第一部分 Cisco路由器的配置

实训一　Cisco 路由器认识

1、Cisco 产品介绍

（1）路由器

模块化路由器

- Cisco 12000 系列：12008、12012、12016
- Cisco 7500 系列：7505、7507、7513、7576
- Cisco 7200 系列：7204、7206
- Cisco 4500 系列：4500M、4700M
- Cisco 3600 系列：3620、3640、3661、3662
- Cisco 2600 系列：2610、2611、2620、2621
- Cisco 1700 系列：1720、1750
- Cisco 1600 系列：1601R、1603R、1605R

固定配置路由器

- Cisco 2500 系列路由器
- Cisco 800 系列路由器

（2）访问服务器

模块化配置

- AS5300、AS5800 系列访问服务器

固定配置

- Cisco 2500 系列：2509、2511

（3）交换机产品

模块化配置

- Catalyst 8500 系列：8540、8510
- Catalyst 6000 系列：6006、6009、6506、6509
- Catalyst 5000 系列：5000、5505、5509、5500
- Catalyst 4000 系列：4003、4006
- Catalyst 2900XL 系列：2912MF-XL、2924M-XL
- Catalyst 2820 系列：2828

固定配置

- Catalyst 3500 系列：3512-XL、3524-XL、3548-XL、3508G
- Catalyst 2900 系列：2948G、2912-XL、2924-XL
- Catalyst 1900 系列：1912、1924、1924C

（4）防火墙产品

- PIX Firewall 系列硬件防火墙

2、Cisco 2600 系列模块化访问路由器介绍

- 1 个网络模块插槽，2 个 WIC 广域接口卡插槽
- 支持的局域网接口类型包括以太网、快速以太网、令牌环
- 支持的广域网接口类型包括同步串口、异步串口、同/异步自适应串口、ISDN BRI、ISDN PRI、ATM、Channelized E1 等
- 可支持多种网络协议，包括 IP、Novell IPX、AppleTalk 和 DECnet 等等
- 可支持多达 60 路 Voice Over IP，实现数据网络与语音网络的融合

系列产品	固定端口（LAN）	广域网插槽（WIC）	网络模块插槽（NM）	高级集成模块（AIM）
Cisco 2610	1 以太网	2	1	1
Cisco 2611	2 以太网	2	1	1
Cisco 2612	1 以太网/1 令牌环	2	1	1
Cisco 2613	1 令牌环	2	1	1
Cisco 2620	1 个 10/100M 自适应以太网	2	1	1
Cisco 2621	2 个 10/100M 自适应以太网	2	1	1

（1）Cisco 2600 系列网络模块-NM

NM-1E	1 口以太网模块
NM-1FE-FX	1 口快速以太网模块 FX 光纤接口
NM-1FE-TX	1 口快速以太网模块 TX 双绞线接口
NM-1V	1 个 Voice/fax 语音卡(VIC)插槽
NM-2V	2 个 Voice/fax 语音卡(VIC)插槽
NM-HDV-1E1-30E	单口 30 Enhanced Channel E1 Voice/Fax 网络模块
NM-HDV-2E1-60	双口 60 Channel E1 Voice/Fax 网络模块
NM-4A/S	4 口同步/异步串口
NM-4B-S/T	4 口 ISDN-BRI
NM-8A/S	8 口 同步/异步 串口 网络 模块
NM-8AM	8 口 模拟 Modem 网络 模块
NM-8B-S/T	8 口 ISDN-BRI 网络 模块
NM-1CE1B	1 口 Channelized E1/ISDN-PRI 平衡式
NM-1CE1U	1 口 Channelized E1/ISDN-PRI 非平衡式
NM-2CE1B	2 口 Channelized E1/ISDN-PRI 平衡式
NM-2CE1U	2 口 Channelized E1/ISDN-PRI 非平衡式
NM-4E	4 口以太网
NM-16A	16 口异步模块
NM-16AM	16 口模拟 Modem
NM-32A	32 口异步模块
NM-1ATM-25	1 口 ATM 25Mbps
NM-COMPR2	压缩模块

（2）语音接口卡-VIC

VIC-2E/M	2 口语音接口卡- E&M
VIC-2FXO	2 口语音接口卡- FXO
VIC-2FXS	2 口语音接口卡- FXS
VIC-2BRI-S/T-TE	2 口语音接口卡- BRI (Terminal)
VWIC-1MFT-E1	1 口 RJ-48 Multiflex Trunk - E1 (配套的 NM-HDV-1E1-30 等将出)
VWIC-2MFT-E1	2 口 RJ-48 Multiflex Trunk - E1 (同上)
VWIC-2MFT-E1-DI	2 口 RJ-48 Multiflex Trunk - E1 With Drop and Insert (同上)

（3）广域网接口卡-WIC

WIC-1T	1 口广域网串口卡
WIC-1B-S/T	1 口 ISDN BRI S/T 广域网串口卡(拨号及专线)
WIC-2A/S	2 口同步/异步串口
WIC-2T	2 口高速同步串口

3、Cisco 2500 系列路由器

- 1 或 2 个高速同步串口（最高至 2.048 M），可通过 DDN 专线、Frame Relay、X.25 等接入广域网。
- 单口、双口型号均提供 AUI 接口，可接驳各种类型以太网。
- 2509,2511 的异步口是 1(2)个 68 针 SCSI 接口,需用 CAB-OCTAL-KIT 线分为 8(16)个异步串口,分别提供 8/16 个异步串口，工作在同步方式时，最高速率 128Kbps;工作在同步方式时，最高速率 115.2Kbps。

系列路由器	Ethernet 以太网口	ISDN BRI	Serial 同步串口 (2.048Mbps)	Async 异步串口 (115.2Kbps)
2501	1 AUI (DB15)	-	2 * DB60	-
2503	1 AUI (DB15)	1 RJ-45	2 * DB60	-
2505	8 UTP Hub RJ-45	-	2 * DB60	-
2507	16 UTP Hub RJ-45	-	2 * DB60	-
2509	1 AUI (DB15)	-	2 * DB60	8 68 针 SCSI II *1
2511	1 AUI (DB15)	-	2 * DB60	1668 针 SCSI II *2
2509-RJ	1 AUI (DB15)	-	1 * DB60	8 RJ-45
2511-RJ	1 AUI (DB15)	-	1 * DB60	16 RJ-45
2516	14 UTP Hub RJ-45	1 RJ-45	2 * DB60	-

2520	1 AUI (DB15)	1 RJ-45	2 * DB60	-
2522	1 AUI (DB15)	1 RJ-45	2 * DB60	-

4、 Cisco 1700 系列模块化多服务路由器

基本型号	WIC 插槽数	VIC 插槽数	Flash	DRAM	IOS 软件
Cisco 1720	2	无	4MB-16MB	16MB–48MB	IP
Cisco 1750	2	1	4MB-16MB	16MB–48MB	IP
Cisco 1750-2V	2	1	8MB-16MB	24MB–48MB	IP Plus Voice
Cisco 1750-4V	2	1	8MB-16MB	24MB–48MB	IP Plus Voice

（1）Cisco 1700 系列路由器的广域网模块-WIC

广域网网卡 WIC	接　口
WIC-1T / WIC-2T	一个 / 二个串行、异步及同步接口
WIC-2A/S	二个低速(28Kbps)串行、异步及同步接口
WIC-1B-S/T	一个 ISDN BRI S/T 接口

（2）Cisco 1750 使用的语音功能模块-VIC

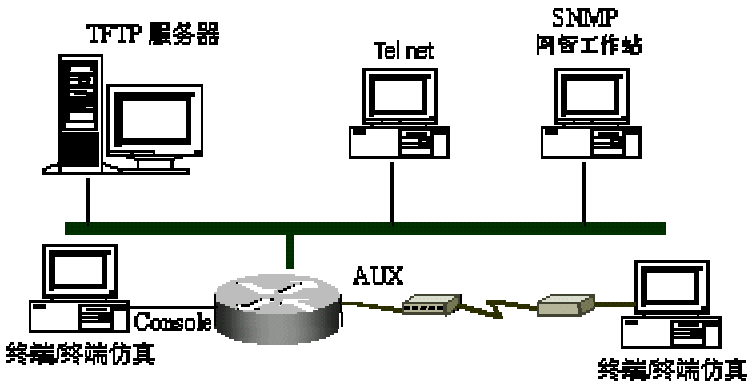
模块名称 VIC	描　述

VIC-2FXS	2 口 FXS 语音/传真接口卡直接接电话机、传真机等设备
VIC-2FXO	2 口 FXO 语音/传真接口卡连接程控交换机(PBX)或按键系统，公用电话网(PSTN)
VIC-2FXM	2 口 E&M 语音/传真接口卡 连接程控交换机(PBX)或按键系统中继线

实训二　路由器的配置基础

路由器在使用时必须进行相关的配置才能起到相应的作用。路由器的配置包括的方面比较多，如：基本配置、静态路由、动态路由协议、广域网协议、远程访问、IP 电话、地址转换、访问列表等，用户应根据网络的具体情况和需求，先进行规划和设计，经分析确认后，有选择地依次对网络中的每个路由器进行相应地配置。

1、路由器的配置方式



①超级终端方式。该方式主要用于路由器的**初始配置**，路由器不需要 IP 地址。基本方法是：计算机通过 COM1/COM2 口和路由器的 Console 口连接，在计算机上启用“超级终端”程序，设置“波特率 ：9600 ，数据位 ：8，停止位 ：1，奇偶校验: 无，校验：无”即可。常用

②Telnet 方式。该方式配置要求路由器必须配置了 **IP 地址**。基本方法是：计算机通过网卡和路由器的以太网接口相连，计算机的网卡和路由器的以太网接口的 IP 地址必须在同一网段。常用

③其他方式 :AUX 口接 MODEM，通过电话线与远方运行终端仿真软件的微机；通过 Ethernet 上的 TFTP 服务器；通过 Ethernet 上的 SNMP 网管工作站。

2、路由器的工作模式

在命令行状态下，主要有以下几种工作模式：

① 一般用户模式。主要用于查看路由器的基本信息，只能执行少数命令，不能对路由器进行配置。提示符为：**Router**>。

② 使能（特权）模式。主要用于查看、测试、检查路由器或网络，不能对接口、路由协议进行配置。提示符为：**Router#** ；进入：Router>enable。

③ 全局配置模式。主要用于配置路由器的全局性参数。提示符为：**Router(confg)#** ；进入：Router#config ter。

④ 全局模式下的子模式。包括：接口、路由协议、线路等。其进入和提示符如下：

Router(confg)#ineterface e0　　//进入接口模式

Router(confg-if)#　　//接口模式提示符

Router(confg)#rip　　//进入路由协议模式

Router(confg-router)#　　//路由协议模式

Router(confg)#line con 0　　//进入线路模式

Router(confg-line)#　　//线路模式提示符

⑤ 监控模式。该模式主要用于 IOS 升级及恢复口令，不能用于正常配置。提示符：>，进入：在路由器加电 60 秒内，在超级终端连接状态下，同时按 Ctrl+Break。

3、常用命令

①“ ？ ”、“ Tab ”的使用

键入“ ？ ”得到系统的帮助；“ Tab ”补充命令。

② 改变命令状态

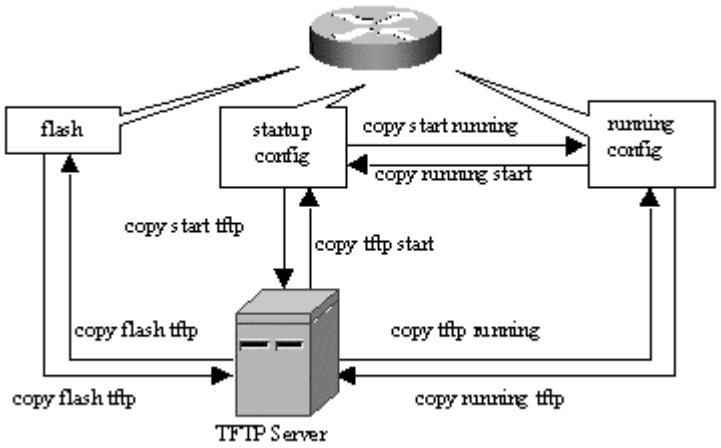
任　务	命　令
进入特权命令状态	enable
进入全局设置状态	config terminal
退出一层命令	exit
进入端口设置状态	interface *type slot/number*
进入线路设置状态	line *type slot/number*
进入路由设置状态	router *protocol*

③ 显示命令

任务	命令
查看版本及引导信息	show version
查看 flash 版本	show flash
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

④ 拷贝命令

用于 IOS 及 CONFIG 的备份和升级



⑤ 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*

⑥ 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
端口设置	interface *type slot/number*
设置 IP 地址	ip address *address subnet-mask*
激活/关闭端口	no shutdown/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*

4、内存体系结构介绍

①ROM：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。

②FLASH：存放的是“ IOS ”，可以通过写入新版本对路由器进行软件升级。

(Show flash)

③DRAM：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“ running-config ”。

(show running-config| show ip route| show mem| show protocols| show processes cpu)

④NVRAM：NVRAM 中包含有路由器配置文件“ startup-config ”，NVRAM 中的内容在系统掉电时不会丢失。

(show startup-config)

注意：

- 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。
- ROM，NVRAM 大小不能调整；FLASH，DRAM 大小能调整。

5、CLI 命令行操作组合键

ctrl+p: 恢复上一条命令

ctrl+n: 恢复下一条命令

ctrl+b: 左移光标

ctrl+f: 右移光标

实训三　路由器的基本配置

0. 路由器的基本配置内容

路由器的基本配置一般包括如下内容：路由器命名、配置口令及加密、配置相关地接口、配置保存与加载、静态路由、默认路由等，它是用户在使用路由器时必须进行地配置，是后续其它配置地基础。

在设计路由器的各种配置时，为便于举例说明，下面以图 1 为工程背景，如有不同时另再说明。

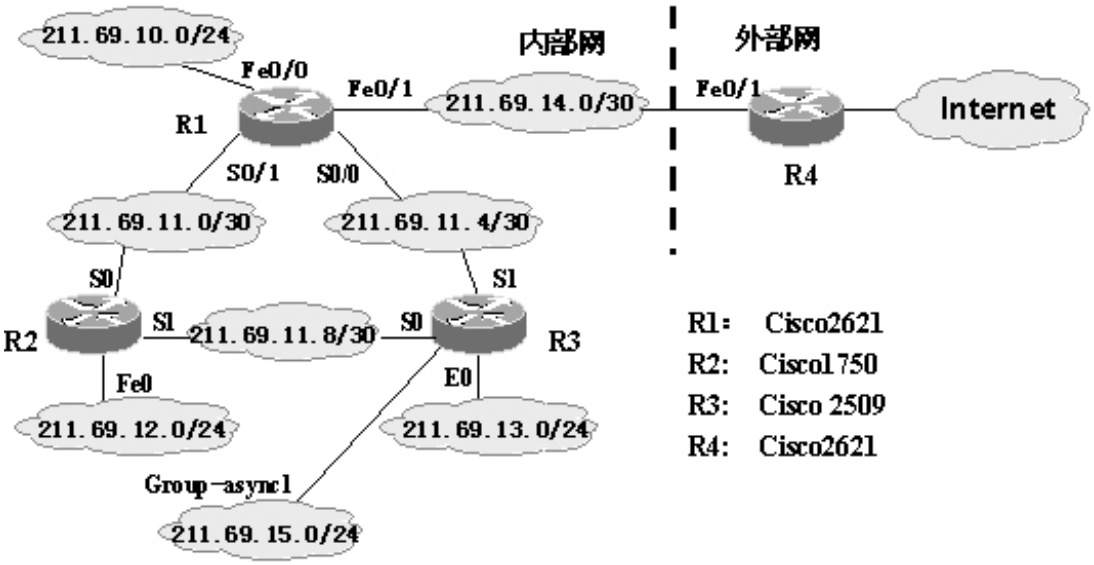


图 1 网络结构示意图

网络结构说明：

该结构模型由 R1(Cisco 2621)、R2(Cisco 1750)、R3(Cisco 2509)三个路由器通过同步串口的 DTE、DCE 电缆将 211.69.10.0/24、211.69.12.0/24、211.69.13.0/24、211.69.15.0/24 四个 C 类网段互联起来，而 211.69.11.0/30、211.69.11.4/30、211.69.11.8/30、211.69.14.0/30 四个子网，每个子网内只有 2 个 IP 地址，用于路由器之间互联的端口使用。

（1）R1(Cisco 2621)：其自带 2 个 10/100Mbps 快速的以太网接口，分别为 FastEthernet0/0(Fe0/0)、FastEthernet0/1(Fe0/1)，分别连接了 211.69.10.0/24、211.69.14.0/30 两个网段；另需配置 1 个 2FAS-WIC 广域网接口模块，通过 DTE/DCE 电缆分别和 R2(Cisco 1750)、R3(Cisco 2509)2 个路由器连接；再配置 1 个 NM-1V 网络模块、1 个 2FSX 的 Voice/Fax 语音接口模块，以实现 IP 电话功能。

（2）R2(Cisco 1750)：其自带 1 个 10/100Mbps 的快速以太网接口为 FastEthernet0/0(Fe0)，连 211.69.12.0/24 这个 C 类网段；另需配置 1 个 2FAS-WIC 广域网接口模块，通过 DTE/DCE 电缆分别和 R1(Cisco 2621)、R3(Cisco 2509)2 个路由器连接；再配置 1 个 NM-1V 网络模块、1 个 2FSX 的 Voice/Fax 语音接口模块，和 R1(Cisco 2621)一起实现 IP 电话功能。

（3）R3(Cisco2509)：其自带 1 个 10Mbps 的以太网接口为 Ethernet0/0(E0)，连 211.69.13.0/24 这个 C 类网段；自带 8 个 Async 异步拨号接口，通过连接 Modem 实现远程拨号访问；另需配置 1 个 2FAS-WIC 广域网接口模块，通过 DTE/DCE 电缆分别和 R1(Cisco 2621)、R2(Cisco1750)2 个路由器连接。

（4）R4(Cisco 2621)：作为外网 ISP 的接入路由器，其自带 2 个 10/100Mbps 快速的以太网接口，通过 FastEthernet0/1(Fe0/1)连接 211.69.14.0/30 和 R1 相连。

各路由器接口的 IP 地址如下：

（1）R1(Cisco 2621)

S0/0 端口的 IP 地址：211.69.11.5/30

S0/1 端口的 IP 地址：211.69.11.1/30

Fe0/0 端口的 IP 地址：211.69.10.1/24

Fe0/1 端口的 IP 地址：211.69.14.1/30

（2）R2(Cisco 1750)上各端口的 IP 地址如下：

S0 端口的 IP 地址：211.69.11.2/30

S1 端口的 IP 地址：211.69.11.9/30

Fe0 端口的 IP 地址：211.69.12.1/24

（3）R3(Cisco 2509)上各端口的 IP 地址如下：

S0 端口的 IP 地址：211.69.11.10/30

S1 端口的 IP 地址：211.69.11.6/30

E0 端口的 IP 地址：211.69.13.1/24

（4）R4(Cisco 2621)

Fe0/1 端口的 IP 地址：211.69.14.2/30

1. 路由器的命名

路由器的名字被称作主机名（hostname），它会在系统提示符中显示，在集中配置一个多路由器环境的网络中，路由器的统一命名，会给管理与配置网络中路由器带来极大的方便。路由器的系统默认名字是 Router。命名需要在全局配置模式下完成，方法如下：

```
Router # config    ter      //进入全局配置模式
Router(config)# hostname    cisco2621      //命名为“ cisco2621 ”
```

2. 配置口令及加密

路由器的口令主要有：enable 口令、console 口口令、aux 口口令及 Telnet 口令等，通过口令配置，增加系统的安全性。默认配置的大部分口令是明码显示，可通过加密的方式，使所有口令在用“ show run ”显示时成为密文。

（1）enable 口令（特权用户）

```
Router(config)#enable password xlx1618     //配置 enable 口令为“ xlx1618 ”，明文显示
Router(config)#enable secret xu1618     //配置 enable 加密口令为“ xu1618 ”，密文显示
```

（2）console 口口令

```
Router(config)#line console 0   //进入 console 口
Router (config-line)#login   //提示输入口令
Router(config-line) #password cisco   //配置 console 口口令为“ cisco ”
```

（3）aux 口口令

```
Router(config)#line aux 0   //进入 aux 口
Router (config-line)#login   //提示输入口令
Router(config-line) #password cisco   //配置 aux 口口令为“ cisco ”
```

（4）Telnet 口令

如果要使用 Telnet 来登陆网络中的路由器进行管理与配置，必须配置 Telnet 口令。路由器一般支持最多 5 个 Telnet 用户。Line vty 0 4 建立 telnet 会话访问时使用的密码保护。

①5 个 Telnet 用户口令相同

```
Router (config)#line vty 0 4   //进入 vty 0 4
Router(config-line) # login   //提示输入口令
Router(config-line) # password cisco     //口令为“ cisco ”
```

②Telnet 用户口令不全相同

```
Router (config)#line vty 0   //进入 vty 0
Router(config-line) # login   //提示输入口令
Router(config-line) # password cisco     //口令为“ cisco0 ”
Router (config)#line vty 1 3 //进入 vty 1 3
Router(config-line) # login   //提示输入口令
Router(config-line) # password cisco     //口令为“ cisco1 ”
Router (config)#line vty 4   //进入 vty 4
Router(config-line) # login   //提示输入口令
Router(config-line) # password cisco     //口令为“ cisco4 ”
```

（5）口令加密

上述除“ enable secret ”为加密口令外，其余口令都为明文显示。如果想加密，

可采用如下命令即可。

Router(config)#service　password-encryption

3. 配置接口

对于以太网口的基本配置，主要包括：IP 地址、速率、双工模式等。对于串口的基本配置，主要包括：IP 地址、封装协议、速率等，串口的其它配置会在后面有关内容中介绍。

配置接口的命令格式如下所示：

Router (config)# interface　type　port-number

其中，“ type ”：接口类型，如“ serial ”、“ Ethemet ”、“ FastEthernet ”等。“ port-number ”：接口号，如“ 0 ”、“ 0/1 ”等。

（1）以太网的基本配置

Router(config)#interface fastEthernet 0/0

Router(config-if)#ip add 20.0.0.1 255.0.0.0　//配置 IP 地址

Router(config-if)#speed 100　　//配置速率为 100Mbps

Router(config-if)#duplex full　　//配置为全双工模式

（2）串口的基本配置

Router(config)#interface serial 0/0

Router(config-if)#ip add 30.0.0.1 255.0.0.0　//配置 IP 地址

Router(config-if)#enca ppp　　//封装 PPP 协议

Router(config-if)#clock rate 128000　　//速率为 128000bps

（3）接口的关闭和开启

Router (config-if)#shutdown　//关闭接口

Router (config-if)#no shutdown　　//开启接口

4．配置静态路由

静态路由是手工配置的，当网络拓扑结构发生改变而需要更新路由时，网络管理员就必须手工更新静态路由信息。当某个网络只能通过一条路由出去时，使用静态路由即可。网络配置静态路由时就避免了动态路由更新所带来的系统和带宽开销。“ ip route　”命令用来设定一条静态路由，语法如下：

ip route network mask {address|interface} [distance] [tag] [permanent]

其中：

network　目标网络或子网地址。

Mask　子网掩码.

Address　下一跳的 IP 地址或相邻路由器的端口地址。

Interface　相邻路由器的端口名称。

Distance　管理距离。

Tag　可选

Permanent　路由的优先级

[例 1] 静态路由的配置

如图 1 所示，要求：内部网之间通过静态路由实现内网各网段 211.69.10.0/24、211.69.12.0/24、211.69.13.0/24 的相互通信。

R1 的配置：

Router(config)#ip route 211.69.12.0 255.255.255.0 211.69.11.2

Router(config)# ip route 211.69.13.0 255.255.255.0 211.69.11.6

R2 的配置：

Router(config)# ip route 211.69.10.0 255.255.255.0 211.69.11.1

Router(config)# ip route 211.69.13.0 255.255.255.0 211.69.11.1

Router(config)# ip route 211.69.11.4 255.255.255.0 211.69.11.1

R3 的配置：

Router(config)# ip route 211.69.10.0 255.255.255.0 211.69.11.5

Router(config)# ip route 211.69.12.0 255.255.255.0 211.69.11.5

Router(config)# ip route 211.69.11.0 255.255.255.0 211.69.11.5

5．配置默认路由

默认路由也是由用户手工配置的，它作为到达目的网络的路由未知时所选择的路径。也就是当路由表中没有明确列出到达某一目的网络的下一跳时，则将选择默认路由所指定的下一跳地址（默认路由的优先级最低）。

实际上，路由器不可能知道到达所有网络的路由，如在图 1 中，R1、R2、R3 路由器，不可能知道内网访问 Internet 时所有路由的目的网络地址，因此，如想让内网用户能够访问 Internet，必须都配置一条默认路由。

[例 2] 默认路由配置

如图 1 所示，要求：内网的所有用户能够访问 Internet。

R1 的配置：

Router(config)#ip route 211.69.12.0 255.255.255.0 211.69.11.2

Router(config)# ip route 211.69.13.0 255.255.255.0 211.69.11.6

Router(config)# ip route 0.0.0.0 0.0.0.0 211.69.14.2

R2 的配置：

Router(config)# ip route 0.0.0.0 0.0.0.0 211.69.11.1

R3 的配置：

Router(config)# ip route 0.0.0.0 0.0.0.0 211.69.11.5

6. 配置保存及导入

（1）将当前配置（running-config）保存到启动配置（startup-config）中。

Router(config)#copy run start　//或者　Router(config)#write

（2）将当前配置（running-config）保存到 Tftp 计算机上保存。

Router(config)#copy run tftp　//需按提示进行 IP 地址、文件名、存放位置进行设置

（3）将 Tftp 上的配置文件导入到当前配置（running-config）

Router(config)#copy tftp run　//需按提示进行 IP 地址、文件名、文件位置进行设置

7．导出和导入 IOS 软件

用 TFTP 服务器可以对系统 IOS 软件进行上传和下载的要求。TFTP 服务器可以是一台装有并运行 TFTP 软件的计算机。可以把 IOS 软件作为备份拷贝到计算机上，也可以利用此方法对 IOS 软件进行升级（导入）。其方法如下：

（1）导出 IOS（备份）。

Router(config)#copy flash tftp　//需按提示进行 IP 地址、文件名、文件位置进行设置

（2）导入 IOS（升级）。

Router(config)#copy tftp flash　//需按提示进行 IP 地址、文件名、文件位置进行设置

8．恢复出厂默认配置

Router#write erase

Router#reload

9．设置日期、时间

Router#clock set hh:mm:ss month day year

Router#show clock

10．地址解析

单区域时：Router(config)#ip domain-name hneeu.edu.cn

Router(config)#ip name-server 211.69.0.8

多区域时：Router(config)# ip domain-name hneeu.edu.cn

Router(config)# ip domain-name hneeu.com.cn

Router(config)# ip name-server 211.69.0.8 211.69.0.2 …..211.69.0.9(最多 6 个)

实训四 路由协议配置

动态路由协议的两个基本功能为：维护路由选择表，以路由更新的形式将信息及时地发布给其他路由器。

路由器最常用的度量有：

· 带宽（bandwidth）：链路的数据承载能力。

· 延迟（delay）：把数据包从源端送到目标端所需的时间。

· 负载（load）：在路由器或链路上的通信信息量。

· 可靠性（reliability）：网络中每条通信链路上的差错率。

· 跳数（hopcount）：数据包从源端到达目的端所必须通过的路由器个数。

· 滴答数（ticks）：数据链路延迟。

基本路由算法可分为两种：距离矢量和链路状态。距离矢量算法是确定网络中任一条链路的方向（矢量）和距离，当从源端到目的端存在多条路径时，以距离最短（HOPS）为最优；链路状态（也称最短路径优先）算法需重建整个网络的拓扑结构，当从源端到目的端存在多条路径时，以代价最小（Costs）为最优。

1. RIP 配置

路由信息协议（RIP）是一种应用较早，使用广泛的内部网关协议。RIP 适用于小型网络，是典型的距离向量算法协议。RIP 路由以距离最短（HOPS）的路径为路由。RIP 有三个时钟，分别是：路由更新时钟（每 30 秒）、路由无效时钟（每 90 秒）、路由取消时钟（每 270 秒）。

RIP-1 版本的最大 hops 数是 15，RIP-2 版本的最大 hops 数是 128，大于 15/128 则认为不可到达。因此，在大的网络系统中，hop 数很可能超过规定值，使用 RIP 是很不现实的。另外，RIP 每隔 30 秒才进行信息更新，因此，在大型网络中，坏的链路信息可能要花很长时间才能传播过来，路由信息的稳定时间可能更长，并且在这段时间内可能产生路由环路。

[例 3]RIP 的配置

如图 1 所示，要求：内网 R1、R2、R3 路由器启用 RIP-2 路由协议。注意，在实验时为保证 RIP 路由的有效性，必须删除静态路由，可以保留默认路由。

R1 配置的主要内容：

```
Router(config)#router rip                    //启用 RIP 协议
Router(config-router)#version 2              //使用 RIP-2 协议
Router(config-router)#network 211.69.10.0    //宣告所连 211.69.10.0 网段
Router(config-router)#network 211.69.14.0    //宣告所连 211.69.14.0 子网
Router(config-router)#network 211.69.11.0    //宣告所连 211.69.11.0 子网
```

Router(config-router)#network 211.69.11.4　　//宣告所连 211.69.11.4 子网

其它路由器的主要配置步骤

对于 R2，将所连 211.69.12.0、211.69.11.0、211.69.11.8 网段宣告出来即可；对于 R3，将所连 211.69.13.0、211.69.11.4、211.69.11.8 网段宣告出来即可。

RIP 配置完成后，可使用“ show ip route ”显示 IP 路由选择表。

[例 4]查看路由表

如图 1 所示，以 R3 为例说明路由表的基本内容。

```
Router #sh ip rout
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR
```

说明：

· C：表示该路由器的直连网络

· R：经 RIP 学习的路由

· via：表示路由器发布这条路由及其下一跳地址

· 00：00：24：RIP 在上一次更新路由的时间。

· 120/1：“ 120 ”为管理距离，管理距离越小，路由最优，RIP 的默认管理距离为 120；“ 1 ”为到目标网络的跳数，即 HOPS 为 1。

注意：OSPF 路由中，“ 110/20 ”：“ 110 ” 为管理距离，“ 20 ”为路由开销。

2. OSPF 配置

OSPF（Open Shortest Path First）路由协议是由 IETF（Internet Engineering Task Force）IGP 工作小组于 1987 年开发的一种链路状态路由协议。OSPF 能够适应大型全局 IP 网络的扩展，OSPF 协议的特性包括：支持 VLSM（可变长子网掩吗）、快速收敛、低网络利用、高级路由选择及可用组播传送报文等。

OSPF 协议配置中主要增加的是 OSPF 协议的区域（area）设置。每个区域都有一个区域号，当网络中存在多个区域时，必须存在 0 区域，它是骨干区域，所有其他区域都通过直接或虚链路连接到骨干区域上。为了优化操作，各区域所包含的路由器不应超过 50-70 个。

[例 5]单区域的 OSPF 配置

如图 1 所示，以 R1、R2、R3 为例说明 OSPF 配置的主要内容。

R1 的配置：

Router(config)#router ospf 100　　//启用 OSPF 路由协议，定义 OSPF 进程 ID 号为 100

//进程 ID：1-65535，只在路由器内部起作用，不同路由器一般要求不同。

Router(config-router)#network 211.69.10.0 0.0.0.255 area 0 //宣告直连网段及所在区域为 0

// area 0 相当于 area 0.0.0.0 ；area 1 相当于 area 0.0.0.1

Router(config-router)#network 211.69.11.0 0.0.0.3 area 0 //宣告直连网段及所在区域为 0

Router(config-router)#network 211.69.11.4 0.0.0.3 area 0 //宣告直连网段及所在区域为 0

Router(config-router)#network 211.69.14.0 0.0.0.3 area 0 //宣告直连网段及所在区域为 0

对于 R2，将所连 211.69.12.0、211.69.11.0、211.69.11.8 网段宣告出来并定义区域为 0 即可；对于 R3，将所连 211.69.13.0、211.69.11.4、211.69.11.8 网段宣告出来并定义区域为 0 即可。注意，R1、R2、R3 的区域（area）ID 号必须相同，才能相互交换路由信息；另外，网端后应是子网掩码的反码（通配符）。

[例 6]多区域的 OSPF 配置

如图 2 所示，以 R1、R2、R3、R4 为例说明 OSPF 配置的主要内容。图中各路由器相关接口的 IP 地址如下图 3 所示。

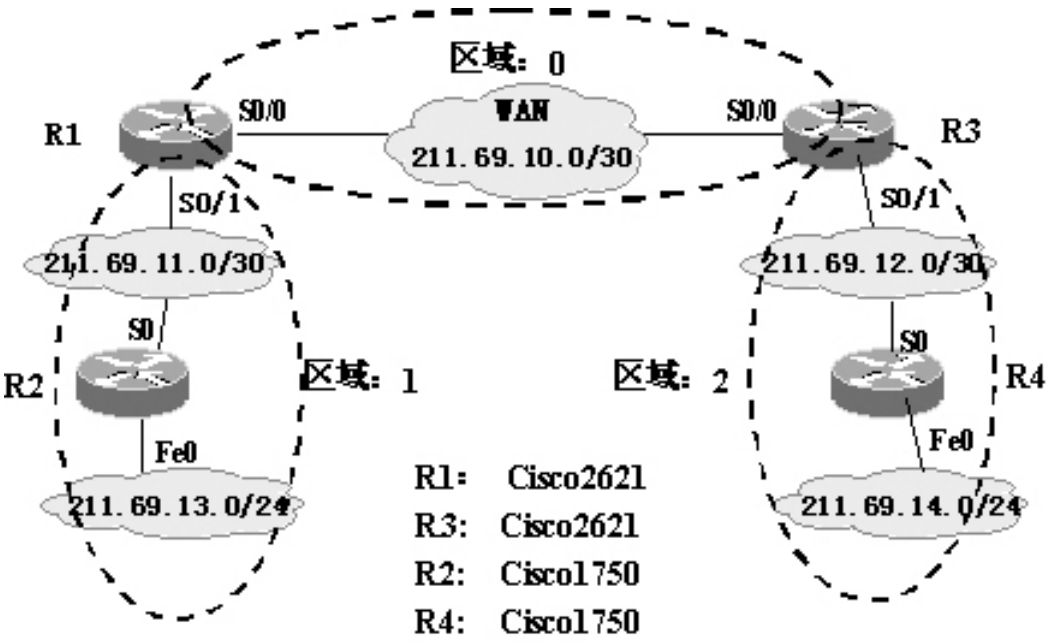


图 2 多区域的 OSPF 配置的网络结构

路由器名称	接口名称	IP地址	子网掩码
R1	S0/0	211.69.10.1	255.255.255.252
	S0/1	211.69.11.1	255.255.255.252
R2	S0	211.69.11.2	255.255.255.252
	FE0	211.69.13.1	255.255.255.0
R3	S0/0	211.69.10.2	255.255.255.252
	S0/1	211.69.12.1	255.255.255.252
R4	S0	211.69.12.2	255.255.255.252
	FE0	211.69.14.1	255.255.255.0

图 3 路由器相关接口的 IP 地址

R1 的主要配置：

```
Router(config)#router ospf 100      //启用 OSPF 路由协议，定义 OSPF 进程 ID 号为 100
Router(config-router)#network 211.69.10.0 0.0.0.3 area 0 //宣告直连网段及所在区域为 0
Router(config-router)#network 211.69.11.0 0.0.0.3 area 1 //宣告直连网段及所在区域为 1
```

R2 的主要配置：

```
Router(config)#router ospf 200      //启用 OSPF 路由协议，定义 OSPF 进程 ID 号为 200
Router(config-router)#network 211.69.11.0 0.0.0.3 area 1 //宣告直连网段及所在区域为 1
Router(config-router)#network 211.69.13.0 0.0.0.255 area 1 //宣告直连网段及所在区域为 1
```

R3 的主要配置：

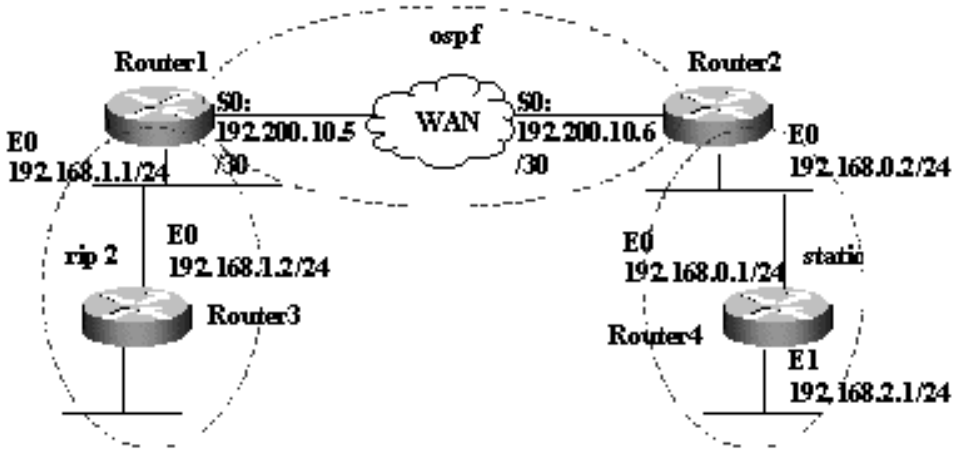
```
Router(config)#router ospf 300      //启用 OSPF 路由协议，定义 OSPF 进程 ID 号为 300
Router(config-router)#network 211.69.10.0 0.0.0.3 area 0 //宣告直连网段及所在区域为 0
Router(config-router)#network 211.69.12.0 0.0.0.3 area 2 //宣告直连网段及所在区域为 2
```

R4 的主要配置：

```
Router(config)#router ospf 400      //启用 OSPF 路由协议，定义 OSPF 进程 ID 号为 400
Router(config-router)#network 211.69.12.0 0.0.0.3 area 2 //宣告直连网段及所在区域为 2
Router(config-router)#network 211.69.14.0 0.0.0.255 area 2 //宣告直连网段及所在区域为 2
```

[例 7]多路由协议配置（重新分配路由或称再分布路由-选讲）

在实际工作中，用户会遇到使用多个 IP 路由协议的网络。为了使整个网络正常地工作，必须在多个路由协议之间进行路由再分配，这样不同的路由协议间就可相互通告路由信息了。（***不配再分配，同一协议间交换，不同协议间不交换路由信息***）



Router1 的 S0 端口和 Router2 的 S0 端口运行 OSPF，在 Router1 的 E0 端口运行 RIP-2，Router3 运行 RIP-2，Router2 有指向 Router4 的 192.168.2.0/24 网段的静态路由，Router4 使用默认静态路由。需要在 Router1 和 Router3 之间重新分配 OSPF 和 RIP 路由，在 Router2 上重新分配静态路由和直连的路由。

涉及的命令：

任　务	命　　令
重新分配直连的路由	redistribute connected
重新分配静态路由	redistribute static
重新分配 ospf 路由	redistribute ospf *process-id* metric *metric-value*
重新分配 rip 路由	redistribute rip metric *metric-value*

Router1 配置：

```
#interface ethernet 0
#ip address 192.168.1.1 255.255.255.0
#interface serial 0
#ip address 192.200.10.5 255.255.255.252
#router ospf 100
#redistribute rip metric 10   //重新分配 RIP 路由，度量值为 10。
#network 192.200.10.4 0.0.0.3 area 0
#router rip
# version 2
#redistribute ospf 100 metric 1 //重新分配 OSPF 路由，度量值为 1。
```

```
#network 192.168.1.0
```

Router2 配置：

```
#interface loopback 1  // Router2 承担路由汇总，可减少网络中路由表的大小。
        // loopback 1 为回送借口，是一个虚拟接口，为 OSPF 指定一个路由器 ID。
# ip address 192.168.3.2 255.255.255.0
      //该地址需是网络中唯一地址，保证此路由器 ID 在整个网络中是独一的。
#interface ethernet 0
# ip address 192.168.0.2 255.255.255.0
#interface serial 0
# ip address 192.200.10.6 255.255.255.252
#router ospf 200
# redistribute connected subnet
# redistribute static subnet
# network 192.200.10.4 0.0.0.3 area 0
#ip route 192.168.2.0 255.255.255.0 192.168.0.1
```

Router3 配置：

```
#interface ethernet 0
# ip address 192.168.1.2 255.255.255.0
#router rip
# version 2
# network 192.168.1.0
```

Router4 配置：

```
#interface ethernet 0
# ip address 192.168.0.1 255.255.255.0
#interface ethernet 1
# ip address 192.168.2.1 255.255.255.0
#ip route 0.0.0.0 0.0.0.0 192.168.0.2
```

实训五 广域网协议配置

目前最流行的 WAN 技术的工作方式以及在 Cisco 路由器上比较常用的广域网协

议配置，包括 PPP、HDLC、帧中继和 DDN 等。

1. PPP 与 HDLC 协议的配置

（1） PPP 协议及配置

PPP（Point to Point Procotol）是 SLIP（Serial Line IP Procotol）协议的继承者，是一种标准的串行线路封装方法，提供了跨过同步和异步电路，实现路由器到路由器或主机到网络的点对点连接。PPP 支持的密码认证协议（PAP）和握手验证协议（CHAP）；还支持动态地址分配、多种协议、及同步、异步通信等。

[例 8] 不需要 PPP 验证的配置

如图 2 所示，以图中 R1、R3 的配置为例进行说明。

R1 的主要配置内容：

```
Router(config)#interface s0/0
Router(config-if)#ip address 211.69.10.1 255.255.255.252
Router(config-if)#enca ppp  //封装 PPP 协议
Router(config-if)#clockrate 130000  //DCE 端需配速率，DTE 端不需配速率
Router(config-if)# no ppp authentication  //默认为不使用验证，因此该步可省略
Router(config-if)#no shutdown
```

R3 的主要配置内容：

```
Router(config)#interface s0/0
Router(config-if)#ip address 211.69.10.2 255.255.255.252
Router(config-if)#enca ppp  //封装 PPP 协议
Router(config-if)#no ppp authentication  //默认为不使用验证，因此该步可省略
Router(config-if)#no shutdown
```

注意：路由的配置

[例 9] CHAP 验证配置

如图 2 所示，以图中 R1、R3 的配置为例进行说明。

R1 的主要配置内容：

```
Router(config)#hostname router1
Router1(config)#username router3 password 1618  //建立对端路由器名和验证密码
Router1(config)#interface s0/0
Router1(config-if)#ip address 211.69.10.1 255.255.255.252
Router1(config-if)#enca ppp  //封装 PPP 协议
Router1(config-if)#clockrate 130000
Router1(config-if)#ppp authentication chap  //配置验证模式为 CHAP
Router(config-if)#no shutdown
```

R3 的主要配置内容：

```
Router(config)#hostname router3
Router3(config)#username router1 password 1618    //建立对端路由器名和验证密码
Router3(config)#interface s0/0
Router3(config-if)#ip address 211.69.10.2 255.255.255.252
Router3(config-if)#enca ppp   //封装 PPP 协议
Router3(config-if)#ppp authentication chap   //配置验证模式为 CHAP
Router(config-if)#no shutdown
```

注意：1、需配置路由，2、两端的验证密码须一致。

（2）HDLC 协议及配置

HDLC（High-level Data Link Control）协议是高级数据链路控制协议，它是 Cisco 串行线路的默认封装协议，与其他供应商设备不兼容，它是 Cisco 的默认封装协议，正常情况下，是不用配置的。

HDLC 配置命令如下：

encapsulation hdlc

其他配置和验证方法同 PPP 配置，此处不再详述。

2. DDN 专线连接的配置

在实际工程中，Cisco 路由器接 DDN 专线时，一般采用 HDLC 协议封装，同步串口需通过 V.35 或 RS232 DTE 线缆连接 CSU/DSU（通信服务单元/数据服务单元），则 Cisco 路由器为 DTE，CSU/DSU 为 DCE，由 DCE 端提供时钟。如果将两台路由器通过 V.35 线缆进行背对背直接相连，则必须由连接 DCE 线缆的一方路由器提供同步时钟。

Cisco2600 系列产品的高速串口最高可支持到 2Mbps，同步-异步串口在同步方式下支持 128Kbps，在异步方式下支持 115.2Kbps。

[例 10] DDN 配置（略）

如图 2 所示，以图中 R1、R3 背对背连接配置为例进行说明。

R1 的主要配置内容：

```
Router(config)#interface serial 0/0
Router(config-if)#ip address 211.69.10.1   255.255.255.252
Router(config-if)#encapsulation hdlc    //封装 HDLC 协议
Router(config-if)#clockrate 2000000    //在 DCE 端配置同步时钟
```

R3 的主要配置内容：

```
Router(config)#interface serial 0/0
Router(config-if)#ip address 211.69.10.2   255.255.255.252
```

Router(config-if)#encapsulation hdlc　//封装 HDLC 协议

实训六　远程访问配置

远程访问可以让网络延伸超越电缆网络的物理边界，延伸到世界的各个角落，只需要一个接收拨入连接的远程访问服务器，一个拥有拨号软件的远程访问客户及一对 Modem 即可。

远程访问连接链路一般都是从网络服务提供商（ISP）那里租用来的。远程客户和远程服务器必须共享至少一个网络传输协议，如 TCP/IP 协议。另外，需要一个链路协议，建立客户机和服务机之间的电话线或 Internet 连接。用于建立连接的协议有：SLIP(Serial Line Intemet Protocol)和 PPP（Point-to-Point Prorocol，目前最常用的是 PPP 协议。

远程访问服务器是一个特殊类型的路由器，它们为通过拨号连接的远程用户提供网络访问服务。大多数访问服务器主要通过调制解调器拨入连接，拨入连接的总数目要由连接到访问服务器的所有租用线路中可用信道的数目来决定。

Cisco 路由器分为固定配置的和模块化的两大类。固定配置路由器，如 2500 系列，预先配备有固定的局域网和广域网接口，不需要另配广域网接口卡或网络模块，一旦选定后，可用的接口就限制在出厂时安装的。

模块化路由器和访问服务器，如 3600，备有 1 个或多个插槽，允许用户根据自己的需要配置不同的插卡。用户可通过选择各种特性插卡、网络模块或广域网接口卡等来确定路由器接口的类型。

[例 11] 远程接入配置

如图 1 所示，以图中 R3 来说明实现路由器拨号访问连接建立的主要配置。

R3 的主要配置：

```
Router(config)#interface group-async1     //定义 group-async1
Router(config-if)#ip unnumbered e0         //引用 E0 端口的 IP 地址
Router(config-if)#ip tcp header-compres passive     //使用 IP 头指针压缩
Router(config-if)#enca ppp                  //封装 PPP 协议
Router(config-if)#async default routing         //允许异步口路由
Router(config-if)#async dynamic routing          //允许异步口动态路由
Router(config-if)#async mode interactive         //异步口交互模式
Router(config-if)#peer default ip address pool xlx   //定义一名为 xlx 的地址池
Router(config-if)#group-rang 1 8               //将 Modem 号 1-8 编组
Router(config)#router rip
Router(config-router)#version 2                    //启用 RIPv2 协议
```

```
Router(config-router)#network 211.69.15.0        //宣告 211.69.15.0 网段
Router(config-router)#exit
Router(config)#ip local pool xlx 211.69.15.1 211.69.15.8  //定义 8 个 IP 地址
Router(config)#line 1 8                  //定义 8 条 Modem 拨号线路
Router(config-line)#autoselect ppp         //自动选择 ppp 协议
Router(config-line)#login local             //将读取用户名和密码
Router(config-line)#modem inout             //允许 Modem 拨入拨出
Router(config-line)#autocommand ppp         //连接建立后，自动进入 ppp 模式
Router(config-line)#transport input all     //连接建立后，允许使用所有协议
Router(config-line)#stopbits 1              //定义 1 位停止位
Router(config-line)#rxspeed 38400           //设置接受速率
Router(config-line)#txspeed 38400           //设置发送速率
Router(config-line)#flowcontrol hard        //设置硬件流控
Router(config-line)#exit
Router(config)#username user1 password 1   //定义拨号用户名和口令
                                           //此处可成批定义拨号用户
```

注意：

- 路由的配置。
- 使用小型程控交换机将异步口的 Modem 和拨号上网微机的 Modem 连接起来，拨号的号码由异步口所连程控交换机的端口号码决定。
- 异步口的发送和接受速率要和所用 Modem 匹配。如果能够拨号，但连接总是建立不起来，可将异步口的速率设置低一些。

实训七　NAT 配置与局域网访问 Internet

如果想连接 Internet，但不想让网络内的所有计算机都拥有一个真正的 IP 地址，通过 NAT（网络地址转换）功能，可以将申请的合法 IP 地址统一管理，当内网的计算机需要上 Internet 时，动态或静态地将内网私有的 IP 地址转换为 Internet 合法的 IP 地址。

最常用的两种地址分配方式为：静态地址分配和动态地址分配。

静态地址分配是用户在地址转换查找表中配置具体的地址转换对，即将指定的内部地址静态地映射到指定的外部地址。内部地址和外部地址的静态映射是一对一的。

动态地址分配是在知道对那些内部地址必须进行转换、可以用那些合法地址做为外部地址时，一个主机根据使用需求被 NAT 设备转换的过程。动态转换可以使用

多个合法外部地址集，也可以共享一个合法外部 IP 地址，后者是通过改变外出数据包的源端口并进行端口映射完成的，这就是 PAT（端口地址翻译）技术。

1. 静态 NAT 的配置

要启用基本的静态 IP 地址转换，需完成下列步骤：

步骤一：在路由器上配置 IP 路由和 IP 地址。

步骤二：用“ ip nat inside source static local-ip global-ip ”全局配置命令。其中，“ local-ip ”指定内部网络中的私用地址，“ global-ip ”指定一个内部全局地址，这个地址须是一个合法 IP 地址。

步骤三：进入相应的接口配置模式，输入“ ip nat {inside|outside} ”命令，在一个内部和一个外部接口上启用 NAT。

[例 12] 静态 NAT 的配置

如图 5 所示，以图中 R1 来说明实现静态 NAT 的配置。

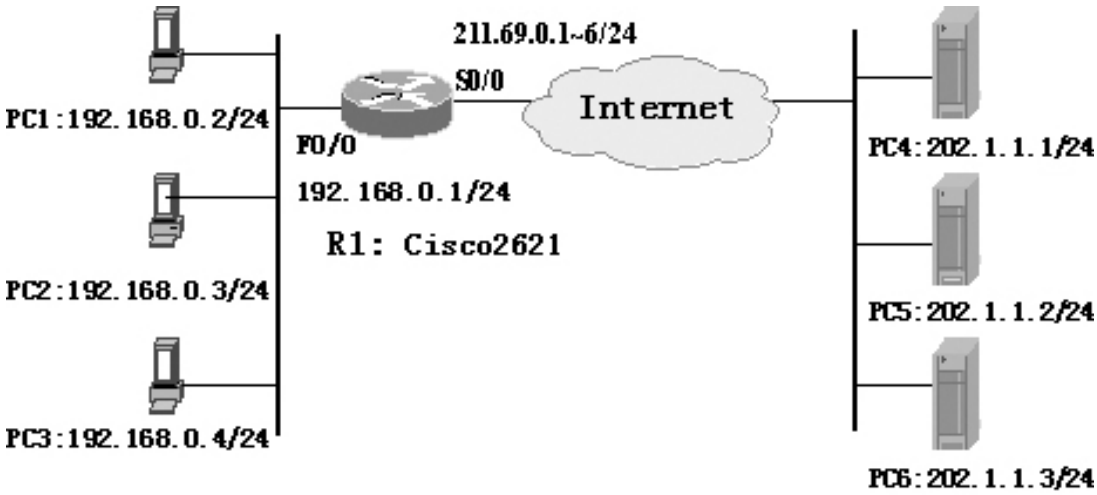


图 4 网络结构示意图

R1 的主要配置：

Router(config)#ip nat inside source static 192.168.0.2 211.69.0.2

//定义内部地址 192.168.0.2，转换外部地址为 211.69.0.2

Router(config)#ip nat inside source static 192.168.0.3 211.69.0.2

//定义内部地址 192.168.0.3，转换外部地址为 211.69.0.2

Router(config)#ip nat inside source static 192.168.0.4 211.69.0.2

//定义内部地址 192.168.0.4，转换外部地址为 211.69.0.2

Router(config)# interface　FastEthernet0/0

```
Router(config-if)# ip address 192.168.0.1 255.255.255.0
```

Router(config-if)# ip nat inside　　//指定 FE0/0 为内网接口
Router(config)# interface　serial 0/0
Router(config-if)# ip address 211.69.0.1 255.255.255.0
Router(config-if)# ip nat outside　　//指定 S0/0 为外网接口

2. 动态 NAT 的配置

要启用动态 IP 地址转换，需完成下列步骤：

步骤一：在路由器上配置 IP 路由和 IP 地址。

步骤二：用“ access-list access-list-number {permit | deny} local-ip-address ”命令为内部网络定义一个标准的 IP 访问控制列表。访问控制列表的内容将在下一节介绍。

步骤三：用“ ip nat pool pool-name start-ip end-ip {netmask netmask | prefix-length prefix-length}[type-rotary] ”，为内部定义一个 NAT 地址池，该命令中参数的含义如下。

（1） pool-name ：地址池的名字
（2） start-ip：地址池中地址范围的开始 IP 地址
（3） end-ip：地址池中地址范围的结束 IP 地址
（4） netmask：地址池中地址所属网络的网络掩码。
（5） prefix-length：掩码中 1 的个数。
（6） type-rotary：真正的内部的主机的地址池中的地址的范围，用于 TCP 负载均衡，此参数可选。

步骤四：用“ ip nat inside source list access-list-number pool-name ”命令将访问控制列表映射到 NAT 地址集。

步骤五：进入相应的接口配置模式，输入“ ip nat {inside | outside} ”命令，以在至少一个内部和一个外部接口上启用 NAT。

[例 13] 动态 NAT 的配置

如图 5 所示，以图中 R1 来说明实现动态 NAT 的配置。

R1 的主要配置：

```
Router(config)# ip nat pool xlx 211.69.0.2 211.69.0.6 netmask 255.255.255.0
```

//定义内部地址池“ XLX ”，地址范围为：211.69.0.2 到 211.69.0.6

```
Router(config)# access-list 1 permit 192.168.1.0  0.0.0.255
```

//定义一个标准访问控制列表“ 1 ”，源地址为 192.168.1.0/24 的网络设为允许

Router(config)#ip nat inside source list 1 pool xlx

//将访问控制列表“1”映射到地址池“XLX”

Router(config)# interface　FastEthernet0/0

Router(config-if)# ip address 192.168.0.1 255.255.255.0

Router(config-if)# ip nat inside　//指定 FE0/0 为内网接口

Router(config)# interface　serial 0/0

Router(config-if)# ip address 211.69.0.1 255.255.255.0

Router(config-if)# ip nat outside　//指定 S0/0 为外网接口

Router(config-if)#ip access-group 1 out　//设置访问控制列表到 S0/0 接口，方向为控制出。

实训八　访问控制列表配置

网络管理最重要的任务之一就是网络安全，实现网络安全的一种方法便是使用路由器提供的基于数据包的过滤功能，即访问控制列表 ACL（Access Control List），其能在路由器接口处决定哪种类型的信息流量被转发，哪种类型的信息流量被拒绝。

在 Cisco 路由器中，每个访问控制列表的执行顺序是“从上到下，顺序判断”，每一条新加的列表项都被安置在访问控制列表的最后面。所以，当一个 ACL 建好之后，就不能通过行号删除某一指定的列表项。当需要另外增加一列表项时，只能采取删处该 ACL，然后再重新建立一个新的带有一系列条件判断语句（列表项）的 ACL。这就是为什么要在一台 PC 上使用文本编辑器编辑好路由器的 ACL 后，再通过 TFTP 把它上传到路由器的原因。

另外，访问控制列表的结尾处有一个隐含的“deny all”，一般情况下，隐含拒绝并不会出现在配置文件中，所以，如果某数据包在 ACL 的最后一条规则上停止，它将被抛弃。

访问控制列表有两种基本类型

- 标准类型。列表号的范围为：1~99，其只对数据包中的源地址进行检查。
- 扩展类型。列表号的范围为：100~199，其可对数据包中的源地址、目标地址、协议及端口号进行检查。

1. 标准访问控制列表有两种基本类型

1、标准访问控制列表的语法

Access-list access-list-number{deny|permit} source[source-wildcard] [log]

可以通过在“access-list”命令前加“no”的形式，来删除一个已经建立的标准 ACL。

access-list 命令参数的含义如下：

（1） access-list-number：访问控制列表号，标准访问控制列表的号码范围是 1~99。

（2） deny：如果满足条件，数据包被拒绝从该入口通过。

（3） permit：如果满足条件，数据包允许从该入口通过。

（4） source：数据包的源网络地址，源网络地址可以是具体的地址或 any（任意），如果源地址是单个 IP 地址时，将“ source ”改成“ host ”，后再写 IP 地址即可。

（5） Source-wildcard：可选项，分配给源地址的通配符的位数，默认时，该字段是 0.0.0.0。

（6） Log：可选项，生成日志信息，记录匹配 permit 或 deny 语句的包。

2. 地址和通配符掩码

当使用标准访问控制列表时，源地址必须被指定。源地址可以是一台主机、一组主机或是整个子网的地址。源地址的范围是由通配符字段来确定。通配符掩码是一个 32 比特位的数字字符串，使用 1 或 0 来表示，它被用“ . ”分成 4 组，每组 8 位。在通配符掩码位中，0 表示“ 检查相应的位 ”，而 1 表示不检查相应位。通配符掩码相当于子网掩码的反码。

[例 14] 通配符掩码的匹配

```
211.69.10.0  0.0.0.255
    //匹配的是 211.69.10.0/24 这个 C 类网段，包括：211.69.10.0~211.69.10.255。
211.69.10.0  0.0.0.3
    //匹配的是 211.69.10.0/30 这个子网段，包括：211.69.10.0~211.69.10.3。
211.69.10.0  0.0.0.15
    //匹配的是 211.69.10.0/28 这个子网段，包括：211.69.10.0~211.69.10.15。
211.69.10.0  0.0.0.31
    //匹配的是 211.69.10.0/27 这个子网段，包括：211.69.10.0~211.69.10.31
211.69.0.0  0.0.15.255
    //匹配的是 211.69.0.0/20 这个网段，包括：211.69.0.0~211.69.15.255。
172.15.0.0  0.0.255.255
    //匹配的是 172.15.0.0/16 这个 B 类网段，包括：172.15.0.0~172.15.255.255。
```

3. 关键字 any 和 host 的用法

（1）any。指定对允许所有的 IP 地址作为源地址。这样，当某环境下允许访问任何目的地址时，我们就不用输入 source 位为“ 0.0.0.0 ”，再输入通配符掩码为“ 255.255.255.255 ”了，直接使用“ any ”就可以了。下面两行指令是等价的。

```
access-list 1 permit 0.0.0.0 255.255.255.255
access-list 1 permit any
```

（2）host。用在访问表中指定通配符掩码是 0.0.0.0。这样某环境下要输入单个的地址，如 172.16.8.1，就不用输入 172.16.8.1 和通配符掩码 0.0.0.0 了，直接在地址前加 host 就可以了。下面两行指令是等价的。

access-list 1 permit 172.16.8.1 0.0.0.0

access-list 1 permit host 172.16.8.1

4．ACL 的使用

在创建了一个访问控制列表并分配了表号之后，为了让该访问控制列表真的起作用，用户必须把它配置到一个接口上且指明应用的数据流方向。

语法是：ip access-group access-list-number {in|out}

对于该命令，要记住的是在每个端口、每个协议、每个方向上只能有一个访问控制列表。其，下面列出了 access-group 命令参数的含义。

（1） Ip：定义所用的协议。

（2） access-list-number：访问控制列表的号码。

（3） in |out：定义 ACL 是被应用到接口的流入方向（in），还是接口的流出方向（out）。

注意：访问控制列表一般配置在内网的出口上。

[例 15] 标准访问控制列表的配置

如图 5 所示，以图中 R1 来说明实现标准访问控制列表的配置。

要求：允许内网 192.168.0.0/24 访问 Internet，但拒绝此网络中主机 192.168.0.2 访问 Internet。

R1 的主要配置：

Router(config)# access-list 1 deny host 192.168.0.2

Router(config)# access-list 1 permit 192.168.0.0 0.0.0.255

Router(config)# interface　fastethernet 0/0

Router(config-if)# ip access-group 1 out

注意：因标准访问控制列表的执行是从上到下顺序进行的，所以，一定要注意每个列表项的书写顺序。

2. 扩展访问控制列表

能进行更精确的包过滤控制，包括：数据包的源地址、数据包的目的地址、协议类型、端口号等。

1．扩展访问控制列表的语法

扩展 ACL 也是在全局配置模式下进行设计的，其命令“access-list”的完全语法格式为：

access-list access-list-number {deny|permit} protocol source[source-mask destination destination-mask] [operator operand] [established]

命令参数的主要含义如下：

（1） access-list-number：访问控制列表号，范围为 100-199。

（2） deny：如果满足条件，数据包被拒绝通过。

（3） permit：如果满足条件，数据包允许通过。

（4） protocol：指定协议类型，如 IP/TCP/UDP/ICMP 等。

（5） source：源地址。

（6） destination：目的地址。

（7） source-mask：源通配符掩码。

（8） destination-mask：目的通配符掩码。

（9） operator operand：可为 it|gt|eq|neq，分别表示“小于|大于|等于|不等于”端口号。

（10） established：可选项。

2．访问控制的参数

（1）协议及协议的端口号

可以使用扩展 ACL 来过滤多种不同协议，如 TCP、UDP、ICMP 和 IP。在扩展 ACL 中，要指定上层 TCP 或 UDP 端口号，从而选择允许或拒绝的协议。常见的端口号及其对应协议为：20/21：FTP；23：Telnet；25：SMTP；69：TFTP；53：DNS；80：Http 等，详细的可参见 Cisco 的有关书目。

（2）地址和通配符掩码

扩展 ACL 的 IP 地址和通配符掩码的使用，同标准 ACL，此处不再详述。

[例 16]扩展访问控制列表的配置

如图 5 所示，以图中 R1 来说明实现扩展访问控制列表的配置。

要求：假设图 5 中的 PC1 为内网的 WWW 服务器，PC2 为内网的 FTP 服务器，PC3 为内网中的特定计算机，PC4 为外网中的特定计算机。现要求，内网的 WWW、FTP 服务器能对外提供服务，内网只有特定计算机 PC3 能访问外网；外网均可访问内网的 WWW、FTP 服务器，外网除特定计算机 PC4 外，均不能访问内网。

说明：本例假设内网的 192.168.0.0/24 地址为可用地址，即为合法的 IP 地址，不再考虑地址转换问题。

R1 的主要配置：

```
Router(config)#access-list 101 permit tcp host 192.168.0.2 any eq 80
Router(config)#access-list 101 permit tcp host 192.168.0.3 any eq 21
Router(config)#access-list 101 permit ip host 192.168.0.4 any
Router(config)#access-list 101 deny ip 192.168.0.0 0.0.0.255 any
Router(config)#access-list 102 permit ip host 202.1.1.1 any
Router(config)#access-list 102 permit ip 202.1.1.0 0.0.0.255 any eq 80
Router(config)#access-list 102 permit ip 202.1.1.0 0.0.0.255 any eq 21
Router(config)#access-list 102 deny ip any any
```

```
Router(config)#interface s0/0
Router(config-if)#ip access-group 101 out
Router(config-if)#ip access-group 102 in
```

实训九　IP 电话的配置（选讲）

如图 1，在 R1、R2 之间路由建立好且 Voice/Fax 语音接口模块配置好的前提下，完成 R1、R2 之间 IP 电话功能的设定。

1．　R1(Cisco 2621)端配置的关键步骤

```
#config ter
*以下为 R1 本端的定义*
#dial-peer voice 262101 pots    //定义第一个语音端口
#destination-pattern 888        //定义电话号码 888
#port 1/0/0                     //指定语音端口
#exit
#dial-peer voice 262102 pots    //定义第二个语音端口
#destination-pattern 777        //定义电话号码 777
#port 1/0/1                     //指定语音端口
#exit
*以下为 R1 对端的定义*
#dial-peer voice 262103 voip    //定义对端的 voip 功能
#destination-pattern 666        //定义电话号码 666
#ip precedence 5                //定义 IP 语音的优先级
#session target ipv4:211.69.11.2 //定义对端的 IP 地址
#exit
#dial-peer voice 262104 voip    //定义对端的 voip 功能
#destination-pattern 555        //定义电话号码 555
#ip precedence 5                //定义 IP 语音的优先级
#session target ipv4:211.69.11.2 //定义对端的 IP 地址
#exit
#copy running-config startup-config        //保存配置
```

2． R2(Cisco 1750)端配置的关键步骤

R2 的配置基本上同 R1，以下仅写出步骤，不再描述。

```
#config termial
*以下为 R2 本端的定义*
#dial-peer voice 175001 pots
#destination-pattern 666
#port 2/0
#exit
#dial-peer voice 175002 pots
#destination-pattern 555
#port 2/1
#exit
*以下为 R2 对端的定义*
#dial-peer voice 175003 voip
#destination-pattern 888
#ip precedence 5
#session target ipv4:211.69.11.1
#exit
#dial-peer voice 175004 voip
#destination-pattern 777
#ip precedence 5
#session target ipv4:211.69.11.1
#exit
#copy running-config startup-config        //保存配置
```

3． 关键问题及注意事项

- R1、R2 路由器的 flash 版本一定要支持 IP 电话功能。
- IP 语音优先级的范围为 0~5，其中 5 为最高级。
- 使用普通电话机即可，无需专用 IP 电话机。
- 两路由器本、对端电话号码的定义务必一致。
- 路由配置。