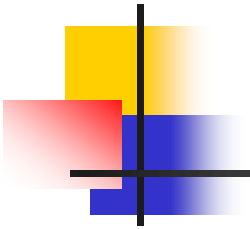
广东开放大学
The Open University of Guangdong



第三章 数据链路层

谢剑刚
广东开放大学

数据链路层

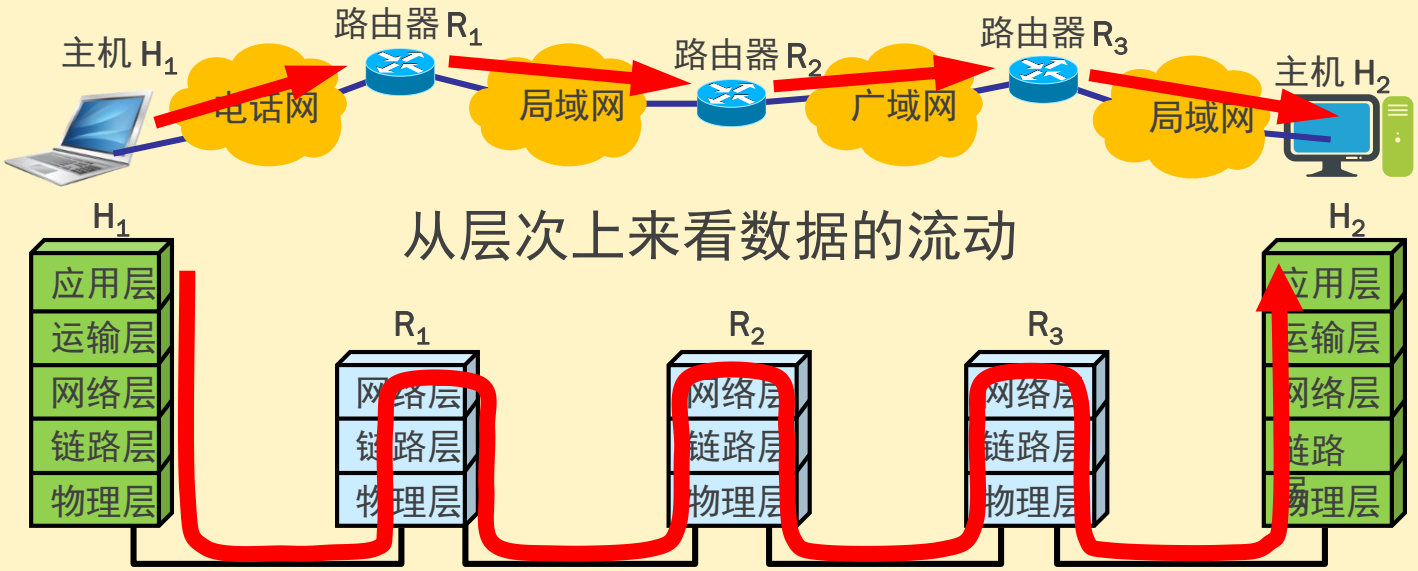
数据链路层使用的信道主要有以下两种类型：

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。

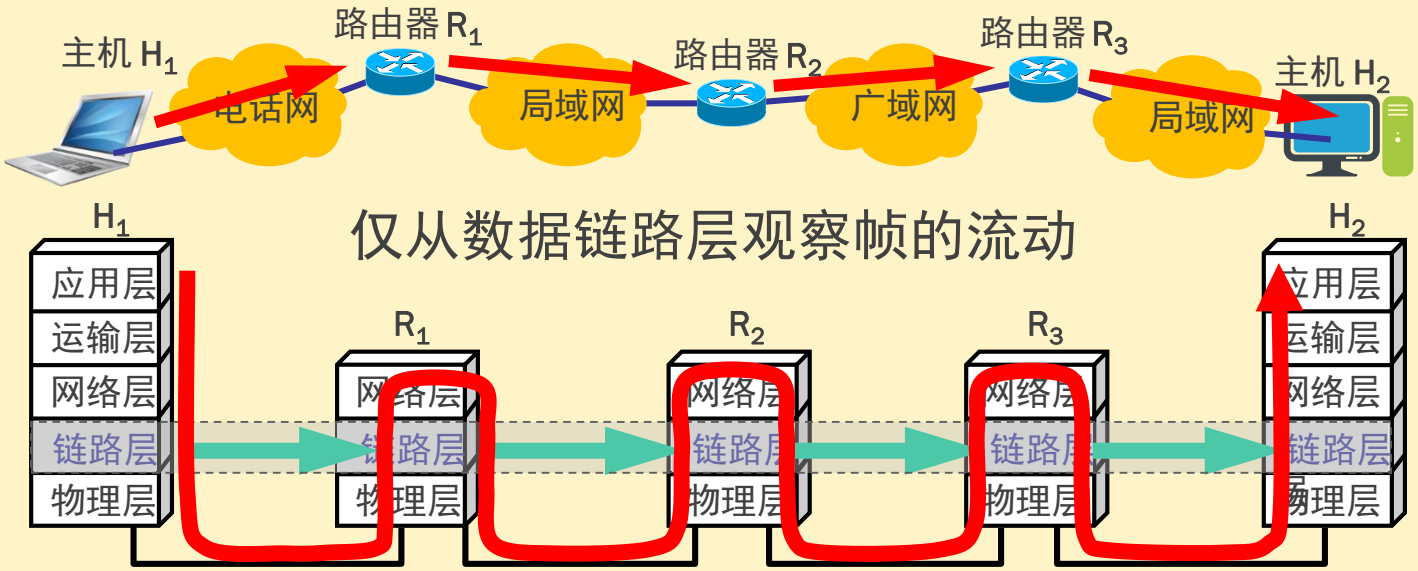
3.1.1 数据链路层所处的地位

- 主机 H_1 向 H_2 发送数据



3.1.1 数据链路层所处的地位

- 主机 H_1 向 H_2 发送数据

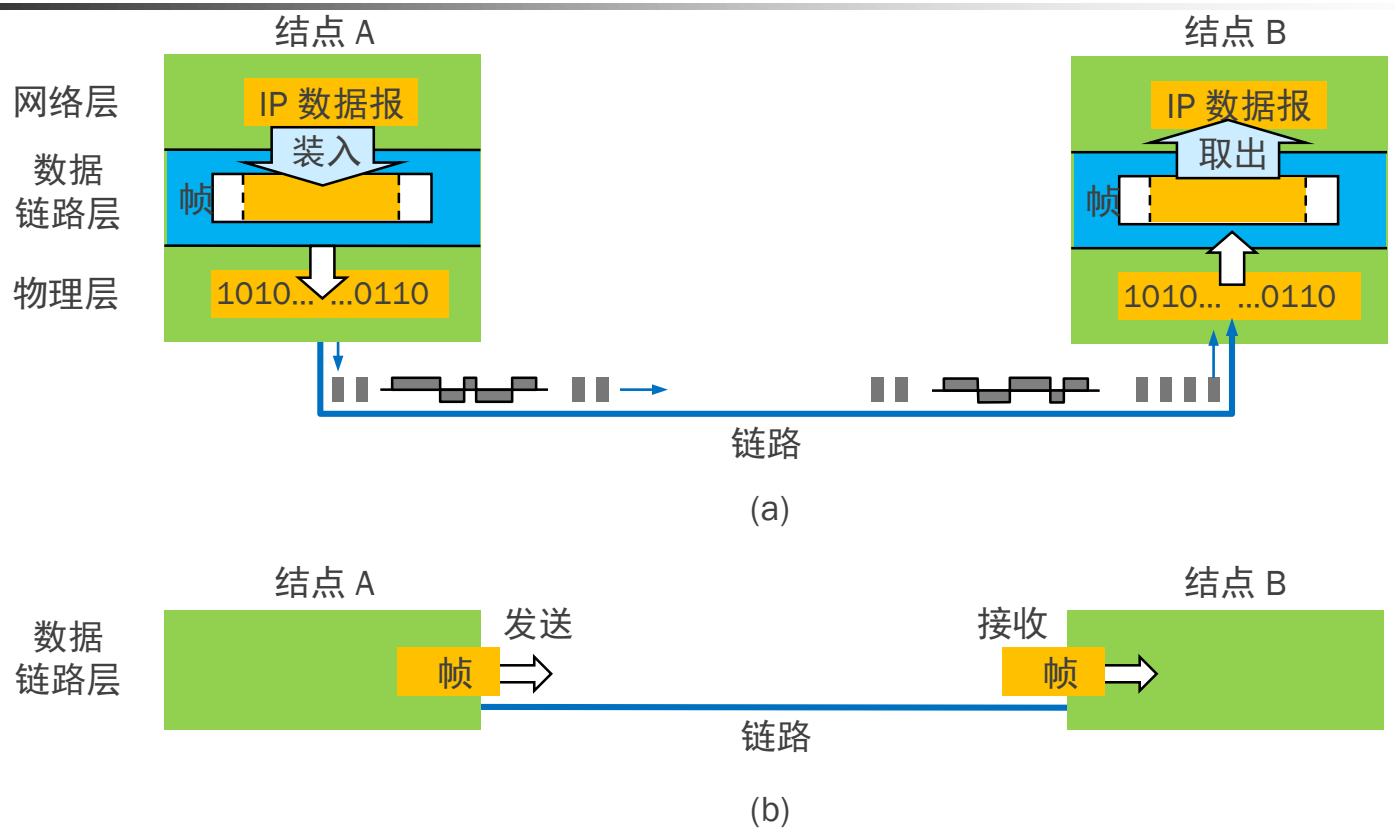


3.1.2 数据链路和帧

- **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。

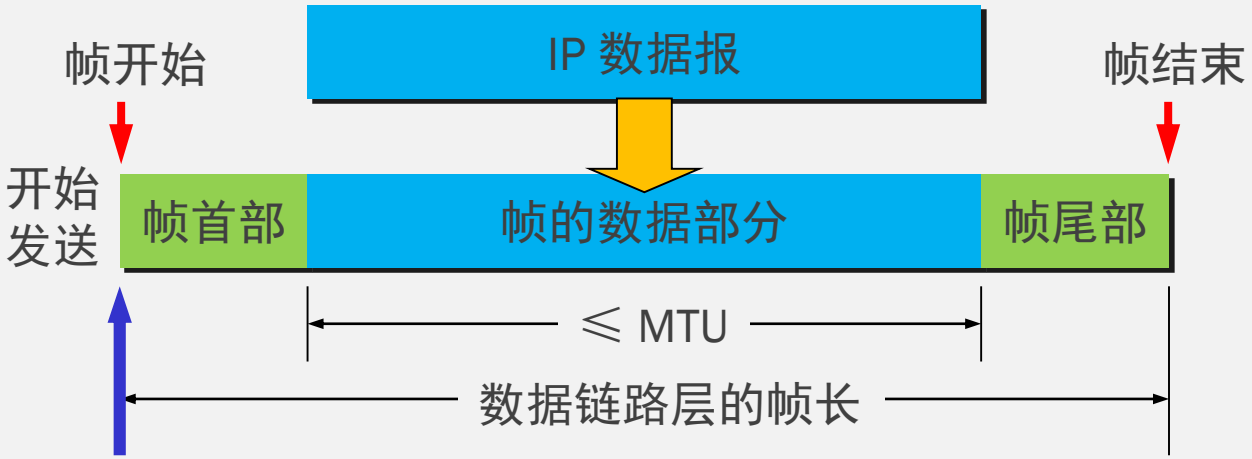
- **数据链路**(data link) 除了物理线路外，还必须有通信协议来控制这些数据的传输。若把实现这些协议的硬件和软件加到链路上，就构成了数据链路。
  - 现在最常用的方法是使用适配器（即网卡）来实现这些协议的硬件和软件。
  - 一般的适配器都包括了数据链路层和物理层这两层的功能。

数据链路层传送的是帧

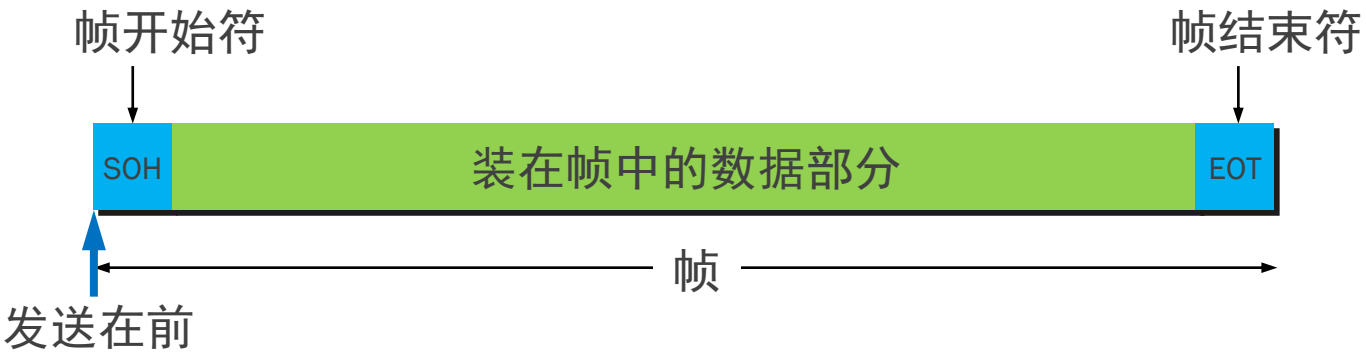

结点 A
结点 B
网络层
数据
链路层
物理层
IP 数据报
装入
帧
1010... ...0110
IP 数据报
取出
帧
1010... ...0110
链路
(a)
结点 A
结点 B
数据
链路层
发送
帧
接收
帧
链路
(b)

3.1.3 封装成帧

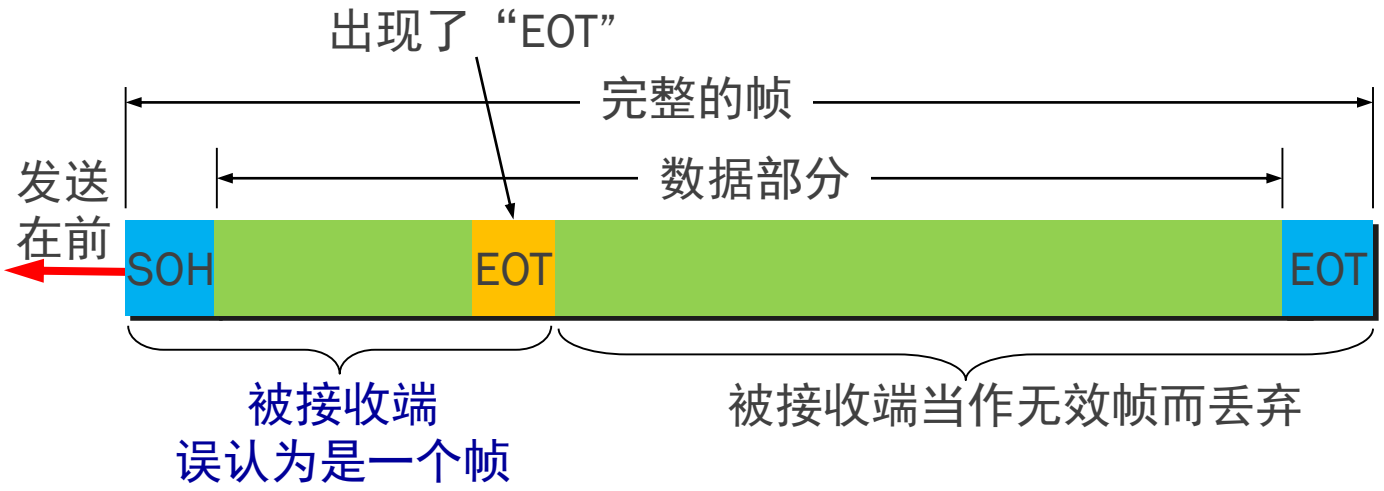
- 封装成帧(framing)就是在一段数据的前后分别添加首部和尾部，然后就构成了一个帧。确定帧的界限。
- 首部和尾部的一个重要作用就是进行帧定界。



用控制字符进行帧定界的方法举例



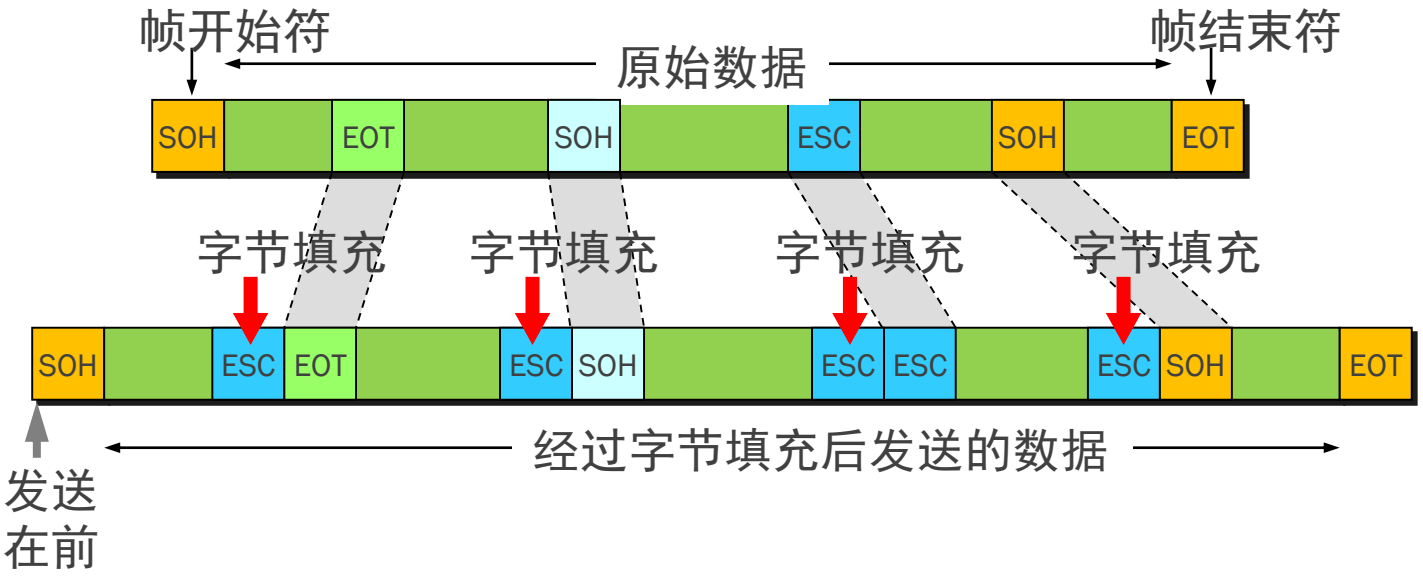
透明传输


出现了“EOT”
完整的帧
数据部分
发送
在前
SOH
EOT
EOT
被接收端
误认为是一个帧
被接收端当作无效帧而丢弃

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。

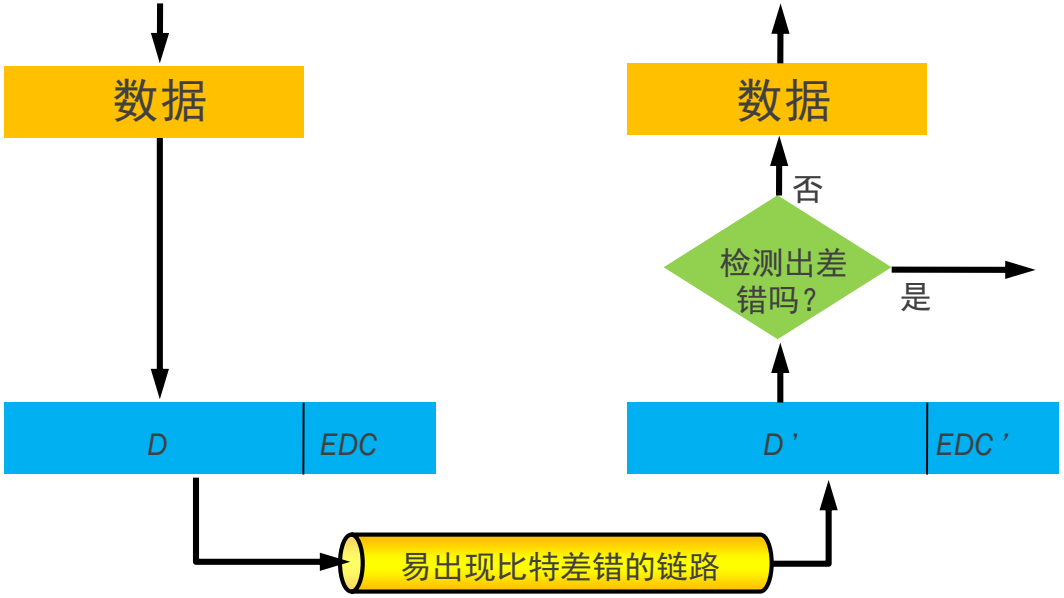
用字节填充法解决透明传输的问题



3.1.4 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。

差错检测的基本原理



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

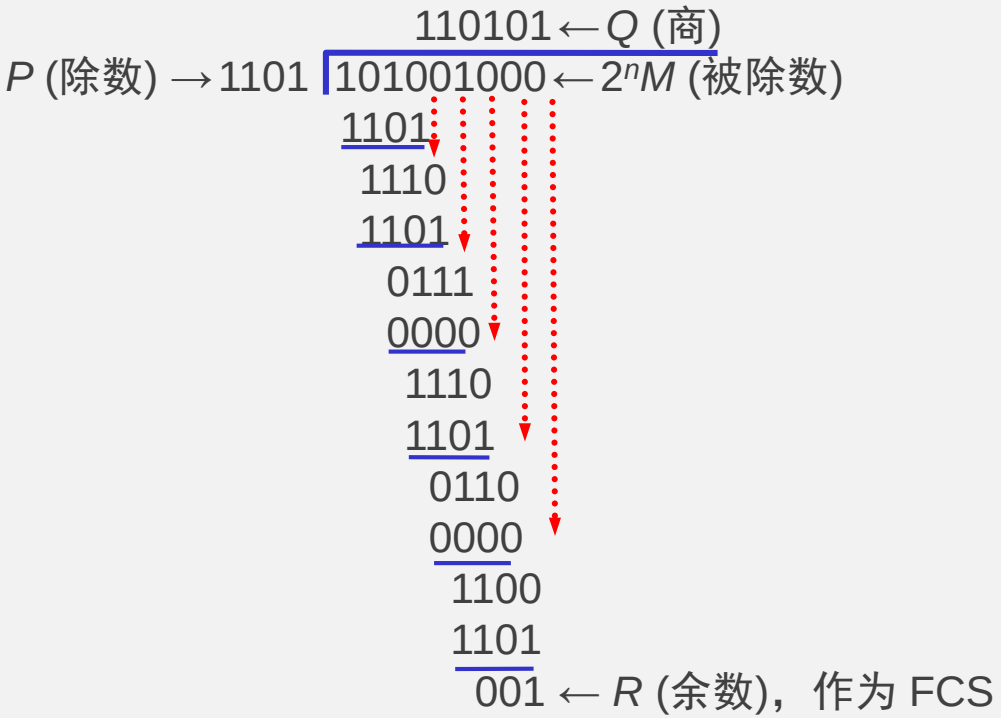
- 用二进制的模 2 运算进行 2^n 乘 M 的运算，这相当于在 M 后面添加 n 个 0。
- 得到的 $(k + n)$ 位的数除以事先选定好的长度为 $(n + 1)$ 位的除数 P，得出商是 Q 而余数是 R，余数 R 比除数 P 少1 位，即 R 是 n 位。

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 $2^nM = 101001000$。
- 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: $2^nM + R$

  即: 101001001, 共 $(k + n)$ 位。

循环冗余检验的原理说明



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

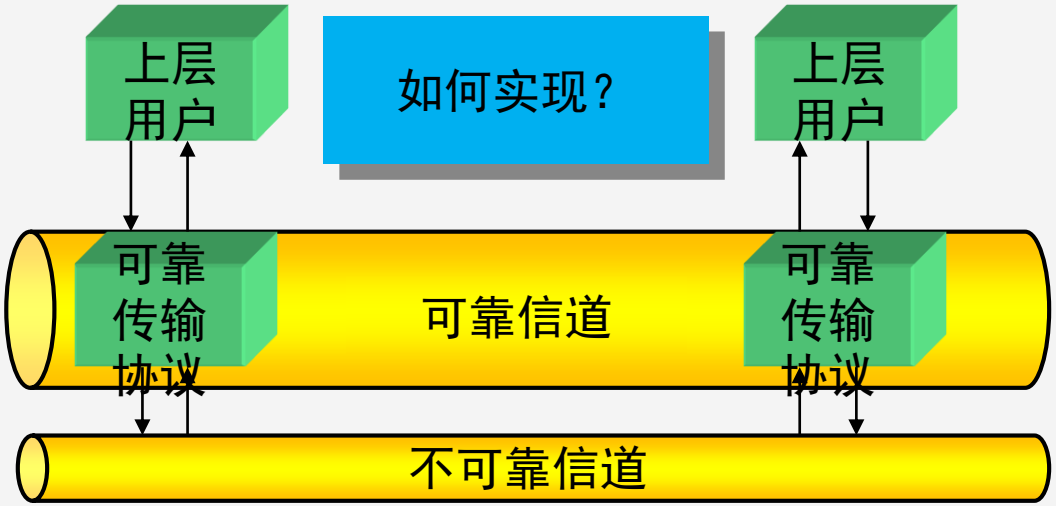
- (1) 若得出的余数 $R = 0$，则判定这个帧没有差错，就接受(accept)。
- (2) 若余数 $R \neq 0$，则判定这个帧有差错，就丢弃。
- 但这种检测方法并不能确定究竟是哪一个或哪几个比特出现了差错。
- 只要经过严格的挑选，并使用位数足够多的除数 P，那么出现检测不到的差错的概率就很小很小。

应当注意

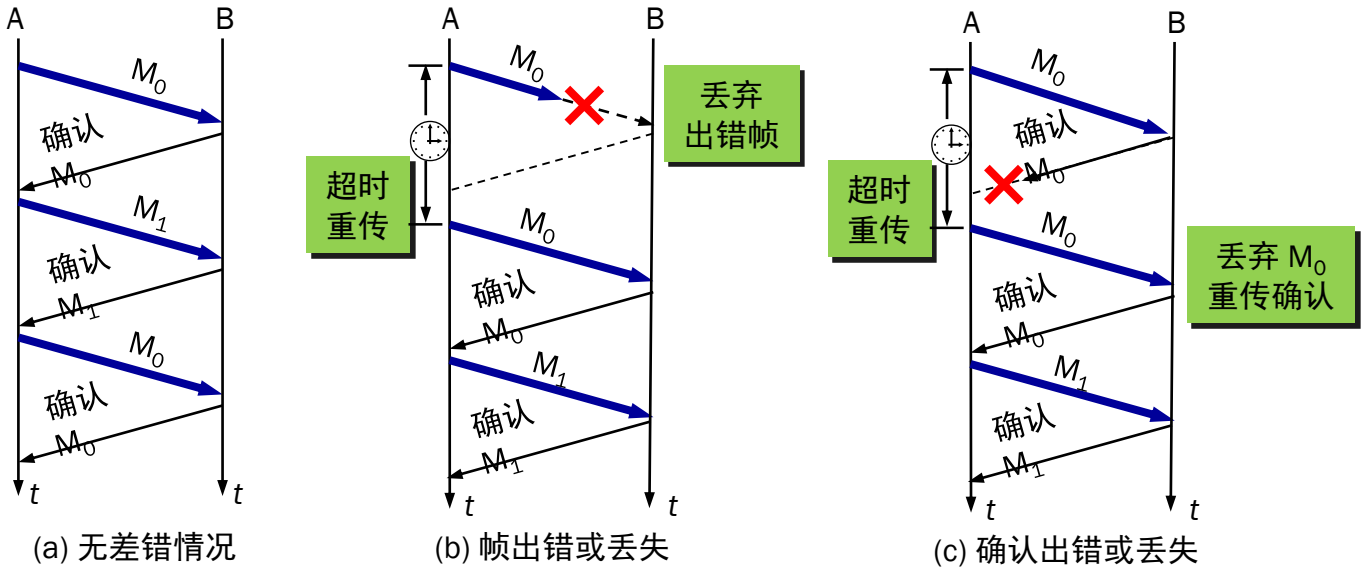
- 仅用循环冗余检验 CRC 差错检测技术只能做到无差错**接受**(accept)。
- “无差错接受”是指：“凡是接受的帧（即**不包括丢弃的帧**），我们都能以非常接近于 1 的概率认为这些帧在传输过程中没有产生差错”。
- 也就是说：“凡是接收端数据链路层接受的帧都没有传输差错”（有差错的帧就丢弃而不接受）。
- 要做到“**可靠传输**”（即发送什么就收到什么）就必须再加上下一节要讲的**确认**和**重传**机制。

3.1.5 可靠传输

- 在不可靠的信道上实现可靠的数据传输为上层提供一条可靠的逻辑通道



1. 停止等待协议



(a) 无差错情况　(b) 帧出错或丢失　(c) 确认出错或丢失

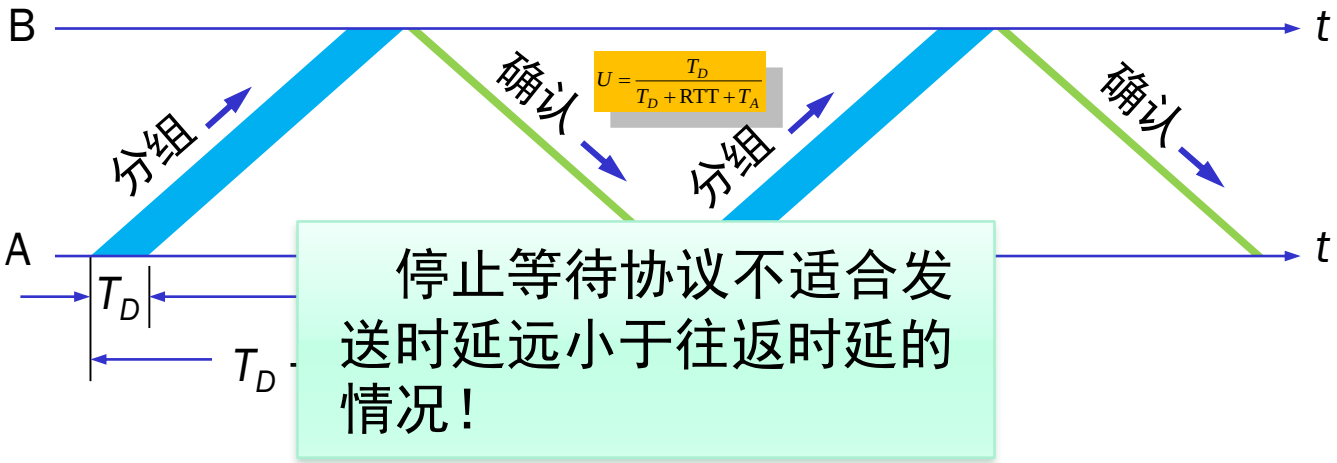
请注意

- 在发送完一个帧后，必须暂时保留已发送的帧的副本。
- 数据帧和确认帧都必须进行编号。
- 只要超过了一段时间还没有收到确认，就认为已发送的帧出错或丢失了，因而重传已发送过的帧。这就叫做**超时重传**。
- 超时计时器的重传时间应当比数据在分组传输的平均往返时间更长一些。

自动重传请求ARQ

- 使用上述的确认和重传机制，我们就可以**在不可靠的传输网络上实现可靠的通信**。
- 这种可靠传输协议常称为**自动重传请求ARQ** (Automatic Repeat reQuest)。
- ARQ 表明重传的请求是**自动**进行的。接收方不需要请求发送方重传某个出错的分组 。

3. 信道利用率

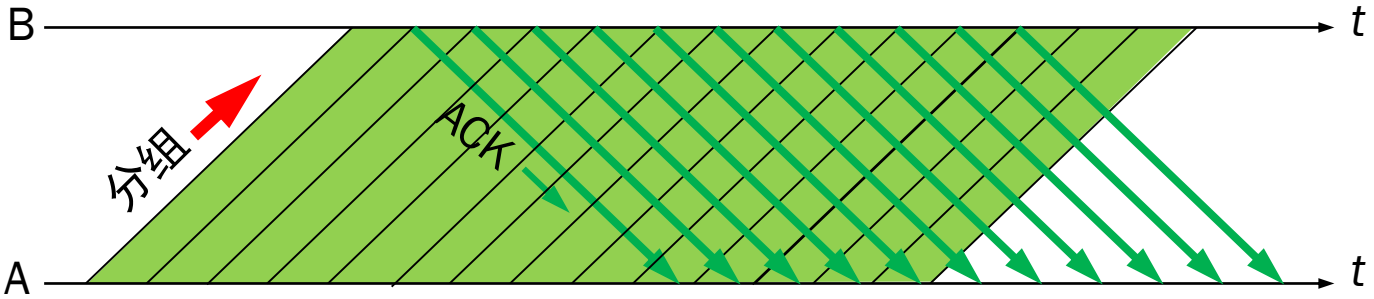


RTT(Round-Trip Time): 往返时延

- **停止等待协议的优点是简单，但缺点是信道利用率低。**

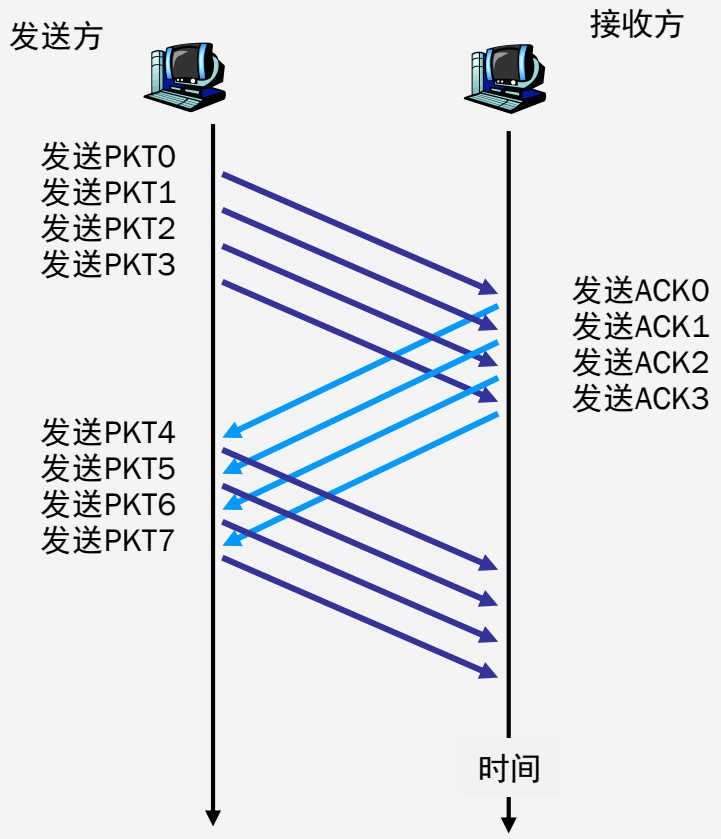
连续ARQ: 流水线传输

- **发送方可连续发送多个分组，不必每发完一个分组就停顿下来等待对方的确认。**
- **由于信道上一直有数据不间断地传送，这种传输方式可获得很高的信道利用率。**



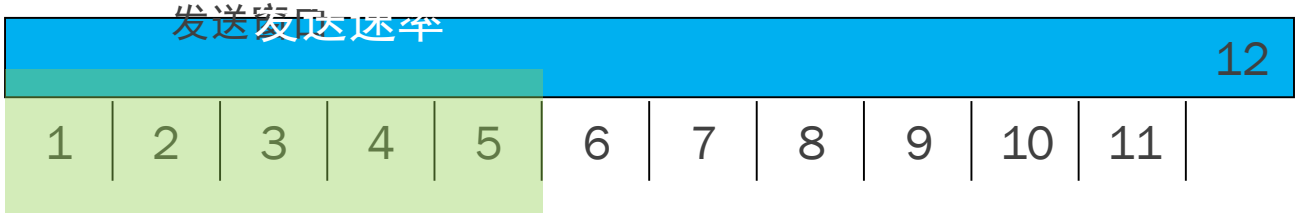
连续不间断发送数据可能导致接收方或网络来不及处理

限制连续发送分组的数目

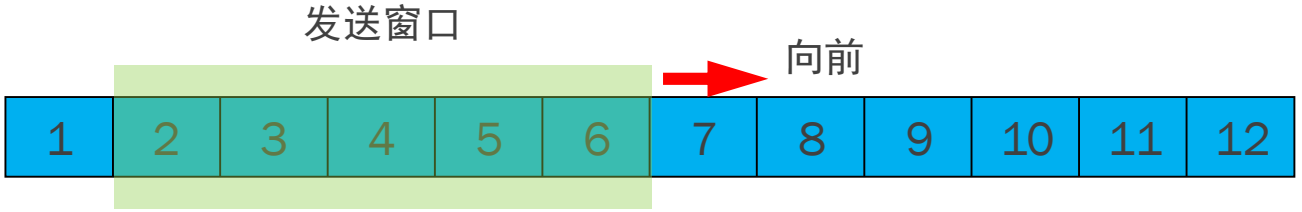


滑动窗口

通过设置发送窗口来限制发送方的



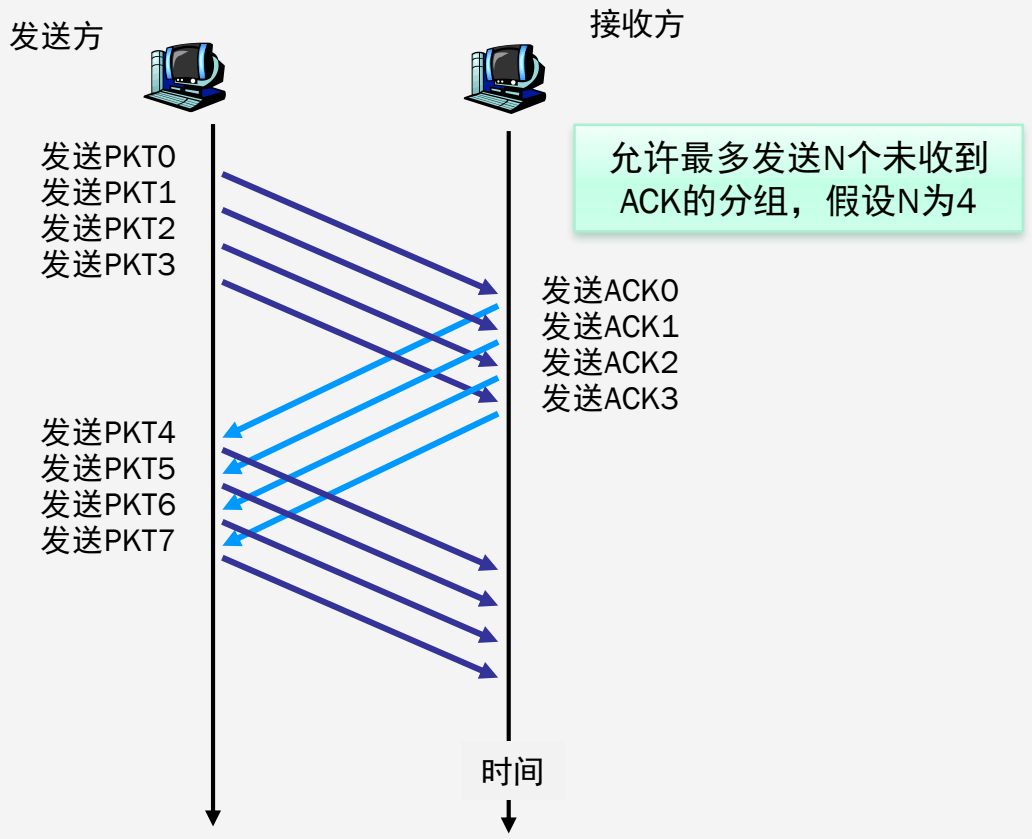
(a) 发送方维持发送窗口（发送窗口是 5）



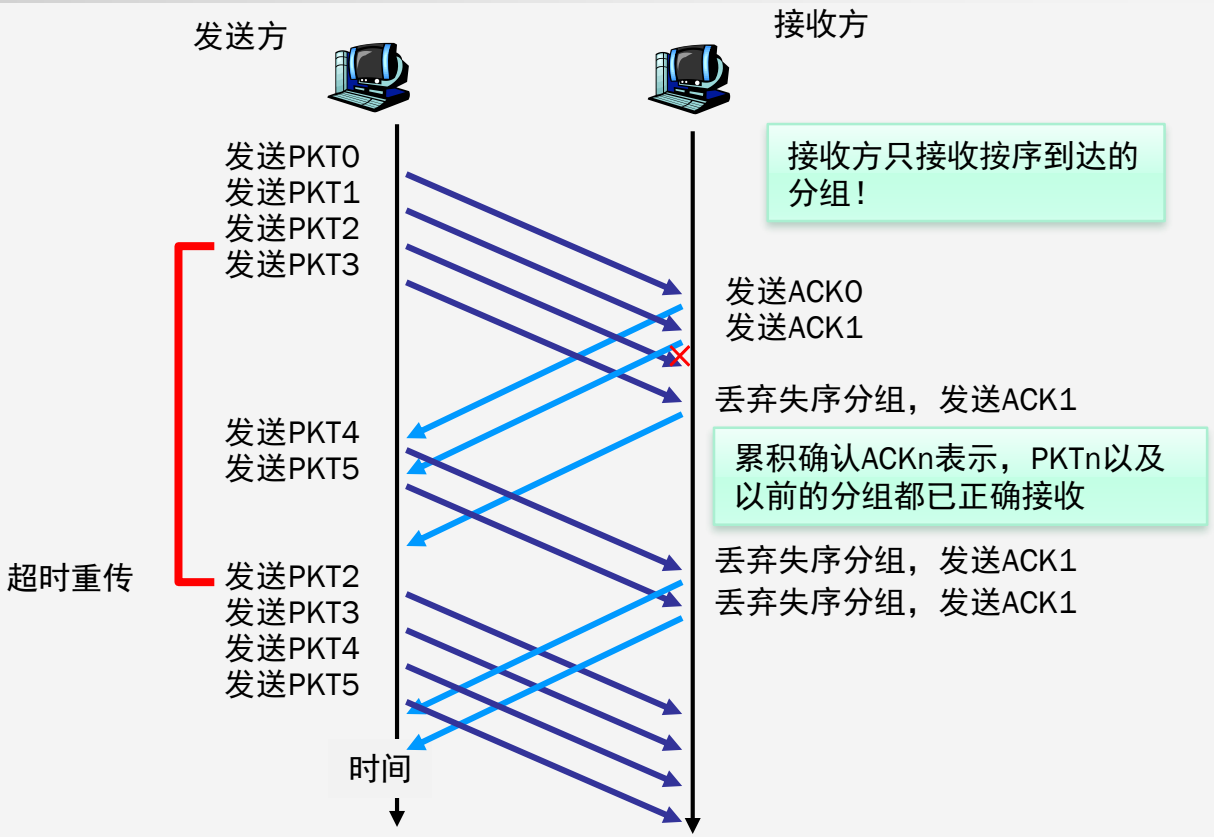
(b) 收到一个确认后发送窗口向前滑动

发送窗口大小是已发送但还没有收到确认的最大分组数

滑动窗口的作用


发送方
接收方
发送PKT0
发送PKT1
发送PKT2
发送PKT3
允许最多发送N个未收到ACK的分组，假设N为4
发送ACK0
发送ACK1
发送ACK2
发送ACK3
发送PKT4
发送PKT5
发送PKT6
发送PKT7
时间

滑动窗口的作用


发送方
接收方
发送PKT0
发送PKT1
发送PKT2
发送PKT3
接收方只接收按序到达的分组！
发送ACK0
发送ACK1
丢弃失序分组，发送ACK1
发送PKT4
发送PKT5
累积确认ACKn表示，PKTn以及以前的分组都已正确接收
丢弃失序分组，发送ACK1
超时重传
发送PKT2
发送PKT3
发送PKT4
发送PKT5
丢弃失序分组，发送ACK1
时间

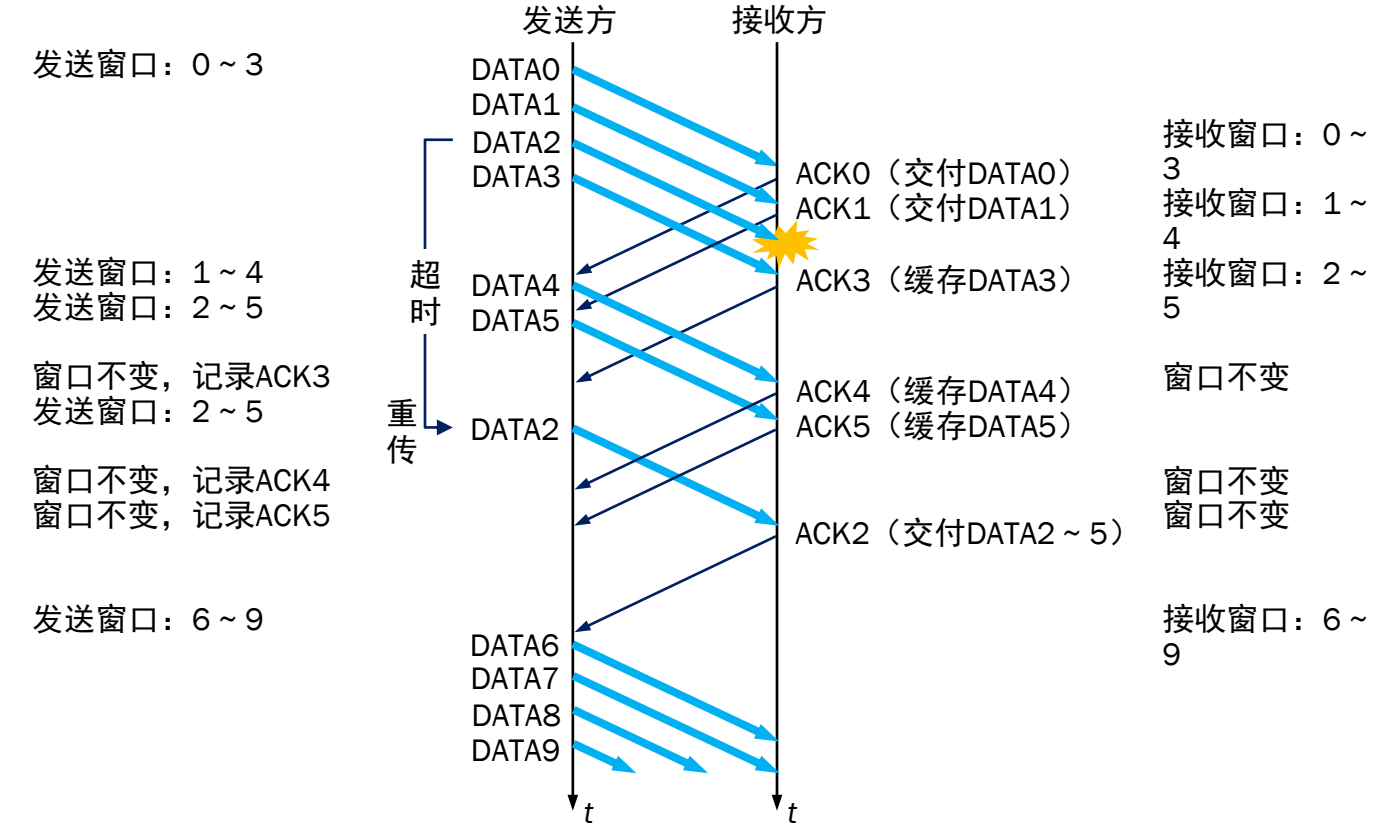
4. Go-back-N（回退 N）协议

- 如果发送方发送了前 5 个分组，而中间的第 3 个分组丢失了。这时接收方只能对前两个分组发出确认。发送方无法知道后面三个分组的下落，而只好把后面的三个分组都再重传一次。
- 这就叫做 Go-back-N（回退 N），表示需要再退回来重传已发送过的 *N* 个分组。

5. 选择重传

- GBN协议存在一个缺点：一个分组的差错可能引起大量分组的重传，这些分组可能已经被接收方正确接收了，但由于未按序到达而被丢弃。
- 可设法只重传出现差错的分组。但必须加大接收窗口，以便先收下失序到达但仍然处在接收窗口中的哪些分组，等到所缺分组收齐后再一并送交上层。这就是**选择重传**SR(Selective Repeat)协议。

5. 选择重传


发送方
接收方
发送窗口：0 ~ 3
DATA0
DATA1
DATA2
DATA3
ACK0（交付DATA0）
ACK1（交付DATA1）
接收窗口：0 ~ 3
接收窗口：1 ~ 4
发送窗口：1 ~ 4
发送窗口：2 ~ 5
超时
DATA4
DATA5
ACK3（缓存DATA3）
接收窗口：2 ~ 5
窗口不变，记录ACK3
发送窗口：2 ~ 5
ACK4（缓存DATA4）
ACK5（缓存DATA5）
窗口不变
窗口不变，记录ACK4
窗口不变，记录ACK5
重传
DATA2
ACK2（交付DATA2 ~ 5）
窗口不变
窗口不变
发送窗口：6 ~ 9
DATA6
DATA7
DATA8
DATA9
接收窗口：6 ~ 9
t
t

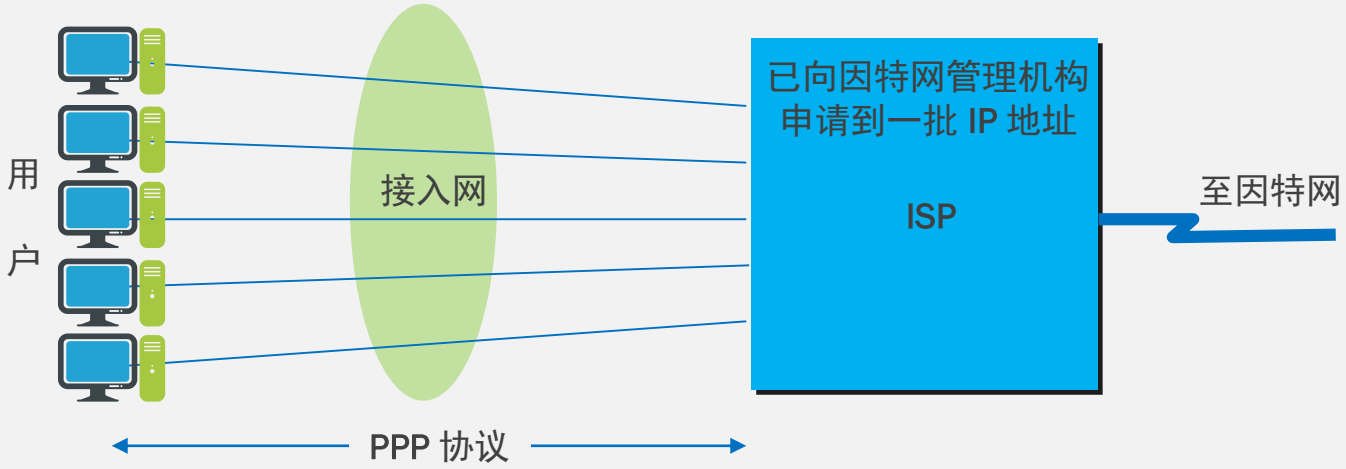
6. 数据链路层的可靠传输

- 实现可靠传输需要付出代价（例如会降低传输效率）。
- 因此，应当根据链路的具体情况来决定是否需要让链路层向上提供可靠传输服务。
- 当链路误码率非常低时，在数据链路层可不实现可靠传输，而是由上层协议（例如，运输层的TCP协议）来完成。
- 但是在使用无线信道传输数据时，由于信道质量较差，在数据链路层仍需要实现可靠传输（例如使用停止等待协议）。

3.2.1 PPP 协议的特点

- 现在全世界使用得最多的点对点数据链路层协议是**点对点协议** PPP (Point-to-Point Protocol)。
- 用户使用拨号电话线接入因特网时，一般都是使用 PPP 协议。

用户到 ISP 的链路使用 PPP 协议



3.2.1 PPP 协议的特点

- 简单——这是首要的要求
- 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

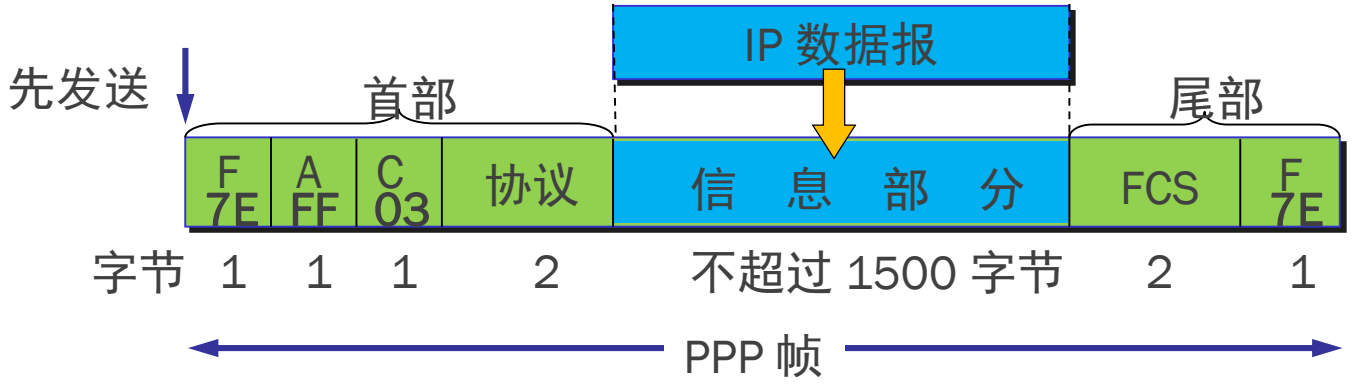
3.2.2 PPP 协议的组成

- **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)。**

3.2.3 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。**
  - **当协议字段为 0x0021 时，PPP 帧的信息字段就是 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，就使用一种特殊的字符填充法。

字符填充

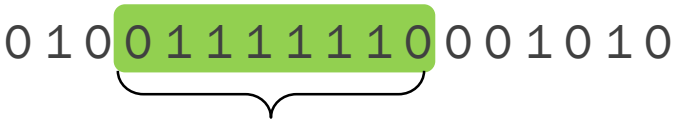
- 将信息字段中出现的每一个 0x7E 字节转变成为 2 字节序列(0x7D, 0x5E)。
- 若信息字段中出现一个 0x7D 的字节, 则将其转变成为 2 字节序列(0x7D, 0x5D)。
- 若信息字段中出现 ASCII 码的控制字符（即数值小于 0x20 的字符），则在该字符前面要加入一个 0x7D 字节，同时将该字符的编码加以改变。

零比特填充

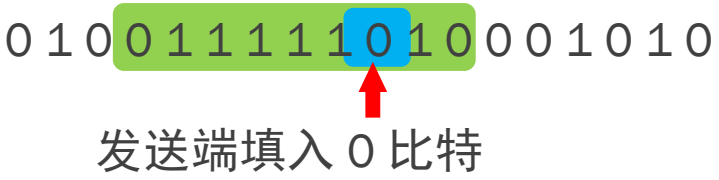
- PPP 协议用在 SONET/SDH 链路时，是使用同步传输（一连串的比特连续传送）。这时 PPP 协议采用零比特填充方法来实现透明传输。
- 在发送端，只要发现有 5 个连续 1，则立即填入一个 0。接收端对帧中的比特流进行扫描。每当发现 5 个连续1时，就把这 5 个连续 1 后的一个 0 删除。

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



发送端在 5 个连 1 之后填入 0 比特再发送出去

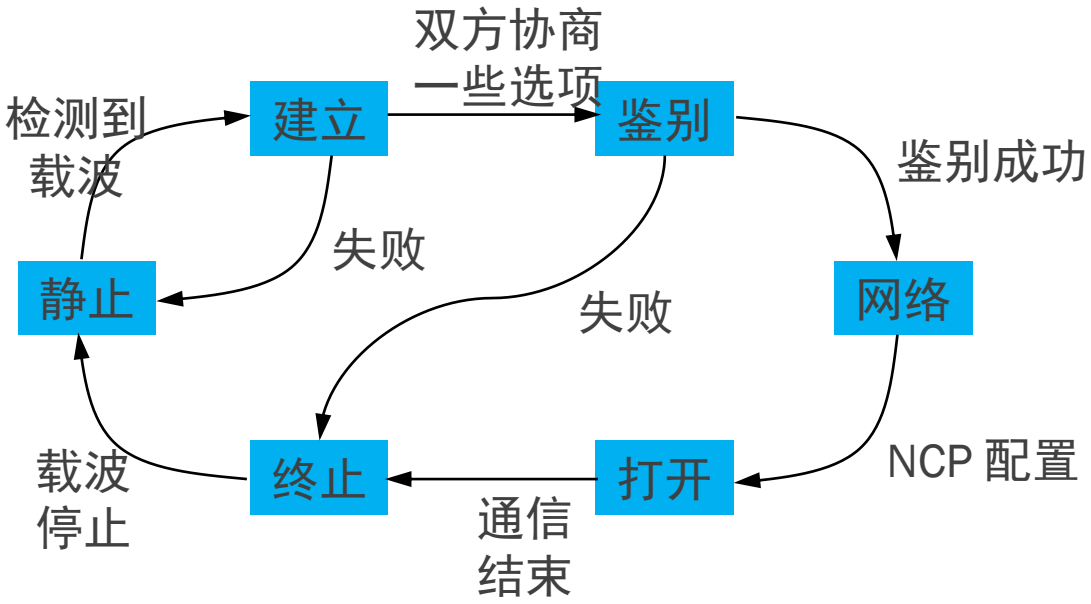


在接收端把 5 个连 1 之后的 0 比特删除

3.2.4 PPP 的工作状态

- 当用户拨号接入 ISP 时，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）。
- 这些分组及其响应选择一些 PPP 参数，和进行网络层配置，NCP 给新接入的 PC机分配一个临时的 IP 地址，使 PC 机成为因特网上的一个主机。
- 通信完毕时，NCP 释放网络层连接，收回原来分配出去的 IP 地址。接着，LCP 释放数据链路层连接。最后释放的是物理层的连接。

3.2.4 PPP 的工作状态



3.3 使用广播信道的数据链路层

- 广播信道可以进行一对多的通信，能很方便且廉价地连接多个邻近的计算机，因此曾经被广泛应用于局域网之中。
- 由于用广播信道连接的计算机共享同一传输媒体，因此使用广播信道的局域网被称为共享式局域网。
- 虽然交换式局域网在有线领域已完全取代了共享式局域网，但无线局域网仍然使用的是共享媒体技术。

3.3.1 媒体接入控制

- 静态划分信道
  - 频分多址、时分多址、码分多址 …
- 动态媒体接入控制（多点接入）
  - 随机接入，如以太网
    - 如何减少冲突，冲突后如何办
  - 受控接入，如令牌环或轮询
    - 在集中或分布式控制下轮流接入

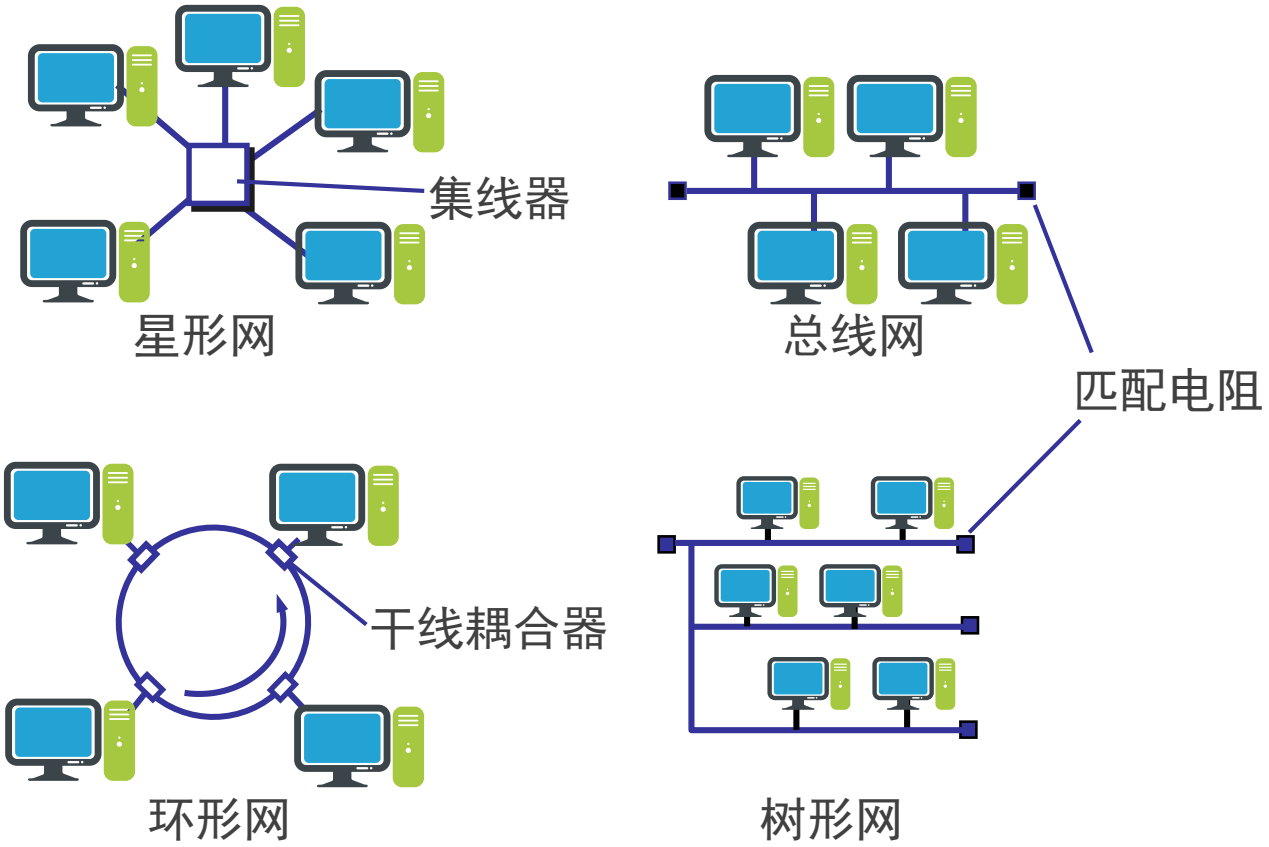
Multiple Access：
多点接入、多址访问

媒体访问/接入控制(MAC)
Medium Access Control

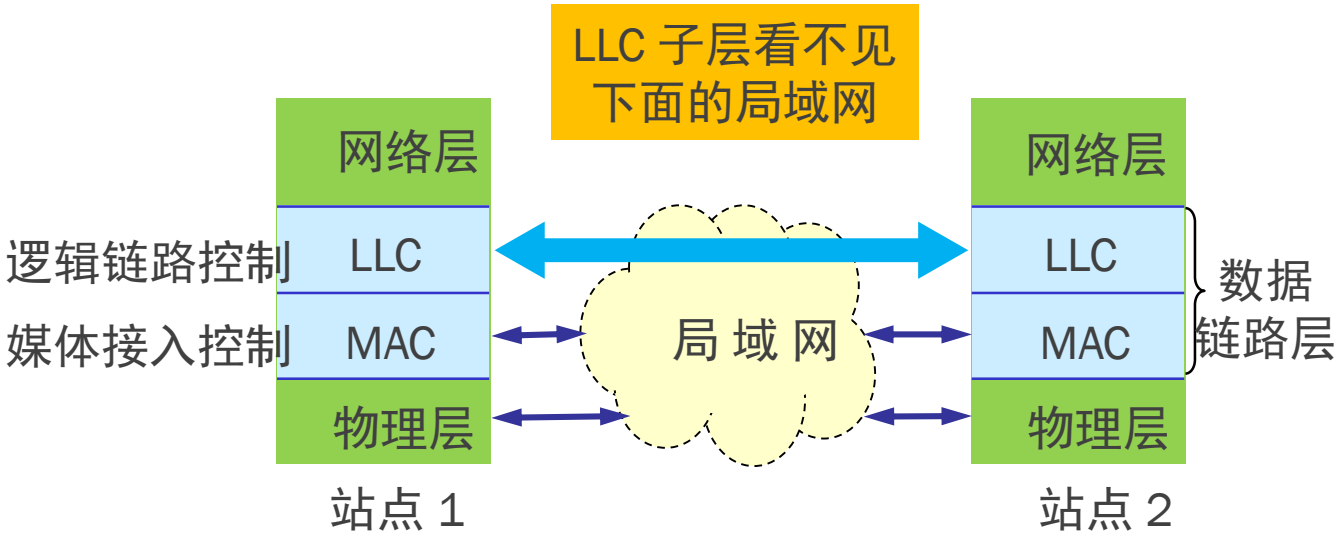
3.3.2 局域网

- 网络为一个单位所拥有，且地理范围和站点数目均有限。
- 最初，主要用来连接一个单位内部的计算机，方便地共享所有连接在局域网上的各种硬件、软件和数据资源。
- 现在，局域网将各种企业、机构、校园中的大量用户接入到互联网中，网络中大部分的信息资源都集中在这些局域网中。

1. 局域网的拓扑



2. 局域网体系结构



由于以太网已经“一统江湖”，LLC已不再重要

数据链路层的两个子层

- 为了使数据链路层能更好地适应多种局域网标准，802 委员会就将局域网的数据链路层拆成两个子层：
  - 逻辑链路控制 LLC (Logical Link Control)子层
  - 媒体接入控制 MAC (Medium Access Control)子层。
- 与接入到传输媒体有关的内容都放在 MAC子层，而 LLC 子层则与传输媒体无关，不管采用何种协议的局域网对 LLC 子层来说都是透明的

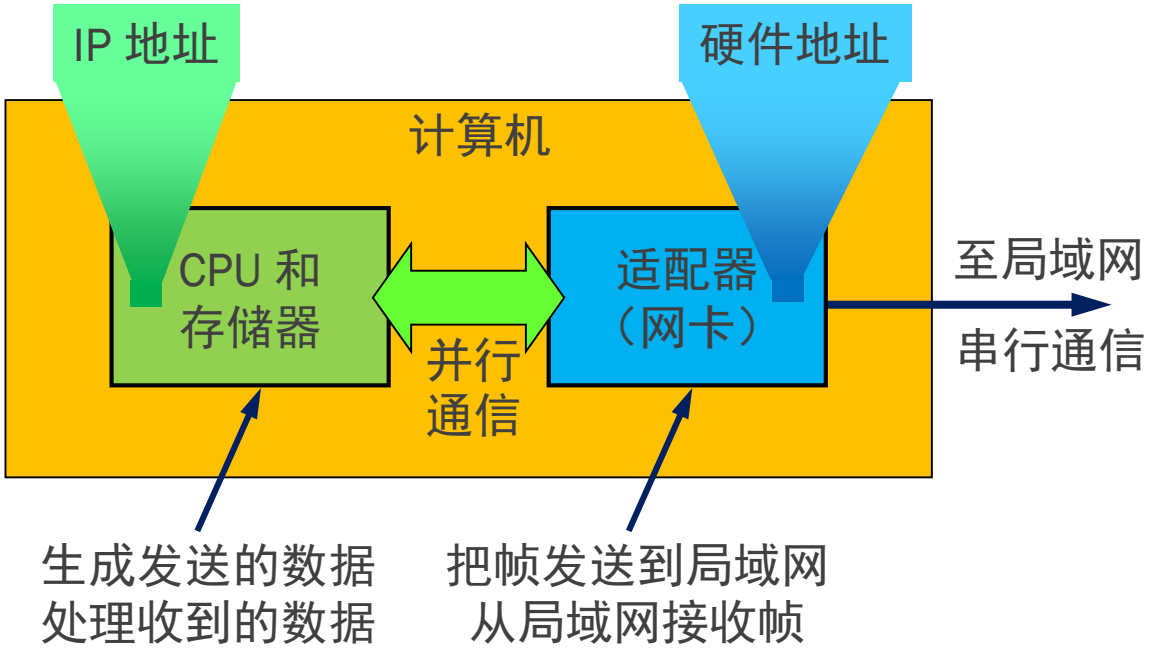
以后一般不考虑 LLC 子层

- 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。

3. 网络适配器

- 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”。
- 适配器的重要功能：
  - 进行串行/并行转换。
  - 对数据进行缓存。
  - 在计算机的操作系统安装设备驱动程序。
  - 实现以太网协议。

计算机通过适配器和局域网进行通信



4. MAC地址

- 在局域网中，硬件地址又称为物理地址，或 MAC 地址。
- 802 标准所说的“地址”严格地讲应当是每一个站的“名字”或标识符。
- 但鉴于大家都早已习惯了将这种 48 位的“名字”称为“地址”，所以本书也采用这种习惯用法，尽管这种说法并不太严格。

48 位的 MAC 地址

- IEEE 的**注册管理机构** RA 负责向厂家分配地址字段的前三个字节(即高位 24 位)。
- 地址字段中的后三个字节(即低位 24 位)由厂家自行指派，称为**扩展标识符**，必须保证生产出的适配器没有重复地址。
- 一个地址块可以生成2^{24}个不同的地址。这种 48 位地址称为 MAC-48，它的通用名称是EUI-48。
- “MAC地址”实际上就是适配器地址或适配器标识符EUI-48。

适配器检查 MAC 地址

- 适配器从网络上每收到一个 MAC 帧就首先用硬件检查 MAC 帧中的 MAC 地址.
  - 如果是发往本站的帧则收下，然后再进行其他的处理。
  - 否则就将此帧丢弃，不再进行其他的处理。
- “发往本站的帧”包括以下三种帧：
  - 单播(unicast)帧（一对一）
  - 广播(broadcast)帧（一对全体）
  - 多播(multicast)帧（一对多）

3.4 共享式以太网

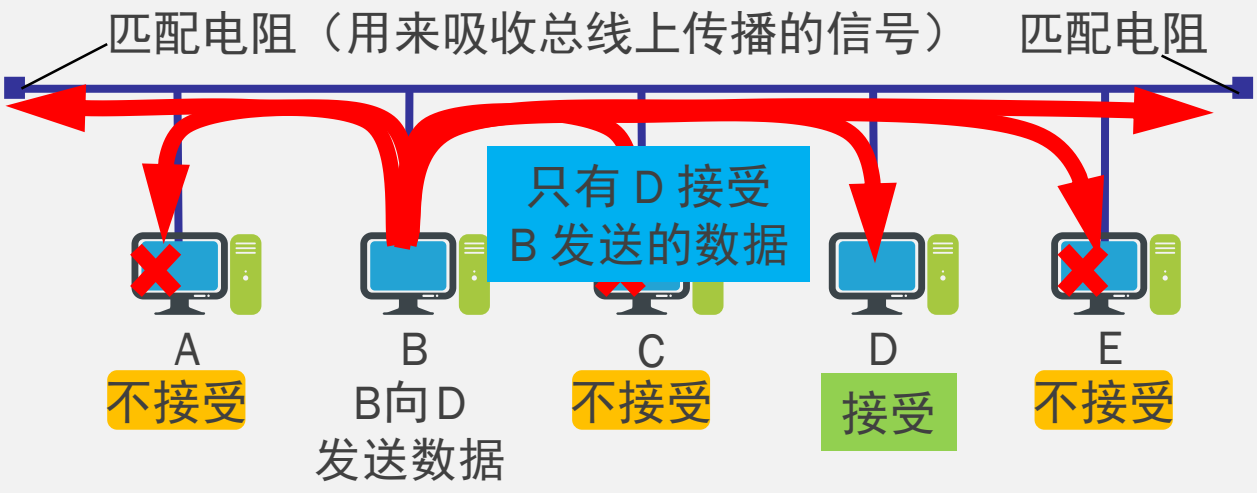
以太网的两个标准

- DIX Ethernet V2。
- 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

3.4.1 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。

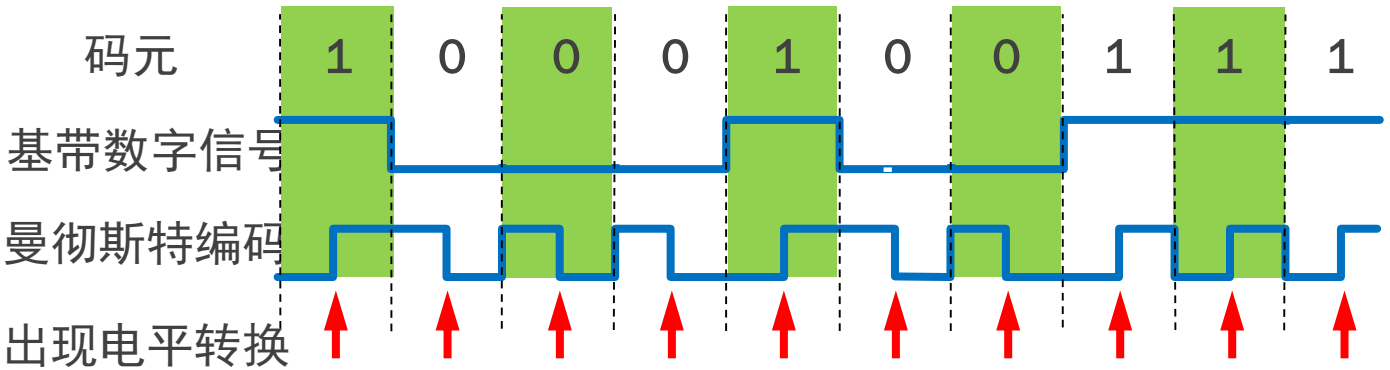
为了通信的简便以太网采取了两种重要的措施

- 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。
  - 这样做的理由是局域网信道的质量很好，因信道质量产生差错的概率是很小的。

以太网提供的服务

- 以太网提供的服务是不可靠的交付，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，其他什么也不做。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，而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



载波监听多点接入/碰撞检测 CSMA/CD

- CSMA/CD 表示 Carrier Sense Multiple Access with Collision Detection。
- “多点接入”表示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”是指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，以免发生碰撞。
- 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计算机发送的数据信号。

碰撞检测

- “**碰撞检测**”就是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”。

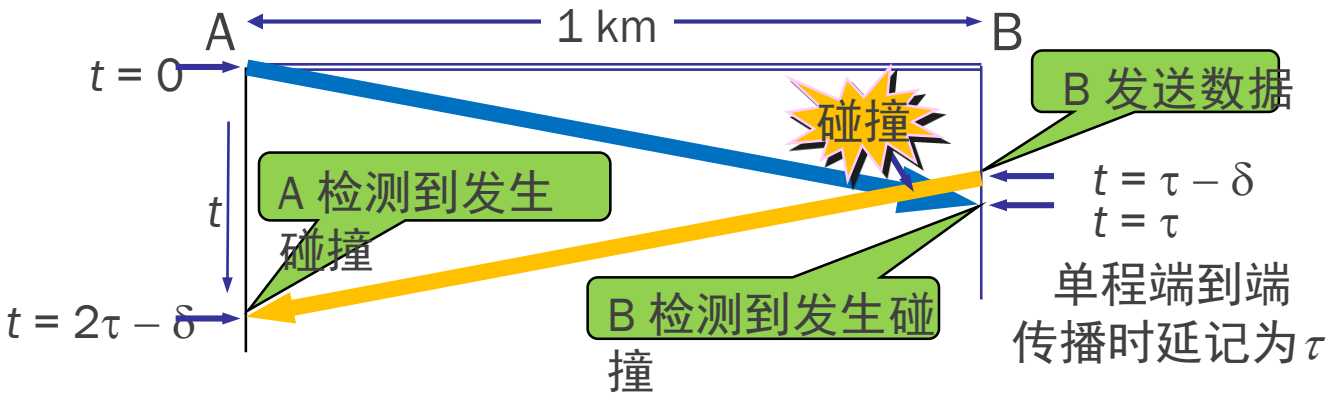
检测到碰撞后

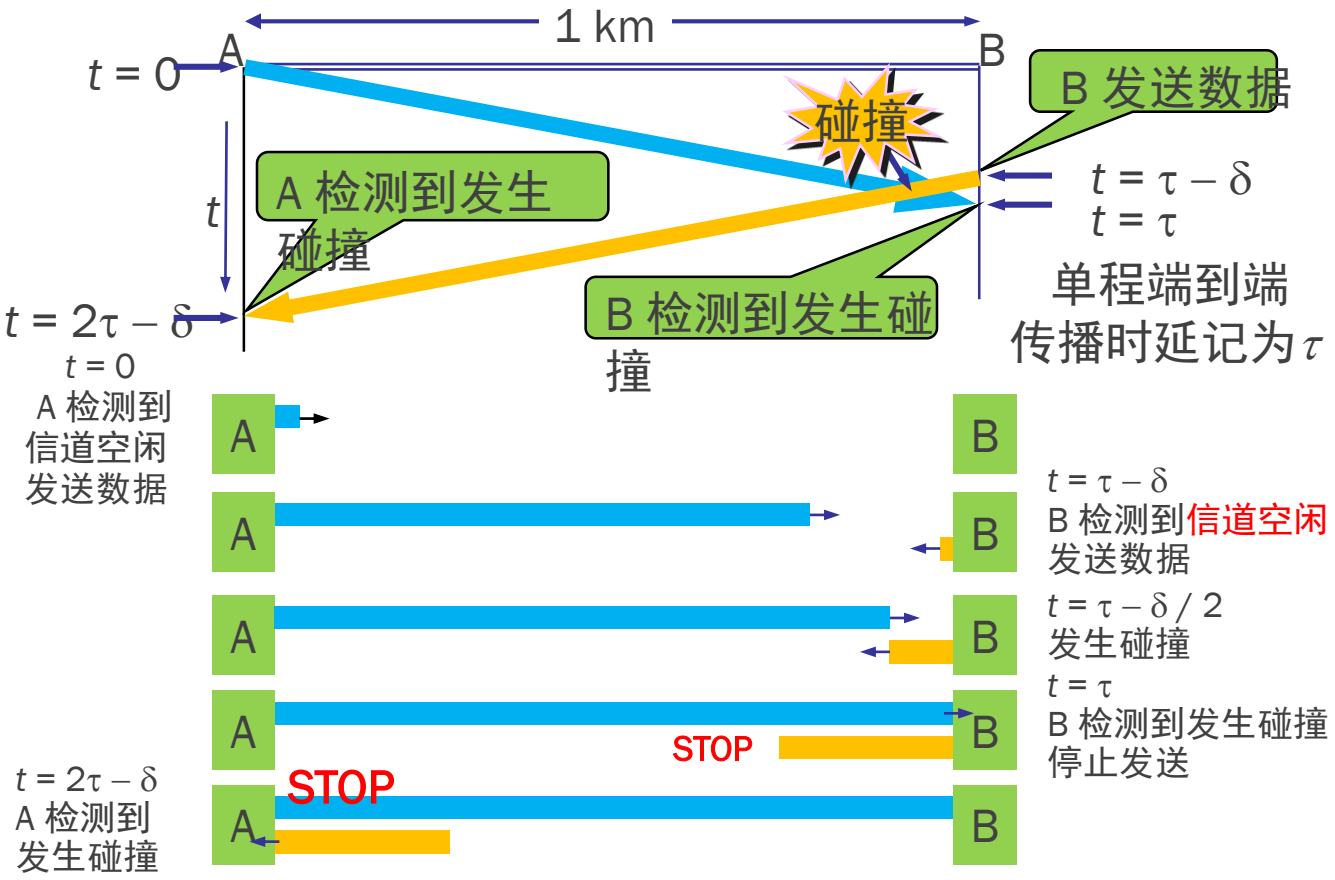
- 在发生碰撞时，总线上传输的信号产生了严重的失真，无法从中恢复出有用的信息来。
- 每一个正在发送数据的站，一旦发现总线上出现了碰撞，就要立即停止发送，免得继续浪费网络资源，然后等待一段随机时间后再次发送。

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响




1 km
A
B
t = 0
碰撞
B 发送数据
A 检测到发生碰撞
t
t = τ − δ
t = τ
单程端到端传播时延记为 τ
t = 2τ − δ
B 检测到发生碰撞
t = 0
A 检测到信道空闲发送数据
t = τ − δ
B 检测到信道空闲发送数据
t = τ − δ / 2
发生碰撞
t = τ
B 检测到发生碰撞停止发送
STOP
STOP
t = 2τ − δ
A 检测到发生碰撞

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，$k \le 10$，即

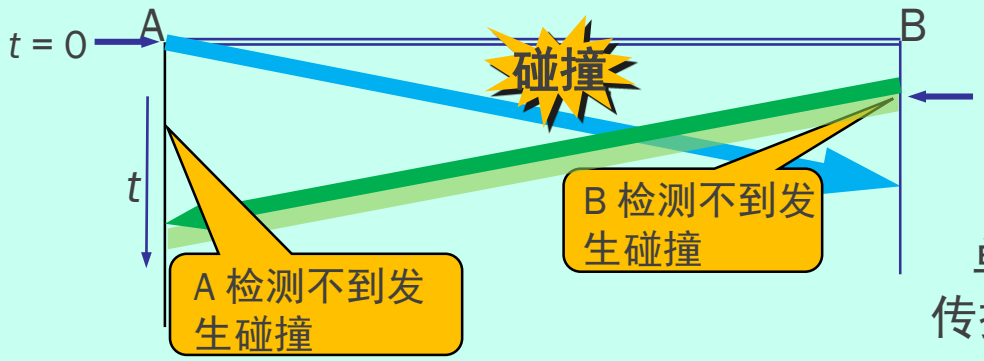
    k = Min[重传次数, 10]
  - 从整数集合[0,1,…, $(2^k - 1)$]中随机地取出一个数，记为 r。重传所需的时延就是 r 倍的基本退避时间。
  - 当重传达 16 次仍不能成功时即丢弃该帧，并向高层报告。

争用期的长度

- 以太网取 51.2 μs 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

- 如果发送的帧太短，有可能检测不到发生的碰撞



单程端到端传播时延记为τ

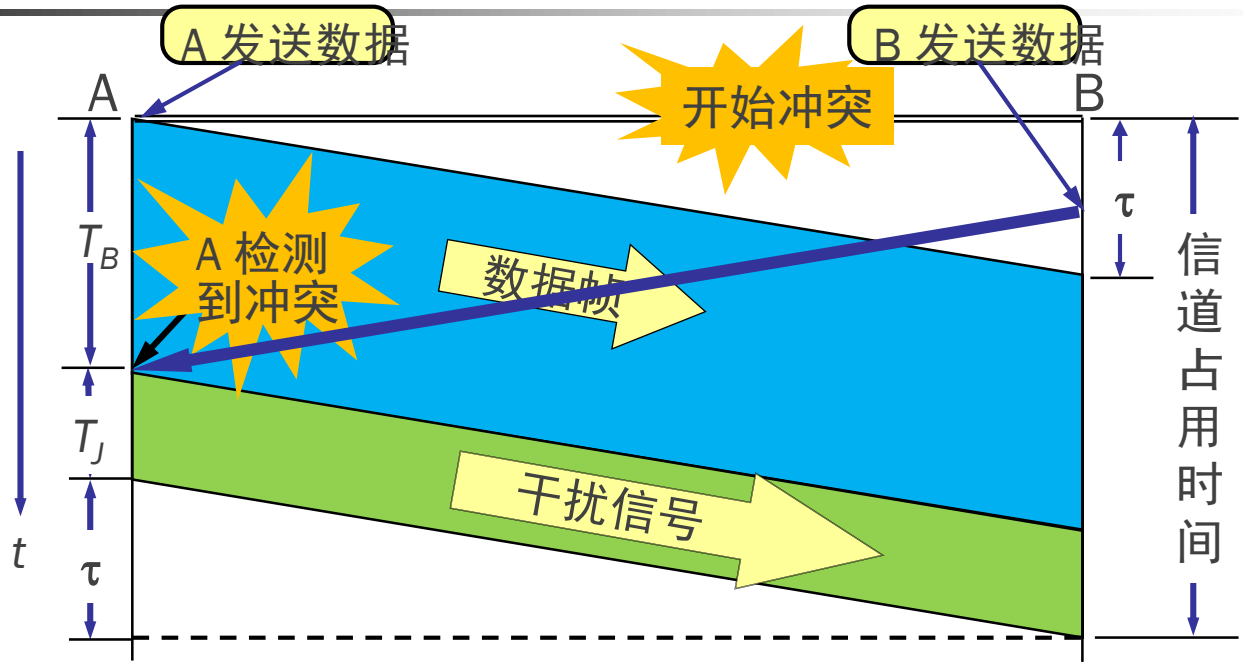
最短有效帧长

- 为保证发送方能检测到所有碰撞，以太网规定了**最短有效帧长**为 64 字节
- 如果发生冲突，就一定是在发送的前 64 字节之内，立即中止发送，这时已经发送出去的数据一定小于 64 字节。
- 因此将长度小于 64 字节的帧都视为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)，以便让所有站点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。

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[illegible]遭遇碰撞的可能性。
- 当连接很多站点时，[illegible]太网的最高数据率小很多。

CSMA/CD协议能否用于广域网？

重要特性

- 网络覆盖范围越大，端到端时延越大，争用期越大，发生碰撞的概率越大，性能越差。
- 10M以太网最大网络长度：
  - $(2\times10^8)\times(51.2/2)=5120m$
  - 但考虑到其它因素，
- 网络中主机越多，发送数 的概率越大，性能越差。

CSMA/CD协议不适合广域网！

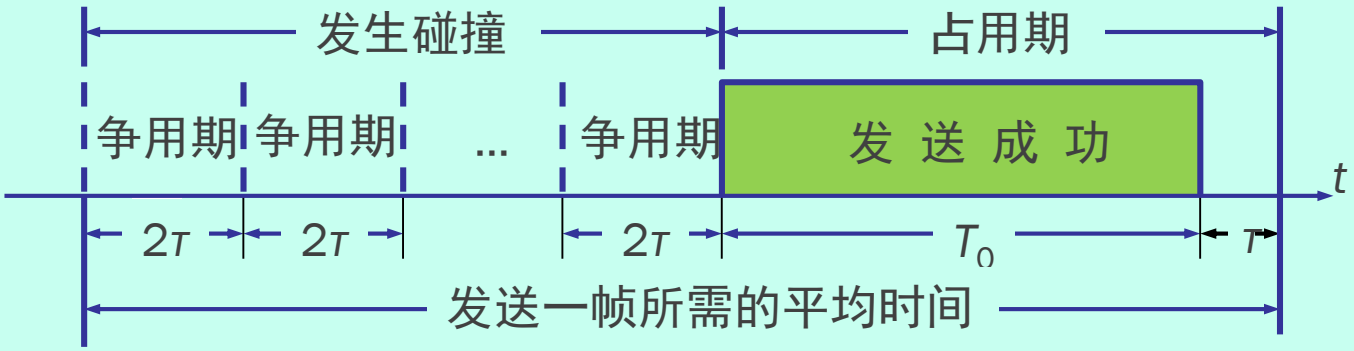
3.4.2 共享式以太网的信道利用率

- 以太网的信道被占用的情况：

  - 争用期长度为 2τ，即端到端传播时延的两倍。检测到碰撞后不发送干扰信号。
  - 帧长为 L (bit)，数据发送速率为 C (b/s)，因而帧的发送时间为 $L/C = T_0$ (s)。

以太网的信道利用率

- **一个帧从开始发送，经可能发生的碰撞后，将再重传数次，到发送成功且信道转为空闲(即再经过时间 τ 使得信道上无信号在传播)时为止，是发送一帧所需的平均时间。**



参数 a

- **要提高以太网的信道利用率，就必须减小 τ 与 T_0 之比。在以太网中定义了参数 *a*，它是以太网单程端到端时延 τ 与帧的发送时间 T_0 之比：**

$$a = \frac{\tau}{T_0} \qquad (3\text{-}4)$$

- $a \to 0$ 表示一发生碰撞就立即可以检测出来，并立即停止发送，因而信道利用率很高。
- a 越大，表明争用期所占的比例增大，每发生一次碰撞就浪费许多信道资源，使得信道利用率明显降低。

对以太网参数的要求

- 当数据率一定时，以太网的连线的长度受到限制，否则 τ 的数值会太大。
- 以太网的帧长不能太短，否则 T_0 的值会太小，使 a 值太大。

信道利用率的最大值 S_{max}

- 在**理想化**的情况下，以太网上的各站发送数据都不会产生碰撞（这显然已经不是 CSMA/CD，而是需要使用一种特殊的调度方法），即总线一旦空闲就有某一个站立即发送数据。
- 发送一帧占用线路的时间是 $T_0 + \tau$，而帧本身的发送时间是 T_0。于是我们可计算出**理想情况下**的极限信道利用率 S_{max}为：

$$S_{max} = \frac{T_0}{T_0 + \tau} = \frac{1}{1 + a} \qquad (3\text{-}5)$$

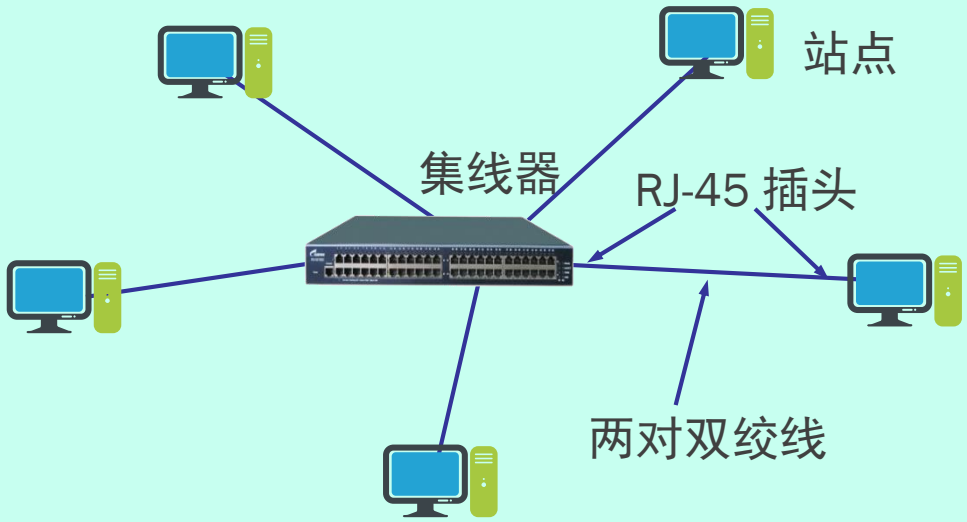
以太网性能分析的结论

- 当网络覆盖范围越大，既端到端时延越大，信道极限利用率越低，即网络性能越差。
- 另外，端到端时延越大或连接的站点越多，都会导致发生冲突的概率变大，网络性能还会进一步降低。
- 可见，共享式以太网只能作为一种局域网技术。

3.4.3 使用集线器的星形拓扑

- 传统以太网最初是使用粗同轴电缆，后来演进到使用比较便宜的细同轴电缆，最后发展为使用更便宜和更灵活的双绞线。
- 这种以太网采用星形拓扑，在星形的中心则增加了一种可靠性非常高的设备，叫做**集线器**(hub)

使用集线器的双绞线以太网



星形网 10BASE-T

- 不用电缆而使用无屏蔽双绞线。每个站需要用两对双绞线，分别用于发送和接收。
- 集线器使用了大规模集成电路芯片，因此这样的硬件设备的可靠性已大大提高了。

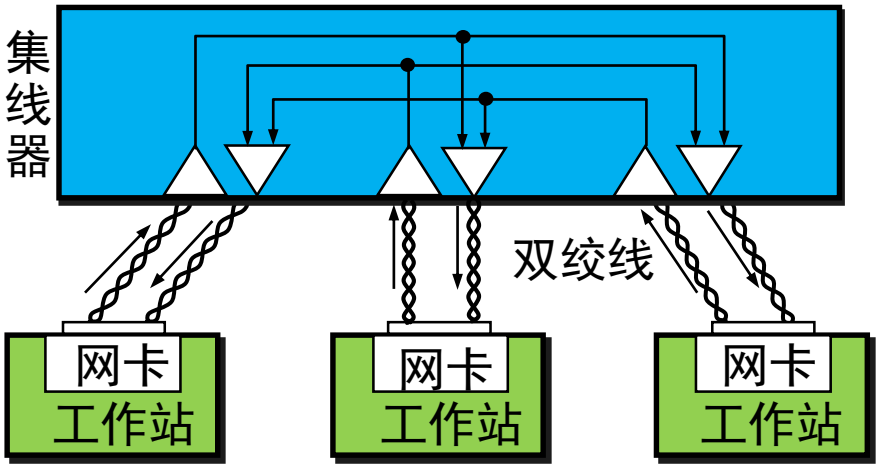
以太网在局域网中的统治地位

- 10BASE-T 的通信距离稍短，每个站到集线器的距离不超过 100 m。
- 这种 10 Mb/s 速率的无屏蔽双绞线星形网的出现，既降低了成本，又提高了可靠性。
- 10BASE-T 双绞线以太网的出现，是局域网发展史上的一个非常重要的里程碑，它为以太网在局域网中的统治地位奠定了牢固的基础。

集线器的一些特点

- 集线器是使用电子器件来模拟实际电缆线的工作，因此整个系统仍然像一个传统的以太网那样运行。
- 使用集线器的以太网在**逻辑上**仍是一个总线网，各工作站使用的还是 CSMA/CD 协议，并共享逻辑上的总线。
- 集线器很像一个多接口的转发器，工作在物理层。

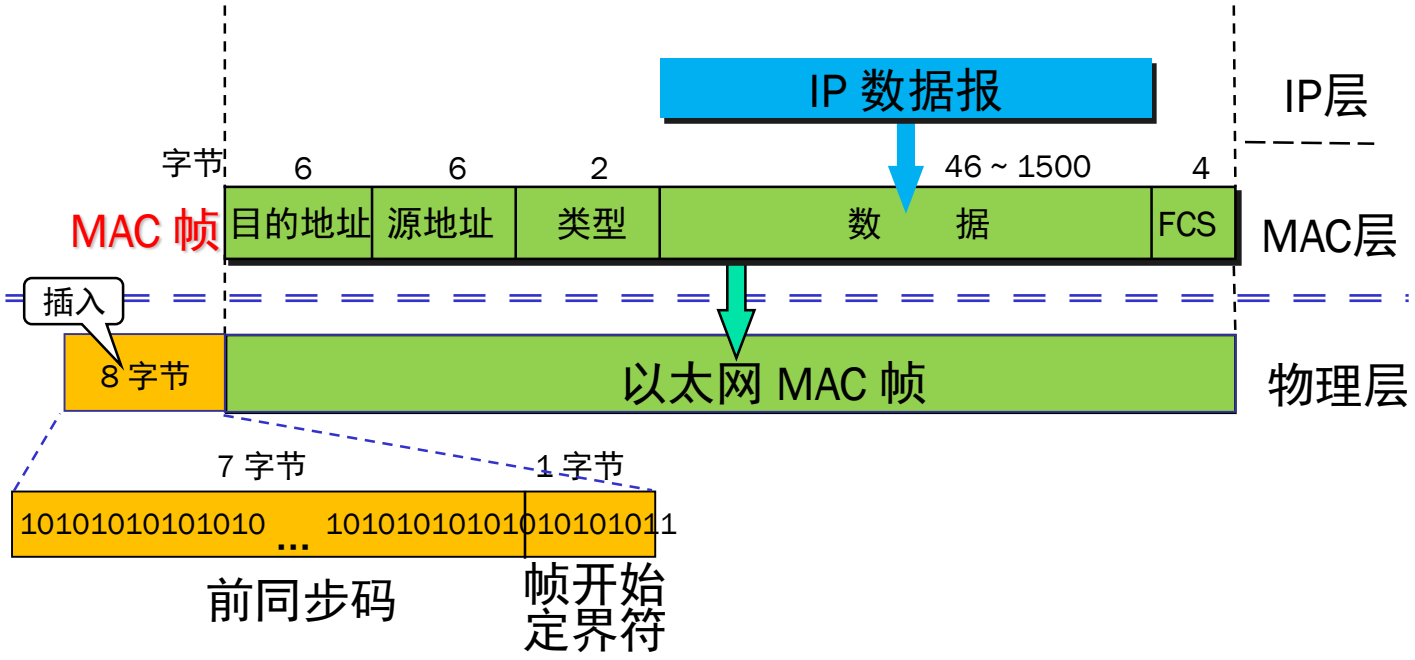
具有三个接口的集线器



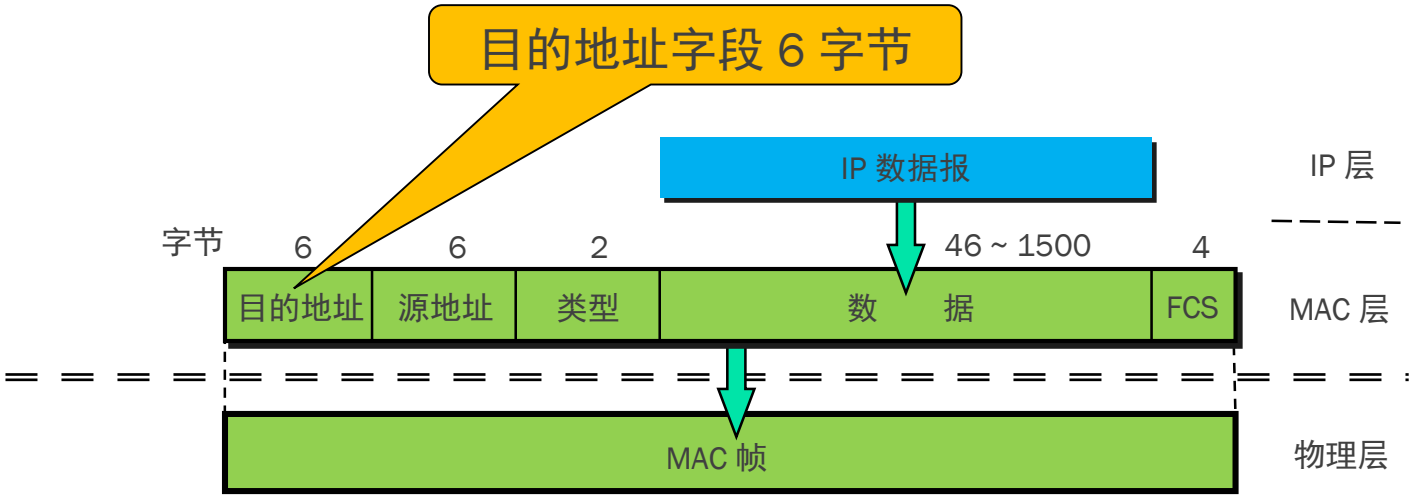
3.4.4 以太网的帧格式

- 常用的以太网MAC帧格式有两种标准：
  - DIX Ethernet V2 标准
  - IEEE 的 802.3 标准
- 最常用的 MAC 帧是以太网 V2 的格式。

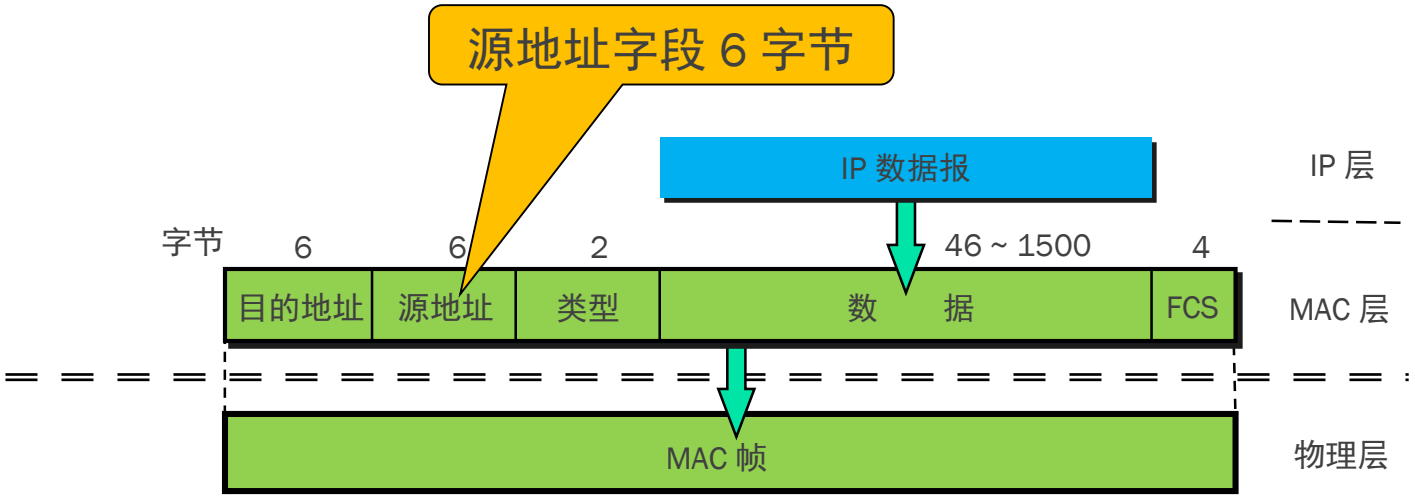
以太网的 MAC 帧格式


IP 数据报
IP层
字节
6
6
2
46 ~ 1500
4
MAC 帧
目的地址
源地址
类型
数
据
FCS
MAC层
插入
8 字节
以太网 MAC 帧
物理层
7 字节
1 字节
10101010101010 ... 10101010101010101011
前同步码
帧开始
定界符

以太网 V2 的 MAC 帧格式

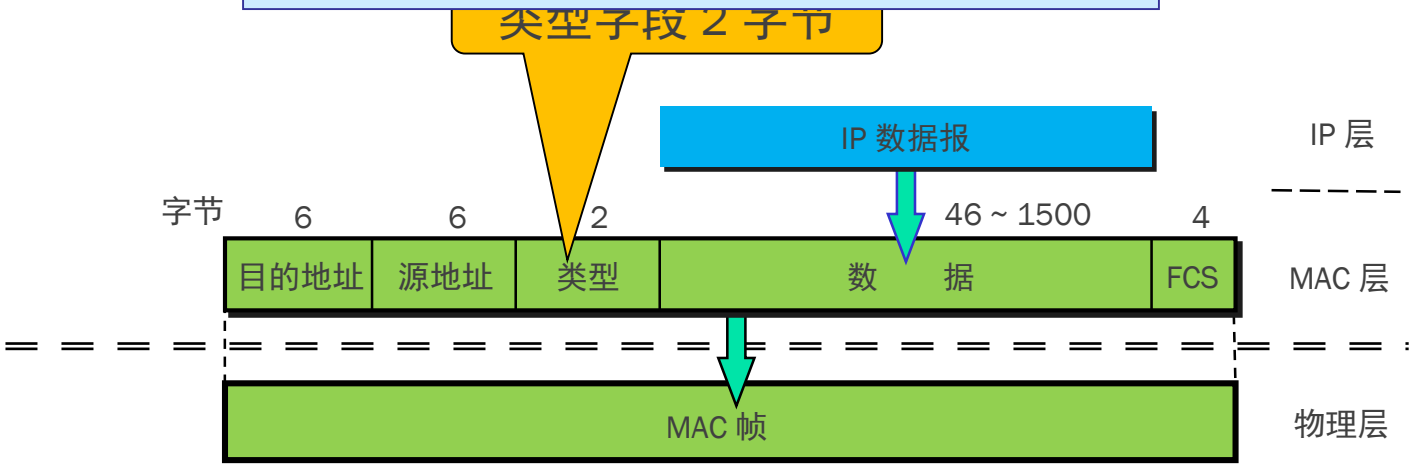


以太网 V2 的 MAC 帧格式



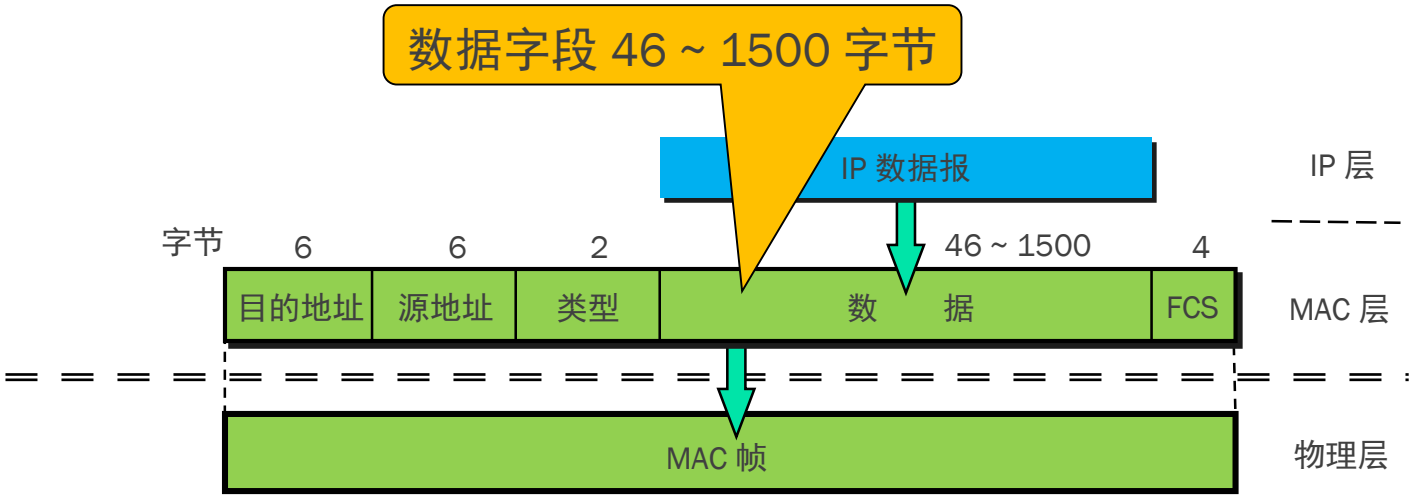
以太网 V2 的 MAC 帧格式

类型字段用来标志上一层使用的是什么协议，以便把收到的 MAC 帧的数据上交给上一层的这个协议。



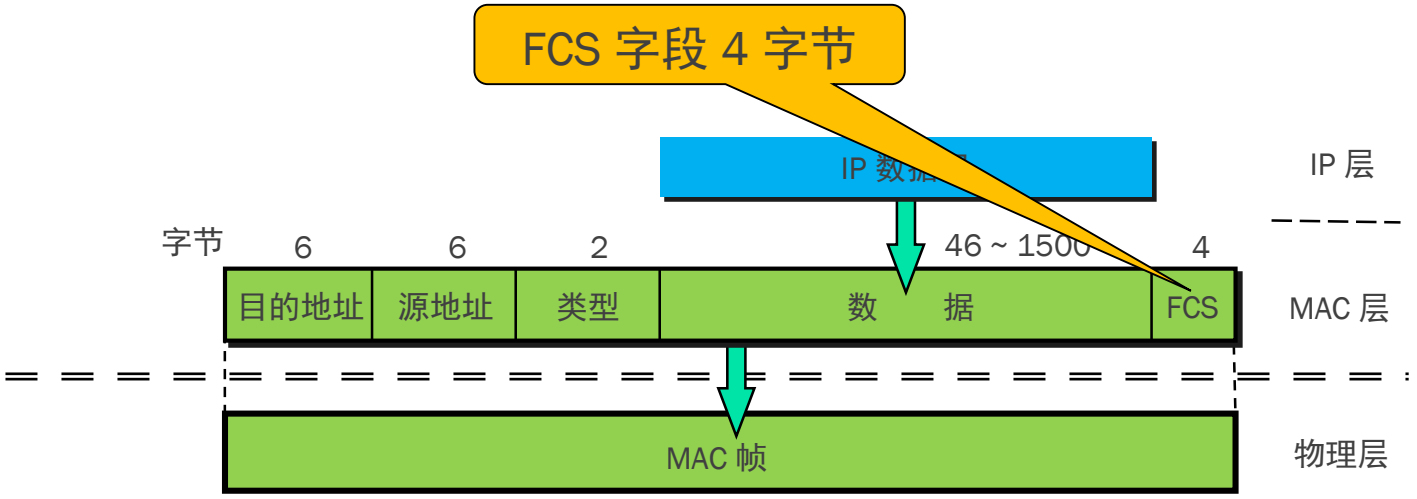
以太网 V2 的 MAC 帧格式

数据字段的正式名称是 MAC 客户数据字段
最小长度 64 字节 – 18 字节的首部和尾部 = 数据字段的最小长度



以太网 V2 的 MAC 帧格式

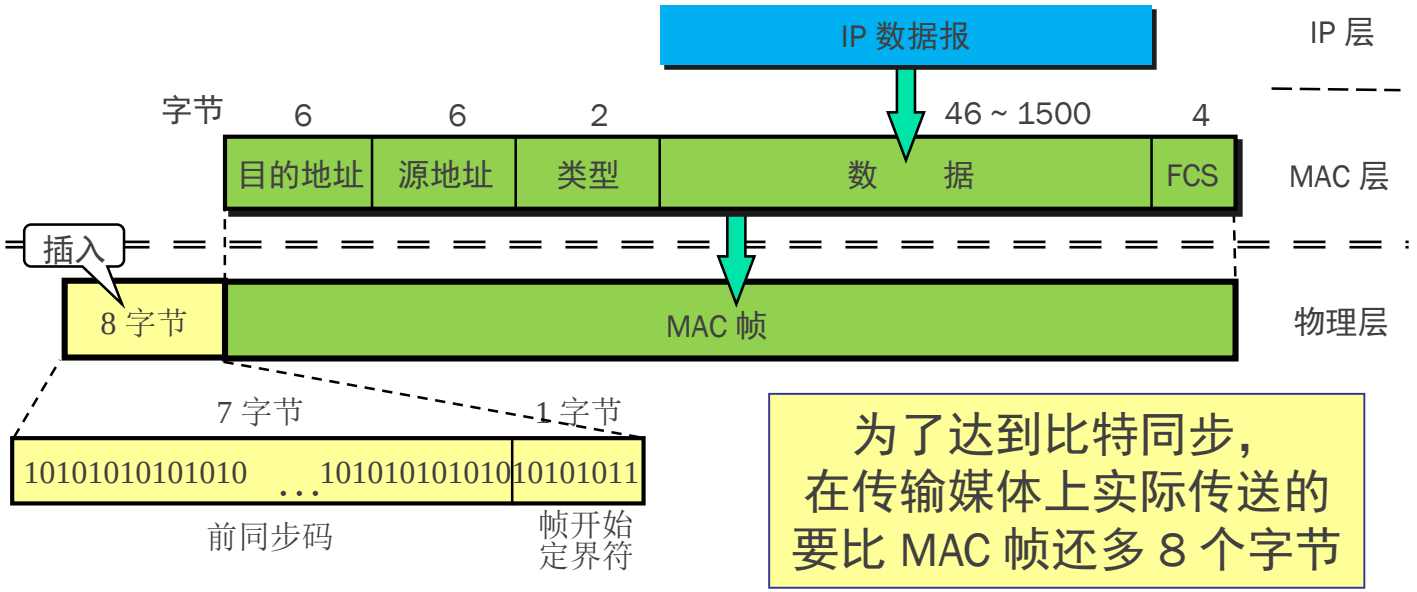
当传输媒体的误码率为 1×10^{-8} 时，
MAC 子层可使未检测到的差错小于 1×10^{-14}。



当数据字段的长度小于 46 字节时，
应在数据字段的后面加入整数字节的填充字段，
以保证以太网的 MAC 帧长不小于 64 字节。

以太网 V2 的 MAC 帧格式

在帧的前面插入的 8 字节中的第一个字段共 7 个字节，
是前同步码，用来迅速实现 MAC 帧的比特同步。
第二个字段是帧开始定界符，表示后面的信息就是MAC 帧。



为了达到比特同步，
在传输媒体上实际传送的
要比 MAC 帧还多 8 个字节

无效的 MAC 帧

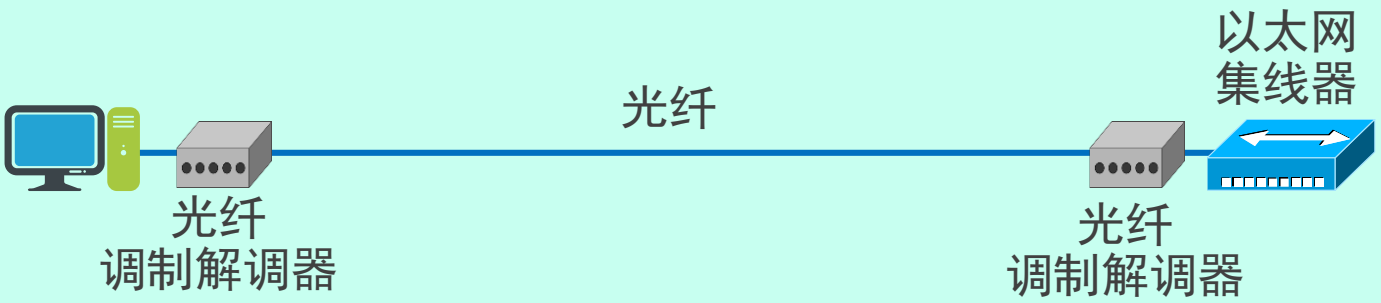
- 数据字段的长度与长度字段的值不一致；
- 帧的长度不是整数个字节；
- 用收到的帧检验序列 FCS 查出有差错；
- 数据字段的长度不在 46 ~ 1500 字节之间。
- 有效的 MAC 帧长度为 64 ~ 1518 字节之间。
- 对于检查出的无效 MAC 帧就简单地丢弃。以太网不负责重传丢弃的帧。

帧间最小间隔

- 帧间最小间隔为 9.6 μs，相当于 96 bit 的发送时间。
- 一个站在检测到总线开始空闲后，还要等待 9.6 μs 才能再次发送数据。
- 帧间间隔用于接收方检测一个帧的结束，同时也使得所有其它站点都能有机会平等竞争信道并发送数据。

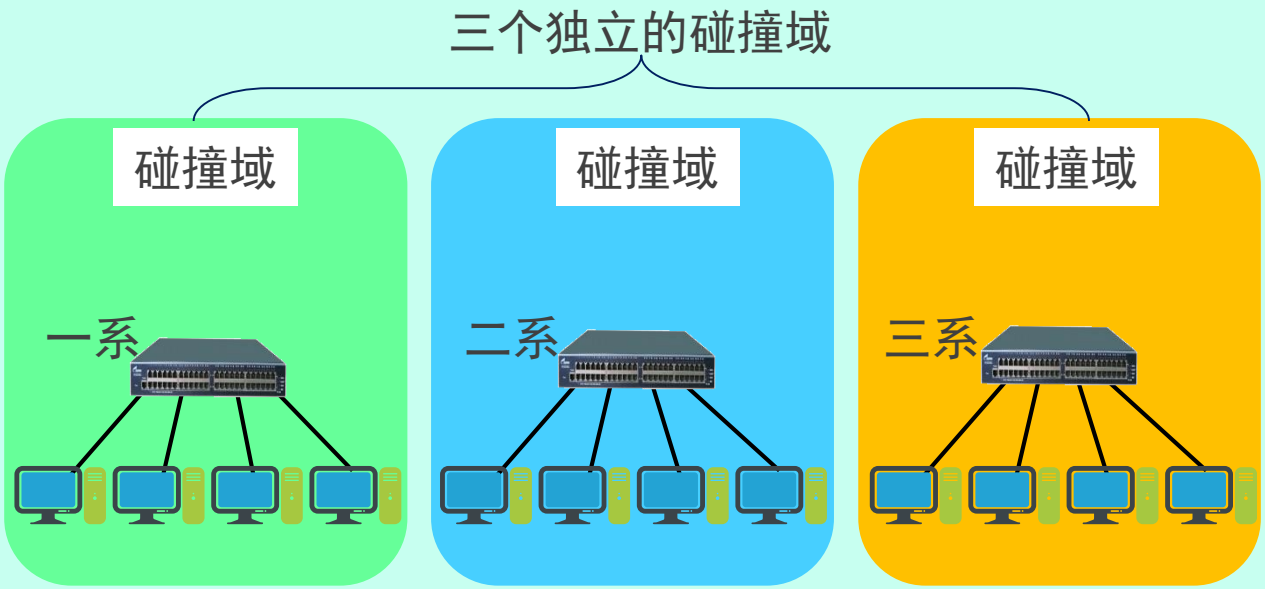
3.5.1 在物理层扩展以太网

- 主机使用光纤和一对光纤调制解调器连接到集线器



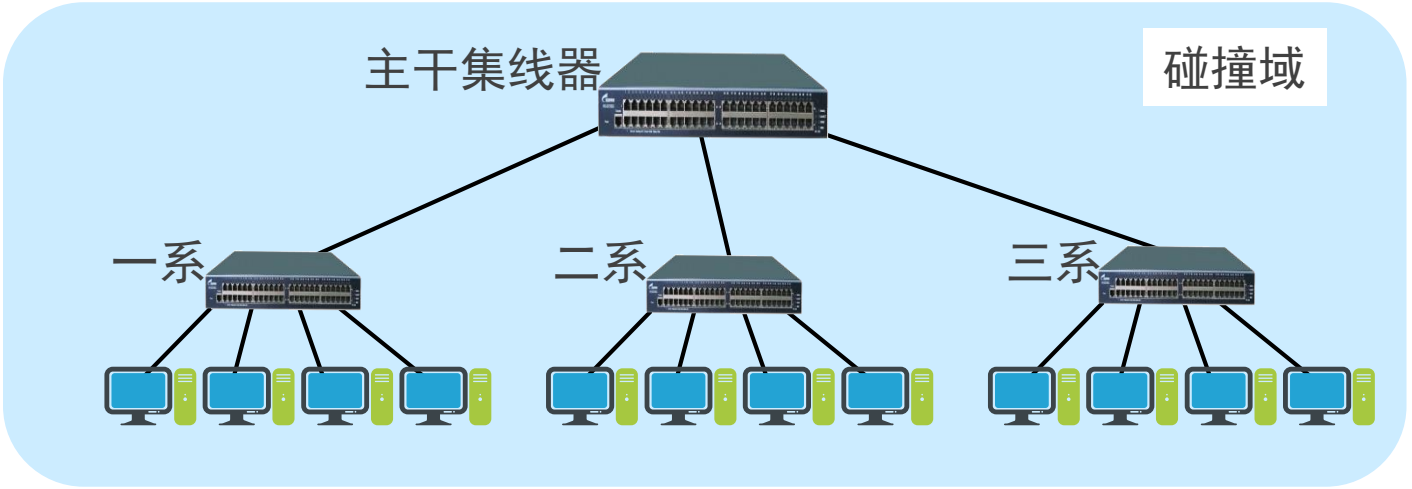
用多个集线器可连成更大的以太网

- 某大学有三个系，各自有一个局域网



用集线器组成更大的以太网都在一个碰撞域中

一个更大的碰撞域



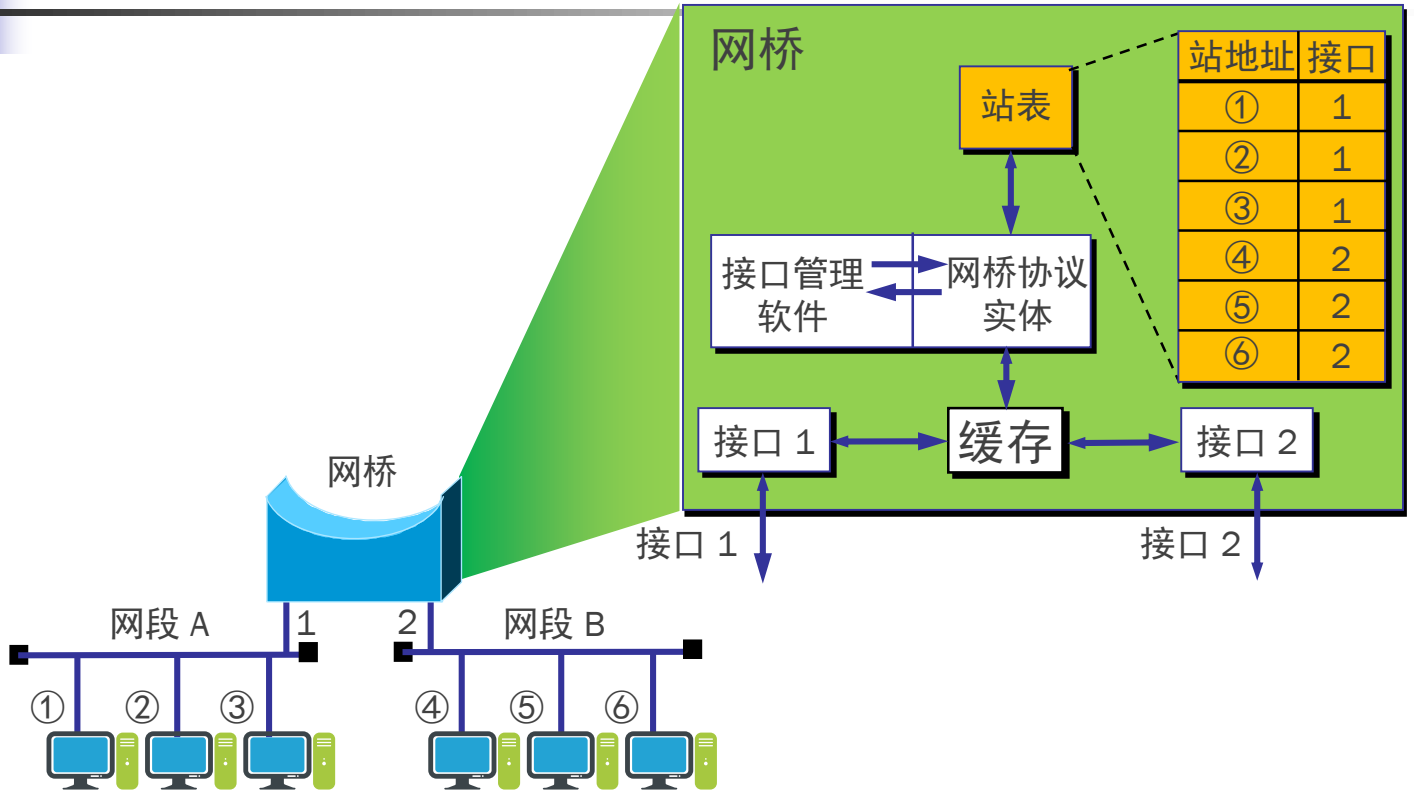
用集线器扩展以太网

- **优点**
  - 使原来属于不同碰撞域的局域网上的计算机能够进行跨碰撞域的通信。
  - 扩大了局域网覆盖的地理范围。
- **缺点**
  - 碰撞域增大了，但总的吞吐量并未提高。
  - 如果不同的碰撞域使用不同的数据率，那么就不能用集线器将它们互连起来。
  - 由于争用期的限制，并不能无限扩大地理覆盖范围

3.5.2 在数据链路层扩展以太网

- 在数据链路层扩展以太网要使用网桥。
- 网桥工作在数据链路层，它根据 MAC 帧的目的地址对收到的帧进行转发。
- 网桥具有过滤帧的功能。当网桥收到一个帧时，并不是向所有的接口转发此帧，而是先检查此帧的目的 MAC 地址，然后再确定将该帧转发到哪一个接口

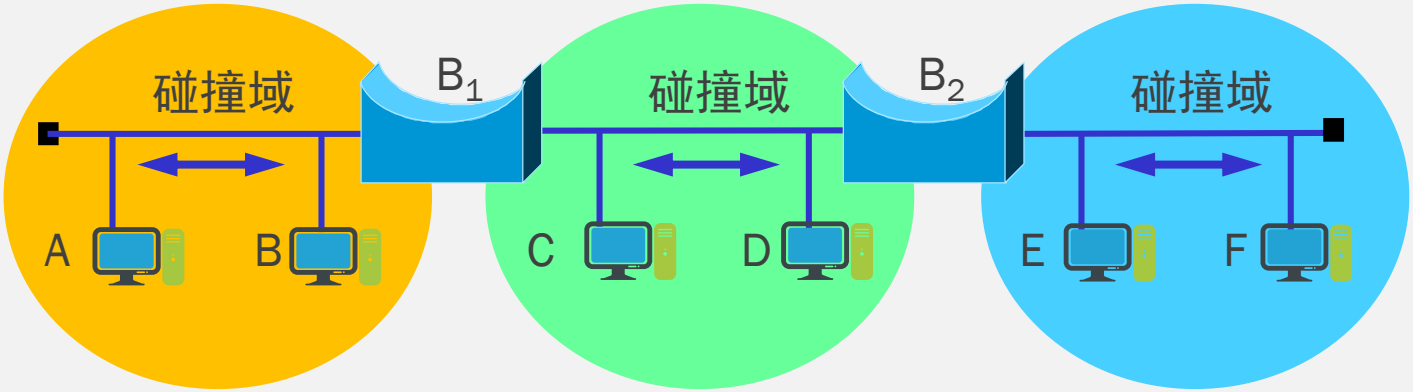
1. 网桥的内部结构


网桥
站表
站地址
接口
①
1
②
1
③
1
④
2
⑤
2
⑥
2
接口管理软件
网桥协议实体
接口 1
缓存
接口 2
接口 1
接口 2
网桥
网段 A
1
2
网段 B
①
②
③
④
⑤
⑥

使用网桥带来的好处

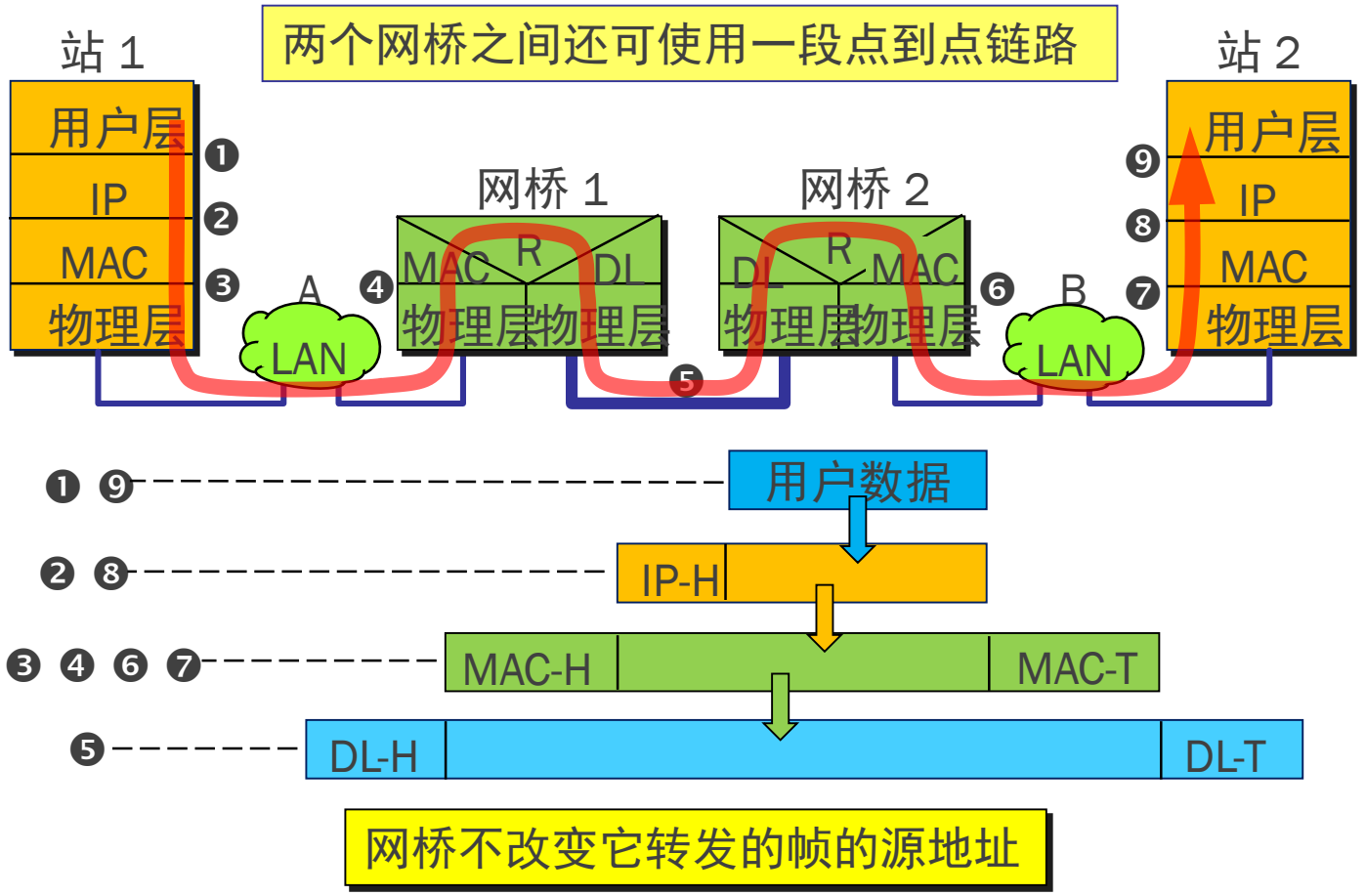
- 过滤通信量。
- 扩大了物理范围。
- 提高了可靠性。
- （由于采用存储转发方式）可互连不同物理层、不同 MAC 子层和不同速率（如10 Mb/s 和 100 Mb/s 以太网）的局域网。

网桥使各网段成为隔离开的碰撞域



使用网桥带来的缺点

- 存储转发增加了时延。
- 在MAC 子层并没有流量控制功能。
- 具有不同 MAC 子层的网段桥接在一起时时延更大。
- 网桥只适合于用户数不太多(不超过几百个)和通信量不太大的局域网，否则有时还会因传播过多的广播信息而产生网络拥塞。这就是所谓的广播风暴。


两个网桥之间还可使用一段点到点链路
站 1
站 2
用户层
IP
MAC
物理层
网桥 1
网桥 2
MAC
R
DL
物理层
A
B
LAN
用户数据
IP-H
MAC-H
MAC-T
DL-H
DL-T
网桥不改变它转发的帧的源地址

网桥和集线器（或转发器）不同

- 集线器在转发帧时，不对传输媒体进行检测。
- 网桥在转发帧之前必须执行 CSMA/CD 算法。
  - 若在发送过程中出现碰撞，就必须停止发送和进行退避。

2. 透明网桥

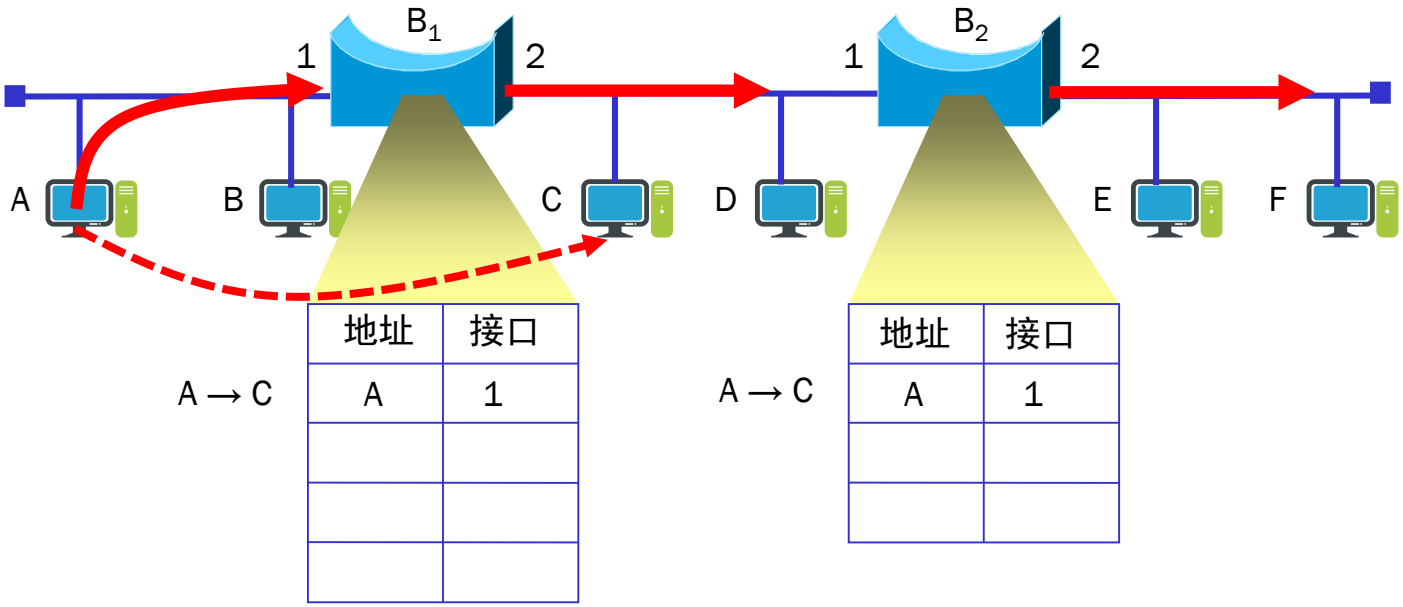
- 目前使用得最多的网桥是透明网桥(transparent bridge)。
- “透明”是指局域网上的站点并不知道所发送的帧将经过哪几个网桥，因为网桥对各站来说是看不见的。
- 透明网桥是一种即插即用设备，其标准是 IEEE 802.1D。

网桥应当按照以下自学习算法处理收到的帧和建立转发表

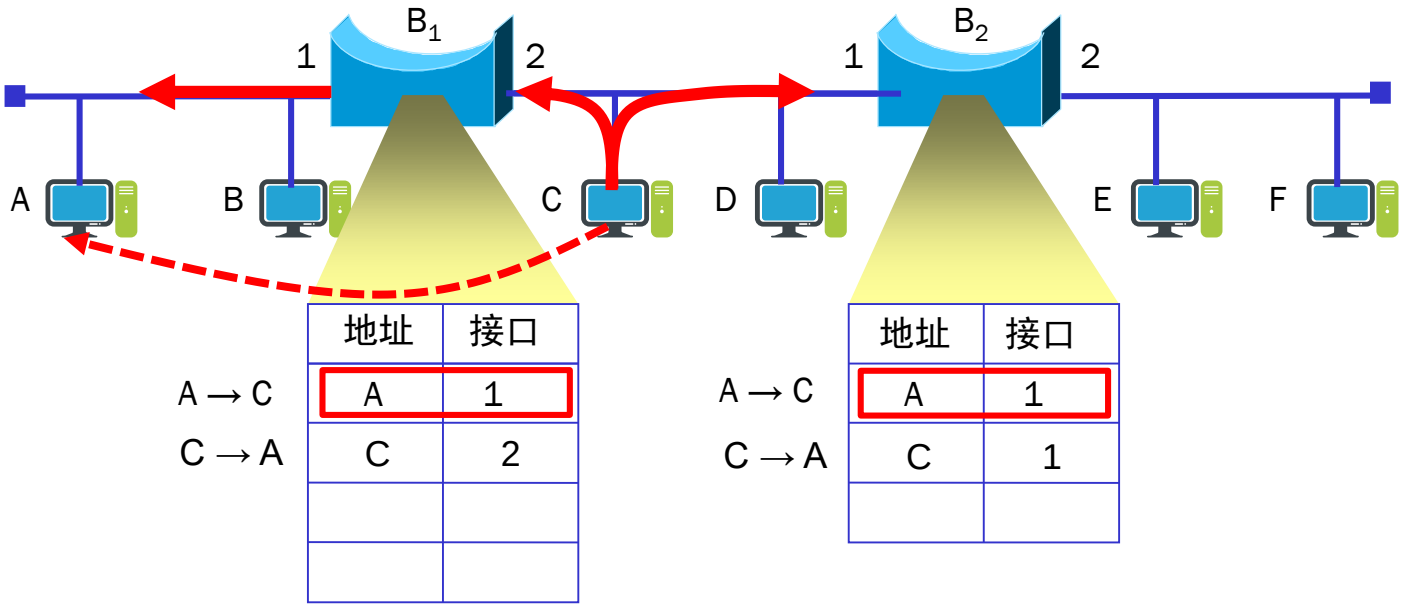
- 若从 A 发出的帧从接口 x 进入了某网桥，那么从这个接口出发沿相反方向一定可把一个帧传送到 A。
- 网桥每收到一个帧，就记下其源地址和进入网桥的接口，作为转发表中的一个项目。
- 在建立转发表时是把帧首部中的源地址写在“地址”这一栏的下面。
- 在转发帧时，则是根据收到的帧首部中的目的地址来转发的。这时就把在“地址”栏下面已经记下的源地址当作目的地址，而把记下的进入接口当作转发接口。

网桥自学习转发表

当网桥找不到目的地址所在接口时向所有其他接口转发！

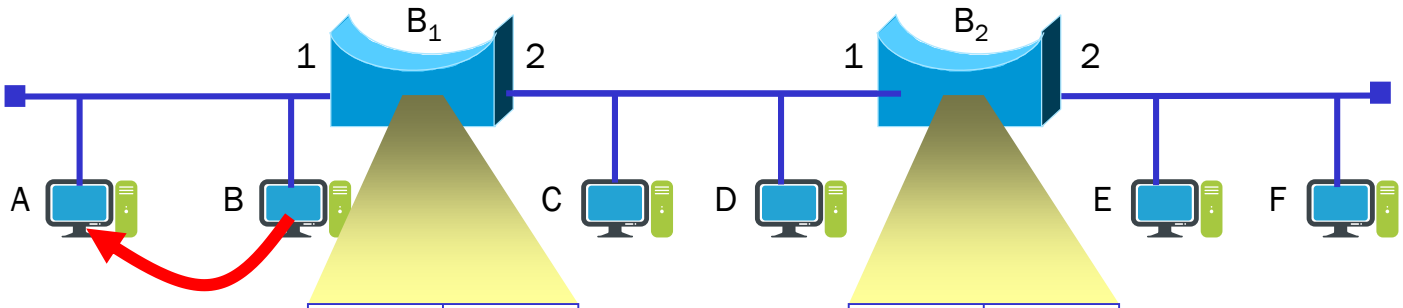


网桥自学习转发表



网桥自学习转发表

通过接收帧的源地址及接收接口学习站点和接口的对应关系！



	地址	接口
A → C	A	1
C → A	C	2
B → A	B	1

	地址	接口
A → C	A	1
C → A	C	1

网桥在转发表中登记以下三个信息

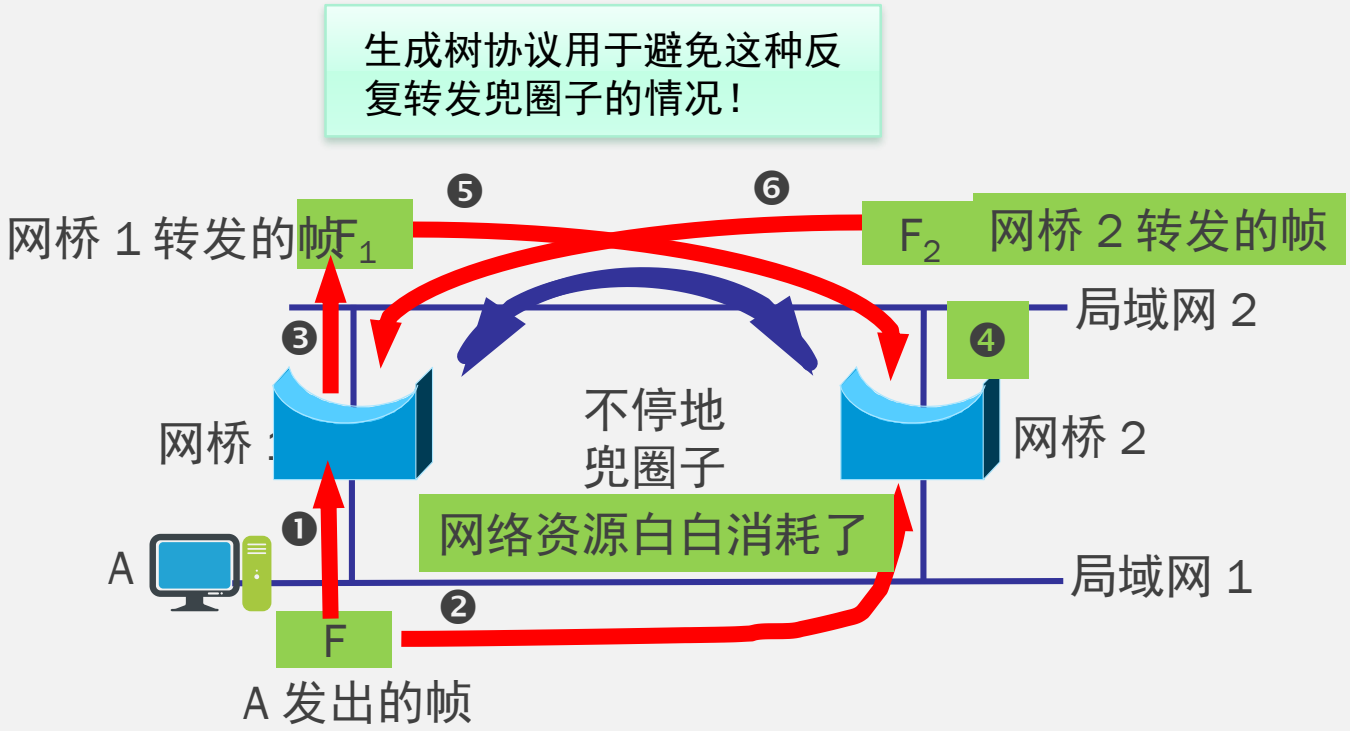
- 在网桥的转发表中写入的信息除了地址和接口外，还有帧进入该网桥的时间。
- 这是因为以太网的拓扑可能经常会发生变化，站点也可能会更换适配器（这就改变了站点的地址）。另外，以太网上的工作站并非总是接通电源的。
- 把每个帧到达网桥的时间登记下来，就可以在转发表中只保留网络拓扑的最新状态信息。这样就使得网桥中的转发表能反映当前网络的最新拓扑状态。

网桥的自学习和转发帧的步骤归纳

- 网桥收到一帧后先进行**自学习**。查找转发表中与收到帧的源地址有无相匹配的项目。如没有，就在转发表中增加一个项目（源地址、进入的接口和时间）。如有，则把原有的项目进行更新。
- **转发帧**。查找转发表中与收到帧的目的地址有无相匹配的项目。
  - 如没有，则通过所有其他接口（但进入网桥的接口除外）按进行转发。
  - 如有，则按转发表中给出的接口进行转发。
  - 若转发表中给出的接口就是该帧进入网桥的接口，则应丢弃这个帧（因为这时不需要经过网桥进行转发）。

3. 生成树协议

- **若帧F的目的地不在网桥1和2的转发表中，会帧F在网络中不断地兜圈子。**



生成树的得出

- 互连在一起的网桥在进行彼此通信后，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，即**在任何两个站之间只有一条路径**。
- 网桥会关闭不在生成树上的那些接口，以确保不存在环路。
- 为了得出能够反映网络拓扑发生变化时的生成树，在生成树上的根网桥每隔一段时间还要对生成树的拓扑进行更新。

网桥自动断开环路

- 网桥会关闭不在生成树上的那些接口，以确保不存在环路。

4. 源路由网桥

- 透明网桥容易安装，但网络资源的利用不充分。
- 源路由(source route)网桥在发送帧时将详细的路由信息放在帧的首部中。
- 源站以广播方式向欲通信的目的站发送一个发现帧，每个发现帧都记录所经过的路由。
- 发现帧到达目的站时就沿各自的路由返回源站。源站在得知这些路由后，从所有可能的路由中选择出一个最佳路由。凡从该源站向该目的站发送的帧的首部，都必须携带源站所确定的这一路由信息。

3.5.3 以太网交换机

- 1990 年问世的**交换式集线器**(switching hub)，可明显地提高局域网的性能。
- 交换式集线器常称为**以太网交换机**(switch)或第二层交换机（表明此交换机工作在数据链路层）。
- 以太网交换机通常都有十几个接口。因此，以太网交换机实质上就是一个**多接口的网桥**，可见交换机工作在数据链路层。

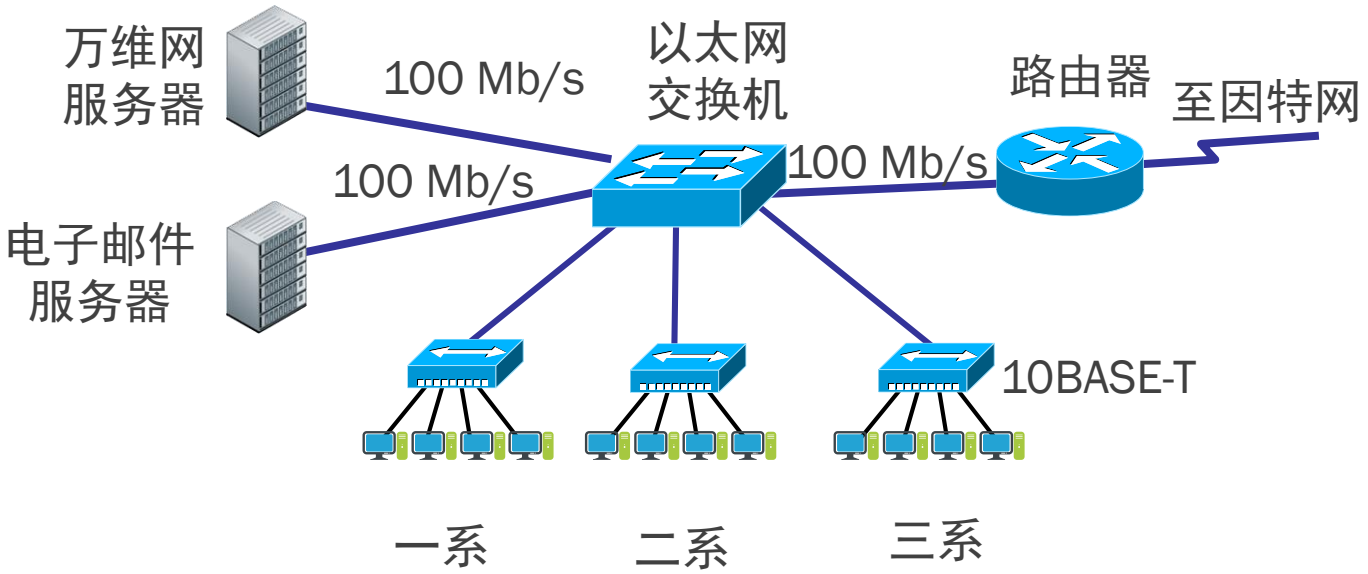
以太网交换机的特点

- 以太网交换机的每个接口都直接与主机相连，并且一般都工作在全双工方式。
- 交换机能同时连通许多对的接口，使每一对相互通信的主机都能像独占通信媒体那样，进行无碰撞地传输数据。
- 以太网交换机由于使用了专用的交换结构芯片，其交换速率较高。

独占传输媒体的带宽

- 对于普通 10 Mb/s 的共享式以太网，若共有 *N* 个用户，则每个用户占有的平均带宽只有总带宽(10 Mb/s)的 *N* 分之一。
- 使用以太网交换机时，虽然在每个接口到主机的带宽还是 10 Mb/s，但由于一个用户在通信时是独占而不是和其他网络用户共享传输媒体的带宽，因此对于拥有 *N* 对接口的交换机的总容量为 *N*×10 Mb/s。这正是交换机的最大优点。

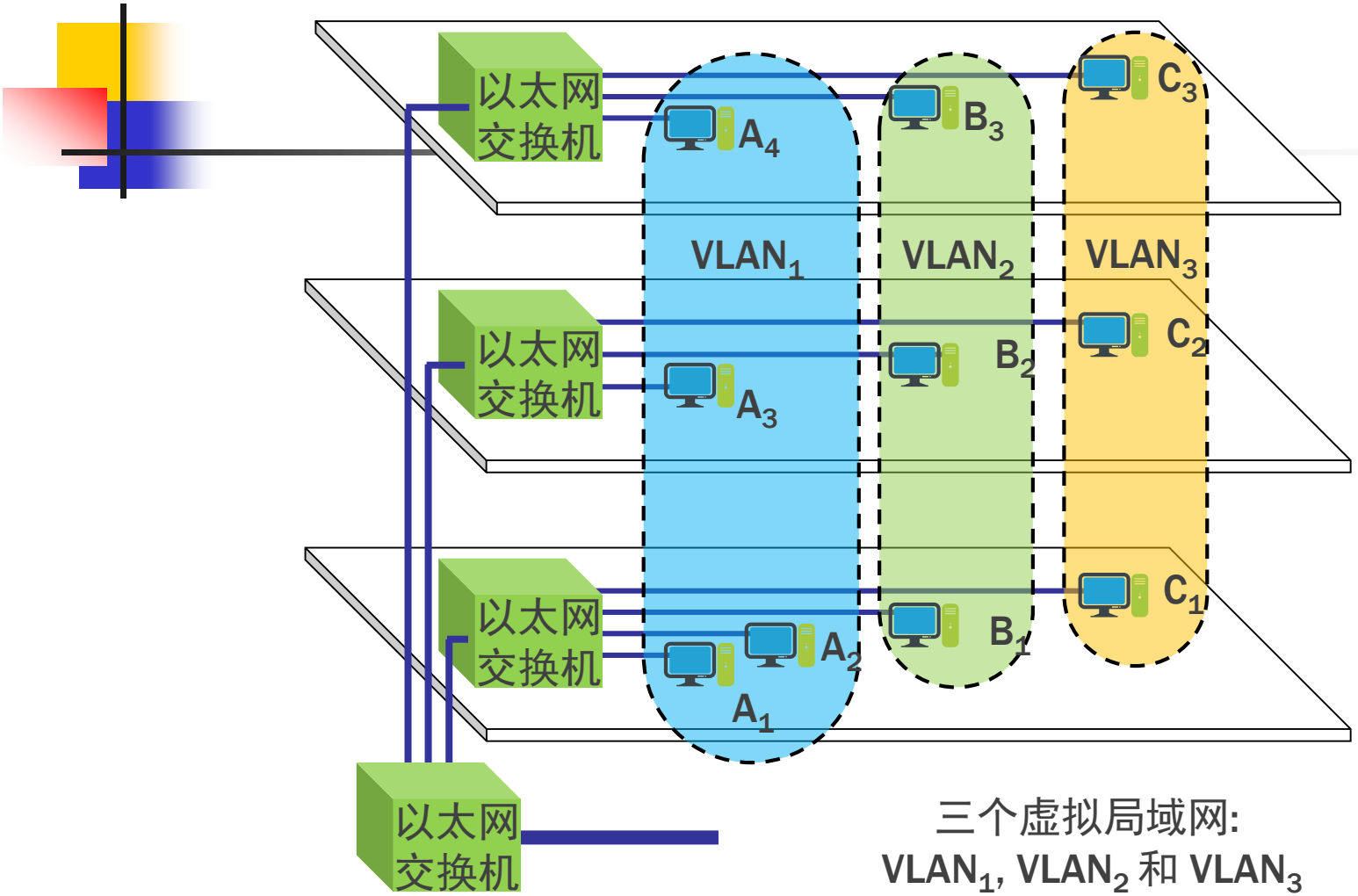
用以太网交换机扩展以太网



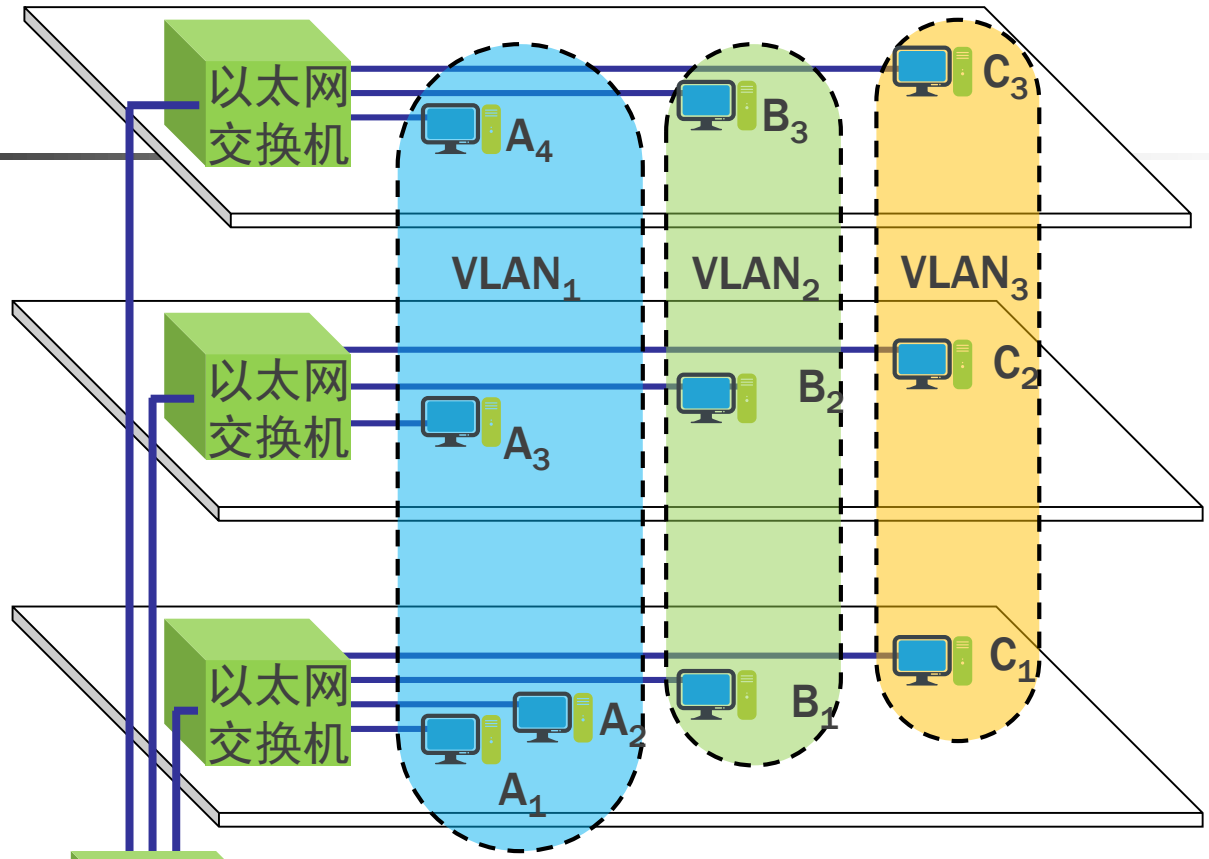
3.5.4 虚拟局域网

- 交换机可以很方便地实现虚拟局域网。
- 管理员可以将连接在交换机上的站点按需要划分为多个与物理位置无关的逻辑组，每个逻辑组就是一个VLAN。
- 属于同一VLAN的站点之间可以直接进行通信，而不属于同一VLAN的站点之间不能直接通信
- 连接在同一交换机上的站点也可以属于不同的VLAN，而属于VLAN中的两个站点可能连接在不同的交换机上。

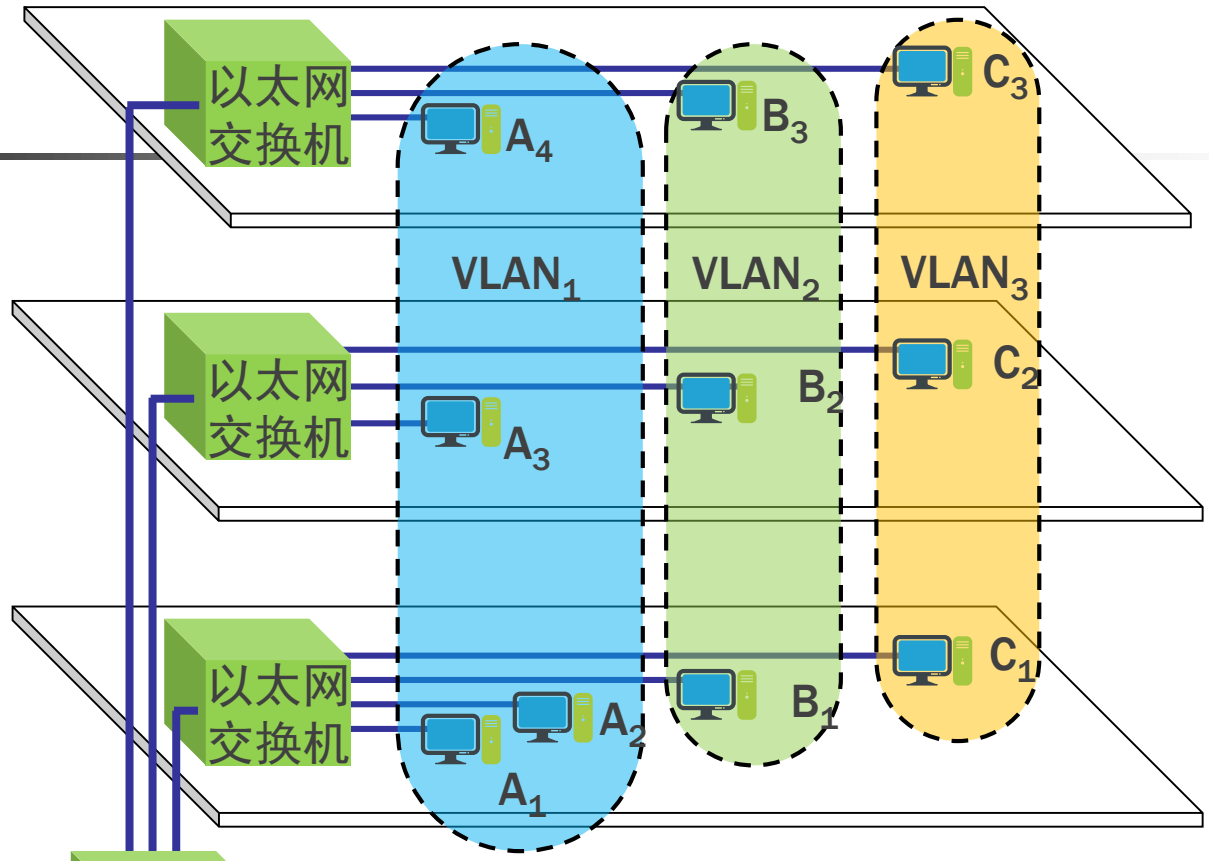
虚拟局域网其实只是局域网给用户提供的一种服务，而不是一种新型局域网！



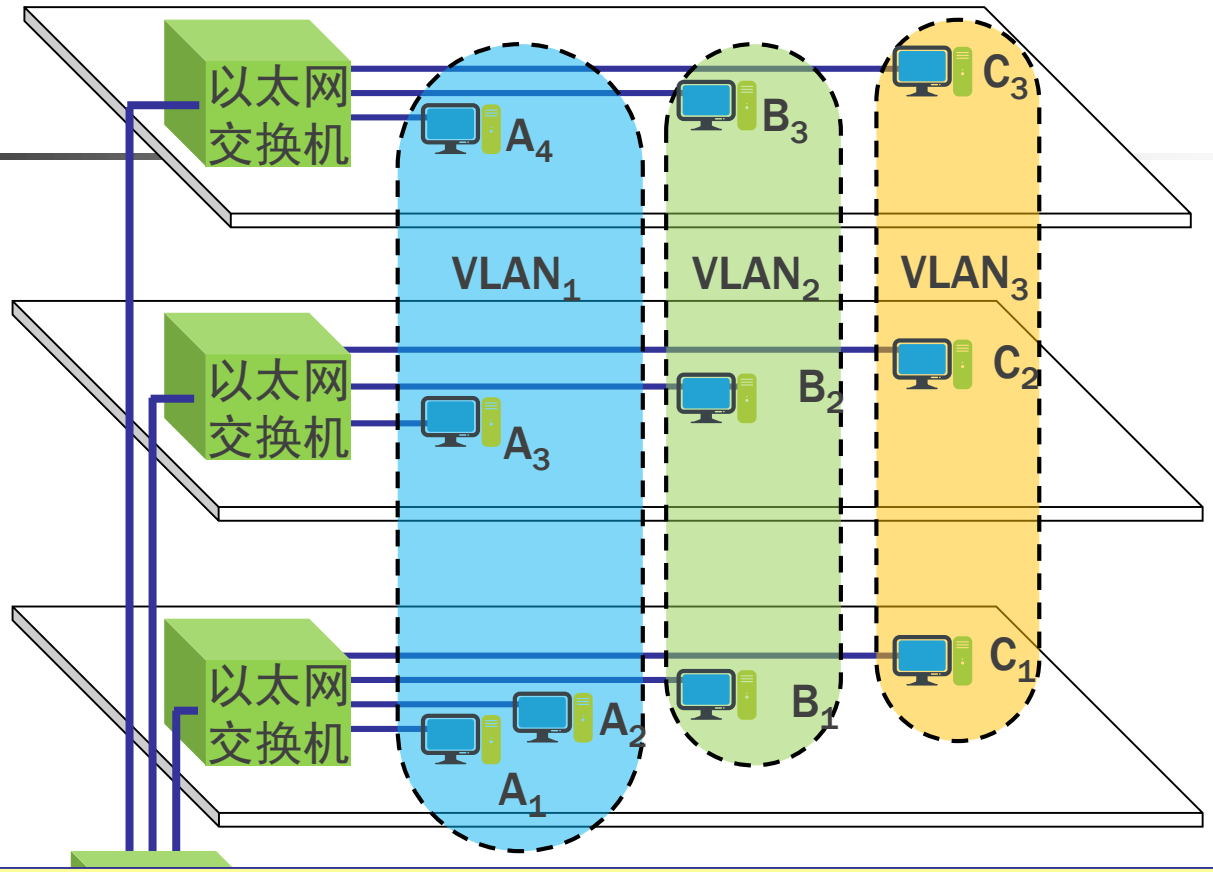
三个虚拟局域网:
$VLAN_1$, $VLAN_2$ 和 $VLAN_3$



当 B_1 向 $VLAN_2$ 工作组内成员发送数据时，
工作站 B_2 和 B_3 将会收到广播的信息。



B1 发送数据时，工作站 A1, A2 和 C1 都不会收到 B1 发出的广播信息。



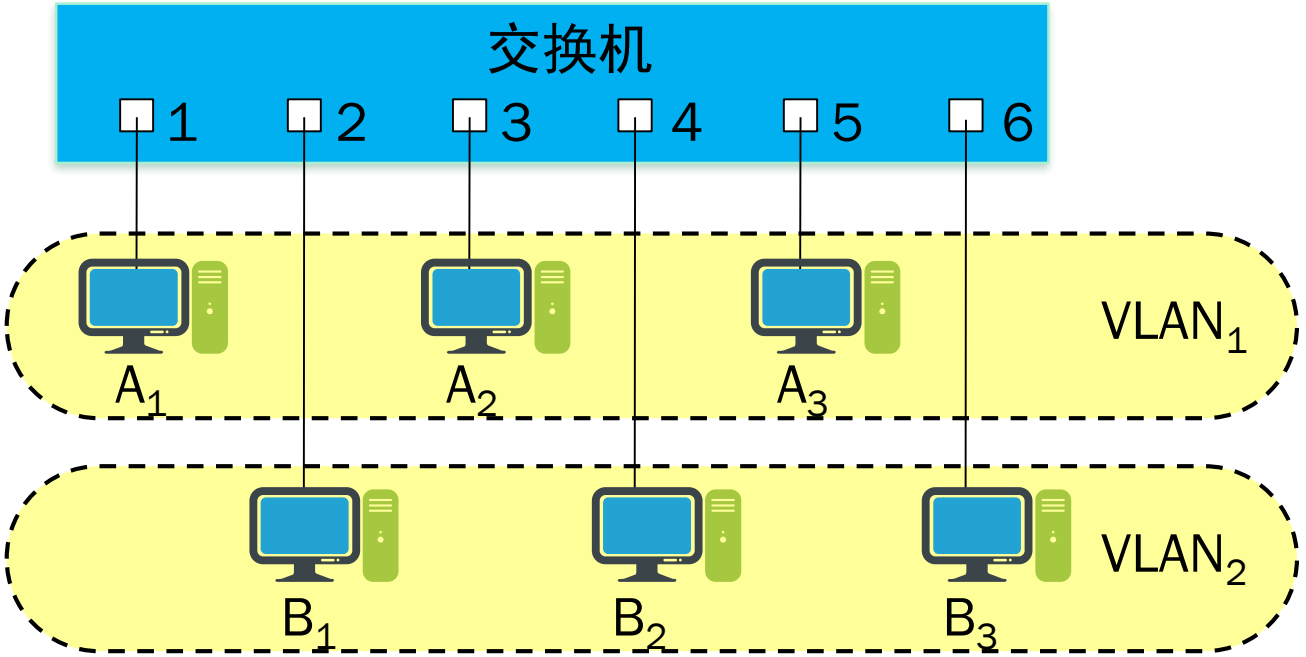
虚拟局域网限制了接收广播信息的工作站数，使得网络不会因传播过多的广播信息(即“广播风暴”)而引起性能恶化。

虚拟局域网的优点

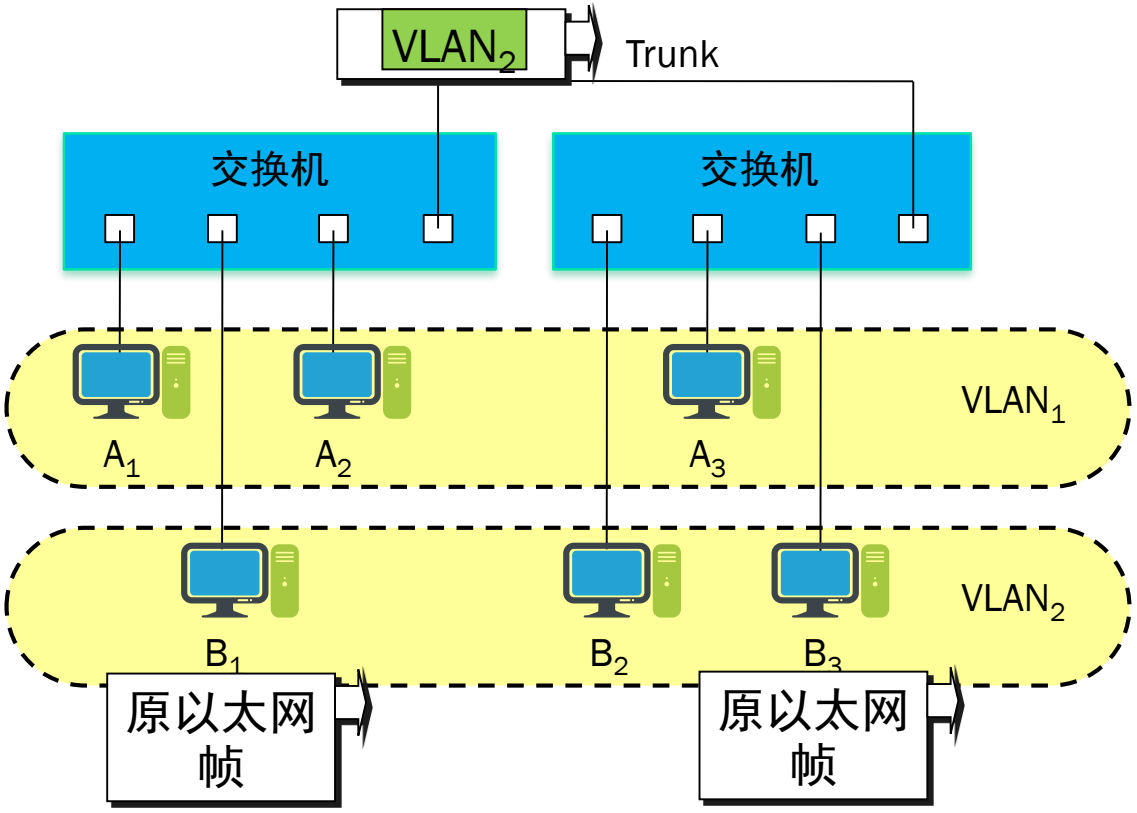
虚拟局域网具有以下优点：

- （1）简化网络管理。当站点从一个工作组迁移到另一个工作组时，仅需调整VLAN配置即可。
- （2）控制广播风暴。VLAN将大的局域网分隔成多个独立的广播域。
- （3）增强网络的安全性。便于管理员根据用户的安全需要隔离VLAN间的通信。

将接口划分到不同VLAN

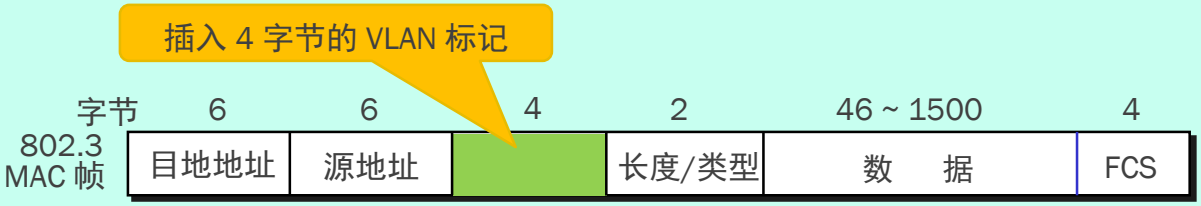


跨越多个交换机的VLAN



虚拟局域网使用的以太网帧格式

- 虚拟局域网协议允许在以太网的帧格式中插入一个 4 字节的标识符，称为VLAN 标记(tag)，用来指明发送该帧的工作站属于哪一个虚拟局域网。
- 802.1Q标准虽然修改了以太网的帧格式，但对所有用户站点是完全透明的，802.1Q标记帧仅在交换机间各VLAN复用的Trunk链路上使用。



3.6.1 100BASE-T 以太网

- 速率达到或超过 100 Mb/s 的以太网称为高速以太网。
- 在双绞线上传送 100 Mb/s 基带信号的星型拓扑以太网，仍使用 IEEE 802.3 的 CSMA/CD 协议。100BASE-T 以太网又称为快速以太网(Fast Ethernet)。

100BASE-T 以太网的特点

- 可在全双工方式下工作而无冲突发生。因此，不使用 CSMA/CD 协议。
- MAC 帧格式仍然是 802.3 标准规定的。
- 保持最短帧长不变，但将一个网段的最大电缆长度减小到 100 m。
- 帧间时间间隔从原来的 9.6 μs 改为现在的 0.96 μs。

三种不同的物理层标准

- 100BASE-TX
  - 使用 2 对 UTP 5 类线或屏蔽双绞线 STP。
- 100BASE-FX
  - 使用 2 对光纤。
- 100BASE-T4
  - 使用 4 对 UTP 3 类线或 5 类线。

3.6.2 吉比特以太网

- 允许在 1 Gb/s 下全双工和半双工两种方式工作。
- 使用 802.3 协议规定的帧格式。
- 在半双工方式下使用 CSMA/CD 协议（全双工方式不需要使用 CSMA/CD 协议）。
- 与 10BASE-T 和 100BASE-T 技术向后兼容。

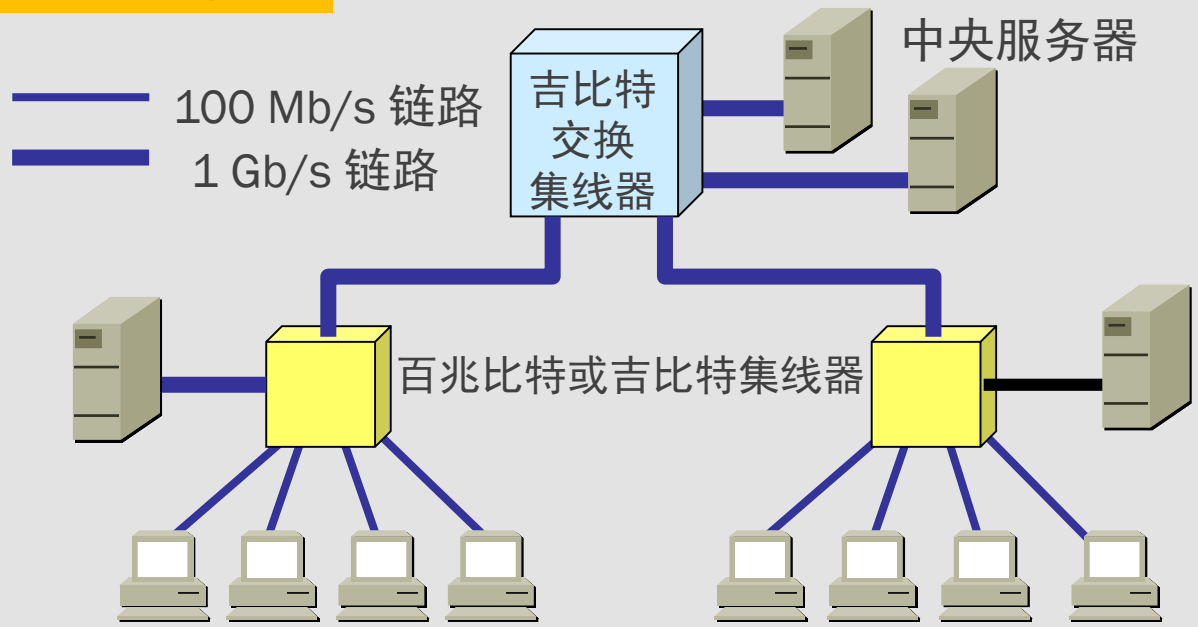
吉比特以太网的物理层

- 1000BASE-X　　基于光纤通道的物理层：
  - 1000BASE-SX　SX表示短波长
  - 1000BASE-LX　LX表示长波长
  - 1000BASE-CX　CX表示铜线
- 1000BASE-T
  - 使用 4对 5 类线 UTP

全双工方式

- 当吉比特以太网工作在全双工方式时（即通信双方可同时进行发送和接收数据），不使用载波延伸和分组突发。

吉比特以太网的配置举例



3.6.3 10 吉比特和100吉比特以太网

- 10 吉比特以太网与 10 Mb/s，100 Mb/s 和 1 Gb/s 以太网的帧格式完全相同。
- 10 吉比特以太网还保留了 802.3 标准规定的以太网最小和最大帧长，便于升级。
- 10 吉比特以太网不再使用铜线而只使用光纤作为传输媒体。
- 10 吉比特以太网只工作在全双工方式，因此没有争用问题，也不使用 CSMA/CD 协议。

端到端的以太网传输

- **10 吉比特和100吉比特以太网的出现，以太网的工作范围已经从局域网（校园网、企业网）扩大到城域网和广域网，从而实现了端到端的以太网传输。**

这种工作方式的好处是：

- 成熟的技术
- 互操作性很好
- 在广域网中使用以太网时价格便宜。
- 统一的帧格式简化了操作和管理。

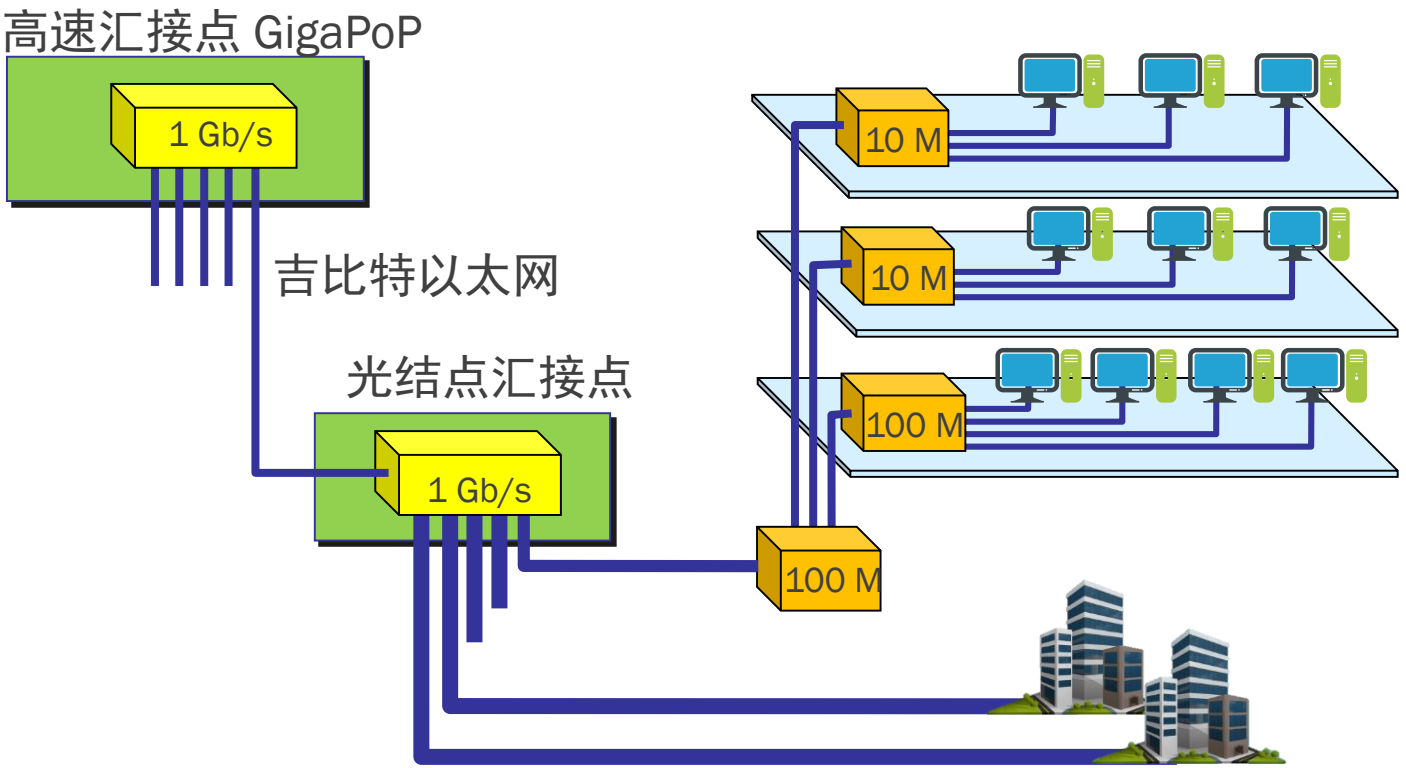
以太网从 10 Mb/s 到10 Gb/s 的演进

- 以太网从 10 Mb/s 到 10 Gb/s 的演进证明了以太网是：
  - 可扩展的（从 10 Mb/s 到 10 Gb/s）。
  - 灵活的（多种传输媒体、全/半双工、共享/交换）。
  - 易于安装。
  - 稳健性好。

3.6.4 使用以太网进行宽带接入

- 以太网已成功地把速率提高到 1 ~ 10 Gb/s，所覆盖的地理范围也扩展到了城域网和广域网，因此现在人们正在尝试使用以太网进行宽带接入。
- 以太网接入的重要特点是它可提供双向的宽带通信，并且可根据用户对带宽的需求灵活地进行带宽升级。
- 采用以太网接入可实现端到端的以太网传输，中间不需要再进行帧格式的转换。这就提高了数据的传输效率和降低了传输的成本。

以太网接入举例：光纤到大楼 FTTB

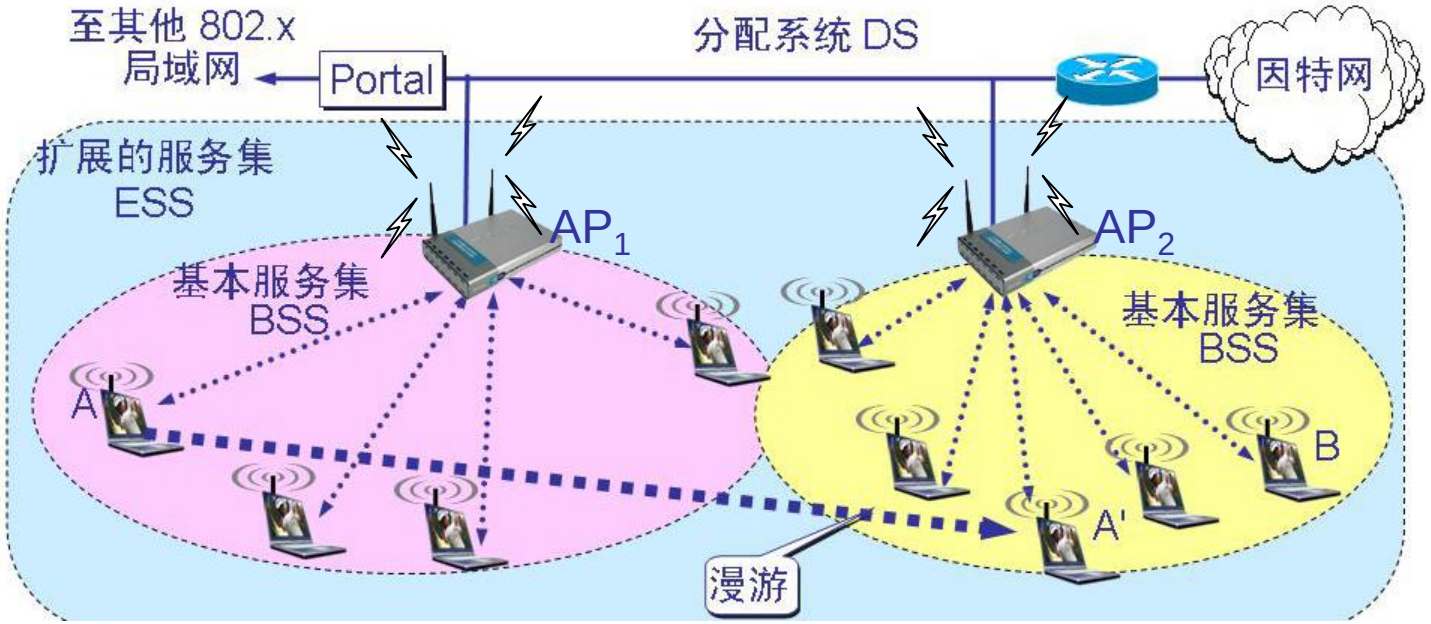


PPPoE (PPP over Ethernet)

- 以太网的帧格式中没有用户名/密码字段，因此以太网没有鉴别用户身份的功能，而这是居民接入网必须的功能。
- 为此PPPoE(PPP over Ethernet)把数据链路层的两个成功的协议结合起来，即把PPP协议中的PPP帧再封装到以太网中来传输。
- 现在的光纤宽带接入FTTx都要使用PPPoE的方式进行接入。
  - 当用户利用ADSL上网时，用户PC到ADSL调制解调器之间也使用PPPoE

3.7.1 无线局域网的组成

1. 有固定基础设施的无线局域网



IEEE 802.11

- 对于有固定基础设施的无线局域网，最有名的就是IEEE 802.11无线局域网。
- 实际上802.11既支持有固定基础设施的网络，也支持无固定基础设施的网络，但使用最多的是它的有固定基础设施的组网方式。
- 凡使用802.11系列协议的局域网又称为Wi-Fi（Wireless Fidelity，即无线保真度）

与接入点 AP 建立关联(association)

- 一个移动站若要加入到一个基本服务集 BSS，就必须先选择一个接入点 AP，并与此接入点建立关联。
- 建立关联就表示这个移动站加入了选定的 AP 所属的子网，并和这个 AP 之间创建了一个虚拟线路。
- 只有关联的 AP 才向这个移动站发送数据帧，而这个移动站也只有通过关联的 AP 才能向其他站点发送数据帧。

移动站与 AP 建立关联的方法

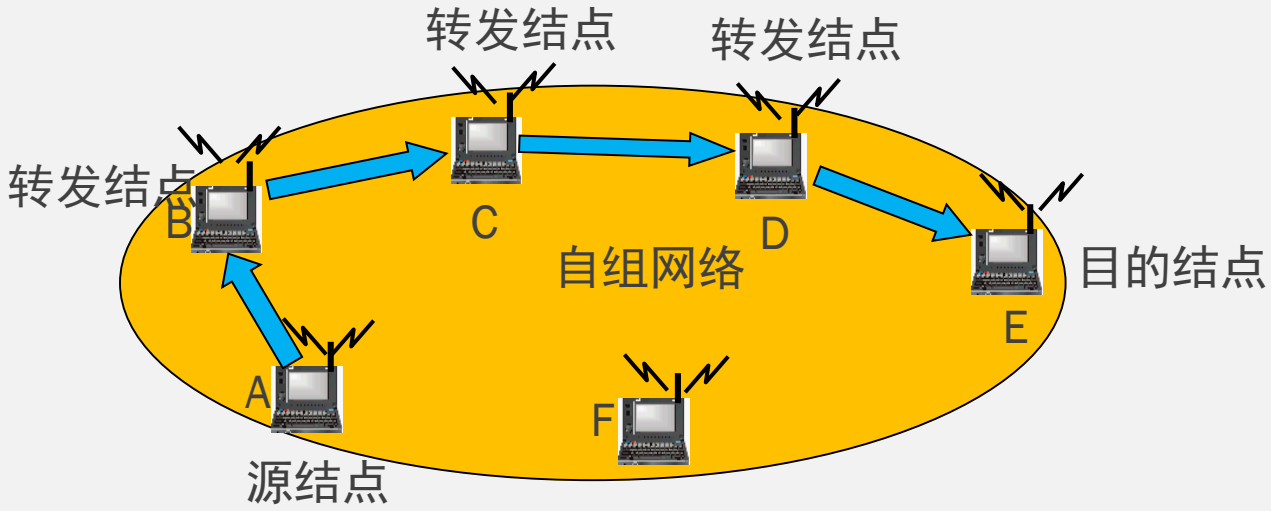
- **被动扫描**，即移动站等待接收接入站周期性发出的**信标帧**(beacon frame)。
- 信标帧中包含有若干系统参数（如服务集标识符 SSID 以及支持的速率等）。
- **主动扫描**，即移动站主动发出**探测请求帧**(probe request frame)，然后等待从 AP 发回的**探测响应帧**(probe response frame)。

热点(hot spot)

- 现在许多地方，如办公室、机场、快餐店、旅馆、购物中心等都能够向公众提供有偿或无偿接入 Wi-Fi 的服务。这样的地点就叫做热点。
- 由许多热点和 AP 连接起来的区域叫做热区(hot zone)。热点也就是公众无线入网点。
- 现在也出现了无线因特网服务提供者 WISP (Wireless Internet Service Provider)这一名词。用户可以通过无线信道接入到 WISP，然后再经过无线信道接入到因特网。

2. 移动自组网络又称自组网络(ad hoc network)

- 自组网络是没有固定基础设施（即没有 AP）的无线局域网。这种网络由一些处于平等状态的移动站之间相互通信组成的临时网络。



移动自组网络的应用前景

- 在军事领域中，携带了移动站的战士可利用临时建立的移动自组网络进行通信。
- 这种组网方式也能够应用到作战的地面车辆群和坦克群，以及海上的舰艇群、空中的机群。
- 当出现自然灾害时，在抢险救灾时利用移动自组网络进行及时的通信往往很有效的，

802.11的ad hoc模式

- 802.11的ad hoc模式允许在通信范围内的各站点间直接进行通信，组成一个无中心不与外界网络连接的自组网络，**支持站点间的单跳通信**，但在标准中并没有包括多跳路由功能。

3.7.2 802.11无线局域网的物理层

- 802.11 无线局域网可再细分为不同的类型。
- 现在最流行的无线局域网是 802.11b，而另外两种（802.11a 和 802.11g）的产品也广泛存在。
- 802.11 的物理层有以下几种实现方法：
  - 直接序列扩频 DSSS
  - 正交频分复用 OFDM
  - 跳频扩频 FHSS （已很少用）
  - 红外线 IR （已很少用）

几种常用的 802.11 无线局域网

标准	频段	数据速率	物理层	优缺点
802.11b	2.4 GHz	最高为 11 Mb/s	DSSS	最高数据率较低，价格最低，信号传播距离最远，且不易受阻碍
802.11a	5 GHz	最高为 54 Mb/s	OFDM	最高数据率较高，价格最高，信号传播距离较短，且易受阻碍
802.11g	2.4 GHz	最高为 54 Mb/s	OFDM	最高数据率较高，信号传播距离最远，且不易受阻碍，价格比 b 贵
802.11n	2.4 GHz 5 GHz	最高为 300Mb/s	MIMO OFDM	使用多个发射和接收天线来允许更高的数据传输率

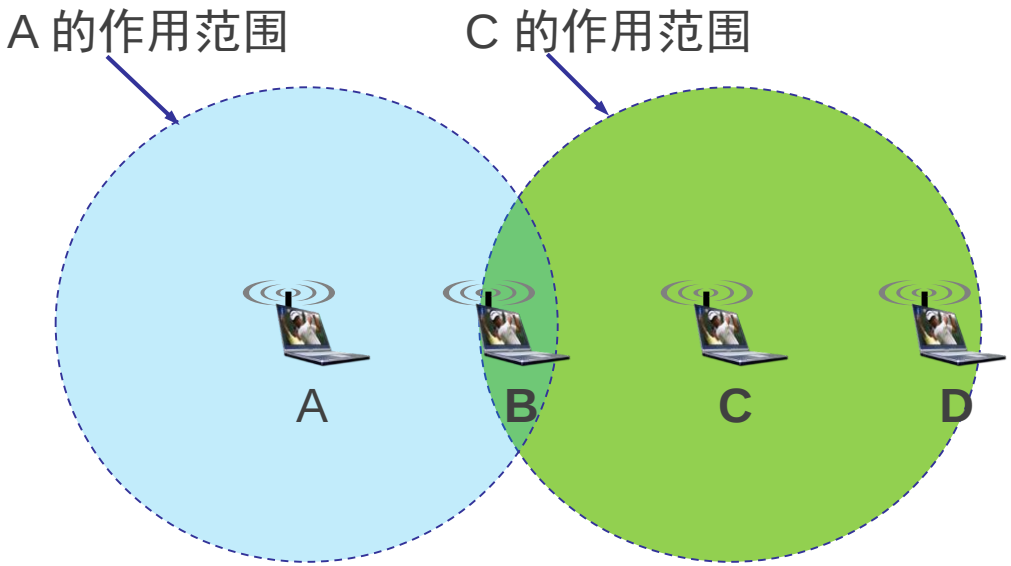
3.7.3 802.11 的 MAC协议

1. 使用CSMA/CA 协议

- 无线局域网不能简单地搬用 CSMA/CD 协
- 议。这里主要有两个原因。
- 对于无线信道，接收信号强度往往会远远小于发送信号强度。如要在无线局域网的适配器上实现碰撞检测，对硬件的要求非常高。
- 即使我们能够实现碰撞检测的功能，并且当我们在发送数据时检测到信道是空闲的，在接收端仍然有可能发生碰撞（隐蔽站问题）。

无线局域网的特殊问题

这种未能检测出媒体上已存在的信号的问题
叫做隐蔽站问题(hidden station problem)



当 A 和 C 检测不到无线信号时，都以为信道是空闲的，
因而都向 B 发送数据，结果发生碰撞。

CSMA/CA 协议

- 无线局域网不能使用 CSMA/CD，而只能使用改进的 CSMA 协议。
- 改进的办法是把 CSMA 增加一个**碰撞避免**(Collision Avoidance)功能。
- 802.11 就使用 CSMA/CA 协议。而在使用 CSMA/CA 的同时，还增加使用**停止等待协议**。
- 下面先介绍 802.11 的 MAC 层。

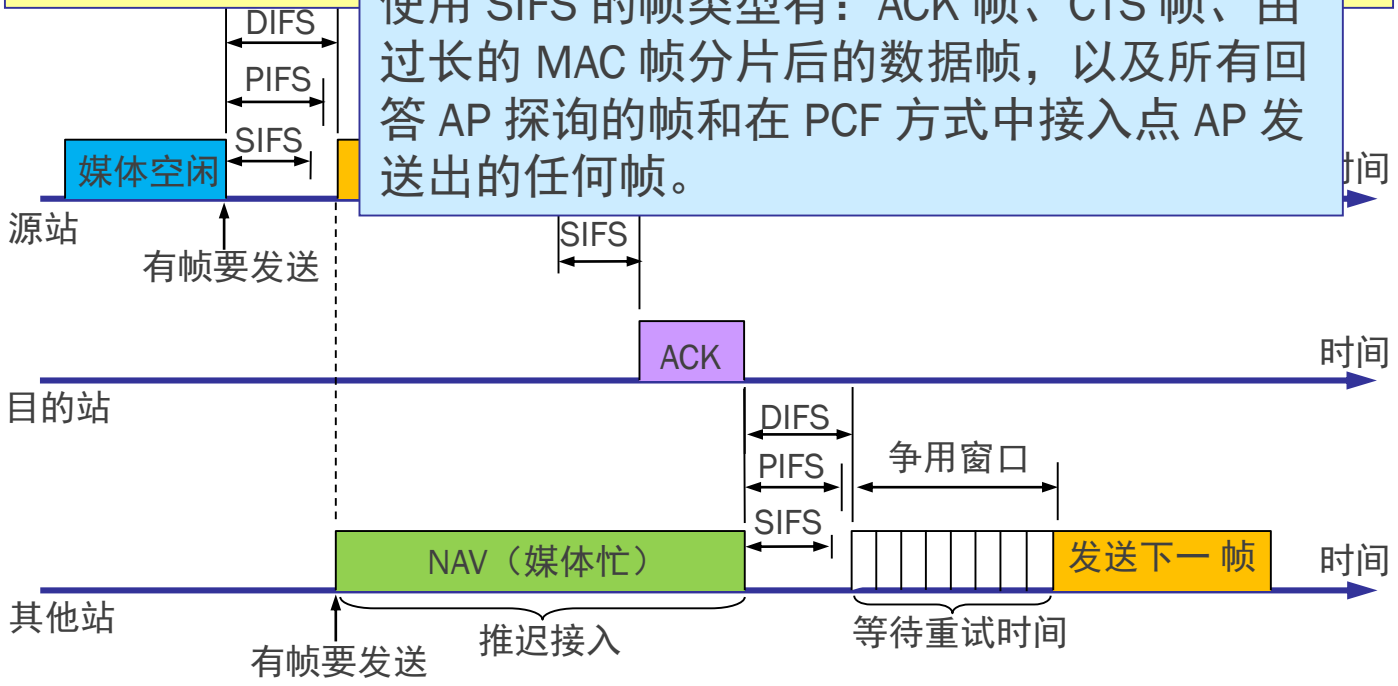
2. 确认与帧间间隔

- 所有的站在完成发送后，必须再等待一段很短的时间（继续监听）才能发送下一帧。这段时间的通称是**帧间间隔** IFS (InterFrame Space)。
- 帧间间隔长度取决于该站欲发送的帧的类型。高优先级帧需要等待的时间较短，因此可优先获得发送权。
- 若低优先级帧还没来得及发送而其他站的高优先级帧已发送到媒体，则媒体变为忙态因而低优先级帧就只能再推迟发送了。这样就减少了发生碰撞的机会。

三种帧间间隔

SIFS，即短(Short)帧间间隔，是最短的帧间间隔，用来分隔开属于一次对话的各帧。一个站应当能够在这段时间内从发送方式切换到接收方式。

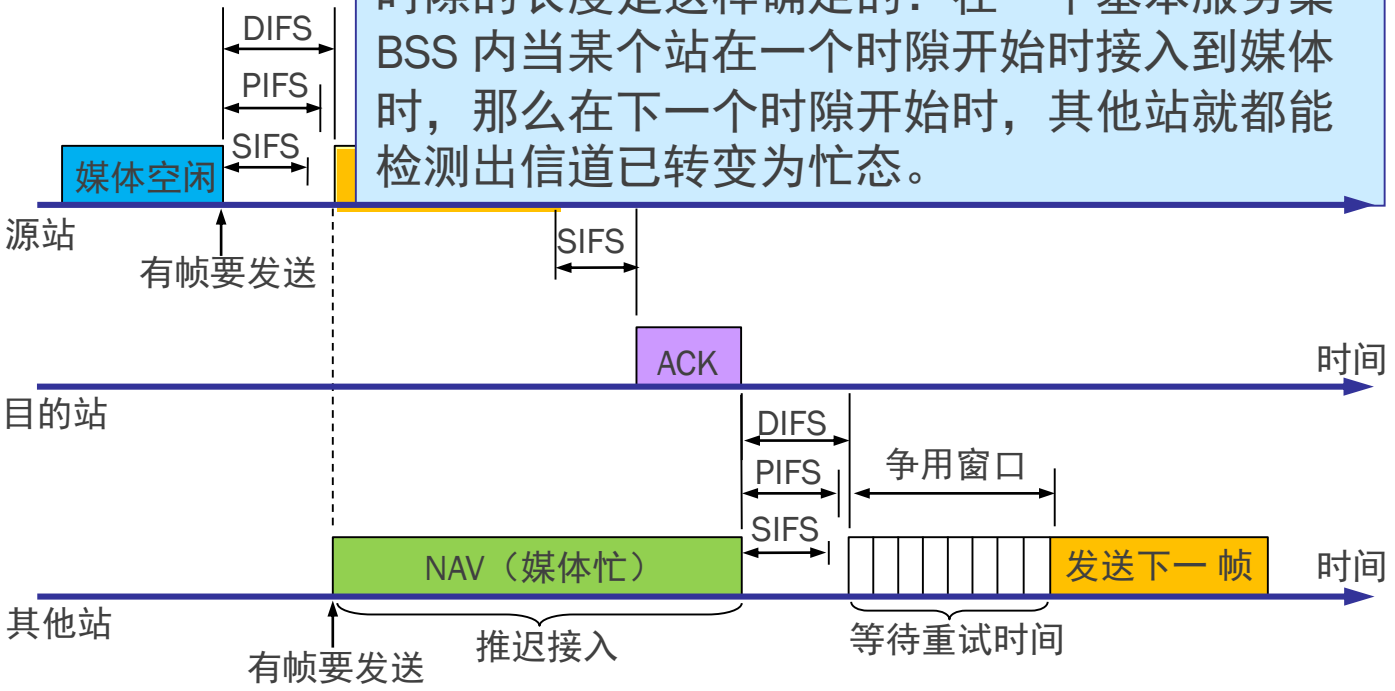
使用 SIFS 的帧类型有：ACK 帧、CTS 帧、由过长的 MAC 帧分片后的数据帧，以及所有回答 AP 探询的帧和在 PCF 方式中接入点 AP 发送出的任何帧。



三种帧间间隔

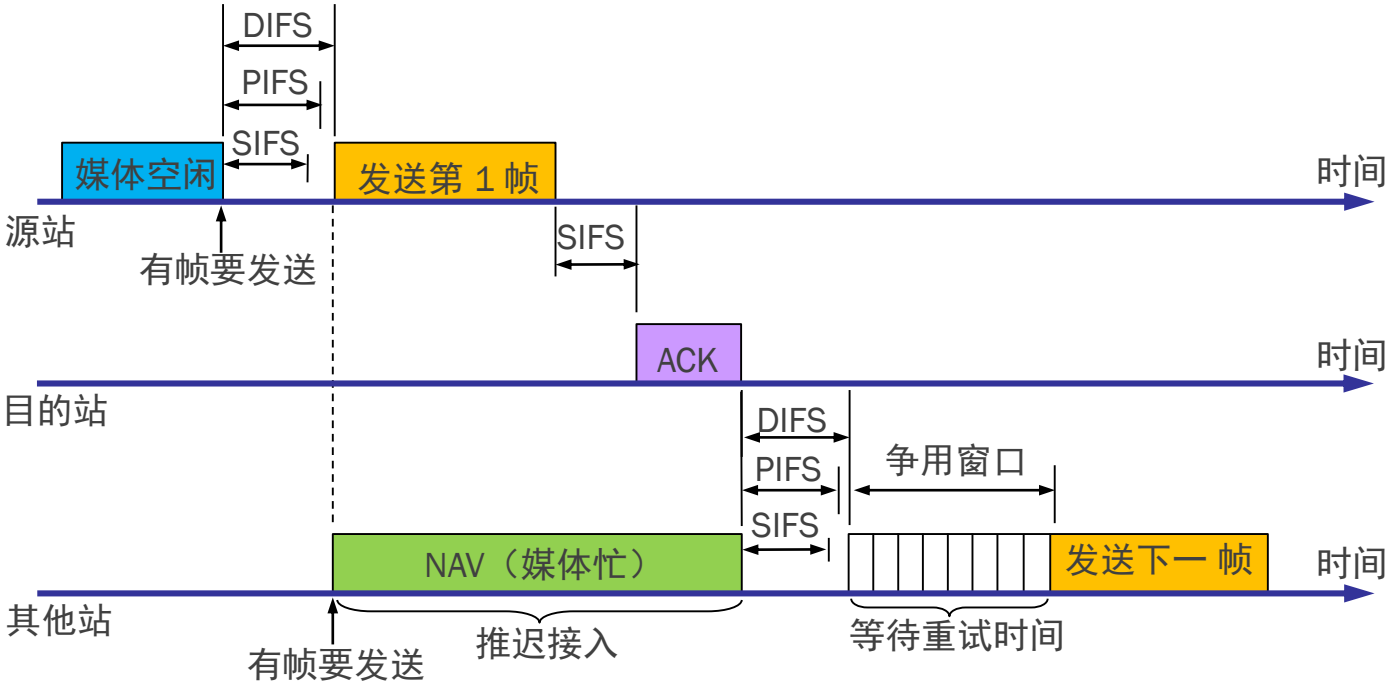
PIFS，即点协调功能帧间间隔，它比 SIFS 长，是为了在开始使用 PCF 方式时（在 PCF 方式下使用，没有争用）优先获得接入到媒体中。PIFS 的长度是 SIFS 加一个时隙(slot)长度

时隙的长度是这样确定的：在一个基本服务集 BSS 内当某个站在一个时隙开始时接入到媒体时，那么在下一个时隙开始时，其他站就都能检测出信道已转变为忙态。



三种帧间间隔

DIFS，即分布协调功能帧间间隔（最长的 IFS），在 DCF 方式中用来发送数据帧和管理帧。DIFS 的长度比 PIFS 再增加一个时隙长度。



CSMA/CA 协议的原理

- 欲发送数据的站先检测信道。在 802.11 标准中规定了在物理层的空中接口进行物理层的载波监听。
- 通过收到的相对信号强度是否超过一定的门限数值就可判定是否有其他的移动站在信道上发送数据。
- 当源站发送它的第一个 MAC 帧时，若检测到信道空闲，则在等待一段时间 DIFS 后就可发送。

为什么信道空闲还要再等待

- 这是考虑到可能有其他的站有高优先级的帧要发送。
- 如有，就要让高优先级帧先发送。

假定没有高优先级帧要发送

- 源站发送了自己的数据帧。
- 目的站若正确收到此帧，则经过时间间隔 SIFS 后，向源站发送确认帧 ACK。
- 若源站在规定时间内没有收到确认帧 ACK（可能是发生碰撞），就必须重传此帧，直到收到确认为止，或者经过若干次的重传失败后放弃发送。
- 确认机制可以认为是一种**间接碰撞检测** 。

3. 退避算法

- 为避免碰撞，如果要发送数据的站发现信道忙，**在信道恢复空闲时并不是立即发送数据**，而是要退避一段随机的时间（大于DIFS）若信道仍然空闲才能发送数据
- 若发送方接收到确认要立即发送下一帧时，为公平竞争，也要执行退避
- 当发送方没有接收到确认，重传帧时，要将随机选择退避时间的范围**扩大一倍**。

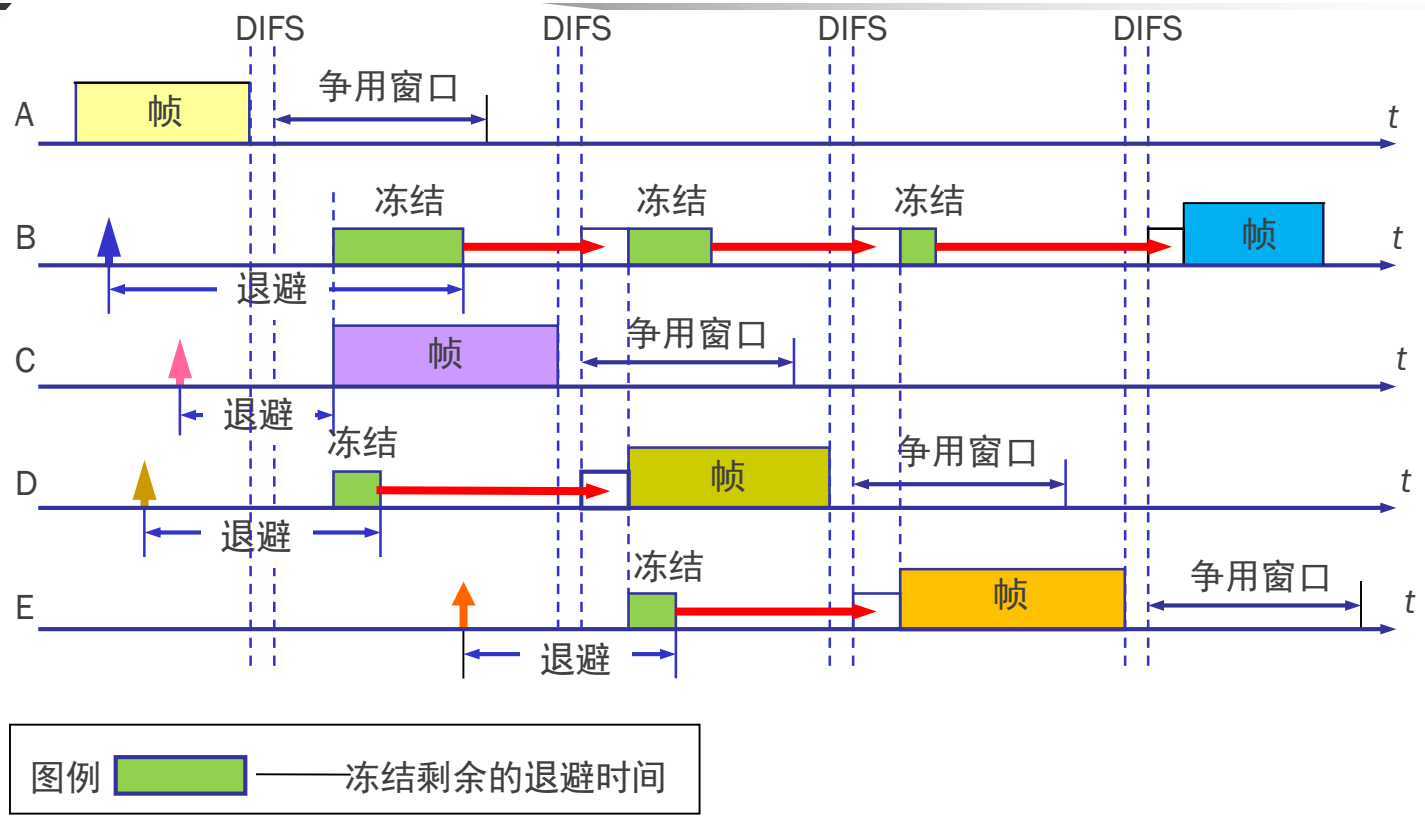
退避计时器(backoff timer)

- 站点每经历一个时隙的时间就检测一次信道。这可能发生两种情况。
  - 若检测到信道空闲，退避计时器就继续倒计时。
  - 若检测到信道忙，就冻结退避计时器的剩余时间，重新等待信道变为空闲并再经过时间DIFS 后，从剩余时间开始继续倒计时。如果退避计时器的时间减小到零时，就开始发送整个数据帧。

退避算法的使用情况

- 仅在下面的情况下才不使用退避算法：检测到信道是空闲的，并且这个数据帧是要发送的第一个数据帧。
- 除此以外的所有情况，都必须使用退避算法。即：
  - 在发送第一个帧之前检测到信道处于忙态。
  - 在每一次的重传后。
  - 在每一次的成功发送后。

802.11 的退避机制


DIFS
DIFS
DIFS
DIFS
A
帧
争用窗口
t
B
冻结
冻结
冻结
帧
t
退避
C
帧
争用窗口
t
退避
冻结
D
帧
争用窗口
t
退避
冻结
E
帧
争用窗口
t
退避
图例
——冻结剩余的退避时间

4. 虚拟载波监听

- **虚拟载波监听**(Virtual Carrier Sense)的机制是让源站将它要占用信道的时间（包括目的站发回确认帧所需的时间）通知给所有其他站，以便使其他所有站在这一段时间都停止发送数据。
- 这样就大大减少了碰撞的机会。
- “虚拟载波监听”是表示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。

虚拟载波监听的效果

- 这种效果好像是其他站都监听了信道。
- 所谓“源站的通知”就是源站在其 MAC 帧首部中的第二个字段“持续时间”中填入了在本帧结束后还要占用信道多少时间（以微秒为单位），包括目的站发送确认帧所需的时间。

网络分配向量

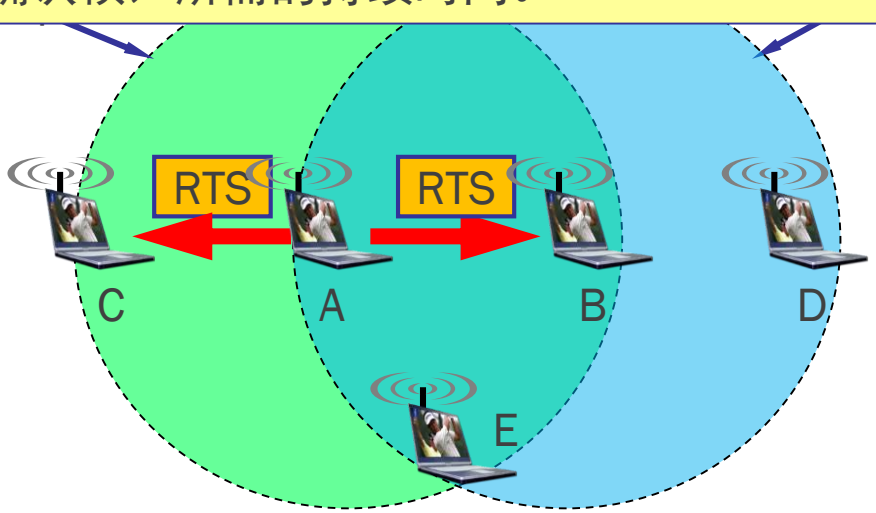
- 当一个站检测到正在信道中传送的 MAC 帧首部的“持续时间”字段时，就调整自己的网络分配向量 NAV (Network Allocation Vector)。
- NAV 指出了必须经过多少时间才能完成数据帧的这次传输，才能使信道转入到空闲状态。

5. 对信道进行预约

- **802.11 允许要发送数据的站对信道进行预约。**

源站 A 在发送数据帧之前先发送一个短的控制帧，叫做请求发送 RTS (Request To Send)，它包括源地址、目的地址和这次通信（包括相应的确认帧）所需的持续时间。

A 的作用范围

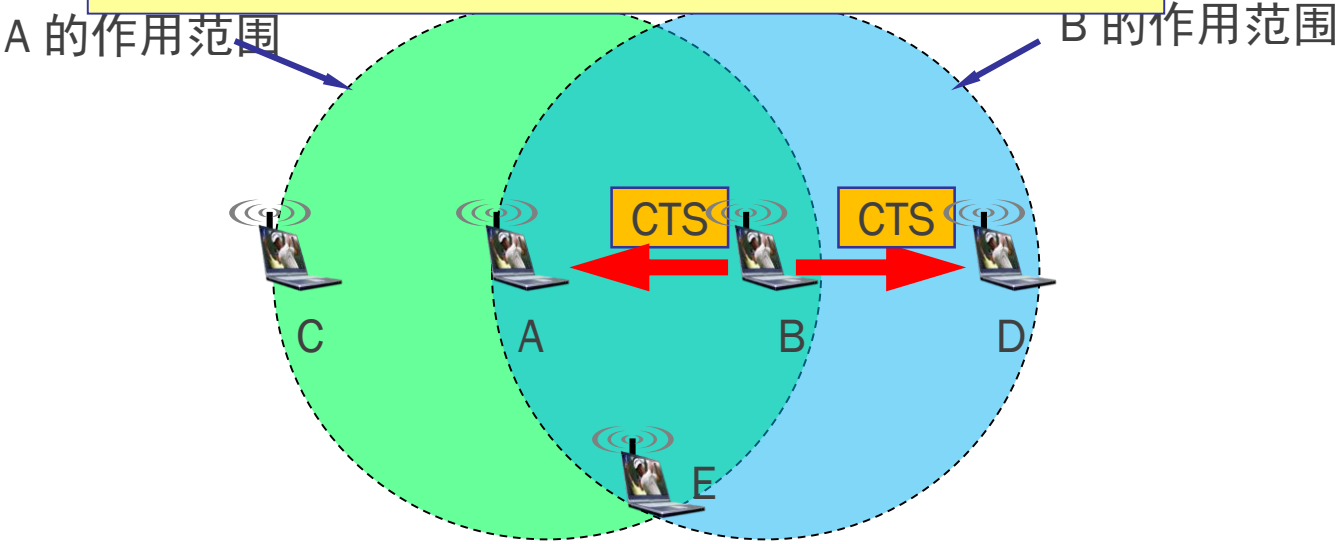


5. 对信道进行预约

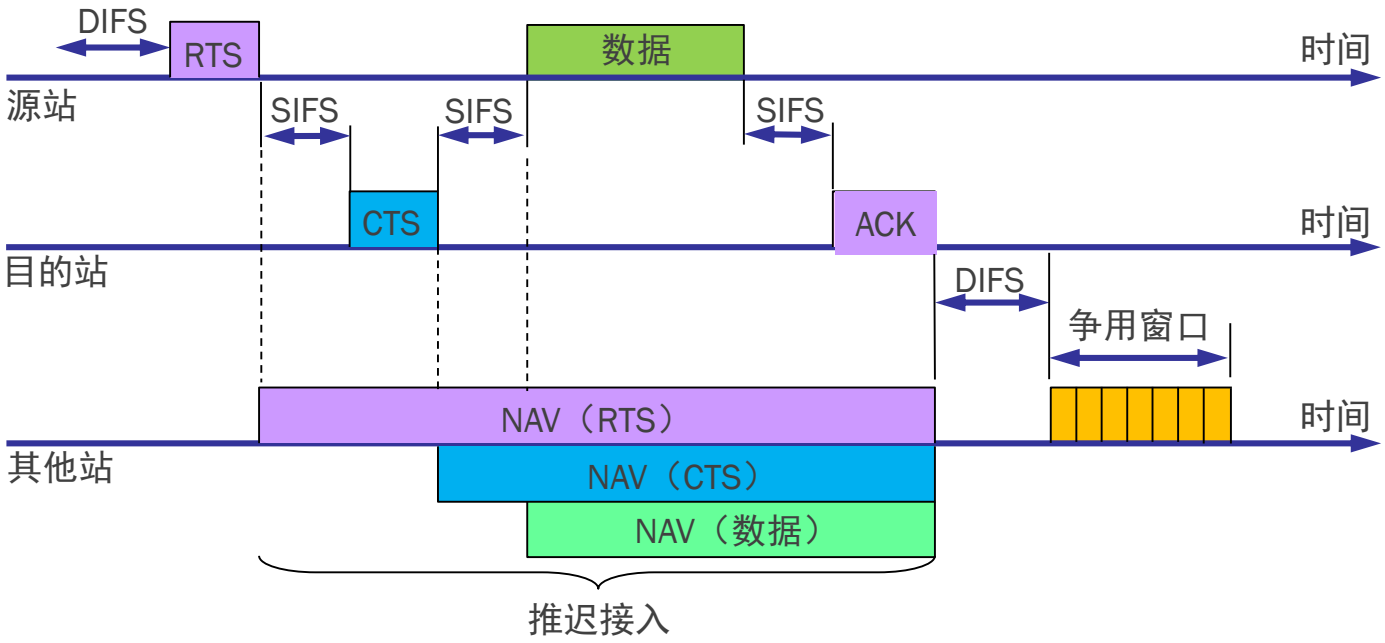
- **802.11 允许要发送数据的站对信道进行预约。**

若媒体空闲，则目的站 B 就发送一个响应控制帧，叫做允许发送 CTS (Clear To Send)，它包括这次通信所需的持续时间（从 RTS 帧中将此持续时间复

A 收到 CTS 帧后就可发送其数据帧。

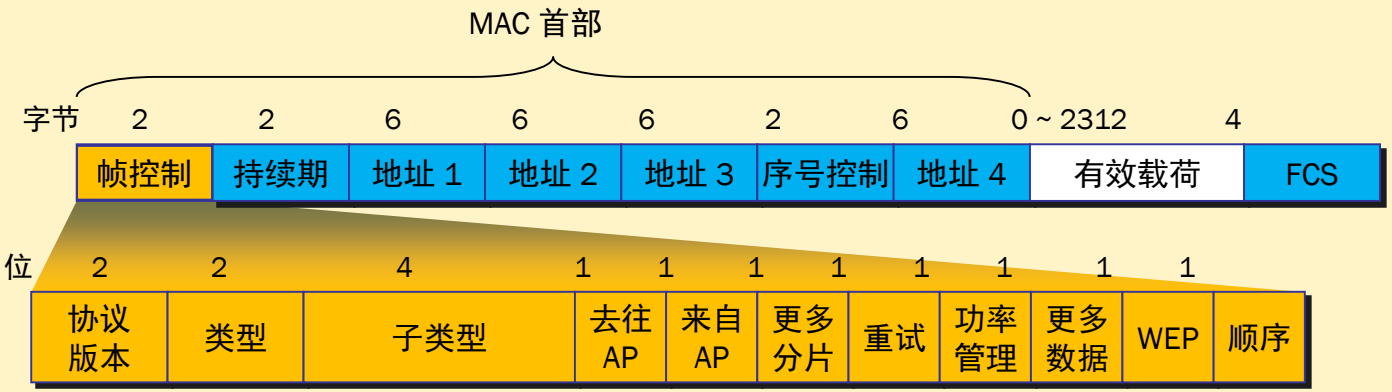


RTS 和 CTS 帧以及数据帧和 ACK 帧的传输时间关系



3.7.4 802.11局域网的MAC帧

- 802.11的MAC帧共有三种类型，即控制帧、数据帧和管理帧。



地址字段的四种使用情况

到DS	从DS	地址1	地址2	地址3	地址4
0	0	目的地址	源地址	BSSID	--
0	1	目的地址	发送AP地址	源地址	--
1	0	接收AP地址	源地址	目的地址	--
1	1	接收AP地址	发送AP地址	目的地址	源地址

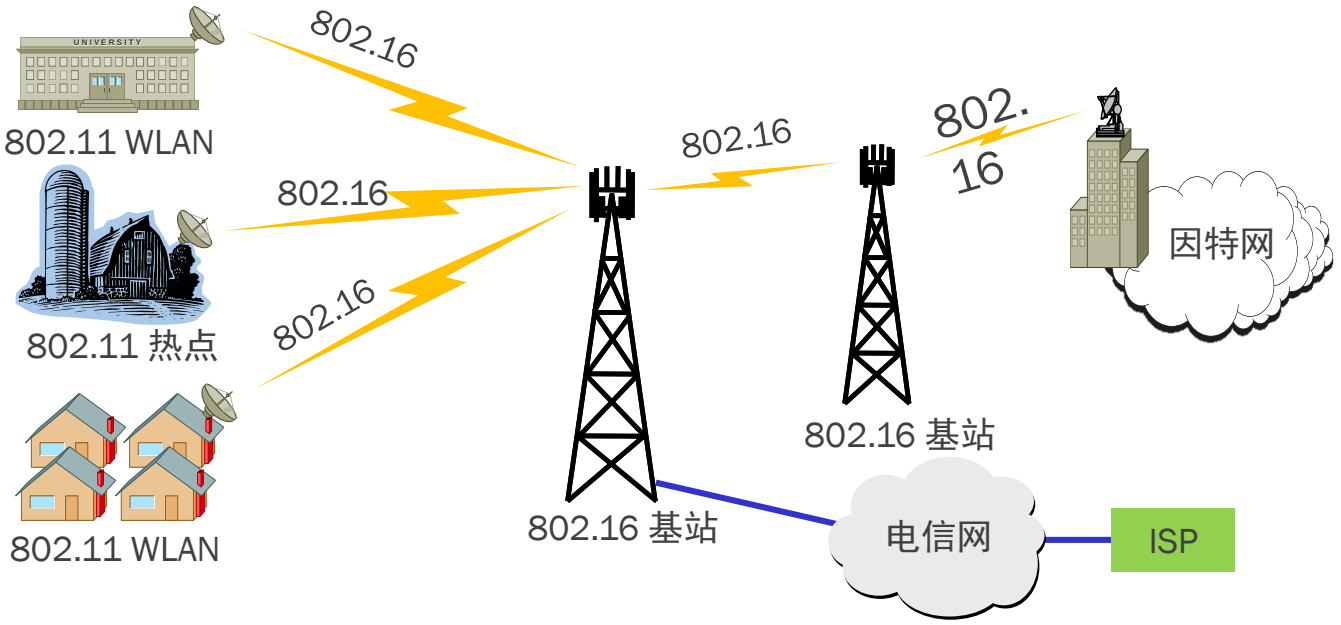
3.7.5 其他无线计算机网络

- (1) 无线个人区域网WPAN (Wireless Personal Area Network)
  - 在个人工作地方把属于个人使用的电子设备用无线技术连接起来自组网络，不需要使用接入点 AP。
  - 整个网络的范围大约在 10 m 左右。
  - 蓝牙 (Bluetooth) 系统（802.15）
  - 超宽带UWB (Ultra-Wide Band)（802.15.3）

3.7.5 其他无线计算机网络

- (2)无线城域网 WMAN(Wireless Metropolitan Area Network)
  - WMAN 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）。
  - 在许多情况下，无线城域网可用来代替现有的有线宽带接入，因此它有时又称为无线本地环路。
  - WiMAX(Worldwide Interoperability for Microwave Access)常用来表示无线城域网 WMAN。

802.16 无线城域网服务范围的示意图



谢谢！