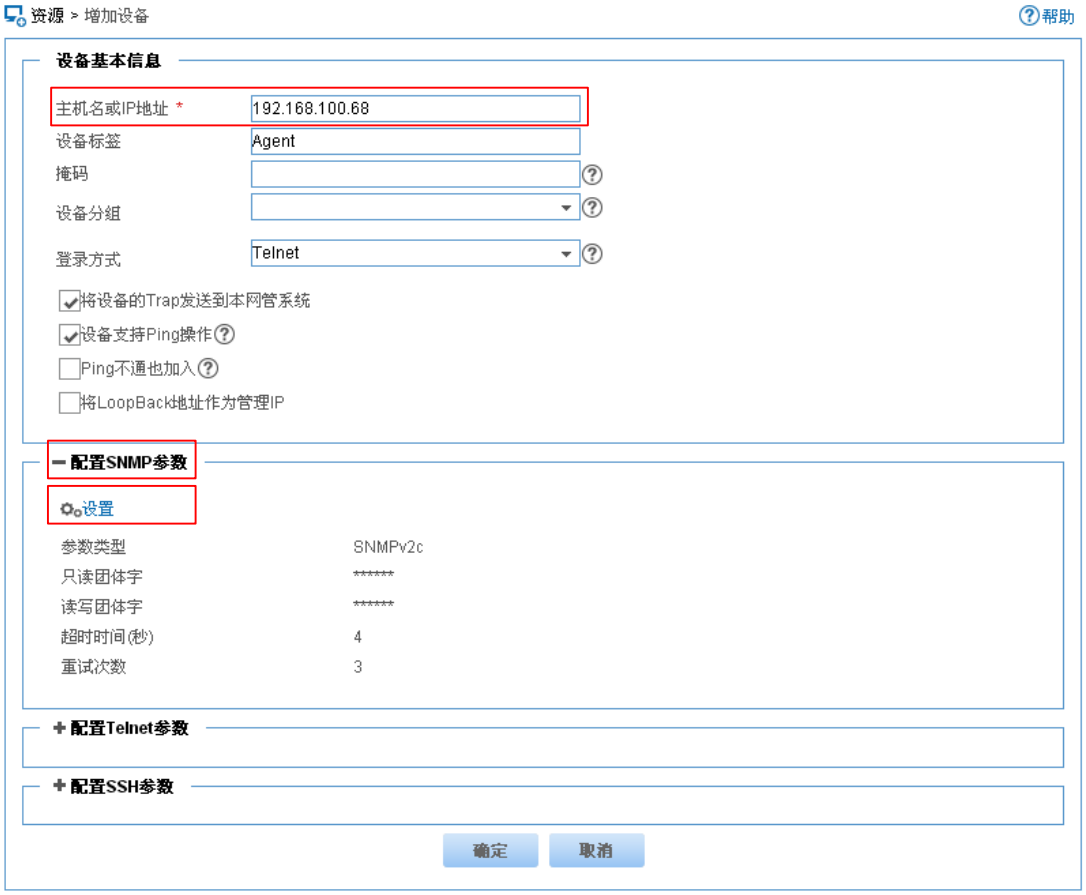
- 登录 iMC，选择“系统管理”页签，单击导航树中的[资源管理/SNMP 模板]菜单项，进入 SNMP 模板配置页面，在该页面中单击<增加>按钮，进入增加 SNMP 模板配置页面。
- 配置 SNMP 模板的名称为 SNMPv3。
- 选择参数类型为 SNMPv3 Priv-Aes128 Auth-Sha。
- 配置 SNMP 用户名为 managev3user。
- 明文认证密码为 123456TESTauth&!。
- 明文加密密码为 123456TESTencr&!。
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图3 增加 SNMP 模板页面



选择“资源”页签，单击导航树中的[资源管理/增加设备]菜单项，进入增加设备配置页面，在该页面中输入设备的主机名或 IP 地址，并点击<配置 SNMP 参数/设置>链接。

图4 增加设备页面



进入 SNMP 参数设置页面配置 SNMP 参数。

- 选择“从已有的 SNMP 参数模板中选取”。
- 选择名称为“SNMPv3”的 SNMP 模板。
- 单击<确定>按钮完成操作，返回到“增加设备”页面。

图5 SNMP 参数设置页面

- 在“增加设备”页面单击<确定>按钮，iMC 返回增加设备成功信息。增加设备成功后，用户即可通过 iMC 对设备进行配置、管理和维护。

图6 增加设备成功页面

2.5 验证配置

完成以上配置之后，在设备上的某个空闲接口执行 **shutdown** 或 **undo shutdown** 操作，设备会向 NMS 发送接口状态改变的 Trap。

在 iMC 的“告警>告警浏览>全部告警”页面中会显示上述接口状态改变的 Trap 信息。

2.6 配置文件

- 基于 RBAC 的配置文件

```
#
 snmp-agent
 snmp-agent sys-info contact Mr.Wang-Tel:3306
 snmp-agent sys-info location telephone-closet,3rd-floor
 snmp-agent sys-info version v3
 snmp-agent trap enable arp
 snmp-agent trap enable syslog
 snmp-agent target-host trap address udp-domain 192.168.100.4 params securityname
managev3user v3 privacy
 snmp-agent usm-user v3 managev3user user-role test cipher authentication-mode sha
$c$3$5JaJZ6gNXlyNRq2FR2ELDT3QQH1exwJRWdYYq7eLfcBewuM5ncM= privacy-mode aes128
$c$3$+bbXZS4+PnsLDyr16OogzBckaLzR6XMDwZQuLBU8RM+dpw==
#
role name test
 rule 1 permit read write oid 1.3.6.1
#
```

- 基于 VACM 的配置文件

```
#
 snmp-agent
 snmp-agent sys-info contact Mr.Wang-Tel:3306
 snmp-agent sys-info location telephone-closet,3rd-floor
 snmp-agent sys-info version v3
 snmp-agent group v3 managev3group privacy read-view mibtest write-view mibtest notify-view
mibtest
 snmp-agent mib-view included mibtest internet
 snmp-agent trap enable arp
 snmp-agent trap enable syslog
 snmp-agent target-host trap address udp-domain 192.168.100.4 params securityname
managev3user v3 privacy
```

```
 snmp-agent usm-user v3 managev3user managev3group cipher authentication-mode sha
$c$3$5JaJZ6gNXlyNRq2FR2ELDT3QQH1exwJRWdYYq7eLfcBewuM5ncM= privacy-mode aes128
$c$3$+bbXZS4+PnsLDyr16OogzBckaLzR6XMDwZQuLBU8RM+dpw==
#
```

2.7 相关资料

- 产品配套“网络管理和监控配置指导”中的“SNMP”。
- 产品配套“网络管理和监控命令参考”中的“SNMP”。

3 SNMP 应用 ACL 限制非法网管访问

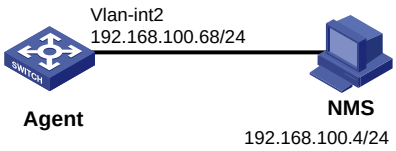
3.1 简介

本案例介绍通过基本 ACL 实现仅指定的网管能够访问交换机的配置方法。

3.2 组网需求

如图 3 所示，iMC 服务器作为 NMS 通过 SNMPv2c 协议对设备（Agent）进行监控管理，只读团体名为 readtest，读写团体名为 writetest，并且当设备出现故障时能够主动向 NMS 发送告警信息。

图3 SNMP 应用 ACL 限制非法网管访问组网图



3.3 配置注意事项

- 用户在设备和 NMS 上配置的 SNMP 版本号和团体字必须一致，否则，NMS 无法对设备进行管理和维护。
- 不同厂商的 NMS 软件配置方法不同，关于 NMS 的详细配置，具体请参考 NMS 的相关手册。本配置举例中，以 iMC PLAT 7.0 (E0202)为例进行介绍。

3.4 配置步骤

1. Agent 的配置

配置接口 Vlan-interface2 的 IP 地址，Agent 使用的 SNMP 版本为 v2c。

```
<Agent> system-view
[Agent] interface Vlan-interface 2
[Agent-Vlan-interface 2] ip address 192.168.100.68 24
[Agent-Vlan-interface 2] quit
[Agent] snmp-agent sys-info version v2c
[Agent] quit
```

配置访问限制，只允许 IP 地址为 1.1.1.1 的 NMS 使用该团体名对设备上缺省视图内的 MIB 对象进行读写操作，禁止其它 NMS 使用该团体名执行写操作。

```
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 192.168.100.4 0.0.0.0
[Sysname-acl-ipv4-basic-2001] rule deny source any
[Sysname-acl-ipv4-basic-2001] quit
```

创建 MIB 视图信息，视图名称为 mibtest，通过 MIB 视图限制网管仅能访问指定的 MIB（OID 为“1.3.6.1.2.1”）。

```
[Sysname] snmp-agent mib-view included mibtest 1.3.6.1.2.1
```

配置只读团体名为 readtest，读写团体名为 writetest。

```
[Agent] snmp-agent community read readtest
[Agent] snmp-agent community write writetest
```

设置设备的联系人和位置信息，以方便维护。

```
[Agent] snmp-agent sys-info contact Mr.Wang-Tel:3306
[Agent] snmp-agent sys-info location telephone-closet,3rd-floor
```

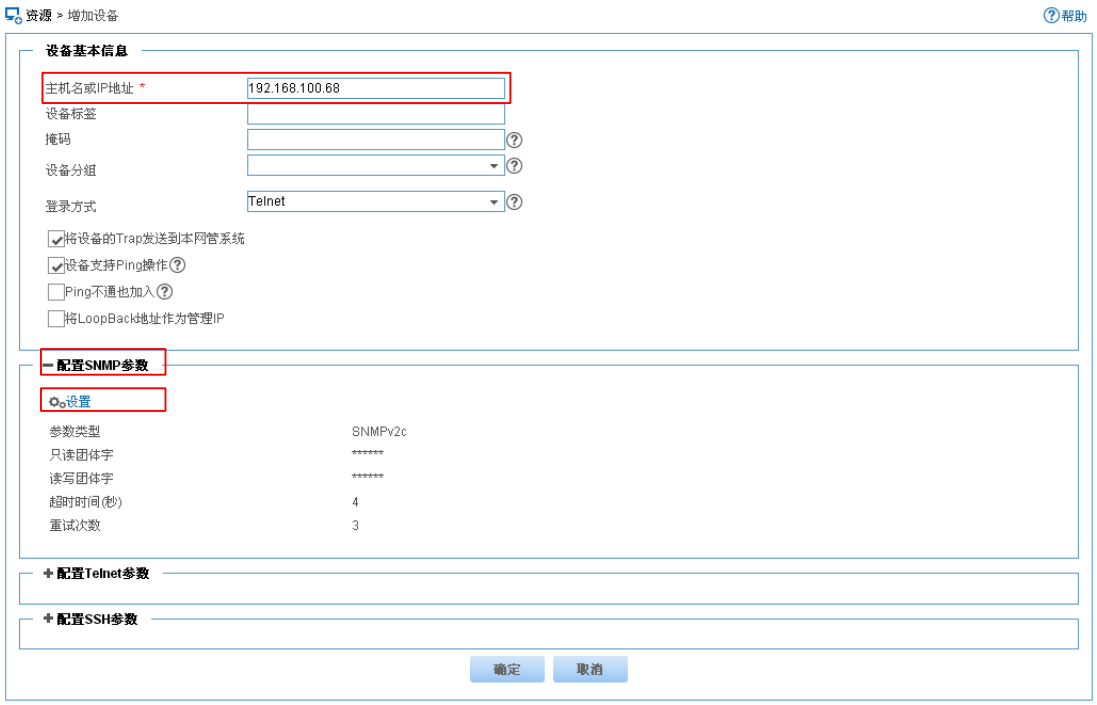
设置允许向 NMS 发送告警信息，使用的团体名为 readtest。

```
[Agent] snmp-agent trap enable
[Agent] snmp-agent target-host trap address udp-domain 192.168.100.4 params securityname readtest v2c
```

2. NMS 的配置

(1) 登录进入 iMC 管理平台，选择“资源”页签，单击导航树中的[增加设备]菜单项，进入增加设备配置页面。在该页面中输入设备的主机名或 IP 地址，并点击<配置 SNMP 参数/设置>链接。

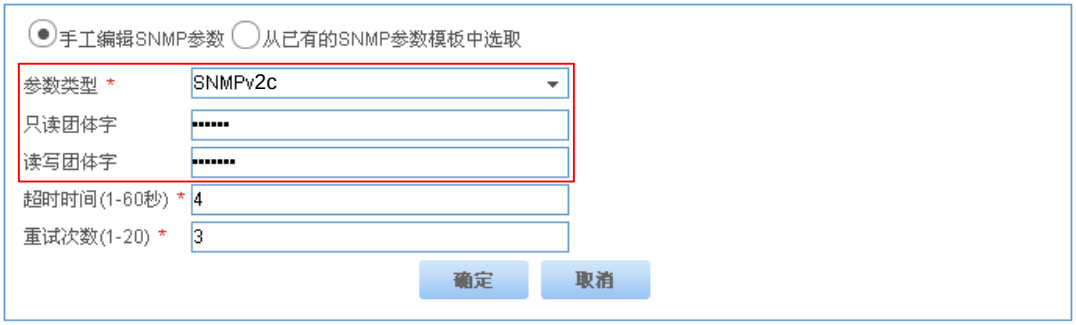
图4 增加设备配置页面



(2) 进入 SNMP 参数设置页面配置 SNMP 参数。

- 设置参数类型为“SNMPv2c”；
- 设置只读团体字为“readtest”；
- 设置读写团体字为“writetest”；
- 其它参数采用缺省值，并单击<确定>按钮完成操作。

图5 SNMP 参数设置页面



(3) 在增加设备配置页面单击<确定>按钮，iMC 返回增加设备成功信息。增加设备成功后，用户即可通过 iMC 对设备进行配置、管理和维护。

图6 增加设备成功页面

3.5 验证配置

完成以上配置之后，在设备上的某个空闲接口执行 **shutdown** 或 **undo shutdown** 操作，设备会向 NMS 发送接口状态改变的 Trap。

在 iMC 的“告警>告警浏览>全部告警”页面中会显示上述接口状态改变的 Trap 信息。

只允许指定 IP 地址 192.168.100.4 的网管读写交换机的指定 MIB。

3.6 配置文件

```
#
 snmp-agent
 acl basic 2001
 rule permit source 192.168.100.68 0.0.0.0
 rule deny source any
 snmp-agent mib-view included mibtest 1.3.6.1.2.1
 snmp-agent community write writetest
 snmp-agent community read readtest
 snmp-agent sys-info contact Mr.Wang-Tel:3306
 snmp-agent sys-info location telephone-closet,3rd-floor
 snmp-agent sys-info version v2c
 snmp-agent trap enable
 snmp-agent target-host trap address udp-domain 192.168.100.4 params securityname readtest
v2c
#
```

3.7 相关资料

- 产品配套“网络管理和监控配置指导”中的“SNMP”。
- 产品配套“网络管理和监控命令参考”中的“SNMP”。

通过静态路由实现公私网路由互通配置指南

目 录

1 配置静态路由实现公私网路由互通

1.1 简介

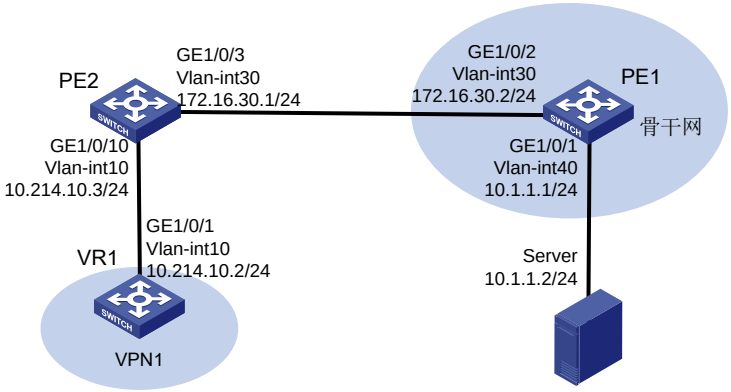
本案例介绍配置静态路由实现公私网路由互通的配置方法。

1.2 组网需求

如图 1 所示，PE1 为公网中的设备，服务器 Server 与 PE1 直连。PE2 连接 VR1，VPN1 通过 PE2 接入公网。需求如下：

实现公私网路由互通，VR1 能够访问到 Server。

图1 配置静态路由实现公私网路由互通组网示意图



1.3 配置思路

要实现 VR1 能够访问到 Server，需要按顺序完成如下配置：

(1) 在 PE1 和 VR1 创建 VLAN 及相应的 VLAN 接口；

(2) 在 PE2 上配置 VPN 实例并将 VR1 接入 PE2；

(3) 在 Server、PE1 和 VR1 上配置静态路由保证公网路由互通；

(4) 在 PE2 上配置静态路由实现公私网路由互通。

1.4 配置步骤

1. 配置 VR1

在 VR1 设备上创建 VLAN10，并将 GigabitEthernet1/0/1 端口加入 VLAN10。

```
<VR1> system-view
[VR1] vlan 10
[VR1-vlan10] quit
[VR1] interface GigabitEthernet 1/0/1
[VR1-GigabitEthernet1/0/1] port link-type trunk
[VR1-GigabitEthernet1/0/1] port trunk permit vlan 10
```

```
[VR1-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[VR1-GigabitEthernet1/0/1] quit
```

配置 Vlan-interface10 接口的 IP 地址为 10.214.10.2/24。

```
[VR1] interface Vlan-interface 10
[VR1-Vlan-interface10] ip address 10.214.10.2 24
[VR1-Vlan-interface10] quit
```

2. 配置 PE1

在 PE1 设备上创建 VLAN30 和 VLAN40，并将 GigabitEthernet1/0/1 端口加入 VLAN40，将 GigabitEthernet1/0/2 端口加入 VLAN30。

```
<PE1> system-view
[PE1] vlan 30
[PE1-vlan30] quit
[PE1] vlan 40
[PE1-vlan40] quit
[PE1] interface GigabitEthernet 1/0/1
[PE1-GigabitEthernet1/0/1] port link-type trunk
[PE1-GigabitEthernet1/0/1] port trunk permit vlan 40
[PE1-GigabitEthernet1/0/1] undo port trunk permit vlan 1
[PE1-GigabitEthernet1/0/1] quit
[PE1] interface GigabitEthernet 1/0/2
[PE1-GigabitEthernet1/0/2] port link-type trunk
[PE1-GigabitEthernet1/0/2] port trunk permit vlan 30
[PE1-GigabitEthernet1/0/2] undo port trunk permit vlan 1
[PE1-GigabitEthernet1/0/2] quit
```

配置 PE1 的 Vlan-interface30 和 Vlan-interface40 接口分的 IP 地址分别为 172.16.30.2/24 和 10.1.1.1/24。

```
[PE1] interface Vlan-interface 30
[PE1-Vlan-interface30] ip address 172.16.30.2 24
[PE1-Vlan-interface30] quit
[PE1] interface Vlan-interface 40
[PE1-Vlan-interface40] ip address 10.1.1.1 24
[PE1-Vlan-interface40] quit
```

3. 配置 PE2

在 PE2 设备上为 VPN1 创建 VPN 实例，名为“vpn1”，并配置该实例的 RD 值为 10:1，接收和发送的 VPN Target 属性均为 111:1。。

```
<PE2> system-view
[PE2] ip vpn-instance vpn1
[PE2-vpn-instance-vpn1] route-distinguisher 10:1
[PE2-vpn-instance-vpn1] vpn-target 111:1
[PE2-vpn-instance-vpn1] quit
```

在 PE2 设备上创建 VLAN10 和 VLAN30，并将 GigabitEthernet1/0/10 端口加入 VLAN10，将 GigabitEthernet1/0/3 端口加入 VLAN30。

```
[PE2] vlan 10
[PE2-vlan10] quit
[PE2] vlan 30
```

```
[PE2-vlan30] quit
[PE2] interface GigabitEthernet 1/0/10
[PE2-GigabitEthernet1/0/10] port link-type trunk
[PE2-GigabitEthernet1/0/10] port trunk permit vlan 10
[PE2-GigabitEthernet1/0/10] undo port trunk permit vlan 1
[PE2-GigabitEthernet1/0/10] quit
[PE2] interface GigabitEthernet 1/0/3
[PE2-GigabitEthernet1/0/3] port link-type trunk
[PE2-GigabitEthernet1/0/3] port trunk permit vlan 30
[PE2-GigabitEthernet1/0/3] undo port trunk permit vlan 1
[PE2-GigabitEthernet1/0/3] quit
```

配置 Vlan-interface10 接口与 VPN1 实例进行绑定，并配置 IP 地址为 10.214.10.3/24。

```
[PE2] interface Vlan-interface 10
[PE2-Vlan-interface10] ip binding vpn-instance vpn1
[PE2-Vlan-interface10] ip address 10.214.10.3 24
[PE2-Vlan-interface10] quit
```

配置 Vlan-interface30 接口的 IP 地址为 172.16.30.1/24。

```
[PE2] interface Vlan-interface 30
[PE2-Vlan-interface30] ip address 172.16.30.1 24
[PE2-Vlan-interface30] quit
```

4. 在 Server、PE1 和 VR1 上配置静态路由

在 Server 上指定静态路由，去往 10.214.10.0 网段的报文，下一跳地址为 10.1.1.1。

```
<Server> system-view
[Server] ip route-static 10.214.10.0 255.255.255.0 10.1.1.1
```

在 PE1 上指定静态路由，去往 10.214.10.0 网段的报文，下一跳地址为 172.16.30.1。

```
<PE1> system-view
[PE1] ip route-static 10.214.10.0 24 172.16.30.1
```

在 VR1 上指定静态路由，去往 10.1.1.0 网段的报文，下一跳地址为 10.214.10.3。

```
<VR1> system-view
[VR1] ip route-static 10.1.1.0 24 10.214.10.3
```

5. 在 PE2 上配置静态路由实现公私网路由互通

在 PE2 上指定静态路由，去往 10.214.10.0 网段的报文，下一跳地址为 10.214.10.2，并将此路由与 VPN1 实例绑定。

```
<PE2> system-view
[PE2] ip route-static 10.214.10.0 24 vpn-instance vpn1 10.214.10.2
```

在 PE2 上指定静态路由，去往 10.1.1.0 网段的报文，下一跳地址为 172.16.30.2，并将此路由与 VPN1 实例绑定。

```
[PE2] ip route-static vpn-instance vpn1 10.1.1.0 24 172.16.30.2 public
```

1.5 验证配置

显示 PE2 上为 VPN1 实例维护的路由信息。

```
[PE2] display ip routing-table vpn-instance vpn1

Destinations : 7        Routes : 7
```

```
Destination/Mask    Proto  Pre  Cost         NextHop         Interface
10.214.10.0/24      Direct 0     0           10.214.10.3     Vlan10
10.214.10.3/32      Direct 0     0           127.0.0.1       InLoop0
127.0.0.0/8         Direct 0     0           127.0.0.1       InLoop0
127.0.0.1/32        Direct 0     0           127.0.0.1       InLoop0
172.16.30.0/24      Direct 0     0           172.16.30.1     Vlan30
172.16.30.1/32      Direct 0     0           127.0.0.1       InLoop0
10.1.1.0/24         Static 60    0           172.16.30.2     Vlan30
```

可以看到，VPN1 的路由表中已经存在指向公网的静态路由。

显示 PE2 上的路由信息。

```
[PE1] display ip routing-table

Destinations : 14        Routes : 14

Destination/Mask   Proto   Pre Cost        NextHop         Interface
0.0.0.0/32         Direct  0   0           127.0.0.1       InLoop0
100.100.11.1/32    Direct  0   0           127.0.0.1       InLoop0
127.0.0.0/8        Direct  0   0           127.0.0.1       InLoop0
127.0.0.0/32       Direct  0   0           127.0.0.1       InLoop0
127.0.0.1/32       Direct  0   0           127.0.0.1       InLoop0
127.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
172.16.30.0/24     Direct  0   0           172.16.30.2     Vlan30
172.16.30.0/32     Direct  0   0           172.16.30.2     Vlan30
172.16.30.2/32     Direct  0   0           127.0.0.1       InLoop0
172.16.30.255/32   Direct  0   0           172.16.30.2     Vlan30
10.214.10.0/24     Static  60  1           10.214.10.2     Vlan10
224.0.0.0/4        Direct  0   0           0.0.0.0         NULL0
224.0.0.0/24       Direct  0   0           0.0.0.0         NULL0
255.255.255.255/32 Direct  0   0           127.0.0.1       InLoop0
```

可以看到，指向私网网段的静态路由已经引入到公网路由表中。

使用 **ping** 命令验证 VR1 到 Server 的网络连通性。

```
<VR1>ping 10.1.1.2
Ping 10.1.1.2 (10.1.1.2): 56 data bytes, press CTRL+C to break
56 bytes from 10.1.1.2: icmp_seq=0 ttl=255 time=3.880 ms
56 bytes from 10.1.1.2: icmp_seq=1 ttl=255 time=0.819 ms
56 bytes from 10.1.1.2: icmp_seq=2 ttl=255 time=0.658 ms
56 bytes from 10.1.1.2: icmp_seq=3 ttl=255 time=1.421 ms
56 bytes from 10.1.1.2: icmp_seq=4 ttl=255 time=0.722 ms

--- Ping statistics for 10.1.1.2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.658/1.500/3.880/1.221 ms
```

1.6 配置文件

- VR1：

```
#
 vlan 10
#
interface Vlan-interface10
 ip address 10.214.10.2 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10
#
 ip route-static 10.1.1.0 24 10.214.10.3
#
```

- PE1：

```
#
vlan 30
#
vlan 40
#
interface Vlan-interface30
 ip address 172.16.30.2 255.255.255.0
#
interface Vlan-interface40
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 40
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 30
#
 ip route-static 10.214.10.0 24 172.16.30.1
#
```

- PE2：

```
#
ip vpn-instance vpn1
 route-distinguisher 10:1
 vpn-target 111:1 import-extcommunity
 vpn-target 111:1 export-extcommunity
#
vlan 10
```

```
#
vlan 30
#
interface Vlan-interface10
 ip binding vpn-instance vpn1
 ip address 10.214.10.3 255.255.255.0
#
interface Vlan-interface30
 ip binding vpn-instance vpn1
 ip address 172.16.30.1 255.255.255.0
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 30
#
interface GigabitEthernet1/0/10
 port link-mode bridge
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 10
#
 ip route-static 10.214.10.0 24 vpn-instance v1 10.214.10.2
 ip route-static vpn-instance v1 10.1.1.0 24 172.16.30.2 public
#
```

1.7 相关资料

- 产品配套“三层技术-IP 路由配置指导”中的“静态路由”。
- 产品配套“三层技术-IP 路由命令参考”中的“静态路由”。

局域网组网案例

目 录

1 小型园区典型组网

1.1 简介

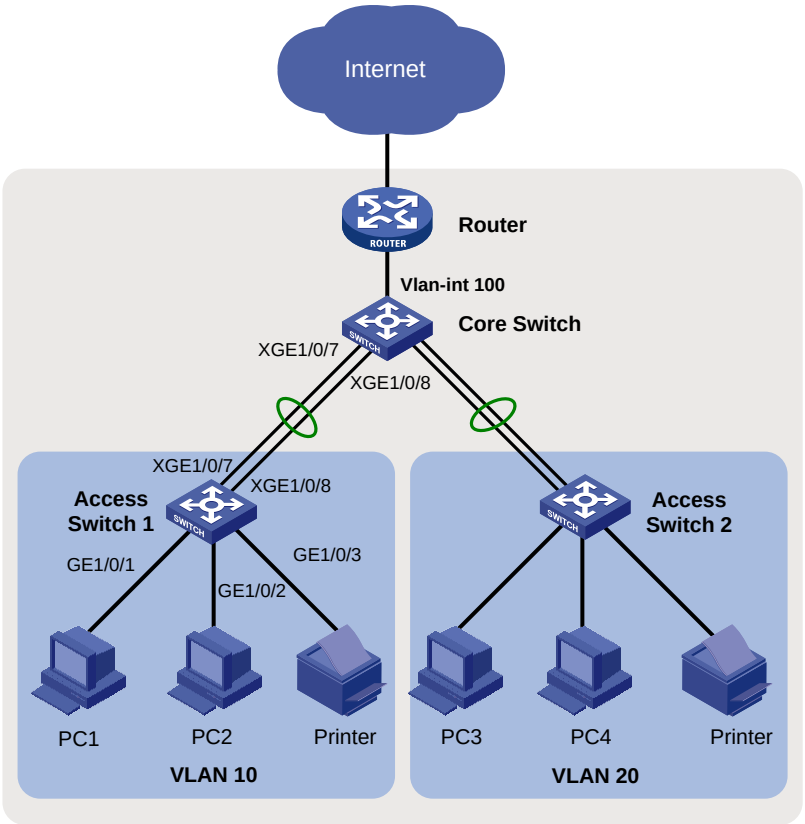
本案例介绍小型园区典型组网配置。

1.2 组网需求

如图 1 所示，在小型园区中，S5130 系列或 S5130S 系列以太网交换机通常部署在网络的接入层，S5560X 系列或 S6520X 系列以太网交换机可部署在网络的核心，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



1.3 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) 登录设备

(2) 配置管理 IP 地址和 Telnet 功能

(3) 配置接口和 VLAN

(4) 配置核心交换机 DHCP 服务器功能

(5) 配置核心交换机路由

(6) 配置出口路由器

(7) 配置接入交换机的 DHCP Snooping 功能

(8) 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Console口登录	设置传输速率等通信参数	PC端通过终端仿真软件登录设备
配置管理IP和telnet功能	管理VLAN	VLAN 5	交换机缺省VLAN为VLAN 1。一般不将其配置为管理VLAN 本文将VLAN5配置为管理VLAN
	管理用以太网口或管理VLAN接口IP地址	10.10.1.1/24	有管理用以太网口的交换机，可为管理用以太网口M-GigabitEthernet0/0/0配置IP地址用于登录交换机 没有管理用以太网口的交换机，可为管理VLAN接口配置IP地址
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

配置步骤	配置项	配置数据	说明
			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	GE0/2：202.101.100.2/30	GE0/2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	GE0/1：10.10.100.2/24	GE0/1为出口路由器连接内网的接口
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

1.4 配置步骤

1.4.1 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) 通过Console口首次登录设备

将PC断电。

因为PC的串口不支持热插拔，请不要在PC带电的情况下，将串口线插入或者拔出PC。

使用产品随机附带的配置口电缆连接PC机和设备。请先将配置口电缆的DB-9（孔）插头插入PC机的9芯（针）串口中，再将RJ-45插头端插入设备的Console口中。

提示

- 连接时请认准接口上的标识，以免误插入其他接口。
- 在拆下配置口电缆时，请先拔出RJ-45端，再拔下DB-9端。

图2 将设备与 PC 通过配置口电缆进行连接

给 PC 上电。

在 PC 上打开终端仿真程序，按照表 2 要求设置终端参数。

表2 终端参数设置

参数	值
波特率	9600
数据位	8
停止位	1
奇偶校验	无
流量控制	无

给设备上电。

在设备自检结束后，用户可键入回车进入命令交互界面。

说明

缺省情况下，通过 Console 登录设备的认证方式为 None，即不需要用户名、密码即可登录设备。首次登录后，建议修改通过 Console 口登录设备的认证方式以增强设备的安全性。有关通过 Console 口登录设备的认证方式的详细介绍，请参见对应的配置手册中“基础配置指导”中的“登录设备”。

(2) 配置 IP 地址和 Telnet

创建 VLAN 5，并将接口 Ten-GigabitEthernet1/0/10 加入到 VLAN 5 中。假设连接网管的接口是 Ten-GigabitEthernet1/0/10。

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] sysname ACCSW1
[ACCSW1] vlan 5
[ACCSW1-vlan5] port ten-gigabitethernet 1/0/10
[ACCSW1-vlan5] quit
```

创建 VLAN 接口 5，并将接口 IP 地址配置为 10.10.1.1/24。

```
[ACCSW1] interface vlan-interface 5
[ACCSW1-Vlan-interface5] ip address 10.10.1.1 24
[ACCSW1-Vlan-interface5] quit
```

开启 Telnet 服务。

```
[ACCSW1] telnet server enable
```

配置 Telnet 登录使用 scheme 认证方式。

```
[ACCSW1] line vty 0 63
[ACCSW1-line-vty0-63] authentication-mode scheme
[ACCSW1-line-vty0-63] quit
```

创建本地用户，并配置本地用户的密码、用户角色和服务类型。本例中用户名和密码均为 admin，服务类型为 telnet，用户角色为 network-admin。

```
[ACCSW1] local-user admin
New local user added.
[ACCSW1-luser-manage-admin] password simple hello12345
[ACCSW1-luser-manage-admin] authorization-attribute user-role network-admin
[ACCSW1-luser-manage-admin] service-type telnet
[ACCSW1-luser-manage-admin] quit
```

在终端上通过 Telnet 登录到设备，输入正确的用户名和密码后，出现用户视图的命令行提示符表示登录成功。

```
C:\Users\Administrator> telnet 10.10.1.1
******************************************************************************
* Copyright (c) 2004-2019 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

login: admin
Password:
...
```

说明

上述终端输出信息是以 S5560X-30C-PWR-EI 设备（Release 1118P07 版本）为例，具体输出信息请以设备实际情况为准。

(3) 配置接口与 VLAN

在接入交换机上创建 VLAN 10。

```
[ACCSW1] vlan 10
[ACCSW1-vlan10] quit
```

配置连接 PC1 的接口 GigabitEthernet1/0/1，并配置为边缘端口。

```
[ACCSW1] interface gigabitethernet 1/0/1
[ACCSW1-GigabitEthernet1/0/1] port link-type access
[ACCSW1-GigabitEthernet1/0/1] port acess vlan 10
[ACCSW1-GigabitEthernet1/0/1] stp edged-port
[ACCSW1-GigabitEthernet1/0/1] quit
```

配置连接 PC2 的接口 GigabitEthernet1/0/2，并配置为边缘端口。

```
[ACCSW1] interface gigabitethernet 1/0/2
[ACCSW1-GigabitEthernet1/0/2] port link-type access
[ACCSW1-GigabitEthernet1/0/2] port acess vlan 10
[ACCSW1-GigabitEthernet1/0/2] stp edged-port
```

```
[ACCSW1-GigabitEthernet1/0/2] quit
```

配置连接打印机的接口 GigabitEthernet1/0/3，并配置为边缘端口。

```
[ACCSW1] interface gigabitethernet 1/0/3
[ACCSW1-GigabitEthernet1/0/3] port link-type access
[ACCSW1-GigabitEthernet1/0/3] port acess vlan 10
[ACCSW1-GigabitEthernet1/0/3] stp edged-port
[ACCSW1-GigabitEthernet1/0/3] quit
```

(4) 配置上行聚合

创建二层聚合接口 1，并配置该接口为动态聚合模式。

```
[ACCSW1] interface bridge-aggregation 1
[ACCSW1-Bridge-Aggregation1] link-aggregation mode dynamic
[ACCSW1-Bridge-Aggregation1] quit
```

分别将端口 Ten-GigabitEthernet1/0/7 至 Ten-GigabitEthernet1/0/8 加入到聚合组 1 中。

```
[ACCSW1] interface ten-gigabitethernet 1/0/7
[ACCSW1-Ten-GigabitEthernet1/0/7] port link-aggregation group 1
[ACCSW1-Ten-GigabitEthernet1/0/7] quit
[ACCSW1] interface ten-gigabitethernet 1/0/8
[ACCSW1-Ten-GigabitEthernet1/0/8] port link-aggregation group 1
[ACCSW1-Ten-GigabitEthernet1/0/8] quit
```

配置二层聚合接口 1 为 Trunk 端口，并允许 VLAN 10 的报文通过。

```
[ACCSW1] interface bridge-aggregation 1
[ACCSW1-Bridge-Aggregation1] port link-type trunk
[ACCSW1-Bridge-Aggregation1] port trunk permit vlan 10
[ACCSW1-Bridge-Aggregation1] quit
```

通过 **display link-aggregation verbose** 命令查看聚合接口 1 配置结果。

```
[ACCSW1] display link-aggregation verbose Bridge-Aggregation 1
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port, M -- Management port, R -- Reference port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation1
Creation Mode: Manual
Aggregation Mode: Dynamic
Loadsharing Type: Shar
Management VLANs: None
System ID: 0x8000, 000f-e267-6c6a
Local:
  Port                Status   Priority Index    Oper-Key              Flag
  XGE1/0/7            S        32768    61       2                     {ACDEF}
  XGE1/0/8            S        32768    62       2                     {ACDEF}
Remote:
  Actor               Priority Index    Oper-Key SystemID              Flag
  XGE1/0/7(R)         32768    111      2        0x8000, 000f-e267-57ad {ACDEF}
```

```
  XGE1/0/8            32768    112      2        0x8000, 000f-e267-57ad {ACDEF}
```

查看 ACCSW1 上 VLAN 10 的配置信息，验证以上配置是否生效。

```
[ACCSW1] display vlan 10
 VLAN ID: 10
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0010
 Name: VLAN 0010
 Tagged ports:   None
 Untagged ports:
    Bridge-Aggregation1
    GigabitEthernet1/0/1          GigabitEthernet1/0/2
    GigabitEthernet1/0/3          Ten-GigabitEthernet1/0/7
    Ten-GigabitEthernet1/0/8
```

(5) 配置 BPDU 保护功能

```
[ACCSW1] stp bpdu-protection
```

(6) 配置 DHCP snooping

开启 DHCP Snooping 功能。

```
[ACCSW1] dhcp snooping enable
```

指定二层聚合接口 1 为 DHCP Snooping 功能的信任端口。

```
[ACCSW1] interface bridge-aggregation 1
[ACCSW1-Bridge-Aggregation1] dhcp snooping trust
[ACCSW1-Bridge-Aggregation1] quit
```

(7) 配置 IP Source Guard

开启接口 GigabitEthernet1/0/1、GigabitEthernet1/0/2 的 IPv4 接口绑定功能，绑定源 IP 地址和 MAC 地址，并启用接口的 DHCP Snooping 表项记录功能。

```
[ACCSW1] interface gigabitethernet 1/0/1
[ACCSW1-GigabitEthernet1/0/1] ip verify source ip-address mac-address
[ACCSW1-GigabitEthernet1/0/1] dhcp snooping binding record
[ACCSW1-GigabitEthernet1/0/1] quit
[ACCSW1] interface gigabitethernet 1/0/2
[ACCSW1-GigabitEthernet1/0/2] ip verify source ip-address mac-address
[ACCSW1-GigabitEthernet1/0/2] dhcp snooping binding record
[ACCSW1-GigabitEthernet1/0/2] quit
```

(8) 保存配置

保存接入交换机上的配置（以 ACCSW1 为例）。

```
[ACCSW1] save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait...
Saved the current configuration to mainboard device successfully.
```

1.4.2 配置核心交换机

说明

有关“登录设备”、“配置 IP 地址和 Telnet”的配置方法，请参见“1.4.1 配置接入交换机”中的“通过 Console 口首次登录设备”、“配置 IP 地址和 Telnet”。

(1) 配置 VLAN 与 VLAN 接口

创建 VLAN 10、VLAN 20 和 VLAN 100。

```
<Sysname> system-view
[Sysname] sysname CORESW1
[CORESW1] vlan 10 20
[CORESW1] vlan 100
[CORESW1-vlan100] port gigabitethernet 1/0/1
[CORESW1-vlan100] quit
```

创建 VLAN 接口 10，并将接口的 IP 地址配置为 10.10.10.1/24。

```
[CORESW1] interface vlan-interface 10
[CORESW1-Vlan-interface10] ip address 10.10.10.1 24
[CORESW1-Vlan-interface10] quit
```

创建 VLAN 接口 20，并将接口的 IP 地址配置为 10.10.20.1/24。

```
[CORESW1] interface vlan-interface 20
[CORESW1-Vlan-interface20] ip address 10.10.20.1 24
[CORESW1-Vlan-interface20] quit
```

创建 VLAN 接口 100，并将接口的 IP 地址配置为 10.10.100.1/24。

```
[CORESW1] interface vlan-interface 100
[CORESW1-Vlan-interface100] ip address 10.10.100.1 24
[CORESW1-Vlan-interface100] quit
```

(2) 配置下行聚合，并查看配置

创建二层聚合接口 1，并配置该接口为动态聚合模式。

```
[CORESW1] interface bridge-aggregation 1
[CORESW1-Bridge-Aggregation1] link-aggregation mode dynamic
[CORESW1-Bridge-Aggregation1] quit
```

分别将端口 Ten-GigabitEthernet1/0/7 至 Ten-GigabitEthernet1/0/8 加入到聚合组 1 中。

```
[CORESW1] interface ten-gigabitethernet 1/0/7
[CORESW1-Ten-GigabitEthernet1/0/7] port link-aggregation group 1
[CORESW1-Ten-GigabitEthernet1/0/7] quit
[CORESW1] interface ten-gigabitethernet 1/0/8
[CORESW1-Ten-GigabitEthernet1/0/8] port link-aggregation group 1
[CORESW1-Ten-GigabitEthernet1/0/8] quit
```

配置二层聚合接口 1 为 Trunk 端口，并允许 VLAN 10 的报文通过。

```
[CORESW1] interface bridge-aggregation 1
[CORESW1-Bridge-Aggregation1] port link-type trunk
[CORESW1-Bridge-Aggregation1] port trunk permit vlan 10
[CORESW1-Bridge-Aggregation1] quit
```

通过 **display link-aggregation verbose** 命令查看聚合接口 1 配置结果。

```
[CORESW1] display link-aggregation verbose Bridge-Aggregation 1
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected, I -- Individual
Port: A -- Auto port, M -- Management port, R -- Reference port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation1
Creation Mode: Manual
Aggregation Mode: Dynamic
Loadsharing Type: Shar
Management VLANs: None
System ID: 0x8000, 000f-e267-6c6a
Local:
  Port                Status   Priority Index    Oper-Key               Flag
  XGE1/0/7(R)         S        32768    61       2                      {ACDEF}
  XGE1/0/8            S        32768    62       2                      {ACDEF}
Remote:
  Actor               Priority Index    Oper-Key SystemID               Flag
  XGE1/0/7            32768    111      2        0x8000, 000f-e267-57ad {ACDEF}
  XGE1/0/8            32768    112      2        0x8000, 000f-e267-57ad {ACDEF}
```

查看 CORESW1 上 VLAN 10、VLAN 100 的配置信息，验证以上配置是否生效。

```
[CORESW1] display vlan 10
 VLAN ID: 10
 VLAN type: Static
 Route interface: Configured
 IPv4 address: 10.10.10.1
 IPv4 subnet mask: 255.255.255.0
 Description: VLAN 0010
 Name: VLAN 0010
 Tagged ports:   None
 Untagged ports:
    Bridge-Aggregation1
    Ten-GigabitEthernet1/0/7      Ten-GigabitEthernet1/0/8
[CORESW1] display vlan 100
 VLAN ID: 100
 VLAN type: Static
 Route interface: Configured
 IPv4 address: 10.10.100.1
 IPv4 subnet mask: 255.255.255.0
 Description: VLAN 0100
 Name: VLAN 0100
 Tagged ports:   None
 Untagged ports:   None
```

(3) 配置 DHCP 服务器，并查看配置

开启 DHCP 服务。

```
[CORESW1] dhcp enable
```

创建 DHCP 地址池 1，用来为 10.10.10.0/24 网段内的客户端分配动态 IP 地址，并配置 DNS 服务器地址、出口网关、租期，为打印机配置固定的 IP 地址 10.10.10.254。

```
[CORESW1] dhcp server ip-pool 1
[CORESW1-dhcp-pool-1] network 10.10.10.0 mask 255.255.255.0
[CORESW1-dhcp-pool-1] gateway-list 10.10.10.1
[CORESW1-dhcp-pool-1] dns-list 202.101.100.199
[CORESW1-dhcp-pool-1] expired day 30
[CORESW1-dhcp-pool-1] static-bind ip-address 10.10.10.254 24 client-identifier
aabb-cccc-dd
[CORESW1-dhcp-pool-1] quit
```

创建 DHCP 地址池 2，用来为 10.10.20.0/24 网段内的客户端分配动态 IP 地址，并配置 DNS 服务器地址、出口网关、租期。

```
[CORESW1] dhcp server ip-pool 2
[CORESW1-dhcp-pool-2] network 10.10.20.0 mask 255.255.255.0
[CORESW1-dhcp-pool-2] gateway-list 10.10.20.1
[CORESW1-dhcp-pool-2] dns-list 202.101.100.199
[CORESW1-dhcp-pool-2] expired day 30
[CORESW1-dhcp-pool-2] quit
```

配置 VLAN 接口 10 和 VLAN 接口 20 工作在 DHCP 服务器模式，并指定接口引用的地址池。

```
[CORESW1] interface vlan-interface 10
[CORESW1-Vlan-interface10] dhcp select server
[CORESW1-Vlan-interface10] dhcp server apply ip-pool 1
[CORESW1-Vlan-interface10] quit
[CORESW1 interface vlan-interface 20
[CORESW1-Vlan-interface20] dhcp select server
[CORESW1-Vlan-interface20] dhcp server apply ip-pool 2
[CORESW1-Vlan-interface20] quit
```

使用 **display dhcp server pool** 命令查看 DHCP 地址池的信息。

```
[CORESW1] display dhcp server pool
Pool name: 1
  Network: 10.10.10.0 mask 255.255.255.0
  dns-list 202.101.100.199
  expired 30 0 0 0
  gateway-list 10.10.10.1
  static bindings:
    ip-address 10.10.10.254 mask 255.255.255.0
      client-identifier aabb-cccc-dd
Pool name: 2
  Network: 10.10.20.0 mask 255.255.255.0
  dns-list 202.101.100.199
  expired 30 0 0 0
  gateway-list 10.10.20.1
```

(4) 配置路由，并查看路由表

配置缺省静态路由，下一跳指向出口路由器，使内网数据可以发到出口路由器。

```
[CORESW1] ip route-static 0.0.0.0 0 10.10.100.2
```

使用 **display ip routing-table** 命令查看路由表信息。

```
[CORESW1] display ip routing-table

Destinations : 21       Routes : 21

Destination/Mask    Proto   Pre Cost        NextHop         Interface
0.0.0.0/0           Static  60  0           10.10.100.2     Vlan100
0.0.0.0/32          Direct  0   0           127.0.0.1       InLoop0
10.10.10.0/24       Direct  0   0           10.10.10.1      Vlan10
10.10.10.0/32       Direct  0   0           10.10.10.1      Vlan10
10.10.10.1/32       Direct  0   0           127.0.0.1       InLoop0
10.10.10.255/32     Direct  0   0           10.10.10.1      Vlan10
10.10.20.0/24       Direct  0   0           10.10.20.1      Vlan20
10.10.20.0/32       Direct  0   0           10.10.20.1      Vlan20
10.10.20.1/32       Direct  0   0           127.0.0.1       InLoop0
10.10.20.255/32     Direct  0   0           10.10.20.1      Vlan20
10.10.100.0/24      Direct  0   0           10.10.100.1     Vlan100
10.10.100.0/32      Direct  0   0           10.10.100.1     Vlan100
10.10.100.1/32      Direct  0   0           127.0.0.1       InLoop0
10.10.100.255/32    Direct  0   0           10.10.100.1     Vlan100
127.0.0.0/8         Direct  0   0           127.0.0.1       InLoop0
127.0.0.0/32        Direct  0   0           127.0.0.1       InLoop0
127.0.0.1/32        Direct  0   0           127.0.0.1       InLoop0
127.255.255.255/32  Direct  0   0           127.0.0.1       InLoop0
224.0.0.0/4         Direct  0   0           0.0.0.0         NULL0
```

(5) 保存配置

保存核心交换机 CORESW1 上的配置。

```
[CORESW1] save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait...
Saved the current configuration to mainboard device successfully.
```

1.4.3 配置出口路由器

说明

有关“登录设备”、“配置 IP 地址和 Telnet”的配置方法，请参见“1.4.1 配置接入交换机”中的“通过 Console 口首次登录设备”、“配置 IP 地址和 Telnet”。

(1) 配置公网接口和内网接口 IP

配置公网接口 IP 地址。

```
[Router] interface GigabitEthernet 0/2
[Router-GigabitEthernet0/2] ip address 202.101.100.2 30
[Router-GigabitEthernet0/2] quit
```

配置内网接口 IP 地址。

```
[Router] interface GigabitEthernet 0/1
[Router-GigabitEthernet0/1] ip address 10.10.100.2 24
[Router-GigabitEthernet0/1] quit
```

(2) 配置允许上网的 ACL

配置 ACL。

```
[Router] acl basic 2000
[Router-acl-ipv4-basic-2000] rule permiet source 10.10.10.0 0.0.0.255
[Router-acl-ipv4-basic-2000] rule permiet source 10.10.20.0 0.0.0.255
[Router-acl-ipv4-basic-2000] rule permiet source 10.10.100.0 0.0.0.255
[Router-acl-ipv4-basic-2000] quit
```

配置报文过滤。

```
[Router] interface gigabitethernet 0/1
[Router-GigabitEthernet0/1] packet-filter 2000 inbound
[Router-GigabitEthernet0/1] quit
[Router] packet-filter default deny
```

使用 **display acl** 命令查看 ACL 的配置信息。

```
[Router] display acl 2000
Basic IPv4 ACL 2000, 3 rules,
ACL's step is 5, start ID is 0
 rule 0 permit source 10.10.10.0 0.0.0.255
 rule 5 permit source 10.10.20.0 0.0.0.255
 rule 10 permit source 10.10.100.0 0.0.0.255
```

使用 **display packet-filter** 命令查看 ACL 在报文过滤中的应用情况。

```
[Router] display packet-filter interface gigabitethernet 0/1 inbound
Interface: GigabitEthernet 0/1
 Inbound policy:
  IPv4 ACL 2000
```

(3) 配置到内网和公网的路由

```
[Router] ip route-static 10.10.10.0 255.255.255.0 10.10.100.1
[Router] ip route-static 10.10.20.0 255.255.255.0 10.10.100.1
[Router] ip route-static 0.0.0.0 0.0.0.0 202.101.100.1
```

(4) 配置 DNS 解析

```
[Router] dns server 202.101.100.199
[Router] dns proxy enable
```

(5) 保存配置

保存出口路由器 Router 上的配置。

```
[Router] save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
```

```
Validating file. Please wait...
Saved the current configuration to mainboard device successfully.
```

1.5 验证配置

(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。

1.6 配置文件

- 接入交换机 ACCSW1：

```
#
 sysname ACCSW1
```

```
#
 telnet server enable
#
 dhcp snooping enable
#
vlan 5
#
vlan 10
#
 stp bpdu-protection
#
interface Bridge-Aggregation1
 port link-type trunk
 port trunk permit vlan 10
 link-aggregation mode dynamic
 dhcp snooping trust
#
interface Vlan-interface5
 ip address 10.10.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 10
 stp edged-port
 ip verify source ip-address mac-address
 dhcp snooping binding record
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 10
 stp edged-port
 ip verify source ip-address mac-address
 dhcp snooping binding record
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port access vlan 10
 stp edged-port
#
interface Ten-GigabitEthernet1/0/7
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 10
 port link-aggregation group 1
#
interface Ten-GigabitEthernet1/0/8
 port link-mode bridge
 port link-type trunk
```

```
 port trunk permit vlan 10
 port link-aggregation group 1
#
interface Ten-GigabitEthernet1/0/10
 port link-mode bridge
 port access vlan 5
#
line vty 0 63
 authentication-mode scheme
#
local-user admin class manage
 password hash
$h$6$/up8ijTTulpXAAkL$s9fFDXwWVzNd0j2F8Rq/ZQEiMbA2s8uW31kkcaDoGHoNyvE/zZLV9HoLp+i0+VcV6J
pm48ufEAxbuKvi6qtWmg==
 service-type telnet
 authorization-attribute user-role network-admin
#
```

- 接入交换机 ACCSW2：

ACCSW2 的配置文件除 VLAN ID、管理 VLAN 接口 IP 地址、聚合接口编号与 ACCSW1 不同外，其他配置与 ACCSW1 相同，配置文件略。

- 核心交换机 CORESW1：

```
#
 sysname CORESW1
#
vlan 10
#
vlan 20
#
vlan 100
#
dhcp server ip-pool 1
 gateway-list 10.10.10.1
 network 10.10.10.0 mask 255.255.255.0
 dns-list 202.101.100.199
 expired day 30
 static-bind ip-address 10.10.10.254 mask 255.255.255.0 client-identifier aaaa-cccc-dd
#
dhcp server ip-pool 2
 gateway-list 10.10.20.1
 network 10.10.20.0 mask 255.255.255.0
 dns-list 202.101.100.199
 expired day 30
#
interface Bridge-Aggregation1
 port link-type trunk
 port trunk permit vlan 10
 link-aggregation mode dynamic
```

```
#
interface Vlan-interface10
 ip address 10.10.10.1 255.255.255.0
 dhcp server apply ip-pool 1
#
interface Vlan-interface20
 ip address 10.10.20.1 255.255.255.0
 dhcp server apply ip-pool 2
#
interface Vlan-interface100
 ip address 10.10.100.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 100
#
interface Ten-GigabitEthernet1/0/7
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 10
 port link-aggregation group 1
#
interface Ten-GigabitEthernet1/0/8
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 10
 port link-aggregation group 1
#
 ip route-static 0.0.0.0 0 10.10.100.2
#
```

- 出口路由器 Router：

```
#
 sysname Router
#
 packet-filter default deny
#
 dns proxy enable
 dns server 202.101.100.199
#
interface GigabitEthernet0/1
 port link-mode route
 ip address 10.10.100.2 255.255.255.0
 packet-filter 2000 inbound
#
interface GigabitEthernet0/2
 port link-mode route
 ip address 202.101.100.2 255.255.255.252
#
```

```
 ip route-static 0.0.0.0 0 202.101.100.1
 ip route-static 10.10.10.0 24 10.10.100.1
 ip route-static 10.10.20.0 24 10.10.100.1
#
acl basic 2000
 rule 0 permit source 10.10.10.0 0.0.0.255
 rule 5 permit source 10.10.20.0 0.0.0.255
 rule 10 permit source 10.10.100.0 0.0.0.255
#
```

1.7 相关资料

- 产品配套“基础配置指导”中的“登录设备”。
- 产品配套“基础命令参考”中的“登录设备”。
- 产品配套“二层技术-以太网交换配置指导”中的“VLAN”。
- 产品配套“二层技术-以太网交换命令参考”中的“VLAN”。
- 产品配套“二层技术-以太网交换配置指导”中的“以太网链路聚合”。
- 产品配套“二层技术-以太网交换命令参考”中的“以太网链路聚合”。
- 产品配套“三层技术-IP 业务配置指导”中的“DHCP”。
- 产品配套“三层技术-IP 业务命令参考”中的“DHCP”。
- 产品配套“ACL 和 QoS 配置指导”中的“ACL”。
- 产品配套“ACL 和 QoS 命令参考”中的“ACL”。
- 产品配套“安全配置指导”中的“IP Source Guard”。
- 产品配套“安全命令参考”中的“IP Source Guard”。

2 中小型园区典型组网

2.1 简介

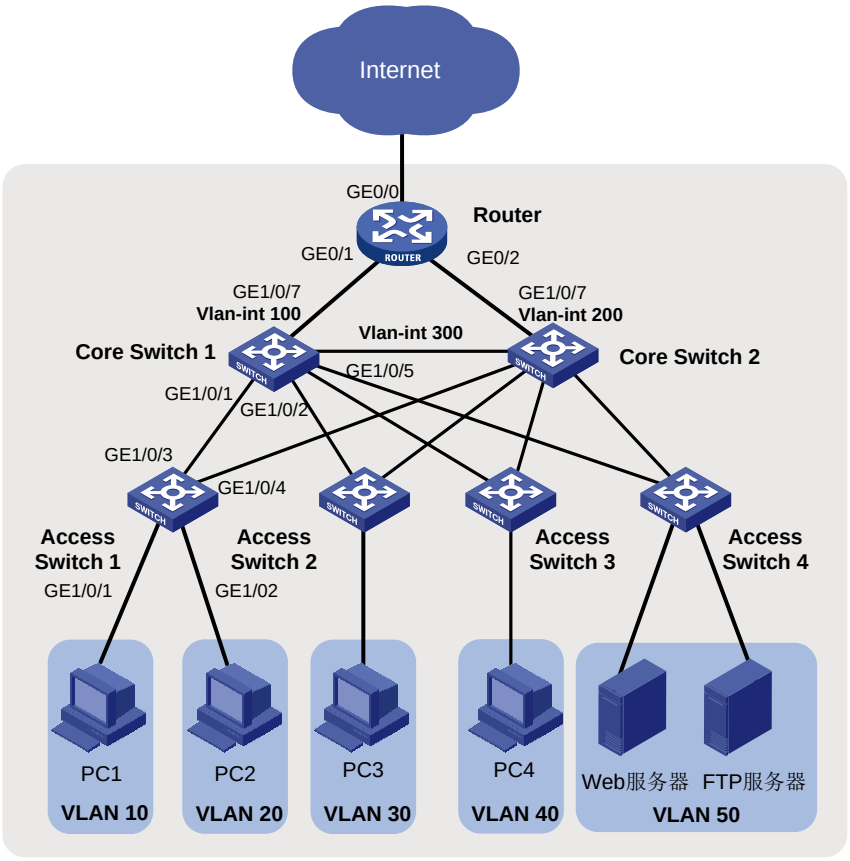
本案例介绍中小型园区典型组网配置。

2.2 组网需求

如图 3 所示，在中小园区中，S5130 系列或 S5130S 系列以太网交换机通常部署在网络的接入层，S5560X 系列或 S6520X 系列以太网交换机通常部署在网络的核心，出口路由器一般选用 MSR 系列路由器。

- 核心交换机配置 VRRP 保证网络可靠性。
- 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 接口三层互通。
- 核心交换机作为 DHCP 服务器，为园区网用户分配 IP 地址。
- 接入交换机上配置 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。
- 在出口路由器上对双向流量配置基于 IP 的限速。

图3 中小型园区典型组网图



2.3 配置思路与数据规划

登录设备后，本例所需配置如下，具体数据规划请参见 2.3 (7)表 3。

(1) 登录设备

(2) 配置管理 IP 地址和 Telnet 功能

(3) 配置网络互连互通

(4) 配置核心交换机 DHCP 功能

(5) 配置核心交换机 OSPF 功能

(6) 配置核心交换可靠性功能

(7) 配置限速

表3 配置数据表

配置步骤	配置项	配置数据	说明
登录设备	通过Console口登录	设置传输速率等通信参数	PC端通过终端仿真软件登录设备
配置管理IP和telnet功能	管理VLAN	VLAN 5	交换机缺省VLAN为VLAN 1。一般不将其配置为管理VLAN 本文将VLAN5配置为管理VLAN
	管理用以太网口或管理VLAN接口IP地址	10.10.1.1/24	此处以ACCSW1为例。 有管理用以太网口的交换机，可为管理用以太网口M-GigabitEthernet0/0/0配置IP地址用于登录交换机 没有管理用以太网口的交换机，可为管理VLAN接口配置IP地址
配置接口和VLAN	端口类型	连接交换机的端口建议设置为trunk，连接PC的端口设置为access。	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 hybrid类型端口是通用端口，既可以用来连接交换机，也可用来连接PC
	VLAN ID	ACCSW1：VLAN 10、20 CORESW1：VLAN 10、20、30、40、50、100、300	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1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	CORESW1、CORESW2	在核心交换机1、核心交换机2上部署DHCPServer
	地址池	VLAN 10：ip pool 10 VLAN 20：ip pool 20	部门A的终端从ip pool 10中获取IP地址 部门B的终端从ip pool 20中获

配置步骤	配置项	配置数据	说明
			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	以CORESW1为例： Vlan-int10：192.168.10.1/24 Vlan-int20：192.168.20.1/24 Vlan-int100：172.16.1.1/24 Vlan-int300：172.16.3.1/24	Vlan-int100用于核心交换机1与园区出口路由器对接。Vlan-int300用于核心交换机1与核心交换机2对接 在核心交换机1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1互访
配置出口路由器	公网接口的IP地址	GE0/0：202.101.100.2/30	GE0/0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Internet
	DNS地址	202.101.100.199	DNS服务器用于将域名解析成IP地址
	内网接口的IP地址	GE0/1：172.16.1.2/24 GE0/2：172.16.2.2/24	GE0/1、GE0/2为出口路由器连接内网的接口，GE0/1连接主设备，GE0/2连接备设备
在接入交换机上配置DHCP Snooping和IP Source Guard	信任接口	GE1/0/1 GE1/0/2	配置信任接口后，用户只会接收从信任接口进入的DHCP报文，防止内网私接小路由器为主机分配IP地址

2.4 配置步骤

2.4.1 配置接入交换机

说明

接入交换机 ACCSW1、ACCSW2、ACCSW3 和 ACCSW4 的配置基本相同。本小节以配置接入交换机 ACCSW1 为例说明配置方法。

(1) 通过 Console 口首次登录设备

将 PC 断电。

因为 PC 的串口不支持热插拔，请不要在 PC 带电的情况下，将串口线插入或者拔出 PC。

使用产品随机附带的配置口电缆连接 PC 机和设备。请先将配置口电缆的 DB-9（孔）插头插入 PC 机的 9 芯（针）串口中，再将 RJ-45 插头端插入设备的 Console 口中。

提示

- 连接时请认准接口上的标识，以免误插入其他接口。
- 在拆下配置口电缆时，请先拔出 RJ-45 端，再拔下 DB-9 端。

图4 将设备与 PC 通过配置口电缆进行连接

给 PC 上电。

在 PC 上打开终端仿真程序，按照表 4 要求设置终端参数。

表4 终端参数设置

参数	值
波特率	9600
数据位	8
停止位	1
奇偶校验	无
流量控制	无

给设备上电。

在设备自检结束后，用户可键入回车进入命令交互界面。

说明

缺省情况下，通过 Console 登录设备的认证方式为 None，即不需要用户名、密码即可登录设备。首次登录后，建议修改通过 Console 口登录设备的认证方式以增强设备的安全性。有关通过 Console 口登录设备的认证方式的详细介绍，请参见对应的配置手册中“基础配置指导”中的“登录设备”。

(2) 配置 IP 地址和 Telnet

创建 VLAN 5，并将接口 Ten-GigabitEthernet1/0/10 加入到 VLAN 5 中。假设连接网管的接口是 Ten-GigabitEthernet1/0/10。

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] sysname ACCSW1
[ACCSW1] vlan 5
[ACCSW1-vlan5] port ten-gigabitethernet 1/0/10
[ACCSW1-vlan5] quit
```

创建 VLAN 接口 5，并将接口 IP 地址配置为 10.10.1.1/24。

```
[ACCSW1] interface vlan-interface 5
[ACCSW1-Vlan-interface5] ip address 10.10.1.1 24
[ACCSW1-Vlan-interface5] quit
```

开启 Telnet 服务 。

```
[ACCSW1] telnet server enable
```

配置 Telnet 登录使用 scheme 认证方式。

```
[ACCSW1] line vty 0 63
[ACCSW1-line-vty0-63] authentication-mode scheme
[ACCSW1-line-vty0-63] quit
```

创建本地用户，并配置本地用户的密码、用户角色和服务类型。本例中用户名和密码均为 admin，服务类型为 telnet，用户角色为 network-admin。

```
[ACCSW1] local-user admin
New local user added.
[ACCSW1-luser-manage-admin] password simple hello12345
[ACCSW1-luser-manage-admin] authorization-attribute user-role network-admin
[ACCSW1-luser-manage-admin] service-type telnet
[ACCSW1-luser-manage-admin] quit
```

在终端上通过 Telnet 登录到设备，输入正确的用户名和密码后，出现用户视图的命令行提示符表示登录成功。

```
C:\Users\Administrator> telnet 10.10.1.1
******************************************************************************
* Copyright (c) 2004-2019 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

login: admin
Password:
...
```

说明

上述终端输出信息是以 S5560X-30C-PWR-EI 设备（Release 1118P07 版本）为例，具体输出信息请以设备实际情况为准。

(3) 配置接口与 VLAN

在接入交换机上创建 VLAN 10 和 VLAN 20。

```
[ACCSW1] vlan 10 20
```

将连接 PC1 的接口 GigabitEthernet1/0/1 加入 VLAN 10，并配置为边缘端口。

```
[ACCSW1] interface gigabitethernet 1/0/1
[ACCSW1-GigabitEthernet1/0/1] port link-type access
[ACCSW1-GigabitEthernet1/0/1] port acess vlan 10
[ACCSW1-GigabitEthernet1/0/1] stp edged-port
[ACCSW1-GigabitEthernet1/0/1] quit
```

将连接 PC1 的接口 GigabitEthernet1/0/2 加入 VLAN 20，并配置为边缘端口。

```
[ACCSW1] interface gigabitethernet 1/0/2
[ACCSW1-GigabitEthernet1/0/2] port link-type access
[ACCSW1-GigabitEthernet1/0/2] port acess vlan 20
[ACCSW1-GigabitEthernet1/0/2] stp edged-port
[ACCSW1-GigabitEthernet1/0/2] quit
```

将接口 GigabitEthernet1/0/3 和 GigabitEthernet1/0/4 的链路类型配置为 Trunk 并允许 VLAN 10 和 VLAN 20 的报文通过。

```
[ACCSW1] interface gigabitethernet 1/0/3
[ACCSW1-GigabitEthernet1/0/3] port link-type trunk
[ACCSW1-GigabitEthernet1/0/3] port trunk permit vlan 10 20
[ACCSW1-GigabitEthernet1/0/3] quit
[ACCSW1] interface gigabitethernet 1/0/4
[ACCSW1-GigabitEthernet1/0/4] port link-type trunk
[ACCSW1-GigabitEthernet1/0/4] port trunk permit vlan 10 20
[ACCSW1-GigabitEthernet1/0/4] quit
```

查看 ACCSW1 上 VLAN 10 和 VLAN 20 的配置信息。

```
[ACCSW1] display vlan 10
 VLAN ID: 10
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0010
 Name: VLAN 0010
 Tagged ports:
    GigabitEthernet1/0/3
    GigabitEthernet1/0/4
 Untagged ports:
    GigabitEthernet1/0/1
[ACCSW1] display vlan 20
 VLAN ID: 20
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0020
 Name: VLAN 0020
 Tagged ports:
    GigabitEthernet1/0/3
    GigabitEthernet1/0/4
 Untagged ports:
    GigabitEthernet1/0/2
```

(4) 配置 BPDU 保护功能

```
[ACCSW1] stp bpdu-protection
```

(5) 配置 DHCP snooping

开启 DHCP Snooping 功能。

```
[ACCSW1] dhcp snooping enable
```

指定 GigabitEthernet1/0/3 为 DHCP Snooping 功能的信任端口。

```
[ACCSW1] interface gigabitethernet 1/0/3
[ACCSW1-GigabitEthernet1/0/3] dhcp snooping trust
[ACCSW1-GigabitEthernet1/0/3] quit
```

(6) 配置 IP Source Guard

开启接口 GigabitEthernet1/0/1、GigabitEthernet1/0/2 的 IPv4 接口绑定功能，绑定源 IP 地址和 MAC 地址，并启用接口的 DHCP Snooping 表项记录功能。

```
[ACCSW1] interface gigabitethernet 1/0/1
[ACCSW1-GigabitEthernet1/0/1] ip verify source ip-address mac-address
[ACCSW1-GigabitEthernet1/0/1] dhcp snooping binding record
[ACCSW1-GigabitEthernet1/0/1] quit
[ACCSW1] interface gigabitethernet 1/0/2
[ACCSW1-GigabitEthernet1/0/2] ip verify source ip-address mac-address
[ACCSW1-GigabitEthernet1/0/2] dhcp snooping binding record
[ACCSW1-GigabitEthernet1/0/2] quit
```

(7) 保存配置

保存接入交换机上的配置（以 ACCSW1 为例）。

```
[ACCSW1] save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait...
Saved the current configuration to mainboard device successfully.
```

2.4.2 配置核心交换机

说明

核心交换机 CORESW1 和 CORESW2 的配置基本相同。本小节如无特殊说明，以配置核心交换机 CORESW1 为例说明配置方法。

(1) 配置接口与 VLAN

创建 VLAN 10、VLAN 20、VLAN 30、VLAN 40、VLAN 50、VLAN 100 和 VLAN 300。

```
<Sysname> system-view
[Sysname] sysname CORESW1
[CORESW1] vlan 10 20 30 40 50 100 300
```

配置接口 GigabitEthernet1/0/1 的链路类型为 Trunk，并允许 VLAN 10 和 20 的报文通过。

```
[CORESW1] interface gigabitethernet 1/0/1
[CORESW1-GigabitEthernet1/0/1] port link-type trunk
[CORESW1-GigabitEthernet1/0/1] port trunk permit vlan 10 20
[CORESW1-GigabitEthernet1/0/1] quit
```

配置接口 GigabitEthernet1/0/5 的链路类型为 Trunk，并允许 VLAN 300 的报文通过。

```
[CORESW1] interface gigabitethernet 1/0/5
[CORESW1-GigabitEthernet1/0/5] port link-type trunk
```

```
[CORESW1-GigabitEthernet1/0/5] port trunk permit vlan 300
[CORESW1-GigabitEthernet1/0/5] quit
```

配置其他接口的链路类型并允许对应的 VLAN 通过，具体配置过程略。

(2) 配置 VLAN 接口

创建 VLAN 接口 10，并将接口的 IP 地址配置为 192.168.10.1/24。

```
[CORESW1] interface vlan-interface 10
[CORESW1-Vlan-interface10] ip address 192.168.10.1 24
[CORESW1-Vlan-interface10] quit
```

创建 VLAN 接口 20，并将接口的 IP 地址配置为 192.168.20.1/24。

```
[CORESW1] interface vlan-interface 20
[CORESW1-Vlan-interface20] ip address 192.168.20.1 24
[CORESW1-Vlan-interface20] quit
```

创建 VLAN 接口 100，并将接口的 IP 地址配置为 172.16.1.1/24。

```
[CORESW1] interface vlan-interface 100
[CORESW1-Vlan-interface100] ip address 172.16.1.1 24
[CORESW1-Vlan-interface100] quit
```

创建 VLAN 接口 300，并将接口的 IP 地址配置为 172.16.3.1/24。

```
[CORESW1] interface vlan-interface 300
[CORESW1-Vlan-interface300] ip address 172.16.3.1 24
[CORESW1-Vlan-interface300] quit
```

创建其他 VLAN 接口，并配置 IP 地址，具体配置过程略。

查看 CORESW1 上 VLAN 10、VLAN 20、VLAN 100、VLAN 300 的配置信息。

```
[CORESW1] display vlan 10
 VLAN ID: 10
 VLAN type: Static
 Route interface: Configured
 IPv4 address: 192.168.10.1
 IPv4 subnet mask: 255.255.255.0
 Description: VLAN 0010
 Name: VLAN 0010
 Tagged ports:
    GigabitEthernet1/0/1
 Untagged ports:   None
[CORESW1] display vlan 20
 VLAN ID: 20
 VLAN type: Static
 Route interface: Configured
 IPv4 address: 192.168.20.1
 IPv4 subnet mask: 255.255.255.0
 Description: VLAN 0020
 Name: VLAN 0020
 Tagged ports:
    GigabitEthernet1/0/2
 Untagged ports:   None
[CORESW1] display vlan 100
 VLAN ID: 100
```

```
 VLAN type: Static
 Route interface: Configured
 IPv4 address: 172.16.1.1
 IPv4 subnet mask: 255.255.255.0
 Description: VLAN 0100
 Name: VLAN 0100
 Tagged ports:   None
 Untagged ports:   None
[CORESW1] display vlan 300
 VLAN ID: 300
 VLAN type: Static
 Route interface: Configured
 IPv4 address: 172.16.3.1
 IPv4 subnet mask: 255.255.255.0
 Description: VLAN 0300
 Name: VLAN 0300
 Tagged ports:
    GigabitEthernet1/0/5
 Untagged ports:   None
```

(3) 配置 VRRP 备份

正常情况下内网用户流量都上送到 CORESW1 进行处理，只有当 CORESW1 或 CORESW1 的上行链路出故障之后，VRRP 备份组切换 CORESW2 为主设备，内网用户流量上送到 CORESW2。

在 CORESW1 上配置 VRRP 备份组功能。

创建 VRRP 备份组 1，并配置 VRRP 备份组 1 的虚拟 IP 地址为 172.16.3.10。

```
[CORESW1] interface vlan-interface 300
[CORESW1-Vlan-interface300] vrrp vrid 1 virtual-ip 172.16.3.10
```

设置 CORESW1 在 VRRP 备份组 1 中的优先级为 120，高于 CORESW2 的优先级 100，以保证 CORESW1 成为 Master 负责转发流量。

```
[CORESW1-Vlan-interface300] vrrp vrid 1 priority 120
```

设置 CORESW1 工作在抢占方式，以保证 CORESW1 故障恢复后，能再次抢占成为 Master，即只要 CORESW1 正常工作，就由 CORESW1 负责转发流量。为了避免频繁地进行状态切换，配置抢占延迟时间为 5000 厘秒。

```
[CORESW1-Vlan-interface300] vrrp vrid 1 preempt-mode delay 5000
[CORESW1-Vlan-interface300] quit
```

创建和上行接口 GigabitEthernet1/0/7 物理状态关联的 Track 项 1。如果 Track 项的状态为 Negative，则说明 CORESW1 的上行接口出现故障。

```
[CORESW1] track 1 interface gigabitethernet 1/0/7
[CORESW1-track-1] quit
```

设置监视 Track 项。

```
[CORESW1] interface vlan-interface 300
[CORESW1-Vlan-interface300] vrrp vrid 1 track 1 priority reduced 30
```

在 CORESW2 上配置 VRRP 备份组功能。创建 VRRP 备份组 1，并配置 VRRP 备份组 1 的虚拟 IP 地址为 172.16.3.10。

```
<Sysname> system-view
[Sysname] sysname CORESW2
[CORESW2] interface vlan-interface 300
[CORESW2-Vlan-interface300] vrrp vrid 1 virtual-ip 172.16.3.10
```

配置 CORESW2 在 VRRP 备份组 1 中的优先级为 100。

```
[CORESW2-Vlan-interface300] vrrp vrid 1 priority 100
```

配置 CORESW2 工作在抢占方式，抢占延迟时间为 5000 厘秒。

```
[CORESW2-Vlan-interface300] vrrp vrid 1 preempt-mode delay 5000
[CORESW2-Vlan-interface300] quit
```

在 CORESW1 上使用 **display vrrp verbose** 命令查询 VRRP 备份组信息。

```
[CORESW1] display vrrp verbose
IPv4 Virtual Router Information:
 Running mode : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface300
     VRID             : 1                 Adver Timer  : 100
     Admin Status     : Up                State        : Master
     Config Pri       : 120               Running Pri  : 120
     Preempt Mode     : Yes               Delay Time   : 5000
     Auth Type        : None
     Virtual IP       : 172.16.3.10
     Virtual MAC      : 0000-5e00-0101
     Master IP        : 172.16.3.1
   VRRP Track Information:
     Track Object   : 1                 State : Positive   Pri Reduced : 30
```

在 CORESW2 上使用 **display vrrp verbose** 命令查询 VRRP 备份组信息。

```
[CORESW2] display vrrp verbose
IPv4 Virtual Router Information:
 Running mode : Standard
 Total number of virtual routers : 1
   Interface Vlan-interface300
     VRID             : 1                 Adver Timer  : 100
     Admin Status     : Up                State        : Backup
     Config Pri       : 100               Running Pri  : 100
     Preempt Mode     : Yes               Delay Time   : 5000
     Become Master    : 27810ms left
     Auth Type        : None
     Virtual IP       : 172.16.3.10
     Virtual MAC      : 0000-5e00-0101
     Master IP        : 172.16.3.1
```

由此可见，VRRP 备份组创建成功，CORESW1 为 Master 设备，CORESW2 为 Backup 设备。

(4) 配置 DHCP 服务器，并查看配置

开启 DHCP 服务。

```
[CORESW1] dhcp enable
```

创建 DHCP 地址池 1，用来为 192.168.10.0/24 网段内的客户端分配动态 IP 地址，并配置 DNS 服务器地址、出口网关、租期，为打印机配置固定的 IP 地址 192.168.10.254。

```
[CORESW1] dhcp server ip-pool 1
[CORESW1-dhcp-pool-1] network 192.168.10.0 mask 255.255.255.0
[CORESW1-dhcp-pool-1] gateway-list 192.168.10.1
[CORESW1-dhcp-pool-1] dns-list 202.101.100.199
[CORESW1-dhcp-pool-1] expired day 30
[CORESW1-dhcp-pool-1] static-bind ip-address 192.168.10.254 24 client-identifier
aabb-cccc-dd
[CORESW1-dhcp-pool-1] quit
```

创建 DHCP 地址池 2，用来为 192.168.20.0/24 网段内的客户端分配动态 IP 地址，并配置 DNS 服务器地址、出口网关、租期。

```
[CORESW1] dhcp server ip-pool 2
[CORESW1-dhcp-pool-2] network 192.168.20.0 mask 255.255.255.0
[CORESW1-dhcp-pool-2] gateway-list 192.168.20.1
[CORESW1-dhcp-pool-2] dns-list 202.101.100.199
[CORESW1-dhcp-pool-2] expired day 30
[CORESW1-dhcp-pool-2] quit
```

配置 VLAN 接口 10 和 VLAN 接口 20 工作在 DHCP 服务器模式。

```
[CORESW1] interface vlan-interface 10
[CORESW1-Vlan-interface10] dhcp select server
[CORESW1-Vlan-interface10] quit
[CORESW1 interface vlan-interface 20
[CORESW1-Vlan-interface20] dhcp select server
[CORESW1-Vlan-interface20] quit
```

使用 **display dhcp server pool** 命令查看 DHCP 地址池的信息。

```
[CORESW1] display dhcp server pool
Pool name: 1
  Network: 192.168.10.0 mask 255.255.255.0
  expired 30 0 0 0
  gateway-list 192.168.10.1
  static bindings:
    ip-address 192.168.10.254 mask 255.255.255.0
      client-identifier aabb-cccc-dd
Pool name: 2
  Network: 192.168.20.0 mask 255.255.255.0
  expired 30 0 0 0
  gateway-list 192.168.20.1
```

(5) 配置 OSPF

CORESW1 的 OSPF 配置。

```
[CORESW1] ospf 100 router-id 2.2.2.2
[CORESW1-ospf-100] area 0
[CORESW1-ospf-100-area-0.0.0.0] network 172.16.1.0 0.0.0.255
[CORESW1-ospf-100-area-0.0.0.0] network 172.16.3.0 0.0.0.255
[CORESW1-ospf-100-area-0.0.0.0] network 192.168.10.0 0.0.0.255
[CORESW1-ospf-100-area-0.0.0.0] network 192.168.20.0 0.0.0.255
```

```
[CORESW1-ospf-100-area-0.0.0.0] quit
[CORESW1-ospf-100] quit
```

CORESW2 的 OSPF 配置。

```
[CORESW2] ospf 100 router-id 3.3.3.3
[CORESW2-ospf-100] area 0
[CORESW2-ospf-100-area-0.0.0.0] network 172.16.2.0 0.0.0.255
[CORESW2-ospf-100-area-0.0.0.0] network 172.16.3.0 0.0.0.255
[CORESW2-ospf-100-area-0.0.0.0] network 192.168.10.0 0.0.0.255
[CORESW2-ospf-100-area-0.0.0.0] network 192.168.20.0 0.0.0.255
[CORESW2-ospf-100-area-0.0.0.0] quit
[CORESW2-ospf-100] quit
```

使用 **display ospf peer** 命令查看 CORESW1 上的 OSPF 邻居信息。

```
[CORESW1] display ospf peer

         OSPF Process 100 with Router ID 2.2.2.2
               Neighbor Brief Information

 Area: 0.0.0.0
 Router ID       Address         Pri Dead-Time  State             Interface
 3.3.3.3         172.16.3.2      1   33         Full/DR           Vlan300
```

使用 **display ospf peer** 命令查看 CORESW2 上的 OSPF 邻居信息。

```
[CORESW2] display ospf peer

         OSPF Process 100 with Router ID 3.3.3.3
               Neighbor Brief Information

 Area: 0.0.0.0
 Router ID       Address         Pri Dead-Time  State             Interface
 2.2.2.2         172.16.3.1      1   36         Full/BDR          Vlan300
```

(6) 保存配置

保存核心交换机上的配置（以 CORESW1 为例）。

```
[CORESW1] save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait...
Saved the current configuration to mainboard device successfully.
```

2.4.3 配置出口路由器

(1) 配置内网接口和公网接口 IP

配置内网接口 IP 地址。

```
[Router] interface GigabitEthernet 0/1
[Router-GigabitEthernet0/1] ip address 172.16.1.2 24
[Router-GigabitEthernet0/1] quit
```

```
[Router] interface GigabitEthernet 0/2
[Router-GigabitEthernet0/2] ip address 172.16.2.2 24
[Router-GigabitEthernet0/2] quit
```

配置公网接口 IP 地址。

```
[Router] interface GigabitEthernet 0/0
[Router-GigabitEthernet0/0] ip address 202.101.100.2 30
[Router-GigabitEthernet0/0] quit
```

(2) 配置允许上网的 ACL

配置 ACL。

```
[Router] acl basic 2000
[Router-acl-ipv4-basic-2000] rule permit source 192.168.10.0 0.0.0.255
[Router-acl-ipv4-basic-2000] rule permit source 192.168.20.0 0.0.0.255
[Router-acl-ipv4-basic-2000] rule permit source 172.16.1.0 0.0.0.255
[Router-acl-ipv4-basic-2000] rule permit source 172.16.2.0 0.0.0.255
[Router-acl-ipv4-basic-2000] rule permit source 172.16.3.0 0.0.0.255
[Router-acl-ipv4-basic-2000] quit
```

配置报文过滤。

```
[Router] interface gigabitethernet 0/1
[Router-GigabitEthernet0/1] packet-filter 2000 inbound
[Router-GigabitEthernet0/1] quit
[Router] interface gigabitethernet 0/2
[Router-GigabitEthernet0/2] packet-filter 2000 inbound
[Router-GigabitEthernet0/2] quit
[Router] packet-filter default deny
```

使用 **display acl** 命令查看 ACL 的配置信息。

```
[Router] display acl 2000
Basic IPv4 ACL 2000, 5 rules,
ACL's step is 5, start ID is 0
 rule 0 permit source 192.168.10.0 0.0.0.255
 rule 5 permit source 192.168.20.0 0.0.0.255
 rule 10 permit source 172.16.1.0 0.0.0.255
 rule 15 permit source 172.16.2.0 0.0.0.255
 rule 20 permit source 172.16.3.0 0.0.0.255
```

使用 **display packet-filter** 命令查看 ACL 在报文过滤中的应用情况。

```
[Router] display packet-filter interface gigabitethernet 0/1 inbound
Interface: GigabitEthernet0/1
 Inbound policy:
  IPv4 ACL 2000
[Router] display packet-filter interface gigabitethernet 0/2 inbound
Interface: GigabitEthernet0/2
 Inbound policy:
  IPv4 ACL 2000
```

(3) 配置 OSPF

配置一条缺省路由指向运营商。

```
[Router] ip route-static 0.0.0.0 0.0.0.0 202.101.100.1
```

出口路由器的 OSPF 配置。在 OSPF 中引入缺省路由，从而连接内网和公网。

```
[Router] ospf 10 router-id 1.1.1.1
[Router-ospf-10] default-route-advertise always
[Router-ospf-10] area 0
[Router-ospf-10-area-0.0.0.0] network 172.16.1.0 0.0.0.255
[Router-ospf-10-area-0.0.0.0] network 172.16.2.0 0.0.0.255
[Router-ospf-10-area-0.0.0.0] quit
[Router-ospf-10] quit
```

使用 **display ospf peer** 命令查看 Router 上的 OSPF 邻居信息。

```
[Router] display ospf peer

         OSPF Process 100 with Router ID 1.1.1.1
               Neighbor Brief Information

 Area: 0.0.0.0
 Router ID       Address         Pri Dead-Time  State             Interface
 2.2.2.2         172.16.1.1      1   31         Full/DR           GE0/1
 3.3.3.3         172.16.2.1      1   39         Full/BDR          GE0/2
```

使用 **display ospf routing** 命令查看 CORESW1 上的 OSPF 路由表信息。

```
[CORESW1] display ospf routing

         OSPF Process 100 with Router ID 2.2.2.2
                  Routing Table

                Topology base (MTID 0)

 Routing for network
 Destination        Cost     Type    NextHop         AdvRouter       Area
 172.16.1.0/24      1        Transit 0.0.0.0         2.2.2.2         0.0.0.0
 172.16.2.0/24      2        Transit 172.16.3.2      1.1.1.1         0.0.0.0
 172.16.2.0/24      2        Transit 172.16.1.2      1.1.1.1         0.0.0.0
 172.16.3.0/24      1        Transit 0.0.0.0         3.3.3.3         0.0.0.0

 Routing for ASEs
 Destination        Cost     Type    Tag         NextHop         AdvRouter
 0.0.0.0/0          1        Type2   1           172.16.1.2      1.1.1.1

 Total nets: 5
 Intra area: 4  Inter area: 0  ASE: 1  NSSA: 0
```

使用 **display ospf routing** 命令查看 CORESW2 上的 OSPF 路由表信息。

```
[CORESW2] display ospf routing

         OSPF Process 100 with Router ID 3.3.3.3
                  Routing Table

                Topology base (MTID 0)
```

```
 Routing for network
 Destination        Cost     Type    NextHop         AdvRouter       Area
 172.16.1.0/24      2        Transit 172.16.3.1      2.2.2.2         0.0.0.0
 172.16.1.0/24      2        Transit 172.16.2.2      2.2.2.2         0.0.0.0
 172.16.2.0/24      1        Transit 0.0.0.0         1.1.1.1         0.0.0.0
 172.16.3.0/24      1        Transit 0.0.0.0         3.3.3.3         0.0.0.0

 Routing for ASEs
 Destination        Cost     Type    Tag         NextHop         AdvRouter
 0.0.0.0/0          1        Type2   1           172.16.2.2      1.1.1.1

 Total nets: 5
 Intra area: 4  Inter area: 0  ASE: 1  NSSA: 0
```

(4) 配置 DNS 解析

```
[Router] dns server 202.101.100.199
[Router] dns proxy enable
```

(5) 配置基于 IP 或 IP 网段的限速

配置 CAR 列表。

```
[Router] qos carl 1 source-ip-address range 192.168.10.1 to 192.168.10.254 per-address
shared-bandwidth
[Router] qos carl 2 source-ip-address range 192.168.20.1 to 192.168.20.254 per-address
shared-bandwidth
[Router] qos carl 3 destination-ip-address range 192.168.10.1 to 192.168.10.254
per-address shared-bandwidth
[Router] qos carl 4 destination-ip-address range 192.168.20.1 to 192.168.20.254
per-address shared-bandwidth
```

配置限速。

```
[Router] interface gigabitethernet 0/1
[Router-GigabitEthernet0/1] qos car inbound carl 1 cir 512
[Router-GigabitEthernet0/1] qos car inbound carl 2 cir 512
[Router-GigabitEthernet0/1] qos car outbound carl 3 cir 512
[Router-GigabitEthernet0/1] qos car outbound carl 4 cir 512
[Router-GigabitEthernet0/1] quit
[Router] interface gigabitethernet 0/2
[Router-GigabitEthernet0/2] qos car inbound carl 1 cir 512
[Router-GigabitEthernet0/2] qos car inbound carl 2 cir 512
[Router-GigabitEthernet0/2] qos car outbound carl 3 cir 512
[Router-GigabitEthernet0/2] qos car outbound carl 4 cir 512
[Router-GigabitEthernet0/2] quit
```

使用 **display qos carl** 命令查看 CAR 列表。

```
[Router] display qos carl
List  Rules
1     source-ip-address range 192.168.10.1 to 192.168.10.254 per-address
shared-bandwidth
2     source-ip-address range 192.168.20.1 to 192.168.20.254 per-address
shared-bandwidth
```

```
3     destination-ip-address range 192.168.10.1 to 192.168.10.254 per-address
shared-bandwidth
4     destination-ip-address range 192.168.20.1 to 192.168.20.254 per-address
shared-bandwidth
```

使用 **display qos car interface** 命令查看接口的流量监管配置情况和统计信息。

```
[Router] display qos car interface gigabitethernet 0/1
Interface: GigabitEthernet0/1
 Direction: inbound
  Rule: If-match carl 1
   CIR 512 (kbps), CBS 32000 (Bytes), EBS 0 (Bytes)
   Green action  : pass
   Yellow action : pass
   Red action    : discard
   Green packets : 0 (Packets), 0 (Bytes)
   Yellow packets: 0 (Packets), 0 (Bytes)
   Red packets   : 0 (Packets), 0 (Bytes)
  Rule: If-match carl 2
   CIR 512 (kbps), CBS 32000 (Bytes), EBS 0 (Bytes)
   Green action  : pass
   Yellow action : pass
   Red action    : discard
   Green packets : 0 (Packets), 0 (Bytes)
   Yellow packets: 0 (Packets), 0 (Bytes)
   Red packets   : 0 (Packets), 0 (Bytes)
 Direction: outbound
  Rule: If-match carl 3
   CIR 512 (kbps), CBS 32000 (Bytes), EBS 0 (Bytes)
   Green action  : pass
   Yellow action : pass
   Red action    : discard
   Green packets : 0 (Packets), 0 (Bytes)
   Yellow packets: 0 (Packets), 0 (Bytes)
   Red packets   : 0 (Packets), 0 (Bytes)
  Rule: If-match carl 4
   CIR 512 (kbps), CBS 32000 (Bytes), EBS 0 (Bytes)
   Green action  : pass
   Yellow action : pass
   Red action    : discard
   Green packets : 0 (Packets), 0 (Bytes)
   Yellow packets: 0 (Packets), 0 (Bytes)
   Red packets   : 0 (Packets), 0 (Bytes)
[Router] display qos car interface gigabitethernet 0/2
Interface: GigabitEthernet0/2
 Direction: inbound
  Rule: If-match carl 1
   CIR 512 (kbps), CBS 32000 (Bytes), EBS 0 (Bytes)
   Green action  : pass
   Yellow action : pass
```

```
  Red action    : discard
  Green packets : 0 (Packets), 0 (Bytes)
  Yellow packets: 0 (Packets), 0 (Bytes)
  Red packets   : 0 (Packets), 0 (Bytes)
 Rule: If-match carl 2
  CIR 512 (kbps), CBS 32000 (Bytes), EBS 0 (Bytes)
  Green action  : pass
  Yellow action : pass
  Red action    : discard
  Green packets : 0 (Packets), 0 (Bytes)
  Yellow packets: 0 (Packets), 0 (Bytes)
  Red packets   : 0 (Packets), 0 (Bytes)
Direction: outbound
 Rule: If-match carl 3
  CIR 512 (kbps), CBS 32000 (Bytes), EBS 0 (Bytes)
  Green action  : pass
  Yellow action : pass
  Red action    : discard
  Green packets : 0 (Packets), 0 (Bytes)
  Yellow packets: 0 (Packets), 0 (Bytes)
  Red packets   : 0 (Packets), 0 (Bytes)
 Rule: If-match carl 4
  CIR 512 (kbps), CBS 32000 (Bytes), EBS 0 (Bytes)
  Green action  : pass
  Yellow action : pass
  Red action    : discard
  Green packets : 0 (Packets), 0 (Bytes)
  Yellow packets: 0 (Packets), 0 (Bytes)
  Red packets   : 0 (Packets), 0 (Bytes)
```

(6) 保存配置

保存出口路由器 Router 上的配置。

```
[Router] save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait...
Saved the current configuration to mainboard device successfully.
```

2.5 验证配置

(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，PC 间是通过 ACCSW1 实现二层互通的。如果用户间互 ping 测试正常，则说明二层互通正常。

```
<PC1> ping 192.168.10.83
Ping 192.168.10.83 (192.168.10.83): 56 data bytes, press CTRL+C to break
56 bytes from 192.168.10.83: icmp_seq=0 ttl=255 time=1.328 ms
```

```
56 bytes from 192.168.10.83: icmp_seq=1 ttl=255 time=0.808 ms
56 bytes from 192.168.10.83: icmp_seq=2 ttl=255 time=0.832 ms
56 bytes from 192.168.10.83: icmp_seq=3 ttl=255 time=0.904 ms
56 bytes from 192.168.10.83: icmp_seq=4 ttl=255 time=0.787 ms

--- Ping statistics for 192.168.10.83 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.787/0.932/1.328/0.202 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 或 CORESW2 实现的。如果用户之间互 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 192.168.20.5
Ping 192.168.20.5 (192.168.20.5): 56 data bytes, press CTRL+C to break
56 bytes from 192.168.20.5: icmp_seq=0 ttl=255 time=69.146 ms
56 bytes from 192.168.20.5: icmp_seq=1 ttl=255 time=1.735 ms
56 bytes from 192.168.20.5: icmp_seq=2 ttl=255 time=1.356 ms
56 bytes from 192.168.20.5: icmp_seq=3 ttl=255 time=1.302 ms
56 bytes from 192.168.20.5: icmp_seq=4 ttl=255 time=1.379 ms

--- Ping statistics for 192.168.20.5 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.302/14.984/69.146/27.082 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。

2.6 配置文件

- 接入交换机 ACCSW1：

```
#
 sysname ACCSW1
#
 telnet server enable
#
 dhcp snooping enable
#
vlan 5
#
vlan 10
#
vlan 20
#
 stp bpdu-protection
#
interface Vlan-interface5
```

```
 ip address 10.10.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 10
 stp edged-port
 ip verify source ip-address mac-address
 dhcp snooping binding record
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port access vlan 20
 stp edged-port
 ip verify source ip-address mac-address
 dhcp snooping binding record
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 10 20
 dhcp snooping trust
#
interface GigabitEthernet1/0/4
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 10 20
#
interface Ten-GigabitEthernet1/0/10
 port link-mode bridge
 port access vlan 5
#
line vty 0 63
 authentication-mode scheme
#
local-user admin class manage
 password hash
$h$6$ZJSf20ub4uEzjy2F$cXW3O3Jt5Ci21ECze7w2MdRpLebMaE4vXBo59frUrIZs+Knxw76oNBu+HiB0zqkTfr
nw1Phe0rSRa5d+OSIIbg==
 service-type telnet
 authorization-attribute user-role network-admin
 authorization-attribute user-role network-operator
#
```

- 接入交换机 ACCSW2、ACCSW3、ACCSW4：

接入交换机 ACCSW2、ACCSW3、ACCSW4 除了 VLAN ID、管理 VLAN 接口 IP 地址、接口编号与 ACCSW1 不同外，其他配置与 ACCSW1 相同，配置文件略。

- 核心交换机 CORESW1

```
#
```

```
 sysname CORESW1
#
track 1 interface GigabitEthernet1/0/7
#
ospf 100 router-id 3.3.3.3
 area 0.0.0.0
  network 172.16.1.0 0.0.0.255
  network 172.16.3.0 0.0.0.255
  network 192.168.10.0 0.0.0.255
  network 192.168.20.0 0.0.0.255
#
 dhcp enable
#
vlan 10
#
vlan 20
#
vlan 30
#
vlan 40
#
vlan 50
#
vlan 100
#
vlan 300
#
ftth
#
dhcp server ip-pool 1
 gateway-list 192.168.10.1
 network 192.168.10.0 mask 255.255.255.0
 dns-list 202.101.100.199
 expired day 30
 static-bind ip-address 192.168.10.254 mask 255.255.255.0 client-identifier aabb-cccc-dd
#
dhcp server ip-pool 2
 gateway-list 192.168.20.1
 network 192.168.20.0 mask 255.255.255.0
 dns-list 202.101.100.199
 expired day 30
#
interface Vlan-interface10
 ip address 192.168.10.1 255.255.255.0
#
interface Vlan-interface20
 ip address 192.168.20.1 255.255.255.0
#
```

```
interface Vlan-interface100
 ip address 172.16.1.1 255.255.255.0
#
interface Vlan-interface300
 ip address 172.16.3.1 255.255.255.0
 vrrp vrid 1 virtual-ip 172.16.3.10
 vrrp vrid 1 priority 120
 vrrp vrid 1 preempt-mode delay 5000
 vrrp vrid 1 track 1 priority reduced 30
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 10
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 20
#
interface GigabitEthernet1/0/5
 port link-mode bridge
 port link-type trunk
 port trunk permit vlan 300
#
```

- 核心交换机 CORESW2：

核心交换机 CORESW2 除了 VLAN ID、接口编号、OSPF 的 router-id、VRRP 备份组 1 的优先级与 CORESW1 不同外，其他配置与 CORESW1 相同，配置文件略。

- 出口路由器 Router

```
#
 sysname Router
#
 packet-filter default deny
#
 qos carl 1 source-ip-address range 192.168.10.1 to 192.168.10.254 per-address
shared-bandwidth
 qos carl 2 source-ip-address range 192.168.20.1 to 192.168.20.254 per-address
shared-bandwidth
 qos carl 3 destination-ip-address range 192.168.10.1 to 192.168.10.254 per-address
shared-bandwidth
 qos carl 4 destination-ip-address range 192.168.20.1 to 192.168.20.254 per-address
shared-bandwidth
#
ospf 10 router-id 1.1.1.1
 default-route-advertise always
 area 0.0.0.0
  network 172.16.1.0 0.0.0.255
```

```
  network 172.16.2.0 0.0.0.255
#
 dns proxy enable
 dns server 202.101.100.199
#
interface GigabitEthernet0/1
 port link-mode route
 ip address 172.16.1.2 255.255.255.0
 packet-filter 2000 inbound
 qos car inbound carl 1 cir 512 cbs 32000 ebs 0 green pass red discard yellow pass
 qos car inbound carl 2 cir 512 cbs 32000 ebs 0 green pass red discard yellow pass
 qos car outbound carl 3 cir 512 cbs 32000 ebs 0 green pass red discard yellow pass
 qos car outbound carl 4 cir 512 cbs 32000 ebs 0 green pass red discard yellow pass
#
interface GigabitEthernet0/2
 port link-mode route
 ip address 172.16.2.2 255.255.255.0
 packet-filter 2000 inbound
 qos car inbound carl 1 cir 512 cbs 32000 ebs 0 green pass red discard yellow pass
 qos car inbound carl 2 cir 512 cbs 32000 ebs 0 green pass red discard yellow pass
 qos car outbound carl 3 cir 512 cbs 32000 ebs 0 green pass red discard yellow pass
 qos car outbound carl 4 cir 512 cbs 32000 ebs 0 green pass red discard yellow pass
#
interface GigabitEthernet0/0
 port link-mode route
 ip address 202.101.100.2 255.255.255.252
#
 ip route-static 0.0.0.0 0 202.101.100.1
#
acl basic 2000
 rule 0 permit source 192.168.10.0 0.0.0.255
 rule 5 permit source 192.168.20.0 0.0.0.255
 rule 10 permit source 172.16.1.0 0.0.0.255
 rule 15 permit source 172.16.2.0 0.0.0.255
 rule 20 permit source 172.16.3.0 0.0.0.255
#
```

2.7 相关资料

- 产品配套“基础配置指导”中的“登录设备”。
- 产品配套“基础命令参考”中的“登录设备”。
- 产品配套“二层技术-以太网交换配置指导”中的“VLAN”。
- 产品配套“二层技术-以太网交换命令参考”中的“VLAN”。
- 产品配套“二层技术-以太网交换配置指导”中的“以太网链路聚合”。
- 产品配套“二层技术-以太网交换命令参考”中的“以太网链路聚合”。

- 产品配套“三层技术-IP 业务配置指导”中的“DHCP”。
- 产品配套“三层技术-IP 业务命令参考”中的“DHCP”。
- 产品配套“三层技术-IP 路由配置指导”中的“OSPF”。
- 产品配套“三层技术-IP 路由命令参考”中的“OSPF”。
- 产品配套“ACL 和 QoS 配置指导”中的“ACL”。
- 产品配套“ACL 和 QoS 命令参考”中的“ACL”。
- 产品配套“ACL 和 QoS 配置指导”中的“QoS”。
- 产品配套“ACL 和 QoS 命令参考”中的“QoS”。
- 产品配套“安全配置指导”中的“IP Source Guard”。
- 产品配套“安全命令参考”中的“IP Source Guard”。

802.1X 快速配置指南

目 录

1 配置 802.1X 本地认证

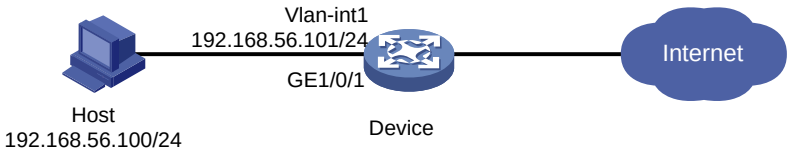
1.1 简介

本案例介绍 802.1X 用户本地认证的配置方法。

1.2 组网需求

如图 1-1 所示，用户通过 Device 的端口 GigabitEthernet1/0/1 接入网络。要求：Device 对从该端口接入的用户采用基于端口的接入控制方式进行 802.1X 本地认证以控制其访问 Internet。

图1-1 802.1X 本地认证配置组网图



1.3 配置注意事项

使能全局的 802.1X 认证功能一般放在最后，因为当相关参数未配置完成时，会造成合法用户无法访问网络。

只有同时开启全局和端口的 802.1X 特性后，802.1X 的配置才能在端口上生效。

1.4 配置步骤

1.4.1 配置 Device

(1) 配置本地用户

添加网络接入类本地用户，用户名为“dot1x”，并进入该用户视图。

```
<Device> system-view
[Device] local-user dot1x class network
New local user added.
```

配置用户“dot1x”的密码为明文 123456TESTplat&!。

```
[Device-luser-network-dot1x] password simple 123456TESTplat&!
```

配置本地用户的服务类型为 lan-access。

```
[Device-luser-network-dot1x] service-type lan-access
[Device-luser-network-dot1x] quit
```

(2) 配置虚接口地址，作为 Host 的网关

```
[Device] interface vlan-interface 1
[Device-Vlan-interface1] ip address 192.168.56.101 255.255.255.0
[Device-Vlan-interface1] quit
```

(3) 配置 802.1X 认证

开启端口 GigabitEthernet1/0/1 的 802.1X 认证。

```
[Device] interface gigabitethernet1/0/1
[Device-GigabitEthernet1/0/1] dot1x
```

配置基于端口的接入控制方式

```
[Device-GigabitEthernet1/0/1] dot1x port-method portbased
[Device-GigabitEthernet1/0/1] quit
```

开启全局 802.1X 认证。

```
[Device] dot1x
```

1.4.2 配置 802.1X 客户端

说明

- 以下使用 iNode PC 7.3（E0518）版本为例介绍 802.1X 客户端的配置。
- 若使用 Windows XP 的 802.1X 客户端，则需要正确设置此连接的网络属性：在网络属性的“验证”页签中，确保选中“启用此网络的 IEEE 802.1x 验证”，并选择要用于此连接的 EAP 认证类型为“MD5-质询”。
- 保证用户在通过认证后，能够及时更新客户端 IP 地址与授权 VLAN 中的资源互通。

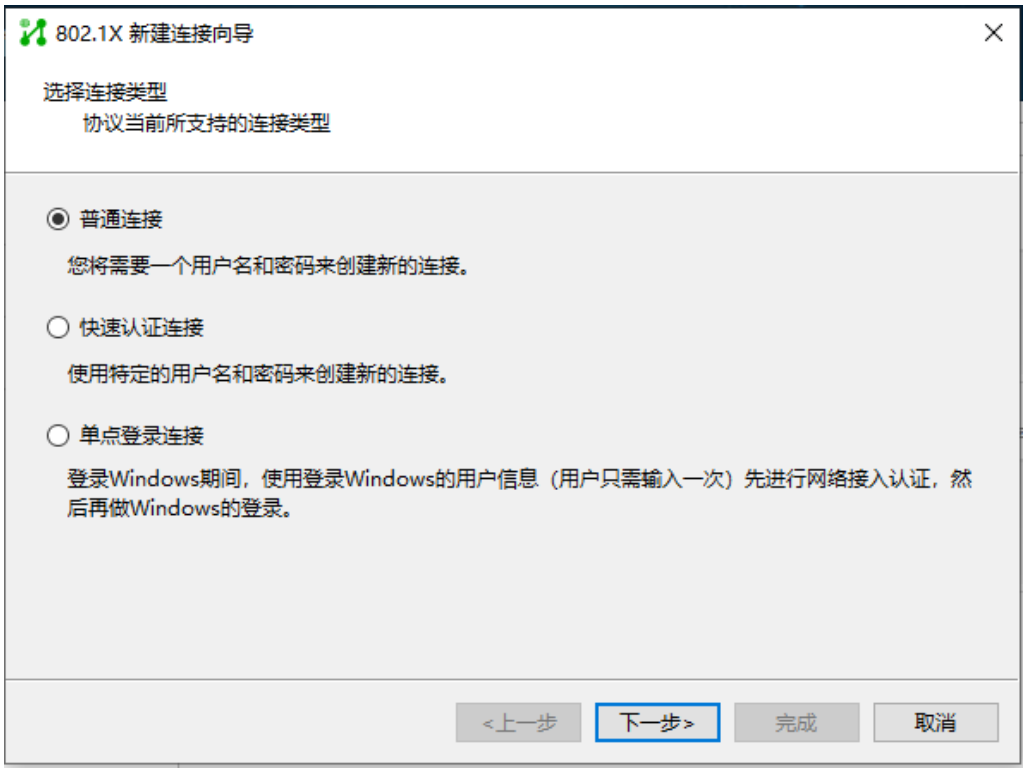
(1) 启动客户端

图1-2 iNode 客户端界面示意图

(2) 新建 802.1X 连接

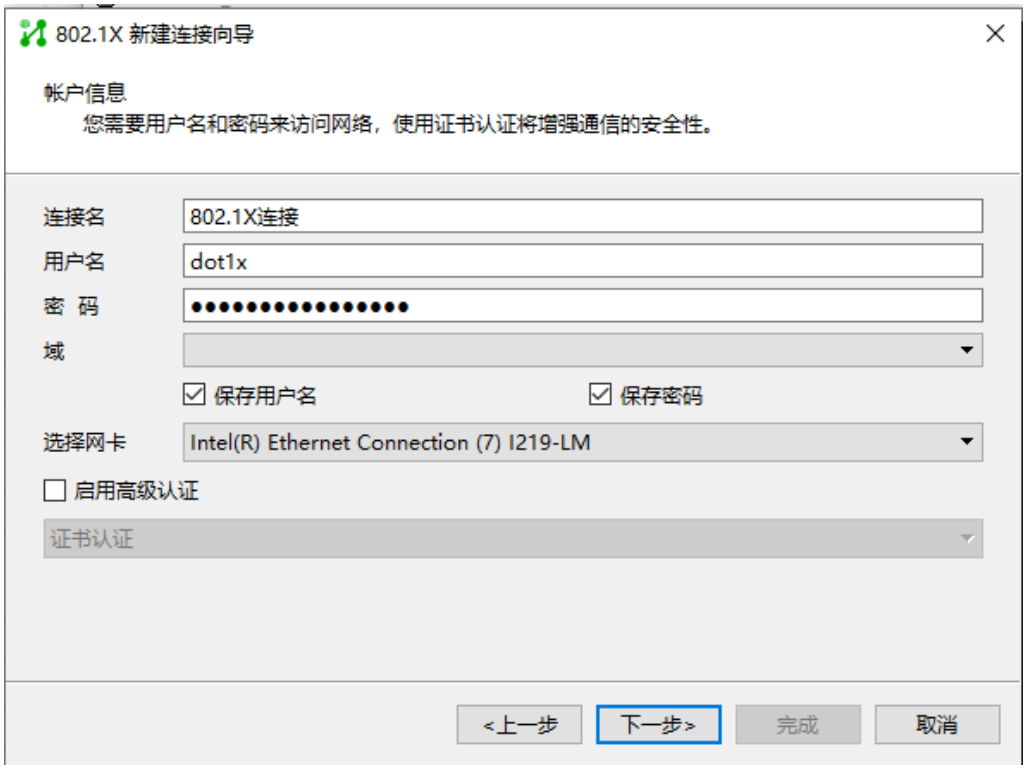
点击<新建>按钮，进入新建连接向导对话框。

图1-3 新建 802.1X 连接示意图



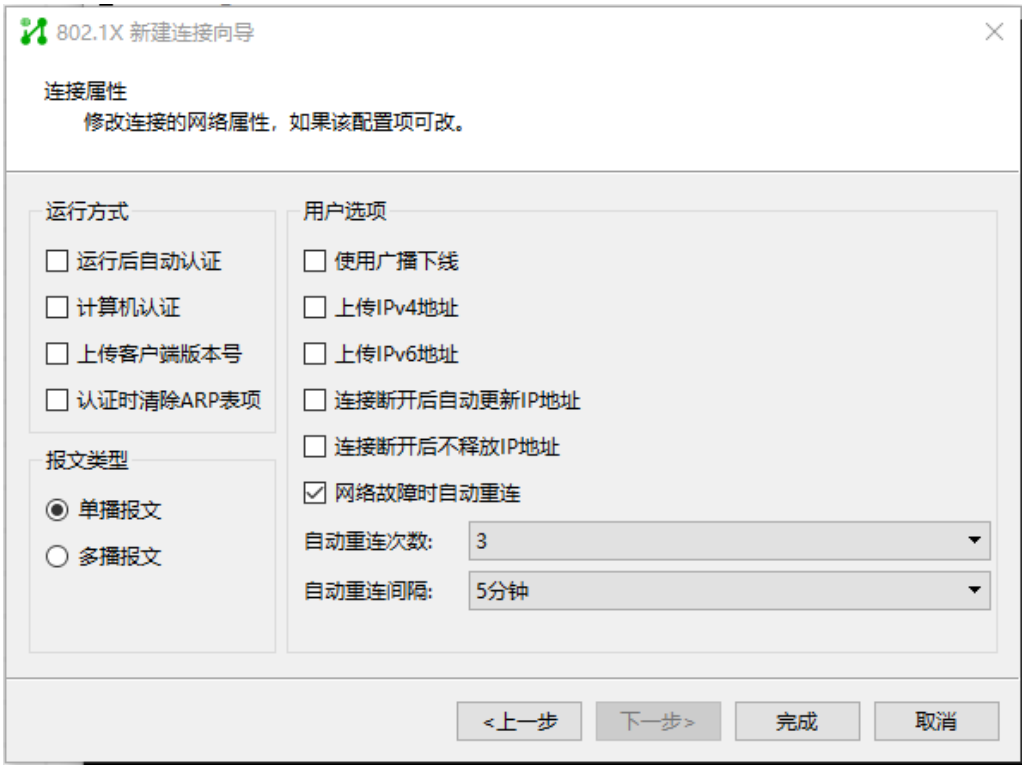
(3) 输入用户名和密码

图1-4 802.1X 用户名、密码配置示意图



(4) 设置连接属性

图1-5 802.1X 连接属性配置示意图



说明

由于本地认证不能对客户端上传的版本号进行识别，请不要勾选“上传客户端版本号”选项。

(5) 发起 802.1X 连接

完成新建连接后，点击 iNode 客户端的<连接>按钮，发起 802.1X 连接。

图1-6 802.1X 启动连接示意图

1.5 验证配置

使用命令 **display dot1x interface** 可以查看端口 GigabitEthernet1/0/1 上的 802.1X 的配置情况。

```
[Device] display dot1x interface gigabitethernet 1/0/1
 Global 802.1X parameters:
   802.1X authentication                : Enabled
   CHAP authentication                  : Enabled
   Max-tx period                        : 30 s
   Handshake period                     : 15 s
   Offline detect period                : 300 s
   Quiet timer                          : Disabled
       Quiet period                     : 60 s
   Supp timeout                         : 30 s
   Server timeout                       : 100 s
   Reauth period                        : 3600 s
   Max auth requests                    : 2
   User aging period for Auth-Fail VLAN : 1000 s
```

```
  User aging period for Auth-Fail VSI  : 1000 s
  User aging period for critical VLAN  : 1000 s
  User aging period for critical VSI   : 1000 s
  User aging period for guest VLAN     : 1000 s
  User aging period for guest VSI      : 1000 s
  EAD assistant function               : Disabled
      EAD timeout                      : 30 min
  Domain delimiter                     : @
Online 802.1X wired users              : 0
GigabitEthernet1/0/1  is link-up
  802.1X authentication            : Enabled
  Handshake                        : Enabled
  Handshake reply                  : Disabled
  Handshake security               : Disabled
  Unicast trigger                  : Disabled
  Periodic reauth                  : Disabled
  Port role                        : Authenticator
  Authorization mode               : Auto
  Port access control              : Port-based
  Multicast trigger                : Enabled
  Mandatory auth domain            : Not configured
  Guest VLAN                       : Not configured
  Auth-Fail VLAN                   : Not configured
  Critical VLAN                    : Not configured
  Critical voice VLAN              : Disabled
  Add Guest VLAN delay             : Disabled
  Re-auth server-unreachable       : Logoff
  Max online users                 : 4294967295
  User IP freezing                 : Disabled
  Reauth period                    : 0 s
  Send Packets Without Tag         : Disabled
  Max Attempts Fail Number         : 0
  Guest VSI                        : Not configured
  Auth-Fail VSI                    : Not configured
  Critical VSI                     : Not configured
  Add Guest VSI delay              : Disabled
  User aging                       : Enabled
  Server-recovery online-user-sync : Disabled
  Auth-Fail EAPOL                  : Disabled
```

```
   Critical EAPOL                   : Disabled
   Discard duplicate EAPOL-Start    : No

   EAPOL packets: Tx 0, Rx 0
   Sent EAP Request/Identity packets : 0
        EAP Request/Challenge packets: 0
        EAP Success packets: 0
        EAP Failure packets: 0
   Received EAPOL Start packets : 0
            EAPOL LogOff packets: 0
            EAP Response/Identity packets : 0
            EAP Response/Challenge packets: 0
            Error packets: 0
   Online 802.1X users: 0
```

当 iNode 客户端输入正确的用户名和密码成功上线后，可使用命令 **display dot1x connection** 查看到上线用户的连接情况。

1.6 配置文件

```
#
interface Vlan-interface1
 ip address 192.168.56.101 255.255.255.0
#
local-user localuser class network
 password cipher $c$3$YPkufRcxFR3KdpUCHFiNkns/YFPmbJkG/pQxBg==
 service-type lan-access
 authorization-attribute user-role network-operator
#
interface GigabitEthernet1/0/1
 dot1x
 dot1x port-method portbased
#
 dot1x
#
```

1.7 相关资料

- 产品配套“安全配置指导”中的“802.1X”。
- 产品配套“安全命令参考”中的“802.1X”。

AAA 快速配置指南

目 录

1 配置 Telnet 用户的 HWTACACS 认证和授权

1.1 简介

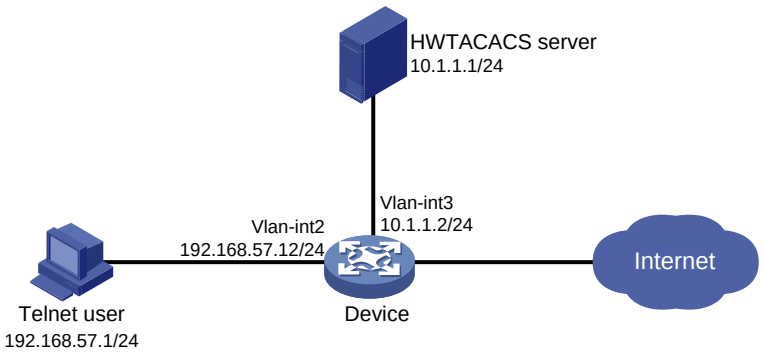
本案例介绍 Telnet 用户的 HWTACACS 认证和授权的配置方法。

1.2 组网需求

如图 1-1 所示，通过在作为 NAS 的 Device 上配置远程 HWTACACS 认证、授权功能，实现 Telnet 用户的安全登录。要求在 Device 上配置实现：

- HWTACACS 服务器对登录 Device 的 Telnet 用户进行认证和授权，登录用户名为 *user*@bbb，密码为 123456TESTplat&!；
- 用户通过认证后可执行系统所有功能和资源的相关 **display** 命令。

图1-1 Telnet 用户的远端 HWTACACS 认证和授权配置组网图



1.3 配置步骤

1.3.1 配置 HWTACACS

说明

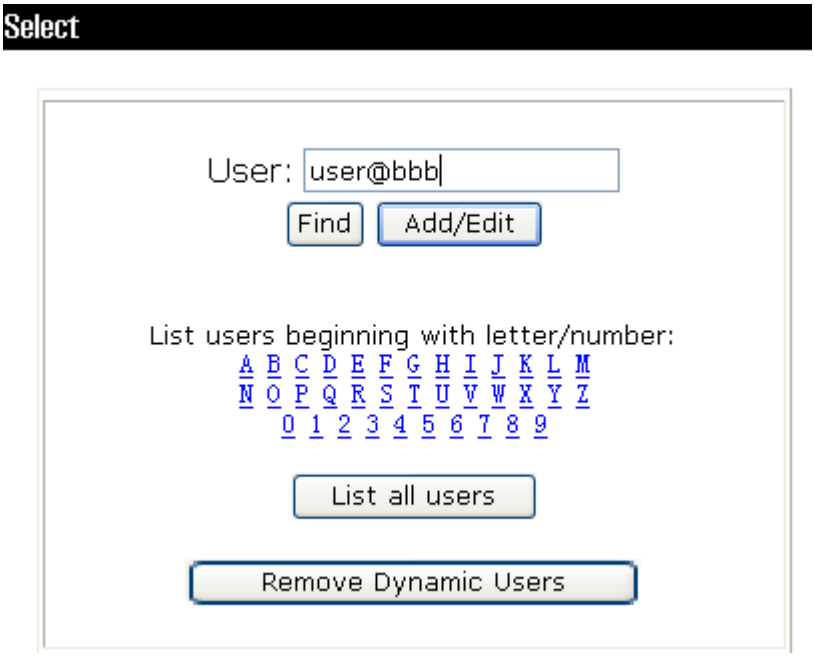
本文以 HWTACACS 服务器 ACS 4.0 为例，说明该例中 HWTACACS 的基本配置。

1. 增加设备管理用户

登录进入 HWTACACS 管理平台，点击左侧导航栏“User-Setup”增加设备管理用户。

- 在界面上输入用户名“user@bbb”；
- 点击按钮“Add/Edit”进入用户编辑页面。

图1-2 用户创建界面

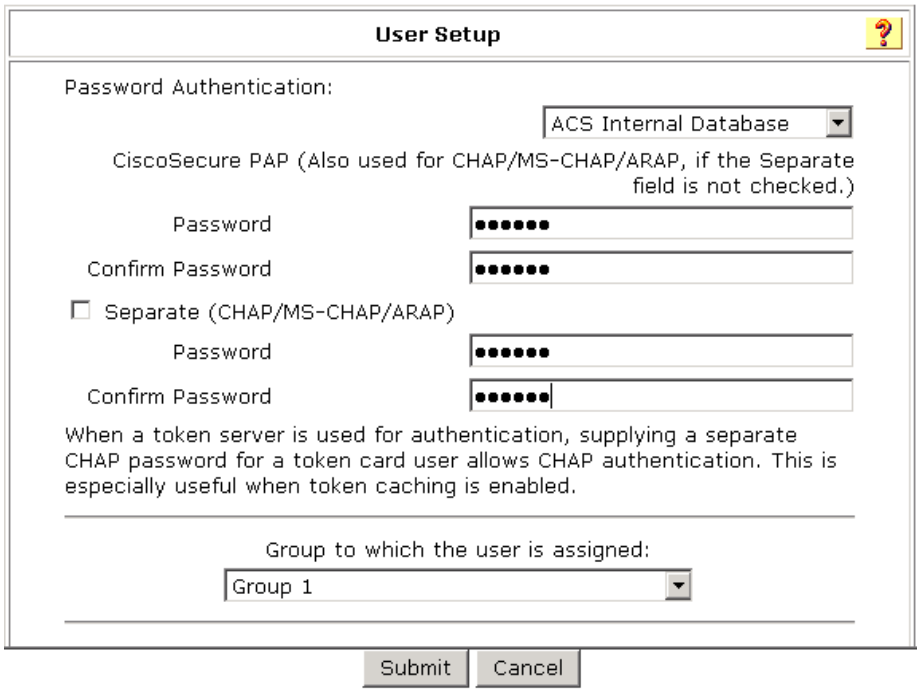


2. 配置设备管理用户

在用户编辑页面上配置设备管理用户。

- 配置用户密码“123456TESTplat&!”；
- 为用户选择组“Group 1”；
- 单击“Submit”完成操作。

图1-3 用户密码配置界面

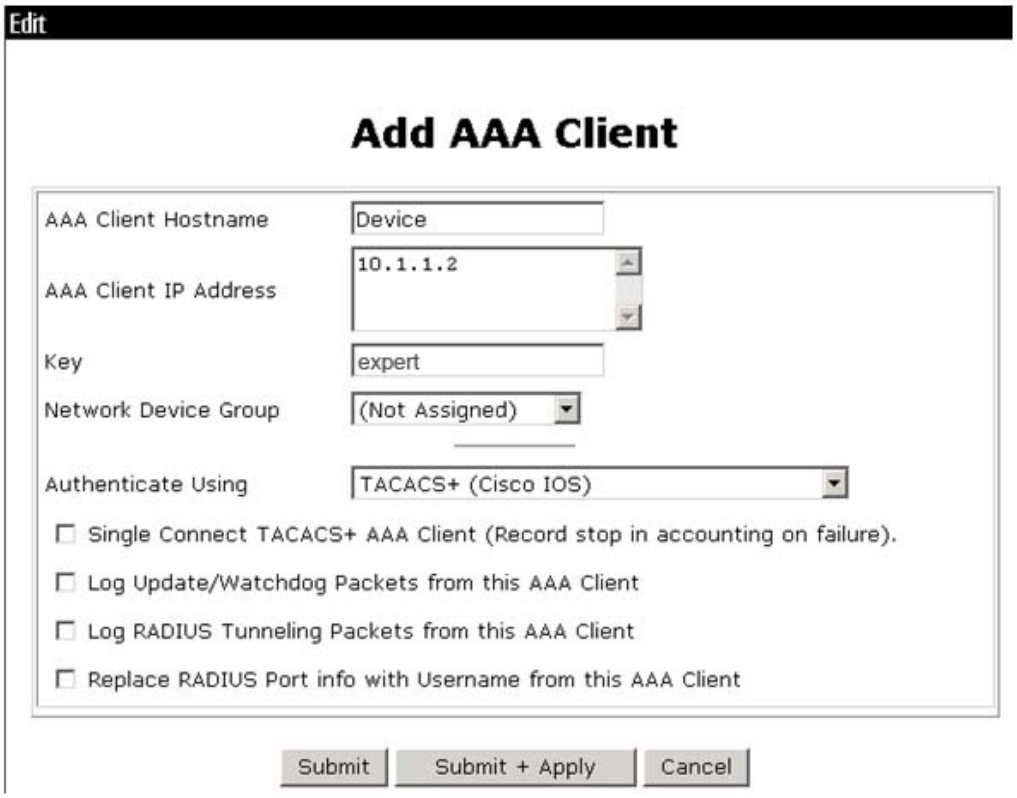


3. 配置网络

点击左侧导航栏“Network Configuration”，在“AAA Client Hostname”处任意命名（本例为“Device”）后开始配置网络。

- “AAA Client IP Address”一栏填写 Device 与 HWTACACS 服务器相连的接口的 IP 地址“10.1.1.2”。
- “Key”一栏填写 HWTACACS 服务器和设备通信时的共享密钥“expert”，必须和 Device 上 HWTACACS 方案里配置的认证、授权和计费共享密钥相同。
- 在“Authenticate Using”的下拉框里选择“TACACS+ (Cisco IOS)”。
- 单击“Submit+Apply”按钮完成配置。

图1-4 网络配置界面



4. 设置组

单击左侧导航栏“Group Setup”，选取“Group 1”（与配置设备管理用户时为用户选择的组一致），单击“Edit Settings”进入编辑区。

- 在多选框中选择“Shell”（用户可以执行命令）；
- 在多选框中选择“Custom attributes”，并在文本框中输入：roles=\”network-operator\”；
- 单击“Submit”后完成操作。

图1-5 选择组界面

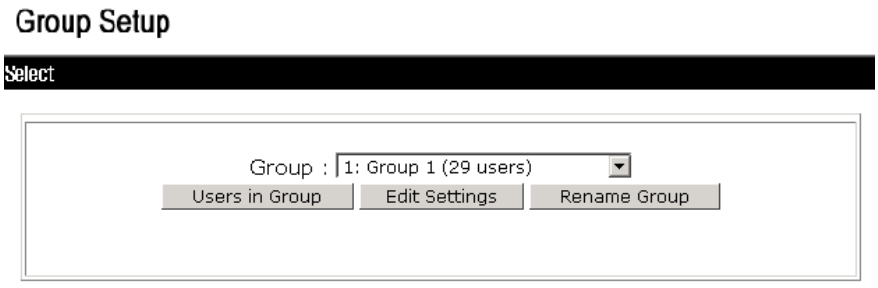
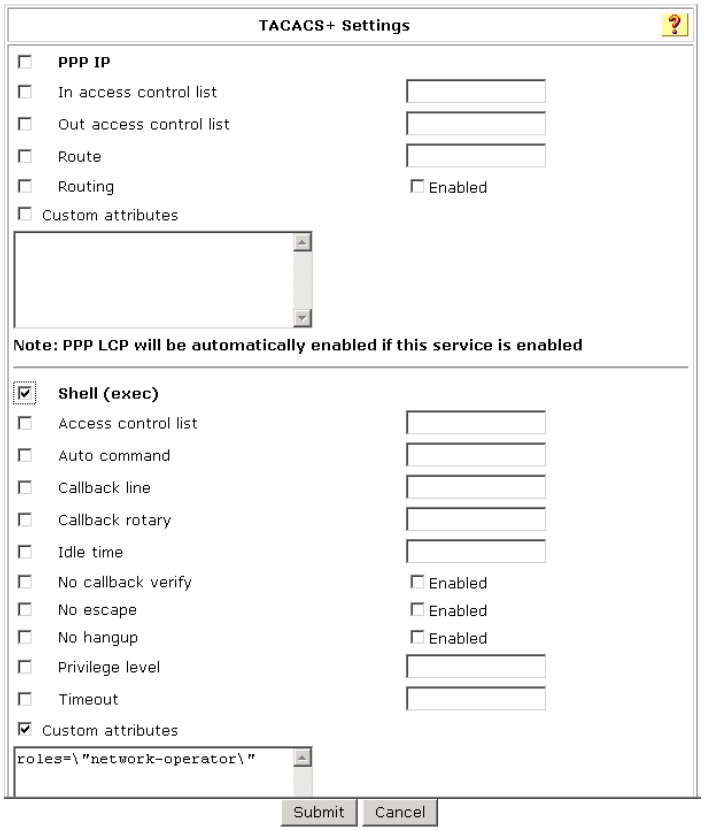


图1-6 组配置界面



1.3.2 配置 Device

创建 VLAN 2，并将 GigabitEthernet1/0/2 加入 VLAN 2。

```
<Device> system-view
[Device] vlan 2
[Device-vlan2] port gigabitethernet 1/0/2
[Device-vlan2] quit
```

配置 VLAN 接口 2 的 IP 地址。

```
[Device] interface vlan-interface 2
[Device-Vlan-interface2] ip address 192.168.57.12 255.255.255.0
[Device-Vlan-interface2] quit
```

创建 VLAN 3，并将 GigabitEthernet1/0/1 加入 VLAN 3。

```
[Device] vlan 3
[Device-vlan3] port gigabitethernet 1/0/1
[Device-vlan3] quit
```

配置 VLAN 接口 3 的 IP 地址。

```
[Device] interface vlan-interface 3
[Device-Vlan-interface3] ip address 10.1.1.2 255.255.255.0
[Device-Vlan-interface3] quit
```

开启 Device 的 Telnet 服务器功能。

```
[Device] telnet server enable
```

配置 Telnet 用户登录的用户界面采用 scheme 方式。

```
[Device] line vty 0 63
[Device-line-vty0-63] authentication-mode scheme
[Device-line-vty0-63] quit
```

配置 HWTACACS 方案 hwtac。

```
[Device] hwtacacs scheme hwtac
```

配置主认证、授权和计费服务器的 IP 地址为 10.1.1.1，认证、授权和计费的端口号为 49（HWTACACS 服务器的认证、授权和计费端口为 TCP 端口 49）。

```
[Device-hwtacacs-hwtac] primary authentication 10.1.1.1 49
[Device-hwtacacs-hwtac] primary authorization 10.1.1.1 49
[Device-hwtacacs-hwtac] primary accounting 10.1.1.1 49
```

配置与认证、授权和计费服务器交互报文时的共享密钥均为明文 expert。

```
[Device-hwtacacs-hwtac] key authentication simple expert
[Device-hwtacacs-hwtac] key authorization simple expert
[Device-hwtacacs-hwtac] key accounting simple expert
[Device-hwtacacs-hwtac] quit
```

配置 ISP 域的 AAA 方案，为 login 用户配置 AAA 认证方法为 HWTACACS 认证、授权和计费。

```
[Device] domain bbb
[Device-isp-bbb] authentication login hwtacacs-scheme hwtac
[Device-isp-bbb] authorization login hwtacacs-scheme hwtac
[Device-isp-bbb] accounting login hwtacacs-scheme hwtac
[Device-isp-bbb] quit
```

1.4 验证配置

Telnet 用户可以使用用户名 user@bbb 和密码 123456TESTplat&!通过认证，并且获得用户角色 network-operator（用户通过认证后可执行系统所有功能和资源的相关 **display** 命令）。

1.5 配置文件

说明

部分交换机的配置文件中会显示 **port link-mode bridge** 命令，请以实际情况为准。

```
#
 telnet server enable
#
vlan 2 to 3
#
interface Vlan-interface2
 ip address 192.168.57.12 255.255.255.0
#
interface Vlan-interface3
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/2
```

```
 port link-mode bridge
 port access vlan 2
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 port access vlan 3
#
line vty 0 63
 authentication-mode scheme
 user-role network-operator
#
hwtacacs scheme hwtac
 primary authentication 10.1.1.1
 primary authorization 10.1.1.1
 primary accounting 10.1.1.1
 key authentication cipher $c$3$X3oR/wjLFjDqIyjdAmvjwAhiuqewGABglQ==
 key authorization cipher $c$3$5pmuq0RJ9UWMWDkRNNERX6HFM0aRv5txFg==
 key accounting cipher $c$3$FSdSiBY1u+ZNkAYYlPw9YkGxJA4iR8MDjw==
#
 domain bbb
  authentication login hwtacacs-scheme hwtac
  authorization login hwtacacs-scheme hwtac
  accounting login hwtacacs-scheme hwtac
#
```

1.6 相关资料

- 产品配套“安全配置指导”中的“AAA”。
- 产品配套“安全命令参考”中的“AAA”。