计算机网络

高等教育出版社

作者：吴国新、吉逸

东南大学计算机学院

编者的话：

本课件强调原理性的介绍，即使一些技术目前已不处于主导地位。之所以这样做，理由很简单，我们教授的是计算机网络的课程，我们的学生在“知其然”的同时，更应知道“其所以然”，即使是一项被淘汰的技术，也应知道淘汰的理由；更何况从原理上说，没有被淘汰的原理，只有不同的适用场所。

另一方面，我们也许正处于一个新名词层出不穷的时代，又有谁能够给出这些新生名词的精确定义？何况许多新名词是张冠李戴，一个帽子而已。

当然，我们也承认课件（包括教材）只能起着“入门”的作用，还需要读者（尤其是教师）去增添新的内容。

我们相信课件中存在许多不尽如意的地方，请读者及时指正。

感谢高等教育出版社为我们搭建了一个相互沟通的平台。

编者（**gwu@seu.edu.cn)**

2008年3月20日

计算机网络

主要内容：

★计算机网络基础知识（原理性知识）

★局域网（常用的局域网技术）

★广域网（常用的广域网组网技术）

★网络互连（网络互连技术，互连设备）

★Internet（Internet技术，TCP/IP的原理与应用）

★网络管理、网络安全

★网络工程设计

目的：了解网络技术的原理和现状。

方式：授课为主，辅以实验和作业。

第1章 计算机网络概述

1.1 网络的发展

计算机网络：计算机的网络（组成）

计算机网络：用于计算机之间通信的网络（应用）

计算机网络 = 计算机技术和通信技术相互渗透和发展的结晶，并在用户需求刺激下发展起来的技术。

计算机网络发展过程：

1946年，ENICA在宾夕法尼亚大学（美）诞生，占地170平米，重30吨，18000个电子管，5000次加法/秒。

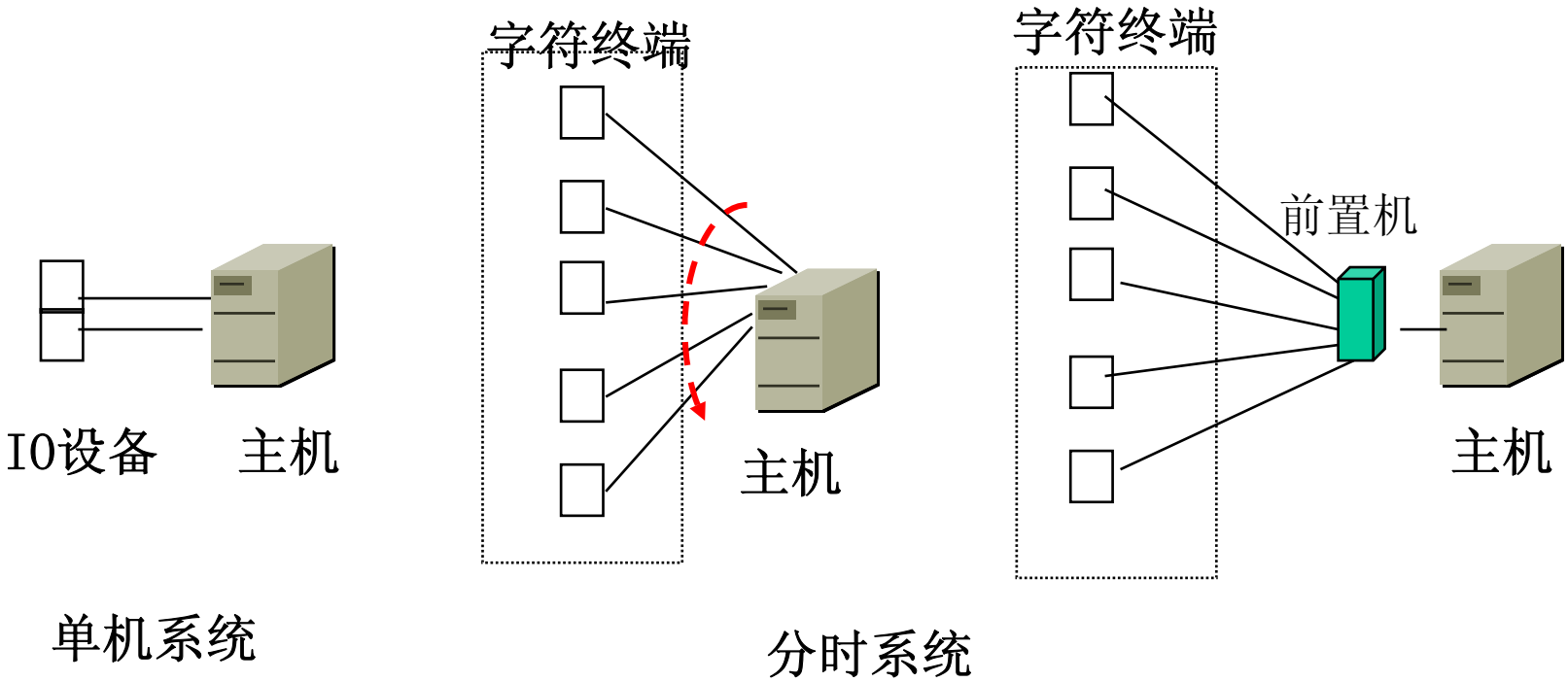
硬件发展：电子管—晶体管—中小规模集成电路—大规模集成电路—（智能机）

软件发展：单用户OS—分时多用户OS—网络OS—分布式OS—

网络的发展

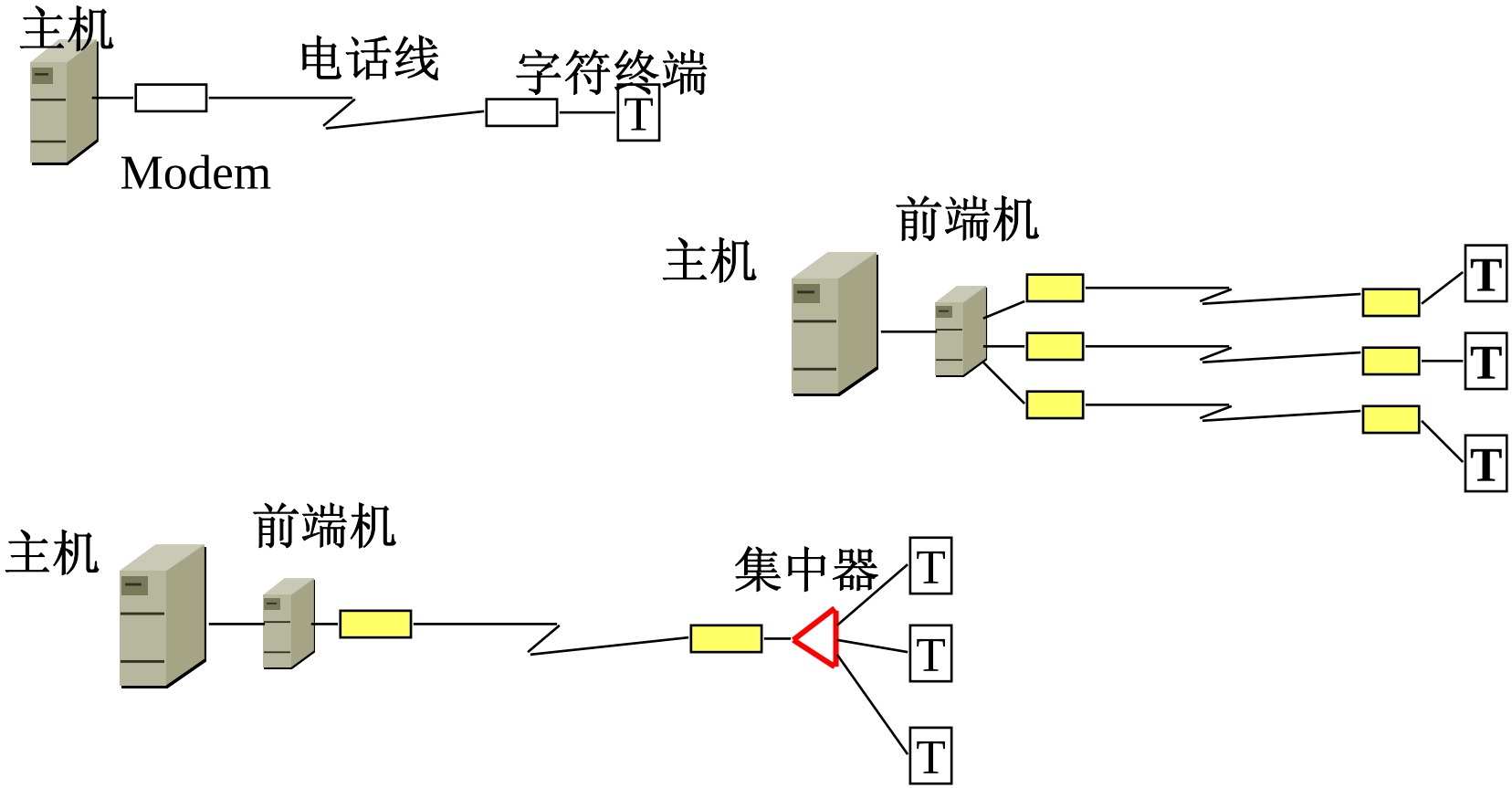
单机： 单个用户独占系统资源（主机）(46年)

分时系统： 分时多用户系统（大型机） (50年代末期)
多个用户利用多台终端共享单台计算机的资源，
主机轮询终端，获取指令，提供服务，返回结果



网络的发展

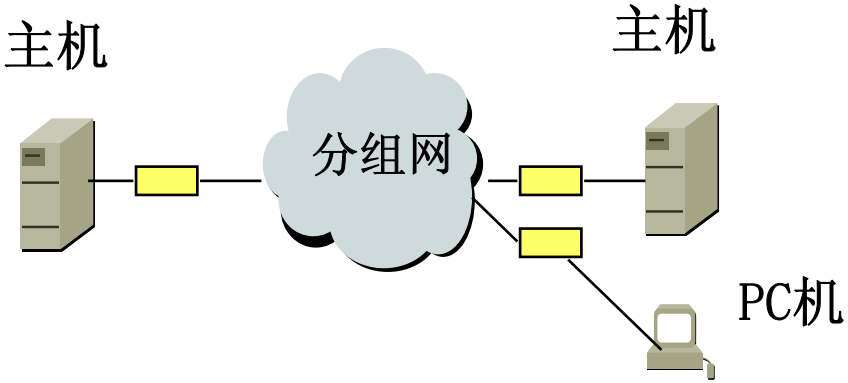
*远程访问系统：*利用通信线路将远程终端连至主机，不受地域限制地使用计算机的资源　(60年代中后期)

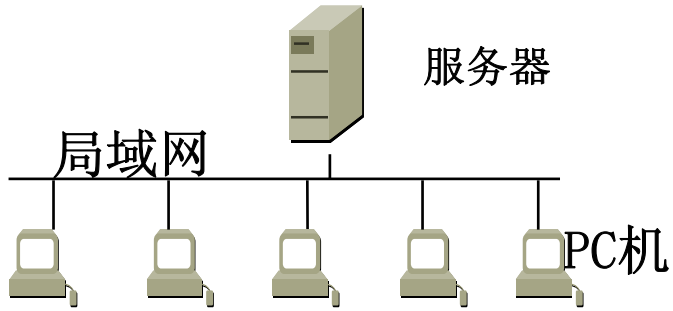


网络的发展

网络： 将多台计算机连在一起，相互共享资源

1968年，世界上第一个计算机网络 ARPANET 诞生



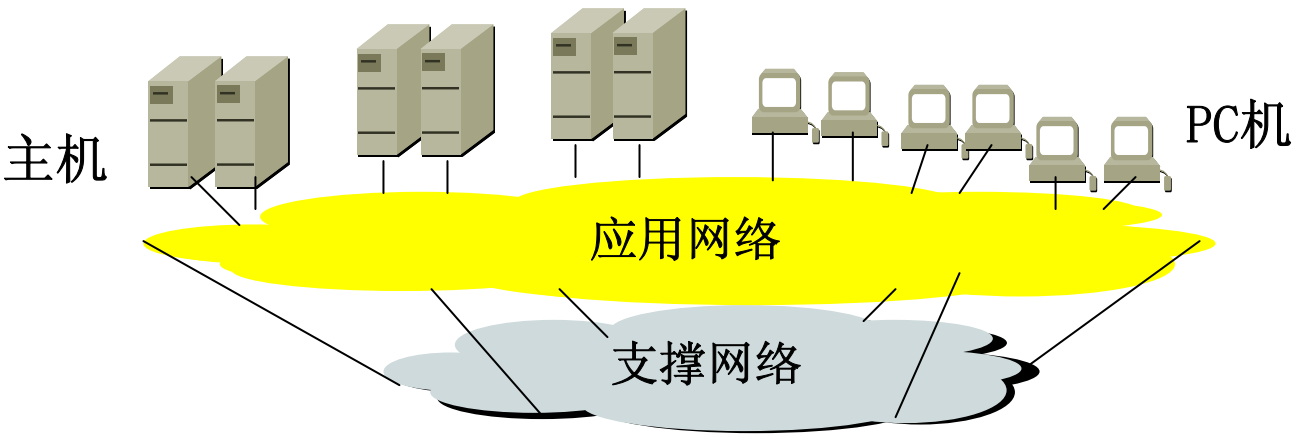


全球网络（国际互联网）： (90年代)

网络的发展

*覆盖网：*面向应用的网络（在支撑网络的基础上增添组件，使其满足各类应用需求）— 21世纪初期

典型系统：以信息资源共享为目的的网格；以闲散资源共享为目标的对等网（P2P网）



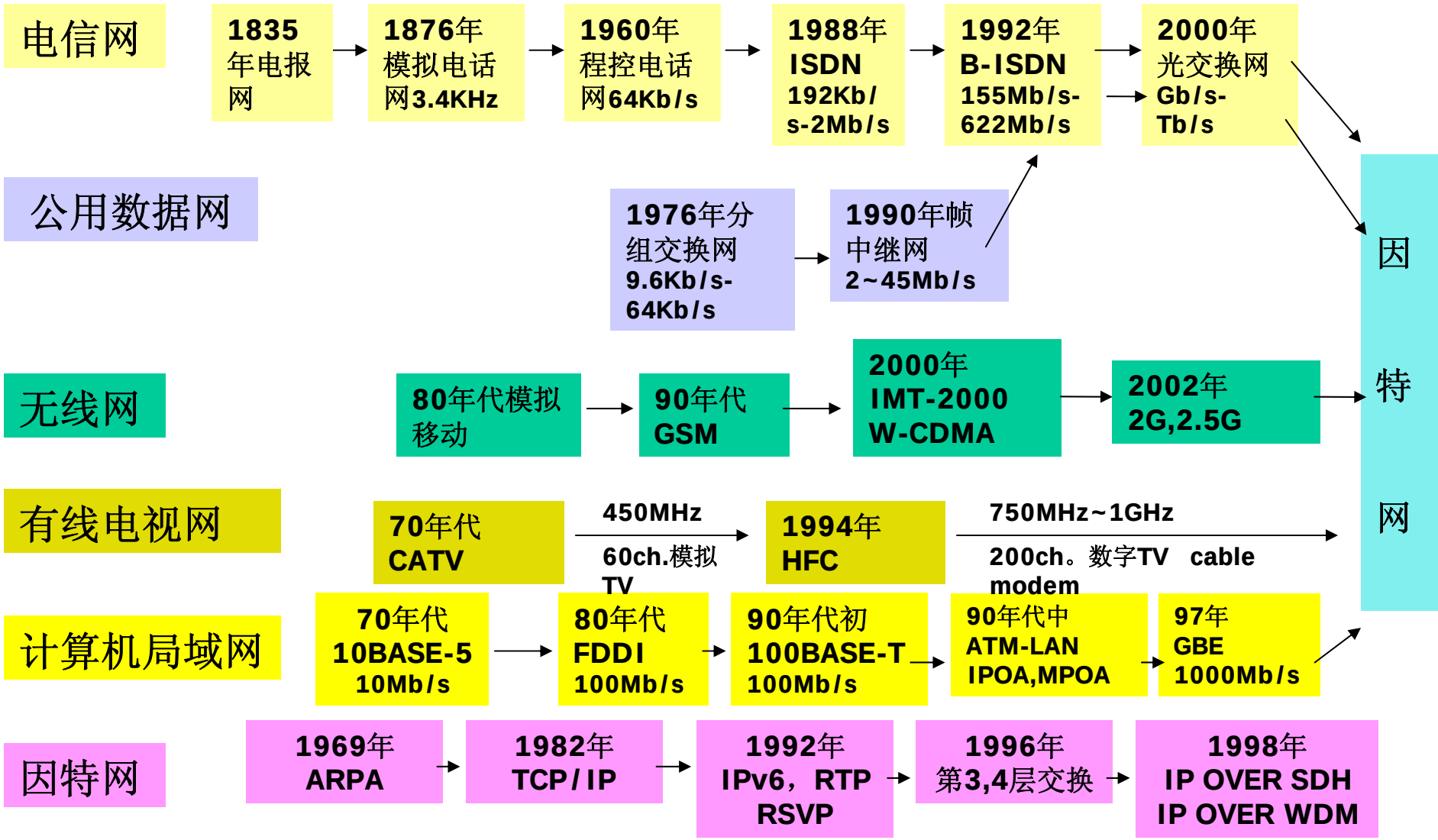
网络的发展—研究角度

70年代，网络协议，（异构）计算机之间通信和互联，
追求网络的（地域）覆盖面；

90年代，网络应用，满足各类应用需求，
追求网络的（行业）覆盖面，无所不在；

本世纪，网络服务，向用户提供满意的、高质量的服务，
以人为本，享受网络。

网络发展示意图


电信网
1835年电报网
1876年模拟电话网3.4KHz
1960年程控电话网64Kb/s
1988年ISDN 192Kb/s-2Mb/s
1992年B-ISDN 155Mb/s-622Mb/s
2000年光交换网 Gb/s-Tb/s
公用数据网
1976年分组交换网 9.6Kb/s-64Kb/s
1990年帧中继网 2~45Mb/s
无线网
80年代模拟移动
90年代GSM
2000年IMT-2000 W-CDMA
2002年2G,2.5G
有线电视网
70年代CATV
450MHz
60ch.模拟TV
1994年HFC
750MHz~1GHz
200ch。数字TV cable modem
计算机局域网
70年代10BASE-5 10Mb/s
80年代FDDI 100Mb/s
90年代初100BASE-T 100Mb/s
90年代中ATM-LAN IPOA,MPOA
97年GBE 1000Mb/s
因特网
1969年ARPA
1982年TCP/IP
1992年IPv6，RTP RSVP
1996年第3,4层交换
1998年IP OVER SDH IP OVER WDM
因特网

计算机网络的定义：

计算机网络是以*共享资源*（硬件、软件和信息等）为目的而连接起来的、*在协议控制下*，由一台或多台计算机、终端设备、数据传输设备等组成的系统之集合。

这些计算机系统应当具有*独立自治*的能力，是可以独立运行的系统。

网络的功能

计算机联网的主要目的—跨越时空：

– 资源共享

硬件共享：大型计算机的处理能力，昂贵的外设；

软件共享：应用软件、系统软件等；

信息共享：用户数据（市场信息）等。

– 数据传输

支持用户之间的数据传输（如电子邮件，IP电话等）；

计算机网络和信息社会

信息社会的特征：信息具有价值；

信息的特点：时效性；

计算机：信息处理的最佳工具；

计算机网络：具有高速的信息传输能力，充分发挥计算机处理的效率，是信息社会得以快速发展的支撑技术；

90年代，美国提出建立信息高速公路（国家信息基础设施—NII），构建贯通全美各大学、研究机构、企业及家庭的全国性网络。全球响应—GII，我国倡导的各项上网工程，网络渗透各行各业，生活中密不可分的一部分。

计算机网络和信息社会

网络对社会的影响：

- 人民生活丰富多彩
  - 工业化社会——物质享受，信息化社会——精神享受
- 经济生活日益变化
  - 产业结构的变革，新兴产业
- 社会功能不断充实
  - 网络世界需要新的法律、法规予以维护
- 国际间合作更加密切
  - “地球村”

网络的类型

★ 根据网络覆盖范围分类

广域网(Wide Area Network--WAN)

局域网(Local Area Network--LAN)

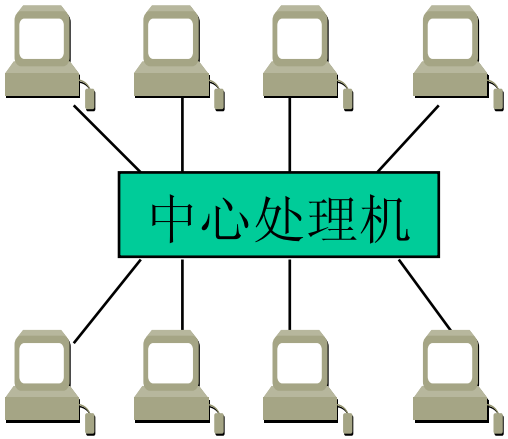
城域网(Metropolitan Area Network--MAN)

园区网(Campus Network/Enterprise Network)

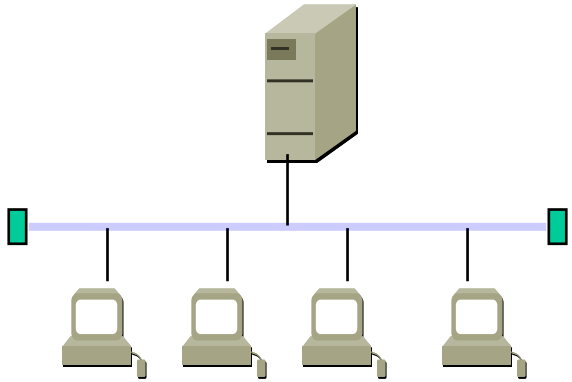
覆盖整个企业，淡化覆盖范围的概念。

不同覆盖范围的网络采用了不同的技术，应用的普及导致范围的淡化，目前习惯用对应的技术来划分网络类型。

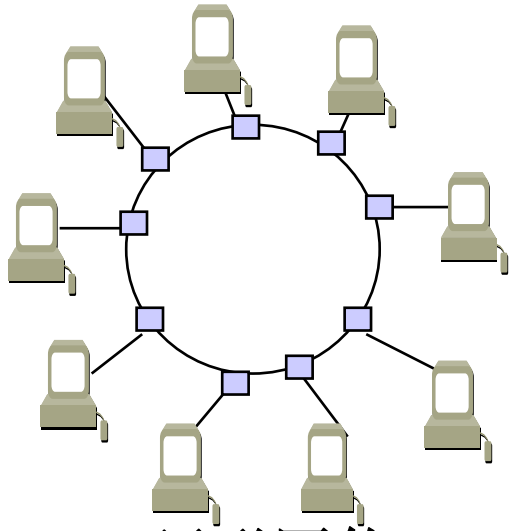
★根据网络拓扑结构分类—依赖线缆铺设



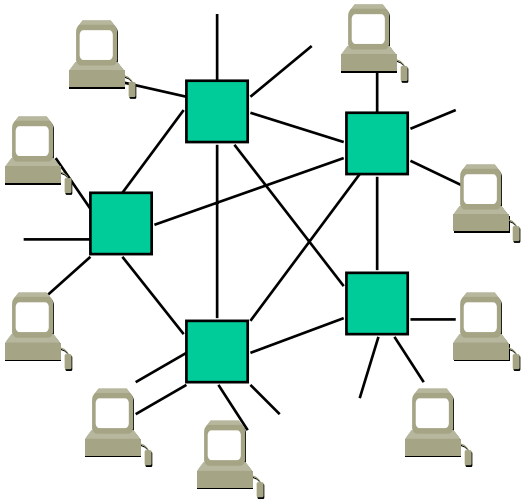
星形网络



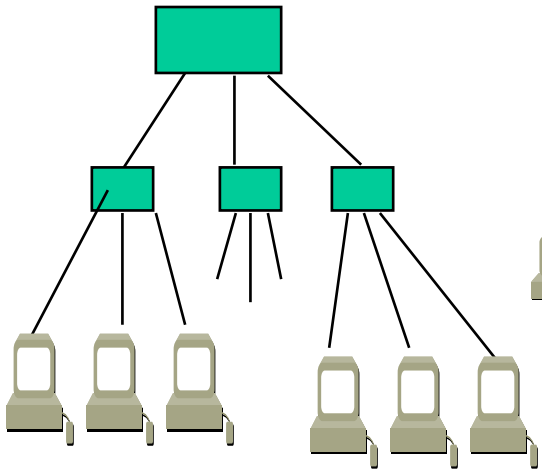
总线网络



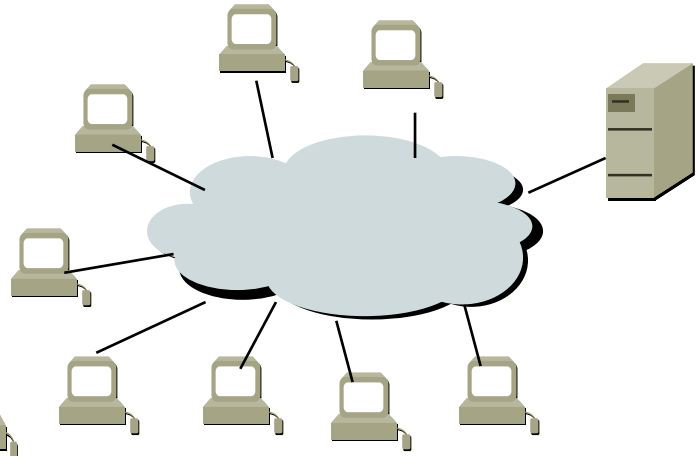
环形网络



网状网络



物理星型网络



逻辑星型网络

★根据管理性质分类

公用网 ：资源可供任何人使用

电话网、公共数据网、DDN等

专用网 ：资源仅供有限对象使用

国家安全网、军事网、气象网、电力网等

利用公用网组建专用网—虚拟专用网（VPN）

金融网，教育网，政府网等

互联网 （Internet—因特网）

内联网 （Intranet，如企业内联网）

外联网 （Extranet，如企业外联网）

★根据交换方式分类

（信息在网络设备（交换机）中的转移方式）

电路交换网 ：类电话交换系统

报文交换网 ：基于存储转发，报文体积不限；

分组交换网 ：基于存储转发，分组体积限制。

目前所有的计算机网络均采用分组交换技术，但因环境不同，分组体积不同。

★根据功能分类—逻辑划分

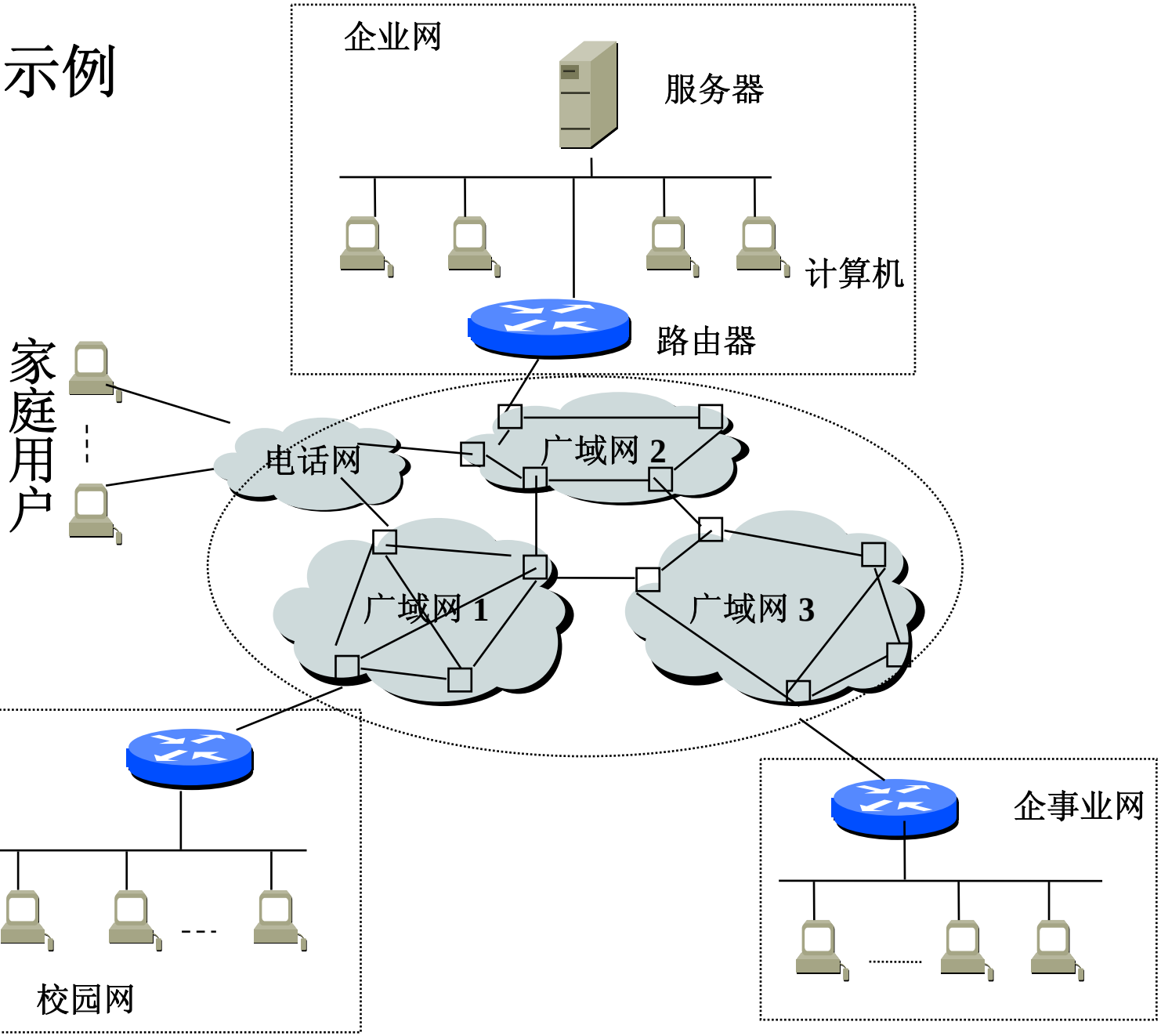
通信子网：支持数据传输或通信的部分资源集合；

如电信部门提供的通信网络；

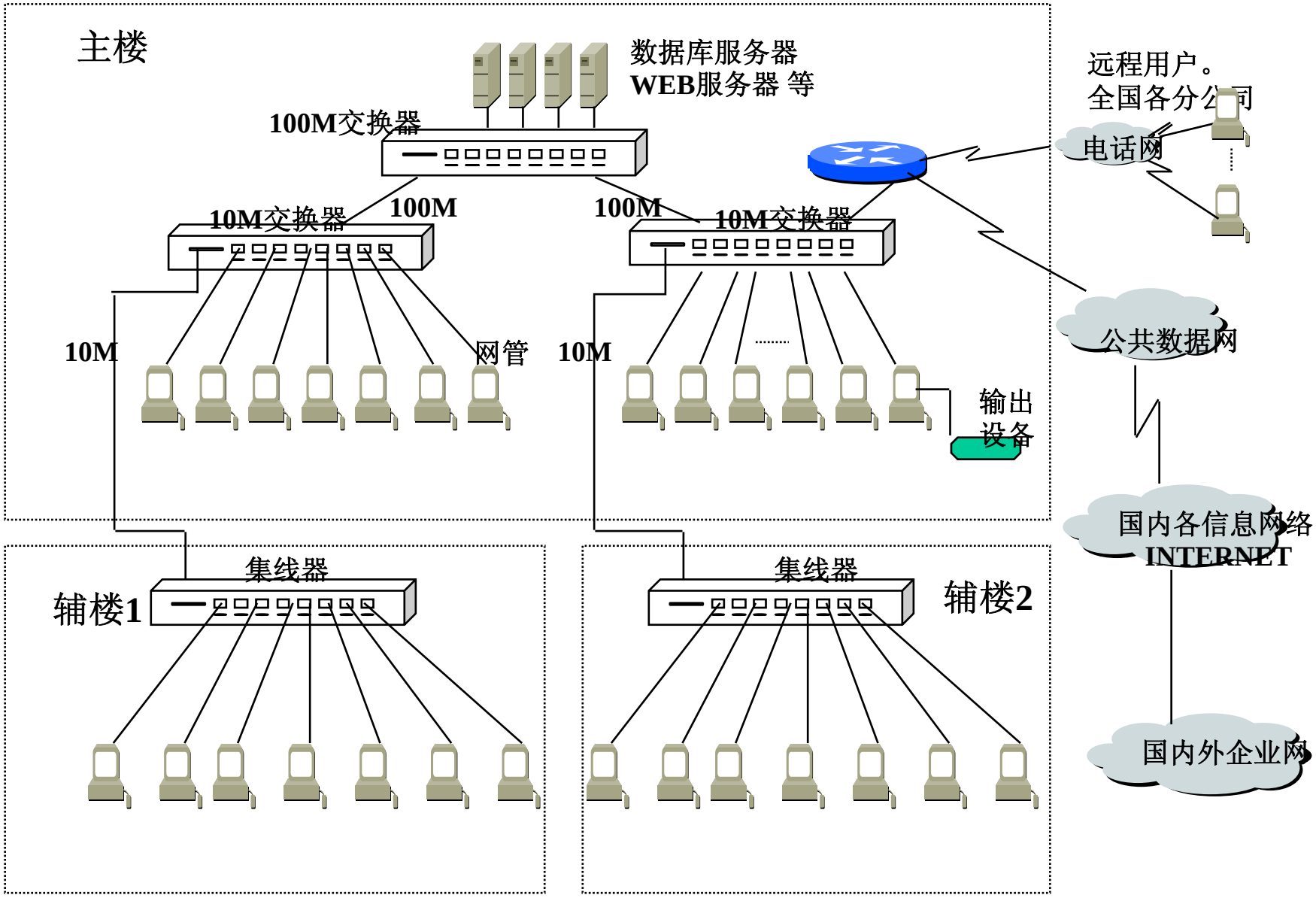
资源子网：支持数据处理的部分资源集合；

如用户端设施。

网络示例



企业网示例

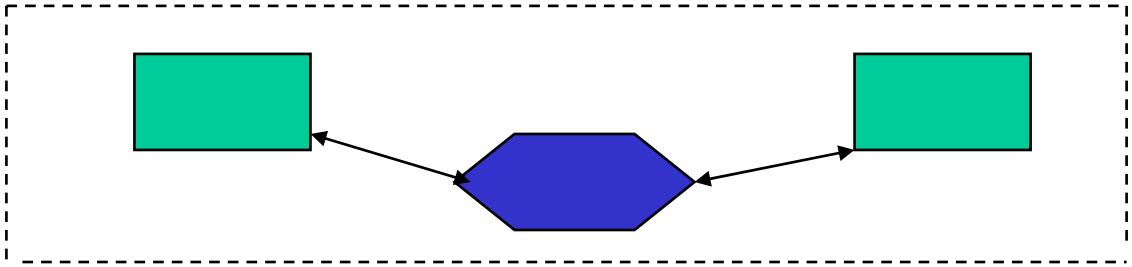

主楼
数据库服务器
WEB服务器 等
100M交换器
远程用户。
全国各分公司
电话网
10M交换器
100M
100M
10M交换器
10M
网管
10M
输出
设备
公共数据网
国内各信息网络
INTERNET
集线器
辅楼1
集线器
辅楼2
国内外企业网

计算机通信的基本原理

☆ 计算机通信的实质：进程（线程）间通信

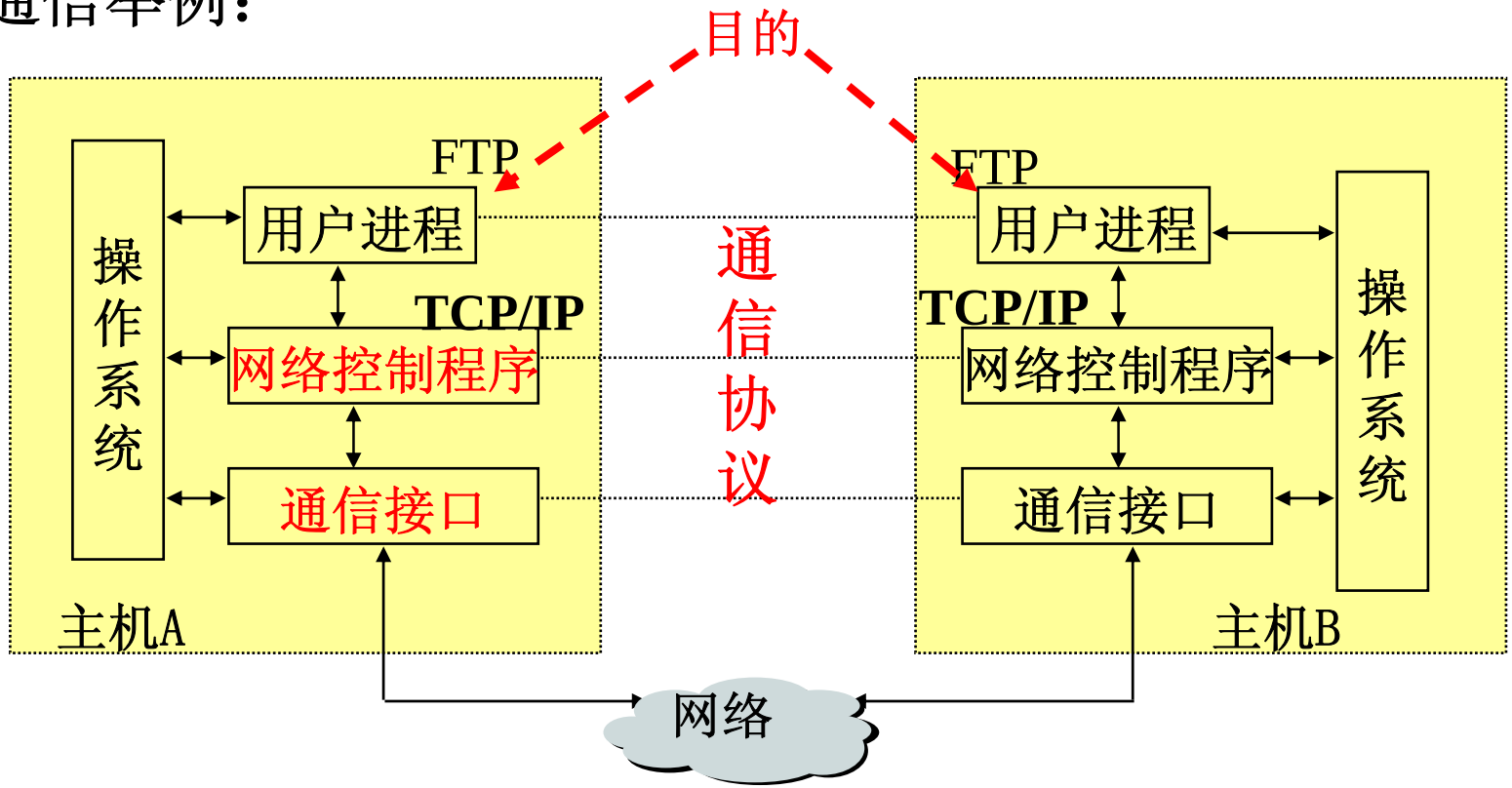
各进程间相互制约的等待或互通消息

同一系统：共享内存、缓冲区、文件等



不同系统：通过网络进行通信，利用线路和中继设备的传输/存储/处理能力

通信举例：



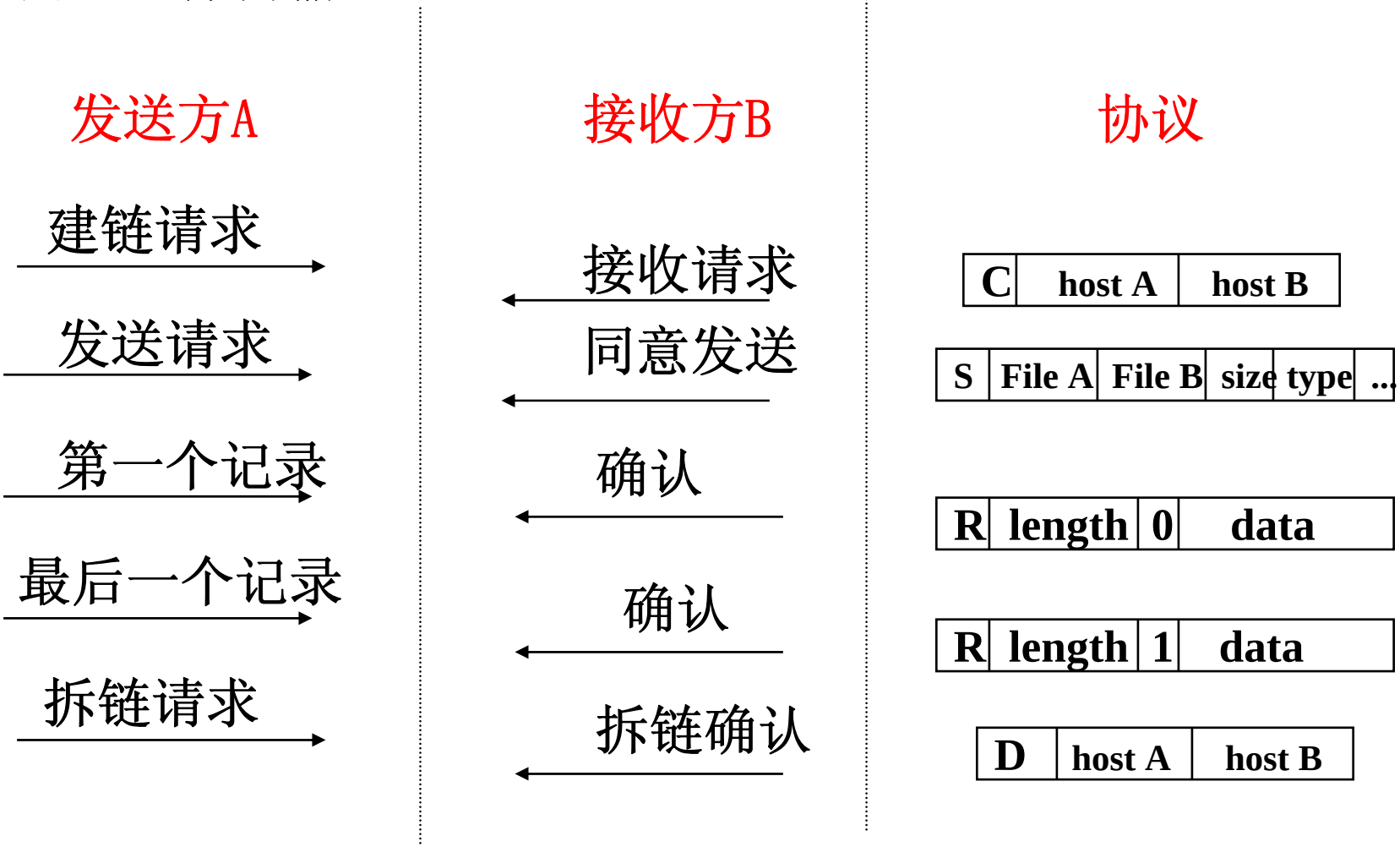
★网络控制程序（NCP）：调度网络资源使用情况；

★通信接口：设备和部件之间的衔接；

★用户进程：提供用户应用服务；

★通信协议：约定通信双方交互的格式（语法）、内容（语义）和时序，由**NCP**执行。

例：文件传输

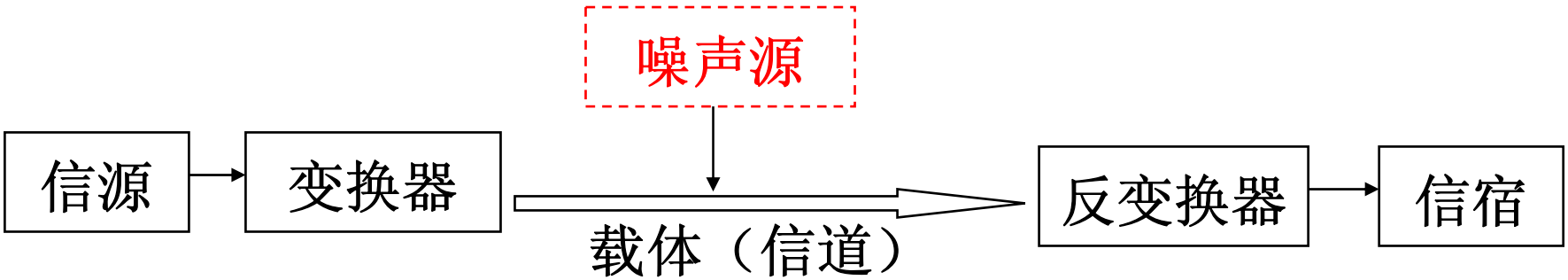


遵循协议是计算机之间得以正确通信的保障！

是计算机网络研究的重点。

第2章 数据通信原理

通信系统的基本组成：



载体：信息的传送通道；

信源：信息的发出者；

信宿：信息的接收者；

变换器：将信息变换成载体上可传输的信号；

反变换器：将载体上传输的信号变换成信宿可识别的信息；

噪声：干扰信号。

2.2 载体（信道）

载体：承载信息/信号的媒体；

信道：信息单向传输通道(二线)，含传输媒体和中继通信设施；

传输媒体类型划分—形式：

- 有线信道：双绞线/缆、同轴电缆、光纤/缆等，能量集中导线附近；
- 无线信道：自由空间，红外、微波等，能量向空间发散。

双绞线/缆：以电磁波形式传输电气信号；

—无屏蔽双绞线（**Unshielded Twisted Pair—UTP**）

—屏蔽双绞线（**Shielded Twisted Pair—STP**）

2.2 载体（信道）

载体： 承载信息/信号的媒体；

信道： 信息单向传输通道(二线)，含传输媒体和中继通信设施；

传输媒体类型划分—形式：

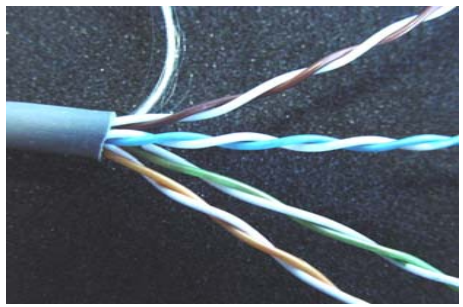
- 有线信道：双绞线/缆、同轴电缆、光纤/缆等，能量集中导线附近；
- 无线信道：自由空间，红外、微波等，能量向空间发散。

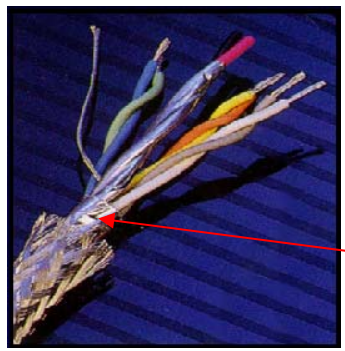
双绞线/缆：以电磁波形式传输电气信号；

—无屏蔽双绞线（**Unshielded Twisted Pair—UTP**）

—屏蔽双绞线（**Shielded Twisted Pair—STP**）

UTP





STP

金属屏蔽层

2.2 载体（信道）

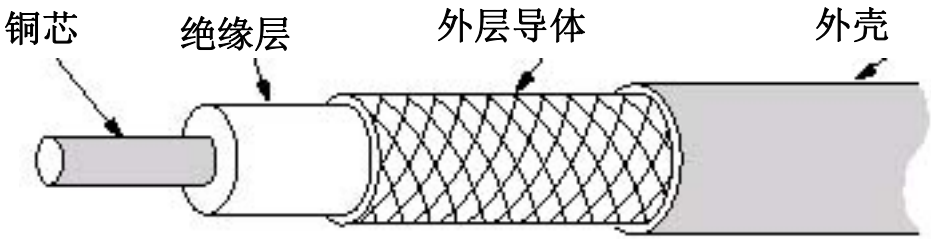
载体： 承载信息/信号的媒体；

信道： 信息单向传输通道(二线)，含传输媒体和中继通信设施；

传输媒体类型划分—形式：

- 有线信道：双绞线/缆、同轴电缆、光纤/缆等，能量集中导线附近；
- 无线信道：自由空间，红外、微波等，能量向空间发散。

同轴电缆：以电磁波形式传输信号；



2.2 载体（信道）

载体： 承载信息/信号的媒体；

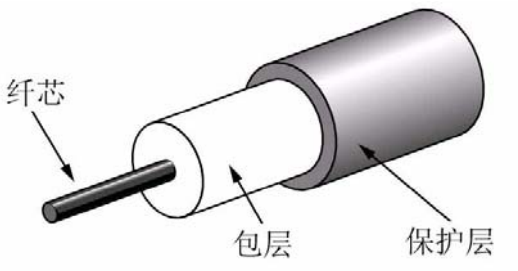
信道： 信息单向传输通道(二线)，含传输媒体和中继通信设施；

传输媒体类型划分—形式：

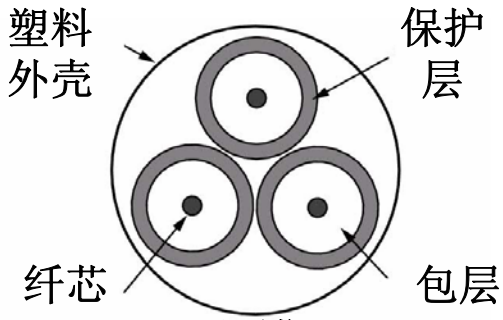
- 有线信道：双绞线/缆、同轴电缆、光纤/缆等，能量集中导线附近；
- 无线信道：自由空间，红外、微波等，能量向空间发散。

光纤/缆：以光波形式传输信号；

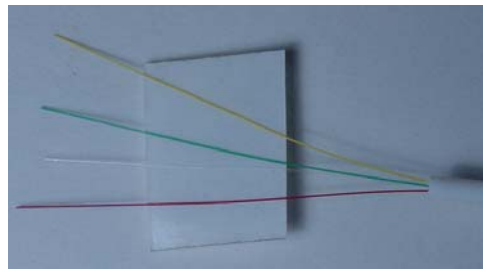
由传导光波的高纯石英玻璃纤维和保护层构成，纤芯的折射率大于包层折射率，保证光信号在纤芯内折射传输。多根光纤封装于外壳中，形成多芯光缆。



光纤



光缆


实际光纤/缆

2.2 载体（信道）

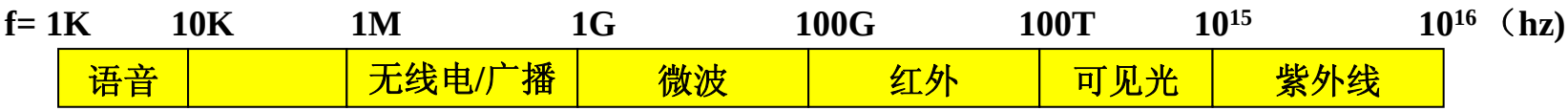
载体： 承载信息/信号的媒体；

信道： 信息单向传输通道(二线)，含传输媒体和中继通信设施；

传输媒体类型划分—形式：

- 有线信道：双绞线/缆、同轴电缆、光纤/缆等，能量集中导线附近；
- 无线信道：自由空间，红外、微波等，能量向空间发散。

无线信道：以无线电频率（射频—**RF**）形式传输信号；



低频**LF**、中频**MF**波段电波沿地表传播；
高频**HF**和甚高频**VHF**波段电波通过电离层反射实现长距离传输；
红外线与毫米波传输：不能穿透障碍物，适用于室内
微波传输：能量集中，天线必须对准。
激光传输：不能穿透雨或浓雾。

2.2 载体（信道）

载体：承载信息/信号的媒体；

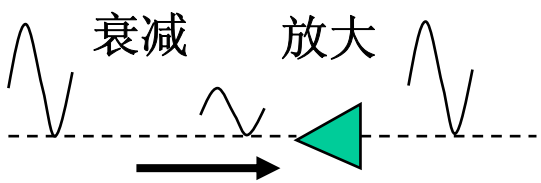
信道：信息单向传输通道(二线)，含传输媒体和中继通信设施；

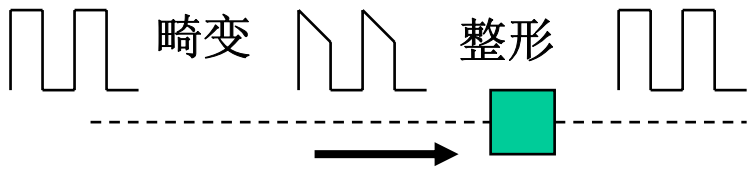
传输媒体类型划分—方式：

- 模拟信道：支持模拟信号传输，如双绞线、同轴电缆等；
- 数字信道：支持数字信号传输，如光纤、双绞线等；

注1：计算机仅能产生数字信号，处理信息；

2：阻抗导致信号衰减，线间电容导致信号畸变，长距离传输时必须放大（补充能量）和整形。





信道带宽与信道容量（信道的物理特性）

信道带宽：　信道可以不失真地传输信号的频率范围；

信道带宽取决于信道的质量，设计信道的指标。

信道容量：　信道在单位时间内可以传输的最大信号量

数据传输速率(bps)：

信道在单位时间内可以传输的最大比特数；

信道容量和信道带宽成正比：带宽越大，容量越大

局域网：10Mbps，100Mbps，千兆bps，10千兆

广域网：64Kbps、2Mbps、155Mbps、622Mbps

2.5Gbps,…

信道的差错率/误码率

由于噪声的影响和信道带宽的限制，

信号在传输过程中可能发生失真

差错率/误码率：传输比特总数与其中出错比特数的比值；

Pe = 出错比特数传输/比特总数

例： 传输10000比特，有2比特出错，

Pe = 2/10000

差错率越高表示信道的质量越差

信道的差错率与信道质量密切相关；

也与信号的传输速率和传输距离成正比。

类似的有：误分组率等；

2.3 变换器/反变换器—调制/解调与编码/解码

模拟传输系统：模拟信道构成的传输系统，如电话网、X.25分组交换网等；

数字传输系统：数字信道构成的传输系统，如宽带ISDN等

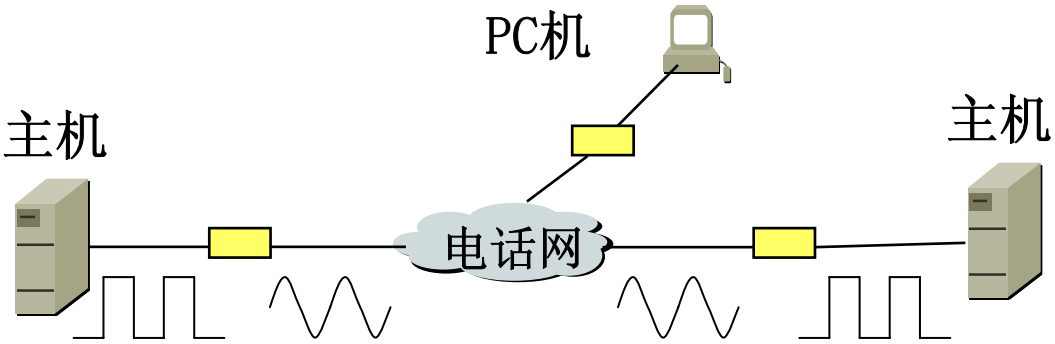
★ 调制/解调：利用模拟信道支持数据信息传输的技术

调制：将数据信息变换成适合于模拟信道上传输的电磁波（载波）信号/码元，（数字-->模拟）

解调：将从模拟信道上收取的载波信号还原成数据信息。（模拟-->数字）

调制解调器：

具有调制/解调功能的通信设备。

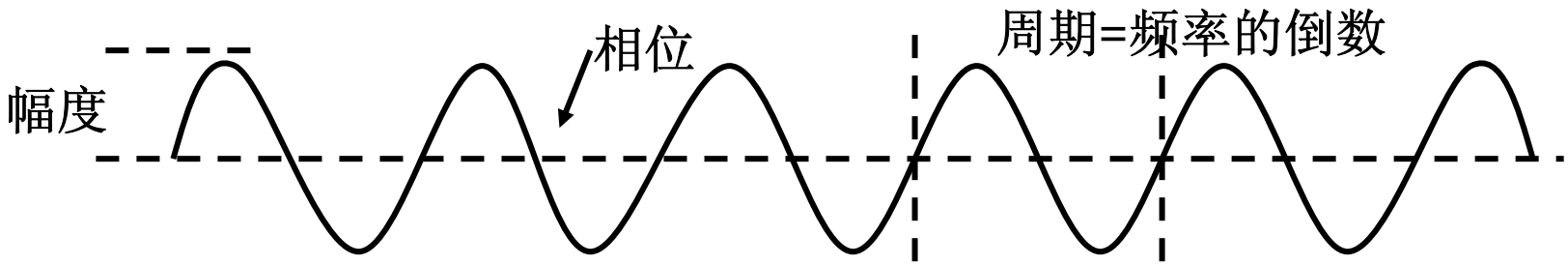


★调制方法—调制依据

1、任何周期为T的函数g(t)都可以展开为Fourier级数（n次谐波叠加），即模拟信号可由三角函数表示

$$g(t)=\frac{1}{2}c+\sum_{n=1}^{\infty}a_n\sin(2\pi nft)+\sum_{n=1}^{\infty}b_n\cos(2\pi nft)$$

2、模拟信号可由三个要素（幅度、频率和相位）予以定义



调制：三个要素的调制。

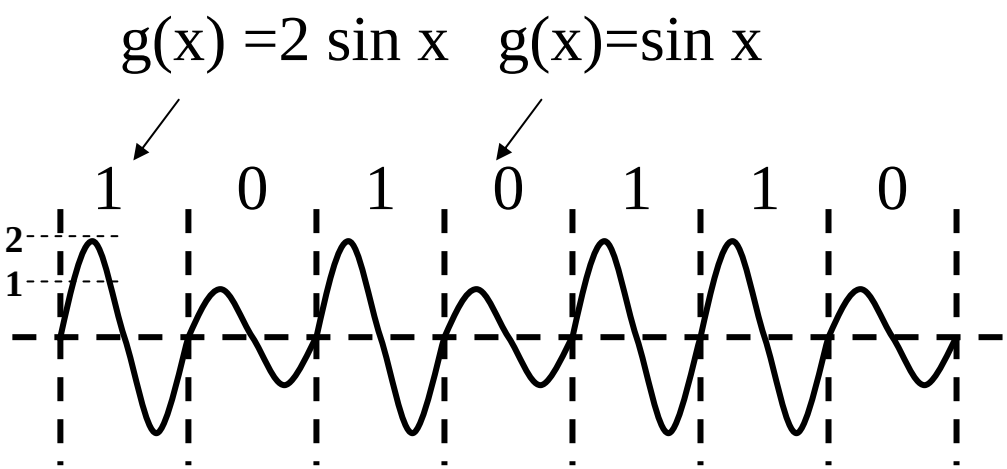
★调制方法：

调幅：（幅度调制或移幅键控法ASK）：

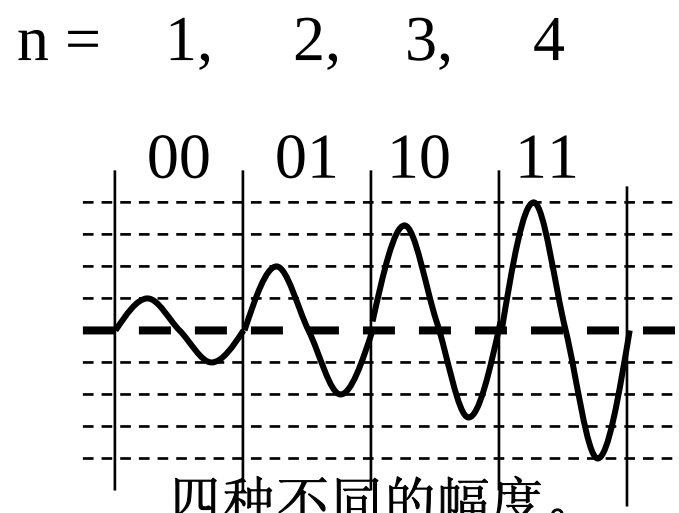
将不同的数据信息（0和1）调制成不同幅度

但*相同频率*的载波信号；

g(x) = n*sin(x)，不同n产生不同幅度的载波信号。



两种不同的幅度。



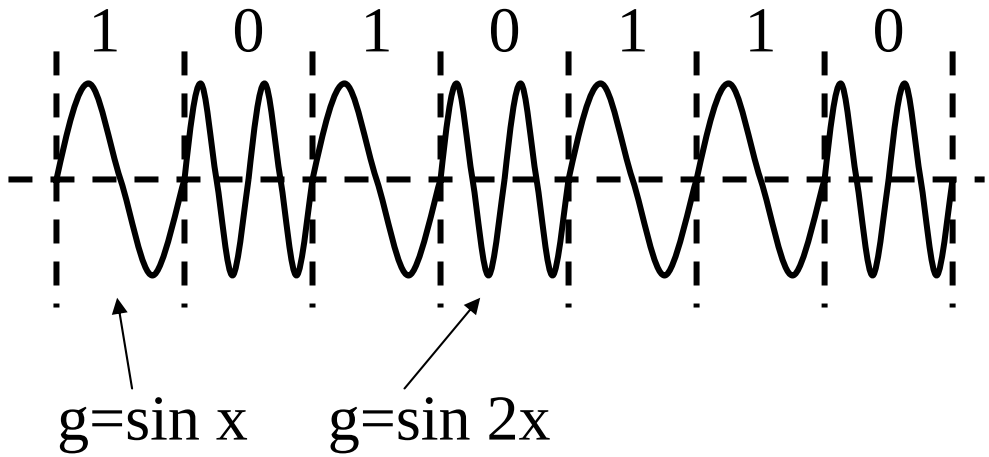
四种不同的幅度。

★调制方法

调频：（频率调制或移频键控法FSK）：

将不同的数据信息（0和1）调制为*相同幅度*，但*不同频率*的载波信号；

g(x) = sin(n*x) 不同n产生不同频率的载波信号



本例仅采用两种不同的频率。

★调制方法

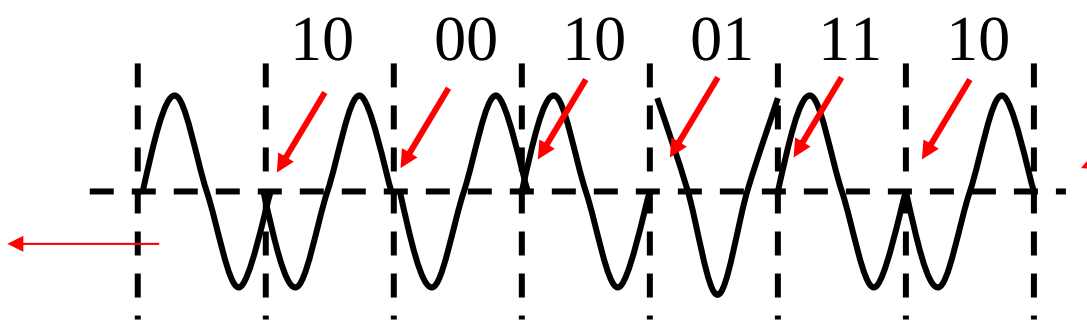
调相：（相位调制或移相键控法PSK）：

利用相邻载波信号的*相位变化*值来表示相邻信号是否具有相同的数据信息值，此时的幅度和频率均不发生变化；

例如：**0**—相位变化**180**度，**1**—相位不变化；
或者：**00**—不变化，**01**—**90**度，**10**—**180**度，**11**—**270**度；

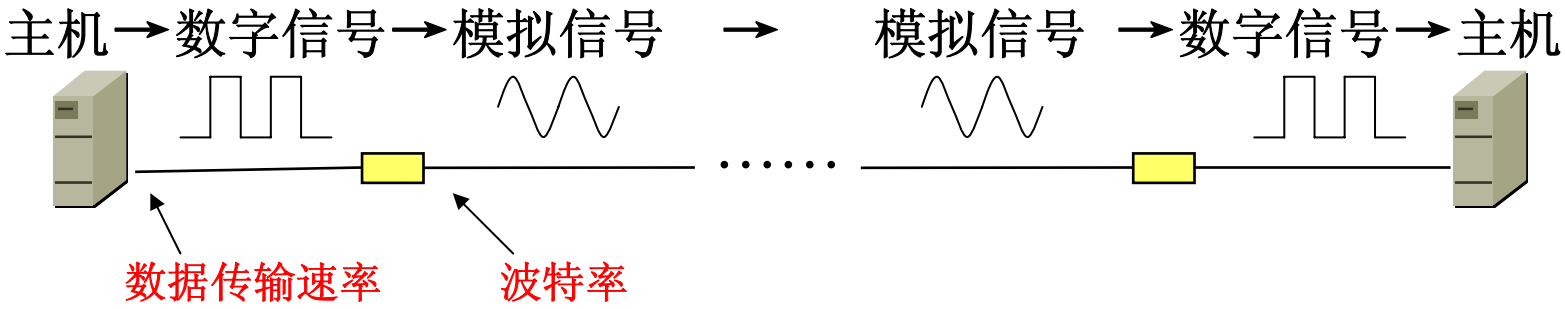
g(x) = sin(n+x) 不同**n**产生相位变化不同的载波信号

相位变化：　π　**0**　π　$\frac{\pi}{2}$　$\frac{3\pi}{2}$　π



位串**1000100 11110**对应的载波信号

调制/解调的结果



调制设备负责将主机端的数字信号调制成可在模拟信道上传输的模拟信号（符号/码元）。

调制设备的性能影响信号调制的速率，数据传输速率。

调制速率（信道速率，或者波特率）：调制设备每秒可调制的符号/码元个数，即信道上每秒传输的符号个数。

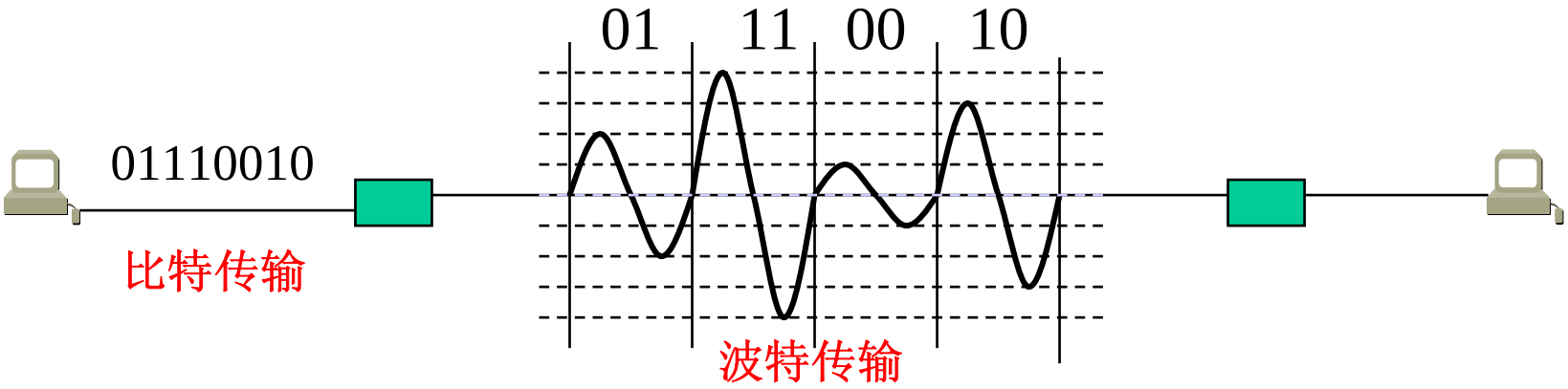
数据传输速率： 信道在单位时间内可以传输的最大比特数

★ 波特率和数据传输速率之间的关系

如果调制设备的调制速率（波特率）为 M，调制出的每个码元具有 N 种取值（线路的状态数），则有：

$$\text{数据传输速率} = M \times \log_2 N = \text{波特率} \times \log_2 N$$

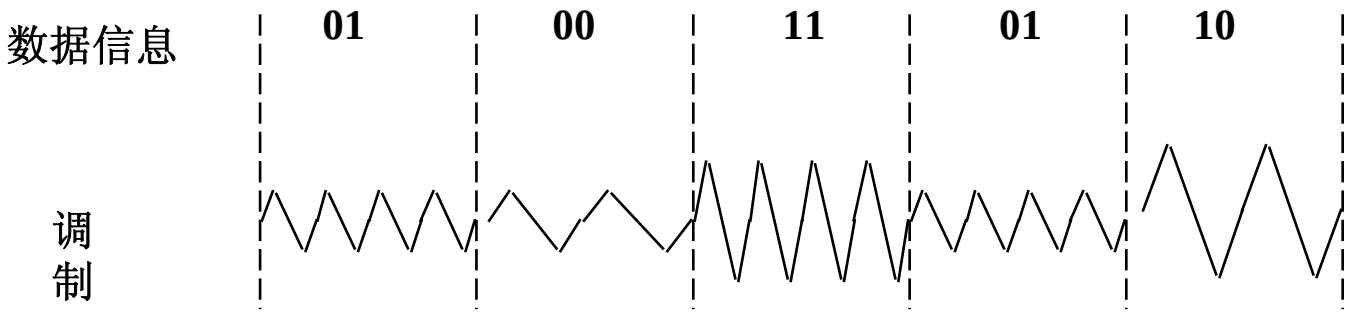
假设调制设备采用调幅调制技术，每秒调制出一个码元，该码元可取四种幅度之一：



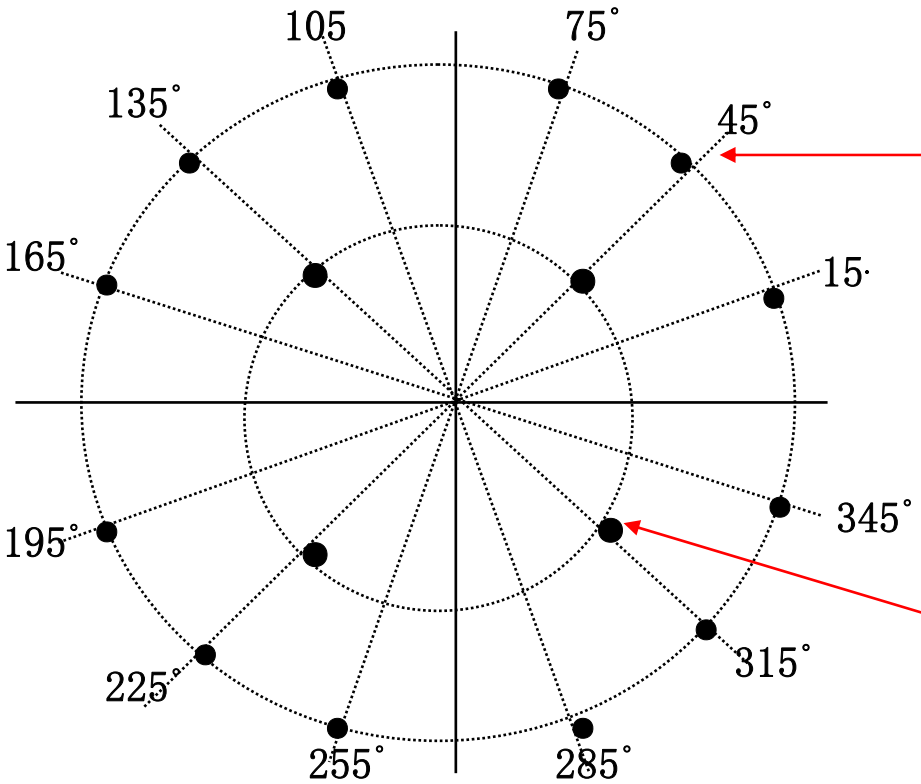
波特率：1码元/秒；　　数据传输速率：2位/秒

组合调制—提高数据传输速率

幅度+频率
（2倍速）



相位+幅度
（4倍速）



高幅相位45度

低幅相位315度

★调制/解调器的选择和应用

1)性能：速率、功能等

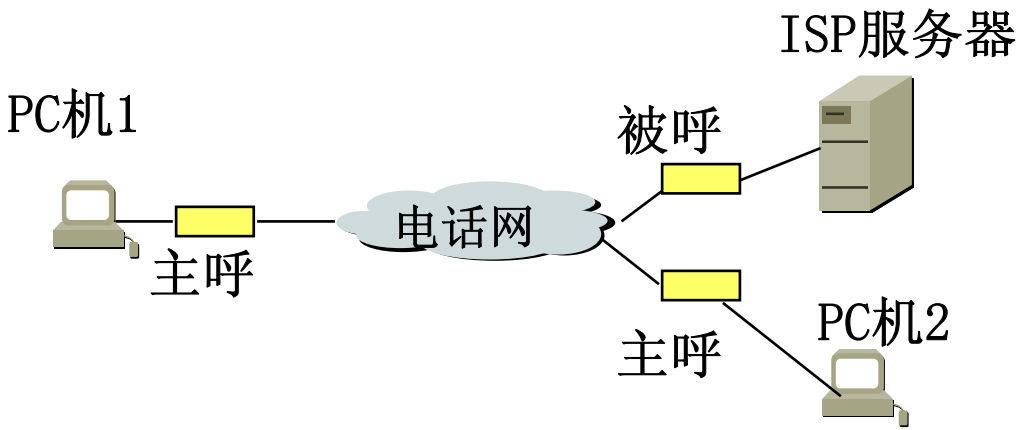
2)用途：使用的场合

3)符合相关标准

4)符合当地有关部门的入网规定

注意：Modem需成对使用，通信双方的Modem一定要匹配

一台主呼，另一台被呼　*用户方一般为主呼*



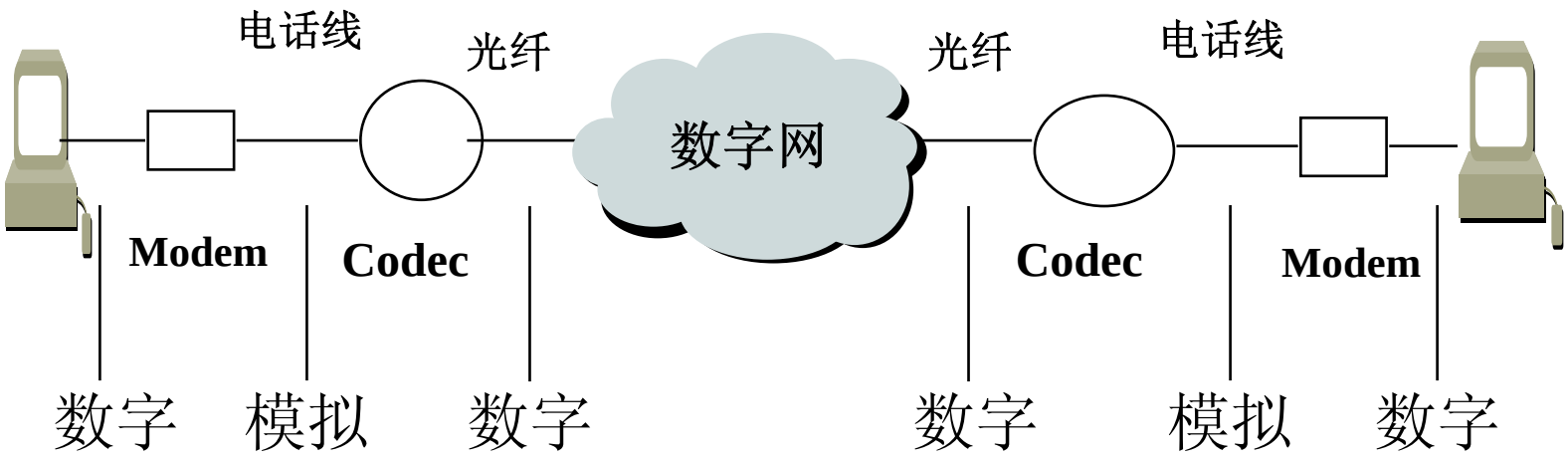
编码/解码(COding and DECoding)

实现模拟信息与数字信号之间的转换

生产控制、用数字信道传输模拟信息等

编码：将模拟信息转换为数字信号的过程

解码：将数字信号还原为模拟信息的逆过程



编码/解码(COding and DECoding)

脉码调制技术（PCM）

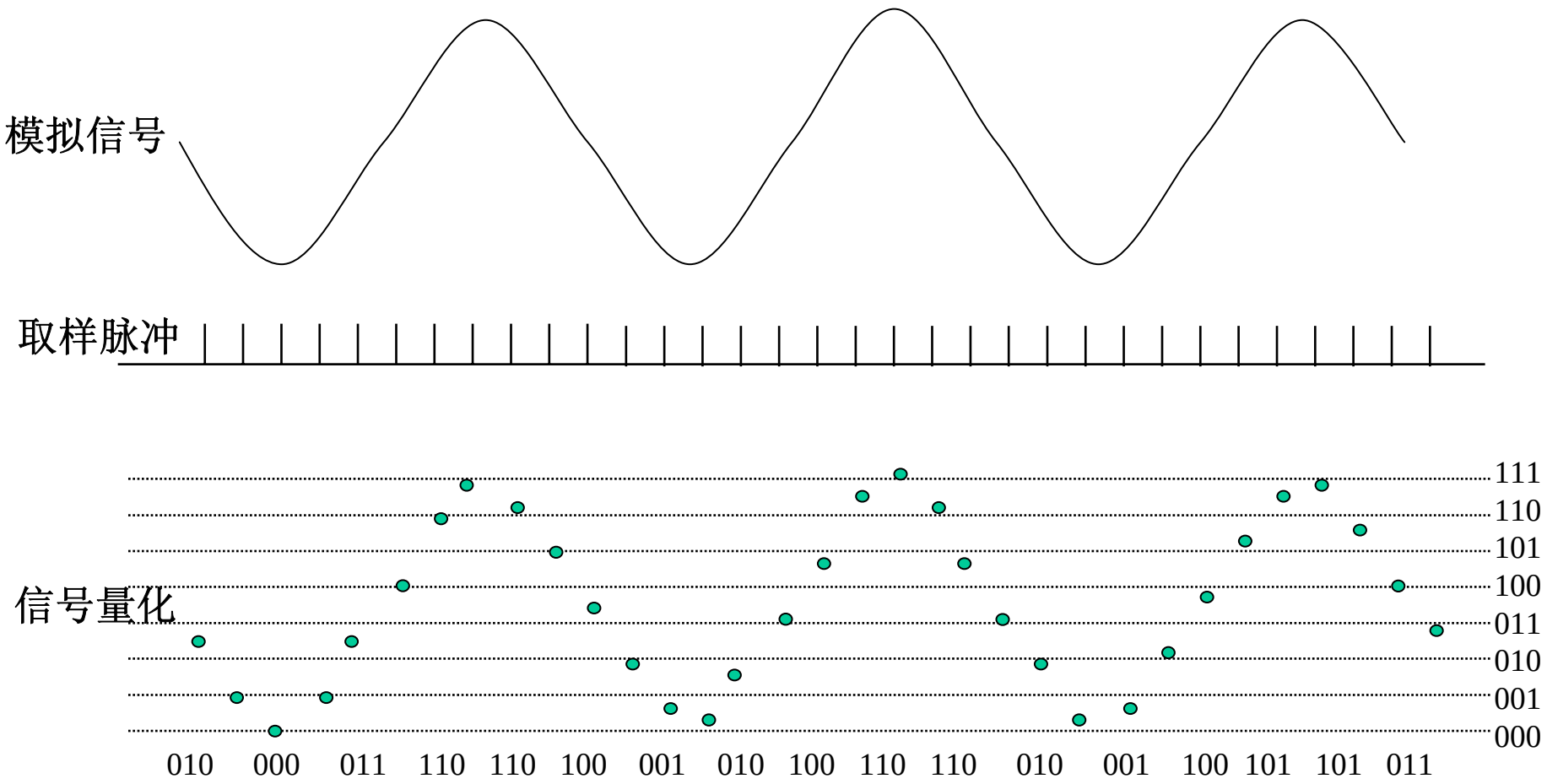
取样：通过某种频率的取样脉冲将模拟信息的值取出，变连续的模拟信息为离散信号。

量化：量化的目的是确定取样出的模拟信号的数值。通过规定一定的量化级，对取样的离散值进行“取整”量化，得到离散信号的具体数值。

编码：将量化后的值编码成一定位数的二进制值。

依据—尼奎斯特取样定理：最大频率为 **F** 的模拟信号被不失真还原的前提条件是取样频率不低于 **2F**。

编码/解码示意

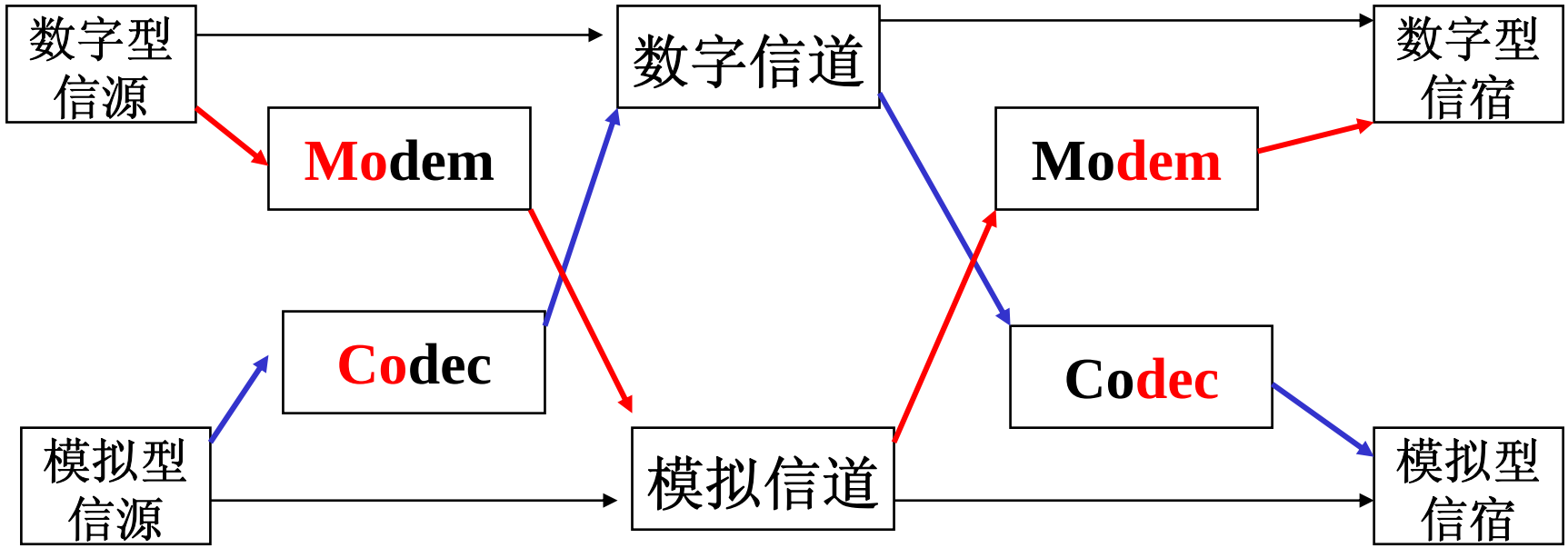


8级量化，可用3位表示。

语音频率小于**4000Hz**，采样频率**8000Hz**，量化**256**级，编码**8**位，传输速率：不小于**64Kbps = 8000**次/秒 * **8**位/次。

变换器和反变换器的效果

通过调制/解调、编码/解码技术，可以保证计算机之间以数字信号的方式进行通信；



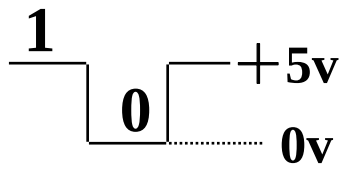
数字信号的发送和接收

数字信号的表示：

二进制数字（0，1）对应两个电平（或光脉冲）

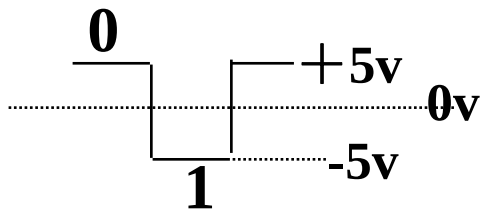
单极性脉冲： 无电压（或者无电流）“0”

恒定正电压（或者有电流）“1”



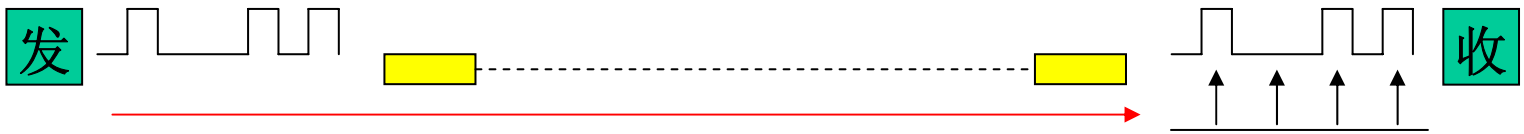
双极性脉冲： 数字信号“0”或者“1”

相同幅度的正电压或者负电压



发送： 发送设备根据自身的时钟分频形成指定频率（发送频率）的数据波（脉冲序列），并发往线路；

接收： 接收端设备则根据自身的时钟形成指定频率（接收频率）的取样脉冲，对信道上的数据波进行取样并通过设置阈值电平识别数据波对应的值。



2.4 传输编码

★字符编码：利用0和1比特的特定组合来表示字符

BCD码、EBCDIC码、IA5码、 ASCII码(美国信息交换标准码，P23)

图形字符：数字、字母、运算符号、语句符号等

控制字符：传输控制、格式控制、信息分隔字符等

ASCII码的表示： $b_7b_6b_5$ $b_4b_3b_2b_1$ (表2-1)

(简记X/Y 或XY：X=$b_7b_6b_5$ Y=$b_4b_3b_2b_1$)

例：A：1000001，记为4/1 或41

(用ASCII码“41”表示字符‘A’)

ASCII码的控制字符：

传输控制字符：用于控制信息的传输

SOH(标题开始，0000001，0/1)，
STX(正文开始，0000010，0/2)　　ETX(正文结束，0/3)
EOT(传输结束,0000100，0/4)，　　ENQ(询问,0/5)，
ACK(确认,0000110，0/6)，　　NAK(否认,1/5)，
DLE(数据转义,0010000，1/0)，　　SYN(同步,1/6)；

格式控制字符：控制打印和显示设备的信息格式和定位

BS(退格,0001000)，　LF(换行,0001010，0/A)
CR(回车,0001101，0/D)

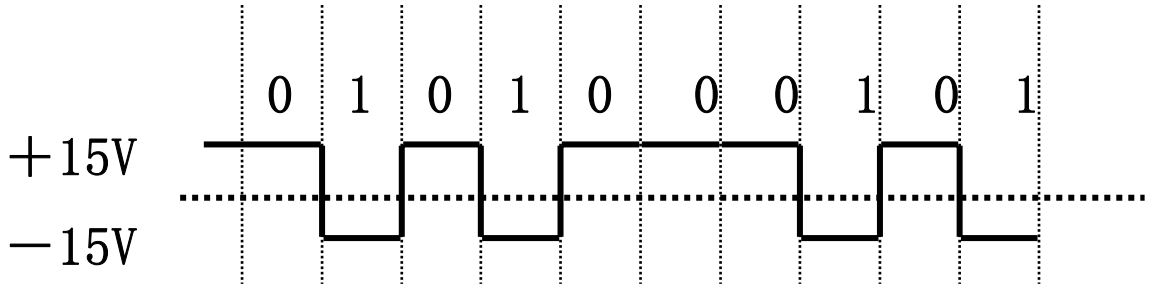
信息分隔字符：用于分隔信息

US(单元分隔,1/F)，RS(记录分隔,1/E)，GS(组分隔,1/D)，
FS(文卷分隔,1/C)。

通信编码

通信编码：利用特定的电平信号来表示0、1比特值，
并通过计算机或者其它通信设备的输入输出端口传输

(1) RS-232编码：利用不同的电平表示不同的二进制值，
(双极性编码) 正电平（+15v）表示数字信号 “ 0”
负电平（-15v）表示数字信号 “1”
PC机的RS232串行通信端口

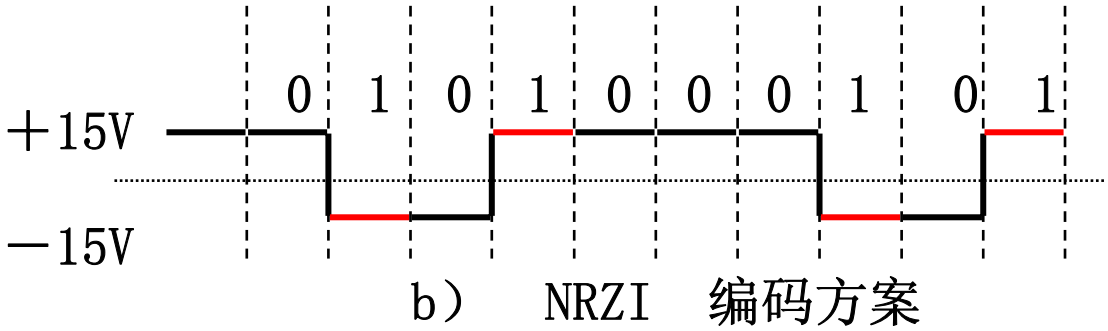


a） RS232 编码方案

(2) 不归0交替编码(NRZI)：根据相邻比特的电平变化状况确定

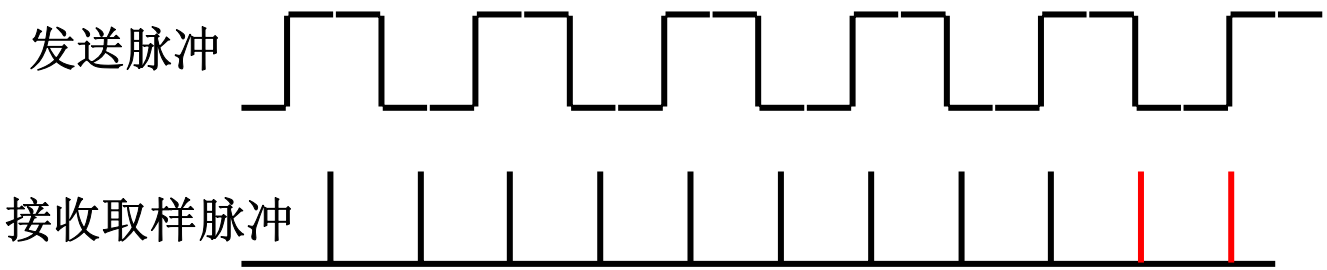
比特间隔发生电平变化表示 “1”

比特间隔不发生电平变化表示 “0”



b） NRZI 编码方案

特点：编码中不含同步信息 发送/接收设备的时钟略有差异时，可能造成误差积累,造成取样脉冲的偏移，出现差错



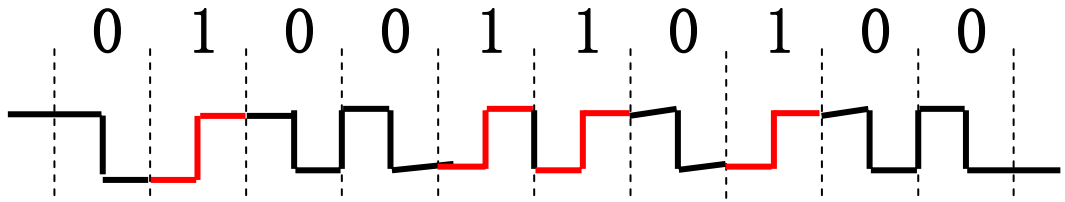
收发设备的误差积累

(3) 曼彻斯特编码

一个比特时间一分为二

比特时间内 发生低电平到高电平的变化表示“1”，

高电平到低电平的变化表示“0”



(4) 差分曼彻斯特编码

编码特征：一个比特时间一分为二，

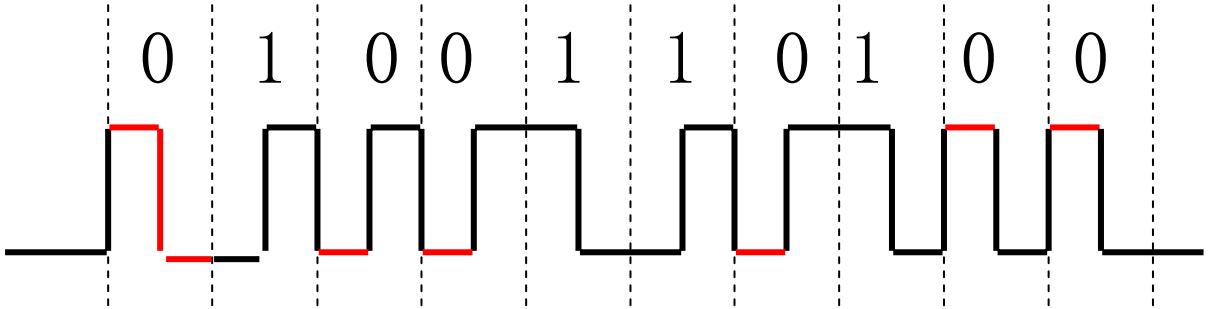
比特时间的中部发生电平变化，

表示的值依赖于前一比特的最终电平状态

当前比特的前半部分电平*不同于*前一比特的最终电平状态（即位间电平发生变化），表示“0”

当前比特的前半部分电平*相同于*前一比特的最终电平状态（即位间电平不发生变化），表示“1”

差分曼彻斯特编码示意



特点：

(3)(4)编码中含有同步信息(每个比特中部的电平跃变信号)

接收方可以根据该同步信息及时调整接收脉冲的产生，可以支持较大数据块的传输

要求发送/接收设备能够产生较高频率的发/收脉冲

（即编码效率较低，50%）

(5) 4b/5b码——光纤应用，降低成本

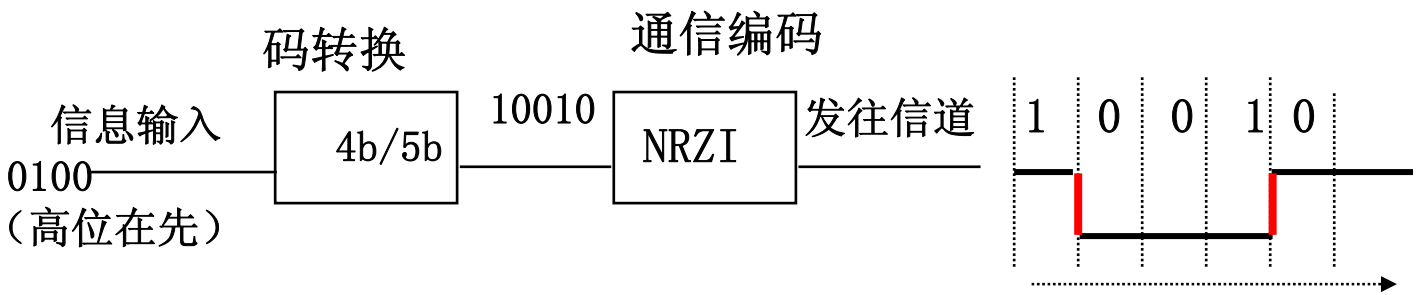
用5位(5b)的符号表示4位(4b)的信息(数据)

采用不归0交替编码(NRZI)表示这5位符号。

要求每个符号中至少应有2个以上的“1”比特（跃变）出现，

例：0010-->01001，0110-->01110 ， 1100-->11010

1000--> 10010， 0000--> 11110



特点：内含同步信号，支持批量数据传输；

编码效率较高，**80%**。

2.5 传输方式

➢ *并行传输*:　　字符编码的各个比特同时传输

特点：　一个比特时间内可传输一个字符，传输速度快，

每个比特传输要求一个单独的信道支持，通信成本高，

远距离传输时，线间干扰导致可靠性下降。

➢ *串行传输*　　将组成字符的各个比特串行地发往线路

特点：传输速度低，一次一个比特；

通信成本较低，只需一个信道

并行传输　　串行传输

★传输方式

➢ *同步传输*：以多个字符或者多个比特组合成的数据块

为单位进行传输，利用独特的同步模式来限定数据块，达到同步接收的目的。

发送：同步符号(起始字符)＋数据块＋同步符号(结束字符)

接收：遇到同步符号，开始接收数据，直到结束符号为止。

同步符号：标识数据块的开始和结束

可能问题：假同步现象—数据块中含有与同步符号相同的内容

解决方法：增加匹配同步符号的难度

SYN, SYN, G, H, …, B, A, SYN, D, E, SYN, SYN ⟶ 传输方向

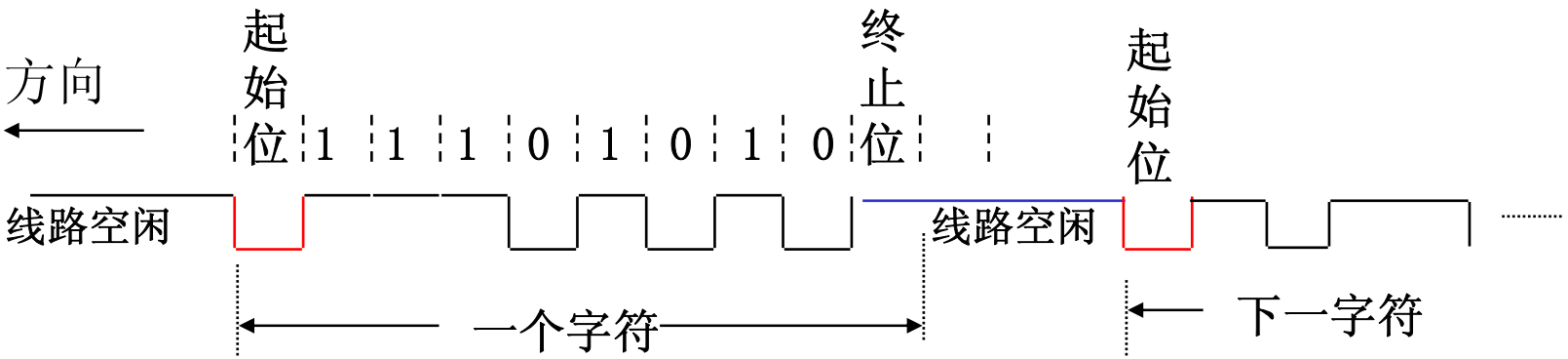
★传输方式

➢异步传输

特点：　字符内部的各个比特采用固定的时间模式，每个字符独立传输，　字符之间间隔任意；

用独特的起始位/终止位来限定每个字符，并同步双方的动作。

传输效率较低。



★同步技术

目的：　　保证接收方在时间上与发送方取得同步，
以便能够正确地识别和接收发送方发来的数据。

位同步：　使接收方可以正确地接收各个比特

自同步法：接收方直接从数据波中获取同步信号（曼码）。

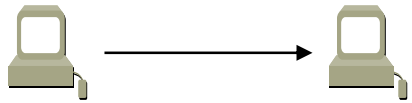
外同步法：发送方在发数据前，先向接收方发一串同步时钟序列，接收方根据这一同步时序锁定接收频率。
（异步传输的起始/终止位）

字符同步：　使接收方可以正确地识别数据群
利用同步传输时的同步字符（SYN）
接收方在识别到独特的同步字符或同步模式后，
才开始真正的数据接收。

接入X.25分组交换网：同步端口

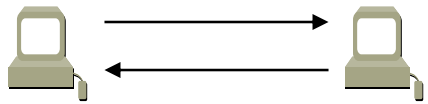
接入电话网：　　异步端口

单工传输：任意时刻只允许向一个方向进行信息传输；

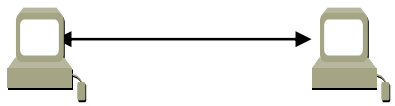
二线 

半双工传输：可以交替改变方向的信息传输，

但在任一特定时刻，信息只能向一个方向传输；



全双工传输：任意时刻信息都可进行双向的信息传输。

四线 

2.7 传输差错处理

目的：保证信息传输的正确性；

噪声导致差错，无差错处理能力的系统是不可用系统。

方法1：反馈重传法(ARQ)

(1) 发送方发送具有检测错误能力的代码（检错码）；

(2) 接收方根据代码的编码规则，验证接收到的数据代码，并将结果反馈给发送方(正确接收/接收有错）；

(3) 发送方根据反馈的结果决定是否执行重传动作，如果接收方未正确接收，则重传；

(4) 在规定的时间内，若未能收到反馈结果（称为超时），则发送方可以认为传输出现差错，进而执行重传动作。

停一等协议

发送一块数据，计时。

等待接收方的反馈结果，

如果接到否定确认，

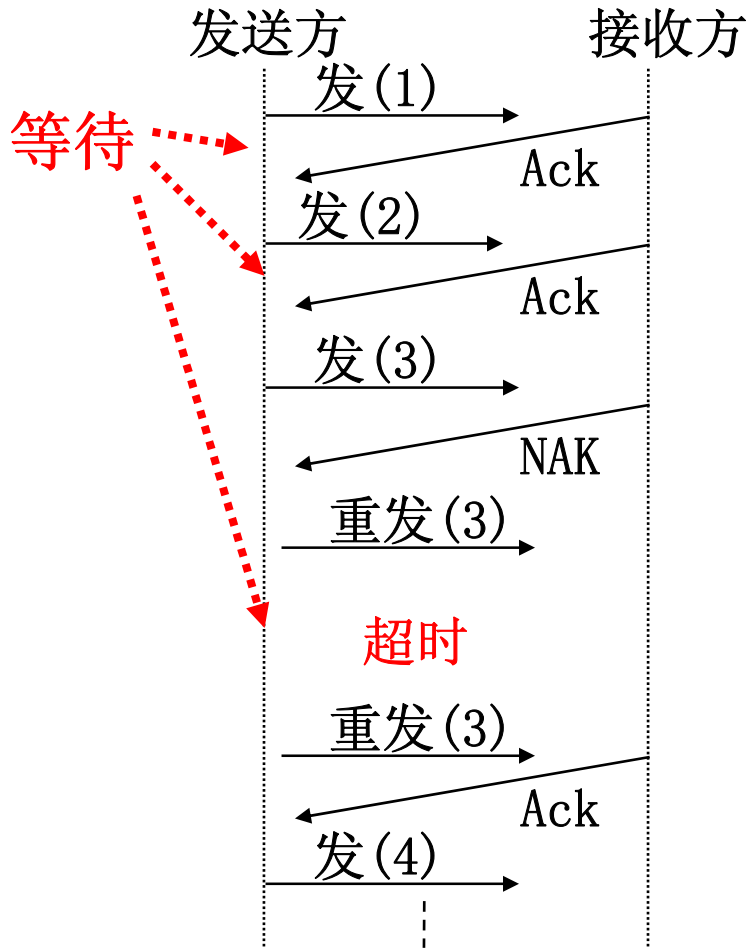
重新传输本数据块；

如果收到接收确认，

继续发送后继块数据；

如果计时器超时，

重新传输本数据块。



滑动窗口协议—停等协议的改进

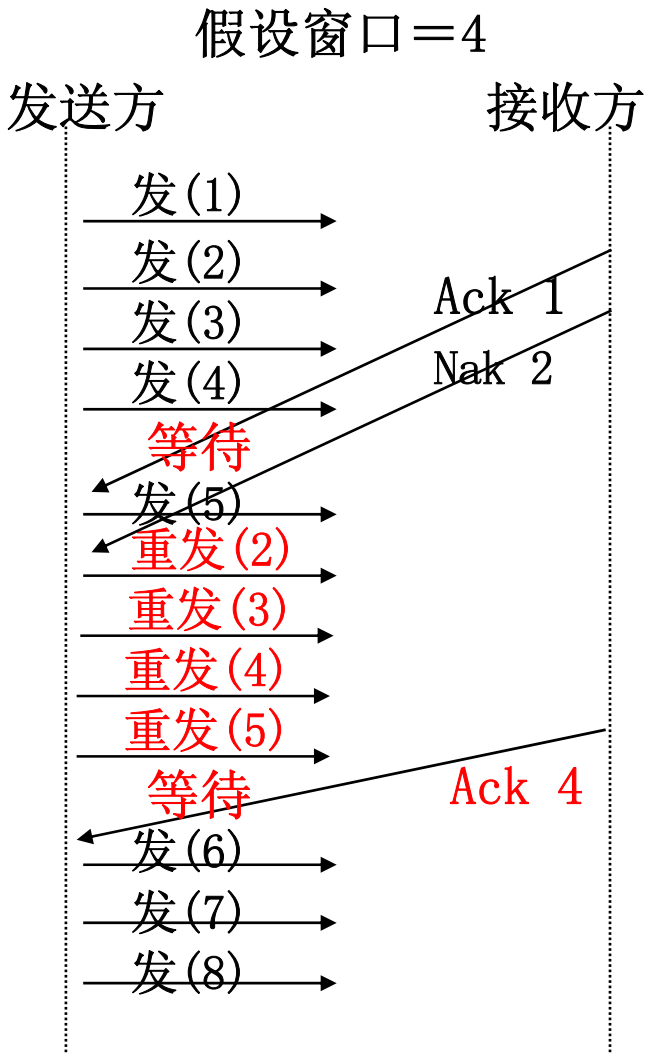
(1) 发方一次连续发送多块数据（块数限于窗口尺寸）；

(2) 收方对每块数据进行差错分析，如果发现错误，立即反馈发送方；

(3) 收方可对收到的多个正确的数据块进行一次性确认；

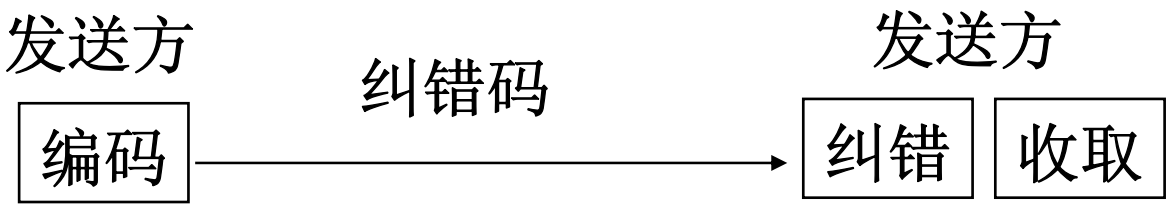
(4) 发方根据反馈的结果，重发指定的数据块，或重发指定数据块及其之后的所有数据块，或者直接发送后续数据块。

（例中重发指定及其后的数据块）



方法2：前向纠错法（FEC）

发送方发送具有纠错能力的编码；
接收方根据编码规则纠正传输中的差错。



特点：无需反馈信道；
编码复杂（纠错能力有限）。

差错处理的核心：检错码/纠错码的构造。

2.8 常用检错码

检错码是差错检测的核心。

检错码＝信息字段＋校验字段（冗余字段）

校验字段和信息字段之间存在相关性、联动性；

校验字段越长，编码检错能力越强，编/解码设施越复杂；

附加的冗余信息在整个编码中所占的比例越大，传输的有效成分越低。

传输顺序：信息字段在前，校验字段在后。

★ 奇/偶校验码

奇/偶校验码的校验字段仅占一个比特（一位，校验位）。

(1) 水平奇/偶校验码　（可发现奇位错）

校验位的取值应使整个码字(包括校验位)中为“1”的比特个数为奇(偶)数。

传输时，形成的校验位附加在信息字段之后传输。

例：	信息字段	奇校验码	偶校验码
⟵	0110001	01100010	01100011

编码效率：Q/(Q+1)　（信息字段占Q个比特）

异步传输方式中采用偶校验，

同步传输方式中采用奇校验。

奇/偶校验码

（2） 垂直奇/偶校验码 （可发现有限位错）

将被传输的信息进行分组，

每个分组（字符）的相同位进行奇/偶校验

例如：4行7列信息组的垂直奇/偶校验码。

信息组：
0111001
0010101
0101011
1010101

垂直奇校验字符 0101101

垂直偶校验字符 1010010

01110010010101010101110101010101 （奇校验）

编码效率为： PQ/P(Q+1) （假设信息分组占Q行P列）

（3） 水平垂直奇/偶校验码（可用于纠一位错）

同时实施水平、垂直校验，只能使用偶校验。

例：4行7列信息组的水平垂直偶校验码。

	信息组	校验位
	0111001	0 1
	0010101	1 0
	0101011	0 1
	1010101	0 1
垂直偶校验字符	1010010	1
奇	0101101	0/1

01110010001010110101011010101010100101

若被传的信息分组占Q行P列， 编码效率为QP/(P+1)(Q+1)

举例：

例：采用8位一组的水平垂直奇偶校验，收到位串序列：

“01010010 10101010 11001010 10011010 10111000”，

传输是否正确？如果有错，能否纠正？

解：应用水平垂直偶校验原理对收到的位串进行校验：

```
 0101001 0
 1010101 0
 1100101 0
 1001101 0
 1011100 0
```

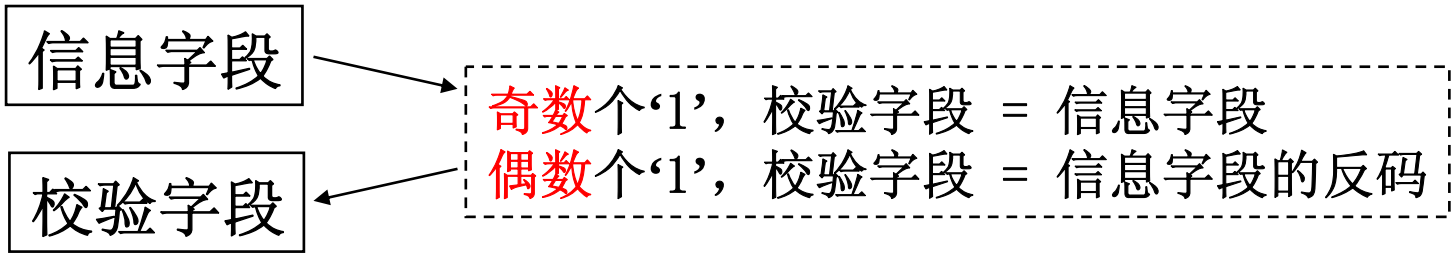
原序列：01000010 10101010 11001010 10011010 10111000；

若为ASCII，且低位先传（1-7,8），则字符应为：BUSY；

高位先传（7-1,0），则字符应为：!TeM；

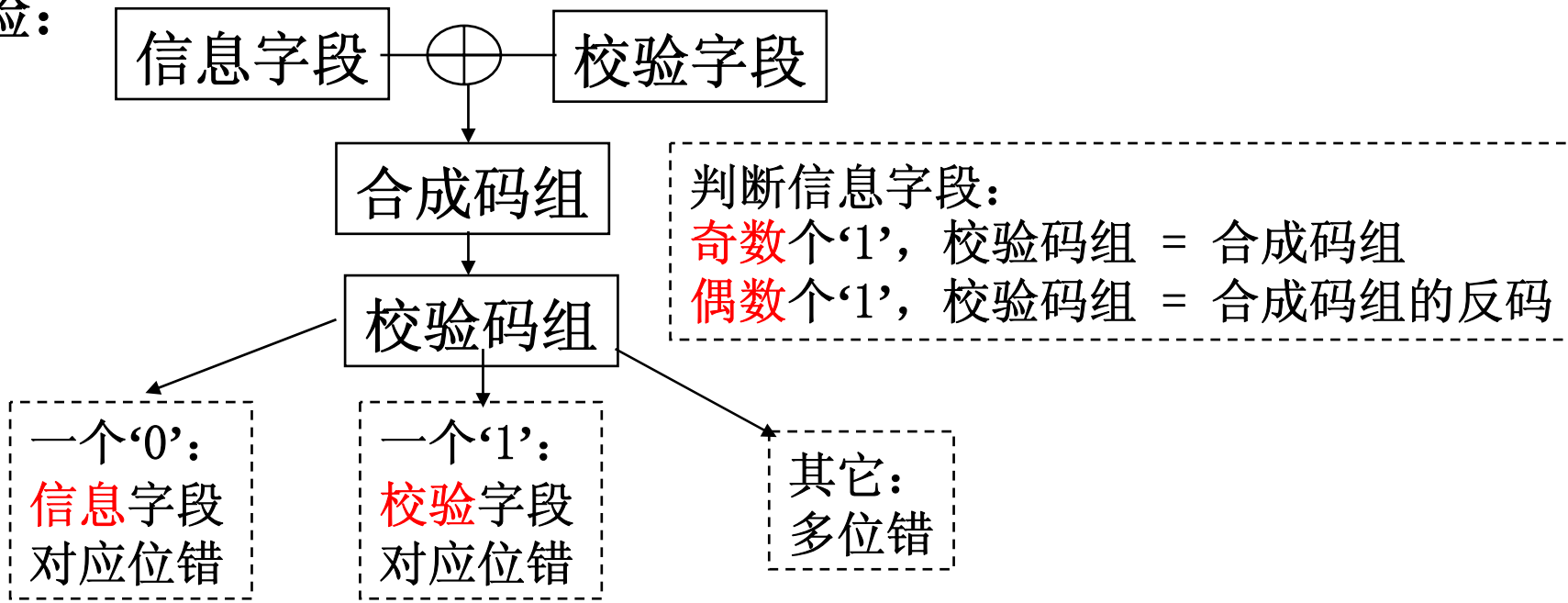
★ 正反码 （可纠一位错）

校验字段与信息字段占有相同的位数



传输：信息字段 + 校验字段

校验：



正反码举例：

接收码字	合成码组	信息字段奇/偶	校验码组	结果	原信息字段
01011**0**1011	00000	奇（不变）	00000	正确	01011
10010**0**1101	11111	偶（取反）	00000	正确	10010
01111**0**1011	00100	偶（取反）	11**0**11	信息位3错	01011
01011**0**1001	00010	奇（不变）	000**1**0	校验位4错	01011

正反码具有纠一位错的能力，其编码效率为50%。

★ 循环校验码(CRC)

原理：当确定字段长度后，任意一个二进制位串（字段）都可以和一个系数仅为0和1取值的多项式一一对应。

例： 1010111： $x^6+x^4+x^2+x+1$

$x^5+x^3+x^2+x+1$： 101111

若信息字段为K位，校验字段为R位，则码字长度为N=K+R；

任一合法码字都可由一个R次多项式g(x)产生。

合法码字 $V(x) = x^R m(x)+r(x) = A(x)g(x)$

m(x)— K-1次信息多项式，信息字段，

r(x)— R-1次校验多项式，校验字段，

g(x)— R次生成多项式

$g(x)=g_0 + g_1x + g_2x^2 + \ldots + g_{(R-1)}x^{(R-1)} + g_Rx^R$。

其中： $g_i = 0$ 或 1，$0<i<R$； $g_0 = g_R = 1$，

☆ 校验字段r(x)生成方法之一：软件方法—多项式除法取余数

例如：信息字段代码为： 1011001　　对应 $m(x)=x^6+x^4+x^3+1$

生成多项式：$g(x)=x^4+x^3+1$　　对应代码：11001

则 x^4 $m(x)=x^{10}+x^8+x^7+x^4$　　对应代码：10110010000

除法：

```
          1101010
11001 ) 10110010000
        11001
         11110
         11001
          11110
          11001
           11100
           11001
            1010
```

校验字段 ⟶ 1010（余数）

4次项g(x)产生4位校验字段

多项式除法使用模2加

接收方使用相同的**g(x)**和除法进行校验：

接收字段/生成码

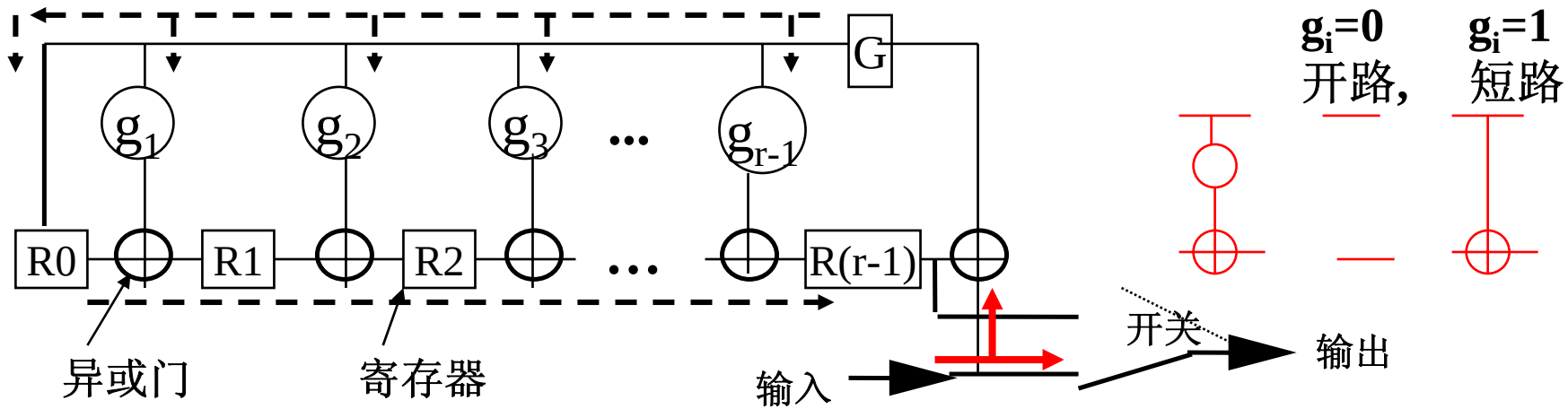
如果除尽，则正确，否则错。

形成码字：10110011010

☆ 校验字段r(x)生成方法之二：硬件实现

根据g(x)构建编码电路，信息字段作为输入，校验字段存寄存器。

$$g(x)=g_0 + g_1x + g_2x^2 + \ldots + g_{(R-1)}x^{(R-1)} + g_Rx^R$$



注：为区分寄存器标识，图中表示的次项的‘R’暂记为‘r’；

输入：发送时为信息字段，或者校验时为接收到的码字。

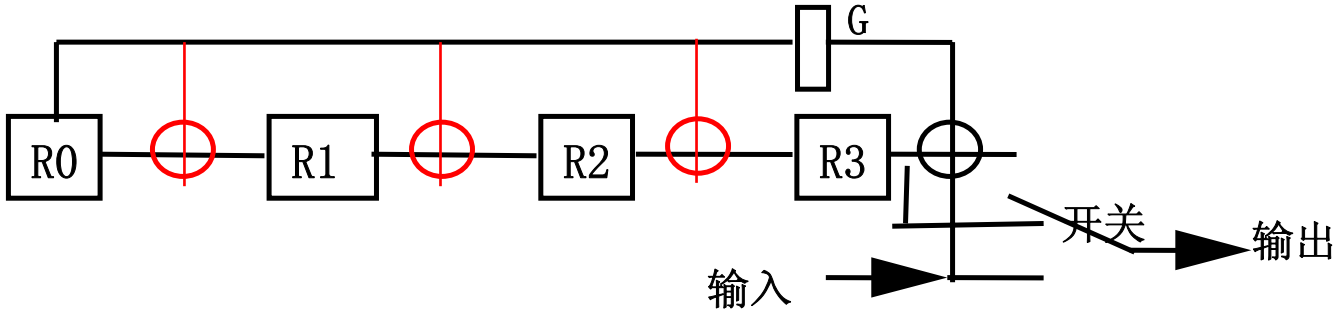
移位寄存器R：发送时逐步形成校验字段，

发送完后开关上拨，逐位输出；

校验时逐步形成校验结果。

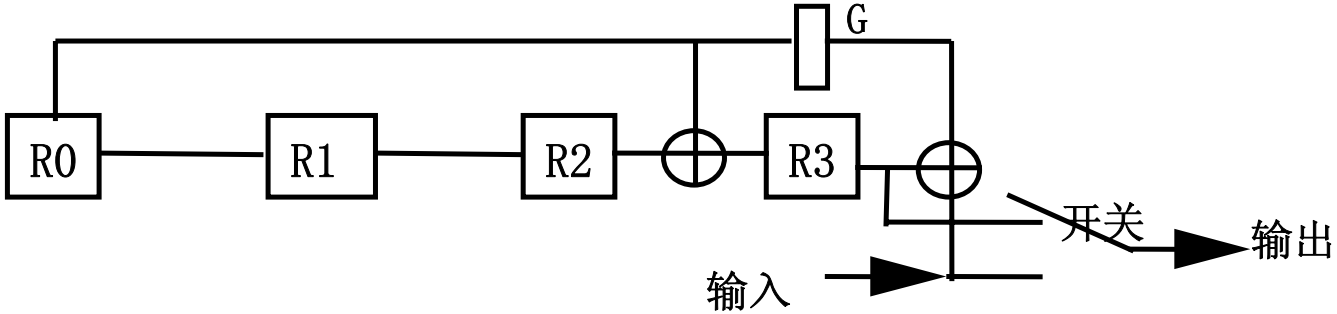
硬件编码使用举例：

g(x)=x^4+x^3+1的编码电路：



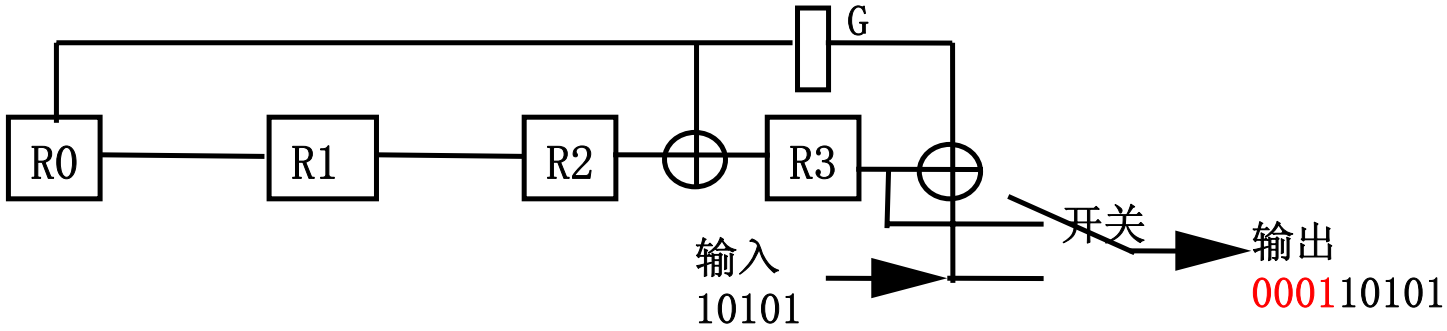
此例： g_0, g_4恒为1， g_3为1， g_1, g_2为0；

编码电路：



硬件编码使用举例：

$g(x)=x^4+x^3+1$的编码电路：



输入	R0	R1	R2	R3	输出	
1	0	0	0	0		R0=G=原R3+I
0	1	0	0	1	1	R1=原R0
1	1	1	0	1	01	R2=原R1
0	0	1	1	0	101	R3=原R2+R0
1	0	0	1	1	0101	
	0	0	0	1	10101	

校验时：整个码字输入完后，移位寄存器Ri应为全0，
否则接收到的码字出错。

CRC校验码使用广泛。

硬件电路主要用于自动生成码字，或者进行校验；
多项式除法主要用于软件编程。

常用的CRC生成多项式g(x)为:

CRC16=$x^{16}+x^{15}+x^2+1$　　R=16，　IBM专用

CRC16=$x^{16}+x^{12}+x^5+1$　　R=16，　CCITT专用

CRC32=$x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^5+x^4+x^2+x+1$

R=32，　LAN中常用

2.9 传输控制规程

目的： 协调通信双方的动作，保证数据信息传输的正确性。

异步传输控制规程： 实现以字符为单位的传输；

同步传输控制规程： 实现以多个字符或比特组合成的数据块为单位的传输；

2.9.1 面向字符型的传输控制规程 （支持字符数据传输）

规程实例：二进制同步通信规程(BSC)

（1）目标

支持任意字符型数据(文本）在计算机之间的传输。

当用于支持位序列传输时，位序列将以7位或8位（有校验位）一组形成字符，不足位补‘0’，最终形成字符串。用户以其他方式说明位序列的实际长度。

例： 0101011 1010101 1100010 1011101 1010000（补0）

ASCII + U b] P +Ub]P

(2) 数据块的组成和歧义问题的解决

★ 数据块的组成：

为了体现信息的逻辑性，借用了字符编码（如ASCII、EBCDIC码）的10个特殊字符（控制字符）：

SOH（0/1，标题开始）、STX（0/2，正文开始）、
ETX（0/3，正文结束）、EOT（0/4，传输结束）、
ETB（1/7，组结束）、DLE(1/0，数据转义)、
ENQ（0/5，询问）、SYN（1/6，同步）、
ACK（0/6，确认）、NAK（1/5，否认）等。

例如：SOH xxxxxx STX xxxxxxxxxxxxxxxx ETX

潜在问题：数据本身可能蕴含这些控制字符：

例：SOH xxx ETB xx STX x DLE SOH xxx ETX

(2) 数据块的组成和歧义问题的解决

★ 歧义问题的解决：字符转义和字符填充；

目的：支持任意字符数据传输。

字符转义：区分控制字符和数据块中的‘假’控制字符，在控制字符前前缀转义字符DLE形成特定语义的控制字符组，增加匹配控制字符组的难度。

DLE SOH、DLE STX、DLE ACK、DLE NAK等

字符填充：在数据DLE前再增加一个DLE，使其转义为一般字符，避免数据中同时出现DLE和控制字符时可能的歧义。

原意：SOH xxxETBxx STX xDLESOHxxx ETX

转义：DLESOH xxxETBxx DLESTX xDLESOHxxx DLEETX

填充：DLESOH xxxETBxx DLESTX xDLEDLESOHxxx DLEETX

动作：若收到两个连续的DLE，则丢弃一个，并认为保留的是数据DLE字符。（此处的控制字符仅仅是一个字符！）

歧义解决方案的补充说明

★ 因特网中歧义问题的解决方案

IP数据报用字符END（0XC0）进行数据块（报文）定界；

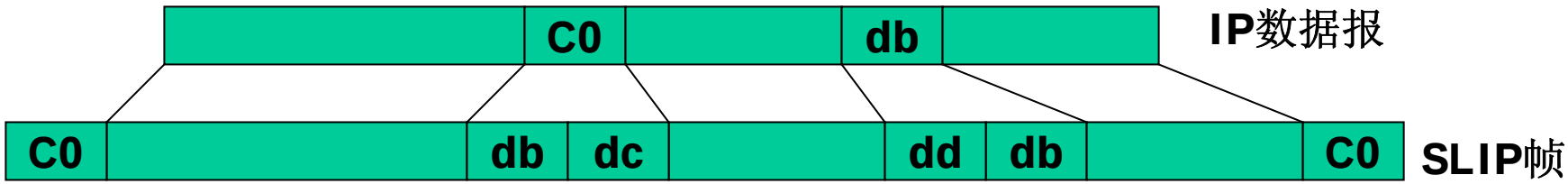
转义字符： 0Xdb；

方案：如果在IP数据中出现END字符（0XC0），就用2字节字符0Xdb，0Xdc代替；

如果IP数据报中有字节为0Xdb，就用0Xdb，0Xdd代替；

接收方执行相反的还原过程。

举例：SLIP（Serial Line IP) 协议



（3）通信双方交换的信息序列类型：

正文信息：　通信双方正常交换的数据（双方均可发送）；

控制序列：控制通信双方交换信息的过程。

★ 控制序列

确认（ACK）：　SYN SYN 0/1 DLE ACK

增加0或1的目的在于区分应答的对象；

否认（NAK）：　SYN SYN DLE NAK

询问（ENQ）：　SYN SYN 站地址 DLE ENQ

拆链（EOT）：　SYN SYN DLE EOT

★ 正文信息序列

基本格式，含标题和正文两部分：

SYN SYN DLESOH 标题 DLESTX 正文 DLEETX 校验码

无标题格式，省略标题时的数据块格式：

SYN SYN DLESTX 正文 DLEETX 校验码

成组格式(多段正文)：

SYN SYN DLESOH 标题 DLESTX 正文组1 DLEETB 校验码

SYN SYN DLESTX 正文组2 DLEETB 校验码

… …

SYN SYN DLESTX 正文组n DLEETX 校验码

校验码：（1）水平垂直奇偶校验

（2）当采用循环校验时，$g(x)=x^{16}+x^{12}+x^5+1$，

校验对象为SYN SYN之后的所有内容。

（4）工作过程

建立链路：　建立链路指建立通信双方的收发关系

数据传输：　在链路建立的基础上，传输数据

拆除链路：　释放通信双方已建的关系

★ 建立链路：

主叫站　　被叫站

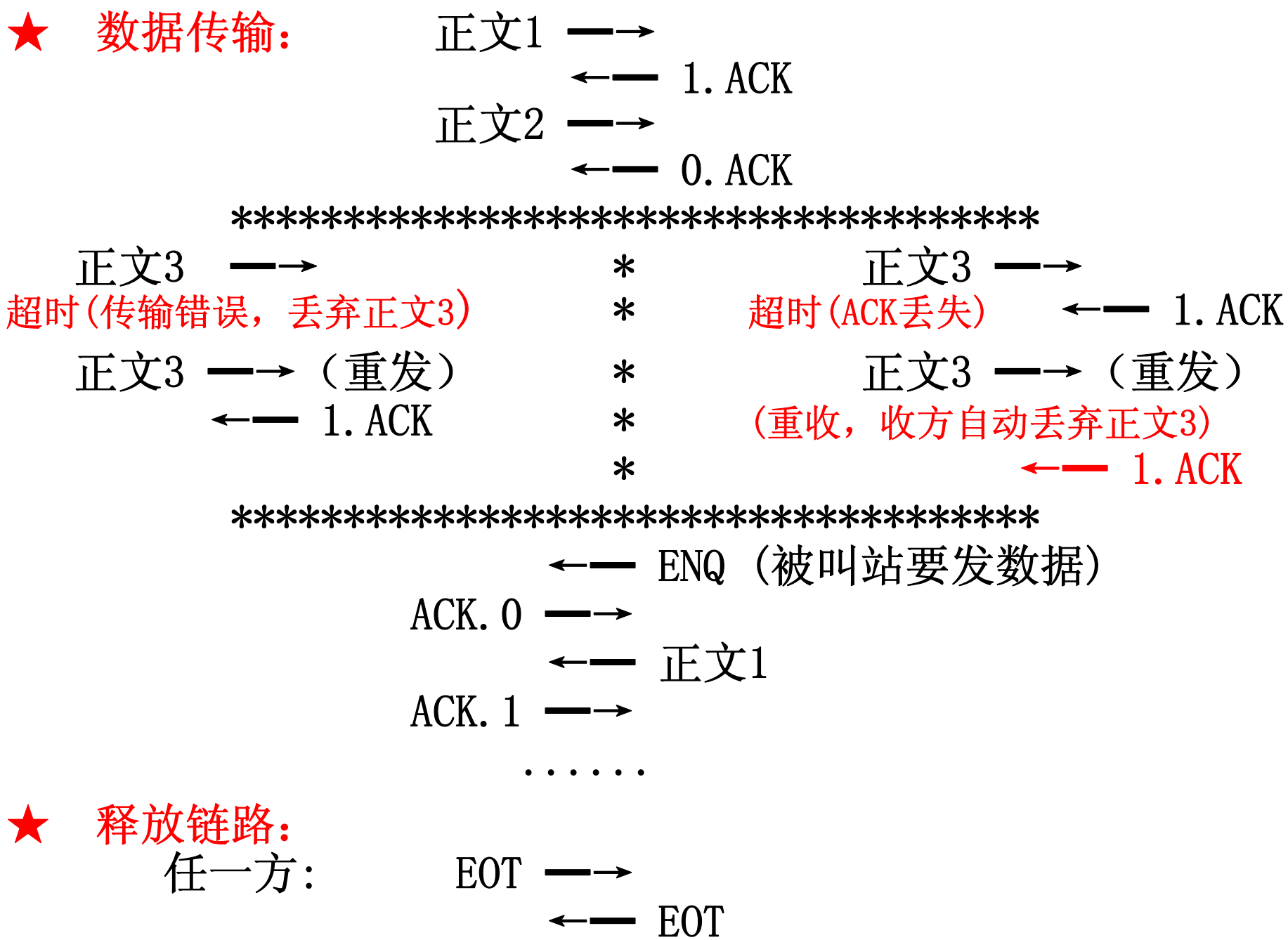
ENQ.被叫地址 ——→

←—— NAK　　（未准备好接收）

ENQ.被叫地址 ——→

←—— 0.ACK　（收发关系建立）

★ 数据传输：



★ 释放链路：

任一方：

面向字符型的传输控制规程的特点：

半双工的停-等协议、超时重发，传输效率较低。

数据块和控制序列格式不统一，易引起二义性。

控制序列的差错校验能力仅依赖于控制字符本身的字符奇偶校验，可靠性较低。

以字符传输为目标，适用性较弱。

仅需要很少的缓存容量，规程简单，易于实现。

2.9.2 面向比特型的传输控制规程

支持任意二进制数据的传输。

常用的标准：ISO的高级数据链路控制规程(ISO HDLC)

CCITT 的平衡型链路访问规程(CCITT X25 LAP-B)

HDLC介绍

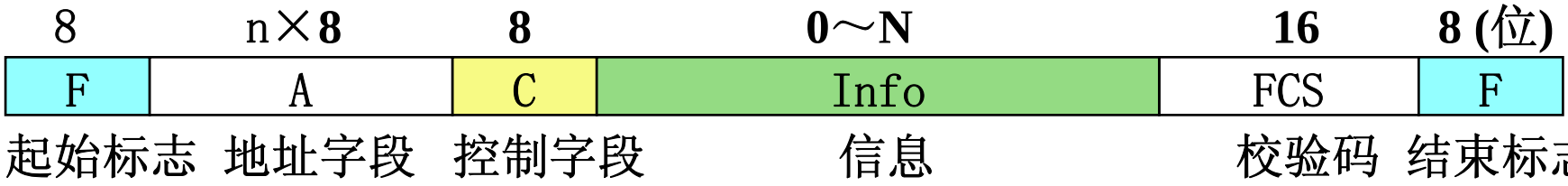
（1） 交换对象

帧： 通信双方交换的最小单位——比特序列。

帧的组成： 帧间隔符 比特序列 终止标志

01111110001101100001011011001101101111110

（2） 一般帧结构



★ **F（间隔符模式）：“01111110”———同步符号、帧之间的填充字符**

01111110111110000111100010101011010101010100101010101111110101111110

☆ **“0”比特插入法：避免帧内出现间隔符‘01111110’模式。**

发送方：逢5个‘1’，自动插入一个‘0’；

接收方：若5个‘1’后为‘0’，移去‘0’；否则帧结束；

01111110111100011100011001111110011011111101110101111110101111110

01111110111100011100011001111101001101111101011101011111101111110

★ **A(地址字段)—** 对方的地址

对应地址字段所属的字节首位为‘0’，表示后继字节仍为地址字段，

字节首位为‘1’，表示本字节为地址字段的最后字节。

★ 帧结构—C(控制字段)： 用于区分帧的类型

	0	1	2	3	4	5	6	7 （位）
信息帧 (I)	0	Ns			P/F	Nr		
监控帧 (S)	1	0	Type		P/F	Nr		
无编号帧(U)	1	1	M1		P/F	M2		

☆ 信息帧（I帧，C_0 = 0），用于传输用户数据

Ns（发送帧序号）说明本帧对应的帧序号（采用模8计数），每发一帧，Ns模8计数一次；

Nr（待收帧序号）：希望接收对方帧的序号，（采用模8计数）；

Nr 隐含指示该序号之前的所有帧已被正确接收；

☆ 信息帧—P/F（Probe/Final--查询/终止指示位）

—要求对方做出响应；

建立链接阶段：

发送方询问对方是否同意链接；

对方需立即响应，并在响应中置**F=1**。（例：同意建链）

数据传送阶段：

发送方置P=1，询问对方是否有数据待发；

如果对方有数据待发，开始发送信息帧（I）；

对方可以连续发送多帧，并在最后一个I帧中，置F=1，示意数据传输完毕；

如果对方无数据待发，直接以S帧（F=1）进行响应，示意无数据可发。

* **P/F总是一一对应的，在接到F=1的帧之前，不允许再发P=1的帧**

☆S(监控帧，C_0C_1 = 10)：用于表示接收状态

四种类型的监控帧。

Type=00，接收准备就绪(RR)，准备接收序号为Nr的帧；

Type=10，未准备就绪(RNR)，告诉对方已经收妥Nr以前的所有帧，但希望对方暂缓发送Nr帧；

Type=01，拒绝接收(REJ)，告诉对方已经收妥Nr以前的所有帧，但编号为Nr的帧有差错，希望对方重发序号为Nr及其以后的所有帧；

Type=11，选择接收(SREJ)，类似REJ监控帧，但希望对方仅仅重发第Nr帧。

☆U(无编号帧， C_0C_1 = 11)：链路控制帧，不含序号

M1，M2表示帧类型

M(M1M2)=11000(SARM)， 置本次链路为异步响应模式；

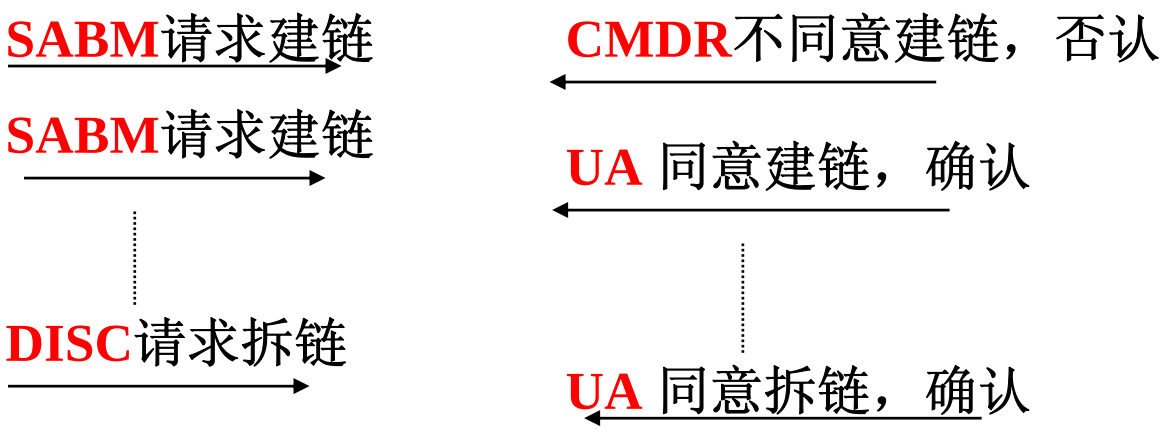
M(M1M2)=00001(SNRM)， 置本次链路为正常响应模式；

M(M1M2)=11100(SABM)， 置本次链路为异步平衡模式；

M(M1M2)=00010(DISC)， 请求释放(拆除)本次链路；

M(M1M2)=00110(UA)， 对对方命令进行确认，类似BSC中的ACK；

M(M1M2)=10001(CMDR)， 对对方命令予以否定，类似BSC中的NAK；



★ 帧结构

★ **Info(信息字段)**： 用于携带用户数据；
仅在**I**帧中出现，任意位串（已实施**‘0’**比特插入）。

★ **FCS**(校验字段)：对A、C和Info字段进行循环校验；

$g(x) = x^{16} + x^{12} + x^5 + 1$ （CCITT和ISO制定）

$g(x) = x^{16} + x^{15} + x^2 + 1$ （IBM公司制定—源于SDLC）

因为HDLC的帧中至少包含A、C、FCS字段，
因此帧长应大于等于32位。

（3） 窗口机制——提高效率的保障

传输窗口：通信双方同意在同一条链路上连续使用的信息帧序号

窗口尺寸：通信双方协商同意的在同一条链路上可连续发送且未被认可的信息帧个数；

HDLC 窗口尺寸确定为7，即任一方可以最多连续发送7帧无需对方的确认，帧序号循环使用（模8）。

在信息帧中用Nr, Ns来表示当前窗口的情况；

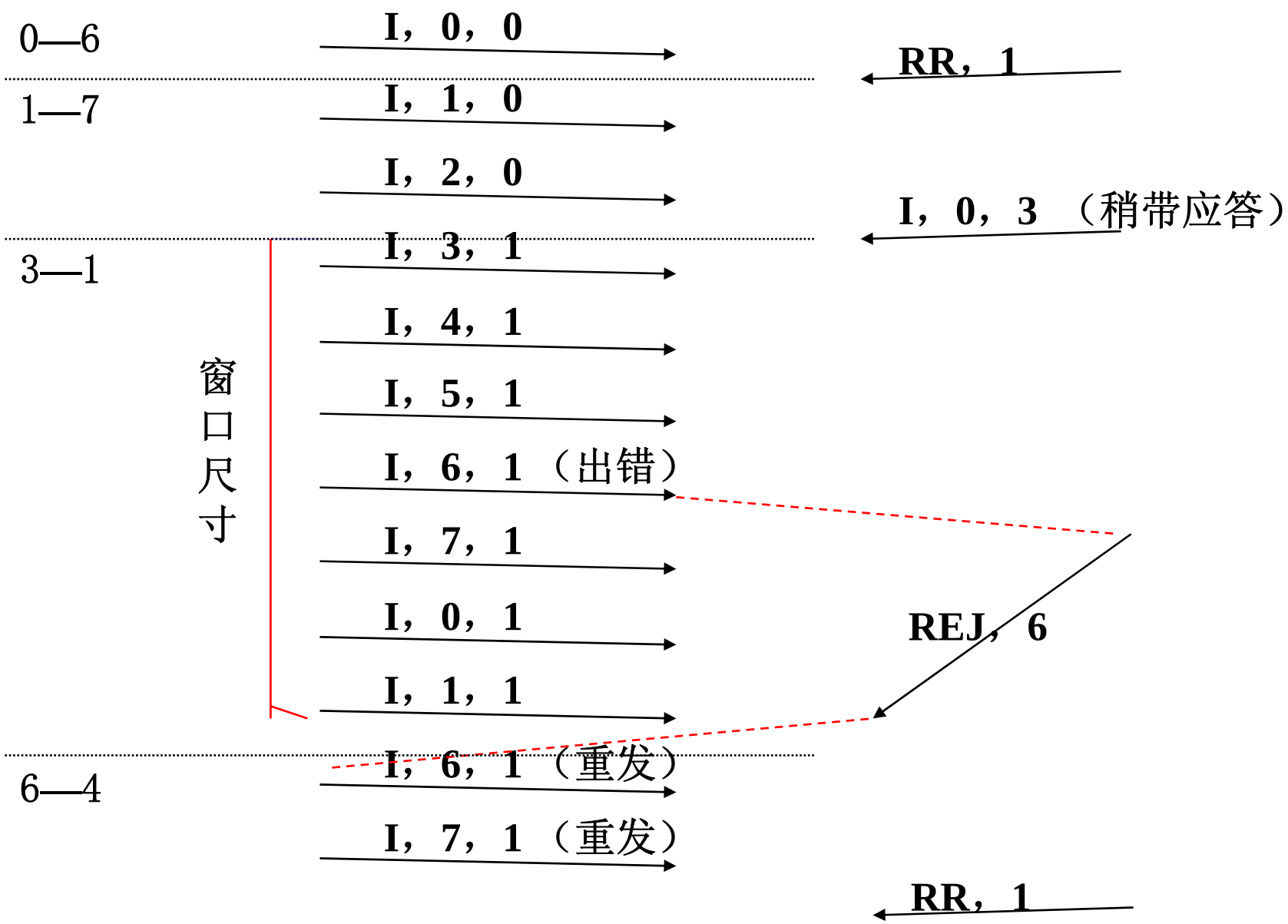
捎带应答：允许在反向传输的信息帧中附带确认信息；

超时重发：超时表示传输故障，准备重发所有未被确认的帧。

发送方每发送一信息帧，计时，直到收到接收方的确认（包括捎带应答），若超时，则重发；

接收方在正确接收到信息帧后，计时；若有数据待发，发送且携带应答；否则若在一定的时间内未收到后继信息，则发RR帧，准备继续接收后续帧。

窗口机制示意


0—6
1—7
3—1
6—4
窗口尺寸
I，0，0
RR，1
I，1，0
I，2，0
I，0，3 （稍带应答）
I，3，1
I，4，1
I，5，1
I，6，1（出错）
I，7，1
REJ，6
I，0，1
I，1，1
I，6，1（重发）
I，7，1（重发）
RR，1

（4） 数据交换过程

★ 建立链路: 置初始化模式和置响应模式；
通信双方确认可以通信，并协商通信的模式。

★ 传输信息帧：通信双方通过交换I帧和S帧，
完成双方的高层数据交换
全双工方式，双方均可发送信息帧和监控帧。

★ 释放(拆除)链路：任意一方在发送完数据之后，
均可用DISC命令要求拆除链路；
对方同意拆链，用UA命令响应。

★ HDLC工作示意

☆ 建立链路

A站	方向	B站	说 明
B:RR, P=1, 0	——→		; A询问B， P=1;
	←——	B:RIM, F=1	; B要求初始化;
B:SIM, P=1	——→		; A置B于初始化模式
	←——	B:UA, F=1	; B肯定答复,进入联机
B:SNRM, P=1	——→		; A置B正常响应模式
	←——	B:UA, F=1	; B肯定答复

☆ 数据传输

A站	方向	B站	说　明
B:RR, P=1, 0	——→		; A要求B传输(全双工)
B:I, 0, P=0, 0	——→		; A发0号帧, 可接B的0号帧
	←——	B:I, 0, F=0, 1	; B发0号帧, 可接A的1号帧
B:I, 1, P=0, 1	——→		; A发1号帧, 可接B的1号帧
B:I, 2, P=0, 1	——→		; A发2号帧, 可接B的1号帧
	←——	B:I, 1, F=0, 3	; B发1号帧, 可接A的3号帧
B:I, 3, P=0, 2	——→		; A发3号帧, 可接B的2号帧
	←——	B:I, 2, F=1, 4	; B发最后2号帧, 可接A的4号
B:I, 4, P=0, 3	——→		; A发4号帧, 收妥B的2号帧
B:I, 5, P=1, 3	——→		; A发5号帧, 要求B的确认
	←——	B:RR, F=1, 6	; B确认A的5号帧
	.....		; 双方继续交换信息

☆ 拆除链路

A站	方向	B站	说　　明
	←—	B:RD	；B请求拆链
B:DISC	—→		；A命令拆链
	←—	B:UA	；B对拆链进行确认

（5） 规程分析

★ HDLC 统一的帧格式：数据、命令和响应具有统一格式，易于实施；

★ 采用“0”比特插入法： 支持任意的比特流传输，提高了信息传输的透明性；

★ 采用窗口机制和捎带应答，支持全双工工作方式，提高信息传输的效率；

★ 采用帧校验序列，以及窗口序号的设置，提高信息传输的正确性和可靠性。

数据通信具有质和量的要求！

质（正确性）—差错处理；量（信道利用率）—多路复用等。

起因：用户操作具有间断性；

目的：使得多路信号可以共用一个信道，

将多路信号组合在一条物理信道上传输，充分利用信道容量。

原理：当物理信道的可用带宽超过单个原始信号的带宽时，

将物理信道的总带宽分割成若干个和被传输的单个信号带宽相同（或者略宽一点）的子信道，并利用每个子信道传输一路信号，达到多路信号共用一个信道的目的，节省线路资源。

技术支持：组合和分离不同用户的信息。

(1) 频分多路复用（FDM）

频分多路复用主要用于模拟信道的复用（铜线、微波线路）

原理：对整个物理信道的可用带宽进行分割，并利用载波调制技术，实现原始信号的频谱迁移，使得多路信号在整个物理信道带宽允许的范围内，保证在频谱上不重叠，从而共用一个信道。

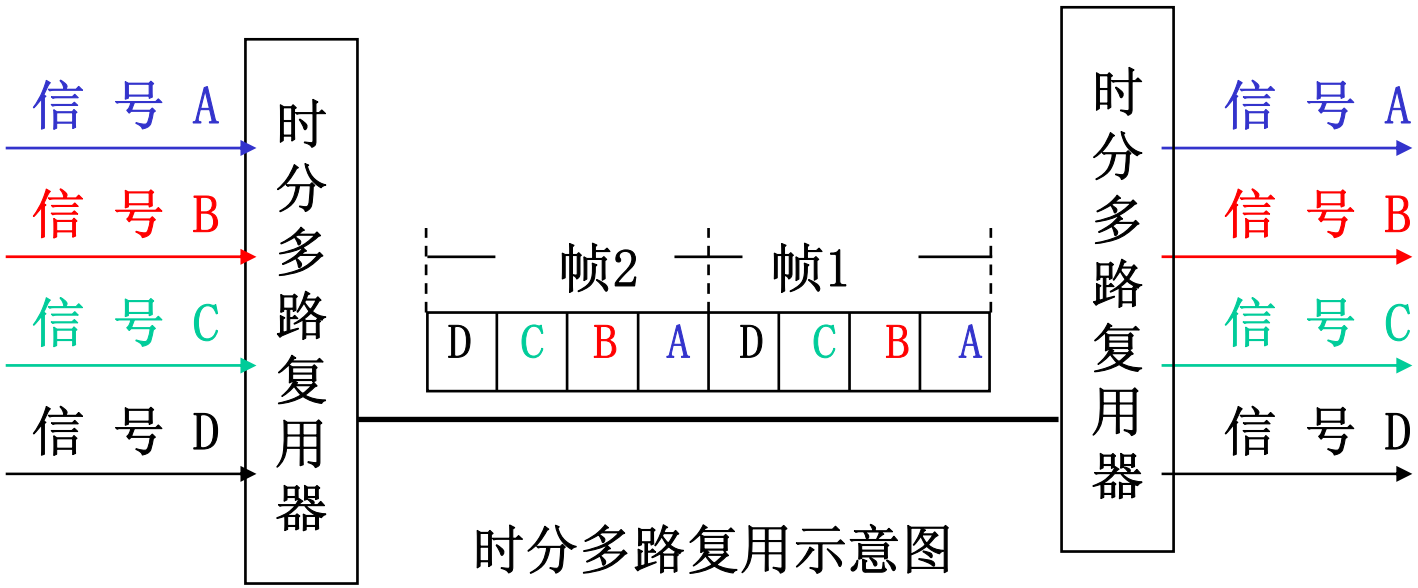
频分多路复用示意图

（2）时分多路复用（TDM）

时分多路复用主要用于数字信道的复用；

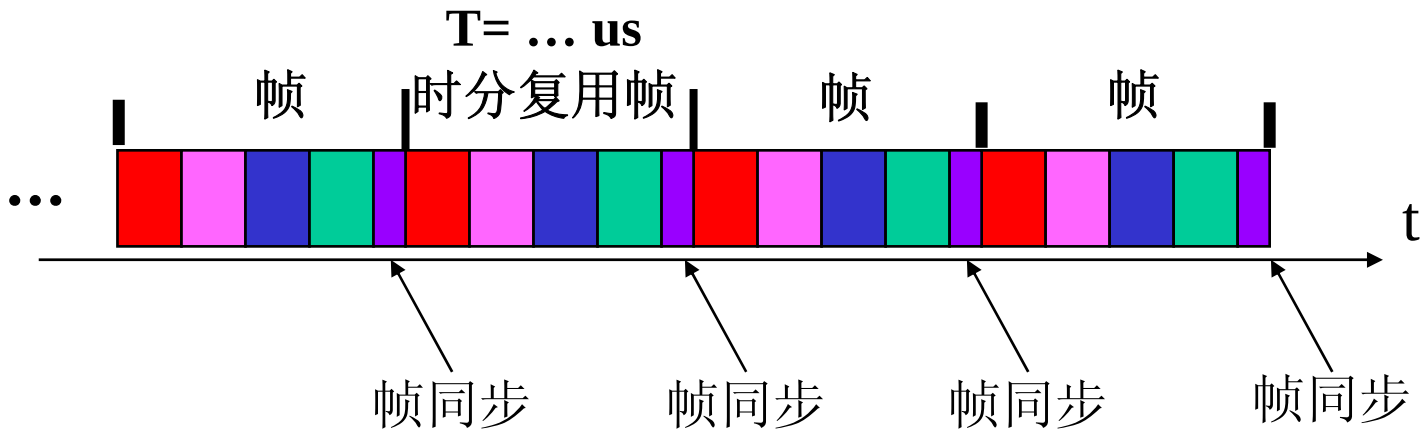
原理：当物理信道可支持的比特传输速率（bps）超过单个原始信号要求的数据传输速率时，可以将该物理信道划分成若干时间片，并将各个时间片轮流地分配给多路信号，使得它们在时间上不重叠。

习惯上，将各子信道组合的结果称之为‘帧’。



时分多路复用示意图

时分多路复用系统示意图

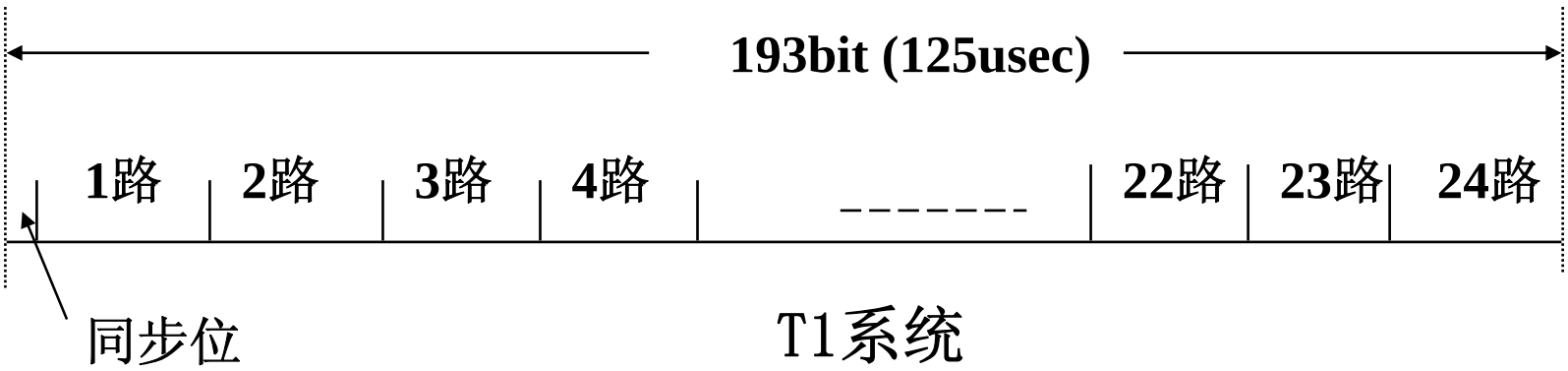


复用数

若：X位/帧，帧/Y微秒，则线路速率＝X/Y，用户速率≈X/YN

★ T1系统（北美）：24路/帧 、8bit/路 、帧/125微秒，
帧 长 度：24×8＝192bit + 1（同步位），
传输速率：193/125微秒＝1.544Mbps （1.536Mbps）

借助T1系统的语音传输：
适用频率：4Khz；采样频率：8Khz（1次采样/125us）；
量化级：256（8位）— 传输速率：64Kbps；
24路语音信息的传输。

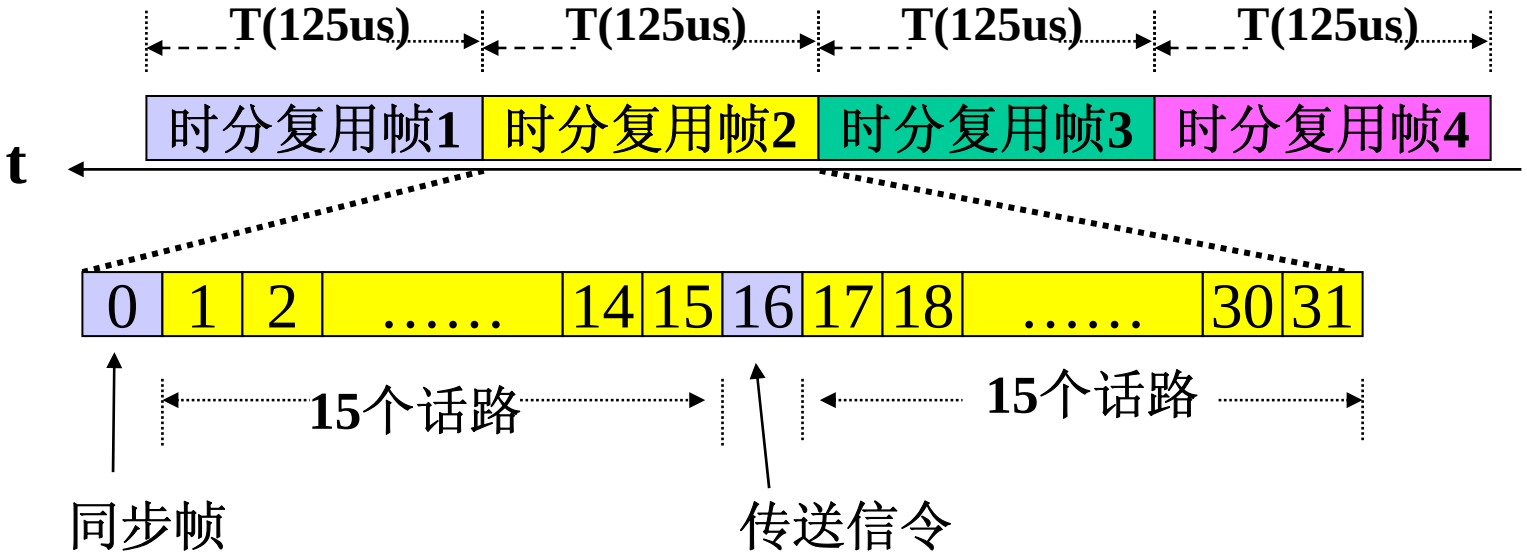


★ E1系统（欧洲）：32路/帧、8bit/路、125微秒/帧

传输速率： 32×8/125微秒＝2.048Mbps

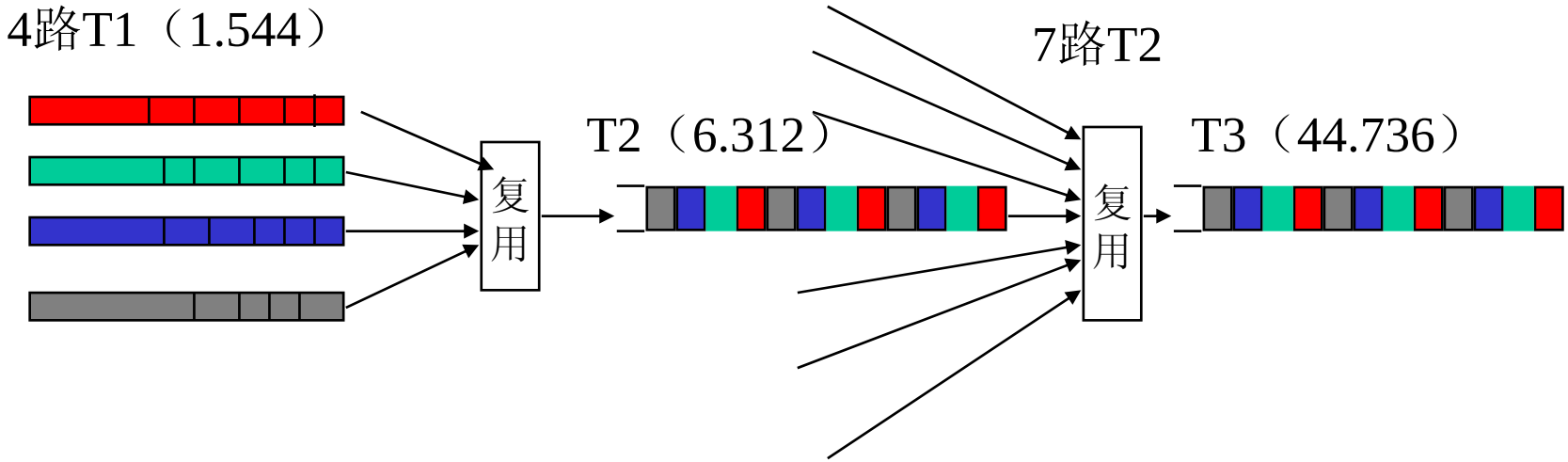
0路和16路用于同步和控制信号。

E1系统可支持30路语音信息的传输。



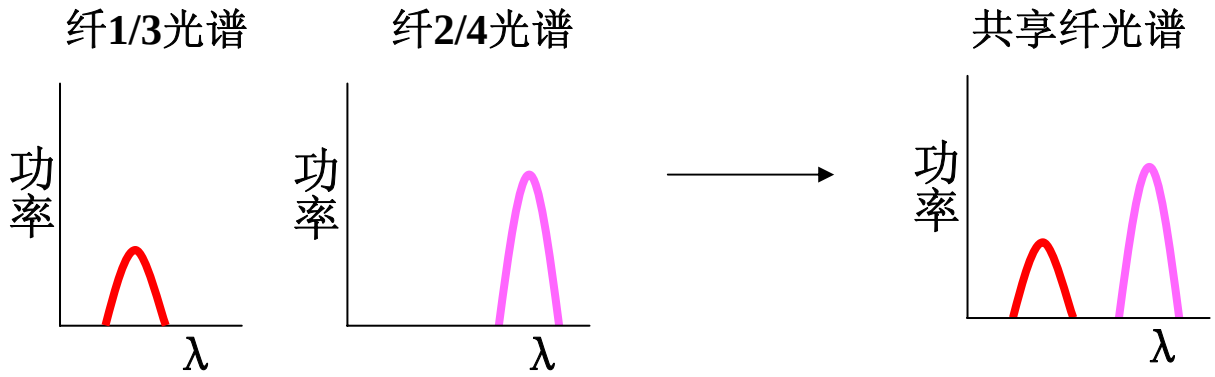
TDM技术支持更多路信号的复用

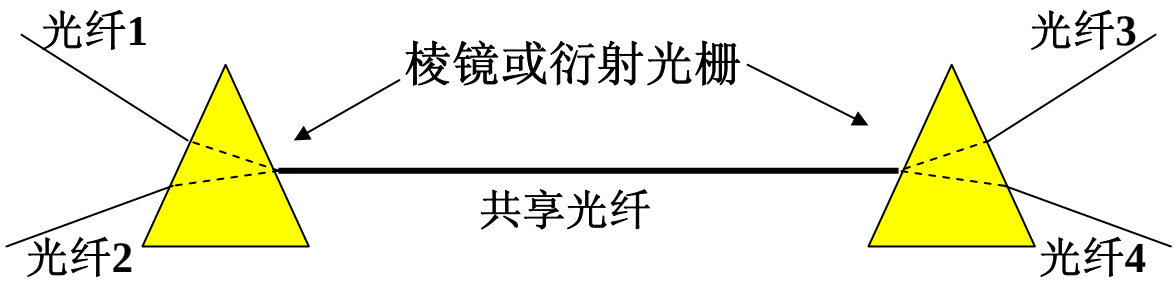
T4 = 6*T3 = 6*7*T2 = 6*7*4*T1 = 274.176 Mbps



（3）波分多路复用（WDM）

波分多路复用主要用于光纤信道；
原理：类似频分多路复用（FDM），将不同路信号调制成不同波长的光，并借助同一光纤信道传输；接收端进行光分离处理。





（4） 集中传输 （对多路复用技术的改进）

多路复用的特点：各个子信道（频分多路复用中的子频段，时分多路复用中的时间片，波分多路复用中的波长） 被静态地分配给各路信号传输，接收方可以直接通过识别固定子频段、时间片或者波长来完成信号分离。

不足之处：信道利用率不够高，信号的传输往往是间断的，在某个时刻，子信道会出现空闲状态（无数据）

解决办法：集中传输！

集中传输：动态按需分配子信道

问题1：如何区分子信道的数据？

解决方法：增加地址标识；

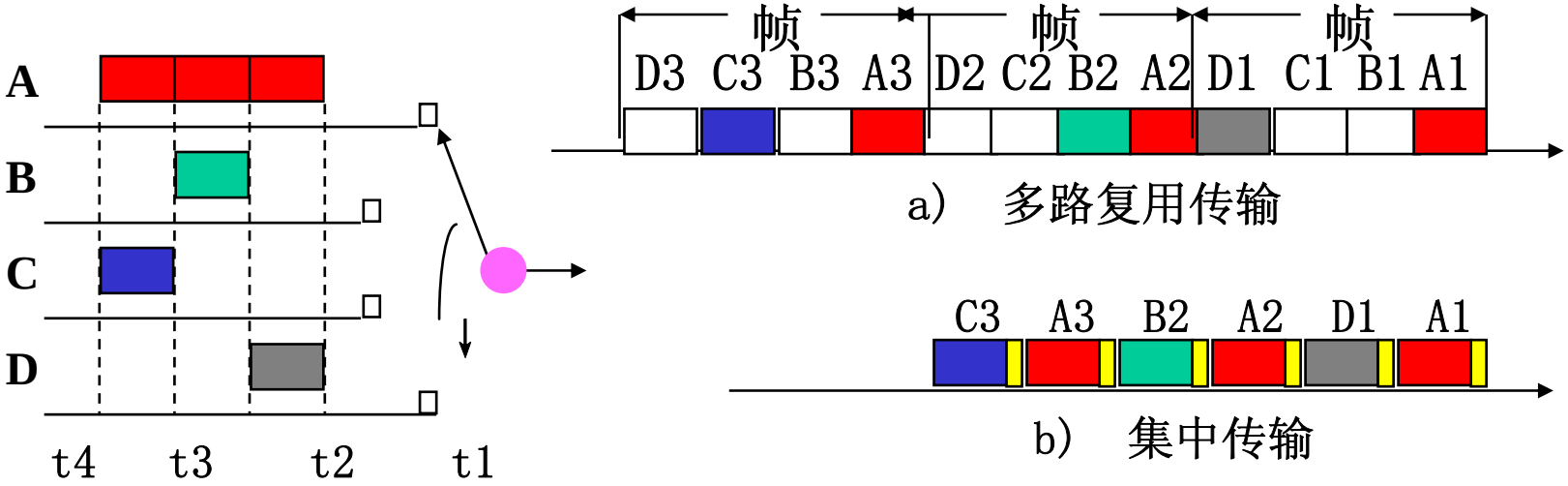
结果：子信道可动态分配给不同用户，系统可以容纳更多用户；

问题2：瞬时输入可能大于总的输出，产生信息丢失；

改进：　集中传输设备具有缓冲存储的能力，

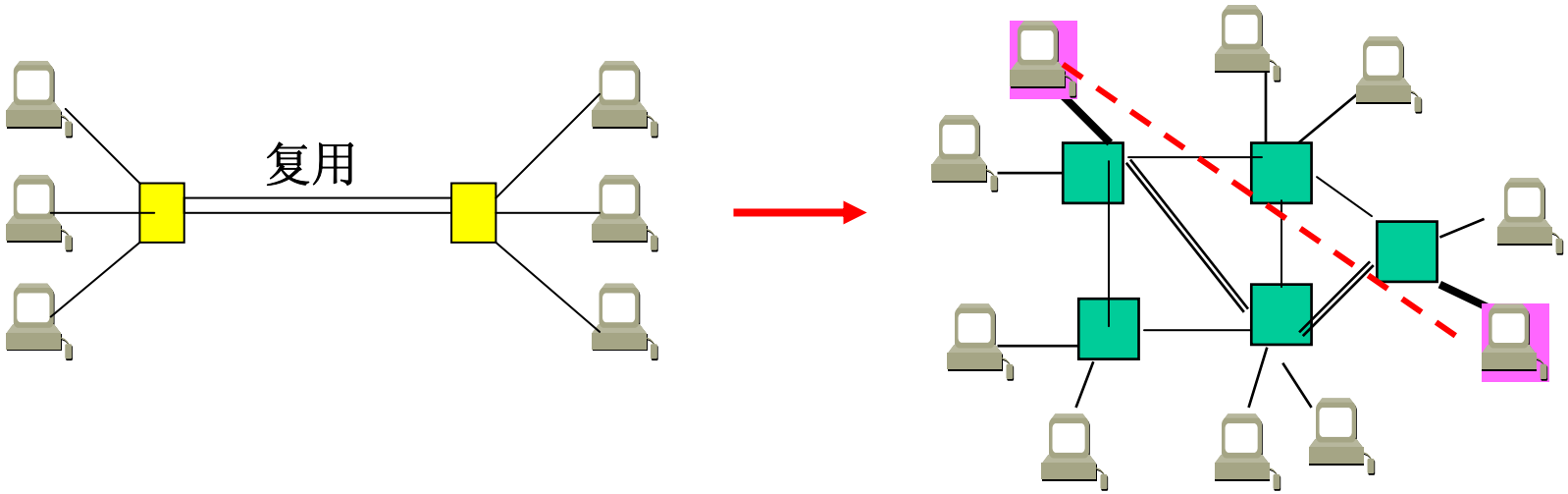
　　临时保存输入的信息，并等待空闲的信道。

称呼：异步时分多路复用或者统计多路复用技术；



时分多路复用 和 集中传输 的 比较

限于媒体的长度和成本限制，为容纳更多的用户，实际通信采用多点接续方式进行，中间结点执行数据交换的过程。



中间结点（交换设备）：不关心被传输的数据内容，仅执行数据交换的动作，将数据从一个端口交换到另一端口，继而传输到另一台中间结点，直至目的地。

数据传输的过程实质上是数据交换的过程。

结点：用于数据交换的中间设备，

站点：发送和接收数据的终端设备。

数据交换方式：线路交换、存储交换（报文交换和分组交换）

（1） 线路交换 （电路交换）

原理：站点之间建立物理通路，无中间存储，类似于电话系统；
过程(三阶段)： 建立线路、占用线路并传输数据、释放线路。

建立线路：发起方站点向接收方站点发送请求，该请求将通过中间结点传输至终点；

如果中间结点有空闲的输出线路（端口），分配线路，接受并下传请求，直至终点。否则拒绝请求，并释放已建线路。

线路一旦分配，在未释放前，将不能被其它站点所使用，即使线路上并没有数据传输。

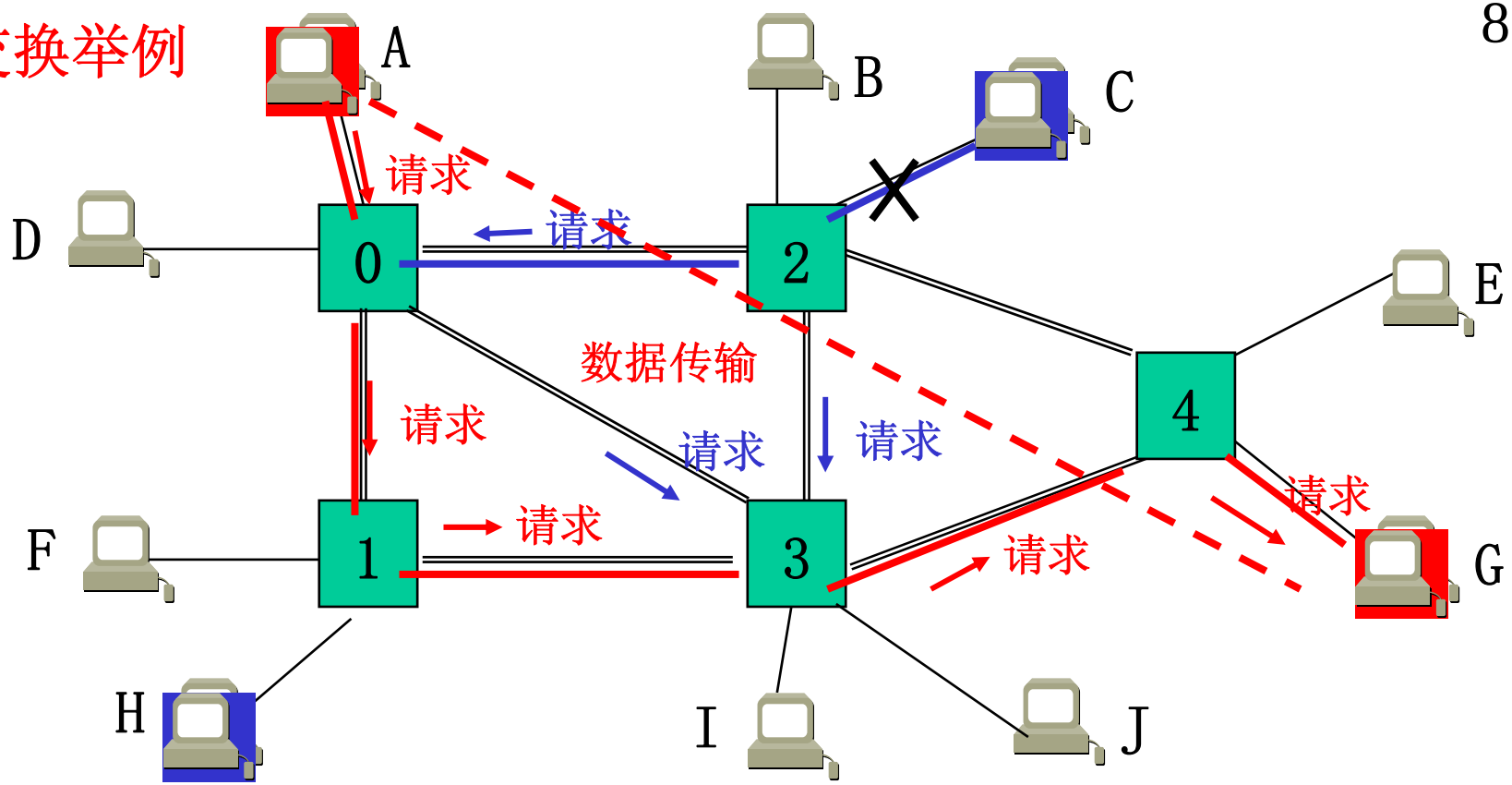
数据传输：物理线路建立后，站点之间进行数据传输。

释放线路：站点之间的数据传输完毕，执行释放线路的动作。

可以由任一站点发起，释放线路请求通过途径的中间结点送往对方，释放线路资源。

线路被释放之后，进入空闲状态，可由其它站点通信所用。

线路交换举例



线路交换的特点：

★ 独占性，线路的利用率较低，易于引起建链时的拥塞；

★ 实时性好，传输延迟小（近似线速，使用整个线路资源）；

★ 线路交换不提供任何缓存装置，数据透明且按序传输；

★ 收发双方自动进行速率匹配（交换机设备比较简单）。

（2） 存储交换—报文交换 （存储－转发报文交换）

指导思想：利用结点的存储能力来提高线路利用率；

中间结点由具有存储能力的计算机承担；

用户信息（报文）附加目的地地址，并传递给中间结点；

中间结点暂存报文，根据地址确定输出端口，排队等待线路空闲时再转发给下一结点，直至终点。

特点：“存储－转发”。

★ 不独占线路，

★ 多个用户的数据可以通过存储和排队共享一条线路，

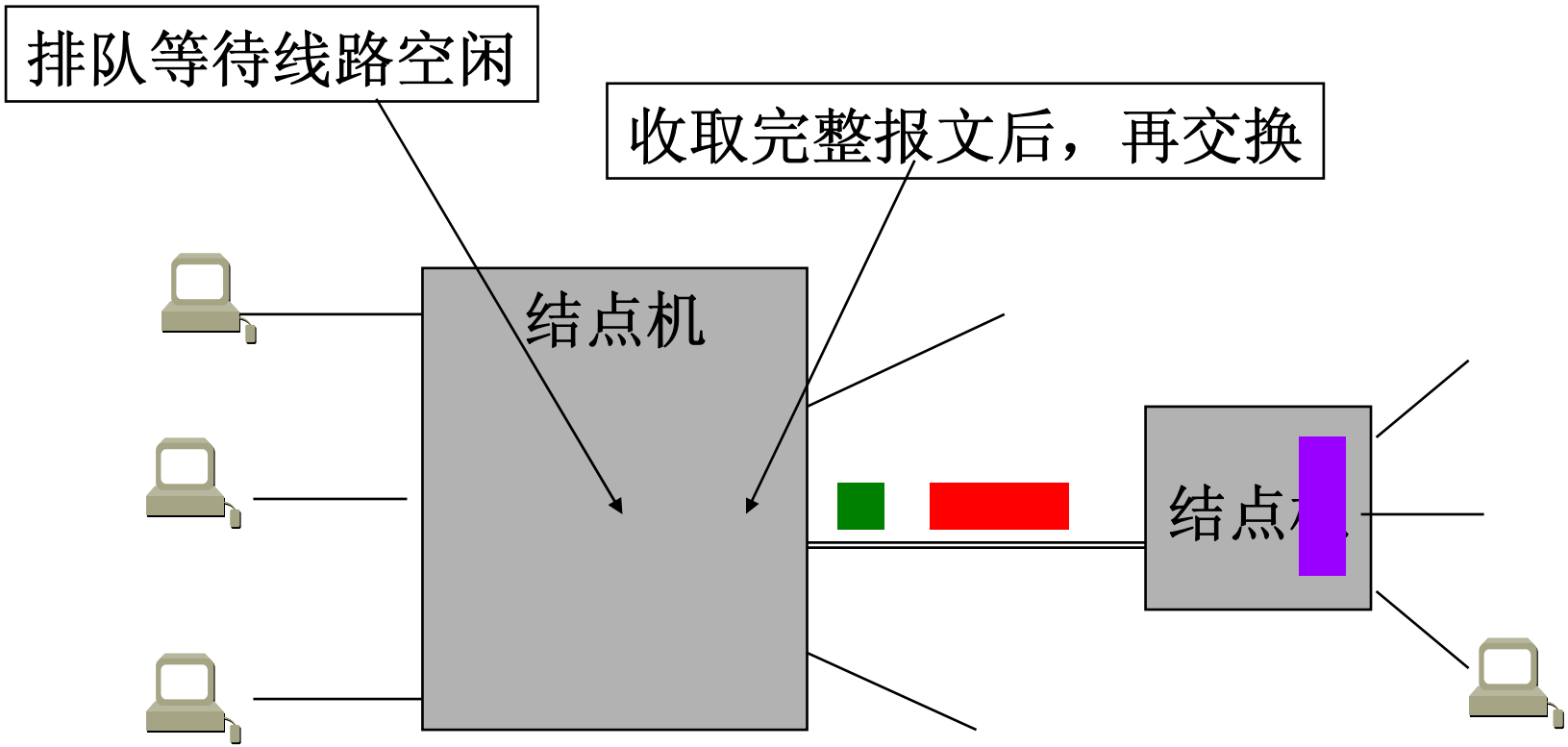
★ 无线路建立的过程，提高了线路的利用率；

★ 报文中增加地址字段，结点根据地址字段进行复制和转发；

★ 可以支持多点传输（一个报文传输给多个用户）；

★ 中间结点可进行数据格式的转换，方便接收站点的收取；增加差错检测功能，避免出错数据的无谓传输等。

报文传输示意图：



不足之处：

1 “存储—转发”可能浪费后续线路资源（等待完整报文的接收）；

2 报文长度未作规定，报文只能暂存在磁盘上，读取磁盘占用了额外的时间；

3 任何报文都必须排队等待（PIPO,公平性不足）：不同长度的报文要求不同长度的处理和传输时间，即使非常短小的报文（如：交互式通信中的会话信息），也难以预测延迟；

4 报文交换难以支持实时通信和交互式通信要求。

（3） 存储交换—分组交换

结合线路交换和报文交换两者的优点，优化性能；

类似报文交换，只是它规定了交换设备处理和传输的数据长度（称之为分组），将长报文分成若干个小分组进行传输。不同站点的数据分组可以交织在同一线路上传输，提高了线路的利用率。

分组长度固定，中间结点可以采用高速缓存技术来暂存分组，提高了转发的速度。

分组长度有限，可以较早利用后继线路的资源。

分组交换实现的关键：分组长度的选择

分组越小，冗余量（分组中的控制信息等）在整个分组中所占的比例越大，影响用户数据传输的效率；

分组越大，数据传输出错的概率越大，增加重传的次数，影响用户数据传输的效率。

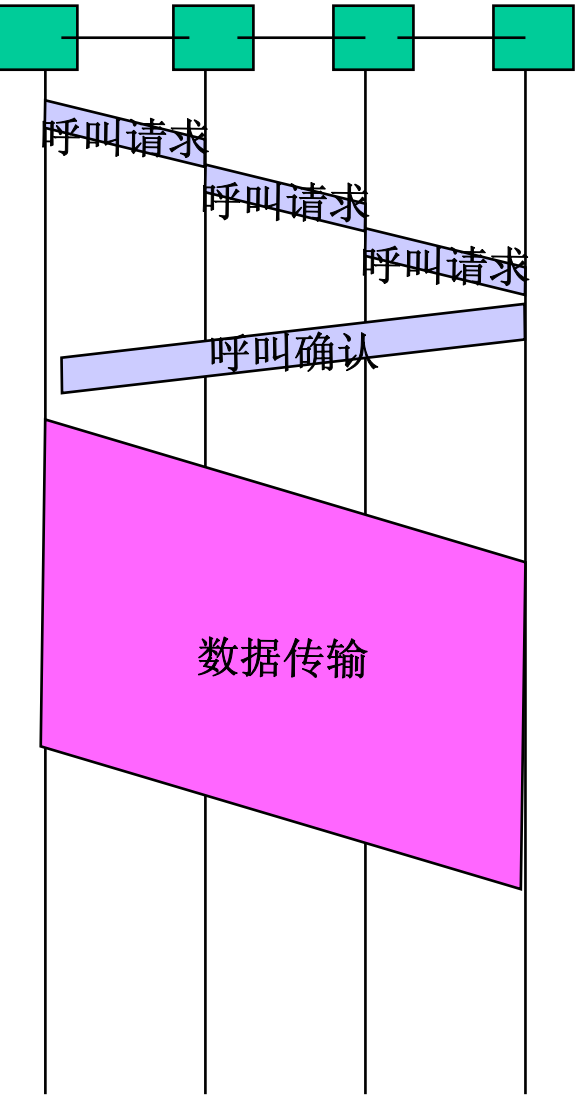
线路质量越好，可支持的分组长度越长。

X.25分组交换网： 分组长度定义为131字节，（包括128字节的用户数据和3字节的控制信息）；

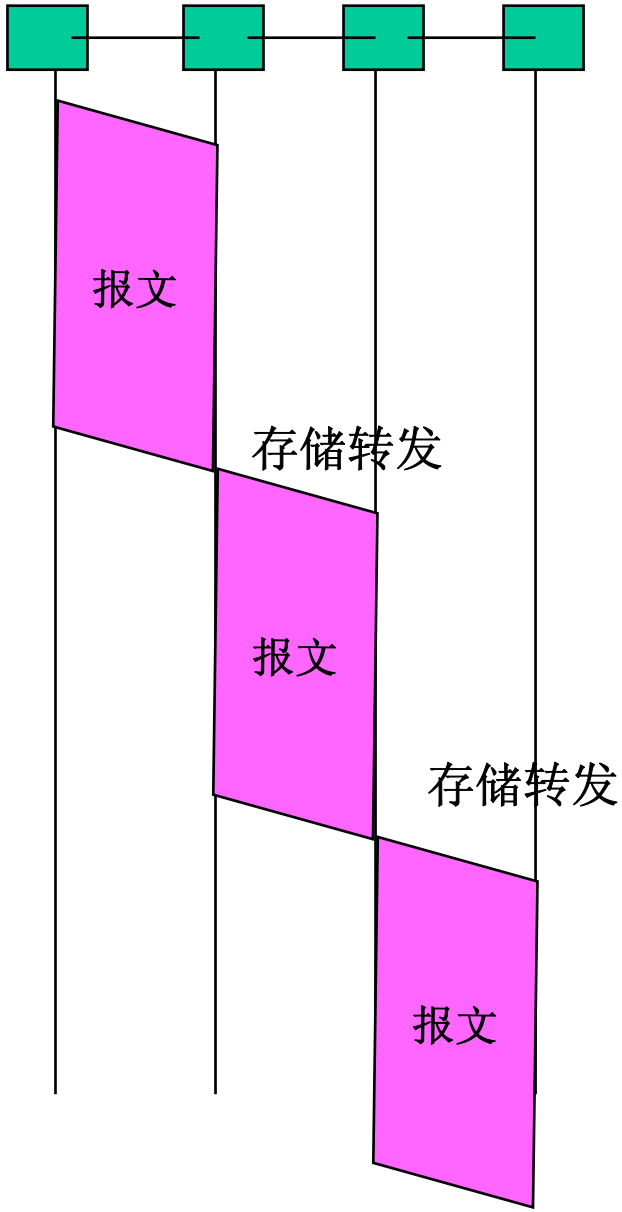
以太网： 分组长度定义为1500字节左右（较好的线路质量和较高的传输速率）；

FDDI网络：约为4800字节（光纤）。

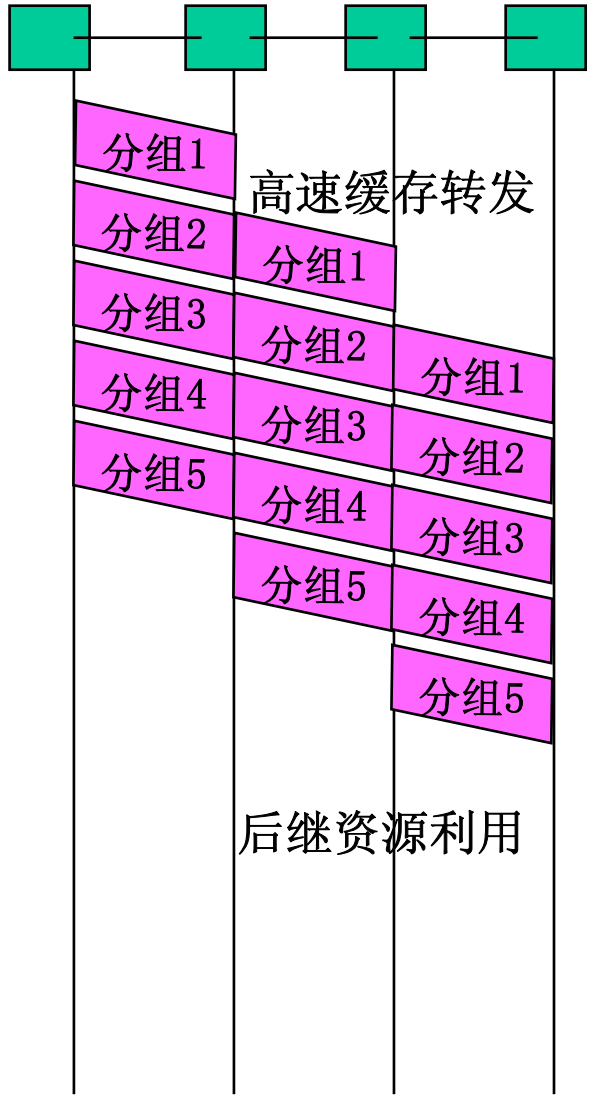
线路交换



报文交换



分组交换



（4） 线路交换和分组交换的比较

1、分配通信资源（主要是线路）的方式：

线路交换：静态分配线路，线路资源浪费，接续困难；

分组交换：动态（按序）分配线路，提高线路利用率；使用缓存技术暂存分组；可能出现内存资源耗尽，而丢弃分组的现象。

2、用户的灵活性：

线路交换：信息传输透明，用户自行定义传输信息内容、速率、体积、格式等，因此可以同时传输语音、数据、图像等；

分组交换：半透明传输，按照分组设备的要求使用基本的参数。

3、数据传输实时性：

线路交换：接续难，传输快；

分组交换：基本满足要求。

4、资费情况：

线路交换网络：依赖通信的距离和使用的时间；

分组交换网络：传输的字节（或者分组）数和连接的时间。

2.12 数据报和虚电路

分组交换技术应用—用户分解报文为分组，网络应解决用户分组流的传输管理问题：数据报和虚电路。

（1） 数据报— 面向无连接的数据传输

借鉴报文交换的思想。传输的分组称为数据报。

数据报的前部具有地址信息字段。网络中的结点根据地址信息和路由规则，独立的选择输出端口，暂存和排队数据报，并在传输媒体空闲时，发往相邻结点，直至最终站点。

当一对站点之间需要传输多个数据报时，由于每个数据报均被独立地路由、排队和传输，在网络中可能会走不同的路径，产生不同的时间延迟。按序发送的多个数据报可能以不同的顺序达到终点。站点必须具有存储和重新排序的能力。

路由技术简介—补充说明

中间结点的目的：对应输入的分组，寻找适合的出口路径予以转发，使该分组可以“尽快”离开网络，到达接收站点。

寻找出口的过程称之为路由选择，对应算法为路由选择算法。

结点处理的一般方法：对应端口，设置缓存区（队列），根据不同的算法，将分组输出到不同的端口，排队等待输出。

算法选择路由的依据：

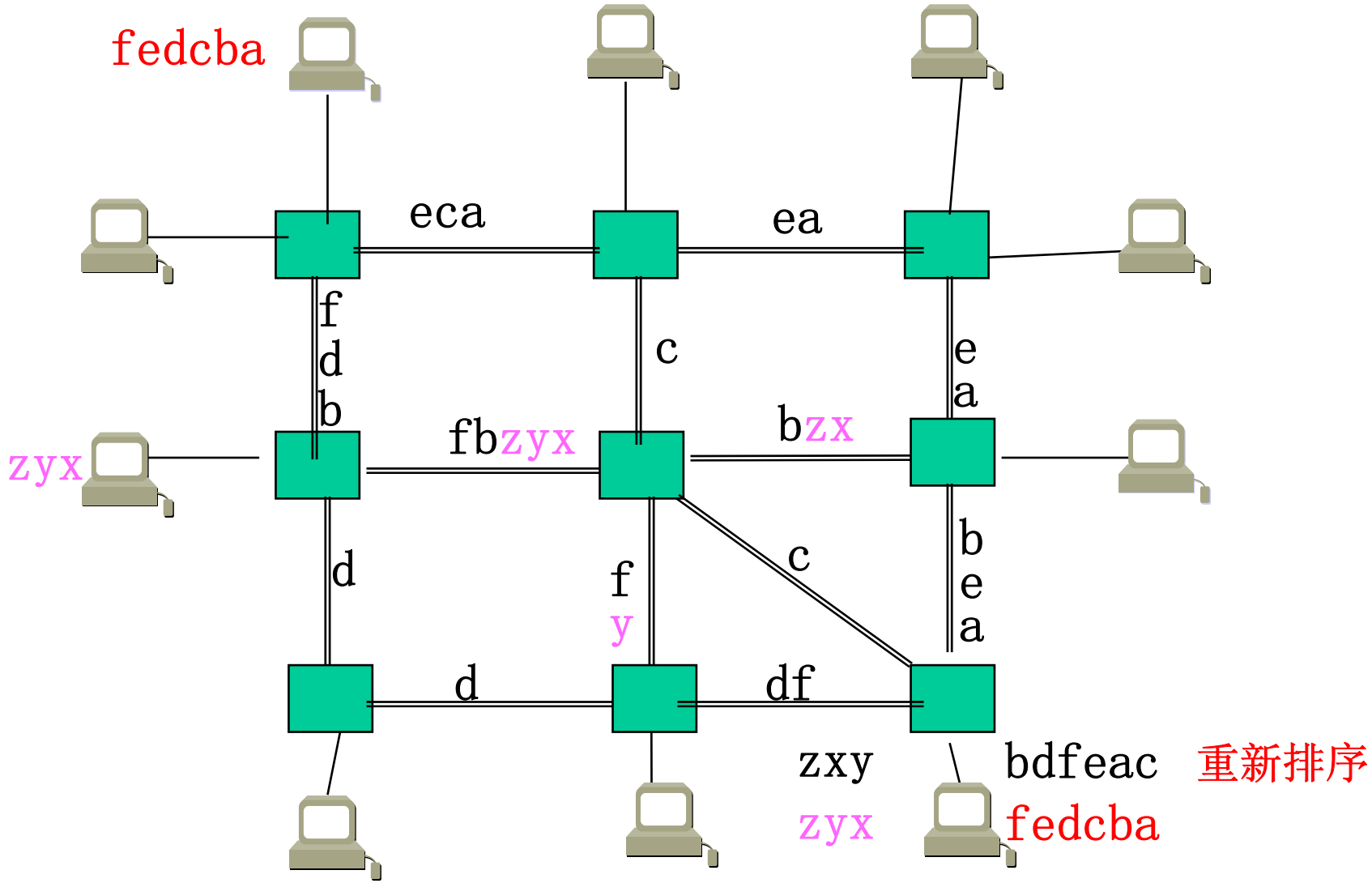
☆ 基于路径的算法：需要收集整个网络的拓扑信息，最短路径的计算。潜在问题：线路是否繁忙？

☆ 基于队列的算法：需要收集线路信息，热土豆算法，尽快输出该结点。潜在问题：多走弯路？

路由算法（具有约束条件的路由）和“缓存队列分配”的研究直接关系到网络本身资源的利用率，吸引众多学者开展研究，未有穷期（本课程略）。

数据报传输示意：

不同站点发出的分组汇聚到网络，分组独立路由导致同一站点发出的分组（数据报）选择不同的路径和不同的投递顺序。



（2） 虚电路——面向连接的数据传输

借鉴线路交换的思想，但电路是虚拟的。

采用多路复用技术，物理媒体被理解为由多个子信道（逻辑信道—LC）组成，子信道的串接形成虚电路（VC），利用不同的虚电路来支持不同的用户数据的传输。

虚电路进行数据传输的过程：

- 虚电路建立：发送方发送含有地址信息的特定的控制信息块（如：呼叫分组），该信息块途经的每个中间结点根据当前的逻辑信道（LC）使用状况，分配LC，并建立输入和输出LC映射表，所有中间结点分配的LC的串接形成虚电路（VC）。

虚电路进行数据传输的过程（续）：

➢数据传输：

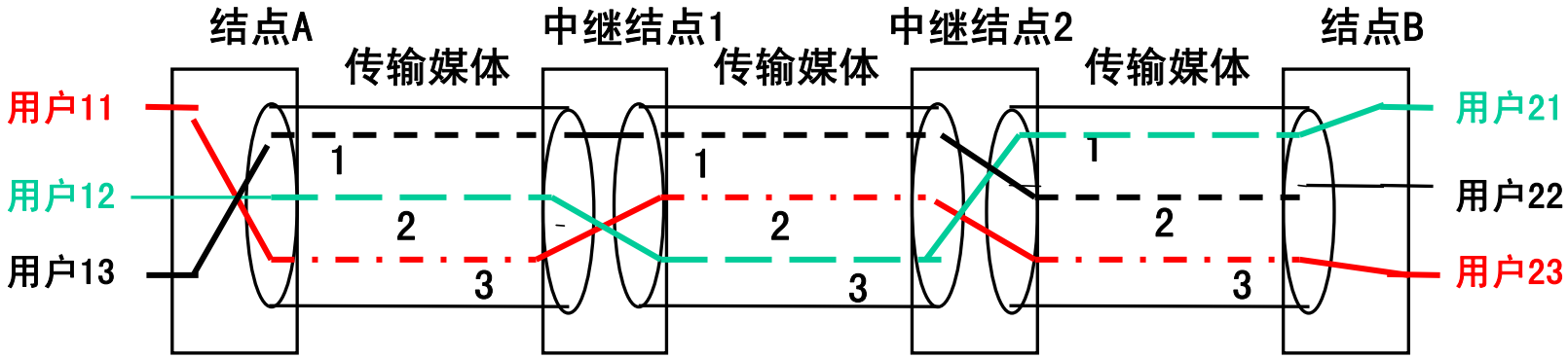
站点发送的所有分组均沿着相同的VC传输，分组的发收顺序完全相同；

分组中只带逻辑信道号，而不带地址。

➢虚电路释放：

数据传输完毕，采用特定的控制信息块（如：拆除分组），释放该虚电路。通信的双方都可发起释放虚电路的动作。

虚电路的形成



VC1（用户11，用户23）= LC1（3）+ LC2（2）+ LC3（3）

VC2（用户12，用户21）= LC1（2）+ LC2（3）+ LC3（1）

VC3（用户13，用户22）= LC1（1）+ LC2（1）+ LC3（2）

虚电路的扩展：

由于虚电路的建立和释放需要占用一定的时间，因此虚电路方式不很适合站点之间具有频繁的、短小数据交换的场合；

永久虚电路PVC 和 呼叫虚电路SVC。

永久虚电路：在两个站点之间事先建立固定的链接，占用固定的逻辑信道，类似于存在一条专用电路，任何时候，站点之间都可以进行通信。

呼叫虚电路：根据需要，动态建立和释放虚电路。

（3） 数据报和虚电路的比较

★ 数据报：

— 传输无需连接建立和释放的过程；

— 每个数据报中需带地址信息（冗余信息），占用信道资源；

— 用户的连续数据块会无序地到达目的地，接收站点予以排序。

— 当使用网状拓扑组建网络时，任一中间结点或者线路的故障不会影响数据报的传输（可以选择不同的路径），可靠性较高。

— 数据报较适合站点之间小批量数据的传输（存储排序占用资源）。

数据报和虚电路的比较（续）：

★ 虚电路：

— 传输需连接建立和释放虚电路的过程；

— 数据分组中仅含少量的地址信息（LC号），用户的连续数据块沿着相同的路径，按序到达目的地；接收站点处理方便。

— 如果虚电路中的某个结点或者线路出现故障，将导致虚电路中断，传输失效。

— 虚电路方式较适合站点之间大块数据的传输（地址冗余量小）。

第3章 计算机网络体系结构和协议

3.1 开放系统互连/参考模式的提出

计算机之间通信的前提：双方遵循数据格式和时序方面的约定（协议）。

计算机通信为基于计算机处理的信息共享创建了基础；

用户的应用需求刺激了有关计算机通信方面的研究；

早期的研究和实现源于计算机厂商，如IBM、DEC公司等；

问题：限于本公司生产的产品的互连通信。

用户不满意：限制了选择的范围；

厂商不满意：难以进入其他厂商已有的领域，限制了产品的通用性和更广阔的市场。

标准国家化和国际化成为大势所趋。

标准化组织

国家标准化组织—国家标准：美国国家标准化协会（ANSI）、中国国家标准委员会（国家技术监督局主管）、…；

区域标准化组织—区域标准：欧洲标准化委员会（CEN）、欧洲计算机制造协会（ECMA），…；

国际标准化组织—国际标准（国家和行业组织作为成员单位）：国际标准化组织（ISO，（电子部标准化技术研究所））、国际电信联盟（ITU，（邮电部标准化技术研究所）），…。

行业/专业标准化组织—行业/业界标准：电子工业协会（EIA）、电气电子工程师协会（IEEE）、因特网工程任务组（IETF），…。

组织的成员：政府代表+研究人员+厂商代表；

标准制定的一般过程：规划阶段（应用需求、厂商建议、授权工程、技术委员会）、研发阶段（研发、验证和草案）、获批阶段（成员投票、修正完善、形成标准）、发布阶段（诞生新标准）。

国际标准通常每4—5年予以复审，推陈出新。

我国的国家标准

国家技术监督局统一指导，中国国家标准化委员会负责实施：

- 等同采用：直接引用国际标准（翻译）；
- 等效采用：技术内容和编写风格略有差异；
- 参照采用：根据国家特点，参照国际标准，制定国家标准。

国家标准以GB XXXX的形式公布。

计算机网络（包括信息技术）方面标准均为等同采用。

其他说明：

标准滞后于实物（研究成果的总结和归纳）；

标准具有时效性（新工艺和新技术对原有标准的改进—刷新）；

标准的制订者：研究人员、厂商代表（具体实施者）；

厂商的重要性：验证标准，标准产业化；

厂商可能的排他性：市场因素。

开放系统互连/参考模式的提出

为促进厂商的网络的互联和户互操作，**ISO于1974年提出计算机网络体系结构和参考模型，以此作为网络标准化活动的基础。**

—开放系统互连参考模式（OSI/RM）

Open System Interconnection / Reference Model

网络体系结构：定义和表述网络设备及相关软件如何交互作用的逻辑结构，包括通信协议、报文格式、互操作规范等。

遵循相同体系结构的网络产品具有兼容性。

对应体系结构/参考模型的总体要求

★ 支持异种计算机之间的通信；

★ 支持各种通信媒体（现有的和未来的）；

★ 支持各种业务处理（现有的和未来的）；

★ 支持高级的人机接口（方便用户使用）；

★ 具有可扩充的能力，适应发展的需要。

3.2 ISO的网络标准设计原理（OSI/RM）

★ 设计思想：抽象

标准的本身应当独立于实现的环境。

确定总体框架和模块的接口方式（如：OSI/RM）；

确定模块的外观特性（可提供的服务）；

确定模块的协议规范（确保服务可提供时应遵循的规则）；

协议：定义数据交换的语法、语义和时序。

★ 设计方法：分解

将整个系统分解为若干易于实现和控制的子模块，并通过对各子模块的功能、交换的数据结构和时序进行约定（协议），协调模块之间的动作，保证系统设计的合理性和互操作性。同时根据子模块间的依赖关系，采用具有层次结构的模型与之对应。

★ 模块划分的原则

— 独立性：减少模块间交互的信息，降低依赖性；

— 单向性：模块间的引用坚持单向性，降低实现难度；

该原则导致系统本身体现层次性（层次结构）；

— 增值性：各模块在使用下层服务的基础上，完成特定的通信功能，提供增值服务；

— 同构性：互连的系统应当具有相同的层次结构；

— 适用性：同构系统的相同层次之间才能进行有意义的通信，并借助于下层服务予以实现。

OSI的最大优势：引入层的概念，在定义接口的基础上，各层可以独立设计、更新，甚至替换。

★ OSI/RM的层次——七层体系结构：

— 物理层（PH），确定物理设备接口，提供点－点的比特流传输的物理链路；

— 数据链路层（DL），利用差错处理技术，提供高可靠传输的数据链路；

— 网络层（N），利用路由技术，实现用户数据的端－端传输；

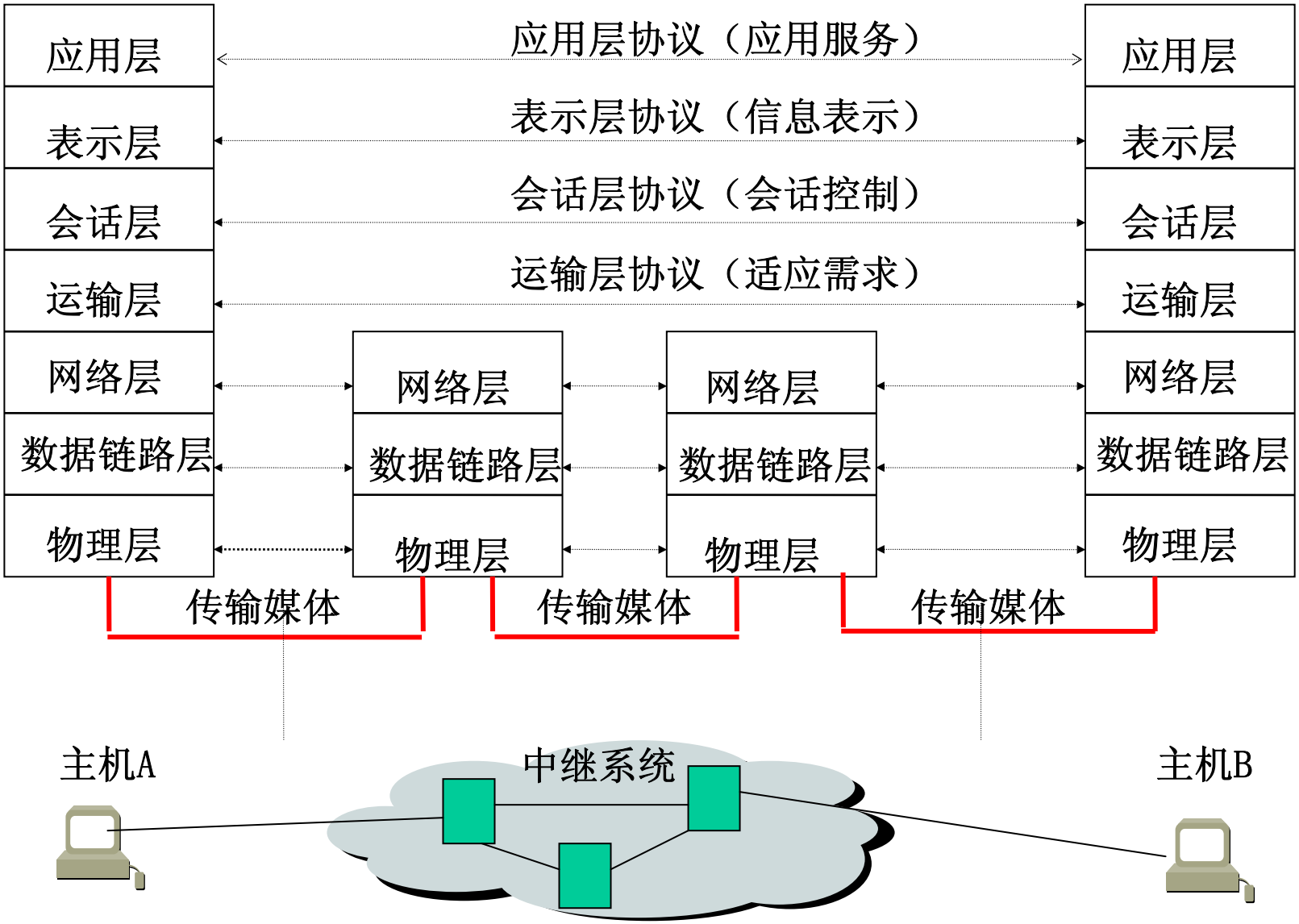
— 运输层（T），屏蔽通信子网差异，以及用户要求和网络服务之间的差异；

— 会话层（S），提供控制会话和数据传输的手段；

— 表示层（P），解决异种系统之间的信息表示问题，屏蔽不同系统在数据表示方面的差异；

— 应用层（A），利用下层的服务，支持各种应用服务要求。

OSI层次示意图


应用层
表示层
会话层
运输层
网络层
数据链路层
物理层
应用层协议（应用服务）
表示层协议（信息表示）
会话层协议（会话控制）
运输层协议（适应需求）
网络层
数据链路层
物理层
网络层
数据链路层
物理层
应用层
表示层
会话层
运输层
网络层
数据链路层
物理层
传输媒体
传输媒体
传输媒体
主机A
中继系统
主机B

★ 对应电话的层次体系解释：

物理层：话机—交换机—交换机—话机的点到点物理连接；

数据链路层：点到点连接的可靠性（话音质量）；

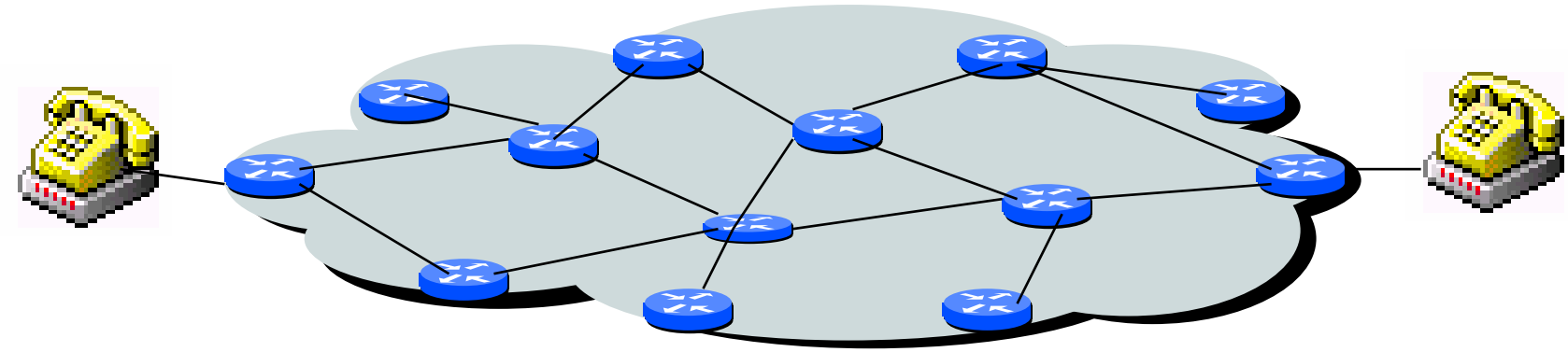
网络层：交换机的协作，支持话机—话机的沟通；

运输层：需求和支持能力的匹配；

会话层：会话时序控制（习惯）；

表示层：表达语言的匹配（包括翻译）；

应用层：商讨具体事务。



3.3 OSI的相关术语

（1） 一般术语

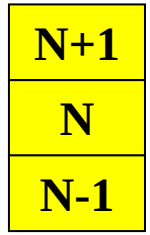
*“开放”：*所遵循的标准是开放的（任何人都可以参照）；遵循标准开发的系统是开放的（可以和任意地方、任意系统进行通信，只要该系统也遵循相同的标准）。

*“开放系统”：*依据OSI标准开发的硬软设施的总称。

*“开放系统互连”：*彼此开放的系统通过联合使用适当的OSI标准进行的信息交换。

开放系统互连参考模式/模型（OSI/RM）：供设计开放系统时参考的模型。

一般术语（续）



“层”：开放系统的逻辑划分，指功能上相对独立的一个子系统。

（N）层表示OSI层次结构中的任一层；

（N＋1）/（N－1）层分别表示指定层次的上邻层/下邻层。

“层功能”：本层具有的通信能力（内在通信能力，标准指定）；

“层服务”：本层向上邻层提供的通信能力。根据OSI增值服务的原则，本层的服务应是下邻层服务与本层功能之和。

即：　（N）服务＝（N）功能＋（N－1）服务

“层协议”：为保证层功能的实现和层服务的提供而定义的一组有关通信方面的、在语义、语法和时序方面的约定。同一层次中可能定义多个协议，只有执行相同协议的系统之间才能进行通信。

“层实体”：层功能实现的真正承担者（相应的硬软件）。

“层用户”：层服务的使用者（上邻层实体）。

（2） 服务原语

层服务被引用的工具。服务原语由原语名和原语参数两部分组成（类似编程时的程序调用和参数传递）。服务原语主要分为两大类：

无确认的原语类型：发出的请求原语无需对方予以确认。

XXXX.REQ ——→ XXXX.IND

有确认的原语类型：发出的请求原语要求得到确认。

XXXX.REQ ——→ XXXX.IND
XXXX.CNF ←—— XXXX.RSP 或

XXXX.REQ ——→ XXXX.IND
XXXX.CNF

服务原语确定了相邻层次之间的接口。

上邻层利用服务原语来通知下邻层要做什么；

下邻层利用服务原语来通知上邻层已做了什么。

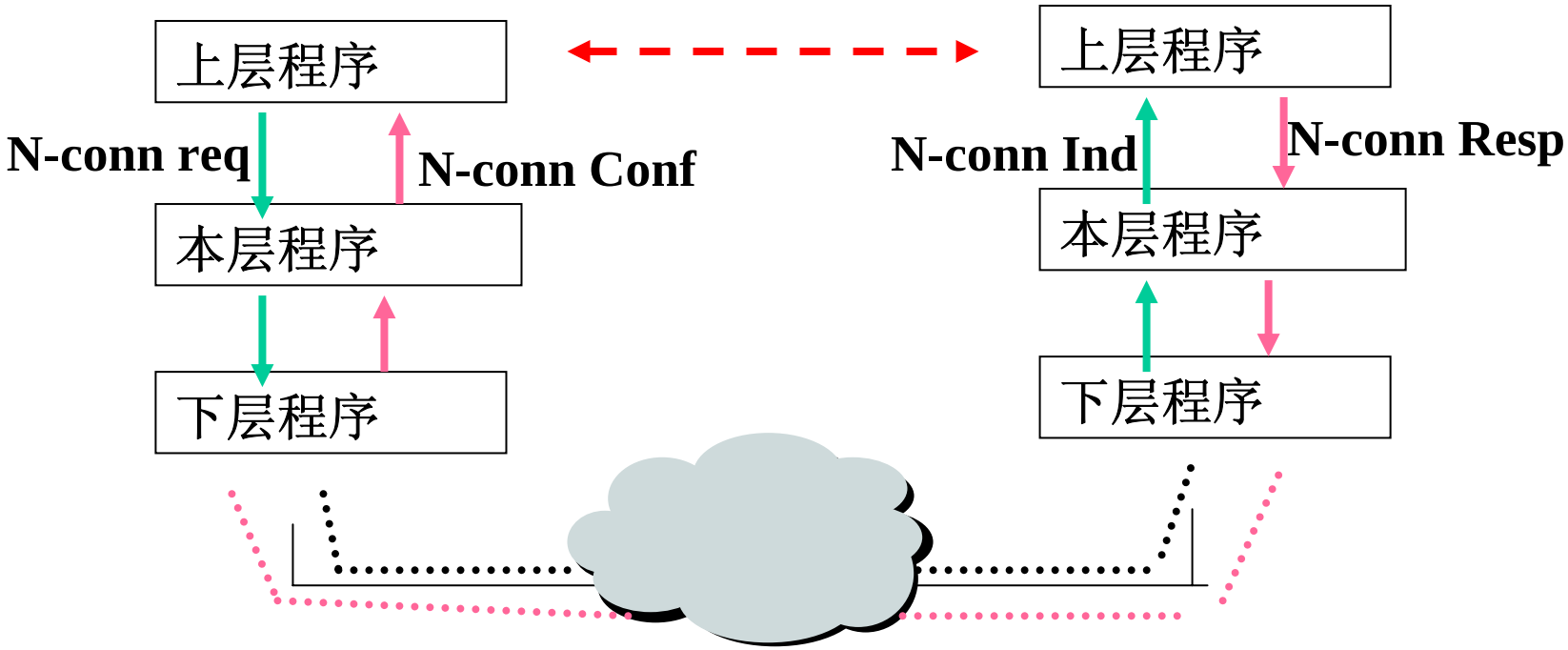
OSI标准仅定义了服务原语的内容。

服务原语举例（网络层原语）：

N-conn Req/Ind	01	N-conn Resp/Conf	02
N-data Req/Ind	03	N-disc Req/Ind	04

原语及参数：

原语使用：



（3） 层间通信

★ 相邻层之间通信：

相邻的上下层之间的通信；属于局部问题，标准中只定义了通信的内容（服务原语），未规定这些内容的具体表现形式和层间通信实现的具体方法。

★ 对等层之间通信：

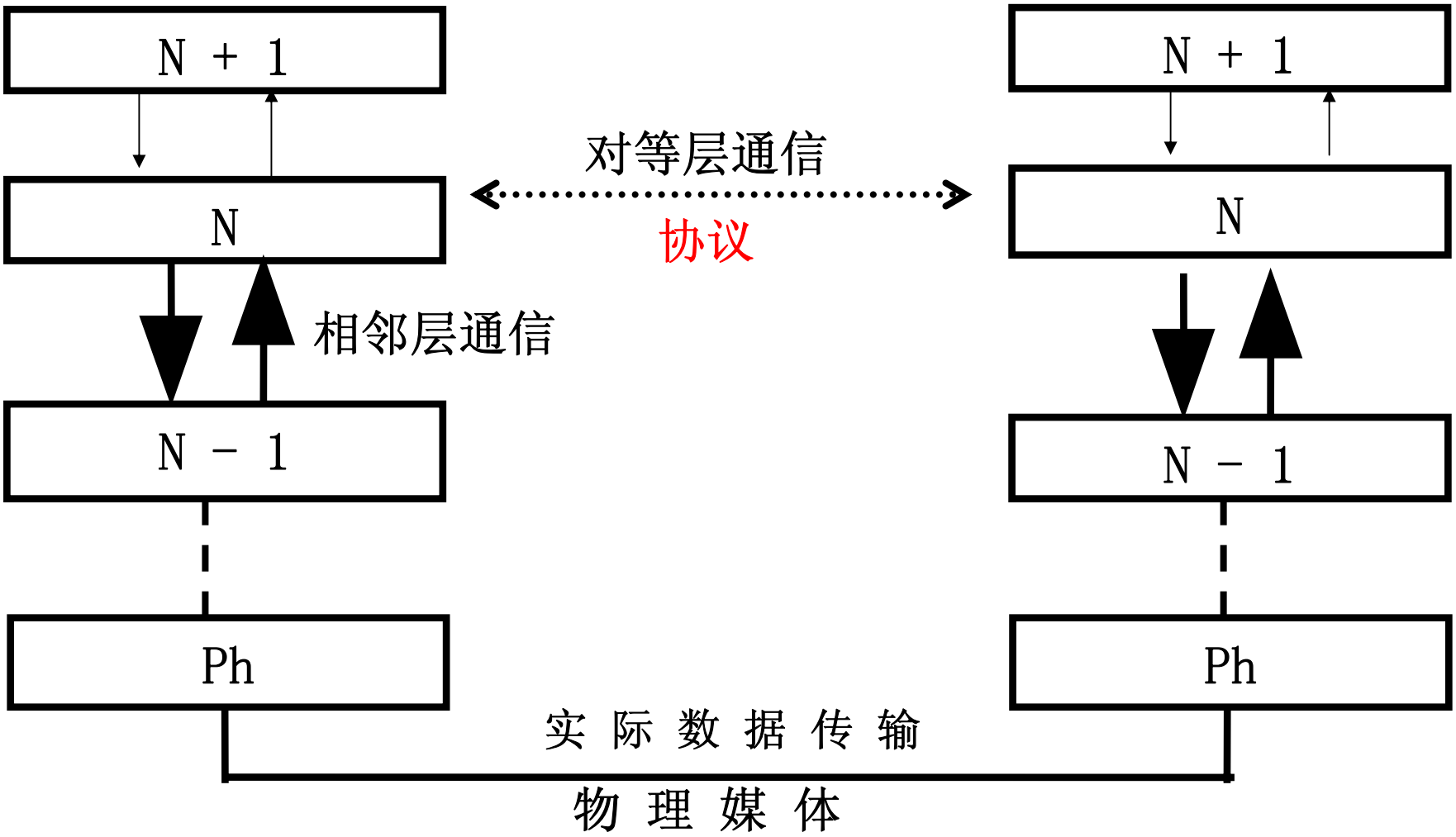
不同开放系统中的相同层次之间的通信，对等层实体之间的信息交换；

OSI标准为每一层的通信都严格定义了协议数据单元的格式。

对等层之间的通信是目的，（对等层实体的协作保证该层功能和服务的实现）；

相邻层之间的通信是手段，（保证对等层实体之间的通信得以实施）。

OSI环境下的层间通信示意图



（4） 数据类型

数据单元（DU）：OSI环境中交换的数据。

服务数据单元（SDU）： 相邻层间交换的数据单元，SDU为服务原语的表现形式。

接口数据单元（IDU）： 相邻层界面上体现的数据单元，

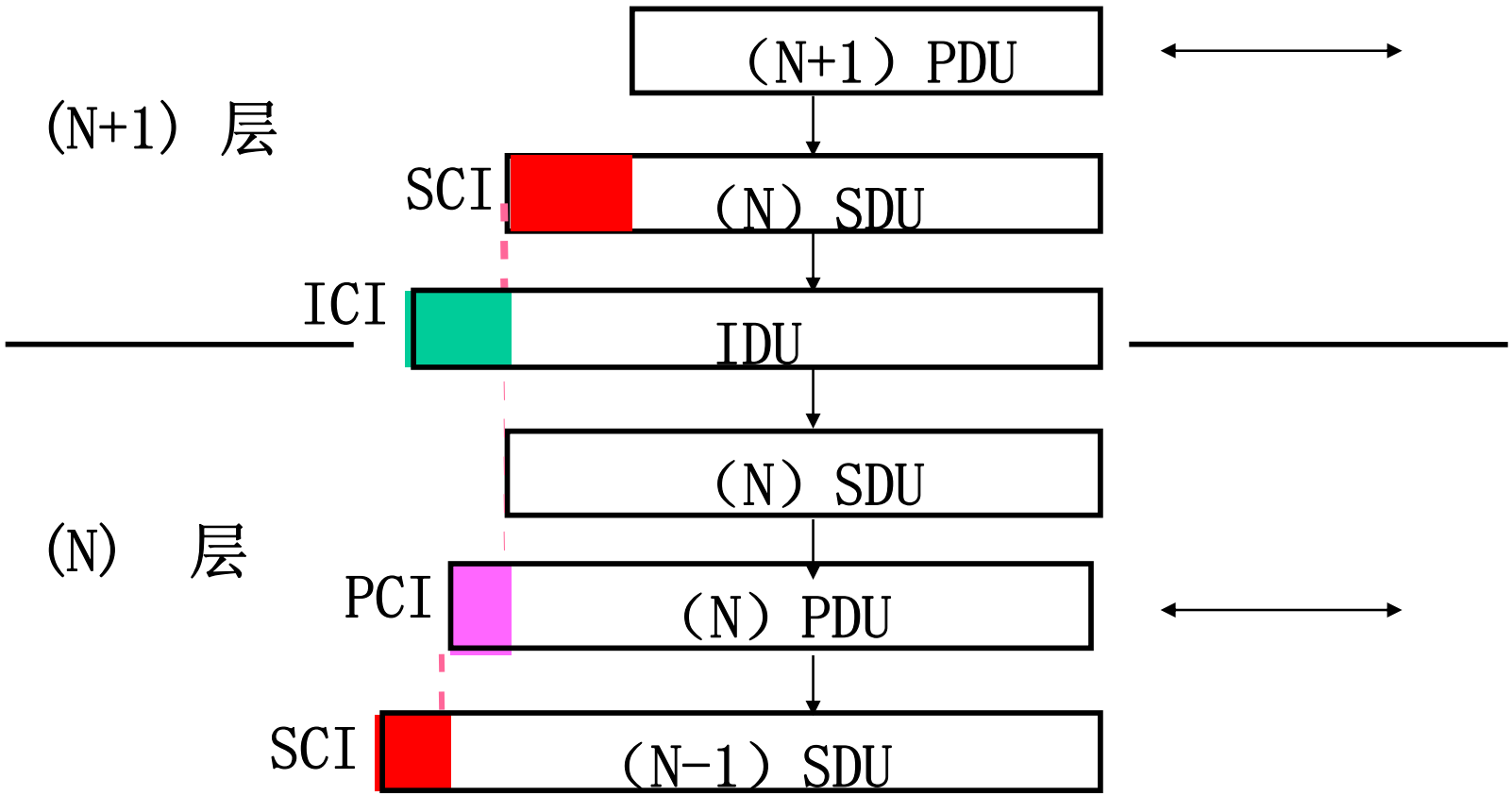
IDU ＝ SDU ＋ 接口控制信息。

*协议数据单元（PDU）：*对等层间交换的数据单元，

PDU的内容和格式由协议精确地定义。

（N）PDU作为（N－1）SDU的一部分，传递给下层，直至对等层实体。

OSI环境下数据单元之间的关系

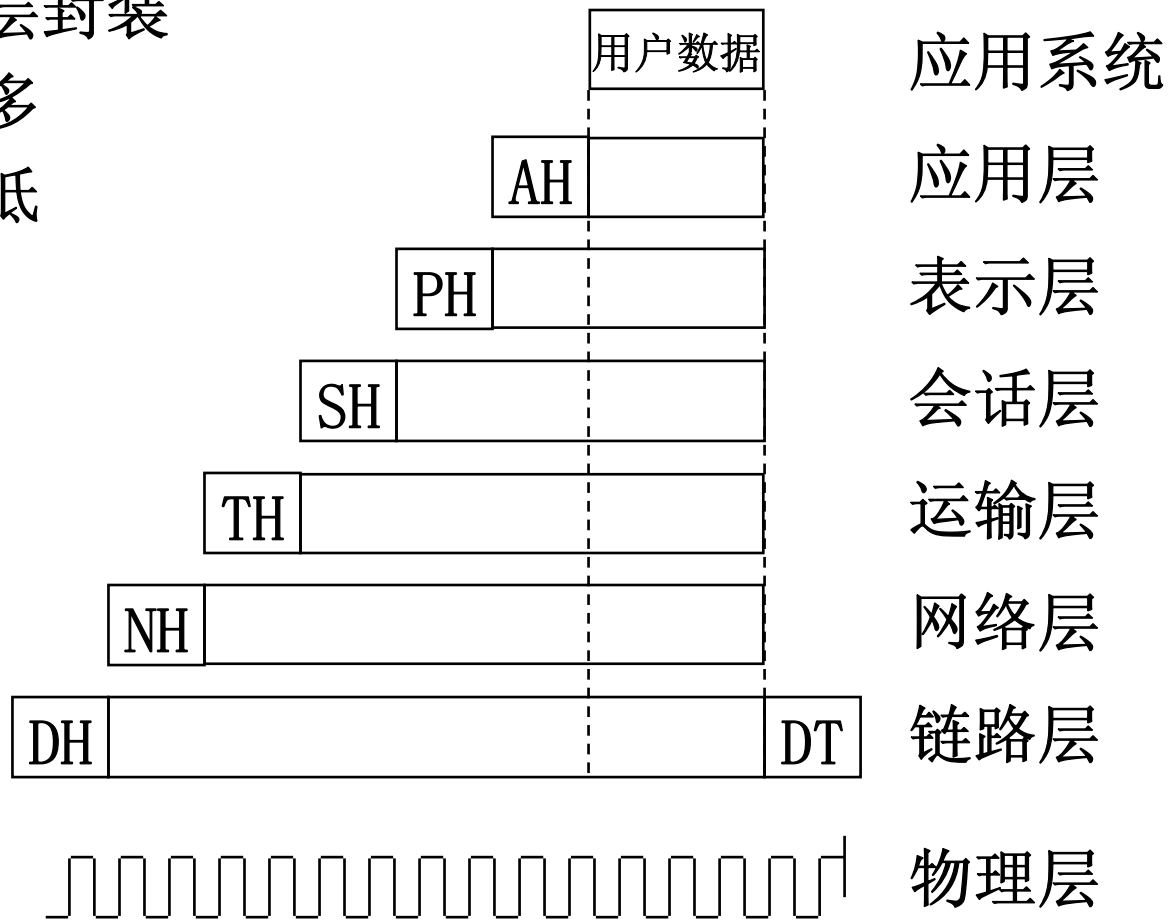


SCI..... 服务控制信息
ICI..... 接口控制信息
PCI..... 协议控制信息

SDU----服务数据单元
PDU----协议数据单元

OSI环境中数据封装

- 数据层层封装
- 层次过多
- 效率校低



OSI通信的特点：

- 规定接口，有利于各个子模块的独立设计，提高设计的灵活性和兼容性；
- 严格定义交换的信息，有利于互操作；
- *层次过多。数据处理过多，耗费了大量的资源*；
- *控制信息层层增加，通信效率随着层次的增加而降低*。

（5） OSI环境下的数据传输方式

★ 面向连接：对等实体在传输PDU之前，必须建立起连接，整个过程包括建立连接、传输数据和释放连接。

建立连接：包括鉴别对等实体的身份、协商数据传输时的控制信息（例如：用户数据的体积、窗口尺寸、使用的协议类别等）；

传输数据：包括传输用户数据，以及为了数据传输而进行的交互控制（例如：数据传输的确认、活动管理、令牌传递等）；

释放连接：释放双方已经建立起来的连接。

特点：传输数据和释放连接时，无需携带地址信息，所有的动作均基于已经建立的连接。

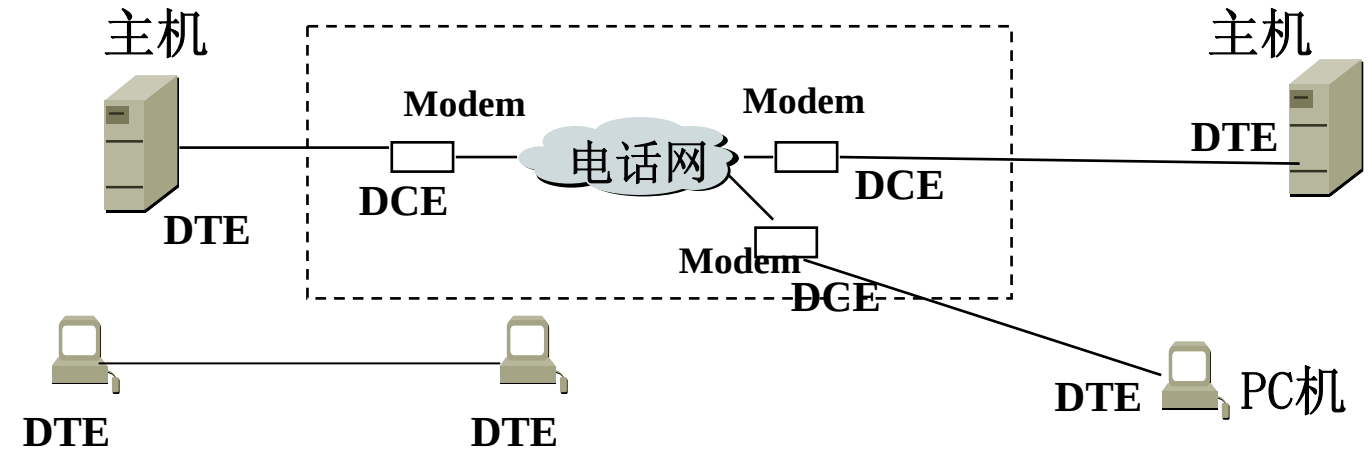
★ 面向无连接：对等实体在传输PDU之前，无需首先建立连接，传输的数据中必须携带地址信息，有关的控制要求只能静态约定。

（1） 术语

数据终端设备（DTE），希望通过网络互连的设备（入网设备），包括：计算机、终端等；

数据电路终接设备（DCE），网络中含有的通信设备（网内设备），包括：通信处理机等；

物理连接：由物理层提供的、在该层用户之间建立起来的一种临时的联系。



（2） 物理层功能

通过规定物理设备和物理媒体之间的接口技术，实现物理设备之间的*比特流透明传输*（包括DTE－DTE和DCE－DCE之间）。

（3） 物理层服务

建立、维持和释放物理连接（标识物理连接、选择服务质量：速率、延迟、传输误码率等），并在物理连接上透明传输比特流（包括排序和故障通知等）。

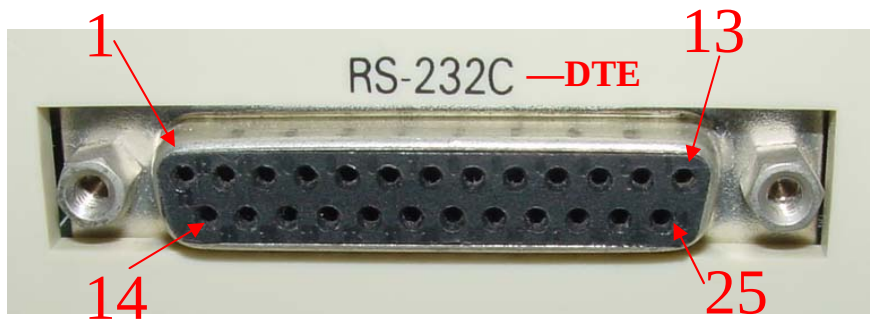
（4） 物理层协议

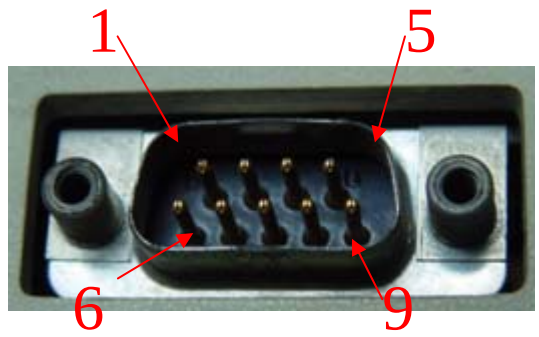
物理层标准从四个方面对物理设备和媒体之间接口进行定义。

- 机械特性：接口部件的尺寸、规格、插脚数和分布等；
- 电气特性：接口部件的信号电平、阻抗、传输速率等；
- 功能特性：接口部件的信号线（数据线、控制线、定时线等）的用途；
- 规程特性：接口部件的信号线在建立、维持、释放物理连接和传输比特流的时序。

25芯或者9芯D型连接器
DB-9和DB-25插针对应关系表

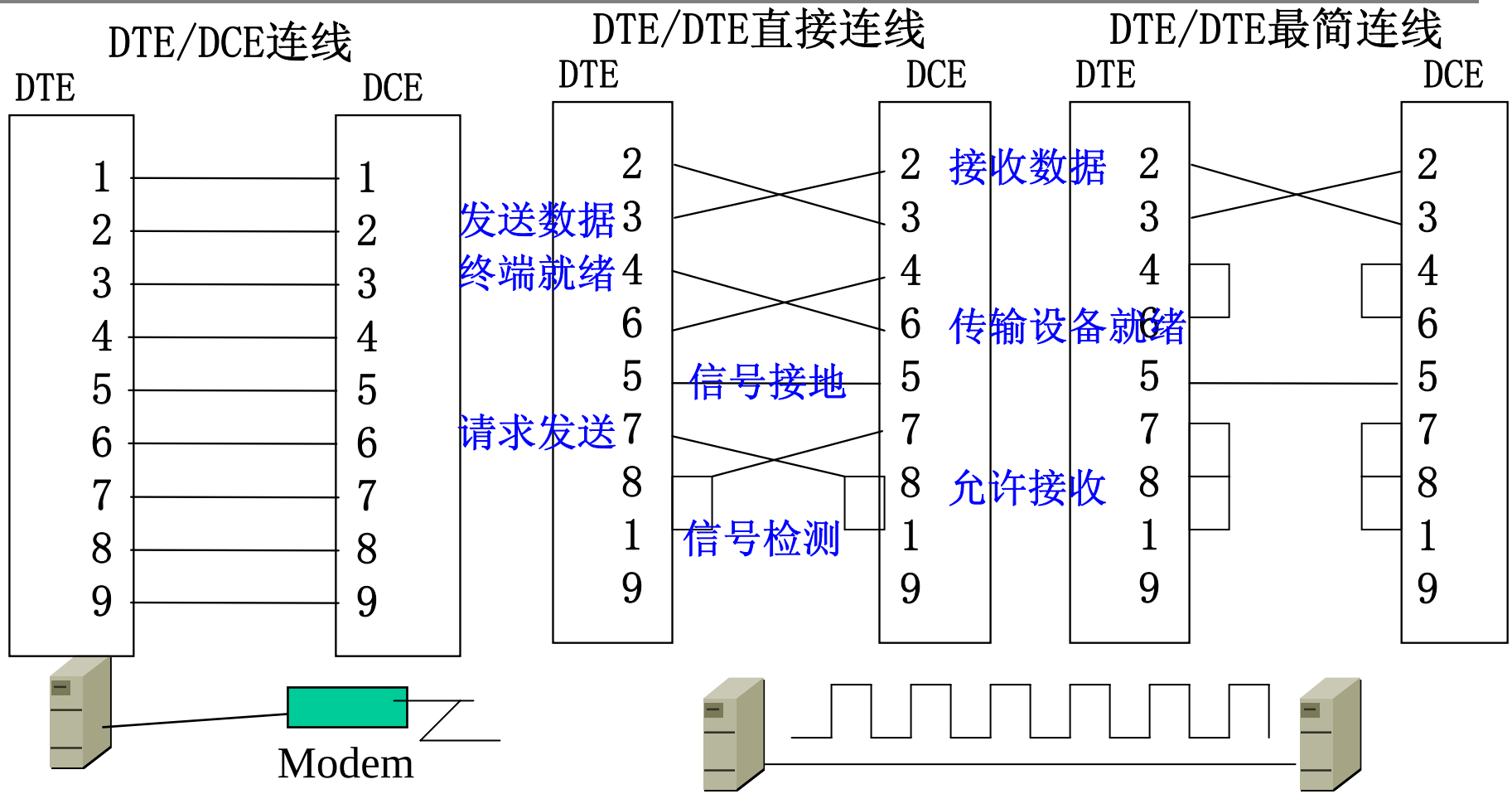
DB-9	DB-25	插针功能说明	标记
1	8	信号检测	DCD
2(RTS)	3	接收数据	RD
3(TDX)	2	发送数据	SD
4	20	数据终端就绪	DTR
5	7	信号地	SG
6	6	数据传输设备就绪	DSR
7	4	请求发送	RTS
8	5	允许接收	CTS
9	22	振铃指示	RI





DTE侧为插座，DCE侧为插针。

RS232接口的连线（DB—9）



RS 232C端口的设置：

端口号： com1, com2,

端口速率：14.4k，28.8k，33.6k，56k

奇偶校验：奇，偶，无

数据位： 7位， 8位

Dos6.0以上版：

客户端—Interlnk

服务器端—Intersvr

速率：150kbps

USB-**Universal Serial Bus**（通用串行总线）

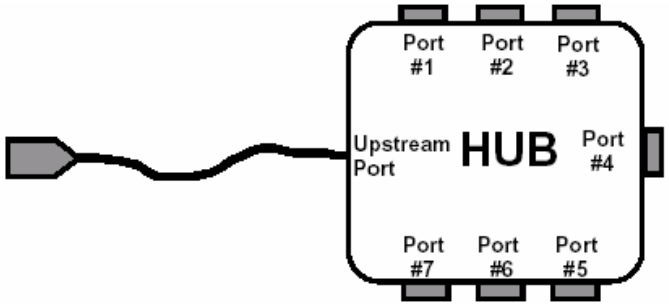
Compaq、HP、Intel、Lucent、Microsoft、NEC、Philips等公司联合制定标准；

目标：支持双向、低成本、低/中速外设接口；

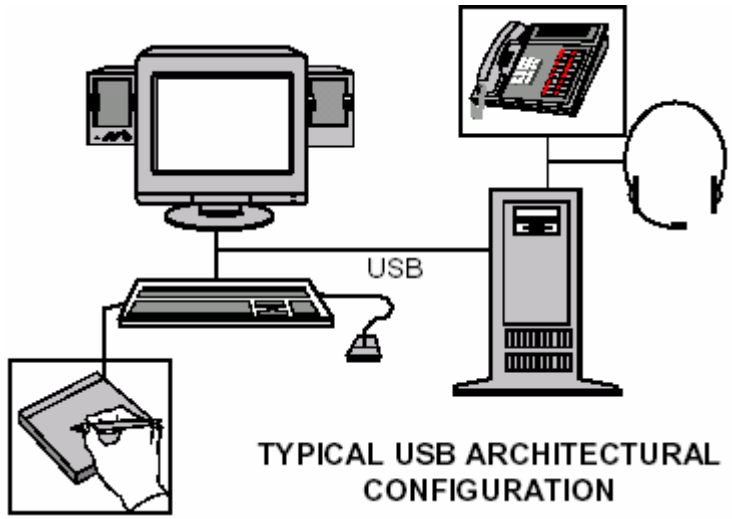
速率（2.0版本）：1.5M(低速)、12M(全速)、480M（高速）；

端口：4针（电源5v、接地、数据入/出）；

编码：NRZI（不归0交替编码）；



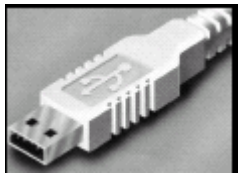
典型的**HUB**结构

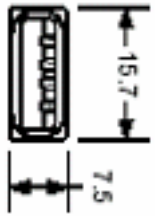


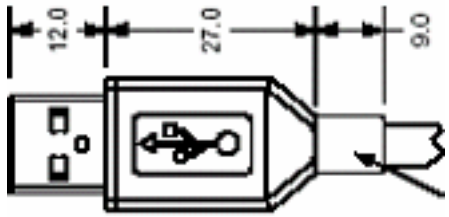
TYPICAL USB ARCHITECTURAL CONFIGURATION

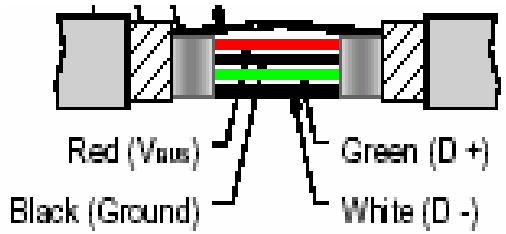
USB-Universal Serial Bus（通用串行总线）

A类连接器

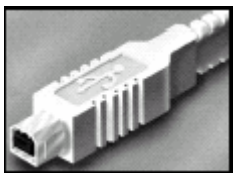


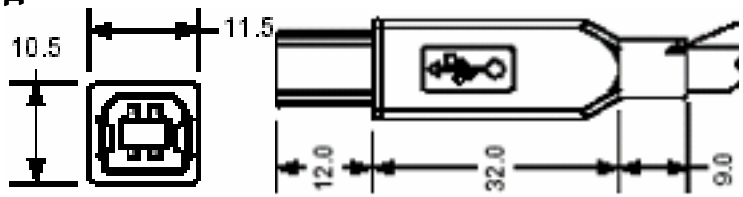


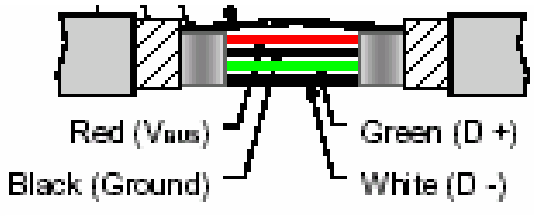


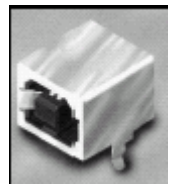


B类连接器

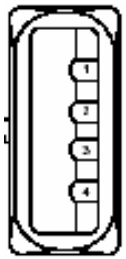






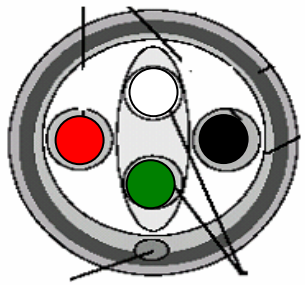


功能特性



1 = VBUS（红色，5v）
2 = D-（白色）
3 = D+（绿色）
4 = Ground（黑色）

线缆剖面



（1）基于物理层的问题：

- 物理连接是有差错和不可靠的。
- 物理设备之间可能存在传输速度不匹配的问题。

（2）数据链路层功能：

- 流量控制技术（等一停协议、窗口机制等），解决速度不匹配的问题。
- 差错处理技术，变不可靠的物理连接为可靠的数据链路，从而保证点一点的数据传输正确性。
- 数据链路是指活动着的物理连接，通信之前，收/发双方互相联系而建立；传输完毕，双方协商而释放。

（3）数据链路层服务：

- 标识和维护数据链路（建立和释放，以及选择服务质量，差错处理机制等）。
- 传输DL SDU（定义帧格式），
- 施行流量控制，
- 进行差错通知（无法处理的差错情况，告知上层用户）。

（4） 数据链路层协议：

约定DL实体之间的控制信息和时序，保证DL服务的提供。

局域网（802.3－CSMA/CD，802.4－令牌总线、802.5－令牌环）

面向字符型的数据链路控制规程——二进制同步控制规程（BSC）；

面向比特型的数据链路控制规程——高级数据链路控制规程（HDLC）。

多链路规程（MLP）

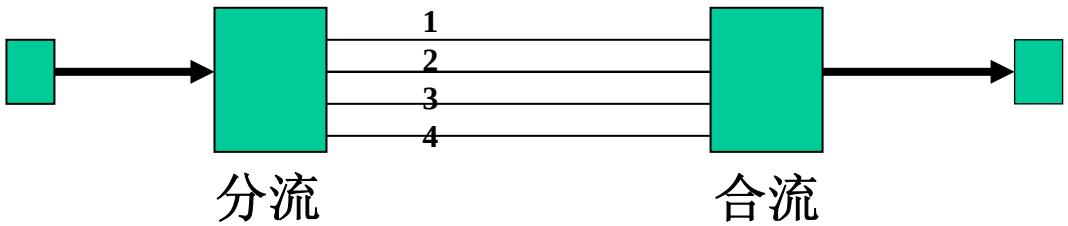
- 指导思想：利用多条物理/逻辑单链路来支持多链路。
- 采用技术：分流/合流

  用多条（N-1）连接来支持单条（N）连接，

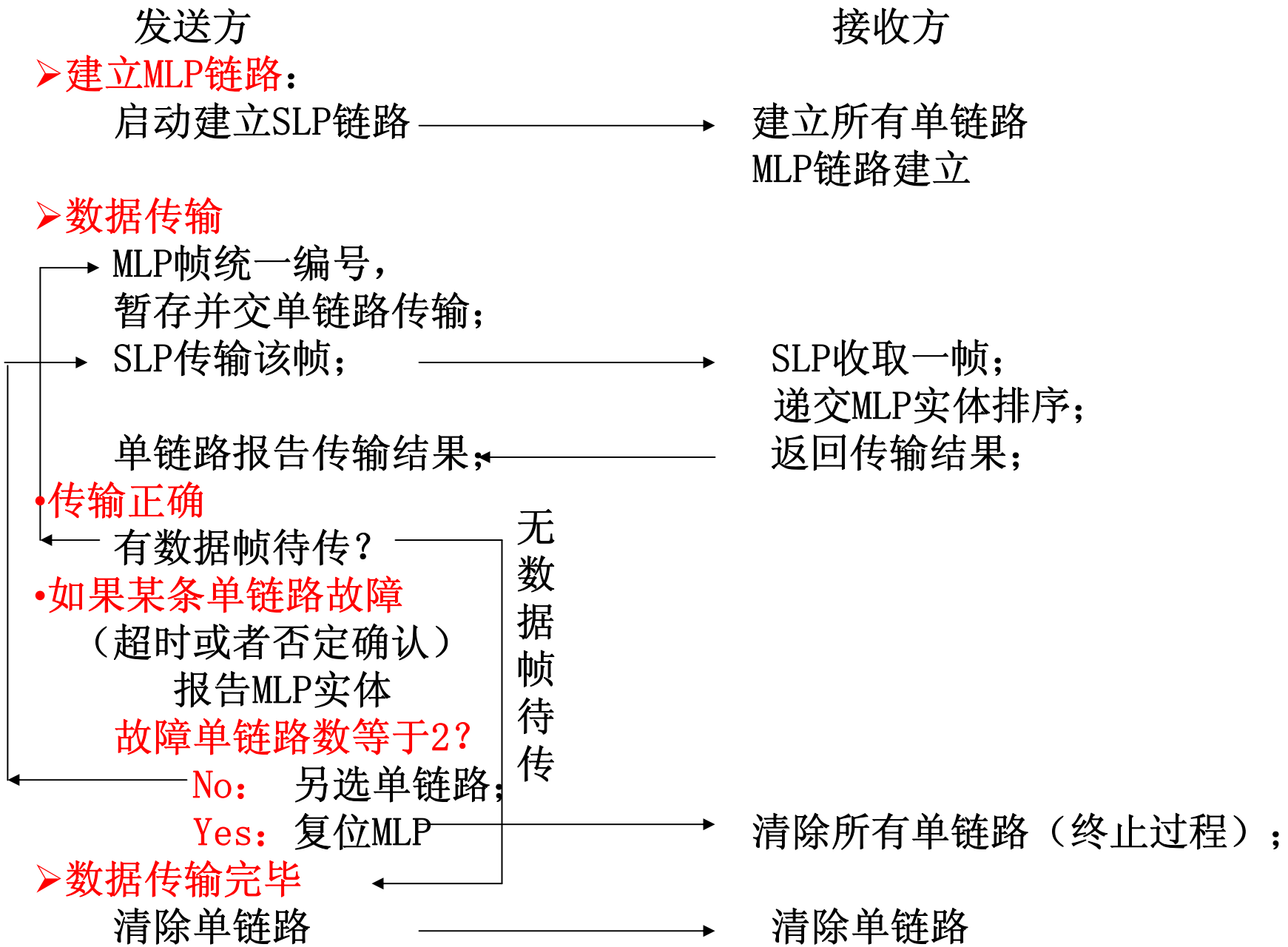
  从多个（N-1）连接中分解出（N）连接的数据传输技术。
- 应用对象：

追求高可靠性时，将相同帧交由多条不同的单链路同时传输；

追求高速率时，将不同帧交由不同单链路传输，MLP的传输速率是各SLP的传输速率之和；



多链路规程（MLP）工作过程



（1） 基于DL层的问题

★ 数据链路层仅提供点对点的数据链路，不能直接提供用户数据的端到端（即DTE和DTE）之间的传输，
（其中可能经过多个DCE的合作和转发）；

★ 当用户设备连入网络时，希望可以和任一其他用户通信；

多个用户可能同时希望传输信息

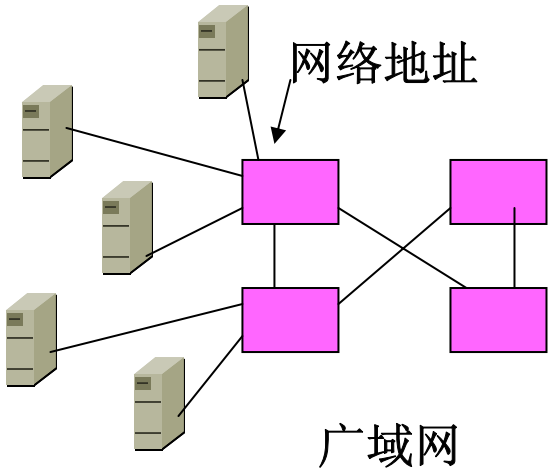
★ 数据链路的利用率较低：用户之间的通信往往是断断续续的。

（2） 网络层功能

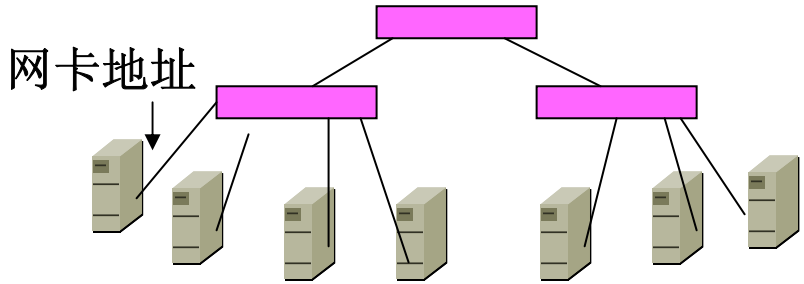
★ 提供编址和路由技术，确保用户数据可以端一端传输。

网络地址：唯一标识网络中设备。

广域网网络地址：指向交换设备（结点机）的输出端口；
局域网网络地址：直接对应到网卡（网卡地址等）



广域网



局域网

路由选择：中间结点根据分组中的的地址和依据某种策略或路由选择算法作出决策，以使分组尽快通过网络送往目的地。

（为减少分组的丢失，网络本身具有吞吐量的限制）

（2） 网络层功能（续）

★ 利用复用/解复用技术，将一条DL划分为若干条逻辑电路（称为逻辑信道LC），并且，采用LC号来区分不同用户的数据，实现多对用户的数据可以交织在同一条数据链路上传输；

★ 提供分组/组装功能，实现用户数据的分组和组装（分组交换），提高链路利用率。

（3） 网络层服务

确定网络地址、标识网络连接、传输数据、分组装拆、排序（按提交顺序投递给用户）、流量控制（限制用户一次性提交给网络的分组个数）等。

（4） 网络层协议

CCITT X.25建议（X.25分组交换网）

局域网：IP协议、IPX协议

Internet：IP协议

（1） 基于网络层的问题：

网络的性能不同，用户的要求不同，网络的性能和用户的要求之间也许存在某种差异。

★ 用户要求高速传输：网络的吞吐量、速率和传输延迟等性能能否满足；

★ 用户要求较低的传输费用，对于传输延时要求不高；网络的吞吐量、速率和传输延迟很好，费用太高，不能满足。

★ 网络的传输差错率不能满足用户的要求；

★ 网络层的分组长度和用户数据的长度不一致；

★ 网络的数据流量；

运输层目的：屏蔽网络性能差异，用户无需了解网络传输细节。

（2） 网络分类（以便更好地屏蔽各类网络）

A型网络服务具有小的残留差错率和小的可通告差错率；

B型网络服务具有小的残留差错率和大的可通告差错率；

C型网络服务具有大的残留差错率。

网络的残留差错率：

在网络连接上传输出错的网络服务数据单元（NSDU）在所有传输的NSDU中所占的比例；

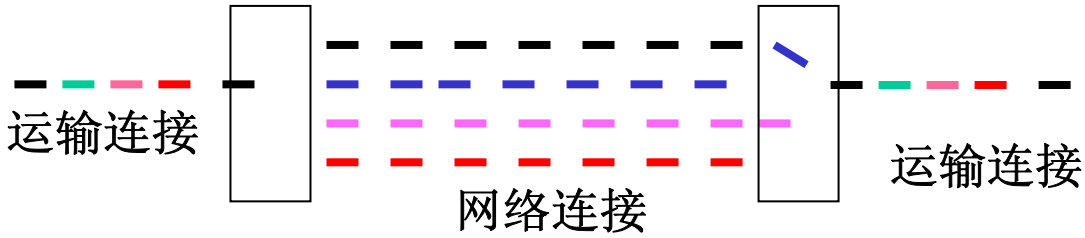
网络的可通告的出错率：

网络中存在的不可恢复的差错与所有可检测的差错中所占的比例。

（3）运输层功能

★ 利用低吞吐量、低速率和高传输延迟的网络支持用户高速传输数据的要求；

分流/合流技术：*多条网络连接支持一条运输连接（类MLP）*。

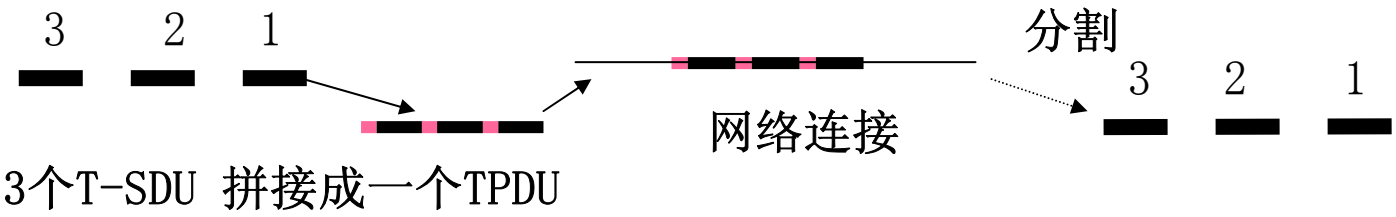


（3）运输层功能（续）

★ 利用高吞吐量、高速率和低传输延迟、且高费用的网络支持用户低传输成本的要求；

复用/解复用技术：将多条运输连接上的数据汇集到一条网络连接上传输（复用网络连接）；

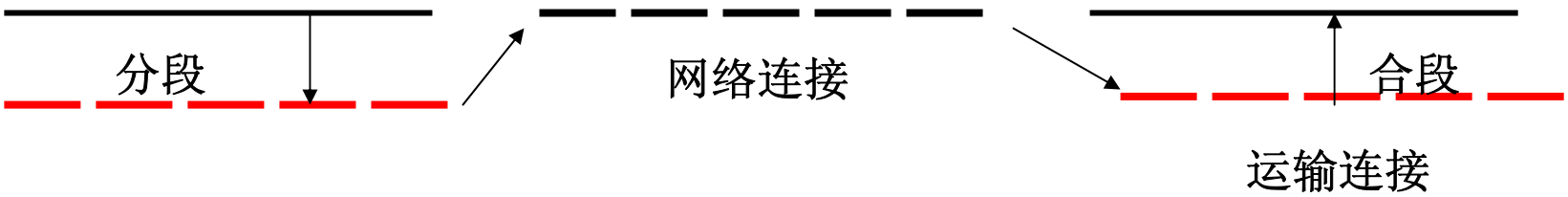
拼接/分割技术：将一条运输连接上的多个TSDU拼接成一个TPDU，并在一条网络连接上传输（借鉴窗口技术）；



（3）运输层功能（续）

★ 利用有限分组长度的网络支持用户的大数据块传输；

分段/合段技术，使得传输有限长度用户数据（分组）的网络可以支持用户的无限长数据的传输



★ 利用差错率较高的网络支持用户高可靠数据传输的要求；

差错检测和恢复技术；

★ 避免网络拥塞；

流量控制技术，限制可连续传输的TPDU个数（窗口技术）。

（4） 运输层服务

标识和维护运输连接（建立和释放连接，以及选择服务质量），提供流量控制和常规数据/加速数据的传输，屏蔽用户要求和网络能力之间的差异。

服务质量： 用户对传输延迟、吞吐量等方面的要求，运输层实体可以根据用户对服务质量的要求决定是否采用分流、复用等技术。

（5） 运输层协议

运输层协议：定义运输层的PDU格式、交换时序，以及其它实施差错校验、分段/合段、分流/合流、复用/解复用、窗口和流量控制等的方法。

相关标准定义了五类运输层协议，不同的运输协议用于不同的环境，网络服务越差，要求的运输协议越复杂。

TP0（简单类）：提供最简单的数据传输能力，仅支持分段/合段功能，它要求网络本身可提供较高质量的数据传输服务，适用于A型网络。

TP1（基本差错恢复类）：在TP0的基础上，增加拼接/分割、差错恢复的能力，可对网络检测出来的差错进行恢复，满足用户可靠传输的要求；适用于B型网络。

（5） 运输层协议（续）

TP2（复用类）：在TP0的基础上，增加复用/解复用、拼接/分割的能力，通常在用户使用高质量的网络，并要求低通信费用时选用，适用于A型网络；

TP3（差错恢复和复用类）：结合TP1和TP2的能力，满足用户低成本、高可靠性的要求，适用于B型网络；

TP4（差错检测和恢复类）：在TP3的基础上，增加差错检测和分流/合流能力，通常在服务质量较差的网络上选用，保证数据传输的可靠性；适用于C型网络。

运输连接建立时，双方协商使用的运输协议类别；

选用不同类别的运输实体之间不能进行通信；

3.8 会话层

（1） 基于运输层的问题

运输层保证用户数据按照要求从网络的一端传输到另一端，用户仍然缺乏管理和控制用户之间的信息交换的手段，尤其是差错恢复的手段。

（2） 部分术语：

会话：用户（表示层实体）之间的信息交换过程；

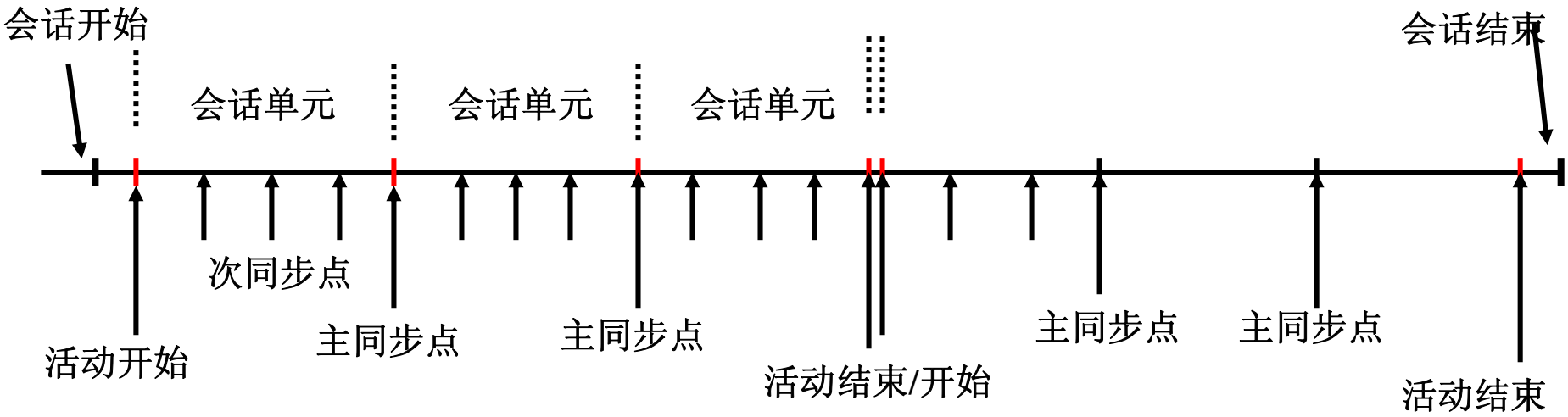
会话连接：用户之间为完成信息交换而按一定规则而在会话层实体之间建立起来的一种暂时的联系；

会话单元：逻辑概念，一组意义上相对完整的数据块传输；

活动：会话用户之间合作的逻辑工作段；可以含有一个或多个会话单元，活动的内容具有相对的独立性和完整性；

同步：对用户数据进行语义上的分割，保证会话层实体之间信息交互（会话）的时序性。

引入活动和同步的目的：使用户可以了解会话的进程，便于控制和管理；如果出现传输故障，可以*从指定的同步点处进行恢复*，减少差错重传的数据量。



数据令牌标识用户发送数据的权利；通过数据令牌的申请和分配，保证用户信息交换的顺序性；

重新同步：是有序地重建用户之间的通信的一种手段；例如：将会话连接置为指定的状态，从指定的同步点处开始新通信。

（3） 会话层功能

会话层的目的：向用户提供组织和控制信息交换的手段。

相关功能包括：

★ 利用令牌技术来保证数据交换、会话同步的有序性；拥有令牌的一方可以发送数据，或者执行其它动作；令牌可以被申请和转让；

★ 利用活动和同步技术来保证用户数据的完整性；并让用户知道整个交换的过程；

★ 利用分段和拼接技术来提高数据交换的效率；多块用户数据可以合并在一起进行传输；

★ 利用重新同步技术来实现用户会话的延续性；支持传输过程中的故障恢复。

（4）会话层协议（在会话协议控制下的用户数据交换过程）。

用户端1	方向	用户端2	说　　明
S-CON.req	—→	S-CON.ind	；会话连接（包括选择
S-CON.cnf	←—	S-CON.rsp	；功能单元和分配令牌）
S-ACT_START.req	—→	S-ACT_START.ind	；活动开始
S-DATA.req	—→	S-DATA.ind	；传输一块数据
S-SYNC-MINOR.req	—→	S-SYNC-MINOR.ind	；检验数据完整性
S-SYNC-MINOR.cnf	←—	S-SYNC-MINOR.rsp	
S-DATA.req	—→	S-DATA.ind	；传输一块数据
S-SYNC-MINOR.req	—→	S-SYNC-MINOR.ind	；检验数据完整性
S-SYNC-MINOR.cnf	←—	S-SYNC-MINOR.rsp	
S-DATA.req	—→	S-DATA.ind	；传输一块数据
……		……	，继续传输动作等
S-DATA.req	—→	S-DATA.ind	；传输一块数据
S-TOKEN-PLEASE.ind	←—	S-TOKEN-PLEASE.req	；用户2请求数据令牌
……		……	；用户1继续保留令牌

（4）会话层协议（续）

用户端1	方向	用户端2	说　　明
S-ACT-END.req	——→	S-ACT-END.ind	；用户1数据传输完毕，
S-ACT-END.cnf	←——	S-ACT-END.rsp	活动结束
S-TOKEN-GIVE.req	——→	S-TOKEN-GIVE.ind	；用户1 释放数据令牌；
S-ACT_START.ind	←——	S-ACT_START.req	；用户2开始传输
S-DATA.ind	←——	S-DATA.req	
S-SYNC-MINOR.ind	←——	S-SYNC-MINOR.req	
S-SYNC-MINOR.rsp	——→	S-SYNC-MINOR.cnf	
	←——	S-DATA.req	；低层故障，用户1未收到数据
S-P-EXECP.ind	←—→	S-P-EXECP.ind	；低层故障报告
S-CON.ind	←——	S-CON.req	；重新连接
S-CON.rsp	——→	S-CON.cnf	
S-ACT-RESUME.ind	←——	S-ACT-RESUME.req	；恢复活动和同步点
S-DATA.ind	←——	S-DATA.req	；用户2继续数据传输

3.9 表示层

(1) 基于会话层的问题

不同的计算机系统具有不同的信息描述和表示方法，而不同的信息描述（表示）将导致不同系统之间无法识别所交换的信息的含义（如不同的码字，对数据的不同表示）。

(2) 表示层功能

语法：数据的描述和表示方法；

抽象语法：数据一般结构的描述方法，独立于具体应用；

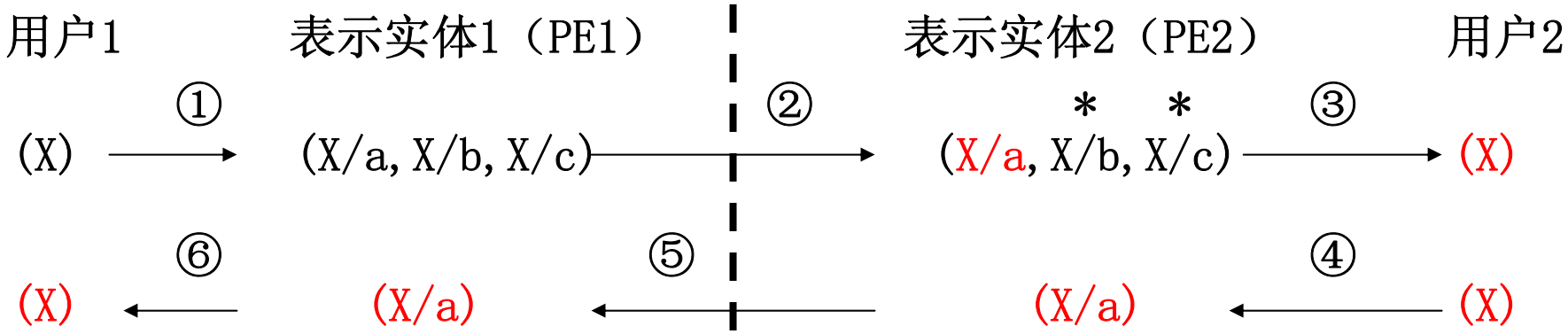
传送语法：开放系统之间传送数据的表示方法；

表示层功能：协商传送语法，并执行抽象语法和传送语法之间的转换，通过这种转换来统一表示被传送的用户数据，使得通信双方都可以互相识别。

(3) 表示层协议

定义对等表示层实体之间交换的PPDU的内容、格式和交换的时序，以保证表示层服务的提供。

传送语法的协商过程示意



说明：
① 用户1（应用实体）希望将抽象语法X描述的数据传送给用户2；
② PE1有能力用三种传送语法（a、b和c）进行描述；
③ PE2可以处理用a描述的数据；
④ 用户2可以处理用X描述的应用数据；
⑤ PE2通知PE1可以用a作为本次传输的传送语法；
⑥ PE1通知用户1可以传送X描述的应用数据。

(4) 通信系统中的一般数据表示方法（8位位组串）

CCITT X.409和ISO 8824定义的抽象语法1（ASN.1）。

一般结构：标记 长度 内容；

举例：

职工信息::=sequence[30]{
姓名；
性别；
出生年月}

姓名::=PrintableString[50]；

性别::=Boolean[51]；

出生年月::=DigjtalString[52]；

则职工张三的信息表示：

30 20 50 09 Z h a n g s h a n 51 01 01 52 04 19 66 06 30

编程实现时的关键：长度值的回填（递归算法）。

3.10 应用层

（1） 应用层的目的

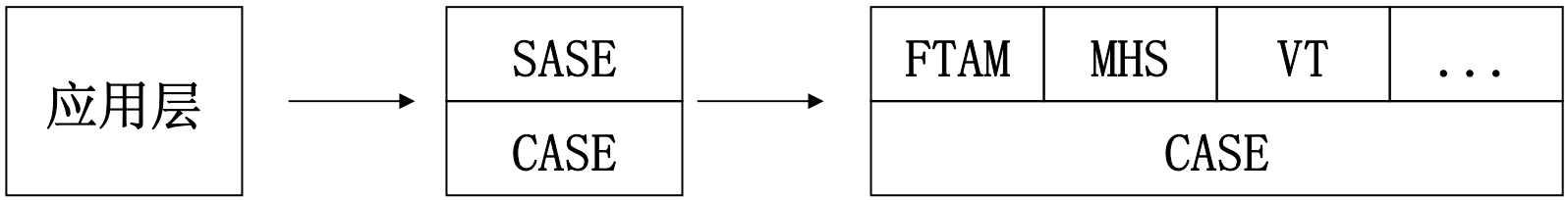
应用层是网络可向最终用户提供应用服务的唯一窗口，其目的是支持用户联网的应用要求。在OSI/RM中，这些应用服务被称为应用服务元素（包括电子邮件、文件传输、虚拟终端、电子数据交换等）。

（2） 应用服务分类

不同的应用服务元素具有共性和特性，可分为两类：

★ 公共应用服务元素（CASE）：提供与特定应用服务无关的公共服务；

★ 特定应用服务元素（SASE）：提供面向特定应用的服务，如FTAM,MHS,EDI等。



(3) 公共应用服务元素（CASE）

CASE提供诸多SASE所共需的功能，主要包括:

★ 应用联系服务元素（ACSE）

提供建立和终止应用联系的能力，并可对应用上下文进行有限的管理。

应用联系指为实现某种特定应用服务而在应用实体之间建立的合作关系，应用联系与表示连接一一对应。

★ 托付、并发和恢复（CCR）服务元素

支持进程的并发处理。

托付：某个进程的提交执行；

并发：几个进程的同时执行，其结果应当等同于各进程按照某种顺序的执行；

恢复：对某个进程的部分或者全部的重新执行。

(4) 特定应用服务元素（SASE）

SASE面向特定的应用，又分两类：

★ 基础服务元素

可靠传输服务（RTS）支持APDU的可靠和完整传输；

远程操作服务（ROS）以请求/响应方式支持交互式操作；

★ 一般服务元素

文件传送访问和管理服务（FTAM）支持文件传输；

虚拟终端服务（VT）支持远程终端的仿真；

电文处理服务（MHS）支持电文的异步传输；

……。

3.11 文件传送访问和管理（FTAM）

（1） FTAM的设计目的

目的：屏蔽不同文件系统在格式和访问方式上的差异，使用户可以同等方便地对本地或远地文件系统进行操作和数据维护；

文件传送：整个或部分文件内容在不同文件系统之间移动；

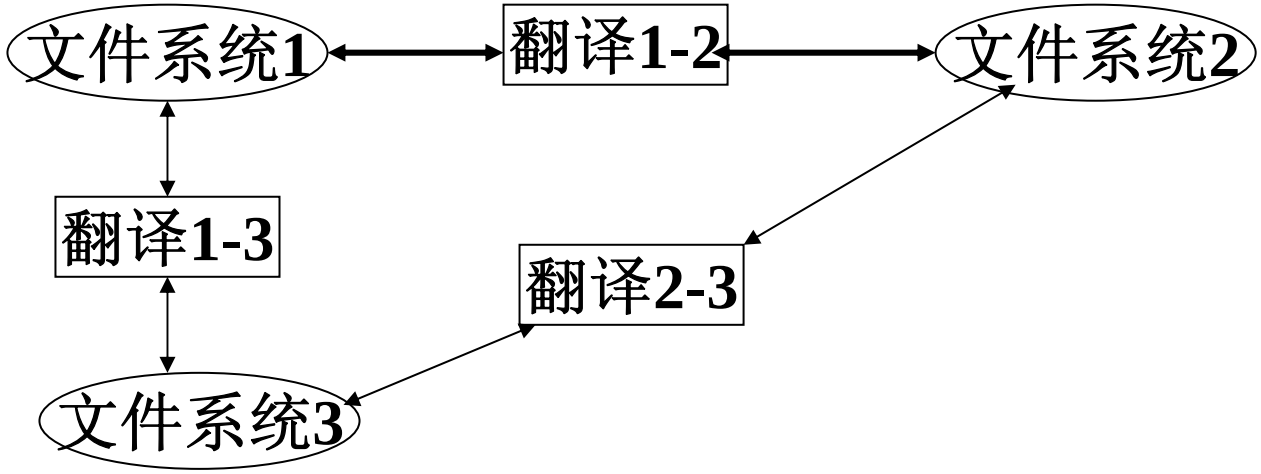
文件访问：对文件的内容进行检查、修改、替换或者擦除；

文件管理：创建和删除整个文件，以及检查或操作文件属性；

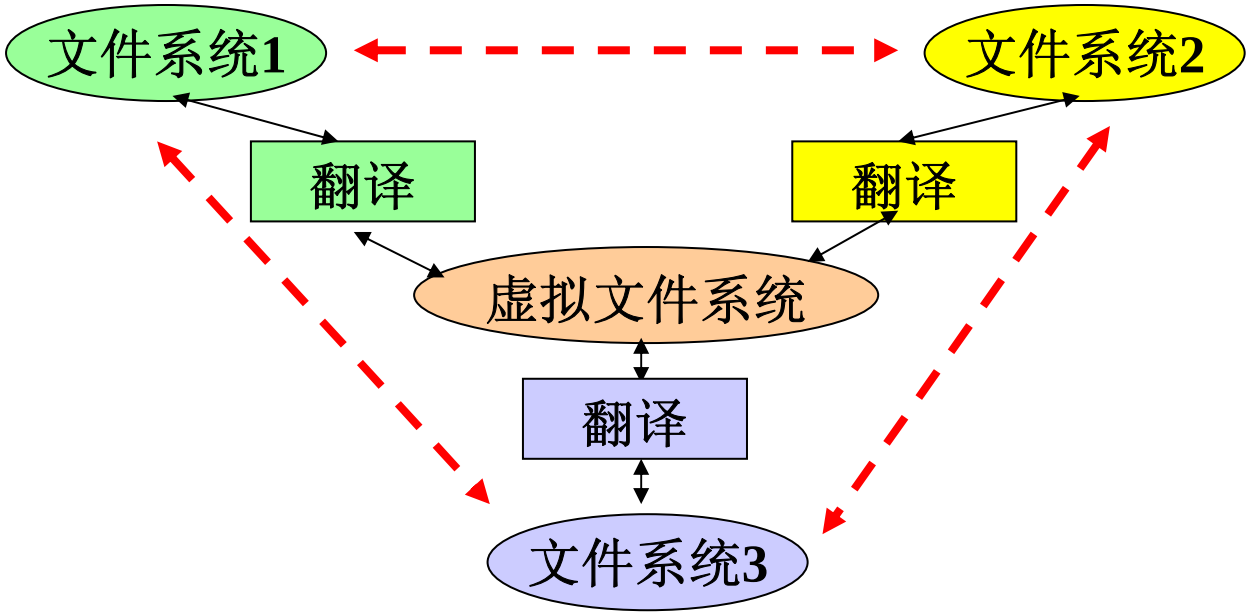
FTAM的设计思想：通过定义一种标准的虚拟文件系统的结构和访问方法，并进行虚/实文件系统映射，从而达到FTAM应用的目的。

虚拟文件系统：对所有实文件系统的抽象，形成抽象的命令集，支持对虚拟文件系统的操作。

文件系统访问的传统方法



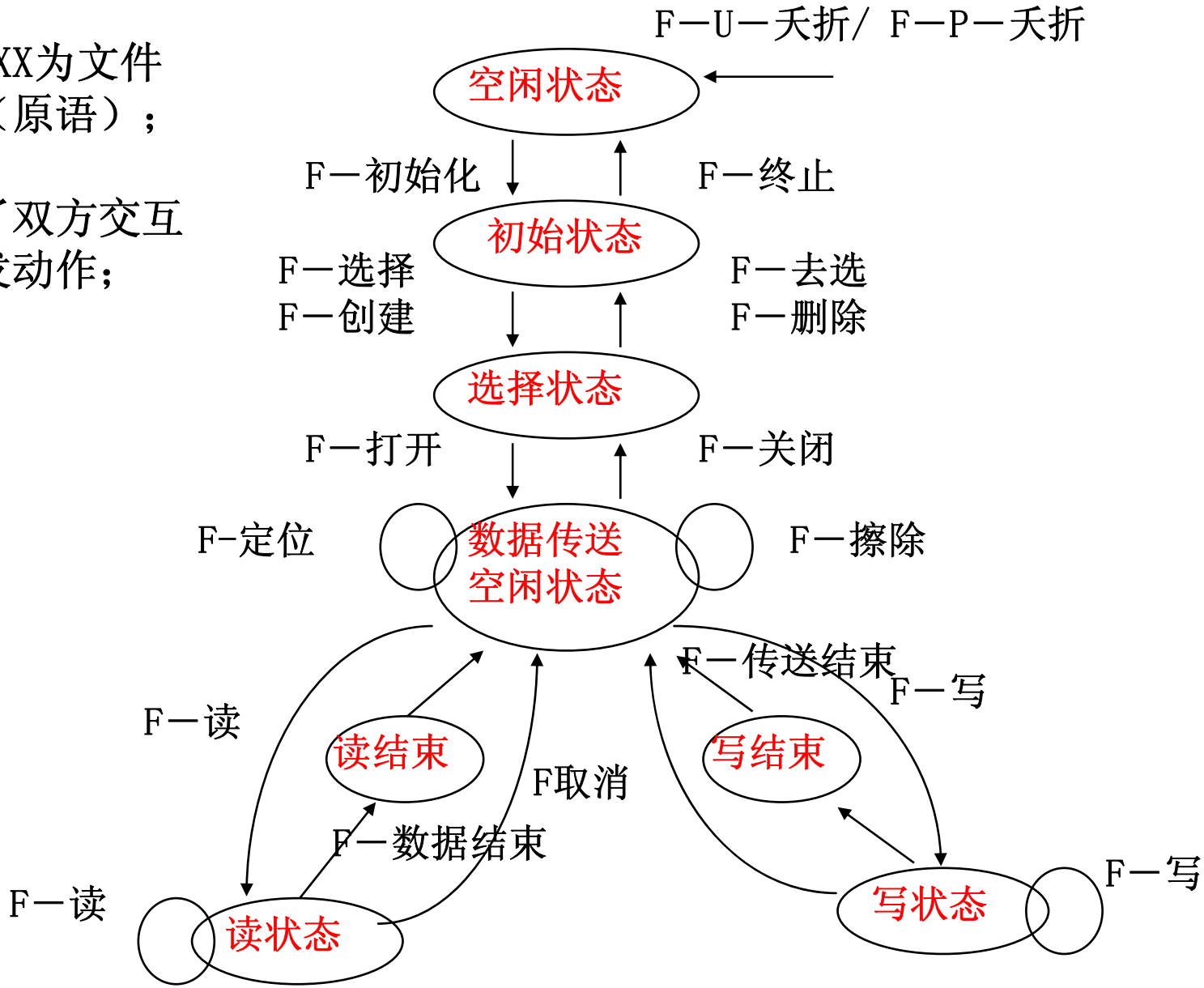
文件系统访问的FTAM方法



简化的发起方状态变迁图

其中 F-XXXX为文件操作命令（原语）；

图中略去了双方交互的数据收发动作；



发送一个文件到远地系统举例：

发起方	响应方	说明
F-INITIALIZE.req	F-INITIALIZE.ind	文件初始化
F-INITIALIZE.cnf	F-INITIALIZE.rsp	
F-CREATE和F-OPEN.req	F-CREATE和F-OPEN.ind	创建/打开文件
F-CREATE和F-OPEN.cnf	F-CREATE和F-OPEN.rsp	
F-WRITE.req	F-WRITE.ind	响应方执行写操作
（本地打开读文件， 远地打开写文件）		
F-DATA.req	F-DATA.ind	发送文件内容
……	……	
F-DATA.req	F-DATA.ind	
F-DATA-END.req	F-DATA-END.ind	文件内容发送结束
F-TRANSFER-END.req	F-TRANSFER-END.ind	本次文件传送结束
F-TRANSFER-END.cnf	F-TRANSFER-END.rsp	
F-CLOSE和F-DESELECT.req	F-CLOSE和F-DESELECT.ind	关闭文件/去选文件
F-CLOSE和F-DESELECT.cnf	F-CLOSE和F-DESELECT.rsp	
F-TERMINATE.req	F-TERMINATE.ind	结束传输
F-TERMINATE.cnf	F-TERMINATE.rsp	

3.12 电文处理系统（MHS）

（1） MHS的目的

★ 目的

满足用户在发送方和一个或多个接收方之间以“存储－转发”的方式交换各种类型信息（正文、图象和数字化声音等）的要求。

MHS系统交换的信息统称为电文（Message），俗称电子邮件。

★ MHS 的特点

— MHS服务的提供要求多个开放系统的合作。

— MHS是唯一的非实时应用服务，支持用户的异步访问。 利用存储转发的能力，使得邮件的发送和接收可以不同时进行；

★ 设计思想

通过定义电文的格式和开辟存储电文的空间（邮箱）来支持用户的异步访问；

（2） MHS系统的基本功能

★ 创建电文，系统应为用户提供编辑器或者文字处理器，允许用户创建和编辑电文；

★ 发送功能，用户指出电文的接收者，系统负责将电文投递到接收者的邮箱；

包括：多址投递（一份邮件可以投递给多个接收者）；

延时投递（约定邮件投递给接收者的时间）；

优先级投递（发送者可以指定邮件的紧急程度）；

邮件转发（收方用户重新指定新的收方）；

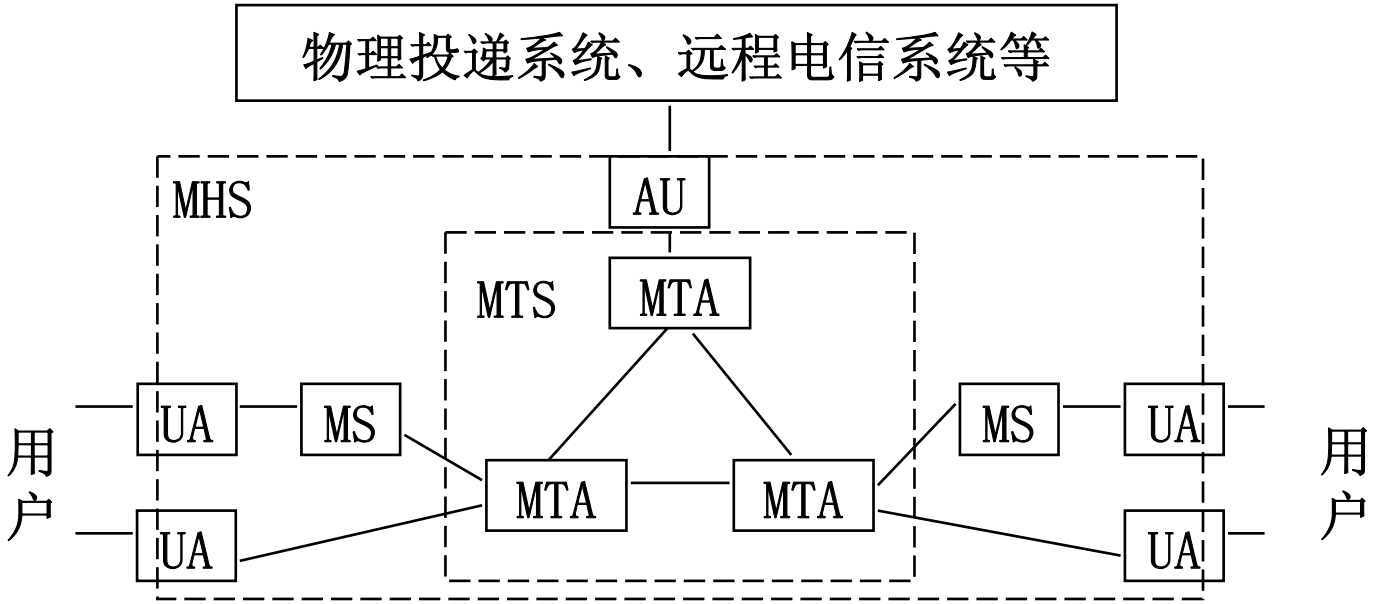
★ 接收功能，接收者调用电子邮件服务来访问和阅读投递来的邮件，必要时也可进行回复；

★ 存储功能，双方都可对指定的电文进行存储归档处理；

★ 回执业务，使得用户可以了解邮件传递的过程，包括投递报告、接收报告等；

★ 支持多种类型信息（正文、图形、语音等）的交换。

（3）MHS的功能模型（可和邮政系统比对）



UA：辅助用户编辑电文、收发电文、管理电文（归档、删除）

MTA（邮局）：中继传输功能：支持电文在系统中的中继和传输（利用存储-转发能力）；含电文调度和语法转换功能。

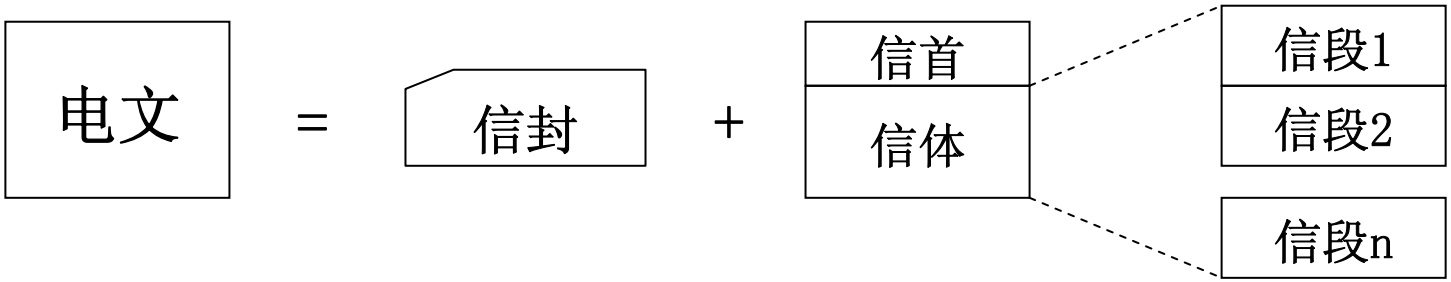
MTS：多个MTA的合作，实现电文在UA之间的透明传送；

MS（邮箱）：实现用户电文的存储；

AU：支持远程用户对系统的访问。

（4） MHS处理的数据单元

★ 电文（Message）：用于携带用户交换的信息。



信封：含提交/传输/投递过程中的控制信息，如地址和投递方式说明等；

信首：标识邮件及发方用户的一些附加要求（如：邮件有效期、标题等）

信体：用户希望传输的真正信息，如正文、数字化声音等。

★探询：由信封构成，含邮件信息，探测系统的传输和投递能力；

★投递/未投递报告：MTA产生，对应电文/探询传输或投递结果；

投递报告：对应电文/探询已投递（或可投递）给指定用户。

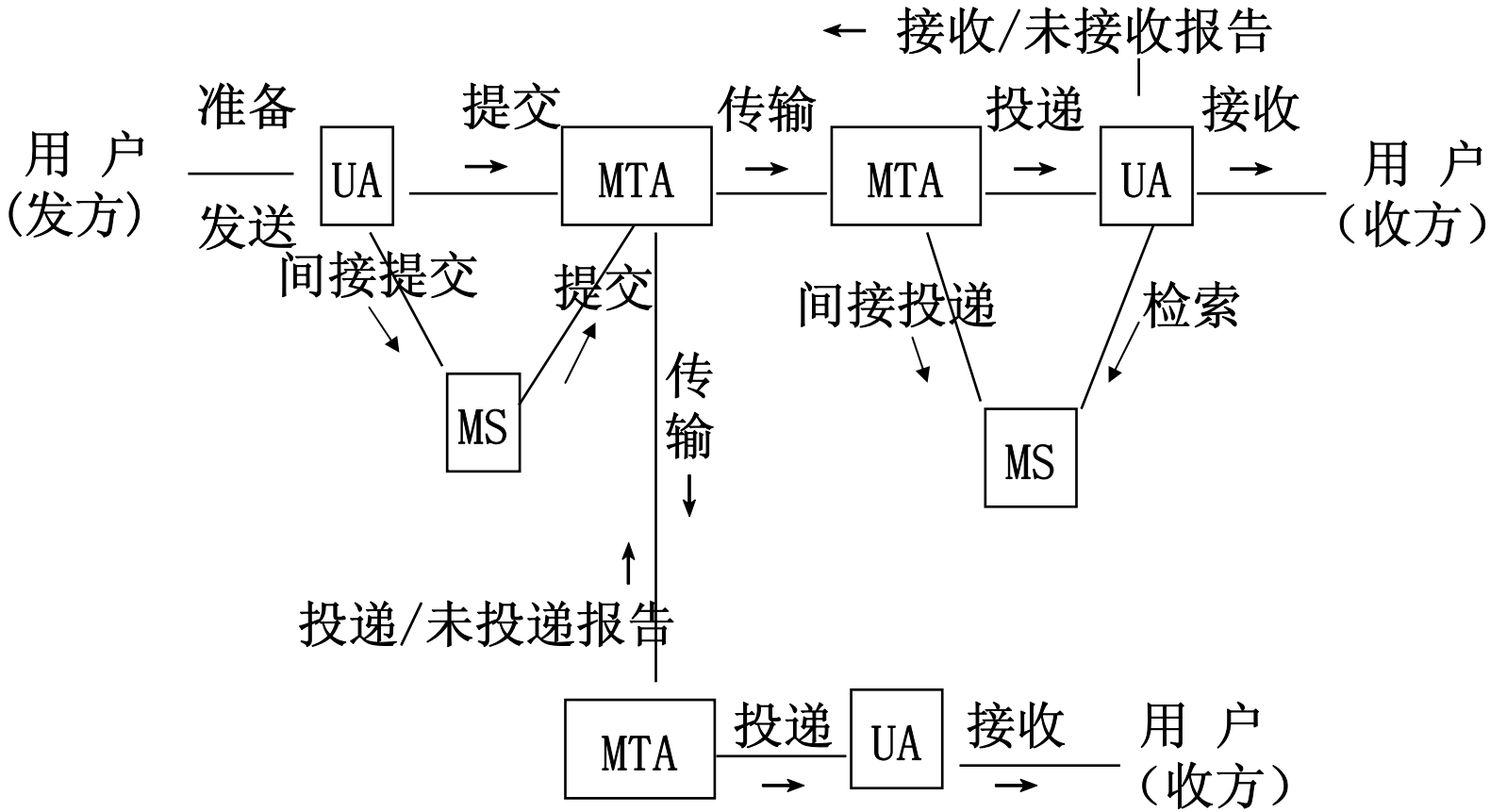
未投递报告：对应电文/探询未能在MTS中继续传输（如：用户地址不支持，数据类型不支持等），或未能投递给指定用户。

★ 接收/未接收报告： 收方UA产生，表示邮件是否被用户读取；

接收报告：表示对方已读取本电文,并给出收取的时间；

未接收报告：未在规定时间内读取，给出未能收取的原因等。

（5）MHS的工作过程示意



3.13 电子数据交换（EDI）

（1） 电子数据交换的定义

★从应用上看，EDI是将与贸易有关的运输、保险、银行和海关等行业信息（如文件、定单、合同等）用一种国际公认的标准格式进行编制，并通过计算机网络，实现各有关部门或者公司之间的数据传输与处理，完成以贸易为核心的全部业务过程。

★从技术上看，EDI被定义为使用统一的标准编制的各种商贸资料在计算机应用进程之间的交换。

★EDI涉及的两个方面

标准：EDIFACT

EDI报文的传输：

FTAM：直接将EDI报文传输到通信方的计算机；

MHS： 利用“存储-转发”功能和邮箱机制；

E-mail：基于SMTP的邮件传输。

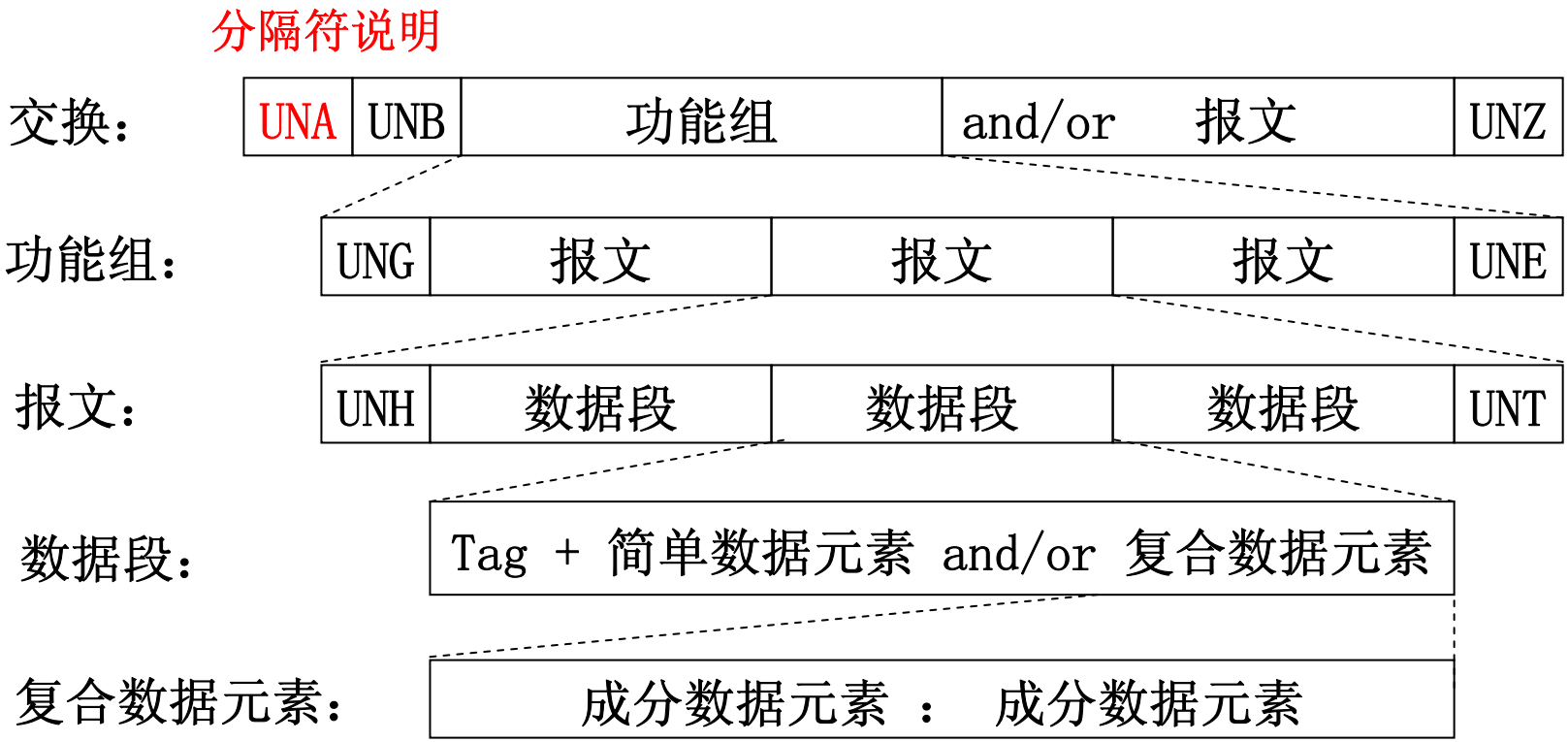
★以单个企业为中心的电子数据交换—BtoC电子商务

企业确定单证格式，用户填写（网上采购）；

★企业间的电子数据交换—B2B电子商务

标准格式：EDIFACT—用于管理、商用和运输的EDI标准；

图表形式的商业文件 ⟷ 正文文件或者字符流（EDI报文）；



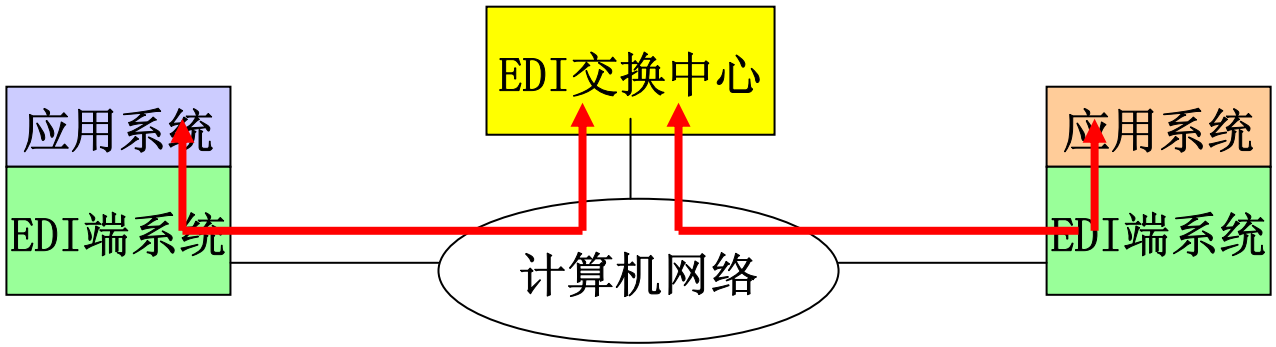
发票举例

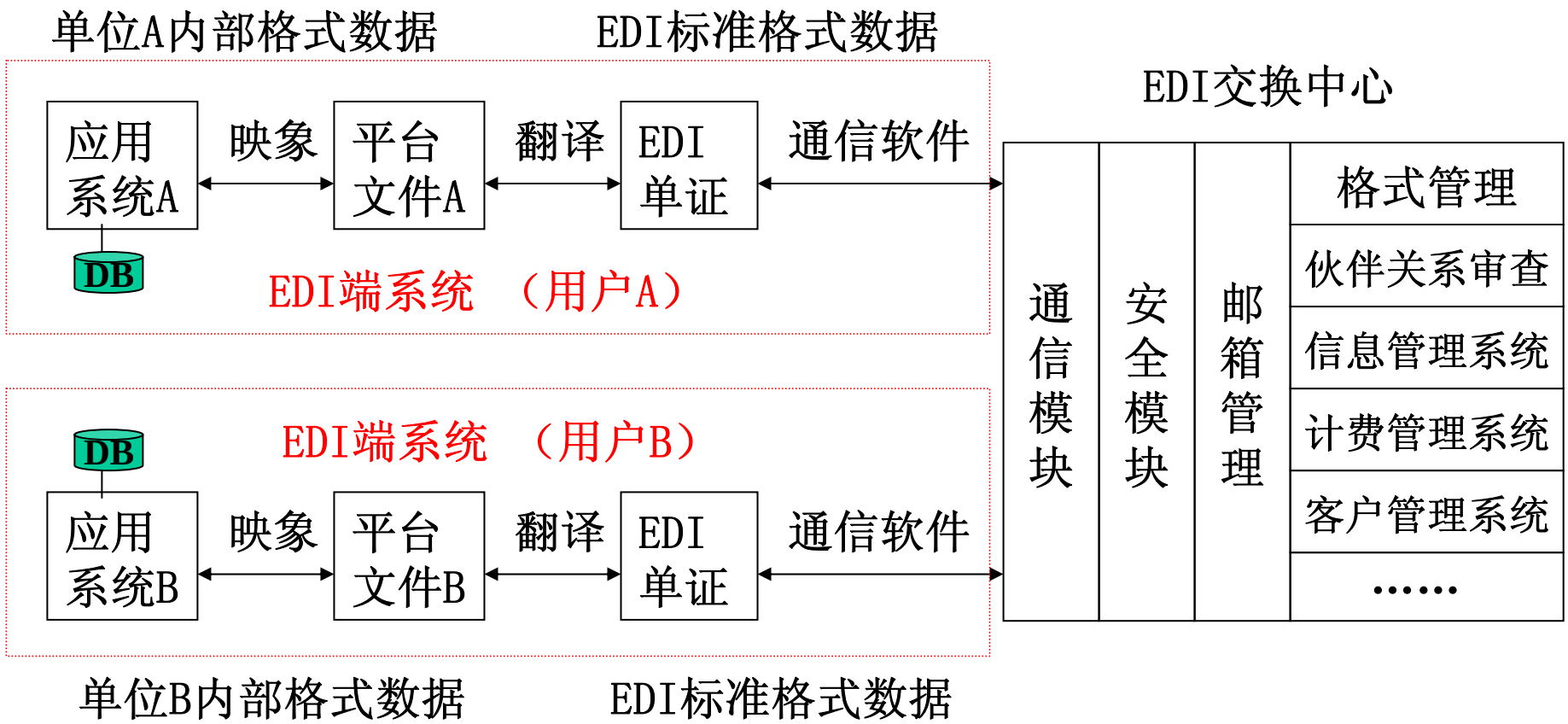
卖方			
买方			
品名	单价	件数	金额
经手人		日期	

UNA：+； （复合元素内部分隔符、段分隔符等）

- **UMB**
  - **UNG**
    - **UNH99**（发票）
      - **20**卖方；**40**买方；
      - **50+**品名：单价：件数：金额；
      - **60**经手人；
      - **70**日期；
    - **UNT**
  - **UNE**
- **UNZ** （最终形成字符串或者文本文件）

（2） EDI系统的基本组成





EDI交换中心的主要功能模块：

★通信模块：支持符合UN/EDIFACT标准的EDI单证传输；

★邮箱管理模块：暂存用户的EDI单证，使其具有异步特征；

★安全模块：保证客户数据信息安全传递，防止非法存取等；

★格式管理模块：格式审查以及不同EDI单证格式之间转换；

★伙伴管理模块：对发生EDI交换的贸易伙伴关系的审核；

★信息管理模块：支持用户交换数据和联机检索等；

★计费模块：支持用户的有偿使用；

★客户管理模块：收集和管理客户资料；

★客户支持模块：提供故障咨询服务等。

（3） EDI的安全措施

★ 可能的问题

— 收发双方对传输单证发生争议时，如何仲裁？

— 经EDI系统交换的电子单证可否作为仲裁的依据？

— EDI传输系统能否保证EDI单证交换的一致性？

★ 解决方法

— EDI立法问题：涉及面广，相应法律难以统一；

— 双方协定（君子协定）

贸易双方协定：约定使用的单证类型、采用的安全方法，双方应当承担的义务和责任，对交换的EDI单证的认可；

用户和服务部门的协定：划定双方的责任范围，服务部门应保证经EDI交换中心传输的EDI单证的一致性，这样的协定依赖于传输技术的可靠性和安全性。

（4）EDI系统的安全性要求：

★ 鉴别通信实体，确定EDI报文的来源；

★ 完整性保障，收发单证的一致性；

★ 私密性保障，确保短期内不被第三方解析单证的内容；

★ 防抵赖性，不仅适用于贸易双方的用户，也应包括EDI单证在网络中进行“存储—转发”的各个功能实体（例如：采用MHS系统支持EDI应用时，EDI单证途径的每个MTA）；

★ 用户身份鉴别，确保只有达成协定的贸易伙伴之间才能通过本系统进行EDI单证交换。

可采用的网络安全技术：

数据加密/解密、访问控制、数字签名、
审计与记录，以及责任传递等。

（5）EDI的应用

具有贸易往来和数据交换的所有部门都可以采用EDI技术；

EDI网络可以将各行各业联系起来，构成一个面向国际市场的贸易－物流－金融－制造－保险等一体化的社会管理体系。

★ 发达国家于70年代末期推行EDI应用；

★ 我国部分涉外行业于80年代中期应用EDI技术（报关）；

★ 90年代初期，我国推进EDI应用进程；

— 金关工程（国家外贸海关信息网络工程），电子化报关，支持我国贸易活动，促进与国际贸易的接轨；

— CHINAEDI（中国公用EDI业务网）：电信总局在上海、北京、天津、广州、南京等十三个城市设立EDI交换中心，通过美国通用电气资讯服务公司（GEIS）的国际商业网络实现全球电子商务。

OSI/RM应用现状

OSI/RM—计算机网络标准，
明确了计算机通信需要解决的问题和解决问题的方法；
70年代提出参考模型（ISO7498），
80—90年代，相关各层的服务/协议陆续提出；
OSI产品多出自于欧洲，我国80年代末也曾设想通过研发OSI产品来缩短和发达国家的差距。

OSI标准未能得到推广的原因？
1、生不逢时（TCP/IP竞争）？新技术推出的一般历程：
　　新生事物（众多研究）—走向市场（巨资投入）
2、强调全面，技术复杂，部分功能（如差错等）重复；
3、缺乏强有力的推动者（TCP/IP集成进UNIX）；

OSI—网络技术学习者的灯塔。

第4章 局域网

4.1 局域网的基本概念

微型机的应用刺激了局域网的发展；

局域网是将分散在有限地理范围内（如一栋大楼，一个部门）的多台计算机通过传输媒体连接起来的通信网络，通过功能完善的网络软件，实现计算机之间的相互通信和共享资源。

美国电气和电子工程师协会局域网标准化(IEEE 802)委员会的定义：

局域网通常是由单个组织拥有、使用和运维的，允许中等地域内的结点以中高速率直接互连通信的对等通信网络。

4.1.1 局域网的特点

（1） LAN的描述或者特性

—传输媒体　双绞线、同轴电缆和光纤（光缆），在特殊环境下，也可以考虑使用微波、红外线和激光等无线传输媒体；

—传输技术　使用传输媒体进行通信的技术，常用的有基带传输和宽带传输；

—网络拓扑　指组网时的电缆铺设形式，常见的有总线形、环形和星形，局域网的网络拓扑描述对应网络中数据收发的方式。

—访问控制方法　网络设备访问传输媒体的控制方法，常用的有竞争、令牌传递和令牌环等。

（2） LAN的特点

★ 网络覆盖范围小（房间、建筑物、校园，10公里以内）
★ 选用较高特性的传输媒体：高的传输速率和低的传输误码率
★ 硬软件设施及协议方面有所简化
★ 媒体访问控制方法相对简单
★ 广播方式传输数据信号，不考虑路由选择和忽略OSI网络层。

（3） 站地址

标识局域网中设备的形式；

★ 通用格式：由网络设备制造商指定的地址，通常占48比特
★ 本地管理地址格式：管理员分配，网络内有效，通常为16比特

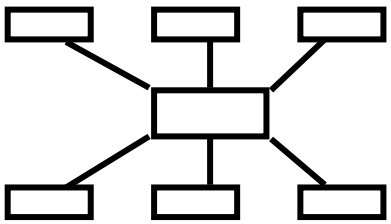
4.1.2 拓扑结构

常指组网是线缆的铺设形式；

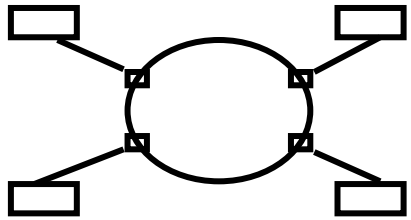
常采用图论的术语：点—结点（计算机和网络设备）、

线—传输媒体。

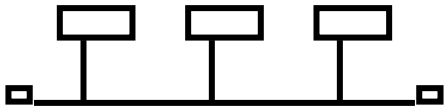
不同的线缆铺设形式导致了不同的媒体访问技术，现阶段常用媒体访问技术来隐指采用的拓扑结构。



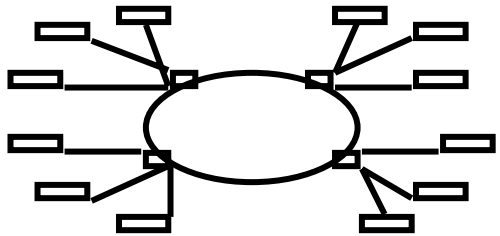
星形结构



环形结构



总线结构



环星形结构

4.1.3 传输媒体和传输技术

（1） 传输媒体的选择：

★费用： 购置、安装和维护媒体所需的费用；

★容量： 媒体的性能应满足现在和未来的应用需求；

★可靠性：接线的可靠性、媒体本身的误码率和抗干扰能力等；

★环境：距离、电磁场影响和地势等因素

（2） 传输媒体的类型

★ 双绞线 （距离百米以内）

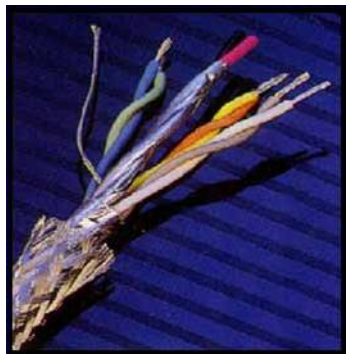
— 非屏蔽双绞线；

— 屏蔽双绞线： 电气干扰小

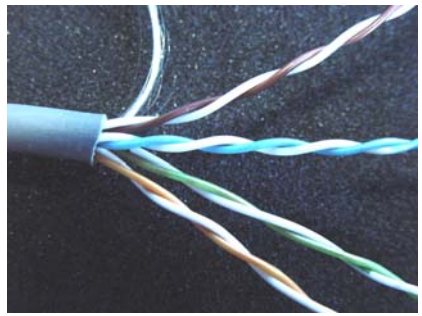
电气/电信业协会（EIA/TIA）

根据线的质量分类：

STP



UTP

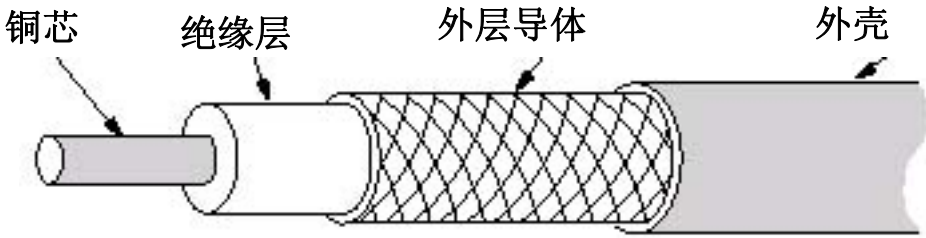


类型	3	4	5	5+	6	7
带宽(MHz)	16MHz	20	100	175	200	600
速率(Mbps)	10	20	100	1000	1000	10G

(2) 传输媒体的类型（续）

★ 同轴电缆（细缆：1.02cm，粗缆：2.54cm）

通信距离可达数公里，传输速率可达100Mbps；



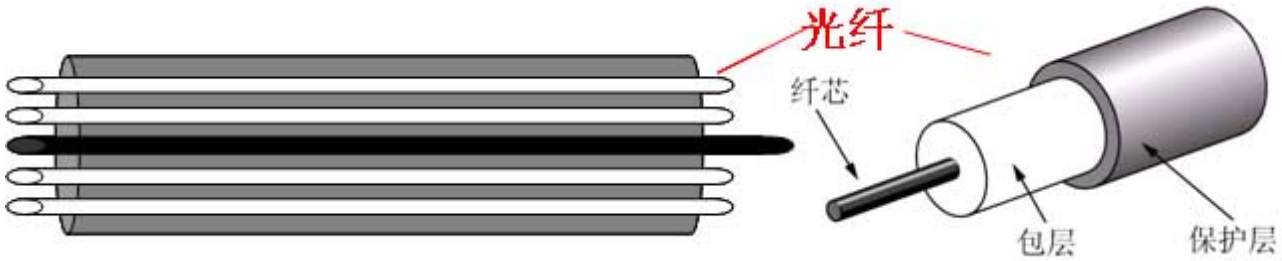
(2) 传输媒体的类型（续）

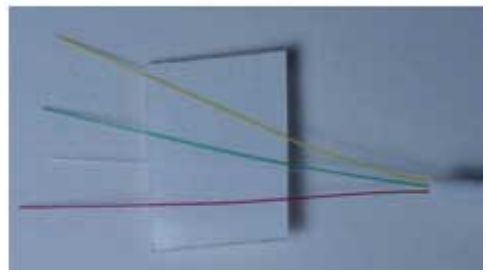
★ 光纤（光缆）：具有误码率低、频带宽、绝缘性能高、抗干扰能力强，体积小和重量轻的特点。

—单模光纤：支持激光传输，距离可达100公里；

—多模光纤：支持荧光传输，距离一般在2公里以内。

实验传输速率可达50Tbps，实用速率已达10Gbps。





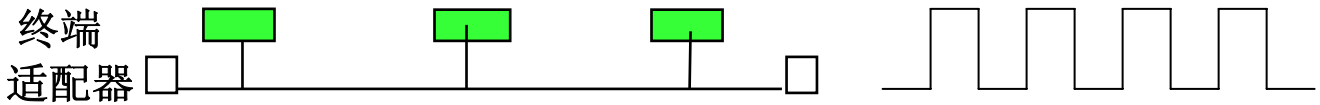
（3） 传输技术

★ 基带传输：

保持数据波的原样进行传输；

常采用时分（或波分）多路复用技术支持多路信号传输；

数据波信号的传输会随着距离的增加而衰减，随着频率的增加而容易发生畸变，因此，基带传输不适合高速和远距离的传输。



★ 宽带传输：

采用调制的方法，以连续不间断的电磁波来传输信号；

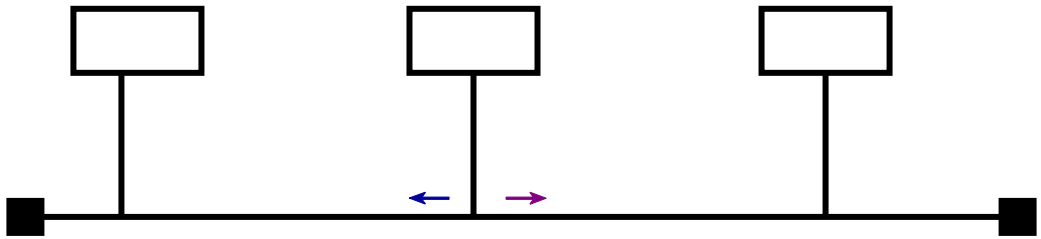
常采用频分多路复用的技术，支持多路信号的传输；

与基带传输相比，具有较高的传输速率和抗干扰的能力。

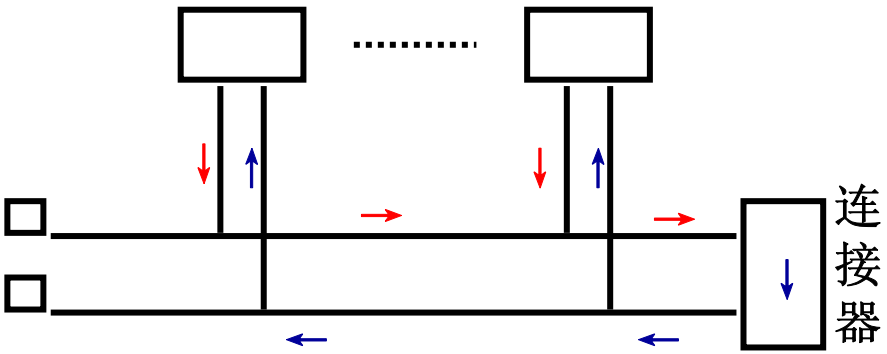
无论基带/宽带，都可保证结点之间的数据传输。

★ 传输方向：信号在媒体中的传输方向

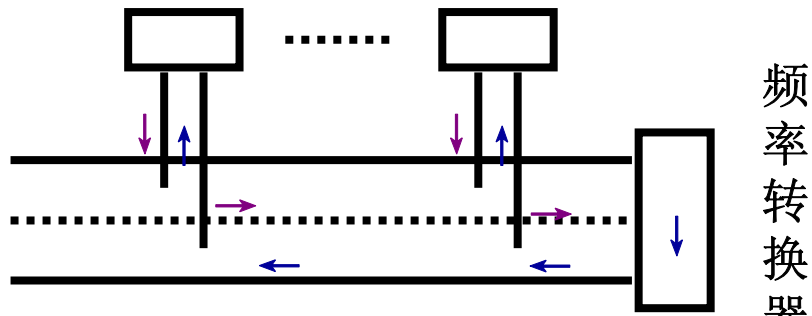
基带传输：基带信号可以同时向两个方向扩散，直至被终端适配器吸收；



宽带传输：模拟信号仅向单个方向传输。



双 缆 宽 带



中 分 宽 带

★距离问题

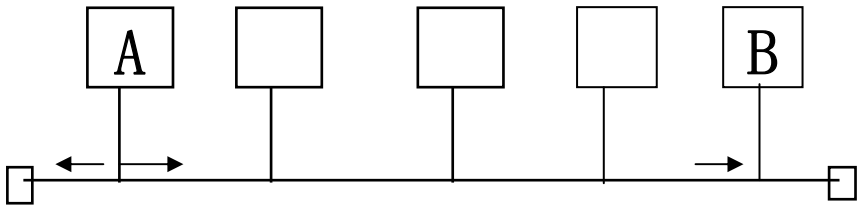
结点之间的实际距离:表示连接两个结点的导线长度，

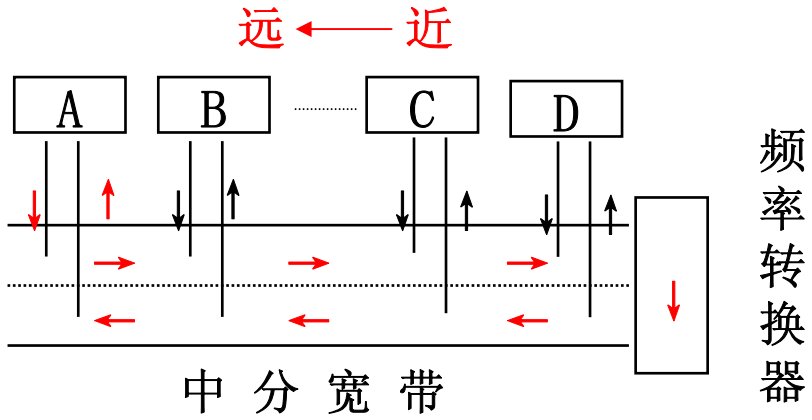
结点之间的传播距离:表示信号从一个结点传播到另一个结点（或者被另一个结点所感知）的距离，

实际距离和传播距离之间并不总是存在正比的关系。

基带传输:信号同时向两个方向扩散，传播时间与实际距离成正比，实际距离最远的两个结点之间的信号传播距离也最远。

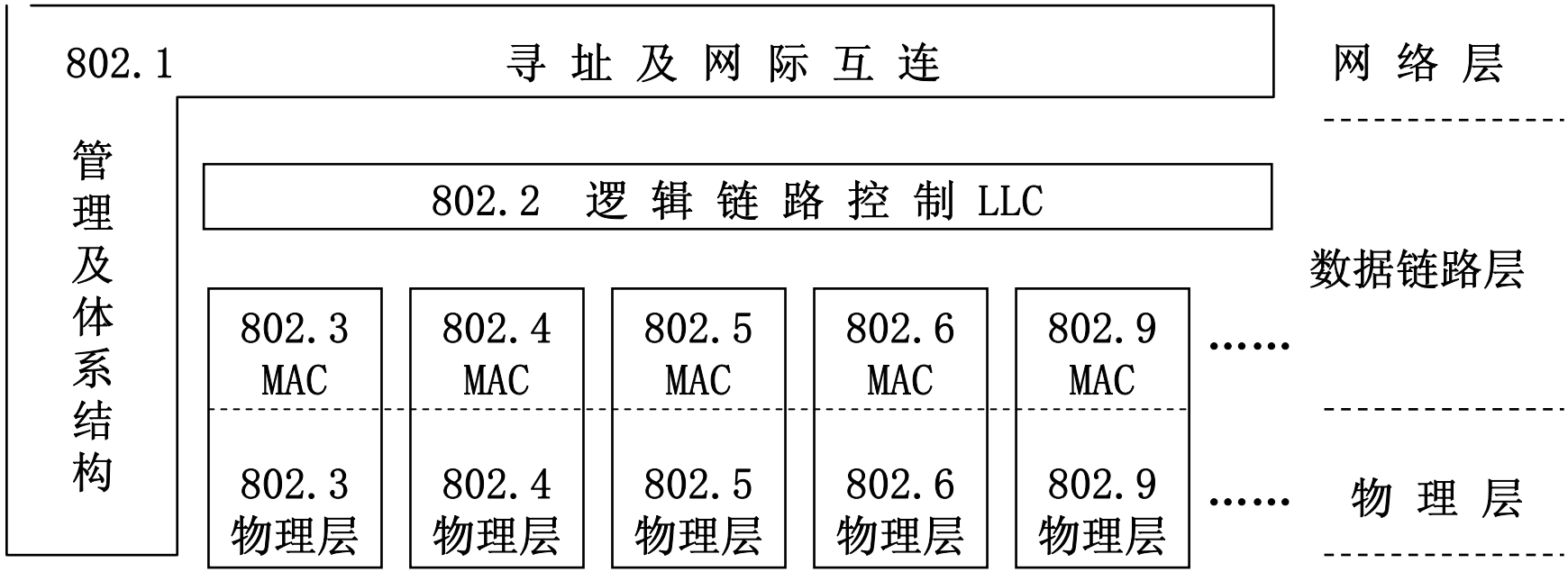
宽带传输:信号仅向一个方向扩散，传播时间与实际距离不一定成正比，相邻两结点传播距离可能最远。传播距离正比于至转换/连接器的距离。





4.1.4 LAN的逻辑结构

局域网使用高性能的传输媒体，导致专门的媒体访问技术，故体系结构可参照OSI/RM，差异仅在下三层；

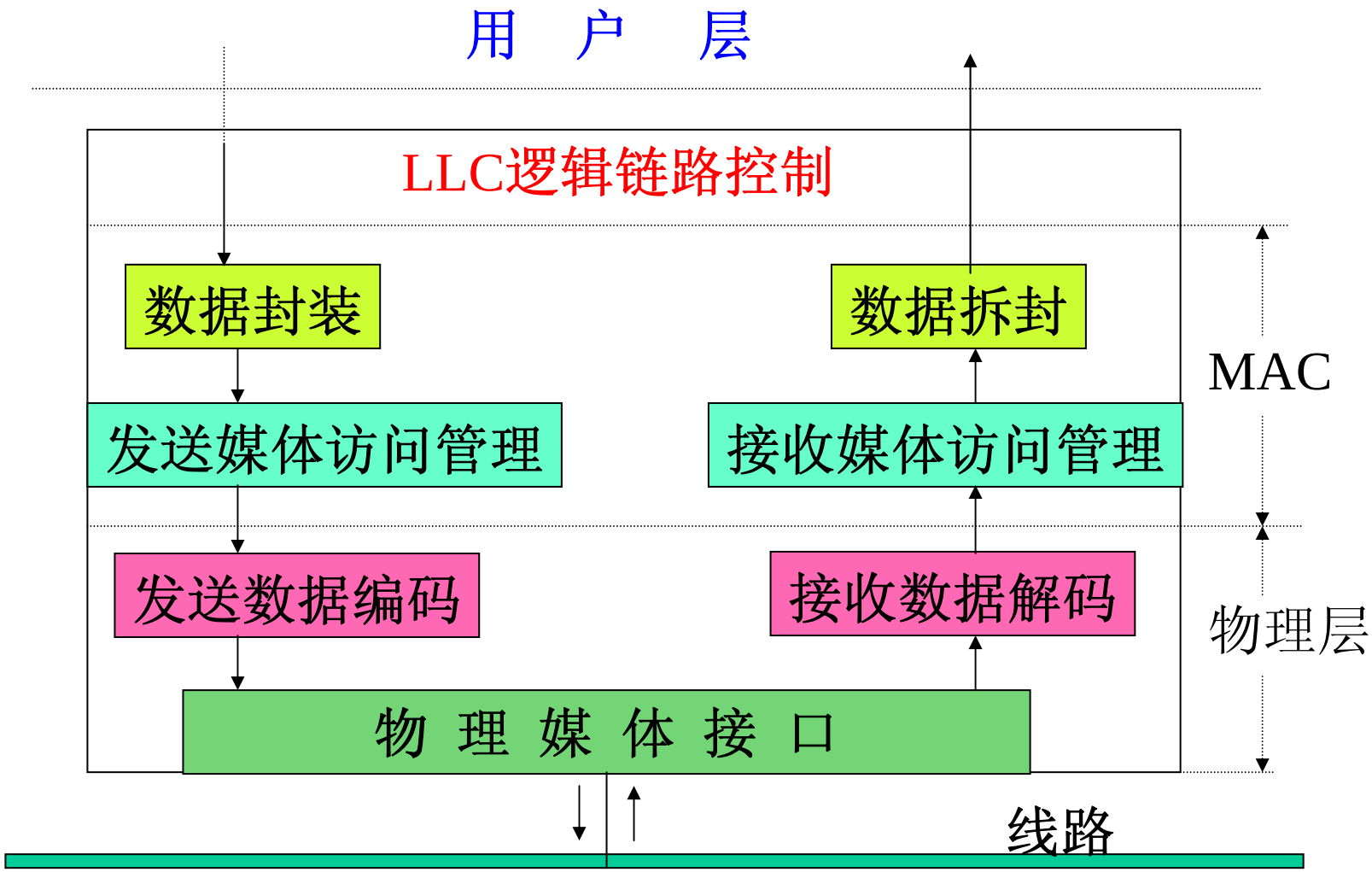


LAN物理层：定义结点和传输媒体的接口特性；

LAN的MAC子层：定义结点共享传输媒体时采用的访问控制技术；

LAN的LLC子层：屏蔽不同MAC子层的差异，提供统一的接口；

局域网设备工作原理


用 户 层
LLC逻辑链路控制
数据封装
数据拆封
发送媒体访问管理
接收媒体访问管理
发送数据编码
接收数据解码
物 理 媒 体 接 口
线路
MAC
物理层

4.2 星形网（结点之间的通信必须经由中央结点）

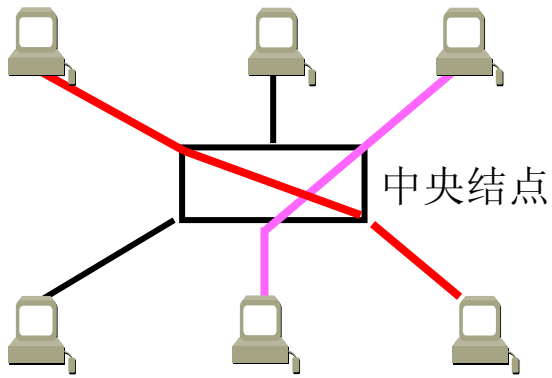
（1）电路交换工作方式

交换机通常可以提供多条链路，

可以同时支持多对结点之间的信息交换，

数据传输完毕，释放物理信道。

电路交换的特点：连接建立和释放需要一定的时间延迟；一旦物理连接建立后，结点之间通信无延迟



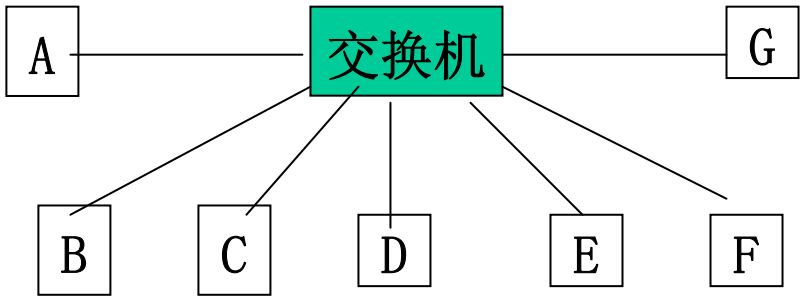
（2） 轮询工作方式

★交换机维护一个轮询表，表中给出轮询结点的顺序(优先级）；

★交换机根据轮询表，依次通知结点发送数据；

★如果结点有数据发送，则数据发送给交换机；交换机根据地址信息，将数据转发给某个或者某些接收结点；

★传输延迟较大，数据交换包括“结点—交换机—结点”的两次转发过程；



轮询表

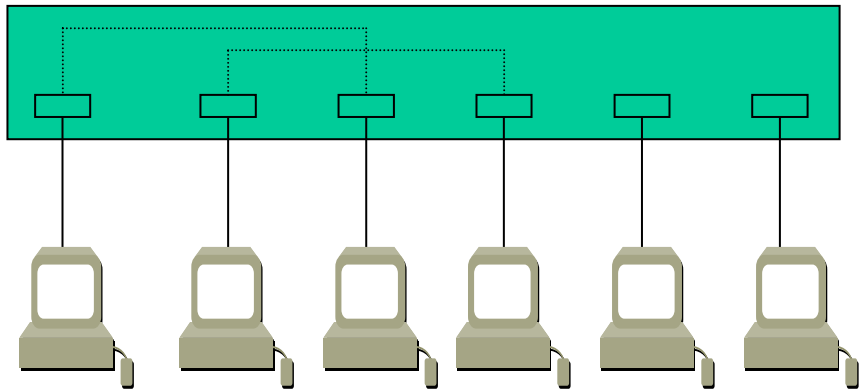
1：A, E, D, G, B, C, F

2：A, B, A, C, A, D, A, E, A, F, A, G

（3） 请求优先级工作方式

轮询与电路交换相结合的工作方式；

交换机按优先级轮询每个交换端口，端口附接的结点有数据发送，根据地址，采用电路硬件交换方式直接传输。



传统的星形网络的优点：控制简单，易于实现；

弱点：交换机—星形网络的瓶颈，控制关系限制了性能；

4.3 总线局域网

4.3.1总线网结构

所有的结点通过专门的网卡附接到一条总线上；

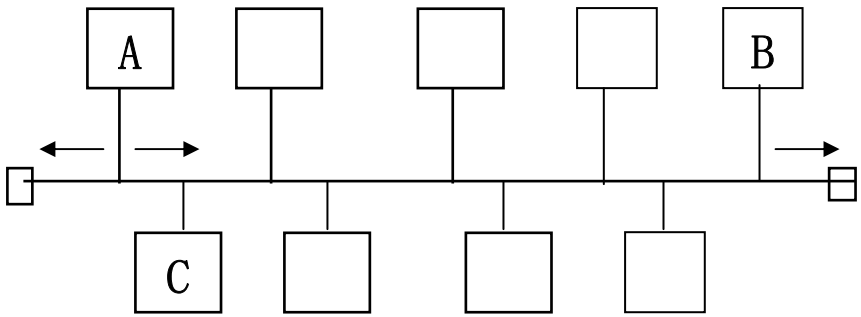
所有结点的信息都发送到同一条总线上（冲突）；

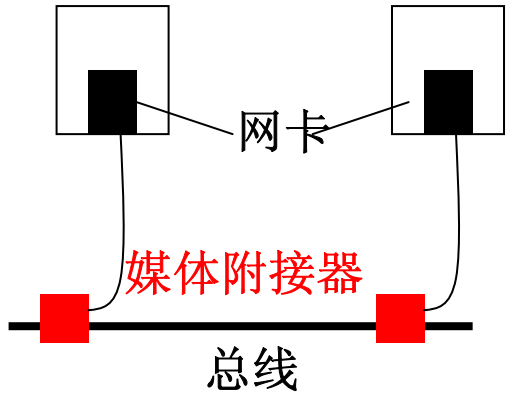
所有结点都从同一媒体上收取信息（广播）；

为了防止信号反射，总线的两端采用终接器，吸收信号

采用分布式方式进行工作，结点之间不存在控制的关系。

应解决的问题：对总线的访问和控制。



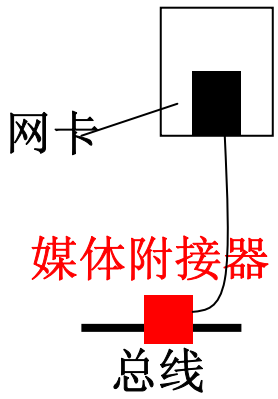


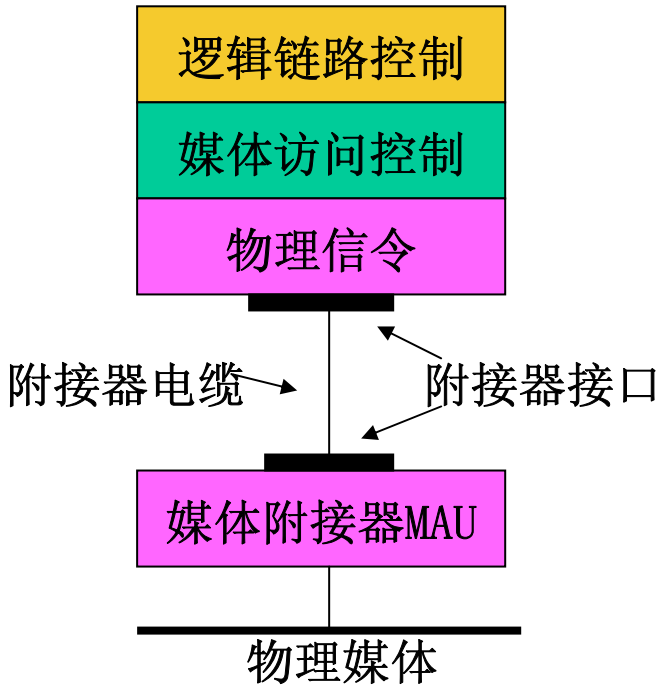
4.3.2 载波侦听多路访问/冲突检测（CSMA/CD）

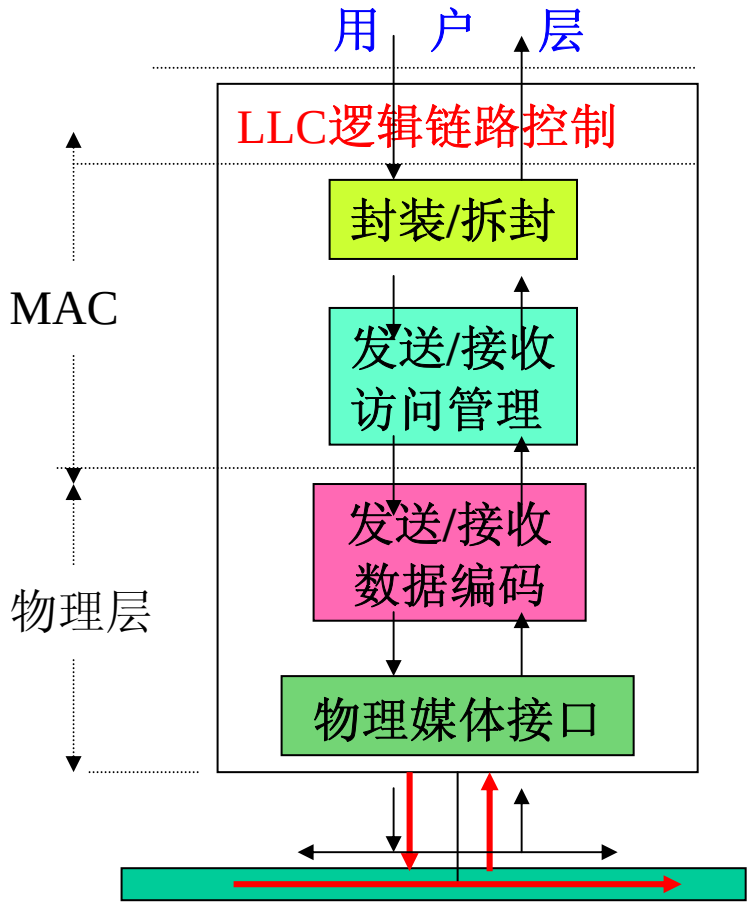
★载波侦听：侦听媒体是否空闲（说前先听）

★多路访问：多个结点共享媒体，多个结点同时获取信息

★冲突检测：监听媒体，检测冲突（边说边听）。



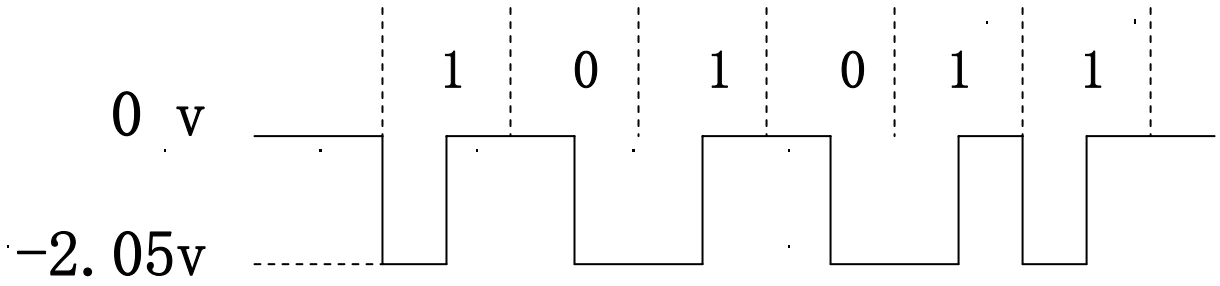




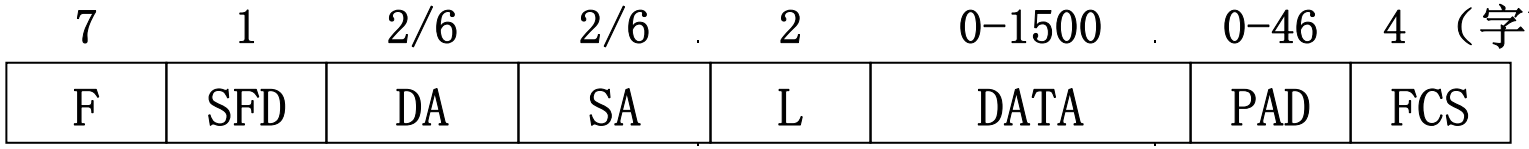
（1） 物理层的功能

★ 接收来自于MAC的比特流，编码并发送至媒体；
接收来自于媒体的比特信号，解码并转发至MAC；
向MAC报告媒体的状态（冲突？比特传输正确/错误？）

★ 使用的比特信号编码：曼彻斯特编码；



（2） CSMA/CD帧的格式



前导码（F） 10101010101010.....10101010（7个字节），同步用

帧开始标志（SFD） 10101011

信宿地址（DA）、信源地址（SA）

单地址的地址字段最高位为0，表示网络中的某个特定的结点；

成组地址的地址字段最高位为1，表示网络中的某些结点；

广播地址的地址字段的所有位均为1，表示网络中的所有结点；

数据长度（L）：有效数据的实际长度；

用户数据（DATA）：小于1500字节，存放高层LLC的信息；

填充字段（PAD）：不大于46字节，采用填充无用字符的方式（以字节为单位）保证整个帧长度不小于64个字节。

帧校验序列（FCS）：循环冗余校验码。

★ 帧最小长度需求的说明

CSMA/CD要求整个帧的长度应不小于64字节。

目的：保证发送结点可以对发生的冲突进行有效的检测。

即：帧发送完之前，应当保证所有结点都可侦听到媒体上有信息在传输，从而暂停发送动作；

或者：若某个其他结点也启动发送过程，则结点应在发送完帧之前感知到冲突信号；

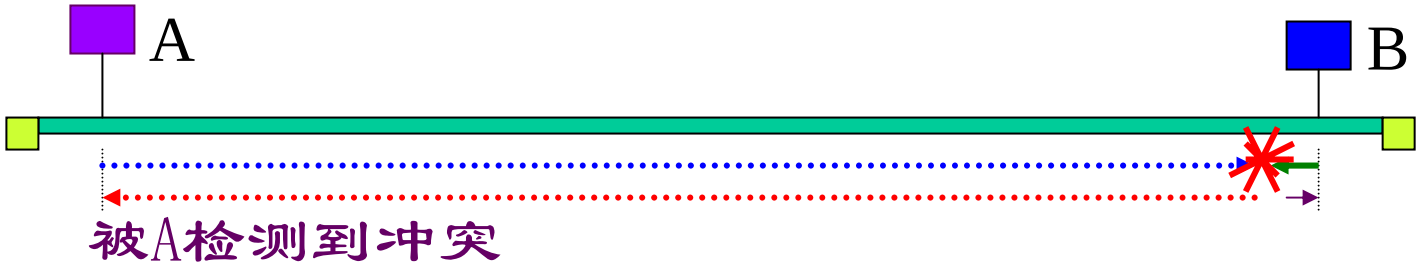
要求：整个帧的发送时间应当不小于信号在网络中“传播距离最大”的两个结点之间传播时间的两倍：

分别对应信号到达“最远”的结点，以及冲突信号从“最远”的结点返回本结点。

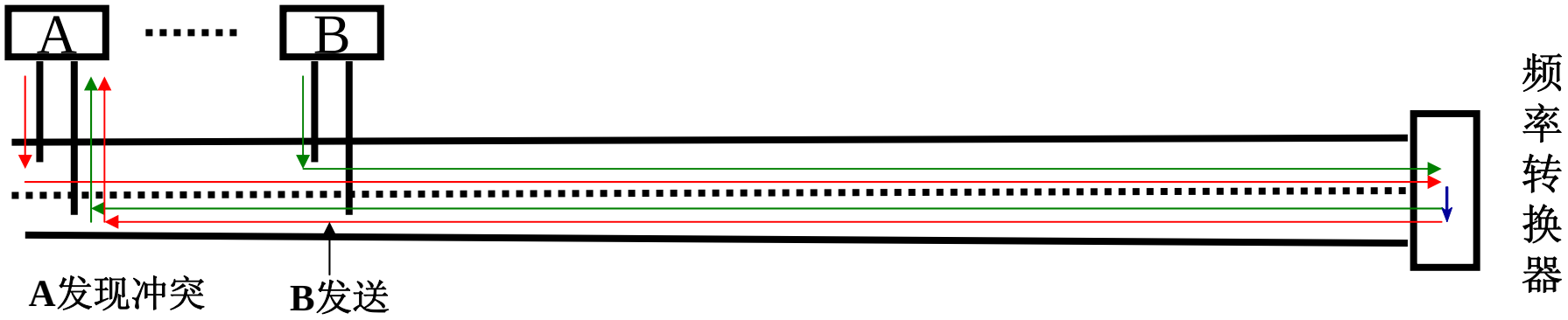
★ 传输冲突示意

基带传输冲突：

AB为最远点



宽带传输冲突：

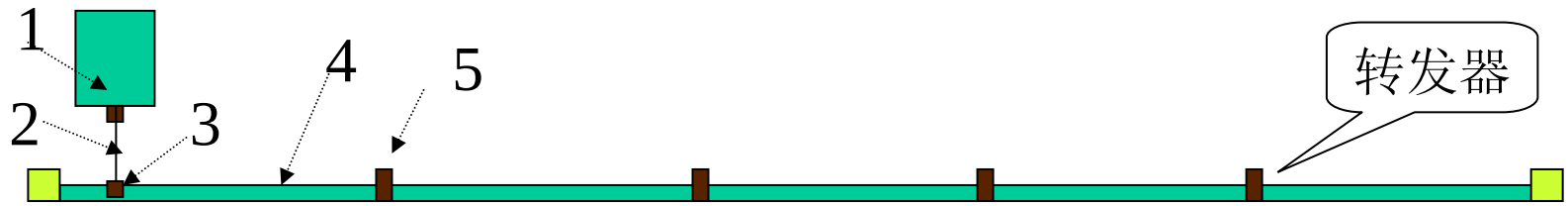


A发送的帧长度必须足够大，确保A在检测到冲突时还在发送数据

★ 帧实际传输时间的估算

帧从结点传输到媒体的时间 + 在媒体上传输的时间 + 可能经过的转发器的处理的时间

CSMA/CD 802.3标准为10Base5
基带传输，速率10Mbps，粗同轴电缆，单段最长500米，5段



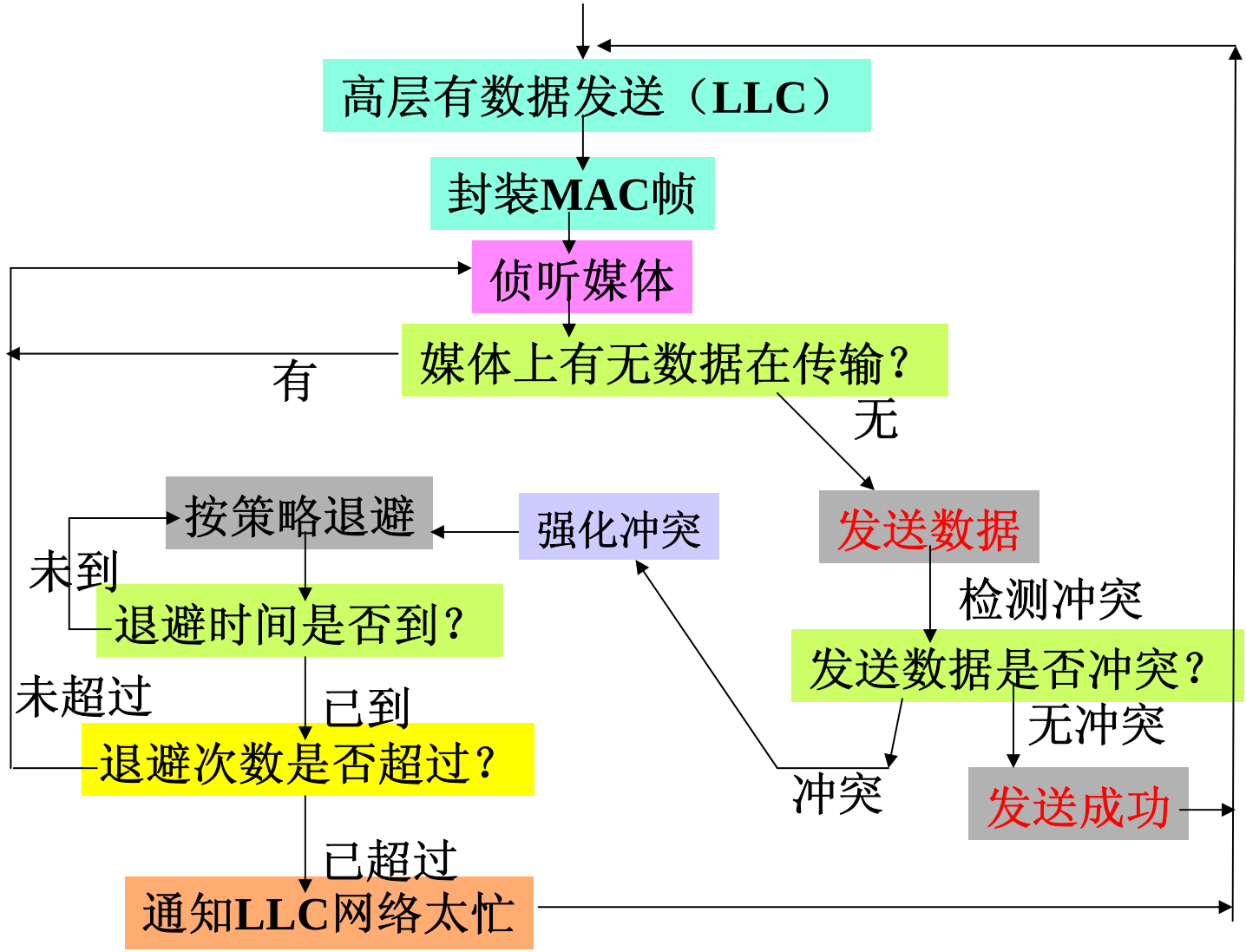
（速率为10Mbps：0.1us/比特时间；
媒体上电信号的传输速率为20万公里/秒：1000米/5us，20米/比特时间）

1、结点处理信号的时间约20比特
2、从结点到媒体的时间（50米）约2.5比特
3、结点MAU转发时间约20比特
4、2500米传输所需时间约125比特
5、4个转发器转发时间约80比特（20比特/转发器）

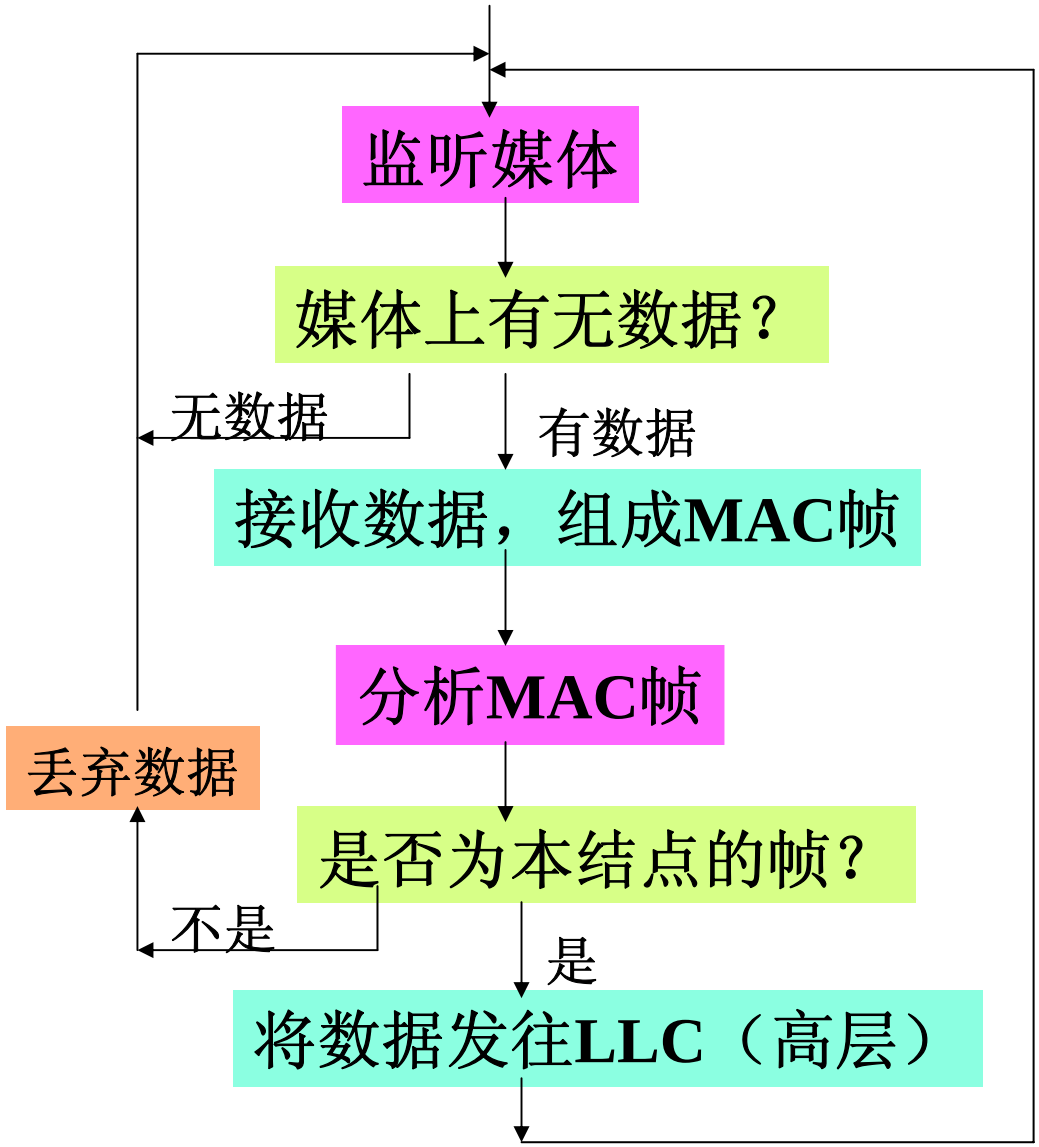
（125+100+22.5）*2
=247.5*2
约需512比特时间
64个字节
18+46（PAD）

(3) CSMA/CD工作过程

★ 数据发送过程



★数据接收过程


监听媒体
媒体上有无数据？
无数据
有数据
接收数据，组成MAC帧
分析MAC帧
丢弃数据
是否为本结点的帧？
不是
是
将数据发往LLC（高层）

★ 二进制指数退避算法

退避时间计算：信号在媒体上的往返时间 * 随机数；

随机数(r)的取值范围依赖于冲突的次数(i)；$0 \leqslant r < 2^i$

思路：错开等待时间，使之随失败次数增多而增加。

冲突次数	随机数（r）取值范围
1	2^1-1：（0，1）
2	2^2-1：（0，1，2，3）
……	
10	$2^{10}-1$：（0，……，1023）
……	
15	$2^{10}-1$：（0，……，1023）
16	向上层报错

（4） CSMA/CD的特点

★ 竞争总线，各结点抢占对共享媒体的访问权；

★ 结点共享媒体，任何时刻只有一个结点可发信息；

★ 轻负载时，冲突少，效率较高（易获访问权）；

★ 重负载时，冲突概率加大，效率低；

★ 发送时间难以预测，可能不适合实时传输。

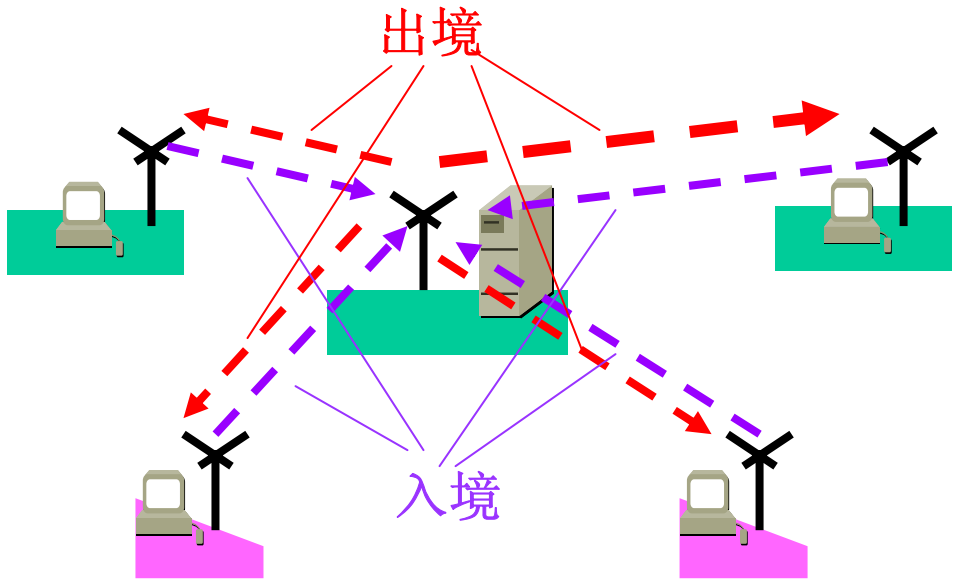
（1） 以太网的起源

60年代末期，夏威夷大学Norman Abramson等研制ALOHA无线网络系统，实现Oahu岛上的主机和其它岛及船上的读卡机和终端通信；

出境信道+地址：主机到终端；

入境信道：终端到主机；200-1500毫微秒未收应答，随机重发；

70年提出ALOHA模型，争用性协议成果获IEEE Kobayashi奖。



（1）以太网的起源（续）

72年Xerox公司研制第一台PC（ALTO），Metcalfe等人阅读Abramson论文，思想用于ALTO互连，形成ALTO ALOHA网络，

73年5月22日，正式运行，命名Ethernet；

77年底，Metcalfe等人获“具有冲突检测的多点数据通信系统”专利；

79年，DEC（技术力量）、Intel（硅片）和Xerox（专利）公司共建产业标准；

80年9月，DIX V1.0—以太网：数据链路层和物理层规范；

82年，DIX V2.0—以太网标准；

凡低二层遵循DIX规范的网络的都可称为以太网。

80年，IEEE成立802委员会研究LAN国际标准；

81年6月，成立802.3分委会，研究基于DIX成果的国际标准；

82年12月，802.3草案标准；83年802.3标准。

（2）DIX规范

DIX V2.0—以太网：数据链路层和物理层规范。

★ 描述方法：速率，传输技术，最大段长；

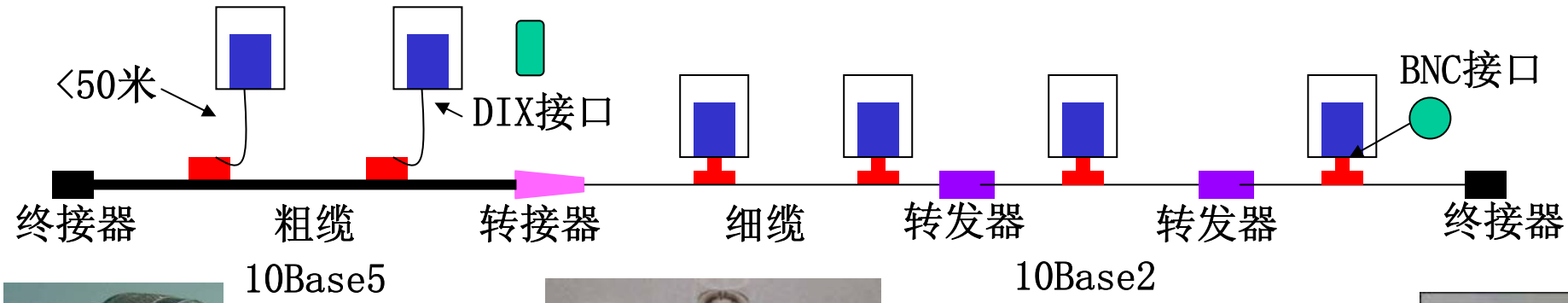
相关标准：10Base5和10Base2。

★ 基本指标：

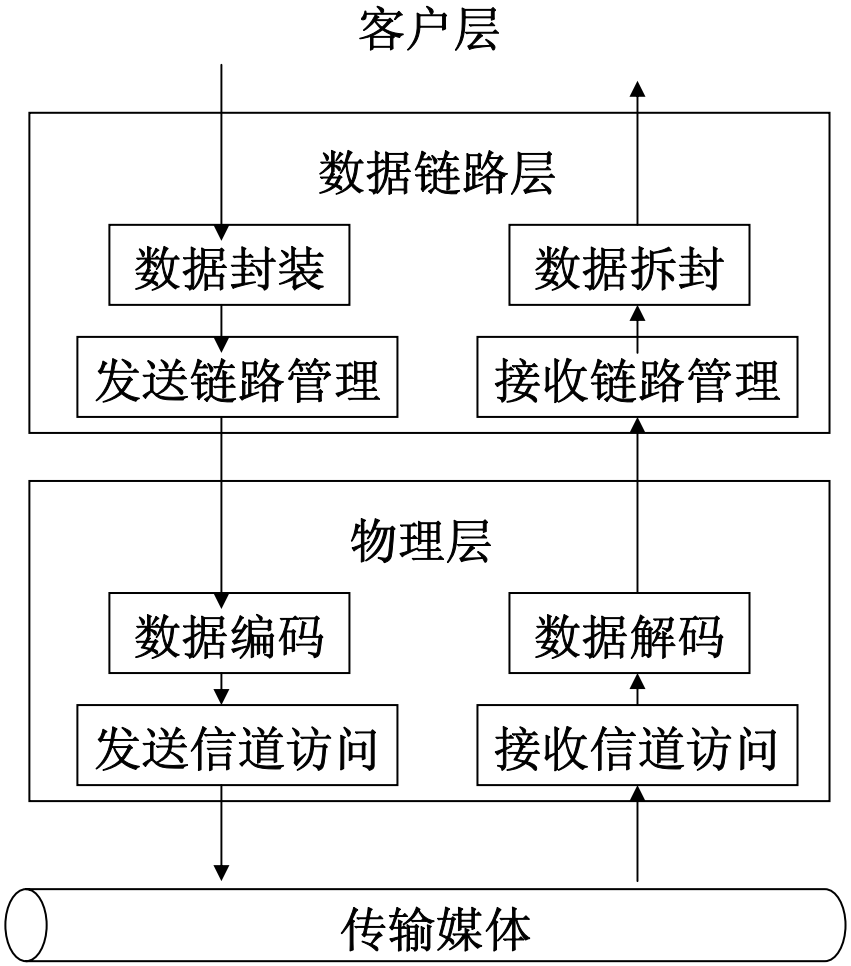
10Base5：粗缆，10Mbps，基带，单段线缆<500米，5段，DIX接口；

10Base2：细缆，10Mbps，基带，单段线缆<200米，5段，BNC接口；

设计时的基本长度换算公式：1米细缆＝3米粗缆



★ 以太网参考模型



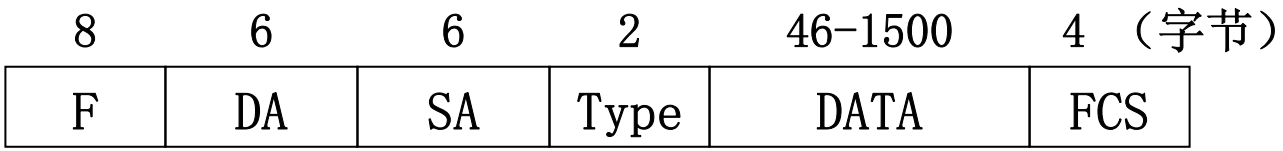
封装/拆封：组帧，包括增加/移去帧中控制信息；

链路管理：包括侦听、冲突强化和重发调度；

编码/解码：曼彻斯特编码；

信道访问：侦听、检测冲突和发/收位信号。

★ 帧格式



F（帧起始符）：‘01010101’* 8，由编码/解码模块形成和移去；

DA/SA（源/宿地址）—网卡地址；

Type（帧类型）：高层定义，包括Ack；

Data（数据）：高层数据，用户满足长度要求；

FCS（帧校验）：CRC。

整个帧长（含起始符）为72—1526字节。

★ 工作过程（接收）

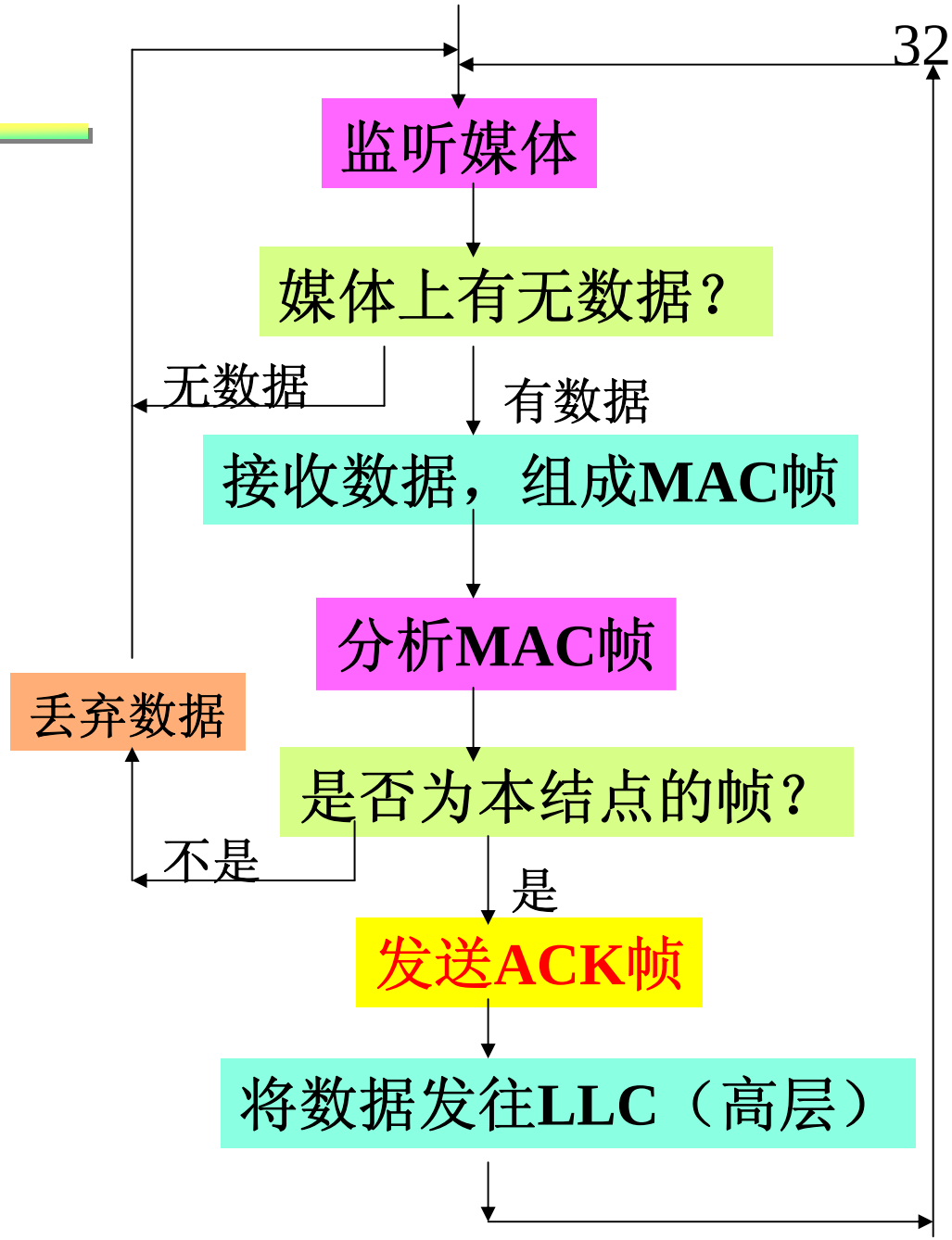
（类似802.3标准）

差异：

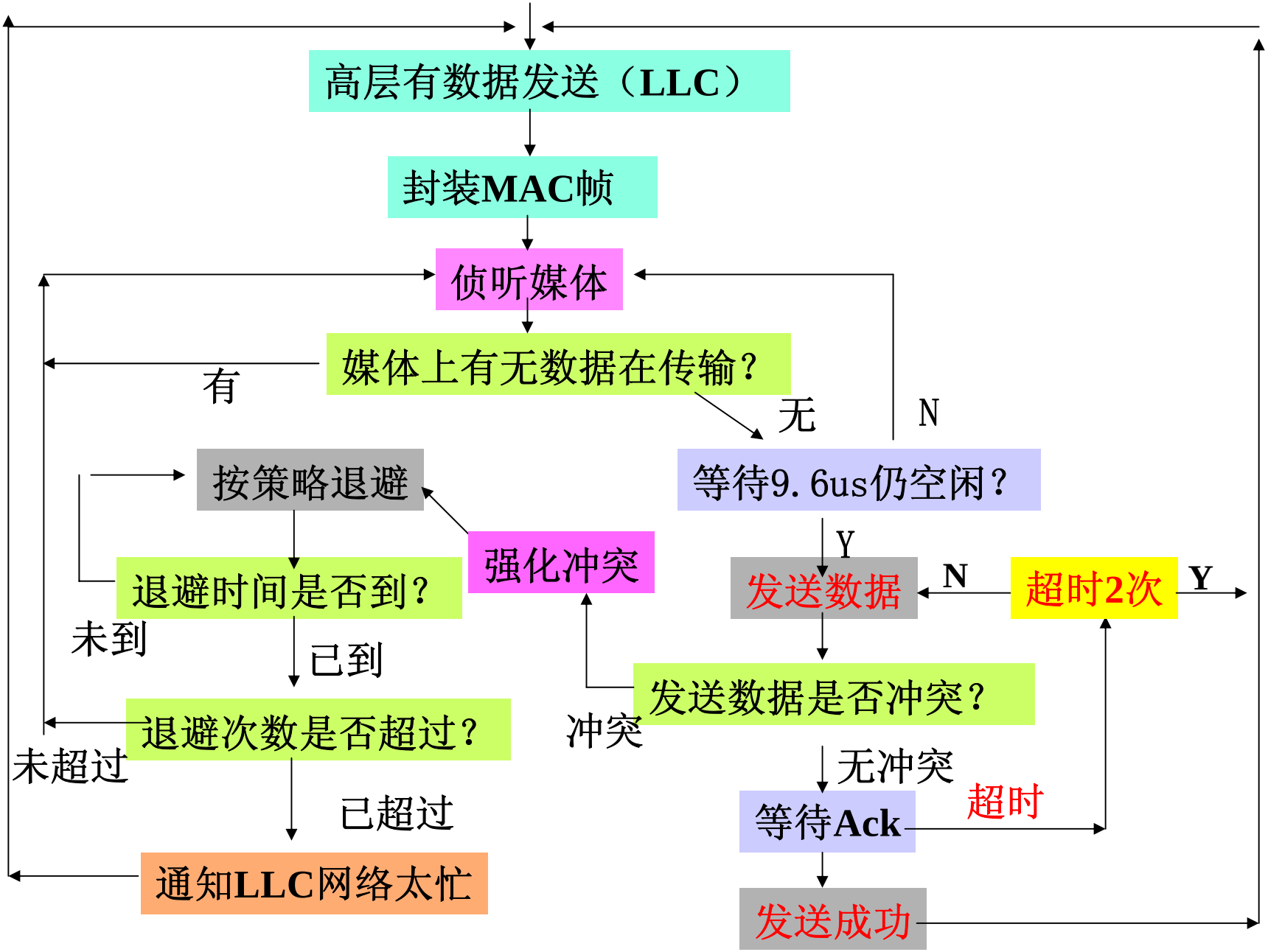
增加了确认帧（ACK帧）和等待ACK帧（9.6us），超时重发；

利用ACK帧来保证传输的有效性。

定义了帧间间隔（不能连续发数据，需等待一个时间间隔,保证ACK帧传输）。



★ 工作过程（发送）


高层有数据发送（LLC）
封装MAC帧
侦听媒体
媒体上有无数据在传输？
有
无
N
等待9.6us仍空闲？
Y
发送数据
N
超时2次
Y
发送数据是否冲突？
冲突
无冲突
等待Ack
超时
发送成功
强化冲突
按策略退避
退避时间是否到？
未到
已到
退避次数是否超过？
未超过
已超过
通知LLC网络太忙

（3） 基于总线的以太网的特点

★ 采用CSMA/CD工作模式，共享总线；

★ 重负载时，碰撞增多，性能下降；

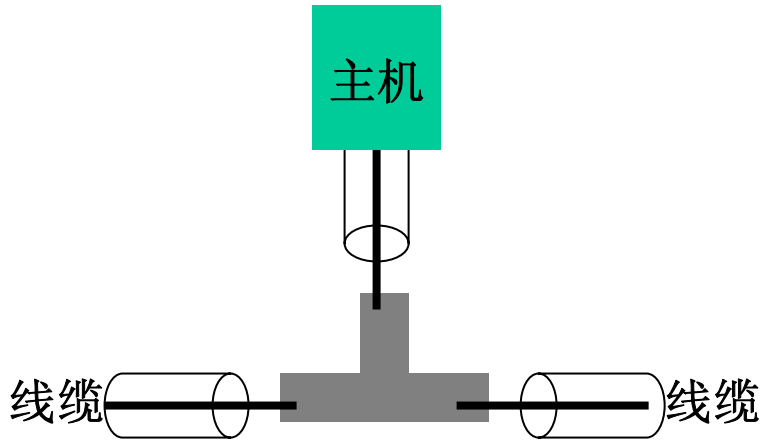
★ 协议简单，控制方便；

★ 用户多，造价低；

★ 接入结点时，需割开线缆，易引起碰线导致整个网络瘫痪；

★ 不利于故障查找、搬迁和布线。

改进：采用双绞线代替同轴电缆。



（4） 以太网的变迁（一）

★ 基于集线器（HUB）的以太网

促进因素：80年代初，光缆实验成果（要求星型结构）；

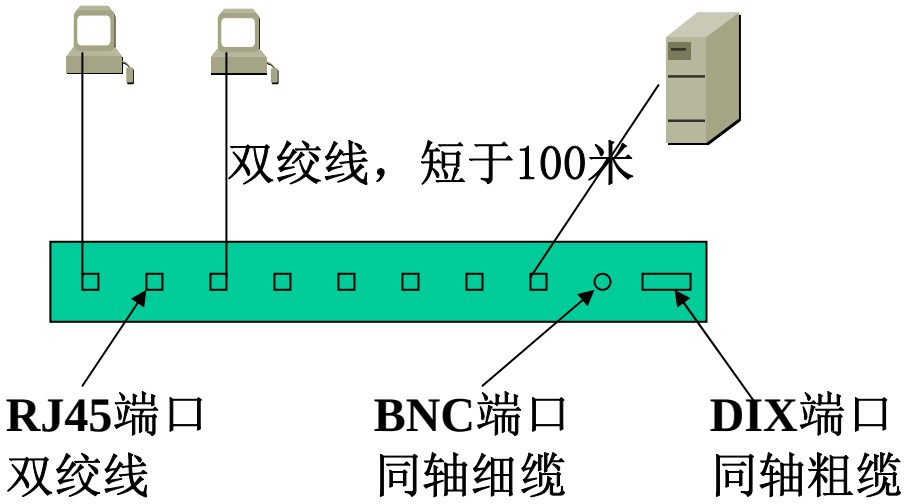
星型结构网的应用（IBM令牌环，Intel StarLAN）；

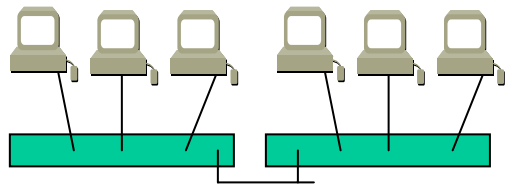
87年8月，SynOptics的基于UTP电话线的以太网产品问世；

同期，HP的多端口中继器方案得到支持；

90年秋，10Base-T（802.3i）公布。

指导思想：总线凝聚为一点（集线器），结点通过双绞线接入；





HUB串接/堆叠

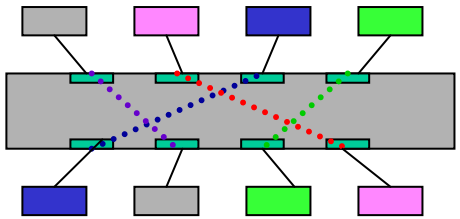
★以太网的变迁（二）—交换以太网

集线器的应用使网络性能改进可集中于“一点”；

80年代末，系列智能型多端口集线器问世；

90年，Kalpana公司推出EtherSwitch产品；

共享式集线器向独享端口的交换器发展。将一个端口的输入交换到指定的另一端口，独享端口的带宽。



1、直通（cut-through）

工作原理：

前14个字节收到后，得知目的地址，直接送往目的地端口，

- 优点：

  延迟小（14个字节），交换速度快。

- 缺点：

  无法检测出冲突帧（14字节）和出错帧。

以太网的变迁（二）—交换以太网（续）

2、存储转发（Store—Forward）

工作原理：

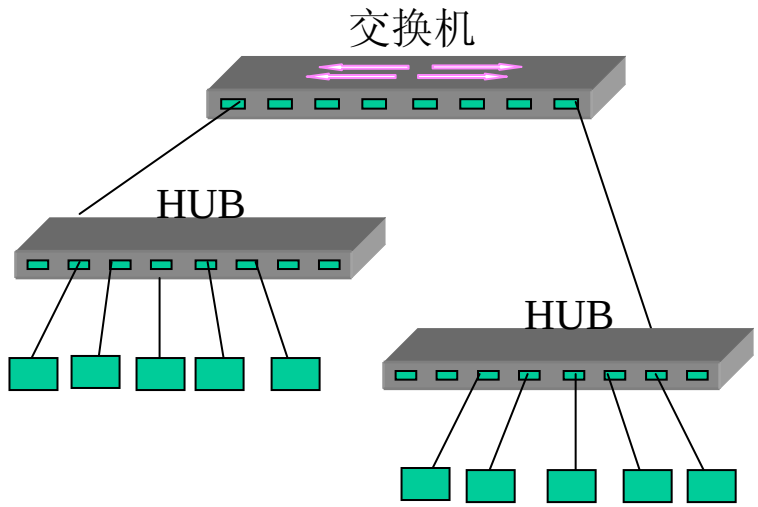
全部帧接收到后，检查出错帧，如无错才送往目的地端口，

- 优点：

可以检查出冲突帧和出错帧，使转发的帧为有效帧。

- 缺点：

延迟较大（整个帧），交换速度较慢。



以太网的变迁（二）—交换以太网（续）

3、自适应（直通/存储转发）

工作原理：

交换机根据网络的状况自动更换数据交换方式。

* 当网络性能好时，单位时间内出错的帧的概率 < 某个阈值，采用“直通”的交换方式；

* 当网络性能差时，单位时间内出错的帧的概率 > 某个阈值，采用“存储转发”的交换方式；

- 特点：

可以提高交换机的数据交换速率。

★以太网的变迁（三）—全双工以太网

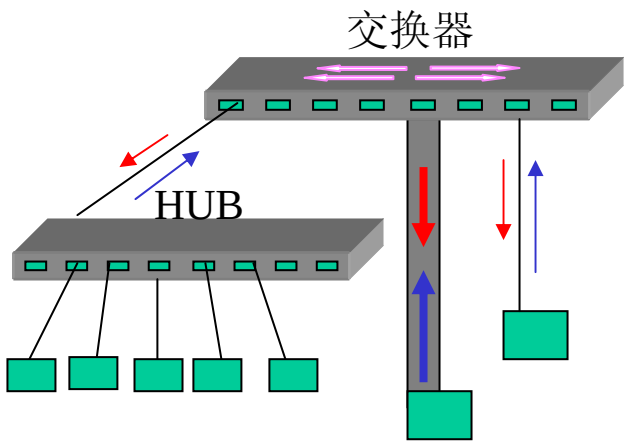
93年，Kalpana公司再次率先推出改进产品—全双工交换器。

全双工方式：

交换器的端口和网卡都可以同时进行MAC帧的发送和接受

交换器的端口可以由用户自己设置，10Mbps的端口如果设置成全双工的方式，理论上可达20Mbps的端口速率。

要求：交换器/网卡，交换器/交换器都必须支持全双工工作。



★以太网的变迁（四）—快速以太网（100Mbps）

92年起，开始研究更高速的以太网，Grand、Intel、Cabletron等成立“快速以太网联盟（FEA）”，促进标准：802.3u。

100 Base-TX：传输编码为4b/5b，

2对5类双绞线，100米

100 Base-FX：传输编码为4b/5b，

光纤，10/2公里（单模/多模）

100 Base-T4：3电平编码，4对3类双绞线，3对线同时传输。

原理：3电平3对线可有27个状态，表示4位数据（类似4b/5b）；

3类线具有25MHz的性能；可使总传输速率达100Mbps。

100 Base-T2：传输编码为5电平编码，

2对3类双绞线，（标准一直未确定）

★以太网的变迁（四）—快速以太网（续）

10/100Mbps自适应——增加自动速度感应功能

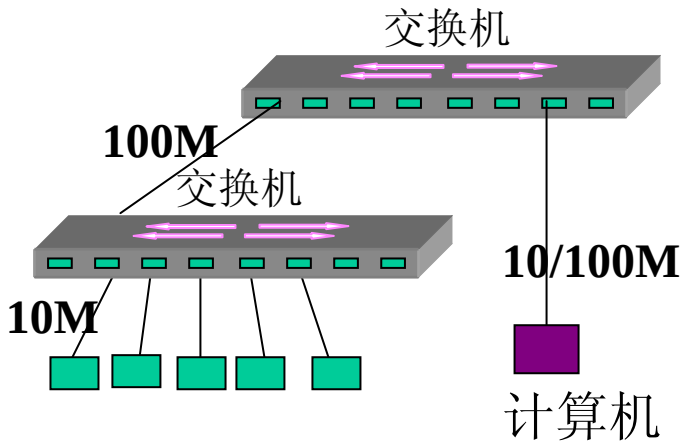
结点要求10/100Mbps自适应网卡支持。

原理：交换器发送高速链路脉冲（FLP），结点检测FLP，协商和确定可支持的最高交换速度，并进行模式调整：

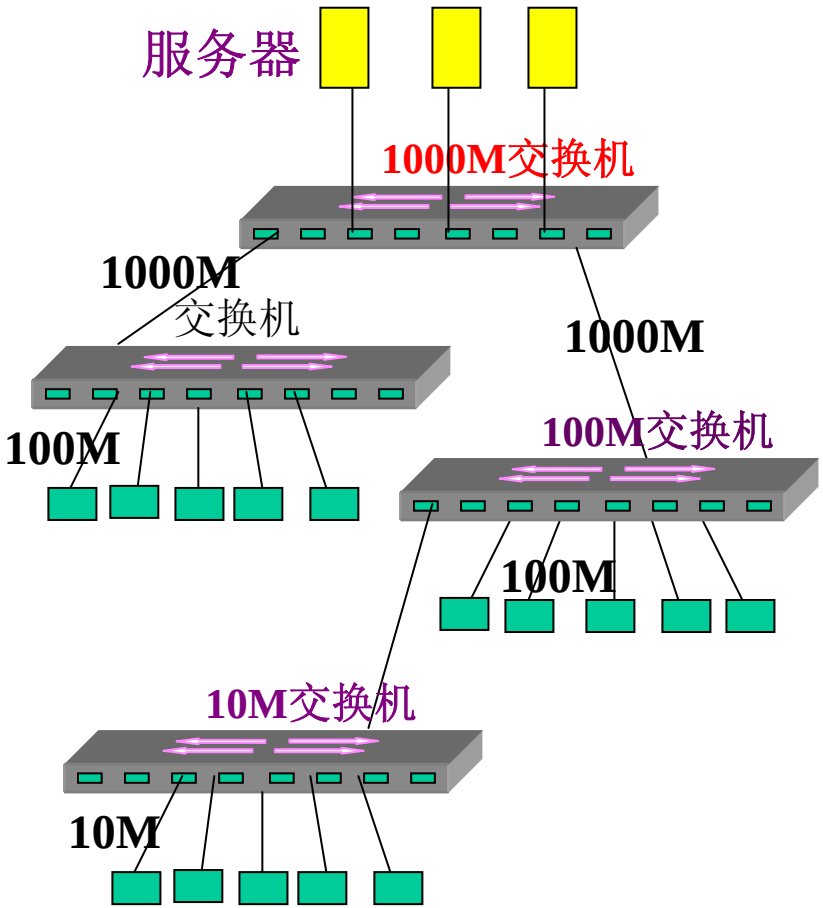
支持100Base-T，或者仍以10Base-T模式工作。

实践表明：使用10/100Mbps自适应，其性能并未有大的改善，

原因：交换器/结点不停地检测和模式改变，反而影响速度。



★以太网的变迁（五）—千兆位以太网



95年末，开始研究Gbps以太网，
标准：803.3z

重点：如何体现冲突检测特性；
方案：帧结联、载波扩展，
增加最短帧的长度。

成果：

1000Base-Sx，多模光纤，
短波（850nm），<300m
1000Base-Lx，　多模光纤，
长波（1300nm），<550m
1000Base-T，　双绞线，<25m

应用：主干网和服务器

例如：交换机—交换机，　交换机—服务器（需要1000Mbps网卡）

★以太网的变迁（六）—十千兆位以太网

1999年3月，开始讨论10G以太网；

2000年1月，802.3ae分委会开始工作，计划02年春出标准；

2000年7月，**3Com、Cisco、Extreme、Intel等10**公司成立**10G**以太网联盟**(10GEA)**，研究10G以太网产品。

2002年7月公布IEEE 802.3ae。

特点：保留以太网帧格式，以及帧长度规定，可和现有系统过渡。

方案：仅支持全双工通信；

光纤传输（波长：**850 nm, 1310 nm, 1550 nm**）；

传输距离：多模光纤：100米和300米；

单模光纤：2公里、10公里和40公里。

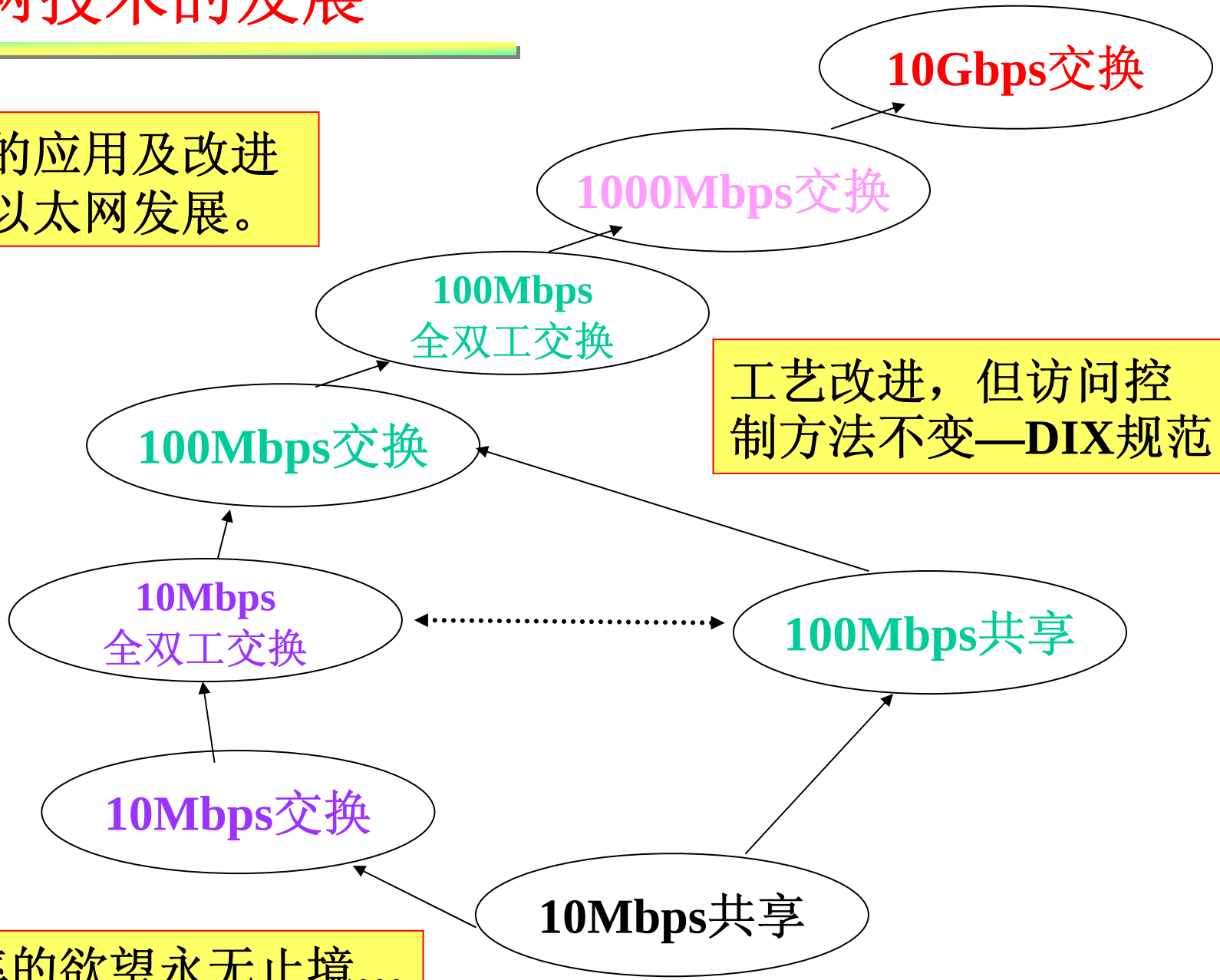
编码：64b/66b编码，速率可达10.3G；

8b/10b编码，则4线并行，4*3.125G=12.5G；

应用对象：主干网。

以太网技术的发展

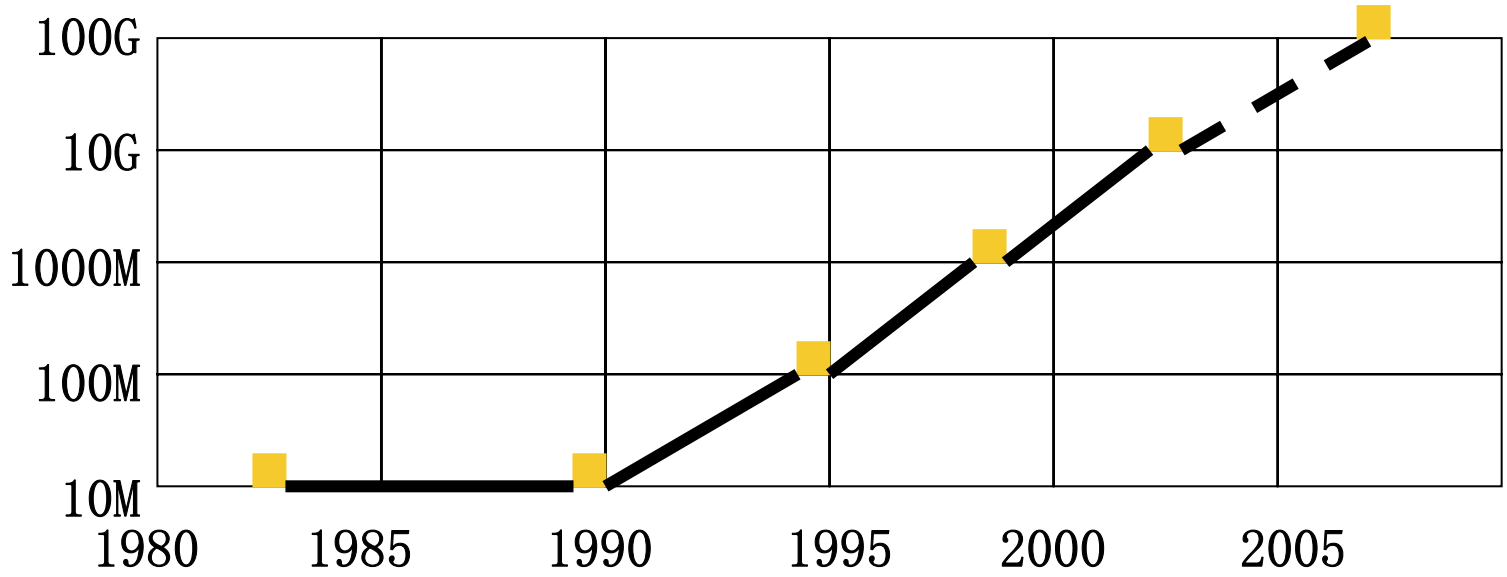
集线器的应用及改进
促进了以太网发展。



工艺改进，但访问控制方法不变—DIX规范。

追求速率的欲望永无止境…

以太网速率变迁示意



★ 集线器的应用，是以太网发展的重要的里程碑；

★ 需求刺激了新技术的研究，新工艺则促进了新产品面世；就以太网而言，原理是永恒的—DIX规范；

★ 集线器的使用使得总线型以太网具有星形拓扑的外观结构，但习惯上仍根据访问控制方法将其列为总线型网络。

以太网系列一览

IEEE802.3 —10BASE5—粗同轴电缆

IEEE802.3a—10BASE2—细同轴电缆

IEEE802.3i —10BASE-T—4对双绞线

IEEE802.3j —10BASE-F—多模/单模光纤

IEEE802.3u—100BASE-T4—4对5类双绞线

100BASE-TX—2 对5类双绞线

100BASE-FX—62.5/125um多模光纤

IEEE802.3z —1000BASE-SX—62.5/50um多模光纤

1000BASE-LX—单模光纤

1000BASE-CX—屏蔽双绞线

IEEE802.3ab—1000BASE-T—4对5类双绞线

IEEE802.3ae—10G Ethernet

4.3.4 令牌总线（Token-Bus）

CSMA/CD：　无序地使用总线——竞争；

Token-Bus：有序地访问总线——令牌（Token）；

令牌：结点获得总线使用权的标志；

标准：IEEE 802.4。

（1） 工作原理

★ 拓扑：总线方式，所有结点附接于总线（类似CSMA/CD）；

★ 逻辑环路：结点之间通过有序传递令牌（特定比特模式）来分配各结点对共享型总线的访问权利，形成闭合的逻辑环路；

★ 半双工操作方式，只有获得令牌的结点才能发送信息，其它结点只能接收信息，或者被动地发送信息（在拥有令牌的结点要求下，发送信息）；

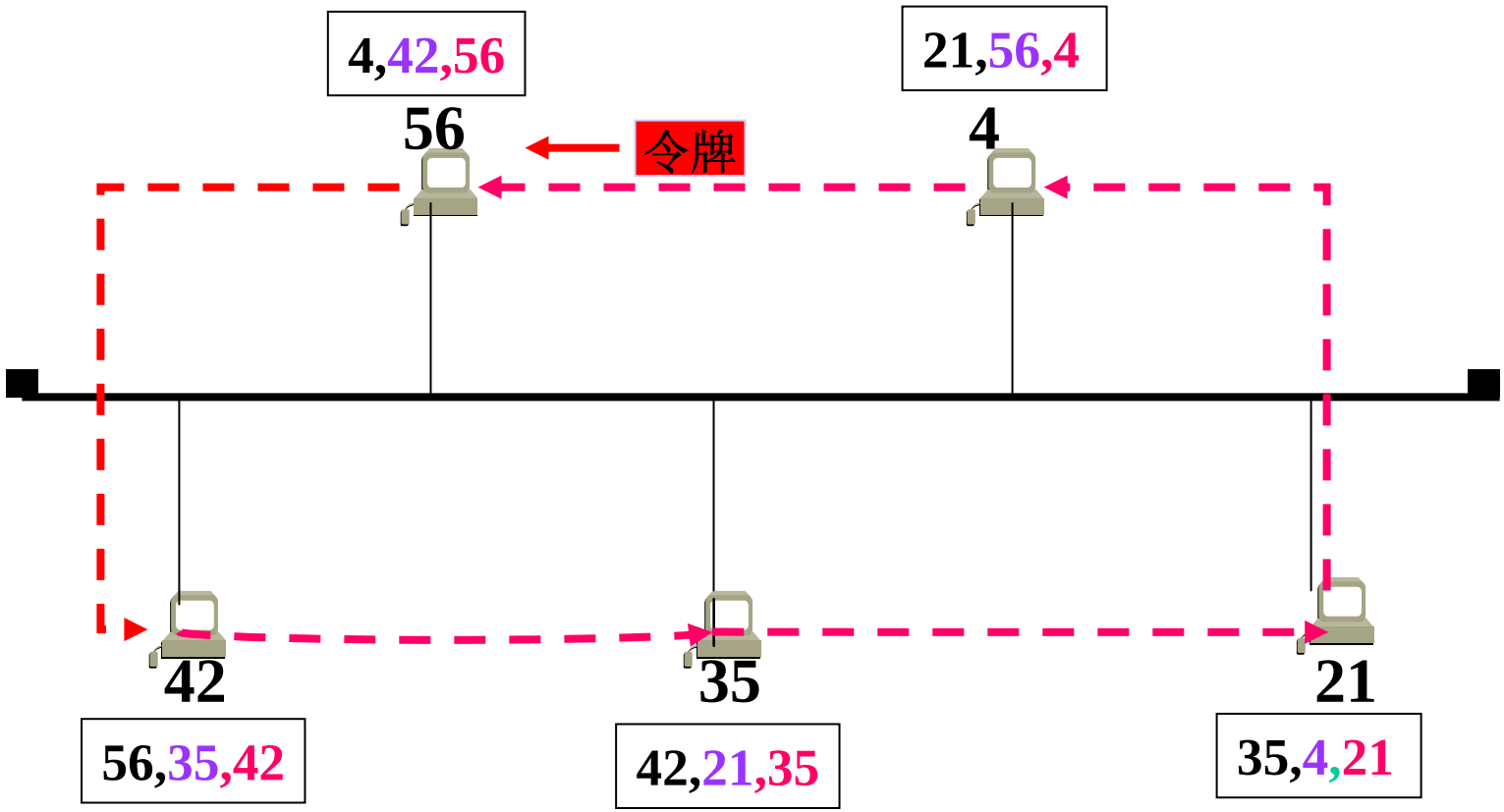
★ 为了保证逻辑闭合环路的形成，每个结点都动态地维护着一个连接表，该表记录着本结点在环路中的前继、后继和本结点的地址，每个结点根据后继地址确定下一占有令牌的结点。

逻辑环路形成示意图：

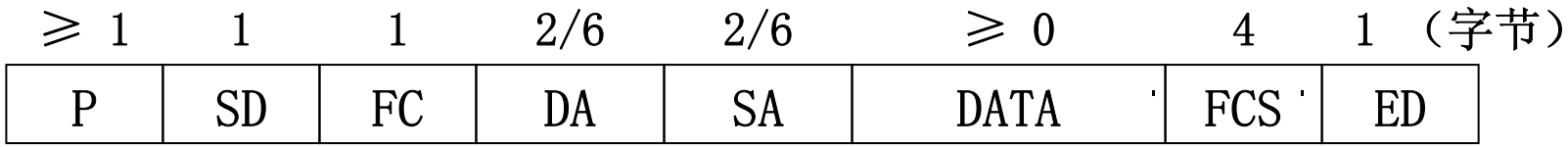
连接表：前继，后继，本地地址；

逻辑环路以地址递减的次序构成；

接到令牌的结点及时填充/修改连接表中的前继地址。



（2） 帧的一般格式



★ 前导码（P），用于收发同步；

★ 帧开始标志（SD），曼彻斯特编码非数据位，LHOLHOOO；

★ 宿/源地址（DA/SA）；

★ 帧控制字段（FC），帧的类型，包括令牌等；

★ 数据字段（DATA），取值依赖于帧控制字段（FC）；

★ 帧校验序列（FCS），对SD和ED之间的所有字段进行CRC；

★ 帧结束标志（ED），曼彻斯特编码非数据位，LH1LH1IE；

其中 I:1 ---- 紧随其后的为一个新帧，

0 ---- 后续无帧；

E:1 ---- 帧出错，该位由转发帧的转发器设置。

帧格式补充说明

★ 令牌总线网使用曼彻斯特编码；SD/ED使用了非数据位；

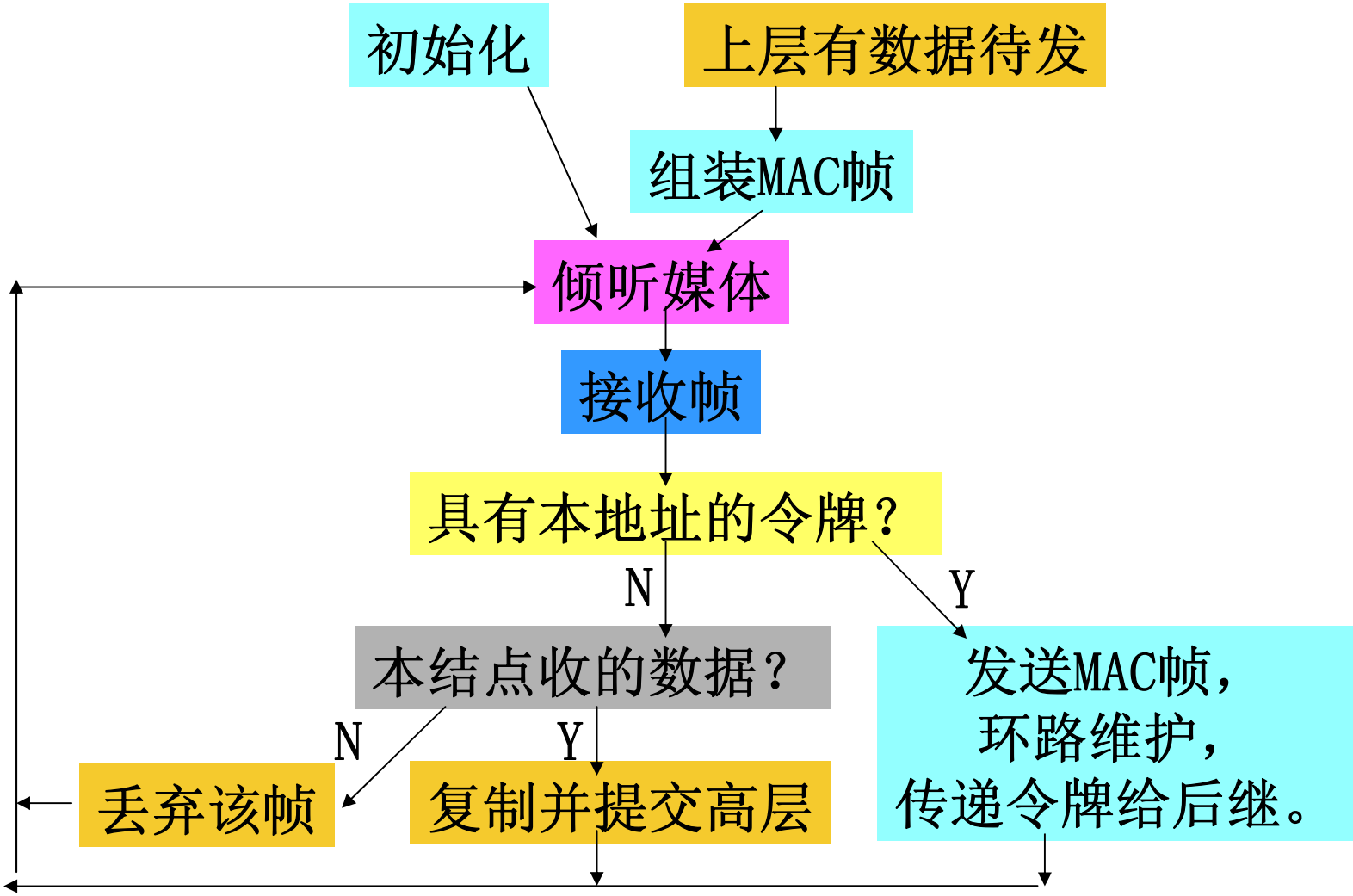
SD：L H 0 L H 0 0 0　　ED：L H 1 L H 1 I E

★ ED标识帧结束的同时，也指出了FCS的位置；

★ 帧控制字段（FC）取值—帧的类型：

取值	名称	说 明
00 H	要求令牌	Claim
01 H	请求后继1	用于新结点加入环路
02 H	请求后继2	用于新结点加入环路，确定后继
03 H	探询后继	当后继退出环路时，确定后继的后继；
04 H	解决冲突	当多个结点响应请求后继1时，予以确定后继
08 H	令牌	用作令牌
0C H	置后继	寻找新的后继

（3）基本工作过程


初始化
上层有数据待发
组装MAC帧
倾听媒体
接收帧
具有本地址的令牌？
N
Y
本结点收的数据？
发送MAC帧，
环路维护，
传递令牌给后继。
N
Y
丢弃该帧
复制并提交高层

（4）令牌维护

问题：令牌的丢失，出现多个令牌，需要进行令牌维护！

★ 令牌传递

拥有令牌的结点，执行环路维护工作，传递令牌给后继结点；

监听媒体是否有合法帧传递（后继结点获得令牌，并工作）；

有合法帧传输，OK；

否则超时（未监听到合法帧传输），执行一次令牌重传；

有合法帧传输，OK；

如仍然未监听到合法帧传输（原后继结点已撤出环路）；

开始寻找后继和环路重构过程。

发送“探询后继”帧，(含原后继结点的地址)，

原后继结点的后继结点用“置后继帧”予以响应；

双方修改连接表，传递令牌，恢复正常工作。

★多个令牌的处理

原则：获得令牌的结点处理环路中同时具有多个令牌的问题。

判断多令牌的方法：获得令牌的结点，如果仍然感知媒体上有信号在传输，表示有其它结点也掌握着令牌（多个令牌）。

解决办法：简单地丢弃令牌，回到原接收状态（目的在于减少环路中令牌的个数）。

可能产生的后果：令牌丢失（转令牌丢失处理）。

★ 令牌丢失的处理

结点设“环不工作计时器”。

— 在规定的时间内，未能监听到媒体上有信号传输，环不工作计时器超时，认为令牌丢失，或者环路处于初始工作状态；

— 所有感知环不工作的结点，采用竞争总线的方法争夺生成令牌的权利：

A .各结点根据本结点地址信息和一定的规则，形成不同长度的“要求令牌帧”，发往媒体并监听媒体；

B .不同的地址形成不同长度的帧几乎“同时”发往媒体时，会产生冲突。

C. 结点在发送帧之后，监听媒体：

短帧的结点会“监听”到其它结点的帧正在传输；

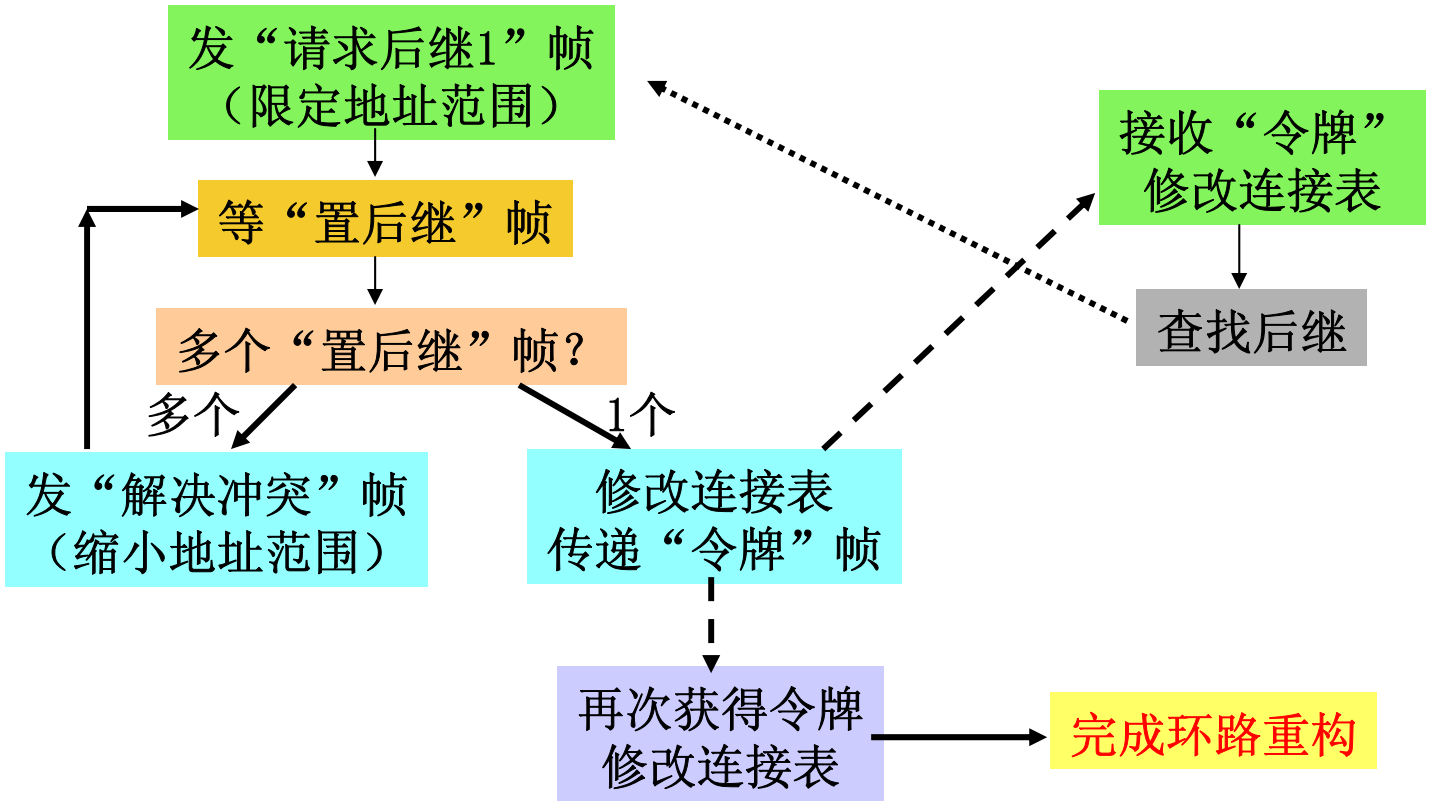
最长帧的结点感觉不到媒体上有其它信号传输，赢得生成令牌的权利，执行环路重构的过程。

（5） 环路维护

★ 环路重构

目的：各结点重新填写连接表，构造逻辑环。

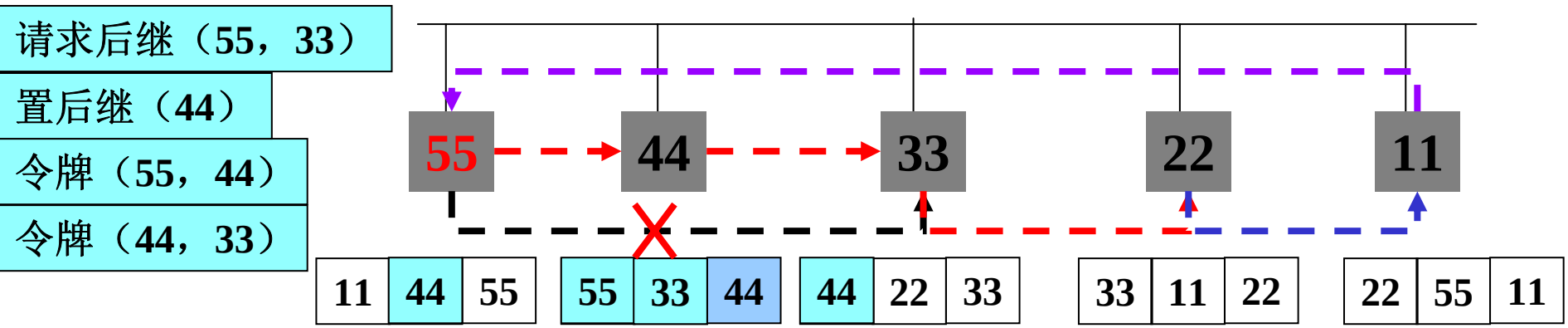
环路不工作后，获得生成令牌权利的结点进行环路维护。



★增加新结点

802.4 规定： 每个结点具有占用令牌的最大时间，

- 结点在信息传输完毕之后，如果时间允许，应执行必要的环路维护工作；
- 发“请求后继1帧”，询问本地址和后继之间的新结点加入；
- 若新结点符合后继的要求，用“置后继帧”响应；
- 结点修改“后继”，并传递令牌给新结点；
- 新结点设置连接表，传输数据，并传递令牌给原结点的后继；
- 后继结点获得令牌，修改前继地址。



★ 结点撤出环路

方法1：结点可以在任意时刻、不采取任何动作地撤出环路。

该结点的前继会自动开始寻找新后继的过程(令牌维护）；

方法2：指定时刻退出环路。

希望撤出环路的结点仅在收到令牌之后，

用“置后继帧”，将其后继结点地址告诉前继结点；

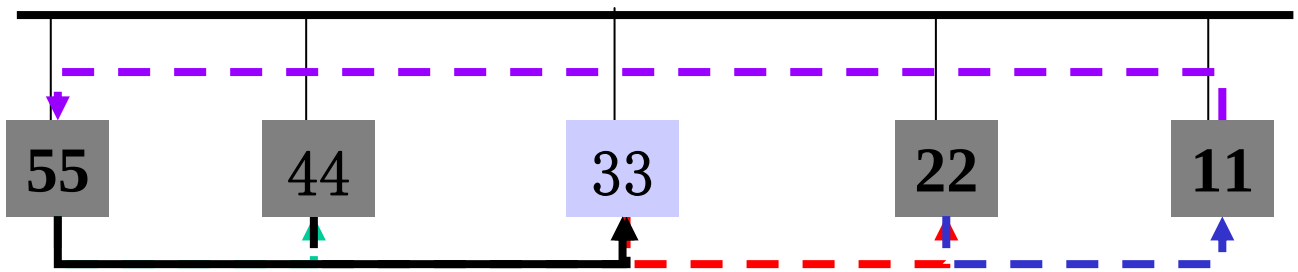
并传递令牌，撤出环路。

获得令牌的结点将及时更新其前继。

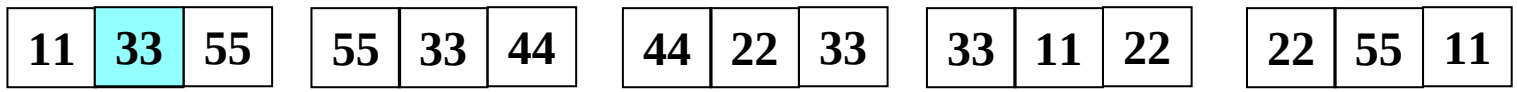
置后继（55，44，33）

55修改后继；

44传递令牌给33；



33仅在收到55的令牌后才修改前继



（6） 令牌总线网的特点

★ 令牌传递，使所有结点可对媒体进行公平和有序地访问；

★ 可传输多种类型的帧，无最小帧长的限制(数据字段data>=0)，控制方式复杂；

★ 整个网络具有最小的传输延时。无数据可传输的结点，仍然需要处理令牌的传递和进行环路维护工作；

★ 可以估算整个网络具有的最大发送延时。帧的长度、最大令牌占有时间和入网的结点个数之后，可以估算出每个结点的最大发送延时；

★ 令牌总线网适合具有一定实时性要求的环境。

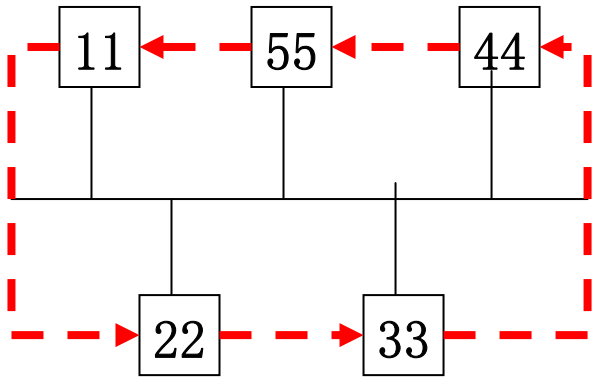
4.3.5 ARCnet

典型的令牌总线网络，77年Datapoint公司研制，工控应用；

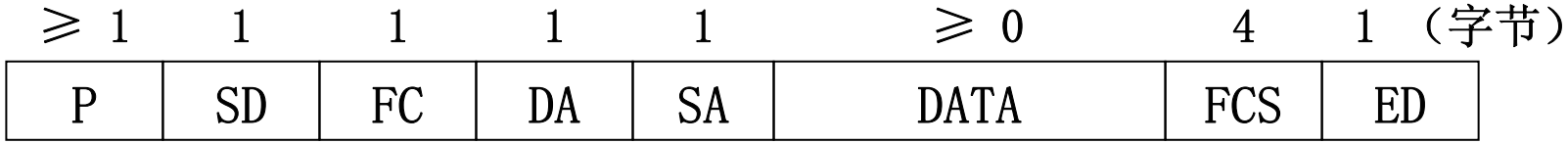
（1） 基本信息

★ ARCnet网络地址：每个结点有一个网络地址，

令牌以递增的结点地址序号，从一个结点传递到另一个结点，形成逻辑环路。环路中最多容纳255个结点。



（2） 帧结构



注意：DA/SA仅占一个字节，表示网络至多容纳255个结点；

其它字段含意类同Token-Bus标准；

★ ARCnet帧类型—FC字段：

数据帧（DATA），用于传送数据

令牌（TOKEN），用于传送令牌

确认（ACK），用于数据、令牌等帧的确认

否认（NAK），用于数据、令牌等帧的否认

探询（ENQ），探询接收结点的接收能力

“环路重构序列”，环路重构用。

（3） 新结点入环

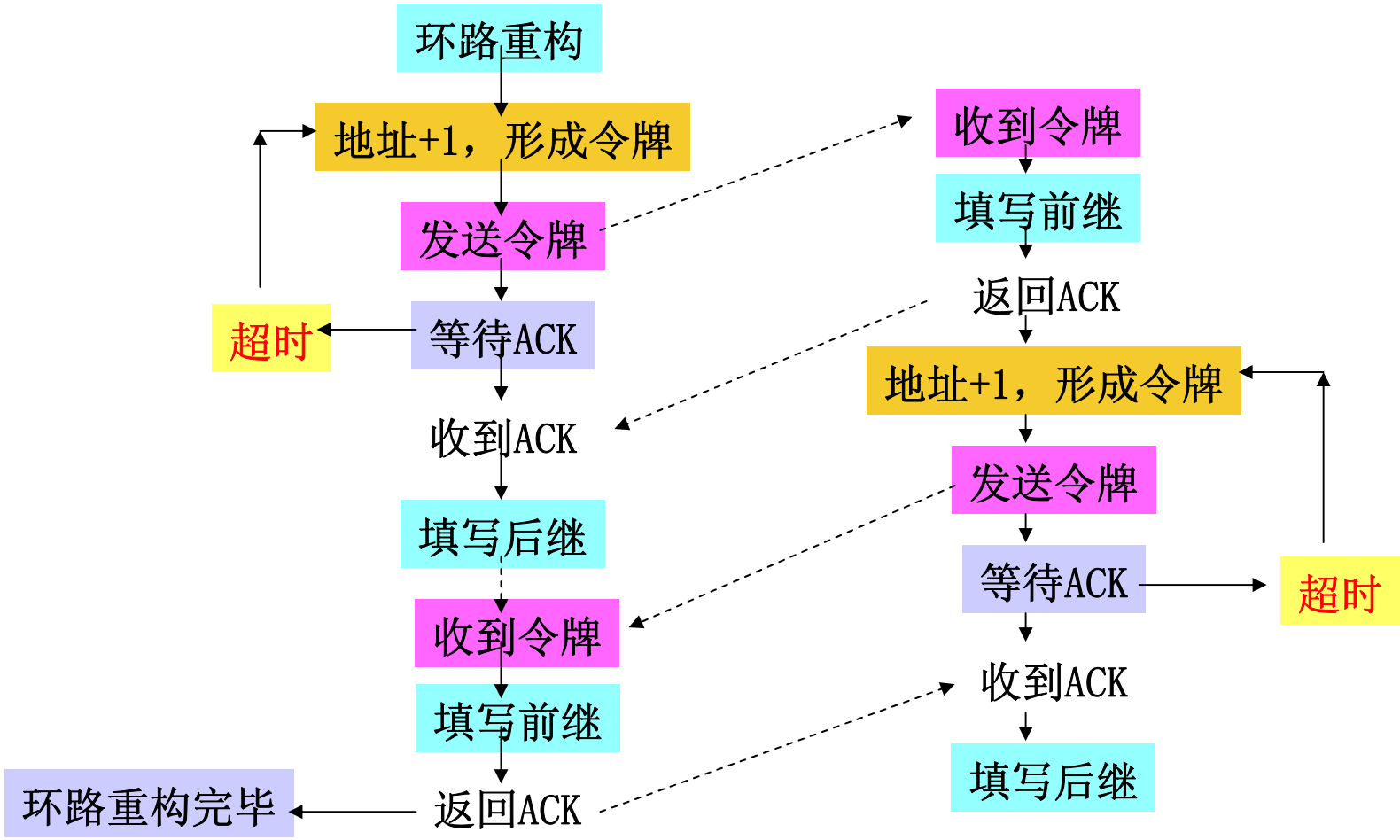
希望入环的结点，发送“环路重构序列”；

该序列帧较长，可以干扰掉正常的令牌，中止网上的一切活动，从而开始环路重构动作。

（4） 环路重构

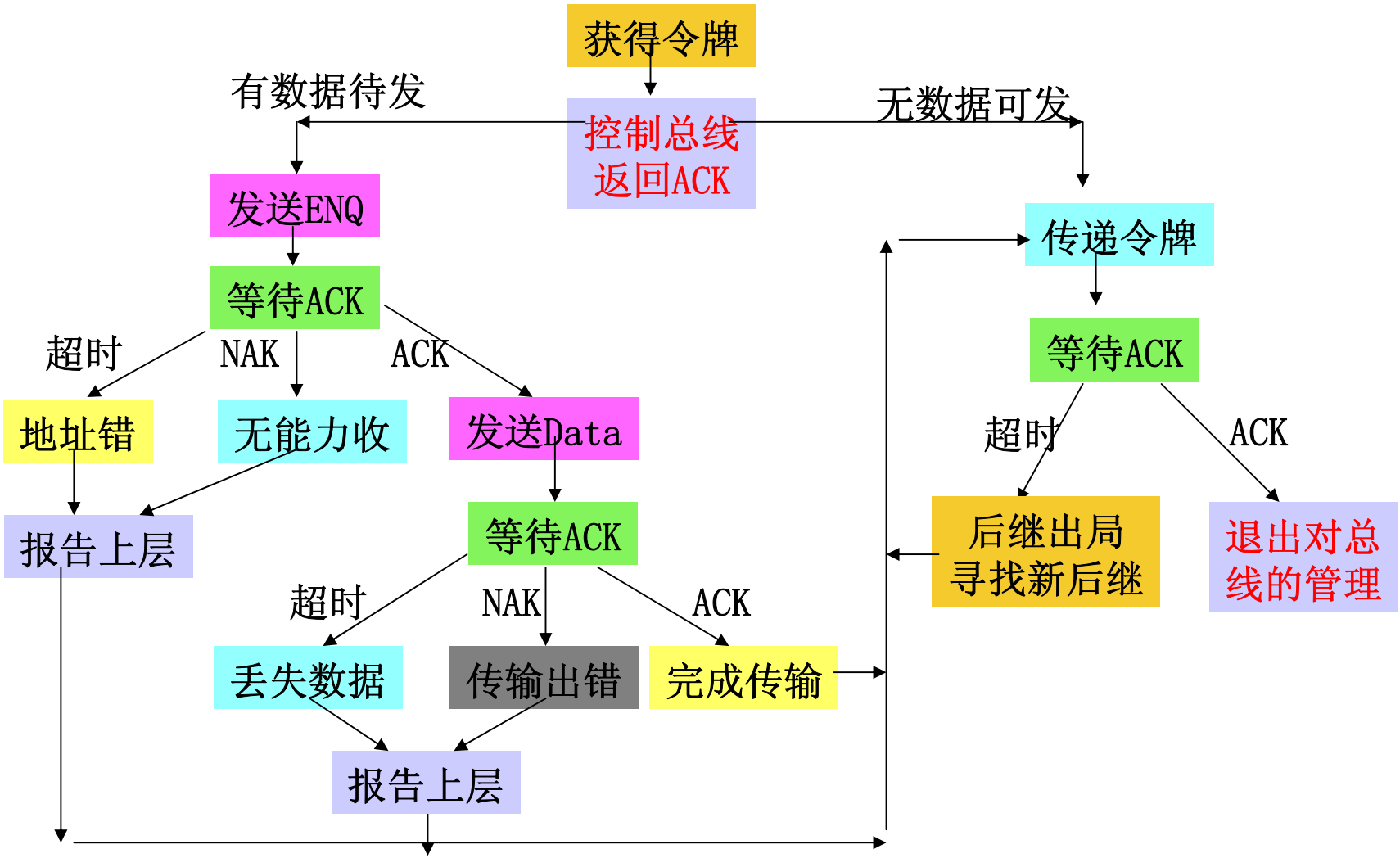
目的：形成逻辑环路，各结点寻找后继，填写结点维护的连接表。

发送“环路重构序列”的结点启动环路重构动作：



（5） ARCnet的工作过程

逻辑环上的各个结点监听环路，并获得帧；



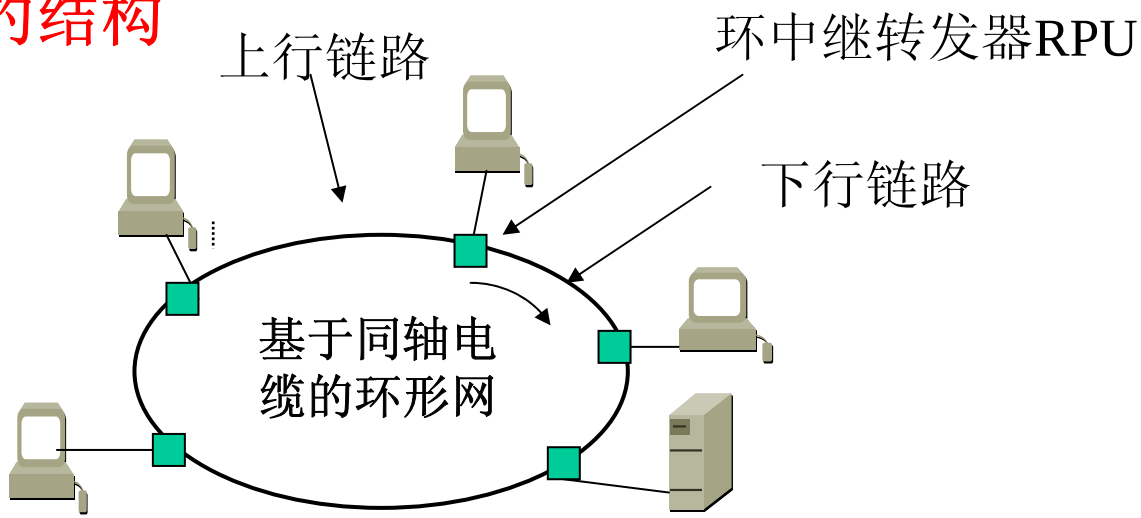
总线型局域网小结

特点：所有结点附接一根总线，通过总线收发帧；对应共享总线可能冲突，采用了各种总线访问方式。

竞争方式： **CSMA/CD—以太网；** 特点：结点抢占总线； 发送前侦听， 发送时检测， 冲突退避； 结论：重载时性能不好， 难以确定帧的发送时间。	按序方式： **TokenBus—ARCnet；** 特点：令牌传递总线访问权； 发送前等待令牌， 发送后传递令牌， 监控令牌唯一性； 结论：具有帧最小发送延迟， 可预测最大发送延迟。

4.4 环形局域网

4.4.1 环形网的结构



★ 结点通过RPU接入环路，每个RPU仅和2个相邻RPU直接连接；

★ RPU从其中的一个环段（称为上行链路）获取帧中的每个位信号，再生(整形和放大)并转发到另一环段(称为下行链路)。如果帧中宿地址与本结点地址一致，复制MAC帧，并送给附接本RPU的结点。

连接网段、信息复制、再生和转发

★ 可以满足“每个结点都可访问网络，发送/收取信息”的要求。

潜在问题

★ RPU故障，可导致网络瘫痪，如何提高环路的可靠性？

★ 如何监视和维护环路？

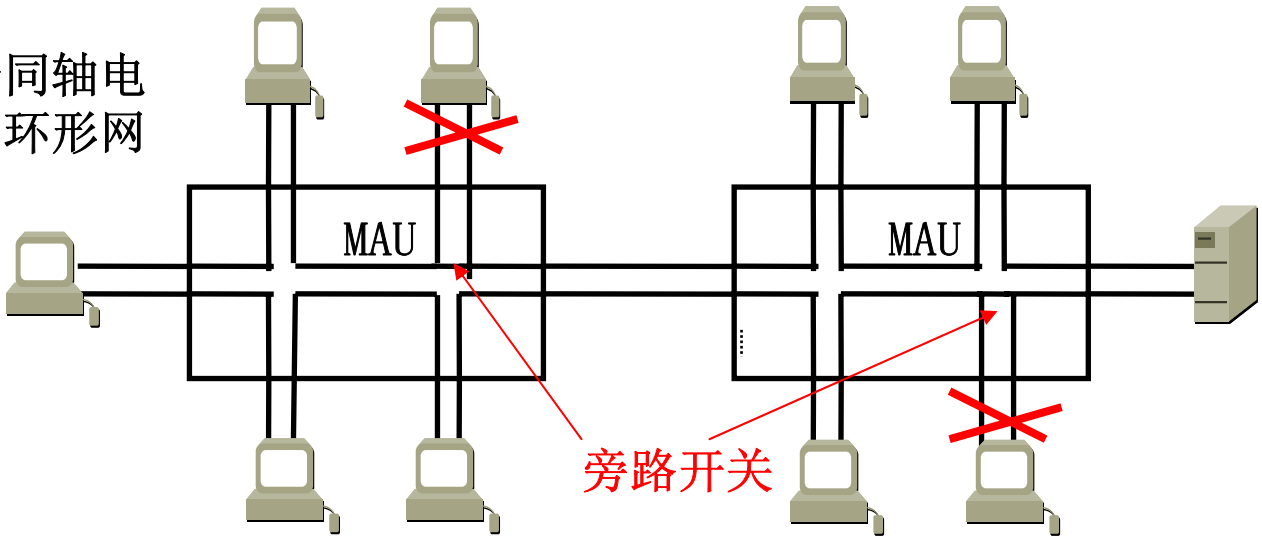
★ MAC帧无休止地在环路中再生和转发，如何进行帧回收工作？

★ 如何控制结点访问环路？

结构方面的改进：

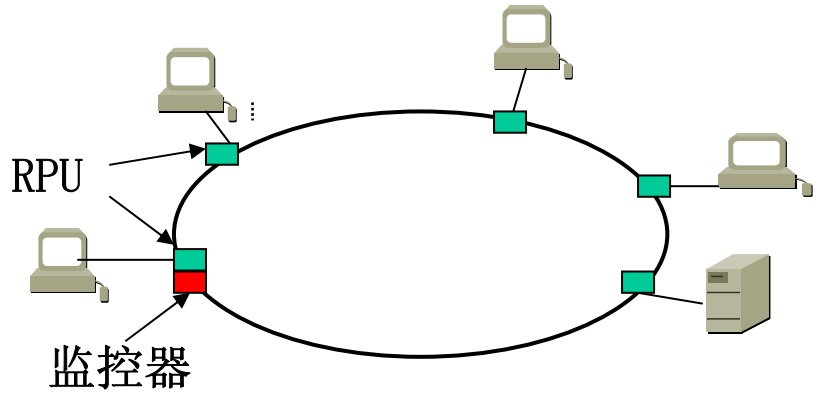
★ 多路访问器（MAU）和环监控器—环星网

基于同轴电缆的环形网



4.4.2 令牌环

（1） 令牌环网工作原理



目标：

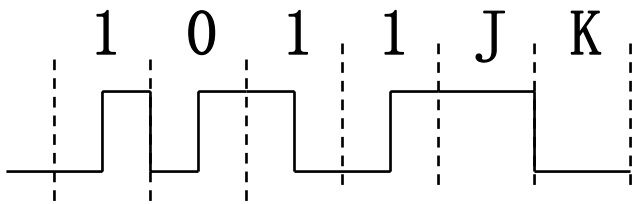
支持结点有序地访问环路；

标准：ISO 8802/5和IEEE 802.5。

★ 标准媒体：屏蔽双绞线，或者同轴电缆；

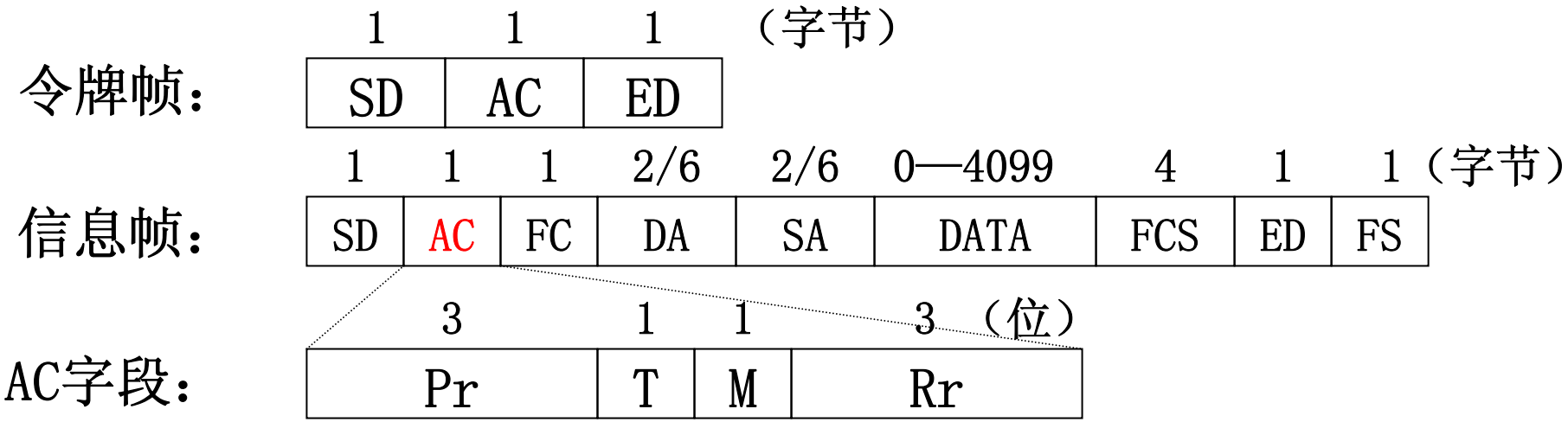
★ 传输速率：1Mbps和4Mbps；或者4Mbps、20Mbps和40Mbps；

★ 传输编码：差分曼彻斯特编码，基带传输；



★ 附加性能：优先级预定和处理机制。

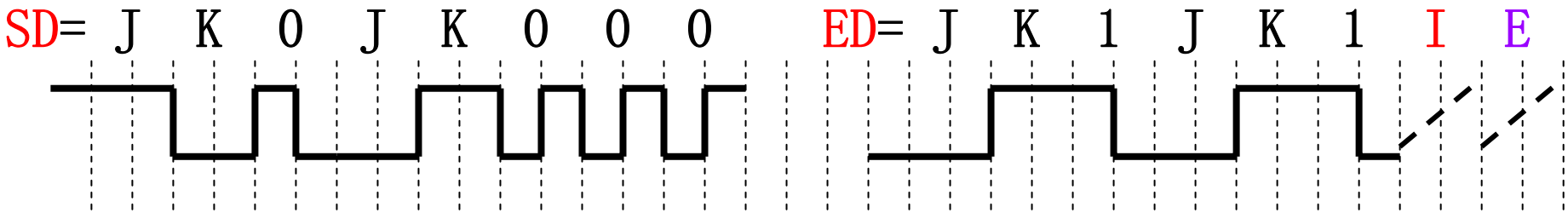
（2） 令牌环的MAC帧格式



帧字段说明：

★ 帧开始/结束标志（SD/ED）；

J/K：位间电平不发生/发生变化的非数据位；



I：多帧说明，类似令牌总线；

E（差错标志）：由RPU置位，RPU在转发每个帧的同时，也执行差错校验动作，并利用RPU具有的一位延迟来置位差错标志。

★ 访问控制字段（AC）：

Pr	T	M	Rr

Pr/Rr：本帧优先级和预定优先级；

T：令牌标识，T＝0（令牌帧），T＝1（其它帧）；

M：监视位，监控器（或者具有监控功能的RPU）填写，发送结点置0，监控器置1；

监控器重收M=1帧（发送结点故障），负责撤帧，并发令牌。

★ 帧控制字段（FC）：格式为“FFzzzzzz”，

FF：帧种类，FF=00，MAC控制帧；FF=10，管理帧；

FF=01，数据帧，数据（LLC帧）存DATA字段；

zzzzzz：MAC控制帧类型。

★ 帧状态标志（FS）：格式为“ACxxACxx”，帧收取状况，

A：地址确认位，发方复位，收方置位，帧宿地址正确；

C：信息复制位，发方复位，收方置位，帧已被正确复制；

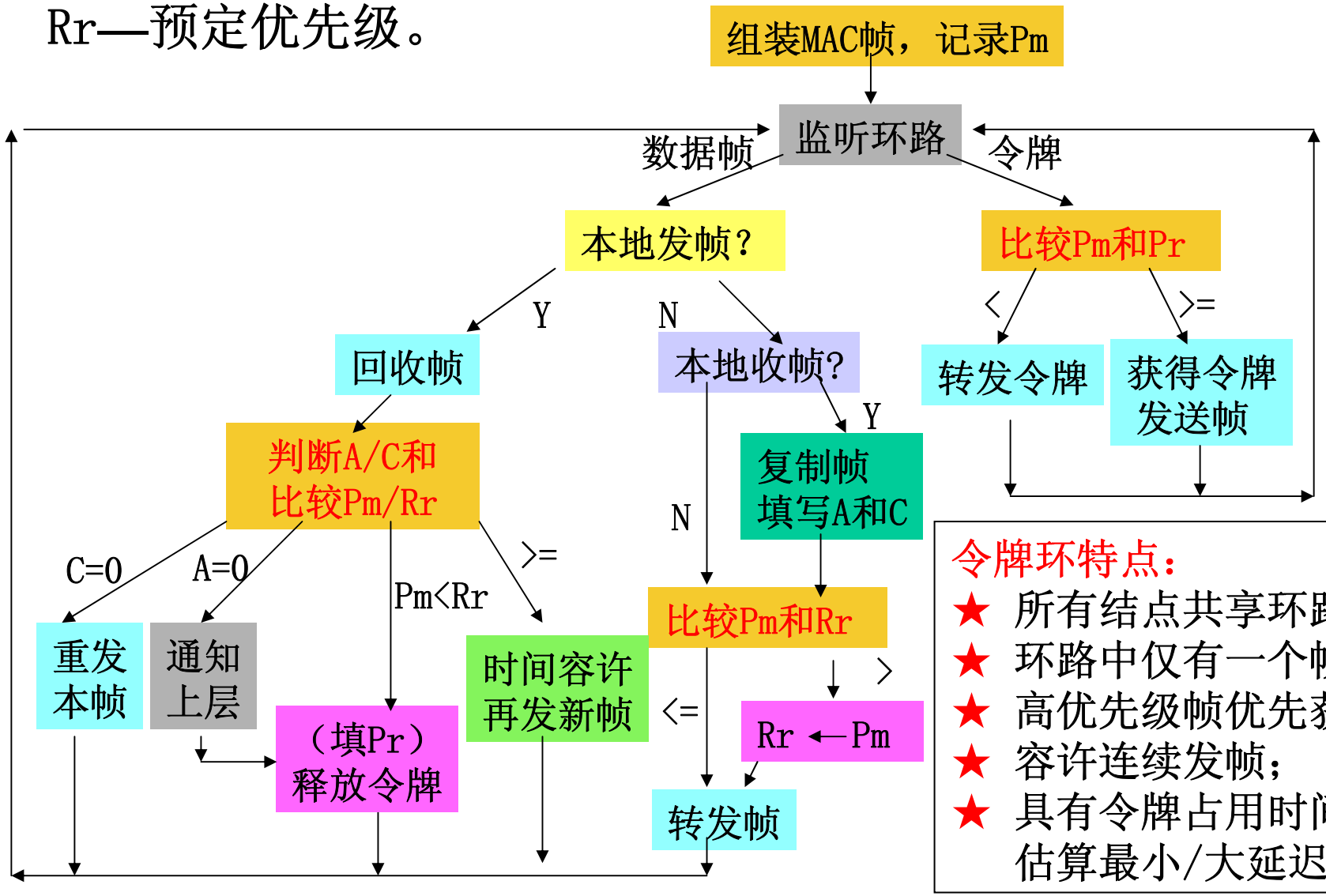
xx：保留未用。

（3） 令牌环网工作过程

AC字节：

Pr	T	M	Rr

具有优先级预约功能，Pm—拟发帧优先级，Pr—指定优先级，Rr—预定优先级。

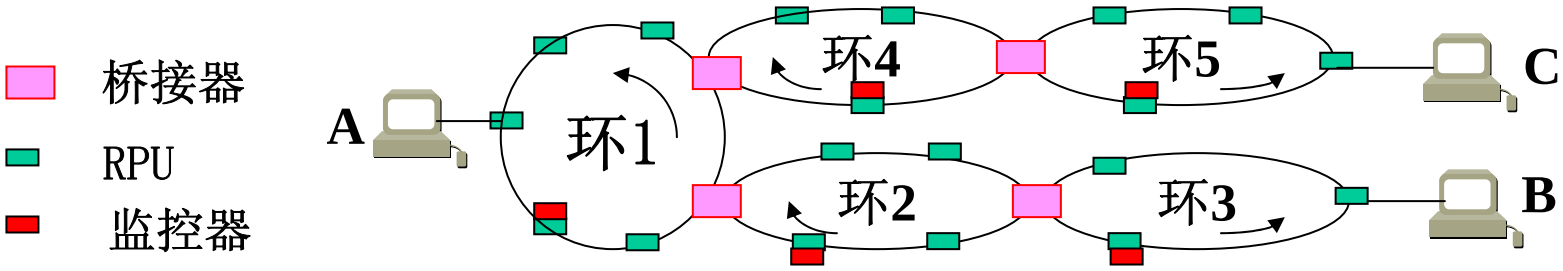


令牌环特点：

- ★ 所有结点共享环路；
- ★ 环路中仅有一个帧；
- ★ 高优先级帧优先获令牌；
- ★ 容许连续发帧；
- ★ 具有令牌占用时间，可估算最小/大延迟时间。

4.4.4 IBM令牌环（IEEE 802.5的一种实现）

（1） IBM令牌环网的结构



桥接器：为容纳更多结点和提高网络性能，划分和连接子网，并负责帧的跨网转发；

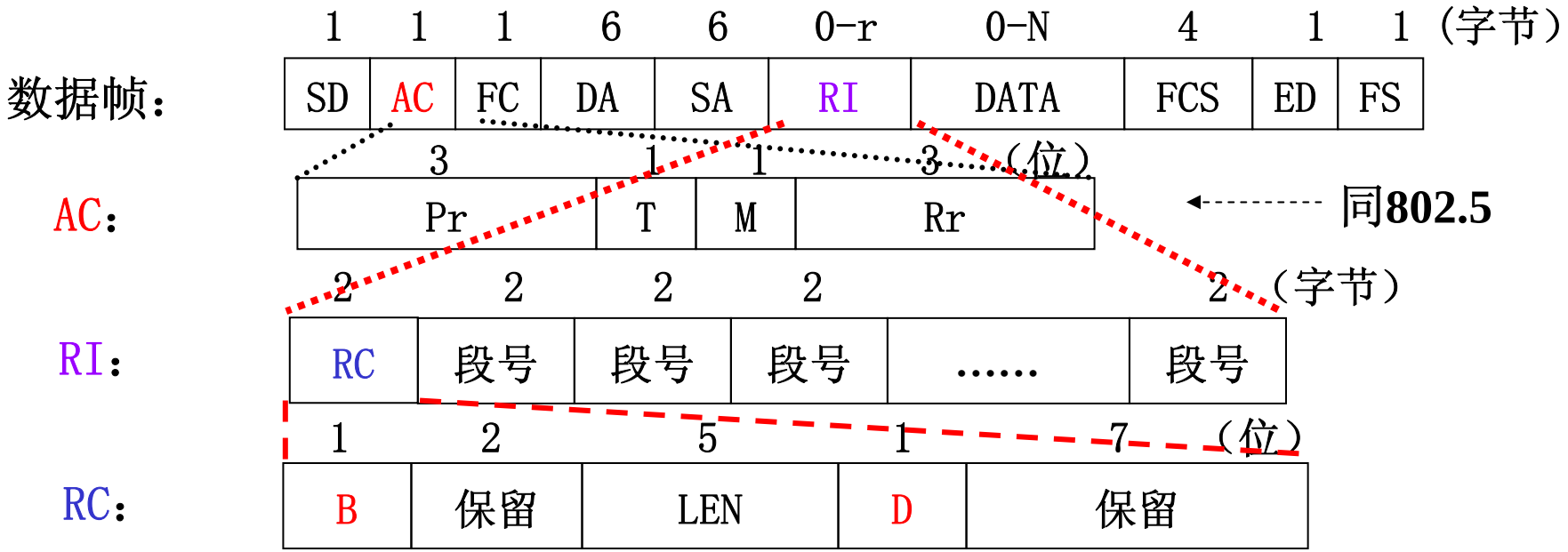
问题1：如果桥接器对每个帧都进行独立地跨网转发（广播），可能导致网络带宽资源的浪费。

解决的设想：控制“广播”，实行“源指定帧的路径”。

问题2：如何确定路径？

解决方案：增加Test帧，专用于源/宿之间的路径发现；测试结果返回源结点，同时暂存在结点中，以作备用。

（2） 帧的一般结构



段号：记录特定子网的特定桥接器；

广播位（B）：确定桥接器的处理动作。

B＝1： 要求桥接器广播（跨网转发）该帧，包括填RI段号；

方向位（D）：说明帧的去向。

D＝0：该帧为发送帧，信源送往信宿；

D＝1：该帧为应答帧（接收方的响应），信宿送往信源。

（3）指定路径的寻径方案

结点在发送数据帧前，如果无源/宿结点的路径，则发送TEST帧（D＝0：源→宿；B=1：广播），以确定源—宿之间的路径；

桥接器本环转发，并复制检查该Test帧：

RI中无本段号和帧记录，RI中增加段号，记录并等待令牌，转发至桥接器连接的其它环段，转发帧由本桥接器回收。

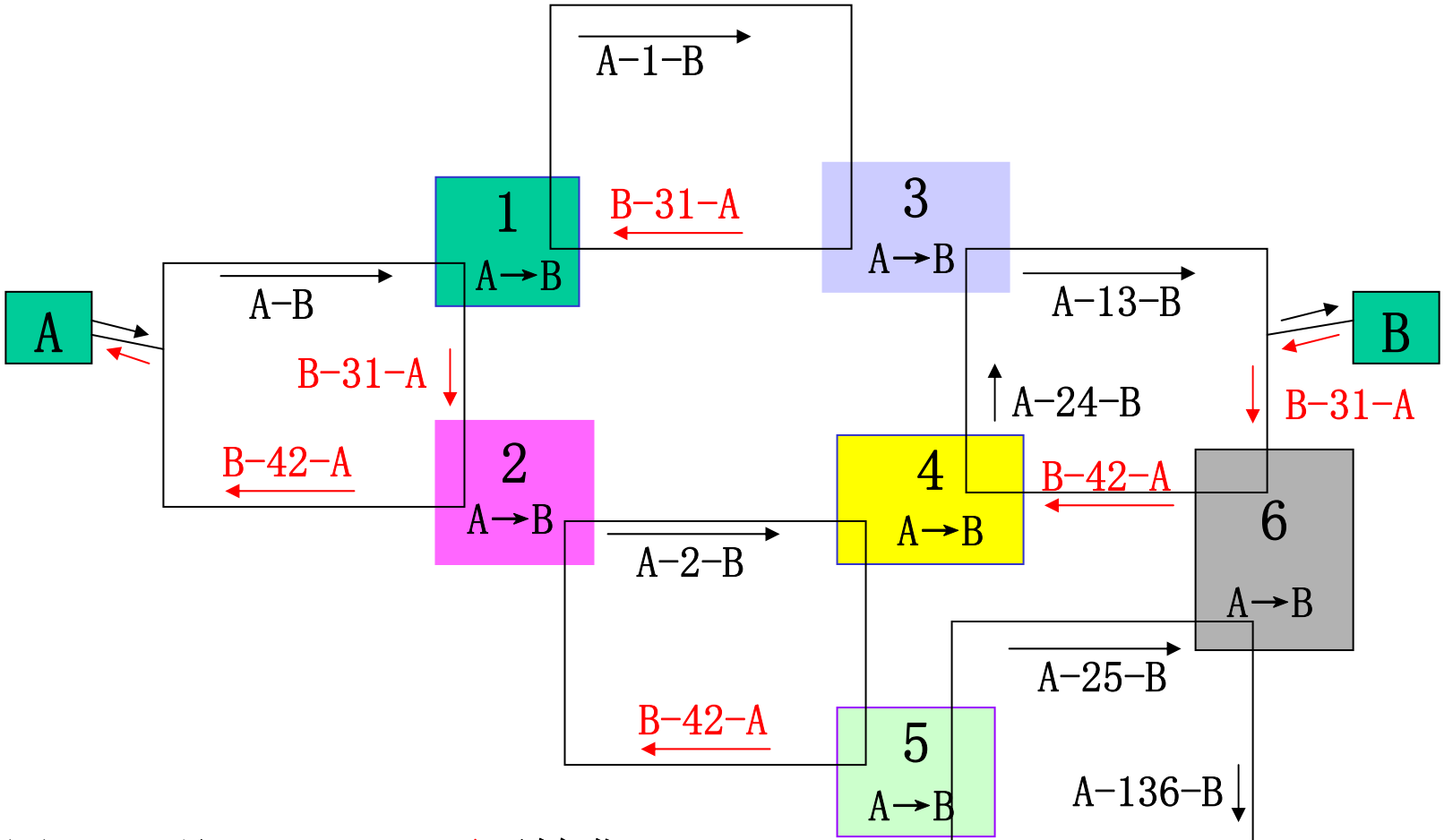
RI中有本段号或该帧记录（处理过该帧），丢弃复制品；

最终，信宿结点可能收到多个具有不同路径的相同Test帧，逐个处理，并根据帧中RI的路由信息返回响应帧（D＝1，B=0）；

当源发结点收到多个响应帧时，根据某种策略选择一个响应帧中的RI信息作为后继数据帧的发送路径，期待数据帧的传输可以获得较佳的路径。

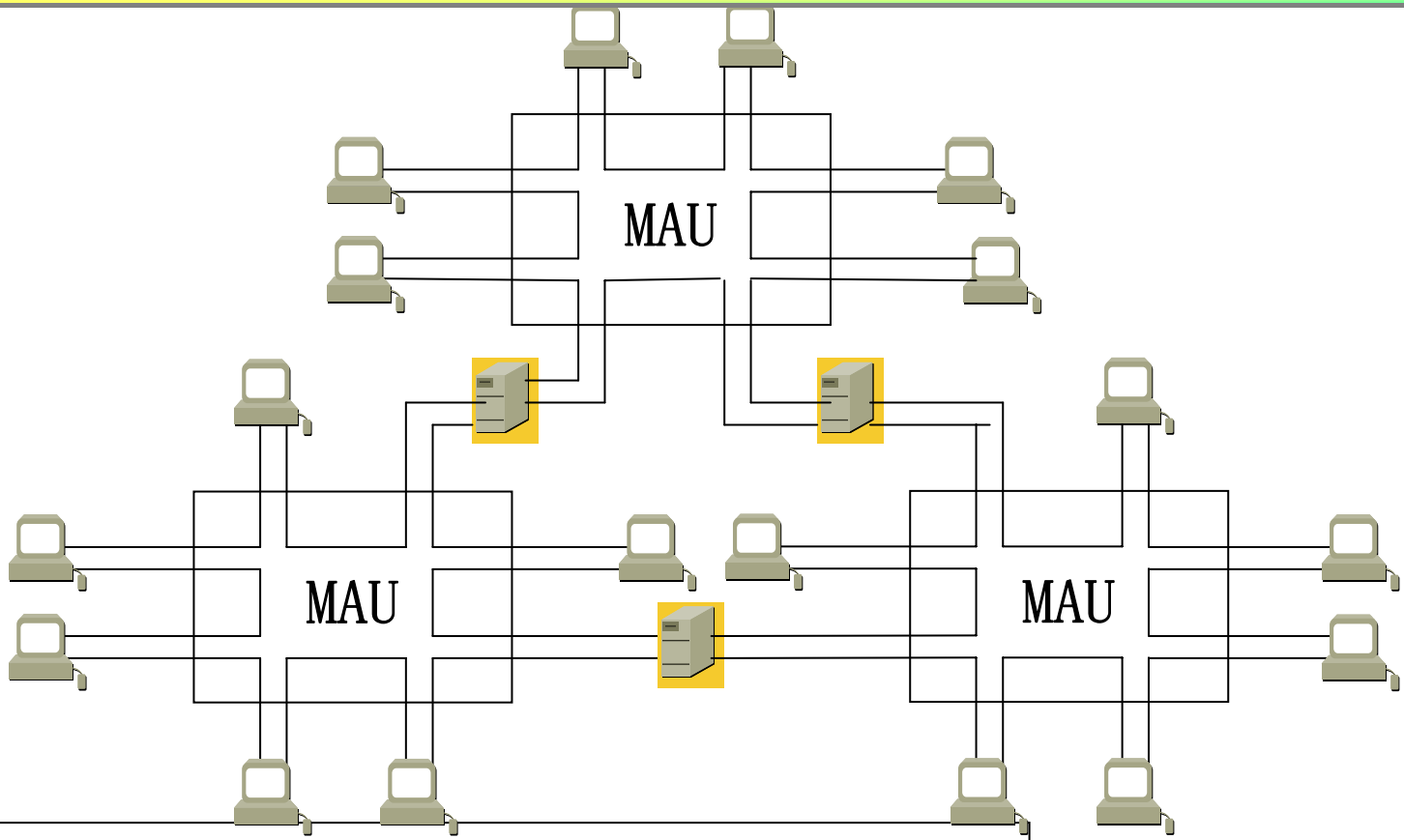
结果：数据帧中包含RI（源指定路由），具有匹配项的转发器转发该数据帧。

（3）指定路径的寻径方案—Test帧寻径示意：Test(A, B)



注：因 3 已处理 A-1-B, 不再转发 A-24-B;
因 6 已处理 A-13-B, 不再转发 A-24-B和A-25-B;
同理：4 不转发 A-13-B; ……。
B 循 3-1 路径返回响应帧;
同理，B 也循 4-2 路径返回响应帧;

（4） IBM令牌环的实际结构：



传输媒体： 屏蔽双绞线；
传输编码： 差分曼彻斯特编码；
传输速率： 4Mbps；
访问机理： 令牌绕环传递（子环内有效）；
优先级传输： 桥接器具有高的优先级；
传输方案： 源指定路径。

4.4.8 FDDI（Fiber Distributed Data Interface）

1982年，光纤高速LAN；86年，ANSI X3T9.5，93年 ISO 9314；
第一个支持多媒体通信的100Mbps环型网；
借鉴相对成熟的通信协议，兼顾光纤的脆弱性，802.5标准；
光纤成本：4b/5b+NRZI编码，125MHz线速达到100Mbps；
可靠性：双环结构，互为备份，自愈合；
4b/5b—5位符号（至少2个‘1’）表示4位数据；
NRZI—不归0编码，0/1—位间电平不变化/变化；

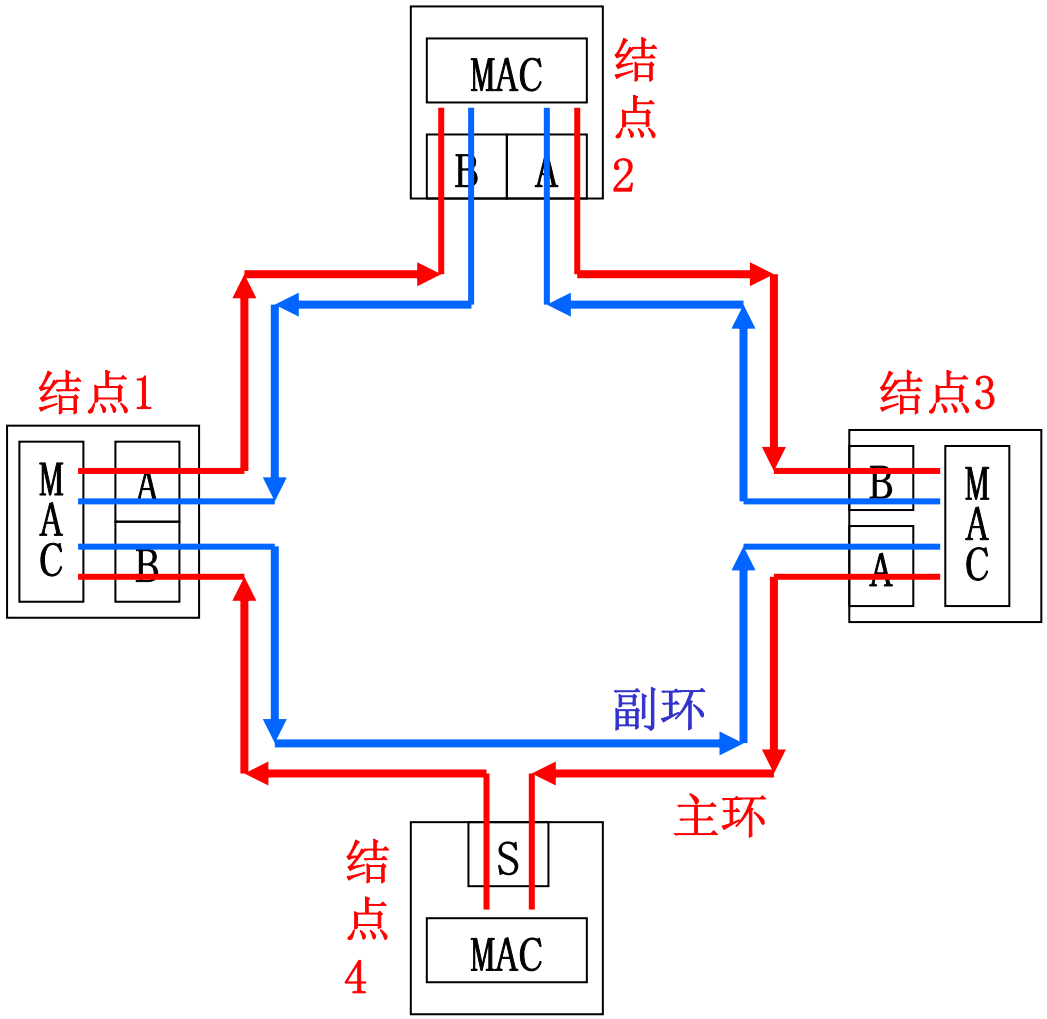
4b	0	1	2	3	4	5	6	7
5b	11110	01001	10100	10101	01010	01011	01110	01111
4b	8	9	A	B	C	D	E	F
5b	10010	10011	10110	10111	11010	11011	11100	11101
4b	S	R	Q	I	H	T	J	K
5b	11001	00111	00000	11111	00100	01101	11000	10001

控制字符：S—Set，R—Reset，Q—Quite，I—Idle，H—Halt，
T—Terminate，J—Start1，K—Start2；

(1) FDDI拓扑结构

FDDI拓扑：冗余设计，双环结构，逆向传输，互为备份。

FDDI部件：双端口部件—可接入双环，单端口部件—仅接入主环。



(2) FDDI帧结构

令牌

PA	SD	FC	ED

帧

PA	SD	FC	DA	SA	INFO	FCS	ED	FS

<=4500字节

（1）前导码（PA），>=16个线路空闲符号I，同步时钟；

（2）帧开始/结束标志，SD（JK）/ED（TT）；

（3）帧控制符（FC），1个字节，帧类型等，CLFFzzzz；其中：
C：同步/异步帧；L：局部/全局（16/48位）地址格式；
FF：帧种类：MAC帧、LLC帧和管理帧；ZZZZ：帧类型。

（4）信宿/信源地址（DA/SA），

（5）被传信息（INFO），用户信息、管理信息和控制信息等；

（6）帧校验序列（FCS），覆盖FC、DA、SA、INFO字段；

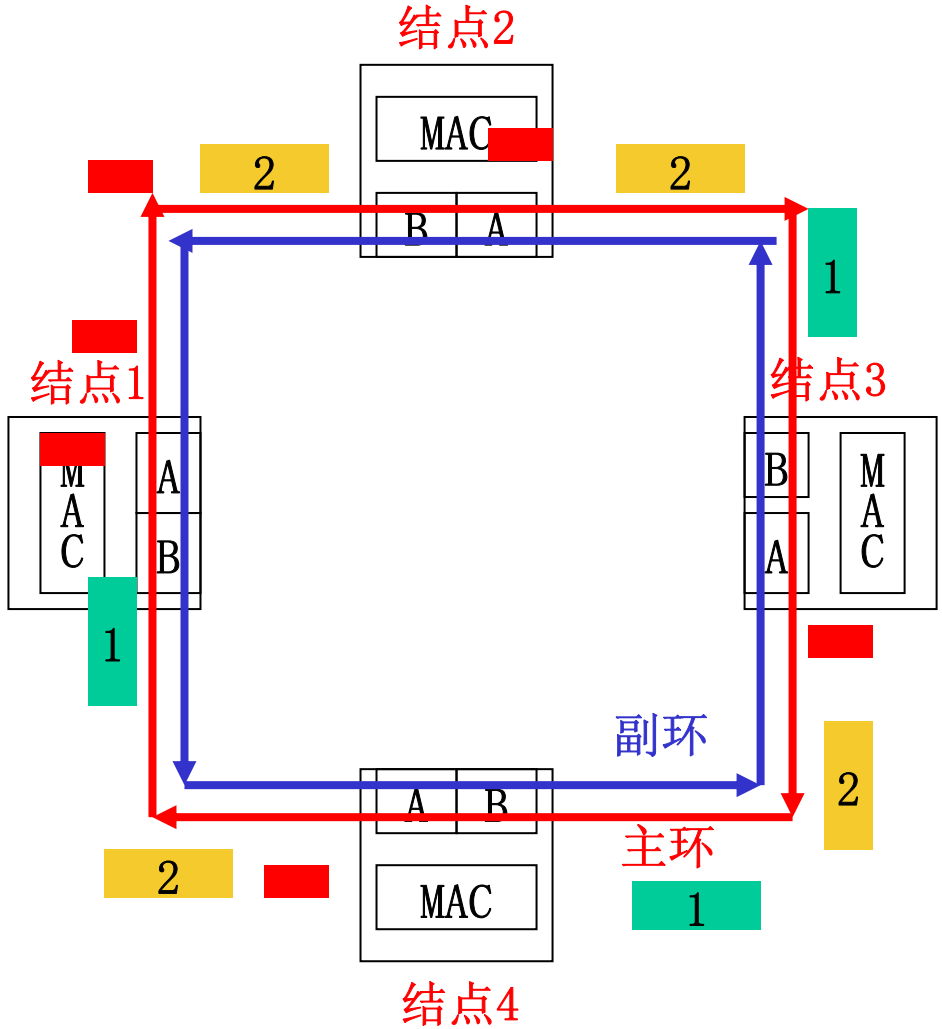
（7）帧状态标志（FS），发方复位（Reset）/收方置位（Set），体现收取状态，包括传输差错（E）、地址识别（A）、和帧复制（C）等。

(3) FDDI工作方式 — 令牌传递，多帧传输

获得令牌，发送数据帧，释放令牌，等待回收数据帧；

所有结点执行帧转发工作，接收结点复制数据帧；

结论：环路中可能同时存在多个结点发送的数据帧。



（4） FDDI和令牌环网的性能比较

	FDDI	令牌环（802.5）
传输媒体	光纤/双绞线	屏蔽双绞线
传输速率	100Mbps	4Mbps或者16Mbps
传输编码	4b/5b编码	差分曼彻斯特编码
控制方式	令牌传递	令牌传递
令牌个数	一个	一个
令牌产生	发送后产生令牌	回收后产生令牌
环路帧数	多个帧	一个帧
令牌协议	定时令牌	优先级预约

（5） 定时令牌

FDDI将传输的数据帧分为两种三类（是否具有实时性要求）：

同步帧（有实时要求）；

异步帧（无实时要求）：受限异步帧：支持会话型的应用；

非受限异步帧：其它应用。

为支持应用，**FDDI**可协商令牌环绕一周的时间（**TTRT**—目标令牌环绕时间）和令牌占有时间（如**2**个同步帧和**1**个异步帧）。

协商时考虑的因素：速率、结点个数、应用对实时性的要求等；

速率和结点数固定，结点发送帧或者令牌的时间可计算；

应用对实时性的要求可以量化；

应用的实时性要求不能满足时，结点发布修改**TTRT**值通知。

结点优先传输同步帧，灵活分配传输异步帧的时间。

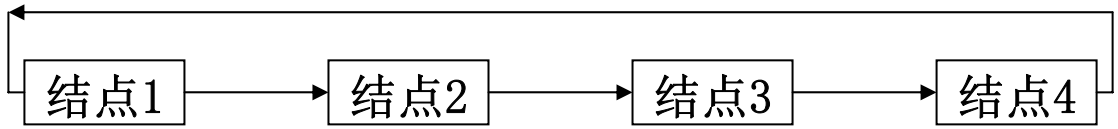
（5） 定时令牌—辅助设施：

结点设置计时器：令牌循环计时器TRT—记录传递令牌至再次获得令牌之间的时间值；令牌可占用时间（THT）—TTRT和TRT之间的差值，可以传输同步帧和异步帧(同步帧优先)。

FDDI的特点：帧发送后，立即传递令牌。

举例：4结点，TTRT=12，结点可传2个同步帧和1个异步帧。

（假设：忽略令牌传递时间）



结点1			结点2			结点3			结点4		
TRT	同步帧	异步帧	TRT	同步帧	异步帧	TRT	同步帧	异步帧	TRT	同步帧	异步帧
	2	1		2	1		2	0		2	0
7	2	3	9	2	1	10	2	0	10	2	0
7	2	2	8	2	2	10	2	0	10	1	1
8	1	0	5	0	0	3	1	6	8	0	3
8	—	—	—	—	—	—	—	—	—	—	—

（6） 环路维护——结点故障排除

结点在2*TTRT时间内未收到令牌，连续发送报警帧；

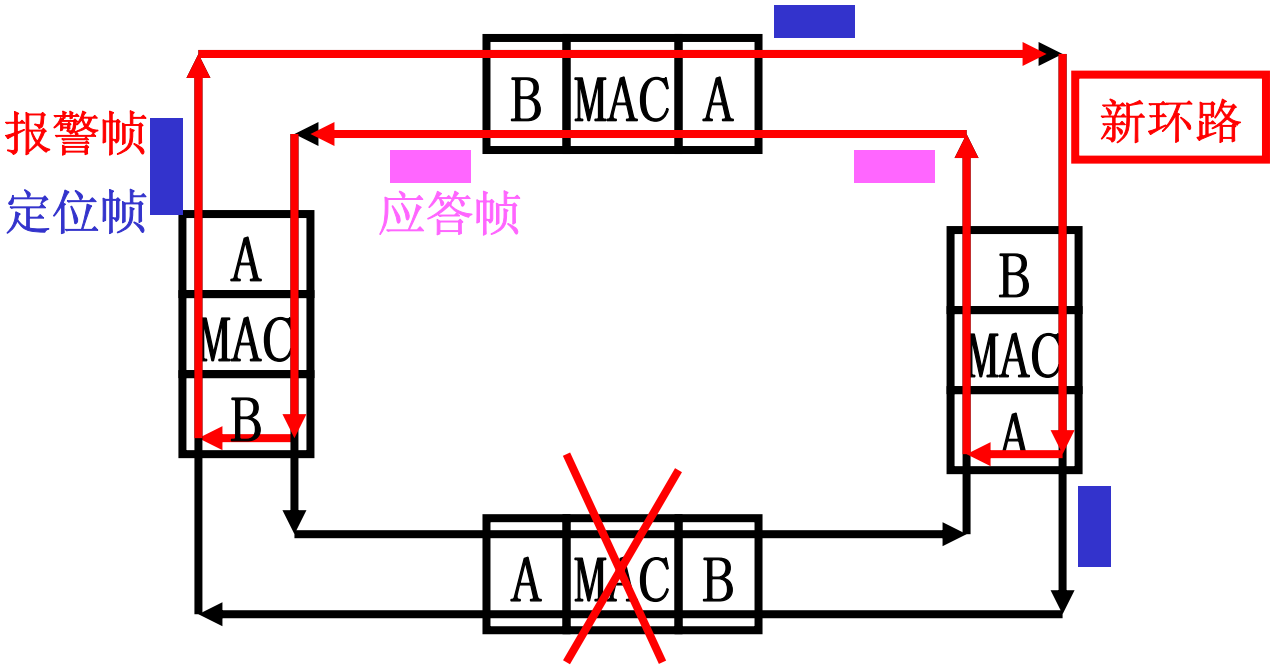
收到报警帧的结点仅执行转发报警帧的操作；

TTRT时间后，发送报警帧的结点执行上游端口旁路；

执行故障定位操作：发送定位帧，

收到定位帧的结点内环应答，主环转发定位帧；

未收到定位帧应答的结点旁路输出端口，形成环路。

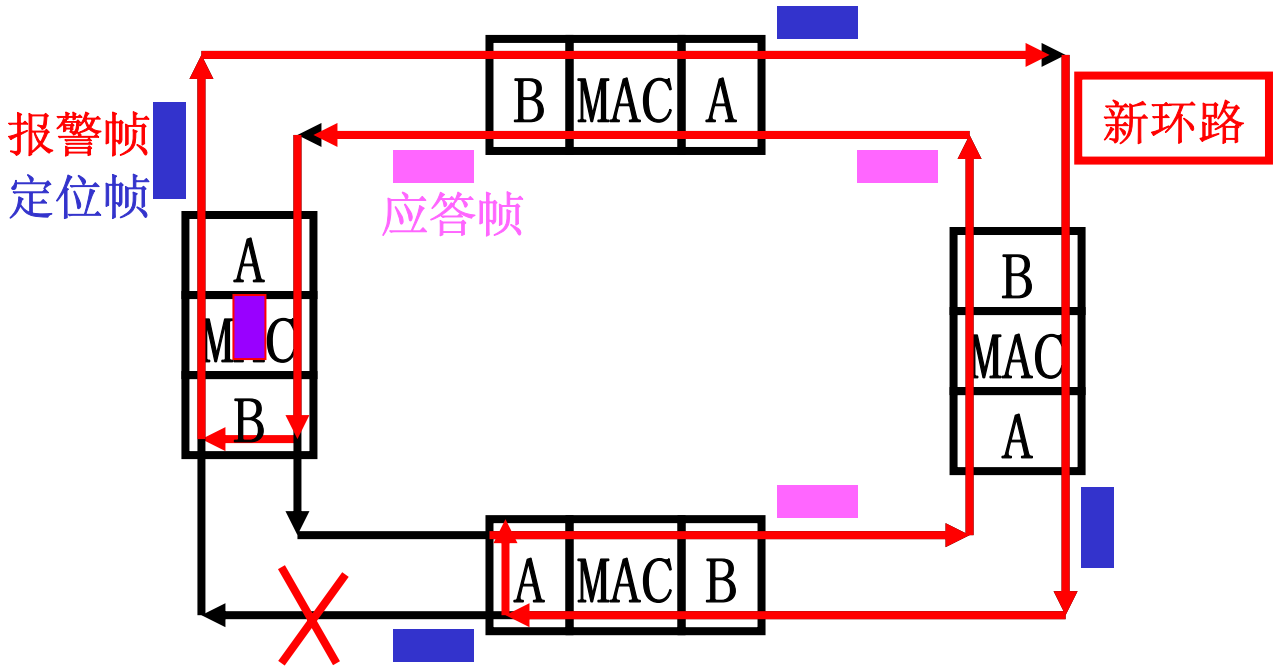


（6） 环路维护——线路故障排除示意

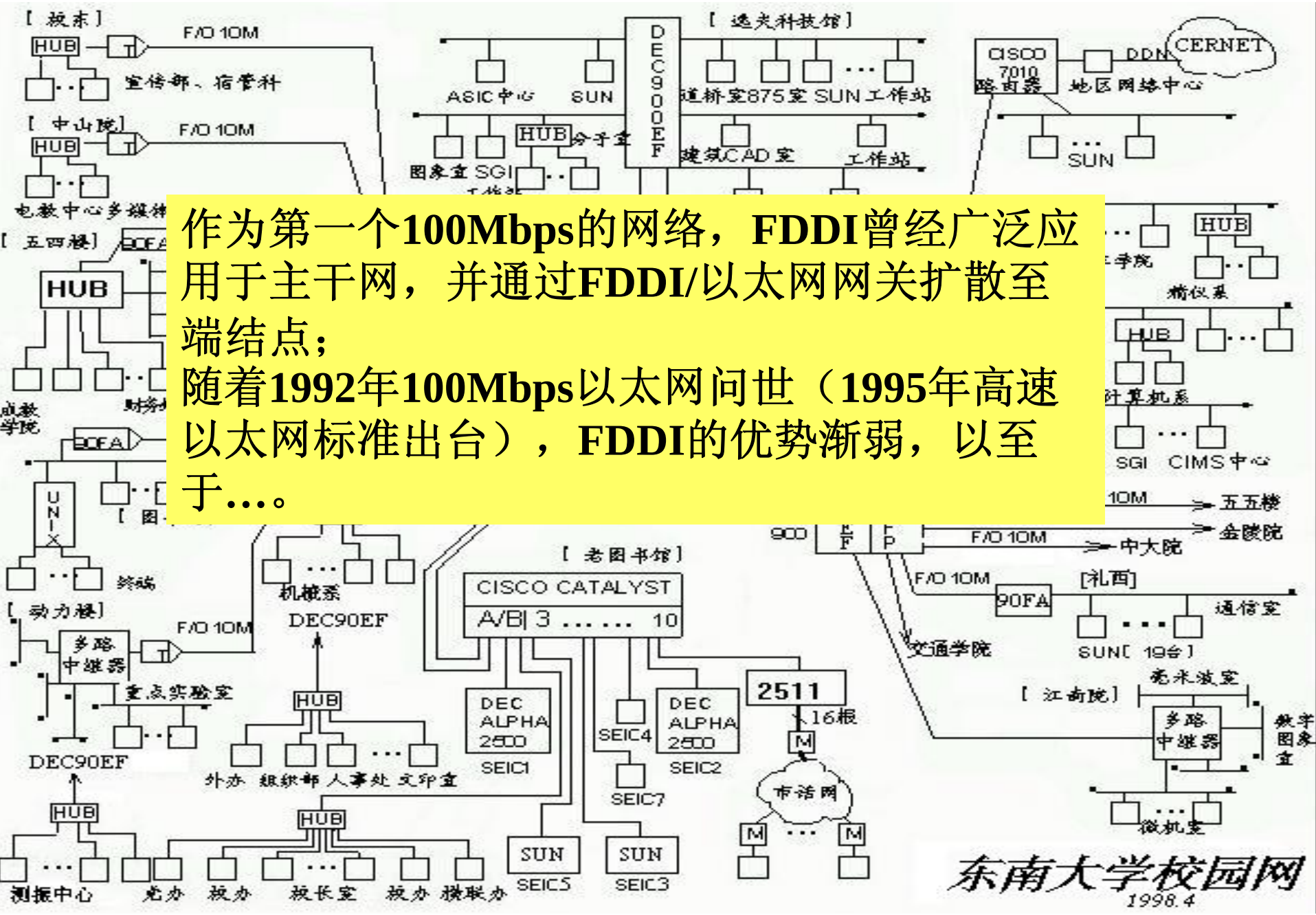
通过报警帧确定故障点的下游，旁路上游端口；

利用定位帧确定故障点的上游，旁路下游端口，形成新环路；

发送定位帧的结点获得令牌。



东南大学校园网拓扑图—1998年4月

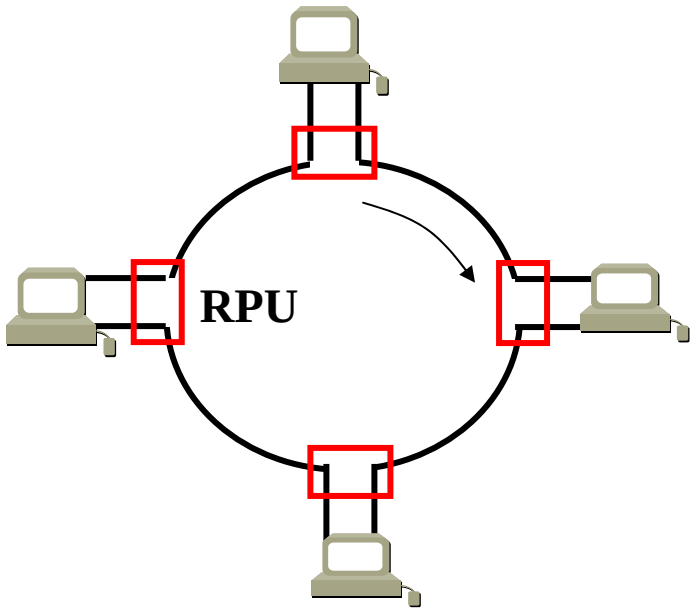


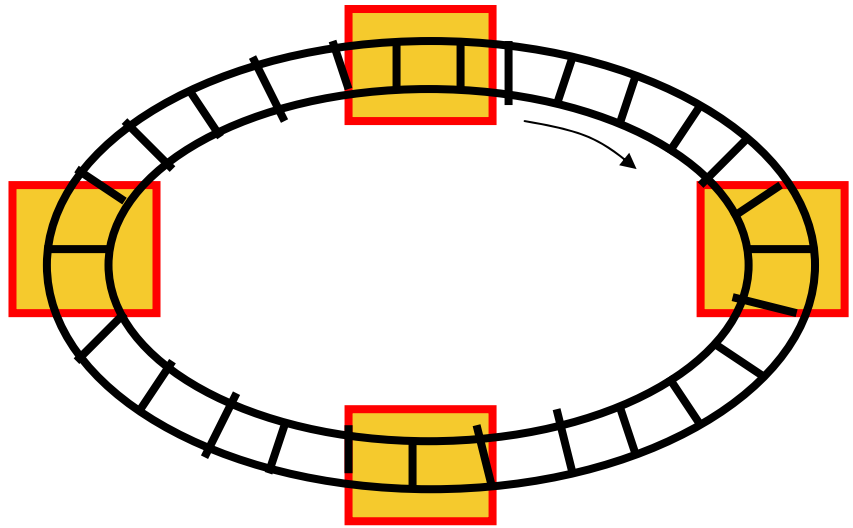
4.4.6 时间片环（也称时隙环，原802.7）

（1） 基本原理

环形网的基本特征：利用转发器（RPU）附接传输媒体的方法形成环路；

由于数据在媒体上的传输，以及经过转发器的处理具有延时的特征，整个环路可以被视为等效的循环移位寄存器，数据在环路中的传输过程可以视为数据在该移位寄存器中的移位操作过程。





位数估算：

循环移位寄存器的位数＝（电信号传播延迟（5us/km）×传输媒体长度＋转发器延时）×数据传输速率。

例如：100个结点组成的环路，结点间距为100米，

若：每个转发器的处理延时为2us（产品的性能特性），

网络传输速率设计为10Mbps（等价于10b/us），

则整个环路等价于2500位的循环移位寄存器，

100个转发器总延时：　　100×2us＝200us；

100段线路传输总延时：

100米×100段＝10000米（延时50us）；

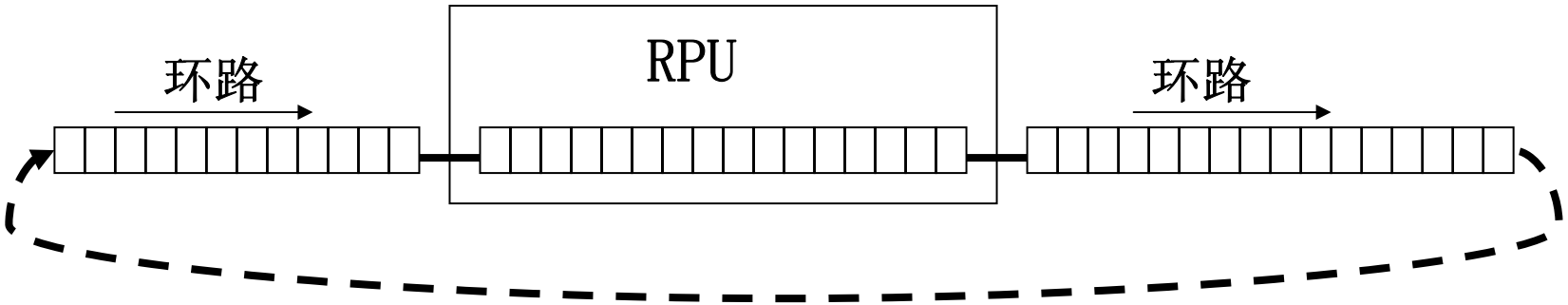
环路等效的循环移位寄存器：

（200＋50）us×10b/us＝2500b。

时间片环的操作思路：

问题1：等价的移位寄存器的位数具有任意性（取决于环路中转发器的个数，以及传输媒体的总长度），如何利用该移位寄存器传输具有特定体积的数据帧？

方案1：每个转发器配置若干位（等同帧长度）的移位寄存器插入环路。

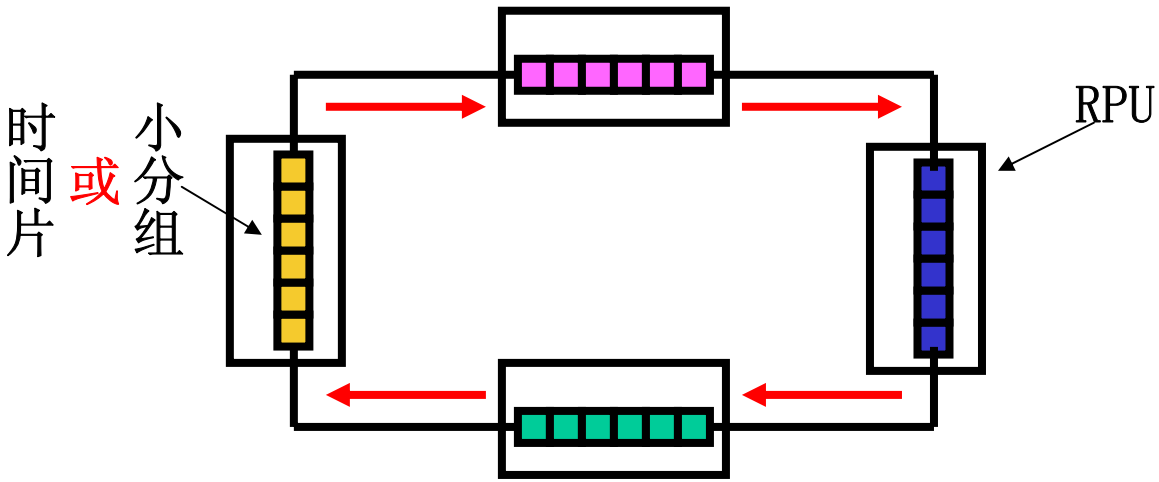


时间片环的操作思路：

问题2：① 配置移位寄存器的成本导致RPU的价格上升，② 帧的位数较多，若RPU个数也较多时，导致环路巨大，影响传输效率。

改进：将帧分解为有限体积的小分组（逻辑小分组），降低RPU插入寄存器的成本。

进一步改进：容许多个结点（RPU）同时插入寄存器，同时传输各自的逻辑小分组，提高环路的利用率。



结论：

① 环路等价于若干位数的移位寄存器，将该移位寄存器分段（时间片、或时隙槽），片/槽的体积等同于逻辑小分组的体积（传输时，携带小分组的数据）。

② 结点负责数据帧和逻辑小分组之间的拆帧和组帧工作；

③ 同一时刻环路上可能有多个结点发送数据（逻辑小分组）；

④ 类似令牌环等，为解决环路维护工作，环路上应设置监控器；

⑤ 为保证环路的正常工作，整个环路对应的循环移位寄存器的位数应是时间片所含位数的整数倍，补整工作由监控器完成。

⑥ 相关标准（IEEE802.7）定义了两种类型的结点（RPU）：

★ 基本型：支持长度为40位的逻辑小分组；

★ 增强型：支持长度为40、56、72和86位的逻辑小分组；

特定时刻，所有结点支持的位数应当一致。

（2） 数据帧格式：

帧格式：

2	2	2/6	2/6	1-65535	0/1	2 (字节)
P	L	DA	SA	DATA	PAD	FCS

帧开始标志（P）：同时指出地址类型（2或6字节—9C9CH或9C9DH）；

数据长度（L）： 帧中DATA字段的实际长度；

信宿/信源地址（DA/SA）：帧的收发结点地址；

填充字段（PAD）：保证DATA和PAD两字段之和为偶数字节；

逻辑小分组：

1	1	1	8	8	(2,4,6,8)×8	2	2	1 (位)
S	F/E	M	da	sa	data	T	R	P

引导比特（S）：‘1’= 逻辑小分组（或者时间片）开始；

槽满/空标识（F/E）：表示当前槽是否已存放数据，满为1，空为0；

监控位（M）：监控槽的运行状态，源发结点置0，监控器置1；

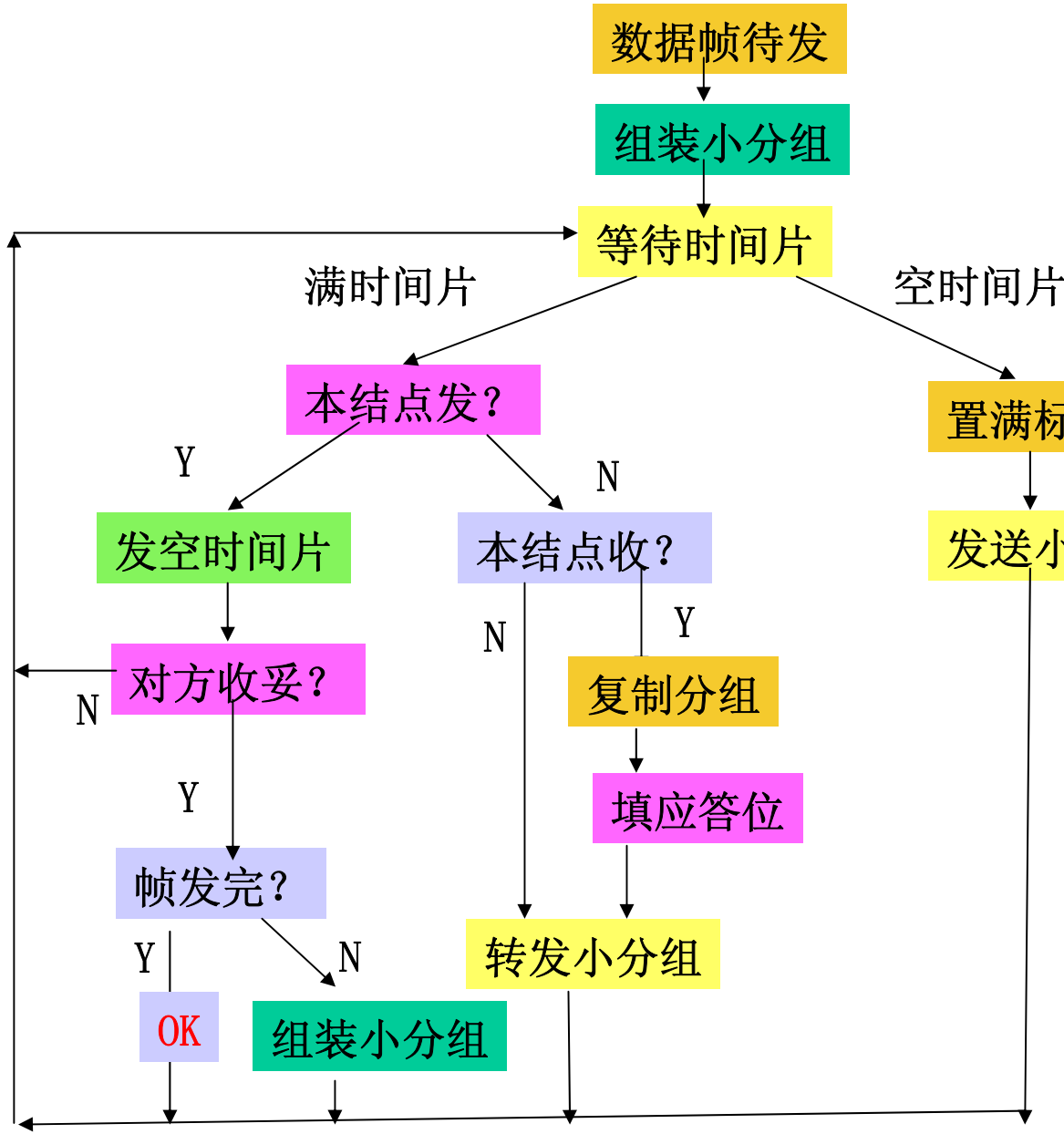
宿/源地址（da/sa）：收/发逻辑小分组的结点地址；

结点类型（T）：结点为基本型（0）或增强型（1）；

应答位（R）：宿结点填写，表示逻辑小分组的接收状态（01=正确收取）；

校验位（P）：偶校验。

（3） 工作过程



规定：

★ 容许多个结点同时传输多个分组；

★ 禁止结点使用同一个时间片连续传送多个分组；

（1） 指导思想

将时间片分为“空/满”两类时间片，分别具有不同的长度（占据不同的位数）；

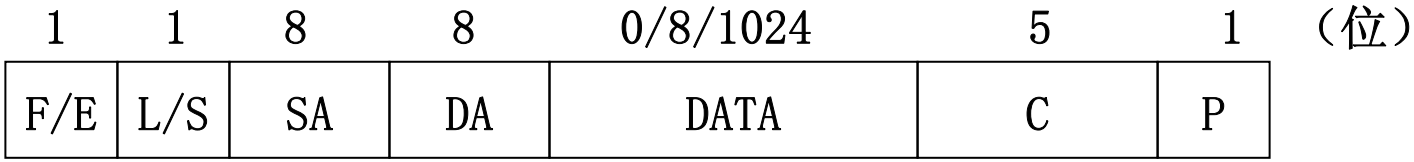
环路的基本延时划分为若干空时间片，空时间片绕环行驶，准备携带用户数据（形成满时间片）；

环路的基本延时也可视为循环移位寄存器，并且环路中设置监控器，除监控环路状态外，也插入一定数量的寄存器，以保证整个环路对应的移位寄存器位数为空时间片长度的整数倍，从而达到充分利用环路资源的目的；

希望发送数据的结点在获得空时间片时，以插入寄存器的方式将满时间片导入环路；

源发结点在回收满时间片后，释放空时间片。

（2） 时间片格式



★满空标识(F/E)：1为满时间片（含用户数据），0为空时间片；

★长短时间片标识（L/S），当F/E=1时，1为长，0为短时间片；

★信源/信宿地址（SA/DA）：发收该时间片的结点地址；

★数据字段（DATA）：用户数据，空时间片时长度取值为0；

短时间片时占8位，长时间片时占1024位。

★控制字段（$C=C_1C_2C_3C_4C_5$）表示信宿结点对该分组的处理结果。

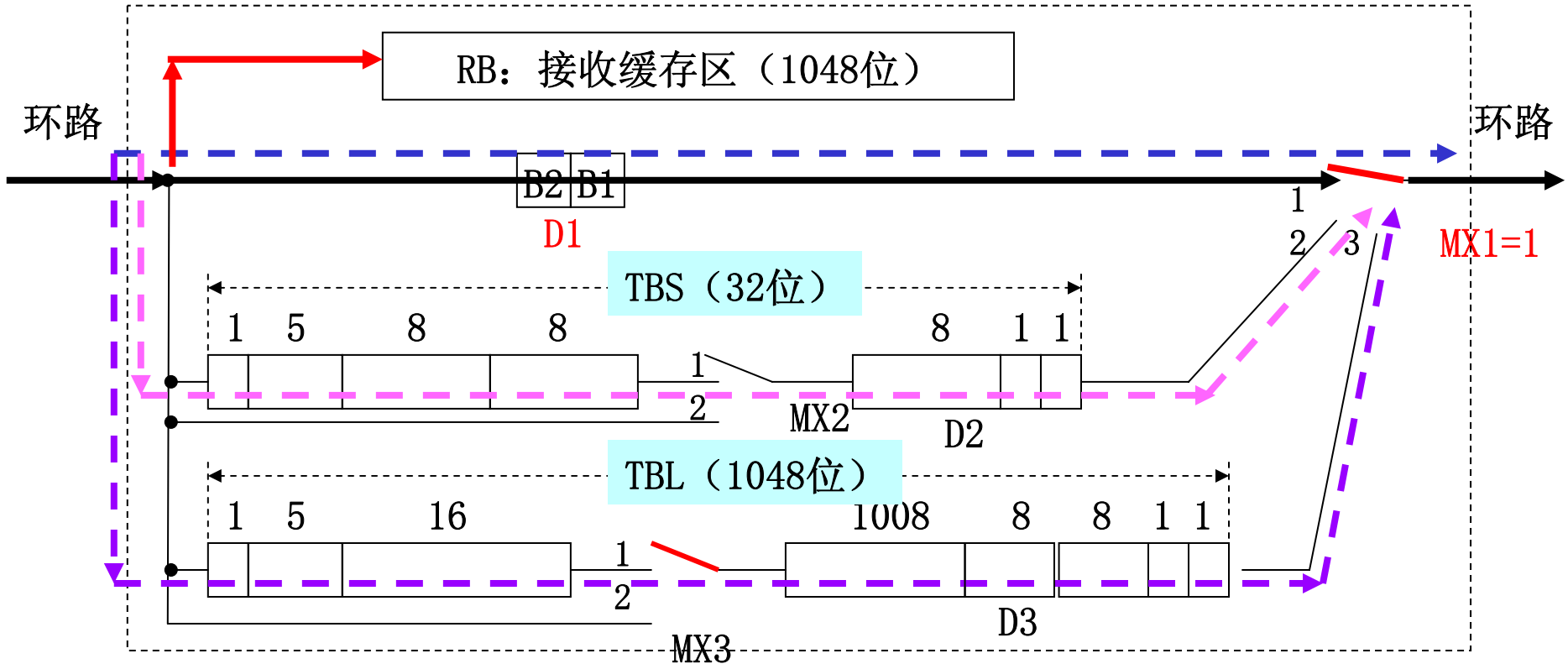
$C_3C_4C_5$=“010”表示正确收取。

★校验字段（P）仅提供偶校验的能力。

联想：一个时间片最多可以携带1024位用户数据。

空时间片的长度为24位。

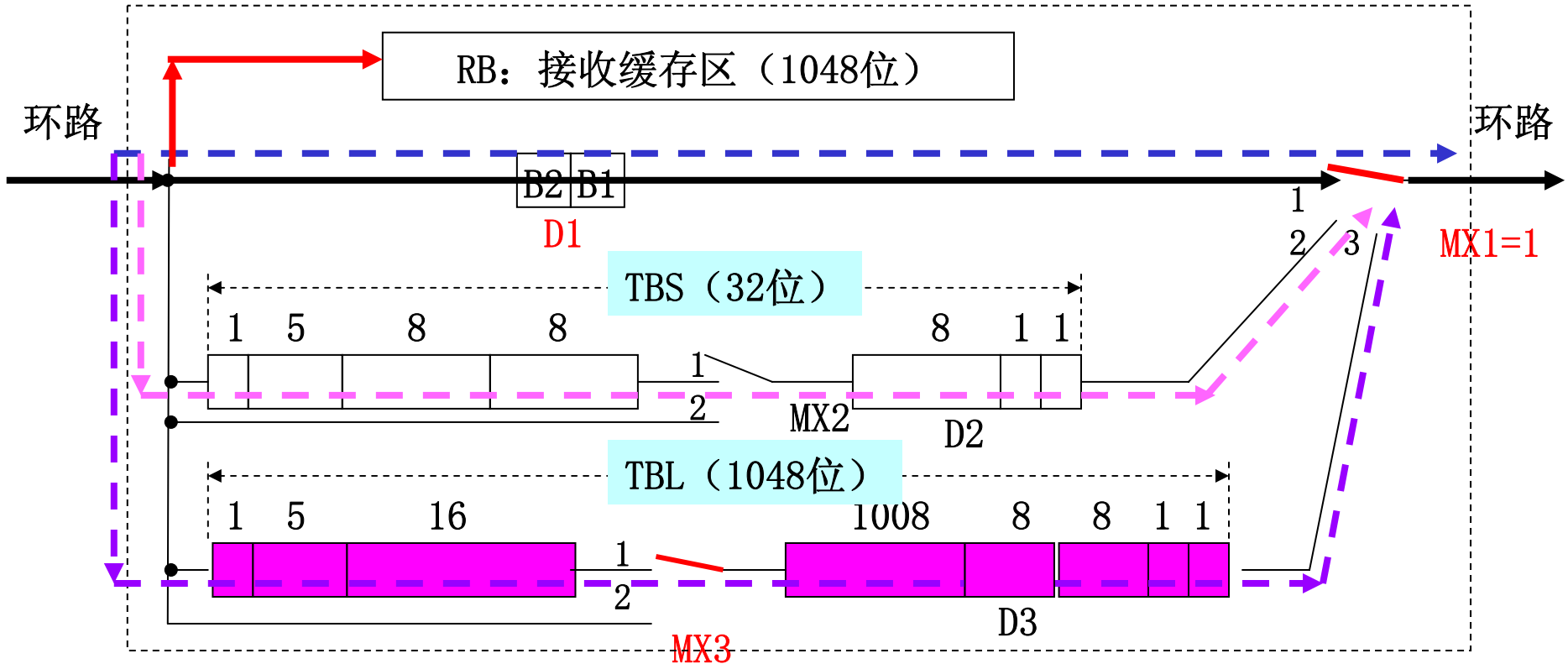
（3） RPU结构及工作过程



说明：

正常情况，MX1=1，RPU插入D1，利用2位延迟，判断空时间片，同时转发数据；

（3） RPU结构及工作过程

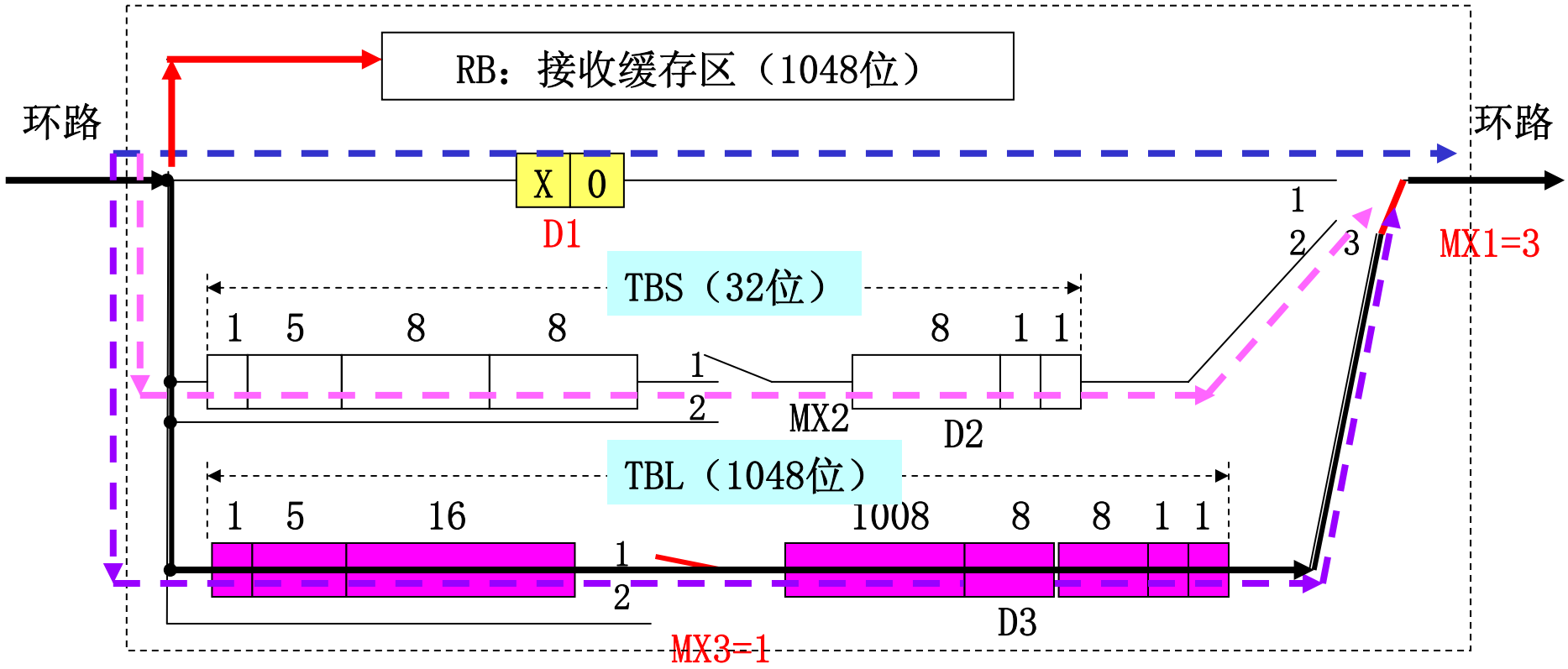


说明：

正常情况，MX1=1，RPU插入D1，利用2位延迟，判断空时间片，同时转发数据；

若有数据传输，形成数据分组，并填入TBS或者TBL（MX3=1）；

（3） RPU结构及工作过程



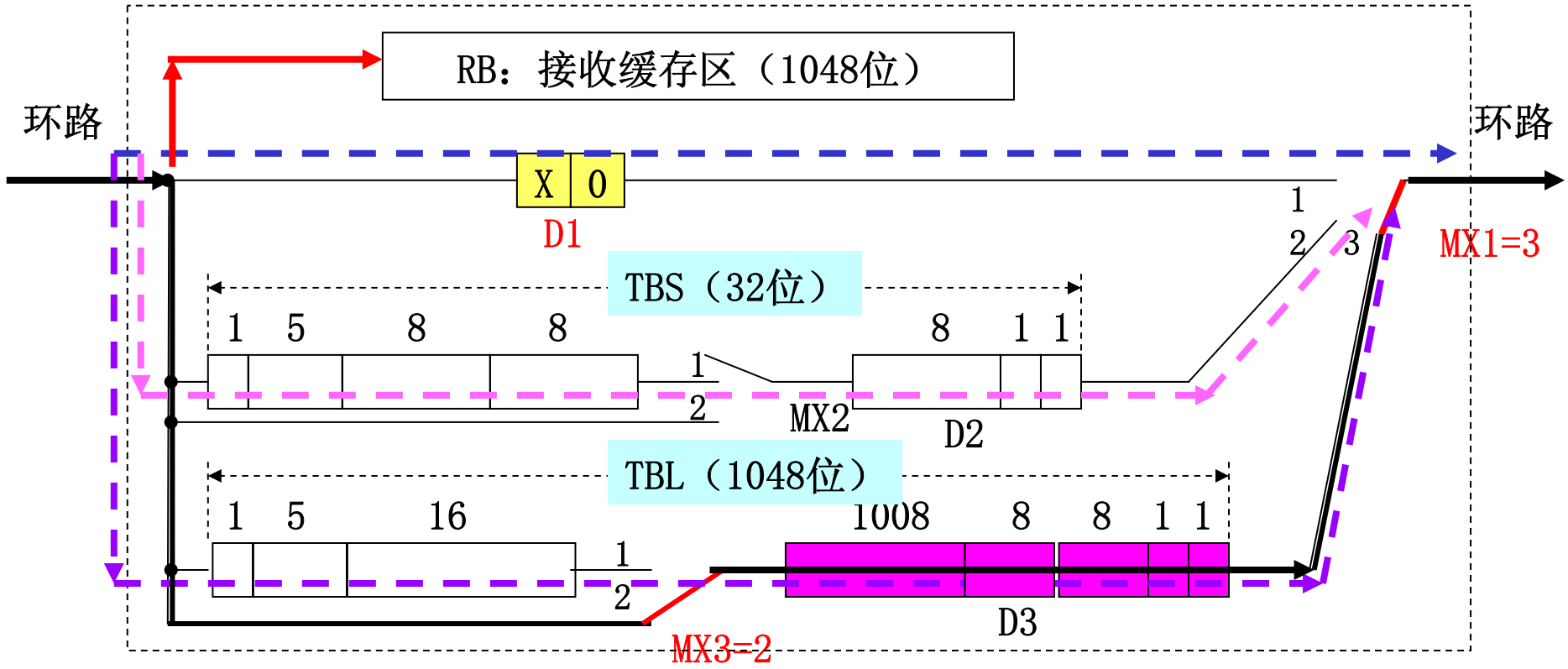
说明：

正常情况，MX1=1，RPU插入D1，利用2位延迟，判断空时间片，同时转发数据；

若有数据传输，形成数据分组，并填入TBS或者TBL（MX3=1）；

当 B1=‘0’（F/E=0，空时间片）时，MX1=3，TBL插入环路，发送数据分组；

（3） RPU结构及工作过程



说明：

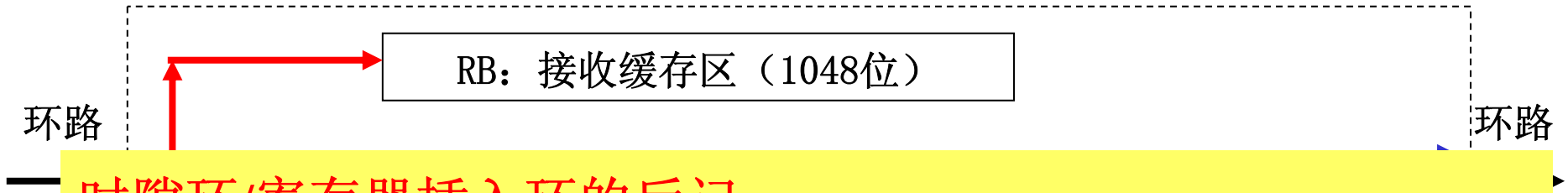
正常情况，MX1=1，RPU插入D1，利用2位延迟，判断空时间片，同时转发数据；

若有数据传输，形成数据分组，并填入TBS或者TBL（MX3=1）；

当 B1=‘0’（F/E=0，空时间片）时，MX1=3，TBL插入环路，发送数据分组；

当移出22位后，MX3=2，仅D3插入环路，继续发送数据分组；

（3） RPU结构及工作过程



时隙环/寄存器插入环的后记

时隙环和寄存器插入环能够充分体现环型网的特点（反映环型网的本质），一度得到重视，也被纳入IEEE标准（IEEE 802.7），但其局限性也显而易见：首先是扩展性较差，延迟随着结点个数增加而增加；其次，生不逢时，802.3、802.4、802.5的成熟，加之本身的优越性并不明显，导致支持的厂商不多，最终似乎也销声匿迹，…。

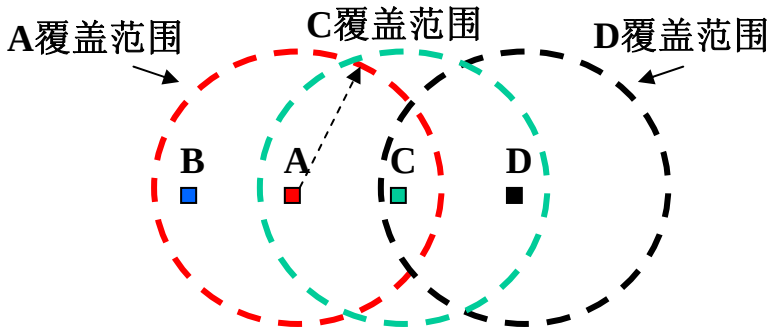
正常情况，MX1=1，RPU插入D1，利用2位延迟，判断空时间片，同时转发数据；
若有数据传输，形成数据分组，并填入TBS或者TBL（MX3=1）；
当 B1=‘0’（F/E=0，空时间片）时，MX1=3，TBL插入环路，发送数据分组；
当移出22位后，MX3=2，仅D3插入环路，继续发送数据分组；
当源发分组的前1018位再次进入D3时，MX1=1，D1及其内容插入环路（空时间片）。
所有分组均进入RB，根据内容进行复制接收，或者源发回收处理。

4.4.9 无线局域网—802.11

结点共享特定频率无线信道，使用天线（无线网卡）收发数据；

潜在问题1：功率决定信号覆盖范围，使用同一频率会造成相互干扰。基本原理可见“以太网起源”的Aloha网；

潜在问题2：隐藏终端（对应A的D），当A向C发数据时，B等待，C接收，但D可能也会发送数据，结果导致C无法正确收取。



解决方案：CSMA/CA（发前侦听，空闲发送，协商频段，避免冲突）；

协商频段：增加RTS（发送请求）/CTS（发送响应）协议；发方A发送RTS，告知C拟发送的数据长度和频段选择；收方C响应CTS，准备收取，同时告知C覆盖范围内的某频段将被占用；收方对收取的数据予以确认（ACK），释放占用的频段。

由于RTS使用相同的信道，如果发生冲突，则执行退避算法：

退避时间：随机数*时间片（8us）；

随机数取值：0～$2^{(重发次数+3)}-1$；

重发次数<=7，第5次以后，随机数均取值255；

可用频率：**2.4—2.4835Ghz**，可分**79**个频带，北美和欧洲；

2.471—2.497Ghz，可分**23**个频带，日本；

2.4465—2.4835Ghz，可分**35**个频带，法国；

传输速率：**1—4.5M**（间隔**0.5M**）、**11Mbps**；

物理层的信号传输采用直序扩频和跳频扩频。

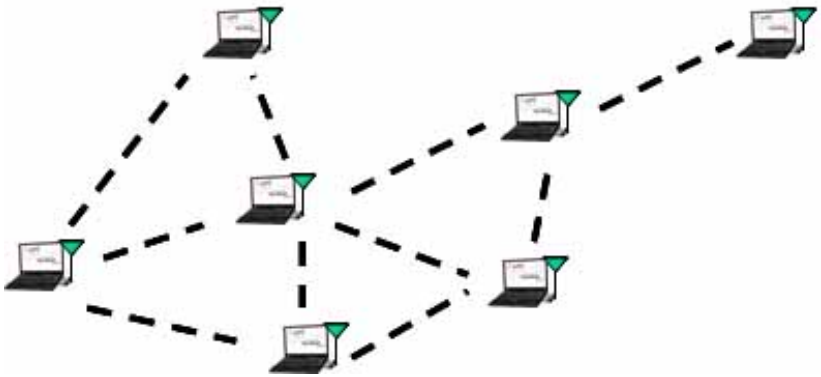
直序扩频：通过公共频段协商双方后续通信的单一频段；

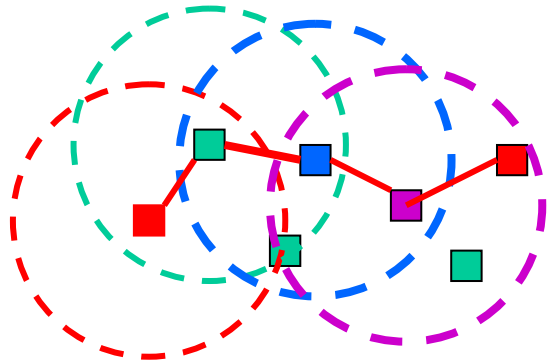
跳频扩频：通过公共频段协商伪随机数，后续通信在若干频段传输；

4.4.9 无线局域网—组网方式—独立基本服务集（IBSS）

结点具有移动性和自治（自组织）能力，结点和结点之间直接通信（包括转发），也称为自组织网（或者Ad Hoc、Manet）。

常用于突发事件（无转发设备的支持），如战场、震区等；





热门话题：信息的转发和路由。

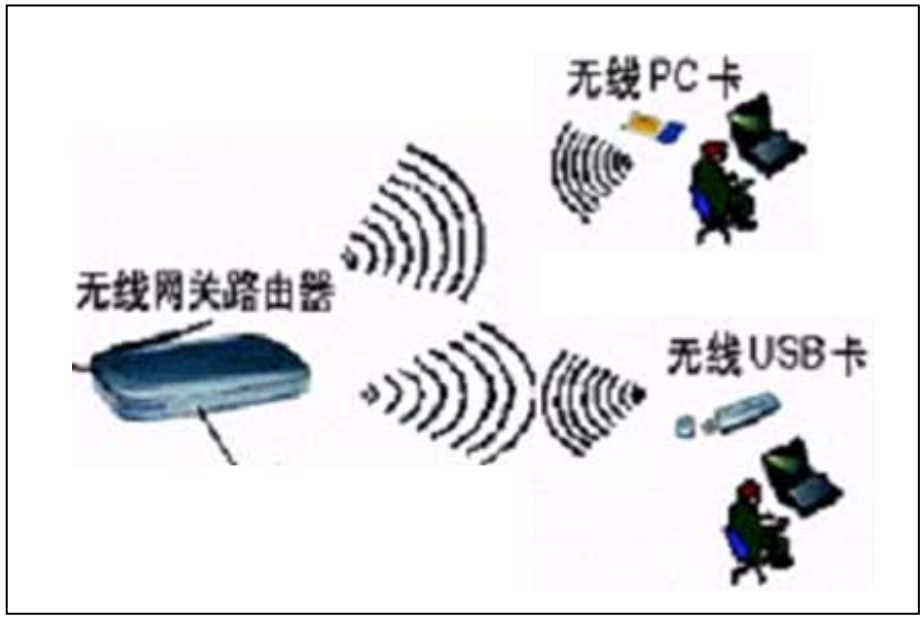
原因：结点的自主移动性，结点的辐射范围有限，结点的电池寿命有限，洪泛的相互干扰等；

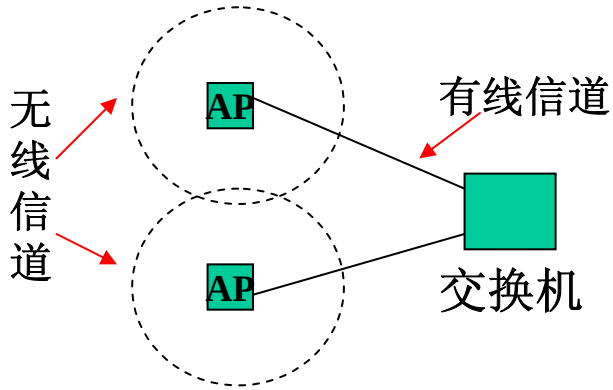
转发方案之一；根据信号强度（距离）计算转发的时间；远距结点先转发；感觉不到“转发”动作的结点进行转发。

4.4.9 无线局域网—组网方式—扩展服务集（ESS）

结点通过无线信道接入中间设备（访问点—**AP**），**AP**接入有线网；

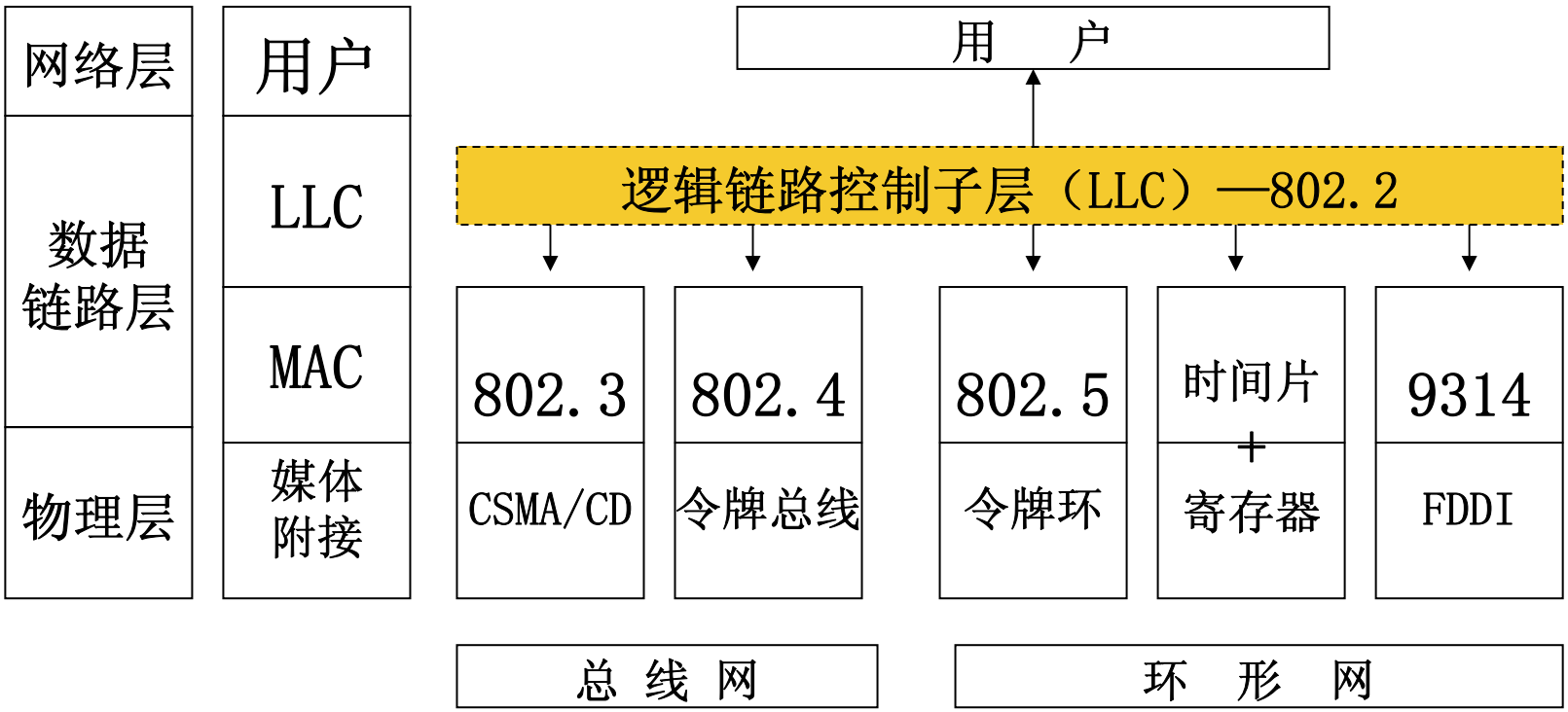
重叠区保证终端的移动性。





4.6 LLC(逻辑链路控制)子层

媒体访问控制（MAC）技术构成局域网的主要内容，
不同的媒体访问控制技术—不同的协议—不同的帧格式；
LLC的目的：屏蔽不同MAC技术，向高层提供统一服务和接口；
参照OSI/RM，LLC具有HDLC（或者SDLC）类似的内容。



（1） LLC/MAC接口服务规范

★ 定义MAC子层应向LLC子层提供的服务，支持LLC子层实体之间交换LLC PDU（LLC帧），该服务与媒体及访问控制方法无关。

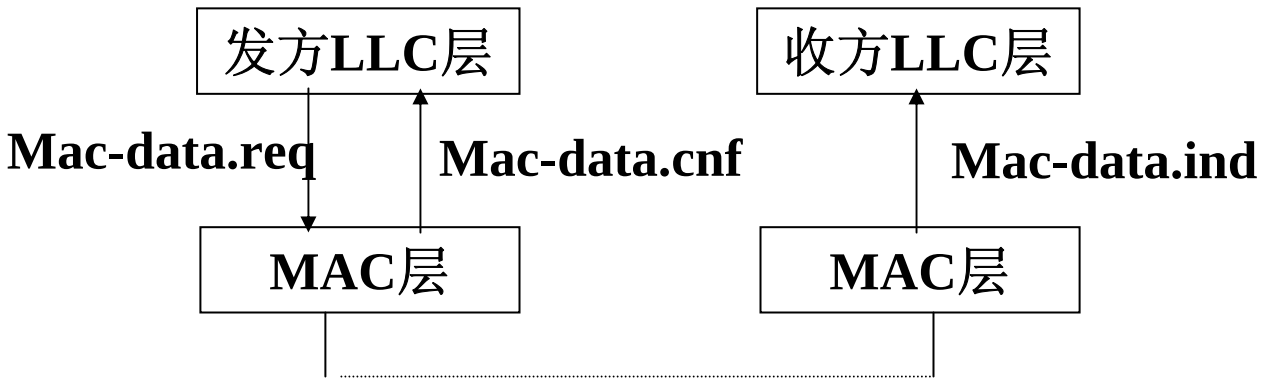
★ MAC服务原语

MAC-DATA.req(RA,LP,SC)，请求发送一个LLC-PDU（LP）至对等实体（RA）；

MAC-DATA.ind(RA,LA,LP,S,SC)，向LLC实体指示收到一个LLC-PDU及其状态；

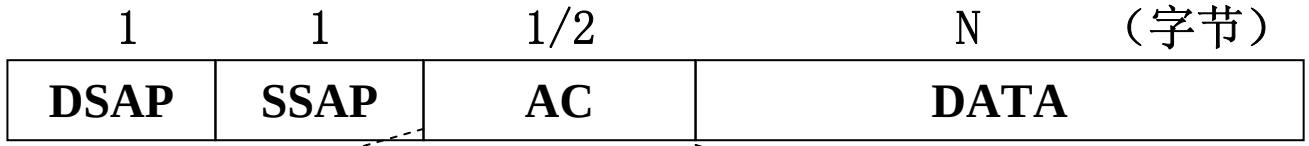
MAC-DATA.cnf(S,SC)，向源发LLC实体报告LLC-PDU的传输结果。

其中：SC—控制信息，S—状态；RA/LA—远程/本地地址。

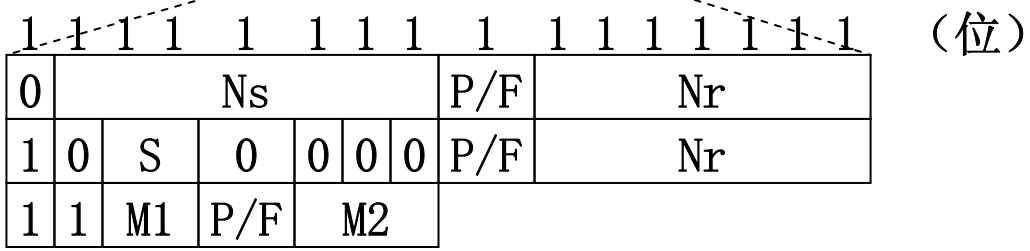


（2） LLC/LLC对等协议规程

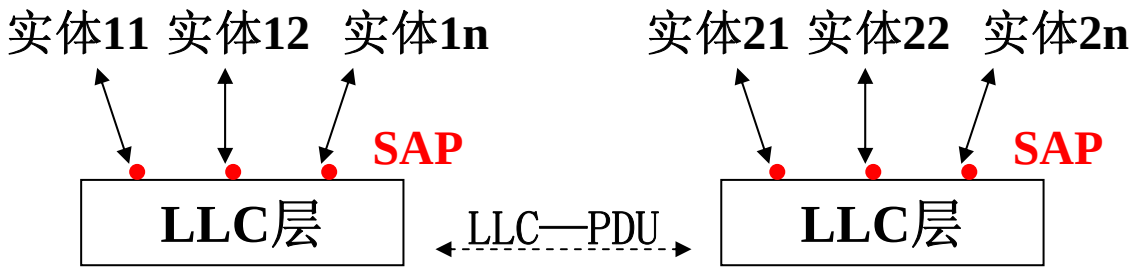
★ 定义LLC实体之间交换的帧格式（类HDLC）。



访问控制字段



SAP（服务访问点）：提供服务的地点：逻辑标识，如端口等；
DSAP（信宿）：首位标识单地址或者组地址（I=0/G=1）；
SSAP（信源）：首位标识命令或者响应（C=0/R=1）；



★ 类型1（Type1）：基本的面向无连接的服务。

数据传输之前，无需进行对等实体之间的连接；

数据传输时，LLC层不提供差错恢复、流量控制和排序功能；

本类型服务适用于对数据传输可靠性要求不高，或者可由高层采取措施保证数据传输可靠性的环境。

相关服务原语：

L-data.req(LA,RA,LS,SC)，

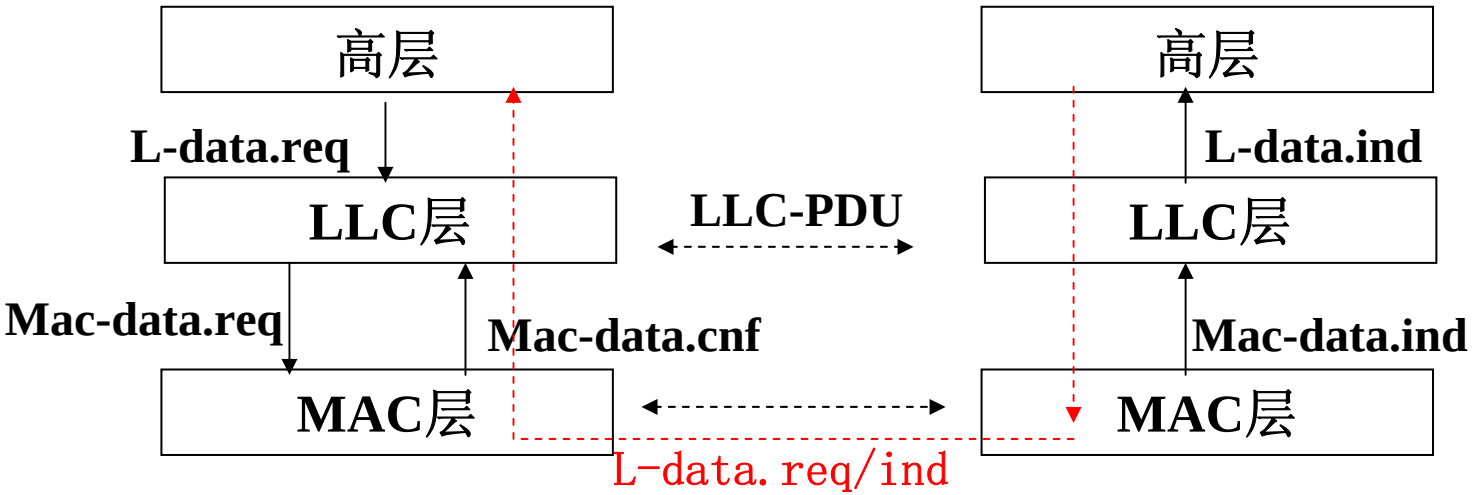
L-data.ind(LA,RA,LS,SC)；

其中：

LA/RA—本地/远程地址，

LS—被传输的LSDU，

SC—控制信息（如优先级）。



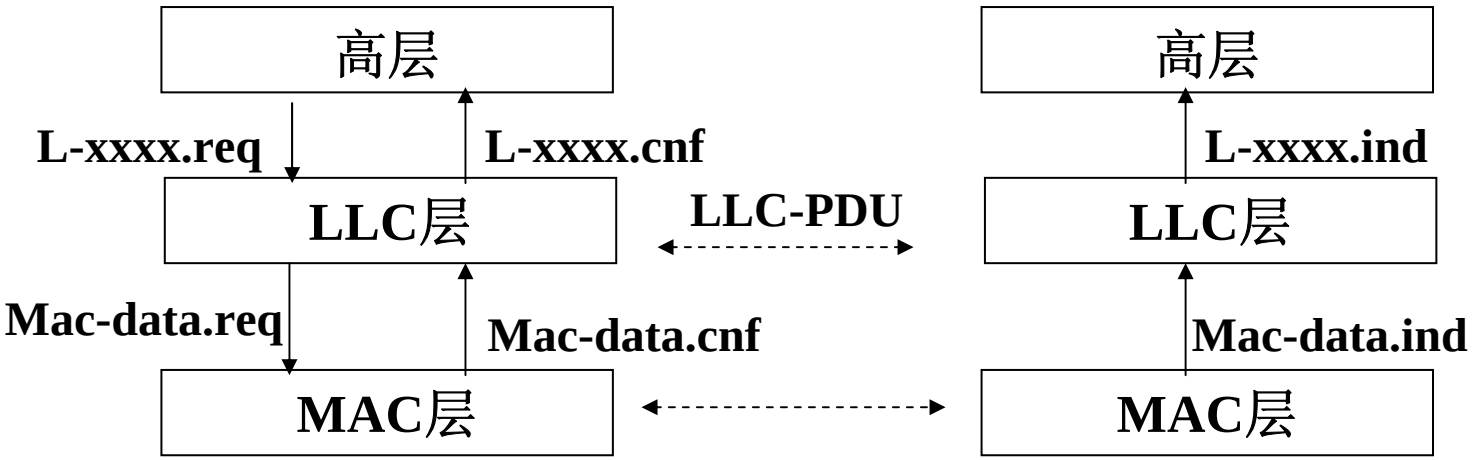
★ 类型2（Type2）：基本的面向连接的服务。

— 在对等实体之间连接建立的基础上传输数据，并提供DL的差错恢复、流量控制和排序等功能。

相关服务原语：　　（略去部分结果参数）

- 建立连接：L-CONNECT.req/ind/cnf(LA,RA,S,SC)；
- 数据传输：L-DATA.req/ind/cnf(LA,RA,LS,SC)；
- 连接复位：L-RESET.req/ind/cnf(LA,RA)；
- 连接释放：L-DISCONNECT.req/ind/cnf(LA,RA)；
- 流量控制：L-CONNECT-FLOWCONTROL.req/ind(LA,RA,A)；

高层实体请求控制来自LLC子层的数据流量。A：允许的数据流量信息。



第5章 广域网

5.1 特点:

★ 支持用户使用计算机进行远距离的信息交换;

★ 覆盖范围广,结点间距离远，考虑因素增多;

☆ 线路成本增加，媒体带宽的利用;

☆ 距离远，传输可靠性，以及线路故障和冗余;

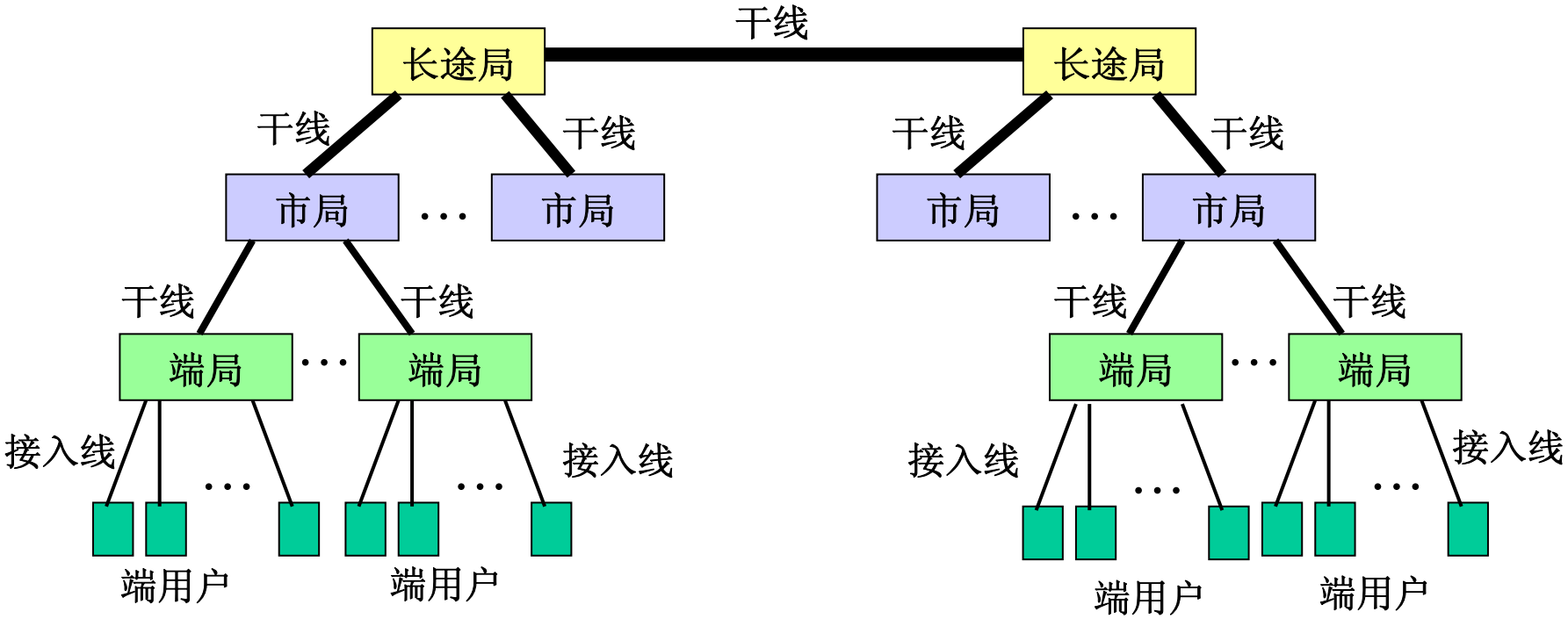
☆ 覆盖范围大，用户多，路由取代LAN中的广播;

★ 电信部门或公司负责组建、管理和维护，并向全社会提供面向通信的有偿服务，流量统计和计费问题;

5.2 SONET/SDH（Synchronous Optical Network/ Synchronous Digital Hierarchy —同步光纤网/同步数字体系）

5.2.1 SONET/SDH的提出

广域网的传输系统— 传统电话网络：



干线：大对数电缆—光纤；

为避免信号衰减，干线上增加放大器，但也等比例放大了噪声；

5.2 SONET/SDH（Synchronous Optical Network/Synchronous Digital Hierarchy —同步光纤网/同步数字体系）

5.2.1 SDH的提出

光纤应用于干线—支持语音信号传输；

语音信号数字化—脉码调制（PCM）：取样（8000次/秒）、量化（256级）、编码（8位），传输速率64Kbps—DS-0级；

★ 中继器替代放大器，鉴别/再生，消除噪声影响；

★ 多路复用，充分利用光纤的带宽，替代（原）通信网的干线；

★ 光缆干线复用标准，一条光纤应支持多少路语音信号传输？端设备成本随路数提升而提升（兼顾各类需求）。

PCM载波标准：

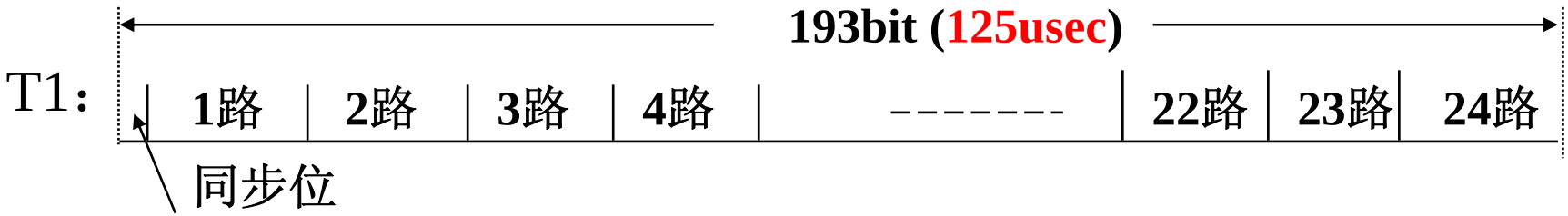
— T系列（北美数字体系），北美（美国、加拿大和澳大利亚等）；

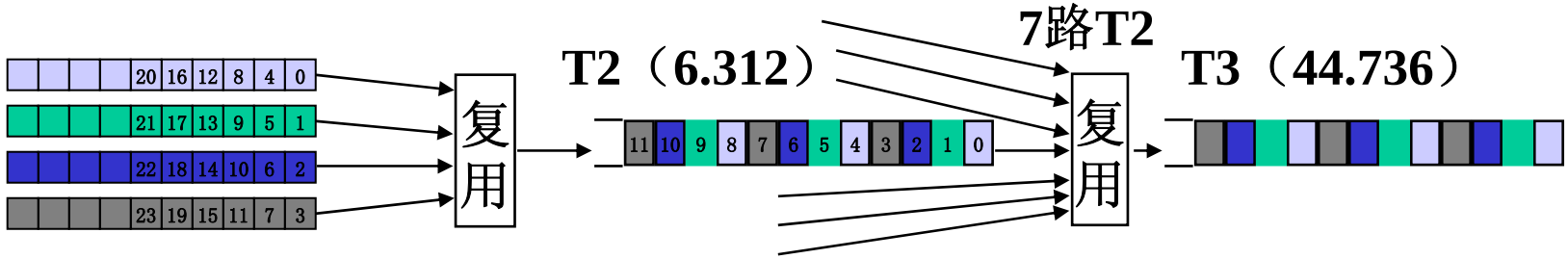
— E系列（欧盟数字体系）：欧洲、南美、非洲、墨西哥和亚洲部分国家；

T载波系列—AT&T等提出

使用时分多路复用技术共享光纤信道，支持数字化语音信息传输；

级别	T1	T2=4T1	T3=7T2	T4=6T3
速率Mbps	1.544	6.312	44.736	274.716
语音路数	24	96	672	4032





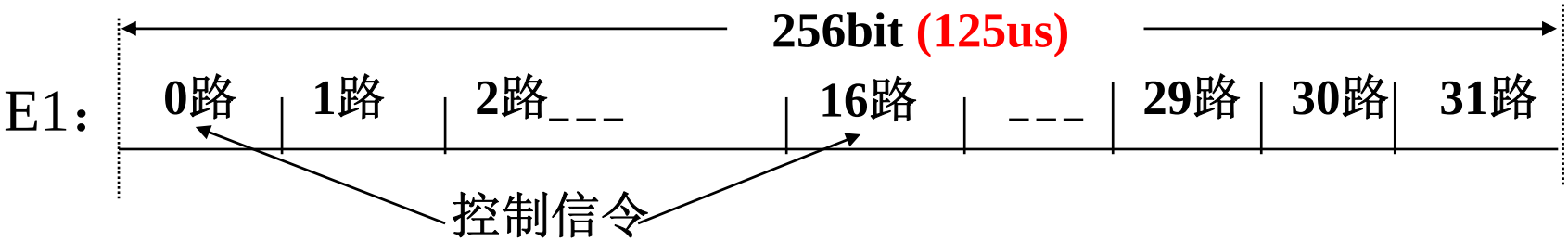
注意：T1→T2→T3采用了逐位复用的方法；增加了若干位用于组帧和管理。

如：6.312 - 4*1.544 = 6.312 - 6.176

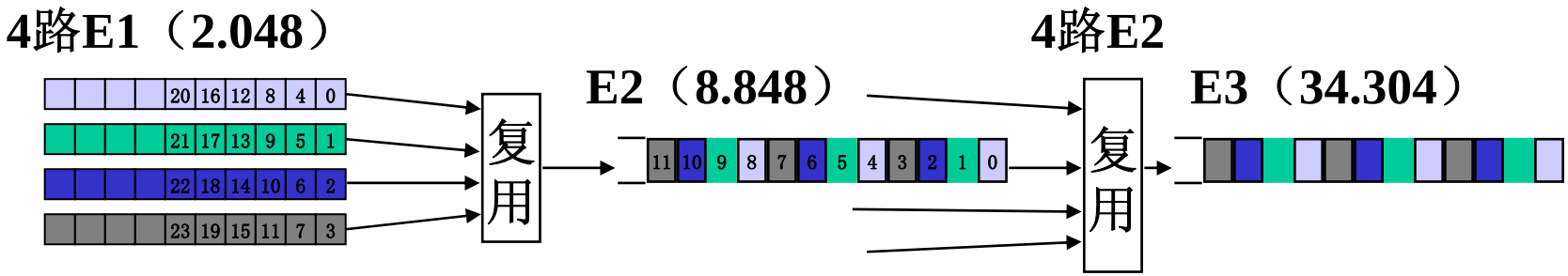
E载波系列

使用时分多路复用技术共享光纤信道，支持数字化语音信息传输；

级别	E1	E2=4E1	E3=4E2	E4=4E3
速率Mbps	2.048	8.848	34.304	138.284
语音路数	32	128	512	2048



E1：每125微秒一帧（32*8=256位），可传递30路语音；
为保证语音质量，各类E帧的传输耗时均限定为125us。



准同步数字体系（PDH）

各个国家独立建立自己的数字同步体系—PDH；

基本思想：逐级复用（如：T1→T2→T3）；

目的：充分利用光纤的带宽，将一“群”用户的信息复用到一条线路上传输；

基群（基本的群）速率：最基本的复用速率。

	基群	二次群	三次群	四次群
欧洲，中国（复用话路）	2.048Mbps/E1 32路	8.848Mbps/E2 4×E1＝128路	34.304Mbps/E3 4×E2＝512路	138.264M 4×E3＝2048路
北美（复用话路）	1.544Mbps/T1 24路	6.312Mbps/T2 4×T1＝96路	44.736Mbps/T3 7×T2＝672路	274.716M 6×T3＝4032路
日本（复用话路）	1.544Mbps/T1 24路	6.312Mbps/T2 4×T1＝96路	32.064Mbps/T3 5×T2＝480路	97.728Mbps 3×T3＝1440路

PDH的缺陷：

★缺乏国际统一的标准接口，互不兼容；

★无法实现光路上互通，光/电转换增加成本，影响效率；

★逐级逐位复用缺乏灵活性，增加了复用/解复用设施的复杂性。

光纤的优越性（应用需求）刺激标准的制定。

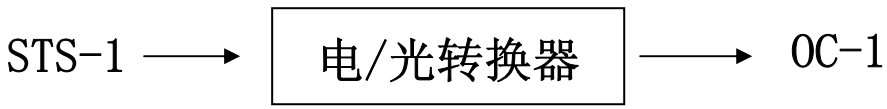
同步光纤网（SONET）标准：　（美国88年制定）

考虑PDH产品（低级别）已相对成熟，并广泛应用；

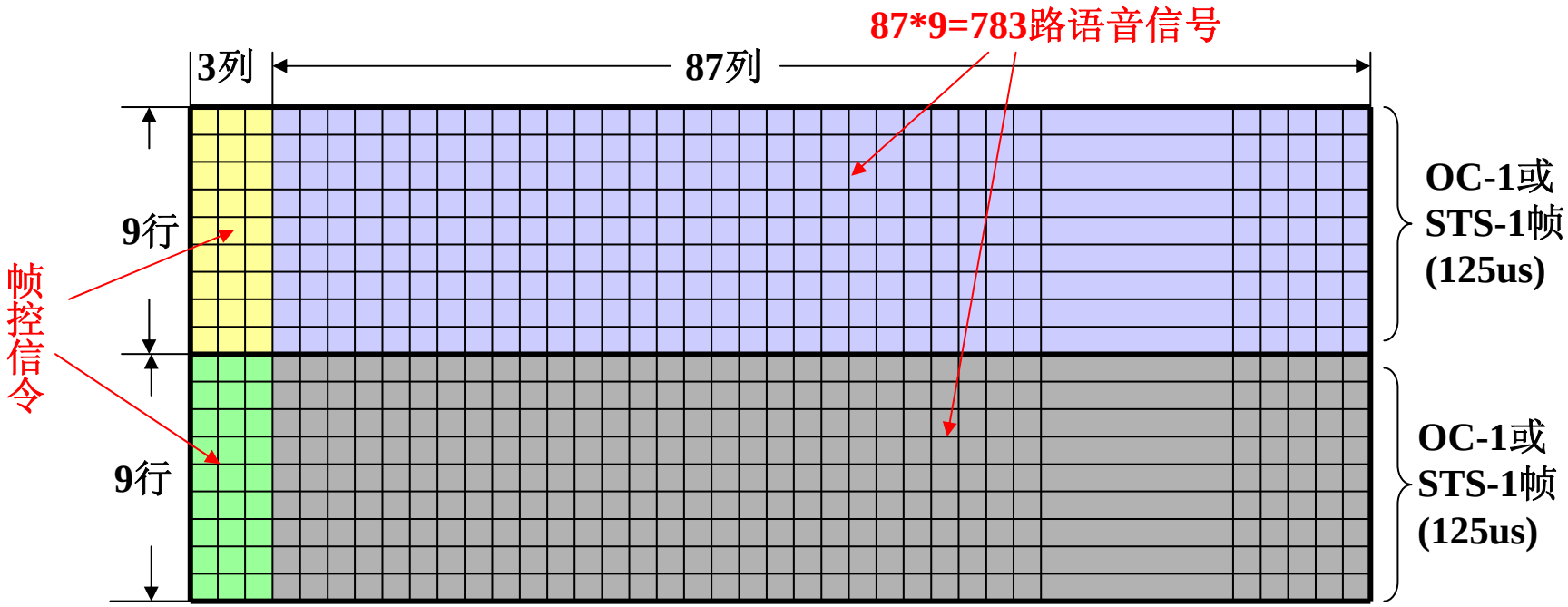
以51.84Mbps为基准进行递增，可支持铜缆和光纤；

基于铜缆的电信号传输称为第一级同步传送信号（STS-1）；

基于光纤的光信号传输称为第一级光载波（OC-1）。



SONET的帧结构



- —— 8位1路语音或者控制信号；

传输速率=90列*9行*8位/125us=51.84Mbps

同步数字体系（SDH） (CCITT制定国际标准)

基本SDH速率为155.520Mbps，称第1级同步传送模块（STM-1）

SDH标准的制定，使得欧洲、北美和日本的三种不同的数字传输体系在STM-1级别上得到了统一。

N路STM-1可以复用为一个STM-N，利于解复用的实现。

SONET/SDH速率对照

线路速率(Mbps)	光载波系列	同步传送信号系列	同步传送模块系列
51.840	OC-1	STS-1	
155.520	OC-3	STS-3	STM-1
466.560	OC-9		STM-3
622.080	OC-12		STM-4
933.120	OC-18		STM-6
1244.160	OC-24		STM-8
1866.240	OC-36		STM-12
2488.320	OC-48		STM-16

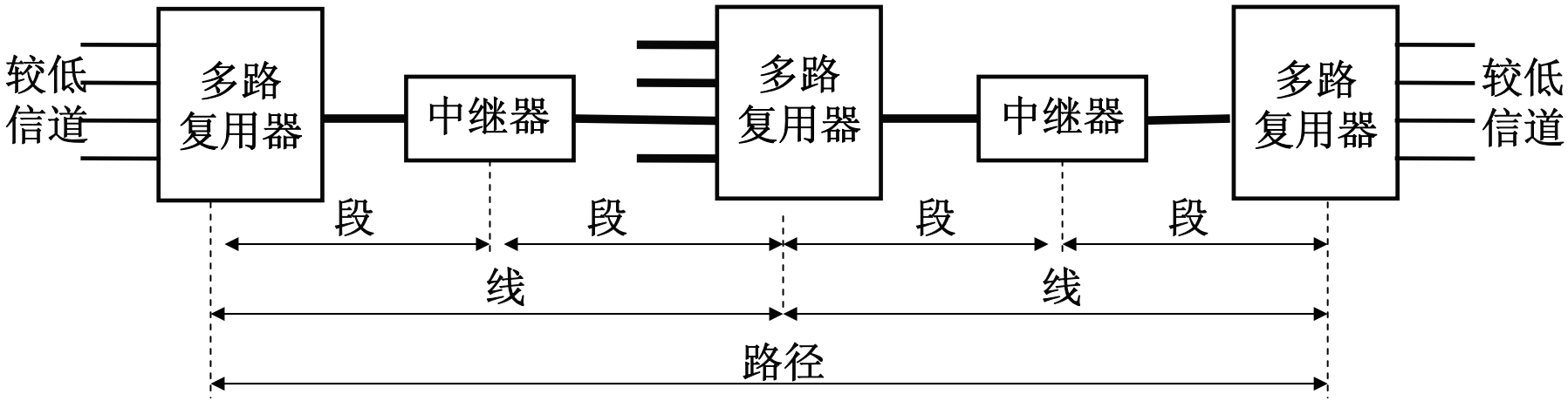
5.2.2 SDH的原理

(1) SDH网络

基于时分多路复用技术的数字传输网络，由多路复用器和中继器组成，并通过光纤进行连接。

多路复用器：多个较低级别的信道复用到一个较高级别信道；

中继器：实现长距离传输时的信号再生和转发。



段：设备之间的连接；

线：复用器之间（可能经过一个或者多个中继器）的连接；

路径：源和宿之间的连接。

（2） SDH帧结构

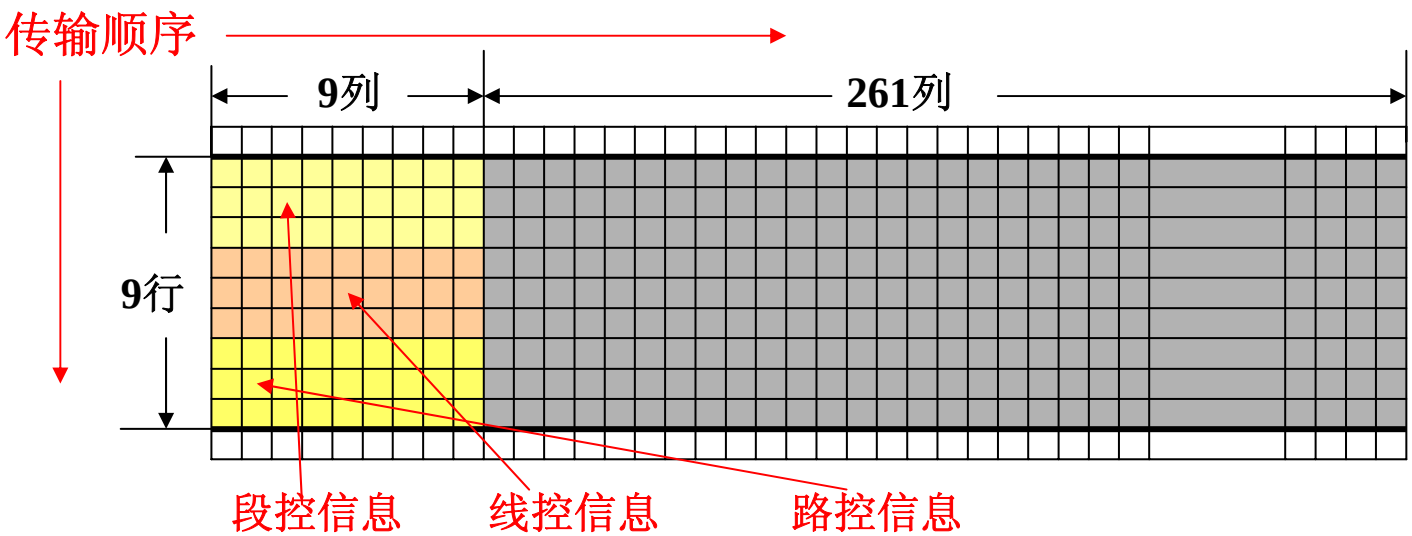
采用同步多路复用技术，被复用的信号组成一个数据块（称为帧）进行传输

STM-1帧（155M）结构：9行*270列=2430个字节；

速率：2430字节*8位/125us = 155.52Mbps

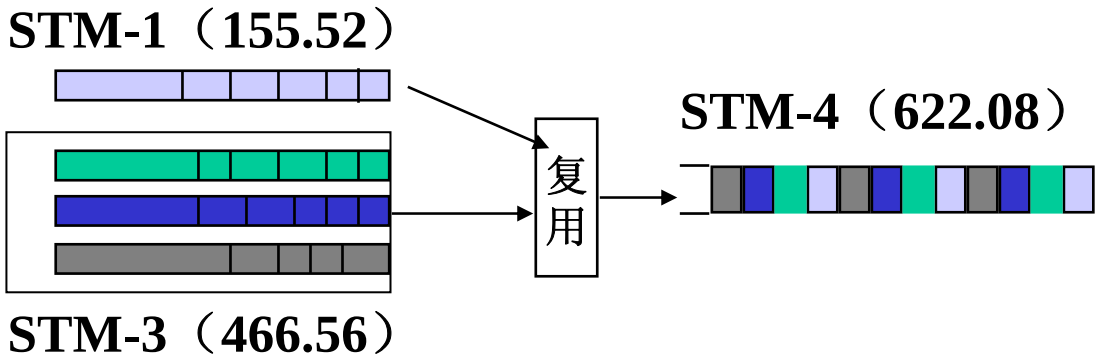
前9行9列：存放控制信息：包括段首SH、线首LH和路径首部PH以及段、线和路径设施处理的各种控制信息，如同步信息、时钟信息、校验信息等；

后9行261列：存放被传输的信息。

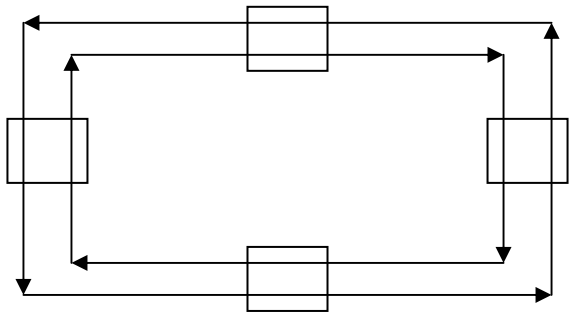


（3） SDH的信道复用

SDH支持不同级别的速率的混合复用，字节复用。

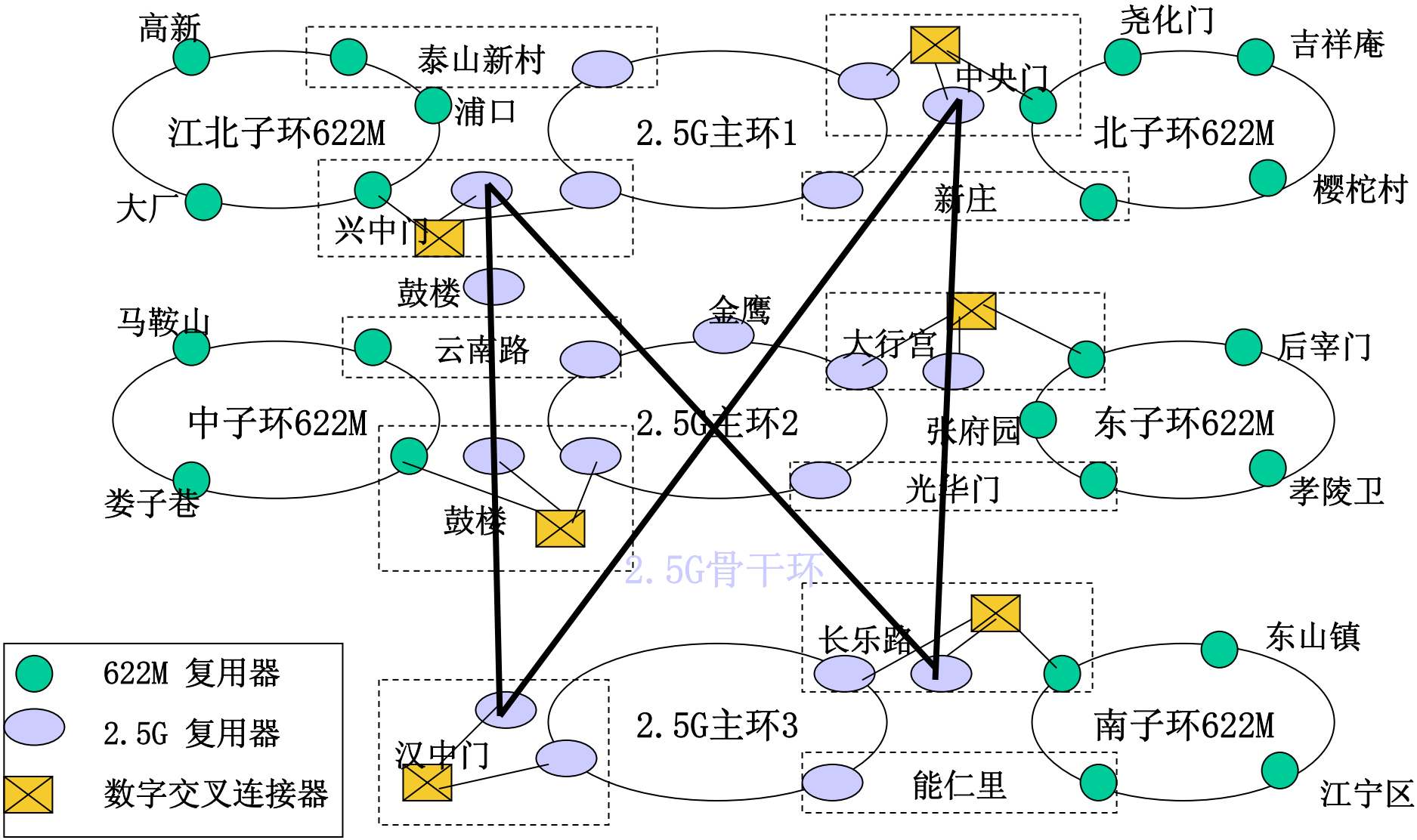


SDH网络主要提供高速的物理信道，构造基于光纤的长途传输干线；
SDH网络本身不提供任何传输协议，仅作为广域网的基础网络；
为提高可靠性，SDH网络采用自愈双环结构（类似FDDI）。



SDH网络实例—南京SDH传输网总体结构（1996年12月）

含4个2.5G(2488.32M。STM-16)骨干主环，5个622M(STM-4)子环。



5.2.3 数字数据网（DDN）

DDN是电信部门向用户提供的一种半永久性的连接电路，提供中高速、高质量的点一点的数字专用电路。

核心技术：基于光纤的时分多路复用技术。

特点：

- DDN是面向用户的数字传输技术，速度较SDH低。
- DDN采用时分多路复用技术将支持数字信息高速传输的光纤通道划分为一系列的子信道（例如：E1信道划分为32路64Kbps的子信道，可以分配给30个用户使用）；
- DDN的基本速率为64Kbps，用户租用的信道速率应为64Kbps的整数倍。
- DDN本身并不提供任何通信协议的支持，在DDN信道上使用何种通信协议由用户自行决定
- DDN仅提供点到点通信的专用信道（专线），因此当一个用户希望和多个其它的用户使用DDN通信时，必须租用多个DDN端口。

★缺点

DDN是固定信道方式，不能进行动态复用，在数据量不大的情况下线路利用率较低；由于是点－点的通信，需要多个**DDN**端口才能支持与多个结点通信，进网的端口数多。

★发展现状和未来发展

DDN专线常作为固定伙伴之间，或者总部/分部之间连通的首选方案，根据信息量的情况向电信部门申请带宽（**64Kbps**的倍数）。

例如：南大—东大（地区网络中心）

受帧中继网络应用的影响，电信部门常以帧中继代替**DDN**出租给用户。

5.3 分组交换数据网络（X25网络）

5.3.1 原理和组成

分组交换数据网以分组交换（存储—转发）方式工作，遵循CCITT X.25建议。

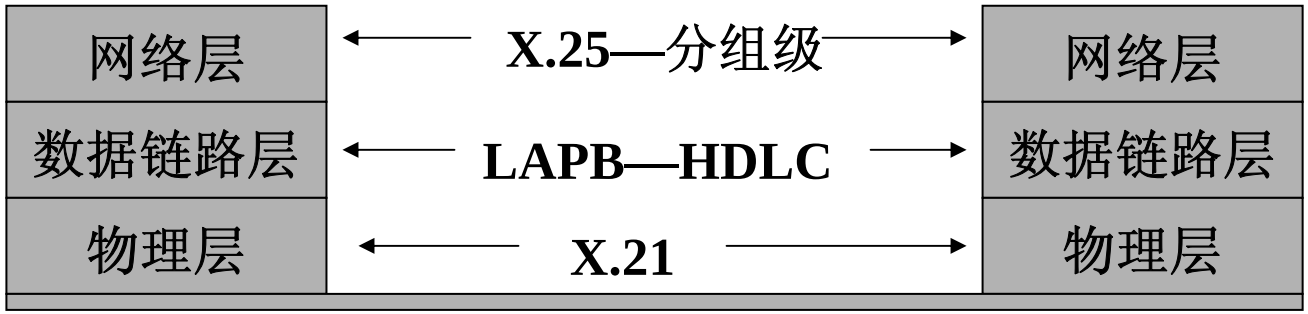
用户数据拆分为分组（131=128+3字节），在X25网络中传输。

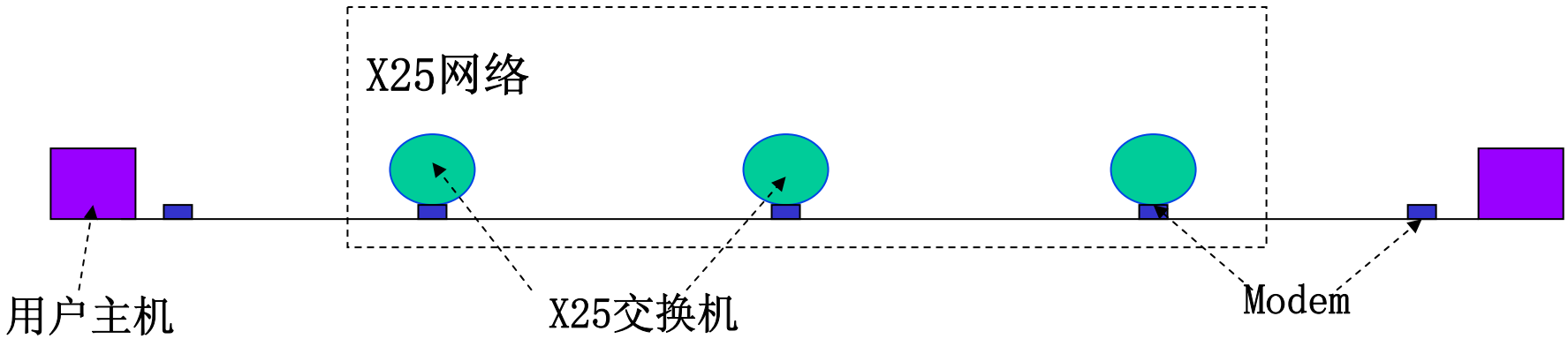
X.25网络采用分布式的网状拓扑结构，有如下特点：

★ 网络扩充和主机入网比较简单，可以很方便地增加结点，或者接纳主机入网；

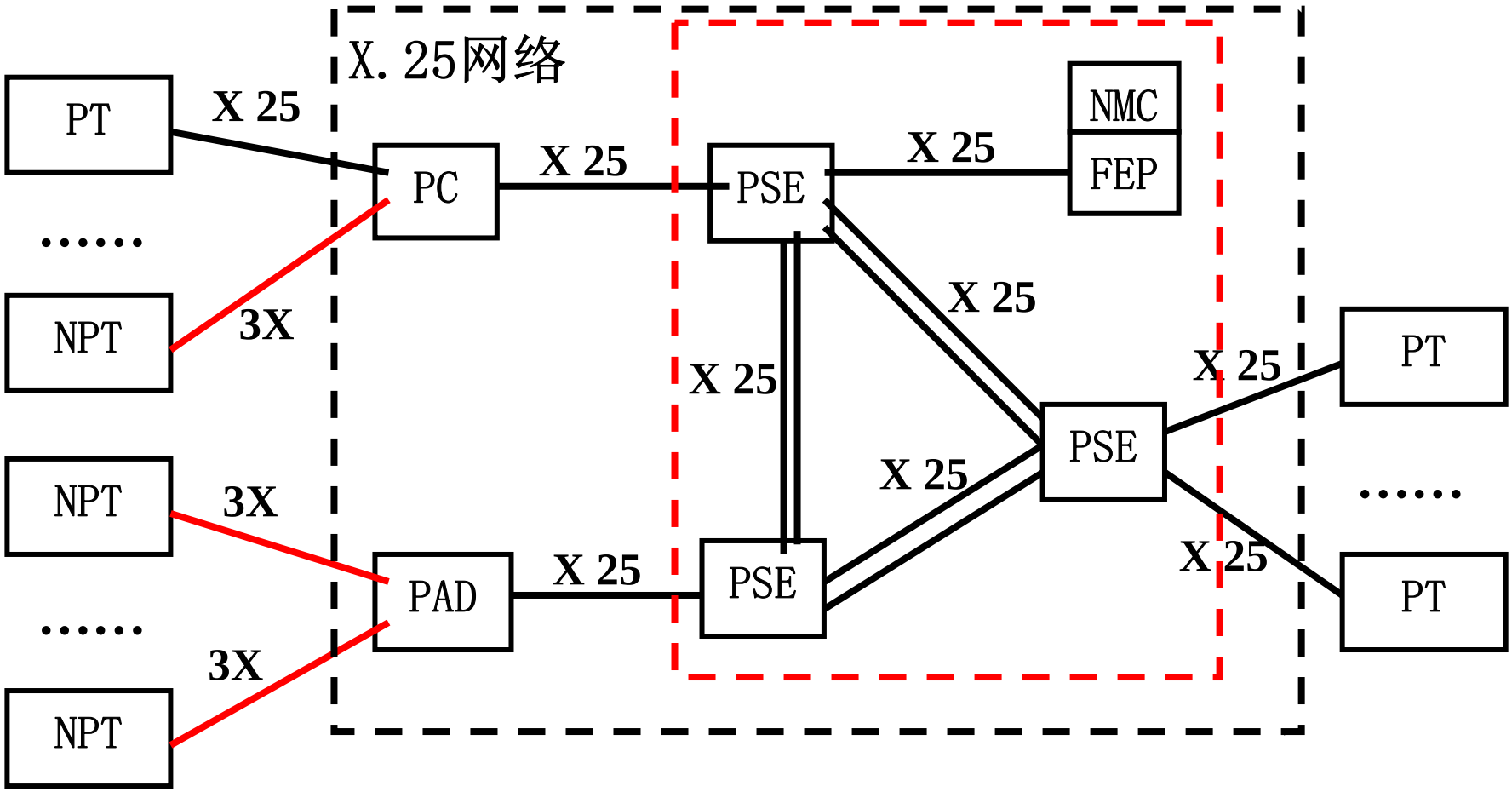
★ 网络完整性和可靠性较高，一对结点之间可以具有一条以上的路径，不会因为某些链路或者结点的故障造成全网的瘫痪。

X25网的体系结构


网络层
X.25—分组级
网络层
数据链路层
LAPB—HDLC
数据链路层
物理层
X.21
物理层


X25网络
用户主机
X25交换机
Modem

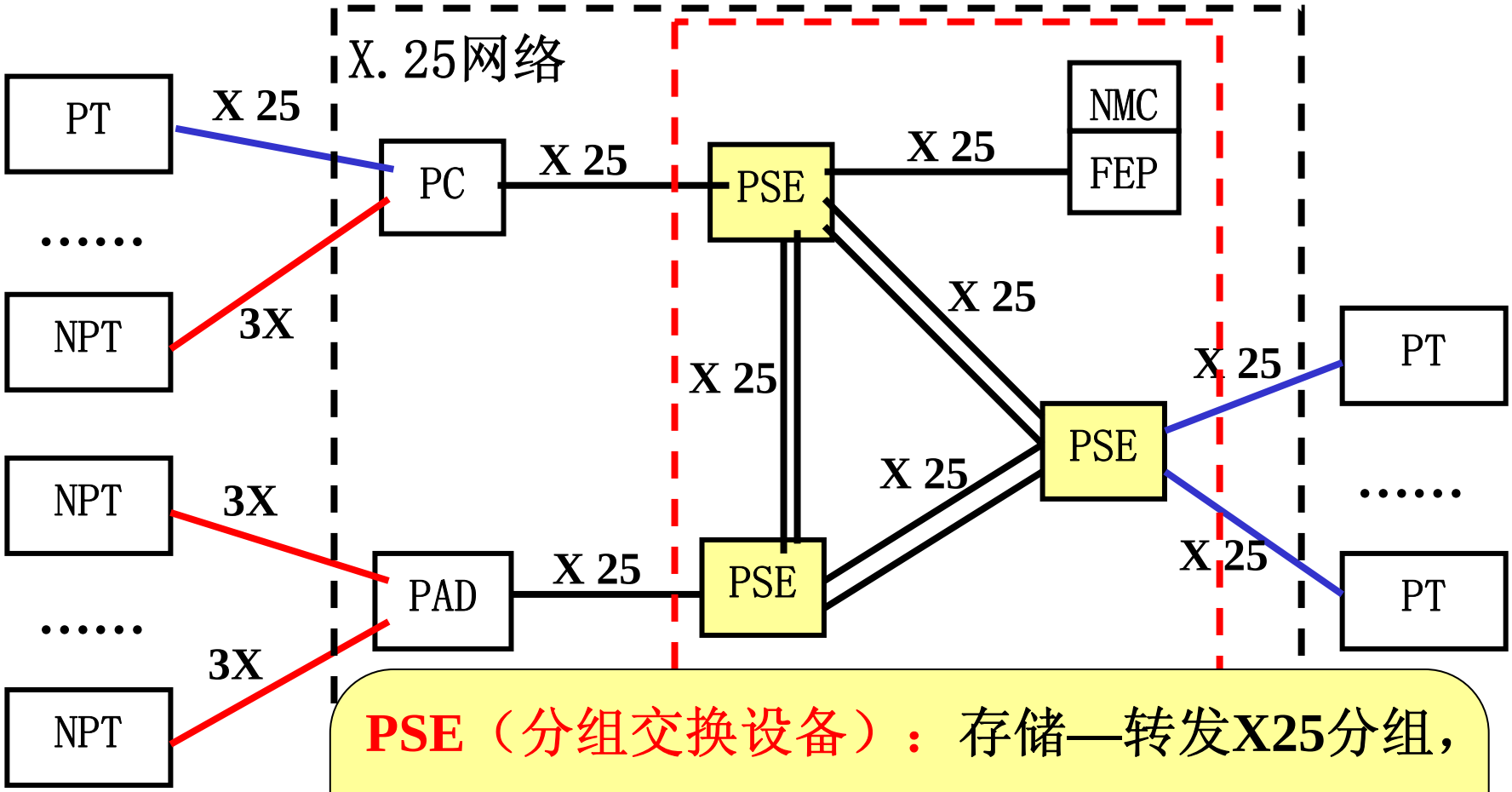
X.25网络结构示意图



PT—分组终端，NPT—非分组终端；3X—X3、X28、X29建议；
PSE—分组交换设备， NMC—网络管理中心， PC—分组集中器，
PAD—分组装拆设施，FEP—前端通信处理机，

红线—异步接入， 黑线—同步接入。

X.25网络结构示意图



PT—分组终端，

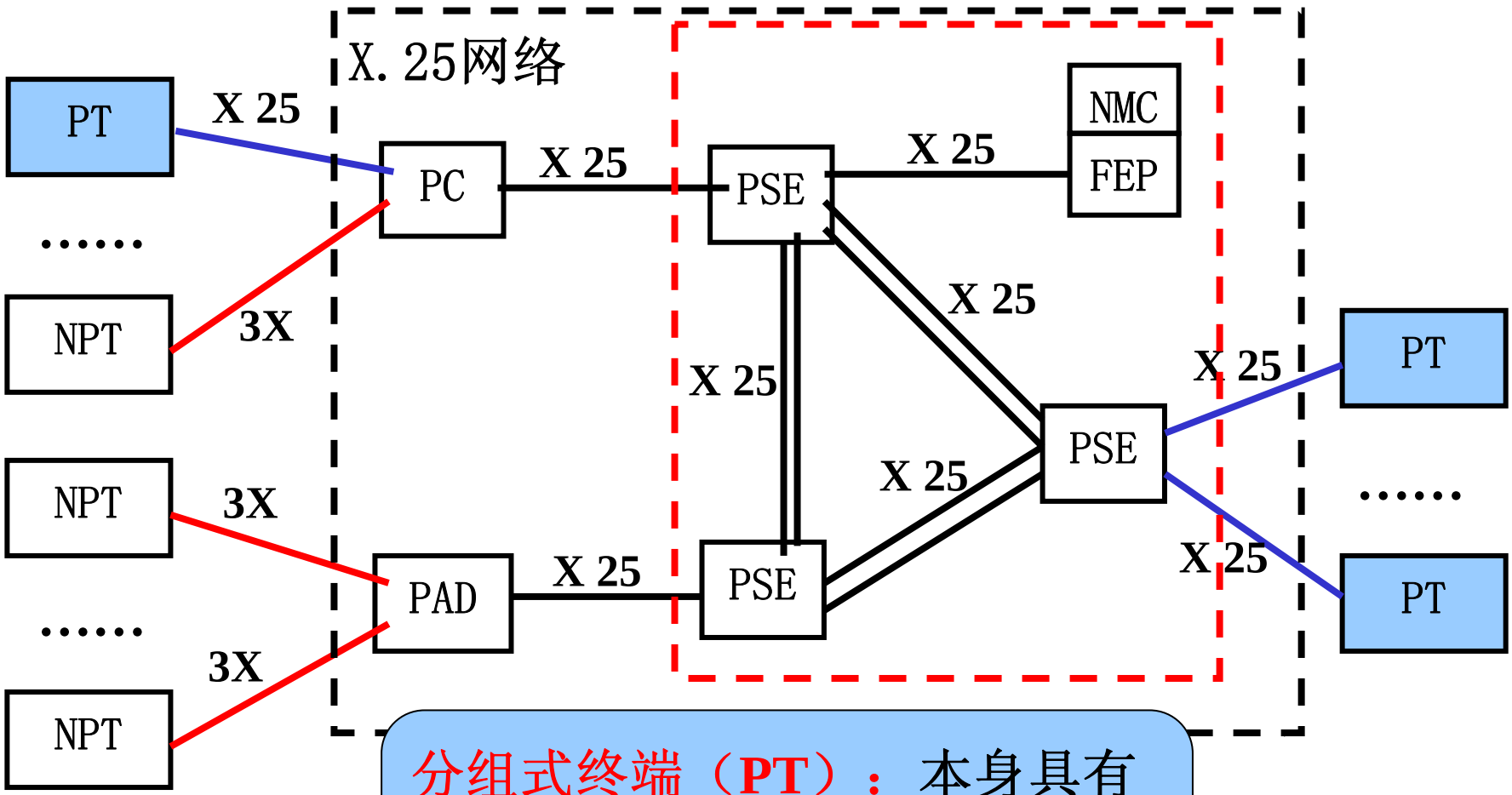
PSE—分组交换

PAD—分组装拆

红线—异步接入，

PSE（分组交换设备）：存储—转发**X25**分组，转发时执行路由选择算法。路由选择的目的是保证用户的数据分组可以尽快地穿越网络，使得网络具有较高的吞吐率。

X.25网络结构示意图

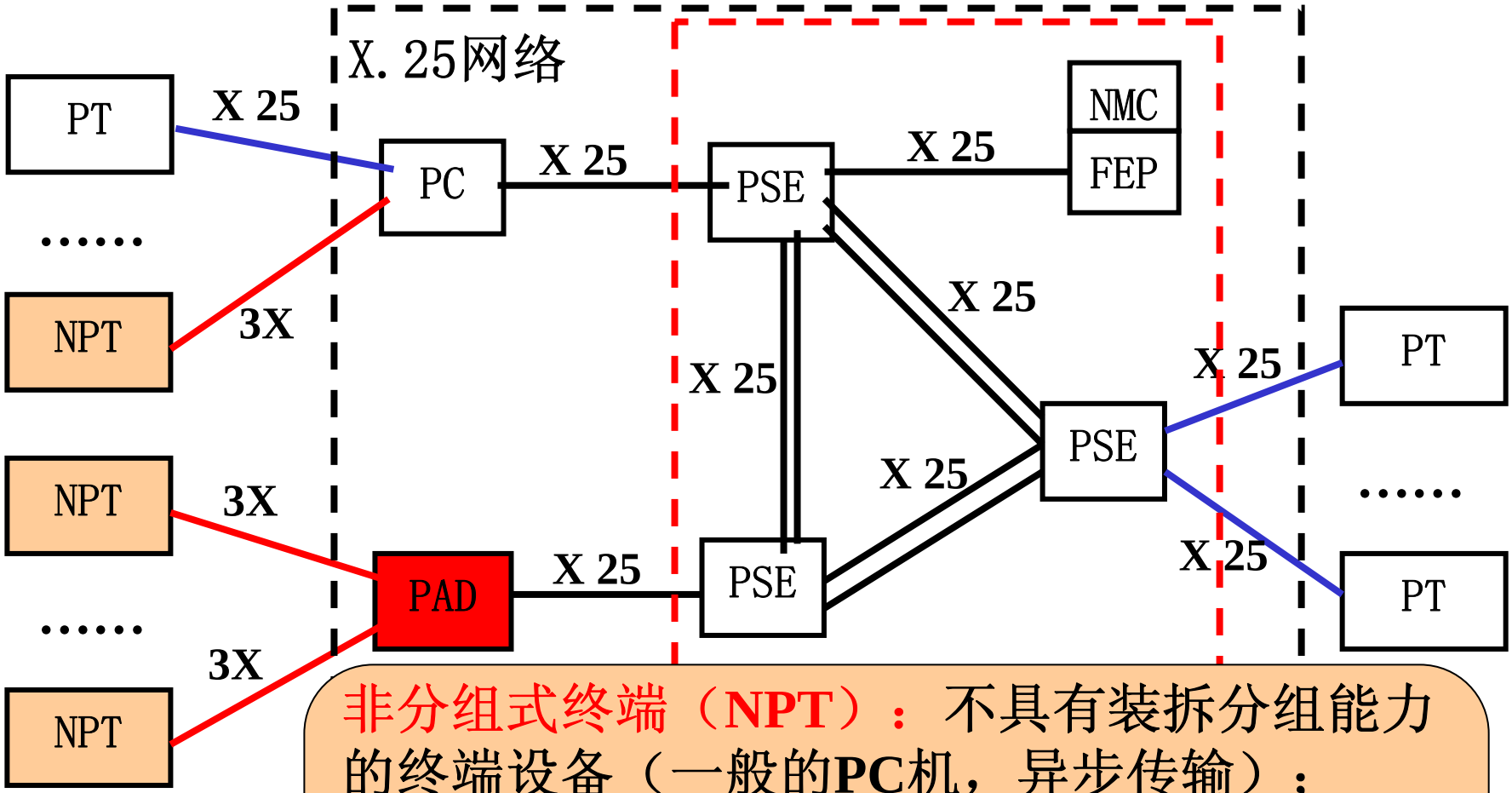


分组式终端（PT）：本身具有装拆分组能力的终端设备（一般主机，同步传输）。

PT—分组终端，N　　9建议；
PSE—分组交换设　　组集中器，
PAD—分组装拆设

红线—异步接入，　兰线—同步接入。

X.25网络结构示意图



PT—分组终端

PSE—分组交

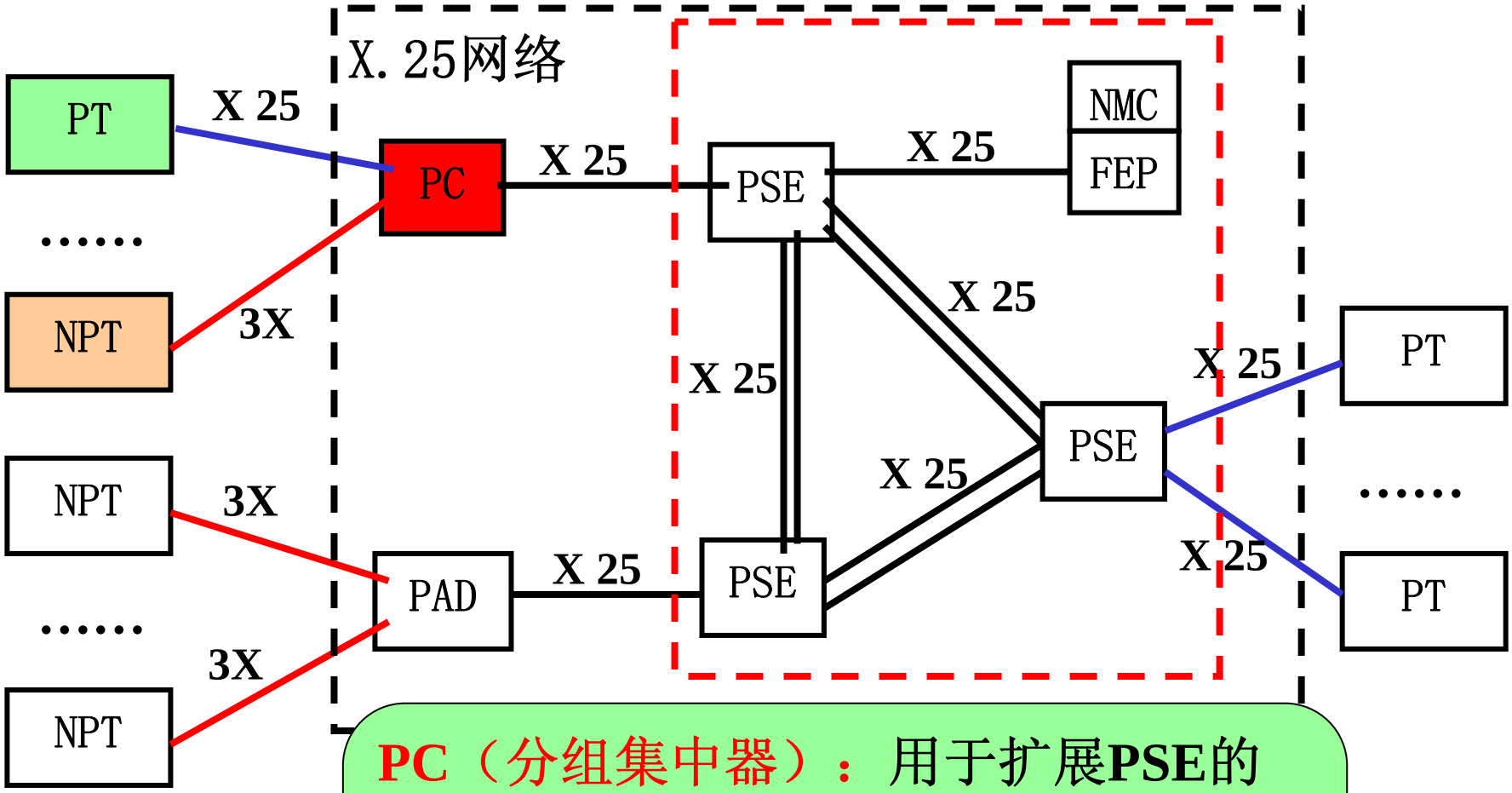
PAD—分组装

红线—异步接

非分组式终端（NPT）：不具有装拆分组能力的终端设备（一般的**PC**机，异步传输）；

PAD（分组装拆设施）：为非分组式用户终端提供接入**PSDN**的能力。将来自于**NPT**的字符流封装成分组，传输给**PSE**，或者将来自于**PSE**的分组拆封成字符流，并传输给**NPT**;

X.25网络结构示意图



PT—分组终端，

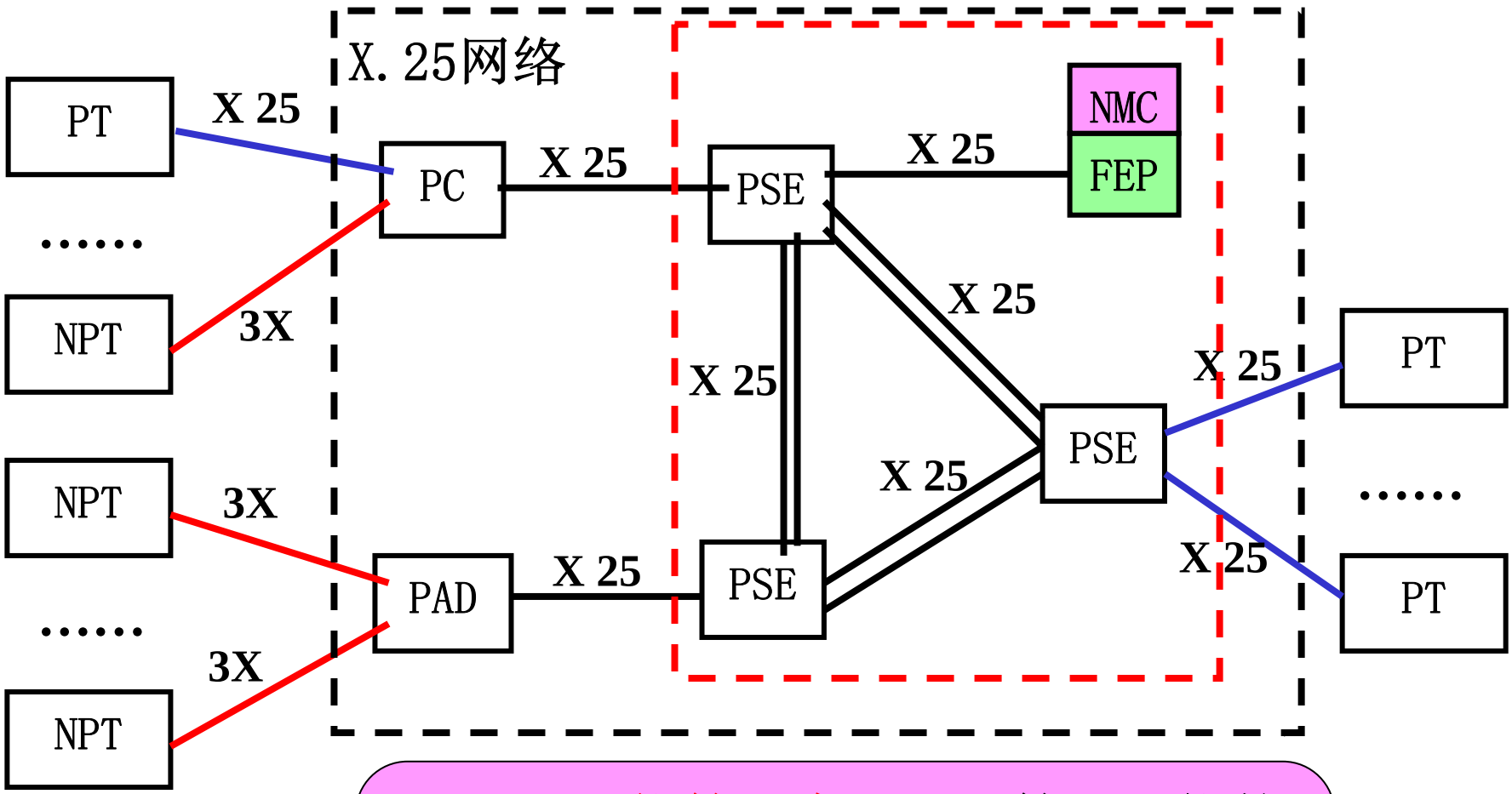
PSE—分组交换

PAD—分组装拆

红线—异步接入

PC（分组集中器）：用于扩展**PSE**的**X.25**端口，将来自于多个分组式或者非分组式用户终端设备的信息流合并为一个**X.25**分组流送往**PSE**。

X.25网络结构示意图



PT—分组终端，

PSE—分组交换

PAD—分组装拆

器，

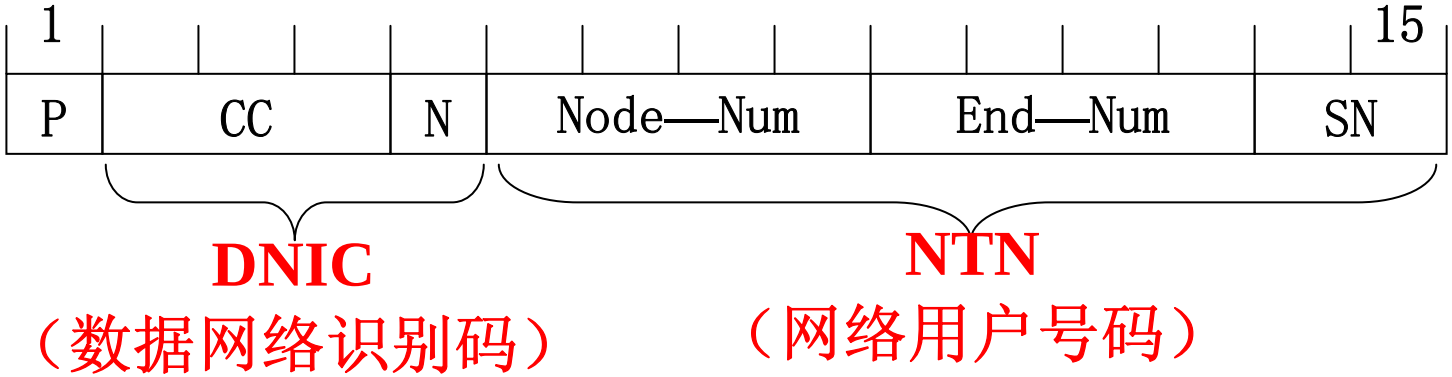
红线—异步接入，

NMC（网络管理中心）：管理网络的运行，包括性能管理、故障检测、差错恢复、用户入网登记及计费等。

NMC一般通过前置机接入X25网络

5.3.2 分组交换数据网的编址方式

网络地址标识附接网络的设备，遵循CCITT X121建议，地址空间不大于40位十进制数表示（目前采用15位）：



P：国际前缀，目前取‘0’；

CC：国家代码，中国460—479，目前取460；

N：国内网络代码，全国统一分配编号，目前取3；

Node-Num：结点机编号，网络管理员分配值；

End-Num：结点机端口号，根据结点机端口数编号；

SN：子地址（供用户自配结点机）

5.3.4 X.25网络实例—CHINAPAC

CHINAPAC（国家公共数据网）1989年开通，94年二期工程，覆盖全国各省会城市和直辖市，通过省网辐射全国，主干速率2M。

（1）特点

★ 遵循OSI下三层标准，提供永久/交换虚电路（PVC/SVC）；

★结点具有存储一转发功能，不同速率的终端可以相互通信；

★PC采用动态复用技术，提高信道利用率，简化物理接口；

★采用虚电路或数据报的方式进行分组传输。

（2）缺点

模拟信道，端口速率低（<=64Kbps），数据传输时延较大。

（3）发展现状及未来发展

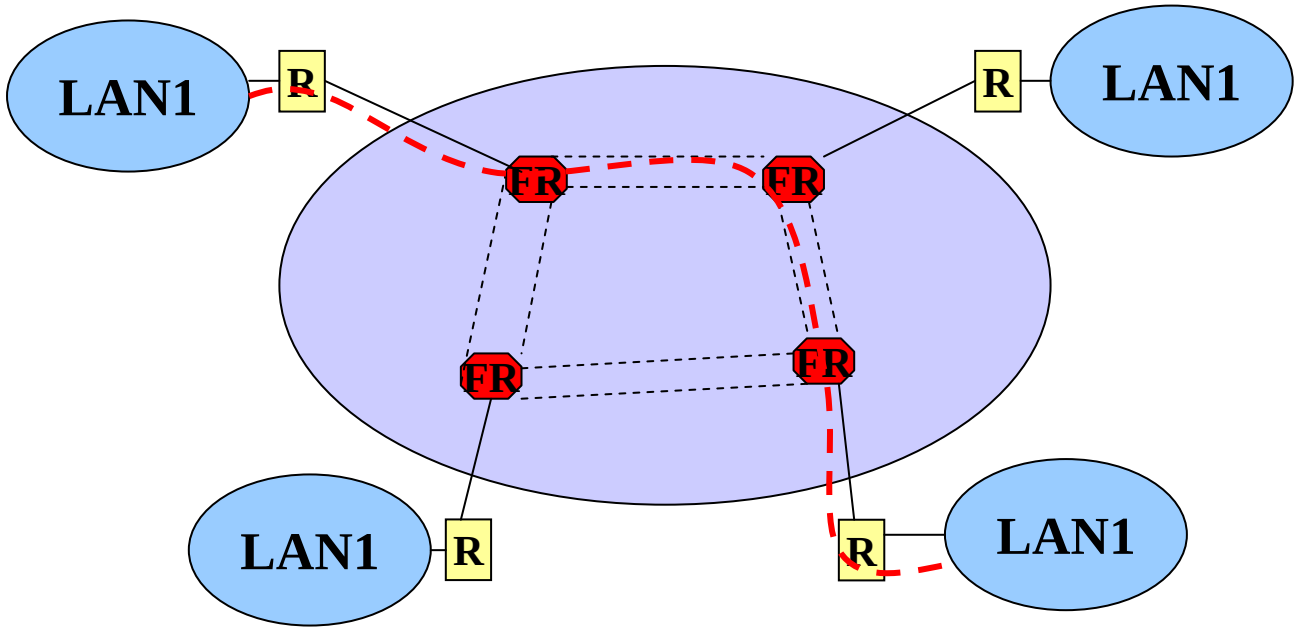
★ 技术规程完备，但因速率较低，逐渐被用户遗忘；

★ 有时被推荐为应用系统的备用方案。

5.4 帧中继网络（Frame Relay）

（1） 帧中继的提出

依据：高质量传输媒体应用，传输差错率下降，简化差错处理；
LAN应用促使LAN-WAN-LAN连通，帧通过WAN进行中继。



5.4 帧中继网络

（2） 帧中继的特点—精简X25协议

★ 采用光纤等高质量传输媒体，提高速率和降低误码率；

★ 分组重发、流量控制、防止拥塞（正向拥塞通知，反向拥塞通知，丢失指示等）等处理由端系统完成，降低网络时延；

★ 将路由选径和简化的2层功能进行集成，提高协议效率；

★ 保持X25永久虚电路特性，提供虚拟专线服务，减少用户成本；

★ 支持按需分配带宽，在“承诺信息速率”的基础上，支持突发性数据量“瞬时”超标；

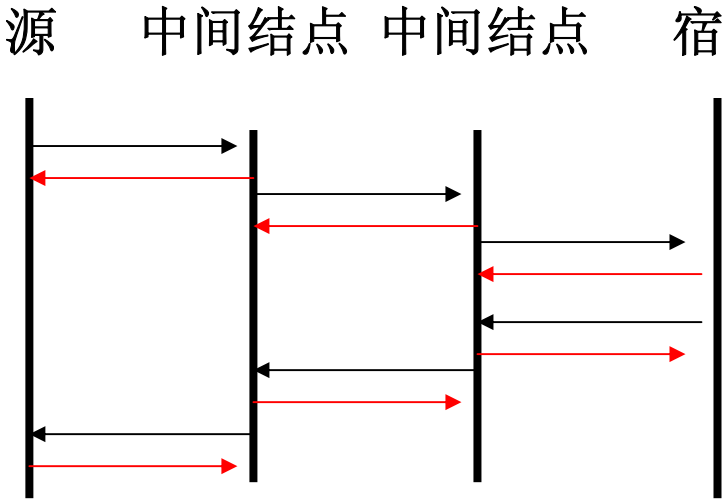
★ 保持网络概念，减少专线方式所需的用户接入线，一条物理连接能够提供多个逻辑连接。

X25和FR在传输数据过程中的比较

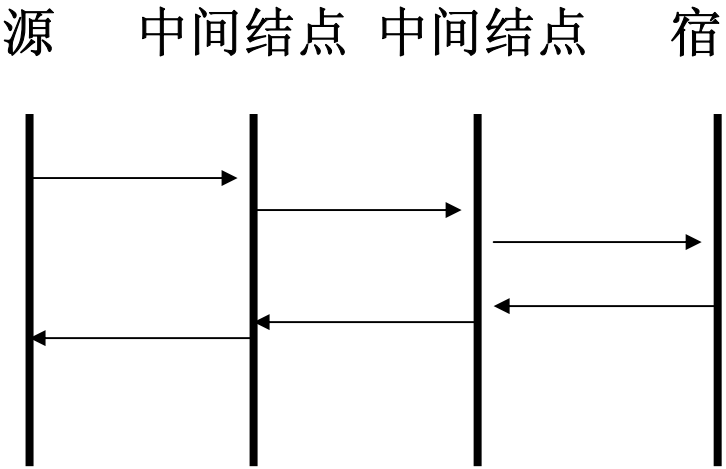
X25网络的中间结点参与帧确认过程，保证数据传输可靠性；

帧中继不提供逐段链路控制能力，由用户来保证端到端的确认；充分利用传输媒体的质量和用户端主机的处理资源。

X25网络的存储—转发

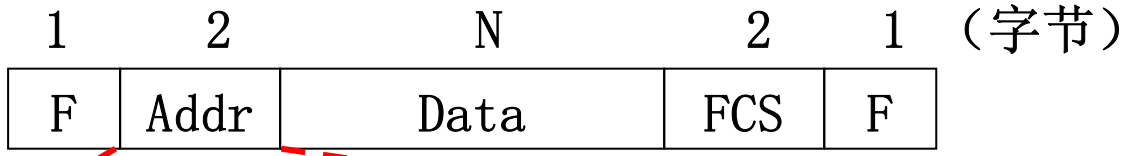


FR网络的帧传输

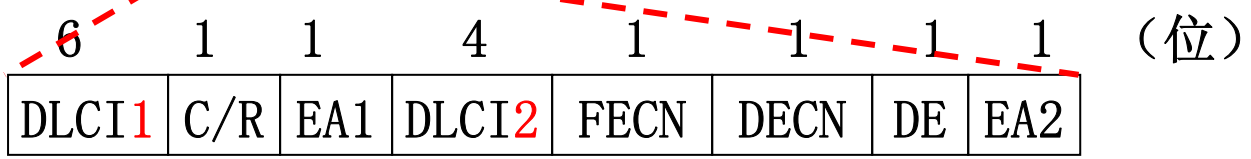


（3） 帧中继的协议和原理

帧一般格式：



Addr的格式：



F—帧间隔符（01111110），FCS—冗余校验，

DLCI（1+2）—链路标识；0—呼叫信令，1-15—保留，

16-1007—链路号，1008-1022—用户定义，1023—管理帧。

C/R—命令/响应（上层确定含意）；

EA—地址扩展位（0—有后续，1—无后续）；

FECN/DECN—正向/反向拥塞指示（中间交换设备设置），

DE—容许丢失指示（1—低优先级，可丢）。

帧中继工作过程

通过呼叫信令（DLCI=0，Data中携带对方地址信息），建立与对方的联系，获得可用的链路号（DLCI）；

利用已建的链路，传输数据；

根据链路的拥塞情况，交换机设置FECN和DECN，通知发送方调整流量；

如果帧故障（差错或者链路号不正确），丢弃该帧；

用户端自行设计应答和超时重传的处理动作；

传输完毕，终止联系。

(4) FR的应用现状

FR和DDN的比较：

DDN：采用复用技术的逻辑数字专线，多端口接入；

FR：具有路由交换功能的数字网络，单端口接入。

帧中继标准已渐成熟，应用需求不断增加，已进入高速发展时期。

帧中继一般在DDN网上配置端口实现，方便用户接入，并降低端口数，减少成本（租金约为DDN线路的1/4）。

目前大多数业务都集中在2Mbps之内，是FR业务的最经济有效的范畴，具有市场发展潜力。

现状：目前企业广域互连的主角。

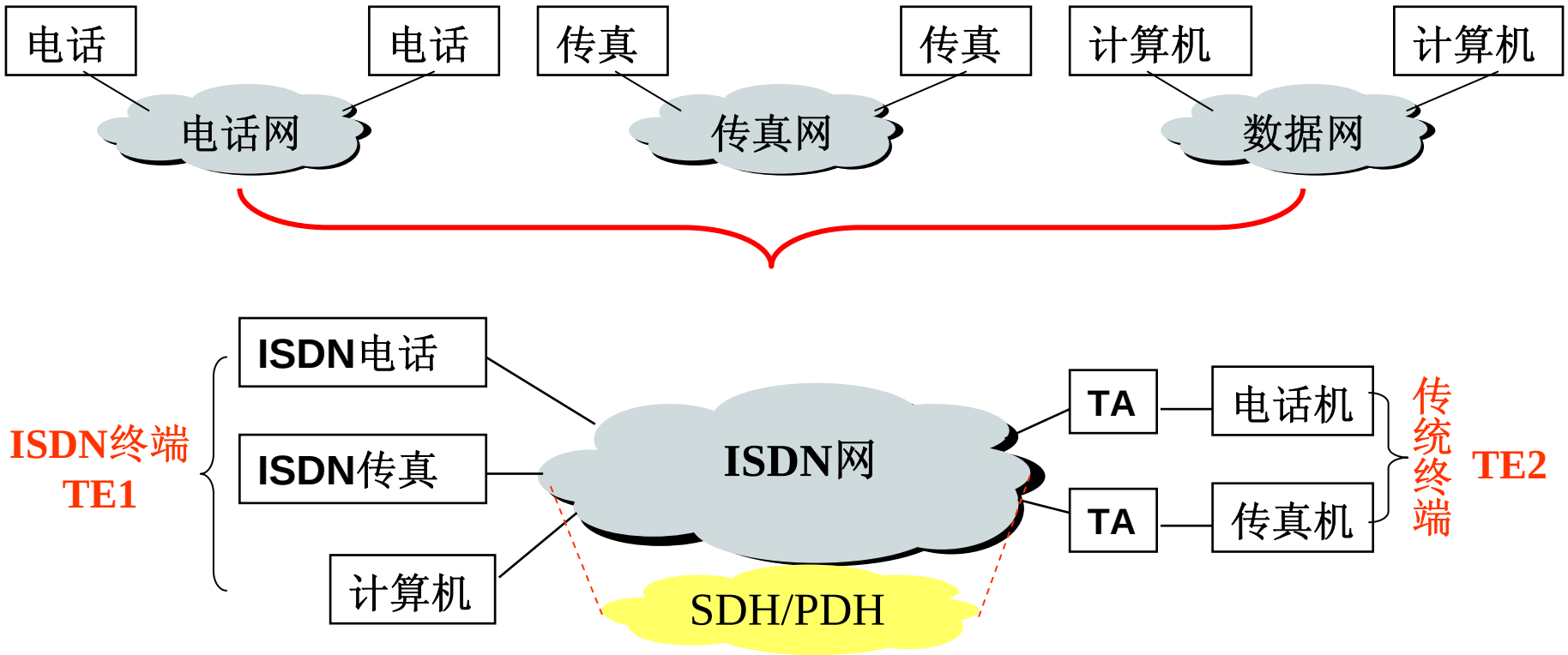
部分DDN业务，实际上已由帧中继替代。

5.5 ISDN（综合业务数据网络）

（1） ISDN的目标

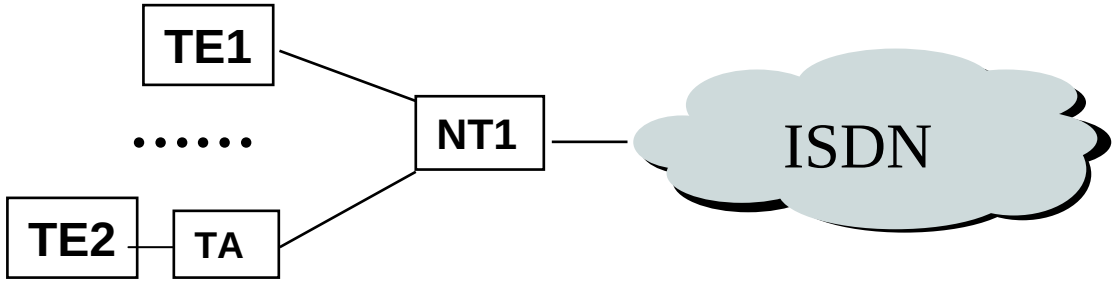
集电话、电报、传真、数据通信为一体，以数字化技术统一处理各种公用网的业务，为用户提供“一线通”服务；

用户线保持双绞线，数字化客户端，使用T或者E载波系统；

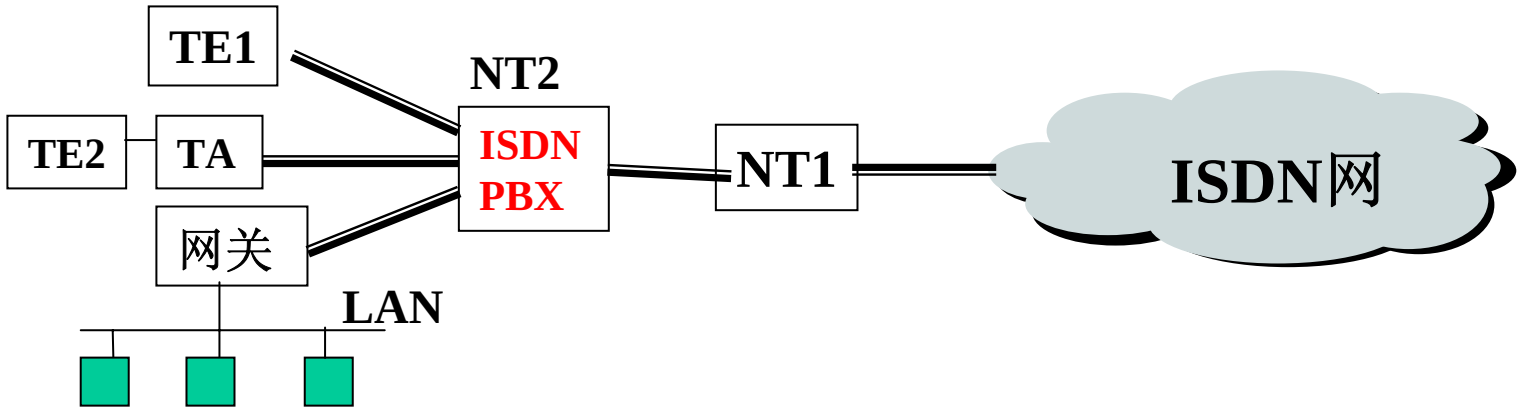


（2） ISDN用户接入

1型端接设备（NT1）接入：设备数<=8，一线通方式，适用于家庭或小企业。



2型端接设备（NT2）接入：通过专用IDSN交换机（NT2），附接更多的用户设备，适合一般企业。



（3） ISDN网络的接入速率

★*基本速率接口（BRI）：*

两个B通路和一个D通路（2B＋D），通常速率为144 Kbps。

两条64 Kbps的B通路，支持话音和数据传输，

一条16 Kbps的D通道，传输控制信号和数据，全双工通道。

适用于家庭或小单位，可以通过BRI接口传送语音、数据、传真及一般质量的图像，可传输可视电话、电视会议。至少可使三个一般的终端同时在2B＋D的信道上传输数据。

★*一次群速率接口（PRI）：*

T1系统（1.544Mbps）： 美国、日本等国采用23个64 Kbps的B通路和1个64 Kbps的D通路的速率接口（23B＋D）。

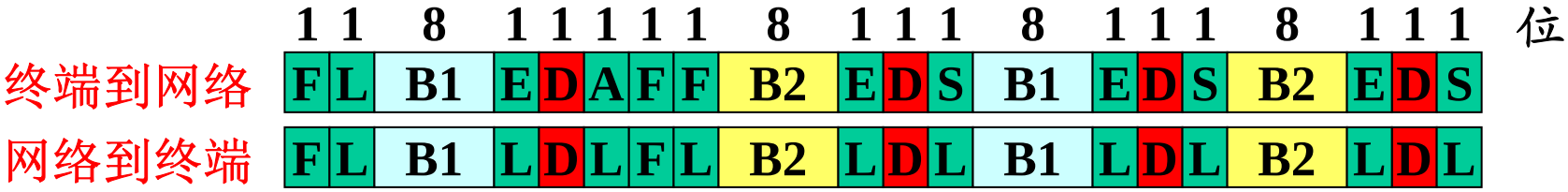
E1系统（2.048Mbps）： 欧洲国家采用的是30个64 Kbps的B通路和1个64 Kbps的D通路的速率接口（30B＋D）；

E1帧中另外8位用于其他控制信息（类似BRI）。

适用于单位接入。

（4） BRI（Basic Rate Interface）复用方式

帧结构（48位）：B1（16位）、B2（16位）和D（4位）；



F-帧标志；L-负载平衡；E-回应；S-备用；A-设备激活；B-B通道；D-D通道

BRI帧的传输频度为每秒4000帧（或帧/250us）；

线路传输速率：192Kbps （48位/帧×4000帧/秒）。

其中：B信道速率：64Kbps（16位/帧×4000帧/秒）；

D信道速率：16Kbps（4位/帧×4000帧/秒）；

即：ISDN的用户数据传输速率：144Kbps（2*64+16）。

（5） 宽带综合业务数字网（B-ISDN）

应用需求：

★ 64Kbps的基准速率无法提供令人满意的服务；

★ 新的数字化编码，语音传输无需64Kbps的带宽；

★ 更多的应用期待更高的带宽，如视频点播、现场转播、全动画邮件、局域网互连、高速数据传输等。

引入宽带ISDN（B-ISDN）：支持实时的应用，也可提供可靠的数据传输业务。

N-ISDN和B-ISDN的比较：

	N—ISDN	**B—ISDN**
长途干线	光缆或双绞线	光缆
用户环线	双绞线	光缆
通道速率	固定速率（**64Kbps**）	速率可变
应用范围	数字化语音为主	多媒体信息

B-ISDN采用另一种传输技术—异步传输模式（ATM）。

ATM—Asynchronous Transfer Mode

5.6 异步传输模式（ATM）

ATM：为满足多媒体传输的要求而出现的一种通信技术。

★数据传输的特点：允许延时，但不能有差错，数据的差错将导致数据含义的不同，引起错误的结果；

★语音传输的特点： 具有固定速率的实时性要求，且允许少量差错，差错只能影响当时的语音质量；

★图象传输的特点： 信息量大，实时性高，允许少量差错，差错只能影响当时的图象质量。

★一般的高速网技术在支持这些应用的不足：

高速以太网（100Mbps）在高负载时的实时传输能力和传输距离有限（LAN）；

FDDI（100Mbps），具有定时传输的优点，但令牌处理和传递占用了宝贵的时间，统计延时为10～200ms。

5.6.2 ATM交换的概念

（1） ATM交换

★同步传输：字符间隔固定，同步模式界定数据块（帧）传输；
★异步传输：字符间隔任意，字符内的起止位界定字符；

★同步多路复用（同步传输模式—STM）：
静态分配子信道（频段、时间片和波长），可能浪费带宽；
★异步多路复用（异步传输模式—ATM）：
按需分配子信道—提高信道的利用率；
为合理使用信道和提高实用性，可增加优先级和排队规则；

★ATM交换：依据异步传输和异步多路复用的原理，交换的对象为53字节的信元(cell)，信元头携带寻址信息，ATM交换机根据输入端口的各个信元的信元头中的信息将信元“交换”到指定的输出端口。

（2） ATM交换的优点

★ 使用固定长度（53字节）的信元作为传输的基本单元，可以简化ATM交换机的处理；

★ 允许混合使用多种高质量的传输媒体（双绞线、同轴电缆和单模/多模光纤），并且可以支持不同的传输速率（25Mbps、45Mbps、155Mbps...、625Mbps）；

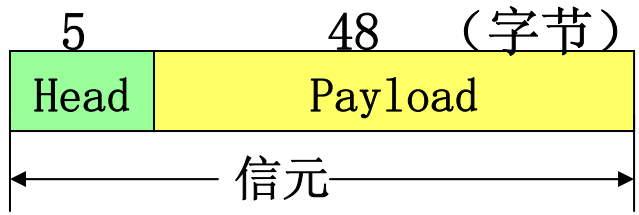
★ 高质量的传输媒体可以使得ATM网络简化差错控制和流量控制的处理，从而提高网络（或者ATM交换机）的吞吐率。

★ ATM网络可以同时支持数据、数字化语音/图象的传输，支持多媒体传输的应用，不同的应用需求具有不同的处理策略。

★ 引入资源预留机制，支持高实时性的应用要求；

★ ATM技术可用于组建各种规模的网络。

5.6.3 ATM的特征



（1） 基于信元的分组交换技术

信元具有固定的长度和格式：

信元头（5字节）：信元穿越网络的路由控制信息等；

数据域—有效载荷（ 48字节）：携带高层数据。

（2） 采用快速交换技术（电路交换和分组交换相结合）

— 直接交换技术，输入端口信元直接交换到输出端口，交换机本身不执行差错控制和流量控制，减少结点处理延时；

— 信元交换的过程，硬件支持，减少交换延时，保证信元在ATM交换机中“逗留”的时间不会超过100us。

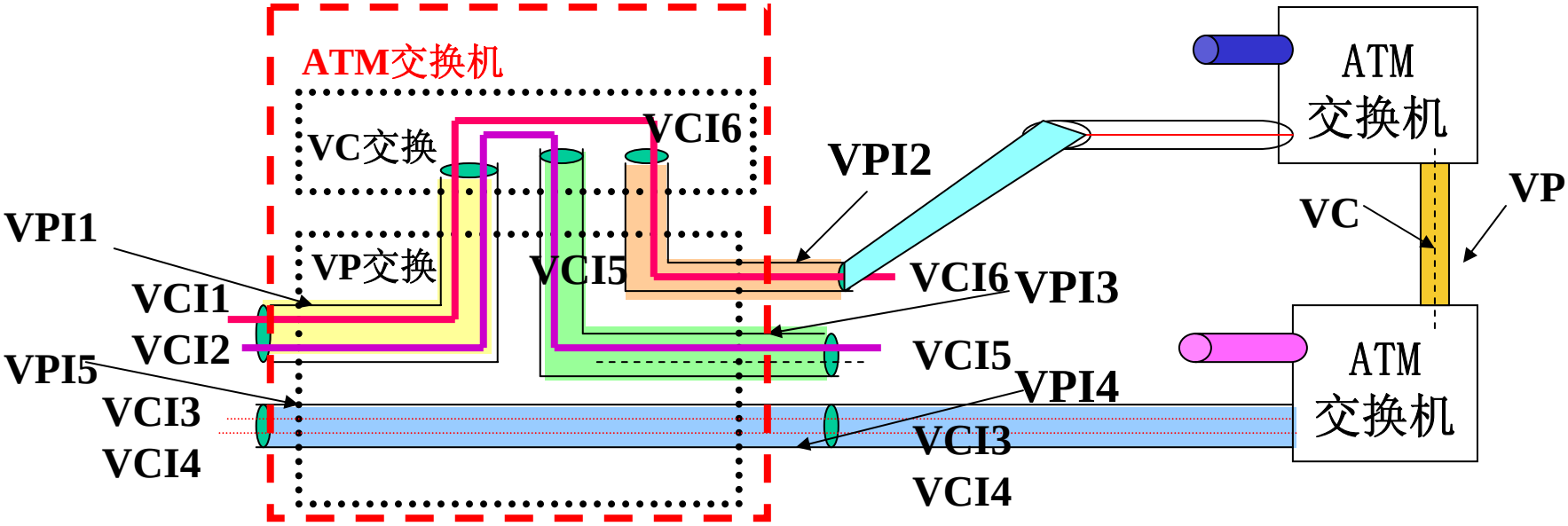
（3） 采用面向连接的信元交换

★面向连接：数据信元交换之前必须建立虚拟连接；

★物理链路逻辑上被分为多条虚拟路径（VP—VPI），VP又被划分为多条虚拟通道（VC—VCI），VPI和VCI的组合（VPI/VCI）及映射唯一地标识了一条虚拟连接；

VP可对应交换机端口和端口的线路，VC对应其中的逻辑信道；

★信元交换基于已建的虚拟连接。



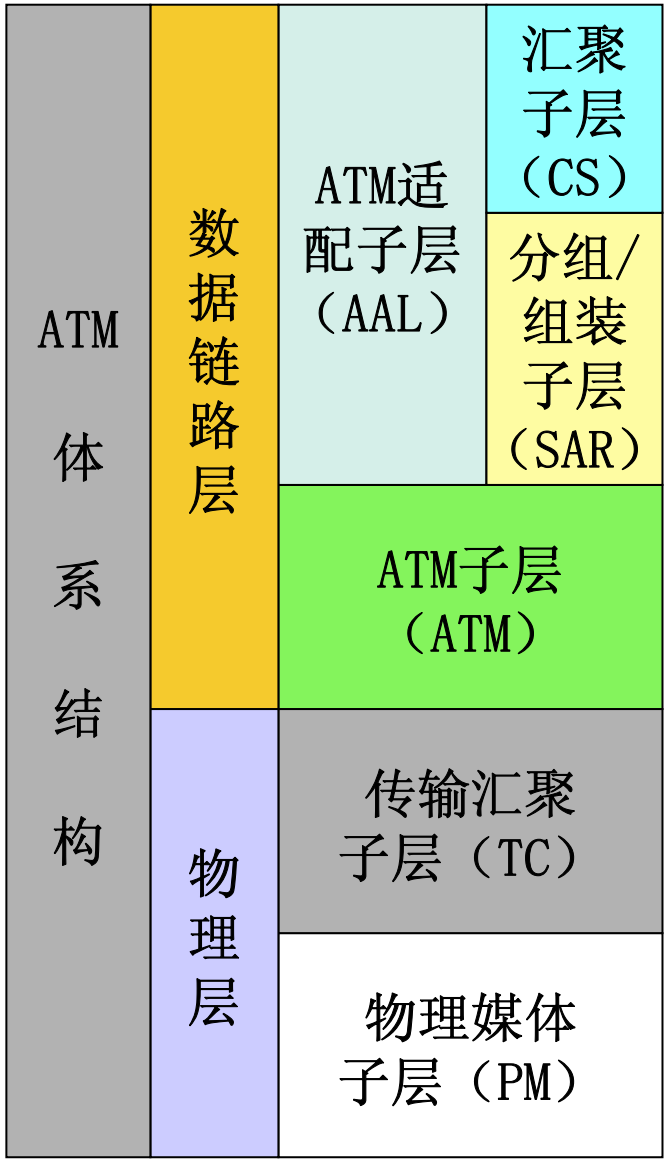
（4） 提供预约带宽机制

★ 在虚拟连接建立时，ATM允许根据应用的需求，进行带宽预约，支持不同的应用，以确保在规定的时间内完成数据信元的传输。

★不同的用户数据分配不同的优先级别，当交换机内部出现信元排队时，高优先级的数据可以优先交换。

★当网络出现拥塞时，低优先级的信元可以被“优先”丢弃。

5.6.4 ATM体系结构



高层数据预处理；

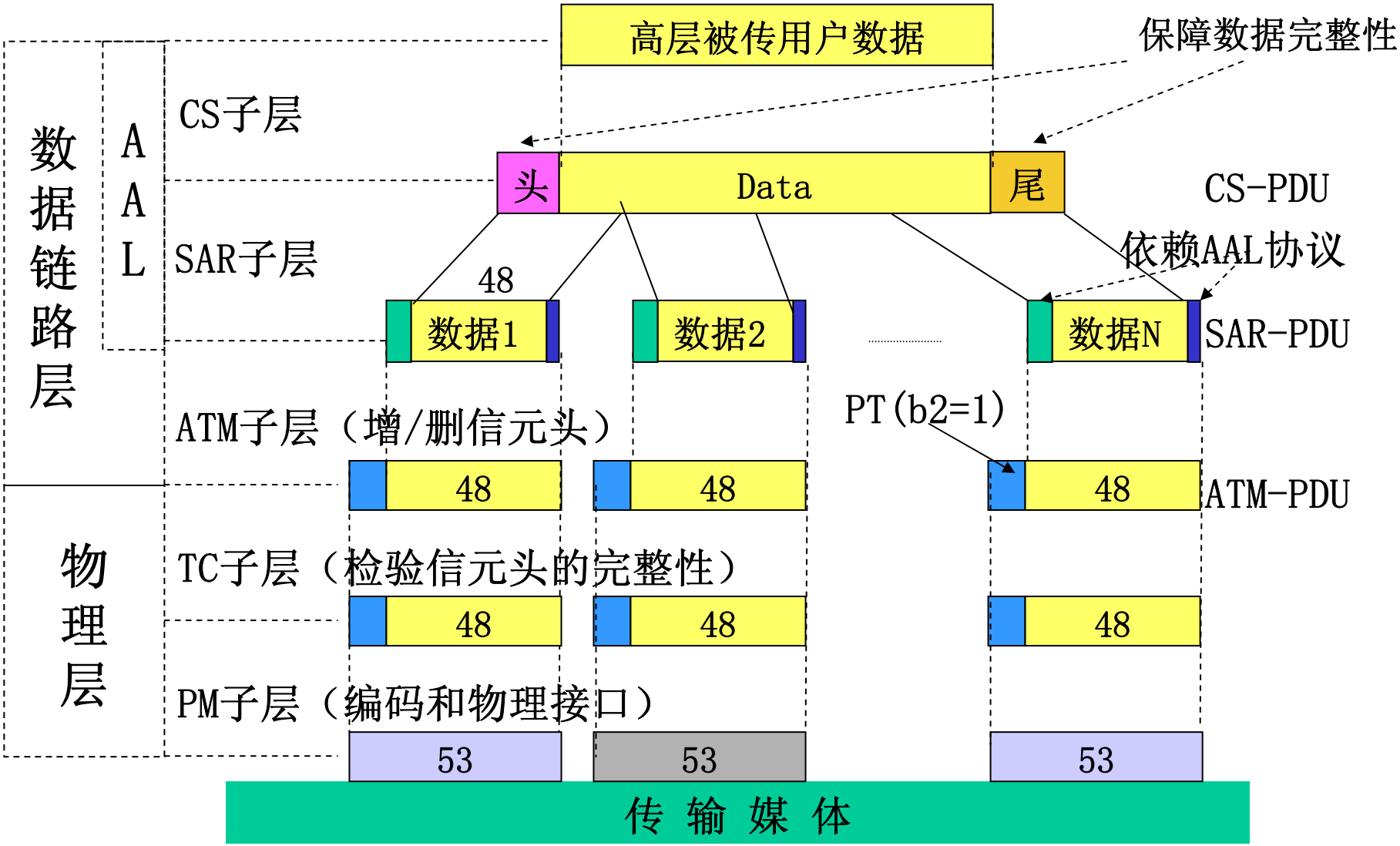
对应不同的应用，选择协议，组成协议体；

对应虚拟连接，增加/修改信元头，形成信元；

信元/位流转换、信元头校验；

媒体/设备接口、编码、位流传递；

层次及其信元的关系

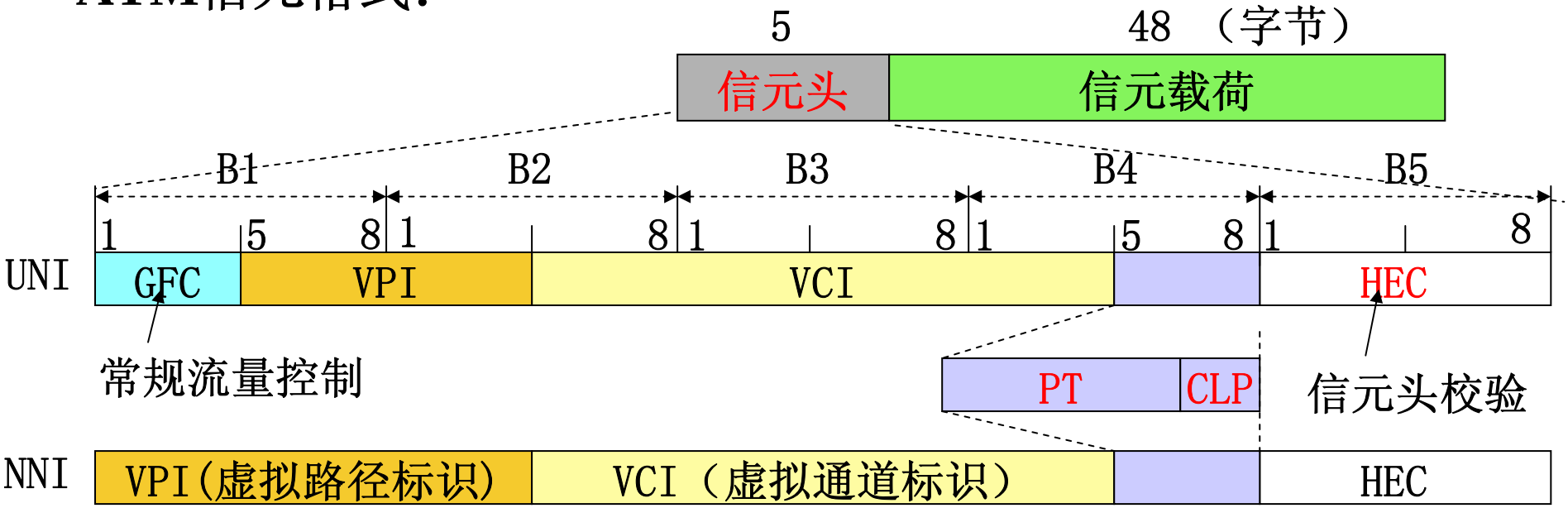


接口方式：

ATM接口和信元格式：

接口方式：

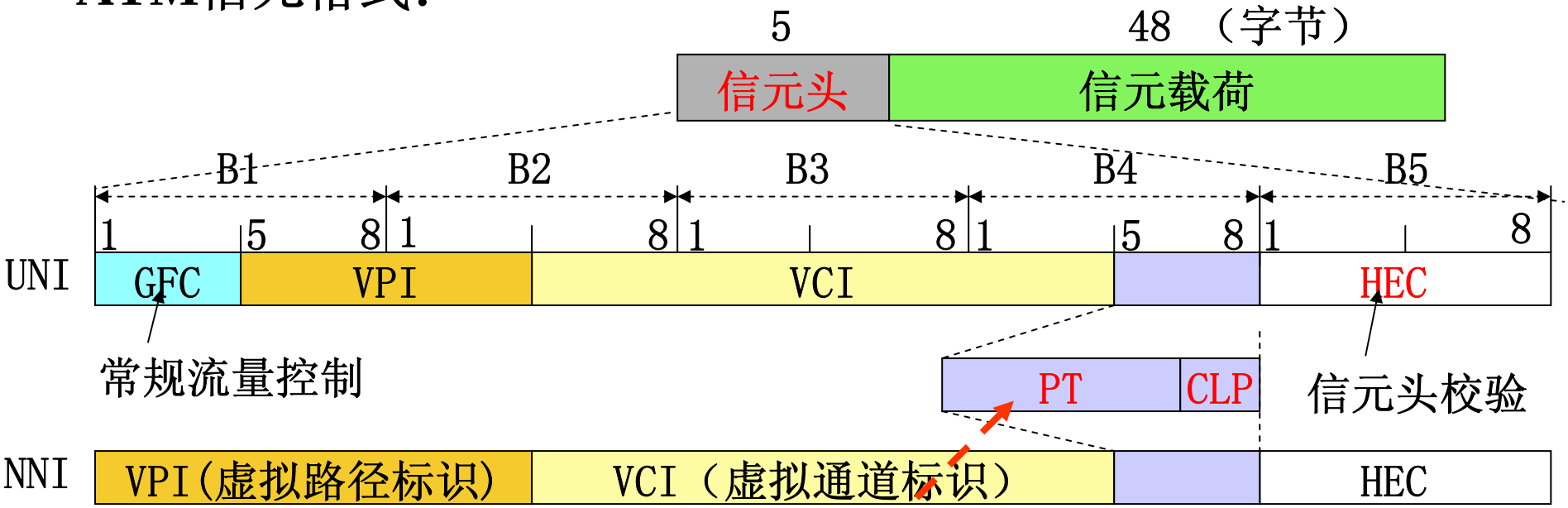
ATM信元格式：



ATM接口和信元格式：

接口方式：

ATM信元格式：



PT（信元负载类型—3位）：

b5=0（用户信息） **b6**：拥塞指示，由交换机根据当前状况设置；

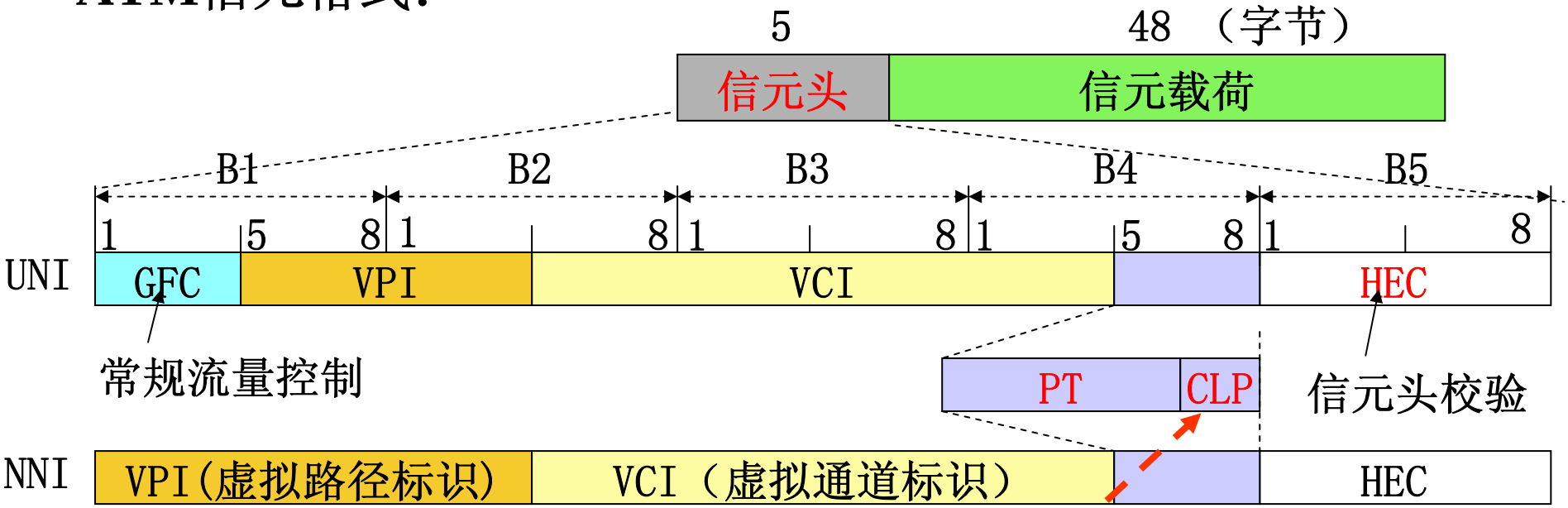
b7：后继信元标识，1—整个CS-PDU的最后一个信元。

b5=1（管理信息） **b6=0**：操作管理信息；**b6=1**：资源管理信息。

ATM接口和信元格式：

接口方式：

ATM信元格式：

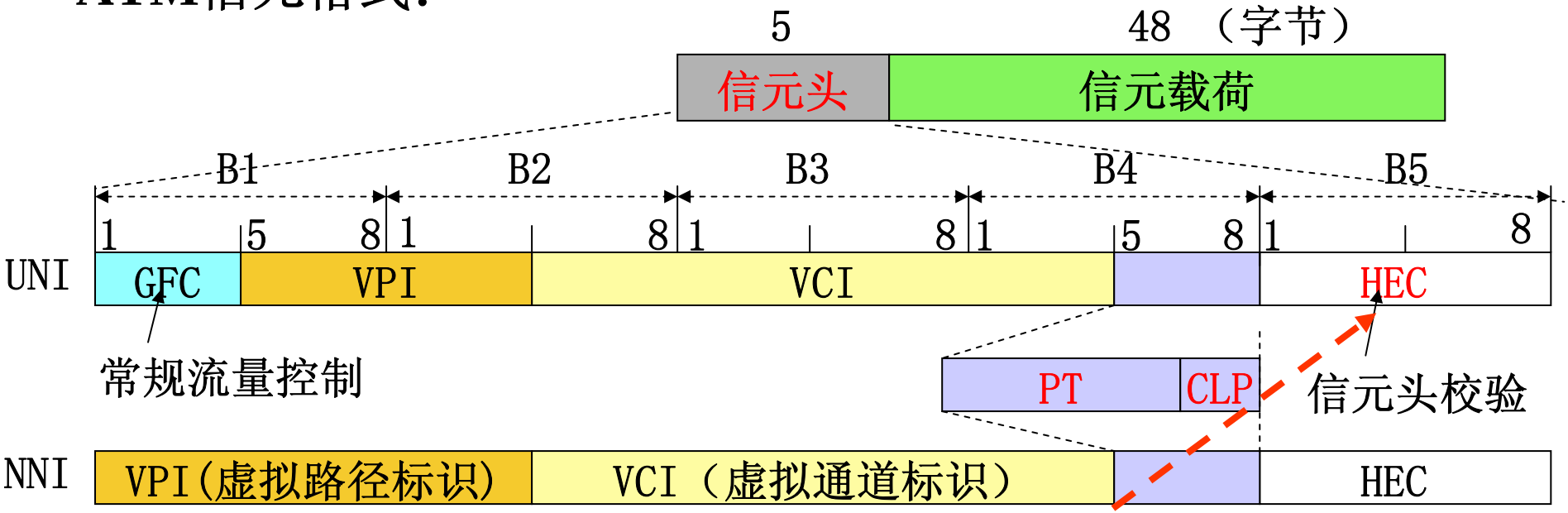


CLP（信元优先级—1位）：**0**—优先传输，**1**—优先丢弃；

ATM接口和信元格式：

接口方式：

ATM信元格式：



HEC（信元头校验）：海明码 或者 g(x)=x8+x2+x+1。

海明码（Hamming Code）补充：— 可纠一位错（源于偶校验）

规则：　$2^r \geqslant k$(信息位数）+ r(校验位数）+ 1；

例：k=4，则满足上式的r应大于等于3（取3）；

对应码字：S（S1S2S3）= b1b2b3b4b5b6b7；因为：2^3=8；

设：S = 0（正确编码），S = 其他（Si=1,编码错误）

S1S2S3	000	001	010	100	011	101	110	111
错码位置	无错	b7	b6	b5	b4	b3	b2	b1

** S1=b5+b3+b2+b1; S2=b6+b4+b2+b1; S3=b7+b4+b3+b1

令S1=S2=S3=0，有：b5=b3+b2+b1；b6=b4+b2+b1；b7=b4+b3+b1；

可得海明码：

b1b2b3b4: 0000 0001 0010 0011 0100 0101 0110 0111 …

b5b6b7 : 000 011 101 110 110 101 011 000 …

若：收0001110，代入**，有S1=1,S2=0,S3=1,纠b3错。

类似有：32位的信元头有效位的校验需6位的HEC。

5.6.5 ATM物理层

- 物理媒体子层（PM）：主要定义物理媒体与物理设备之间的接口（包括光电转换的准则），以及线路上的传输编码，最终支持位流在媒体上的传输。
- 传输汇聚子层（TC）：主要定义控制线路的方法。

（1） 线路空闲时所用的闲置信元，用于双方TC实体保持同步；

（2）物理层操作和管理信元（PLOAM）的功能，以便对物理媒体进行性能监控、故障探测和传输差错报告等。

（3）将来自于PM子层的位流或者字节流识别为信元。

（4）提供信元头校验功能

5.6.6 ATM层

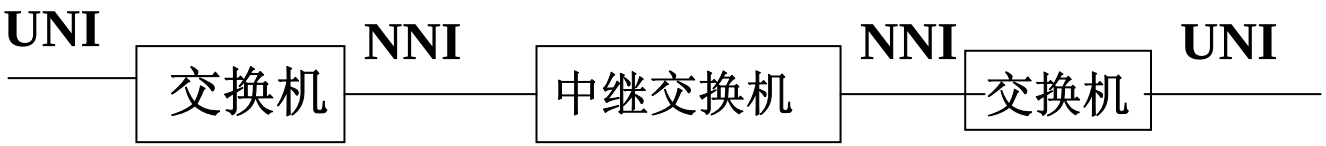
定义信元头的结构，以及使用物理链路的方法。

ATM层的功能

（1） 信元的分检：负责将输入端口的信元分检到不同的输出端口；

（2） 当多个输入端口的信元汇集到相同的输出端口时，对信元进行必要的队列处理；

（3） VPI/VCI的管理：根据VPI/VCI映射表，将输入端口来的信元中的VPI/VCI映射成输出端口对应的VPI/VCI，并填充进信元头；



经过交换机的处理，信元头的内容发生变化，需要重填写。

ATM层的功能

（4）信元头的增删：发送方增加信元头，接收方删除信元头。

（5）信元速率调整：不同的链路需要不同的信元速率

例如：SDH STM-1链路（线路速率为155.520Mbps，数据速率为150.336Mbps）每秒应传输35000多个信元；如果输入的实际信元不够时，ATM层必须生成空信元填充信道。

5.6.7 ATM适配层（AAL）

（1） 主要功能

★ 将高层的信息转换成适合ATM网络传输要求的格式；

★ 为支持多媒体的应用，定义了业务种类及支持的协议。

（2）ATM支持的业务分类

★CLASS A：支持源/宿之间具有实时要求的恒定位速率（CBR）业务，如支持恒定位速率的话音。采用面向连接的工作方式；

★CLASS B：支持源/宿间具有实时性要求的可变位速率（VBR）业务，如支持可变位速率的视频传输。采用面向连接的方式；

★CLASS C：支持源/宿之间无实时性要求的可变位速率（VBR）业务，例如：面向连接的数据传输业务，高速数据传输等；

★CLASS D：支持面向无连接的数据传输服务，例如：LAN等。

CLASS A/B支持实时信息的传输（例如：视频和话音传输）；

CLASS C/D支持非实时要求的信息传输（例如：高速数据传输）

（3） AAL协议分类：

	AAL1	AAL2	AAL3/4	AAL5
连接模式	面向连接	面向连接	面向无连接	面向连接
端端定时	要求定时	要求定时	无定时要求	无定时要求
位速率	恒定速率	可变速率	可变速率	可变速率
业务类型	**Class A**	**Class B**	**Class C/D**	**Class C/D**

标准中主要定义了AAL5，简单高效的适配层（SEAL），AAL3/4简化，可以同时支持CLASS C和CLASS D业务。

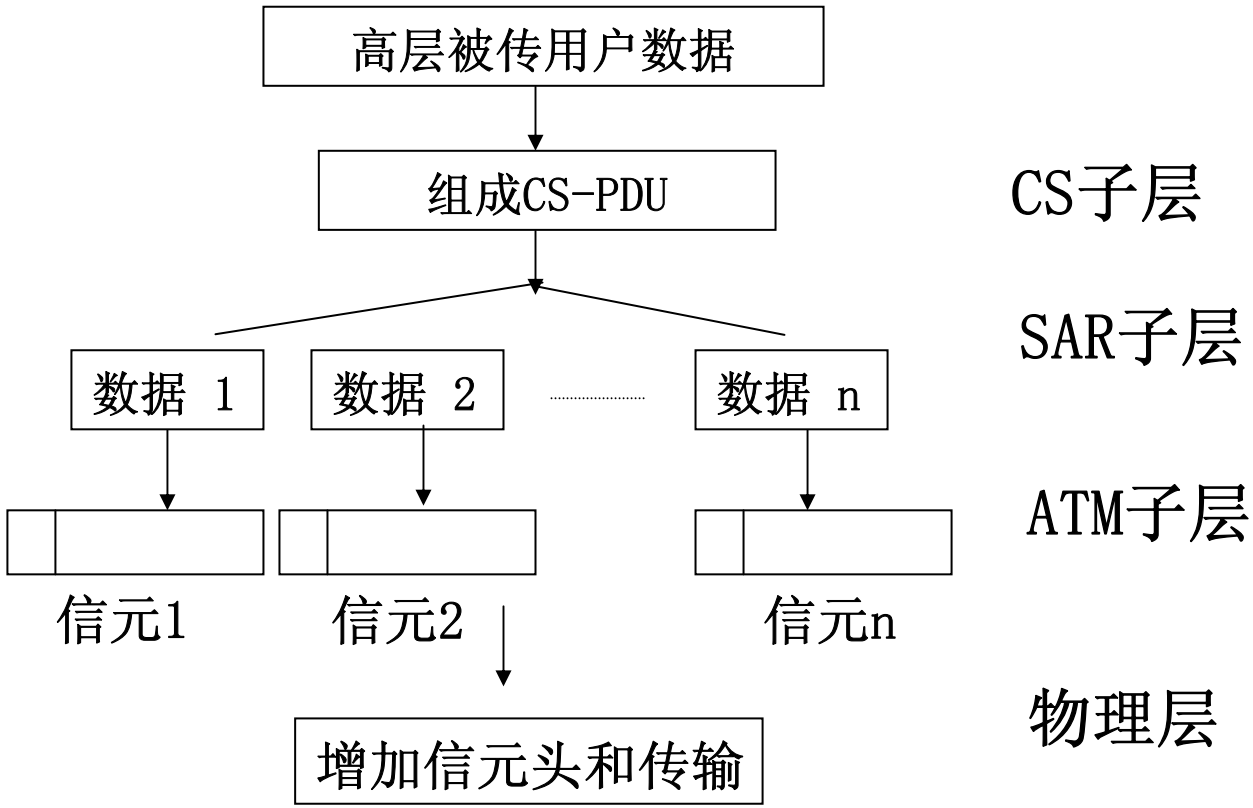
（4） 辅助说明（AAL5）队列处理：

输入的信元根据先进先出的原则在输出端口予以排队；

输出队列满时先丢弃AAL5、AAL3/4中丢弃位（优先级）置起的信元，必要时也包括该位未置起的信元；

采用快速交换机制减少队列的等待时间。

（5） AAL5的工作过程


高层被传用户数据
组成CS-PDU
数据 1
数据 2
数据 n
信元1
信元2
信元n
增加信元头和传输
CS子层
SAR子层
ATM子层
物理层

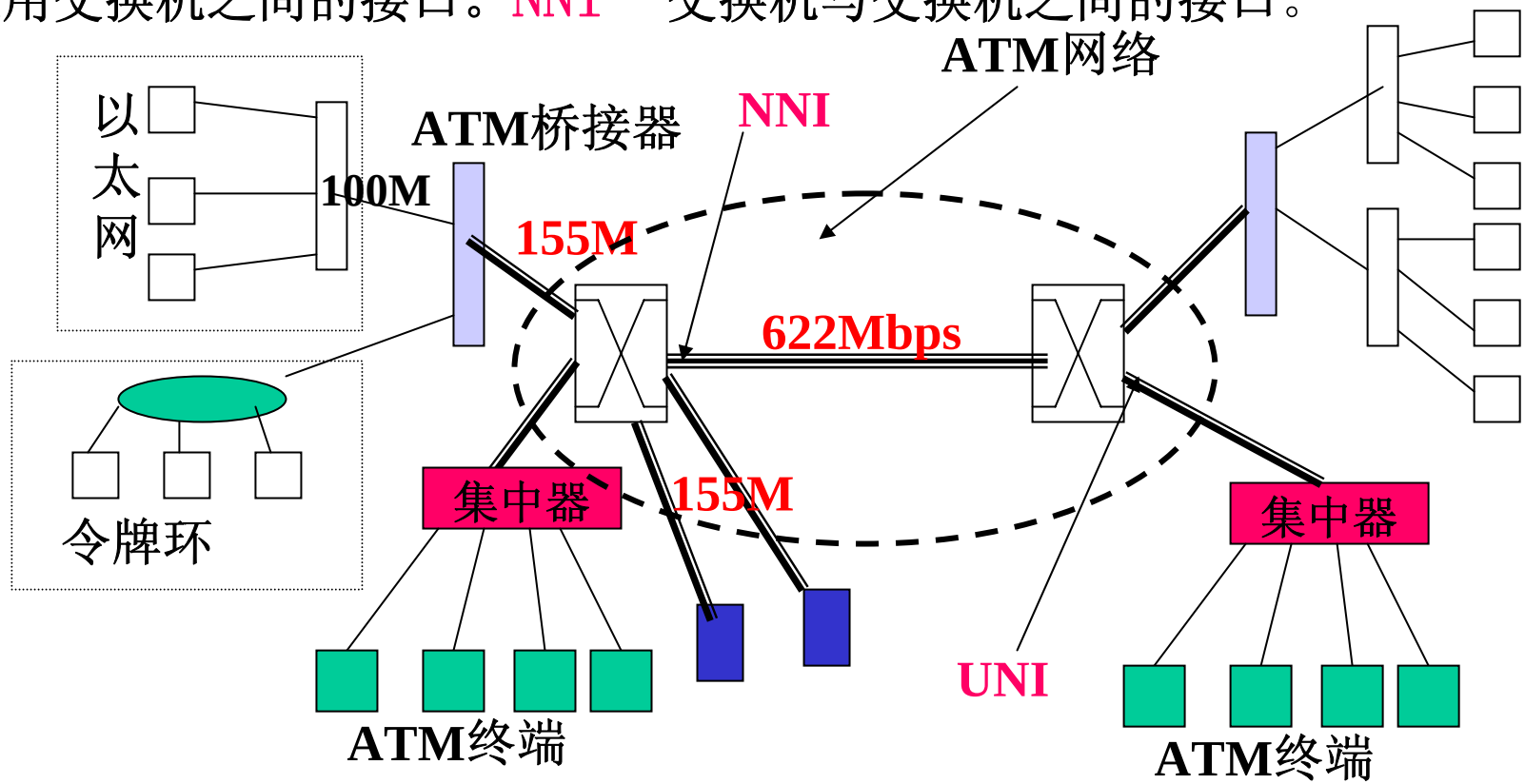
5.6.8 ATM网络

（1） 网络环境

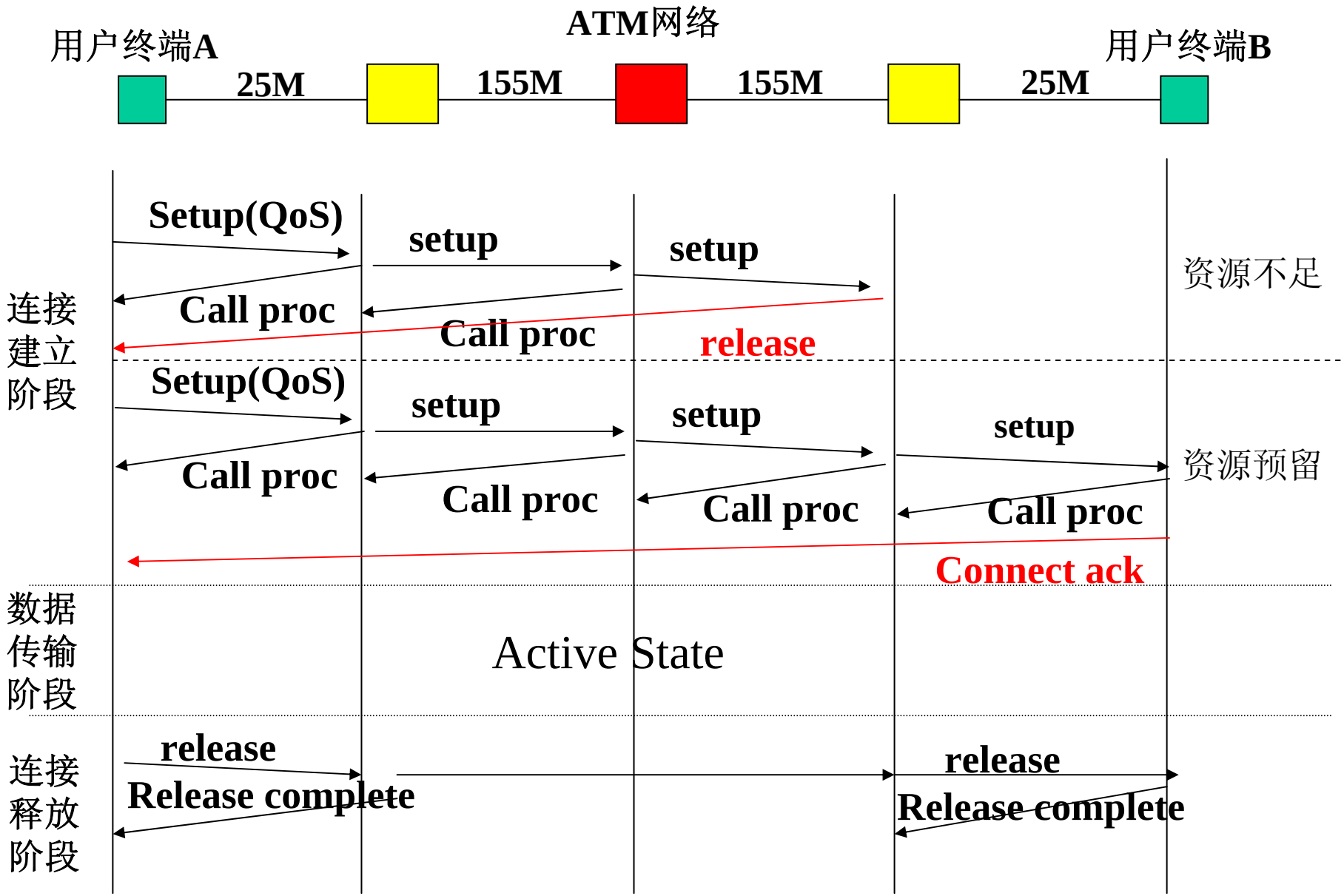
★ ATM网络：由ATM交换机和传输媒体组成；

★ ATM终端用户：ATM网络的用户设备，主机、互连设备（如路由器等），通过ATM适配卡接入ATM网络；

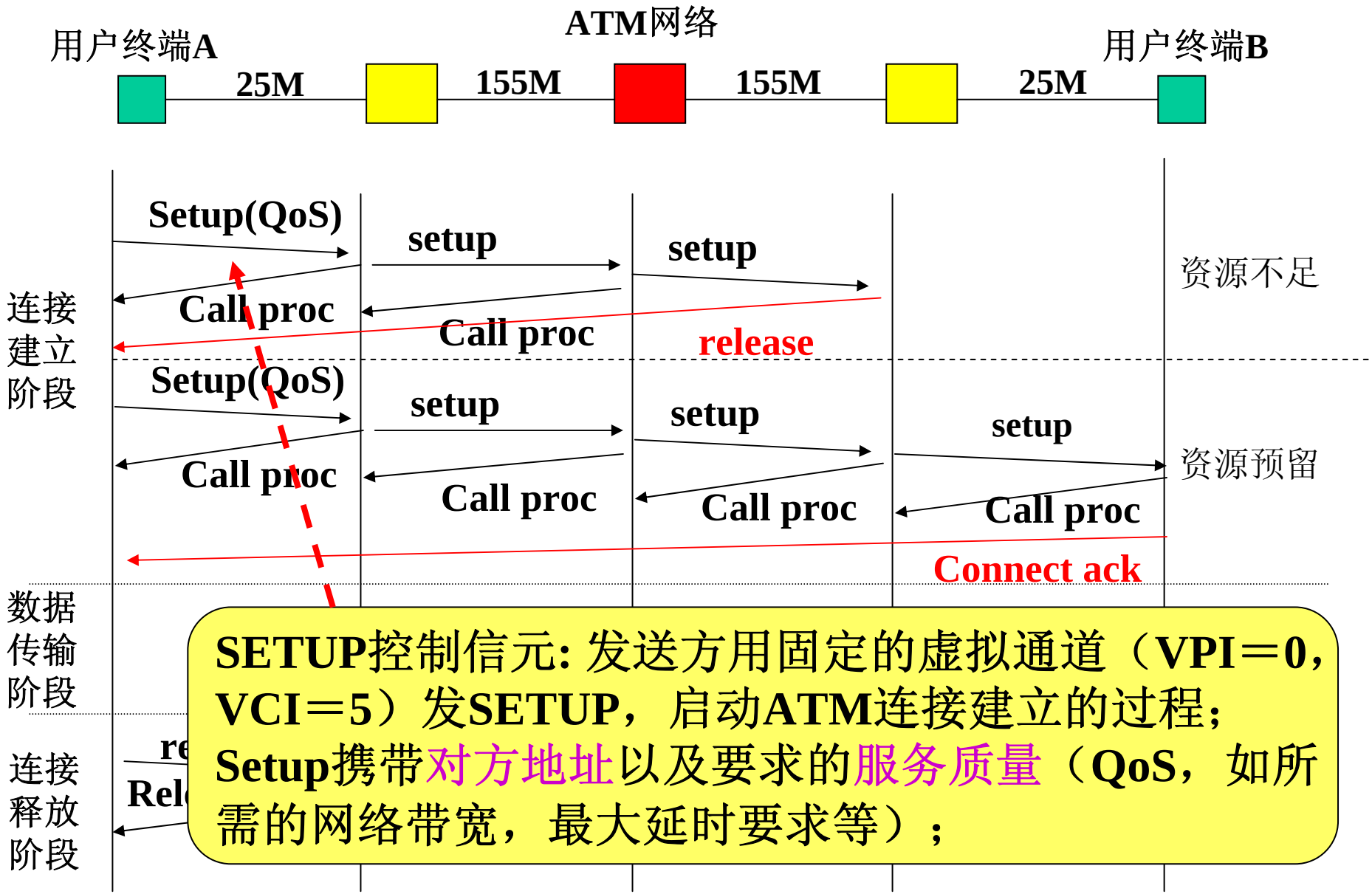
★ 接口标准：UNI—终端用户与交换机之间的接口，包括专用交换机与通用交换机之间的接口。NNI—交换机与交换机之间的接口。



（2） ATM网络的工作过程

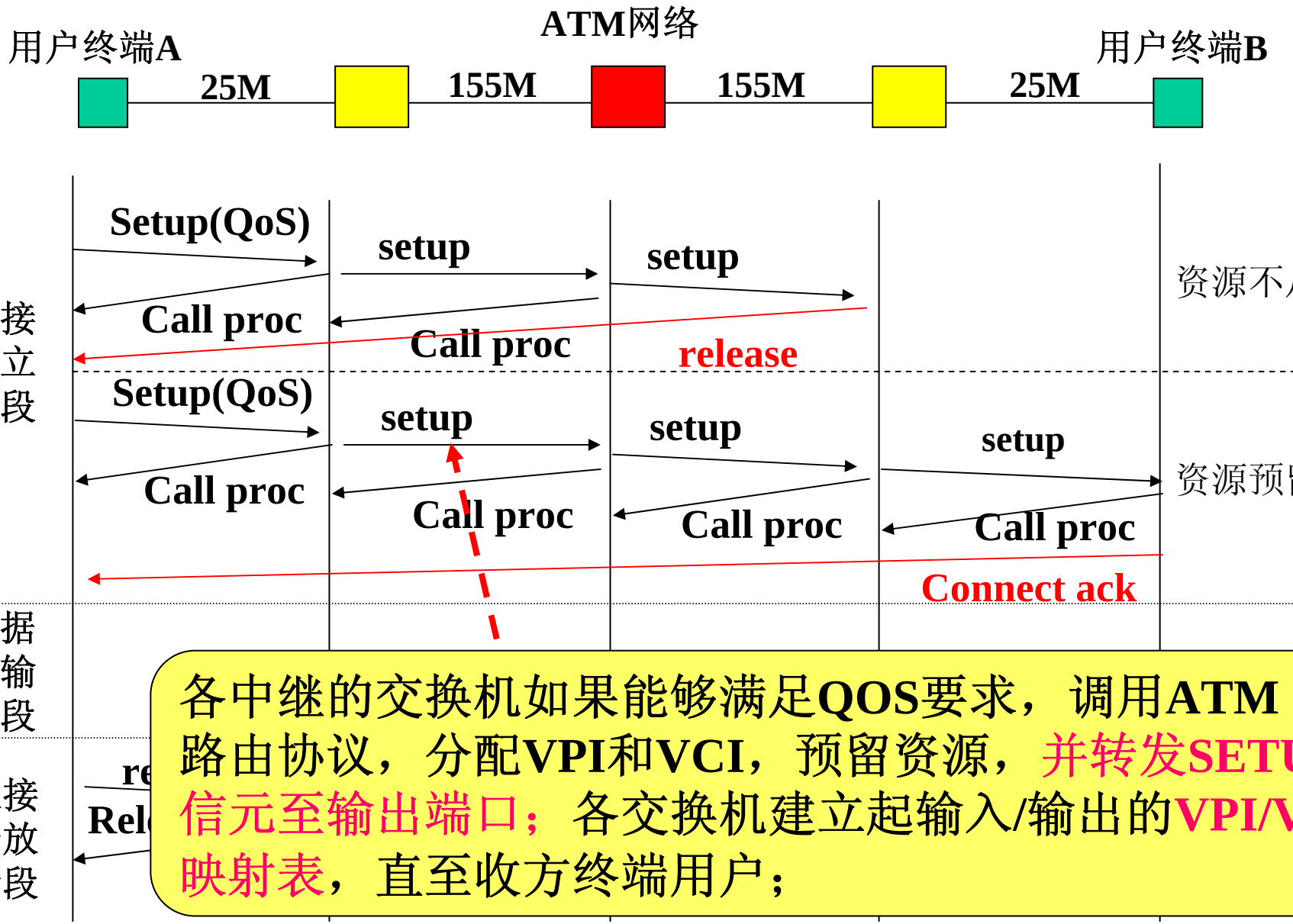


（2） ATM网络的工作过程



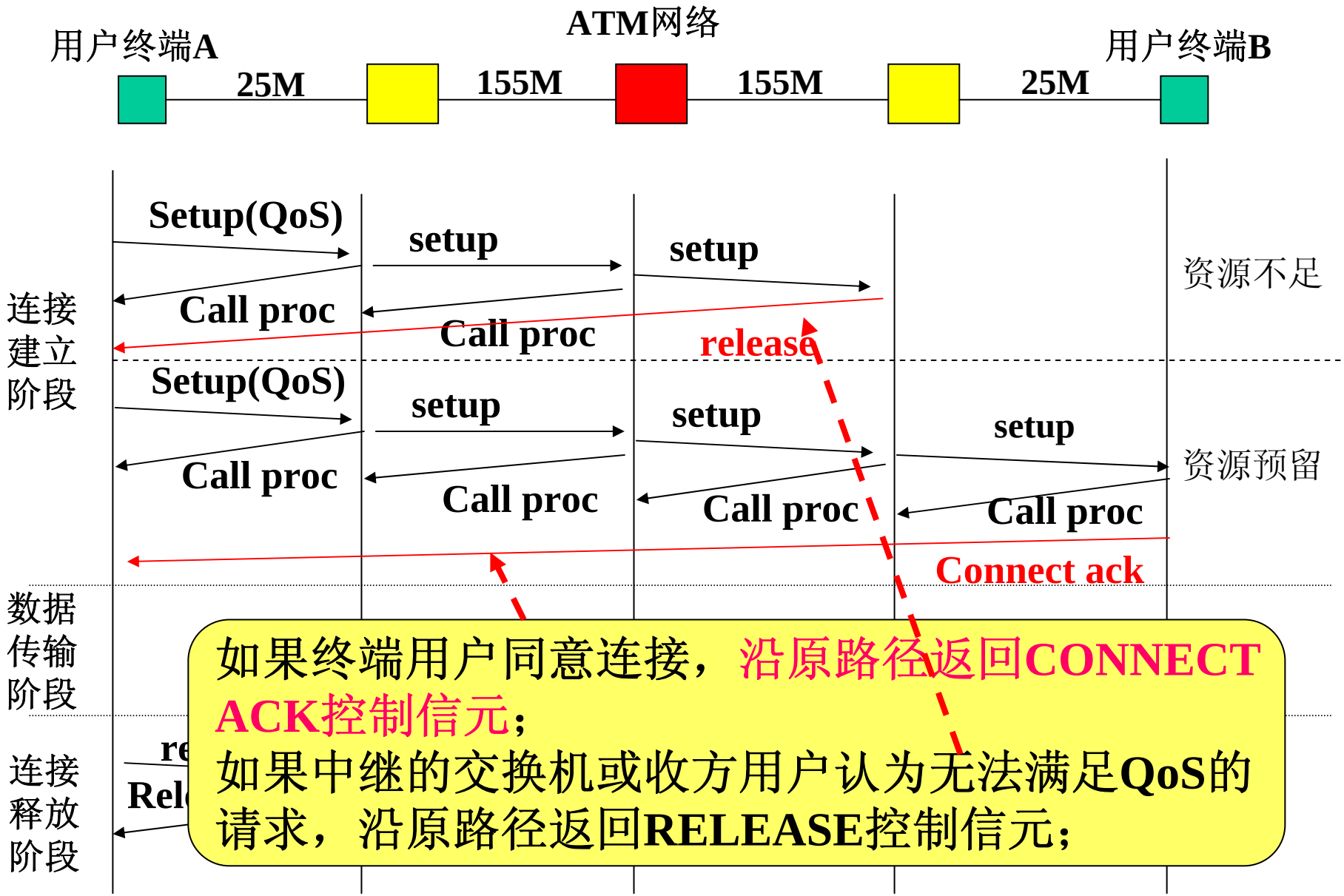
SETUP控制信元: 发送方用固定的虚拟通道（VPI＝0，VCI＝5）发SETUP，启动ATM连接建立的过程；Setup携带对方地址以及要求的服务质量（QoS，如所需的网络带宽，最大延时要求等）；

（2） ATM网络的工作过程

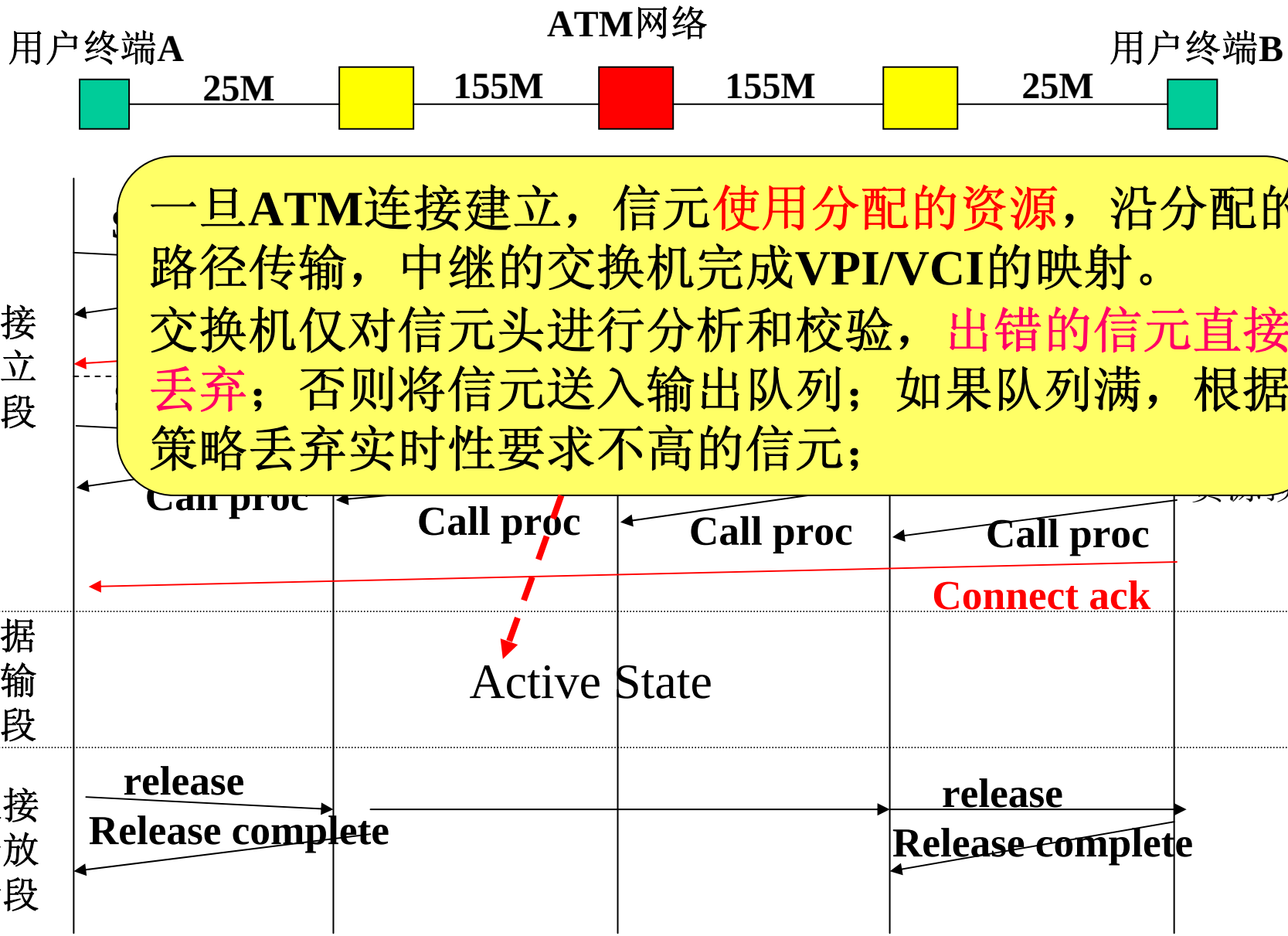


各中继的交换机如果能够满足QOS要求，调用ATM路由协议，分配VPI和VCI，预留资源，并转发SETUP信元至输出端口；各交换机建立起输入/输出的VPI/VCI映射表，直至收方终端用户；

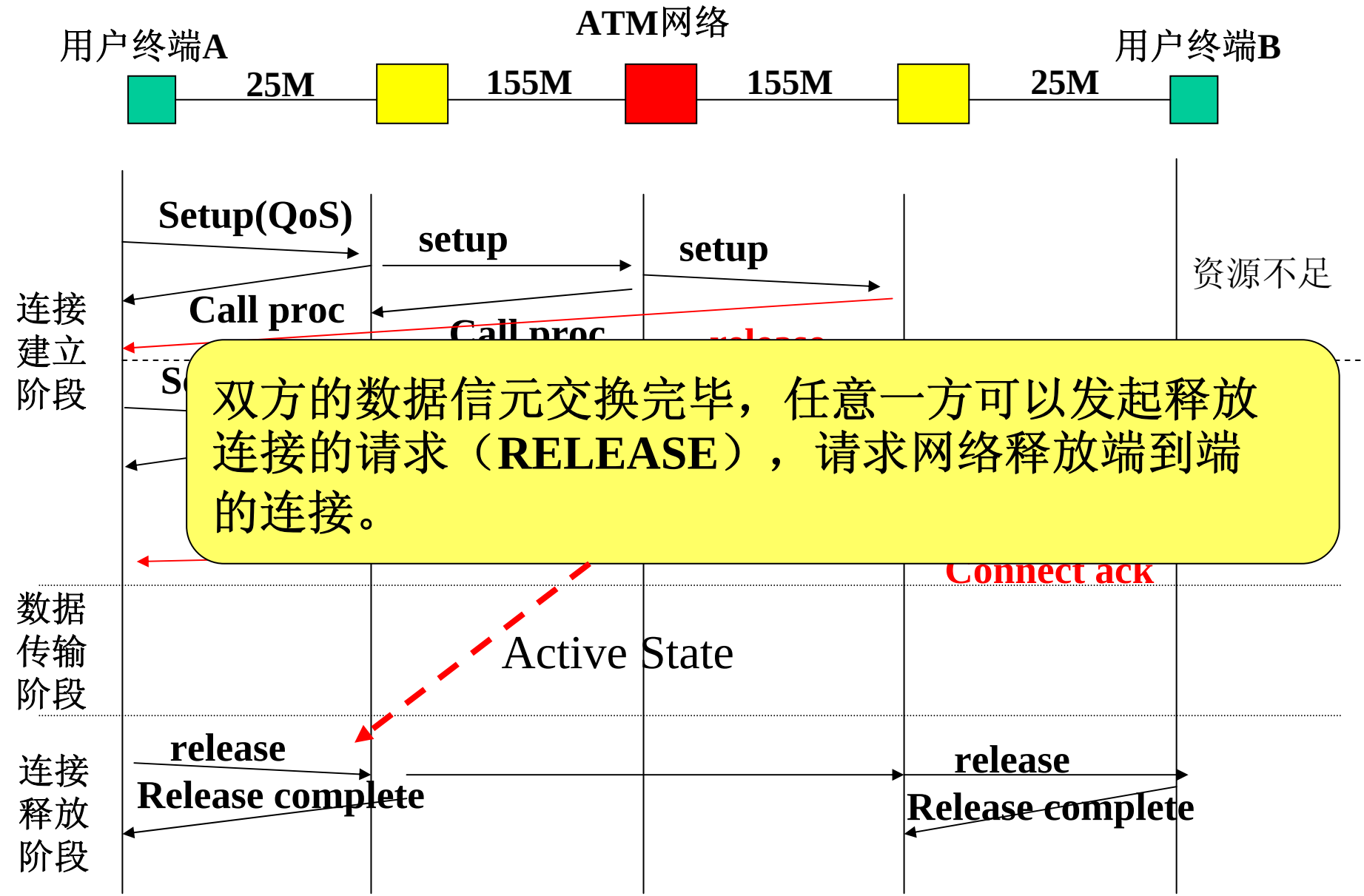
（2） ATM网络的工作过程



（2） ATM网络的工作过程



（2） ATM网络的工作过程



（3） ATM网络的应用前景

ATM具有带宽预约的功能，

是专为多媒体应用设计的网络；

ATM技术可以构建局域网和广域网；

10G以太网的推出影响了ATM技术的推广。

宽带用户接入方式

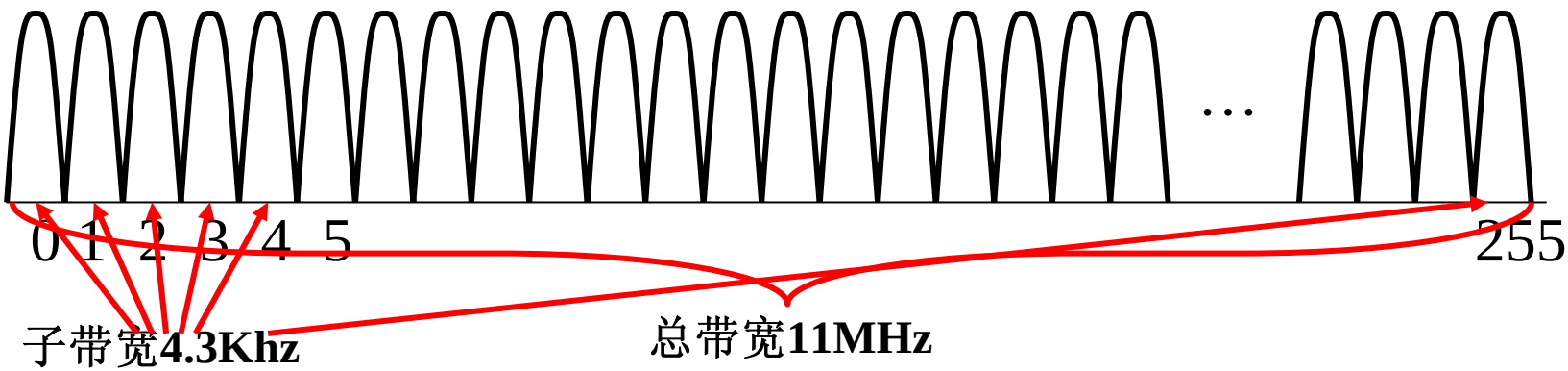
1 高速数字用户线接入（xDSL）：借助复用和调制技术，利用电话线支持用户高速接入方式的统称；

基本思路：在质量和距离（<5km）的限制下，用户端电话线约有11MHz的带宽，通常只用4KHz的带宽支持语音传输，高频段的开发有利于提高线路的利用率；

xDSL将11MHz的带宽划分为256个4.3125Khz的子带宽，分别用于支持语音和数据传输；

0道—语音传输，1-5道—保留，6-N—上行，N+1-255—下行；

不同的子带宽分配策略和调制方式导致不同的DSL。



宽带用户接入方式

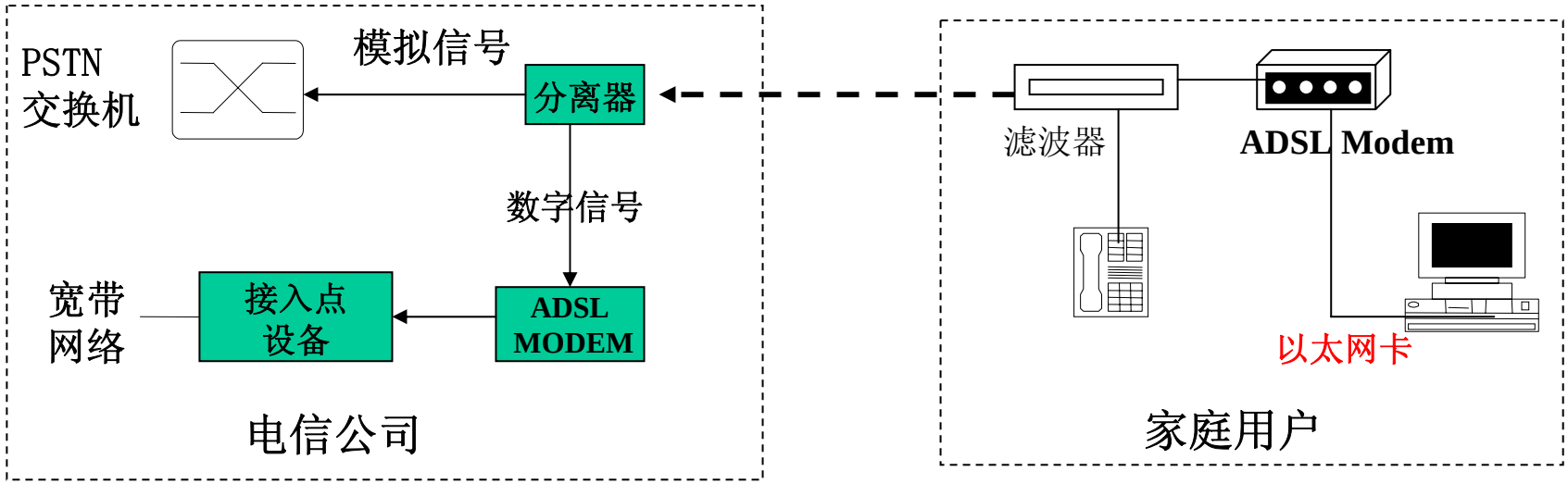
xDSL类型：

名称	上行速率	下行速率	距离
ADSL 非对称数字用户线	**64—640Kbps**	**1.5—6Mbps**	**3km**
ADSL Lite 简型非对称数字用户线	**<384Kbps**	**<1.5Mbps**	**5.4km**
HDSL 高位速对称数字用户线	**2Mbps**	**2Mbps**	**3.5km**
RADSL 速率自适应数字用户线	**120—1000Kbps**	**640—2000Kbps**	**5.4km**
VDSL 超高速数字用户线	**1.5M—** 下行	**13—52Mbps**	**1.2km**
……	……	……	……

注：速率依赖于距离和线路质量，通常会作自适应的降级适配。

宽带用户接入方式

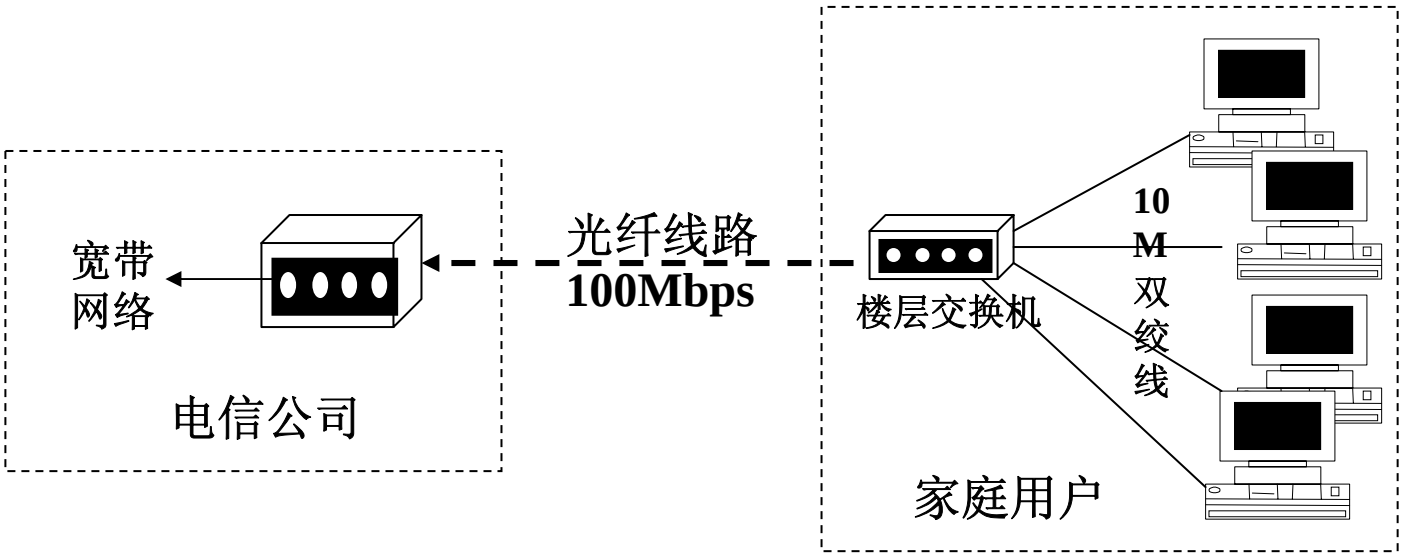
xDSL接入方式：



宽带用户接入方式（续）

2 以太网接入：支持广域应用的10G以太网的应用促成了以太网到户。

光纤到楼层网络设备（交换机），专线（双绞线）入户，10M/100M速率。



（广域网介绍完）

第六章　网络互连 — 6.1 概述

（1） 网络互连的目的

将两个或者两个以上具有独立自治能力的计算机网络连接起来，实现数据流通，扩大资源共享范围，或者容纳更多用户。

网络互连包括同构网络、异构网络的互连，并主要体现为局域网与局域网（LAN/LAN）的互连、局域网与广域网（LAN/WAN）或者局域网经广域网的互连。

（2）网络互连的优点

★ 扩大资源共享的范围 — 容纳更多的用户和资源；

★ 提高网络的性能 — 划分子网，有利于避免相互干扰；

★ 降低成本 — 统一入/出口，有利于降低外联的总体成本；

★ 提高安全性 — 入/出口监控，有利于统一管理和维护；

★ 提高可靠性 — 子网划分，有利于冗余设计。

（3） 网络互连的准则

★ 对原有网络的硬件和软件或者网络结构和协议不应作太大的修改（保持原有网络的特性）。

★ 不应为提高网络之间传输的性能而影响各个子网内部的传输功能和性能。

★ 执行网络互连的部件应当提供协调子网不同特性的能力。例如：编址方案、分组体积、访问机制和协议转换等。

（4） 网络互连应考虑的基本因素

不同的子网在性能和访问控制诸多方面存在差异，网络互连可能导致子网的部分特性损失（如总线形和环形）；

除了应当提供不同子网之间的网络通路之外，还应采取措施屏蔽或者容纳子网的差异。

★ 寻址方式；

★ 分组限制；

★ 访问控制；

★ 连接方式；

★ 不同子网的差错恢复机制对全网的影响；

★ 不同子网的用户接入限制；

★ 通过互连部件的网络流量控制等。

6.2 网络互连部件—互连的核心

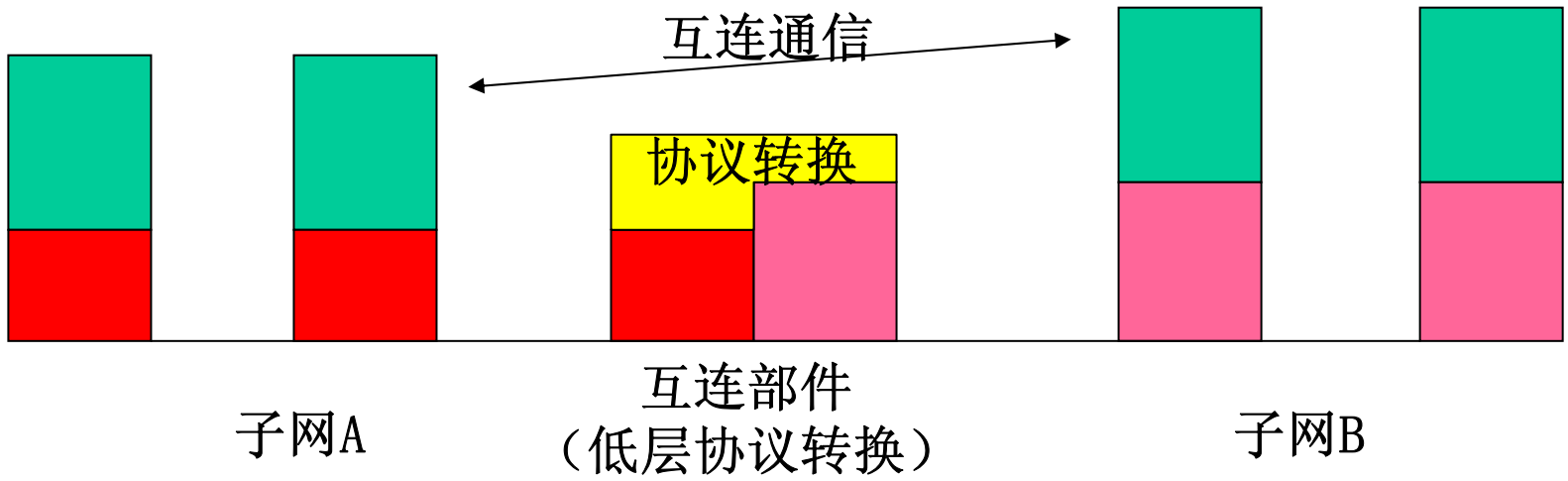
（1）原理：

执行不同协议的实体之间无法通信，因此互连部件应当：

★ 内部执行各子网的协议，成为子网的一部分，

★ 实现不同子网协议之间的转换，保证执行两种不同协议的网络之间可以进行互连通信。

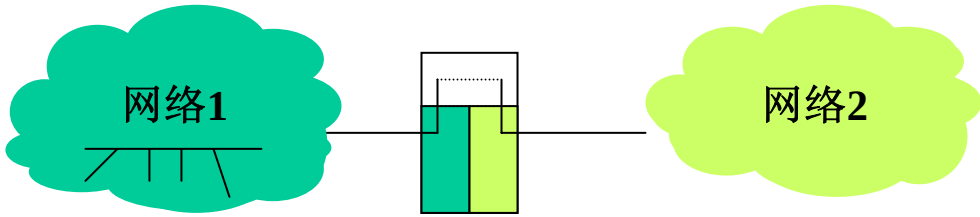
★ 协议转换包括协议数据格式的转换、地址映射、速率匹配、网间流量控制等。



（2） 网络互连的形式

★ 单部件（网关）互连

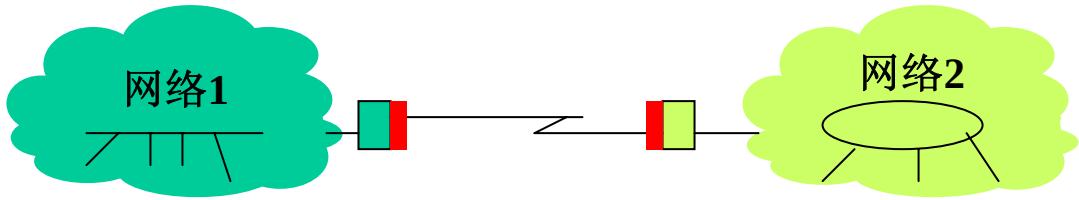
通过某个专门的互连部件连接两个或者两个以上的网络（子网）



两个子网执行不同协议时，单网关进行必要的协议转换；

★ 半部件（网关）互连

通过一对提供互连功能的部件进行两个网络（子网）的互连；



互连部件只能屏蔽对应层之下各层次的差异，为了保证更高层实体之间的通信，通信双方应当执行相同的高层协议。

（3） 网络互连部件分类

互连部件的作用：低层协议的转换；

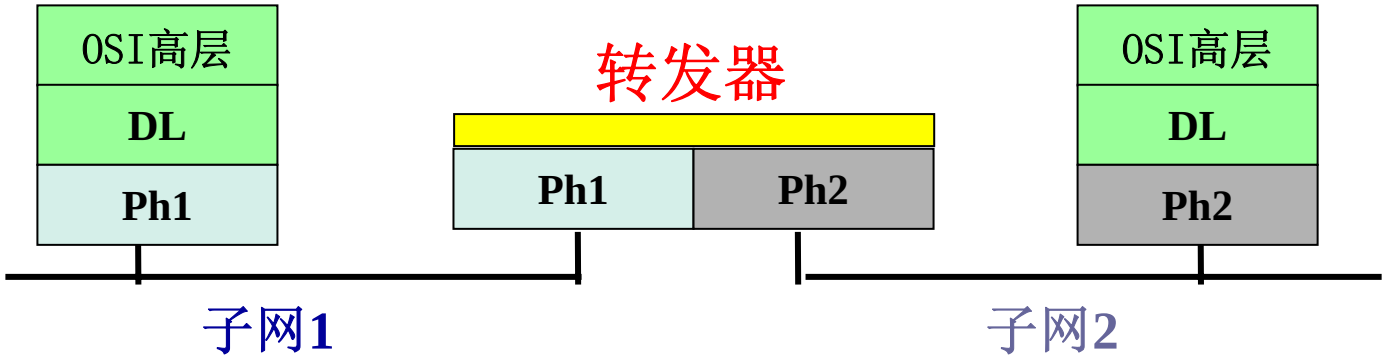
原则上可以对应到OSI的任何层次。

转换发生层次	物理层	链路层及以下层	网络层及以下层	运输层及以上层
互连部件称呼	转发器	网桥	路由器	网关

有时，也将所有的互连部件统称为网关。

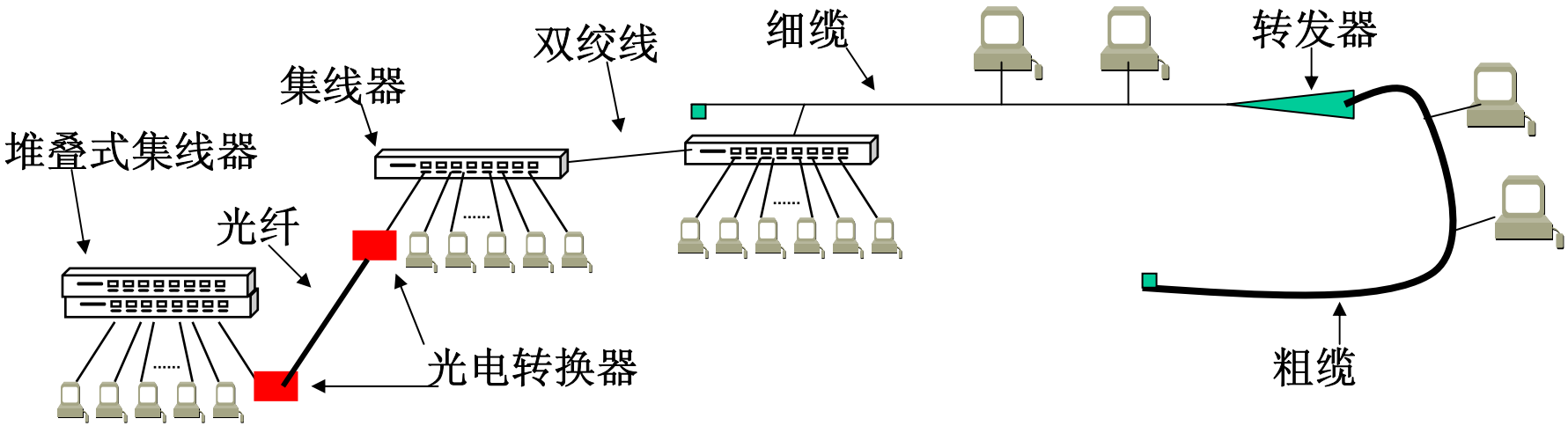
6.3 网络互连部件—转发器（中继器、集线器）

目的：延伸网段，改变传输媒体，同构网络互连；



过程：信号（含噪声）的接收和再生—补偿信号衰减；

形式：电缆延伸、光电转换等；

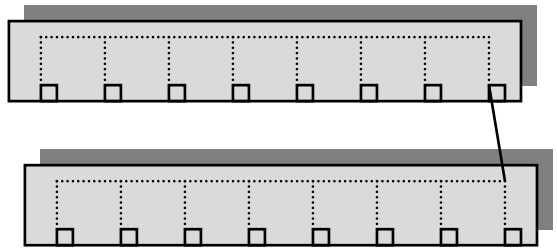


常用集线器（HUB）

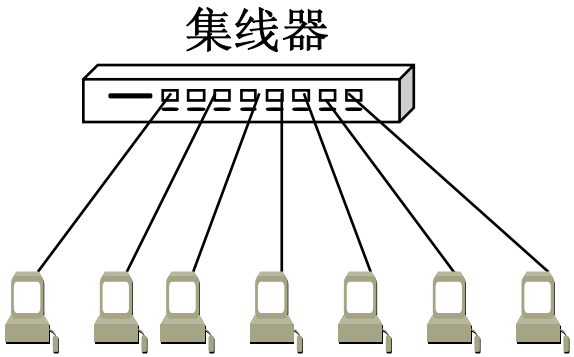
共享式集线器（10/100M)

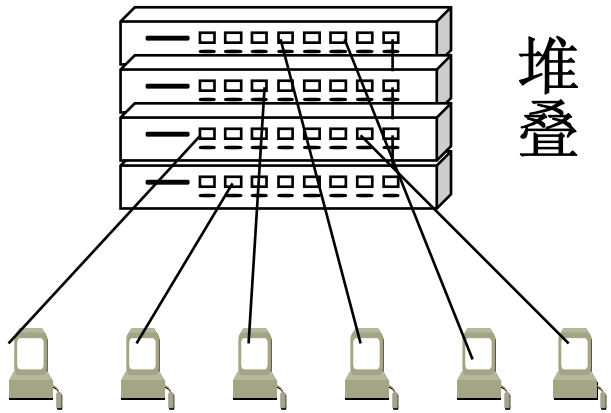
叠堆式集线器

端口数为8的倍数；



级连





堆叠

转发器的特点：

延伸网段，信号（含噪声）的接收和再生；

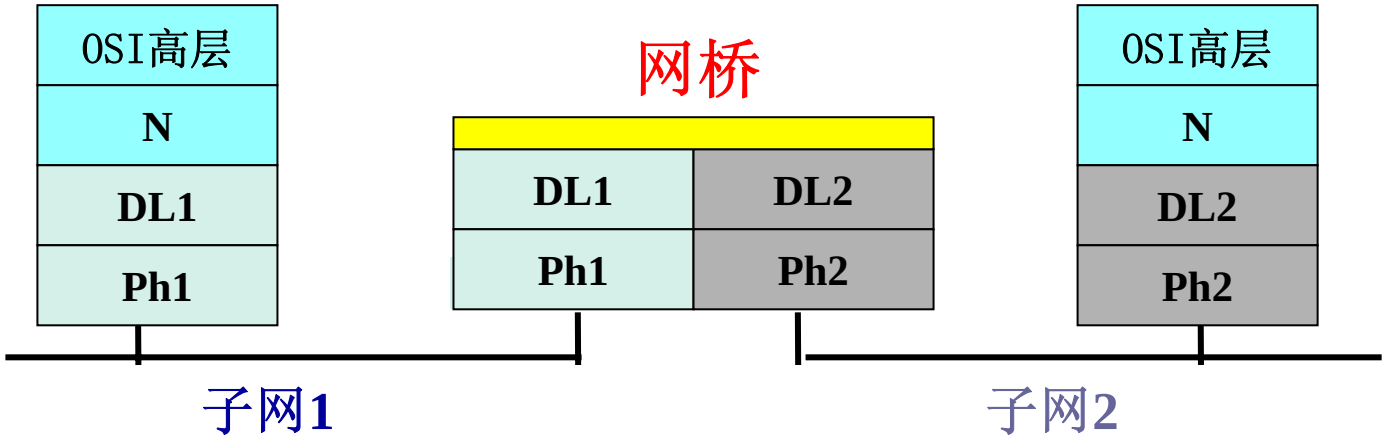
易于实现，成本低；

通过转发器互连的设备处于同一广播域，一个结点发出的信息被域中所有结点感知，限制了域中结点数。

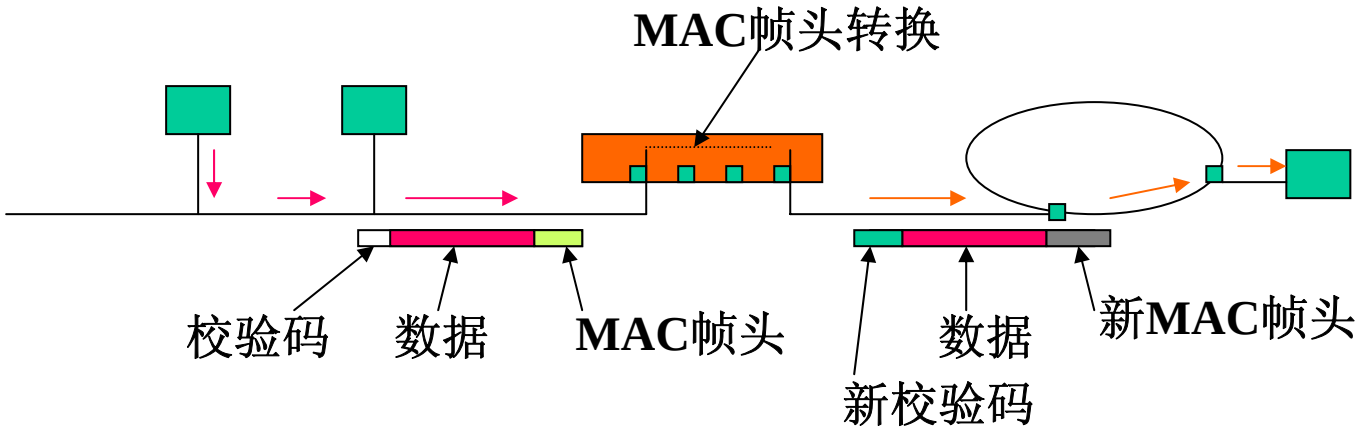
6.4 网络互连部件—网桥（含交换器）

（1） 原理

目的：互连两个独立的、仅在低两层实现上有差异的子网；



过程：信息帧的转发（含异构网互连时的重新封装）



（2） 常用场合

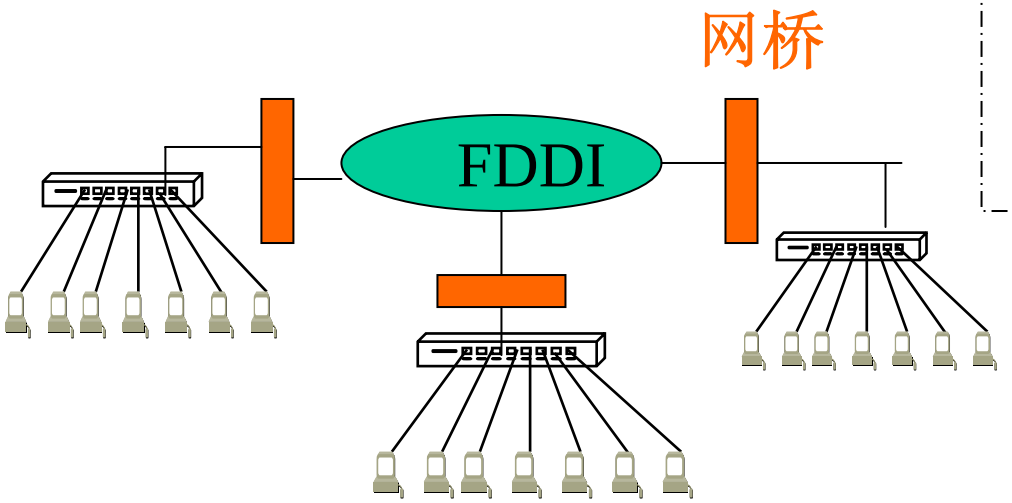
“相同”或者仅在底2层“相异”的网络互连；

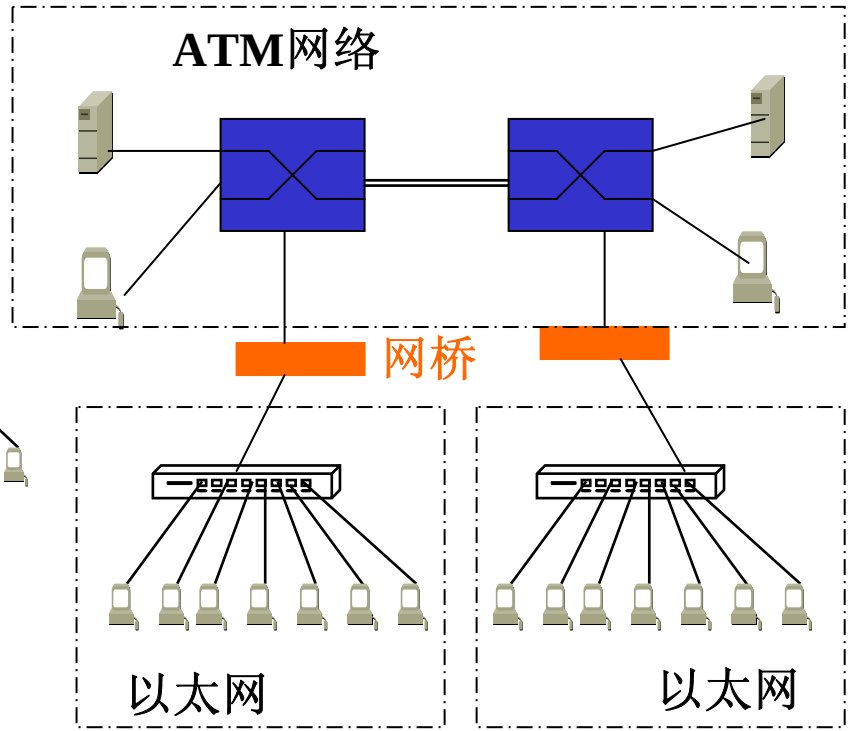
以太网—以太网（相同网络，如交换器）

以太网—**FDDI**（网桥）

以太网—令牌环（网桥）

以太网—**ATM**网（网桥）





（3） 网桥的功能及特点

★ 地址过滤.

具有统一的数据链路层的编址格式，网桥能够识别各种地址，并根据数据帧的宿地址，有选择地让数据帧穿越网桥。

★ 帧限制

网桥不对帧进行分段，只进行必要的帧格式转换，以适应不同子网。超长帧被丢弃。各子网相对独立，控制帧不能穿越网桥。

★ 监控功能

作为单个子网的一部分，参与对子网的监控和对信息帧的校验。具有“存储-转发”的能力，接收帧、检查帧和转发帧。

★ 缓存能力

适应不同子网对媒体访问的控制方式。

★ 透明性。

不应影响原有子网的通信能力。

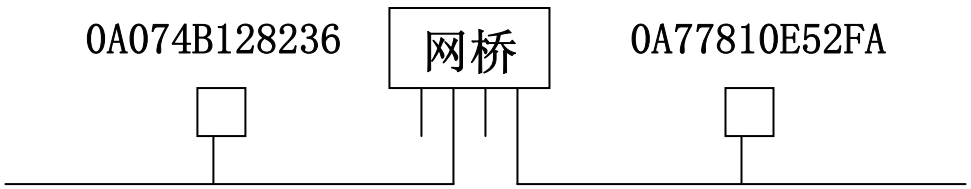
（4） 网桥的路径选择—避免广播风暴

原始网桥对信息帧宿地址的处理：如果该地址不属于原子网，则向所有的端口转发（广播）。

结果：大量的“无用帧”散布到网上—广播风暴。
可能导致帧在网络上的无限制的转发。

解决方法：设置地址映射表—有选择地转发；
设置计数器—丢弃转发过的帧。

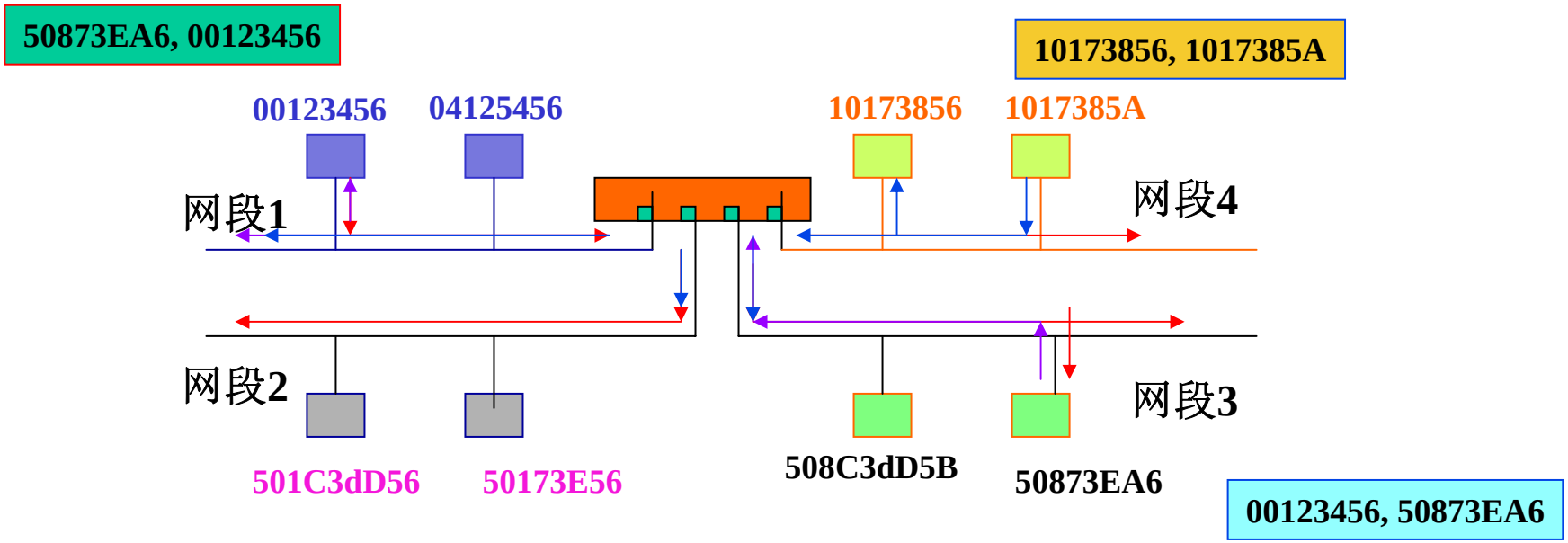
地址映射表的结构：



结点地址	端口编号
0A074B128236	**2**
0A77810E52FA	**4**

地址映射表的使用：分析途经网桥的每个帧，
如果宿地址出现在映射表中，封装/转发该帧至对应网段（端口），否则广播。

地址映射表的动态构造（自学习）



地址映射表：

MAC地址	端口
00123456	网段1
50873EA6	网段3
1017385A	网段4
……	…

网桥分析收到的每个帧：

源地址：加入/修改地址表

地址 + 所属端口；

宿地址：查地址表，

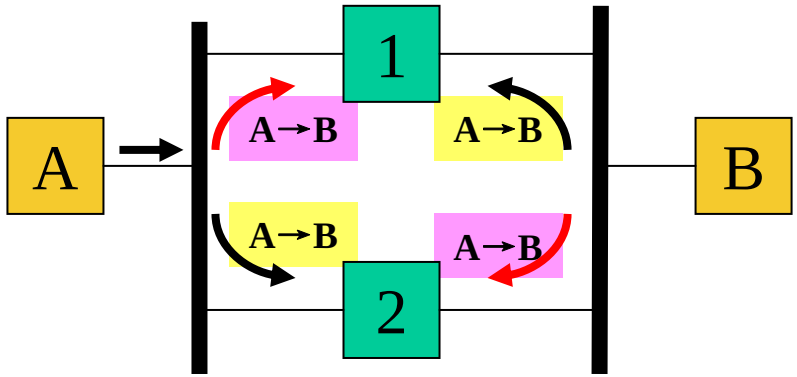
已存在，转发到指定网段

无，广播到所有子网；

（5） 网桥循环的避免—冗余网桥及生成树

为提高网络可靠性，通常需设置冗余网桥或者冗余连接；

问题：可能导致地址映射表无法正常工作。



解决方法：不转发已转发过的帧？

潜在问题：如何保存和判别转发过的帧？

结点增加，子网增多时问题更为严重。

解决方法：对于存在环路的网络，执行构树过程，确保网络中任意两个结点之间有且仅有一条路径。

冗余网桥及生成树算法（续）

★ 解决方法：执行生成树算法，消除循环，多余资源留作备用；

★ 目标：任意两个结点之间仅有一条（跨越不同网段）的路径；

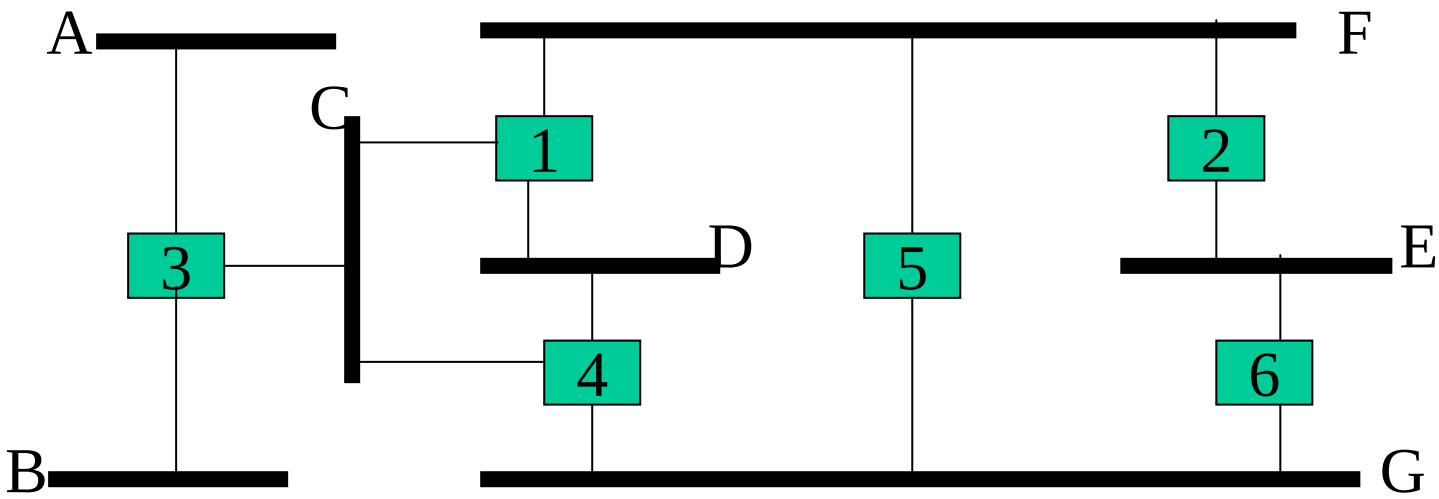
★ 原理：逐个增加网桥（端口），一旦出现环路，则阻塞引起该环路的端口；

★ 算法依据：网段为点，桥为边的图中求生成树（支撑树）；

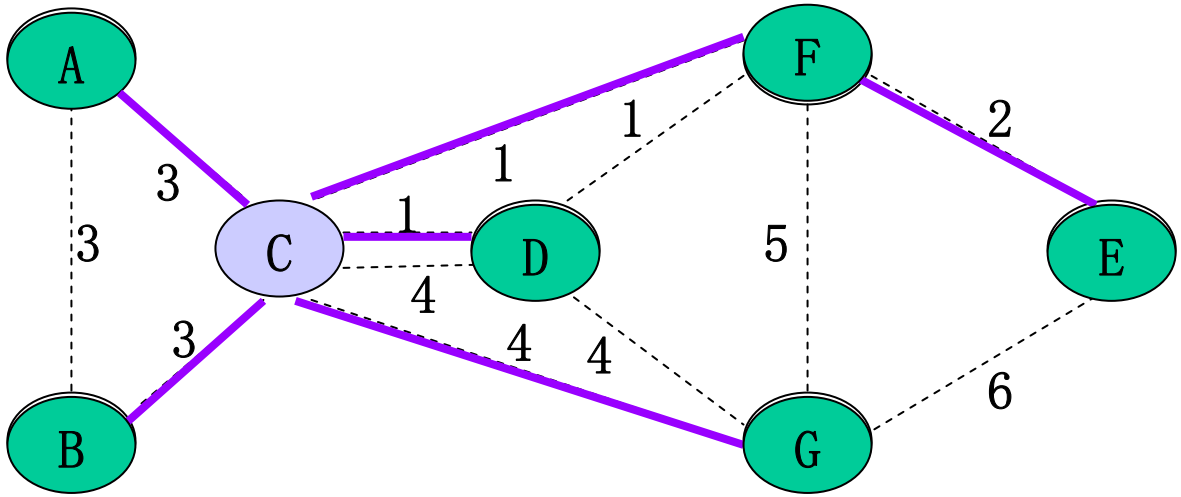
★ 辅助设施：网桥具有网桥标识和端口（网段）编号；端口可设置“转发”、“阻塞”等状态。

★ 过程及原则：①根网桥（指定或最小地址的桥）周期性（1-4s）发出Hello广播报文； ②所有网桥记录并转发该报文； ③多个桥向同一网段转发该报文时，小地址桥的端口置为“转发”状态，其它桥的相应端口可置为“阻塞（不转发）”； ④保证每个网段都（仅）有一个桥（端口）负责转发； ⑤当同一桥的多个端口冲突时，阻塞编号较高的端口。

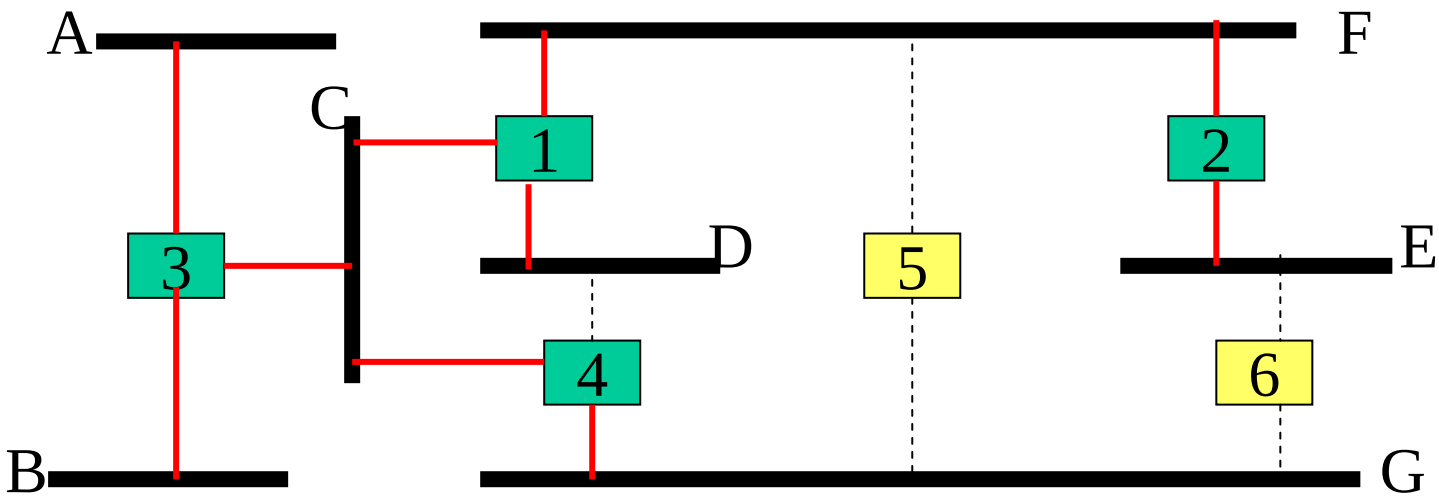
冗余网桥及生成树示意



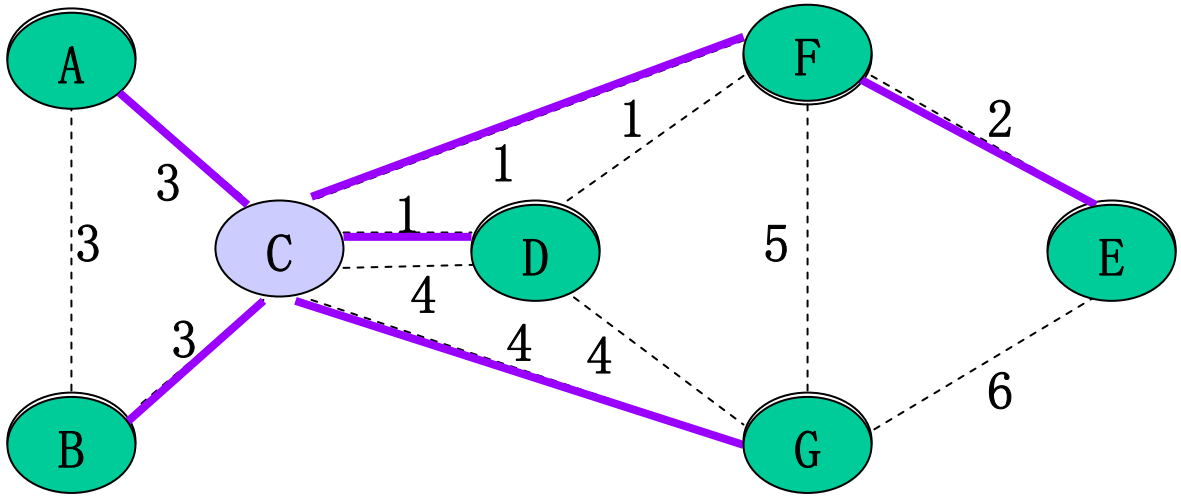
图（网段为点，桥为边）及生成数（支撑树），小号边优先；



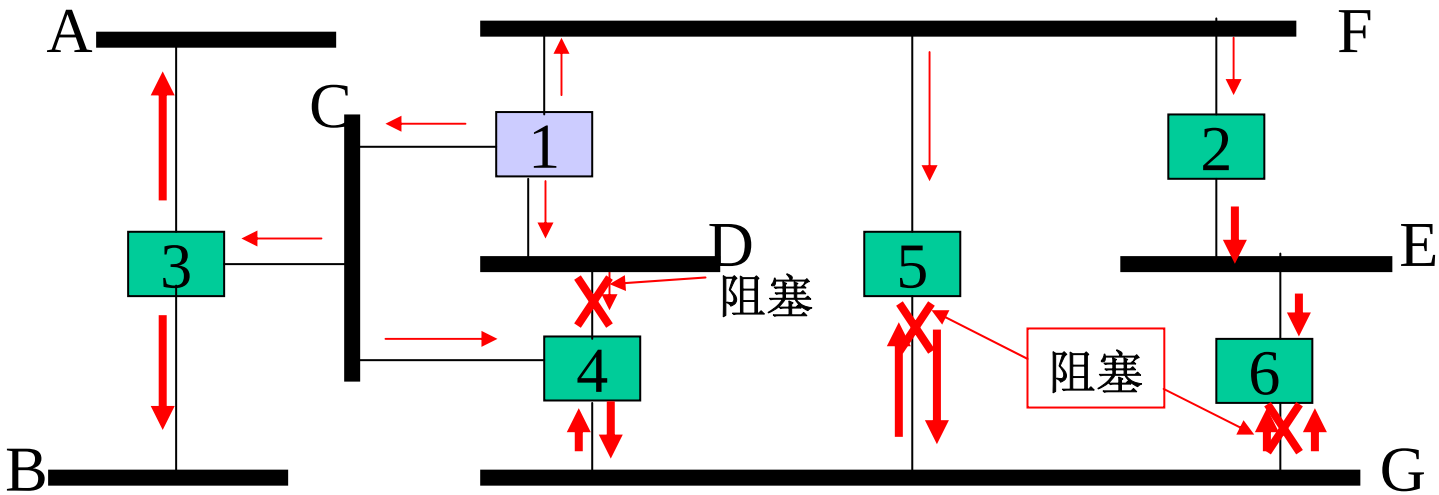
冗余网桥及生成树示意



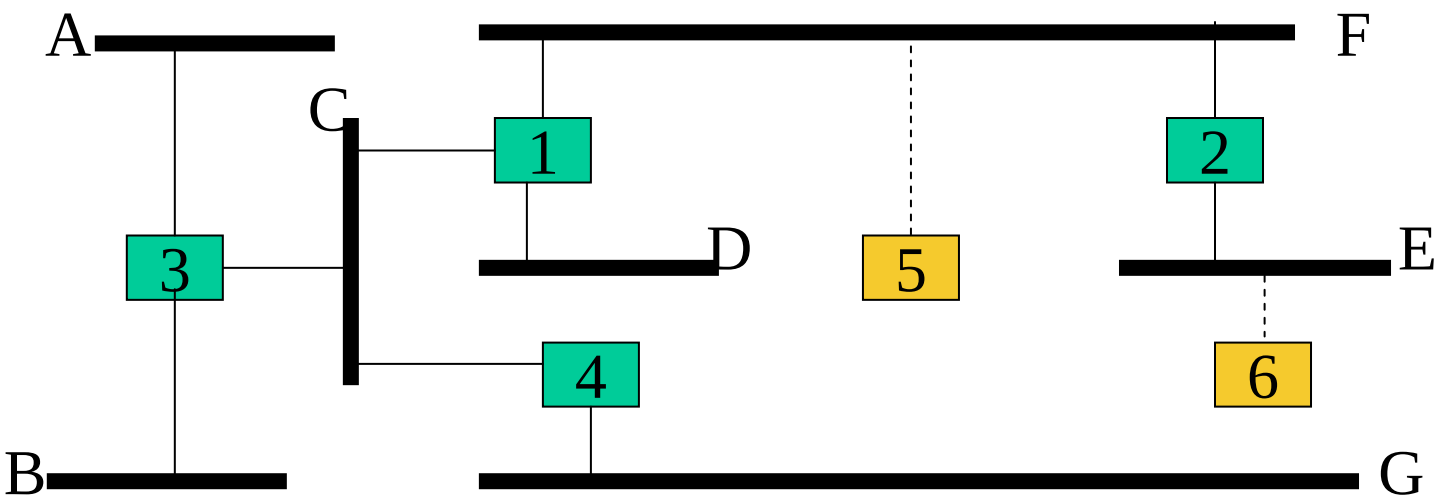
图（网段为点，桥为边）及生成数（支撑树），小号边优先；



冗余网桥及生成树示意（同一网段多转入时，大号端口阻塞）



结果



（6） 网桥实例—以太网交换器（交换式集线器）

目的：用于互连相同类型的LAN（以太网）

特点：具有分割子网的能力—网桥的特性，

每个端口对应一个子网；

每个端口独享指定的带宽—区分于共享式集线器。

地址映射表空间有限—提高查表速度；

地址表更新—自学习方式；

具有2层交换（帧交换）的能力，硬件支持—提高速度；

直通式交换，仅分析帧源/宿地址后即转发，

特点：速度快，错帧转发浪费资源；

存储—转发式交换，分析整个帧后转发，

特点：提高转发的可靠性，影响转发速度；

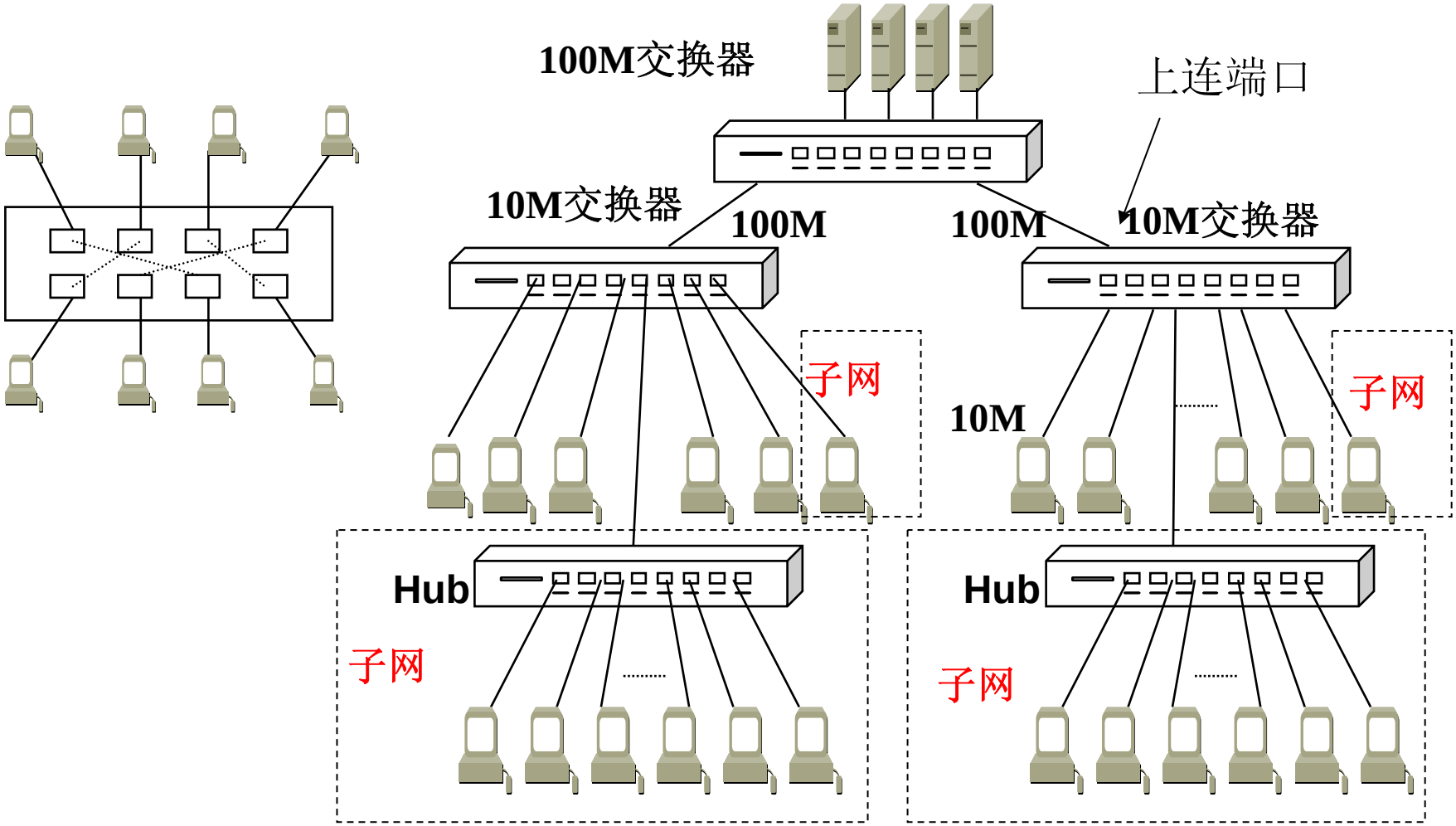
混合式，根据线路质量，选择直通或者存储-转发交换

支持少量的帧缓存能力，避免端口冲突；

常用的交换器一般具有1-2个上连端口，8、16、24、48个下连端口，端口一般为RJ45端口；配上光纤模块，可以附接光纤（光缆）。

以太网交换器的应用

快速交换—基于 MAC地址的硬件交换



6.5 网络互连部件—路由器

（1）原理

网桥的限制：仅适合低二层有差异的网络互连；

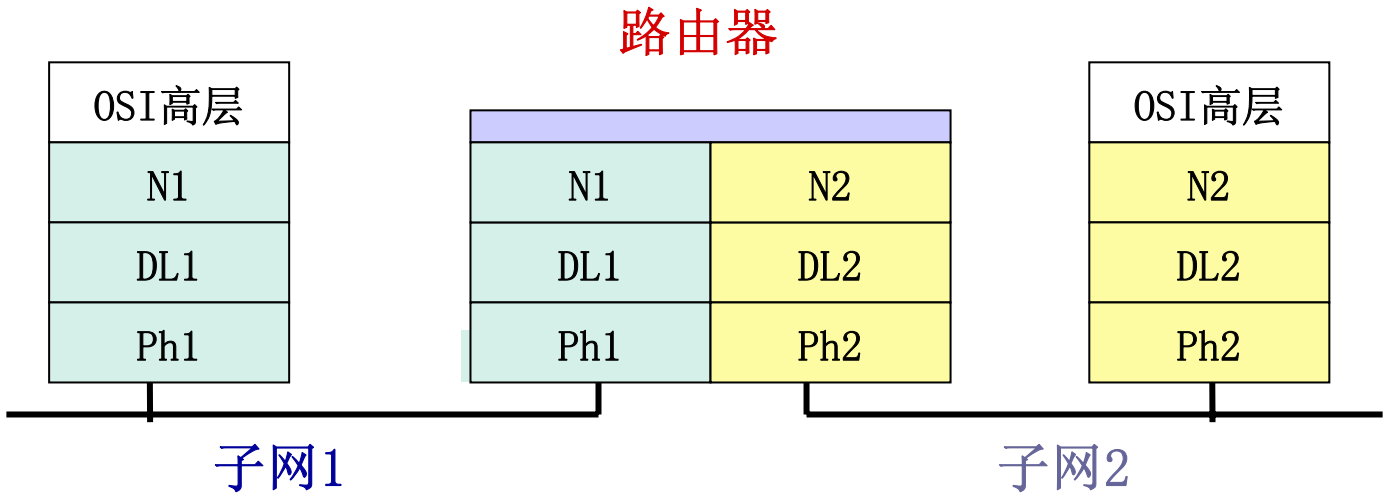
目的：互连两个或多个独立的同构或异构的网络，

如局域网/广域网、局域网/局域网的互连；

过程：分组的封装和转发，屏蔽3层以下的差异，

OSI网络层的主要功能：路由选择—路由器；

路由器的体系结构：



（2） 路由器的主要功能

★ 寻址：全网地址格式统一，如IP地址；

★ 路由选择：了解互连的子网工作状态，旁路故障和防止拥塞；

★ 分组分段/合段：根据子网的分组长度要求，进行分组的分段和合段；

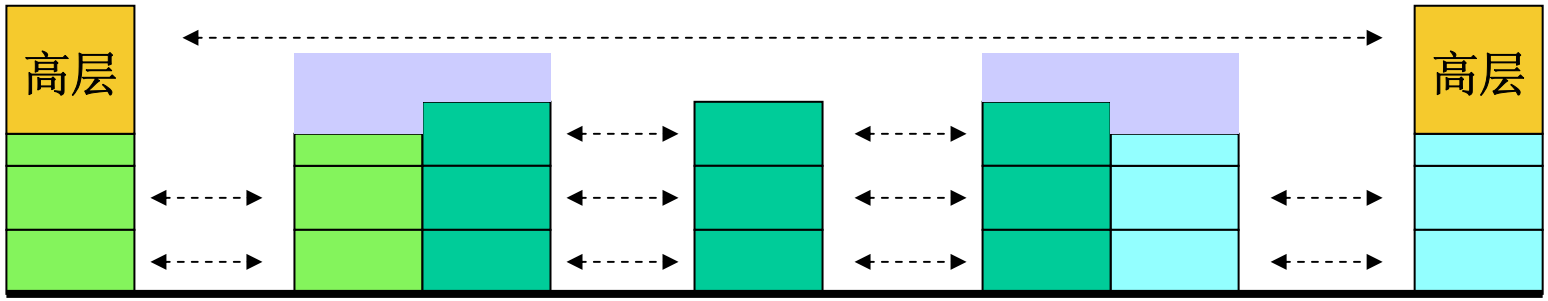
★ 格式封装：构建适合子网传输和处理的分组；

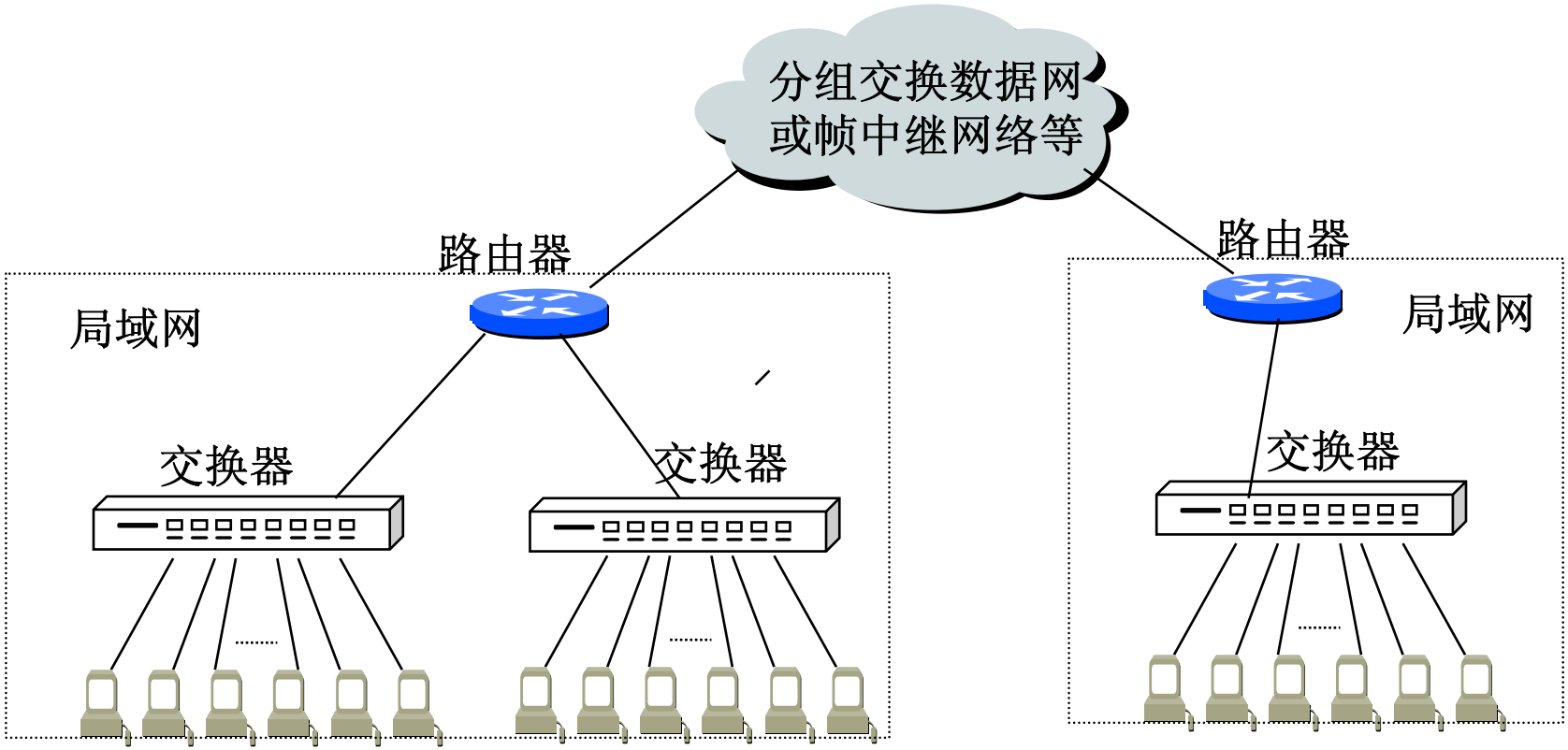
★ 存储—转发（分组过滤）：分组校验（丢弃出错的分组）、存储和转发。

路由器功能主要由软件完成，效率较低，高性能的路由器具有高的价格。

（3） 路由器的主要应用

局域网—广域网—局域网互连





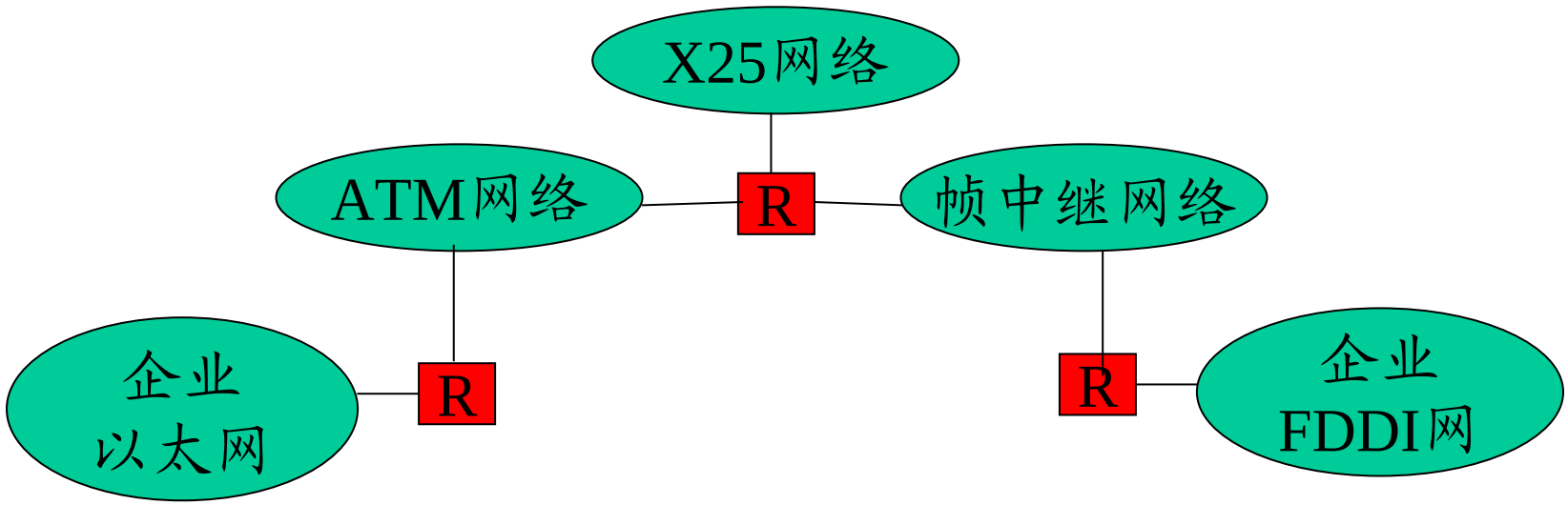
常用路由器的端口配置

1-2个以太网端口（10/100/1000M自适应）：连接局域网；

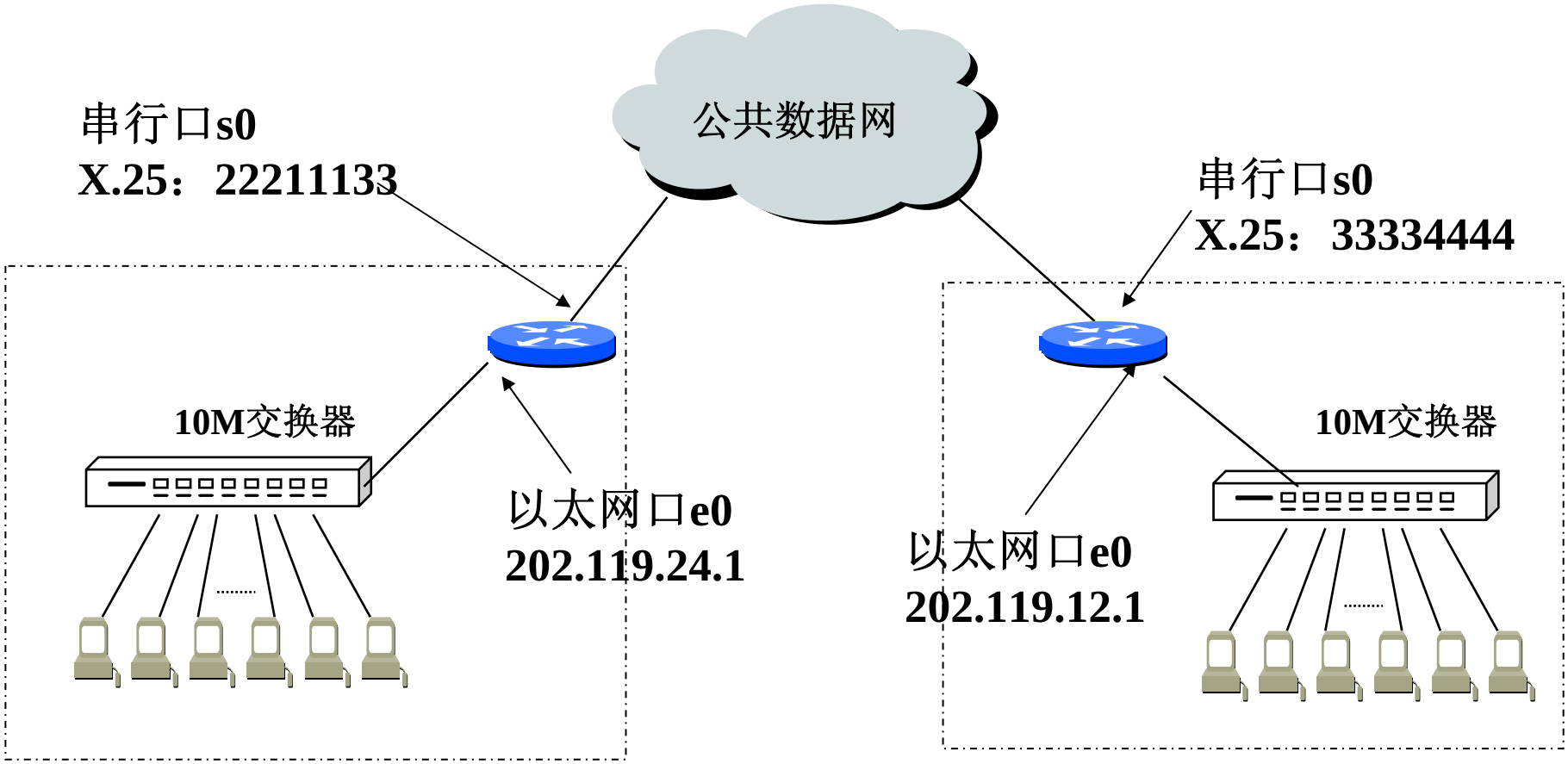
若干个同步/异步端口（可设置）：连接广域网；

若干个可扩展槽：配置不同的模块，附接不同的网络（如ATM、FDDI、帧中继等）；

实用中，路由器主要用于企业网的对外接口，企业网内部使用网桥（交换器）附接结点。



广域网路由器的配置实例

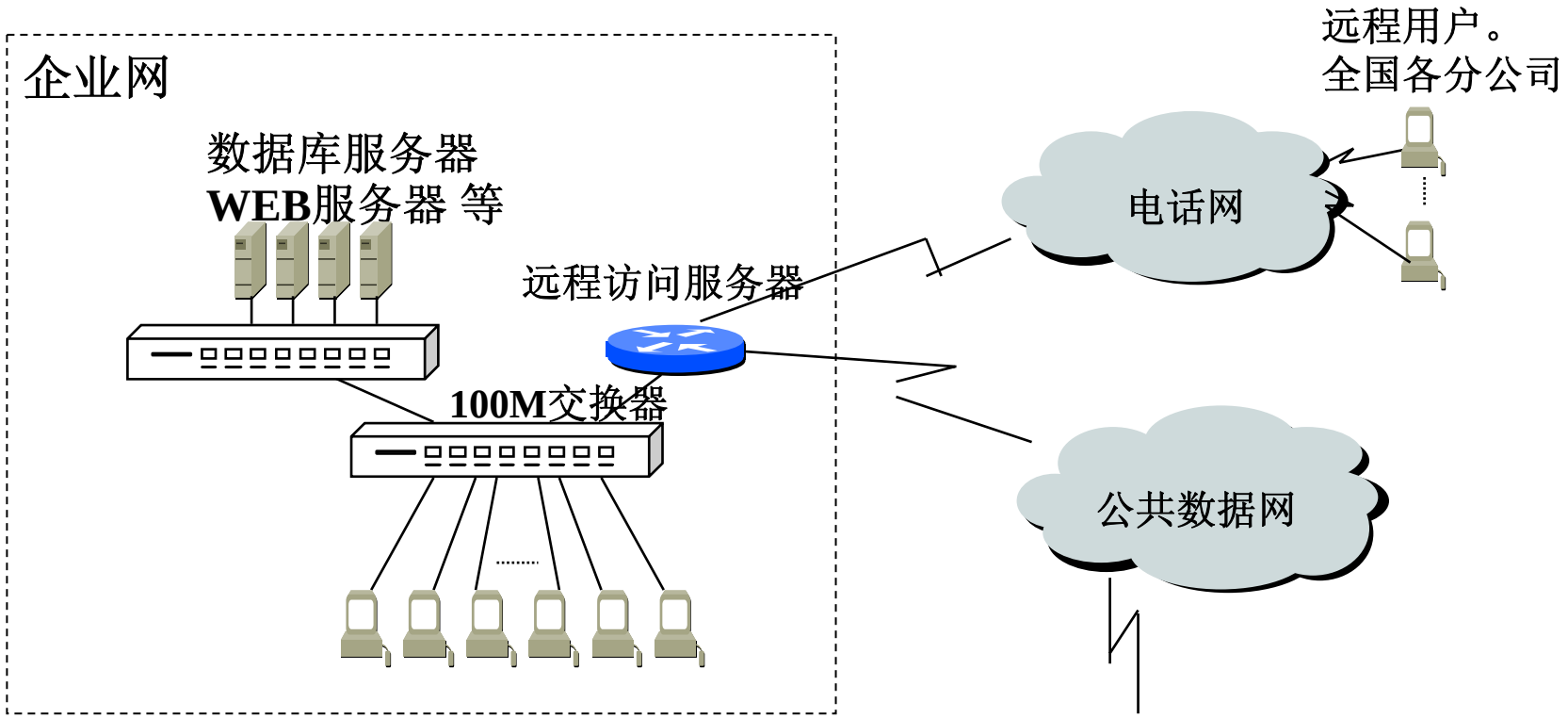


远程访问服务器—路由器之一

含异步/同步（可选）端口和以太网端口；

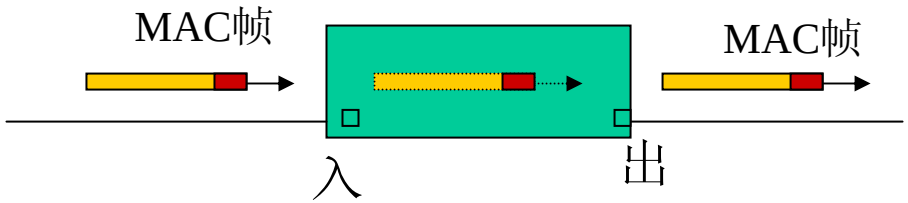
支持用户通过电话网拨号上网，利用电话网的资源；

远程用户（乡、镇）、网线不易铺设的单位、出差在外的访问。



（4） 二层/三层交换（L2/L3交换）

L2交换：交换机根据帧的宿地址和映射表，不作修改地交换至输出端口；交换对象：帧。

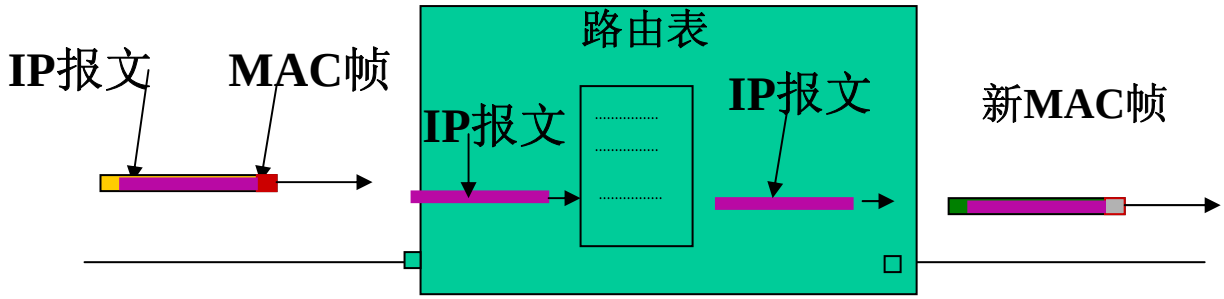


L2交换

L3交换：根据分组的宿地址和路由表，在路由器上实现分组的交换。

路由表

IP地址	端口
202.119.11	T1
202.119.2.	T2
202.119.24	T3
⋮	



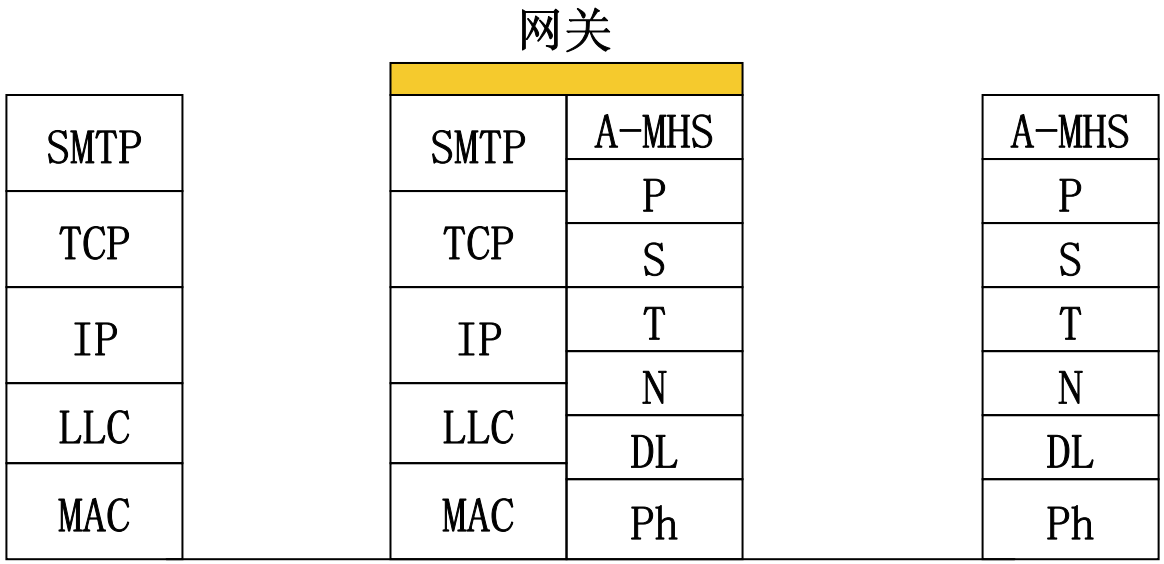
L3交换

6.6 网络互连部件—网关（信关）

目的：支持更高层的协议转换（主要是应用协议的转换），
如：电子邮件的转换等；

实施方法：软件实现。

网关的实质：解出对应层的用户数据，用新协议进行封装和传输。



6.7 企业组网的一般讨论

★ 企业网通常采用层次结构，由主干网和分支网组成。

★ 主干网辐射到各个部门，
分支网连接部门内的各台计算机。

★ 主干网通常采用高速网络（如：高速以太网、**FDDI**等）；
随着分支网下沉，交换机档次降低（如：千兆、百兆、十兆等）
根据应用的不同选择不同的交换网络设备；

★ 当需要跨越广域网互连时，必须选择路由器；

★ 主要网络设备：网络适配器（卡）、共享式集线器（**HUB**）、
交换器（**Switch**）、路由器（**Router**）；

目前大多采用国外的设备：**IBM**、**CISCO**、**3COM**，…；
国内厂商：巨（龙）、大（唐）、中（兴）、华（为），……。

企业组网的一般方式

★ 小规模企业（十几台计算机，传输文本和数据信息）
可直接使用**HUB**连接，形成局域网

★ 中等规模企业（几十台计算机）
交换器＋**HUB**，形成局域网

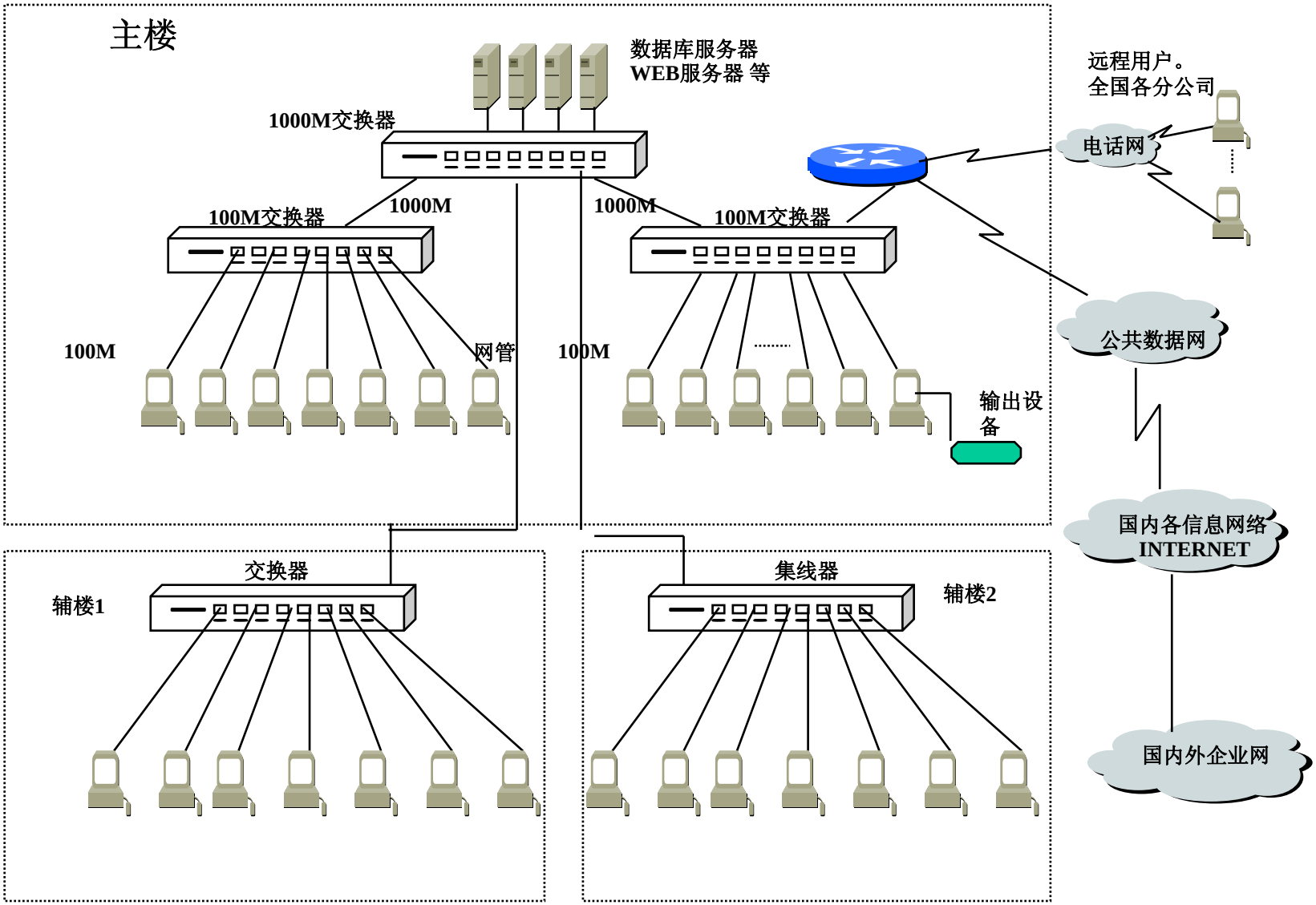
★ 稍大规模企业
主交换机＋交换器＋**HUB**；形成园区网

★ 大规模企业　主交换机构成主干网，通过交换器＋**HUB**辐射园区网

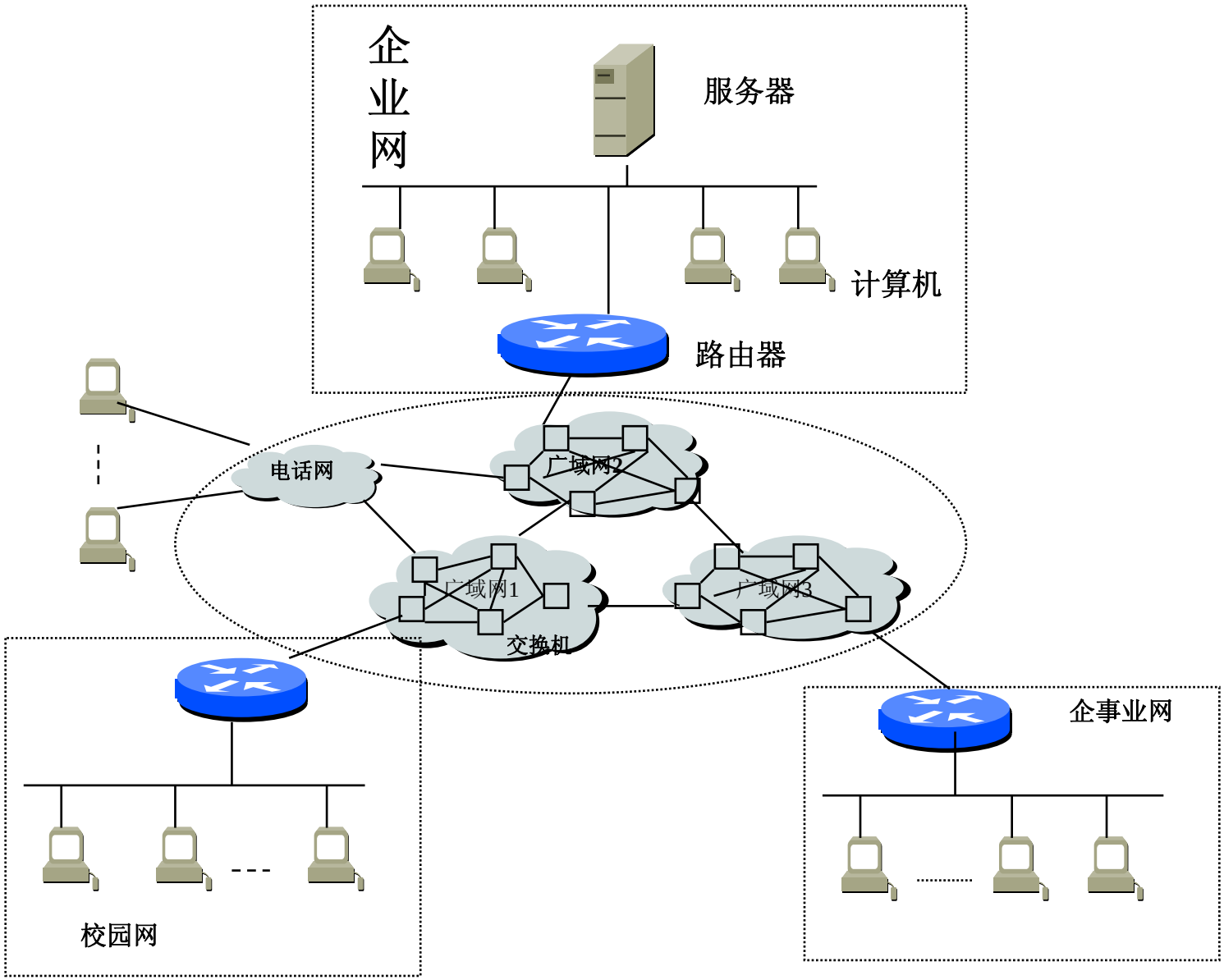
★ 企业间或者跨区域互连
增加路由器，接入广域网（包括专线方式连接）

所有入网设备应配置网络适配卡；
网卡选型注意和传输媒体配套；
所有的设计都应考虑应用对带宽的要求。

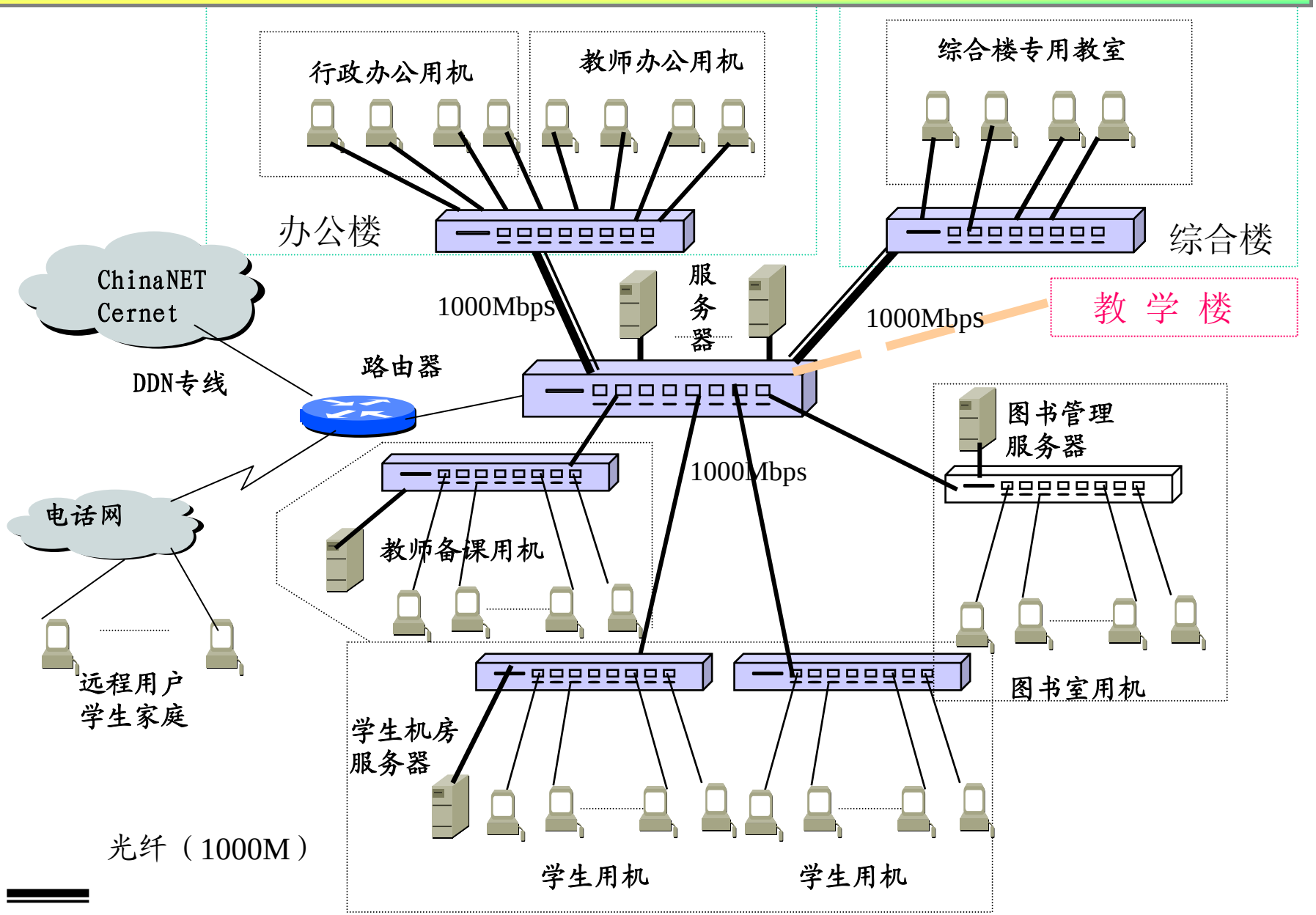
网络举例


主楼
数据库服务器
WEB服务器 等
1000M交换器
远程用户。
全国各分公司
电话网
1000M
1000M
100M交换器
100M交换器
100M
网管
100M
输出设备
公共数据网
国内各信息网络
INTERNET
交换器
辅楼1
集线器
辅楼2
国内外企业网

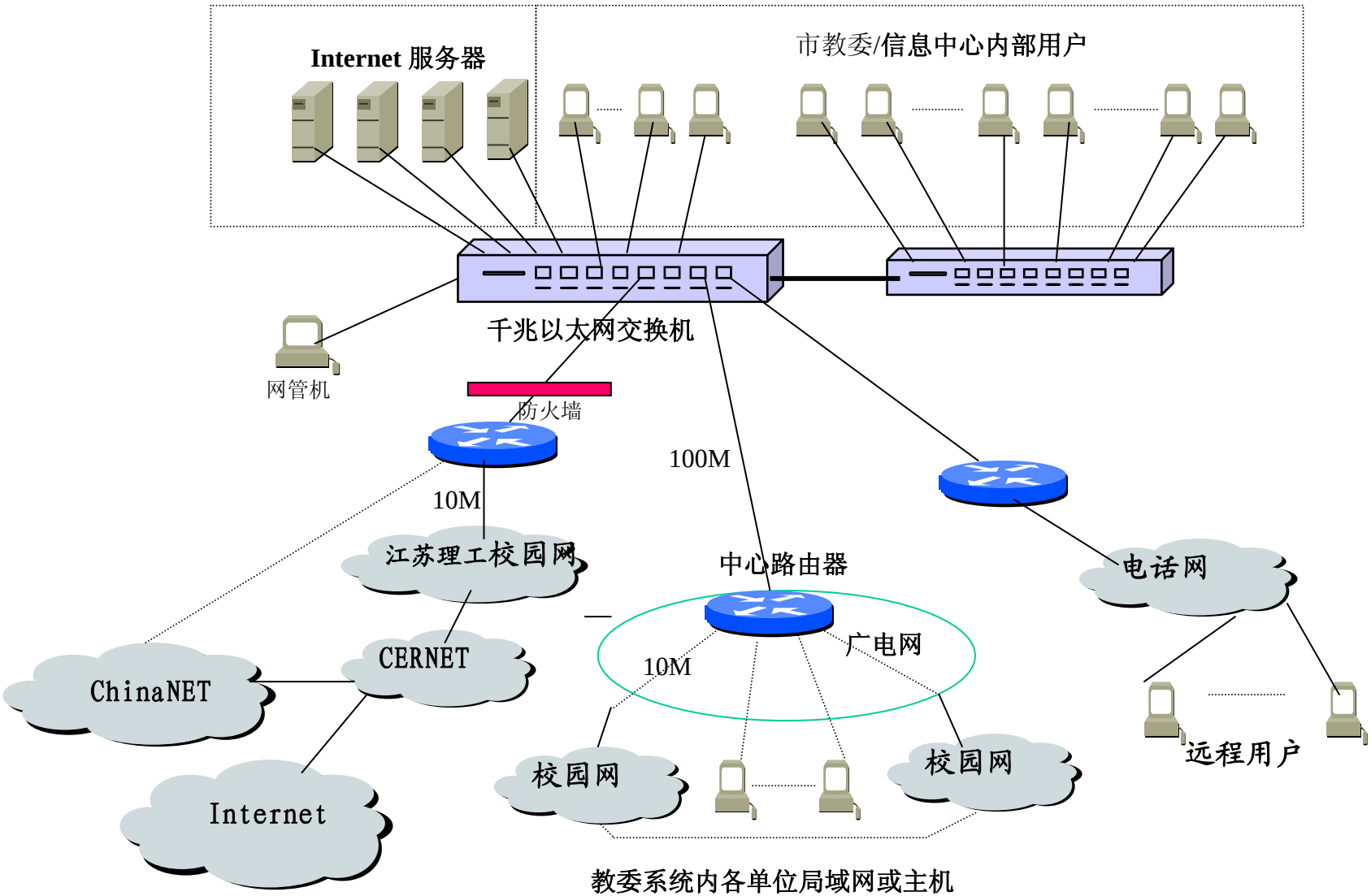
网络举例



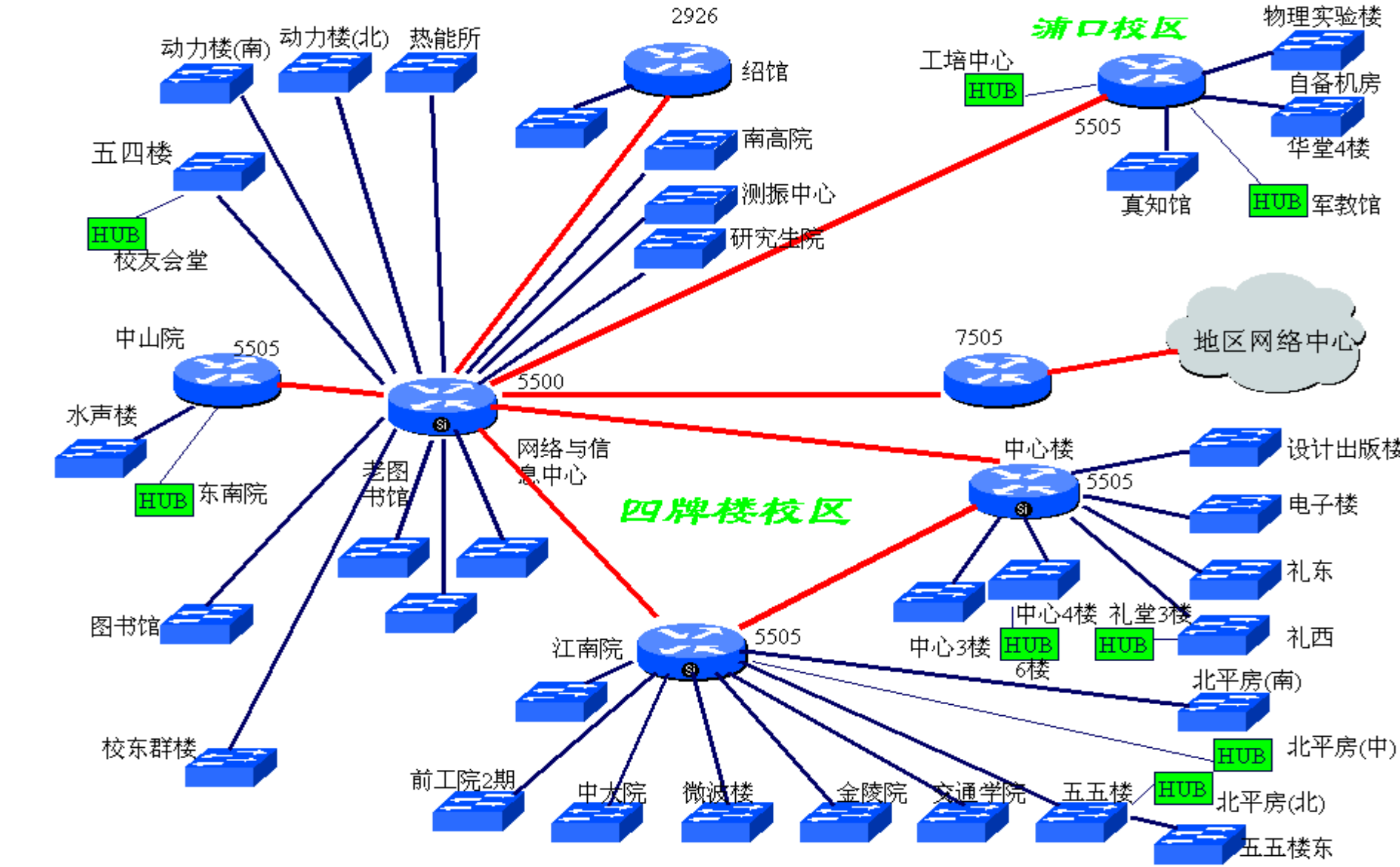
某中学校园网拓扑图


行政办公用机
教师办公用机
综合楼专用教室
办公楼
综合楼
ChinaNET
Cernet
DDN专线
路由器
1000Mbps
服务器
1000Mbps
教 学 楼
1000Mbps
图书管理
服务器
电话网
教师备课用机
远程用户
学生家庭
学生机房
服务器
图书室用机
光纤（1000M）
学生用机
学生用机

某市教育信息中心网络拓扑图

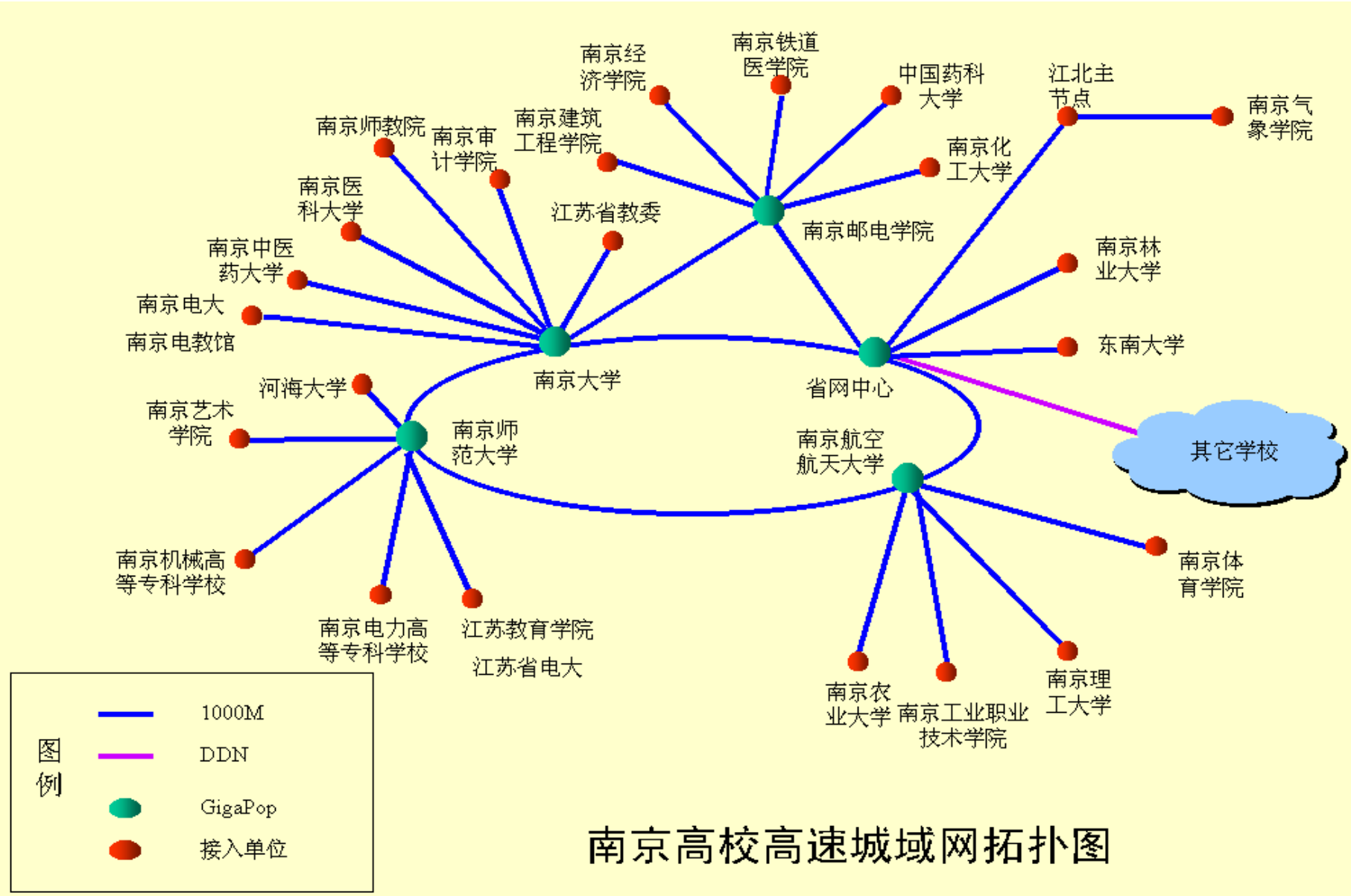


高速校园网(千兆网)



东南大学校园网逻辑拓扑结构图(1999年底)

基于千兆的城域网



南京高校高速城域网拓扑图

第7章 因特网(Internet)

7.1 因特网概述

（1） 因特网的提出

1968年，DARPA资助BBN开发ARPAnet，要求具有抗毁性；

其它厂商也在致力联网技术的研究和应用；

结果：**ARPAnet扩展（原协议不适）及多厂商网络并存（需求互连），**

80年代初，DARPA开始“The Interneting Project”；

采用Cerf.V和Kahn.R提出的TCP/IP协议集（74年）；

政府促进：入网主机必须执行TCP/IP协议集（83年）；

BBN+Berkeley公司将该协议集嵌入UNIX操作系统；

90年代初，MCI、IBM和MERIT公司联合组建“高级网络服务公司ANS”，对因特网实现商业化管理（91年容许商用）；

政府资助 + 商业支持 + 缺乏更多的选择余地等，

促进了**TCP/IP**技术和因特网的普及，渗透全球和各行各业。

（2）因特网大事记—源自Hobbes的互联网大事记

1957年，苏联发射了人类第一颗人造地球卫星"Sputnik"。作为响应，美国国防部(DoD)组建了高级研究计划局(ARPA)，开始将科学技术应用于军事领域 。

1961年7月，MIT的Leonard Kleinrock发表相关分组交换的论文："Information Flow in Large Communication Nets"。

1967年，MIT的Lawrence G. Roberts发表第一篇关于ARPANET设计的论文"Multiple Computer Networks and Intercomputer Communication"。

1968年，Bolt Beranek and Newman (BBN)公司获得研制接口消息处理机(IMP，分组交换机)和研发ARPANET的合同。

1969年，使用BBN的IMP和AT&T的50kpbs的通信线路，构建了4个结点的ARPANET（加州大学洛杉矶分校(UCLA) 、斯坦福研究院(SRI) 、加州大学圣巴巴拉分校(UCSB) 和犹他州大学（Utah））。

1971年，ARPANET上连接了15个节点(23台主机)：UCLA、SRI、UCSB、Univ of Utah、BBN、MIT、RAND、SDC、Harvard、Lincoln Lab、Stanford、UIU(C)、CWRU、CMU、NASA/Ames。

1973年，ARPANET首次进行国际联网：伦敦大学(英国)和NORSAR(挪威)。

因特网大事记—源自Hobbes的互联网大事记（续）

1974年，Vinton Cerf和Bob Kahn发表相关TCP协议设计的论文：A Protocol for Packet Network Interconnection；

1978年，TCP分解成TCP和IP两个协议。

1981年,美国国家科学基金会提供启动资金，Univ of Delaware、Purdue Univ、Univ of Wisconsin、RAND公司和BBN的计算机科学家们合作建立了CSNET(计算机科学网络)，

1982年，首次将“Internet”定义为通过TCP/IP协议连接起来的“internet”。美国国防部(DoD)宣布将TCP/IP协议作为DoD标准网络协议。

1983年1月1日，ARPANET从NCP协议切换为TCP/IP协议。CSNET与ARPANET的网关开始启用，ARPANET分成ARPANET（研究网）和MILNET（军用网）两部分。

1986年，具有五个超级计算中心的NSFnet建成(主干网速率为56K bps)，NSF资助的SDSCNET、JVNCNET、SURANET、NYSERNET接入Internet，开始运营。

1987年，NSF签定合作协议，将NSFnet主干网的管理权移交给由IBM公司、MCI公司和Merit公司联合成立的ANS管理。

1990年，ARPANET停止运营。

1991年，NSF解除了Internet商业应用的限制；中国香港(HK)、中国台湾(TW)连入Internet；

1994年，中国(CN)、中国澳门(MO)连入Internet。

（3） 中国的因特网记事

★ **1986年，国家“七五”项目：OSI标准的制定和验证；**

软件所、15所、清华、复旦、上海交大、南京工学院等9所科研院所，遵循OSI标准，实现上海和北京的机器互连通信，服务：MHS、FTAM和VT；

★ **1988年，中国科研网（CRN）启动；**

1989年5月，CRN通过德国研究网（DFN）的网关与Internet沟通，开通电子邮件和文件传输服务，成员单位包括：电科院、 15所、清华大学、30所、54所、复旦大学和上海交大、东南大学等单位。

★ **1990年10月，中国注册登记顶级域名CN；**

因中国尚未正式接入因特网，德国卡尔斯鲁厄大学运行CN域名服务器。

★ **1993年12月，中关村地区教育/科研示范网络（NCFC）完工**

1989年9月启动，覆盖北大、清华和中科院，高速互联网和超级计算中心。

★ **1994年4月，中国正式接入因特网；**

1992年6月，首次提出接入因特网，美国政府干涉（政治障碍）；

1994年4月，通过美国Sprint公司连入因特网的64K国际专线开通，实现了与因特网的全功能连接，中国成为开通因特网的国家。

★ **1994年5月21日，中国科学院计算机网络信息中心接管中国国家顶级域名(CN)。**

中国因特网记事（续）

★ 1994年9月，电信启动中国公用计算机互联网（Chinanet）；
通过美国Sprint公司，开通2条64K专线：北京和上海，95年1月社会服务。

★ 1994年10月，启动中国教育和科研计算机网（CERNET）；
连接全国大部分高校和中学，推动我国教育和科研事业的发展。

★ 1995年4月，中科院启动“百所联网”工程；

★ 1995年12月开通"中国科技网"（CSTNet）；

★ 1996年9月6日，中国金桥信息网（CHINAGBN）开通；

★ 1997年，公用网（CHINANET）、科技网（CSTNET）、教育网（CERNET）、金桥网（CHINAGBN）互连互通；

★ 1997年6月3日，国务院信息化工作领导小组办公室宣布，在中科院计算机网络信息中心组建中国互联网络信息中心(CNNIC)，行使国家互联网络信息中心的职责，发布中国因特网的统计信息。

★ 1999年2月，中国国家信息安全测评认证中心（CNISTEC）正式运行。……。

（4） 中国因特网统计数据（来源：CNNIC报告）

统计时间	上网计算机数	用户数	注册域名数	WWW站点数	国际容量
1997年10月	29.9万	62万	4066	1500	25.408M
1999年01月	74.7万	210万	18396	5300	143.256M
2000年01月	350万	890万	48695	15153	351M
2001年01月	892万	2250万	122099	265405	2799M
2002年01月	1254万	3370万	127319	277100	7597.5M
2003年01月	2083万	5910万	179544	371600	9380M
2004年01月	3089万	7950万	340040	595550	27216M
2005年01月	4160万	9400万	432077	668900	74429M
2006年01月	4950万	11100万	2592410	694200	136106M
2006年07月	5450万	12300万	2950500	788400	214175M
2007年01月	5940万	13700万	4109020	843000	256696M

上网人数剧增：因特网在中国逐渐普及；
站点数剧增：通过因特网对外宣传，网络市场意识增强；
国际容量剧增：中国进入国际市场和对外交流的步伐加快；
因特网普及的原因：社会需求、用户支持、协议简洁。

（5）因特网的认识 — 一个非常奇特的网络

★ 一无所有的网络：

因特网不属于任何个人、企业和部门；

因特网没有任何固定的设备和传输媒体；

★ 无所不在的网络：

覆盖世界各地、各行各业；

★ 包罗万象的网络：

蕴含的内容异常丰富：天文地理、政治时事、人文喜好等；

蕴含无穷资源的“赛伯（SPACE）”空间。

★ 崇尚自由的网络：

可以自由“接入”和“退出”，做自己想做的事情。

（6） 因特网的管理：

因特网协会（Internet Society—ISOC）

民间组织，志愿者组成，负责技术管理和指导工作；

因特网组织委员会（Internet Architecture Board—IAB）

志愿者组成，制定标准和分配资源（如IP地址）；

因特网工程任务组（Internet Engineering Task Force—IETF）

志愿者组成，讨论因特网的运作和技术问题；

任何人都可以向IETF提出值得研究的问题，当足够多的人对该问题表示兴趣时，形成工作小组，提交研究报告，或者报IAB，形成因特网标准。

所有文档或者标准均以IETF文档形式（RFC XXXX）公布上网，推荐给用户。

例如：ftp.pku.edu.cn上具有所有的IETF文档；

所有文档均予以永久性保留；更新的文档标注以Updates、Updated by、Obsoletes、Obsoleted by字样。

RFC文件举例（源自RFC INDEX）

……

2068 Hypertext Transfer Protocol -- HTTP/1.1.
R. Fielding, J. Gettys, J. Mogul, H. Frystyk,
T. Berners-Lee. January 1997. (Format:
TXT=378114 bytes) (Obsoleted by RFC2616)
(Status: PROPOSED STANDARD)

……

2616 Hypertext Transfer Protocol -- HTTP/1.1.
R. Fielding, J. Gettys,J. Mogul, H. Frystyk,
L. Masinter, P. Leach, T. Berners-Lee. June1999.
(Format: TXT=422317, PS=5529857, PDF=550558 bytes)
(ObsoletesRFC2068) (Updated by RFC2817) (Status:DS)

……

2817 Upgrading to TLS Within HTTP/1.1. R. Khare,
S.Lawrence. May2000. (Format: TXT=27598 bytes)
(Updates RFC2616) (Status: PROPOSED STANDARD)

（7） 因特网的组成

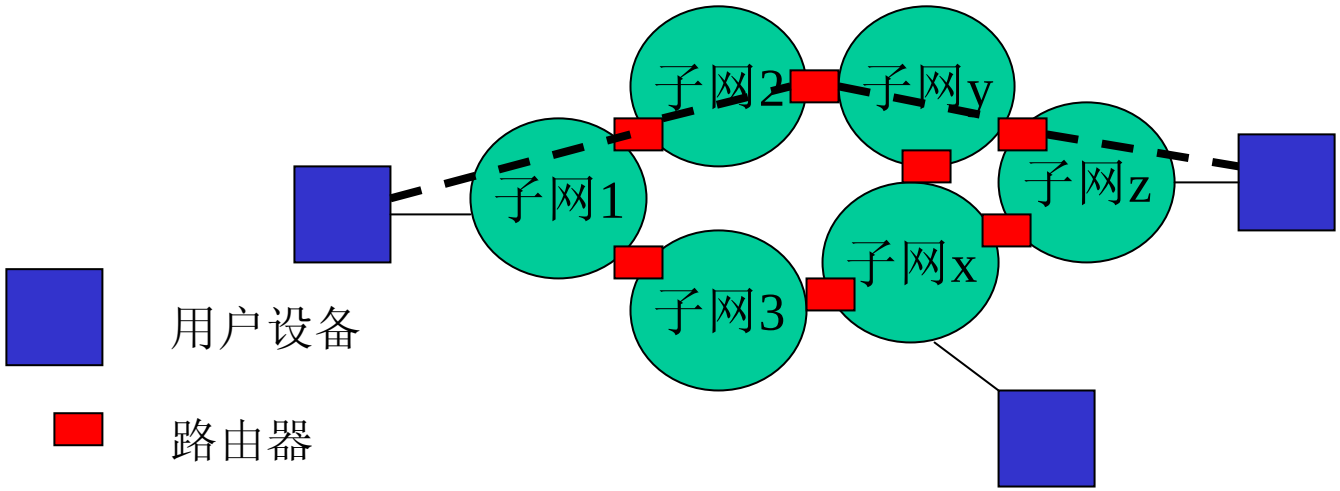
因特网是由网络互连而成的网络；

因特网是由路由器和用户端设备（包括主机）构成的网络：

路由器：互连网络；

用户端设备：辅助用户访问因特网的资源，向因特网提供各种信息资源。

用户端接入因特网的必要条件：具有接入网络的接口（转发服务）、运行统一的软件（**TCP/IP**协议集）、具有全网的唯一标识（**IP**地址）；

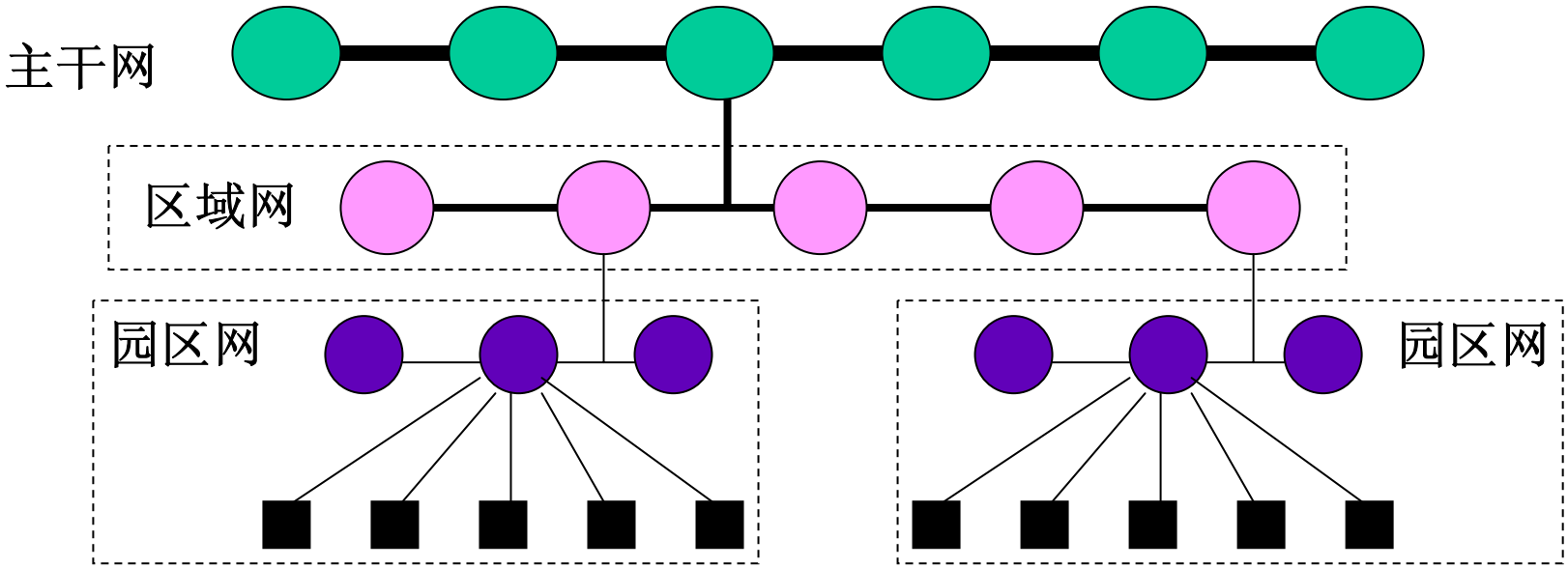


（8） 因特网的结构—层次结构，逐级覆盖和管理

主干网：由代表国家或者行业的有限个中心结点通过专线连接形成；覆盖到国家一级；连接各个国家的因特网互连中心，如中国互联网信息中心（CNNIC）

次级网（区域网）：若干个作为中心结点代理的次中心结点组成，容许级内分级，如CERNET，华东（北）片，…；

园区网（校园网、企业网）：直接面向用户的网络。



7.2 因特网地址

网络地址：标识和识别网络设备的唯一手段；

（1） 因特网地址之一：IP地址

IP地址唯一地标识因特网上的一个设备

上网的每个设备应至少获得一个IP地址。

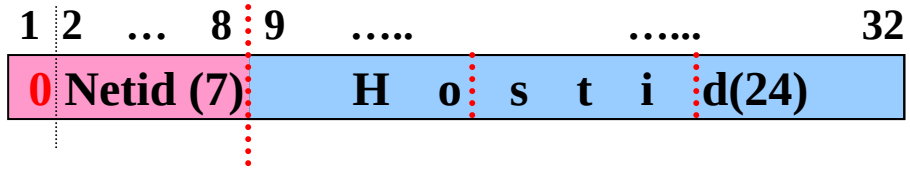
★ IP地址格式（IPv4）：32位（4个字节）

一般格式：类别 + Netid（网络标识）＋ Hostid（主机标识）

点分十进制表示法：X1.X2.X3.X4 例：202.119.11.1

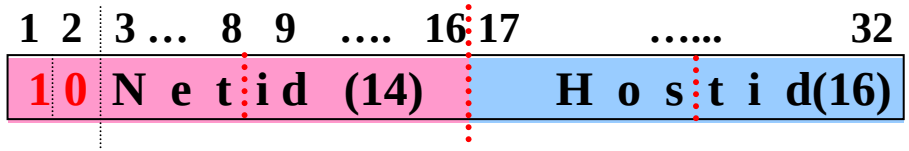
1）A类地址（2^7）：

X1取值：1-126



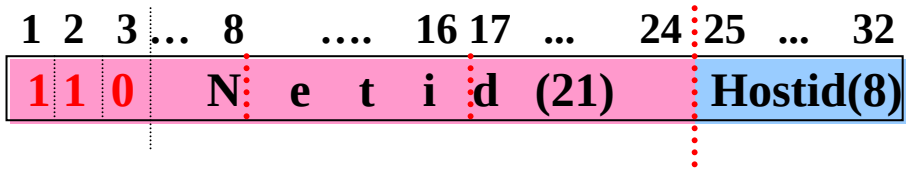
2）B类地址（2^{14}）

X1取值：128-191



3）C类地址（2^{21}）

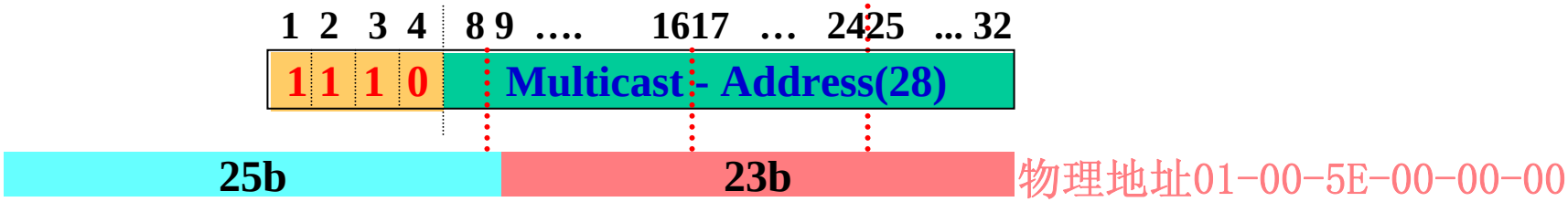
X1取值：192-223



（1） 因特网地址之一：IPv4地址

4）D类地址，用于多址投递系统。

X1取值：224-239



5）E类地址，保留备用。

X1取值：240-255　　一般结构为：1111(4) ...

特殊的地址：

Hostid为全‘0’：不分配给任何主机，表示某网络的网络地址；

Hostid为全‘1’：不分配给任何主机，用作广播地址，对应分组传递给该网络中的所有结点；

32位为全‘1’：　本网的广播地址

32位为全‘0’：　本机地址；

127.0.0.0：　为回送地址(lookback address)，用于网络软件测试及本机进程间通信，（ 127.0.0.1　LocalHost)。

★ IP地址的分配：—子网接入

组网者可以根据*网络的规模*和*用户的数目*，向较高层次的网络管理中心申请IP地址；网络中心根据申请分配若干个连续的网络号（Netid），网内的Hostid则由该网的管理员进行指定。

组网者：中国科技网（crn.cn）
中国教育科研网（edu.cn）
中国电信网（Chinanet）
……。

IP地址分配机构— ICANN（因特网命名和配号协会）；

区域因特网注册机构：**ARIN（美国）、APNIC（亚太）、RIPENCC（欧洲）**

本地因特网注册机构：**CNNIC、…。**

★ IP地址的分配：—子网接入

因特网网络地址数 = 2^7（A）+ 2^{14}（B） + 2^{21}（C）

	2004年1月—CNNIC报告		2007年1月—CNNIC报告	
地区	IP地址个数	折合网数	IP地址个数	折合网数
中国大陆	41456128	2A+120B+146C	98015744	5A+215B+154C
台湾地区	13033216	198B+223C	18158336	1A+21B+19C
香港特区	5037312	76B+221C	6670336	101B+200C
澳门特区	45056	176C	144640	2B+53C

运营商	IP地址个数	折合网数	IP地址个数	折合网数
中国电信	13107200	200B	36090880	2A+38B+180C
中国网通	8273920	126B	20316160	1A+54B
中国教育网	7448576	113B+168C	12184064	185B+234C
中国铁通	2818048	43B	7012352	107B
中国联通	1875968	28B+160C	1835008	28B
中国移动	1736704	26B+128C	1736704	26B+128C
其它	…	…	…	…

★ IP地址的分配：—子网接入

例如：

CERNET华东（北）地区网管中心向CERNET管理中心申请地址；

东南大学向CERNET华东（北）地区网管中心申请地址；

计算机系向东南大学校园网管理中心申请地址；

问题：机构IP地址获取的最小单位：C类地址（256个）

结果：地址浪费、地址紧缺；

解决方法：① 扩展地址空间，**IPv6**（**32**位→**128**位）；

② 缩小地址分配空间：地址掩码（**MASK**）；

③ 动态分配**IP**地址；

④ 地址空间转换：专用**IP**地址（虚拟**IP**地址）。

➢ IPv4地址的扩展—IPv6地址

IPv6地址占128位(16字节），记为：X:X:X:X:X:X:X:X;

其中：X表示4个16进制数:xxxx，每个x取值 0—F;

例如：CDCD:910A:2222:5498:8475:1111:3900:2020,

2000:0123:00FA:CDCD:0000:0000:0000:0001

均为合法的IPv6地址;

为简化表示，起始的0可以省略，若干个0可以用空隙代替，

如： 2000:0123:00FA:CDCD:0000:0000:0000:0001

可表示为：2000:123:FA:CDCD::1;

0000:0000:0000:0000:0000:0000:ABCD:1234

可以简化为： ::ABCD:1234;

注：连续两个冒号“::”在一个地址中只能出现一次;

为了与IPv4兼容，**X:X:X:X:X:X:d.d.d.d**为合法地址;

IPv4地址的IPv6表示：::d.d.d.d，如 ::202.119.11.1

☆ IPv6地址的分配—研究/示范阶段—CNNIC报告

	2005年1月	2006年1月
中国大陆	**14/32+/48**	/29+20/32+2/48
台湾地区	16/32+/48	/21+2/26+/27+/28+20/32+/48
香港特区	4/32+/64	6/32+/64
澳门特区	/32	2/32
中国电信	/32	/32+/48
中国网通	/32	/32
中国教育网	3/32+/48	7/32+/48
中国铁通	/32	/32
中国联通	/32	/32
中国移动	/32	/32
其它	…	…

其中：**M/N是IPv6的地址个数表示方法，等价于M个$2^{(128-N)}$；**
例如：5/32等价于$5*2^{(128-32)}=5*2^{96}$个IPv6地址。

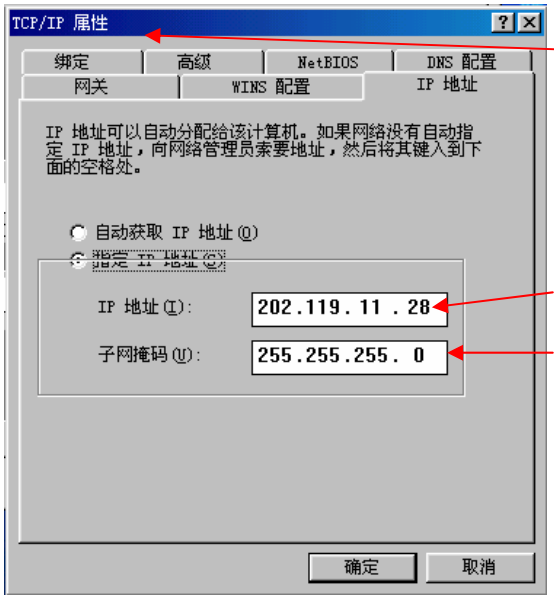
★ 子网掩码地址（subnet mask address)

目的：缩小子网的地址分配空间，减少地址浪费。

方法：将**Hostid**的一部分作为网络**Netid**的延伸；

掩码地址的格式：前**N**位**1**+后**M**位**0**；（**N+M=32**）

掩码地址“与”**IP**地址 = 对应子网的“实际网络地址”。



实际子网地址：

202.119.11.28

∧255.255.255.0

= 202.119.11.0

注意：掩码地址的应用使得实际网络地址（**Netid**）共占**N**位。

☆ 子网掩码地址 — 举例

学校将202.183.56.0（C类地址）分配给两个系，每个系约有120台计算机，则掩码地址可定义为：255.255.255.128

系1的地址范围：202.183.56.1—202.183.56.126

子网地址：202.183.56.0

= 11001010 10110111 00111000 0xxxxxxx

系2的地址范围：202.183.56.129—202.183.56.254

子网地址：202.183.56.128

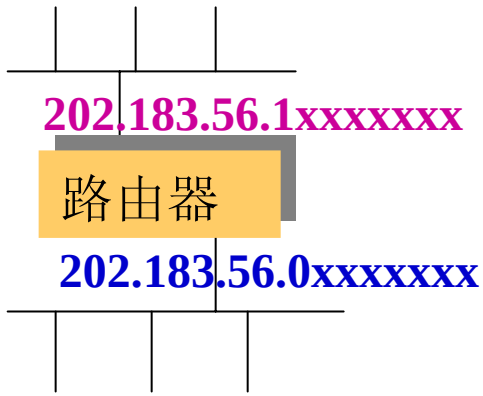
= 11001010 10110111 00111000 1xxxxxxx

正常情况下的掩码地址：

A类地址网络的掩码：255. 0 . 0 . 0

B类地址网络的掩码：255.255. 0 . 0

C类地址网络的掩码：255.255. 255. 0



☆ 子网掩码地址扩展使用—无类域间选路（超网）

目的：扩大C类网的地址空间。

原因：B类网个数偏少，C类网偏多，子网间转发需要路由器的支持；能否减少路由器的个数，或者提高路由效率？

方法：将若干连续的C类网地址聚集使用，也即将C类网的Netid的一部分作为Hostid的延伸；

掩码地址的格式：前N位1+后M位0；（N+M=32）

掩码地址“与”IP地址 = 对应子网的“实际网络地址”。

举例：某系约有1000台计算机，申请4个C类地址：

202.183.0.0—202.183.3.0；

掩码地址可定义为：255.255.252.0；

对应的网络地址（Netid）：202.118.0.0

网络可用IP地址：202.118.0.1 — 202.118.3.254（1022个）

结果：4个C类地址属于一个子网，可由一个路由器负责选路。

结论：子网掩码决定实际子网Netid所占的位数。

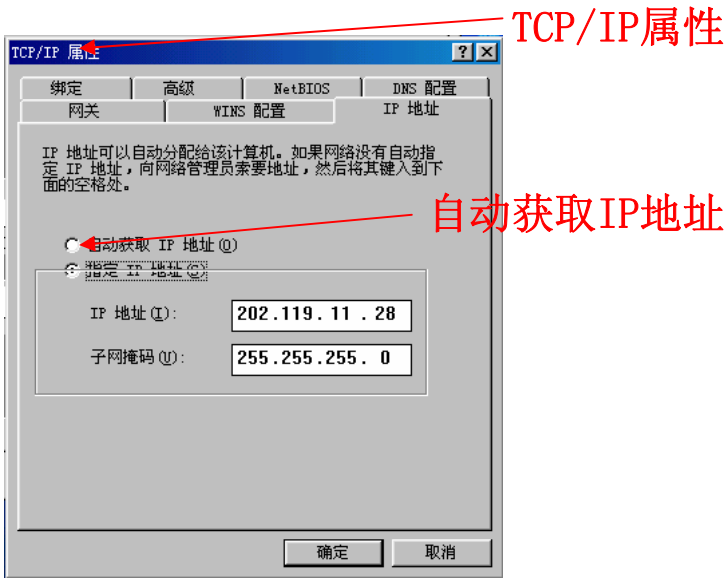
★ 动态分配IP地址

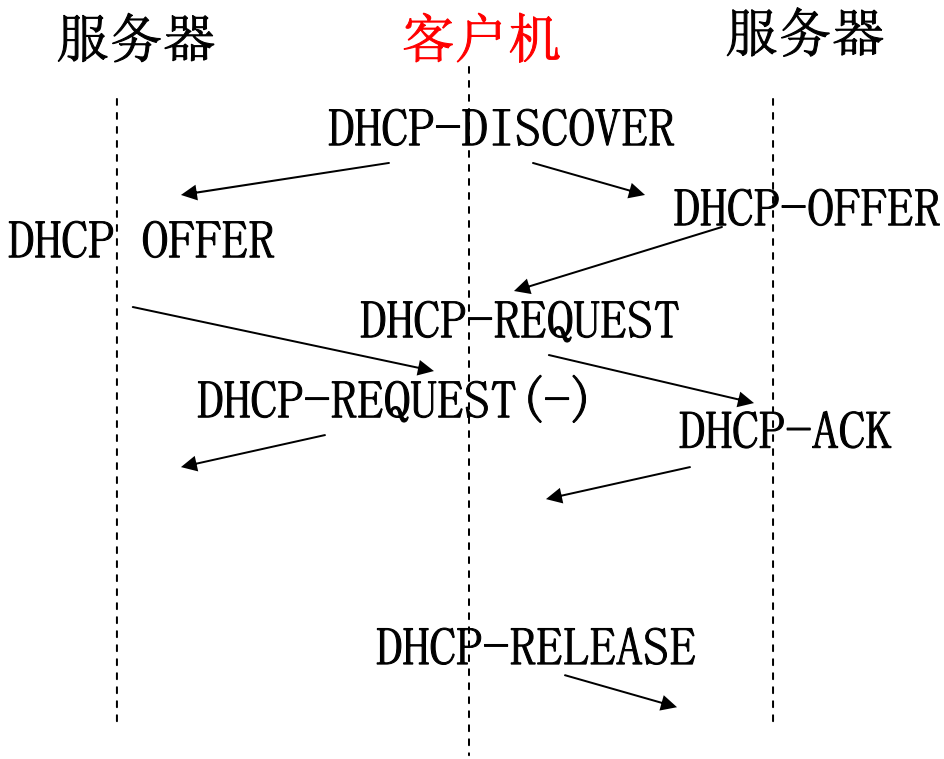
目的：动态调整，按需分配IP地址给希望上网的用户机。

原理：地址分配服务器维护IP地址池，希望上网的用户向其申请IP地址，使用后释放IP地址，提高地址利用率。

过程（RFC2131—动态主机配置协议DHCP）：广播寻找服务器，租用地址。

注：地址租用具有时间限制，续租或者回收。





★ IP地址的补充说明—专用IP地址

TCP /IP协议需要IP地址支持，IP地址资源具有告急的趋势，使用IP地址的组织未必要求接入因特网。

解决方案：定义一些可由用户自行支配使用的IP地址，仅限于用户组织内部使用（RFC1918）

原理：将IP地址分为两大类：

全局IP地址用于因特网—公共主机；

专用IP地址仅限于组织的专用网内部—本地主机。

公共主机和本地主机可以共存于同一网络和进行互访；

本地主机必须经网络地址迁移服务器（NAT或代理服务器）才能访问因特网。

RFC1918定义的专用IP地址：

10.0.0.0 — 10.255.255.255　　1个A类地址；

172.16.0.0 — 172.31.255.255　　16个连续的B类地址；

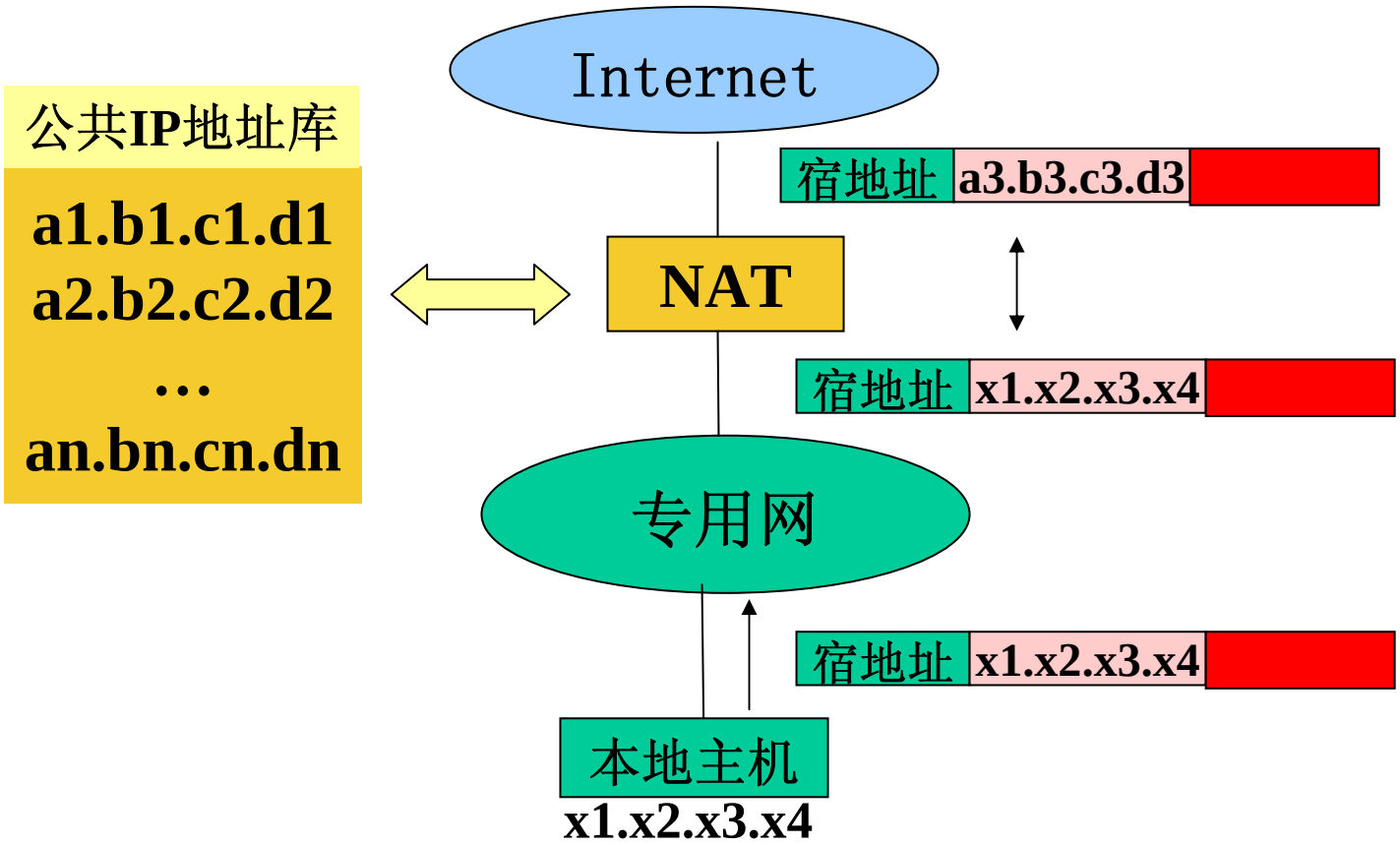
192.168.0.0 — 192.168.255.255　256个连续的C类地址。

业界支持：大多数路由器不转发携带本地IP地址的分组。

☆ 本地主机对外访问—地址迁移

—本地地址仅限于内部使用，外访必须借助于地址迁移技术；

地址迁移原理：NAT服务器维护一组公共IP地址，动态分配给希望对外访问的本地主机（地址迁移），或者仅在内部主机希望对外访问时进行地址迁移；



★ IPv4地址的扩展—IPv6地址

IPv6地址占128位(16字节），记为：X:X:X:X:X:X:X:X;

其中：X表示4个16进制数:xxxx，每个x取值 0—F;

例如：CDCD:910A:2222:5498:8475:1111:3900:2020,

2000:0123:00FA:CDCD:0000:0000:0000:0001

均为合法的IPv6地址;

为简化表示，起始的0可以省略，若干个0可以用空隙代替，

如： 2000:0123:00FA:CDCD:0000:0000:0000:0001

可表示为：2000:123:FA:CDCD::1;

0000:0000:0000:0000:0000:0000:ABCD:1234

可以简化为： ::ABCD:1234;

注：连续两个冒号“::”在一个地址中只能出现一次;

为了与IPv4兼容，X:X:X:X:X:X:d.d.d.d为合法地址;

IPv4地址的IPv6表示：::d.d.d.d，如 ::202.119.11.1

☆ IPv6地址的分配—研究/示范阶段—CNNIC报告

	2005年1月	2007年1月
中国大陆	14/32+/48	/29+20/32+2/48
台湾地区	16/32+/48	/21+2/26+/27+/28+20/32+/48
香港特区	4/32+/64	6/32+/64
澳门特区	/32	2/32
中国电信	/32	/32+/48
中国网通	/32	/32
中国教育网	3/32+/48	7/32+/48
中国铁通	/32	/32
中国联通	/32	/32
中国移动	/32	/32
其 它	…	…

其中：M/N是IPv6的地址个数表示方法，等价于M个$2^{(128-N)}$；
例如：5/32等价于$5*2^{(128-32)}=5*2^{96}$个IPv6地址。

（2） 因特网地址之二：域名地址（Domian Name ）

IP地址的问题：标识网络中的每台主机
用数字表示，缺乏规律、难以记忆；
改善的方法：选用有助记忆的符号名—域名地址；

域名：表示某个范围，采用层次命名结构：
格式： 子域(.父域 (.父域））—体现一种隶属关系
例： **edu.cn** 中国.教育科研网
seu.edu.cn 中国.教育科研网.东南大学

主机名 + 域名 = 域名地址
唯一标识因特网中的一台设备
例：www.seu.edu.cn

域名地址的维护：域名系统(DNS)；
实现域名地址与IP地址的映射；
保证域名地址在因特网中唯一性。

/etc/hosts文件 (Unix 系统）

IP地址	**主机名**
127.0.0.1	**Localhost**
202.119.83.1	**route1**
202.119.83.5	**wwwserver**
202.119.83.29	**ftpserver**
202.119.83.135	**mailserver**
……	

★ 因特网域名的取值

因特网定义了域名的格式和主要域名的取值，
任何组织均可根据域名语法构造本组织内部的域名。

一级域名（因特网规定了一些国际通用的域名）

.com　.edu　.gov　.mil　.net　.org　.int

国家名　**.cn　.ca　……**

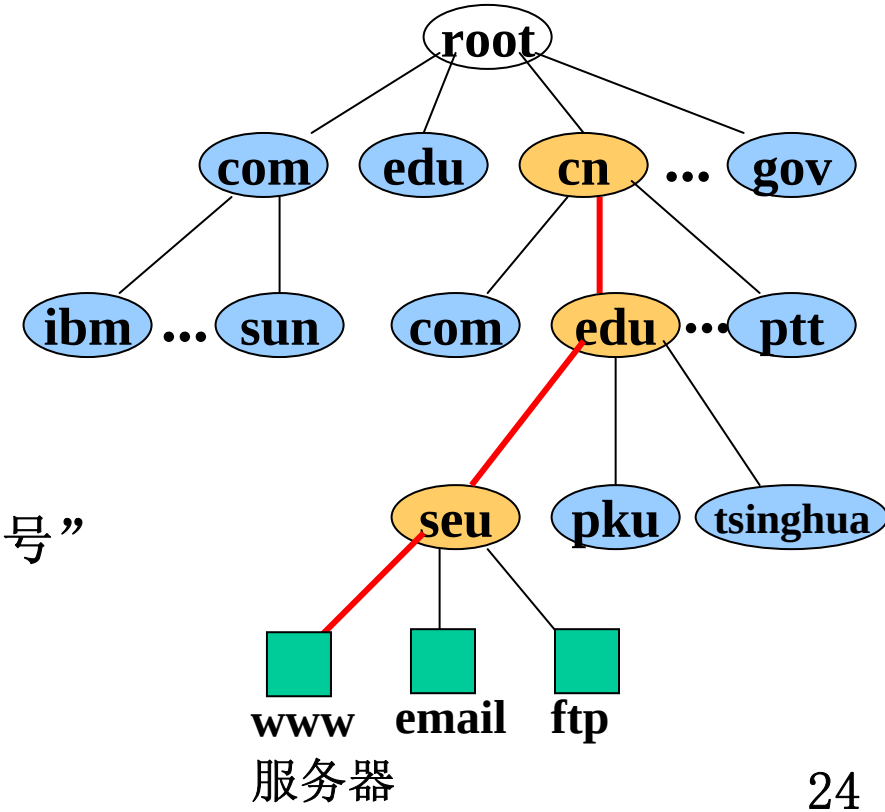
域名注册：

CNNIC——中国域名注册管理机构

www.cnnic.net.cn

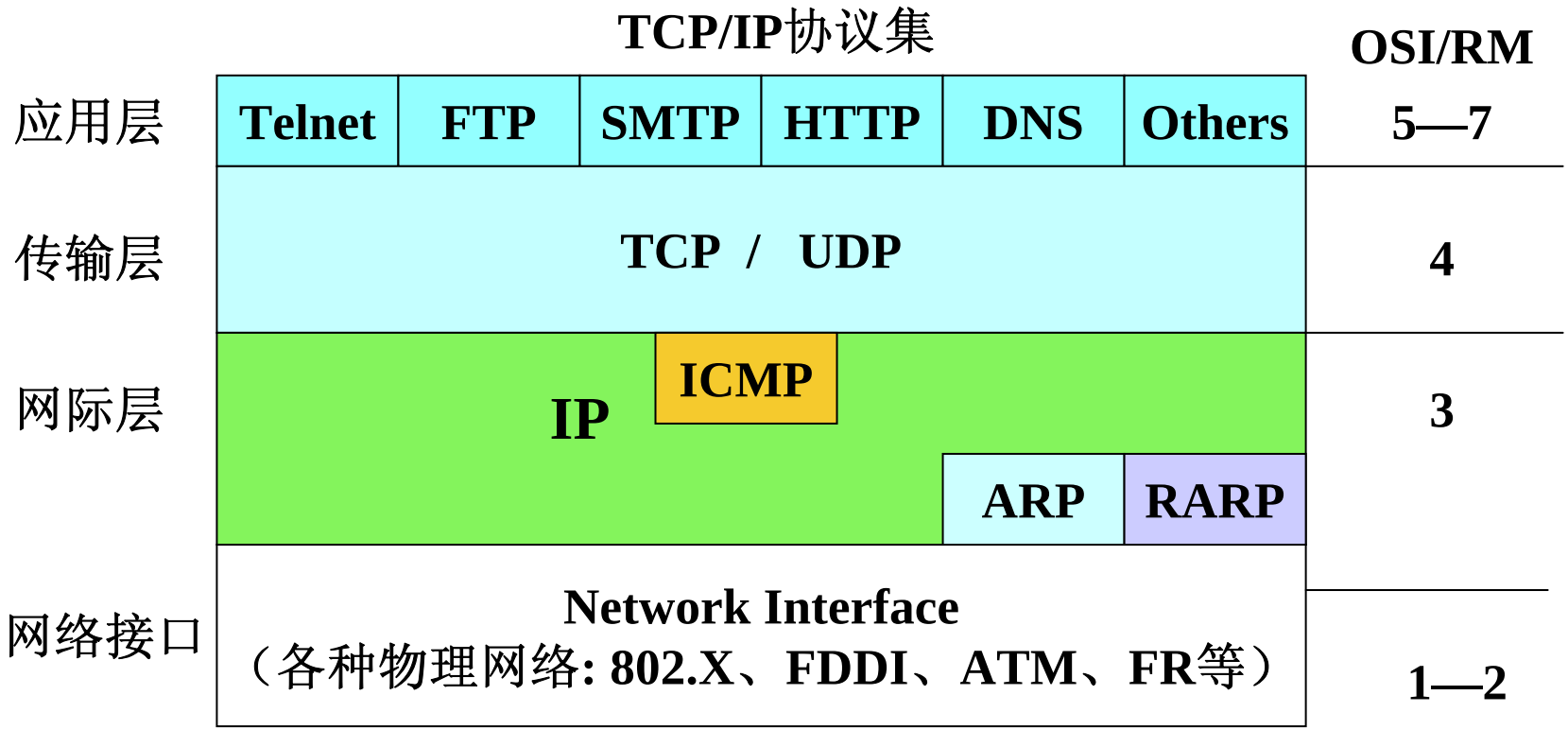
结点主机：因特网上的计算机，
主机名.域名（主机所在域）
www.seu.edu.cn

因特网用户名：结点主机上的用户“帐号”
用户名@结点主机
gwu@seu.edu.cn



7.3 因特网协议集

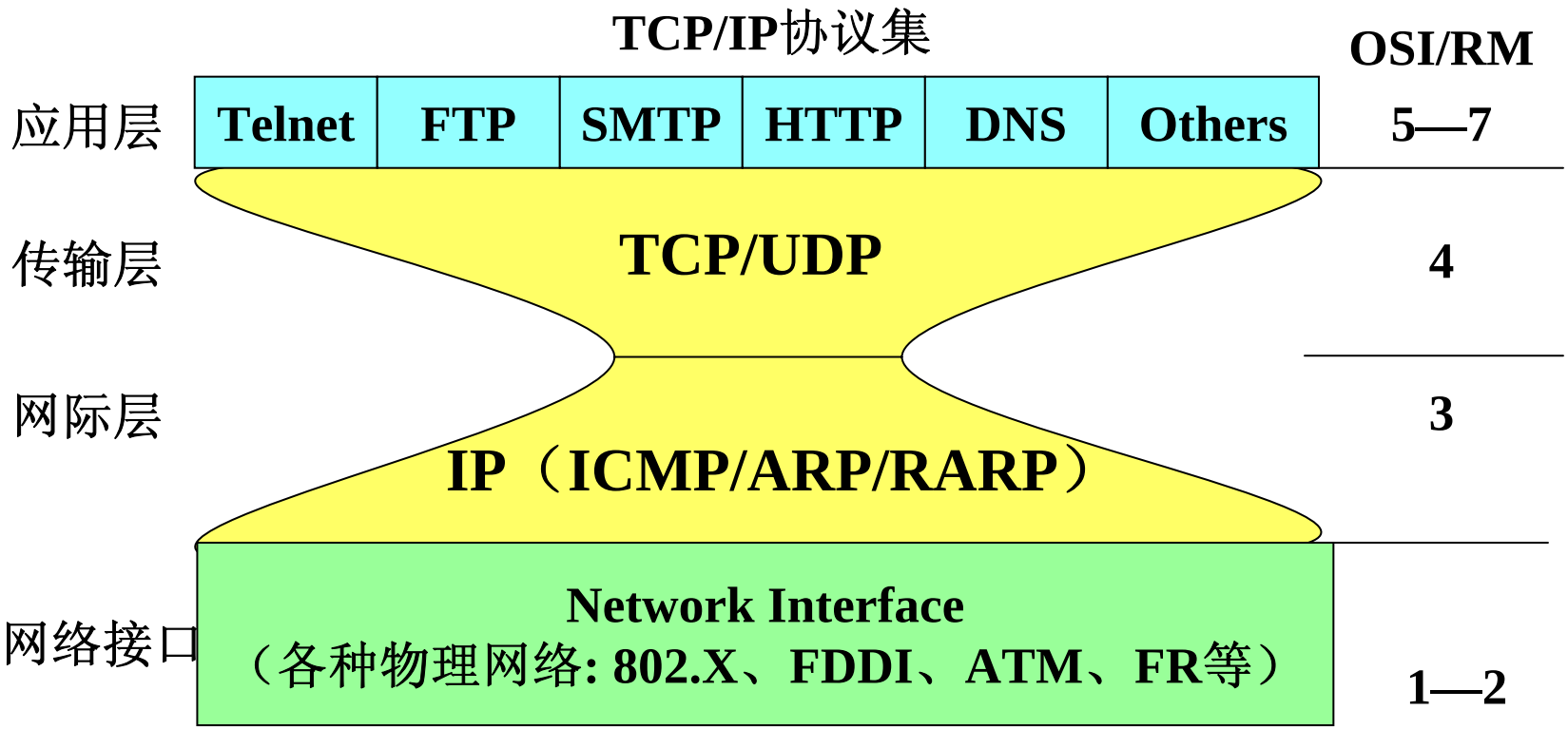
（1） 因特网的结构/协议集：



Telnet：远程登录； **FTP**：文件传输； **SMTP**：电子邮件； **DNS**：域名系统；
HTTP：超文本传输； **TCP**：传输控制协议； **UDP**：用户数据报协议；
ICMP：网际报文控制；**IP**：网际协议；**ARP**：地址解析；**RARP**：反向地址解析。

特点：利用网络接口屏蔽不同子网的差异，定义相同的高层（IP之上层）协议，提供多种应用服务。

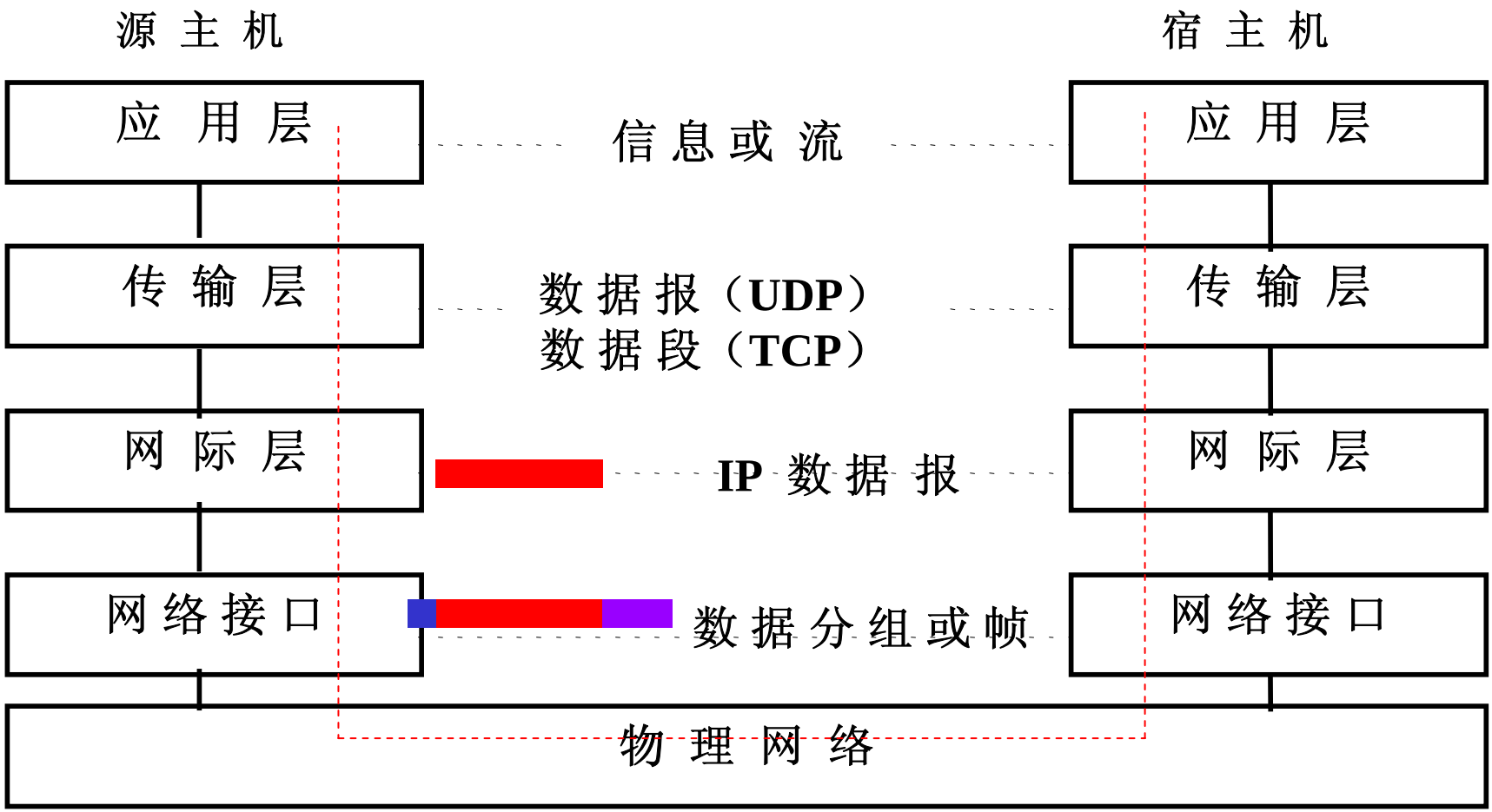
因特网的体系结构—沙漏型结构：



因特网结构的包容性：上可支持各种应用，下可兼容/依托各种物理网络，简化中间结构；

有人预测，任何对IP的功能扩展都有违于该包容性原则，可能都无法推行；认为相应的扩展应在应用层完成—覆盖网。

（2） 基于因特网的信息流


源 主 机
宿 主 机
应 用 层
信 息 或 流
应 用 层
传 输 层
数 据 报（UDP）
数 据 段（TCP）
传 输 层
网 际 层
IP 数 据 报
网 际 层
网 络 接 口
数 据 分 组 或 帧
网 络 接 口
物 理 网 络


帧
帧尾
帧头
IP数据报

7.4 地址映射

（1） 因特网上的地址类型：

★ 域名地址：人类识别因特网中的设施；

★ IP地址：因特网设施可识别的地址；

★ 物理地址：支撑网络中标识/识别设施的地址；

以太网：网卡MAC地址

X.25网：X.25地址

★ 地址映射：

物理地址 ⟷ IP地址 ⟷ 域名地址

（2）IP地址向物理地址的映射——ARP（地址解析协议）

★ 具有广播能力的网络（如，各种类型的局域网）

主机（或路由器）A与主机B进行数据通信：

① A发ARP请求广播帧（带接收方IP地址、本机IP地址和物理地址）；

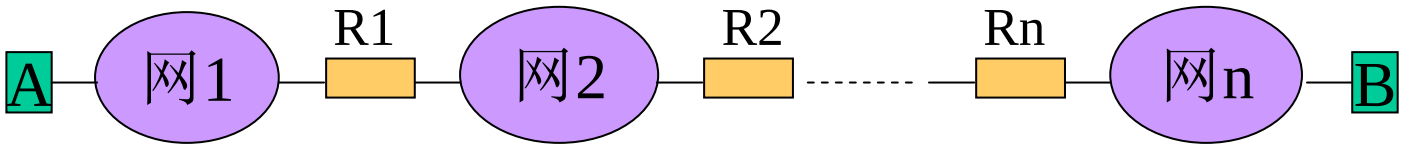
② B收到A发来的ARP请求，予以响应，发ARP响应帧，返回自己的物理地址

③ 双方用物理地址在物理网中进行数据通信。

（2）IP地址向物理地址的映射——ARP（续）

★ 无广播能力的网络，或者需要跨网解析

借助因特网网关（路由器 R）实现



路由器代替请求者转发**ARP**请求；

如果属于同一个子网，直接转发给特定**IP**地址的结点；

否则，转发给其它的路由器；…。

同时，路由器也将收到的**ARP**响应沿原路径反馈请求者。

路由器（或者服务器）记录相应**IP**地址/物理地址的映射表；

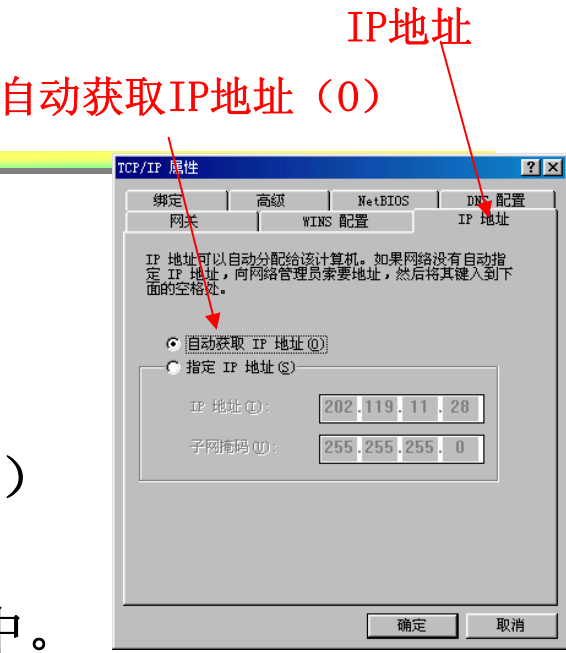
地址解析是一个物理网络的局部过程。

也即：A或者得到 B 的物理地址（本网），

或者得到 R1 的物理地址（跨网）。

（3）物理地址向IP地址的映射

——RARP（反向地址解析协议）



★ 无盘工作站： 网卡上增加了专用的ROM模块

启动时通过网络由服务器引导（BOOTP）

其IP地址保留在服务器上。

当主机加电时，ROM模块中驻留的软件（以广播的方式）发出携带本结点物理地址的RARP请求，

服务器予以响应，返回该结点的IP地址，保存在内存中。

★ 动态主机配置协议（DHCP—RFC1531）

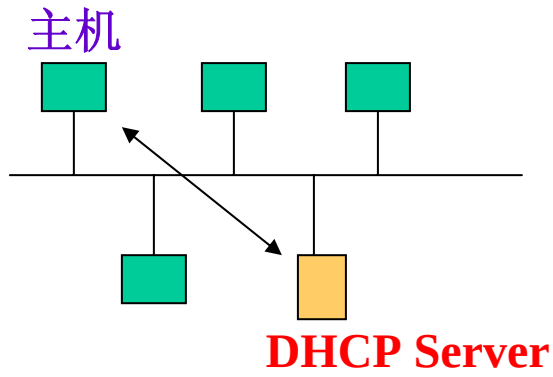
提高IP地址的利用率借助于地址服务器动态获取IP地址

客户端IP地址设为自动获取IP地址

启动时，向DHCP服务器发出请求IP地址的DHCP请求；

DHCP服务器接到DHCP请求时，分配一个空闲的IP地址。

IP地址的分配和回收策略：租用期；

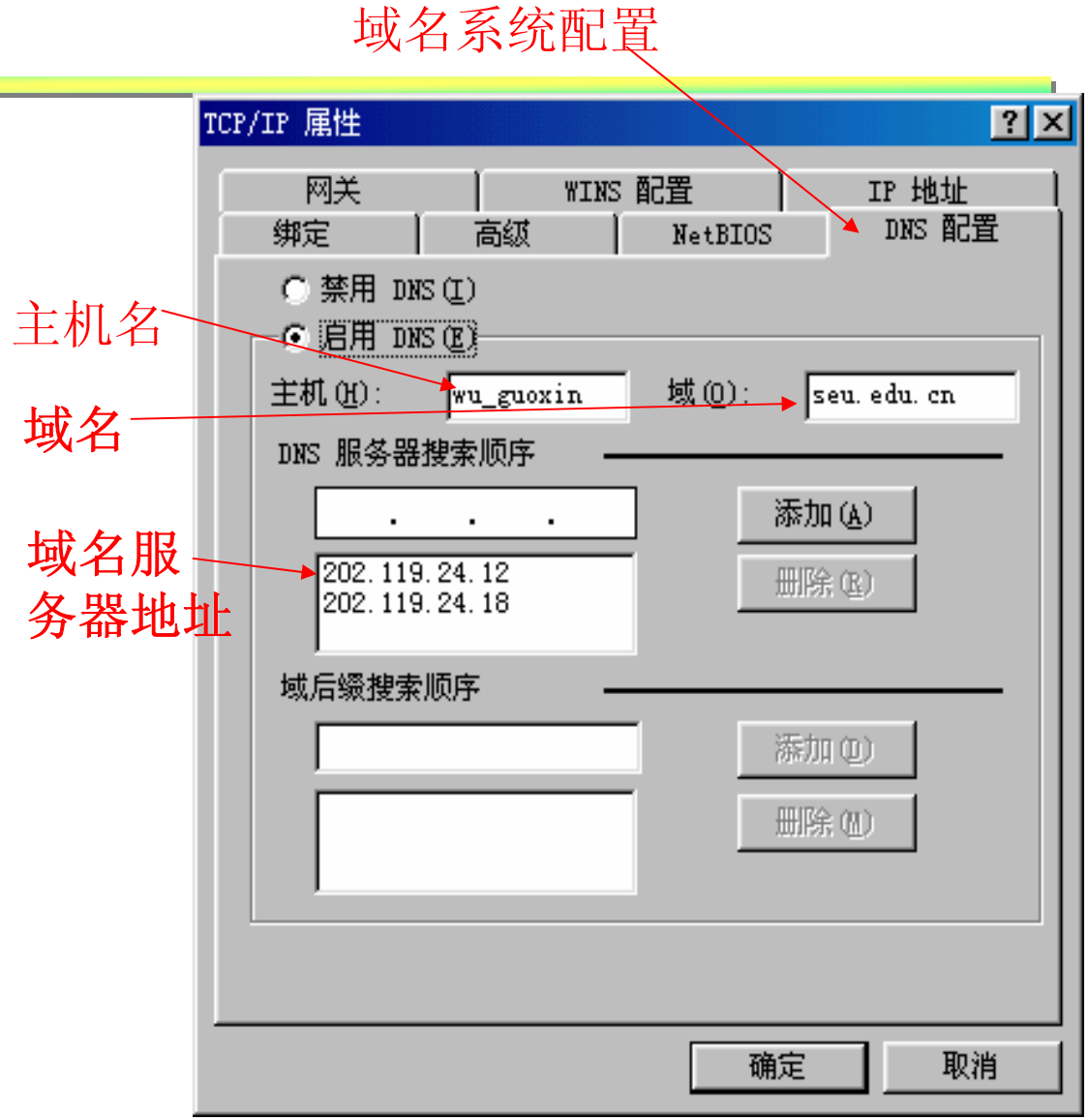


（4） 域名地址和IP地址的映射
—DNS（域名系统）

★ 域名服务器

因特网中设置一系列的域名服务器，记录本域内的主机域名和IP地址的映射信息，以及上一级域名服务器的IP地址等，并以C/S模式响应客户机的请求。

为保证用户主机可以访问因特网，主机应保存域名服务器的信息；



Windows 98上DNS配置

★ DNS的工作过程—逐级解析

举例： 美国某大学的用户访问 **www.seu.edu.cn**

用户主机：**user.mit.edu**

应用程序调用**Gethostbyname( )--** resolver

主机 ⟶ MIT域名服务器（请求解析www. seu. edu. cn）

User ⟶ **MIT DNS**

MIT DNS ⟶ **edu DNS**

root

MIT DNS ⟶ **root**

cn DNS

MIT DNS ⟶ **cn DNS**

MIT DNS ⟶ **edu.cn DNS**

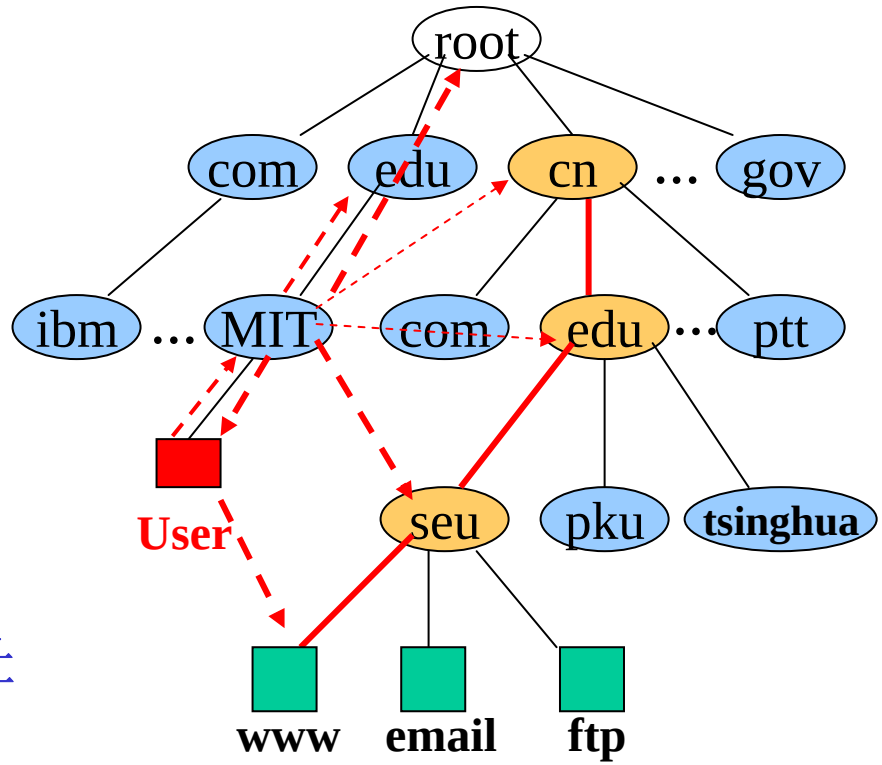
MIT DNS ⟶ **seu.edu.cn**

www. seu. edu. cn

MIT DNS ⟶ **User**

返回www.seu.edu.cn的IP地址

User ⟷ **www.seu.edu.cn**



DNS的扩展说明

★ **DNS域名查询的效率改进：**

☆ 扩充第一级域名服务器的域名表（域名数据库）；

☆ 第一级域名服务器直接向根服务器查询；

☆ 充分利用机器的高速缓存，暂存解析后的IP地址；

理由：用户可能习惯连续地访问相同的系统。

★ 补充说明

☆ 一台计算机可以有多个域名；

☆ 按名访问，无需知道该计算机的物理位置；

☆ 主机IP地址改变，不会影响对该主机的访问；

☆ 主机IP地址改变，需要在本地DNS服务器上进行维护。

（修改DNS数据库）

7.5 IP协议(RFC 791)

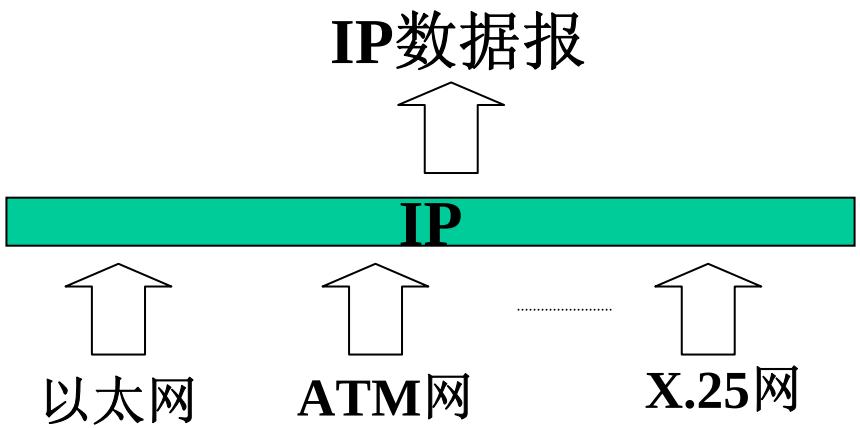
IP协议：因特网中的基础协议；

IP数据报：由IP协议控制传输的协议单元。

IP数据报中含有发/收方的IP地址。

IP协议屏蔽下层各种物理网络的差异，

向上层（主要是TCP层或UDP层）提供统一的IP数据报。



（1） IP提供的服务

IP提供无连接的、不可靠的、尽力的数据报投递服务

★ 无连接的投递服务

每个数据报独立处理和传输，

一台主机发出的数据报序列，可能取不同的路径，

甚至其中的一部分数据报会在传输过程中丢失；

★ 不可靠的投递服务

IP协议本身不保证数据报投递的结果。

在传输的过程中，数据报可能会丢失、重复、延迟和乱序等，

IP协议不对内容作任何检测，也不将这些结果通知收发双方；

IP数据报的丢失，通过路由器发ICMP报文告知；

必要时，由高层实体（如TCP）负责差错恢复动作。

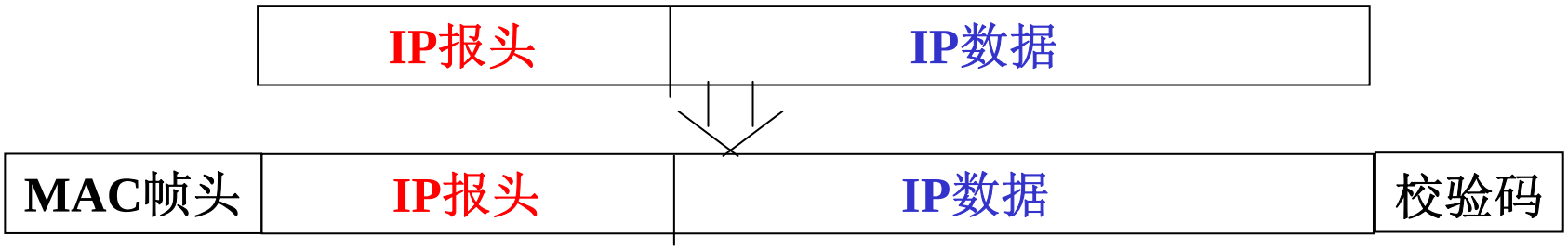
★ 尽力投递服务

执行数据报的分段和封装，以适应具体的传输网络，

由最终结点的IP模块进行合段处理。

（2） IP数据报封装

网络接口模块负责将IP数据报封装到具体网络的帧（LAN）或者分组（X25网络）中。



不同物理网络对传输的帧/分组的体积有不同的规定；

最大传输单元（**MTU—Maximun Transfer Unit**）

当数据报长度>**MTU**时，需对数据报分段。

对应每个物理网络的封装，都有一个**RFC**文档与之对应；

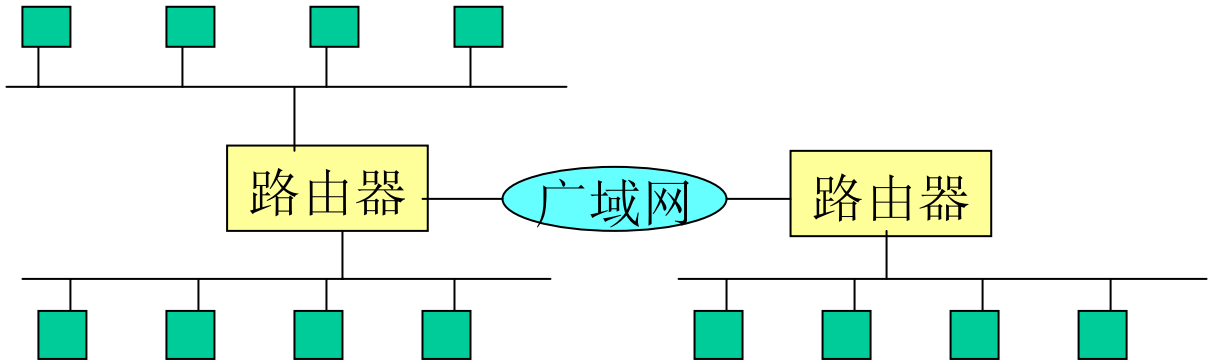
例：**RFC894 IP over Ethernet networks**

RFC1188 IP over FDDI networks

RFC1932 IP over ATM

（3） IP路由

IP数据报的传输可能需要跨越多个子网，子网之间的数据报传输由路由器实现



IP路由算法：

发送结点（或者路由器）根据接收方地址和缓存的信息，判断是否为本网投递

本网投递：

（1）利用**ARP**，获得接收方物理地址

（2）**IP**数据报进行分段和封装

（3）将数据帧发往目的地

跨网投递：

（1）利用**ARP**，获得路由器的对应端口的物理地址

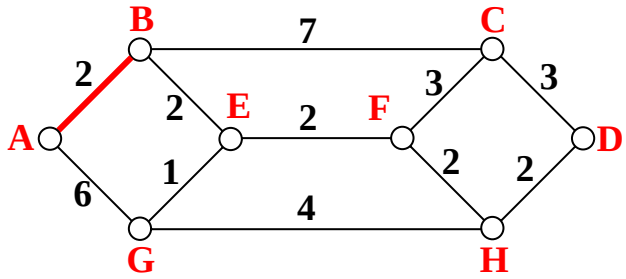
（2）**IP**数据报进行分段和封装

（3）将数据帧/分组发往路由器

……

最短路径算法举例（Dijkstra算法）：A—D

算法的核心：搜索最短路径距离的结点；
距离：通常以邻居的响应时间为依据；



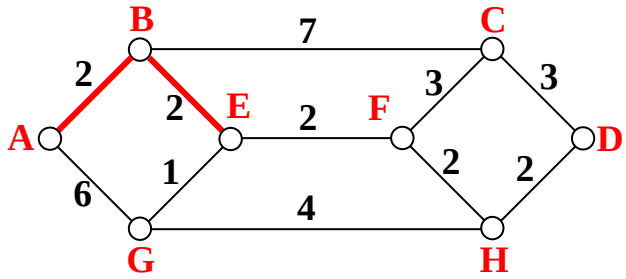
目的地	A	B	C	D	E	F	G	H
距　离	0	2	∞	∞	∞	∞	6	∞
出　口	A	B					G	
路　径	A	AB					AG	

最短路径距离的结点加入示意：

A-B

最短路径算法举例（Dijkstra算法）：A—D

算法的核心：搜索最短路径距离的结点；
距离：通常以邻居的响应时间为依据；



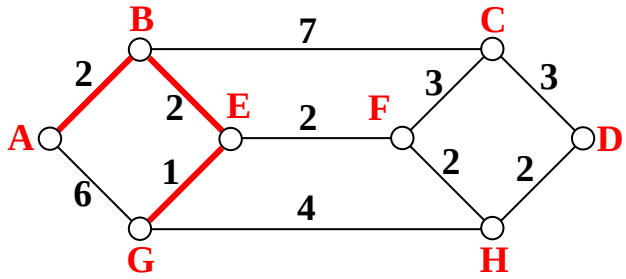
目的地	A	B	C	D	E	F	G	H
距　离	0	2	∞	∞	4	∞	6	∞
出　口	A	B			B		G	
路　径	A	AB			ABE		AG	

最短路径距离的结点加入示意：

A-B-E

最短路径算法举例（Dijkstra算法）：A—D

算法的核心：搜索最短路径距离的结点；
距离：通常以邻居的响应时间为依据；



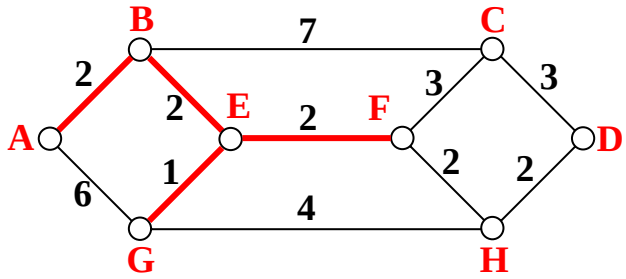
目的地	A	B	C	D	E	F	G	H
距　离	0	2	∞	∞	4	∞	5	∞
出　口	A	B			B		B	
路　径	A	AB			ABE		ABEG	

最短路径距离的结点加入示意：

A-B-E-G

最短路径算法举例（Dijkstra算法）：A—D

算法的核心：搜索最短路径距离的结点；
距离：通常以邻居的响应时间为依据；



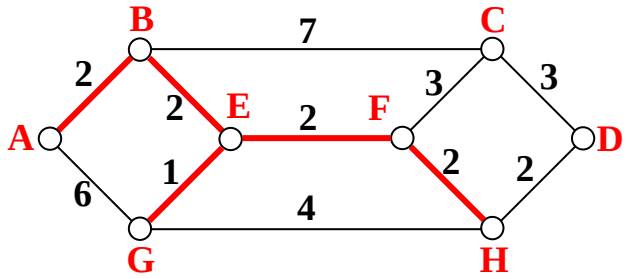
目的地	A	B	C	D	E	F	G	H
距　离	0	2	∞	∞	4	6	5	∞
出　口	A	B			B	B	B	
路　径	A	AB			ABE	ABEF	ABEG	

最短路径距离的结点加入示意：

A-B-E-G-F

最短路径算法举例（Dijkstra算法）：A—D

算法的核心：搜索最短路径距离的结点；
距离：通常以邻居的响应时间为依据；



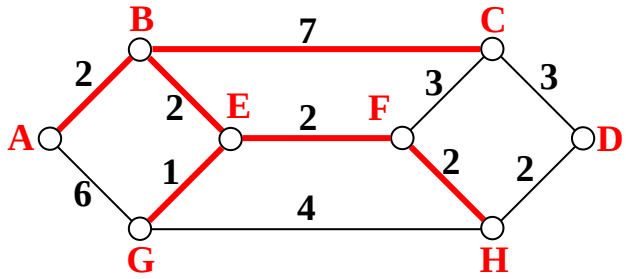
目的地	A	B	C	D	E	F	G	H
距　离	0	2	∞	∞	4	6	5	8
出　口	A	B			B	B	B	B
路　径	A	AB			ABE	ABEF	ABEG	ABEFH

最短路径距离的结点加入示意：

A-B-E-G-F-H

最短路径算法举例（Dijkstra算法）：A—D

算法的核心：搜索最短路径距离的结点；
距离：通常以邻居的响应时间为依据；



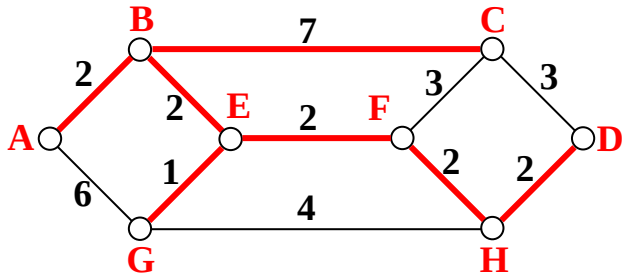
目的地	A	B	C	D	E	F	G	H
距　离	0	2	9	∞	4	6	5	8
出　口	A	B	B		B	B	B	B
路　径	A	AB	ABC		ABE	ABEF	ABEG	ABEFH

最短路径距离的结点加入示意：

A-B-E-G-F-H-C

最短路径算法举例（Dijkstra算法）：A—D

算法的核心：搜索最短路径距离的结点；
距离：通常以邻居的响应时间为依据；



目的地	A	B	C	D	E	F	G	H
距　离	0	2	9	10	4	6	5	8
出　口	A	B	B	B	B	B	B	B
路　径	A	AB	ABC	ABEFHD	ABE	ABEF	ABEG	ABEFH

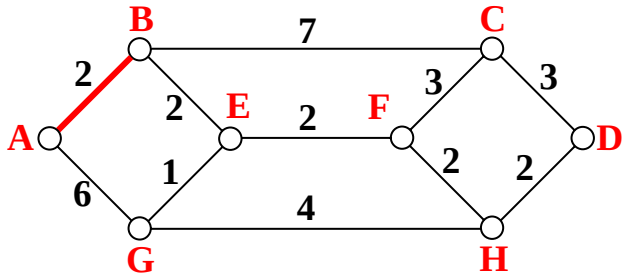
最短路径距离的结点加入示意：

A-B-E-G-F-H-C-D

A至所有结点的最短距离。

路由表变化示意：

算法的核心：邻居间定期交换路由表，
根据邻居结点路由表信息进行调整；
目的：寻找至其他结点的最短距离（邻居的响应时间可测）；

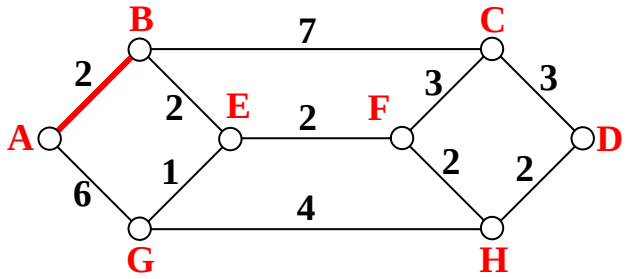


各结点路由表示意：

目的地	A	B	C	D	E	F	G	H
A-目的地	0/A	2/B	∞	∞	∞	∞	6/G	∞
B-目的地	2/A	0/B	7/C	∞	2/E	∞	∞	∞
C-目的地	∞	7/B	0/C	3/D	∞	3/F	∞	∞
D-目的地	∞	∞	3/C	0/D	∞	∞	∞	2/H
E-目的地	∞	2/B	∞	∞	0/E	2/F	1/G	∞
F-目的地	∞	∞	3/C	∞	2/E	0/F	∞	2/H
G-目的地	6/A	∞	∞	∞	1/E	∞	0/G	4/H
H-目的地	∞	∞	∞	2/D	∞	2/F	4/G	0/H

路由表变化示意：

算法的核心：邻居间定期交换路由表，
根据邻居结点路由表信息进行调整；
目的：寻找至其他结点的最短距离（邻居的响应时间可测）；



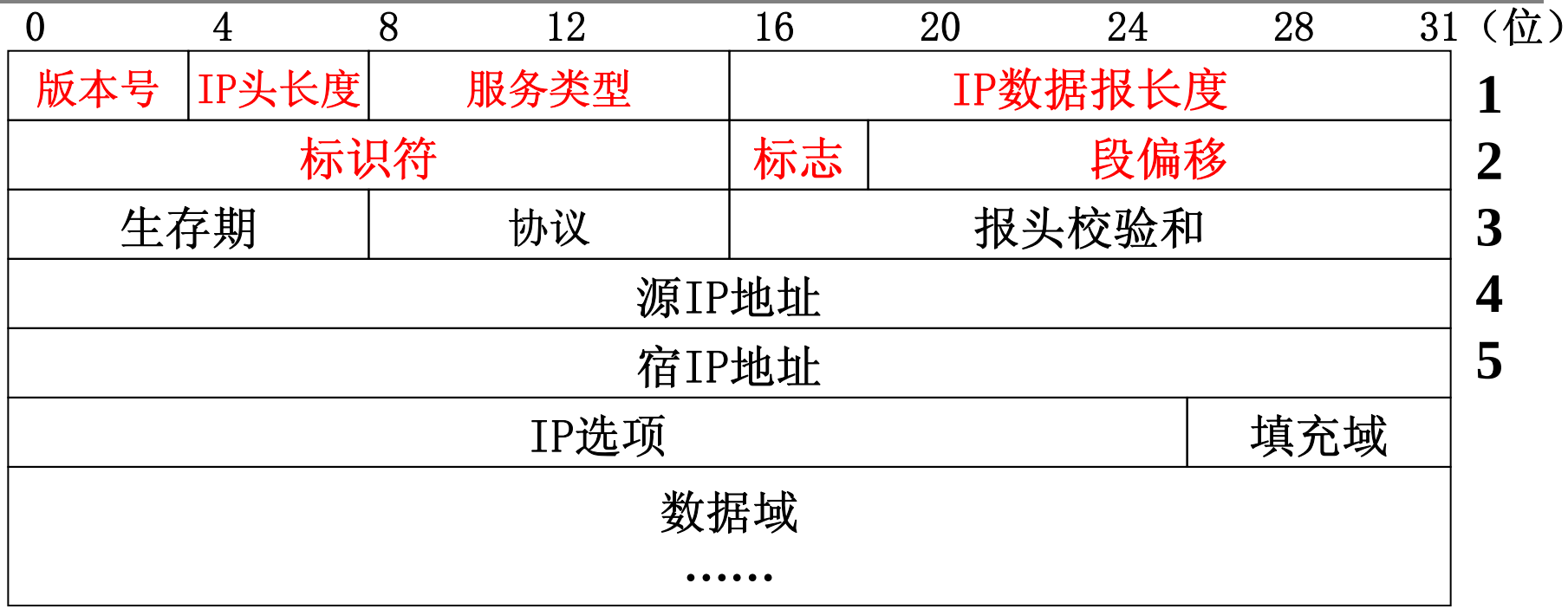
第一次调整前（A路由表）

目的地	A	B	C	D	E	F	G	H
A-路由表	0/A	2/B	∞	∞	∞	∞	6/G	∞
B-路由表	2/A	0/B	7/C	∞	2/E	∞	∞	∞
G-路由表	6/A	∞	∞	∞	1/E	∞	0/G	4/H

第一次调整后（A路由表）

目的地	A	B	C	D	E	F	G	H
A-路由表	0/A	2/B	9/B	∞	4/B	∞	6/G	10/G
B-路由表	2/A	0/B	7/C	10/C	2/E	4/E	8/E	∞
G-路由表	6/A	2/E	∞	6/H	1/E	3/E	0/G	4/H

（4） IP数据报结构（IPv4）



版本号：当前使用的协议版本，如**4—IPv4**；

IP报头长度：以**32**位的字长为单位，基本长度为**5**（**20**字节）；

服务类型（8位）：优先级（**3**）、延迟（**1**）、吞吐率（**1**）、可靠性（**1**）；

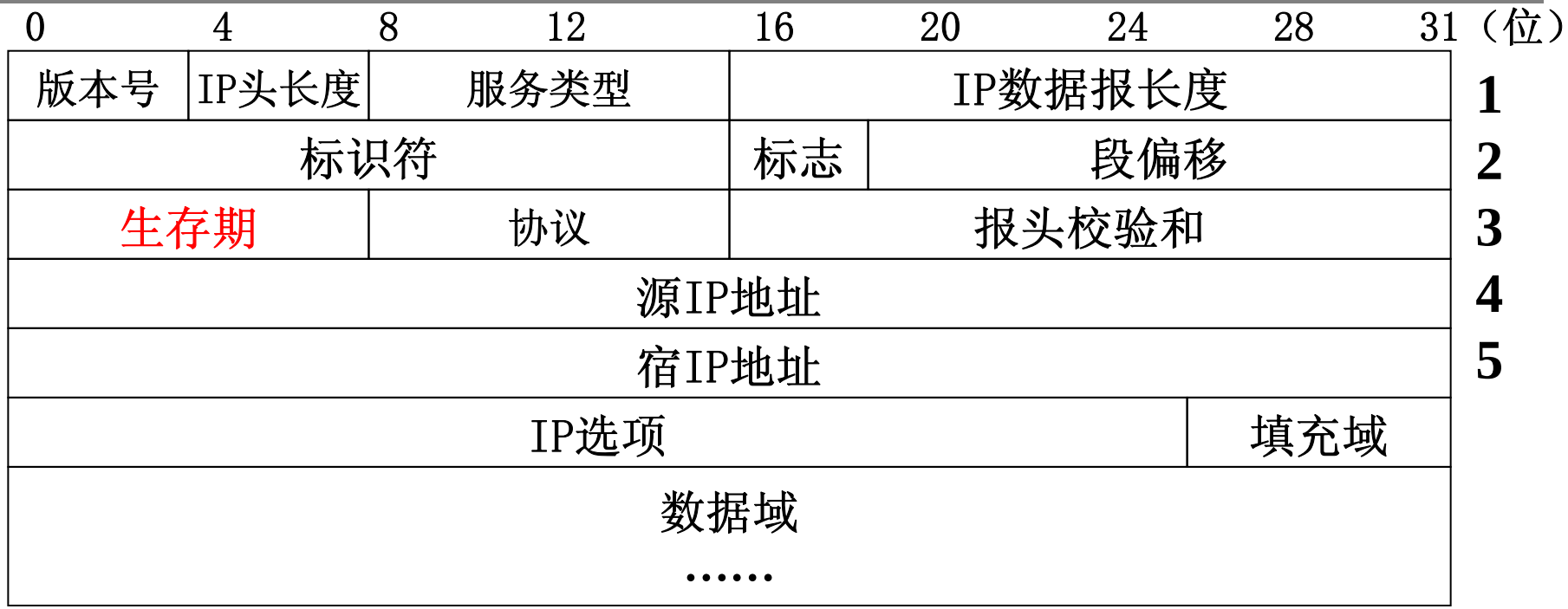
IP数据报长度：整个**IP**数据报的长度，以字节为单位；

标识符（16位）：数字串，标识本**IP**报文，发方指定，用于辅助数据分段；

标志（3位）：保留（**0**），容许/不容许分段（**0/1**），最后/更多段（**0/1**）；

段偏移（13位）：本段在原始数据报中的位置；

（4） IP数据报结构（IPv4）



生存期（8位）：本段可在网络中停留（生存）的时间。常以跳数为单位；

目的：避免IP数据报在网络中无限制的转发（独立投递）。

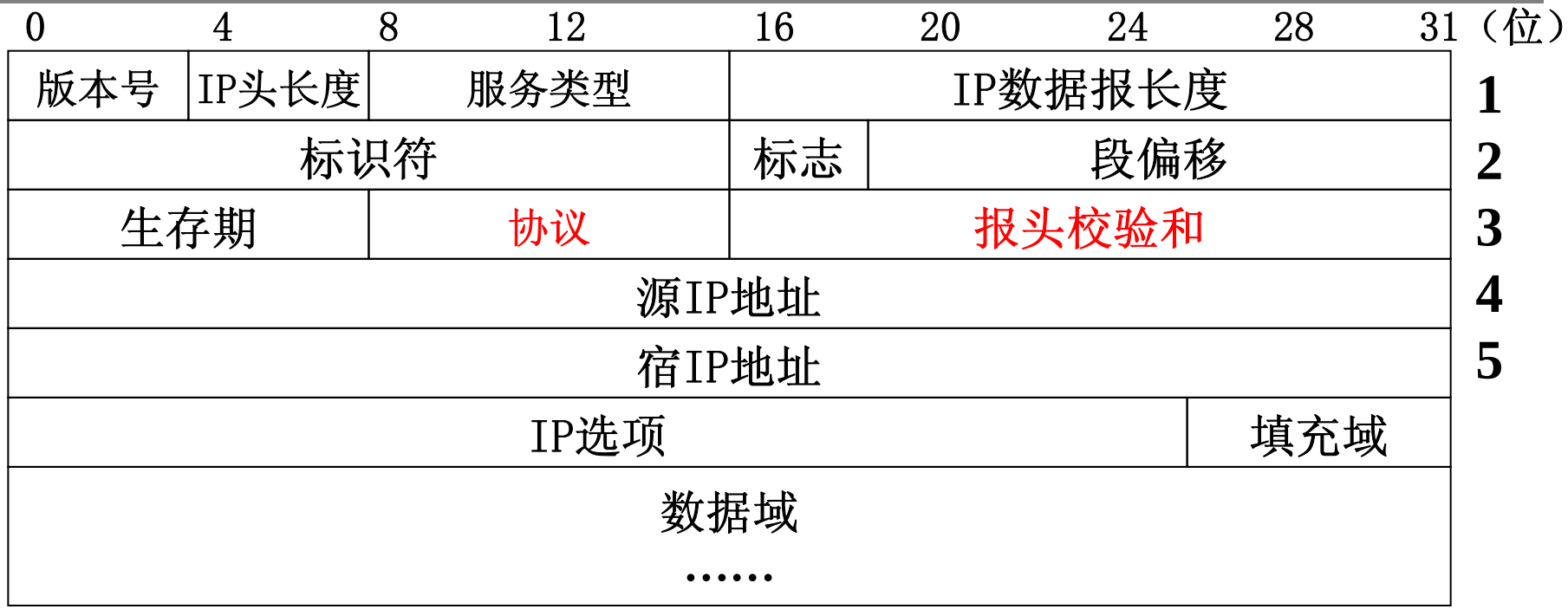
处理过程：数据报的源发端设置该字段，

每经过一个路由器（分析IP数据报），数值减一；

该值为 0 表示该数据报生存期已满，丢弃本数据报；

否则，转发。

（4） IP数据报结构（IPv4）



协议（8位）：本段携带的上层用户协议，如TCP/6、UDP/17等；

WindowsXP见：C:\WINDOWS\system32\drivers\etc\protocol文件

校验和（16位）：IP头部的16位和的补码。

用于路由器检测IP数据报报头的正确性；

校验算法：头部的16位为单位的反码求和的反码（初始置0）；

报头的内容在经过路由器时发生变化，IP数据报途径的每个路由器重新计算生成该值，并由下一跳的路由器验证；

路由器的IP模块丢弃出错的数据报，并通过ICMP告知发送方。

★ 数据报分段示意图：

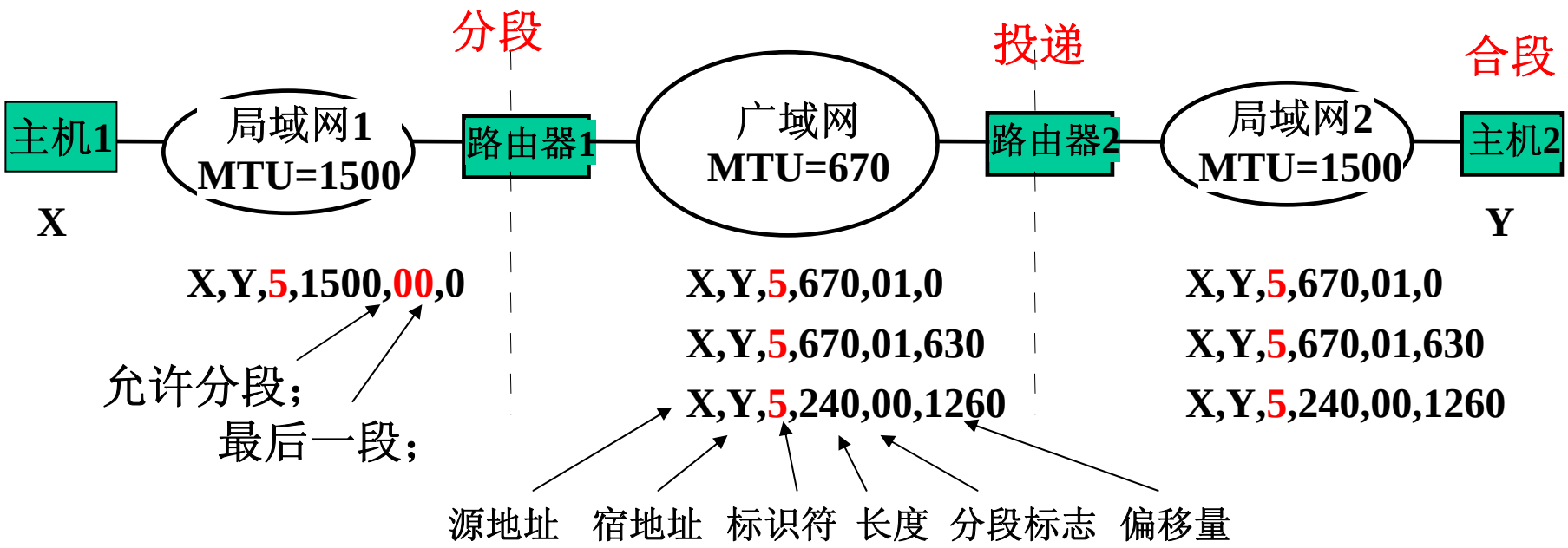
假设：IP头部不含任何选项，则IP头部占20字节；

局域网的帧头/帧尾，或者广域网的分组头等占20字节。

则：局域网1上长度为1500字节的IP数据报含用户数据1460字节；

广域网的用户数据实际长度：630字节；

分段：1460=630+630+200



基于以太网的IP数据报实例分析

—源自EtherDetect捕获的数据片段（帧）

```
0000  00   50   BA   66   91   74   00   0D   60   13   60   C0   08   00   45   00
0010  01   99   0E   39   40   00   80   06   32   FC   CA   77   0B   1B   CA   77
0020  18   20   04   D6   00   50   F6   18   95   F9   CB   66   19   C6   50   18
0030  44   70   E7   D6   00   00   47   45   54   20   2F   77   2A   2A   55   6E
0040  52   65   67   2A   2A   75   2E   66   69   6C   65   73   2F   68   6D   61
0050  ……
```

以太网帧结构

8	6	6	2	46-1500	4 （字节）
F	DA	SA	Type	DATA	FCS

IP数据报格式：

版本号	IP头长	服务类型8	IP数据报长度16	标识符16	标志3 + 段偏移13
生存期8		高层协议8	报头校验和16	源IP地址16	
宿IP地址16					
IP头其他选项 + 数据域 …					

基于以太网的IP数据报实例分析

—源自EtherDetect捕获的数据片段（帧）

```
0000  00  50  BA  66  91  74  00  0D  60  13  60  C0  08  00  45  00
0010  01  99  0E  39  40  00  80  06  32  FC  CA  77  0B  1B  CA  77
0020  18  20  04  D6  00  50  F6  18  95  F9  CB  66  19  C6  50  18
0030  44  70  E7  D6  00  00  47  45  54  20  2F  77  2A  2A  55  6E
0040  52  65  67  2A  2A  75  2E  66  69  6C  65  73  2F  68  6D  61
0050  ……
```

DA：宿MAC地址

SA：源MAC地址

Type：以太帧

Data：IP数据报

以太网帧结构

8	6	6	2	46-1500	4 （字节）
F	DA	SA	Type	DATA	FCS

基于以太网的IP数据报实例分析

—源自EtherDetect捕获的数据片段（帧）

```
0000  00  50  BA  66  91  74  00  0D  60  13  60  C0  08  00  45  00
0010  01  99  0E  39  40  00  80  06  32  FC  CA  77  0B  1B  CA  77
0020  18  20  04  D6  00  50  F6  18  95  F9  CB  66  19  C6  50  18
0030  44  70  E7  D6  00  00  47  45  54  20  2F  77  2A  2A  55  6E
0040  52  65  67  2A  2A  75  2E  66  69  6C  65  73  2F  68  6D  61
0050  ……
```

标志位+段偏移：容许分段，段偏移为0

标识符：3641

版本号：v4，报头长度：5个32位字

IP数据报长度：409字节

服务类型：无优先级等方面的要求

IP数据报格式：

版本号	IP头长	服务类型8	IP数据报长度16	标识符16	标志3 + 段偏移13
生存期8		高层协议8	报头校验和16	源IP地址16	
宿IP地址16					
IP头其他选项 + 数据域 …					

基于以太网的IP数据报实例分析

—源自EtherDetect捕获的数据片段（帧）

```
0000  00  50  BA  66  91  74  00  0D  60  13  60  C0  08  00  45  00
0010  01  99  0E  39  40  00  80  06  32  FC  CA  77  0B  1B  CA  77
0020  18  20  04  D6  00  50  F6  18  95  F9  CB  66  19  C6  50  18
0030  44  70  E7  D6  00  00  47  45  54  20  2F  77  2A  2A  55  6E
0040  52  65  67  2A  2A  75  2E  66  69  6C  65  73  2F  68  6D  61
0050  ……
```

生存期：128跳

高层协议：TCP协议

报头校验和

源IP地址：202.119.11.27

宿IP地址： 202.119.24.32（www.seu.edu.cn服务器）

IP数据报数据域，TCP协议

IP数据报格式：

版本号	IP头长	服务类型8	IP数据报长度16	标识符16	标志3 + 段偏移13
生存期8		高层协议8	报头校验和16	源IP地址16	
宿IP地址16					
IP头其他选项 + 数据域 …					

★ IP协议的升级—新型IP协议（IPv6）

☆ IPv4的局限性：

— 32位的IP地址空间不足，地址资源耗尽。

— 不定长的数据报头域处理影响了路由器的性能提高。

— 安全性考虑较少。

☆征询IPng—RFC1550（1993年10月）；

目标：

1 支持几乎无限大的地址空间；

2 减少路由器的路由表体积，支持路由器高效处理数据报；

3 提供更好的安全性（IP级的安全性）；

4 支持多种范围类型，包括组播；

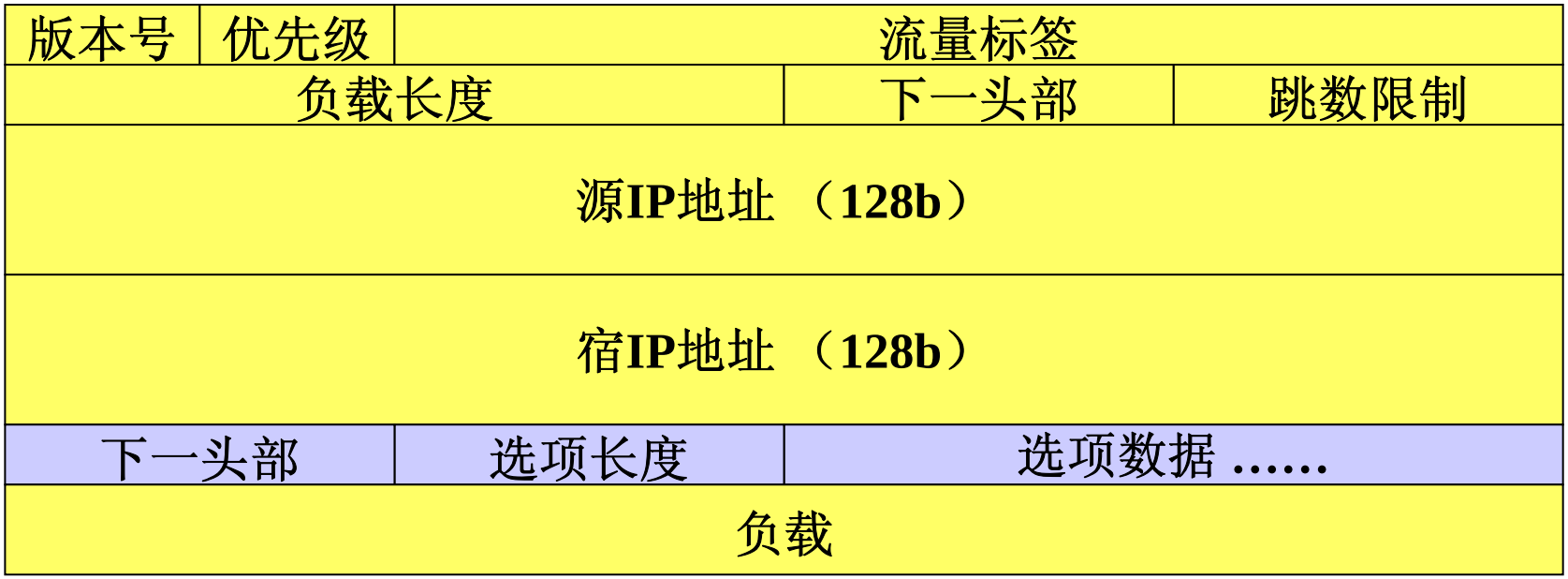
5 支持自动地址配置，容许主机不更改地址实现异地漫游；

6 支持IPv4和Ipng的共存；

7 支持可移动主机和网络；

……。

★ IPv6的帧格式—简化头部，提高R的工作效率



版本号（Version：4b）：6；
优先级（Priority：4b）：
流量标签（FlowLable：24b）：便于流量分类；
负载长度（PayloadLength：16b）；字节为单位；
下一头部（Next Header：8b）：头部选项的类型；
跳数限制（HopLimit：8b）：等同TTL；
源地址（Source Address：128b）；
宿地址（Destination Address：128b）。

★ IPv6的帧格式—可能的选项头部

NoOption（59）
Hop-by-Hop Options header（0） — 逐跳选项；
Destination Options header （60） — 宿选项；
Routing header （43） — 路由选项；
Fragment header（44） — 分段选项；
Authentication header — 认证选项；
Encapsulating Security Payload header — 封装安全负载选项
……。

NextHeader 8	Opt Data Len	Option Data ……

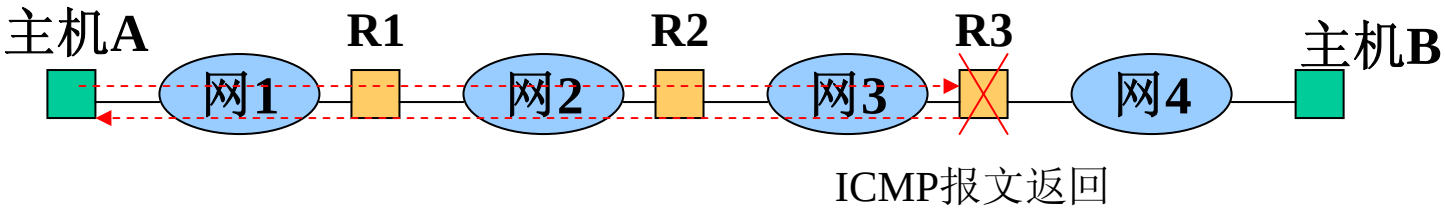
注：**IPv6**公布于**1995**年，升级工作并不顺利：**IPv4**被广泛应用，目前仅处于实验阶段。

7.5.2 因特网控制报文协议（ICMP—RFC792、950）

★ 功能：网络设备和结点之间的控制和差错报告报文的传输。

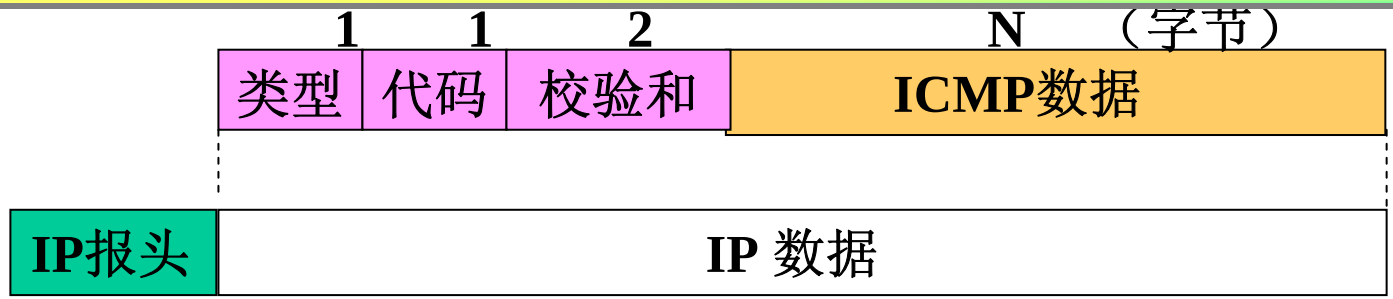
IP协议本身没有内在的机制获取差错信息并进行相应的控制，而导致传输差错的因素众多：
如：通信线路出错、网关或主机出错、信宿主机不可到达、数据报生存期（TTL时间）到、系统拥塞等等。

ICMP可视为对IP协议的补充：弥补部分差错报告的功能。



ICMP协议：当中间路由器发现传输错误（借助报头校验和）时，IP模块丢弃该IP数据报，ICMP实体向信源主机返回ICMP报文，报告出错情况，以便信源主机采取相应的措施。

★ ICMP报文格式



ICMP报文由路由器产生，
被封装在**IP**数据报的数据区中进行传输；

IP报头中协议字段=1表示ICMP报文；

ICMP报文类型：

报文无法投递： 网络、信宿、协议、端口、分段、源路由；

投递超时： TTL转发超时、合段超时；

分段问题： 指针（偏移量计算）错；

源抑制（用于拥塞控制），

……。

★ ICMP的应用 —网络诊断工具

☆ Ping软件：

借助于ICMP回应请求/应答报文测试宿主机的可达性。

☆ 跟踪IP数据报的路由（Tracerouter）：

利用路由器对IP数据报中的生存期值作减1处理，一旦生存期值为0 就丢弃该IP数据报，并返回主机不可达的ICMP报文的特点。

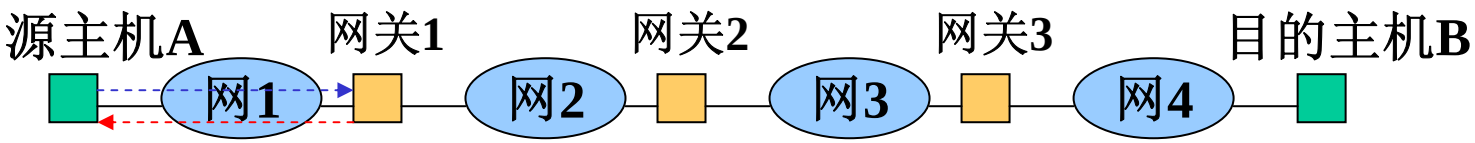
— 测试过程：

① 源发端形成一系列收方结点无法处理的IP数据报（如具有非法端口，且生存期值不同的数据报），逐个发往网络；

② 第一个数据报的生存期为1；第一路由器返回主机不可达ICMP报文，继续发送生存期为2，3，4的数据报；

③ 由于主机和路由器中对路由信息的缓存能力，IP数据报将沿着原路径向宿结点前进；

④ 通过返回N个主机不可达报文和一个端口不可达报文的信息，了解IP数据报的整个路由。



7.6 传输控制协议（TCP—RFC793，UDP—RFC768）

（1） TCP的能力

在IP协议软件的基础上，提供面向连接的、端到端（应用进程之间）的、可靠的、面向流的投递服务；

功能类似OSI的IP4。

（2） TCP原理及特性：

★ 以文件操作方式为设计准则，操作对象为进程间的“管道”；

★ 面向流的投递服务（支持数据字节流的传输）；

★ 可靠传输服务：差错校验，超时重发，排序等；

★ 端到端传输：支持应用进程之间的数据信息交换；

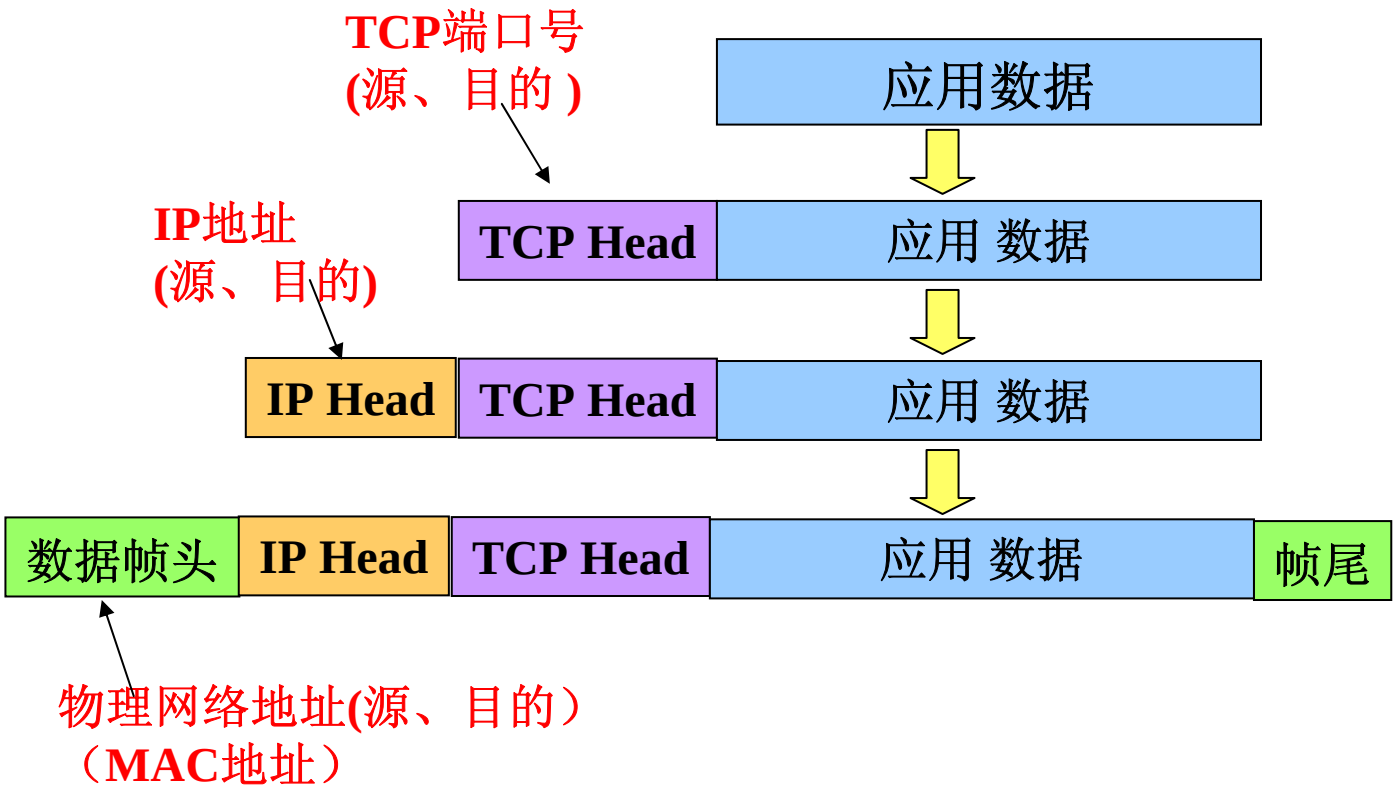
★ 面向连接的投递服务：具有建连等过程，支持状态的维护；

★ 全双工传输：双方进程可在同一条连接上发送数据；

★ 流量控制：收方控制的滑动窗口机制；

★ 利用端口（TCP端口或者TU端口）标识和区分应用进程。

（3） TCP数据的封装


TCP端口号
(源、目的)
应用数据
IP地址
(源、目的)
TCP Head
应用 数据
IP Head
TCP Head
应用 数据
数据帧头
IP Head
TCP Head
应用 数据
帧尾
物理网络地址(源、目的）
（MAC地址）

（4） 用户数据报协议（UDP）—RFC768

UDP直接利用IP特性进行UDP数据报的传输，

提供无连接、不可靠的数据报投递服务。

UDP常用于短小信息，或者可靠性要求不高的数据传输，

例如：域名系统中域名地址/IP地址的映射请求和应答（Named）

Ping，BOOTP，TFTP

减少TCP连接的过程，提高工作效率。

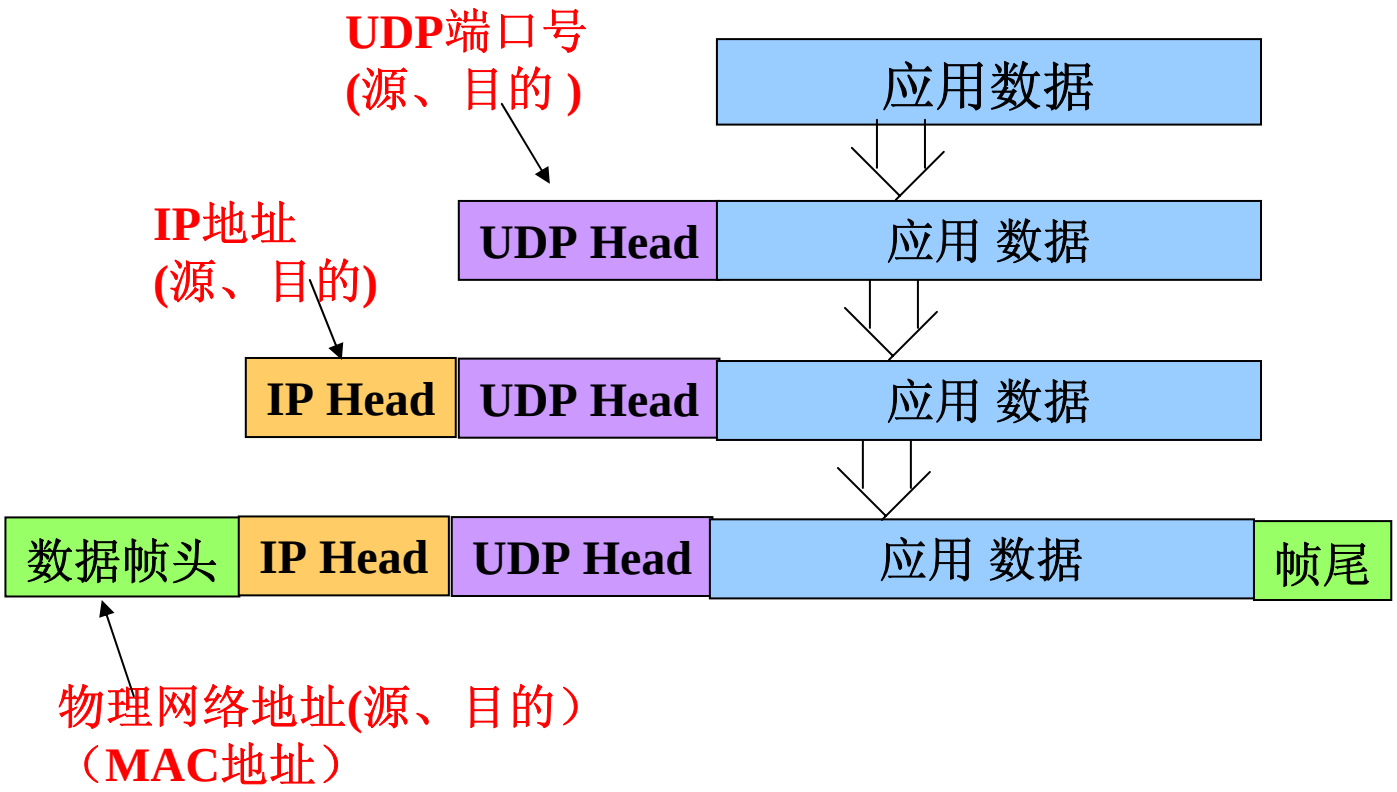
当使用UDP协议传输信息流时，

用户应用程序负责解决排序，差错确认等问题。

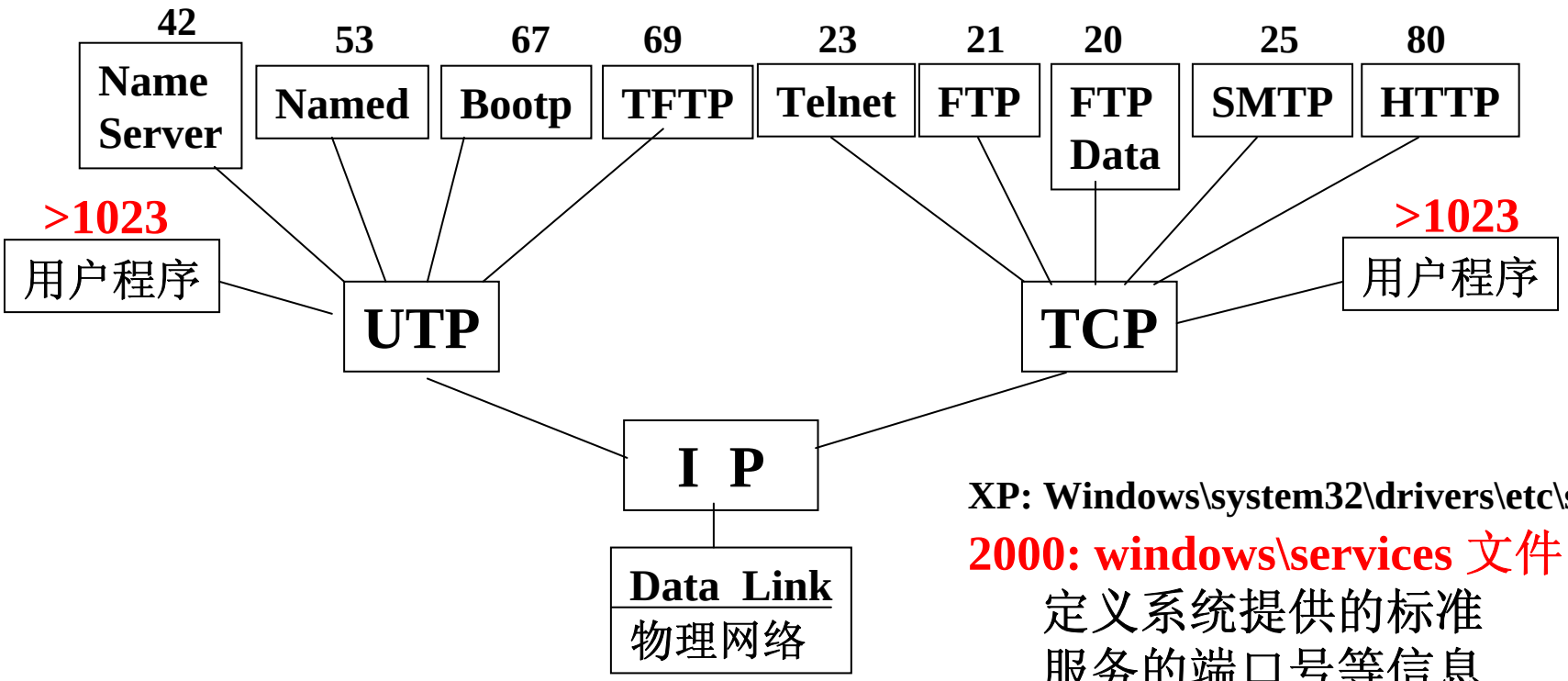
在多媒体应用中，常用TCP支持数据传输，

UDP支持音频/视频传输。

（5） UDP数据的封装


UDP端口号
(源、目的)
IP地址
(源、目的)
物理网络地址(源、目的）
（MAC地址）
应用数据
UDP Head
应用 数据
IP Head
UDP Head
应用 数据
数据帧头
IP Head
UDP Head
应用 数据
帧尾

★ TCP/UDP端口（简称TU端口）—标识和区分应用实体



XP: Windows\system32\drivers\etc\services

2000: windows\services 文件：
定义系统提供的标准
服务的端口号等信息

TCP/UDP模块可为多种（个）应用程序提供传输服务

区分方法：为每种服务定义访问端口——TCP/UDP协议端口，
并分配端口号。0—1023（保留端口号,标准服务）
1024以上是自由端口号，用户应用服务使用。

IP地址+TCP/UDP端口号确定因特网中的某主机上的某个应用进程。

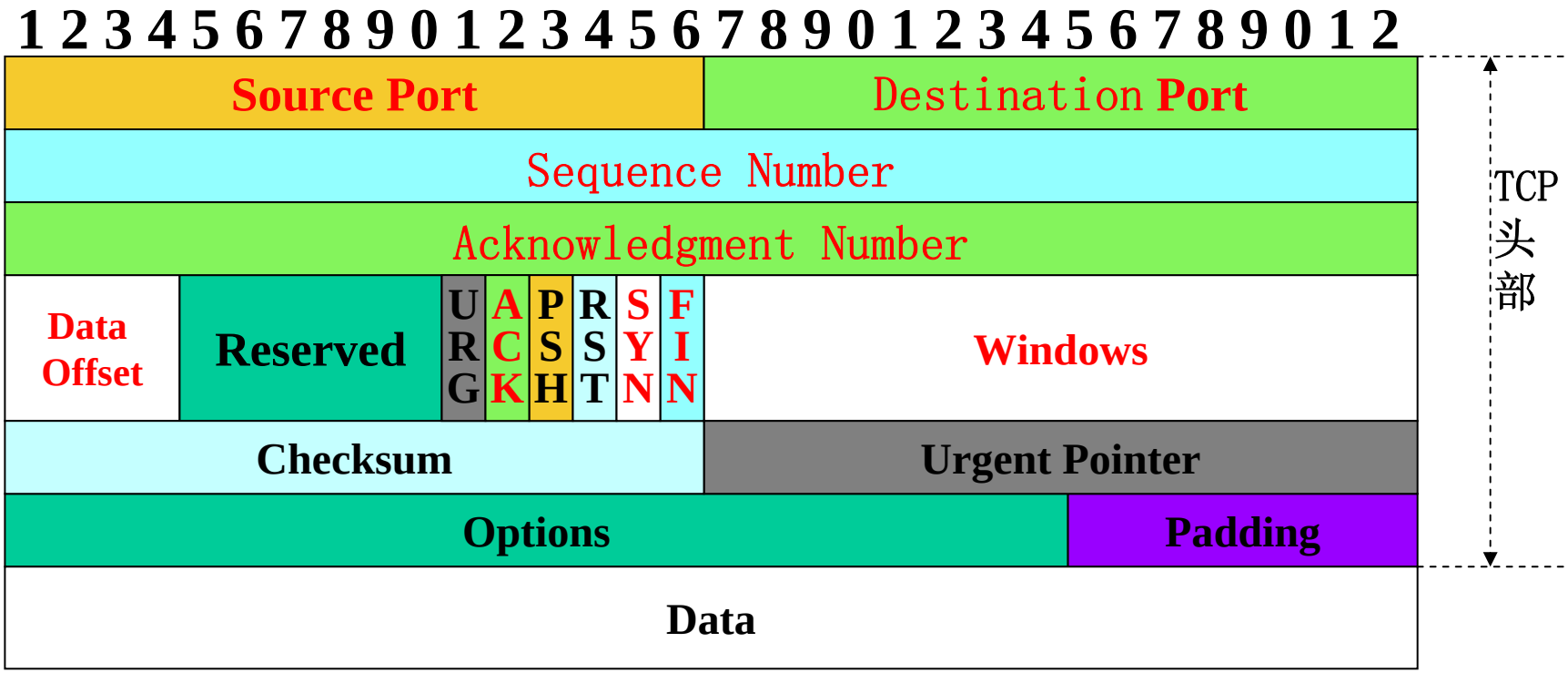
☆ 常用的TCP端口号

源自 **XP: Windows\system32\drivers\etc\services**

应用进程	TU端口	说明
ftp-data	**20/tcp**	**#FTP, data**
ftp	**21/tcp**	**#FTP. control**
telnet	**23/tcp**	**#Remote terminator**
smtp	**25/tcp**	**#Simple Mail Transfer Protocol**
domain	**53/tu**	**#Domain Name Server**
tftp	**69/udp**	**#Trivial File Transfer**
http	**80/tcp**	**#World Wide Web**
pop2	**109/tcp**	**#Post Office Protocol - Version 2**
pop3	**110/tcp**	**#Post Office Protocol - Version 3**
snmp	**161/udp**	**#Simple network management Protocol**
snmptrap	**162/udp**	**#SNMP trap**
l2tp	**1701/udp**	**#Layer Two Tunneling Protocol**
pptp	**1723/tcp**	**#Point-to-point tunnelling protocol**
radius	**1812/udp**	**#RADIUS authentication protocol**
radacct	**1813/udp**	**#RADIUS accounting protocol**

应用丰富，促使专用**TU**端口号已超过**1023**

★ TCP数据段的格式



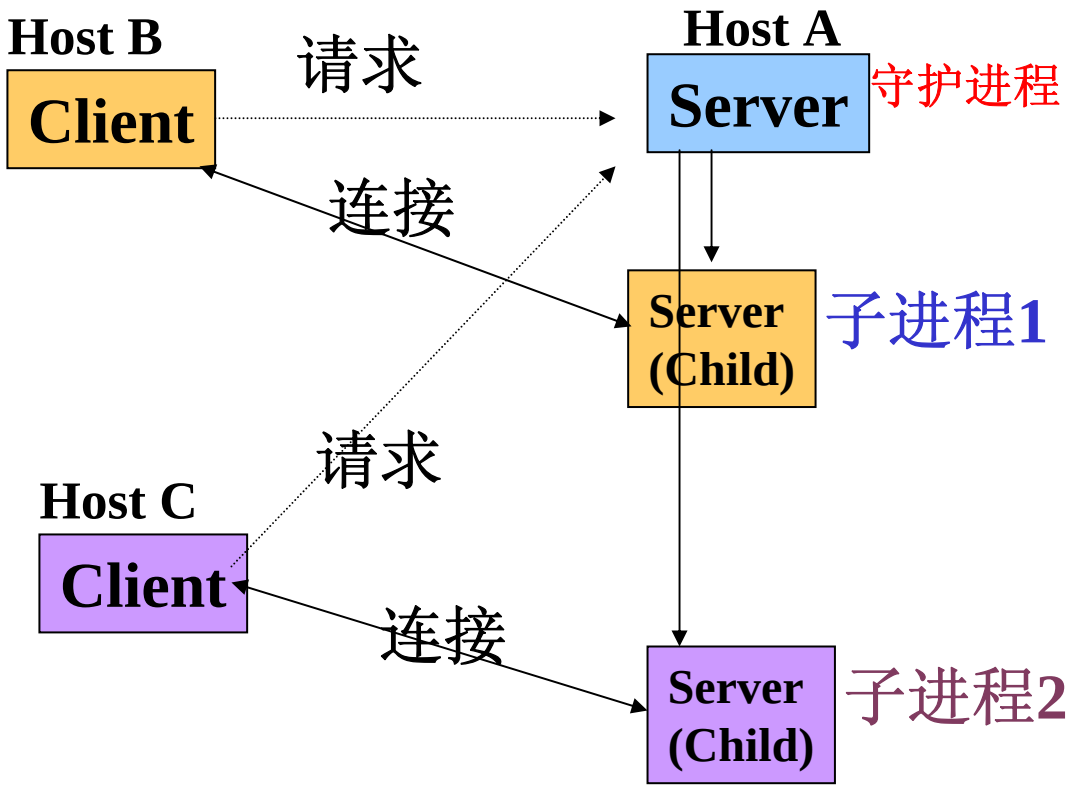
Source/Destination Port（16位）：源/宿端口号，标识应用进程；
Sequence Number：序列号，Data域中首字节在整个数据流中的序号；
Acknowledgment Number：期望收取的数据字节序号，类似Nr；
Data Offset（4位）：数据域位置， 报头的字数；
ACK=1，Acknowledgment Number有效；
SYN=1，同步序号（建立连接）；　　**FIN**=1，终止连接；
Windows：期望接收的字节数；

Data域的长度蕴含在IP报头的16位的“IP报文长度”中。

★ TCP/IP应用服务的原理：

采用客户机/服务器工作模式，服务器端启动守护进程，等待客户机端的请求；

对应客户的请求，派生子进程，提供服务；



☆ TCP/UDP接口—Berkeley的TCP服务原语（API）：

— 创建套接字—新的通信端点

sockid=Socket(af,type,protocol)

— 绑定本地地址和端点（套接字）

bind(sockid, local addr, addrlen)

— （服务器端）显示愿意接受远程（客户端）的连接请求

listen(Sockid ,quenlen)

— 服务器端等待从端点处接收客户连接请求

newsockid=accept (sockid， clientaddr, paddrlen)

— （客户端）主动发起建立（服务器/客户端）的TCP连接

Connect(sockid, destaddr, addrlen)

— 发送/接收数据

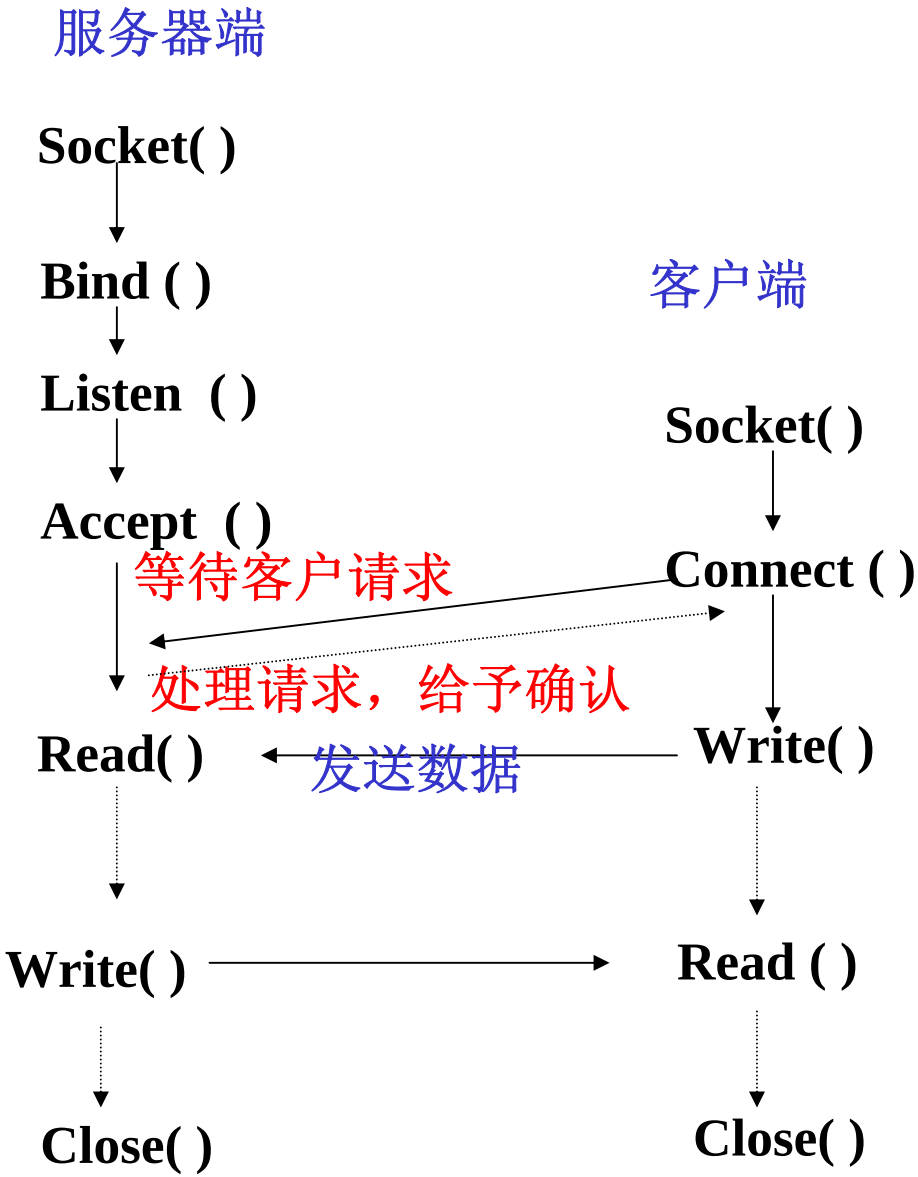
面向连接（TCP）： **write(sockid, buff, bufflen)** **read( )**

面向无连接（UDP）： **sendto(sockid,buff,…,addrlen)** **recvfrom( )**

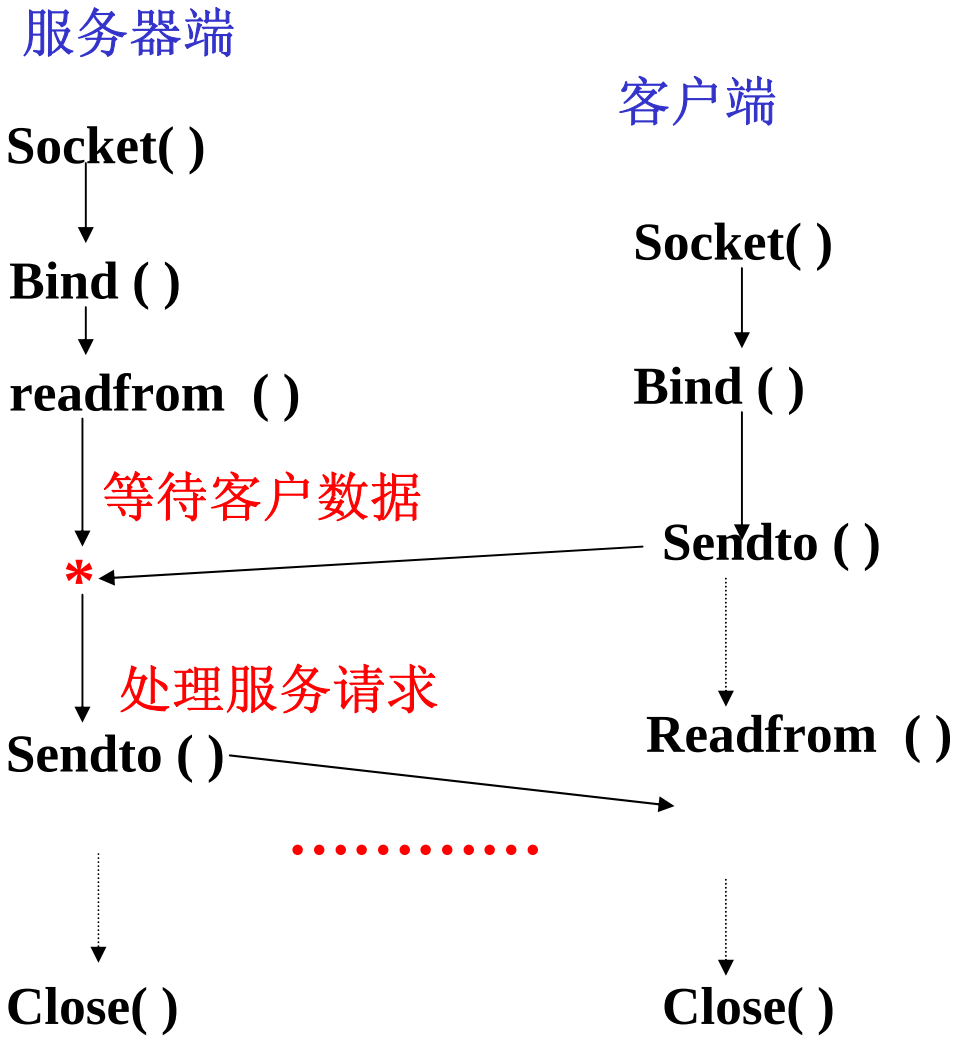
— 释放连接（套接字）

close(sockid)

☆ Socket编程流图—面向连接



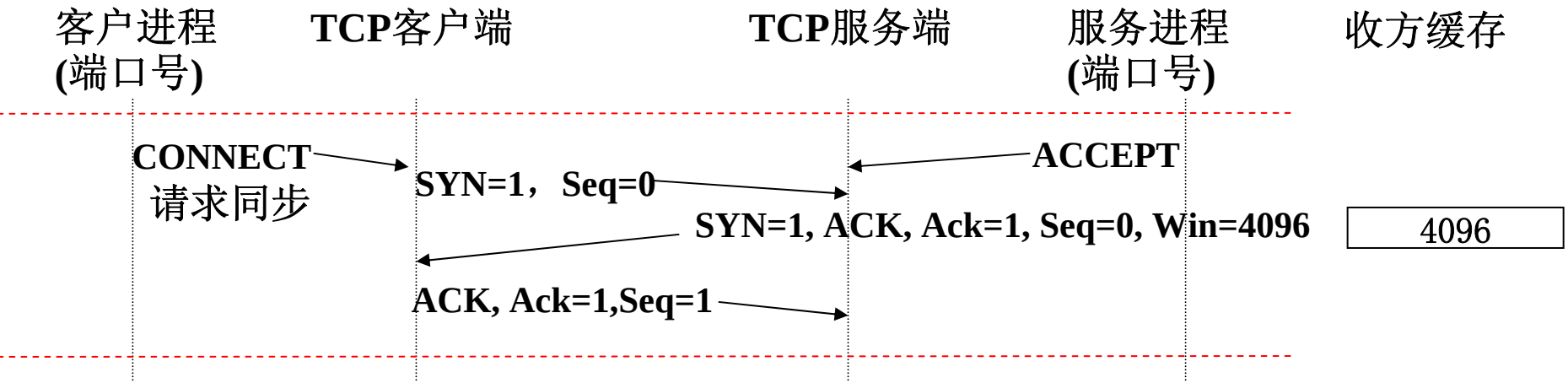
☆ Socket编程流图—面向无连接



★ TCP的工作过程—基于窗口的字节流传输

TCP提供面向连接的、端到端（应用进程之间）的、可靠的、面向字节流的全双工报文投递服务；

面向连接（三次握手）

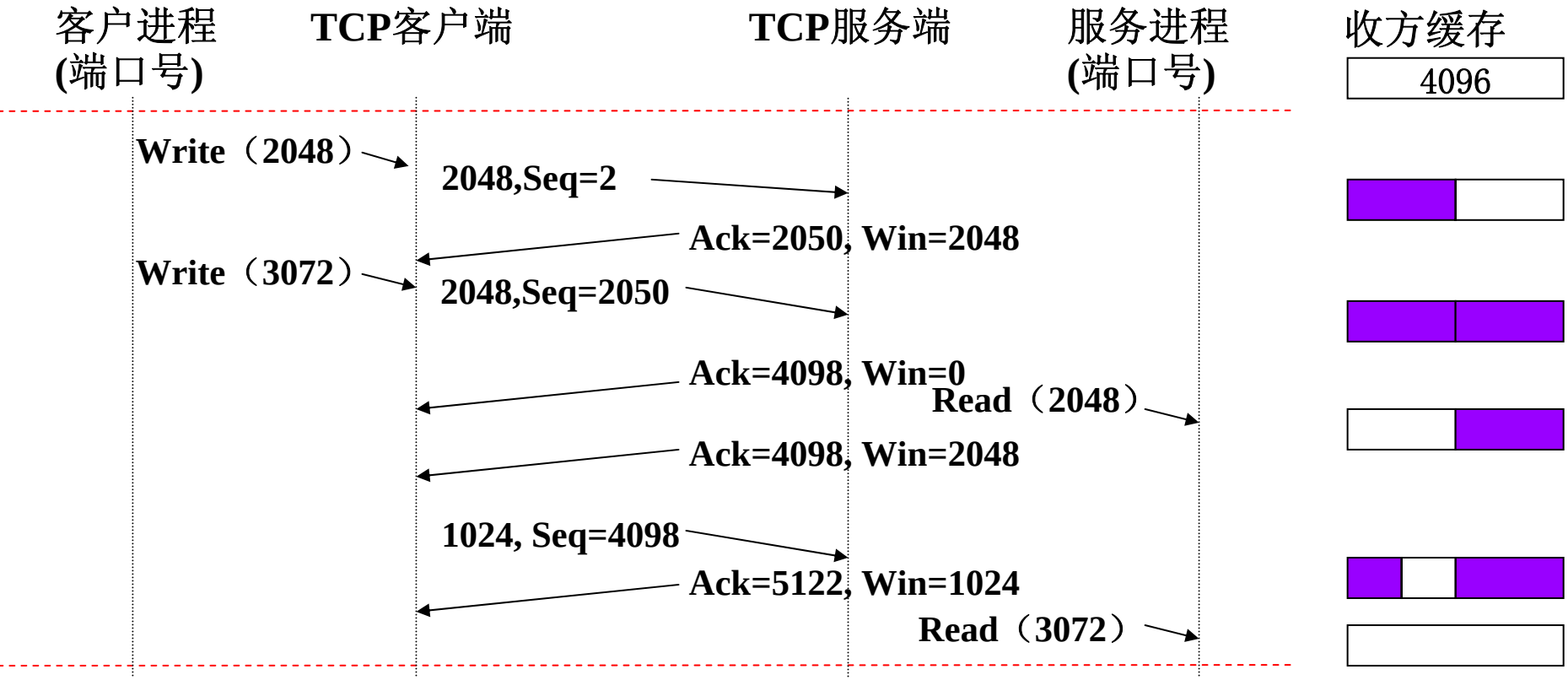


当服务进程收到**SYN=1**（请求同步/连接）的报文后，预留资源；
反馈**SYN=1**的报文， 希望同步并建立服务—客户的连接；
当客户端收到**SYN=1**的报文后，也可预留资源，并予以应答。
三次握手（客户—服务—客户—服务）后，建立双向通道。
本例中仅示意客户端到服务端的数据传输，故应答中**Windows**字段为**0**。

潜在问题：如果客户无应答会如何？

★ TCP的工作过程—基于窗口的字节流传输

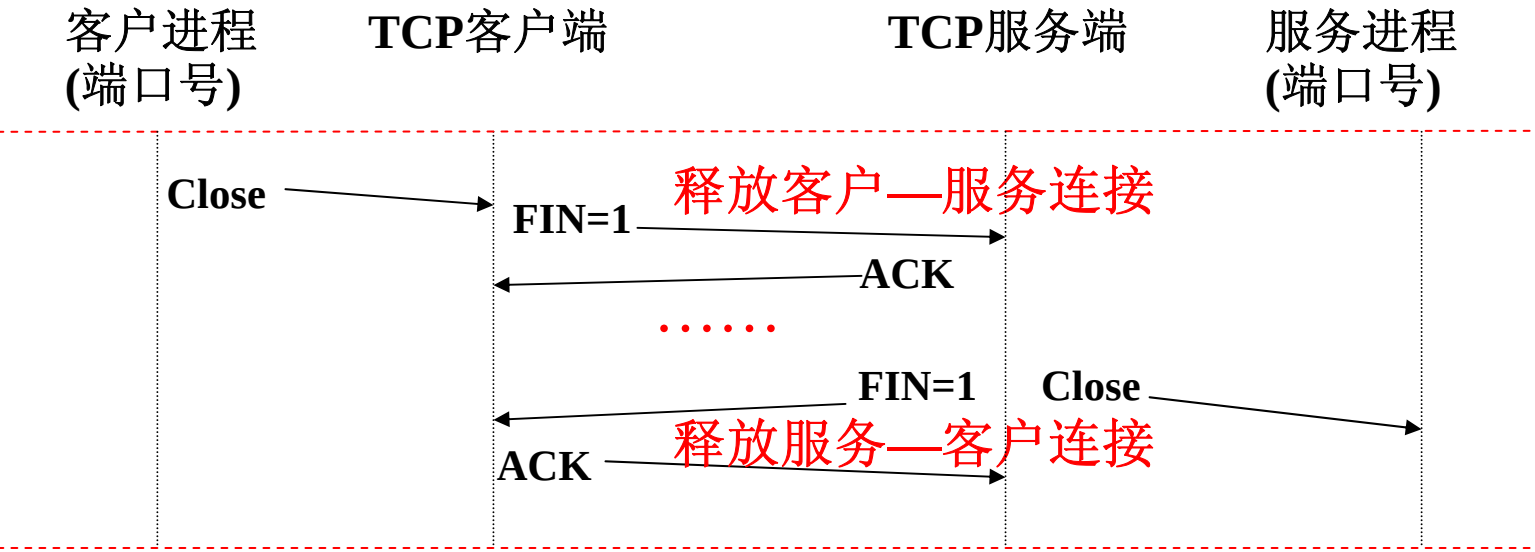
字节流传输：



双方均可主动发送数据，并利用**ACK**等符号位予以捎带应答；
收方利用**Windows**字段控制发方的发送速率；
发方维护计时器，超时（未应答）则予以重发。

★ TCP的工作过程—基于窗口的字节流传输

释放连接（4 或 3阶段，全双工）：



TCP的全双工连接可视为两个单工的连接；

任意一方都可发起释放过程—释放对应本端的单工连接；

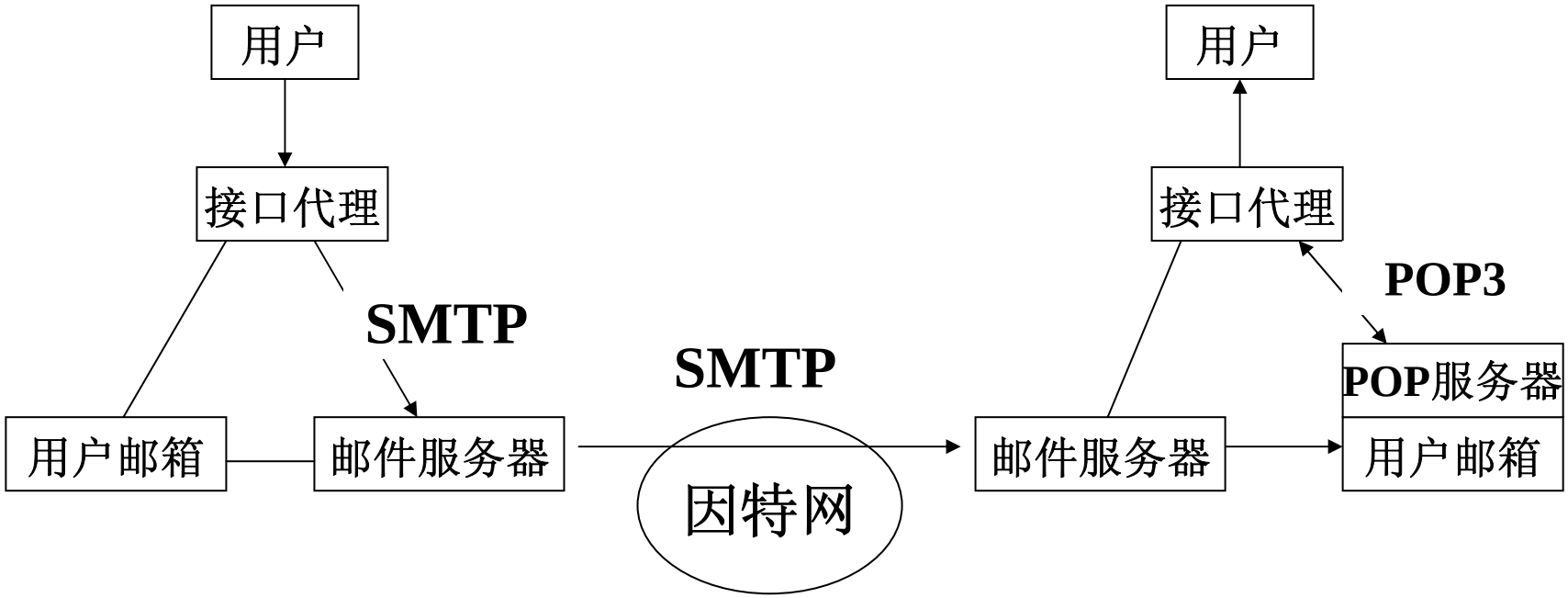
若对应**FIN=1**的**TCP**端未收到**ACK**，也会超时自动断连。

7.8 因特网基本的应用服务

（1） 服务举例—电子邮件（SMTP—RFC821）

提供简单的电子邮件服务（**Simple Mail Transfer Protocol**）；
使用**TCP**连接，端口号为**25**；
邮件地址： 用户名@主机名

★ **SMTP**的基本模型（为支持用户的异步操作，引入**POP**服务器）
POP—Post Office Protocol



★ 常用SMTP指令（服务器—服务器）：

邮件服务器启动守护进程，监听TCP端口25的请求；

常用的请求指令（请求方—>响应方）：

HELO hostname—向响应方标识请求方
MAIL FROM：sender_id—发信人的邮件地址
RECP TO：receiver_id—收信人的邮件地址
DATA—邮件正文，以仅含句点的行结束
VERY user—请求响应方核实user的有效性（注册用户）
RESET—取消刚才的指令
QUIT—退出连接

常用的响应指令（响应方—>请求方，响应码+空格+说明）

220 服务就绪（在Socket连接成功时返回此信息）
221 正在处理
250 请求指令正确执行
354 开始发送邮件
500 语法错误
550 邮箱无效

所有命令均可用TCP原语（API）中**write( )**和**read( )**进行交换。

★ SMTP协议交互过程（S/RH—Sending/Receiving Host ）

RH启动守护进程（Smtpd），监听TCP端口25的请求；
接到来自SH的connect请求后，双方交换信息如下：

RH: 220 sina.com SMTP service ready
SH : HELO seu.edu.cn
RH: 250 sina.com says hello to seu.edu.cn
SH: MAIL FROM：gwu@seu.edu.cn
RH: 250 gwu@seu.edu.cn OK
SH : VERY usr1
RH: 252 Cannot Very usr1
SH : RCPT TO: usr2
RH: 250 usr2@sina.com OK
SH : DATA
RH: 354 send mail;end with “.” on a line by itself
SH : From: gwu@seu.edu.cn
SH : To: usr2@sina.com
……
SH : .
RH: 250 message accept
SH : QUIT
RH: 221 seu.edu.cn closing connection

★ 常用POP3（RFC1939）指令（客户端—服务器）：

POP3服务器启动守护进程，监听TCP端口110的请求；

常用的请求指令（客户—>POP3服务器）：

USER username—向服务器指示客户的帐户
PASS password—向服务器指示客户的口令（密码）
STAT—要求报告未读的邮件列表
LIST [m]，要求列出所有（或第m份）邮件的体积
RETR m—索取编号为m的邮件
DELE m—将编号为m的邮件标记为“删除”
RSET—去除所有邮件的“删除”标记
TOP m n—索取编号为m的邮件的前n行内容
QUIT—释放TCP连接，清除标记为“删除”的邮件。

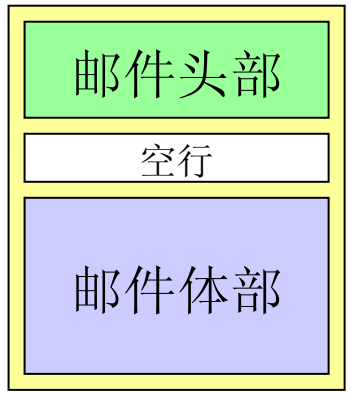
常用的响应指令（POP3服务器—>客户）

+OK 请求正确，响应结果
-ERR 请求有误

所有命令均可用TCP原语（API）中write( )和read( )进行交换。

★ 邮件结构（RFC822）

邮件 = 邮件头 + 空行 + 邮件体



常用头部字段：

Date—发送邮件的日期

From—发方名和邮件地址

To—收方名和邮件地址

Subject—邮件主题

Return-Path—返回邮件发方的路径

Reply-To—回复邮件的收方

Cc—邮件复本的收方

Message-ID—邮件标识符

Received from—SMTP发方主机

Received by—SMTP收方主机

RFC822仅支持**ASCII**文本。

邮件实例：

From：xxx@sina.com
Return-Path：xxx@sina.com
Received: from sina.com by seu.edu.cn
Date: Sun, 20 May 2005 08:54:07
Message-id: 901023487@sina.com
To: gwu@seu.edu.cn
Subject: XXXXXXXXX

YYYYYYYYYYYYYYY
YYYYYYYYYYYYYYY

★ 邮件内容—非ASCII文本的表示

为了使用邮件系统支持非ASCII文本的传输，IETF定义MIME；
MIME—Multipurpose Internet Mail Extensions（RFC1521/22）。

邮件头部增加MIME头部字段：

MIME-Version：使用MIMIE版本，v1.0兼容RFC1521和1522；

Content-Type：邮件体的数据类型（正文、图象、视频、音频等）；

Content-Transfer-Encoding：传输邮件体使用的编码；

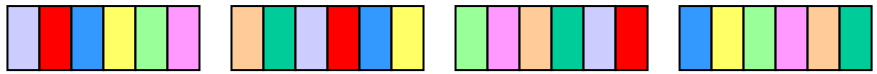
……。

常用的Content-Trasfer-Encoding：

base64：使用4个6位字符表示3个8位位组的方案；

3个8位位组：

4个6位字符：



2^6可表示数值0—63，0—25对应A—Z，26—51对应a—z，
52—61对应0—9，62对应+，63对应/；

不足3字节时，填充1或2个全0的字节继续编码，编码后加1或2个“=”字符。

（2）因特网基本的应用服务—文件传输服务（FTP）

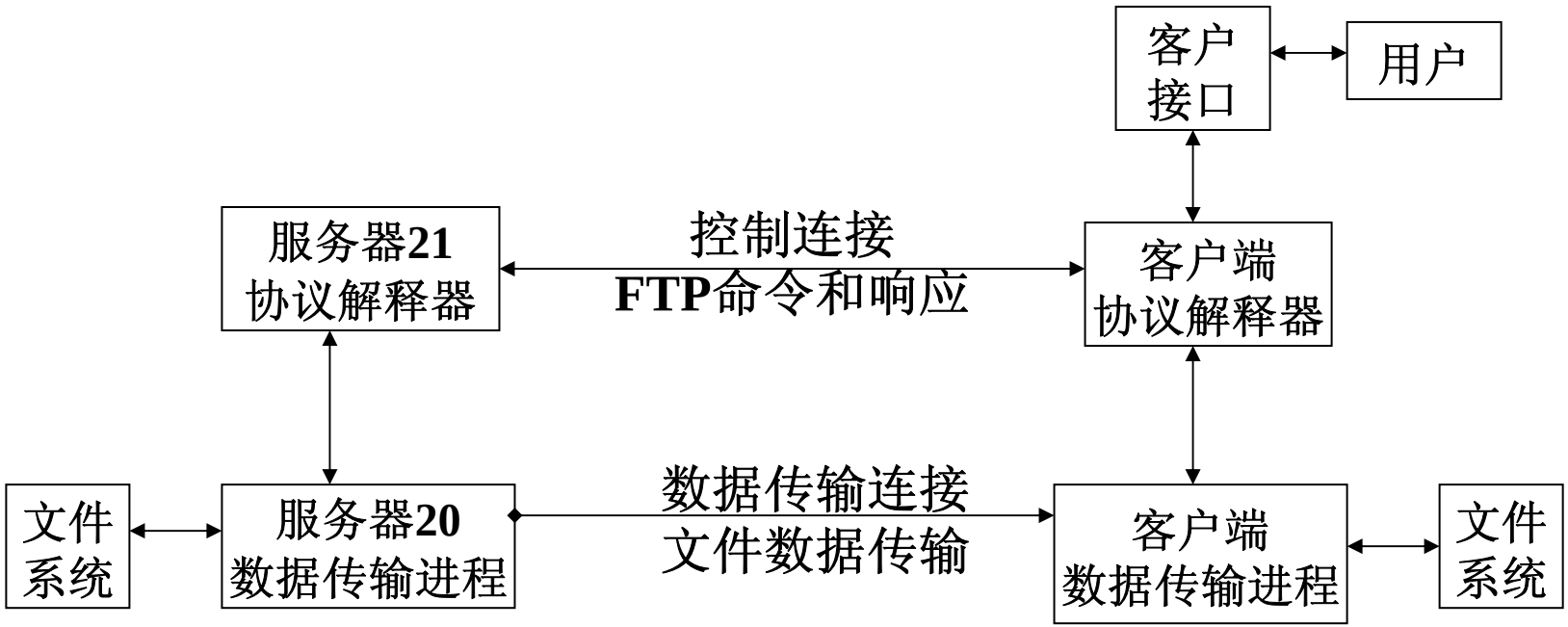
FTP—File Transfer Protocol（RFC 959）

提供文件系统间的文件交换；

使用TCP连接，控制命令使用21端口，数据传输使用20端口；

ftp 远程IP地址

★ FTP的基本模型



★ 常用FTP指令（客户端—服务器）：

FTP服务器启动守护进程（ftpd)，监听TCP端口21的请求；

常用的请求指令（请求方—>响应方）：

get remotefile [localfile]—获取一个文件，同名/改名
mget remotefile1 … remotefilen—获取多个文件
put localfile [remotefile]—传输一个文件，同名/改名
mput localfile1 … localfilen—传输多个文件，同名
cd xxx—进入新的远地目录
lcd xxx—进入新的本地目录
dir—列出当前目录列表
pwd—列出远程当前目录名
mkdir xxx—服务器断创建目录
ascii—后续以ASCII传输文件内容
binary—后续以二进制形式传输文件内容

所有命令均用TCP原语（API）中**write( )**和**read( )**进行交换。

（2） 因特网基本应用服务—WWW（World Wide Web）服务

★ 目标

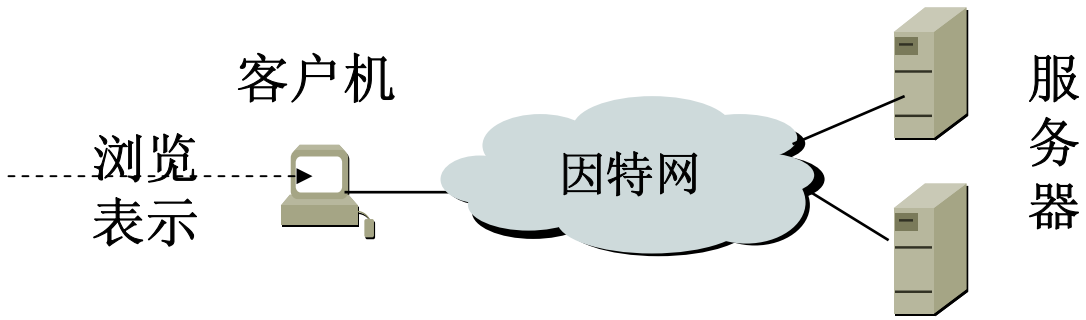
支持构建分布式的协作超媒体信息系统，将整个因特网的信息资源组合在一起，信息以页面的形式提供给客户。

页面及其关系以链接的方式形成—超文本；混合了音频/视频的内容，需要多种播放媒体的支持—超媒体。

★ 基本原理

服务器监听TU端口（缺省值为80），获取客户（浏览器）的指令（方法），并返回信息；浏览器解释和显示获取的信息。

支撑协议：**HTML**（超文本标记语言**RFC2854**）—页面表示；
HTTP（超文本传输协议**RFC1945/2616**）—页面传输



★ HTTP—HyperText Transfer Protocol（超文本传输协议）

定义浏览器和服务器之间的指令和页面的交换。

相关标准：

RFC1738—Uniform Resource Locators (URL), 1994.10;

RFC1866—Hypertext Markup Language 2.0, 1995.11;

RFC1945—Hypertext Transfer **Protocol -- HTTP/1.0, 1996.5;**

RFC2616—Hypertext Transfer Protocol --
HTTP/1.1, 1999.6;

URL（统一资源定位器）：确定信息（页面）的位置、名称和获取方式；

一般格式：Protocol: // Host [:port] [资源的路径]

举例：Http://www.seu.edu.cn/seu/welcome.html

ftp://ftp.pku.edu.cn/pub/rfc/index.txt

Web访问命令：

浏览器的主要指令（方法）

- GET—检索所需的页面；
- HEAD—检索页面的标头；
- POST—信息加入指定的页面（修改页面）；
- PUT—特定页面传递给服务器（形成或者取代页面）；
- DELETE—删除服务器上的某个页面；

服务器通过设置来确定在什么情况下可以执行哪些指令；

服务器的响应

- 1xx（状态报告，2项）：收取指令，正在处理；
- 2xx（成功，7项）：指令正确处理完毕，返回结果页面；
- 3xx（转向，8项）：要求补充新的指令完成页面的传输；
- 4xx（客户故障，18项）：指令错误（如语法错，无法执行）；
- 5xx（服务器故障，6项）：服务器错误，不能完成合法的指令。

举例 指令 get /seu/welcome.html Http/1.1 Host: www.seu.edu.cn

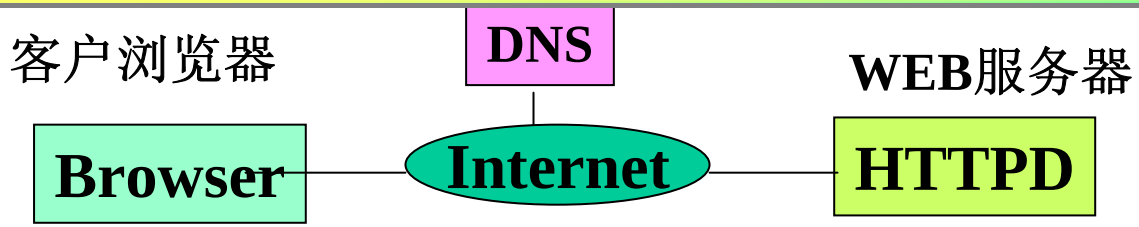
响应 200 OK

页面标头

CRLF

页面体部

★ 实际工作过程



Http://www.seu.edu.cn/seu/welcome.htm

— 浏览器向DNS获取web服务器的IP地址：202.119.24.32；

— 浏览器与IP地址为202.119.24.32的服务器进行TCP连接，端口为80；

— 浏览器执行HTTP协议，发送GET /seu/welcome.htm 命令，请求读取文件；

— www.seu.edu.cn服务器返回/seu/welcome.htm 文件到客户端；

— 释放TCP连接；（注）

— 浏览器解释/seu/welcome.htm 内容，并显示对应页面。

注：一个页面可能包含多个文件（URL）的内容—页面逐渐丰满；

早期版本对于每个URL建立一个TCP连接；

HTTP1.1容许一个TCP连接支持多个URL（指令和响应）的传输，并在最后一个URL传输时协商释放TCP连接。

响应中指出　Connection: close

★ Web技术的扩展应用—对C/S模式的改进（B/C/S或者B/A/S）

C/S模式的弱点：

客户端软件的升级和维护复杂。

B/C/S模式的优点：

用户统一使用浏览器，操作方便；

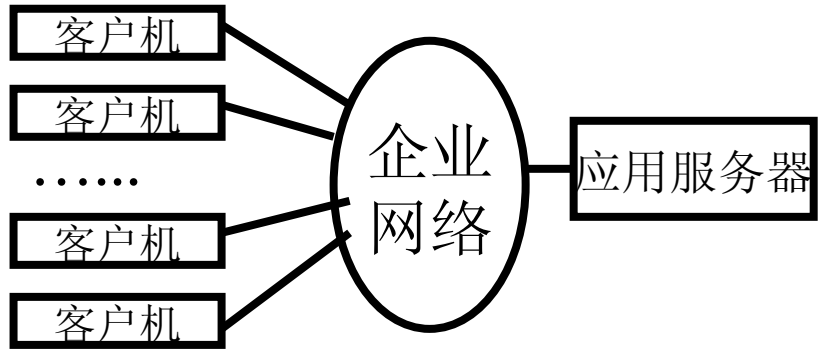
便于应用系统的维护和更新。

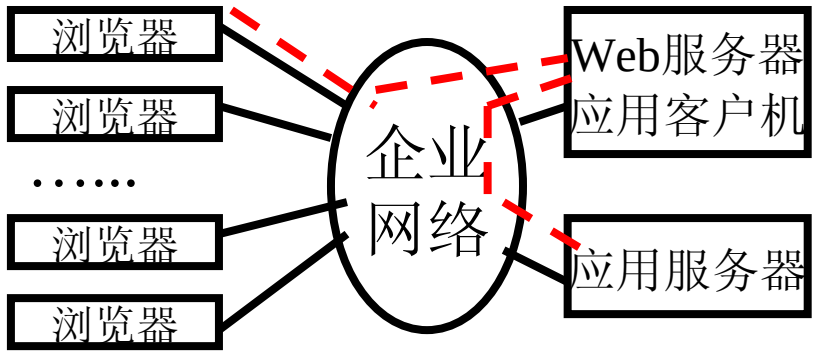
B/C/S模式的弱点：

工作效率有所下降。

改进方法：

使用高性能的服务器。



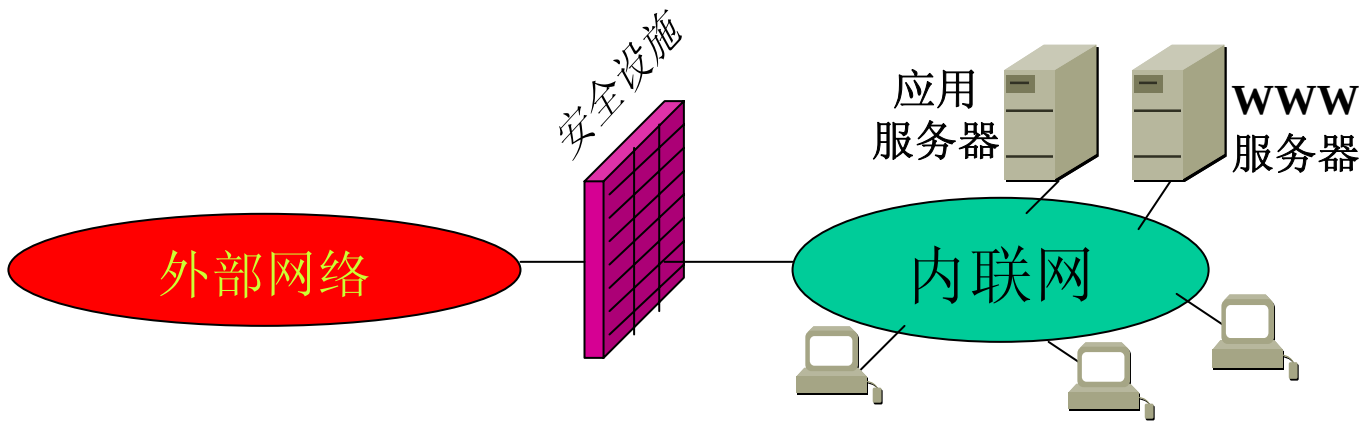


（3） IP技术的推广应用

★ IP技术的应用—内联网（Intranet）

内联网是应用因特网技术构建的企业内部网，该网络也执行TCP/IP技术，具有IP地址，提供类似因特网服务。目前，内联网用户使用的最多的服务是WWW，包括应用B/W/D（三层结构）构建的应用服务。

通常，内联网用户不与外部发生联系，或者通过互连部件和安全设施（如防火墙）有限制的与外部世界（如因特网）联系。此处的安全设施意在保护内联网的安全性。

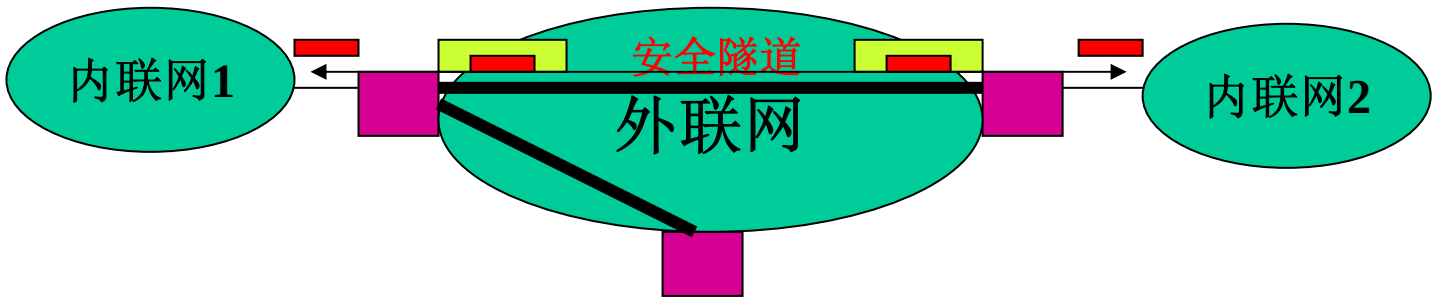


★ IP技术的应用—外联网（Extranet）

外联网是为适应企业网之间，或者跨区域的企业内部部门网之间的安全交换信息而形成的网络；

外联网的基础是广域网，如X25网络、帧中继网络，也可以是因特网。

外联网的核心技术是在企业网之间构建隧道（有时，隧道技术也可被理解为封装技术，即用支撑协议封装被传输的数据），隧道的两端执行相关的安全操作和封装操作，而中间的广域网仅执行透明的数据传输。



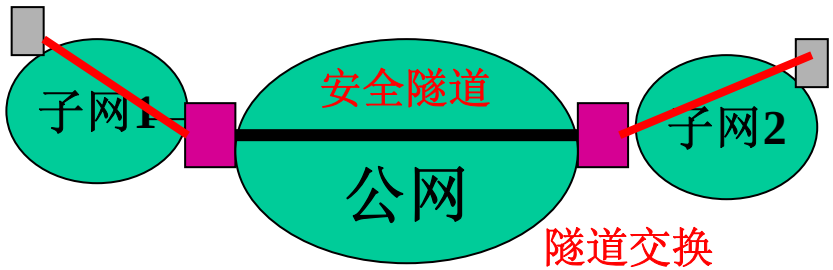
★ IP技术的应用—虚拟专用网（VPN）

VPN是外联网的外延，施加安全技术在公网的基础上构建的专用网络，此处的公网可以是因特网或者内联网； 类似外联网，**VPN**的核心也是隧道技术；

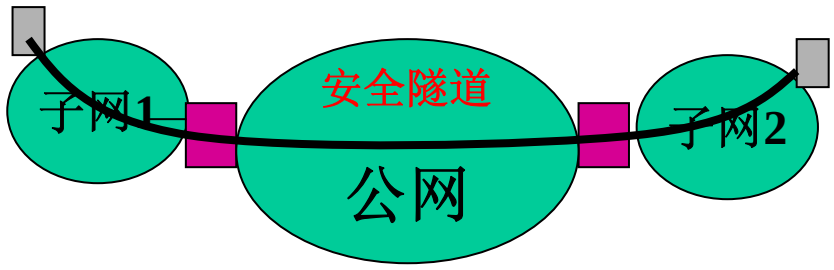
流行的基于因特网的**VPN**：

★ 基于**IPsec**的**VPN**：用**IP**协议封装了其它各种安全协议，支持封装后的数据单元在**IP**网络上传输。因**NAT**防火墙对**IP**地址的迁移，无法提供端到端的保障（要求隧道的交换）；（专业维护）

★ 基于**SSL**的**VPN**：用**TCP**之上的**SOCKS**封装用户数据，透明穿越防火墙，可提供端到端的安全保障。（用户维护）



（1） 基于IPsec的VPN



（2） 基于SSL的VPN

8.1 网络管理

（1） 网管概述

目的：对组成网络的各种硬软件设施的综合管理，以达到充分（优化）利用这些资源的目标。

对象：网络设备、主机；

管理的方法：收集、分析和配置参数；

（1） 网管概述

必要性：

单机性能问题：软件本身、系统设置和配置，
系统工具+人工；

网络性能问题：影响因素众多，网络应用、网络流量、
设备的运行状况等；

设备的分布性，需要相应的工具协助管理员—网络管理。

网络规模扩展，网络应用的普及，意义日益显著。

☆ 用户视角：价廉物美地使用网络，快捷可靠传输信息，丰富资源；

☆运营商视角：资源（带宽和设备缓存等）充分利用；

☆企业组网者：满足应用需求，成本（资源利用率）；

（1） 网管概述

实质：对各种网络资源状态及其使用进行监测、控制和记录，并在网络出现故障时，及时报告和处理，向管理员报警，以便尽快维护。

关键：获取网络设备的工作状态；

问题：设备依赖于厂商，不同厂商具有不同的数据采集方法；

解决方法—标准化：网络普及和多厂商设备（异构性）融合，导致标准化的需求；

标准化的目标：统一管理的对象，定义为支持管理而需要交换的数据单元的格式和交换时序。

（2） ISO 网络管理标准化

1979年，启动ISO OSI网络管理标准化工作；
—CMIS（ISO10164，公共管理信息服务）定义网管功能和服务；
—CMIP（ISO10165，公共管理信息协议）定义支持功能和访问的协议。

基于**OSI**标准的产品（主要用于电信部门）：

AT&T的Accumaster
DEC的EMA
HP的OpenView最初版本。

（2） ISO 网络管理标准化—网络管理的功能

配置管理：定义、监测和管理系统的配置参数，
使得网络资源可用、性能较优。

故障管理：对网络设备进行监控，包括故障检测、隔离和恢复；
必要时通知系统管理员，进行人工干预。

计费管理：记录网络资源的使用情况，
统计已被使用的网络资源和估算用户应付的费用；

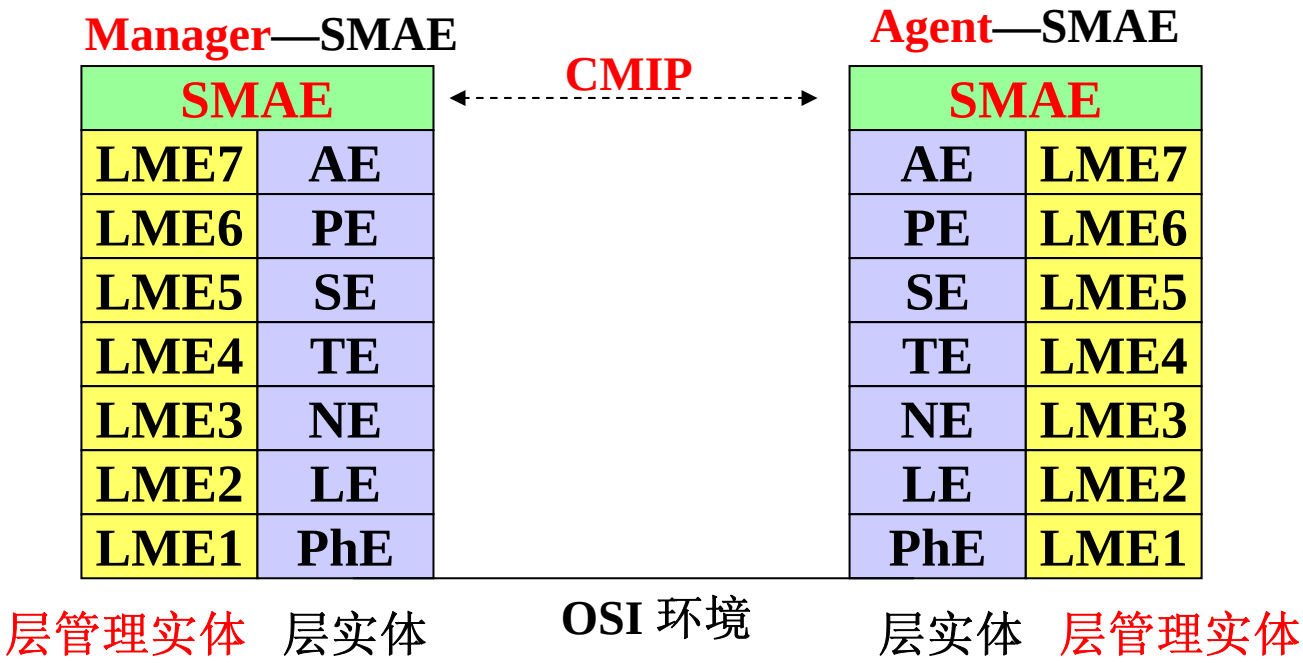
性能管理：收集和统计网络系统的数据（如网络的吞吐量、
用户响应时间和网络资源的利用率等），以便根据
统计信息来评价网络资源的使用等系统性能，分析
系统资源的使用趋势，或者平衡系统资源的负载。

安全管理：资源的授权管理、访问控制管理、安全检查跟踪
和事件处理、密钥管理（密钥分配）等。

（2） ISO 网络管理标准化—网管的体系结构

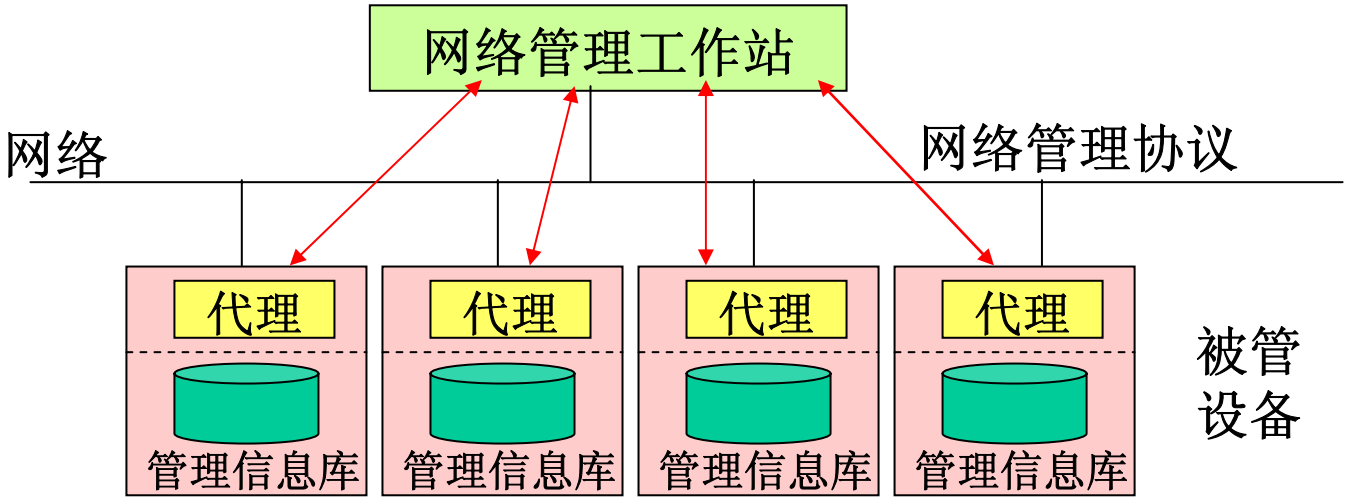
网管面向用户，属OSI应用层服务—

微观	网管涉及所有层次，因此，每层均设置对应实体； 各层管理实体协作，保证本层协议/功能正常运行/提供；
宏观	ISO/OSI的SAME分管理员和代理两类实体： 管理员：负责对整个网络的资源进行管理； 代　理：驻留在被管对象上，响应管理员的指令。 管理员和代理之间遵循公共管理信息协议（CMIP）。



LAN介绍时的维护周期？

（2） ISO 网络管理标准化—网管的基本模型



网络管理工作站：运行网管软件，收集被管网络设施的信息，进行汇总分析和反馈。

被管结点：网络交换设备、集中器、线路设备、用户结点等；运行网管（代理）软件，将被管设备的信息通过网络管理协议提供给管理工作站，包括主动监测和记录故障并报于管理工作站。

管理信息库：保存为网络管理目的而收集的信息。

网络管理协议：支持网管工作站（网管软件）和被管结点（代理软件）之间的数据交换。

（2） ISO 网络管理标准化—信息获取方式

收集被管设备数据的方法：主动轮询，被动中断。

—主动轮询：工作站周期性地轮询被管设备；

可能的问题：

轮询间隔的设置：长—及时性不好，短—占用资源多；

轮询顺序：设备之间的相互影响；

灾难响应：实时性略欠，主动性不足。

—被动中断（自陷）：被管设备主动传递数据

可能的问题：

传递周期设置：可能消耗资源；

设备故障数据的可传递性（优先级）。

CMIP采用类同“中断”的事件处理方式。

ISO OSI网管现状，受**OSI**产品影响，仅在电信部门少量使用。

（3） 网络管理实例—因特网网络管理

为支持因特网的管理，**IETF于1987年11月公布RFC1028—SGMP(Simple Gateway Monitoring Protocol—简单网关监控协议)**，集中监控网关的状态；

其后，因特网快速发展，**SGMP**不适应，研发新网管刻不容缓，并提出能力方面的要求：

—可伸缩性，可管理绝大部分符合**Internet**标准的设备；

—扩展性，通过定义新的“被管理对象”，可方便扩展管理能力；

—健壮性，即使设备发生严重故障，也不应影响管理者的正常工作（设备的独立性）。

研发成果：

—基于CMIP，研发CMOT (Common Management Over TCP/IP)，1989年4月公布RFC1095；（未推广）

—扩展SGMP，形成临时性的解决方案；1989年4月公布RFC1098—SNMP（Simple Network Management Protocol）。

★ 因特网网管协议—简单网络管理协议（SNMP）

为促进因特网网络管理标准化，IETF成立两个工作组。

管理信息库（MIB）工作组负责定义交换的元素及结构（对象）；

网络管理协议（SNMP）工作组定义管理实体之间交换的协议（交换的方式、格式和时序）；

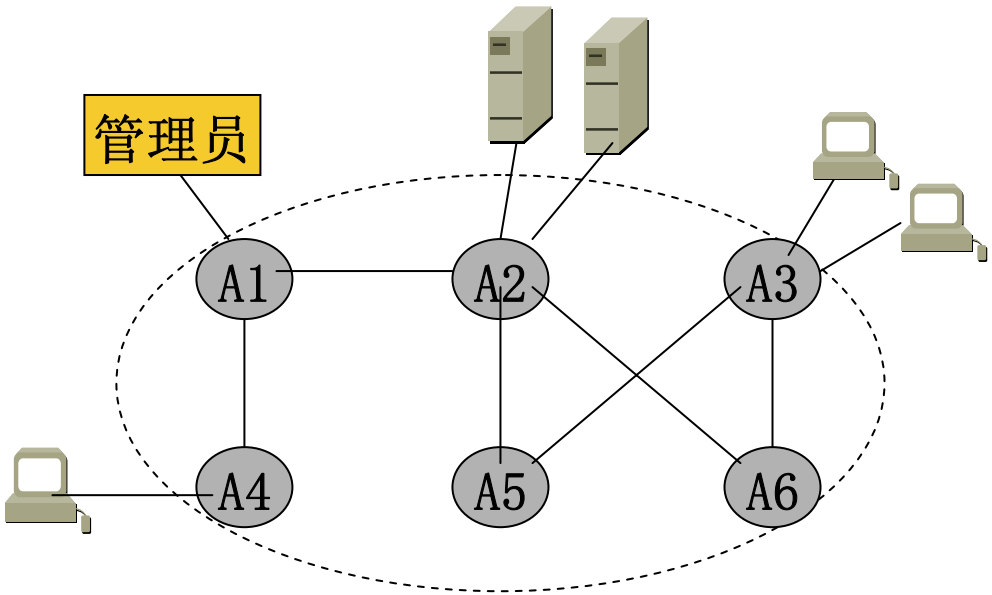
工作成果（1990年5月公布）：

RFC1157，Simple Network Management Protocol (SNMP) —简记SNMPv1；

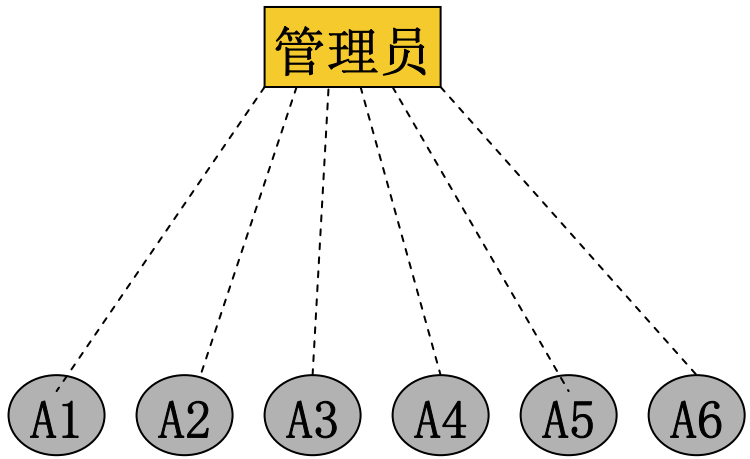
RFC1156，Management Information Base for network management of TCP/IP-based internets — 简记MIBv1；

☆ 简单网络管理协议（SNMPv1—RFC1157）

SNMPv1（RFC1157）采用集中管理模式，一个管理员管理多个代理；前者监控网络元素的状态，后者借助管理代理（**Agent**）执行网络管理的指令。



SNMPv1物理结构



SNMPv1逻辑结构

★ 因特网网络管理的工作方式

为了使一个管理员可以管理多个代理，同时，代理又可以主动报告出现的问题，**SNMP**采用具有自陷能力的轮询机制；

- 管理员和代理之间主要以请求/应答方式工作；

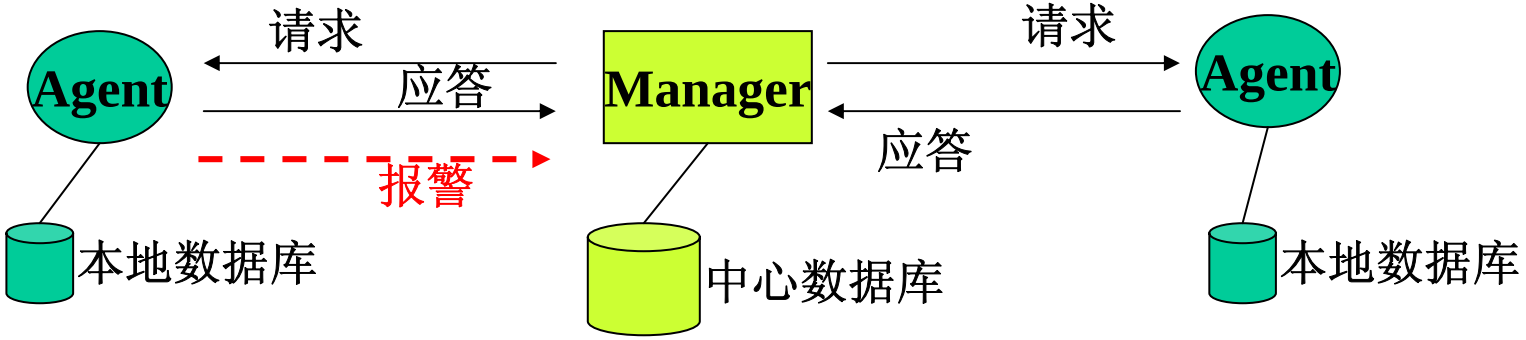
  管理员周期性向代理发出“请求”指令，获取或者设置网络元素的参数；代理向管理员返回“应答”响应，报告“请求”的执行结果；

- 如果代理发现设备故障，主动向管理员报警（自陷）。

为了使得管理工作可以延续，管理员和代理分别维护全局和本地数据库（习惯上称管理信息库—**MIB**）。

本地数据库保存结点的参数及运行状况；

中心数据库保存全网（或者区域）的设备参数等。



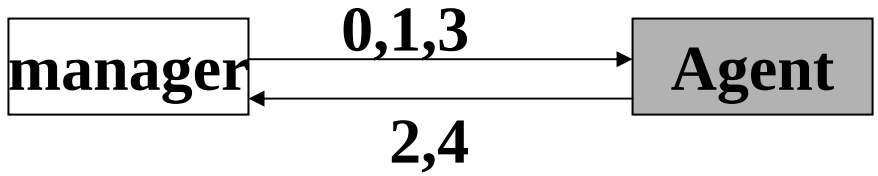
☆ 简单网络管理协议（SNMPv1—RFC1157）

SNMP作用于应用层，利用UDP的两个端口（161和162）实现管理员和代理之间的管理信息交换。

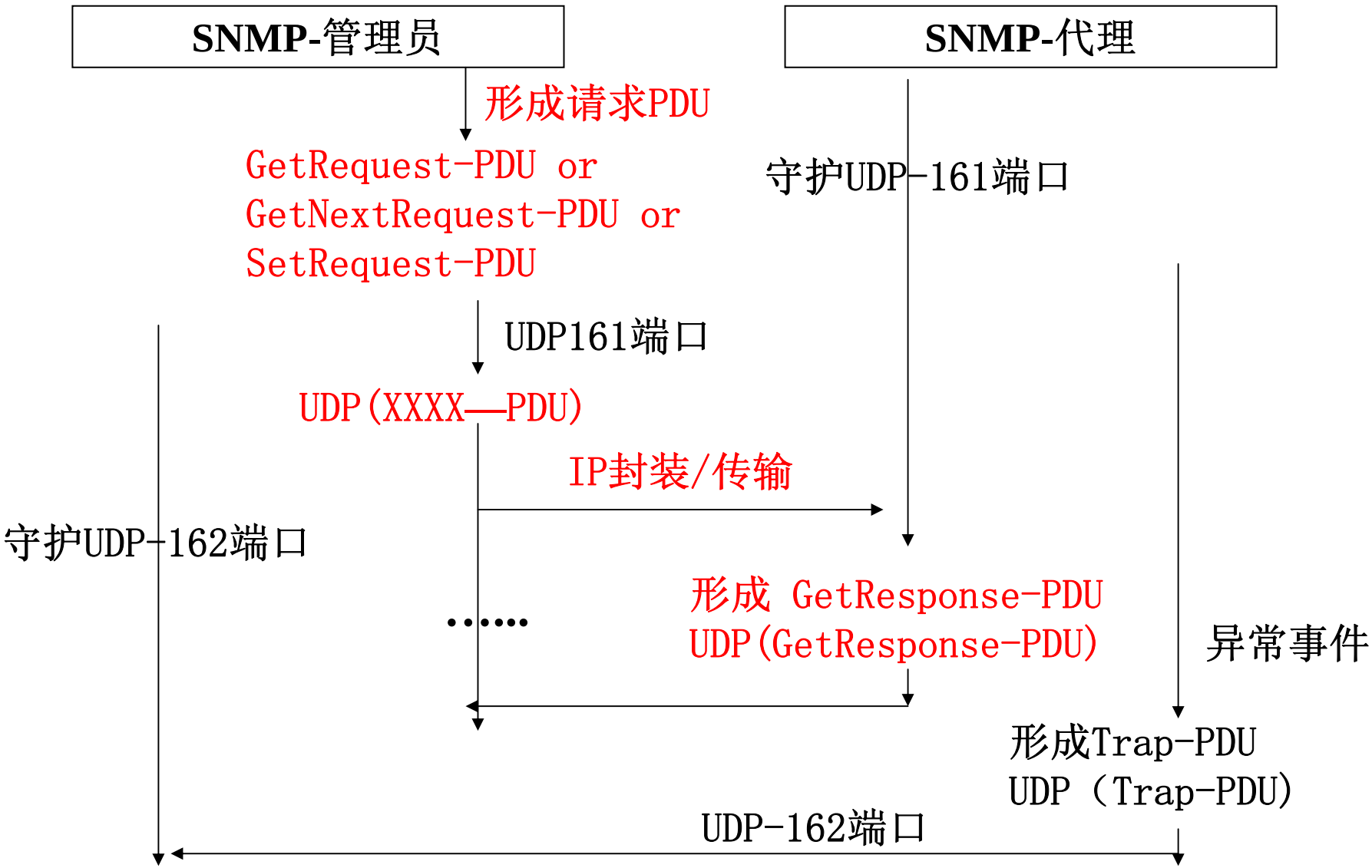
UDP端口161用于数据收发，UDP端口162用于代理报警；

管理员/代理之间交换的PDU（五种类型）：

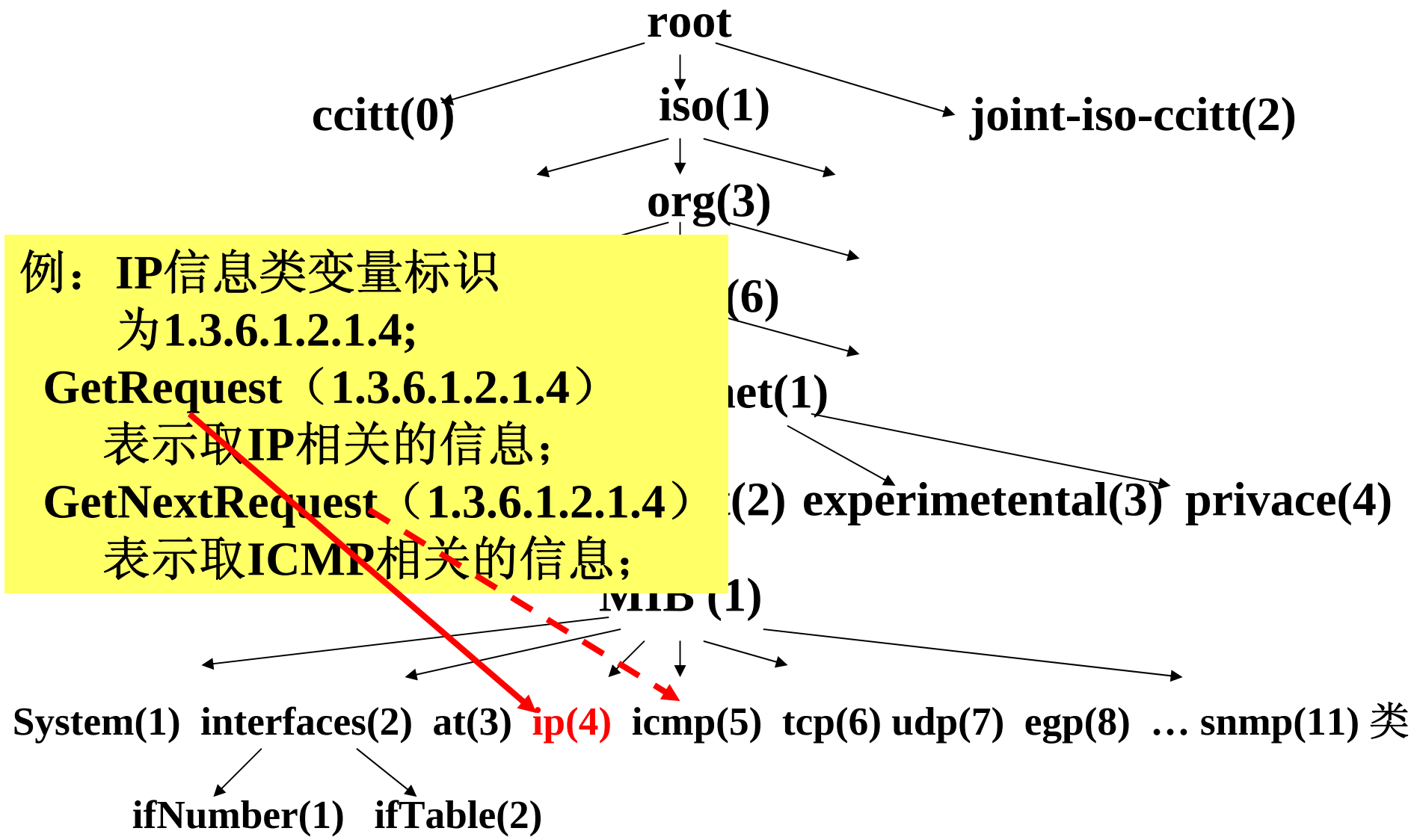
名称	编码	功能说明
GetRequest	0	管理员至代理，查询指定变量的值；
GetNextRequest	1	管理员至代理，查询下一变量的值；
GetResponse	2	代理至管理员，回送执行结果（正确/差错）；
SetRequest	3	管理员至代理，设置代理维护的某个变量的值；
Trap	4	代理至管理员，主动传递报警信息。



☆ SNMPv1的信息交换过程—基于UDP的请求/应答



☆ MIB库中变量的标识（交换的对象）：

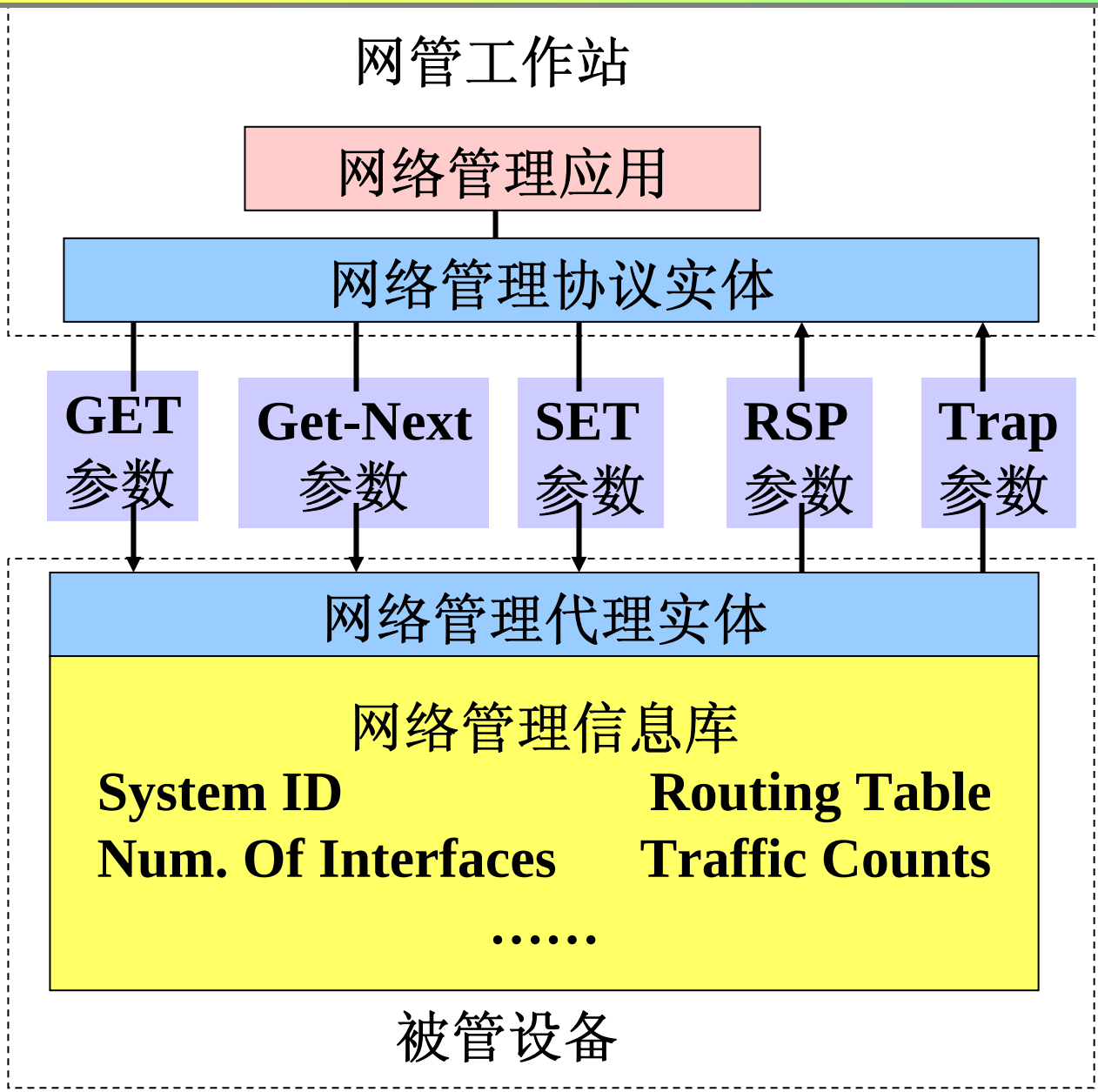


树状结构有利于体现变量的唯一性。

☆ SNMP信息分类（11类，175项）

编码	类/组别	项数	内 容 描 述
1	系统类	7	元素名称、厂商、硬件类型、软件版本、启停时间等
2	接口类	23	网络元素的接口数目、带宽、流量等
3	地址迁移类	3	物理地址和网络地址（如IP地址）对应关系等
4	IP类	42	进、出、丢弃IP数据报统计，IP地址及掩码、路由信息等
5	ICMP类	26	ICMP报文的统计信息，含出错分类统计
6	TCP类	19	TCP连接数、收发TCP报文统计，重发算法及次数统计等
7	UDP类	6	收发的UDP报文统计
8	EGP类	20	支持外部网关协议（EGP）的流量统计信息
9	保留	0	待扩充
10	保留	0	待扩充
11	SNMP类	29	SNMP报文统计信息（包括通信量统计）

SNMP基本通信结构：


网管工作站
网络管理应用
网络管理协议实体
GET
参数
Get-Next
参数
SET
参数
RSP
参数
Trap
参数
网络管理代理实体
网络管理信息库
System ID
Routing Table
Num. Of Interfaces
Traffic Counts
……
被管设备

★ 因特网网络管理协议—简单网络管理协议（SNMPv2）

随着规模扩大，集中管理方式受限，管理员成为瓶颈，**IETF**于**1992**年启动升级工作；

目标：

1、分域管理，提高效率；

2、安全和高效传递管理信息，包括提供验证、加密和时间同步机制，以及增加批量索取的能力）等。

成果：**SNMPv2**和**MIBv2**

因安全性方面存在分歧，故**1996**年**1**月提出的**SNMPv2**草案仅解决了分域管理和高效传输问题。

RFC1905，Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)；

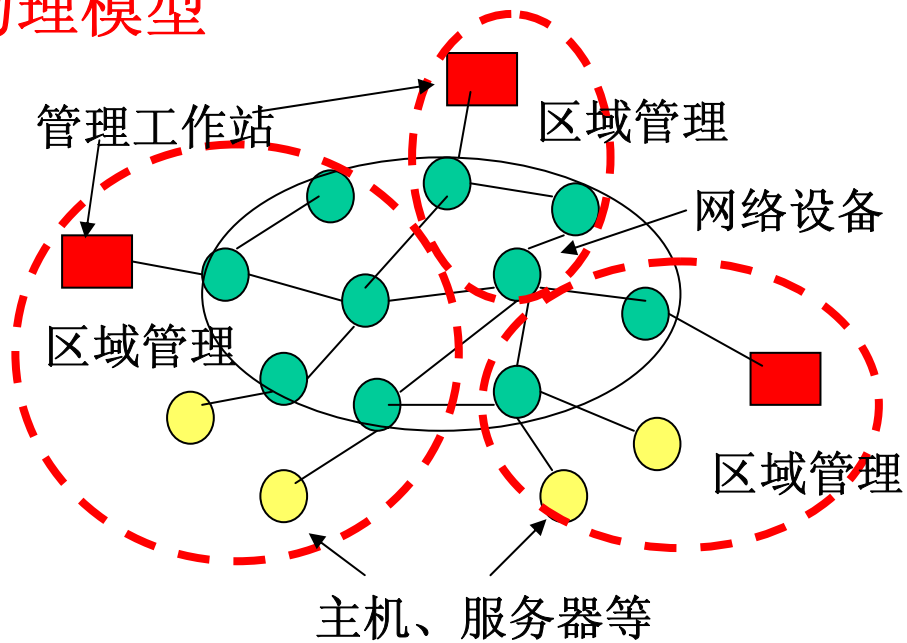
RFC1907 Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)；

（3） 网络管理实例—因特网网络管理

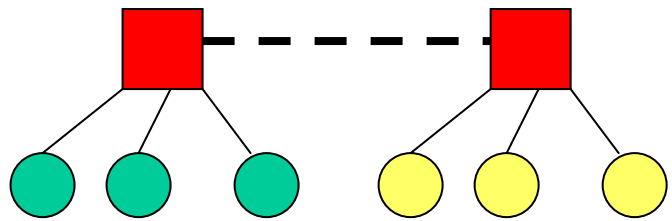
★ SNMPv2网络管理模型

SNMPv2采用域内集中、域间分布的分域管理思路。

物理模型



逻辑模型

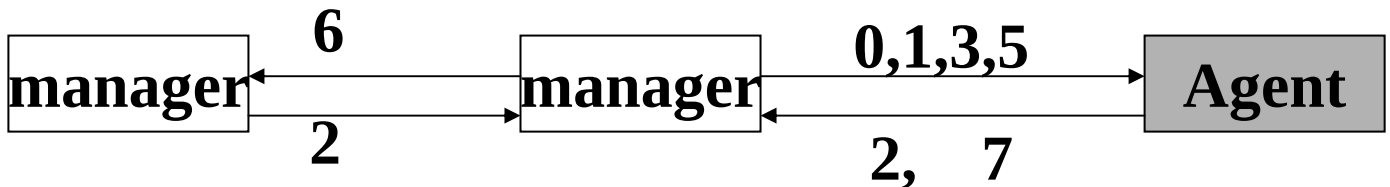


网络元素

☆ 简单网络管理协议（SNMPv2—RFC1905）

SNMPv2引进区域管理（分布式管理）的思想，扩充了管理员之间的操作。并用Snmpv2-Trap取代了原Trap报警PDU。

名称	编码	功能说明
GetRequest	0	管理员至代理，查询指定变量的值；
GetNextRequest	1	管理员至代理，查询下一变量的值；
Response	2	至管理员，回送执行结果（正确/差错）；
SetRequest	3	管理员至代理，设置代理维护的某个变量的值；
GetBulkRequest	5	管理员至代理，传递批量信息；
InformRequest	6	管理员至管理员，传递参数处理请求；
SNMPV2-Trap	7	代理至管理员，传递报警信息；（取代原4）



★ 因特网网络管理协议—简单网络管理协议（SNMPv3）

为解决**SNMPv2**的遗留问题，**1997**年**4**月，**IETF**成立了**SNMPv3**工作组。**SNMPv3**的重点是安全、可管理的体系结构和远程配置。

针对可能的威胁：未授权的修改信息、操作指令、报文流的修改、拒绝服务、流量分析等；

工作成果：2002年公布SNMPv3。

RFC3412，Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)；

RFC3413，Simple Network Management Protocol (SNMP) Applications;

RFC3414，User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)；

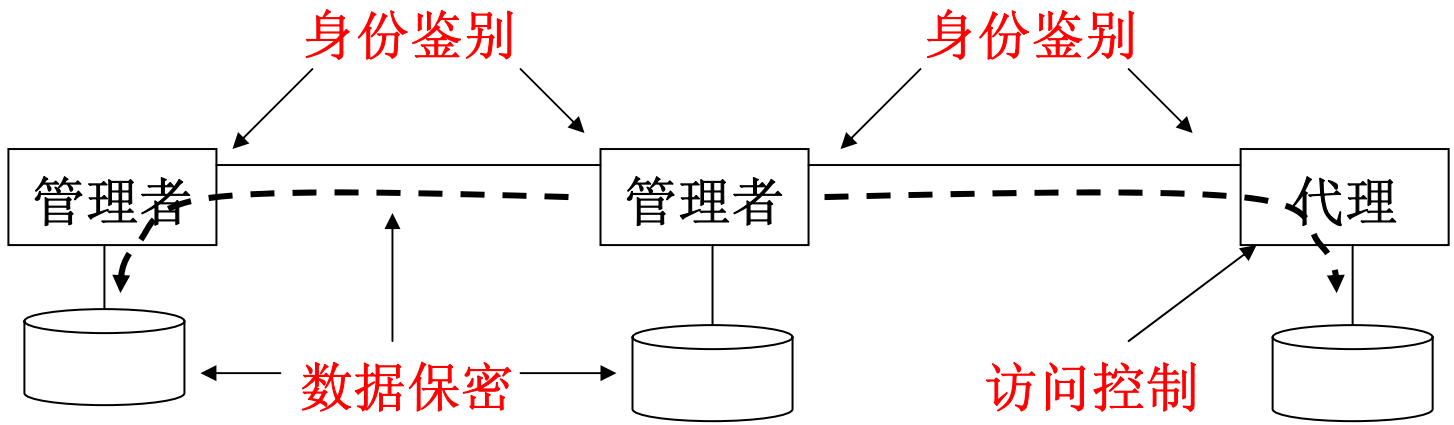
☆ 简单网络管理协议（SNMPv3—RFC2273）

在SNMPv2的基础上，扩充相关安全功能；

身份鉴别：实体鉴别，确保收到的指令或者数据来自于真实的实体；

数据保密：MIB信息存储保密和PDU传输保密，确保指令或者数据不被截取、伪造、篡改和重放；

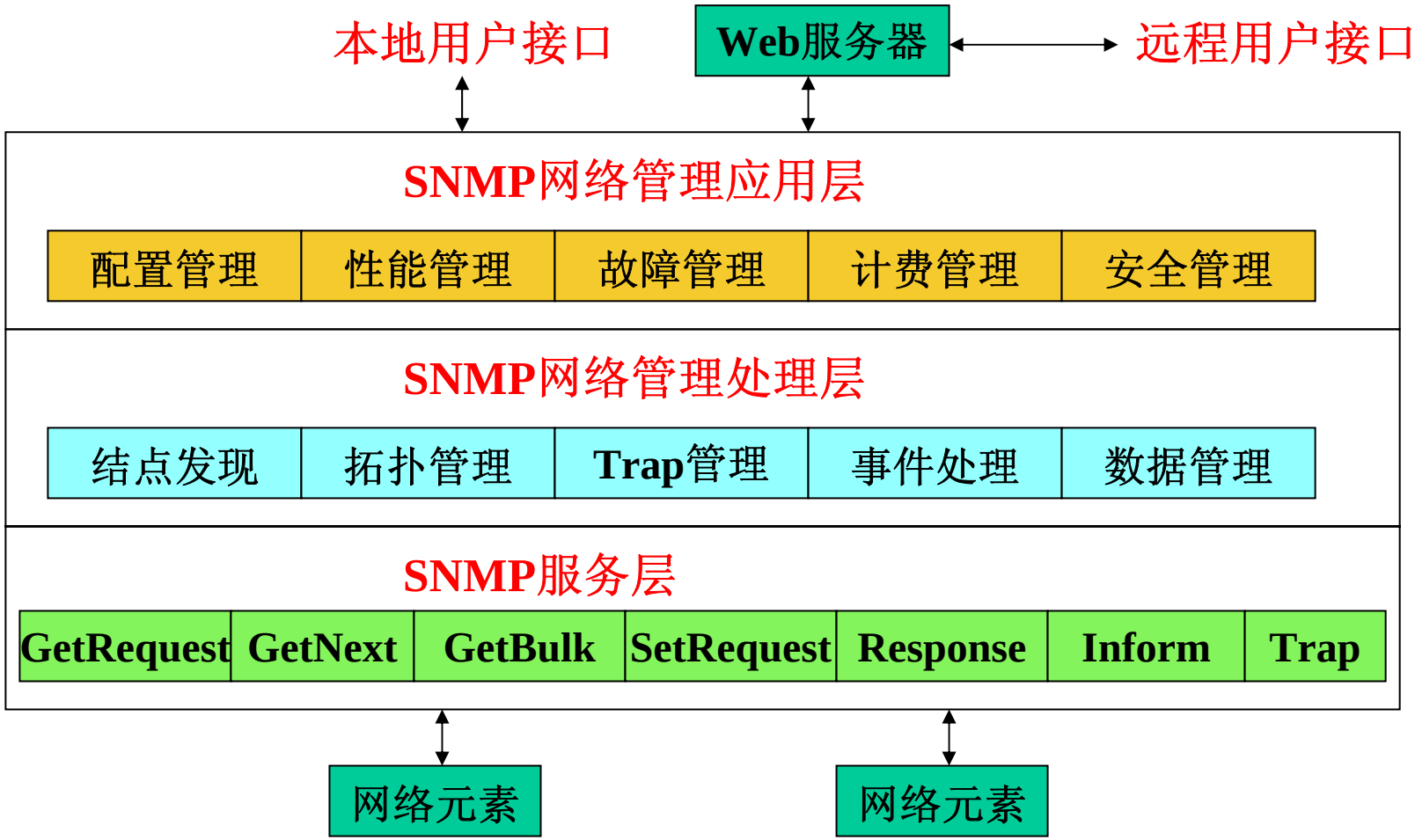
访问控制：实体授权和访问控制，禁止越权或者非授权操作。



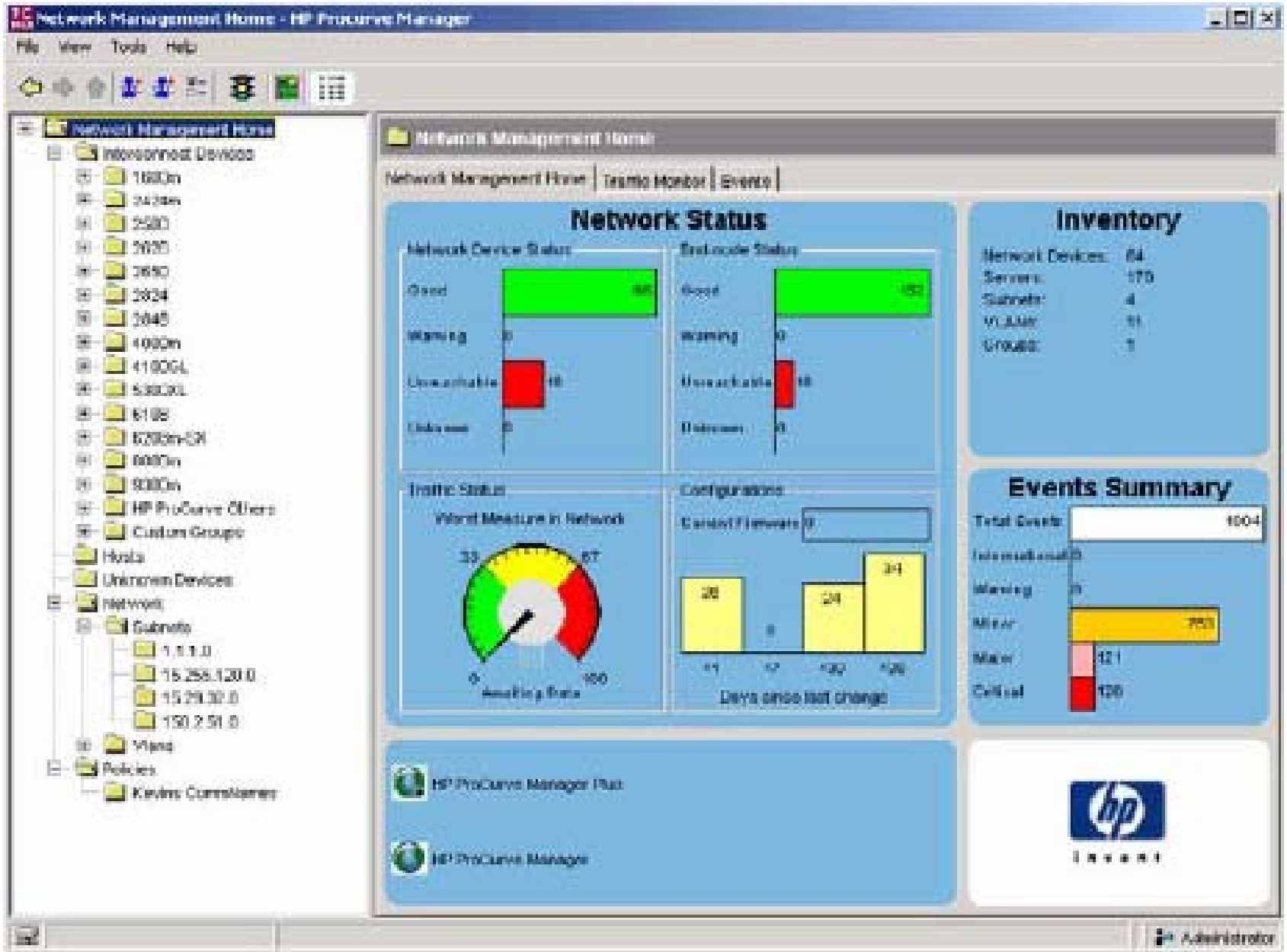
现状：目前实用的大部分管理系统仍然基于SNMPv2；

☆ SNMP产品的一般结构

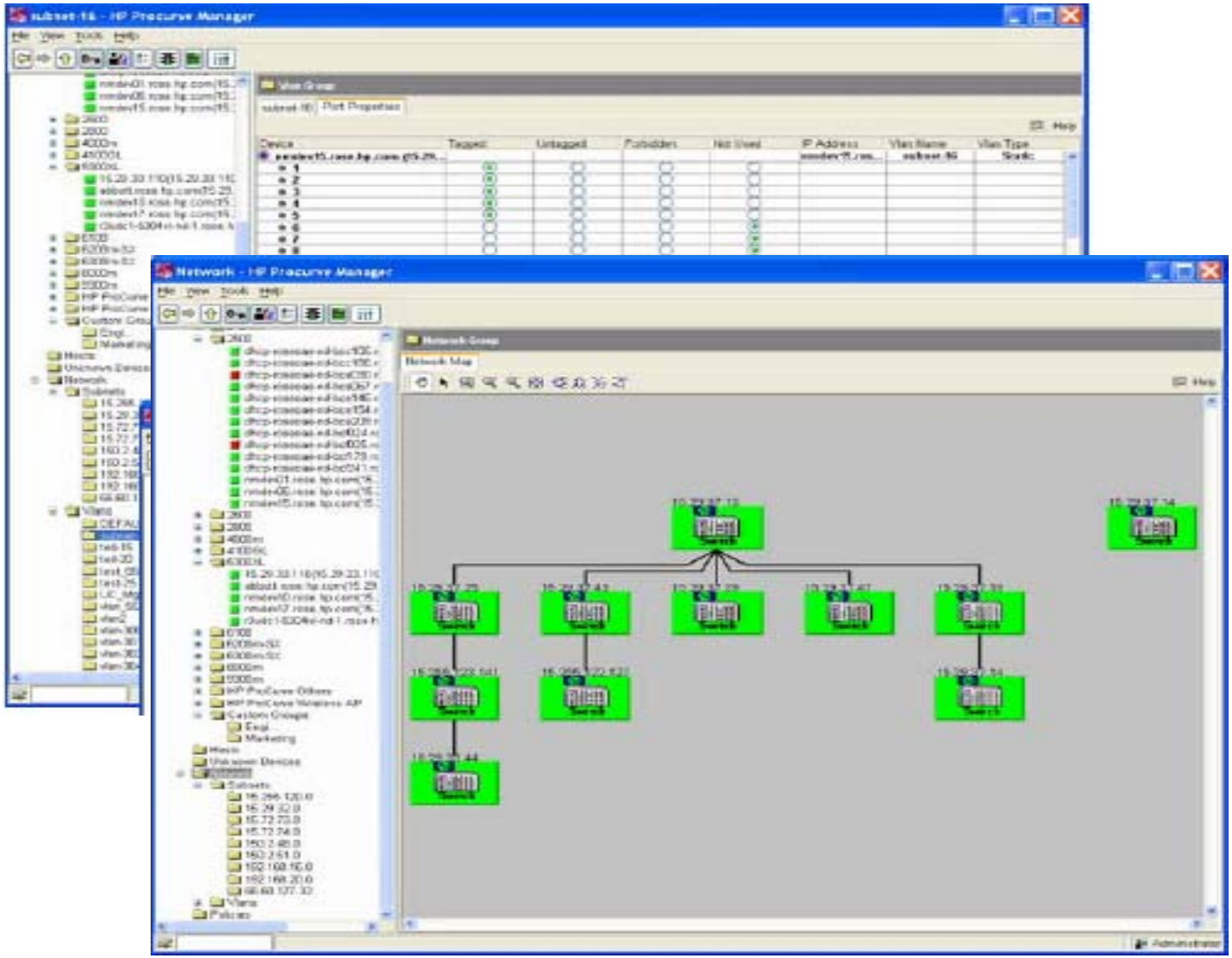
SNMP仅定义了网络元素的参数传递，如何利用这些参数为人类管理员服务是产品追求的目标。



HP ProCurve Manager（实例）—直观：



HP ProCurve Manager（实例）—直观：

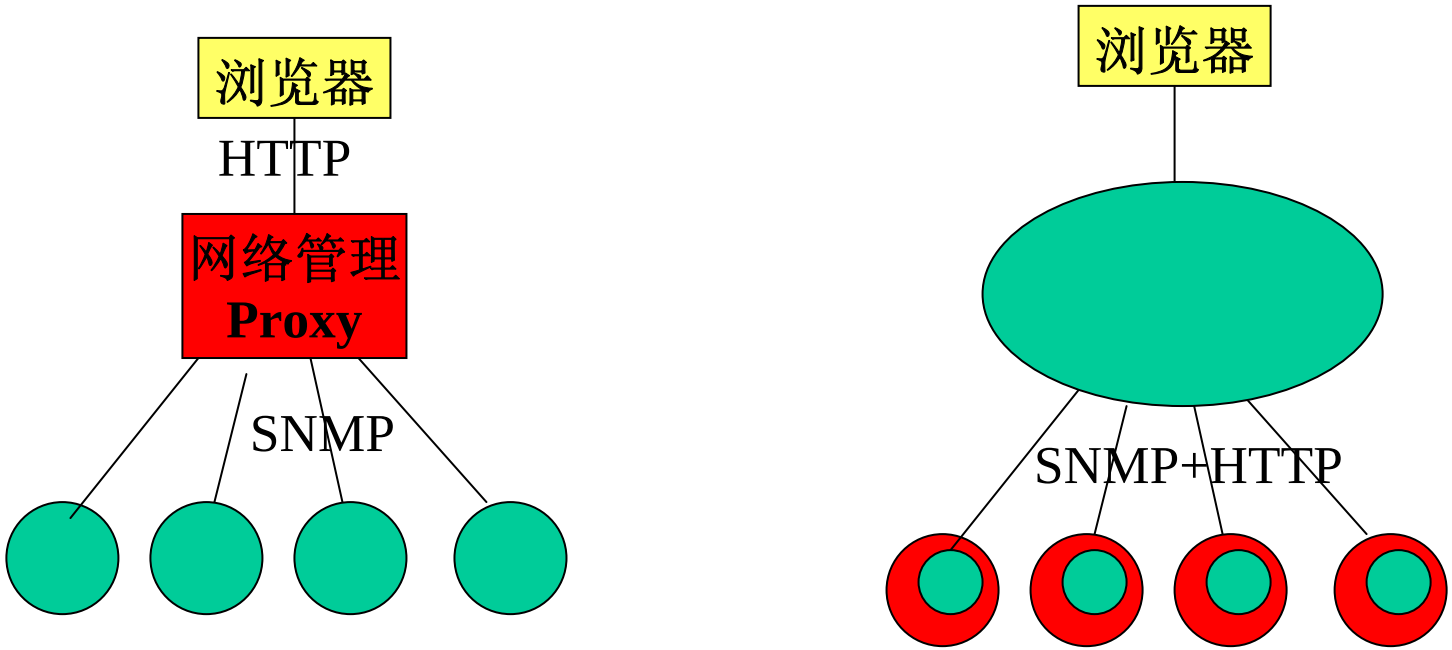


因特网网络管理的可能发展趋势：

基于**Web**的管理：易用

—Web分离（代理方式）：

—Web嵌入（**Web**功能嵌入被管设备）。



网管软件选择时需考虑的一些问题

网络管理是一个渐进过程，在规划网管系统时，要重点考虑以下几个方面：

1、基于现有网络，兼顾升级额外的功能；

2、符合工业标准，支持第三方插件的能力；；

3、统一数据库，在不同的网络管理平台进行管理，而不需建立不同的映像和相应的数据库；

4、产品具有通用性，企业环境具有独特性，适配企业和二次开发具有必然性，提供接口的必要性；

5、网管系统运行和企业管理机制、人员分配、职责划分等管理因素有着密切相关。

网管软件选购原则

- 以业务为中心：满足应用需求，支持业务流程，具有基于策略的主动网管能力，多种报警方式。
- 为应用和服务提供环境：保证网络及部件能提供与用户完成业务流程所需的资源，服务水平与企业需要的匹配。
- 具有可用性、可扩展性和易用性：简单、直观、易于使用（培训成本）和一致，以便提高二次开发的效率。
- 性能价格比：可解决各部门需求不一致的冲突。
- 标准支持和协议的独立性：支持现有甚至新兴的标准，包括支持**SNMP**、**DHCP**和**DNS**、**DMI**（桌面管理规范）。

8.2 网络安全

（1） 概述

① 资源共享与安全

联网的目的：资源（信息、软件、硬件等）的共享；

信息资源具有宿主，具有使用的价值，驱使合法或者非法用户的获取或者窃取；

信息资源往往具有有效期价值，为非法获取形成一定的障碍；

期望：信息资源的安全共享；

网络安全：与网络相关设施（网络架构、介质、数据/信息）的安全/防护，确保网络资源按照预定的策略仅供授权用户使用；

（1） 概述

① 资源共享与安全

★ 信息的安全：

信息系统的安全，涉及操作系统、应用软件等，包括病毒、软件Bug和系统运行环境等；

数据的安全，涉及数据的存储、访问，包括权限等；

★ 网络环境的安全问题：

安全的模糊性（安全是相对的、复杂的、安全链条）

网络的开放性（互不了解、匿名使用、恶意系统）；

产品的垄断性（厂家保护知识产权，容易出现安全漏洞）；

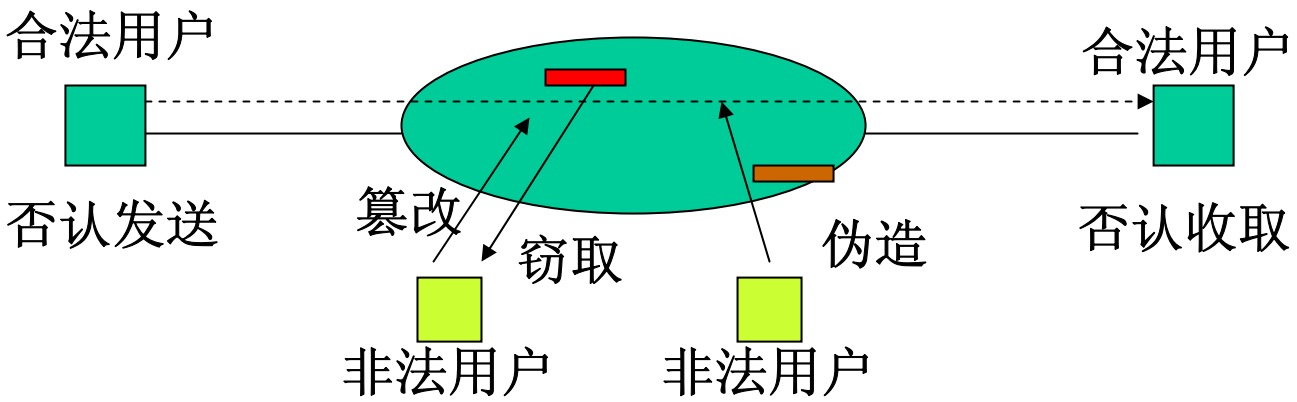
人类的天性（好奇心/表现欲、惰性/求方便导致可乘之机）；

技术的快速发展导致难以掌握系统的安全特性，……。

② 网络安全的目的

保护网络资源（此处主要指信息资源），免受攻击；

基于网络的应用可能受到的安全威胁：



截取（窃取）：非法截取网络信息，窃取其中的机密；
篡改：对截取的数据进行部分/全部篡改，再送到目的地；
伪造：冒充合法用户进行网络操作，嫁祸于人；
重播/插播：干扰用户的正常操作；
发方否认：否认已向接受者发送过数据；
收方否认：否认已收取过发送方发送的数据。

其它：……。

③ 抵御攻击的安全服务

网络安全服务	功能描述	
内容保密	防止报文内容被未授权地阅读，防窃取；	
内容完整性	保证被交换的报文未被篡改，防篡改；	
序列完整性	防止数据的重播和丢失，防重播和插播；	
实体鉴别	鉴别数据的来源和通信实体的身份，防伪造/冒充；	
抗发方否认	防御发送方否认曾经发送过报文；	防否认
抗收方否认	防御接收方否认曾经收取过报文。	

注：所有的服务只能保证出现的攻击可以被识别，并不能防止攻击的发生。

上述安全服务的基础：密码学—数据加密技术

（2） 基础技术

① 数据加密技术 — 也称密码技术

★ 术语

加密：明文（原文）到密文，对应的算法称加密算法；

解密：密文还原明文，对应的算法称解密算法；

密码算法：加/解密算法统称, 实现明文和密文之间映射的算法；

—密码算法应当具有放大功能，使得当明文**X1**和**X2**差别很小时，对应生成的密文**Y1**和**Y2**差别很大；

—数据加密实质上是数据表示形式的变换，加密/解密与语义有关，具有相对性。

密钥：参与加密/解密过程的参数，密码算法的可变参数。

—密码算法应当是稳定安全的，即密钥的**n**个比特对密码体系安全性的贡献比较平均，无论攻击者知道其中哪**K**个比特，其破译难度是相同的。

① 数据加密技术 — 术语

代换：用一组(个)符号(字符)替换另一(组)个符号(字符)，改变明文内容的表示形式，但内容元素之间的相对位置保持不变。

置换：依据某种规则变换明文信息的顺序，改变明文内容元素的相对位置，但保持内容的表现形式不变。

—代换表（密码本）和置换规则构成参与变换的参数，

成为加密/解码的核心。

数据加密的目的：利用某种变换技术，将原文（明文）变换为一般用户无法识别的密文，即数据以密文的形式在网络上传输；

传统加密技术：仅采用代换和置换（包括多重使用）的加密技术

例： **AB** （**01000001 01000010**）

循环右移**4**位（或左右**4**位交换）

DC4（控制字符） **$**（**00010100 00100100**）

★ 传统加密技术举例：

代换：英文字母位置颠倒，空格变*号等；—映射表

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z　*+-?/

Z Y X W V U T S R Q P O N M L K J I H G F E D C B A*　-+/?

置换：**34251**

则：

原文：**I told you**

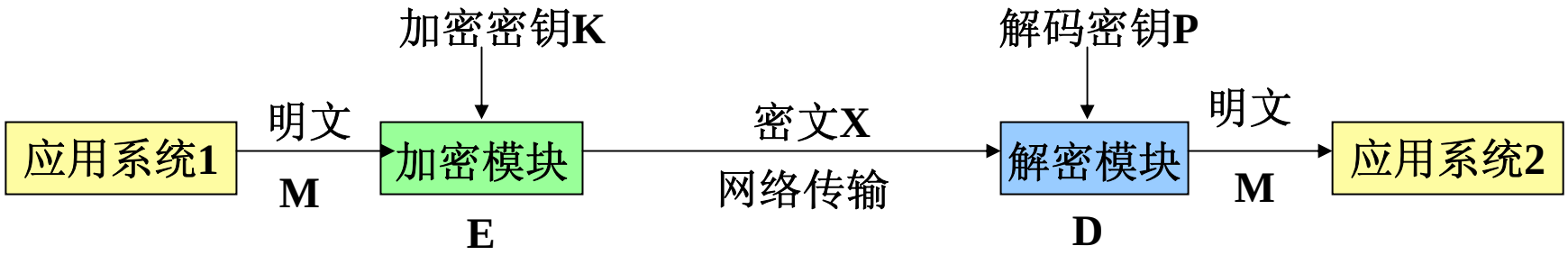
代换：**R*glow*blf**

置换：**gl*oRbl*fw**

设想：如果利用编程予以实现，则映射表和置换规则可以作为加密程序的参数（密钥），使用不同的参数可以得到不同的结果。

★ 加密/解密过程

明文到密文 和 密文还原明文 的过程。



习惯记法：

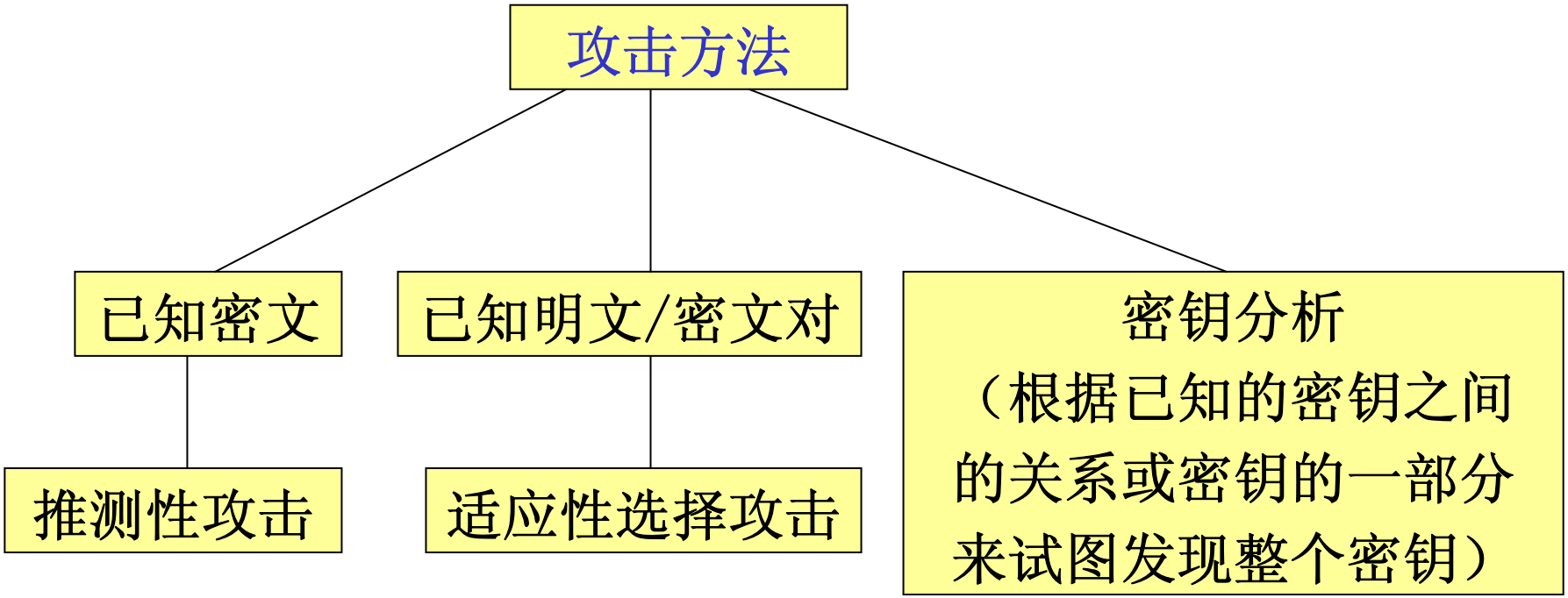
对应明文M、密文X、加密密钥K和解密密钥P，有：

$X = E_K$（M）—用密钥K对明文M进行加密，形成密文X；

$M = D_P$（X）—用密钥P对密文X进行解密，还原明文M；

针对上面的模型有：　$M = D_P(E_K(M))$

加密系统的一般攻击方法



评价加密算法指标：强度（破译难度，信息具有时效性），
速度（系统开销），
算法的可公开性（方便应用）。

一切秘密应寓于在密钥中：密码（加/解密）算法是可以公开的，而密钥内容不可全部公开。

★ 数据加密算法 —密码系统的计算安全性

- 若能从密文X推出明文M或密钥K，或从明文M和密文X推出密钥K，则称对应的密码算法是可破译的。
- 若无论有多少密文X都不能推出明文M，则称对应的密码算法是理论不可破译的。
- 若密码系统原则上可破译，但无法在希望的时间内或允许的经济条件下实现破译，则它是实际不可破译的。

加密算法安全性评估：

- 加密算法的安全性基于计算可行性
  - —破译的代价是否大于可能获得的结果
  - —破译的时间是否大于结果的有效期
  - —能否产生足够多的数据供破译使用
- 对某种密码算法的破译能力本身也是一个秘密。

★ 数据加密算法 —算法分类：

按加密模式分类：

— 序列密码（流密码）：按位或字节加密，密文不仅与最初给定的密码算法和密钥有关，同时也是被处理的数据段在明文（或密文）中所处的位置的函数。

— 分组密码（块密码）：将明文分成固定长度的组作为输入，输出也是固定长度的密文。密文仅与最初给定的密码算法和密钥有关，与被处理的数据段在明文（或密文）中所处的位置无关。（常用）

➢ 分组密码体制的设计要求

— 分组长度要足够大，以防止穷举明文空间攻击。例如8比特分组只有256个可能的值。

— 密钥要有足够长度，以防止穷举密钥攻击。

— 密码算法应足够复杂，不存在简洁的数学破译方法。

★ 数据加密算法 —算法分类：

按密钥体制分类：

依据：加密密钥和解密密钥之间的关系；

$$M = D_P（E_K（M））$$

— 对称密钥加密体系（秘密密钥 / 单密钥加密体系），加密密钥与解密密钥相同，或者一个可以从另一个导出；

— 非对称密钥加密体系（公开密钥 / 双密钥加密体系），从一个密钥去推导另一个密钥是计算不可行的。

★ 数据加密算法 — 对称密钥加密算法

秘密密钥加密体系（一类加密算法）：

解密密钥等同于加密密钥，或者可以由加密密钥导出；

即通信双方共享一个密钥（**K=P**），**$M=D_K(E_K(M))$**。

典型算法：**DES**算法，以及由此而延伸出的**3DES**、**IDEA**等；

基本原理：代换和置换的多重使用；

特点：通信双方维护相同的密钥（静态分配密钥）；

对应**N**个通信伙伴应维护**N**个密钥，用户维护信息量大；

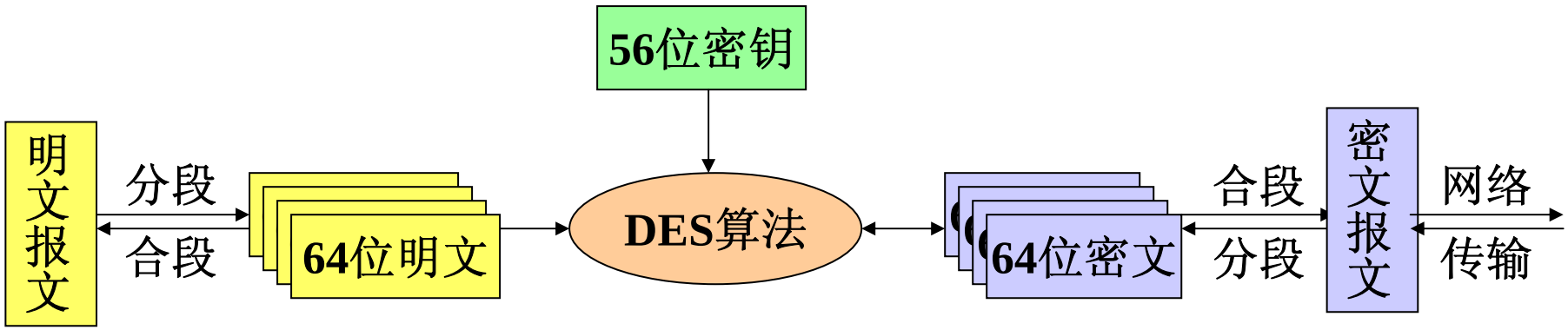
无法用于群组内的安全通信；

算法较简单，加密/解密速度快。

DES加密算法：

1973年5月和1974年8月美国国家标准局征求用于计算机的加密算法，选择了1972年IBM公司的W.Tuchman和C.Meyer研制的Luciffer加密算法，1975年3月公开征求意见，1977年1月定为数据加密标准（DES），1979年美国银行协会批准使用，1980年成为美国标准化协会（ANSI）的标准，1984年2月纳入国际标准。

原理：通过64位的密钥将64位的明文（密文）加密（解密）为密文（明文）；64位密钥对应8字节，实际使用56位（8位校验），因此，密钥空间2^{56}；循环迭代使用移位、置换（换序）、选择（64b→56b→48b→32b）、扩展（32b → 48b）和模2加操作来获得结果。



DES加/解密算法伪代码：

DES加密算法：

```
Decrypt（M，K）
{
  K_T=IP_{64-56}（K）
  For i=1 to 16 do {   /*密钥*/
    K_T=MP(K_T) ;
    K_i = IP_{56-48}（K_T）；  }
  L_0R_0 =  IP（M）
  For i=1 to 16 do {   /*加密* /
    L_i = R_{i-1};
    R_i = L_{i-1} + f(R_{i-1},K_i);  }
C = IP^{-1}(R_16L_16)
}
```

DES解密算法：

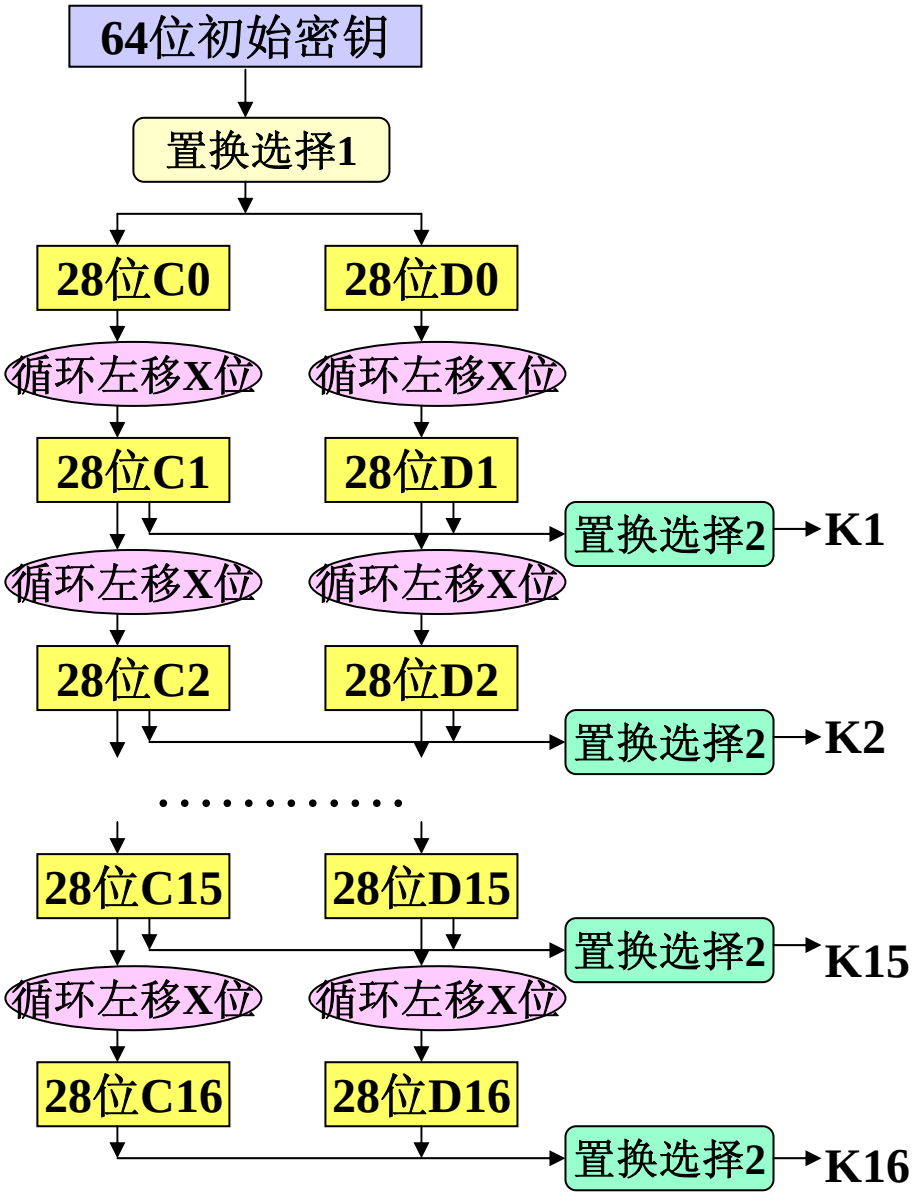
```
Encrypt（C，K）
{
  K_T=IP_{64-56}（K）
  For i=1 to 16 do {  /*密钥*/
    K_T=MP(K_T) ;
    K_i = IP_{56-48}（K_T）；  }
  L_16R_16 =  IP（C）
  For i=16 to 1 do {  /解密*/
    R_{i-1} =  L_i ;
    L_{i-1} = R_i + f(L_i, K_i);}
  M = IP^{-1}(L_0R_0)
 }
```

M—64位明文，C—64位密文；

MP—移位；　　K—初始密钥；

IP—置换；　　IP^{-1}—逆置换。

密钥的形成：



移位X = 1 i=1,2,9,16;
2 i=3-8,10-15;

置换选择1（64位中取56位）：

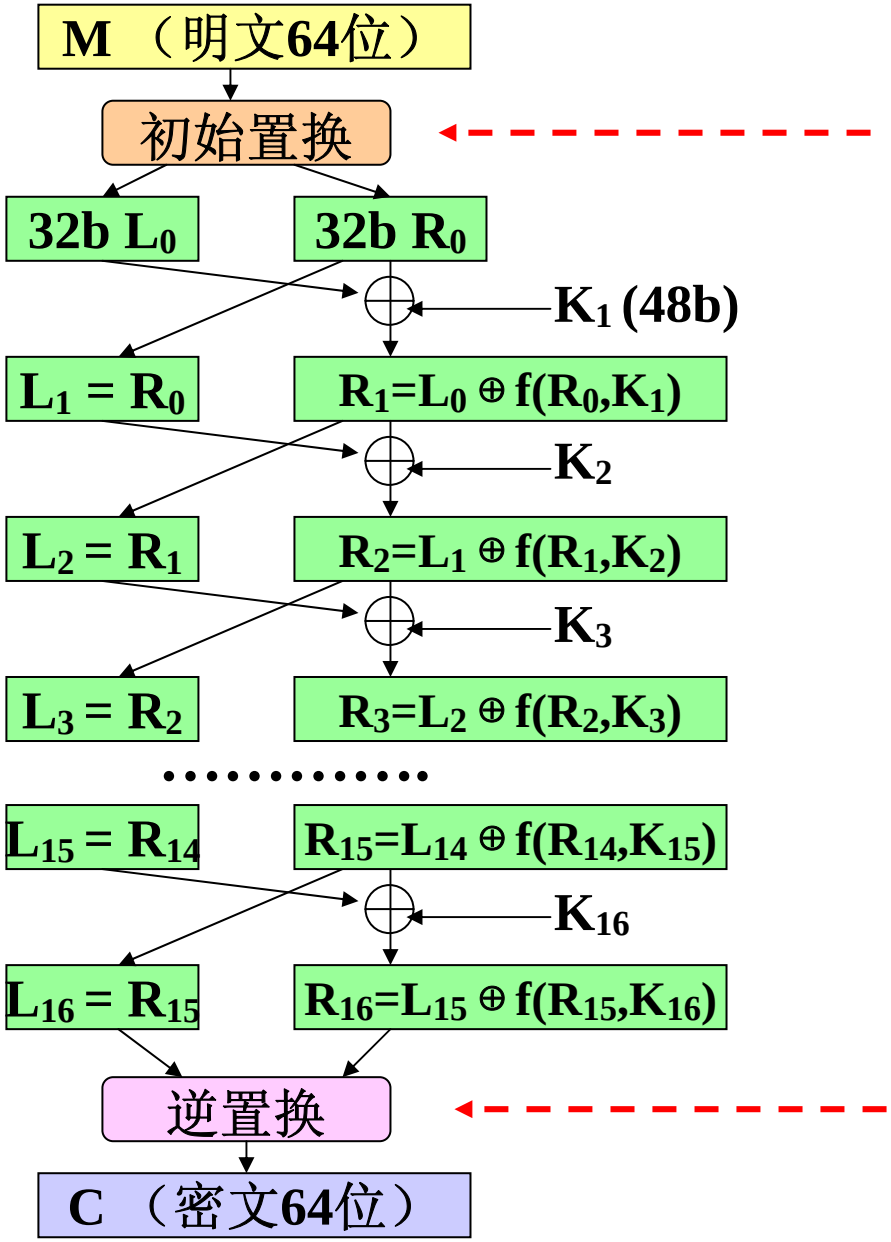
C0：57 49 41 33 25 17 9 1
58 50 42 34 26 18 10 2
59 51 43 35 27 19 11 3
60 52 44 36

D0：63 55 47 39 31 23 15 7
62 54 46 38 30 22 14 6
61 53 45 37 29 21 13 5
28 20 12 4

置换选择2（56位中取48位）：

14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

DES加密算法：　64b明文 → 64b密文



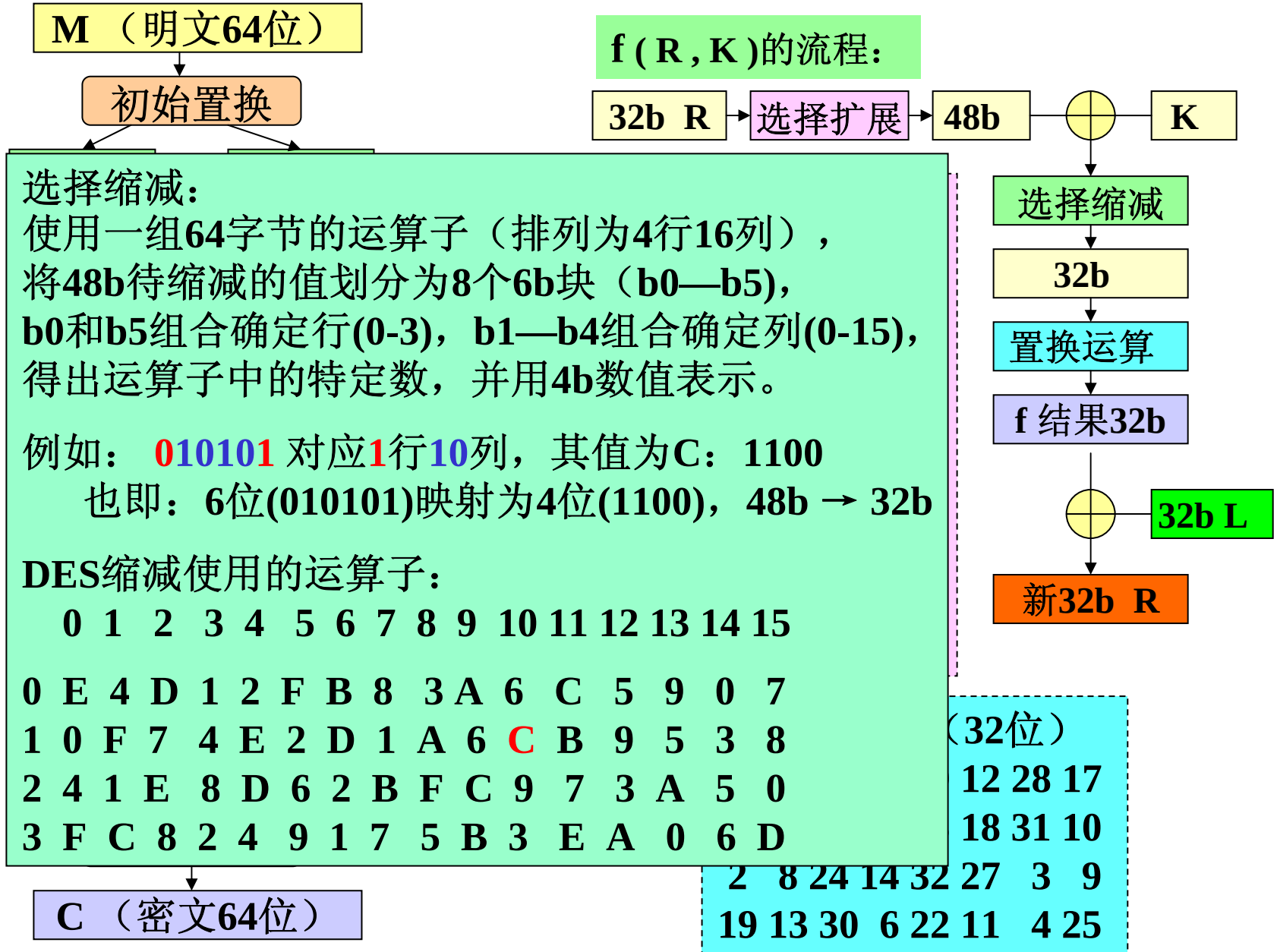
初始置换：（64位）

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	35	37	29	21	13	5
63	55	47	39	31	19	15	7

逆置换：（64位）

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

DES加密算法：　64b明文 → 64b密文



选择缩减： 48b → 32b

事先定义一组64B的运算子排列为4行16列，
再将48b待缩减的值划分为8个6b块，
b0和b5的组合对应行（0-3），b1b2b3b4的组合对应列，
得出运算子中的特定数，转换为4b的数值表示。

缩减块举例（48b中的某个6b）：

010101 对应1行10列，其值为C：1100

也即：6位(010101)映射为4位(1100)，48b → 32b

运算子举例：

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7
1	0	F	7	4	E	2	D	1	A	6	C	B	9	5	3	8
2	4	1	E	8	D	6	2	B	F	C	9	7	3	A	5	0
3	F	C	8	2	4	9	1	7	5	B	3	E	A	0	6	D

DES加/解密算法伪代码：

DES加密算法：

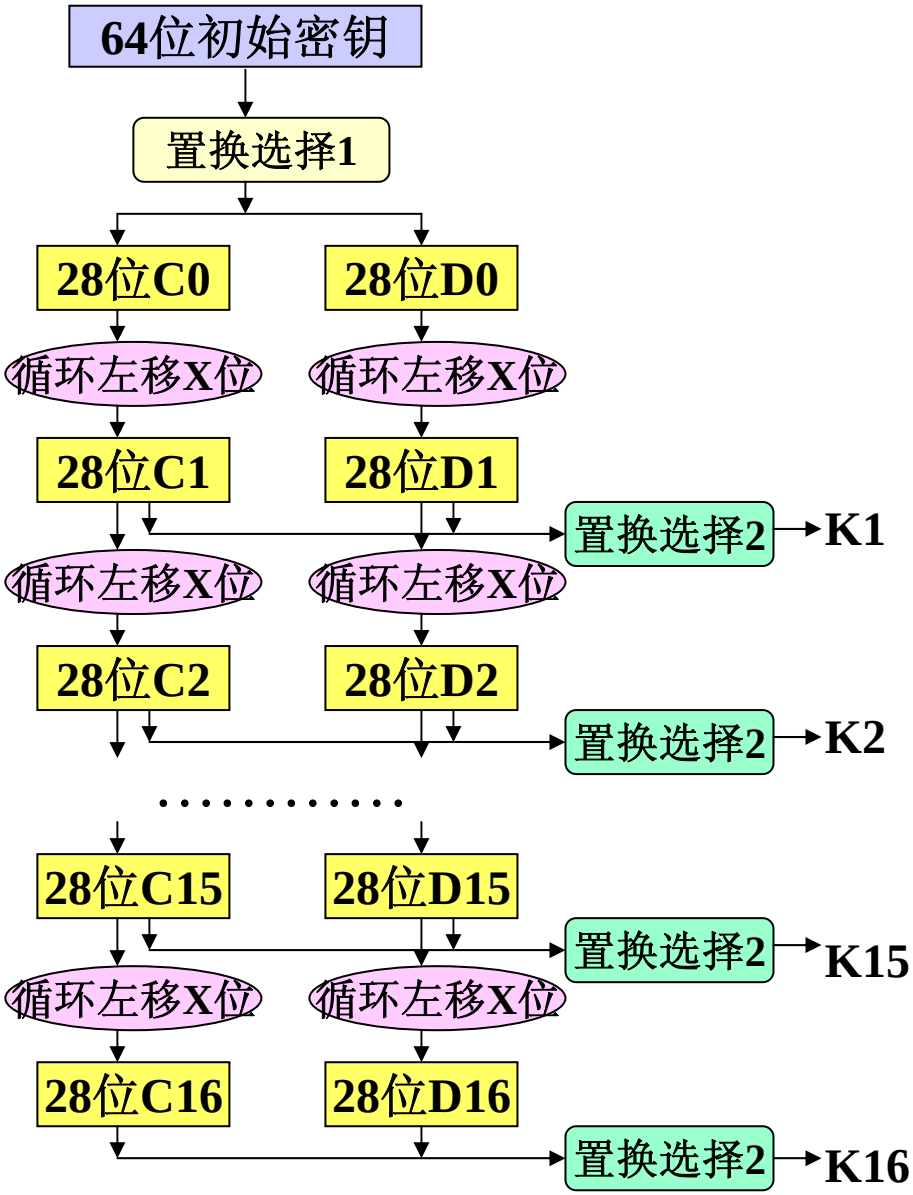
```
Decrypt（M，K）
{
  K_T=IP_{64-56}（K）
  For i=1 to 16 do {   /*密钥*/
    K_T=MP(K_T) ;
    K_i = IP_{56-48}（K_T）；  }
  L_0R_0 =  IP（M）
  For i=1 to 16 do {   /*加密* /
    L_i = R_{i-1};
    R_i = L_{i-1} + f(R_{i-1},K_i);  }
C = IP^{-1}(R_16L_16)
}
```

DES解密算法：

```
Encrypt（C，K）
{
  K_T=IP_{64-56}（K）
  For i=1 to 16 do {  /*密钥*/
    K_T=MP(K_T) ;
    K_i = IP_{56-48}（K_T）；  }
  L_16R_16 =  IP（C）
  For i=16 to 1 do {  /解密*/
    R_{i-1} =  L_i ;
    L_{i-1} = R_i + f(L_i, K_i);}
  M = IP^{-1}(L_0R_0)
 }
```

M—64位明文，C—64位密文；
MP—移位；　　K—初始密钥；
IP—置换；　　IP^{-1}—逆置换。

密钥的形成（同加密）：



移位X = 1 i=1,2,9,16;
2 i=3-8,10-15;

置换选择1（64位中取56位）：

C0：57 49 41 33 25 17 9 1
58 50 42 34 26 18 10 2
59 51 43 35 27 19 11 3
60 52 44 36

D0：63 55 47 39 31 23 15 7
62 54 46 38 30 22 14 6
61 53 45 37 29 21 13 5
28 20 12 4

置换选择2（56位中取48位）：

14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

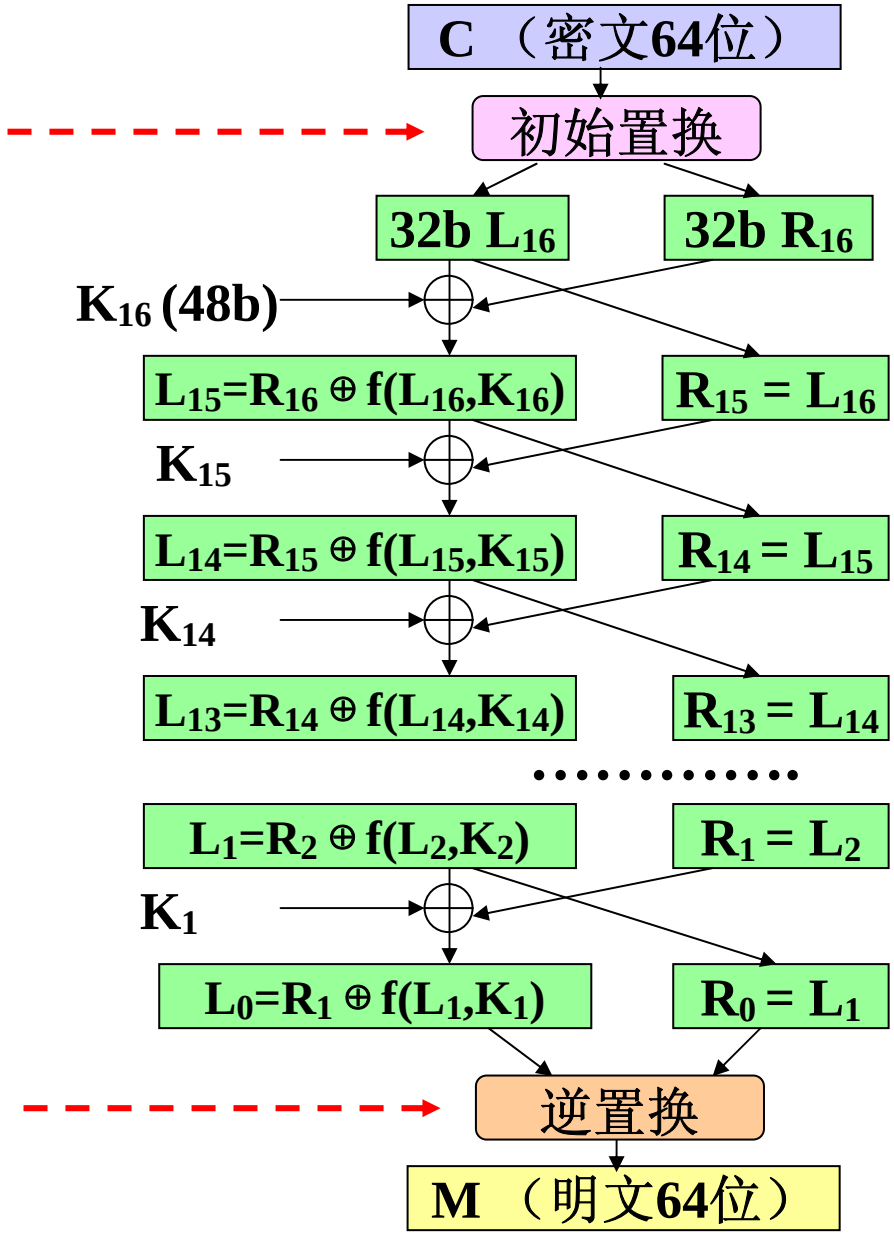
DES解密算法：　64b密文 → 64b明文

初始置换：（64位）

40 8 48 16 56 24 64 32
39 7 47 15 55 23 63 31
38 6 46 14 54 22 62 30
37 5 45 13 53 21 61 29
36 4 44 12 52 20 60 28
35 3 43 11 51 19 59 27
34 2 42 10 50 18 58 26
33 1 41 9 49 17 57 25

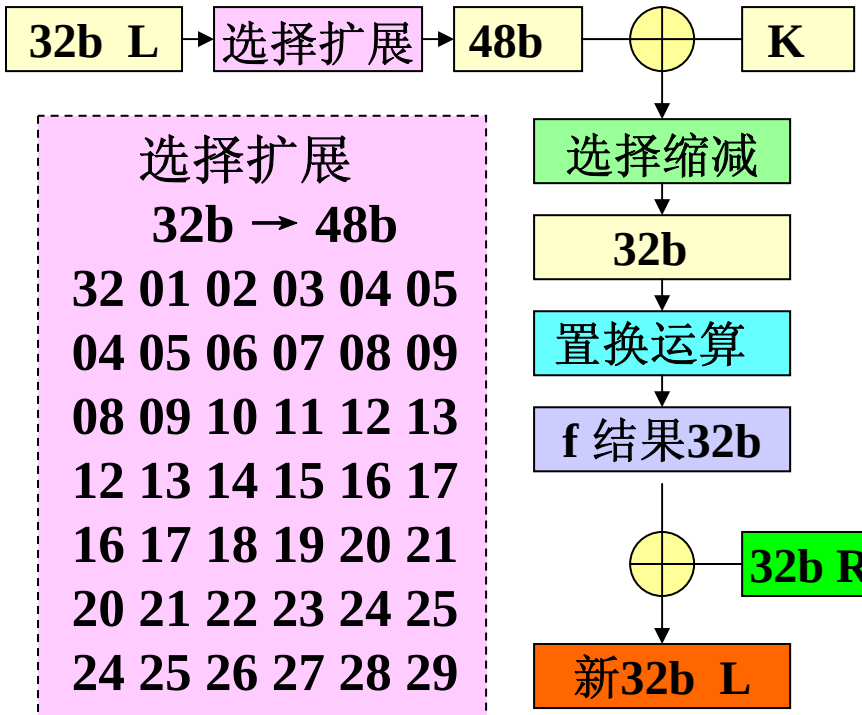
逆置换：（64位）

58 50 42 34 26 18 10 2
60 52 44 36 28 20 12 4
62 54 46 38 30 22 14 6
64 56 48 40 32 24 16 8
57 49 41 33 25 17 9 1
59 51 43 35 27 19 11 3
61 53 35 37 29 21 13 5
63 55 47 39 31 19 15 7



DES加密算法：　64b明文 → 64b密文

f (L , K)的流程：

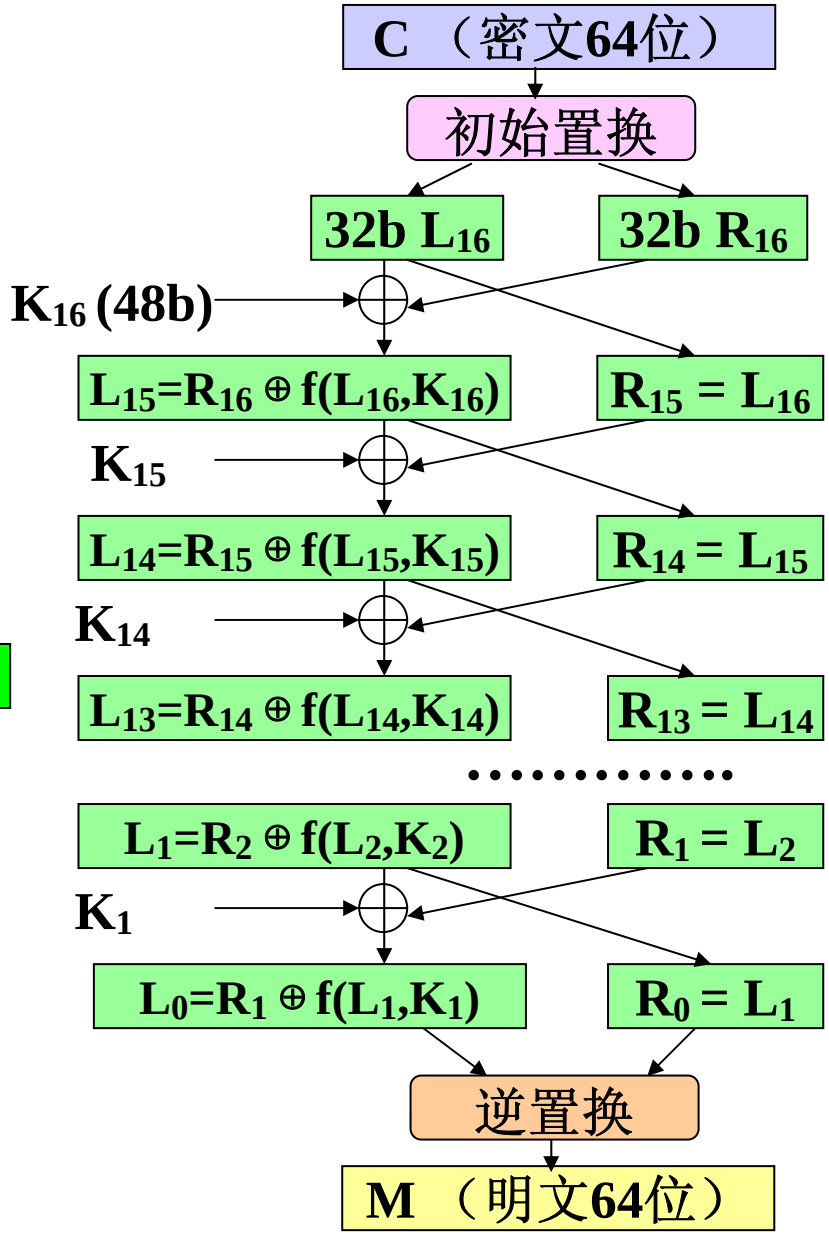


选择扩展
32b → 48b

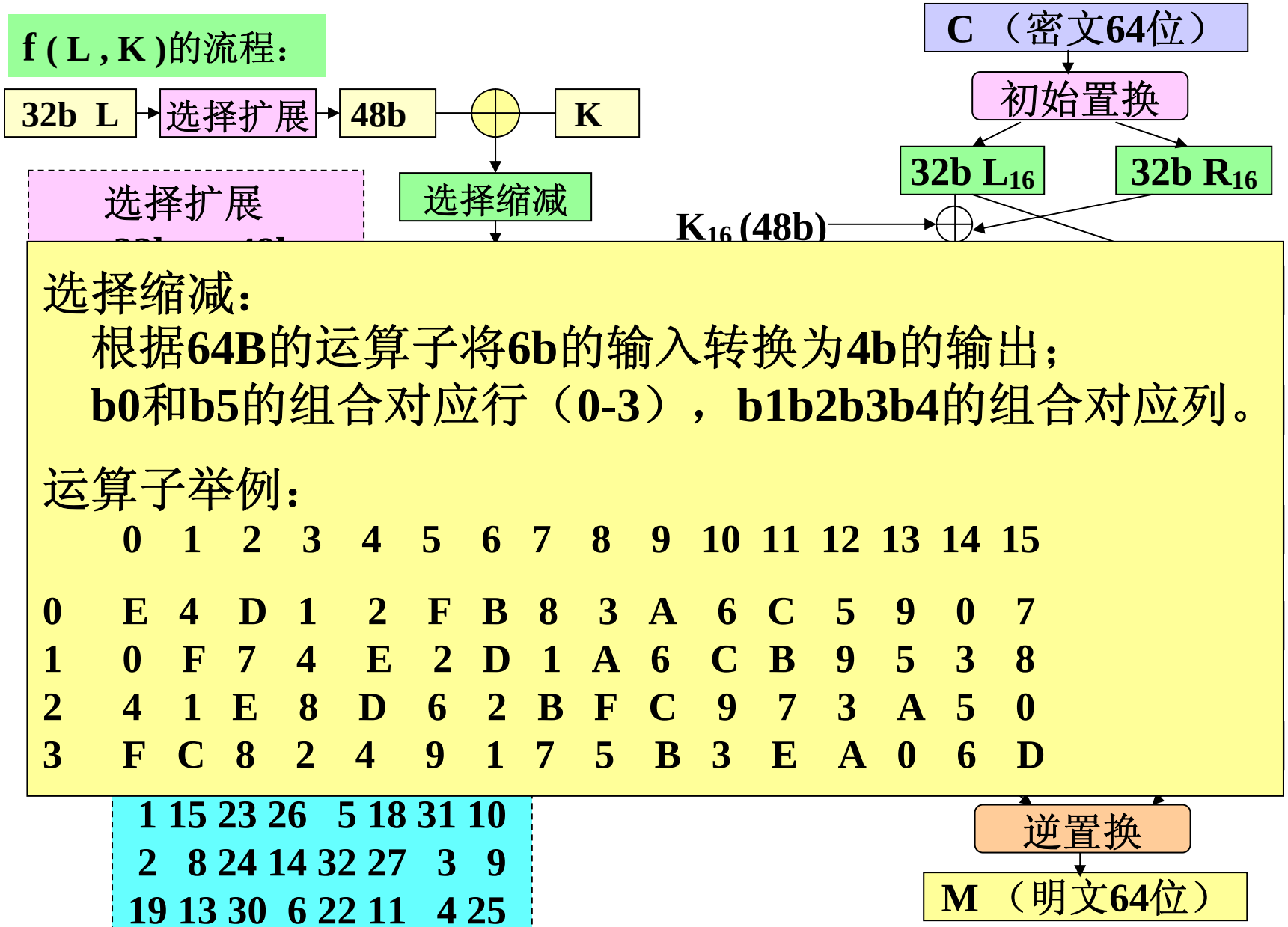
32	01	02	03	04	05
04	05	06	07	08	09
08	09	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	01

置换运算：（32位）

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25



DES加密算法：　64b明文 → 64b密文



选择缩减：

根据64B的运算子将6b的输入转换为4b的输出；

b0和b5的组合对应行（0-3），b1b2b3b4的组合对应列。

运算子举例：

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7
1	0	F	7	4	E	2	D	1	A	6	C	B	9	5	3	8
2	4	1	E	8	D	6	2	B	F	C	9	7	3	A	5	0
3	F	C	8	2	4	9	1	7	5	B	3	E	A	0	6	D

1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

DES的强度和破解

DES算法具有很强的抗密码分析能力，密钥有效长度为56比特，密钥空间有2^{56} = 72,057,584,037,927,936 ≈ 7.2亿亿之多，当采用每秒亿次运算能力的计算机进行蛮力攻击时，猜测密码约需8340天；

随着计算机运算能力的增加，56比特长度的密码系统显得不够安全。

实际上，自DES使用以来，人们也一直在检验其破解能力。

1998年7月，在美国Electronic Freedom Foundation（EFF）资助下，John Gilmore和Paul Kocher使用价值25万美元的计算机耗费56小时攻破DES。

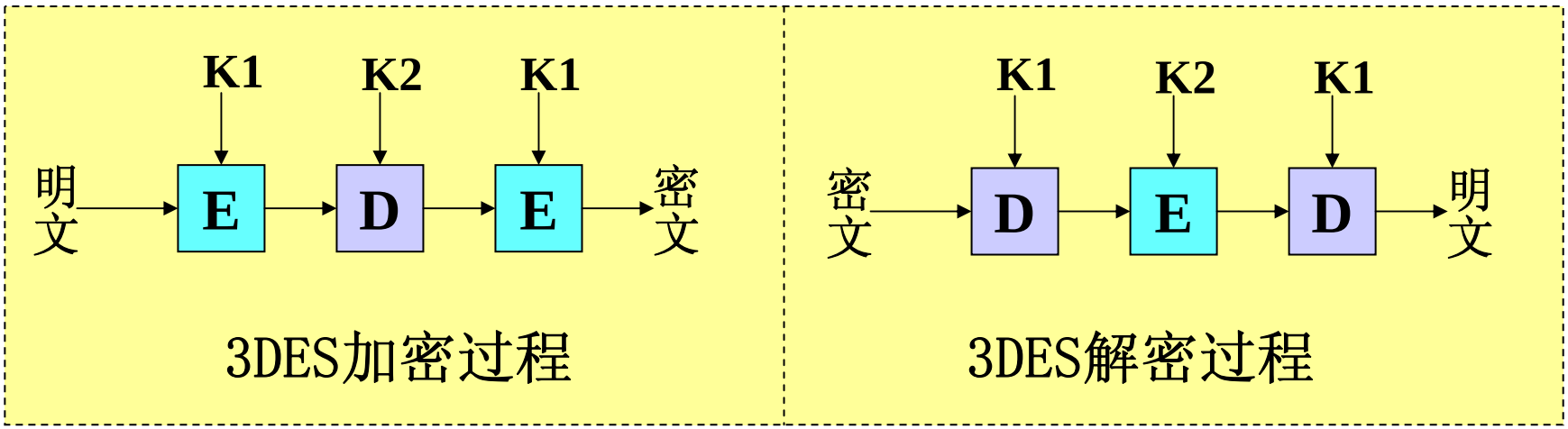
1999年，美国政府资助的另一项目，使用超级计算机耗时22小时。

DES的替代品

在**DES**应用的同时，人们也在寻找替代品，①使用全新的替代算法； ②增加密钥的长度，使用DES的变形。

对应前者：美国国家标准化协会（NIST）于1997年征集高级加密标准（AES）算法，1999年8月选出5个候选者：① IBM的MARS；② RSA实验室的RC6；③ Joan Daemen等人提出的Rijndael；④ Ross Anderson等提出的Serpent；⑤ Bruce Scheier等提出的Twofish。遗憾的是没有明显的优胜者。

对应后者：Triple DES（3DES或3重DES）被广泛使用，密钥长度128位。



对称密钥加密体制的特点

- 通信双方维护相同的密钥（静态分配密钥）；
- 对应N个通信伙伴应维护N个密钥，用户维护信息量大；
- 无法用于群组内的安全通信；
- 算法主要执行置换、代换和位操作，加密/解密速度快。

实用场合：

常用于批量数据的加密。

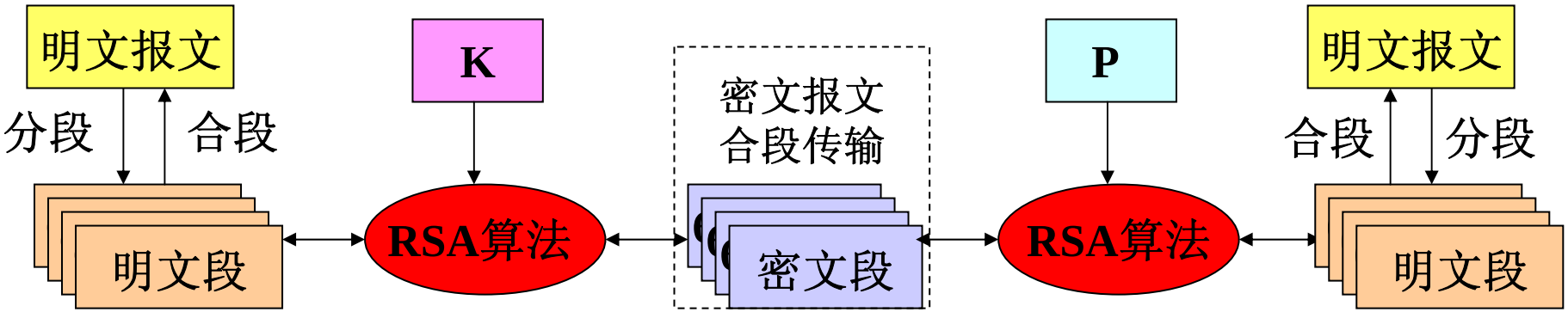
☆ 公开密钥加密体系（非对称密钥加密体系）：

存在一对密钥，可互作加密/解密用；

无法从加密密钥**K**中导出解密密钥**P**；

即：$K <> P$，$M = D_P(E_K(M)) = D_K(E_P(M))$

典型算法：**RSA**；



特点：每个用户具有一对密钥，一个公开**P**，一个私有**K**；

所有的公开密钥**P**可公共存储；用户只需维护自己的私钥**K**。

用户**(A/B)**之间的秘密通信：

$$M = \underbrace{D_{PB}(D_{KA}(E_{PA}(E_{KB}(M))))}_{A \leftarrow B} = \underbrace{D_{PA}(D_{KB}(E_{PB}(E_{KA}(M))))}_{B \leftarrow A}$$

1977年，由L.Rivest，A.Shamir和L.Adleman提出并命名。

基本原理：大合数分解，$M^{Sk*Pk} = M \ (\mathrm{mod}\ r)$；

基于RSA的加密/解密算法：

1 选择素数p和q，计算模数 r = p * q;

2 计算欧拉函数：φ（r）=（p-1) * (q-1);

3 选择与φ(r)互素的量K1，定义为秘密密钥Sk，或公开密钥Pk;

4 计算另一量K2，满足K1*K2=1（mod φ(r)），定义为Pk或Sk;

5 将明文X（值在0到r-1之间），自乘K1（或K2）次后按r取模作加密运算，形成密文Y（值也在0到r-1之间）;

6 将密文Y（值在0到r-1之间），自乘K2（或K1）次后按r取模作解密运算，恢复明文X（值也在0到r-1之间）。

注：为方便计算，有;

如果R = M mod N, 则$R^x \bmod N = M^x \bmod N$;

举例：设p=11, q=7, 有r=p*q=77, $\phi(r)=(p-1)*(q-1)=60$;

若选择Pk=47（与60互素），
则有：
60=47*1+13,
47=13*3+8,
13=8*1+5,
8=5*1+3,
5=3*1+2,
3=2*1+1;

计算Sk：
1=3-2*1
=3-(5-3*1)*1=3*2-5*1
=(8-5*1)*2-5*1=8*2-5*3
=8*2-(13-8*1)*3=8*5-13*3
=(47-13*3)*5-13*3=47*5-13*18
=47*5-(60-47*1)*18=47*23-60*18;
即：Sk=23

加密35（0—77），Sk=47，　理由：

$35^2 \pmod{77}=70$; $35^4 \pmod{77}=49$; $35^8 \pmod{77}=14$;
$35^{16} \pmod{77}=42$; $35^{32} \pmod{77}=70$; $35^{40} \pmod{77}=56$;
$35^{44} \pmod{77}=49$; $35^{46} \pmod{77}=42$; $35^{47} \pmod{77}=7$;

解密7，Pk=23：

$7^2 \pmod{77}=49$; $7^4 \pmod{77}=14$; $7^8 \pmod{77}=42$; $7^{16} \pmod{77}=70$;
$7^{20} \pmod{77}=56$; $7^{22} \pmod{77}=49$; $7^{23} \pmod{77}=35$;

注：RSA中Pk和Sk的计算时，需验证$1=Pk*Sk \pmod{\phi(r)}$

RSA的特点：

数论方面的知识表明，当所取的素数足够大（如1000位）时，破译密文在理论上是行不通的，具有较高的破译难度。

密钥量与用户数呈线性关系，对应N个通信伙伴，每个用户仍只需维护自己的私密，并通过某种方式获得对方的公钥，用户维护的密钥量小；

密钥具有个人特征，每个用户可以选择自己的密钥对，一个公开（公钥），一个私密（私钥）；

密钥（公钥）传递可以使用开放信道；

可满足不可信用户之间的保密性要求。

可用于支持群组内的安全通信；

采用乘法运算，加密/解密速度慢，常用于少量数据的加密。

② 摘录技术—也称散列技术

原理：对报文进行某种运算，形成与报文密切相关、且长度有限的摘录值或者指纹（**Fingerprint**），由此验证报文；

要求：不同内容的报文形成相同摘录值的概率几乎为零；
根据摘录值无法还原原报文；

典型的摘录算法：

CRC校验算法—利用该算法可检测传输过程中产生的差错；
采用不同的产生式可以形成特定长度（如**32b**）的校验和；

报文摘录算法（**MD2**）—**RFC1319**
产生**128**位的摘录值，**1992**年**4**月；

报文摘录算法（**MD4**）—**RFC1320**
产生**128**位的摘录值，**1992**年**4**月；

报文摘录算法（**MD5**）—**RFC1321**
产生**128**位的摘录值，**1992**年**4**月；

完全散列算法（**SHA-1**）—**RFC2202**
产生**160**位的摘录值，**1997**年**9**月。

摘录技术可用于提供网络安全中的内容完整性服务。

② 摘录技术—MD5（Message Digest v5）算法，RFC1321

作者：MIT的R. Rivest；思路：摘录值应与每个比特相关；

基本算法：

- 信息摘录长度为128比特（4个字），记为d0、d1、d2、d3；
- 报文填充“10…0”达到448 mod 512, 增加*64b*指出原始信息长度；结果是报文长度为512b的整数倍；
- 分块（512b = 16个字），记为m0、 m1、...、m15；
- 每块处理含四遍扫描，每遍对d0,d1,d2,d3使用不同的扰乱函数和移位操作进行计算；
- 处理前（包括初值）/后的信息摘录的相加成为下一块处理时信息摘录的当前值；最后一块信息处理之后的信息摘录当前值即为最终的信息摘录值（结果）。

详见RFC1321。

MD5算法的补充说明：

1、摘录算法的目的是对应不同的报文，应产生不同的摘录值，但考虑到大空间向小空间映射的特点，重复可能难免；故只能追求无法刻意得出相同的摘录值；

2、MD5仅含逻辑操作和移位操作，因此计算速度较快；

3、虽然MD5被认为是迄今最好的摘录算法，但山东大学王小云教授声称已得出破解MD5（包括其它摘录算法）的方法。

4、考虑到这种破解尚未得到广泛的认同，且尚未推出更好的摘录算法，故本课程仍然认为可以使用MD5算法。

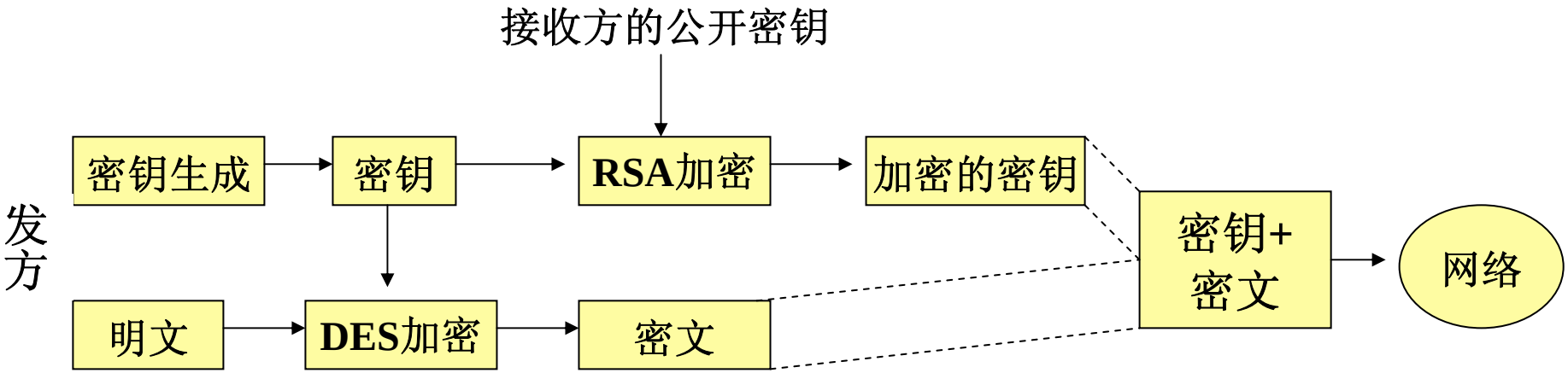
后期讨论的安全保护主要基于前述的加密和摘录技术。

（3） 网络安全服务

① 内容保密—防窃取

直接采用加密技术对数据进行加密；

为提高加密的效率，混合使用秘密密钥加密体系和公开密钥加密体系的算法。



特点：对应每次通信，形成一个一次性密钥（随机数）；
只有指定的收方才可以获得密钥，解密密文；
使用DES算法和该密钥对明文加密，提高效率；
使用RSA算法对密钥加密，保护密钥的秘密性。

加密技术可用于提供网络安全中的内容保密服务。

直接依赖摘录技术的特性（报文和摘录息息相关）。

工作过程：

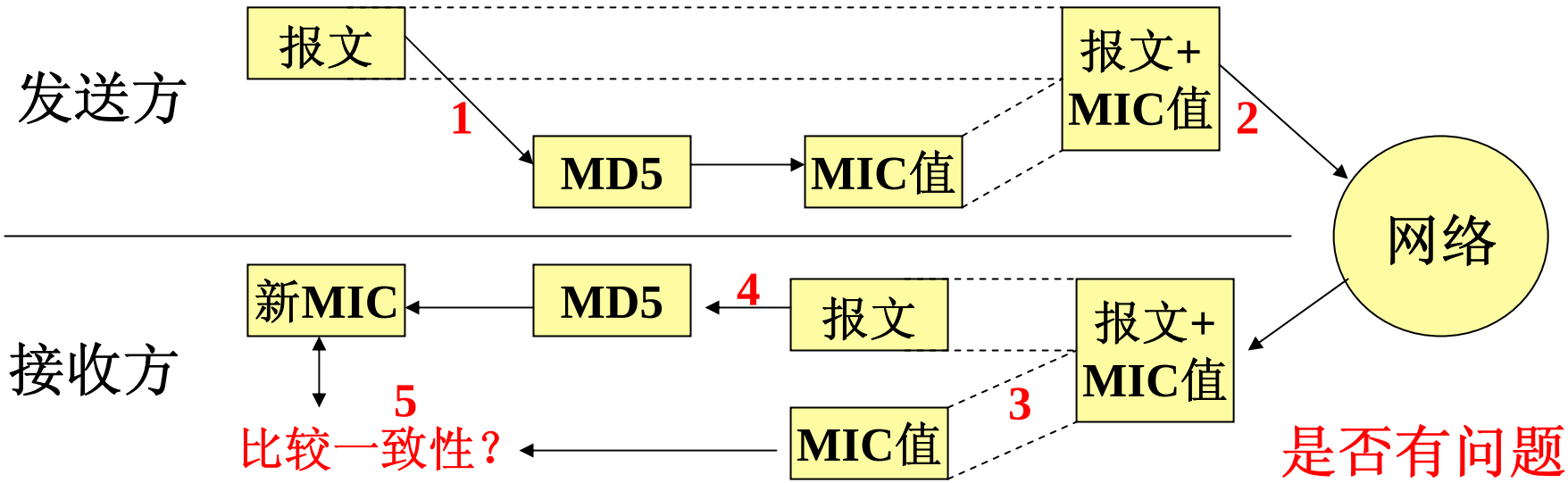
1 发送方利用摘录算法（如MD5）形成摘录值（报文完整性检查值—MIC值）；

2 报文连同MIC值一起传递给接收方；

3 接收方分隔报文和MIC值；

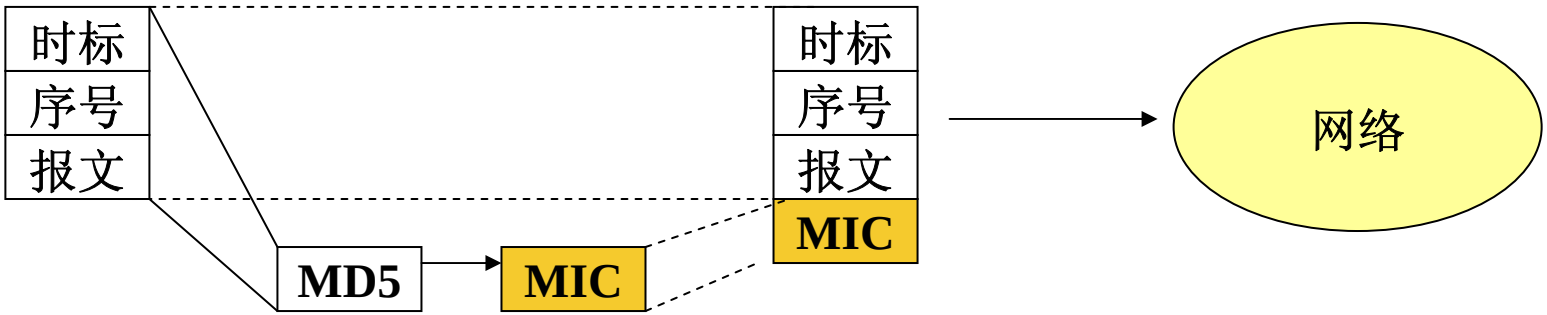
4 对报文执行相同的摘录算法，形成新的MIC值；

5 新 / 原MIC值比较，判断报文在传输过程中是否被修改。



③ 序列完整性—防重播

在报文中增加序号和时标（报文形成或者发送的时间值）；
接收方按序接受报文。



④ 实体鉴别：—防冒充（假冒）

含身份鉴别和数据源鉴别。

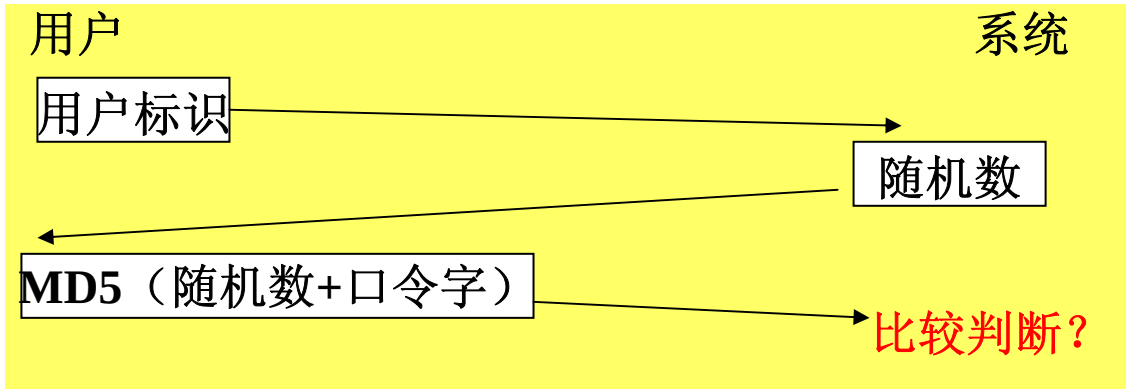
★ 身份鉴别—鉴别对等实体的身份。

进入系统时常用的鉴别身份的方法为传递用户标识和口令字，并和系统内保留的用户标识和口令字进行比较，验证用户的合法性。

问题：传递过程中，用户标识和口令字被窃取；

用户标识和口令字加密传输？仍然存在窃取的可能！

解决方法：口令字不传输（两次握手—挑战challenge）。

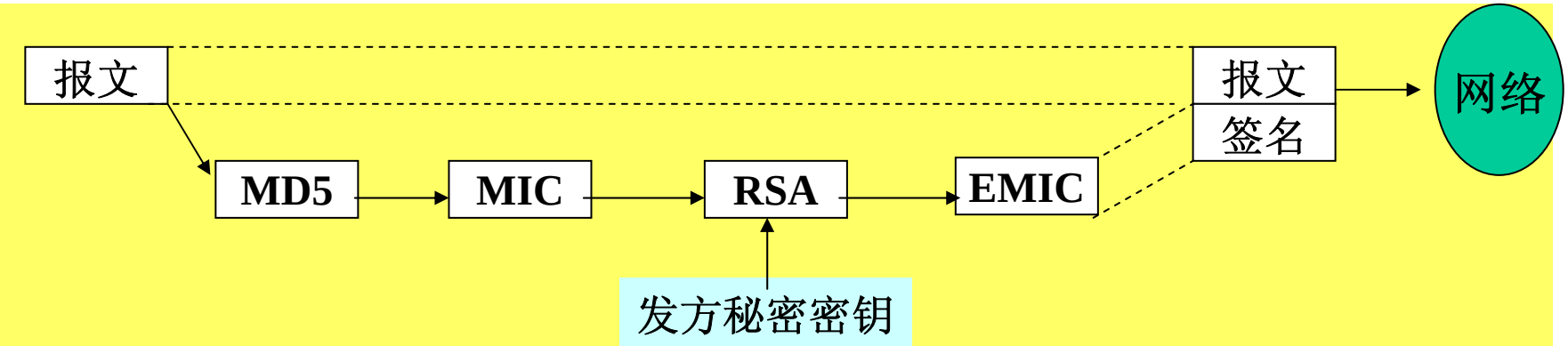


结果：随机数可以蕴含时间信息；口令字始终不在线路上传输；摘录值随随机数和口令字而变，仅一次有效。

④ 实体鉴别（续）：—防冒充（假冒）

★ 数据源鉴别—鉴别数据真实性，确实来自期望的发送方。

数字签名技术支持数据源的鉴别。



描述：形成的报文数字签名和报文内容及发方密钥密切相关；

收方利用发方的公钥处理签名，获得原始**MIC**值；

收方利用**MD5**对报文求**MIC**值；

如果新**MIC**值和原始**MIC**值一致，可认为报文确实来自于期望的发送方，且在传输过程中内容未被篡改。

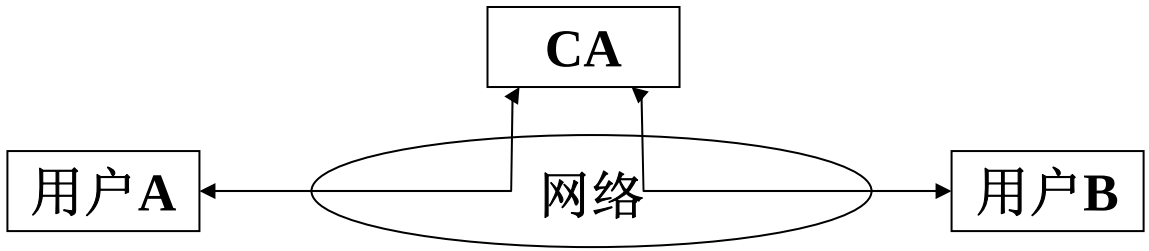
依据：只有发方才掌握发方的私钥。

⑤ 抗否认服务—抵御合法用户对所作的操作进行否认（抵赖）

和前述方案的差异：变“外来攻击”为“内部攻击”；

理想的解决方案：第三方的参与和仲裁。

措施：至少维护一个双方可信的认证中心（CA），合法用户需在中心注册，获得自己的密钥对；CA以安全的方式转发通信双方的报文，并予以记录，作为产生异议时的仲裁依据。



推荐的过程：A以CA的公钥和A的私钥向CA认证自身，并获得B的公钥；A以B的公钥形成密文（容许含随机密钥的秘密加密），并提交CA；CA记录全部或者部分（如MIC值）信息后，转发密文至B；B收取报文后，应向CA返回确认信息。

⑥ CA及其证书的应用—对通信双方加以保障

CA被认为是保障安全通信的基础；

接受合法用户的注册，形成证书和密钥对，并予以私钥发放；

当用户希望和其他用户通信时，向CA求证对方的合法性；

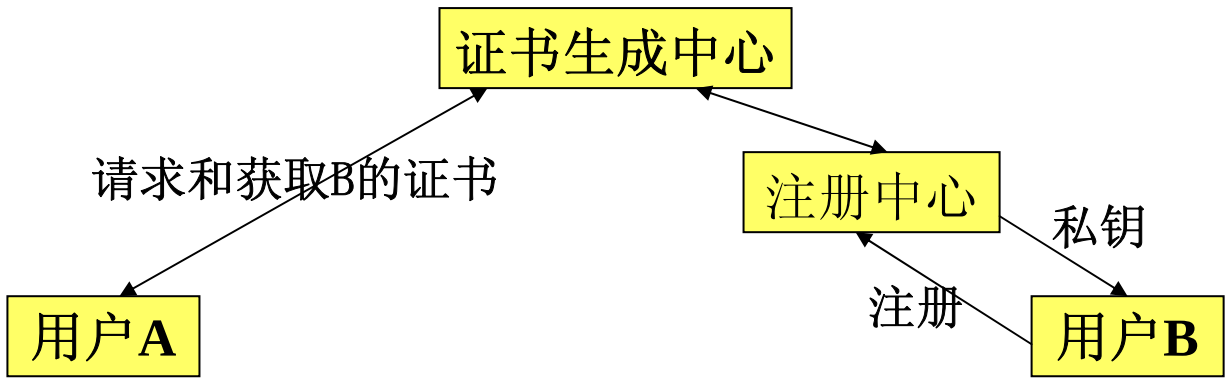
求证结果获得对方的证书（含对方的公钥）；

对方用户可以使用相同的方法获得本用户的证书；

通信双方利用证书信息实现数据交换；

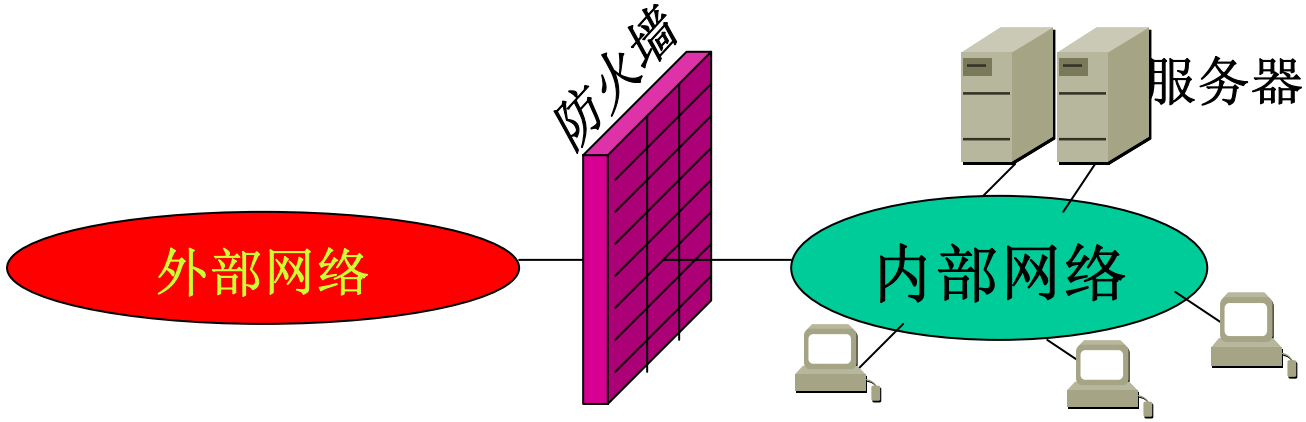
如果发生争执，CA通过双方提交的交换信息进行仲裁。

理想状态：认证中心（CA）之间的完美协作，保证全球用户的可认证性。



（4） 网络安全技术的延伸—个体防护为集体防护

防火墙：保护内部网络的资源免受外界的侵袭。



网络互连的原理表明，从降低成本的角度出发，一个群体希望进入外部世界时，最好先联成网络，并通过互连部件接入外部世界。

从安全的角度看，先形成内部网络，并规定唯一（或者有限）的出入口，更利于安全措施的实施。

最安全的方法是物理隔绝，但这将剥夺了内部用户访问外部世界的权利。

① 防火墙的设置原则：

- 保护共同利益者；
- 应综合考虑网络的安全防卫要求、所能承受的代价，以及系统被攻破之后可能产生的损失；
- 要考虑性能代价（性价比）；

  —防火墙适合于保护内部主机安全管理不太严格的园区网；

  —防火墙适用于长久外连的环境；
- 防火墙的设置不能影响网络的正常使用

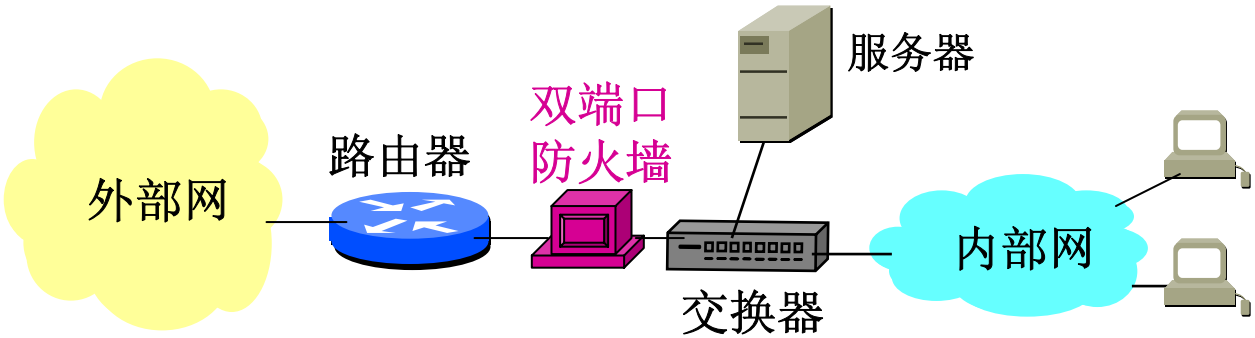
  — 例如：如果允许外出报文设置**Don‘t Fragment (DF)**位，就必须允许**ICMP**的**Destination Unreachable / Fragmentation Needed**出错报文进入

② 防火墙的位置

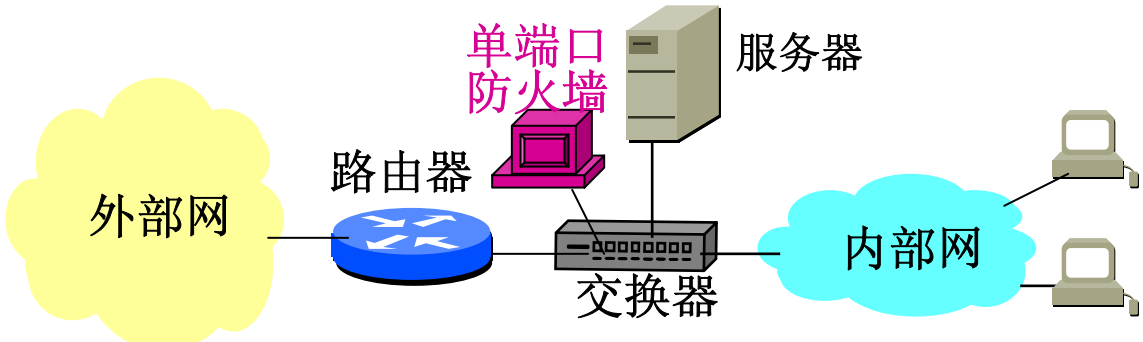
网络互连部件是连通网络的关键设备，鉴于内部网常采用局域网技术，外部网常为广域网，此时互连的部件为路由器，因此路由器所在的位置也应是防火墙的位置；有时，路由器中也集成了防火墙的功能。

防火墙设施通常具有2个或者1个端口；

双端口时，分别接外部网和内部网；



单端口时，则需交换设备的端口绑定。



③ 防火墙的原理—分组过滤

原理：分析IP报文，对应其中的所有参数，设置过滤策略，允许或者拒绝该报文穿越防火墙；

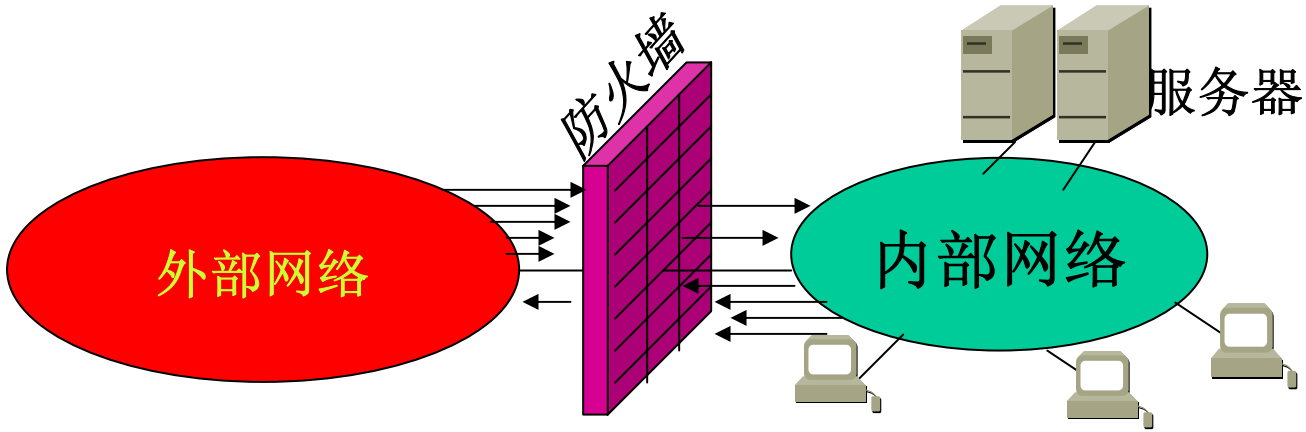
过滤规则的一般描述：

规则序号	协议类型	源地址	端口号	宿地址	端口号	动作

分析的参数有：源IP地址（仅允许哪些设备访问内部网）、宿IP地址（仅允许访问哪些结点）、端口号（允许使用哪些服务）等；

设置的策略包括：访问的时间段、并发访问的个数等；

一般策略为：不明确表示“允许”的就是禁止。



分组过滤式防火墙举例

策略库的构建：假设仅支持企业用户访问本地邮件服务器；
注意：简单邮件传输协议（**SMTP**）基于**TCP**的服务；
SMTP服务器（即接受者）使用端口**25**；
客户机（即发送者）使用大于**1023**的任意端口。

传输方向	传输协议类型	报文源地址	主机端口号	报文宿地址	主机端口号	控制操作	
IN	TCP	外部	> 1023	S地址	25	允许	远程访问
OUT	TCP	S地址	25	外部	25	允许	服务器互访
IN	TCP	外部	25	S地址	25	允许	服务器互访
BOTH	任意	任意	任意	任意	任意	不允许	

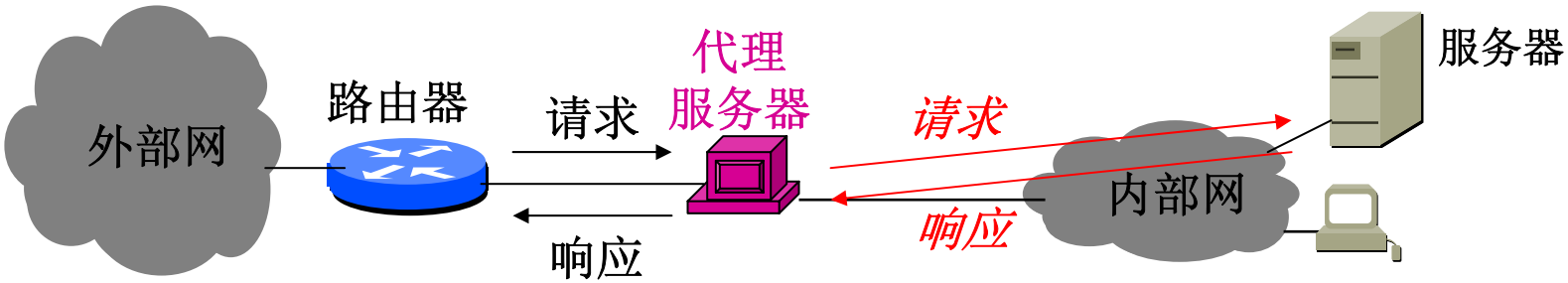
④ 防火墙的原理—代理服务

代理外部（或内部）用户访问内部（或外部）网络，杜绝内部和外部的直接访问。

代理服务器分析客户的请求，根据制定的策略决定允许或者拒绝某个特定的请求；当一个请求被允许时，代理服务器就“代表”该客户执行访问操作，并将结果返回客户。

此处的“代表”隐含了分组中**IP地址的替换（迁移）**。

此类防火墙安全较高，但效率受影响，常用于特定的应用服务（如**FTP**服务、**Telnet**服务、远程拨号服务等）。

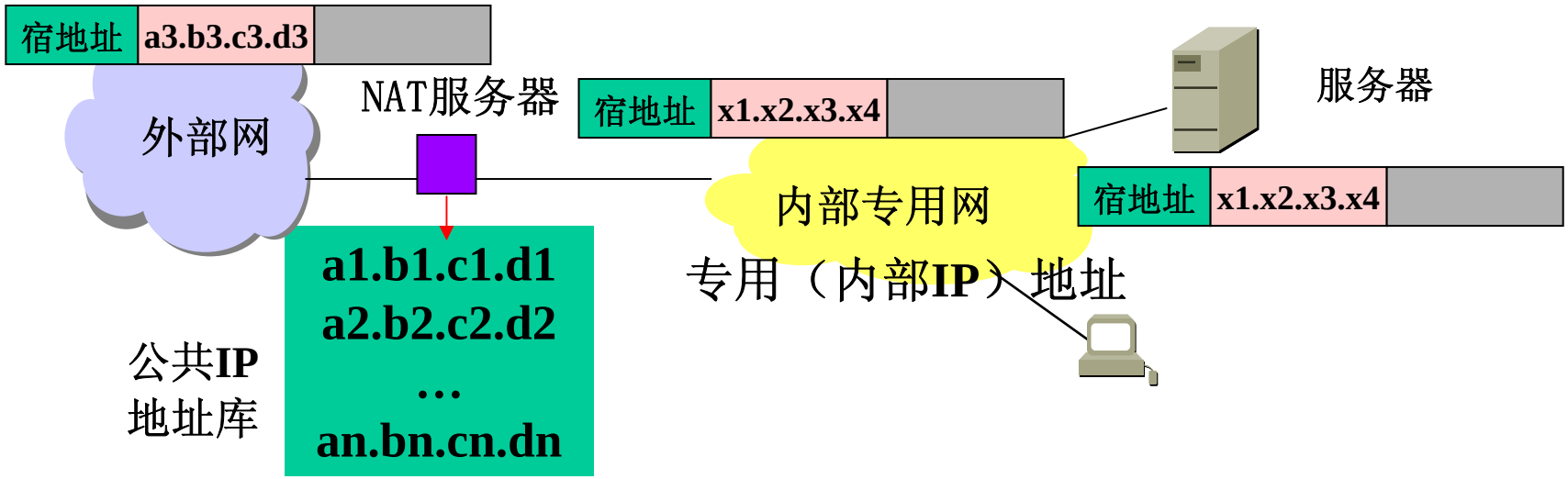


⑤ 防火墙的原理—地址迁移（NAT）

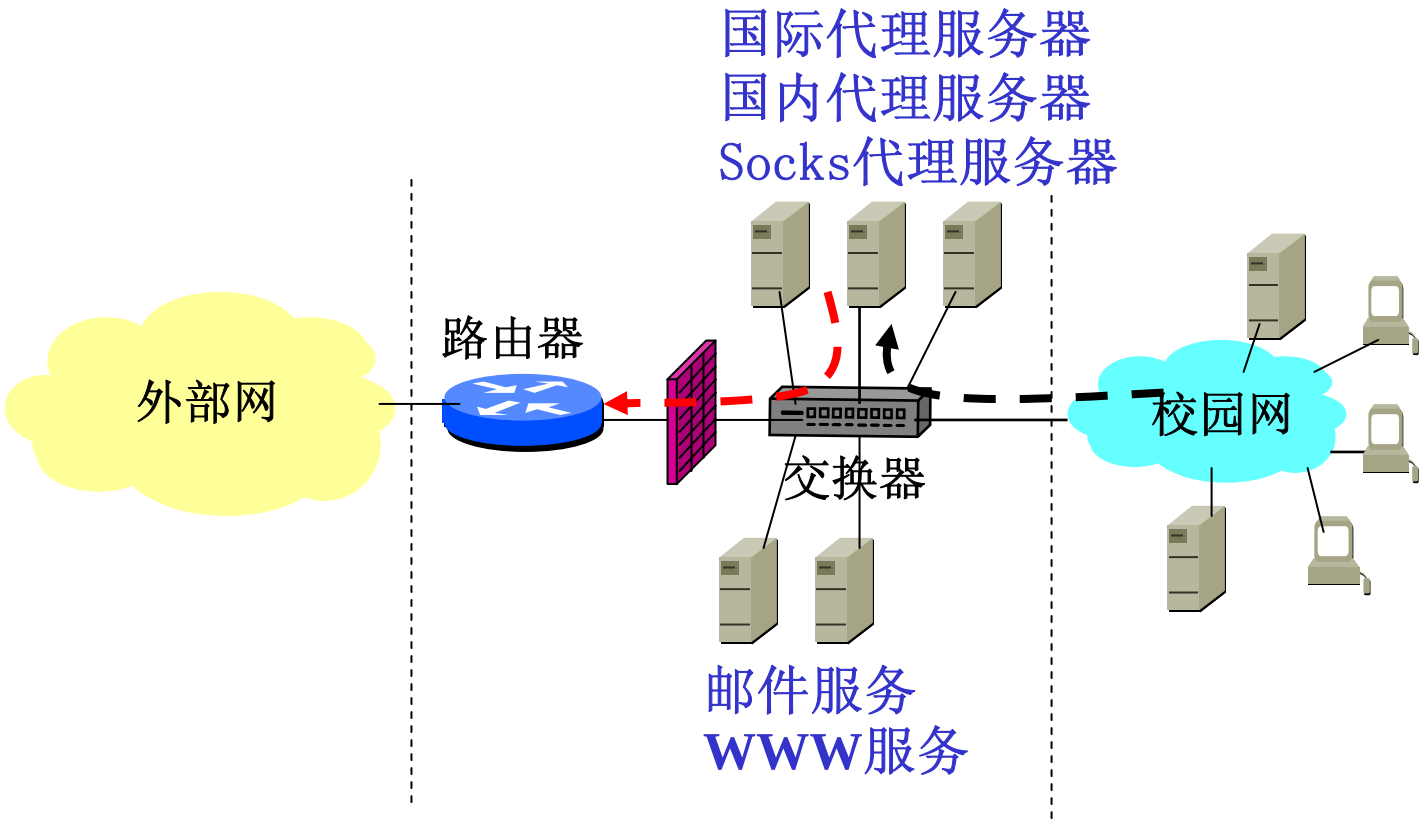
针对IP地址告急和专用IP地址在部分企业网中的应用，出现了地址迁移路由器（NAT路由器或者NAT服务器）。

当内外用户希望相互访问时，NAT路由器负责全局/本地IP地址的映射，屏蔽内部IP地址；

NAT服务器专门进行地址迁移工作，并增加各种安全策略，限制地址的转换，隔离内外网络。



⑥ 东大防火墙示意



其它说明：

防火墙仅用于隔绝内部网和外部网的直接连通，无法防御内部网自身的侵袭，例如内部网用户的越权访问；因此，内部网的资源仍需设置必要的访问控制（主要是访问权限设置）；

访问控制技术：

访问控制：对系统中资源的访问动作进行安全控制的安全服务和安全机制；

访问控制的基本要素：

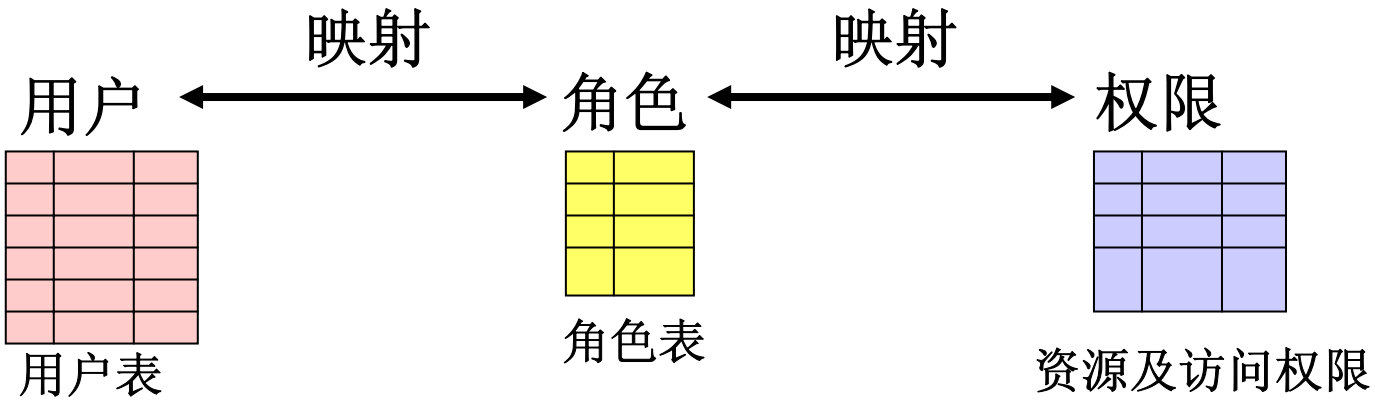
- 主体（**Subject**）：提出请求或实施访问操作的实体
  - 可以是用户或其它任何代理用户行为的实体（例如进程、作业和程序）
- 客体（**Object**）：接受其他实体访问的被动实体
  - 凡是可以被操作的信息、资源、对象都可以认为是客体。
- 控制策略：主体对客体的操作行为集和约束条件集
  - 控制策略是主体对客体的访问规则集，这个规则集直接定义了主体对客体可以的作用行为和客体对主体的条件约束。
  - 访问策略体现了一种授权行为，也就是客体对主体的权限允许，这种允许不超越规则集。

基于角色的访问控制技术（**RBAC—Role-Based AC**）

应用系统设计时，为避免用户和权限的密切相关性，通常增加角色及映射关系，以利于简化系统设计。

RBAC提供了一种描述用户和权限之间的多对多关系，角色可以划分成不同的等级，通过角色等级关系来反映一个组织的职权和责任关系，这种关系具有传递性和非对称性特点，通过继承行为形成了一个偏序关系。

注：角色与用户之间的关系不是一一对应的，因此要检查和防止权限冲突和安全漏洞（如合计和出纳）。



计算机信息系统安全保护等级划分准则

- **GB 17859-1999，2001年1月1日起实施**
- 标准规定了计算机信息系统安全保护能力的五个等级，等级越高，安全性越强
  - 第一级:用户自主保护级
  - 第二级:系统审计保护级
  - 第三级:安全标记保护级
  - 第四级:结构化保护级
  - 第五级:访问验证保护级

计算机信息系统安全保护等级划分准则

- **GB 17859-1999，2001年1月1日起实施**
- 标准规定了计算机信息系统安全保护能力的五个等级，等级越高，安全性越强

☆ 第一级:用户自主保护级

通过隔离用户与数据，使用户具备自主安全保护的能力；

可对用户实施访问控制，避免其他用户对数据的非法读写与破坏。

– 自主访问控制
– 身份鉴别
– 数据完整性。

计算机信息系统安全保护等级划分准则

- **GB 17859-1999，2001年1月1日起实施**
- 标准规定了计算机信息系统安全保护能力的五个等级，等级越高，安全性越强

☆ 第一级:用户自主保护级

☆ 第二级:系统审计保护级

实施粒度更细的自主访问控制，通过登录规程、审计安全性相关事件和隔离资源，使用户对自己的行为负责。

- 自主访问控制
- 身份鉴别
- 客体重用
- 审计
- 数据完整性。

计算机信息系统安全保护等级划分准则

- **GB 17859-1999，2001年1月1日起实施**
- 标准规定了计算机信息系统安全保护能力的五个等级，等级越高，安全性越强

☆ 第一级:用户自主保护级

☆ 第二级:系统审计保护级

☆ 第三级:安全标记保护级

具有系统审计保护级的所有功能，并提供有关安全策略模型、数据标记以及主体对客体强制访问控制的非形式化描述，具有准确标记输出信息和消除通过测试发现的任何错误的能力；

- 自主访问控制
- 强制访问控制
- 标记
- 身份鉴别
- 客体重用
- 审计
- 数据完整性

计算机信息系统安全保护等级划分准则

- **GB 17859-1999，2001年1月1日起实施**
- 标准规定了计算机信息系统安全保护能力的五个等级，等级越高，安全性越强

☆ 第一级:用户自主保护级

☆ 第二级:系统审计保护级

☆ 第三级:安全标记保护级

☆ 第四级:结构化保护级

系统模型需经形式化描述和测试；具有自主和强制访问控制能力；具有隐蔽通道；计算机信息系统和接口应能经受更充分的测试和更完整的复审；具有鉴别机制；提供可信设施管理；增强了配置管理控制；系统具有相当的抗渗透能力。

- 自主访问控制
- 强制访问控制
- 标记
- 身份鉴别
- 客体重用
- 审计
- 数据完整性
- 隐蔽信道分析
- 可信路径

计算机信息系统安全保护等级划分准则

- **GB 17859-1999，2001年1月1日起实施**
- 标准规定了计算机信息系统安全保护能力的五个等级，等级越高，安全性越强

☆ 第一级:用户自主保护级

☆ 第二级:系统审计保护级

☆ 第三级:安全标记保护级

☆ 第四级:结构化保护级

☆ 第五级:访问验证保护级

满足访问监控器需求，可访问监控器仲裁主体对客体的全部访问；支持安全管理员职能；扩充审计机制，当发生与安全相关的事件时发出信号；提供系统恢复机制；系统具有很高的抗渗透能力。

– 自主访问控制　– 强制访问控制　– 标记
– 身份鉴别　– 客体重用　– 审计
– 数据完整性　– 隐蔽信道分析　– 可信路径
– 可信恢复

题外话

网络技术的发展很快，新的技术，或者新的产品迅速面世，但原理性的变化并不多；

正因为发展很快，需要诸位自身的努力，以便适应新技术；

也是因为发展很快，且年轻人具有适应的优势，因此，只要有兴趣，肯定会更强；

一位教授的解词也许意味着什么？！

CHINA：

—中国高速信息网络体系