

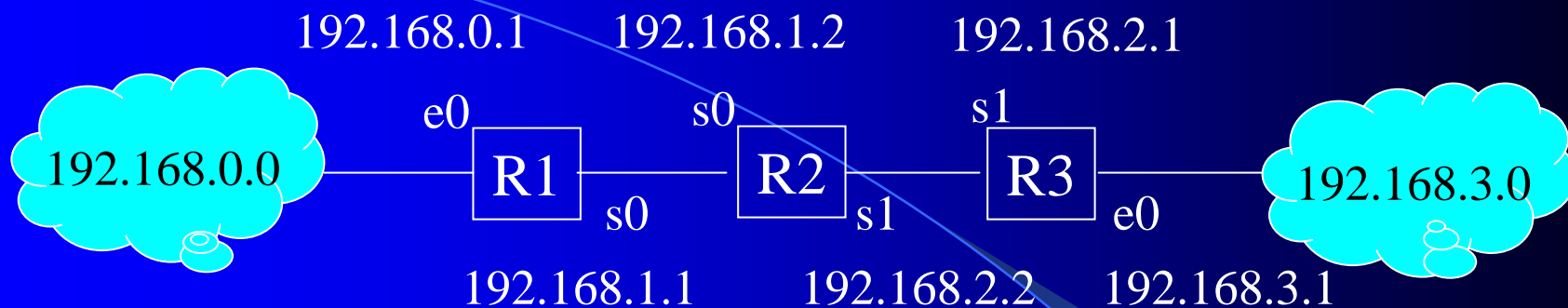
路由器的高级配置

- 主要内容

- 掌握静态路由的配置
- 掌握动态路由的配置（RIP、IGRP协议的配置）
- 掌握路由器访问控制列表的（标准与扩展访问列表）配置
- 了解路由器对X.25网络的配置
- 了解路由器对ISDN网络配置
- 了解路由器对帧中继网络的配置
- 掌握路由器CDP协议的配置
- 了解广域网协议PPP、PAP、CHAP的配置
- 了解路由器的备份与恢复(OS)
- 了解路由器灾难恢复

路由表中的路由

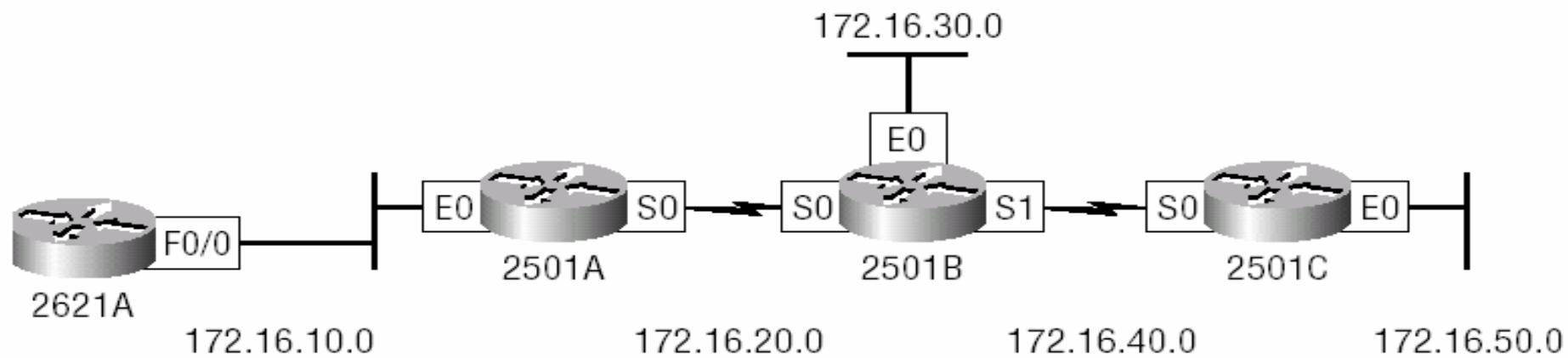
- 直连路由（connected）
 - 与路由器直接相连的网络，会自动生成直连路由。
- 静态路由（static）
 - 与路由器没有直接相连的网络，用户手工生成的路由。
- 动态路由（dynamic）
 - 与路由器没有直接相连的网络，由路由协议动态发现路由



R1的路由表：

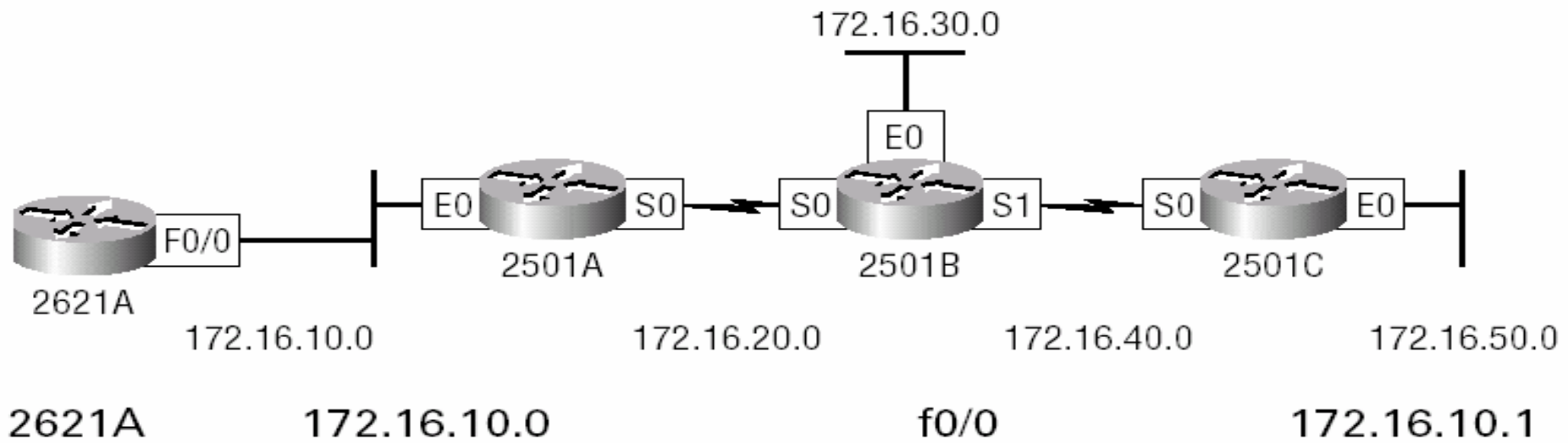
目标网络	掩码	下一跳	接口	类型
192.168.0.0	24	192.168.0.1	e0	直连路由
192.168.1.0	24	192.168.1.1	s0	直连路由
192.168.2.0	24	192.168.1.2	s0	非直连路由
192.168.3.0	24	192.168.1.2	s0	非直连路由

对于非直连路由，下一跳为相邻路由器的IP地址。



Network Addressing for the IP Network

Router	Network Address	Interface	Address
2621A	172.16.10.0	f0/0	172.16.10.1
2501A	172.16.10.0	e0	172.16.10.2
2501A	172.16.20.0	s0	172.16.20.1
2501B	172.16.20.0	s0	172.16.20.2
2501B	172.16.40.0	s1	172.16.40.1
2501B	172.16.30.0	e0	172.16.30.1
2501C	172.16.40.0	s0	172.16.40.2
2501C	172.16.50.0	e0	172.16.50.1



a. 2621A Configuration

```
Router>en
```

```
Router#config t
```

```
Router (config)#hostname 2621A
```

```
2621A(Config)#interface fa0/0
```

```
2621A(Config-if)#ip address 172.16.10.1 255.255.255.0
```

```
2621A(Config-if)#no shut
```

a.2621A Configuration

2621A# **show ip route**

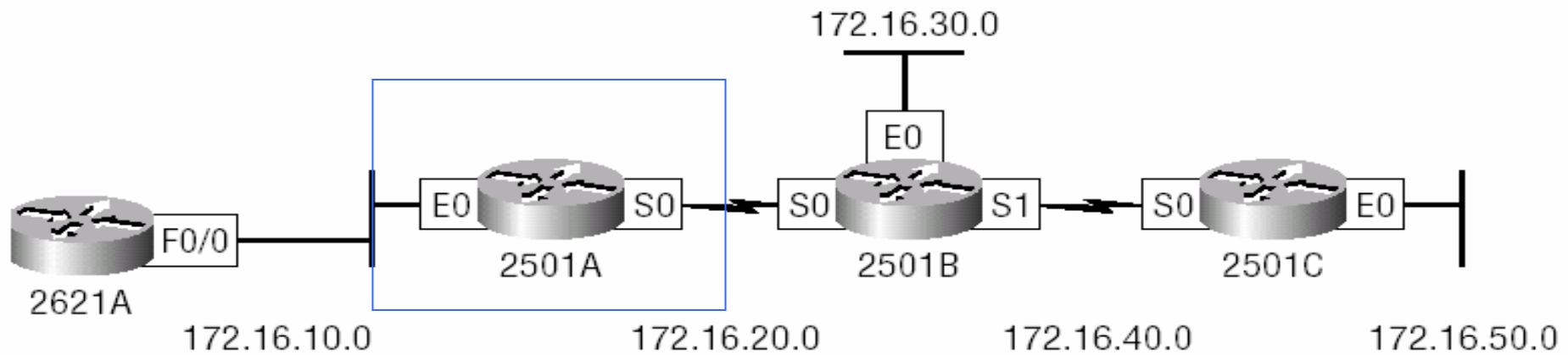
Codes: C - connected, S - static, I - IGRP, R - RIP, M -mobile,
B – BGP D - EIGRP, EX - EIGRP external, O - OSPF,
IA - OSPF inter area N1 - OSPF NSSA external type 1,
N2 - OSPF NSSA external type 2 E1 - OSPF external type 1,
E2 - OSPF external type 2, E – EGP i - IS-IS, L1 - IS-IS level-1,
L2 - IS-IS level-2, * - candidate default, U - per-user static route,
o - ODR, P - periodic downloaded static route
T - traffic engineered route

Gateway of last resort is not set

172.16.0.0/24 is subnetted, 1 subnets

C 172.16.10.0 is directly connected, FastEthernet0/0

2621A#



2501A	172.16.10.0	e0	172.16.10.2
2501A	172.16.20.0	s0	172.16.20.1

b. 2501A Configuration

```
Router>en
```

```
Router#config t
```

```
Router(config) # hostname 2501A
```

```
2501A(config)# int e0
```

```
2501A(config-if)# ip address 172.16.10.2 255.255.255.0
```

```
2501A(config-if)# no shut
```

```
2501A(config-if)# int s0
```

```
2501A(config-if)# ip address 172.16.20.1 255.255.255.0
```

```
2501A(config-if)# no shut
```

b. 2501A Configuration

```
2501A#show ip route
```

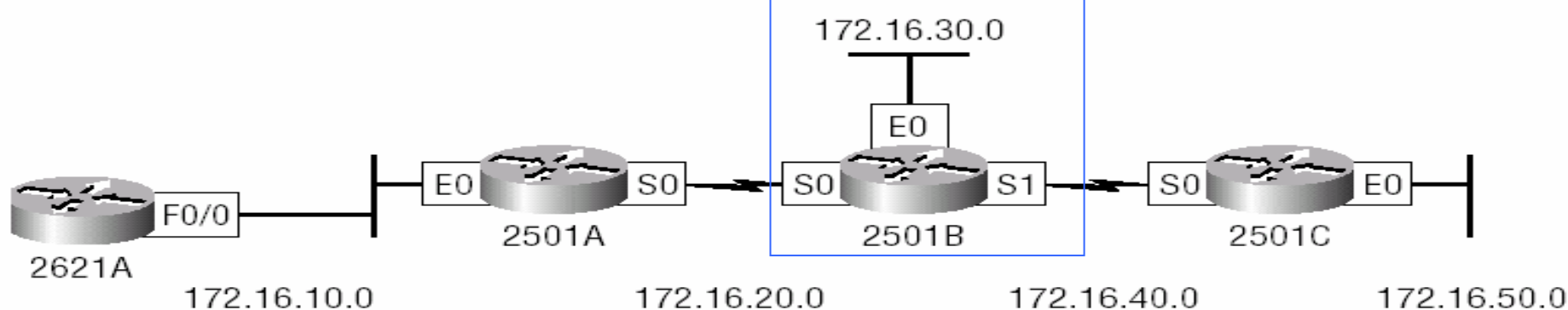
Codes: C - connected, S - static, I - IGRP, R - RIP,
Gateway of last resort is not set

172.16.0.0/24 is subnetted, 2 subnets

C 172.16.20.0 is directly connected, Serial0

C 172.16.10.0 is directly connected, Ethernet0

```
2501A#
```

c. 2501B Configuration

Router>en

Router#config t

Router(config)#hostname 2501B

2501B(config)#int e0

2501B(config-if)#ip address 172.16.30.1 255.255.255.0

2501B(config-if)#no shut

2501B(config-if)#int s0

2501B(config-if)#ip address 172.16.20.2 255.255.255.0

2501B(config-if)#clock rate 64000

2501B(config-if)#no shut

2501B(config-if)#int s1

2501B(config-if)#ip address 172.16.40.1 255.255.255.0

2501B(config-if)#clock rate 64000

2501B(config-if)#no shut

2501B	172.16.20.0	s0	172.16.20.2
2501B	172.16.40.0	s1	172.16.40.1
2501B	172.16.30.0	e0	172.16.30.1

显示串口是DCE还是DTE:

Show controller serial 0

c. 2501B Configuration

2501B#show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP,
Gateway of last resort is not set

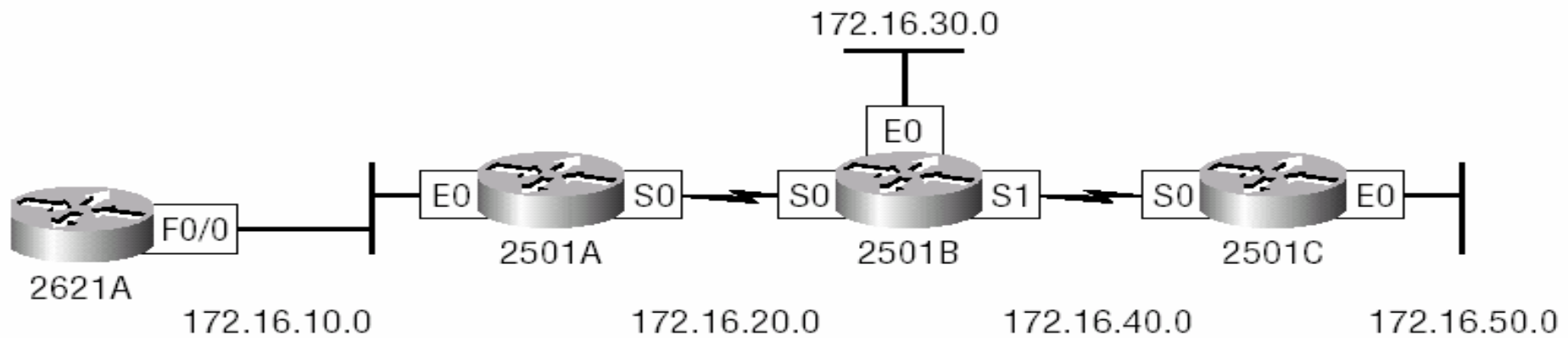
172.16.0.0/24 is subnetted, 3 subnets

C 172.16.40.0 is directly connected, Serial1

C 172.16.30.0 is directly connected, Ethernet0

C 172.16.20.0 is directly connected, Serial0

2501B#



2501C	172.16.40.0	s0	172.16.40.2
2501C	172.16.50.0	e0	172.16.50.1

d. 2501C Configuration

```
Router>en
```

```
Router#config t
```

```
Router(config)# hostname 2501C
```

```
2501C(config)# int e0
```

```
2501C(config-if)# ip address 172.16.50.1 255.255.255.0
```

```
2501C(config-if)# no shut
```

```
2501C(config-if)# int s0
```

```
2501C(config-if)# ip address 172.16.40.2 255.255.255.0
```

```
2501C(config-if)# no shut
```

d. 2501C Configuration

2501C#**show ip route**

Codes: C - connected, S - static, I - IGRP, R - RIP,
Gateway of last resort is not set

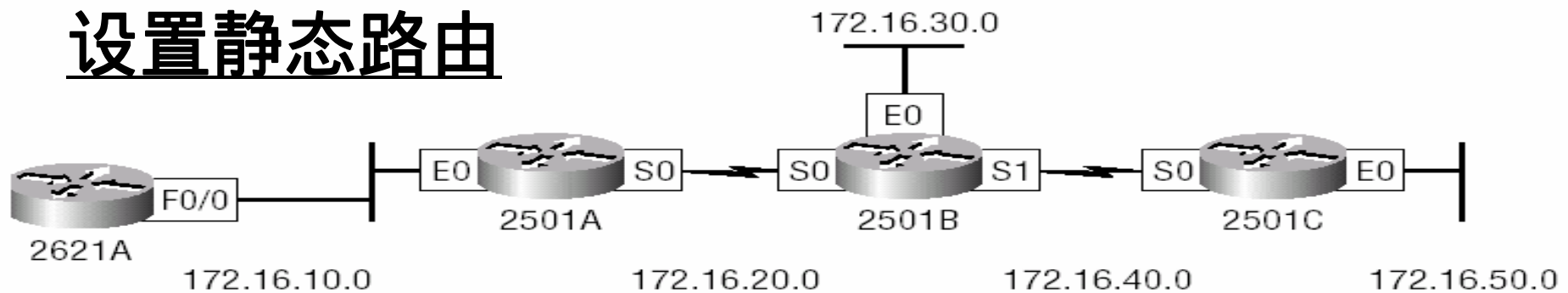
172.16.0.0/24 is subnetted, 2 subnets

C 172.16.50.0 is directly connected, Ethernet0

C 172.16.40.0 is directly connected, Serial0

2501C#

设置静态路由



a. 2621A

The following networks must be configured in the routing table:

- 172.16.20.0
- 172.16.30.0
- 172.16.40.0
- 172.16.50.0

```
2621A(Config)# ip route 172.16.20.0 255.255.255.0 172.16.10.2  
2621A(Config)# ip route 172.16.30.0 255.255.255.0 172.16.10.2  
2621A(Config)# ip route 172.16.40.0 255.255.255.0 172.16.10.2  
2621A(Config)# ip route 172.16.50.0 255.255.255.0 172.16.10.2
```

a. 2621A

2621A#show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP,
Gateway of last resort is not set

172.16.0.0/24 is subnetted, 5 subnets

S 172.16.50.0 [1/0] via 172.16.10.2

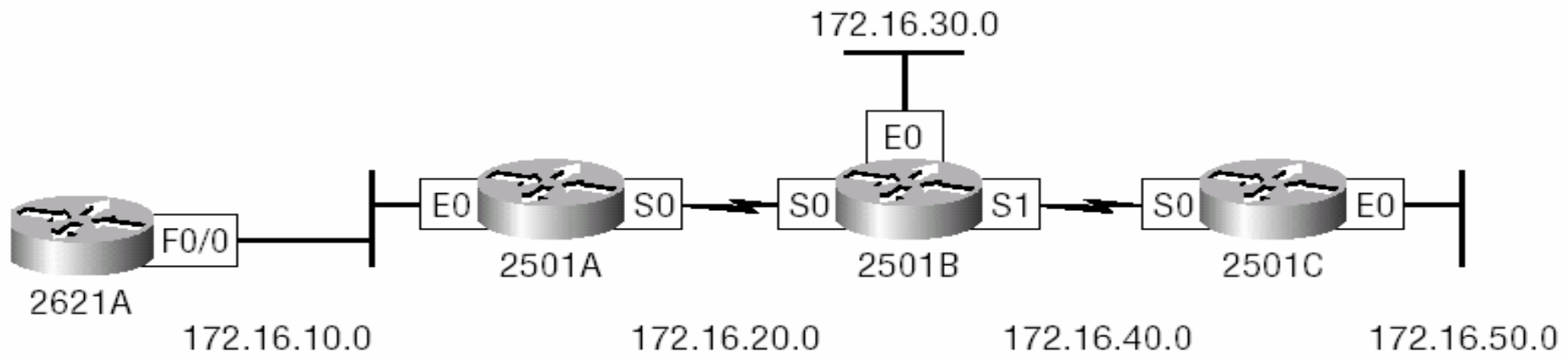
S 172.16.40.0 [1/0] via 172.16.10.2

S 172.16.30.0 [1/0] via 172.16.10.2

S 172.16.20.0 [1/0] via 172.16.10.2

C 172.16.10.0 is directly connected, FastEthernet0/0

2621A#



b. 2501A

The following static routes must be configured on the 2501A router:

- 172.16.30.0
- 172.16.40.0
- 172.16.50.0

```
2501A(Config)# ip route 172.16.30.0 255.255.255.0 172.16.20.2
```

```
2501A(Config)# ip route 172.16.40.0 255.255.255.0 172.16.20.2
```

```
2501A(Config)# ip route 172.16.50.0 255.255.255.0 172.16.20.2
```

b. 2501A

2501A#**show ip route**

Codes: C - connected, S - static, I - IGRP, R - RIP,
Gateway of last resort is not set

172.16.0.0/24 is subnetted, 5 subnets

S 172.16.50.0 [1/0] via 172.16.20.2

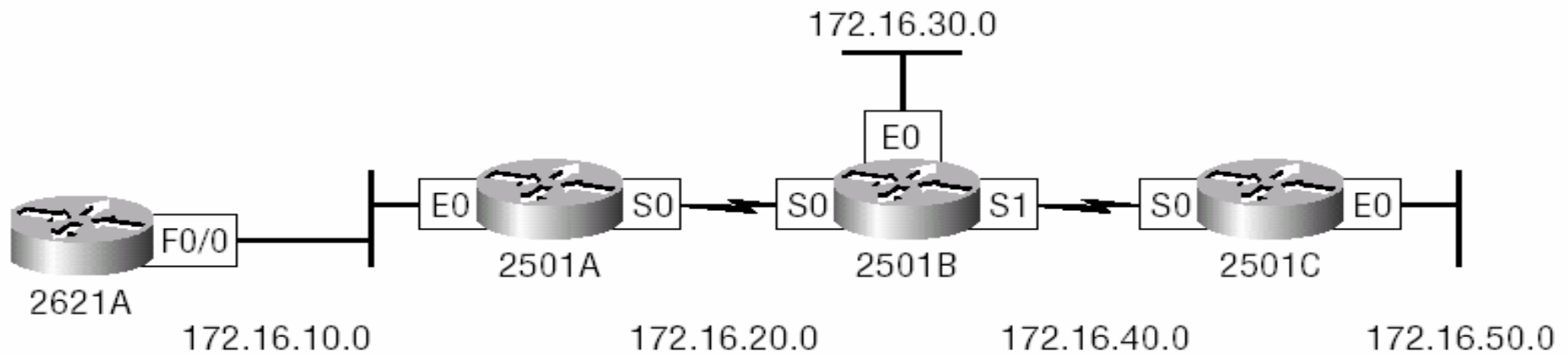
S 172.16.40.0 [1/0] via 172.16.20.2

S 172.16.30.0 [1/0] via 172.16.20.2

C 172.16.20.0 is directly connected, Serial0

C 172.16.10.0 is directly connected, Ethernet0

2501A#



c. 2501B

Only two routers need to be added:

- 172.16.10.0
- 172.16.50.0.

```
2501B(Config)#ip route 172.16.10.0 255.255.255.0 172.16.20.1
```

```
2501B(Config)#ip route 172.16.50.0 255.255.255.0 172.16.40.2
```

c. 2501B

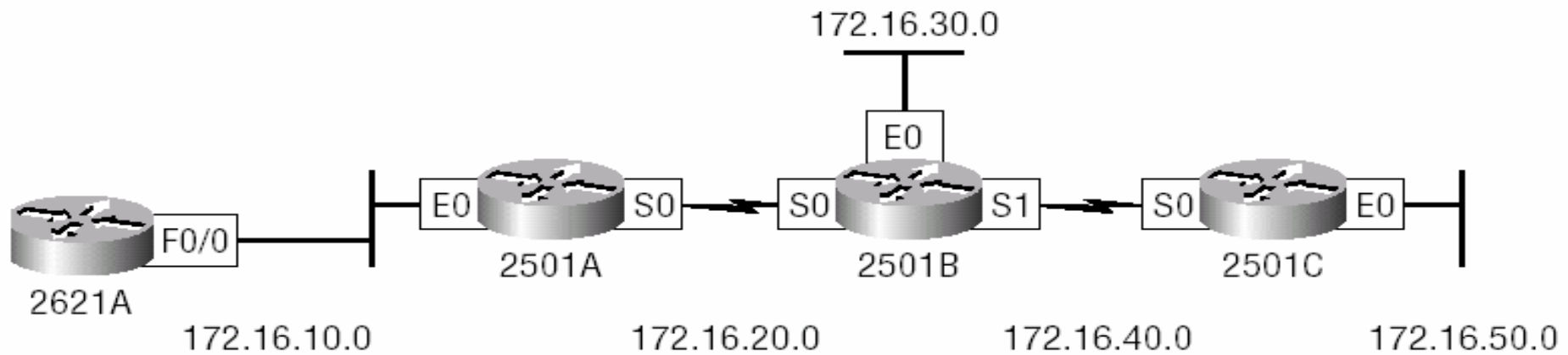
2501B#**show ip route**

Codes: C - connected, S - static, I - IGRP, R - RIP,
Gateway of last resort is not set

172.16.0.0/24 is subnetted, 5 subnets

S	172.16.50.0 [1/0] via 172.16.40.2
C	172.16.40.0 is directly connected, Serial1
C	172.16.30.0 is directly connected, Ethernet0
C	172.16.20.0 is directly connected, Serial0
S	172.16.10.0 [1/0] via 172.16.20.1

2501B#



d. 2501C

The routing table needs to know about networks

- 172.16.10.0
- 172.16.20.0
- 172.16.30.0

```
2501C(Config)# ip route 172.16.10.0 255.255.255.0 172.16.40.1
```

```
2501C(Config)# ip route 172.16.20.0 255.255.255.0 172.16.40.1
```

```
2501C(Config)# ip route 172.16.30.0 255.255.255.0 172.16.40.1
```

d. 2501C

2501C#sh ip route

Codes: C - connected, S - static, I - IGRP, R - RIP,
Gateway of last resort is not set

172.16.0.0/24 is subnetted, 5 subnets

C	172.16.50.0 is directly connected, Ethernet0
C	172.16.40.0 is directly connected, Serial0
S	172.16.30.0 [1/0] via 172.16.40.1
S	172.16.20.0 [1/0] via 172.16.40.1
S	172.16.10.0 [1/0] via 172.16.40.1

2501C#

Verifying Your Configuration

2621A# **ping 172.16.50.1**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.50.1, timeout is 2 seconds:

.!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 64/66/68 ms

2621A#

2501C# **ping 172.16.10.1**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.10.1, timeout is 2 seconds:

!!!!

Success rate is 80 percent (4/5), round-trip min/avg/max = 64/67/72 ms

路由协议分类

- 按自治系统

- IGP（内部路由协议）：RIP、IGRP、OSPF
- EGP（外部路由协议）：BGP

- 按路由算法

- 距离矢量：RIP、IGRP、BGP
- 链路状态：OSPF

● 距离矢量路由协议

- Router间周期性地交换路由表，经过层层交换，使每个路由器获得所有网络信息，并采用算法得出到达每一个网络最佳路径，生成路由表。
- 周期性交换路由表的缺点在于会带来额外的流量。
- 每个Router不知道网络的拓扑结构，只知道与自己相连的网络情况，因此对网络变化收敛的速度慢。

● 链路状态路由协议

- 每个Router与所有其它Router交换LSA（链路状态），最终获得所有Router的LSA，并将之放在一个LSA数据库中，再将LSADB转为一张带权有向图，即是对整个网络拓扑的真实反应。每个Router在图中以自己为根，使用算法得出到达每一点的最短路径，生成路由表。
- 因为路由器知道整个网络的拓扑，所以对网络的变化收敛速度快。
- 路由器不周期的交换路由表，只在网络变化时发送更新信息，因此流量小。

● 路由权（metric）

- 路由协议能发现到达目标网络的所有路径，它每一条路径生成一条metric，metric值最小的路径被认为是达到目标的最佳路径，加入到路由表中。
- 不同路由协议对metric的计算所用的度量值不一样，所以metric只用于同一个路由协议产生的路径比较，它不能用于不同路由协议间路径的比较。

- **Distance（管理级别）**

- 代表一个路由协议的可信度。如果一个路由器同时启用了多个路由协议，而这多个路由协议都发现了到达同一个目标的路径，则只有Distance高的路由协议发现的路由才会被加入到路由表中。

- **默认的Distance**

- **Connected 0**
- **Static 1**
- **EIGRP 90**
- **IGRP 100**
- **OSPF 110**
- **RIP 120**

RIP协议的配置

a. 2621A

```
2621A# config t
```

```
2621A(config)# no ip route 172.16.20.0 255.255.255.0 172.16.10.2
```

```
2621A(config)# no ip route 172.16.30.0 255.255.255.0 172.16.10.2
```

```
2621A(config)# no ip route 172.16.40.0 255.255.255.0 172.16.10.2
```

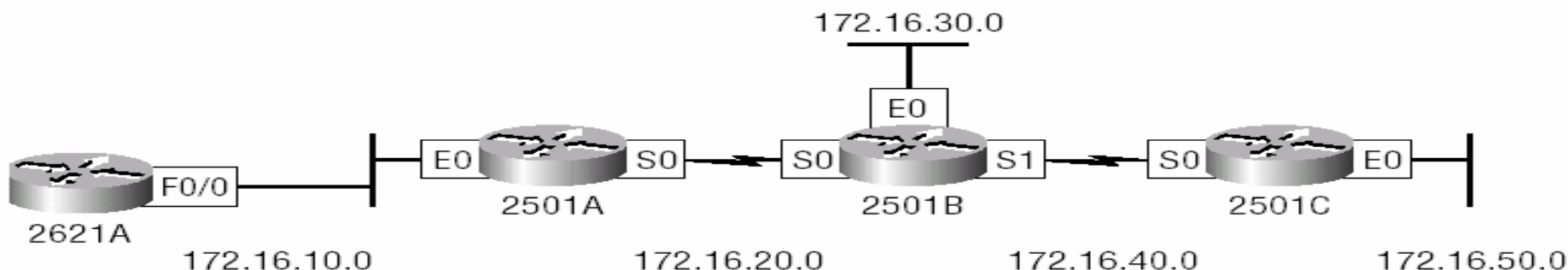
```
2621A(config)# no ip route 172.16.50.0 255.255.255.0 172.16.10.2
```

```
2621A(config)# router rip
```

```
2621A(config-router)# network 172.16.0.0
```

```
2621A(config-router)# ^Z
```

```
2621A#
```



b. 2501A

```
2501A# config t
```

```
2501A(config)# no ip route 172.16.30.0 255.255.255.0  
172.16.20.2
```

```
2501A(config)# no ip route 172.16.40.0 255.255.255.0  
172.16.20.2
```

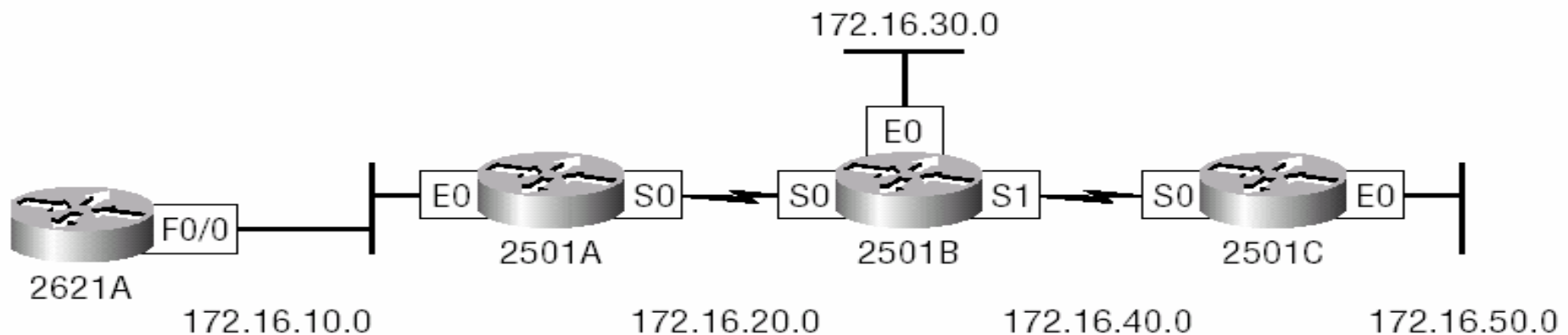
```
2501A(config)# no ip route 172.16.50.0 255.255.255.0  
172.16.20.2
```

```
2501A(config)# router rip
```

```
2501A(config-router)# network 172.16.0.0
```

```
2501A(config-router)# ^Z
```

```
2501A#
```



c. 2501B

```
2501B# config t
```

```
2501B(config)# no ip route 172.16.10.0 255.255.255.0  
172.16.20.1
```

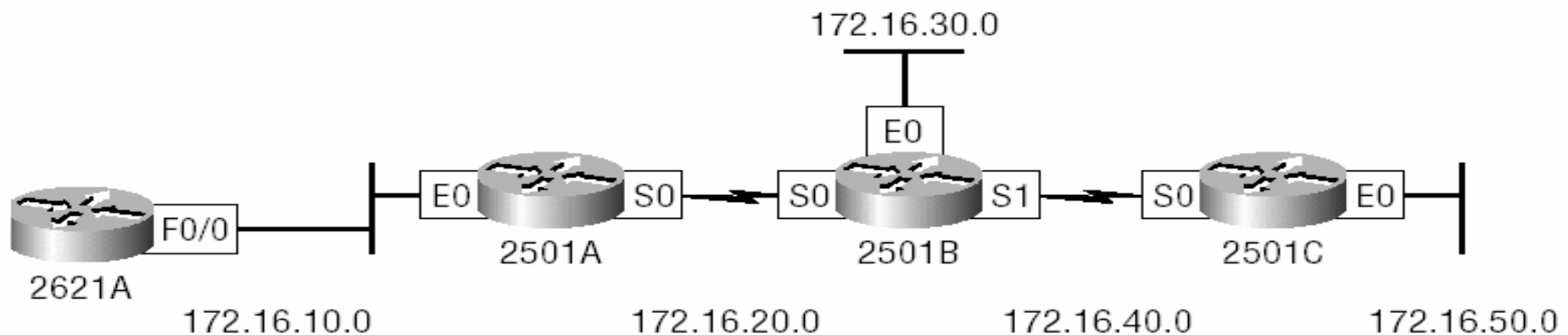
```
2501B(config)# no ip route 172.16.50.0 255.255.255.0  
172.16.40.2
```

```
2501B(config)# router rip
```

```
2501B(config-router)# network 172.16.0.0
```

```
2501B(config-router)# ^Z
```

```
2501B#
```



d. 2501C

```
RouterC# config t
```

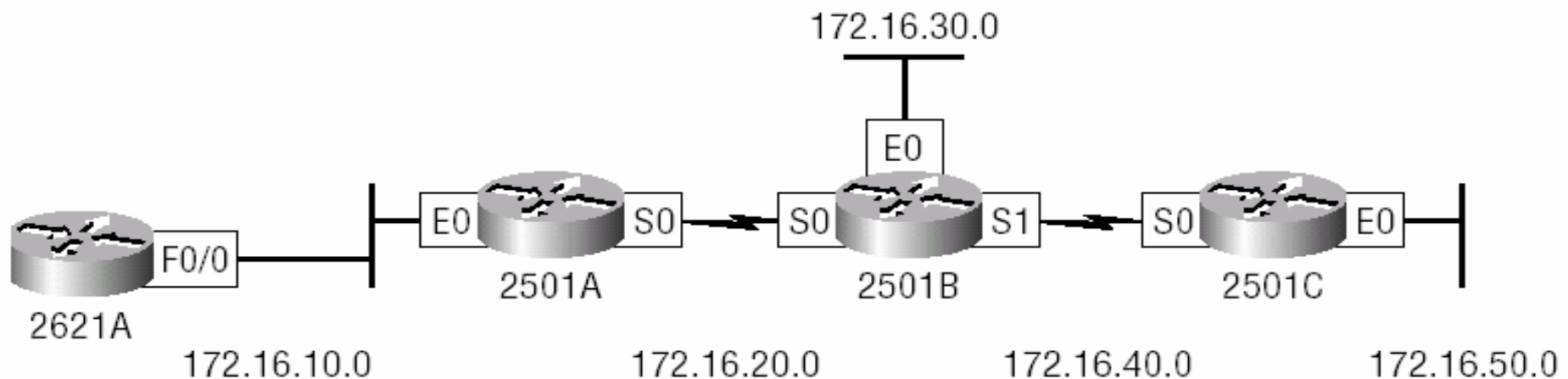
```
RouterC(config)# no ip route 0.0.0.0 0.0.0.0 172.16.40.1
```

```
RouterC(config)# router rip
```

```
RouterC(config-router)# network 172.16.0.0
```

```
RouterC(config-router)# ^Z
```

```
RouterC#
```



Verifying the RIP Routing Tables

a. 2621A

2621A# **show ip route**

Codes: C - connected, S - static, I - IGRP, R - RIP, M –
Gateway of last resort is not set

172.16.0.0/24 is subnetted, 5 subnets

```
R    172.16.50.0 [120/3] via 172.16.10.2, FastEthernet0/0
R    172.16.40.0 [120/2] via 172.16.10.2, FastEthernet0/0
R    172.16.30.0 [120/2] via 172.16.10.2, FastEthernet0/0
R    172.16.20.0 [120/1] via 172.16.10.2, FastEthernet0/0
C    172.16.10.0 is directly connected, FastEthernet0/0
```

2621A#

IGRP协议的配置

a. 2621A

```
2621A# config t
```

```
2621A(config)# router igrp ?
```

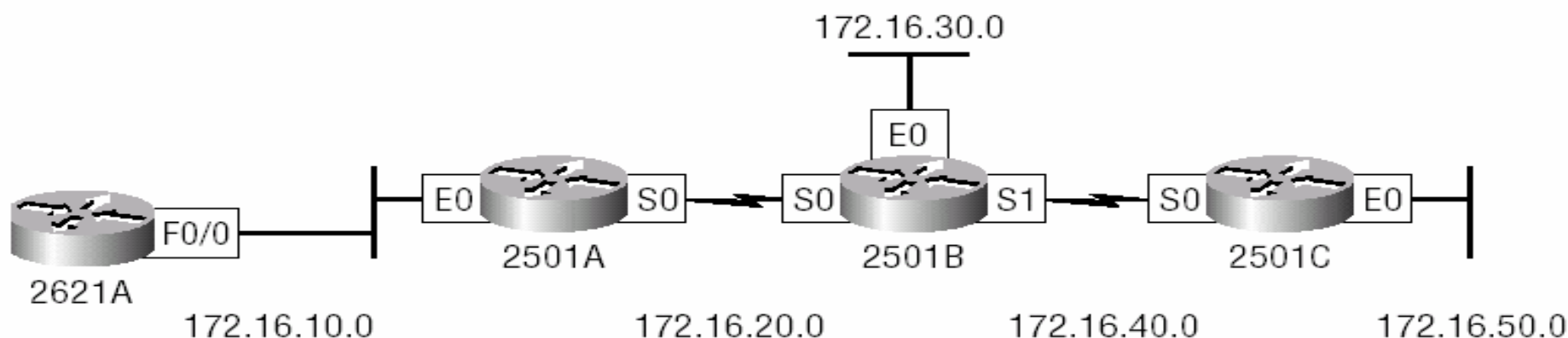
```
<1-65535> Autonomous system number
```

```
2621A(config)# router igrp 10
```

```
2621A(config-router)#network 172.16.0.0
```

```
2621A(config-router)#^Z
```

```
2621A#
```



b. 2501A

```
2501A# config t
```

```
2501A(config)# router igrp 10
```

```
2501A(config-router)# netw 172.16.0.0
```

```
2501A(config-router)# ^Z
```

```
2501A#
```

c.2501B

```
2501B#config t
```

```
2501B(config)# router igrp 10
```

```
2501B(config-router)# netw 172.16.0.0
```

```
2501B(config-router)#^Z
```

```
2501B#
```

d. 2501C

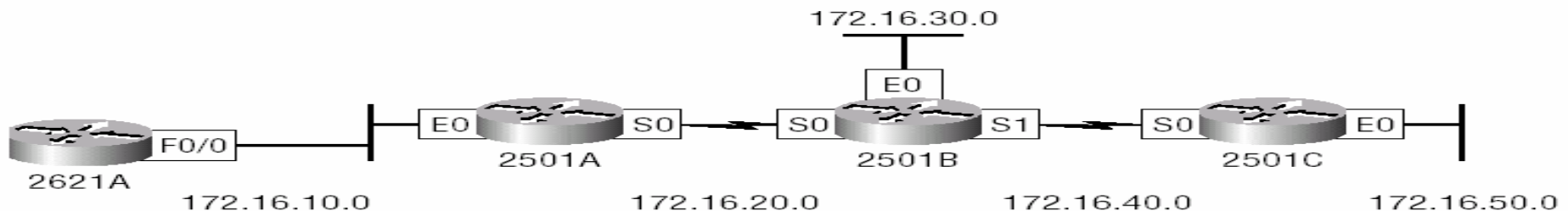
```
2501C# config t
```

```
2501C(config)# router igrp 10
```

```
2501C(config-router)# netw 172.16.0.0
```

```
2501C(config-router)#^Z
```

```
RouterC#
```



Verifying the IGRP Routing Tables

a. 2621A

2621A# **show ip route**

Codes: C - connected, S - static, I - IGRP, R - RIP,
Gateway of last resort is not set

172.16.0.0/24 is subnetted, 5 subnets

I	172.16.50.0 [100/160360] via 172.16.10.2, FastEthernet0/0
I	172.16.40.0 [100/160260] via 172.16.10.2, FastEthernet0/0
I	172.16.30.0 [100/158360] via 172.16.10.2, FastEthernet0/0
I	172.16.20.0 [100/158260] via 172.16.10.2, FastEthernet0/0
C	172.16.10.0 is directly connected, FastEthernet0/0

访问控制列表（ACL）

- 主要内容：
 - 访问控制列表的作用
 - 访问控制列表的种类
 - 访问控制列表的建立

访问控制列表的作用

- 在路由器接口处，决定哪种类型的通信流量被转发，哪种类型的通信流量被阻塞。例如可以允许e-mail通信流量被路由，同时拒绝所有的telnet通信流量。
- 提供网络访问的基本安全手段。例如可以允许某一主机访问你的网络，而阻止另一主机访问同样的网络。

按正确顺序创建ACL

- 在ACL中各描述语句的放置顺序很重要。当路由器决定某一数据包是被转发还是被阻塞时，Cisco IOS按照各描述语句的顺序，根据各描述语句的判断条件，对数据包进行检查。一旦找到某一匹配条件，就结束比较过程，不再检查以后的其他条件判断语句。
- 如果你创建了一个允许所有通信流量通过的条件判断语句，那么后面的所有条件判断语句形同虚设，是不会被检查。如果需要另外的条件判断语句，则必须删除该ACL，然后重新建立一个新的带有一系列条件判断语句的ACL。

访问控制列表的种类

- 标准访问控制列表
 - 只限制IP数据包中的源地址。
- 扩展访问控制列表
 - 可针对IP数据包五元素中任一项进行限制。

源IP	目标IP	协议	源Port	目标Port
-----	------	----	-------	--------

- 访问列表用号码来标识。使用什么号码可由你随意决定，但必须符合：标准ACL使用1—99，扩展ACL使用100 — 199。
- 对一个表的所有语句必须使用相同的号码。

访问控制列表的种类

- 标准访问控制列表
 - 只限制IP数据包中的源地址。
- 扩展访问控制列表
 - 可针对IP数据包五元素中任一项进行限制。

源IP	目标IP	协议	源Port	目标Port
-----	------	----	-------	--------

- 访问列表用号码来标识。使用什么号码可由你随意决定，但必须符合：标准ACL使用1—99，扩展ACL使用100 — 199。
- 对一个表的所有语句必须使用相同的号码。

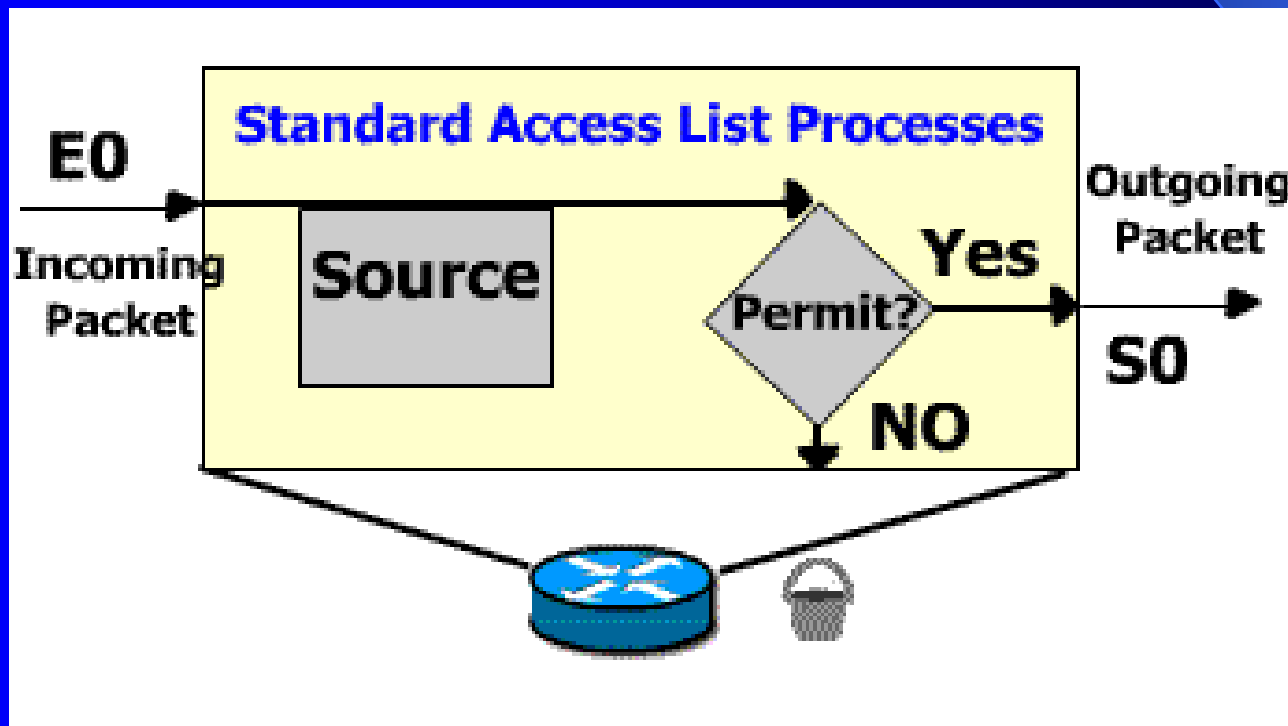
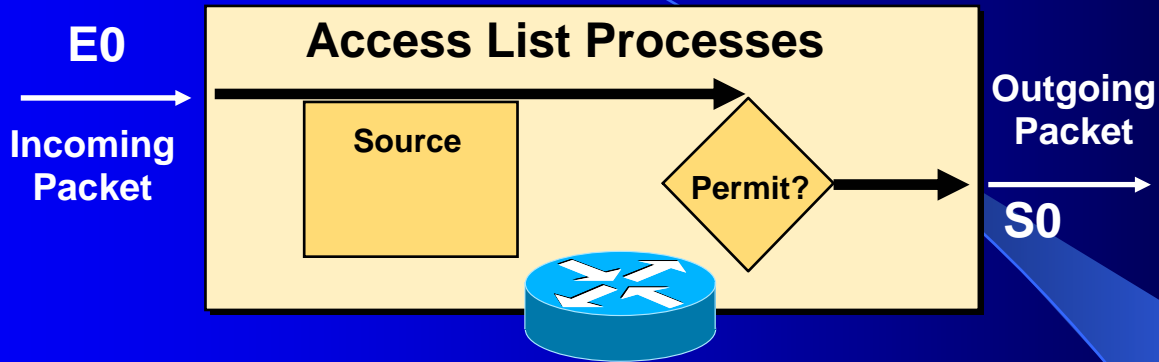
访问控制列表的种类

- 标准访问控制列表
 - 只限制IP数据包中的源地址。
- 扩展访问控制列表
 - 可针对IP数据包五元素中任一项进行限制。

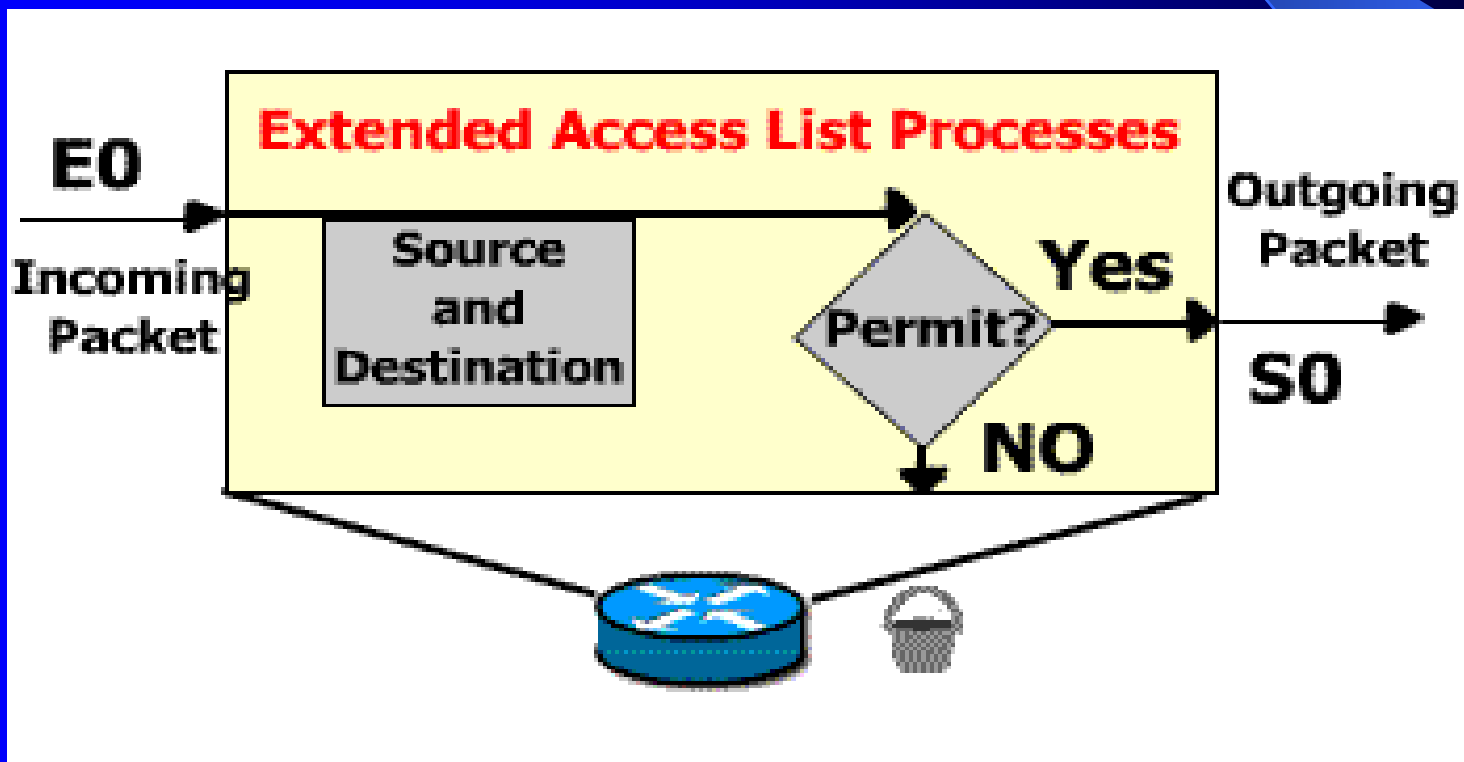
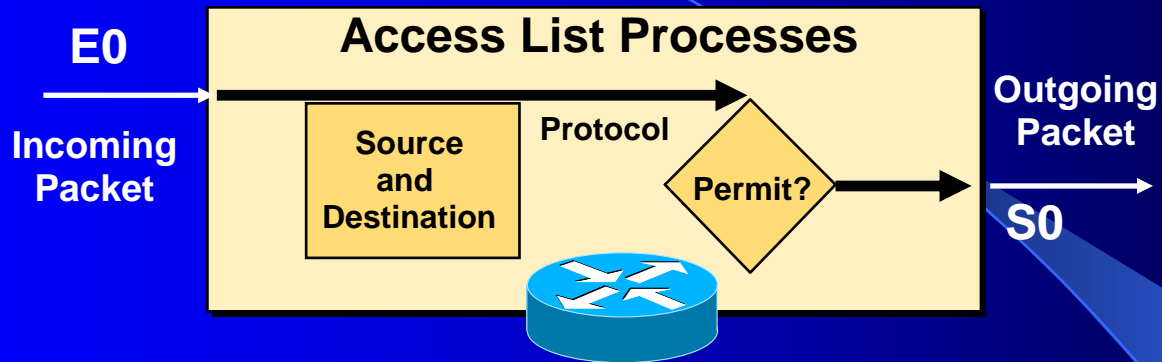
源IP	目标IP	协议	源Port	目标Port
-----	------	----	-------	--------

- 访问列表用号码来标识。使用什么号码可由你随意决定，但必须符合：标准ACL使用1—99，扩展ACL使用100 — 199。
- 对一个表的所有语句必须使用相同的号码。

标准ACL图示



扩展ACL图示



标准ACL建立命令

- 第一步：定义标准ACL

```
Router(config) # access-list access-list-number  
                  {permint | deny} {test-conditions}
```

- 第二步：将ACL应用到某一接口

```
Router(config-if) # ip access-group access-list-number  
                                   {in | out}
```

在定义{test-conditions}时，要使用到反向掩码（通配符掩码）。同时，每一个ACL最后都隐藏了一个语句“deny all”。

反向掩码表示法

- 反向掩码是一个32比特位的数字串，它被用点号分成4个8位组，每个8位组包含8个比特。在反向掩码中，0表示“检查相应的位”，而1表示“不检查相应的位”。反向掩码跟IP地址是成对出现的，通过“1”或“0”来明确如何处理相应的IP地址位。
- 在IP子网掩码中“1”或“0”是用来决定是网络还是相应的主机IP地址。而在ACL的反向掩码中，掩码位“1”或“0”用来决定相应的IP地址是被忽略，还是被检查。

反向掩码表示示例

- 表示一台主机
 - 172.30.16.29 0.0.0.0
 - host 172.30.16.29
- 表示一个网络
 - 172.30.0.0 0.0.255.255
- 表示任何网络
 - 0.0.0.0 255.255.255.255
 - any

反向掩码：

192.168.0.99 0.0.0.255

→ 192.168.0.0/24

反向掩码

192.168.0.99 255.255.255.0

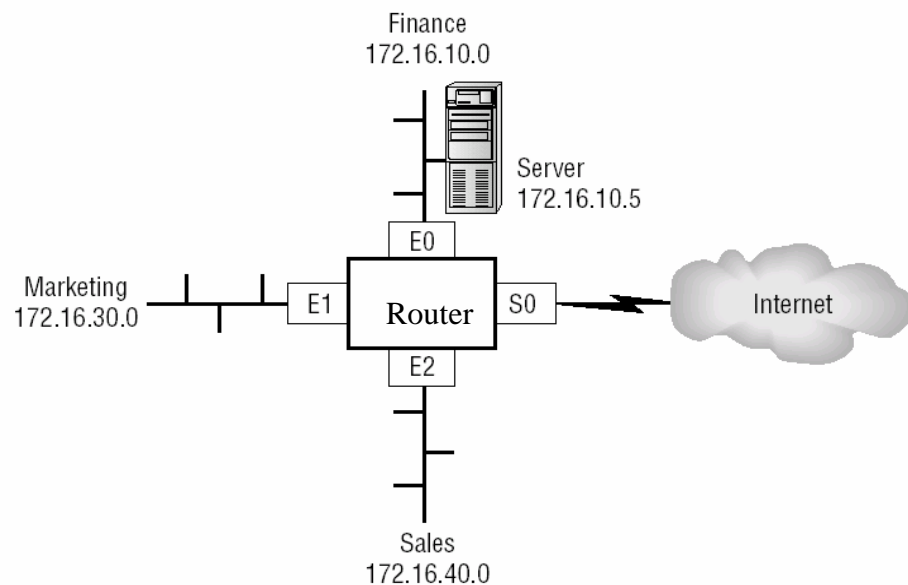
→ 以99结尾的地址

标准ACL例

- (1) access-list 1 deny host 192.168.0.99
(限制所有主机)
- (2) access-list 2 deny host 192.168.0.99
access-list 2 permit any
(只限制IP地址为 192.168.0.99 的主机)
- (3) access-list 3 permit host 192.168.0.99
(除192.168.0.99 的主机都deny)
- (4) access-list 4 deny 192.168.0.99 0.0.0.255
access-list 4 permit any
(限制99结尾的地址)

功能：拒绝来自于172.16.40子网的所有主机访问Server.

IP access list example with three LANs and a WAN connection



Router # config t

Router(config) # access-list 10 deny 172.16.40.0 0.0.0.255

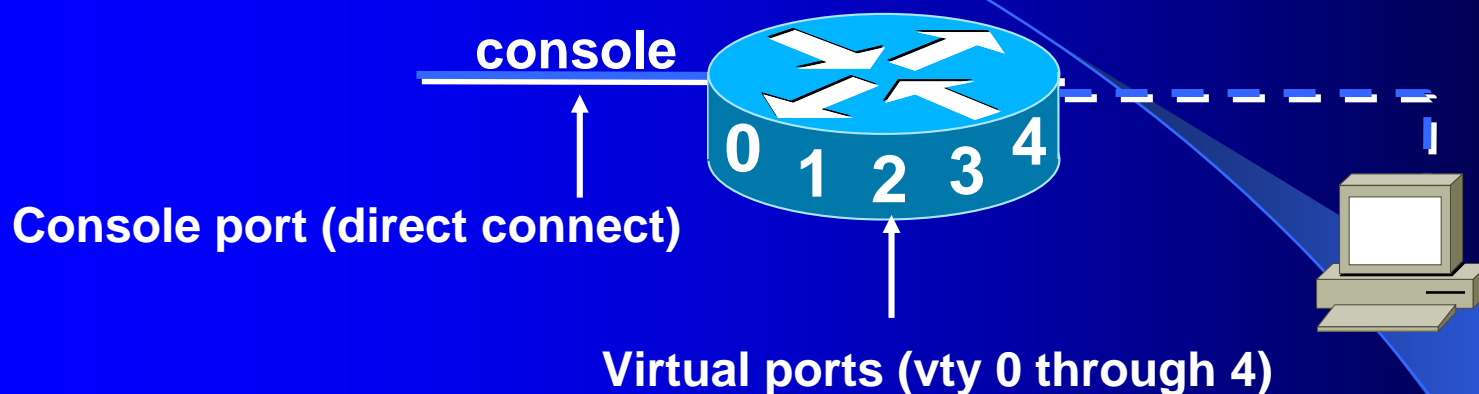
Router(config) # access-list 10 permit any

(or Router(config) # access-list 10 permit 0.0.0.0 255.255.255.255)

Router(config) # interface ethernet 0

Router(config-if) # ip access-group 10 out

功能：通过标准ACL限制主机172.16.10.3对路由器的Telnet访问



```
RouterA(config)# access-list 50 permit host 172.16.10.3
```

```
RouterA(config)#line vty 0 4
```

```
RouterA(config-line)#access-class 50 in
```


扩展ACL建立命令

- 建立扩展ACL

Router(config) # access-list access-list-number {permint | deny} protocol source [source-mask destination destination-mask] [operator operand]

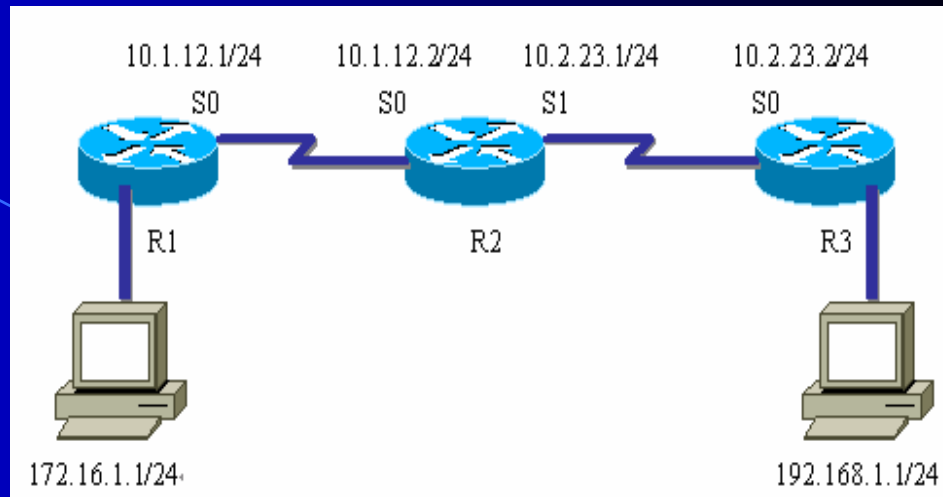
参数	参数说明
access-list-number	访问控制列表表号,使用范围100---199
permit deny	允许或者拒绝后面指定的特定地址通信流量
protocol	指定协议类型,如IP,TCP,UDP,ICMP等
source destination	标识源地址和目的地址
source-mask destination-mask	反向掩码,与源地址和目的地址相对应
operator operand	lt,gt,eq,neg(小于 , 大于 , 等于 , 不等于) 端口号

- 将扩展ACL应用到某一接口

**Router(config-if) # ip access-group
access-list-number {in|out}**

参数	参数说明
access-list-number	指出连接到这个接口的访问控制列表表号
in out	通过选择in还是out来表示该ACL是应用到入站接口还是出站接口。如果没有指定，默认是out。

功能：在R2上用扩展列表
禁止R3 telnet、FTP到R1。



R2 # config t

R2(config) # access-list 120 deny tcp 10.2.23.0 0.0.0.255 host 10.1.12.1 eq 23

R2(config) # access-list 120 deny tcp 10.2.23.0 0.0.0.255 172.16.1.0
0.0.0.255 eq 23

R2(config) # access-list 120 deny tcp 10.2.23.0 0.0.0.255 host 10.1.12.1 eq 21

R2(config) # access-list 120 permit ip any any

R2(config) # interface serial 0

R2(config-if) # ip access-group 120 out

1)限制主机192.168.0.222到网络131.107.0.0/16的ICMP流量

```
RB(config)#access 101 deny icmp host 192.168.0.222 131.107.0.0 0.0.255.255
```

```
RB(config)#access 101 permit ip any any
```

```
RB(config)#int e0
```

```
RB(config-if)#ip access-group 101 in
```

```
RB(config-if)#no ip access-group 101 in
```

2)限制网络192.168.0.0/24到所有网络的ICMP流量

```
RB(config)#access 102 deny icmp 192.168.0.0 0.0.0.255 any
```

```
RB(config)#access 102 permit ip any any
```

```
RB(config)#int e0
```

```
RB(config-if)#ip access-group 102 in
```

```
RB(config-if)#no ip access-group 102 in
```

3) 只允许主机192.168.0.99通过Telnet访问131.107.0.0/16网段

```
RB(config)#access 103 permit tcp host 192.168.0.99 131.107.0.0 0.0.255.255 eq 23
```

```
RB(config)#int e0
```

```
RB(config-if)#ip access-group 103 in
```

```
RB(config-if)#no ip access-group 103 in
```

4) 使所有其他网段只能访问192.168.0.0/24的WWW、FTP、TELNET服务

```
RB(config)#access 104 permit tcp any 192.168.0.0 0.0.0.255 eq www
```

```
RB(config)#access 104 permit tcp any 192.168.0.0 0.0.0.255 eq ftp
```

```
RB(config)#access 104 permit tcp any 192.168.0.0 0.0.0.255 eq telnet
```

了解路由器对X.25网络的配置

- X.25协议是CCITT (ITU) 建议的一种协议，它定义终端和计算机到分组交换网络的连接。分组交换网络在一个网络上为数据分组选择到达目的地的路由。X.25是一种很好实现的分组交换服务，传统上它是用于将远程终端连接到主机系统的。这种服务为同时使用的用户提供任意点对任意点的连接。来自一个网络的多用户的信号，可以通过多路选择通过X.25接口而进入分组交换网络，并且被分发到不同的远程地点。一种称为虚电路的通信信道在一条预定义的路径上连接端点站点通过网络。虽然X.25吞吐率的主要部分是由于错误检查开销的，X.25接口不支持高达64kbps的线路，CCITT在1992年重新制定了这个标准，并将速率提高到2Mbps。

了解路由器对X.25网络的配置

- X.25的分组交换体系结构具有一些优点和缺陷。信息分组通过散列网络的路由是根据这个分组头中的目的地址信息进行选择的。用户可以与多个不同的地点进行连接，而不象面向电路的网络那样在任何两点之间仅仅存在一条专用线路。由于分组可以通过路由器的共享端口进行传输的，所以就存在一定的分发延迟。虽然许多网络能够通过选择回避拥挤区域的路由来支持过载的通信量，但是随着访问网络人数的增多，用户还是可以感觉到性能变慢。与此相反，面向电路的网络在两个地点之间提供一个固定的带宽，它不能适应超过这个带宽的传输的要求。

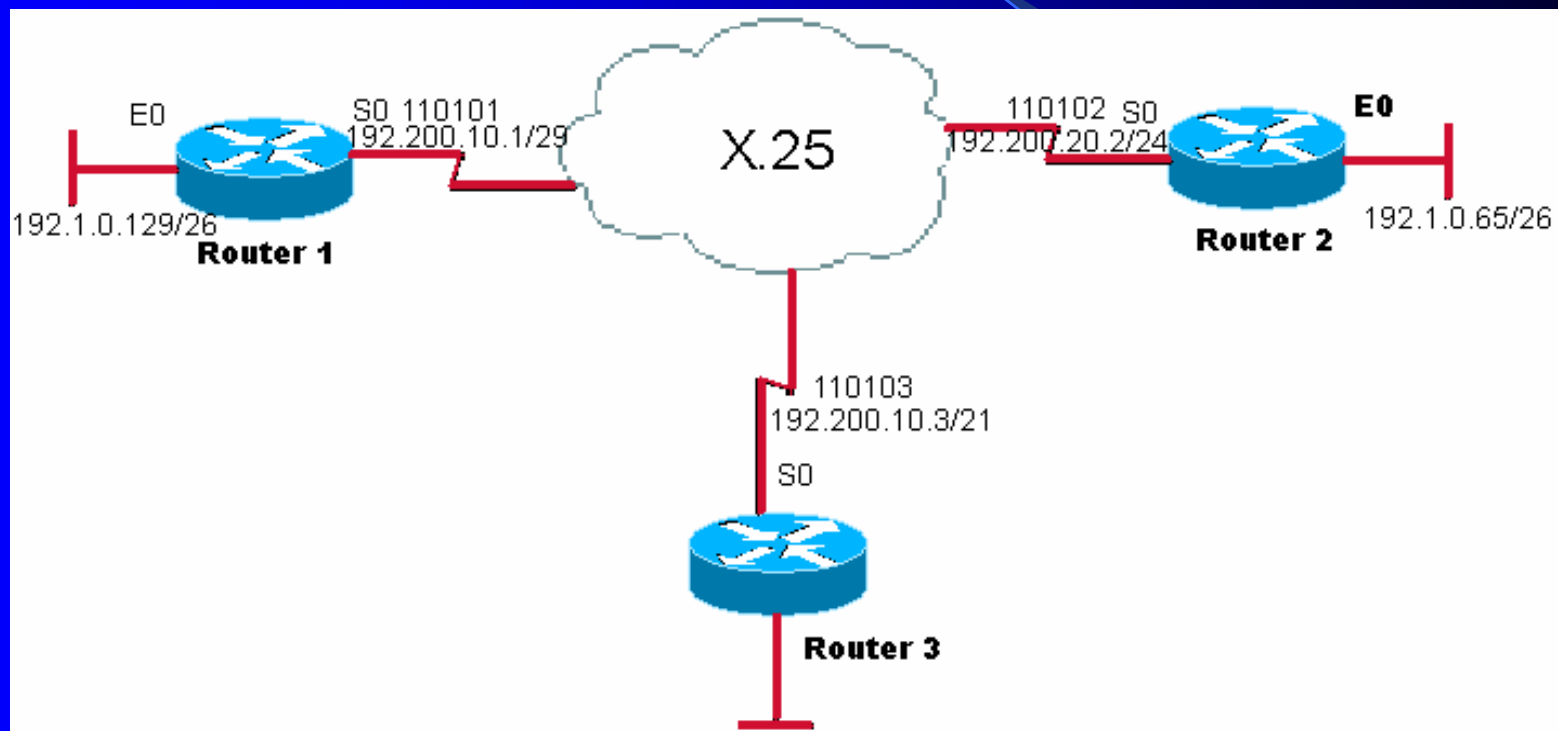
了解路由器对X.25网络的配置

- X.25的开销比帧中继要高许多。例如，X.25中，在一个分组的传输路径上的每个结点都必须完整地接收一个分组，并且在发送之前还必须完成错误检查。帧中继结点只是简单地查看分组头中的目的地址信息，并立即转发该分组，在一些情况下，甚至在它完整地接收一个分组之前就开始转发。帧中继不需要X.25中必须在每个中间结点中存在的用于处理管理、流控和错误检查的状态表。端点结点必须对丢失的帧进行检查，并请求重发。

了解路由器对X.25网络的配置

- X.25受到了低性能的影响，它不能适应许多实时LAN对LAN应用的要求。然而，X.25很容易建立，很容易理解，并且已被远程终端或计算机访问，以及传输量较低的许多情况所接收。X.25可能是电话系统网络不可靠的国家建立可靠网络链路的唯一途径。在很多国家已经被帧中继技术替代。

配置X.25



配置X.25

- 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
```

配置X.25

- 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
```

配置X.25

- Router3:

```
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
```

路由器对ISDN网络配置

什么是综合业务数字网（ISDN）

- CCITT定义ISDN为：ISDN是以综合数字网为基础发展演变而成的通信网，能够提供端到端的数字连接，用来支持包括语音和非语音在内的多种电信业务，用户能够通过有限的一组标准化的多用途的用户—网络接口接入网内。

ISDN业务

- 基本速率接口 (BRI)
- 主要速率接口 (PRI)

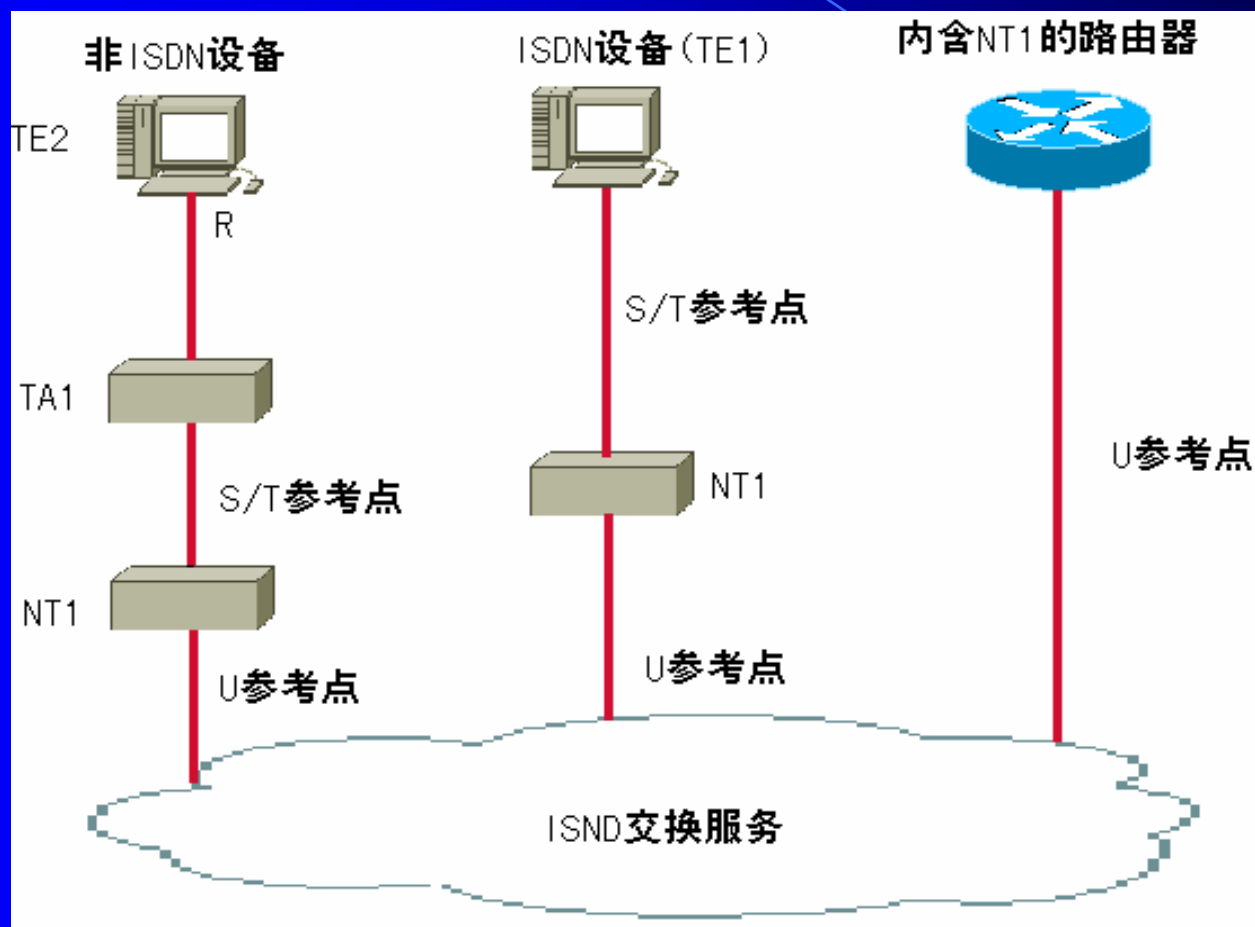
基本速率接口（BRI）

- ISDN BRI包括三个独立的信道。其中两个信道称为B信道（Bearer，承载信道），通信速率为64kbit/s，用于传递声音或数据。第三条信道称为D信道，它是16kbit/s的信号通道，用于传输指导电话网络如何操作每个B信道的指示信息。三个信道总的数据传输率达到144kbit/s，ISDN BRI通常也被称为“2B+D”。
- ISDN提供了很高的灵活性，因为它的每个B通道可以各自独立地传输声音或数据应用。例如，在使用一条ISDN 64kbit/s的B信道来从企业通信网下载一个长文档的同时，另一条B信道可以同时用来浏览Web网页。在设计阶段需要注意保证所选的设备能够充分利用这种灵活性。

主要速率接口（PRI）

- ISDN PRI（Primary Rate Interface）通常也称为“23B+D”（在美国和日本），其速率为1.55Mbit/s，或者称为“30B+D”（在欧洲、澳洲等世界上其它地区），速率为2.048Mbit/s。PRI的通常应用是为了在企业办公室或其它中心站点上传输大量的ISDN入局呼叫。

BRI功能组与参照点



ISDN配置

- 在Cisco的router上配置ISDN的时候，在接口配置模式下执行isdn spid1和isdn spid2命令。这些都是由ISDN服务商提供.SPID配置的第二部分是定义SPID的本地目录号，这个是可选的。如下：

```
RouterA(config)#isdn switch-type basic-ni
```

```
RouterA(config)#int bri0
```

```
RouterA(config-if)#encap ppp
```

```
RouterA(config-if)#isdn spid1 086506610100 8650661
```

```
RouterA(config-if)#isdn spid1 086506620100 8650662
```

- 注意：上面的encap ppp命令也是可选命令，执行isdn switch-type命令用于全局配置模式下，使整个router的所有BRI接口都生效；但是假如只有1个BRI接口的话，在全局模式使用这个命令和在BRI的接口配置模式使用这个命令效果是一

路由器对帧中继网络的配置

什么是帧中继网络

- 帧中继（Frame Relay）是为了解决新兴数据应用不断改变的需要，动态并且快速前进的商业和计算机环境，以及应用处理能力的提高而特别建立的。它的出现填补传统服务所造成的空白，解决商业组织结构变化的问题，以及满足更快和更好的通信需求。

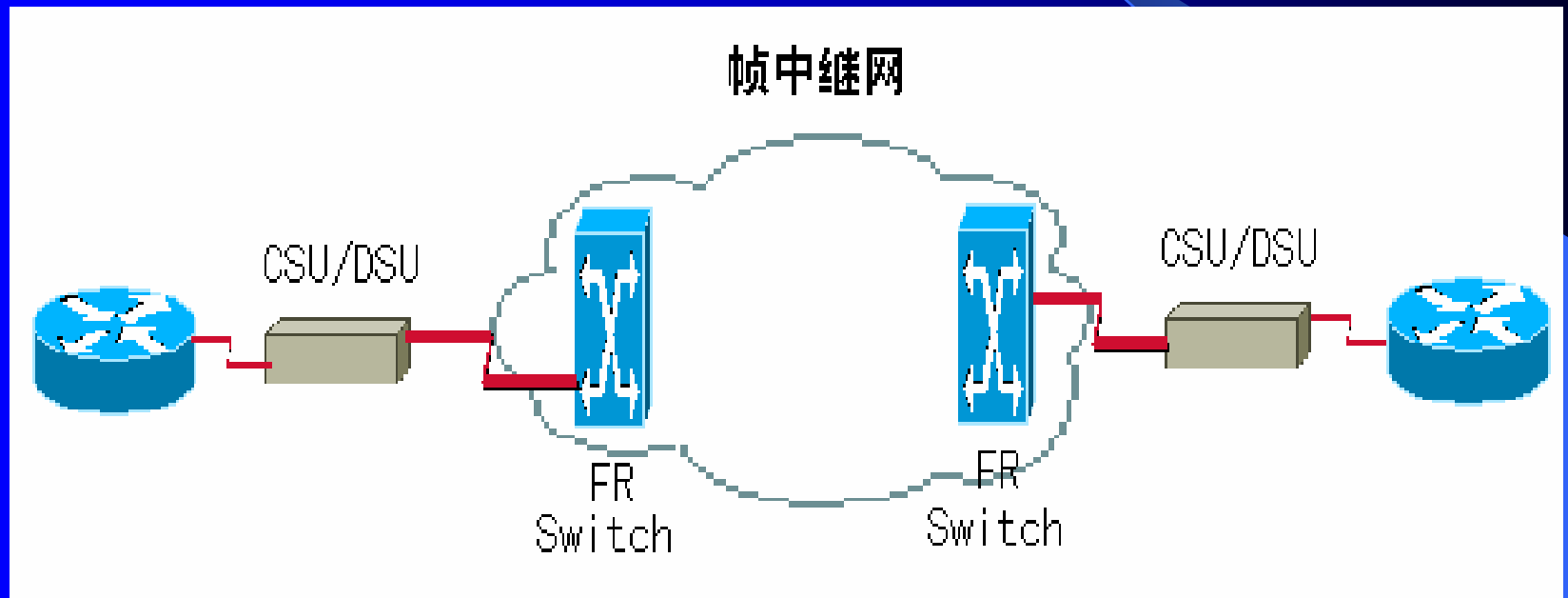
什么是帧中继网络

- 帧中继是一种独特的网络解决方案，它是多种成熟技术的组合。帧中继源于使用时分多路复用技术的电路交换和使用统计多路复用技术的X.25分组交换，它将时分多路复用技术的高速度和低延迟的特征与统计多路复用技术的带宽共享和分组交叉存取功能结合起来，允许单个物理网络接口支持多个逻辑连接。它通过虚连接既提供了专线的安全性，但同时也允许对网络容量进行统计分配，这意味着只有现在进行的应用可以访问共享的带宽资源，空闲的应用不占用任何网络带宽，从而避免带宽白白的被闲置浪费。

什么是帧中继网络

- 帧中继与X.25不同的是，它不进行额外的传输纠错处理。相反，它将这种功能交给处于每一个连接的智能化设备和较高层协议来完成。帧中继是X.25的改进版本，它只使用OSI参考模型的第一层和第二层，不进行差错控制和流量控制，消除了不必要的功能后，帧中继得以更快更有效的运行。

帧中继网络连接及术语介绍



帧中继网络连接及术语介绍

- 帧中继定义了两种接口，即UNI（用户网络接口）和NNI（网络网络接口）。UNI在用户与公众帧中继网络之间提供接口，而NNI则负责在两个帧中继服务网络之间提供接口。用户一方面通过路由器或帧中继访问设备（Frame Relay Access Device，FRAD）经由UNI与其它FRND相连（如FR Switch），另一方面NNI将所有的FRND连接在一起。

帧中继网络连接及术语介绍

- 帧中继最为重要的部分是虚电路，共有两种类型的帧中继虚电路连接，即永久虚电路（Permanent Virtual Circuit, PVC）和交换虚电路（Switched Virtual Circuit, SVC）。虚电路的运行与租用线路类似，但是其不同之处在于虚电路是在软件中定义而不是在物理硬连接线上定义的，这就在服务供应上提供了灵活性，使得初装、移动、增加和改变相当方便。

永久虚电路

- 永久虚电路（PVC）意味着一旦它在两个端口连接间分配，它就会始终存在和有效（除非网络不能从故障中恢复时）。在PVC上传输的帧每次都能使用相同的路径并且按序传输。网络无需在目的地将帧重新排列得到正确序列。尽管服务提供商在公众帧中继网络上建立了多个用户，每一个PVC只能分配给一个用户。目前，帧中继服务提供商大多只向用户提供PVC服务，而很少提供SVC服务。

交换虚电路

- 交换虚电路（SVC）不是始终存在的，它是当信息需要被发送时，在用户设备和服务提供商的网络之间通过智能化协商而建立起来的。在完成传输后，网络的连接也将被释放，虚电路立即消失。SVC允许在已经同网络连接的站点之间建立自发的连接，这尤其适用于需要与某些地点进行不定时连接的那些应用。

数据流（Data Flow）相关术语

- 访问速率（access rate）：每个帧中继接口可以传输的最大带宽。
- 约定信息速率（committed information rate, CIR）：正常情况下，帧中继网络传输数据的速率，它是在最小单位时间内的传输数据平均值，单位为bps。
- 约定猝发速率（committed burst rate, CBR）：表示帧中继网络可通过的数据最大的传输速率，单位是bps。
- 丢弃适选者位（Discard Eligibility, DE）：由DTE设备设置，长度为1位。用来表示1个帧的重要性比正在传输的其它帧低。在网络发生拥塞状态后，首先将丢弃那些设置了DE位的帧。
- 向前显式拥塞通知（Forward Explicit Congestion Notification, FECN）：长度为1位。当它被设置为1的时候，说明帧在从源地址到目标地址的传输线路上出现了拥塞。
- 向后显式拥塞通知（Backward Explicit Congestion Notification, BECN）：长度为1位。当它被设置为1的时候，说明帧在从源地址到目标地址的传输线路的相反方向上出现了拥塞。

数据链路连接标识符

- 每条帧中继许电路都要用DLCI来标识自己，DLCI一般由服务商比如电信公司指定。而且DLCI是局部性的，也就是说DLCI在帧中继网络中不是惟一的。

链路管理接口

本地管理接口（Local Management Interface，LMI）是对基本的帧中继标准的扩展集。它是用户的router和第一个帧中继switch之间的信令（signaling）标准。LMI使得DLCI具有全局性而不再是局部性。即DLCI的值成了DTE设备的地址。它提供以下信息。

- keepalives：通过这个来验证数据是否有进行传输。
- 组播：可选的LMI扩展。使用保留DLCIs 1019到1022。
- 全局寻址（global addressing）：使得DLCI具有全局性，使得帧中继网络看上去就像是LAN那样工作

链路管理接口

router的定义了封装类型为帧中继的接口从服务提供商的帧中继switch接收和更新虚电路的状态。3种不同的状态：

- 活跃（active）状态：配置正常，router之间可以交换信息。
- 非活跃（inactive）状态：router接口为up状态，而且可以和帧中继switch进行通信，但是远端router没有工作。
- 删除（deleted）状态：没有LMI信息在router接口和帧中继switch之间进行传递。可能是线路问题或者映射（mapping）出错。

帧中继的配置

- 封装类型：当对Cisco的router进行配置帧中继的时候，必须定义串行接口的封装类型。在接口配置模式下执行encapsulation frame-relay命令，如下：

```
Router(config)#int s0
```

```
Router(config-if)#encap frame-relay ?
```

```
ietf Use RFC1490 encapsulation
```

```
<cr>
```

帧中继的配置

- LMI类型设置：3种LMI信息类型：Cisco，ANSI和Q.933A。根据电信公司switch的类型和配置而不同。Cisco的设备默认LMI类型是Cisco。从IOS版本11.2开始，LMI类型就是自动检测。如果用户的设备没有这个功能，那就要手动配置，如下：

RouterA#(config-if)#frame-relay lmi-type ?

cisco

ansi

q933a

帧中继的配置

- 地址映射：路由表中的下一跳网关地址（三层协议地址）必须要被正确解析为相应的帧中继DLCI号码才能正常使用。这种三层协议地址到而层帧中继DLCI号码的映射可以通过两种方式进行，一种是利用Map命令静态指定；另一种是利用Inverse ARP机制自动建立帧中继映射。

Map命令静态指定

- 如果一些设备不支持动态建立映射，可以采用静态指定的方式，命令如下：

```
Router(config-if)#frame-relay map ip  
202.120.1.1 101
```

- //下一跳IP网关地址为202.120.1.1，本地DLCI号码为101

Inverse ARP动态映射

- 路由器在初始化LMI交换时从交换机那里知道所有正在使用的DLCI，然后路由器就向每个DLCI发送一个Inverse ARP请求，询问端口上配置的每个协议（如果支持相应协议）。从Inverse ARP返回的信息就可以用来建立路由器的帧中继映射。

Inverse ARP动态映射

子接口：现在来看看1个物理接口配置多个虚电路的实例。首先要创建子接口。子接口是逻辑接口，多个子接口可以只占用1个物理接口。这个也叫多路复用multiplexing。具体这样配置：先定义物理串行接口的封装类型；然后创建子接口，一般来说每个子接口1条PVC，如下：

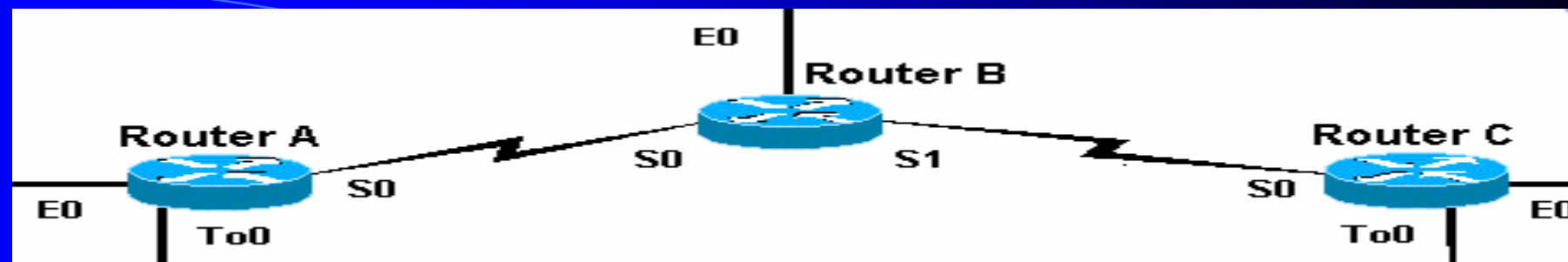
- RouterA(config)#int s0
- RouterA(config-if)#encap frame-relay
- RouterA(config-subif)#int s0.16 ?
- Multipoint Treat as a multipoint link
- point-to-point Treat as a point-to-point link
- RouterA(config-subif)#int s0.16 point-to-point

帧中继验证命令

- show frame lmi：提供本地router和帧中继switch的LMI信息交换的统计信息，包含LMI错误信息和LMI类型等。
- show frame pvc：显示所有配置了的PVC和DLCI信息，提供每条PVC的连接信息和流量统计，还有每条PVC上接收到的BECN和FECN包的信息。如果具体想显示PVC 16的话，就执行show frame pvc 16命令。
- show interface：检查LMI流量，显示封装类型和OSI参考模型的层2和层3的信息。还包括协议，DLCI等信息。
- show frame mDap：显示OSI参考模型中的网络层到DLCI的映射。
- debug frame lmi：允许根据交换了的正确的LMI信息来验证和排错帧中继连接。

CDP协议

- CDP : Cisco Discovery Protocol
 - Cisco发现协议，运行于IOS10.3版本后的Cisco设备。运行CDP协议的Cisco设备会自动检测到运行CDP的相邻的Cisco设备，并与之交换信息，使管理员可获取这些设备的信息。
- 命令：show cdp ?



Router A			Router B			Router C		
Device	IP Address	IPX	Device	IP Address	IPX	Device	IP Address	IPX
Ethernet 0	172.16.11.1		Ethernet 0	172.16.10.6		Ethernet 0	172.16.50.1	
Serial 0	172.16.20.1		Serial 0	172.16.20.2		Serial 0	172.16.40.2	
Token Ring 0	172.16.15.1		Serial1	172.16.40.1		Token Ring 0	172.16.55.1	

RouterA Con0 is now available

Press RETURN to get started.

User Access Verification

Password:

RouterA>en

RouterA#show cdp ?

entry Information for specific neighbor entry

interface CDP interface status and configuration

neighbors CDP neighbor entries

traffic CDP statistics

<cr>

1. 显示邻居信息 show cdp neighbors

```
RouterB#show cdp neighbors
```

```
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge  
S - Switch, H - Host, I - IGMP, r - Repeater
```

Device ID	Local Intrfce	Holdtme	Capability	Platform	Port ID
RouterC	Ser 1	121	R	2500	Ser 0
RouterA	Ser 0	178	R	2500	Ser 0

```
RouterA#|
```

2. 显示接口信息 show cdp interface

```
RouterB#show cdp interface
```

```
Ethernet0 is up, line protocol is up
```

```
Encapsulation ARPA
```

```
Sending CDP packets every 60 seconds
```

```
Holdtime is 180 seconds
```

```
Serial0 is up, line protocol is up
```

```
Encapsulation HDLC
```

```
Sending CDP packets every 60 seconds
```

```
Holdtime is 180 seconds
```

```
Serial1 is up, line protocol is up
```

```
Encapsulation HDLC
```

```
Sending CDP packets every 60 seconds
```

```
Holdtime is 180 seconds
```

3. 显示与之相直连的设备(show cdp entry *)

```
RouterB#sh cdp entry *
-----
Device ID: RouterC
Entry address(es):
IP address: 172.16.40.2
Interface: Serial1, Port ID (outgoing port): Serial0
Holdtime : 175 sec

-----
Device ID: RouterA
Entry address(es):
IP address: 172.16.20.1
Interface: Serial0, Port ID (outgoing port): Serial0
Holdtime : 130 sec
```

```
RouterB#show cdp entry routerc
-----
Device ID: RouterC
Entry address(es):
IP address: 172.16.40.2
Interface: Serial1, Port ID (outgoing port): Serial0
Holdtime : 175 sec
```

广域网协议PPP、PAP、 CHAP的配置

PPP的组成

- PPP是OSI参考模型层2协议，可以使用在异步串行连接比如拨号（dial-up）或者同步串行连接比如ISDN上。它使用链路控制协议（Link Control Protocol，LCP）来建立和保持连接。PPP的主要目的是通过数据链路层点对点的传输OSI参考模型层3数据包。注意PPP的协议栈只定义在OSI参考模型的层1和层2。NCP用于建立和配置多种网络层协议。PPP允许采用多种网络层协议。PPP可以工作在任何DCE/DTE接口比如EIA/TIA-323-C（以前为RS-232-C），ITU-T（原CCITT）V.35等，惟一要求是必须提供全双工线路。

PPP链路操作

下面是PPP链路建立的过程：

- Link Dead阶段。
- 连接建立阶段。
- 验证阶段。
- 网络协议阶段。
- 连接结束阶段。

PPP认证协议（PAP和CHAP）

- 密码验证协议（Password Authentication Protocol，PAP）：PAP是2种验证方法中比较不安全的一种。密码使用英文（clear text）的方式发送。PAP只在初始化连接的时候执行。当PPP连接完成后，远端节点发回源router的用户名和密码直到验证被确认。
- 挑战握手验证协议（Challenge Handshake Authentication Protocol，CHAP）：用于初始化连接的时候，周期性对连接进行检查保证通信方没有改变被替换。当初始化连接的阶段完成后。本地router发送个挑战请求给远端设备。然后远端设备发送回1个用MD5方式加密的值给发送方。如果值不匹配，连接将立即被终止。

PPP配置

在每个路由器上设置用户名和密码。

- Router(config)#username username password secret
- Name：远端路由器的主机名，注意它是区分大小写的。
- Secret：在Cisco路由器上要求通信双方的secret密码相同。
- 进入需要配置的接口的接口配置模式。
- 为接口配置PPP封装。
- Router(config-if)# encapsulation ppp

配置ppp认证。

- Router(config-if)# ppp authentication { chap | chap pap | pap chap | pap }

如果CHAP和PAP都被使用了，那么在链路协商阶段将用第一个指定的方式发起请求。如果对方建议使用第二种方法或者只是简单地拒绝使用第一种方式，那么将采用第二种方式。

在Cisco IOS 11.1和更高的版本中，如果要配置路由器发送PAP消息，则必须在该接口上使用PAP协议，因为PAP默认是无效的。

- Router(config-if)# **ppp pap sent**username username password password

路由器的备份与恢复 (OS)

OS的备份

- 把操作系统文件保存在网络中的服务器上是一个很好的做法，帮助用户在系统文件丢失时，尽快恢复系统正常运行。
- 拷贝系统镜像到网络服务器，首先显示IOS文件的文件名：show flash，拷贝系统文件到TFTP Server：copy flash tftp。

OS的恢复

- 在路由器的日常维护中，有时路由器不能正常启动，只能进入ROM Monitor 模式。
- 这时就需要恢复IOS。通常只要有一台TFTP服务器、一根交叉网线和一根CONSOLE的配置线。在TFTP服务器上安装有ciscotftp软件，将它的根目录设置成存放IOS的目录。用交叉网线连接TFTP服务器网卡和路由器的以太网接口，CONSOLE 配置线连接TFTP服务器的串口和路由器的CONSOLE口，在TFTP服务器上运行ciscotftp软件。打开仿真终端（配置参数为：波特率9600、数据位8位、停止位1位）出现ROMMON 1 。
- 在ROMMON 1 后输入IP ADDR=ROUTER的IP地址（与TFTP服务器的IP地址同一网段）。
- 出现 ROMMON 2 在此后输入IP_SUBNET_MASK=ROUTER的子网掩码。
- 出现 ROMMON 3 在此后输入DEFAULT_GATEWAY=默认网关（可无，也可是TFTP服务器）。
- 出现 ROMMON 4 在此后输入TFTP_SERVER=TFTP服务器的IP地址。
- 出现 ROMMON 5 在此后输入TFTP_FILE=IOS文件名（不带路径）。
- 出现 ROMMON 6 输入tftpdnload 回车。
- 在执行tftpdnload命令完后，根据提示选择可完成文件传输。
- 至此，IOS就恢复。

路由器灾难恢复

- 随着互联网规模的不断扩大，网络与人们的生活已经越来越接近，许多政府、学校和公司都组建了自己的信息网。这使得路由器的使用越来越广泛。在使用路由器的过程中经常会出现忘记密码的情况，使维护人员无法登录，影响工作的进一步开展。同时，在操作过程中有时会因为一些意想不到的原因，将路由器内部的版本映像文件损坏，使路由器无法正常工作，路由器退回到监控状态，使用常用的版本拷贝命令无法更新版本。这两个问题都是较常见，但又是初学者感到比较棘手的问题。
- 对于版本的获得一般可以通过网站下载，或与供应商联系提供，也可以在路由器正常工作利用常规命令将版本备份到服务器上，以备应急之用。Cisco路由器品种较多，各种路由器的密码恢复和版本的灾难恢复情况又不同，现分别叙述。

2500系列路由器密码恢复

- 利用DB25转换接口，和交叉线将Cisco 2500 系列中的2509路由器的CONSOLE口和计算机串口相连，启动计算机超级终端，设置其参数为波特率9600，数据位8，奇偶校验为无，停止位为1，流控选择无。开启路由器电源，在开机60秒内按快捷键“ctrl+break”使路由器进入rom monitor 状态，提示符 >。

2500系列路由器密码恢复

- 查看configure –register值，并将该值记下。命令如下：

```
>e/s2000002
```

- 返回值正常时一般为2102。

2500系列路由器密码恢复

- 更新configure-register 值使路由器启动时跳过配置文件，直接启动，以便使原来的密码不起作用。命令如下：

```
>o/r0x0142
```


2500系列路由器密码恢复

- 重新启动路由器。
- 启动后进入特权模式，执行如下命令使原来的配置信息有效。

router(config)#config mem。

- 此时可以按照正常操作查看原来的密码，或修改为新的密码。

2500系列路由器密码恢复

- 重新启动路由器。
- 启动后进入特权模式，执行如下命令使原来的配置信息有效。

router(config)#config mem。

- 此时可以按照正常操作查看原来的密码，或修改为新的密码。

2500系列路由器密码恢复

- 将configure-register 值复原，并重新启动路由器。此时即可恢复正常。

Router(config)#configure-register 0x2102。

Router(config)#wri

Router(config)#reload

2500系列路由器版本灾难性恢复

- 与其它路由器不同的是2509在rom内部有一个引导监控模式，内含一个小的映象版本，当flash中版本损坏时，可以用于正式版本下载。
- 在计算机串口和2509CONSLOE 口相连的同时，还必须准备一个AUI 与RJ45的转换接口，以便可以使用交叉线将AUI口与计算机网口相连。
- 在引导监控模式下，进入特权模式，配置以太口的接口地址和掩码，使其与计算机网口地址在同一子网，（假定计算机地址位168.1.32.206 255.255.0.0 路由器以太口地址位168.1.32.207 255.255.0.0 ）。

```
router(boot)#config t
```

```
router(boot)(config)#int ethernet 0
```

```
router(boot)(config-if)#ip address 168.1.32.207 255.255.0.0
```

2500系列路由器版本灾难性恢复

- 验证网络互通性。

```
router(boot)#ping 168.1.32.206
```

- 计算机上启动tftp服务器，将需要下载的版本放在服务器的指定目录下。
- 在超级终端上执行如下命令。

```
router(boot)#copy tftp flash
```

- 将新的版本下载到路由器的flash中。
- 重新启动路由器，运行新的正常版本。

```
router(boot)#reload
```

2600系列路由器密码恢复

- (1) 将路由器的CONSOLE口和计算机串口相连，启动计算机超级终端，开启路由器电源，在开机60秒内按快捷键“ctrl+break”使路由器进入rom monitor 状态，提示符rommon1>

2600系列路由器密码恢复

(2) 重新配置组态寄存器

- rommon1>confreg
- 当出现 do you wish to change the configuration (y/n) 时选择y
- 接下来的选项选择n
- 当出现 enable "ignore system configuration information" (y/n) 选择y
- 接下来的选项选择n

2600系列路由器密码恢复

- (3) 重新启动路由器

rommon1>reset

- (4) 启动后进入特权模式，执行如下命令使原来的配置信息有效。

router(config)#config mem

- (5) 可以进一步查看密码或更改密码

2600系列路由器灾难性恢复

- 一般此系列路由器提供了两种灾难性恢复版本的方法，tftpdnld 和 xmodem 方式。

tftpdnld方式

- (1) 将计算机串口和路由器CONSLE口相连，将计算机网口与路由器以太网口相连。
- (2) 启动TFTP服务器，并将要下载的版本放于指定目录下面。
- (3) 开启路由器电源，由于没有有效版本，路由器启动后将直接进入监控模式。

Rommon1>

tftpdnld方式

(4)按如下命令设置参数。

```
Rommon2>IP_ADDRESS=168.1.32.207
```

```
Rommon3>IP_SUBNET_MASK=255.255.0.0
```

```
Rommon4>DEFAULT_GATEWAY=168.1.32.206
```

```
Rommon5>TFTP_FILE=c2600-i-mz.121-3.T
```

```
Rommon6>tftpdnld
```

以上假定计算机地址为168.1.32.206 255.255.0.0，命令
IP_ADDRESS=168.1.32.207

在监控模式下将168.1.32.207地址配置到路由器的第一个以太网口，从而建立起路由器与TFTP服务器之间的连接，正常下载版本。

tftpdnld方式

(5) 组态配置寄存器

Rommon7>confreg

当出现do you wish to change the configuration ?y/n
选择y

其它选择n

当出现 change the boot charaterist ?y/n 选择 y

选择参数2

(6) 启动版本

Rommon8> reset

xmodem 方式下载

- 该种方式下载不需要以太网口电缆，只需超级终端即可。缺点是花费时间太多，速度太慢。Xmodem 是个人计算机通信中广泛使用的异步文件传输协议，以128字节块的形式传输数据，并且每个块都进行校验，如果接受对方校验正确，则发送认可信息，发送方发送下一个字块。Ymodem 异步传输协议，传输字块大小为1024，增加了批处理的功能。

xmodem 方式下载

(1) 用超级终端与路由器连接好后，启动路由器，路由器进入监控模式状态。

Rommon1>

(2) 启动执行xmodem 命令。

Rommon2>xmodem -cx ? 敲入“enter”键
当出现do you wish to continous 时选择y。

xmodem 方式下载

(3) 打开超级终端的“传送”菜单，选择传送文件则打开了传送文件窗口。

输入版本文件的位置，并选择xmodem 方式，确认后，经过几秒后，版本文件则会以xmodem的方式从计算机下载到路由器中。

修改相应命令和选项，也可以以ymodem的方式进行传送。

(4) 以上述同样的方法配置confreg 命令，重新启动后，路由器会进入正常状态。

3600系列路由器密码恢复

- 3600系列路由器的密码恢复和2600系列路由器基本相似，都是进入监控模式，执行confreg命令，启动时忽略配置文件，进行直接启动。此方法同样适用于4500,7500和12000系列路由器。

3600系列路由器版本恢复

- 3600的版本恢复没有提供tftpdnld命令，只提供了xmodem 命令，使用方法与2600系列相同。

四种进入ROM状态的方法

- 对于cisco的各种路由器进入rom状态的方法不尽相同，但一般通过如下两种方法可以进入rom状态，在使用过程中可以分别试用进入。
- 如果break 未被屏蔽，可以在开机60秒内按快捷键“ctrl+break”中断启动过程，进入rom状态。
- 如果break键已经屏蔽，可以通过循环开机的方法进入rom状态。
- 方法是：路由器开机后，将电源关闭。间隔5秒后重新开机，一般会进入rom状态。此方法适用与7500 12000等路由器

四种进入ROM状态的方法

- 将超级终端通讯波特率设置为1200，数据位8，奇偶位1 停止位无。开启路由器电源，启动后，关机。停5秒后，重新开机，同时一直按住空格键12秒后放开，等路由器启动完成后，重新更改超级终端位默认值。通讯波特率设置为9600，数据位8，奇偶位1 停止位无。重新连接后，从终端上可以看到已经进入rom状态。注意在波特率位1200时终端上没有内容显示。此方法适用于2500，2600，4500等系列路由器。