CISCO 路由器配置命令详解及实例

目录

第一章：路由器配置基础

一、基本设置方式

一般来说，可以用 5 种方式来设置路由器：
1．Console 口接终端或运行终端仿真软件的微机；
2．AUX 口接 MODEM，通过电话线与远方的终端或运行终端仿真软件的微机相连；
3．通过 Ethernet 上的 TFTP 服务器；
4．通过 Ethernet 上的 TELNET 程序；
5．通过 Ethernet 上的 SNMP 网管工作站。
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

二、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 RXBOOT 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。
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。

三、设置对话过程

显示提示信息
全局参数的设置
接口参数的设置
显示结果
利用设置对话过程可以避免手工输入命令的烦琐，但它还不能完全代替手工设置，一些特殊的设置还必须通过手工输入的方式完成。
进入设置对话过程后，路由器首先会显示一些提示信息：

```
--- System Configuration Dialog ---
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
```

这是告诉你在设置对话过程中的任何地方都可以键入“？”得到系统的帮助，按ctrl-c 可以退出设置过程，缺省设置将显示在‘[]’中。然后路由器会问是否进入设置对话：

```
Would you like to enter the initial configuration dialog? [yes]:
```

如果按 y 或回车，路由器就会进入设置对话过程。首先你可以看到各端口当前的状况：

```
First, would you like to see the current interface summary? [yes]:
Any interface listed with OK? value "NO" does not have a valid
configuration
Interface  IP-Address  OK?  Method  Status  Protocol
Ethernet0  unassigned  NO  unset  up  up
Serial0  unassigned  NO  unset  up  up
……  ……  …  ……  …  …
```

然后，路由器就开始全局参数的设置：

```
Configuring global parameters:
```

1. 设置路由器名：

```
Enter host name [Router]:
```

2.设置进入特权状态的密文(secret)，此密文在设置以后不会以明文方式显示：

```
The enable secret is a one-way cryptographic secret used
instead of the enable password when it exists.
Enter enable secret: cisco
```

3. 设置进入特权状态的密码(password)，此密码只在没有密文时起作用，并且在设置以后会以明文方式显示：

```
The enable password is used when there is no enable secret
and when using older software and some boot images.
Enter enable password: pass
```

4. 设置虚拟终端访问时的密码：

```
Enter virtual terminal password: cisco
```

5. 询问是否要设置路由器支持的各种网络协议：

Configure SNMP Network Management? [yes]:
Configure DECnet? [no]:
Configure AppleTalk? [no]:
Configure IPX? [no]:
Configure IP? [yes]:
Configure IGRP routing? [yes]:
Configure RIP routing? [no]:
……
6. 如果配置的是拨号访问服务器，系统还会设置异步口的参数：
Configure Async lines? [yes]:
1) 设置线路的最高速度：
Async line speed [9600]:
2) 是否使用硬件流控：
Configure for HW flow control? [yes]:
3) 是否设置 modem：
Configure for modems? [yes/no]: yes
4) 是否使用默认的 modem 命令：
Configure for default chat s cript? [yes]:
5) 是否设置异步口的 PPP 参数：
Configure for Dial-in IP SLIP/PPP access? [no]: yes
6) 是否使用动态 IP 地址：
Configure for Dynamic IP addresses? [yes]:
7) 是否使用缺省 IP 地址：
Configure Default IP addresses? [no]: yes
8) 是否使用 TCP 头压缩：
Configure for TCP Header Compression? [yes]:
9) 是否在异步口上使用路由表更新：
Configure for routing updates on async links? [no]: y
10) 是否设置异步口上的其它协议。
接下来，系统会对每个接口进行参数的设置。
1. Configuring interface Ethernet0:
1) 是否使用此接口：
Is this interface in use? [yes]:
2) 是否设置此接口的 IP 参数：
Configure IP on this interface? [yes]:
3) 设置接口的 IP 地址：
IP address for this interface: 192.168.162.2
4) 设置接口的 IP 子网掩码：
Number of bits in subnet field [0]:
Class C network is 192.168.162.0, 0 subnet bits; mask is /24
在设置完所有接口的参数后，系统会把整个设置对话过程的结果显示出来：
The following configuration command s cript was created:
hostname Router
enable secret 5 1W5Oh$p6J7tIgRMBOIKVXVG53Uh1

enable password pass
……
请注意在 enable secret 后面显示的是乱码，而 enable password 后面显示的是设置的内容。
显示结束后，系统会问是否使用这个设置：
Use this configuration? [yes/no]: yes
如果回答 yes，系统就会把设置的结果存入路由器的 NVRAM 中，然后结束设置对话过程，使路由器开始正常的工作。

四、常用命令

1. 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。
2. 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
3. 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 router
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　trace 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
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

五、配置 IP 寻址

1. IP 地址分类

IP 地址分为网络地址和主机地址二个部分，A 类地址前 8 位为网络地址，后 24 位为主机地址，B 类地址 16 位为网络地址，后 16 位为主机地址，C 类地址前 24 位为网络地址，后 8 位为主机地址，网络地址范围如下表所示：

种类 网络地址范围
A 1.0.0.0 到 126.0.0.0 有效 0.0.0.0 和 127.0.0.0 保留
B 128.1.0.0 到 191.254.0.0 有效 128.0.0.0 和 191.255.0.0 保留
C 192.0.1.0 到 223.255.254.0 有效 192.0.0.0 和 223.255.255.0 保留
D 224.0.0.0 到 239.255.255.255 用于多点广播
E 240.0.0.0 到 255.255.255.254 保留 255.255.255.255 用于广播

2. 分配接口 IP 地址

任务 命令
接口设置 interface type slot/number
为接口设置 IP 地址 ip address ip-address mask

掩玛（mask）用于识别 IP 地址中的网络地址位数，IP 地址（ip-address）和掩码（mask）相与即得到网络地址。

3. 使用可变长的子网掩码

通过使用可变长的子网掩码可以让位于不同接口的同一网络编号的网络使用不同的掩码，这样可以节省 IP 地址，充分利用有效的 IP 地址空间。

如下图所示：

Router1 和 Router2 的 E0 端口均使用了 C 类地址 192.1.0.0 作为网络地址，Router1 的 E0 的网络地址为 192.1.0.128, 掩码为 255.255.255.192, Router2 的 E0 的网络地址为 192.1.0.64,掩码为 255.255.255.192，这样就将一个 C 类网络地址分配给了二个网，既划分了二个子网，起到了节约地址的作用。

4. 使用网络地址翻译（NAT）

NAT（Network Address Translation）起到将内部私有地址翻译成外部合法的全局地址的功能，它使得不具有合法 IP 地址的用户可以通过 NAT 访问到外部 Internet.

当建立内部网的时候,建议使用以下地址组用于主机,这些地址是由 Network Working Group(RFC 1918)保留用于私有网络地址分配的.
?; Class A:10.1.1.1 to 10.254.254.254
?; Class B:172.16.1.1 to 172.31.254.254
?; Class C:192.168.1.1 to 192.168.254.254
命令描述如下：
任务　命令
定义一个标准访问列表　access-list access-list-number permit source [source-wildcard]
定义一个全局地址池　ip nat pool name start-ip end-ip {netmask netmask | prefix-length prefix-length} [type rotary]
建立动态地址翻译　ip nat inside source {list {access-list-number | name} pool name [overload] | static local-ip global-ip}
指定内部和外部端口　ip nat {inside | outside}
如下图所示，
路由器的 Ethernet 0 端口为 inside 端口，即此端口连接内部网络，并且此端口所连接的网络应该被翻译，Serial 0 端口为 outside 端口，其拥有合法 IP 地址（由 NIC 或服务提供商所分配的合法的 IP 地址),来自网络 10.1.1.0/24 的主机将从 IP 地址池 c2501 中选择一个地址作为自己的合法地址，经由 Serial 0 口访问 Internet。命令 ip nat inside source list 2 pool c2501 overload 中的参数 overload,将允许多个内部地址使用相同的全局地址(一个合法 IP 地址，它是由 NIC 或服务提供商所分配的地址）。命令 ip nat pool c2501 202.96.38.1 202.96.38.62 netmask 255.255.255.192 定义了全局地址的范围。
设置如下：

```
ip nat pool c2501 202.96.38.1 202.96.38.62 netmask 255.255.255.192
interface Ethernet 0
ip address 10.1.1.1 255.255.255.0
ip nat inside
!
interface Serial 0
ip address 202.200.10.5 255.255.255.252
ip nat outside
!
ip route 0.0.0.0 0.0.0.0 Serial 0
access-list 2 permit 10.0.0.0 0.0.0.255
! Dynamic NAT
!
ip nat inside source list 2 pool c2501 overload
line console 0
exec-timeout 0 0
!
line vty 0 4
end
```

六、配置静态路由

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。
以下在 Router1 上设置了访问 192.1.0.64/26 这个网下一跳地址为 192.200.10.6,即当有目的地址属于 192.1.0.64/26 的网络范围的数据报，应将其路由到地址为 192.200.10.6 的相邻路由器。在 Router3 上设置了访问 192.1.0.128/26 及 192.200.10.4/30 这二个网下一跳地址为 192.1.0.65。由于在 Router1 上端口 Serial 0 地址为 192.200.10.5，192.200.10.4/30 这个网属于直连的网，已经存在访问 192.200.10.4/30 的路径，所以不需要在 Router1 上添加静态路由。
Router1:
ip route 192.1.0.64 255.255.255.192 192.200.10.6
Router3:
ip route 192.1.0.128 255.255.255.192 192.1.0.65
ip route 192.200.10.4 255.255.255.252 192.1.0.65
同时由于路由器Router3除了与路由器Router2相连外,不再与其他路由器相连,所以也可以为它赋予一条默认路由以代替以上的二条静态路由,
ip route 0.0.0.0 0.0.0.0 192.1.0.65
即只要没有在路由表里找到去特定目的地址的路径,则数据均被路由到地址为 192.1.0.65 的相邻路由器。

第二章：广域网协议设置

一、HDLC

HDLC 是 CISCO 路由器使用的缺省协议，一台新路由器在未指定封装协议时默认使用 HDLC 封装。
1. 有关命令
端口设置

任务　命令
设置 HDLC 封装　encapsulation hdlc
设置 DCE 端线路速度　clockrate speed
复位一个硬件接口　clear interface serial unit
显示接口状态　show interfaces serial [unit] 1
注:1.以下给出一个显示 Cisco 同步串口状态的例子.
Router#show interface serial 0
Serial 0 is up, line protocol is up
Hardware is MCI Serial
Internet address is 150.136.190.203, subnet mask is 255.255.255.0
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
Encapsulation HDLC, loopback not set, keepalive set (10 sec)
Last input 0:00:07, output 0:00:00, output hang never
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
Five minute input rate 0 bits/sec, 0 packets/sec
Five minute output rate 0 bits/sec, 0 packets/sec
16263 packets input, 1347238 bytes, 0 no buffer
Received 13983 broadcasts, 0 runts, 0 giants
2 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 2 abort
22146 packets output, 2383680 bytes, 0 underruns
0 output errors, 0 collisions, 2 interface resets, 0 restarts
1 carrier transitions
2. 举例

设置如下：
Router1:
interface Serial0
ip address 192.200.10.1 255.255.255.0
clockrate 1000000
Router2:
interface Serial0
ip address 192.200.10.2 255.255.255.0
!
3. 举例使用 E1 线路实现多个 64K 专线连接.
相关命令:
任务　命令
进入 controller 配置模式　controller {t1 | e1} number
选择帧类型　framing {crc4 | no-crc4}
选择 line-code 类型　linecode {ami | b8zs | hdb3}
建立逻辑通道组与时隙的映射　channel-group number timeslots range1
显示 controllers 接口状态　show controllers e1 [slot/port]2
注: 1. 当链路为 T1 时,channel-group 编号为 0-23, Timeslot 范围 1-24; 当链路为 E1 时, channel-group 编号为 0-30, Timeslot 范围 1-31.

2.使用 show controllers e1 观察 controller 状态,以下为帧类型为 crc4 时 controllers 正常的状态.

```
Router# show controllers e1
e1 0/0 is up.
Applique type is Channelized E1 - unbalanced
Framing is CRC4, Line Code is HDB3 No alarms detected.
Data in current interval (725 seconds elapsed):
0 Line Code Violations, 0 Path Code Violations
0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
Total Data (last 24 hours) 0 Line Code Violations, 0 Path Code Violations,
0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins,
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
```

以下例子为 E1 连接 3 条 64K 专线, 帧类型为 NO-CRC4,非平衡链路,路由器具体设置如下:

```
shanxi#wri t
Building configuration...
Current configuration:
!
version 11.2
no service udp-small-servers
no service tcp-small-servers
!
hostname shanxi
!
enable secret 5 $1$XN08$Ttr8nfLoP9.2RgZhcBzkk/
enable password shanxi
!
!
ip subnet-zero
!
controller E1 0
framing NO-CRC4
channel-group 0 timeslots 1
channel-group 1 timeslots 2
channel-group 2 timeslots 3
!
interface Ethernet0
ip address 133.118.40.1 255.255.0.0
media-type 10BaseT
!
interface Ethernet1
no ip address
shutdown
!
interface Serial0:0
```

```
ip address 202.119.96.1 255.255.255.252
no ip mroute-cache
!
interface Serial0:1
ip address 202.119.96.5 255.255.255.252
no ip mroute-cache
!
interface Serial0:2
ip address 202.119.96.9 255.255.255.252
no ip mroute-cache
!
no ip classless
ip route 133.210.40.0 255.255.255.0 Serial0:0
ip route 133.210.41.0 255.255.255.0 Serial0:1
ip route 133.210.42.0 255.255.255.0 Serial0:2
!
line con 0
line aux 0
line vty 0 4
password shanxi
login
!
end
```

二、PPP

PPP(Point-to-Point Protocol)是 SLIP(Serial Line IP protocol)的继承者，它提供了跨过同步和异步电路实现路由器到路由器(router-to-router)和主机到网络(host-to- network)的连接。

CHAP(Challenge Handshake Authentication Protocol)和 PAP(Password Authentication Protocol) (PAP)通常被用于在 PPP 封装的串行线路上提供安全性认证。使用 CHAP 和 PAP 认证,每个路由器通过名字来识别，可以防止未经授权的访问。

CHAP 和 PAP 在 RFC 1334 上有详细的说明。

1. 有关命令

端口设置

任务　命令

设置 PPP 封装　encapsulation ppp1

设置认证方法　ppp authentication {chap | chap pap | pap chap | pap} [if-needed] [list-name | default] [callin]

指定口令　username name password secret

设置 DCE 端线路速度　clockrate speed

注：1、要使用 CHAP/PAP 必须使用 PPP 封装。在与非 Cisco 路由器连接时，一般采用 PPP 封装，其它厂家路由器一般不支持 Cisco 的 HDLC 封装协议。

2. 举例
路由器Router1和Router2的S0口均封装PPP协议，采用CHAP做认证，在Router1中应建立一个用户，以对端路由器主机名作为用户名，即用户名应为router2。同时在Router2中应建立一个用户，以对端路由器主机名作为用户名，即用户名应为router1。所建的这两用户的 password必须相同。
设置如下：
Router1:
```
hostname router1
username router2 password xxx
interface Serial0
ip address 192.200.10.1 255.255.255.0
clockrate 1000000
ppp authentication chap
!
```
Router2:
```
hostname router2
username router1 password xxx
interface Serial0
ip address 192.200.10.2 255.255.255.0
ppp authentication chap
!
```

三、x.25

1. X25技术
X.25规范对应OSI三层，X.25的第三层描述了分组的格式及分组交换的过程。X.25的第二层由LAPB（Link Access Procedure, Balanced）实现，它定义了用于DTE/DCE连接的帧格式。X.25的第一层定义了电气和物理端口特性。
X.25网络设备分为数据终端设备（DTE）、数据电路终端设备（DCE）及分组交换设备（PSE）。DTE是X.25的末端系统，如终端、计算机或网络主机，一般位于用户端，Cisco路由器就是DTE设备。DCE设备是专用通信设备，如调制解调器和分组交换机。PSE是公共网络的主干交换机。
X.25定义了数据通讯的电话网络，每个分配给用户的x.25 端口都具有一个x.121地址，当用户申请到的是SVC（交换虚电路）时，x.25一端的用户在访问另一端的用户时，首先将呼叫对方x.121地址，然后接收到呼叫的一端可以接受或拒绝，如果接受请求，于是连接建立实现数据传输，当没有数据传输时挂断连接，整个呼叫过程就类似我们拨打普通电话一样，其不同的是x.25可以实现一点对多点的连接。其中x.121地址、htc均必须与x.25服务提供商分配的参数相同。X.25 PVC（永久虚电路），没有呼叫的过程，类似DDN专线。
2. 有关命令:
任务　命令
设置X.25封装　encapsulation x25 [dce]
设置X.121地址　x25 address x.121-address
设置远方站点的地址映射　x25 map protocol address [protocol2

address2[...[protocol9 address9]]] x121-address [option]
设置最大的双向虚电路数 x25 htc citcuit-number1
设置一次连接可同时建立的虚电路数 x25 nvc count2
设置 x25 在清除空闲虚电路前的等待周期 x25 idle minutes
重新启动 x25,或清一个 svc,启动一个 pvc 相关参数 clear x25 {serial number | cmns-interface mac-address} [vc-number] 3
清 x25 虚电路 clear x25-vc
显示接口及 x25 相关信息 show interfaces serial show x25 interface show x25 map show x25 vc
注：1、虚电路号从 1 到 4095，Cisco 路由器默认为 1024，国内一般分配为 16。
2、虚电路计数从 1 到 8，缺省为 1。
3、在改变了 x.25 各层的相关参数后，应重新启动 x25(使用 clear x25 {serial number | cmns-interface mac-address} [vc-number]或 clear x25-vc 命令)，否则新设置的参数可能不能生效。同时应对照服务提供商对于 x.25 交换机端口的设置来配置路由器的相关参数，若出现参数不匹配则可能会导致连接失败或其它意外情况。
3. 实例：
3.1. 在以下实例中每二个路由器间均通过 svc 实现连接。
路由器设置如下：
Router1:
interface Serial0
encapsulation x25
ip address 192.200.10.1 255.255.255.0
x25 address 110101
x25 htc 16
x25 nvc 2
x25 map ip 192.200.10.2 110102 broadcast
x25 map ip 192.200.10.3 110103 broadcast
!
Router2:
interface Serial0
encapsulation x25
ip address 192.200.10.2 255.255.255.0
x25 address 110102
x25 htc 16
x25 nvc 2
x25 map ip 192.200.10.1 110101 broadcast
x25 map ip 192.200.10.3 110103 broadcast
!
Router:
interface Serial0
encapsulation x25
ip address 192.200.10.3 255.255.255.0
x25 address 110103

```
x25 htc 16
x25 nvc 2
x25 map ip 192.200.10.1 110101 broadcast
x25 map ip 192.200.10.2 110102 broadcast
!
```
相关调试命令：
```
clear x25-vc
show interfaces serial
show x25 map
show x25 route
show x25 vc
```
3.2. 在以下实例中路由器 router1 和 router2 均通过 svc 与 router 连接，但 router1 和 router2 不通过 svc 直接连接，此三个路由器的串口运行 RIP 路由协议，使用了子接口的概念。由于使用子接口，router1 和 router2 均学习到了访问对方局域网的路径，若不使用子接口， router1 和 router2 将学不到到对方局域网的路由。

子接口（Subinterface）是一个物理接口上的多个虚接口，可以用于在同一个物理接口上连接多个网。我们知道为了避免路由循环，路由器支持 split horizon 法则，它只允许路由更新被分配到路由器的其它接口，而不会再分配路由更新回到此路由被接收的接口。

无论如何，在广域网环境使用基于连接的接口(象 X.25 和 Frame Relay)，同一接口通过虚电路(vc)连接多台远端路由器时，从同一接口来的路由更新信息不可以再被发回到相同的接口，除非强制使用分开的物理接口连接不同的路由器。Cisco 提供子接口（subinterface）作为分开的接口对待。你可以将路由器逻辑地连接到相同物理接口的不同子接口, 这样来自不同子接口的路由更新就可以被分配到其他子接口，同时又满足 split horizon 法则。

Router1:
```
interface Serial0
encapsulation x25
ip address 192.200.10.1 255.255.255.0
x25 address 110101
x25 htc 16
x25 nvc 2
x25 map ip 192.200.10.3 110103 broadcast
!
router rip
network 192.200.10.0
!
```
Router2:
```
interface Serial0
encapsulation x25
ip address 192.200.11.2 255.255.255.0
x25 address 110102
x25 htc 16
```

```
x25 nvc 2
x25 map ip 192.200.11.3 110103 broadcast
!
router rip
network 192.200.11.0
!
Router:
interface Serial0
encapsulation x25
x25 address 110103
x25 htc 16
x25 nvc 2
!
interface Serial0.1 point-to-point
ip address 192.200.10.3 255.255.255.0
x25 map ip 192.200.10.1 110101 broadcast
!
interface Serial0.2 point-to-point
ip address 192.200.11.3 255.255.255.0
x25 map ip 192.200.11.2 110102 broadcast
!
router rip
network 192.200.10.0
network 192.200.11.0
!
```

四、Frame Relay

1. 帧中继技术

帧中继是一种高性能的WAN协议,它运行在OSI参考模型的物理层和数据链路层。它是一种数据包交换技术,是X.25的简化版本。它省略了X.25的一些强健功能,如提供窗口技术和数据重发技术,而是依靠高层协议提供纠错功能,这是因为帧中继工作在更好的WAN设备上,这些设备较之X.25的WAN设备具有更可靠的连接服务和更高的可靠性,它严格地对应于OSI参考模型的最低二层,而X.25还提供第三层的服务,所以,帧中继比X.25具有更高的性能和更有效的传输效率。帧中继广域网的设备分为数据终端设备(DTE)和数据电路终端设备(DCE),Cisco路由器作为 DTE 设备。

帧中继技术提供面向连接的数据链路层的通信,在每对设备之间都存在一条定义好的通信链路,且该链路有一个链路识别码。这种服务通过帧中继虚电路实现,每个帧中继虚电路都以数据链路识别码(DLCI)标识自己。DLCI的值一般由帧中继服务提供商指定。帧中继即支持PVC也支持SVC。

帧中继本地管理接口(LMI)是对基本的帧中继标准的扩展。它是路由器和帧中继交换机之间信令标准,提供帧中继管理机制。它提供了许多管理复杂互联网络的特性,其中包括全局寻址、虚电路状态消息和多目发送等功能。

2. 有关命令:
端口设置
任务　命令
设置 Frame Relay 封装　encapsulation frame-relay[ietf] 1
设置 Frame Relay LMI 类型　frame-relay lmi-type {ansi | cisco | q933a}2
设置子接口　interface interface-type
interface-number.subinterface-number [multipoint|point-to-point]
映射协议地址与 DLCI　frame-relay map protocol protocol-address dlci
[broadcast]3
设置 FR DLCI 编号　frame-relay interface-dlci dlci [broadcast]
注：1.若使 Cisco 路由器与其它厂家路由设备相连，则使用 Internet 工程任务组（IETF）规定的帧中继封装格式。
2.从 Cisco IOS 版本 11.2 开始，软件支持本地管理接口（LMI）“自动感觉”，“自动感觉”使接口能确定交换机支持的 LMI 类型，用户可以不明确配置 LMI 接口类型。
3.broadcast 选项允许在帧中继网络上传输路由广播信息。
4. ISDN 访问首都在线 263 网实例:
本地局部网地址为 10.0.0.0/24,属于保留地址，通过 NAT 地址翻译功能，局域网用户可以通过 ISDN 上 263 网访问 Internet。263 的 ISDN 电话号码为 2633，用户为 263，口令为 263，所涉及的命令如下表：
任务　命令
指定接口通过 PPP/IPCP 地址协商获得 IP 地址　ip address negotiated
指定内部和外部端口　ip nat {inside | outside}
使用 ppp/pap 作认证　ppp authentication pap callin
指定接口属于拨号组 1　dialer-group 1
定义拨号组 1 允许所有 IP 协议　dialer-list 1 protocol ip permit
设定拨号，号码为 2633　dialer string 2633
设定登录 263 的用户名和口令　ppp pap sent-username 263 password 263
设定默认路由　ip route 0.0.0.0 0.0.0.0 bri 0
设定符合访问列表 2 的所有源地址被翻译为 bri 0 所拥有的地址　ip nat inside source list 2 interface bri 0 overload
设定访问列表 2，允许所有协议　access-list 2 permit any
具体配置如下：

```
hostname Cisco2503
!
isdn switch-type basic-net3
!
ip subnet-zero
no ip domain-lookup
ip routing
!
interface Ethernet 0
ip address 10.0.0.1 255.255.255.0
ip nat inside
```

```
no shutdown
!
interface Serial 0
shutdown
no des cription
no ip address
!
interface Serial 1
shutdown
no des cription
no ip address
!
interface bri 0
ip address negotiated
ip nat outside
encapsulation ppp
ppp authentication pap callin
ppp multilink
dialer-group 1
dialer hold-queue 10
dialer string 2633
dialer idle-timeout 120
ppp pap sent-username 263 password 263
no cdp enable
no ip split-horizon
no shutdown
!
ip classless
!
! Static Routes
!
ip route 0.0.0.0 0.0.0.0 bri 0
!
! Access Control List 2
!
access-list 2 permit any
!
dialer-list 1 protocol ip permit
!
! Dynamic NAT
!
ip nat inside source list 2 interface bri 0 overload
snmp-server community public ro
!
```

```
line console 0
exec-timeout 0 0
!
line vty 0 4
!
end
```

五. Cisco765M 通过 ISDN 拨号上 263

由于 Cisco765 的设置命令与我们常用的 Cisco 路由器的命令不同，所以以下列举了通过 Cisco765 上 263 访问 Internet 的具体命令行设置步骤。

```
>set system c765
c765> set multidestination on
c765> set switch net3
c765> set ppp multilink on
c765> cd lan
c765AN> set ip routing on
c765AN> set ip address 10.0.0.1
c765AN> set ip netmask 255.0.0.0
c765:LAN> set briding off
c765:LAN>cd
c765> set user remotenet
New user remotenet being created
c765:remotenet> set ip routing on
c765:remotenet> set bridging off
c765:remotenet> set ip framing none
c765:remotenet> set ppp clientname 263
c765:remotenet> set ppp password client
Enter new Password: 263
Re-Type new Password: 263
c765:remotenet> set ppp authentication out none
c765:remotenet> set ip address 0.0.0.0
c765:remotenet> set ip netmask 0.0.0.0
c765:remotenet> set ppp address negotiation local on
c765:remotenet> set ip pat on
c765:remotenet> set ip route destination 0.0.0.0/0 gateway 0.0.0.0
c765:remotenet> set number 2633
c765:remotenet> set active
```

命令描述如下：

任务　命令

设置路由器系统名称　set system c765

允许路由器呼叫多个目的地　set multidestination on

设置 ISDN 交换机类型为 NET3　set switch net3

允许点到点间多条通道连接实现负载均衡　set ppp multilink on

关掉桥接 set briding off
建立用户预制文件用于设置拨号连接参数- 可以设置多个用户预制文件用于相同的物理端口对应于不同的连接。 set user remotenet
使用 PPP/IPCP set ip framing none
设置上网用户帐号 set ppp clientname 263
设置上网口令 set ppp password client Enter new Password: 263 Re-Type new Password: 263
不用 PPP/CHAP 或 PAP 做认证 set ppp authentication out none
允许地址磋商 set ppp address negotiation local on
设置地址翻译 set ip pat on
设置默认路由 set ip route destination 0.0.0.0/0 gateway 0.0.0.0
设置 ISP 的电话号码 set number 2633
激活用户预制文件 set active

六、PSTN

电话网络(PSTN)是目前普及程度最高、成本最低的公用通讯网络，它在网络互连中也有广泛的应用。电话网络的应用一般可分为两种类型，一种是同等级别机构之间以按需拨号(DDR)的方式实现互连，一种是 ISP 为拨号上网为用户提供的远程访问服务的功能。
1. 远程访问
1.1.Access Server 基本设置：
选用 Cisco2511 作为访问服务器,采用 IP 地址池动态分配地址.远程工作站使用 WIN95 拨号网络实现连接。
全局设置：
任务 命令
设置用户名和密码 username username password password
设置用户的 IP 地址池 ip local pool {default | pool-name low-ip-address [high-ip-address]}
指定地址池的工作方式 ip address-pool [dhcp-proxy-client | local]
基本接口设置命令：
任务 命令
设置封装形式为 PPP encapsulation ppp
启动异步口的路由功能 async default routing
设置异步口的 PPP 工作方式 async mode {dedicated | interactive}
设置用户的 IP 地址 peer default ip address {ip-address | dhcp | pool [pool-name]}
设置 IP 地址与 Ethernet0 相同 ip unnumbered ethernet0
line 拨号线设置：
任务 命令
设置 modem 的工作方式 modem {inout|dialin}
自动配置 modem 类型 modem autoconfig discovery
设置拨号线的通讯速率 speed speed

设置通讯线路的流控方式 flowcontrol {none | software [lock] [in | out] | hardware [in | out]}
连通后自动执行命令 autocommand command
访问服务器设置如下：

```
Router:
hostname Router
enable secret 5 $1$EFqU$tYLJLrynNUKzE4bx6fmH//
!
interface Ethernet0
ip address 10.111.4.20 255.255.255.0
!
interface Async1
ip unnumbered Ethernet0
encapsulation ppp
keepalive 10
async mode interactive
peer default ip address pool Cisco2511-Group-142
!
ip local pool Cisco2511-Group-142 10.111.4.21 10.111.4.36
!
line con 0
exec-timeout 0 0
password cisco
!
line 1 16
modem InOut
modem autoconfigure discovery
flowcontrol hardware
!
line aux 0
transport input all
line vty 0 4
password cisco
!
end
```

相关调试命令：

```
show interface
show line
```

1.2. Access Server 通过 Tacacs 服务器实现安全认证：
使用一台 WINDOWS NT 服务器作为 Tacacs 服务器，地址为 10.111.4.2,运行 Cisco2511 随机带的 Easy ACS 1.0 软件实现用户认证功能.
相关设置：
任务 命令
激活 AAA 访问控制 aaa new-model

用户登录时默认起用 Tacacs+做 AAA 认证 aaa authentication login default tacacs+
列表名为 no_tacacs 使用 ENABLE 口令做认证 aaa authentication login no_tacacs enable
在运行 PPP 的串行线上采用 Tacacs+做认证 aaa authentication ppp default tacacs+
由 TACACS+服务器授权运行 EXEC aaa authorization exec tacacs+
由 TACACS+服务器授权与网络相关的服务请求。 aaa authorization network tacacs+
为 EXEC 会话运行记帐.进程开始和结束时发通告给 TACACS+服务器。 aaa accounting exec start-stop tacacs+
为与网络相关的服务需求运行记帐包括 SLIP,PPP,PPP NCPs,ARAP 等.在进程开始和结束时发通告给 TACACS+服务器。 aaa accounting network start-stop tacacs+
指定 Tacacs 服务器地址 tacacs-server host 10.111.4.2
在 Tacacs+服务器和访问服务器设定共享的关键字，访问服务器和 Tacacs+服务器使用这个关键字去加密口令和响应信息。这里使用 tac 作为关键字。 tacacs-server key tac
访问服务器设置如下：

```
hostname router
!
aaa new-model
aaa authentication login default tacacs+
aaa authentication login no_tacacs enable
aaa authentication ppp default tacacs+
aaa authorization exec tacacs+
aaa authorization network tacacs+
aaa accounting exec start-stop tacacs+
aaa accounting network start-stop tacacs+
enable secret 5 $1$kN4g$CvS4d2.rJzWntCnn/OhvE0
!
interface Ethernet0
ip address 10.111.4.20 255.255.255.0
!
interface Serial0
no ip address
shutdown
interface Serial1
no ip address
shutdown
!
interface Group-Async1
ip unnumbered Ethernet0
encapsulation ppp
```

```
async mode interactive
peer default ip address pool Cisco2511-Group-142
no cdp enable
group-range 1 16
!
ip local pool Cisco2511-Group-142 10.111.4.21 10.111.4.36
tacacs-server host 10.111.4.2
tacacs-server key tac
!
line con 0
exec-timeout 0 0
password cisco
login authentication no_tacacs
line 1 16
login authentication tacacs
modem InOut
modem autoconfigure type usr_courier
autocommand ppp
transport input all
stopbits 1
rxspeed 115200
txspeed 115200
flowcontrol hardware
line aux 0
transport input all
line vty 0 4
password cisco
!
end
```

2. DDR（dial-on-demand routing）实例

此例通过 Cisco 2500 系列路由器的 aux 端口实现异步拨号 DDR 连接。Router1 拨号连接到 Router2。其中采用 PPP/CHAP 做安全认证，在 Router1 中应建立一个用户，以对端路由器主机名作为用户名，即用户名应为 Router2。同时在 Router2 中应建立一个用户，以对端路由器主机名作为用户名，即用户名应为 Router1。所建的这两用户的 password 必须相同。

相关命令如下：

任务　命令

设置路由器与 modem 的接口指令　chat-s cript s cript-name EXPECT SEND EXPECT SEND (etc.)

设置端口在挂断前的等待时间　dialer idle-timeout seconds

设置协议地址与电话号码的映射　dialer map protocol next-hop-address [name hostname] [broadcast] [modem-s cript modem-regexp] [system-s cript system-regexp] [dial-string]

设置电话号码　dialer string dial-string

指定在特定线路下路由器默认 使用的chat-s cript s cript {dialer|reset} s cript-name

Router1:

```
hostname Router1
!
enable secret 5 $1$QKI7$wXjpFqC74vDAyKBUMallw/
!
username Router2 password cisco
chat-s cript cisco-default "" "AT" TIMEOUT 30 OK "ATDT \T" TIMEOUT 30 CONNECT \c
!
interface Ethernet0
ip address 10.0.0.1 255.255.255.0
!
interface Async1
ip address 192.200.10.1 255.255.255.0
encapsulation ppp
async default routing
async mode dedicated
dialer in-band
dialer idle-timeout 60
dialer map ip 192.200.10.2 name Router2 modem-s cript cisco-default 573
dialer-group 1
ppp authentication chap
!
ip route 10.0.1.0 255.255.255.0 192.200.10.2
dialer-list 1 protocol ip permit
!
line con 0
line aux 0
modem InOut
modem autoconfigure discovery
flowcontrol hardware
```

Router2:

```
hostname Router2
!
enable secret 5 $1$F6EV$5U8puzNt2/o9g.t56PXHo.
!
username Router1 password cisco
!
interface Ethernet0
ip address 10.0.1.1 255.255.255.0
!
interface Async1
```

```
ip address 192.200.10.2 255.255.255.0
encapsulation ppp
async default routing
async mode dedicated
dialer in-band
dialer idle-timeout 60
dialer map ip 192.200.10.1 name Router1
dialer-group 1
ppp authentication chap
!
ip route 10.0.0.0 255.255.255.0 192.200.10.1
dialer-list 1 protocol ip permit
!
line con 0
line aux 0
modem InOut
modem autoconfigure discovery
flowcontrol hardware
!
```

相关调试命令：

```
debug dialer
debug ppp authentication
debug ppp error
debug ppp negotiation
debug ppp packet
show dialer
```

3. 异步拨号备份 DDN 专线：

此例主连接采用 DDN 专线，备份线路为电话拨号。当 DDN 专线连接正常时，主端口 S0 状态为 up，line protocol 亦为 up,则备份线路状态为 standby，line protocol 为 down,此时所有通信均通过主接口进行。当主接口连接发生故障时，端口状态为 down，则激活备份接口，完成数据通信。此方法不适合为 X.25 做备份。因为，配置封装为 X.25 的接口只要和 X.25 交换机之间的连接正常其接口及 line protocol 的状态亦为 up,它并不考虑其它地方需与之通信的路由器的状态如何，所以若本地路由器状态正常，而对方路由器连接即使发生故障，本地也不会激活备份线路。例 4 将会描述如何为 X.25 做拨号备份。

以下是相关命令：

任务　命令

指定主线路改变后，次线路状态发生改变的延迟时间　backup delay {enable-delay | never} {disable-delay | never}

指定一个接口作为备份接口　backup interface type number

```
hostname c2522rb
!
enable secret 5 $1$J5vn$ceYDe2FwPhrZi6qsIIz6g0
enable password cisco
```

```
!
username c4700 password 0 cisco
ip subnet-zero
chat-s cript cisco-default "" "AT" TIMEOUT 30 OK "ATDT \T" TIMEOUT 30
CONNECT \c
chat-s cript reset atz
!
interface Ethernet0
ip address 16.122.51.254 255.255.255.0
no ip mroute-cache
!
interface Serial0
backup delay 10 10
backup interface Serial2
ip address 16.250.123.18 255.255.255.252
no ip mroute-cache
no fair-queue
!
interface Serial1
no ip address
no ip mroute-cache
shutdown
!
interface Serial2
physical-layer async
ip address 16.249.123.18 255.255.255.252
encapsulation ppp
async mode dedicated
dialer in-band
dialer idle-timeout 60
dialer map ip 16.249.123.17 name c4700 6825179
dialer-group 1
ppp authentication chap
!
interface Serial3
no ip address
shutdown
no cdp enable
!
interface Serial4
no ip address
shutdown
no cdp enable
!
```

```
interface Serial5
no ip address
no ip mroute-cache
shutdown
!
interface Serial6
no ip address
no ip mroute-cache
shutdown
!
interface Serial7
no ip address
no ip mroute-cache
shutdown
!
interface Serial8
no ip address
no ip mroute-cache
shutdown
!
interface Serial9
no ip address
no ip mroute-cache
shutdown
!
interface BRI0
no ip address
no ip mroute-cache
shutdown
!
router eigrp 200
network 16.0.0.0
!
ip classless
!
dialer-list 1 protocol ip permit
!
line con 0
line 2
s cript dialer cisco-default
s cript reset reset
modem InOut
modem autoconfigure discovery
rxspeed 38400
```

```
txspeed 38400
flowcontrol hardware
line aux 0
line vty 0 4
password cisco
login
!
end
c2522rb#
```

4. 异步拨号备份 X.25:

设置X.25的拨号备份,首先X.25连接的端口必须运行动态路由协议,异步拨号口必须使用静态路由.本例选择EIGRP作为路由选择协议,将静态路由的 Metric 的值设置为200,由于EIGRP的默认Metric为90,所以当同时有两条路径通往同一网段时,其中Metric值小的路径生效,而当 X.25连接出现问题时,路由器无法通过路由协议学习到路由表，则此时静态路由生效，访问通过拨号端口实现。当X.25连接恢复正常时，路由器又可以学习到路由表，则由于 Metric 值的不同，静态路由自动被动态路由所代替，这样就实现了备份的功能。

路由器Router1配置如下:

```
hostname router1
!
enable secret 5 $1$UTvD$99YiY2XsRMxHudcYeHn.Y.
enable password cisco
!
username router2 password cisco
ip subnet-zero
chat-s cript cisco-default "" "AT" TIMEOUT 30 OK "ATDT \T" TIMEOUT 30
CONNECT \c
chat-s cript reset atz
interface Ethernet0
ip address 202.96.38.100 255.255.255.0
!
interface Serial0
ip address 202.96.0.1 255.255.255.0
encapsulation x25
x25 address 10112227
x25 htc 16
x25 map ip 202.96.0.2 10112225 broadcast
!
interface Serial1
no ip address
shutdown
!
!
interface Async 1
```

```
ip address 202.96.1.1 255.255.255.252
encapsulation ppp
dialer in-band
dialer idle-timeout 60
dialer map ip 202.96.1.2 name router2 modem-s cript cisco-default 2113470
dialer-group 1
ppp authentication chap
!
router eigrp 200
redistribute connected
network 202.96.0.0
!
ip route 202.96.37.0 255.255.255.0 202.96.1.2 200
dialer-list 1 protocol ip permit
line con 0
line aux 0
s cript dialer cisco-default
s cript reset reset
modem InOut
modem autoconfigure discovery
transport input all
rxspeed 38400
txspeed 38400
flowcontrol hardware
line vty 0 4
password cisco
login
!
end
```

路由器 Router2 配置如下:

```
hostname router2
!
enable secret 5 $1$T4IU$2cIqak8f/E4Ug6dLT0k.J0
enable password cisco
!
username router1 password cisco
ip subnet-zero
chat-s cript cisco-default "" "AT" TIMEOUT 30 OK "ATDT \T" TIMEOUT 30
CONNECT \c
chat-s cript reset atz
!
interface Ethernet0
ip address 202.96.37.100 255.255.255.0
!
```

```
interface Serial0
ip address 202.96.0.2 255.255.255.0
no ip mroute-cache
encapsulation x25
x25 address 10112225
x25 htc 16
x25 map ip 202.96.0.1 10112227 broadcast
!
interface Serial1
no ip address
shutdown
!
interface Async1
ip address 202.96.1.2 255.255.255.252
encapsulation ppp
keepalive 30
async default routing
async mode dedicated
dialer in-band
dialer idle-timeout 60
dialer wait-for-carrier-time 120
dialer map ip 202.96.1.1 name router1 modem-s cript cisco-default 2113469
dialer-group 1
ppp authentication chap
!
router eigrp 200
redistribute static
network 202.96.0.0
!
no ip classless
ip route 202.96.38.0 255.255.255.0 202.96.1.1 200
dialer-list 1 protocol ip permit
!
line con 0
exec-timeout 0 0
line aux 0
s cript reset reset
modem InOut
modem autoconfigure discovery
transport input all
rxspeed 38400
txspeed 38400
flowcontrol hardware
line vty 0 4
```

```
password cisco
login
!
end
```

第三章：路由协议设置

一、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
Router1:

```
router rip
version 2
network 192.200.10.0
network 192.20.10.0
!
```

相关调试命令：

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

二、IGRP 协议
IGRP (Interior Gateway Routing Protocol)是一种动态距离向量路由协议，它由 Cisco 公司八十年代中期设计。使用组合用户配置尺度，包括延迟、带宽、可靠性和负载。
缺省情况下，IGRP 每 90 秒发送一次路由更新广播，在 3 个更新周期内(即 270 秒)，没有从路由中的第一个路由器接收到更新，则宣布路由不可访问。在 7 个更新周期即 630 秒后，Cisco IOS 软件从路由表中清除路由。

1. 有关命令
任务　命令
指定使用 RIP 协议　router igrp autonomous-system1
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
Router1:
router igrp 200
network 192.200.10.0
network 192.20.10.0

三、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 是链路状态路有协议，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-id1
指定与该路由器相连的网络　network address wildcard-mask area area-id2
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. 基本配置举例:
Router1:
interface ethernet 0
ip address 192.1.0.129 255.255.255.192
!
interface serial 0
ip address 192.200.10.5 255.255.255.252
!
router ospf 100

```
network 192.200.10.4 0.0.0.3 area 0
network 192.1.0.128 0.0.0.63 area 1
!
Router2:
interface ethernet 0
ip address 192.1.0.65 255.255.255.192
!
interface serial 0
ip address 192.200.10.6 255.255.255.252
!
router ospf 200
network 192.200.10.4 0.0.0.3 area 0
network 192.1.0.64 0.0.0.63 area 2
!
Router3:
interface ethernet 0
ip address 192.1.0.130 255.255.255.192
!
router ospf 300
network 192.1.0.128 0.0.0.63 area 1
!
Router4:
interface ethernet 0
ip address 192.1.0.66 255.255.255.192
!
router ospf 400
network 192.1.0.64 0.0.0.63 area 1
!
```

相关调试命令：

```
debug ip ospf events
debug ip ospf packet
show ip ospf
show ip ospf database
show ip ospf interface
show ip ospf neighbor
show ip route
```

下 OSPF 不使用区域验证。通过两种方法可启用身份验证功能，纯文本身份验证和消息摘要(md5)身份验证。纯文本身份验证传送的身份验证口令为纯文本，它会被网络探测器确定，所以不安全，不建议使用。而消息摘要(md5)身份验证在传输身份验证口令前，要对口令进行加密，所以一般建议使用此种方法进行身份验证。

使用身份验证时，区域内所有的路由器接口必须使用相同的身份验证方法。为起用身份验证，必须在路由器接口配置模式下，为区域的每个路由器接口配置口令。

任务　命令

指定身份验证 area area-id authentication [message-digest]
使用纯文本身份验证 ip ospf authentication-key password
使用消息摘要(md5)身份验证 ip ospf message-digest-key keyid md5 key
以下列举两种验证设置的示例,示例的网络分布及地址分配环境与以上基本配置举例相同，只是在 Router1 和 Router2 的区域 0 上使用了身份验证的功能。:
例 1.使用纯文本身份验证
Router1:
interface ethernet 0
ip address 192.1.0.129 255.255.255.192
!
interface serial 0
ip address 192.200.10.5 255.255.255.252
ip ospf authentication-key cisco
!
router ospf 100
network 192.200.10.4 0.0.0.3 area 0
network 192.1.0.128 0.0.0.63 area 1
area 0 authentication
!
Router2:
interface ethernet 0
ip address 192.1.0.65 255.255.255.192
!
interface serial 0
ip address 192.200.10.6 255.255.255.252
ip ospf authentication-key cisco
!
router ospf 200
network 192.200.10.4 0.0.0.3 area 0
network 192.1.0.64 0.0.0.63 area 2
area 0 authentication
!
例 2.消息摘要(md5)身份验证:
Router1:
interface ethernet 0
ip address 192.1.0.129 255.255.255.192
!
interface serial 0
ip address 192.200.10.5 255.255.255.252
ip ospf message-digest-key 1 md5 cisco
!
router ospf 100
network 192.200.10.4 0.0.0.3 area 0
network 192.1.0.128 0.0.0.63 area 1

```
area 0 authentication message-digest
!
Router2:
interface ethernet 0
ip address 192.1.0.65 255.255.255.192
!
interface serial 0
ip address 192.200.10.6 255.255.255.252
ip ospf message-digest-key 1 md5 cisco
!
router ospf 200
network 192.200.10.4 0.0.0.3 area 0
network 192.1.0.64 0.0.0.63 area 2
area 0 authentication message-digest
!
```

相关调试命令：

```
debug ip ospf adj
debug ip ospf events
```

四、重新分配路由

在实际工作中，我们会遇到使用多个 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成功的路由再分配。

以下列举了 OSPF 与 RIP 之间重新分配路由的设置范例：

Router1 的 Serial 0 端口和 Router2 的 Serial 0 端口运行 OSPF，在 Router1 的 Ethernet 0 端口运行 RIP 2，Router3 运行 RIP2，Router2 有指向 Router4 的 192.168.2.0/24 网的静态路由，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。

范例所涉及的命令

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:
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
```

```
network 192.200.10.4 0.0.0.3 area 0
!
router rip
version 2
redistribute ospf 100 metric 1
network 192.168.1.0
!
Router2:
interface loopback 1
ip address 192.168.3.2 255.255.255.0
!
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:
interface ethernet 0
ip address 192.168.1.2 255.255.255.0
!
router rip
version 2
network 192.168.1.0
!
Router4:
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
!
```

五、IPX 协议设置

IPX 协议与 IP 协议是两种不同的网络层协议，它们的路由协议也不一样，IPX 的路由协议不象 IP 的路由协议那样丰富，所以设置起来比较简单。但 IPX 协议在以太网上运行时必须指定封装形式。

1. 有关命令

启动 IPX 路由 ipx routing

设置 IPX 网络及以太网封装形式 ipx network network [encapsulation encapsulation-type]1

指定路由协议，默认为 RIP ipx router {eigrp autonomous-system-number | nlsp [tag] | rip}

注：1.network 范围是 1 到 FFFFFFFD.

IPX 封装类型列表

接口类型 封装类型 IPX 帧类型

Ethernet novell-ether (默认) arpa sap snap Ethernet_802.3 Ethernet_II Ethernet_802.2 Ethernet_Snap

Token Ring sap (默认) snap Token-Ring Token-Ring_Snap

FDDI snap (默认) sap novell-fddi Fddi_Snap Fddi_802.2 Fddi_Raw

举例：

在此例中，WAN 的 IPX 网络为 3a00,Router1 所连接的局域网 IPX 网络号为 2a00,在此局域网有一台 Novell 服务器，IPX 网络号也是 2a00, 路由器接口的 IPX 网络号必须与在同一网络的 Novell 服务器上设置的 IPX 网络号相同。路由器通过监听 SAP 来建立已知的服务及自己的网络地址表，并每 60 秒发送一次自己的 SAP 表。

Router1:

```
ipx routing
interface ethernet 0
ipx network 2a00 encapsulation sap
!
interface serial 0
ipx network 3a00
!
ipx router eigrp 10
network 3a00
network 2a00
!
```

Router2:

```
ipx routing
interface ethernet 0
ipx network 2b00 encapsulation sap
!
interface serial 0
ipx network 3a00
```

```
!
ipx router eigrp 10
network 2b00
network 3a00
!
```
相关调试命令：
```
debug ipx packet
debug ipx routing
debug ipx sap
debug ipx spoof
debug ipx spx
show ipx eigrp interfaces
show ipx eigrp neighbors
show ipx eigrp topology
show ipx interface
show ipx route
show ipx servers
show ipx spx-spoof
```

第四章：服务质量及访问控制

一、协议优先级设置

1. 有关命令

任务　命令

设置优先级表项目　priority-list list-number protocol protocol {high | medium | normal | low} queue-keyword keyword-value

使用指定的优先级表　priority-group list-number

2. 举例

Router1:

```
priority-list 1 protocol ip high tcp telnet
priority-list 1 protocol ip low tcp ftp
priority-list 1 default normal
interface serial 0
priority-group 1
```

二、队列定制

1. 有关命令
任务　命令
设置队列表中包含协议　queue-list list-number protocol protocol-name queue-number queue-keyword keyword-value
设置队列表中队列的大小　queue-list list-number queue queue-number byte-count byte-count-number
使用指定的队列表　custom-queue-list list
2. 举例
Router1:
```
queue-list 1 protocol ip 0 tcp telnet
queue-list 1 protocol ip 1 tcp www
queue-list 1 protocol ip 2 tcp ftp
queue-list 1 queue 0 byte-count 300
queue-list 1 queue 1 byte-count 200
queue-list 1 queue 2 byte-count 100
interface serial 0
custom-queue-list 1
```

三、访问控制

1. 有关命令
任务　命令
设置访问表项目　access-list list {permit | deny} address mask
设置队列表中队列的大小　queue-list list-number queue queue-number byte-count byte-count-number
使用指定的访问表　ip access-group list {in | out}
2. 举例
Router1:
```
access-list 1 deny 192.1.3.0 0.0.0.255
access-list 1 permit any
interface serial 0
ip access-group 1 in
```

第五章：虚拟局域网（VLAN）路由

一、虚拟局域网(VLAN)

当前在我们构造企业网络时所采用的主干网络技术一般都是基于交换和虚拟网络的。交换技术将共享介质改为独占介质,大大提高网络速度。虚拟网络技术打破了地理环境的制约,在不改动网络物理连接的情况下可以任意将工作站在工作组或子网之间移动,工作站组成逻辑工作组或虚拟子网,提高信息系统的运作性能,均衡网络数据流量,合理利用硬件及信息资源。同时,利用虚拟网络技术,大大减轻了网络管理和维护工作的负担,降低网络维护费用。随着虚拟网络技术的应用，随之必然产生了在虚拟网间如何通讯的问题。

二、交换机间链路（ISL）协议

ISL(Interior Switching Link)协议用于实现交换机间的 VLAN 中继。它是一个信息包标记协议，在支持 ISL 接口上发送的帧由一个标准以太网帧及相关的 VLAN 信息组成。如下图所示，在支持 ISL 的接口上可以传送来自不同 VLAN 的数据。

三、虚拟局域网（VLAN）路由实例

3.1. 例一：

设备选用Catalyst5500交换机1台,安装WS-X5530-E3管理引擎,多块WS-X5225R及WS-X5302路由交换模块,WS- X5302被直接插入交换机，通过二个通道与系统背板上的VLAN 相连,从用户角度看认为它是1个1接口的模块,此接口支持ISL。在交换机内划有3个虚拟网，分别名为default、qbw、rgw，通过WS- X5302实现虚拟网间路由。
以下加重下横线部分，如set system name 5500C为需设置的命令。
设置如下：
Catalyst 5500配置：

```
begin
set password $1$FMFQ$HfZR5DUszVHIRhrz4h6V70
set enablepass $1$FMFQ$HfZR5DUszVHIRhrz4h6V70
set prompt Console>
set length 24 default
set logout 20
set banner motd ^C^C
!
#system
```

```
set system baud 9600
set system modem disable
set system name 5500C
set system location
set system contact
!
#ip
set interface sc0 1 10.230.4.240 255.255.255.0 10.230.4.255
set interface sc0 up
set interface sl0 0.0.0.0 0.0.0.0
set interface sl0 up
set arp agingtime 1200
set ip redirect enable
set ip unreachable enable
set ip fragmentation enable
set ip route 0.0.0.0 10.230.4.15 1
set ip alias default 0.0.0.0
!
#Command alias
!
#vtp
set vtp domain hne
set vtp mode server
set vtp v2 disable
set vtp pruning disable
set vtp pruneeligible 2-1000
clear vtp pruneeligible 1001-1005
set vlan 1 name default type ethernet mtu 1500 said 100001 state active
set vlan 777 name rgw type ethernet mtu 1500 said 100777 state active
set vlan 888 name qbw type ethernet mtu 1500 said 100888 state active
set vlan 1002 name fddi-default type fddi mtu 1500 said 101002 state active
set vlan 1004 name fddinet-default type fddinet mtu 1500 said 101004 state
active bridge 0x0 stp ieee
set vlan 1005 name trnet-default type trbrf mtu 1500 said 101005 state
active bridge 0x0 stp ibm
set vlan 1003 name token-ring-default type trcrf mtu 1500 said 101003
state active parent 0 ring 0x0 mode srb aremaxhop 7 stemaxhop 7
!
#set boot command
set boot config-register 0x102
set boot system flash bootflash:cat5000-sup3.4-3-1a.bin
!
#module 1 : 2-port 1000BaseLX Supervisor
set module name 1
```

```
set vlan 1 1/1-2
set port enable 1/1-2
!
#module 2 : empty
!
#module 3 : 24-port 10/100BaseTX Ethernet
set module name 3
set module enable 3
set vlan 1 3/1-22
set vlan 777 3/23
set vlan 888 3/24
set trunk 3/1 on isl 1-1005
#module 4 empty
!
#module 5 empty
!
#module 6 : 1-port Route Switch
set module name 6
set port level 6/1 normal
set port trap 6/1 disable
set port name 6/1
set cdp enable 6/1
set cdp interval 6/1 60
set trunk 6/1 on isl 1-1005
!
#module 7 : 24-port 10/100BaseTX Ethernet
set module name 7
set module enable 7
set vlan 1 7/1-22
set vlan 888 7/23-24
set trunk 7/1 on isl 1-1005
set trunk 7/2 on isl 1-1005
!
#module 8 empty
!
#module 9 empty
!
#module 10 : 12-port 100BaseFX MM Ethernet
set module name 10
set module enable 10
set vlan 1 10/1-12
set port channel 10/1-4 off
set port channel 10/5-8 off
set port channel 10/9-12 off
```

```
set port channel 10/1-2 on
set port channel 10/3-4 on
set port channel 10/5-6 on
set port channel 10/7-8 on
set port channel 10/9-10 on
set port channel 10/11-12 on
#module 11 empty
!
#module 12 empty
!
#module 13 empty
!
#switch port analyzer
!set span 1 1/1 both inpkts disable
set span disable
!
#cam
set cam agingtime 1-2,777,888,1003,1005 300
end
5500C> (enable)
```

WS-X5302 路由模块设置：

```
Router#wri t
Building configuration...
Current configuration:
!
version 11.2
no service password-encryption
no service udp-small-servers
no service tcp-small-servers
!
hostname Router
!
enable secret 5 $1$w1kK$AJK69fGOD7BqKhKcSNBf6.
!
ip subnet-zero
!
interface Vlan1
ip address 10.230.2.56 255.255.255.0
!
interface Vlan777
ip address 10.230.3.56 255.255.255.0
!
interface Vlan888
ip address 10.230.4.56 255.255.255.0
```

```
!
no ip classless
!
line con 0
line aux 0
line vty 0 4
password router
login
!
end
Router#
```

3.1. 例二：

交换设备仍选用 Catalyst5500 交换机 1 台，安装 WS-X5530-E3 管理引擎，多块 WS-X5225R 在交换机内划有 3 个虚拟网，分别名为 default、qbw、rgw，通过 Cisco3640 路由器实现虚拟网间路由。交换机设置与例一类似。

路由器 Cisco3640，配有一块 NM-1FE-TX 模块，此模块带有一个快速以太网接口可以支持 ISL。Cisco3640 快速以太网接口与交换机上的某一支持 ISL 的端口实现连接，如交换机第 3 槽第 1 个接口（3/1 口）。

```
Router#wri t
Building configuration...
Current configuration:
!
version 11.2
no service password-encryption
no service udp-small-servers
no service tcp-small-servers
!
hostname Router
!
enable secret 5 $1$w1kK$AJK69fGOD7BqKhKcSNBf6.
!
ip subnet-zero
!
interface FastEthernet1/0
!
interface FastEthernet1/0.1
encapsulation isl 1
ip address 10.230.2.56 255.255.255.0
!
interface FastEthernet1/0.2
encapsulation isl 777
ip address 10.230.3.56 255.255.255.0
!
interface FastEthernet1/0.3
```

```
encapsulation isl 888
ip address 10.230.4.56 255.255.255.0
!
no ip classless
!
line con 0
line aux 0
line vty 0 4
password router
login
!
end
Router#
```

第六章：知识参考

一、路由器初始化

1、Cisco 路由器口令恢复
当 Cisco 路由器的口令被错误修改或忘记时，可以按如下步骤进行操作：
1. 开机时按<Ctrl+Break>使进入 ROM 监控状态
2. 按 o 命令读取配置寄存器的原始值
> o　　一般值为 0x2102
3. 作如下设置，使忽略 NVRAM 引导
>o/r0x**4*　　Cisco2500 系列命令
rommon 1 >confreg 0x**4*　Cisco2600、1600 系列命令
一般正常值为 0x2102
4. 重新启动路由器
>I
rommon 2 >reset
5. 在“Setup”模式，对所有问题回答 No
6. 进入特权模式
Router>enable
7. 下载 NVRAM
Router>configure memory
8. 恢复原始配置寄存器值并激活所有端口
“hostname”#configure terminal
“hostname”(config)#config-register 0x“value”
“hostname”(config)#interface xx
“hostname”(config)#no shutdown
9. 查询并记录丢失的口令
“hostname”#show configuration (show startup-config)

10. 修改口令
“hostname”#configure terminal
“hostname”(config)line console 0
“hostname”(config-line)#login
“hostname”(config-line)#password xxxxxxxxx
“hostname”(config-line)#<ctrl+z>
“hostname”(config-line)#write memory(copy running-config startup-config)

二、IP 分配

地址类 网络主机 网络地址范围 标准二进制掩码
A N.H.H.H 1-126 1111 1111 0000 0000 0000 0000 0000 0000
B N.N.H.H 128-191 1111 1111 1111 1111 0000 0000 0000 0000
C N.N.N.H 192-223 1111 1111 1111 1111 1111 1111 0000 0000
子网位个数 子网掩码 子网数 主机数
B 类地址
2 255.255.192.0 2 16382
3 255.255.224.0 6 8198
4 255.255.240.0 14 4894
5 255.255.248.0 30 2846
6 255.255.252.0 62 1822
7 255.255.254.0 126 518
8 255.255.255.0 254 254
9 255.255.255.128 518 126
10 255.255.255.192 1822 62
11 255.255.255.224 2846 30
12 255.255.255.240 4894 14
13 255.255.255.248 8198 6
14 255.255.255.252 16382 2
C 类地址
2 255.255.255.192 2 62
3 255.255.255.224 6 30
4 255.255.255.240 14 14
5 255.255.255.248 30 6
6 255.255.255.252 62 2