杭州中联培训中心

CISCO CCNA 实验指导

课程代号：（640-802）

杭州中联培训中心

二零零七年 十月

地址：杭州市文三路 369 号 1010 室
联系电话：0571-56776040 56776041
网址：http://www.zltrain.com

目录

实验一：认识 CISCO 设备

CISCO 设备描述

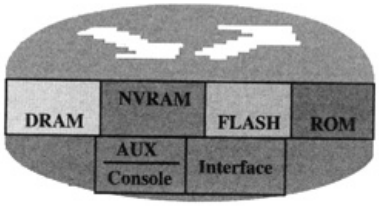
物理端口介绍

CISCO 设备包含以下几种常用端口

- 高速同步串口，最大支持 2.048M 的 E1 速率。通过软件配置，该种端口可以连接 DDN，帧中继（Frame Relay），X.25，PSTN（模拟电话线路）。
- 同步/异步串口，该种端口可以用软件设置为同步工作方式。在同步工作方式下，最大支持 128K，异步方式下，最大支持 115.2K。
- AUI 端口，即粗缆口。一般需要外接转换器（AUI-RJ45），连接 10Base-T 以太网络。
- AUX 端口，该端口为异步端口，最大支持 3 8 4 0 0 的速率，主要用于远程配置或拨号备份。
- Console 口，主要连接终端或运行终端仿真程序的计算机，在本地配置路由器。
- 高密度异步端口，该端口通过一转八线缆，可以连接八条异步线路。

内存体系结构介绍

Cisco 路由器的软件部分即网络操作系统。通过 IOS，Cisco 路由器可以连接 IP，IPX，IBM，DEC，AppleTalk 的网络，并实现许多丰富的网络功能。软件是需要内存的，Cisco 系列路由器的内存体系结构，如图：



ROM 相当于 PC 机的 BIOS，Cisco 路由器运行时首先运行 ROM 中的程序。该程序主要进行加电自检，对路由器的硬件进行检测。

FLASH 是一种可擦写、可编程的 ROM，FLASH 包含 IOS 及微代码。可以把它想象和 PC 机的硬盘功能一样，但其速度快得多。

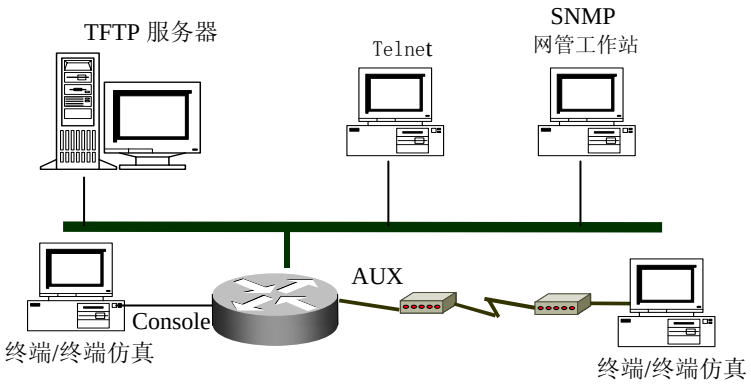
DRAM：动态内存。该内存中的内容在系统掉电时会完全丢失。DRAM 中主要包含路由表，ARP 缓存，fast-switch 缓存，数据包缓存等。DRAM 中也包含有正在执行的路由器配置文件。

NVRAM：NVRAM 中包含有路由器配置文件，NVRAM 中的内容在系统掉电时不会丢失。

一般地，路由器启动时，首先运行 ROM 中的程序，进行系统自检及引导，然后运行 FLASH 中的 IOS，并在 NVRAM 中寻找路由器的配置，并将装入 DRAM 中。

配置途径

一台新路由器买来，不象ＨＵＢ或一般的交换机插上线路就能用，需要根据所连接的网络用户的需求进行一定的设置才能使用。



可以通过多种途径配置 Cisco 路由器，如上图：

1、通过 console 进行设置，这种方式是用户对路由器的主要设置方式。

2、通过 AUX 端口连接 Modem 进行远程配置。

3、通过 Telnet 方式进行配置。可以在网络中任一位置对路由器进行配置.

4、通过网管工作站进行配置，这就需要在您的网络中有至少一台运行 Ciscoworks 及 CiscoView 等的网管工作站。

5、通过 tftp 服务器下载路由器配置文件。

CONSOLE 配置连接

用串口对 CISCO 设备进行配置是我们在工作中最基本的方法。用串口配置时需要用专用配置电缆连接到设备的的 CONSOLE 口和主机的串口：具体操作步骤如下：

1、 接串口配置线缆，如果已经连接，请确认连接的主机串口是 com1 还是 com2；

2、 建超级终端会话，windows 的附件中都有此软件；

3、 选择通信串口（com1 或 com2）；

4、 配置串口工作参数；(但路由器的第一次设置必须通过第一种方式进行, 此时终端的硬件设置如下:

波特率 ：9600

数据位 ：8

停止位 ：1

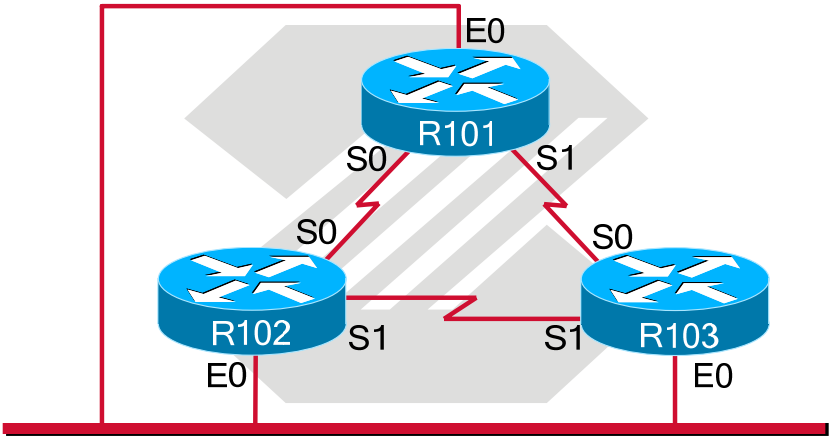
奇偶校验：无

具体配置界面如下：

注：一般设置为还原为默认值即可

使用中联实验机架

中联 CCNA 实验设备共分 4 组，结构一致，以下以第一组为例，其他组的设备将设备名称第一位数字改成相应的组号即可。实验拓扑图如下：



使用方法：

1. 连接配置服务器

终端服务器登录地址：

CCNA01	192．168．1．227
CCNA02	192．168．1．228
CCNA03	192．168．1．229
CCNA04	192．168．1．230

终端服务器登录口令：

小写 cisco

登陆方式：在命令行下使用 telnet *终端服务器地址*

输入口令

提示符为 CCNA> 表示登陆成功

2. 通过 CONSOLE 连入相应的设备

在 CCNA>提示符下输入相应的设备名称，配置服务器将自动通过 Console 线路连接到设备

注：登陆下一台设备重复 1.2 步即可。

实验二：CISCO 设备基本命令认识

命令状态

1. router>

路由器处于用户命令状态，这时用户可以看路由器的连接状态，访问其它网络和主机，但不能看到和更改路由器的设置内容。

2. router#

在 router>提示符下键入 enable,路由器进入特权命令状态 router#,这时不但可以执行所有的用户命令，还可以看到和更改路由器的设置内容。

3. router(config)#

在 router#提示符下键入 configure terminal,出现提示符 router(config)#，此时路由器处于全局设置状态，这时可以设置路由器的全局参数。

4. router(config-if)#;

router(config-line)#;

router(config-router)#;...

路由器处于局部设置状态，这时可以设置路由器某个局部的参数。

5. >

路由器处于 ROM Monitor 状态，在开机后 60 秒内按 ctrl-break 可进入此状态，这时路由器不能完成正常的功能，只能进行软件升级和手工引导。

6. 设置对话状态

这是一台新路由器开机时自动进入的状态，在特权命令状态使用 SETUP 命令也可进入此状态，这时可通过对话方式对路由器进行设置。

常用命令

帮助

在 IOS 操作中，无论任何状态和位置，都可以键入“？”得到系统的帮助。

改变命令状态

任务	命令
进入特权命令状态	enable
退出特权命令状态	disable
进入设置对话状态	setup
进入全局设置状态	config terminal
退出全局设置状态	end
进入端口设置状态	interface *type slot/number*
进入子端口设置状态	interface *type number.subinterface* [point-to-point | multipoint]
进入线路设置状态	line *type slot/number*
进入路由设置状态	router *protocol*
退出局部设置状态	exit

显示命令

任务	命令
查看版本及引导信息	show version
查看运行设置	show running-config
查看开机设置	show startup-config
显示端口信息	show interface *type slot/number*
显示路由信息	show ip route

拷贝命令

用于 IOS 及 CONFIG 的备份和升级

确认配置正确无误后将配置文件复制到 NVRAM 中去。其命令为 copy running-config startup-config

如果想用 NVRAM 中的配置覆盖 DRAM 中的配置用命 copy startup-config running-config

可以将 NVRAM 中的配置复制到 tftp 服务器中进行备份，用命令 copy startup-config tftp

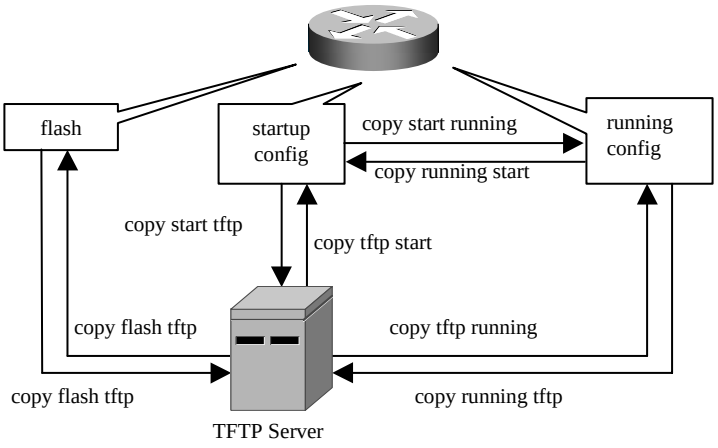
也可以将 DRAM 中的配置复制到 tftp 服务器中进行备份,用命令 copy running-config tftp 路由器会询问你的 tftp 服务器的 IP 地址及以何文件名存盘，输入正确的服务器 IP 地址和文件名后，即可。

可以将 tftp 中的配置文件复制到路由器的 DRAM 中，用命令 copy tftp running-config

可以将 tftp 中的配置文件复制到路由器 NVRAM 中，用命令 copy tftp startup-config 路由器会询问 tftp 服务器根目录下的配置文件名及在路由器上以什么名字复制该配置文件。

如果想删除 NVRAM 中的所有配置，用命令 erase nvram

各命令用途如下图：



网络命令

任务	命令
登录远程主机	telnet *hostname/IP address*
网络侦测	ping *hostname/IP address*
路由跟踪	traceroute *hostname/IP address*

在超级权限模式下

1、 ping 目地地址

或

ping 回车，

通过提示进行扩展的ping，通过ping可以检测下三层，即物理层，数据链路层，IP层是否工作正常。

2、 traceroute 目地地址

可以跟踪数据通过哪一条路径到达目地

3、 telnet 目地地址

可以检测应用层是否工作正常

基本设置命令

任务	命令
全局设置	config terminal
设置访问用户及密码	username *username* password *password*
设置特权密码	enable secret password
设置路由器名	hostname *name*
设置静态路由	ip route destination subnet-mask next-hop
启动 IP 路由	ip routing
启动 IPX 路由	ipx routing
端口设置	interface type slot/number
设置 IP 地址	ip address address subnet-mask
设置 IPX 网络	ipx network *network*
激活端口	no shutdown
物理线路设置	line type number
启动登录进程	login [local|tacacs server]
设置登录密码	password *password*

全局设置模式

全局设置上可以设置一些全局性的参数，要进入全局设置模式，必须首先进入特权模式，然后，在特权模式下键 入 configure terminal 回车即进入全局设置模式。

其缺省提示符为

Router (config)#

如果设置了路由器的名字,则其提示符为

路由器的名字(config)#

这里先介绍几个配置命令

配置路由器的名字

hostname 路由器的名字

设置进入特权模式时的口令

enable password 口令字符串

或

enable secret 口令字符串

其中用 enable password 设置的口令没有进行加密的，可以查看到口令字符串：用 enable secret 设置的口令是加密的，设置后无法查看到口令字符串。

注意:设置口令后，一定不要忘记，否则，要进入特权模式会带来麻烦，在某些情况下，除非重新回忆起口令，否则，你就无法进入特权模式。

其他设置模式

这里主要介绍几种其它设置模式。

要进入其它设置模式，首先必须进入全局设置模式

端口设置模式

在全局设置模式下：

interface 端口号

2500 及 1600 系列的端口主要有

- interface serial 号码

  高速同步串口的号码由 0 开始

- interface ethernet 号码
  以太口的号码由 0 开始
- line console 0
  配置 console 口
  为安全起见，可以配置口令，配置如下
  line con 0
  login
  passwprd 口令字符串

实验三：IP 协议配置

实验目的：通过对直连链路的简单配置，使直连链路可以连通。（能 PING 通即可）

规则：

1、一般地，路由器的物理网络端口通常要有一个IP地址

2、相邻路由器的相邻端口IP地址必须在同一IP网络上

3、同一路由器的不同端口的IP地址必须在不同IP网段上

4、除了相邻路由器的相邻端口外，所有网络中路由器所连接的网段即所有路由器的任何两个非相邻端口都必须不在同一网段上。

IP协议配置的主要任务：

1、配置端口IP地址

2、配置广域网线路协议

3、配置路由

4、其它设置

配置端口 IP 地址

为端口设置一个IP地址，在**端口设置**状态下

ip address 本端口IP地址 子网掩码

另外，在同一端口中可以设置两个以上的不同网段的IP地址，这样可以实现连接在同一局域网上不同网段之间的通讯。一般由于一个网段对于用户来说不够用，可以采用这种办法。

在端口设置状态下

ip address 本端口IP地址 子网掩码 secondary

配置 IP 广域网络链路封装

Cisco HDLC 协议配置

ISO HDLC协议由IBM SDLC协议演化过来，ISO HDLC 采用SDLC的帧格式，支持同步，全双工操作，ISO GDLC分为物理层及LLC （逻辑链路子层）二层。

但Cisco HDLC无LLC层，这意味着Cisco HDLC对上层数据只进行物理帧封装，没有任何应答机制，重传机制，所有的纠错处理由上层协议处理。

在Cisco路由器之间用同步专线连接时，采用Cisco HDLC比采用PPP协议效率高得多，但是，如果将Cisco路由器与非Cisco路由器进行同步专线连接时，不能用Cisco HDLC，因为它们不支持Cisco HDLC，可以采用PPP协议。

建议：●在DDN专线上，Cisco 路由器之间采用Cisco HDLC协议。

●Cisco路由器与非Cisco路由器之间采用PPP协议。

注意：Cisco系列同步串口，缺省状态下为HDLC封装，同步/异步串口缺省状态为同步工作方式HDLC封装，因此，一般地无需显示封装HDLC。

配置步骤：

在端口配置状态下：

- 封装HDLC

  encapsulation hdlc
- 配置端口IP地址及掩码

  ip address IP 地址 子网掩码
- 如果本端口连接的是DCE线缆，则要设同步时钟

  clock rate 时钟频率

注意：在实际应用中，Cisco 路由器接DDN专线时，同步串口需通过V.35或RS232 DTE线缆连接CSU/DSU，则Cisco 路由器为DTE，CSU/DSU为DCE，由CSU/DSU提供时钟，因此无须设置同步时钟。如果将二台路由器通过V.35或RS232线缆进行直连时，则必须由连接DCE线缆的一方提供同步时钟，如果路由器为DCE，则必须配置。

CISCO 系列产品高速同步串口最高可支持到2M，同步/异步串口同步方式下支持128K，异步方式下支持115.2K。

PPP 协议设置

配置步骤

- 在端口设置状态下，封装PPP协议

  encapsulation ppp
- 设置本端口IP地址

  ip address 本端口IP地址 子网掩码

帧中继（Frame Relay）配置

帧中继设置中可分为DCE端和DTE设置，在实际应用中，Cisco路由器为DTE端，通过V.35线缆连接CSU/DSU，如果将两个路由器通过V.35线缆直连，连接V.35 DCE线缆的路由器充当DCE的角色，并且需要提供同步时钟。

DTE端配置

- 在端口配置中，封装帧中继

  encapsulation frame-relay ietf

  Cisco路由器缺省为帧中继数据包封装格式为IETF，可以不用显示设置，另外，国内帧中继线路一般为IETF格式的封装，如果不同，请与当地电信管理部门联系，采用其它装格式。
- 设置LMI信令格式

  frame-relay lmi-type Cisco

  Cisco路由器缺省的LMI信令格式为Cisco，可以不用设置，国内帧中继线路一般采用Cisco的LMI信令格式。如果不同，请与当地电信管理部门联系，采用相应的LMI信令格式。
- 映射IP地址与帧中继地址

  frame-relay map ip 对方路由器的IP 地址 本端口的帧中继号码{broadcast}

  broadcast参数表示允许在帧中继线路上传送路由广播信息
- 设置带宽

bandwith 带宽 单位为K

注：这条命令会影响路由选择操作，如IGRP协议，因为它用于定义链路的度量值

- 本端口IP地址

  ip address 本端口IP地址 子网掩码

充当DCE端的路由器设置(模拟为帧中继交换机)

- 在全局配置状态下，打开帧中继交换

  frame-relay switching

- 在端口设置状态下，封装帧中继

  encapsulation frame-relay IETF

- 设置本端口在帧中继线路中充当DCE

  frame-relay intf-type DCE

- 在端口模式下，建立DLCI值到出站端口的映射表，并打上新的DLCI值。

frame-relay route *DLCI1* interface 出站接口 *DLCI2*

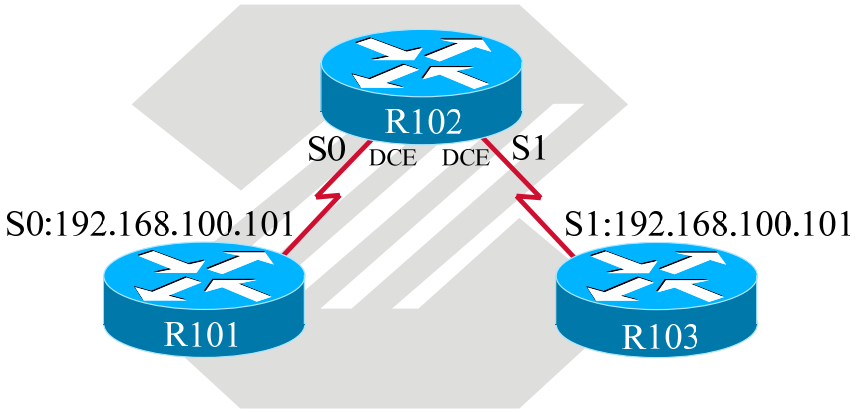
其中DLCI1为进入端口的DLCI值，即本端口所连路由器发出数据包所打上的DLCI值

DLCI2为出站时的打上的DLCI值，即出站端口所连接路由器发出数据包所打上的DLCI值

- 设置同步时钟

  clock rate 同步时钟

  举例：



在此实例中，将使用机架中的组一的三台路由器来验证帧中继的配置。

其中R102作为帧中继交换机。R101流出的数据包的DLCI号为103，R103流出的数据包的DLCI号为301

配置命令如下：

R101的配置：

```
R101#conf t
R101(config)#int s0
R101(config-if)#ip add 192.168.100.101 255.255.255.0
R101(config-if)#encapsulation frame-relay ietf
R101(config-if)#frame-relay map ip 192.168.100.103 103 broadcast
R101(config-if)#no shut
```

R103的配置：

```
R103#conf t
R103(config)#int s1
R103(config-if)#ip add 192.168.100.103 255.255.255.0
```

```
R103(config-if)#encapsulation frame-relay ietf
R103(config-if)#frame-relay map ip 192.168.100.101 301 broadcast
R103(config-if)#no shut
R102的配置：
R102(config)#frame-relay switching
R102(config)#int s0
R102(config-if)#enc frame-relay
R102(config-if)# frame-relay intf-type dce
R102(config-if)# frame-relay route 103 interface Serial 1 301
R102(config-if)#no shut
R102(config)#int s1
R102(config-if)#enc frame-relay
R102(config-if)# frame-relay intf-type dce
R102(config-if)# frame-relay route 301 interface Serial 0 103
R102(config-if)#no shut
```

注意：如果通过直连方式将两路由器连接起来，则两路由器的帧中继地址必须一致，地址可以随意设置。在实际应用中，申请的帧中继地址只有本地意义，两边进行通讯的路由器的帧中继地址可以不同。

实验四：IP 路由协议配置

CISCO 路由器上可以配置以下三种路由

1. 静态路由
2. 动态路由
3. 缺省路由

静态路由

通过配置静态路由，用户可以人为地指定对某一网络访问时所要经过的路径,在网络结构比较简单，且一般到达某一网络所经过的路径唯一的情况下采用静态路由。

任务	命令
建立静态路由	**ip route** *prefix mask {address | interface}* [*distance*] [**tag** *tag*] [**permanent**]

Prefix :所要到达的目的网络
mask :子网掩码
address :下一个跳的 IP 地址，即相邻路由器的端口地址。
interface :本地网络接口
distance :管理距离（可选）
tag *tag* :tag 值（可选）
permanent :指定此路由即使该端口关掉也不被移掉。

配置举例：

实验目的：使所有网络都能够正常通信。

拓扑结构：

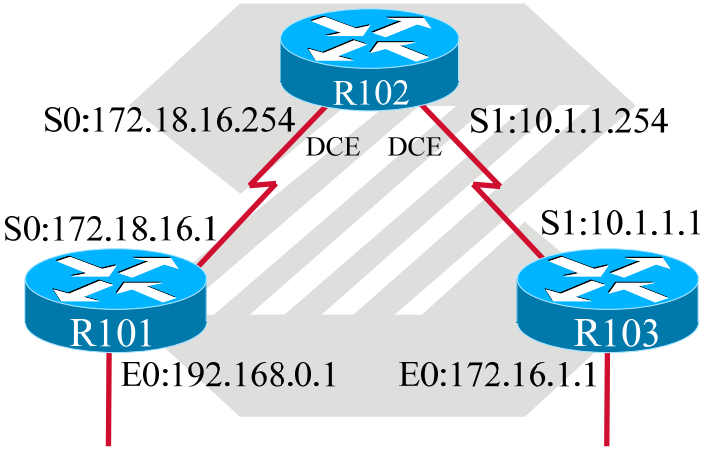


图 4-1 路由协议实验拓扑

路由器R101 配置：

```
router>enable
router#conf t
router(config)#hostname r101
r101(config)#enable password cisco
r101(config)#int s0
r101(config-if)#ip add 172.18.16.1 255.255.255.0
r101(config-if)#no shut
r101(config-if)#int e0
r101(config-if)#ip add 192.168.0.1 255.255.255.0
r101(config-if)#exit
r101(config)#ip router 10.1.1.0 255.255.255.0 172.18.16.254
r101(config)#ip router 172.16.1.0 255.255.255.0 172.18.16.254
r101(config)#line vty 0 4
r101(config-line)#password cisco
r101(config-line)#login
r101(config-line)#exit
r101(config)#exit
r101#wri
```

路由器R102 配置：

```
router>enable
router#conf t
router(config)#hostname r102
r102(config)#enable password cisco
r102(config)#int s0
r102(config-if)#ip add 172.18.16.254 255.255.255.0
r102 (config-if)#clock rate 64000
r102(config-if)#no shut
```

```
r102(config-if)#int s1
r102(config-if)#ip add 10.1.1.254 255.255.255.0
r102(config-if)#clock rate 64000
r102(config-if)#exit
r102(config)#ip router 192.168.0.0 255.255.255.0 172.18.16.1
r102(config)#ip router 172.16.1.0 255.255.255.0 10.1.1.1
r102(config)#line vty 0 4
r102(config-line)#password cisco
r102(config-line)#login
r102(config-line)#exit
r102(config)#exit
r102#wri
```

路由器R103 配置：

```
router>enable
router#conf t
router(config)#hostname r103
r103(config)#enable password cisco
r103(config)#int s0
r103(config-if)#ip add 10.1.1.1 255.255.255.0
r103(config-if)#no shut
r103(config-if)#int e0
r103(config-if)#ip add 172.16.1.1 255.255.255.0
r103(config-if)#exit
r103(config)#ip router 192.168.0.0 255.255.255.0 10.1.1.254
r103(config)#ip router 172.18.16.0 255.255.255.0 10.1.1.254
r103(config)#line vty 0 4
r103(config-line)#password cisco
r103(config-line)#login
r103(config-line)#exit
r103(config)#exit
r103#wri
```

连通性测试：

```
R101#ping 10.1.1.1
R101#ping 172.16.1.1
R102#ping 192.168.0.1
R102#ping 172.16.1.1
R103#ping 172.18.16.1
R103#ping 192.168.0.1
```

默认路由

在全局配置模式下

```
ip route 0.0.0.0  0.0.0.0  相邻路由器的相邻端口地址或本地物理端口号
```

注：静态路由中只能在点对点链路上使用流出端口

动态路由

RIP 协议

RIP(Routing information Protocol)是应用较早、使用较普遍的内部网关协议(Interior Gateway Protocol,简称 IGP)，适用于小型同类网络，是典型的距离向量(distance-vector)协议。文档见 RFC1058、RFC1723。

RIP 通过广播 UDP 报文来交换路由信息，每 30 秒发送一次路由信息更新。RIP 提供跳跃计数(hop count)作为尺度来衡量路由距离，跳跃计数是一个包到达目标所必须经过的路由器的数目。如果到相同目标有二个不等速或不同带宽的路由器，但跳跃计数相同，则 RIP 认为两个路由是等距离的。RIP 最多支持的跳数为 15，即在源和目的网间所要经过的最多路由器的数目为 15，跳数 16 表示不可达。

1.有关命令

任务	命令
指定使用 RIP 协议	router rip
指定 RIP 版本	version {1|2}[1]
指定与该路由器相连的网络	network *network*

注：1、Cisco 的 RIP 版本 2 支持验证、密钥管理、路由汇总、无类域间路由(CIDR)和变长子网掩码(VLSMs)

2.举例

拓扑如图 4-1

路由器R101 配置：

```
router>enable
router#conf t
router(config)#hostname r101
r101(config)#enable password cisco
r101(config)#int s0
r101(config-if)#ip add 172.18.16.1 255.255.255.0
r101(config-if)#no shut
r101(config-if)#int e0
r101(config-if)#ip add 192.168.0.1 255.255.255.0
r101(config-if)#exit
r101(config)#router rip
r101(config-router)#network 192.168.0.0
r101(config-router)#network 172.18.0.0
r101(config-router)#exit
r101(config)#line vty 0 4
r101(config-line)#password cisco
r101(config-line)#login
r101(config-line)#exit
r101(config)#exit
r101#wri
```

路由器R102 配置：

```
router>enable
router#conf t
```

```
router(config)#hostname r102
r102(config)#enable password cisco
r102(config)#int s0
r102(config-if)#ip add 172.18.16.254 255.255.255.0
r102 (config-if)#clock rate 64000
r102(config-if)#no shut
r102(config-if)#int s1
r102(config-if)#ip add 10.1.1.254 255.255.255.0
r102(config-if)#clock rate 64000
r102(config-if)#exit
r102(config)#router rip
r102(config-router)#network 172.18.0.0
r102(config-router)#network 10.0.0.0
r102(config-router)#exit
r102(config)#line vty 0 4
r102(config-line)#password cisco
r102(config-line)#login
r102(config-line)#exit
r102(config)#exit
r102#wri
```

路由器R103 配置：

```
router>enable
router#conf t
router(config)#hostname r103
r103(config)#enable password cisco
r103(config)#int s0
r103(config-if)#ip add 10.1.1.1 255.255.255.0
r103(config-if)#no shut
r103(config-if)#int e0
r103(config-if)#ip add 172.16.1.1 255.255.255.0
r103(config-if)#exit
r103(config)#router rip
r103(config-router)#network 172.16.0.0
r103(config-router)#network 10.0.0.0
r103(config-router)#exit
r103(config)#line vty 0 4
r103(config-line)#password cisco
r103(config-line)#login
r103(config-line)#exit
r103(config)#exit
r103#wri
```

相关调试命令：

```
show ip protocol
show ip route
```

连通性测试：

```
R101#ping 10.1.1.1
R101#ping 172.16.1.1
R102#ping 192.168.0.1
R102#ping 172.16.1.1
R103#ping 172.18.16.1
R103#ping 192.168.0.1
```

EIGRP 协议

1.有关命令

任务	命令
指定使用 RIP 协议	router eigrp *autonomous-system*[1]
指定与该路由器相连的网络	network *network*
指定与该路由器相邻的节点地址	neighbor *ip-address*

注：1、*autonomous-system* 可以随意建立，并非实际意义上的 *autonomous-system*,但运行 IGRP 的路由器要想交换路由更新信息其 *autonomous-system* 需相同。

2. 举例

拓扑如图 4-1

路由器R101 配置：

```
router>enable
router#conf t
router(config)#hostname r101
r101(config)#enable password cisco
r101(config)#int s0
r101(config-if)#ip add 172.18.16.1 255.255.255.0
r101(config-if)#no shut
r101(config-if)#int e0
r101(config-if)#ip add 192.168.0.1 255.255.255.0
r101(config-if)#exit
r101(config)#router eigrp 10
r101(config-router)#network 192.168.0.0
r101(config-router)#network 172.18.0.0
r101(config-router)#exit
r101(config)#line vty 0 4
r101(config-line)#password cisco
r101(config-line)#login
r101(config-line)#exit
r101(config)#exit
r101#wri
```

路由器R102 配置：

```
router>enable
router#conf t
router(config)#hostname r102
r102(config)#enable password cisco
r102(config)#int s0
r102(config-if)#ip add 172.18.16.254 255.255.255.0
r102 (config-if)#clock rate 64000
r102(config-if)#no shut
r102(config-if)#int s1
r102(config-if)#ip add 10.1.1.254 255.255.255.0
r102(config-if)#clock rate 64000
r102(config-if)#exit
r102(config)#router eigrp 10
r102(config-router)#network 172.18.0.0
r102(config-router)#network 10.0.0.0
r102(config-router)#exit
r102(config)#line vty 0 4
r102(config-line)#password cisco
r102(config-line)#login
r102(config-line)#exit
r102(config)#exit
r102#wri
```

路由器R103 配置：

```
router>enable
router#conf t
router(config)#hostname r103
r103(config)#enable password cisco
r103(config)#int s0
r103(config-if)#ip add 10.1.1.1 255.255.255.0
r103(config-if)#no shut
r103(config-if)#int e0
r103(config-if)#ip add 172.16.1.1 255.255.255.0
r103(config-if)#exit
r103(config)#router eigrp 10
r103(config-router)#network 172.16.0.0
r103(config-router)#network 10.0.0.0
r103(config-router)#exit
r103(config)#line vty 0 4
r103(config-line)#password cisco
r103(config-line)#login
r103(config-line)#exit
r103(config)#exit
r103#wri
```

相关调试命令：

```
show ip protocol
show ip route
```

连通性测试：

连通性测试：

```
R101#ping 10.1.1.1
R101#ping 172.16.1.1
R102#ping 192.168.0.1
R102#ping 172.16.1.1
R103#ping 172.18.16.1
R103#ping 192.168.0.1
```

OSPF 协议

OSPF(Open Shortest Path First)是一个内部网关协议(Interior Gateway Protocol,简称 IGP)，用于在单一自治系统(autonomous system,AS)内决策路由。与 RIP 相对，OSPF 是链路状态路由协议，而 RIP 是距离向量路由协议。

链路是路由器接口的另一种说法，因此 OSPF 也称为接口状态路由协议。OSPF 通过路由器之间通告网络接口的状态来建立链路状态数据库，生成最短路径树，每个 OSPF 路由器使用这些最短路径构造路由表。

文档见 RFC2178。

1. 有关命令

全局设置

任务	命令
指定使用 OSPF 协议	router ospf *process-id*[1]
指定与该路由器相连的网络	network *address wildcard-mask* area *area-id*[2]
指定与该路由器相邻的节点地址	neighbor *ip-address*

注：1、OSPF 路由进程 *process-id* 必须指定范围在 1-65535，多个 OSPF 进程可以在同一个路由器上配置，但最好不这样做。多个 OSPF 进程需要多个 OSPF 数据库的副本，必须运行多个最短路径算法的副本。*process-id* 只在路由器内部起作用，不同路由器的 *process-id* 可以不同。

2、*wildcard-mask* 是子网掩码的反码，网络区域 ID *area-id* 在 0-4294967295 内的十进制数，也可以是带有 IP 地址格式的 x.x.x.x。当网络区域 ID 为 0 或 0.0.0.0 时为主干域。不同网络区域的路由器通过主干域学习路由信息。

2. 举例

实验拓扑见图4-1

路由器R101 配置：

```
router>enable
router#conf t
router(config)#hostname r101
r101(config)#enable password cisco
r101(config)#int s0
r101(config-if)#ip add 172.18.16.1 255.255.255.0
```

```
r101(config-if)#no shut
r101(config-if)#int e0
r101(config-if)#ip add 192.168.0.1 255.255.255.0
r101(config-if)#int loopback 0
r101(config-if)#ip add 1.1.1.1 255.255.255.255
r101(config-if)#exit
r101(config)#router ospf 10
r101(config-router)#router-id 1.1.1.1
r101(config-router)#network 192.168.0.0 0.0.0.255 area 0
r101(config-router)#network 172.18.0.0 0.0.0.255 area 0
r101(config-router)#exit
r101(config)#line vty 0 4
r101(config-line)#password cisco
r101(config-line)#login
r101(config-line)#exit
r101(config)#exit
r101#wri
```

路由器R102 配置：

```
router>enable
router#conf t
router(config)#hostname r102
r102(config)#enable password cisco
r102(config)#int s0
r102(config-if)#ip add 172.18.16.254 255.255.255.0
r102 (config-if)#clock rate 64000
r102(config-if)#no shut
r102(config-if)#int s1
r102(config-if)#ip add 10.1.1.254 255.255.255.0
r102(config-if)#clock rate 64000
r101(config-if)#int loopback 0
r101(config-if)#ip add 2.2.2.2 255.255.255.255
r102(config-if)#exit
r102(config)#router ospf 10
r102(config-router)#router-id 2.2.2.2
r102(config-router)#network 172.18.0.0 0.0.0.255 area 0
r102(config-router)#network 10.0.0.0 0.0.0.255 area 0
r102(config-router)#exit
r102(config)#line vty 0 4
r102(config-line)#password cisco
r102(config-line)#login on
r102(config-line)#exit
r102(config)#exit
r102#wri
```

路由器R103 配置：

```
router>enable
router#conf t
router(config)#hostname r103
r103(config)#enable password cisco
r103(config)#int s0
r103(config-if)#ip add 10.1.1.1 255.255.255.0
r103(config-if)#no shut
r103(config-if)#int e0
r103(config-if)#ip add 172.16.1.1 255.255.255.0
r101(config-if)#int loopback 0
r101(config-if)#ip add 3.3.3.3 255.255.255.255
r103(config-if)#exit
r103(config)#router ospf 10
r101(config-router)#router-id 3.3.3.3
r103(config-router)#network 172.16.0.0 0.0.0.255 area 0
r103(config-router)#network 10.0.0.0 0.0.0.255 area 0
r103(config-router)#exit
r103(config)#line vty 0 4
r103(config-line)#password cisco
r103(config-line)#login
r103(config-line)#exit
r103(config)#exit
r103#wri
```

相关调试命令：

```
show ip protocol
show ip route
show ip ospf database
show ip ospf neighbour
```

连通性测试：

```
R101#ping 10.1.1.1
R101#ping 172.16.1.1
R102#ping 192.168.0.1
R102#ping 172.16.1.1
R103#ping 172.18.16.1
R103#ping 192.168.0.1
```

实验五：访问控制列表

访问控制列表（ACL）是应用在路由器接口的指令列表。随着网络应用及技术的日益发展，在一些核心的路由交换机，甚至边缘交换机上也应用了这一技术，以期在网络的各个部分实现分布式的有效的控制。ACL 指令列表用来告诉路由器（交换机）哪些数据报可以接收、哪一些需要拒绝。至于是接收还是被拒绝，可以由类似源地址、目的地址、端口号等的特定条件来决定。

ACL 通过在访问控制列表中对目的地址进行归类，来管理通信流量和处理待定的数据包。归类处理每个特定接口的 ACL ，从而通过该接口的所有通信流量都要按照 ACL 所指定的条件接受检测。

ACL 适用于所有的路由协议， 如 IP、IPX 等。当这些协议的数据包经过路由器（交换机）时，都可以利用 ACL 来过滤它们。可以在路由器（交换机）上配置 ACL ，用来控制对某一网络或子网的访问。ACL 通过在路由器（交换机）接口处控制数据包是被转发还是被阻塞来过滤网络通信流量。路由器（交换机）根据 ACL 中指定的条件来检测通过的每个数据包。这个条件既可以是数据包的源地址，也可以是目的地址，还可以是上层协议或其他因素。

ACL 的定义是基于所有协议的。换言之，如果想要控制某种协议的通信数据流，那么必须要对该接口处的这种协议定义单独的 ACL（对有些协议来说，ACL 就像一个过滤器）。例如，要把路由器（交换机）接口配置成支持 3 种协议，那么你至少要定义 3 个访问控制列表。通过灵活的增加访问控制列表，ACL 可以当作一种网络控制的有力工具，用来过滤进出路由器（交换机）接口的数据包。

建立 ACL 可以用来：

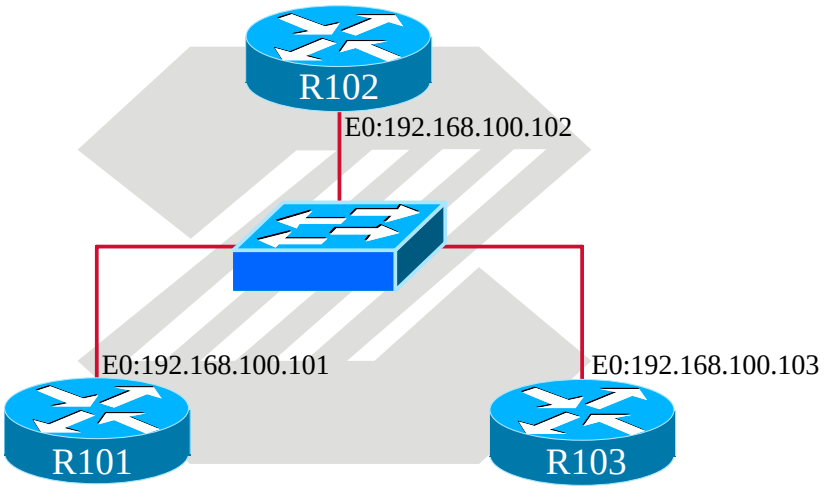
- 限制网络流量，提高网络性能
- 提供对网络流量的控制手段
- 提供网络访问的基本安全手段
- 在路由器接口处，决定哪种类型的通信流量被转发，哪种被阻塞

实验举例：

1）标准访问控制列表

预期效果：在使用标准访问控制列表，让 R101 可以访问 R102，而 R103 不能访问 R102。

拓扑图：



首先做好基本配置，并测试连通性：

R101 上的配置：

```
R101#conf t
R101(config)#int e0
R101(config-if)#ip add 192.168.100.101 255.255.255.0
R101(config-if)#no shut
```

R102 上的配置：

```
R102#conf t
R102(config)#int e0
R102(config-if)#ip add 192.168.100.102 255.255.255.0
R102(config-if)#no shut
```

R103 上的配置：

```
R103#conf t
R103(config)#int e0
R103(config-if)#ip add 192.168.100.103 255.255.255.0
R103(config-if)#no shut
```

测试连同性：

```
R101#ping 192.168.100.102
R103#ping 192.168.100.102
```

如果全通，则可以进行下面的实验：

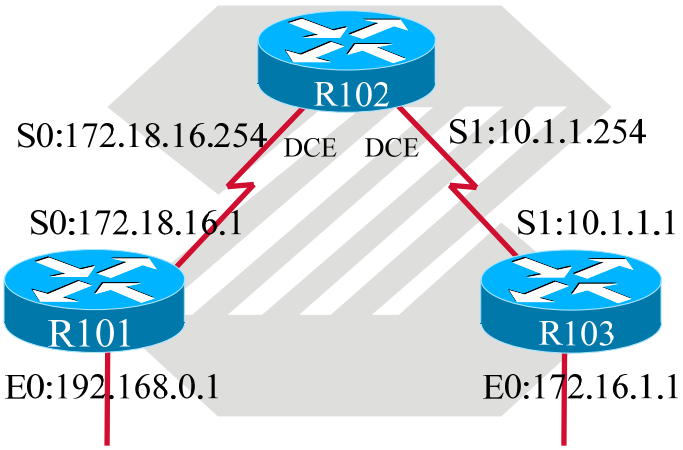
```
R102#conf t
R102(config)#access-list 1 permit host 192.168.100.101     /建立访问控制列表
R102(config)#access-list 1 deny host 192.168.100.103
R102(config)#ing e0
R102(config-if)#ip access-group 1 in    /将访问控制列表绑在接口上，注意是 in 还是 out
```

效果测试：

```
R101#ping 192.168.100.102
R103#ping 192.168.100.102    /注意与前面测试的效果有何不同
```

2）扩展访问控制列表

实验拓扑：



首先做好基本配置，并测试连通性：

R101 上的配置：

```
R101#conf t
R101(config)#int s0
R101(config-if)#ip add 172.18.16.1 255.255.255.0
R101(config-if)#no shut
R101(config-if)#int e0
R101(config-if)#ip add 192.168.0.1 255.255.255.0
R101(config-if)#no shut
R101(config)#ip route 0.0.0.0 0.0.0.0 172.18.16.254
```

R102 上的配置：

```
R102#conf t
R102(config)#int s0
R102(config-if)#ip add 172.18.16.254 255.255.255.0
R102(config-if)#clock rate 64000
R102(config-if)#no shut
R102(config-if)#int s1
R102(config-if)#ip add 10.1.1.254 255.255.255.0
R102(config-if)#clock rate 64000
R102(config-if)#no shut
R102(config-if)#ip route 192.168.0.0 255.255.255.0 172.18.16.1
R102(config-if)#ip route 172.16.1.0 255.255.255.0 10.1.1.1
```

R103 上的配置：

```
R103#conf t
R103(config)#int s1
R103(config-if)#ip add 10.1.1.254.255.255.255.0
R103(config-if)#no shut
R103(config-if)#int e0
R103(config-if)#ip add 172.16.1.1 255.255.255.0
R103(config-if)#no shut
R103(config-if)#ip route 0.0.0.0 0.0.0.0 10.1.1.254
```

连通性测试：

```
R101#ping 10.1.1.1
R101#ping 172.16.1.1
R102#ping 192.168.0.1
R102#ping 172.16.1.1
R103#ping 172.18.16.1
R103#ping 192.168.0.1
```

如果全通，则可以进入下面的实验：

预期效果：在 R102 上使用扩展访问控制列表，使 R101,可以通过 10.1.1.1 telnet 到 r103，但无法 ping 通 10.1.1.1，可以 ping 通地址 172.16.1.1，R101 通过 R102 的其他访问全部拒绝，其他通过 R102 的访问全部都不受影响

实现命令：

```
R102(config)#access-list 100 permit icmp host 172.18.16.1 host 172.16.1.1 echo
R102(config)#access-list 100 permit tcp host 172.18.16.1 host 10.1.1.1 eq telnet
R102(config)#access-list 100 deny ip host 172.18.16.1 any
R102(config)#access-list 100 permit ip any any
R102(config)#int s1
R102(config-if)#ip access-group 100 out
```

效果测试：

```
R101#ping 172.18.16.1
R101#telnet 172.18.16.1
R101#telnet 10.1.1.1
R101#ping 10.1.1.1
```

实验六：NAT 地址转换

所谓的地址转换，即 NAT 功能，就是指在一个组织网络内部，根据需要可以随意自定义的 IP 地址（不需要经过申请）即私有 IP 地址。在本组织内部，各计算机间通过私有 IP 地址进行通讯。而当组织内部的计算机要与外部 internet 网络进行通讯时，具有 NAT 功能的设备（这里是 cisco 路由器）负责将其私有 IP 地址转换为公有 IP 地址，即该组织申请的合法 IP 地址进行通信。

简单地说，NAT 就是通过某种方式将 IP 地址进行转换。

NAT 有以下几种应用：

你想连接 Internet，但不想让你的网络内的所有计算机都拥有一个公有的 internet IP 地址。通过 NAT 功能，可以将申请的合法的 Internet IP 地址统一管理，当内部的计算机需要上 Internet 时，动态或静态地将私有 IP 转换为合法的 IP 地址。

你不想让外部网络用户知道你的网络的内部结构，可以通过 NAT 将内部网络与外部 Internet 隔离开，则外部用户根本不知道你的假 IP 地址。

你申请的合法 Internet IP 地址很少，而你的内部网络用户很多。可以通过 NAT 功能实现多个用户同时公开一个合法 IP 与外部 Internet 进行通信。

注意：Cisco2500 及 2600 系列路由器在 IOS 为 11.2 版本以上支持 NAT 功能。

设置 NAT 功能的路由器至少要有一个 Inside(内部)端口及至少一个 Outside(外部)端口。内部端口连接的网络内的用户使用的是私有 IP 地址，及内部端口连接内部网络。且内部端口可以为任意一个路由器端口。外部端口连接的是外部的网络，如 Internet 。外部端口可以为路由器上的任意端口。

典型的应用，NAT 设置在内部网与外部公用网的连接处的路由器上。当 IP 数据包离开内部网时 NAT 负责将内部的私有 IP 源地址转换成合法 IP 地址。当 IP 数据包进入内部网时，NAT 将合法 IP 目的地址转换成内部私有 IP 地址。

启用 NAT 功能的路由器，一定不能将内部网络路由信息广播到外部。然而，从外部广播来的路由信息，该路由器可以接受。

NAT 的几个概念：

内部本地地址（Inside local address）：分配给内部网络中的计算机的私有 IP 地址

内部合法地址（Inside global address）：对外进行 IP 通信时，代表一个或多个内部本地地址的合法 IP 地址。

NAT 设置可以分为静态地址转换、动态地址转换、复用动态地址转换。

静态地址转换

静态地址转换将内部本地地址与内部合法地址进行一对一的转换，且需要指定和哪个合法地址进行转换。如果内部网络有 E-mail 服务器或 FTP 服务器等可以为外部用户共的服务，这些服务器的 IP 地址必须采用静态地址转换，以便外部用户可以使用这些服务。

动态地址转换：

动态地址转换也是将本地地址与内部合法地址一对一的转换，但是是从内部合法地址池中动态地选择一个未使用的地址对内部本地地址进行转换。

复用动态地址转换：

复用动态地址转换首先是一种动态地址转换，但是它可以允许多个内部本地地址共用一个内部合法地址。只申请到少量 IP 地址但却经常同时有多于合法地址个数的用户上外部网络的情况，这种转换极为有用。

注意：当多个用户同时使用一个 IP 地址，外部网络如何进行识别呢？路由器内部会利用上层的如 TCP 或 UDP 端口号等唯一标识某台计算机。

静态地址转换基本配置步骤：

在内部本地地址与内部合法地址之间建立静态地址转换。

Ip nat inside source static 内部本地地址 内部合法地址

指定连接网络的内部端口

在端口设置状态下

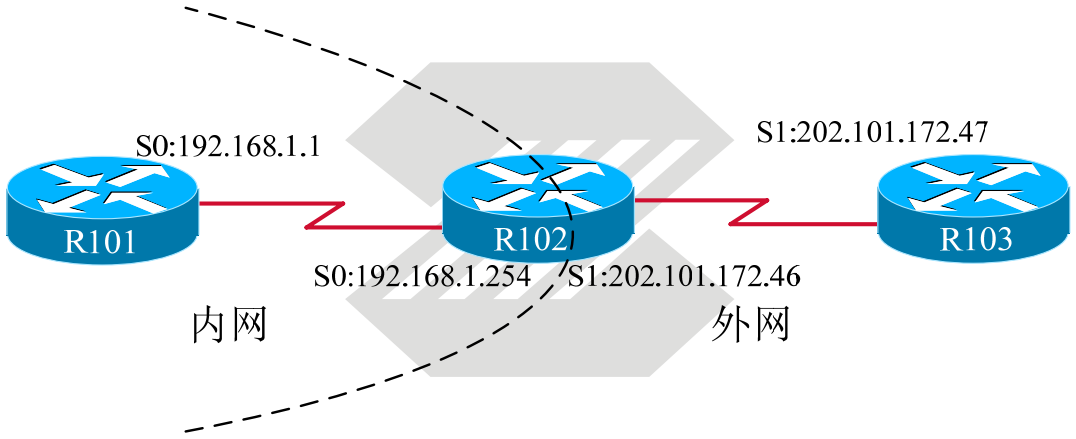
ip nat inside

指定连接外部网络的外部端口

在端口设置状态下

ip nat outside

举例



本实验将 R102 做为 NAT 服务器，将 R101 模拟为内网的主机，默认网关为：192.168.1.254，R103 为公网上的一台主机。

基本配置：

R101 上的配置：

```
Router#conf t
Router(config)#hostname R101
R101(config)#no ip routing
R101(config)#ip default-gateway 192.168.1.254     /模拟为 PC，网关为 192.168.1.254
R101(config)#int s0
R101(config-if)#ip add 192.168.1.1 255.255.255.0
R101(config-if)#no shut
R101(config)#line vty 0 4
R101(config-line)#password cisco
R101(config-line)#login
```

R102 上的配置：

```
R102#conf t
R102(config)#int s0
R102(config-if)#ip add 192.168.1.254 255.255.255.0
R102(config-if)#clock rate 64000
R102(config-if)#no shut
R102(config)#int s1
R102(config-if)#ip add 202.101.172.46 255.255.255.0
R102(config-if)#clock rate 64000
R102(config-if)#no shut
```

R103 上的配置

```
Router#conf t
Router(config)#hostname R103
R103(config)#int s0
R103(config-if)#ip add 192.168.1.1 255.255.255.0
R103(config-if)#no shut
```

注意：R103 上并没有指向内网地址段的路由，这与实际情况是相符的。（Internet 上的路由器不可能有私有地址的路由）

1）配置静态 NAT

```
R102#conf t
R102(config)#ip nat inside source static 192.168.1.1 202.101.172.46
R102(config)#int s0
R102(config-if)#ip nat inside
R102(config-if)#int s1
R102(config-if)#ip nat outside
```

验证：

```
R101#ping 202.101.172.47     /R1 PING R3 会通吗？
R103#ping 192.168.1.1        /反过来了，会通吗？为什么？
R103#telnet 202.101.172.46   /注意，登陆到的主机名是什么？
```

查看静态 NAT 的配置

```
Show ip nat translations
Show ip nat statistics
Show ip nat translations verbose
Debug ip nat
```

2）配置动态 PAT

首先删除静态 NAT 设置

```
R102(config)#no ip nat inside source static 192.168.1.1 202.101.172.46
R102(config)#int s0
R102(config-if)#no ip nat inside
R102(config-if)#int s1
```

```
R102(config-if)#no ip nat outside
```

动态 PAT 配置如下

```
R102(config)#access-list 1 permit 192.168.1.0 0.0.0.255          /定义转发的网段
R102(config)#ip nat inside source list 1 interface serial 0/1 overload   /将符合的地址转
                                                                  换为端口的地址，也可使用地址池
R102(config)#int s0
R102(config-if)#ip nat inside
R102(config-if)#int s1
R102(config-if)#ip nat outside
```

实验七：交换机实验

VLAN 是英文 Virtual Local Area Network 的缩写，即虚拟局域网。VLAN 建立在局域网交换机的基础之上。VLAN 与普通局域网从原理上讲没有什么不同，但从用户使用和网络管理的角度来看，VLAN 与普通局域网最基本的差异体现在：VLAN 并不局限于某一网络或物理范围，VLAN 中的用户可以位于一个园区的任意位置，甚至位于不同的国家。

VLAN 具有以下优点：

一、控制网络的广播风暴：采用 VLAN 技术，可将某个交换端口划到某个 VLAN 中，而一个 VLAN 的广播风暴不会影响其它 VLAN 的性能。

二、确保网络安全：共享式局域网之所以很难保证网络的安全性，是因为只要用户插入一个活动端口，就能访问网络。而 VLAN 能限制个别用户的访问，控制广播组的大小和位置，甚至能锁定某台设备的 MAC 地址，因此 VLAN 能确保网络的安全性。

三、简化网络管理：网络管理员能借助于 VLAN 技术轻松管理整个网络。例如需要为完成某个项目建立一个工作组网络，其成员可能遍及全国或全世界，此时，网络管理员只需设置几条命令，就能在几分钟内建立该项目的 VLAN 网络，其成员使用 VLAN 网络，就像在本地使用局域网一样。 VLAN 的分类主要有以下几种：

四、基于端口的 VLAN ：基于端口的 VLAN 是划分虚拟局域网最简单也是最有效的方法，这实际上是某些交换端口的集合，网络管理员只需要管理和配置交换端口，而不管交换端口连接什么设备。

五、基于 MAC 地址的 VLAN ：由于只有网卡才分配有 MAC 地址，因此按 MAC 地址来划分 VLAN 实际上是将某些工作站和服务器划属于某个 VLAN。事实上，该 VLAN 是一些 MAC 地址的集合。当设备移动时，VLAN 能够自动识别。网络管理需要管理和配置设备的 MAC 地址，显然当网络规模很大，设备很多时，会给管理带来难度。

六、基于第 3 层的 VLAN：基于第 3 层的 VLAN 是采用在路由器中常用的方法：IP 子网和 IPX 网络号等。其中，局域网交换机允许一个子网扩展到多个局域网交换端口，甚至允许一个端口对应于多个子网。

七、基于策略的 VLAN ：基于策略的 VLAN 是一种比较灵活有效的 VLAN 划分方法。该方法的核心是采用什么样的策略？目前，常用的策略有（与厂商设备的支持有关）：

1、 按 MAC 地址
2、 按 IP 地址
3、 按以太网协议类型
4、 按网络的应用等

1. VLAN VTP 设置

```
Switch#conf t
Switch(config)# vtp domain domain-name
```

```
Switch(config)# vtp domain domain-name password password-value
Switch(config)# vtp server
Switch# show vtp status
```

若想 Disable VTP，只须将 VTP 模式改为 transparent

即 Switch(config)# vtp transparent

2. 增加 VLAN。Catalyst 2900XL 系列交换机最大支持 64 个激活的 VLAN，

VLAN ID 号从 1－1005。

```
Switch#conf t
Switch(conf t)# vlan vlan-id
Switch# show vlan
Switch(config)# no vlan vlan-id //删除 VLAN
```

3. 将端口加入 VLAN。

```
Switch# configure terminal
Switch(config)# interface interface
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan vlan-id
Switch(config-if)# end
Switch# show interface interface-id switchport
```

4. 配置 trunk 端口。

```
Switch# configure terminal
Switch(config)# interface interface
Switch(config-if)# switchport trunk encapsulation isl
Switch(config-if)# switchport mode trunk
Switch(config-if)# end
Switch# show interface interface switchport
```

5. 配置 trunk 上允许的 VLAN。

```
Switch(config)# interface interface
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan remove vlan-id-range
Switch(config-if)# switchport trunk allowed vlan add vlan-id-range
Switch(config-if)# end
Switch# show interface interface switchport allowed-vlan
```

若想取消 trunk 端口，只需

```
Switch(config-if)# no switchport mode
```

6. 使用 STP 实现负载。

实现负载分担有两种方法：

1) 使用端口优先级。

配置：

```
Switch_1(config-if)# interface fa0/1
Switch_1(config-if)# spanning-tree vlan 8 9 10 port-priority 10
Switch_1(config)# interface fa0/2
Switch_1(config-if)# spanning-tree vlan 3 4 5 6 port-priority 10
```

2) 使用路径值。例如：

```
Switch_1(config)# interface fa0/1
```

```
Switch_1(config-if)# spanning-tree vlan 2 3 4 cost 30
Switch_1(config)# interface fa0/2
Switch_1(config-if)# spanning-tree vlan 8 9 10 cost 30
```

7.多层交换机 VLAN 间路由

```
Switch#conf t
Switch(config)#ip routing                          /打开多层交换机的路由功能
Switch(config)#interface vlan 10                   /进入 VLAN 10 虚拟接口
Switch(config-if)#ip add 10.0.0.1 255.255.255.0    /指定 VLAN 10 的虚拟接口 IP，用来进行
                                                    VLAN 间路由
Switch(config-if)#no shut

Switch(config)#interface vlan 20
Switch(config-if)#ip add 10.0.1.1 255.255.255.0
Switch(config-if)#no shut                          /此时 VLAN 10 与 VLAN 20 之间可以通信了
```

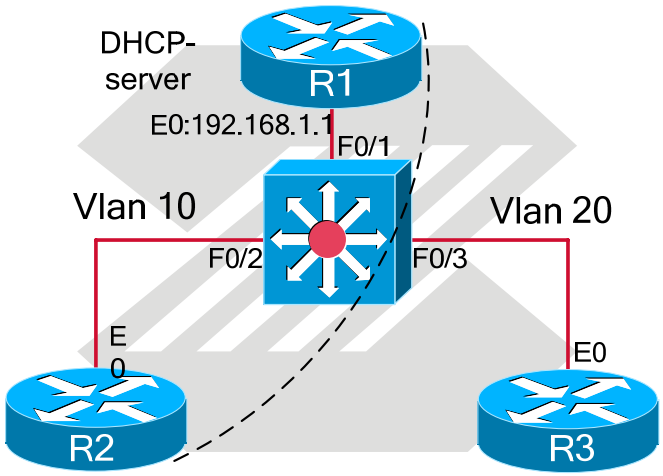
实验八：DHCP 配置

DHCP 服务可为主机自动分配 IP 地址，免除了逐个设置的麻烦。

举例：

在这个例子中，我们了解一下 DHCP 服务器在 VLAN 内使用和在 VLAN 间使用分别怎样配置。此实验可在中联 CCIE 机架上完成，交换机必须支持三层。

拓扑如下：



R1 为 DHCP 服务器，和 R2 同属于 VLAN 10，R3 属于 VLAN 20。R1、R2 模拟成 PC 机

首先进行基本配置

R2 上的配置

```
Router>en
Router#conf t
Router(config)#hostname r2
```

```
R2(config)#no ip routing      /关闭路由器路由功能，模拟成 PC 机
R2(config)#int e0/0
R2(config-if)#ip add dhcp
R2(config-if)#no shutdown
```

R3 上的配置

```
Router>en
Router#conf t
Router(config)#hostname r3
R3(config)#no ip routing
R3(config)#int e0/0
R3(config-if)#ip add dhcp
R3(config-if)#no shutdown
```

sw1 上的配置

```
sw1#conf t
sw1(config)#int f0/1
sw1(config-if)#switchport mode access
sw1(config-if)#switchport access vlan 10
sw1(config-if)#int f0/2
sw1(config-if)#switchport mode access
sw1(config-if)#switchport access vlan 10
sw1(config-if)#int f0/3
sw1(config-if)#switchport mode access
sw1(config-if)#switchport access vlan 20
```

下面进行 DHCP 的配置

R1 上的配置

```
Router>en
Router#conf t
Router(config)#hostname DHCP
DHCP(config)#int e0/0
DHCP(config-if)#ip add 192.168.1.1 255.255.255.0
DHCP(config)#ip dhcp pool zl_01                        /建立 DHCP 池，池名为 zl1
DHCP(dhcp-config)#network 193.168.1.0 255.255.255.0  /指定池所包含的 IP 地址段，和子网掩码
DHCP(dhcp-config)#default-router 193.168.1.254       /指定自动分配的网关
DHCP(dhcp-config)#dns-server 202.101.172.46          /指定自动分配的 DNS
DHCP(dhcp-config)#ip dhcp pool zl_02
DHCP(dhcp-config)#network 192.168.2.0 255.255.255.0
DHCP(dhcp-config)#default-router 192.168.2.254
DHCP(dhcp-config)#dns-server 202.101.172.46
DHCP(dhcp-config)#exit
DHCP(config)#ip dhcp excluded-address 192.168.1.1 193.168.1.100  /保留哪些地址不用来分配
DHCP(config)#ip dhcp excluded-address 192.168.2.1 193.168.2.100
DHCP(config)#ip route 192.168.2.0 255.255.255.0 192.168.1.254   /配置静态路由
sw1(config-if)#int vlan 10
```

```
sw1(config-if)#ip add 192.168.1.254 255.255.255.0
sw1(config-if)#no shut
sw1(config-if)#int valn 20
sw1(config-if)#ip add 192.168.2.254 255.255.255.0
sw1(config-if)#ip helper-address 192.168.1.1  /IP helper-address 作用是将 DHCP 请求的广播
                                               数据包转化为单播请求，路由器才会响应
sw1(config-if)#no shut
```

实验九：IPv6

IPv6 将 IPv4 的地址长度 32 位增加到了 128 位

IPv6 地址类型:单播(一对一),任意播(一到最近),多播(一到多),没有广播的概念

IPv6 的地址格式: IPv6 的地址被表示为一系列的 16 位字段,共分 8 个字段,每个字段被转换为 16 进制数,字段之间用冒号隔开,格式为: x:x:x:x:x:x:x:x 如(2031:0000:130F:0000:0000:09C0:0001:130B)

简化 IPv6 地址书写方式: IPv6 地址中常常包含多个连续的值为 0 的字段,为简化这种地址,可使用双冒号来表示这些值为 0 的连续字段.可以在地址的开头、中间和末尾这样做,但每个地址中只能使用一次.以上示例中地址可写为 2031:0:130F::09C0:1:130B

IPv6 的前缀: 为区分网络所使用的,如 2001:1::1/16

IPv6 的配置：


```
R101 上的配置
Router#conf t
Router(config)#hostname R101
R101(config)#int s0
R101(config-if)#ipv6 add 2001:0:0:0:0:0:ABCD:0001/64      /为接口分配一个 IPV6 的地址，想
                                                            一想，这个地址还可以怎样写？
R101(config-if)#no shut

R102 上的配置
Router#conf t
Router(config)#hostname R102
R102(config)#int s0
R102(config-if)#ipv6 add 2001::ABCD:2/64
R102(config-if)#clock rate 64000
R102(config-if)#no shut
```

IPv6 的测试和查看

查看：R101#show ipv6 interface brief

测试：R101#ping 2001::ABCD:2

实验十：无线网络应用举例

在这个实验里我们来介绍一个使用无线连接共享上网的例子。

如今，笔记本的普及率越来越高，笔记本大多带有无线网卡，在家中或者宾馆中，有两台笔记本，而只有一根网线，怎样实现两台笔记本同时上网？此时，使用宽带路由器显然有点浪费。其实可以使用一台笔记本使用物理网卡连接网线，而使用无线网卡与另外一台笔记本进行无线连接即可轻松实现。

方法如下：

1、设置 Internet 连接共享。

1）打开物理网卡的本地连接属性，并选择高级标签（如图 10-1）。

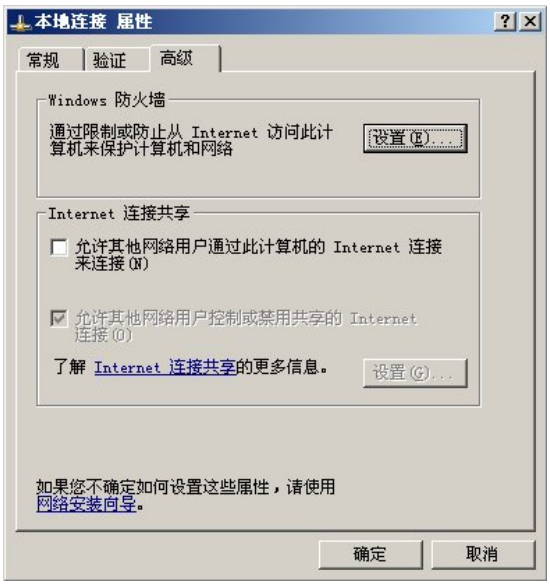


图 10-1

2）勾选‘允许其他网络用户通过此计算机的 Internet 连接来连接’，并点击确定。将出现如图 10-2 所示对话匡，点击‘是’。此时另一块网卡（即无线网卡）的地址将自动被指定为 192.168.0.1。之后可手动改为其它地址，但应保证不与物理网卡在同一网段。

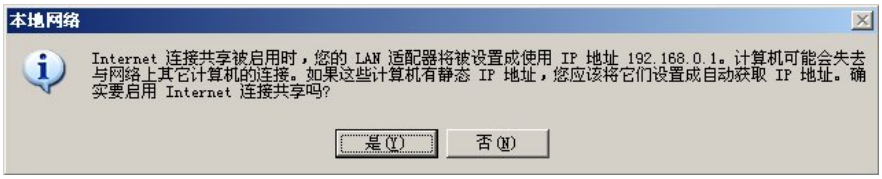


图 10-2

2、设置点对点的无线网络。

1）打开无线网卡的属性窗口，选择无线网络配置标签。在此标签中点击添加按钮，将出现如图 10-3 所示画面。

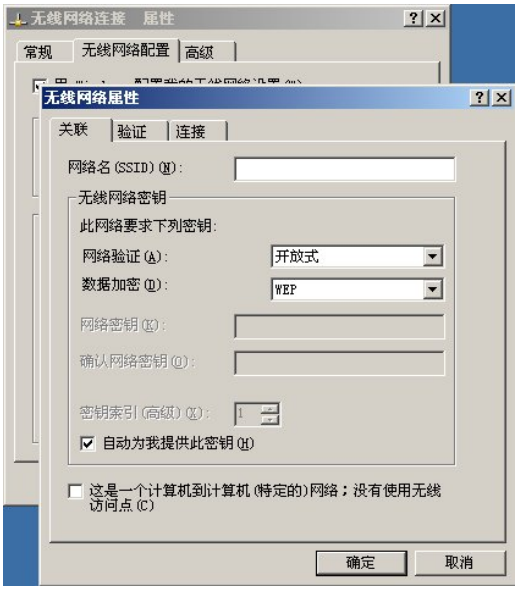


图 10-3

2）在 SSID 项填写建立的网络名，去掉‘自动为我提供此密钥’并手动分配密钥。勾选‘这是一个计算机到计算机（特定的）网络；没有使用无线访问点’。填好后如图 10-4，点击确定。

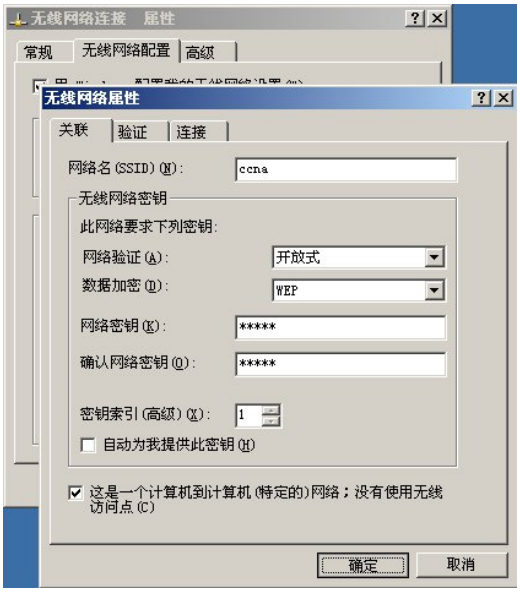


图 10-4

3、连接到无线 。

1）在另一台计算机上，打开查看无线连接对话框，点击刷新网络列表，一般需要多刷新几次，直到出现刚才所建立的网络连接项。点击连接，并输入刚才所分配的密钥。如图 10-5 所示。

2）为无线网卡分配 IP、网关和 DNS。其中 IP 要与之前那台机器的无线网卡的设在同一个网段。网关要填写第一台笔记本的 IP。

此时，两台计算机都可以正常访问 Internet 了。

附录：路由器传输故障排除方法

端口及线路协议的状态常见问题

端口及线路协议的状态共有以下六种

Serial x is up, line protocol is up

Serial x is down, line protocol is down

Serial x is up, line protocol is down

Serial x is up, line protocol is up (looped)

Serial x is administratively down, line protocol is down

下表给出解决方案

端口及线路协议状态	错误原因	解决方案
Serial x is up, line protocol is up		此状态为正确状态
Serial x is down, line protocol is down	路由器未检测到载波信号 1.传输线路不通 2.路由器的连接线未连接，或未连接正确。 3.路由器硬件故障	步骤 1 检测传输线路 步骤 2 检查你是否使用正确的电缆与端 口 步骤 3 改换路由器另外端口，以确认是否为硬件故障
Serial x is up, line protocol is down	1.本地或远程路由器配置错误 2.远程路由器未配置 keepalives 参数。 3.传输线路错误：problem---noisy line, or misconfigured or failed switch 4.本地或远端的 CSU/DSU 故障 5.路由器硬件故障	步骤 1 设置端口本地自环，再用 show interfaces serial command 观察线路协议是否为 up,若为 up 状态则表明故障原因在于传输线路或远程路由器配置错误 步骤 2 确认电缆插在正确的端口，正确的 CSU/DSU，和正确的配线架端口上 步骤 3 如认为路由器硬件故障，更换端口进行测试。
Serial x is up, line protocol is up (looped)	线路中存在自环设置： 1. 硬件自环 2. 软件自环	步骤 1 使用 show running-config 命令察看端口设置中是否有 loopback 设置 步骤 2 若存在 loopback 设置 用 no loopback 去掉此设置 步骤 3 若不存在 loopback 设置，检查 CSU/DSU 是否存在自环设置
Serial x is administratively down, line protocol is down	1.路由器端口配置中存在 shutdown 命令 2.重复的 IP 地址	步骤 1 检查路由器配置是否存 shutdown 命令 步骤 2 使用 no shutdown 端口命令去掉 shutdown 命令 步骤 3 使用 show running-config 命令检查是否存在重叠的 IP 地址。 步骤 4 若存在，则改变 IP 地址。

本地节点不能访问远程节点

故障原因	解决方法
缺省网关没有指定或远程节点配置错误	如果主机没有运行 routed ,就必须配置缺省网关 步骤 1 检测主机是否设置网关。用如下命令 unix-host% netstat -rn 步骤 2 如发现网关配置不正确，用如下命令设置网关 unix-host% route add default address 1 步骤 3 在命令行方式下加入网关后，在 UNIX 主机上将网关地址加入到如下文件内 /etc/defaultrouter UNIX host file. 若主机为 windows 平台，可在 control panel 内修改网关设置。
DNS 设置不正确	如果 DNS 设置有错误，不能对 IP 地址进行解析，就无法用域名进行访问。
某些路由器路由设置不正确。	步骤 1 使用 traceroute 命令察看路由走向 步骤 2 当发现需检测的路由器时，用 show ip route 命令察看路由表，看是否存在所需路由

主机不能访问某些网段

故障原因	解决方法
主机未设置网关	为主机设置缺省网关，详细设置见表 3.1
路由器设置的 access list 有错误	步骤 1 使用 show ip routes 检查路由表及使用相应的 debug 命令检查路由协议交换的情况 例如 debug ip igrp 和 debug ip rip 步骤 2 检查与你无法通信的网段的相应信息 步骤 3 检查 access-list 的设置看是否将相关的网络过滤了。 步骤 4 禁止 access-list ,察看是否能够与该网段通信。若是则重新设置正确的 accesss-list