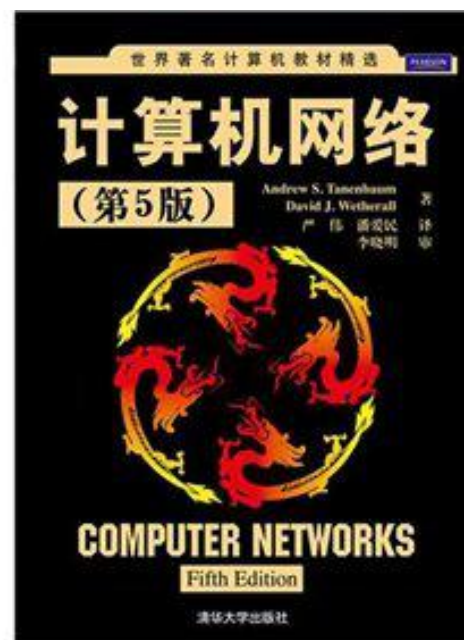


计算机网络

Andrew S. Tanenbaum (5 Edition)



1



安徽大学 互联网学院
School of Internet Anhui University

数字调制与多路复用

- **基带传输**：信号传输占据传输介质上从0到最大值的所有频率。
- 基带信号往往包含有较多的低频成分，甚至有直流成分，而许多信道并不能传输这种低频分量或直流分量。因此必须对基带信号进行**调制**或**编码**。
- **通带传输**：把基带信号经过载波调制后，把信号的频率范围搬移到较高的频段以便在信道中传输（即仅在一段频率范围内能够通过信道）。

计算机网络

第1章 引言

第2章 物理层

第3章 数据链路层

第4章 介质访问控制子层

第5章 网络层

第6章 传输层

第7章 应用层

第8章 网络安全



第4章 介质访问控制子层

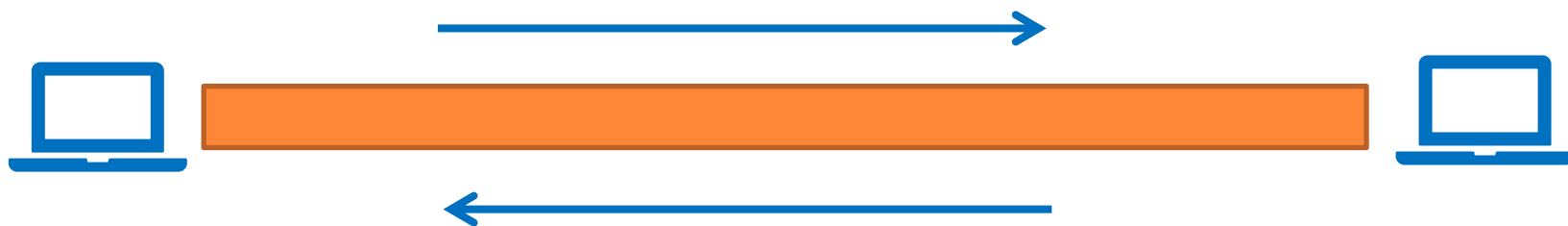


- 4.1 信道分配问题
- 4.2 多路访问协议
- 4.3 以太网
- 4.4 无线局域网
- 4.5 宽带无线
- 4.6 蓝牙
- 4.7 RFID
- 4.8 数据链路交换

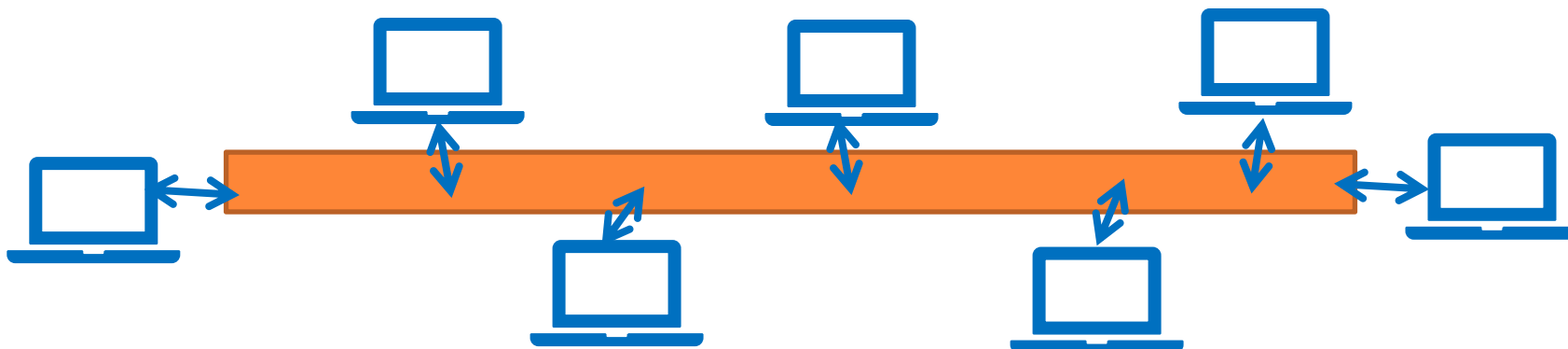


介质访问控制子层

- 之前的协议主要考虑发送-接收双方的协调



- 链路层使用的通信，可能存在多个节点共用一个信道的问题
。需要在网络中多个节点进行



4.1 信道分配技术

- 静态信道分配
- 多路复用技术存在的问题：如果流量数据呈突发性，分配的信道会被浪费。广播 vs 互联网
- 按照排队论计算结果，帧的平均时延 $T = 1/(\mu C - \lambda)$
- 如果按照复用方式均分信道，帧的平均时延 $T = N/(\mu C - \lambda)$
- 两者相差 N 倍。



4.1 信道分配技术

- 动态信道分配的几个假设
- 流量独立： N 个站点之间相互独立，期望帧数为 λ ，服从泊松分布。
- 单信道：所有站点共用一个信道
- 冲突可观察：两帧同时传输会相互干扰，称为冲突。所有站点可检测到信道里的冲突。
- 时间连续或分槽：时间连续
- 载波侦听或不听：载波侦听表明站点发送数据前会检测信道是否空闲或忙（被使用）反之不检测。



4.2 多路访问协议

∞ ALOHA

- 纯ALOHA

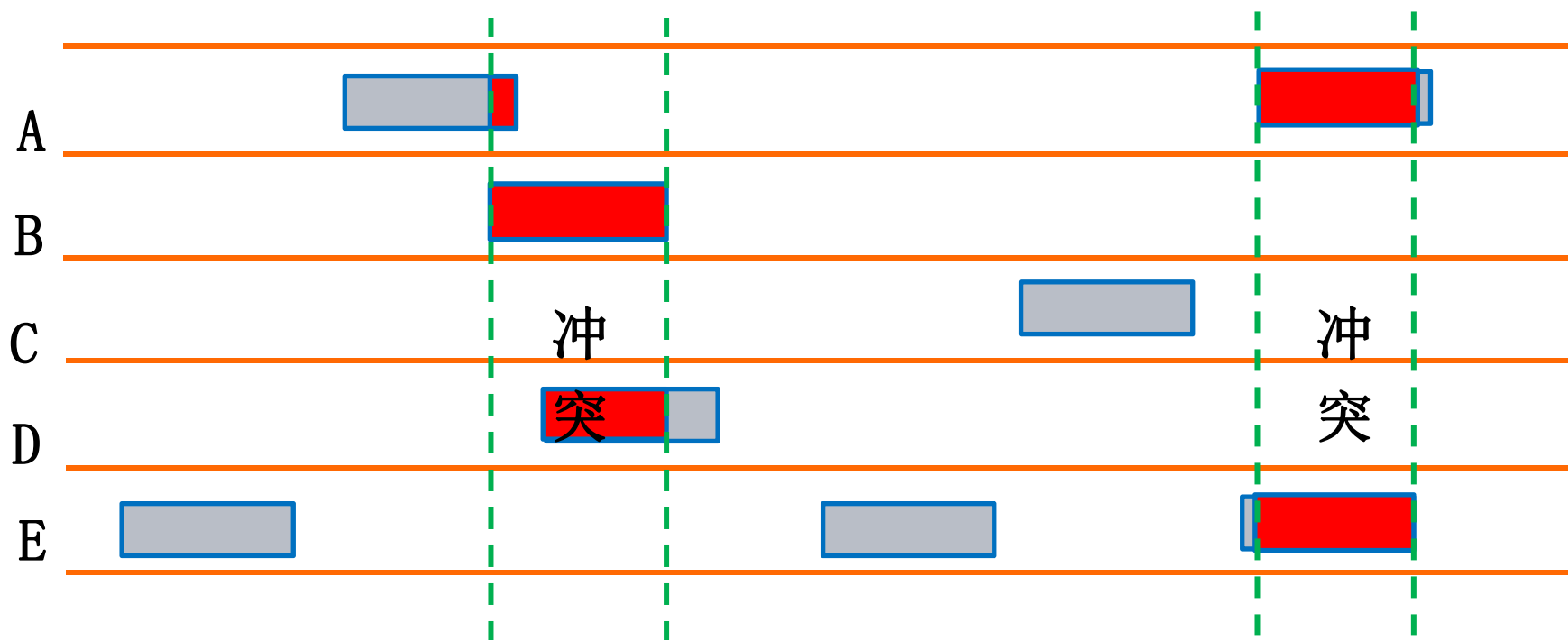
- 分槽ALOHA



4.2 多路访问协议

❧ 纯ALOHA

- ❧ 基本思想：当用户有数据需要发送时就传输。
- ❧ 多个用户共享一个信道会产生冲突，这样的系统称为竞争系统。
- ❧ 帧的发送次序是任意的

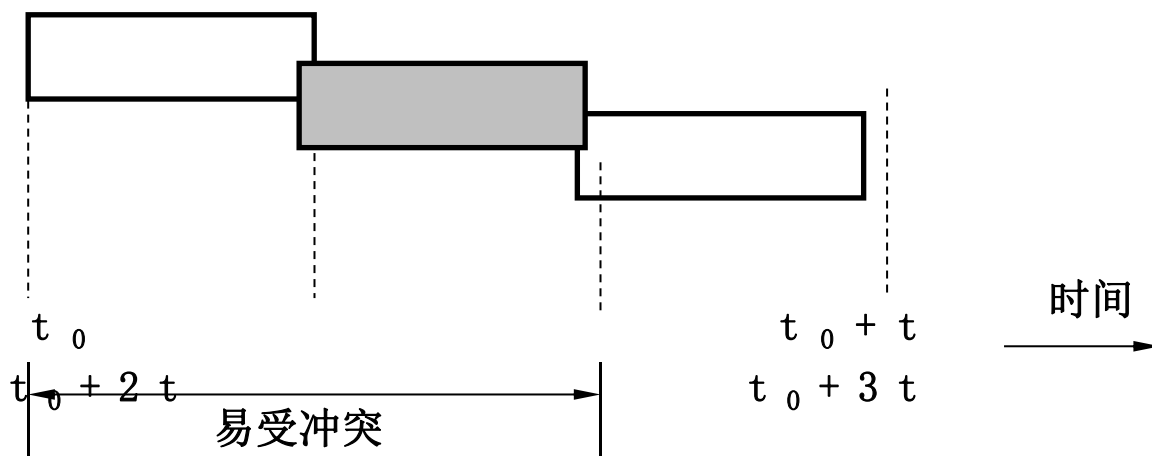


4.2 多路访问协议

纯ALOHA的原理

在纯ALOHA中，站点一旦产生新帧则立即发送，如果一个标准长度的帧的发送时间为 t ，在 t_0+t 时刻允许生成一个新帧，除此新帧之外，在 $t_0 \sim t_0+2t$ 时间内不能有其它帧产生，否则冲突，即冲突危险区为 $2t$

- 当网络比较闲时，效率较好
- 当网络较忙时，会频繁发生冲突。这种冲突时的信道的利用率只能达到18%



4.2多路访问协议

纯ALOHA

- 帧时：传输一个标准的、固定长度的帧所需要的时间（即帧的长度除以比特率）
- 可以把纯ALOHA的发送过程看出每帧时中发送帧数量期望为 G 的泊松分布，而网络吞吐量 $S = GP_0$, 因此有：

$$P_r[k] = \frac{G^k e^{-G}}{k!}$$

可见，在整个易冲突期内不发送帧的概率是 $P_0 = e^{-2G}$, 因此有：

$$S = GP_0 = Ge^{-2G}$$

4.2多路访问协议

分槽ALOHA

- 基本思想：将时间分成离散的间隔，称为时间槽
- 每个时间槽对应传输一帧
- 要求用户遵守统一的时间槽边界
- 系统容量增加一倍 $S = Ge^{-G}$ 。
- 冲突概率为 $1 - e^{-G}$ ，k次成功率为 $P_k = e^{-G}(1 - e^{-G})^{k-1}$
- 每帧传输次数期望 $E = \sum_{k=1}^{\infty} kP_k = e^G$
- 分槽ALOHA对于共享竞争信道（例如：REID、蓝牙）有很好的应用价值



4.2 多路访问协议

ALOHA

- 纯ALOHA：当用户有数据需要发送时就传输
- 分槽ALOHA：时间被分成离散槽，所有帧都必须同步到时间槽中
- 在简单网络中，纯ALOHA具有优势；复杂网络中，基站多，分槽频繁，分槽ALOHA具有优势。

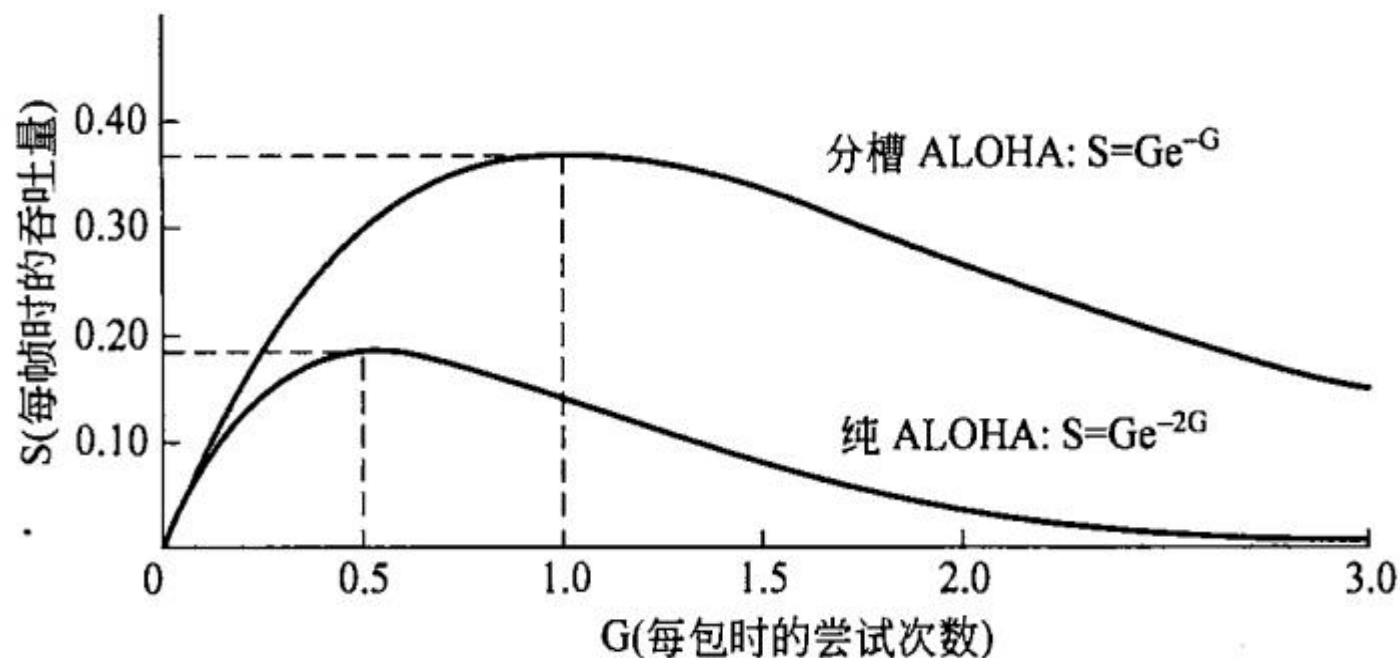


图 4-3 ALOHA 系统的吞吐量与负载的关系

4.2 多路访问协议——载波侦听多路访问协议 CSMA

- 载波侦听协议定义：如果一个协议中，站监听是否存在载波（即是否有传输），并据此采取相应的动作，称为**载波侦听协议**。
- 1 – 坚持CSMA
- 非坚持CSMA
- p – 坚持CSMA（适用于分时间槽信道）



4.2 多路访问协议

载波侦听多路访问协议CSMA

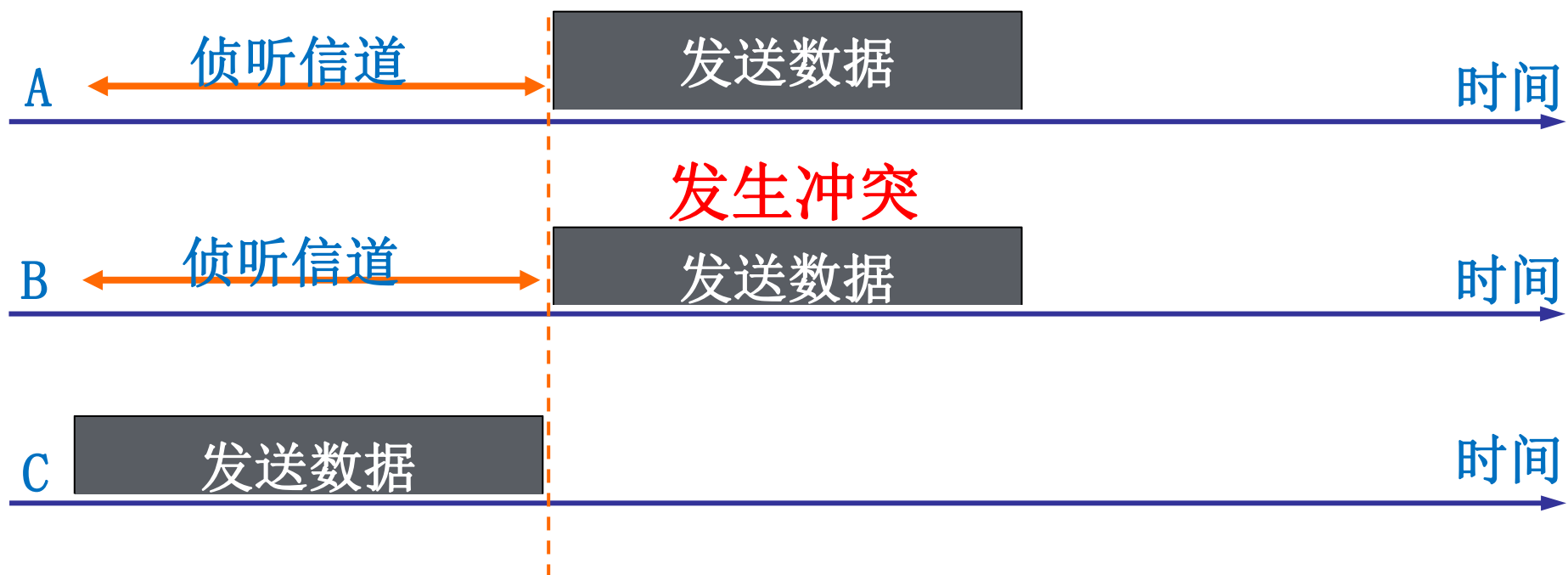
- **1 – 坚持CSMA**
- 每个站在发送前，**先侦听**信道，如信道正忙(其他站点在发送数据)，则**等待**并持续侦听，**如果信道空闲，就发送数据**（发送的概率为**1**）。如果发生冲突，则等待一段随机时间后，重新发送。
- **存在的问题**
- 如果两个站点在信道忙时，都等待发送数据，一旦信道空闲，两者同时发送，导致冲突发生。



4.2 多路访问协议

载波侦听多路访问协议CSMA

○ 1 – 坚持CSMA



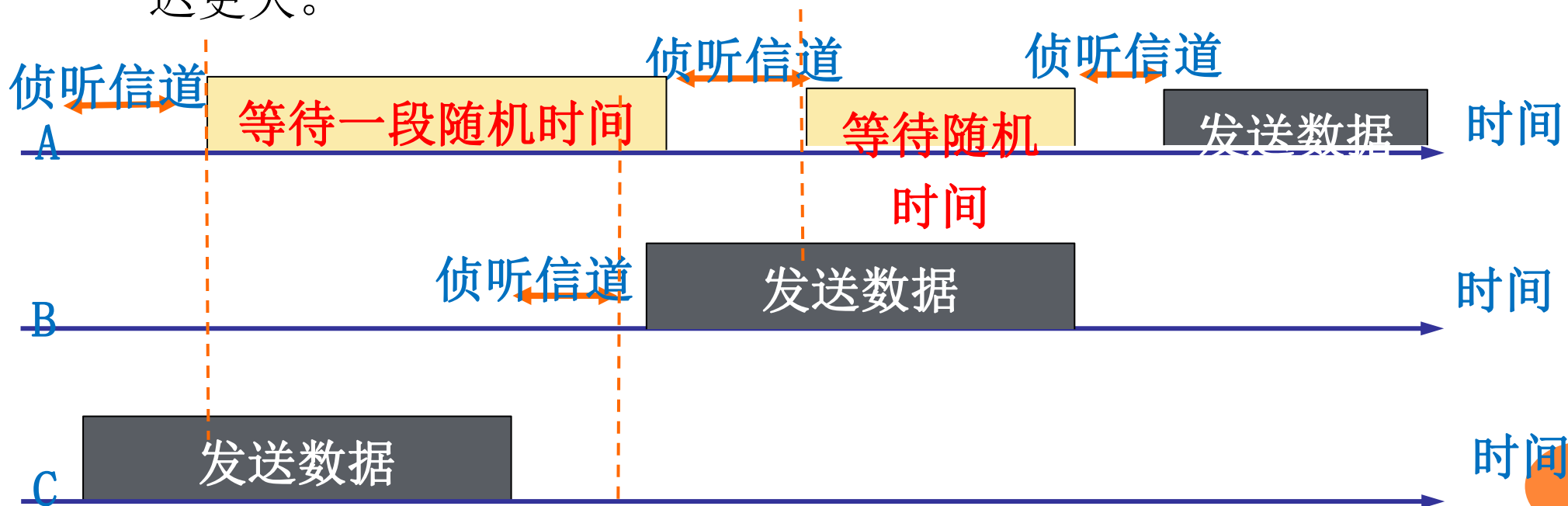
4.2 多路访问协议

载波侦听多路访问协议CSMA

- 非坚持CSMA

每个站在发送前，先侦听信道，如信道正忙，则不再继续侦听，而是等待一段随机时间后，再侦听信道。

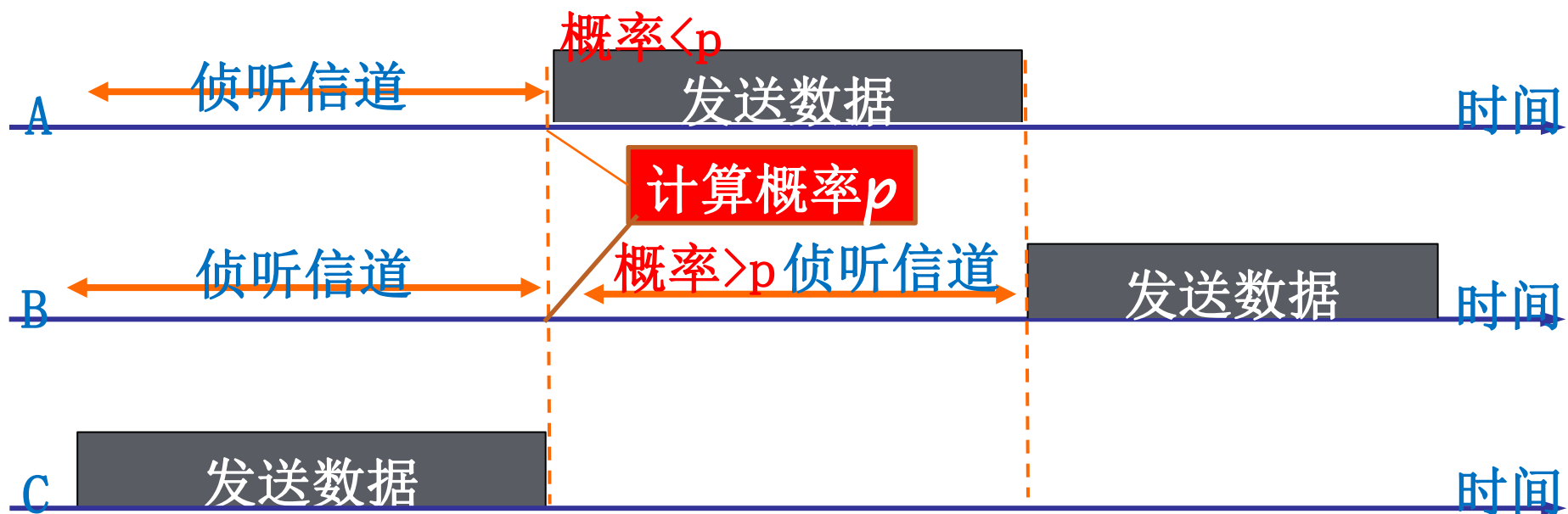
- 一定程度上能避免空闲时几个站同时发送的问题，但延迟更大。



4.2 多路访问协议

载波侦听多路访问协议 CSMA

- p - 坚持 CSMA
- 先侦听信道，如信道正忙，则等待到下一时间槽；如信道空闲，则以概率 p 发送，而以概率 $q=(1-p)$ 把本次发送延至下一时间槽，直至发送成功。
- 结合了上述两种协议的优点。



4.2 多路访问协议

载波侦听协议定义：如果一个协议中，站监听是否存在载波（即是否有传输），并据此采取相应的动作。

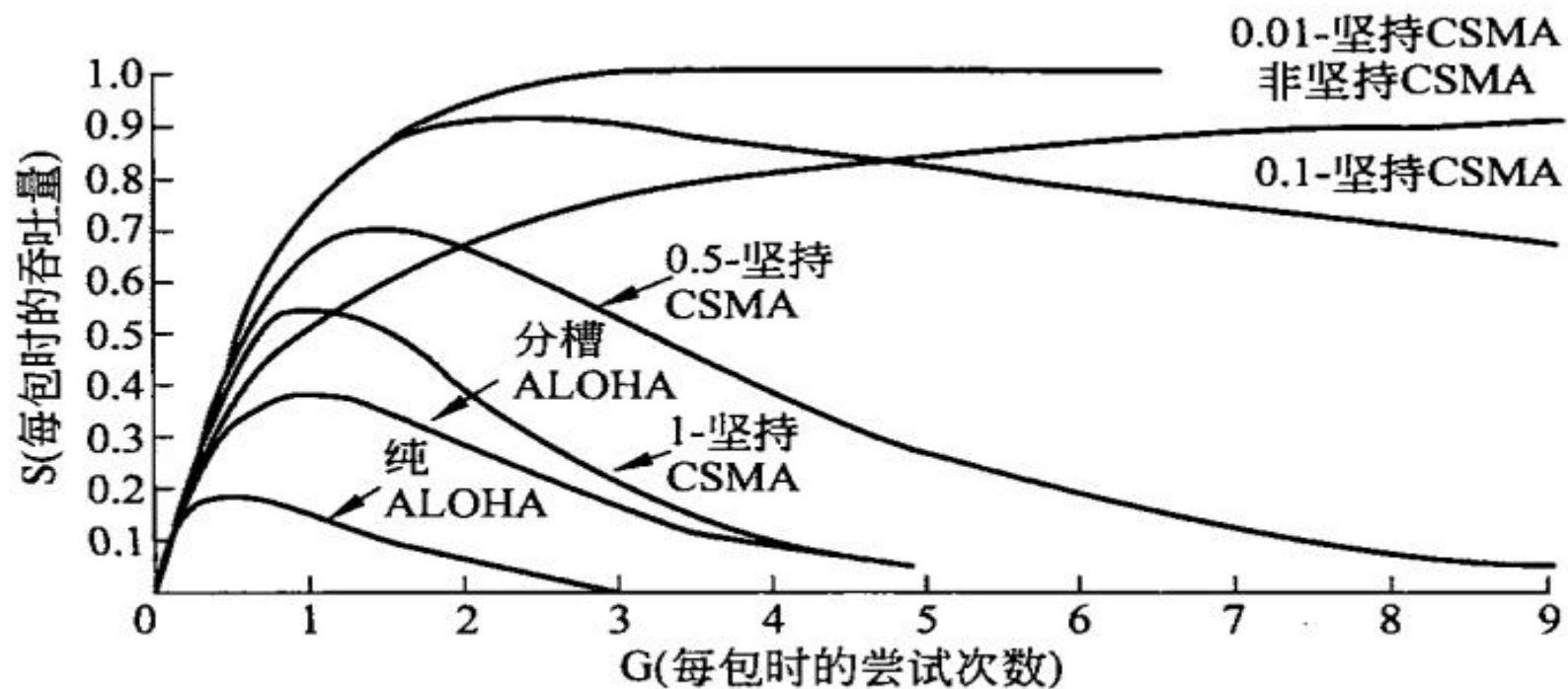


图 4-4 不同随机访问协议的信道使用率与负载比较

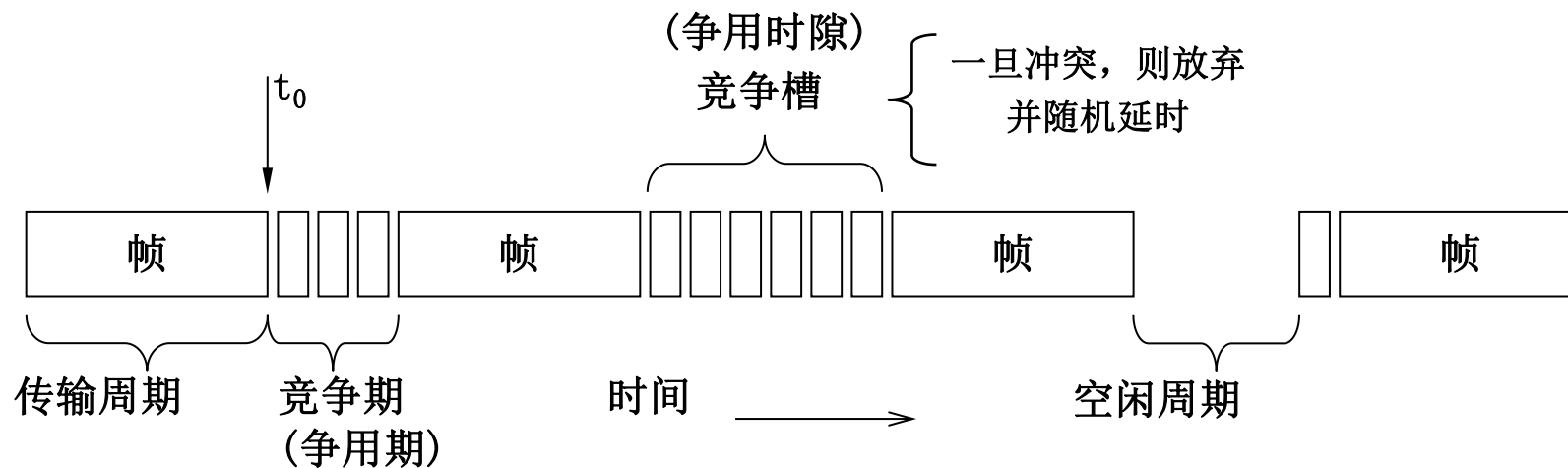
4.2多路访问协议

CSMA/CD (CARRIER SENSE MULTIPLE ACCESS / COLLISION DETECTION)

带冲突检测的载波侦听多路访问(载波监听多路访问/冲突检测)

定义: *CSMA/CD* 协议是经典以太网的基础, 加入了一个冲突检测的模拟过程。

- 站点侦听信道, 如果信道忙则等待。如果空闲, 则发送数据。一旦发现检测到总线上发生冲突, 就要立即停止发送, 然后等待一段随机时间后再次发送。



CSMA/CD的概念模型

4.2 多路访问协议——CSMA/CD

- **多点接入**：许多计算机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一下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，以免发送碰撞。
- 总线上并没有什么“载波”。因此，“载波监听”就是用电子技术检测总线上有没有其他的数据信号。
- **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**

4.2 多路访问协议——CSMA/CD

CSMA/CD的重要特性

- 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）。
- 每个站点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。

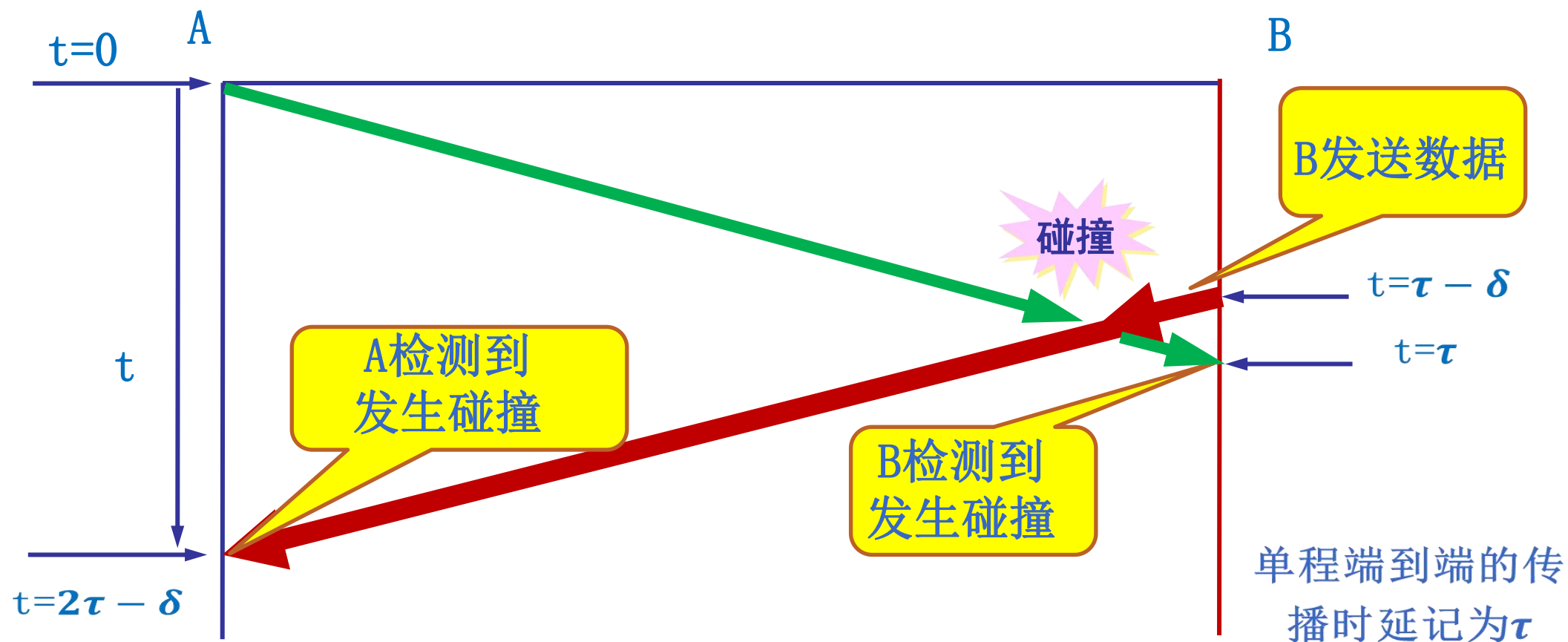
4.2 多路访问协议——CSMA/CD

CSMA/CD——传播时延对载波监听的影响

- 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。两个发送站都需要重新发送数据。

4.2 多路访问协议——CSMA/CD

CSMA/CD——传播时延对载波监听的影响

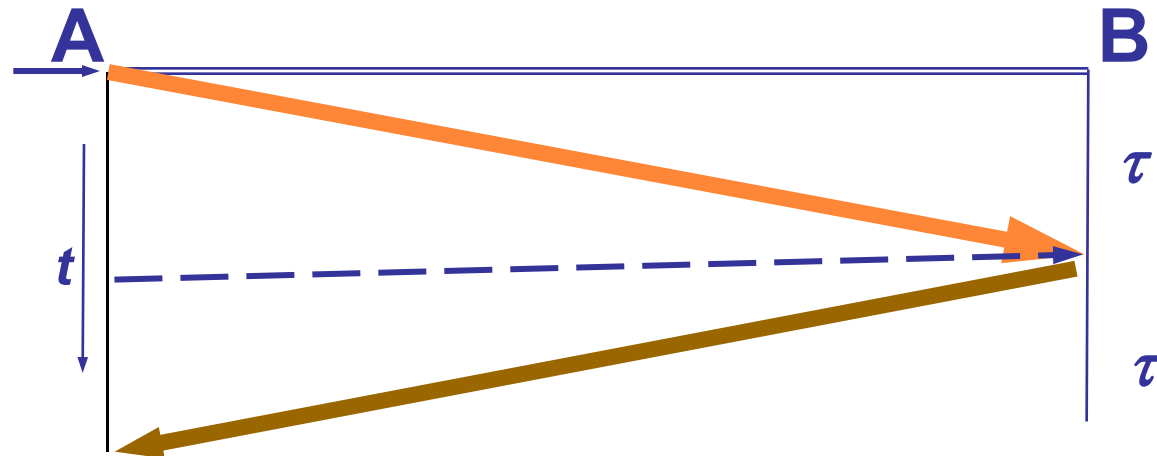


4.2 多路访问协议——CSMA/CD



4.2 多路访问协议——CSMA/CD

- 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**竞争期**，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。



4.2 多路访问协议——CSMA/CD

CSMA/CD—争用期的长度

- 以太网取 $51.2\mu s$ 为争用期的长度
- 对于10Mb/s以太网，在争用期内可发送512bit，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。

4.2 多路访问协议——CSMA/CD

CSMA/CD—最短有效帧长

- 如果发生冲突，就一定是在发送的前64字节以内。
- 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字节的帧都是由冲突而异常中止的无效帧。

4.2 多路访问协议——CSMA/CD

CSMA/CD—二进制指数后退算法

二进制指数后退算法:

- CSMA/CD发送方在检测到冲突后，双方（或多方）都将延时一段时间再发送数据。
 - 确定基本退避时间，一般是取为争用期为 2τ 。
 - 定义重传次数 i , $i \leq 10$, 即 $i = \text{Min}[\text{重传次数}, 10]$
 - 从整数集合 $[0, 1, \dots, (2^i - 1)]$ 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（ $2^r \tau$ ）。
 - 当重传达16次仍不能成功时即丢弃该帧，并报告。



4.2 多路访问协议——CSMA/CD

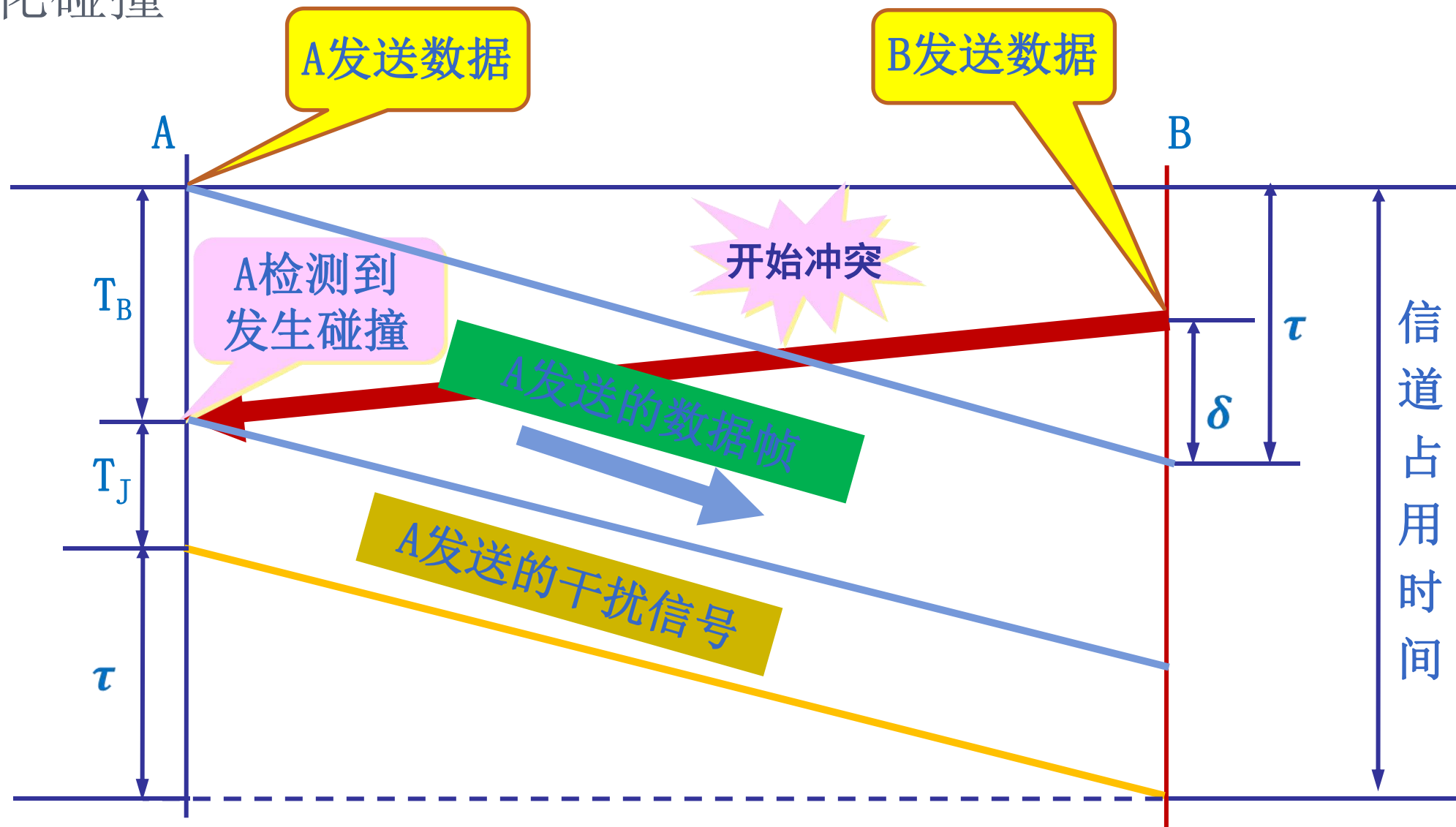
强化碰撞

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



4.2 多路访问协议——CSMA/CD

强化碰撞



4.2 多路访问协议——CSMA/CD

CSMA/CD协议与分槽ALOHA协议的区别：

- ❑ CSMA/CD：只有一个站能用来传输的时间槽，在传输完毕之前，信道会被一个站占据，即信道被捕获（抓住）。
- ❑ 而分槽ALOHA的每个时间槽都需要进行竞争。

4.2 多路访问协议——无冲突协议

- 位图协议
- 令牌传递
- 二进制倒数计数



4.2 多路访问协议——无冲突协议

- 位图协议（基本位图法）：声明—》排队—》传输



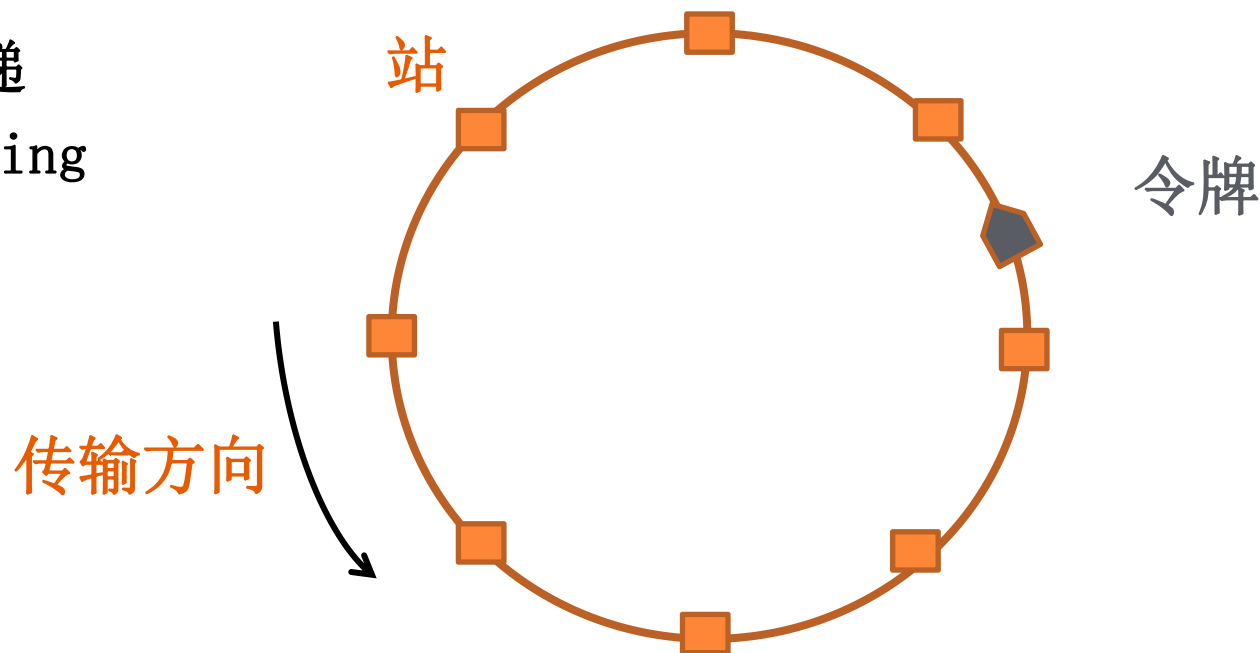
图 4-6 基本位图协议

竞争期包含 N 个槽，每个槽分别对应某个编号的站点，如果该站点需要发送数据，则在对应的槽内填1，这样其他站点会得知哪个站将要发送数据。如此反复。

这种传输前广播数据发送愿望的协议称为预留协议。

4.2 多路访问协议——无冲突协议

- 令牌传递
- Token ring



- 网络拓扑结构被用来定义站的发送顺序。拿到令牌的站才能发送。注意实际的网络中不需要物理环来实现，可以基于总线型实现。
- 在令牌环协议中，站点间通过传递一个称为令牌的短消息，分配发送权限



4.2 多路访问协议——无冲突协议

- 二进制倒数计数
- 站点以位串的形式广播自己的地址，按照一定的优先级竞争使用信道：所有的站点只要看到自己的地址位中的0被改写成1则放弃竞争。这种方法的信道利用率为： $d/(d+\log_2 N)$

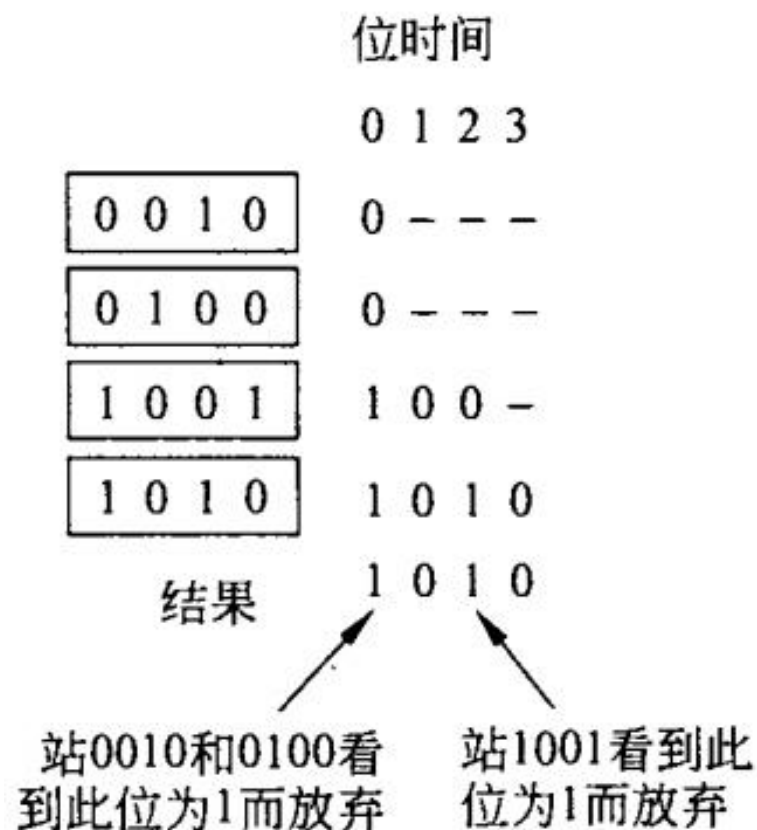


图 4-8 二进制倒数计数协议
虚线表示不参与

4.2 多路访问协议——有限竞争协议

- 对于低负载信道，竞争协议更为理想
- 对于高负载信道，无竞争协议更为理想

$$\text{Pr}[p \text{ 为最佳值时的成功概率}] = \left(\frac{k-1}{k}\right)^{k-1}$$

- 结合两者特点，可以获得良好的信道使用效率，这样的协议称为有限竞争协议。

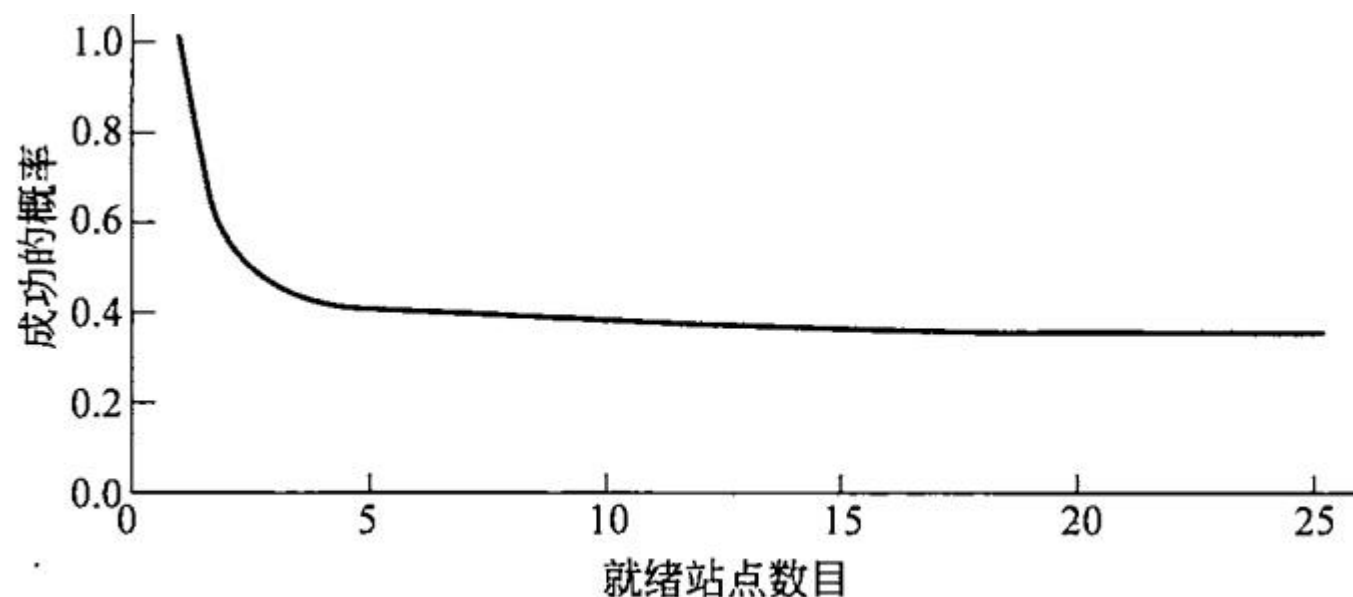
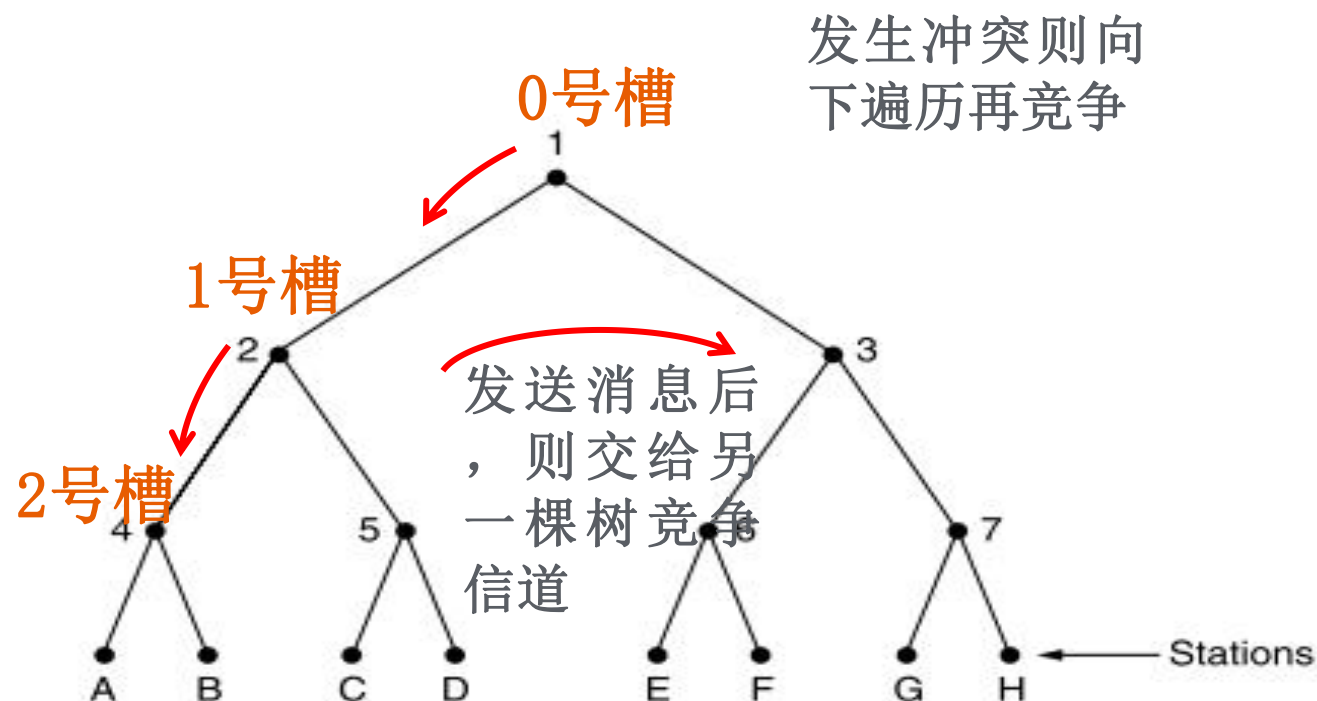


图 4-9 对称竞争信道的获得概率

4.2 多路访问协议——有限竞争协议

- 自适应树遍历协议
- 类似于二分法查找，或者二叉树索引方法



4.2 多路访问协议——无线局域网协议

- 相比有线网络，接收的信号有时太弱，无线通信不能检测正在发生的冲突，只能时候通过确认机制发现冲突。
- 由于无线通信的开放式环境，存在隐藏终端和暴露终端问题，将在 *CSMA/CD* 基础上改进，需要发送和接收双方协商解决。

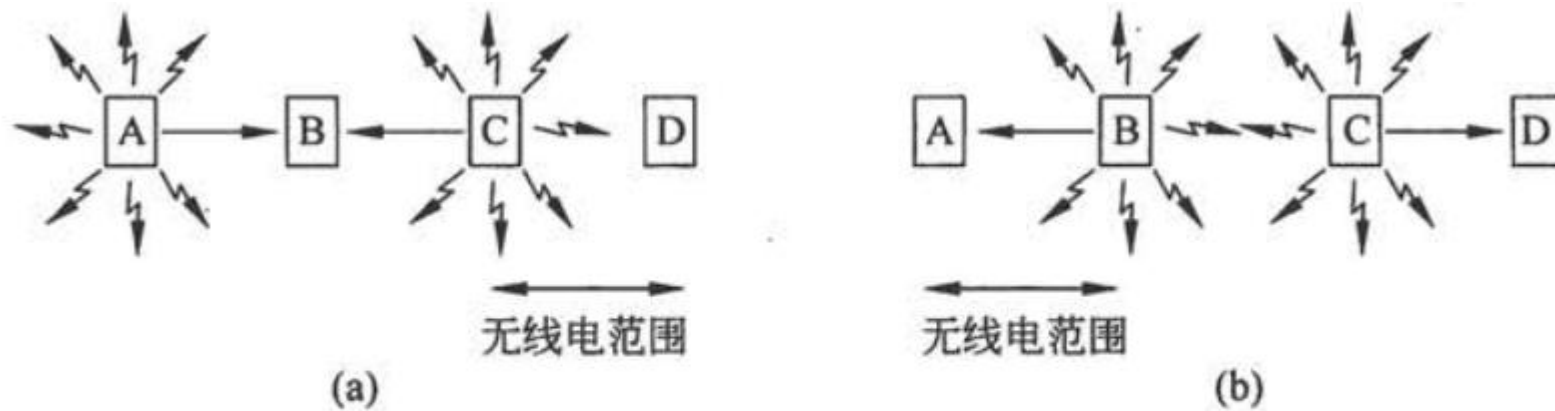


图 4-11 一个无线 LAN

(a) 在给 B 传输时 A 和 C 是隐藏终端； (b) 在给 A 和 D 传输时 B 和 C 是暴露终端

4.2 多路访问协议——无线局域网协议

- 无线的广播特性，传播范围限制，可以基于 *CSMA* 的思想，尝试解决无线局域网的通信冲突避免多路访问（*MACA*）协议

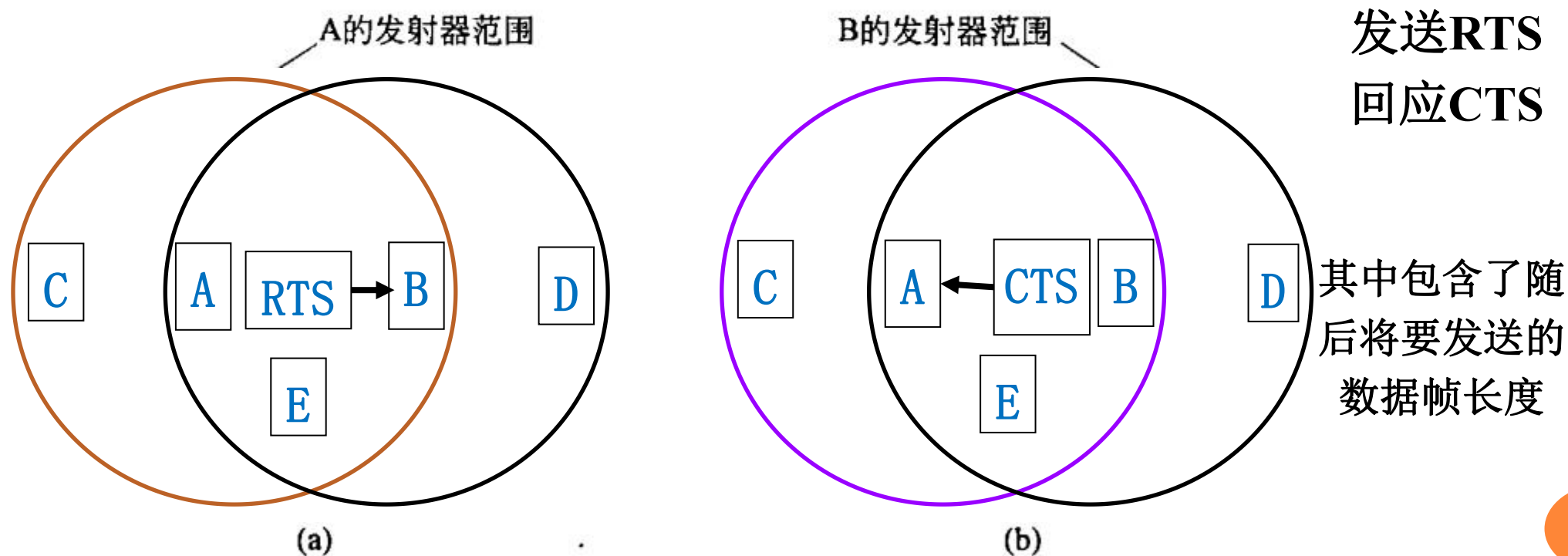


图 4-12 MACA 协议

(a) A 给 B 发送一个 RTS; (b) B 作为响应给 A 返回一个 CTS

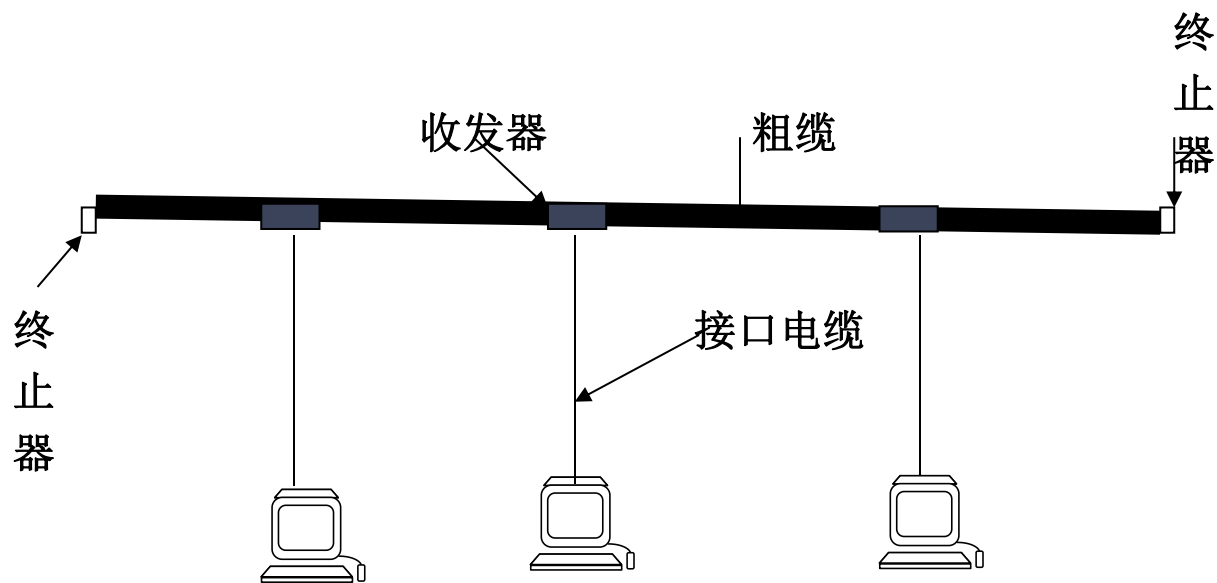
4.3 以太网

- 以太网是局域网的技术一种，也是现在局域网的主流，协议为*IEEE802.3*，其他同时代的局域网协议大部分被淘汰了。所以有些不严格的场合，以太网就指代（有线）局域网。
- 经典以太网：*3-10Mbps*
- 交换式以太网：*100M*以上

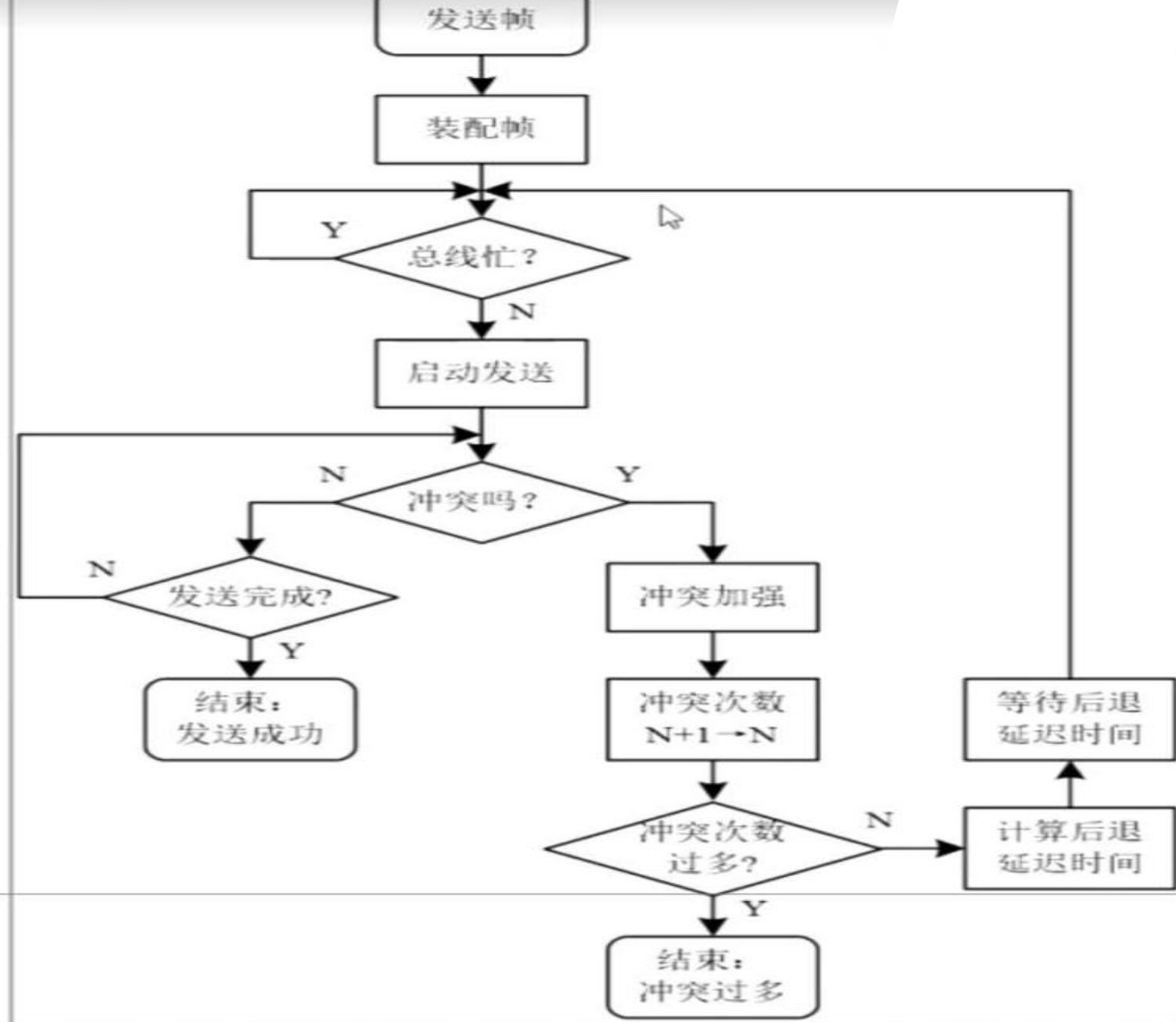


4.3.1 经典以太网物理层

- 经典以太网使用一根电缆连接所有计算机，结构如图所示。
最早的称为粗以太网。



以太网数据发送流程



经典以太网MAC子层协议

- 以太网的帧结构



7个字节的**10101010**,
用于时钟同步, 最后一个
字节为帧定界符



经典以太网MAC子层协议

- 以太网的帧结构



硬件地址（*MAC*地址）：被写入网卡的6个字节的地址，全球唯一，由*IEEE*分配给网卡生产商。

全1的地址为广播地址

经典以太网MAC子层协议

- 以太网的帧结构



类型或长度字段



经典以太网MAC子层协议

- 以太网的帧结构



网络层交下来的数据，
<1500字节，且 ≥ 46 字节

经典以太网MAC子层协议

- 以太网的帧结构



以太网帧长 ≥ 64 字节，如果数据过少，则填充一些无用数据以达到64字节

经典以太网MAC子层协议

- 为什么帧的最短长度为64个字节？
- 为了确认发送帧是否正确到达目的站点，必须保证可能的冲突信号返回时帧的发送尚未结束，如果在 2τ 内没有冲突信号返回，则发送成功，发送结束后即使冲突也无法检测，所以最短帧长应与 2τ 相当。



经典以太网MAC子层协议

- 为什么帧的最短长度为64个字节
- 在极限条件下，802.3局域网中发送方和接收方间允许接有4个中继器，最大距离为2500 m，往返5000 m，在传输速率为10M bps 条件下，如果在信号传播过程的尽头发生冲突，往返的时间大约需要50μs，再考虑一些安全余量以及 2的整次幂的因素，所以通常取51.2 μs为竞争槽的时间长度（51.2 μs即传输512 bit，即64字节所耗费的时间），所以帧的长度至少为64个字节



经典以太网MAC子层协议

- 以太网的帧结构



*CRC*校验

经典以太网MAC子层协议

- 在一个时隙的起始处，两个CSMA/CD站点同时发送一个帧，按照二进制指数后退算法，求前4次竞争都冲突的概率？
- 第一次竞争冲突的概率为1；
- 第一次冲突后，A、B都将在等待0个或1个时隙之间选择，选择的组合有：00、01、10、11，共4种，其中00和11将再次冲突，所以第二次竞争时，冲突的概率为0.5
- 第二次冲突后：A、B都将在0、1、2、3之间选择，选择的组合有：00、01、02、03、10、11、12、13、20、21、22、23、30、31、32、33共16种，其中00、11、22、33将再次冲突，所以第三次竞争时，冲突的概率为0.25
- 第三次冲突后：A、B都将在0、1、2、3、4、5、6、7之间选择，选择的组合共有64种，其中00、11、... ..、77将再次冲突，所以第四次竞争时，冲突的概率为0.125
- 前四次竞争都冲突的概率为： $1 \times 0.5 \times 0.25 \times 0.125 = 0.015625$



- 假设在稳定重载荷的情况下，有 k 个站点参与信道竞争，每个站点在每个时间槽中的发送概率为 p ，每个站点获得信道的概率为 $A = kp(1-p)^{k-1}$ ，当 $p = 1/k$ 时， A 将取最大值

当 $k \rightarrow \infty$ 时， $A \rightarrow 1/e$

- 平均竞争间隔 $w = 2\tau / A$

$$\text{信道效率} = \frac{\text{每帧发送时间 (P)}}{\text{每帧发送时间 (P)} + \text{平均竞争时间 (w)}}$$



以太网性能

- 帧长为 F ，网络带宽为 B ，电缆长度为 L 信号传播速率为 c （典型的为 $5\mu s/km$ ），每帧传输时间为 $P=F/B$ ，信号的最大传播延迟 $\tau = L/c$ ，在有 e 个竞争时隙的情况下

$$\text{即最佳的信道效率} = \frac{\frac{F}{B}}{\frac{F}{B} + \frac{2Le}{c}} = \frac{1}{1 + \frac{2BLE}{cF}}$$

- 以太网有最大长度限制，增加网络带宽或远距离传输，将使信道效率降低.所以，在高带宽或广域网条件下，以太网可能不是最合适的

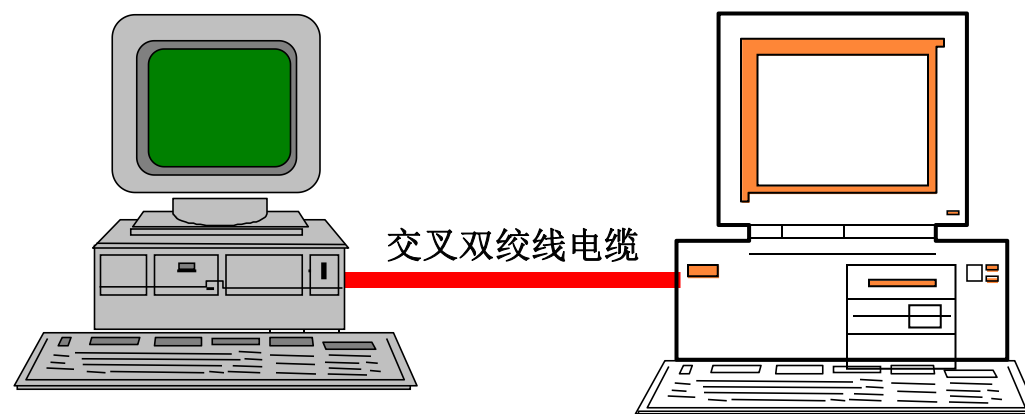


以太网性能

- 现有的以太网的性能很多基于网络流量播送分布的假设。
- 实际的网络流量呈现出自相似/突发性。
- 相关研究可参见相关的研究内容
 1. Crovella M E, Bestavros A. Self-similarity in World Wide Web traffic: evidence and possible causes
 2. Leland W E, Taqqu M S, Willinger W, et al. On the self-similar nature of Ethernet traffic
 3. Park K, Kim G, Crovella M E. Effect of traffic self-similarity on network performance
 4. Liang Q. Ad hoc wireless network traffic-self-similarity and forecasting



最简单的以太网网络



网络互联设备

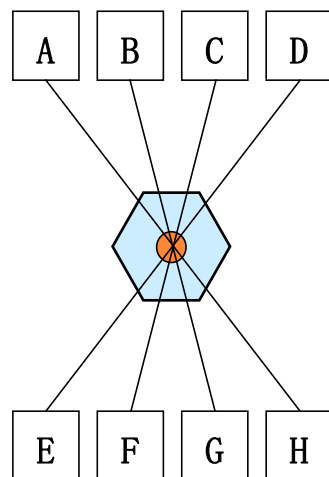
- 不同的协议层有不同的网络互联设备

应用层	应用网关
传输层	传输网关
网络层	路由器
数据链路层	网桥、交换机
物理层	中继器、集线器

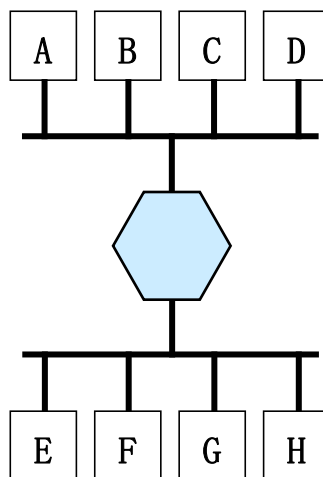


集线器、网桥和交换机

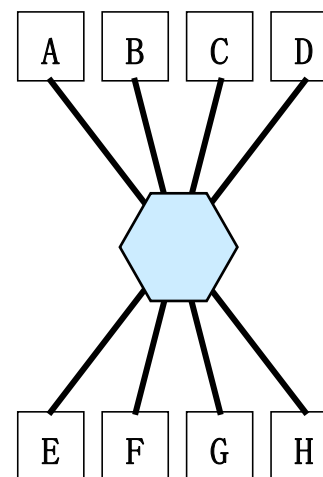
集线器



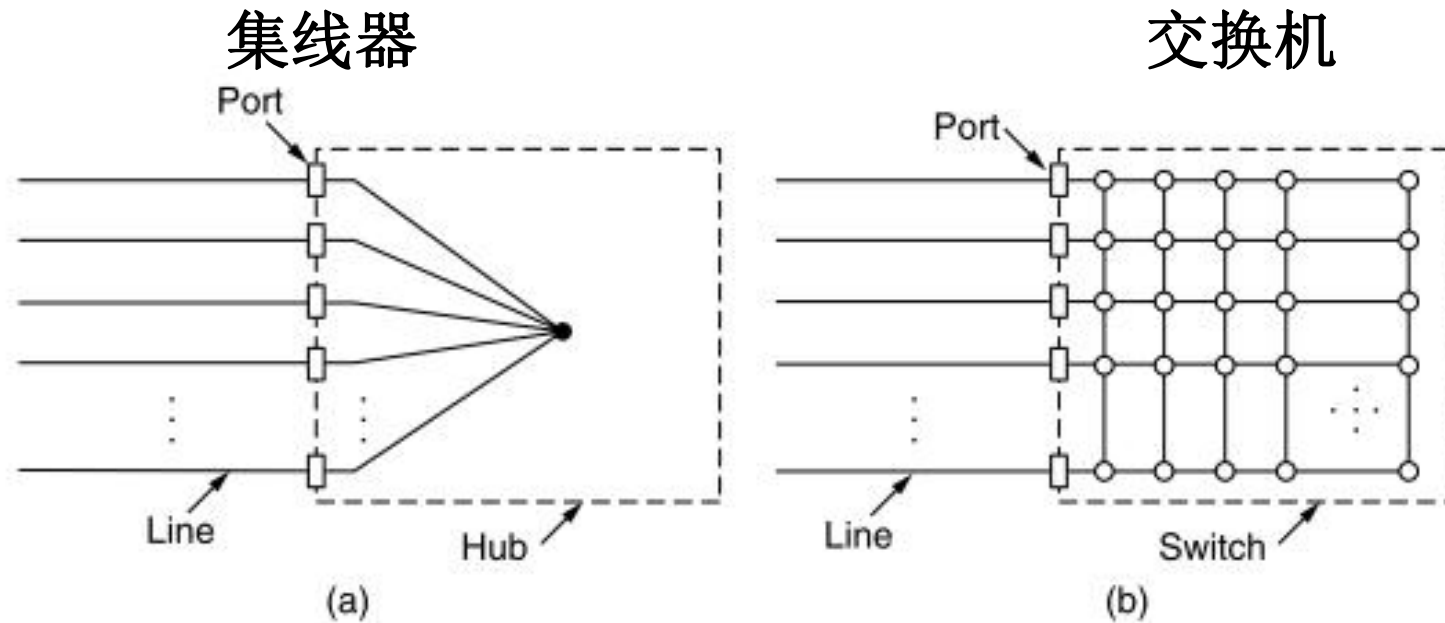
网桥



交换机



交换式以太网图例



- 交换机有一个高速的背板，速率可达 **$1G\ b/s$** 或更高
- 背板上可插入若干个模块（有的模块还可插入子模块）
- 每个模块（或子模块）上有 **$4 \sim 8$** 个 **$RJ-45$** 的端口，甚至更多，每个模块实际上是一个规模较小的局域网，即一个模块就是一个共享域（以太网中，共享域即冲突域）

交换式以太网

- 一个模块上任一时刻只能有一个站点发送，但分属不同模块上的端口可并行工作，这可理解为组交换：模块内共享，模块间交换
- 当每个模块都退化成只有一个端口时，即一个共享域中只有一个端口，则该交换机是全交换的
- 交换式以太网通常以百兆交换机或千兆交换机作为局域网的核心交换设备，交换机的每个端口都可用于连接一个网段或一台主机
- 每个端口连接的网段形成一个冲突域，端口之间帧的传输不受 $CSMA/CD$ 的限制
- 交换机上不同类型的端口支持不同类型的传输介质，不同类型的端口其最大传输距离也不尽相同



快速以太网

- 也称为百兆以太网, **100**兆以太网最短帧长不变, **MAC**层没有变化, 所以与**10**兆以太网兼容。为了将速率提高**10**倍, 将最长的传输距离缩小**10**倍, 网段中的最长的电缆长度减小到**100**米。不支持同轴电缆。
- 采用星型连接方式, 由一个百兆的集线器连接所有机器
- **100BASE-T4**: 4对**3**类双绞线, **3**对发送用, **1**对接受, 用**6B8T-NRZ**编码方式
- **100BASE-TX**: 2对无屏蔽**5**类双绞线或屏蔽双绞线, 用“多电平传输”的编码方式
- **100BASE-FX**: 2对光纤, 采用**4B5B**编码



千兆以太网

- 采用载波扩充 (*carrier extension*) 办法, 扩充帧长度, 低于512的都填充到512位
- 采用帧突发办法, 将多个待发的短帧级连后一起发送
- 1000BASE-SX: 多模光纤, 传输距离为275m或550m
- 1000BASE-LX: 多模光纤, 传输距离为550m或5km
- 1000BASE-CX: 屏蔽双绞线, 传输距离25m
- 1000BASE-T: 4对5类双绞线, 传输距离100m
- 万兆以太网
 - 主要用于数据中心和交换局内部, 用于连接高端路由器、交换机、服务器等。
 - 只支持全双工操作, 不再使用CSMA/CD。



无线局域网

- 802.11体系结构与协议栈
- 802.11物理层
- 802.11MAC子层协议
- 802.11帧结构



802.11体系结构与协议栈

- 802.11定义了两种组网模式
- 自组织Ad-Hoc 模式：没有固定接入点，所有点都可以式中继点。
- 有架构模式：有客户端和接入点（AP，Access point/热点）。客户端收发数据包都要通过热点。接入点还能够与有线网络（分布式系统）连接在一起，形成扩展的802.11网络



802.11标准中的物理层

- 2.4GHz或5GHz频段，属于ISM，可以免费使用
- 802.11：1997年，速度2Mbps
- 802.11a：1999年，工作频率5GHz，速度20Mbps（OFDM）
- 802.11b：1999年，工作频率2.4GHz，速度11Mbps
- 802.11g：2003年，工作频率2.4GHz，速度20Mbps
- 802.11n：2009年，工作频率2.4G和5GHz，速度600Mbps（MIMO）
- 802.11ac：2013年，工作频率5GHz，速度3.4-6.9Gbps
- 802.11ax：WiFi 6，工作频率2.4G和5GHz，速度9.6Gbps



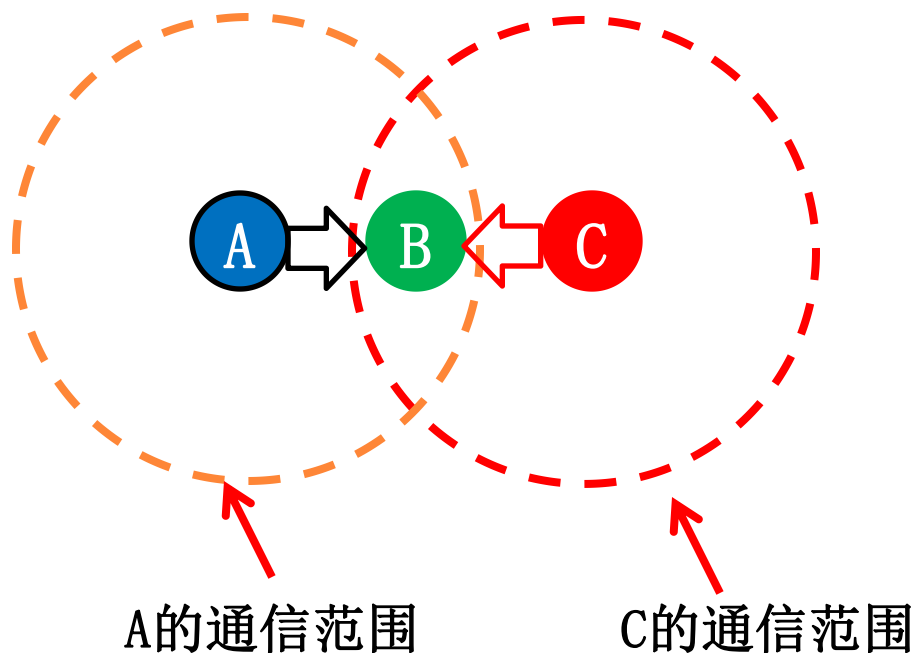
802.11的MAC子层协议

- CSMA/CA:载波侦听多路访问/冲突避免 (Carrier Sense Multiple Access with Collision Avoidance)
 - ✎ 功能：工作在无线网络MAC层，用于协调各节点通信，避免冲突
- 不直接采用有线网络CSMA/CD协议的原因：
 - 1、硬件成本太高，难以实现冲突检测
 - 2、存在隐蔽站和暴露站问题

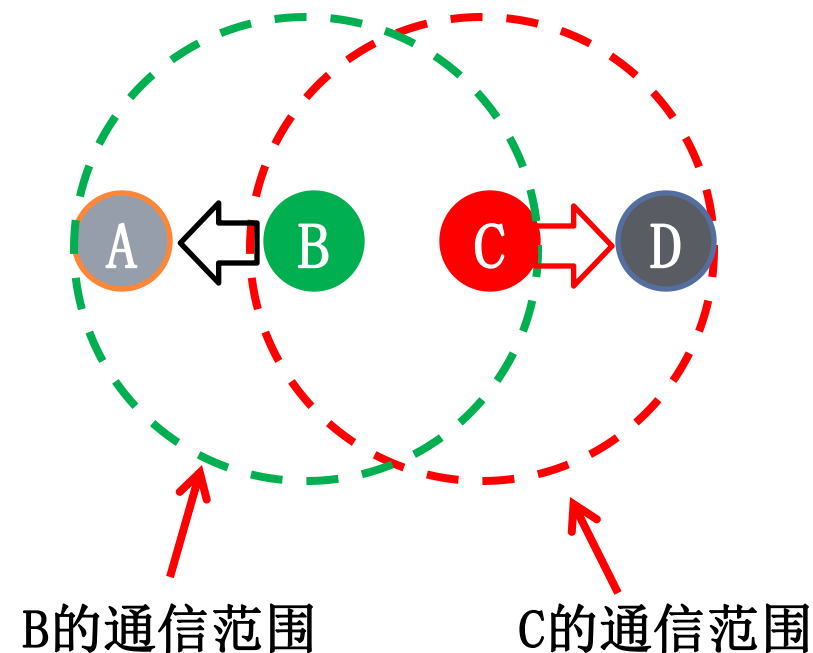


802.11的MAC子层协议

WLAN通信中的问题



隐藏终端问题
(hidden station problem)

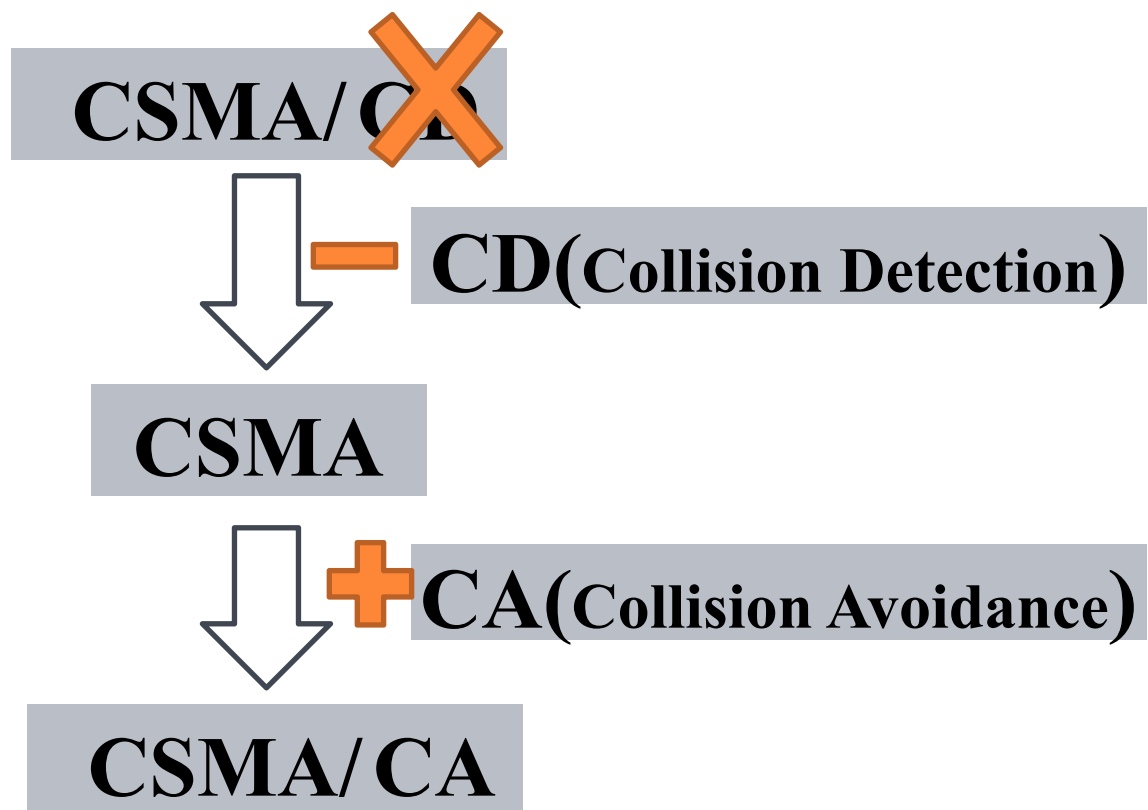


暴露终端问题
(exposed station problem)



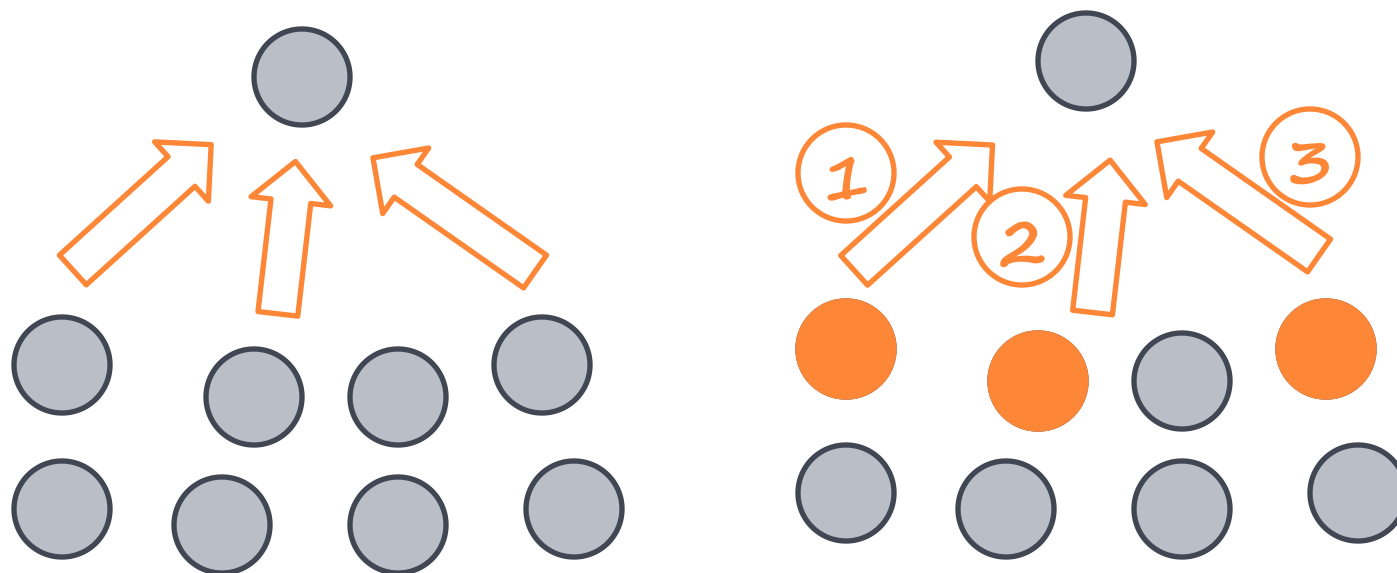
802.11的MAC子层协议

- 基于上述问题，需要根据无线网络通信特点设计节点接入的协议。



802.11的MAC子层协议

发言规则

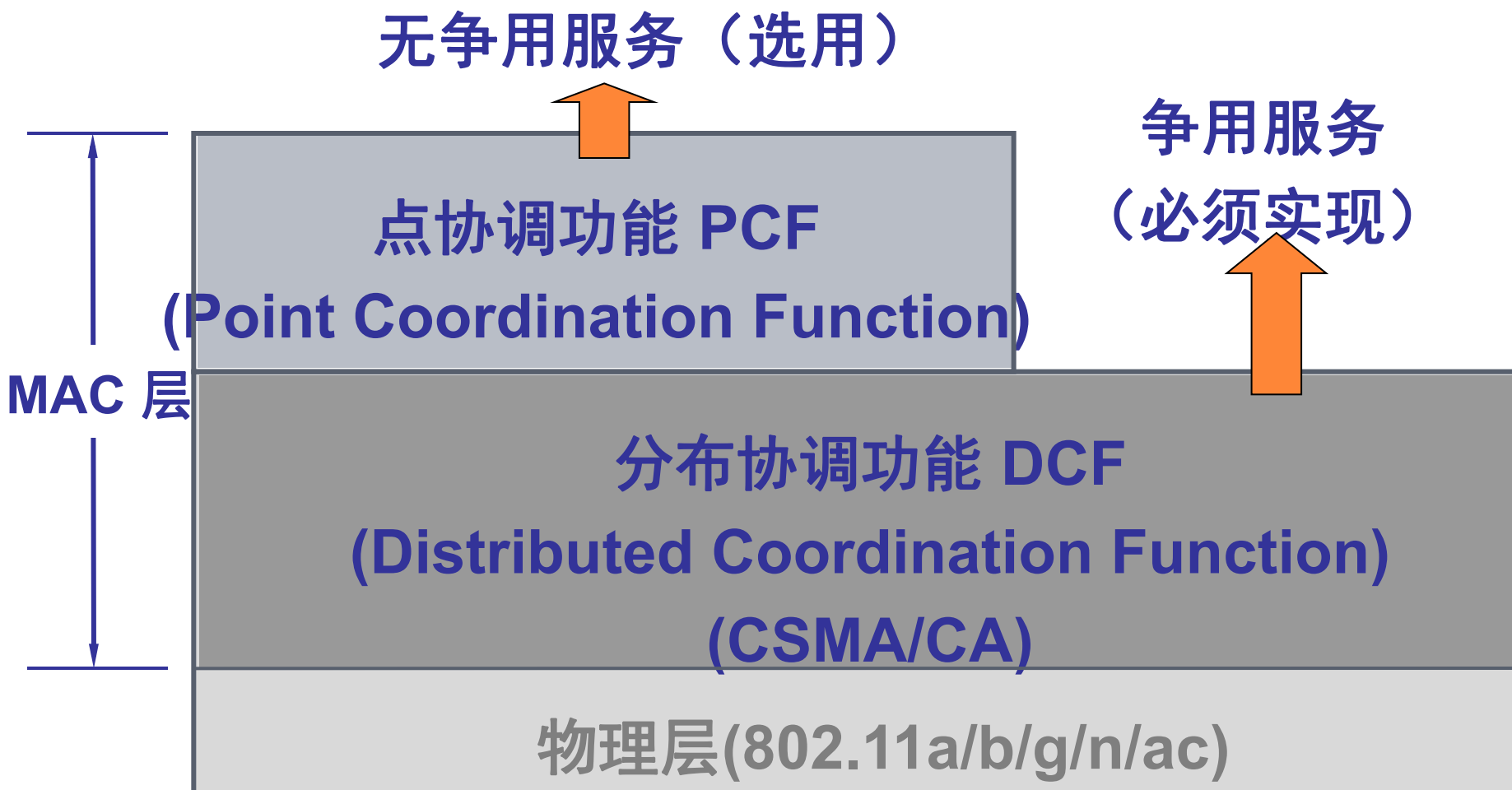


- CSMA/CA协议就是无线局域网中的“举手-发言机制”

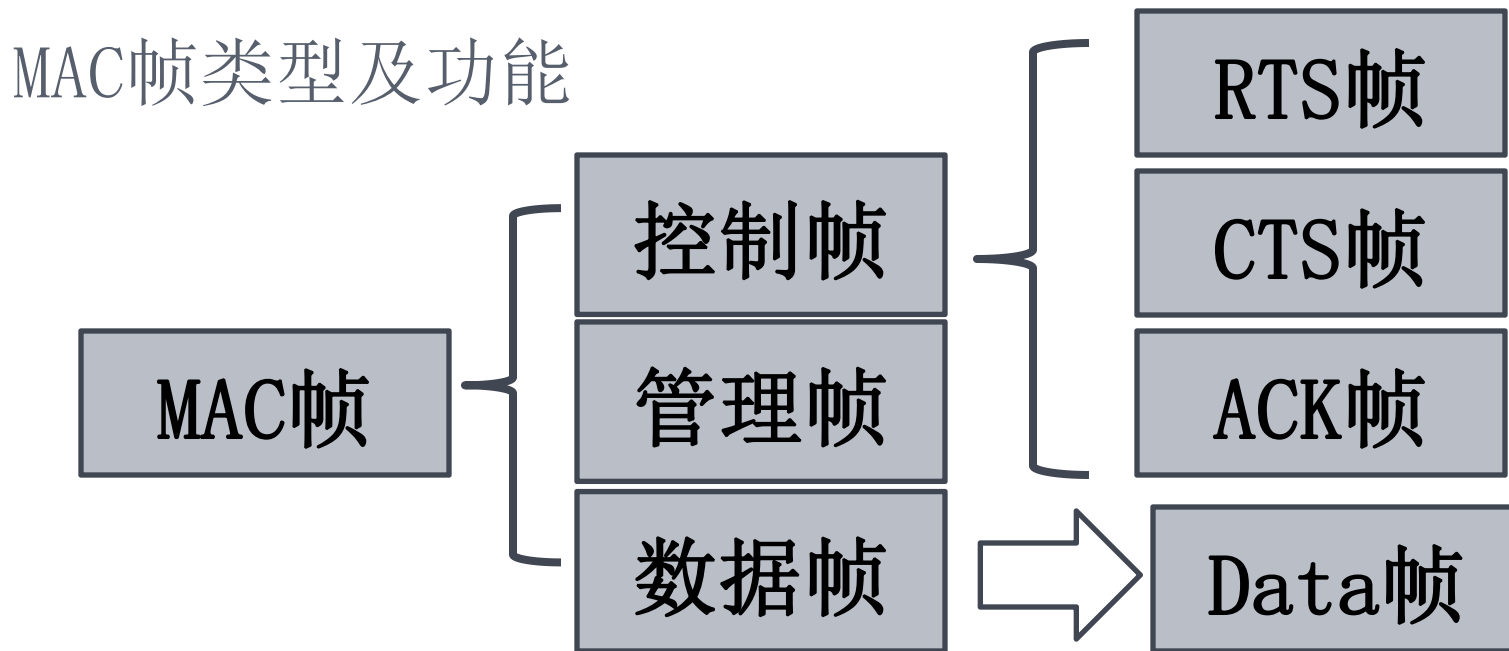


802.11的MAC子层协议

- 802.11 MAC层的结构



802.11的MAC子层协议



- RTS (Request To Send 请求发送帧): 预约信道
- CTS (Clear To Send 允许发送帧): 回复RTS
- ACK (Acknowledgement 确认帧): 回复Data帧

802.11的MAC子层协议

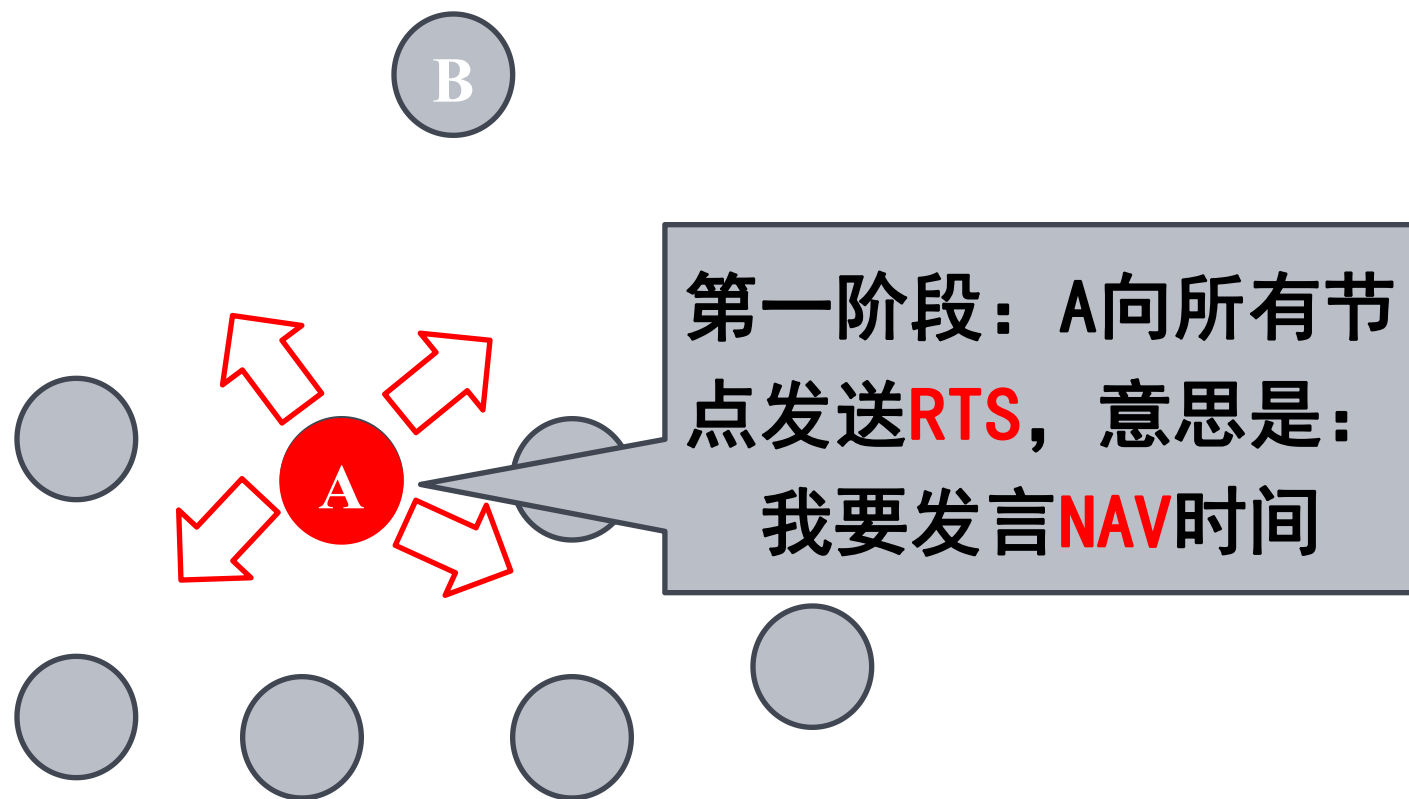
○ CSMA/CA 协议工作流程

- 1、**源节点**检测信道，若信道忙，执行退避机制，等待信道空闲。
- 2、若信道空闲，则等待DIFS后，倒计时计数器，如果计数到0就发送数据（其中包含一系列帧的发送）。
- 3、**目的节点**收到数据，发送ACK帧确认。
- 4、**其他节点**在信道忙期间冻结计数器，等通信结束，再争用信道。
- 5、发送后不检测冲突。数据是否发送成功是由ACK报文完成。如发送方没有收到ACK，就认为报文丢失了，并采用二进制指数后退算法



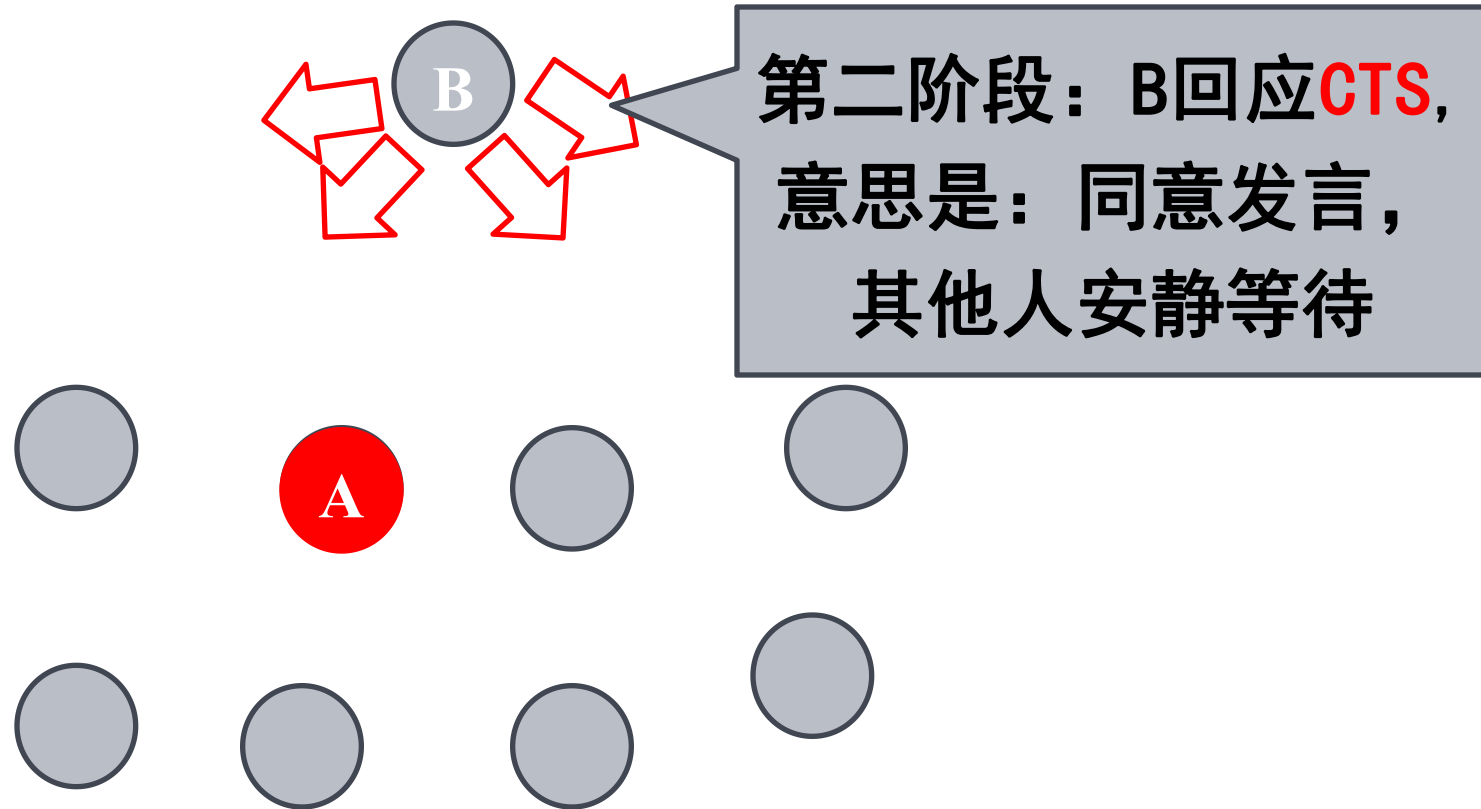
802.11的MAC子层协议

○ CSMA/CA 协议工作流程



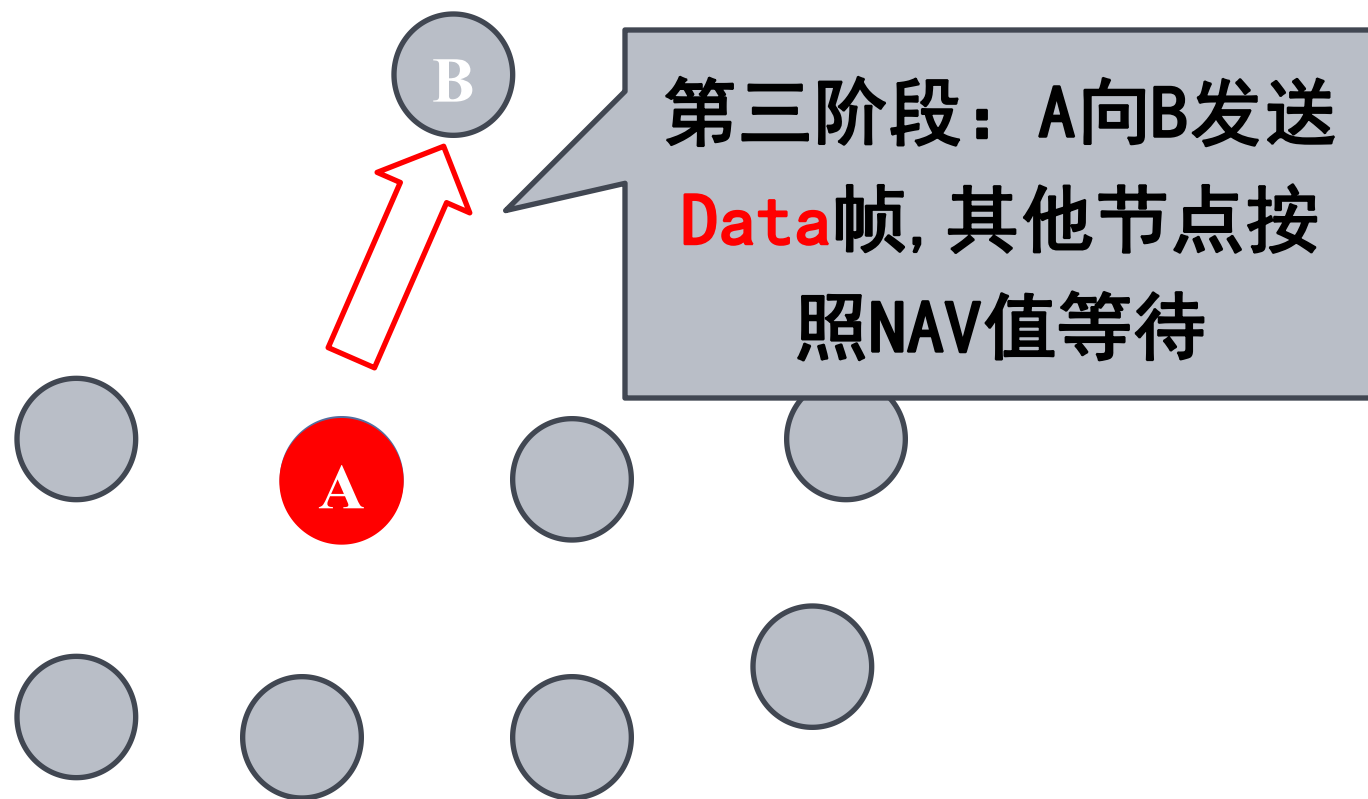
802.11的MAC子层协议

○ CSMA/CA 协议工作流程



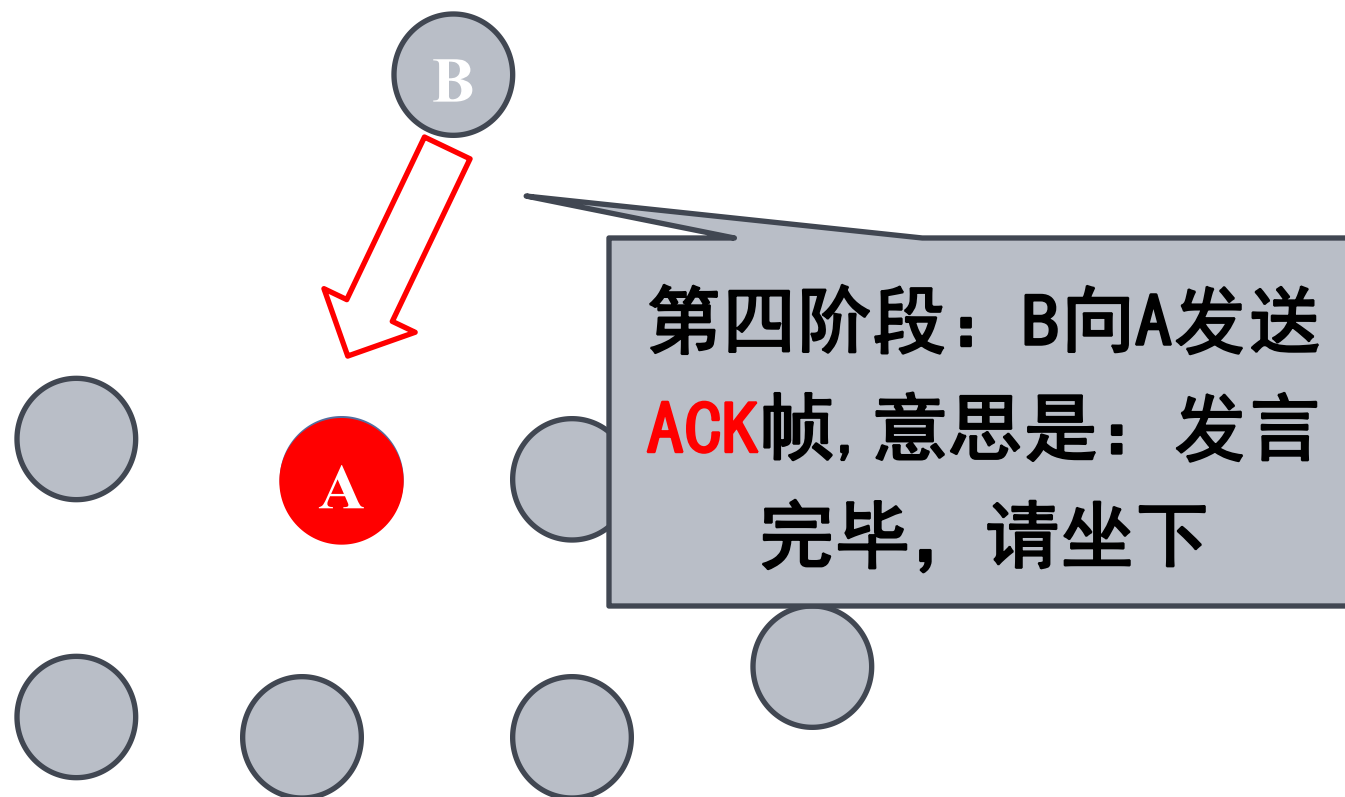
802.11的MAC子层协议

○ CSMA/CA 协议工作流程



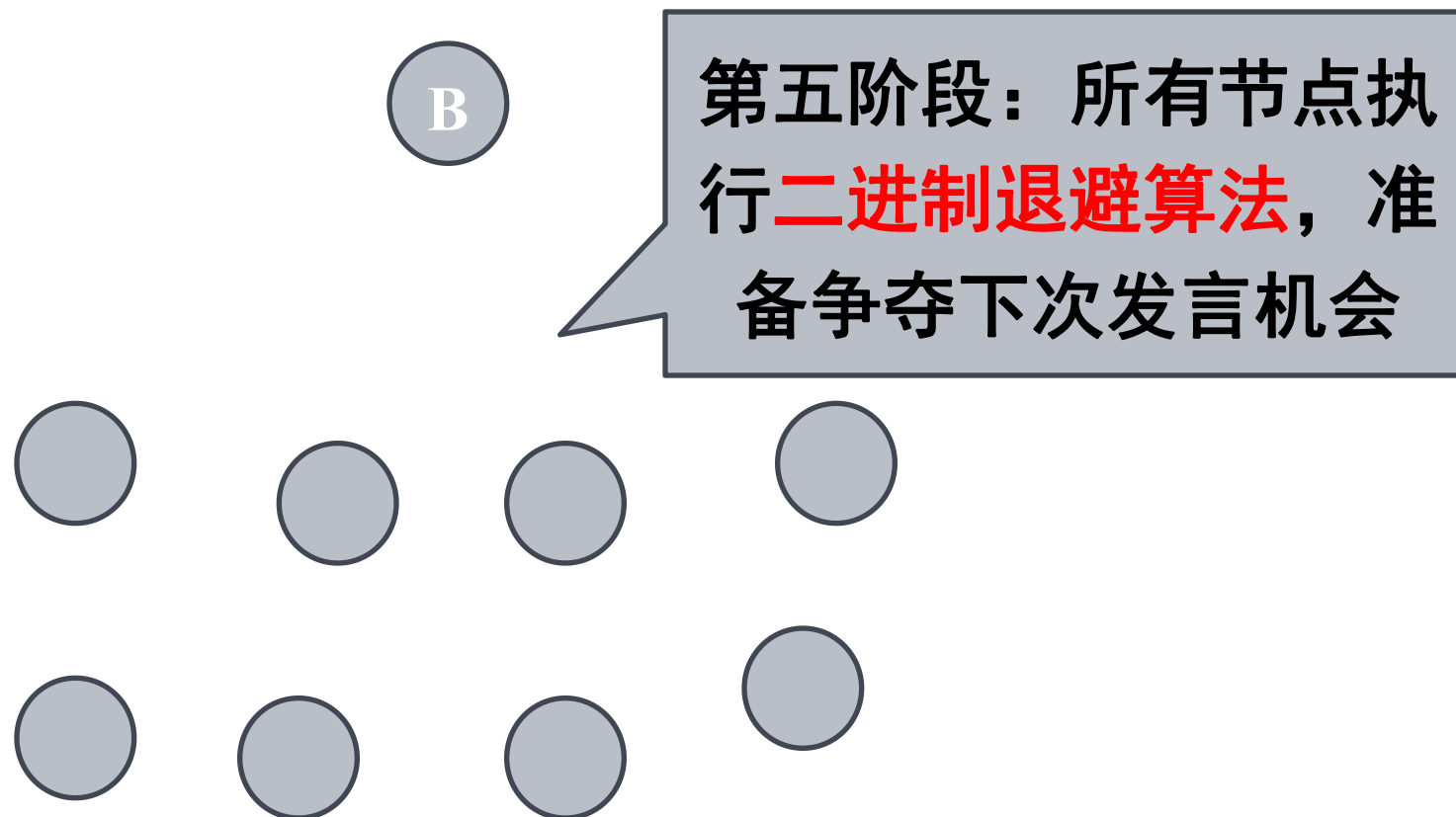
802.11的MAC子层协议

○ CSMA/CA 协议工作流程



802.11的MAC子层协议

○ CSMA/CA 协议工作流程

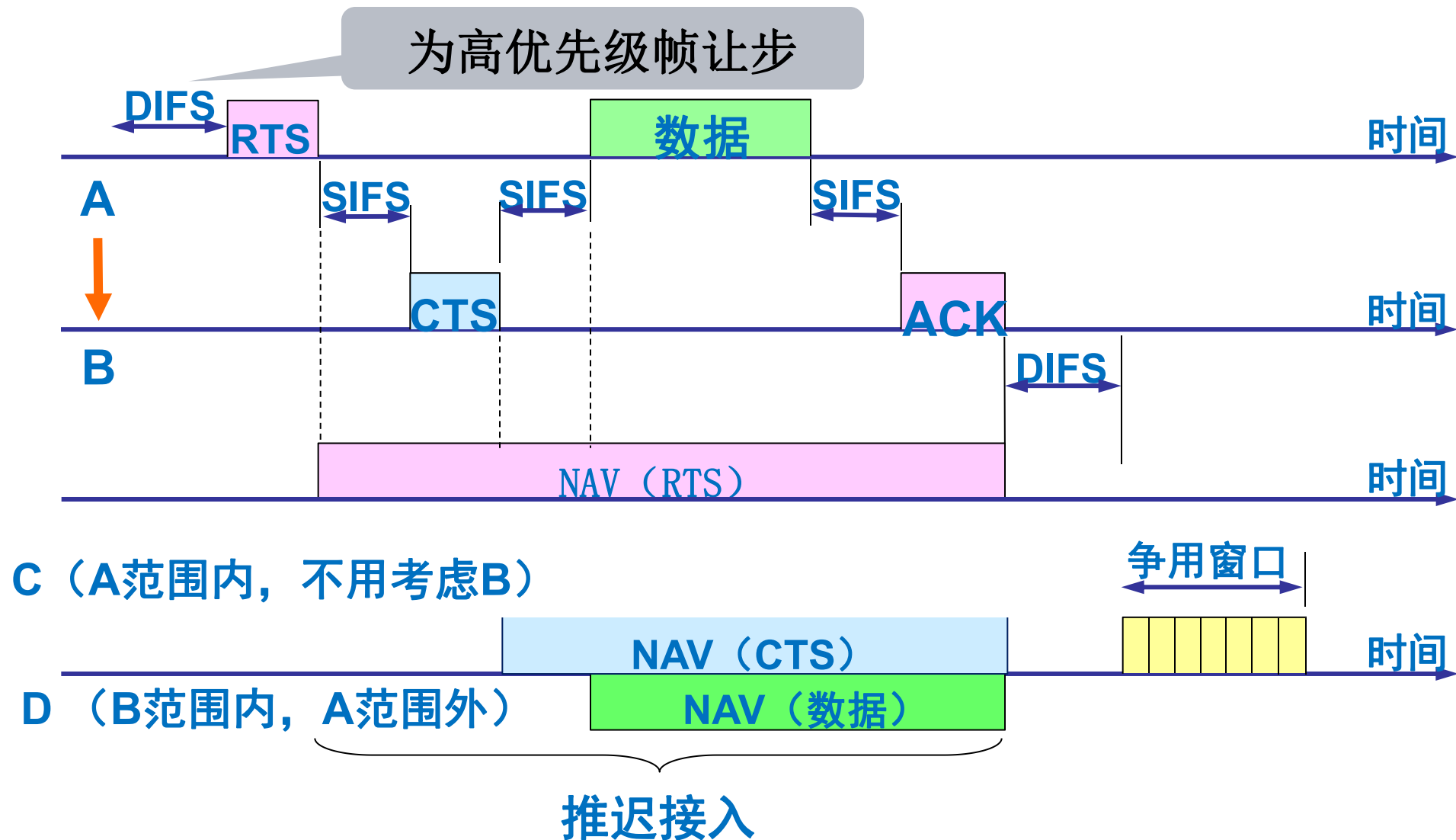


802.11的MAC子层协议

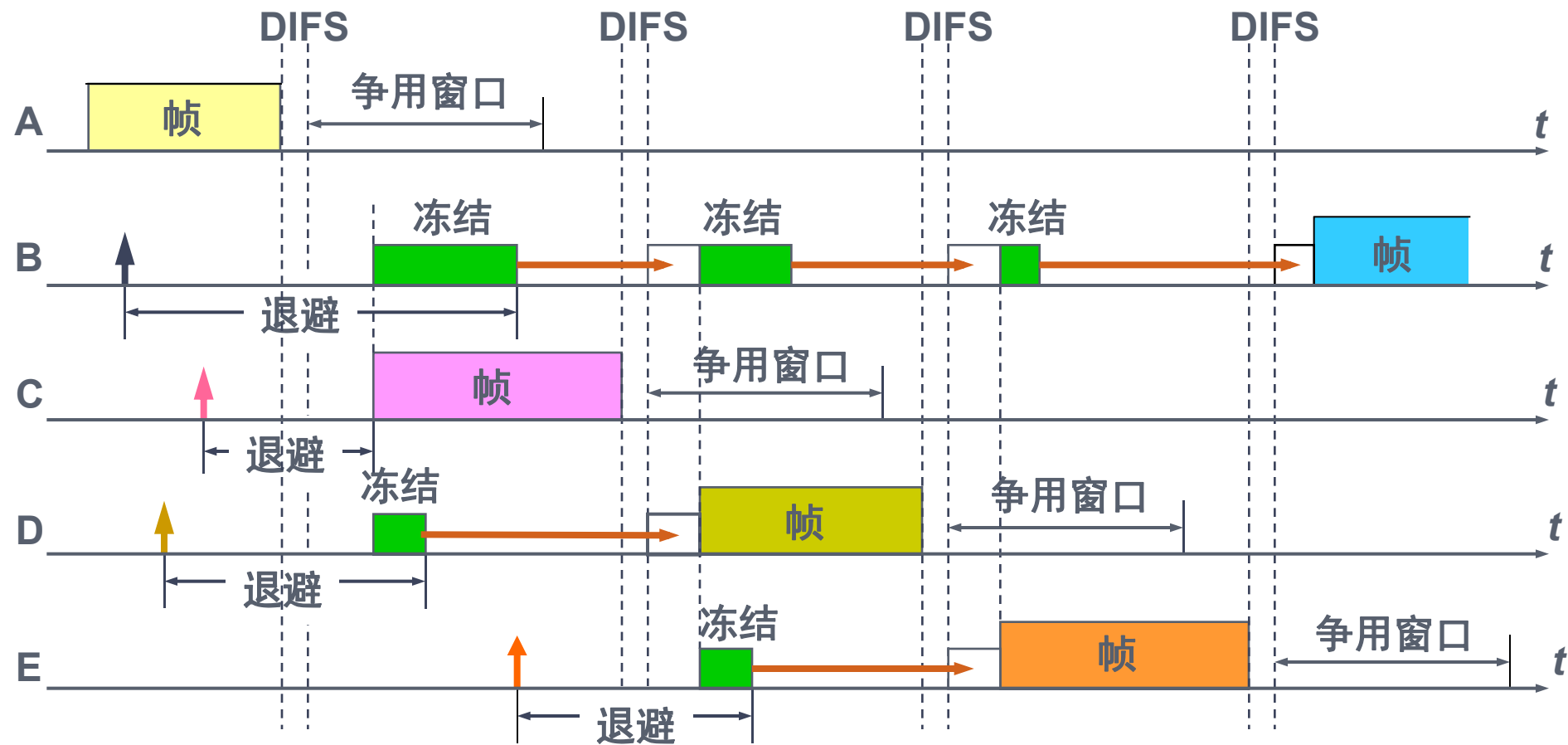
- IFS: 帧间间隔 (InterFrame Space)
 - ∞ 节点在完成发送后, 必须再等待一段很短的时间才能发送下一帧。
这段时间的通称是IFS。
- SIFS: Short IFS 短帧间间隔
- DIFS: Distributed IFS 分布协调功能帧间间隔
- AIFS1和AIFS4: Arbitration IFS仲裁帧间空间
- EIFS: Extended IFS 扩展帧间间隔
- 长度对比EIFS > AIFS4 > DIFS > AIFS1 > SIFS



802.11的MAC子层协议



802.11 的退避机制



图例 ——— 冻结剩余的退避时间



802.11的MAC子层协议相关机制

○ 提高可靠性

- ✎ 发送短帧，将数据分为更小的单位（段），以降低冲突后重发的代价。一旦获得信道，突发多个段。

○ 节省电源

- ✎ 利用信标帧，客户端告诉AP自己已休眠，而AP通过beacon唤醒客户端，通过缓存实现流量的集中发送
- ✎ 自动省电交付，AP不再主动唤醒客户端，避免频繁的交互

○ 提高服务质量

- ✎ 利用帧间间隔



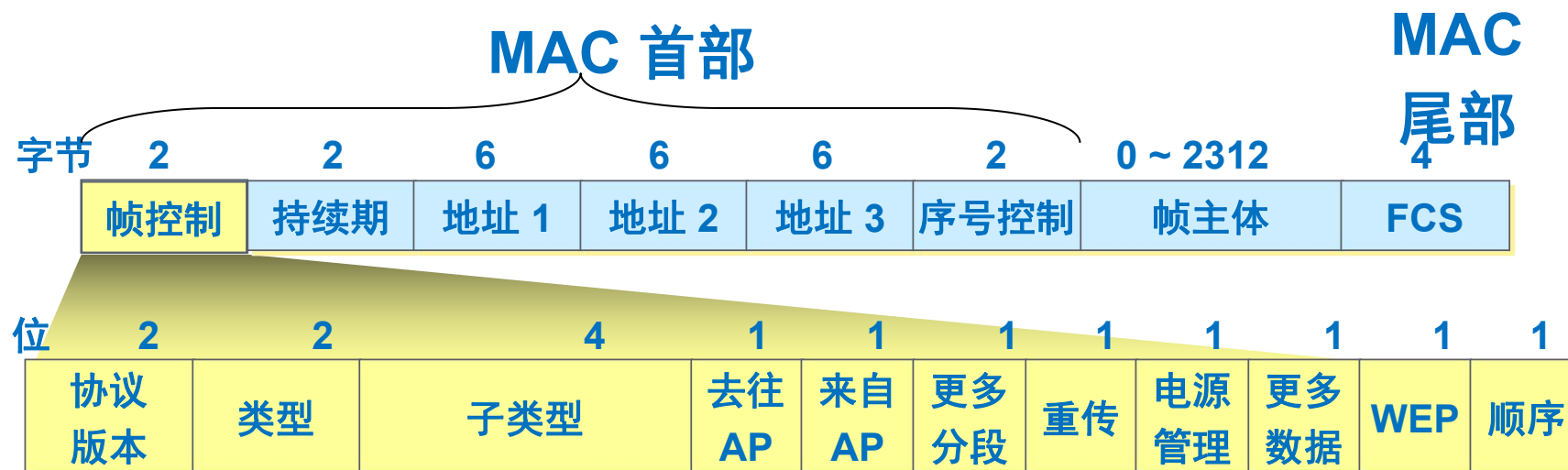
802.11的MAC子层协议相关机制

- CSMA/CA没有碰撞检测机制，即便发生碰撞，仍然发送完。因此为了避免碰撞，在不同情况下（信道忙、重传前、成功发送后需要再次发送），通过退避算法错开发送时机。通过帧间间隔实现冲突避免。
- 当信道从忙转为空闲时，任何站在发送数据前，都要采用二进制后退算法减少发生冲突的概率。
- CSMA/CD则在检测碰撞时，立即停止发送，再退避。
- CSMA/CA使用的是虚拟载波侦听(Virtual Carrier Sense)的机制实际上其他站并没有监听信道，而是由于其他站收到了“源站的通知”才不发送数据。



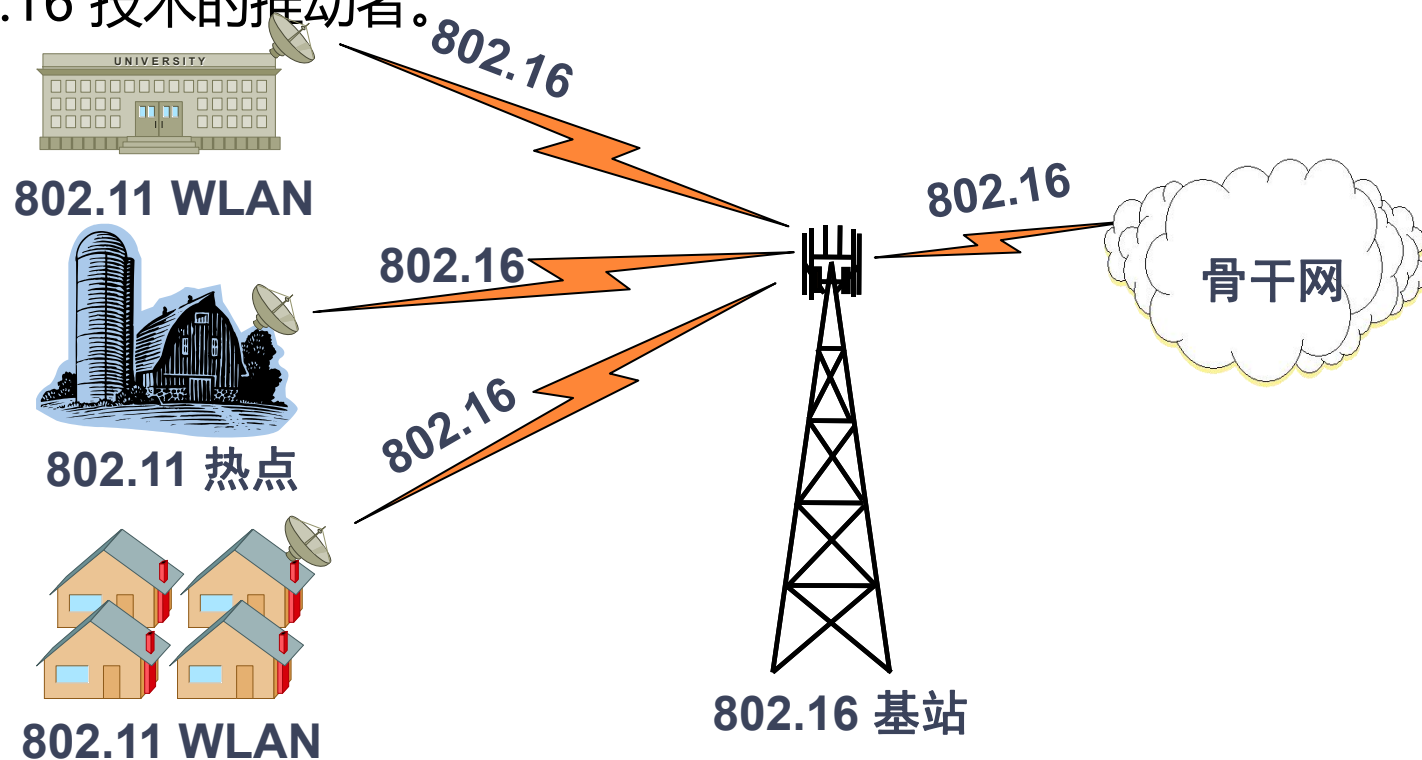
802.11帧结构

- 802.11标准包括数据帧、控制帧和管理帧。
- 地址1：接收方地址
- 地址2：发送方地址
- 地址3：远程端点地址（最终目的地址）
- 实际帧长一般1500字节



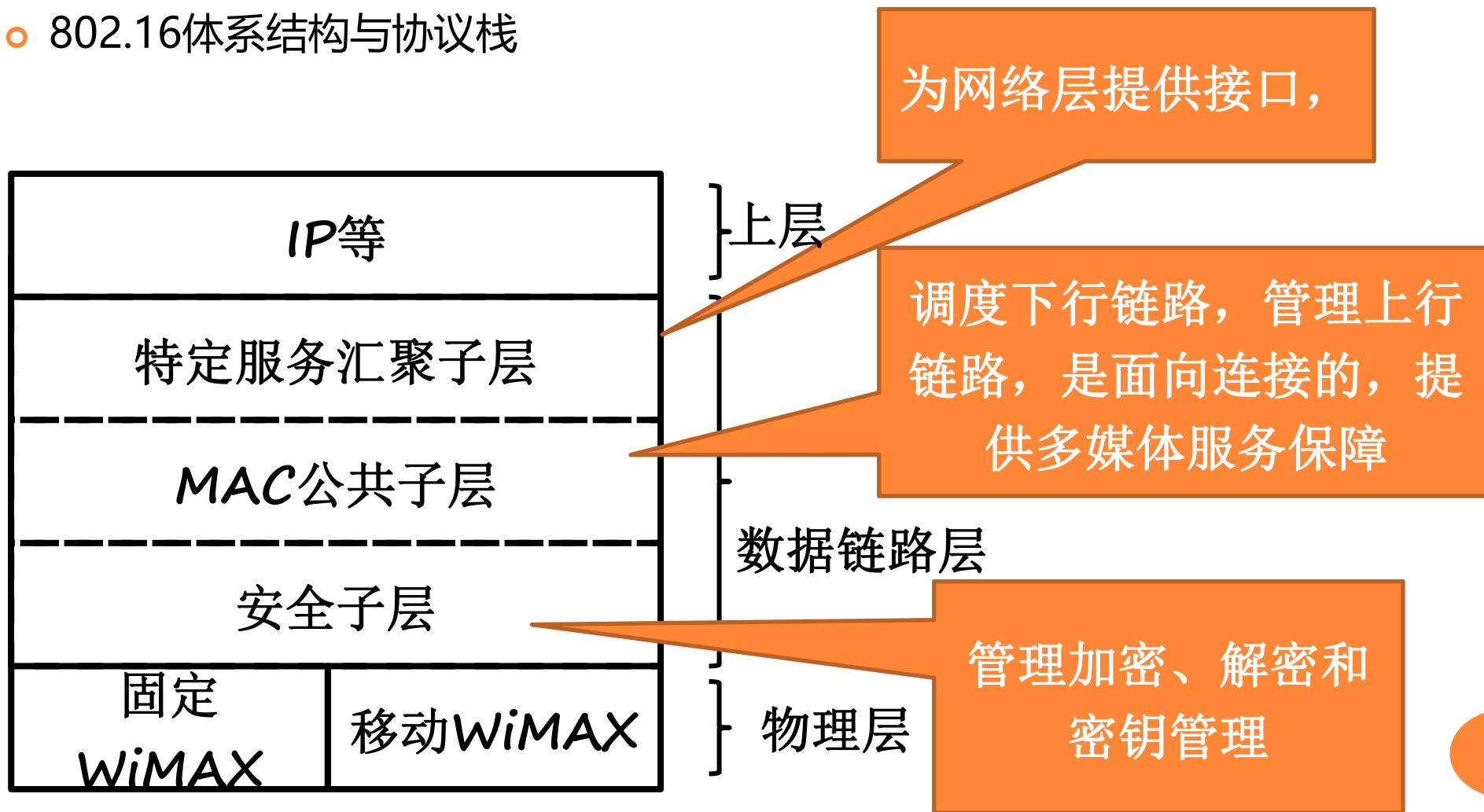
4.5 宽带无线

- WiMAX 可提供“最后一英里”的宽带无线接入（固定的、移动的和便携的）2001年12月第一个802.16标准获批，2003-2005年被陆续修订。
- IEEE 的 802.16 工作组是无线城域网标准的制订者，而 WiMAX 论坛则是 802.16 技术的推动者。



4.5 宽带无线

- 802.16体系结构与协议栈



4.5 宽带无线

- **802.16物理层**

- 通信频率2GHz-11GHz之间，采用OFDM技术，利用QPSK-QAM-16或QAM64调制方案。

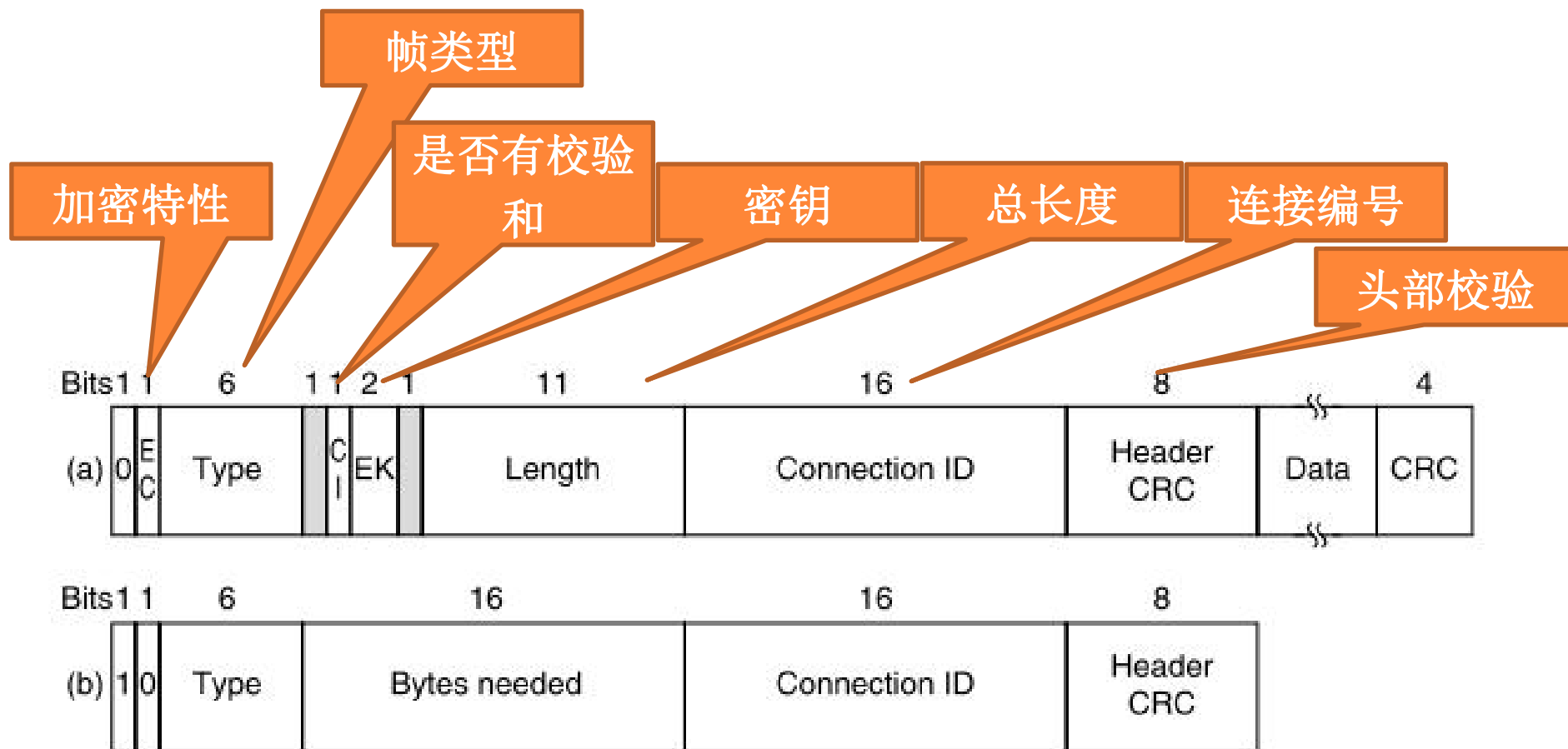
- **802.16MAC子层协议**

- 下行链路：协调控制物理层突发的传输
- 上行链路：
 - ⌘ 提供恒定比特流服务：语音服务
 - ⌘ 实时可变比特率服务：多媒体服务
 - ⌘ 非实时可变比特率服务：大文件传输服务
 - ⌘ 尽力而为服务：一般应用服务



4.5 宽带无线

802.16帧结构



4.6 蓝牙

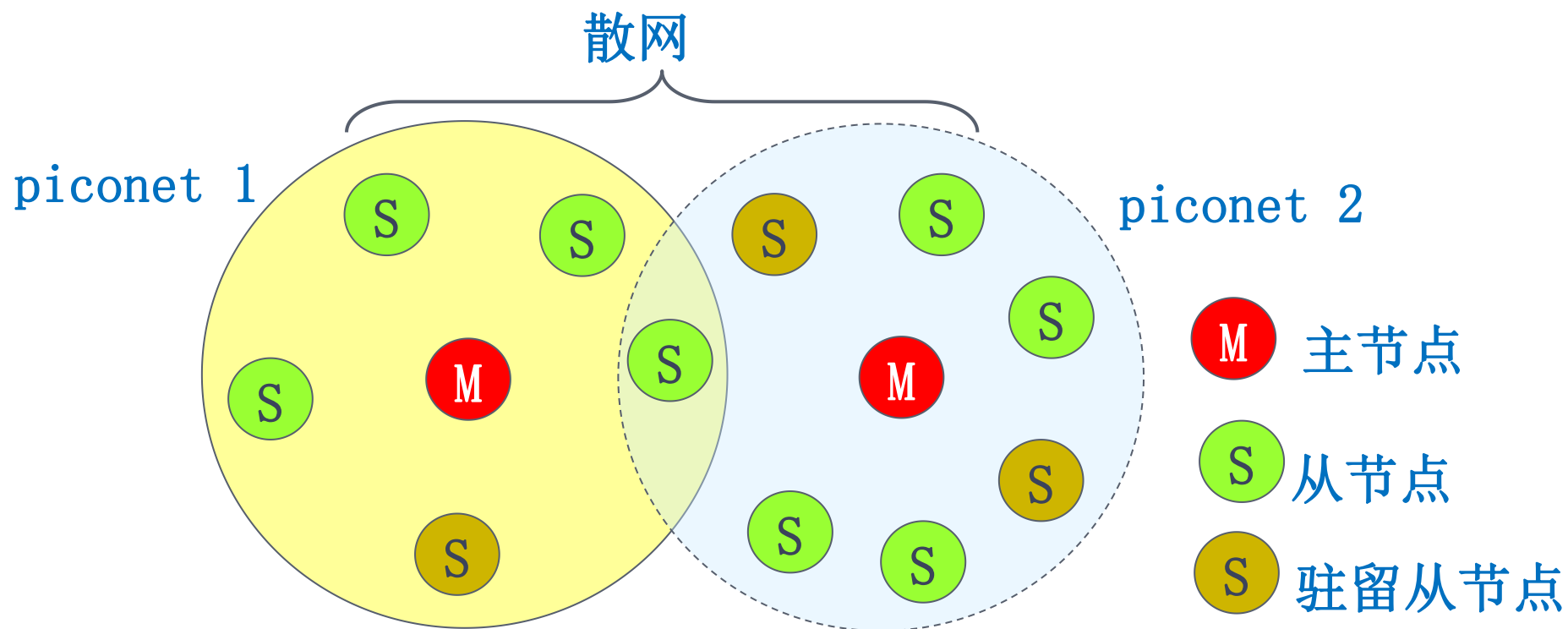
- 1999年1月发布蓝牙1.0版本，2004年发布2.0，2009年发布3.0.同年12月发布4.0版本可进行低功率操作。
- 用于构建10米左右小型的局域网，广泛应用于各类电子设备，传输速率1Mbps。
- 蓝牙使用 TDM 方式和扩频跳频 FHSS 技术组成不用基站的皮可网(piconet)，直译就是“微微网”，表示这种无线网络的覆盖面积非常小。



4.6 蓝牙

○ 蓝牙体系结构

每一个piconet有一个主设备和最多7个工作的从设备，还可以有255个驻留节点（低功耗专题，只处于保持和嗅探状态）。



4.6 蓝牙

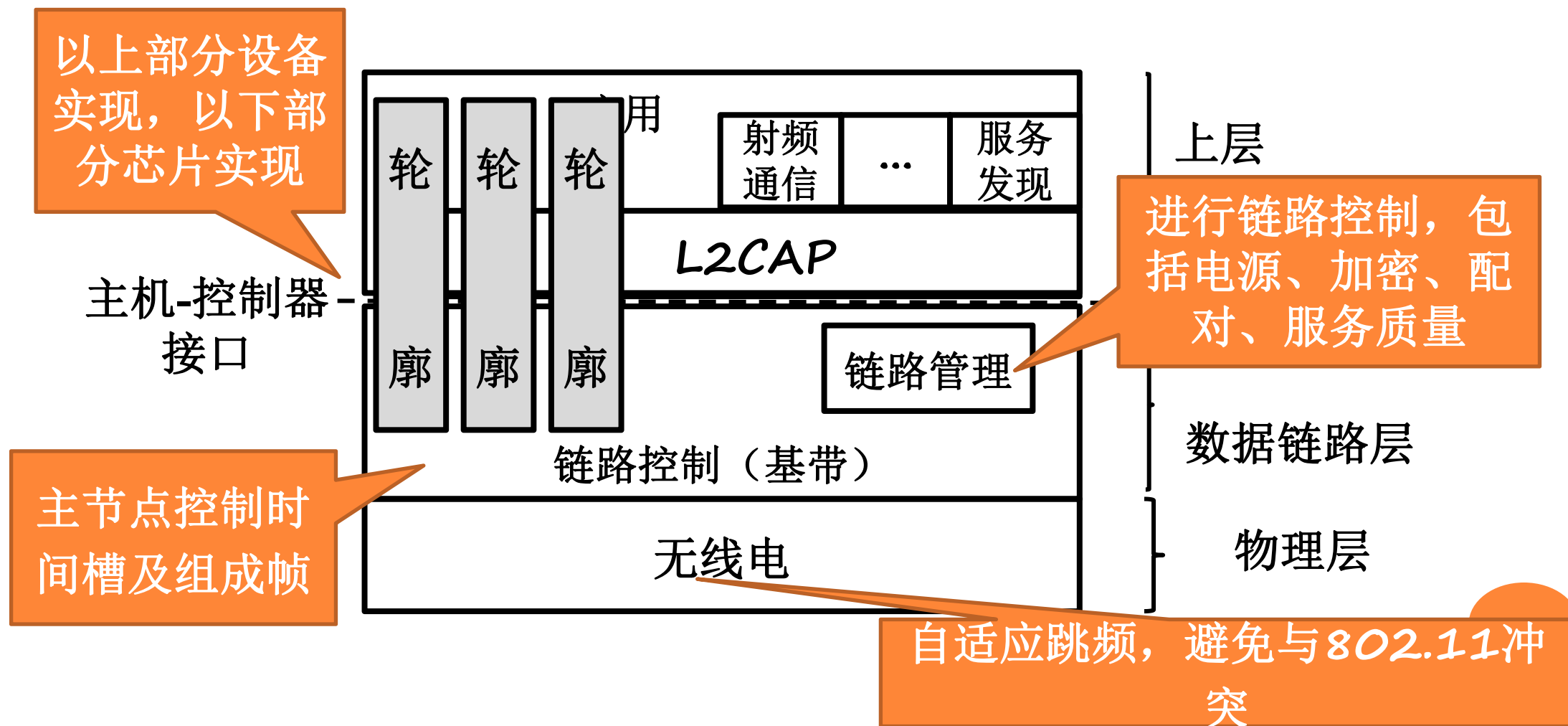
○ 蓝牙应用

- ✓ 蓝牙SIG列出了所支持的各类应用以及对应的协议栈。共支持25种应用，称为profiles（轮廓、协议、应用、配置…）
- ✓ 对讲机、无线耳麦、免提、人机接口定义了一些非组网的模式。
- ✓ 个域网等可形成自组织网络，通过接入点访问其他网络



4.6 蓝牙

蓝牙协议栈



4.6 蓝牙

- **蓝牙链路层**

- 链路管理协议负责建立逻辑信道，包括配对、建立链路

- 配对

 - ❧ 旧配对方法：配置相同的PIN（个人识别号）

 - ❧ 新配对方法：输入密码

- 建立链路

 - ❧ 同步有连接：实时数据传输

 - ❧ 异步无连接：尽力而为的投递，无服务质量保证



4.6 蓝牙

○ 蓝牙帧结构

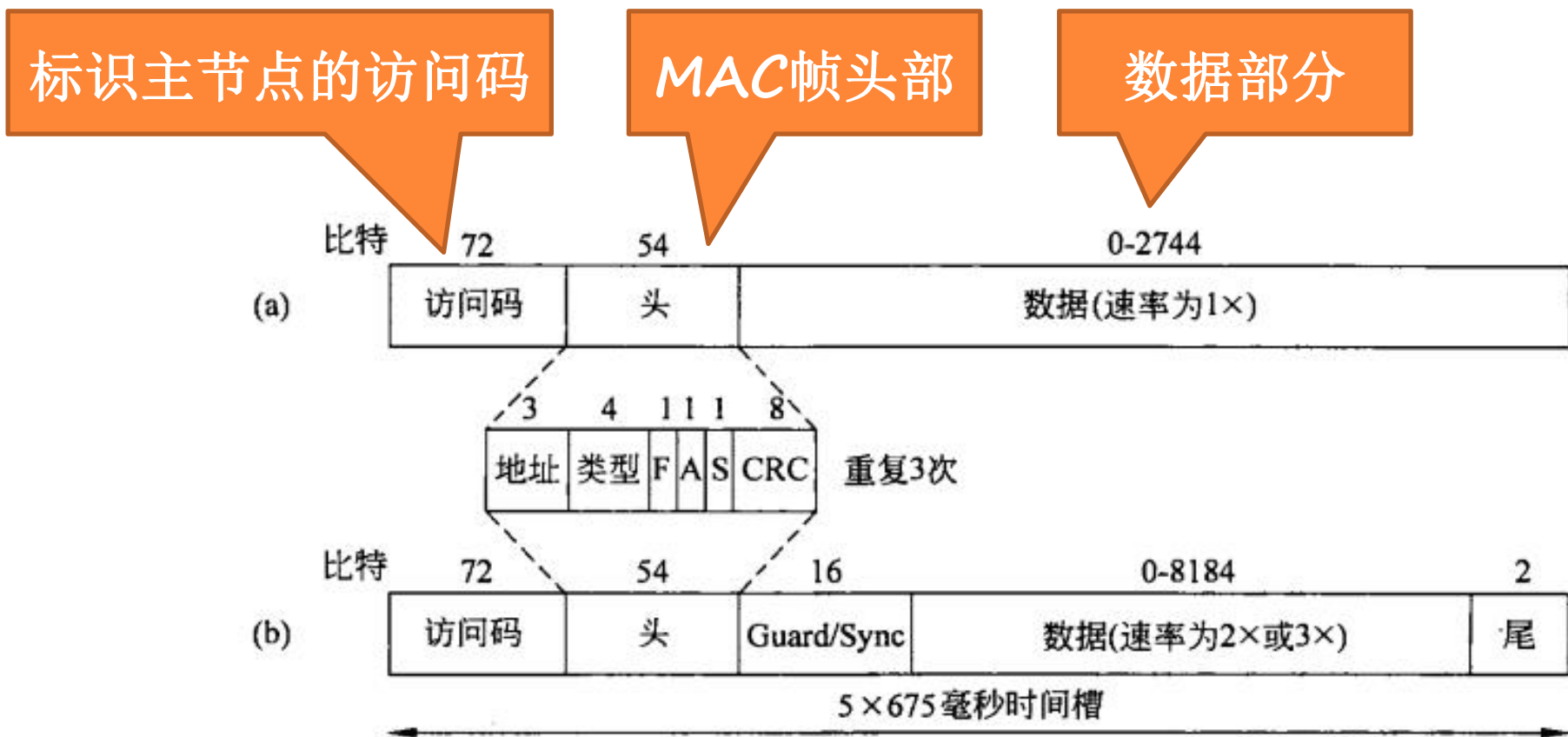


图 4-36 两种情况下的典型蓝牙数据帧
(a) 基本型; (b) 增强型

4.7 RFID无线射频识别

- EPC Gen2体系结构与物理层
- 包括标签和读写器。读写器从标签种读取96位EPC识别码和内存信息。
- 使用后向散射技术
 - ∞ 标签使用读写器发送的信号获取能量，改变信号或反射信号，完成数据的传输

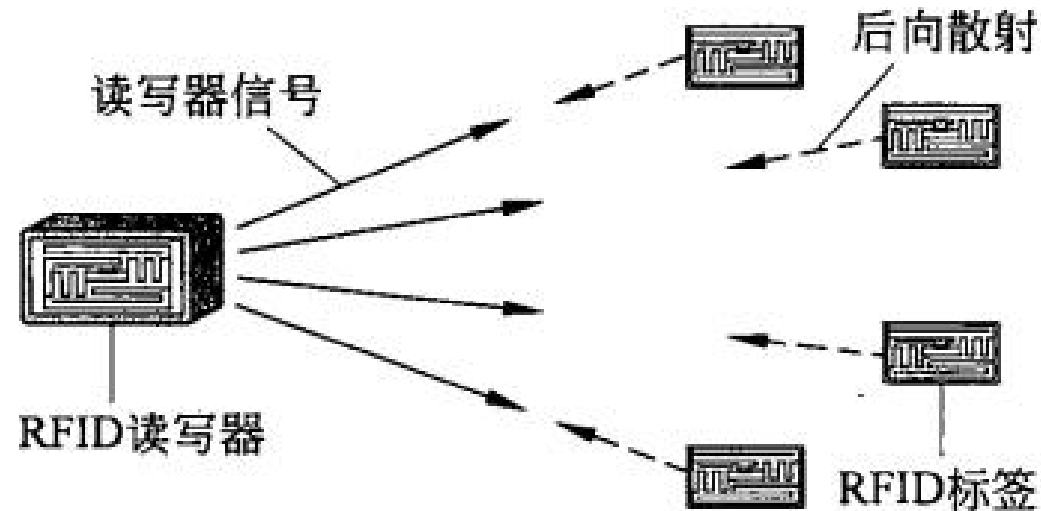
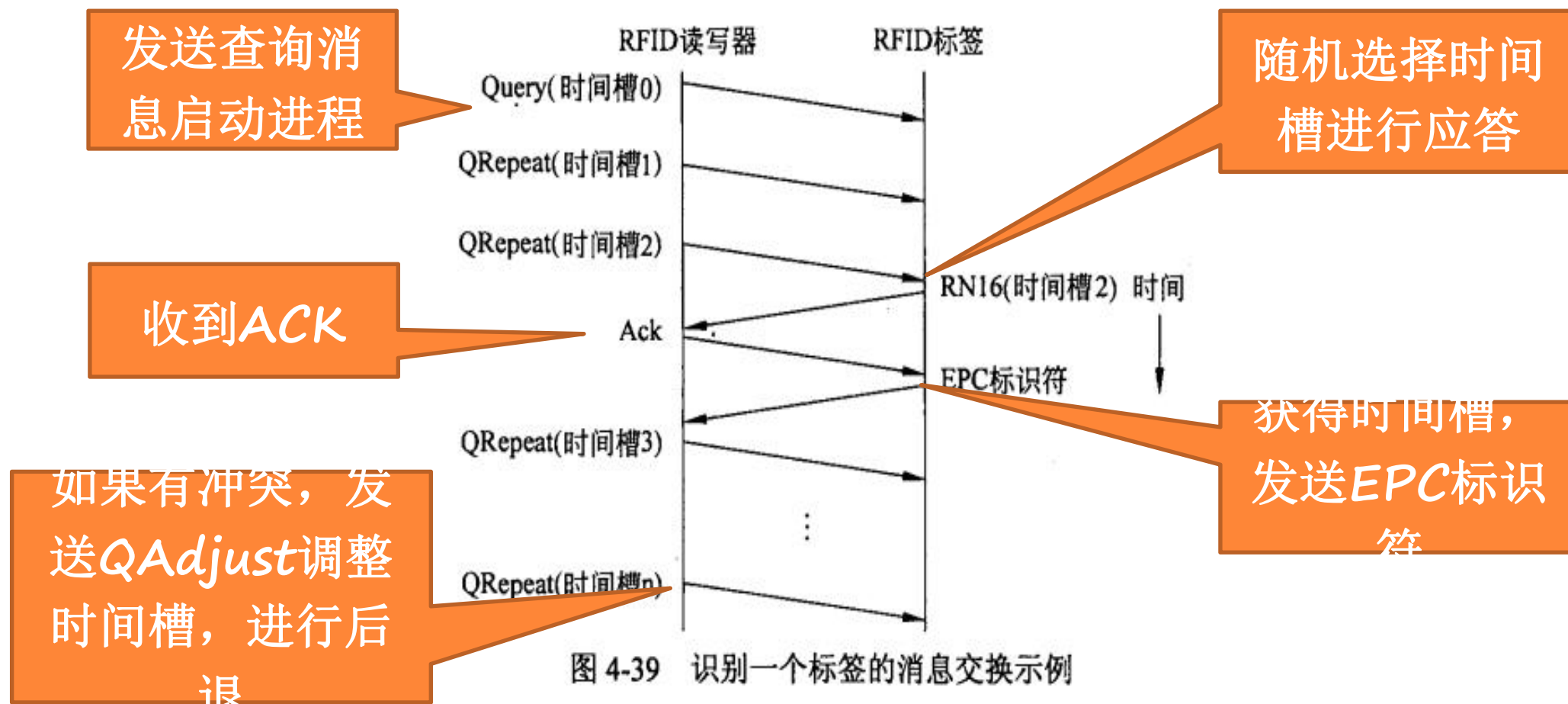


图 4-37 RFID 体系结构

4.7 RFID无线射频识别

○ EPC Gen2标签识别层



4.7 RFID无线射频识别

标签标识消息格式



图 4-40 查询消息的格式

标识消息是
查询消息

标志位: *DR*、*M*、*TR*,
确定了读写器传输和标
签响应的物理层参数

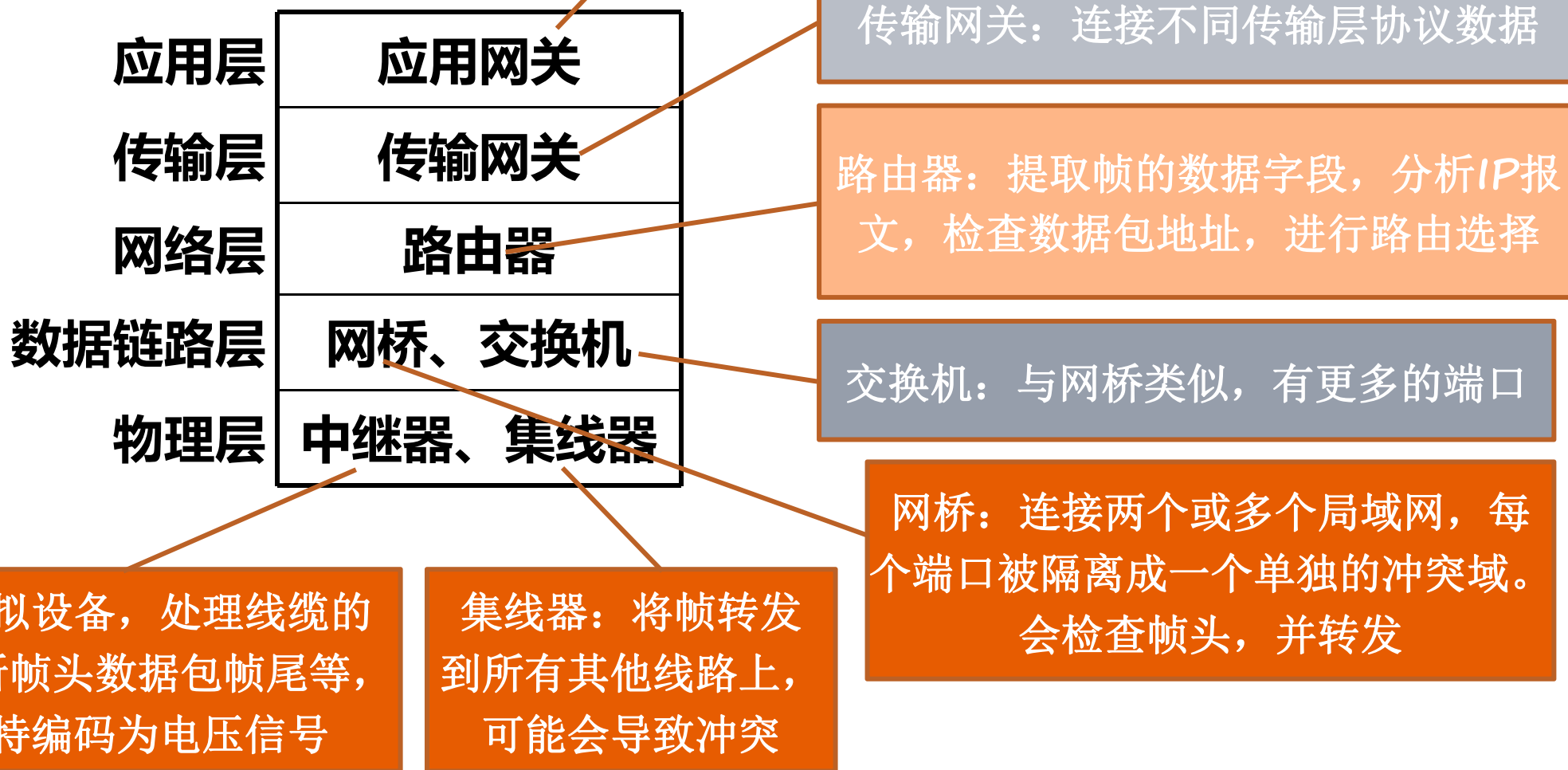
选择标签作出回应, 标签最多可
跟踪四个并发的会话以及它们是
否在这些会话中已被识别

4.8 数据链路层交换

- 如果要组建更大的网络，将各局域网连接起来。如何相互连接？
- 集线器、网桥、交换机、路由器、网关等
- 分别运行在不同层次上，传递不同类型的数据包。



不同的网络互联设备



4.8 数据链路层交换

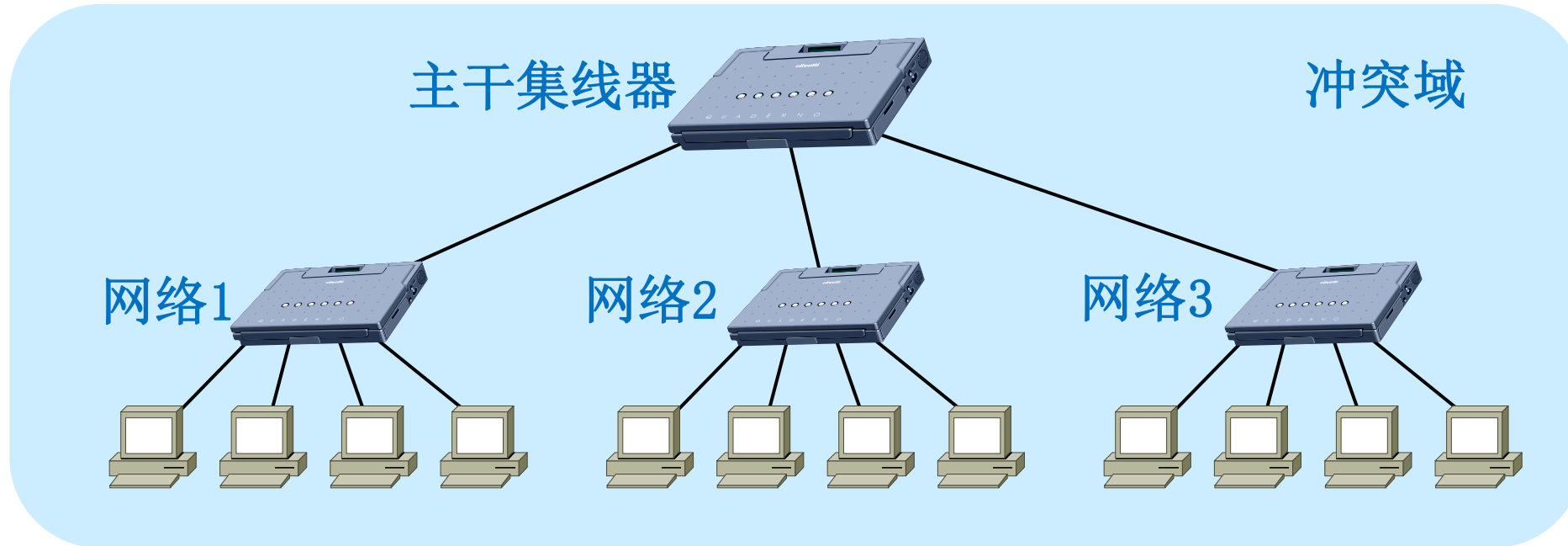
- 网桥：工作在链路层，通过检查链路层地址来转发帧。可以把多个物理局域网连接成一个逻辑局域网。
- 虚拟局域网：把一个物理局域网划分为多个逻辑局域网



4.8 数据链路层交换

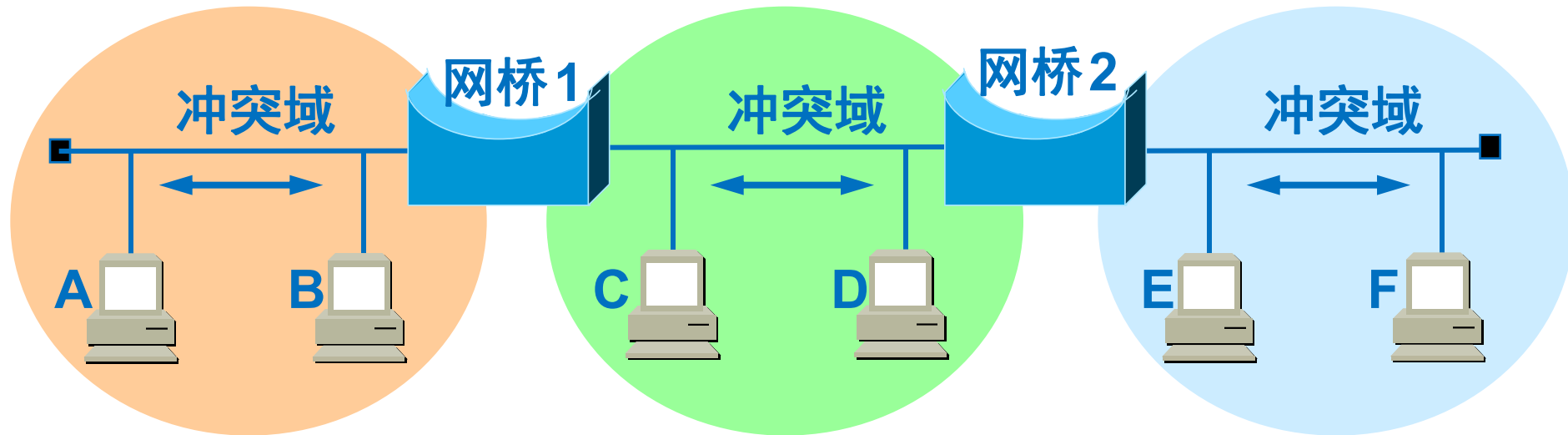
- 用集线器组成更大的局域网都在一个碰撞域中

一个更大的冲突域



4.8 数据链路层交换

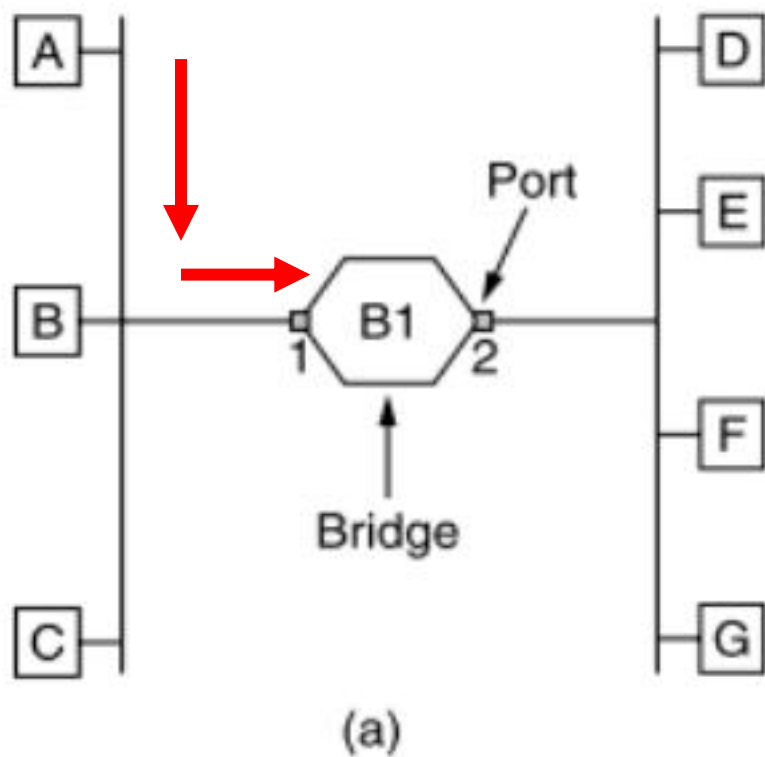
- 用网桥使各网段成为隔离开的冲突域



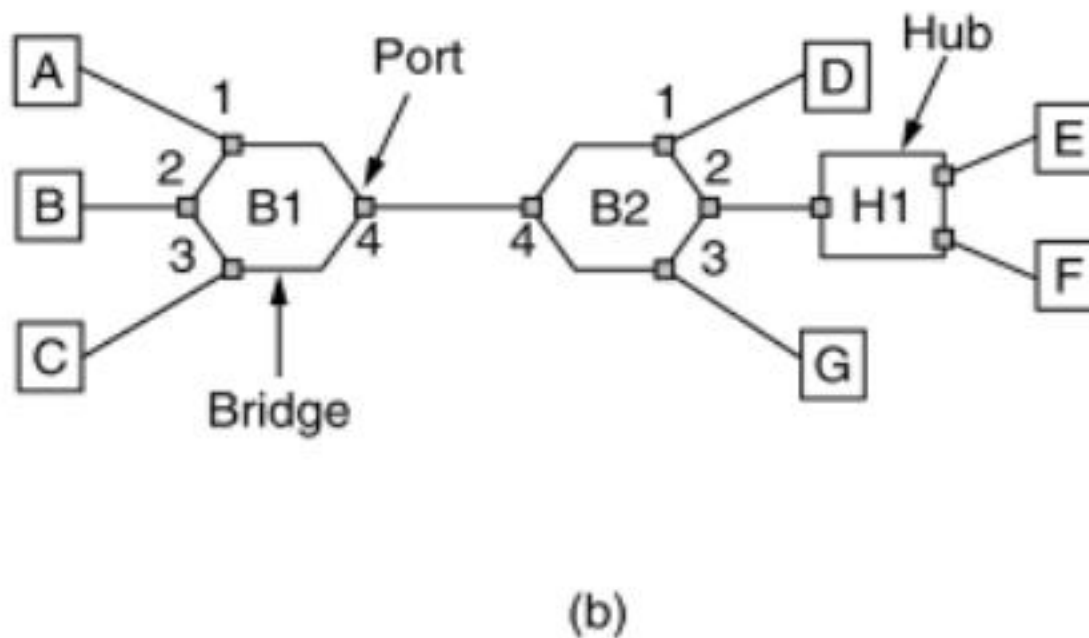
4.8.2 学习网桥

○ 学习网桥:

连接两个多点LAN



连接点到点LAN



4.8.2 学习网桥

- 网桥如何建立这种哈希表？

- ✓ 第一次接入网络时，所有哈希表都是空的。使用泛洪算法（flooding），网桥将接收到的帧发送到所有端口（来源的输入端口除外），随时间推移，网桥学习到每个目标地址在那里。一旦知道了一个目标地址，以后发给该地址的帧只被放到正确的端口，而不再被泛洪到所有端口。

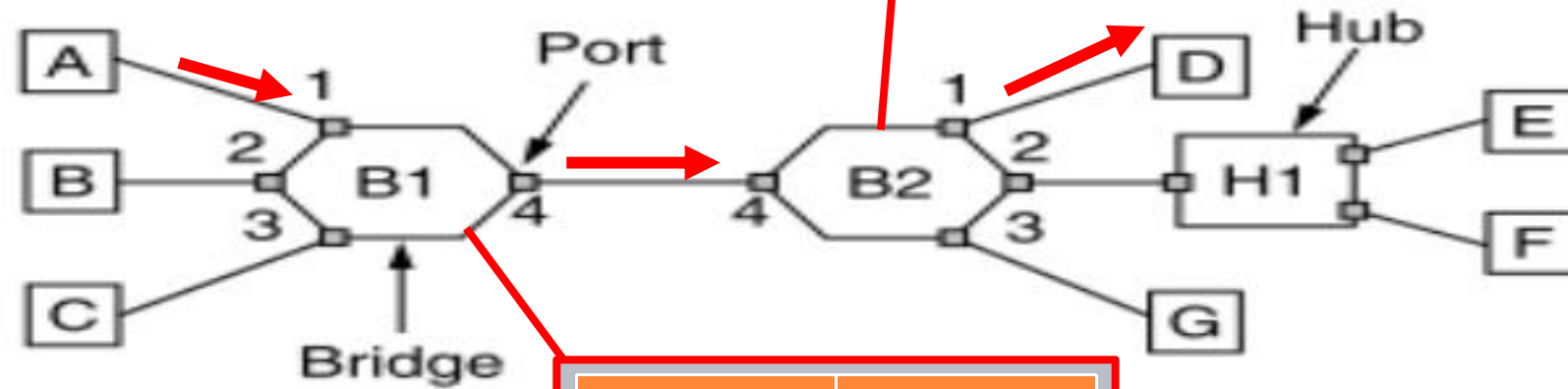
- ✓ 转发过程如下：

为了应对拓扑变化的情况，在表中加入时间，表项总是最新的地址记录。定期扫描哈希表，以确保数据周期的更新。



4.8.2 学习网桥

○ 学习网桥:



B2的哈希表

目的	端口
A	4
B	4
C	4
D	1

B1的哈希表

目的	端口
A	1
B	2
C	3
D	4

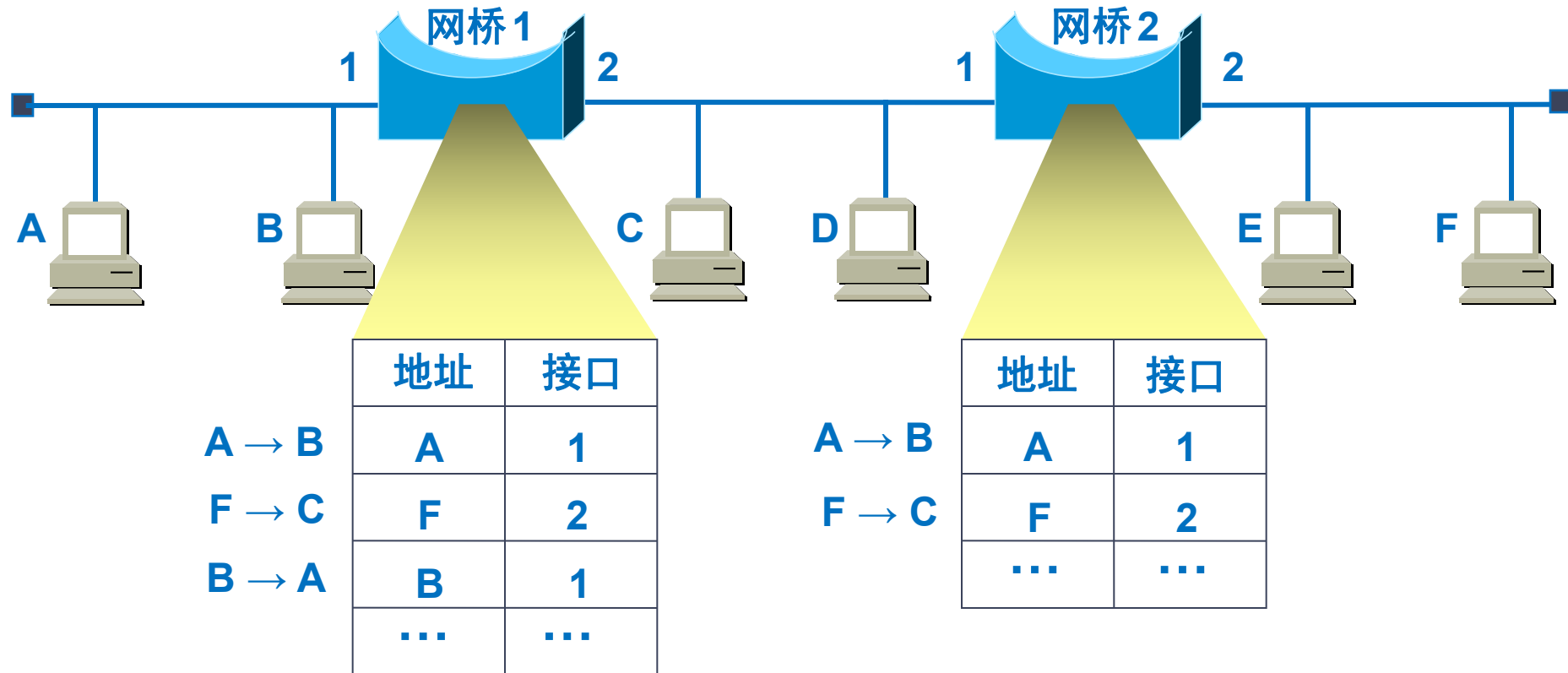
4.8.2 学习网桥

- 网桥如何建立这种哈希表?
- 建立起哈希表后，网桥转发过程如下
- 如果目的地址端口与源端口相同，丢弃
- 如果目的地址端口与源端口不同，转发
- 如果目的地址端口位置，使用泛洪算法（不包括输入端口）



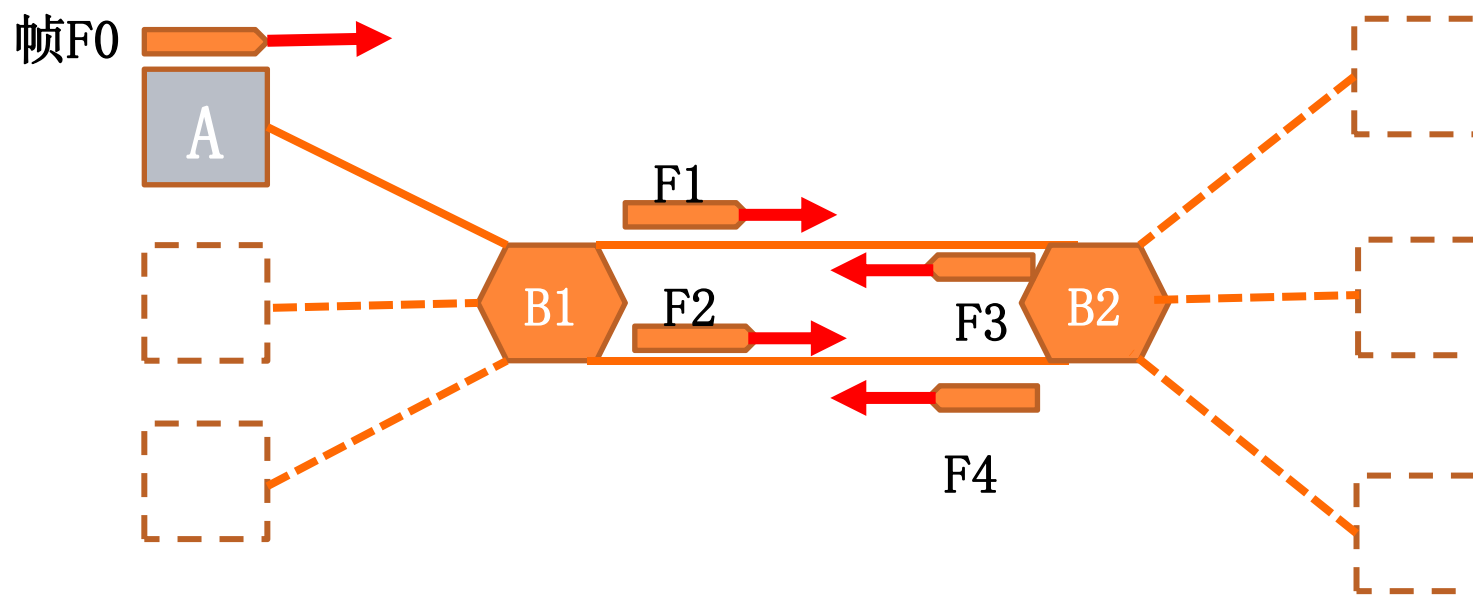
4.8 数据链路层交换

- 网桥如何建立这种哈希表？



4.8.3 生成树网桥

- 生成树网桥：为解决冗余链路的无限循环问题，使用树形结构构造网络拓扑图。



4.8 数据链路层交换

- 生成树网桥802.1D
- 让网桥之间相互通信，用一棵可以到达每个网桥的生成树覆盖实际的拓扑。这个无环拓扑是实际拓扑的一个子集。
- 所有网桥首先选择一个网桥作为生成树的根，通过比较相互之间标识符的大小选出最低数字的作为根节点，然后构造根到每个网桥的最短路径树。
- 最终每个源到每个目标都只有唯一的一条路径，不再会产生环路。



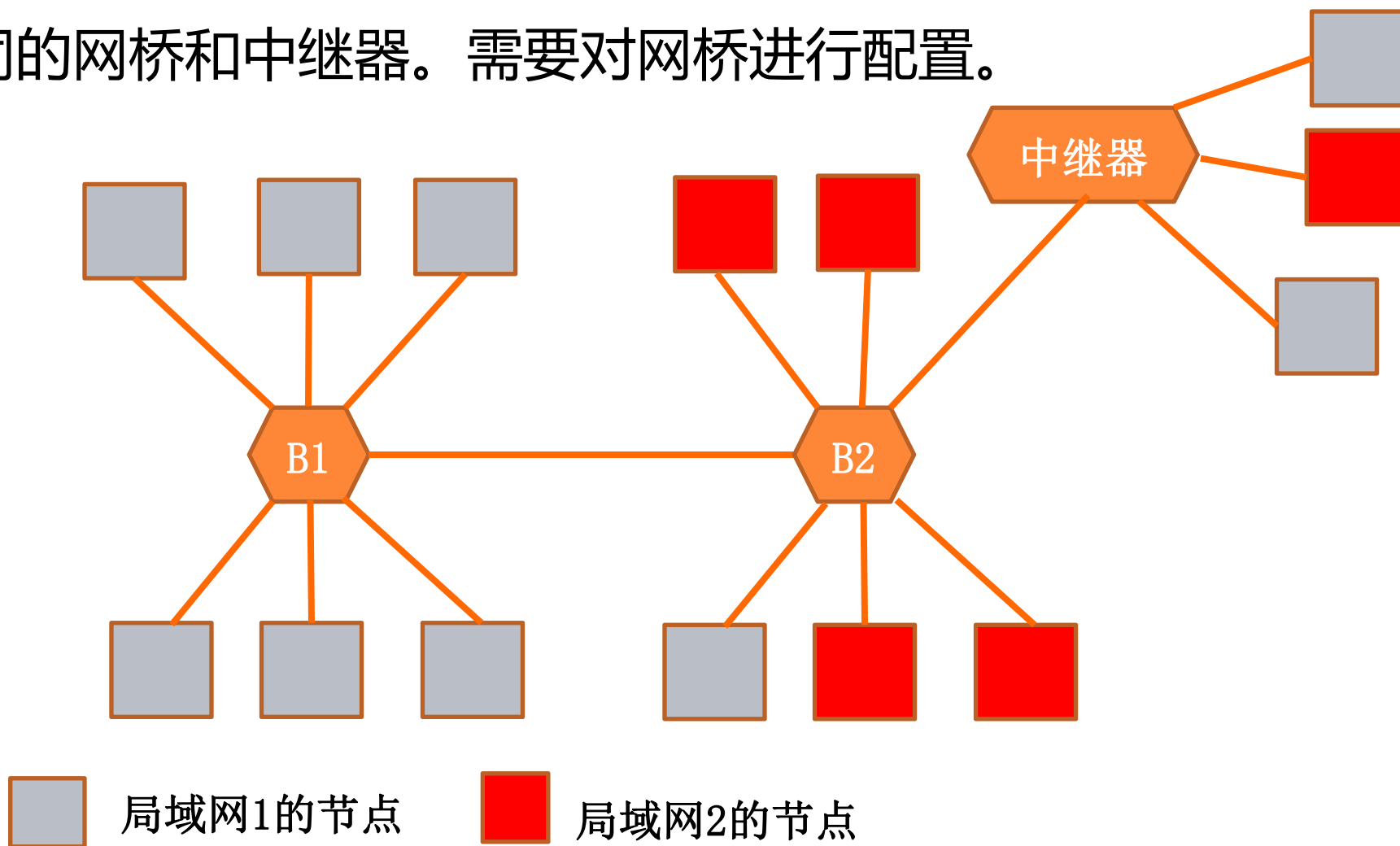
4.8.5 虚拟局域网

- 为什么要对局域网进行划分？
- 信息安全与业务需求。需要将不同部门之间的计算机从逻辑上隔离开。
- 负载均衡问题，需要将重负载的网络与其他网络分开。
- 避免广播风暴：网络规模越大，广播信息越占资源。
- 采用虚拟局域网技术，将实际的物理连接的局域网划分为若干逻辑上不相连的规模更小的多个局域网。
- 虚拟局域网其实只是局域网给用户提供服务的一种服务，而并不是一种新型局域网。



4.8.5 虚拟局域网

- 如图所示红蓝两个不同的局域网，其中的计算机分别连接不同的网桥和中继器。需要对网桥进行配置。



IEEE 802.1Q 标准

VLAN标准802.1Q于1998年公布

- 802.1Q必须解决的两个问题:

- ∞ VLAN必须有一个VLAN的*field*来标志

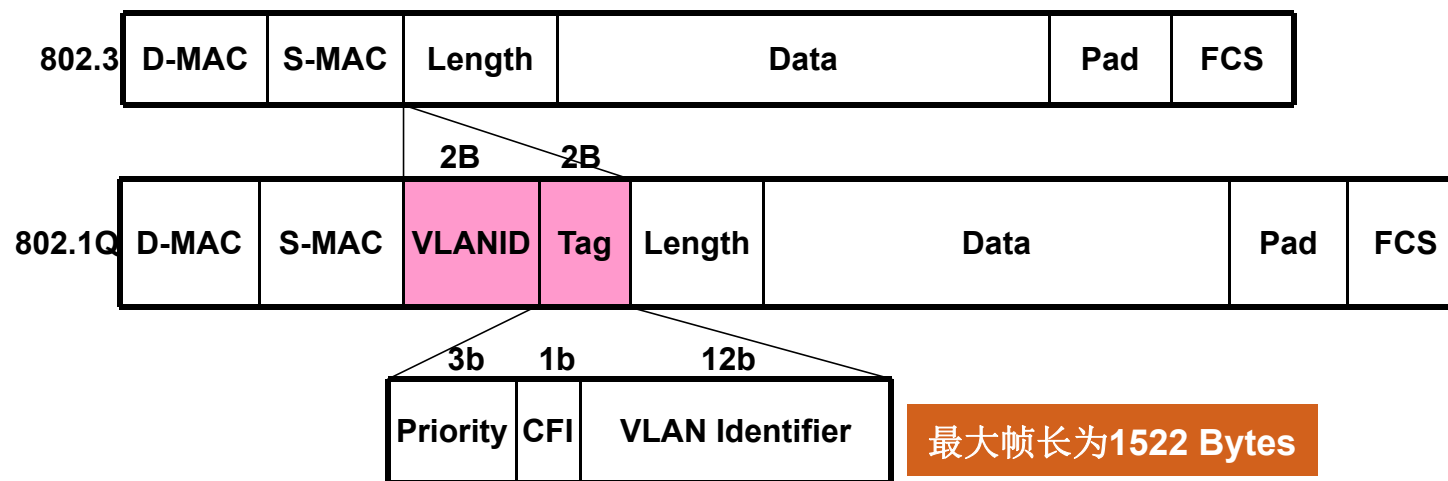
- ∞ 802.1Q必须与802.3标准相兼容

数据帧的成帧工作由数据链路层完成，即由网卡完成，但现有网卡不支持802.1Q



以太网中的VLAN标志域

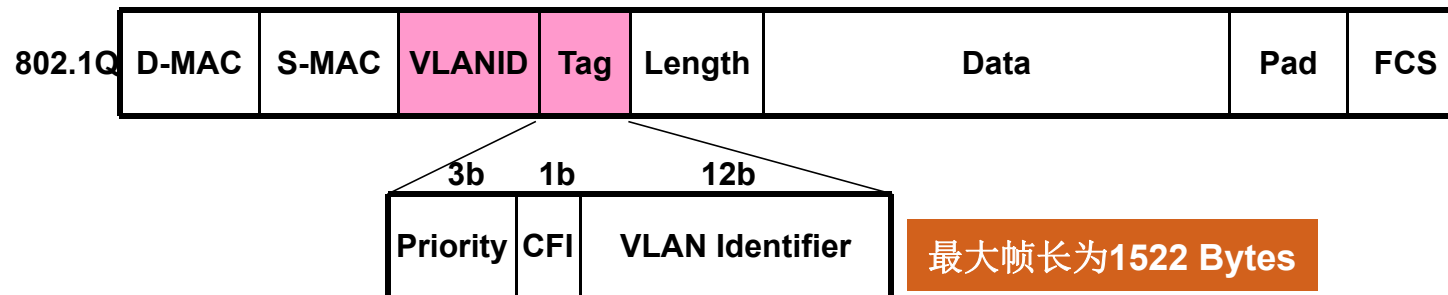
802.1Q 的以太网帧格式



Tnbn P335 Fig. 4-51 802.3和802.1Q以太网帧格式

802.1Q 的以太帧格式说明

- VLAN-ID 16 bit
 - ∞ VLAN协议标识, 恒为0x8100
- Priority 3 bit
 - ∞ Priority, 暂且保留
- CFI 1 bit
 - ∞ 标准格式标志位
- VLAN Identifier 12 bit
 - ∞ VLAN标识, VLAN编号



IEEE 802.1Q 标准

VLAN标准802.1Q在1998年公布

- 802.1Q必须解决的两个问题:
 - ✎ VLAN必须有一个VLAN的*field*来标志
 - ✎ 802.1Q必须与802.3标准相兼容

数据帧的成帧工作由数据链路层完成，即由网卡完成，但现有网卡不支持802.1Q



与802.3标准兼容

- 802.3协议包括：
 - ✎ 802.3 10M bps的以太网协议
 - ✎ 802.3u 100M bps的快速以太网协议
 - ✎ 802.3z 1000M bps的千兆以太网协议
- 千兆以太网的网卡已支持VLAN
 - ✎ 可识别和生成帧长为1522 Bytes的帧

802.3的帧长为1518 Bytes



传统帧格式与VLAN兼容

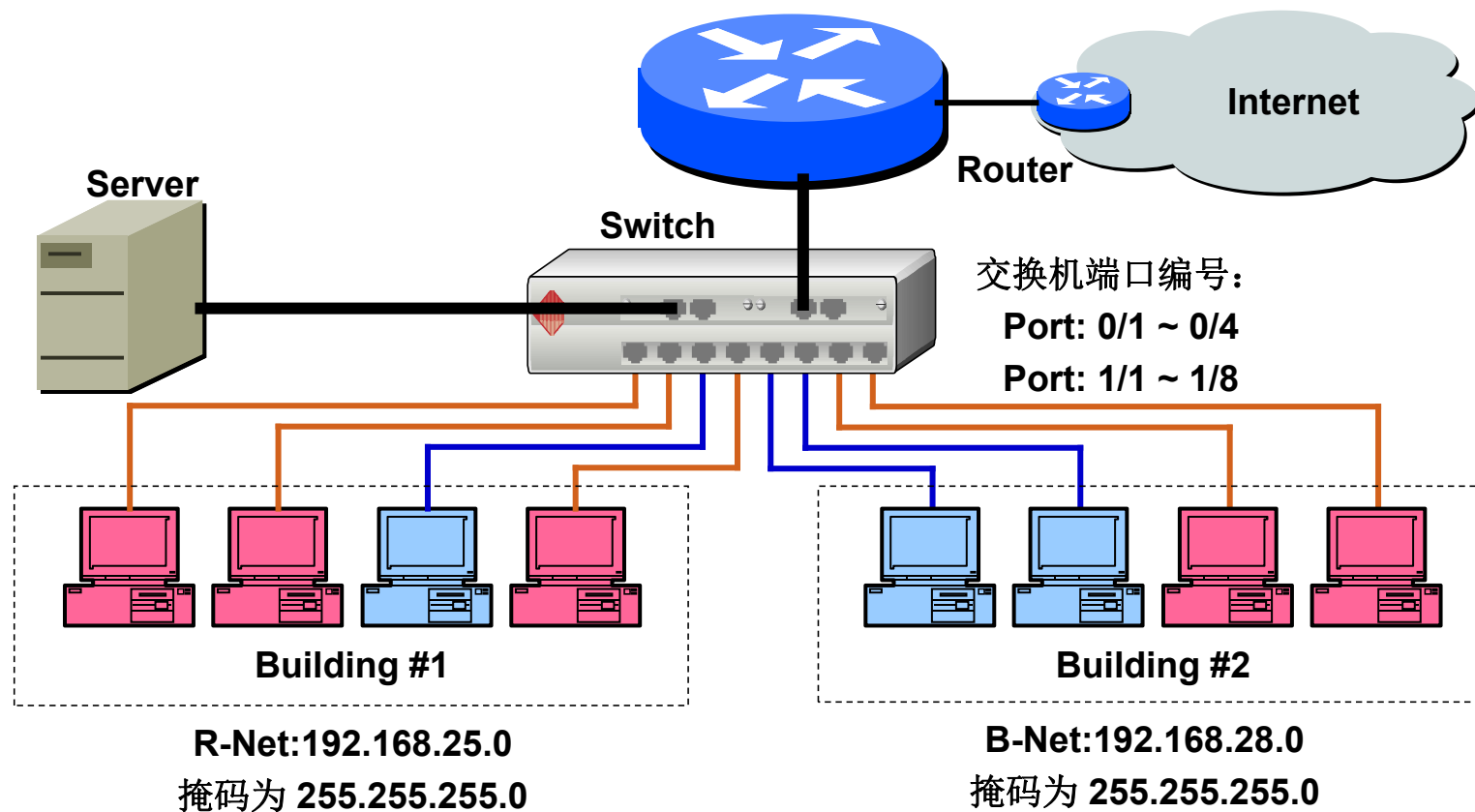
对VLAN 敏感（**aware**）的和不敏感的交换机必须允许混合使用

- VLAN标志是供交换机（网桥）来识别该帧的源站点主机属哪个VLAN
- 目前使用的网卡基本都对VLAN不敏感，即不允许帧长超过1518 Bytes
：既不能识别或也不能生成VLAN标志
- 如一个VLAN涉及多台交换机，则在帧的传输中，第一台VLAN敏感的交换机负责在帧格式中添加VLAN标志，并由最后一台交换机删除VLAN标志



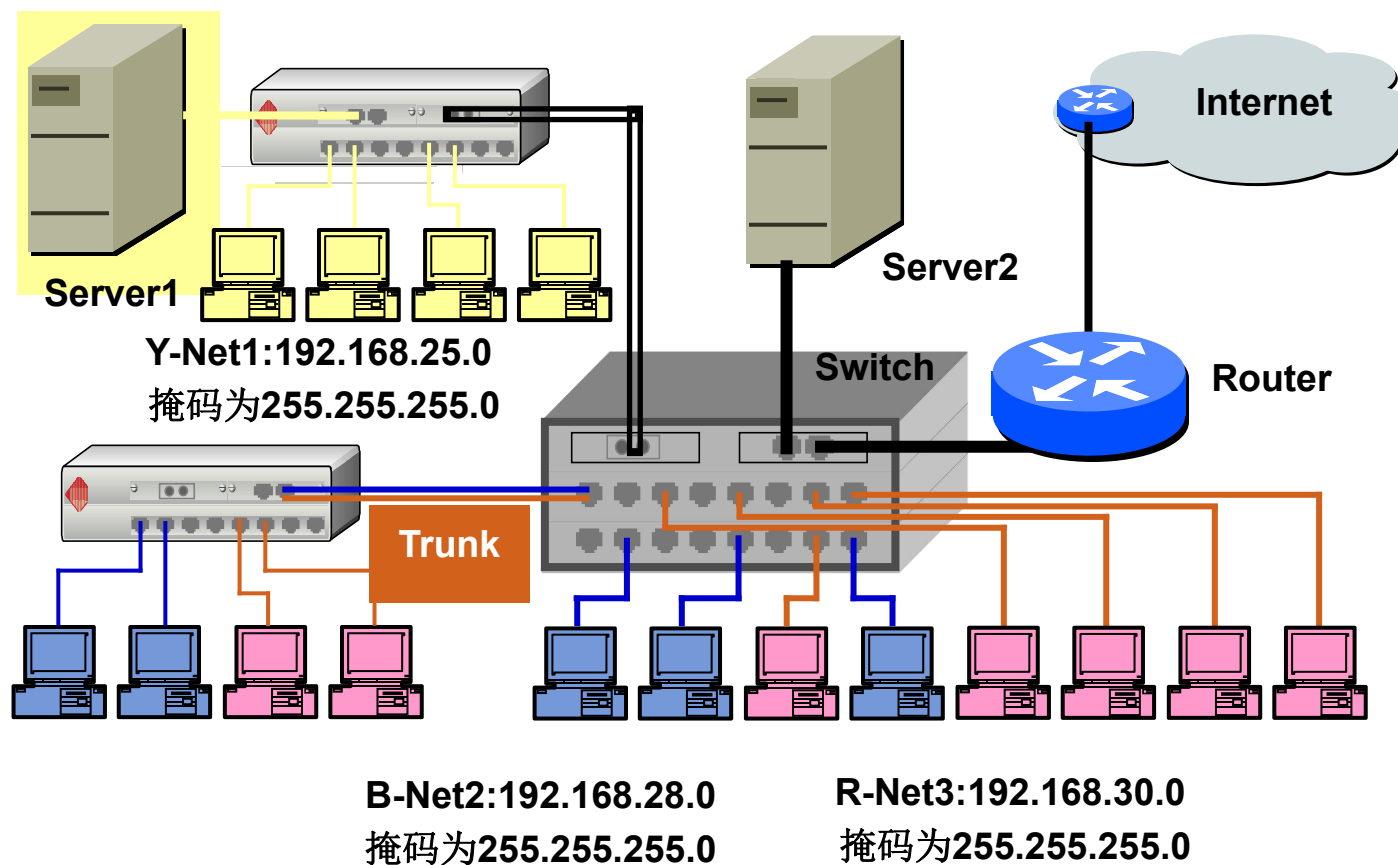
VLAN的标志

- 各主机所属VLAN由交换机识别，送给主机的帧格式中无需添加VLAN标志



VLAN的标志（续）

- 两台交换机间要传输VLAN信息，帧格式中必须包含VLAN标志，这就是Trunk功能



第4章 习题

第一次：6、18（已完成）

第二次：24、31、34、38

