

实验1 网络设备基本操作

1.1 实验内容与目标

完成本实验，您应该能够：

- 使用 Console 口登录设备
- 使用 Telnet 终端登录设备
- 掌握基本系统操作命令的使用
- 掌握基本文件操作命令的使用
- 使用 FTP、TFTP 上传下载文件

1.2 实验组网图

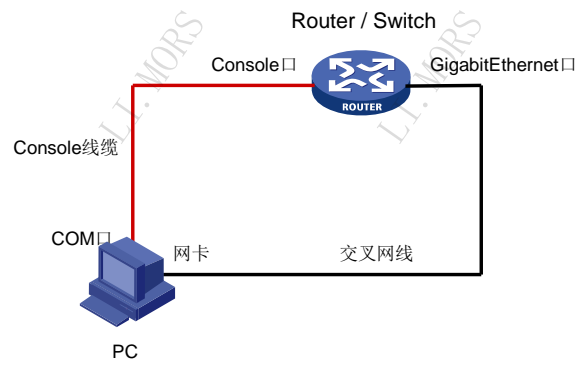


图1-1 实验组网图

1.3 实验设备与版本

本实验所需之主要设备器材如表 1-1 所示。

表1-1 实验设备器材

名称和型号	版本	数量	描述
MSR36-20	CMW 7.1.049-R0106	1	
PC	Windows 7	1	安装PuTTY软件
Console串口线	--	1	
第5类UTP以太网连接线	--	1	

1.4 实验过程

本实验以一台 MSR 路由器作为演示设备，使用交换机亦可。

实验任务一：通过 Console 登录

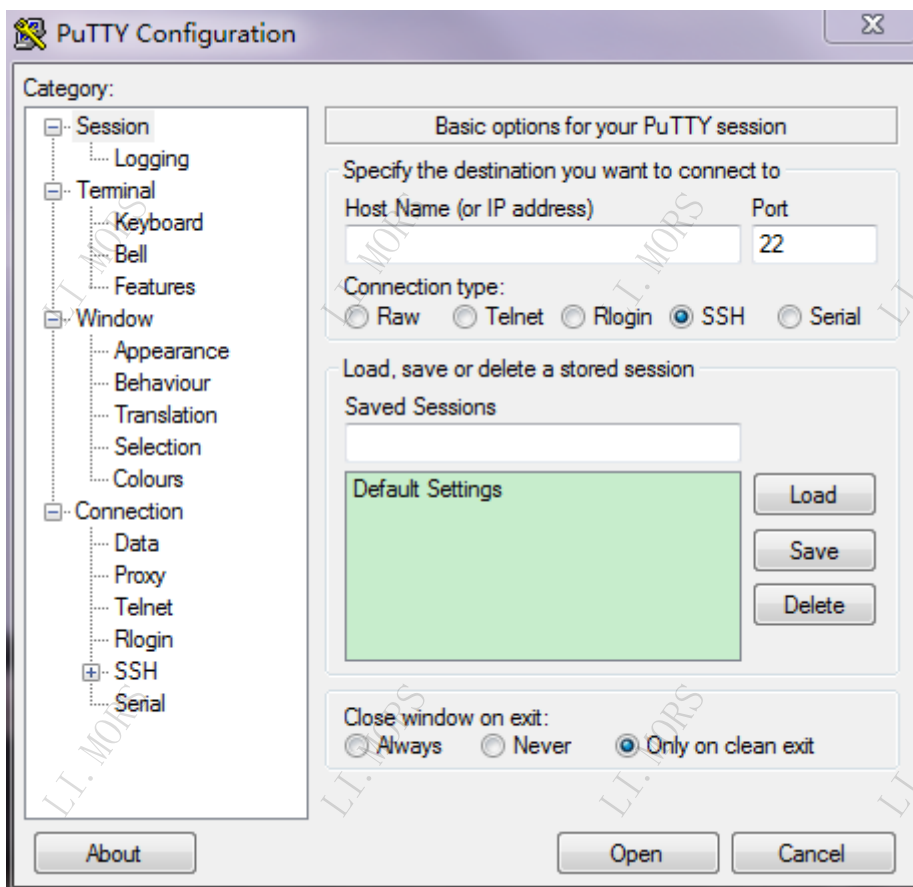
本实验的主要任务是学员熟悉并掌握通过 Console 电缆连接进行设备配置的方法。

步骤一：连接配置电缆

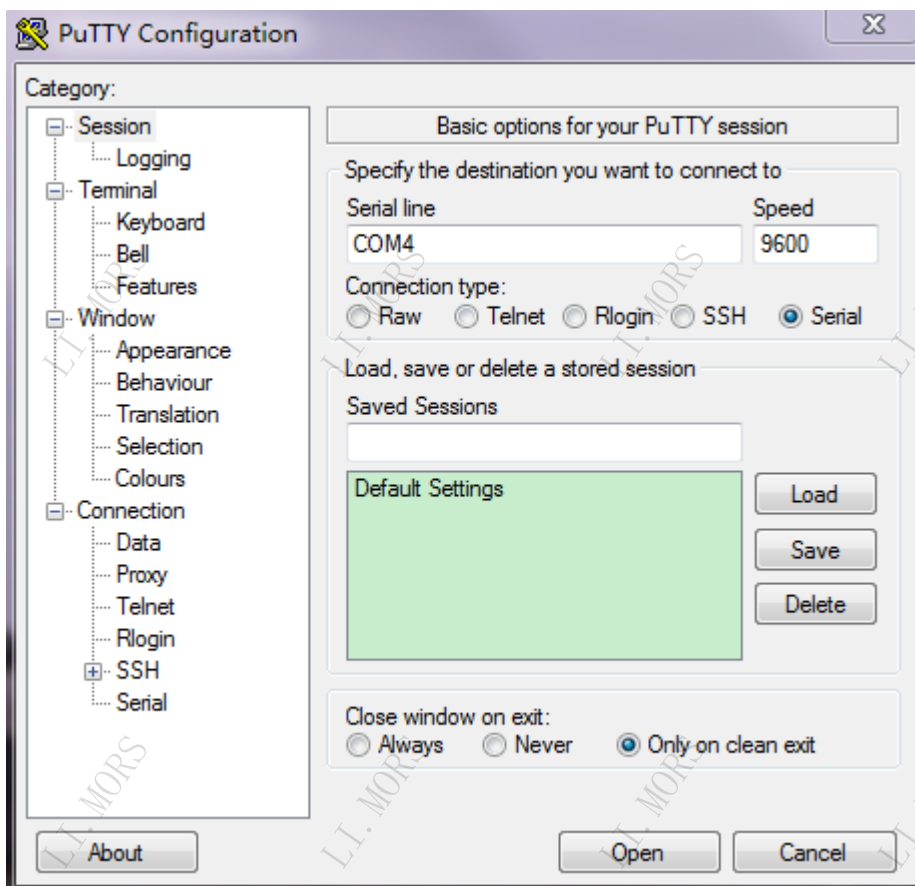
将 PC（或终端）的串口通过标准 Console 电缆与路由器的 Console 口连接。电缆的 RJ-45 头一端连接路由器的 Console 口；9 针 RS-232 接口一端连接计算机的串行口。

步骤二：启动 PC，运行超级终端

在 PC 桌面上运行软件 PuTTY，会显示出连接会话页面。如图所示：



在通过 Console 口登录设备时，选择连接方式为 Serial（串口）。在串口线中选择合适的 COM 口，本实验中 PC 连接 Console 线缆的接口是 COM4。波特率使用默认的参数 9600 即可。如图所示：



步骤三：进入 Console 配置界面

配置好之后，点选“Open”，即可进入设备配置页面。如图所示：



实验任务二：使用系统操作及文件操作的基本命令

步骤一：进入系统视图

完成实验任务一时，配置界面处于用户视图下，此时执行 **system-view** 命令进入系统视图。

```
<H3C>system-view
System View: return to User View with Ctrl+Z.
[H3C]
```

此时提示符变为 “[xxx]” 形式，说明用户已经处于系统视图。

在系统视图下，执行 **quit** 命令可以从系统视图切换到用户视图。

```
[H3C]quit
<H3C>
```

步骤二：学习使用帮助特性和补全健

H3C Comware 平台支持对命令行的输入帮助和智能补全功能。

输入帮助特性：在输入命令时，如果忘记某一个命令的全称，可以在配置视图下仅输入该命令的前几个字符，然后键入 **<?>**，系统则会自动列出以刚才输入的前几个字符开头的所有命令。当输入完一个命令关键字或参数时，也可以用 **<?>** 来查看紧随其后可用的关键字和参数。

在系统视图下输入 **sys**，再键入 **<?>**，系统会列出以 **sys** 开头的所有命令：

```
[H3C]sys?
sysname
```

在系统视图下输入 **sysname**，键入空格和 **<?>**，系统会列出 **sysname** 命令后可以输入的命令关键字和参数。

```
[H3C]sysname ?
TEXT Host name (1 to 64 characters)
```

智能补全功能：在输入命令时，不需要输入一条命令的全部字符，仅输入前几个字符，再键入 **<Tab>** 键，系统会自动补全该命令。如果有多个命令都具有相同的前缀字符的时候，连续键入 **<Tab>**，系统会在这几个命令之间切换。

在系统视图下输入 **sys**：

```
[H3C]sys
```

键入 **<Tab>**，系统自动补全该命令：

```
[H3C]sysname
```

在系统视图下输入 **in**：

```
[H3C]in
```

键入 **<Tab>**，系统自动补全 **in** 开头的第一个命令。

```
[H3C]interzone
```

再键入 **<Tab>**，系统在以 **in** 为前缀的命令中切换。

```
[H3C]interface
```

步骤三：更改系统名称

使用 **sysname** 命令更改系统名称。

```
[H3C]sysname YourName
[YourName]
```

可见此时显示的系统名已经由初始的 H3C 变为 YourName。

步骤四：更改系统时间

首先查看当前系统时间，用户视图和系统视图均可查看。

```
[YourName]display clock
10:52:55 UTC Thu 10/30/2014
```

使用 **quit** 命令退出系统视图，修改系统时间。

```
[YourName]quit
<YourName>clock datetime 10:10:10 10/01/2015
```

再次查看当前系统时间。

```
<YourName>display clock
10:10:11 UTC Thu 10/01/2015
```

可见系统时间已经改变。

由于系统有自动识别功能，所以在输入命令行时，为方便操作，有时仅输入前面几个字符即可，当然前提是这个几个字符可以唯一表示一条命令。

```
<YourName>dis clo
10:10:41 UTC Thu 10/01/2015
```

步骤五：显示系统运行配置

使用 **display current-configuration** 命令显示系统当前运行的配置，由于使用的设备及模块不同，操作时显示的具体内容也会有所不同。在如下配置信息中，请注意查看刚刚配置的 **sysname YourName** 命令，同时请查阅接口信息，并与设备的实际接口和模块进行比对。

```
<YourName>display current-configuration
#
version 7.1.049, Release 0106
#
sysname YourName
#
clock protocol none
#
password-recovery enable
#
vlan 1
#
controller Cellular0/0
#
controller Cellular0/1
#
interface Aux0
#
interface Serial1/0
#
interface Serial2/0
#
interface NULL0
#
---- More ----
```

使用空格键可以继续翻页显示，<Enter>进行翻行显示，或使用<Ctrl+C>结束显示，这里使用空格继续显示配置。

```

interface NULL0
#
interface GigabitEthernet0/0
port link-mode route
combo enable copper
ip address 1.1.1.1 255.255.255.0
#
interface GigabitEthernet0/1
port link-mode route
#
interface GigabitEthernet0/2
port link-mode route
#
scheduler logfile size 16
#
line class aux
user-role network-admin
#
line class tty
user-role network-operator
#
line class vty
user-role network-operator
#
line aux 0
---- More ----

```

可以看到 **sysname YourName** 已经显示在系统当前配置中了。从当前配置中，可以看出该路由器拥有五个物理接口，分别是 **interface Serial1/0**、**interface Serial2/0**、**interface GigabitEthernet0/0**、**interface GigabitEthernet0/1**、**interface GigabitEthernet0/2**，具体的实际接口数目和类型与当前设备的型号和所插板卡有关。

步骤六：显示保存的配置

使用 **display saved-configuration** 命令显示当前系统的保存配置。

```

<YourName>display saved-configuration
<YourName>

```

结果显示当前系统没有保存的配置文件，但是为什么显示运行配置（**current-configuration**）时有配置呢？那是因为运行配置实际上是保存在临时存储器中，而不是固定的存储介质中，所以设备重启后运行配置会丢失。因此，要求将正确的运行配置及时保存。而保存配置（**saved-configuration**）存储在 **CF** 卡（或 **Flash**、硬盘等）上，这里我们并没有进行保存操作，所以在 **CF** 卡上并没有保存配置文件。这就是运行配置和保存配置的不同之处。

步骤七：保存配置

使用 **save** 命令保存配置。

```

<YourName>save
The current configuration will be written to the device. Are you sure? [Y/N]:

```

选择 **Y**，确定将当前运行配置写进设备存储介质中。

```

Please input the file name(*.cfg)[cfa0:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):

```

系统提示请输入保存配置文件的文件名，注意文件名的格式为 ***.cfg**。该实验中系统默认将配置文件保存在 **CF** 卡中，保存后文件名为 **startup.cfg**，如果不更改系统默认保存的文件名，请按回车键。键入回车：

```
Validating file. Please wait...  
Configuration is saved to device successfully.
```

这是第一次保存配置文件的过程。如果以后再次保存配置文件，则显示如下：

```
<YourName>save  
The current configuration will be written to the device. Are you sure? [Y/N]:y  
Please input the file name(*.cfg)[cfa0:/startup.cfg]  
(To leave the existing filename unchanged, press the enter key):  
Cfa0:/startup.cfg exists, overwrite? [Y/N]:y  
Validating file. Please wait...  
Configuration is saved to device successfully.
```

键入回车后，系统会提示是否覆盖以前的配置文件，因为你还是选择了系统默认文件名 **startup.cfg** 来保存配置文件。

再次显示保存的配置：

```
<YourName>display saved-configuration  
#  
version 7.1.049, Release 0106  
#  
sysname YourName  
#  
clock protocol none  
#  
password-recovery enable  
#  
vlan 1  
#  
controller Cellular0/0  
#  
controller Cellular0/1  
#  
interface Aux0  
#  
interface Serial1/0  
#  
interface Serial2/0  
#  
interface NULL0  
#  
interface GigabitEthernet0/0  
port link-mode route  
combo enable copper  
ip address 1.1.1.1 255.255.255.0  
#  
interface GigabitEthernet0/1  
port link-mode route  
#  
interface GigabitEthernet0/2  
port link-mode route  
#  
scheduler logfile size 16  
#  
line class aux  
user-role network-admin  
#  
line class tty  
user-role network-operator  
#  
line class vty  
user-role network-operator  
#  
line aux 0  
<YourName>
```

由于执行了 **save** 命令，保存配置与运行配置一致。

步骤八：删除和清空配置

当需要删除某条命令时，可以使用 **undo** 命令进行逐条删除。例如删除 **sysname** 命令后，设备名称恢复成 **H3C**。

```
[YourName]undo sysname
[H3C]
```

当需要恢复到出厂默认配置时，首先在用户视图下执行 **reset saved-configuration** 命令用于清空保存配置（只是清除保存配置，当前配置还是存在的），再执行 **reboot** 重启整机后，配置恢复到出厂默认配置。

```
[YourName]quit
<YourName>reset saved-configuration
The saved configuration file will be erased. Are you sure? [Y/N]:y
Configuration file in cfa0: is being cleared.
Please wait ...
Configuration file is cleared.
<YourName>reboot
Start to check configuration with next startup configuration file, please
wait.....DONE!
Current configuration may be lost after the reboot, save current configuration?
[Y/N]:Y
```

步骤九：显示文件目录

首先使用 **pwd** 命令显示当前路径。

```
<YourName> pwd
cfa0:

<YourName>
```

可见当前路径是 **cfa0:/**。因为 **CF** 卡下保存有其他的文件夹目录，而且有的路由器拥有多个硬盘和 **Flash** 卡，所以使用 **pwd** 命令就能清楚的让你知道当前所在的路径。

然后，使用 **dir** 命令显示 **CF** 卡上所有文件列表：

```
<YourName>dir
Directory of cfa0:
 0 drw-      -   Aug 11 2014 11:22:22   diagfile
 1 -rw-      158  Oct 30 2014 11:12:46   ifindex.dat
 2 drw-      -   Aug 11 2014 11:22:22   license
 3 drw-      -   Aug 11 2014 11:22:22   logfile
 4 -rw-    10381312 Dec 15 2011 09:00:00   msr36-cmw710-boot-r0106.bin
 5 -rw-    2006016 Dec 15 2011 09:00:00   msr36-cmw710-data-r0106.bin
 6 -rw-    351232 Dec 15 2011 09:00:00   msr36-cmw710-security-r0106.bin
 7 -rw-    47564800 Dec 15 2011 09:00:00   msr36-cmw710-system-r0106.bin
 8 -rw-    1724416 Dec 15 2011 09:00:00   msr36-cmw710-voice-r0106.bin
 9 drw-      -   Aug 11 2014 11:22:22   seclog

252164 KB total (191572 KB free)
```

在上例中，**dir** 命令显示出的第一列为编号；第二列为属性，**drw-**为目录，**-rw-**为可读写文件；第三列为文件大小。通过属性列，可看出 **logfile** 实际是一个目录。

步骤十：显示文本文件内容

使用 **more** 命令显示文本文件内容。


```
<YourName>more startup.cfg
#
version 7.1.049, Release 0106
#
sysname YourName
#
clock protocol none
#
password-recovery enable
#
vlan 1
#
controller Cellular0/0
#
controller Cellular0/1
#
interface Aux0
#
interface Serial1/0
#
interface Serial2/0
#
interface NULL0
#
interface GigabitEthernet0/0
port link-mode route
combo enable copper
ip address 1.1.1.1 255.255.255.0
#
interface GigabitEthernet0/1
port link-mode route
#
interface GigabitEthernet0/2
port link-mode route
#
scheduler logfile size 16
#
line class aux
user-role network-admin
#
line class tty
user-role network-operator
#
line class vty
user-role network-operator
#
line aux 0
<YourName>
```

步骤十一：改变当前工作路径

使用 **cd** 命令改变当前的工作路径。

进入 **logfile** 子目录。

```
<YourName>cd logfile/
<YourName>dir
Directory of cfa0:/logfile
The directory is empty.

252164 KB total (191538 KB free)
```

退出当前目录。

```
<YourName>cd ..
<YourName>pwd
```

```
cfa0:
```

```
<YourName>
```

步骤十二：文件删除

用 **save** 命令保存一个配置文件并命名为 **20141030.cfg**，再使用 **delete** 删除该配置文件。

```
<YourName>save 20141030.cfg
The current configuration will be saved to cfa0:/20141030.cfg. Continue? [Y/N]:y
Now saving current configuration to the device.
Saving configuration cfa0:/20141030.cfg. Please wait...
Configuration is saved to device successfully.
```

```
<YourName>dir
```

```
Directory of cfa0:
```

```
 0 -rw-      1996 Oct 30 2014 14:01:34 20141030.cfg
 1 -rw-      32087 Oct 30 2014 14:01:34 20141030.mdb
 2 drw-        - Aug 11 2014 11:22:22 diagfile
 3 -rw-       158 Oct 30 2014 14:01:34 ifindex.dat
 4 drw-        - Aug 11 2014 11:22:22 license
 5 drw-        - Aug 11 2014 11:22:22 logfile
 6 -rw-    10381312 Dec 15 2011 09:00:00 msr36-cmw710-boot-r0106.bin
 7 -rw-    2006016 Dec 15 2011 09:00:00 msr36-cmw710-data-r0106.bin
 8 -rw-    351232 Dec 15 2011 09:00:00 msr36-cmw710-security-r0106.bin
 9 -rw-    47564800 Dec 15 2011 09:00:00 msr36-cmw710-system-r0106.bin
10 -rw-    1724416 Dec 15 2011 09:00:00 msr36-cmw710-voice-r0106.bin
11 drw-        - Aug 11 2014 11:22:22 seclog
12 -rw-       1996 Oct 30 2014 11:28:29 startup.cfg
13 -rw-      32087 Oct 30 2014 11:28:29 startup.mdb
```

```
252164 KB total (191504 KB free)
```

```
<YourName>delete 20141030.cfg
```

```
Delete cfa0:/20141030.cfg?[Y/N]:y
```

```
Deleting file cfa0:/20141030.cfg... Done.
```

删除 **20141030.cfg** 配置文件后，再次查看文件列表，确认该文件已经删除。

```
<YourName>dir
```

```
Directory of cfa0:
```

```
 0 -rw-      32087 Oct 30 2014 14:01:34 20141030.mdb
 1 drw-        - Aug 11 2014 11:22:22 diagfile
 2 -rw-       158 Oct 30 2014 14:01:34 ifindex.dat
 3 drw-        - Aug 11 2014 11:22:22 license
 4 drw-        - Aug 11 2014 11:22:22 logfile
 5 -rw-    10381312 Dec 15 2011 09:00:00 msr36-cmw710-boot-r0106.bin
 6 -rw-    2006016 Dec 15 2011 09:00:00 msr36-cmw710-data-r0106.bin
 7 -rw-    351232 Dec 15 2011 09:00:00 msr36-cmw710-security-r0106.bin
 8 -rw-    47564800 Dec 15 2011 09:00:00 msr36-cmw710-system-r0106.bin
 9 -rw-    1724416 Dec 15 2011 09:00:00 msr36-cmw710-voice-r0106.bin
10 drw-        - Aug 11 2014 11:22:22 seclog
11 -rw-       1996 Oct 30 2014 11:28:29 startup.cfg
12 -rw-      32087 Oct 30 2014 11:28:29 startup.mdb
```

```
252164 KB total (191500 KB free)
```

此时，虽然选择了 **Y** 删除该文件，但是在删除该文件前后，为什么 **CF** 卡的可用内存空间却反而变为了 **191500KB free** 了呢？

那是因为使用 **delete** 命令删除文件时，创建了回收站文件夹，添加的一些标记会占用存储空间，且被删除的文件仍会被保存在回收站中占用存储空间。如果用户经常使用该命令删除文件，则可能导致设备的存储空间不足。如果要彻底删除回收站中的某个废弃文件，必须在文件

的原归属目录下执行 **reset recycle-bin** 命令，才可以将回收站中的废弃文件彻底删除，以回收存储空间。

使用 **dir /all** 命令来显示当前目录下所有的文件及子文件夹信息，显示内容包括非隐藏文件、非隐藏文件夹、隐藏文件和隐藏子文件夹，回收站文件夹名为 **“.trash”**，可以通过命令 **dir /all .trash** 来查看回收站内有哪些文件。

```
<YourName>dir /all
Directory of cfa0:
 0 -rw-      32087 Oct 30 2014 14:15:18 20141030.mdb
 1 drw-          - Aug 11 2014 11:22:22 diagfile
 2 -rw-      158 Oct 30 2014 14:15:17 ifindex.dat
 3 drw-          - Aug 11 2014 11:22:22 license
 4 drw-          - Aug 11 2014 11:22:22 logfile
 5 -rw-    10381312 Dec 15 2011 09:00:00 msr36-cmw710-boot-r0106.bin
 6 -rw-    2006016 Dec 15 2011 09:00:00 msr36-cmw710-data-r0106.bin
 7 -rw-    351232 Dec 15 2011 09:00:00 msr36-cmw710-security-r0106.bin
 8 -rw-    47564800 Dec 15 2011 09:00:00 msr36-cmw710-system-r0106.bin
 9 -rw-    1724416 Dec 15 2011 09:00:00 msr36-cmw710-voice-r0106.bin
10 drw-          - Aug 11 2014 11:22:22 seclog
11 -rw-      1996 Oct 30 2014 11:28:29 startup.cfg
12 -rw-      32087 Oct 30 2014 11:28:29 startup.mdb
13 drwh          - Oct 30 2014 14:15:30 .trash

252164 KB total (191500 KB free)

<YourName>dir /all .trash
Directory of cfa0:/.trash
 0 -rw-      1996 Oct 30 2014 14:15:18 20141030.cfg_0001
 1 -rwh        51 Oct 30 2014 14:15:30 .trashinfo

252164 KB total (191500 KB free)
```

可见文件 **20141030.cfg** 仍然存在于 CF 卡中，使用 **reset recycle-bin** 命令清空回收站回收存储空间。

```
<YourName>reset recycle-bin
Clear cfa0:/20141030.cfg?[Y/N]:y
Clearing file cfa0:/20141030.cfg... Done.

<YourName>dir /all .trash
Directory of cfa0:/.trash
 0 -rwh          0 Oct 30 2014 14:26:49 .trashinfo

252164 KB total (191504 KB free)
```

清空回收站后，可见已经删除了 **20141030.cfg** 文件，并且可用内存空间已经变为 **191504KB**。

还有另一种方法可以直接删除文件，而不需要经过清空回收站。使用 **delete /unreserved** 命令删除某个文件，则该文件将被彻底删除，不能再恢复。其效果等同于执行 **delete** 命令之后，再在同一个目录下执行了 **reset recycle-bin** 命令。

```
<YourName>delete /unreserved 20141030.mdb
The file cannot be restored. Delete cfa0:/20141030.mdb?[Y/N]:y
Deleting the file permanently will take a long time. Please wait...
Deleting file cfa0:/20141030.mdb... Done.
<YourName>dir /all .trash
Directory of cfa0:/.trash
 0 -rwh          0 Oct 30 2014 14:26:49 .trashinfo
```

252164 KB total (191536 KB free)

实验任务三：通过 Telnet 登录

步骤一：通过 Console 口配置 Telnet 用户

```
<YourName>sys
System View: return to User View with Ctrl+Z.
[YourName]
```

创建一个用户，用户名为 **test**。

```
[YourName]local-user test
New local user added.
```

为该用户创建登入时的认证密码，密码为 **test**。这里可用 **password** 命令指定密码配置方式。密码有两种配置方式，**simple** 关键字指定以明文方式配置密码，**cipher** 则指定以密文方式配置密码。

```
[YourName-luser-manage-test] password simple test
```

设置该用户使用 **telnet** 服务类型，该用户的用户角色 **user-role** 为 **level-0**（**level-number** 中的 **number** 对应用户角色的级别，数值越小，用户的权限级别越低）。

```
[YourName-luser-manage-test] service-type telnet
[YourName-luser-manage-test] authorization-attribute user-role level-0
[YourName-luser-manage-test] quit
[YourName]
```

步骤二：配置 super 口令

super 命令用来将用户从当前级别切换到指定级别。设置将用户切换到 **level-15** 的密码为 **H3C**，密码使用明文配置。

```
[YourName] super password role level-15 simple H3C
```

步骤三：配置登录欢迎信息

设置登录验证时的欢迎信息为“Welcome to H3C world!”。“%”为 **text** 的结束字符，在显示文本后输入“%”表示文本结束，退出 **header** 命令。

```
[YourName]header login
Please input banner content, and quit with the character '%'.
Welcome to H3C world!%
[YourName]
```

步骤四：配置对 Telnet 用户使用缺省的本地认证

进入 **VTY 0~63** 用户线，系统支持 **64** 个 **VTY** 用户同时访问。**VTY** 口属于逻辑终端线，用于对设备进行 **Telnet** 或 **SSH** 访问。

```
[YourName]line vty 0 63
```

路由器可以采用本地或第三方服务器来对用户进行认证，这里使用本地认证授权方式（认证模式为 **scheme**）。

```
[YourName-line-vty0-63]authentication-mode scheme
```

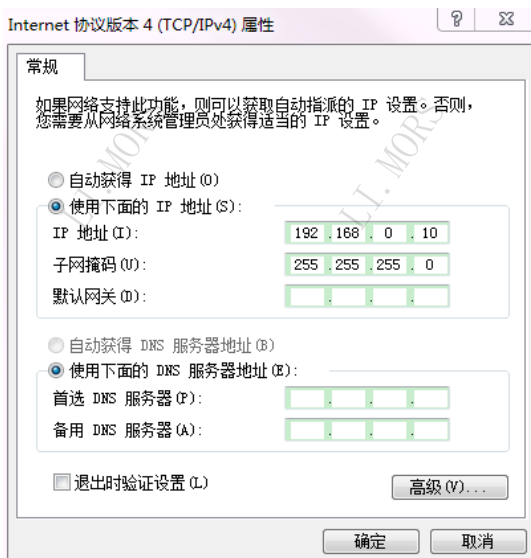
步骤五：进入接口视图，配置以太口和 PC 网卡地址

使用 **interface** 命令进入以太网接口视图，使用命令 **ip address** 配置路由器以太口地址。

```
[YourName]interface GigabitEthernet 0/1
```

```
[YourName-GigabitEthernet0/1]ip add 192.168.0.1 255.255.255.0  
[YourName-GigabitEthernet0/1]
```

同时为 PC 设置一个与路由器接口相同网段的 IP 地址 192.168.0.10/24。



配置完 PC 后，在 PuTTY 上能看到路由器接口 GigabitEthernet0/1 自动 UP 的信息。

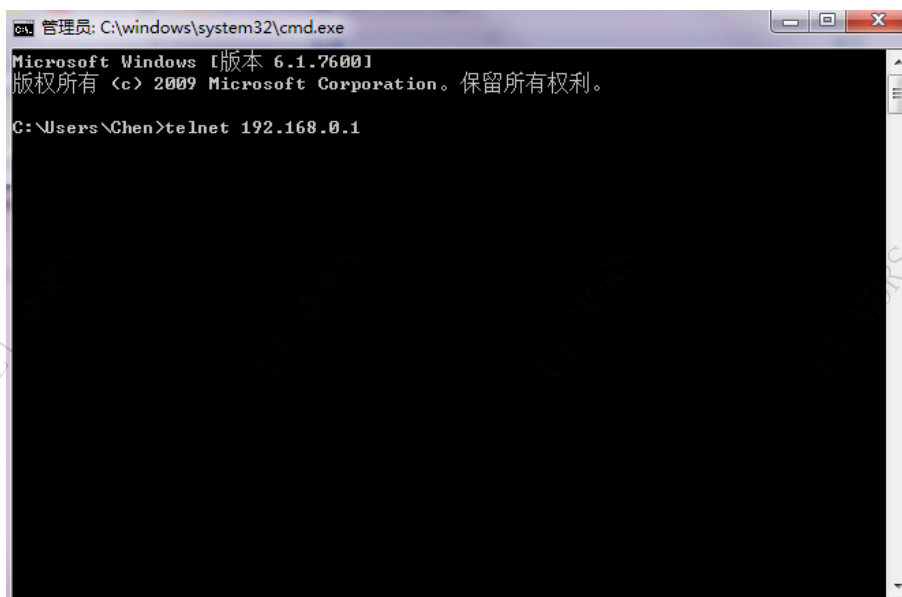
```
%Oct 30 14:44:53:892 2014 YourName IFNET/3/PHY_UPDOWN: Physical state on the  
interface GigabitEthernet0/1 changed to up.  
%Oct 30 14:44:53:893 2014 YourName IFNET/5/LINK_UPDOWN: Line protocol state on  
the interface GigabitEthernet0/1 changed to up.
```

步骤六：打开 Telnet 服务

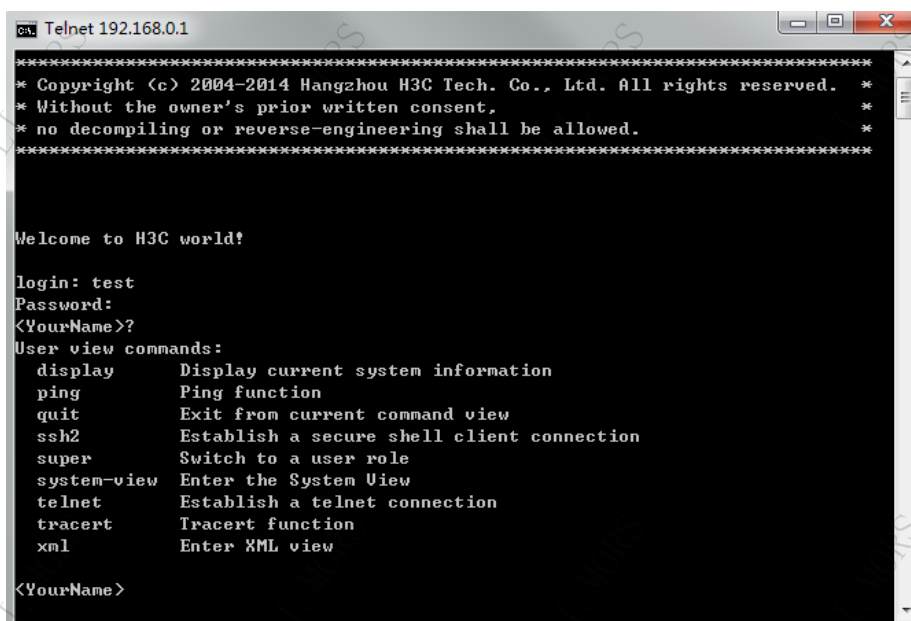
```
[YourName]telnet server enable
```

步骤七：使用 Telnet 登录

使用交叉网线连接 PC 和路由器的以太网口 GigabitEthernet0/1，在 PC 命令行窗口中，Telnet 路由器的以太网口 IP 地址，并键入回车。



输入 Telnet 用户名及口令, 进入配置界面, 使用<?>查看此时该用户角色(level-0)可使用的命令。由于此时登录用户处于最低级别, 所以只能看到并使用有限的几个命令。

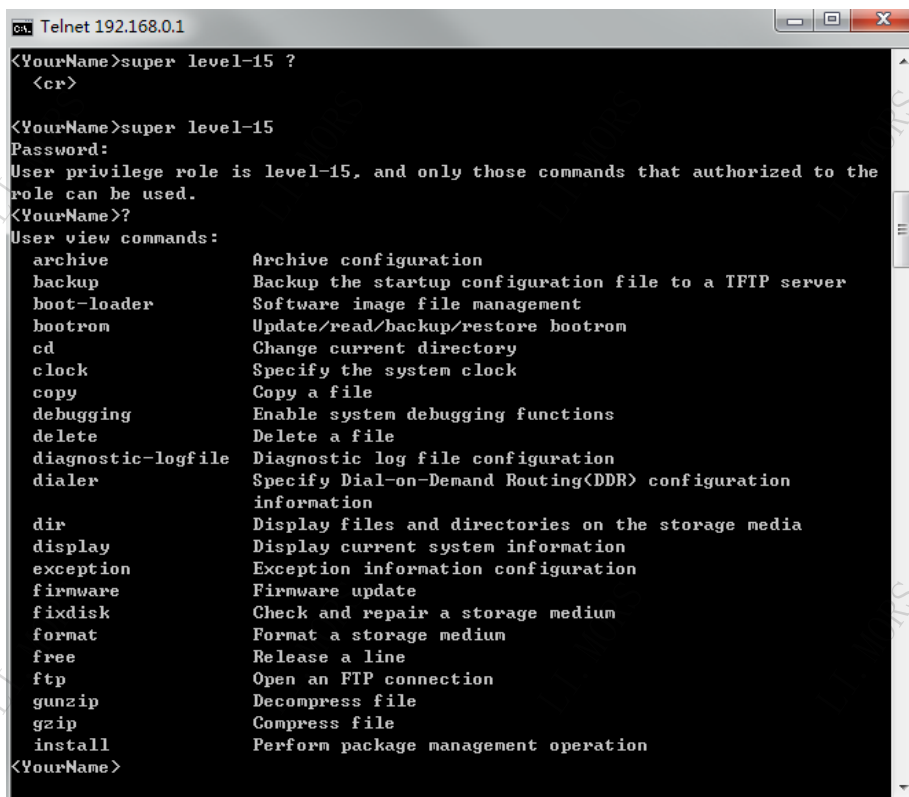


同时, PuTTY 上会有如下信息显示, 表明源 IP 为 192.168.0.10 的设备远程登入到路由器上。

```
<YourName>
%Oct 30 14:50:41:823 2014 YourName SHELL/5/SHELL_LOGIN: test logged in from
192.168.0.10.
```

步骤八：更改登录用户级别

使用 **super** 命令切换用户级别，输入 **super** 口令，进入 **level-15**，与 **level0** 能够使用的命令进行对比。



```
cs: Telnet 192.168.0.1
<YourName>super level-15 ?
<cr>

<YourName>super level-15
Password:
User privilege role is level-15, and only those commands that authorized to the
role can be used.
<YourName>?
User view commands:
archive          Archive configuration
backup           Backup the startup configuration file to a TFTP server
boot-loader      Software image file management
bootrom          Update/read/backup/restore bootrom
cd               Change current directory
clock            Specify the system clock
copy             Copy a file
debugging        Enable system debugging functions
delete           Delete a file
diagnostic-logfile Diagnostic log file configuration
dialer           Specify Dial-on-Demand Routing(DDR) configuration
information
dir              Display files and directories on the storage media
display          Display current system information
exception         Exception information configuration
firmware         Firmware update
fixdisk          Check and repair a storage medium
format           Format a storage medium
free             Release a line
ftp              Open an FTP connection
gunzip           Decompress file
gzip             Compress file
install          Perform package management operation
<YourName>
```

步骤九：保存配置，重新启动

先使用 **save** 命令保存当前配置到设备存储介质中，再使用 **reboot** 命令重新启动系统。

```

bootrom          Update/read/backup/restore bootrom
cd               Change current directory
clock           Specify the system clock
copy            Copy a file
debugging        Enable system debugging functions
delete          Delete a file
diagnostic-logfile Diagnostic log file configuration
dialer           Specify Dial-on-Demand Routing(DDR) configuration
                 information
dir             Display files and directories on the storage media
display          Display current system information
exception        Exception information configuration
firmware         Firmware update
fixdisk          Check and repair a storage medium
format           Format a storage medium
free            Release a line
ftp             Open an FTP connection
gunzip           Decompress file
gzip            Compress file
install          Perform package management operation

<YourName>save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[cfa0:/startup.cfg]
<To leave the existing filename unchanged, press the enter key>:
cfa0:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait...
Configuration is saved to device successfully.
<YourName>reboot
Start to check configuration with next startup configuration file, please wait..
.....DONE!
This command will reboot the device. Continue? [Y/N]:y
Now rebooting, please wait...

```

实验任务四：使用 FTP 上传下载系统文件

步骤一：通过 Console 口配置 FTP 用户

```

[YourName]local-user test_ftp
New local user added.
[YourName-luser-manage-test_ftp] password simple test_ftp

```

设置该用户使用 FTP 服务类型，并设置该用户的用户角色为 level-15。

```

[YourName-luser-manage-test_ftp] service-type ftp
[YourName-luser-manage-test_ftp] authorization-attribute user-role level-15

```

步骤二：打开 FTP 服务

```

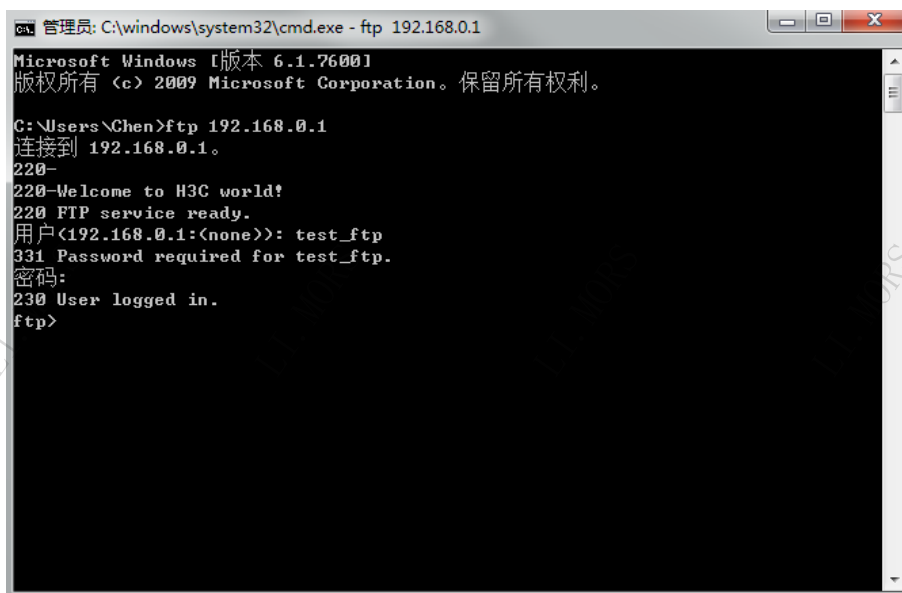
[YourName]ftp server enable

```

步骤三：使用 FTP 登录

使用交叉网线连接 PC 和路由器的以太网口 GigabitEthernet0/1，在 PC 命令行窗口中，FTP 路由器的以太网口 IP 地址，并键入回车。

输入 FTP 用户名及口令：

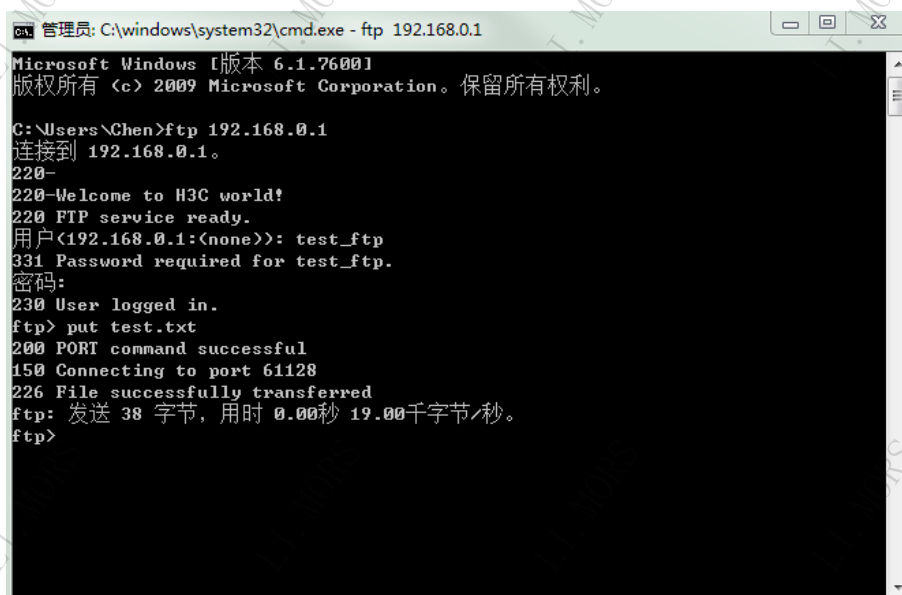


```
管理员: C:\windows\system32\cmd.exe - ftp 192.168.0.1
Microsoft Windows [版本 6.1.7600]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\Chen>ftp 192.168.0.1
连接到 192.168.0.1。
220-
220-Welcome to H3C world!
220 FTP service ready.
用户(192.168.0.1:(none)): test_ftp
331 Password required for test_ftp.
密码:
230 User logged in.
ftp>
```

步骤四：使用 FTP 上传文件

使用 `put` 命令上传系统文件。实验中任意创建一个大小合适的文件来模拟系统文件，该上传文件应该存在于上传者的本地目录中，这里本地目录是 `C:\Users\Chen`。



```
管理员: C:\windows\system32\cmd.exe - ftp 192.168.0.1
Microsoft Windows [版本 6.1.7600]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\Chen>ftp 192.168.0.1
连接到 192.168.0.1。
220-
220-Welcome to H3C world!
220 FTP service ready.
用户(192.168.0.1:(none)): test_ftp
331 Password required for test_ftp.
密码:
230 User logged in.
ftp> put test.txt
200 PORT command successful
150 Connecting to port 61128
226 File successfully transferred
ftp: 发送 38 字节, 用时 0.00秒 19.00千字节/秒。
ftp>
```

步骤五：使用 FTP 下载文件

使用 FTP 中的 `get` 命令下载配置文件到本地目录。

```

管理员: C:\windows\system32\cmd.exe

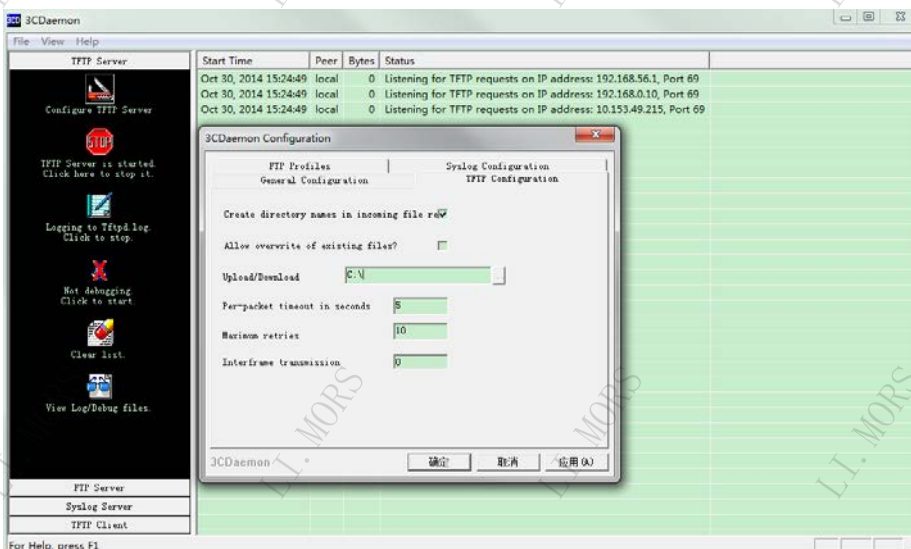
-rwxrwxrwx 1 0 0 10381312 Dec 15 2011 msr36-cmw710-boot-
r0106.bin
-rwxrwxrwx 1 0 0 2006016 Dec 15 2011 msr36-cmw710-data-
r0106.bin
-rwxrwxrwx 1 0 0 351232 Dec 15 2011 msr36-cmw710-secu-
rity-r0106.bin
-rwxrwxrwx 1 0 0 47564800 Dec 15 2011 msr36-cmw710-syste
m-r0106.bin
-rwxrwxrwx 1 0 0 1724416 Dec 15 2011 msr36-cmw710-voice
r0106.bin
drwxrwxrwx 2 0 0 2048 Aug 11 11:22 seclog
-rwxrwxrwx 1 0 0 2563 Oct 30 14:55 startup.cfg
-rwxrwxrwx 1 0 0 42834 Oct 30 14:55 startup.mdb
226 12 matches total
ftp: 收到 971 字节, 用时 0.01秒 194.20千字节/秒。
ftp> get startup.cfg
200 PORT command successful
150 Connecting to port 61109
226 File successfully transferred
ftp: 收到 2690 字节, 用时 0.01秒 269.00千字节/秒。
ftp> bye
221-Goodbye. You uploaded 0 and downloaded 3 kbytes.
221 Logout.
C:\Users\Chen>

```

实验任务五：使用 TFTP 上传下载系统文件

步骤一：启动 TFTP 服务器端程序

本实验以 3CDaemon 程序作为 TFTP 的服务器端为例介绍。设置 TFTP Server 参数，选择当前用于上传和下载的本地目录（C:\）。



步骤二：使用 TFTP 下载文件

```
<YourName>tftp 192.168.0.10 get MUI.txt
```

```
Press CTRL+C to abort.
```

```

% Total      % Received % Xferd  Average Speed   Time    Time     Time  Current
   Dload  Upload  Total    Spent    Left     Speed
100  598  100  598    0    0    25817      0  --:--:-- --:--:-- --:--:-- 116k

```

步骤三：使用 TFTP 上传文件

```
<YourName>tftp 192.168.0.10 put startup.cfg
Press CTRL+C to abort.
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload  Total  Spent    Left  Speed
 100  2563    0    0  100  2563    0  124k  --:--:--  --:--:--  --:--:--  417k
```

1.5 实验中的命令列表

表1-2 命令列表

命令	描述
system-view	进入系统视图
sysname	更改设备名
quit	退出
clock	更改时钟配置
display current-configuration	显示当前配置
display saved-configuration	显示保存配置
reset saved-configuration	清空保存配置
pwd	显示当前目录
dir	列目录
more	显示文本文件
cd	更改当前目录
delete	删除文件
reset recycle-bin	清空回收站
local-user	配置本地用户
super password role	配置Super口令
header login	配置Login欢迎信息
line vty	进入用户线
authentication-mode	设置认证模式
telnet server enable	启动Telnet
save	保存配置
reboot	重启系统
ftp server enable	启动FTP Server
tftp get	使用TFTP
tftp put	使用TFTP

1.6 思考题

1. 在实验任务二的步骤五中，为何看不到在步骤四中配置的系统时间？

答：**clock** 属于更改系统硬件参数的命令，即时生效，因此并不作为配置命令显示在当前配置或保存配置文件中。

2. 在实验任务二的步骤十二中，使用命令 **save 20141030.cfg** 保存配置文件后，使用 **dir** 可以查看到这时在 **cfa0:/** 目录下有两个 **.cfg** 配置文件，当系统重启后，将自动载入哪个配置文件？

答：系统重新启动后，将自动载入系统默认的 **startup.cfg** 配置文件。使用命令 **display startup** 可以清楚地看到系统下一次启动时所要加载的配置文件。

同时，我们也可以使用命令 **startup saved-configuration** 来更改系统重启后加载的配置文件的顺序（主用和备用）。

3. 在实验任务三中步骤四中，如果要求用户 **Telnet** 后无需密码认证直接登入到系统，该如何修改配置？

答：将配置命令 **authentication-mode scheme** 改成 **authentication-mode none** 即可。注意，当用户远程登入后，仍然需要通过 **Super** 命令来切换用户角色。

4. 在实验任务四的步骤一中，如果不授权用户角色为 **level-15**，后续实验会有何结果？

答：由于缺省的用户角色为 **network-operator**，执行 **PUT** 操作时将被设备拒绝。

实验2 网络设备基本连接与调试

2.1 实验内容与目标

完成本实验，您应该能够：

- 掌握路由器通过串口相连的基本方法
- 掌握 ping、tracert 系统连通检测命令的使用方法
- 掌握 debug 命令的使用方法

2.2 实验组网图

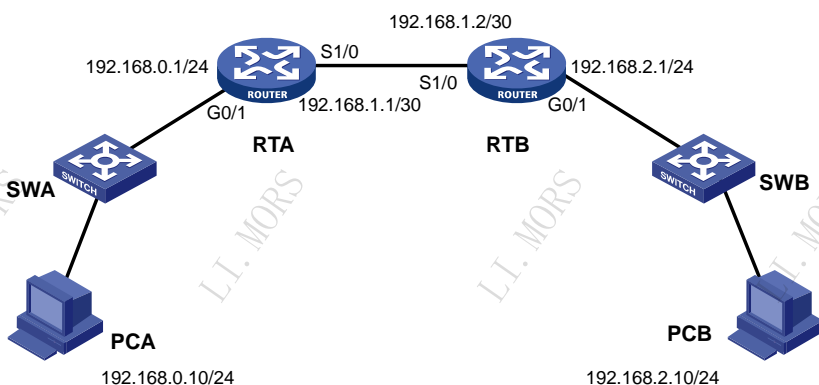


图2-1 实验组网图

2.3 实验设备与版本

本实验所需主要设备器材如表 2-1 所示。

表2-1 实验设备器材

名称和型号	版本	数量	描述
MSR36-20	CMW 7.1.049-R0106	2	
S5820V2	CMW 7.1.035-R2210	2	
PC	Windows 7	2	
DTE串口线	--	1	
DCE串口线	--	1	
第5类UTP以太网连接线	--	4	

2.4 实验过程

实验任务一：搭建基本连接环境

本实验任务供学员熟悉并掌握路由器、交换机、PC 的基本网络连接配置。

步骤一：完成 PC、交换机、路由器互连

在教师指导下，完成两台路由器通过串口电缆背靠背相连；路由器以太网口分别下接一台交换机（S5820V2）；PC 通过网线连接到交换机端口上。

步骤二：配置 IP 地址

将所有设备的配置清空重启后开始下面的配置。

使用 `ip address` 命令配置路由器的串口和以太网口 IP 地址。

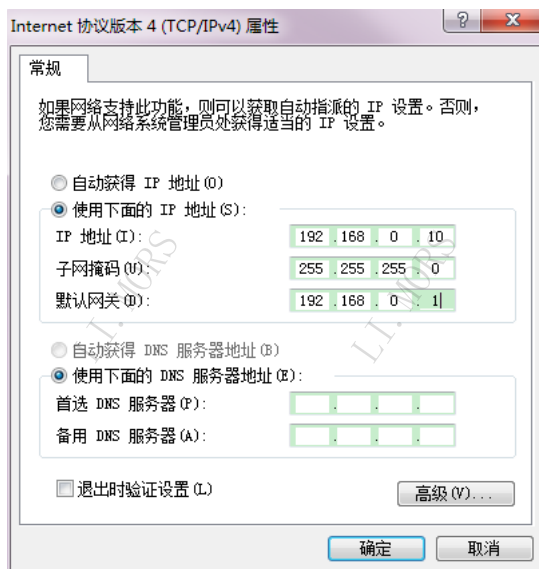
RTA 的配置如下：

```
[H3C]sysname RTA
[RTA]interface GigabitEthernet 0/1
[RTA-GigabitEthernet0/1]ip add 192.168.0.1 24
[RTA]interface Serial 1/0
[RTA-Serial1/0]ip address 192.168.1.1 30
```

RTB 的配置如下：

```
[H3C]sysname RTB
[RTB]interface GigabitEthernet 0/1
[RTB-GigabitEthernet0/1]ip add 192.168.2.1 24
[RTA]interface Serial 1/0
[RTA-Serial1/0]ip address 192.168.1.2 30
```

PCA 的网络 IP 地址设置如下：



PCA 通过二层交换机连接到路由器接口 G0/1，那么 PCA 的网关地址应设置为路由器的接口 G0/1 的 IP 地址。

实验任务二：使用 ping 命令检查连通性

步骤一：RTA ping RTB

通过 PuTTY 登入到 RTA 后，ping RTB 的串口 S1/0，检查路由器之间串口的连通性。

```
[RTA]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=255 time=24.696 ms
56 bytes from 192.168.1.2: icmp_seq=1 ttl=255 time=24.235 ms
56 bytes from 192.168.1.2: icmp_seq=2 ttl=255 time=24.058 ms
56 bytes from 192.168.1.2: icmp_seq=3 ttl=255 time=24.251 ms
56 bytes from 192.168.1.2: icmp_seq=4 ttl=255 time=24.121 ms

--- Ping statistics for 192.168.1.2 ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 24.058/24.272/24.696/0.224 ms
[RTA]%Oct 30 16:56:30:560 2014 RTA PING/6/PING_STATISTICS: Ping statistics for
192.168.1.2: 5 packets transmitted, 5 packets received, 0.0% packet loss,
round-trip min/avg/max/std-dev = 24.058/24.272/24.696/0.224 ms.
```

结果显示，RTA 收到了 ICMP 的 Echo Reply 报文，RTA 可以 ping 通 RTB。反之亦然。

这里路由器默认是发送 5 个 ICMP 请求报文，大小是 56bytes，所以 ping 成功后，会收到 5 个 Reply 报文。而 Windows 默认是发送 4 个 ICMP 请求报文，大小是 32bytes。

查看路由器 ping 命令携带的参数：

```
<RTA>ping ?
-a          Specify the source IP address
-c          Specify the number of echo requests
-f          Specify packets not to be fragmented
-h          Specify the TTL value
-i          Specify an outgoing interface
-m          Specify the interval for sending echo requests
-n          Numeric output only. No attempt will be made to lookup host
            addresses for symbolic names
-p          No more than 8 "pad" hexadecimal characters to fill out the
            sent packet. For example, -p f2 will fill the sent packet with
            000000f2 repeatedly
-q          Display only summary
-r          Record route. Include the RECORD_ROUTE option in the
            ECHO_REQUEST packets and display the route
-s          Specify the payload length
-t          Specify the wait time for each reply
-topology   Specify a topology
-tos        Specify the TOS value
-v          Display the received ICMP packets other than ECHO-RESPONSE
            packets
-vpn-instance Specify a VPN instance
STRING<1-253> IP address or hostname of remote system
ip          IP information
ipv6        IPv6 information
```

例如，可以使用参数 -c 来设定发送 50 个 ping 报文：

```
<RTA>ping -c 50 192.168.1.2
```

可以使用 -s 参数来设定发送 ping 报文的字节为 512bytes：

```
<RTA>ping -s 512 192.168.1.2
Ping 192.168.1.2 (192.168.1.2): 512 data bytes, press CTRL_C to break
512 bytes from 192.168.1.2: icmp_seq=0 ttl=255 time=140.468 ms
512 bytes from 192.168.1.2: icmp_seq=1 ttl=255 time=140.232 ms
512 bytes from 192.168.1.2: icmp_seq=2 ttl=255 time=140.099 ms
512 bytes from 192.168.1.2: icmp_seq=3 ttl=255 time=140.228 ms
```

```
512 bytes from 192.168.1.2: icmp_seq=4 ttl=255 time=140.216 ms
```

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

```
5 packets transmitted, 5 packets received, 0.0% packet loss
```

```
round-trip min/avg/max/std-dev = 140.099/140.249/140.468/0.120 ms
```

```
[RTA]Oct 30 17:00:57:047 2014 RTA PING/6/PING_STATISTICS: Ping statistics for 192.168.1.2: 5 packets transmitted, 5 packets received, 0.0% packet loss, round-trip min/avg/max/std-dev = 140.099/140.249/140.468/0.120 ms.
```

也可以使用 **-a** 参数来设定 ping 报文的源地址，在网络调试中常常使用加源 ping 来检查网络的连通性。这里使用 RTA 接口 G0/1 地址为源，ping PCB：

```
<RTA>ping -a 192.168.0.1 192.168.2.10
```

```
Ping 192.168.2.10 (192.168.2.10) from 192.168.0.1: 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 192.168.2.10 ---
```


```
5 packets transmitted, 0 packets received, 100.0% packet loss
```

```
[RTA]Oct 30 17:01:44:917 2014 RTA PING/6/PING_STATISTICS: Ping statistics for 192.168.2.10: 5 packets transmitted, 0 packets received, 100.0% packet loss.
```

加源地址 ping 时，只能使用设备自身的本地接口地址。此时 ping 不通的原因，请先思考，在后面的步骤三中会找到答案。

步骤二：PCA ping RTA

进入 PCA 命令行窗口，ping RTA 的 G0/1 口和 S1/0 口地址。



```

CA 管理员: C:\windows\system32\cmd.exe

Microsoft Windows [版本 6.1.7600]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\Chen>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=1ms TTL=255
来自 192.168.0.1 的回复: 字节=32 时间=20ms 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 = 0ms, 最长 = 20ms, 平均 = 5ms

C:\Users\Chen>
  
```



```
管理员: C:\windows\system32\cmd.exe

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=20ms 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 = 0ms, 最长 = 20ms, 平均 = 5ms

C:\Users\Chen>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=20ms TTL=255
来自 192.168.1.1 的回复: 字节=32 时间<1ms TTL=255
来自 192.168.1.1 的回复: 字节=32 时间<1ms TTL=255
来自 192.168.1.1 的回复: 字节=32 时间<1ms TTL=255

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 = 0ms, 最长 = 20ms, 平均 = 5ms

C:\Users\Chen>
```

步骤三: PCA ping RTB

进入 PCA 命令行窗口, ping RTB 的接口 S1/0 的 IP 地址。

```
管理员: C:\windows\system32\cmd.exe

C:\Users\Chen>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=20ms TTL=255
来自 192.168.1.1 的回复: 字节=32 时间<1ms TTL=255
来自 192.168.1.1 的回复: 字节=32 时间<1ms TTL=255
来自 192.168.1.1 的回复: 字节=32 时间<1ms TTL=255

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 = 0ms, 最长 = 20ms, 平均 = 5ms

C:\Users\Chen>ping 192.168.1.2

正在 Ping 192.168.1.2 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。

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

C:\Users\Chen>
```

步骤四: PCA ping PCB

进入 PCA 命令行窗口, ping PCB 的 IP 地址。

```

管理员: C:\windows\system32\cmd.exe

最短 = 0ms, 最长 = 20ms, 平均 = 5ms

C:\Users\Chen>ping 192.168.1.2

正在 Ping 192.168.1.2 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。

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

C:\Users\Chen>ping 192.168.2.10

正在 Ping 192.168.2.10 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。

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

C:\Users\Chen>

```

结果显示，PCA 无法 ping 通 PCB 的 IP 地址。这是为什么呢？

让我们一步一步来排查为什么 ping 不通。

首先，PCA ping RTA 的 G0/1 端口和 S1/0，结果显示可以 ping 通。

其次，PCA ping RTB 的 S1/0 端口，结果显示无法 ping 通。

最后，PCA ping PCB，结果显示无法 ping 通。

结果证明，由 PCA 发送给 RTB 和 PCB 的 ICMP 请求报文（Echo Request），没有收到回应报文（Echo Reply）。

在 RTA 上使用 display ip routing-table 命令查看一下 RTA 的路由表：

```

[RTA]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
192.168.0.0/24	Direct	0	0	192.168.0.1	GE0/1
192.168.0.0/32	Direct	0	0	192.168.0.1	GE0/1
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	GE0/1
192.168.1.0/30	Direct	0	0	192.168.1.1	S1/0
192.168.1.0/32	Direct	0	0	192.168.1.1	S1/0
192.168.1.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.1.2/32	Direct	0	0	192.168.1.2	S1/0
192.168.1.3/32	Direct	0	0	192.168.1.1	S1/0
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

在路由表 Destination 项中，没有看到 192.168.2.0 表项，所以 RTA 当收到 PCA 发送给 PCB 的 ping 报文后，不知道如何转发，会丢弃该报文。结果就是 PCA 无法 ping 通 PCB。

但是在路由表中，有具体路由表项 192.168.1.2，为什么 PCA 还是无法 ping 通 RTB 的串口 S1/0 呢？因为在 RTB 的路由表中没有 192.168.0.0 表项，所以虽然 RTA 将 PCA ping 请求报文发送给了 RTB，但是 RTB 不知道如何转发 ping 的回应报文给 PCA。所以，PCA 也无法 ping 通 RTB 的串口 S1/0。

通过上面的分析，对步骤一最后一项测试 “<RTA>ping -a 192.168.0.1 192.168.2.10” 不通的原因就非常清楚了，就是 RTA 没有到 192.168.2.0/24 网段的路由，RTB 也没有到达 192.168.0.0/24 网段的路由。

步骤五：配置静态路由

使用 ip route-static 命令分别在路由器 RTA 和 RTB 上配置静态路由，目的网段为对端路由器与 PC 的互连网段，并将路由下一跳指向对端路由器的接口地址。

RTA 上配置

```
[RTA]ip route-static 192.168.2.0 255.255.255.0 192.168.1.2
```

RTB 上配置

```
[RTB]ip route-static 192.168.0.0 255.255.255.0 192.168.1.1
```

步骤六：PCA ping PCB



可见，在 RTA 和 RTB 上配置完静态路由后，PCA 可以 ping 通 PCB。

步骤七：以 RTA 接口 G0/1 地址为源，ping PCB

```
[RTA]ping -a 192.168.0.1 192.168.2.10
Ping 192.168.2.10 (192.168.2.10) from 192.168.0.1: 56 data bytes, press CTRL_C
to break
56 bytes from 192.168.2.10: icmp_seq=0 ttl=255 time=24.344 ms
56 bytes from 192.168.2.10: icmp_seq=1 ttl=255 time=24.124 ms
56 bytes from 192.168.2.10: icmp_seq=2 ttl=255 time=24.203 ms
56 bytes from 192.168.2.10: icmp_seq=3 ttl=255 time=26.307 ms
56 bytes from 192.168.2.10: icmp_seq=4 ttl=255 time=24.233 ms
```

```

--- Ping statistics for 192.168.2.10 ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 24.124/24.642/26.307/0.835 ms
[RTA]%Oct 30 17:23:57:840 2014 RTA PING/6/PING_STATISTICS: Ping statistics for
192.168.2.10: 5 packets transmitted, 5 packets received, 0.0% packet loss,
round-trip min/avg/max/std-dev = 24.124/24.642/26.307/0.835 ms.

```

实验任务三：使用 tracert 命令检查连通性

通过使用 **tracert** 命令，用户可以查看报文从源设备传送到目的设备所经过的路由节点。当网络出现故障时，用户可以使用该命令分析出现故障的网络节点。

步骤一：PCA tracert PCB

进入 PCA 命令行窗口，tracert PCB 的 IP 地址。

```

Microsoft Windows [版本 6.1.7600]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\Chen>tracert 192.168.2.10

通过最多 30 个跃点跟踪到 192.168.2.10 的路由

 1  19 ms    <1 毫秒    <1 毫秒  192.168.0.1
 2  22 ms    22 ms    22 ms    192.168.1.2
 3  27 ms    26 ms    26 ms    192.168.2.10

跟踪完成。

C:\Users\Chen>

```

从显示结果看，PCA 收到了三个 TTL 超时 ICMP 报文，第一跳为 192.168.0.1 表明第一个报文是由 RTA 返回，以此类推，第二个报文由 RTB 返回，第三个报文由 PCB 返回，可见这三个网络节点都是 IP 可达的。如果其中一个节点是不可达的，则不会返回 TTL 超时报文，从而判断该网络节点为故障网络节点，IP 不可达。

步骤二：在 RTA 上 tracert PCB

在 RTA 上执行 tracert PCB 的 IP 地址：

```

<RTA>tracert 192.168.2.10
traceroute to 192.168.2.10 (192.168.2.10), 30 hops at most, 52 bytes each packet,
press CTRL_C to break
 1  192.168.1.2 (192.168.1.2)  16.691 ms  16.620 ms  16.556 ms
 2  192.168.2.10 (192.168.2.10)  16.636 ms  16.624 ms  16.569 ms

```

结果显示第一跳为 RTB，第二跳为 PCB。

查看路由器 **tracert** 命令携带的参数：

```

<RTA>tracert ?
-a          Specify the source IP address used by TRACERT
-f          Specify the TTL value for the first packet

```

```

-m          Specify the maximum TTL value
-p          Specify the destination UDP port number
-q          Specify the number of probe packets sent each time
-t          Set the Type of Service (ToS) value
-topology   Specify a topology
-vpn-instance Specify a VPN instance
-w          Set the timeout to wait for each reply
STRING<1-253> IP address or hostname of the destination device
ipv6        IPv6 information

```

实验任务四：使用 debugging 命令察看调试信息

步骤一：开启 RTB 终端对信息的监视和显示功能

在 RTB 上执行命令 **terminal monitor** 用于开启终端对系统信息的监视功能，执行命令 **terminal debugging** 用于开启终端对调试信息的显示功能。

```

<RTB>terminal monitor
The current terminal is enabled to display logs.
<RTB>terminal debugging
The current terminal is enabled to display debugging logs.

```

步骤二：打开 RTB 上 ICMP 的调试开关

在 RTB 上执行命令 **debugging ip icmp** 用于开启系统 ICMP 模块的调试功能。

```
<RTB>debugging ip icmp
```

步骤三：在 RTA 上 ping RTB，观察 RTB 调试信息输出

在 RTA 上 ping RTB 的串口地址，连续发送 10 个 ping 报文。

```
<RTA>ping -c 10 192.168.1.2
```

在 RTB 上观察 **debugging** 信息输出：

```

*Oct 30 17:41:30:970 2014 RTB SOCKET/7/ICMP:
Time(s):1414690890 ICMP Input:
ICMP Packet: src = 192.168.1.1, dst = 192.168.1.2
                type = 8, code = 0 (echo)

*Oct 30 17:41:30:970 2014 RTB SOCKET/7/ICMP:
Time(s):1414690890 ICMP Output:
ICMP Packet: src = 192.168.1.2, dst = 192.168.1.1
                type = 0, code = 0 (echo-reply)

*Oct 30 17:41:31:195 2014 RTB SOCKET/7/ICMP:
Time(s):1414690891 ICMP Input:
ICMP Packet: src = 192.168.1.1, dst = 192.168.1.2
                type = 8, code = 0 (echo)

*Oct 30 17:41:31:195 2014 RTB SOCKET/7/ICMP:
Time(s):1414690891 ICMP Output:
ICMP Packet: src = 192.168.1.2, dst = 192.168.1.1
                type = 0, code = 0 (echo-reply)

```

第一条信息为 RTB 收到 ICMP 报文，类型 Type=8 为 Echo 报文，源地址为 192.168.1.1，目的地址为 192.168.1.2。第二条信息为 RTB 发出的 ICMP 报文，类型 Type=0 为 Echo-Reply 报文，源地址为 192.168.1.2，目的地址为 192.168.1.1。

步骤四：关闭调试开关

调试结束后，使用 **undo debugging all** 命令，关闭所有模块的调试开关。

2.5 实验中的命令列表

表2-2 命令列表

命令	描述
ip address	配置IP地址
ip route-static	配置静态路由
ping	检测连通性
tracert	探测转发路径
terminal monitor	开启终端对系统信息的监视功能
terminal debugging	开启终端对调试信息的显示功能
debugging	打开系统指定模块调试开关

2.6 思考题

1. 在实验任务二的步骤一中，使用的是“ping 192.168.1.2”基本 ping 命令，如果使用“ping -a 192.168.0.1 192.168.1.2”扩展 ping 命令，效果有何不同，路由器对报文处理有何不同？

答：不使用扩展 ping 命令时，“ping 192.168.1.2”发出的 ICMP 响应请求报文的源地址为出接口地址 192.168.1.1。使用扩展命令后，源地址将被指定为 192.168.0.1。因此 RTB 在回应 ICMP 响应时的目的 IP 地址是不同的。

实验3 配置 VLAN

3.1 实验内容与目标

完成本实验，您应该能够：

- 掌握 VLAN 的基本工作原理
- 掌握 Access 链路端口和 Trunk 链路端口的配置

3.2 实验组网图

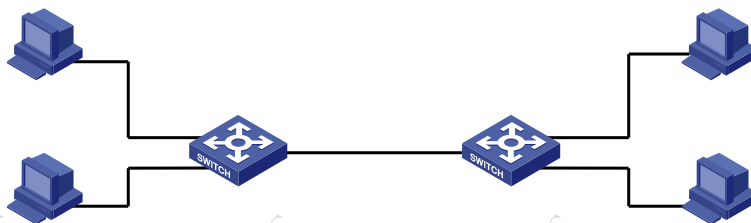


图3-1 VLAN 实验环境图

实验组网如图 3-1 所示。

3.3 实验设备与版本

本实验所需之主要设备器材如表 3-1 所示。

表3-1 设备列表

名称和型号	版本	数量	描述
S5820V2	CMW710-R2311P03	2	
PC	Windows XP SP2	4	
第5类UTP以太网连接线	--	5	

3.4 实验过程

实验任务一：配置 Access 链路端口

本实验任务通过在交换机上配置 Access 链路端口而使 PC 间处于不同 VLAN，隔离 PC 间的访问，从而使学员加深对 Access 链路端口的理解。

步骤一：建立物理连接

按照图 3-1 进行连接,并检查设备的软件版本及配置信息,确保各设备软件版本符合要求,所有配置为初始状态。如果配置不符合要求,请读者在用户模式下擦除设备中的配置文件,然后重启设备以使系统采用缺省的配置参数进行初始化。

以上步骤可能会用到以下命令:

```
<SWA> display version
<SWA> reset saved-configuration
<SWA> reboot
```

步骤二：观察缺省 VLAN

在交换机上查看 VLAN, 如下所示:

```
[SWA]display vlan
The following VLANs exist:
  1(default)

[SWA]display vlan 1
VLAN ID: 1
VLAN Type: static
Route Interface: not configured
Description: VLAN 0001
Tagged Ports: none
Untagged Ports:
  GigabitEthernet1/0/1      GigabitEthernet1/0/2
  GigabitEthernet1/0/3      GigabitEthernet1/0/5
  GigabitEthernet1/0/4      GigabitEthernet1/0/6
  GigabitEthernet1/0/7      GigabitEthernet1/0/8
  GigabitEthernet1/0/9      GigabitEthernet1/0/10
  GigabitEthernet1/0/12     GigabitEthernet1/0/11
  GigabitEthernet1/0/13     GigabitEthernet1/0/14
  GigabitEthernet1/0/15     GigabitEthernet1/0/16
  GigabitEthernet1/0/18     GigabitEthernet1/0/17
  GigabitEthernet1/0/19     GigabitEthernet1/0/20
  GigabitEthernet1/0/21     GigabitEthernet1/0/22
  GigabitEthernet1/0/24     GigabitEthernet1/0/23
  GigabitEthernet1/1/1      GigabitEthernet1/1/2
  GigabitEthernet1/1/3
  GigabitEthernet1/1/4

[SWA]display interface GigabitEthernet 1/0/1
.....
PVID: 1
Mdi type: auto
Port link-type: access
Tagged VLAN ID : none
Untagged VLAN ID : 1
Port priority: 0
.....
```

从以上输出可知, 交换机上的缺省 VLAN 是 VLAN 1, 所有的端口处于 VLAN 1 中; 端口的 PVID 是 1, 且是 Access 链路端口类型。

步骤三：配置 VLAN 并添加端口

分别在 SWA 和 SWB 上创建 VLAN 2，并将 PCA 和 PCC 所连接的端口 GigabitEthernet1/0/1 添加到 VLAN 2 中。

配置 SWA:

```
[SWA]vlan 2
[SWA-vlan2]port GigabitEthernet 1/0/1
```

配置 SWB:

```
[SWB]vlan 2
[SWB-vlan2]port GigabitEthernet 1/0/1
```

在交换机上查看有关 VLAN 2 的信息，如下所示：

```
[SWA]display vlan
The following VLANs exist:
  1(default), 2

[SWA]display vlan 2
VLAN ID: 2
VLAN type: Static
Route interface: Not configured
Description: VLAN 0002
Name: VLAN 0002
Tagged Ports: none
Untagged Ports:
GigabitEthernet1/0/1

[SWB]display vlan
The following VLANs exist:
  1(default), 2

[SWB]display vlan 2
VLAN ID: 2
VLAN type: Static
Route interface: Not configured
Description: VLAN 0002
Name: VLAN 0002
Tagged ports: None
Untagged Ports:
GigabitEthernet1/0/1
```

步骤四：测试 VLAN 间的隔离

我们在 PC 上配置 IP 地址，通过 Ping 命令来测试处于不同 VLAN 间的 PC 能否互通。

表3-2 IP 地址列表

设备名称	IP 地址	网关
PCA	172.16.0.1/24	--
PCB	172.16.0.2/24	--
PCC	172.16.0.3/24	--
PCD	172.16.0.4/24	--

按表 3-2 所示在 PC 上配置 IP 地址。

配置完成后，在 PCA 上用 Ping 命令来测试到其它 PC 的互通性。其结果应该是 PCA 与 PCB 不能够互通，PCC 和 PCD 不能够互通。证明不同 VLAN 之间不能互通，连接在同一交换机上的 PC 被隔离了。

实验任务二：配置 Trunk 链路端口

本实验任务是在交换机间配置 Trunk 链路端口，来使同一 VLAN 中的 PC 能够跨交换机访问。通过本实验，学员应该能够掌握 Trunk 链路端口的配置及作用。

步骤一：跨交换机 VLAN 互通测试

在上个实验中，PCA 和 PCC 都属于 VLAN 2。在 PCA 上用 Ping 命令来测试与 PCC 能否互通。其结果应该是不能，如下所示：

```
C:\Documents and Settings\Administrator>ping 172.16.0.3

Pinging 172.16.0.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.16.0.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

PCA 与 PCC 之间不能互通。因为交换机之间的端口 GigabitEthernet 1/0/24 是 Access 链路端口，且属于 VLAN 1，不允许 VLAN 2 的数据帧通过。

要想让 VLAN 2 数据帧通过端口 GigabitEthernet 1/0/24，需要设置端口为 Trunk 链路端口。

步骤二：配置 Trunk 链路端口

在 SWA 和 SWB 上配置端口 GigabitEthernet 1/0/24 为 Trunk 链路端口。

配置 SWA:

```
[SWA]interface GigabitEthernet 1/0/24
[SWA-GigabitEthernet1/0/24]port link-type trunk
[SWA-GigabitEthernet1/0/24]port trunk permit vlan all
```

配置 SWB:

```
[SWB]interface GigabitEthernet 1/0/24
[SWB-GigabitEthernet1/0/24]port link-type trunk
[SWB-GigabitEthernet1/0/24]port trunk permit vlan all
```

配置完成后，查看 VLAN 2 信息：

```
<SWA>display vlan 2
VLAN ID: 2
VLAN type: Static
Route interface: Not configured
Description: VLAN 0002
Name: VLAN 0002
Tagged Ports:
    GigabitEthernet1/0/24
Untagged Ports:
    GigabitEthernet1/0/1
```

可以看到，VLAN 2 中包含了端口 GigabitEthernet 1/0/24，且数据帧是以带有标签(Tagged)的形式通过端口的。

再查看端口 GigabitEthernet 1/0/24 信息：

```
<SWA>display interface GigabitEthernet 1/0/24
.....
PVID: 1
Mdi type: auto
Port link-type: trunk
  VLAN passing : 1(default vlan), 2
  VLAN permitted: 1(default vlan), 2-4094
  Trunk port encapsulation: IEEE 802.1q
.....
```

从以上信息可知，端口的 PVID 值是 1，端口类型是 Trunk，允许所有的 VLAN（1—4094）通过，但实际上是 VLAN 1 和 VLAN 2 能够通过此端口（因为交换机上仅有 VLAN 1 和 VLAN 2）。SWB 上 VLAN 和端口 GigabitEthernet 1/0/24 的信息与此类似，不再赘述。

步骤三：跨交换机 VLAN 互通测试

在 PCA 上用 Ping 命令来测试与 PCC 能否互通。其结果应该是能够互通，如下所示：

```
C:\Documents and Settings\Administrator>ping 172.16.0.3

Pinging 172.16.0.3 with 32 bytes of data:

Reply from 172.16.0.3: bytes=32 time<1ms TTL=128
Reply from 172.16.0.3: bytes=32 time<1ms TTL=128
Reply from 172.16.0.3: bytes=32 time<1ms TTL=128
Reply from 172.16.0.3: bytes=32 time<1ms TTL=128

Ping statistics for 172.16.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

说明跨交换机 VLAN 间能够互通。

3.5 实验中的命令列表

表3-3 VLAN 实验命令列表

命令	描述
display vlan	显示交换机上的VLAN信息
display interface [<i>interface-type</i> [<i>interface-number</i>]]	显示指定接口当前的运行状态和相关信息
display vlan <i>vlan-id</i>	显示交换机上的指定VLAN信息
vlan <i>vlan-id</i>	创建VLAN并进入VLAN视图
port <i>interface-list</i>	向VLAN中添加一个或一组Access端口
port link-type { access hybrid trunk }	设置端口的链路类型
port trunk permit vlan { <i>vlan-id-list</i> all }	允许指定的VLAN通过当前Trunk端口

3.6 思考题

1. 在实验任务二中,还可以使用哪种链路端口类型而使交换机端口 G1/0/24 允许 VLAN 2 的数据帧通过?

答: 可以使用 Hybrid 链路端口。

2. 在实验任务二中, 如果配置 SWA 的端口 G1/0/24 为 Trunk 类型, PVID 为 1, SWB 的端口 G1/0/24 为 Access 类型, PVID 也为 1, 则 PCB 与 PCD 能够互通吗?

答: 可以。链路端口类型只定义了数据帧进入和离开端口时的行为。交换机并不知道也不关心对端端口的链路类型。

实验4 配置生成树

4.1 实验内容与目标

完成本实验，您应该能够：

- 了解 STP 的基本工作原理
- 掌握 STP 的基本配置方法

4.2 实验组网图

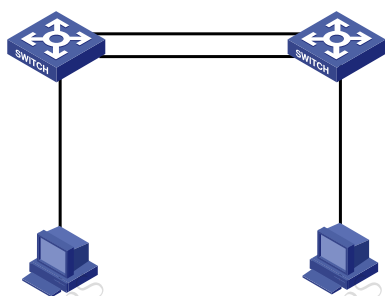


图4-1 STP 实验组网图

4.3 实验设备与版本

本实验所需之主要设备器材如表 4-1 所示。

表4-1 设备列表

名称和型号	版本	数量	描述
S5820V2	CMW710-R2311P03	2	
PC	Windows XP SP2	2	
第5类UTP以太网连接线	--	4	

4.4 实验过程

实验任务一：STP 基本配置

本实验通过在交换机上配置 STP 根桥及边缘端口，来使读者掌握 STP 根桥及边缘端口的配置命令和查看方法。然后通过观察端口状态迁移，来加深了解 RSTP/MSTP 协议的快速收敛特性。

步骤一：建立物理连接

按照图 4-1 进行连接，并检查设备的软件版本及配置信息，确保各设备软件版本符合要求，所有配置为初始状态。如果配置不符合要求，请读者在用户模式下擦除设备中的配置文件，然后重启设备以使系统采用缺省的配置参数进行初始化。

以上步骤可能会用到以下命令：

```
<SWA> display version
<SWA> reset saved-configuration
<SWA> reboot
```

注意：

如果建立物理连接后，交换机面板上的端口 LED 不停闪烁，且 Console 口对配置命令无响应，则很可能是广播风暴导致。如有此情况，请断开交换机间的线缆，配置完成后再连接。

步骤二：配置 STP

本实验任务是配置 STP 根桥及边缘端口。在系统视图下启用 STP，并设置 SWA 的优先级为 0，以使 SWA 为根桥；并且配置连接 PC 的端口为边缘端口。

配置 SWA：

```
[SWA]stp global enable
[SWA]stp priority 0
[SWA]interface GigabitEthernet 1/0/1
[SWA-GigabitEthernet1/0/1] stp edged-port
```

配置 SWB：

```
[SWB]stp global enable
[SWB]stp priority 4096
[SWB]interface GigabitEthernet 1/0/1
[SWB-GigabitEthernet1/0/1] stp edged-port
```

步骤三：查看 STP 信息

分别在 SWA 和 SWB 上查看 STP 信息。正确信息应如下所示：

```
[SWA]display stp
-----[CIST Global Info][Mode MSTP]-----
CIST Bridge      :0.000f-e24a-df50
Bridge Times     :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC   :0.000f-e24a-df50 / 0
CIST RegRoot/IRPC :0.000f-e24a-df50 / 0
.....
```

```
[SWA]display stp brief
MSTID    Port                               Role STP State   Protection
0        GigabitEthernet1/0/1             DESI FORWARDING NONE
0        GigabitEthernet1/0/23          DESI FORWARDING NONE
0        GigabitEthernet1/0/24          DESI FORWARDING NONE
```

以上信息表明，SWA 是根桥，其上所有端口是指定端口（DESI），处于转发状态。

```
[SWB]display stp
-----[CIST Global Info][Mode MSTP]-----
CIST Bridge      :4096.000f-e23e-f9b0
Bridge Times     :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC   :0.000f-e24a-df50 / 200
CIST RegRoot/IRPC :4096.000f-e23e-f9b0 / 0
.....
[SWB]display stp brief
MSTID    Port                               Role STP State   Protection
0        GigabitEthernet1/0/1             DESI FORWARDING NONE
```

0	GigabitEthernet1/0/23	ROOT	FORWARDING	NONE
0	GigabitEthernet1/0/24	ALTE	DISCARDING	NONE

以上信息表明，SWB 是非根桥，端口 G1/0/23 是根端口，处于转发状态，负责在交换机之间转发数据；端口 G1/0/24 是备份根端口，处于阻塞状态；连接 PC 的端口 G1/0/1 是指定端口，处于转发状态。

步骤四：STP 冗余特性验证

STP 不但能够阻断冗余链路，并且能够在活动链路断开时，通过激活被阻断的冗余链路而恢复网络的连通。

表4-2 IP 地址列表

设备名称	IP 地址	网关
PCA	172.16.0.1/24	--
PCB	172.16.0.2/24	--

按表 4-2 所示在 PC 上配置 IP 地址。

配置完成后，在 PCA 上执行命令 “Ping 172.16.0.2 -t”，以使 PCA 向 PCB 不间断发送 ICMP 报文。如下所示：

```
C:\Documents and Settings\Administrator>ping 172.16.0.2 -t

Pinging 172.16.0.2 with 32 bytes of data:

Reply from 172.16.0.2: bytes=32 time<1ms TTL=128
Reply from 172.16.0.2: bytes=32 time<1ms TTL=128
Reply from 172.16.0.2: bytes=32 time<1ms TTL=128
.....
```

在 SWB 上查看 STP 端口状态，确定交换机间哪一个端口（本例中是 G1/0/23）处于转发状态。将交换机之间处于 STP 转发状态的端口上电缆断开，观察 PCA 上发送的 ICMP 报文有无丢失。正常情况下，应该没有报文丢失或仅有一个报文丢失。

再次在 SWB 上查看 STP 端口状态，看端口状态是否有变化。如下所示：

```
[SWB]display stp brief
MSTID      Port                      Role STP State      Protection
0          GigabitEthernet1/0/1      DESI FORWARDING  NONE
0          GigabitEthernet1/0/24      ROOT FORWARDING  NONE
```

可以看到，原来处于阻塞状态的端口 G1/0/24 迁移到了转发状态。

无报文丢失说明目前 STP 的收敛速度很快。其实，这就是 RSTP/MSTP 相对于 STP 的改进之一。缺省情况下，交换机运行 MSTP，SWB 上的两个端口中有一个是根端口，另外一个为备份根端口。当原根端口断开时，备份根端口快速切换到转发状态。

注意：

如果在 PCA 上 Ping 172.16.0.2 -t 时出现 “Request timed out.”，表明 PCB 无回应，需要检查 PCB 是否开启了防火墙或交换机配置是否有问题。

步骤五：端口状态迁移查看

在交换机 SWA 上断开端口 G1/0/1 的电缆，再重新连接，并且在 SWA 上查看交换机输出信息。如下：

```
[SWA]
```

```

.....
GigabitEthernet1/0/1: link status is UP
%Apr 26 14:04:53:880 2000 SWA MSTP/2/PFWD:Instance 0's GigabitEthernet1/0/1 has
been set to forwarding state!

```

可以看到，端口在连接电缆后马上成为转发状态。这是因为端口被配置成边缘端口，无须延迟而进入转发状态。这也是 RSTP/MSTP 相对于 STP 的改进之一。

在前面实验中，端口状态迁移速度很快。为了清晰观察端口状态，我们在连接 PC 的端口 G1/0/1 上取消边缘端口配置，如下：

配置 SWA:

```

[SWA]interface GigabitEthernet 1/0/1
[SWA-GigabitEthernet1/0/1] undo stp edged-port

```

配置完成后，断开端口 G1/0/1 的电缆，再重新连接，并且在 SWA 上查看端口 G1/0/1 的状态。注意每隔几秒钟执行命令查看一次，以能准确看到端口状态的迁移过程。例如：

```

[SWA]display stp brief
MSTID      Port                      Role STP State      Protection
0          GigabitEthernet1/0/1      DESI DISCARDING   NONE
0          GigabitEthernet1/0/24  DESI FORWARDING   NONE
[SWA]display stp brief
MSTID      Port                      Role STP State      Protection
0          GigabitEthernet1/0/1      DESI LEARNING     NONE
0          GigabitEthernet1/0/24  DESI FORWARDING   NONE
[SWA]display stp brief
MSTID      Port                      Role STP State      Protection
0          GigabitEthernet1/0/1      DESI LEARNING     NONE
0          GigabitEthernet1/0/24  DESI FORWARDING   NONE
.....
#Apr 26 14:02:24:934 2000 SWA MSTP/1/PFWD:hwPortMstiStateForwarding: Instance 0's
Port 0.9371648 has been set to forwarding state!
%Apr 26 14:02:24:940 2000 SWA MSTP/2/PFWD:Instance 0's GigabitEthernet1/0/1 has
been set to forwarding state!
MSTID      Port                      Role STP State      Protection
0          GigabitEthernet1/0/1      DESI FORWARDING   NONE
0          GigabitEthernet1/0/24  DESI FORWARDING   NONE

```

可知，端口从 Discarding 状态先迁移到 Learning 状态，最后到 Forwarding 状态。从以上实验可知，取消边缘端口配置后，STP 收敛速度变慢了。

4.5 实验中的命令列表

表4-3 实验命令列表

命令	描述
stp global enable	开启或关闭全局或端口的STP特性
stp mode { mstp pvst rstp stp }	设置MSTP的工作模式
stp [instance instance-list vlan vlan-id-list] priority priority	配置设备的优先级
stp edged-port	将当前的以太网端口配置为边缘端口
display stp [instance instance-list vlan vlan-id-list] [interface interface-list slot slot-number] [brief]	显示生成树的状态信息与统计信息

4.6 思考题

1. 实验中，交换机 SWB 选择端口 G1/0/23 作为根端口，转发数据。能否使交换机选择另外一个端口 G1/0/24 作为根端口？

答：可以。缺省情况下，端口的 Cost 值是 200（100M 端口的缺省值），如果调整端口 G1/0/24 的 Cost 值为 100，SWB 从端口 G1/0/24 到达 SWA 的开销小于从端口 G1/0/23 到达 SWA 的开销，则 STP 会选择端口 G1/0/24 作为根端口。

实验5 交换机端口安全技术

5.1 实验内容与目标

完成本实验，您应该能够：

- 掌握 802.1X 的基本配置
- 掌握端口隔离基本配置

5.2 实验组网图

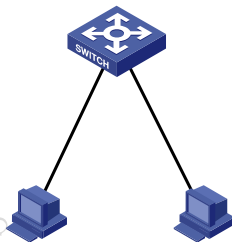


图5-1 以太网端口安全实验图

5.3 实验设备与版本

本实验所需之主要设备器材如表 5-1 所示。

表5-1 设备列表

名称和型号	版本	数量	描述
S5820V2	CMW710-R2311P03	1	
PC	Windows XP SP2	2	
第5类UTP以太网连接线	--	2	

5.4 实验过程

实验任务一：配置 802.1X

本实验通过在交换机上配置 802.1X 协议，使接入交换机的 PC 经过认证后才能访问网络资源。通过本实验，学员能够掌握 802.1X 认证的基本原理和 802.1X 本地认证的基本配置。

步骤一：建立物理连接

按照图 5-1 进行连接，并检查设备的软件版本及配置信息，确保各设备软件版本符合要求，所有配置为初始状态。如果配置不符合要求，请读者在用户模式下擦除设备中的配置文件，然后重启设备以使系统采用缺省的配置参数进行初始化。

以上步骤可能会用到以下命令：

```
<SWA> display version
<SWA> reset saved-configuration
<SWA> reboot
```

步骤二：配置 802.1X 协议

在交换机上启用 802.1X 协议并创建本地用户。

配置 SWA：

```
[SWA]dot1x
[SWA-GigabitEthernet1/0/1] dot1x
[SWA]local-user abcde class network
[SWA-luser-network-abcde] service-type lan-access
[SWA-luser-h3c]password simple 12345
```

步骤三：802.1X 验证

表5-2 IP 地址列表

设备名称	IP 地址	网关
PCA	172.16.0.1/24	--
PCB	172.16.0.2/24	--

在 PCA 和 PCB 上配置 IP 地址，如上表所示。

配置完成后，在 PCA 上用 ping 命令来测试到 PCB 的互通性。因为交换机上启用了 802.1X 认证，所以结果应该是 PCA 与 PCB 不能够互通。如下所示：

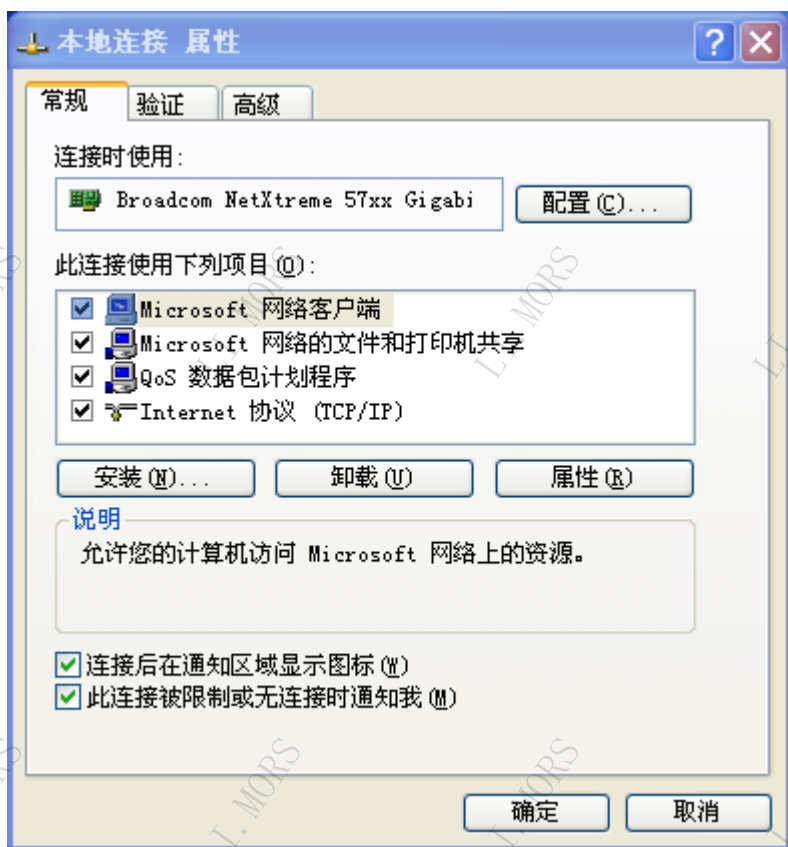
```
C:\Documents and Settings\Administrator>ping 172.16.0.2

Pinging 172.16.0.2 with 32 bytes of data:

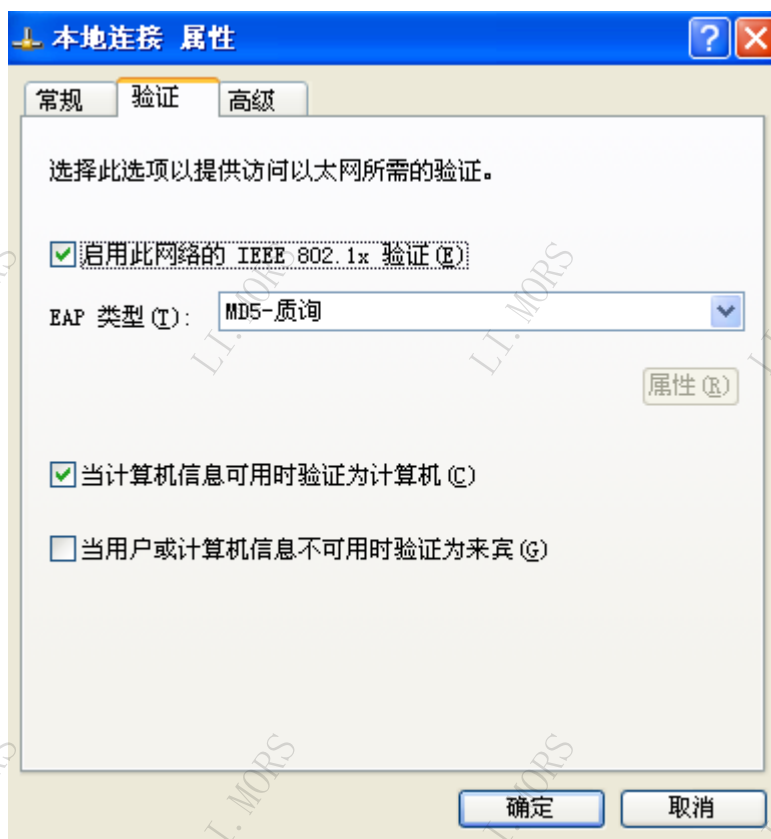
Request timed out.
Request timed out.
Request timed out.
.....
```

PC 可以使用 802.1X 客户端软件或 Windows 系统自带客户端接入交换机。本实验以 Windows 系统自带客户端为例说明如何进行设置。

在 Windows 操作系统的【控制面板】中选择【网络和 Internet 连接】，选取【网络连接】中的【本地连接】，点击【属性】，如下所示：

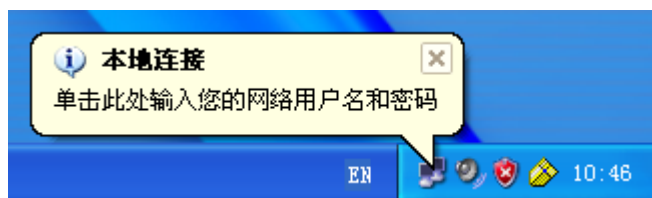


再选取【验证】，并勾选【启用此网络的 IEEE802.1x 验证】，如下所示：



然后单击【确定】，保存退出。

等待几秒钟后，屏幕右下角会自动弹出要求认证的相应提示，如下所示：



按提示要求点击，系统弹出对话框，要求输入用户名和密码，如下所示：



在对话框中输入用户名 `abcde` 和密码 `12345` 后，系统提示通过验证。

在 PCA 与 PCB 都通过验证后，在 PCA 上用 `ping` 命令来测试到 PCB 的互通性。结果应该是 PCA 与 PCB 能够互通。如下所示：

```
C:\Documents and Settings\Administrator>ping 172.16.0.2

Pinging 172.16.0.2 with 32 bytes of data:

Reply from 172.16.0.2: bytes=32 time<1ms TTL=128
Reply from 172.16.0.2: bytes=32 time<1ms TTL=128
Reply from 172.16.0.2: bytes=32 time<1ms TTL=128
.....
```

注意：

如果 Windows 系统长时间没有自动弹出要求认证提示，或认证失败需要重新认证，可以将电缆断开再连接，以重新触发 802.1X 认证过程。

实验任务二：配置端口隔离

本实验通过在交换机上配置端口隔离，使处于隔离组内的两台 PC 不能互相访问，但 PC 能够访问上行端口的 PC。通过本实验，使学员能够掌握端口隔离的基本原理和配置。

步骤一：建立物理连接

按照图 5-1 进行连接，并检查设备的软件版本及配置信息，确保各设备软件版本符合要求，所有配置为初始状态。如果配置不符合要求，请读者在用户模式下擦除设备中的配置文件，然后重启设备以使系统采用缺省的配置参数进行初始化。

以上步骤可能会用到以下命令：

```
<SWA> display version
<SWA> reset saved-configuration
```

```
<SWA> reboot
```

步骤二：配置端口隔离

在交换机上启用端口隔离，设置端口 GigabitEthernet1/0/1、GigabitEthernet1/0/2 为隔离组的普通端口，端口 GigabitEthernet1/0/24 为隔离组的上行端口。

配置 SWA:

```
[SWA]port-isolate group 1
[SWA-GigabitEthernet1/0/1] port-isolate enable group 1
[SWA] interface GigabitEthernet 1/0/2
[SWA-GigabitEthernet1/0/2] port-isolate enable group 1
```

配置完成后，用以下命令显示隔离组的信息：

```
<SWA>display port-isolate group 1
Port isolation group information:
Group ID: 1
Group members:
    GigabitGigabitEthernet1/0/47    GigabitGigabitEthernet1/0/48
```

步骤三：端口隔离验证

表5-3 IP 地址列表

设备名称	IP 地址	网关
PCA	172.16.0.1/24	--
PCB	172.16.0.2/24	--

在 PCA 和 PCB 上配置 IP 地址，如上表所示。

未在接口上配置隔离端口，用 ping 命令测试，其结果应该是能够互通。如下所示：

```
C:\Documents and Settings\Administrator>ping 172.16.0.2

Pinging 172.16.0.2 with 32 bytes of data:

Reply from 172.16.0.2: bytes=32 time<1ms TTL=128
Reply from 172.16.0.2: bytes=32 time<1ms TTL=128
Reply from 172.16.0.2: bytes=32 time<1ms TTL=128
```

配置完成后，在 PCA 上用 ping 命令来测试到 PCB 的互通性。其结果应该是 PCA 与 PCB 不能够互通。如下所示：

```
C:\Documents and Settings\Administrator>ping 172.16.0.2

Pinging 172.16.0.2 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
.....
```

5.5 实验中的命令列表

表5-4 实验命令列表

命令	描述
dot1x	开启全局/端口的802.1X特性
port-isolate group	创建隔离组
port-isolate enable group-number	将指定端口加入到隔离组中作为隔离组的普通端口
display port-isolate group	显示端口隔离组信息

5.6 思考题

1. 在实验任务一中，使用交换机内置本地服务器对用户进行了本地认证。可不可以不在交换机上配置用户名、密码等信息，而对用户进行认证？

答：可以，但需要在网络中增加一台远程认证服务器。通过交换机与远程认证服务器协同工作，由交换机把用户名、密码等信息发送到远程服务器而完成认证过程。

实验6 配置链路聚合

6.1 实验内容与目标

完成本实验，您应该能够：

- 了解以太网交换机链路聚合的基本工作原理
- 掌握以太网交换机静态链路聚合的基本配置方法

6.2 实验组网图

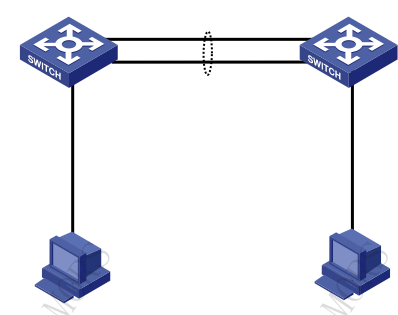


图6-1 链路聚合实验组网图

6.3 实验设备与版本

本实验所需之主要设备器材如表 6-1 所示。

表6-1 设备列表

名称和型号	版本	数量	描述
S5820V2	CMW710-R2311P03	2	
PC	Windows XP SP2	2	
第5类UTP以太网连接线	--	4	

6.4 实验过程

实验任务一：交换机静态链路聚合配置

本实验通过在交换机上配置静态链路聚合，使读者掌握静态链路聚合的配置命令和查看方法。然后通过断开聚合组中的某条链路并观察网络连接是否中断，来加深了解链路聚合所实现的可靠性。

步骤一：建立物理连接

按照图 6-1 进行连接，并检查设备的软件版本及配置信息，确保各设备软件版本符合要求，所有配置为初始状态。如果配置不符合要求，请读者在用户模式下擦除设备中的配置文件，然后重启设备以使系统采用缺省的配置参数进行初始化。

以上步骤可能会用到以下命令：

```
<SWA> display version
<SWA> reset saved-configuration
<SWA> reboot
```

注意：

如果建立物理连接后，交换机面板上的端口 LED 不停闪烁，且 Console 口对配置命令无响应，则很可能是广播风暴导致。如有此情况，请断开交换机间的线缆，配置完成后再连接。

步骤二：配置静态聚合

链路聚合可以分为静态聚合和动态聚合，本实验任务是验证静态聚合。首先在系统视图下创建聚合端口，然后把物理端口加入到聚合组中。

配置 SWA:

```
[SWA] interface bridge-aggregation 1
[SWA] interface GigabitEthernet 1/0/23
[SWA-GigabitEthernet1/0/23] port link-aggregation group 1
[SWA] interface GigabitEthernet 1/0/24
[SWA-GigabitEthernet1/0/24] port link-aggregation group 1
```

配置 SWB:

```
[SWB] interface bridge-aggregation 1
[SWB] interface GigabitEthernet 1/0/23
[SWB-GigabitEthernet1/0/23] port link-aggregation group 1
[SWB] interface GigabitEthernet 1/0/24
[SWB-GigabitEthernet1/0/24] port link-aggregation group 1
```

步骤三：查看聚合组信息

分别在 SWA 和 SWB 上查看所配置的聚合组信息。正确信息应如下所示：

```
[SWA]display link-aggregation summary

Aggregation Interface Type:
BAGG -- Bridge-Aggregation, RAGG -- Route-Aggregation
Aggregation Mode: S -- Static, D -- Dynamic
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Actor System ID: 0x8000, 000f-e23e-f9b0
```

AGG Interface	AGG Mode	Partner ID	Select Ports	Unselect Ports	Share Type
BAGG1	S	none	2	0	Shar

```
[SWB]display link-aggregation summary
```

```
Aggregation Interface Type:
BAGG -- Bridge-Aggregation, RAGG -- Route-Aggregation
Aggregation Mode: S -- Static, D -- Dynamic
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Actor System ID: 0x8000, 000f-e24a-df50
```

AGG Interface	AGG Mode	Partner ID	Select Ports	Unselect Ports	Share Type
BAGG1	S	none	2	0	Shar

以上信息表明，交换机上有一个链路聚合端口，其 ID 是 1，组中包含了 2 个 **Selected** 状态端口，并工作在负载分担模式下。

步骤四：链路聚合组验证

表6-2 IP 地址列表

设备名称	IP 地址	网关
PCA	172.16.0.1/24	--
PCB	172.16.0.2/24	--

按表 6-2 所示在 PC 上配置 IP 地址。

配置完成后，在 PCA 上执行 **ping** 命令，以使 PCA 向 PCB 不间断发送 ICMP 报文。如下所示：

```
C:\Documents and Settings\Administrator>ping 172.16.0.2 -t

Pinging 172.16.0.2 with 32 bytes of data:

Reply from 172.16.0.2: bytes=32 time<1ms TTL=128
Reply from 172.16.0.2: bytes=32 time<1ms TTL=128
Reply from 172.16.0.2: bytes=32 time<1ms TTL=128
.....
```

注意观察交换机面板上的端口 LED 显示灯，闪烁表明有数据流通过。将聚合组中 LED 显示灯闪烁的端口上电缆断开，观察 PCA 上发送的 ICMP 报文有无丢失。

正常情况下，应该没有报文丢失。

无报文丢失说明聚合组中的两个端口之间是互相备份的。当一个端口不能转发数据流时，系统将数据流从另外一个端口发送出去。

注意：

如果在 PCA 上 Ping 172.16.0.2 -t 时出现 “Request timed out.”，表明 PCB 无回应，需要检查 PCB 是否开启了防火墙或交换机配置是否有问题。

6.5 实验中的命令列表

表6-3 实验命令列表

命令	描述
interface bridge-aggregation <i>interface-number</i>	创建聚合端口
port link-aggregation group <i>number</i>	将以太网端口加入聚合组中
display link-aggregation summary	查看链路聚合的概要信息

6.6 思考题

1. 实验中，如果交换机间有物理环路产生广播风暴，除了断开交换机间链路外，还有什么处理办法？

答：可以在交换机上用命令 **stp enable** 来在交换机上启用生成树协议，用生成树协议来阻断物理环路。

实验7 ARP

7.1 实验内容与目标

完成本实验，您应该能够：

- 掌握 ARP 的工作机制
- 掌握 ARP 代理的工作原理及配置方法

7.2 实验组网图

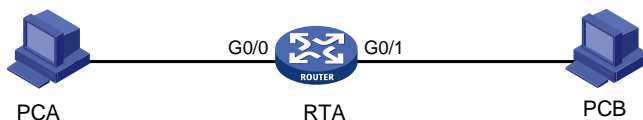


图7-1 ARP 实验组网图

7.3 实验设备与版本

本实验所需之主要设备器材如表 7-1 所示。

表7-1 设备列表

名称和型号	版本	数量	描述
MSR36-20	Version 7.1	1	
PC	Windows 系统	2	
第5类UTP以太网连接线	--	2	连接主机与路由器

7.4 实验过程

实验任务一：ARP 表项观察

本实验通过观察设备上的 ARP 表项建立过程，使学员能够了解 ARP 协议的基本工作原理。

步骤一：建立物理连接

按照图 7-1 进行连接，并检查设备的软件版本及配置信息，确保各设备软件版本符合要求，所有配置为初始状态。如果配置不符合要求，请读者在用户模式下擦除设备中的配置文件，然后重启设备以使系统采用缺省的配置参数进行初始化。

以上步骤可能会用到以下命令：

```

<RTA> display version
<RTA> reset saved-configuration
<RTA> reboot

```

步骤二：配置 PC 及路由器的 IP 地址

表7-2 IP 地址列表

设备名称	接口	IP 地址
PCA	--	172.16.0.1/24
PCB	--	172.16.1.1/24
RTA	G0/0	172.16.0.254/24
RTA	G0/1	172.16.1.254/24

根据上表所示在 PC 上配置 IP 地址和网关。配置完成后，在 PC 的“命令提示符”窗口下，键入命令 **ipconfig** 来验证 PC 的 IP 地址是否配置正确。PCA 的结果应该如下所示：

```

C:\Documets and Settings>ipconfig
Windows IP Configuration
Ethernet adapter 本地连接:
    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 172.16.0.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

```

PCB 的结果应该如下所示：

```

C:\Documets and Settings>ipconfig
Windows IP Configuration
Ethernet adapter 本地连接:
    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 172.16.1.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

```

然后在 RTA 的接口上配置 IP 地址及掩码，如下：

```

[RTA]interface GigabitEthernet0/0
[RTA-GigabitEthernet0/0]ip address 172.16.0.254 24
[RTA]interface GigabitEthernet0/1
[RTA-GigabitEthernet0/1]ip address 172.16.1.254 24

```

步骤三：查看 ARP 信息

首先，我们在 RTA 及 PCA、PCB 上用命令来查看它们的 IP 地址和 MAC 地址。

RTA 的接口 MAC 地址与 IP 地址如下：

```

[RTA]display interface GigabitEthernet 0/0
GigabitEthernet0/0
Current state: UP
Line protocol state: UP
Description: GigabitEthernet0/0 Interface
Bandwidth: 100000kbps
Maximum Transmit Unit: 1500
Internet Address is 172.16.0.254/24 Primary
IP Packet Frame Type:PKTFMT_ETHNT_2, Hardware Address: 70ba-ef80-0958
.....
.....

```

```
[RTA]display interface GigabitEthernet 0/1
GigabitEthernet0/1
Current state: UP
Line protocol state: UP
Description: GigabitEthernet0/1 Interface
Bandwidth: 1000000kbps
Maximum Transmit Unit: 1500
Internet Address is 172.16.1.254/24 Primary
IP Packet Frame Type:PKTFMT_ETHNT_2, Hardware Address: 70ba-ef80-0959
.....
.....
```

PCA 的接口 MAC 地址与 IP 地址如下:

```
C:\Documents and Settings\Administrator>ipconfig/all
```

```
.....
Ethernet adapter 本地连接:
```

```
Connection-specific DNS Suffix . : h3c.com
Description . . . . . : Broadcom NetXtreme 57xx Gigabit Cont
roller
Physical Address. . . . . : A4-5D-36-59-26-4F
Dhcp Enabled. . . . . : No
IP Address. . . . . : 172.16.0.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
```

PCB 的接口 MAC 地址与 IP 地址如下:

```
C:\Documents and Settings\Administrator>ipconfig/all
```

```
.....
Ethernet adapter 本地连接:
```

```
Connection-specific DNS Suffix . : h3c.com
Description . . . . . : Broadcom NetXtreme 57xx Gigabit Cont
roller
Physical Address. . . . . : 44-37-E6-AB-7D-F0
Dhcp Enabled. . . . . : No
IP Address. . . . . : 172.16.1.1
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
```

根据以上信息, 我们做一张表, 表的内容是 PC 及 RTA 的 IP 地址与 MAC 地址对应关系, 如下所示:

表7-3 IP 地址与 MAC 地址对应关系列表

设备名称	接口	IP 地址	MAC 地址
PCA	--	172.16.0.1/24	A4-5D-36-59-26-4F
PCB	--	172.16.1.1/24	44-37-E6-AB-7D-F0
RTA	G0/0	172.16.0.254/24	70ba-ef80-0958
RTA	G0/1	172.16.1.254/24	70ba-ef80-0959

然后, 分别在 PCA 和 PCB 的“命令提示符”窗口下用 ping 命令来测试 PC 到 RTA 的可达性, 以使 PC 及 RTA 建立 ARP 表项。例如, 在 PCA 的测试如下:

```
C:\Documents and Settings\Administrator>ping 172.16.0.254
```

Pinging 172.16.0.254 with 32 bytes of data:

```
Reply from 172.16.0.254: bytes=32 time<1ms TTL=255
Reply from 172.16.0.254: bytes=32 time<1ms TTL=255
Reply from 172.16.0.254: bytes=32 time<1ms TTL=255
.....
```

在 PCB 的测试如下:

```
C:\Documents and Settings>ping 172.16.1.254
Pinging 172.16.1.254 with 32 bytes of data:
Reply from 172.16.1.254: bytes=32 time<1ms TTL=255
Reply from 172.16.1.254: bytes=32 time<1ms TTL=255
Reply from 172.16.1.254: bytes=32 time<1ms TTL=255
.....
```

测试完成后, 分别在 PCA、PCB 和 RTA 上查看 ARP 表项信息。PCA 的信息如下所示:

```
C:\Documents and Settings\Administrator>arp -a

Interface: 172.16.0.1 --- 0x30002
Internet Address      Physical Address      Type
172.16.0.254          70-ba-ef-80-09-58     dynamic
```

PCB 的正确信息应如下所示:

```
C:\Documents and Settings\Administrator>arp -a

Interface: 172.16.1.1 --- 0x2
Internet Address      Physical Address      Type
172.16.1.254          70-ba-ef-80-09-59     dynamic
```

RTA 的正确信息应如下所示:

```
[RTA]display arp all
Type: S-Static D-Dynamic O-Openflow M-Multiport I-Invalid
IP address  MAC address  VLAN  Interface  Aging Type
172.16.0.1  a45d-3659-264f  N/A   GE0/0      18      D
172.16.1.1  4437-e6ab-7df0  N/A   GE0/1      19      D
```

把我们所做的表 7-3 和 PC 及 RTA 上的 ARP 表项对比一下。可知, PC 及 RTA 都建立了正确的 ARP 表项, 表项中包含了 IP 地址和对应的 MAC 地址。

注意:

学员实验过程中所显示的 MAC 地址与本指导手册中的不同, 是正常现象。

实验任务二: ARP 代理配置

本实验通过在设备上配置 ARP 代理, 使设备能够对不同子网间的 ARP 报文进行转发, 使学员能够了解 ARP 代理的基本工作原理, 掌握 ARP 代理的配置方法。

步骤一: 建立物理连接

按照图 7-1 进行连接, 并检查设备的软件版本及配置信息, 确保各设备软件版本符合要求, 所有配置为初始状态。如果配置不符合要求, 请读者在用户模式下擦除设备中的配置文件, 然后重启设备以使系统采用缺省的配置参数进行初始化。

以上步骤可能会用到以下命令：

```
<RTA> display version
<RTA> reset saved-configuration
<RTA> reboot
```

步骤二：配置 PC 及路由器的 IP 地址

表7-4 IP 地址列表

设备名称	接口	IP 地址
PCA	--	172.16.0.1/16
PCB	--	172.16.1.1/16
RTA	G0/0	172.16.0.254/24
RTA	G0/1	172.16.1.254/24

根据表 7-4 所示在 PC 上配置 IP 地址。配置完成后，在 PC 的“命令提示符”窗口下，键入命令 `ipconfig` 来验证 PC 的 IP 地址是否配置正确。PCA 的结果应该如下所示：

```
C:\Documents and Settings>ipconfig
Windows IP Configuration
Ethernet adapter 本地连接:
    Connection-specific DNS Suffix  . :
    IP Address. . . . . : 172.16.0.1
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway. . . . . :
```

PCB 的结果应该如下所示：

```
C:\Documents and Settings>ipconfig
Windows IP Configuration
Ethernet adapter 本地连接:
    Connection-specific DNS Suffix  . :
    IP Address. . . . . : 172.16.1.1
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway. . . . . :
```

然后在 RTA 的接口上配置 IP 地址及掩码，如下：

```
[RTA]interface GigabitEthernet0/0
[RTA-GigabitEthernet0/0]ip address 172.16.0.254 24
[RTA]interface GigabitEthernet0/1
[RTA-GigabitEthernet0/1]ip address 172.16.1.254 24
```

步骤三：ARP 代理配置

此时，PCA 和 PCB 之间是不可达的。如果在 PCA 上测试到 PCB 之间的可达性，结果应该如下所示：

```
C:\Documents and Settings\Administrator>ping 172.16.1.1

Pinging 172.16.1.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
.....
```

为什么呢？因为尽管 PCA 和 PCB 处于同一个子网内（掩码都是 255.255.0.0），但 RTA 上两个接口的子网是不同的（分别为 172.16.0.0/24 和 172.16.1.0/24），所以它不会在两个不同

子网之间转发 ARP 报文。但如果配置了 ARP 代理，路由器可以像二层交换机一样转发 ARP 报文。

在 RTA 上配置 ARP 代理：

```
[RTA]interface GigabitEthernet0/0
[RTA-GigabitEthernet0/0] proxy-arp enable
[RTA]interface GigabitEthernet0/1
[RTA-GigabitEthernet0/1] proxy-arp enable
```

配置完成后，在 PCA 上用 ping 命令测试到 PCB 的可达性，此时应该是可达，如下：

```
C:\Documents and Settings\Administrator>ping 172.16.1.1

Pinging 172.16.1.1 with 32 bytes of data:

Reply from 172.16.1.1: bytes=32 time<1ms TTL=127
Reply from 172.16.1.1: bytes=32 time=1ms TTL=127
Reply from 172.16.1.1: bytes=32 time<1ms TTL=127
.....
```

步骤四：查看 ARP 信息

在 PCA 上查看 ARP 表项，如下所示：

```
C:\Documents and Settings\Administrator>arp -a

Interface: 172.16.0.1 --- 0x30002
   Internet Address      Physical Address      Type
   172.16.1.1           70-ba-ef-80-09-58   dynamic
```

ARP 表项中 172.16.1.1 对应的 MAC 地址与 RTA 接口 G0/0 的 MAC 地址相同。也就是说，在 PCA 看来，RTA 的接口 G0/0 就是 PCB。实际上，是 RTA 的接口 G0/0 执行了 ARP 代理功能，为 PCA 发出的 ARP 请求提供了代理应答。

同理，PCB 也会认为 RTA 的接口 G0/1 就是 PCA。在 PCB 上查看 ARP 表项，如下所示：

```
C:\Documents and Settings\Administrator>arp -a

Interface: 172.16.1.1 --- 0x2
   Internet Address      Physical Address      Type
   172.16.0.1           70-ba-ef-80-09-59   dynamic
```

在 RTA 上的 ARP 表项如下：

```
[RTA]display arp all
Type: S-Static D-Dynamic O-Openflow M-Multiport I-Invalid
IP address      MAC address      VLAN      Interface      Aging Type
172.16.0.1      a45d-3659-264f   N/A       GE0/0          19 D
172.16.1.1      4437-e6ab-7df0   N/A       GE0/1          19 D
```

7.5 实验中的命令列表

表7-5 实验命令列表

命令	描述
proxy-arp enable	开启端口的ARP代理特性
display arp all	显示ARP表项

7.6 思考题

1. 上述实验中，RTA 的 ARP 表项中的“Aging”含义是什么？

答：表示相关 ARP 表项的超时时间。

实验8 DHCP

8.1 实验内容与目标

完成本实验，您应该能够：

- 了解 DHCP 协议工作原理
- 掌握设备作为 DHCP 服务器的常用配置命令
- 掌握设备作为 DHCP 中继的常用配置

8.2 实验组网图

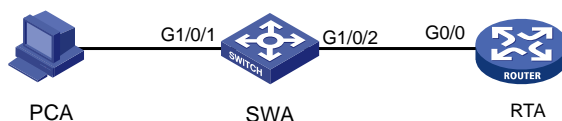


图8-1 DHCP 实验组网图

8.3 实验设备与版本

本实验所需之主要设备器材如表 8-1 所示。

表8-1 设备列表

名称和型号	版本	数量	描述
MSR36-20	Version 7.1	1	
S5820V2	Version 7.1	1	
PC	Windows	1	
第5类UTP以太网连接线	--	2	

8.4 实验过程

实验任务一：PCA 直接通过 RTA 获得 IP 地址

本实验通过配置 DHCP 客户机从处于同一子网中的 DHCP 服务器获得 IP 地址、网关等信息，使学员能够掌握路由器上 DHCP 服务器的配置。

步骤一：建立物理连接

按照图 8-1 进行连接，并检查设备的软件版本及配置信息，确保各设备软件版本符合要求，所有配置为初始状态。如果配置不符合要求，请读者在用户模式下擦除设备中的配置文件，然后重启设备以使系统采用缺省的配置参数进行初始化。

以上步骤可能会用到以下命令：

```
<H3C> display version
<H3C> reset saved-configuration
<H3C> reboot
```

步骤二：在路由器接口配置 IP 地址

表8-2 IP 地址列表

设备名称	接口	IP 地址	网关
RTA	G0/0	172.16.0.1/24	--

按表 8-2 所示在路由器接口上配置 IP 地址。

配置 RTA:

```
[RTA-GigabitEthernet0/0]ip address 172.16.0.1 24
```

步骤三：配置 RTA 作为 DHCP 服务器

配置 RTA:

```
[RTA]dhcp enable
[RTA]dhcp server forbidden-ip 172.16.0.1
[RTA]dhcp server ip-pool pool1
[RTA-dhcp-pool-pool1]network 172.16.0.0 mask 255.255.255.0
[RTA-dhcp-pool-pool1]gateway-list 172.16.0.1
```

配置完成后，可以用以下命令来查看 RTA 上 DHCP 地址池相关配置：

```
<RTA>display dhcp server pool
Pool name: pool1
Network: 172.16.0.0 mask 255.255.255.0
expired 1 0 0 0
gateway-list 172.16.0.1
#
```

步骤四：PCA 通过 DHCP 服务器获得 IP 地址

在 Windows 操作系统的“控制面板”中选择“网络和 Internet 连接”，选取“网络连接”中的“本地连接”，点击【属性】，在弹出的窗口中选择“Internet 协议（TCP/IP）”，点击【属性】，出现界面如下：

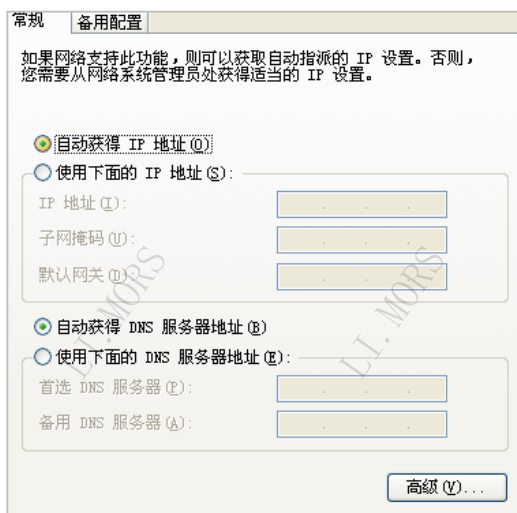


图8-2 Internet 协议（TCP/IP）属性

如图 8-2 所示，选中【自动获得 IP 地址】和【自动获得 DNS 服务器地址】并确定，以确保 PCA 配置为 DHCP 客户端。

在 PCA 的“命令提示符”窗口下，键入命令 `ipconfig` 来验证 PCA 能否获得 IP 地址和网关等信息。正确的结果应该如下所示：

```
C:\Documents and Settings>ipconfig
Windows IP Configuration
Ethernet adapter 本地连接:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 172.16.0.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 172.16.0.1
```

如果无法获得 IP，请检查线缆连接是否正确，然后在“命令提示符”窗口下用 `ipconfig /renew` 命令来使 PCA 重新发起 DHCP 请求。

步骤五：查看 DHCP 服务器相关信息

在 RTA 上用命令 `display dhcp server statistics` 查看 DHCP 服务器的统计信息：

```
<RTA>display dhcp server statistics
Pool number: 1
Pool utilization: 0.39%
Bindings:
  Automatic: 1
  Manual: 0
  Expired: 0
  Conflict: 0
Messages received: 2
  DHCPDISCOVER: 1
  DHCPREQUEST: 1
  DHCPDECLINE: 0
  DHCPRELEASE: 0
  DHCPINFORM: 0
  BOOTPREQUEST: 0
Messages sent: 2
  DHCPOFFER: 1
  DHCPACK: 1
  DHCPNAK: 0
```

```
BOOTPREPLY: 0
Bad Messages: 0
```

从以上输出可以得知，目前路由器上有一个地址池，有一个 IP 被自动分配给了客户端。

在 RTA 上用 `display dhcp server ip-in-use` 来查看 DHCP 服务器已分配的 IP 地址：

```
<RTA>display dhcp server ip-in-use
IP address      Client identifier/   Lease expiration      Type
                Hardware address
172.16.0.2      0144-37e6-ab7d-f0    Dec 30 14:40:31 2014  Auto(C)
```

以上信息表明 172.16.0.2 被服务器分配给了 PCA。

用 `display dhcp server free-ip` 来查看 DHCP 服务器可供分配的 IP 地址资源：

```
[RTA]display dhcp server free-ip
Pool name: pool1
Network: 172.16.0.0 mask 255.255.255.0
IP ranges from 172.16.0.3 to 172.16.0.255
```

可知，IP 地址 172.16.0.2、172.16.0.1、172.16.0.0 不是可分配的 IP 地址资源，因为 172.16.0.1 被禁止分配，172.16.0.2 已被分配给了 PCA，172.16.0.0 是网络地址。

实验任务二：PCA 通过 DHCP 中继方式获得 IP 地址

本实验通过配置 DHCP 客户机从处于不同子网的 DHCP 服务器获得 IP 地址、网关等信息，使学员能够掌握 DHCP 中继的配置。

步骤一：建立物理连接

按照图 8-1 进行连接，并检查设备的软件版本及配置信息，确保设备软件版本符合要求，所有配置为初始状态。如果配置不符合要求，请读者在用户模式下擦除设备中的配置文件，然后重启设备以使系统采用缺省的配置参数进行初始化。

以上步骤可能会用到以下命令：

```
<H3C> display version
<H3C> reset saved-configuration
<H3C> reboot
```

步骤二：在设备上配置 IP 地址及路由

表8-3 设备 IP 地址列表

设备名称	物理接口	IP 地址	VLAN 虚接口
SWA	G1/0/1	172.16.1.1/24	Vlan-interface1
	G1/0/2	172.16.0.1/24	Vlan-interface2
RTA	G0/0	172.16.0.2/24	--

按表 8-3 所示在交换机及路由器上配置 IP 地址。

在 SWA 上配置 VLAN 虚接口及 IP：

```
[SWA]vlan 2
[SWA]interface GigabitEthernet 1/0/2
[SWA-GigabitEthernet1/0/2]port access vlan 2
[SWA]interface Vlan-interface 1
```

```
[SWA-Vlan-interface1]ip address 172.16.1.1 24
[SWA]interface Vlan-interface 2
[SWA-Vlan-interface2]ip address 172.16.0.1 24
```

在 RTA 上配置接口 IP 及静态路由:

```
[RTA-GigabitEthernet0/0]ip address 172.16.0.2 24
[RTA]ip route-static 172.16.1.0 24 172.16.0.1
```

步骤三：在 RTA 上配置 DHCP 服务器及在 SWA 上配置 DHCP 中继

配置 RTA:

```
[RTA]dhcp enable
[RTA]dhcp server forbidden-ip 172.16.1.1
[RTA]dhcp server ip-pool pool1
[RTA-dhcp-pool-pool1]network 172.16.1.0 mask 255.255.255.0
[RTA-dhcp-pool-pool1]gateway-list 172.16.1.1
```

配置 SWA:

```
[SWA]dhcp enable
[SWA]interface Vlan-interface 1
[SWA-Vlan-interface1]dhcp select relay
[SWA-Vlan-interface1]dhcp relay server-address 172.16.0.2
```

步骤四：PCA 通过 DHCP 中继获取 IP 地址

断开 PCA 与 SWA 之间的连接电缆，再接上，以使 PCA 重新发起 DHCP 请求。

完成重新获取地址后，在 PCA 的“命令提示符”窗口下，键入命令 `ipconfig` 来验证 PCA 能否获得 IP 地址和网关等信息。正确的结果应该如下所示:

```
C:\Documents and Settings>ipconfig
Windows IP Configuration
Ethernet adapter 本地连接:
    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 172.16.1.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 172.16.1.1
```

如果无法获得 IP，请检查线缆连接是否正确，然后在“命令提示符”窗口下用 `ipconfig /renew` 命令来使 PCA 重新发起 DHCP 请求。

步骤五：查看 DHCP 中继相关信息

在 SWA 上查看 DHCP 服务器地址信息:

```
<SWA>display dhcp relay server-address
Interface name      Server IP address
Vlan-interface1     172.16.0.2
```

再查看 DHCP 中继的相关报文统计信息:

```
<SWA>display dhcp relay statistics
DHCP packets dropped:      0
DHCP packets received from clients:  5
    DHCPDISCOVER:          1
    DHCPREQUEST:           4
    DHCPINFORM:            0
    DHCPRELEASE:           0
    DHCPDECLINE:           0
    BOOTPREREQUEST:        0
DHCP packets received from servers:  2
    DHCP OFFER:            1
    DHCPACK:               1
```



```

DHCPNAK:                0
BOOTPREPLY:             0
DHCP packets relayed to servers: 5
  DHCPDISCOVER:         1
  DHCPREQUEST:          4
  DHCPINFORM:           0
  DHCPRELEASE:          0
  DHCPDECLINE:          0
  BOOTPREQUEST:         0
DHCP packets relayed to clients: 2
  DHCPPOFFER:           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
  DHCPPOFFER:           0
  DHCPACK:              0
  DHCPNAK:              0
  BOOTPREPLY:           0

```

学员可自行在 RTA 上用命令查看 DHCP 服务器的相关信息。具体命令及输出请参考前面的实验任务一中相关内容。

8.5 实验中的命令列表

表8-4 命令列表

命令	描述
dhcp enable	使能DHCP服务
network <i>network-address</i> [<i>mask-length</i> mask <i>mask</i>]	配置动态分配的IP地址范围
gateway-list <i>ip-address</i>	配置为DHCP客户端分配的网关地址
dhcp server forbidden-ip <i>low-ip-address</i> [<i>high-ip-address</i>]	配置DHCP地址池中不参与自动分配的IP地址
dhcp server ip-pool <i>pool-name</i>	创建DHCP地址池并进入DHCP地址池视图
dhcp relay server-group <i>group-id</i> ip <i>ip-address</i>	配置DHCP服务器组及组中DHCP服务器的IP地址
dhcp select relay	配置接口工作在DHCP中继模式
dhcp relay server-address <i>ip-address</i>	配置在DHCP中继上指定DHCP服务器的地址
display dhcp server free-ip	显示DHCP地址池的可用地址信息

命令	描述
display dhcp server forbidden-ip	显示DHCP地址池中不参与自动分配的IP地址
display dhcp server statistics	显示DHCP服务器的统计信息
display dhcp relay server-address [interface interface-type interface-number]	显示工作在DHCP中继模式的接口上指定的 DHCP服务器地址信息
display dhcp relay statistics [interface interface-type interface-number]	显示DHCP中继的相关报文统计信息

8.6 思考题

1. 在实验任务一里，如果设置 RTA 的 DHCP 地址池为 192.168.0.0/24，那么 PCA 能否获得该子网的 IP 地址？为什么？

答：不能获得。这是网络设备上的一个检查机制。因为 RTA 不仅是 DHCP 服务器，而且作为 PCA 的网关，还承担了转发数据的工作。如果 RTA 分配了与接口不同子网的 IP 地址给 PCA，PCA 与 RTA 之间无法通信，地址分配就失去了意义。因此它发现自己收到 DHCP 请求的接口子网与地址池资源所属子网不同时，它不会响应 DHCP 客户机的请求的，因此也就不会把错误的地址分配出去。

2. 在实验二的环境下，如果设置 RTA 地址池为 192.168.0.0/24，那么 PCA 能否获得该子网的 IP 地址？为什么？

答：PCA 将无法获得该子网的地址。因为 DHCP 中继在向 DHCP 服务器转发 DHCP 客户端发出的 DHCP 报文时，会把自己接收到 DHCP 客户端请求的接口地址填入 DHCP 报文中。服务器会根据 DHCP 中继接口所属的子网来分配正确的 IP 地址资源，如果地址池中 IP 资源与中继接口 IP 所在子网不匹配，地址不能被分配。

实验9 IPv6

9.1 实验内容与目标

完成本实验，您应该能够：

- 掌握如何在路由器上配置 IPv6 地址
- 掌握如何用 IPv6 Ping 命令进行 IPv6 地址可达性检查
- 掌握如何用命令行来查看 IPv6 地址配置和邻居信息

9.2 实验组网图

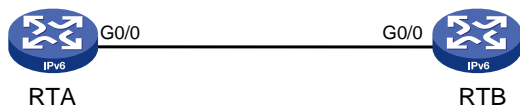


图9-1 IPv6 实验组网

9.3 实验设备与版本

本实验所需之主要设备器材如表 9-1 所示。

表9-1 实验设备列表

名称和型号	版本	数量	描述
MSR36-20	Version 7.1	2	每台至少带有一个以太网口
PC	Windows系统均可	1	路由器配置用机
第5类UTP以太网连接线		1	路由器之间互连用

9.4 实验过程

实验任务一：IPv6 地址配置及查看

本实验通过让学员在路由器上配置 IPv6 地址，然后用命令行观察 IPv6 邻居表项，再用命令行来测试 IPv6 邻居的可达性，从而让学员建立对 IPv6 地址的认知，建立起对邻居发现协议功能的初步了解。本实验中所用到的所有命令均在表 9-2 中，学员可根据实验步骤中的描述进行选取。

步骤一：建立物理连接

按照图 9-1 进行连接，并检查路由器的软件版本及配置信息，确保路由器软件版本符合要求，所有配置为初始状态。如果配置不符合要求，请读者在用户模式下擦除设备中的配置文件，然后重启路由器以使系统采用缺省的配置参数进行初始化。

以上步骤可能会用到以下命令：

```
<RTA> display version
<RTA> reset saved-configuration
<RTA> reboot
```

步骤二：配置接口自动生成链路本地地址及测试可达性，查看邻居信息

配置 RTA:

配置接口 G0/0 自动生成链路本地地址。

```
[RTA] interface GigabitEthernet0/0
[RTA-GigabitEthernet0/0] ipv6 address auto link-local
```

配置 RTB:

配置接口 G0/0 自动生成链路本地地址。

```
[RTB] interface GigabitEthernet0/0
[RTB-GigabitEthernet0/0] ipv6 address auto link-local
```

以上配置完成后，路由器会自动生成前缀为 FE80::的链路本地地址。用命令来查看生成的链路本地地址，记录下来并测试可达性。如下所示：

```
[RTA] display ipv6 interface GigabitEthernet0/0 brief
*down: administratively down
(s): spoofing
Interface          Physical Protocol IPv6 Address
GigabitEthernet0/0 up          up          FE80::72BA:EFF:FE80:419

[RTB] display ipv6 interface GigabitEthernet0/0 brief
*down: administratively down
(s): spoofing
Interface          Physical Protocol IPv6 Address
GigabitEthernet0/0 up          up          FE80::72BA:EFF:FE7F:F78C

[RTA] [RTA] ping ipv6 FE80::72BA:EFF:FE7F:F78C -i GigabitEthernet0/0
Ping6(56 data bytes) FE80::72BA:EFF:FE80:419 --> FE80::72BA:EFF:FE7F:F78C,
press CTRL_C to break
56 bytes from FE80::72BA:EFF:FE7F:F78C, icmp_seq=0 hlim=64 time=0.911 ms
56 bytes from FE80::72BA:EFF:FE7F:F78C, icmp_seq=1 hlim=64 time=0.212 ms
56 bytes from FE80::72BA:EFF:FE7F:F78C, icmp_seq=2 hlim=64 time=0.238 ms
56 bytes from FE80::72BA:EFF:FE7F:F78C, icmp_seq=3 hlim=64 time=0.189 ms
.....
```

同时，通过命令来查看路由器的邻居信息。如下所示：

```
[RTA] display ipv6 neighbors all
Type: S-Static D-Dynamic O-Openflow I-Invalid
IPv6 address      Link layer      VID Interface      State T Age
FE80::72BA:EFF:FE7F:F78C 70ba-ef7f-f78c N/A GE0/0 STALE D 17
```

可以看到，RTA 的 IPv6 邻居就是 RTB，是通过动态（Dynamic）方式来获得的。路由器的 IPv6 链路本地地址是符合 EUI-64 规范的地址。

步骤三：配置接口生成全球单播地址并测试可达性，查看邻居信息

配置 RTA:

在接口 **G0/0** 配置全球单播地址 **3001::1**。

```
[RTA] interface GigabitEthernet0/0
[RTA-GigabitEthernet0/0] ipv6 address 3001::1/64
```

配置 RTB:

在接口 **G0/0** 上配置全球单播地址 **3001::2**。

```
[RTB] interface GigabitEthernet0/0
[RTB-GigabitEthernet0/0] ipv6 address 3001::2/64
```

以上配置完成后，路由器接口会生成全球单播地址。用命令来查看生成的全球单播地址并测试可达性。如下所示：

```
[RTA] display ipv6 interface GigabitEthernet 0/0 brief
*down: administratively down
(s): spoofing
Interface                               Physical Protocol IPv6 Address
GigabitEthernet0/0                     up      up      3001::1

[RTB] display ipv6 interface GigabitEthernet 0/0 brief
*down: administratively down
(s): spoofing
Interface                               Physical Protocol IPv6 Address
GigabitEthernet0/0                     up      up      3001::2

[RTA] ping ipv6 3001::2
  Ping6(56 data bytes) 3001::1 --> 3001::2, press CTRL_C to break
56 bytes from 3001::2, icmp_seq=0 hlim=64 time=0.853 ms
56 bytes from 3001::2, icmp_seq=1 hlim=64 time=0.187 ms
56 bytes from 3001::2, icmp_seq=2 hlim=64 time=0.173 ms
56 bytes from 3001::2, icmp_seq=3 hlim=64 time=0.162 ms
.....
```

同时，通过命令来查看路由器的邻居信息。如下所示

```
[RTA] display ipv6 neighbors all
Type: S-Static      D-Dynamic      O-Openflow      I-Invalid
IPv6 address        Link layer          VID Interface      State T Age
3001::2              70ba-ef7f-f78c N/A GE0/0            STALE D 9
FE80::72BA:EFF:FE7F:F78C 70ba-ef7f-f78c N/A GE0/0            REACH D 29
```

可以看到，RTA 与 RTB 间除了有链路本地地址的邻居外，还有全球单播地址的邻居。

9.5 实验中的命令列表

表9-2 IPv6 实验命令列表

命令	命令执行视图	描述
ipv6 address { <i>ipv6-address prefix-length</i> <i>ipv6-prefix/prefix-length</i> }	接口视图	手工配置接口的IPv6全球单播地址

命令	命令执行视图	描述
ipv6 address auto link-local	接口视图	配置系统自动为接口生成链路本地地址
display ipv6 interface [<i>interface-type interface-number</i> brief]	任意视图	显示接口的IPv6信息
ping ipv6	任意视图	测试对端设备的IPv6可达性
display ipv6 neighbors { <i>ipv6-address</i> all dynamic interface <i>interface-type interface-number</i> static vlan <i>vlan-id</i> } [verbose]	任意视图	显示邻居信息

9.6 思考题

1. 在进行 IPv6 邻居的查看时，邻居表项中的 **state** 一栏中的显示是什么？它表示什么意思？

答：显示有可能为 INCMP、REACH、STALE、DELAY 及 PROBE 之中的一种。INCMF 表示正在解析地址，邻居的链路层地址尚未确定；REACH 表示邻居可达；STALE、DELAY 及 PROBE 表示未确定邻居是否可达。ND 协议用此表示邻居地址的可信度，结合更多的操作，从而实现比 ARP 协议更高的安全性。

实验10 IP 路由基础

10.1 实验内容与目标

完成本实验，您应该能够：

- 掌握路由转发的基本原理
- 掌握静态路由、缺省路由的配置方法
- 掌握查看路由表的基本命令

10.2 实验组网图

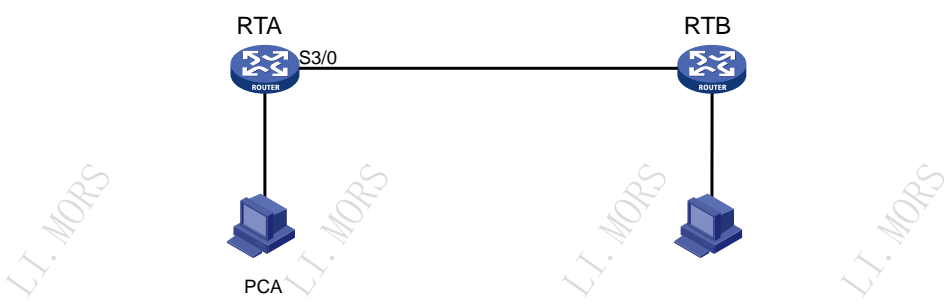


图10-1 静态路由配置实验

10.3 实验设备与版本

本实验所需之主要设备器材如表 10-1 所示。

表10-1 设备列表

名称和型号	版本	数量	描述
MSR3620	CMW7.1.049-R0106P18	2	
PC	Windows XP	2	
V.35 DTE串口线	--	1	
V.35 DCE串口线	--	1	
第5类UTP以太网连接线	--	2	

10.4 实验过程

实验任务一：查看路由表

本实验主要是通过通过在路由器上通过查看路由表，观察路由表中路由项。通过本次实验，学员能够掌握如何使用命令来查看路由表，及了解路由项中要素的含义。

步骤一：建立物理连接

按照图 10-1 进行连接，并检查路由器的软件版本及配置信息，确保路由器软件版本符合要求，所有配置为初始状态。如果配置不符合要求，请读者在用户模式下擦除设备中的配置文件，然后重启路由器以使系统采用缺省的配置参数进行初始化。

以上步骤可能会用到以下命令：

```
<H3C> display version
<H3C> reset saved-configuration
<H3C> reboot
```

步骤二：在路由器上查看路由表

首先，在路由器上查看路由表，如下所示：

```
[RTA]display ip routing-table
```

```
Destinations : 8          Routes : 8
```

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
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

由以上输出可知，目前路由器有 8 条路由，其中目的地址是 127.0.0.0 的路由，是路由器的环回地址直连路由。

表10-2 IP 地址列表

设备名称	接口	IP 地址	网关
RTA	S3/0	192.168.1.1/24	--
	G0/0	192.168.0.1/24	--
RTB	S3/0	192.168.1.2/24	--
	G0/0	192.168.2.1/24	--
PCA	--	192.168.0.2/24	192.168.0.1
PCB	--	192.168.2.2/24	192.168.2.1

按表 10-2 所示在路由器接口上分别配置 IP 地址。

配置 RTA:

```
[RTA-GigabitEthernet0/0]ip address 192.168.0.1 24
[RTA-Serial3/0]ip address 192.168.1.1 24
```


配置 RTB:

```
[RTB-GigabitEthernet0/0]ip address 192.168.2.1 24
[RTB-Serial3/0]ip address 192.168.1.2 24
```

配置完成后, 再次查看路由表。例如, 在 RTA 上查看路由表, 如下:

```
[RTA]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
192.168.0.0/24	Direct	0	0	192.168.0.1	GE0/0
192.168.0.0/32	Direct	0	0	192.168.0.1	GE0/0
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	GE0/0
192.168.1.0/24	Direct	0	0	192.168.1.1	Ser3/0
192.168.1.0/32	Direct	0	0	192.168.1.1	Ser3/0
192.168.1.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.1.2/32	Direct	0	0	192.168.1.2	Ser3/0
192.168.1.255/32	Direct	0	0	192.168.1.1	Ser3/0
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

由以上输出可知, 在 RTA 上配置了 IP 地址 192.168.0.1 和 192.168.1.1 以及在 RTB 上配置 192.168.1.2 后, RTA 的路由表中有了直连路由 192.168.0.0/24, 192.168.0.1/32, 192.168.1.0/24, 192.168.1.1/32, 192.168.1.2/32。这其中, 192.168.0.1/32, 192.168.1.1/32, 192.168.1.2/32 是主机路由, 192.168.0.0/24, 192.168.1.0/24 是子网路由。直连路由是由链路层协议发现的路由, 链路层协议 UP 后, 路由器会将其加入路由表中。如果我们关闭链路层协议, 则相关直连路由也消失。

在 RTA 上关闭接口, 如下:

```
[RTA-GigabitEthernet0/0]shutdown
```

查看路由表, 如下:

```
[RTA]display ip routing-table
```

```
Destinations : 13      Routes : 13
```

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
192.168.1.0/24	Direct	0	0	192.168.1.1	Ser3/0
192.168.1.0/32	Direct	0	0	192.168.1.1	Ser3/0
192.168.1.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.1.2/32	Direct	0	0	192.168.1.2	Ser3/0
192.168.1.255/32	Direct	0	0	192.168.1.1	Ser3/0
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

可知, 在接口 shutdown 后, 所运行的链路层协议关闭, 直连路由也就自然消失了。

再开启接口，如下：

```
[RTA-GigabitEthernet0/0]undo shutdown
```

等到链路层协议 up 后，再次查看路由表，可以发现接口 GigabitEthernet0/0 的直连路由又出现了。

实验任务二：静态路由配置

本实验主要是通过通过在路由器上配置静态路由，从而达到 PC 之间能够互访的目的。通过本次实验，学员能够掌握静态路由的配置，加深对路由环路产生原因的理解。

步骤一：在 PC 配置 IP 地址

按表 10-2 所示在 PC 上配置 IP 地址和网关。配置完成后，在 Windows 操作系统的【开始】里选择【运行】，在弹出的窗口里输入 CMD，然后在【命令提示符】下用 ipconfig 命令来查看所配置的 IP 地址和网关是否正确。

在 PC 上用 Ping 命令来测试到网关的可达性。例如，在 PCA 上测试到网关（192.168.0.1）的可达性，如下所示：

```
C:\Documents and Settings\Administrator>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time<1ms TTL=255
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

再测试 PC 之间的可达性。例如，在 PCA 上用 Ping 命令测试到 PCB 的可达性，如下：

```
C:\Documents and Settings\Administrator>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.0.1: Destination net unreachable.
Reply from 192.168.0.1: Destination net unreachable.
Reply from 192.168.0.1: Destination net unreachable.
Reply from 192.168.0.1: Destination net unreachable.

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

以上输出信息显示，RTA（192.168.0.1）返回了目的网络不可达的信息给 PCA，说明 RTA 没有到达 PCB（192.168.2.2）的路由。

在 RTA 上查看路由表，如下所示：

```
[RTA]display ip routing-table

Destinations : 13          Routes : 13

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
192.168.1.0/24	Direct	0	0	192.168.1.1	Ser3/0
192.168.1.0/32	Direct	0	0	192.168.1.1	Ser3/0
192.168.1.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.1.2/32	Direct	0	0	192.168.1.2	Ser3/0
192.168.1.255/32	Direct	0	0	192.168.1.1	Ser3/0
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

问题原因发现了,是因为 RTA 路由表中没有到 PCB 所在网段 192.168.2.0/24 的路由。PCA 发出报文到 RTA 后, RTA 就会丢弃并返回不可达信息给 PCA。我们可以通过配置静态路由而使网络可达。

步骤二：静态路由配置规划

请学员考虑,在 RTA 和 RTB 上应该配置到何目的网络的静态路由,其下一跳应该指向哪个 IP 地址?

步骤三：配置静态路由

配置 RTA:

```
[RTA]ip route-static 192.168.2.0 24 192.168.1.2
```

配置 RTB:

```
[RTB]ip route-static 192.168.0.0 24 192.168.1.1
```

配置完成后,在路由器上查看路由表。例如,在 RTA 上查看路由表,如下:

```
[RTA]display ip routing-table
```

```
Destinations : 18      Routes : 18
```

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
192.168.0.0/24	Direct	0	0	192.168.0.1	GE0/0
192.168.0.0/32	Direct	0	0	192.168.0.1	GE0/0
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	GE0/0
192.168.1.0/24	Direct	0	0	192.168.1.1	Ser3/0
192.168.1.0/32	Direct	0	0	192.168.1.1	Ser3/0
192.168.1.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.1.2/32	Direct	0	0	192.168.1.2	Ser3/0
192.168.1.255/32	Direct	0	0	192.168.1.1	Ser3/0
192.168.2.0/24	Static	60	0	192.168.1.2	Ser3/0
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

测试 PC 之间的可达性。例如,在 PCA 上用 Ping 命令测试到 PCB 的可达性,如下:

```
C:\Documents and Settings\Administrator>ping 192.168.2.2
```

```
Pinging 192.168.2.2 with 32 bytes of data:
```

```
Reply from 192.168.2.2: bytes=32 time=20ms TTL=126
```

```

Reply from 192.168.2.2: bytes=32 time=20ms TTL=126
Reply from 192.168.2.2: bytes=32 time=20ms TTL=126
Reply from 192.168.2.2: bytes=32 time=20ms TTL=126

```

```

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 20ms, Maximum = 20ms, Average = 20ms

```

在 PCA 上用 Tracert 命令来查看到 PCB 的路径，如下所示：

```
C:\Documents and Settings\Administrator>tracert 192.168.2.2
```

```
Tracing route to 192.168.2.2 over a maximum of 30 hops
```

```

  1    <1 ms    <1 ms    <1 ms    192.168.0.1
  2    23 ms    23 ms    23 ms    192.168.1.2
  3    28 ms    27 ms    28 ms    192.168.2.2

```

```
Trace complete.
```

以上结果说明，数据报文是沿 PCA→RTA→RTB→PCB 的路径被转发的。

步骤四：路由环路观察

为了人为造成环路，需要在 RTA 和 RTB 上分别配置一条缺省路由，下一跳互相指向对方。因为路由器之间是用串口相连的，所以可以配置下一跳为本地接口。

配置 RTA:

```
[RTA]ip route-static 0.0.0.0 0.0.0.0 s3/0
```

配置 RTB:

```
[RTB]ip route-static 0.0.0.0 0.0.0.0 s3/0
```

配置完成后，在路由器上查看路由表。例如，在 RTA 上查看路由表，显示结果如下：

```
[RTA]display ip routing-table
```

```
Destinations : 19          Routes : 19
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0.0/0	Static	60	0	0.0.0.0	Ser3/0
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
192.168.0.0/24	Direct	0	0	192.168.0.1	GE0/0
192.168.0.0/32	Direct	0	0	192.168.0.1	GE0/0
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	GE0/0
192.168.1.0/24	Direct	0	0	192.168.1.1	Ser3/0
192.168.1.0/32	Direct	0	0	192.168.1.1	Ser3/0
192.168.1.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.1.2/32	Direct	0	0	192.168.1.2	Ser3/0
192.168.1.255/32	Direct	0	0	192.168.1.1	Ser3/0
192.168.2.0/24	Static	60	0	192.168.1.2	Ser3/0
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

可知，缺省路由配置成功。

然后在 PC 上用 Tracert 命令来观察环路情况。例如，在 PCA 上用 Tracert 命令来追踪到目的 IP 地址 3.3.3.3 的路径：

```
C:\Documents and Settings\Administrator>tracert 3.3.3.3
```

```
Tracing route to 3.3.3.3 over a maximum of 30 hops
```

```
  1    <1 ms    <1 ms    <1 ms  192.168.0.1
  2    23 ms    23 ms    23 ms  192.168.1.2
  3    27 ms    27 ms    27 ms  192.168.1.1
  4    51 ms    51 ms    50 ms  192.168.1.2
  5    56 ms    55 ms    55 ms  192.168.1.1
.....
 29   385 ms   387 ms   386 ms  192.168.1.1
 30   409 ms   409 ms   409 ms  192.168.1.2
```

```
Trace complete.
```

由以上输出可以看到，到目的地址 3.3.3.3 的报文匹配了缺省路由，报文被转发到了 RTB（192.168.1.2），而 RTB 又根据它的缺省路由，把报文转发回了 RTA（192.168.1.1）。这样就形成了转发环路，报文在两台路由器之间被循环转发，直到 TTL 值到 0 后被丢弃。

所以在不同路由器上配置到相同网段的静态路由时，不要配置路由的下一跳互相指向对方，否则就形成了环路。

10.5 实验中的命令列表

表10-3 IP 路由原理实验命令列表

命令	描述
ip route-static <i>dest-address</i> { <i>mask-length</i> <i>mask</i> } { <i>interface-type</i> <i>interface-number</i> [<i>next-hop-address</i>] <i>next-hop-address</i> }	配置静态路由目的网段（包括子网长度）及下一跳
display ip routing-table <i>ip-address</i> [<i>mask</i> <i>mask-length</i>]	显示IP路由表摘要信息或显示匹配某个目的网段或地址的路由
ipconfig	在Windows系统上查看IP配置

10.6 思考题

1. 在本实验中，如果仅在 RTA 上配置静态路由，不在 RTB 上配置，那么 PCA 发出的数据报文能到达 PCB 吗？PCA 能够 Ping 通 PCB 吗？

答：PCA 发出的数据报文能够到达 PCB。因为 RTA 有路由，从而转发到 RTB，而 RTB 上有直连路由到 PCB 所在网段，所以能够将报文转发到 PCB。但是 PCA 不能 Ping 通 PCB，因为 RTB 上没有到 PCA 的回程路由，而 Ping 报文是双向的，从 PCB 返回的 Ping 报文在 RTB 被丢弃。

在实际应用中，从一个网段到另一个网段的单通意义不大。因为基本所有常用应用（HTTP，FTP，E-mail 等）都是基于 TCP 的，都需要三方握手，也就是需要互相可达才能建立连接。

2. 路由器和 PC 之间会形成路由环路吗？

答：不会，正常情况下 PC 不具备转发功能，因此当路由器将数据报文转发给 PC 时，如果目的地址不是该 PC，报文会被丢弃而不是继续转发。

实验11 配置 RIP

11.1 实验内容与目标

完成本实验，您应该能够：

- 加深 RIP 协议原理的理解
- 了解 RIP 实现运行机制
- 熟悉 RIP 路由配置
- 熟悉 RIP 路由维护

11.2 实验组网图

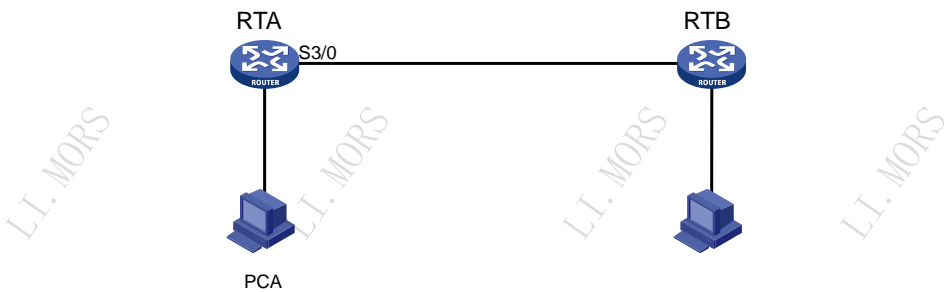


图11-1 RIP 实验组网图

11.3 实验设备与版本

本实验所需之主要设备器材如表 11-1 所示。

表11-1 设备列表

名称和型号	版本	数量	描述
MSR3620	CMW7.1.049-R0106P18	2	每台带有一个以太网口，一个串口
PC	Windows XP	2	
V.35 DTE串口线	--	1	
V.35 DCE串口线	--	1	
第5类UTP以太网连接线	--	2	交叉线，路由器与PC机连接用

11.4 实验过程

实验任务一：配置 RIPv1

本实验主要通过配置在路由器上配置 RIPv1 协议，达到 PC 之间能够互访的目的。通过本次实验，学员应能够掌握 RIPv1 协议的基本配置。

步骤一：建立物理连接

按照图 11-1 进行连接，并检查路由器的软件版本及配置信息，确保路由器软件版本符合要求，所有配置为初始状态。如果配置不符合要求，请读者在用户模式下擦除设备中的配置文件，然后重启路由器以使系统采用缺省的配置参数进行初始化。

以上步骤可能会用到以下命令：

```
<RTA> display version
<RTA> reset saved-configuration
<RTA> reboot
```

步骤二：在 PC 和路由器配置 IP 地址

表11-2 IP 地址列表

设备名称	接口	IP 地址	网关
RTA	S3/0	192.168.1.1/24	--
	G0/0	192.168.0.1/24	--
RTB	S3/0	192.168.1.2/24	--
	G0/0	192.168.2.1/24	--
PCA	--	192.168.0.2/24	192.168.0.1
PCB	--	192.168.2.2/24	192.168.2.1

按表 11-2 所示在路由器接口上配置 IP 地址。

配置 RTA:

```
[RTA-GigabitEthernet0/0]ip address 192.168.0.1 24
[RTA-Serial3/0]ip address 192.168.1.1 24
```

配置 RTB:

```
[RTB-GigabitEthernet0/0]ip address 192.168.2.1 24
[RTB-Serial3/0]ip address 192.168.1.2 24
```

按表 11-2 所示在 PC 上配置 IP 地址和网关。配置完成后，在 Windows 操作系统的【开始】里选择【运行】，在弹出的窗口里输入 CMD，然后在【命令提示符】下用 ipconfig 命令来查看所配置的 IP 地址和网关是否正确。

在 PC 上用 Ping 命令来测试到网关的可达性。例如，在 PCA 上测试到网关（192.168.0.1）的可达性，如下所示：

```
C:\Documents and Settings\Administrator>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:
```



```

Reply from 192.168.0.1: bytes=32 time<1ms TTL=255
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255

```

```

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

```

再测试 PC 之间的可达性。例如，在 PCA 上用 Ping 命令测试到 PCB 的可达性，如下：

```
C:\Documents and Settings\Administrator>ping 192.168.2.2
```

```
Pinging 192.168.2.2 with 32 bytes of data:
```

```

Reply from 192.168.0.1: Destination net unreachable.
Reply from 192.168.0.1: Destination net unreachable.
Reply from 192.168.0.1: Destination net unreachable.
Reply from 192.168.0.1: Destination net unreachable.

```

```

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

```

PC 的网关返回了目的网络不可达的信息。这说明路由器没有路由到达目的地。在路由器上查看路由表。例如，在 RTA 上查看路由表，如下：

```
[RTA]display ip routing-table
```

```
Destinations : 13          Routes : 13
```

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
192.168.1.0/24	Direct	0	0	192.168.1.1	Ser3/0
192.168.1.0/32	Direct	0	0	192.168.1.1	Ser3/0
192.168.1.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.1.2/32	Direct	0	0	192.168.1.2	Ser3/0
192.168.1.255/32	Direct	0	0	192.168.1.1	Ser3/0
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，RTA 路由表中没有到 PCB 所在网段 192.168.2.0/24 的路由。所以当 PCA 发出的报文到 RTA 后，RTA 就丢弃并返回不可达信息给 PCA。我们可以在路由器上配置 RIP 协议来解决这个问题。

步骤三：启用 RIP 协议

配置 RTA:

```

[RTA]rip
[RTA-rip-1]network 192.168.0.0
[RTA-rip-1]network 192.168.1.0

```

配置 RTB:

```

[RTB]rip
[RTB-rip-1]network 192.168.1.0
[RTB-rip-1]network 192.168.2.0

```

配置完成后，在路由器上查看路由表。例如，在 RTA 上查看路由表，如下：

```
[RTA]display ip routing-table
```

```
Destinations : 18      Routes : 18
```

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
192.168.0.0/24	Direct	0	0	192.168.0.1	GE0/0
192.168.0.0/32	Direct	0	0	192.168.0.1	GE0/0
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	GE0/0
192.168.1.0/24	Direct	0	0	192.168.1.1	Ser3/0
192.168.1.0/32	Direct	0	0	192.168.1.1	Ser3/0
192.168.1.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.1.2/32	Direct	0	0	192.168.1.2	Ser3/0
192.168.1.255/32	Direct	0	0	192.168.1.1	Ser3/0
192.168.2.0/24	RIP	100	1	192.168.1.2	Ser3/0
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

可以看到路由表中有到目的网络 192.168.2.0/24 的路由，这个路由是通过 RIP 协议学习到的。然后再测试 PC 之间的可达性。例如，在 PCA 上用 Ping 命令测试到 PCB 的可达性，如下：

```
C:\Documents and Settings\Administrator>ping 192.168.2.2
```

```
Pinging 192.168.2.2 with 32 bytes of data:
```

```
Reply from 192.168.2.2: bytes=32 time=20ms TTL=126
Reply from 192.168.2.2: bytes=32 time=20ms TTL=126
Reply from 192.168.2.2: bytes=32 time=19ms TTL=126
Reply from 192.168.2.2: bytes=32 time=20ms TTL=126
```

```
Ping statistics for 192.168.2.2:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 19ms, Maximum = 20ms, Average = 19ms
```

可以看到，PC 间可达了。

步骤四：查看 RIP 的运行状态

在 RTA 上用命令 display rip 查看：

```
[RTA]display rip
Public VPN-instance name:
RIP process: 1
RIP version: 1
Preference: 100
Checkzero: Enabled
Default cost: 0
Summary: Enabled
Host routes: Enabled
Maximum number of load balanced routes: 6
Update time : 30 secs Timeout time : 180 secs
Suppress time : 120 secs Garbage-collect time : 120 secs
Update output delay: 20(ms) Output count: 3
TRIP retransmit time: 5(s) Retransmit count: 36
Graceful-restart interval: 60 secs
Triggered Interval : 5 50 200
```

```

Silent interfaces: None
Default routes: Disabled
Verify-source: Enabled
Networks:
    192.168.0.0          192.168.1.0
Configured peers: None
Triggered updates sent: 2
Number of routes changes: 3
Number of replies to queries: 1

```

从以上输出信息可知，目前路由器运行的是 **RIPv1**，自动聚合功能是打开的；路由更新周期（Update time）是 30 秒，network 命令所指定的网段是 192.168.0.0 和 192.168.1.0。

打开 RIP 的 debugging，观察 RIP 收发协议报文的情况。

```

<RTA>terminal debugging
<RTA>debugging rip 1 packet
<RTA>
*Dec 3 01:41:15:325 2014 H3C RIP/7/RIPDEBUG: RIP 1 : Sending response on interface
GigabitEthernet0/0 from 192.168.0.1 to 255.255.255.255
*Dec 3 01:41:15:325 2014 H3C RIP/7/RIPDEBUG: Packet: version 1, cmd response,
length 44
*Dec 3 01:41:15:325 2014 H3C RIP/7/RIPDEBUG: AFI 2, destination 192.168.1.0,
cost 1
*Dec 3 01:41:15:325 2014 H3C RIP/7/RIPDEBUG: AFI 2, destination 192.168.2.0,
cost 2
*Dec 3 01:41:15:326 2014 H3C RIP/7/RIPDEBUG: RIP 1 : Sending response on interface
Serial3/0 from 192.168.1.1 to 255.255.255.255
*Dec 3 01:41:15:326 2014 H3C RIP/7/RIPDEBUG: Packet: version 1, cmd response,
length 24
*Dec 3 01:41:15:326 2014 H3C RIP/7/RIPDEBUG: AFI 2, destination 192.168.0.0,
cost 1
*Dec 3 01:41:37:819 2014 H3C RIP/7/RIPDEBUG: RIP 1 : Receiving response from
192.168.1.2 on Serial3/0
*Dec 3 01:41:37:819 2014 H3C RIP/7/RIPDEBUG: Packet: version 1, cmd response,
length 24
*Dec 3 01:41:37:819 2014 H3C RIP/7/RIPDEBUG: AFI 2, destination 192.168.2.0,
cost 1

```

由以上输出可知，RTA 在接口 GigabitEthernet0/0 上发送的路由更新包含路由 192.168.1.0（度量值为 1）和 192.168.2.0（度量值为 2），在接口 Serial3/0 上发送的路由更新包含了路由 192.168.0.0（度量值为 1）；以上更新是以广播方式发送的。在接口 Serial3/0 上接收到了来自 RTB（192.168.1.2）的路由更新，包含了路由 192.168.2.0（度量值为 1）。

分析以上的路由更新，可以发现，RTA 在接口 Serial3/0 上收到路由 192.168.2.0，而不会再把此路由从接口 Serial3/0 上发出去。原因是路由器启用 RIP 后，水平分割功能缺省是打开的。

步骤五：查看水平分割与毒性逆转

在 RTA 的接口 Serial3/0 上取消水平分割，观察收发协议报文的情况。

```

[RTA-Serial3/0]undo rip split-horizon

*Dec 3 01:43:41:826 2014 H3C RIP/7/RIPDEBUG: RIP 1 : Sending response on interface
Serial3/0 from 192.168.1.1 to 255.255.255.255
*Dec 3 01:43:41:826 2014 H3C RIP/7/RIPDEBUG: Packet: version 1, cmd response,
length 64
*Dec 3 01:43:41:827 2014 H3C RIP/7/RIPDEBUG: AFI 2, destination 192.168.0.0,
cost 1
*Dec 3 01:43:41:827 2014 H3C RIP/7/RIPDEBUG: AFI 2, destination 192.168.1.0,
cost 1

```

```
*Dec 3 01:43:41:827 2014 H3C RIP/7/RIPDEBUG: AFI 2, destination 192.168.2.0, cost 2
```

由以上输出可知，在水平分割功能关闭的情况下，RTA 在接口 Serial3/0 上发送的路由更新包含了路由 192.168.0.0、192.168.1.0 和 192.168.2.0。也就是说，路由器把从接口 Serial3/0 学到的路由 192.168.2.0 又从接口发送了出去。这样容易造成路由环路。

另外一种避免环路的方法是毒性逆转。在 RTA 的接口 Serial3/0 上启用毒性逆转，再观察收发协议报文的情况。

```
[RTA-Serial3/0]rip poison-reverse

*Dec 3 01:45:05:325 2014 H3C RIP/7/RIPDEBUG: RIP 1 : Sending response on interface Serial3/0 from 192.168.1.1 to 255.255.255.255
*Dec 3 01:45:05:325 2014 H3C RIP/7/RIPDEBUG: Packet: version 1, cmd response, length 44
*Dec 3 01:45:05:325 2014 H3C RIP/7/RIPDEBUG: AFI 2, destination 192.168.0.0, cost 1
*Dec 3 01:45:05:325 2014 H3C RIP/7/RIPDEBUG: AFI 2, destination 192.168.2.0, cost 16
```

由以上输出信息可知，启用毒性逆转后，RTA 在接口 Serial 3/0 上发送的路由更新包含了路由 192.168.2.0，但度量值为 16（无穷大）。相当于显式地告诉 RTB，从 RTA 的接口 Serial3/0 上不能到达网络 192.168.2.0。

步骤六：用 silent-interface 来控制协议报文发送

在前面实验中，路由器在所有接口都发送协议报文，包括连接 PC 的接口。实际上，PC 并不需要接收 RIP 协议报文。我们可以用 silent-interface 命令使接口只接收而不发送 RIP 协议报文。

配置 RTA:

```
[RTA-rip-1]silent-interface GigabitEthernet 0/0
```

配置 RTB:

```
[RTB-rip-1]silent-interface GigabitEthernet 0/0
```

配置完成后，用 debugging 命令来观察 RIP 收发协议报文的情况。可以发现，RIP 不再从接口 GigabitEthernet0/0 发送协议报文了。

这种方法的另外一个好处是防止路由泄漏而造成网络安全隐患。比如，公司某台运行 RIP 的路由器连接到公网，那就可以通过配置 silent-interface 而防止公司内网中的路由泄漏到公网。上。

此步骤完成后，在路由器上关闭 debugging，以免影响后续实验。

```
<RTA>undo debugging all
<RTB>undo debugging all
```

实验任务二：配置 RIPv2

本实验首先通过让 RIPv1 在划分子网的情况下不能正确学习路由，从而让学员了解到 RIPv1 的局限性；然后指导学员启用 RIPv2 协议。通过本实验，学员应该能够了解 RIPv1 的局限性，并掌握如何在路由器上配置 RIPv2。

步骤一：建立物理连接

按照图 11-1 进行连接，并检查路由器的软件版本及配置信息，确保路由器软件版本符合要求，所有配置为初始状态。如果配置不符合要求，请读者在用户模式下擦除设备中的配置文件，然后重启路由器以使系统采用缺省的配置参数进行初始化。

以上步骤可能会用到以下命令：

```
<RTA> display version
<RTA> reset saved-configuration
<RTA> reboot
```

步骤二：在 PC 和路由器上配置 IP 地址

表11-3 IP 地址列表

设备名称	接口	IP 地址	网关
RTA	S3/0	192.168.1.1/24	--
	G0/0	192.168.0.1/24	--
RTB	S3/0	192.168.1.2/24	--
	G0/0	10.0.0.1/24	--
PCA	--	192.168.0.2/24	192.168.0.1
PCB	--	10.0.0.2/24	10.0.0.1

按表 11-3 所示在路由器接口上配置 IP 地址。

配置 RTA:

```
[RTA-GigabitEthernet0/0]ip address 192.168.0.1 24
[RTA-Serial3/0]ip address 192.168.1.1 24
```

配置 RTB:

```
[RTB-GigabitEthernet0/0]ip address 10.0.0.1 24
[RTB-Serial3/0]ip address 192.168.1.2 24
```

按表 11-3 所示在 PC 上配置 IP 地址和网关。配置完成后，在 Windows 操作系统的【开始】里选择【运行】，在弹出的窗口里输入 CMD，然后在【命令提示符】下用 ipconfig 命令来查看所配置的 IP 地址和网关是否正确。

步骤三：配置 RIPv1，观察路由表

配置 RTA:

```
[RTA]rip
[RTA-rip-1]network 192.168.0.0
[RTA-rip-1]network 192.168.1.0
```

配置 RTB:

```
[RTB]rip
[RTB-rip-1]network 192.168.1.0
[RTB-rip-1]network 10.0.0.0
```

配置完成后，在 RTA 上查看路由表，如下：

```
[RTA]display ip routing-table
```

Destinations : 18

Routes : 18

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
10.0.0.0/8	RIP	100	1	192.168.1.2	Ser3/0
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
192.168.0.0/24	Direct	0	0	192.168.0.1	GE0/0
192.168.0.0/32	Direct	0	0	192.168.0.1	GE0/0
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	GE0/0
192.168.1.0/24	Direct	0	0	192.168.1.1	Ser3/0
192.168.1.0/32	Direct	0	0	192.168.1.1	Ser3/0
192.168.1.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.1.2/32	Direct	0	0	192.168.1.2	Ser3/0
192.168.1.255/32	Direct	0	0	192.168.1.1	Ser3/0
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

由上述路由表信息可看到，RTA 路由表中通过 RIP 协议学习到路由 10.0.0.0/8，但实际上在 RTB 的网络是 10.0.0.0/24，RTA 并没有正确学习到路由。

在 RTA 上打开 debugging，观察 RTA 收发协议报文的情况：

```
<RTA>terminal debugging
<RTA>debug rip 1 packet
<RTA>
*Dec 3 01:49:06:381 2014 H3C RIP/7/RIPDEBUG: RIP 1 : Receiving response from
192.168.1.2 on Serial3/0
*Dec 3 01:49:06:381 2014 H3C RIP/7/RIPDEBUG: Packet: version 1, cmd response,
length 24
*Dec 3 01:49:06:381 2014 H3C RIP/7/RIPDEBUG: AFI 2, destination 10.0.0.0, cost
1
```

以上输出表示 RTA 收到 RTB 发出的路由更新，更新中有路由 10.0.0.0，但是并没有掩码。所以 RTA 假定此路由 10.0.0.0 的掩码是自然掩码，即 10.0.0.0/8。

由此可知，路由器间不能正确学习路由，其原因为 RIPv1 协议报文中不携带掩码信息。通过将 RIP 运行版本修改为 RIPv2，可以解决这个问题。

步骤四：配置 RIPv2

配置 RTA:

```
[RTA-rip-1]version 2
[RTA-rip-1]undo summary
```

配置 RTB:

```
[RTB-rip-1]version 2
[RTB-rip-1]undo summary
```

配置完成后，在 RTA 上查看路由表，如下所示：

```
[RTA]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
10.0.0.0/8	RIP	100	1	192.168.1.2	Ser3/0
10.0.0.0/24	RIP	100	1	192.168.1.2	Ser3/0

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
192.168.0.0/24	Direct	0	0	192.168.0.1	GE0/0
192.168.0.0/32	Direct	0	0	192.168.0.1	GE0/0
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	GE0/0
192.168.1.0/24	Direct	0	0	192.168.1.1	Ser3/0
192.168.1.0/32	Direct	0	0	192.168.1.1	Ser3/0
192.168.1.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.1.2/32	Direct	0	0	192.168.1.2	Ser3/0
192.168.1.255/32	Direct	0	0	192.168.1.1	Ser3/0
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，现在 RTA 能够正确学习到路由 10.0.0.0/24。

路由表中仍然有路由 10.0.0.0/8，其原因是 RIP 路由的老化时间是 180 秒。当未收到关于此路由的更新超过 180 秒后，RIP 才会把此路由从 IP 路由表中撤销。

观察 RIP 的运行状态。例如，在 RTA 上查看 RIP 的运行状态，如下：

```
[RTA]display rip
Public VPN-instance name:
RIP process: 1
  RIP version: 2
  Preference: 100
  Checkzero: Enabled
  Default cost: 0
  Summary: Disabled
  Host routes: Enabled
  Maximum number of load balanced routes: 6
  Update time : 30 secs Timeout time : 180 secs
  Suppress time : 120 secs Garbage-collect time : 120 secs
  Update output delay: 20(ms) Output count: 3
  TRIP retransmit time: 5(s) Retransmit count: 36
  Graceful-restart interval: 60 secs
  Triggered Interval : 5 50 200
  Silent interfaces: None
  Default routes: Disabled
  Verify-source: Enabled
  Networks:
    192.168.0.0      192.168.1.0
  Configured peers: None
  Triggered updates sent: 7
  Number of routes changes: 6
  Number of replies to queries: 1
```

由以上信息可知，当前 RIP 的运行版本是 RIPv2。

再观察 RTA 收发协议报文的情况：

```
<RTA>terminal debugging
<RTA>debug rip 1 packet
<RTA>
*Dec 3 01:51:50:879 2014 H3C RIP/7/RIPDEBUG: RIP 1 : Receiving response from
192.168.1.2 on Serial3/0
*Dec 3 01:51:50:879 2014 H3C RIP/7/RIPDEBUG: Packet: version 2, cmd response,
length 24
*Dec 3 01:51:50:879 2014 H3C RIP/7/RIPDEBUG: AFI 2, destination
10.0.0.0/255.255.255.0, nexthop 0.0.0.0, cost 1, tag 0
```

可以观察到，RIPv2 的协议报文中携带了掩码信息。

步骤五：配置 RIPv2 认证

RIPv2 支持认证，目的是加强协议的安全性。我们先在两端路由器上配置不同的密码，看路由器之间能否正确学习路由信息。

配置 RTA:

```
[RTA-Serial3/0]rip authentication-mode md5 rfc2453 plain aaaaa
```

配置 RTB:

```
[RTB-Serial3/0]rip authentication-mode md5 rfc2453 plain abcde
```

因为原有的路由需要过一段时间才能老化，所以可以将接口关闭再启用，加快重新学习路由的过程。例如，关闭再启用 RTA 的接口 Serial3/0，如下：

```
[RTA-Serial3/0]shutdown
[RTA-Serial3/0]undo shutdown
```

配置完成后，在路由器上查看路由表。例如，在 RTA 上查看，如下：

```
[RTA-rip-1]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
192.168.0.0/24	Direct	0	0	192.168.0.1	GE0/0
192.168.0.0/32	Direct	0	0	192.168.0.1	GE0/0
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	GE0/0
192.168.1.0/24	Direct	0	0	192.168.1.1	Ser3/0
192.168.1.0/32	Direct	0	0	192.168.1.1	Ser3/0
192.168.1.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.1.2/32	Direct	0	0	192.168.1.2	Ser3/0
192.168.1.255/32	Direct	0	0	192.168.1.1	Ser3/0
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

再观察 RTA 收发协议报文的情况：

```
<RTA>terminal debugging
<RTA>debug rip 1 packet
<RTA>
*Dec 3 02:02:34:456 2014 H3C RIP/7/RIPDEBUG: RIP 1 : Receiving response from
192.168.1.2 on Serial3/0
*Dec 3 02:02:34:456 2014 H3C RIP/7/RIPDEBUG: Packet: version 2, cmd response,
length 48
*Dec 3 02:02:34:456 2014 H3C RIP/7/RIPDEBUG: Authentication-mode: MD5 Digest:
105e1a47.8ad5ec5f.87da0a29.258da4a8
*Dec 3 02:02:34:456 2014 H3C RIP/7/RIPDEBUG: Sequence: 8ad5ec5f (1340)
*Dec 3 02:02:34:456 2014 H3C RIP/7/RIPDEBUG: AFI 2, destination
10.0.0.0/255.255.255.0, nexthop 0.0.0.0, cost 1, tag 0
*Dec 3 02:02:34:456 2014 H3C RIP/7/RIPDEBUG: RIP 1 : Authentication fail - MD5
Checksum error.
*Dec 3 02:02:34:456 2014 H3C RIP/7/RIPDEBUG: RIP 1 : Ignored this packet.
Authentication validation failed.
*Dec 3 02:02:34:456 2014 H3C RIP/7/RIPDEBUG: RIP 1 : Failed to find receiving
interface for source address 10.0.0.1.
```

可以看到，因认证密码不一致，RTA 不能够学习到对端设备发来的路由。

此时再将 RTA 的密码改成与 RTB 的密码相同，来看路由器是否能正确交换路由信息。

配置 RTA:

```
[RTA-Serial3/0]rip authentication-mode md5 rfc2453 plain abcde
```

配置完成后，需要等待更新周期到来，RTA 收到 RTB 发出的路由更新后，再查看 RTA 上的路由表，如下：

```
[RTA-rip-1]display ip routing-table
```

```
Destinations : 18      Routes : 18

Destination/Mask    Proto   Pre  Cost           NextHop         Interface
0.0.0.0/32          Direct  0    0              127.0.0.1       InLoop0
10.0.0.0/24          RIP     100  1              192.168.1.2     Ser3/0
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
192.168.0.0/24          Direct  0    0              192.168.0.1     GE0/0
192.168.0.0/32          Direct  0    0              192.168.0.1     GE0/0
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     GE0/0
192.168.1.0/24          Direct  0    0              192.168.1.1     Ser3/0
192.168.1.0/32          Direct  0    0              192.168.1.1     Ser3/0
192.168.1.1/32          Direct  0    0              127.0.0.1       InLoop0
192.168.1.2/32          Direct  0    0              192.168.1.2     Ser3/0
192.168.1.255/32      Direct  0    0              192.168.1.1     Ser3/0
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，RTA 路由表中有了正确的路由 10.0.0.0/24。

再观察 RTA 收发协议报文的情况：

```
<RTA>
```

```
*Dec 3 02:05:58:490 2014 H3C RIP/7/RIPDEBUG: RIP 1 : Receiving response from
192.168.1.2 on Serial3/0
*Dec 3 02:05:58:490 2014 H3C RIP/7/RIPDEBUG: Packet: version 2, cmd response,
length 48
*Dec 3 02:05:58:491 2014 H3C RIP/7/RIPDEBUG: Authentication-mode: MD5 Digest:
521af24b.cd086740.9295b6e9.d04f82bb
*Dec 3 02:05:58:491 2014 H3C RIP/7/RIPDEBUG: Sequence: cd086740 (1542)
*Dec 3 02:05:58:491 2014 H3C RIP/7/RIPDEBUG: AFI 2, destination
10.0.0.0/255.255.255.0, nexthop 0.0.0.0, cost 1, tag 0
```

可以看到，RTA 能够正确的接收从 RTB 发出的路由更新。

11.5 实验中的命令列表

表11-4 IP 路由原理实验命令列表

命令	描述
rip [process-id]	创建RIP 进程并进入RIP 视图
network network-address [wildcard-mask]	在指定网段接口上使能RIP

命令	描述
version { 1 / 2 }	指定RIP版本
undo summary	取消路由自动聚合
rip authentication-mode { md5 { rfc2082 { cipher cipher-string plain plain-string } key-id rfc2453 { cipher cipher-string plain plain-string } } simple { cipher cipher-string plain plain-string } }	指定RIP认证方式和认证字
rip poison-reverse	在接口使能毒性逆转功能
undo rip split-horizon	在接口取消水平分割功能
display rip	显示指定RIP进程的当前运行状态及配置信息
terminal debugging	终端显示调试信息
debugging rip 1 packet	查看RIP协议收发报文的情况

11.6 思考题

1. 上述实验中，路由器不再收到路由更新后 180 秒才能将此路由从 IP 路由表中撤销。能否将此时间缩短？

答：可以将老化定时器设置为一个较小的值，缩短路由的老化时间，加快网络收敛。例如，配置老化定时器到 60 秒：

```
[RTA-rip-1] timers timeout 60
```

2. 上述 RIP 认证实验中，RTA 上查看收发 RIP 协议报文时，看不到所配置的密码，为什么？

答：实验中所配置的认证为 MD5 密文认证。如果配置了明文认证，则可以在收发协议报文中看到密码。但明文认证的安全性不如 MD5 密文认证。

实验12 配置 OSPF

12.1 实验内容与目标

完成本实验，您应该能够：

- 掌握单区域 OSPF 配置方法
- 掌握 OSPF 优先级的配置方法
- 掌握 OSPF Cost 的配置方法
- 掌握 OSPF 路由选择的方法
- 掌握多区域 OSPF 的配置方法

12.2 预备知识和技能

掌握 OSPF 的工作原理，熟悉 OSPF 的基本配置命令。

12.3 实验组网图

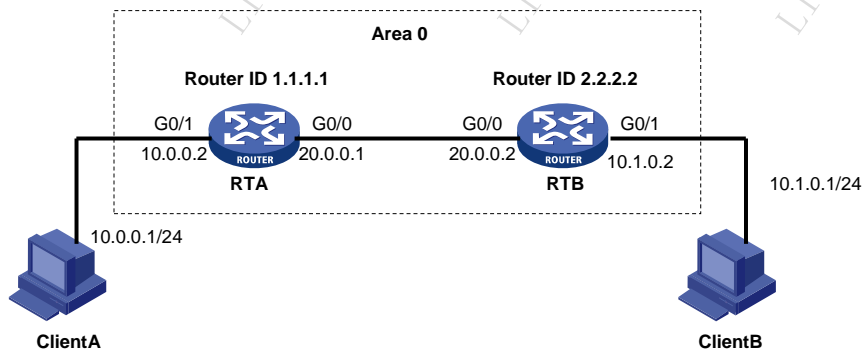


图12-1 实验任务一环境图

实验任务一组网如图 12-1 所示。本组网模拟单区域 OSPF 的应用。RTA 和 RTB 分别是客户端 ClientA 和 ClientB 的网关。RTA 设置 loopback 口地址 1.1.1.1 为 RTA 的 Router ID，RTB 设置 loopback 口地址 2.2.2.2 为 RTB 的 Router ID，RTA 和 RTB 都属于同一个 OSPF 区域 0。RTA 和 RTB 之间的网络能互通，客户端 ClientA 和 ClientB 能互通。

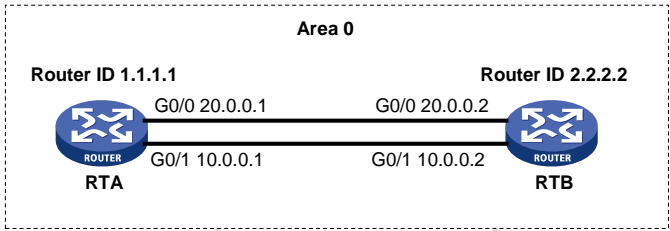


图12-2 实验任务二环境图

实验任务二组网如图 12-2 所示，由 2 台 MSR3020（RTA、RTB）路由器组成。本组网模拟实际组网中 OSPF 的路由选择。RTA 设置 loopback 口地址 1.1.1.1 为 RTA 的 Router ID，RTB 设置 loopback 口地址 2.2.2.2 为 RTB 的 Router ID，RTA 和 RTB 都属于同一个 OSPF 区域 0。RTA 和 RTB 之间有两条链路连接。

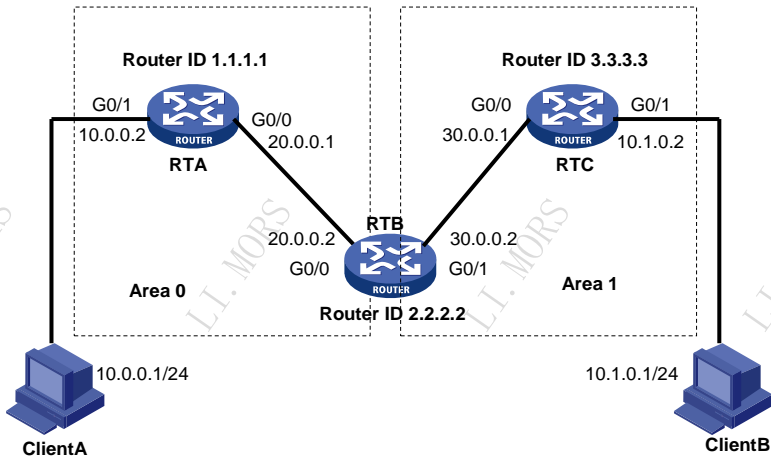


图12-3 实验任务三环境图

实验任务三组网如图 12-3 所示，由 3 台 MSR3020（RTA、RTB、RTC）路由器、2 台 PC（ClientA、ClientB）组成。本组网模拟实际组网中多区域 OSPF 的应用。RTA 和 RTC 分别是客户端 ClientA 和 ClientB 的网关。RTA 设置 loopback 口地址 1.1.1.1 为 RTA 的 Router ID，RTB 设置 loopback 口地址 2.2.2.2 为 RTB 的 Router ID，RTC 设置 loopback 口地址 3.3.3.3 为 RTC 的 Router ID。RTA 和 RTB 的 G0/0 口属于同一个 OSPF 区域 0，RTB 的 G0/1 口和 RTC 属于同一个 OSPF 区域 1。RTA、RTB 和 RTC 之间的网络能互通，客户端 ClientA 和 ClientB 能互通。

12.4 实验设备与版本

本实验所需之主要设备器材如表 12-1 所示。

表12-1 设备列表

名称和型号	版本	数量	描述
-------	----	----	----

MSR3620	CMW7.1.049-R0106P18	3	路由器
PC	Windows XP SP2	3	主机
第5类UTP以太网连接线		3	直通线

12.5 实验过程

实验任务一：单区域 OSPF 基本配置

步骤一：搭建实验环境

首先，依照图 12-1 搭建实验环境。配置客户端 ClientA 的 IP 地址为 10.0.0.1/24，网关为 10.0.0.2；配置客户端 ClientB 的 IP 地址为 10.1.0.1/24，网关为 10.1.0.2。

步骤二：基本配置

在路由器上完成接口 IP 地址等基本配置。

```
[RTA]interface G0/0
[RTA-GigabitEthernet0/0]ip address 20.0.0.1 24
[RTA-GigabitEthernet0/0]interface G0/1
[RTA-GigabitEthernet0/1]ip address 10.0.0.2 24
[RTA-GigabitEthernet0/1]interface loopback 0
[RTA-Loopback0]ip address 1.1.1.1 32

[RTB]interface G0/0
[RTB-GigabitEthernet0/0]ip address 20.0.0.2 24
[RTB-GigabitEthernet0/0]interface G0/1
[RTB-GigabitEthernet0/1]ip address 10.1.0.2 24
[RTB-GigabitEthernet0/1]interface loopback 0
[RTB-Loopback0]ip address 2.2.2.2 32
```

步骤三：检查网络连通性和路由器路由表

在 ClientA 上 ping ClientB(IP 地址为 10.1.0.1)，显示如下：

```
C:\>ping 10.1.0.1

Pinging 10.1.0.1 with 32 bytes of data:

From 10.0.0.2 : Destination Net Unreachable
From 10.0.0.2 : Destination Net Unreachable
From 10.0.0.2 : Destination Net Unreachable
From 10.0.0.2 : Destination Net Unreachable
From 10.0.0.2 : Destination Net Unreachable

Ping statistics for 10.1.0.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

结果显示，从 ClientA 无法 ping 通 ClientB。这是因为在 RTA 上没有到 10.1.0.1 的路由。

在 RTA 上使用 display ip routing-table 查看 RTA 的路由表，显示如下：

```
[RTA]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
1.1.1.1/32          Direct  0    0          127.0.0.1       InLoop0
```

10.0.0.0/24	Direct	0	0	10.0.0.2	GE0/1
10.0.0.0/32	Direct	0	0	10.0.0.2	GE0/1
10.0.0.2/32	Direct	0	0	127.0.0.1	InLoop0
10.0.0.255/32	Direct	0	0	10.0.0.2	GE0/1
20.0.0.0/24	Direct	0	0	20.0.0.1	GE0/0
20.0.0.0/32	Direct	0	0	20.0.0.1	GE0/0
20.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
20.0.0.255/32	Direct	0	0	20.0.0.1	GE0/0
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
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

RTA 上只有直连路由，没有到达 ClientB 的路由表，故从 ClientA 上来的数据报文无法转发给 ClientB。

在 RTB 上也执行以上的操作，查看相关信息。

步骤四：配置 OSPF

在 RTA 上配置 OSPF：

```
[RTA]router id 1.1.1.1
[RTA]ospf 1
[RTA-ospf-1]area 0.0.0.0
[RTA-ospf-1-area-0.0.0.0]network 1.1.1.1 0.0.0.0
[RTA-ospf-1-area-0.0.0.0]network 10.0.0.0 0.0.0.255
[RTA-ospf-1-area-0.0.0.0]network 20.0.0.0 0.0.0.255
```

在 RTB 上配置 OSPF：

```
[RTB]router id 2.2.2.2
[RTB]ospf 1
[RTB-ospf-1]area 0.0.0.0
[RTB-ospf-1-area-0.0.0.0]network 2.2.2.2 0.0.0.0
[RTB-ospf-1-area-0.0.0.0]network 10.1.0.0 0.0.0.255
[RTB-ospf-1-area-0.0.0.0]network 20.0.0.0 0.0.0.255
```

步骤五：检查路由器 OSPF 邻居状态及路由表

在 RTA 上使用 display ospf peer 查看路由器 OSPF 邻居状态，显示如下：

```
[RTA]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        20.0.0.2         1   32           Full/DR        GE0/0
```

RTA 与 Router ID 为 2.2.2.2（RTB）的路由器上配置 IP 地址 20.0.0.2 的接口互为邻居，RTB 的配置 IP 地址 20.0.0.2 的接口为该网段的 DR 路由器。此时，邻居状态达到 Full，说明 RTA 和 RTB 之间的链路状态数据库已经同步，RTA 具备到达 RTB 的路由信息。

在 RTA 上使用 display ospf routing 查看路由器的 OSPF 路由表，显示如下：

```
[RTA]display ospf routing

      OSPF Process 1 with Router ID 1.1.1.1
      Routing Table

Routing for network
Destination      Cost      Type      NextHop      AdvRouter      Area
20.0.0.0/24      1          Transit  0.0.0.0      2.2.2.2        0.0.0.0
10.0.0.0/24      1          Stub     0.0.0.0      1.1.1.1        0.0.0.0
2.2.2.2/32       1          Stub     20.0.0.2     2.2.2.2        0.0.0.0
10.1.0.0/24      2          Stub     20.0.0.2     2.2.2.2        0.0.0.0
1.1.1.1/32       0          Stub     0.0.0.0      1.1.1.1        0.0.0.0

Total nets: 5
Intra area: 5  Inter area: 0  ASE: 0  NSSA: 0
```

在 RTA 上使用 `display ip routing-table` 查看路由器全局路由表，显示如下：

```
[RTA]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
1.1.1.1/32        Direct 0  0      127.0.0.1    InLoop0
2.2.2.2/32        O_INTRA 10 1      20.0.0.2     GE0/0
10.0.0.0/24       Direct 0  0      10.0.0.2     GE0/1
10.0.0.0/32       Direct 0  0      10.0.0.2     GE0/1
10.0.0.2/32       Direct 0  0      127.0.0.1    InLoop0
10.0.0.255/32     Direct 0  0      10.0.0.2     GE0/1
10.1.0.0/24       O_INTRA 10 2      20.0.0.2     GE0/0
20.0.0.0/24       Direct 0  0      20.0.0.1     GE0/0
20.0.0.0/32       Direct 0  0      20.0.0.1     GE0/0
20.0.0.1/32       Direct 0  0      127.0.0.1    InLoop0
20.0.0.255/32     Direct 0  0      20.0.0.1     GE0/0
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
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
```

RTA 路由器全局路由表里加入了到达 RTB 的 2.2.2.2/32 和 10.1.0.0/24 网段的路由。

在 RTB 上也执行以上的操作，查看相关信息。

步骤六：检查网络连通性

在 ClientA 上 ping ClientB(IP 地址为 10.1.0.1)，显示如下：

```
C:\>ping 10.1.0.1

Pinging 10.1.0.1 with 32 bytes of data:

Reply from 10.1.0.1: bytes=32 time=1ms TTL=126
Reply from 10.1.0.1: bytes=32 time=1ms TTL=126
Reply from 10.1.0.1: bytes=32 time=1ms TTL=126
Reply from 10.1.0.1: bytes=32 time=1ms TTL=126

Ping statistics for 10.1.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

在 ClientB 上 ping ClientA(IP 地址为 10.0.0.1), 显示如下:

```
C:\>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:

Reply from 10.0.0.1: bytes=32 time=1ms TTL=126
Reply from 10.0.0.1: bytes=32 time=1ms TTL=126
Reply from 10.0.0.1: bytes=32 time=1ms TTL=126
Reply from 10.0.0.1: bytes=32 time=1ms TTL=126

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

实验任务二：单区域 OSPF 增强配置

步骤一：搭建实验环境

首先，依照图 12-2 搭建实验环境。

步骤二：基本配置

在路由器上完成接口 IP 地址、OSPF 等基本配置。

```
[RTA]interface G0/0
[RTA-GigabitEthernet0/0]ip address 20.0.0.1 24
[RTA-GigabitEthernet0/0]interface G0/1
[RTA-GigabitEthernet0/1]ip address 10.0.0.1 24
[RTA-GigabitEthernet0/1]interface loopback 0
[RTA-Loopback0]ip address 1.1.1.1 32
[RTA-Loopback0]quit
[RTA]router id 1.1.1.1
[RTA]ospf 1
[RTA-ospf-1]area 0.0.0.0
[RTA-ospf-1-area-0.0.0.0]network 1.1.1.1 0.0.0.0
[RTA-ospf-1-area-0.0.0.0]network 10.0.0.0 0.0.0.255
[RTA-ospf-1-area-0.0.0.0]network 20.0.0.0 0.0.0.255
```

```
[RTB]interface G0/0
[RTB-GigabitEthernet0/0]ip address 20.0.0.2 24
[RTB-GigabitEthernet0/0]interface G0/1
[RTB-GigabitEthernet0/1]ip address 10.0.0.2 24
[RTB-GigabitEthernet0/1]interface loopback 0
[RTB-Loopback0]ip address 2.2.2.2 32
[RTB-Loopback0]quit
[RTB]router id 2.2.2.2
[RTB]ospf 1
[RTB-ospf-1]area 0.0.0.0
[RTB-ospf-1-area-0.0.0.0]network 2.2.2.2 0.0.0.0
[RTB-ospf-1-area-0.0.0.0]network 10.0.0.0 0.0.0.255
[RTB-ospf-1-area-0.0.0.0]network 20.0.0.0 0.0.0.255
```

步骤三：检查路由器 OSPF 邻居状态及路由表

在 RTA 上使用 display ospf peer 查看路由器 OSPF 邻居状态，显示如下：

```
[RTA]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     20.0.0.2    1 38      Full/DR    GE0/0
2.2.2.2     10.0.0.2    1 34      Full/DR    GE0/1
```

RTA 与 Router ID 为 2.2.2.2 (RTB) 的路由器建立了两个邻居，RTA 的 G0/0 接口与 RTB 配置 IP 地址 20.0.0.2 的接口建立一个邻居，该邻居所在的网段为 20.0.0.0/24，RTB 配置 IP 地址 20.0.0.2 的接口为该网段的 DR 路由器；另外，RTA 的 G0/1 接口与 RTB 配置的 IP 地址 10.0.0.2 的接口建立一个邻居，该邻居所在的网段为 10.0.0.0/24，RTB 配置 IP 地址 10.0.0.2 的接口为该网段的 DR 路由器。

在 RTA 上使用 `display ospf routing` 查看路由器 OSPF 路由表，显示如下：

```
[RTA]display ospf routing

OSPF Process 1 with Router ID 1.1.1.1
Routing Table

Routing for network
Destination      Cost      Type      NextHop      AdvRouter      Area
20.0.0.0/24      1          Transit   0.0.0.0      2.2.2.2        0.0.0.0
10.0.0.0/24      1          Transit   0.0.0.0      2.2.2.2        0.0.0.0
2.2.2.2/32       1          Stub      10.0.0.2     2.2.2.2        0.0.0.0
2.2.2.2/32       1          Stub      20.0.0.2     2.2.2.2        0.0.0.0
1.1.1.1/32       0          Stub      0.0.0.0      1.1.1.1        0.0.0.0

Total nets: 5
Intra area: 5  Inter area: 0  ASE: 0  NSSA: 0
```

在 RTA 的 OSPF 路由表上有两条到达 RTB 的 2.2.2.2/32 网段的路由，一条是邻居 20.0.0.2 发布的，另一条是邻居 10.0.0.2 发布的，这两条路由的 Cost 相同。

在 RTA 上使用 `display ip routing-table` 查看路由器全局路由表，显示如下：

```
[RTA]display ip routing-table

Destinations : 18      Routes : 19

Destination/Mask  Proto  Pre Cost      NextHop      Interface
0.0.0.0/32        Direct 0 0          127.0.0.1    InLoop0
1.1.1.1/32        Direct 0 0          127.0.0.1    InLoop0
2.2.2.2/32        O_INTRA 10 1          10.0.0.2     GE0/1
                  20.0.0.2     GE0/0
10.0.0.0/24       Direct 0 0          10.0.0.1     GE0/1
10.0.0.0/32       Direct 0 0          10.0.0.1     GE0/1
10.0.0.1/32       Direct 0 0          127.0.0.1    InLoop0
10.0.0.255/32     Direct 0 0          10.0.0.1     GE0/1
20.0.0.0/24       Direct 0 0          20.0.0.1     GE0/0
20.0.0.0/32       Direct 0 0          20.0.0.1     GE0/0
20.0.0.1/32       Direct 0 0          127.0.0.1    InLoop0
20.0.0.255/32     Direct 0 0          20.0.0.1     GE0/0
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
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
```

在 RTA 路由器全局路由表内，有两条到达 RTB 的 2.2.2.2/32 网段的等价 OSPF 路由。在 RTB 上也执行以上的操作，查看相关信息。

步骤四：修改路由器接口开销

在 RTA 的 G0/0 接口上增加配置 `ospf cost 150`。

```
[RTA]interface G0/0
[RTA-GigabitEthernet0/0]ospf cost 150
```

步骤五：检查路由器路由表

在 RTA 上使用命令 `display ospf routing` 查看路由器 OSPF 路由表，显示如下：

```
[RTA]display ospf routing

OSPF Process 1 with Router ID 1.1.1.1
Routing Table

Routing for network
Destination      Cost      Type      NextHop      AdvRouter      Area
20.0.0.0/24      150       Transit  0.0.0.0      2.2.2.2        0.0.0.0
10.0.0.0/24      1         Transit  0.0.0.0      2.2.2.2        0.0.0.0
2.2.2.2/32       1         Stub    10.0.0.2     2.2.2.2        0.0.0.0
1.1.1.1/32       0         Stub    0.0.0.0      1.1.1.1        0.0.0.0

Total nets: 4
Intra area: 4  Inter area: 0  ASE: 0  NSSA: 0
```

由于 RTA 的 G0/0 接口的开销配置为 150，远高于 G0/1 接口的开销，故在 RTA 的 OSPF 路由表上仅有一条由邻居 10.0.0.2（该邻居与 RTA 的 G0/1 接口连接）发布的到达 RTB 的 2.2.2.2/32 网段的路由。

在 RTA 上使用 `display ip routing-table` 查看路由器全局路由表，显示如下：

```
[RTA-GigabitEthernet0/0]display ip routing-table

Destinations : 18      Routes : 18

Destination/Mask  Proto  Pre Cost      NextHop      Interface
0.0.0.0/32        Direct 0  0      127.0.0.1    InLoop0
1.1.1.1/32        Direct 0  0      127.0.0.1    InLoop0
2.2.2.2/32        O_INTRA 10 1      10.0.0.2     GE0/1
10.0.0.0/24       Direct 0  0      10.0.0.1     GE0/1
10.0.0.0/32       Direct 0  0      10.0.0.1     GE0/1
10.0.0.1/32       Direct 0  0      127.0.0.1    InLoop0
10.0.0.255/32     Direct 0  0      10.0.0.1     GE0/1
20.0.0.0/24       Direct 0  0      20.0.0.1     GE0/0
20.0.0.0/32       Direct 0  0      20.0.0.1     GE0/0
20.0.0.1/32       Direct 0  0      127.0.0.1    InLoop0
20.0.0.255/32     Direct 0  0      20.0.0.1     GE0/0
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
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
```

在 RTA 路由器全局路由表内，仅有一条通过 G0/1 到达 RTB 的 2.2.2.2/32 网段的路由。

在 RTB 上也执行以上的操作，查看相关信息。

步骤六：修改路由器接口优先级

在 RTB 的 G0/0 上修改接口优先级为 0。

```
[RTB]interface G0/0
[RTB-GigabitEthernet0/0]ospf dr-priority 0
```

步骤七：在路由器上重启 OSPF 进程

先将 RTB 的 OSPF 进程重启，再将 RTA 的 OSPF 进程重启。

```
<RTB>reset ospf 1 process
Warning : Reset OSPF process? [Y/N]:y
```

```
<RTA>reset ospf 1 process
Warning : Reset OSPF process? [Y/N]:y
```

步骤八：在路由器 OSPF 邻居状态

在 RTA 上使用 **display ospf peer** 查看路由器 OSPF 邻居状态，显示如下：

```
[RTA]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        20.0.0.2         0   39           Full/DROther   GE0/0
2.2.2.2        10.0.0.2         1   38           Full/DR        GE0/1
```

由于 RTB 的 G0/0 接口的 dr 优先级为 0，不具备 DR/BDR 选举权，故后启动 OSPF 的 RTA 接口 G0/0 成为该网段的 DR 路由器，RTB 的 G0/0 变为 DROther 路由器。

在 RTB 上也执行以上的操作，查看相关信息。

实验任务三：多区域 OSPF 基本配置**步骤一：搭建实验环境**

首先，依照图 12-3 搭建实验环境。配置客户端 ClientA 的 IP 地址为 10.0.0.1/24，网关为 10.0.0.2；配置客户端 ClientB 的 IP 地址为 10.1.0.1/24，网关为 10.1.0.2。

步骤二：基本配置

在路由器上完成接口 IP 地址、OSPF 基本配置。

```
[RTA]interface G0/0
[RTA-GigabitEthernet0/0]ip address 20.0.0.1 24
[RTA-GigabitEthernet0/0]interface G0/1
[RTA-GigabitEthernet0/1]ip address 10.0.0.1 24
[RTA-GigabitEthernet0/1]interface loopback 0
[RTA-Loopback0]ip address 1.1.1.1 32
[RTA-Loopback0]quit
[RTA]router id 1.1.1.1
[RTA]ospf 1
[RTA-ospf-1]area 0.0.0.0
[RTA-ospf-1-area-0.0.0.0]network 1.1.1.1 0.0.0.0
[RTA-ospf-1-area-0.0.0.0]network 10.0.0.0 0.0.0.255
[RTA-ospf-1-area-0.0.0.0]network 20.0.0.0 0.0.0.255
```

```
[RTB]interface G0/0
[RTB-GigabitEthernet0/0]ip address 20.0.0.2 24
[RTB-GigabitEthernet0/0]interface G0/1
[RTB-GigabitEthernet0/1]ip address 30.0.0.2 24
[RTB-GigabitEthernet0/1]interface loopback 0
[RTB-Loopback0]ip address 2.2.2.2 32
[RTB-Loopback0]quit
[RTB]router id 2.2.2.2
```

```

[RTB]ospf 1
[RTB-ospf-1]area 0.0.0.0
[RTB-ospf-1-area-0.0.0.0]network 2.2.2.2 0.0.0.0
[RTB-ospf-1-area-0.0.0.0]network 20.0.0.0 0.0.0.255
[RTB-ospf-1-area-0.0.0.0]quit
[RTB-ospf-1-area]area 1
[RTB-ospf-1-area-0.0.0.1]network 30.0.0.0 0.0.0.255

[RTC]interface G0/0
[RTC-GigabitEthernet0/0]ip address 30.0.0.1 24
[RTC-GigabitEthernet0/0]interface G0/1
[RTC-GigabitEthernet0/1]ip address 10.1.0.2 24
[RTC-GigabitEthernet0/1]interface loopback 0
[RTC-Loopback0]ip address 3.3.3.3 32
[RTC-Loopback0]quit
[RTC]router id 3.3.3.3
[RTC]ospf 1
[RTC-ospf-1]area 1
[RTC-ospf-1-area-0.0.0.1]network 3.3.3.3 0.0.0.0
[RTC-ospf-1-area-0.0.0.1]network 10.1.0.0 0.0.0.255
[RTC-ospf-1-area-0.0.0.1]network 30.0.0.0 0.0.0.255

```

步骤三：检查路由器 OSPF 邻居状态及路由表

在 RTB 上使用 **display ospf peer** 查看路由器 OSPF 邻居状态，显示如下：

```

[RTB]display ospf peer

        OSPF Process 1 with Router ID 2.2.2.2
        Neighbor Brief Information

Area: 0.0.0.0
Router ID      Address          Pri Dead-Time  State          Interface
1.1.1.1        20.0.0.1         1   39           Full/DR        GE0/0

Area: 0.0.0.1
Router ID      Address          Pri Dead-Time  State          Interface
3.3.3.3        30.0.0.1         1   35           Full/DR        GE0/1

```

RTB 与 Router ID 为 1.1.1.1 (RTA) 的路由器在 Area 0.0.0.0 内，RTB 的 G0/0 接口与 RTA 配置 IP 地址为 20.0.0.1 的接口建立邻居关系，该邻居所在的网段为 20.0.0.0/24，RTA 配置 IP 地址为 20.0.0.1 的接口为该网段的 DR 路由器。

RTB 与 Router ID 为 3.3.3.3 (RTC) 的路由器在 Area 0.0.0.1 内，RTB 的 G0/1 接口与 RTC 配置 IP 地址为 30.0.0.1 的接口建立邻居关系，该邻居所在的网段为 30.0.0.0/24，RTC 配置 IP 地址为 30.0.0.1 的接口为该网段的 DR 路由器。

在 RTB 上使用 **display ospf routing** 查看路由器 OSPF 路由表，显示如下：

```

[RTB]display ospf routing

        OSPF Process 1 with Router ID 2.2.2.2
        Routing Table

Routing for network
Destination      Cost      Type      NextHop      AdvRouter      Area
20.0.0.0/24      1         Transit   0.0.0.0      1.1.1.1        0.0.0.0
10.0.0.0/24      2         Stub      20.0.0.1     1.1.1.1        0.0.0.0
3.3.3.3/32       1         Stub      30.0.0.1     3.3.3.3        0.0.0.1
2.2.2.2/32       0         Stub      0.0.0.0      2.2.2.2        0.0.0.0
10.1.0.0/24      2         Stub      30.0.0.1     3.3.3.3        0.0.0.1
30.0.0.0/24      1         Transit   0.0.0.0      3.3.3.3        0.0.0.1
1.1.1.1/32       1         Stub      20.0.0.1     1.1.1.1        0.0.0.0

```

```
Total nets: 7
Intra area: 7 Inter area: 0 ASE: 0 NSSA: 0
```

在 RTB 的 OSPF 路由表上有到达全部网络的路由。

在 RTB 上使用 `display ip routing-table` 查看路由器全局路由表，显示如下：

```
[RTB]display ip routing-table
```

```
Destinations : 21          Routes : 21
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
1.1.1.1/32	O_INTRA	10	1	20.0.0.1	GE0/0
2.2.2.2/32	Direct	0	0	127.0.0.1	InLoop0
3.3.3.3/32	O_INTRA	10	1	30.0.0.1	GE0/1
10.0.0.0/24	O_INTRA	10	2	20.0.0.1	GE0/0
10.1.0.0/24	O_INTRA	10	2	30.0.0.1	GE0/1
20.0.0.0/24	Direct	0	0	20.0.0.2	GE0/0
20.0.0.0/32	Direct	0	0	20.0.0.2	GE0/0
20.0.0.2/32	Direct	0	0	127.0.0.1	InLoop0
20.0.0.255/32	Direct	0	0	20.0.0.2	GE0/0
30.0.0.0/24	Direct	0	0	30.0.0.2	GE0/1
30.0.0.0/32	Direct	0	0	30.0.0.2	GE0/1
30.0.0.2/32	Direct	0	0	127.0.0.1	InLoop0
30.0.0.255/32	Direct	0	0	30.0.0.2	GE0/1
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
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

在 RTB 路由器全局路由表内，有到达全部网络的路由。

在 RTA、RTC 上也执行以上的操作，查看相关信息。

步骤四：检查网络连通性

在 ClientA 上 ping ClientB(IP 地址为 10.1.0.1)，显示如下：

```
C:\>ping 10.1.0.1
```

```
Pinging 10.1.0.1 with 32 bytes of data:
```

```
Reply from 10.1.0.1: bytes=32 time=1ms TTL=126
```

```
Reply from 10.1.0.1: bytes=32 time=1ms TTL=126
```

```
Reply from 10.1.0.1: bytes=32 time=1ms TTL=126
```

```
Reply from 10.1.0.1: bytes=32 time=1ms TTL=126
```

```
Ping statistics for 10.1.0.1:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

在 ClientB 上 ping ClientA(IP 地址为 10.0.0.1)，显示如下：

```
C:\>ping 10.0.0.1
```

```
Pinging 10.0.0.1 with 32 bytes of data:
```

```
Reply from 10.0.0.1: bytes=32 time=1ms TTL=126
```

```
Reply from 10.0.0.1: bytes=32 time=1ms TTL=126
```

```

Reply from 10.0.0.1: bytes=32 time=1ms TTL=126
Reply from 10.0.0.1: bytes=32 time=1ms TTL=126

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

```

12.6 实验中的命令列表

表12-2 OSPF 实验命令列表

命令	描述
router id <i>router-id</i>	配置router id
ospf <i>process-id</i>	启动OSPF进程
area <i>area-id</i>	配置区域
network <i>network ip-address wildcard-mask</i>	指定网段接口上启动OSPF
ospf dr-priority <i>priority</i>	配置OSPF接口优先级
ospf cost <i>value</i>	配置OSPF接口cost

12.7 思考题

1. 在本实验二的步骤四里修改了 RTA 的 G0/0 接口 cost 值，那么在步骤五里，如果在 RTB 上查看路由表，会有几条到达 RTA 的 1.1.1.1/32 网段的路由？为什么？

答：2 条等价路由，修改 RTA 的 G0/0 接口 cost 值，只能影响 RTA 到 RTB 的路由计算，不能影响 RTB 到 RTA 的路由计算。
2. 在 OSPF 区域内指定网段接口上启动 OSPF 时，是否必须包含 Router ID 的地址？为什么配置时往往会将 Router ID 的地址包含在内？

答：不需要。在 OSPF 区域内指定网段接口上启动 OSPF 时，配置 Router ID 地址其实是发布路由器的 loopback 接口地址。
3. 如何通过配置 OSPF 接口 cost 来实现路由器路由备份？

答：将备份接口的接口 cost 通过命令 `ospf cost` 配置为较大值，只有当主接口失效的情况下，OSPF 路由才会选择备份接口。

实验13 ACL 包过滤

13.1 实验内容与目标

完成本实验，您应该能够：

- 了解访问控制列表的简单工作原理
- 掌握访问控制列表的基本配置方法
- 掌握访问控制列表的常用配置命令

13.2 实验组网图

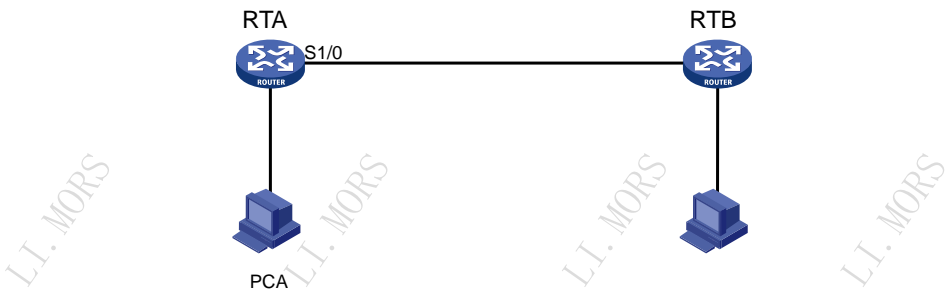


图13-1 访问控制列表实验图

13.3 实验设备与版本

本实验所需之主要设备器材如表 13-1 所示。

表13-1 实验设备列表

名称和型号	版本	数量	描述
MSR 36-20	CMW 7.1.049-R0106	2	
PC	Windows 7	2	安装有FTP服务器软件
V.35 DTE串口线	--	1	
V.35 DCE串口线	--	1	
第5类UTP以太网连接线	--	2	交叉线，路由器与PC机连接用

13.4 实验过程

实验任务一：配置基本 ACL

本实验任务主要是通过通过在路由器上实施基本 ACL 来禁止 PCA 访问本网段外的网络，使学员熟悉基本 ACL 的配置和作用。

步骤一：建立物理连接

按照图 13-1 进行连接，并检查路由器的软件版本及配置信息，确保路由器软件版本符合要求，所有配置为初始状态。如果配置不符合要求，请读者在用户模式下擦除设备中的配置文件，然后重启路由器以使系统采用缺省的配置参数进行初始化。

以上步骤可能会用到以下命令：

```
<RTA> display version
<RTA> reset saved-configuration
<RTA> reboot
```

步骤二：配置 IP 地址及路由

表13-2 IP 地址列表

设备名称	接口	IP 地址	网关
RTA	S1/0	192.168.1.1/24	--
	G0/0	192.168.0.1/24	--
RTB	S1/0	192.168.1.2/24	--
	G0/0	192.168.2.1/24	--
PCA	--	192.168.0.2/24	192.168.0.1
PCB	--	192.168.2.2/24	192.168.2.1

按表 13-2 所示在 PC 上配置 IP 地址和网关。配置完成后，在 Windows 操作系统的【开始】里选择【运行】，在弹出的窗口里输入 CMD，然后在【命令提示符】下用 ipconfig 命令来查看所配置的 IP 地址和网关是否正确。

按表 13-2 所示在路由器接口上配置 IP 地址。

配置 RTA:

```
[RTA-GigabitEthernet0/0]ip address 192.168.0.1 24
[RTA-Serial1/0]ip address 192.168.1.1 24
```

配置 RTB:

```
[RTB-GigabitEthernet0/0]ip address 192.168.2.1 24
[RTB-Serial1/0]ip address 192.168.1.2 24
```

学员可自己选择在路由器上配置静态路由或任一种动态路由，来达到全网互通。

例如，我们可以使用 RIP 协议，其配置如下：

配置 RTA:

```
[RTA]rip
```



```
[RTA-rip-1]network 192.168.0.0
[RTA-rip-1]network 192.168.1.0
```

配置 RTB:

```
[RTB]rip
[RTB-rip-1]network 192.168.1.0
[RTB-rip-1]network 192.168.2.0
```

配置完成后,请在 PCA 上通过 ping 命令来验证 PCA 与路由器、PCA 与 PCB 之间的可达性。应该是可达,如下:

```
C:\Documents and Settings\Administrator>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=20ms TTL=253
来自 192.168.2.2 的回复: 字节=32 时间=1ms TTL=253
来自 192.168.2.2 的回复: 字节=32 时间=1ms TTL=253
来自 192.168.2.2 的回复: 字节=32 时间=1ms TTL=253
```

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 = 20ms, 平均 = 5ms
```

如果不可达,请参考本教材相关章节来检查路由协议是否设置正确。

步骤三: ACL 应用规划

本实验的目的是使 PCA 不能访问本网段外的网络。请学员考虑如何在网络中应用 ACL 包过滤的相关问题:

- 需要使用何种 ACL?
- ACL 规则的动作是 deny 还是 permit?
- ACL 规则中的反掩码应该是什么?
- ACL 包过滤应该应用在路由器的哪个接口的哪个方向上?

下面是有关 ACL 规划的答案:

- 仅使用源 IP 地址就能够识别 PCA 发出的数据报文,因此使用基本 ACL 即可;
- 目的是要使 PCA 不能访问本网段外的网络,因此 ACL 规则的动作是 deny;
- 只需要限制从单台 PC 发出的报文,因此反掩码设置为 0.0.0.0;
- 因为需要禁止 PCA 访问本网段外的网络,所以可以在 RTA 连接 PCA 的接口 G0/0 上应用 ACL,方向为 Inbound。

步骤四: 配置基本 ACL 并应用

在路由器 RTA 上定义 ACL 如下:

```
[RTA]acl basic 2001
[RTA-acl-basic-2001]rule deny source 192.168.0.2 0.0.0.0
```

RTA 上包过滤防火墙功能默认开启,默认动作为 permit。

在 RTA 的 GigabitEthernet0/0 上应用 ACL:

```
[RTA-GigabitEthernet0/0]packet-filter 2001 inbound
```

步骤五：验证防火墙作用

在 PCA 上使用 ping 命令来测试从 PCA 到 PCB 的可达性，结果应该是不可达。如下：

```
C:\Documents and Settings\Administrator>ping 192.168.2.2
```

正在 Ping 192.168.2.2 具有 32 字节的数据：

请求超时。

请求超时。

请求超时。

请求超时。

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)，

同时，在 RTA 上通过命令行来查看 ACL 及包过滤防火墙的状态和统计：

```
[RTA]display acl 2001
Basic IPv4 ACL 2001, 1 rule,
ACL's step is 5
rule 0 deny source 192.168.0.2 0 (5 times matched)
```

可以看到，有数据报文命中了 ACL 中定义的规则。

```
[RTA]display packet-filter interface inbound
Interface: GigabitEthernet0/0
In-bound policy:
IPv4 ACL 2001
IPv4 default action: Permit
[RTA]display packet-filter statistics sum inbound 2001
Sum:
In-bound policy:
IPv4 ACL 2001
rule 0 deny source 192.168.0.2 0 (429 packets)
Totally 0 packets permitted, 429 packets denied
Totally 0% permitted, 100% denied
```

可以看到，路由器启用了包过滤防火墙功能，使用 ACL 2001 来匹配进入接口 GE0/0 的报文，过滤方向是 inbound。

实验任务二：配置高级 ACL

本实验任务是通过在路由器上实施高级 ACL 来禁止从 PCA 到网络 192.168.2.0/24 的 FTP 数据流，使学员熟悉高级 ACL 的配置和作用。

开始前，请清除设备上的 ACL 包过滤相关配置，即恢复到完成实验任务一的步骤二时的配置。

步骤一：ACL 应用规划

本实验的目的是禁止从 PCA 到网络 192.168.2.0/24 的 FTP 数据流，但允许其它数据流通过。请学员考虑如何在网络中应用 ACL 包过滤的相关问题：

- 需要使用何种 ACL？
- ACL 规则的动作是 deny 还是 permit？
- ACL 规则中的反掩码应该是什么？
- ACL 包过滤应该应用在路由器的哪个接口的哪个方向上？

下面是有关 ACL 规划的答案:

- 本实验目的是要禁止从 PCA 到网络 192.168.2.0/24 的 FTP 数据流。需要使用协议端口号来识别 PCA 发出的 FTP 数据报文, 因此必须使用高级 ACL;
- 本实验目的是要使 PC 之间不可达, 因此 ACL 规则的动作是 deny;
- 本实验中只需要限制从单台 PC 发出的到网络 192.168.2.0/24 的报文, 因此需要设置源 IP 地址反掩码为 0.0.0.0, 目的 IP 反掩码为 0.0.0.255;
- 因为需要禁止 PCA 发出的数据, 所以可以在 RTA 连接 PCA 的接口 G0/0 上应用 ACL, 方向为 inbound。

步骤二: 配置高级 ACL 并应用

在路由器 RTA 上定义 ACL 如下:

```
[RTA]acl advanced 3002
[RTA-acl-ipv4-adv-3002]rule deny tcp source 192.168.0.2 0.0.0.0 destination
192.168.2.1 0.0.0.255 destination-port eq ftp
[RTA-acl-ipv4-adv-3002]rule permit ip source 192.168.0.2 0.0.0.0 destination
192.168.2.0 0.0.0.255
```

RTA 上包过滤防火墙功能默认开启, 默认动作为 permit。

在 RTA 的 GigabitEthernet0/0 上应用 ACL:

```
[RTA-GigabitEthernet0/0]packet-filter 3002 inbound
```

步骤三: 验证防火墙作用

在 PCA 上使用 ping 命令来测试从 PCA 到 PCB 的可达性。结果应该是可达, 如下:

```
C:\Documents and Settings\Administrator>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=27ms TTL=253
来自 192.168.2.2 的回复: 字节=32 时间=1ms TTL=253
来自 192.168.2.2 的回复: 字节=32 时间=2ms TTL=253
来自 192.168.2.2 的回复: 字节=32 时间=1ms TTL=253
```

```
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 = 27ms, 平均 = 7ms
```

在 PCB 上开启 FTP 服务, 然后在 PCA 上使用 FTP 客户端软件连接到 PCB。结果应该是 FTP 未连接, 如下:

```
C:\Documents and Settings\Administrator>ftp 192.168.2.2
ftp> dir
未连接。
ftp>
```

同时, 在 RTA 上可以通过命令行来查看 ACL 及防火墙的状态和统计:

```
[RTA]display acl 3002
Advanced IPv4 ACL 3002, 2 rules,
ACL's step is 5
 rule 0 deny tcp source 192.168.0.2 0 destination 192.168.2.0 0.0.0.255
 destination-port eq ftp (12 times matched)
```

```
rule 5 permit ip source 192.168.0.2 0 destination 192.168.2.0 0.0.0.255 (2 times matched)
```

可以看到，分别有数据报文命中了 ACL 3002 的两个规则。

```
[RTA]display packet-filter interface inbound
Interface: GigabitEthernet0/0
In-bound policy:
  IPv4 ACL 3002
  IPv4 default action: Permit
[RTA]display packet-filter statistics sum inbound 3002
Sum:
In-bound policy:
  IPv4 ACL 3002
    rule 0 deny tcp source 192.168.0.2 0 destination 192.168.2.0 0.0.0.255
    destination-port eq ftp (9 packets)
    rule 5 permit ip source 192.168.0.2 0 destination 192.168.2.0 0.0.0.255
    Totally 0 packets permitted, 9 packets denied
    Totally 0% permitted, 100% denied
```

可以看到，路由器启用了包过滤防火墙功能，使用 ACL 3002 来匹配进入接口 GE0/0 的报文，过滤方向是 inbound。

13.5 实验中的命令列表

表13-3 使用 ACL 实验包过滤实验命令列表

命令	描述
packet-filter default deny	配置缺省过滤方式
packet-filter [ipv6 mac] { acl-number name acl-name } { inbound outbound }	配置接口的报文过滤功能
acl [ipv6] { advanced basic } { acl-number name acl-name } [match-order { auto config }]	创建ACL并进入相应ACL视图
rule [rule-id] { deny permit } [counting fragment logging source { object-group address-group-name source-address source-wildcard any } time-range time-range-name vpn-instance vpn-instance-name]	定义一个基本IPv4 ACL规则

命令	描述
rule [<i>rule-id</i>] { deny permit } protocol [{ { ack <i>ack-value</i> fin <i>fin-value</i> psh <i>psh-value</i> rst <i>rst-value</i> syn <i>syn-value</i> urg <i>urg-value</i> } established } counting destination { object-group <i>address-group-name</i> <i>dest-address</i> <i>dest-wildcard</i> any } destination-port { object-group <i>port-group-name</i> <i>operator port1</i> [<i>port2</i>] } { dscp <i>dscp</i> { precedence <i>precedence</i> tos <i>tos</i> } } fragment icmp-type { <i>icmp-type</i> [<i>icmp-code</i>] <i>icmp-message</i> } logging source { object-group <i>address-group-name</i> <i>source-address</i> <i>source-wildcard</i> any } source-port { object-group <i>port-group-name</i> <i>operator port1</i> [<i>port2</i>] } time-range <i>time-range-name</i> vpn-instance <i>vpn-instance-name</i>]	定义一个高级IPv4 ACL规则
display acl [<i>ipv6</i> <i>mac</i> <i>wlan</i>] { <i>acl-number</i> all name <i>acl-name</i> }	显示配置的ACL的信息
display packet-filter { interface [<i>interface-type</i> <i>interface-number</i>] [inbound outbound] zone-pair security [source <i>source-zone-name</i> destination <i>destination-zone-name</i>] }	查看包过滤防火墙的应用情况

13.6 思考题

列出要提出的思考题，或要提问的知识点。

1. 在实验任务一中，在配置 ACL 2001 的时候，最后是否需要配置如下一条允许其他所有报文的规则，为什么？

[RTA-acl-ipv4-basic-2001]rule permit source any

答：不需要，因为防火墙的缺省过滤方式是 Permit，也就意味着系统将转发没有命中 ACL 匹配规则的数据报文。

2. 在实验任务二中，可以把 ACL 应用在 RTB 上吗？

答：可以，起到的效果是一样的。但在 RTA 上应用可以减少不必要的流量处理与转发。

实验14 配置 NAT

14.1 实验内容与目标

完成本实验，您应该能够：

- 掌握 Basic NAT 的配置方法
- 掌握 NATPT 的配置方法
- 掌握 Easy IP 的配置方法
- 掌握 NAT Server 的配置方法

14.2 预备知识和技能

掌握 Basic NAT、NAPT 的工作原理，熟悉 NAT 的基本配置命令。

14.3 实验组网图

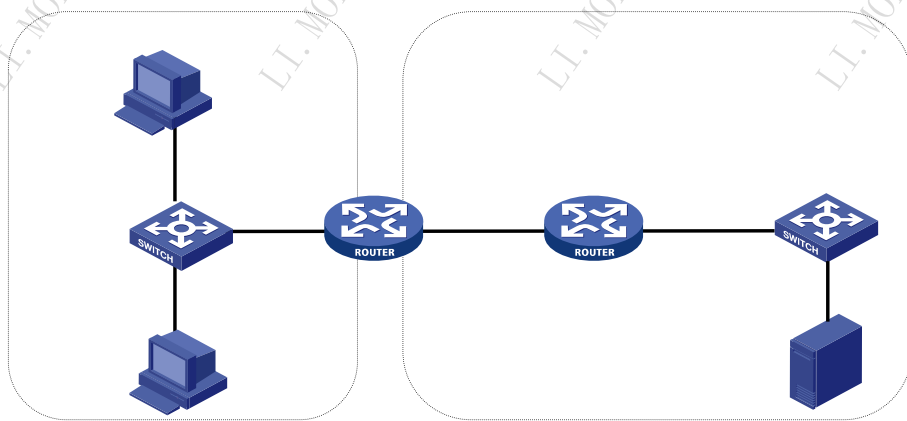


图14-1 NAT 实验环境图

实验组网如图 14-1 所示，由 2 台 MSR3620（RTA、RTB）路由器、2 台 S5820V2（SW1、SW2）交换机、3 台 PC（Client_A、Client_B、Server）组成，互连方式和 IP 地址分配参见图 14-1。

Client_A、Client_B 位于私网，网关为 RTA，RTA 同时为 NAT 设备，有 1 个私网接口（G0/0）和 1 个公网接口（G0/1），公网接口与公网路由器 RTB 互连。Server 位于公网，网关为 RTB。

本组网模拟了实际组网中涉及的几种 NAT 主要应用。Easy IP 配置最为简单，一般用于拨号接入互联网的场合；Basic NAT 不如 NAPT 普及；NAPT 可以提高公网 IP 的利用效率，适用于私网作为客户端访问公网服务器的场合；NAT Server 则用于私网需要对公网提供服务的场合。

14.4 实验设备与版本

本实验所需之主要设备器材如表 14-1 所示。

表14-1 设备列表

名称和型号	版本	数量	描述
MSR36-20	CMW 7.1.049-R0106	2	路由器
S5820V2	CMW 7.1.035-R2210	2	交换机
PC	Windows 7	3	主机
第5类UTP以太网连接线		6	直通线

14.5 实验过程

实验任务一：配置 Basic NAT

本实验中，私网客户端 Client_A、Client_B 需要访问公网服务器 Server，而 RTB 上不能保有私网路由，因此将在 RTA 上配置 Basic NAT，动态地为 Client_A、Client_B 分配公网地址。

步骤一：搭建实验环境

首先，依照图示搭建实验环境，完成路由器 RTA 与 RTB 的接口 IP 地址的配置。为了对去往 Server 的数据包提供路由，在私网出口路由器 RTA 上需要配置一条静态路由，指向公网路由器 RTB，下一跳为 RTB 的接口 G0/0。这时 RTA 应该能 ping 通 Server。配置主机 Client_A 的 IP 地址为 10.0.0.1/24，网关为 10.0.0.254；配置主机 Client_B 的 IP 地址为 10.0.0.2/24，网关为 10.0.0.254。

步骤二：基本配置

完成 IP 地址、路由等基本配置。

```
[RTA]interface GigabitEthernet 0/0
[RTA-GigabitEthernet0/0]ip address 10.0.0.254 24
[RTA]interface GigabitEthernet 0/1
[RTA-GigabitEthernet0/1]ip address 198.76.28.1 24
[RTA]ip route-static 0.0.0.0 0 198.76.28.2

[RTB]interface GigabitEthernet 0/0
[RTB-GigabitEthernet0/0]ip address 198.76.28.2 24
[RTB]interface GigabitEthernet 0/1
[RTB-GigabitEthernet0/1]ip address 198.76.29.1 24
```

步骤三：检查连通性

分别在 Client_A 和 Client_B 上 ping Server（IP 地址为 198.76.29.4）。显示如下：

```
C:\>ping 198.76.29.4
```

```
正在 Ping 198.76.29.4 具有 32 字节的数据：
请求超时。
请求超时。
请求超时。
```

请求超时。

198.76.29.4 的 Ping 统计信息：

数据包：已发送 = 4，已接收 = 0，丢失 = 4 (100% 丢失)，

结果显示，从 Client_A、Client_B 无法 ping 通 Server。这是因为在公网路由器上不可能有私网的路由，从 Server 回应的 ping 响应报文到 RTB 的路由表上无法找到 10.0.0.0 网段的路由。

步骤四：配置 Basic NAT

在 RTA 上配置 Basic NAT：

通过 acl 定义一条源地址属于 10.0.0.0/24 网段的流。

```
[RTA]acl basic 2000
[RTA-acl-ipv4-basic-2000]rule 0 permit source 10.0.0.0 0.0.0.255
```

配置 NAT 地址池 1，地址池中的用于地址转换的地址从 198.76.28.11 到 198.76.28.20 共 10 个。

```
[RTA]nat address-group 1
[RTA-address-group-1]address 198.76.28.11 198.76.28.20
```

进入接口模式视图：

```
[RTA]interface GigabitEthernet 0/1
```

将地址池 1 与 ACL 2000 关联，并在接口下发，方向为出方向。

```
[RTA-GigabitEthernet0/1]nat outbound 2000 address-group 1 no-pat
```

由配置可见，在 RTA 上配置了公网地址池 address-group 1，地址范围为 198.76.28.11～198.76.28.20。参数 no-pat 表示使用一对一的地址转换，只转换数据包的地址而不转换端口信息。此时路由器 RTA 会对该接口上出方向并且匹配 acl 2000 的流量做地址转换。

步骤五：检查连通性

从 Client_A、Client_B 分别 ping Server，能够 ping 通：

```
C:\>ping 198.76.29.4
```

正在 Ping 198.76.29.4 具有 32 字节的数据：

来自 198.76.29.4 的回复：字节=32 时间=46ms TTL=253

来自 198.76.29.4 的回复：字节=32 时间=1ms TTL=253

来自 198.76.29.4 的回复：字节=32 时间=1ms TTL=253

来自 198.76.29.4 的回复：字节=32 时间=1ms TTL=253

198.76.29.4 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 = 46ms，平均 = 12ms

步骤六：检查 NAT 表项

完成上一步骤后，立即在 RTA 上检查 NAT 表项：

```
<RTA>display nat session
Initiator:
Source      IP/port: 10.0.0.2/249
Destination IP/port: 198.76.29.4/2048
DS-Lite tunnel peer: -
```



```

VPN instance/VLAN ID/VLL ID: -/-/-
Protocol: ICMP(1)

Initiator:
Source      IP/port: 10.0.0.1/210
Destination IP/port: 198.76.29.4/2048
DS-Lite tunnel peer: -
VPN instance/VLAN ID/VLL ID: -/-/-
Protocol: ICMP(1)

Total sessions found: 2

<RTA>display nat no-pat
Local  IP: 10.0.0.1
Global IP: 198.76.28.12
Reversible: N
Type   : Outbound

Local  IP: 10.0.0.2
Global IP: 198.76.28.11
Reversible: N
Type   : Outbound

Total entries found: 2

```

从显示信息中可以看出，该 ICMP 报文的源地址 10.0.0.1 已经转换成公网地址 198.76.28.12，源端口号为 249，目的端口号为 2048。源地址 10.0.0.2 已经转换成公网地址 198.76.28.11，源端口号为 210，目的端口号为 2048。一分钟以后再次观察此表项，发现表中后两项消失了，四分钟以后再次观察，发现表项全部消失，显示如下：

```

<RTA>display nat session
Total sessions found: 0

```

这是因为 NAT 表项具有一定的老化时间（aging-time），一旦超过老化时间，NAT 会删除表项。可以通过命令 **display session aging-time state** 查看路由器会话的默认老化时间：

```

[RTA]display session aging-time state
State      Aging Time(s)
SYN        30
TCP-EST    3600
FIN        30
UDP-OPEN   30
UDP-READY  60
ICMP-REQUEST 60
ICMP-REPLY 30
RAWIP-OPEN 30
RAWIP-READY 60
UDPLITE-OPEN 30
UDPLITE-READY 60
DCCP-REQUEST 30
DCCP-EST   3600
DCCP-CLOSEREQ 30
SCTP-INIT  30
SCTP-EST   3600
SCTP-SHUTDOWN 30
ICMPV6-REQUEST 60
ICMPV6-REPLY 30

```

如有必要，还可以通过命令 **session aging-time** 对 NAT 会话各连接的老化时间进行修改。

除此之外，还可以观察 NAT 的调试信息，显示如下：

```

<RTA>terminal monitor
The current terminal is enabled to display logs.
<RTA>terminal debugging
The current terminal is enabled to display debugging logs.
<RTA>debugging nat packet
<RTA> *Nov 13 10:05:09:565 2014 RTA NAT/7/COMMON:
  PACKET: (GigabitEthernet0/0-out) Protocol: ICMP
           10.0.0.1:    0 -    198.76.29.4:    0(VPN:    0) ----->
           198.76.28.14: 0 -    198.76.29.4:    0(VPN:    0)

```

上述调试信息中的转换信息表明：在 GigabitEthernet0/0-out 方向，ICMP 报文的源地址 10.0.0.1 转换成 198.76.28.14。

注意：

虽然理论上每个 IP 地址有 65535 个端口，除去协议已占用和保留端口外，实际可用于地址转换的端口远少于理论值。

步骤七：恢复配置

在 RTA 上删除 Basic NAT 相关配置。

删除 NAT 地址池。

```
[RTA]undo nat address-group 1
```

在接口下删除 NAT 绑定。

```

[RTA]interface GigabitEthernet 0/1
[RTA-GigabitEthernet0/1]undo nat outbound 2000

```

实验任务二：NAPT 配置

私网客户端 Client_A、Client_B 需要访问公网服务器 Server，但由于公网地址有限，在 RTA 上配置的公网地址池范围为 198.76.28.11~198.76.28.11，因此配置 NAPT，动态地为 Client_A、Client_B 分配公网地址和协议端口。

步骤一：搭建实验环境

搭建实验环境，如同实验任务一中的步骤一和步骤二。

步骤二：检查连通性

从 Client_A、Client_B ping Server（IP 地址为 198.76.29.4），显示如下：

```
C:\>ping 198.76.29.4
```

```

正在 Ping 198.76.29.4 具有 32 字节的数据：
请求超时。
请求超时。
请求超时。
请求超时。

```

```
198.76.29.4 的 Ping 统计信息：
```

```
数据包：已发送 = 4，已接收 = 0，丢失 = 4 (100% 丢失)，
```

结果显示，从 Client_A、Client_B 无法 ping 通 Server。

步骤三：配置 NAPT

在 RTA 上完成 NAPT 相关配置：

通过 acl 定义一条源地址属于 10.0.0.0/24 网段的流。

```
[RTA]acl basic 2000
[RTA-acl-ipv4-basic-2000]rule 0 permit source 10.0.0.0 0.0.0.255
```

配置 NAT 地址池 1，地址池中只放入一个地址 198.76.28.11。

```
[RTA]nat address-group 1
[RTA-address-group-1]address 198.76.28.11 198.76.28.11
```

在接口视图下将 NAT 地址池与 acl 2000 绑定并下发。

```
[RTA]interface GigabitEthernet 0/1
[RTA-GigabitEthernet0/1]nat outbound 2000 address-group 1
```

此时未携带 **no-pat** 关键字，意味着 NAT 要对数据包进行端口的转换。

步骤四：检查连通性

从 Client_A、Client_B 上分别 ping Server，能够 ping 通：

```
C:\>ping 198.76.29.4
```

正在 Ping 198.76.29.4 具有 32 字节的数据：

来自 198.76.29.4 的回复： 字节=32 时间=46ms TTL=253

来自 198.76.29.4 的回复： 字节=32 时间=1ms TTL=253

来自 198.76.29.4 的回复： 字节=32 时间=1ms TTL=253

来自 198.76.29.4 的回复： 字节=32 时间=1ms TTL=253

198.76.29.4 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 = 46ms，平均 = 12ms

步骤五：检查 NAT 表项

完成上一步骤后，立即在 RTA 上检查 NAT 表项：

```
[RTA]display nat session verbose
Initiator:
  Source      IP/port: 10.0.0.1/247
  Destination IP/port: 198.76.29.4/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: ICMP(1)
Responder:
  Source      IP/port: 198.76.29.4/2
  Destination IP/port: 198.76.28.11/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: ICMP(1)
State: ICMP_REPLY
Application: OTHER
Start time: 2014-11-13 10:19:04 TTL: 15s
Interface(in) : GigabitEthernet0/0
Interface(out): GigabitEthernet0/1
Initiator->Responder:          5 packets          420 bytes
Responder->Initiator:          5 packets          420 bytes

Initiator:
  Source      IP/port: 10.0.0.2/218
```

```

Destination IP/port: 198.76.29.4/2048
DS-Lite tunnel peer: -
VPN instance/VLAN ID/VLL ID: -/-/-
Protocol: ICMP(1)
Responder:
Source      IP/port: 198.76.29.4/3
Destination IP/port: 198.76.28.11/0
DS-Lite tunnel peer: -
VPN instance/VLAN ID/VLL ID: -/-/-
Protocol: ICMP(1)
State: ICMP_REPLY
Application: OTHER
Start time: 2014-11-13 10:19:09 TTL: 22s
Interface(in) : GigabitEthernet0/0
Interface(out): GigabitEthernet0/1
Initiator->Responder:          4 packets      336 bytes
Responder->Initiator:          4 packets      336 bytes

Total sessions found: 2

```

从表项中可以看到源地址 10.0.0.1 和 10.0.0.2 都转换成同一个公网地址 198.76.28.11，所不同的是转换后的端口，10.0.0.1 转换后的端口为 12289，10.0.0.2 转换后的端口为 12288。当 RTA 出接口收到目的地址为 198.76.28.11 的回程流量时，正是用当初转换时赋予的不同的端口来分辨该流量是转发给 10.0.0.1 还是 10.0.0.2。NAPT 正是靠这种方式，对数据包的 IP 层和传输层信息同时进行转换，显著地提高公有 IP 地址的利用效率。

步骤六：恢复配置

在 RTA 上删除 NAPT 相关配置：

```

[RTA]undo nat address-group 1
[RTA]interface G0/1
[RTA-GigabitEthernet0/1]undo nat outbound 2000

```

实验任务三：Easy IP 配置

私网客户端 Client_A、Client_B 需要访问公网服务器 Server，使用公网接口 IP 地址动态为 Client_A、Client_B 分配公网地址和协议端口。

步骤一：搭建实验环境

搭建实验环境，如同任务一中的步骤一和步骤二。

步骤二：检查连通性

从 Client_A、Client_B ping Server（IP 地址为 198.76.29.4），无法 ping 通。

步骤三：配置 Easy IP

在 RTA 上完成 Easy IP 相关配置：

通过 acl 定义一条源地址属于 10.0.0.0/24 网段的流。

```

[RTA]acl basic 2000
[RTA-acl-ipv4-basic-2000]rule 0 permit source 10.0.0.0 0.0.0.255

```

在接口视图下将 acl 2000 与接口关联下发 NAT。

```

[RTA]interface GigabitEthernet 0/1

```

```
[RTA-GigabitEthernet0/1]nat outbound 2000
```

步骤四：检查连通性

从 Client_A、Client_B 分别 ping Server，能够 ping 通。

步骤五：检查 NAT 表项

完成上一步骤后，立即在 RTA 上检查 NAT 表项。

```
[RTA]display nat session verbose
Initiator:
  Source      IP/port: 10.0.0.1/255
  Destination IP/port: 198.76.29.4/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: ICMP(1)
Responder:
  Source      IP/port: 198.76.29.4/2
  Destination IP/port: 198.76.28.1/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: ICMP(1)
State: ICMP_REPLY
Application: OTHER
Start time: 2014-11-13 10:24:56 TTL: 15s
Interface(in) : GigabitEthernet0/0
Interface(out): GigabitEthernet0/1
Initiator->Responder:      5 packets      420 bytes
Responder->Initiator:      5 packets      420 bytes

Initiator:
  Source      IP/port: 10.0.0.2/219
  Destination IP/port: 198.76.29.4/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: ICMP(1)
Responder:
  Source      IP/port: 198.76.29.4/3
  Destination IP/port: 198.76.28.1/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: ICMP(1)
State: ICMP_REPLY
Application: OTHER
Start time: 2014-11-13 10:24:59 TTL: 19s
Interface(in) : GigabitEthernet0/0
Interface(out): GigabitEthernet0/1
Initiator->Responder:      5 packets      420 bytes
Responder->Initiator:      5 packets      420 bytes

Total sessions found: 2

<RTA>display nat session

There are currently 2 NAT sessions:
```

Protocol	GlobalAddr	Port	InsideAddr	Port	DestAddr	Port
1	198.76.28.1	12290	10.0.0.1	1024	198.76.29.4	1024
VPN: 0,	status:	11,	TTL: 00:01:00,		Left: 00:00:29	
1	198.76.28.1	12289	10.0.0.2	512	198.76.29.4	512
VPN: 0,	status:	11,	TTL: 00:01:00,		Left: 00:00:26	

从显示信息中可以看到，源地址 10.0.0.1 和 10.0.0.2 都转换为 RTA 的出接口地址 198.76.28.1。

请思考一个问题：在步骤四中，完成 NAT 配置后，从 Client_A 能够 ping 通 Server，但是如果从 Server 端 ping Client_A 呢？ping 命令结果显示如下：

```
C:\>ping 10.0.0.1
```

```
正在 Ping 10.0.0.1 具有 32 字节的数据：
```

```
请求超时。
```

```
请求超时。
```

```
请求超时。
```

```
请求超时。
```

```
10.0.0.1 的 Ping 统计信息：
```

```
数据包：已发送 = 4，已接收 = 0，丢失 = 4 (100% 丢失)，
```

结果显示 Server 不能 ping 通 Client_A。为什么呢？

仔细思考，不难发现在 RTA 上始终没有 10.0.0.0/24 网段的路由，所以 Server 直接 ping Client_A 是不可达的。而 Client_A 能 ping 通 Server 是因为，由 Server 回应的 ICMP 回程报文源地址是 Server 的地址 198.76.29.4，但是目的地址是 RTA 的出接口地址 198.76.28.1，而不是 Client_A 的实际源地址 10.0.0.1。也就是说这个 ICMP 连接必须是由 Client 端来发起连接，触发 RTA 做地址转换后转发。还记得我们在 RTA 出接口 Eth 0/1 下发 NAT 配置时的那个 outbound 吗？NAT 操作是在出方向使能有效。所以，如果从 Server 端始发 ICMP 报文 ping Client 端，是无法触发 RTA 做地址转换的。

那么，要想让 Server 端能够 ping 通 Client_A，应该怎么做呢？在实验任务四中，可以找到答案。

步骤六：恢复配置

在 RTA 上删除 Easy IP 相关配置。

```
[RTA]undo nat address-group 1
[RTA]interface GigabitEthernet 0/1
[RTA-GigabitEthernet0/1]undo nat outbound 2000
```

实验任务四：NAT Server 配置

Client_A 需要对外提供 ICMP 服务，在 RTA 上为 Client_A 静态映射公网地址和协议端口，公网地址为 198.76.28.11。

步骤一：检查连通性

从 Server ping Client_A 的私网地址 10.0.0.1，无法 ping 通。

步骤二：配置 NAT Server

在 RTA 上完成 NAT Server 相关配置。

```
[RTB]interface GigabitEthernet 0/1
```

在出接口上将私网服务器地址和公网地址做一对一 NAT 映射。

```
[RTB-GigabitEthernet0/1]nat server protocol icmp global 198.76.28.11 inside
10.0.0.1
```

步骤三：检查连通性

从 Server 主动 ping Client_A 的公网地址 198.76.28.11，能够 ping 通。

```
C:\>ping 198.76.28.11
Pinging 198.76.28.11 with 32 bytes of data:

Reply from 198.76.28.11: bytes=32 time=1ms TTL=126
Reply from 198.76.28.11: bytes=32 time=1ms TTL=126
Reply from 198.76.28.11: bytes=32 time=1ms TTL=126
Reply from 198.76.28.11: bytes=32 time=1ms TTL=126

Ping statistics for 198.76.28.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

步骤四：检查 NAT 表项

在 RTA 上检查 NAT Server 表项。

```
[RTA]display nat session verbose
Initiator:
  Source      IP/port: 198.76.29.4/236
  Destination IP/port: 198.76.28.11/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: ICMP(1)
Responder:
  Source      IP/port: 10.0.0.1/236
  Destination IP/port: 198.76.29.4/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/VLL ID: -/-/-
  Protocol: ICMP(1)
State: ICMP_REPLY
Application: OTHER
Start time: 2014-11-13 10:31:45 TTL: 26s
Interface(in) : GigabitEthernet0/1
Interface(out): GigabitEthernet0/0
Initiator->Responder:          5 packets          420 bytes
Responder->Initiator:          5 packets          420 bytes

Total sessions found: 1
[RTA]display nat server
Server in private network information:
  There are currently 1 internal servers
  Interface:GigabitEthernet0/1, Protocol:1(icmp),
    [global]    198.76.28.11:    ---- [local]    10.0.0.1:    ----
```

表项信息中显示出公网地址和私网地址的一对一的映射关系。

步骤五：恢复配置

在 RTA 上删除 NAT Server 相关配置。

```
[RTA]interface GigabitEthernet 0/1
[RTA-GigabitEthernet0/1]undo nat server protocol icmp global 198.76.28.11
```

NAT Server 特性就是为了满足公网客户端访问私网内部服务器的需求，将私网地址/端口静态映射成公网地址/端口，以供公网客户端访问。比如在实际应用中，客户的私有网络中的一

台 WEB 或 FTP 服务器需要对公网客户提供服务,这时需要使用 NAT Server 特性对外映射一个公网地址给自己的私网服务器。请思考,这时如果 Client_A 主动 ping Server 能否 ping 通? Client_B 能否 ping 通 Server? 为什么?

按照上面 RTA 中的 NAT Server 的配置命令,如果 Client_A 是一台 FTP 服务器,能否对外提供 FTP 服务?当然可以,只要修改 NAT Server 的相关配置。NAT Server 相关配置如下所示:

```
[RTB]interface GigabitEthernet 0/1
[RTB-GigabitEthernet0/1]nat server protocol tcp global 198.76.28.11 ftp inside
10.0.0.1 ftp
```

14.6 实验中的命令列表

表14-2 NAT 实验命令列表

命令	描述
nat address-group <i>group-number</i>	配置地址池
address <i>start-addr end-addr</i>	在地址池中加入地址
nat outbound <i>acl-number address-group</i> <i>group-number no-pat</i>	配置地址转换
nat server protocol <i>pro-type</i> global <i>global-addr [global-port] inside host-addr</i> <i>[host-port]</i>	配置 NAT Server
display nat session <i>[source { global</i> <i>global-address inside inside-address }]</i> <i>[destination dst-address]</i>	查看 NAT 会话信息

14.7 思考题

列出要提出的思考题,或要提问的知识点。

1. 在本实验中公网地址池使用公网接口地址段,如果使用其他地址段,需要在 RTB 上增加哪些配置?

答: 需要在 RTB 上添加指向公网地址池的静态路由。

2. **nat server** 命令中的 **global-address** 一定是 Internet 地址吗?

答: 不一定,其实 **global**、**inside** 是相对的,配置了 **nat server** 命令的接口所连接的网络就是 **global**。

实验15 配置 HDLC

15.1 实验内容与目标

完成本实验，您应该能够：

- 了解 HDLC 协议的基本原理
- 掌握 HDLC 的基本配置方法
- 掌握 HDLC 的常用配置命令

15.2 实验组网图

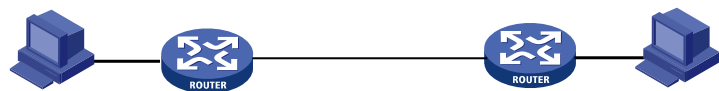


图15-1 HDLC 实验环境图

15.3 实验设备与版本

本实验所需之主要设备器材如表 15-1 所示。

表15-1 实验设备列表

名称和型号	版本	数量	描述
MSR 36-20	CMW 7.1.049-R0106	2	
PC	Windows 7	2	
V.35 DTE串口线	--	1	
V.35 DCE串口线	--	1	
第5类UTP以太网连接线	--	2	交叉线

15.4 实验过程

本实验中的 PC 以及路由器的 IP 地址规划如表 15-2 所示。

表15-2 IP 地址规划

设备	接口	IP 地址/掩码	备注
PCA	--	192.168.1.2/30	网关192.168.1.1
PCB	--	192.168.2.2/30	网关192.168.2.1
RTA	S1/0	10.1.1.1/30	
RTB	S1/0	10.1.1.2/30	

实验任务一：实现 PCA 与 PCB 的互通

在开始实验前，将路由器配置恢复到默认状态。

步骤一：依据规划，分别设置 PC 以及其对应网关的 IP 地址

步骤二：在路由器的广域网上配置 HDLC 协议封装以及对应的 IP 地址

在 RTA 路由器为 DCE 时的配置例示如下：

```
[RTA]interface Serial 1/0
[RTA-Serial1/0]link-protocol hdlc
[RTA-Serial1/0]baudrate 2048000
[RTA-Serial1/0]ip address 10.1.1.1 255.255.255.252
[RTB]interface Serial 1/0
[RTB-Serial1/0]link-protocol hdlc
[RTB-Serial1/0]ip address 10.1.1.2 255.255.255.252
```

说明：

baudrate 命令用来设置同步串口的波特率。波特率为 2048000 即说明同步串口的速率为 2M。注意此命令只在 DCE 设备上有效。

配置完成后使用 **display interface** 命令查看接口状态：

```
<RTA>display interface Serial 1/0
Serial1/0
Current state: UP
Line protocol state: UP
Description: Serial1/0 Interface
Bandwidth: 2048kbps
Maximum Transmit Unit: 1500
Hold timer: 10 seconds
Internet Address is 10.1.1.1/30 Primary
Link layer protocol: HDLC
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last clearing of counters: Never
Physical layer: synchronous, Baudrate: 2048000 bps
Interface: DCE
Cable type: V35
Clock mode: DCECLK
Last 300 seconds input rate: 3.17 bytes/sec, 25 bits/sec, 0.24 packets/sec
```

```

Last 300 seconds output rate: 3.02 bytes/sec, 24 bits/sec, 0.21 packets/sec
Input:
  1675 packets, 24809 bytes
  0 broadcasts, 0 multicasts
  174 errors, 0 runts, 1 giants
  0 CRC, 173 align errors, 0 overruns
  0 aborts, 0 no buffers, 0 frame errors
Output:
  1489 packets, 21049 bytes
  0 errors, 0 underruns, 0 collisions
  0 deferred
DCD: UP, DTR: UP, DSR: UP, RTS: UP, CTS: UP

```

从上述输出可以看到，接口状态为 **UP**，表明线路可用。带宽为 **2048kbps**，即 **2M**。接口类型为 **DCE**，线缆类型为 **V35**。

说明：

路由器串口可以自动侦测并决定接口类型是 **DCE** 还是 **DTE**。如果 **DCE** 串口电缆连接到串口卡上，则此接口为 **DCE**；反之，如果 **DTE** 串口电缆连接到串口卡上，则此接口为 **DTE**。

步骤三：检查路由器的互通性以及 PC 与路由器网关的互通性

可以通过 **ping** 命令检查 **RTA** 与其相连的 **PCA** 的互通性：

```

[RTA]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=0.962 ms
56 bytes from 192.168.1.2: icmp_seq=1 ttl=64 time=1.656 ms
56 bytes from 192.168.1.2: icmp_seq=2 ttl=64 time=1.007 ms
56 bytes from 192.168.1.2: icmp_seq=3 ttl=64 time=0.792 ms
56 bytes from 192.168.1.2: icmp_seq=4 ttl=64 time=0.715 ms

--- Ping statistics for 192.168.1.2 ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.715/1.026/1.656/0.333 ms

```

在 **RTA** 上检查其与 **RTB** 广域网接口的互通性：

```

[RTA]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=1.125 ms
56 bytes from 10.1.1.2: icmp_seq=1 ttl=255 time=0.980 ms
56 bytes from 10.1.1.2: icmp_seq=2 ttl=255 time=0.956 ms
56 bytes from 10.1.1.2: icmp_seq=3 ttl=255 time=0.960 ms
56 bytes from 10.1.1.2: icmp_seq=4 ttl=255 time=0.969 ms

--- Ping statistics for 10.1.1.2 ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.956/0.998/1.125/0.064 ms

```

步骤四：分别在两台路由器上设置到达对方局域网网段的路由

在 **RTA** 上设置到达 **PCB** 网段的路由：

```
[RTA]ip route-static 192.168.2.0 255.255.255.252 10.1.1.2
```

在 **RTB** 上设置到达 **PCA** 网段的路由：

```
[RTB]ip route-static 192.168.1.0 255.255.255.252 10.1.1.1
```

步骤五：用 ping 命令检查 PCA 与 PCB 的互通性：

在 **PCA** 上 Ping **PCB** 的 IP 地址，正常连通的情况下的显示：

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=19ms TTL=253
来自 192.168.2.2 的回复：字节=32 时间=1ms TTL=253
来自 192.168.2.2 的回复：字节=32 时间=2ms TTL=253
来自 192.168.2.2 的回复：字节=32 时间=2ms TTL=253

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 = 19ms，平均 = 6ms

15.5 实验中的命令列表

表15-3 HDLC 实验命令列表

命令	描述
link-protocol hdlc	对广域网的协议进行封装，H3C路由器的默认封装是PPP

15.6 思考题

1. 如果通信双方的 Keepalive 值设置不一样，该链路还能正常连接吗？

答：两端的 Keepalive 时间值不一样，可能导致 HDLC 协议状态频繁 UP/DOWN，而无法正常工作。

实验16 配置 PPP

16.1 实验内容与目标

完成本实验后，学员将能够：

- 完成 PPP 连接的基本配置
- 独立完成 PPP PAP 验证的配置
- 独立完成 PPP CHAP 验证的配置
- 了解和熟悉 PPP 的常用监控以及维护命令预备知识和技能

16.2 实验组网图

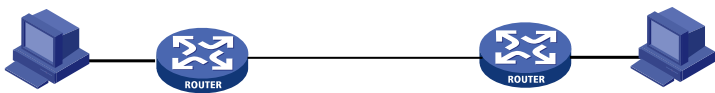


图16-1 PPP 实验环境图

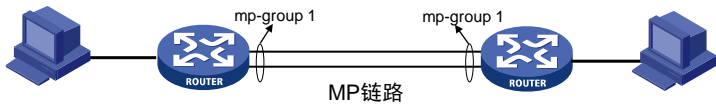


图16-2 PPP MP 实验环境图

16.3 实验设备与版本

本实验所需之主要设备器材如表 16-1 所示。

表16-1 实验设备列表

名称和型号	版本	数量	描述
MSR 36-20	CMW 7.1.049-R0106	2	
PC	Windows 7	2	
V.35 DTE串口线	--	2	
V.35 DCE串口线	--	2	
第5类UTP以太网连接线	--	2	其中包括交叉线2根

16.4 实验过程

本实验中的 PC 以及路由器的 IP 地址规划如表 16-2 所示。

表16-2 IP 地址规划

设备	接口	IP 地址/掩码	备注
PCA	--	192.168.1.2/30	网关192.168.1.1
PCB	--	192.168.2.2/30	网关192.168.2.1
RTA	S1/0	10.1.1.1/30	PPP实验使用
	Mp-group 1	10.1.1.1/30	PPP MP实验使用
RTB	S1/0	10.1.1.2/30	PPP实验使用
	Mp-group 2	10.1.1.2/30	PPP MP实验使用

实验任务一：PPP 协议基本配置

在开始实验前，将路由器配置恢复到默认状态。

步骤一：设置 PC 以及其对应网关的 IP 地址

依据规划，分别设置 PC 以及其对应网关的 IP 地址。

步骤二：将 RTA 广域网接口封装 PPP 协议并配置 IP 地址

```
[RTA]interface Serial 1/0
[RTA-Serial1/0]link-protocol ppp          // 路由器串口默认封装是 PPP
[RTA-Serial1/0]ip address 10.1.1.1 255.255.255.252
[RTA-Serial1/0]baudrate 2048000
```

通过 `display interface` 命令查看接口封装 PPP 以后的显示信息，主要观察 LCP、IPCP 等相关信息：

```
[RTA]display interface Serial 1/0
Serial1/0
Current state: UP
Line protocol state: UP
Description: Serial1/0 Interface
Bandwidth: 2048kbps
Maximum Transmit Unit: 1500
Hold timer: 10 seconds
Internet Address is 10.1.1.1/30 Primary
Link layer protocol: PPP
LCP: opened, IPCP: opened
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last clearing of counters: Never
Physical layer: synchronous, Baudrate: 2048000 bps
Interface: DCE
Cable type: V35
Clock mode: DCECLK
Last 300 seconds input rate: 1.88 bytes/sec, 15 bits/sec, 0.15 packets/sec
Last 300 seconds output rate: 2.17 bytes/sec, 17 bits/sec, 0.17 packets/sec
```

```

Input:
  573 packets, 7272 bytes
  0 broadcasts, 0 multicasts
  0 errors, 0 runts, 0 giants
  0 CRC, 0 align errors, 0 overruns
  0 aborts, 0 no buffers, 0 frame errors
Output:
  579 packets, 7362 bytes
  0 errors, 0 underruns, 0 collisions
  0 deferred
DCD: UP, DTR: UP, DSR: UP, RTS: UP, CTS: UP

```

步骤三：将 RTB 广域网接口封装 PPP 协议并配置 IP 地址

分别将 RTB 广域网接口封装 PPP 协议，并配置 IP 地址、查看接口信息。

```

[RTB]interface Serial 1/0
[RTB-Serial1/0]link-protocol ppp          // 路由器串口默认封装是 PPP
[RTB-Serial1/0]ip address 10.1.1.2 255.255.252

```

通过 `display interface` 命令查看接口封装 PPP 以后的显示信息，主要观察 LCP、IPCP 等相关信息：

```

<RTB>display interface Serial 1/0
Serial1/0
Current state: UP
Line protocol state: UP
Description: Serial1/0 Interface
Bandwidth: 64kbps
Maximum Transmit Unit: 1500
Hold timer: 10 seconds
Internet Address is 10.1.1.2/30 Primary
Link layer protocol: PPP
LCP: opened, IPCP: opened
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last clearing of counters: Never
Physical layer: synchronous, Virtual baudrate: 64000 bps
Interface: DTE
Cable type: V35
Clock mode: DTECLK1
Last 300 seconds input rate: 4.02 bytes/sec, 32 bits/sec, 0.22 packets/sec
Last 300 seconds output rate: 4.00 bytes/sec, 32 bits/sec, 0.22 packets/sec
Input:
  112 packets, 1742 bytes
  0 broadcasts, 0 multicasts
  0 errors, 0 runts, 0 giants
  0 CRC, 0 align errors, 0 overruns
  0 aborts, 0 no buffers, 0 frame errors
Output:
  112 packets, 1738 bytes
  0 errors, 0 underruns, 0 collisions
  0 deferred
DCD: UP, DTR: UP, DSR: UP, RTS: UP, CTS: UP

```

步骤四：检查路由器的互通性以及 PC 与路由器网关的互通性

可以通过 `ping` 命令检查 RTA 与其相连的 PCA 的互通性：

```

[RTA]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=2.204 ms
56 bytes from 192.168.1.2: icmp_seq=1 ttl=64 time=1.191 ms
56 bytes from 192.168.1.2: icmp_seq=2 ttl=64 time=1.462 ms
56 bytes from 192.168.1.2: icmp_seq=3 ttl=64 time=1.376 ms

```

```
56 bytes from 192.168.1.2: icmp_seq=4 ttl=64 time=1.489 ms

--- Ping statistics for 192.168.1.2 ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.191/1.544/2.204/0.346 ms
<RTA>%Oct 31 14:54:19:533 2014 RTA PING/6/PING_STATISTICS: Ping statistics for
192.168.1.2: 5 packets transmitted, 5 packets received, 0.0% packet loss,
round-trip min/avg/max/std-dev = 1.191/1.544/2.204/0.346 ms.
```

在 RTA 上检查其与 RTB 广域网接口的互通性:

```
[RTA]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=1.214 ms
56 bytes from 10.1.1.2: icmp_seq=1 ttl=255 time=0.973 ms
56 bytes from 10.1.1.2: icmp_seq=2 ttl=255 time=0.983 ms
56 bytes from 10.1.1.2: icmp_seq=3 ttl=255 time=0.955 ms
56 bytes from 10.1.1.2: icmp_seq=4 ttl=255 time=0.960 ms

--- Ping statistics for 10.1.1.2 ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.955/1.017/1.214/0.099 ms
<RTA>%Oct 31 14:55:04:019 2014 RTA PING/6/PING_STATISTICS: Ping statistics for
10.1.1.2: 5 packets transmitted, 5 packets received, 0.0% packet loss, round-trip
min/avg/max/std-dev = 0.955/1.017/1.214/0.099 ms.
```

步骤五：分别在两台路由器上设置到达对方局域网网段的路由

在 RTA 上设置到达 PCB 网段的路由:

```
[RTA]ip route-static 192.168.2.0 255.255.255.252 10.1.1.2
```

在 RTB 上设置到达 PCA 网段的路由:

```
[RTB]ip route-static 192.168.1.0 255.255.255.252 10.1.1.1
```

步骤六：在 PCA 或 PCB 上通过 ping 命令检查 PCB 与 PCA 的互通性

在 PCA 上 Ping PCB 的 IP 地址，正常情况下的显示如下:

```
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=18ms TTL=253
来自 192.168.2.2 的回复: 字节=32 时间=1ms TTL=253
来自 192.168.2.2 的回复: 字节=32 时间=1ms TTL=253
来自 192.168.2.2 的回复: 字节=32 时间=1ms TTL=253
```

```
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 = 18ms, 平均 = 5ms
```

实验任务二：PPP PAP 认证配置

在开始实验前，将路由器配置恢复到默认状态。(注：也可以在实验任务一的基础上直接进行下面的步骤二)。

步骤一：设置 PC 和路由器的局域网 IP 地址并确认互通性

依据规划，分别设置 PC 以及路由器的局域网的 IP 地址并确认互通性。具体命令可以参考实验任务一，此时要通过 ping 检测 PC 与路由器之间的互通，此时依据默认封装，RTA 与 RTB 的广域网连接是可以互通的。

步骤二：在 RTA 上配置本地以 PAP 方式验证对端 RTB

首先在 RTA 上配置本地用户名和密码，此用户名和密码要与对端 RTB 发送的用户名和密码一致：

```
[RTA]local-user rtb class network
[RTA-luser-network-rtb]service-type ppp
[RTA-luser-network-rtb]password simple pwdpwd
```

其次在 RTA 上配置本地验证对端 RTB 的方式为 PAP：

```
[RTA]interface serial 1/0
[RTA-Serial1/0]link-protocol ppp
[RTA-Serial1/0]ppp authentication-mode pap
[RTA-Serial1/0]ip address 10.1.1.1 255.255.255.252
```

如果接口的 IP 地址已经配置好，再配置认证，配置完认证后请复位接口：

```
[RTA-Serial1/0]shutdown
[RTA-Serial1/0]undo shutdown
```

步骤三：查看接口状态并验证互通性

通过 **display interface** 查看步骤二配置的接口信息，此时在 RTA 上通过 PING 来测试能否通达 RTB：

```
[RTA]display interface Serial 0/0
Serial1/0
Current state: UP
Line protocol state: DOWN
Description: Serial1/0 Interface
Bandwidth: 64kbps
Maximum Transmit Unit: 1500
Hold timer: 10 seconds
Internet Address is 10.1.1.1/30 Primary
Link layer protocol: PPP
LCP: closed
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last clearing of counters: Never
Physical layer: synchronous, Baudrate: 64000 bps
Interface: DCE
Cable type: V35
Clock mode: DCECLK
Last 300 seconds input rate: 2.68 bytes/sec, 21 bits/sec, 0.22 packets/sec
Last 300 seconds output rate: 2.44 bytes/sec, 19 bits/sec, 0.20 packets/sec
Input:
  805 packets, 10971 bytes
  0 broadcasts, 0 multicasts
  1 errors, 0 runts, 0 giants
  0 CRC, 1 align errors, 0 overruns
  0 aborts, 0 no buffers, 0 frame errors
Output:
  806 packets, 10980 bytes
  0 errors, 0 underruns, 0 collisions
  0 deferred
DCD: UP, DTR: UP, DSR: UP, RTS: UP, CTS: UP
[RTA]ping 10.1.1.2
Ping 10.1.1.2 (10.1.1.2): 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 10.1.1.2 ---
5 packets transmitted, 0 packets received, 100.0% packet loss

```

步骤四：在 RTB 上配置 PAP 验证时发送的用户名和密码

在 RTB 上配置本地被对端 RTA 以 PAP 方式验证时发送的 PAP 用户名和密码，并配置相应的 IP 地址：

```

[RTB]interface serial 1/0
[RTB-Serial1/0]link-protocol ppp
[RTB-Serial1/0]ppp pap local-user rtb password simple pwdpwd
[RTB-Serial1/0]ip address 10.1.1.2 255.255.255.252

```

这里要回想一下 PAP 验证的过程。PAP 验证是两次握手完成的，PAP 验证的第一步就是被验证方以明文的方式发送用户名和密码到验证方。在本实验中，RTB 作为被验证方，要把用户名 rtb 和密码 pwdpwd 以明文的方式发送给验证方 RTA，然后由 RTA 来确认。由此也可以看到 PAP 验证的不安全性。

步骤五：查看接口状态以及验证 RTA 与 RTB 的互通性

通过 ping 验证，并用 display interface Serial1/0 命令显示：

```

<RTA>display interface Serial 1/0
Serial1/0
Current state: UP
Line protocol state: UP
Description: Serial1/0 Interface
Bandwidth: 64kbps
Maximum Transmit Unit: 1500
Hold timer: 10 seconds
Internet Address is 10.1.1.1/30 Primary
Link layer protocol: PPP
LCP: opened, IPCP: opened
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last clearing of counters: Never
Physical layer: synchronous, Baudrate: 64000 bps
Interface: DCE
Cable type: V35
Clock mode: DCECLK
Last 300 seconds input rate: 2.68 bytes/sec, 21 bits/sec, 0.22 packets/sec
Last 300 seconds output rate: 2.44 bytes/sec, 19 bits/sec, 0.20 packets/sec
Input:
  844 packets, 11470 bytes
  0 broadcasts, 0 multicasts
  1 errors, 0 runts, 0 giants
  0 CRC, 1 align errors, 0 overruns
  0 aborts, 0 no buffers, 0 frame errors
Output:
  839 packets, 11448 bytes
  0 errors, 0 underruns, 0 collisions
  0 deferred
DCD: UP, DTR: UP, DSR: UP, RTS: UP, CTS: UP
<RTA> 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=24.403 ms
56 bytes from 10.1.1.2: icmp_seq=1 ttl=255 time=24.026 ms
56 bytes from 10.1.1.2: icmp_seq=2 ttl=255 time=24.139 ms
56 bytes from 10.1.1.2: icmp_seq=3 ttl=255 time=24.168 ms
56 bytes from 10.1.1.2: icmp_seq=4 ttl=255 time=24.150 ms

```

```

--- Ping statistics for 10.1.1.2 ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 24.026/24.177/24.403/0.123 ms

```

步骤六：在 PCA 或 PCB 上通过 ping 命令检查 PCB 与 PCA 的互通性

在 PCA 上 Ping PCB 的 IP 地址，正常情况下的显示如下：

```

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=42ms TTL=253
来自 192.168.2.2 的回复: 字节=32 时间=19ms TTL=253
来自 192.168.2.2 的回复: 字节=32 时间=19ms TTL=253
来自 192.168.2.2 的回复: 字节=32 时间=19ms TTL=253

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 = 19ms, 最长 = 42ms, 平均 = 24ms

```

实验任务三：PPP CHAP 认证配置

在开始实验前，将路由器配置恢复到默认状态。（也可以在实验任务一的基础上直接进行下面的步骤二）。

步骤一：设置 PC 以及路由器的局域网的 IP 地址并确认互通性

依据规划，分别设置 PC 以及路由器的局域网的 IP 地址并确认互通性。具体命令可以参考实验一。通过 ping 检测 PC 与路由器之间的互通性，确认两端路由器通过默认封装 PPP 是可以互通的。

步骤二：在 RTA 上配置本地用户名和密码以及配置验证方式为 CHAP

```

<RTA> system-view
[RTA]local-user rtb class network
[RTA-luser-network-rtb] password simple pwdpwd
[RTA-luser-network-rtb] service-type ppp
[RTA-luser-network-rtb] quit
[RTA]interface serial 1/0
[RTA-Serial1/0] ppp authentication-mode chap
[RTA-Serial1/0] ip address 10.1.1.1 255.255.255.252
[RTA-Serial1/0] quit

```

如果接口的 IP 地址已经配置好，再配置认证，配置完认证后请复位接口：

```

[RTA-Serial1/0]shutdown
[RTA-Serial1/0]undo shutdown

```

步骤三：查看接口状态并检测路由器之间的互通

通过 display interface 查看步骤二配置的接口信息，并通过 ping 来测试能否通达 RTB：

```

[RTA]display interface Serial 1/0
Serial1/0
Current state: UP
Line protocol state: DOWN
Description: Serial1/0 Interface
Bandwidth: 64kbps
Maximum Transmit Unit: 1500
Hold timer: 10 seconds
Internet Address is 10.1.1.1/30 Primary
Link layer protocol: PPP
LCP: closed

```

```

Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last clearing of counters: Never
Physical layer: synchronous, Baudrate: 64000 bps
Interface: DCE
Cable type: V35
Clock mode: DCECLK
Last 300 seconds input rate: 3.81 bytes/sec, 30 bits/sec, 0.20 packets/sec
Last 300 seconds output rate: 3.68 bytes/sec, 29 bits/sec, 0.18 packets/sec
Input:
  907 packets, 12790 bytes
  0 broadcasts, 0 multicasts
  3 errors, 0 runts, 0 giants
  0 CRC, 3 align errors, 0 overruns
  0 aborts, 0 no buffers, 0 frame errors
Output:
  900 packets, 12778 bytes
  0 errors, 0 underruns, 0 collisions
  0 deferred
DCD: UP, DTR: UP, DSR: UP, RTS: UP, CTS: UP
[RTA]ping 10.1.1.2
Ping 10.1.1.2 (10.1.1.2): 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 10.1.1.2 ---
5 packets transmitted, 0 packets received, 100.0% packet loss

```

步骤四：在 RTB 上配置验证方式为 CHAP，并设置本地用户名和密码

配置如下：

```

[RTB]interface serial 1/0
[RTB-Serial1/0]ppp chap user rtb
[RTB-Serial1/0]ppp chap password simple pwdpwd

```

步骤五：查看接口状态并验证互通性

通过 `display interface serial1/0` 命令查看接口状况，并通过 ping 验证连通性：

```

[RTA-Serial1/0]display interface Serial 1/0
Serial1/0
Current state: UP
Line protocol state: UP
Description: Serial1/0 Interface
Bandwidth: 64kbps
Maximum Transmit Unit: 1500
Hold timer: 10 seconds
Internet Address is 10.1.1.1/30 Primary
Link layer protocol: PPP
LCP: opened, IPCP: opened
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last clearing of counters: Never
Physical layer: synchronous, Baudrate: 64000 bps
Interface: DCE
Cable type: V35
Clock mode: DCECLK
Last 300 seconds input rate: 3.08 bytes/sec, 24 bits/sec, 0.20 packets/sec
Last 300 seconds output rate: 3.03 bytes/sec, 24 bits/sec, 0.18 packets/sec

```

```

Input:
  929 packets, 13092 bytes
  0 broadcasts, 0 multicasts
  3 errors, 0 runts, 0 giants
  0 CRC, 3 align errors, 0 overruns
  0 aborts, 0 no buffers, 0 frame errors
Output:
  920 packets, 13091 bytes
  0 errors, 0 underruns, 0 collisions
  0 deferred
DCD: UP, DTR: UP, DSR: UP, RTS: UP, CTS: UP
[RTA]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=24.292 ms
56 bytes from 10.1.1.2: icmp_seq=1 ttl=255 time=24.182 ms
56 bytes from 10.1.1.2: icmp_seq=2 ttl=255 time=24.188 ms
56 bytes from 10.1.1.2: icmp_seq=3 ttl=255 time=24.150 ms
56 bytes from 10.1.1.2: icmp_seq=4 ttl=255 time=24.169 ms

--- Ping statistics for 10.1.1.2 ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 24.150/24.196/24.292/0.050 ms

```

步骤六：在 PCA 或 PCB 上通过 ping 命令检查 PCB 与 PCA 的互通性

在 PCA 上 Ping PCB 的 IP 地址，正常情况下的显示如下：

```

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=36ms TTL=253
来自 192.168.2.2 的回复: 字节=32 时间=19ms TTL=253
来自 192.168.2.2 的回复: 字节=32 时间=19ms TTL=253
来自 192.168.2.2 的回复: 字节=32 时间=19ms TTL=253

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 = 19ms, 最长 = 36ms, 平均 = 23ms

```

实验任务四：PPP MP 配置

在开始实验前，将路由器配置恢复到默认状态。

步骤一：依据要求，使用两对 V.35 电缆分别连接 RTA 和 RTB

步骤二：在 RTA 和 RTB 上创建 Mp-group 接口并配置 IP 地址

分别在 RTA 和 RTB 上创建 Mp-group 接口，并配置相应的 IP 地址。

在 RTA 上配置如下：

```

[RTA]interface MP-group 1
[RTA-MP-group1]ip address 10.1.1.1 30

```

在 RTB 上配置如下：

```

[RTB]interface MP-group 1
[RTB-MP-group1]ip address 10.1.1.2 30
[RTB-MP-group1]quit

```

步骤三：在 RTA 和 RTB 上将相应物理接口加入 MP-group 接口

分别在 RTA 和 RTB 上将相应的物理接口加入到 MP-group 接口中，并将相应的物理接口封装 PPP 协议。

在 RTA 上配置如下：

```
[RTA]interface serial 1/0
[RTA-Serial1/0]link-protocol ppp
[RTA-Serial1/0]ppp mp MP-group 1
[RTA]interface serial 2/0
[RTA-Serial2/0]link-protocol ppp
[RTA-Serial2/0]ppp mp MP-group 1
```

在 RTB 上配置如下：

```
[RTB]interface serial 1/0
[RTB-Serial1/0]link-protocol ppp
[RTB-Serial1/0]ppp mp MP-group 1
[RTB]interface serial 2/0
[RTB-Serial2/0]link-protocol ppp
[RTB-Serial2/0]ppp mp MP-group 1
```

步骤四：验证并查看 MP 效果

```
[RTA] display ppp mp
Template: MP-group1
max-bind: 16, fragment: enabled, min-fragment: 128
Master link: MP-group1, Active members: 2, Bundle Multilink
Peer's endPoint descriptor: MP-group1
Sequence format: long (rcv)/long (sent)
Bundle Up Time: 2014/10/31 15:24:45:770
0 lost fragments, 0 reordered, 0 unassigned, 0 interleaved
Sequence: 0 (rcv)/0 (sent)
Active member channels: 2 members
    Serial1/0          Up-Time:2014/10/31 15:24:45:770
    Serial2/0          Up-Time:2014/10/31 15:24:54:470

[RTA] display interface Mp-group 1
MP-group1
Current state: UP
Line protocol state: UP
Description: MP-group1 Interface
Bandwidth: 128kbps
Maximum Transmit Unit: 1500
Hold timer: 10 seconds
Internet Address is 10.1.1.1/30 Primary
Link layer protocol: PPP
LCP: opened, MP: opened, IPCP: opened
Physical: MP, baudrate: 128000 bps
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 2 packets, 24 bytes, 0 drops
Output: 2 packets, 20 bytes, 0 drops
```

在 RTA 上 ping 对端 IP：

```
[RTA] 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=25.906 ms
56 bytes from 10.1.1.2: icmp_seq=1 ttl=255 time=25.684 ms
56 bytes from 10.1.1.2: icmp_seq=2 ttl=255 time=25.678 ms
56 bytes from 10.1.1.2: icmp_seq=3 ttl=255 time=25.655 ms
56 bytes from 10.1.1.2: icmp_seq=4 ttl=255 time=25.577 ms

--- Ping statistics for 10.1.1.2 ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 25.577/25.700/25.906/0.110 ms
```

16.5 实验中的命令列表

表16-3 实验命令列表

命令	描述
link-protocol ppp	用来配置接口封装的链路层协议为PPP
ppp authentication-mode { chap pap } [[call-in] domain isp-name]	用来设置本端PPP协议对对端设备的验证方式
ppp chap password { cipher simple } password	用来配置进行CHAP验证时采用的默认口令
ppp chap user username	用来配置采用CHAP认证时的用户名
ppp mp	用来配置封装PPP的接口工作在MP方式
ppp mp MP-group number	用来将当前接口加入指定的MP-Group，使接口工作在MP方式
ppp pap local-user username password { cipher simple } password	用来配置本地设备被对端设备采用PAP方式验证时发送的用户名和口令

16.6 思考题

1. 在配置 CHAP 验证的时候，如果 RTB 接口 S1/0 上不配置 `ppp chap password simple pwdpwd`，那么 RTB 收到 RTA 的验证请求后，该如何处理才能完成 CHAP 验证的第二次握手操作并给 RTA 发送 Response？这个时候 RTB 上需要其他配置吗？

答：按照 CHAP 验证的原理，如果被验证方检查发现本端接口上没有配置默认的 CHAP 密码，则被验证方根据此报文中主验证方的用户名在本端的用户表查找该用户对应的密码，因此这个时候需要在 RTB 上配置本地用户名和对端密码：

```
[RTB]local-user rta class network
[RTB-luser-network-rta]service-type ppp
[RTB-luser-network-rta]password simple pwdpwd
```

当然这个时候在 RTA 上也需要将用户名 rta 通过 `ppp chap user` 命令发送出来。

```
[RTA]interface Serial1/0
[RTA-Serial1/0]ppp chap user rta
```

2. 如果 MP 需要验证，那么该如何配置呢？

答：在加入 MP-group 的物理接口下配置验证即可，如：

```
[RTB]interface serial 1/0
[RTB-Serial1/0] link-protocol ppp
[RTB-Serial1/0] ppp authentication-mode pap
[RTB-Serial1/0] ppp pap local-user rtb password simple pwdpwd
```

3. 实验任务一的步骤二、三中，当查看接口信息时，RTA 端显示 Baudrate is 2048000 bps，而 RTB 端显示 Virtual baudrate is 64000 bps，两端波特率显示不一致，这是为什么？

答：同步串口根据外接电缆类型完成电气特性的选择。本实验中 RTB 是 DTE 端。同步串口作为 DTE 设备时，接受 DCE 设备提供的时钟，端口显示的是虚波特率，不影响使用，实际上其波特率与 DCE 端同步。我们也可以利用如下命令将虚拟波特率修改成与 DCE 端一致：

```
[RTB]interface serial 1/0
[RTB-Serial1/0]virtualbaudrate 2048000
[RTB-Serial1/0]shutdown
[RTB-Serial1/0]undo shutdown
```


实验17 配置 3G（选修）

17.1 实验内容与目标

完成本实验后，学员将能够：

- 完成 3G 的基本配置
- 了解和熟悉 3G 的常用监控以及维护命令

17.2 实验组网图



图17-1 配置 3G 实验环境图

17.3 实验设备与版本

本实验所需之主要设备器材如表 17-1 所示。

表17-1 实验设备列表

名称和型号	版本	数量	描述
MSR 930-GU	CMW 5.20, Release 2513	1	若选用MSR930-GT设备则需要电信SIM
联通3G SIM卡	--	1	

17.4 实验过程

本实验需要通过 console 口连接设备来完成配置。

实验任务一： 配置 3G 拨号

在开始实验前，将路由器配置恢复到默认状态。

步骤一：配置拨号串并设置 IP 地址协商获得

3G 拨号时，cellular 口的 IP 地址通常由运营商分配。

```
[H3C]dialer-rule 1 ip permit
[H3C]interface Cellular0/0
[H3C-Cellular0/0]ip address ppp-negotiate
```

步骤二：配置接口的链路协议

配置拨号口的链路协议为 ppp，并设置认证所用的用户名和密码。

拨号具体所使用的认证方式和用户名、密码，需由运营商提供，在使用前向运营商咨询。

```
[H3C-Cellular0/0]async mode protocol
[H3C-Cellular0/0]link-protocol ppp
[H3C-Cellular0/0]ppp chap user card
[H3C-Cellular0/0]ppp chap password simple card
[H3C-Cellular0/0]ppp pap local-user card password simple
```

步骤三：配置拨号规则

拨号串是在配置 3G 拨号时必须配置的内容，拨号串需根据接入的运营商来确定。联通和移动的拨号串为*99#，电信的为#777。

```
[H3C-Cellular0/0]dialer enable-circular
[H3C-Cellular0/0]dialer-group 1
[H3C-Cellular0/0]dialer timer idle 60
[H3C-Cellular0/0]dialer number *99#
```

步骤四：配置路由

配置默认路由从接口 Cellular0/0 出去。

```
[H3C]ip route-static 0.0.0.0 0.0.0.0 Cellular0/0
```

步骤五：在 TTY 上配置允许 modem 呼入和呼出

首先通过 display user-interface 命令查看到 cellular 接口对应的 TTY 号：

```
[H3C]display user-interface
```

Idx	Type	Tx/Rx	Modem	Privi	Auth	Int
12	TTY 12	9600	-	0	N	Cellular0/0
80	AUX 0	9600	-	3	N	-
81	VTY 0	-	-	0	P	-
82	VTY 1	-	-	0	P	-
83	VTY 2	-	-	0	P	-
84	VTY 3	-	-	0	P	-
85	VTY 4	-	-	0	P	-

之后在对应的 TTY 口下，配置允许 modem 呼入和呼出：

```
[H3C]user-interface tty 12
[H3C-ui-tty12]modem both
```

实验任务二：查看 3G 拨号的状态

步骤一：查看当前 cellular 接口的信息

在查看 3G 拨号的状态时，主要通过分析 `display cellular 0/0 all` 命令的显示信息，来看当前状态是否正常。

```
<H3C>display cellular 0/0 all
Modem State:
Hardware Information
=====
Model = DM11-2
Manufacturer = Wistron NeWeb Corp.
Modem Firmware Version = DM11-2-M9615A-CETWTBZM-6.0.15216-4.5
International Mobile Equipment Identity (IMEI) = 354083060196258
International Mobile Subscriber Identity (IMSI) = 460010076902094
Hardware Version = 20004
Modem Status = Online

Profile Information
=====
Profile index = 1
PDP Type = IPv4v6, Header Compression = OFF
Data Compression = OFF
Access Point Name (APN) = njkx.gzdt.jsapn
Authentication = NONE
Username =
* - Default profile

Network Information
=====
Current Service Status = Service Available
Registration Status = Registered
Current Service = Combined
Current Roaming Status = Home
Current Data Bearer Technology = UMTS
Network Selection Mode = Automatic
Mobile Country Code (MCC) = 460
Mobile Network Code (MNC) = 01
Location Area Code (LAC) = 53506
Cell ID = 100858970

Radio Information
=====
Technology Preference = No preference specified (AUTO)
Technology Selected = UMTS

WCDMA related info
-----
Current RSSI = -37 dBm
Current ECIO = -2 dBm

Modem Security Information
```

17.5 实验中的命令列表

表17-2 实验命令列表

命令	描述
link-protocol ppp	用来配置接口封装的链路层协议为ppp
async mode protocol	配置接口工作在协议模式
ppp chap user username ppp chap password simple password	配置chap认证的用户名密码
ppp pap local-user username password simple password	配置采用CHAP认证时的用户名密码
ip address ppp-negotiate	配置本端接口接收ppp协商产生的由对端分配的地址
dialer enable-circular	使能轮询DCC
dialer-rule group-number { protocol-name { deny permit } acl { acl-number name acl-name } }	配置拨号访问组及拨号访问控制条件
dialer-group group-number	将接口加入拨号访问组
modem both	配置允许modem呼入和呼出

17.6 思考题

1. 如果忘记配置拨号串会怎样？

答：如果漏配了拨号串，设备将无法完成拨号功能。

实验18 配置 WLAN（选修）

18.1 实验内容与目标

完成本实验，您应该能够：

- 了解 SSID 服务集标识的意义
- 熟悉 SSID 的常见配置选项
- 掌握 SSID 服务集标识的配置命令

18.2 实验组网图

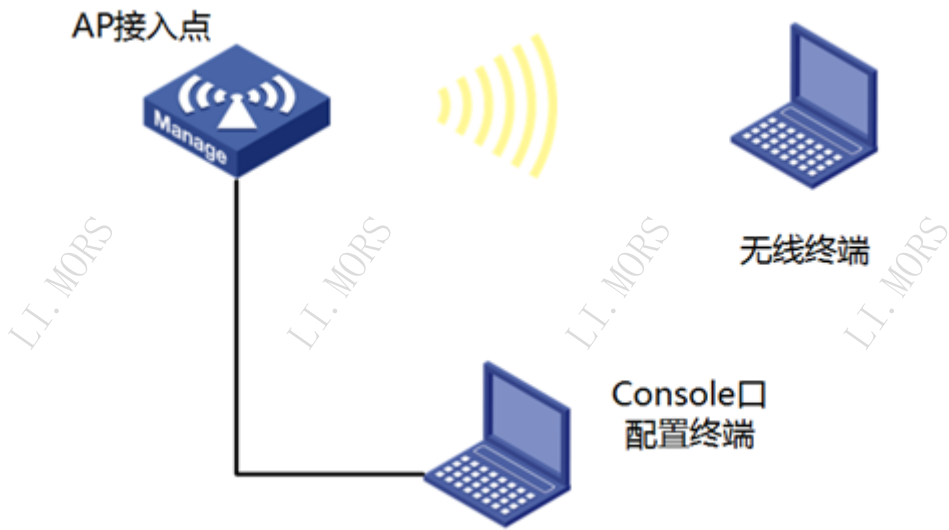


图18-1 实验组网图

配置终端通过串口线连接到无线接入点的 Console 口上，用于无线接入点的配置。笔记本电脑上要求安装上无线网卡，通过无线链路和无线接入点相联系。

18.3 实验设备与版本

本实验所需之主要设备器材如表 18-1 所示：

表18-1 实验设备列表

名称和型号	版本	数量	描述
WA1208E	R1102	1	增强型无线接入点
PC	Windows 7	2	一台带有串口（或 USB 转串口）， 一台带有无线网卡

名称和型号	版本	数量	描述
Console 线	--	1	

18.4 实验过程

本实验的任务是创建一个 SSID，并配置相关选项。

实验任务一：SSID 的创建

要实现无线业务，首先必须配置 SSID（Service Set ID），首先需要在 WA1208E 上设置 SSID 标识，系统缺省的 SSID 标识是 wa1208e。

步骤一：进入系统视图

在用户视图下输入 `system-view` 命令后回车，即进入系统视图。在此视图下提示为：`[H3C]`。只有在系统视图下才可以创建 SSID。

步骤二：增加 SSID

```
[H3C]ssid wa1208e
[H3C-ssid-wa1208e]
```

SSID 是用来唯一标识无线网络的、大小写敏感的一组字符串，由 2 到 32 个字符或数字组成。注意：WA208E 支持多达 8 个 SSID。这样在无线网卡侧，可以最多找到 8 个 SSID 组。

实验任务二：SSID 的绑定

只有在无线端口上绑定了设置的 SSID，无线终端设备（如无线网卡）才能收到无线端口广播的 SSID 标识，才能接入无线局域网。

步骤一：进入系统视图

在用户视图下输入 `system-view` 命令后回车，即进入系统视图。在此视图下提示为：`[H3C]`。

步骤二：绑定无线接口

```
[H3C]interface Wireless-access 1/2
[H3C-Wireless-access1/2]bind ssid wa1208e
bind the ssid sucessfully!
```

注意：步骤一创建的 SSID 只有和具体的无线接口绑定，才能生效。也就是说，才可以在无线网卡端发现创建的 SSID 组。“`wireless-access1/2`”这里的表示的是射频卡 1 的一个无线接口 2，“/”标识符前的数字表示射频卡号。

实验任务三：SSID 的隐藏

SSID 可以配置成隐藏模式，这样无线终端（如笔记本电脑、PDA 设备等）就不会找到该 SSID，需要手动的设置该 SSID 才能接入 WA1208E。

步骤一：进入系统视图

在用户视图下输入 `system-view` 命令后回车，即进入系统视图。在此视图下提示为：`[H3C]`。

步骤二：进入 SSID 视图并隐藏 SSID

```
[H3C]ssid wal208e
[H3C-ssid-wal208e]hide-ssid
```

注意：在此情况下无线网卡是无法找到该 SSID 组的，需要手动添加；如果不希望隐藏 SSID，使用 UNDO 命令取消该配置。

实验任务四：SSID 的接入用户数目的限制

WA1208E 可以同时接入多个用户，为了防止设备上接入过多的用户而影响性能，可以设置允许接入的最大数目。

步骤一：进入系统视图

在用户视图下输入 **system-view** 命令后回车，即进入系统视图。在此视图下提示为：**[H3C]**。

步骤二：进入 SSID 视图并设置允许接入的最大数目

```
[H3C]ssid wal208e
[H3C-ssid-wal208e] max-user-number 30
```

上面命令配置 WA1208E 最多允许接入 30 个用户数目。

18.5 实验中的命令列表

表18-2 命令列表

命令	描述
system-view	使用户从用户视图进入系统视图
ssid ssid-name	创建一个 SSID
bind ssid ssid-name	将 SSID 和一个无线接口绑定
hide-ssid	隐藏服务集标识
max-user-number number	设置允许接入的最大用户数