

第 3 章 数据链路层

陈东华

对外经济贸易大学信息学院

复习回顾

1. 物理层的接口有哪几个方面的特性？
2. 给出极限信息传输速率的计算方法，这是_____定义的。
3. 常用的传输媒体有哪几种？各有什么特点？
4. 假定用4 kHz带宽的电话信道传送64 kbit/s的数据（无差错传输），则该信道的信噪比为_____比值（_____分贝）。
5. 假设一种双绞线是0.7dB/km，若允许有20dB的衰减，则该链路工作距离为_____km。

复习回顾（续）

6. 假设给站S分配的码片序列为01011101，给站T分配的码片序列为10111000，这样的分配正确吗？
7. 若收到的码片序列与某一站的码片序列的规格化内积为-1，则该站发送的情况是
- A. 发送了比特1
 - B. 发送了比特0
 - C. 未发送数据
 - D. 以上都不对

第 3 章 数据链路层

3.1 使用点对点信道的数据链路层

3.1.1 数据链路和帧

3.1.2 三个基本问题

3.2 点对点协议 PPP

3.2.1 PPP 协议的特点

3.2.2 PPP 协议的帧格式

3.2.3 PPP 协议的工作状态

第 3 章 数据链路层（续）

3.3 使用广播信道的数据链路层

3.3.1 局域网的数据链路层

3.3.2 CSMA/CD 协议

3.4 使用广播信道的以太网

3.4.1 使用集线器的星形拓扑

3.4.2 以太网的信道利用率

3.4.3 以太网的 MAC 层

第 3 章 数据链路层（续）

3.5 扩展的以太网

3.5.1 在物理层扩展以太网

3.5.2 在数据链路层扩展以太网

3.6 高速以太网

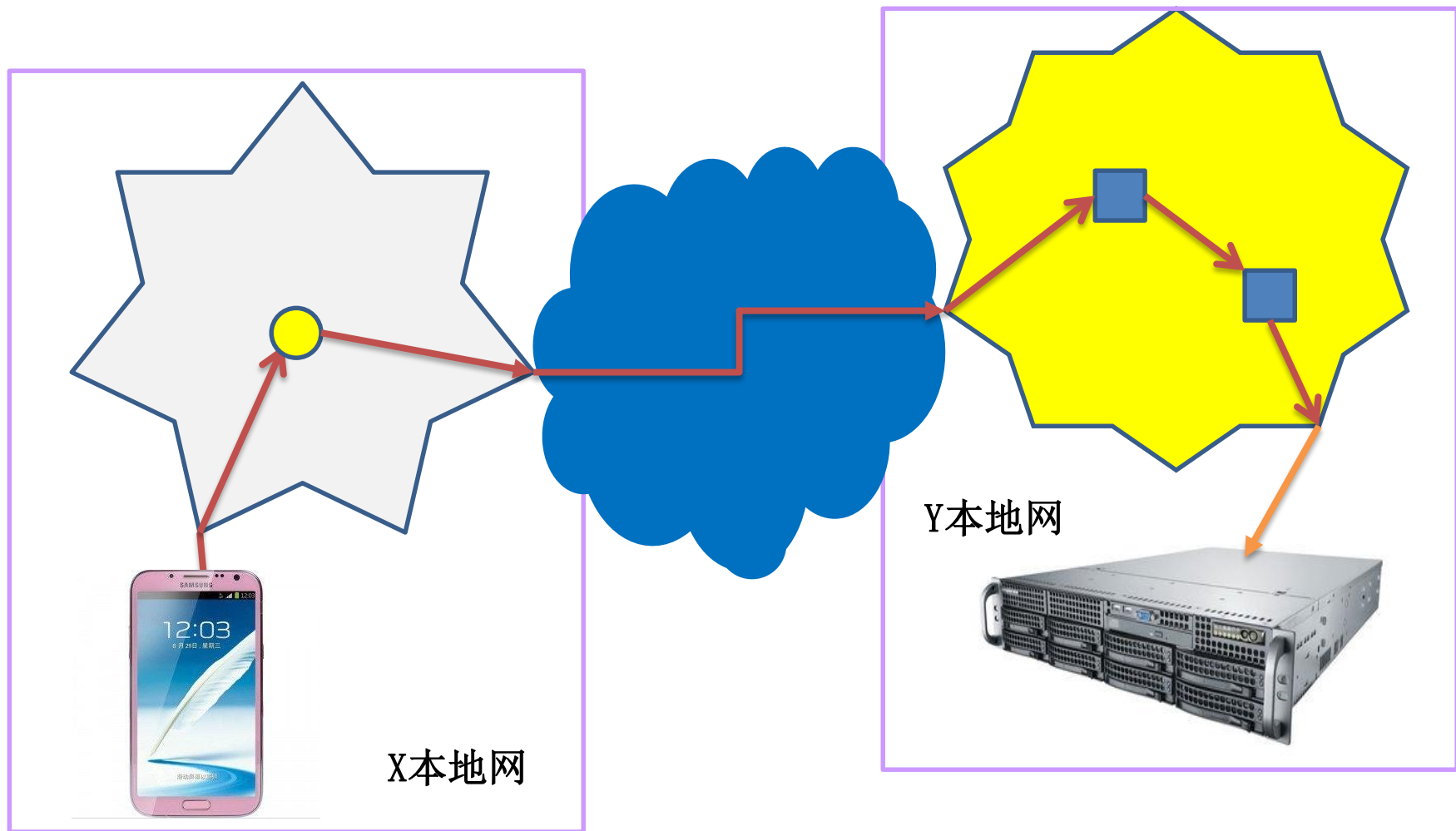
3.6.1 100BASE-T 以太网

3.6.2 吉比特以太网

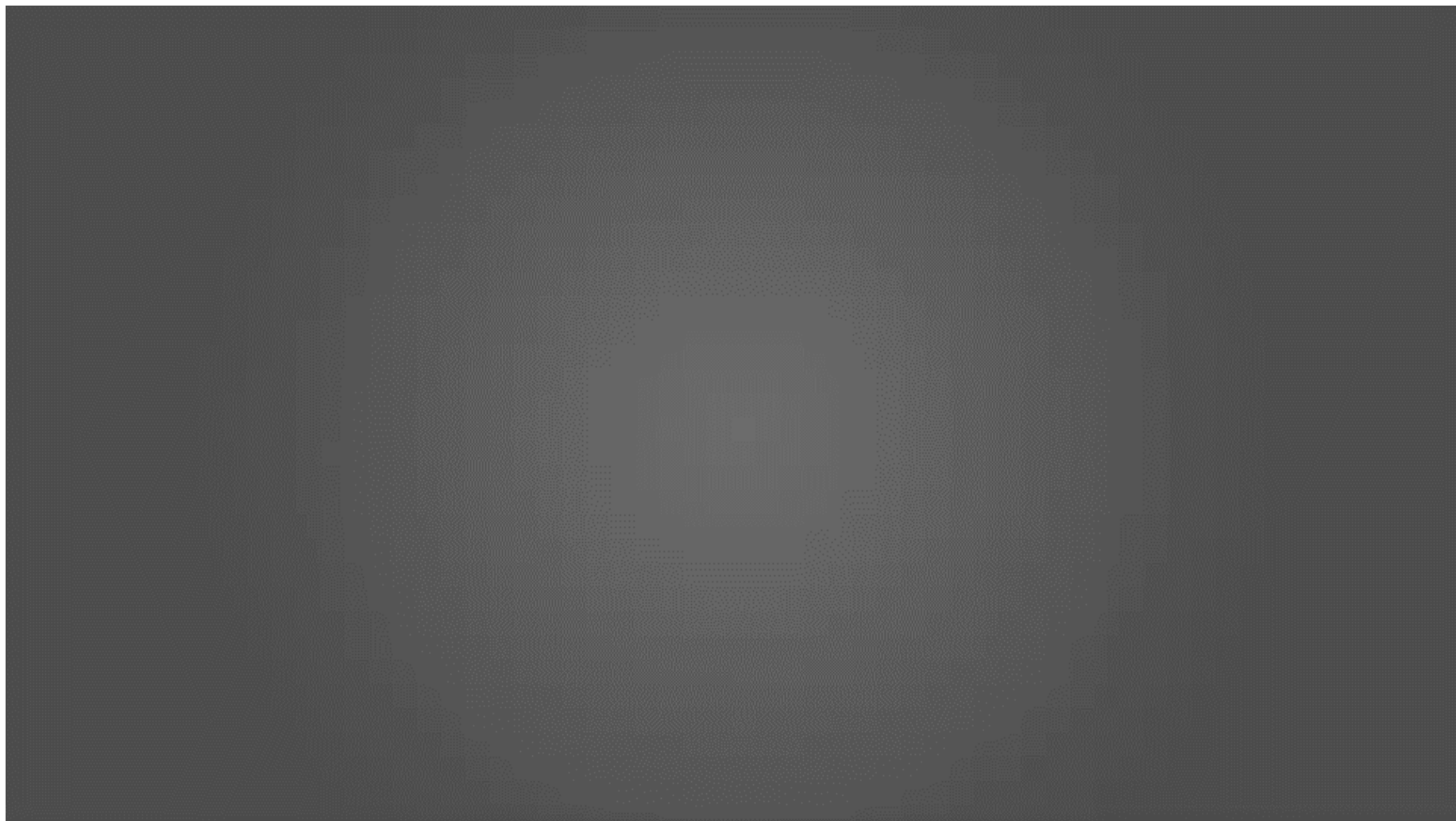
3.6.3 10 吉比特和100吉比特以太网

3.6.4 使用高速以太网进行宽带接入

为什么有数据链路层



思考：为什么有数据链路层



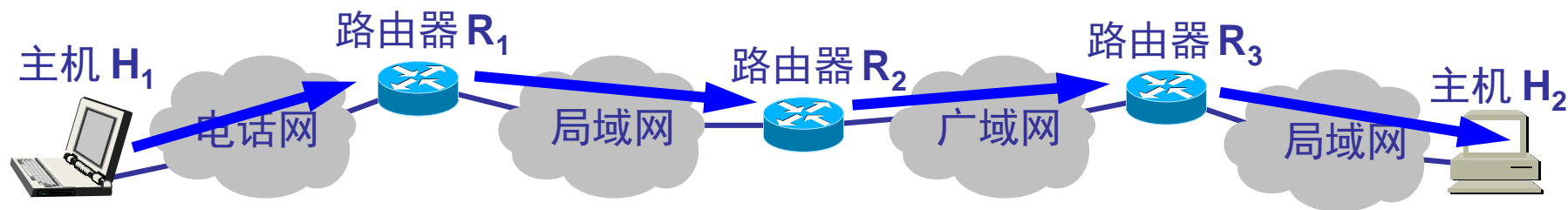
数据链路层

数据链路层使用的信道主要有以下两种类型：

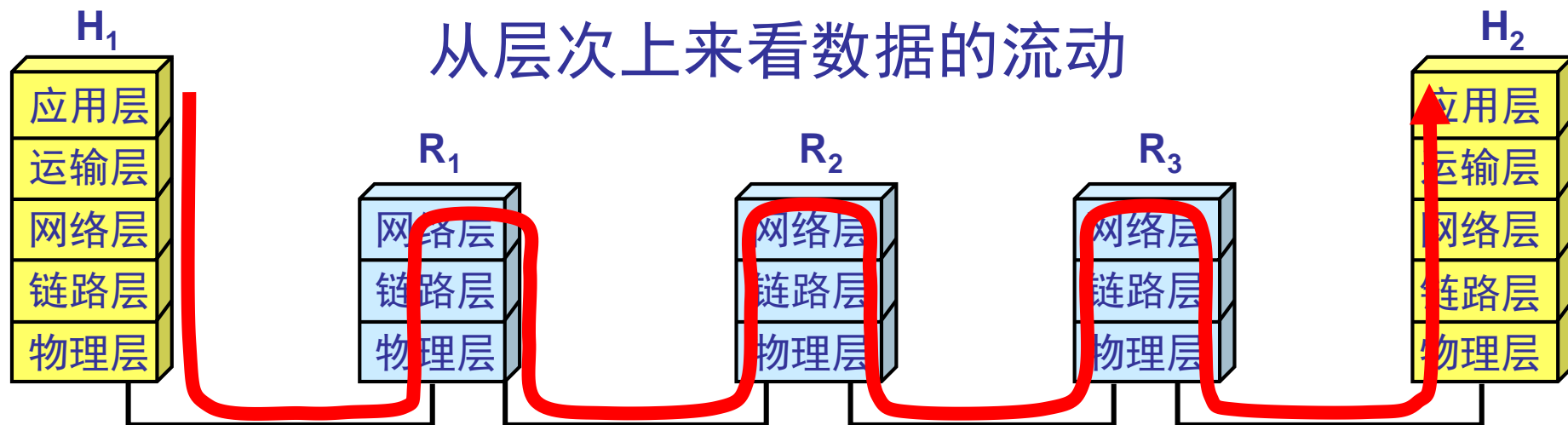
- **点对点信道**。这种信道使用**一对一**的点对点通信方式。
- **广播信道**。这种信道使用**一对多**的广播通信方式，因此过程比较复杂。广播信道上连接的主机很多，因此必须使用**专用的共享信道协议**来协调这些主机的数据发送

数据链路层的简单模型

主机 H_1 向 H_2 发送数据

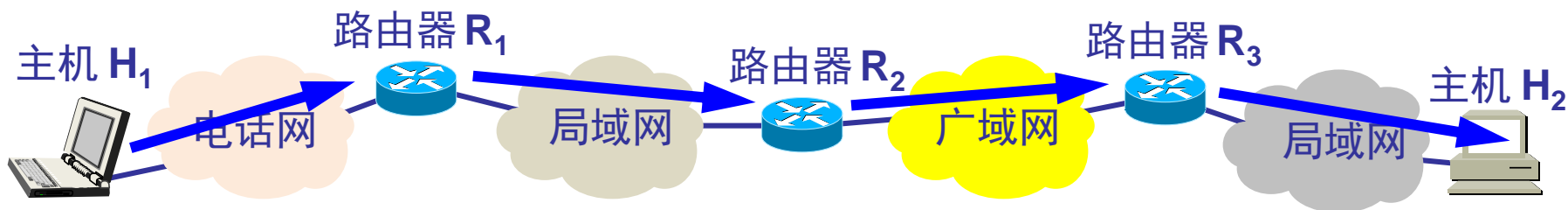


从层次上来看数据的流动

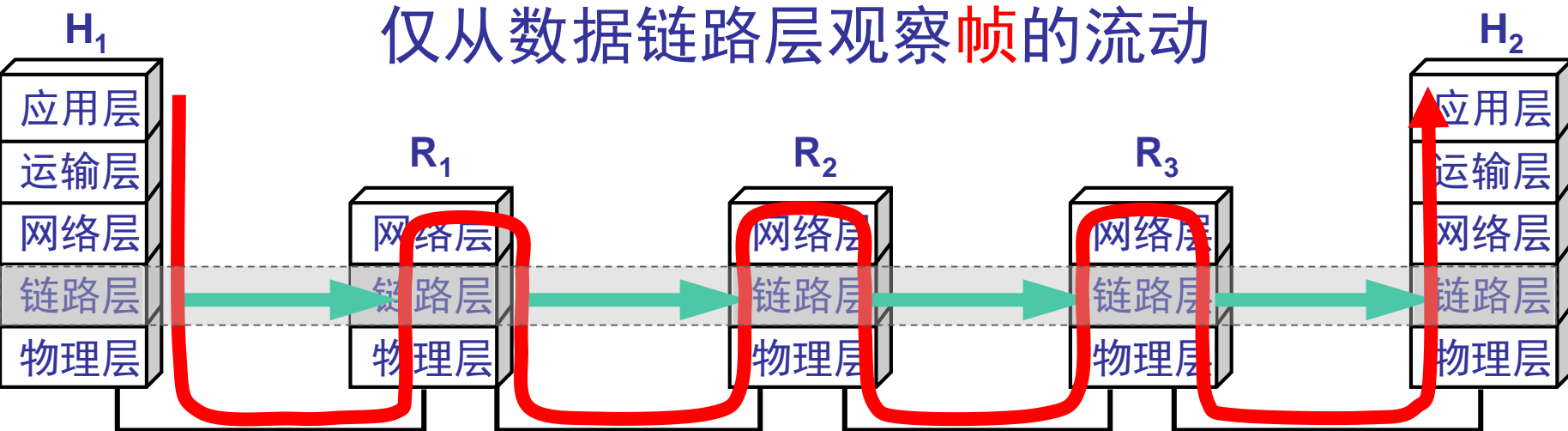


数据链路层的简单模型（续）

主机 H_1 向 H_2 发送数据



仅从数据链路层观察帧的流动

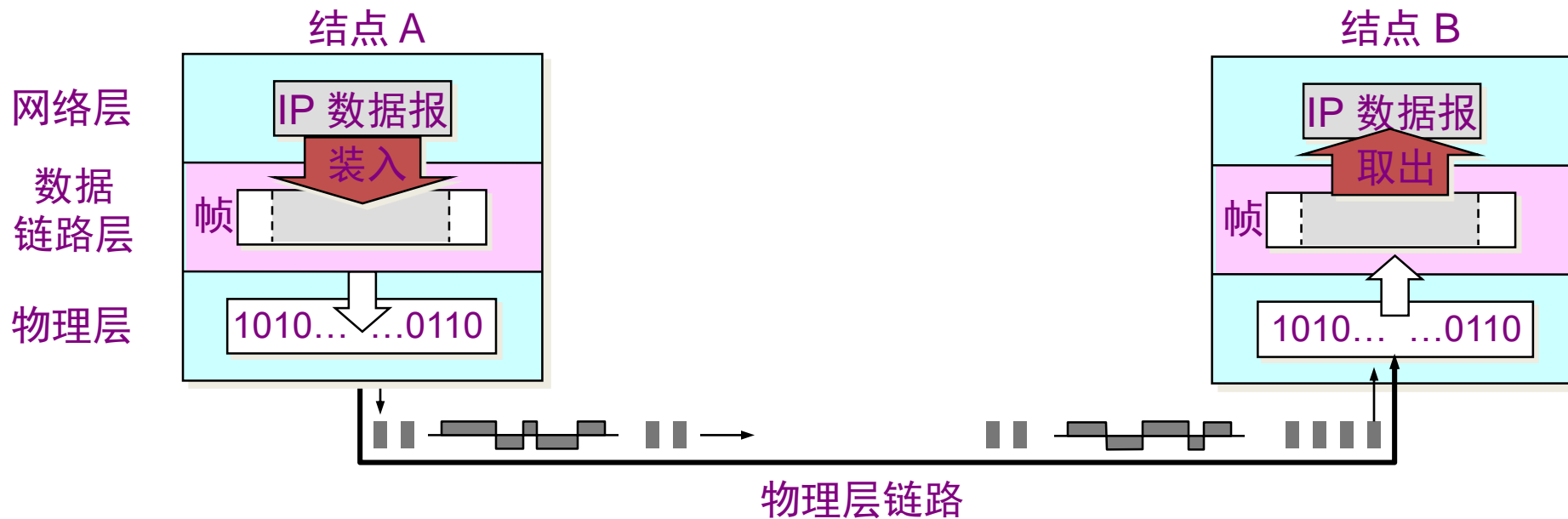


3.1 使用点对点信道的数据链路层

3.1.1 数据链路和帧

- **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。
 - 一条链路**只是一条通路的一个组成部分**。
- **数据链路** (data link) 除物理线路外，必须有**通信协议**来控制这些数据的传输。实现这些协议的硬件和软件加到链路上，就构成了数据链路。
 - 现在最常用的方法是使用**适配器**来实现这些协议的硬件和软件。
 - 一般的适配器都包括了**数据链路层和物理层**这两层的功能。

数据链路层传送的是帧



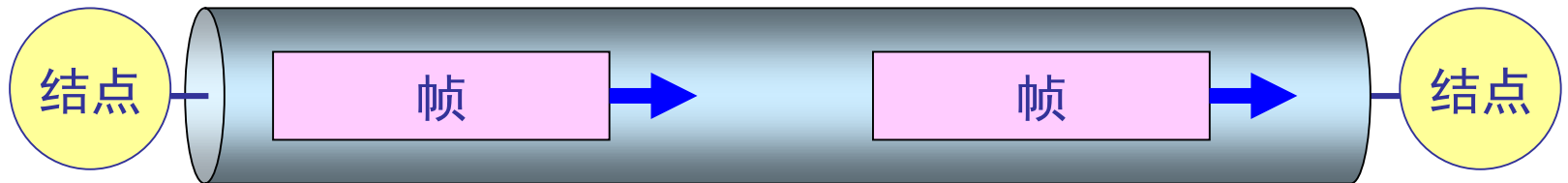
(a)



(b)

数据链路层像个数字管道

- 常在两个对等的的数据链路层之间画出一个数字管道，而在这条数字管道上传输的数据单位是帧。

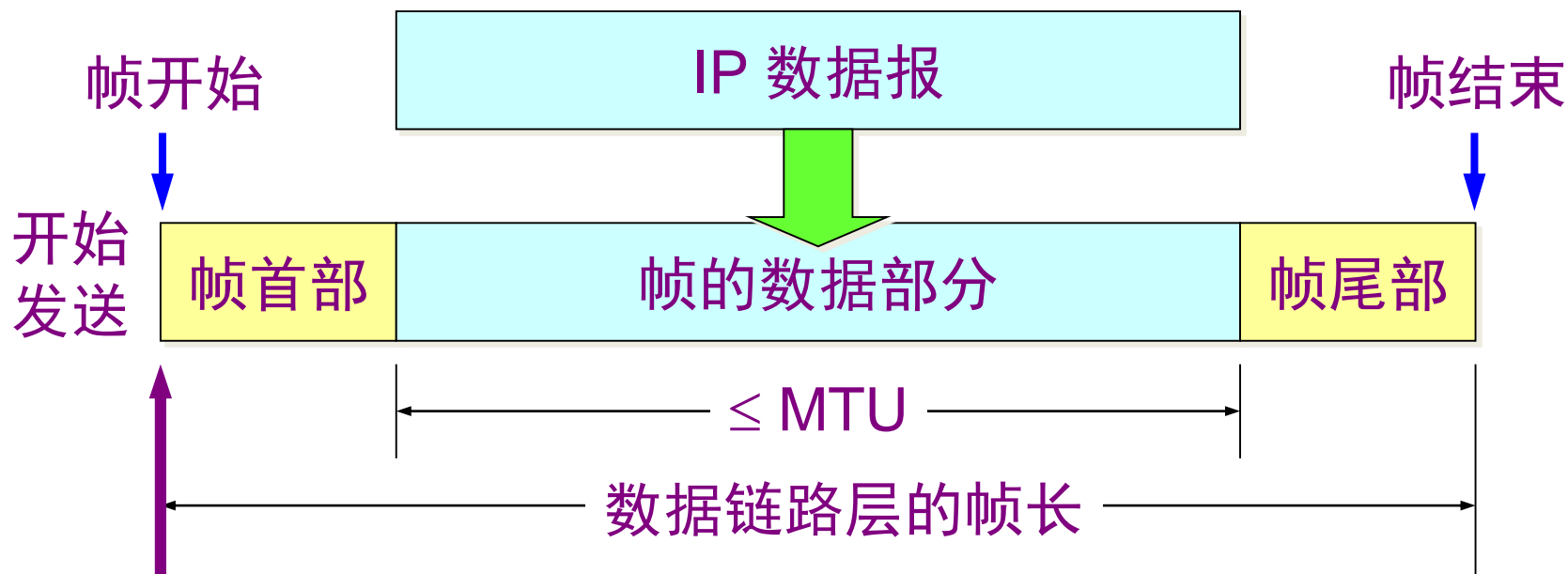


3.1.2 三个基本问题

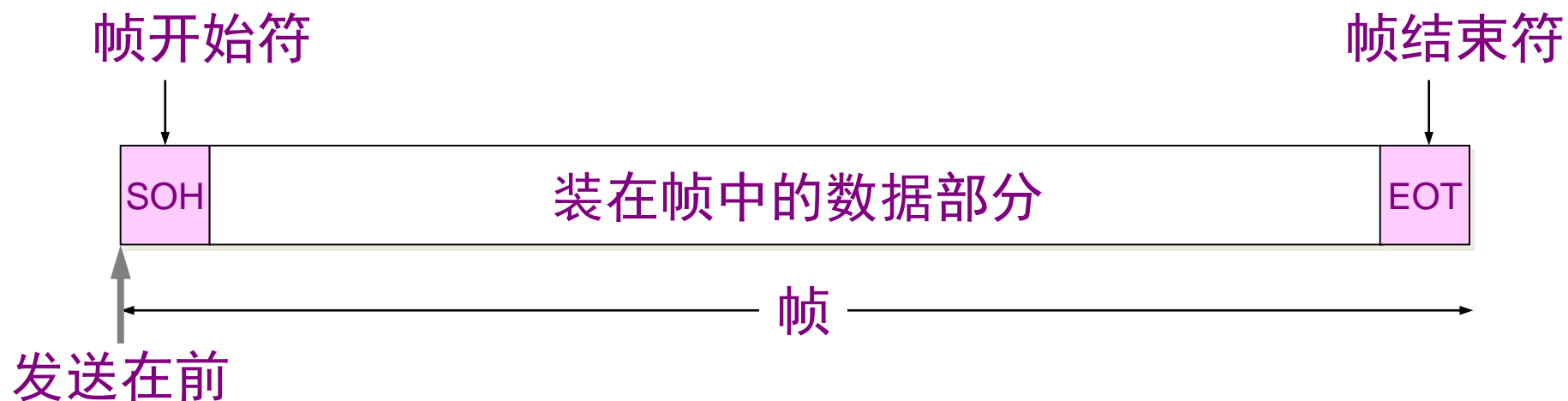
- (1) 封装成帧
- (2) 透明传输
- (3) 差错控制

1. 封装成帧

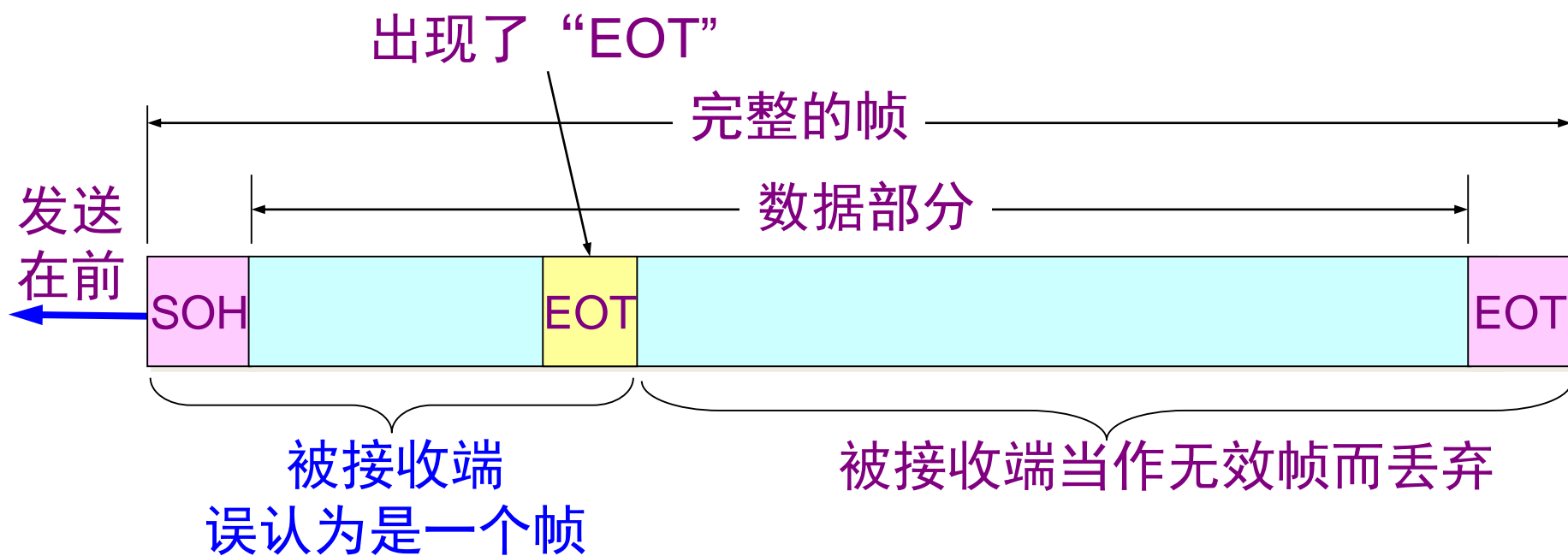
- 封装成帧 (framing) 就是在一段数据的前后分别添加首部和尾部，然后就构成了一个帧。确定帧的界限。
- 首部和尾部的一个重要作用就是进行帧定界。



用控制字符进行帧定界的方法举例



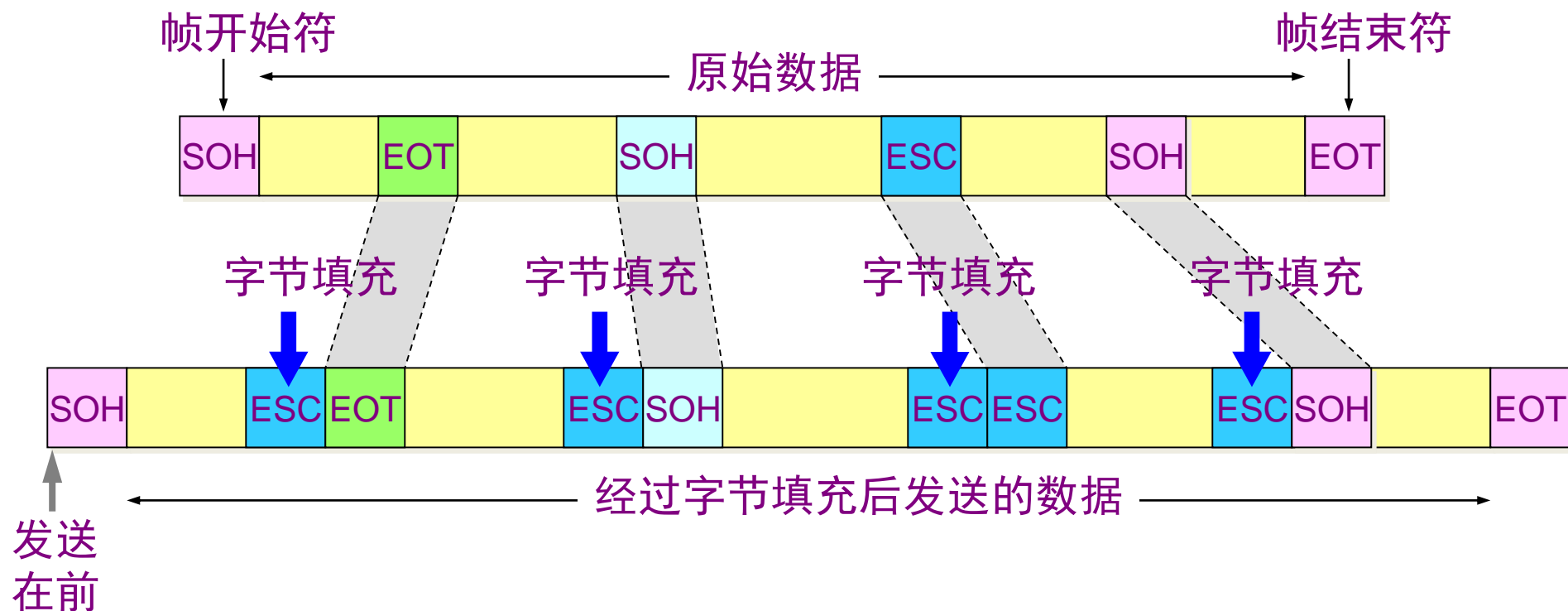
2. 透明传输



解决透明传输问题

- 发送端的数据链路层在数据中出现控制字符“SOH”或“EOT”的前面插入一个转义字符“ESC”(其十六进制编码是 1B)。
- **字节填充**(byte stuffing)或**字符填充**(character stuffing)——接收端的数据链路层在将数据送往网络层之前删除插入的转义字符。
- 如果转义字符也出现数据当中，那么应在转义字符前面插入一个转义字符。当接收端收到连续的两个转义字符时，就删除其中前面的一个。

用字节填充法解决透明传输的问题



3. 差错检测

- 在传输过程中可能会产生比特差错：1 可能会变成 0 而 0 也可能变成 1。
- 在一段时间内，传输错误的比特占所传输比特总数的比率称为误码率 BER (Bit Error Rate)。
- 误码率与信噪比有很大的关系。
- 为了保证数据传输的可靠性，在计算机网络传输数据时，必须采用各种差错检测措施。

循环冗余检验的原理

- 在数据链路层传送的帧中，广泛使用了循环冗余检验 CRC 的检错技术。
- 在发送端，先把数据划分为组。假定每组 k 个比特。
- 假设待传送的一组数据 $M = 101001$ （现在 $k = 6$ ）。我们在 M 的后面再添加供差错检测用的 n 位冗余码一起发送。

冗余码的计算

1. 根据除数 P ，在被除数（要发送的数据）的尾部补 $P-1$ 位0
2. 除数由生成多项式得出（一会儿会讲）
3. 用补零之后的被除数除以除数（其实是取模运算，不借位！！！！）
4. 取模所得的余数就是冗余码，余数的位数也要等于 $P-1$ 位，不足向前取0

冗余码的计算举例

- 现在 $k = 6$, $M = 101001$ 。
- 设 $n = 3$, 除数 $P = 1101$,
- 被除数是 $2^n M = 101001000$ 。
- 模 2 运算的结果是：商 $Q = 110101$,
余数 $R = 001$ 。
- 把余数 R 作为冗余码添加在数据 M 的后面发送出去。
发送的数据是： $2^n M + R$
即： 101001001 , 共 $(k + n)$ 位。

循环冗余检验的原理说明

$$\begin{array}{r} \text{P (除数)} \rightarrow 1101 \overline{) 101001000} \leftarrow 2^n M \text{ (被除数)} \\ \underline{1101} \\ 1110 \\ \underline{1101} \\ 0111 \\ \underline{0000} \\ 1110 \\ \underline{1101} \\ 0110 \\ \underline{0000} \\ 1100 \\ \underline{1101} \\ 001 \leftarrow R \text{ (余数), 作为 FCS} \end{array}$$

帧检验序列 FCS

- 在数据后面添加上的冗余码称为帧检验序列 FCS (Frame Check Sequence)。
- 循环冗余检验 CRC 和帧检验序列 FCS 并不等同。
 - CRC 是一种常用的检错方法，而 FCS 是添加在数据后面的冗余码。
 - FCS 可以用 CRC 这种方法得出，但 CRC 并非用来获得 FCS 的唯一方法。

接收端对收到的每一帧进行 CRC 检验

- (1) 若得出的余数 $R = 0$ ，则判定这个帧没有差错，就接受 (accept)。
- (2) 若余数 $R \neq 0$ ，则判定这个帧有差错，就丢弃。
- 但这种检测方法并不能确定究竟是哪一个或哪几个比特出现了差错。
- 只要经过严格的挑选，并使用位数足够多的除数 P ，那么出现检测不到的差错的概率就很小很小。

CRC应用

名称	生成多项式	简记式*	应用举例
CRC-4	x^4+x+1	3	ITU G.704
CRC-8	$x^8+x^5+x^4+1$	31	DS18B20
CRC-12	$x^{12}+x^{11}+x^3+x+1$	5E	
CRC-16	$x^{16}+x^{15}+x^2+1$	8005	IBM SDLC
CRC-ITU**	$x^{16}+x^{12}+x^5+1$	1021	ISO HDLC, ITU X.25, V.34/V.41/V.42, PPP-FCS
CRC-32	$x^{32}+x^{26}+x^{23}+...+x^2+x+1$	04C11DB7	ZIP, RAR, IEEE 802 LAN/FDDI, IEEE 1394, PPP-FCS
CRC-32c	$x^{32}+x^{28}+x^{27}+...+x^8+x^6+1$	1EDC6F41	SCTP

应当注意

- 仅用循环冗余检验 CRC 差错检测技术只能做到无差错**接受** (accept)。
- “无差错接受”是指：“凡是接受的帧（即**不包括丢弃的帧**），以非常接近于 1 的概率认为这些帧在传输过程中没有产生差错”。或说：“凡是接收端数据链路层接受的帧都没有传输差错”（有差错的帧丢弃而不接受）。
- 做到“**可靠传输**”（即发送什么就收到什么）就必须再加上**确认**和**重传**机制。

提醒

- 旧的提法：数据链路层可以把一条有可能出差错的实际链路，转变成为了让网络层向下看起来好像是一条不出差错的链路。
- 新的提法：数据链路层的传输**不能**让网络层向下看起来好像是一条不出差错的链路。
- 答：原来基于OSI体系结构的。OSI体系结构的数据链路层采用的是面向连接的HDLC协议，它提供可靠传输的服务。旧式的提法对OSI体系结构是正确的。
- 因特网的数据链路层协议使用最多的是PPP协议和CSMA/CD协议（这种情况就是使用拨号入网或使用以太网入网）。不使用序号和确认机制，因此不能“让网络层向下看起来好像是一条不出差错的链路。”

- 当接收端通过差错检测发现了帧在传输中出了差错，大多数情况是默默丢弃(silently discard)而不进行任何其他处理（当使用PPP协议或CSMA/CD协议时）
- 或者使用重传机制要求发送方重传（当使用HDLC协议时），但这种情况现在很少使用。
- 如果需要可靠传输，那么就由高层的TCP协议负责重传。但数据链路层并不知道这是重传的帧。

习题

1. 数据链路指的是
 - A. 从一个结点到相邻结点的一段物理线路，而中间没有任何其他的交换结点。
 - B. 一条物理线路以及一些必要的通信协议来控制数据的传输。

2. 链路控制的三个主要功能是1) _____； 2) _____； 3) _____。

3. 上层交下来的数据，不管是什么形式的比特组合，都必须能够正确传送。这是指数据链路层的哪个基本问题？
 - A. 封装成帧
 - B. 透明传输
 - C. 差错检测

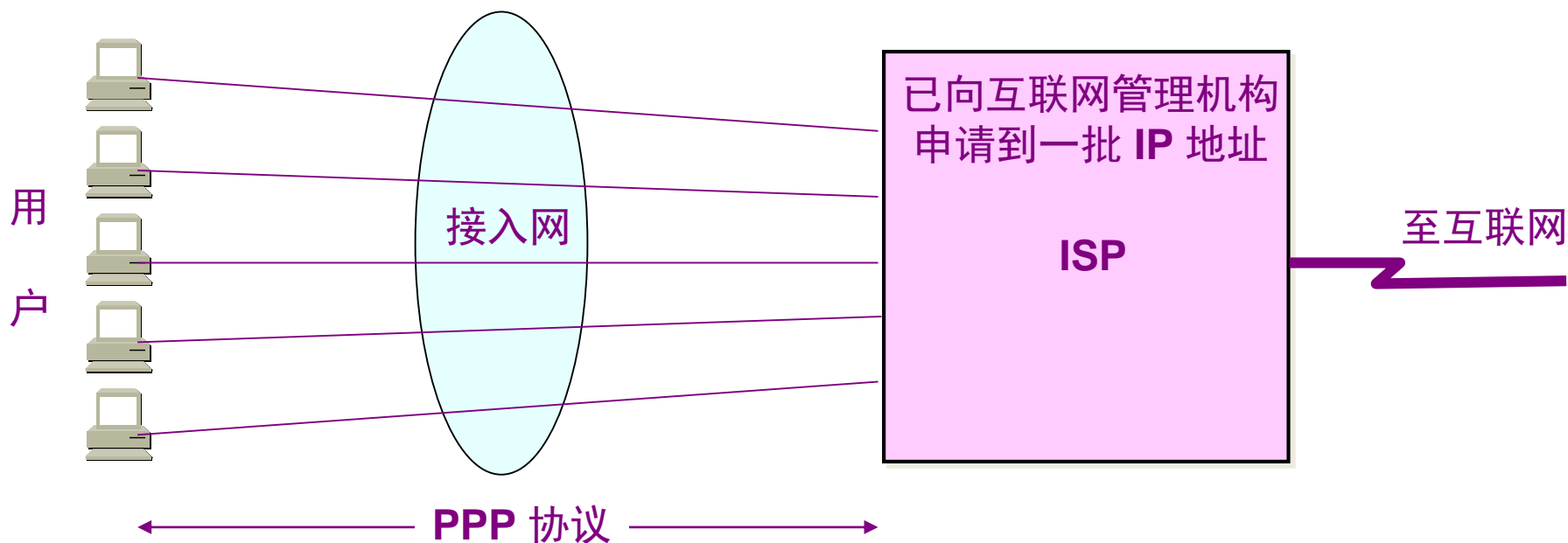
4. 使用CRC检验后，数据链路层传输变成了可靠传输。【判断】

3.2 点对点协议 PPP


1. PPP 协议的特点

- 现在全世界使用得最多的数据链路层协议是点对点协议 PPP (Point-to-Point Protocol)。
- 用户使用拨号电话线接入互联网时，一般都是使用 PPP 协议。

用户到 ISP 的链路使用 PPP 协议



理解PPP协议



Understanding
Point-to-Point
Protocols

1. PPP 协议应满足的需求

- 简单
- 封装成帧
- 透明性
- 多种网络层协议
- 多种类型链路
- 差错检测
- 检测连接状态
- 最大传送单元
- 网络层地址协商
- 数据压缩协商

2. PPP 协议不需要的功能

- 纠错
- 流量控制
- 序号和确认机制
- 多点线路
- 半双工或单工链路

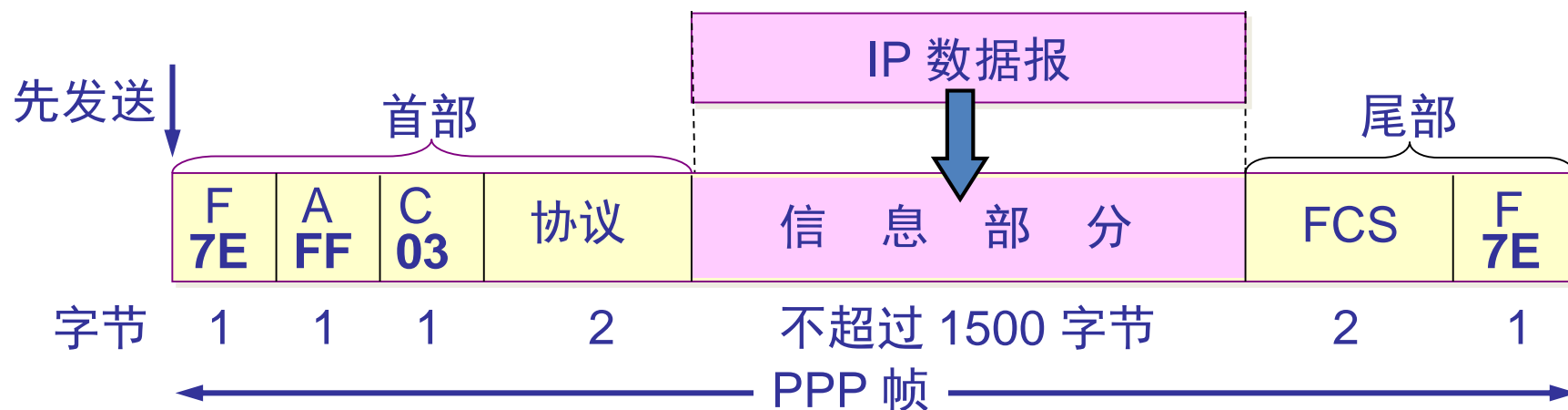
3. PPP 协议的组成

- 1992 年制订了 PPP 协议。经过 1993 年和 1994 年的修订，现在的 PPP 协议已成为互联网的正式标准[RFC 1661]。
- PPP 协议有三个组成部分
 - 一个将 IP 数据报封装到串行链路的方法。
 - 链路控制协议 LCP (Link Control Protocol)。
 - 网络控制协议 NCP (Network Control Protocol)。

2 PPP 协议的帧格式

- 标志字段 F = 0x7E （符号“0x”表示后面的字符是用十六进制表示。十六进制的 7E 的二进制表示是 01111110）。
- 地址字段 A 只置为 0xFF。地址字段实际上并不起作用。
- 控制字段 C 通常置为 0x03。
- PPP 是面向字节的，所有的 PPP 帧的长度都是整数字节。

PPP 协议的帧格式



- PPP 有一个 2 个字节的协议字段。
 - 若为 0x0021 时, PPP 帧的信息字段是 IP 数据报。
 - 若为 0xC021, 则信息字段是 PPP 链路控制数据。
 - 若为 0x8021, 则表示这是网络控制数据。

透明传输问题

- 当 PPP 用在同步传输链路时，协议规定采用硬件来完成比特填充（和 HDLC 的做法一样）。
- 当 PPP 用在异步传输时，使用一种特殊的字符填充法。

字符填充

- 将信息字段中出现的每一个 0x7E 字节转变成成为 2 字节序列(0x7D, 0x5E)。
- 若信息字段中出现一个 0x7D 的字节, 则将其转变成成为 2 字节序列(0x7D, 0x5D)。
- 若信息字段中出现 ASCII 码的控制字符 (即数值小于 0x20 的字符), 则在该字符前面要加入一个 0x7D 字节, 同时将该字符的编码加以改变。

零比特填充

- PPP 协议用在 SONET/SDH 链路时，使用同步传输（一连串的比特连续传送）。
- PPP 协议采用零比特填充方法来实现透明传输。
 - 在发送端，只要发现有 5 个连续 1，则立即填入一个 0。
 - 接收端对帧中的比特流进行扫描。每当发现 5 个连续1时，就把这 5 个连续 1 后的一个 0 删除。

零比特填充

信息字段中出现了和
标志字段 F 完全一样
的 8 比特组合

0 1 0 0 1 1 1 1 1 0 0 0 1 0 1 0
会被误认为是标志字段 F

发送端在 5 个连 1 之后
填入 0 比特再发送出去

0 1 0 0 1 1 1 1 1 0 1 0 0 0 1 0 1 0
发送端填入 0 比特

在接收端把 5 个连 1
之后的 0 比特删除

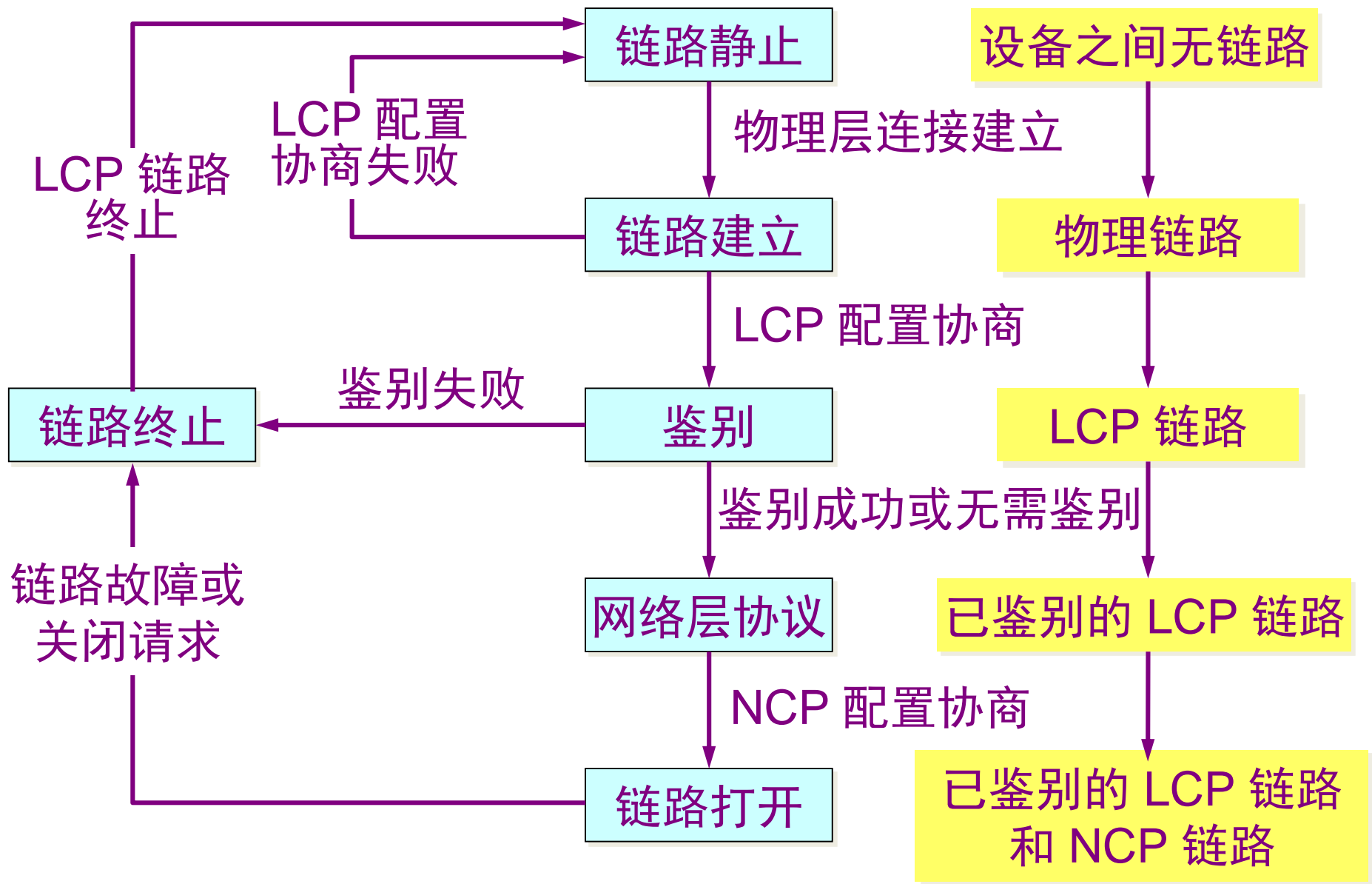
0 1 0 0 1 1 1 1 1 0 1 0 0 0 1 0 1 0
接收端删除填入的 0 比特

不提供使用序号和确认的可靠传输

- PPP 协议之所以不使用序号和确认机制是出于以下的考虑：
 - 在数据链路层出现差错的概率不大时，使用比较简单的 PPP 协议较为合理。
 - 在互联网环境下，PPP 的信息字段放入的数据是 IP 数据报。数据链路层的可靠传输并不能够保证网络层的传输也是可靠的。
 - 帧检验序列 FCS 字段可保证无差错接受。

3 PPP 协议的工作状态

- 拨号接入 ISP 时，ISP 中路由器的调制解调器对拨号做出确认，并建立一条物理连接。
- PC 机向路由器发送一系列的 LCP 分组（封装成多个 PPP 帧）。
- 这些分组及响应选择 PPP 参数，并进行网络层配置，NCP 给新接入的 PC 机分配一个临时的 IP 地址。
- 通信完毕，NCP 释放网络层连接，收回原来分配出去的 IP 地址。
- LCP 释放数据链路层连接。
- 最后释放物理层的连接。



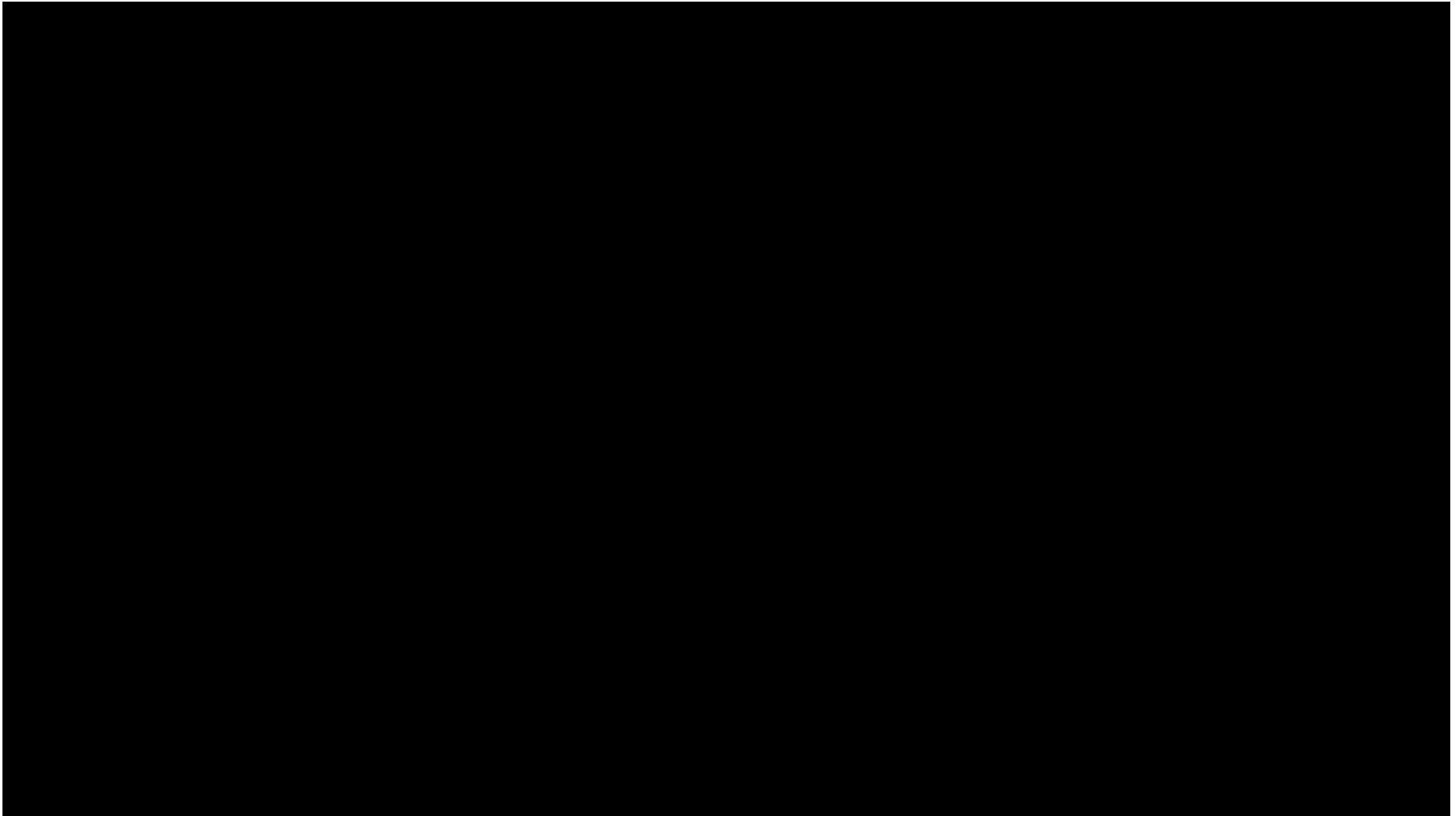
3.3 使用广播信道的数据链路层

3.3.1 局域网的数据链路层

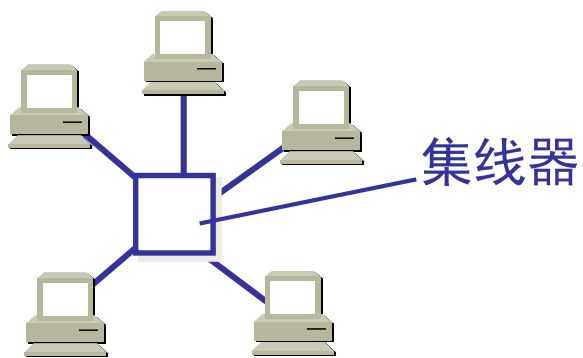
- 局域网最主要的特点是：网络为一个单位所拥有，且地理范围和站点数目均有限。
- 局域网具有如下的一些主要优点：
 - 具有广播功能，从一个站点可很方便地访问全网。局域网上的主机可共享连接在局域网上的各种硬件和软件资源。
 - 便于系统的扩展和逐渐地演变，各设备的位置可灵活调整和改变。
 - 提高了系统的可靠性、可用性和生存性。

3.3 使用广播信道的数据链路层

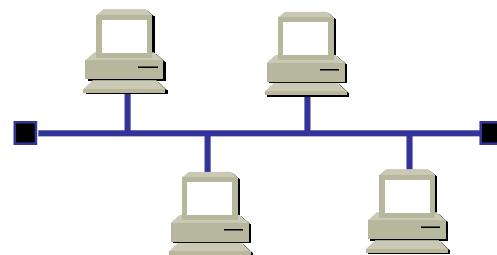
3.3.1 局域网的数据链路层



局域网的拓扑

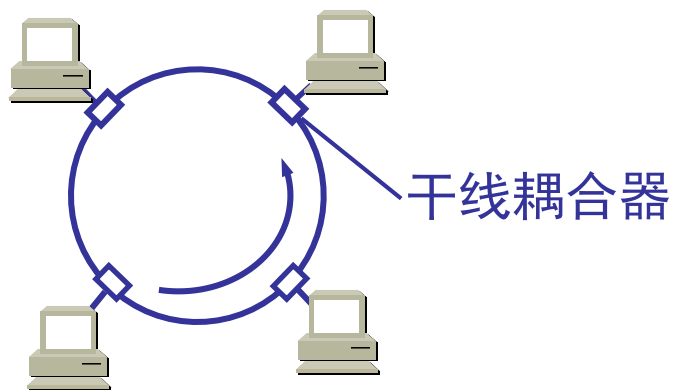


星形网

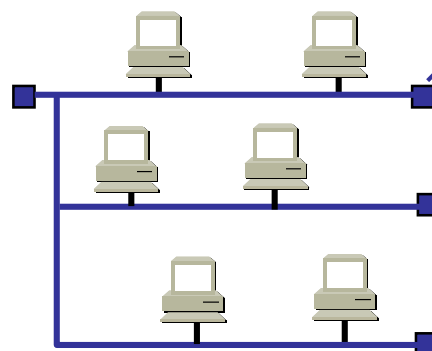


总线网

匹配电阻

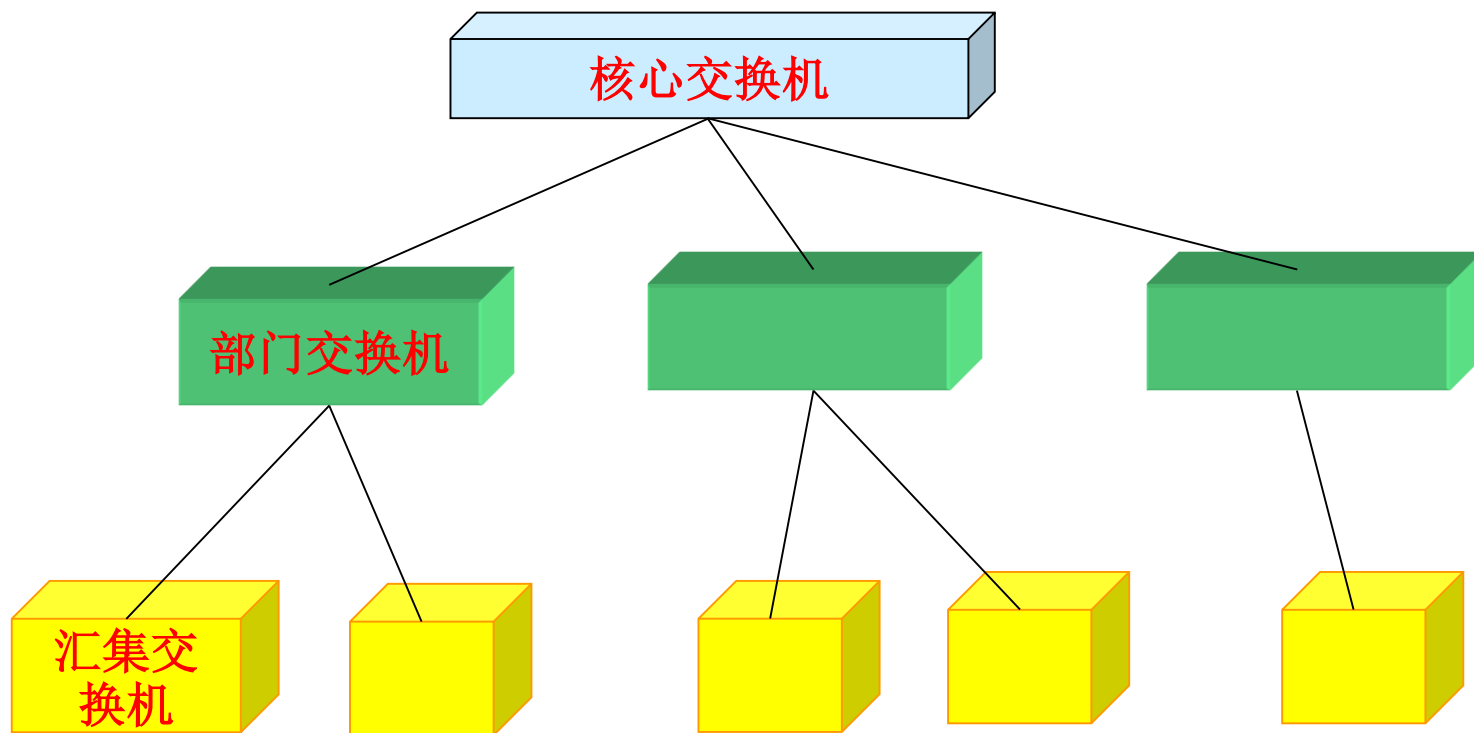


环形网



树形网

树型结构



媒体共享技术

- 静态划分信道

- 频分复用
- 时分复用
- 波分复用
- 码分复用

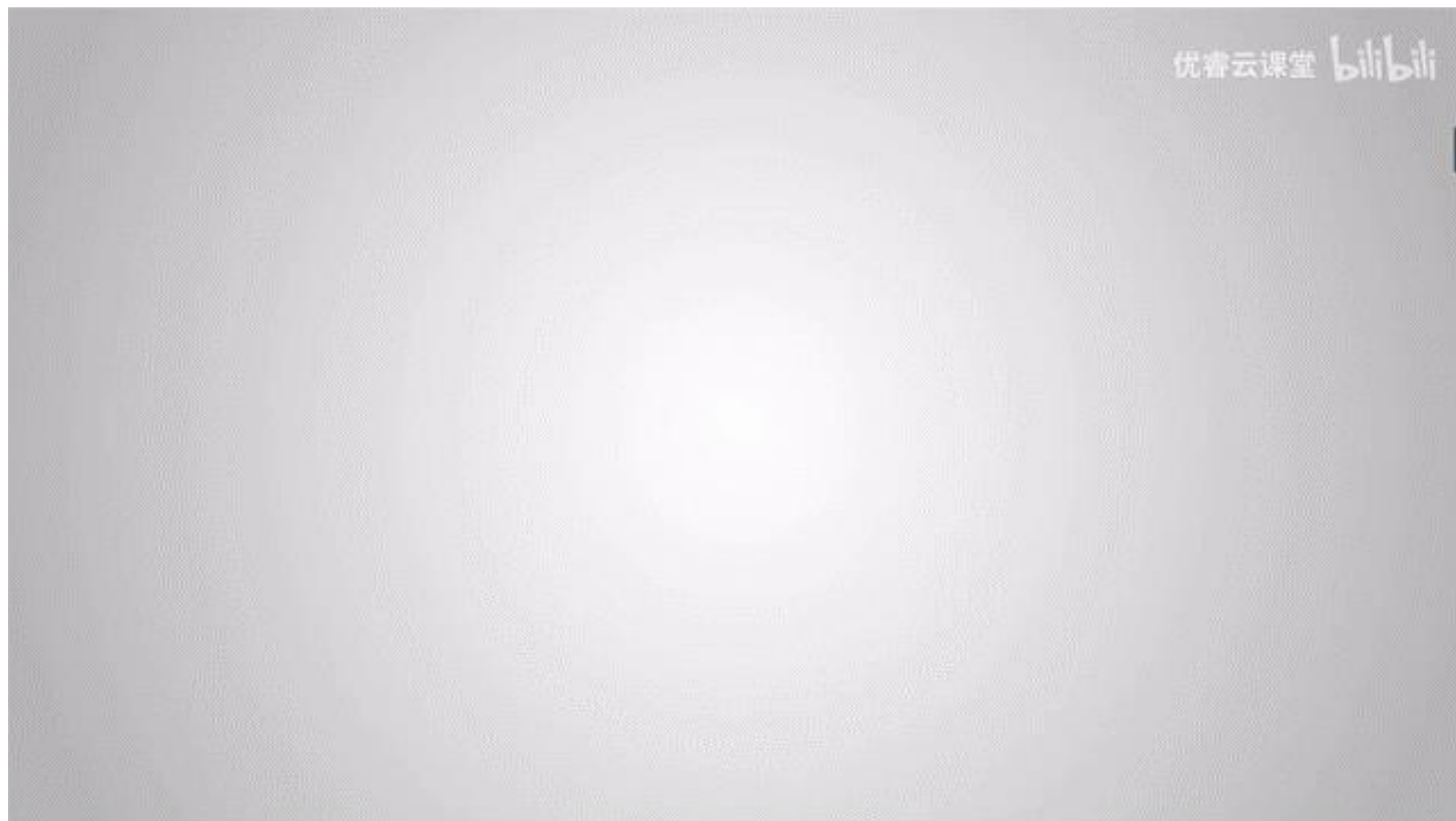
- 动态媒体接入控制（多点接入）

- 随机接入:容易产生碰撞
- 受控接入，如多点线路探询(polling)，或轮询。

以太网的两个标准

- DIX Ethernet V2 是世界上第一个局域网产品（以太网）的规约。
- IEEE 的 802.3 标准。
- DIX Ethernet V2 标准与 IEEE 的 802.3 标准只有很小的差别，因此可以将 802.3 局域网简称为“以太网”。
- 严格说来，“以太网”应当是指符合 DIX Ethernet V2 标准的局域网

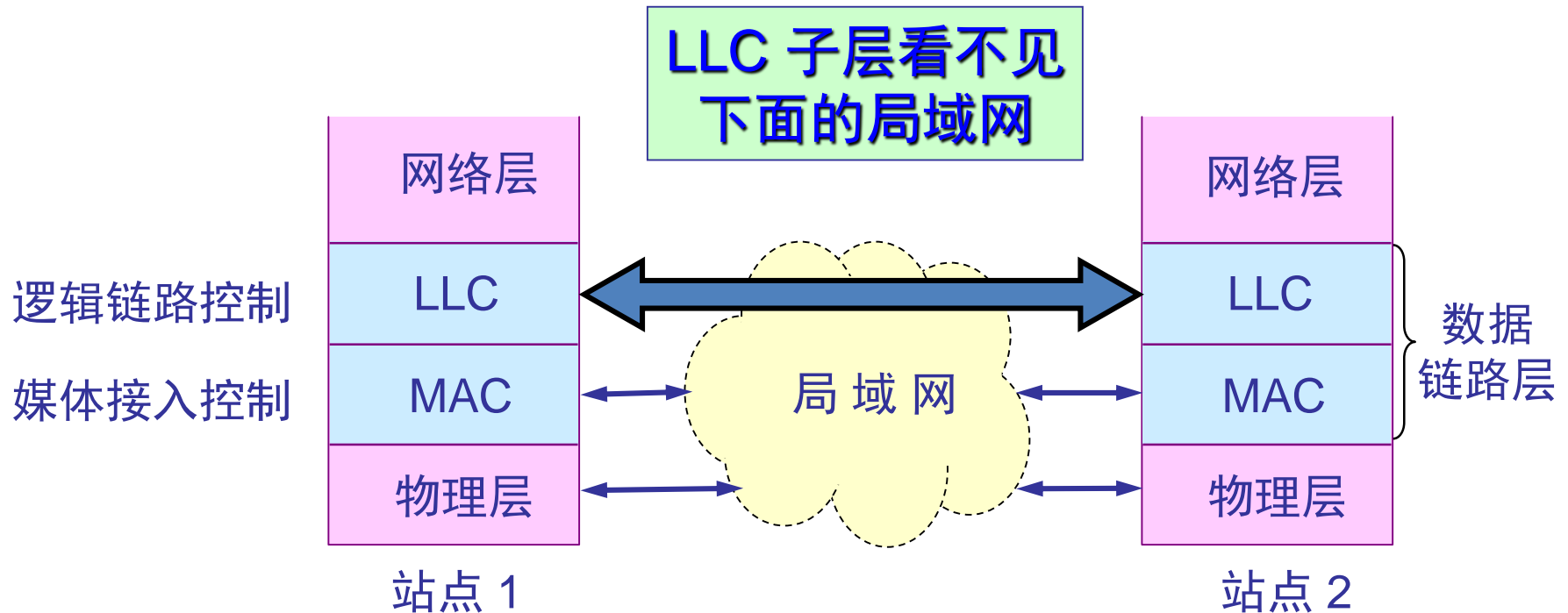
看视频思考：以太网的组成



数据链路层的两个子层

- 局域网的数据链路层被拆成两个子层：
 - 逻辑链路控制 LLC (Logical Link Control)
 - 媒体接入控制 MAC (Medium Access Control)
- 与接入到传输媒体有关的内容- MAC子层，
- LLC 子层与链路的控制有关，与传输媒体无关

局域网对 LLC 子层是透明的

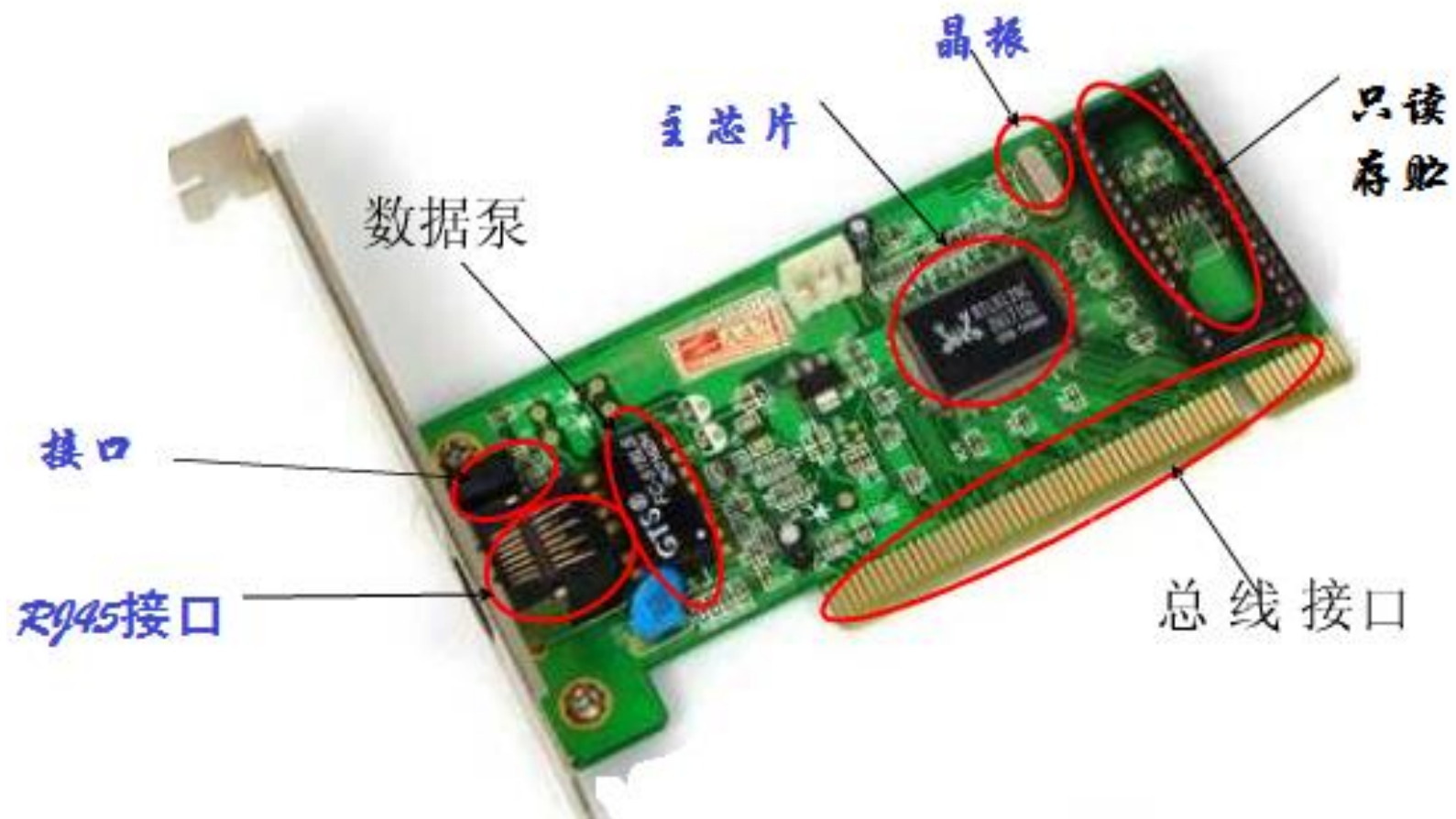


以后一般不考虑 LLC 子层

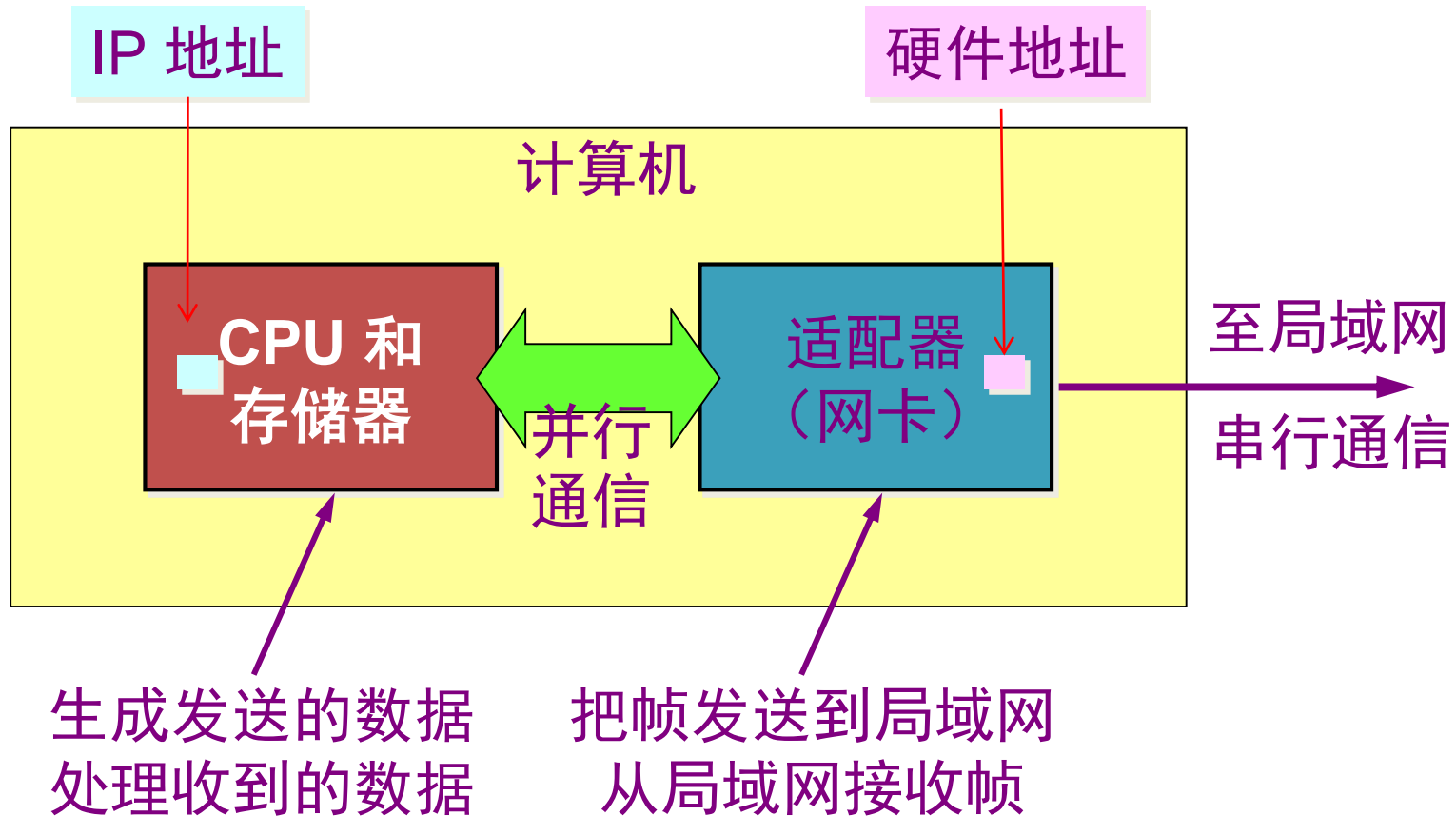
- 由于 TCP/IP 体系经常使用的局域网是 DIX Ethernet V2 而不是 802.3 标准中的几种局域网，因此现在 802 委员会制定的逻辑链路控制子层 LLC（即 802.2 标准）的作用已经不大了。
- 很多厂商生产的适配器上就仅装有 MAC 协议而没有 LLC 协议。

2 适配器的作用

- 网络接口板又称为**通信适配器** (adapter) 或 **网络接口卡** NIC (Network Interface Card), 或 “**网卡**”。
- 适配器的主要功能：
 - 进行串行/并行转换。
 - 对数据进行缓存, 有硬件缓冲存储部件。
 - 信号转换 (数字-电、光信号)。
- 实现物理层和数据链路控制协议, 所以需要安装驱动。



计算机通过NIC和局域网进行通信

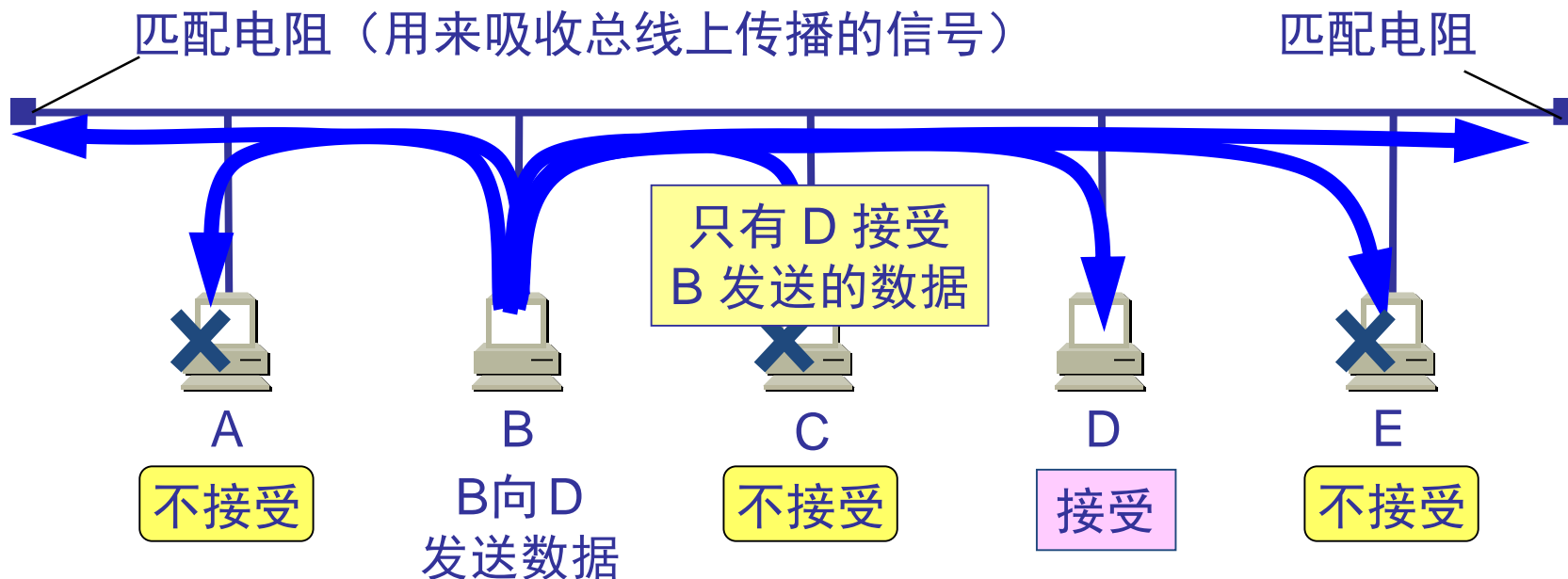


习题

1. 在PPP协议的状态转换图中，物理层连接建立后，下一步是？
A. 鉴别 B. 链路建立 C. 网络层协议 D. 链路打开
2. 第一个局域网产品的规约是IEEE 802.3标准。
3. MAC子层在现在已经很少在用了。
4. 在PPP协议帧格式中，若使用协议字段0xC021，则信息字段是
A. IP数据报 B. LCP数据 C. NCP数据
5. 一般的适配器都包括哪两层 *
A. 数据链路层 B. 网络层 C. 物理层 D. 应用层 E. 传输层
6. 局域网采用广播通信方式。

3 CSMA/CD 协议

- 最初的以太网是将许多计算机都连接到一根总线上。当初认为这样的连接方法既简单又可靠，因为总线上没有有源器件。



以太网的广播方式发送

总线上的每一个工作的计算机都能检测到 B 发送的数据信号。

由于只有计算机 D 的地址与数据帧首部写入的地址一致，因此只有 D 才接收这个数据帧。

其他所有的计算机（A, C 和 E）都检测到不是发送给它们的数据帧，因此就丢弃这个数据帧而不能够收下来。

具有广播特性的总线上实现了一对一的通信。

为了通信的简便 以太网采取了两种重要的措施

采用较为灵活的无连接的工作方式，即不必先建立连接就可以直接发送数据。

以太网对发送的数据帧不进行编号，也不要求对方发回确认。

- 理由是认为局域网信道的质量很好，因信道质量产生差错的概率很小。

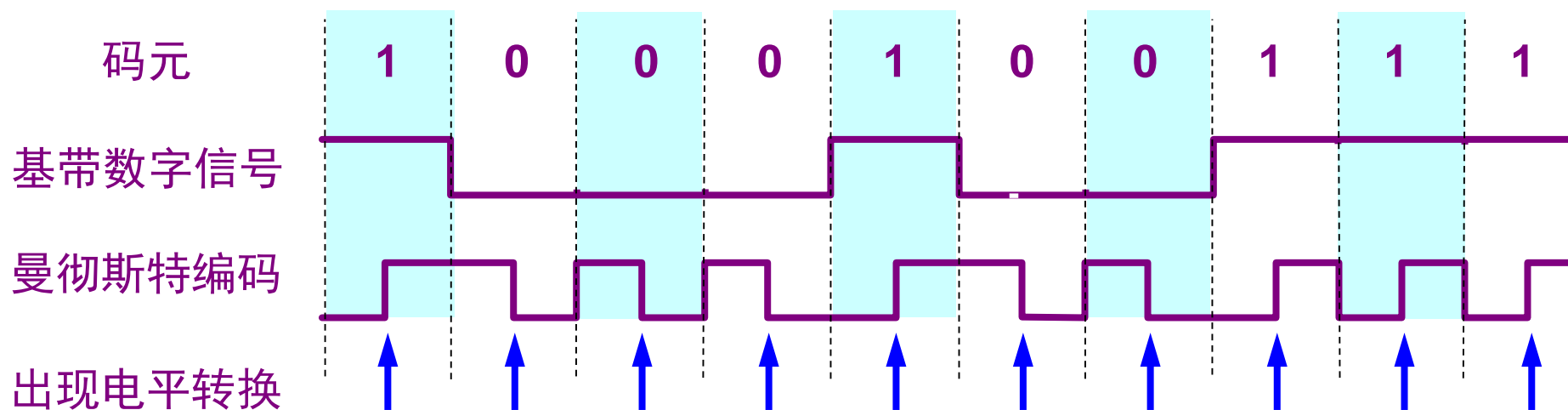
以太网提供的服务

以太网提供的服务是不可靠的数据帧交付，即尽最大努力的交付。

当目的站收到有差错的数据帧时就丢弃此帧。差错的纠正由高层来决定。

如果高层发现丢失了一些数据而进行重传，但以太网并不知道这是一个重传的帧，是当作一个新的数据帧来发送。

以太网发送的数据都使用 曼彻斯特(Manchester) 编码



曼彻斯特编码（Manchester Encoding），也叫做相位编码(PE)，是一个同步时钟编码技术，被物理层使用来编码一个同步位流的时钟和数据。

相关说法

- 在曼彻斯特编码中，用电压跳变的相位不同来区分1和0，即用正的电压跳变表示0，用负的电压跳变表示1。因此，这种编码也称为**相位编码**。
- 由于跳变都发生在每一个码元中间，接收端可以方便地利用它作为位同步时钟，因此，也称为**自同步编码**。

数据表示的约定-两种相反的数据表示约定

第一种是由G. E. Thomas, Andrew S. Tanenbaum等人在1949年提出的, 它规定0是由低-高的电平跳变表示, 1是高-低的电平跳变。

第二种约定: 在IEEE 802.4(令牌总线)和低速版的IEEE 802.3 (以太网)中规定, 按照这样的说法, 低-高电平跳变表示1, 高-低的电平跳变表示0。

总结一下

- 不是面向连接的传输，可能发生更多的重新发送
- 因为曼彻斯特编码，码元比原来提高一倍，增加了负担
- 广播式发送，不用预约发送，产生数据碰撞。
- 所以要CSMA/CD。

CSMA/CD工作原理（动画视频）



CSMA/CD工作原理

- 发送数据前 先侦听信道是否空闲，若空闲，则立即发送数据。若信道忙碌，则等待一段时间至信道中的信息传输结束后再发送数据
- 发送过程中若侦听到冲突, 则立即停止发送数据，等待一段随机时间, 再重新尝试。
- 总结为：先听后发，边发边听，冲突停发，随机延迟后重发。

载波监听多点接入/碰撞检测 CSMA/CD

- CSMA/CD – Carrier Sense Multiple Access with Collision Detection.
- “多点接入”：许多计算机（站）以多点接入的方式连接在一根总线上。
- “载波监听”：每一个站在发送数据之前先要检测总线上是否有其他计算机在发送数据，如果有，则暂时不要发送数据，以免发生碰撞。
- “载波监听”就是用电子技术检测总线上有没有其他计算机发送的数据信号。

碰撞检测

- “碰撞检测”：计算机边发送数据边检测信道上的信号电压大小。
- 当几个站同时在总线上发送数据时，总线上的信号电压摆动值将会增大（互相叠加）。
- 当一个站检测到的信号电压摆动值超过一定的门限值时，就认为总线上至少有两个站同时在发送数据，表明产生了碰撞。
- 所谓“碰撞”就是发生了冲突。因此“碰撞检测”也称为“冲突检测”。

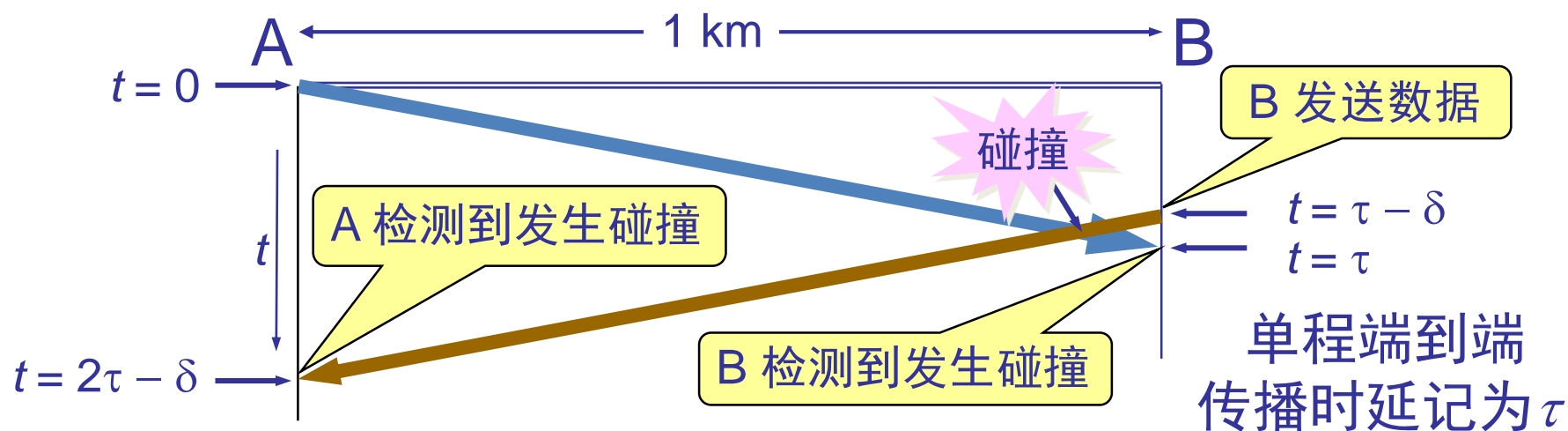
检测到碰撞后

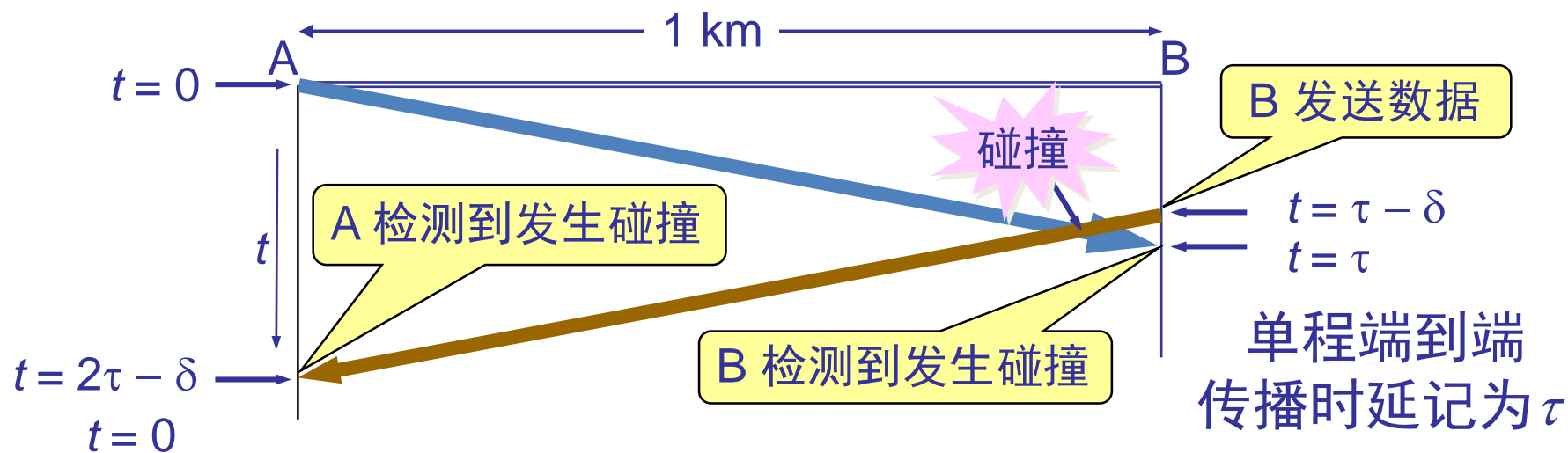
- 在发生碰撞时，总线上传输的信号产生了严重的失真，无法从中恢复出有用的信息。
- 每一个正在发送数据的站，一旦发现总线上出现了碰撞，就要立即停止发送，免得继续浪费网络资源，然后等待一段随机时间后再次发送。

电磁波在总线上的 有限传播速率的影响

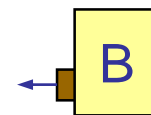
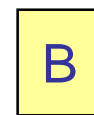
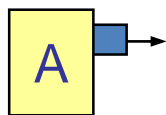
- 当某个站监听到总线是空闲时，也可能总线并非真正是空闲的。
- A 向 B 发出的信息，要经过一定的时间后才能传送到 B。
- B 若在 A 发送的信息到达 B 之前发送自己的帧(因为这时 B 的载波监听检测不到 A 所发送的信息)，则必然要在某个时间和 A 发送的帧发生碰撞。
- 碰撞的结果是两个帧都变得无用。

传播时延对载波监听的影響

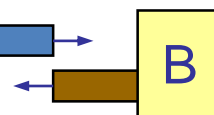




A 检测到
信道空闲
发送数据



$t = \tau - \delta$
B 检测到信道空闲
发送数据



$t = \tau - \delta / 2$
发生碰撞



$t = \tau$
B 检测到发生碰撞
停止发送

$t = 2\tau - \delta$
A 检测到
发生碰撞



重要特性

- 使用 CSMA/CD 协议的以太网不能进行全双工通信，只能进行双向交替通信（半双工通信）。
- 每个站在发送数据之后的一小段时间内，存在着遭遇碰撞的可能性。
- 这种发送的不确定性使整个以太网的平均通信量远小于以太网的最高数据率。

争用期

- 最先发送数据帧的站，在发送数据帧后至多经过时间 2τ （两倍的端到端往返时延）就可知道发送的数据帧是否遭受了碰撞。
- 以太网的端到端往返时延 2τ 称为争用期，或碰撞窗口。
- 经过争用期这段时间还没有检测到碰撞，才能肯定这次发送不会发生碰撞。

二进制指数类型退避算法

(truncated binary exponential type)

- 发生碰撞的站在停止发送数据后，要推迟（退避）一个随机时间才能再发送数据。
 - 确定基本退避时间，一般是取为争用期 2τ 。
 - 定义重传次数 k ， $k \leq 10$ ，即
$$k = \text{Min}[\text{重传次数}, 10]$$
 - 从整数集合 $[0, 1, \dots, (2^k - 1)]$ 中随机地取出一个数，记为 r 。重传所需的时延就是 r 倍的基本退避时间。
 - 当重传达 16 次仍不能成功时即丢弃该帧，并向高层报告。

争用期的长度

- 以太网取 $51.2 \mu\text{s}$ 为争用期的长度。
- 对于 10 Mb/s 以太网，在争用期内可发送 512 bit ，即 64 字节。
- 以太网在发送数据时，若前 64 字节没有发生冲突，则后续的数据就不会发生冲突。

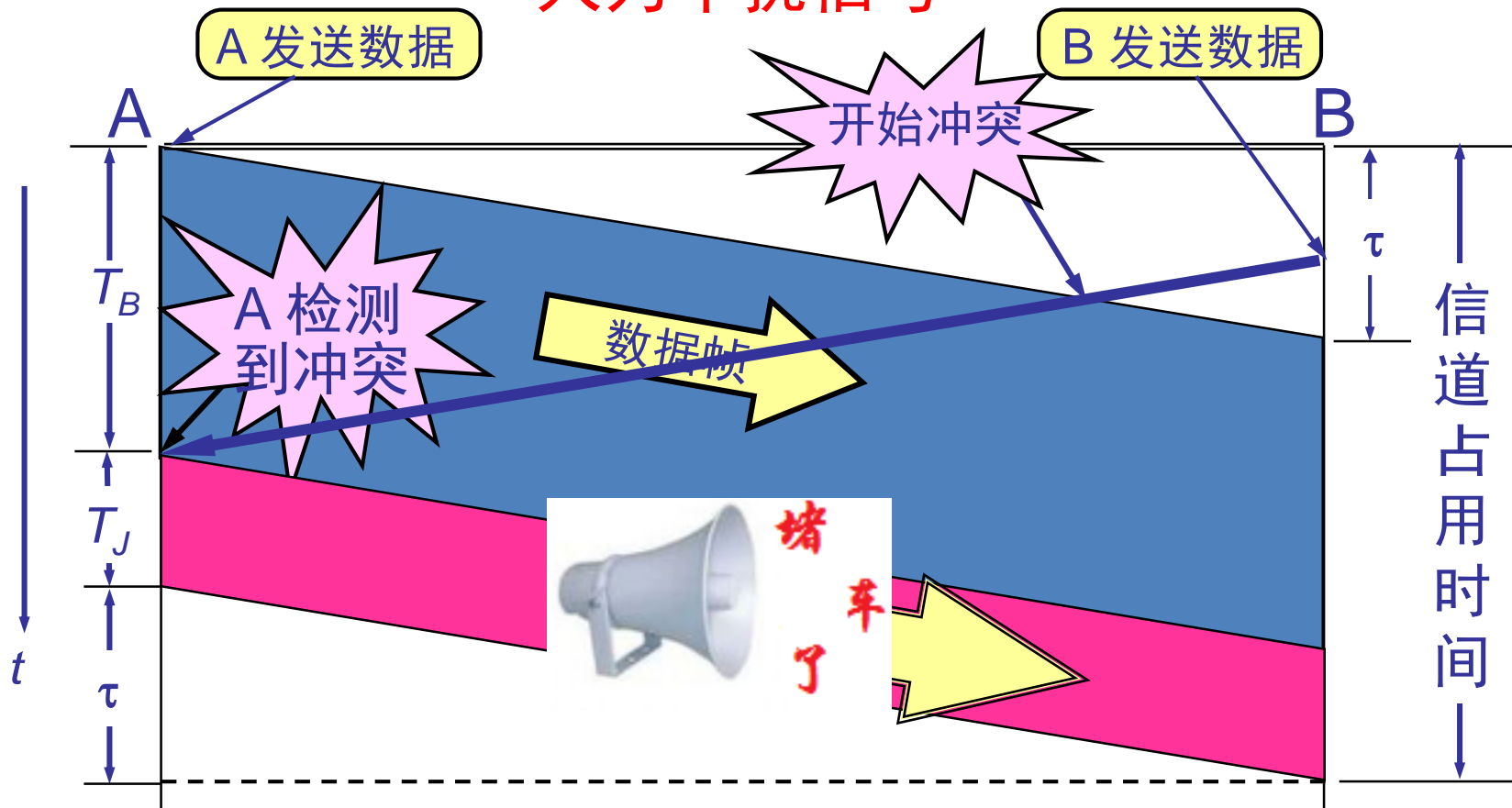
最短有效帧长

- 如果发生冲突，就一定是在发送的前 64 字节之内。
- 由于一检测到冲突就立即中止发送，这时已经发送出去的数据一定小于 64 字节。
- 以太网规定了最短有效帧长为 64 字节，凡长度小于 64 字节的帧都是由于冲突而异常中止的无效帧。

强化碰撞

- 当发送数据的站一旦发现发生了碰撞时：
 - 立即停止发送数据；
 - 再继续发送若干比特的人为干扰信号(jamming signal)，以便让所有用户都知道现在已经发生了碰撞。

人为干扰信号



B 也能够检测到冲突，并立即停止发送数据帧，接着就发送干扰信号。这里为了简单起见，只画出 A 发送干扰信号的情况。

● 综上，可以将CSMA-CD的要点归纳为：

- 1. 准备发送：适配器从网络层获得一个分组，加上以太网的首部和尾部，组成以太网帧，放入适配器的缓存中；
- 2. 检测信道，若信道忙，则不停地检测，直到信道转为空闲，若检测到信道空闲，则等待96比特时间，然后发送帧；
- 3. 在发送过程中仍不停地检测信道，若在争用期内都没有检测到冲突，则成功发送，若检测到冲突，则执行指数退比算法，等待 r 倍的512比特时间，然后再重发，重发16次均失败则放弃帧，向高层汇报。

习题

1. 以太网发送的数据使用_____编码的信号。
2. CSMA/CD中“载波”指的是频分复用FDM 的载波。
3. 在以太网中发生了碰撞表明这时一定出现了某种故障。
4. 在以太网中，可能在发送了512 bit (64 B) 以后发生碰撞？
5. 要发送的数据为101110。采用CRC的生成多项式是 $P(X)=X^3+1$ ，试求在数据后面的余数。

课后任务

复习第三章剩余部分内容