



CCNA 640-802

课程讲义



课程内容

第一部分 基础知识

第一章 **OSI**模型简介

第二章 认识路由器

第三章 无线局域网

第四章 路由器基本操作

第五章 **IP**网络规划



第二部分 路由协议

第一章 路由原理

第二章 静态路由

第三章 动态路由 - **RIP**

第四章 动态路由 - **IGRP**

第五章 动态路由 - **EIGRP**

第六章 动态路由 - **OSPF**

第七章 访问控制列表

第八章 故障排除方法

课程内容

第三部分	交换原理
第一章	以太网交换
第二章	交换机基础配置
第三章	生成树
第四章	虚拟局域网

第五部分	附录
附录一	术语表
附录二	CCNA考试简介

第四部分	广域网
第一章	广域网技术
第二章	PPP
第三章	ISDN与DDR
第四章	Frame Relay
第五章	NAT



第一部分 基础知识

第一章 OSI模型简介

第二章 认识路由器

第三章 无线局域网

第四章 路由器基本操作

第五章 IP网络规划

第一章 OSI模型简介

本章主要介绍OSI七层模型和TCP/IP模型。

参加该课程的学员应具备本章的基础，此处不作详述，可参见其他网络基础教材。



第二章 认识路由器

从大家熟悉的PC入手：

如果要使一台计算机正常工作，需要的硬件和软件包括？各部件的作用？

硬件

CPU

Mainboard

MEM

Display

Monitor

NIC

HDD

Mouse

Keyboard

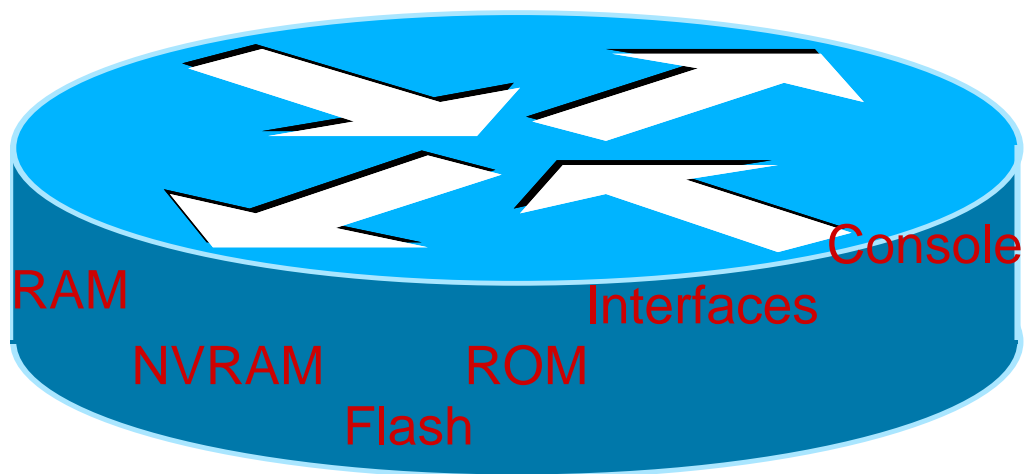
软件

OS



第二章 认识路由器

广域网路由器，是一种特殊类型的计算机。

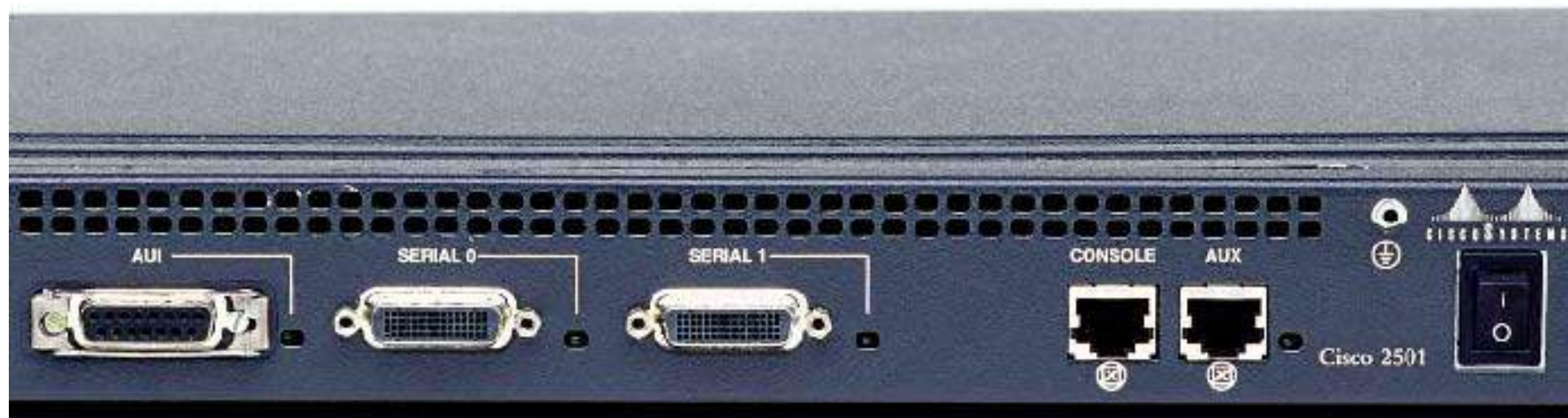


第二章 认识路由器



Cisco 2500系列路由器前视图

第二章 认识路由器



AUI接口 (Ethernet口)

串口

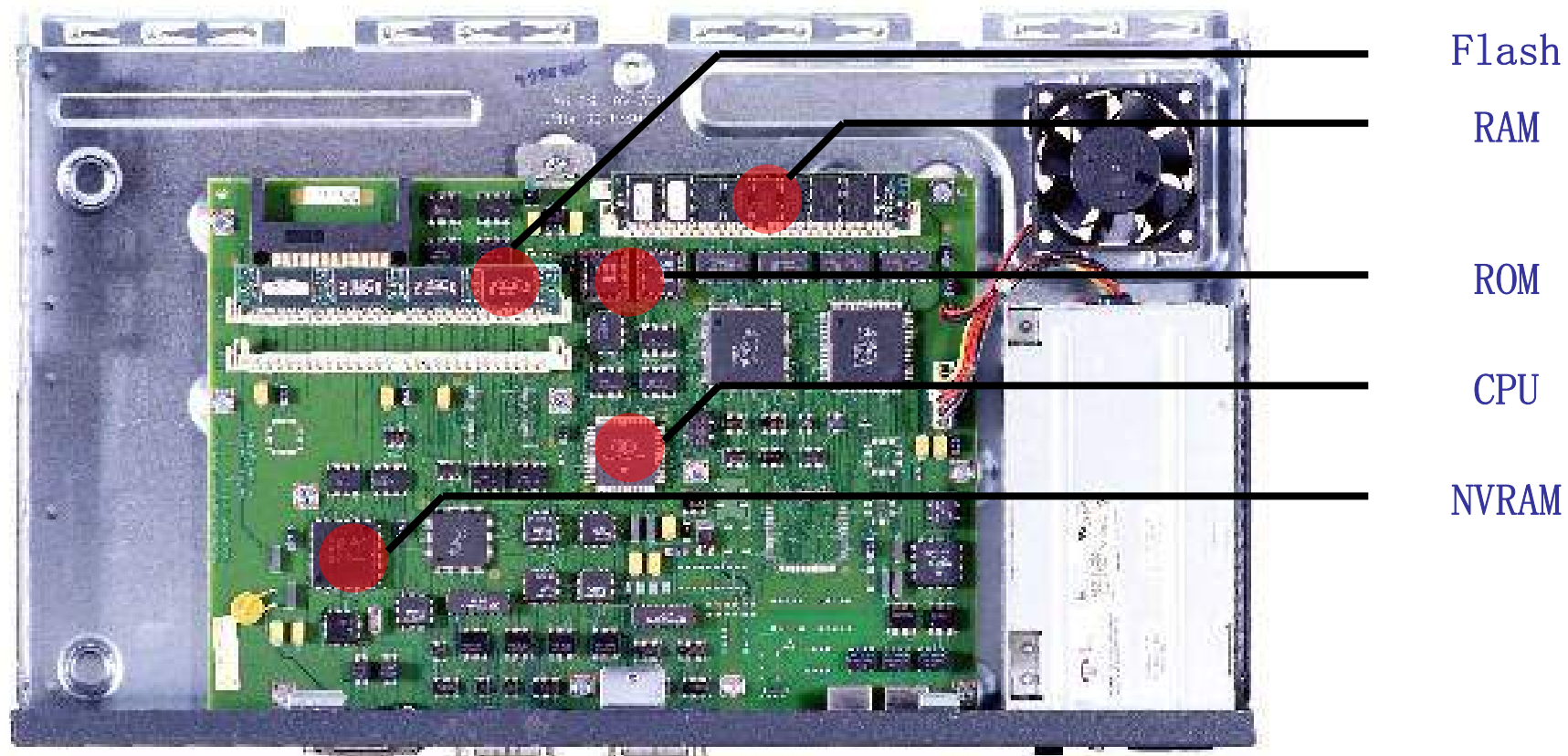
控制口 辅助口

电源开关



后视图

第二章 认识路由器



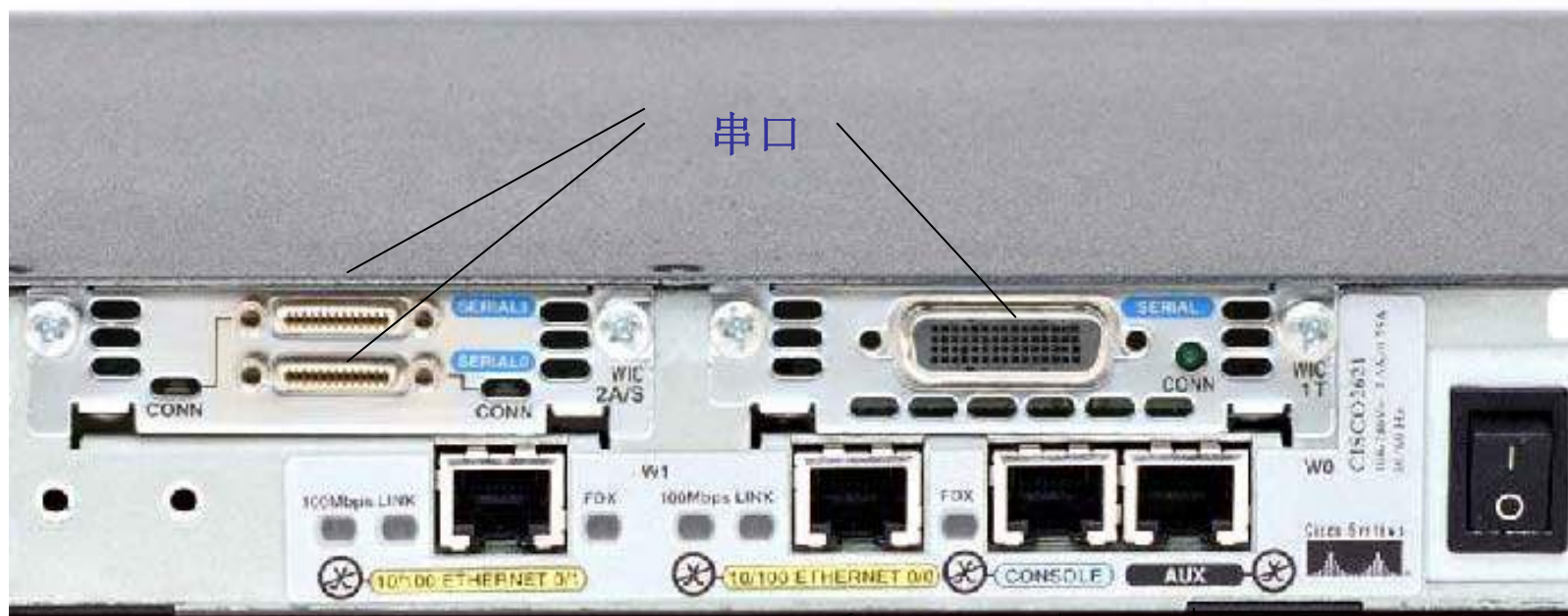
内视图

第二章 认识路由器



Cisco 2600系列路由器前视图

第二章 认识路由器



串口

10/100M快速以太网口

控制口 辅助口



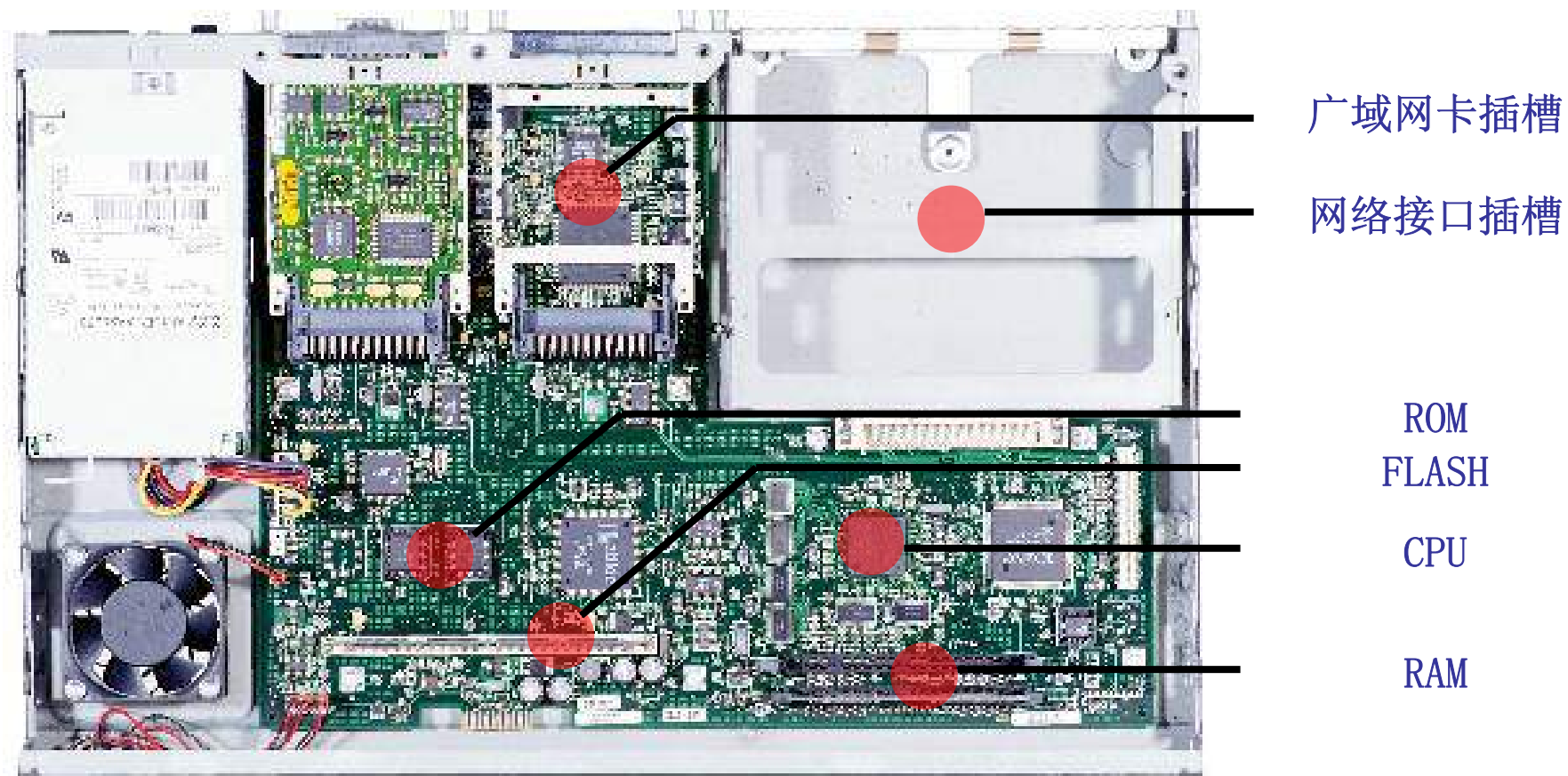
后视图

第二章 认识路由器



扩展卡

第二章 认识路由器



内视图

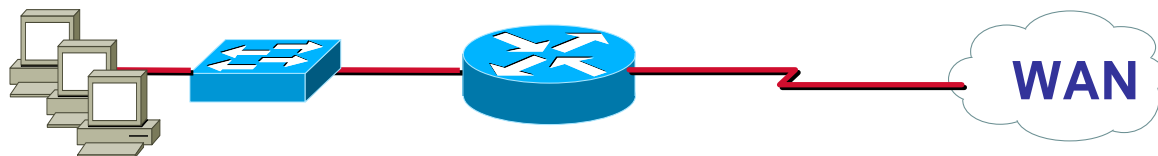
第二章 认识路由器

- 1、Interfaces** 外部可见的各类接口，如串口（Serial）、以太网（Ethernet）、快速以太网（FastEthernet）等
- 2、CPU** 不同于PC机上常用的Intel与AMD两大厂家的产品
- 3、RAM** 与PC所用内存功能类似，用于存放临时运行文件
- 4、NVRAM** 非易失性RAM，固化在主板上
和RAM不同，掉电后内容不会丢失，用于存放启动配置文件，供路由器启动后加载
- 5、FLASH** 主要用于存放操作系统IOS
- 6、ROM** 固化在主板上，存放一个小型的操作系统

第二章 认识路由器

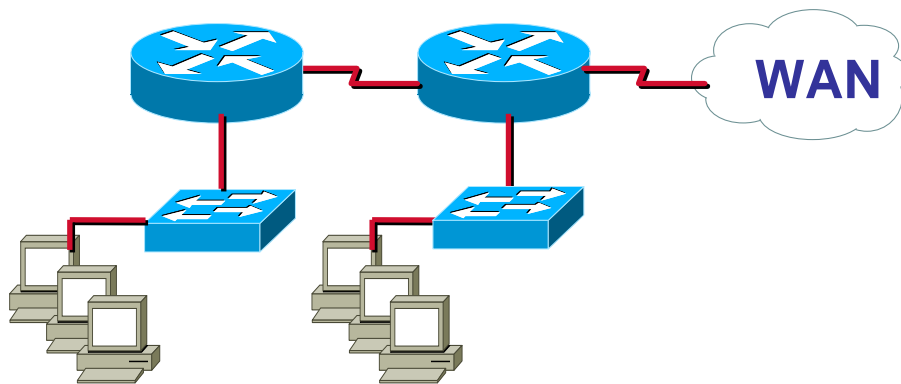
按路由器的接口可否更换划分，可分为固定配置（Fixed）和模块化（Module）两大类，在设计网络时，要考虑到网络的可扩展性，选择合适的设备。

如一个小型的网络，可采用如下的网络拓朴和设备。



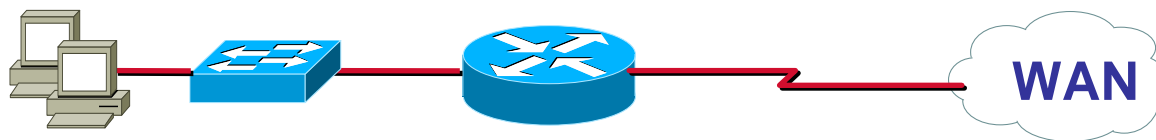
但考虑到网络的扩展，如规模扩大，机器设备数量增多的情况，如果在上图的基础上进行扩展，则可能的网络拓朴如下：

该图中，为分隔网络，增加了一台路由器和交换机

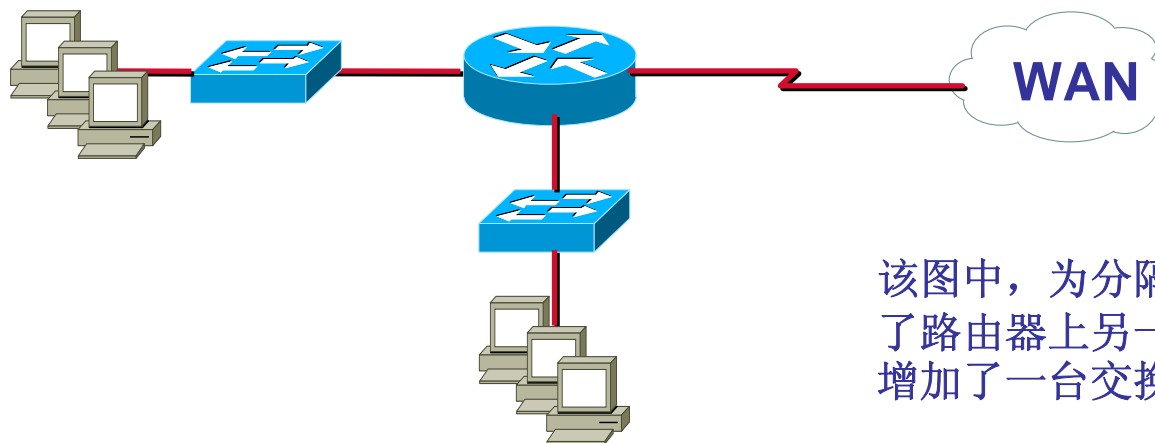


第二章 认识路由器

而如果初始时采用模块化路由器，则初始时：



网络需要扩展时：



该图中，为分隔网络，启用了路由器上另一个以太网口，增加了一台交换机

仅需要增加或更换相应的模块，便于网络的扩展，保护投资。

第二章 认识路由器



串口线



第二章 认识路由器



串口线



第二章 认识路由器

DTE: Data Terminal Equipment, 数据终端设备, 指的是位于用户网络接口用户端的设备。数据终端设备通过数据通信设备（例如, 调制解调器）连接到一个数据网络上, 并且通常使用数据通信设备产生的时钟信号。数据终端设备包括计算机等。

DCE: Data Communication Equipment, 数据通信设备。它提供了到网络的一条物理连接、转发业务量, 并且提供了一个用于同步DCE设备和DTE设备之间数据传输的时钟信号, 如调制解调器。DCE为通信提供时钟信号。



通常情况下, 路由器端为DTE端。

查看路由器的接口线缆类型: Router>show controllers serial 0

需要在DCE端配置时钟频率: Router(config-if)#clock rate 56000

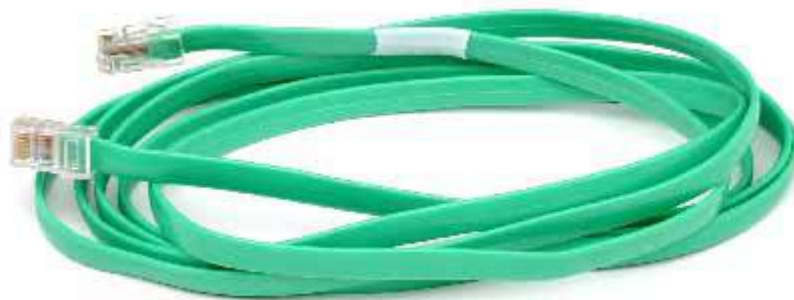
第二章 认识路由器



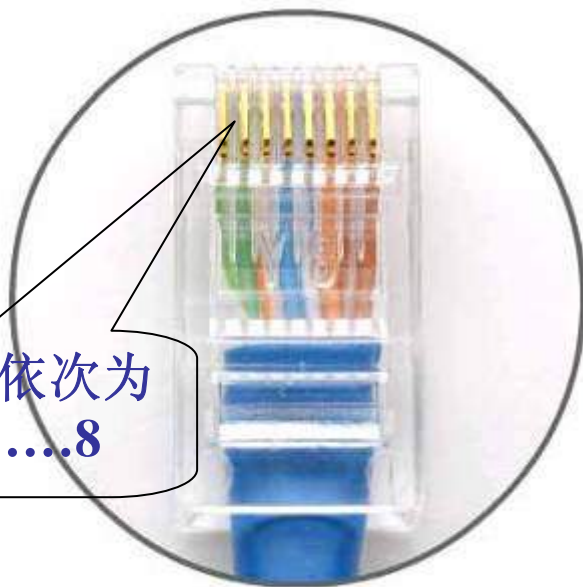
RJ45-DB9或DB25



控制线

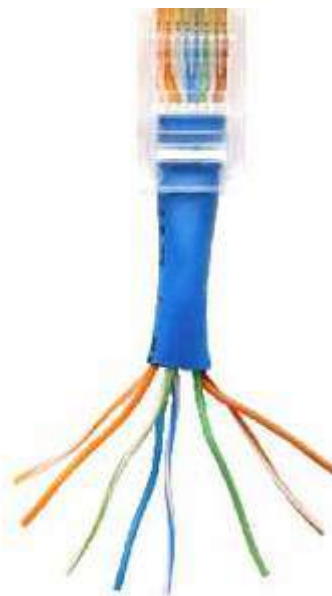


第二章 认识路由器



从左至右依次为
1、2、3.....8

双绞线



第二章 认识路由器

	1	2	3	4	5	6	7	8
568A	白 (绿)	绿	白 (橙)	兰	白 (兰)	橙	白 (棕)	棕
568B	白 (橙)	橙	白 (绿)	兰	白 (兰)	绿	白 (棕)	棕

直通线 (Straight-through) : 568B——568B

交叉线 (Cross-over) : 568A——568B

控制线 (Roll-over) : 两头线序相反

第二章 认识路由器

- 1、PC机的网卡和交换机连接使用何种双绞线？
- 2、两台PC机通过网卡连接起来，使用何种双绞线？
- 3、PC机的网卡和路由器的以太口使用何种双绞线连接？
- 4、交换机或集线器接口上标记的“X”是什么含义？
- 5、为什么有些交换机的接口上，只有接口编号，没有“X”标记？
- 6、交换机的“Uplink”口和其他普通接口有什么区别？
- 7、交换机的普通接口和另一台交换机的普通接口用何种双绞线连接？和Uplink口呢？

第二章 认识路由器

仍以PC机为例。

PC机的启动过程：

- 1、开机自检
- 2、加载操作系统，如开机的时候你可以选择进入Windows XP或者Windows 2003
- 3、加载配置，如注册表文件、启动项等

路由器的启动过程类似。

第二章 认识路由器

路由器的启动过程

- 1、POST (Power On Self Test) : 加电自检
- 2、执行ROM中的普通自举程序加载器 (Generic Boottrap Loader)
- 3、加载IOS (Internetwork Operating System)

IOS可以从下列位置加载: Flash、Tftp、ROM

IOS映像文件的来源, 是由配置寄存器 (Config Register) 的设置来确定的, 默认为0x2102, 表明路由器应查找配置文件中是否有boot system的命令。

如果没有, 则

首先, 从路由器自身的Flash中加载IOS,

如果没有, 则尝试从TFTP服务器中加载IOS,

如果不能, 则从路由器的ROM中加载IOS。

第二章 认识路由器

4、加载配置文件

如果成功加载IOS，路由器在NVRAM中寻找配置文件。

如果没有有效的配置文件，路由器将通过所有的活动接口通过广播的形式搜索TFTP服务器，如果仍然没有，则进入到Setup模式，以对话的形式进行配置。

第二章 认识路由器

- 1、路由器在POST后，先查看寄存器的值，这个值是一组4个十六进制的数字，而其中的最后的一位影响启动的过程。
- 2、在NVRAM的配置文件中查看boot system命令，这个命令告诉引导程序在哪里寻找IOS。
- 3、如果在NVRAM的配置文件中没有找到boot system命令，引导程序使用flash中所找到的第一个有效的IOS镜像。
- 4、如果flash中没有有效的IOS镜像，引导程序将生成一个TFTP本地广播以定位TFTP服务器。
- 5、如果没有找到TFTP服务器，引导程序将加载ROM中的MINI IOS（RXBOOT 模式）。
- 6、如果ROM中有MINI IOS，那么MINI IOS在随后加载并且进入RXBOOT模式；否则路由器不是重新试图寻找IOS镜像，就是加载ROMMON并且进入ROM Monitor模式。

第三章 无线局域网

传统有线网络由于受设计或环境条件的制约，在物理、逻辑和资金方面普遍存在着一系列问题，特别是当涉及到网络移动和重新布局时。

无线局域网的出现使有线网络所遇到的问题迎刃而解，它可以使用户任意对有线网络进行扩展和延伸，只需在有线网络的基础上通过接入点设备AP（Access Point）、无线网卡、网络桥接器和天线等无线设备使无线通信得以实现。在不进行传统布线的同时，提供有线局域网的所有功能，并能够随着用户的需要随意的更改扩展网络，实现移动应用。

下列情形可能需要无线局域网：

无固定工作场所的使用者；

有线局域网络架设受环境限制；

作为有线局域网络的备用系统；

热点地区。



第三章 无线局域网

无线局域网主要标准

1、802.11（波段是2.4GHz）

最高2Mbps，传输距离100米，用于传送数据

2、802.11b（波段是2.4GHz）

最高5.5和11Mbps，传输距离100~300米，用于传送数据、图像

3、802.11a（波段是5GHz，与其它标准不兼容且成本太高）

最高54Mbps，传输距离5~10千米，用于传送数据、图像、语音

4、802.11g（波段是2.4GHz）

最高54Mbps，传输距离5~10千米，用于传送数据、图像、语音

第三章 无线局域网

802.11b是802.11标准的升级版本，它采用2.4-2.4835GHz频带和DSSS扩频方式。该标准可提供11Mbps的数据速率，大约是IEEE802.11标准无线LAN速度的5倍，还能够支持5.5Mbps和11Mbps两个新速率，而且802.11b实现了动态速率转换，可以在11Mbps、5.5Mbps、2Mbps、1Mbps的不同速率之间自动切换。802.11b使用不同的调制方式以实现不同的传输速率：传输速率为1Mbps时使用DBPSK（Differential Binary Phase Shift Keying）二进制差分移相键控，传输速率为2Mbps时使用DQPSK（Differential Quart Phase Shift Keying）四进制差分移相键控，传输速率为5.5/11Mbps时使用CCK（Complementary Code Keying）补码键控。

802.11b是目前使用最为广泛的一种无线局域网标准。

第三章 无线局域网

802.11a标准扩充了标准的物理层，工作在5GHz U-NII(unlicensed national information infrastructure)频带，采用正交频分复用（OFDM）的调制技术，传输速率为6Mbps-54Mbps，物理层速率可达54Mb/s，传输层可达25Mbps，支持速率为6、9、12、18、24、36、48、54Mbps。传输距离较802.11b短，与802.11b、802.11不兼容。

802.11g标准使用了802.11a标准相同的调制技术OFDM，因此能达到54Mbps的传输速率。802.11g标准也使用2.4GHz频带，可以兼容现有的802.11b标准。

第三章 无线局域网

	802.11	802.11b	802.11a	802.11g
频带范围	2.4 GHz	2.4 GHz	5 GHz	2.4GHz
数据速率	1-2 Mbps	11 Mbps	54 Mbps	54 Mbps
调制方式	跳频扩频	正交序列扩频	直接序列扩频	正交序列扩频
适用范围	数据	数据、图象	语音、数据、图象	语音、数据、图象

第三章 无线局域网

无线局域网的优点

- 1、建设速度快
- 2、安装灵活方便，可“现用现装”
- 3、节约建设投资（预埋电缆常常投入使用时已经落后）
- 4、维护成本低（明线的维护困难且费用高）
- 5、安全性好（明线容易发生故障，易受雷击、火灾等影响）
- 6、适用范围：不便布线场所；频繁变更办公场人员；多局域间的连接

第三章 无线局域网

Access Point，又叫无线接入点，是有线局域网络与无线局域网络的桥梁，装有无线网卡的PC可通过AP互联，或通过AP去分享有线局域网络甚至广域网络的资源除此之外，AP本身还有许多其它的附加功能，如通过MAC地址限制接入的终端，简单的防火墙功能等。

无线网卡，与传统的以太网的差别在于它是通过无线电波传输数据，而后者则是通过一般的网线来传送。

无线局域网天线，与一般电视，手机所用之天线不同，其原因是因为频率不同所致，WLAN所用的频率为较高2.4GHz之频段

第三章 无线局域网

WLAN距离与速率的关系

两台无线设备相互靠近,它们将以两个接口所支持的最高速率通信。但是,如果以最高传输速率通信,传输距离可能小于以较低速率传输的距离。这就是WLAN接口要提供自动选择速率机制的原因。

无线接口总是以尽可能高的速率进行传输,如果以某速率传输失败,无线网卡将以相同的速率重新“传输丢失的报文”,如果第二次也传输失败了,无线接口将自动切换至另一较低的速率。

第三章 无线局域网

Wireless-LAN组成

1、对等模式无线网络

无线网卡+无线网卡

2、基本模式无线网络

无线网卡+无线Access Point (无线HUB; 无线路由)

第三章 无线局域网

在跳频扩频技术FHSS (Frequency-Hopping Spread Spectrum) 中, 将整个信道分为很多个子信道, 发射与接收两端以特定形式的窄频电波来传送信号, 收发两端传送资料经过一段极短的时间后, 便同时切换到另一个频段。由于不断的切换频段, 因此较能减少在一个特定频道受到干扰, 也不容易被窃听。FCC规定使用75个以上的跳频信号, 且跳频至下一个频率的最大时间间隔为400ms, 即每秒跳频2.5次。

802.11中将最大时间间隔定为250ms, 也就是每秒跳4次, 将83.5mhz (2483.5-2400) 分为79个频道, 每个频道大约1mhz。

为避免信号受到干扰采用FSK (Frequency Shift Keying频移键控) 技术, 使进行无线通讯的设备同步且同时地选择某个特定频道, 并且每隔一段时间就跳到另一个频道继续联系。

第三章 无线局域网

直接序列扩频技术 (Direct Sequence Spread Spectrum) 是将原来的记号[1]或者[0]，利用10个以上的chips来代表[1]或[0]位，使得原来较高功率，较窄频率变成具有较宽频的低功率频率。而每个bit使用多少个chips称作Spreading Ratio，一个较高的Spreading Ratio可以增加抗噪声干扰，而一个较低Spreading Ratio可以增加用户的人数。

基本上，在DSSS的Spreading Ratio是相当少的。例如在几乎所有2.4GHz的无线局域网络产品所使用的Spreading Ratio皆少于20。而在IEEE802.11的标准内，其Spreading Ratio是11。IEEE802.11b采用这种扩频方式。

第三章 无线局域网

正交频分复用（Orthogonal Frequency Division Multiplexing）是一种多载波数字调制技术，具有频谱利用率高、抗多径干扰等特点。OFDM系统能够有效地抵抗无线信道带来的影响，例如信道的频率选择性衰落、脉冲噪声和共信道干扰的影响。其主要思想是：将信道分成许多正交子信道，在每个子信道上进行窄带调制和传输，这样减少了子信道之间的相互干扰。

第三章 无线局域网

第一代WLAN安全依靠唯一的SSID和MAC进行认证。

SSID是一个1-32个字符的ASCII字符串，它会输入到客户端和AP中。在802.11中，任何具有空SSID的客户可以连接到任何AP上，而不管AP的SSID。IEEE标准要求广播SSID，SSID广播选项允许发送信标帧广播SSID。

基于MAC的认证在802.11规范中定义。某些厂商在AP上支持一个合法的MAC地址列表，某些厂商允许AP在一个集中服务器上查询MAC地址。

第三章 无线局域网

IEEE 802.11标准使用WEP来保护WLAN。

IEEE 802.11标准指定一个静态40位密钥，可以导出并在别处使用。当使用WEP时，无线客户端和AP必须拥有一对匹配的WEP密钥。WEP使用RC4（Rivest Cipher 4）加密算法。

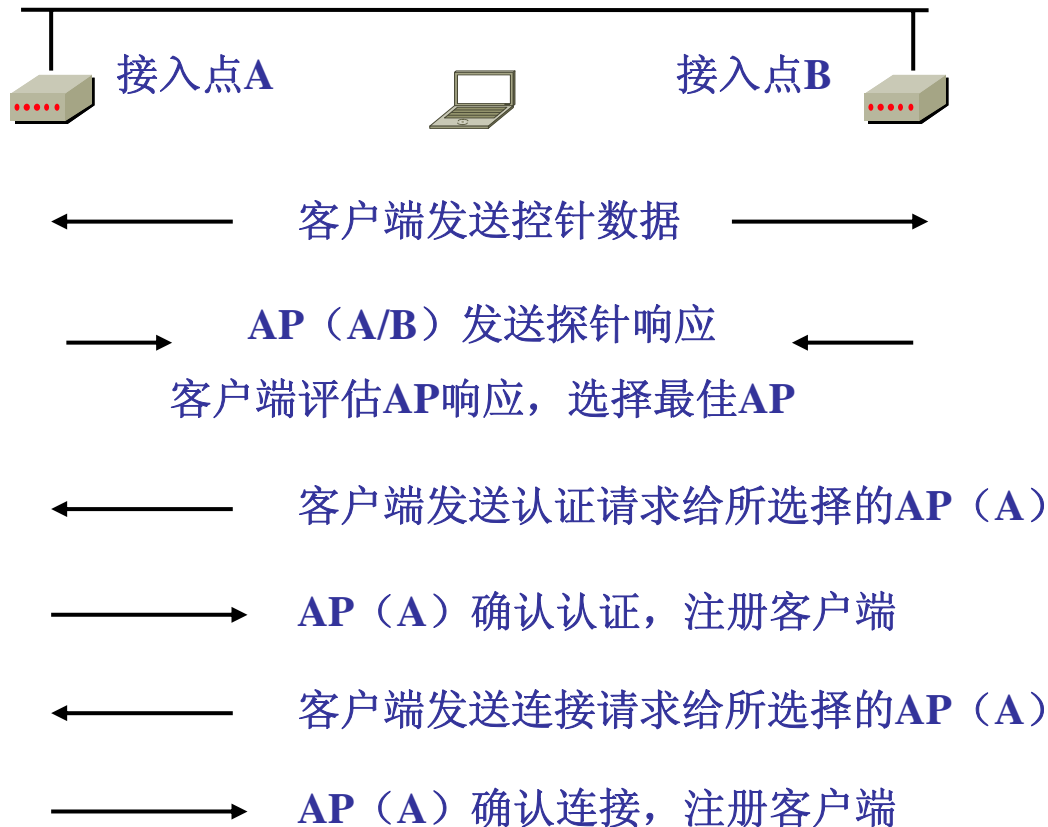
IEEE 802.11标准提供了两种机制定义用于WLAN的WEP密钥。

在第一种机制中，无线子系统中的所有设备，包括客户端和AP，最多共享4个默认密钥。一个客户端获得默认密钥后，它可以与其他所有的设备进行通信。当密钥被广泛分发后，安全性会降低。

第二种机制中，每个客户端和另外一台无线设备建立密钥映射关系。这种方式比较安全，因为拥有密钥的设备较少，但分发这个唯一的密钥会随着无线设备的增多而变得困难。

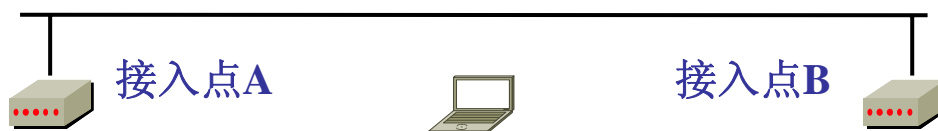
第三章 无线局域网

开放认证



第三章 无线局域网

共享密钥认证



← 客户端发送控针数据 →

→ AP (A/B) 发送探针响应 ←

客户端评估AP响应，选择最佳AP

← 客户端发送认证请求给所选择的AP (A)

→ AP (A) 使用包含未加密的Challenge文本响应认证

← 客户端使用WEP密钥加密Challenge文本，并发送给AP (A)

→ AP (A) 将未加密的Challenge文本与加密的Challenge文本进行比较，如果相同，则允许客户端连接进入WLAN

第三章 无线局域网

WEP的局限性

认证：

- ☆认证是基于设备的，而不是基于用户的

- ☆客户端不对网络认证

- ☆现有的认证数据库不能负载分担

密钥管理：

- ☆密钥长度不变

- ☆设备和AP共享密钥

- ☆如果一个适配器或设备被盗，所有设备和AP的密钥都必须重置

基于RC4的WEP密钥：

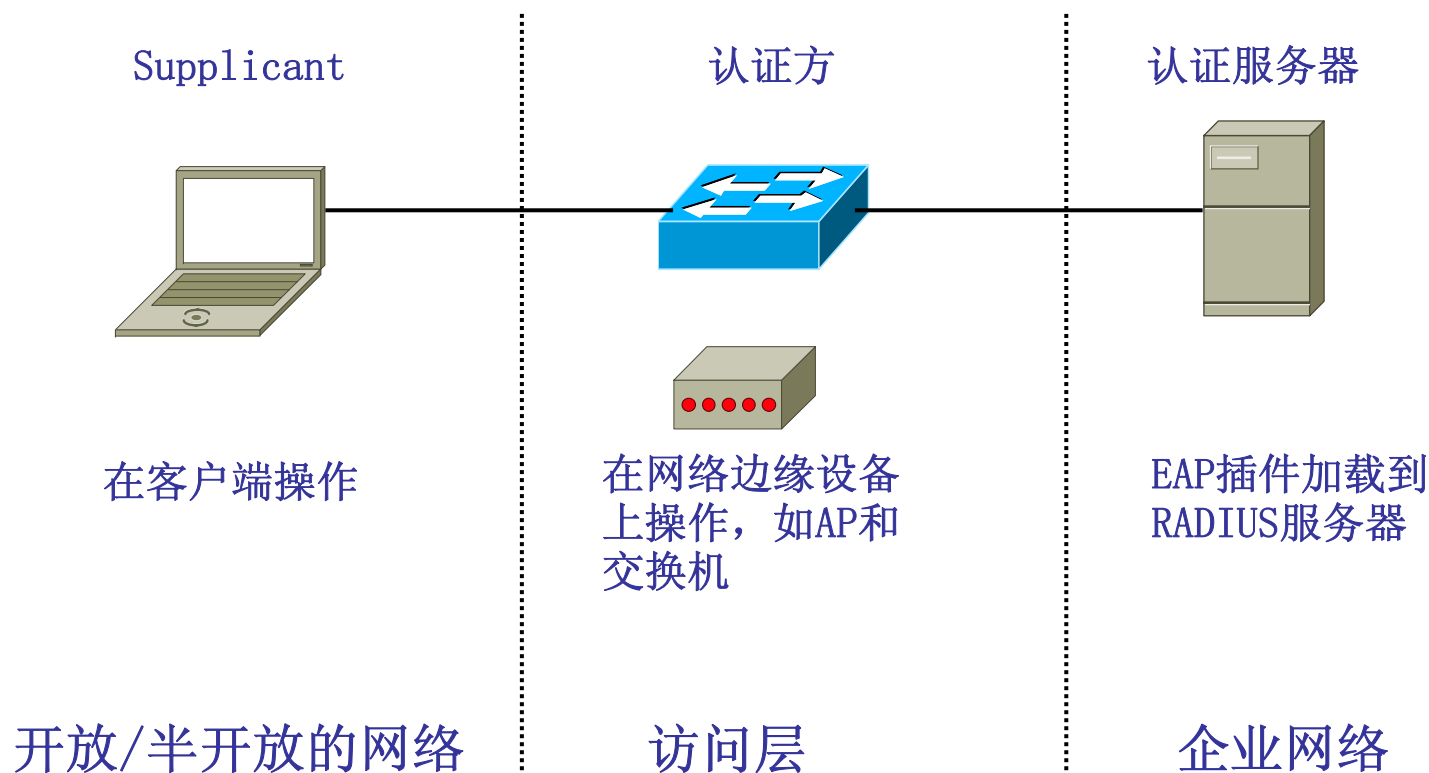
- ☆加密算法容易受到攻击

- ☆消息的完整性不能得到保证

第三章 无线局域网

WPA允许通过IEEE 802.1x协议对用户认证，它可以控制有线和无线局域网的入口，提供相互认证，网络和用户可以互相证明其身份。

802.11x标准的要求在客户端、AP和认证服务器上都提供支持。



第三章 无线局域网

- 1、客户端关联到AP后，Supplicant询问登录用户名和密码，开始EAP over LAN (EAPOL)
- 2、客户端响应用户名和密码
- 3、通过802.1x和EAP，Supplicant将用户名和密码单向哈希值发送给AP
- 4、AP封装请求，并将它发送给RADIUS服务器
- 5、RADIUS服务器根据数据库检查用户名和密码，决定用户是否有权访问网络
- 6、如果客户端认证通过，RADIUS服务器发送访问询问给AP，然后转发给客户端
- 7、客户端通过AP将访问询问的EAP响应发送给RADIUS服务器

第三章 无线局域网

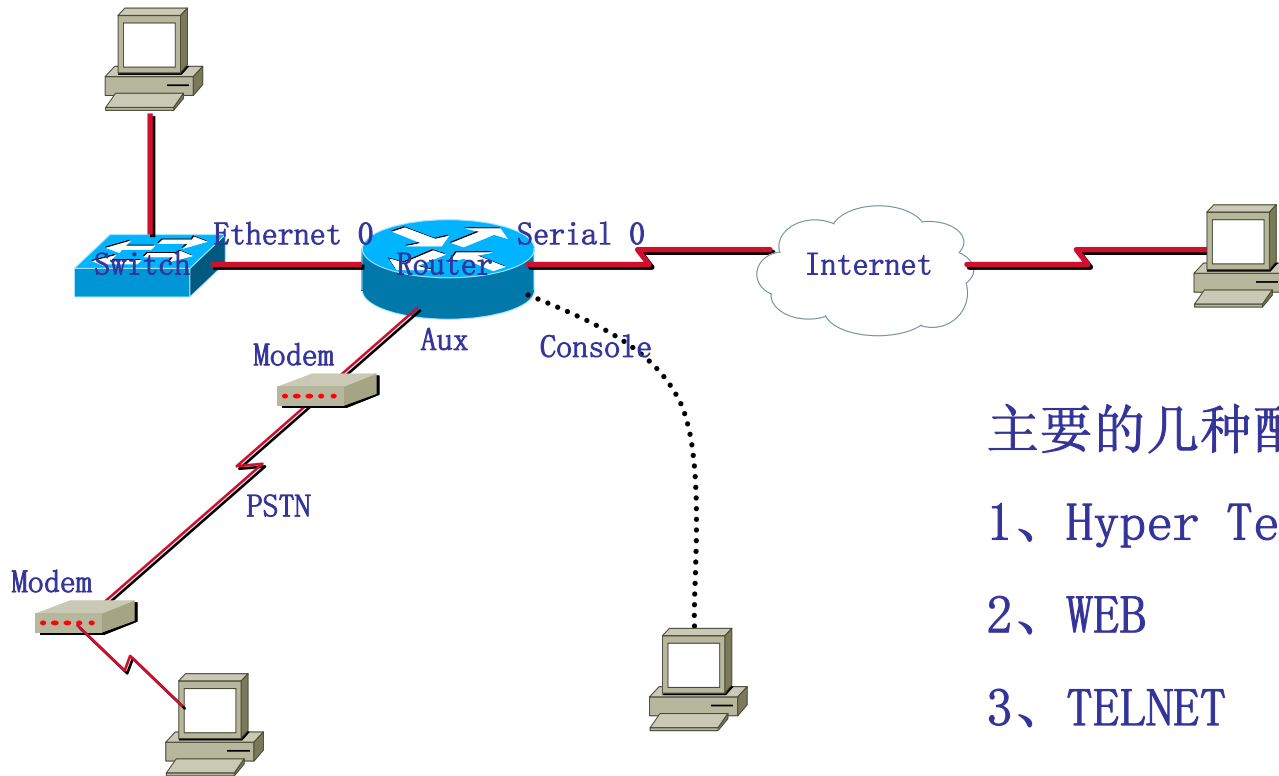
- 8、如果客户端发送的响应正确，RADIUS服务器将接入成功消息和会话WEK密钥（无线网络上的EAP）通过AP发送给客户端。同样的会话WEK密钥也会发送给AP
- 9、客户端和AP使用会话WEK密钥进行通信。组播的WEK密钥由AP直接发送给客户端。它使用会话WEK密钥加密
- 10、客户端退出后，AP回到初始状态，仅允许802.1x数据通过

第三章 无线局域网

	LEAP	EAP-TLS	EAP-PEAP
服务器认证	密码	证书/PKI	证书/PKI
客户端认证	密码	证书/PKI	密码1
单点登录	是	是	否2
密码攻击弱点	否3	否	否
OTP/LDAP支持	否	N/A	是
附加架构	否	是/CA	是/CA

- 1、不是局限于密码机制，但现在可以使用密码
- 2、微软自己的Supplicant与EAP-MS-CHAPv2支持SSO
- 3、要求使用强密码（密钥长度超过64位）

第四章 路由器基本操作



主要的几种配置方式

- 1、Hyper Terminal
- 2、WEB
- 3、TELNET
- 4、Dial

第四章 路由器基本操作

CLI (Command Line Interface) ， 命令行界面，可在用户提示符下键入可执行指令的界面。

Cisco设备的配置是通过命令的输入和执行来完成的，如：

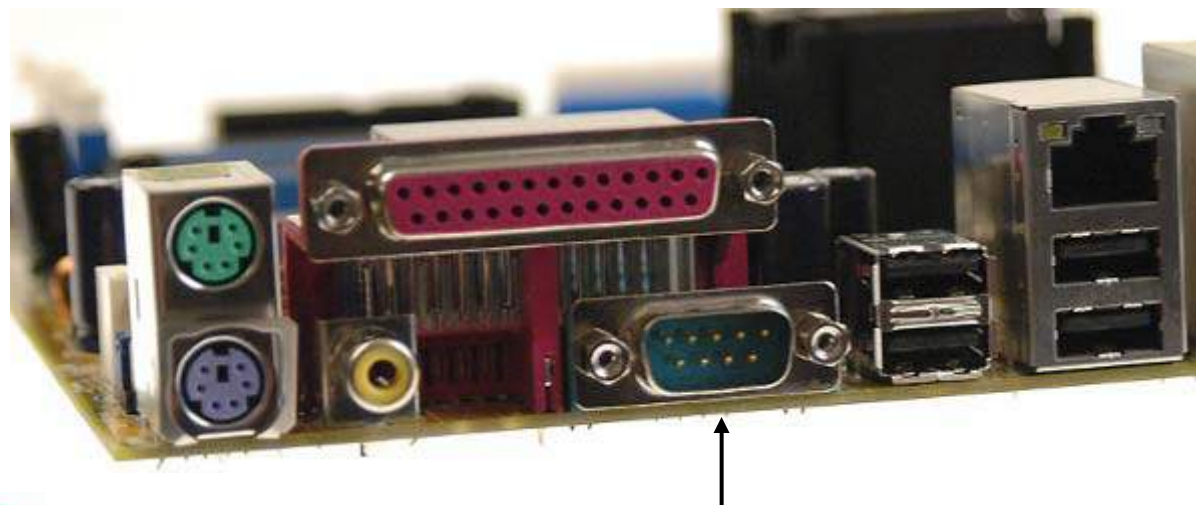
```
Router#show running-config
```

...

和CLI形式相对应的是GUI (Graphic User Interface) ， 图形用户界面。

第四章 路由器基本操作

控制台连接



Com



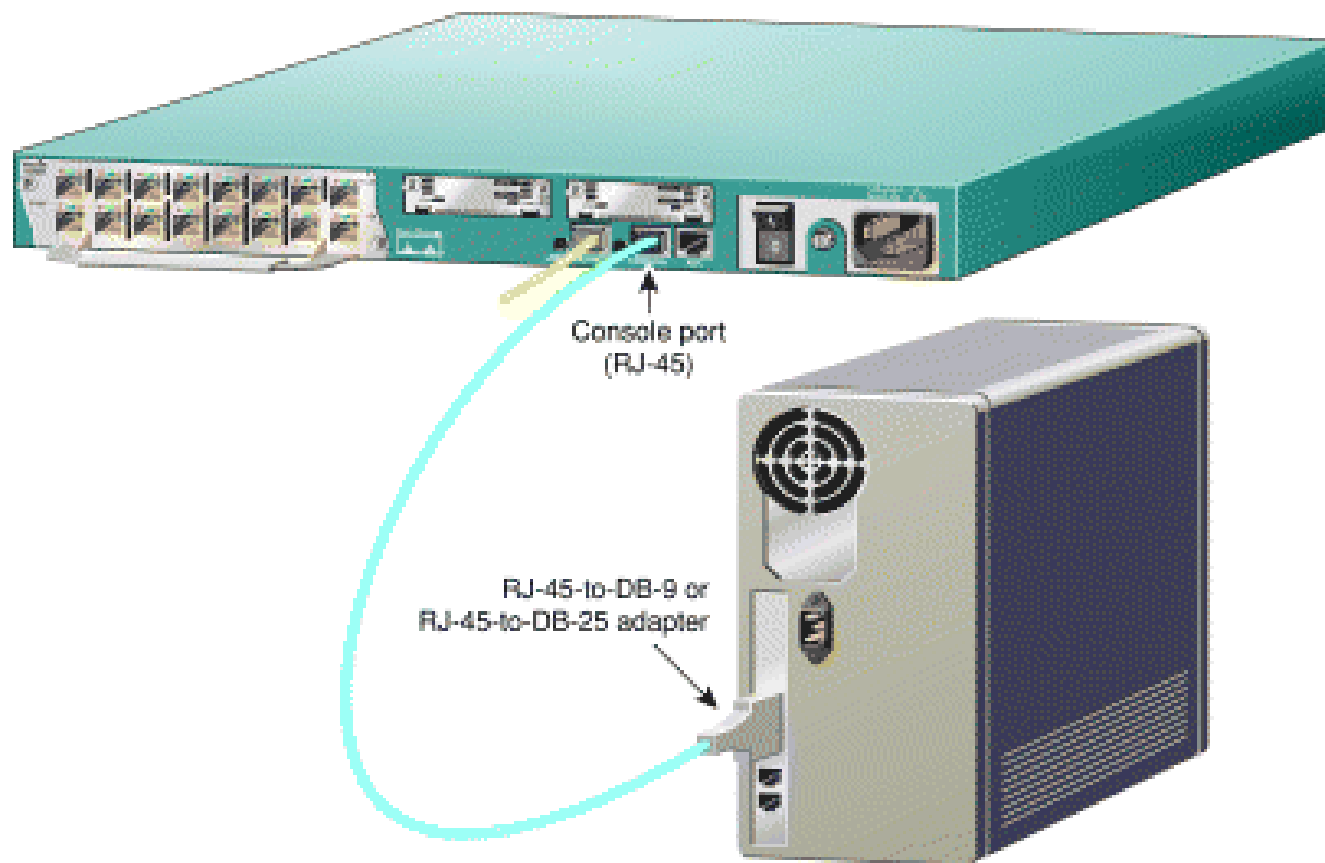
10/100BASE-T
Ethernet 0/0
(RJ-45)

Console
port (RJ-45)

Auxiliary port
(RJ-45)

第四章 路由器基本操作

控制台连接



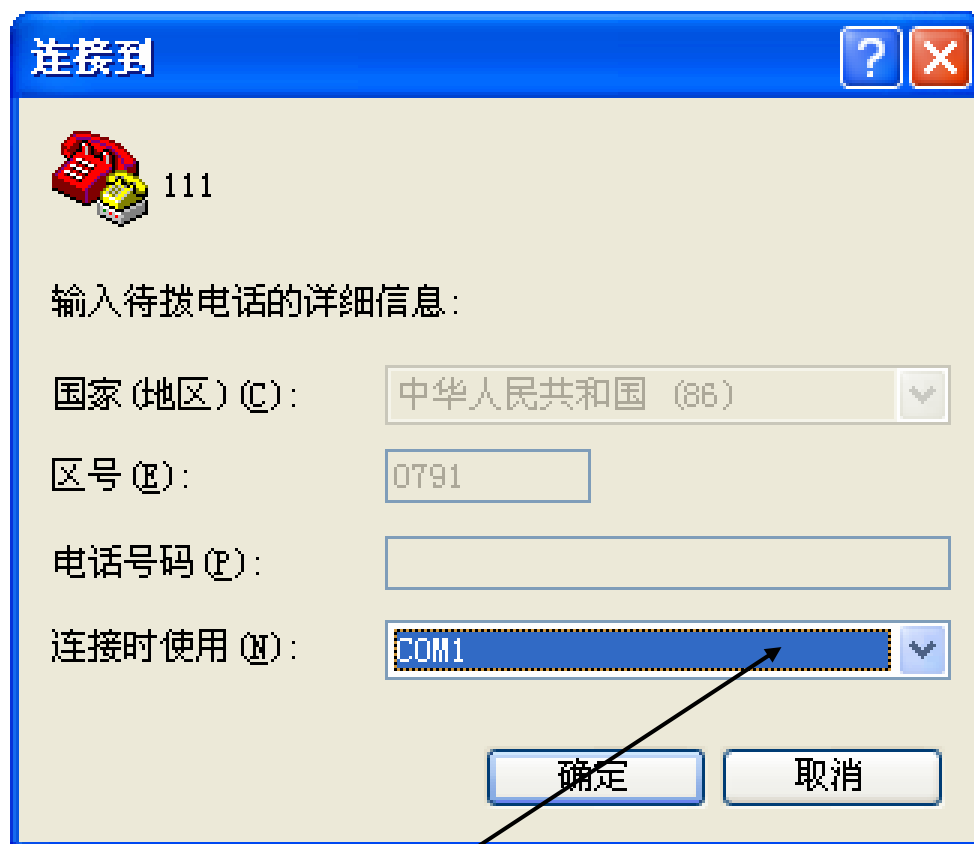
第四章 路由器基本操作

使用超级终端配置路由器：

开始→程序→附件→通讯→超级终端



第四章 路由器基本操作



通过下拉菜单选择相应的端口，如COM1

第四章 路由器基本操作



通过下拉菜单修改各项参数，然后点击确定

或直接点击“还原为默认值”，然后点击确定



第四章 路由器基本操作

路由器的启动

同样的，类似常用的PC机，自检→定位操作系统（光驱？软驱？USB？硬盘？）→加载操作系统（XP？Linux？）→加载配置文件（用户？桌面？）

Power on self test (POST)

Load and run bootstrap code

Find the IOS software

Load the IOS software

Find the configuration

Load the configuration

Run

第四章 路由器基本操作

Setup模式

如果设备之前没有被配置过，或者配置文件被删除，或者配置文件被忽略（未加载），该设备将进入Setup模式，通过对话的方式进行基本配置。

--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog?

[yes/no]:y

...

在设置过程中可以随时键入“？”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。

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 '[]'.

第四章 路由器基本操作

接下来，会让你进行主机名、密码、接口等相关设置。在配置完成的最后将出现如下选项：

- [0] Go to the IOS command prompt without saving this config.
- [1] Return back to the setup without saving this config.
- [2] Save this configuration to nvram and exit.

Enter your selection [2]:

第四章 路由器基本操作

Router>

基本操作模式

操作提示符

主机名

用户模式 > User Mode

特权模式 # Privileged Mode

类似于Windows操作系统下，可以把用户分为Guest、User、Administrator等，不同用户有不同的权限。

在路由的用户模式下没有更改路由器配置的权限。

第四章 路由器基本操作

router> 用户模式
路由器处于用户命令状态，这时用户可以查看路由器的连接状态，访问其它网络和主机，但不能查看和更改路由器的设置。

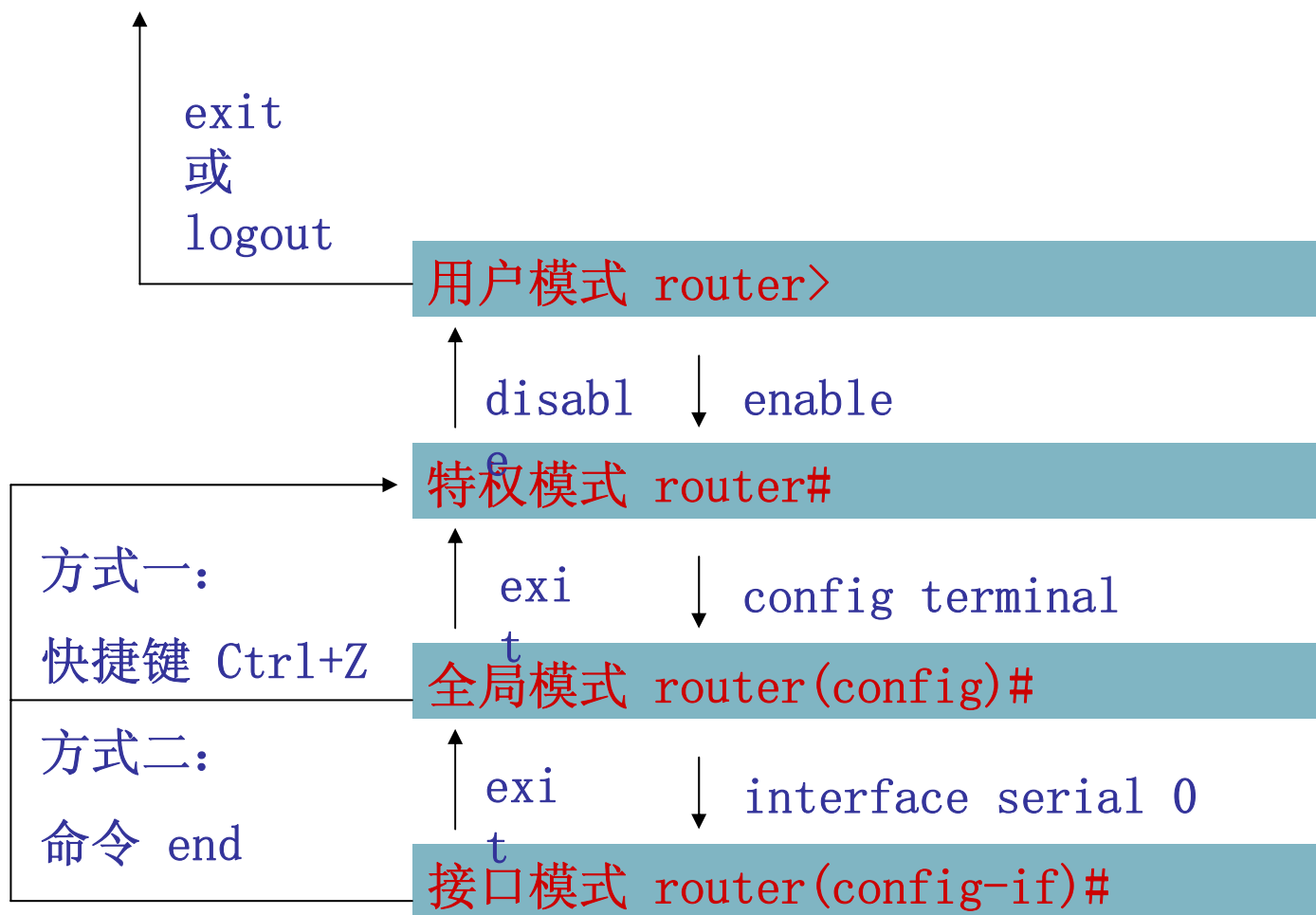
router# 特权模式
路由器处于特权命令状态，这时不但可以执行所有的用户命令，还可以看到和更改路由器的设置。

router(config)# 全局配置模式
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。

其他

router(config-if)# 接口配置模式
router(config-router)# 路由协议配置模式
.....

第四章 路由器基本操作



第四章 路由器基本操作

Router>?

在任何模式下，直接输入? 将列出在当前模式下可运行的所有命令及参数。

Exec commands:

access-enable Create a temporary Access-List entry

access-profile Apply user-profile to interface

...

ping Send echo messages

ppp Start IETF Point-to-Point Protocol (PPP)

resume Resume an active network connection

--More--

当页面下方出现“--More--”提示符时，输入空格将显示下一屏，输入回车将显示下一行，其他键结束。

第四章 路由器基本操作

实验任务：修改路由器的时间。

既然是要对路由器进行修改，就需要相应的权限，要进入到特权模式下进行配置。如果不知道用什么命令，最直接的方法就是用问号。

Router#?

Exec commands:

access-enable Create a temporary Access-List entry

...

clear Reset functions

clock Manage the system clock

configure Enter configuration mode

...

注意到命令列表中有一个clock，
通过后面的解释，初步判断也许
可以用来配置系统时间

第四章 路由器基本操作

Router#clock

% Incomplete command.

Router#clock ?

set Set the time and date

直接输入clock，得到一个错误提示：命令未完成，表明需要继续输入相应的参数。

在clock后面跟上问号，得到提示：需要跟上set参数。

Router#clock set ?

hh:mm:ss Current Time

Router#clock set 18:04:34 ?

<1-31> Day of the month

MONTH Month of the year

继续使用问号，得到时间格式为小时、分、秒，中间用冒号隔开，并需要配置日期和月。

第四章 路由器基本操作

```
Router#clock set 18:04:34 16 3
```

```
% Invalid input detected at '^' marker.
```

将数字3改为英文的“march”，并继续使用问号，最终完成命令。

假设当前日期是3月16日，当输入数字3的时候，得到了一个错误提示“^（向上的小箭头）”。这个符号表明这条命令从箭头所指处错误，之前的命令字符都是正确的。

```
Router#clock set 18:04:34 16 march ?
```

```
<1993-2035> Year
```

```
Router#clock set 18:04:34 16 march 2007
```

```
Router#show clock
```

配置完成后，查看配置结果，将显示新的时间。

第四章 路由器基本操作

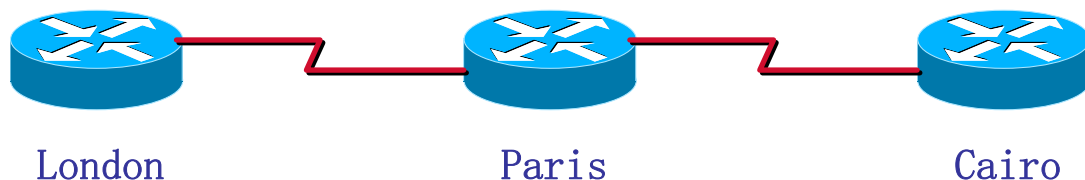
修改路由器名称

默认情况下，Cisco路由器的名称为Router，为便于管理，给路由器配置名称。

语法格式：Router(config)#hostname name

在全局模式下，用hostname命令指定，后面跟相应的名称，如

Router(config)#hostname london



第四章 路由器基本操作

配置串口

在配置串口前，首先需要查看该接口的类型是DTE还是DCE。如果为DCE端，需配置时钟频率（ClockRate）。

查看该接口所连接的线缆类型：

```
Router#show controllers serial 0
```

将会看到三种结果：no cable、dte或dce。

在DCE端如下配置：

```
Router(config)#interface serial 0
```

```
Router(config-if)#clockrate 64000
```

```
Router(config-if)#no shutdown
```

第四章 路由器基本操作

配置以太网口

```
Router(config)#interface ethernet 0
```

```
Router(config-if)#ip address 10.0.0.1 255.0.0.0
```

```
Router(config-if)#no shutdown
```

如配置错误，可在相应模式下用新配置语句覆盖旧配置语句，或用no语句取消原配置，如

```
Router(config-if)#no ip address
```

配置接口描述（Description）

```
Shanghai(config-if)#description connect to Beijing
```



第四章 路由器基本操作

配置域名解析

如果输入错误的命令或名称，如

```
Router#enabel
```

将出现如下错误提示

```
Translating "enabel"...domain server (255.255.255.255)
```

```
% Unknown command or computer name, or unable to find  
computer address
```

由于路由器不识别该命令，就会认为enabel是网络中的某个主机的名称，将通过其活动接口以广播的形式查找网络中的域名服务器，试图解析出“enabel”这个设备的IP地址。

关闭域名服务

```
Router(config)#no ip domain-lookup
```

第四章 路由器基本操作

Router#show version

Cisco Internetwork Operating System Software

IOS (tm) 2500 Software (C2500-I-L), Version 12.1(7), RELEASE SOFTWARE (fc1)

...

Router uptime is 3 hours, 30 minutes

System returned to ROM by power-on

...

System image file is "flash:c2500-i-l.121-7.bin"

...

cisco 2500 (68030) processor (revision F) with 16384K/2048K bytes of memory.

...

1 Ethernet/IEEE 802.3 interface(s)

2 Serial network interface(s)

32K bytes of non-volatile configuration memory.

16384K bytes of processor board System flash (Read ONLY)

Configuration register is 0x2102

show version

显示路由器的软硬件信息

第四章 路由器基本操作

router#show running-config

查看路由器当前运行配置，存放于RAM中

router#show startup-config

查看路由器启动配置，存放于NVRAM中

router#copy running-config startup-config

保存配置

router#write erase

删除配置

第四章 路由器基本操作

常用快捷键

Tab: 自动完成命令的剩余部分

↑ ↓: 重复上一条或下一条历史命令。
路由器或交换机等在缓存中保存有历史命令，默认保存10条，最大256条，但缓存过大会影响路由器的性能。

修改历史命令大小

```
Router#terminal history size 256
```

查看

```
Router#show terminal
```

```
...
```

```
History is enabled, history size is 256.
```

```
...
```

```
Router#show history
```

第四章 路由器基本操作

通过Web方式配置路由器。

- 1、建立物理连接；
- 2、建立网络连接；
- 3、启用路由器的Http服务，语法：

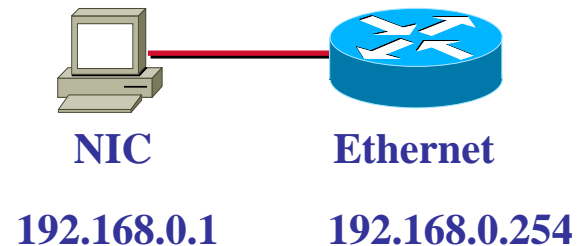
```
Router(config)#ip http server
```

- 4、配置登录用户名和密码，语法：

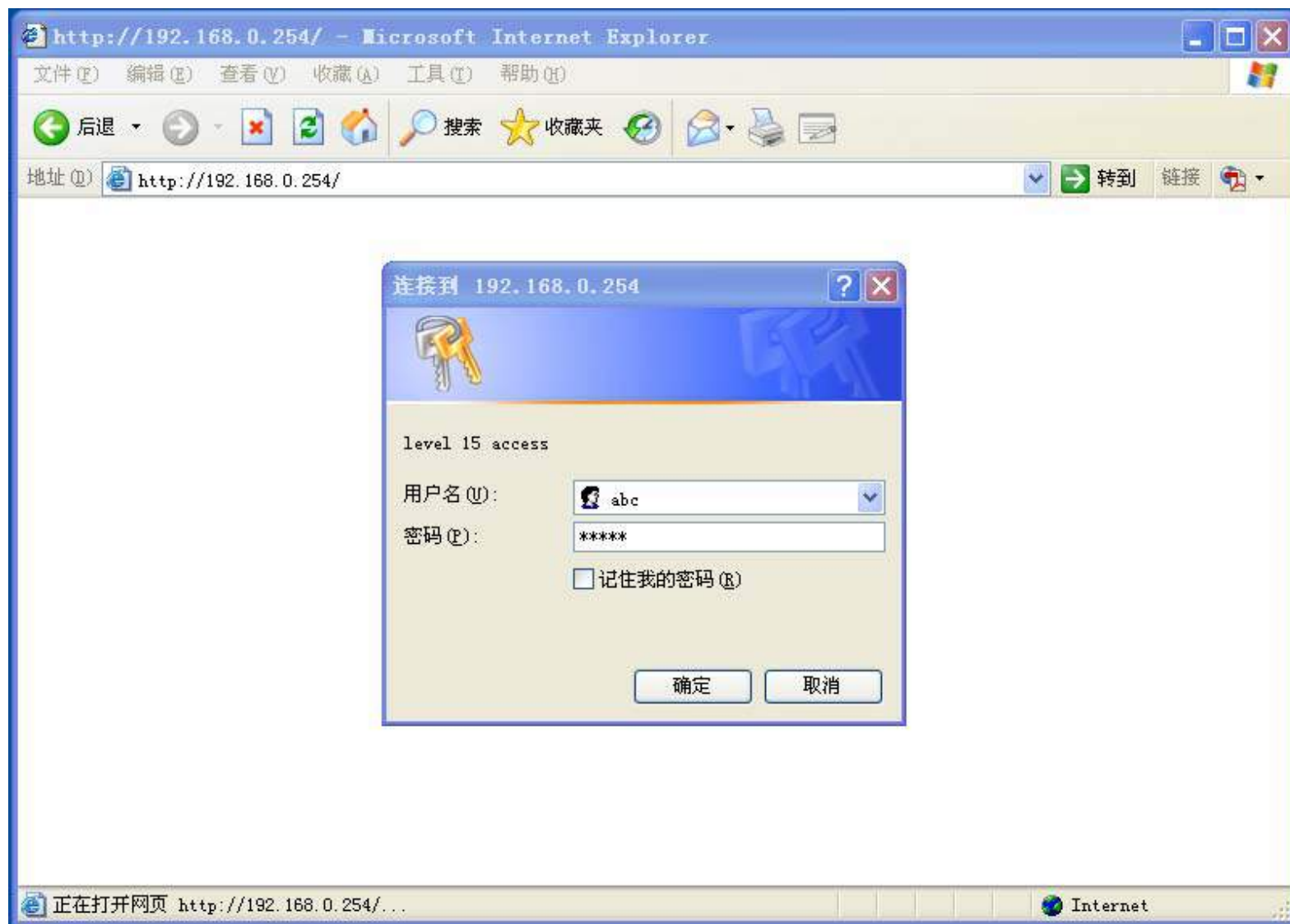
```
Router(config)#username name password password
```

```
Router(config)#username abc password cisco
```

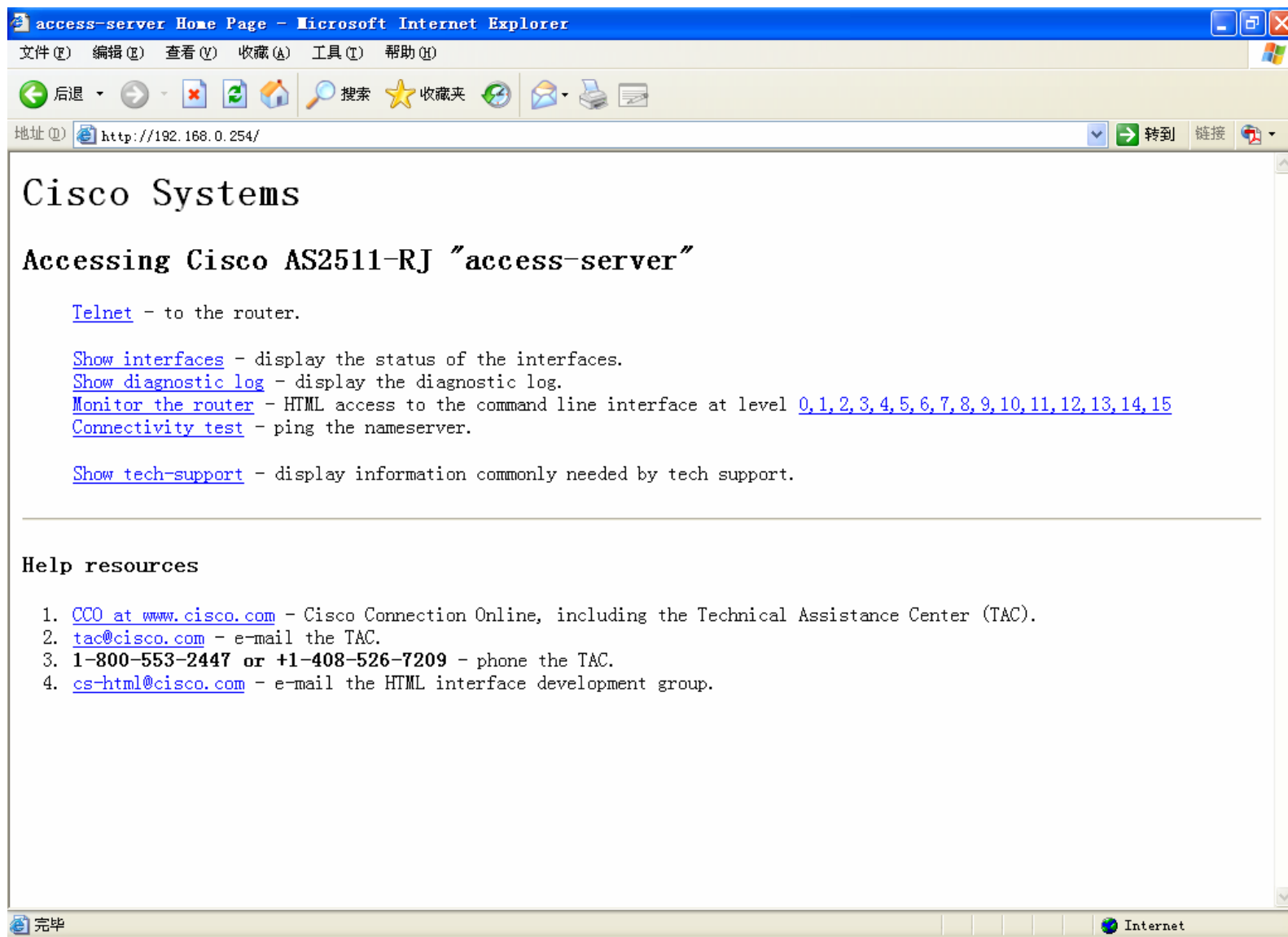
- 5、打开浏览器，输入路由器的地址。



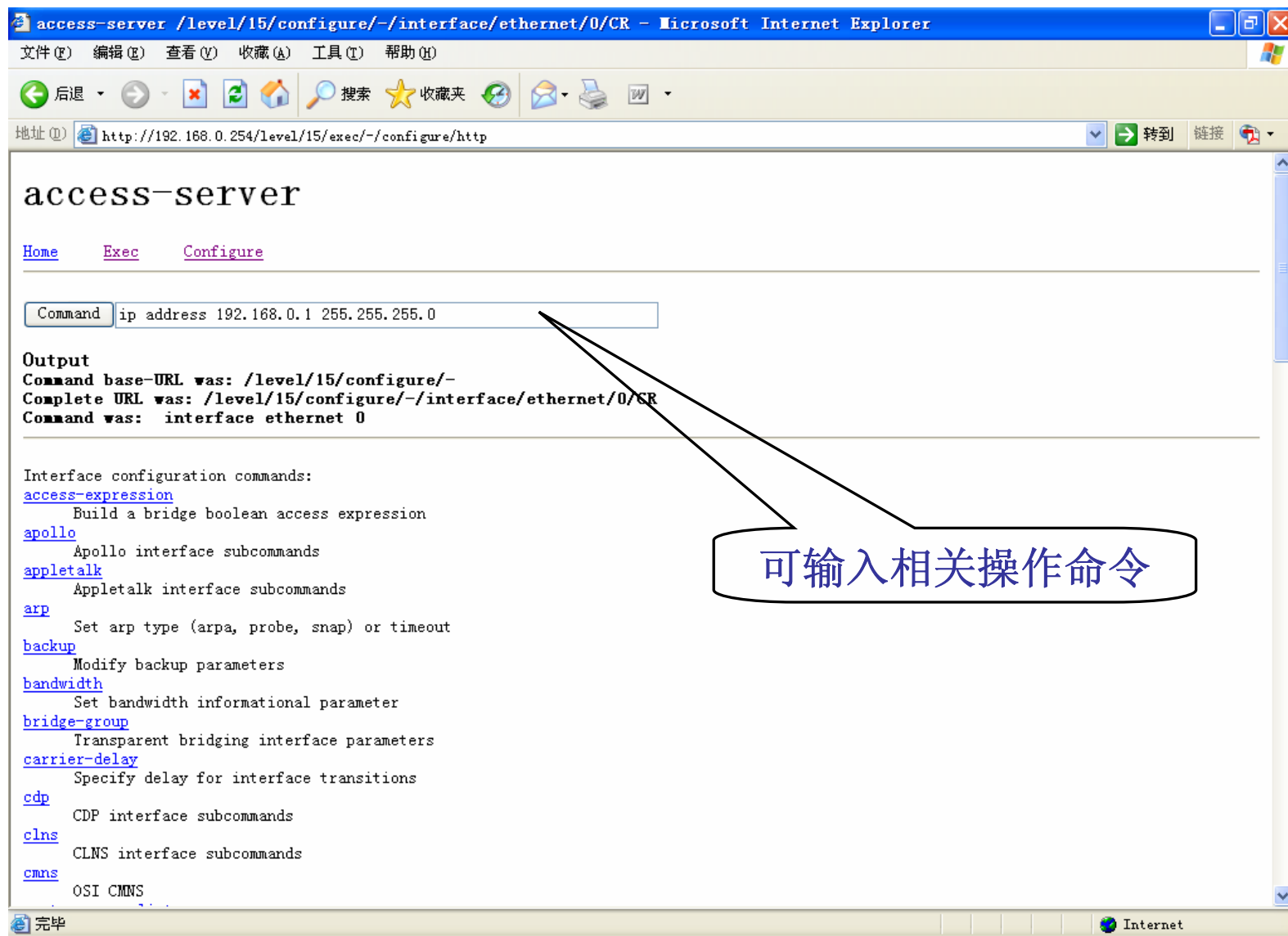
第四章 路由器基本操作



第四章 路由器基本操作



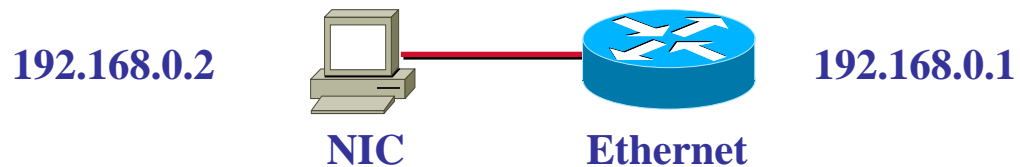
第四章 路由器基本操作



第四章 路由器基本操作

通过Telnet配置路由器

在PC机上发起Telnet，进入DOS窗口：`telnet 192.168.0.1`



第四章 路由器基本操作



发起Telnet，可在用户及特权两种模式下：

Router#telnet ip address 或 name

如：RA>telnet 10.0.0.2

为便于管理，可配置IP地址与设备名称的映射。

语法，在全局模式下：

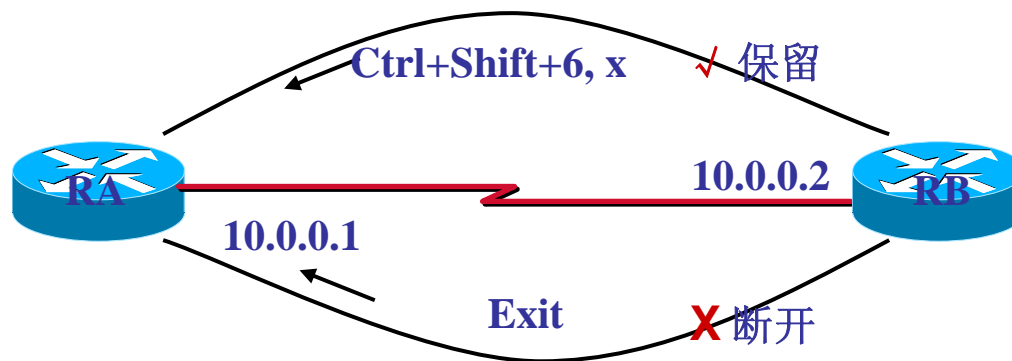
Router(config)#ip host name ip address

如：RA(config)#ip host sale 10.0.0.2

配置成功后，可用主机名替代IP地址。

RA>telnet sale

第四章 路由器基本操作



返回：从RA发起Telnet登录到RB后，返回RA时可有两种方式：

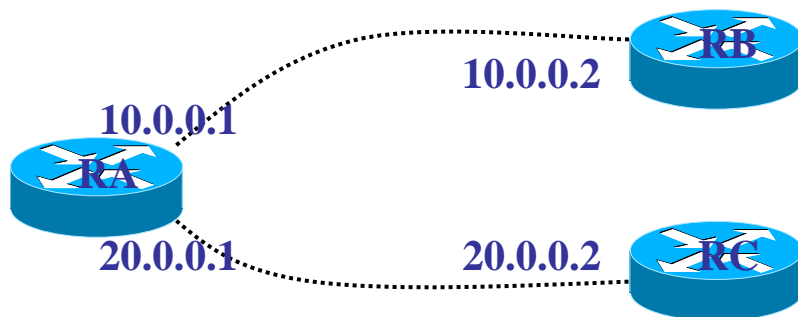
1、结束会话并返回

在远程系统（RB）上输入exit，将断开此次Telnet会话并返回RA。

2、保持会话并返回

在远程系统（RB）上通过键组合：ctrl+shift+6, x。Ctrl与Shift与6三个键同时按下，然后按X，将保持此会话并返回RA。

第四章 路由器基本操作



查看、恢复及断开会话

若从RA已分别发起Telnet至RB与RC，则

1、查看会话

RA#show sessions

Conn	Host	Address	Byte	Idle	Conn Name
1	RB	10.0.0.2	0	0	RB
* 2	RC	20.0.0.2	0	0	RC

看到两个会话，前面有编号，其中带有*号的是当前连接。

第四章 路由器基本操作

2、恢复会话

RA#resume 1

将恢复第1条会话，即恢复到RB的会话

若直接回车，将恢复带有*号的某个会话，此处将恢复到RC的会话。

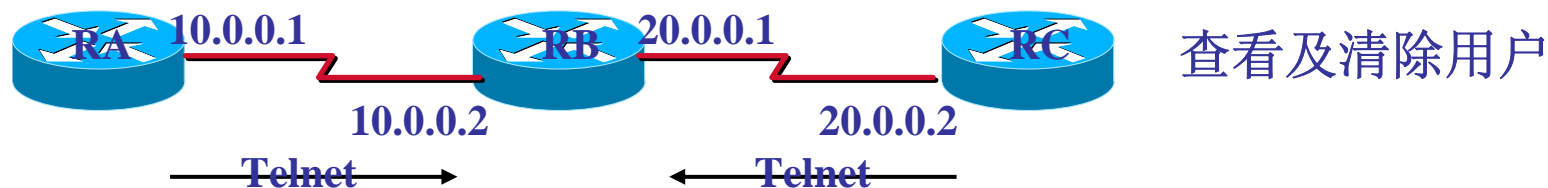
3、断开会话

RA#disconnect 2

将断开第2条会话，即断开到RC的会话

继续查看会话，发现只剩下编号为1的会话。

第四章 路由器基本操作



若从RA、RC分别发起到RB的Telnet会话，则在RB上

1、查看用户

```
RB#show users
```

Line	User	Host(s)	Idle	Location	
4	tty 4	incoming	00:10:43	RA	查看到两个访问用户， 分别来自 RA 和 RC ，编 号为 4 和 16 。
16	tty 16	incoming	00:10:46	RC	

2、清除用户

```
RB#clear line 16
```

清除编号为16的连接，即断开来自RC的telnet访问
继续查看用户，会发现只剩下编号为4的用户。

第四章 路由器基本操作

管理密码的设置

```
router(config)#enable secret cisco  
router(config)#enable password cisco1
```

两个密码不能相同

密码配置完成后，退到用户模式下，输入enable后，分别用刚才配置的cisco1和cisco尝试。

认识两种密码的区别：

- 1、MD5/Clear text
- 2、权限及优先级别

第四章 路由器基本操作

控制口登录密码

```
router(config)#line console 0  
router(config-line)#login  
router(config-line)#password cisco
```

配置完成后，在特权模式下logout登出，再敲回车查看。

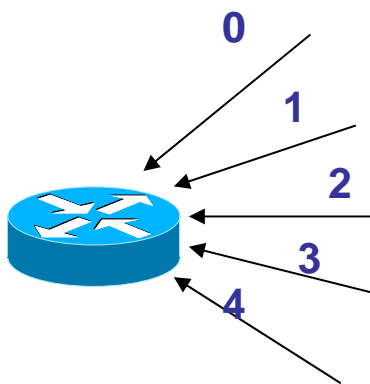
未授权的用户不能进入到路由器的用户模式。

第四章 路由器基本操作

远程登录密码

```
router(config)#line vty 0 4  
router(config-line)#login  
router(config-line)#password cisco
```

未授权的用户不能通过远程登录的方式对路由器进行操作。



第1个用户，占用编号为0的接口

第2个用户，占用编号为1的接口

第3个用户，占用编号为2的接口

第4个用户，占用编号为3的接口

第5个用户，占用编号为4的接口

第四章 路由器基本操作

默认情况下，路由器支持最多五个用户登录，编号从0到4。

可以给不同编号分配不同的密码，如：

```
router(config)#line vty 0  
router(config-line)#password cisco1
```

```
router(config)#line vty 1 2  
router(config-line)#password cisco2
```

```
router(config)#line vty 3 4  
router(config-line)#password cisco3
```

此时，第一个用户的登录密码为cisco1，第二三个用户的登录密码为cisco2，第四五个用户为cisco3。

第四章 路由器基本操作

如果配置如下，远程用户可否登录？

```
router(config)#line vty 0
router(config-line)#login
router(config-line)#no password

router(config)#line vty 1 4
router(config-line)#login
router(config-line)#password cisco
```


第四章 路由器基本操作

明文的加密

```
router(config)#service password-encryption
```

默认情况下，控制口、远程登录等密码均以明文的形式显示在配置文件中，通过这种方式对明文密码进行加密显示。

第四章 路由器基本操作

未加密, Router#show running-config

...

line con 0

password cisco

...

line vty 0 4

password cisco

加密后, Router#show running-config

...

line con 0

password 7 110A1016141D

...

line vty 0 4

password 7 01100F175804

第四章 路由器基本操作

常用寄存器值

0x102	 Ignores break 9600 console baud
0x1202	1200 baud rate
0x2101	Boots into bootstrap Ignores break Boots into ROM if initial boot fails 9600 console baud rate
0x2102	 Ignores break Boots into ROM if initial boot fails 9600 console baud rate default value for most platforms
0x2120	Boots into ROMmon 19200 console speed

第四章 路由器基本操作

0x2122	 Ignores break Boots into ROM if initial boot fails 19200 console baud rate
0x2124	 NetBoot Ignores break Boots into ROM if initial boot fails 19200 console speed
0x2142	 Ignores break Boots into ROM if initial boot fails 9600 console baud rate Ignores the contents of NonVolatile RAM(ignores configuration)

第四章 路由器基本操作

路由器密码恢复（2500系列）

1、reload或重新启动路由器

2、开机60S之内按“break” 或“ctrl+break”，中断启动过程

3、此时提示符为“>”（rom monitor模式），输入o/r 0x2142，修改寄存器值，使之启动时不加载配置

4、输入i（initialize），重新初始化路由器，即重启

5、路由器重启后将进入setup对话框

```
Would you like to enter the initial configuration dialog?  
[yes/no]: n
```

6、此时提示符为router>，输入enable进入特权模式

7、router#copy startup-config running-config，加载原配置

8、router#config terminal，进入全局模式

第四章 路由器基本操作

9、router(config)#enable secret cisco, 修改特权模式密码为cisco

10、router(config)#exit, 退到特权模式下

11、router#copy running-config startup-config, 保存新密码

此时密码已经被修改为cisco, 配置也已成功保存, 下一次路由器断电重启后能否正常工作?

第四章 路由器基本操作

12、router#show version, 最后一行显示寄存器值为0x2142, 需要修改为正常的0x2102, 否则路由器下次重启时仍然不加载配置文件, 将不能正常工作

13、router(config)#config-register 0x2102, 修改为正常值

14、router#show version, 查看最后一行, 显示如下:
Configuration register is 0x2142 (will be 0x2102 at next reload)

15、router#reload, 保存配置并重启路由器, 完成操作

第四章 路由器基本操作

路由器密码恢复（2600系列）

1、reload或重新启动路由器

2、开机60S之内按“break”键或“ctrl+break”，中断启动过程

3、此时提示符为“rommon1>”（rom monitor模式），输入confreg 0x2142，修改寄存器值，使之启动时不加载配置

4、在rommon2>后输入reset，重新启动路由器

5、路由器重启后将进入setup对话框

Would you like to enter the initial configuration dialog?
[yes/no]: n

6、此时提示符为router>，输入enable进入特权模式

7、router#copy startup-config running-config，加载配置

8、router#config terminal，进入全局模式

9、router(config)#enable secret cisco，修改特权模式密码为cisco

第四章 路由器基本操作

- 10、router(config)#config-register 0x2102, 修改为正常值
- 11、router#copy running-config startup-config, 保存新密码
- 12、router#show version, 查看最后一行, 显示如下:
Configuration register is 0x2142 (will be 0x2102 at next reload)
- 13、 router#reload, 保存配置并重启路由器, 完成操作

第四章 路由器基本操作

备份与恢复

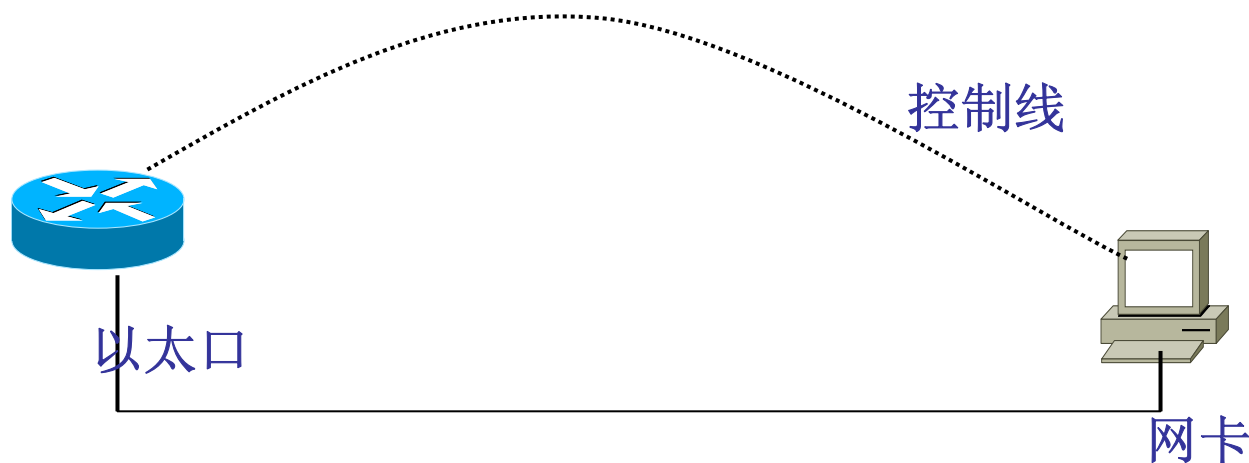
使用TFTP服务器备份路由器Flash中的IOS映像

使用TFTP服务器升级路由器IOS软件/恢复路由器IOS软件

使用TFTP服务器备份/恢复配置文件

第四章 路由器基本操作

1、建立物理连接



选用合适的线缆建立此物理连接，此处显示的是一个最简单的网络拓扑

第四章 路由器基本操作

2、建立网络连接，测试连通性

配置路由器以太口地址为192.168.1.254/24

配置PC机（TFTP服务器）的网卡地址为192.168.1.253/24

在路由器配置窗口中：

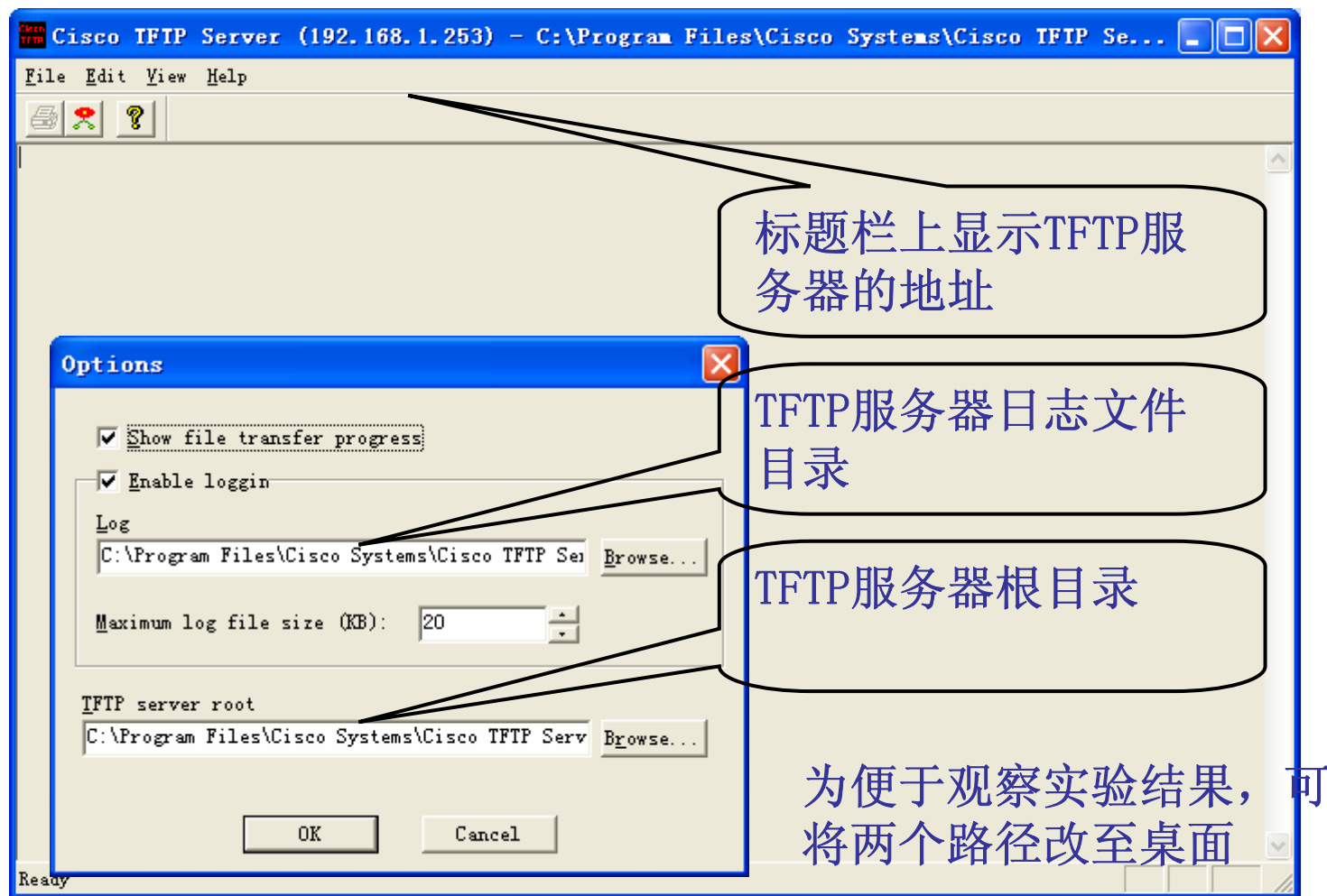
```
router#ping 192.168.1.253
```

在PC机中开启一个DOS窗口：

```
C:>ping 192.168.1.254
```

第四章 路由器基本操作

3、配置TFTP服务器



第四章 路由器基本操作

4、备份IOS

通过show flash或show version命令，查看IOS文件名，形如c2500-i-1.bin（.bin表示这是一个二进制的压缩文件），复制该文件名备用。

使用copy命令进行备份，格式如下：

copy 源路径下的源文件 目标路径下的目标文件

此实验中，要备份的IOS文件存放于FLASH中

```
copy flash tftp
```

5、备份配置文件

```
copy running-config tftp
```

```
copy startup-config tftp
```

6、查看备份结果

通过TFTP服务器的日志文件

通过路由器的显示结果

通过记事本/写字板查看备份的配置文件

第四章 路由器基本操作

7、恢复/升级操作系统

首先确认要路由器的硬件配置是否满足新的IOS的运行要求。

```
copy tftp flash
```

8、恢复配置文件

```
copy tftp running-config
```

```
copy tftp startup-config
```

第四章 路由器基本操作

路由器上插有两个8M的FLASH, show flash显示:

System flash directory, partition 1:

File	Length	Name/status
------	--------	-------------

Flash分区的合并

1	7883292	c2500-i-1.121-7.bin
---	---------	---------------------

[7883356 bytes used, 505252 available, 8388608 total]

8192K bytes of processor board System flash (Read ONLY)

System flash directory, partition 2:

No files in System flash

[0 bytes used, 8388608 available, 8388608 total]

8192K bytes of processor board System flash (Read/Write)

第四章 路由器基本操作

1、将flash:2:删除

```
Router#erase flash:2:
```

2、合并两个flash

```
Router(config)#partition flash 1
```

3、show flash:

```
System flash directory:
```

```
File Length Name/status
```

```
1 7883292 c2500-i-1.121-7.bin
```

```
[7883356 bytes used, 8893860 available, 16777216 total]
```

```
16384K bytes of processor board System flash (Read ONLY)
```

第四章 路由器基本操作

使用tftpdnld的方式恢复IOS

```
rommon 1 >IP_ADDRESS=192.168.0.1 (路由器第一个以太口的ip地址)
rommon 2 >IP_SUBNET_MASK=255.255.255.0
rommon 3 >DEFAULT_GATEWAY=192.168.0.2
rommon 4 >TFTP_SERVER=192.168.0.2 (TFTP服务器的IP地址)
rommon 5 >TFTP_FILE=c2600-i-mz.120-7.T.bin (上传文件的名称)
rommon 6 >sync (保存)
rommon 7 >set (查看)
rommon 8 >tftpdnld (传送文件) 出现提示选择y
```

第四章 路由器基本操作

用Xmodem的方式恢复IOS

- 1、使用超级终端，把IOS放在超级终端的指定目录下
- 2、在rommon下使用xmodem或ymodem命令，如： `xmodem -rc c4500flash`
- 3、在超级终端发送文件c4500flash
- 4、传输完成后，系统会加载
- 5、此时系统在ram中，并不在flash里，要把IOS拷贝到flash中

第四章 路由器基本操作

CDP: Cisco Discovery Protocol, 思科发现/查找协议。

- 1、私有
- 2、工作在数据链路层
- 3、用于发现直接连接的Cisco邻居设备
- 4、默认启用
- 5、可查看到第三层信息

第四章 路由器基本操作

```
Router>show cdp
```

```
Router>show cdp interface
```

```
Router>show cdp neighbors
```

```
Router>show cdp neighbors detail
```

```
Router>show cdp entry *
```

```
Router>show cdp entry rod (rod为某个邻居的主机名)
```

第四章 路由器基本操作



```
rb#show cdp neighbors
```

```
...
```

Device ID	Local Intrfce	Holdtme	Capability	Platform	Port ID
Ra	Ser 1	161	R	2500	Ser 0

Device ID 邻居设备的主机名

Local Intrfce 路由器RB自身的接口，即连接到邻居的接口

Holdtme 保持计时器

Capability 类型，此处显示为R，表明邻居是路由器

Platform 平台，此处为2500系列

Port ID 对端的接口

即：RB通过自己的Serial 1接口连接到一台名称为RA的2500系列的路由器的Serial 0接口。

第四章 路由器基本操作



CDP的两个计时器：更新时间为60S，保持时间为180S

假设当RA在第5秒时发送CDP的广播并被RB所接收，RB启用计时器进行倒计时。

RB期望在60秒之后即65秒时收到来自RA的CDP更新。

如果在第65秒时正常收到更新，RB刷新计时器，重新开始倒计时。

如果在第65秒时没有收到，RB并不是立刻把RA从CDP邻居表中删除，而是继续等待直到保持时间超时。RB将在180秒之后，即185秒时将RA从CDP邻居表中移除。

第四章 路由器基本操作



CDP的启用与关闭

默认情况下，CDP是启用的

在全局模式下：Router(config)# (no) cdp run

在接口模式下：Router(config-if)# (no) cdp enable

如图，要关闭S1接口的CDP

```
Router(config)# cdp run
```

```
Router(config)# interface serial 1
```

```
Router(config-if)# no cdp enable
```


第五章 IP网络规划

什么是IP地址？

IP地址由一个32位长的二进制数字表示，这32位又分为4个8比特数。由于我们日常习惯用十进制表示数字，因此以十进制来表示每个8比特数，范围从0~255。这4个十进制用小圆点隔开，称为点分十进制表示法，如172. 16. 122. 204。

一个IP地址主要由两部分组成：一部分是用于标识该地址所隶属的网络号；另一部分用于指明该网络上某个特定主机的主机号。

第五章 IP网络规划

为什么要使用IP地址？

一个IP地址是用来标识网络中的一个通信实体，比如一台主机，或者是路由器的某一个端口。在基于IP协议网络中传输的数据包，也都必须使用IP地址来进行标识。每个被传输的数据包包括一个源IP地址和一个目的IP地址。当该数据包在网络中进行传输时，这两个地址保持不变，以确保网络设备始终能够根据确定的IP地址，将数据包从源通信实体送往指定的目的通信实体。

如同我们写一封信，要标明收信人的通信地址和发信人的地址，而邮局则通过该地址来决定邮件的去向。

第五章 IP网络规划

基础知识：十进制、二进制与十六进制的转换及运算

You have the binary number 10011101. Convert it to its decimal and hexadecimal equivalents.

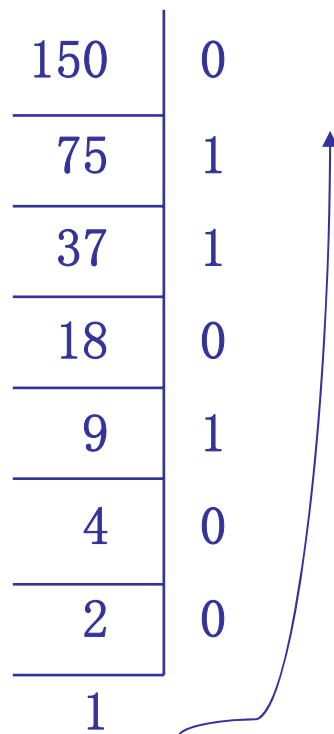
- | | | |
|--------|---------|---------|
| A. 158 | B. 0x9D | C. 156 |
| D. 157 | E. 0x19 | F. 0x9F |

答案：B、D。

- 1、10011101一定为奇数，可排除A、C选项，得出十进制值为157。
- 2、1001的十进制肯定不为1或者F，则十进制应为9，排除E选项。
- 3、1101的十进制同样肯定不为F，排除F选项。

第五章 IP网络规划

150	0
75	1
37	1
18	0
9	1
4	0
2	0
1	



通过二进制的除法，最后得出

150=10010110

第五章 IP网络规划

How do you express the binary number 11111000 in decimal?

- A. 220 B. 224 C. 240 D. 248
E. 256

答案：D

1、11111111=255

2、111=7

3、11111000=11111111-00000111=255-7=248

第五章 IP网络规划

How would you express the number 231 in its binary form?

- A. 11011011 B. 11110011 C. 11100111
D. 11111001 E. 11010011

答案：C

1、 $11111111=255$

2、 $255-231=24=16+8$

3、即在11111111的第4位和第5位上取0



第五章 IP网络规划

IP地址的分类

A类：最高位为0，前8比特表示网络号，后24比特表示主机号，范围为0~127，对应二进制值范围00000000~01111111。因为网络号全为0的地址保留，实际上A类地址从1开始。同时因为127的地址保留给回送地址，因此实际上A类地址范围为1~126，共126个地址。
每个A类网络中最多可容纳 $2^{24}-2=16777214$ 台主机。

B类：最高位为10，前16比特表示网络号，后16比特表示主机号。取值范围128~191，对应二进制范围10000000~10111111。
B类网络共有 $2^{14}=16384$ 个，每个B类网络中最多可容纳 $2^{16}-2=65534$ 台主机。

C类：最高位为110，前24比特表示网络号，后8比特表示主机号。取值范围192~223，对应二进制范围11000000~11011111。
C类网络共有 $2^{21}=2097152$ 个，每个C类网络中最多可容纳 $2^8-2=254$ 台主机。

D类，最高位为1110，224~239，组播地址。

E类，最高位为11110，240~255，保留试验使用。

第五章 IP网络规划

私有地址:

10.0.0.0~10.255.255.255

172.16.0.0~172.31.255.255

192.168.0.0~192.168.255.255

第五章 IP网络规划

IP地址使用规则

网络号全为0的地址保留，不能作为标识网络使用；

主机号全为0的地址保留，作为表示网络地址；

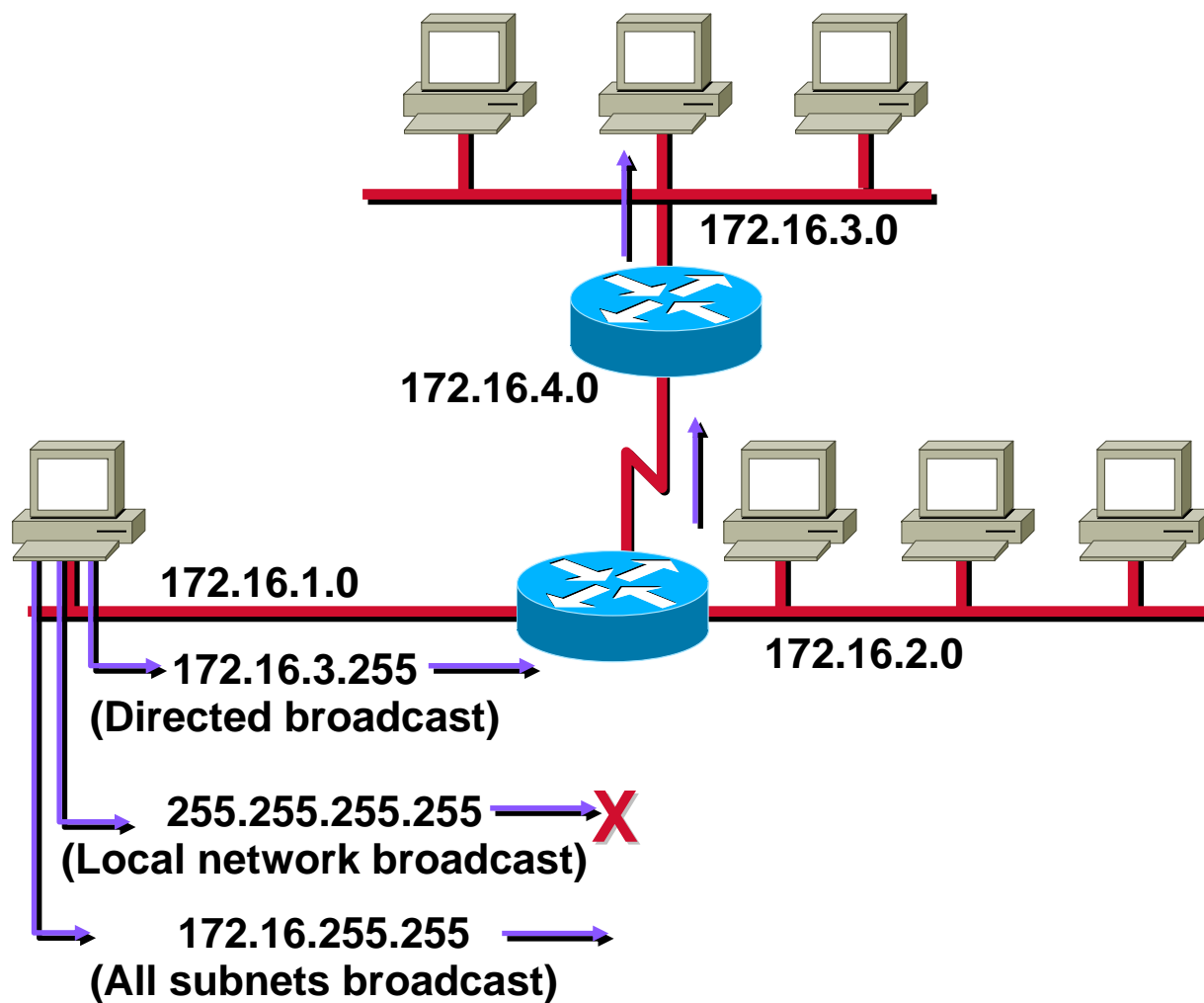
网络号全为1，节点号全为0的地址表示子网掩码；

主机号全为1的地址为广播地址，如172.16.255.255，称为直接广播或定向广播，表示对172.16.0.0中的所有主机进行广播，这类广播可以跨越路由器。

地址0.0.0.0表示默认路由；

地址255.255.255.255表示本地广播，这种广播在缺省情况下不能跨越路由器。

第五章 IP网络规划



第五章 IP网络规划

子网掩码（Subnet Mask）概述

子网掩码用于区别某个IP地址中哪部分为网络部分，哪部分为主机部分。子网掩码由1和0组成，长32位，从前向后连续全为1的位代表网络部分。

默认子网掩码，不是所有的网络都需要子网：

A类IP地址的默认子网掩码为255.0.0.0；

B类IP地址的为255.255.0.0；

C类的为255.255.255.0。

第五章 IP网络规划

子网掩码的主要功能是告知网络设备：某个特定的IP地址的哪一部分是网络部分，哪一部分是主机部分。只要识别出目的IP的网络部分，路由器即可做出路由寻址决策，IP地址的主机部分不参与路由器的路由寻址操作。

子网掩码使用与IP地址相同的编址格式，子网掩码为1的部分对应网络（及子网）部分，子网掩码为0的部分对应主机部分。

将子网掩码和IP地址作“与”操作后，IP地址的主机部分将被丢弃，剩余的是网络地址和子网地址。

例如：一个IP地址为10.2.45.1，子网掩码为255.255.252.0，“与”运算得到：10.2.44.0，则网络设备认为该IP地址的网络号与子网号为10.2.44.0，属于10.2.44.0/22网络，其中/22表示子网掩码长度为22位，即从前向后连续的22个1。

与运算

00001010.00000010.00101101.00000001

11111111.11111111.11111100.00000000

第五章 IP网络规划

Classless Inter-Domain Routing (CIDR)，无类域间路由

掩码255.0.0.0: /8(A类地址默认掩码)

掩码255.128.0.0: /9

掩码255.192.0.0: /10

掩码255.224.0.0: /11

掩码255.240.0.0: /12

掩码255.248.0.0: /13

掩码255.252.0.0: /14

掩码255.254.0.0: /15

掩码255.255.0.0: /16(B类地址默认掩码)

掩码255.255.128.0: /17

掩码255.255.192.0: /18

掩码255.255.224.0: /19

掩码255.255.240.0: /20

掩码255.255.248.0: /21

掩码255.255.252.0: /22

掩码255.255.254.0: 23

掩码255.255.255.0: /24(C类地址默认掩码)

掩码255.255.255.128: /25

掩码255.255.255.192: /26

掩码255.255.255.224: /27

掩码255.255.255.240: /28

掩码255.255.255.248: /29

掩码255.255.255.252: /30

第五章 IP网络规划

子网划分（subnetting）的好处

减少网络流量
提高网络性能
提高安全性

为了提高IP地址的使用效率，一个网络可以划分为多个子网。

采用借位的方式，从主机最高位开始借位变为新的子网位，剩余部分仍为主机位。这使得IP地址的结构分为三部分：网络位、子网位和主机位。

划分子网后，子网号为全0或全1的子网原则上不可使用。

第五章 IP网络规划

默认情况下，192.168.0.0属于C类地址，子网掩码为24位。此时：

11000000.10101000.00000000.00000000

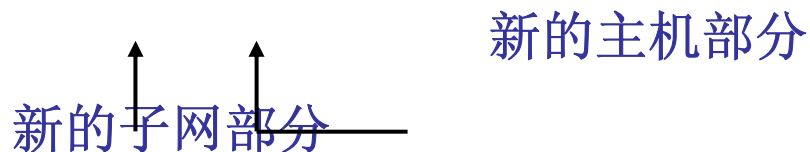
|-----网络位-----|---主机位---|

如要将192.168.0.0/24划分子网，从原来的主机部分取三位作为新的子网位。

11000000.10101000.00000000.00000000

|-----网络位-----|---|----|

新的子网部分 新的主机部分



可划分出000、001、010、011、100、101、110、111共8个子网。

此时，网络部分为24+3=27位，子网掩码为/27，表示为十进制为255.255.255.224，主机部分为5位。

第五章 IP网络规划

方法一、利用子网数来计算

如：欲将B类IP地址168. 195. 0. 0划分成27个子网。

公式： $2^n - 2 \geq x$ ，其中x为所需的子网数，n为所需借的子网位数。

168. 195. 00000000. 00000000

从原来的主机部分开始，从前向后借子网位。

该例中需27个子网，按公式，需借5位，可划分出如下子网：

168. 195. 00000 000. 00000000 ...

168. 195. 00001 000. 00000000 168. 195. 11101 000. 00000000

168. 195. 00010 000. 00000000 168. 195. 11110 000. 00000000

... 168. 195. 11111 000. 00000000

共 $2^5=32$ 个子网，其中有效子网30个，掩码均为/21。

第五章 IP网络规划

如需将200.0.0.0/24划分子网，分配给ABCD四个部门。

方法如下：

在未划分前，主机位为8位。现在需划分子网，则从主机位入手。

可将将8位主机部分视为一个新的IP地址，8位中，前若干位为网络部分，后若干位为主机部分，如下所示。

200.0.0. 000 0000000

暂时忽略 网络部分 主机部分

因为需要将子网分配给四个部门，则需要4个子网。又因为子网号为全0和全1的子网不能用，则至少需要6个子网。

按公司 $2^n - 2 \geq$ 所需子网数

此时 $n=3$ ，可划分出8个子网。

第五章 IP网络规划

	网络号	主机地址范围	广播地址
000	子网号全为0，不使用		
001	200.0.0.32/27	001 00001~11110	001 11111
010	200.0.0.64/27	010 00001~11110	001 11111
011	200.0.0.96/27	011 00001~11110	001 11111
100	200.0.0.128/27	100 00001~11110	001 11111
101	200.0.0.160/27	101 00001~11110	001 11111
110	200.0.0.192/27	110 00001~11110	001 11111
111	子网号全为0，不使用		

第五章 IP网络规划

注意到每个子网的主机地址范围都是00001~11110，广播地址都是11111，那么有了每个子网的网络号后，每个子网的地址范围就很容易推出。

如100子网，网络地址为200.0.0.128/27，则该子网中第一个主机（host）IP为128+1=129，即100 00001，用二进制的10000000（网络部分）+00000001（主机部分）；最后一个主机IP为128+30=158，即100 11110，用二进制的10000000（网络部分）+00011110（主机部分）；广播地址为128+31=159，即100 11111，用二进制的10000000（网络部分）+00011111（主机部分全为1的地址是广播地址）。

另外，如果用广播地址加1，则成为下一个子网的网络地址。

第五章 IP网络规划

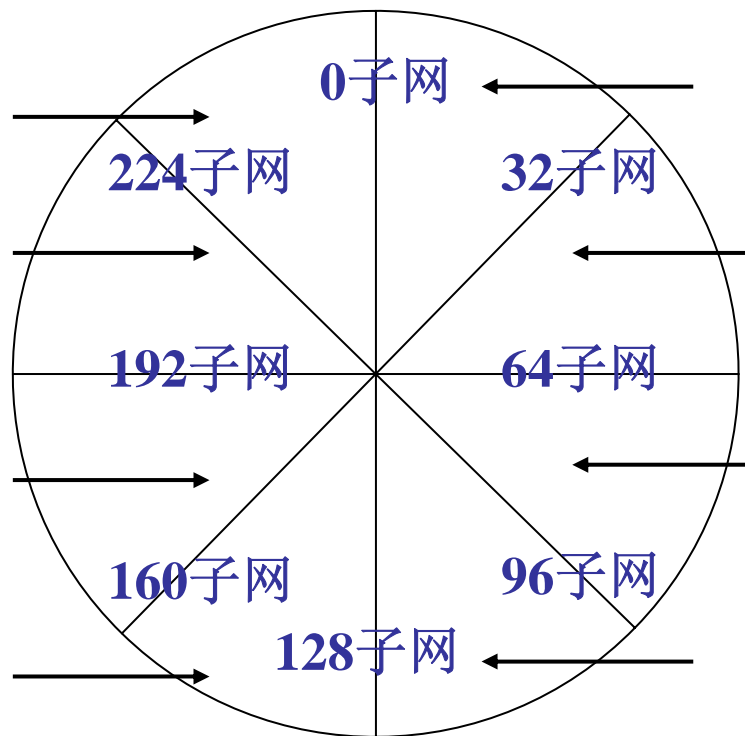
另一种思维方法： 要将200.0.0/24划分子网给四个部门使用，这就需要将该网络划分为8个子网。而且每个子网的大小相等，这意味着将200.0.0/24网络中原有的256个IP地址八等分。

第8个子网：225至255。其中255为广播地址，有效主机地址为225至254。

第7个子网：193至223。其中223为广播地址，有效主机地址为193至222。

第6个子网：161至191。其中191为广播地址，有效主机地址为161至190。

第6个子网：129至159。其中159为广播地址，有效主机地址为129至158。



第1个子网：1至31。其中31为广播地址，有效主机地址为1至30。

第2个子网：33至63。其中63为广播地址，有效主机地址为33至62。

第3个子网：65至95。其中95为广播地址，有效主机地址为65至94。

第4个子网：97至127。其中127为广播地址，有效主机地址为97至126。

第五章 IP网络规划

例，如需将某C类地址划分20个子网，问第三个有效子网的网络地址、主机地址范围和广播地址？

解决步骤：

- 1、需20个子网，则需子网位为5，剩余主机位为3，子网的大小为8。
- 2、 $8*3=24$ ，则第三个有效子网的地址为24/29。（第一问）
- 3、 $24+8=32$ ，下一个子网的地址为32/29。
- 4、广播地址为后一个子网的网络地址减1，为31。（第三问）
- 5、主机地址范围为25至30。

验证…

第五章 IP网络规划

方法二、利用主机数来计算

如欲将B类IP地址168. 195. 0. 0划分成若干子网，每个子网内有主机700台。

公式： $2^n - 2 \geq x$ ，其中x为所需的主机数，n为所需借的主机位数。

168. 195. 00000000. 00000000

从原来的主机部分开始，从后向前借主机位。

该例中每子网需700个地址，按公式，需借10位，划分出如下子网：

168. 195. 000000 00. 00000000 ...

168. 195. 000001 00. 00000000 168. 195. 111101 00. 00000000

168. 195. 000010 00. 00000000 168. 195. 111110 00. 00000000

... 168. 195. 111111 00. 00000000

共 $2^6=64$ 个子网，其中有效子网62个，掩码均为/22。

第五章 IP网络规划

划分子网的几个注意事项：

- 1、你所选择的子网掩码将会产生多少个子网？
- 2、有效子网？
- 3、每个子网的起、止范围？
- 4、每个子网的有效主机地址范围？

第五章 IP网络规划

Variable Length Subnet Masks(VLSM)

VLSM的作用：节约IP地址空间；减少路由表大小。
使用VLSM时，所采用的路由协议必须能够支持它，这些路由协议包括RIPv2、OSPF、EIGRP和BGP等。

第五章 IP网络规划

某单位有一个C类网络**200.1.1**，共有四个部门，准备划分子网。这四个部门内的主机数目分别是：**A 60台； B 28台； C 20台； D 5台。**

- (1) 给出一种可能的子网掩码安排来完成规划。**
- (2) 如果部门D的主机数目增长到34台，又如何解决？**

第五章 IP网络规划

第1问解决方法:

每个部门分配一个子网, 部门A、B、C、D的子网大小分别是: $2^6=64$; $2^5=32$; $2^5=32$; $2^3=8$ 。

以部门A为例, 所需IP地址数为60, 主机地址需从后向前取6位, 剩余2位作为子网使用, 子网号可分别为01和10。其他部门类推。

该题可有多种答案, 给出其中一种:

部门A的地址范围为: 200.1.1.01 000000~01 111111, 主机地址范围为200.1.1.65~126, 掩码为255.255.255.192。

部门B的地址范围为: 200.1.1.100 000000~100 11111, 主机地址范围为200.1.1.129~158, 掩码为255.255.255.224。

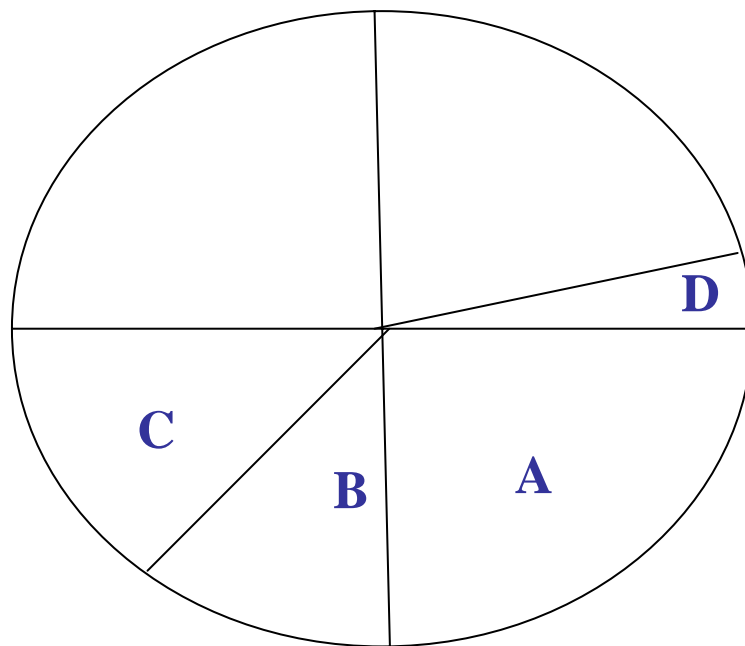
部门C的地址范围为: 200.1.1.110 000000~110 11111, 主机地址范围为200.1.1.193~222, 掩码为255.255.255.224。

部门D的地址范围为: 200.1.1.1110 000~11100 111, 主机地址范围为200.1.1.225~230, 掩码为255.255.255.248。

第2问解决方法类似。

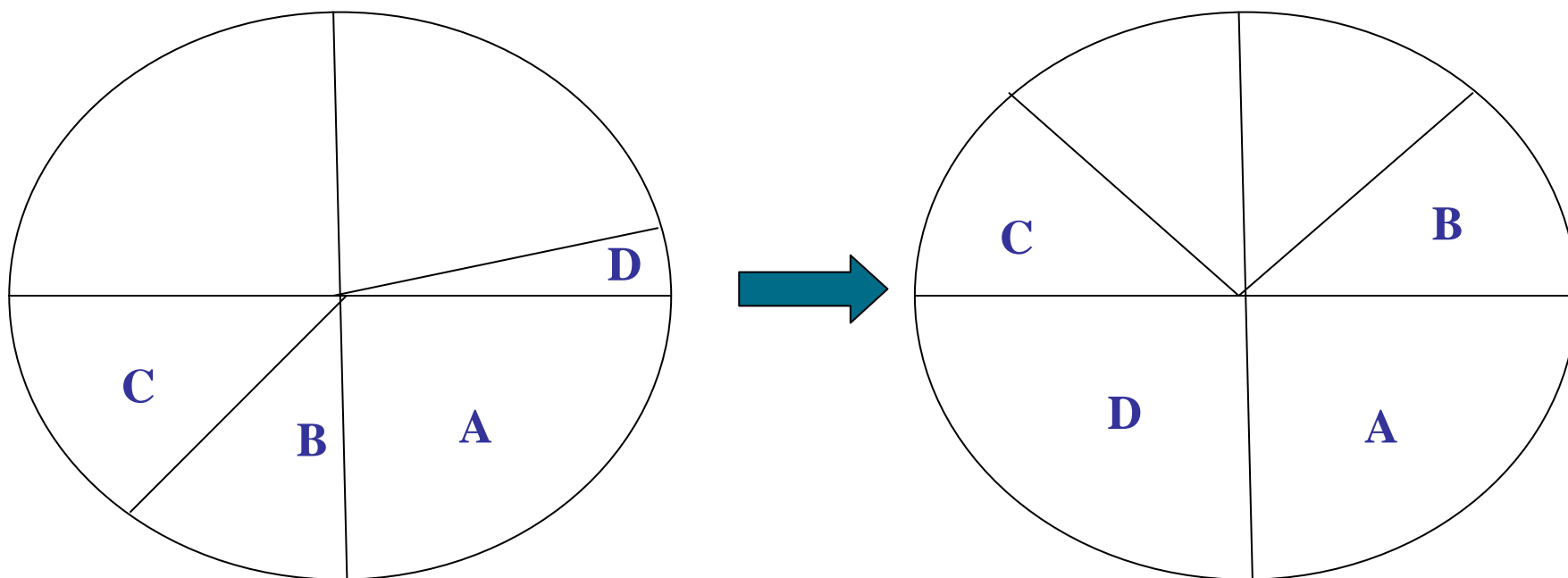
第五章 IP网络规划

- 1、先解决部门A。
- 2、然后解决部门B。
- 3、再解决部门C。
- 4、最后解决部门D。

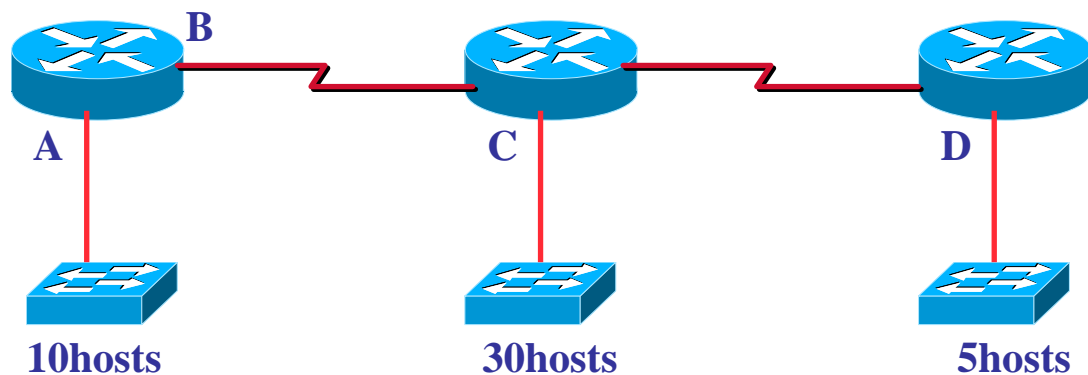


第五章 IP网络规划

如果部门**D**的主机数目增长到34台，又如何解决？



第五章 IP网络规划



如图：A、B、C、D为路由器的不同接口，请为这些接口选择合适的IP地址。

192.168.0.13/28

192.168.0.5/30

192.168.0.33/27

192.168.0.25/29

192.168.0.4/30

192.168.0.17/28

192.168.0.193/26

192.168.0.9/29

第五章 IP网络规划

IPV6简介

全球范围内WLAN、2.5G、3G无线移动数据网络的发展加快了以互联网为核心的通信模式的形成，由于移动通信用户的增长要比固定用户快得多，特别是各种具有联网功能的移动终端的迅猛发展，考虑到随时随地、任何形式的个人多媒体通信的需要，现有的IPv4已远远不能满足网络市场对地址空间、端到端的IP连接、服务质量、网络安全和移动性能的要求。因此人们寄希望于新一代的IP协议来解决以上问题。

IPv6协议正是基于这一思想提出的，它是“互联网协议第六版”的缩写。在设计IPv6时不仅仅扩充了IPv4的地址空间，而且对原IPv4协议各方面都进行了重新考虑，做了大量改进。除了提出庞大的地址数量外，IPv6与IPv4相比，还有很多的工作正在进行以期得到更高的安全性、更好的可管理性，对QoS (Quality of Service) 和多播技术的支持也更为良好。

第五章 IP网络规划

报头格式

IPv4报头包含20bit+选项，13个字段，包括3个指针。

IPv6报头由基本报头+扩展报头链组成，其中基本报头如表2所示，包含40bit，8个字段。

IPv6报头采用基本报头+扩展报头链组成的形式，这种设计可以更方便地增添选项以达到改善网络性能、增强安全性或添加新功能的目的。

0	4	8	16	24	32
版本	IHL	业务类别	总长度		
标识					
生存时间		协议	报头校验		
32bit源地址					
32bit目标地址					
选项和填充					

0	4	8	16	24	32
版本	业务类别		流标记		
载荷长度			下一个报头 跳限		
128bit源地址					
128bit目标地址					

第五章 IP网络规划

固定的IPv6基本报头

IPv6基本报头被固定为40bit，使得路由器可以加快对数据包的处理速度，提高了转发效率，从而提高网络的整体吞吐量，使信息传输更加快速。

简化的IPv6基本报头

IPv6基本报头中去掉了IPv4报头中阴影部分的字段，其中段偏移和选项和填充字段被放到IPv6扩展报头中进行处理。

去掉了报头校验（HeaderChecksum），中间路由器不再进行数据包校验。去掉此字段的原因有三：一是因为大部分二层链路层已经对数据包进行了校验和纠错控制，链路层的可靠保证使得三层网络层不必再进行报头校验；二是端到端的四层传输层协议也有校验功能以发现错包；三是报头校验需随着TTL值的变化在每一跳重新进行计算，增加包传送的时延。

IPv6基本报头中去掉与IP分片相关的域，使路由器无需再对数据包进行分片，而分片工作由源终端设备根据最大传输单元MTU路径发现来进行。这样IPv6的数据包可以远远超过64kbit/s，应用程序可以获得更快、更可靠的数据传输。

第五章 IP网络规划

IPv6报头新增流标记字段

IPv6协议不仅保存了IPv4报头中的业务类别字段，而且新增了流标记字段，使得业务可以根据不同的数据流进行更细的分类，实现优先级控制和QoS保障，极大地改善了IPv6的服务质量。

IPv6报头采用128bit地址长度

这是IPv4与IPv6最主要的区别。IPv4采用32bit长度，理论上可以提供大约43亿个IP地址，这么多的IP地址似乎可以满足网络连接的需要，但事实上是网络中缺乏足够地址满足各种潜在的用户。

IPv6采用128bit长度，相对IPv4，增加了296倍的地址空间。按保守方法估算IPv6实际可分配的地址，整个地球的每平方米面积上仍可分配1000多个地址。这样几乎可以不受限制地提供IP地址，从而确保了端到端连接的可能性。

第五章 IP网络规划

IPv6协议可根据用户的需要进行层状地址分配，这和IPv4采用块状地址分配是不同的，后者方式导致某些地址无法使用。在IPv6的分层地址分配方式中，高级网络管理部门可为下级网络管理部门划分地址分配区域，下级网络管理部门则可为更下层的管理部门进一步划分。

IPv6将用户划分成3种类型：

使用企业内部网络和Internet；

目前使用企业内部网络，将来可能会用到Internet；

通过家庭、机场、旅馆以及其他地方的电话线和Internet网络互联。

第五章 IP网络规划

IPv6协议为这些用户提供了不同地址分配方式。

4种类型的点到点通信/单播地址；用于标识单一网络设备接口，单播通信传播的分组可传送到地址标识的接口。

改进的多播地址格式；用于标识归属于不同节点的设备接口集合，多播通信的分组可发送到地址标识的所有接口，这种地址方式是非常有用的。例如，可将网络中发送的新消息传送给所有登记的用户。特殊的多播地址可限制在特定网络链路或特定的系统组中进行通信。IPv6协议没有定义广播地址，但可使用多播地址替代。

新的任意播(Anycast)地址格式；IPV6协议中引入了任意播地址，用于标识属于不同节点的设备接口集合，任意播传送的分组可发送到地址标识的某一接口，接收到信息的接口通常是最近距离的网络节点，这种方式可提高路由选择的效率，网络节点可通过地址表示通信过程传输路由可经过的中间跳数，即信息传输路由可不必由路由器决定。

第二部分 路由协议

第一章 路由原理

第二章 静态路由

第三章 动态路由 - **RIP**

第四章 动态路由 - **IGRP**

第五章 动态路由 - **EIGRP**

第六章 动态路由 - **OSPF**

第七章 访问控制列表

第八章 故障排除方法

第一章 路由原理

路由协议（**Routing Protocol**）：用于路由器动态寻找网络最佳路径，保证所有路由器拥有相同的路由表，如**OSPF**、**RIP**、**IGRP**、**EIGRP**等。

可路由协议（**Routed protocol**）：当所有的路由器了解整个网络的拓扑结构以后，可路由协议就可以用来发送数据，如**IP**和**IPX**。

路由协议的类型：

内部网关协议（**IGP**）；如**RIP**、**IGRP**、**OSPF**、**EIGRP**、**IS-IS**等；

外部网关协议（**BGP**）：是一种域间路由选择协议，也称为**EGP**。

第一章 路由原理

当一台主机要发送数据包给同一网络中的另一台主机时，它将直接把数据包送到网络上；而要送给不同IP网络中的主机时，它将选择一个能到达目标网络的路由器或缺省网关(**default gateway**)，由它负责把数据包送到目的地。

路由器转发数据包时，只根据目标IP地址的网络部分，查找路由表，选择合适的接口，将数据包发送出去。

如果路由器的接口所连接的就是目标网络，将直接通过接口把包送到目标网络；否则，将选择其他邻居路由器。路由器也可以有它的缺省网关，用来传送不知道往哪儿送的IP包。这样，路由器把知道如何传送的IP包转发出去，不知道的IP包送给缺省网关，通过不断的转发，数据包最终将送到目的地，送不到目的地的则被丢弃。

当路由器收到一个目标网络没有在路由表中列出的包的时候，它并不发送广播寻找目标网络，而是直接丢弃。

第一章 路由原理

路由器通过建立路由选择表并与其他路由器交换路由选择表中的网络信息来完成两项主要功能：

- 为进入数据分组选择最佳路径；
- 将分组交换到适当的出站端口。

第一章 路由原理

路由：负责把一个数据包从某个设备发送到不同网络里的另一个设备上去。路由器并不关心某个具体的主机，只负责将数据包送达某个网络，它们只关心网络的状态和网络中的最佳路径。

路由器要路由数据包，需要知道以下信息：

- 1、目标地址（**destination address**）
- 2、可以学习到远端网络的邻居**Router**
- 3、到达远端网络的所有路由
- 4、到达远端网络的最佳路径
- 5、如何保持和验证路由信息

在未配置路由协议之前，路由器只知道与其接口直接相连的网络或子网。

第一章 路由原理

直连路由：路由器通过接口所连接的网络。

管理距离：**Administrative Distance**，简称**AD**。用来衡量对某种路由协议的信任程度，取值范围为**0~255**，数值越大，信任程度越低。如果为**255**，则表示完全不信任。

直接路由的管理距离为**0**

查看路由表：**show ip route**

第一章 路由原理

Router>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, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, * - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C 10.0.0.0/8 is directly connected, Serial0

C 192.168.0.0/24 is directly connected, Ethernet0

代码C为直连路由，表明该路由器通过Serial0直接连接了10.0.0.0/8网络，通过Ethernet0直接连接了192.168.0.0/24网络。

第二章 静态路由

静态路由是由管理员手工配置的到达某个网络的路径。

相关命令：

ip route [dest-network] [mask] [next-hop address或exit interface][administrative distance] [permanent]

ip route: 创建静态路由

dest-network: 目标网络

mask: 目标网络的子网掩码

next-hop address: 到达目标网络所经过的下一跳的地址

exit interface: 到达目标网络的发送接口（本路由器的出口）

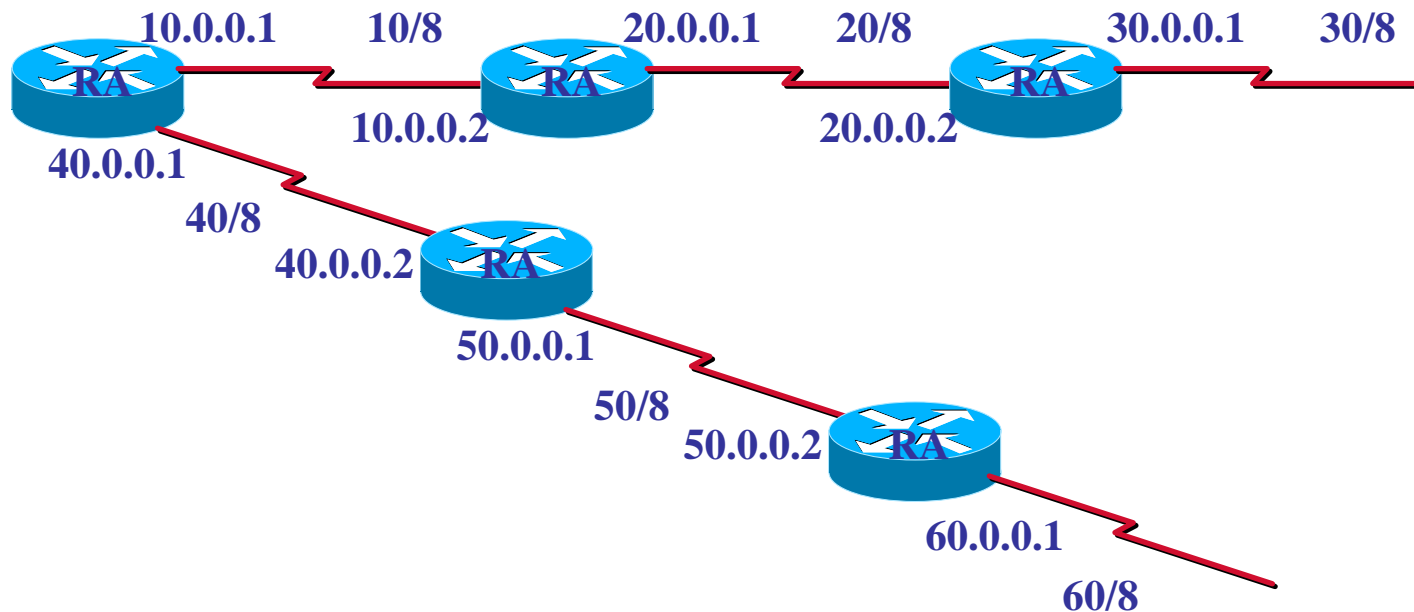
administrative distance: 管理距离。默认情况下静态路由的管理距离是1，如果用**exit interface**代替**next-hop address**，则管理距离是0。

permanent: 如果接口被**shutdown**了或者路由器不能和下1跳路由器通信，这条路由线路将自动从路由表中被删除。使用这个参数保证即使出现上述情况，这条路由仍然保持在路由表中。

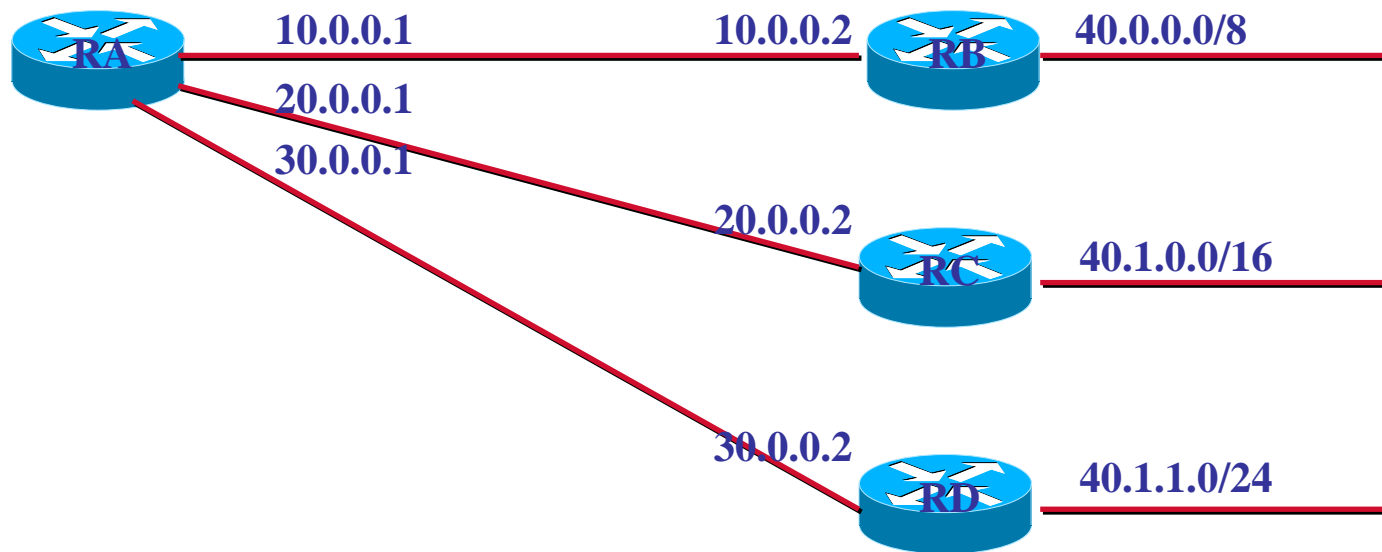
第二章 静态路由

Next Hop Address, 下一跳地址, 即到达目标网络路径中邻居路由器的接口IP地址。

如图所示: **RA**到达**20.0.0.0/8**网络的下一跳IP地址为**10.0.0.2**, 那么到达**30.0.0.0/8**网络的下一跳IP地址为什么? 到达**60.0.0.0/8**网络的下一跳IP地址为什么?



第二章 静态路由



如图所示的网络中，RA配置了三条静态路由：

```
ip route 40.0.0.0 255.0.0.0 10.0.0.2
```

```
ip route 40.1.0.0 255.255.0.0 20.0.0.2
```

```
ip route 40.1.1.0 255.255.255.0 30.0.0.2
```

当RA收到一个目的地址是40.1.1.1的数据包时，它将选择哪条路由，发向哪一个下一跳地址？或者三条路径都发送，实现负载均衡？

第二章 静态路由

使用下一跳地址和本地出口的区别

1、优先级（管理距离）值不同

默认情况下，使用下一跳地址时管理距离为**1**，使用本地出口时管理距离为**0**，此时在查看路由表时，静态路由类似直连路由。

2、路由方式不同

采用本地出口时，仅需要在路由表中查找一次，采用下一跳地址时，需要在路由表中查找两次。第一次判断数据包应按照哪条静态路由执行路由，第二次判断、选择应从哪个接口送交给下一跳地址。

第二章 静态路由



三台路由器正确配置接口后，路由表分别表示如下：

C 172.16.0.0/16

C 172.16.0.0/16

C 192.168.0.0/24

C 192.168.0.0/24

其中：

A路由器缺少到达192.168.0.0/24的路由；

C路由器缺少到达172.16.0.0/16的路由；

而B路由器可通过直连路由到达这两个网络，不需要额外配置。

第二章 静态路由



首先在A路由器上配置静态路由

```
Ra(config)#ip route 192.168.0.0 255.255.255.0 172.16.0.1
```

查看路由表

```
Ra#show ip route static
```

```
S 192.168.0.0 [1/0] via 172.16.0.1
```

S 通过静态路由学习到

192.168.0.0 远端网络

[1/0] 管理距离

via 经过，通过

172.16.0.1 下一跳地址

此时C路由器尚未配置。问：

1、RA能否ping通192.168.0.1

2、RA能否ping通192.168.0.2

3、为什么

4、如何解决

第二章 静态路由



此时，从RA可以ping通192.168.0.1，表明RA可以正确发送到达192.168.0.0/24网络的数据包，但不能ping通192.168.0.2。

分析和解决

在RB和RC上分别开启debug（需在特权模式下），之后继续从RA分别出Ping 192.168.0.1和192.168.0.2，观察结果。

```
RB#debug ip packet
```

```
RC#debug ip packet
```

分析Ping的过程，ICMP Echo Request和ICMP Echo Reply

解释成功或失败的原因

排除故障

第二章 静态路由

了解和认识管理距离AD的作用：

对刚配置的静态路由的语句进行修改

- 1、将管理距离改为**100**，查看路由表
- 2、继续将管理距离改为**255**，查看路由表
- 3、将下一跳地址改为本地出口，查看路由表

第二章 静态路由

修改管理距离的作用



如图所示，到达某个网络可能存在多条通路，路由器可能会分别通过动态路由和静态路由学习到多条路径。此时，路由器将比较不同路由协议的管理距离，选择管理距离数值比较小的路径放入路由表。

如果将静态路由的管理距离值修改为较大，如200，则正常情况下由A路径发送，当A路径失败时，可转由B路径发送，起到备份和冗余的作用。

第二章 静态路由

优点：

- 1、没有额外的路由器的CPU负担
- 2、节约带宽
- 3、安全

缺点：

- 1、网络管理员必须了解网络的整个拓扑结构
- 2、如果网络拓扑发生变化，管理员要在相关路由器上手动修改
- 3、不适合于大型网络

第二章 静态路由

防止错误配置导致路由环路



Ra(config)#ip route 200.0.0.0 255.255.255.0 10.0.0.2

Rb(config)#ip route 200.0.0.0 255.255.255.0 10.0.0.1

Ra将把目标网络为**200.0.0/24**的数据包发送给**Rb**，**Rb**又会发送给**Ra**，造成环路。

第二章 静态路由

默认路由（**Default Routing**）：一般使用在**stub**网络（只有**1**条出口路径的网络）中，使用默认路由来发送那些目标网络没有包含在路由表中的数据包。

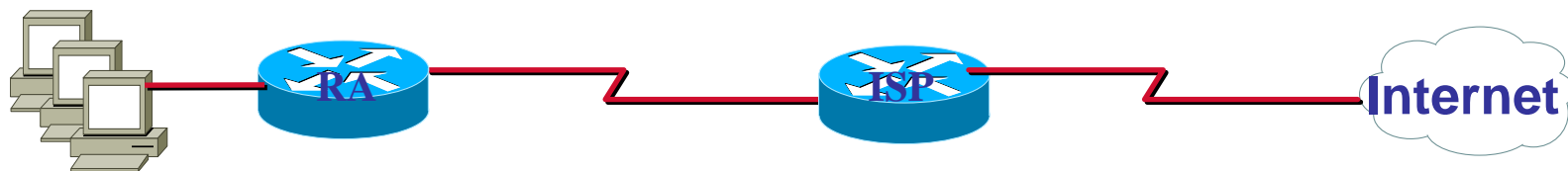
```
Ra(config)#ip route 0.0.0.0 0.0.0.0 172.16.0.1
```

```
Ra#show ip route
```

```
S* 0.0.0.0 [1/0] via 172.16.0.1
```

第二章 静态路由

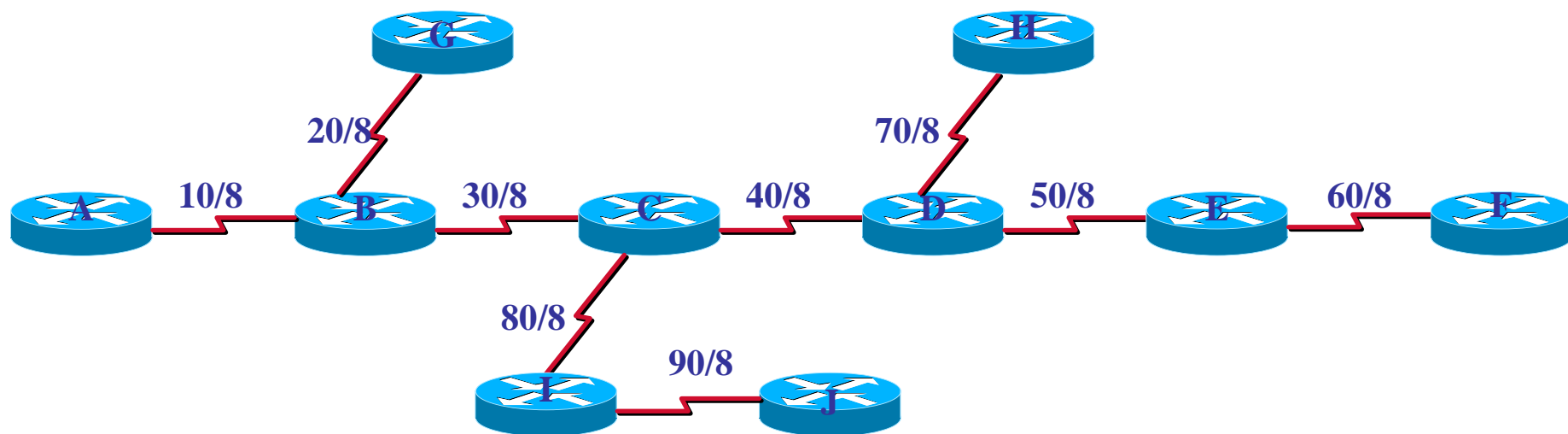
如图所示的网络中，如果在**RA**上配置静态路由来提供从内部网络来的对**Internet**的访问请求，如何实现？



对**www.yahoo.com (209.131.36.158)** 的请求 →
对**www.sohu.com (121.14.0.31)** 的请求 →
对某个游戏服务器的请求 →
对**59.61.32.211**的**QQ**视频请求 →

由于**RA**到达远端（非本地）的任何一个目标网络都需要经过某个固定的下一跳（或者固定从某个接口发送），可以在**RA**上配置默认路由。

第二章 静态路由



如图所示的拓扑结构中，共包括9个网段，正确配置各路由器的接口后，每台路由器的路由表中只有直连路由，路由表不完整，需要如何配置？

- 1、以A为例，它到达这个拓扑结构中任何一个网络均需要通过B，可否配置默认路由？
- 2、G、H等路由器上可否配置默认路由？
- 3、B是否可以配置默认路由？除去问题2中的那些路由器，还有哪些？
- 4、C、D是否可以配置默认路由？如何配置？

第三章 动态路由 - RIP

IGP与EGP

内部网关协议（**IGP, Interior Gateway Protocol**）被设计用于由一个组织控制或者管理的网络中。**IGP**被设计用来发现穿越网络的最佳路径。

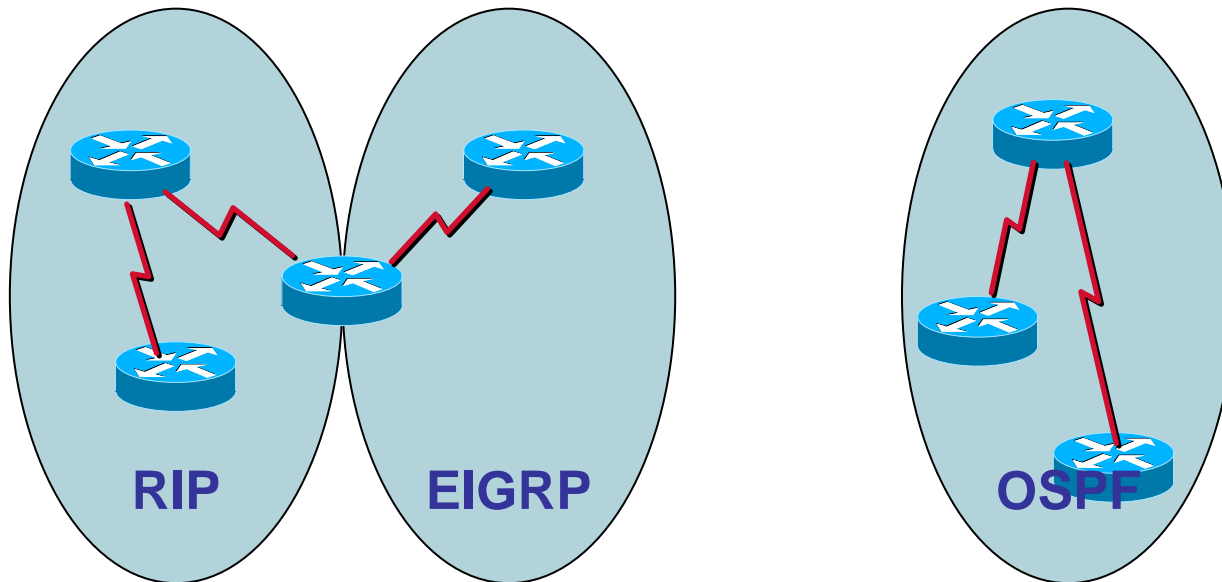
外部网络协议（**EGP, Exterior Gateway Protocol**）被设计用于两个不同组织所控制的网络之间。**EGP**必须隔离自治系统。

第三章 动态路由 - RIP

自治系统（**Autonomous System**，简称**AS**）：是处于公共管理下的网络集合，共享公共的路由选择策略。

美国**Internet**数字注册机构（**ARIN**）负责为每个**AS**分配标识编号，该编号是一个**16**比特的数字，**IGRP**和**EIGRP**在配置中使用**AS**编号。

自治系统将全球的互连网络分为更小的和更易管理的网络。每个**AS**拥有自己的规则策略集，**AS**编号将其与其他的自治系统分开。



第三章 动态路由 - RIP

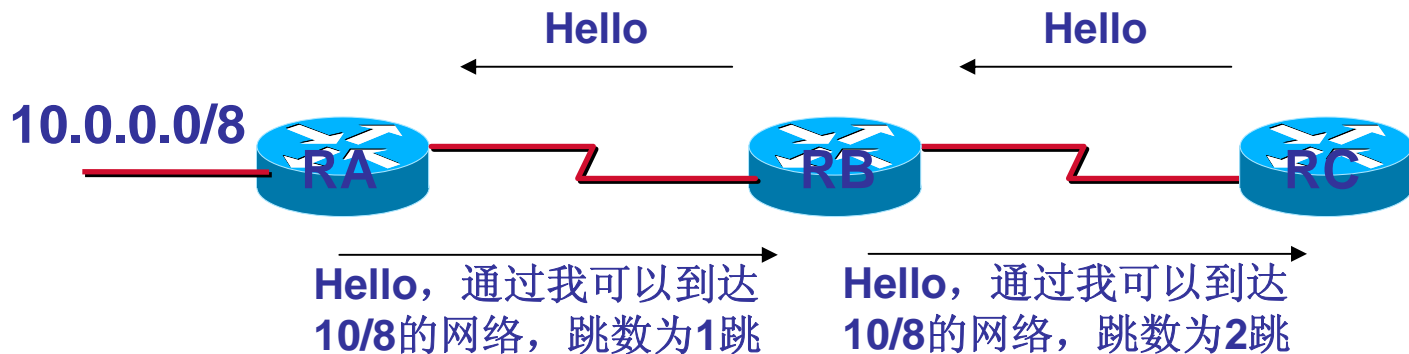
动态路由选择允许网络快速地更新和适应变化。

动态路由选择的成功基于两个功能：

- 1、路由选择表的维护；
- 2、以路由选择更新的形式，将信息适时地发布给其他路由器。

动态路由协议包括：**RIP**、**IGRP**、**EIGRP**、**OSPF**等。

度量值（**Metric**）包括：带宽、延迟、负载、可靠性、跳数、开销等。



第三章 动态路由 - RIP

路由选择算法可以分为以下两类：

距离矢量（**Distance Vector**）

链路状态（**Link State**）

距离矢量路由选择协议方法确定互连网络中任何一条链路的方向（矢量）和距离，定期地将路由选择表的拷贝从一个路由器发往另一个路由器。

链路状态路由选择协议方法也被称为最短路径优先（**SPF**），它重建整个互连网络的精确拓朴结构。

平衡混合路由选择协议方法（如**EIGRP**）结合了链路状态和距离矢量算法的特点。

比较链路状态路由协议和距离矢量路由协议，运行前者的路由器需要更多的内存并消耗更多的**CPU**资源，对路由器的性能有更高的要求。

第三章 动态路由 - RIP

链路状态路由选择使用以下内容：

链路状态通告（**LSA**， **Link State Advertisement**）

拓朴数据库

最短路径优先（**SPF**， **Shortest Path First**）算法——生成**SPF**树

路由选择表

链路状态路由选择的网络发现使用以下过程：

- 1、交换**LSA**；
- 2、每台路由器构建一个由**LSA**组成的拓朴数据库；
- 3、通过**SPF**算法计算网络的可达性，以自己为树根生成**SPF**树，使用**SPF**选择路径；
- 4、在路由表中列出最佳路径和接口。

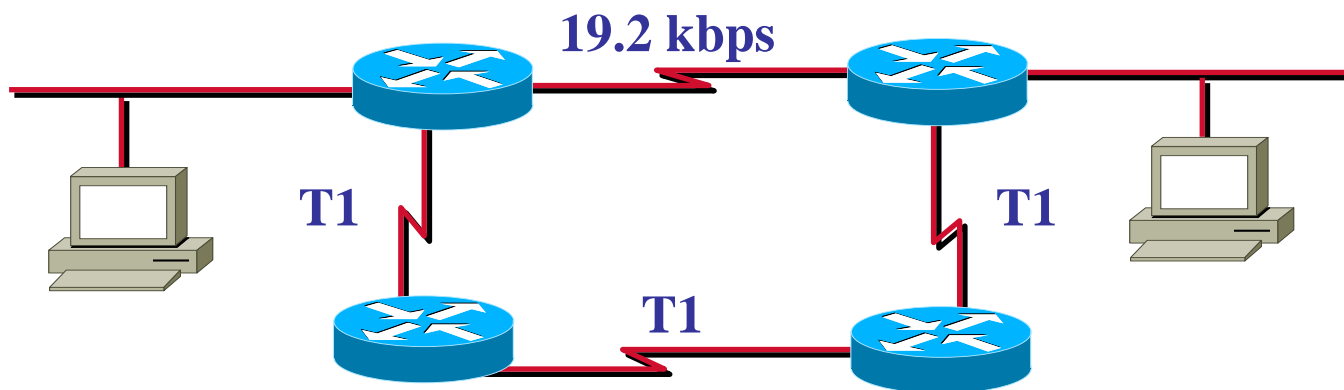
第三章 动态路由 - RIP

路由信息协议——**RIP** (**R**outing **i**nformation **P**rotocol) 是应用较早、使用较普遍的内部网关协议，适用于小型同类网络，基于**V-D**算法，使用跳数来决定最佳路径。

V-D是**Vector-Distance**（距离向量）的缩写，因此**V-D**算法又称为距离向量算法。这种算法在**Arpanet**早期用于网络中路由的计算。

距离向量路由算法将完整的路由表传给相邻路由器，然后这个路由器再把收到的表的选项加上自己的表来完成整个路由表，这个过程被称为**routing by rumor**（流言路由），因为这个路由器是从相邻路由器接收更新而非自己去发现网络的变化。

第三章 动态路由 - RIP



特点：典型的距离矢量路由选择协议

使用跳数作为路径选择的度量标准

最大跳数为**15**跳，大于**15**时，丢弃使用该路由的转发分组

默认情况下，路由选择的更新每**30**秒广播一次

分为版本**1**和版本**2**，版本**2**具有以下增强特性

- ◆能够承载附加的分组路由选择信息
- ◆认证机制以确保表更新的安全
- ◆支持子网掩码

第三章 动态路由 - RIP

RIP工作原理

运行RIP的路由器都维护一张RIP路由表。

◆下一跳（**next hop**）

◆接口表示本地出口

◆度量（**metric**）代表把数据包从本路由器送达目的站所需的花费（**cost**）。

◆RIP协议以跳数作为度量，最大有效度量为**15**，当一条路由的度量到达**16**后，那条路由就被认为无效，认为某目标网络不可达；

◆标志位标志此路由最近是否发生变化，以备触发更新时用到；

◆年龄，定时器，用于维护每条路由。若某条路由经过**180**秒后仍未被刷新，则该路由被认为不再有效，将其度量置成**16**。

目的	下一跳	接口	度量	标志	年龄
A	Local	E1	1	0	20
B	Local	E1	1	0	12
C	Router2	S1	0	0	0
D	Router2	S1	0	0	0

第三章 动态路由 - RIP

RIP工作原理

◆启用**RIP**后，将通过接口以广播的形式向邻居发送请求，请求邻居给自己发送完整的路由表。

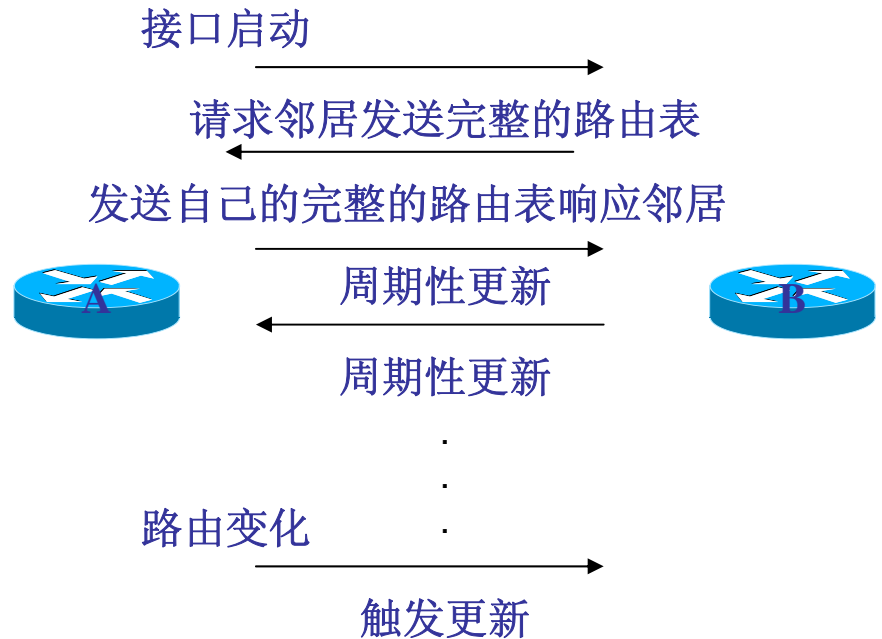
◆邻居路由器收到请求后发送路由表进行响应，即<目的，度量>。

◆接收到该响应的路由器依据度的大小来判断路由的好坏，把度量最小的一条路由放入路由表。判断过程如下：

- (1) 查看路由表中是否已有到该目的路由；
- (2) 如果没找到，则添加该路由；
- (3) 如果找到，只有在新度量更小时才更新路由，否则忽略。

◆之后两台路由器开始周期发送并更新路由表。

◆当检测到路由变化时，向邻居发送触发更新，通知路由变化。

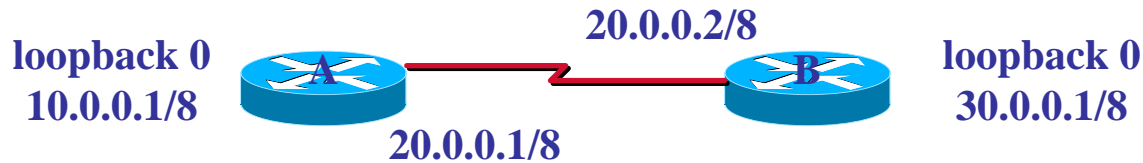


第三章 动态路由 - RIP

RIP使用计时器来调节它的性能：

- 1、更新计时（**update timer**），路由器发送路由表副本给相邻路由器的周期性时间，默认时间是**30秒**。
- 2、无效计时（**invalid timer**），如果经过**180秒**，某条路由的选项都没有得到确认，将会认为它已失效了。
- 3、保持计时器（**holddown timer**），当路由器得知某条路由无效后，将进入**holddown**状态，默认时间是**180秒**。如果在这**180秒**里，**router**接收到路由更新以后或者超过**180秒**，保持计时器停止计时。
- 4、刷新时间（**route flush timer**）：如果经过**240秒**，某条路由表项仍未得到确认，它就被从路由表中删除。

第三章 动态路由 - RIP



当两台路由器未配置**RIP**之前，两台路由器的路由表简单表示如下：

A路由器	C 10.0.0.0/8	B路由器	C 20.0.0.0/8
	C 20.0.0.0/8		C 30.0.0.0/8

接下来，在两台路由器上分别启用**RIP**

Ra(config)#router rip

Ra(config-router)#network 10.0.0.0

Ra(config-router)#network 20.0.0.0

Rb(config)#router rip

Rb(config-router)#network 20.0.0.0

Rb(config-router)#network 30.0.0.0

为查看**RIP**通过接口收、发路由请求及更新，在特权模式下 **debug ip rip**

第三章 动态路由 - RIP



```
rc(config-router)#network 20.0.0.0
```

01:22:11: RIP: sending request on Serial1 to 255.255.255.255

//RIP启动后，RC首先通过Serial 1接口以广播的形式向外发送请求

01:22:11: RIP: received v1 update from 20.0.0.1 on Serial1

01:22:11: 10.0.0.0 in 1 hops

//邻居（RB）收到请求后，发送自己的路由表作为回应，响应的内容为<10.0.0.0, 1>。

//此处还可以看出，请求和回应是即时的，RC在01:22:11秒发送请求后立刻收到了邻居的回应。

//之后，周期性每隔30秒发送路由更新。

第三章 动态路由 - RIP

Rc#show ip route rip //仅查看通过**RIP**学习到的路由
R 10.0.0.0 [120/1] via 20.0.0.1, 00:00:07, Serial1

R **RIP**的标识代码

10.0.0.0 通过**RIP**所学习到的网络

120 管理距离

1 到达目标网络的跳数

via 经过，通过

20.0.0.1 下一跳地址，到达**10.0.0.0**网络需要经过的邻居路由器的地址
或者理解为学习到该条路由的来源，关于**10.0.0.0**这条路由表
项是由**20.0.0.1**发送来的，通过**20.0.0.1**学习到

00:00:07 所学习到的时间，即这条路由是在7秒钟之前学习到，或者
是在7秒钟之前更新过

serial0 本地接口，即**Rc**是通过自己的**Serial1**接口学习到

第三章 动态路由 - RIP

Rc#show ip protocols

Routing Protocol is "rip"

Sending updates every 30 seconds, next due in 7 seconds

Invalid after 180 seconds, hold down 180, flushed after 240

//计时器：每30秒发送更新，下一次发送更新将是在7秒之后，无效时间180秒，抑制时间180秒，移除时间240秒

...

Redistributing: rip

//重分布

Default version control: send version 1, receive any version

Interface	Send	Recv	Key-chain
------------------	-------------	-------------	------------------

serial1	1	1	1 2
----------------	----------	----------	------------

//发送V1，接收V1和V2

第三章 动态路由 - RIP

Automatic network summarization is in effect

//自动网络汇总默认是生效的

Maximum path: 4

//最大路径数为4

Routing for Networks:

//路由了哪些网络

20.0.0.0

Routing Information Sources:

Gateway	Distance	Last Update
----------------	-----------------	--------------------

20.0.0.1	120	00:00:23
-----------------	------------	-----------------

//网关地址为20.0.0.1，上一次更新时间在23秒之前

Distance: (default is 120)

//管理距离默认为120

第三章 动态路由 - RIP

RIP V1是有类的（Classful）路由协议

Classful路由协议在路由更新时不携带掩码

Classful路由协议只能支持定长子网掩码（FLSM）

同一个大类网络下的子网信息当掩码长度一致时可以相互穿越。掩码长度不一致时子网信息不能传递

Classful路由协议不支持非连续的子网（Discontiguous subnet）

子网信息穿过另外一个大类网络时将在网络边界做自动汇总

Classless路由协议在路由更新时携带掩码

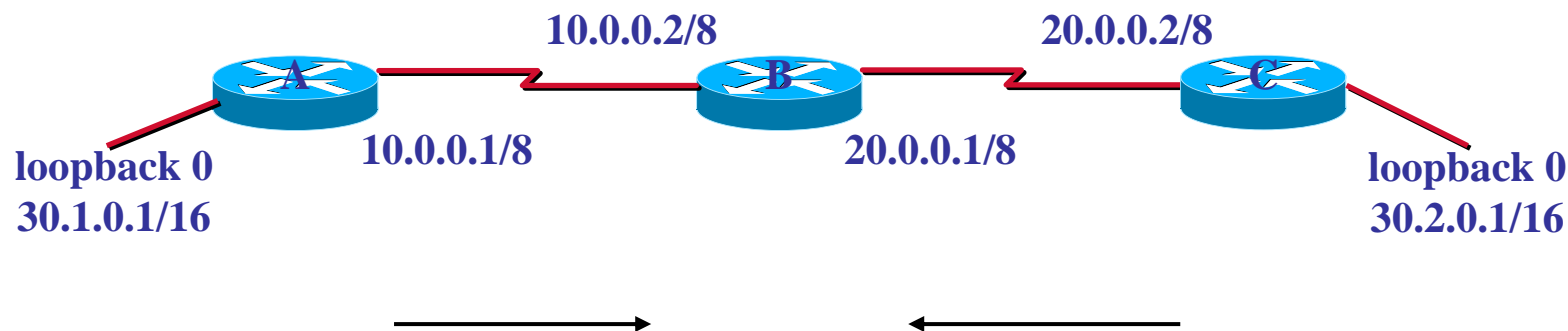
Classless路由协议能支持变长子网掩码（VLSM）

Classless路由协议可以支持非连续的子网（Discontiguous subnet）

第三章 动态路由 - RIP

自动汇总和版本导致的问题

在A和C路由器上分别启用回环接口，并重新配置RIP

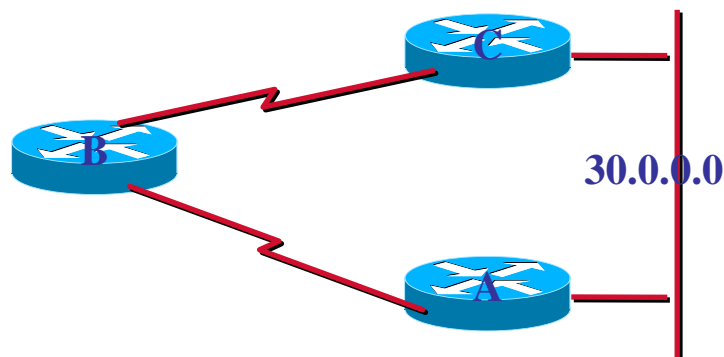


Ra发送给Rb一条关于30网
络的路由，跳数为1跳

同样的，Rc发送给Rb一条关
于30网络的路由，跳数为1跳

第三章 动态路由 - RIP

由于30属于A类地址，子网掩码默认为8位。**RIP**版本1会分别将30.1/16和30.2/16汇总为30/8，这将导致造成**Rb**错误的认为，通过**Ra**或**Rc**均可到达30/8网络，且两条路径是等值路径（等跳数）。**Rb**认为网络拓扑如下图所示：



原因：**RIP**的Datagram里面只有IP地址，没有子网掩码。

解决方法：

- 1、启用**RIP V 2**
- 2、关闭自动汇总

第三章 动态路由 - RIP

Roc#debug ip rip

注意版本1和版本2的区别，注意关闭自动汇总前后的区别

01:01:52: RIP: sending v1 update to 255.255.255.255 via Serial1 (10.0.0.1)

01:01:52: RIP: build update entries

01:01:52: network 30.0.0.0 metric 1

版本1下，发送V1更新，地址是广播地址，没有携带子网掩码

Roc(config-router)#version 2

01:02:19: RIP: sending v2 update to 224.0.0.9 via Serial1 (10.0.0.1)

01:02:19: RIP: build update entries

01:02:19: 30.0.0.0/8 via 0.0.0.0, metric 1, tag 0

启用版本2后，发送V2更新，地址是组播地址，携带有子网掩码，但子网掩码仍然为8位

第三章 动态路由 - RIP

Roc(config-router)#no auto-summary

01:03:09: RIP: sending v2 update to 224.0.0.9 via Serial1 (10.0.0.1)

01:03:09: RIP: build update entries

01:03:09: 30.1.0.0/16 via 0.0.0.0, metric 1, tag 0

关闭自动汇总后，发送更新时子网掩码为16位

第三章 动态路由 - RIP

被动接口（**Passive Interface**）只接收路由更新，不发送路由更新：

router(config-router)#passive-interface serial 0

计时器：调整这些时间来适合网络的需要：

router(config-router)#timers basic update invalid holddown flushed

管理距离：

router(config-router)#distance 130 //默认为120

最大路径数：

router(config-router)#maximum-paths 6 //默认为4

修改接口上**RIP**接收和发送的版本：

Router(config-if)#ip rip send/receive version 1 2

启用无类**IP**子网（默认启用）：

Router(config)#ip classless

第三章 动态路由 - RIP

验证：**RIP**支持验证（仅限于**V2**），验证的方式包括两种：**Clear Text**和**MD5**。



RA的主要配置

```
Ra(config)#key chain aaa
```

```
Ra(config-key-chain)#key 1
```

```
Ra(config-keychain-key)#key-string 1234
```

```
Ra(config)#interface serial 0
```

```
Ra(config-if)#ip rip authentication mode text
```

```
Ra(config-if)#ip rip authentication key-chain aaa
```

RB的主要配置

```
Rb(config)#key chain bbb
```

```
Rb(config-key-chain)#key 1
```

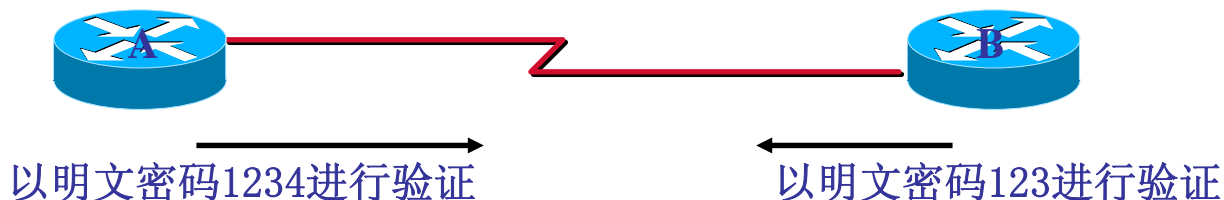
```
Rb(config-keychain-key)#key-string 1234
```

```
Rb(config)#interface serial 0
```

```
Rb(config-if)#ip rip authentication mode text
```

```
Rb(config-if)#ip rip authentication key-chain bbb
```

第三章 动态路由 - RIP



```
RA#debug ip rip
```

```
01:53:15: RIP: received packet with text authentication 123
```

```
01:53:15: RIP: ignored v2 packet from 10.0.0.2 (invalid authentication)
```

A路由器上接收到密码为123的更新包，因密码不匹配导致验证失败，丢弃更新包。

```
01:53:43: RIP: received packet with text authentication 123
```

```
01:53:43: RIP: received v2 update from 10.0.0.2 on Serial0
```

```
01:53:43:      20.0.0.0/8 via 0.0.0.0 in 1 hops
```

修改密码后，验证成功，能正确接收更新。

第三章 动态路由 - RIP

相邻的两台路由器，用于验证的key chain可以不同，key编号可以不同，但用于验证的密码必须相同。

采用明文验证方式时，可以查看到明文的密码，安全性较差。

MD5验证：

```
Rb(config-if)#ip rip authentication mode md5
```

```
Rb(config-if)#ip rip authentication key-chain bbb
```


第三章 动态路由 - RIP



路由环路的产生

1、两台路由器的路由表分别为：

RA	RB
C 10/8	C 10/8
C 20/8	

2、设第1秒时RA启用RIP，第2秒时RB启用RIP，则第2秒时的路由表为：

RA	RB
C 10/8	C 10/8
C 20/8	R 20/8 1

RA将在第31秒时发送更新，RB将在第32秒时发送更新。

3、第31秒时，RA正常更新，两台路由器的路由表保持不变，如上。

4、设第31.5秒时，20网络断开，则此刻两台路由器的路由表分别为：

RA	RB
C 10/8	C 10/8
	R 20/8 1

5、第32秒时，RB发送更新，将自己路由表中[R 20/8 1]发送给RA，同时跳数加1，变为[R 20/8 2]。而此时RA路由表中缺少到达20/8网络的路由，RA将此条路由放入路由表。此刻两台路由器的路由表分别为：

RA	RB
C 10/8	C 10/8
R 20/8 2	R 20/8 1

RA认为通过RB可以到达20/8网络，而RB又认为通过RA可以到达，错误产生。

第三章 动态路由 - RIP

网络中所有的路由器都拥有一致的认识和正确的路由选择表，这时网络被称为已经收敛。

路由选择环路的产生，使得网络产生了慢收敛。

为了防止环路的产生，可采用下列方法：

- 定义最大跳数

- 水平分割 (**Split Horizon**)

- 触发更新 (**Triggered Update**)

- 路由中毒 (**Route Poisoning**) 和毒性反转 (**Poison Reverse**)

- 抑制 (**Holddown**)

第三章 动态路由 - RIP

定义最大跳数

在任何情况下，当度量标准值超过最大值时，网络被认为不可达。

如果环路中的路由器继续相互交换错误的路由信息，跳数不断增加，总有某一时候到达最大跳数，之后发出的路由更新将会超过允许值，被认为不可达。

RIP的最大跳数为15；

IGRP的最大跳数默认为100，可修改为255。

第三章 动态路由 - RIP



水平分割

按照水平分割原则，如果关于**20/8**网络的路由更新从**RA**发出，那么**RB**就不能再返回给**RA**关于**20/8**网络的信息。

水平分割减少了错误的路由选择信息，也减少了路由选择开销。

在使用水平分割时，路由器记录下收到各路由的接口，而当这路由器通告路由时，就不会把该路由再通过那个接口送回去，即通过水平分割机制，路由器不会通过学习端口再次发送关于同一个网络的路由信息。

在该例中，路由器**RB**最初时由**S1**接口学习到**20/8**网络，它将不会把到达**20/8**网络的距离为2的错误路由再通告给**RA**。因此，一旦**RA**与**20/8**网络的连接失效，**RA**也不会因为**RB**学习到错误的路由。

第三章 动态路由 - RIP



触发更新

即立即更新，路由器一旦检测到拓扑发生变化就向邻居路由器发送更新，而不等待更新定时器期满。

本例中，**RA**在**31**秒时正常发送路由更新，在**31.5**秒时检测到**20/8**网络断开，**RA**将立即发送更新给邻居路由器**RB**，而不会等到**61**秒时再发送。

第三章 动态路由 - RIP

路由中毒

一般通过将跳数设置为最大跳数加1（即不可达）来实现。

毒性反转

一旦从一个接口学习到了一个被毒化的路由，那么这个路由作为不可达路由从同一个接口回送。

第三章 动态路由 - RIP

抑制

迫使参与协议工作的路由器，在收到关于某网络不可达的信息后的一段固定时间内，忽略任何关于该网络的路由信息。

收到来自**RA**的更新，**30/8**不可达
(之前到达**30/8**的跳数为**10**)



标记该路由不可达，启动抑制定时器

在定时器期满前，收到来自**RA**的更新，**30/8**可达

标记该路由可达，删除抑制定时器

在定时器期满前，收到来自**RC**的更新，**30/8**可达，跳数为**8**

标记该路由可达，删除抑制定时器

在定时器期满前，收到来自**RC**的更新，**30/8**可达，跳数为**11**

忽略该更新

第四章 动态路由 - IGRP

IGRP，内部网关路由协议（**Interior Gateway Routing Protocol**），是由**Cisco**公司在八十年代中期设计。内部网关路由协议使用复合度量，复合度量包括下列五个方面：

- 1、带宽（**Bandwidth**）
- 2、延迟（**Delay**）
- 3、负荷（**load**）
- 4、可靠性（**Reliability**）
- 5、最大传输单元（**MTU**）

第四章 动态路由 - IGRP

IGRP的两个局限：

- 1、**IGRP**是**Cisco**私有路由协议，不能在其他厂家的设备中使用。
- 2、**IGRP**是一个有类距离向量路由协议，不能很好地扩展。

IGRP发送整个路由表的定期广播。**IGRP**初始化时，类似于**RIP**，通过接口向广播地址发送路由请求。然后**IGRP**检查收到的更新，并周期性发送更新。

IGRP更新中认识三种路由：

- 1、内部(**Interior**)路由：直接与路由器接口连接的网络。
- 2、系统(**system**)路由：在同一**IGRP**自治系统内部，其他邻居通知的路由。
- 3、外部(**Exterior**)路由：从不同自治系统学习的路由。

第四章 动态路由 - IGRP

IGRP的度量

Bellman-Ford算法用下列方程计算路由的总度量。

Metric=[**K1** × 带宽+(**K2** × 带宽)/(256-负载)+**K3** × 延迟] × [**K5**/(可靠性+**K4**)]

默认情况下，**K2**、**K4**、**K5**取值为0，**K1**、**K3**取值为1，计算公式简化为**Metric**= $10^7 / \text{Min}_{\text{BW}} + \sum \text{Delay} / 10$

从公式可以看出，如果带宽越小、延时越大，则度量值越大，路径越差。

K值可通过该语句修改，但如果相邻路由器的**K**值取值不同，两台路由器将不能交换路由信息。

Router(config-router)#metric weights tos k1 k2 k3 k4 k5

Router(config-router)#default-metric bandwidth delay reliability load mtu

第四章 动态路由 - IGRP

IGRP默认的最大跳数为100，最大可改为255

Router(config-router)#metric maximum-hops <1-255>

IGRP的默认管理距离为100

Router(config-router)#distance <1-255>

IGRP计时器（Timers）

Router(config-router)#TIMERS BASIC	update	invalid	holddown	flush
默认的计时器为	90	270	280	630

要关闭保持定时器，在路由器配置方式中输入下列命令：

Router(config-router)#no metric holddown

第四章 动态路由 - IGRP

负载均衡(Load Balancing)

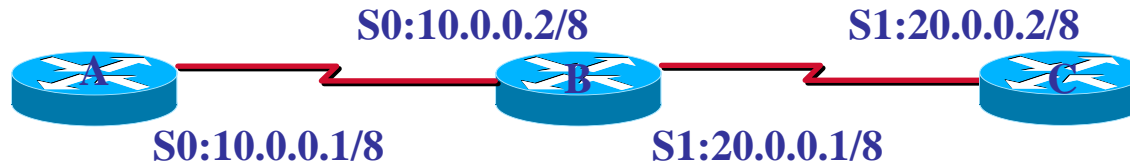
负载均衡就是路由器采用多条路径发送同一目标的数据，提高发送速度，减少在单一路径上的流量。要改变负载均衡IGRP的路径数，在路由器配置方式中输入下列命令：

Router(config-router)#maximum-paths <1-6>

和RIP类似，IGRP和EIGRP默认可在4条路径上做负载均衡，最大可修改为6条。

但和RIP不同，IGRP与EIGRP可以在不等值路径上做负载均衡，而其他路由协议只能在等值路径上负载均衡。

第四章 动态路由 - IGRP



如图配置网络，以RA为例，首先开启debug:

```
Ra#debug ip igrp events
```

```
Ra(config)#router igrp 10
```

```
Ra(config-router)#network 10.0.0.0
```

```
01:29:42: IGRP: broadcasting request on Ethernet0
```

```
01:29:42: IGRP: sending update to 255.255.255.255 via Serial0 (10.0.0.1)
```

类似RIP，IGRP被启用后通过接口以广播地址向邻居发送路由请求

```
01:29:42: IGRP: Update contains 0 interior, 0 system, and 0 exterior routes.
```

IGRP的三种路由：内部路由、系统路由、外部路由

第四章 动态路由 - IGRP

Ra#show ip route igrp

I 20.0.0.0/8 [100/10476] via 10.0.0.2, 00:00:02, Serial0

I 通过**IGRP**学习到的路由

20.0.0.0/8 远程网络

100 **IGRP**的管理距离

10476 到达**20.0.0.0**网络的度量值，计算如下：

$$10476 = 10^7 / 1544 + 20000 * 2 / 10$$

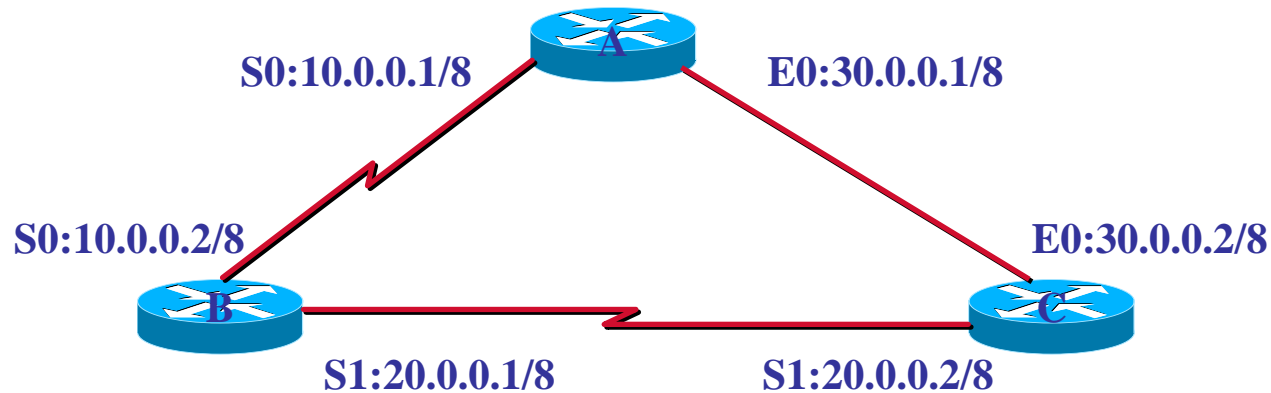
1544为到达目标网络的链路的带宽

20000为**Serial**接口的延时，经过两个**Serial**接口

10.0.0.2 下一跳地址

00:00:02 学习到的时间或上一次更新是在**2**秒之前

第四章 动态路由 - IGRP



修改网络拓扑如图，重新查看三台路由器的路由表，如下：

Ra: I 20.0.0.0/8 [100/8576] via 30.0.0.2, 00:00:01, Ethernet0

Rb: I 30.0.0.0/8 [100/8576] via 20.0.0.2, 00:00:03, Serial1

[100/8576] via 10.0.0.1, 00:00:03, Serial0

Rc#: I 10.0.0.0/8 [100/8576] via 30.0.0.1, 00:00:02, Ethernet0

注意到Ra到达20.0.0.0网络的路径发生了变化，改由Ethernet0接口发送。

第四章 动态路由 - IGRP

原因：

Ra到达**20.0.0.0/8**网络的路由

原来的度量值= $10^7/1544+2*2000$ （两个串口延时）=**10476**

新的度量值= $10^7/1544+2000$ （串口延时）+**100**（以太网延时）=**8576**

由于延时发生了改变，引起度量值的变化，**Ra**发现了一条度量值更小的更好的路径。

而**Rb**发现从**Serial 0**和**Serial 1**接口到达**30.0.0.0**网络的两条路径的度量值相等，在路由表中出现两条等值路径。

Rc同**Ra**。

第四章 动态路由 - IGRP

Ra#show ip protocols

Routing Protocol is "igrp 10"

Sending updates every 90 seconds, next due in 19 seconds

//计时器

Invalid after 270 seconds, hold down 280, flushed after 630

...

IGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0

//K值

IGRP maximum hopcount 100

//默认最大跳数为100跳

IGRP maximum metric variance 1

//变化值默认为1

Redistributing: igrp 10

//重分布

Maximum path: 4

//默认最大路径数为4

Routing for Networks:

//路由了哪些网络

20.0.0.0

30.0.0.0

Routing Information Sources:

Gateway	Distance	Last Update
---------	----------	-------------

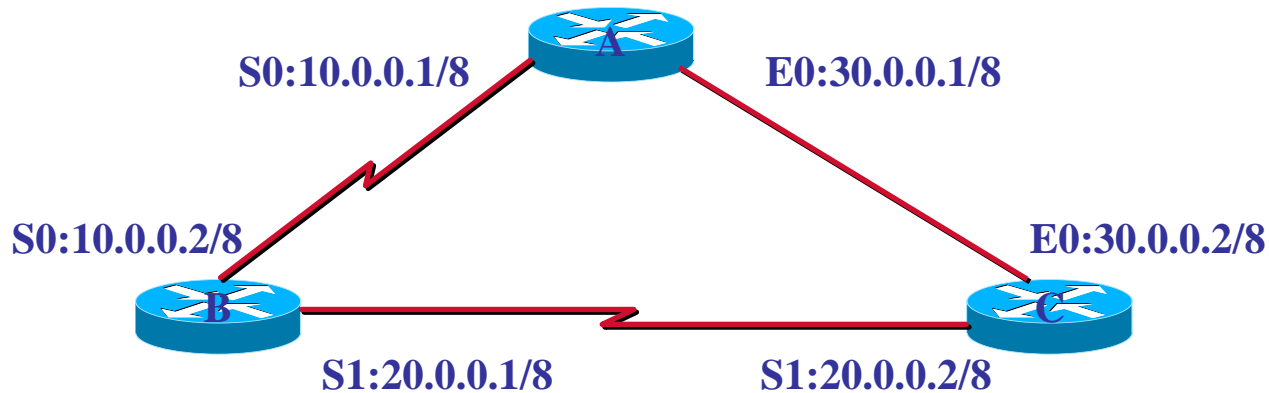
20.0.0.1	100	00:01:08
----------	-----	----------

30.0.0.1	100	00:00:00
----------	-----	----------

Distance: (default is 100)

//管理距离默认为100

第四章 动态路由 - IGRP



Variance取值范围从1到128，默认为1。根据**Variance**取值的不同，可以决定有哪些路径能够进入到路由表。

当前从**Ra**出发，经**E0**到达20/8网络的度量值为8576；经**S0**到达20/8网络的度量值为10476。

由于默认情况下**Variance=1**，此时只有具有最小度量值的路由表项才能进入到路由表，所以在**Ra**和**Rc**的路由表中只能查看到一条最好的路径。而**Rb**的两条路径的度量值相等，都是最小度量，所以路由表中有两条路径。

第四章 动态路由 - IGRP

最小度量值 \leq 可能进入到路由表的路径度量值 \leq 最小度量值 * **Variance**

此时，若修改**Variance**值取**2**，则度量值在**8576**到**17152**（即**8576**×**2**）之间的，均可进入到路由表。

Ra(config-router)#variance 2

Ra#show ip route igrp

I 20.0.0.0/8 [100/8576] via 30.0.0.2, 00:00:03, Ethernet0
[100/10476] via 20.0.0.2, 00:00:03, Serial1

发现**Ra**此时的路由表中，到达**20**网络有两条不等值路径，可以利用这两条路径实现负载均衡。

第五章 动态路由 - EIGRP

EIGRP是典型的平衡混合路由选择协议，融合了距离矢量和链路状态两种协议的优点，使用扩散更新算法（**DUAL**），实现了很高的路由性能。

EIGRP的四个组件：

1、PDMs（Protocol-Dependent Modules）（**PDMs**，协议独立模块，支持**IP**、**IPX**、**AppleTalk**等多种可路由协议）

2、Reliable Transport Protocol (RTP，可靠传输协议)

RTP负责**EIGRP**数据包到所有邻居的有保证和按顺序的传输。**RTP**确保在相邻路由器间正在进行的通信能够被维持，它为邻居维护了一张重传表，该表指示还没有被邻居确认的数据包，未确认的可靠数据包最多可以被重传**16**次或直到保持时间超时，以它们当中时间更长的那个为限。

3、Neighbor Discovery/Recovery (邻居发现/恢复)

4、Diffusing Update Algorithm（DUAL，扩散更新算法）

第五章 动态路由 - EIGRP

运行**EIGRP**的路由器之间形成邻居关系并交换路由信息。相邻路由器之间通过周期性发送和接收**Hello**包来保持并维护邻居关系。当链路带宽 $\geq T1$ 时，**hello**时间为5秒，保持时间为15秒；当链路带宽 $< T1$ 时，**hello**时间为60秒，保持时间为180秒。

运行**EIGRP**的路由器存储所有与其相邻路由器的路由表信息，以便快速适应路由变化；如果没有合适的路由存在，**EIGRP**将查询其相邻的路由器，以发现可以替换的路由。

采用触发更新，即只在路由器度量改变或拓扑出现变化时发送部分更新信息。

支持可变长子网掩码（**VLSM**）和不连续的子网，支持对自动路由汇总功能的设定。

支持多种网络层协议，除**IP**协议外、还支持**IPX**、**AppleTalk**等。

同时维护邻居表、拓扑表和路由表。

使用**DUAL**算法，具有很好的路由收敛特性。

具有相同自治系统号的**EIGRP**和**IGRP**之间彼此交换路由信息。

第五章 动态路由 - EIGRP

邻居关系

EIGRP使用**Hello**包来建立与维护邻居路由器的邻居关系。

EIGRP维护邻居表，存储邻居的路由器信息，包括邻居路由器的**IP**地址、保持时间间隔、平滑往返定时器（**SRTT**）和队列信息，可以帮助确定何时发生了需要传递到邻居路由器的拓扑改变。

只有两个邻居启动通信时，**EIGRP**才通知整个路由表。这时两个邻居相互通知整个路由表。学习到邻居的直接连接和已知路由之后，只传递路由表的改变部分。

EIGRP不广播**EIGRP**分组，而是向**224.0.0.10**发送组播**Hello**。每个**Hello**分组包含**EIGRP**版本号、**AS**号码、**K**值和保持时间。要和邻居路由器建立邻居关系，就要使用相同**AS**号码和**K**值。

第五章 动态路由 - EIGRP

EIGRP使用扩散更新算法（**DUAL, Diffusing Update Algorithm**）进行度量计算，可以快速聚合，这个算法具有下列功能：

- 1、备份路由决定（如果有）
- 2、支持可变长度子网掩码（**VLSM**）
- 3、动态路由恢复
- 4、查询邻居的未知替换路由
- 5、在找不到路由时发送替换路由查询

DUAL最大的优点是加速收敛，只在需要时才重新计算路由。

三种情形使**DUAL**重新计算：

- 1、找不到替换路由。
- 2、新的最佳路由仍然通过原先的后继。
- 3、新的最佳的路由不通过可行后继。

第五章 动态路由 - EIGRP

EIGRP有5种协议报文：

Hello： 建立邻居关系，**224.0.0.10**，不需要确认

Update： 发送路由更新。第一次为组播，如果邻居没有返回确认，以单播重传，最多重传**16**次

Query： 向邻居查询路由。当**EIGRP**丢失可行后继路由，会向邻居发**query**包，查询到目标网络路由。发送查询包之后，最多等待**300s**。如果只有一个邻居，发送单播；如果有多个邻居，发送组播

Reply： 对**query** 的回复。当**EIGRP**路由器向邻居发查询包时，如果邻居有到目的地的路由，将会返回**reply**包。**Reply**总是单播。

上**3**种报文需要进行显式确认（即每个报文需要单独确认），并设置序列号以便重传，次数限制为**16**。

ACK： 确认。**Update**、**Query**、**Reply**都需要确认，**Ack**总是单播。

由于**DUAL**的机制需要，**EIGRP**必须保证可靠传输，这是由**RTP**协议来完成的。

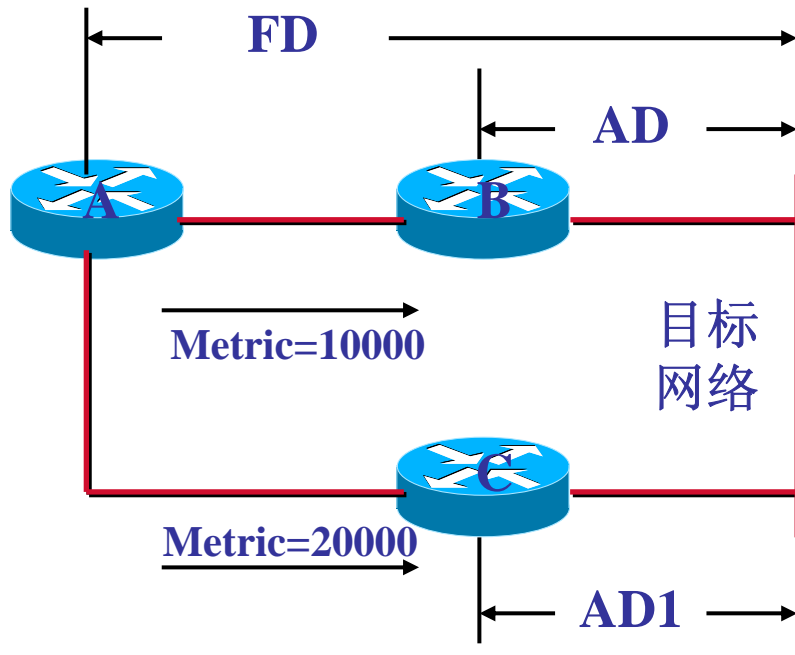
第五章 动态路由 - EIGRP

路由标志：路由标志区别通过不同**EIGRP**会话学习的路由。定义不同**AS**号之后，**EIGRP**可以在一个路由器上运行多个会话。使用相同**AS**号的路由器相互交流，共享路由信息，包括路由学习和拓扑改变。内部**EIGRP**路由的管理距离为**90**，外部**EIGRP**路由的管理距离为**170**。

路由计算：**IGRP**更新使用**24**位格式，而**EIGRP**更新用**32**位格式增加精度，**EIGRP**的度量值是**IGRP**度量值的**256**倍。

冗余链路计算：拓扑数据库存储所有到达目标的已知路由并计算最佳路径的度量。计算出最佳路由之后，将其放进路由表中，拓扑表中最多可以存储六个到达目标的路由，即**EIGRP**可以计算到达目标的最多六个冗余路径。利用到达目标的已知度量，路由器确定哪个路径是主路径，哪个路径是备份路径。具有最小度量的主路由成为**Successor**（后继），被加入路由表，其它路由器成为**Feasible Successor**（可行性后继）。

第五章 动态路由 - EIGRP



FD: Feasible Distance, 可行距离, 具有最低开销的路径度量值。

AD: Advised Distance, 通告距离, 指下一跳路由器到目标网络的路径开销, 即邻居的可行距离。也被称为 **RD, Reported Distance**。

Successor: 后继, 即到达目标网络的下一跳。

FS: Feasible Successor, 可行后继, 即到达目标网络的备份路径。

A通过B到达目标网络的度量值为10000, 通过C到达目标网络的度量值为20000, 所以当前路径为A→B→目标, B成为Successor。

C要成为FS的前提是: C到达目标网络的度量值, 要小于当前的FD。即 $AD1 < 10000$ 。

第五章 动态路由 - EIGRP

更新与改变

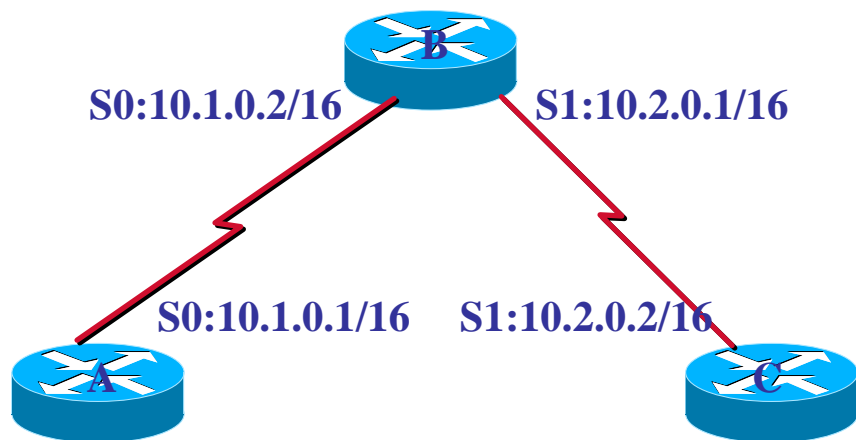
更新有两种情况，如果路由更新包含更佳度量或新路由，则路由器交换信息。如果路由更新信息显示网络无法访问或度量更差，则要寻找替换路径。寻找替换路径时，路由器首先去搜索拓扑数据库中的可行后继。如果没有可行后继，则组播查询所有邻居路由器。根据邻居路由器响应查询的情况，采用不同路径。可能发生两个操作：

- 1、如果最终发现路由信息，则将路由加进路由表中并发送更新。
- 2、如果邻居路由器的响应不包含路由信息，则从拓扑表和路由表中删除这个路由。

更新路由表之后，新信息通过组播发送给所有邻居路由器。

RTP可以保证**EIGRP**路由更新按顺序送达。

第五章 动态路由 - EIGRP



以B为例：

```
Rb(config)#router eigrp 10
```

```
Rb(config-router)#network 10.0.0.0
```

或

```
Rb(config-router)#network 10.1.0.0 0.0.255.255
```

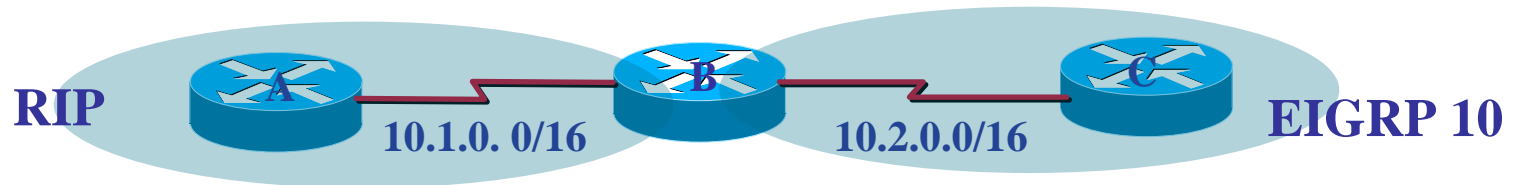
```
Rb(config-router)#network 10.2.0.0 0.0.255.255
```

第五章 动态路由 - EIGRP

与**IGRP**和**RIP**不同，**EIGRP**在宣告网络时，如果是主网地址（即**A**、**B**、**C**类的主网，没有划分子网的网络），只需输入此网络地址；如果是子网的话，则必须在网络号后面写入反掩码。

反掩码是用广播地址减去子网掩码得到的地址。

也可以在对子网的声明中只写入主网的网络地址，这表明此网络的所有子网都加入了**EIGRP**路由进程。

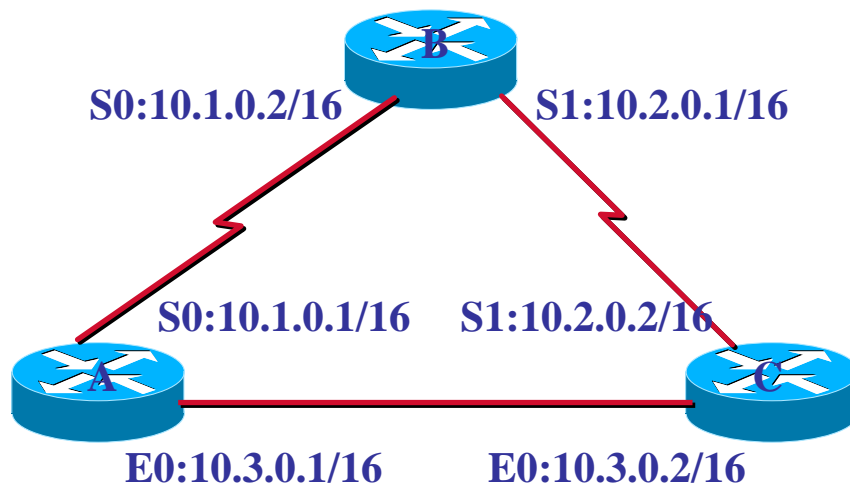


如果网络如图所示，则需要如下配置

```
RB(config)#router eigrp 10
```

```
Rb(config-router)#network 10.2.0.0 0.0.255.255
```

第五章 动态路由 - EIGRP



修改网络拓扑，分别查看每台路由器的路由表和拓扑表。
可以发现，路由表中只有到达目标网络的最佳路径，但拓扑表中可以有多个路径。

Q: 在何种情况下，运行EIGRP的路由器在何种情况下可以有备份路由（FS）？

修改配置，查看结果。

第五章 动态路由 - EIGRP

查看路由表

show ip route (eigrp)

查看拓扑表

show ip eigrp topology

列出由**EIGRP**协议所获取的所有路由信息，但并不是所有这些信息都进入路由表并被路由器所使用，只有最佳的路由才被使用，即度量值最小的路由。

查看邻居表

show ip eigrp neighbors (detail)

查看协议

show ip protocol

第五章 动态路由 - EIGRP

排错:

debug ip eigrp

debug ip eigrp summary

debug eigrp packets

debug ip eigrp as no

debug eigrp neighbors

debug eigrp transmit

EIGRP中默认设置使用接口带宽的**50%**，这个默认值可以在接口模式下修改:

Router(config-if)#ip bandwidth-percent eigrp as-number percent

第五章 动态路由 - EIGRP

配置**EIGRP**的验证：

```
Router(config)#key chain au
```

```
//定义一个名为au的key chain
```

```
Router(config-key-chain)#key 1
```

```
Router(config-keychain-key)#key-string cisco
```

```
//用于验证的密码为cisco
```

```
Router(config)# #interface serial 0
```

```
Router(config)# ip authentication mode eigrp 10 md5
```

```
//eigrp 10的自治系统下采用md5的验证方式
```

```
Router(config)# ip authentication key-chain eigrp 10 au
```

```
//eigrp 10的自治系统下调用之前配置的名为au的key chain进行验证
```

第六章 动态路由 - OSPF

OSPF（Open Shortest Path First，开放式最短路径优先），是一种链路状态路由协议。

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。所谓链路状态是指路由器接口的状态，如**UP，DOWN，IP**及网络类型等。

链路状态信息通过链路状态公告（**LSA，Link State Advertisement**）发布到每台路由器，而运行距离矢量路由协议的路由器是将部分或全部的路由表传递给与其相邻的路由器。

每台路由器通过**LSA**信息建立一个关于网络的拓扑数据库。

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，运行**OSPF**的路由器使用这些最短路径来构造路由表。

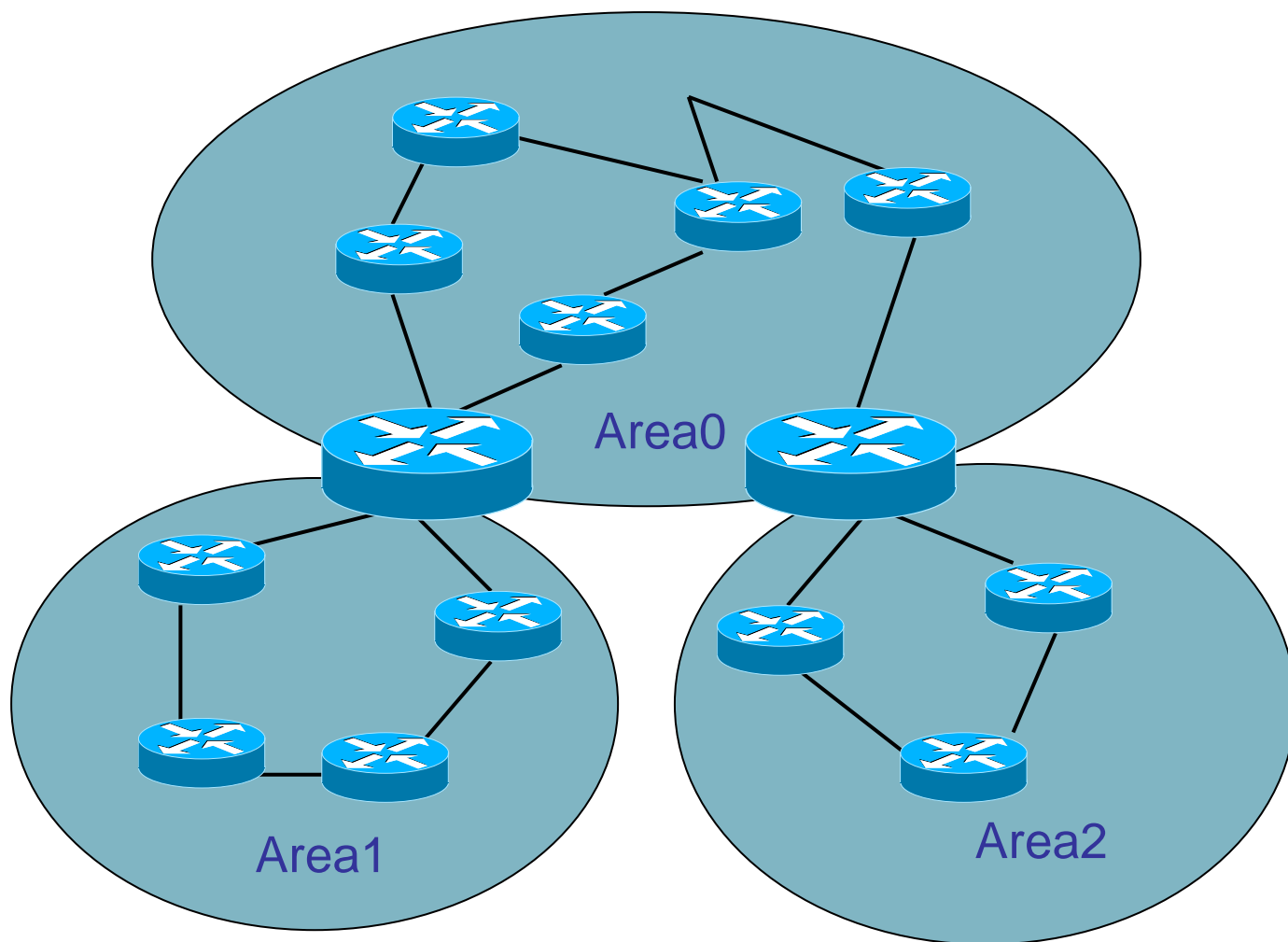
第六章 动态路由 - OSPF

OSPF定义的**AS**（自治系统）是指在用链路状态协议时，交换路由信息的一组路由器。

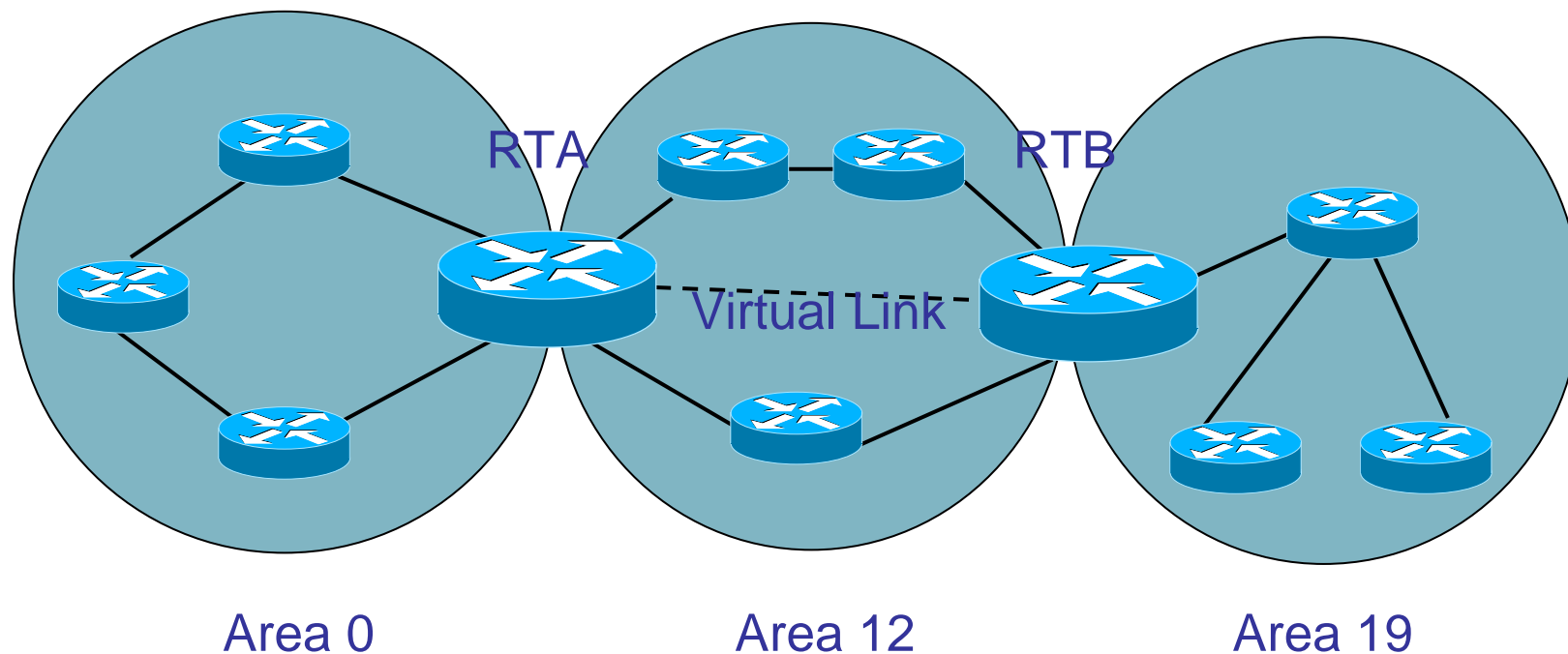
OSPF是一种层次化的路由选择协议，使用区域（**Area**）来为自治系统分段。

区域**0**是一个**OSPF**网络中所必须的区域，也称为主干区域（**Backbone Area**），其他所有区域要求通过区域**0**互连到一起。

第六章 动态路由 - OSPF



第六章 动态路由 - OSPF



第六章 动态路由 - OSPF

OSPF的数据包格式

在OSPF路由协议的数据包中，其数据包头长为24个字节，包含如下8个字段：

- * **Version number:** 所采用的OSPF路由协议的版本。

- * **Type:** 定义OSPF数据包类型。

- Hello:** 用于建立和维护相邻的两个OSPF路由器的关系，该数据包是周期性地发送的。

- Database Description:** 用于描述整个数据库，该数据包仅在OSPF初始化时发送。

- Link state request:** 用于向相邻的OSPF路由器请求部分或全部的数据，这种数据包是在当路由器发现其数据已经过期时才发送的。

- Link state update:** 是对LSR的响应，即通常所说的LSA数据包。

- Link state acknowledgment:** 是对LSA数据包的响应。

第六章 动态路由 - OSPF

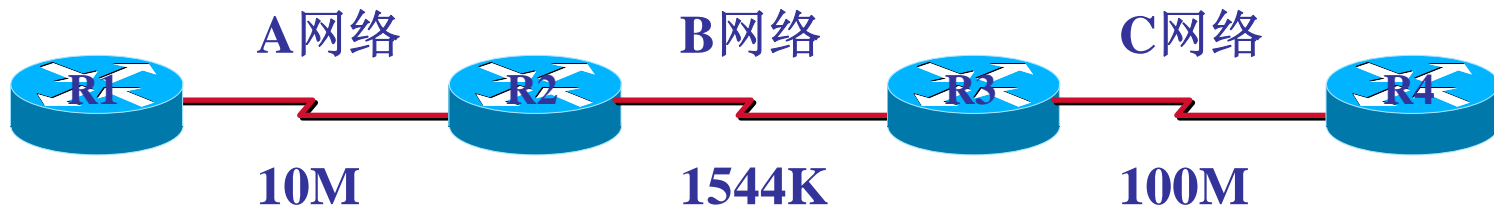
- * **Packet length:** 定义整个数据包的长度。
- * **Router ID:** 用于描述数据包的源地址，以IP地址的形式表示。
- * **Area ID:** 用于区分OSPF数据包属于的区域号，所有的OSPF数据包都属于一个特定的OSPF区域。
- * **Checksum:** 校验位，用于标记数据包在传递时有无误码。
- * **Authentication type:** 定义OSPF验证类型。
- * **Authentication:** 包含OSPF验证信息，长为8个字节。

第六章 动态路由 - OSPF

SPF算法及最短路径树

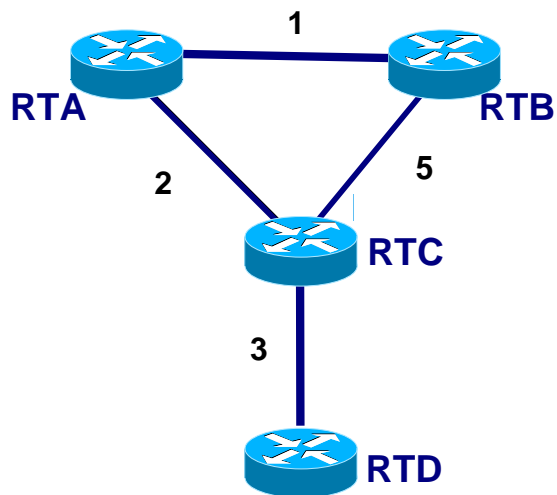
SPF（最短路径优先）算法是**OSPF**协议的基础。**SPF**算法也被称为**Dijkstra**算法。该算法将每一个路由器作为根（**ROOT**）来计算其到每一个目的路由器的距离。每一个路由器根据一个统一的数据库计算出拓扑结构图，该结构图类似于一棵树，称为最短路径树。在**OSPF**路由协议中，最短路径树的树干长度，即**OSPF**路由器至每一个目的路由器的距离，称为**OSPF**的开销（ $\text{Cost} = \sum 100 \times 10^6 / \text{链路带宽}$ ）。

其中，链路带宽的单位为**bps**。这表明，**OSPF**的**Cost**与链路的带宽成反比，带宽越高，**Cost**越小。例如，**FDDI**或快速以太网的**Cost**为1，**2M**串行链路的**Cost**为48，**10M**以太网的**Cost**为10等。

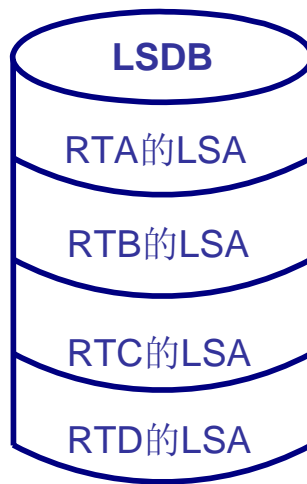


则**R1**到**A网络**的开销为10，到**B网络**的开销为 $10+64=74$ ，到**C网络**的开销为 $10+64+1=75$ 。

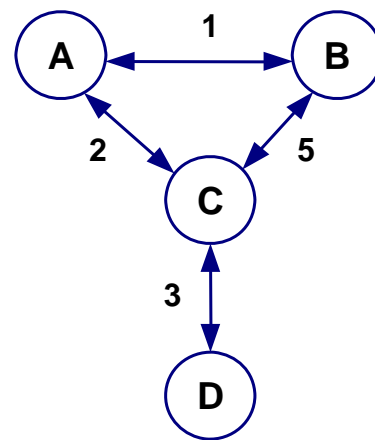
第六章 动态路由 - OSPF



(一) 网络的拓扑结构

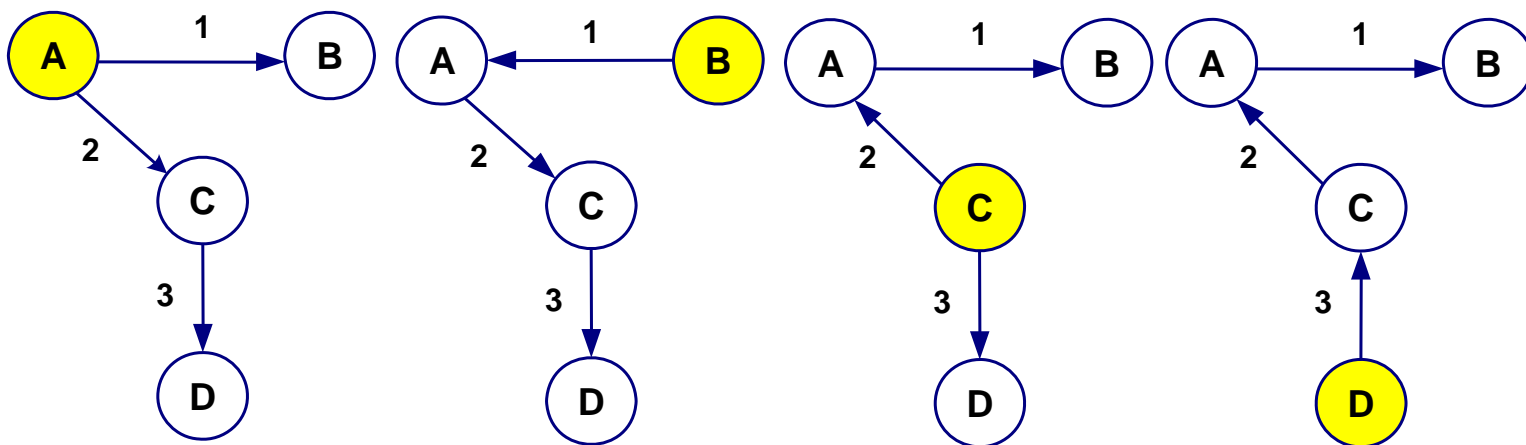


(二) 每台路由器的链路状态数据库



(三) 由链路状态数据库得到的带权有向图

第六章 动态路由 - OSPF



(四) 每台路由器分别以自己为根节点计算最小生成树

第六章 动态路由 - OSPF

OSPF 链路状态的算法非常简单，概括为以下四个步骤：

1、当路由器初始化或当网络结构发生变化（例如增减路由器，链路状态发生变化等）时，路由器会产生链路状态通告**LSA**，该数据包里包含路由器上所有相连链路，即所有端口的状态信息。

2、所有路由器会通过洪泛（**Flooding**）来交换链路状态数据。

洪泛是指路由器将其**LSA**数据包传送给所有与其相邻的路由器，邻居路由器根据所收到的链路状态信息更新自己的数据库，并再次将该链路状态信息转送给与其相邻的路由器，直至稳定的一个过程。

3、当网络重新稳定下来，或者说**OSPF**路由协议收敛下来时，所有的路由器会根据其各自的链路状态信息数据库计算出各自的路由表。该路由表中包含路由器到每一个可到达目的地的**Cost**以及到达该目的地的下一个路由器（**next-hop**）。

4、当网络状态比较稳定时，网络中传递的链路状态信息是较少的，也就是说，当网络稳定时，网络中是比较安静的。这也正是链路状态路由协议区别与距离矢量路由协议的一大特点。

第六章 动态路由 - OSPF

建立OSPF邻居关系

OSPF路由协议通过建立交互关系来交换路由信息，但是并不是所有相邻的路由器会建立**OSPF**交互关系。

OSPF协议通过**Hello**报文来建立和维护相邻关系，同时也用其来保证相邻路由器之间的双向通信。**OSPF**路由器会周期性地发送**Hello**数据包，当这个路由器看到自身被列于其它路由器的**Hello**数据包里时，这两个路由器之间建立起双向通信。在多路访问（**MultiAccess**）的网络环境中，**Hello**数据包还用于发现指定路由器（**Designated Router**），通过**DR**来控制与哪些路由器建立交互关系。

两个**OSPF**路由器建立双向通信这后的第二个步骤是进行数据库的同步，数据库同步是所有链路状态路由协议最大的共性。在**OSPF**路由协议中，数据库同步关系仅仅在建立邻居关系的路由器之间保持。

数据库同步通过数据库描述（**DBD, Database Description Packets**）来进行。**OSPF**路由器周期性地产生数据库描述数据包，该数据包携带有序列号，并将这些数据包向相邻路由器广播。若发现接收到的序列号比自身的序列号大，则会针对序列号较大的数据发出请求，并用请求得到的数据来更新本地链路状态数据库。

第六章 动态路由 - OSPF

建立完全的OSPF邻居关系的7个步骤：

1、Down：这是OSPF建立交互关系的初始状态，表示在一定时间之内没有接收到从邻居路由器发送来的Hello包。在非广播网络环境下，OSPF路由器还可能对处于Down状态的路由器发送Hello数据包。

2、Init：在该状态下，OSPF路由器已经接收到相邻路由器发送来的Hello数据包，但自身的ID并没有出现在该Hello数据包内。双向的通信还没有建立起来。

3、2-Way：这个状态是真正建立交互的开始。在这个状态，路由器看到自身已经处于相邻路由器的Hello数据包内，双向通信已经建立。指定路由器DR及备份指定路由器BDR的选举正是在这个状态完成的。在这个状态，OSPF路由器还可以根据其中的一个路由器是否指定路由器或是根据链路是否点对点或虚拟链路来决定是否建立交互关系。

第六章 动态路由 - OSPF

4、Exstart: 这个状态是建立交互状态的第一个步骤。在这个状态，路由器要决定用于数据交换初始的数据库描述数据包的序列号，以保证路由器得到的永远是最新的链路状态信息。同时，在这个状态路由器还必须决定路由器之间的主备（**Master/Slave**）关系，处于主控地位的路由器会向处于备份地位的路由器请求链路状态信息。

5、Exchange: 路由器向相邻的**OSPF**路由器发送数据库描述数据包来交换链路状态信息，每一个数据包都有一个序列号。在这个状态，路由器还可能向相邻路由器发送链路状态请求。此时，**OSPF**处于**Flood**状态。

6、Loading: 该状态下，**OSPF**路由器会就其发现的相邻路由器新的链路状态数据及自身已经过期的数据向相邻路由器提出请求，并等待相邻路由器的回答。

7、Full: 两个**OSPF**路由器建立交互关系的最后一个状态。这时，建立起交互关系的路由器之间已经完成了数据库同步的工作，它们的链路状态数据库已经一致。

第六章 动态路由 - OSPF

Router-id: 一个路由器的**ID**是该路由器的标识，可以是指该路由器的环回端口或是该路由器上活动的物理接口中最大的**IP**地址，也可以通过**router-id**手工配置。

若如下配置：

- 1、**Router(config)#router ospf 1**
- 2、**Router(config-router)#router-id 2.2.2.2**
- 3、**Router(config)#interface loopback 0**
- 4、**Router(config-if)#ip address 10.0.0.1 255.0.0.0**
- 5、**Router(config)#interface ethernet 0**
- 6、**Router(config-if)#ip address 20.0.0.1 255.0.0.0**
- 7、**Router(config)#interface serial 0**
- 8、**Router(config-if)#ip address 30.0.0.1 255.0.0.0**
- 9、**Router(config-if)#shutdown**

第六章 动态路由 - OSPF

Router ID产生的顺序

- 1、查找有没有**Router-id**的配置语句；
- 2、若没有手工配置**Router-id**，则查找有没有回环接口，如果有多个回环接口，则选取其中**IP**地址最大的；
- 3、如果没有配置**Router-id**和回环接口，则查找物理接口，该接口必须是活动的（**no shutdown**），如果有多个活动的物理接口，同样选取其中**IP**地址最大的。

若路由器如上配置，则**router id**为**2.2.2.2**

若删除前两条语句，则**router id**为**10.0.0.1**

若删除前四条语句，则**router id**为**20.0.0.1**（虽然**Serial 0**接口的**IP**地址比**Ethernet 0**的大，但该接口处于**shutdown**状态，不能作为**router id**）

第六章 动态路由 - OSPF

DR: Designated Router, 指定路由器

BDR: Backup Designated Router, 备份指定路由器

DR的选举是通过**OSPF**的**Hello**数据包来完成的。在**OSPF**路由协议初始化的过程中, 会通过**Hello**数据包在一个多路访问的网段上选出一个**ID**最大的路由器作为**DR**, 并且选出**ID**次大的路由器作为**BDR**, **BDR**在**DR**失效后能自动提升为**DR**。

OSPF用**DR**保持在一个**LAN**内的所有路由。这样减少了在一个**LAN**内的路由更新, 节省了**LAN**带宽。连接到同一个**LAN**上的**OSPF**路由器只有当他们自身的路由表没有目标的地址项目时, 才向指派路由器请示一个路由。为了使网络有效和有冗余, **OSPF**同时启用了**BDR**。

当一个网段上的**DR**和**BDR**选择产生后, 该网段上的其余所有路由器都只与**DR**及**BDR**建立相邻关系。

第六章 动态路由 - OSPF



DR和BDR的选举不仅仅考虑到**Router ID**的大小，还要比较**OSPF**的端口优先级。

端口优先级取值范围从**0**到**255**，数值越大，优先级越高。若取值为**0**，则不能成为**DR**或**BDR**。

首先比较**OSPF**的端口优先级，数值较高的路由器将成为**DR**，其次高的成为**BDR**。若优先级数值相同，然后比较**Router ID**的大小，数值较大的成为**DR**，其次大的成为**BDR**。

RA(config-if)#ip ospf priority 5 **RB(config-if)#ip ospf priority 4**

若如上配置，虽然**R2**的**Router ID**比**R1**大，但因为**R2**的端口优先级较小，**R1**将成为**DR**。

第六章 动态路由 - OSPF

OSPF协议的优点：

基于国际标准，开放性强，被众多网络设备厂商所支持；

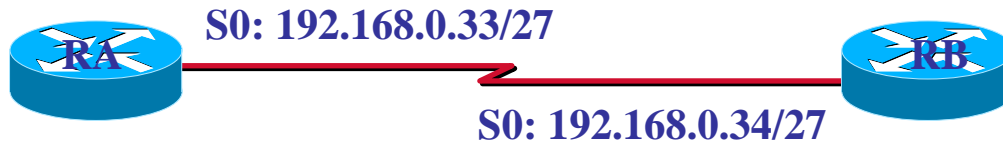
支持**VLSM**；

支持验证；

使用触发更新，快速适应网络变化，减少协议本身对网络的占用；

支持大型网络，并能进行优化路由更新；

第六章 动态路由 - OSPF



RA#debug ip ospf adj

//查看OSPF邻居关系的建立的几个过程

RA(config)#router ospf 1

//1表示进程号，取值范围为1至65535。进程号仅本地有效，不同路由器上进程号可以不同。

RA(config-router)#network 192.168.0.32 0.0.0.31 area 0

//网络号、反掩码、区域号

RB(config)#router ospf 2

RB(config-router)#network 192.168.0.32 0.0.0.31 area 0

第六章 动态路由 - OSPF

RA#show ip route

RA#show ip protocols

RA#show ip ospf neighbors

//查看OSPF邻居

RA#show ip ospf database

//查看OSPF数据库

第六章 动态路由 - OSPF

OSPF路由协议验证

在OSPF协议数据包结构中，包含有一个验证域及一个64位长度的验证数据域，用于特定的验证方式的计算。

OSPF数据交换的验证是基于区域来定义的，某区域的所有路由器上采用相同的验证方式。另外一些与验证相关的参数也可以基于每一个端口来定义，例如当采用单一口令验证时，我们可以对某一区域内部的每一个网络设置不同的口令字。

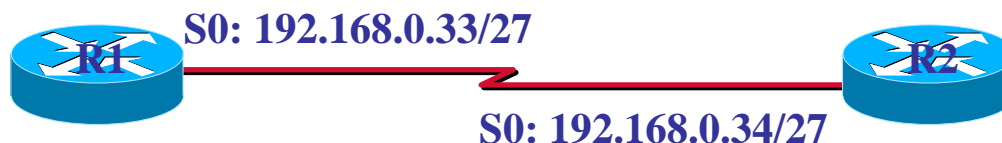
OSPF路由协议定义了两种协议验证方式：

方式0：不验证。默认情况下OSPF不使用区域验证。OSPF的数据包头内64位的验证数据位可以包含任何数据，OSPF接收到路由数据后对数据包头内的验证数据位不作任何处理。

方式1：简单口令字验证（Clear text）。

方式2：MD5（Message digest）。

第六章 动态路由 - OSPF



验证方式1, clear text:

```
interface serial 0
```

```
ip ospf authentication-key cisco
```

//在接口模式下, 指定用于验证的密码

```
router ospf 100
```

```
area 0 authentication
```

//在路由配置模式下, 指定验证的方式

验证方式2, message digest

```
interface serial 0
```

```
ip ospf message-digest-key 1 md5 cisco
```

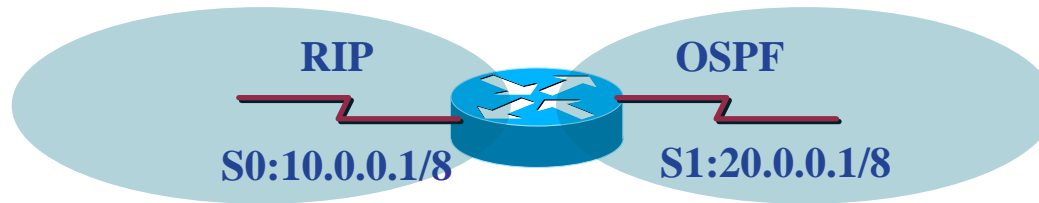
//在接口模式下, 指定用于验证的密码

```
router ospf 200
```

```
area 0 authentication message-digest
```

//在路由配置模式下, 指定验证的方式

第六章 动态路由 - OSPF



```
Router(config)#router ospf 1
```

```
Router(config-router)#network 20.0.0.0 0.255.255.255 area 0
```

```
Router(config-router)#redistribute rip metric 128
```

//以开销**128**重分布

```
Router(config-router)#exit
```

```
Router(config)#router rip
```

```
Router(config-router)#network 10.0.0.0
```

```
Router(config-router)#redistribute ospf 1 metric 5
```

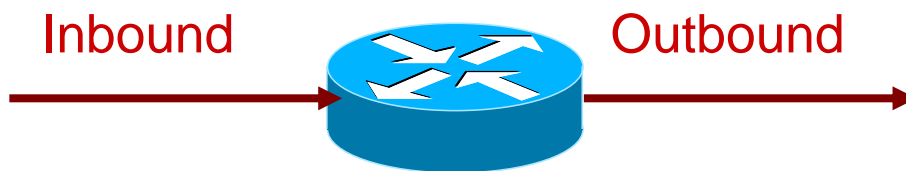
//以跳数**5**重分布

第七章 访问控制列表

Access Control List (ACL)

访问控制列表（ACL）是一种包过滤技术，是应用在路由器接口的指令列表。ACL告诉路由器哪些数据报可以允许、哪些需要拒绝。至于允许还是拒绝，可以由类似源地址、目的地址、端口号等条件来作过滤决定。

ACL可以用来：限制网络流量、提高网络性能，同时ACL也是网络访问控制的基本安全手段。



需要把ACL应用到接口上，而且还要定义过滤的方向：

- 1、inbound ACL：先路由，再处理
- 2、outbound ACL：先处理，再路由

第七章 访问控制列表

访问控制列表分为标准访问控制列表（编号为**1到99**）和扩展访问控制列表（编号为**100到199**）两类。

1、标准访问列表（standard access lists）：只使用源IP地址来做过滤决定。

标准访问控制列表检查数据包的源地址，从而允许或拒绝基于网络、子网或主机的IP地址的所有通信流量通过路由器的出口。

2、扩展访问列表（extended access lists）：使用源IP地址和目标IP地址，第三层的协议字段，第四层的端口号来做过滤决定。

扩展访问控制列表更具有灵活性和可扩充性，即可以对同一地址允许使用某些协议通信流量通过，而拒绝使用其他协议的流量通过。

3、命名访问控制列表（named access lists）

命名访问控制列表使用字母或数字组合的字符串来代替数字编号。使用命名访问控制列表可以用来删除某一条特定的条目，便于修改。

在使用命名访问控制列表时，要求路由器的IOS版本在**11.2**以上。

使用**ip access-list**命令来创建命名访问控制列表。

第七章 访问控制列表

设置ACL的规则：

- 1、对于每个接口、每个方向、每种协议，只能设置1个ACL。
- 2、按ACL语句的顺序，先比较第一行，再比较第二行……直到最后一行。找到一条符合条件的语句以后，剩余的语句就不再继续执行。

例如，要求禁止192.168.0.0/24网络中的192.168.0.32/27子网通过。

如果ACL这样配置

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

```
Router(config)#access-list 1 deny 192.168.0.32 0.0.0.31
```

当路由器收到源地址为192.168.0.32网段的数据包时，会发现该数据包属于192.168.0.0网段，按访问控制列表的顺序执行，结果该数据包将会被允许通过。

为解决这个问题，组织好ACL的顺序，条件严格的放在ACL的顶部。将两条语句的顺序调换。

第七章 访问控制列表

3、不能从ACL中去除一行，这将删除整个ACL，命名访问控制列表（**named access lists**）例外。

如上例，发现语句顺序有误，需要调整，若删除其中某一条，将会删除整个ACL。

4、新的语句只能加在现有语句的最后。如果必须要修改，只有先删除现有的访问控制列表，再创建一个新的访问控制列表。

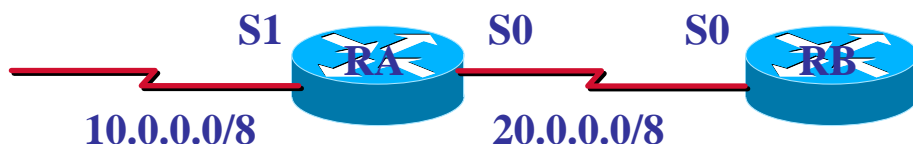
5、默认ACL结尾语句是**deny any**，所以在ACL里至少要有一条**permit**语句。

如果访问控制列表的语句都是**deny**，那么加上最后隐含的**deny any**，该接口将会拒绝所有流经该接口的数据。

6、创建ACL后要应用在需要过滤的接口上，并指明方向。

第七章 访问控制列表

7、ACL是用于过滤经过路由器的数据包，它并不会过滤路由器本身所产生的数据包。



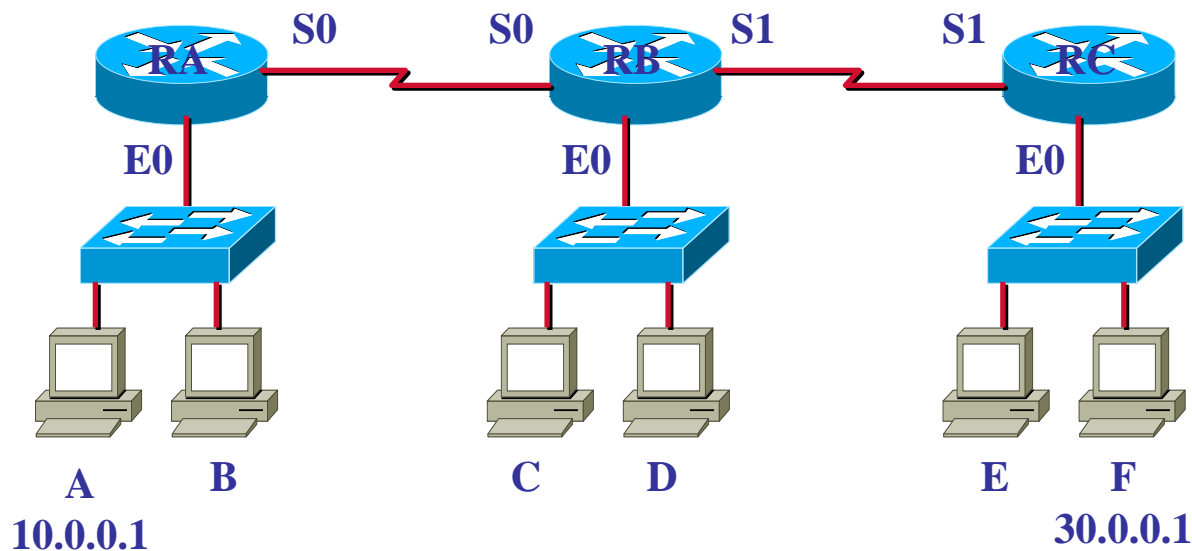
如图所示的网络中，若要求过滤来自10.0.0.0/8网络中所有的数据包。就不能把ACL放在RA的S1接口的in方向或者RA的S0接口的out方向，而只能放在RB的S0接口的in方向。

因为RA的S1接口IP地址也是属于10.0.0.0/8网络，RA不能过滤自己接口所产生的数据包。

8、把标准ACL放置在尽可能靠近目标的接口，把扩展ACL放置在尽可能靠近源的接口。

第七章 访问控制列表

标准访问控制列表，只检查源地址



要求：

- 1、采用标准访问列表
- 2、阻止HostA访问HostF

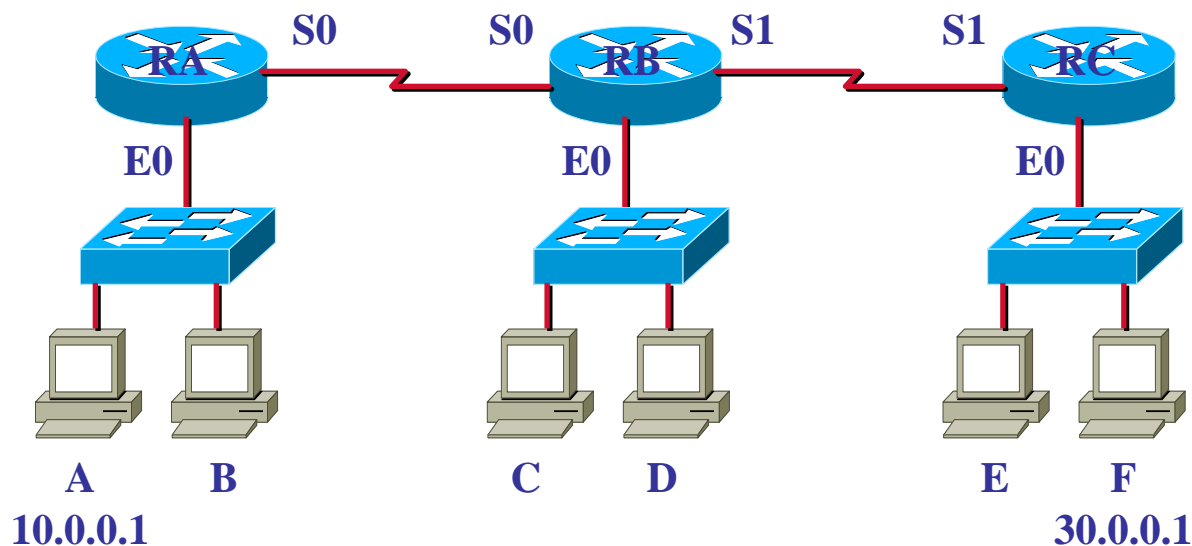
问题：

- 1、放置在哪个路由器的哪个接口的哪个方向上可行？
- 2、放置在哪个路由器的哪个接口的哪个方向上最好？

对于标准访问列表，放置在离目标最近的接口上。

第七章 访问控制列表

扩展访问控制列表，检查源地址、目标地址、协议、端口号



要求：

- 1、采用扩展访问列表
- 2、阻止HostA访问HostF

问题：

- 1、放置在哪个路由器的哪个接口的哪个方向上可行？
- 2、放置在哪个路由器的哪个接口的哪个方向上最好？

对于扩展访问列表，放置在离源最近的接口上。

第七章 访问控制列表

通配符掩码（Wildcast Mask）

通配符掩码是一个32比特位的数字字符串。

通配符掩码与子网掩码工作原理是不同的。在IP子网掩码中，数字1和0用来决定是网络、子网，还是相应的主机的IP地址。

在通配符掩码位中，0表示“检查相应的位，并且需要匹配”，1表示“不检查相应的位，不需要匹配”。

如表示172.16.0.0这个网段，使用通配符掩码应为0.0.255.255。

通配符掩码中，用255.255.255.255表示所有IP地址，可以用any代替，因为全为1说明所有32位都不检查；0.0.0.0则表示所有32位都要进行匹配，这样只能表示一个IP地址，可以用host表示。

有些教材中介绍说通配符掩码就是反掩码=255.255.255.255 - 子网掩码。尽管通配符掩码有时候看起来很像反掩码，但它们的作用是不一样的。

第七章 访问控制列表

如要允许172.16.16.0/20网段：

10101100.00010000.00010000.00000000



00000000.00000000.00001111.11111111

若收到数据包地址为172.16.15.1

172.16.15.1 = 10101100.00010000.00001111.00000000



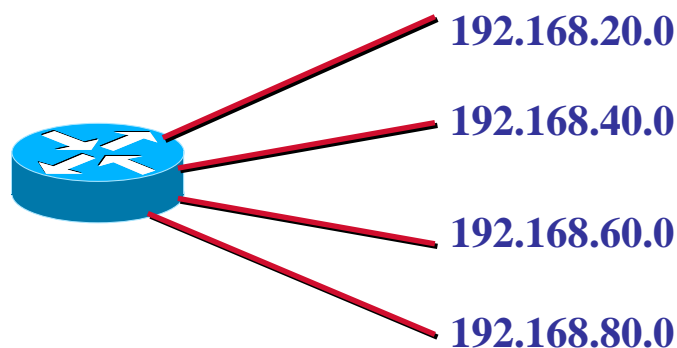
ACL将从前向后逐位检查，到第**20**位时发现与设置的规则不匹配：预设的**ACL**将允许第**20**位为**1**的数据包，但该数据包为**1**，不属于该**ACL**语句所允许的范围。

第七章 访问控制列表

Q1: 如要定义192.168.0.96/27网络，通配符掩码为多少？

Q2: 如要限定192.168.0.0/24网络中偶数位IP，通配符掩码为多少？

Q3: 如图，如只允许192.168.80.0，则通配符掩码可以为多少？为减少检查的位，最好可以为多少？如只允许40呢？如只允许60呢？



第七章 访问控制列表

配置标准访问列表

Router(config)#access-list *access-list-number deny/permit source-address source-wildcard*

access-list-number: 取值范围1~99

deny|permit: 拒绝或允许匹配ACL的数据包

source-address: 某一个或某一段源地址

source-wildcard: 通配符掩码

应用访问列表到接口

Router(config-if)#ip access-group *access-list-number in/out*

In: 通过接口进入路由器的报文

Out: 通过接口离开路由器的报文

第七章 访问控制列表

配置标准的访问控制列表



HostA:10.0.0.2 E0:10.0.0.1

实验要求：禁止hostA访问RA的E0

RA(config)#access-list 1 deny 10.0.0.2 0.0.0.0

RA(config)#access-list 1 permit any

RA(config)#interface ethernet 0

RA(config-if)#ip access-group 1 in

在HostA上ping 测试。

在HostA上修改IP地址，如10.0.0.3，再测试

第七章 访问控制列表

show access-list: 显示路由器上配置的所有的ACL信息

show access-list [number]: 显示具体第几条编号ACL信息

RA#show ip access-lists 1

Standard IP access list 1

deny 10.0.0.2, wildcard bits 0.0.0.0 check=64

permit any (64 matches) //表示有64个匹配条件的数据包

RA#clear access-list counters //清空计数器

show ip interface: 显示接口的信息和配置的ACL信息。

show ip interface [端口号]: 显示某接口的信息和配置的ACL信息。

RA#show ip interface ethernet 0

Outgoing access list is not set

Inbound access list is 1

第七章 访问控制列表

配置扩展访问列表

Router(config)#access-list *access-list-number* *permit/deny* *protocol* *source-address* *source-wildcard* *source-port* *destinaiton* *address* *destination-wildcard* *destination-port*

access-list-number: 编号范围为100~199。

Protocol: 需要被过滤的协议的类型，如IP、TCP、UDP、ICMP、EIGRP等。

port: 端口号，可以是eq（等于）、gt（大于）、lt（小于）、neq（不等于）、range（范围）等。

第七章 访问控制列表

配置扩展的访问控制列表



HostA:10.0.0.2 E0:10.0.0.1

实验要求：允许HostA远程登录RA，但是不可PING

```
RA(config)#access-list 100 deny icmp host 10.0.0.2 host 10.0.0.1 echo
```

```
RA(config)#access-list 100 permit tcp host 10.0.0.2 host 10.0.0.1 eq 23
```

```
RA(config)#access-list 100 permit ip any any
```

```
RA(config)#interface ethernet 0
```

```
RA(config-if)#ip access-group 100 in
```

在HostA上分别用ping和telnet目标10.0.0.1测试。

在HostA上修改IP地址，如10.0.0.3，再测试。

第七章 访问控制列表

命名IP访问列表通过一个名称而不是一个编号来引用的。

命名的访问列表可用于标准的和扩展的访问表中。

名称的使用区分大小，并且必须以字母开头，可以包含字母、数字和字符。

名称的最大长度为100个字符。

名字能更直观地反映出访问列表完成的功能。

命名访问列表突破了标准和扩展访问列表的数目限制，能够定义更多的访问列表。

命名IP访问列表允许删除单独某条语句，而编号访问列表将删除整个访问列表。

单个路由器上命名访问列表的名称必须是唯一的，不同路由器上的命名访问列表名称可以相同。

第七章 访问控制列表

命名的访问控制列表



HostA:10.0.0.2 E0:10.0.0.1

实验要求：仅允许HostA远程登录

```
RA(config)#ip access-list standard telnet
```

```
RA(config-std-nacl)#permit host 10.0.0.2
```

```
RA(config-std-nacl)#deny any
```

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

```
RA(config-line)#access-class telnet in
```

分别用ping和telnet测试。

在HostA上修改IP地址，如10.0.0.3，再测试。

第七章 访问控制列表

从**IOS 12.0**开始，**Cisco**路由器新增加了一种基于时间的访问控制，可以根据一天中不同时间或/和根据一周中的不同日期控制网络数据包的转发。

这种基于时间的访问列表在原来标准访问列表和扩展访问列表中加入时间范围来更合理有效地控制网络。它先定义一个时间范围，然后在原来的各种访问列表的基础上应用它，对于编号访问表和名称访问表均适用。

实现基于时间的访问表需要两个步骤：

第一步是定义一个时间范围；

第二步是在访问列表中用**time-range**引用时间范围。

第七章 访问控制列表

可以用“**time-range**”来指定时间范围的名称，然后用“**absolute**”或者一个或多个“**periodic**”来具体定义时间范围，命令格式为：

time-range time-range-name absolute [start time date] [end time date]
periodic days-of-the week hh:mm to [days-of-the week] hh:mm

time-range: 用来定义时间范围

time-range-name: 时间范围的名称，用来标识时间范围，以便在后面的访问列表中引用

一个时间范围只能有一个**absolute**语句，但可以有几条**periodic**语句。

第七章 访问控制列表

absolute: 用来指定绝对时间范围，后面紧跟**start**和**end**两个关键字，以24小时制和“**hh:mm**”表示，其格式为“小时:分钟”，日期按照“日/月/年”形式表示。这两个关键字也可以都省略。如果省略**start**及其后面的时间，表示与之相关联的**permit**或**deny**语句立即生效，并一直作用到**end**时间为止；若省略**end**及其后面的时间，表示与之相联系的**permit**或**deny**语句在**start**时间开始生效，并且永远发生作用。

定义绝对时间：

absolute [start start-time start-date] [end end-time end-date]

第七章 访问控制列表

periodic: 主要以星期几为参数来定义时间范围，如**Monday**、**Tuesday**、**Wednesday**、**Thursday**、**Friday**、**Saturday**、**Sunday**中的一个或者几个的组合，也可以是**daily**（每天）、**weekday**（周一到周五）或者**weekend**（周末，周六和周日）。

定义周期、重复使用的时间范围

periodic days-of-the-week hh:mm to days-of -the-week hh:mm

如果要表示每天早8点到晚6点开始起作用，可以用这样的语句：

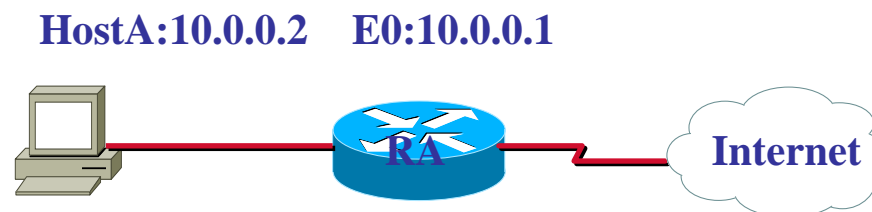
absolute start 8:00 end 18:00

比如表示每周一到周五的早9点到晚10点半：

periodic weekday 9:00 to 22:00

第七章 访问控制列表

基于时间的访问控制列表



实验要求：允许内网主机在**2007年1月1日到2007年12月31日**的每个工作日中午**12:00到14:00**上网浏览

```
RA(config)#access-list 100 permit tcp 10.0.0.0 0.255.255.255 any eq 80  
time-range http
```

```
RA(config)#time-range http
```

```
RA(config-time-range)#asbsolute start 1 Jan 2007 end 31 December 2007
```

```
RA(config-time-range)#periodic weekdays 12:00 to 14:00
```

```
RA(config)#interface ethernet 0
```

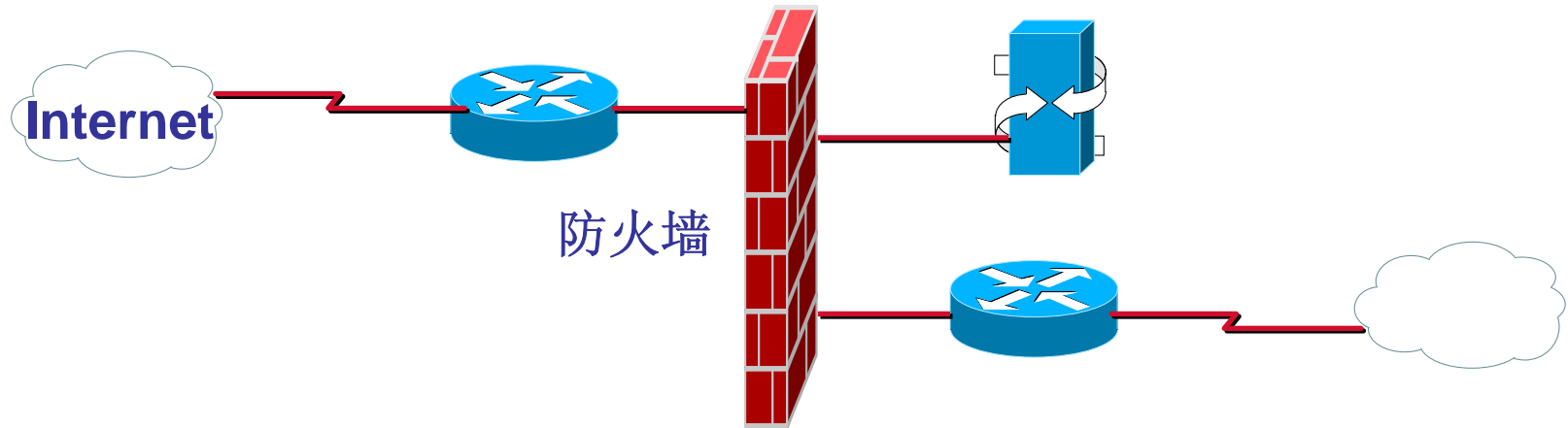
```
RA(config-if)#ip access-group 100 in
```

修改路由器的时间，查看访问控制列表的状态：**Active/Inactive**。

第七章 访问控制列表

防火墙

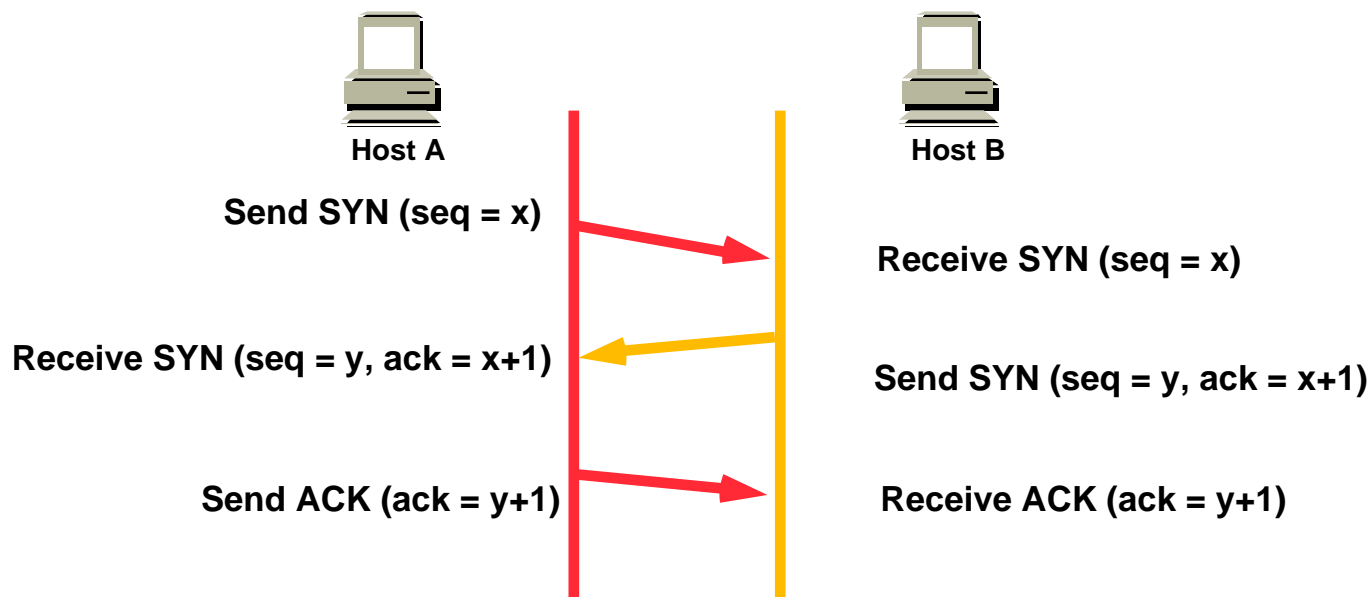
防火墙是存在于用户和外部世界之间，用于保护内部网络免受外部入侵攻击的一种计算机或者网络设备。



第七章 访问控制列表

TCP三次握手（Three-way Handshake）

- 1、客户端发送一个包含SYN标志的TCP报文给服务器端；
- 2、服务器在收到客户端的SYN报文后，返回一个SYN+ACK的报文，表示客户端的请求被接受；
- 3、客户端返回一个ACK确认给服务器，一个TCP连接完成。



第七章 访问控制列表

半连接：收到**SYN**包而还未收到**ACK**包时的连接状态称为半连接，即尚未完全完成三次握手的**TCP**连接。

半连接队列：在三次握手协议中，服务器维护一个半连接队列，该队列为每个客户端的**SYN**包(**SYN=i**)开设一个条目，该条目表明服务器已收到**SYN**包，并向客户发出确认，正在等待客户的确认包。这些条目所标识的连接在服务器处于**SYN_RECV**状态，当服务器收到客户的确认包时，删除该条目，服务器进入**ESTABLISHED**状态。

Backlog参数：表示半连接队列的最大容纳数目。

SYN-ACK重传次数：服务器发送完**SYN-ACK**包，如果未收到客户确认，服务器进行重传，如果等待一段时间仍未收到客户确认包，将再次重传，如果重传次数超过系统规定的最大重传次数，系统将该连接信息从半连接队列中删除。每次重传等待的时间不一定相同。

半连接存活时间：是指半连接队列的条目存活的最长时间，也即服务从收到**SYN**包到确认这个报文无效的最长时间，该时间值是所有重传请求包的最长等待时间总和。有时也称半连接存活时间为**Timeout**时间、**SYN_RECV**存活时间。

上面三个参数对系统的**TCP**连接状况有很大影响。

第七章 访问控制列表

在攻击事件中，**SYN泛洪攻击**是最常见又最容易被利用的一种**DoS攻击**手法。

SYN泛洪攻击属于**DoS攻击**的一种，它利用**TCP**协议缺陷，通过发送大量的半连接请求，耗费**CPU**和内存资源。**SYN攻击**除了能影响主机外，还可以危害路由器、防火墙等网络系统，事实上**SYN攻击**并不管目标是什么系统，只要这些系统打开**TCP**服务就可以实施。

配合**IP欺骗**，**SYN攻击**能达到很好的效果。通常，客户端在短时间内伪造大量不存在的**IP**地址，向服务器不断地发送**SYN**包，服务器回复确认包，并等待客户的确认，由于源地址是不存在的，服务器需要不断的重发直至超时，这些伪造的**SYN**包将长时间占用未连接队列，正常的**SYN**请求被丢弃，目标系统运行缓慢，严重者引起网络堵塞甚至系统瘫痪。

第七章 访问控制列表

TCP拦截

在TCP连接请求到达目标主机之前，TCP拦截通过拦截和验证来阻止这种攻击。TCP拦截可以在拦截和监视两种模式下工作。

在拦截模式下，路由器拦截到达的TCP SYN请求，同时代表服务器建立与客户机的连接，如果连接成功，则代表客户机建立与服务器的连接，并将两个连接进行透明合并。在整个连接期间，路由器会一直拦截和发送数据包。对于非法的连接请求，路由器提供更为严格的半连接（**half-open**）超时限制，以防止自身的资源被SYN攻击耗尽。

在监视模式下，路由器被动地观察流经路由器的连接请求，如果连接超过了所配置的建立时间，路由器就会关闭此连接。

第七章 访问控制列表

TCP拦截的配置

开启TCP拦截

ip tcp intercept list access-list-number

设置TCP拦截模式

ip tcp intercept mode intercept（拦截模式） | watch（监视模式）

配置路由器等待时间

ip tcp intercept watch-timeout seconds（等待时间，单位为秒）

第七章 访问控制列表

配置删除TCP半连接的阈值

ip tcp intercept max-incomplete high number

Number: 路由器开始删除连接之前，能够存在的最大半连接数

ip tcp inercept max-incomplete low number

Number: 路由器停止删除连接之前，能够存在的最大半连接数

ip tcp intercept one-minute high number

Number: 路由器开始删除连接之前，每分钟内能存在的最大半连接数目

ip tcp intercept one-minute low number

Number: 路由器停止删除连接之前，每分钟内能存在的最大半连接数目

第七章 访问控制列表

设置路由器删除半连接的方式

ip tcp intercept drop-mode oldest|random

oldest: 删除建立时间最早的连接

random: 随机删除已经建立的连接

查看TCP拦截信息

show tcp intercept connections

show tcp intercept statistics

第七章 访问控制列表

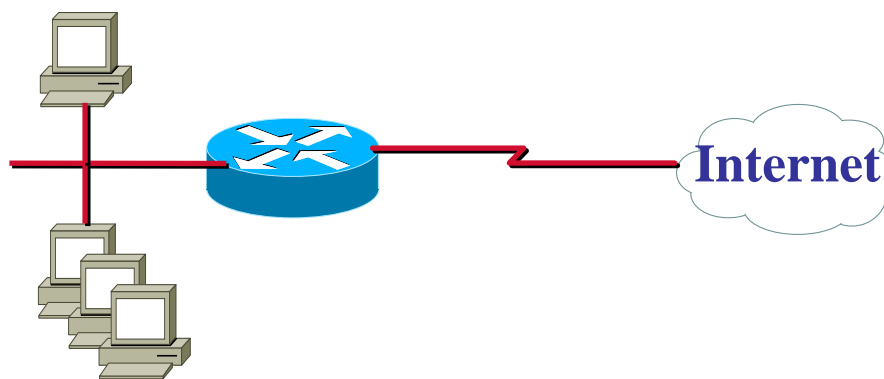
Web服务器地址为**10.0.0.1**，配置路由器进行**TCP拦截**，以保护Web服务器不受**SYN洪水攻击**。

要求采用拦截和监视两种模式分别配置。

在拦截模式下，设置最大半连接数的高、低值分别为**500**和**300**；每分钟保持连接数的高、低值分别为：**500**和**300**，删除连接的方式采用缺省值。

在监视模式下，设置路由器等待时间为**20**秒。

Web服务器：**10.0.0.1**



第七章 访问控制列表

拦截模式

router(config)#access-list 101 permit tcp any host 10.0.0.1

router(config)# ip tcp intercept mode intercept

router(config)# ip tcp intercept max-incomplete high 500

router(config)# ip tcp intercept max-incomplete low 300

router(config)# ip tcp intercept one-minute high 500

router(config)# ip tcp intercept one-minute low 300

router(config)# ip tcp intercept list 101

第七章 访问控制列表

监视模式

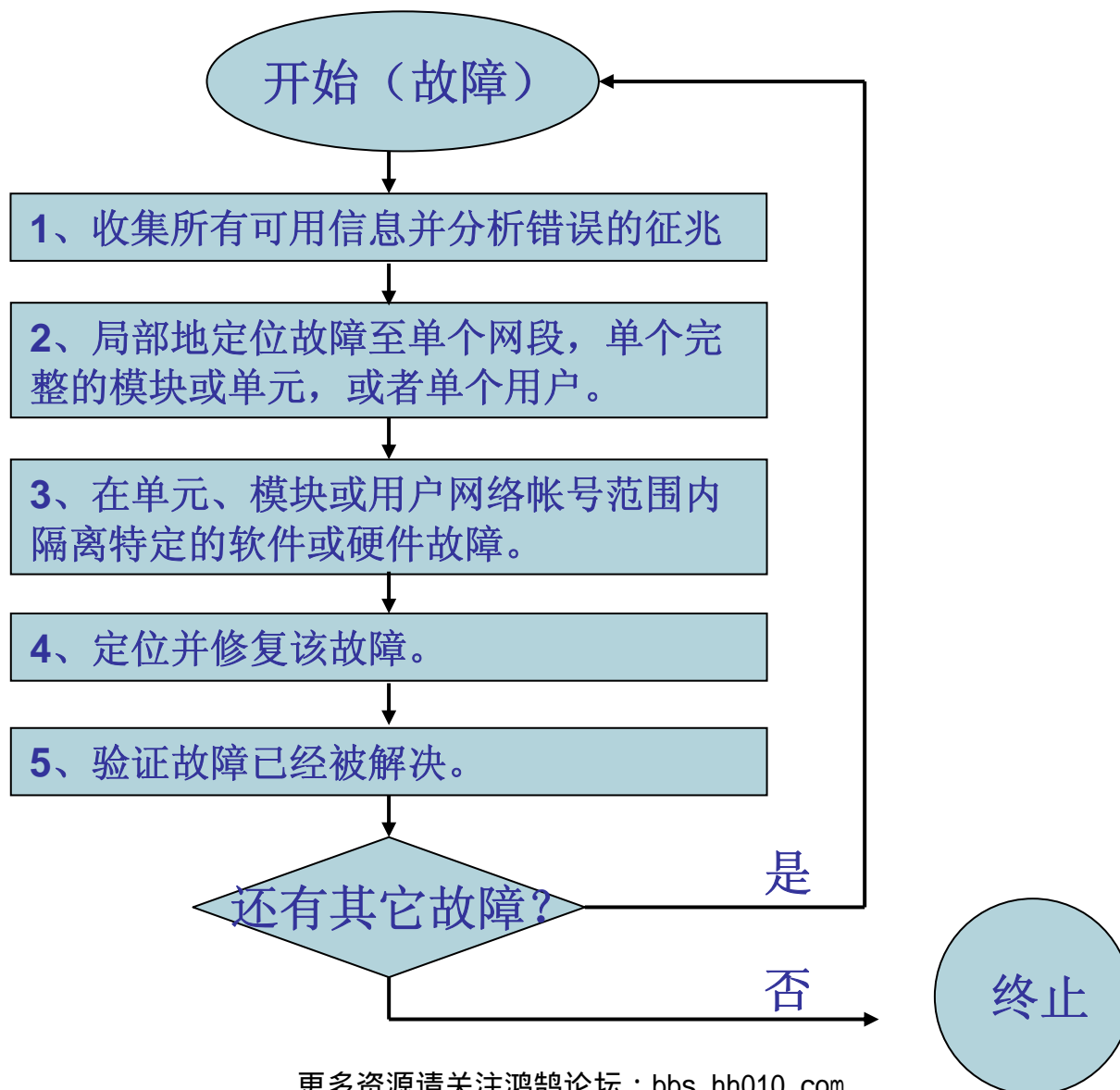
```
router(config)#access-list 101 permit tcp any host 10.0.0.1
```

```
router(config)# ip tcp intercept mode watch
```

```
router(config)# ip tcp intercept watch-timeout 20
```

```
router(config)# ip tcp intercept list 101
```

第八章 故障排除方法



第八章 故障排除方法

第一层常见故障：

电缆损坏

未连接电缆

电缆连接到错误的端口

电缆连接间歇性中断

对于当前任务使用了错误的电缆

收发器故障

DCE/DTE电缆故障

设备掉电

第八章 故障排除方法

第二层常见故障：

不正确地配置串行接口

不正确地配置以太网接口

不正确的封装

串行接口上不正确的时钟设置

NIC故障

第八章 故障排除方法

第三层常见故障：

路由选择协议没有启用

启用了错误的路由选择协议

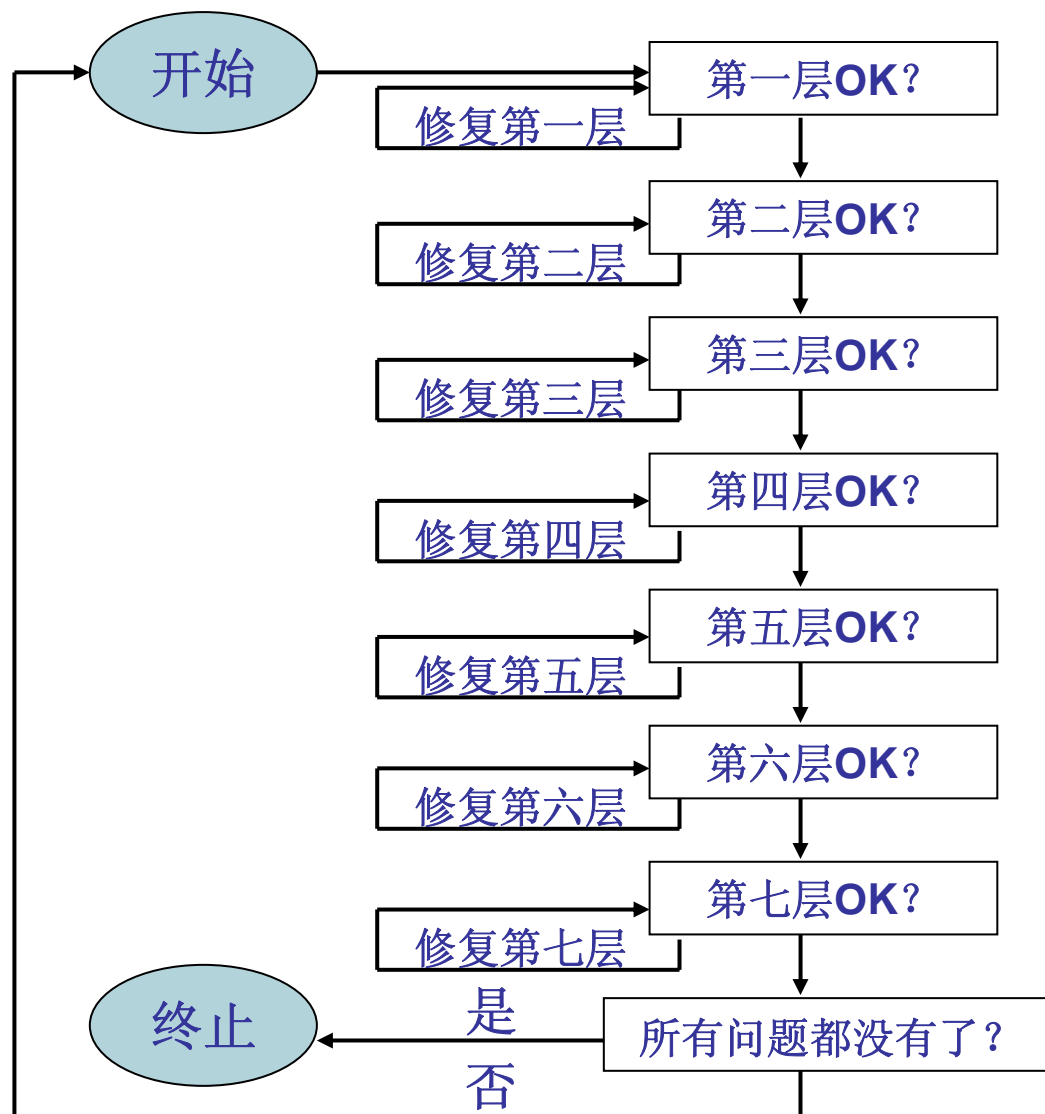
不正确地配置路由选择协议

不正确的**IP**地址

不正确的子网掩码

不正确的缺省网关

第八章 故障排除方法



第八章 故障排除方法

show ip route

show ip protocols

路由类型	管理距离
直连路由	0
静态路由	1
EIGRP 汇总路由	5
外部边界网关协议（ eBGP ）	20
EIGRP （内部）	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EIGRP （外部）	170
内部边界网关协议（ iBGP ）	200

第八章 故障排除方法

Router#show interface

Router#show cdp

Router#traceroute

Router#show controllers

Router#debug

...

第八章 故障排除方法

使用指示灯排除第一层故障

使用**Ping**命令排除第三层故障

使用**Telnet**处理第七层故障

第八章 故障排除方法

Ping

echo协议用来测试协议分组是否被路由。**Ping**命令使用的是**Internet**控制消息协议（**ICMP**），向目的主机发送一个分组，然后等待一个来自该主机的应答分组。**Echo**协议的结果将有助于评估到目的主机的路径的可靠性、路径延迟以及该主机是否能够到达或是否正在运行。

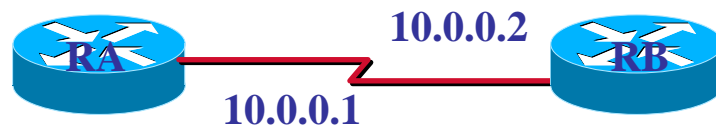
RA>ping 10.0.0.2

Sending 5, 100 byte ICMP Echos to 10.0.0.2,

timeout is 2 seconds:

!!!!

Success rate is 100 percent



第八章 故障排除方法

代码	含义	可能的原因
!	每个感叹号表示接收到一个ICMP回应应答	Ping 成功
.	每个句号表示等待一个应答时网络服务超时	可能表示出现以下问题： Ping 请求被访问控制列表或防火墙阻隔； 路径上某台路由器没有到达目的主机的路由，也没有返回 ICMP 目标不可达消息； 路径上的某处发生了物理连接问题。
U	收到一条 ICMP 不可达消息	路径上的一台路由器没有到达目的主机的路由
C	收到一条 ICMP 源抑制消息	路径上的一台设备（可能是目的主机）收到过多的流量
&	收到一条 ICMP 超时消息	可能发生路由环路

第八章 故障排除方法

Traceroute

Traceroute通过发送小的数据包到目的设备并直到其返回，测量其需要多长时间。一条路径上的每个设备**Traceroute**要测3次。输出结果中包括每次测试的时间(ms)和设备的名称（如有的话）及其IP地址。

Traceroute有一个固定的时间等待响应（**ICMP TTL**到期消息）。如果这个时间过了，它将打印出一系列的*号表明：在这个路径上，这个设备不能在给定的时间内发出**ICMP TTL**到期消息的响应。

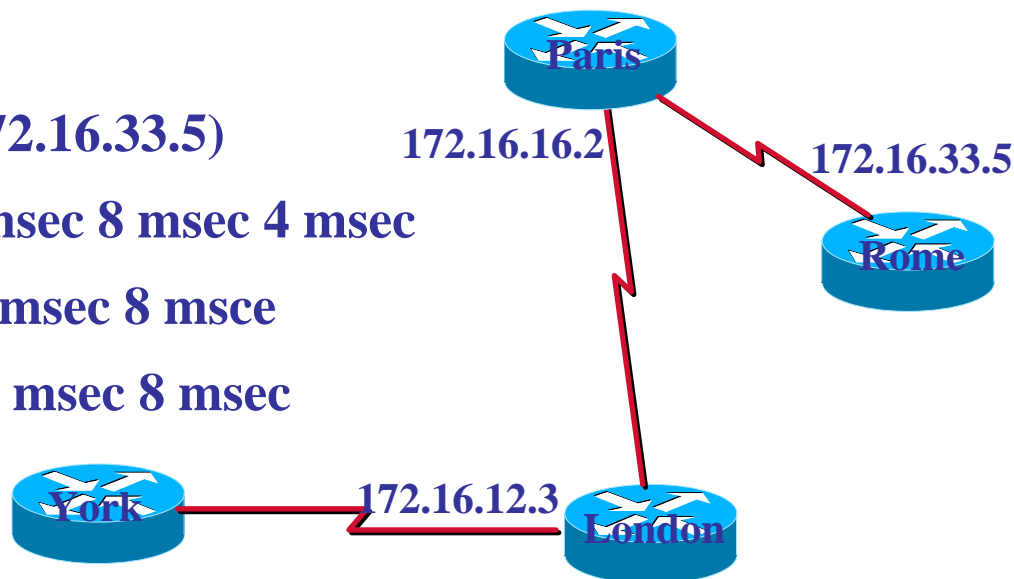
York#traceroute Rome

Tracing the route to Rome (172.16.33.5)

1 London (172.16.12.3) 1000 msec 8 msec 4 msec

2 Paris (172.16.16.2) 8 msec 8 msec 8 msec

3 Rome (172.16.33.5) 8 msec 8 msec 8 msec



第八章 故障排除方法

Traceroute利用了**ICMP**及**IP**报头的**TTL (Time To Live)** 位。

首先，**traceroute**送出一个**TTL**是**1**的报文到目的，当路径上的第一个路由器收到这个报文时，它将**TTL**减**1**。此时，**TTL**变为**0**，该路由器将会丢弃此报文，并送回一个**icmp time exceeded**消息，源主机收到这个消息后，便知道这个路由器位于这条路径上的第一跳，接着再送出一个**TTL**是**2**的报文，发现第二个路由器……通过将每次送出的报文的**TTL**加**1**来发现下一个路由器，一直持续到报文抵达目的地。

当报文到达目的地后，该主机并不会送回**icmp time exceeded**消息，因为它已经是目的地了，那么**traceroute**如何得知目的地到达了呢？

Traceroute在送出报文到目的地时，它所选择的端口号一般是一个应用程序都不会用的号码（如**30000**以上），所以当此报文到达目的地后该主机会送回一个**ICMP port unreachable**的消息，而当源主机收到这个消息时，便知道目的地已经到达了。

第三部分 交换原理

第一章 以太网交换

第二章 交换机基础配置

第三章 生成树

第四章 虚拟局域网

第一章 以太网交换

以太网是指运行**IEEE 802.3**以太网协议的网络。局域网运行的协议常见的主要有以太网协议、令牌总线、令牌环网，在没有特别指明的情况下，局域网通常是指以太局域网。

以太网严格遵循**CSMA/CD**（载波侦听多路访问/冲突检测，**Carrier Sensor Multiple Access /Collision Detection**）协议。计算机在发送数据前必须先进行侦听，只有当信道空闲才能发送数据。如果两个以上的主机同时监听到信道空闲并同时发送数据帧，就会产生冲突，发送的帧都成为无效帧，发送失败。检测到冲突后，主机等待一个随机的时间，然后重新进行侦听，尝试发送。一台主机发送数据帧时，网络中的其他主机只能接收，属于半双工通讯方式。

第一章 以太网交换

集线器是一种多端口的中继器，共享带宽，属于物理层设备，是星形拓扑结构的中心节点。

集线器的基本功能是使用广播技术进行信息分发，将一个端口上接收到的信号，以广播的方式发送到集线器的其他所有端口。各端口接收到广播信息后，若发现该信息是发给自己的，则接收，否则丢弃。

一般而言，使用**10Mbps**集线器时，其工作站点不宜超过**25**个；使用**100Mbps**集线器时，不宜超过**35**个。

第一章 以太网交换

冲突域：是指连接到同一物理介质上的一组设备所构成的区域。

使用同轴电缆以总线结构或使用集线器以星型结构搭建的以太网，所有节点处于一个共同的冲突域。如果有两台设备同时要使用传输介质（发送或接收数据），就会造成冲突。当主机增多时，冲突将成倍增加，带宽和速度将显著下降。

广播域：是指可以接收广播消息的一组设备所构成的区域，也就是广播帧所能到达的范围。如采用集线器的网络中，如果一个站点发出一个广播，集线器将把该消息传播给连接在该集线器上的所有站点，因此集线器的所有端口处在同一个广播域，此时冲突域和广播域的地域范围是相同的。

而连接在一个没有划分VLAN的交换机上的设备，它们分别属于不同的冲突域，交换机的每一个端口，构成一个冲突域，不同的端口属于不同的冲突域，但都属于同一个广播域，即交换机的所有端口构成了一个广播域。

第一章 以太网交换

冲突域、广播域的比较

设备	工作层	冲突域	广播域
HUB	Physical Layer	所有端口处在同一冲突域	所有端口处在同一广播域
Bridge	Data Link Layer	每个端口处于同一冲突域	所有端口处在同一广播域
Switch	Data Link Layer	每个端口处于同一冲突域	不划分VLAN：所有端口处在同一广播域 划分VLAN：同一VLAN处在同一广播域
Router	Network Layer	每个端口处于同一冲突域	每个端口处于同一广播域

第一章 以太网交换

CSMA/CD（Carrier Sensor Multi Access/Collision Detection）

CSMA/CD是一种使用争用的方法来决定对媒体访问权的协议，这种争用协议只适用于逻辑上属于总线拓扑结构的网络。在总线网络中，每个站点都能独立地决定帧的发送，若两个或多个站同时发送帧，就会产生冲突，导致所发送的帧都出错。因此，一个用户发送信息成功与否，在很大程度上取决于监测总线是否空闲的算法，以及当两个不同节点同时发送的分组发生冲突后所使用的中断传输的方法。总线争用技术可分为载波监听多路访问CSMA和具有冲突检测的载波监听多路访问CSMA/CD两大类。

第一章 以太网交换

在CSMA中，由于信道传播时延的存在，如果总线上两个站点没有监听到载波信号而发送帧时，就可能发生冲突。由于CSMA算法没有冲突检测功能，即使冲突已发生，仍然将已破坏的帧发送完，使总线的利用率降低。

CSMA的改进方案是使发送站点传输过程中仍继续监听媒体，以检测是否存在冲突。如果发生冲突，信道上可以检测到超过发送站点本身发送的载波信号的幅度，由此判断产生冲突。一旦检测到冲突，就立即停止发送，并向总线上发送阻塞信号，以通知总线上其它站点，这样就可以提高总线的利用率。这种方案称做载波监听多路访问/冲突检测协议，简写为CSMA/CD，这种协议已广泛应用于局域网中。

第一章 以太网交换

在基于广播的以太网中，所有的工作站都可以收到发送到网上的信息帧。每个工作站都要确认该信息帧是不是发送给自己的，一旦确认是发给自己的，就将它发送到高一层的协议层。

在采用CSMA / CD传输介质访问的以太网中，任何一个工作站在任何一时刻都可以访问网络。发送数据前，工作站要侦听网络是否堵塞，只有检测到网络空闲时，工作站才能发送数据。

在基于竞争的以太网中，只要网络空闲，任一工作站均可发送数据。当两个工作站发现网络空闲而同时发出数据时，就发生冲突。这时，两个传送操作都遭到破坏，工作站必须在一定时间后重发，何时重发由延时算法决定。

第一章 以太网交换

以太网的工作过程如下：

当以太网中的一台主机要传输数据时，它将按如下步骤进行：

- 1、帧听信道上收否有信号在传输。如果有，表明信道处于忙状态，就继续侦听，直到信道空闲为止。
- 2、若没有侦听到任何信号，就传输数据。
- 3、传输的时候继续侦听，如果发现冲突则执行退避算法，重新执行步骤1。

第一章 以太网交换

常用的退避算法有：非坚持、1-坚持、P-坚持三种。

1、非坚持算法

(1)如果媒本是空闲的，则可以立即发送。

(2)如果媒体是忙的，则等待一个由概率分布决定的随机重发延迟后，再重复前一步骤。

采用随机的重发延迟时间可以减少冲突发生的可能性。非坚持算法的缺点是：即使有几个站点为都有数据要发送，但由于大家都在延迟等待过程中，致使媒体仍可能处于空闲状态，使用率降低。

第一章 以太网交换

1. 坚持算法

- (1) 如果媒体空闲的，则可以立即发送。
- (2) 如果媒体忙，则继续监听，直至检测到媒体空闲，立即发送。
- (3) 如果有冲突（在一段时间内未收到肯定的回复），则等待一随机时间，重复步骤(1)~(2)。

这种算法的优点是：只要媒体空闲，站点就立即可发送，避免了媒体利用率的损失；其缺点是：假若有两个或两个以上的站点有数据要发送，冲突就不可避免。

第一章 以太网交换

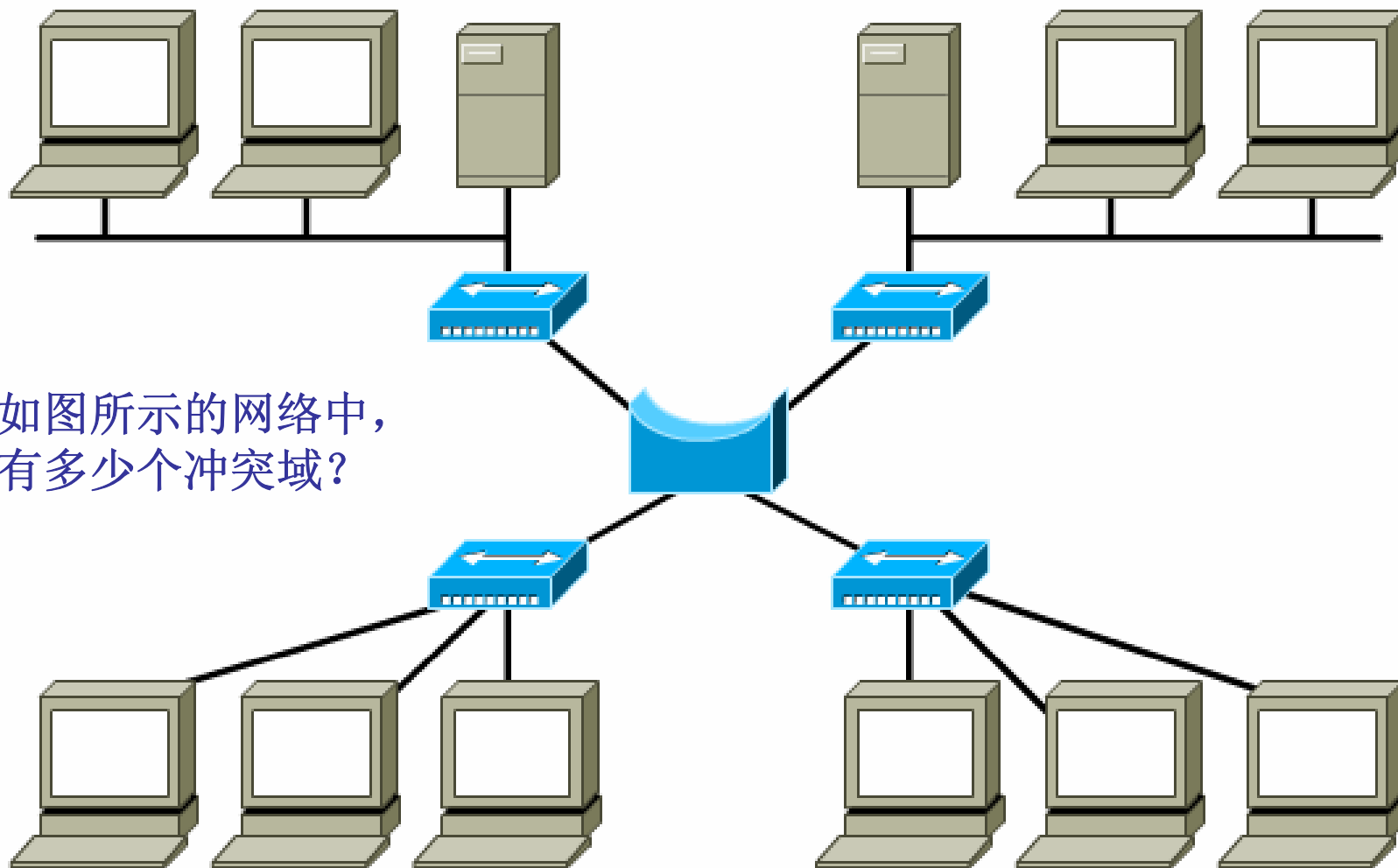
P-坚持算法

- (1) 监听总线，如果媒体是空闲的，则以 P 的概率发送，而以 $(1-P)$ 的概率延迟一个时间单位。一个时间单位通常等于最大传播时延的2倍。
- (2) 延迟一个时间单位后，再重复步骤(1)。
- (3) 如果媒体是忙的，继续监听直至媒体空闲并重复步骤(1)。

P-坚持算法是一种既能像非坚持算法那样减少冲突，又能像**1-坚持算法**那样减少媒体空闲时间的中间方案。

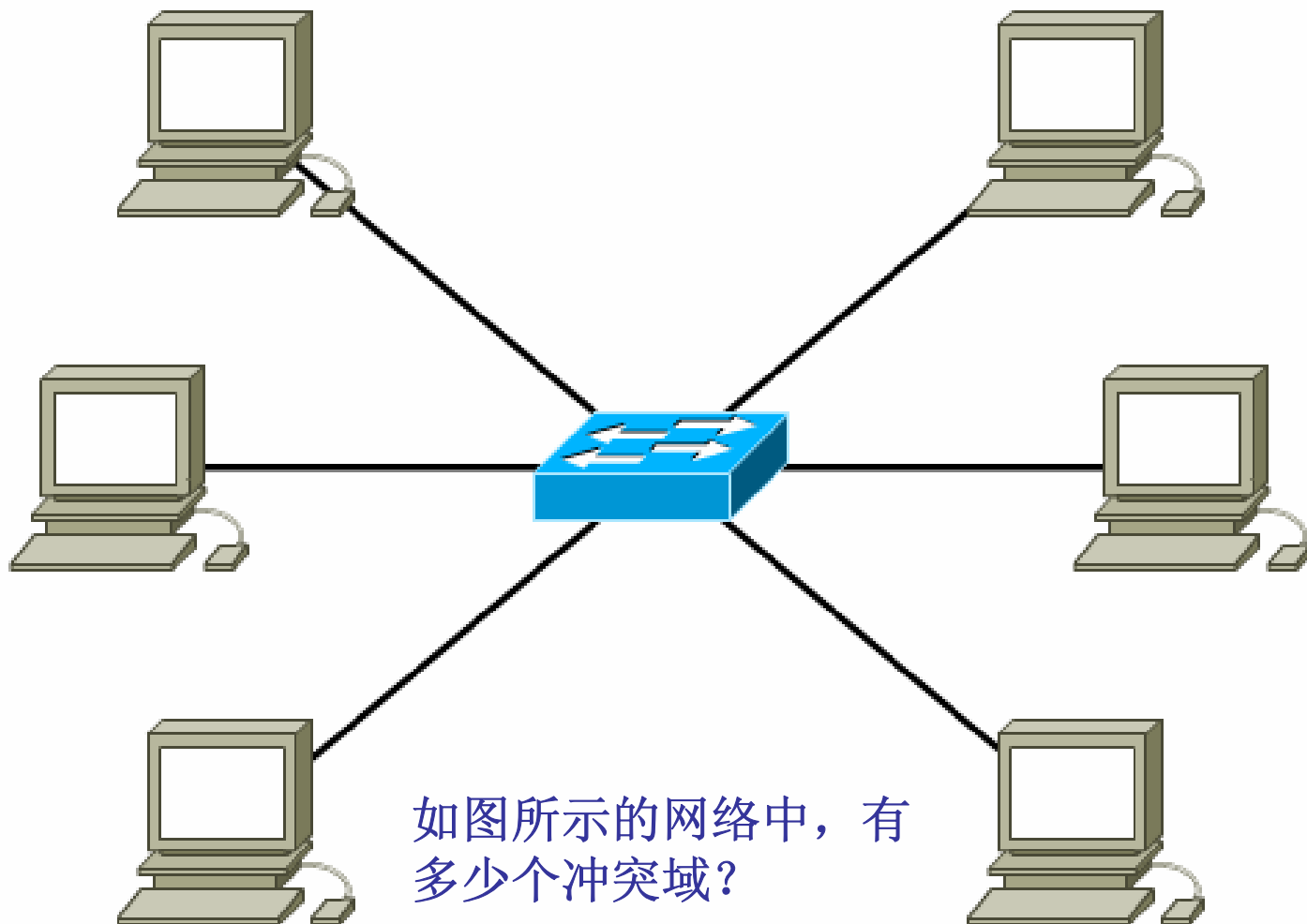
问题在于如何选择 P 的取值，这要考虑到避免重负载下系统所处的不稳定状态。假如有 N 个站有数据等待发送，则将要试图传输的站的总期望数为 $N \cdot P$ 。如果选择 P 过大，使 $NP > 1$ ，冲突将不可避免。最坏的情况是，随着冲突概率的不断增大，而使吞吐量降低到零。所以必须选择适当 P 值使 $NP < 1$ 。而如果 P 值选得过小，媒体利用率又会大大降低。

第一章 以太网交换

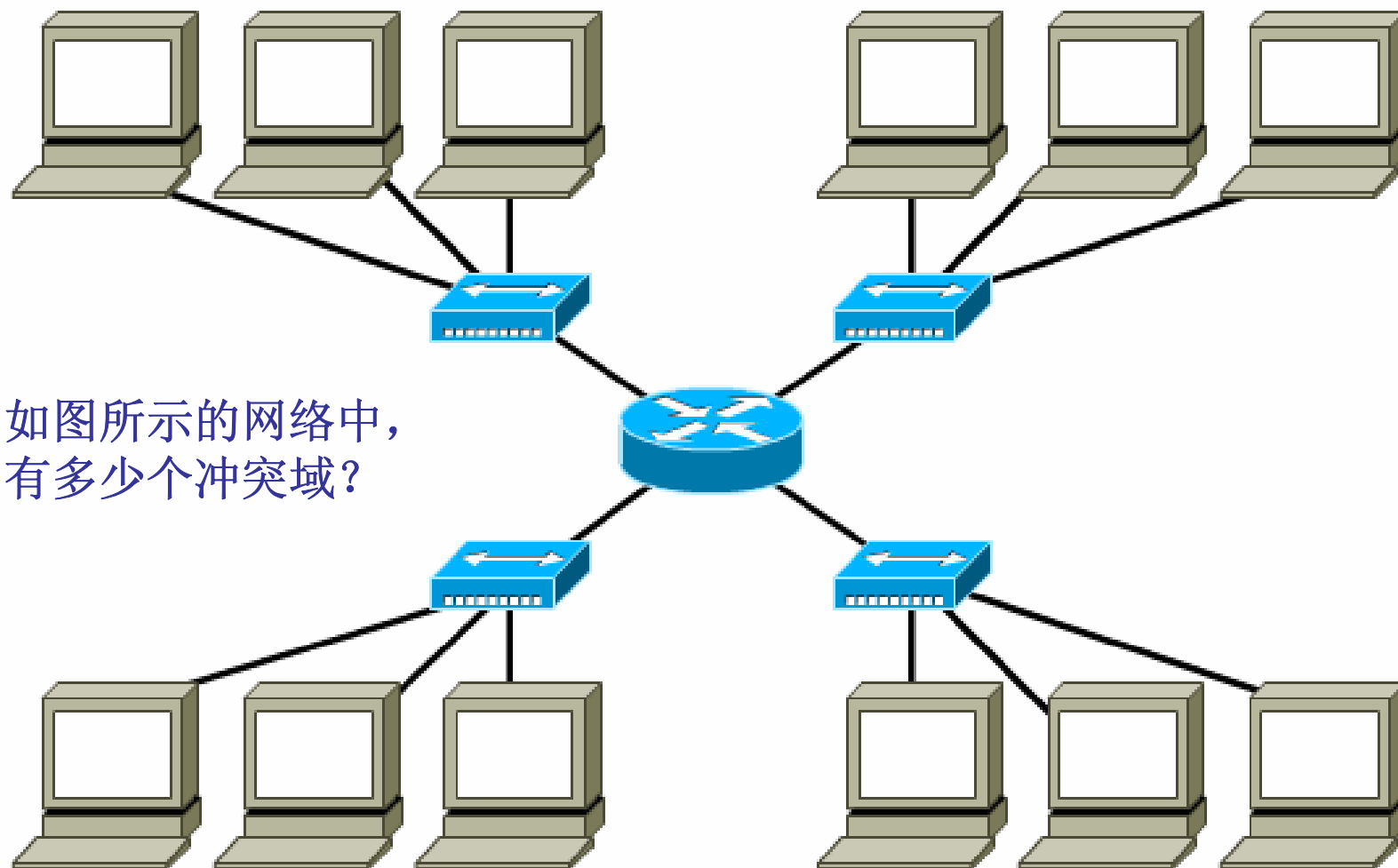


如图所示的网络中，
有多少个冲突域？

第一章 以太网交换

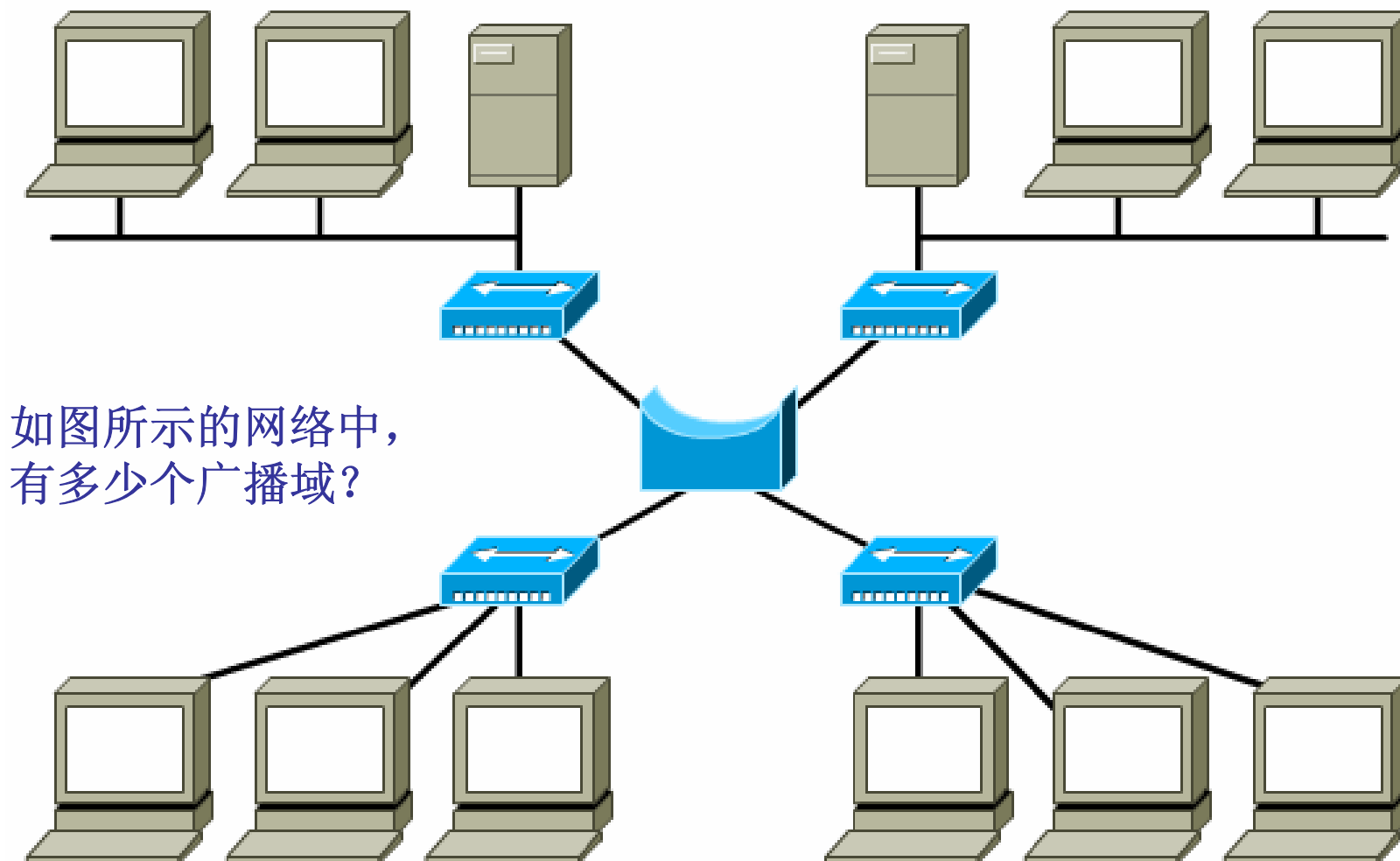


第一章 以太网交换



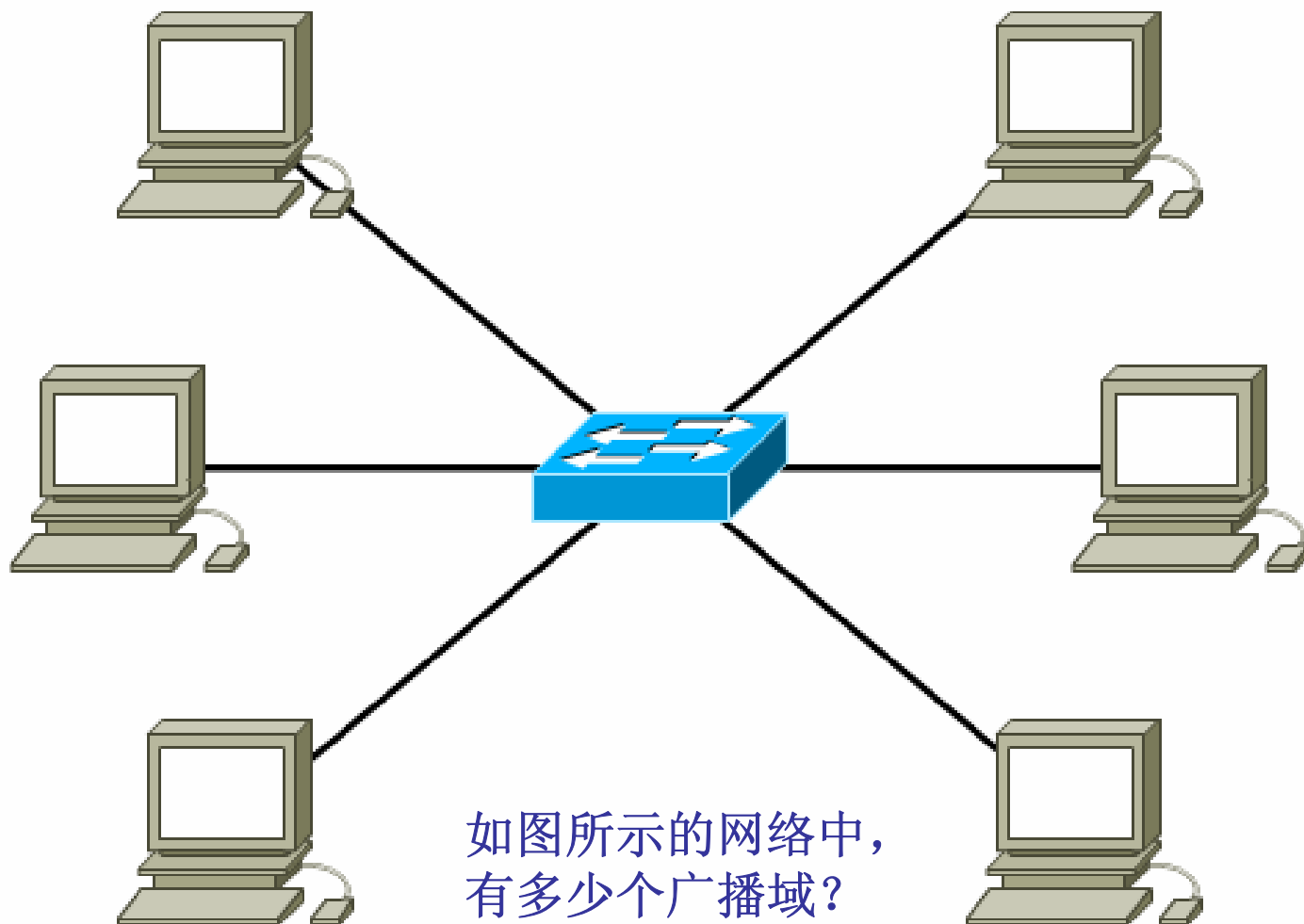
如图所示的网络中，
有多少个冲突域？

第一章 以太网交换

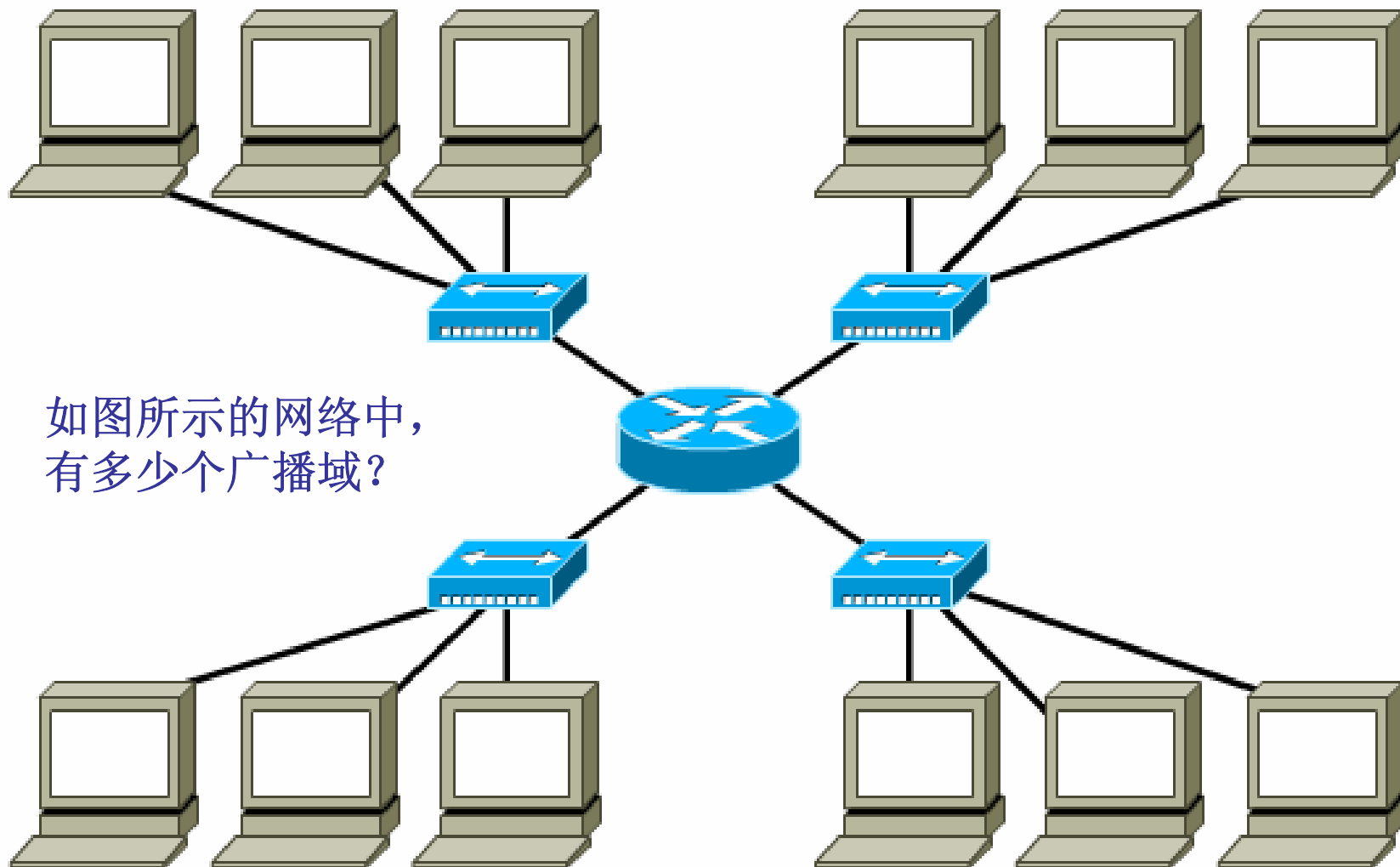


如图所示的网络中，
有多少个广播域？

第一章 以太网交换



第一章 以太网交换



如图所示的网络中，
有多少个广播域？

第一章 以太网交换

最早的以太网交换机出现在1995年，可简单理解为多端口网桥，连接在端口上的主机或网段独享带宽。交换机的算法相对较简单，硬件厂商将算法进行固化，生产出了交换机的核心ASIC芯片，实现了基于硬件的线速度交换机。

交换机是工作于OSI的第2层，能识别MAC地址，通过解析数据帧中目的主机的MAC地址，能将数据帧快速地从源端口转发至目的端口，提高了网络的交换和传输速度。

交换机的工作原理是存储转发，它将某个端口发送的数据帧先存储下来，通过解析数据帧，获得目的MAC地址，然后在交换机的MAC地址与端口对应表中，检索该目的主机所连接到的交换机端口，找到后就立即将数据帧从源端口直接转发到目的端口。

交换机各端口是独享带宽，并可实现全双工通讯。利用交换机提高了数据的交换处理速度和效率，但连接在交换机上的所有设备仍都处于同一个广播域。

第一章 以太网交换

二层交换机的主要功能：

- 1、地址学习（**address learning**）：通过查看帧的源MAC地址来加进转发/过滤表的MAC地址数据库里。
- 2、转发/过滤决定（**forward/filter decisions**）：当接口收到一个帧的时候，交换机查看目标MAC地址，寻找MAC地址数据库和接口，然后向符合条件的那个目标端口转发。
- 3、循环避免（**loop avoidance**）：假如有冗余的连接，可能会造成环路的产生，**STP**就用来阻止这些环路。

第一章 以太网交换

MAC地址

以太网上的主机在相互通讯时，需要一个用来识别该主机的介质访问控制地址（**Media Access Control**），即**MAC地址**，通常也称为物理地址或硬件地址。**MAC地址**被记录在网卡的**ROM**存储器中，全球唯一。网络中的计算机就是通过**MAC地址**来识别主机，并进行相互通讯的。

MAC地址采用**6字节48位**二进制编码表示，前**24位**是由生产厂家向**IEEE**申请的厂商地址，后**24位**是由生产厂家给网卡设定的一个编号，**MAC地址**显示格式为：**00-20-ED-6B-EE-B7**，采用十六进制数表示。在运行**IOS**操作系统的交换机中，**MAC地址**采用点三分格式表达，即表达为**0020.ed6b.eeb7**格式。

第一章 以太网交换

MAC地址表

交换机维护MAC地址表，通常也称为交换表。MAC地址表是交换机正常工作的基础，用于存放与该交换机端口所连设备的MAC地址的对应信息。

当某一设备接入交换机的某个端口之后，交换机会自动学习并添加该MAC地址与端口的对应关系到MAC地址表中，以后当有数据帧需要发送给该MAC地址时，交换机会首先在地址表中，找到对应该MAC地址的端口，然后直接将数据帧转发到该端口，到达目标。

查看交换机的MAC地址表：**show mac-address-table**

查看交换表老化时间：**show mac-address-table aging-time**

查看交换表中的地址数量和交换表的大小：**show mac-address-table count**

第一章 以太网交换

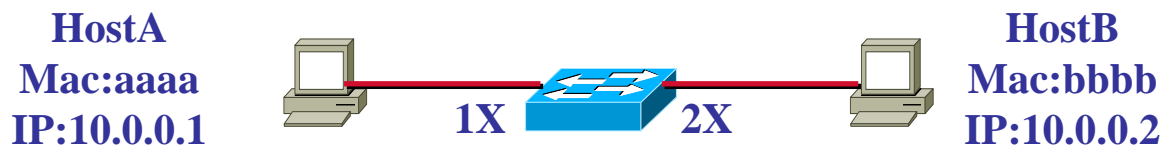


交换机初始化时MAC表为空。此时如果A向B发送数据，在收到A的数据帧后，首先抽取该帧中的源MAC并和相应的端口号保存到MAC表中，该过程称为地址学习。接下来，由于交换机还未学习到目标MAC对应哪个端口，它将洪泛该帧到除接收端口外的所有端口上。若B收到数据帧并响应，交换机收到后采取以下工作：

- 一、抽取该帧中源MAC值并和对应的端口保存到MAC表中；
- 二、抽取该帧中目标MAC值并以此值查找MAC表中对应的端口号；
- 三、如果查找成功将此帧只转发到该端口，如果不成功则洪泛。

经过一段时间的学习后交换机将会在MAC表中保存所有连接的MAC地址及其对应的端口号，并保存一定时间（默认30分钟）。如果某条记录在一定时间内没有被刷新，交换机将会删掉这条记录。

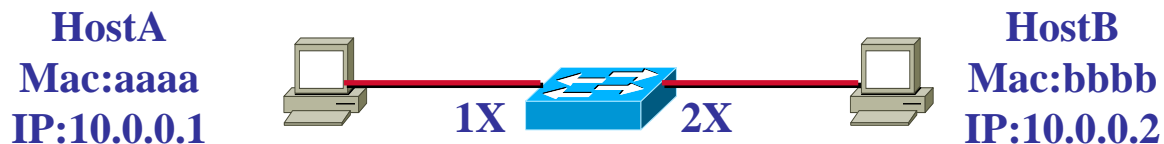
第一章 以太网交换



如图所示，HostA要与HostB通信，初始时PC机的ARP表为空，交换机的MAC表也为空。

- 1、HostA与HostB通信，源IP为10.0.0.1，目标IP为10.0.0.2，源MAC为aaaa，目标MAC为ffff（广播）；
- 2、交换机收到该帧，进行地址学习，根据源MAC和相应的端口号建立MAC表：1X----AAAA；
- 3、交换机进行洪泛，将该帧向除接收端口以外的所有端口发送；
- 4、HostB收到后，建立起ARP表，并回应。此时源IP为10.0.0.2，目标IP为10.0.0.1，源MAC为bbbb，目标MAC为aaaa；
- 5、交换机收到回应，继续地址学习，添加MAC记录：2X----BBBB；
- 6、交换机查找MAC表，得知MAC表中目标MAC为aaaa对应的端口号为1x，将回应帧从1x发出；

第一章 以太网交换



7、HostA接收，构建ARP表，通信完成。

8、在以后的通信过程中，因为HostA和HostB均建立了ARP表，且交换机维护MAC地址表，如果HostA继续与HostB通信，将在交换机的1X和2X进行转发，而不会发送到其他接口。除非HostA或HostB的ARP地址表被人为清空或超时老化，或者交换机的MAC地址表超时老化，此时将重复以上步骤。

9、如果新加入某主机HostC，也将按上述过程建立通信。

第一章 以太网交换

三种交换模式：

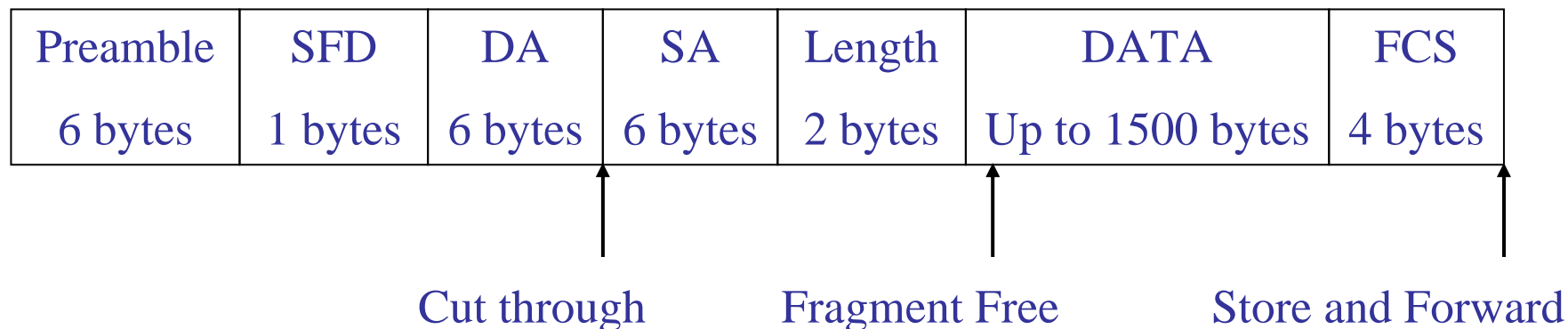
1、cut-through: 又称为**fastforward**或者**real time**模式。交换机只读取到帧的目标地址为止，延时小，但不适合高错误率的网络。转发速度最快，效率最高，可靠性最低。

2、fragmentfree: 交换机读取帧的前64字节，是**Catalyst 1900**的默认模式。由于一般情况下冲突发生在数据帧的前64字节内，所以在这种模式下交换机读取数据帧的前64字节内容才转发，转发速度中等，效率中等，可靠性中等。

3、store-and-forward: 在这个模式下，交换机复制整个帧到缓冲区，然后计算**CRC**，帧的长短可能不一样，所以延时因帧的长短而变化。如果**CRC**不正确，帧将被丢弃；如果正确，交换机查找硬件目标地址然后转发它们。转发速度最慢，效率最低，可靠性最高。

延时（latency）：指数据包进入一个网络设备到离开该设备的出口接口所花的时间，根据不同的交换模式而不同。

第一章 以太网交换



三种不同的转发模式

第一章 以太网交换

交换式以太网技术的优点：

交换式以太网不需要改变网络其它硬件，包括电缆和用户的网卡，仅需要用交换机替换共享式集线器，节省用户网络升级的费用。

可在高速与低速网络间转换，实现不同网络的协同。目前大多数交换式以太网都具有**100M bps**的端口，通过与之相对应的**100M bps**的网卡接入到服务器上，成为局域网升级时首选的方案。

它同时提供多个通道，比传统的共享式集线器提供更高的带宽。传统共享式**10/100M**以太网采用广播式通信方式，每次只能在一对用户间进行通信，而交换式以太网允许不同用户间进行传送。比如，一个**16**端口的以太网交换机允许**16**个站点在**8**条链路间通信。

第一章 以太网交换

交换机的性能指标

影响交换机性能的指标主要是**Mpps**和背板带宽。

Mpps是**Million Packet Per Second**的缩写，即每秒可转发多少个百万数据包。其值越大，交换机的交换处理速度也就越快。

背板带宽也是衡量交换机的重要指标之一，它直接影响交换机包转发和数据流处理能力。对于由几百台计算机构成的中小型局域网，几十**G bps**的背板带宽一般可满足应用需求；对于由几千甚至上万台计算机而构成的大型局域网，比如高校校园网或城域教育网，则需要支持几百**G bps**的大型三层交换机。

第一章 以太网交换

交换机的功能指标

- 1、地址学习（ **Address learning** ）
- 2、转发/过滤决定（ **Forward/filter decision** ）
- 3、避免环路（ **Loop avoidance** ）

第二章 交换机基础配置

配置交换机端口

端口选择

选择一个端口: **interface type mod/port**

Switch(config)#interface fastethernet 0/10

选择多个端口: **interface range type mod/startport - endport**

Switch(config)#interface range fastethernet 0/1 - 24

设置端口通讯速度: **speed [10|100|1000|auto]**

Switch(config-if)#speed 100

设置端口的单双工模式: **duplex [full|half|auto]**

Switch(config-if)#duplex full

控制端口协商

Switch(config-if)#(no) negotiation auto

第二章 交换机基础配置

配置交换机地址：

Switch(config)#interface vlan 1

Switch(config-if)#ip address

默认情况下，交换机的所有端口均属于VLAN1，VLAN1是交换机默认创建和管理的VLAN。

第二章 交换机基础配置

端口安全

端口安全是通过对MAC地址表的配置，来实现在某一端口只允许一台或者几台确定的设备（MAC）访问交换机的某个端口，从而增强交换机的安全性，提高局域网的安全性。

```
Switch(config)#mac-address-table secure 0008.a343.b581
```

```
Switch(config)#interface fastethernet0/12
```

```
Switch(config-if)#port-security maximum 1
```

```
Switch(config-if)#port-security violation shutdown
```

第二章 交换机基础配置

交换机密码恢复

1、交换机重新加电，按住**mode**按钮直到第一个**LED**灯熄灭

//中断正常启动

2、**switch: flash_init**

//初始化flash

3、**rename flash:config.text flash:*****

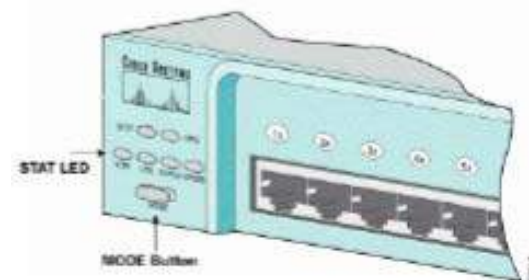
//将存放于**flash**中的配置文件改名，***为修改后的文件名

4、**switch: boot**

//重新启动交换机

5、**Would you like to enter the initial configuration dialog? [yes/no]: n**

//由于启动配置**config.text**的文件名被修改，交换机再次重启时将会找不到有效的配置文件，将进入到**Setup**模式，选择**No**



第二章 交换机基础配置

6、Switch>enable

//进入特权模式

7、Switch#rename flash:*** flash:config.text

//将在第3步中修改的文件名再回来

8、Switch#copy flash:config.text system:running-config

//将配置文件加载到内存

9、Switch(config)#enable secret cisco

//修改密码

10、Switch#copy running-config startup-config

//保存配置

第三章 生成树



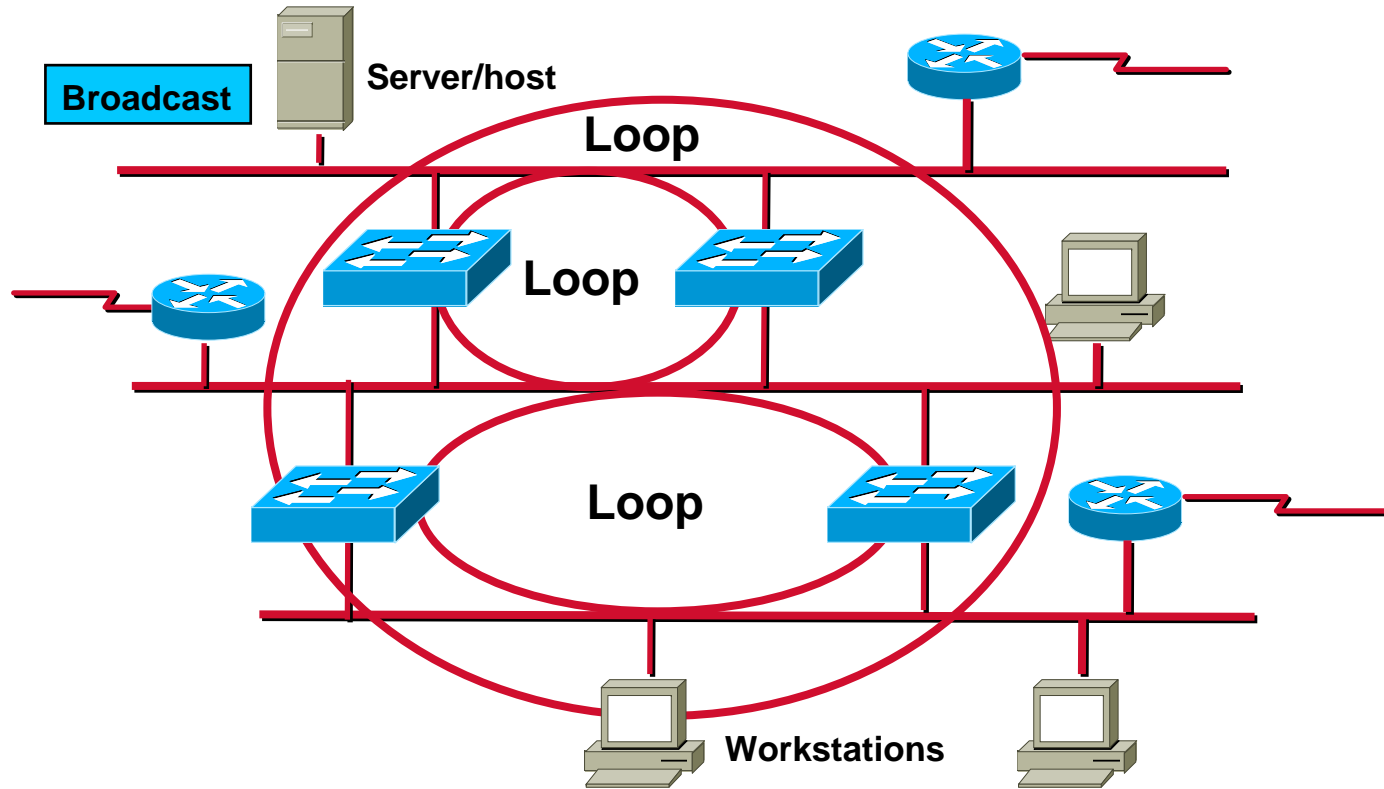
在网络中，为了防止单点的故障，设计了冗余的网络结构，但这种网络冗余结构可能会造成广播风暴和MAC地址表不稳定。

生成树协议（**Spanning Tree Protocol**）通过修改网络物理拓扑结构来构建一个无环路逻辑拓扑结构，提供了物理线路的冗余连接，消除了网络风暴，提高网络的稳定性和减少网络故障的发生率。

STP最早是**DEC**公司开发出来，后来被**802.1d**所采用。运行**STP**的交换机以一定的频率（默认每2秒发送一次）通过**BPDU**（**Bridge Protocol Data Unit**）互相交换信息。

STP的主要任务是防止第二层的环路，**STP**使用生成树算法（**Spanning-Tree Algorithm, STA**）来创建拓扑数据库，然后查找出冗余连接并阻止环路的产生。

第三章 生成树



复杂的网络结构可能会导致多个环路的产生

第三章 生成树

根桥（Root Bridge）：拥有最好的**Bridge ID**的交换机。

Bridge ID：由交换机优先级和MAC地址符合而成，ID最低的成为根桥。

非根桥（Nonroot Bridge）：不是根桥的交换机。

根端口（Root Port）：直接连接到根桥的端口，或者是到根桥开销最小的接口。如果开销相同就比较**Bridge ID**，低的将被选用。

指定端口（Designated Port）：根交换机的端口，作为转发端口。

端口开销（Port Cost）：由带宽决定。

非指定端口（nondesignated port）：开销较高，工作在阻塞模式（**Blocking Mode**），不转发帧。

转发端口（Forwarding Port）：转发端口用来转发帧。

阻塞端口（Blocked Port）：不转发帧，用来防止循环的产生，但可以监听（**Listen**）。

第三章 生成树

STP的任务就是查找出第二层网络中的所有连接，并关闭些会造成环路的冗余连接。

STP首先选举一个根桥，当所有的交换机认同了选举出来的根桥后，所有的交换机开始查找根端口。假如在交换机之间有许多连接，只能有1个端口作为指定端口。

1、选举根交换机

在一个网络中只能存在一个根交换机，具有最低**Bridge ID**的交换机成为根交换机。根交换机上的所有端口都是指定端口，处于转发状态。由于每两秒交换机交换**Bridge ID**，通过**STA**算法最终得出一个根交换机，其它交换机为非根桥交换机。

Bridge ID用来在**STP**域里选举根桥和决定根端口，这个ID 8字节长，包括2个字节的**Bridge Priority**（32768）和6个字节的**Bridge MAC**。**IEEE**版本的**STP**的默认优先级是32768。优先级的数值越小，优先级越高。如果优先级相同，则比较MAC地址，MAC地址小的成为根交换机。

第三章 生成树

2、每个非根桥交换机选举根端口

各个非根桥交换机根据到达根交换机的路径开销的大小选出根端口，根端口工作在转发状态。端口开销是一个可以累加的基于带宽的值。多段路径的开销进行累加，开销较小的成为为根端口。下面是一些典型的耗费标准：

10Gbps: 2

1Gbps: 4

100Mbps: 19

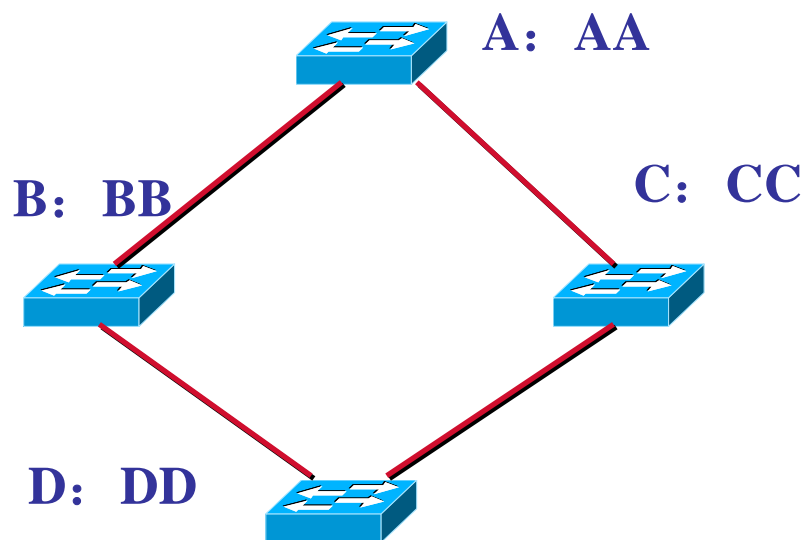
10Mbps: 100

3、每个段选举一个指定端口

在根桥基础上再选择指定端口。首先根据到根桥的端口开销，如果相同，再比较哪台交换机的**Bridge ID**，较低的成为指定端口，非指定端口处于阻塞状态。

第三章 生成树

如图所示的网络中，设四台交换机A、B、C、D的MAC地址分别为AA、BB、CC、DD。



1、选举根交换机

选举根交换机时，首先比较优先级，再比较MAC地址。

若优先级不同，则优先级数值最低的将成为根交换机。

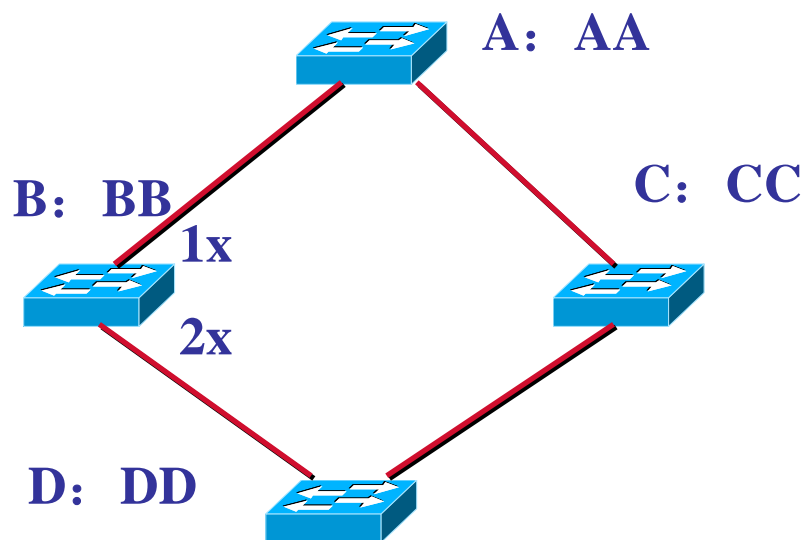
若四台交换机的优先级相同，则根据MAC，A交换机将成为根交换机。

此时A交换机上的两个端口成为指定端口，处于转发状态。

第三章 生成树

2、选举根端口

根交换机产生后，接下来选举根端口，选举根端口的原则：



首先比较从不同端口到达根交换机的开销，开销小的成为根端口。

假设每段链路均为100M带宽。

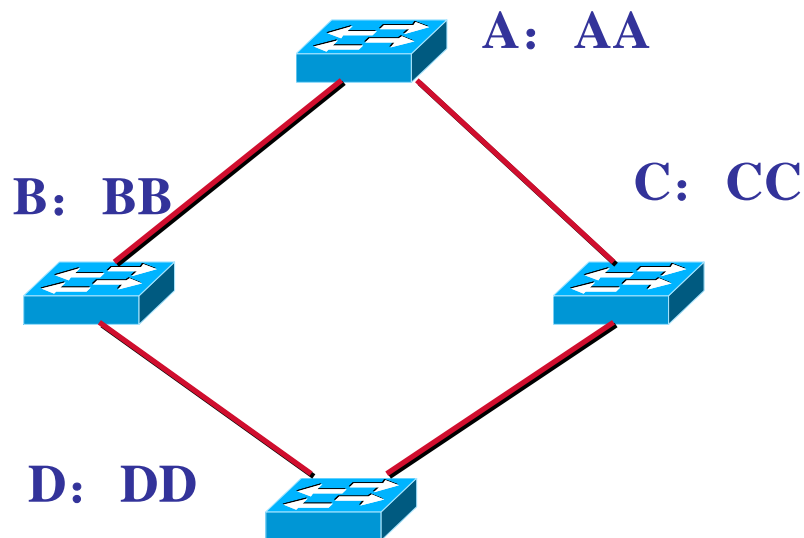
以B交换机为例，从B直接到A的路径开销为19，从B经D、C到A的路径开销为 $3 \times 19 = 57$ ，B交换机将会选择1x作为根端口。

若AB间带宽为10M，则从B直接到A的路径开销为100，B交换机将会选择2x作为根端口。

第三章 生成树

其次，比较从不同端口所接收到的**Bridge ID**。

仍假设各段带宽均为**100M**。



此时**D**交换机到达根交换机通过不同路径的开销相同，将比较从不同端口所接收的**Bridge ID**。

先比较所接收的端口优先级。

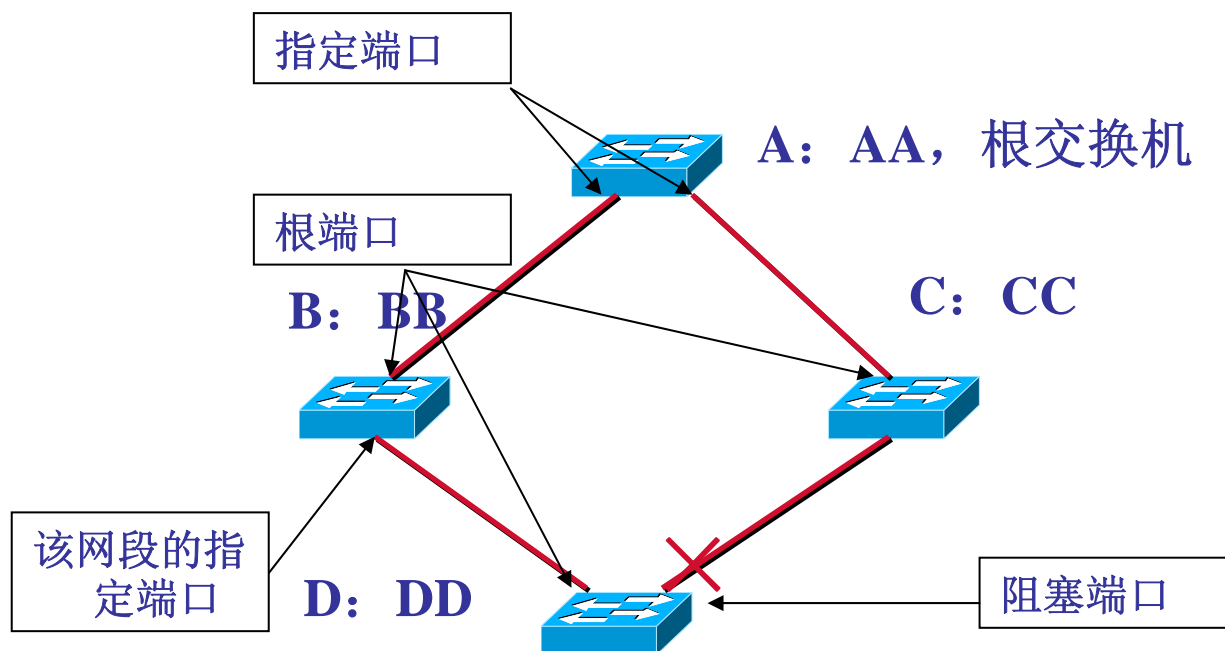
B和**C**分别连接到**D**交换机，若**C**交换机的端口优先级数值较小，则优先级较高，**D**交换机将会选择通过**C**到达根交换机，而关闭连接到**B**的端口。

如果端口优先级相同，再比较端口**MAC**。

由于**B**交换机的**MAC**地址小于**C**交换机，此时**D**交换机将会选择通过**B**到达根交换机，而关闭连接到**C**的端口。

第三章 生成树

在该拓扑中，如果所有链路的带宽、交换机优先级和端口优先级均相同，则最后的网络结构将如图所示。



由于大部分的网络流量都将经过根交换机，实际环境中，管理员可以通过修改优先级、设置开销等措施来设计指定配置比较高的、性能比较好的交换机来成为根交换机。

第三章 生成树

运行STP的5种端口状态

- 1、阻塞（**Blocking**）：端口不能接收或发送数据帧，也不能向MAC表中添加MAC地址，它只能接收BPDU以获取其它交换机信息。默认情况下，交换机启动时所有端口均为阻塞状态。
- 2、侦听（**Listening**）：端口侦听BPDU，来决定在传送数据帧之前没有环路产生。当该端口将被选为根端口或指定端口时，该端口将从阻塞状态转变为侦听状态，准备开始转发数据。处于此状态的端口不能接收或发送数据帧，但能接收或发送BPDU。
- 3、学习（**Learning**）：侦听BPDU和学习所有路径，学习MAC地址表，不转发帧。此状态下端口能够接收数据帧并能添加MAC地址，也能接收或发送BPDU。
- 4、转发（**Forwarding**）：转发和接收数据帧。工作状态，既能接收或发送数据，也接收或发送BPDU。
- 5、禁用（**Disabled**）：不参与帧的转发和STP。这种状态是由于人为关闭的。

第三章 生成树

默认情况下，从阻塞状态转到侦听状态需要**15秒**，从侦听状态转到学习状态需要**15秒**，从学习状态转到转发状态需要**20秒**。

一般来说，端口只处于转发和堵塞状态，如果网络拓扑发生了变化，端口会进入侦听和学习状态，这些状态是临时的。

第三章 生成树

Switch#show spanning-tree	//查看生成树
Switch#show spanning-tree brief	//查看生成树的主要信息
Switch#show spanning-tree vlan 1	//查看某VLAN下的生成树
Switch#show spanning-tree interface fastethernet 0/1	//查看某接口的生成树
Switch(config)#spanning-tree priority	//修改交换机的STP优先级
Switch(config-if)#spanning-tree cost	//修改端口的STP开销
Switch(config-if)#spanning-tree port-priority	//修改端口的STP优先级

第三章 生成树

快速生成树协议

为根端口和指定端口设置了快速切换用的替换端口（**Alternate Port**）和备份端口（**Backup Port**）两种角色，当根端口/指定端口失效的情况下，替换端口/备份端口就会无时延地进入转发状态。

在只连接了两个交换端口的点对点链路中，指定端口只需与下游网桥进行一次握手就可以无时延地进入转发状态。

直接与终端相连而不是把其他网桥相连的端口定义为边缘端口（**Edge Port**）。边缘端口可以直接进入转发状态，不需要任何延时。

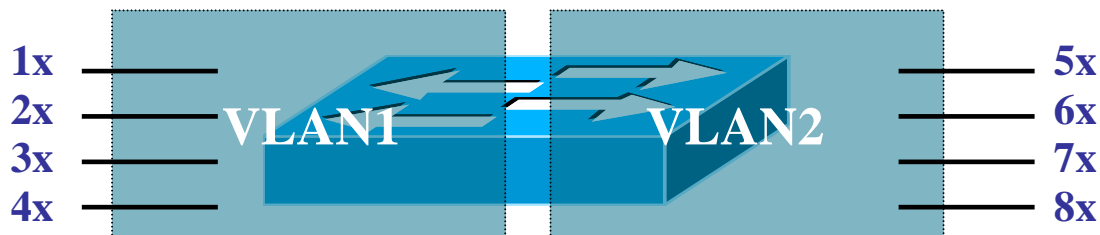
第四章 虚拟局域网

虚拟局域网（**Virtual Local Area Network, VLAN**）是将局域网从逻辑上划分为一个个的网段，从而实现虚拟工作组的一种交换技术。

使用集线器或交换机所构成的一个物理局域网，整个网络属于同一个广播域，广播帧或多播帧（**Multicast Frame**）都将被广播到整个局域网中的每一台主机。在网络通讯中，广播信息是普遍存在的，这些广播帧将占用大量的网络带宽，导致网络速度和通讯效率的下降，并额外增加了网络主机为处理广播信息所产生的负荷。

交换技术的发展，允许物理上分散的组织在逻辑上成为一个新的工作组，而且同一工作组的成员能够改变其物理地址而不必重新配置，这就是用到所谓的虚拟局域网技术（**VLAN**）。

第四章 虚拟局域网



划分VLAN，可起到以下方面的作用：

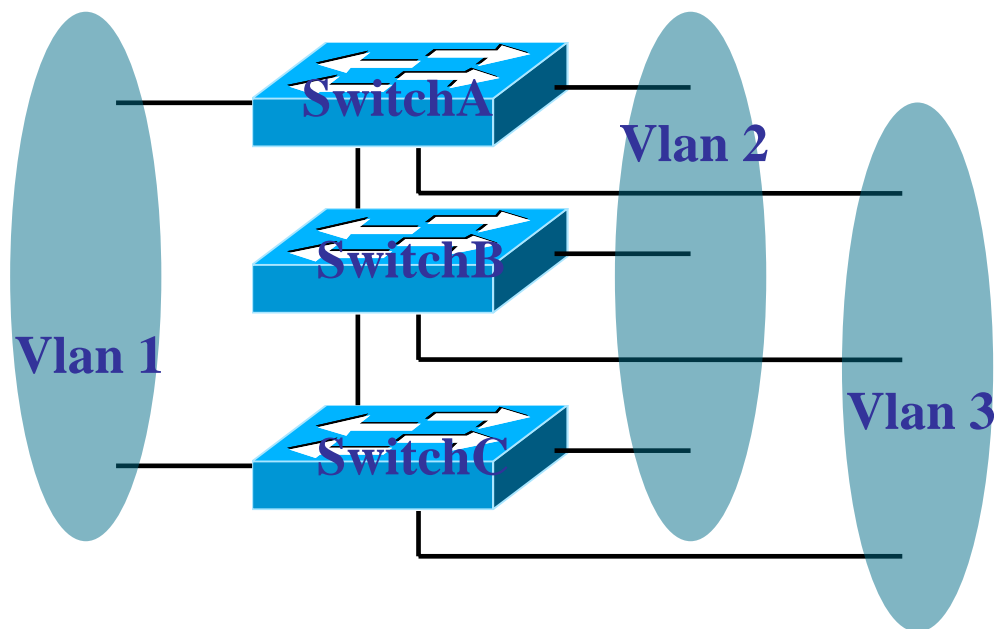
1、控制网络的广播，增加广播域的数量，减小广播域的大小。

该例中，未划分VLAN时，交换机的8个端口同属一个广播域；划分VLAN后，交换机的8个端口分属两个广播域。若划分更多的VLAN，则产生更多的广播域，广播域的范围越来越小。

2、增强网络的安全性。

在缺少路由的情况下，VLAN之间不能直接通讯，从而起到了隔离作用，并提高了VLAN中用户的安全性。VLAN间的通讯，可通过应用访问控制列表，来实现VLAN间的安全通讯。

第四章 虚拟局域网



3、便于对网络进行管理和控制。

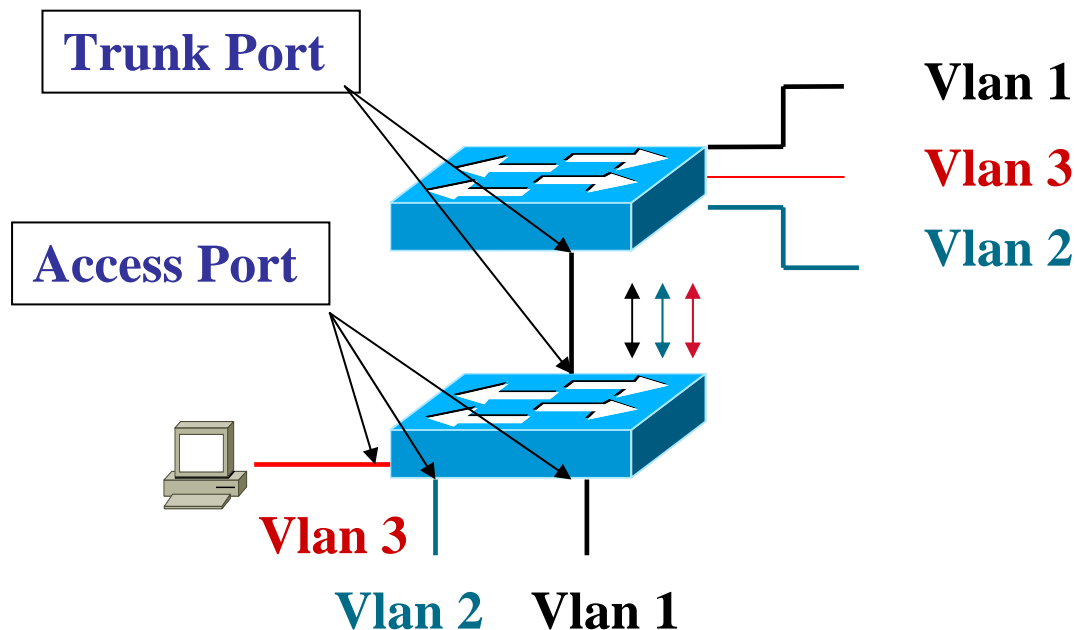
VLAN的设置不受任何物理连接的限制，同一VLAN中的用户，可以连接在不同的交换机，并且可以位于不同的物理位置，增加了网络连接、组网和管理的灵活性。

注意：划分VLAN后，每个VLAN将分别运行STP。

第四章 虚拟局域网

Access Port: 访问端口。指的是只属于某一个VLAN，且仅向该VLAN转发数据帧的端口，默认情况下交换机所有端口都属于访问端口。交换机在把帧从访问端口发送出去之前，需要移去任何的VLAN信息。

Trunk Port: 汇聚端口。指的是能够转发多个不同VLAN的通信的端口，该端口不属于某个VLAN。



第四章 虚拟局域网

静态VLAN

静态VLAN是明确指定各端口所属VLAN的设定方法，也称为基于端口的VLAN。属于同一个VLAN的端口，可来自一台交换机，也可来自多台交换机。

静态VLAN，需要逐个端口进行设置，适用于网络拓扑结构不是经常变化的情况，是最常用的一种VLAN划分方式。

动态VLAN

动态VLAN是根据每个端口所连的计算机，动态设置端口所属VLAN的方法，划分方法可基于MAC地址、子网或用户。

基于MAC地址的VLAN，是根据端口所连计算机的网卡MAC地址，来决定该端口所属的VLAN。

基于子网的VLAN，是根据端口所连计算机的IP地址，来决定端口所属的VLAN。

基于用户的VLAN，是根据端口所连计算机的当前登录用户，来决定该端口所属的VLAN。

第四章 虚拟局域网

创建静态VLAN:

vlan vlan-id name vlan-name

vlan-id 要创建的VLAN的数字编号

vlan-name VLAN的名称（可选）。

例:

Switch#vlan database

Switch(vlan)#vlan 2 name abc

Switch(vlan)#apply

Switch(vlan)#exit

Switch#

默认情况下，交换机会自动创建和管理VLAN 1，VLAN 1作为管理VLAN，不能被删除、修改。

第四章 虚拟局域网

查看VLAN

Switch#show vlan

VLAN	Name	Status	Ports
-----	-----	-----	-----
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20, Fa0/21, Fa0/22, Fa0/23, Fa0/24
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

第四章 虚拟局域网

划分端口

首先选择端口，然后在接口配置模式，通过以下配置命令来实现：

switchport access vlan vlan-id

其中，**vlan-id**为VLAN的id号，表示将端口划入哪一个VLAN。

Switch(config)#interface fastethernet 0/1

Switch(config-if)#switchport mode access

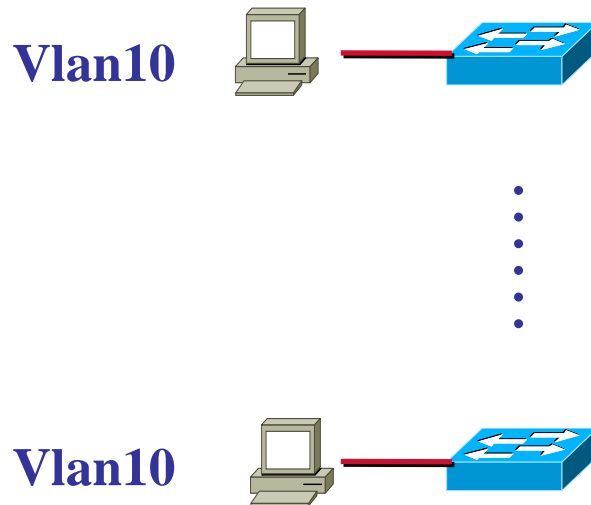
Switch(config-if)#switchport access vlan 2

配置完成后，查看VLAN信息，将会发现F0/1不再属于VLAN1。

第四章 虚拟局域网

VLAN的汇聚链接与封装协议，VTP

在实际应用中，通常需要跨越多台交换机的多个端口划分VLAN。例如，不同部门的员工组成的项目小组，可能会分布在不同的建筑物或不同的楼层中，此时的VLAN，就将跨越多台交换机。

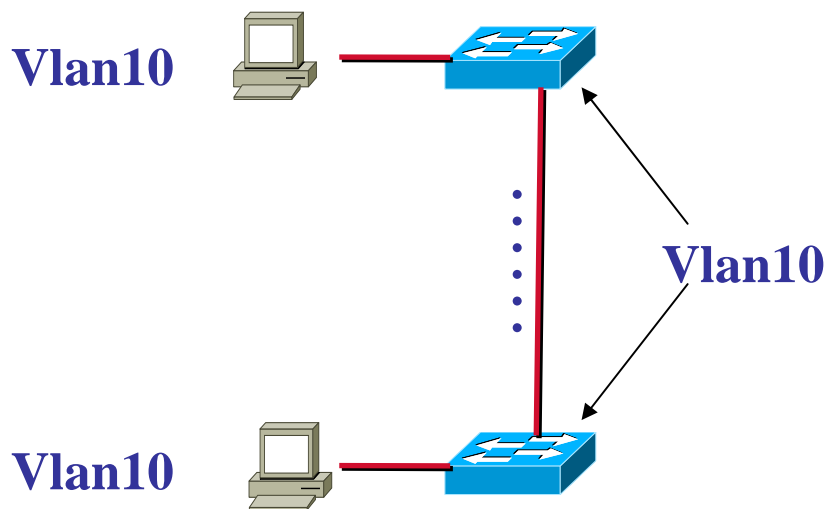


第四章 虚拟局域网

当同一VLAN成员分布在多台交换机上时，相互之间如何通讯？

一种解决的办法就是在交换机上各拿出一个端口，用于将两台交换机连接起来，这两个端口属于这个VLAN，专门用于该VLAN的跨交换机相互通讯。有多少个VLAN，就对应地需要占用多少个端口。

这种方法虽然解决了问题，但每增加一个VLAN，就需要在交换机间添加一条链路，并占用交换机端口，是一种严重的浪费，而且扩展性和可管理性都很差。

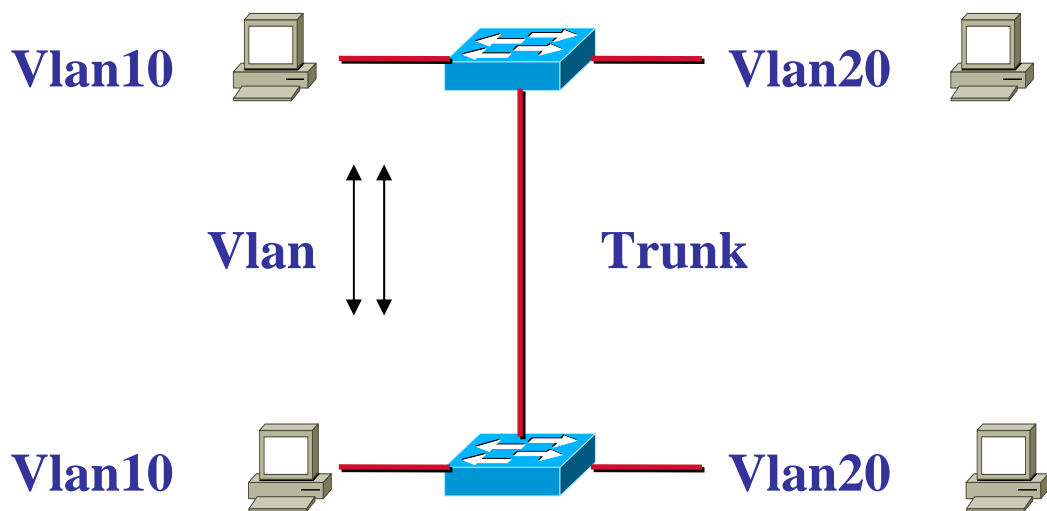


第四章 虚拟局域网

汇聚链路

为了避免这种低效率的连接方式和对交换机端口的大量占用，有效的解决办法是让交换机间的互联链路汇集到一条链路上，让该链路允许指定VLAN的通讯流经过，这样就可解决对交换机端口的额外占用，这条用于实现各VLAN在交换机间通讯的链路，称为交换机的汇聚链路或主干链路（**Trunk Link**）。

用于提供汇聚链路的端口，称为汇聚端口。只有100Mbps或以上的端口，才能作为汇聚端口使用。



第四章 虚拟局域网

由于汇聚链路承载了所有VLAN的通讯流量，为标识各数据帧属于哪一个VLAN，需要对流经汇聚链接的数据帧进行打标（**Tag**）封装，以附加上VLAN信息，这样交换机就可通过VLAN标识，将数据帧转发到对应的VLAN中。

Frame tagging: 帧标签。当帧到达交换机后，首先检查**VLAN ID**，然后决定如何对帧进行处理。当帧到达和**VLAN ID**所匹配的端口时，交换机移去VLAN标识符后从端口发送。

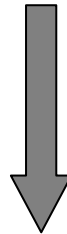
目前交换机支持的打标封装协议有**IEEE 802.1Q**和**ISL**。其中**802.1Q**是经过**IEEE**认证的对数据帧附加VLAN识别信息的协议，属于国际标准协议，适用于各个厂商生产的交换机，该协议通常也简称为**dot1q**。

802.1Q所附加的VLAN识别信息，位于数据帧中“发送源**MAC**地址”和“类别域（**Type Field**）”之间，所添加的内容为2字节的**TPID**和2字节的**TCI**，共计4个字节。

第四章 虚拟局域网

Ethernet

目标MAC地址	源MAC地址	类型	数据部分	CRC
6 bytes	6 bytes	2 bytes	46~1500 bytes	4 bytes



IEEE 802.1Q

目标MAC地址	源MAC地址	TPID	TCI	数据部分	新的CRC
6 bytes	6 bytes	2 bytes	2 bytes	46~1500 bytes	4 bytes

第四章 虚拟局域网

ISL是**Inter Switch Link**的缩写，是**Cisco**系列交换机用于在汇聚链路上附加**VLAN**信息的协议，可用于以太网和令牌环网。

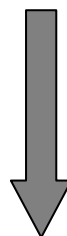
ISL对数据帧进行打标封装时，采取在数据帧的头部附加**26**字节的**ISL**包头，并且在数据帧的尾部带上对包括**ISL**包头在内的整个数据帧进行计算后得到的**4**字节的**CRC**值。**ISL**协议保留数据帧原来的**CRC**，然后再附加上一个新的**CRC**，即封装时总共增加了**30**个字节的信息。当数据帧离开汇聚链路时，**ISL**只需简单地去除**ISL**包头和新**CRC**就可以了，由于数据帧原来的**CRC**被完整保留，因此无需重新计算。大多数**Cisco**设备都支持**ISL**。**ISL**是由硬件**ASIC**完成的，速度快，**ISL**最多支持**1024**个**VLAN**。

ISL与**IEEE802.1Q**协议互不兼容，**ISL**是**Cisco**的私有协议。

第四章 虚拟局域网

Ethernet

目标MAC地址	源MAC地址	类型	数据部分	CRC
6 bytes	6 bytes	2 bytes	46~1500 bytes	4 bytes



ISL

ISL头	目标MAC地址	源MAC地址	类型	数据部分	原来的CRC	新的CRC
26 bytes	6 bytes	6 bytes	2 bytes	46~1500 bytes	4 bytes	4 bytes

包含VLAN编号

第四章 虚拟局域网

配置汇聚链路，先选择要配置的交换机端口，设置封装协议，然后再通过**switchport mode trunk**配置命令来启用该端口的**trunking**功能：

```
Switch(config)#interface fastethernet 0/1
```

```
Switch(config-if)#switchport mode trunk
```

```
Switch(config-if)#switchport trunk encapsulation [isl|dot1q]
```

Switchport mode trunk命令用于激活启用端口的链路聚集功能。若要在该端口上禁用**trunking**功能，则使用**no switchport mode trunk**配置命令。

Switchport trunk encapsulation用于设置汇聚链路采用的打标封装协议，**isl**或**dot1q**。

第四章 虚拟局域网

VTP（VLAN Trunking Protocol，VLAN链路聚集协议）是一个在建立了汇聚链路的交换机之间同步和传递**VLAN**配置信息的协议，以在同一个**VTP**域中维持**VLAN**配置的一致性。在同一个**VTP**域中的交换机，可通过**VTP**协议来互相学习**VTP**信息。**VTP**协议对于运行**ISL**或**IEEE802.1Q**封装协议的汇聚链路都适用。

VTP的主要目的是在交换网络中管理**VLAN**。**VTP**允许增加，删除和修改**VLAN**，然后这些修改后的信息传播到整个**VTP**域里的所有交换机上，并修改**VLAN**数据库。

在创建**VLAN**之前，应先定义**VTP**管理域。**VTP**消息能在同一个**VTP**管理域内，同步和传递**VLAN**配置信息。另外，利用**VTP**协议，还能实现从汇聚链路中，裁剪掉不需要的**VLAN**流量。

第四章 虚拟局域网

VTP有Server、Client和Transparent（透明）三种工作模式，这些工作模式决定了交换机管理VLAN、VTP如何传送和同步VLAN配置。

Server模式：是交换机默认的工作模式。该模式下允许创建、修改和删除本地VLAN数据库中的VLAN，并允许发布VLAN数据库的更新和接收同一个VTP域内其他交换机发送来的同步信息。

Client模式：该模式下不能创建、修改和删除VLAN，也不能在NVRAM中存储VLAN配置，如果重启或掉电，将丢失所有的VLAN信息。该该模式下主要通过VTP域内其他交换机的VLAN配置信息来同步和更新自己的VLAN配置。

Transparent模式：可以创建、修改和删除本地VLAN数据库中的VLAN，但VLAN配置的变化，不会传播给其他交换机，仅对交换机自身有效。

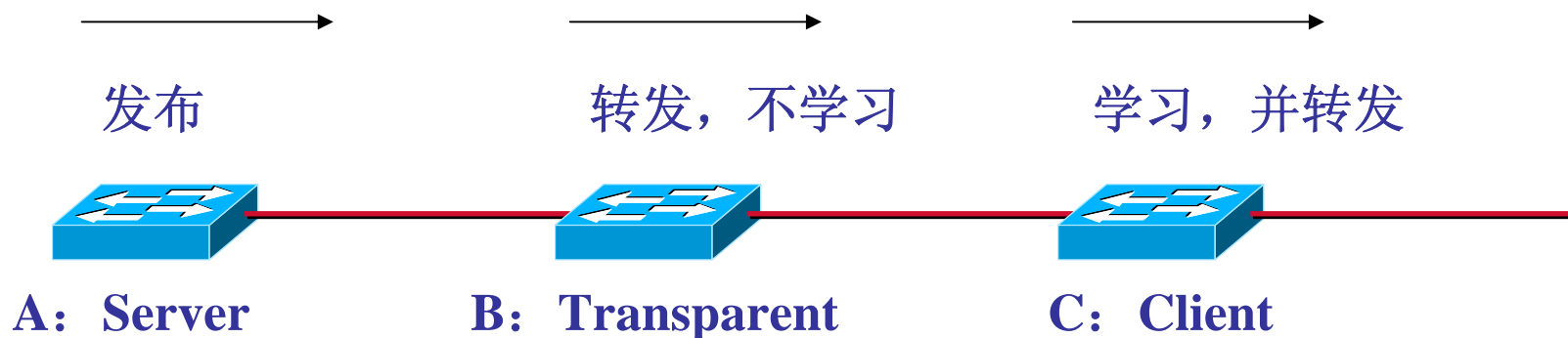
第四章 虚拟局域网

设三台交换机A、B、C均属于同一个VTP域中，工作模式如图所示。

当在A交换机上创建了一个新的VLAN后，A交换机的VTP配置版本加1，将向外发布。

由于B交换机的工作模式是透明模式，B交换机将不会学习这个新的VLAN，不会把这个新的VLAN添加到自己的VLAN数据库中，B交换机仅仅向下转发。

C交换机收到后，修改自己的VLAN数据库，添加新的VLAN。



第四章 虚拟局域网

创建VTP管理域： `vtp domain domain_name`

只有属于同一个vtp域的交换机彼此间才能交换VLAN信息。一个交换机只能同时属于某一个VTP域。

domain_name代表要创建的vtp管理域。名称是区分大小写的，仅用于同步VLAN配置信息。

Switch(vlan)#vtp domain cisco

设置VTP模式： `vtp [server|client|transparent]`

该命令在vlan数据库配置模式下运行，用于设置VTP的工作模式。

Switch(vlan)#vtp server

第四章 虚拟局域网

配置端口

Switch(config)#interface fastethernet 0/1

Switch(config-if)#switchport mode trunk

//配置该语句后查看VLAN，将发现该接口不属于某一个VLAN

Switch(config-if)#switchport trunk encapsulation isl 或 dot1q

Switch(config-if)#switchport trunk allowed vlan all

//默认情况下，允许所有VLAN通过

Switch(config-if)#switchport trunk allowed vlan remove 3

//VLAN 3将被移除

Switch(config-if)#switchport trunk allowed vlan add 4

//VLAN 4将被增加

第四章 虚拟局域网

Switch#show vtp status

VTP Version	: 2
Configuration Revision	: 10
Maximum VLANs supported locally	: 68
Number of existing VLANs	: 8
VTP Operating Mode	: Server
VTP Domain Name	: cisco
VTP Pruning Mode	: Disabled
...	

第四章 虚拟局域网

注意到其中的**Configuration Revision**（配置修订号或配置版本号），当交换机成功地增加或删除VLAN时，每Apply一次，配置版本号的计数将加1，初始值为0。

交换机通过VTP通告来检测VLAN变化并更新VLAN数据库，如果检测到VTP的版本号比本交换机的版本高，则更新VLAN数据库。



A: Server模式，配置版本号为10

**VLAN数据库中有4、5、6、7、8
五个VLAN**

B: Client模式，配置版本号为12

**Vlan数据库中有2、3、4、5、6
五个VLAN**

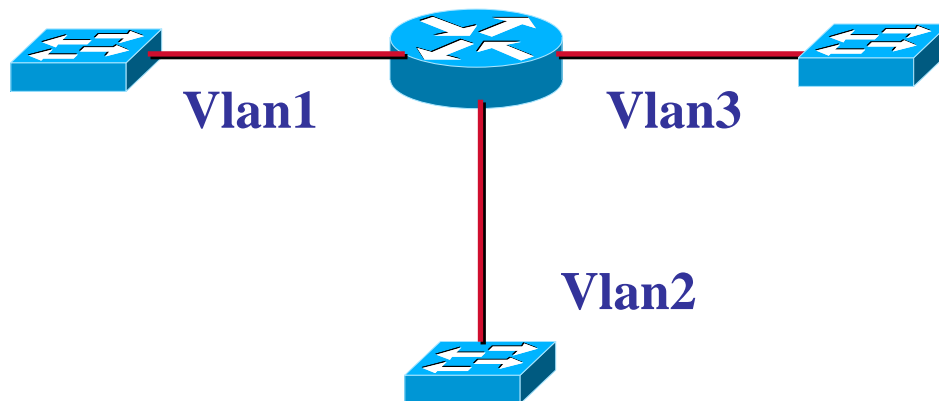
若两台交换机正确的配置了汇聚链路并在同一个VTP域中，两台交换机最后会有哪些VLAN存在？

第四章 虚拟局域网

划分VLAN后，VLAN间是不能进行直接通信的，从而就实现了对广播域的分割和隔离。

若要实现VLAN间的通讯，就必须为VLAN设置路由，这可使用路由器或三层交换机来实现。

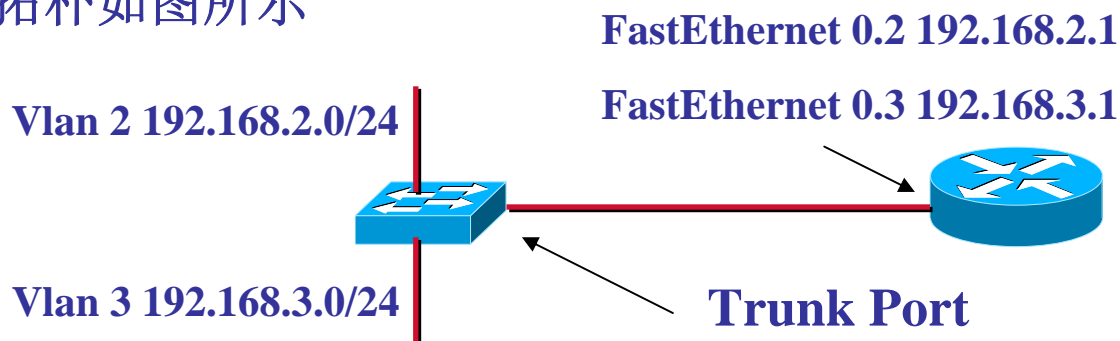
当VLAN数目比较少时，可用如下拓扑结构，路由器的每个以太网口对应一个VLAN。



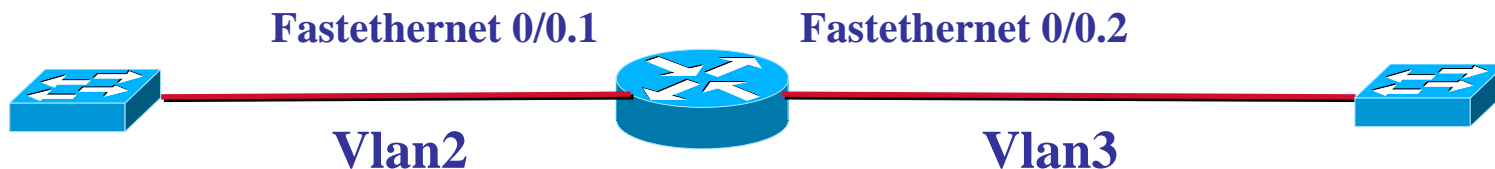
第四章 虚拟局域网

但当VLAN数目比较多，这时候可以采用划分子接口的形式来实现路由。这种方式称为单臂路由（**route on a stick**）。

此时的物理拓扑如图所示



逻辑拓扑如图所示



第四章 虚拟局域网

采用外部路由的方式时，路由器的快速以太网接口与交换机的端口以汇聚链路的方式相连，并在路由器的快速以太网接口上，为每一个VLAN创建一个对应的虚拟子接口，并设置虚拟子接口的IP地址，该IP地址以后就成为该VLAN的默认网关（路由）。路由器会自动在路由表中，为各VLAN添加路由，从而实现VLAN间的路由转发。

```
Trunkrouter(config-if)#int f0/0.1
```

```
Trunkrouter(config-subif)#encapsulation isl 1    //对应VLAN 1
```

```
Trunkrouter(config-subif)#ip address 172.16.10.1 255.255.255.0
```

```
Trunkrouter(config-if)#int f0/0.2
```

```
Trunkrouter(config-subif)#encapsulation isl 2    //对应VLAN 2
```

```
Trunkrouter(config-subif)#ip address 172.16.20.1 255.255.255.0
```

```
...
```

第四章 虚拟局域网

第三层交换

三层交换机是指具备路由功能的交换机，其端口（接口）可以实现基于三层寻址的分组转发，每个三层接口都定义了一个单独的广播域，在为接口配置好IP协议后，该接口就成为连接在该接口的同一个广播域的网关。

三层交换机的路由模块与交换模块共同使用ASIC硬件芯片，可实现高速数据转发，并且在对第一个数据帧进行路由后，将产生一个MAC地址与IP地址的映射表，当同样的数据帧再次通过时，交换机会直接从二层转发，而不需要再通过路由，从而提高了数据包转发的效率。另一方面，交换机的路由模块与交换模块是在交换机内部直接汇聚连接的，可以提供相当高的带宽。因此，使用三层交换机来提供VLAN间的通讯，比使用二层交换机和路由器更好，配置和使用也更方便。

第四章 虚拟局域网

一个具有第三层交换功能的设备是一个带有第三层路由功能的第二层交换机，但并不是简单的把硬件及软件简单地进行叠加，它是二者的有机结合。

第三层交换具有以下突出特点：

1、有机的硬件结合使得数据交换加速

从硬件上看，第二层交换机的接口模块都是通过高速背板/总线（速率可高达几十G bit/s）交换数据的。在第三层交换机中，与路由器有关的第三层路由硬件模块也插接在高速背板/总线上，这种方式使得路由模块可以与需要路由的其他模块间高速的交换数据，从而突破了传统的路由器外部接口速率的限制。

2、优化的路由软件使得路由过程效率提高

对于数据包的转发：如IP/IPX包的转发，通过硬件得以高速实现。

对于第三层路由软件：如路由信息的更新、路由表维护、路由计算、路由的确定等功能，用优化、高效的软件实现。

第四章 虚拟局域网

3、除了必要的路由选择过程外，大部分数据转发由第二层交换处理。假设两台机器通过第三层交换机进行通信的过程。

A机在发送时，已知目的IP地址，但不知道B机的MAC地址，要用ARP来确定目的MAC地址。A机把自己的IP地址与目的IP地址比较，确定B机是否与自己在同一子网内。

若在同一子网，A机广播一个ARP请求，B机返回其MAC地址，A机将这一地址缓存起来，并用此MAC地址封包转发数据，第二层交换模块查找MAC地址表确定将数据包发向目的端口。

若不在同一子网，A机向默认网关发送ARP请求，而默认网关实际上对应三层交换机的交换模块。若交换模块在以往的通信中已得知B机的MAC地址，则向A机回复B机的MAC地址；若未知，交换模块将根据路由信息向目标设备广播ARP请求，B机回复其MAC地址，交换模块保存此地址并回复给A机。

以后，若A与B继续通信，将用最终的目标主机的MAC地址封装，数据转发过程全部交给第二层交换处理，信息得以高速交换。即所谓的一次路由，多次交换。

第四部分 广域网通信

第一章 广域网技术

第二章 **PPP**

第三章 **ISDN与DDR**

第四章 **Frame Relay**

第五章 **NAT**

第一章 广域网技术

WAN: Wide Area Network

WAN是覆盖地理范围相对较为广阔的数据通信网络，它一般是利用公共载体(比如电信公司)提供的设备进行传输。**WAN**技术运行在**OSI**的最下**3**层。

通常需要从服务提供商（**ISP**）处租用**WAN**服务。最终用户并不关心服务商采用什么样的技术和信令，对于用户是透明的。

第一章 广域网技术

专线：也称为点到点连接或专用连接。

通过服务商网络在用户和远程互连网络之间提供一条预先建立的WAN通信路径。

专线不存在共享连接所存在的保密性、安全性和呼叫建立与拆除等问题，但价格昂贵。

专线通常采用同步串行连接，最大速率可达T3/E3（45Mbit/s），一般使用HDLC和PPP的封装格式。

第一章 广域网技术

电路交换：呼叫期间，收发双方之间必须有专用的电路路径，如电话和**ISDN**。

每次呼叫时，将临时建立一条路径，整个呼叫期间，路径保持不变，但以后的呼叫可能会使用其他路径。

通常用于偶尔使用**WAN**的环境中。

第一章 广域网技术

分组交换（包交换）：多个用户的网络设备共享一条点到点或点到多点链路，通过服务商网络将分组从源传输到目的，如帧中继。

分组交换技术能够使网络节点动态的分享网络介质和可用带宽。分组交换网络支持可变长度数据包，数据的传输更加有效和灵活。所有的数据包基于交换机制在不同的网段之间进行传递，直到到达最终的目的地。分组交换网络使用统计复用技术控制网络接入，使网络带宽的使用更加灵活和高效。

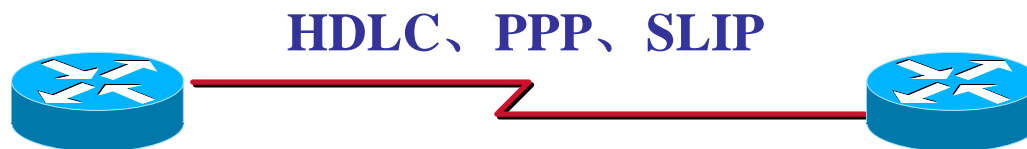
分组交换使用永久虚电路（PVC）或交换虚电路（SVC）来提供端到端的连接性。

和专线类似，服务商和客户之间有专用的带宽。但帧被传递到服务商后，将与其他用户共享带宽。

信元交换：类似于分组交换，但数据被分为定长的信元，然后通过虚电路进行传输。如ATM。

第一章 广域网技术

专线



分组交换



电路交换



第一章 广域网技术

HDLC: 高级数据链路控制, 是Cisco路由器默认的封装类型, 用于点到点专用链路和电路交换。

PPP: 点到点, 是一种标准, 提供路由器到路由器以及主机到网络的连接, 支持多种物理标准, 支持多种网络层协议, 内置了安全机制如**PAP** (密码验证协议) 和**CHAP** (挑战握手验证协议), 还支持**DHCP**和压缩。

SLIP: 串行线路Internet协议, 用于使用TCP/IP的点到点串行连接的标准协议, 已被PPP替代。

LAPB: 平衡链路接入过程, 定义了如何在DTE和DCE之间建立和维护连接, 以便远程终端和计算机能够通过不可靠的链路进行接入和通信。是1种面向连接的协议, 一般和X.25技术一起进行数据传输。因为它有严格的窗口和超时功能, 所以使得代价很高。

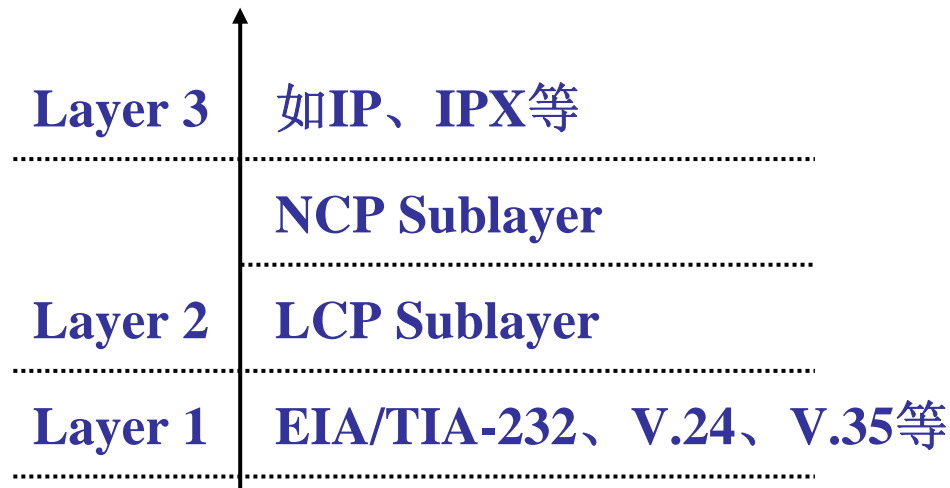
Frame-Relay: 帧中继, 是一种基于分帧技术的行业标准数据链路层协议, 能够处理多条虚电路。

ATM: 异步传输模式, 是一种信元中继国际标准, 以定长的 (长度为53字节) 信元传输多种数据流。由于信元长度固定, 因此可以使用硬件进行处理, 降低延迟。

第二章 PPP

PPP（Point-to-Point Protocol）即点对点协议，该协议提供在链路层的全双工操作，并按照顺序传递数据包，目前已成为各种主机、网桥和路由器之间通过拨号或专线方式建立点对点连接的首选方案。

PPP同时协商网络层服务，分为两个子层：**LCP**（链路控制协议）和**NCP**（网络控制协议）。**PPP**使用**NCP**来封装多种协议，使用**LCP**来协商和设置**WAN**数据链路的控制选项。



第二章 PPP

LCP提供不同的**PPP**封装选项包括：

☆验证：用于验证呼叫方身份，包括**PAP**和**CHAP**

☆压缩（**Compression**）：加快数据收发，在接收方解压缩

☆错误检测（**Error Detection**）：使用**Quality**和**Magic Number**来保证数据可靠性

☆多重连接（**Multilink**）：从**IOS**版本**11.1**开始

☆回呼（**Callback**）：客户端连接远端并进行验证，验证通过后，远端将终止连接，然后由服务器端重新发起连接。

LCP的三种帧：

链路建立帧：建立和配置链路

链路终止帧：终止链路

链路维护帧：管理和维护链路

第二章 PPP

PPP会话的建立:

- 1、链路建立阶段：该阶段中，每台**PPP**设备都发送**LCP**分组，以配置和检测数据链路。分组中包含配置选项，让设备对包括压缩、身份验证等选项进行协商。
- 2、身份验证阶段（可选）
- 3、网络层协议阶段：该阶段中，**PPP**设备发送**NCP**分组，以选择并配置一种或多种网络层协议。

第二章 PPP

RouterA#show int s0

Serial0 is up, line protocol is up

...

Encapsulation PPP, loopback not set, keepalive set (10 sec)

LCP Open

Listen: IPXCP

Open: IPCP, CDPCP, ATCP

第二章 PPP

口令验证协议**PAP**（**Password Authentication Protocol**）：是一种简单的明文验证方式。网络接入服务器**NAS**（**Network Access Server**）要求用户提供用户名和口令，用户在链路上发送用户名和密码，直至认证通过，否则连接终止。

挑战握手验证协议**CHAP**（**Challenge-Handshake Authentication Protocol**）：是一种加密的验证方式，能够避免建立连接时传送用户的真实密码。**NAS**向远程用户发送一个挑战口令，其中包括会话**ID**和一个任意生成的挑战字符串（**Arbitrary Challenge String**）。远程客户必须使用**MD5**单向哈希算法返回用户名和加密的挑战口令，会话**ID**以及用户口令，其中用户名以非哈希方式发送。

第二章 PPP

PPP配置步骤:

配置本地路由器名

配置本地路由器口令

配置对端路由器的用户名和口令

封装PPP协议

指定PPP协议验证方式

第二章 PPP

封装PPP协议

encapsulation PPP

设置对端拨号的用户名和口令

username *username* password *password*

其中**username**为对端的用户名，**password**为对端用户名对应的口令。

配置验证方式

**ppp authentication {chap | chap pap | pap chap | pap} [list-name]
[callin]**

两端的路由器必须使用相同的验证方式

设置压缩算法

compress mppc|predictor|stac

第二章 PPP

PAP验证

使用两次握手为远程节点提供了一种简单的验证方法，只在建立链路时进行。

密码以明文方式通过链路传输，不能防御重复尝试。

登录尝试的频率和时间由远程节点控制。



第二章 PPP



```
ra(config)#interface serial 0
ra(config-if)#ip address 10.0.0.1 255.0.0.0
ra(config-if)#encapsulation ppp
ra(config-if)#ppp pap sent-username roa password abcd
rb(config)#username roa password abcd
rb(config-if)#interface Serial0
rb(config-if)#ip address 10.0.0.2 255.0.0.0
rb(config-if)#encapsulation ppp
rb(config-if)#ppp authentication pap
debug ppp authentication, 查看验证过程
```

第二章 PPP

CHAP验证

在建立链路时运行，并定期运行，使用三次握手来核实远程节点的身份。

链路建立阶段结束后，本地路由器向远程节点发送挑战信息，后者使用一个单向**Hash**函数计算得到的值进行响应。**MD5**哈希值是根据挑战信息、密码、随机数等得到的。本地路由器将远程路由器响应的值与自己计算得到的哈希值进行比较，如果相同，能通过，不同则终止连接。



第二章 PPP



```
ra(config)#username rb password abcd
```

```
ra(config-if)#interface Serial0
```

```
ra(config-if)#ip address 10.0.0.1 255.0.0.0
```

```
ra(config-if)#encapsulation ppp
```

```
ra(config-if)#ppp authentication chap
```

```
rb(config)#username ra password abcd
```

```
rb(config-if)#interface Serial0
```

```
rb(config-if)#ip address 10.0.0.2 255.0.0.0
```

```
rb(config-if)#encapsulation ppp
```

```
rb(config-if)#ppp authentication chap
```

第三章 ISDN与DDR

ISDN (Integrated Service Digital Network)：是以综合数字电话网 (IDN) 为基础发展演变而成的通信网，在已有的电话线路上传输语音和数据等数字服务。ISDN参考了ITU-T标准，运行在OSI参考模型的下三层。

ISDN标准定义了硬件和呼叫建立的机制来保证端到端的数字化连接。

☆可以同时传输语音、数据和视频

☆建立会话的速度比传统拨号要快，数据传输快

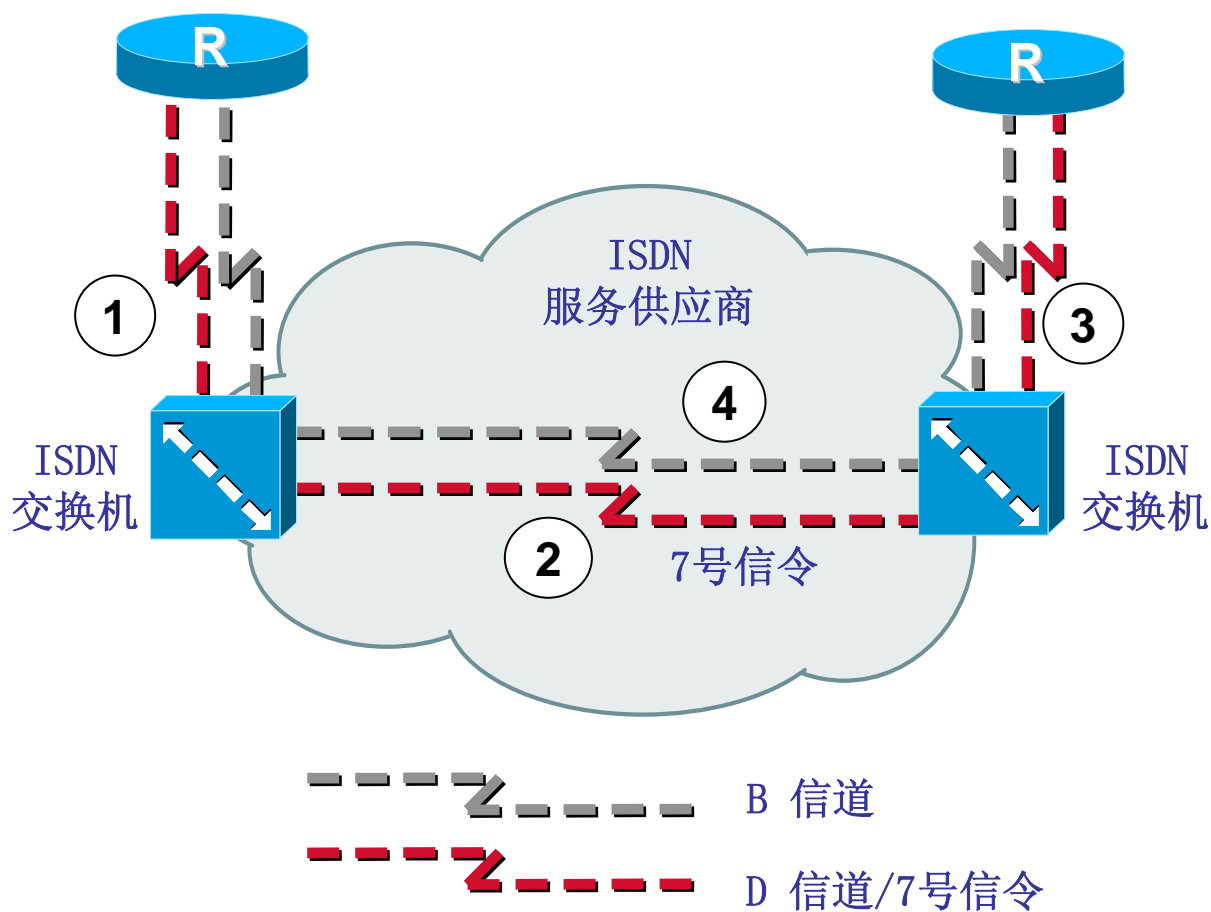
☆成本较低，是小型办公和家庭用户比较经济的解决方案

☆可以用做租用线路的备份连接

☆可以使用按需拨号 (dial-on-demand, DDR)

第三章 ISDN与DDR

ISDN的呼叫过程



第三章 ISDN与DDR

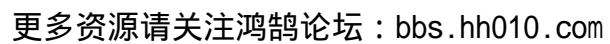
B通路：具有定时的64Kbit/s通路，用于传递广泛的各种用户数据，不传递ISDN电路交换的信令信息。

D通路：主要用于传递ISDN电路交换的信令信息，也可以传递控制信息和分组交换机数据。

基本B通路接口（BRI, Basic Rate Interface）：由2个B通路和1个D通路组成，即2B+D。在本结构中，D通路的传输速率为16Kbit/s。

基群速率B通路接口（PRI, Primary Rate Interface）：30B+D，此时D通路的传输速率为64Kbit/s；23B+D，此时D通路的传输速率为64Kbit/s。

在北美和日本，ISDN PRI提供23B+D，总速率可达1.544Mbps；在欧洲、澳大利亚等国家，ISDN PRI提供30B+D，总速率可达2.048Mbps。我国提供的ISDN PRI为30B+D。



第三章 ISDN与DDR

ISDN的网络分层模型表示一个**ISDN**终端或网络节点所包含的全部协议。模型由三个平面组成，分别对应着三种不同类型的信息。

控制平面C：是关于控制信令的协议，共分七层，它覆盖了所有对呼叫和网络性能的控制。

用户平面U：是关于用户信息的协议，也分七层，它覆盖了在用户信息传送的信道上实行数据交换的全部规则。

管理平面M：不分层，是关于终端或**ISDN**节点内部操作功能的规则。

一般来说，**C**平面和**U**平面可以通过原语和管理平面**M**进行通信，由**M**平面中的管理实体来协调**C**和**U**之间的动作，**C**和**U**之间不直接通信。

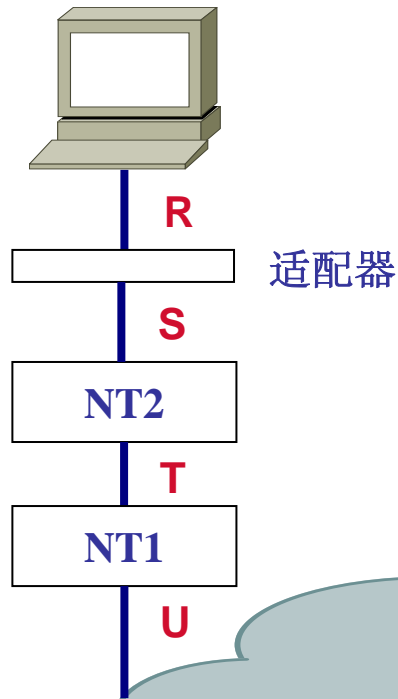
第三章 ISDN与DDR

当建立。求执。用传
例：建面请下接知数据
为络中平该互连通数
式网控制中交路体始
方在了节体的理开
换求到络实间管上，
交请送网制之过信道
路层转在控端通B信
电输而，层终再到B
以传调络高叫后送
的，面协网的被实数据
的行，平的到上主证数
进用实后平建接可
样的理释一络连即
这它管解同网路议
时，过求其使电协
信数据通请在，到的
通数求个层作得上
的输请这络动面平
点传个将网制平平
对始这层由控制户
点开，三，接控用
，要接低理连的时
中需连的处的端此
结构路面层列终，
该叫个制低一主平面
在主一控经行当户输。

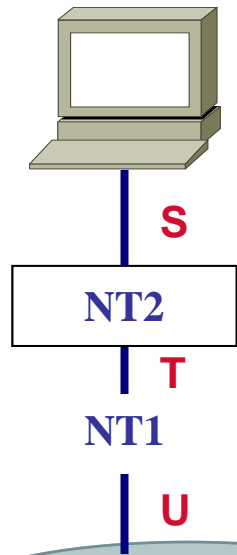
在同一用户——网络接口上，**B**信道和**D**信道传送不同的信息，根据他们各自传送的信息特征，可以认为：**B**信道的协议对应U平面的控制，而**D**信道则由C面上的协议来控制参照前述的分层结构。

第三章 ISDN与DDR

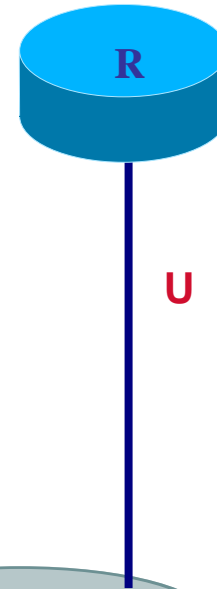
不带有ISDN标准接口的设备



带有ISDN标准接口的设备



具有NT1的路由器



ISDN 的功能点(Function Point) 和参考点(Reference Point)

功能点是硬件设备

参考点是接口或界线

第三章 ISDN与DDR

NT1 (Network Terminal 1) : 包含OSI第一层的功能, ISDN在用户处的物理和电器终端装置, 在NT1上要处理D信道竞争的问题

NT2 (Network Terminal 2) : 包含OSI一到三层的功能

TE1 (Terminal Equipment 1) : 是ISDN的标准终端

TE2 (Terminal Equipment 2) : 是非ISDN标准的终端, 例如模拟话机

TA (Terminal Adapter) : 使TE2接入ISDN的标准接口, 完成将TE2接入ISDN的速率和协议等方面的适配功能

第三章 ISDN与DDR

T参考点：用户与网络的分界点，NT1与NT2之间，是用户和网络之间的分界点（NT1属于网管部门，NT2属于用户）

S参考点TE1和NT2之间，对应于单个ISDN终端设备接入网络的接口，将用户终端和与网络有关的功能分开

U参考点：对应于用户线，用来描述用户线上的双向数据信号

R参考点：位于TE2和TA之间，用于提供非标准ISDN标准终端的入网接口

第三章 ISDN与DDR

网络终端 (NT)

一类网络终端 (NT1)

智能网络终端 (NT2)

ISDN用户终端

ISDN适配卡

ISDN适配器

ISDN数字电话

ISDN可视电话



NT1



ISDN适配卡



TA128适配器



ISDN 数字话机

第三章 ISDN与DDR

定义ISDN交换机类型

Router(config)# isdn switch-type //国内一般为basic-net3

Router(config-if)# isdn switch-type

设置服务供应商的标识（SPID，由服务供应商提供的一系列的数字，用来识别到ISDN交换机的连接）

Router(config-if)#isdn spid1 <spid-number> [ldn]

Router(config-if)#isdn spid2 <spid-number> [ldn]

设置协议地址与电话号码的映射

**Router(config-if)#dialer map protocol next-hop-address [name
hostname] [broadcast] [dial-string]**

启动PPP多连接

Router(config-if)#ppp multilink

第三章 ISDN与DDR

设置启动另一个B通道的阈值

Router(config-if)#dialer load-threshold load

显示ISDN有关信息

Router#show isdn {active | history | memory | services | status [dsl | interface-type number] | timers}

设置接口支持PPP回拨

Router(config-if)#ppp callback accept

在全局模式下为PPP回拨设置映射类别

Router(config)#map-class dialer classname

通过查找注册在dialer map里的主机名来决定回拨

Router(config-if)#dialer callback-server [username]

设置接口要求PPP回拨

Router(config-if)#ppp callback request

第三章 ISDN与DDR

相关调试命令

debug dialer

debug isdn event

debug isdn q921

debug isdn q931

debug ppp authentication

debug ppp error

debug ppp negotiation

debug ppp packet

show dialer

show isdn status

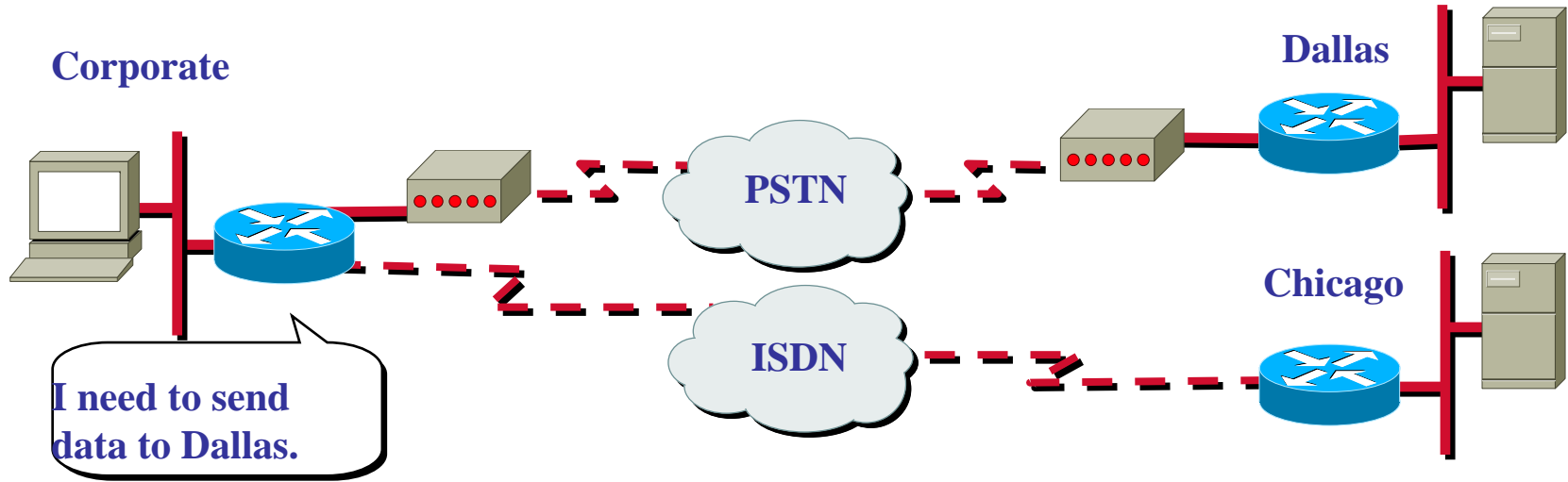
第三章 ISDN与DDR

DDR (Dial on Demand Routing) 即按需拨号路由，是利用拨号链路实现网络互连的一种常用技术。DDR适用于用户对速率要求不高，偶尔有数据传输或只是在特定时候传输数据等等情况。

DDR主要实现4个功能：

- ☆将数据包从被拨号的接口进行路由；
- ☆决定何种数据包可以触发拨号，即确定“感兴趣”包
- ☆触发拨号
- ☆决定什么时候终止连接

第三章 ISDN与DDR



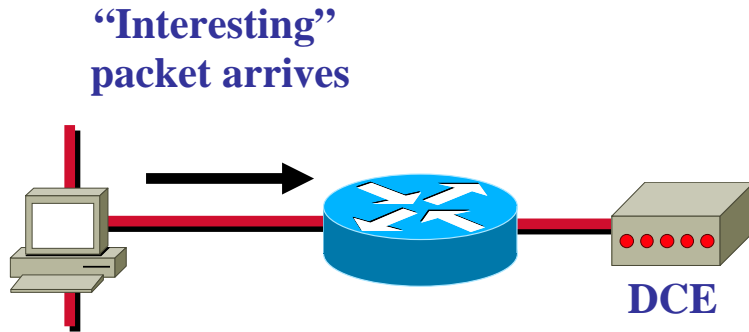
按需拨号

完成后即可挂断连接

一般使用在PSTN或ISDN

多用于小流量数据传输，周期性的网络访问

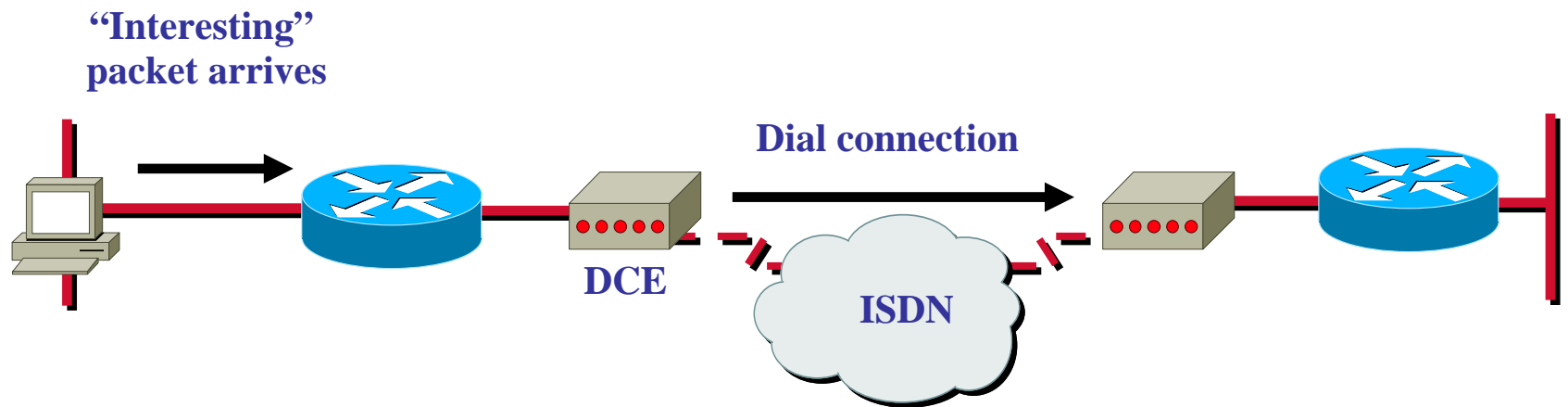
第三章 ISDN与DDR



- 1、查寻默认路由
- 2、敏感数量触发拨号
- 3、定义拨号相关信息
- 4、数据传输
- 5、终止传输

当一个感兴趣的包到达路由器时，产生一个DDR请求。路由器发送呼叫建立信息给指定的接口设备，这个呼叫就把本地和远程的设备连接起来。一旦没有数据传输，空闲时间开始计时，超过设置的空闲时间，终止连接。

第三章 ISDN与DDR



第三章 ISDN与DDR

定义静态路由

Router(config)#ip route [dest-network] [mask] [next-hop address或exit interface]

指明启动拨号的流量

使用**dialer-list**

Router(config)# dialer-list <dailer-list> protocol <protocol> permit

使用**access-list**

Router(config)# dialer-list <dailer-list> protocol <protocol> list <access-list>

第三章 ISDN与DDR

设置拨号信息

Router(config-if)# Dialer map <protocol> <next-hop-addr> [name <hostname>] [speed 56|64] [broadcast] dial-string

Name 是远端设备的名称

Broadcast 保证路由更新信息能在线路上传送

在接口启动**DDR**

Router(config-if)# dialer-group <dialer-list #>

负载平衡

Router(config-if)#dialer load-threshold <load> [outbound | inbound | either]

设置链路断开前链路空闲的时间

Router(config-if)#dialer idle-timeout <seconds>

缺省的空闲时间为 120 秒

第三章 ISDN与DDR

Router#show dialer

Router#show isdn active

Router#show isdn status

第四章 Frame Relay

帧中继（**Frame Relay**）使用包交换的方式，工作在OSI模型的物理层和数据链路层，由CCITT（国际电报电话咨询委员会）和ANSI（美国国家标准协会）共同制定，是一种典型的包交换技术。

帧中继可以看作是X.25协议的简化版本，它省略了X.25协议的一些功能，例如窗口技术和重传技术。这主要是因为目前帧中继技术所使用的广域网环境比起过去使用X.25协议时，无论在服务的稳定性还是质的量方面都有了很大的提高和改进。此外，帧中继是一种严格意义上的第二层协议，可以把一些复杂的控制和管理功能交由上层协议完成，这就大大提高了帧中继的性能和传输速度，使其更加适合广域网环境下的各种应用。

通信的数字化提高了网路的可靠性和终端设备的智能化程度，使数据传输的差错率降低到可以忽略不计的地步。帧中继正是利用现代通信网的这一优点，以帧为单位在网络上传输，中间结点只转发帧而不回送确认帧，只是在目的结点收到后才回送端到端的确认。并且帧中继将流量控制、纠错等功能全部交由智能终端设备处理，从而加快了网络的传输速率。

第四章 Frame Relay

帧中继是一种面向连接的协议。

帧中继认为帧的传输基本上不会出错，因此只要知道帧的目的地址，就立即开始转发，而无需等待接收完整帧并检测这个帧是否正确。如果帧在传输过程中出现差错，帧中继将丢弃该帧，并请求源节点重发。帧中继在传输过程中，一旦发现差错，立即停止转发，并将该帧丢弃，并请求源节点重发。帧中继在传输过程中，一旦发现差错，立即停止转发，并将该帧丢弃，并请求源节点重发。帧中继在传输过程中，一旦发现差错，立即停止转发，并将该帧丢弃，并请求源节点重发。

帧中继只定义了用户前置设备（CPE，也称为数据终端设备DTE），和服务提供商的本地交换设备（也称为数据通信设备DCE）之间的接口规范，而并没有定义在帧中继的云中数据是如何传输的。

帧中继提供一种统计多路服务，通过为每一对通信的DTE间安排一对标识，同一物理连接上可以存在许多个逻辑连接（虚电路）。服务提供商的交换设备构造一个表，保存这些标识和连接标识，然后将帧通过相应的端口转发出去。已经建立到达目的网络设备完整路径的帧被优先转发。

第四章 Frame Relay

帧中继和分组交换类似，但却以比分组容量大的帧为单位而不是以分组为单位进行数据传输；而且，它在网络上的中间节点对数据不进行误码纠错。

帧中继技术在保持了分组交换技术的灵活及较低的费用同时，缩短了传输时延，提高了传输速率。因此，它成为了当今实现局域网（LAN）互连、局域网与广域网（WAN）连接及宽带接入等应用的理想解决方案。

和其他的通讯协议相比，它具有较高的性价比，通讯带宽可达到64k到2M，具有动态带宽和拥塞机制。

特点：

- ☆按需分配带宽，网络资源利用率高，网络费用低廉；
- ☆采用虚电路技术，适用于突发性业务的使用；
- ☆不采用存储转发技术，时延小、传输速率高、数据吞吐量大；
- ☆兼容X.25、SNA、DECNET、TCP/IP等多种网络协议，可为各种网络提供快速、稳定的连接；

第四章 Frame Relay

帧中继提供的功能及其应用范围

局域网间互连：帧中继可应用于银行、证券等金融及大型企业、政府部门的总部与各地分支机构的局域网之间的互连。

局域网与广域网的连接：帧中继构成的高速局域网与广域网的连接，可以提高租用线路的带宽利用率。

虚拟专用网：帧中继只使用了通信网络的物理层和链路层的一部分来执行其交换功能，网络利用率很高，利用它构成的虚拟专用网，不但具有高速率和高吞吐量，其费用也相当低。

电子文件传输：由于帧中继使用的是虚电路，信号通路及带宽可以动态分配，特别适用于突发性的使用，因而它在远程医疗、金融机构及CAD/CAM（计算机辅助设计/计算机辅助生产）的文件传输、计算机图像、图表查询等业务方面有着特别好的适用性。

第四章 Frame Relay

帧中继虚拟电路

帧中继提供的是一种面向连接的数据链路层通信，任何两台设备之间都存在一条预先定义的通信通道，由连接标识符进行识别。帧中继通过使用虚拟电路实现上述功能。所谓虚拟电路，就是指跨越帧中继交换网络，在两台数据终端设备之间创建的逻辑连接。

虚拟电路可以提供DTE设备之间的双向通信，使用唯一的数据链路层连接标识（**DLCI**）识别虚拟连接。一条物理电路可以被复用为多条虚拟电路，从而降低了网络和设备的复杂程度。

帧中继虚拟电路包括交换性虚拟电路（**SVC**）和永久性虚拟电路（**PVC**）两种。

第四章 Frame Relay

交换式虚电路（SVC）

交换式虚电路是一种临时性的连接，主要适用于数据传输量较少的DTE设备之间的网络连接。通过SVC建立的通信会话包括以下4种运行状态：

呼叫建立：在两台帧中继DTE设备之间创建虚拟电路。

数据传输：通过虚电路在两台DTE设备之间传输数据。

空闲状态：DTE设备之间的连接仍然存在，但是没有数据进行传输。当SVC处于空闲状态超过预定时间之后，当前呼叫将被自动终止。

呼叫终止：终止两台DTE设备之间的虚拟电路。

当虚拟电路被终止后，如果DTE设备之间还需要进行数据交换的话，必须重新创建一条新的SVC。由于很少有厂商提供支持SVC的DCE设备，所以交换性虚拟电路在今天的帧中继网络中的实际应用很少。

第四章 Frame Relay

永久虚电路（PVC）

永久虚电路创建的是一种永久的连接，主要用于经常需要进行持续的数据传输的**DTE**设备之间的网络连接。与**SVC**相比，通过**PVC**进行的通信不包含呼叫建立和终止状态。**PVC**总是在以下两种状态下运行：

数据传输：通过虚拟电路在**DTE**设备之间传输数据。

空闲状态：**DTE**设备之间的连接仍然存在，但是没有数据进行传输。不同于**SVC**，**PVC**不会因为处于空闲状态而自动被终止。

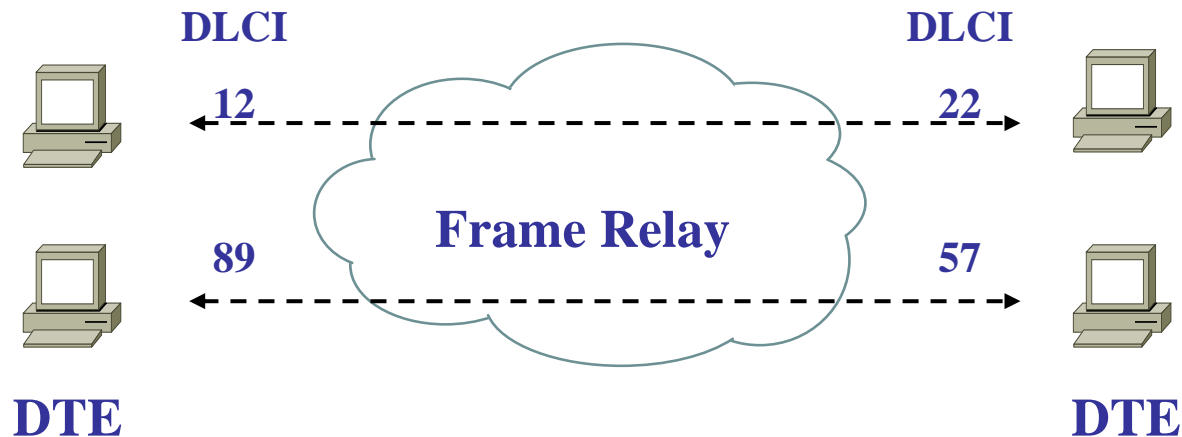
因为**PVC**创建的是永久性的连接，所以**DTE**设备可以在任何需要进行通信的时候传输数据。

第四章 Frame Relay

数据链路层连接标识（DLCI）

帧中继使用数据链路层连接标识（**Data Link Connection Identifier**）来标识网络所设置的永久虚电路，该标识通常由帧中继服务商提供。在帧中继帧的地址字段中，有一个长10比特的数字用于标识路由器和帧中继交换机之间的逻辑虚电路。**DLCI**只在本地有意义，它指的是本地路由器及其连接的帧中继交换机之间的连接。

帧中继提供了一种多路复用的手段，它通过为每对数据终端设备分配不同的**DLCI**来实现物理传输介质的复用，从而在同一条物理线路上建立多条永久虚电路。



第四章 Frame Relay

拥塞控制机制

在网络控制方面，为了降低系统开销，帧中继采用了简单的拥塞通知机制，而没有使用显式的基于每一条虚拟电路的控制机制。这主要是因为帧中继通常运行在比较稳定的网络介质之上，所以完全可以将流量控制功能交由上层协议完成，而不会影响到数据的完整性。帧中继所采用的拥塞通知机制由以下两部分组成：前向拥塞标识（FECN）和后向拥塞标识（BECN）。

FECN和**BECN**都是由位于帧中继帧头部的比特位控制。除了**FECN**和**BECN**位之外，还提供了一个可丢弃指示位（**DE**），用来标识当出现网络拥塞时可以丢弃的非重要数据。

可丢弃指示比特位（**DE**, Discard Eligibility）

DTE设备通过将帧中继帧中的**DE**位设置为1，标识非重要数据帧。当网络变得拥挤时，**DCE**就会首先丢弃那些已经设置了**DE**位的帧以释放出更多的网络资源。当网络状况下降时，这一机制可以有效的确保关键数据仍然能够稳定，可靠的传输。**DE**的长度为1。

第四章 Frame Relay

前向显式拥塞通知（**Forward Explicit Congestion Notification**）：是帧中继帧头中地址字段的一个比特。发生拥塞时，将帧的**FECN**位设为**1**，当这个帧传输到目标设备时，**FECN**位通知该设备在网络传输时，从源地址到目标地址的传输线路上产生了拥塞。

当**DTE**设备向帧中继网络发送数据时，如果网络出现拥塞，**DCE**设备（例如交换机等）将会自动把帧的**FECN**位设定为**1**。当数据帧到达目标接收**DTE**设备时，通过分析地址域（包含已经设置为**1**的**FECN**位）就可以知道该帧是否在传输过程中经历网络拥塞。位于接收方的**DTE**设备会把收到的信息传递给高层协议进一步处理。

第四章 Frame Relay

后向显式拥塞通知（**Backward Explicit Congestion Notification**）：是帧中继帧头中地址字段中的一个比特。发生拥塞时，将帧的**BECN**位设为**1**，当这个帧传输到源设备时，**BECN**位通知该设备在网络传输时，帧在从源地址到目标地址的传输线路的相反方向上产生了拥塞。

当设置过**FECN**位的帧中继的帧反向传输时，**DCE**设备会根据网络情况对**BECN**位进行设置以通知接收方，该数据帧在反向传输过程中是否遇到网络拥塞。

第四章 Frame Relay

错误校验

帧中继采用了循环冗余码校验（**CRC**）作为错误校验机制。**CRC**通过对比两个计算值可以确定在信息传递过程中是否出现错误。为了降低网络开销，帧中继只采用了错误校验机制，而没有提供任何的错误修复功能。这主要是因为帧中继的网络运行环境较好，所以可以在不损害数据完整性的前提下，把错误修复功能交由上层协议完成。

第四章 Frame Relay

帧中继本地管理接口（**LMI, Local Management Interface**）

LMI：在CPE和帧中继交换机间的信号标准，它负责管理设备间的连接和维护它们之间的状态，提供了用于管理复杂网络的多项扩展，如全局定位、简单的流量控制、虚拟电路状态消息以及多点传送等。

LMI是对基本的帧中继标准的扩展集，是路由器和第一个帧中继交换机之间的信令标准。**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（如路由器）的地址。**LMI**提供以下信息：

Keepalives：验证数据是否有进行传输

组播：可选的**LMI**扩展，使用保留**DLCI**编号从1019到1022，可以建立不同的多点传送组，根据具体的路由器组传送相应的路由更新和地址解析信息，从而有效的节省了占用带宽。

全局寻址：**LMI**全局定址扩展功能可以使**DLCI**在整个帧中继广域网有效，成为每一台DTE设备的唯一网络地址。全局定位扩展增强了帧中继网络的管理功能，任何一个单独的网络接口或末端节点都可以使用标准的地址解析技术进行识别。

第四章 Frame Relay

虚电路状态：可以在帧中继DTE和DCE设备之间实现通信和同步。上述消息被用来定期通报PVC的链路状态，以避免数据被发入黑洞（已经不存在的PVC）。

虚电路的三种状态

活跃（active）：正常，可以交换信息

非活跃（inactive）状态：路由器的接口为up状态，而且可以和帧中继交换机进行通信，但是远端路由器没有工作

删除（deleted）状态：没有LMI信息在路由器和帧中继交换机之间交换，可能是线路问题或者映射（mapping）的问题

LMI可以手工配置。在IOS 11.2版本以后，路由器可以通过向帧中继交换机发送状态查询信息自动获取有关的LMI类型信息。Cisco路由器支持三种LMI类型：**cisco、ansi和q933a。**

Cisco的设备默认LMI类型是Cisco。从IOS版本11.2开始，LMI类型可以自动检测了。

第四章 Frame Relay

本地接入速率：数据进入或离开网络的最大速率。

承诺信息速率：**CIR**（**Committed Information Rate**），传输数据是最大平均速率。

反向地址解析协议：**Inverse ARP**，动态地将远程网络层地址与本地**DLCI**关联起来。

承诺突发量（**Committed Burst**）：在正常情况下，在测量时间间隔**T**内，网络允许传送的数据的最大限制。

附加突发量（**Excess Burst**）：在正常情况下，在测量时间间隔**T**内，在承诺突发量的基础上，网络试图再额外传送的数据的最大限制。

认购超额（**Oversubscribe**）：当通过该结点的所有连接的**CIR**超过这个结点的容量时，称为**oversubscribe**。此时的帧会被抛弃。

第四章 Frame Relay

帧中继帧结构

Flags 8bytes	Address 16bytes	Data (Variable)	FCS 16bytes	Flags 8bytes
-------------------------------	----------------------------------	----------------------------------	------------------------------	-------------------------------

第四章 Frame Relay

帧中继帧结构

标志字段（Flags）：标志一帧的开始和结束。该字段值固定不变，使用**01111110**表示。

地址字段（Address）：地址字段包含多种信息，较为重要的有：

DLCI：长度为**10**个比特，是帧中继帧的关键部分。**DLCI**的值代表了**DTE**设备和交换机之间的虚拟连接电路。每一条复用到物理链路的虚拟连接都使用一个唯一的**DLCI**识别。**DLCI**值只是本地有效。

拥塞控制：拥塞控制由**FECN**，**BECN**和**DE** 3个比特位组成，主要用于控制帧中继拥塞通知机制。

数据字段（Data）：包含被封装的用户数据或负载。该字段长度不固定，最大可以达到**16000**个字节。数据字段的作用主要是通过帧中继网络传递上层协议数据包，例如**PDU**等。

帧校验序列字段（FCS）：**FCS**字段可以确保传输数据的完整性。该字段值由发送设备计算，在抵达接收设备之后进行验证，以确定数据是否完整。

第四章 Frame Relay

帧中继建立：路由器接口初始化时，与交换机通信，初始化链路，并尝试通过**IARP**映射远程**IP**地址。

- 1、路由器通过**CSU/DSU**连接到帧中继交换机。
- 2、接口上配置帧中继后，路由器向帧中继交换机发送状态查询信息。该信息将路由器的状态告诉给交换机，并询问交换机和要和此路由器进行通讯的远端路由器的状态。。
- 3、交换机收到请求后，用状态消息进行响应，包括**PVC**的**DLCI**，即本地路由器通过这些**PVC**可以将数据发送给远程路由器。
- 4、对于每个活动的**DLCI**，路由器都发送一个**IARP**分组，其中包括自己的**IP**，并询问对方的网络层地址。

第四章 Frame Relay

5、这时两个路由器都会接收到**IARP**响应数据包，路由器将在各自的帧中继映射表中加入一个表项，其中包括有本端的**DLCI**和远端路由器网络层地址的一个映射关系。帧中继映射表可能出现以下三种状态：

活动状态：连接是激活的，有数据交换发生；

停止状态：本地路由器到帧中继交换机的连接工作，而远端路由器到帧中继交换机的连接没有工作；

删除状态：本地路由器收不到来自帧中继交换机的信号，或者用户和帧中继交换机没有建立服务关系。

如果**IARP**失败或者远程路由器不支持**IARP**，由必须配置静态映射。

6、每隔**60S**，路由器在所有活动**DLCI**上发送一条**IARP**。

7、每隔**10S**，用户端的路由器会向帧中继交换机发送一个**keepalive**信息，以确认帧中继交换机是否处于活动的状态。

第四章 Frame Relay

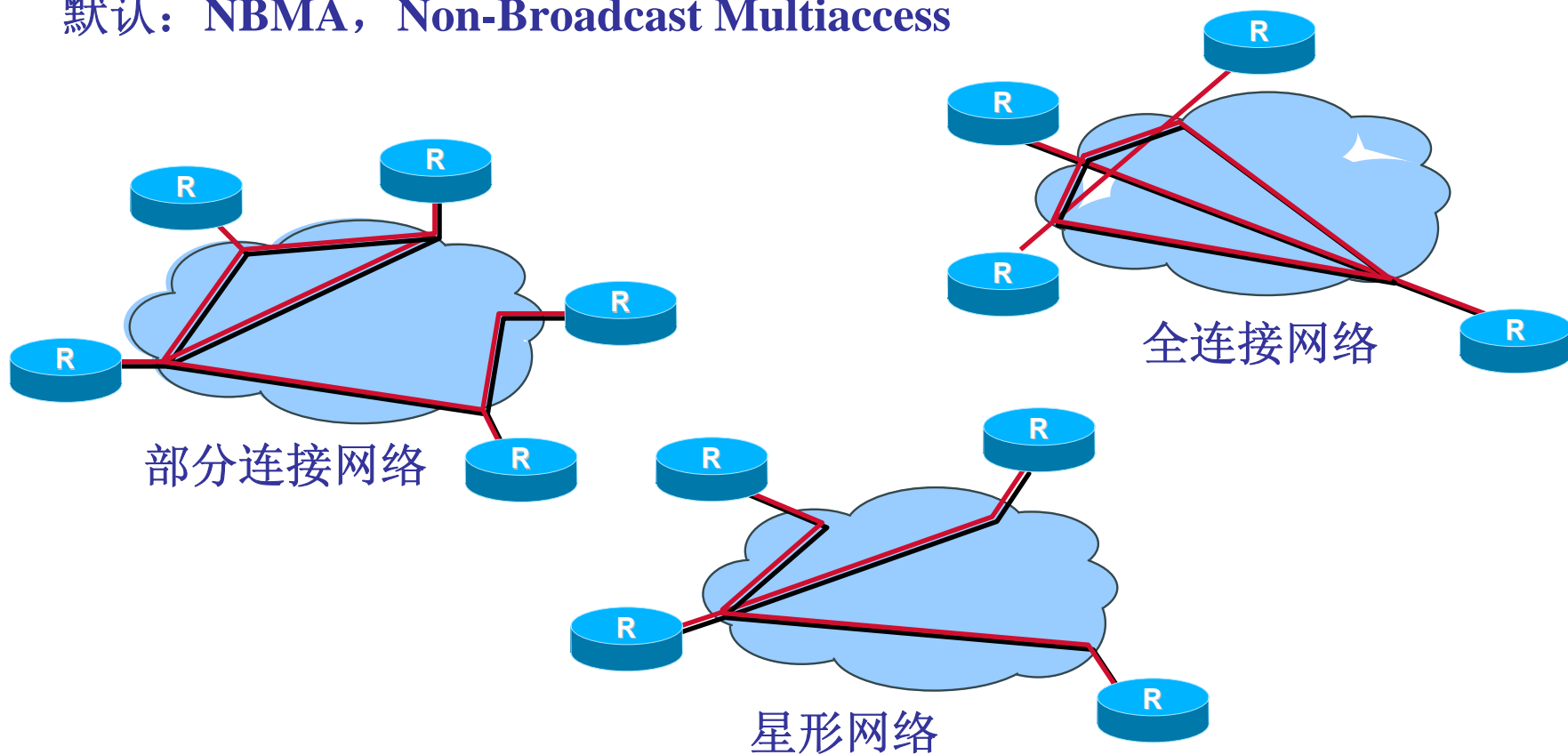
帧进入帧中继交换机后，交换机执行下述操作：

- 1、查看帧的入站**DLCI**号。
- 2、根据映射表确定应将帧发送到哪个出站**DLCI**。
- 3、交换机将帧和两个**DLCI**值转发到合适的端口。

第四章 Frame Relay

帧中继的网络拓扑结构

默认：NBMA，Non-Broadcast Multiaccess



第四章 Frame Relay

帧中继配置步骤

配置帧中继协议封装格式

配置IP地址

配置本地虚电路的DLCI号

配置动态或静态地址映射

配置本地管理端口LMI。如果IOS的版本是11.1或者更早，需要指定LMI的类型，如IOS是11.2以后的版本，不需要该步骤，因为LMI的类型可自动检测。

第四章 Frame Relay

帧中继的配置命令

封装帧中继协议

encapsulation frame-relay [cisco|ietf]

Cisco路由器的默认格式为**cisco**，在**Cisco**路由器与其它厂家路由设备相连时，应使用**ietf**格式。

设置虚电路的**DLCI**号

frame-relay interface-dlci dlci-number [broadcast]

dlci-number为**DLCI**号，其取值范围为**16~1007**

映射协议地址与**DLCI**号

frame-relay map protocol-type protocol-address dlci [broadcast]

protocol-type指协议地址的类型，包括**IP**，**IPX**等；

protocol-address代表具体的协议地址；

broadcast选项允许在帧中继网络上传输路由广播信息。

第四章 Frame Relay

设置LMI类型

frame-relay lmi-type {ansi | cisco | q933a}

LMI定义了帧中继的接口信念标准，用于管理和维护两个通信设备间的运行状态。

显示帧中继相关信息命令

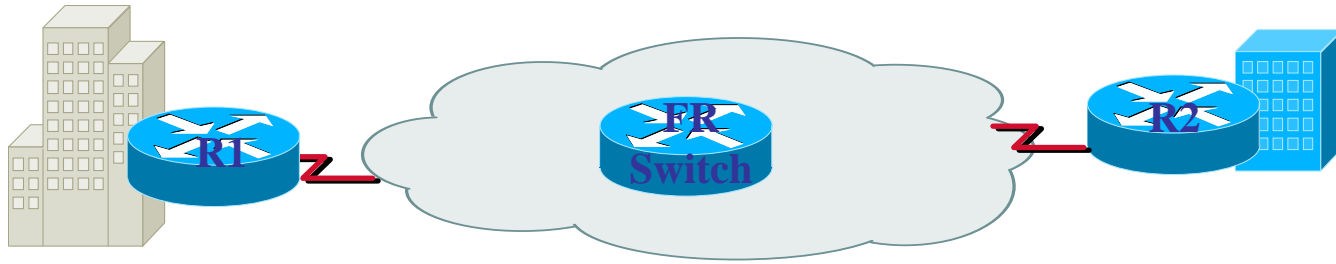
show frame-relay lmi

show frame-relay map

show frame-relay pvc

show frame-relay route

第四章 Frame Relay



```
R1(config)#interface serial 0
```

```
R1(config-if)#ip address 10.0.0.1 255.0.0.0
```

```
R1(config-if)#encapsulation frame-relay
```

```
R1(config-if)#frame-relay map ip 10.0.0.2 102 cisco
```

```
R2(config)#interface serial 0
```

```
R2(config-if)#ip address 10.0.0.2 255.0.0.0
```

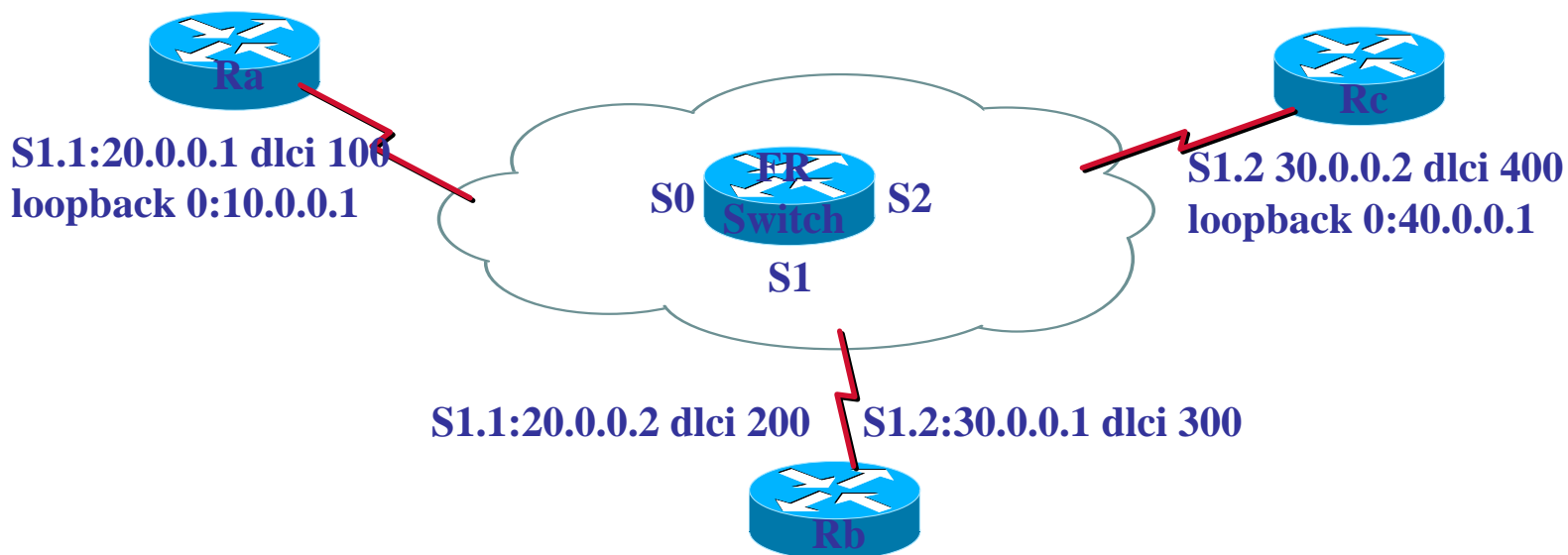
```
R2(config-if)#encapsulation frame-relay
```

```
R2(config-if)#frame-relay map ip 10.0.0.1 201 cisco
```

第四章 Frame Relay

```
FR(config)#frame-relay switching           //启动路由器的帧中继交换功能
FR(config)#interface serial 0
FR(config-if)#no ip address
FR(config-if)#encapsulation frame-relay
FR(config-if)#clockrate 64000
FR(config-if)#frame-relay lmi-type cisco
FR(config-if)#frame-relay intf-type dce
FR(config-if)#frame-relay route 102 interface serial 1 201
FR(config-if)#interface serial 1
FR(config-if)#no ip address
FR(config-if)#encapsulation frame-relay
FR(config-if)#clockrate 64000
FR(config-if)#frame-relay lmi-type cisco
FR(config-if)#frame-relay intf-type dce
FR(config-if)#frame-relay route 201 interface serial 0 102
```

第四章 Frame Relay



第四章 Frame Relay

```
Ra(config)#interface loopback0
Ra(config-if)#ip address 10.0.0.1 255.0.0.0
Ra(config-if)#interface serial 1
Ra(config-if)#encapsulation frame-relay
Ra(config-if)#interface serial 1.1 point-to-point
Ra(config-if)#ip address 20.0.0.1 255.0.0.0
Ra(config-if)#frame-relay interface-dlci 100
Ra(config)#router rip
Ra(config-router)#network 10.0.0.0
Ra(config-router)#network 20.0.0.0
Ra(config-router)#neighbor 20.0.0.2
```

第四章 Frame Relay

```
Rb(config-if)#interface serial 1
Rb(config-if)#encapsulation frame-relay
Rb(config-if)#interface serial 1.1 point-to-point
Rb(config-if)# ip address 20.0.0.2 255.0.0.0
Rb(config-if)# frame-relay interface-dlci 200
Rb(config-if)#interface serial 1.2
Rb(config-if)#ip address 30.0.0.1 255.0.0.0
Rb(config-if)#frame-relay interface-dlci 300
Rb(config)#router rip
Rb(config-router)#network 20.0.0.0
Rb(config-router)#network 30.0.0.0
Rb(config-router)#neighbor 20.0.0.1
Rb(config-router)#neighbor 30.0.0.2
```

第四章 Frame Relay

```
Rc(config)#interface loopback0
Rc(config-if)#ip address 40.0.0.1 255.0.0.0
Rc(config-if)#interface serial 1
Rc(config-if)#encapsulation frame-relay
Rc(config-if)#interface serial 1.1 point-to-point
Rc(config-if)# ip address 30.0.0.2 255.0.0.0
Rc(config-if)# frame-relay interface-dlci 400
Rc(config)#router rip
Rc(config-router)#network 30.0.0.0
Rc(config-router)#network 40.0.0.0
Rc(config-router)#neighbor 30.0.0.1
```

第四章 Frame Relay

```
fr(config)#frame-relay switching
fr(config)#interface Serial 0
fr(config-if)#no ip address
fr(config-if)#encapsulation frame-relay
fr(config-if)#clockrate 64000
fr(config-if)#frame-relay lmi-type cisco
fr(config-if)#frame-relay intf-type dce
fr(config-if)#frame-relay route 100 interface Serial 1 200
fr(config-if)#interface Serial 1
fr(config-if)#no ip address
fr(config-if)#encapsulation frame-relay
fr(config-if)#clockrate 64000
fr(config-if)#frame-relay lmi-type cisco
fr(config-if)#frame-relay intf-type dce
fr(config-if)#frame-relay route 200 interface Serial 0 100
fr(config-if)#frame-relay route 300 interface Serial 2 400
```

```
fr(config-if)#interface Serial 2
fr(config-if)#no ip address
fr(config-if)#encapsulation frame-relay
fr(config-if)#clockrate 64000
fr(config-if)#frame-relay lmi-type cisco
fr(config-if)#frame-relay intf-type dce
fr(config-if)#frame-relay route 400 interface
Serial 1 300
```

第五章 NAT

NAT (Network Address Translation, 网络地址翻译)，是由**IETF**定义的一种把内部私有地址翻译成合法公有地址的技术，允许一个机构中**Intranet**的主机透明连接到公共区域中，无需内部主机拥有注册的**Internet**地址。

简单的说，**NAT**是在局域网内部使用内部地址，而当内部节点要与外部网络进行通讯时，在网关处将内部地址替换成公用地址，从而在外部公网正常使用。

NAT使多台计算机共享**Internet**连接。通过**NAT**，可以只申请一个合法**IP**地址，就把整个局域网中的计算机接入**Internet**中。这时，**NAT**屏蔽了内部网络，所有内部网计算机对于公共网络来说是不可见的，而内部网络的用户也不会意识到**NAT**的存在。

第五章 NAT

NAT功能通常被集成到路由器、防火墙、**ADSL**路由器或者单独的**NAT**设备中。

NAT有三种类型：静态（**Static**）**NAT**、动态地址（**Pooled**）**NAT**、网络地址端口转换**NAPT**（**Port Level NAT**）。

静态**NAT**是最简单和最容易的一种，内部网络中的主机被永久映射成外部网络中的某个合法的地址。

动态地址**NAT**为内部地址分配一个临时的外部地址，采用动态分配的方法映射到内部网络。当远程用户连接上之后，动态地址**NAT**就会分配给他一个**IP**地址，用户断开时，这个**IP**地址就会被释放而留待以后使用。

网络地址端口转换**NAPT**（**Network Address Port Translation**）则是把内部地址映射到外部网络的一个**IP**地址的不同端口上。**NAPT**普遍应用于接入设备中，它可以将中小型网络隐藏在一个合法的**IP**地址后面。与动态地址**NAT**不同，它将内部连接映射到外部网络中的一个单独的**IP**地址上，同时在该地址上加上一个由**NAT**设备选定的**TCP**端口号。

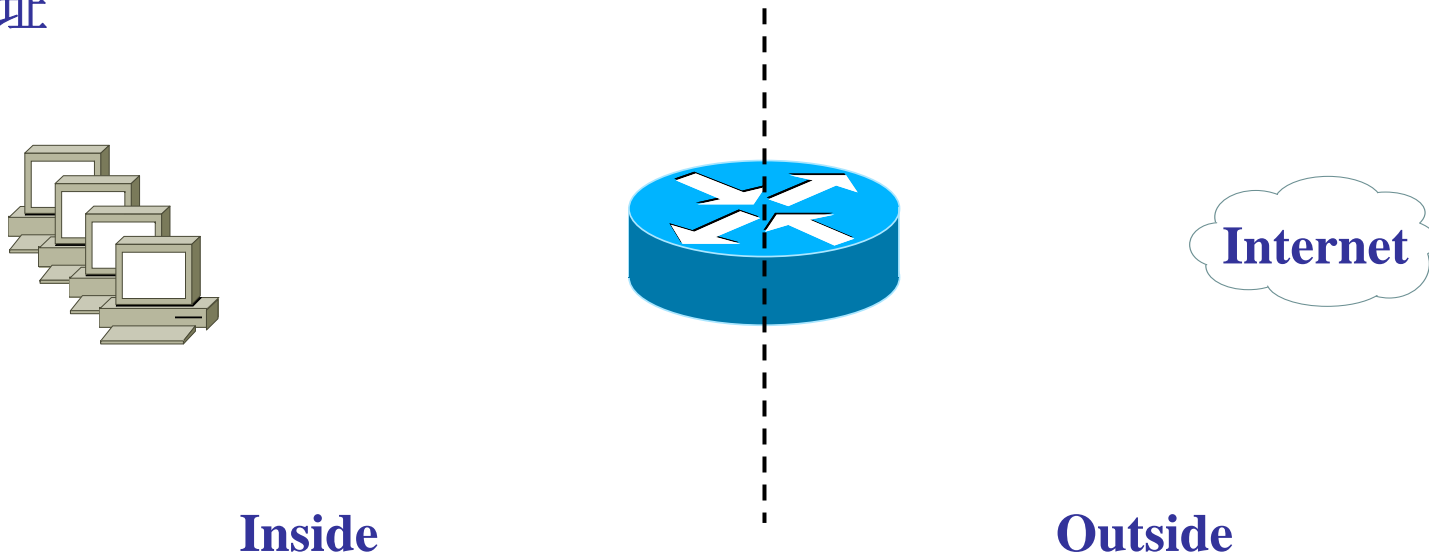
第五章 NAT

内部本地地址（**Inside Local Address**）：内部网络主机使用的**IP**地址

内部全局地址（**Inside Global Address**）：内部网络使用的公有**IP**地址

外部本地地址（**Outside Local Address**）：外部网络主机使用的**IP**地址

外部全局地址（**Outside Global Address**）：外部网络主机使用的**IP**地址



第五章 NAT

配置接口的类型

Router(config-if)#ip nat { inside | outside }

配置内部全局地址池

Router(config)#ip nat pool pool-name start-ip end-ip { netmask netmask | prefix-length prefix-length }

pool-name: 地址池的名称

start-ip和end-ip: 地址池的起始地址和结束地址

netmask: 掩码

prefix-length: 网络占用的二进制位数

第五章 NAT

配置内部源地址转换

Router(config)#ip nat inside source { list access-list-number pool name [overload] | static local-ip global-ip }

access-list-number: 访问列表编号

overload: 允许将多个内部本地地址转换为一个的内部全局地址;

static: 静态地址转换

local-ip: 内部本地地址

global-ip: 内部全局地址。

配置使用单一内部全局地址的内部源地址转换

Router(config)#ip nat inside source list access-list-number interface interface-type [overload]

第五章 NAT

配置NAT超时时间

Router(config)#ip nat translation timeout seconds

其他命令

查看生效的NAT设置

Router(config)#show ip nat translations

查看NAT统计信息

Router(config)# show ip nat statistics

清除所有动态NAT配置

Router(config)# clear ip nat translation *

清除单个动态NAT配置
<global-ip>

Router(config)# clear ip nat translation

第五章 NAT

静态NAT：将内部主机IP一对一的翻译成外部地址。

在内部主机连接到外部网络时，当数据包到达NAT路由器时，路由器检查它的NAT表，因为是NAT是静态配置的，可以查询出来，然后路由器将数据包的内部本部IP（源地址）更换成内部全局地址，再转发出去。外部主机接收到数据包后，用内部全局地址来响应，NAT接受到外部回来的数据包，再根据NAT表把地址翻译成内部本部IP。



R2负责NAT转换，**R3**为外网节点，**R1**模拟为内网主机。

要求通过静态NAT实现192.168.0.2到20.0.0.2（外网）的访问。

第五章 NAT

R2(config)#interface serial 1

R2(config-if)#ip address 192.168.0.1 255.255.255.0

R2(config-if)#ip nat inside //指定路由器的内部接口

R2(config-if)#interface serial 0

R2(config-if)#ip address 20.0.0.1 255.0.0.0

R2(config-if)#ip nat outside //指定路由器的外部接口

R2(config-if)#exit

R2(config)#ip nat inside source static 192.168.0.2 20.0.0.3

//建立静态映射，其中内部本部地址是192.168.0.2、内部全局地址是20.0.0.3。

R2(config)#ip route 0.0.0.0 0.0.0.0 serial 0 //实现路由

第五章 NAT

R1 (config)#no ip routing //关闭路由功能

R1(config)#interface serial 0

R1(config-if)#ip address 192.168.0.2 255.255.255.0

R1(config-if)#ip default-gateway 192.168.0.1 //指定缺省网关

R3(config-if)#interface serial 1

R3(config-if)#ip address 20.0.0.2 255.0.0.0

第五章 NAT

测试:

R1#ping 20.0.0.2

R2#debug ip nat

R2#

02:15:51: NAT*: s=192.168.0.2->20.0.0.3, d=20.0.0.2 [509]

02:15:51: NAT*: s=20.0.0.2, d=20.0.0.3->192.168.0.2 [509]

...

R2把R1发送的源地址为192.168.0.2的IP包转换为源地址为20.0.0.3的IP包，其目的为20.0.0.2。

R3将收到源地址为20.0.0.3的请求，并回应。

R2把从R3传来的目标地址为20.0.0.3的IP包转换为目的地址为192.168.0.2的IP包。

第五章 NAT

R2#show ip nat statistics

Total active translations: 1 (1 static, 0 dynamic; 0 extended)

Outside interfaces:

Serial0

Inside interfaces:

Serial1

...

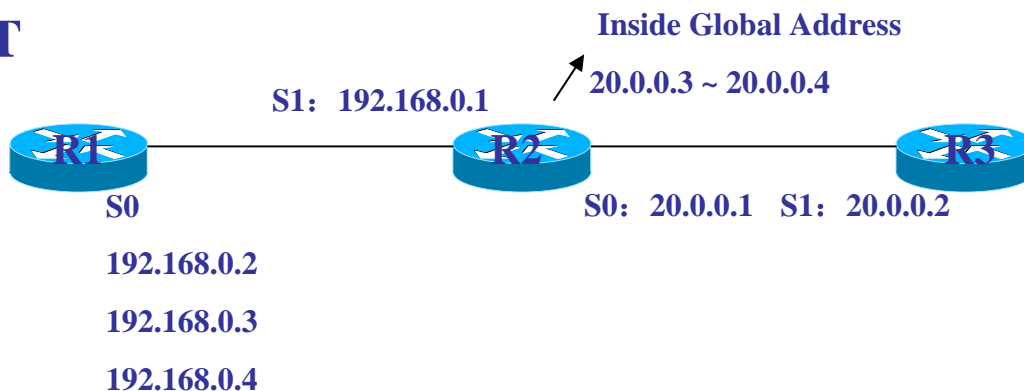
总的NAT活动转换数为1，其中静态转换数为1，其余类型的转换数为0。内部接口为S1，外部接口为S0。

R2#show ip nat translations

Pro	Inside global	Inside local	Outside local	Outside global
---	20.0.0.3	192.168.0.2	---	---

第五章 NAT

动态NAT



```
R2(config)# ip nat pool test 20.0.0.3 20.0.0.4 netmask 255.0.0.0
```

//定义一个名为test的NAT地址池

```
R2(config)#ip nat inside source list 1 pool test
```

//指定动态地址转换，由访问列表1定义的地址范围内的内网地址允许进行地址转换，转换后的地址是名为test的地址池中的IP地址，方式为动态转换

```
R2(config)#access-list 1 permit 192.168.0.0 0.0.0.255
```

//定义192.168.0.0/24网段，即内网网段

第五章 NAT

R1(config)#interface serial 0

R1(config-if)#ip address 192.168.0.2 255.255.255.0

R1(config-if)#ip address 192.168.0.3 255.255.255.0 secondary

R1(config-if)#ip address 192.168.0.4 255.255.255.0 secondary

R1(config-if)#exit

R1(config)#ip default-gateway 192.168.0.1

R1(config)#no ip routing

R3配置不变

第五章 NAT

R1#ping 20.0.0.2

R2#debug ip nat

R2#

00:28:00: NAT*: s=192.168.0.2->20.0.0.3, d=20.0.0.2 [25]

00:28:00: NAT*: s=20.0.0.2, d=20.0.0.3->192.168.0.2 [25]

...

R2#sh ip nat translation

Pro	Inside global	Inside local	Outside local	Outside global
---	20.0.0.3	192.168.0.2	---	---

第五章 NAT

继续在R1上使用扩展ping，用192.168.0.3作为源地址访问外网。

R2#sh ip nat translation

Pro	Inside global	Inside local	Outside local	Outside global
---	20.0.0.3	192.168.0.2	---	---
---	20.0.0.4	192.168.0.3	---	---

可以查看到又建立起一个NAT翻译。

继续在R1上使用扩展ping，用192.168.0.4作为源地址访问外网，将会观察到访问失败，同时在R2上通过debug将会观察到翻译失败。

原因：地址池内只有两个地址，被耗尽后，余下的内网主机将无法被翻译，不能访问外网。

第五章 NAT

R2#clear ip nat translation *

//动态建立的映射的生存周期缺省为24小时，清空动态映射后，查看NAT转换信息，发现列表是空的，没有任何映射存在，从R3向地址池中的任何地址发出的ping测试都是失败的，表明从外网到内网的方向上不能进行动态NAT转换。

R2#clear ip nat translation inside 20.0.0.3 192.168.0.2

在清除NAT翻译后，余下主机可以访问外网。

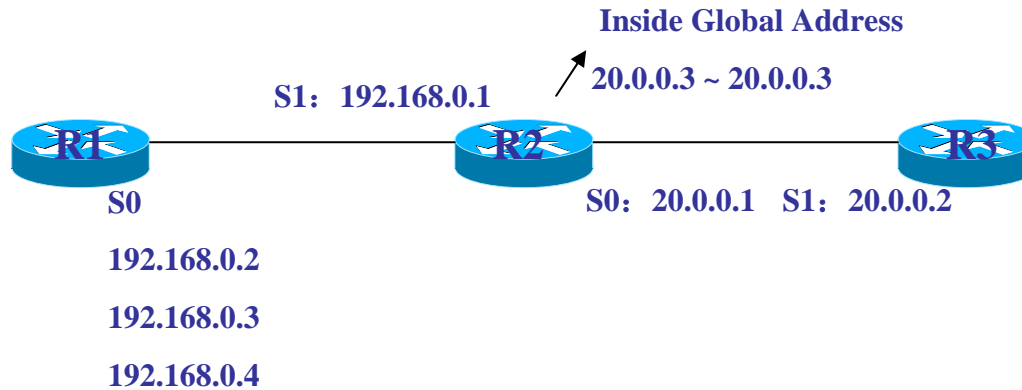
R2(config)#ip nat translation timeout 60

//设置NAT的超时时间，单位为秒

通过适当设置超时时间，可及时清除空闲连接，提供给有需要的内网主机。

第五章 NAT

NAPT



内部全局地址复用（overloading inside global addresses）

使用地址和端口，将多个内部地址映射到比较少的外部地址，也是所谓的**PAT（Port Address Translation）**。和内部地址翻译一样，路由器同样也负责查表和翻译内部**IP**地址，唯一的区别就是由于使用了复用，路由器将复用同样的内部全局**IP**地址。

第五章 NAT

R2(config)#ip nat pool test 20.0.0.3 20.0.0.3 netmask 255.0.0.0

//定义一个名为test的NAT地址池，开始和结束地址均为20.0.0.3

R2(config)#ip nat inside source list 1 pool test overload

//关键字overload，启用地址复用功能。由访问列表1定义的地址范围内的内网IP地址将被地址转换，转换后的地址是名为lab的NAT地址池中的IP地址，方式为动态转换

R2(config)#access-list 1 permit 192.168.0.0 0.0.0.255

R1与R3配置不变。

第五章 NAT

R1#ping

Protocol [ip]:

Target IP address: 20.0.0.2

Extended commands [n]: y

Source address or interface: 192.168.0.3

R2#show ip nat translations

Pro	Inside global	Inside local	Outside local	Outside global
icmp	20.0.0.2:2032	192.168.0.3:2032	20.0.0.3:2032	20.0.0.3:2032

可以观察到复用了20.0.0.3的不同端口号。

附录一 名词解释（A）

AARP: AppleTalk地址解析协议。把数据链路地址映射成网络地址的AppleTalk协议栈中的协议。

AC: 交流电。有规律地交替其方向的电流。它是用于住宅楼和商业楼的电流形式。

Access list: 访问表。由Cisco路由器保存用来为许多服务控制出/入此路由器的表。

Access server: 接入服务器。通过网络和终端仿真软件把异步设备连接到某一局域网或广域网上的通信处理器。完成所支持的协议的同步选路和异步选路。有时也叫作网络接入服务器。

ACK: acknowledgment。为确认某事件（例如接收到一条消息），从一个网络设备向另一个网络设备发出的通知。

Active hub: 有源集线器。放大局域网传输信号的多端口设备。

Adapter: 适配器。

Address: 地址。用来识别独特实体的（如特定的进程或网络设备）数据结构或逻辑约定。

附录一 名词解释（A）

Address mapping: 地址映射。通过把地址从一种格式转换为另一种格式而使得不同的协议能够协同工作的技术。例如，在X.25网上为IP选择路由，IP地址必须被映像成X.25地址以便IP数据包能被X.25网络传送。

Address mask: 地址掩码。用于描述地址的哪一部分是网络或子网，哪一部分是主机的比特组合。有时简称为掩码。

Address resolution: 地址解析。通常指解决计算机寻址方式之间差别的方法。地址解析通常指把网络层（第三层）地址映射成数据链路层（第二层）地址的方法。

Address Resolution Protocol: 地址解析协议。

Adjacency: 邻接。为交换路由选择信息在选择的邻近路由器和端节点间形成的关系。邻接基于同一介质段的使用。

Adjacent nodes: 相邻节点。1、SNA中，不经过中间节点就直接连接到某一节点的节点。2、在DECnet和OSI中，共享同一网络段（例如在以太网、FDDI、令牌环网络中）的节点。

附录一 名词解释（A）

Administrative distance: 管理距离。路由选择信息源的可信度的级别。在Cisco路由器中，管理位距由从0到255的数值表示。数值越高，可信度级别越低。

Advertising: 通知。每隔一段时间发送路由选择或服务更新，以便网络上的其它路由器能维护一张有用的路由表的路由器过程。

Algorithm: 算法。是解决问题的明确的规则或程序。在网络中，算法通常用于确定业务量从一个特定信源到特定信宿的最好路由。

AppleTalk: 苹果计算机公司设计出来的通信协议系列。目前有两个阶段。第一个阶段是早期的版本，支持只有一个网络号和只在一个地区的单个物理网络。第二个阶段是比较新的版本，支持单个物理网路上的多个逻辑网并允许网络分布在不止一个地区。

Application layer: 应用层，OSI参考模型的第七层。该层向OSI模型的应用程序（如电子邮件、文件传送和终端仿真）提供服务，识别并证实目的通信方的可用性（以及必须和它们连接的资源），使协同工作的应用程序同步，并协商错误恢复和数据完整性控制的过程。

附录一 名词解释（A）

Area: 区域。网段（CLNS-、DECnet-或基于OSPF）逻辑装置及其所连接的设备，区域通常通过路由器和其它区域相连，从而形成一个自主系统。

Area border router: 区域边界路由器。

ARP: 地址解析协议。把IP地址映射到MAC地址的因特网协议。

ARPANET: 高级研究项目代理网。建立于1969年，是分组交换网络发展的里程碑。七十年代，BBN对ARPANET进行了开发，并由ARPA（后来的DARPA）提供资金。ARPANET最后演化成因特网。ARPANET这一名词在1990年正式被取消。

ARQ: 自动重复请求。接收设备检测错误和请求重传的通信技术。

AS: autonomous system。

ASBR: 自主系统边界路由器。位于OSPF自主系统和非OSPF网络之间。ASBRs可以运行OSPF和另一路由选择协议（如RIP）。ASBR必须处于非存根OSPF区域中。

ASCII: 美国信息交换标准码。字符用8比特码来表示（7比特加上校验位）。

附录一 名词解释 (A)

Asynchronous Transfer Mode: 异步传输模式。在ATM中，各种服务类型（例如语音、视频或数据）都以固定长度（53字节）信元的形式进行传送。固定长度的信元使得可以在硬件中对信元进行处理，从而减少了延迟。ATM的设计应能利用高速传输介质如E3，SONET和T3。

Asynchronous transmission: 异步传输。此术语用于描述不需要精确定时就能被传送的数字信号。这样的信号通常具有不同的频率和相位关系。异步传输通常把单个字符封装在用于指明每个字符的开始和结束的控制比特（也叫起止比特）里。

Attachment unit interface: 附连单元接口。MAU和NIC（网络接口卡）之间的IEEE 802.3接口。AUI这一名词也可以指后面板端口（AUI电缆连接在它上面）。AUI也叫做收发信机电缆。

Attenuation: 衰减。通讯信号能量的减少。

Autonomous system: 自主系统。在共享一公共路由选择策略公共管理下的网络集合。自主系统按区域细分，一个自主系统必须由IANA分配一个独特的16比特号码。

Autonomous system boundary router: 自主系统边界路由器。

附录一 名词解释（B）

Back bone: 主干网。网络的一部分，作为那些经常来自或去向其他网络业务的主要路径。

Backbone cabling: 主干电缆。提供配线室之间、配线室与POP之间以及同一局域网大楼之间的相互连接的电缆。

Back off: 退避。发生冲突时的强制性重传延迟。

Backward explicit congestion notification: 向后显式拥挤通告。

Backward learning: 后向学习。用于路由选择业务的算法过程，该业务通过假定处于对称网络条件下来推测信息。例如，如果节点A通过中间节点C收到来自节点B的分组，后向学习路由选择算法就假定A能最优化地通过C到达B。

Bandwidth: 带宽。网络信号所能达到的最高频和最低频之差。这一术语也用于描述某网络介质或协议的额定吞吐能力。

Bandwidth reservation: 带宽预留。把带宽分配给用户和网络服务的应用程序的过程。包括根据业务流重要性和延迟敏感性为不同业务流分配优先级。这样就最大限度地利用了带宽，如果网络发生拥塞，低优先级的业务就被丢弃。有时也称为带宽分配。

附录一 名词解释（B）

Baseband: 基带。只用一段载波频率的网络技术特性。Ethernet是基带网的一个例子，也称窄带，相对于broadband而言。

Baud: 波特。信令速率单位，即每秒传送的离散信号元的数量，如果每个信号元代表1比特，波特相当于每秒传送的比特数（bps）。

Bc: 传送极限。在帧中继互联网络中通过的业务公制。一个帧中继互联网络应接受并在CIR传送的最大数据量（以比特计算）。

B channel: B信道。在ISDN中，用于传送用户数据的全双工64Kbps承载信道。

Be: 超量极限。在帧中继网络中通过的业务公制。在Bc之后，一个帧中继网络企图传送的比特量是可以调节的。因为Be数据会被网络标记为DE，所以一般地，Be数据有比Bc数据更低的传送可能性。

BECN: 向后显式拥挤通告。在与遇到一拥塞路径的传输方向相反的帧中，由帧中继网络设置的比特，DTE（接收带有BECN比特设置的帧）会请示较高层协议采取合适的流量控制行动。

Bellman-Ford routing algorithm: 贝尔曼-福特路由选择算法。

附录一 名词解释（B）

BGP：边界网关协议。替代EGP的区域间路由选择协议。

BGP4：边界网关协议4.0版本。BGP4.0版。因特网上所用的主要区域间路由选择协议的第4版。它支持CIDR并使用路由集合机制减小路由表的大小。

Binary：二进制。以1和0表示为特点的计数系统（1=开0=关）。

BISDN：宽带综合业务数字网。ITU-T通信标准的设计应能处理高宽带应用（如视频）。BISDN目前在基于SONET的传输电路上使用ATM技术，以提供从155到622Mbps甚至更高的数据速率。

Bit：比特。二进制计数系统中使用的二进制位。可以是0或1。

Bit rate：比特速率。通常用每秒比特数（bps）表示。

Bits per second：每秒比特数。缩写为bps。

Blocking：阻塞。指在交换系统中，没有路径可使用来完成回路的情况，该术语也用来描述只有当另一个活动完成时，一活动才能开始的情况。

附录一 名词解释（B）

BNC connector: BNC连接器。用于把IEEE 802.3 10Base2同轴电缆连接到MAU的标准连接器。

BOOTP: 启动协议。由网络节点用来确定以太网接口IP地址，以便网络引导的协议。

Boot PROM: 引导可编程只读存储器。安装在印刷电路板上用于向计算机设备提供引导指令的芯片。

Border gateway: 边界网关。与其他自主系统的路由器进行通信的路由器。

Border Gateway Protocol: 边界网关协议。

BPDU: 网桥协议数据单元。是一种生成树协议问候数据包，它以可配置的间隔发出，用来在网络的网桥间进行信息交换。

BRI: 基本速率接口。ISDN接口由用于话音、视频和数据电路交换通信的两个B信道和一个D信道组成。

Bridge: 网桥。在使用相同通信协议的两个网段间连接和传递分组的装置。网桥在OSI参考模型的数据链路层（第二层）上运行。

附录一 名词解释（B）

Bridge protocol data unit: 网桥协议数据单元。

Broadband ISDN: 宽带综合业务数字网。

Broadcast: 广播。传给网络所有节点的数据包。

Broadcast address: 广播地址。预留给向所有站点传送信息的特殊地址。

Broadcast domain: 广播区域。能接收集合内任一设备发出的广播帧所有设备的集合。因为路由器不转发广播帧，广播区域一般由路由器设定边界。

Broadcast storm: 广播风暴。一种讨厌的网络事件，事件发生时，许多广播同时也在所有网段上传送。广播风暴占用相当可观的网络带宽，并且一般会引起网络超时。

Buffer: 缓冲器。用于处理转接数据的存储区域。缓冲区用在互联网络中可以退避网络设备间处理速度的差别。数据突发可存在缓冲区，直到它们可以被较慢的设备处理。有时也称为包缓冲区。

Bus: 总线。由电线或其他媒介组成的公共物理信号路径，通过该路径信号可从计算机的一部分传送到另一部分。有时也称母线。

附录一 名词解释（B）

Bus topology: 总线拓扑。线型局域网结构，在该结构中，网络站点的传输传送介质的长度并且可以被所有其他站点接收。

Byte: 字节。该术语指作为单位操作的一系列连续的二进制数（例如8比特字节）。

附录一 名词解释 (C)

Cable: 电缆。指的是包裹在保护套中的铜线或光纤传输介质。

Cable television: 有线电视。

CAM: Content-addressable memory。内容可寻址存储器。

Carrier: 载波。电磁波或单一频率的交流电流, 用于被另外的承载数据的信号所调制。

Carrier Detect: 载波检测。

Carrier sense multiple access collision detect: 载波监听多路访问及冲突检测技术。

Category 1 cabling: 第一类电缆。第一类电缆是EIA/TIA-568B标准中所描述的五类非屏蔽双绞线电缆之一。它用于电话通信, 但不适于传输数据。

Category 2 cabling: 第二类电缆。第二类电缆是EIA/TIA-568B标准中所描述的五类非屏蔽双绞线电缆之一。它能够以高达4Mbps的速率传输数据。

附录一 名词解释（C）

Category 3 cabling: 第三类电缆。第三类电缆是EIA/TIA-568B标准中所描述的五类非屏蔽双绞线电缆之一。它用于10BaseT的网络中，并且能够以高达10Mbps的速率传输数据。

Category 4 cabling: 第四类电缆。第四类电缆是EIA/TIA-568B标准中所描述的五类非屏蔽双绞线电缆之一。它用于令牌环网络中，并且能够以高达16Mbps的速率传输数据。

Category 5 cabling: 第五类电缆。第五类电缆是EIA/TIA-568B标准中所描述的五类非屏蔽双绞线电缆之一。它用于运行CDDI，并且能够以高达100Mbps的速率传输数据。

CCITT: 国际电报电话咨询委员会。负责开发通信协议的国际组织。现在改名为国际电信联盟—电信标准化部分。

CD: 载波检测。用于指示一个接口是否处于活动状态的信号。也指由调制解调器产生的用于指示一个呼叫是否已经被连接的信号。

CDDI: Copper Distributed Data Interface。铜缆分布式数据接口。在屏蔽和非屏蔽双绞线上实现的FDDI协议。铜缆分布式数据接口的传输距离相对较短（约100米），提供了使用双环冗余结构上100Mbps的数据速率。

附录一 名词解释（C）

CDP: Cisco查找协议。与介质和协议无关的设备查找协议，它能够在所有Cisco公司制造的设备上运行，包括路由器、访问服务器、网桥和交换机。使用Cisco查找协议，一个设备能够把它自身存在的信息通知给位于同一局域网或广域网远端上的其它设备，同时也可以接收这些设备存在的信息。Cisco查找协议可以在所有支持SNAP的介质上运行，这些介质包括局域网、帧中继和ATM网。

Cell: 信元。ATM网络交换和复用的基本单元。信元包含的标识信息致命了该数据流的归属。每个信元包含5字节的信息头和48字节的数据。

Challenge Handshake Authentication Protocol: 挑战握手验证协议。

Channel: 信道。1、通信路径。在某些环境下可以把多个信道复用到一根电缆上。2、在IBM的术语中，信道指的是大型计算机间的特定路径以及与之相连的外围设备。

Channel service unit: 信道服务单元。

附录一 名词解释（C）

CHAP: 挑战握手鉴权协议。为防止未授权访问而使用端对端协议封装的线路上所支持的安全特性。它自己本身并不能防止未授权的访问，它只是用于辨识终端。然后路由器或访问服务器就能够决定该用户是否可以访问。

Checksum: 校验和。用于检验被传输的数据的完整性的方法。校验和是对一序列的八位组经过一系列算术运算而得到的整数值。在数据接收端，该值被重新计算并与发送时计算的值相比较，从而实现对数据的校验。

CIDR: 无级别域内路由。BGP4支持的基于路由累加的技术，它允许路由器为了减少核心路由器携带的路由信息而把路由组合成组。通过使用CIDR，几个IP网络对于组外的网络而言就像是单一的大网络。

CIR: 指定信息速率。帧中继网络在正常条件下允许的信息传送速率，它是在最小的一段时间里的速率均值。CIR是以每秒多少比特计算的，它是tariff metrics协商出中的一个关键计量单位。

Circuit: 电路。两个或多个端点间的通信路径。

附录一 名词解释（C）

Circuit switching: 电路交换。在呼叫进行期间，发送方和接收方必须存在一条专用的物理电路的交换系统即电路交换。它主要应用于电话公司网络中。作为信道访问技术，可以与争用和令牌环传递技术相比；作为交换技术，可以与报文交换和分组交换技术相比。

Class of service: 1、服务类别。有关上层协议需要下层协议怎样处理它的报文的指示。在SNA子区路由选择中，COS定义被子区节点用来确定最佳的路由以建立给定会话。COS定义包含一个虚的路由号和一个传输优先级域。也被称作TOSTOS（服务类型）。2、开放系统协会。通过一致性测试、证明和相关活动发布OSI协议的用途的组织。

CLI: 命令行界面的缩写。它被用于监控和控制一个ATM网络、用户节点或者向服务器申请服务的软件程序。

Client: 客户。指节点或软件程序（前端设备），它们需要来自服务器的服务。

Coaxial cable: 同轴电缆。包着一根内部线缆的空心的圆柱状导体，当前用于局域网的两种同轴电缆是：用于数字信令的50-ohm电缆，和用于模拟信号和高速数字信令的75-ohm电缆。

Coding: 编码。用于传输二进制信号的电子技术。

附录一 名词解释 (C)

Collision: 冲突。在以太网中，当两个节点同时传输数据时，从两个设备发出的帧将会碰撞，当它们在物理介质上相遇时，彼此的数据都会被破坏。

Collision detection: 冲突检测。

Collision domain: 冲突域。在以太网中，冲突域指的是位于传播发生的帧冲突的网络区域。重发器和集线器都会传播冲突；局域网交换机，网桥和路由器不会传播冲突。

Committed information rate: 指定信息速率。

Concentrator: 集中器。

Conductor: 导体。任何对电流具有低阻抗的材料。任何能够传输电流的材料。

Configuration register: 配置寄存器。在路由器中，配置寄存器是一个16位的用户定义的值，它决定了路由器在初始化时如何工作。配置寄存器可以存储在硬件或者软件中。当存储在硬件上时，通过使用跳线设定各位的位置；当存储在软件上时，用配置命令通过制定一个16进制数的值来设定各位的位置。

附录一 名词解释 (C)

Congestion: 拥塞。当业务量超过网络的容量时的状态。

Congestion avoidance: 拥塞避免。它是一种这样的机制，即运用基于LightStream的ATM网络来控制进入网络的业务量，从而将时延最小化。为了更有效地使用网络资源，如果网络情况表明低优先级的业务量将不能被传递，那么该业务量将在网络的边缘被丢弃。拥塞避免有时缩写为CA。

Connectionless: 无连接。用来描述在不需要虚电路的情况下的数据传送的术语。

Connection-oriented: 面向连接。用来描述需要虚电路设立的数据传送的术语。

Connection-Oriented Network Protocol: 面向连接网络协议。

Console: 控制台。DTE，通过它命令进入主机。

Convergence: 集中/收敛。在互联网的拓扑结构有变化以后，一组运行特定的路由选择协议的互联网连接设备同意该拓扑结构变化的速度和能力。

Core gateway: 核心网关。因特网中主要的路由器。

附录一 名词解释 (C)

Core router: 核心路由器。在数据分组交换星形拓扑结构中的路由器，它是主干网的一部分，作为来自外围网络的所有业务量必须沿路径传送到其它外围网络的单一管道。

Cost: 代价/开销。通常基于跳跃计数、介质带宽或其它测量方法的任意值。它是由网络管理员所分配，并通过互联网来比较不同的路径。路由选择协议利用代价值来确定最佳路径：代价越小，路径越佳。

Count to infinity: 无穷计数。会聚缓慢的路由选择算法中可能出现的问题。路由器会连续地增加特定网络的跳跃计数值。一般来说，设置某个任意的跳跃计数限制值可以预防这个问题的出现。

CPE: 用户站设备。电话公司提供的终接设备，比如终端，电话，调制解调器。它安装在用户所在地点，并和电话公司的网络相连。

CRC: Cyclic redundancy check。循环冗余校验。一种差错校验技术。帧的接收端通过把帧的内容除以原始二进制除数来计算余数，并把计算所得的余数和发送端存储在帧中的值相比较。

附录一 名词解释 (C)

Cross talk: 串音。从一个电路传到另一个电路的干扰能量。

CSMA/CD: 带有冲突检测的载波侦听多路访问。一种介质访问机制, 在这种机制下, 准备传输数据的设备首先检查载波通道。如果在一定时间内没有侦听到载波, 那么一个设备就可以发送数据。如果两个设备同时发送数据, 冲突就会发生并被所有冲突设备所检测到。这种冲突便延缓了这些设备的重传, 使得它们在隔某一随机时间后才发送数据。CSMA/CD访问用于以太网和IEEE 802。

CSU: 通道服务单元。把终端用户和本地数字电话环路相连的数字接口设备。通常它和DSU统称为CSU/DSU。

CTS: 1、清除发送。EIA/TIA-232规范中, 当DCE准备接收来自DTE的数据时所激活的电路。2、公共传输语义。IBM战略的基础。它为网络软件开发商提供一个API, 并使应用程序运行在APPN、OSI或TCP/IP上。

Cut-through packet switching: 伺机通过分组交换。一种分组交换方法。它通过交换机传送数据, 使得分组的前面部分在整个分组进入输入端口前, 在交换机上的输出端口上离开交换机。使用伺机通过分组交换的设备在检查目的端地址和确定输出端口时, 便读取, 处理和转发分组。它也称为on-the-fly分组交换。请和存储和转发分组交换比较。

附录一 名词解释（D）

Data communications equipment: 数据通信设备。数据通信设备（EIA扩展的）或者数据电路终端设备（ITU-T扩展的）。该设备和其与通信网络的连接构成了网络终端的用户网络接口，提供了到网络的一条物理连接、转发业务量，并且提供了一个用于同步DCE设备和DTE设备之间数据传输的时钟信号。如解调器和接口卡。

Datagram: 数据报。指在没有事先建立一个虚电路的情况下，在传输介质上作为网络层单元发送的信息的逻辑分组。

Data-link connection identifier: 数据链路连接标识。数据链路连接标识符。指的是在帧中继网络中表示PVC（永久虚电路）或SVC（交换式虚电路）的值。在基本的帧中继规范中，数据链路连接标识符在局部内是很重要的（连接的设备可能会用不同的值来表示相同的连接）。在LMI（层管理接口）扩展规范中，数据链路连接标识符在全局内都很重要的（数据链路连接标识符表示单一的终端设备）。

Data link layer: 数据链路层。它指的是OSI参考模型的第二层。该层提供了通过物理链路的可靠数据传输。数据链路层主要关心物理寻址、网络拓扑、线路描述、按顺序传输各帧和流控。IEEE已经把数据链路层分成了两个子层：MAC子层和LLC子层。数据链路层有时只简单地叫作链路层。它大致对应于SNA模型中的数据链路控制层。

附录一 名词解释（D）

Data set ready: 数传机就绪。指的是当DCE（数据通信设备）上电并准备就绪时，EIA/TIA-232接口电路被激活。

Data service unit: 数据业务单元。指的是用于数字传输中的一种设备，它能够把DTE设备上的物理层接口适配到T1或者E1等通信设施上。数据业务单元也负责信号计时等功能，它通常与CSU（信道业务单元）一起提及，称作CSU/DSU。

Data stream: 数据流。指在单一的读或写操作中所有经过通信线路传输的数据。

Data terminal equipment: 数据终端设备。指的是位于用户网络接口用户端的设备，它能够作为信源、信宿或同时为二者。数据终端设备通过数据通信设备（例如，调制解调器）连接到一个数据网络上，通常使用数据通信设备产生的时钟信号。数据终端设备包括计算机、协议翻译器以及多路分解器等设备。

Data terminal ready: 数据终端就绪。指的是当DTE（数据终端设备）准备好收发数据时，EIA/TIA-232接口电路被激活来通知DCE（数据通信设备）。

DB: Decibels. 分贝。

附录一 名词解释（D）

DC：直流。只向一个方向传播的电流。直流电通常用于电子电路中。

D channel：D信道。1、数据信道。全双工、速率为6-kbps（BRI，基本速率接口）或64-kbps（PRI基群速率接口）的ISDN信道。2、在SNA（系统网络体系结构）中，它指的是一个把处理器和主存储器与外围设备相连接的设备。

DDR：Dial-on-demand routing。拨号请求路由选择。Cisco路由器能够根据发送工作站的请求，自动初始化和结束一个电路交换的会话的一种技术。路由器一直伪装成激活状态，从而使得终端工作站一直认为该会话处于激活状态。拨号请求路由选择允许在ISDN线路或者在使用了一个ISDN终端适配器或调制解调器的电话线路上进行路由选择。

DE：可丢弃的。

Deadlock：死锁。1、指对资源使用时产生的不可解决的争抢。2、在APPN（先进的对等层联网）中，它指的是在一个进程恢复运行之前，进程的两个部分互相等待对方的操作或响应的现象。

附录一 名词解释（D）

DECnet: 由DEC公司开发和支持的通信产品（包括协议套件）系列。

Dedicated line: 专线。永久地被保留用于传输的通信线路，而不是当有传输请求时由交换得到的通信线路。

Default route: 缺省路由。指的是路由表中未直接列出的路由选择项，它用于指示数据帧下一跳的方向。

Delay: 延时。指的是发送方初始化一项事务和接收方第一次响应该事务之间的时间差。它也指在一定路径上把数据分组从信源端传输到信宿端所需的时间。

Demarc: 分界。承载设备和计算机外围设备（CPE）间的分界点。

Demodulation: 解调。指的是将调制信号还原成起始形式的过程。调制解调器接收一个模拟信号，然后通过解调把信号还原成初始（数字）的形式。

DES: 数据加密标准。由美国NBS开发的标准加密算法。

Designated bridge: 指定网桥。指的是当从一个网段向路由网桥转发一帧数据时，承担最低路径费用的网桥。

附录一 名词解释（D）

Designated router: 指定路由器。指的是能够为多接入网络产生LSAs的 OSPF（开放最短路径优先）路由器，在运行OSPF中它还具有其它的特殊责任。每一个具有至少两个路由器的OSPF多接入网络都有一个有OSPF Hello协议选出的指定路由器。指定路由器使得在多接入网络中邻域的数目减少了，这又反过来减小了路由选择协议通信的数量和拓扑数据库的大小。

Destination address: 目的地址。接收数据的网络设备的地址。

Destination MAC: 目的MAC（介质存取控制）。指的是在一个数据分组的地址域中所指明的MAC地址。

Dial backup: 备用拨号（线路）。这是Cisco路由器所支持的特性，它通过允许网络管理员通过电路交换的连接来配置后备串行线路，提供了在广域网关闭时的保护。

Dial-up line: 拨号线路。指的是使用电话公司的网络、由电路交换连接建立起来的通信电路。

附录一 名词解释（D）

Differential encoding: 差分编码。指的是一种数字编码技术，其中的二进制值是由一个信号跃变来标识的，而不是用一个特定的信号电平。

Differential Manchester encoding: 差分曼彻斯特编码。指的是一种数字编码技术，其中中间比特时间的状态迁移被用作时钟信息，在每一个比特时间的开始处的状态迁移代表0。它是IEEE 802.5标准和令牌环网使用的编码方案。

Diffusing Update Algorithm: 扩散修正算法。

Digital Network Architecture: 数字网络结构。这是由DEC公司开发的一种网络结构。内部嵌入了数字网络结构（包括通信协议）的产品被总称为DECnet。

Digital signal: 数字信号。计算机语言只包含两个状态：由一系列电压脉冲代表的开与关。

Direct memory access: 直接存储器存取。

Distance Vector Multicast Routing Protocol: 位移矢量组播路由选择协议。

附录一 名词解释（D）

Distance vector routing algorithm: 位移矢量路由选择算法。指的是一类路由算法，它遍历一个路由的所有跳数来寻找一个最短路径展开树。位移矢量路由选择算法需要每个路由器在更新器路由表后向它的邻接路由器发送出整个更新路由选择表。位移矢量路由选择算法虽然易于形成环路路由，但是它比链路状态路由选择算法计算起来简单。它也被叫作Bellman-Ford路由选择算法。

DMA: 直接存储器存取。它指的是不经过微处理器就能够从硬盘等外围设备把数据传输到存储器。它可以在没有处理器开销的情况下以高速将数据传入存储器。

DNS: Domain Naming System。域名命名系统。该系统用在互联网中用来把网络节点的名字翻译成网络地址。

Domain: 域。1、在互联网中，它指的是命名等级树的一部分，它是根据组织或者地理位置的通用网络分组。2、在SNA（系统网络体系结构）中，它指的是一个系统服务控制点和它所控制的资源。3、在IS-IS（中介系统到中介系统）中，它指的是一个网络的逻辑集合。

附录一 名词解释（D）

Dot address: 点分地址。指的是常用的形如a. b. c. d的IP地址的符号，其中每一个十进制数代表4字节IP地址中的一个字节。它也被叫作点分符号或者四部分的点分符号。

DRAM: 动态随机存取存储器。将信息存储在电容中的随机存取存储器必须定期更新。当动态随机存取存储器更新其内容时，由于此时处理器不能访问它，故而有可能产生时延。然而动态随机存取存储器比SRAM（静态随机存取存储器）结构简单，而且容量更大。

DUAL: 扩散更新算法。它是一种用于改善的IGRP中的收敛算法，它提供的无循环操作能够以极快的速度完成一次路由计算。它允许在网络拓扑发生改变时，受到影响的路由器的调整能够与网络拓扑的改变同步进行，而未受影响的路由器不作任何改变。

Dual homing: 双宿。指的是一种网络拓扑，其中的设备通过两个独立的接入点（连接点）。其中一个接入点是主连接；另一个是备用连接，只有当主连接出现故障时它才被激活。

Dynamic routing: 动态路由选择。它指的是能够自动适应网络拓扑或者通信变化的路由选择。它也称作自适应路由选择。

附录一 名词解释 (E)

E1: 指的是主要用于欧洲的广域数字传输方案, 它以2.048 Mbps的速率传输数据。可以从公共电信服务商那里租用E1线路作为专用线路。

E3: 指的是主要用于欧洲的广域数字传输方案, 它以34.368 Mbps的速率传输数据。可以从共用载波那里租用E3线路作为专用线路。

EDI: Electronic data interchange。电子数据互换。指的是组织之间进行的类如订单和发票的电子数据通信。

EEPROM: Electrically erasable programmable read-only memory。电可擦可编程只读存储器。指的是可以使用专门接线端所用的电子信号来擦除的EPROM（可编程只读存储器）。

EGP: Exterior Gateway Protocol。外部网关协议。它是一个在自治系统之间交换路由选择信息的因特网协议。它定义在RFC 904文档中。外部网关协议是一个过时的协议, 它已经被BGP协议所代替。

EIA: Electronic Industries Association。电子工业协会。它是一个制定电子传输标准的组织。电子工业协会和TIA（电信工业协会）制定了大量的有名的通信标准, 例如EIA/TIA-232标准和EIA/TIA-449标准。

附录一 名词解释（E）

EIA/TIA-232：指的是由电子工业协会和电信工业协会联合开发的通用物理层接口标准，它能够支持高达64 kbps信号速率的非均衡电路。它与V. 24规范非常相近。

EIA/TIA-449：指的是由电子工业协会和电信工业协会联合开发的通用的物理层接口标准。它是EIA/TIA-232标准的一个速率更高（高达2 Mbps）的版本，而且支持更长的电缆。正式名称是RS-449。

EIA/TIA-568：指的是描述了不同等级的非屏蔽双绞线电缆的特点和应用的标准。

EIA/TIA-606：指的是商业建筑电信基础设施的管理标准。它包括如下的管理范围：终端、介质、路径、空间、分界和接地。

EIGRP：Enhanced Interior Gateway Routing Protocol。改进的内部网关路由协议。它是由Cisco公司开发的内部网关路由协议的高级版本。它提供了超级汇聚性能和高效操作性，并且把链路状态协议的优点与位移矢量协议的优点相结合。

Electronic mail：电子邮件(电子信箱)。。它是一种广泛使用的网络应用，它可以在使用不同类型的网络协议的终端用户之间用电子装置传输邮件。

附录一 名词解释（E）

Encapsulation: 封装。把数据包装到带有一个特殊协议报头中。例如，以太网数据在传输之前被封装到一个以太网报头中。同样地，当在不同类的网络中桥接时，发自一个网络的所有帧只需简单地放入接收端网络使用的数据链路层协议报头中。

Encryption: 加密。应用特定的算法对数据进行处理，从而改变数据的表面形式，使得那些未被授权查看信息者无法理解这些数据。

Error control: 差错控制。指的是一种用于检测和纠正数据传输中的错误的技术。

Error-correcting code: 纠错码。它拥有足够的智能，并且包含足够的信令信息，这使得它能够检测并纠正接收方的许多错误。

Error-detecting code: 检错码。指的是一种码，它根据数据对相应的结构指南的遵循程度，对接收数据进行分析，从而能够检测出数据传输的错误。

Ethernet: 以太网。指的是由Xerox公司创建并由Xerox、Intel和DEC公司联合开发的基带局域网规范。以太网使用CSMA/CD（载波监听多路访问及冲突检测技术）技术，并以10 Mbps的速率运行在多种类型的电缆上。

附录一 名词解释 (E)

Excess Burst: 超量突发。

Excess rate: 超出速率。指的是在给定的连接上超出了安全速率的通信。特别地，超出速率等于最大速率减去安全速率。超出的通信只有当网络资源够用时才会被传送，当网络处于拥塞时，超出的通信将被丢弃。

附录一 名词解释 (F)

Fast Ethernet: 快速以太网。快速以太网是指任何一个速率达到100M比特率的以太网。快速以太网在保持帧格式、MAC机制和MTU质量的前提下，其速率比10Base-T的以太网增加了10倍。二者之间的相似性使得10Base-T以太网上现有的应用程序和网络管理工具能够在快速以太网上使用。快速以太网是基于扩充的IEEE802.3标准的。

FCC: 联邦通讯委员会。美国政府监督、批准和管理电子和电磁传输标准的团体。

FCS: Frame check sequence。帧校验序列。为进行差错控制而加入到一个帧中的额外符号。帧校验序列用在高级数据控制规程 (HDLC)、帧中继和其他数据链路层协议中。

FDDI: Fiber Distributed Data Interface。光纤分布式数据接口。它是一个ANSIX3T9X9.5规范，指的是传输距离达2公里，速率每秒100兆位(100Mbps)，利用光纤电缆进行令牌传输的局域网络。它采用双令牌结构以保证冗余度。

FECN: Forward explicit congestion notification。前向显式拥塞通知。由帧中继网络设置的标志位来通知接收该帧的数据终端设备 (DTE) 从源到目的地的路径发生拥挤。接收到带有前向显式拥挤通知标志位的数据终端设备能要求高层协议进行适当的流量控制。

附录一 名词解释 (F)

Fiber-optic cable: 光缆。能够传导调制光信号的物理传输介质。与其他传输介质比较, 光纤电缆更加昂贵, 但是它不受电磁干扰, 而且能达到更高的数据传输速率。有时它被称为光导纤维。

File Transfer Protocol: 文件传输协议。作为TCP/IP协议组一部分的应用协议, 用来在网络节点间传输文件。

Filter: 过滤器。通常来讲, 过滤器是一个进程或设备。它筛选出具有某些特征的网络数据流, 例如源地址, 目的地址或协议, 并且按照建立的标准决定是转发还是丢弃该数据流。

Firewall: 防火墙。它是指路由器或访问服务器、或者几个路由器或访问服务器被设计为任意相连的公用网络和专用网络之间的缓冲区。防火墙路由器使用访问列表和其他方法保证专用网络的安全。

Firmware: 固件。永久性或半永久性的存储在只读存储器 (ROM) 中的软件指令。

Flash memory: 快闪内存。由Intel公司发展起来并授权给其他半导体公司的一项技术。它是永久性的存取器, 能够电擦除存储内容并可再次编程。在必要的情况下, 允许软件映像存储, 引导和再次写入。

附录一 名词解释 (F)

Flooding: 扩散法。交换机和网桥使用的信息传输技术。指的是在交换机或网桥中，当从一个接口接收到信息后，将其从该设备除最初接收到它的接口以外的所有接口发送出去的方法。

Flow: 信息流。两个终端通过网络传输的数据流（例如，从一个局域网网站到另一个局域网网站）。多路信息流能够在一条电路上传送。

Flow control: 流量控制。保证一个发送设备，例如调制解调器，其发送数据的速率不超过接收设备接收速率的技术。当接收设备中的缓冲区充满时，就发送一条消息给发送设备暂停传送，直到缓冲区内的数据被处理掉。在IBM网络中，这项技术被称为调步。

FM: 频率调制。不同频率的信号表示不同数据值的调制技术。

Forwarding: 转发。通过互联网连接设备将一帧信息向它的最终目的地发送的过程。

Forwarding priority: 转发优先级。

Fourier transform: 傅里叶变换。用于对时间序列模式评价其不同频率周期重要性的技术。

附录一 名词解释 (F)

Fragment: 报片。被分为很多小单元的大数据分组中的一片。

Fragmentation: 分片。当网络传输介质不能支持数据分组的原始大小时，将数据分组分为较小单元的过程。

Frame: 帧。作为数据链路层单元在传输介质上传送的逻辑信息组。包含在一帧中的用户数据通常是被用来进行同步化和差错控制的报头和报尾包围的。在OSI参考模型的各个层和不同的技术环节数据报、报文、数据分组和段等术语也都被用来描述逻辑信息组。

Frame Relay: 帧中继。处理多个虚拟电路的工业标准，是在互连设备之间使用高级数据控制规程（HDLC）封装的交换数据链路层协议。它比X.25分组协议更有效，通常被认为是对X.25分组协议的替换。

Frequency: 频率。交流信号每单位时间内的周期数，单位为赫兹。

Full duplex: 全双工。能够在发送站点和接收站点之间同时进行数据传输的能力。

Full mesh: 全贯通网。用来描述网络设备被组织为网状拓扑结构的网络的术语，其中每一个网络节点有一个物理电路或虚拟电路将它与其他网络节点相连。全贯通网络提供了大量冗余，但因为它实现起来过于昂贵，所以通常专门用于骨干网络。

附录一 名词解释（G）

Gateway: 网关。在因特网协议（IP）范畴中，原始的含义指一个路由选择设备。而现在，是用路由器一词来表示具有路由选择功能的节点；网关则被用来指一种特殊用途的设备，它能够在应用层将信息堆栈从一种协议转化为另一种协议，不同于router。

Get Nearest Server: 获取最近服务器。

GNS: 获取最近的服务器（协议）。基于IPX协议的网络客户发出请求包以定位相对于它最近的某特定类型活动服务器。基于IPX协议的网络客户发布GNS请求以期获得一个相联服务器的直接响应或一个路由器的响应，此响应用以确定因特网网络服务的提供地点。GNS是IPX协议的服务布告协议（SAP）的一部分。

GRE: 通用路由选择封装。CISCO隧道协议能够封装IP隧道中的多种协议包类型，并在因特网上创建一个到远程CISCO路由器的虚拟点到点链接。在单协议主干网络环境中，通过连接多协议通信子网，IP隧道化工作利用GRE（通用路由封装）功能使网络能在此（单协议主干网）环境中得到扩展。

GUI: Graphical user interface。图形用户界面。这是一种用户使用环境，它使用图形和文字表达应用系统、层次数据结构或其他数据结构的输入输出结果，这些数据结构用以存储信息。

附录一 名词解释（H）

Half duplex: 半双工。发送站和接收站之间，数据的传输在某一时刻只能向一个方向进行。

Handshake: 信号握手。数据通信中，当两台或更多网络设备连接时，为保证传输的同步，而进行的信息序列的交换。

HDLC: High-Level Data Link Control。高级数据链路控制。由国际标准化组织（ISO）制定的面向比特的同步数据链路层协议。起源于SDLC，高级数据链路控制（HDLC）定义了同步串行链接时，使用字符帧及校验和进行数据封装的模式。

Header: 报头。为了网络传输进行数据封装时，放在数据前面的控制信息。

Hierarchical routing: 分层（级）路由选择。路由选择基于层次地址系统。例如，IP路由选择规则使用包含网络号、子网号和主机号的IP地址。

Holddown: 阻持。路由器在一段阻持时间中，所处于的一种既不通告路由也不接收路由通告的状态。阻持用于从网络的所有的路由器中冲掉有关一个路由的不利信息。典型的阻持如，当某路由的一个链接失败时，此路由将被置为阻持状态。

附录一 名词解释（H）

Hop: 跳。描述两个网络节点间（如两个路由器之间）的一个数据数据包通路的术语。

Hop count: 跳计数。路由选择度量，它用来测量来源地和目的地之间的距离。RIP用跳计数作为它唯一的度量。

Host: 主机。指网络计算机系统。类似 node（节点），但host（主机）通常是指一个计算机系统，而节点则一般用于任何联网的系统，其中包括访问服务器和路由器。

Hot Standby Router Protocol: 热备份路由器协议。提供了网络的高实用性和网络拓扑变化的透明性。HSRT建立一个有引导路由器的热备份路由器组来服务所有发送到热备份路由器地址的数据包。引导路由器受组里的其它路由器监控，如果引导路由器失效，这些备份路由器中的一个就会继承引导路由器的地位和热备份路由器组的地址。

HTML: Hypertext markup language。超文本链接标识语言。简单的超文本文档格式语言，采用标识来说明已给出的部分文档应如何被浏览程序解释，例如万维网（WWW）浏览器。

附录一 名词解释（H）

Hub：集线器。1、通常，该术语用来描述一个起星形拓扑网络中心点作用的设备。2、包含多种独立的，但是连接了网络模块和因特网设备的硬件或软件装置。集线器可以是主动方式（它们能重复通过它们发送的信号）或被动方式（它们不重复，而仅仅拆分通过它们发送的信号）。3、在以太网和IEEE 802.3中，指一个以太网多端口中继器，有时称为concentrator（集中器）。

Hypertext：超文本。电子化存储的文本，通过链接码直接访问其它文本。超文本文档可以利用HTML（超文本链接标识语言）来建立，通常将图像、声音和其它媒体合成一个整体，一般使用WWW浏览器观看。

IANA：Internet地址和域名分配组织。它是作为IAB的一部分、在ISOC的支持下运作的组织。IANA把IP地址空间分配和域名分配的权力授予NIC及其它组织。IANA还负责维护一个用于TCP/IP堆栈的分配协议标识符数据库，包括自主系统号码。

ICMP：ICMP Router Discovery Protocol。Internet控制信息协议。是网络层的因特网协议，它负责报告错误，并提供与IP数据包处理相关的其它信息。

附录一 名词解释（I）

IEEE：电气和电子工程师协会。是一个专业组织，其活动包括通信和网络标准的开发。IEEE LAN标准是当今居于主导地位的LAN标准。

IEEE 802.1：IEEE规范，它描述通过生成扩展树来阻止网桥回路的一种算法。该算法是由数字设备公司（Digital Equipment Corporation）发明的。Digital算法和IEEE 802.1算法并不完全相同，也不兼容。

IEEE 802.12：IEEE LAN标准，确定物理层和数据链接层的MAC子层。IEEE 802.12以100 Mbps的速率在许多物理介质上使用命令优先级介质访问方案。

IEEE 802.2：IEEE LAN协议，它规定数据链接层的LLC子层的实现。IEEE 802.2处理错误、组帧、流量控制和网络层服务接口。它在IEEE 802.3和IEEE 802.5 LAN中使用。

IEEE 802.3：IEEE LAN协议，它确定物理层和数据链接层的MAC子层的实现。IEEE 802.3在许多物理介质上以不同速度使用CSMA/CD访问。IEEE 802.3标准的扩充版规定了快速以太网的实现。原始IEEE 802.3规范的物理更改包括10Base2、10Base5、10BaseF、10BaseT和10Broad36。快速以太网的物理更改包括 100BaseT、100BaseT4和100BaseX。

附录一 名词解释（I）

IEEE 802.3i: 原始IEEE 802.3规范的物理更改，它要求通过双绞线网络介质，使用以太网类型的信令。标准设定信令速度为10兆比特每秒，使用一个通过双绞线电缆传输的基带信令图，该双绞线电缆采用星形或延伸的星形拓扑。

IEEE 802.4: IEEE LAN协议，它规定物理层和数据链接层的MAC子层的实现。IEEE 802.4在总线拓扑上使用令牌传送，并建立在令牌总线LAN体系结构上。IEEE 802.5: IEEE LAN协议，它规定物理层和数据链接层MAC子层的实现。IEEE 802.5以4或16 Mbps的速率在屏蔽双绞线（SIP）上使用令牌传送，与IBM令牌环相似。

IEEE 802.6: 基于分布队列双总线（DQDP）技术的IEEE MAN规则。IEEE 802.6支持从1.5到155Mbps的数据速度。

IETF: 因特网工程部。工程部包括80多个负责开发因特网标准的工作小组。IETF在ISOC的支持下运作。

IGMP: 因特网组管理协议。IP主机用它将主机的组播组成员人数报告给临近的组播路由器。

IGP: 内部网关协议。在自治系统中交换路由选择信息的因特网协议。常用的因特网内部网关协议有IGRP、OSPR和RIP。

附录一 名词解释（I）

IGRP: Interior Gateway Routing Protocol. 内部网关路由选择协议。是由Cisco公司开发的IGP，用于解决在大的异类网络中与路由选择有关的问题。

In-band signaling: 带内信令。在一个频率范围内进行的传输。

Infrared: 红外线。 频率范围高于微波、但低于可见光的电磁波。

Insured burst: 安全突发量。 超过安全速率的、在永久虚拟电路上被暂时允许的最大数据突发量，它在网络堵塞的时候不会被业务量管制功能加上标记，予以丢弃。安全突发量用字节或信元来规定。请与最大的突发量相对比。

Integrated Services Digital Network: 综合业务数字网。

Interface: 接口。1、指两个系统或者两个设备之间的联接。2、在路由选择的术语中，指网络联接。3、在电话行业，指一个共享边界，该共享边界是通过一般的物理互连特性、信号特性，以及交换信号的含义来定义的。4、指OSI模型相邻层之间的边界。

Intermediate system: 中介系统。是在一个OSI网络中的路由选择节点。

附录一 名词解释（I）

International Standards Organization: 国际标准组织。

Internet: 因特网。互连网（internetwork）的缩写。该术语指最大的全球互联网，它联接上万个全球网络，并有一种将注意力集中在基于现实生活利用的研究和标准化上的“文化环境”。许多领先的适当的网络技术都来自于因特网环境。因特网是从APRA网中演变而来的，它曾被称为DARPA Internet

Internet address: 因特网地址。

Internetwork: 互联网。通过路由器和其它设备互相连接的网络的集合，它的功能（一般）就象是一个单一的网络。

Interoperability: 互操作性。由不同供应商制造的计算设备所具有的能力，它通过网络可以成功地实现与其它设备的通信。

Inverse ARP: Inverse Address Resolution Protocol。逆向ARP。逆向地址解析协议。是在一个网络中建立动态路由的方法，允许一个存取服务器发现一个与虚拟电路相联的设备的网络地址。

IP: Internet protocol, 因特网协议。是TCP/IP栈中的网络层协议，它提供一个无连接的互联网服务。IP提供寻址的功能、服务类型的规范、分段存储和重新组合、以及安全的特性。

附录一 名词解释（I）

IP address: IP地址。应用TCP/IP协议分配给主机的32位地址。一个IP地址属于五种类型（A、B、C、D或E）之一。每个地址都包含一个网络号、一个可选的子网络号和一个主机号。

IP multicast: IP组播。是一种路由选择技术，它允许IP业务量从一个信源向一个目的端传播，或者从许多信源向许多目的端传播。不是将一个数据包传送给每个目的端，而是将一个数据包传送给一个由单独的IP目的端组地址进行识别的组播组。

IPX: 互联网分组交换。是NetWare网络层（第三层）协议，用于从服务器向工作站传输数据。IPX与IP及XNS类似。

ISA: 工业标准体系结构。用于基于Intel的个人计算机的16位总线。

ISDN: 综合业务数字网。是由电话公司提供的通信协议，它允许电话网络传送数据、声音和其它的信源业务量。

IS-IS: Intermediate System-to-Intermediate System中介系统中介系统。是建立在DECnet Phase V路由选择基础上的OSI链接状态层次的路由选择协议，IS（路由器）借此根据单一的距离度量交换路由选择信息，从而确定网络拓扑。与集成的IS-IS相对应。

附录一 名词解释（I）

ISO：国际标准化组织。该国际组织负责大范围的标准，包括那些与因特网相关的标准。ISO开发了开放系统互连（OSI）参考模型，这是一个流行的网络连接参考模型。

附录一 名词解释（J）

Jumper: 跳线。1、指代接线柜中定位接插线的术语。2、指的是由许多引线和（一个可以用多种不同方式附着在引线上的接线器组成的）电开关。不同的电路由接线器附着在不同的引线上创建。

附录一 名词解释 (L)

LAN: 局域网。高速、少错的数据网，它覆盖一个相对较小的地区(最多几千平方米)。局域网在一个单独的大楼内或其它有限区域连接工作站、外围设备、终端及其它装置。局域网标准规定在OSI模型的物理层和数据链路层布缆和信令。以太网、FDDI（光纤分布式数据接口）及令牌环被局域网技术广泛地使用。

LAN switch: 局域网交换机。在数据链路网段间转发数据分组的高速交换机。大多数局域网交换机基于MAC地址转发业务量。这种局域网交换机有时被叫做帧交换机。局域网交换机经常依照它们转发业务量所使用的方案进行分类：丢弃数据分组交换或存储转发数据分组交换。多层交换机是局域网交换机的一种智能子集。

LAPB: Link Access Procedure, Balanced。平衡的链路访问规程。X.25协议栈中的数据链路层协议。LAPB是一个起源自HDLC的一个面向比特的协议。

LAPD: Link Access Procedure on the D channel。D信道上的链路访问规程。D信道的ISDN数据链路层协议。LAPD起源于LAPB协议，而且主要是为满足ISDN基速率访问的信令需求而设计的。它由标准ITU-T Q.920和Q.921定义。

附录一 名词解释 (L)

Laser: 激光器。辐射激发的光放大。它是一种模拟传输设备，其中的相应源材料被外部激发产生连贯的窄光束，这个光束可以被调制为脉冲以携带数据。基于激光技术的网络有时在SONET上运行。

Laser: 激光器。辐射激发的光放大。它是一种模拟传输设备，其中的相应源材料被外部激发产生连贯的窄光束，这个光束可以被调制为脉冲以携带数据。基于激光技术的网络有时在SONET上运行。

Latency: 延迟。1、设备请求访问网络的时间和被准许发送权限的时间之间的时延。2、设备接收帧的时间和那个帧被目的端口转发出去的时间之间的时延。

Leased line: 租用线路。通信服务商为用户私人使用而预留的传输线路。租用线路是专用线的一种类型。

LED (light emitting diode): 发光二极管。通过转换电能引起发光的半导体设备。

LLC: 逻辑链路控制。数据链路层两个子层中更高级的一层，它由IEEE定义。逻辑链路控制子层处理错误控制、流控制、帧同步和MAC子层寻址。最常用的逻辑链路控制协议是IEEE 802.2协议，它包括无连接和面向连接两种变量。

附录一 名词解释（L）

LMI: Local Management Interface. 本地管理接口。它是基本帧中继规范的增强集。本地管理接口包括对“保留”机制（检验数据是流动的）、组播机制（提供有局部DLCI和组播DLCI的网络服务器）、全球寻址（在帧中继网络中给DLCIs 全球的超过本地的有效位）和状态机制（提供被交换机辨别出的DLCIs的现行状态报告）的支持。

Load balancing: 负载平衡。在路由选择中，路由器在它所有的到目的端地址均是同样距离的网络端口上分配业务量的能力。一个好的负载平衡算法使用线路速度和可靠性信息两者。负载平衡增加网段的使用率，从而增加有效的网络带宽。

Logical address: 逻辑地址。

Logical channel: 逻辑信道。指的是非专用的，两个或多个网络节点之间的数据分组交换通信路径。它是一种数据分组交换，允许多个逻辑信道同时地存在于单一物理信道上。

Loop: 回路。数据分组从未到达它们目的端的路由，只是简单循环，再三地通过一连串固定的网络节点。

Loopback test: 回送测试。信号被发送后沿着通信路径从一些节点返回它们的信源的测试。回送测试经常被用来检验网络接口的可用性。

附录一 名词解释（L）

LSA: Link-state advertisement. 链路状态公告。由链路状态协议使用的广播数据分组，它包含有关邻居和路径成本的信息。接收路由器使用链路状态公告以维护它们的路由选择表。有时也被称作链路状态数据分组（LSP）。

附录一 名词解释 (M)

MAC: 介质访问控制。IEEE定义的数据链路层里两个子层中的底层。MAC子层处理对共享介质的访问，比如是否使用令牌环传送或冲突。

MAC address: MAC地址。和局域网相连的每个端口或设备所需的标准的数据链路层地址。网络中的其它设备利用这些地址来定位网络上的特定端口，并生成和修改路由表及数据结构。MAC地址有六个字节长，并受IEEE控制。也称为硬件地址。

MAN: Metropolitan-area network。城域网。

Manchester encoding: 曼彻斯特编码。IEEE802.3和以太网使用的数字编码方案。在这个方案中，每个比特传输时间的中间值的变换用于定时，1表示相应比特传输时间的前半部分是高电平。

Mask: 掩码。

MAU: 介质连接单元。这是在以太网和IEEE802.3网络使用的设备，提供了工作站AUI端口和以太网公共介质的接口。MAU可以附属在工作站上或者是个单独的设备，它完成物理层的功能，包括来自以太网接口的数字数据的转换，冲突检测，以及把比特发送到网络上。它有时也称为介质访问单元，其简写也是MAU，或者收发器。在令牌环网络中，MAU是作为多站访问单元，且常常简写为MSAU来避免混淆。

附录一 名词解释 (M)

Maximum burst: 最大突发量。它规定了超过安全速率的数据最大突发量。它可以在ATM PVC暂时性地存在,而且,在业务量监控功能允许的边缘下也不会被丢弃,即使它超过了最大速率也是如此。最大突发量只允许临时性的存在,平均而言,源业务量速率应该在最大速率范围内。单位是字节数或者信元数。

Maximum rate: 最大速率。给定虚拟电路上允许的总的最大数据吞吐量。它等于来自源业务量的安全业务量和非安全业务量的总和。如果网络出现拥塞,那么非安全业务量可能被丢弃。最大速率不能超过介质速率,表示虚电路将要发送的最大数据吞吐量,单位是比特/秒或信元/秒。

MD5: Message Digest 5. 第五类报文摘要。这是用于SNMP v.2中报文认证的算法。MD5负责验证通信的完整性,认证信源,并检验合时性。

Media: 介质。传输信号经过的不同的物理环境。常见的网络介质有双绞线,同轴电缆,光纤电缆和空气(微波、激光和红外线传输都发生在此)。它有时也称为物理介质。

Media access unit: 介质访问单元。

Media attachment unit: 介质连接单元。

附录一 名词解释 (M)

Mesh: 网格。这是一种网络拓扑结构，其中的设备以可管理的分段方式组织，在网络节点间存在许多常常是冗余的策略上的交叉连接。

Message: 报文。信息在应用层（第七层）的逻辑分组，通常是由许多底层的逻辑分组组成，比如分组。datagram(数据报)，frame(帧)，packet(分组)和网段这些术语也用来描述OSI参考模型不同层和不同技术周期内的逻辑信息分组。

Microsegmentation: 微分段。把网络分成更小段的分割方法，其目的通常是给网络设备增加总带宽。

Modem: 调制解调器。调制器-解调器。是转换数字信号和模拟信号的设备。在发送端，调制解调器把数字信号转换为适合在模拟通信设施上传输的信号。在目的端，模拟信号被转换回数字信号。调制解调器允许数据在话音等级的电话线上传输。

Modulation: 调制。把电子信号特性转换成代表信息的过程。调制类型包括AM、FM和PAM。

MTU: Maximum transmission unit。最大传输单元。特定接口可以处理的最大分组大小，它以字节为单位。

附录一 名词解释 (M)

Multicast: 组播。复制并发送到网络地址中特定子集的单个分组。这些地址在目的端地址域中指明。

Multimode fiber: 多模光纤。支持光波的多频传播的光纤。

附录一 名词解释 (N)

NAK: 否定确认。从接收设备返回到发送设备的应答，表示所接收到的信息包含错误。

Narrowband: 窄带。

NBMA (Nonbroadcast multiaccess): 非广播多重访问。这个术语用来描述不能支持广播(比如X.25)或者广播不切实际(例如，太大的SMDS广播组或太大的扩展以太网)的多重访问网络。

Neighborhood discovery: 寻找邻居。

Neighboring routers: 邻近路由器。在OSPF中，具有连向公共网络的接口的两个路由器。在多重访问网络时，邻居是由OSPF Hello协议动态地寻找到的。

NetBIOS: Network Basic Input/Output System. 网络基本输入/输出系统。IBM LAN上的应用程序使用的API，它用来请求得到底层网络进程的服务。这些服务可能包括会话的建立和终止，以及信息传输。

NetWare: Novell开发的、流行的分布式NOS。它提供了透明的远程文件访问和许多其它的分布式网络服务。

NetWare Link Services Protocol: Netware 链路服务协议。

附录一 名词解释 (N)

Network: 计算机，打印机，路由器，交换机和其它一些能在传输介质上相互通信的设备的集合。

Network address: 网络地址。网络层地址，指的是网络设备的逻辑地址，而非物理地址。也称它为协议地址。

Network analyzer: 网络分析仪。负责维护有关网络及其相连设备状态的统计信息的网络监控设备。大多数先进的网络分析仪使用了人工智能技术，可以检测、定义和修复网络上的故障。

Network layer: 网络层。OSI 参考模型的第三层。这一层提供两个终端系统间的连接机制和路径选择。网络层是进行路由选择的那一层，和SNA模型的路径控制层大致对应。

NFS: Network File System。网络文件系统。常用的Sun Microsystem制定的分布式文件系统协议组，它允许网络上的远程文件访问。实际上，NFS只是协议组中的一个简单协议。NFS协议组包括NFS、RPC、XDR及其它。这些协议是SUN称之为ONC的大型结构的一部分。

NIC: Network interface card。网络接口卡。能提供网络通信能力的板子，以便和计算机系统进行发送和接收。

附录一 名词解释 (N)

N-ISDN: Narrowband ISDN。窄带ISDN。ITU-T为基带网络制定的通信标准。它基于64-kbps的B信道和16-或 64kbps的D信道。

Node: 1、网络连接的端点，或者网络上两个或更多个线路的结合点。节点可以是处理器、控制器、或工作站。各个节点在路由选择和其它功能上都有所不同，它们可以通过链路相互连接，也可以作为网络的控制点。节点有时用来指任何可以访问网络的实体，而且经常和device互换使用。2、在SNA中，网络的基本组成。一个（或更多个）功能单元连接多个信道（或数据电路）所在的点。

Noise: 噪声。不希望有的通信信道信号。

Non-stub area: 非存根区。资源密集的OSPF区，它含有缺省路由、静态路由、内部路由，区间路由和外部路由。非存根区域是可以包含虚拟链路横跨其中的唯一OSPF区，也是唯一可以包含ASBR的区。

NOS: Network operating system。网络操作系统。用来描述真正的分布式文件系统的通称。NOS的例子包括有LAN Manager、Netware、NFS和VINES。

Null modem: 空调制解调器。用来直接将计算设备相连的小盒子或电缆。

附录一 名词解释 (N)

NVRAM (Nonvolatile random-access memory)：非易失的RAM。当电源掉电时，它依然能保存所存有的内容。在Cisco产品中，NVRAM用来存储配置信息。

附录一 名词解释（0）

Open shortest path first: 开放式最短路径优先。

Open System Interconnection: 开放式系统互连。

Optical fiber: 光纤。

OSI: 开放式系统互连。这是OSI和ITU-T制定的国际标准计划，用来制定方便多厂商设备互操作性的数据联网标准。

OSI reference model: 开放式系统互连参考模型。这是ISO和ITU-T制定的网络结构模型。这个模型包括七层，每层都规定了特定的网络功能，比如寻址，流量控制，差错控制，封装和可靠报文传输。最高层（应用层）和用户最近，最底层（物理层）和介质技术最近。紧接着最底层的那一层通过软件和硬件实现，而更高的那五层都是通过软件实现的。OSI参考模型通常作为讲授和理解网络功能性的方法来使用。和SNA类似。

OSPF: 开放式最短路径优先。这是反映链路状态的分层IGP路由选择算法，被认为是因特网中RIP的取代者。OSPF特性包括最低代价路由选择，多路径路由选择，和加载平衡。OSPF来源于ISIS协议的一个早期版本。

附录一 名词解释（0）

Out-of-band signaling: 带外信令。所用频率或信道超出了信息正常传输时使用的频率或信道的传输。带外信令通常用于带内信令被任何网络故障所影响时的错误报告。

附录一 名词解释（P）

Packet: 数据分组。数据报、帧、报文 和 段这些术语都是用来描述OSI参考模型的不同层和不同技术周期内的逻辑信息分组。

Packet switching: 分组交换。节点间通过发送分组来共享带宽的联网机制。

PAP: Password Authentication Protocol。密码认证协议。这个协议允许PPP类用户相互认证。试图和本地路由器连接的远程路由器必须发送一个认证请求。和CHAP不一样，PAP显式传送密码和主机名字或用户名。PAP自身不会防止非法访问，仅是识别远程终端。路由器或访问服务器然后确定用户是否允许访问。PAP只使用在PPP线路上。

Parallel transmission: 并行传输。这是一种数据传输机制。在这种机制下，数据字符中的比特可以同时许多信道传输。

Parity check: 奇偶校验。检验字符完整性的过程。通过增加一个比特来使一个字符或字（不包括校验位）中二进制数字‘1’的总数为奇数（奇校验）或者（偶校验）。

附录一 名词解释 (P)

Partial mesh: 部分网格。这是用来描述其中设备为网格状拓扑结构的网络的术语，一些网络节点为完全网格状，另一些只是和网络中一个或两个其它节点相连。部分网格不提供完全网格拓扑结构中的冗余度，但是它实现的代价要低。部分网格拓扑结构通常用于和完全网格的骨干网相连的外围网。

PDU: Protocol data unit, 协议数据单元。用于分组的OSI术语。

Peak cell rate: 峰值信元速率。

Peak rate: 峰值速率。虚拟电路中能传送的最大速率，单位为千比特/秒。

Permanent virtual circuit: 永久虚电路。

Permanent virtual connection: 永久虚连接。

Permanent virtual path: 永久虚路径。

PGP: Pretty Good Privacy (高度保密)。这是一个给公开密钥加密的应用程序，它实现安全的文件和报文交换。此应用程序的开发和使用中存在一些争论，其部分原因是出于美国国家安全的考虑。

附录一 名词解释 (P)

Physical layer: 物理层，这是OSI 参考模型的第一层。物理层定义了电气规范，机械规范，过程规范和功能规范，这些规范用于激活，维护和终止终端系统间物理链路的工作。物理层和SNA模型中的physical control layer对应。

PIM: Protocol Independent Multicast. 协议独立的组播。组播路由选择结构允许在现有的IP网络上增加IP的组播路由选择。PIM是独立的一点广播路由选择协议，可以工作在两种模式下：密集和稀疏模式。

PIM DM: PIM dense mode, PIM密集模式。是数据驱动的，类似于典型的组播路由选择协议。分组发送到所有输出接口上，直到出现分组截取。在密集模式下，接收器分布较为密集，而且假定下行网络想接收并很可能使用发送给它们的数据报。使用密集模式的代价是它缺省的溢出行为。有时，它也称为密集模式PIM或PIM DM。

PIM SM: PIM sparse mode. PIM稀疏模式。PIM稀疏模式试图限制数据分布，以便让网络上最少数量的路由器来接收它。在RP（会合点）处显式需要它们的时候，分组才被发送出去。在稀疏模式下，接收器分布很广泛，而且假定下行网络不必要的使用发送给它们的分组。使用稀疏模式的代价就是它对显式加入报文的刷新和它对RP的需求。有时它也称为稀疏模式PIM或PIM SM。

附录一 名词解释 (P)

Ping: 分组因特网查询进程。ICMP反射报文和它的应答，它通常用来测试网络设备的可到达性。

Polling: 轮询。主网络设备利用这种接入机制来有序查询从设备是否有数据发送。查询以报文的形式发送给每个从设备，从而把传输权利赋予此从设备。

Port: 端口。1、互联网设备上的接口（比如说路由器）；2、在IP术语中，用来表示正接收底层信息的高层过程；3、重写软件或微代码，以便它可以在不同的硬件平台上或不同的软件环境下运行，而不是在原先的条件下运行；4、插线板的母插头，它接受和RJ45插头同样大小的插头。在这些端口上用接插线把连到线路板上的计算机交叉连接起来。这种交叉连接使得LAN可以正常工作。

POST (Power-on self test): 上电自检。是在硬件设备上电以后，运行此设备上的硬件诊断操作。

PPP: Point-to-Point Protocol. 点到点协议。作为SLIP的替代者，PPP提供了同步和异步电路上的路由到路由和主机到网络的连接。

附录一 名词解释（P）

Presentation layer: 表示层。OSI参考模型的第六层。这一层确保了一个系统的应用层所发送的信息可以被另一个系统的应用层读取。表示层也和程序使用的数据结构有关，和应用层得数据传输语法进行协商。它和SNA模型的表示服务层大致对应。

Presentation services layer: 表示服务层。SNA参考模型的第六层。这一层提供了网络资源管理，会话表示服务和一些应用程序管理，和OSI模型的表示层大致对应。

PRI: 基群速率接口。ISDN的基群速率访问接口。基群速率访问包含一个64Kbps的D信道和23（T1）或30（E1）个话音或数据的B信道。

Protocol: 协议。规定网络设备如何交换信息的规则和约定集合的正式描述。

Protocol converter: 协议转换器。使得具有不同数据格式的设备，可以通过把一个设备的数据传输代码翻译为另一个设备的数据传输代码，来进行相互通信。

Protocol stack: 协议栈。OSI参考模型上一些层或所有层里，相互协作或作为一个组来进行通信的相关通信协议的集合。

附录一 名词解释（P）

Protocol translator: 协议翻译器。把一个协议转换为另外一个相似协议的网络设备或软件。

Proxy: 代理。从效率上看，基本上能代表另一个实体的实体。

Proxy ARP: Proxy Address Resolution Protocol。代理ARP。ARP协议的一种变换形式。在这种形式下，中间设备（比如路由器）代表目的端发送一个ARP应答给发送请求的主机。代理APR可以减少低速WAN链路上的带宽。

PSDN: 分组交换数据网。

PSE: 分组交换机。本质上说，它就是一个交换机。PSE术语通常指的是X.25 PSN中的交换机。

PSN: 1、分组交换网。利用分组交换技术进行数据传输的网络。有时也称为packet-switched data network（分组交换数据网PSDN）。2、分组交换节点。能执行分组交换功能的网络节点。

PSTN: Public Switched Telephone Network。公共交换电话网。世界范围内的电话网和服务的变化形式的总称。有时也称为plain old telephone service（无格式的老式电话服务POTS）。

附录一 名词解释（P）

PVC：永久虚电路。永久性建立的虚电路。PVC在某些虚电路必须一直存在的情况下，保存和电路建立及拆卸相关的带宽。称为permanent virtual connection(永久虚连接)。

PVP：永久虚路径。包含PVC的虚路径。

附录一 名词解释（Q）

QOS (Quality of service)：服务质量。它是传输系统性能的标准，反映了传输的质量和服务的可靠性。

Query：查询。用来查询某个变量或者一套变量值的消息。

Queue：队列。1、一般指等待处理的元素的有序队列。2、在路由中，指等待从路由器接口发送的一队数据包。

附录一 名词解释 (R)

RAM (Random-access memory) : 随机访问存储器。

RARP (Reverse Address Resolution Protocol) : 反向地址解析协议。是TCP/IP协议堆栈中的协议, 基于MAC地址寻找IP地址的方法。

Reassembly: 重组。指的是数据在源端或者在中间媒质节点分成自带寻址信息的IP数据包, 这些数据包在终端重新组合。

Redirect: 重定向。它是ICMP协议和ES-IS协议的一部分。它允许路由器告诉主机使用另一个效率更高的路由器。

Redistribution (Route redistribution) : 重新分配。允许把从一个路由表中寻找到的路由信息重新分配在另一个路由协议中的更新信息。有时也称为路由重新分配。

Redundancy: 冗余。1、网络中, 为防止故障而配备的备份设备、业务或连接。这样, 在出现故障时使用这些冗余设备, 业务或者连接。2、在电话业务中, 是指一个消息中所含的整个信息的一部分, 这部分可以删除而不丢失消息的基本信息或意思。

Relay: 中继。描述连接两个或者多个网络系统的设备的OSI术语。一个数据链路层(第二层)的中继器是一个网桥; 一个网络层(第三层)的中继器是路由器。

附录一 名词解释（R）

Reliability: 可靠度。一个链路可以预期的保持正常接收的比率。如果这个比率很高，链路就可靠。作为一个路由选择量度来使用。

Reload: 重新装载。指的是Cisco路由器出现的启动事件，或者引起路由器重新启动的命令。

Repeater: 重发器。在两个网段之间再生和传播电信号的设备。

RFC (Request For Comments): 请评论文档。在互联网中作为通信信息主要含义使用的文件系列。有些RFC文档是由IAB设计，作为互联网标准。大部分RFC文件协议是Telnet和FTP规则，但是有些不实际或者过时。请评论文档可以通过在线方式为多个源端使用。

Ring: 环路。连接两个或者多个工作站得连接拓扑电路。信息持续在活动的工作站间传递。令牌环，FDDI和CDDI都是基于这种拓扑。

RIP (Routing Information Protocol): 路由信息协议。是一种UNIX BSD 系统提供的IGP（内部网关协议）。是互联网中最普通的IGP。路由信息协议使用网段跳数作为路由计量单位。

ROM: Read-only memory. 只读存储器。只能阅读，不能由微处理器进行写操作的不易失存储器。

附录一 名词解释 (R)

Root bridge: 根网桥。它在一个展开树型网络结构中指定网桥交换拓扑信息，以便在拓扑需要改变时通知网络中所有其它网桥。这样可以防止环路，并提供了抵御线路故障功能的方法。

Route: 路由。通过互联网络的路径。

Routed protocol: 被动路由协议。可通过路由器引导路由的协议。路由器必须能够把逻辑上的互联网络翻译为路由协议中的规则。如AppleTalk协议，DECnet和IP协议。

Route map: 路由映射。在路由域之间控制路由重新分配的方法。

Route summarization: 路由摘要。指的是在OSPF和IS-IS中广播来明确地址，这会使地区边缘路由器将一条路由摘要广播给其它地区。

Router: 路由器。是使用一种或者更多度量因素的网络层设备，它决定网络通信的最佳路径，依据网络层信息将数据包从一个网络转发到另一个网络。也称为网关。

Routing: 路由选择。寻找到达一个终端主机的路径的过程。选择路由在大型网络中非常复杂，因为在一个数据包在到达终端之前将经过许多潜在的中间信宿。

附录一 名词解释（R）

Routing metric: 路由量度。指的是选择路由算法决定一条路径优于另一条路径的方法。这个信息存储在路由表中。这些度量包括带宽，通信费用，时延，跳数，负载，最大传输单元，路径费用和可靠性。有些时候只简单地当作一种度量。

Routing protocol: 主动路由协议。指的是通过执行一个特殊选择路由算法实现路由选择的协议。选择路由协议的例子包括内部网关路由协议，最短开通道优先协议和路由信息协议。

Routing table: 路由表。指的是路由器或者其它互联网网络设备上存储的表，该表中存有到达特定网络终端的路径，在某些情况下，还有一些与这些路径相关的度量。

Routing update: 路由更新。从路由器发出的包含网络是否可以到达以及相关费用信息的信息。通常在固定时间间隔和网络拓扑发生变化之后发路由刷新消息。

RP (Rendezvous point/Route Processor) : 1、路由处理器。包含CPU，系统软件，和路由器使用的大部分存储器元件。有时称为管理处理器。2、集合地点。PIM稀疏模式定的路由器，在多点投递组中跟踪成员，发送信息来了解多点投递组地址。

附录一 名词解释 (R)

RPC (Remote-procedure call)：远端过程调用。它是客户机/服务器计算机体系的技术基础。远端过程调用是由用户建立或者规定的过程调用，它在服务器上执行，并将执行结果通过网络传递给用户。

RPM (Reverse Path Multicasting)：反向路径组播。指除了用来传送单点数据的接收接口之外，其它所有的接收接口将多点投递报文传送给发出多点投递报文的源端，这种技术称为报文多点投递技术。

RS-232：一种流行的物理层接口。现在称为EIA/TIA-232。

RSP (Route/Switch Processor)：路由/交换处理器。

RTP (Rapid Transport Protocol/Routing Table Protocol)：快速传输协议。1、路由表协议。基于RIP协议的VINES路由协议。它分布网络拓扑信息，帮助VINES服务器找到相邻用户，服务器和路由器。它使用延时作为路由选择的量度。2、快速传输协议。当APPN数据通过APPN网络时，提供步距和误码恢复。当使用快速传输协议，误码恢复和流量控制都是端到端的操作，而不是对每个节点的。快速传输协议能够防止阻塞，而不是对阻塞做出反应。

附录一 名词解释（R）

RTS (Ready To Send)：准备发送。是一个EIA/TIA-232控制信号，该信号请求在一条通信线路上传输数据。

RTT：往返时间。网络通信从源端到终端再返回所需要的时间。往返时间包括终端处理从源端发送的信息的时间和产生应答的时间。往返时间在一些选择路由算法中使用，来帮助计算最佳路径。

附录一 名词解释 (S)

SAP (Service access point/Service Advertisement Protocol) : 1、服务接入点。它是由IEEE 802.2规定的域，是地址规范的一部分。这样，信宿和DSAP定义了包的接收方。这同样应用于SSAP。2、服务公告协议。是一种IPX协议，是借助路由器和服务器提供信息给网络用户的一种方式，这些信息包括网络中可以使用的资源和服务。

SDH (Synchronous Digital Hierarchy) : 同步数字序列。它是欧洲一个标准，规定了在光纤中传输光信息的一套速率和格式标准。SDH与SONET类似，具有基本的SDH速率155.52Mbps，在STM-1规定。

SDLC (Synchronous Data Link Control) : 同步数据链路控制。SNA (系统网络体系结构) 数据链路层通信协议。是面向比特，全双工串口协议，它产生了很多类似的协议，如HDLC和LAPB。

Segment: 段。1、网段，网络的一个部分，由网桥，路由器，或者交换机确定边界。2、在一个使用总线拓扑局域网中，一个段是一条连续电路，经常通过中继器与其它段相连接。3、TCP规范中使用的术语，描述一个传输层的信息单元。datagram、frame、message和packet也用来描述OSI参考模型不同层和不同技术范围中的逻辑消息组。

附录一 名词解释 (S)

Serial transmission: 串行传输。数据字符的比特流通过这种方式在一个信道中持续传输。

Server: 服务器。为客户提供服务的节点或者软件程序。

Session: 会话。1、两个或者更多网络设备之间的相关通信事务。2、在SNA中，指的是允许两个NAU进行通信的逻辑连接。

Session layer: 会话层。指的是OSI参考模型的第五层。该层建立，管理和终止服务间的会晤，管理表示层实体间的数据交换。它对应于SNA模型中的数据流量控制层。

Shielded cable: 屏蔽电缆。为减少电磁干扰而覆有绝缘层的电缆。

Signaling: 信令。指的是在物理介质上为进行通信发送一个传输信号的过程

Simplex: 单工。数据在一个发送工作站和一个接收工作站之间只能单向传输的能力。

Single-mode fiber: 单模光纤。是有一个窄芯的光纤光缆，它仅允许光从一个角度进入光纤。这样的光缆比多模光纤有更高的带宽，但是要求窄谱宽光源(例如，激光器)。又称为单一模式光纤。

附录一 名词解释 (S)

SLIP (Serial Line Internet Protocol)：串行线路互联网协议。使用更改的TCP/IP协议的点对点串行连接的标准协议。是点对点连接的处理器。

SMTP (Simple Mail Transfer Protocol)：简单邮件传输协议。提供电子邮件服务的互联网协议。

SNA (Systems Network Architecture)：系统网络结构。它是IBM公司1970年开发的大型，复杂，多功能网络结构。与OSI参考模型的某些概念类似，但也有很多不同。SNA基本也由七层组成。

SNMP (Simple Network Management Protocol)：简单网络管理协议。几乎所有的TCP/IP网络都使用的网络管理协议。简单网络管理协议提供监视和控制网络设备，管理配置，统计收集，性能，和安全的一种方式。

Socket：插口。指的是在一个网络设备中作为通信终端使用的软件结构。

SONET (Synchronous Optical Network)：同步光纤网络。由Bellcore开发的高速(大于2.5 Gbps)同步网络规范。STS-1是同步光网络基本的建筑块。在1988年成为国际标准。

附录一 名词解释 (S)

SPAN: 交换式端口分析仪。它将现存网络分析仪的监视功能扩展到以太网环境。SPAN将一个交换网段的服务流镜像到一个预先指定的SPAN端口。一个附着在SPAN端口的网络分析仪可以监视从其它任何Catalyst交换端口出来的服务流。

Span (Switched Port Analyzer): 在两个数字设备之间的全双工数字传输线路。

Spanning tree: 生成树。指的是网络拓扑的一种自由环子集。

Spanning-tree algorithm: 生成树算法。指的是生成树协议使用的算法，用来生成一个生成树。有时简称为STA。

Spanning-Tree Protocol: 生成树协议。保证一个已知的网桥在网络拓扑中沿一个环动态工作。网桥交换BPDU消息来监测环路，然后关闭选择的网桥接口取消环路。有时简称为STP。

SPF (Shortest path first algorithm): 最短路径优先。它是一种选择路由算法，在所有路径上遍历以计算最短路径生成树。通常用在链路状态选择路由算法。有时称为 Dijkstra's algorithm (Dijkstra 算法)。

附录一 名词解释 (S)

SPID (Service Profile Identifier): 服务类型标识。一些服务提供者使用的数字, 用来定义ISDN (综合服务数字网) 设备预订的服务。当访问交换机时ISDN设备使用SPID, 该交换机初始化与服务提供者的连接。

Split-horizon updates: 分区更新。是一种选择路由技术, 它阻止接收的路由信息从路由接口中离开。分区更新在防止路由循环方面很有用。

Spoofing: 电子欺骗。1、Cisco路由器使用的方案, 它使得主机认为一个接口已经开放并且支持会话。路由器电子欺诈依赖于从主机发来的保持激活消息, 以便使主机清楚会话仍在继续。电子欺诈在DDR等选择路由环境很有用, 在没有服务流通过时关闭电路交换链路来节省开支。2、数据包不合规定地声明发送地址, 而实际上并不是从这个地址发送的。电子欺诈用来绕过滤波器和访问名单等网络安全机制。

SPX: Sequenced Packet Exchange. 顺序分组交换。是可靠的面向连接的协议, 是网络层(第三层)协议提供的报文服务的补充。Novell从XNS协议套件中的SPP派生出这个通常使用的NetWare传输协议。

SS7 (Signaling System number 7): 7号信令系统。宽带ISDN和ISDN使用的标准共信道信令系统。由Bellcore开发。

附录一 名词解释（S）

Static route: 静态路由。它是明确得被配置和填入路由表中的路由。在路由选择上静态路由比动态路由协议优先。

Store and forward packet switching: 存储转发分组交换。一种分组交换技术。在这种技术中，帧在转发到合适的端口前经过了完全的处理。处理过程包括计算CRC和检验目的端地址。此外，这些帧必须暂时存储起来，直到有网络资源来转发报文。

STP (Shielded twisted-pair): 1、屏蔽双绞线。STP连接电缆包含一个屏蔽的绝缘层来减少EMI。2、Spanning-Tree Protocol。

Stub area: 存根区域。包含缺省路由，区域内路由和区域间路由但不包含外部路由的 OSPF区域，虚链路不能在存根区域中配置，也不能包含ASBR。

Stub network: 存根网络。只包含一个和路由器的连接的网络。

Subinterface: 子接口。

Subnet: 子网。

Subnet address: 子网地址。IP地址的一部分。它用子网掩码来表示子网。

附录一 名词解释（S）

Subnet mask: 子网掩码。用于IP中的32比特地址掩码，它表示用于子网地址的IP地址中的比特位。有时，它也称为 mask（掩码）。

Subnetwork: 子网。1、IP网络中，共享特定子网地址的网络。子网是网络管理员任意分段的网络，用以提供多级和分层路由选择结构，同时消除子网和其所连接网络的寻址复杂度。2、OSI网络中，ES和IS的集合。它受单一管理域的控制，使用的是单一网络访问协议。

Super Frame: 超帧。

SVC (Switched virtual circuit/switched virtual connection) : 交换虚电路。根据需求动态建立而在传输完成时加以拆卸的虚电路。SVC用于数据传输是随机的情况下。在ATM术语学中，它称为switched virtual connection（交换虚电路）。

Switch: 1、交换机过滤，转发和涌出基于每帧目的端地址的帧的网络设备。交换机工作在OSI模型的数据链路层。2、一种常用术语，用于描述允许按需建立连接并在无需会话支持时加以拆卸的电子设备或机械设备。

Synchronization: 同步。在发送端和接收端公共定时的建立。

附录一 名词解释（S）

Synchronous transmission: 同步传输。用于描述精确定时传输的数字信号的术语。这种信号具有相同的频率，封装在控制比特（叫start bits（开始比特）和stop bits（停止比特）中的字符表示字符的开始和结束。

附录一 名词解释 (T)

T1: 数字广域网承载设备。在电话-交换机网络中以DS-1格式传输1.544 Mbps的数据, 它使用AMI或者B8ZS编码。

T3: 数字广域网承载设备。在电话-交换机网络中以DS-3格式传输44.736 Mbps的数据。

TCP (Transmission Control Protocol): 传输控制协议。面向连接的传输层协议, 提供可靠的, 全双工数据传输。TCP是TCP/IP协议堆栈的一部分。

TCP/IP (Transmission Control Protocol/Internet Protocol): 传输控制协议/因特网协议。美国国防部在70年代开发的一套协议的通用名称, 支持全球互联网的结构。TCP和IP是这套协议中最著名的两个协议。

Telnet: 在TCP/IP协议堆栈中的标准终端仿真协议。Telnet用于远程终端连接, 使用户登录到一个远程系统, 就象连接到一个本地系统一样使用资源。

Terminal: 终端。通常有一个监视器和一个键盘, 但是没有处理器或者本地硬盘驱动器。数据可以进入, 或者从网络上获得数据的简单设备。

附录一 名词解释 (T)

Terminal adapter: 终端适配器。指的是连接ISDN BRI连接和现有EIA/TIA-232等接口的设备。一般指ISDN调制解调器。

Terminal emulation: 终端仿真。一种网络应用，即在一台计算机运行一个软件，使其在远程主机上看起来好象是直接附带的终端。

Terminal server: 终端服务器。指的是通信处理器，用于连接终端、打印机、主机和调制解调器等异步设备到任何使用TCP/IP协议，X.25协议或者LAT协议的本地网或者广域网。终端服务器提供连接设备不能获得的的网络互联智能。

Terminator: 终结器。是在传输线路终端提供电防护的设备，它吸收线路上的信号，从而防止回波反射和被网络工作站重复接收。

TFTP (Trivial File Transfer Protocol): 试用文件传输协议。FTP的简化版本，允许文件通过网络从一个计算机传输到另一个计算机。

Thinnet: 细电缆网。在IEEE 802.3 10Base2标准中用来定义一个廉价细电缆版本的规范术语。

Throughput: 吞吐量。指的是信息到达的和可能通过网络系统中一个特定点的比特率。

附录一 名词解释 (T)

TIA (Telecommunications Industry Association): 电信工业协会。开发电信技术相关标准的组织。TIA和EIA一道制定数据传输的电特性标准，比如EIA/TIA-232。

Time-out: 超时。指的是当网络设备想在一个特定时间内从另一个网络设备上收听信息，但是失败的情况。超时的结果通常是重新传输信息或者解除两个设备之间的会话。

Token: 令牌。指的是包含控制信息的帧。令牌过程允许网络设备向网络传输数据。

Token bus: 令牌环总线。是一种本地网结构，它在总线拓扑上使用令牌传递访问。这个本地网结构是IEEE 802.4本地网规范的基础。

Token passing: 令牌环传递。指的是网络设备用一种排序方式访问物理媒质的访问方法，该排序方式基于一个称为令牌的小帧处理。

Token Ring: 令牌环。IBM开发和支持的令牌-传递本地网。令牌环在环形拓扑上传输速率为4或者16 Mbps。与IEEE 802.5类似。

Topology: 拓扑。在网络结构中网络节点和媒质的物理分布。

TOS (Type of service): 服务类型。

附录一 名词解释（T）

Traffic shaping: 通信整形。它使用队列来限制可能引起网络拥塞的数据急增。数据被缓存之后，再以一个规定的数量向网络发送，这个规定数量保证业务流限定在特定连接承诺的业务外形之内。通信整形应用于ATM网络，帧中继网络和其它类型的网络。

Trailer: 报尾。为网络传输而封装数据时，附加给数据的控制信息。

Transceiver: 收发器。

Trap: 警报。SNMP（简单网络管理协议）代理发送给NMS，控制台或终端的消息，表明发生了重要事件，如达到了特殊定义的条件或门限。

Trunk: 干线。指的是两个ATM交换机之间的物理和逻辑连接，业务流通过该连接在ATM网络上传输。ATM骨干由大量干线组成。

TTL (Time To Live): 存活时间。IP报头里的域，指明一个数据包在多长时间之内被认为有效。

Tunneling: 隧道。旨在提供对任何标准点对点封装机制而必需的服务的结构体系。

附录一 名词解释 (T)

Twisted pair: 双绞线。指的是相对低速的传输介质，它由两根规则螺旋状的绝缘导线组成。传输线可以是屏蔽或非屏蔽的两种。双绞线在电话应用中很普及，而且在数据网络中也逐渐广泛应用。

附录一 名词解释（U）

UDP (User Datagram Protocol)：用户报文协议。TCP/IP协议站内无连接传输层协议。用户报文协议是一个简单的协议，在不确认和保证传送的前提下交换报文，至于差错处理和重发需要其他协议来处理。

Unicast：单播。指的是只发向一个网络目的地的消息。

Unicast address：单点广播地址。指明一个网络设备的地址。

UPS：不间断电源。旨在万一出现电源故障时提供不间断电源的后援设备。

URL (Universal Resource Locator)：通用资源定位器。用WWW浏览器访问超文本和其他服务时使用的标准地址编码方案。

UTP (Unshielded twisted-pair)：非屏蔽双绞线。指的是用于多种网络中的四对导线。非屏蔽双绞线不需要对于同轴电缆必需的连接间的固定距离。有五种常用的非屏蔽双绞线传输线：1类线、2类线、3类线, 4类线和 5类线。比较STP。

附录一 名词解释（V）

VC (Virtual circuit)：虚拟电路。建立以确保两个网络设备间可靠通信的逻辑电路。虚拟电路由一对VPI/VCI定义，而且可以是永久的（PVC）或者交换的（SVC）。虚拟电路在帧中继和X.25中使用。在ATM中，虚拟电路被称作virtual channel(虚拟信道)。

Vector：矢量。SNA报文的数据段。一个矢量由一个长度域，一个描述矢量类型的关键字和矢量特定数据组成。

VLAN (Virtual LAN)：虚拟局域网。局域网上的一组设备，经配置（用管理软件）后它们可以就如同连接在同一线路上那样进行通信，而实际上它们位于许多不同的局域网段。因为虚拟局域网基于逻辑而非物理连接，所以极为灵活。

VLSM (variable-length subnet mask)：变长子网掩码。能够为有相同网号的不同子网指定不同的子网掩码。变长子网掩码有助于优化可用的地址空间。

附录一 名词解释（W）

WAN：广域网。指的是能在很宽的地理区域内为用户服务的数据通信网络，此网络通常使用由公共设备商提供的传输设备。帧中继、SMDS和X.25都是广域网的例子。

Wildcard mask：通配符掩码。是与一个IP地址相关的32位比特量，用来决定当这个IP地址与另一个IP地址比较时，这个IP地址的哪些比特可以忽略。在建立接入表时，需指明网卡掩码。

WWW：万维网（World Wide Web）。指的是拥有因特网服务器的大型网络，为运行诸如WWW应用的客户终端提供超文本和其他服务。

附录一 名词解释（X）

X. 121: 指的是描述用于X. 25网络编址方案的ITU-T标准。X. 121地址有时亦称作IDNS（国际数据码）。

X. 21: 同步数字线上的串行通信ITU-T标准。X. 21协议主要用于欧洲和日本。

X. 25: 是一个ITU-T标准，它定义了PDN上如何维持DTE与DCE之间用于远程终端接入和计算机通信的连接。X. 25规定了一个数据链路层协议LAPB，和一个网络层协议PLP。帧中继在一定程度上已经取代了X. 25。

XNS: Xerox Network Systems。erox网络系统。是最初由PARC设计的协议组。许多PC网络公司，如3Com、Banyan、Novell和UB Networks等都曾经或正使用各种XNS作为他们的主要传输协议。

X Windows: MIT开发的分布式、网络透明、设备独立、多任务窗口技术和图形系统，它用于X终端与UNIX工作站之间的通信。

附录一 名词解释 (Num)

10Base2: 指的是使用50欧姆细同轴电缆的10-Mbps的基带以太网规范。它是IEEE 802.3规范的一部分, 在每个网段上的距离限制是185米。

10Base5: 指的是使用标准的(粗)50欧姆基带同轴电缆的10-Mbps的基带以太网规范。它是IEEE 802.3基带物理层规范的一部分, 在每个网段上的距离限制是500米。

10BaseF: 10-Mbps基带以太网规范, 是指光纤电缆连接上的以太网10BaseFB、10BaseFL和10BaseFP标准。

10BaseFB: 指的是使用光纤连接的10-Mbps基带以太网规范。它是IEEE 10BaseF规范的一部分。它不用于连接用户工作站, 而是用于提供一个同步的信令骨干网, 该网允许附加网段和中继器连接到网络上。10BaseFB的网段长度可达2000米。

10BaseFL: 指的是使用光纤连接的10-Mbps基带以太网规范。它是IEEE 10BaseL规范的一部分。尽管它可以与FOIRL进行互操作, 但是制定它是为了取代FOIRL规范。如果和FOIRL一起使用, 10BaseFL的网段长度可达1000米; 而如果仅仅使用10BaseFL, 则10BaseFL的网段长度可达2000米。

附录一 名词解释 (Num)

10BaseFP: 指的是使用光纤电缆连接的10-Mbps无源光纤基带以太网规范。它是IEEE 10BaseF规范的一部分。它在不使用中继器的情况下将多个计算机组织成星形拓扑。10BaseFP的网段长度可达500米。

10BaseT: 指的是使用两对双绞线电缆连接（第3、4、或5类电缆）的10-Mbps基带以太网规范。其中一对电缆用于发送数据；另一对电缆用于接收数据。它是IEEE 802.3规范的一部分，在每个网段上的距离限制大约是100米。

10Broad36: 指的是使用宽带同轴电缆的10-Mbps基带以太网规范。它是IEEE 802.3规范的一部分，在每个网段上的距离限制是3600米。

100BaseFX: 指的是在每个链路中使用两股多模光纤电缆的100-Mbps基带快速以太网规范。为了保证合适的信号计时，一个100BaseFX链路不能超过400米长。它基于IEEE 802.3标准。

100BaseT: 指的是使用非屏蔽双绞线接线的100-Mbps基带快速以太网规范。像它所基于的10BaseT技术一样，在网段上没有业务量时，100BaseT通过网段发送链接脉冲。然而这些链接脉冲所包含的信息多于10BaseT中使用的链接脉冲所包含的信息。

附录一 名词解释 (Num)

100BaseT4: 指的是使用四对(第3、第4、或第5类)非屏蔽双绞线接线的100-Mbps基带快速以太网规范。为了保证合适的信号定时,一个100BaseT4网段长度不能超过100米。它基于IEEE 802.3标准。

100BaseTX: 指的是使用两对非屏蔽双绞线接线或者屏蔽双绞线接线的100-Mbps基带快速以太网规范。其中第一对线路用于接收数据;第二对线路用于发送数据。为了保证合适的信号定时,一个100BaseTX网段长度不能超过100米。它基于IEEE 802.3标准。

100BaseX: 100-Mbps基带快速以太网规范,指的是在光纤电缆连接上的快速以太网100BaseFX 和 100BaseTX标准,基于IEEE 802.3标准。

100VG-AnyLAN: 指的是使用四对(第3、第4或第5类)非屏蔽双绞线电缆连接的100 Mbps快速以太网和令牌环介质技术。这种由Hewlett-Packard公司开发的高速传输技术基于IEEE 802.12标准,可以在现有的10BaseT以太网上使用。

24th channel signaling: 第24信道信令。

370 block mux channel: 370阻塞式复用信道。

附录二 CCNA考试介绍

考试注册

你需要提供以下注册资料：

身份证

电子邮件地址

邮寄地址

预约考试时间

CCNA的考试费用为125美金，不同的考场可能会按不同的汇率折算成人民币。如果您有折扣券，请提供给考场注册。

附录二 CCNA考试介绍

考试前调查

时间：15 分钟

形式：选择题、填空题

内容：学习资料、从业经历等

考场的考试管理员将协助您完成此项调查。

该项内容与您实际的考试无关。

附录二 CCNA考试介绍

例如：

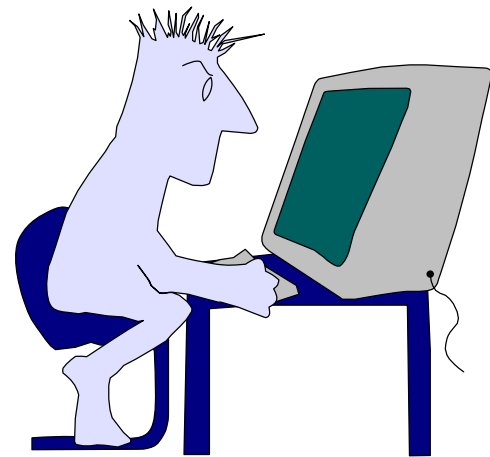
How long have you been installing, configuring, supporting or troubleshooting small to medium-sized multi-protocol enterprise networks on a daily basis?

- ☐ A. I have not worked with networks on a daily basis.
- ☐ B. less than 6 months
- ☐ C. 6 months to 18 months
- ☐ D. 18 months to 3 years
- ☐ E. 3 years to 5 years
- ☐ F. more than 5 years

附录二 CCNA考试介绍

正式考试开始前，您将能看到一个Flash模拟的考试过程，指导您如何正确操作，进行考试。

考试过程中遇到问题，如页面不能正常显示、死机等，请在座位上呼叫考试管理员请求帮助。



附录二 CCNA考试介绍

考试题型：选择题、拖曳题、实验题

试题总数：55道题左右。您可以在屏幕的右下方看到31/55的字样。表明您的总题量为55题，您现在正在做第31题。

推荐模考站点：<http://www.celticrover.com>

附录二 CCNA考试介绍

选择题包括单项选择、多项选择

单项选择题的选项为○

多项选择题的选项为□。并且，根据提示，您将知道该题需要选择几个选项。例如，题目会提醒您select the best或者choose three。

单选题例：

How do you express the binary number 11111000 in decimal?

- | | | |
|--------|--------|--------|
| A. 220 | B. 224 | C. 240 |
| D. 248 | E. 256 | |

附录二 CCNA考试介绍

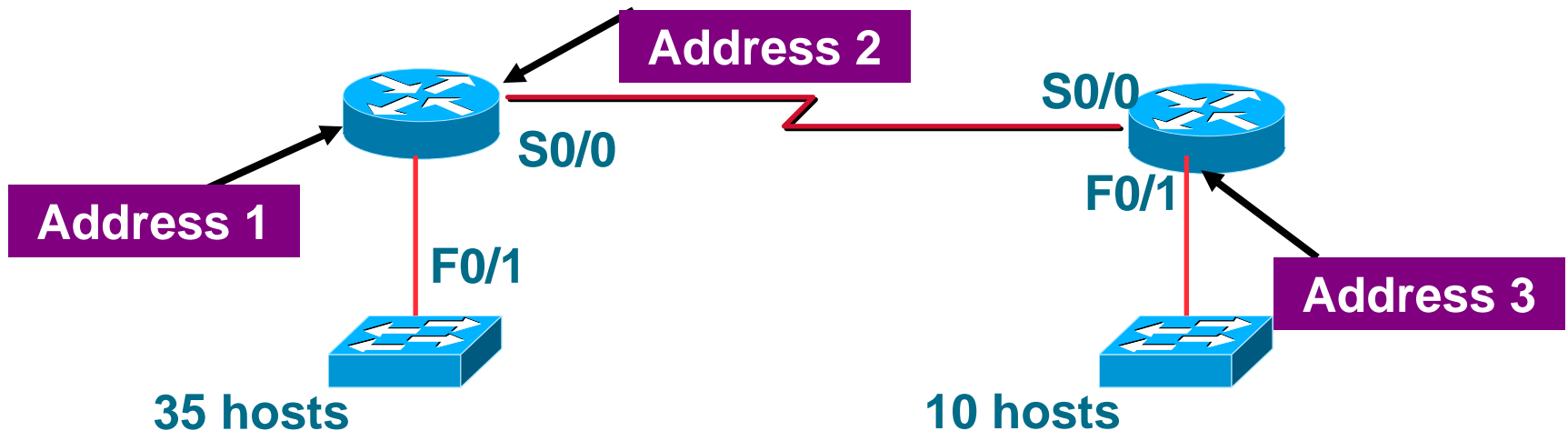
多选题例：

You have the binary number 10011101. Convert it to its decimal and hexadecimal equivalents. (Select two)

- | | | |
|--------|---------|---------|
| A. 158 | B. 0x9d | C. 156 |
| D. 157 | E. 0x19 | F. 0x9f |

附录二 CCNA考试介绍

拖曳题例



192.168.10.65/26

192.168.10.248/30

192.168.10.64/26

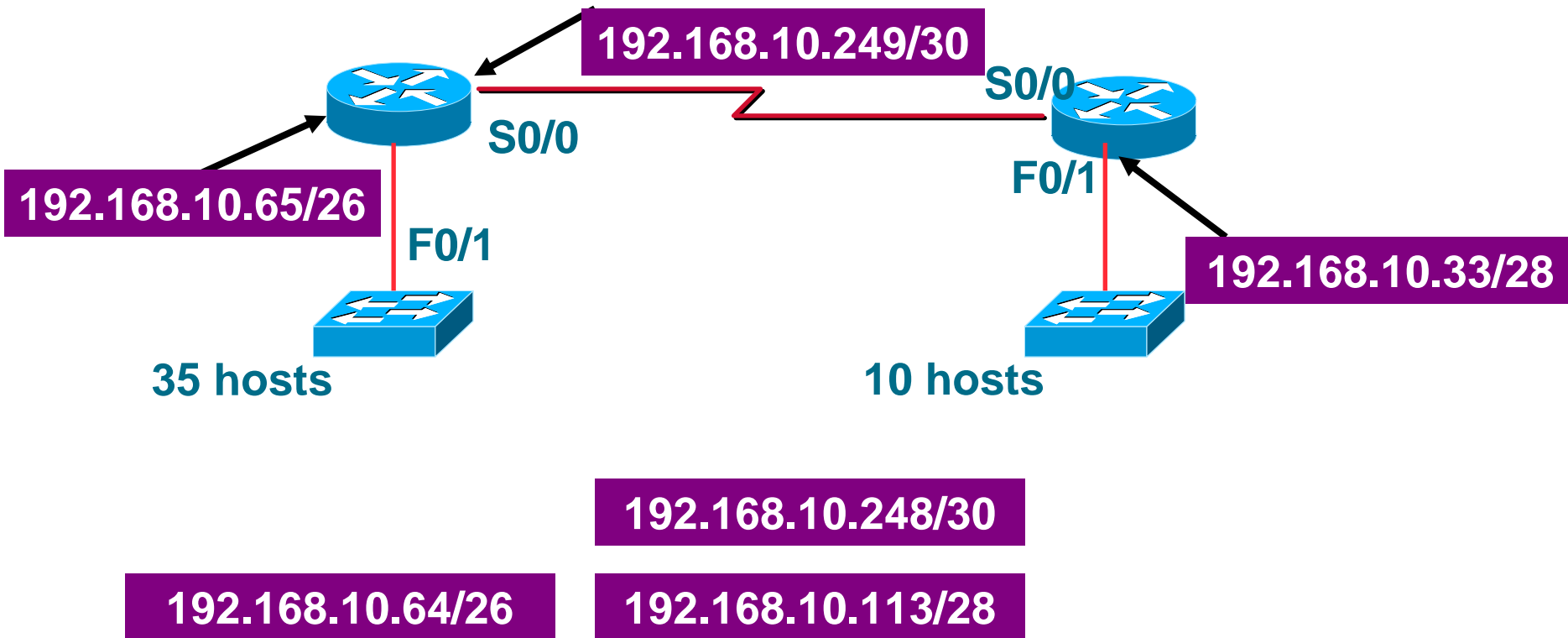
192.168.10.113/28

192.168.10.249/30

192.168.10.33/28

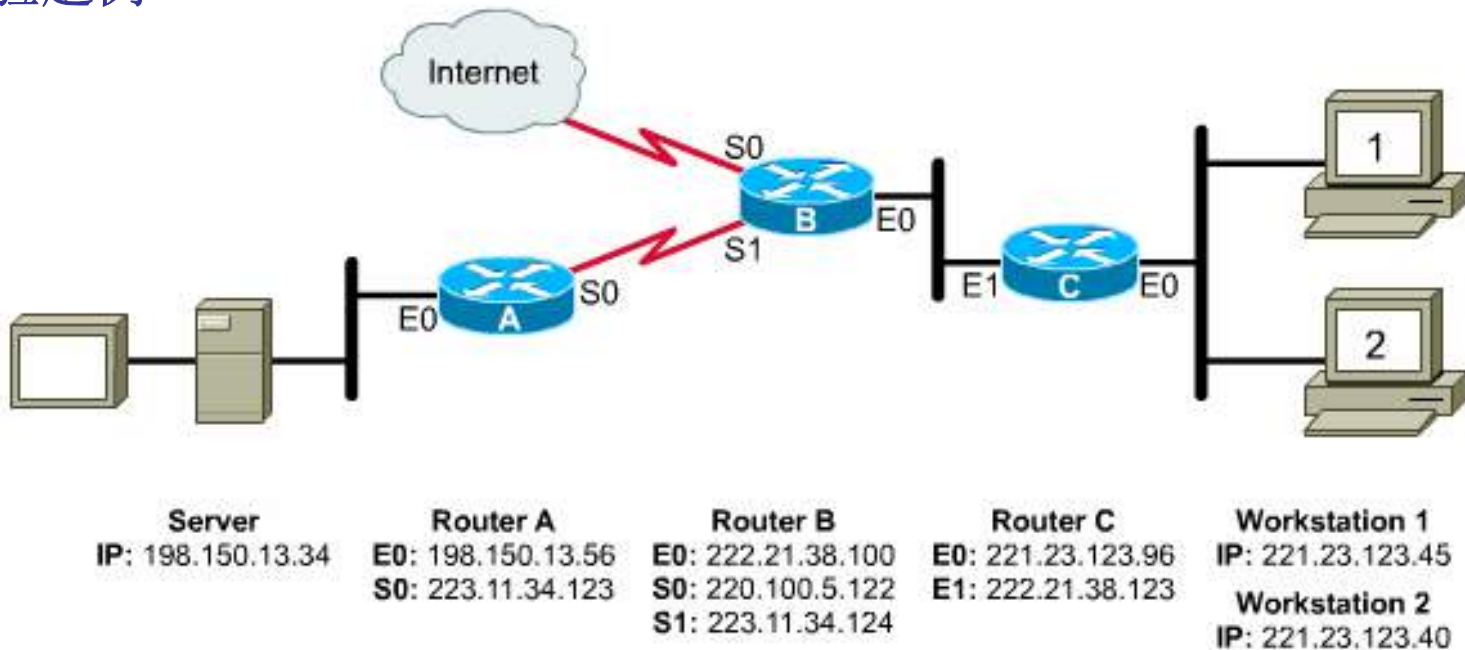
附录二 CCNA考试介绍

拖曳题例



附录二 CCNA考试介绍

实验题例



实验题将要求完成某个网络，或对现有网络进行排错。

Which router will it
be entered into?

Select Router

Select Port

Which router port
will it be on?

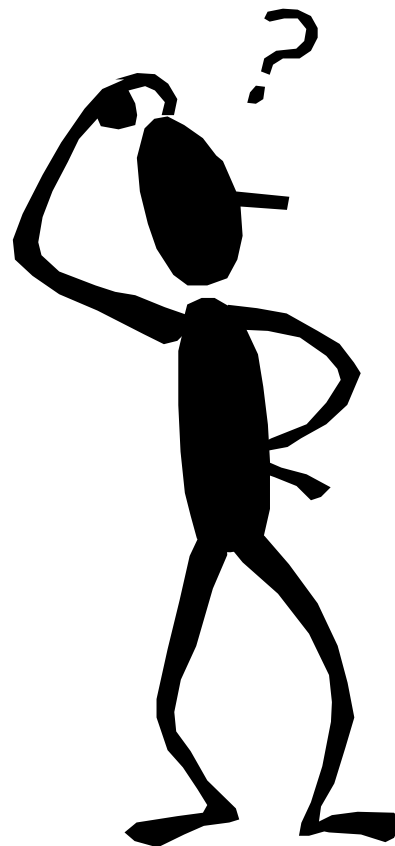
附录二 CCNA考试介绍

考试建议

用答题板（向考试管理员索取）绘出简单拓扑图，记下相关要点，如IP地址、协议、网络、接口等相关信息。

答题完毕后，用ping、show等相关命令检测配置结果。

对于实验题，尤其注意保存配置。



附录二 CCNA考试介绍

时间：90 +30 分钟

正常考试时间是90分钟。

对于母语非英文的国家，考试延长了30分钟。

如果您没有及时完成考试，系统会自动提交。

倒计时，您将在屏幕的右上角看到您所剩余的时间。



附录二 CCNA考试介绍

考试特点：有进无退

考试只能向前进，不能回退，请慎重对待，核实每一道题正确无误后点击“Next”。



附录二 CCNA考试介绍

考试结束后，点击屏幕右下角的“End Exam”即可提交考试。
随后，考试系统将打印出您的考试成绩单，以及各项的正确率。
CCNA考试的通过成绩为849，满分1000。
您将能看到如下的结果：

Congratulations!!!

附录二 CCNA考试介绍

在您的考试成绩单将会有两个ID:

Registration ID:123456789

Validation ID:123456789

您可以到如下网站进行验证, 同时获取您的CISCO ID:

<https://www.pearsonvue.com/authenticate>

附录二 CCNA考试介绍



December 28, 2005

- Test Taker Services
- Test Program Information
- Test Delivery Solutions
- Become a Test Center
- Purchase Vouchers
- About Us
- Contact

SIGN IN

[Forgot your password or username?](#)
[Create an Account](#)

[Home](#) | [Schedule a Test](#) | [Locate a Test Center](#) | [FAQs](#) 

Authenticate Score Report

This page allows you to verify that a score report from the Pearson VUE Testing System is authentic. You will find the registration number and the validation number on the score report.

Registration Number:

Validation Number:

AUTHENTICATE



スコアレポート確認



Enter your Registration and Validation Numbers above to
Get your first 30 days FREE!

附录二 CCNA考试介绍

到思科官方网站:

<https://i7lp.integral7.com/durango/do/login?ownername=cisco&channel=cisco&basechannel=integral7>

Cisco Systems

Search

Products & Services | Ordering | Technical Support & Documentation | Learning & Events | Partners & Resellers | About Cisco

HOME
LEARNING AND EVENTS
CAREER CERTIFICATIONS AND PATHS
CERTIFICATION RESOURCES
CERTIFICATION TRACKING SYSTEM
About Certification Tracking System
Certification Tracking System Tool

Career Certifications & Paths
Certification Tracking System

Welcome to the Cisco Career Certifications Tracking System!

Register for the first time
If you are using the Tracking System for the very first time, you will need to set up a password for future access. Please [click here](#) to set up your password.

Existing users sign in here:

Test ID* or Cisco Certification ID (CSCOID):

Password:

Passwords are case-sensitive.

* Your Cisco ID can be found on your exam score report. This is not the same as your Cisco.com login ID.

[Forgot Cisco ID, or password?](#) [Help logging in](#)

Related Tools
[CCIE Verification](#)
[Certifications Online Support](#)
[Partner Help Online](#)

Related Links
[Recertification](#)
[CCIE](#)
[Cisco Certification](#)

Discover the value of certifications
[More Information](#)

初次用户点击此处

附录二 CCNA考试介绍



Create Web Login

First Name

Your name

Last Name

Registration ID

Your registration id


Instructions


- Enter the information in the above fields and click on "submit"
- **NOTE:** ALL of the above fields are required
- The above information can be found on any of your Cisco exam score reports.
- If you do NOT have a Cisco score report, please contact the test delivery provider that you used to take your exam. They will mail a copy of your score report to you:
 - **Pearson VUE** in US/Canada at: 1.877.404.EXAM to request a copy. All other locations please go to www.vue.com/cisco

Submit

在接下来的页面里设置您的密码。

附录二 CCNA考试介绍



Search 

Products & Services | Ordering | Technical Support & Documentation | Learning & Events | Partners & Resellers | About Cisco

HOME

LEARNING AND EVENTS

CAREER CERTIFICATIONS AND PATHS

CERTIFICATION RESOURCES

CERTIFICATION TRACKING SYSTEM

About Certification Tracking System

Certification Tracking System Tool

Career Certifications & Paths

Certification Tracking System

Welcome to the Cisco Career Certifications Tracking System!

Register for the first time
If you are using the Tracking System for the very first time, you will need to set up a password for future access. Please [click here](#) to set up your password.

Existing users sign in here:

Test ID* or
Cisco Certification ID
(CSCCID)

* Your Cisco ID can be found on
your exam score report. This is
not the same as your Cisco.com
login ID.

Password:

Passwords are case-sensitive.

[Forgot Cisco ID or password?](#) [Help logging in](#)

Related Tools

[CCIE Verification](#)

[Certifications Online Support](#)


[Partner Help Online](#)

Related Links

[Recertification](#)


[CCIE](#)

[Cisco Certifications Community](#)


[More Information](#)

以您的**CISCO ID**以及您的密码登录。

附录二 CCNA考试介绍



Logout

[Logout](#)

Home

[Personal Information](#)

[Update Personal Info](#)

[Change Password](#)

Help

[FAQ](#)

[Contact Us](#)

Personal Information

Jianhua Hu - CSC011212886

Candidate Record

Initially, and every 180 days, we like to verify your demographic information. Please verify your information or use the Update Personal Info link to the left to make the appropriate changes. Once verified, you may access the other areas of the site.

General Information

Verify that name is as it should appear on certificate.

First Name	San	ID Name	ID	Last Updated
Middle Name		VUE ID	12345678	07/28/2007
Last Name	Zhang	PROMETRIC ID	12345678	07/28/2007
Birth Date		Cisco ID	CSC012345678	07/28/2007
Company Name	No			

Addresses

Preferred Mailing Address	Mailing Address	Edit Shipping Label
		Delete Shipping Label
Mailing Address	NO.1 Chang An Street	
City	BeiJing	
State/Province	100001	
Postal Code		
Country	CHINA	

修改您的个人信息，包括信箱、中英文地址、联系电话等等。

修改密码

结语

最后，祝大家通过自己的努力，能够学到有用的知识，实现自己的梦想和人生价值。

谢谢！