



北京邮电大学

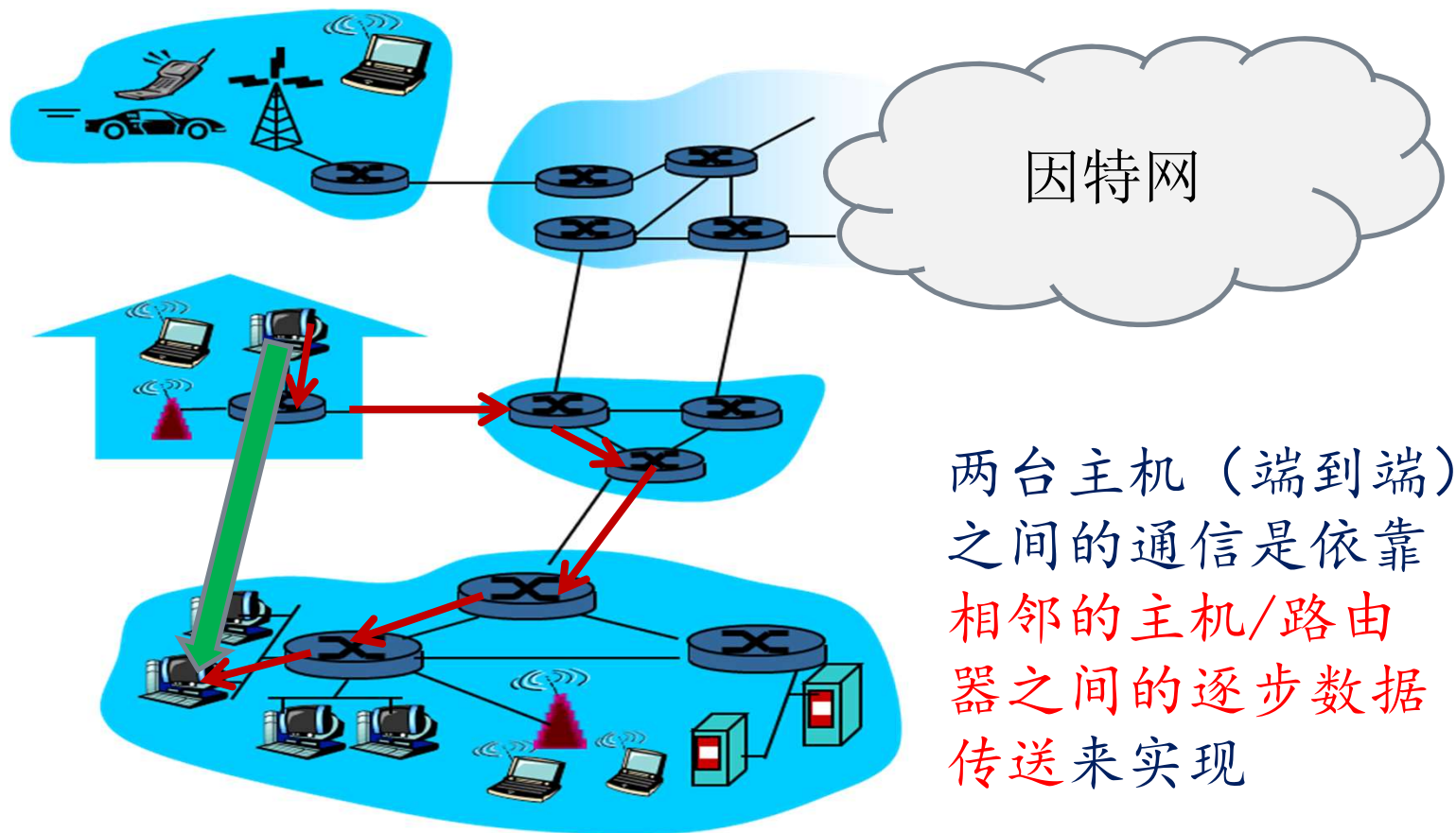
计算机网络

第五章 数据链路层

计算机学院

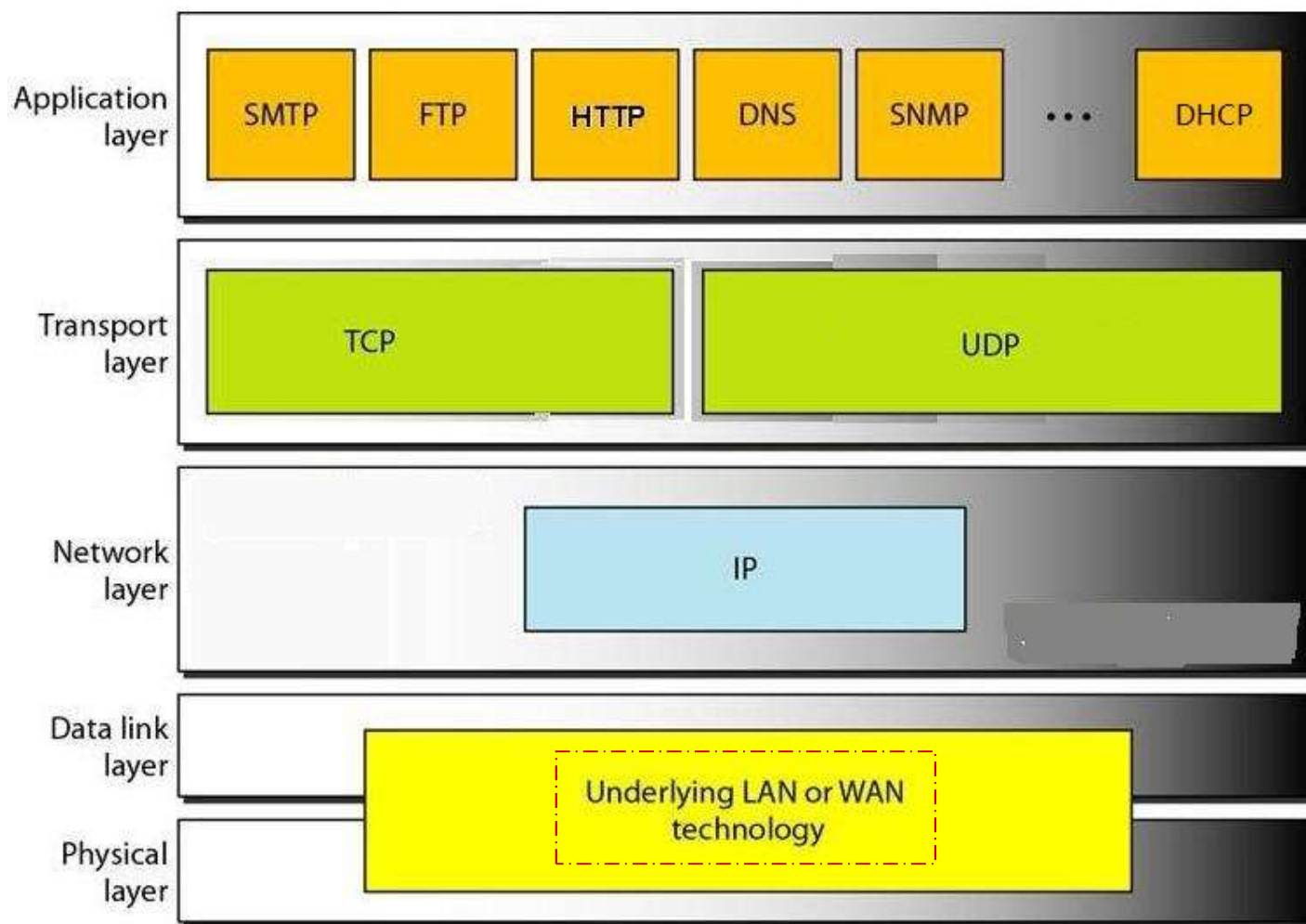
2018年12月

数据链路层的作用？



[Kurose]

TCP/IP协议栈



教学要求及内容

◆ 掌握数据链路层的功能和实现的技术要点

- 数据成帧方法
- 差错检测方法：CRC校验
- 编址方法

◆ 了解数据链路层的协议实例

- HDLC
- PPP

内容提要

- ◆ 5.1 数据链路层的功能及服务
- ◆ 5.2 数据链路层的成帧原理
- ◆ 5.3 差错检测与纠错技术
- ◆ 5.4 数据链路层的编址
- ◆ 5.5 数据链路层的协议实例
- ◆ 5.6 数据链路层的安全隐患

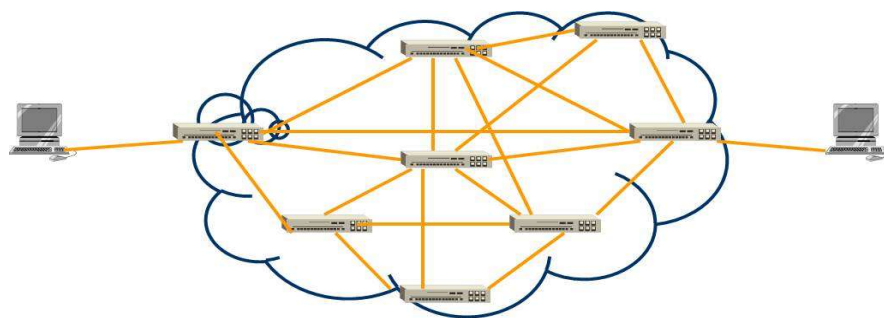
为什么需要数据链路层？

- ◆ 物理信道是不可靠的！
 - 噪声的干扰可能导致数据传输差错
 - 需要进行差错检测和纠正
 - 发送方的速率可能大于接收方的速率，从而导致数据丢失
 - 需要进行流量控制
- ◆ 数据链路层实现相邻主机/路由器间的可靠的数据传输

数据链路层的信道类型

◆ 点到点信道

- 一条信道上只有两台设备
- 独占信道
- 一对一通信
- 本章学习



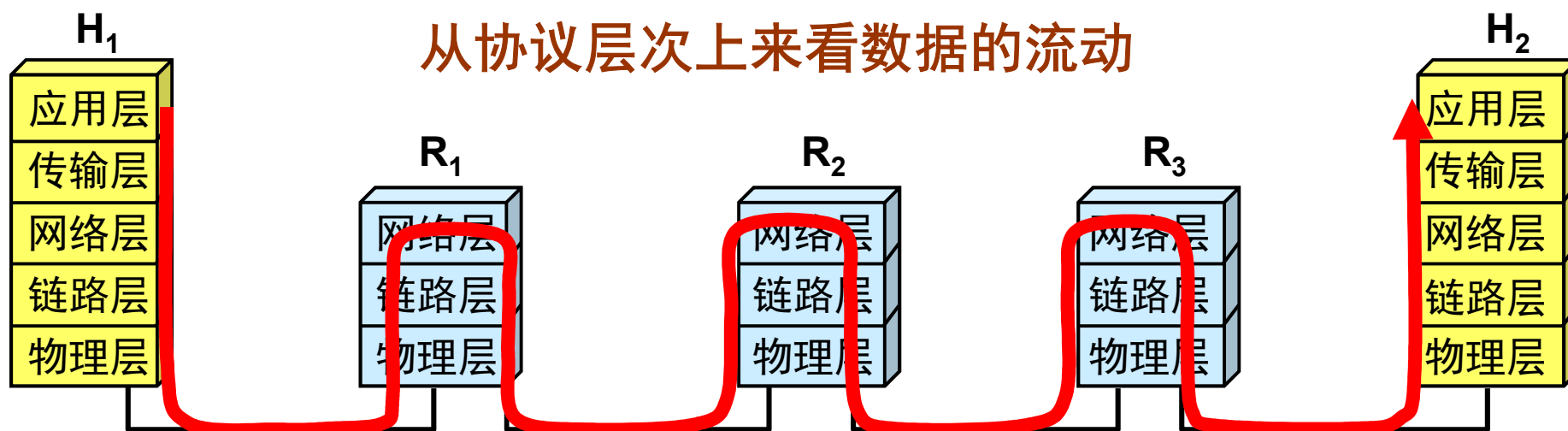
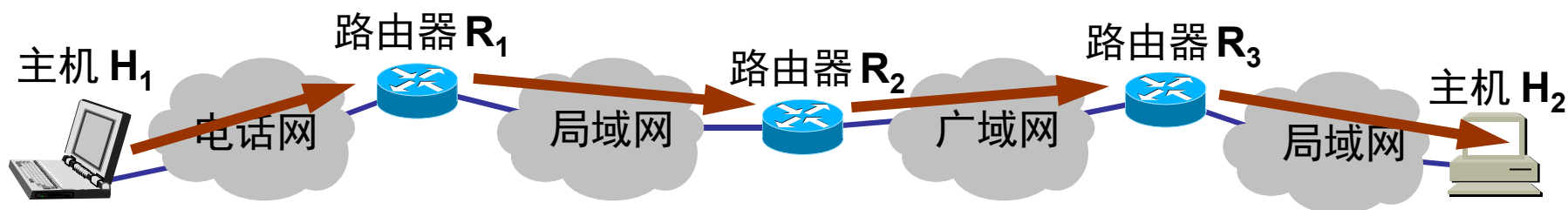
◆ 广播信道

- 多个设备共享一条公共信道
- 一对多通信
- 需要解决信道竞争
- LAN采用
- 在第6章学习



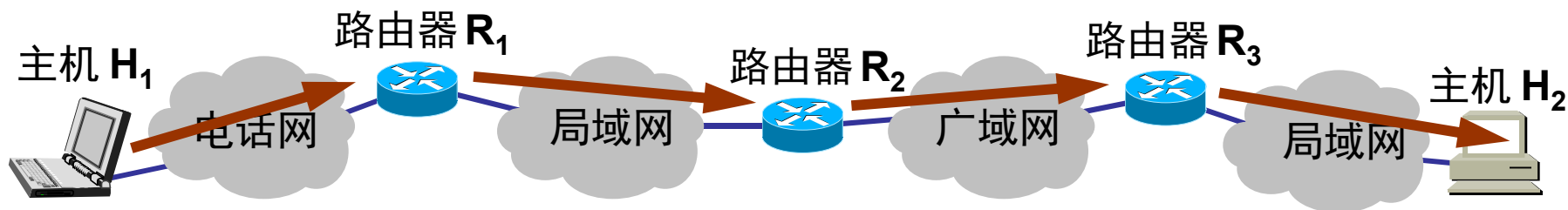
网络层：主机-主机通信

主机 H_1 向 H_2 发送数据

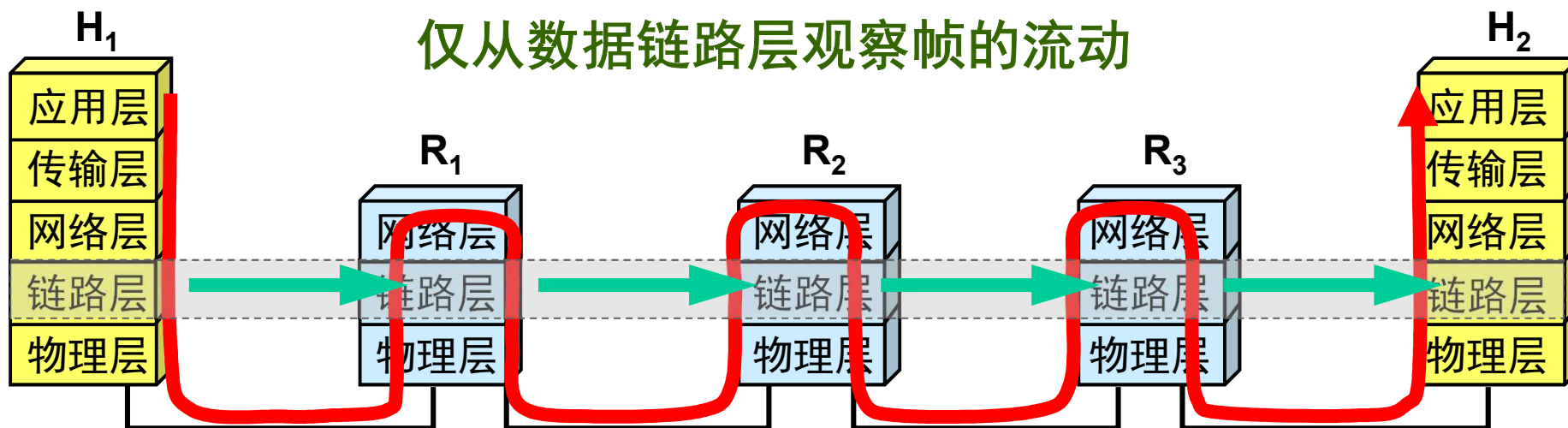


数据链路层：点到点通信

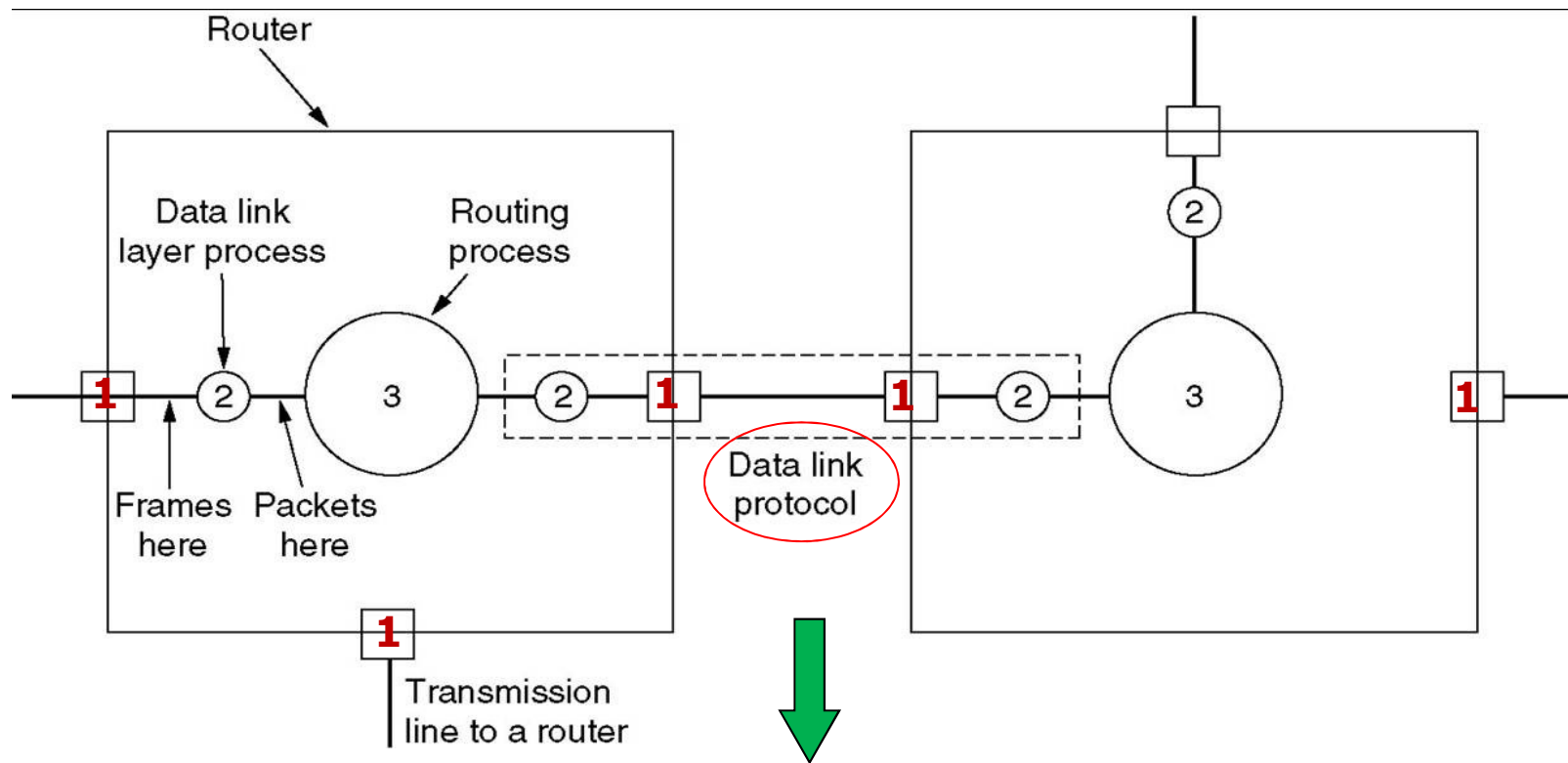
主机 H_1 向 H_2 发送数据



仅从数据链路层观察帧的流动



数据链路层的功能



- ➡流量控制：可以发送多少数据？
- ➡差错控制：如何发现传输差错并纠正？
- ➡访问控制：谁能发送？

数据链路层的主要功能

◆ 链路管理

- 数据链路的建立、维护和释放，以提供面向连接的服务，

◆ 封装成帧

- 将网络层的数据（如IP包）加上首部和尾部，组成帧

◆ 差错控制

- 检查物理层的传输差错，并纠正错误

◆ 透明传输

- 允许网络层的数据包含任何比特串

◆ 链路寻址：给网卡编址（物理地址/硬件地址）

数据链路层的服务

◆ 无确认的无连接服务

- 只发送不确认
- 适合于低误码率的信道，如LAN

◆ 有确认的无连接服务

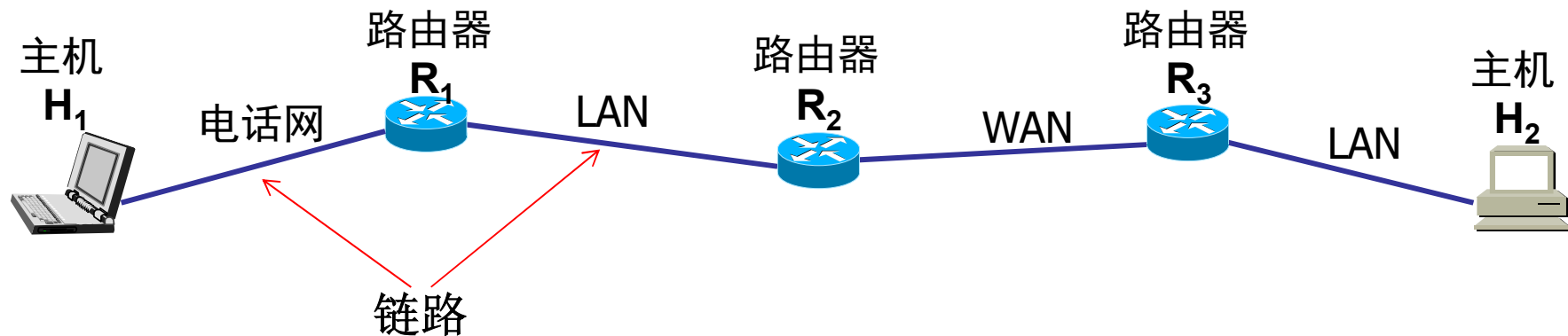
- 接收方收到数据后要回送确认
- 适合于误码率相对较高的不可靠信道，如WLAN

◆ 面向连接的服务

- 在发送数据之前首先要建立连接，确保数据传输的可靠性
- WAN采用

链路和数据链路

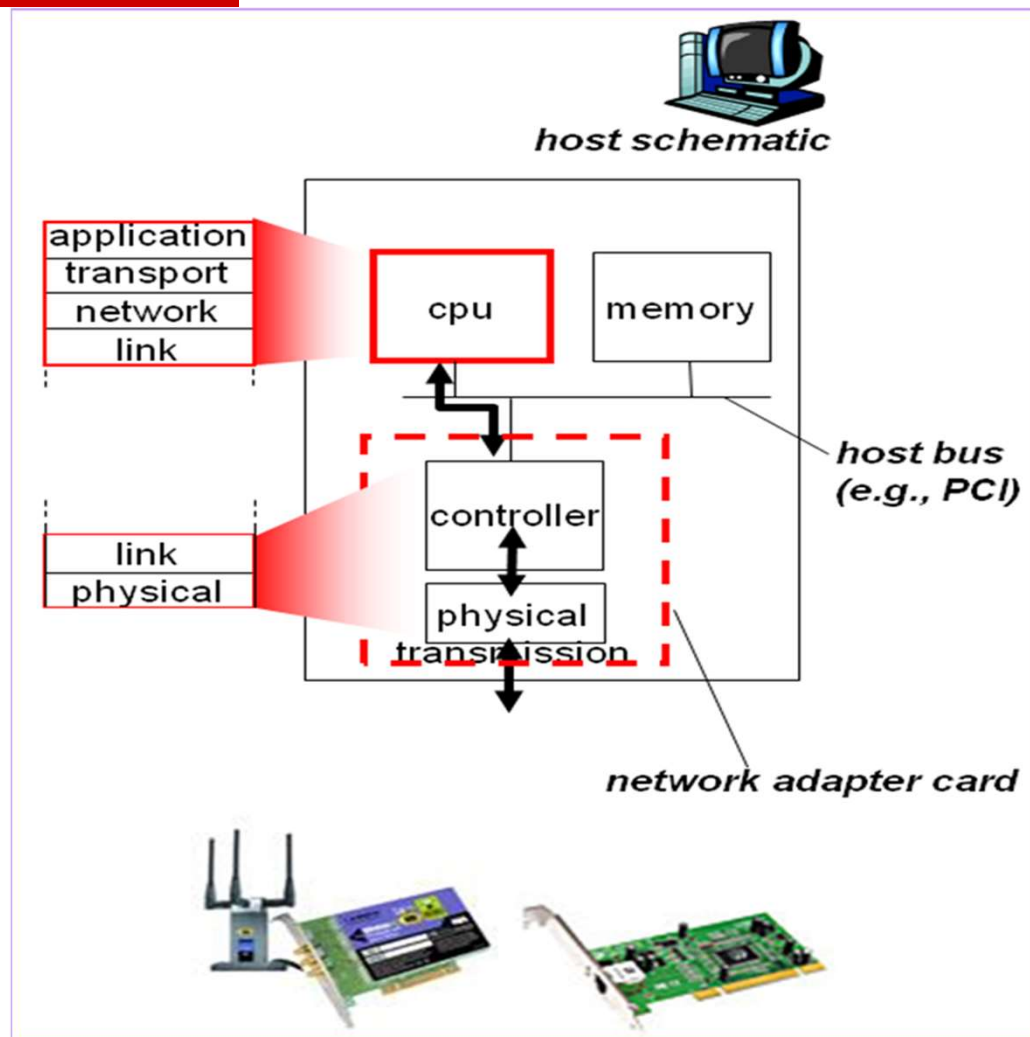
- ◆ **链路 (link)**: 是一条无源的点到点的物理线路段, 中间没有任何其他的交换结点
 - 链路是一条路径的组成部分
- ◆ **数据链路 (data link)**: 链路+数据链路层协议
 - 不同的链路可能采用不同的协议



数据链路层协议一般由网卡实现

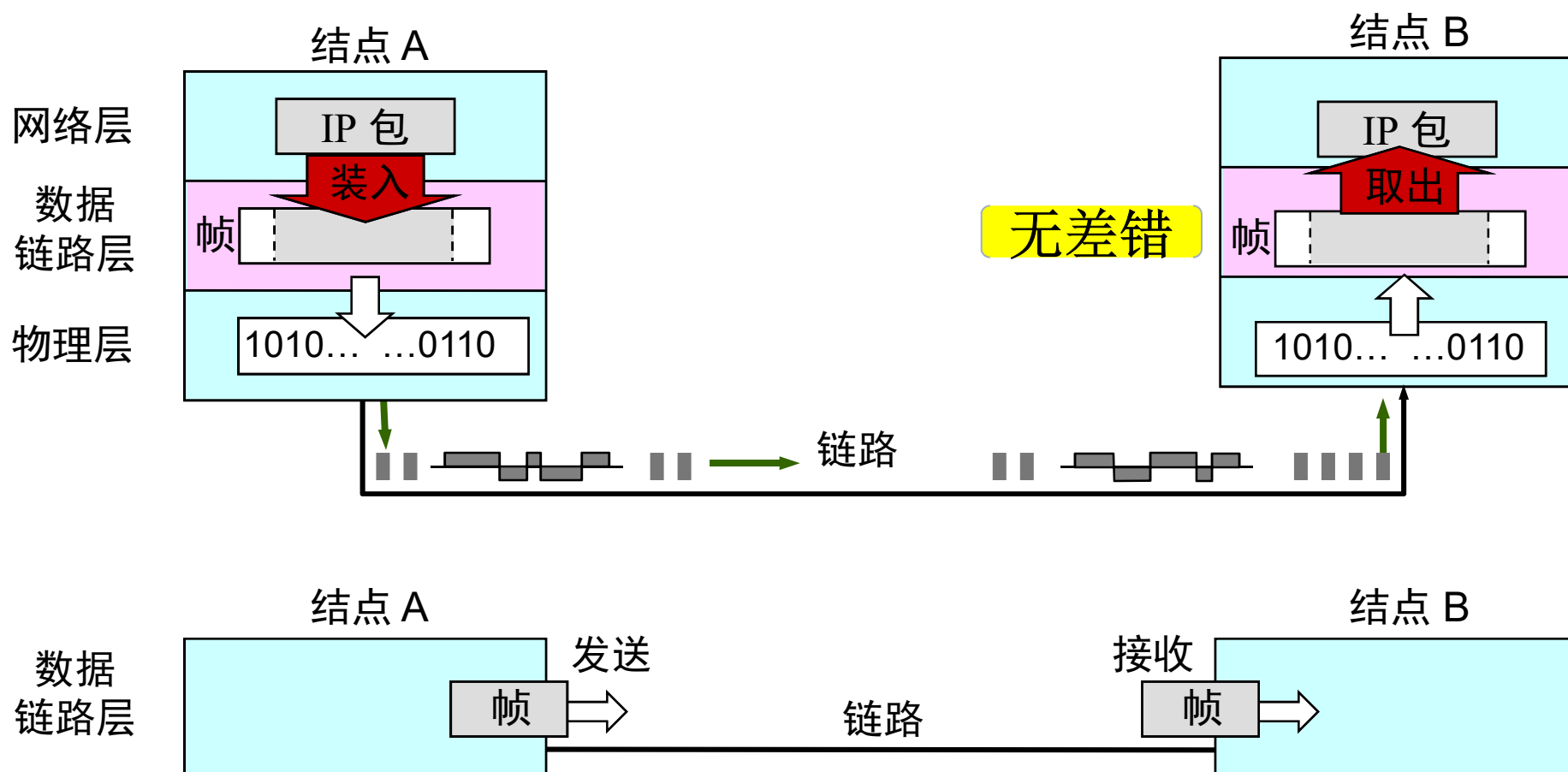
◆ 网卡

- 网络适配器：NIC
- 一般实现数据链路层协议和物理层协议



数据链路和帧

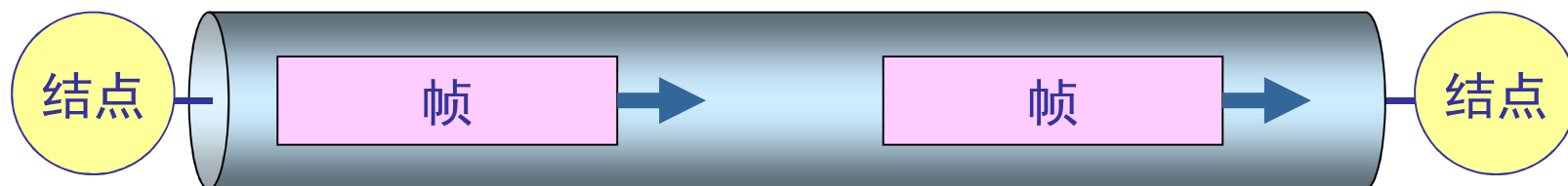
◆ 帧：数据链路上传输的数据单元



数据链路和帧

◆ 数据链路层像个数字管道

在这条数字管道上传输的数据单位是帧



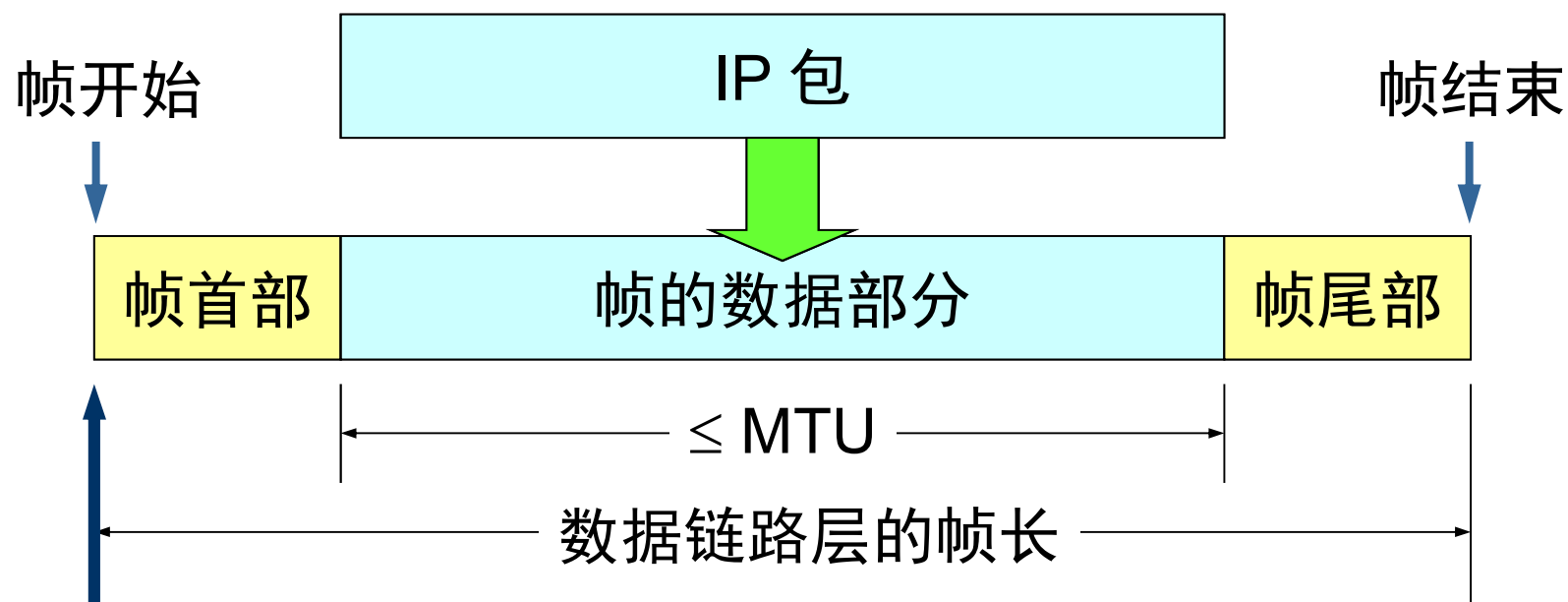
➤ 早期的数据通信协议曾叫作通信规程 (procedure)。因此在数据链路层，规程和协议是同义词。

内容提要

- ◆ 5.1 数据链路层的功能及服务
- ◆ 5.2 数据链路层的成帧原理
- ◆ 5.3 差错检测与纠错技术
- ◆ 5.4 数据链路层的编址
- ◆ 5.5 数据链路层的协议实例
- ◆ 5.6 数据链路层的安全隐患

什么是成帧？

- ◆ 在上层数据的前后分别添加首部和尾部，就构成了一个帧
- ◆ 首部和尾部的一个重要作用就是进行帧定界（帧同步），即标记帧的开始和结束



成帧方法：字符计数法

- ◆ 在帧中增加一个长度字段，表示帧的总字节数
- ◆ 早期的DDCMP协议使用

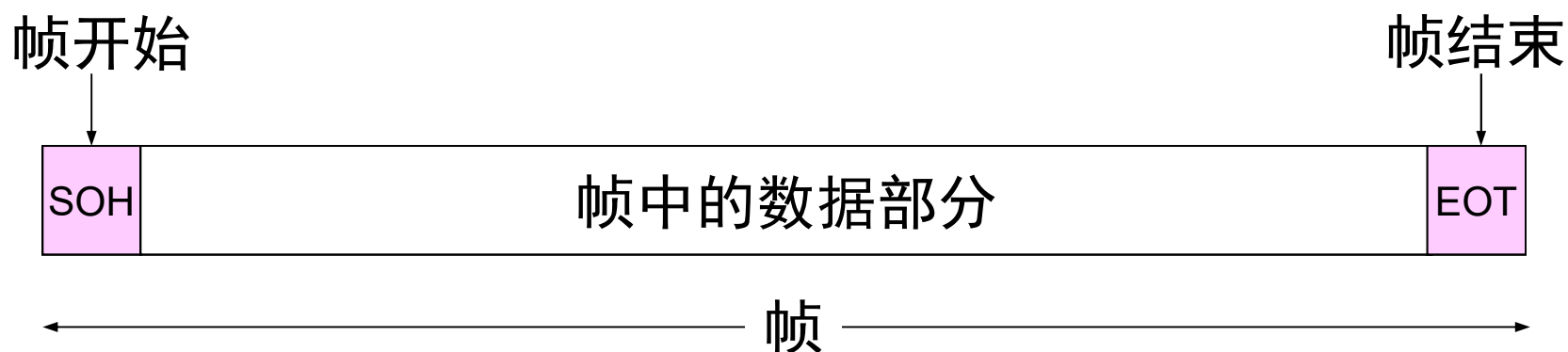


- ◆ 问题：一旦帧长度字段出错，无法再恢复同步！



成帧方法：字符填充法（1）

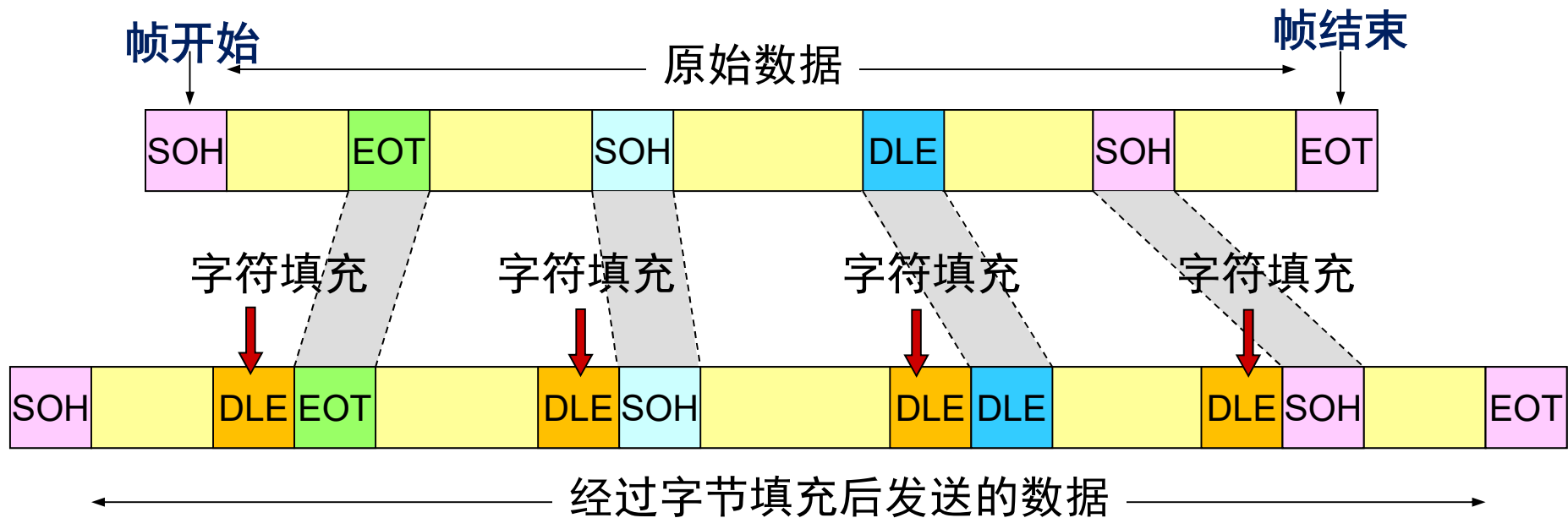
- ◆ 采用固定的字符作为帧首部和尾部
- ◆ 示例：IBM的BISYNC协议
 - 帧首字符：SOH (0x01)
 - 帧尾字符：EOT (0x04)



成帧方法：字符填充法（2）

- ◆ 透明传输：帧的数据中可以包含任何字符，即可以出现与帧首、帧尾相同的字符
- ◆ 字符填充：一旦数据中出现和帧首/尾字符相同的字符，则填充**转义字符**，以进行区别
- ◆ 转义字符：**DLE** (0x10)

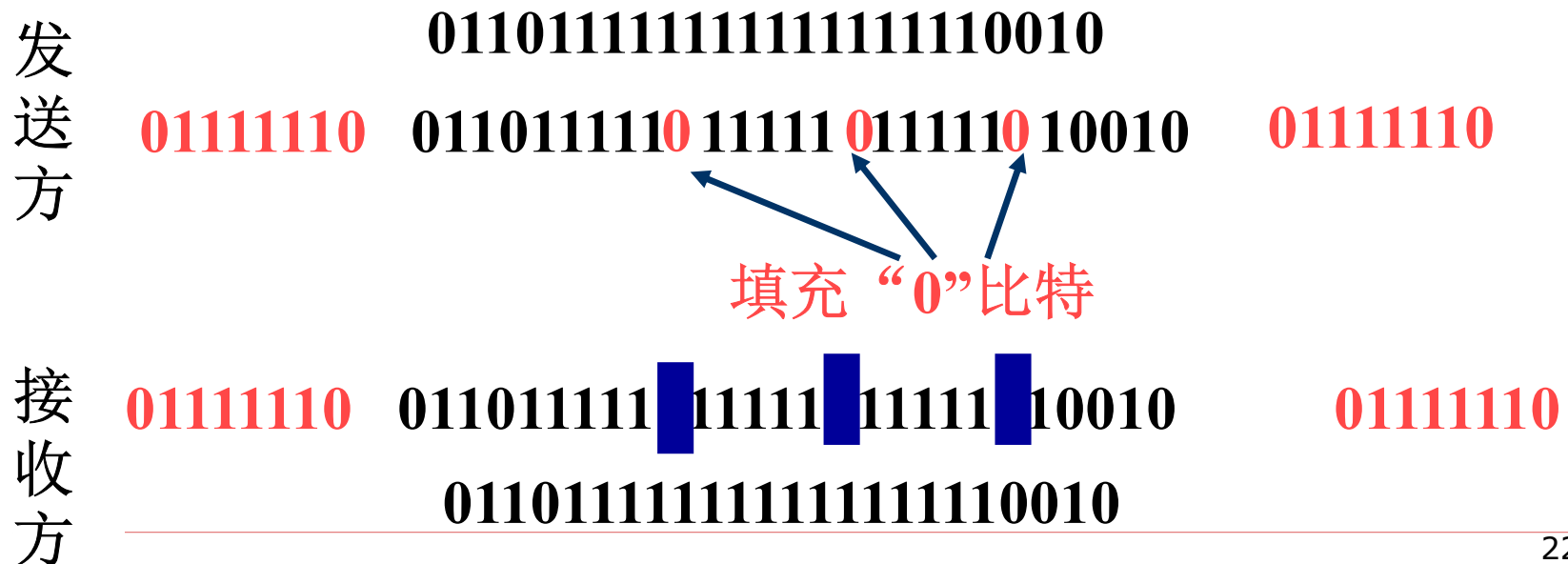
缺点：依赖于字符集



成帧方法：零比特填充法

- ◆ 帧的长度为任意比特数
- ◆ 不依赖于字符集
- ◆ 帧首尾标志：0111 1110
- ◆ 透明传输：零比特填充

➤ 当帧中的数据出现连续5个1时，在其后插入一个0



成帧方法：物理层编码违例法

◆ 物理层编码有冗余



- 曼彻斯特编码：码元中间的跳变表示0和1
- 中间无跳变的码元即是冗余码元，可以表示帧的开始和结束
- 无需填充！



内容提要

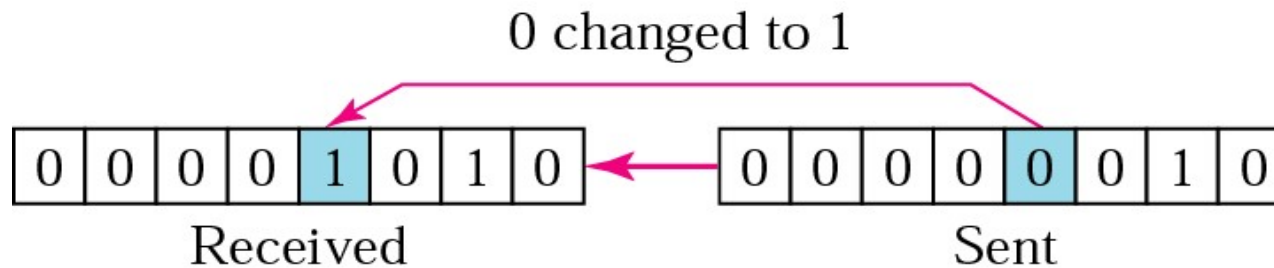
- ◆ 5.1 数据链路层的功能及服务
- ◆ 5.2 数据链路层的成帧原理
- ◆ 5.3 差错检测与纠错技术
- ◆ 5.4 数据链路层的编址
- ◆ 5.5 数据链路层的协议实例
- ◆ 5.6 数据链路层的安全隐患

什么是差错控制？

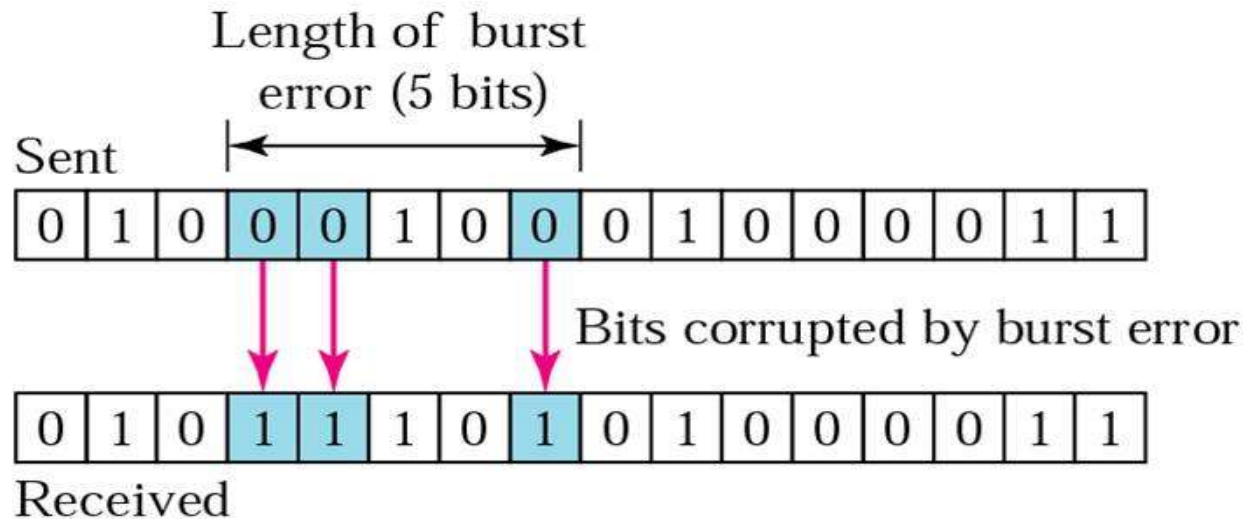
- ◆ 由于噪声的影响，数据在传输过程中可能会产生**比特差错**：1-→0，0-→1，增加、删除1个比特
- ◆ 误码率 BER (Bit Error Rate)：在一段时间内，传输错误的比特占所传输比特总数的比率
- ◆ 差错种类
 - 单比特差错 
 - 突发差错
- ◆ 差错控制
 - 差错检测：发现传输差错 
 - 差错纠正：恢复正确数据

单比特差错与突发差错

◆ 单比特差错：只有1个比特错误



◆ 突发差错：两个比特或更多比特发生错误



差错检测方法：奇偶校验

- ◆ 检错码：发送方在传输的数据中加入校验信息，接收方通过计算可以发现传输差错

- ◆ 奇偶校验码

- 1个校验比特

- 奇校验：加入校验位后，1的个数为奇数

1	0	1	1	1	0	1	0	0
---	---	---	---	---	---	---	---	---

0	0	1	1	1	0	1	0	0
---	---	---	---	---	---	---	---	---

1-bit error

0	0	0	1	0	0	1	0	0
---	---	---	---	---	---	---	---	---

3-bit error

0	0	1	1	1	1	1	0	0
---	---	---	---	---	---	---	---	---

2-bit error

- 偶校验：加入校验位后，1的个数为偶数

1	0	1	1	1	0	1	0	1
---	---	---	---	---	---	---	---	---

- 检错能力：如果发生错误的比特总数为奇数个，能发现

差错检测方法：循环冗余校验

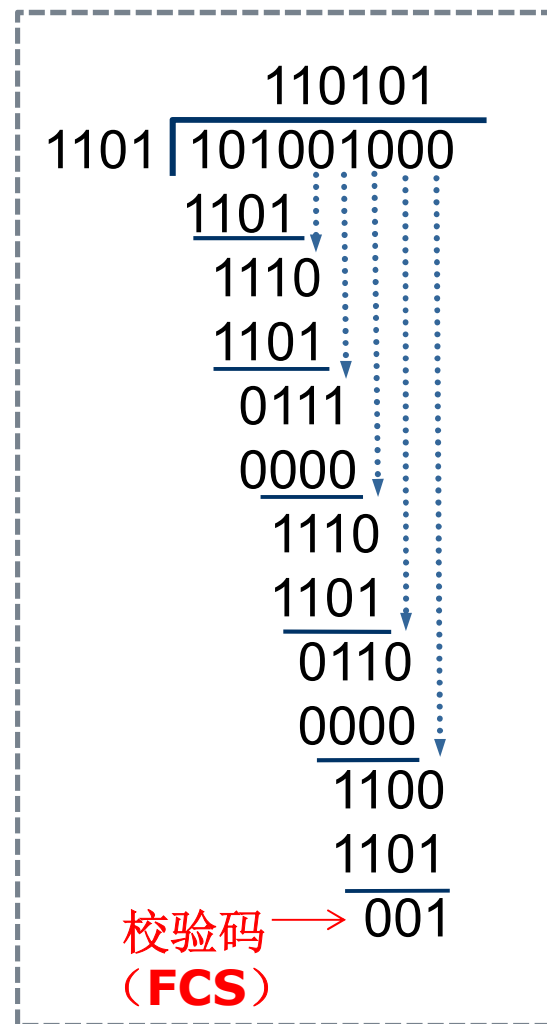
- ◆ CRC (Cyclic Redundancy Code), 又称为多项式编码
- ◆ 把被处理的数据块看做是一个n阶的二进制多项式： $a_0x_0 + a_1x_1 + \dots + a_{n-1}x_{n-1}$
 - 如10110101对应的多项式是： $x^7 + x^5 + x^4 + x^2 + 1$
- ◆ 采用模二除法计算校验码
- ◆ 生成多项式G(x): 发送方和接收方约定, 作为除数
- ◆ 校验码: 余数

CRC的计算方法

- ◆ 若生成多项式 $G(x)$ 为 $r+1$ 个比特，即最高阶为 r ，则在待校验数据后面增加 r 个0
- ◆ 采用模二除法，除以 $G(x)$
 - 对应比特异或
 - 不进位、不借位
- ◆ 余数即是所求的校验码
- ◆ 将余数附在数据之后发送到信道上

CRC的计算示例

- ◆ 待校验数据：101001
- ◆ 生成多项式 $G(x) = x^3 + x^2 + 1$
- ◆ 被除数：101001 000
- ◆ 除数：1101
- ◆ 余数：001
- ◆ 发送的数据：101001001
- ◆ 接收方：
 - 用收到的数据比特串除以 $G(x)$ ，余数=0，则认为传输正确；否则，认为传输有差错



CRC的检错能力

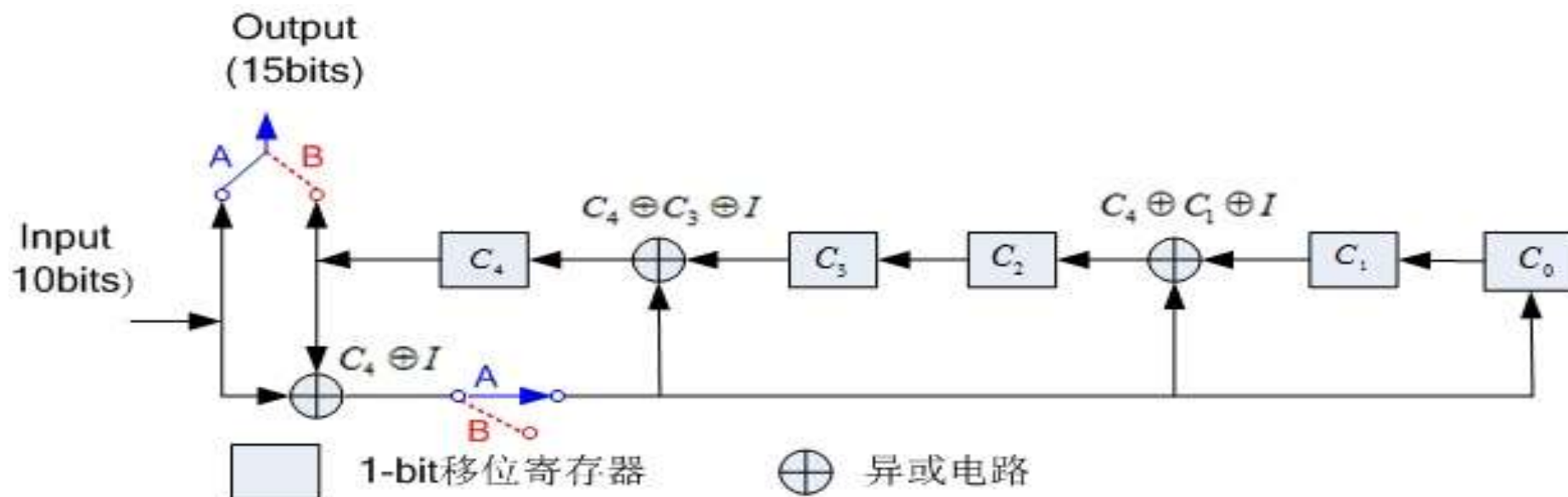
- ◆ 若 $G(x)$ 为 r 阶，则可以检测出长度不超过 r 的突发错误
- ◆ 可以检测出任意两个孤立的单比特错误
- ◆ 可以检测出错误比特数为奇数的错误
- ◆ 对于长度超过 r 的突发错误
 - 无法检测出差错的概率为 2^{-r}

CRC的标准

- ◆ CRC-12码： 传送6位字符串
- ◆ CRC-16码： 传送8位字符，美国采用
- ◆ CRC-CCITT码： 传送8位字符，HDLC采用
- ◆ CRC-32码： LAN采用
- ◆ 常用的CRC标准生成多项式：
 - CRC-16: $X^{16}+X^{15}+X^2+1$
 - CRC(CCITT): $X^{16}+X^{12}+X^5+1$
 - CRC-32:
 $X^{32}+X^{26}+X^{23}+X^{16}+X^{12}+X^{11}+X^{10}+X^8+X^7+X^5+X^4+X^2+X+1$

CRC的硬件实现方法

◆ 移位寄存器+异或门电路



- ◆ $G(x) = x^5 + x^4 + x^2 + 1$
- ◆ 初始时移位寄存器 $C_0 \sim C_4$ 清0
- ◆ 10个信息位发送之后，断开A接通B，发送5位校验和

差错纠正方法

◆ 纠错码

- 校验码足够长，不但能够检测出差错，而且能够发现差错的位置，直接恢复原始数据
- 示例：汉明码（Hamming code，海明码），能纠正一比特错误

◆ 重传（ARQ协议）

- 发送方发送完一帧数据后，启动一个定时器
- 接收方发现错误后，丢弃收到的数据帧
- 发送方定时器超时，重发数据帧

纠错码示例：汉明码

- ◆ 基本思想：将待校验数据信息按某种规律分成若干组，每组安排一个校验比特，进行奇偶校验，因此能提供多比特检错信息，以发现出错的比特，从而将其纠正
- ◆ 实质上，汉明码是一种多重校验
- ◆ 位置分布：从左至右，对数据比特进行编号，编号为2的幂次的位置保留给校验比特
 - 例如：要校验的数据是 1011

编号:	1	2	3	4	5	6	7
传输的码字:	1	0	1	1	0	1	1

汉明码的校验方法（1）

◆ 发送方编码：

$$3=1+2, \quad 5=1+4, \quad 6=2+4, \quad 7=1+2+4$$

即第1个校验比特是对编号为3、5和7的数据比特校验的值，第2个校验比特对编号为3、6和7的数据比特校验，...

◆ 以奇校验为例，数据比特串为 $\overset{b_3}{1} \overset{b_5}{0} \overset{b_6}{1} \overset{b_7}{1}$

$$p1 \oplus b3 \oplus b5 \oplus b7 = 1, \text{ 求出 } p1=1$$

$$p2 \oplus b3 \oplus b6 \oplus b7 = 1, \text{ 求出 } p2=0$$

$$p4 \oplus b5 \oplus b6 \oplus b7 = 1, \text{ 求出 } p4=1$$

因此传输的比特串为1011011

汉明码的校验方法（2）

◆ 接收方纠错

若 $b_1 \oplus b_3 \oplus b_5 \oplus b_7 = 1$, 则 $k=0$; 否则 $k=1$

若 $b_2 \oplus b_3 \oplus b_6 \oplus b_7 = 1$, 则 $k=0$; 否则 $k=2$

若 $b_4 \oplus b_5 \oplus b_6 \oplus b_7 = 1$, 则 $k=0$; 否则 $k=4$

出错比特的编号：出错校验比特编号之和，即 $\sum k$

◆ 示例：假设收到的比特串为 1011001

$b_1 \oplus b_3 \oplus b_5 \oplus b_7 = 1$, 无错 $k=0$

$b_2 \oplus b_3 \oplus b_6 \oplus b_7 = 0$, 有错 $k=2$

$b_4 \oplus b_5 \oplus b_6 \oplus b_7 = 0$, 有错 $k=4$

因此出错的比特的编号 $= \sum k = 2 + 4 = 6$

汉明码的开销

- ◆ 设待校验的数据（有效信息）为 m 比特，校验信息为 r 比特
- ◆ 发送的码字： $n=m+r$ 比特
- ◆ 合法码字有 2^m 个
- ◆ 一个合法码字错1位而产生的非法码字有 n 个
- ◆ 合法码字与非法码字一共 $(n+1)2^m$ 个

$$(n+1)2^m \leq 2^n$$

$$(m+r+1) \leq 2^r$$

例如： $m=4, r \geq 3$

内容提要

- ◆ 5.1 数据链路层的功能及服务
- ◆ 5.2 数据链路层的成帧原理
- ◆ 5.3 差错检测与纠错技术
- ◆ 5.4 数据链路层的编址
- ◆ 5.5 数据链路层的协议实例
- ◆ 5.6 数据链路层的安全隐患

物理地址

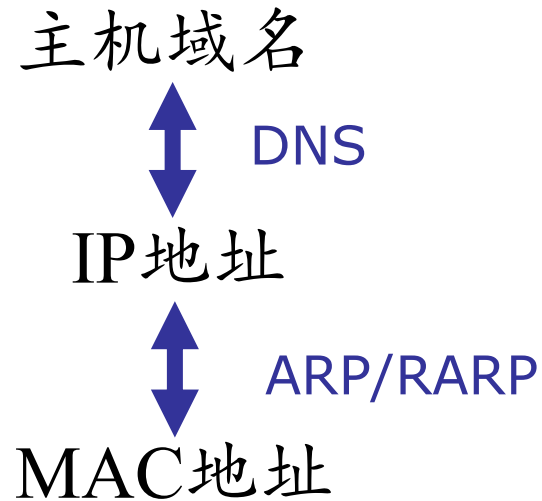
- ◆ 数据链路层的地址又称为物理地址或硬件地址
- ◆ 每个网络接口（网卡）一个地址
- ◆ 示例：MAC（媒体访问控制/介质访问控制）地址
 - LAN内使用
 - 48位，以16进制表示
 - 前24位为生产厂商标识OUI（Organizationally Unique Identifier）
 - 后24位为由厂商设定的内部编号

F0-DE-F1-3C-A7-0F



Wistron InfoComm Co.

地址转换



- ◆ 地址解析协议：ARP(Address Resolution Protocol)
 - 将IP地址转换为MAC地址
- ◆ 逆向地址解析协议：RARP (Reverse ARP)
 - 有MAC地址，查找对应的IP地址
 - 无盘工作站启动时，请求IP地址

ARP缓存表

```
C:\Users\chengli>arp -a
```

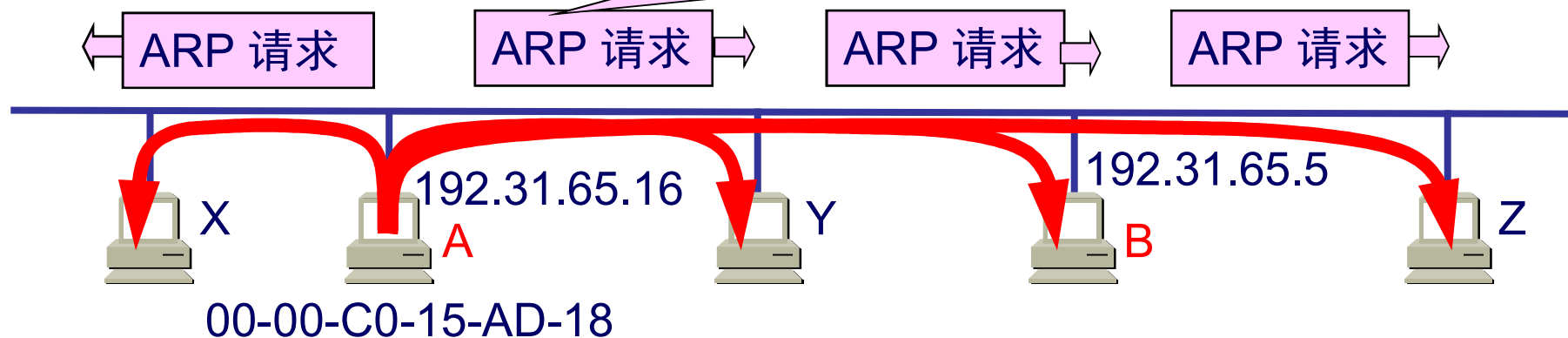
```
接口: 192.168.0.101 --- 0xe
```

Internet 地址	物理地址	类型
192.168.0.1	78-54-2e-e2-f9-24	动态
192.168.0.255	ff-ff-ff-ff-ff-ff	静态

- ◆ LAN的每个站点都有一个ARP缓存表，记录MAC地址与IP地址的映射关系
- ◆ 在LAN内发送IP包之前，源节点广播ARP请求，包含目的节点的IP地址
- ◆ 目的节点将自己的MAC地址放到ARP响应中，单播发送给源节点
- ◆ 源节点将ARP映射关系加入ARP表
- ◆ ARP缓存表会定时删除无用的内容

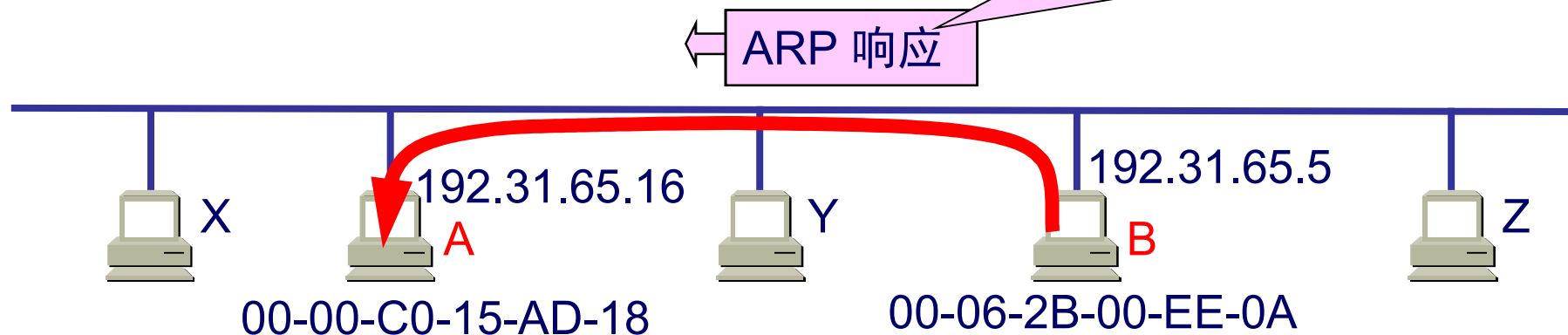
A 广播ARP请求

我是 192.31.65.16，硬件地址是 00-00-C0-15-AD-18
我想知道主机 192.31.65.5的硬件地址



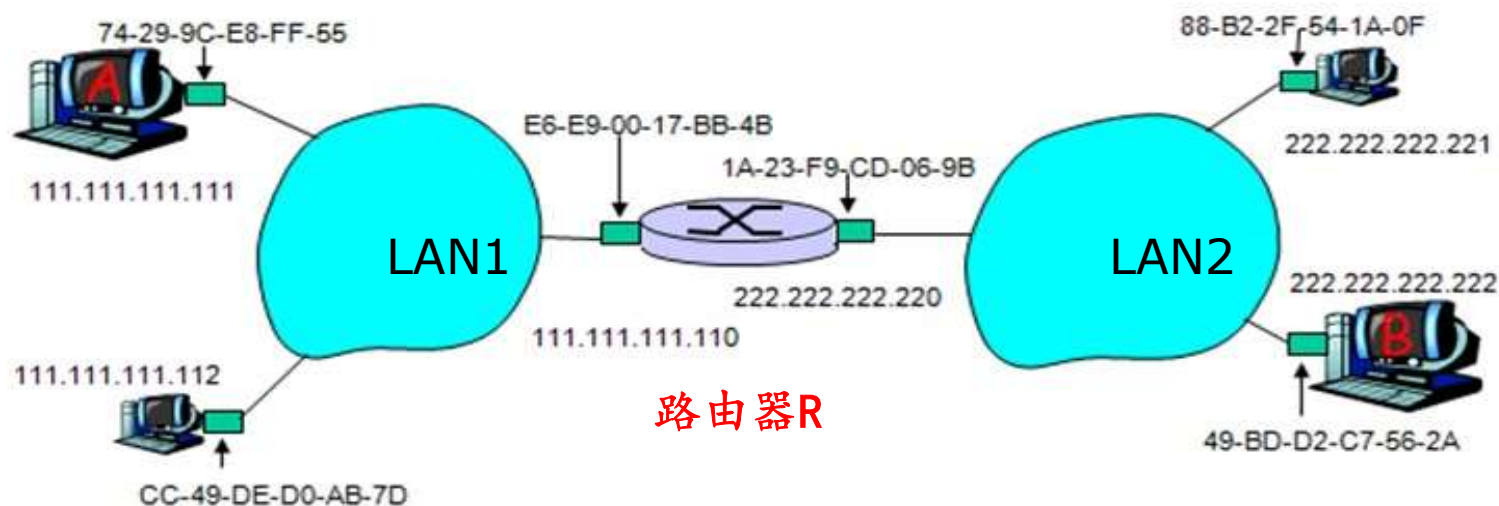
B 发送ARP响应给 A

我是 192.31.65.5
硬件地址是 00-06-2B-00-EE-0A



跨子网的数据传输过程

◆ 源主机A和目的主机B不在同一个子网



A-R: 源IP 111.111.111.111

目的IP 222.222.222.222

源MAC 74-29-9C-E8-FF-55

目的MAC E6-E9-00-17-BB-4B

R-B: 源IP 111.111.111.111

目的IP 222.222.222.222

源MAC 1A-23-F9-CD-06-9B

目的MAC 49-BD-D2-C7-56-2A

内容提要

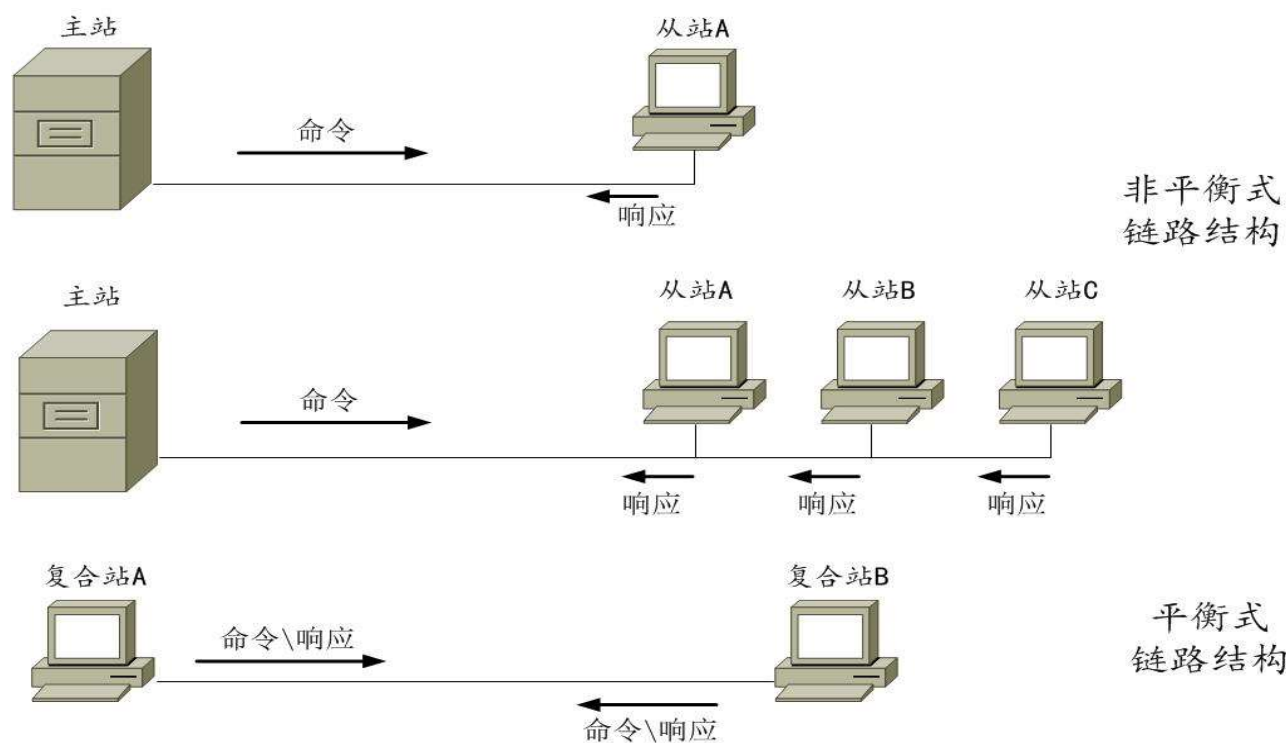
- ◆ 5.1 数据链路层的功能及服务
- ◆ 5.2 数据链路层的成帧原理
- ◆ 5.3 差错检测与纠错技术
- ◆ 5.4 数据链路层的编址
- ◆ 5.5 数据链路层的协议实例
 - HDLC协议
 - PPP协议
- ◆ 5.6 数据链路层的安全隐患

HDLC协议

- ◆ 高级数据链路控制规程（High-Level Data Link Control）
- ◆ 面向比特的协议，支持全双工传输
- ◆ 采用**零比特填充**方式实现透明传输
- ◆ 提供了点对点 and 点对多点两种连接方式
- ◆ 应用场合：
 - 广域网
 - X.25分组交换网（LAPB）
 - ISDN（LAPD）
 - 帧中继（LAPF）
 - PPP
 - LAN：LLC子层协议

HDLC的站类型

- ◆ 主站：控制通信，发送命令，维护数据链路
- ◆ 从站：不能主动发起通信，只能响应主站的命令
- ◆ 复合站：双方都可以发送命令或响应



HDLC的数据响应方式

◆ 正常响应方式 (NRM)

- 应用于非平衡式链路结构

◆ 异步响应方式 (ARM)

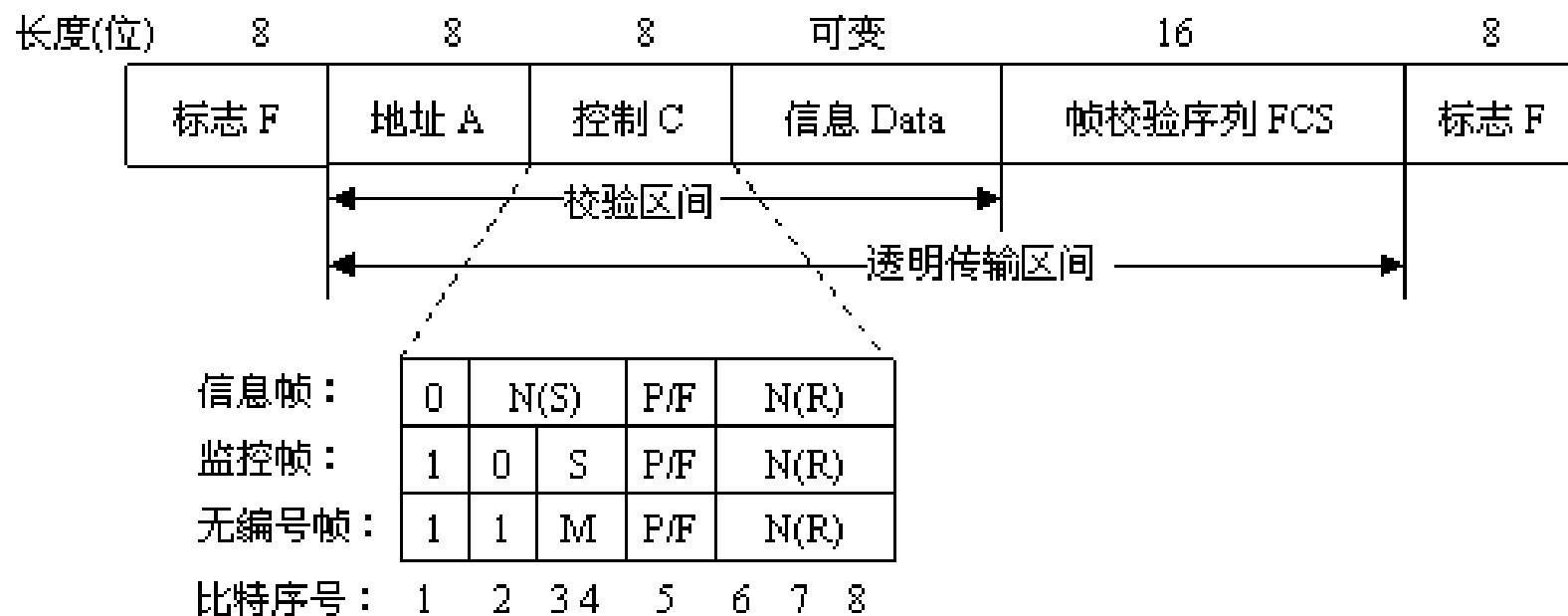
- 应用于非平衡式链路结构；允许从站自行开始传输数据，主站仍然负责链路管理

◆ 异步平衡方式 (ABM)

- 应用于平衡式链路结构
- 任何一个复合站均可以开始通信

HDLC协议规定的帧结构

- ◆ 数据帧和控制帧采用统一的帧结构
- ◆ 帧首尾标志：0111 1110
- ◆ 地址：从站/应答站的地址
- ◆ FCS：采用CRC-16计算出的校验信息



HDLC的帧的类型

➤ 信息帧（I帧）Information

用来传输用户数据；

帧标志	地址	控制	数据	帧校验	帧标志
-----	----	----	----	-----	-----

➤ 监控帧（S帧）Supervisory，监督帧

用来传输控制信息（如流量和差错控制信息）；

帧标志	地址	控制	帧校验	帧标志
-----	----	----	-----	-----

➤ 无序号帧（U帧）Unnumbered，无编号帧

用来传输网络管理信息；

帧标志	地址	控制	管理信息	帧校验	帧标志
-----	----	----	------	-----	-----

HDLC帧中的控制字段

标识帧的类型和功能，使对方站执行特定的操作。

	bit		1	3	1	3	
信息帧			0	N(s)	P/F	N(R)	
监督帧			1	0	S	P/F	N(R)
无编号帧			1	1	M1	P/F	M2

HDLC帧中的控制字段：信息帧

	bit	1	3	1	3
信息帧		0	N(s)	P/F	N(R)

N(s) - 发送序号

表示当前发送的信息帧的序号，使用滑动窗口技术，3位序号，发送窗口 $W_s=7$;

N(r) - 接收序号（确认序号）

表示本站期望收到的帧的发送序号，而不是最后一个已收到的帧序号;

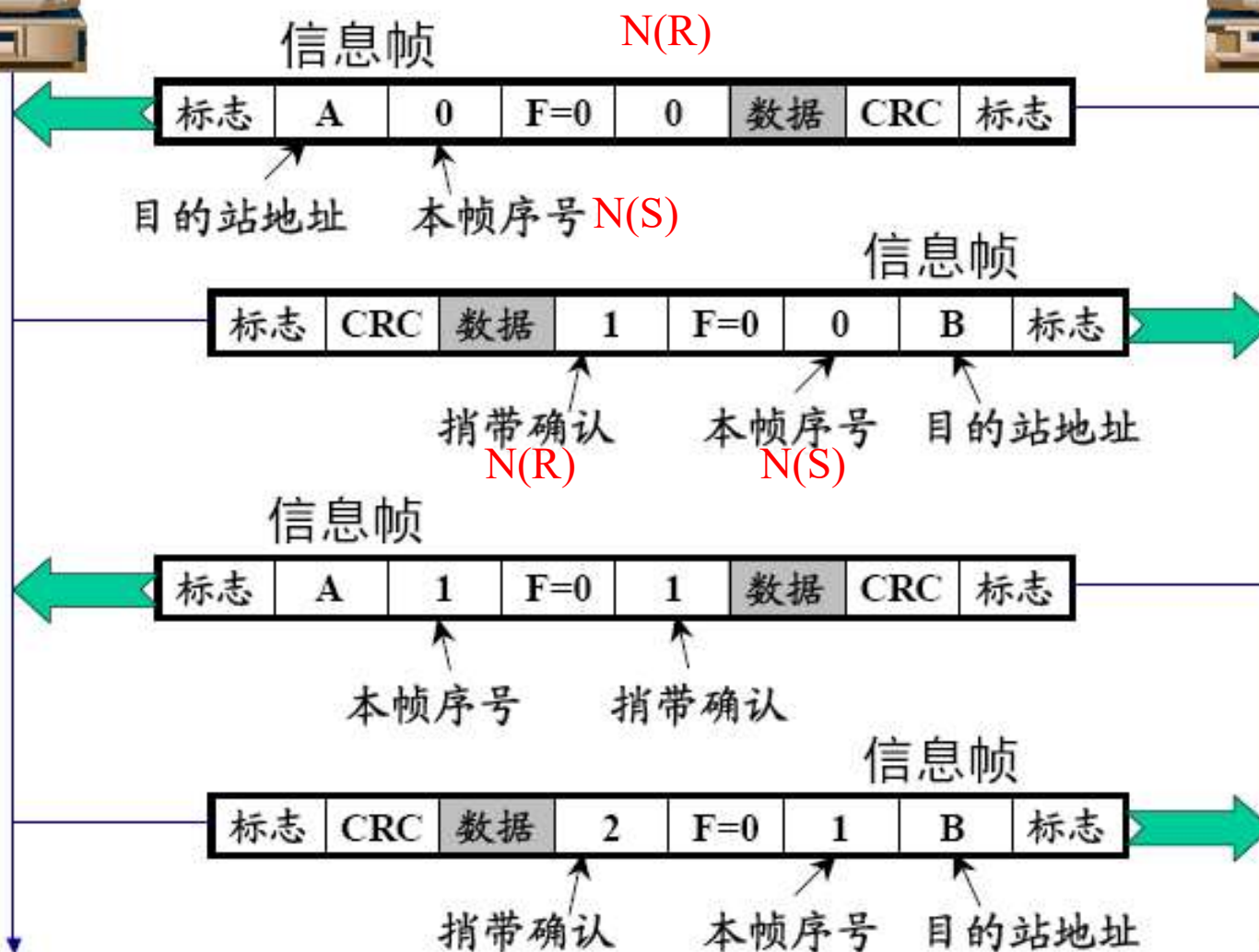
它具有捎带确认功能。

复合站A



HDLC帧的捎带确认

复合站B



HDLC帧中的控制字段：监督帧

bit	1	1	2	1	3
	1	0	S	P/F	N(R)
S	帧 名		功 能		
00	RR（接收准备就绪）		准备接收下一帧 确认序号为N(R)-1及其以前的各帧		
10	RNR（接收未就绪）		暂停接收下一帧 确认序号为N(R)-1及其以前的各帧		
01	REJ（拒绝）		否认从N(R)起以后的所有帧		
11	SREJ（选择拒绝）		只否认N(R)帧		

RR和RNR具有流量控制作用。

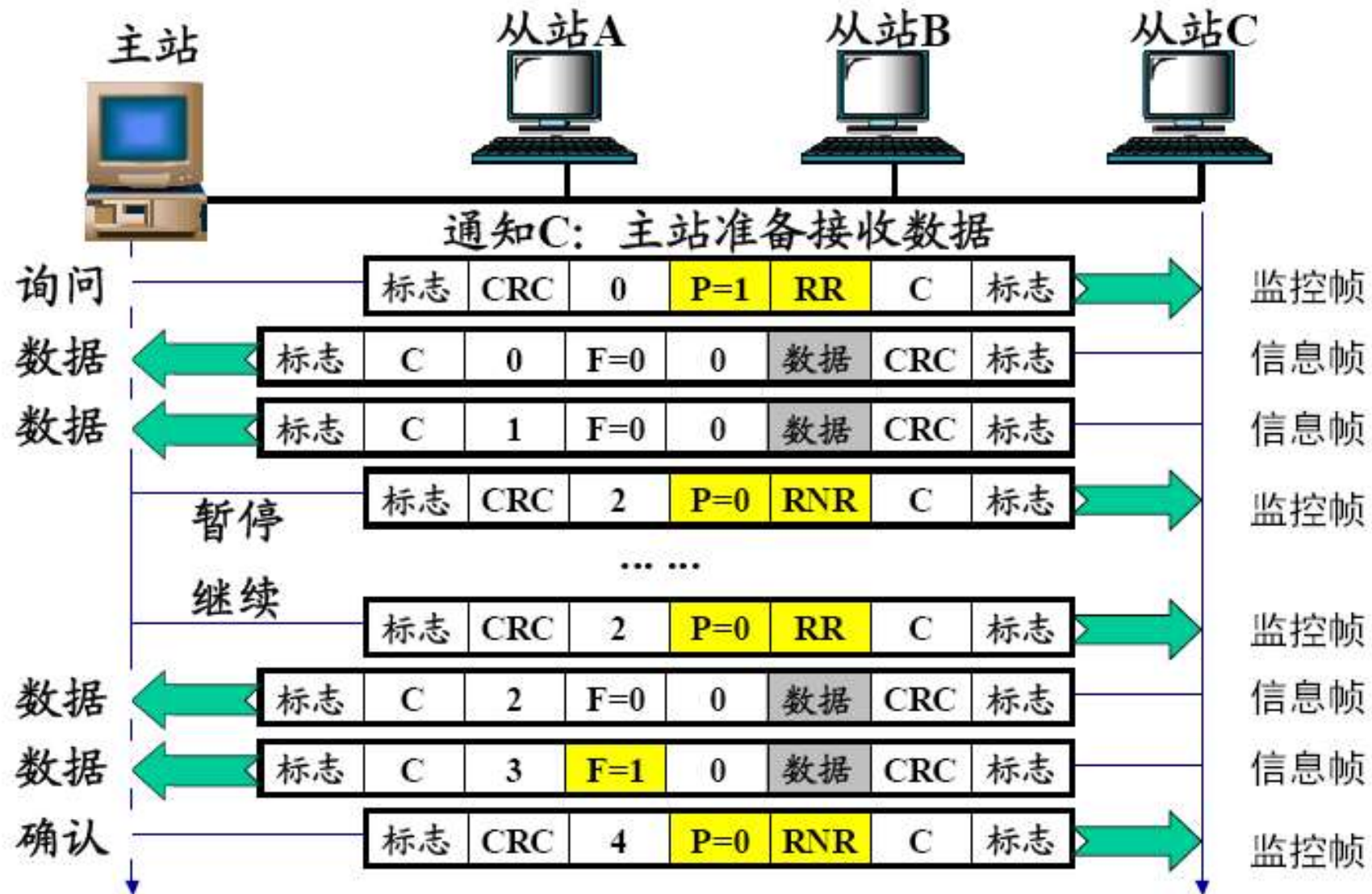
REJ用于回退N帧 ARQ协议； SREJ用于选择重发协议。

回退N步（Go-back-N）

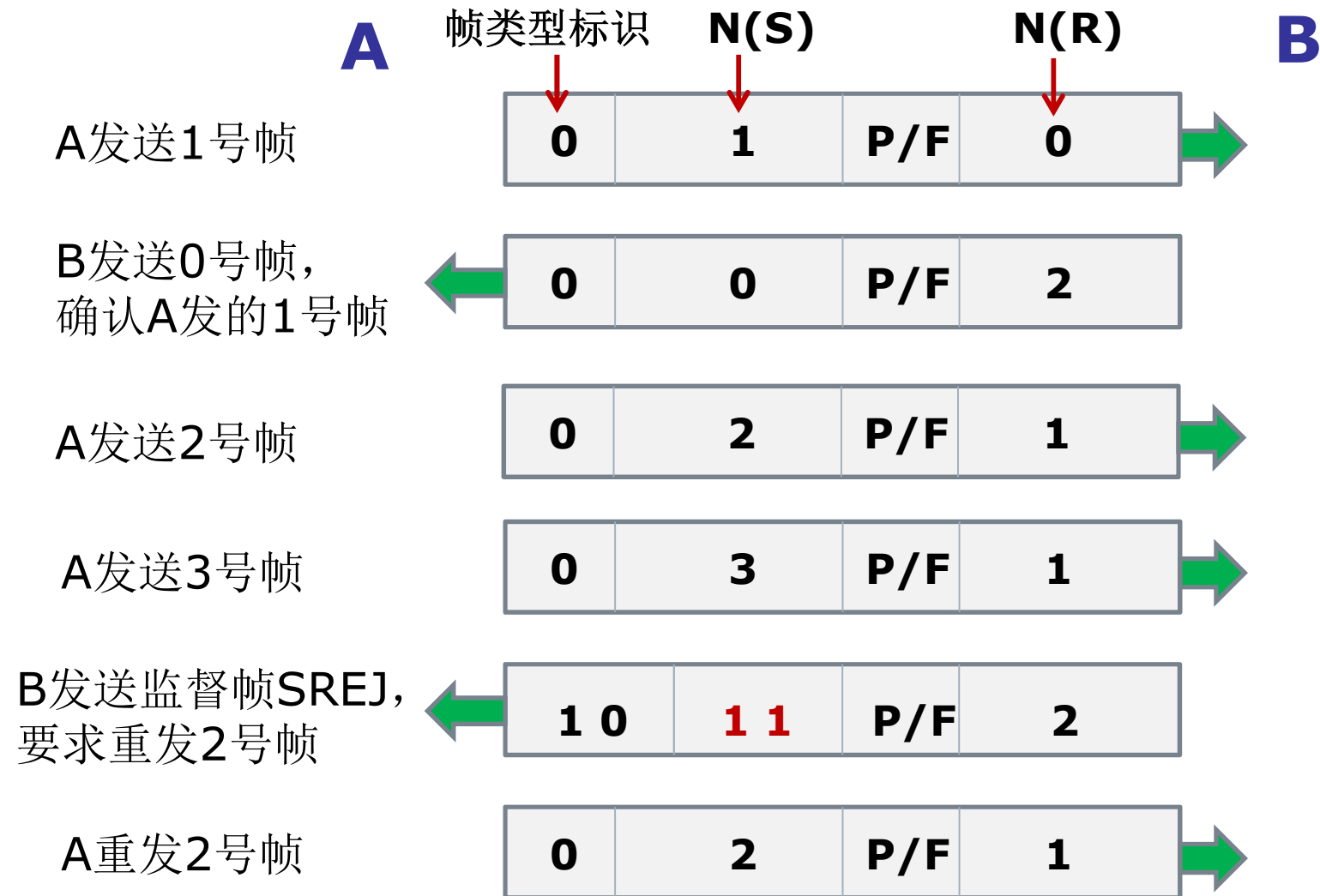
[来源于网络] 54

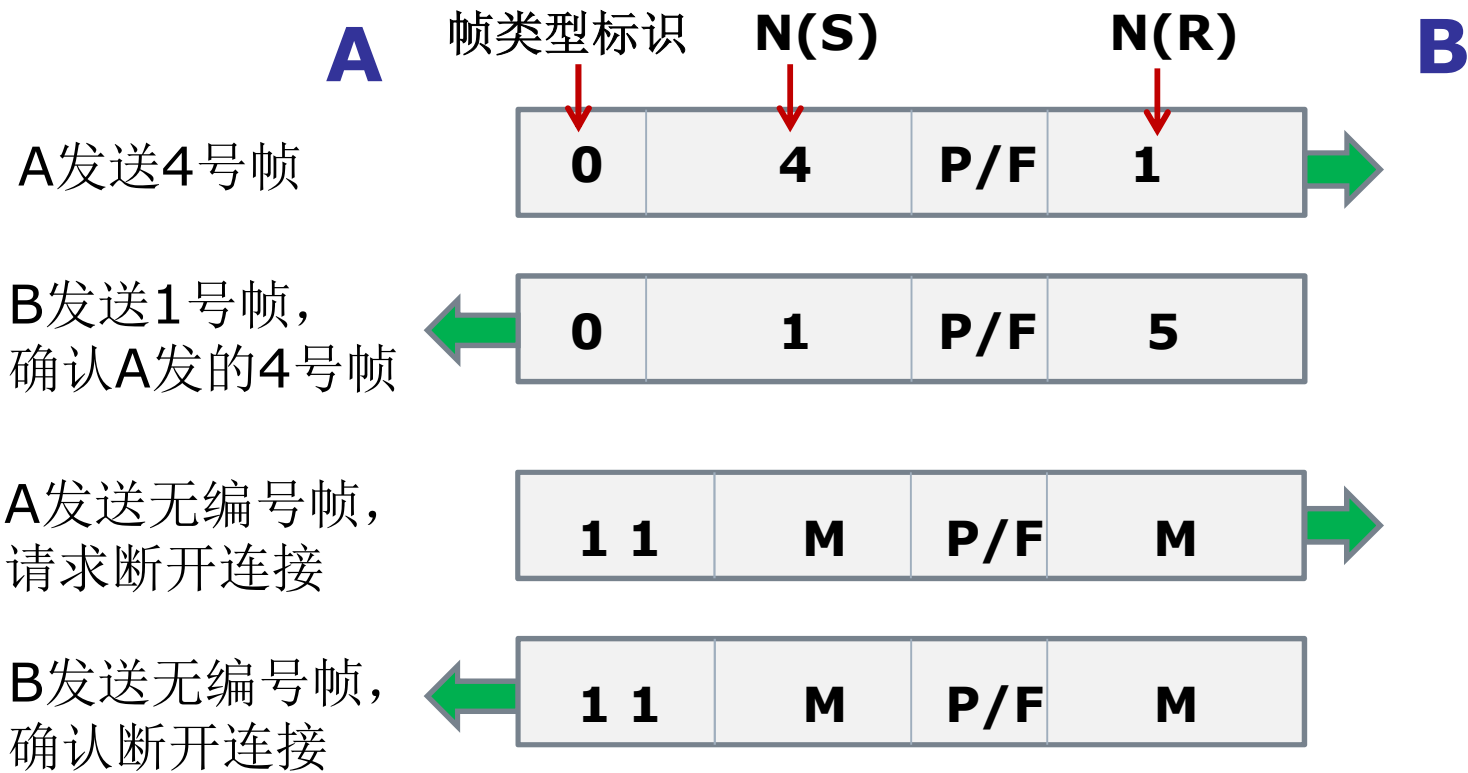
监督帧的应用示例：

从站数据→主站

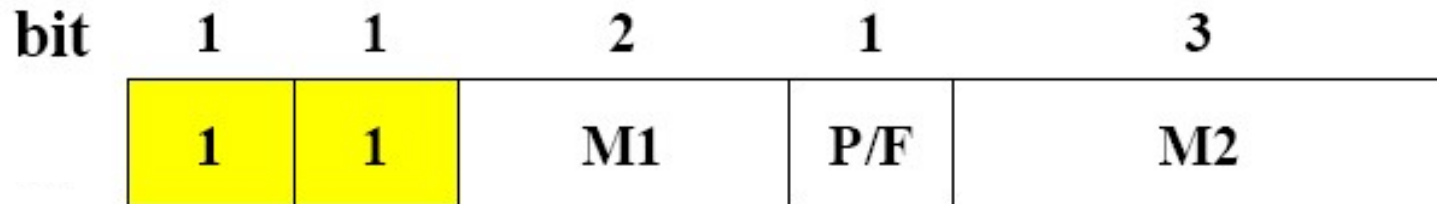


HDLC数据传输示例（书p177 图5-15）



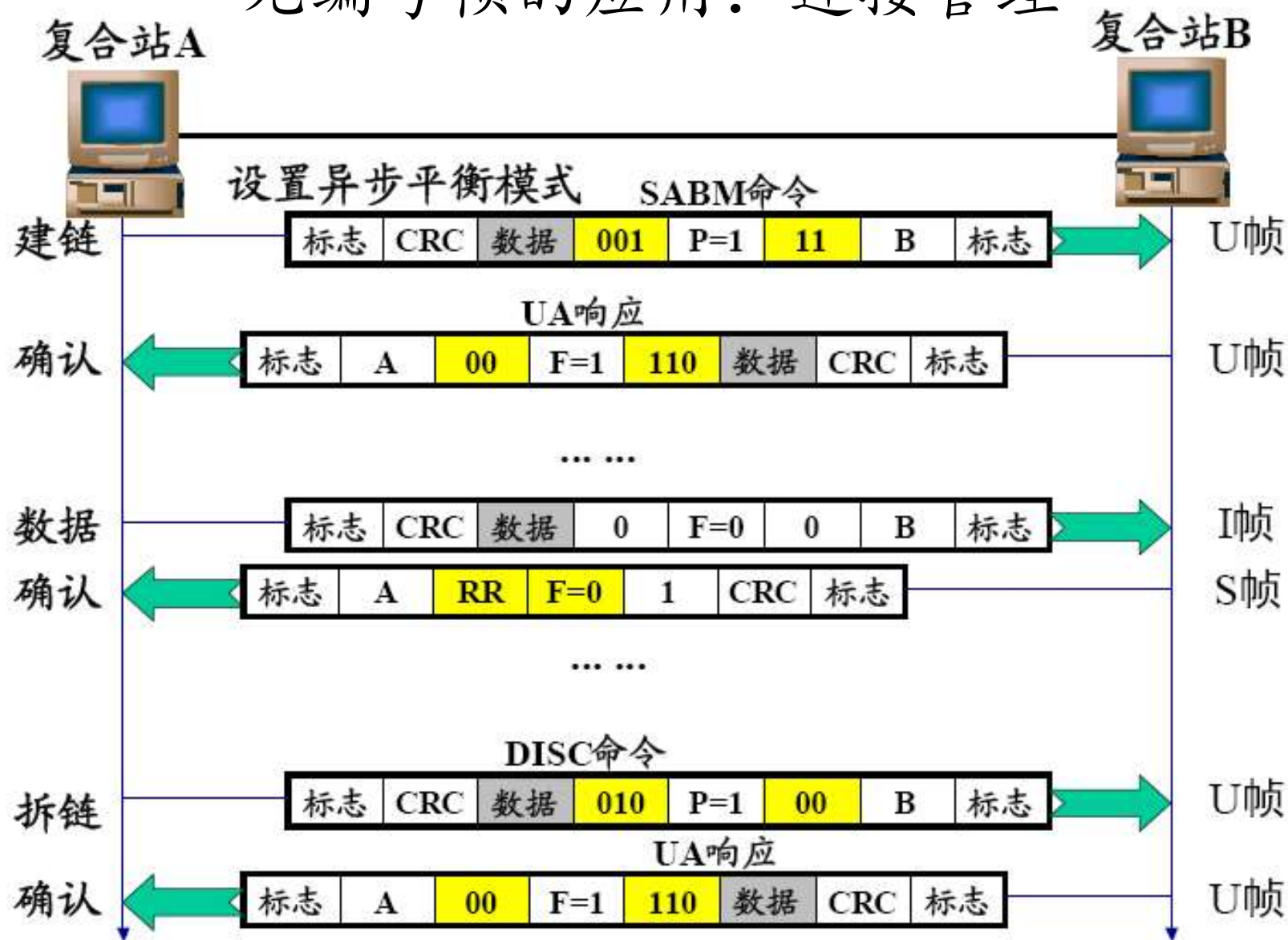


HDLC帧中的控制字段：无编号帧



M1	M2	帧 名	功 能
00	001	SNRM (命令)	设置正常响应模式
11	000	SARM (命令)	设置异步响应模式
11	100	SABM (命令)	设置异步平衡模式
00	010	DISC (命令)	断开连接
00	110	UA (响应)	对U帧命令确认
...

无编号帧的应用：连接管理

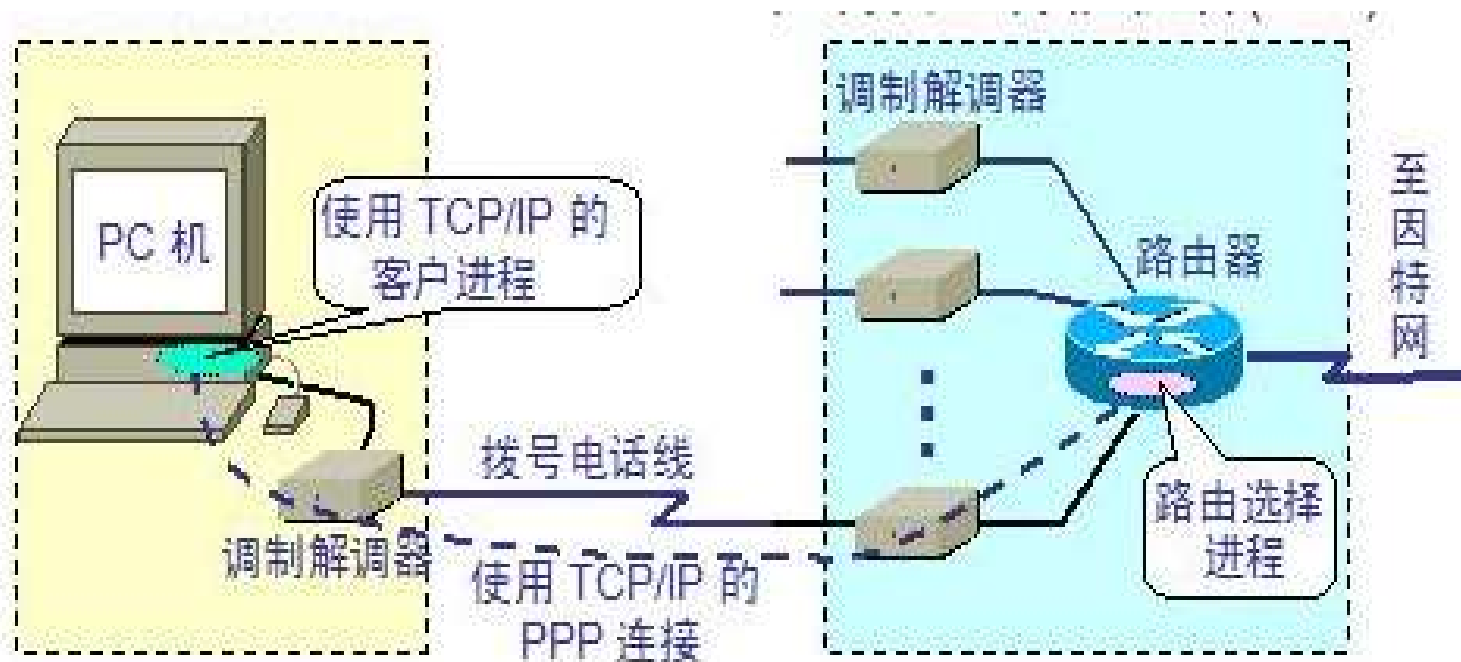


内容提要

- ◆ 5.1 数据链路层的功能及服务
- ◆ 5.2 数据链路层的成帧原理
- ◆ 5.3 差错检测与纠错技术
- ◆ 5.4 数据链路层的编址
- ◆ 5.5 数据链路层的协议实例
 - HDLC协议
 - PPP协议
- ◆ 5.6 数据链路层的安全隐患

PPP协议

- ◆ 点对点协议（Point-to-Point Protocol）
- ◆ 用户使用电话线接入因特网时使用
 - 用户与ISP之间的通信协议

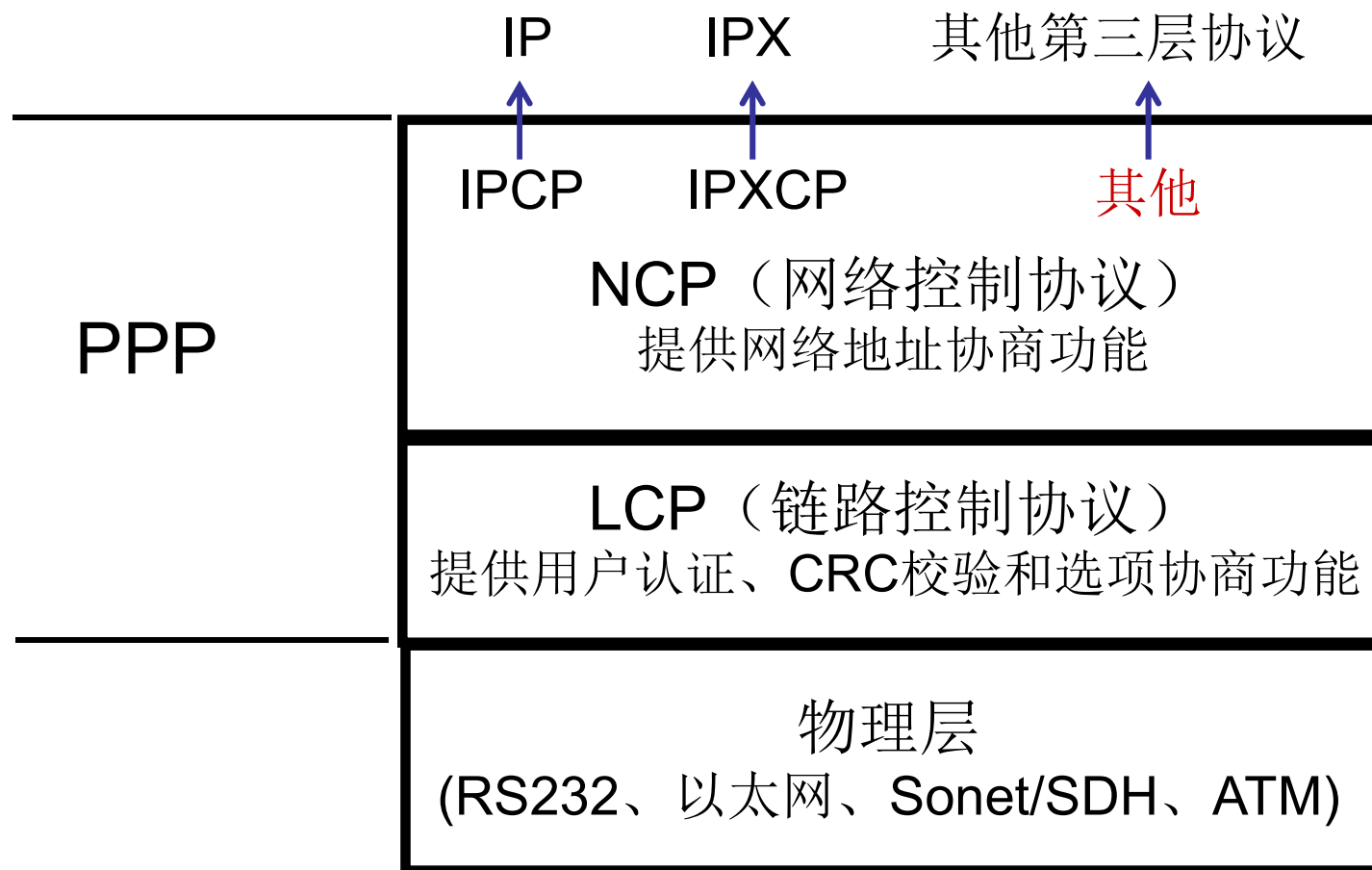


PPP协议的特点

RFC 1661,1662,1663

- ◆ 简单
- ◆ 面向连接
- ◆ 支持多种网络层协议
- ◆ 支持多种类型的物理链路
- ◆ 提供了建立数据链路连接、用户认证、帧头压缩协商等多种能力
- ◆ PPP取消了HDLC的下列功能：
 - 差错恢复（只检错不纠错）
 - 流量控制
 - 序号
 - 点到多点链路

PPP的三个子层

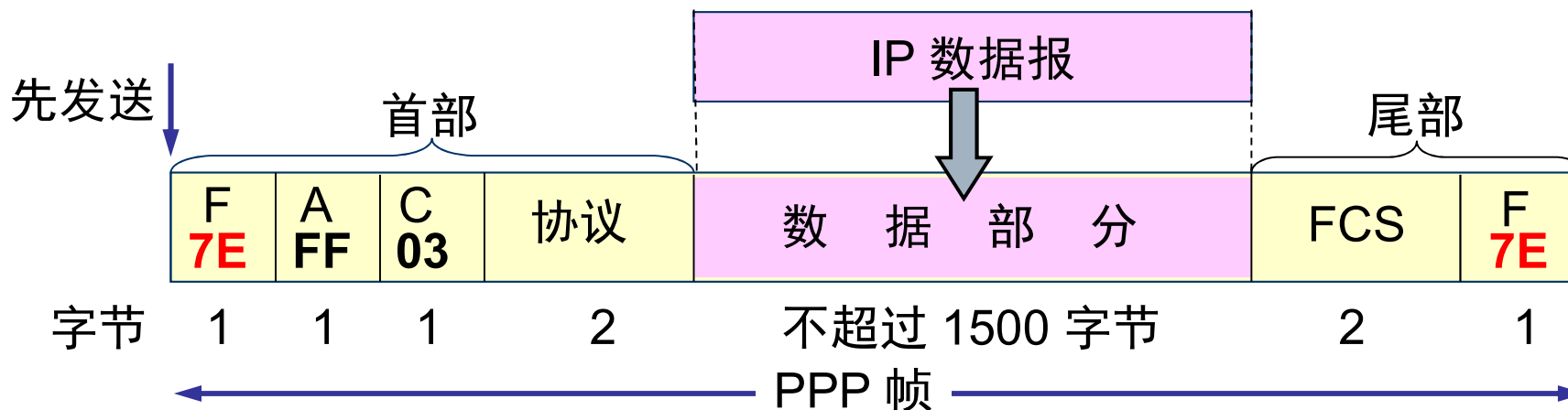


PPPoE: PPP over Ethernet

PPP支持的传输模式

- ◆ 同步传输：以多个字符或多个比特组成的数据块——帧为传输单位，在帧的起始进行同步，使帧内维持固定的时钟
 - 位同步
 - 字节同步
- ◆ 异步传输：以字符作为独立的传输单位，在每个字符的起始处开始对字符内的比特实现同步，但字符与字符之间的间隔时间是不固定的(字符之间是异步)

PPP的帧格式：PPPoE



- ◆ **面向字符**，即整个帧的长度为字节的整数倍
- ◆ **地址**：FF表示任意站点
- ◆ **控制**：03表示无编号帧
- ◆ **协议**：表示数据部分是哪个协议的数据包，例如LCP、NCP、IP、IPX、AppleTalk.....
- ◆ **FCS**：采用CRC-16

PPP的透明传输

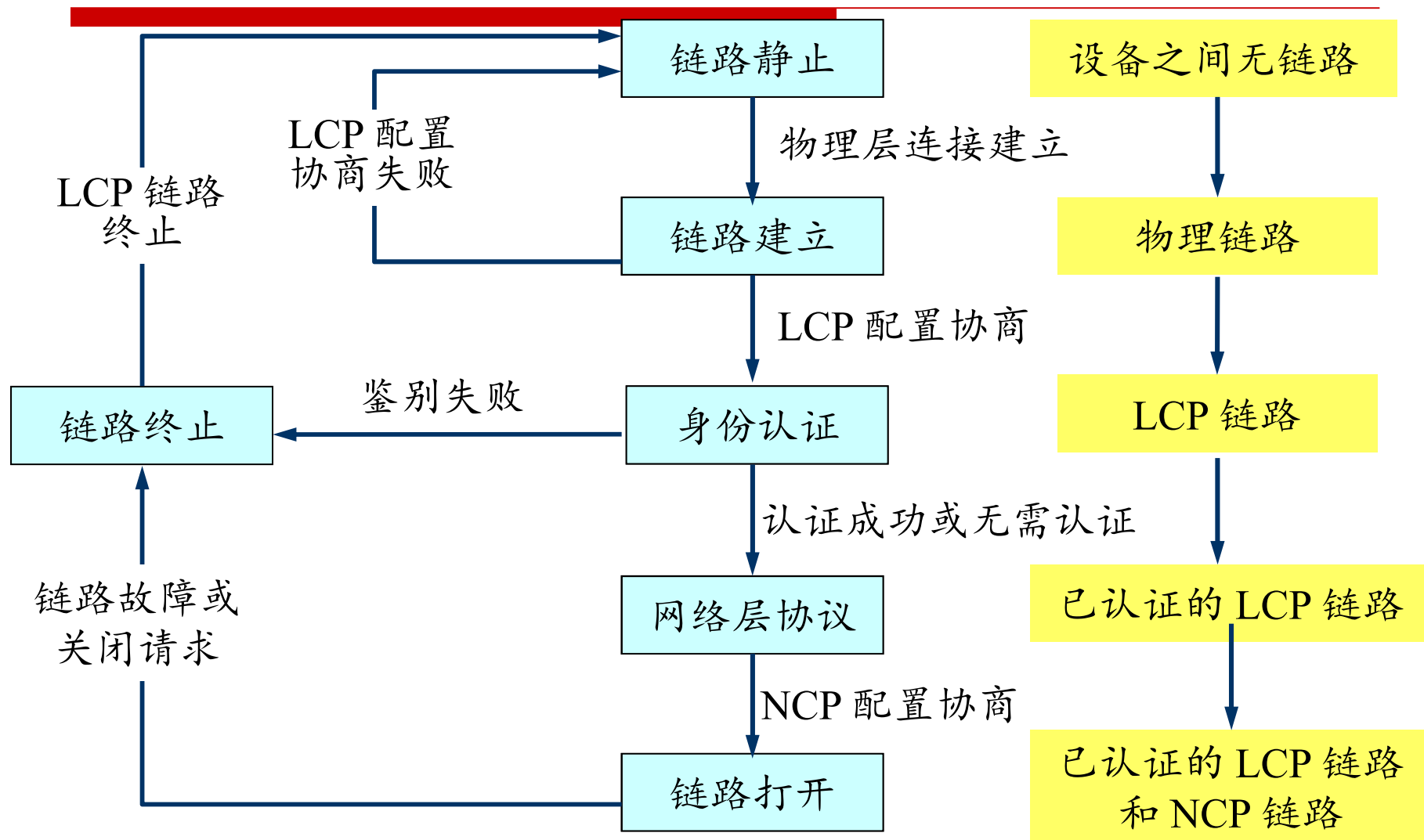
- ◆ 在异步传输模式和字节同步传输模式下，采用字符填充
 - 转义字符：0x7D
 - 0x7E → 0x7D 0x5E
 - 0x7D → 0x7D 0x5D
 - 在ASCII码控制字符($\leq 0x20$)前面也要加上0x7D

- ◆ 在位同步传输模式下，采用零比特填充
 - 用于同步传输的SONET/SDH链路时，在连续的5个“1”比特之后填充一个比特“0”

PPP协议的工作过程：拨号上网

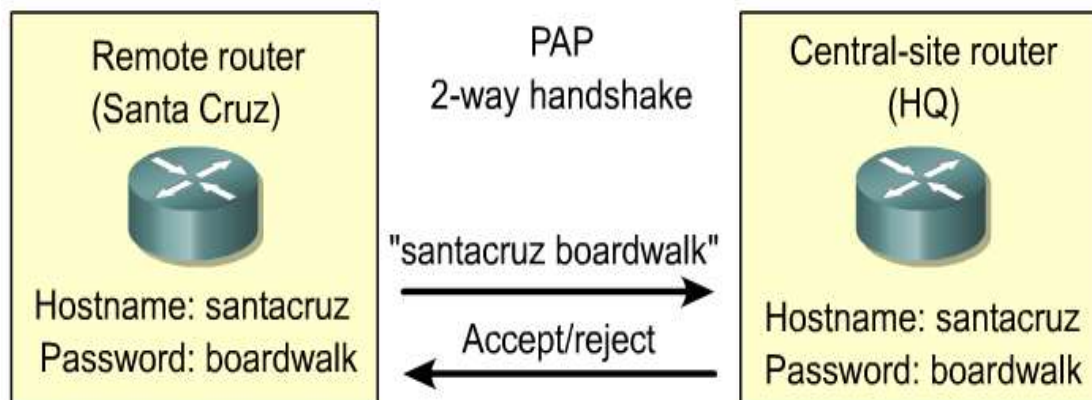
- ◆ 当用户拨号接入ISP时，ISP的路由器（接入服务器）确认并建立一条物理连接
- ◆ 用户计算机向路由器发送多个LCP分组，建立数据链路连接，进行用户认证和MTU、压缩标准等选项协商
- ◆ 使用NCP，为用户计算机分配IP地址，开始网络通信
- ◆ 通信结束后，收回IP地址，释放数据链路连接
- ◆ 释放物理连接

拨号上网时，PPP工作过程



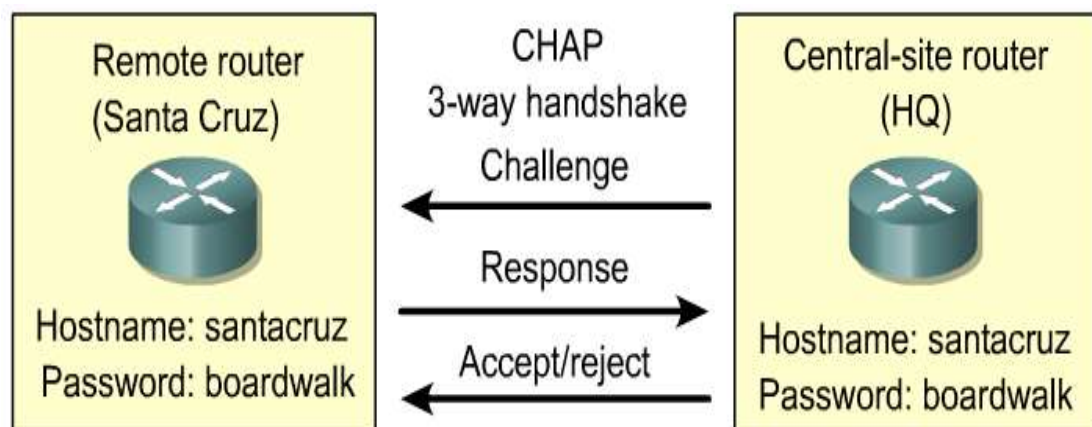
PPP 身份认证: PAP 或 CHAP

PAP: Password Authentication Protocol



- ◆ 密码明文传输
- ◆ 用户控制尝试登录的次数

CHAP: Challenge Handshake Authentication Protocol



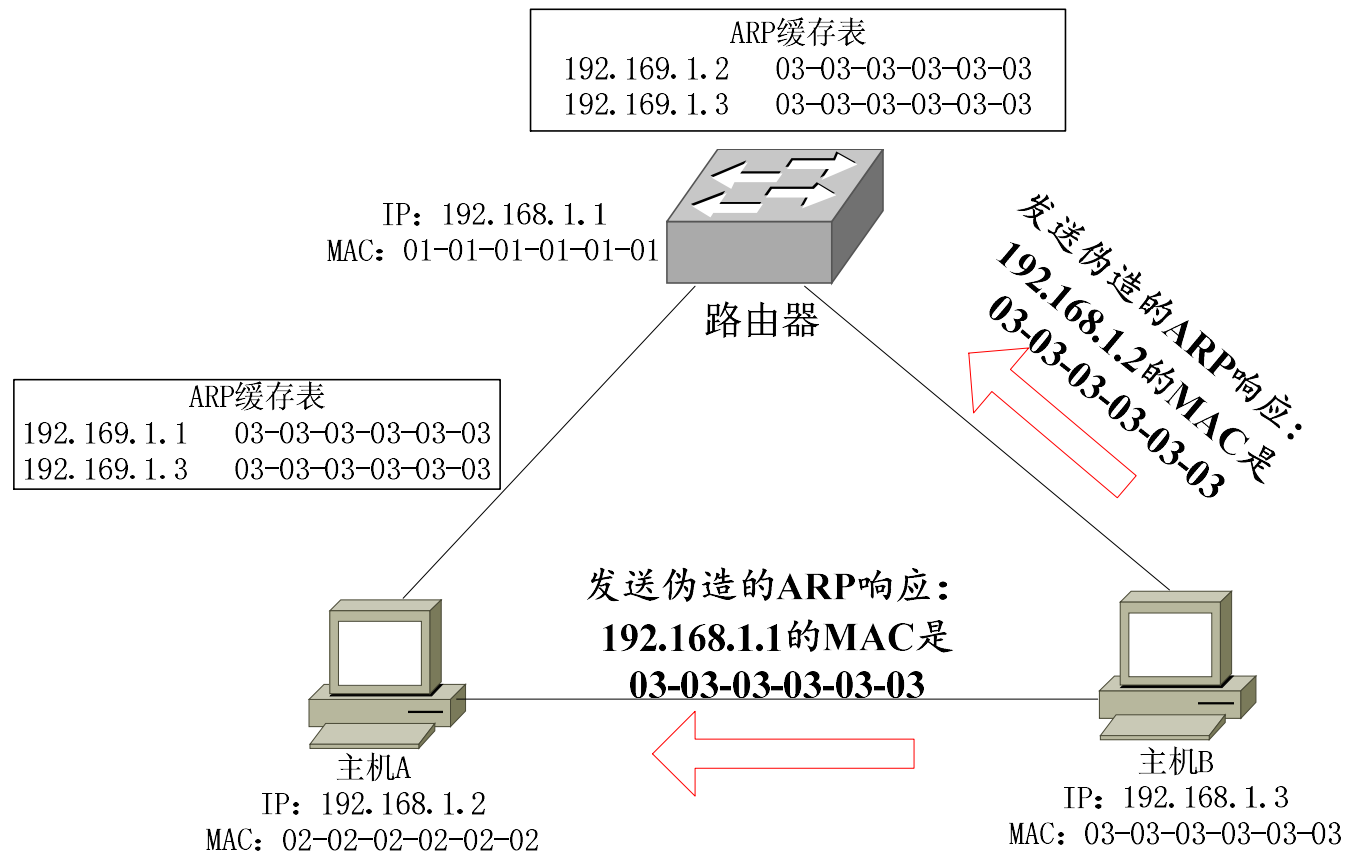
- ◆ ISP 路由器发送 Challenge 消息, 包含一个由 MD5 计算出的值
- ◆ 用户根据 Challenge 值产生响应
- ◆ 密码加密传输
- ◆ 登录次数由 ISP 控制

内容提要

- ◆ 5.1 数据链路层的功能及服务
- ◆ 5.2 数据链路层的成帧原理
- ◆ 5.3 差错检测与纠错技术
- ◆ 5.4 数据链路层的编址
- ◆ 5.5 数据链路层的协议实例
- ◆ 5.6 数据链路层的安全隐患

ARP欺骗

- ◆ 伪造IP地址和MAC地址，发送虚假的ARP请求/响应报文，导致LAN内的其他主机在ARP缓存表中记录错误的信息，从而将IP包发送给假冒主机



MAC地址洪泛攻击

- ◆ 在LAN交换机中，交换机的端口与所连接设备的MAC地址的映射保存在CAM (Content Addressable Memory, 内容寻址存储器)中
- ◆ 收到数据帧时，LAN根据CAM表确定转发的端口
- ◆ MAC地址泛洪攻击又称为CAM表溢出攻击
- ◆ 攻击者向交换机发送大量虚构的具有不同源MAC地址的数据帧，导致交换机的CAM表填满，交换机进入失效开放（fail open）模式，对收到的数据帧进行洪泛式转发
- ◆ 攻击者将截获来自所有其他主机的信息

第五章小结

◆ 数据链路层的功能及服务

◆ 数据链路层的技术要点

- 成帧及透明传输：字符填充、比特填充、物理层编码违例法
- 差错控制：CRC的原理、汉明码的原理
- MAC地址和ARP的功能

◆ 数据链路层协议实例

- HDLC的主要概念
- PPP的应用场合、分层及主要协议、成帧

◆ ARP欺骗和MAC洪泛攻击的概念

版权说明

- ◆ 本讲义中有部分图片来源于下列教材所附讲义：
 - Andrew S. Tanenbaum, Computer Networks, Fourth Edition, 清华大学出版社（影印版），2004，引用时标记为[Tanenbaum];
 - 谢希仁，计算机网络，第五版，电子工业出版社，2008年1月,引用时标记为[谢];
 - Behrouz A. Forouzan, Data Communications and Networking, Fourth Edition, McGraw-Hill Higher Education, 2007年1月，引用时标记为[Forouzan]
 - James F. Kurose, Keith W. Ross著，陈鸣译，计算机网络：自顶向下方方法，机械工业出版社，2009，引用时标记为[Kurose];
 - 部分图片来源于网络，未找到确切来源，引用时标记为[来源于网络]。

本章作业 (1)

◆ Q1-2: 教材p182-183: 5-8, 5-9,

补充题:

◆ Q3: 设要传输的数据是: 0001 0000 0111 1110 1110 1111
1111 1100, (1) 分别写出采用下列方法构成的帧:

(a) 字符计数法;

(b) BISYNC的字符填充法;

(c) 零比特填充法;

(d) RS-232 串行传输: 每个8比特字符前面增加1个起始比特“0”, 后面增加1个停止比特“1”。

(2) 计算上述每种方法的效率 (有效数据量/传输总数据量)

本章作业 (2)

- ◆ Q4: 若要传输一个ASCII字符m(1101101), 采用汉明码进行校验 (假定采用偶校验)
 - (1) 校验信息至少应该为多少比特?
 - (2) 请写出完整的传输码字。
- ◆ Q5: RARP 协议和DHCP/BOOTP协议都是通过MAC地址来获得本主机的IP 地址, 这两个协议有哪些区别?
- ◆ Q6: 在本讲义45页的图中, 主机A要发送一个IP 包给主机B, 假设主机A和路由器的ARP 缓存表均为空, 请写出这个IP 包的传输过程。
- ◆ Q7: 教材p187 5.9.3

本章勘误表(1)

页码	位置	原文	更正
165	标题5.1.2下第4行	事后也不用解释逻辑连接	事后也不用 释放 逻辑连接
166	第4行	识别比特流信息	识别 帧首部 和 帧尾部 信息
169	第1行	奇偶校验只可检查单个错误	奇偶校验只可检查单个 比特 错误
169	第6行	$D(x)=1x_7+0x_6+1x_5+1x_4+0x_3+1x_2+0x+1$	$D(x)=1x^7+0x^6+1x^5+1x^4+0x^3+1x^2+0x+1$
170	标题5.3.2下第9行	若行和列同时出现偶数	若行和列同时出现偶数 个错误
171	第12行	1011进行汉明编码（奇数）	1011进行汉明编码（ 奇校验 ）

本章勘误表(1)

页码	位置	原文	更正
165	标题5.1.2下第4行	事后也不用解释逻辑连接	事后也不用 释放 逻辑连接
166	第4行	识别比特流信息	识别 帧首部 和 帧尾部 信息
169	第1行	奇偶校验只可检查单个错误	奇偶校验只可检查单个 比特 错误
169	第6行	$D(x)=1x_7+0x_6+1x_5+1x_4+0x_3+1x_2+0x+1$	$D(x)=1x^7+0x^6+1x^5+1x^4+0x^3+1x^2+0x+1$
170	标题5.3.2下第9行	若行和列同时出现偶数	若行和列同时出现偶数 个错误
171	第12行	1011进行汉明编码（奇数）	1011进行汉明编码（ 奇校验 ）

本章勘误表(2)

页码	位置	原文	更正
172	图5-9下第1行	广播地址是48个连续1组成的字符串	广播地址是48个连续1 组成的 比特串
172	标题5.4.2下第2行	是获取网络中节点物理地址的一个TCP/IP	是获取网络中节点物理地址的一个TCP/IP 协议
173	第2行	每个接收节点都把该帧的ARP分组传递给它的父节点	每个接收节点都把该帧的ARP分组传递给 网络层
176	第2行	并要求采用拉回方式重发	并要求采用 回退N步（Go-Back-N） 方式重发
176	表5-1中，S类型的“应答”列（第3-6行）	RNR RNR REJ SREJ	删去，S类型帧无应答要求

本章勘误表(3)

页码	位置	原文	更正
176	表5-1中，第4行的“控制字段各位”列	1 0 0 1 P/F N(R)	1 0 1 0 P/F N(R)
176	表5-1中，第5行的“控制字段各位”列	1 0 1 0 P/F N(R)	1 0 0 1 P/F N(R)
177	图5-14	无符号帧	无 编号 帧
177	图5-15		参见本讲义p59-60 图
178	第10行	帧中最大接收单元（MRU） 的默认值为1500字节	帧中最大 传送 单元（ MTU ） 的默认值为1500字节

本章勘误表(4)

页码	位置	原文	更正
179	图5-18下第1行	标志字段F为0x7E（0x表示7E）	标志字段F为0x7E（0x表示 十六进 制 ）
182	第6行	PPP是最常用的面向位的数据 链路层协议	PPP是最常用的 面向字符 的数据 链路层协议