

计算机网络

第5章 链路层和局域网

目 录

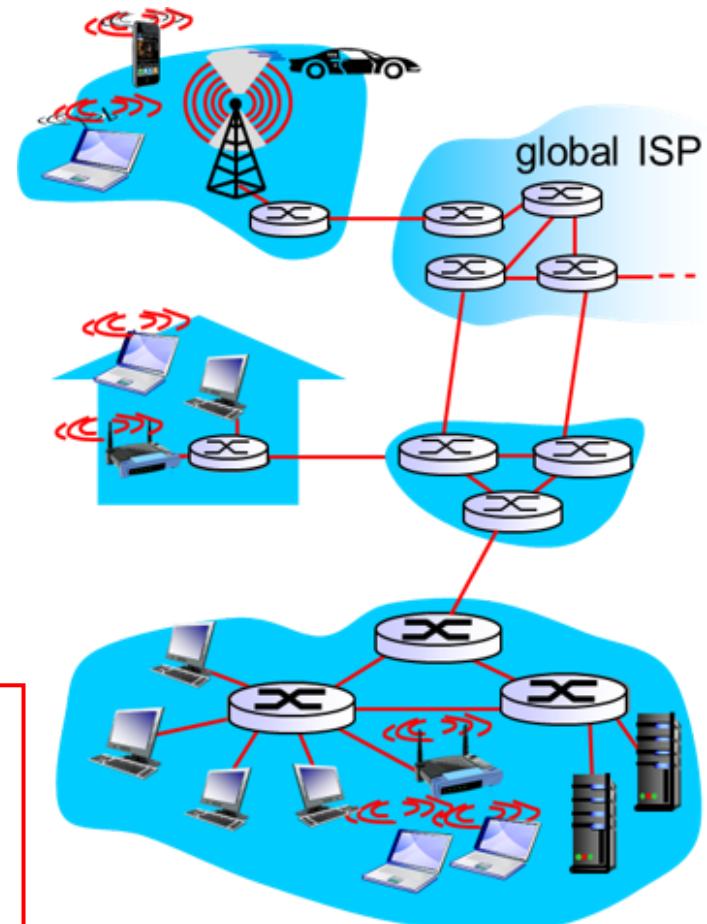
- 链路层概述
- 差错检测和纠正技术
- 多路访问链路和协议
- 局域网
- 链路虚拟化：网络作为链路层
- 数据中心网络
- 回顾：Web页面请求的历程

5.1 链路层概述

■ 术语

- 节点：主机和路由器
- 链路：沿着通信路径连接相邻节点的通信信道
 - 有线链路
 - 无线链路
- 帧：数据链路层的分组单元

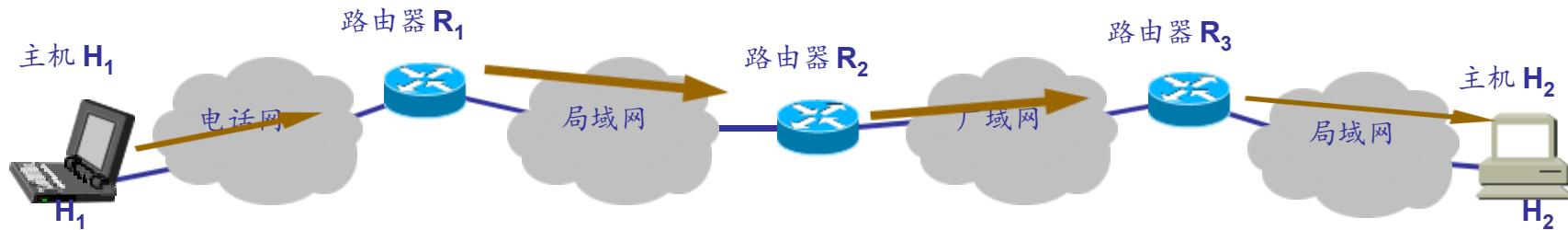
数据链路层负责将数据报通过链路从一个节点传输到物理上相邻的下一个节点



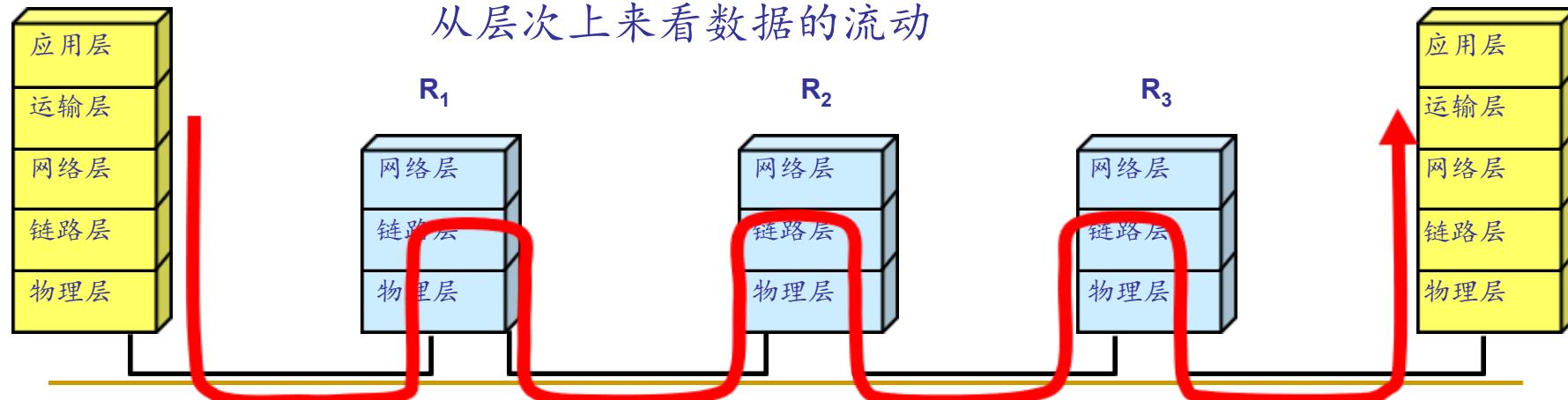
5.1 链路层概述

■ 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



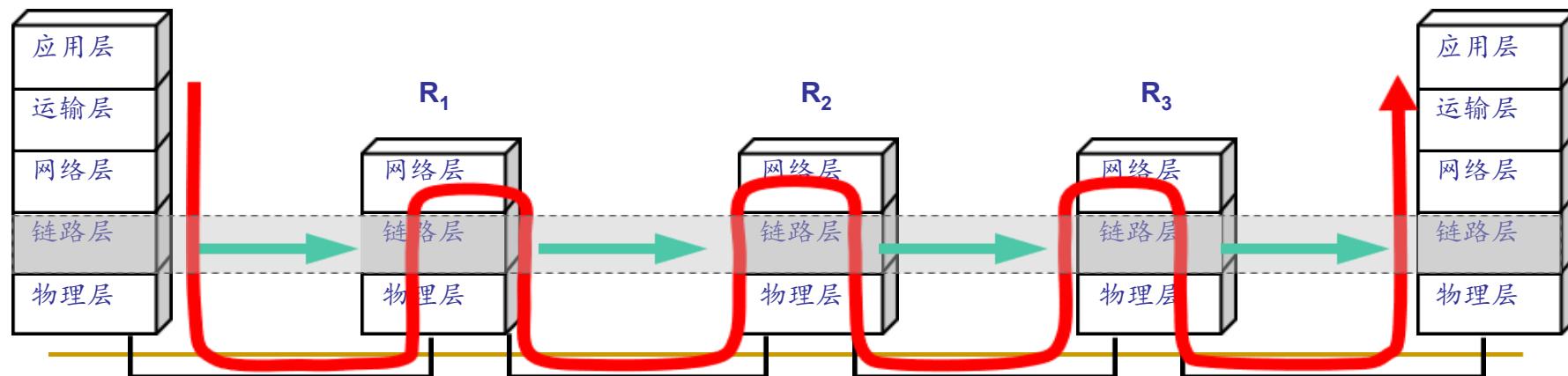
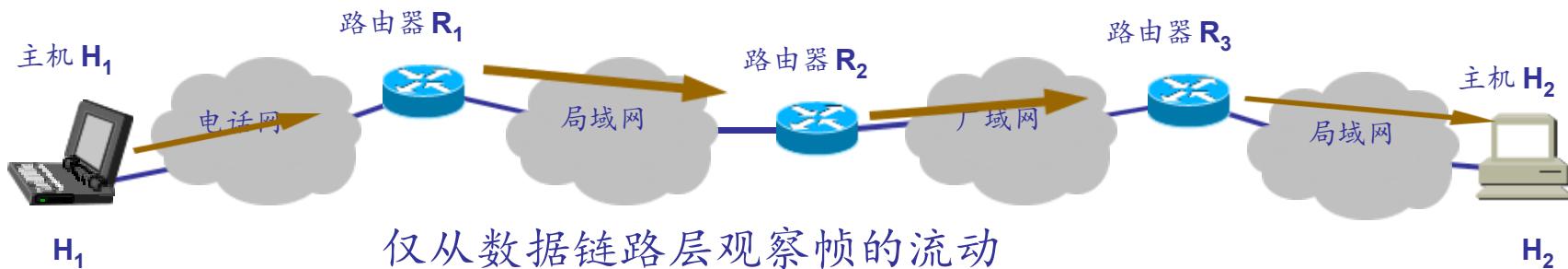
2020年11月10日

4

5.1 链路层概述

■ 数据链路层的简单模型

主机 H_1 向 H_2 发送数据



5.1 链路层概述

□ 几点特别说明

- 数据报在不同链路上可能由不同的链路层协议进行处理
 - 例如：第一段链路上由PPP处理，最后一段链路上由以太网处理，中间链路上由广域链路层协议处理
- 不同的链路层协议可能提供不同的服务
 - 例如：可靠传递、不可靠传递

5.1 链路层概述

■ 链路层提供的服务

□ 成帧、链路访问

- 将数据加上头部和尾部，封装成数据帧
- 共享介质的信道访问
- 帧头部用MAC地址标识源和目的（不同于IP地址）

□ 可靠传递

- 很少用于误码率低的链路（光纤、双绞线链路）
- 用于误码率高的链路（无线链路）

□ 流量控制

- 在相邻的收发节点间限制流量

5.1 链路层概述

■ 链路层提供的服务

□ 差错检测

- 信号衰减和电磁干扰噪声导致出错
- 接收方检测到错误存在：
 - 给发送方发送信号要求重传或丢弃该数据帧

□ 差错纠正

- 接收方检测和纠正帧中错误，不用重传

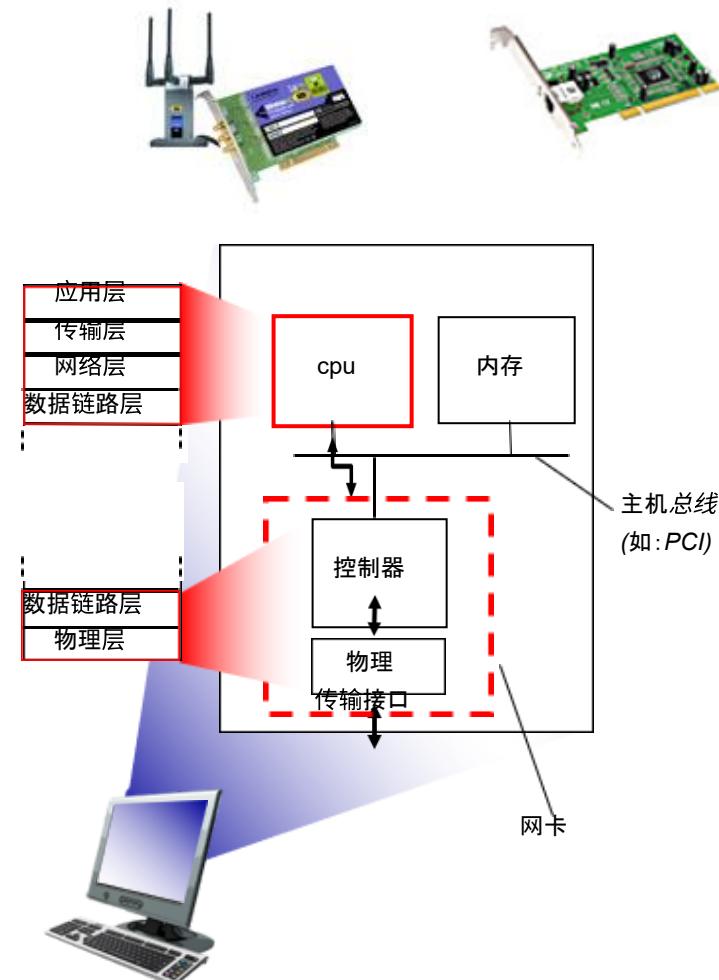
□ 半双工和全双工

- 半双工时，链路两端的节点都能传输分组，但不能同时传输

5.1 链路层概述

■ 链路层的实现

- 在每一台设备上（主机、交换机、路由器）
- 链路层在“适配器”（网卡NIC）或者芯片上实现
- 直接与主机的系统总线相连
- 是硬件、软件和固件的结合体



5.1 链路层概述

■ 适配器通信

□ 发送方

- 在一个帧内封装数据报
- 增加差错检测位，可靠交付，流量检测等

□ 接收方

- 查找错误，可靠交付，流量控制等
- 取出数据报，交给网络层

□ 适配器是半自治单元

- 帧的接收和发送、检错、丢弃均是自主进行
- 向上提交数据时，需要节点干预
- 最终受控于节点

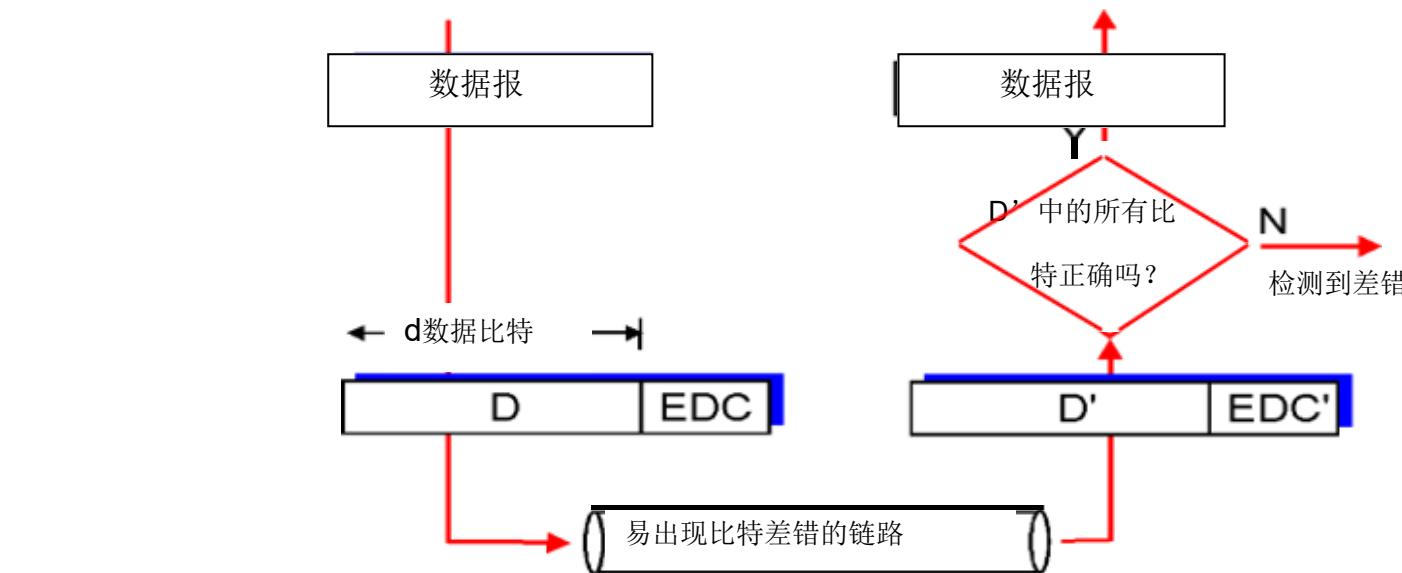
5.2 差错检测和纠正技术

■ 差错检测模型

EDC= Error Detection and Correction bits 差错检测和纠错比特

D = Data 差错检测位保护的数据，可包括头部

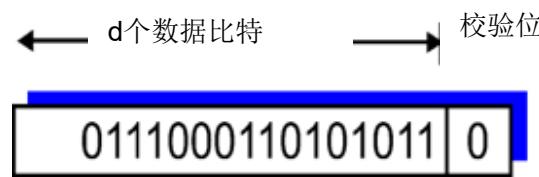
差错检测不是100%可靠的，EDC越长，查出错的概率越低！



5.2 差错检测和纠正技术

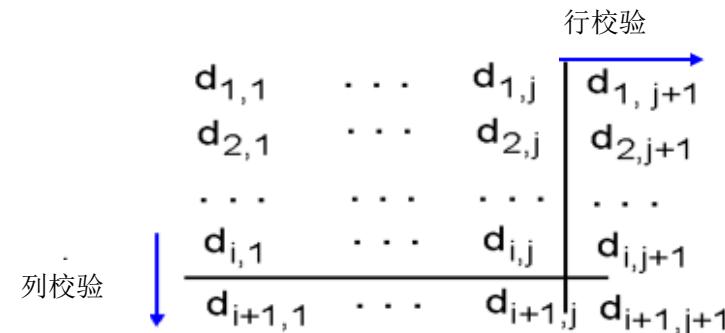
单比特奇偶校验:

检测单个比特错误



二维奇偶校验:

检测和纠正单个比特错误



101011
111100
011101
101010

无差错

101011
101100
011101
101010

校验错
校验错

可纠正单比特差错

single bit error

5.2 差错检测和纠正技术

■ 因特网检查和

□ 发送方

- 将数据段的内容作为16比特的整数序列
- 校验和: 累加求和, 计算和的1的补码
- 发送方将得到的校验和值放入PDU校验和字段

□ 接收方

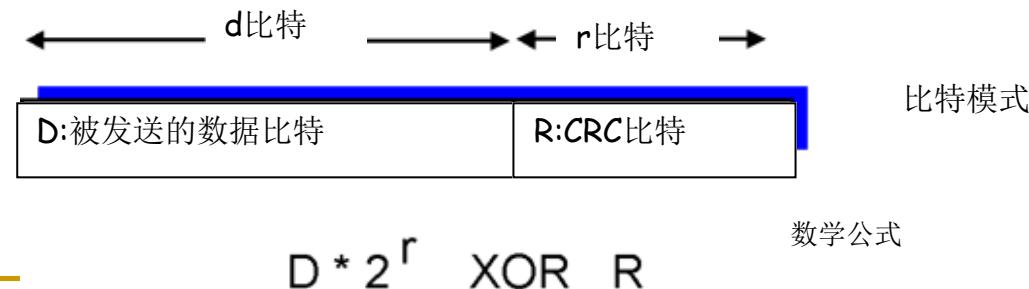
- 计算收到的数据段的校验和
- 检查计算出的校验和与校验和字段中的值是否相同:
 - NO - 检测到错误
 - YES - 没有错误

□ 特别注意: 仅用于TCP、UDP和IPv4协议中

5.2 差错检测和纠正技术

■ 循环冗余校验码

- d 比特的数据, D
- 选择 $r+1$ 比特模式(生成多项式), 表示为 G
- 目标: 选择 r 个CRC比特, R , 以便
 - $\langle D, R \rangle$ 恰好能被 G 整除 (模2计算)
 - 接收方已知 G , 用 G 去除 $\langle D, R \rangle$, 若余数非0, 则检测到错误
 - 能检测到所有少于 $r+1$ 比特的错误
- 在实践中被广泛应用 (ATM, HDLC)



5.2 差错检测和纠正技术

- 如果要:

$$D^{*}2^r \text{ XOR } R = nG$$

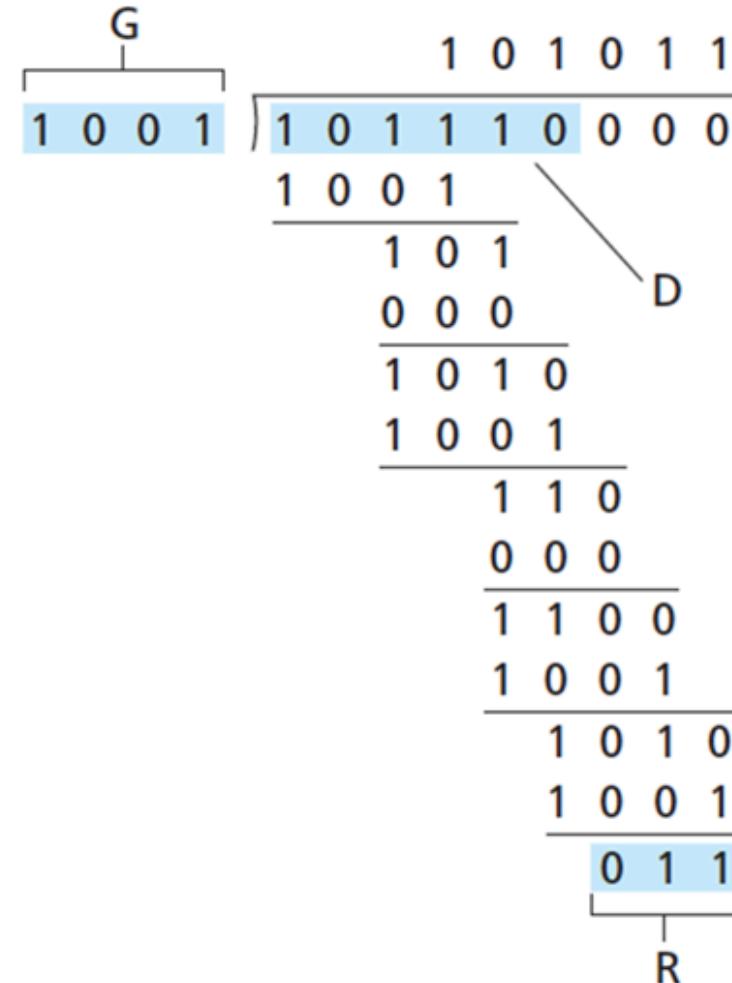
- 两边都异或R, 得到:

$$D^{*}2^r = nG \text{ XOR } R$$

- 即:

$D^{*}2^r$ 除以 G , 得到余数 R

$$R = \text{remainder}[\frac{D \cdot 2^r}{G}]$$



5.3 多路访问链路和协议

■ 两种链路

□ 点到点链路

- PPP/以太网交换机和主机之间的点到点链路

□ 广播链路(共享线路或介质)

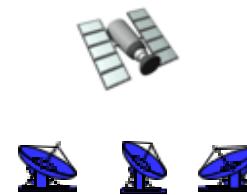
- 传统以太网/802.11无线LAN



shared wire (e.g.,
cabled Ethernet)



shared RF
(e.g., 802.11 WiFi)



shared RF
(satellite)



humans at a
cocktail party
(shared air, acoustical)

5.3 多路访问链路和协议

■ 广播链路的特点

- 单个共享广播信道
- 两个或多个节点同时传输：相互干扰
 - 碰撞：一个节点同时收到两个或多个信号

■ 多址访问协议

- 分布式算法决定节点如何共享信道，如节点何时可以传输数据
- 特别注意：有关共享信道的通信（协商）需使用信道本身
 - 没有额外的信道来进行协调

5.3 多路访问链路和协议

■ 理想的多址访问协议需满足：

- 假定：信道为速率为 R b/s的广播信道
- 当只有一个节点有数据发送时，该节点的吞吐量为 R
- 当 M 个节点有数据发送时，每个节点吞吐量为 R/M
- 分散
 - 没有特定节点用于调整传输
 - 没有时钟同步
- 简单

5.3 多路访问链路和协议

■ 多址访问协议分类

□ 信道划分协议

- 将信道划分成小的“片”（时隙、频率、编码）
- 将“片”分配给节点使用

□ 随机访问协议

- 信道没有被分割，允许碰撞
- 碰撞恢复

□ 轮流协议

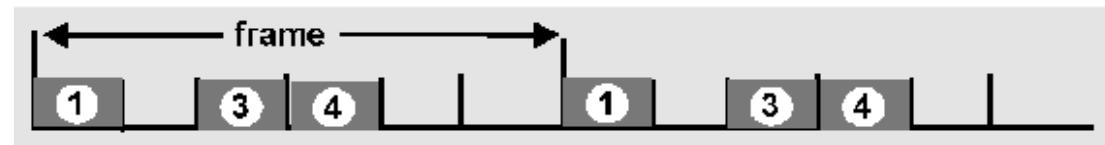
- 节点轮流传送，但数据量大的节点轮流更长时间

5.3 多路访问链路和协议

■ 信道划分协议

□ TDMA(Time Division Multiple Access)

- 循环访问信道
- 每个节点在每次循环中得到固定长度的时隙（时隙长度=传输单个分组时间）
- 没有数据发送的时隙空闲
- 例如：6-节点 LAN, 时隙1,3,4 有数据发送, 2,5,6 的时隙空闲

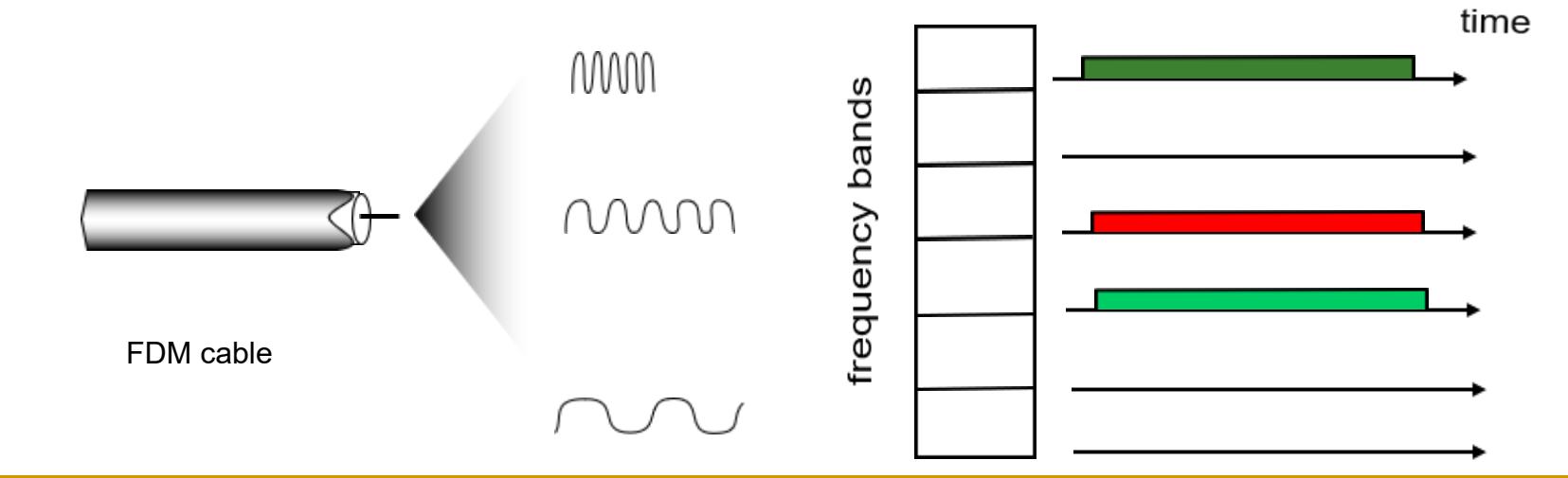


5.3 多路访问链路和协议

■ 信道划分协议

□ FDMA(Frequency Division Multiple Access)

- 信道按频谱分成若干频段
- 每个节点分配固定频段
- 在频段不用时该部分信道被闲置和浪费



5.3 多路访问链路和协议

■ 随机访问协议

- 当节点有数据发送时
 - 以信道全部速率R传输
 - 没有主节点起协调作用
- 两个或多个节点传送时——碰撞
- 随机访问协议解决
 - 如何检测碰撞
 - 如何从碰撞中恢复（如：延时后重传）
- 随机访问协议举例：
 - ALOHA、时隙ALOHA
 - CSMA, CSMA/CD, CSMA/CA

5.3 多路访问链路和协议

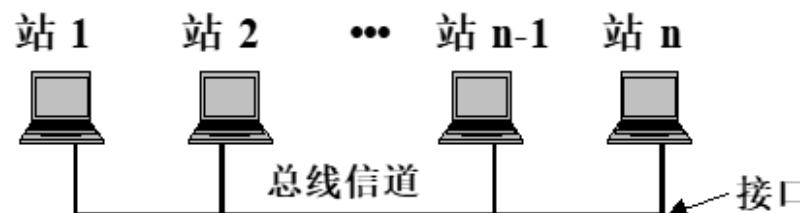
■ ALOHA

□ ALOHA的由来

- ALOHA 乃 Additive Link On-Line HAwaii system 简写，ALOHA恰好还是夏威夷方言的“你好”。ALOHA网是计算机网络早期发展中一个著名的网络，也是第一个无线计算机网络，现仍在运行之中。

□ ALOHA网的特征

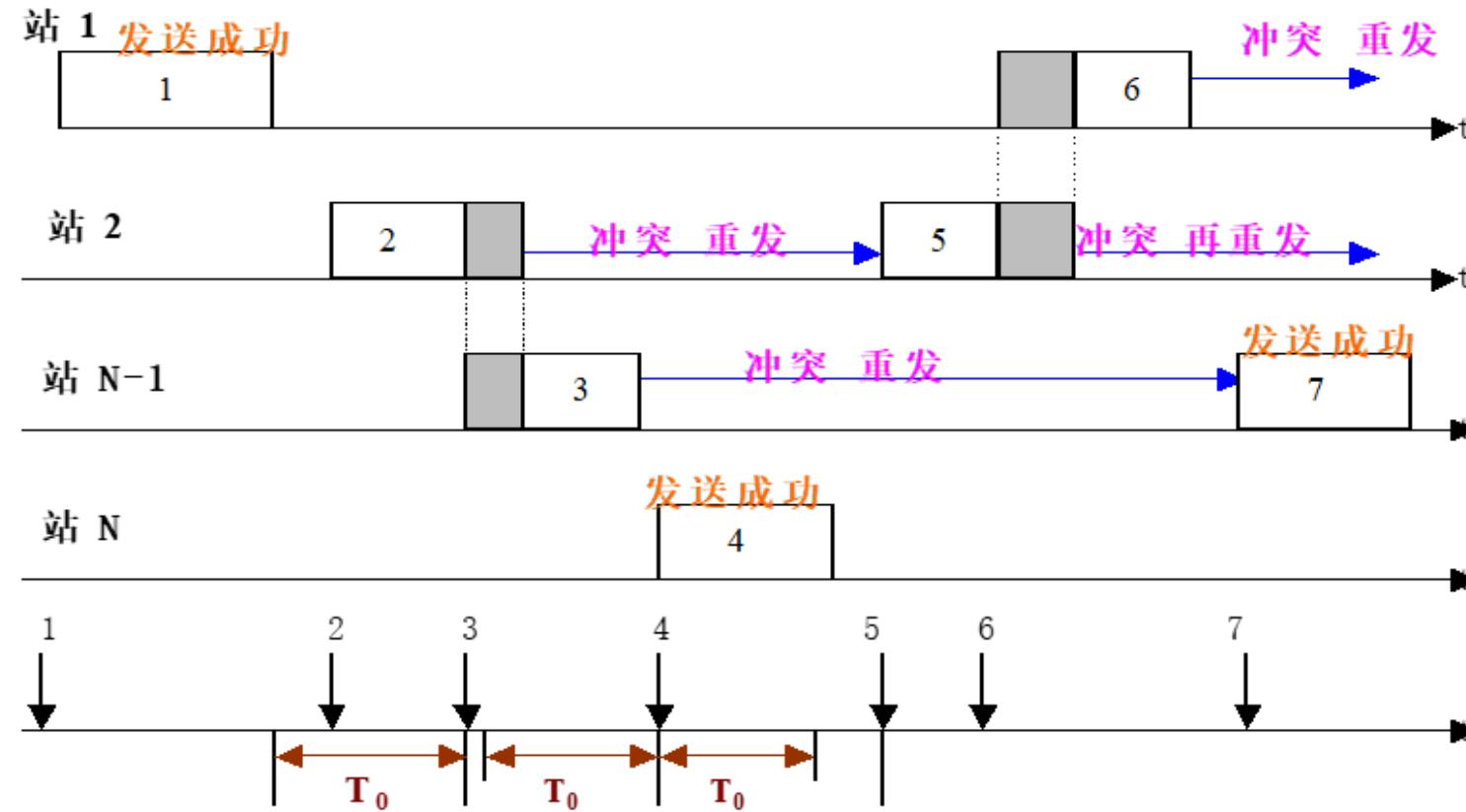
- 因群岛位置的散布，网络拓扑采用了星型结构；
- 为节省费用和易于组网，网络中各站点的通信采用了无线传输介质。
- 由于采用无线电信道，考虑到无法申请更多的频率点，因而所有站点都使用统一的频率通过主机交换信息。



ALOHA 系统的一般模型

5.3 多路访问链路和协议

■ 纯ALOHA



2020年11月10日

纯 ALOHA 系统的工作原理

24

5.3 多路访问链路和协议

■ 纯ALOHA的工作效率

$$P(\text{给定节点成功概率}) = P(\text{给定节点传送}) \cdot$$

$$P(\text{在 } [t_0-1, t_0] \text{ 没有其它节点传送})$$

$$P(\text{在 } [t_0, t_0+1] \text{ 没有其它节点传送})$$

$$= p \cdot (1-p)^{N-1} \cdot (1-p)^{N-1}$$

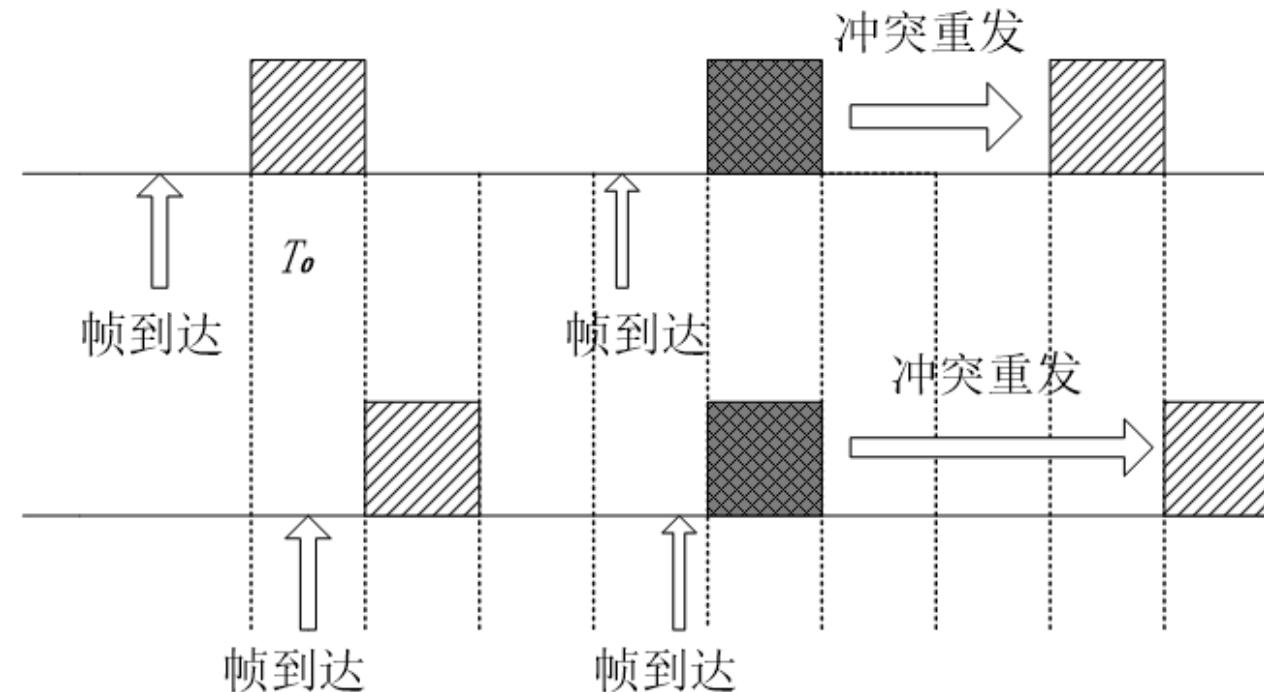
$$= p \cdot (1-p)^{2(N-1)}$$

… 选择最合适p,n趋于无穷，取极限…

$$= 1/(2e) = 0.18$$

5.3 多路访问链路和协议

■ 时隙ALOHA



5.3 多路访问链路和协议

■ 时隙ALOHA的工作效率

$P(\text{给定节点成功概率}) = P(\text{给定节点传送}) \cdot$

$P(\text{没有其它节点传送})$

$$= p \cdot (1-p)^{N-1}$$

… 选择最合适 p, n 趋于无穷，取极限…

$$= 1/e = 0.37$$

5.3 多路访问链路和协议

■ CSMA(**Carrier Sense Multiple Access**)

- 传输前监听
 - 如果信道空闲，传送整个帧
 - 如果信道忙，推迟传送
- 为人处事的规则之一：不要打断别人的发言！

5.3 多路访问链路和协议

■ CSMA分类

□ 非坚持(nonpersistent)CSMA

一旦监听到信道忙（即发现有其他站在发送数据），就不

再坚持听下去，而是根据协议的算法延迟一个随机的时间后重新再监听。若进行载波监听时发现信道空闲，则将准备好的帧发送出去。

□ 时隙非坚持CSMA

采用划分时隙的随机接入CSMA协议，协议规定只能在每

个时隙开始时才能发送帧。

5.3 多路访问链路和协议

■ CSMA分类

□ 1坚持CSMA

当一个站点要传送数据时，首先侦听信道，看是否有其他站点正在传送。如果信道正忙，它就持续等待直到它侦听到信道空闲时，便将数据送出。若发生冲突，站点就等待一个随机长的时间，然后重新开始。

□ P坚持CSMA

当一个站点要传送数据时，首先侦听信道，看是否有其他站点正在传送。如果信道正忙，它就持续等待直到它侦听到信道空闲时，以概率P发送数据，而以概率 $(1-P)$ 延迟一段时间T(网络中最远的端到端的传播时延)，重新监听信道。若发生冲突，站点就等待一个随机长的时间，然后重新开始。

5.3 多路访问链路和协议

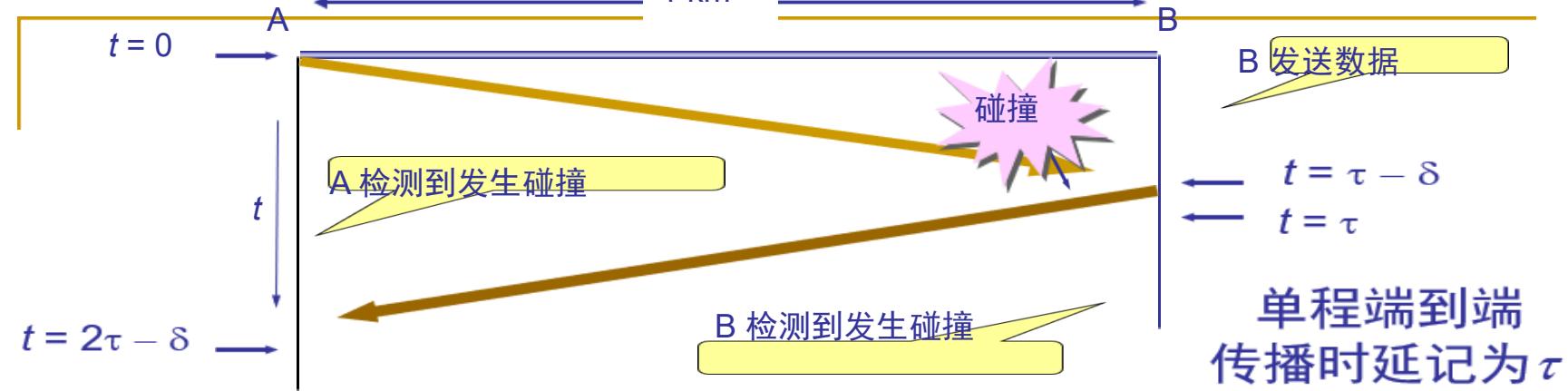
■ CSMA比较

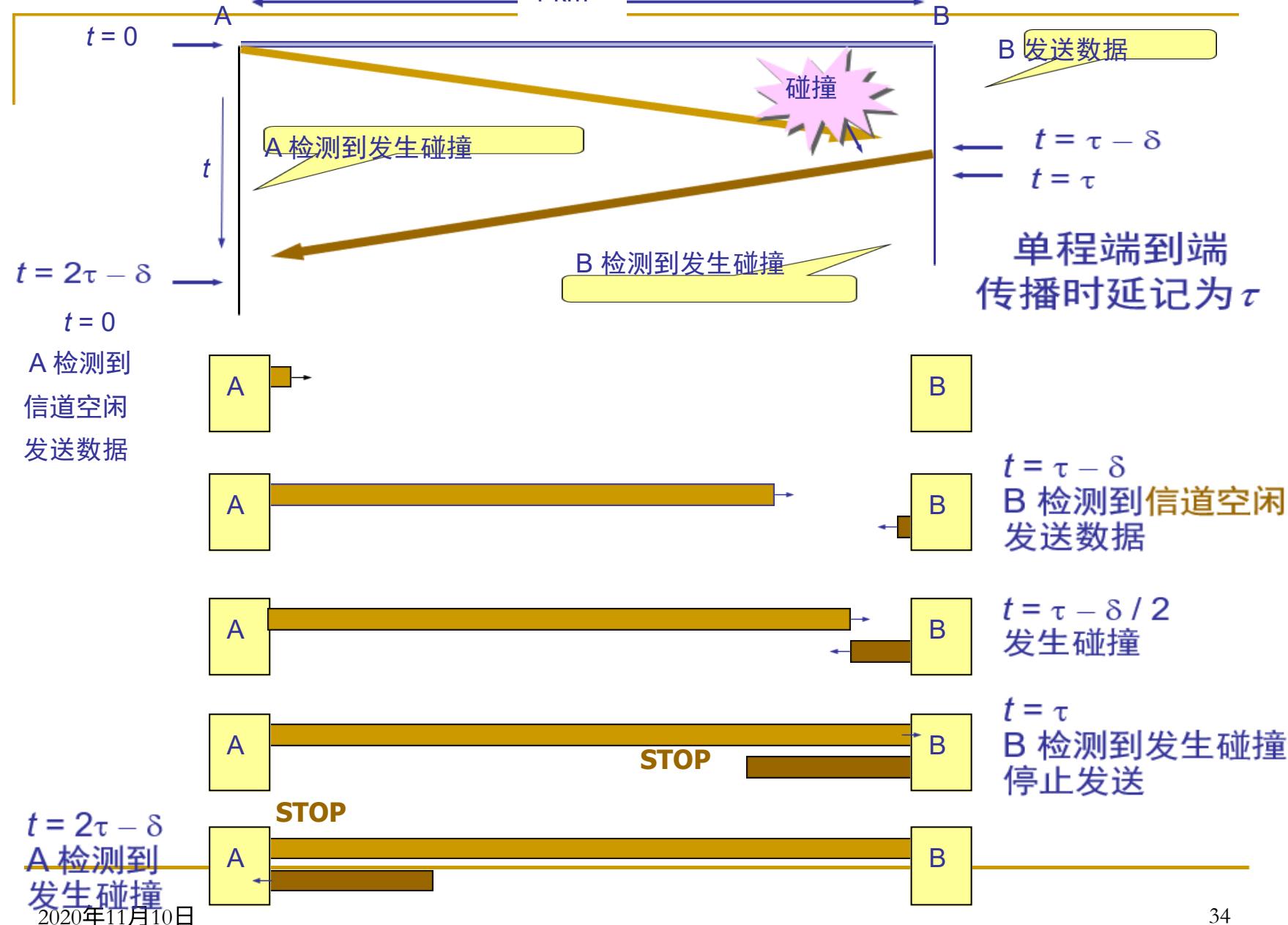
- 非坚持：不能充分利用信道刚刚转入空闲期的这段时间。
- 1坚持：容易在上述这段时间产生冲突。
- P坚持：可以在一定程度上克服这些缺点，但却很难选择一个能用于各种通信量强度的P值。所以在实际网络中常选择1坚持。

5.3 多路访问链路和协议

■ CSMA/CD

- 在短时间内碰撞被检测
 - 在有线LANs中比较容易:测量信号强度, 比较收、发的信号
 - 在无线LANs中比较困难: 传输时接收器是关闭的
- 碰撞后停止传输, 减少信道浪费

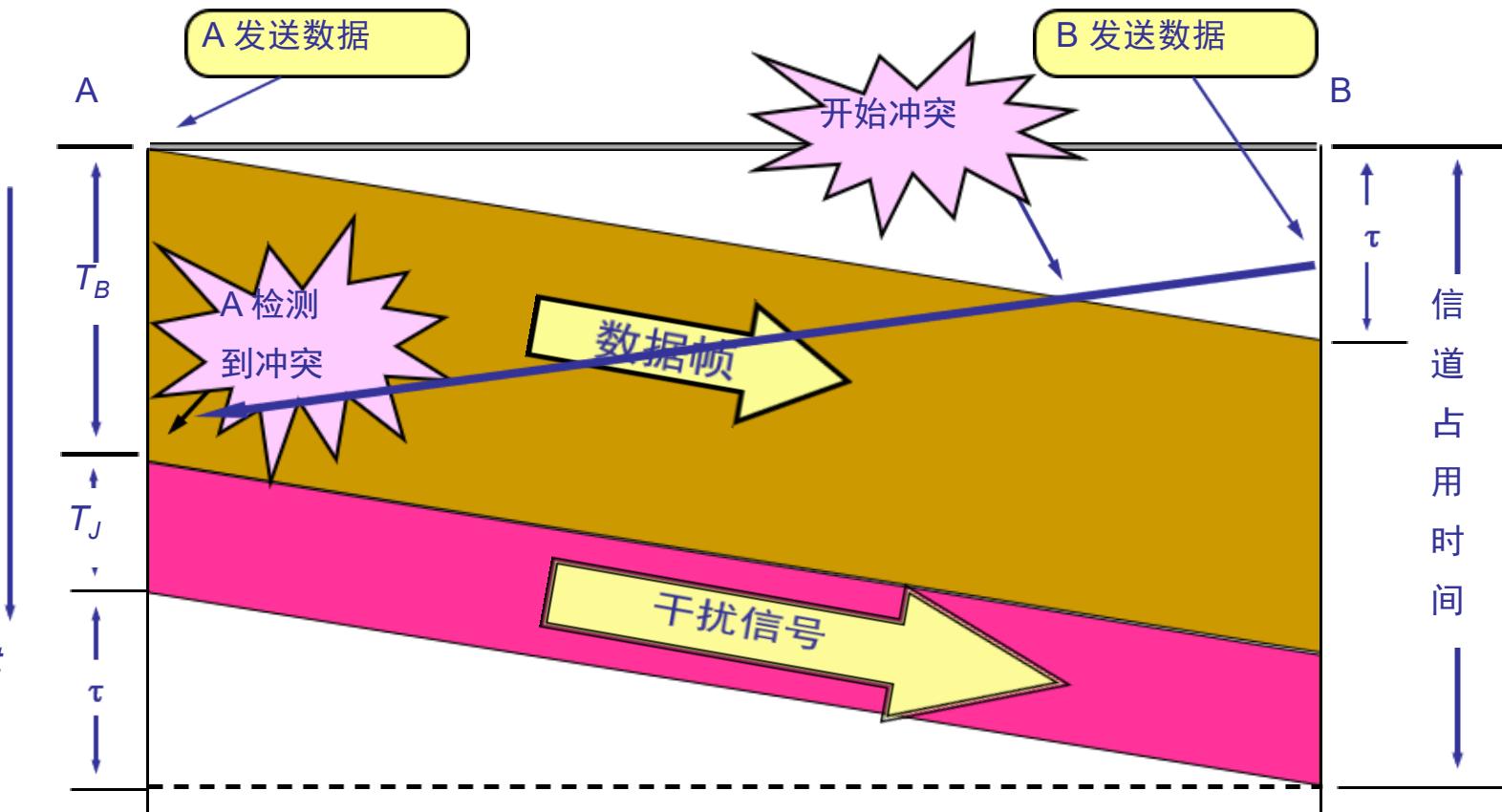




5.3 多路访问链路和协议

□ 强化碰撞

- 当发送数据的站一旦发现发生了碰撞时，除了立即停止发送数据外，还要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。



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。

5.3 多路访问链路和协议

□ 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。

5.3 多路访问链路和协议

■ 轮流协议

□ 问题的背景

■ 信道划分协议

- 在重负荷时，共享信道有效、公平
- 在轻负荷时效率低：信道访问延时，即使只有一个活动节点，也只能分配到 $1/N$ 的带宽

■ 随机访问协议

- 轻负荷时效率高：只有一个节点时，能充分利用信道
- 在重负荷下：碰撞的开销

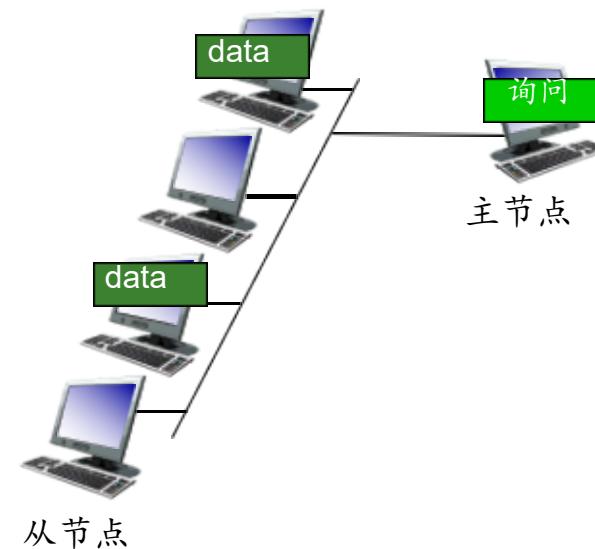
■ 轮流协议

- 在两个方面寻求最佳的解决方案！

5.3 多路访问链路和协议

□ 轮询协议

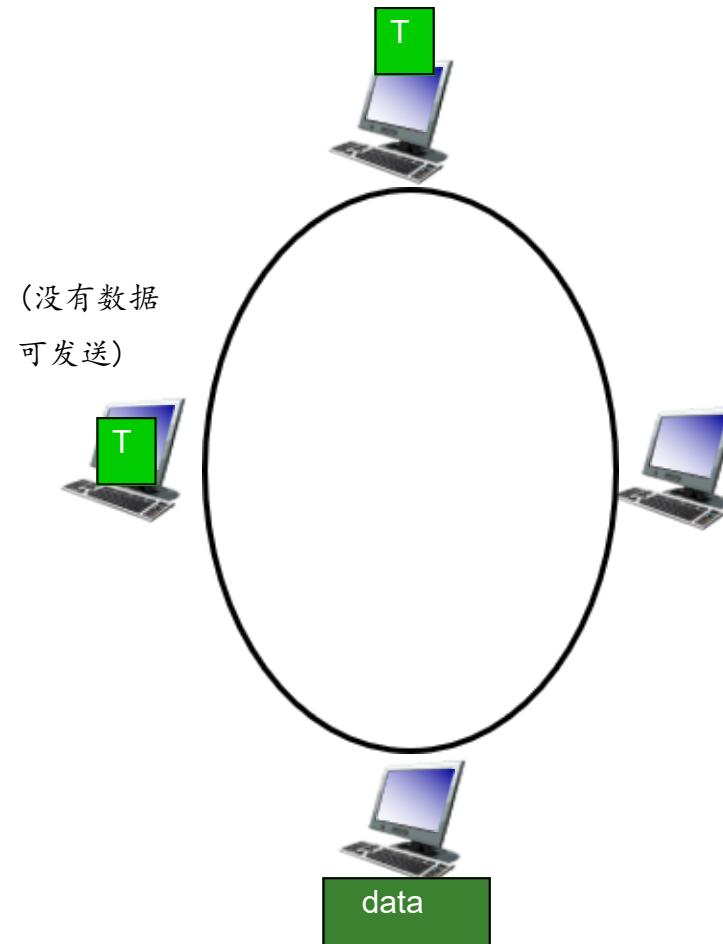
- 主节点邀请从节点轮流传输
- 关注
 - 轮询开销
 - 等待时间
 - 单点失效(主节点)



5.3 多路访问链路和协议

□ 令牌传递协议

- 控制令牌依次通过各个结点
- 令牌报文
- 关注
 - 令牌的开销
 - 等待时间
 - 单点失效(token)



5.3 多路访问链路和协议

■ 对于共享介质能做什么？

- 信道划分，基于时间、频率、编码
 - 时分，频分
- 随机划分（动态），
 - ALOHA, S-ALOHA, CSMA, CSMA/CD
 - 载波侦听：有线“易行”、无线“困难”
 - CSMA/CD 用于以太网
 - CSMA/CA 用于 802.11
- 轮流
 - 主节点轮询，令牌传递

5.4 局域网

■ MAC地址

□ 作用

- 在数据链路层标识每块网络适配器，使得能够在广播信道上寻址目标节点

□ 组成

- 48bit (e.g.: 1A-2F-BB-76-09-AD)
- 前24bit由IEEE分配管理——OUI号
- 后24bit由厂商自行分配

特别注意： MAC地址烧入网络适配器的ROM中，不可
更改

5.4 局域网

□ 与IP地址的比较

■ MAC地址是平面地址，类似于身份证号

IP地址是层次地址，类似于邮政通信地址

■ MAC地址在不同的网络间迁移时，不会改变

IP地址在不同的网络间迁移时，需要改变以适应新的
网络配置

特别注意：无线网络中进行漫游时，如果在不同的网络
间切换时，改变网络设置，会导致连接中
断，为维持连接正常工作，第六章将介绍无
线移动管理

5.4 局域网

■ 地址解析协议 (ARP)

- 目标
 - 根据目标的IP地址获取其MAC地址

- ARP高速缓存

- 局域网节点的IP/MAC地址映射

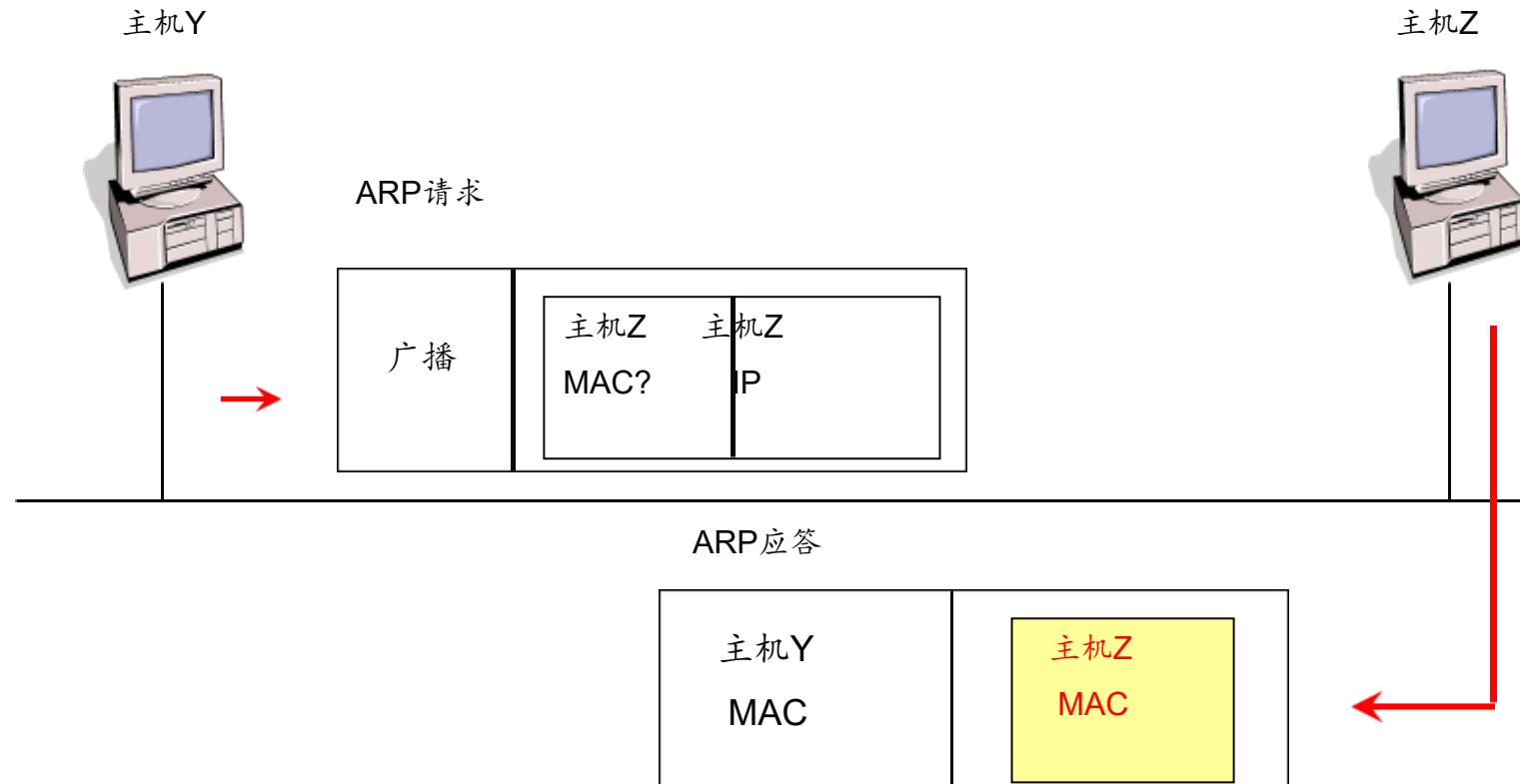
- < IP; MAC; TTL >

- TTL (Time To Live): 超过TTL的地址映射会被删除 (一

- 般为20分钟)

5.4 局域网

□ ARP协议：同一局域网内工作流程



5.4 局域网

□ ARP协议：同一局域网内工作流程

■ 建立ARP请求包

MAC报头		IP报头		ARP请求报文		
目标	源	目标	源	你的MAC地	址是什么？	
FF-FF-FF-FF-FF-FF	02-60-8C-01-02-03	197.15.22.126	197.15.22.33			

■ 广播发送该ARP请求包

5.4 局域网

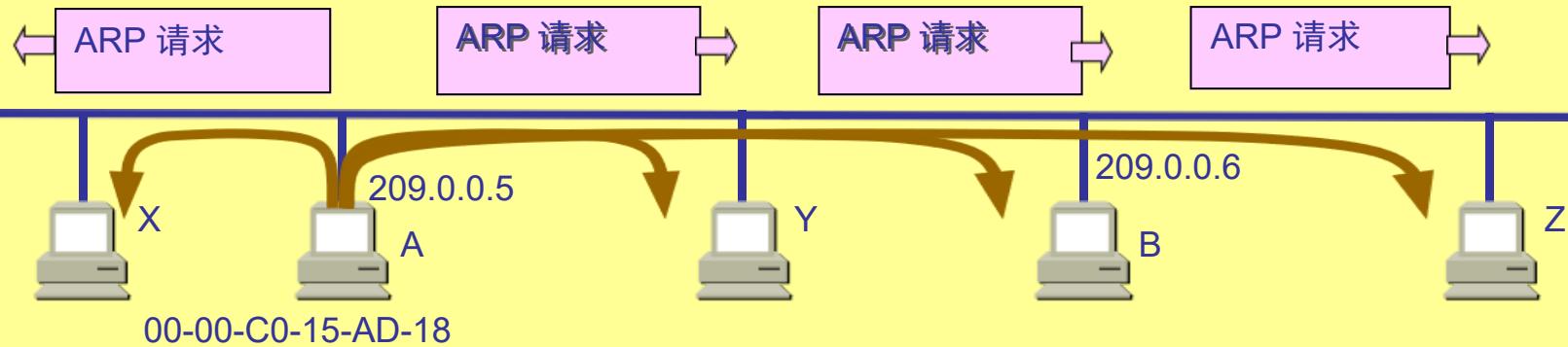
- 目的197.15.22.126接收到该ARP请求包，建立包含自己MAC地址的ARP应答包（请注意，应答包和请求包的源、目标是不一致的）

MAC报头		IP报头		ARP应答报文	
目标	源	目标	源	我的MAC地	
02-60-8C-01-02-03	08-00-02-89-90-80	197.15.22.33	197.15.22.126	址是.....	

- 直接向源197.15.22.33发送该ARP应答包
- 197.15.22.33更新ARP高速缓存

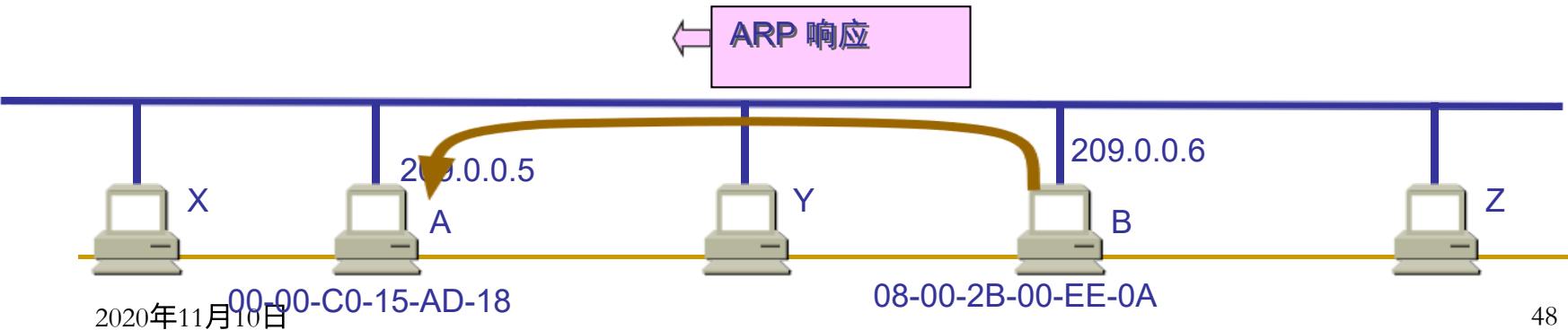
主机 A 广播发送
ARP 请求分组

我是 209.0.0.5，硬件地址是 00-00-C0-15-AD-18
我想知道主机 209.0.0.6 的硬件地址



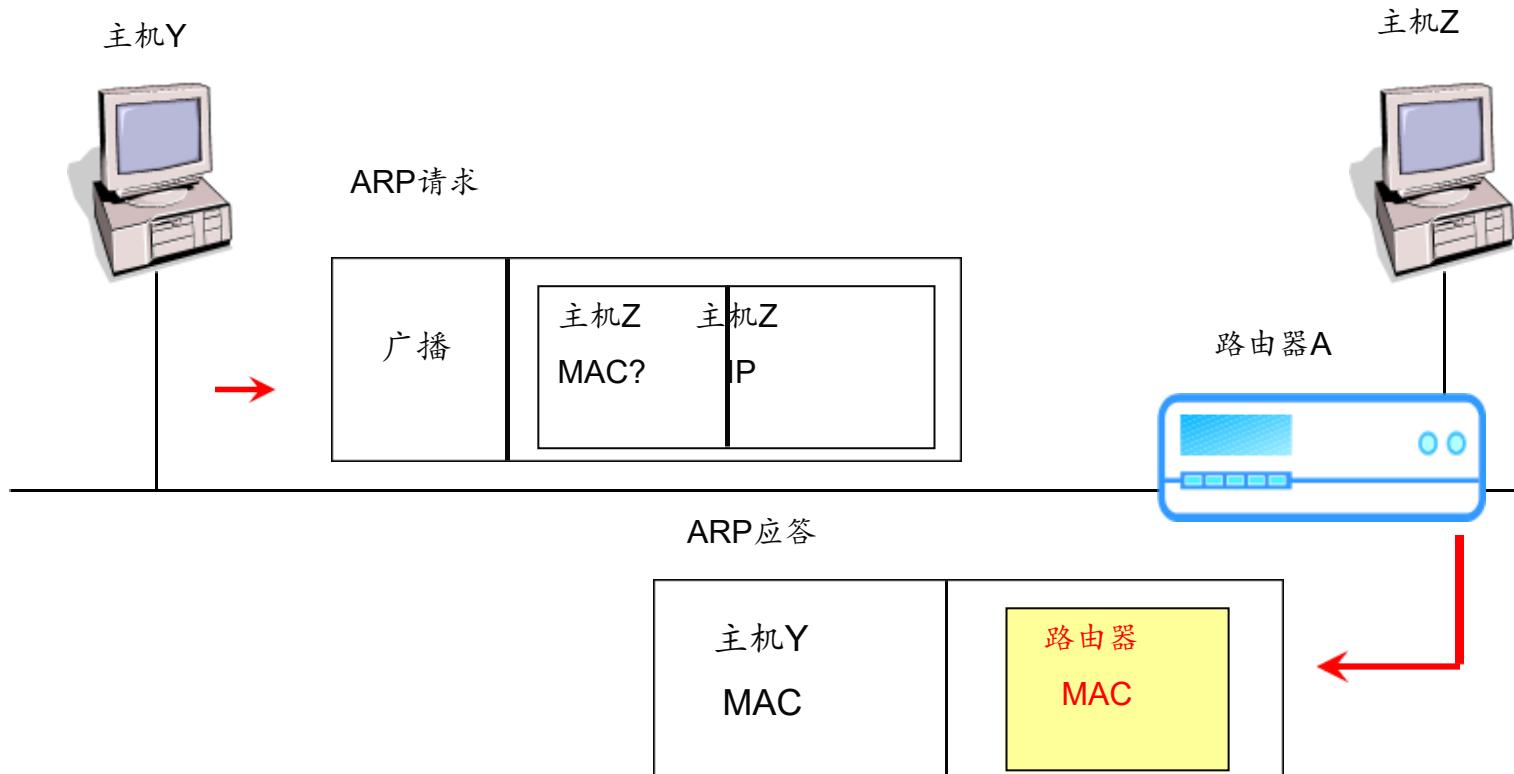
主机 B 向 A 发送
ARP 响应分组

我是 209.0.0.6
硬件地址是 08-00-2B-00-EE-0A



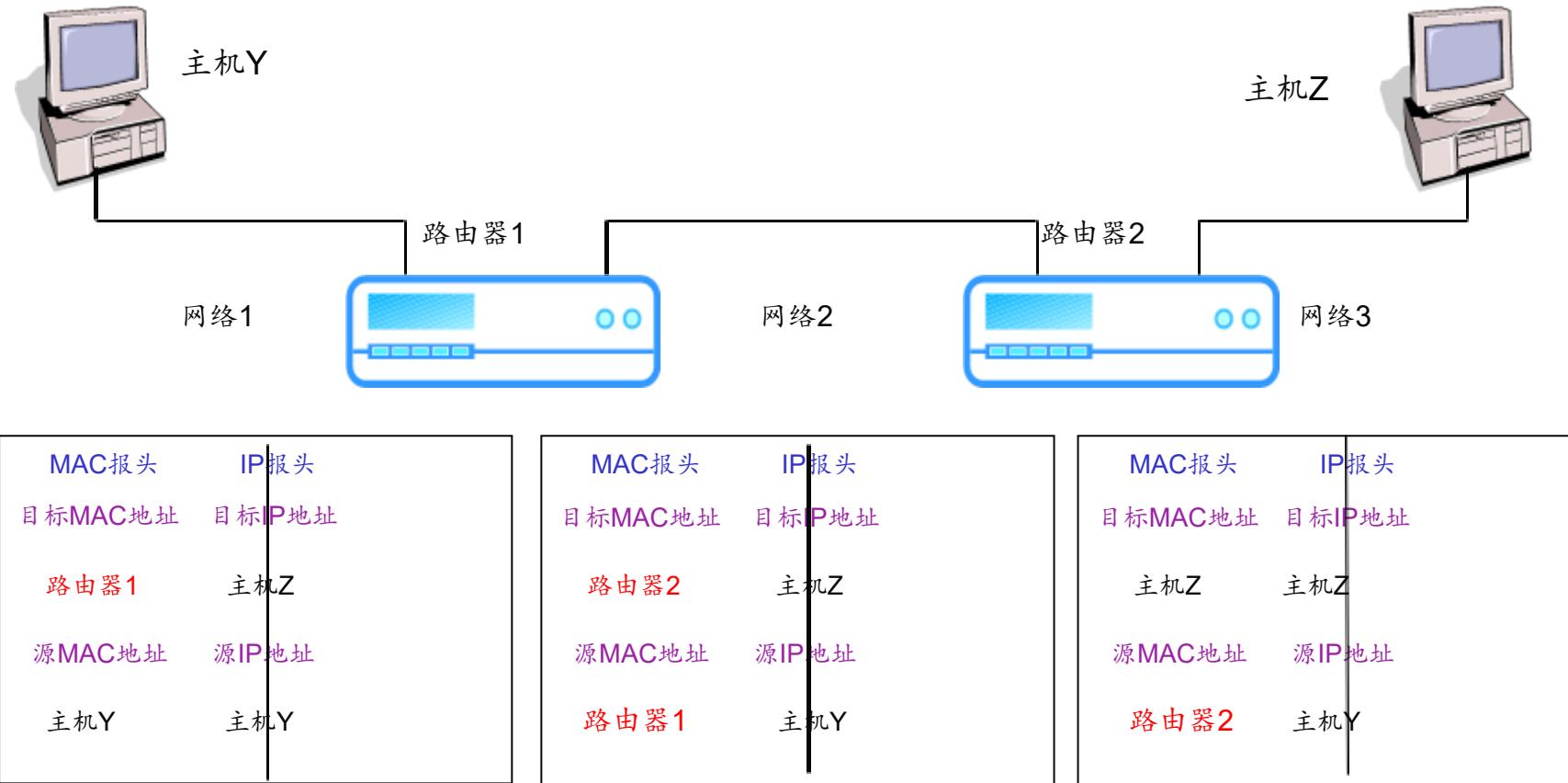
5.4 局域网

□ ARP协议：路由到其它LAN



5.4 局域网

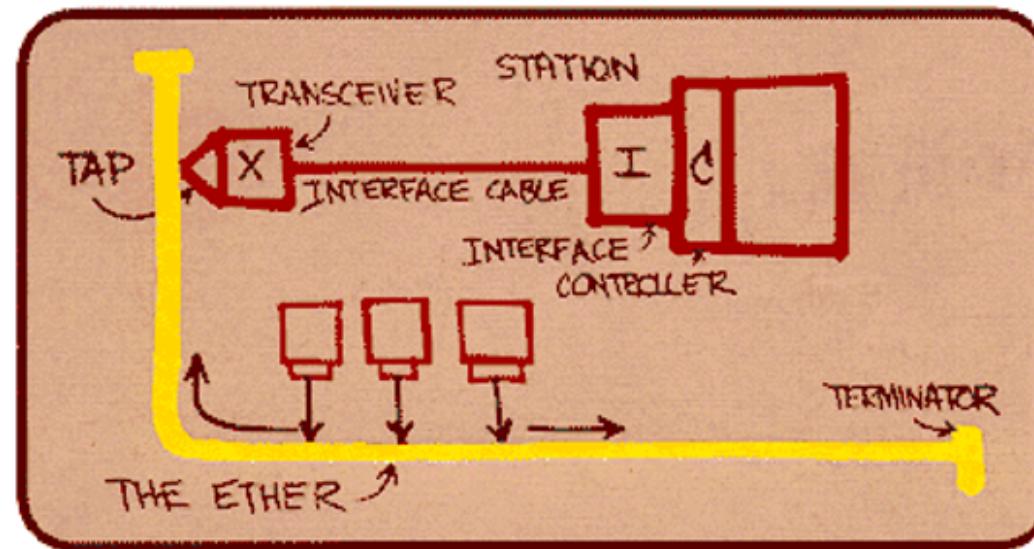
□ 互联网环境下的ARP



5.4 局域网

■ 以太网概述

- 20世纪70年代由Bob Matcalfe和David Boggs发明

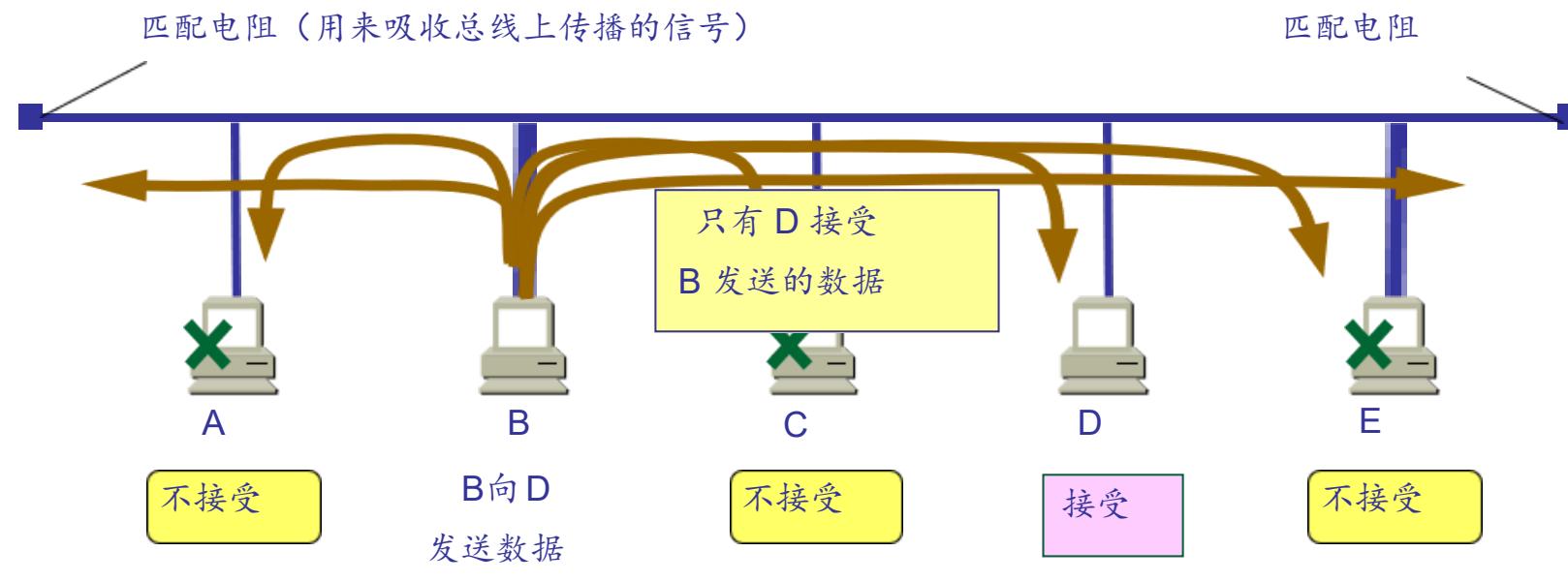


- 最先被广泛应用的局域网技术
- 便宜
- 速度：10Mbps->100Mbps->1Gbps->10Gbps

5.4 局域网

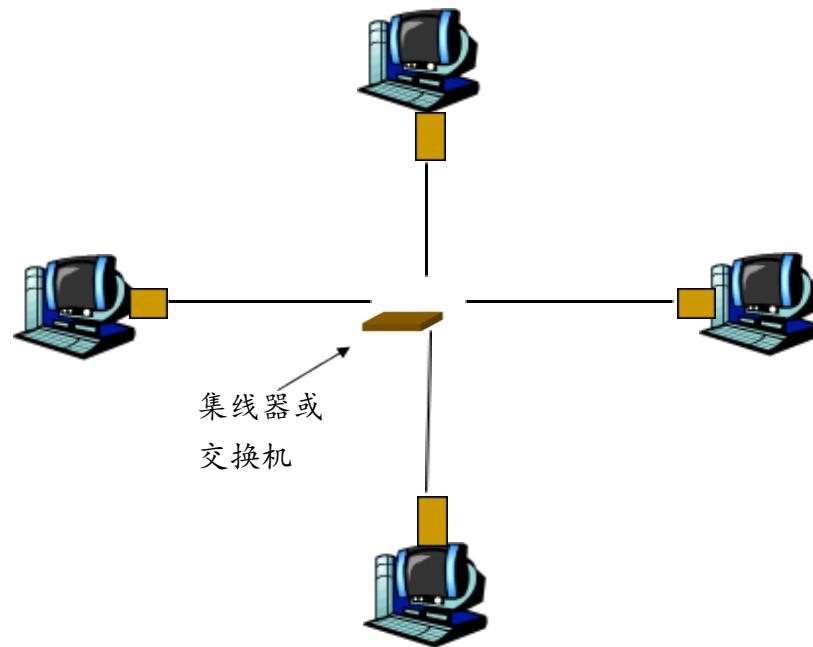
■ 以太网类型

□ 总线式以太网



5.4 局域网

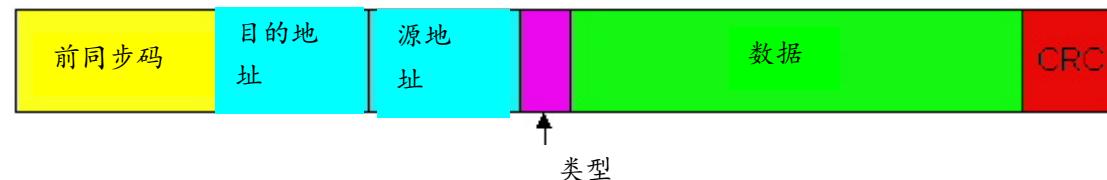
□ 交换式以太网



5.4 局域网

■ 以太网的帧结构

- 数据字段: (46字节, 1500字节)
- 前同步码:
 - 总共8字节, 前7字节的格式为 10101010 , 最后一个字节格式为10101011
 - 用于同步发送方与接收方时钟



5.4 局域网

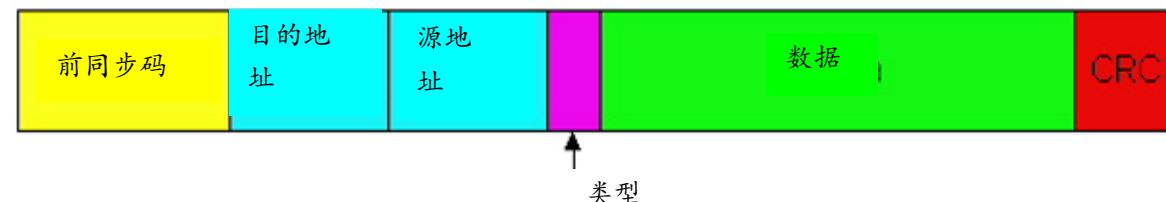
□ 地址: 6 字节

- 若适配器收到以太网帧，目的地址为自己的MAC地址或广播地址（如ARP包），就将帧中的数据传给网络层。
- 否则，适配器丢弃该帧

□ **类型:** 上层协议类型 (大多为IP协议，也支持其它协议如Novell IPX 和AppleTalk)

□ **CRC:** 由接收方检查,若检测到错误，就将该帧

丢弃



5.4 局域网

■ 以太网提供的服务

- **无连接服务:** 在送适配器和接收适配器之间不需要握手
- **不可靠服务:** 接收适配器不发送确认帧或否认帧给发送方
 - 交给网络层的数据报可能存在间隙
 - 若应用使用TCP, 间隙会被填充
 - 否则, 应用就会看见间隙

5.4 局域网

■ 以太网使用的CSMA/CD

□ 特点

- 没有时隙
- 当适配器侦听到其它适配器在传输，则它不传输帧，即**载波侦听**
- 正在传输的适配器若检测到其它适配器也在传输，则它中止自己的传输，即**碰撞检测**
- 在重新传输之前，适配器要等待一段随机时间，即**随机访问**

5.4 局域网

□ 算法

- 适配器收到来自网络层的数据报，创建帧
- 若适配器检测到信道空闲，则开始传输帧；若检测到信道忙，就开始等待，直到信道空闲再开始传输该帧
- 若适配器传输了整个帧而没有检测到其它适配器的传输，则该适配器完成该帧的传输
- 若适配器在传输时检测到其它适配器也在传输，则停止传输，发送拥塞信号
- 中止传输后，适配器进入指数回退阶段，在经历第 m 次碰撞后，适配器随机从 $\{0, 1, 2, \dots, 2^m - 1\}$ 中选择K值。适配器在等待 $K \cdot 512$ 比特时间后，返回第2步

5.4 局域网

□ 几个定义

- **拥塞信号:** 用来确保所有传输者都能检测到碰撞而传输的信号；48比特长
- **比特时间:** 传输1比特所需时间。在10Mbps的以太网中，当K=1023时，等待时间大约为50ms

5.4 局域网

□ 指数回退算法

- 目的: 适配器重传时试图估计正确的负载
 - 重载: 随机等待的时间可能会更长
- 第一次碰撞: 从 $\{0,1\}$ 中选择 K; 延迟是 $K \cdot 512$ 比特传输时间
- 第二次碰撞后: 从 $\{0,1,2, 3\}$ 中选择 K
- 第十次碰撞后: 从 $\{0,1,2,3,4,\dots,1023\}$ 中选择 K

5.4 局域网

□ 重要特性

- 使用 CSMA/CD 协议的以太网不能进行全双工通信而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。

5.4 局域网

□ 争用期长度

- 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 字节没有发生碰撞，则后续的数据就不会发生碰撞。

□ 最短有效帧长

- 如果发生碰撞，就一定是在发送的前 64 字节之内。
- 由于一检测到碰撞就立即中止发送，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**。

5.4 局域网

■ 传统以太网的物理层

以太网媒体接入控制 MAC

10BASE5

粗缆

10BASE2

细缆

10BASE-T

双绞线

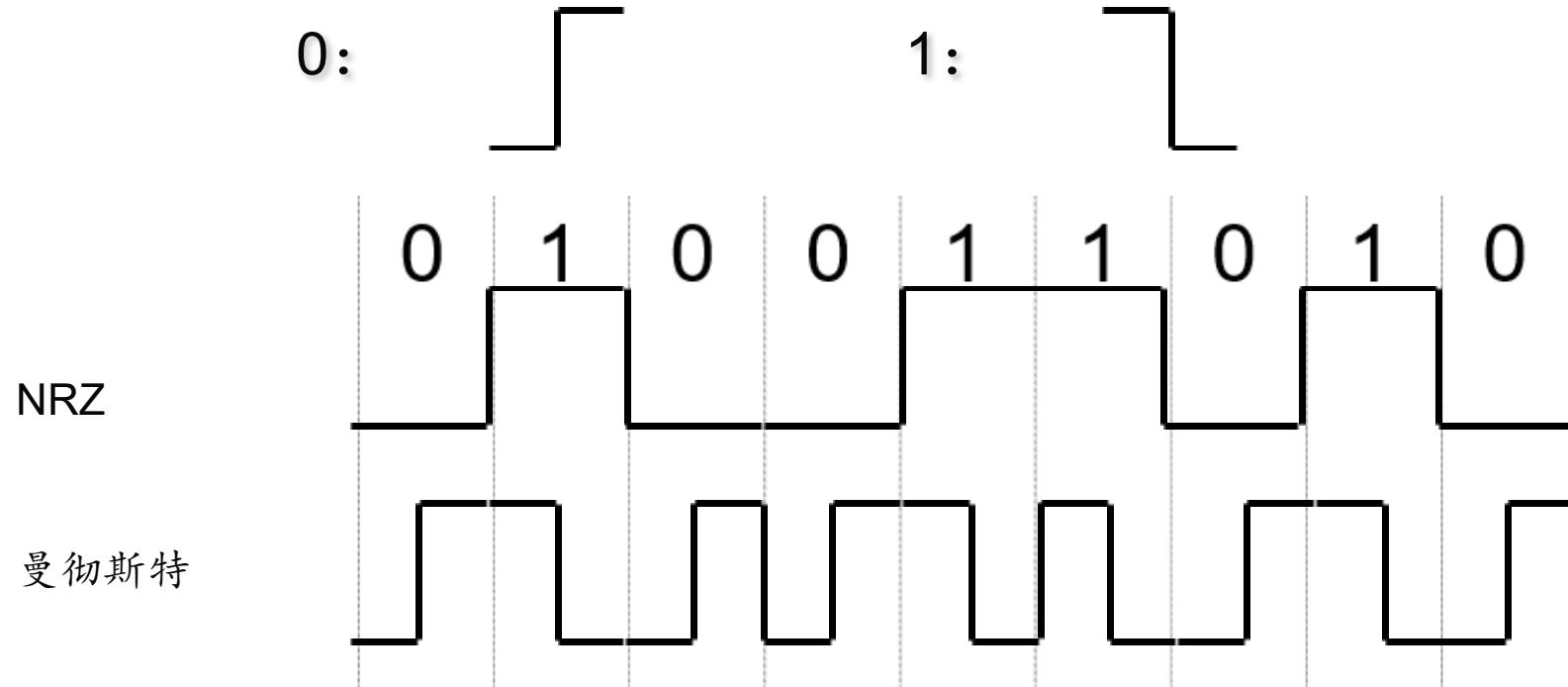
10BASE-F

光缆

5.4 局域网

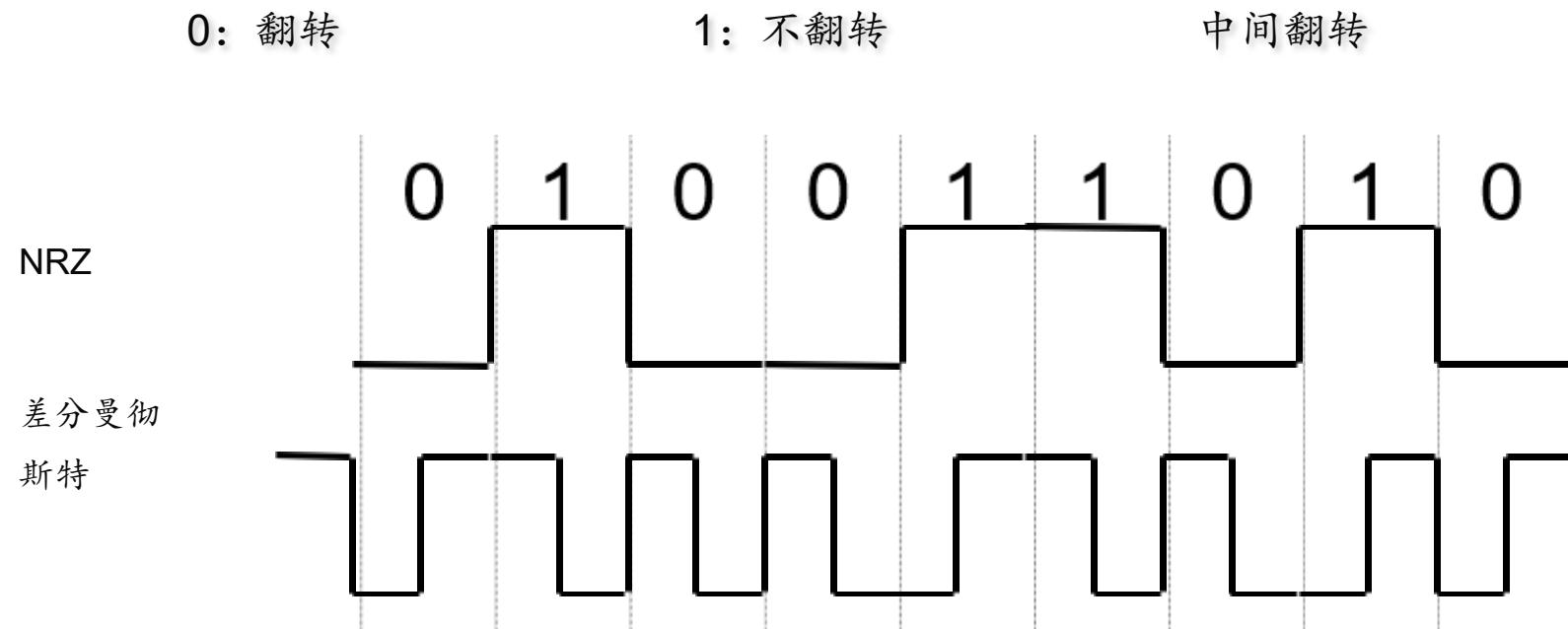
■ 信号编码

□ 曼彻斯特编码



5.4 局域网

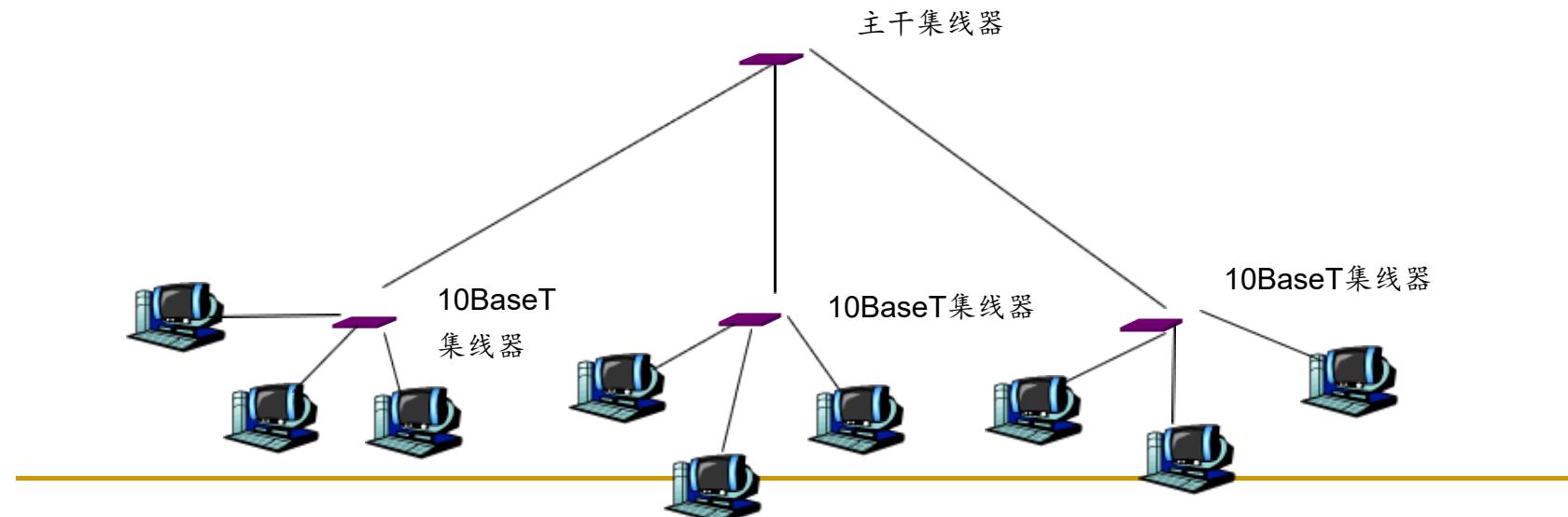
□ 差分曼彻斯特编码



5.4 局域网

■ 集线器（或转发器）互联

- 主干集线器将LAN网段互联起来
- 扩展了节点间的最大距离
- 原先独立的网段碰撞域变成了一个大的碰撞域
- 不能将10BaseT 和 100BaseT以太网互联



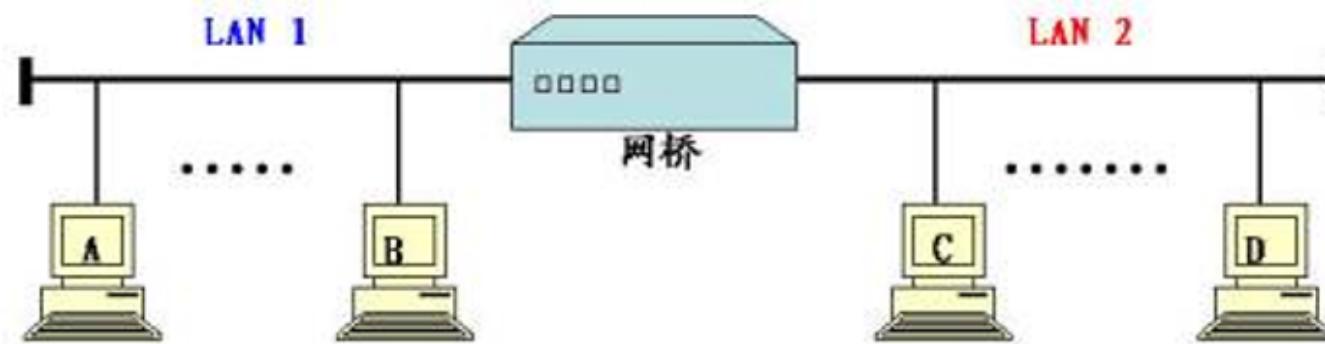
2020年11月10日

66

5.4 局域网

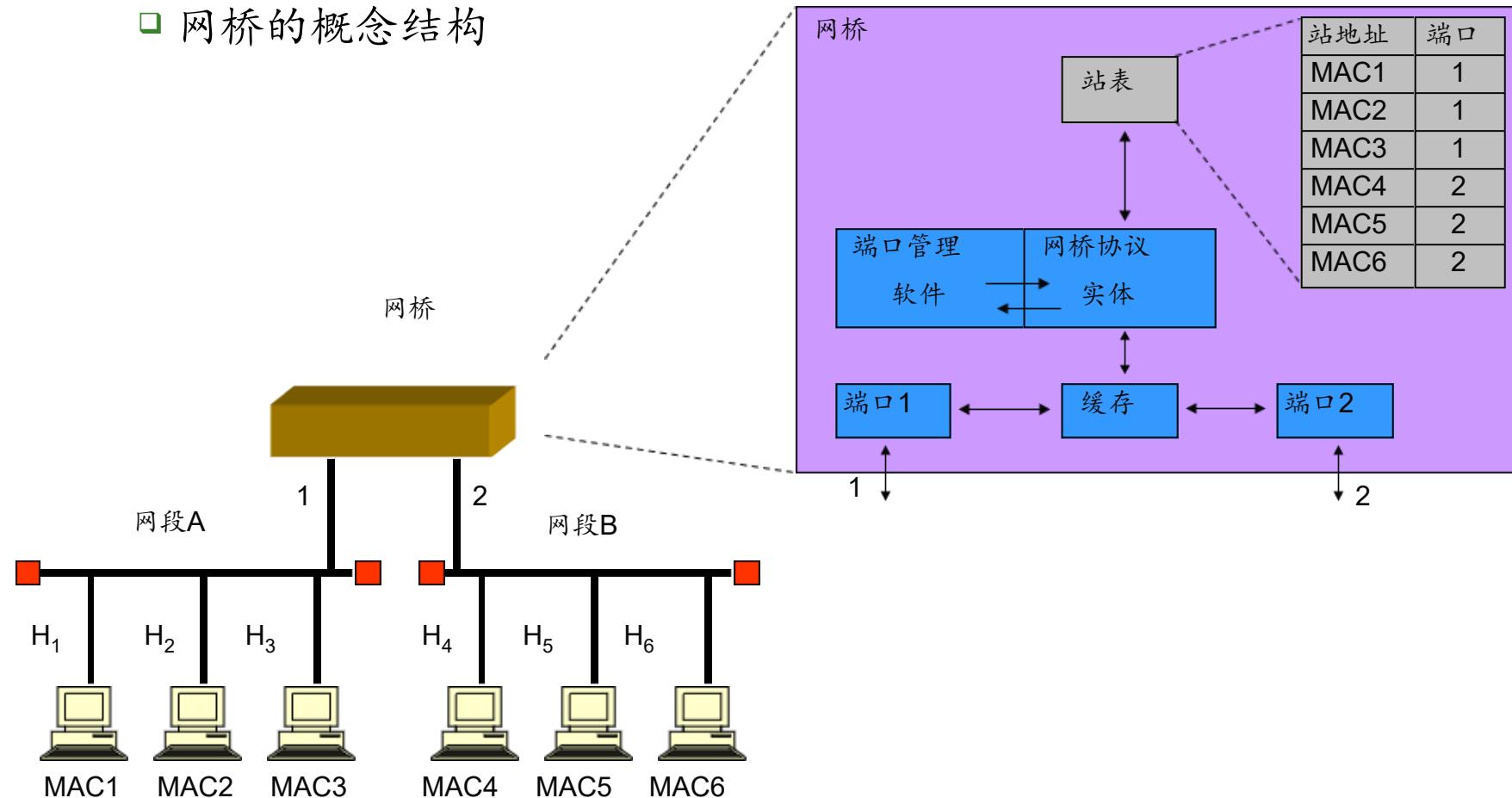
■ 网桥互联

- 网桥（Bridge）实质上就是一种存储—转发设备，用来实现MAC层的LAN互连



5.4 局域网

网桥的概念结构



5.4 局域网

□ 网桥的工作原理

- 不断监听各端口是否有信号
- 收到无差错的帧则缓存，反之将差错帧丢弃
- 若所收帧的目的MAC地址属另一网段，则通过站表决定向何端口转发
- 网桥不转发同一网段内通信的帧
- 网桥不修改所转发的帧的源地址

5.4 局域网

□ 网桥的优势

- 过滤通信量
- 扩大了局域网的物理范围
- 提高了可靠性
- 可互连不同物理层、不同MAC子层和不同速率的
局域网

5.4 局域网

□ 网桥的缺点

- 由于要接收和转发，**增加了时延**
- MAC子层没有流量控制功能，网络负荷重时，网桥缓存空间可能发生溢出，产生**帧丢失**现象
- 不同MAC子层的网段桥接时，在转发帧之前要修改帧的某些字段，这也需要**耗费时间**
- 出现**广播风暴**。网桥只适合用户少于几百个和通信量不太大的局域网，否则有时会因传播过多广播信息而产生网络拥塞

5.4 局域网

□ 网桥和集线器的区别

- 集线器只是将网络的覆盖距离简单的延长，而且距离有限，具体实现在物理层；网桥不仅具有将LAN的覆盖距离延长的作用，而且理论上可做到无限延长，具体实现MAC层。
- 集线器仅具有简单的信号整形和放大的功能；网桥则属于一种智能互连设备，它主要提供信号的存储/转发、数据过滤、路由选择等能力。
- 集线器仅是一种硬设备，而网桥既包括硬件又包括软件。
- 集线器仅只能互连同类LAN，而网桥可支持不同类型的LAN互连。

5.4 局域网

□ 透明网桥

- 这里所谓“**透明**”是指局域网上的每个站并不知道所发送的帧将经过哪几个网桥，即网桥对各站来说是看不见的



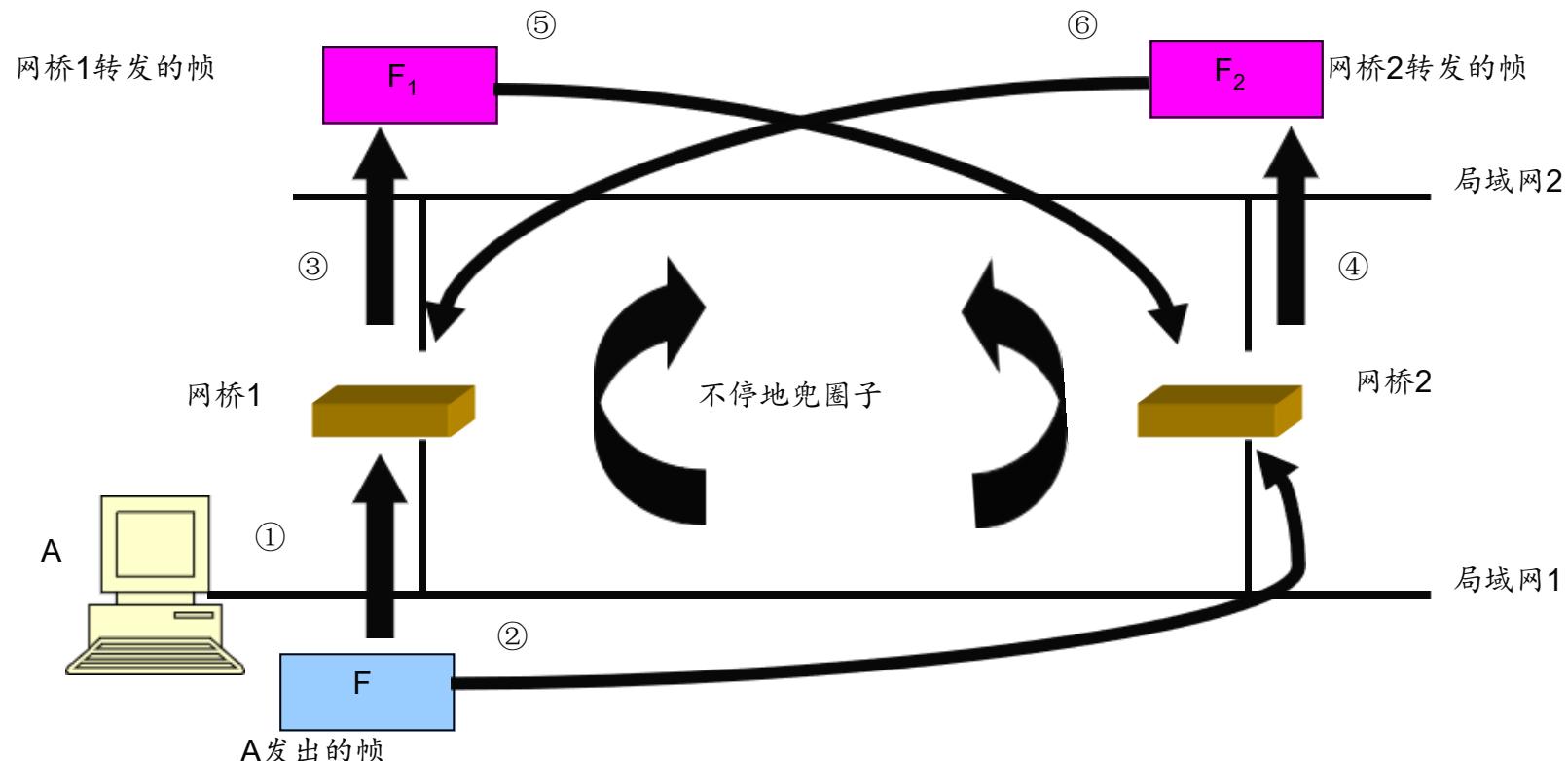
5.4 局域网

□ 透明网桥选路原理

- ① 从端口x收到帧，有差错则丢弃，否则在站表中查找目的站MAC地址；
- ② 找到有，则取出相应的端口d，转③，否则转⑤；
- ③ 如果所给MAC地址的端口d=x，则丢弃此帧（不需要转发），否则从端口d转发此帧；
- ④ 转到⑥；
- ⑤ 向网桥除x以外的所有端口转发此帧（可保证找到目的站）
- ⑥ 如源站不在站表中，则将源站MAC地址写入站表，登记该帧进入网桥的端口号和时间，设置计时器，然后转⑧。否则转⑦；
- ⑦ 更新计时器（由于网络拓扑经常变化，因此，超时记录要删除，以反映最新状态）；
- ⑧ 等待新的数据帧。转①

5.4 局域网

□ 透明网桥存在的问题——兜圈子



5.4 局域网

□ 解决方案——支撑树算法

- 互连在一起的网桥彼此通信后，就能找出原来的网络拓扑的一个子集，在这个子集里整个连通的网络中不存在回路。一旦支撑树确定了网桥就会将某些端口断开，以确保从原来的拓扑得出一个支撑树
- 支撑树算法选择一个网桥为树的根，然后以最短路径为依据，找到树上的每一个结点
- 为了让支撑树能反映网络拓扑的变化，每隔几秒钟每一个网桥要广播其标识号，和它所知道的所有其他网桥

缺点：互连局域网数目非常大时，支撑树算法可能花很多时间。

5.4 局域网

■ 以太网交换机——多端口网桥

□ 链路层设备

- 存储和转发以太网帧
- 检查帧头部，根据目的MAC地址转发帧
- 当帧转发到LAN网段，用CSMA/CD 访问 LAN网段

□ 透明

- 主机不知道交换机的存在

□ 即插即用，自学习

- 交换机不需配置

□ 直通交换：帧从入端口转发到出端口不需收集整个帧

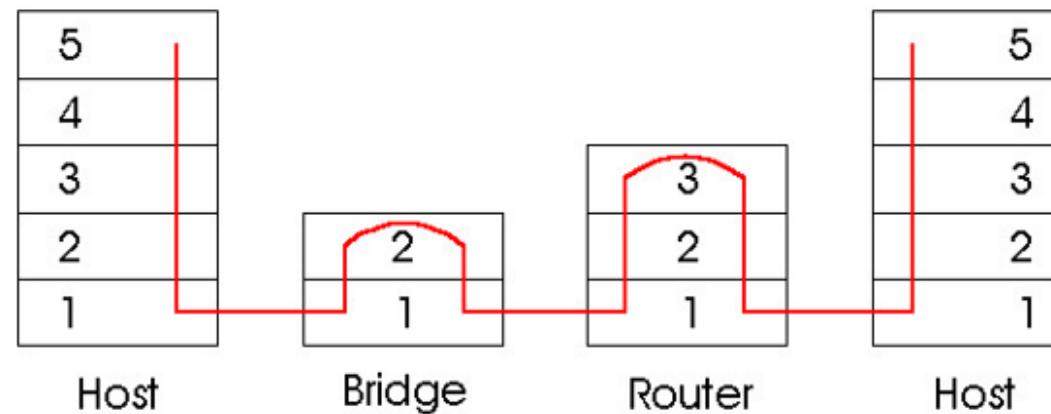
- 能少量减少延迟

□ 共享/专用的、10/100/1000Mbps接口的结合

5.4 局域网

■ 以太网交换机 vs 路由器

- 两者都是存储转发设备
 - 路由器：网络层设备（检查网络层头部）
 - 交换机是链路层设备
- 路由器维护路由表，实现路由算法
- 交换机维护交换表，实现MAC地址过滤、学习算法



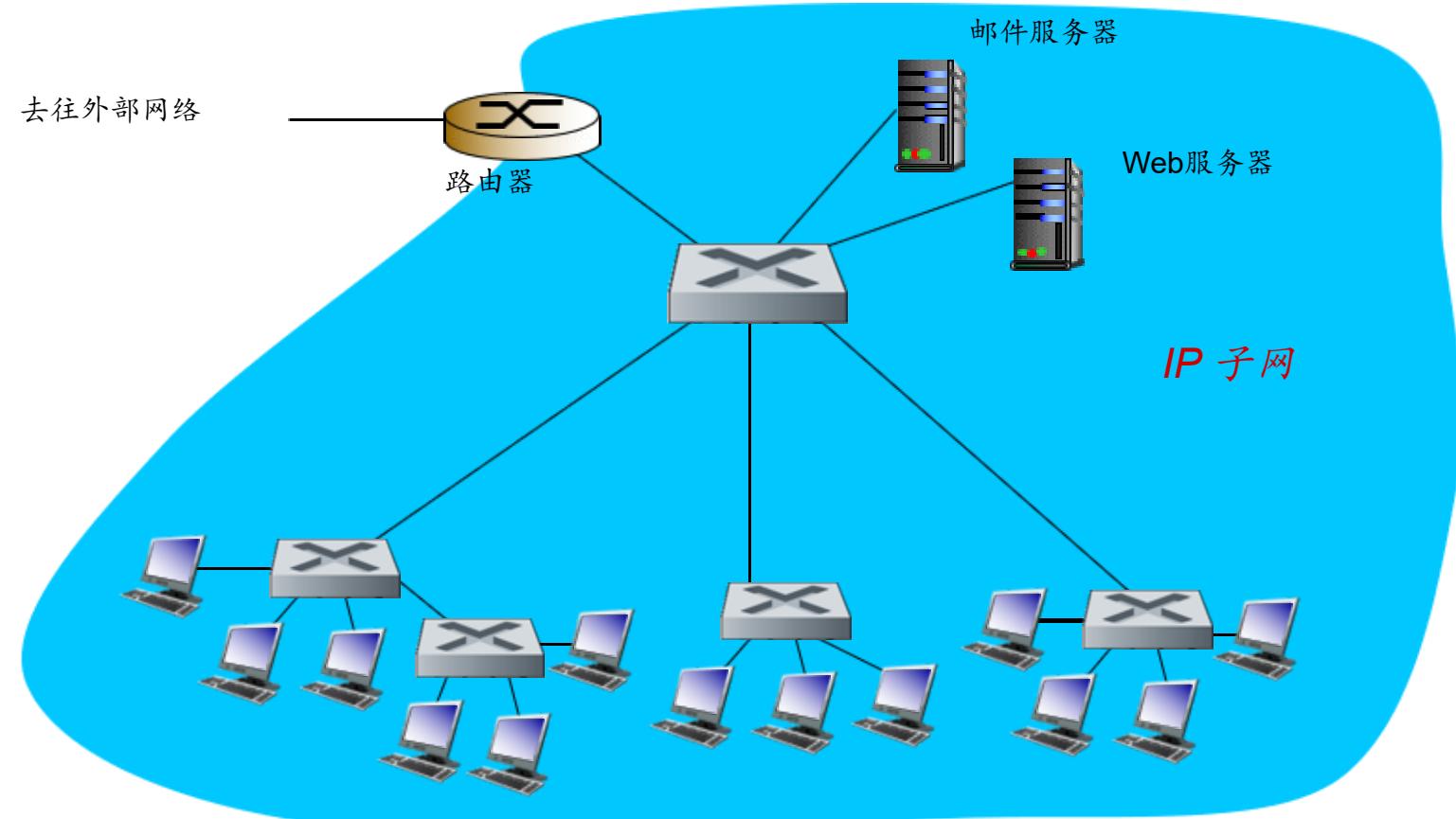
5.4 局域网

■ 集线器 vs 以太网交换机 vs 路由器

	集线器	路由器	交换机
流量隔离	无	有	有
即插即用	有	无	有
优化选路	无	有	无
直通交换	有	无	有

5.4 局域网

■ 一般的企业网络



5.4 局域网

■ 虚拟局域网VLAN

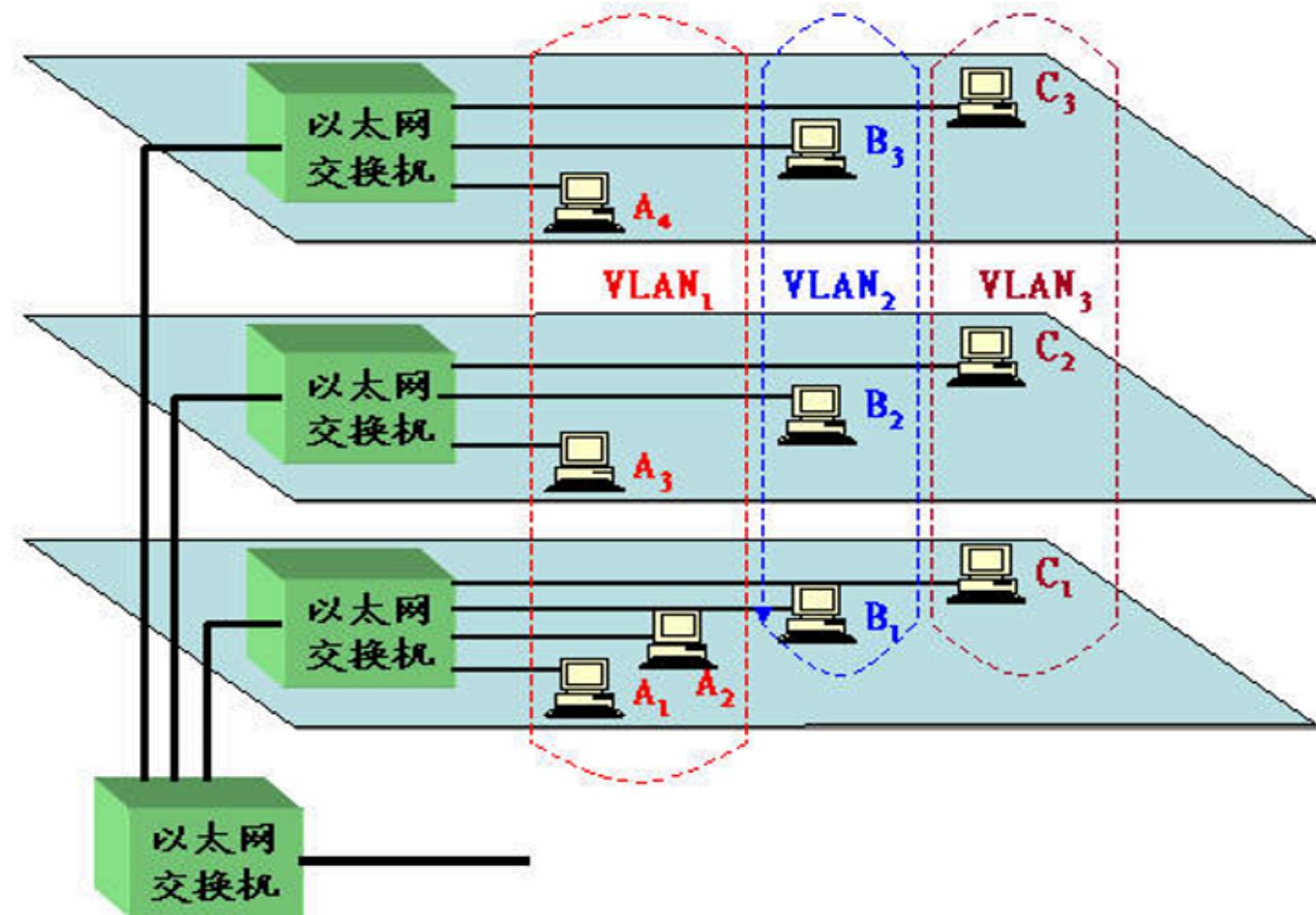
□ 概念——虚拟局域网VLAN（Virtual LAN）是指以软件方式来实现逻辑工作组划分与管理的一种网络工作组组建技术。

□ 特征

- 局域网交换机是组建虚拟局域网的核心设备。
- 组成逻辑工作组的各结点不受物理位置的限制，换言之同一逻辑工作组的成员不一定要连接在同一个物理网段上。
- 当一个结点从一个逻辑工作组转移到另一个逻辑工作组时，只需要通过软件设定，而不需要改变它在网络中的物理位置。

5.4 局域网

示例



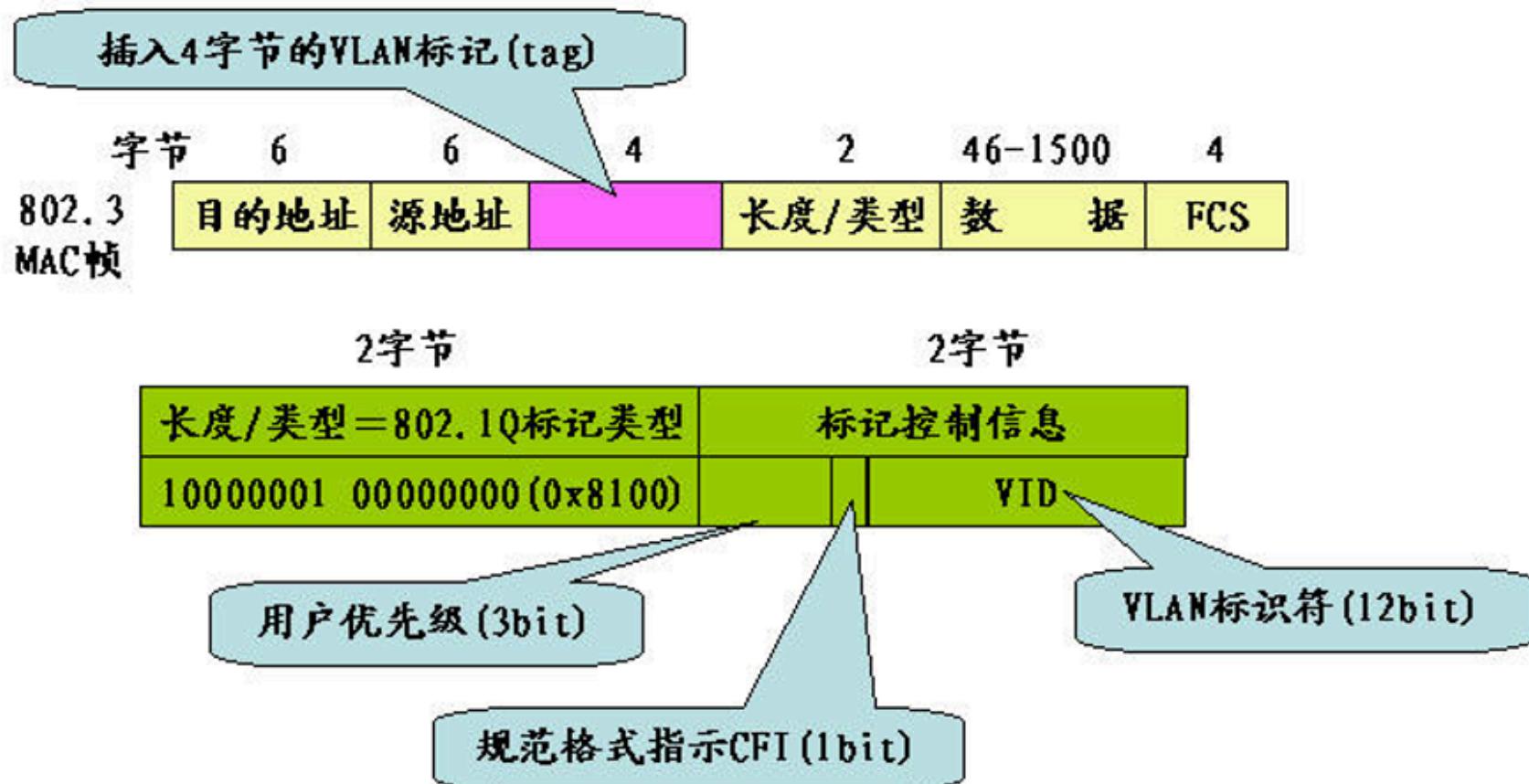
5.4 局域网

□ 构建方式

- 基于交换机端口号
- 基于MAC地址
- 基于IP地址

5.4 局域网

□ 基于802.1Q的VLAN帧格式



额外的例子：PPP 点对点协议

■ 点到点数据链路控制

□ 一个发送方，一个接收方，一条链路，比广播

链路更容易实现

- 没有媒体访问控制
- 不需要 MAC 地址
- 如：拨号链路，ISDN 电路

□ 流行的点到点协议

- PPP (point-to-point protocol)
- HDLC: High level data link control (数据链路被认为
是协议栈中的高层)

额外的例子：PPP 点对点协议

■ PPP设计要求[RFC 1547]

- **分组成帧：**网络层的数据报封装成帧的数据
 - 携带任意网络层协议（不仅仅IP）的网络层数据
 - 有向上分用的能力
- **比特透明：**携带的数据可以是任何比特模式的
- **差错检测（不纠错）**
- **连接的活性：**检测链路层故障，并向网络层通知该差错情况
- **网络层地址协商：**端点能获知/配置相互通信的网络层地址

额外的例子：PPP 点对点协议

■ PPP不要求实现

- 错误纠错/恢复
- 流量控制
- 有序
- 多点链路 (如：轮询)

错误恢复，流量控制，数据排序交给上层处理

额外的例子：PPP 点对点协议

■ PPP数据帧格式

- **标志:** 分隔符 (标志帧的开始和结束)
- **地址:** 没有用 (只是一个选项)
- **控制:** 没有用; 今后可能使用控制域
- **协议:** 帧中封装的数据所属的上层协议 (如PPP-LCP, IP, IPCP等)
- **信息:** 携带的上层数据
- **校验和:** 用于差错检测的循环冗余校验和



额外的例子：PPP 点对点协议

■ 字节填充

- “数据透明” 要求：数据域可以使用标志字段的值 $<01111110>(7E)$

■ Q: 收到的 $<01111110>(7E)$ 是数据还是标志？

- 发送方

- $<01111110>(7E) \longrightarrow <01111101\ 01011110>(7D\ 5E)$
- $<01111101>(7D) \longrightarrow <01111101\ 01011101>(7D\ 5D)$

- 接收方

- 反之即可

额外的例子：PPP 点对点协议

■ PPP数据控制协议

□ 链路创建

■ LCP配置请求帧

□ 链路最大帧长度、使用的认证协议……

■ 配置确认帧

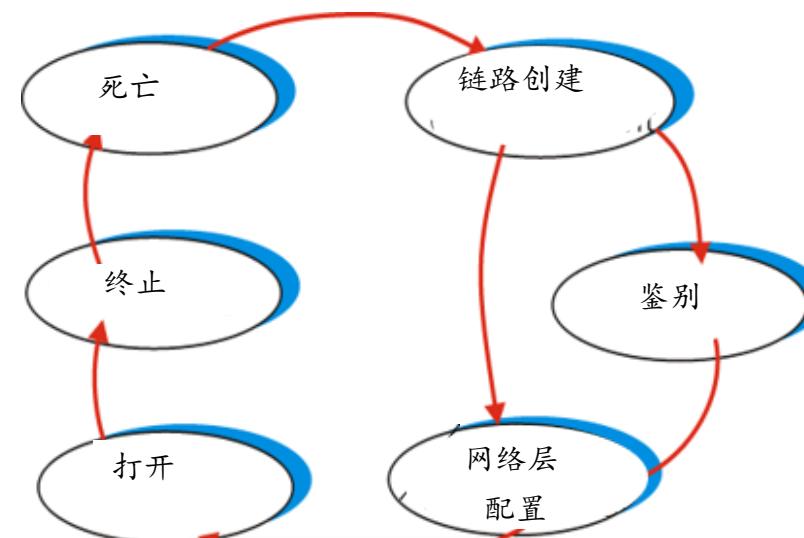
■ 配置否认帧

■ 配置拒绝帧

□ 网络层配置

■ 双方网络层模块协商地址

及相关配置



第五章: 总结

- 数据链路层服务原理:
 - 错误检测, 纠错
 - 共享广播信道: 多路访问
 - 链路层寻址
- 不同链路层技术示例和实现
 - 以太网
 - 交换局域网
 - PPP

课后思考题

- 复习题 2、4、6、10、12
- 习 题 5、9、14~19