
《通信网络基础》 实验指导书

张文慧

广东工业大学信息工程学院

二〇一六年一月印刷

目 录

序论 路由器基本操作.....	1
实验一 基本组网实验.....	8
实验二 路由协议实验（RIP、OSPF）.....	12
实验三 访问控制列表（ACL）配置实验.....	19
实验四 地址转换（NAT）的配置实验.....	25

注：

1. 本实验为本学期《宽带网络技术》实验的先修课程，请妥善保管，以便开展其他实验前做好复习工作。
2. 实验室设备繁多，且各种设备的额定电压不同，请尽量不要打开、连接使用与实验无关的设备。若要使用，请确认电源线所提供的电压和设备相匹配，**若因操作不当引起设备损坏，自行负责。**
3. 实验过程中可能需要存储一定的实验数据和结果显示图，请准备存储设备以备用。

序论 路由器基本操作

一、简介

H3C AR 18-2X 系列路由器是华为 3Com 公司开发的新一代专业的宽带路由器，它将路由和交换设备有机地结合在一起，为中小企业和网吧提供交换及接入的一体化解决方案。AR 18-2X 系列路由器包括 AR 18-21A、AR 18-21、AR 18-22、AR 18-22-8、AR 18-23-1、AR 18-22S-8、AR 18-23S-1 和 AR 18-22-24 几款设备。

H3C AR 18-22-24 路由器采用 32 位的高性能微处理器技术的 CPU，提供高性能的数据转发功能。该产品缺省内存配置是 64MB，Flash 大小为 8MB，其接口采用固定配置，提供 2 个 10/100M 以太网口（WAN）、24 个 10/100M 二层交换以太网接口（LAN）和 1 个配置口。

H3C AR 28-1x 系列路由器是华为 3Com 公司面向企业用户的模块化接入路由器，在提供了固定的快速以太网接口、AUX 口、同异步串口和 E1 端口的同时，还提供了丰富的可选配的智能接口卡 SIC 及多功能接口模块 MIM，可与 H3C 系列路由器、以太网交换机一起为行业用户和 SMB 用户提供全方位的端到端的网络解决方案。

二、登录路由器

步骤如下：

(1) 连接路由器到配置终端

如图 1 所示，将配置口电缆的 RJ45 一端与路由器的配置口相连，DB9 一端与电脑的串口相连。

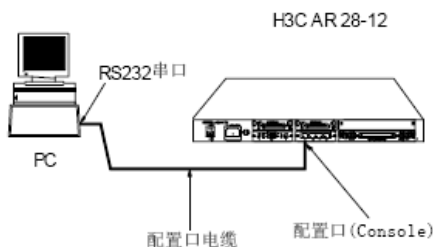


图 1 通过 CON 口与路由器相连

(2) 设置配置终端的参数

在本地 PC 上，创建超级终端，在“开始”——“程序”——“附件”——“通讯”，运行“超级终端”，可以为“超级终端”取个名字，如 aaa，进入下一步。



图 2 新建连接

选择连接端口。如图 3 所示，【连接时使用】一栏选择连接的串口（注意选择的串口应该与配置电缆实际连接的串口一致）。



图 3 选择串口

设置串口参数。如图 4 所示，在串口的属性对话框中设置波特率为 9600，数据位为 8，奇偶校验为无，停止位为 1，流量控制为无，按<确定

>按钮，返回超级终端窗口。



图 4 串口参数设置

配置超级终端属性。在超级终端中选择[属性/设置]一项，进入图 5 所示的属性设置。



图 5 终端类型设置

置窗口。选择终端仿真类型为“VT100”或“自动检测”，按<确定>按钮，返

回超级终端窗口。

确认路由器与配置终端的连接正确，确认已经完成配置终端参数的设置后，即可对路由器上电。随后路由器上出现自检内容。（注：路由器型号及软件版本不同，显示的内容不一样）

系统启动过程如下：

```
Starting at 0x1c00000...
```

```
*****
*
*      H3C 2800 Routers Boot ROM, V9.19      *
*
*****
```

```
Copyright(c) 2004-2006 Hangzhou Huawei-3Com Technology Co., Ltd.
```

```
Testing memory...OK!
128M   bytes  SDRAM
32768k bytes  flash memory
Hardware Version is MTR 3.0
CPLD Version is CPLD 1.0
```

```
Press Ctrl-B to enter Boot Menu
The current starting file is main application file--flash:/main.bin!

The main application file is self-decompressing.....
.....
.....
.....OK!
```

```
System is starting...
Starting at 0x10000...
```

```
User interface Con 0 is available.
```

```
Press ENTER to get started.
```

启动完毕，回车，超级终端里显示<Quidway>或<H3C>字样。（注：此字样的意思为路由器当前命名，当路由器处于初始状态时，显示此字样）

输入命令：`display current-configuration` 可以查看当前路由器的配置情况。

三、路由器的视图

华为系列路由器具有用户视图、系统视图和接口视图，不同视图对应一组相关命令，完成不同的功能。

不同视图的表现形式：

(1) 用户视图

表现形式是一对尖括号 (<>) 括起的路由器名称，如：<Quidway>。

可以输入“?”查看在当前视图下具有哪些命令。

在系统视图下，通过组合键“ctrl+z”进入用户视图。

(2) 系统视图

在用户视图下，输入命令：system-view（注：也可只输入 sys，在没有歧义时路由器会自动识别不完整词，很多命令都可以只输入每个单词的前几个字符）就进入系统视图。表现形式是一对中括号 ([]) 括起的路由器名称，如：[Quidway]。也可输入“?”查看当前视图下可以执行的命令。

(3) 接口视图

在系统视图下，输入 interface 命令就进入接口视图，如：interface e1/0 就进入 e1/0 口。接口视图的表现形式是中括号括起的路由器名-接口名，如：[R1-Ethernet1/0]，即 R1 路由器的以太网的 1/0 口。同样也可输入“?”查看当前视图下可以执行的命令。

四、清除路由器的配置

为了试验能顺利进行，我们常常在配置路由器前都需要恢复路由器的默认配置，避免以前的配置对试验造成影响，按如下步骤操作可以清除路由器的配置：

(1) 在用户视图下执行 reset saved-configuration 命令，擦除 FLASH 中的信息。

(2) 在用户视图下执行 reboot 命令，重启路由器。

(3) 路由器启动后，自动进入用户视图，此时，执行 display current-configuration 查看配置信息。

五、常用命令

(1) 从用户视图切换到系统视图：system

(2) 从系统视图切换到接口视图(假设切换到 s0/0 接口)：interface s0/0

- (3) 从一个视图返回到上级视图：quit
- (4) 配置路由器接口地址（在接口视图下）：ip address（后连 ip 地址和子网掩码）
- (5) 查看当前路由器配置：dis current
- (6) 查看已经保存的启动配置：dis saved-config
- (7) 查看路由器的版本信息：dis version
- (8) 更改路由器的名字：sysname
- (9) 重新启动路由器：reboot
- (10) 设置路由器的系统时间：clock
- (11) 保存配置：save
- (12) 看接口状态：dis interface
- (13) 查看路由表：dis ip routing-table
- (14) 查看路由器负载（CPU 使用情况）：dis cpu
- (15) 取消已经配置的命令：undo XXXX（XXXX 为先前配置的命令）

六、获得命令帮助

Quidway 系列路由器提供了丰富的在线帮助：

- (1) 在任一视图下，键入“?”获取该视图下所有命令及其简单描述。
- (2) 键入一命令，后接以空格分隔的“?”键，如果问号所在位置为关键字，则列出全部关键字及其简单描述。
- (3) 键入一命令，后接以空格分隔的“?”键，如果该位置为参数，则列出有关的参数描述。
- (4) 键入一字符串，其后紧接“?”，列出以该字符串开头的命令。
- (5) 键入一命令，后接一字符串紧接“?”键，列出该命令以该字符串开头的有关关键字。

七、路由表内容

```
System View: return to User View with Ctrl+Z.
[routerG]dis ip r
  Routing Table: public net
Destination/Mask  Protocol  Pre   Cost      Nexthop      Interface
0.0.0.0/0         IS-IS    15    10         172.16.17.1   Ethernet0/1
127.0.0.0/8      DIRECT   0     0          127.0.0.1     InLoopBack0
127.0.0.1/32     DIRECT   0     0          127.0.0.1     InLoopBack0
172.16.15.164/30 IS-IS    15    20         172.16.17.1   Ethernet0/1
172.16.17.0/27   DIRECT   0     0          172.16.17.2   Ethernet0/1
172.16.17.2/32   DIRECT   0     0          127.0.0.1     InLoopBack0
172.16.17.32/27  DIRECT   0     0          172.16.17.33  Ethernet0/0
172.16.17.33/32  DIRECT   0     0          127.0.0.1     InLoopBack0
172.16.17.252/32 IS-IS    15    20         172.16.17.1   Ethernet0/1
172.16.17.253/32 DIRECT   0     0          127.0.0.1     InLoopBack0
172.16.17.254/32 IS-IS    15    20         172.16.17.34  Ethernet0/0
[routerG]
```

每一行代表一条路由，内容从左往右包括：

- 目的地址/掩码长度：用来标识 IP 报文的目的地址或目的网络。
- 协议：用来标志本条路径采用的协议。
- 优先级：用来标识本条路径所采用协议的优先级别。数值越小，优先等级越高。
- 度量值：用来标识本条路径上的损耗等其他开销状况。
- 下一跳 IP 地址：说明 IP 包所经由的下一个路由器。
- 输出接口：说明 IP 报文将从该路由器哪个接口转发。

实验一 基本组网实验

实验项目名称：基本组网实验

实验项目性质：普通实验

所属课程名称：现代通信网

实验计划学时：2

一、实验目的

自己组建小型网络，学习最简单的静态路由协议并测试网络连通性。

二、实验内容和要求

常用的路由协议主要有：静态路由、RIP、OSPF、IS-IS、BGP，小型网络一般使用静态路由、RIP，大中型网络一般使用 OSPF、IS-IS，BGP 协议是用于大型网络自治系统 AS 之间的选路协议。

通过在路由器上配置静态路由协议命令，可以利用路由器把不同的网段连接起来，从而实现不同网段的 PC 互相 PING 通。

利用一台 PC 和 AR18、AR28 搭建小型网络环境，实现相邻小组 PC 互相 PING 通。

静态路由命令格式：`ip route X Y Z`，其中 X 是目标网段，如 172.16.1.0；Y 是子网掩码，如 255.255.255.0；Z 是去往该目标网段的下一跳（网关）的 IP 地址，如 182.168.1.254。

三、实验主要仪器设备和材料

AR28 路由器、AR18 路由器，一台 PC 机。

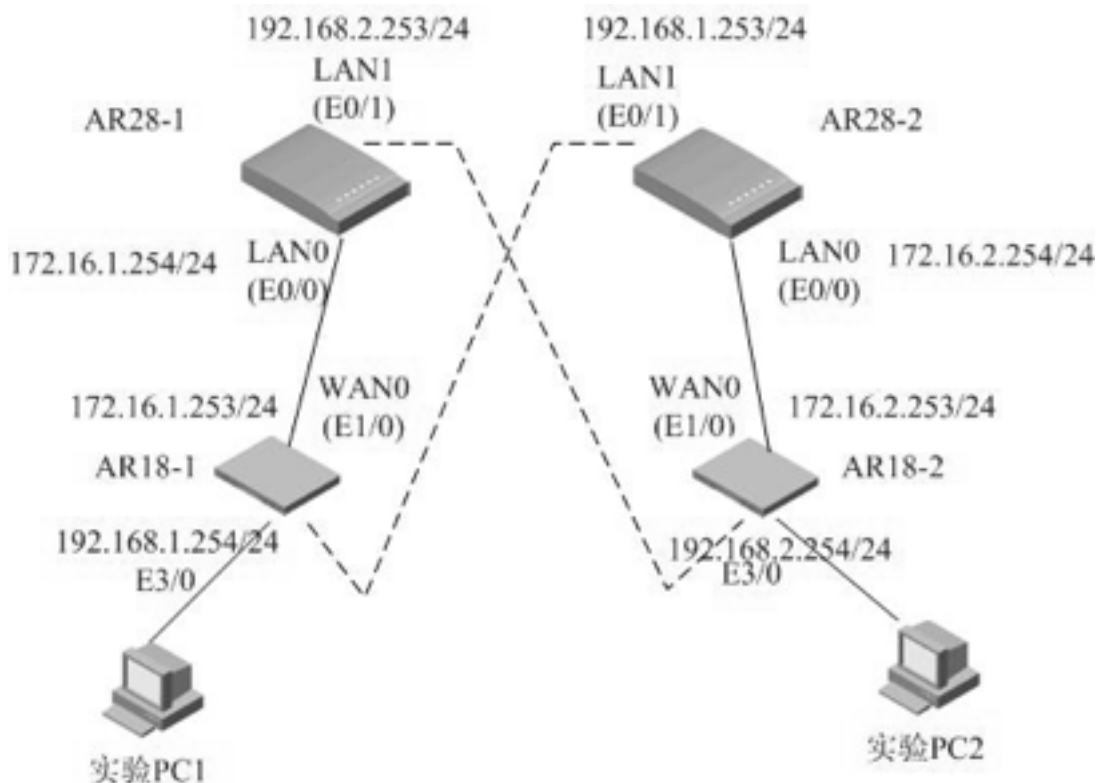
四、实验方法、步骤及结果测试

为了方便测试，本实验需要借助另一小组的一台 PC 做测试，因此需要把相邻两个小组的设备连接起来。同时需要添加一些为了测试方便而做的配置，这些配置用斜体字加粗表示，具体见拓扑图。

1、连接设备

其中实验 PC1 用网线接到 AR18-1 路由器的 1-24 口中的任意一口。

其中实验 PC2 用网线接到 AR18-2 路由器的 1-24 口中的任意一口。
 AR28-1 的 LAN1 口用网线接到 AR18-2 路由器的 1-24 口中的任意一口。
 AR28-2 的 LAN1 口用网线接到 AR18-1 路由器的 1-24 口中的任意一口。



PC1 的默认网关为 AR18-1 的 E3/0 地址 192.168.1.254；PC2 的默认网关为 AR18-2 的 E3/0 地址 192.168.2.254，子网掩码均为 255.255.255.0。

2、实验实际配置：（粗体字部分）请对照前面的拓扑图。

第 1 组配置：

AR18-1 配置：

用超级终端进入路由器后，

```
<quidway>sys //进入系统视图
[quidway] sysname ar18-1 //更改路由器名字为 ar18-1
[ar18-1] interface e3/0 //进入 e3/0 接口并配置 IP 地址
Ip address 192.168.1.254 255.255.255.0
Quit
[ar18-1] Interface e1/0 //进入 1/0 接口并配置 IP 地址
Ip address 172.16.1.253 255.255.255.0
```

Quit

```
[ar18-1] Ip route 0.0.0.0 0.0.0.0 172.16.1.254 //配置静态路由，这里是最简单的缺省路由，下一跳是 172.16.1.254
```

AR28-1 配置：

用超级终端进入路由器后，

```
<quidway> sys //进入系统视图
[quidway] sysname ar28-1 //更改路由器名字为 ar28-1
[ar28-1] interface e0/0 //进入 e0/0 接口并配置 IP 地址
Ip address 172.16.1.254 255.255.255.0
Quit
[ar28-1] Interface e0/1 //进入 e0/1 接口并配置 IP 地址
Ip address 192.168.2.253 255.255.255.0
Quit
[ar28-1] Ip route 0.0.0.0 0.0.0.0 172.16.1.253 //配置静态路由，这里是最简单的缺省路由，下一跳是 172.16.1.253
[ar28-1] ip route 172.16.2.0 255.255.255.0 192.168.2.254 //配置静态路由，
// 去往 172.16.2.0 网段的下一跳是 192.168.2.254。
// 这里是为了方便测试而添加的配置。
```

第 2 组配置：

AR18-2 配置：

用超级终端进入路由器后，

```
<quidway> sys //进入系统视图
[quidway] sysname ar18-2 //更改路由器名字为 ar18-2
[ar18-2] interface e3/0 //进入 e3/0 接口并配置 IP 地址
Ip address 192.168.2.254 255.255.255.0
Quit
[ar18-2] Interface e1/0 //进入 e1/0 接口并配置 IP 地址
Ip address 172.16.2.253 255.255.255.0
Quit
[ar18-2] Ip route 0.0.0.0 0.0.0.0 172.16.2.254 //配置静态路由，这里是最
```

简单的静态缺省路由，下一跳是 172.16.2.254

AR28-2 配置：

用超级终端进入路由器后，

```
<quidway>sys //进入系统视图
[quidway]sysname ar28-2 //更改路由器名字为 ar28-2
[ar28-2] interface e0/0 //进入 e0/0 接口并配置 IP 地址
    Ip address 172.16.2.254 255.255.255.0
    Quit
[ar28-2] Interface e0/1 //进入 e0/1 接口并配置 IP 地址
    Ip address 192.168.1.253 255.255.255.0
    Quit
[ar28-2] Ip route 0.0.0.0 0.0.0.0 172.16.2.253 //配置静态路由，这里是最
简单的静态缺省路由，下一跳是 172.16.2.253
[ar28-2]ip route 172.16.1.0 255.255.255.0 192.168.1.254 //配置静态路由，去
往 172.16.1.0 网段的下一跳是 192.168.1.254.
这里是为了方便测试而添加的配置。
```

用 `dis ip routing-table` 命令查看路由表，看是否具有上述两条路由。

PC1 的网关为 AR18 的 E3/0 的接口地址 192.168.1.254/24，PC2 的网关为 AR18 的 E3/0 的接口地址 192.168.2.254/24 看是否能够实现两台电脑的互相 PING 通。

五、实验报告要求

弄清静态路由的工作原理，分析两台 PC 互相 PING 通的过程。

六、思考题

- 1、实验中，如果不添加斜体字加粗的部分，是否还能实现两台 PC 互相 PING 通？
- 2、静态缺省路由（目标网段为 0.0.0.0 0.0.0.0）和明细的静态路由（有目标网段的静态路由）有什么区别？

实验二 路由协议实验 (RIP、OSPF)

实验项目名称：路由协议实验 (RIP、OSPF)

实验项目性质：普通实验

所属课程名称：现代通信网

实验计划学时：2

一、实验目的

常见的路由协议有静态，RIP，OSPF 等，静态路由一般用于较小的网络环境，RIP 一般用于不超过 15 台路由器的环境，OSPF 常用于大型的网络环境，是目前主流的网络路由协议之一。

二、实验内容和要求

- 1、如何配置路由器，并掌握基本的命令
- 2、学习常见的网络路由协议配置方法

三、实验主要仪器设备和材料

AR28 路由器、AR18 路由器，一台 PC 机器。

为了方便测试，本实验需要借助另一小组的一台 PC 做测试，因此需要把相邻两个小组的设备连接起来。同时需要添加一些为了测试方便而做的配置，这些配置用斜体字加粗表示，具体见拓扑图。

四、实验方法、步骤及结果测试

实验拓扑结构和连线图：如下：

其中实验 PC1 用网线接到 AR18-1 路由器的 1-24 口中的任意一口。

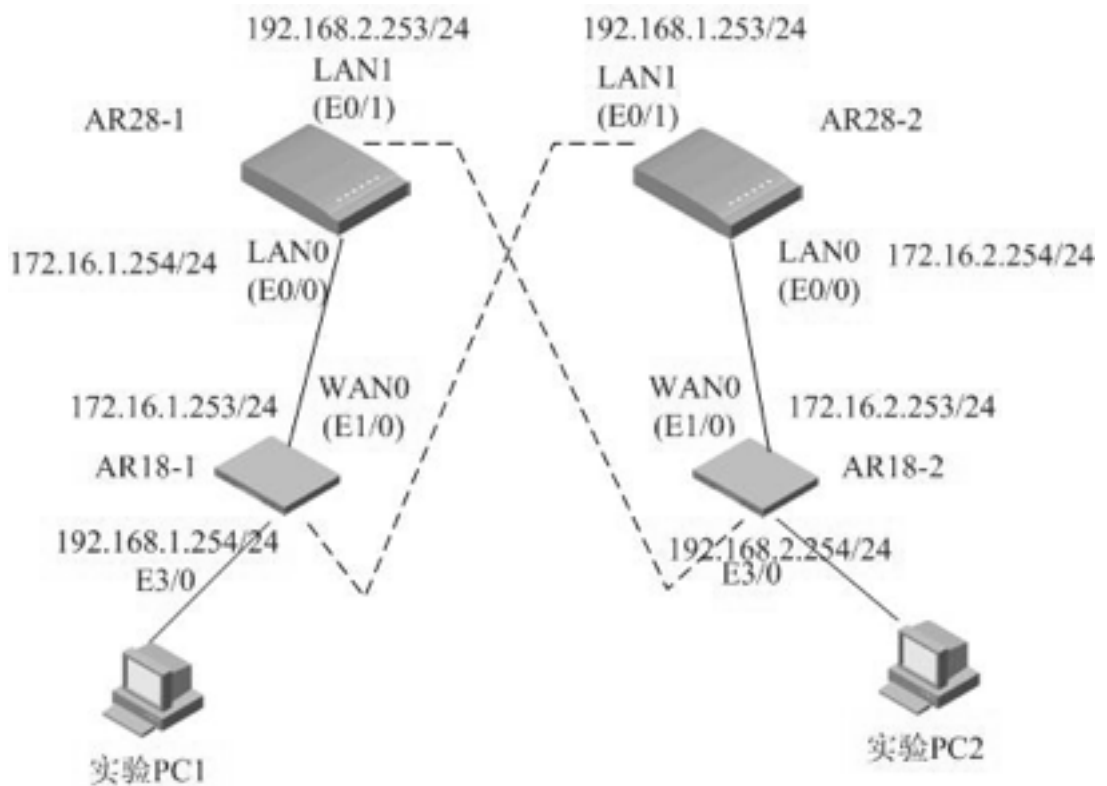
其中实验 PC2 用网线接到 AR18-2 路由器的 1-24 口中的任意一口。

AR28-1 的 LAN1 口用网线接到 AR18-2 路由器的 1-24 口中的任意一口。

AR28-2 的 LAN1 口用网线接到 AR18-1 路由器的 1-24 口中的任意一口。

注意：

AR28 的 LAN0 口与本小组的 AR18 的 WAN0 口相连采用交叉线。



PC1 的网关为 AR18 的 E3/0 的接口地址 192.168.1.254；PC2 的网关为 AR18 的 E3/0 的接口地址 192.168.2.254，子网掩码均为 255.255.255.0。

1) RIP 路由协议实验：

第 1 小组配置：（粗体字部分）

AR18-1 配置：

```

<quidway> Sys //进入系统视图
[quidway] Sysname ar18-1 //更改路由器名字为 ar18-1
[ar18-1] interface e3/0 //进入 e3/0 接口并配置 IP 地址
Ip address 192.168.1.254 255.255.255.0
Rip version 2
Quit
[ar18-1] Interface e1/0 //进入 1/0 接口并配置 IP 地址
Ip address 172.16.1.253 255.255.255.0
Rip version 2

```

Quit

```
[ar18-1] Rip //起用 RIP 路由协议
Network 172.16.1.0 //发布网段 172.16.1.0
Network 192.168.1.0 //发布网段 192.168.1.0
Undo summary //去掉 RIP 协议的自动汇总, RIP
//的自动汇总常常会导致路由故障
```

AR28-1 配置:

```
<quidway> Sys //进入系统视图
[quidway] Sysname ar28-1 //更改路由器名字为 ar28-1
[ar28-1] interface e0/0 //进入 e0/0 接口并配置 IP 地址
Ip address 172.16.1.254 255.255.255.0
Rip version 2
Quit
[ar28-1] Interface e0/1 //进入 e0/1 接口并配置 IP 地址
Ip address 192.168.2.253 255.255.255.0
Rip version 2
Quit
[ar28-1] Rip
Network 172.16.1.0 //发布网段 172.16.1.0
Network 192.168.2.0 //为了方便测试添加的配置
Undo summary
```

第 2 小组配置: (粗体字部分)

AR18-2 配置:

```
<quidway> Sys //进入系统视图
[quidway] Sysname ar18-2 //更改路由器名字为 ar18-2
[ar18-2] interface e3/0 //进入 e3/0 接口并配置 IP 地址
Ip address 192.168.2.254 255.255.255.0
Rip version 2
Quit
```



```
[ar18-2] Interface e1/0 //进入 e1/0 接口并配置 IP 地址
Ip address 172.16.2.253 255.255.255.0
Rip version 2
Quit
```

```
[ar18-2] Rip
Network 172.16.2.0
Network 192.168.2.0
Undo summary
```

AR28-2 配置:

```
<quidway>Sys //进入系统视图
[quidway]Sysname ar28-2 //更改路由器名字为 ar28-2
[ar28-2]interface e0/0 //进入 e0/0 接口并配置 IP 地址
Ip address 172.16.2.254 255.255.255.0
Rip version 2
Quit
[ar28-2]Interface e0/1 //进入 e0/1 接口并配置 IP 地址
Ip address 192.168.1.253 255.255.255.0
Rip version 2
Quit
[ar28-2]Rip
Network 172.16.2.0
Network 192.168.1.0 //为了方便测试添加的配置
Undo summary
```

测试:

- 1、用 `dis ip routing-table` 查看是否有路由信息
- 2、PC1 的网关为 AR18 的 E3/0 的接口地址 192.168.1.254/24, PC2 的网关为 AR18 的 E3/0 的接口地址 192.168.2.254/24, 看 PC1 能否 PING 通 PC2, 这两台 PC 是否可以 PING 通网络中的任何一个接口的 IP 地址。

2) OSPF 路由协议实验:

第 1 小组配置：（粗体字部分）

AR18-1 配置：（粗体字部分）

<quidway>Sys 进入系统视图

[quidway]Sysname ar18-1 //更改路由器名字为 ar18-1

[ar18-1]interface e3/0 //进入 e3/0 接口并配置 IP 地址

Ip address 192.168.1.254 255.255.255.0

Quit

[ar18-1]Interface e1/0 //进入 1/0 接口并配置 IP 地址

Ip address 172.16.1.253 255.255.255.0

Quit

[ar18-1]Router id 1.1.1.1 //为 OSPF 配置路由器 ID (RID) , RID 为每台运行 OSPF 的路由器的标志, 不可以重复。

[ar18-1]ospf //起用 OSPF 协议

area 0 //所有网络在区域 0, 区域 0 是 OSPF 协议的一个特殊的区域, 又叫骨干区域, 当有多个区域时, 不同区域之间的互相连通需要经过区域 0。

Network 172.16.1.0 0.0.0.255 //发布网段 172.16.1.0

Network 192.168.1.0 0.0.0.255 //发布网段 192.168.1.0

AR28-1 配置：（粗体字部分）

<quidway>Sys //进入系统视图

[quidway]Sysname ar28-1 //更改路由器名字为 ar28-1

[ar28-1]interface e0/0 //进入 e0/0 接口并配置 IP 地址

Ip address 172.16.1.254 255.255.255.0

Quit

[ar28-1]Interface e0/1 //进入 e0/1 接口并配置 IP 地址

Ip address 192.168.2.253 255.255.255.0

Quit

[ar28-1]Router id 2.2.2.2

ospf

```
area 0
Network 172.16.1.0 0.0.0.255
Network 192.168.2.0 0.0.0.255 //为了方便测试添加的配置
```

第 2 小组配置：（粗体字部分）

AR18-2 配置：（粗体字部分）

```
<quidway>Sys //进入系统视图
[quidway]Sysname ar18-2 //更改路由器名字为 ar18-2
[ar18-2]interface e3/0 //进入 e3/0 接口并配置 IP 地址
    Ip address 192.168.2.254 255.255.255.0
    Quit
[ar18-2]Interface e1/0 //进入 e1/0 接口并配置 IP 地址
    Ip address 172.16.2.253 255.255.255.0
    Quit

[ar18-2]Router id 3.3.3.3 //为 OSPF 配置 RID，RID 为每台运行
//OSPF 的路由器的标志，不可以重复。

[ar18-2]ospf //起用 OSPF 协议
    area 0 //所有网络在区域 0
    Network 172.16.2.0 0.0.0.255 //发布网段 172.16.2.0
    Network 192.168.2.0 0.0.0.255 //发布网段 192.168.2.0
```

AR28-2 配置：（粗体字部分）

```
<quidway>Sys //进入系统视图
[quidway]Sysname ar28-2 //更改路由器名字为 ar28-2
[ar28-2]interface e0/0 //进入 e0/0 接口并配置 IP 地址
    Ip address 172.16.2.254 255.255.255.0
    Quit
[ar28-2]Interface e0/1 //进入 e0/1 接口并配置 IP 地址
    Ip address 192.168.1.253 255.255.255.0
    Quit

[ar28-2]Router id 4.4.4.4
```

```
ospf
area 0
Network 172.16.2.0 0.0.0.255
Network 192.168.1.0 0.0.0.255    //为了方便测试添加的配置
```

测试：

- 1、看 PC1 能否 PING 通 PC2，这两台 PC 是否可以 PING 通网络中的任何一个接口的 IP 地址。
- 2、用 `dis ip routing-table` 命令查看路由表是否正确。

五、 实验报告要求

弄清楚 RIP 和 OSPF 协议的工作原理，结合实验分析其工作原理。

六、 思考题

能否在路由器上同时配置两种路由协议，如果能配置，哪一种路由协议会生效。

实验三 访问控制列表 (ACL) 配置实验

实验项目名称：访问控制列表 (ACL) 配置实验

实验项目性质：普通实验

所属课程名称：宽带网络技术

实验计划学时：2

一、实验原理

1、ACL 的定义和作用

路由器为了过滤数据包，需要配置一系列的规则，以决定什么样的数据包能够通过，这些规则就是通过访问控制列表 ACL (Access Control List) 定义的。访问控制列表是由 permit | deny 语句组成的一系列有顺序的规则，这些规则根据数据包的源地址、目的地址、端口号等来描述。ACL 通过这些规则对数据包进行分类，这些规则应用到路由器接口上，路由器根据这些规则判断哪些数据包可以接收，哪些数据包需要拒绝。

2、访问控制列表的分类

按照访问控制列表的用途，可以分为四类：

• 基本的访问控制列表 (basic acl)

基本访问控制列表只能使用源地址信息，做为定义访问控制列表的规则的元素。通过简单 acl 命令，可以创建一个基本的访问控制列表，同时进入基本访问控制列表视图，在基本访问控制列表视图下，可以创建基本访问控制列表的规则。

如：`rule 1 deny source 1.1.1.1 0 logging`

• 高级的访问控制列表 (advanced acl)

高级访问控制列表可以使用数据包的源地址信息、目的地址信息、IP 承载的协议类型、针对协议的特性，例如 TCP 的源端口、目的端口，ICMP 协议的类型、代码等内容定义规则。可以利用高级访问控制列表定义比基本访问控制列表更准确、更丰富、更灵活的规则。

如：`rule 1 deny ip source 1.1.1.1 0 destination 2.2.2.1 0`

- **基于接口的访问控制列表 (interface-based acl)**

- **基于 MAC 的访问控制列表 (mac-based acl)**

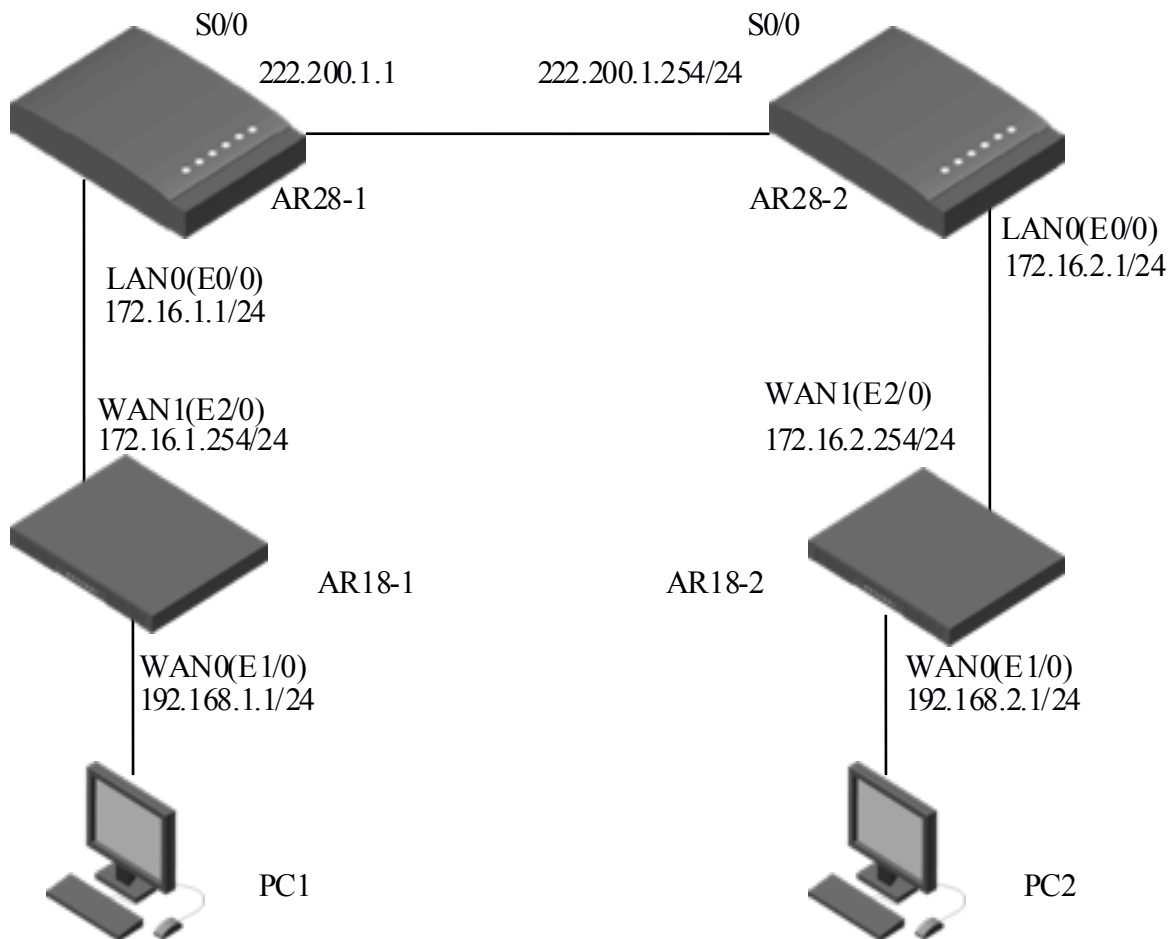
访问控制列表的使用用途是依靠数字的范围来指定的，1000～1999 是基于接口的访问控制列表，2000～2999 范围的数字型访问控制列表是基本的访问控制列表，3000～3999 范围的数字型访问控制列表是高级的访问控制列表，4000～4999 范围的数字型访问控制列表是基于 MAC 地址访问控制列表。

二、 实验内容和要求

- 1、完成拓扑连接，完成对路由器 IP 配置；
- 2、了解高级访问控制列表的原理和配置方法

三、 实验主要仪器设备和材料

需要 AR28 路由器、AR18 路由器，一台 PC 机器各两台，以太网线若干，串行线一套。拓扑图如下：



PC1 的 IP 地址为 192.168.1.254/24, 默认网关为 AR18-1 的 WAN0 地址; PC2 的 IP 地址为 192.168.2.254/24, 默认网关为 AR18-2 的 WAN0 地址。

四、 实验方法、步骤及结果测试

按照拓扑图连线, 注意:

AR28-1 与 AR28-2 的 S0/0 口是用一套串行线相连接的 (接通后可以看到 LINK ACT 0 灯在闪烁)

1、没有配如 ACL 访问控制列表的操作:

(1) 配置 AR18-1 的端口 IP 地址:

```
sys
```

```
[Quidway]sysname AR18-1
```

```
[AR18-1]interface Ethernet 1/0
```

```
[AR18-1-Ethernet1/0]ip address 192.168.1.1 255.255.255.0
[AR18-1-Ethernet1/0]quit
[AR18-1]interface Ethernet 2/0
[AR18-1-Ethernet2/0]ip address 172.16.1.254 255.255.255.0
[AR18-1-Ethernet2/0]quit
```

(2) 配置 AR18-1 的静态路由：

```
[AR18-1]ip route-static 172.16.2.0 255.255.255.0 172.16.1.1
[AR18-1]ip route-static 192.168.2.0 255.255.255.0 172.16.1.1
[AR18-1]ip route-static 222.200.1.0 255.255.255.0 172.16.1.1
[AR18-1]quit
```

(3) 配置 AR28-1 的端口 IP 地址和静态路由

```
<H3C>sys
[H3C]sysname AR28-1
[AR28-1]interface e0/0
[AR28-1-Ethernet0/0]ip address 172.16.1.1 255.255.255.0
[AR28-1-Ethernet0/0]quit
[AR28-1]interface Serial 0/0
[AR28-1-Serial0/0]ip address 222.200.1.1 255.255.255.0
[AR28-1-Serial0/0]quit
[AR28-1]ip route-static 172.16.1.0 255.255.255.0 172.16.1.254
[AR28-1]ip route-static 192.168.1.0 255.255.255.0 172.16.1.254
[AR28-1]ip route-static 172.16.2.0 255.255.255.0 222.200.1.254
[AR28-1]ip route-static 192.168.2.0 255.255.255.0 222.200.1.254
```

(4) 第二组对 AR28-2 与 AR18-2 的配置

```
<H3C>sys
[H3C]sysname AR28-2
[AR28-2]interface Serial 0/0
[AR28-2-Serial0/0]ip address 222.200.1.254 255.255.255.0
[AR28-2-Serial0/0]quit
[AR28-2]interface Ethernet 0/0
[AR28-2-Ethernet0/0]ip address 172.16.2.1 255.255.255.0
[AR28-2-Ethernet0/0]quit
```



```
[AR28-2]ip route-static 172.16.2.0 255.255.255.0 172.16.2.254
[AR28-2]ip route-static 192.168.2.0 255.255.255.0 172.16.2.254
[AR28-2]ip route-static 172.16.1.0 255.255.255.0 222.200.1.1
[AR28-2]ip route-static 192.168.1.0 255.255.255.0 222.200.1.1
[AR28-2]quit
```

<Quidway>sys

```
[Quidway]sysname AR18-2
[AR18-2]interface Ethernet 1/0
[AR18-2-Ethernet1/0]ip address 192.168.2.1 255.255.255.0
[AR18-2-Ethernet1/0]quit
[AR18-2]interface Ethernet 2/0
[AR18-2-Ethernet2/0]ip address 172.16.2.254 255.255.255.0
[AR18-2-Ethernet2/0]quit
[AR18-2]ip route-static 222.200.1.0 255.255.255.0 172.16.2.1
[AR18-2]ip route-static 172.16.1.0 255.255.255.0 172.16.2.1
[AR18-2]ip route-static 192.168.1.0 255.255.255.0 172.16.2.1
[AR18-2]quit
```

测试一：试从 AR18-1 端的 PC 机向对端使用“飞鸽传书”传输数据，和使用 PING 与对方通信。实验效果，实验效果：可以飞鸽传书，可以 PING 通对方的 IP

说明：

飞鸽传书不能自动识别不同网段的主机地址，在和对方通信的时候，需要手动添加对方主机的 IP 地址。设置方式：右键单击右下角飞鸽传书图标，选择“服务设置”，在“局域网外广播设置”的左框填入对方主机的 IP 地址，点击“>>”键，确定即可。

2、在 AR28-1 上配置高级访问控制列表：

```
[AR28-1]firewall enable //防火墙功能启动
[AR28-1]acl number 3000 //创建一个高级访问控制列表 3000
[AR28-1-acl-adv-3000]rule deny tcp source 192.168.1.254 255.255.255.0
destination 192.168.2.254 255.255.255.0 //在高级访问控制列表视图
```

下，配置一个 ACL 规则，阻止从 192.168.1.254 到 192.168.2.254 网络的 TCP 文件包的通信。

```
[AR28-1-acl-adv-3000]quit
[AR28-1]interface Serial 0/0 //将访问控制列表绑定到 S0/0 端口上
```

```
[AR28-1-Serial0/0]firewall packet-filter 3000 outbound //绑定为 S0/0 的出口
[AR28-1-Serial0/0]quit
```

测试二：试从 AR18-1 端的 PC 机向对端使用“飞鸽传书”传输数据，和使用 PING 与对方通信。实验效果：Router A/B 这一组是通过配置 AR28-1 的 ACL，使得与 Router C/D 这一组的 PC 机的飞鸽传书不能传输数据，可以发送聊天信息，可以 PING 通对方 IP。

*若要禁止聊天信息，只需要在高级访问控制列表中添加规则，禁止 UDP 文件包即可。

然后到配置 AR28-2：

```
[AR28-2]firewall enable
[AR28-2]acl number 3000
[AR28-2-acl-adv-3000]rule deny icmp source any destination any //配置
一个 ACL 规则，阻止一切 ICMP（使用 PING 时发送的协议包）的通信，用“any”
代表源地址 0.0.0.0，通配符 255.255.255.255，即所有 IP 地址。
[AR28-2-acl-adv-3000]quit
[AR28-2]interface Serial 0/0
[AR28-2-Serial0/0]firewall packet-filter 3000 outbound
[AR28-2-Serial0/0]quit
```

测试三：试从 AR18-1 端的 PC 机向对端使用“飞鸽传书”传输数据，和使用 PING 与对方通信。实验效果：双方 PC 机不能 PING 通。

五、思考题

试分析交换机中 ACL 配置信息的内容和作用。

实验四 地址转换 (NAT) 的配置实验

实验项目名称：地址转换 (NAT) 的配置实验

实验项目性质：普通实验

所属课程名称：宽带通信网

实验计划学时：2

一、实验原理

1、地址转换概述

如 RFC1631 所描述，NAT (Network Address Translation, 地址转换) 是将 IP 数据报报头中的 IP 地址转换为另一个 IP 地址的过程。在实际应用中，NAT 主要用于实现私有网络访问外部网络的功能。这种通过使用少量的公有 IP 地址代表多数的私有 IP 地址的方式将有助于减缓可用 IP 地址空间枯竭的速度。

说明：

私有地址是指内部网络或主机地址，公有地址是指在因特网上全球唯一的 IP 地址。

RFC 1918 为私有网络预留出了三个 IP 地址块，如下：

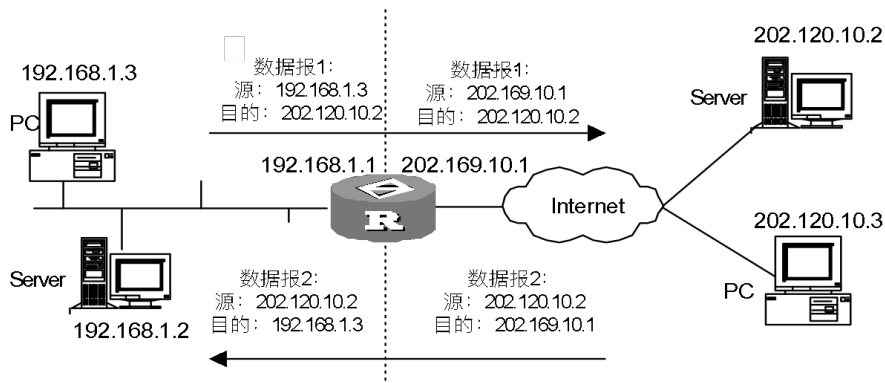
A 类：10.0.0.0~10.255.255.255

B 类：172.16.0.0~172.31.255.255

C 类：192.168.0.0~192.168.255.255

上述三个范围内的地址不会在因特网上被分配，因而可以不必向 ISP 或注册中心申请而在公司或企业内部自由使用。

下图描述了一个基本的 NAT 应用。



地址转换的基本过程

NAT 服务器处于私有网络和公有网络的连接处。当内部 PC (192.168.1.3) 向外部服务器 (202.120.10.2) 发送一个数据报 1 时, 数据报将通过 NAT 服务器。NAT 进程查看报头内容, 发现该数据报是发往外网的, 那么它将数据报 1 的源地址字段的私有地址 192.168.1.3 换成一个可在 Internet 上选路的公有地址 202.169.10.1, 并将该数据报发送到外部服务器, 同时在网络地址转换表中记录这一映射; 外部服务器给内部 PC 发送应答报文 2 (其初始目的地址为 202.169.10.1), 到达 NAT 服务器后, NAT 进程再次查看报头内容, 然后查找当前网络地址转换表的记录, 用原来的内部 PC 的私有地址 192.168.1.3 替换目的地址。

2、多对多地址转换及地址转换的控制

在实际应用中, 我们可能希望某些内部的主机具有访问 Internet (外部网络) 的权利, 而某些主机不允许访问。即当 NAT 进程查看数据报报头内容时, 如果发现源 IP 地址是为那些不允许访问网络的内部主机所拥有的, 它将不进行 NAT 转换。这就是一个对地址转换进行控制的问题。

H3C 系列路由器可以通过定义地址池来实现多对多地址转换, 同时利用访问控制列表来对地址转换进行控制的。

- **地址池**: 用于地址转换的一些公有 IP 地址的集合。用户应根据自己拥有的合法 IP 地址数目、内部网络主机数目以及实际应用情况, 配置恰当的地址池。地址转换的过程中, 将会从地址池中挑选一个地址做为转换后的源地址。

- **利用访问控制列表限制地址转换**: 只有满足访问控制列表条件的数据报文才可以进行地址转换。这可以有效地控制地址转换的使用范围, 使特定主机能够有权利访问 Internet。

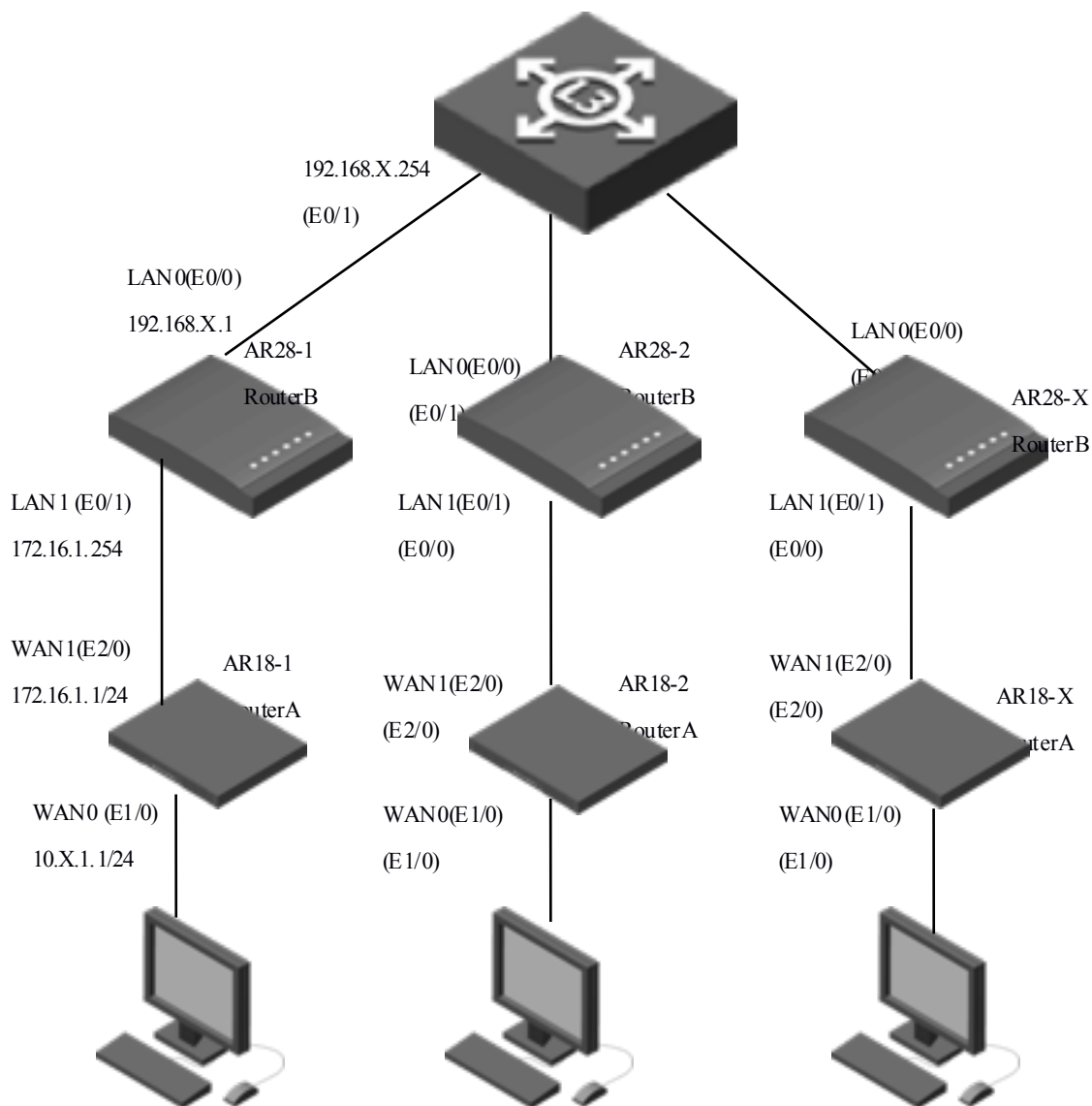
二、 实验内容和要求

- 1、熟悉路由器命令及其配置;
- 2、掌握地址转换 NAT 的原理和配置方法。

三、 实验主要仪器设备和材料

需要 AR28 路由器、AR18 路由器, 一台 PC 机器各一台, 以太网线若干。拓扑图如下:

H3C 3600 核心交换



四、 实验方法、步骤及结果测试

按照拓扑图连线，注意：

H3C 3600 核心交换机为每个小组设置了一个接入的网关地址，为 192.168.X.254，X 为小组号，如第 6 小组，则 3600 上相应的网关为 192.168.6.254，因此需要把实验 PC 和核心 3600 交换机之间的网络配置好，确保实验 PC 和核心 3600 交换机之间的网络连通。

配置 AR28-1 的端口 IP 地址，注意公网跟私网的 IP，公网地址为

192.168.X.1

以第六小组为例子，配置如下：

```
sys
[H3C]sysname AR28-1
[AR28-1]router id 2.2.2.2
[AR28-1]interface Ethernet 0/0
[AR28-1-Ethernet0/0]ip address 192.168.X.1 255.255.255.0
[AR28-1-Ethernet0/0]quit
[AR28-1]interface Ethernet 0/1
[AR28-1-Ethernet0/1]ip address 172.16.1.254 255.255.255.0
[AR28-1-Ethernet0/1]quit
# 使用 OSPF 作为路由选择协议
[AR28-1]ospf 1
[AR28-1-ospf-1]area 0
[AR28-1-ospf-1-area-0.0.0.0]network 0.0.0.0 0.0.0.0
[AR28-1-ospf-1-area-0.0.0.0]quit
[AR28-1-ospf-1]quit
[AR28-1]ip route-static 10.X.1.0 255.255.255.0 172.16.1.1
# 配置地址池和访问控制列表，
[AR28-1]nat address-group 1 192.168.X.5 192.168.X.18
//定义一个地址池 1 公网开始为 192.168.X.5 结束为
192.168.X.18 的连续 IP 地址，这里以 6 小组为例
[AR28-1]acl number 2000 // 创建 ACL 编号 2000
// 进入 ACL 视图
[AR28-1-acl-basic-2000]rule 1 permit //在 ACL 下定义规则
[AR28-1-acl-basic-2000]quit
[AR28-1]interface Ethernet 0/0 //绑定到端口上
[AR28-1-Ethernet0/0]nat outbound 2000 address-group 1
// 将访问控制列表和地址池关联
// 后，即可实现多对多地址转换
[AR28-1-Ethernet0/0]quit
#配置私网内部的路由器 AR18-1
```

```

<Quidway>sys
[Quidway]sysname AR18-1
[AR18-1]router id 1.1.1.1
[AR18-1]interface Ethernet 2/0
[AR18-1-Ethernet2/0]ip address 172.16.1.1 255.255.255.0
[AR18-1-Ethernet2/0]quit
[AR18-1]interface Ethernet 1/0
[AR18-1-Ethernet1/0]ip address 10.X.1.1 255.255.255.0
[AR18-1-Ethernet1/0]quit
[AR18-1]ospf 1
[AR18-1-ospf-1]area 0
[AR18-1-ospf-1-area-0.0.0.0]network 0.0.0.0 0.0.0.0
[AR18-1-ospf-1-area-0.0.0.0]quit
[AR18-1-ospf-1]quit

```

测试：打开 NAT 的 Debug 开关，根据路由器上的 Debug 调试信息，初步定位错误，然后使用其它命令作进一步的判断。调试时，注意观察转换后的源地址，要保证这个地址是希望转换的地址，否则可能会是地址池配置错误。同时要注意想要访问的网络必须要有回到地址池中地址段的路由。注意防火墙以及地址转换本身的访问控制列表对地址转换造成的影响，同时注意路由的配置。在用户视图下：

开始：<AR28-1>debugging nat packet

结束：<AR28-1>terminal debugging

在 PC 机 ping 192.168.X.254（如六小组：192.168.6.254）

得出以下效果（10.6.1.254为第六小组设定 PC 的地址，各小组可自行设定）：

```
<AR28-1>
```

```
*0.1444032 AR28-1 NAT/8/debug:
```

```
(Ethernet0/0-out :)Pro : ICMP
```

```
( 10.6.1.254: 512 - 192.168.6.254: 512) ----->
```

```
( 192.168.6.17: 12288 - 192.168.6.254: 512)
```

```
*0.1444043 AR28-1 NAT/8/debug:
```

```
(Ethernet0/0-in :)Pro : ICMP
```

```

( 192.168.6.254: 512 - 192.168.6.17:12288) ----->
( 192.168.6.254: 512 - 10.6.1.254: 512)
*0.1445031 AR28-1 NAT/8/debug:
(Ethernet0/0-out :)Pro : ICMP
( 10.6.1.254: 512 - 192.168.6.254: 512) ----->
( 192.168.6.17: 12288 - 192.168.6.254: 512)
*0.1445032 AR28-1 NAT/8/debug:
(Ethernet0/0-in :)Pro : ICMP
( 192.168.6.254: 512 - 192.168.6.17:12288) ----->
( 192.168.6.254: 512 - 10.6.1.254: 512)
*0.1446032 AR28-1 NAT/8/debug:
(Ethernet0/0-out :)Pro : ICMP
( 10.6.1.254: 512 - 192.168.6.254: 512) ----->
( 192.168.6.17: 12288 - 192.168.6.254: 512)
*0.1446033 AR28-1 NAT/8/debug:
(Ethernet0/0-in :)Pro : ICMP
( 192.168.6.254: 512 - 192.168.6.17:12288) ----->
( 192.168.6.254: 512 - 10.6.1.254: 512)
*0.1447031 AR28-1 NAT/8/debug:
(Ethernet0/0-out :)Pro : ICMP
( 10.6.1.254: 512 - 192.168.6.254: 512) ----->
( 192.168.6.17: 12288 - 192.168.6.254: 512)
*0.1447032 AR28-1 NAT/8/debug:
(Ethernet0/0-in :)Pro : ICMP
( 192.168.6.254: 512 - 192.168.6.17:12288) ----->
( 192.168.6.254: 512 - 10.6.1.254: 512)

```

五、思考题

试分析如何在实际中利用 NAT 保护内部网络。