

Chapter 3 data link layer

- [1. 数据链路层概述](#)

- [1.1. 数据链路层在网络体系结构中所处的地位](#)
- [1.2. 链路、数据链路和帧](#)
 - [1.2.1. 链路 \(Link\)](#)
 - [1.2.2. 数据链路 \(Data Link\)](#)
 - [1.2.3. 帧 \(Frame\)](#)

- [2. 数据链路层的三个重要问题](#)

- [2.1. 封装成帧和透明传输](#)
 - [2.1.1. 封装成帧](#)
 - [2.1.2. 透明传输](#)
 - [2.1.2.1. 字节填充](#)
 - [2.1.2.2. 比特填充](#)
- [2.2. 差错检测](#)
- [2.3. 误码的相关概念](#)
- [2.4. 奇偶校验](#)
- [2.5. 循环冗余校验](#)
 - [2.5.1. CPC基本思想](#)
 - [2.5.2. 发送方CRC操作](#)
 - [2.5.3. 接收方CRC操作](#)
 - [2.5.4. 生成多项式](#)
 - [2.5.5. CRC举例](#)
 - [2.5.6. 注意](#)
- [2.6. 可靠传输](#)
 - [2.6.1. 可靠传输的相关基本概念](#)
 - [2.6.1.1. 不可靠传输](#)
 - [2.6.1.2. 可靠传输](#)
 - [2.6.1.3. 传输差错](#)
 - [2.6.2. 停止-等待协议 \(Stop-and-Wait, SW\)](#)
 - [2.6.2.1. 实现原理](#)
 - [2.6.2.2. 信道利用率](#)
 - [2.6.3. 回退N帧协议 \(Go-back-N, GBN\)](#)
 - [2.6.4. 选择重传协议 \(Selective Repeat, SR\)](#)

- [3. 点对点协议](#)

- [3.1. 点对点协议PPP概述](#)
- [3.2. PPP的帧格式](#)
- [3.3. PPP帧的透明传输](#)
- [3.4. PPP帧的差错检测](#)
- [3.5. PPP的工作状态](#)

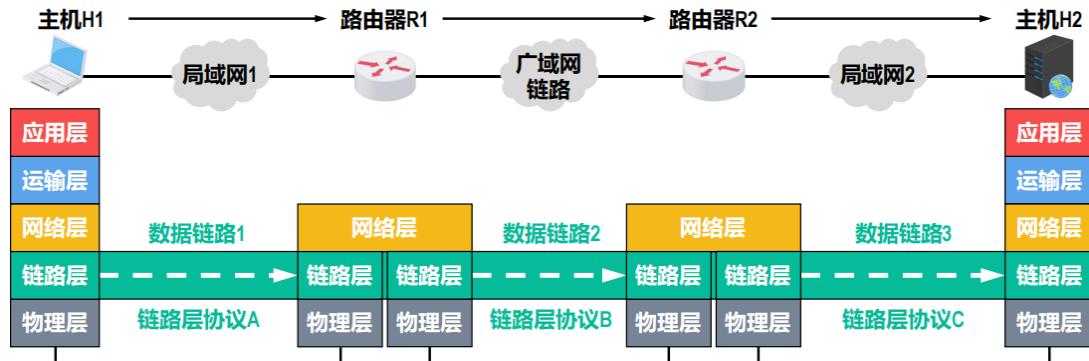
- [4. 共享式以太网](#)

- [4.1. 概述](#)
- [4.2. 网络适配器和MAC地址](#)
 - [4.2.1. 网络适配器](#)
 - [4.2.2. MAC地址](#)
 - [4.2.2.1. 概念](#)
 - [4.2.2.2. IEEE 802局域网的MAC地址格式](#)
 - [4.2.2.3. IEEE 802局域网的MAC地址发送顺序](#)
 - [4.2.2.4. 单播MAC地址举例](#)
 - [4.2.2.5. 广播MAC地址举例](#)
 - [4.2.2.6. 多播MAC地址举例](#)
- [4.3. CSMA/CD协议](#)
 - [4.3.1. CSMA/CD协议的基本原理](#)
 - [4.3.1.1. 多址接入 MA](#)
 - [4.3.1.2. 载波监听 CS](#)
 - [4.3.1.3. 碰撞检测CD](#)
 - [4.3.2. 共享式以太网的争用期](#)
 - [4.3.3. 共享式以太网的最小帧长和最大帧长](#)
 - [4.3.4. 共享式以太网的退避算法](#)
 - [4.3.4.1. 截断二进制指数退避](#)
 - [4.3.5. 共享式以太网的信道利用率](#)
- [4.4. 使用集线器的共享式以太网](#)
 - [4.4.1. 粗 \(->细\) 同轴电缆的共享总线以太网](#)
 - [4.4.2. 集线器](#)
 - [4.4.3. 对比](#)
 - [4.4.4. BASE-T星型以太网](#)
- [4.5. 在物理层扩展以太网](#)
 - [4.5.1. 扩展站点与集线器之间的距离](#)
 - [4.5.2. 扩展共享式以太网的覆盖范围和站点数量](#)
- [4.6. 在数据链路层扩展以太网](#)
 - [4.6.1. 使用网桥在数据链路层扩展以太网](#)
 - [4.6.2. 网桥的主要结构和基本工作原理](#)
 - [4.6.3. 透明网桥的自学习和转发帧的流程](#)
 - [4.6.4. 透明网桥的生成树协议STP](#)
- [5. 交换式以太网](#)
 - [5.1. 交换式以太网](#)
 - [5.2. 以太网交换机](#)
 - [5.3. 共享式以太网与交换式以太网的对比](#)
- [6. 以太网的MAC帧格式](#)
 - [6.1. 以太网V2的MAC帧](#)
- [7. 虚拟局域网](#)
 - [7.1. 虚拟局域网VLAN的诞生背景](#)
 - [7.1.1. 巨大的广播域会带来一系列问题](#)

- [7.1.2. 分割广播域的方法](#)
- [7.2. 虚拟局域网VLAN概述](#)
- [7.3. 虚拟局域网VLAN的实现机制 —— IEEE 802.1Q帧](#)
 - [7.3.1. IEEE 802.1Q帧](#)
 - [7.3.2. 以太网交换机的接口类型](#)
- [8. 以太网的发展](#)
 - [8.1. BASE-T以太网](#)
 - [8.2. 吉比特以太网](#)
 - [8.2.1. 简介](#)
 - [8.2.2. 载波延伸](#)
 - [8.2.3. 分组突发](#)
 - [8.2.4. 物理层标准](#)
 - [8.3. 吉比特以太网](#)
 - [8.3.1. 简介](#)
 - [8.3.2. 物理层标准](#)
 - [8.4. 吉比特/100吉比特以太网](#)
 - [8.4.1. 简介](#)
- [9. 无线局域网](#)
 - [9.1. 无线局域网的组成](#)
 - [9.1.1. 无线局域网分类](#)
 - [9.1.1.1. 有固定基础设施的](#)
 - [9.1.1.2. 无固定基础设施的](#)
 - [9.2. 无线局域网的物理层](#)
 - [9.2.1. 概述](#)
 - [9.2.2. 近年新的物理层标准](#)
 - [9.3. 无线局域网使用CSMA/CA协议的原因](#)
 - [9.3.1. 区别](#)
 - [9.3.2. 原因](#)
 - [9.4. CSMA/CA协议的基本工作原理](#)
 - [9.4.1. DIFS](#)
 - [9.4.2. 虚拟载波监听 \(Virtual Carrier Sense\) 机制](#)
 - [9.4.3. SIFS](#)
 - [9.4.4. 退避算法](#)
 - [9.4.4.1. 使用情况](#)
 - [9.4.4.2. 算法内容](#)
 - [9.4.4.3. 对信道进行预约](#)
 - [9.5. 无线局域网的MAC帧](#)
- [10. 题目](#)

1. 数据链路层概述

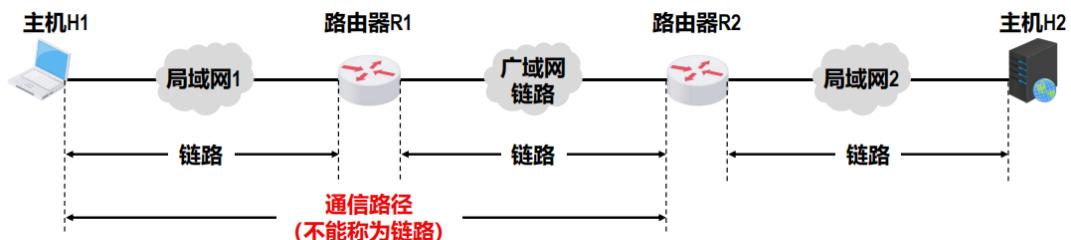
1.1. 数据链路层在网络体系结构中所处的地位



1.2. 链路、数据链路和帧

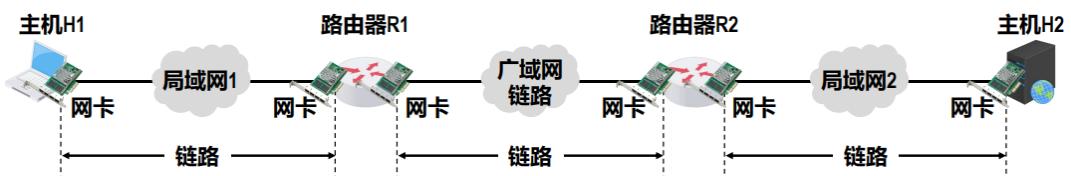
1.2.1. 链路 (Link)

- 指从一个节点到相邻节点的一段物理线路（有线或无线），而中间没有任何其他的交换节点。



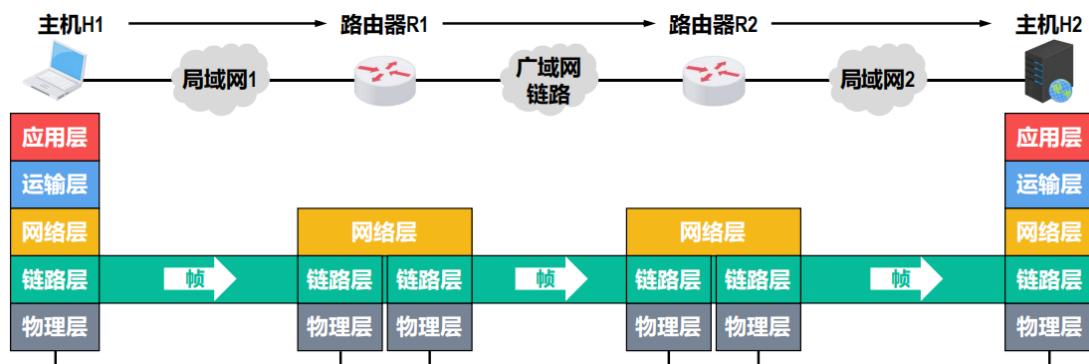
1.2.2. 数据链路 (Data Link)

- 数据链路是基于链路的。
- 当在一条链路上传送数据时，除需要链路本身，还需要一些必要的通信协议来控制这些数据的传输，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。
- 计算机中的网络适配器（俗称网卡）和其相应的软件驱动程序就实现了这些协议。
- 一般的网络适配器都包含了物理层和数据链路层这两层的功能。



1.2.3. 帧 (Frame)

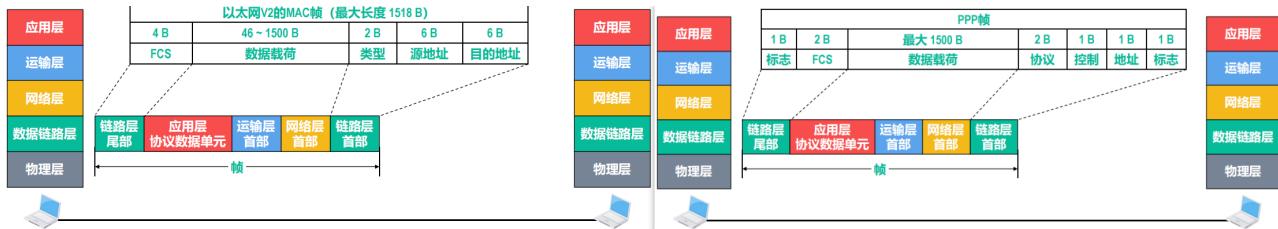
- 是数据链路层对等实体之间在水平方向进行逻辑通信的协议数据单元PDU。



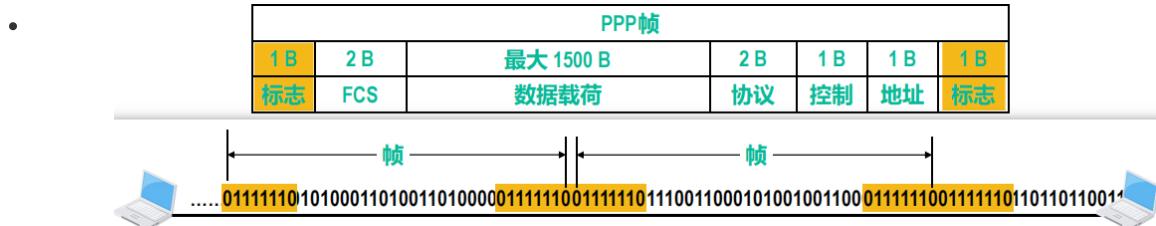
2. 数据链路层的三个重要问题

2.1. 封装成帧和透明传输

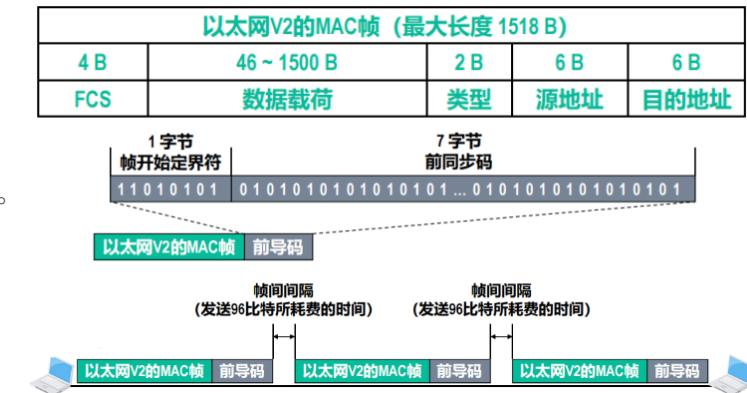
2.1.1. 封装成帧



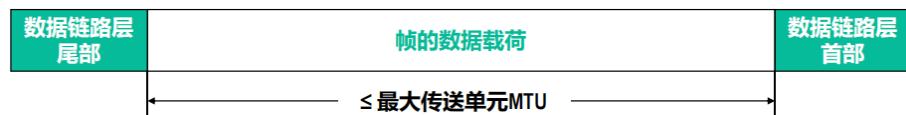
- 是指数据链路层给上层交付下来的协议数据单元PDU添加一个首部和一个尾部，使之成为帧。
 - 帧的首部和尾部中包含有一些重要的控制信息。
 - 帧首部和尾部的作用之一就是帧定界。
- 帧定界：接收端根据帧首部和帧尾部的标志字段，就可以从收到的比特流中识别出帧的开始和结束



- 并不是每一种数据链路层协议的帧都包含有帧定界标志。



- 为了提高数据链路层传输帧的效率，应当使帧的数据载荷的长度尽可能地大于首部和尾部的长度。
- 考虑到对缓存空间的需求以及差错控制等诸多因素，每一种数据链路层协议都规定了帧的数据载荷的长度上限，即最大传送单元 (Maximum Transfer Unit, MTU)。



- 例如，以太网的MTU为1500个字节。

2.1.2. 透明传输



- 透明传输：数据链路层对上层交付下来的协议数据单元PDU没有任何限制，就好像数据链路层不存在一样。

2.1.2.1. 字节填充

- 插入转义字符、帧定界符



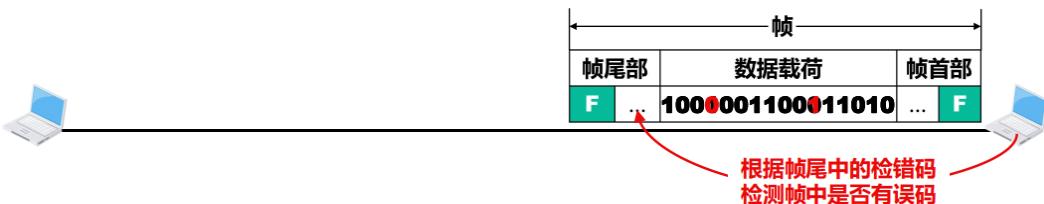
2.1.2.2. 比特填充

- 如每遇到5个连续的比特1，就再其后面插入一个比特0（HDLC协议）

2.2. 差错检测

2.3. 误码的相关概念

- 比特差错
 - 比特在传输过程中：比特1可能变成比特0；比特0可能变成比特1。
- 误码率（Bit Error Rate, BER）：传输错误的比特数量占所传输比特总数的比率
 - 提高链路的信噪比，可以降低误码率。
 - 在实际的通信链路上，不可能使误码率下降为零。



- 使用差错检测技术来检测数据在传输过程中是否产生了比特差错，是数据链路层所要解决的重要问题之一。
 - 帧在传输的过程中可能出现误码。
 - 接收方根据发送方添加在帧尾部中的检错码，可以检测出帧是否出现了误码。（采用与发送方相同的检错技术）
 - 帧检验序列（FCS）：帧尾部中用来存放检错码的字段

2.4. 奇偶校验

- 奇校验是在待发送的数据后面添加1个校验位，使得添加该校验位后的整个数据中比特1的个数为奇数。



- 偶校验是在待发送的数据后面添加1个校验位，使得添加该校验位后的整个数据中比特1的个数为偶数。



- 奇数误码可检出，偶数误码会漏检。
- 在实际使用时，奇偶校验又可分为垂直奇偶校验、水平奇偶校验以及水平垂直奇偶校验。

2.5. 循环冗余校验

- 数据链路层广泛使用漏检率极低的循环冗余校验（Cyclic Redundancy Check, CRC）检错技术。

2.5.1. CPC基本思想

- 收发双方约定好一个生成多项式 $G(X)$ 。
- 发送方基于待发送的数据和生成多项式 $G(X)$ ，计算出差错检测码（冗余码），将冗余码添加到待发送数据的后面一起传输。
- 接收方收到数据和冗余码后，通过生成多项式 $G(X)$ 来计算收到的数据和冗余码是否产生了误码。

2.5.2. 发送方CRC操作



2.5.3. 接收方CRC操作



2.5.4. 生成多项式

- 举例

【生成多项式举例】

$$\begin{aligned} G(X) &= X^4 + X^2 + X + 1 \\ &= \boxed{1} \cdot X^4 + \boxed{0} \cdot X^3 + \boxed{1} \cdot X^2 + \boxed{1} \cdot X^1 + \boxed{1} \cdot X^0 \end{aligned}$$

生成多项式各项系数构成的比特串: 10111 (计算冗余码时作为除数)

- 常用的生成多项式

【常用的生成多项式】

算法要求生成多项式必须包含最低次项

$$\begin{aligned} \text{CRC - 16} &= x^{16} + x^{15} + x^2 + \boxed{1} \\ \text{CRC - CCITT} &= x^{16} + x^{12} + x^5 + \boxed{1} \\ \text{CRC - 32} &= x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + \boxed{1} \end{aligned}$$

2.5.5. CRC举例

- 发送方

【CRC举例】待发送的数据为101001，生成多项式为 $G(X) = X^3 + X^2 + 1$ ，计算冗余码。



- 接收方

【CRC举例】接收到的信息为101101001，生成多项式为 $G(X) = X^3 + X^2 + 1$ ，判断传输是否误码？



2.5.6. 注意

- 奇偶校验、循环冗余校验等差错检测技术，只能检测出传输过程中出现了差错，但并不能定位错误，因此无法纠正错误。
- 要想纠正传输中的差错，可以使用冗余信息更多的纠错码（例如海明码）进行前向纠错。但纠错码的开销比较大，在计算机网络中较少使用。
- 在计算机网络中，通常采用我们后续课程中将要介绍的检错重传方式来纠正传输中的差错，或者仅仅丢弃检测到差错的帧，这取决于数据链路层向其上层提供的是可靠传输服务还是不可靠传输服务。
- 循环冗余校验CRC具有很好的检错能力（漏检率极低），虽然计算比较复杂，但非常易于用硬件实现，因此被广泛应用于数据链路层。

2.6. 可靠传输

2.6.1. 可靠传输的相关基本概念

2.6.1.1. 不可靠传输

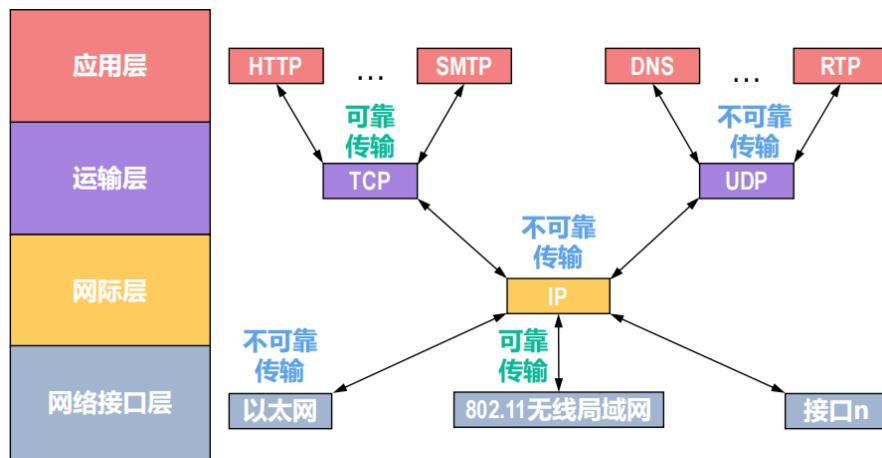
- 直接丢弃有误码的帧，其他什么也不做。

2.6.1.2. 可靠传输

- 通过某种机制实现，实现发送方发送什么，接收方最终都能正确收到。
- 有线链路的误码率比较低，并不要求数据链路层向其上层提供可靠传输服务。
- 无线链路易受干扰，误码率比较高，因此要求数据链路层必须向其上层提供可靠传输服务。

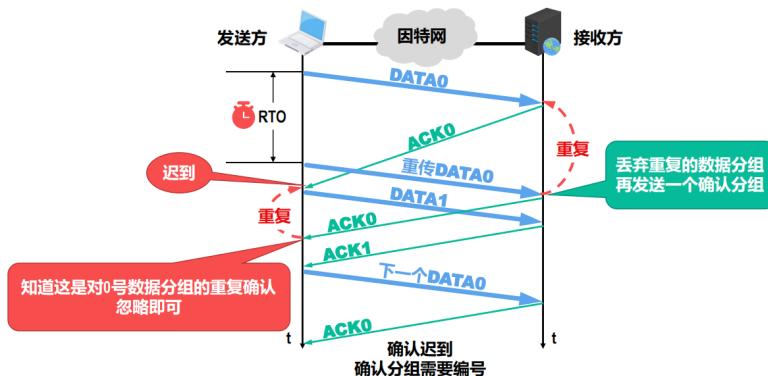
2.6.1.3. 传输差错

- 数据链路层及其下层
 - 误码（比特差错）
- 数据链路层的上层
 - 分组丢失
 - 分组失序
 - 分组重复
- 可靠传输服务并不局限于数据链路层，其他各层均可选择实现可靠传输。
- 可靠传输的实现比较复杂，开销比较大，是否使用可靠传输取决于应用需求。



2.6.2. 停止-等待协议 (Stop-and-Wait, SW)

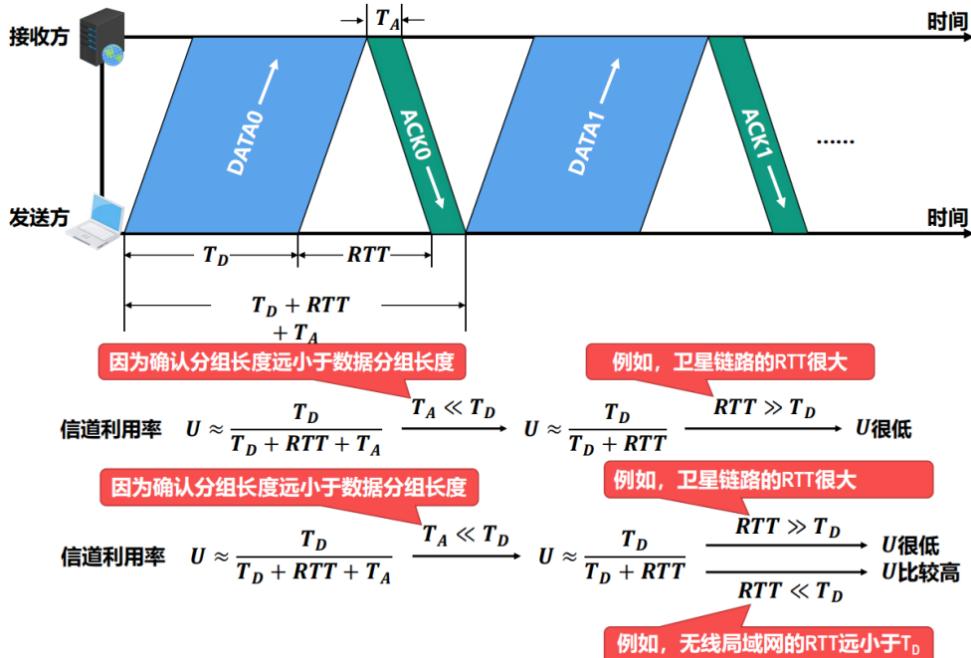
2.6.2.1. 实现原理



- 确认、否认和重传
 - 使用超时重传机制后，就可以不使用否认机制了，这样可使协议实现起来更加简单。但是，如果点对点链路的误码率较高，使用否认机制可以使发送方在超时计时器超时前就尽快重传。
 - 超时重传时间 (Retransmission Time-Out, RTO)：一般将RTO设置为略大于收发双方的平均往返时间RTT
 - 在数据链路层，点对点的往返时间RTT比较固定，RTO就比较好设定。
 - 在运输层，由于端到端往返时间非常不确定，设置合适的超时重传时间RTO有时并不容易。
- 分组编号 (数据分组+确认分组)

- 只需1个比特编序号即可，即序号0和序号1。
- 数据链路层一般不会出现确认分组迟到的情况，因此在数据链路层实现停止-等待协议可以不用给确认分组编号。
- 停止-等待协议属于自动请求重传（Automatic Repeat reQuest，ARQ）协议。即重传的请求是发送方自动进行的，而不是接收方请求发送方重传某个误码的数据分组。

2.6.2.2. 信道利用率



- 若出现超时重传，对于传送有用的数据信息来说，信道利用率还要降低。
- 在往返时间RTT相对较大的情况下，为了提高信道利用率，收发双方不适合采用停止-等待协议，而可以选择使用回退N帧（GBN）协议或选择重传（SR）协议。

2.6.3. 回退N帧协议（Go-back-N，GBN）

发送方	接收方
<ul style="list-style-type: none"> ■ 发送窗口W_T的取值范围是$1 < W_T \leq (2^n - 1)$，其中，n是构成分组序号的比特数量。 <ul style="list-style-type: none"> □ 如果$W_T = 1$ 变成了停止-等待协议 □ 如果$W_T > (2^n - 1)$ 接收方无法分辨新旧数据分组 ■ 可在未收到接收方确认分组的情况下，将序号落入发送窗口内的多个数据分组全部发送出去。 ■ 只有收到对已发送数据分组的确认分组时，发送窗口才能向前滑动到相应位置。 ■ 收到多个重复确认时，可在重传计时器超时前尽早开始重传，由具体实现决定。 ■ 发送窗口内某个已发送的数据分组产生超时重传时，发送窗口内该数据分组的后续已发送的数据分组也必须全部重传，这就是回退N帧（Go-back-N，GBN）协议名称的由来。 	<ul style="list-style-type: none"> ■ 接收窗口$W_R = 1$的，因此只能按序接收数据分组。 ■ 只接收序号落入接收窗口内且无误码的数据分组，并且将接收窗口向前滑动一个位置，与此同时给发送方发送相应的确认分组。 ■ 为了减少开销，接收方不必每收到一个按序到达且无误码的数据分组就给发送方发送一个相应的确认分组。 <ul style="list-style-type: none"> □ 可以在连续收到多个按序到达且无误码的数据分组后（数量由具体实现决定），才针对最后一个数据分组发送确认分组，这称为累积确认。 □ 或者可以在自己有数据分组要发送时才对之前按序接收且无误码的数据分组进行捎带确认。 ■ 接收方收到未按序到达的数据分组后，除丢弃外，还可对之前最后一个按序到达的数据分组进行重复确认，以便发送方尽快重传。

回退N帧协议在流水线传输的基础上，利用发送窗口来限制发送方连续发送数据分组的数量，是一种连续ARQ协议。
 在回退N帧协议的工作过程中，发送窗口和接收窗口不断向前滑动，因此这类协议又称为滑动窗口协议。
 在信道质量较差（容易出现误码）的情况下，回退N帧协议的信道利用率并不比停止-等待协议的信道利用率高。

2.6.4. 选择重传协议（Selective Repeat，SR）

用 $n(n > 1)$ 个比特给分组编号，发送窗口 W_T 与接收窗口 W_R 的关系如下：

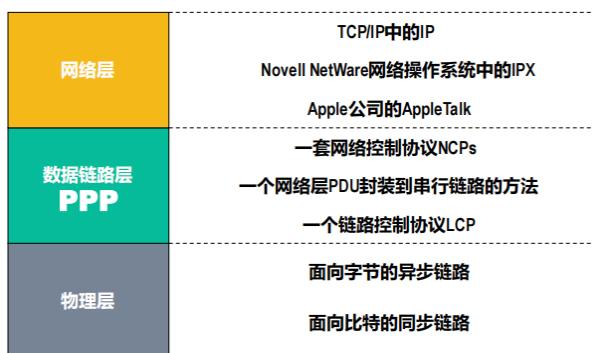
W_R 超过 W_T 没有意义 确保接收窗口向前滑动后，落入接收窗口内的新序号与之前的旧序号没有重叠，避免无法分辨新旧数据分组。	$\left. \begin{array}{l} 1 < W_R \leq W_T \\ W_T + W_R \leq 2^n \end{array} \right\} 1 < W_R \leq 2^{(n-1)}$	当 W_R 取最大值 $2^{(n-1)}$ 时， W_T 能取到的最大值也为 $2^{(n-1)}$ 。
---	--	--

发送方	接收方
<ul style="list-style-type: none"> ■ 可在未收到接收方确认分组的情况下，将序号落入发送窗口内的多个数据分组全部发送出去。 ■ 只有按序收到对已发送数据分组的确认分组时，发送窗口才能向前滑动到相应位置。 ■ 如果收到未按序到达的确认分组，应对其进行记录，以防止其相应数据分组的超时重发，但发送窗口不能向前滑动。 	<ul style="list-style-type: none"> ■ 可接收未按序到达但没有误码并且序号落入接收窗口内的数据分组。 ■ 为了使发送方仅重传出现差错的分组，接收方不再采用累积确认，而需要对每一个正确接收到的数据分组进行逐一确认。 ■ 只有在按序接收数据分组后，接收窗口才能向前滑动到相应位置。

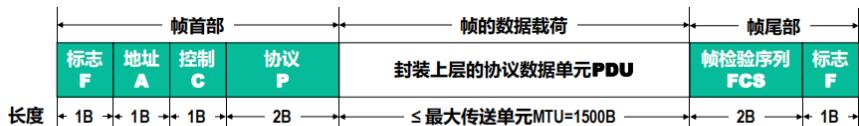
3. 点对点协议

3.1. 点对点协议PPP概述

- 点对点协议（Point-to-Point Protocol，PPP）是目前使用最广泛的点对点数据链路层协议。
- 点对点协议PPP是因特网工程任务组（Internet Engineering Task Force，IETF）于1992年制定的。经过多次修订，目前PPP已成为因特网的正式标准[RFC1661，RFC1662]。
- 应用
 - 用户接入因特网，用户计算机与ISP通信。
 - 广泛应用于广域网路由器之间的专用线路。
- 从网络体系结构的角度看点对点协议PPP的组成



3.2. PPP的帧格式



标志（Flag）字段：PPP帧的定界符，取值为0x7E。

地址（Address）字段：取值为0xFF，预留（目前没有什么作用）。

控制（Control）字段：取值为0x03，预留（目前没有什么作用）。

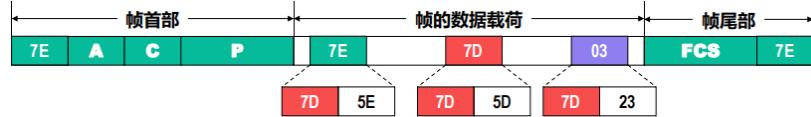
协议（Protocol）字段：其值用来指明帧的数据载荷应向上交付给哪个协议处理。

7E	FF	03	0021	IP数据报	FCS	7E
7E	FF	03	C021	LCP分组	FCS	7E
7E	FF	03	8021	NCP分组	FCS	7E

帧检验序列（Frame Check Sequence，FCS）字段：其值是使用循环冗余校验CRC计算出的检错码。

3.3. PPP帧的透明传输

- 面向字节的异步链路使用字节填充来实现透明传输[RFC1662]



发送方的处理：

- (1) 将数据载荷中出现的每一个`0x7E`减去`0x20`（相当于异或`0x20`），然后在其前面插入转义字符`0x7D`。
 - (2) 若数据载荷中原来就含有`0x7D`，则把每一个`0x7D`减去`0x20`，然后在其前面插入转义字符`0x7D`。
 - (3) 将数据载荷中出现的每一个`ASCII码控制字符`（即数值小于`0x20`的字符），加上`0x20`（相当于异或`0x20`，将其转换成非控制字符），然后在其前面插入转义字符`0x7D`。

接收方的处理：

进行与发送方相反的变换，就可以正确地恢复出未经过字节填充的原始数据载荷。

- 面向比特的同步链路使用零比特填充来实现透明传输



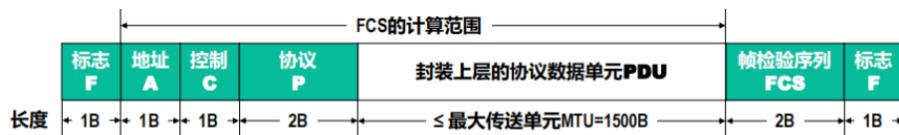
发送方的处理：

对帧的数据载荷进行扫描（一般由硬件完成），每出现5个连续的比特1，则在其后填充一个比特0。

接收方的处理：

对帧的数据载荷进行扫描，每出现5个连续的比特1时，就把其后的一个比特0删除。

3.4. PPP帧的差错检测



帧检验序列FCS字段：其值是使用循环冗余校验CRC计算出的检错码。

CRC采用的生成多项式为 $CRC - CCITT = X^{16} + X^{12} + X^5 + 1$

[RFC1662]文档的附录部分给出了FCS的计算方法的C语言实现（查表法）

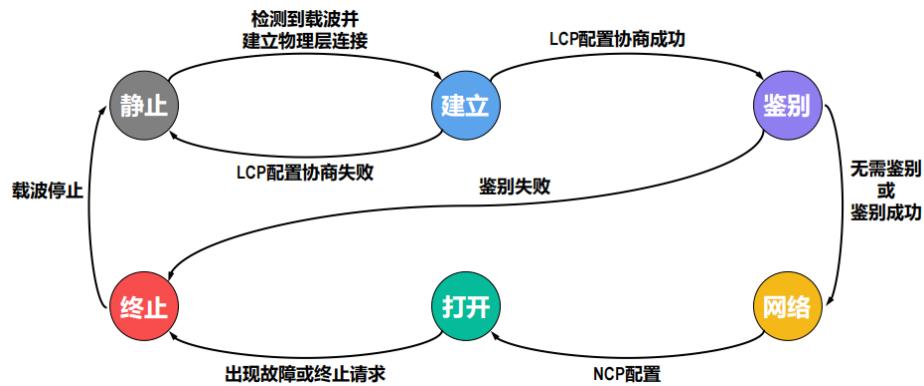
```
 1  // FFC.hxx - FFC in HLLC.hx
 2
 3  #include "datatracker.h"
 4
 5  //-----+
 6  // Datatracker
 7
 8  //-----+
 9  // C.2 FFC Computation Method
10
11  The following code provides a table lookup computation for
12  calculating the Frame Check Sequence as data arrives at the
13  interface. This implementation is based on [7], [8], and [9].
14
15  /* w65 represents an unsigned 16-bit number. Adjust the typedef for
16  * your hardware.
17  */
18  typedef unsigned short u16;
19
20  /* FFC lookup table as calculated by the table generator.
21  */
22
23  static u16 ffcTab[256];
24
25  /*-----+
26  //-----+
27  //-----+
28  //-----+
29  //-----+
30  //-----+
31  //-----+
32  //-----+
33  //-----+
34  //-----+
35  //-----+
36  //-----+
37  //-----+
38  //-----+
39  //-----+
40  //-----+
41  //-----+
42  //-----+
43  //-----+
44  //-----+
45  //-----+
46  //-----+
47  //-----+
48  //-----+
49  //-----+
50  //-----+
51  //-----+
52  //-----+
53  //-----+
54  //-----+
55  //-----+
56  //-----+
57  //-----+
58  //-----+
59  //-----+
60  //-----+
61  //-----+
62  //-----+
63  //-----+
64  //-----+
65  //-----+
66  //-----+
67  //-----+
68  //-----+
69  //-----+
70  //-----+
71  //-----+
72  //-----+
73  //-----+
74  //-----+
75  //-----+
76  //-----+
77  //-----+
78  //-----+
79  //-----+
80  //-----+
81  //-----+
82  //-----+
83  //-----+
84  //-----+
85  //-----+
86  //-----+
87  //-----+
88  //-----+
89  //-----+
90  //-----+
91  //-----+
92  //-----+
93  //-----+
94  //-----+
```

接收方每收到一个PPP帧，就进行CRC检验。若CRC检验正确，就收下这个帧；否则，就丢弃这个帧。

使用PPP的数据链路层，向上提供的是不可靠数据传输服务。

3.5. PPP的工作状态

- 以用户主机拨号接入因特网服务提供者ISP的拨号服务器的过程为例



4. 共享式以太网

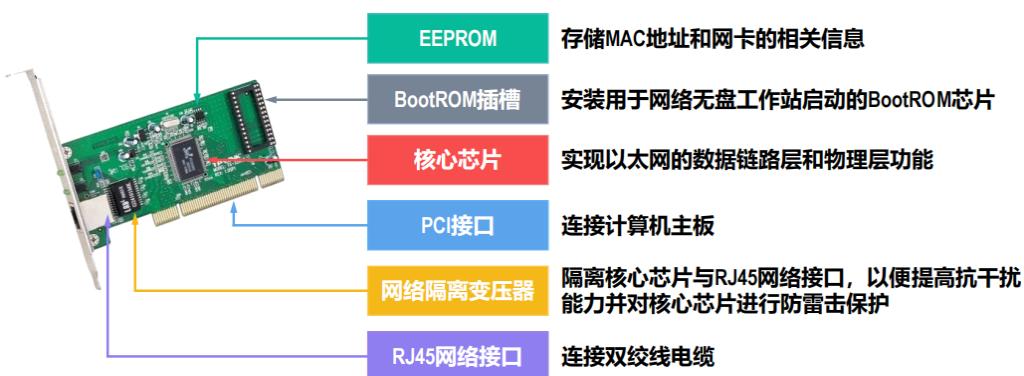
4.1. 概述

- 以太网（Ethernet）以曾经被假想的电磁波传播介质——以太（Ether）来命名。
- 以太网最初采用无源电缆（不包含电源线）作为共享总线来传输帧，属于基带总线局域网，传输速率为2.94Mb/s。
- 发展
 - 1975 以太网诞生
 - 1976 以太网里程碑论文
 - 1979 3Com公司成立
 - 1980 以太网标准V1
 - 1982 以太网标准V2
 - 1983 IEEE以太网标准
- 以太网目前已经从传统的共享式以太网发展到交换式以太网，传输速率已经从10Mb/s提高到100Mb/s、1Gb/s甚至10Gb/s。

4.2. 网络适配器和MAC地址

4.2.1. 网络适配器

- 网络适配器（Adapter）（一般简称为“网卡”）：将计算机连接到以太网。



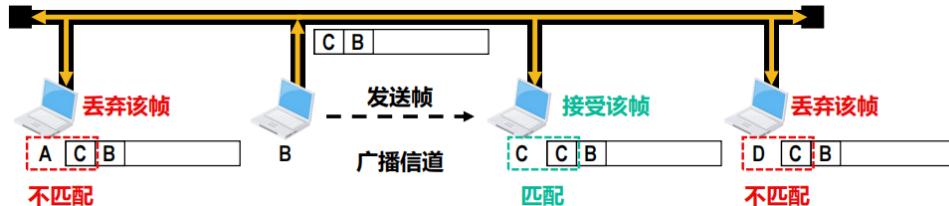
- 在计算机内部，网卡与CPU之间的通信，一般是通过计算机主板上的I/O总线以并行传输方式进行
- 网卡与外部以太网（局域网）之间的通信，一般是通过传输媒体（同轴电缆、双绞线电缆、光纤）以串行方式进行的。
- 网卡除要实现物理层和数据链路层功能，其另外一个重要功能就是要进行并行传输和串行传输的转换。由于网络的传输速率和计算机内部总线上的传输速率并不相同，因此在网卡的核心芯片中都会包含用于缓存数据的存储器。

- 在确保网卡硬件正确的情况下，为了使网卡正常工作，还必须要在计算机的操作系统中为网卡安装相应的设备驱动程序。驱动程序负责驱动网卡发送和接收帧。

4.2.2. MAC地址

4.2.2.1. 概念

- 当多个主机连接在同一个广播信道上，要想实现两个主机之间的通信，则每个主机都必须有一个唯一的标识，即一个数据链路层地址。
- MAC地址：用于媒体接入控制（Medium Access Control, MAC）；每个主机发送的帧的首部中，携带有发送主机（源主机）和接收主机（目的主机）的数据链路层地址。



- MAC地址一般被固化在网卡的电可擦可编程只读存储器EEPROM中，因此MAC地址也被称为硬件地址。
- MAC地址有时也被称为物理地址。
- 普通用户计算机中往往会包含两块网卡
 - 用于接入有线局域网的以太网卡
 - 用于接入无线局域网的Wi-Fi网卡
- 每块网卡都有一个全球唯一的MAC地址。
- MAC地址是对网络上各接口的唯一标识，而不是对网络上各设备的唯一标识。

4.2.2.2. IEEE 802局域网的MAC地址格式



第1字节		第2~5字节					第6字节									
b7	b6	b5	b4	b3	b2	b1	b0	b7	b6	b5	b4	b3	b2	b1	b0
G/L (Global/Local)		I/G (Individual/Group)					I/G =0: 单播地址					I/G =1: 多播地址				
G/L=0: 全球管理		I/G =0: 单播地址					I/G =1: 多播地址									
G/L=1: 本地管理																

第1字节的b1位	第1字节的b0位	MAC地址类型	地址占比	地址数量
0	0	全球单播 (由厂商生产网络设备时固化在设备中)	1/4	2^{48} ≈ 280 万亿
	1	全球多播 (交换机、路由器等标准网络设备所支持的多播地址)	1/4	
1	0	本地单播 (由网络管理员分配, 优先级高于网络接口的全球单播地址)	1/4	
	1	本地多播 (可由用户对网卡编程实现, 以表明其属于哪些多播组)	1/4	

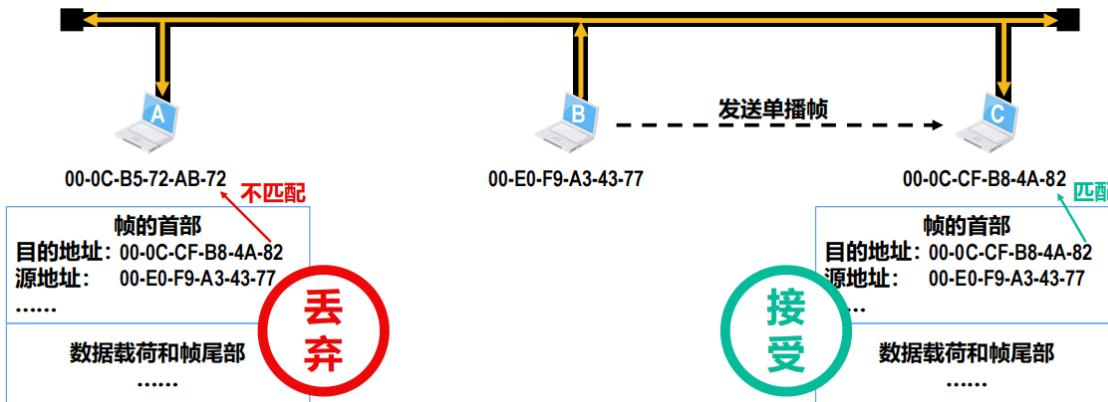
4.2.2.3. IEEE 802局域网的MAC地址发送顺序



字节发送顺序: 第1字节 ——> 第6字节

字节内的比特发送顺序: b0 ——> b7

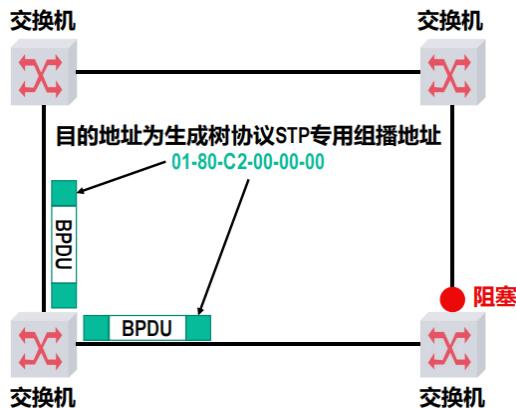
4.2.2.4. 单播MAC地址举例



4.2.2.5. 广播MAC地址举例



4.2.2.6. 多播MAC地址举例



- 网卡从网络上每收到一个帧，就检查帧首部中的目的MAC地址，按以下情况处理：
 - (1) 如果目的MAC地址是广播地址 (FF-FF-FF-FF-FF-FF)，则接受该帧。
 - (2) 如果目的MAC地址与网卡上固化的全球单播MAC地址相同，则接受该帧。
 - (3) 如果目的MAC地址是网卡支持的多播地址，则接受该帧。
 - (4) 除上述 (1)、(2) 和 (3) 情况外，丢弃该帧。
- 网卡还可被设置为一种特殊的工作方式：混杂方式（Promiscuous Mode）。工作在混杂方式的网卡，只要收到共享媒体上传来的帧就会收下，而不管帧的目的MAC地址是什么。
 - 对于网络维护和管理人员，这种方式可以监视和分析局域网上的流量，以便找出提高网络性能的具体措施。
 - 嗅探器（Sniffer）就是一种工作在混杂方式的网卡，再配合相应的工具软件（WireShark），就可以作为一种非常有用的网络工具来学习和分析网络。
 - 混杂方式就像一把“双刃剑”，黑客常利用这种方式非法获取网络用户的口令。

全球单播MAC地址就如同身份证上的身份证号码，具有唯一性，它往往与用户个人信息绑定在一起。因此，用户应尽量确保自己拥有的全球单播MAC地址不被泄露。

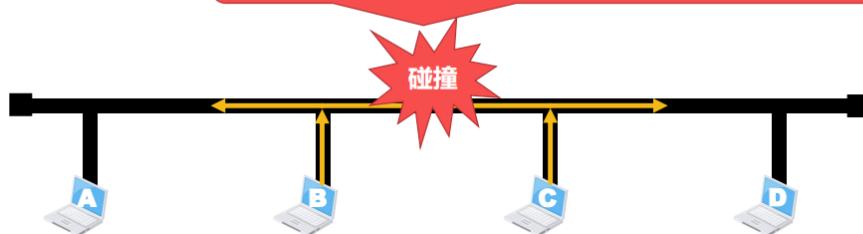
为了避免用户设备连接Wi-Fi热点时MAC地址泄露的安全问题，目前大多数移动设备都已经采用了随机MAC地址技术。

4.3. CSMA/CD协议

4.3.1. CSMA/CD协议的基本原理

- 为了解决各站点争用总线的问题，共享总线以太网使用了一种专用协议CSMA/CD，它是载波监听多址接入/碰撞检测（Carrier Sense Multiple Access Collision Detection）的英文缩写词。

共享总线以太网的一个重要问题：如何协调总线上的各站点争用总线。



- 载波监听检测到总线空闲，但总线并不一定空闲。
- 使用CSMA/CD协议的共享总线以太网上的各站点，只是尽量避免碰撞并在出现碰撞时做出退避后重发的处理，但不能完全避免碰撞。

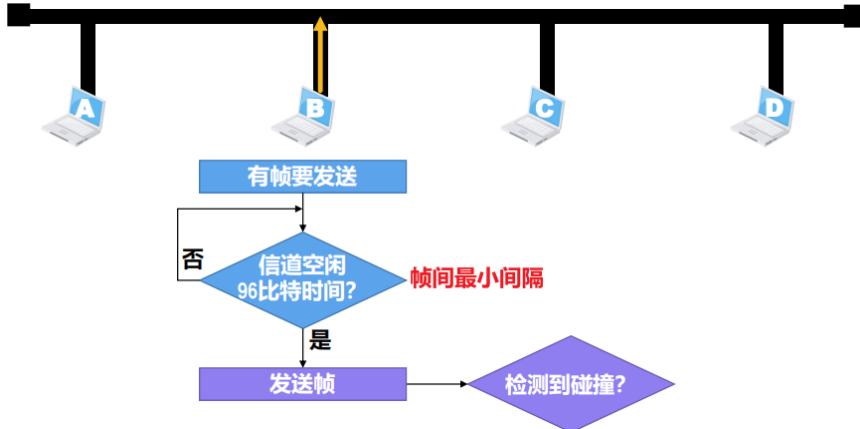
- 在使用CSMA/CD协议时，由于正在发送帧的站点必须“边发送帧边检测碰撞”，因此站点不可能同时进行发送和接收，也就是不可能进行全双工通信，而只能进行半双工通信（双向交替通信）。

4.3.1.1. 多址接入 MA

- 多个站点连接在一条总线上，竞争使用总线。

4.3.1.2. 载波监听 CS

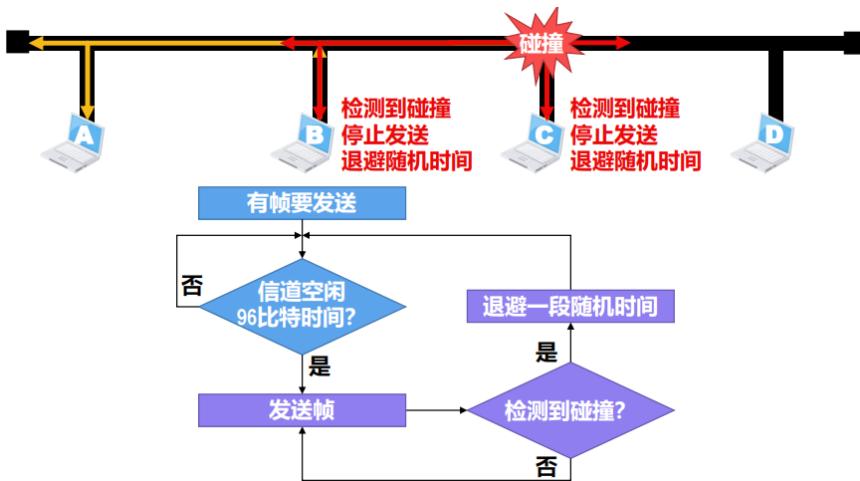
- 每个站点在发送帧之前，先要检测一下总线上是否有其他站点在发送帧（“先听后说”）



4.3.1.3. 碰撞检测 CD

- 每个正在发送帧的站点边发送边检测碰撞（“边说边听”）

- 一旦冲突，立即停说，等待时机，重新再说

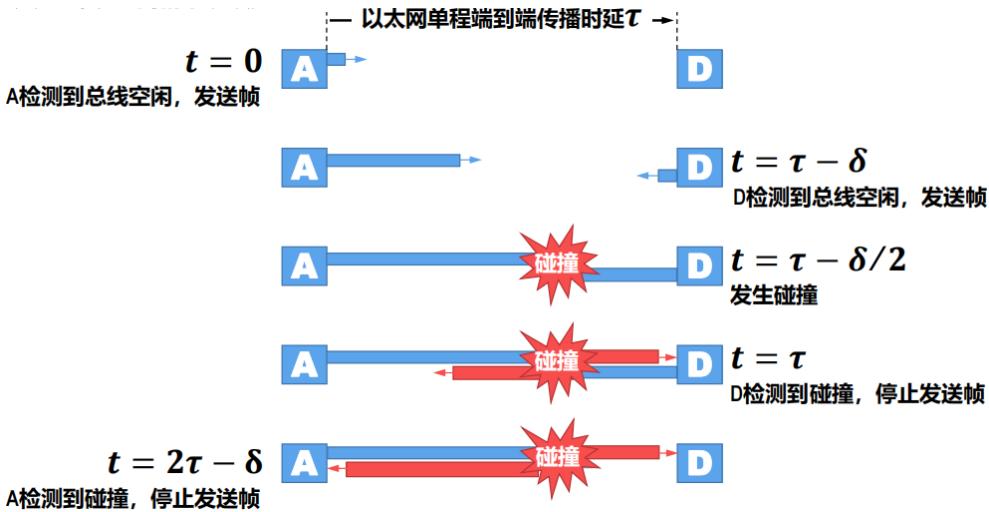


- 强化碰撞

- 发送帧的站点一旦检测到碰撞，除了立即停止发送帧外，还要再继续发送32比特或48比特的人为干扰信号（Jamming Signal），以便有足够的碰撞信号使所有站点都能检测出碰撞。

4.3.2. 共享式以太网的争用期

- 共享总线以太网的端到端往返时间 2τ 被称为争用期（Contention Period）或碰撞窗口（Collision Window）
- 站点从发送帧开始，最多经过时长 2τ （即 $\delta \rightarrow 0$ ）就可检测出所发送的帧是否遭遇了碰撞。



- 从争用期的概念可以看出，共享总线以太网上的每一个站点从发送帧开始，到之后的一小段时间内，都有可能遭遇碰撞，而这一小段时间的长短是不确定的，它取决于另一个发送帧的站点与本站点的距离，但不会超过总线的端到端往返传播时延，即一个争用期 2τ 。
 - 总线的长度越长（单程端到端传播时延越大），网络中站点数量越多，发生碰撞的概率就越大。
 - 共享以太网的总线长度不能太长，接入的站点数量也不能太多。

4.3.3. 共享式以太网的最小帧长和最大帧长

- 最小帧长 = 数据传输速率 * 争用期 2τ
 - 为了确保共享总线以太网上的每一个站点在发送完一个完整的帧之前，能够检测出是否产生了碰撞，帧的发送时延就不能少于共享总线以太网端到端的往返时间，即一个争用期 2τ 。
 - 对于10mb/s的共享总线以太网，其争用期 2τ 的值规定51.2μs，因此其最小帧长为512b，即64B。

■ 10Mb/s共享总线以太网（传统以太网）规定：争用期 2τ 的值为512比特的发送时间，即51.2μs。

$$\text{争用期 } 2\tau = \frac{512 \text{ b}}{10 \text{ Mb/s}} = \frac{512 \text{ b}}{10 \times 10^6 \text{ b/s}} = 51.2 \mu\text{s}$$

除考虑了信号传播时延外，还考虑到网络中可能存在转发器所带来的时延以及产生碰撞时继续发送32比特或48比特人为干扰信号所持续的时间等。

$$\text{单程端到端传播时延 } \tau = \frac{51.2 \mu\text{s}}{2} = 25.6 \mu\text{s}$$

假设信号的传播速率为 $2 \times 10^8 \text{ m/s}$

$$\text{则总线长度为 } 2 \times 10^8 \text{ m/s} \times 25.6 \mu\text{s} = 5120 \text{ m}$$

共享总线以太网规定：
总线长度不能超过2500m。

$$10 \text{ Mb/s} \times 51.2 \mu\text{s} = 512 \text{ b} = 64 \text{ B}$$

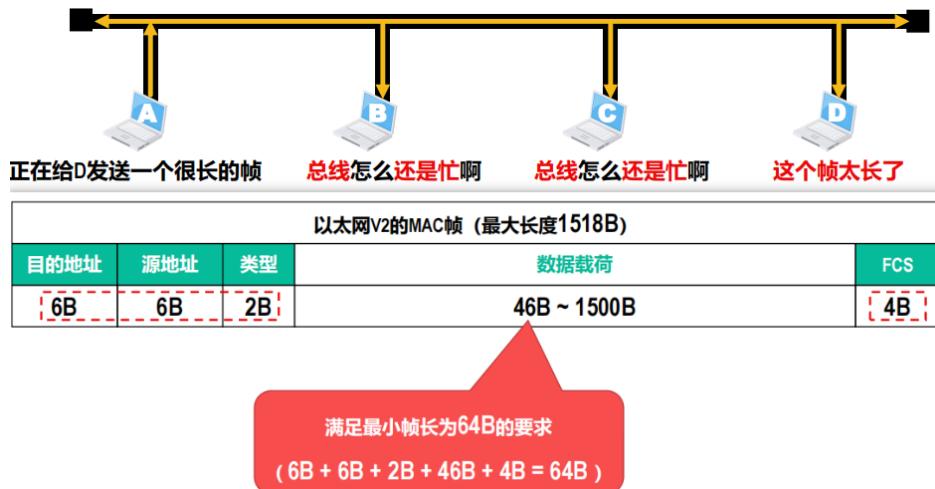
- 当某个站点在发送帧时，如果帧的前64B没有遭遇碰撞，那么帧的后续部分也就不会遭遇碰撞。也就是说，如果遭遇碰撞，就一定是在帧的前64B之内。
- 由于发送帧的站点边发送帧边检测碰撞，一旦检测到碰撞就立即中止帧的发送，此时已发送的数据量一定小于64B。因此，接收站点收到长度小于64B的帧，就可判定这是一个遭遇了碰撞而异常中止的无效帧，将其丢弃即可。

• 最大帧长

- 一般来说，帧的数据载荷的长度应远大于帧首部和尾部的总长度，这样可以提高帧的传输效率。

首部	帧的数据载荷	尾部
----	--------	----

- 然而，如果不限制数据载荷的长度上限，就可能使得帧的长度太长，这会带来一些问题。



4.3.4. 共享式以太网的退避算法

- 在使用CSMA/CD协议的共享总线以太网中，正在发送帧的站点一边发送帧一边检测碰撞，当检测到碰撞时就立即停止发送，**退避一段随机时间**后再重新发送。

4.3.4.1. 截断二进制指数退避

- 共享总线以太网中的各站点采用截断二进制指数退避 (Truncated Binary Exponential Backoff) 算法来选择退避的随机时间。

$$\text{退避时间} = \text{基本退避时间} \times \text{随机数 } r$$

基本退避时间

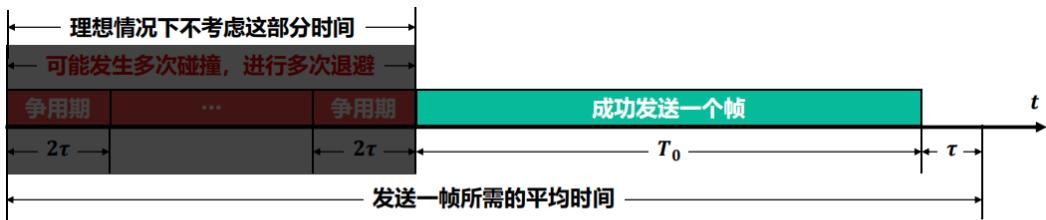
争用期 2τ

随机数 r
 r 从离散的整数集合 $\{0, 1, \dots, (2^k - 1)\}$ 中随机选出一个数， $k = \min[\text{重传次数}, 10]$

重传次数	k	离散的整数集合 $\{0, 1, \dots, (2^k - 1)\}$	可能的退避时间
1	1	{0, 1}	$0 \times 2\tau, 1 \times 2\tau$
2	2	{0, 1, 2, 3}	$0 \times 2\tau, 1 \times 2\tau, 2 \times 2\tau, 3 \times 2\tau$
12	10	{0, 1, 2, 3, 4, 5, ..., 1023}	$0 \times 2\tau, 1 \times 2\tau, 2 \times 2\tau, \dots, 1023 \times 2\tau$

- 如果连续多次发送碰撞，就表明可能有较多的站点参与竞争信道。但使用上述退避算法可使重传需要推迟的平均时间随重传次数而增大（即动态退避），因而减小产生碰撞的概率。
- 当重传达16次仍不能成功时，就表明同时打算发送帧的站点太多，以至于连续产生碰撞，此时应放弃重传并向高层报告。

4.3.5. 共享式以太网的信道利用率



■ 考虑以下这种理想情况：

- 总线一旦空闲就有某个站点立即发送帧
- 各站点发送帧都不会产生碰撞
- 发送一帧占用总线的时间为 $T_0 + \tau$ ，而帧本身的发送时间是 T_0

$$\text{极限信道利用率 } S_{max} = \frac{T_0}{T_0 + \tau} = \frac{1}{1 + \frac{\tau}{T_0}} = \frac{1}{1 + a}$$

$$\text{极限信道利用率 } S_{max} = \frac{T_0}{T_0 + \tau} = \frac{1}{1 + \frac{\tau}{T_0}} = \frac{1}{1 + a}$$

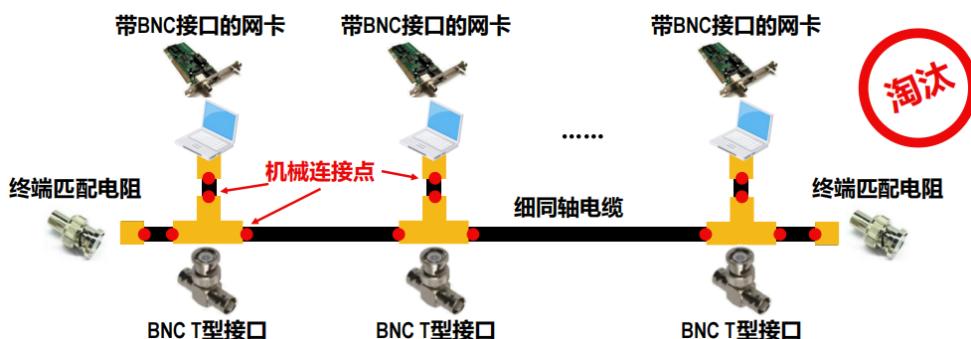
参数a的值应尽量小，以提高信道利用率

$$a = \frac{\tau}{T_0}$$

共享总线以太网端到端的距离不应太长
帧的长度应尽量大

4.4. 使用集线器的共享式以太网

4.4.1. 粗 (->细) 同轴电缆的共享总线以太网

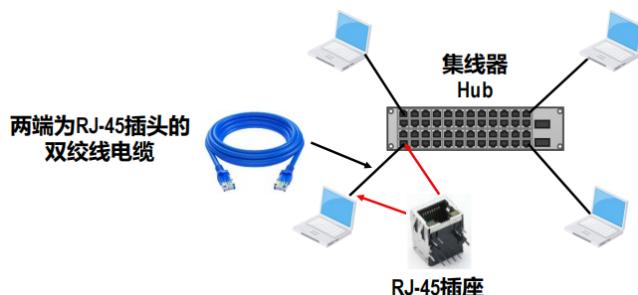


- 若总线上的某个机械连接点接触不良或断开，则整个网络通信就不稳定或彻底断网。

4.4.2. 集线器

- 集线器 (Hub) :

- 使用大规模集成电路来替代总线，并且可靠性非常高的设备。
- 站点连接到集线器的传输媒体也转而使用更便宜、更灵活的双绞线电缆。

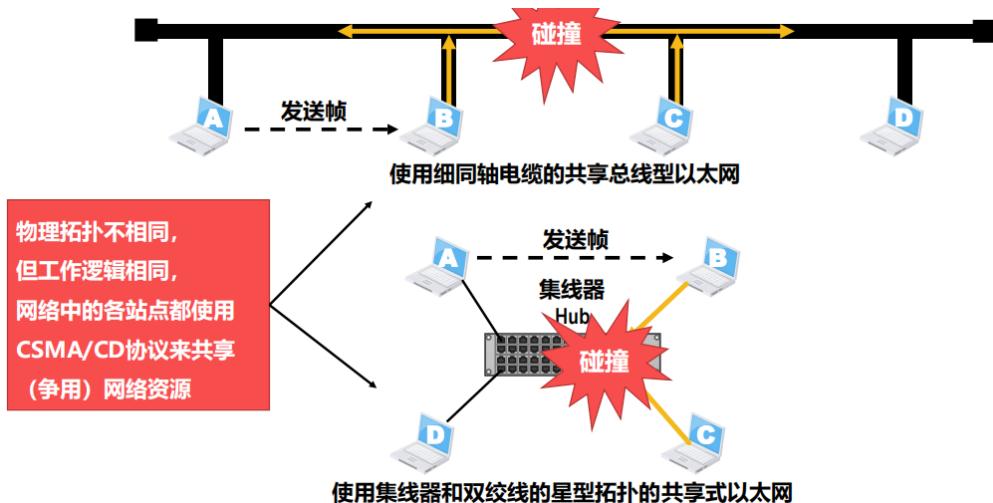


- 特点

- 物理拓扑是星型的，但在逻辑上仍然是一个总线网。总线上的各站点共享总线资源，使用的还是 CSMA/CD 协议。
- 只工作在物理层，仅简单地转发比特，并不进行碰撞检测。碰撞检测的任务由各站点中的网卡负责。

- 有少量的容错能力和网络管理功能
 - 例如，若网络中某个站点的网卡出现了故障而不停地发送帧，集线器可以检测到这个问题，在内部断开与出故障网卡的连线，使整个以太网能正常工作。

4.4.3. 对比



4.4.4. BASE-T星型以太网

- IEEE于1990年制定了10BASE-T星型以太网的标准802.3i，这种以太网是局域网发展史上的一座非常重要的里程碑，它为以太网在局域网中的统治地位奠定了牢固的基础。
- 10BASE-T以太网的通信距离较短，每个站点到集线器的距离不能超过100m。
- IEEE 802.3以太网还可使用光纤作为传输媒体，相应的标准为10BASE-F，“F”表示光纤。光纤主要用作集线器之间的远程连接。



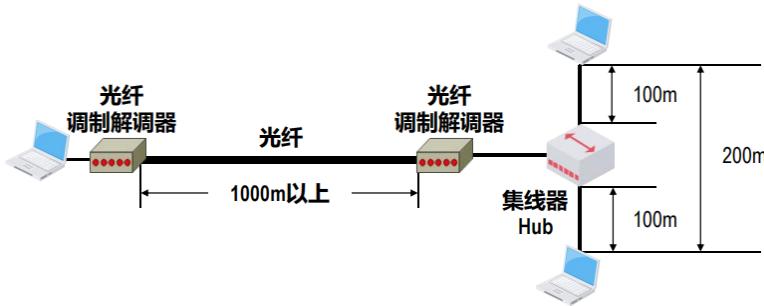
4.5. 在物理层扩展以太网

4.5.1. 扩展站点与集线器之间的距离

- 中两站点之间的距离太远会使传输的信号就会衰减到使CSMA/CD协议无法正常工作。
- 在早期广泛使用粗同轴电缆或细同轴电缆共享总线以太网时，为了提高网络的地理覆盖范围，常用的是工作在物理层的转发器。
- IEEE 802.3标准规定，两个网段可用一个转发器连接起来，任意两个站点之间最多可以经过三个网段。



- 在10BASE-T星型以太网中，可使用光纤和一对光纤调制解调器来扩展站点与集线器之间的距离。
 - 这种扩展方法比较简单，所需付出的代价是：为站点和集线器各增加一个用于电信号和光信号转换的光纤调制解调器，以及它们之间的一对通信光纤。
- 信号在光纤中的衰减和失真很小，因此使用这种方法可以很简单地将站点与集线器之间的距离扩展到1000以上。



- 在物理层扩展的共享式以太网仍然是一个碰撞域，不能连接太多的站点，否则可能会出现大量的碰撞，导致平均吞吐量太低。

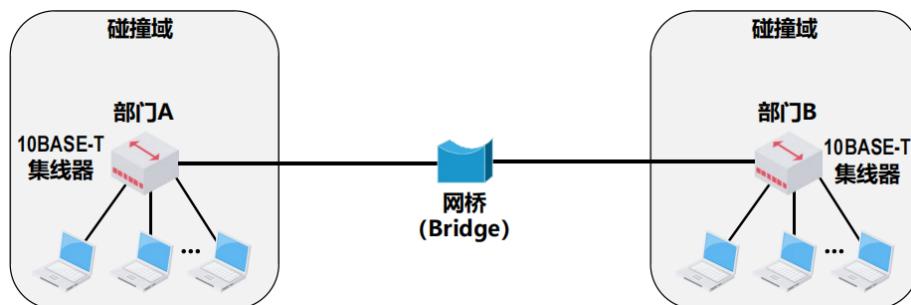


4.5.2. 扩展共享式以太网的覆盖范围和站点数量

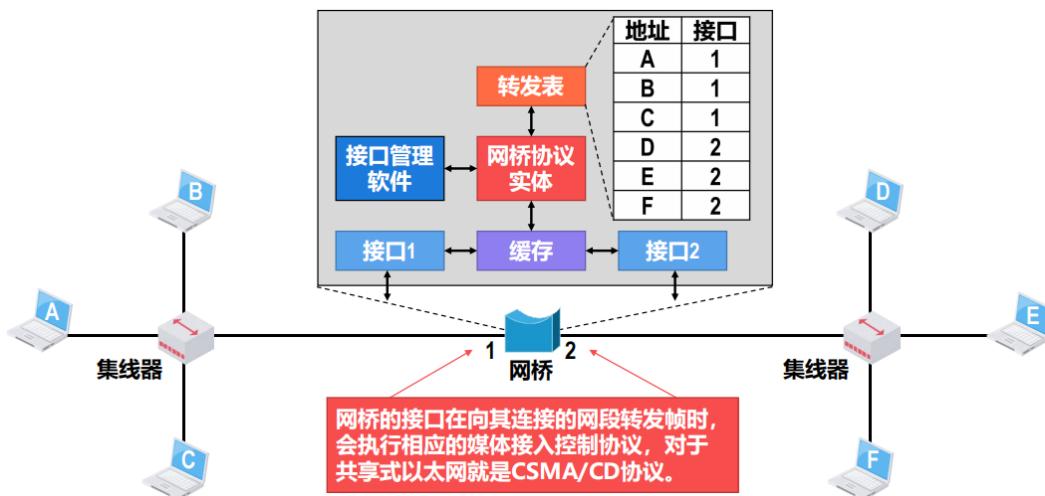
4.6. 在数据链路层扩展以太网

4.6.1. 使用网桥在数据链路层扩展以太网

- 网桥（bridge）工作在数据链路层（包含其下的物理层），因此网桥具备属于数据链路层范畴的相关能力。
 - 网桥可以识别帧的结构。
 - 网桥可以根据帧首部中的目的MAC地址和网桥自身的帧转发表来转发或丢弃所收到的帧。



4.6.2. 网桥的主要结构和基本工作原理



4.6.3. 透明网桥的自学习和转发帧的流程

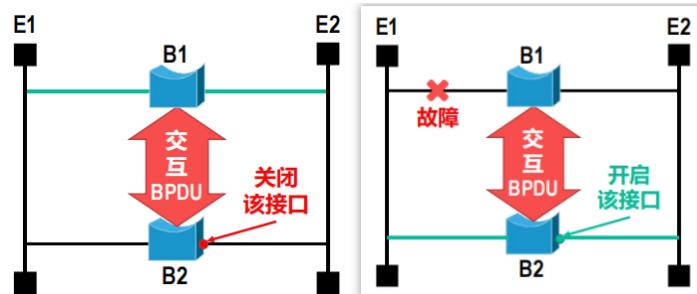
- 透明网桥（Transparent Bridge）通过自学习算法建立转发表。
 - “透明”，是指以太网中的各站点并不知道自己所发送的帧将会经过哪些网桥的转发，最终到达目的站点。也就是说，以太网中的各网桥对于各站点而言是看不见的。
 - 透明网桥的标准是IEEE 802.1D，它通过一种自学习算法基于以太网中各站点间的相互通信逐步建立起自己的转发表。
- ① 网桥收到帧后进行登记（即自学习），登记的内容为帧的源MAC地址和进入网桥的接口号。**
- ② 网桥根据帧的目的MAC地址和网桥的转发表对帧进行转发，包含以下三种情况：**
- **明确转发**：网桥知道应当从哪个接口转发帧。
 - **盲目转发**：网桥不知道应当从哪个接口转发帧，只能将其通过除进入网桥的接口外的其他所有接口转发。
 - **丢弃**：网桥知道不应该转发该帧，将其丢弃。

请同学们注意：

- (1) 如果网桥收到有误码的帧则直接丢弃。
- (2) 如果网桥收到一个无误码的广播帧，则不用进行查表，而是直接从除接收该广播帧的接口的其他接口转发该广播帧。
- (3) 转发表中的每条记录都有其有效时间，到期自动删除！这是因为各站点的MAC地址与网桥接口的对应关系并不是永久性的，例如某个站点更换了网卡，其MAC地址就会改变。

4.6.4. 透明网桥的生成树协议STP

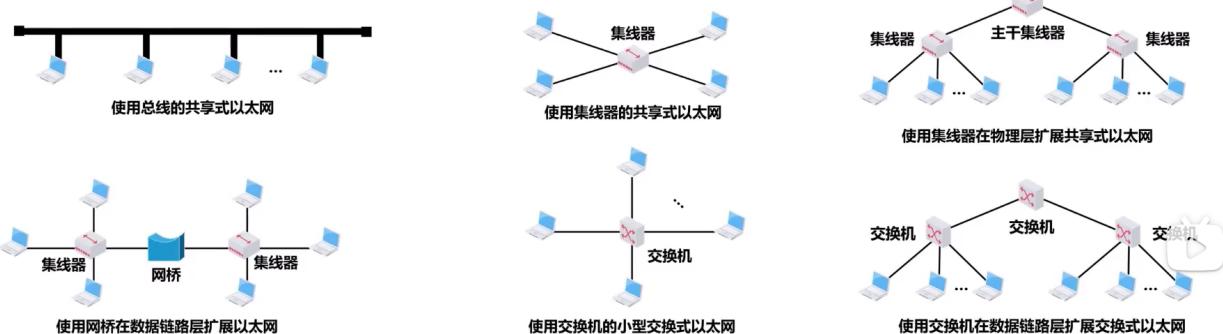
- 为了提高以太网的可靠性，有时需要在两个以太网之间使用多个透明网桥来提供冗余链路。
 - 在增加冗余链路提高以太网可靠性的同时，却给网络引入了环路。
 - 网络中的广播帧将在环路中永久兜圈，造成广播帧充斥整个网络，网络资源被白白浪费，而网络中的主机之间无法正常通信！
- **生成树协议（Spanning Tree Protocol, STP）**
 - 避免广播帧在环路中永久兜圈；可以在增加冗余链路提高网络可靠性的同时，又避免环路带来的问题。
 - 不管网桥之间连接成了怎样复杂的带环拓扑，网桥之间通过交互网桥协议单元（Bridge Protocol DataUnit, BPDU），找出原网络拓扑的一个连通子集（即生成树），在这个子集里整个连通的网络中不存在环路。
 - 当首次连接网桥或网络拓扑发生变化时（人为改变或出现故障），网桥都会重新构造生成树，以确保网络的连通。



5. 交换式以太网

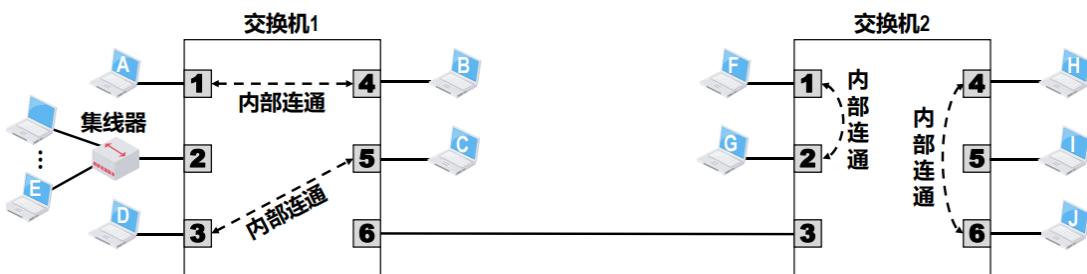
5.1. 交换式以太网

- 网桥的接口数量很少，通常只有2~4个，一般只用来连接不同的网段。
- 1990年面世的交换式集线器（Switching Hub），实质上是具有多个接口的网桥，常称为以太网交换机（Switch）或二层交换机。
 - “二层”是指以太网交换机工作在数据链路层（包括物理层）。
 - 与网桥相同，交换机内部的转发表也是通过自学习算法，基于网络中各主机间的通信，自动地逐步建立起来的。
 - 另外，交换机也使用生成树协议STP，来产生能够连通全网但不产生环路的通信路径。
- 仅使用交换机（而不使用集线器）的以太网就是交换式以太网。

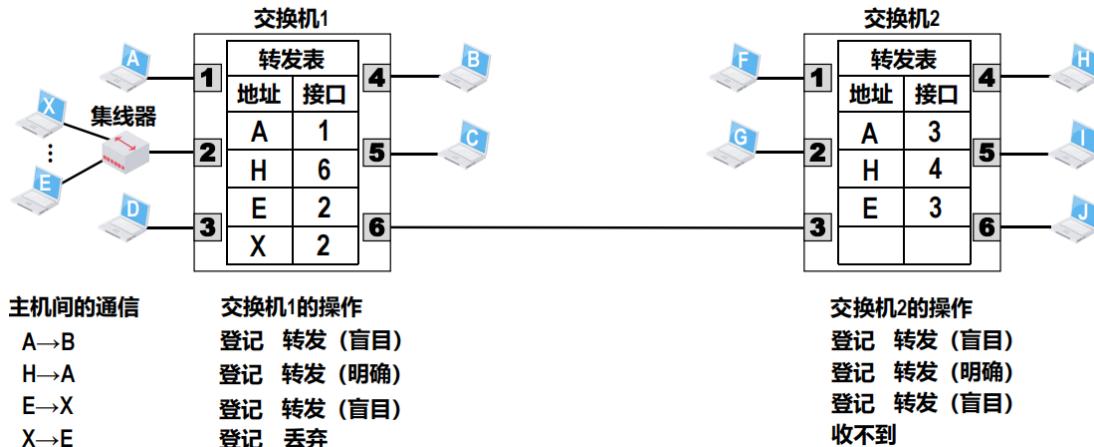


5.2. 以太网交换机

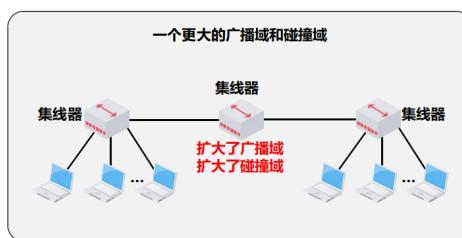
- 以太网交换机
 - 本质上就是一个多接口的网桥
 - 交换机自学习和转发帧的流程与网桥是相同的
 - 交换机也使用生成树协议STP，来产生能够连通全网但不产生环路的通信路径。
- 交换机的每个接口可以连接计算机，也可以连接集线器或另一个交换机。
 - 当交换机的接口与计算机或交换机连接时，可以工作在全双工方式，并能在自身内部同时连通多对接口，使每一对相互通信的计算机都能像独占传输媒体那样，无碰撞地传输数据，这样就不需要使用CSMA/CD协议了。
 - 当交换机的接口连接的是集线器时，该接口就只能使用CSMA/CD协议并只能工作在半双工方式。
 - 现在的交换机和计算机中的网卡都能自动识别上述两种情况，并自动切换到相应的工作方式。
 - 交换机一般都具有多种速率的接口，例如10Mb/s、100Mb/s、1Gb/s甚至10Gb/s的接口，大部分接口支持多速率自适应。



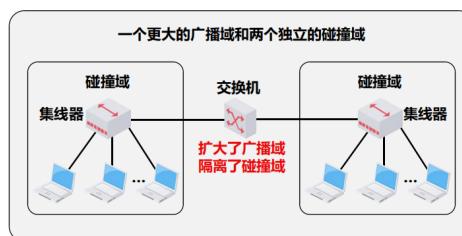
【练习题】交换机自学习和转发帧的流程（参考网桥自学习和转发帧的流程）



5.3. 共享式以太网与交换式以太网的对比



- 集线器
 - 扩大了广播域
 - 扩大了碰撞域

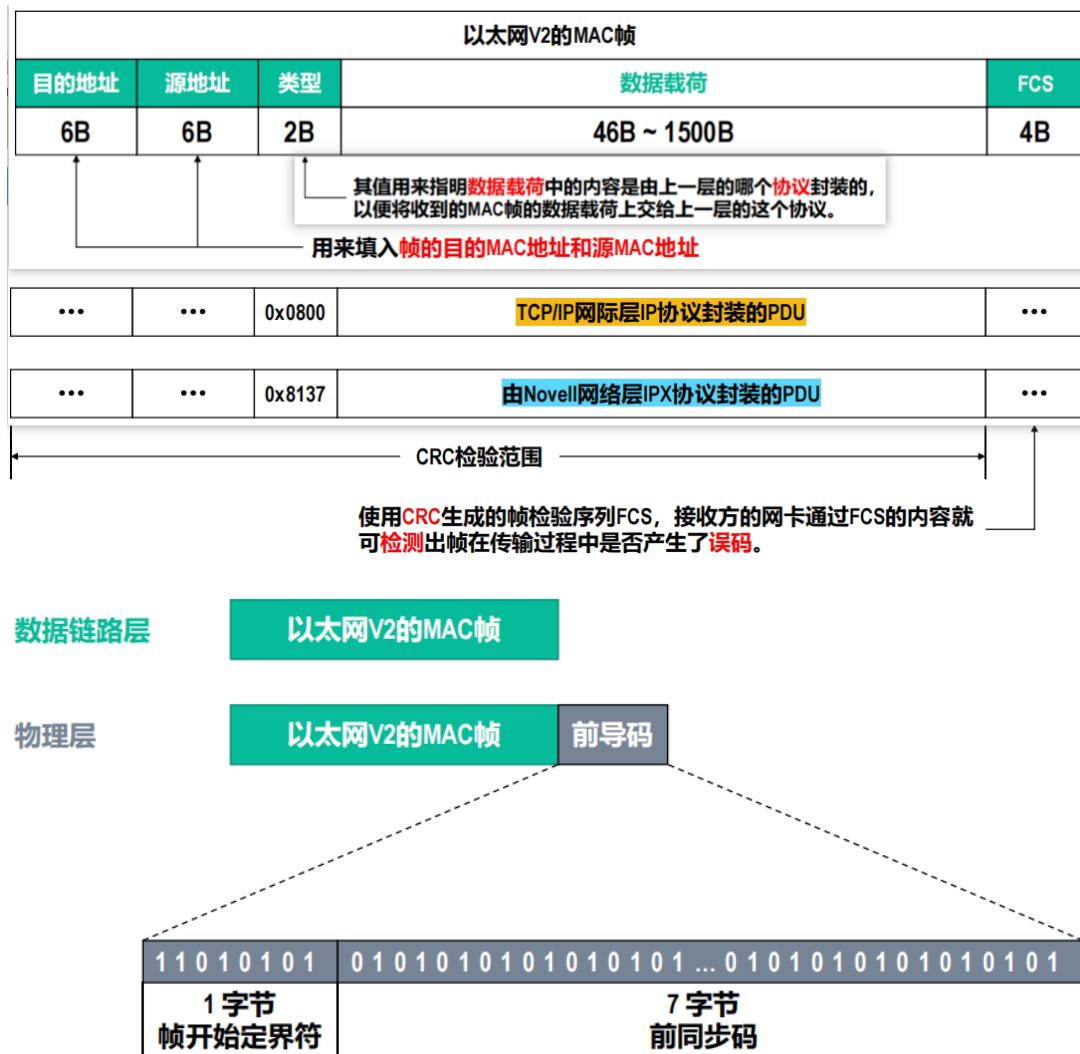


- 交换机
 - 扩大了广播域
 - 隔离了碰撞域
- 交换式以太网的网络性能远高于共享式以太网，集线器早已被交换机取代。

6. 以太网的MAC帧格式



6.1. 以太网V2的MAC帧



- 接收方可能收到的无效MAC帧包括以下几种：
 - MAC帧的长度不是整数个字节
 - 通过MAC帧的FCS字段的值检测出帧有误码
 - MAC帧的长度不在64~1518字节之间
- 接收方收到无效的MAC帧时，就简单将其丢弃，以太网的数据链路层没有重传机制。

7. 虚拟局域网

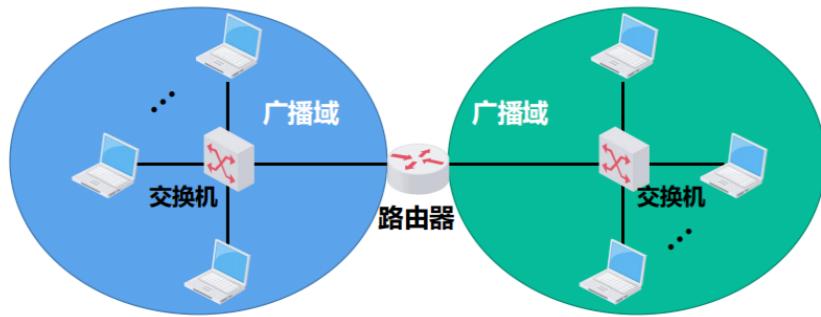
7.1. 虚拟局域网VLAN的诞生背景

- 将多个站点通过一个或多个以太网交换机连接起来就构建出了交换式以太网。
- 交换式以太网中的所有站点都属于同一个广播域。
- 随着交换式以太网规模的扩大，广播域也相应扩大。

7.1.1. 巨大的广播域会带来一系列问题

- 广播风暴（广播风暴会浪费网络资源和各主机的CPU资源）
- 难以管理和维护，带来潜在的安全问题。

7.1.2. 分割广播域的方法



- 使用路由器可以隔离广播域（成本较高）
- 虚拟局域网技术应运而生

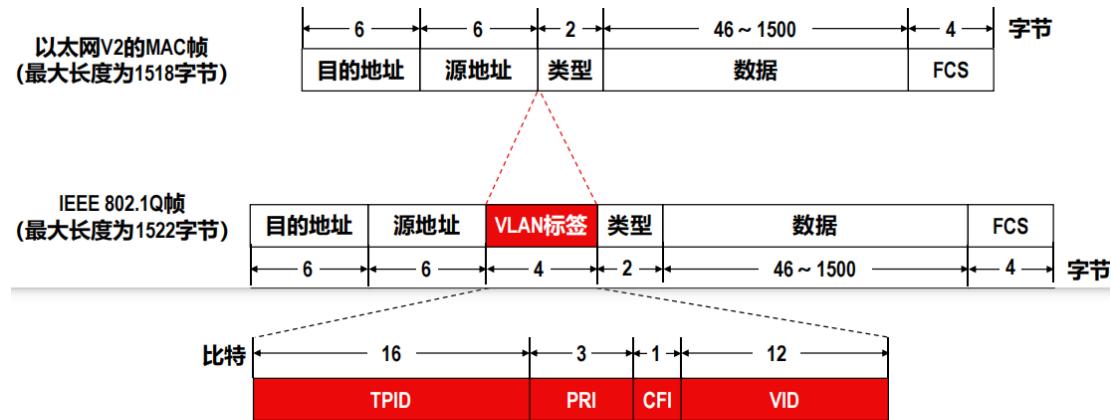
7.2. 虚拟局域网VLAN概述

- 虚拟局域网（Virtual Local Area Network, VLAN）是一种将局域网内的站点划分成与物理位置无关的逻辑组的技术，一个逻辑组就是一个VLAN，VLAN中的各站点具有某些共同的应用需求。
- 属于同一VLAN的站点之间可以直接进行通信，而不同VLAN中的站点之间不能直接通信。
- 网络管理员可对局域网中的各交换机进行配置来建立多个逻辑上独立的VLAN
 - 连接在同一交换机上的多个站点可以属于不同的VLAN，而属于同一VLAN的多个站点可以连接在不同的交换机上。
- 虚拟局域网VLAN并不是一种新型网络，它只是局域网能够提供给用户的一种服务。

7.3. 虚拟局域网VLAN的实现机制——IEEE 802.1Q帧

7.3.1. IEEE 802.1Q帧

- 虚拟局域网VLAN有多种实现技术。
- 最常见的就是基于以太网交换机的接口来实现VLAN。
- 这就需要以太网交换单元能够实现以下两个功能：
 - 能够处理带有VLAN标记的帧，也就是IEEE 802.1Q帧。
 - 交换机的各接口可以支持不同的接口类型，不同接口类型的接口对帧的处理方式有所不同。
- IEEE 802.1Q帧也称为Dot One Q帧，它对以太网V2的MAC帧格式进行了扩展：
 - 在源地址字段和类型字段之间插入了4字节的VLAN标签（tag）字段。
 - 最大长度为1522字节



标签协议标识符TPID: 长度为16比特，其值固定为0x8100，表示该帧是IEEE 802.1Q帧。

优先级PRI: 长度为3比特，取值范围是0~7，值越大优先级越高。当网络阻塞时，设备优先发送优先级高的802.1Q帧。

规范格式指示符CFI: 长度为1比特，取值为0表示MAC地址以规范格式封装，取值为1表示MAC地址以非规范格式封装。对于以太网，CFI的取值为0。

虚拟局域网标识符VID: 长度为12比特，取值范围是0~4095，其中0和4095保留不使用。

VID是802.1Q帧所属VLAN的编号，设备利用VID来识别帧所属的VLAN。

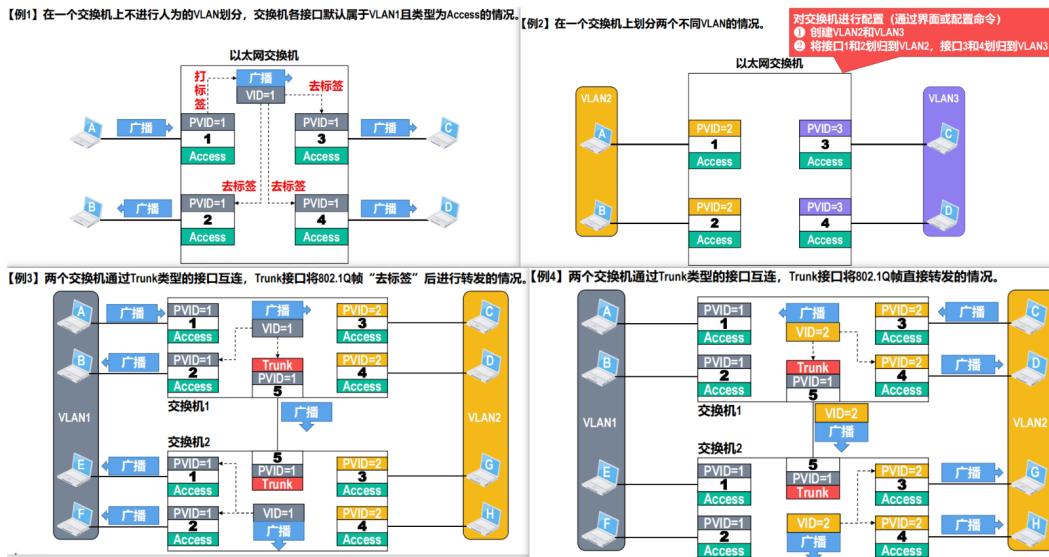
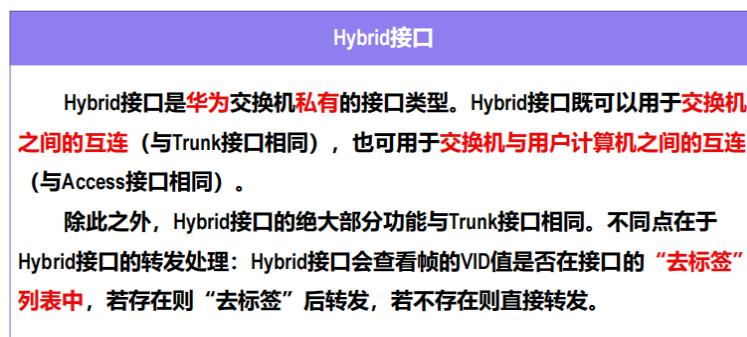
广播帧只在同一VLAN内转发，这样就将广播域限制在了一个VLAN内。

- 802.1Q帧一般不由用户主机处理，而是由以太网交换机来处理：
 - “打标签”：
 - 当交换机收到普通的以太网MAC帧时，会给其插入4字节的VLAN标签使之成为802.1Q帧。
 - “去标签”
 - 当交换机转发802.1Q帧时，可能会删除其4字节的VLAN标签使之成为普通的以太网MAC帧。
 - 交换机转发802.1Q帧时也有可能不进行“去标签”处理，是否进行“去标签”处理取决于交换机的接口类型。

7.3.2. 以太网交换机的接口类型

- 根据接口在接收帧和发送帧时对帧的处理方式的不同，以及接口连接对象的不同，以太网交换机的接口类型一般分为Access和Trunk两种。
- 当以太网交换机上电启动后，若之前未对其各接口进行过VLAN的相关设置，则各接口的接口类型默认为Access，并且各接口的缺省VLAN ID为1，即各接口默认属于VLAN1。
 - 对于思科交换机，接口的缺省VLAN ID称为本征VLAN (Native VLAN)。
 - 对于华为交换机，接口的缺省VLAN ID称为端口VLAN ID (Port VLAN ID)，简记为PVID。
- 交换机的每个接口有且仅有一个PVID

Access接口	Trunk接口
<p>Access接口一般用于连接用户计算机，由于其只能属于一个VLAN，因此Access接口的PVID值与其所属VLAN的ID相同，其默认值为1。</p> <p>● 接收处理 一般只接受“未打标签”的普通以太网MAC帧，根据接收帧的接口的PVID给帧“打标签”，即插入4字节的VLAN标签字段，VLAN标签字段中的VID取值就是接口的PVID值。</p> <p>● 转发处理 若帧中的VID值与接口的PVID值相等，则给帧“去标签”后再进行转发，否则不转发帧。因此，从Access接口转发出的帧，是不带VLAN标签的普通以太网MAC帧。</p>	<p>Trunk接口一般用于交换机之间的互连。Trunk接口可以属于多个VLAN，即Trunk接口可以通过属于不同VLAN的帧。Trunk接口的默认PVID值为1，一般不建议用户修改，若互连的Trunk接口的PVID值不相等，则可能出现转发错误。</p> <p>● 接收处理 既可以接收“未打标签”的普通以太网MAC帧，也可以接收“已打标签”的802.1Q帧。若接收到普通以太网MAC帧时，根据接收帧的接口的PVID给帧“打标签”，这与Access接口的处理相同。</p> <p>● 转发处理 对于帧的VID值等于接口的PVID值的802.1Q帧，将其“去标签”转发；对于帧的VID值不等于接口的PVID值802.1Q帧，将其直接转发。因此，从Trunk接口转发出的帧，可能是普通以太网MAC帧，也可能是802.1Q帧。</p>



8. 以太网的发展



8.1. BASE-T以太网

- 100BASE-T以太网是指在双绞线上传输基带信号的速率为100Mb/s的以太网，也称为快速以太网（Fast Ethernet）。



■ 100BASE-T以太网与10Mb/s标准以太网（传统以太网）一样，仍然使用IEEE 802.3的帧格式和CSMA/CD协议。

■ 100BASE-T以太网为了与10Mb/s标准以太网保持兼容，需要以太网最小帧长保持不变，即仍为64字节。

- 网段的最大电缆长度从1000m减小到100m
- 争用期缩短为 $5.12\mu s$
- 帧间最小间隔缩短为 $0.96\mu s$

100BASE-T以太网还可以使用以太网交换机来提供比集线器更好的服务质量，即在全双工方式下无碰撞工作。因此，使用交换机的100BASE-T以太网，工作在全双工方式下，并不使用CSMA/CD协议。

■ 1995年，IEEE的802委员会正式批准100BASE-T以太网的标准为802.3u。实际上，IEEE 802.3u只是对原有IEEE 802.3标准的补充。

■ 除100BASE-T以太网外，百兆以太网有多种不同的物理层标准：

名称	传输介质	网段最大长度	说 明
100BASE-TX	铜缆	100m	两对UTP5类线或屏蔽双绞线STP
100BASE-T4	铜缆	100m	4对UTP3类线或5类线
100BASE-FX	光缆	2000m	两根光纤，发送和接收各用一条

8.2. 吉比特以太网

8.2.1. 简介

■ 吉比特以太网也称为千兆以太网（Gigabit Ethernet）。1998年，千兆以太网的标准802.3z成为正式标准。

■ 近几年来，千兆以太网已迅速占领市场，成为了以太网的主流产品。

■ IEEE 802.3z千兆以太网的主要特点有：

- 速率为1000Mb/s (1Gb/s)
- 使用IEEE 802.3的帧格式（与10Mb/s和100Mb/s以太网相同）
- 支持半双工方式（使用CSMA/CD协议）和全双工方式（不使用CSMA/CD协议）
- 兼容10BASE-T和100BASE-T技术

8.2.2. 载波延伸

- 当千兆以太网工作在半双工方式时，需要使用CSMA/CD协议。由于速率已经提高到了1000Mb/s，因此只有减小网段最大长度或增大最小帧长，才能使3.4.2节中介绍的以太网的参数 a (τ/T_0) 保持为较小的数值。
- 若将网段最大长度减小到10m，则网络基本失去了应用价值。
 - 若将最小帧长增大到640字节，则当上层交付的待封装的协议数据单元PDU很短时，开销就会太大。

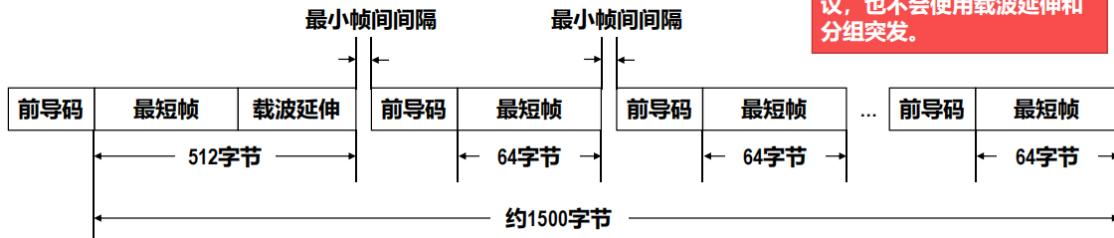
千兆以太网的网段最大长度仍保持为100m，最小帧长仍保持为64字节（与10BASE-T和100BASE-T兼容）。

- 这就需要使用载波延伸 (Carrier Extension) 的办法，将争用期增大为512字节的发送时间而保持最小帧长仍为64字节。
- 只要发送的MAC帧的长度不足512字节时，就在MAC帧尾部填充一些特殊字符，使MAC帧的长度增大到512字节。



8.2.3. 分组突发

- 在使用载波延伸的机制下，如果原本发送的是大量的64字节长的短帧，则每一个短帧都会被填充448字节的特殊字符，这样会造成很大的开销。
- 因此，千兆以太网还使用了分组突发 (Packet Bursting) 功能。也就是当有很多短帧要连续发送时，只将第一个短帧用载波延伸的方法进行填充，而其后面的一系列短帧不用填充就可一个接一个地发送，它们之间只需空开必要的帧间最小间隔即可。
- 这样就形成了一连串分组的突发，当累积发送1500字节或稍多一些为止。



8.2.4. 物理层标准

- 千兆以太网有多种不同的物理层标准：

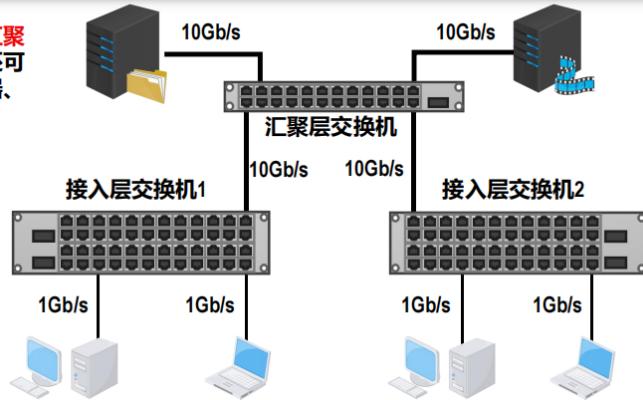
名 称	传 输 介 质	网 段 最 大 长 度	说 明
1000BASE-SE	光缆	550m	多模光纤 (50和62.5μm)
1000BASE-LX	光缆	5000m或550m	单模光纤 (10μm) 或多模光纤 (50和62.5μm)
1000BASE-CX	铜缆	25m	使用2对屏蔽双绞线电缆STP
1000BASE-T	铜缆	100m	使用4对UTP5类线

8.3. 吉比特以太网

8.3.1. 简介

- 2002年6月，IEEE 802.3ae委员会通过**10吉比特以太网（10GE）**的正式标准，10GE也称为**万兆以太网**。
- 万兆以太网并不是将千兆以太网的速率简单地提高了10倍。万兆以太网的目标是将以太网从**局域网范围**（校园网或企业网）**扩展到城域网与广域网**，成为城域网和广域网的主干网的主流技术之一。
- IEEE 802.3ae万兆以太网的主要特点有：
 - 速率为10Gb/s
 - 使用IEEE 802.3标准的帧格式（与10Mb/s、100Mb/s和1Gb/s以太网相同）
 - 保留IEEE 802.3标准对以太网最小帧长和最大帧长的规定。这是为了用户升级以太网时，仍能和较低速率的以太网方便地通信。
 - 只工作在全双工方式而不存在争用媒体的问题，因此不需要使用CSMA/CD协议，这样传输距离就不再受碰撞检测的限制。
 - 增加了支持城域网和广域网的物理层标准

- 万兆以太网交换机常作为千兆以太网的**汇聚层交换机**，与千兆以太网交换机相连，还可以连接对传输速率要求极高的视频服务器、文件服务器等设备。



8.3.2. 物理层标准

- 万兆以太网有多种不同的物理层标准：

名称	传输介质	网段最大长度	说 明
10GBASE-SR	光缆	300m	多模光纤 (850nm)
10GBASE-LR	光缆	10km	单模光纤 (1300nm)
10GBASE-ER	光缆	40km	单模光纤 (1500nm)
10GBASE-CX4	铜缆	15m	使用4对双芯同轴电缆 (twinax)
10GBASE-T	铜缆	100m	使用4对6A类UTP双绞线

8.4. 吉比特/100吉比特以太网

8.4.1. 简介

- 2010年，IEEE发布了**40吉比特/100吉比特以太网**（40GE/100GE）的IEEE 802.3ba标准，40GE/100GE也称为**四万兆/十万兆以太网**。
- 为了使**以太网能够更高效、更经济地满足局域网、城域网和广域网的不同应用需求**，IEEE 802.3ba标准定义了**两种速率类型**：
 - 40Gb/s主要用于**计算应用**
 - 100Gb/s主要用于**汇聚应用**
- IEEE 802.3ba标准**只工作在全双工方式（不使用CSMA/CD协议）**，但仍**使用IEEE 802.3标准的帧格式并遵守最小帧长和最大帧长的规定**。
- IEEE 802.3ba标准的**两种速率各有4种不同的传输媒体**

物理层	40GE	100GE
在背板上传输至少超过1m	40GBASE-KR4	
在铜缆上传输至少超过7m	40GBASE-CR4	100GBASE-CR10
在多模光纤上传输至少100m	40GBASE-SR4	100GBASE-SR10
在单模光纤上传输至少10km	40GBASE-LR4	100GBASE-LR4
在单模光纤上传输至少40km		100GBASE-ER4

9. 无线局域网

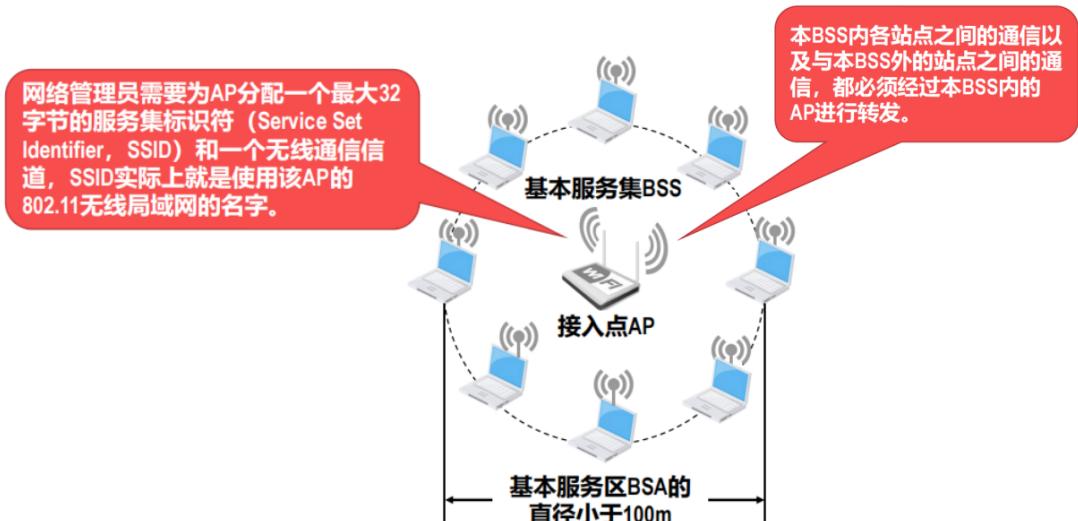
9.1. 无线局域网的组成

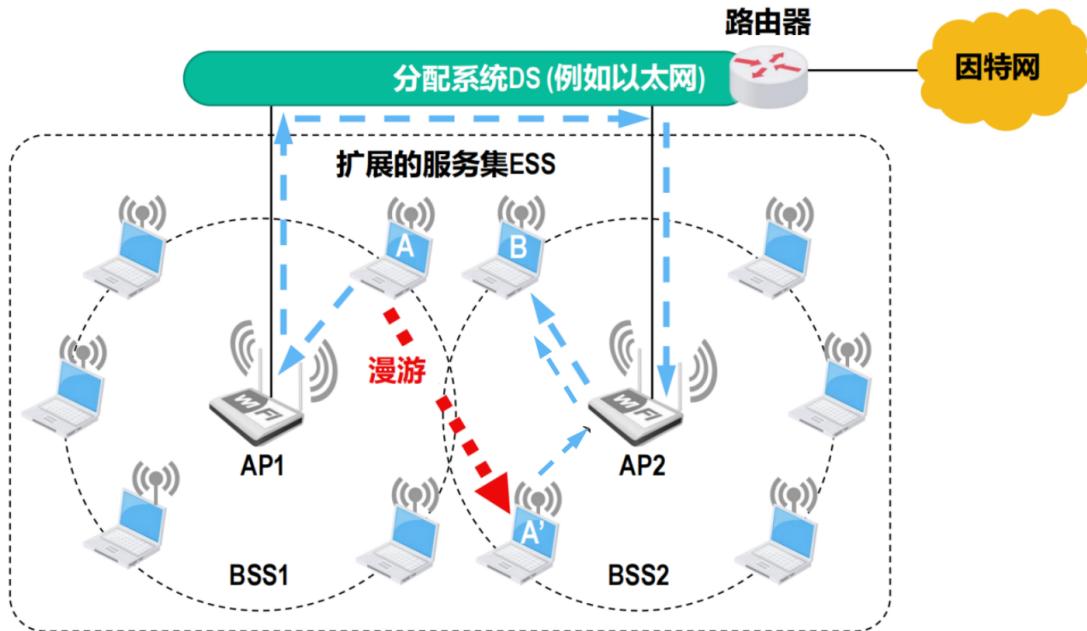
- 随着移动通信技术的发展，**无线局域网**（Wireless Local Area Network，WLAN）自20世纪80年代末以来逐步进入市场。
- IEEE于1997年制定了**无线局域网**的协议标准802.11，**802.11无线局域网**是目前应用最广泛的**无线局域网**之一，人们更多地将其简称为**Wi-Fi**（Wireless Fidelity，无线保真度）。
- 802.11**无线局域网**使用最多的是它的**固定基础设施的组网方式**。

9.1.1. 无线局域网分类

9.1.1.1. 有固定基础设施的

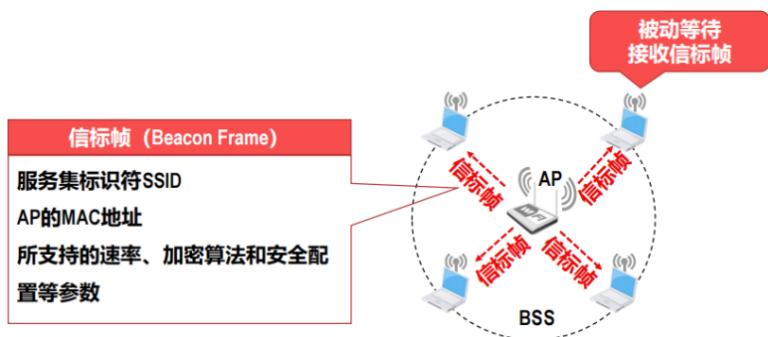
- 固定基础设施
 - 预先建立的
 - 能够覆盖一定地理范围的
 - 多个固定的通信基站



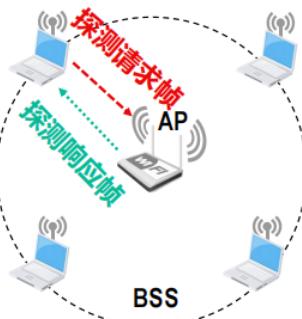


- 802.11标准并没有定义实现漫游的具体方法，仅定义了以下一些基本服务

- 关联 (Association) 服务
 - 移动站与接入点AP建立关联的方法有以下两种：
 - 被动扫描
 - 主动扫描



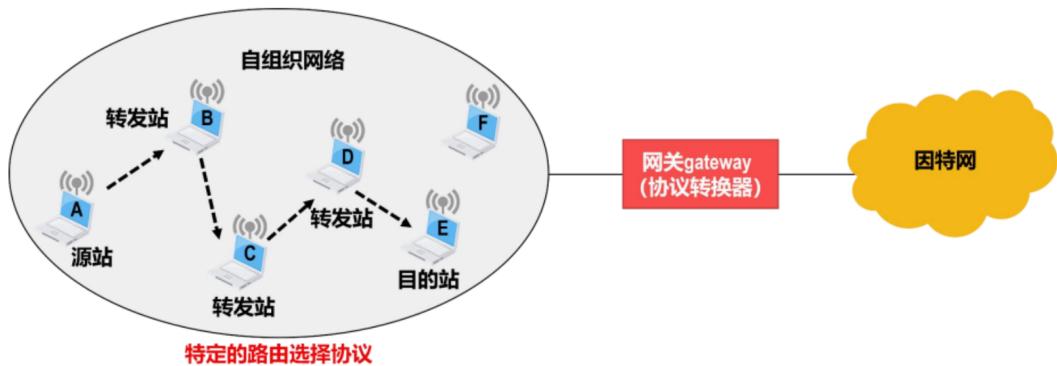
- 主动扫描



- 重建关联 (Reassociation) 服务和分离 (Dissociation) 服务
 - 如果一个移动站要把与某个接入点AP的关联转移到另一个AP，就可以使用重建关联服务；若要终止关联服务，就应使用分离服务。

9.1.1.2. 无固定基础设施的

- 自组织网络 (ad hoc Network)
 - 无基站或接入点AP
 - 是由一些对等的移动站点构成的临时网络
 - 数据在网络中被多跳存储转发
 - 转发站需要路由功能



自组织网络组网方便，不需要基站，并且具有非常好的生存性，这使得自组织网络在军用和民用领域都有很好的应用前景。

802.11无线局域网的ad hoc模式允许网络中的各站点在其通信范围内直接通信，也就是支持站点间的单跳通信，而标准中并没有包括多跳路由功能。因此，802.11无线局域网的ad hoc模式应用较少。

9.2. 无线局域网的物理层

9.2.1. 概述

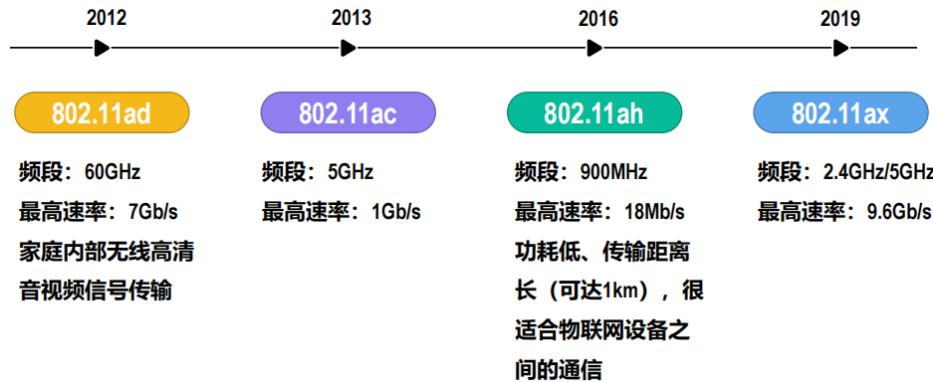
- 802.11无线局域网的物理层非常复杂，依据工作频段、调制方式、传输速率等，可将其分为多种物理层标准

标准	频段	调制方式	最高速率	特 点	时间
802.11b	2.4GHz	DSSS	11Mb/s	信号传播距离远且不易受阻碍，最高速率较低	1999年
802.11a	5GHz	OFDM	54Mb/s	信号传播距离较短且易受阻碍，最高速率较高，支持更多用户同时上网	1999年
802.11g	2.4GHz	OFDM	54Mb/s	信号传播距离远且不易受阻碍，最高速率较高，支持更多用户同时上网	2003年
802.11n	2.4GHz 5GHz	MIMO OFDM	600Mb/s	使用多个发射和接收天线达到更高的最高速率，使用双倍带宽 (40MHz) 时最高速率可达600Mb/s	2009年

- 802.11无线网卡一般会被做成多模的，以便能适应多种不同的物理层标准，例如支持802.11b/g/n。
- 无线局域网最初还使用红外技术 (infrared, IR) 和跳频扩频 (Frequency Hopping Spread Spectrum, FHSS) 技术，但目前已经很少使用了。
- 跳频技术的发明人，是好莱坞黄金时代的著名女星海蒂·拉玛，跳频技术为CDMA和Wi-Fi等无线通信技术奠定了基础。因此，海蒂·拉玛被誉为“Wi-Fi之母”。

9.2.2. 近年新的物理层标准

- 最近几年，802.11无线局域网又有一些新的物理层标准陆续推出



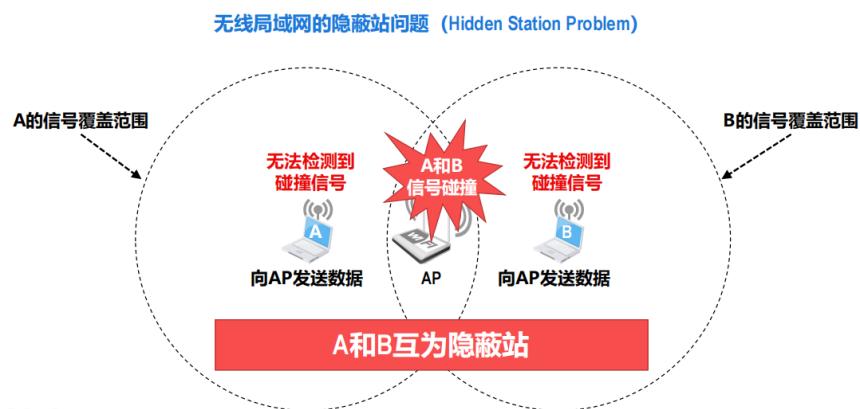
9.3. 无线局域网使用CSMA/CA协议的原因

9.3.1. 区别

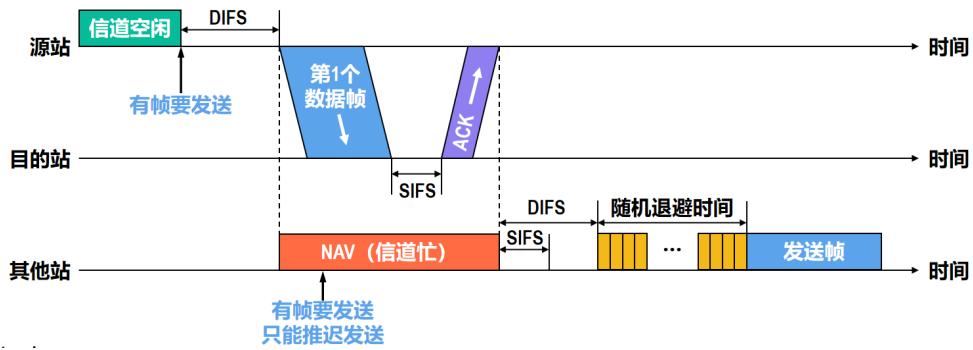
- 对于802.11无线局域网，其使用无线信道传输数据，这与共享总线以太网使用有线传输介质不同。因此，802.11无线局域网不能简单照搬共享总线以太网使用的CSMA/CD协议。
- 802.11无线局域网采用了另一种称为CSMA/CA的协议，也就是载波监听多址接入/碰撞避免（Carrier Sense Multiple Access/Collision Avoidance, CSMA/CA）。
- CSMA/CA协议仍然采用CSMA/CD协议中的CSMA，以“先听后说”的方式来减少碰撞的发生，但是将“碰撞检测CD”改为了“碰撞避免CA”。
 - 尽管CA表示碰撞避免，但并不能避免所有的碰撞，而是尽量减少碰撞发生的概率。

9.3.2. 原因

- 由于无线信道的传输环境复杂且信号强度的动态范围非常大，在802.11无线网卡上接收到的信号强度一般都远远小于发送信号的强度，信号强度甚至相差百万倍。因此，如果要在802.11无线网卡上实现碰撞检测，对硬件的要求非常高。
- 即使能够在硬件上实现碰撞检测功能，但由于无线电波传播的特殊性（存在隐蔽站问题），还会出现无法检测到碰撞的情况，因此实现碰撞检测并没有意义。
 - 无线局域网的隐蔽站问题（Hidden Station Problem）



9.4. CSMA/CA协议的基本工作原理



9.4.1. DIFS

- DCF帧间间隔DIFS的长度为 $128\mu s$ ，在DCF方式中，DIFS用来发送数据帧和管理帧。DCF是分布式协调功能（Distributed Coordination Function，DCF）的英文缩写词。在DCF方式下，没有中心控制站点，每个站点使用CSMA/CA协议通过争用信道来获取发送权。DCF方式是802.11定义的默认方式（必须实现）。
 - 等待DIFS间隔是考虑到可能有其他的站有高优先级的帧要发送。

9.4.2. 虚拟载波监听 (Virtual Carrier Sense) 机制

- 帧首部中的“持续时间”字段的值指出了源站要占用信道的时间（包括目的站发回确认帧所需的时间）
 - 当某个站检测到正在信道中传送的帧首部中的“持续时间”字段时，就调整自己的网络分配向量（Network Allocation Vector， NAV）。NAV指出了完成这次帧的传送且信道转入空闲状态所需的时间。

9.4.3. SIFS

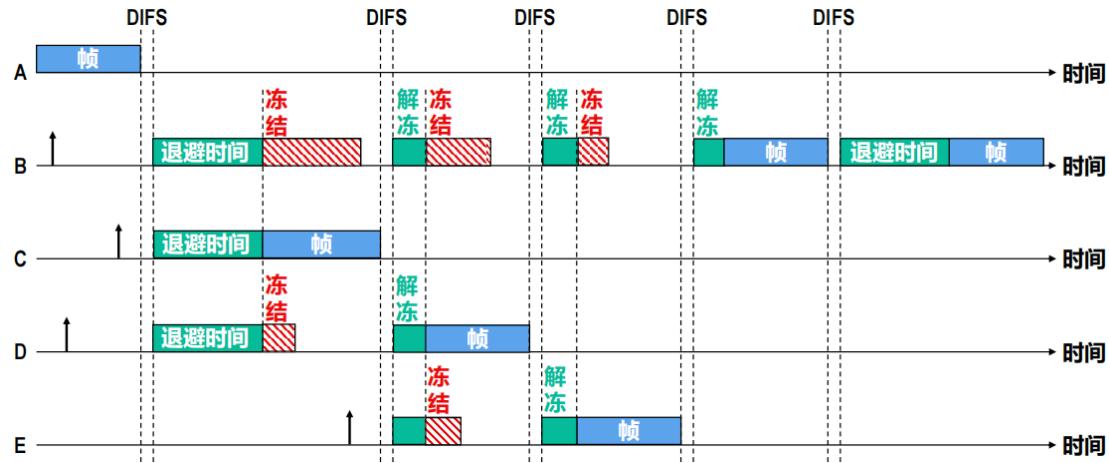
- 短帧间间隔 (Short Interframe Space, SIFS) 的长度为 $28\mu s$, 它是最短的帧间间隔, 用来分隔开属于一次对话的各帧。一个站点应当能够在这段时间内从发送方式切换到接收方式。使用SIFS的帧类型有ACK帧、CTS帧等。
 - 由于无线信道的误码率较高, CSMA/CA协议还需要使用停止——等待的确认机制来实现可靠传输, 这与使用CSMA/CD协议的共享式以太网不同。
 - 当某个站在发送帧时, 很可能有多个站都在监听信道并等待发送帧, 一旦信道空闲, 这些站几乎同时发送帧而产生碰撞。

9.4.4. 退避算法

9.4.4.1. 使用情况

- 为了避免上述情况，所有要发送帧的站检测到信道从忙转为空闲后，都要执行退避算法。这样不仅可以减少发生碰撞的概率，还可避免某个站长时间占用无线信道。
 - 当某个站要发送数据帧时，仅在这种情况下才不使用退避算法：检测到信道空闲，并且该数据帧不是成功发送完上一个数据帧之后立即连续发送的数据帧。除此之外的以下情况，都必须使用退避算法：
 - 在发送帧之前检测到信道处于忙态
 - 在每一次重传一个帧时
 - 在每一次成功发送帧后要连续发送下一个帧时

9.4.4.2. 算法内容



- 在执行退避算法时，站点为退避计时器设置一个随机的退避时间：
 - 当退避计时器的时间减小到零时，就开始发送数据；
 - 当退避计时器的时间还未减小到零时而信道又转变为忙状态，这时就冻结退避计时器的数值，重新等待信道变为空闲，再经过帧间间隔DIFS后，继续启动退避计时器。
- 在进行第*i*次退避时，退避时间在时隙编号{0, 1, ..., 2^{i-1}-1}中随机选择一个，然后乘以基本退避时间（也就是一个时隙的长度）就可以得到随机的退避时间。当时隙编号达到255时（对应于第6次退避）就不再增加了。

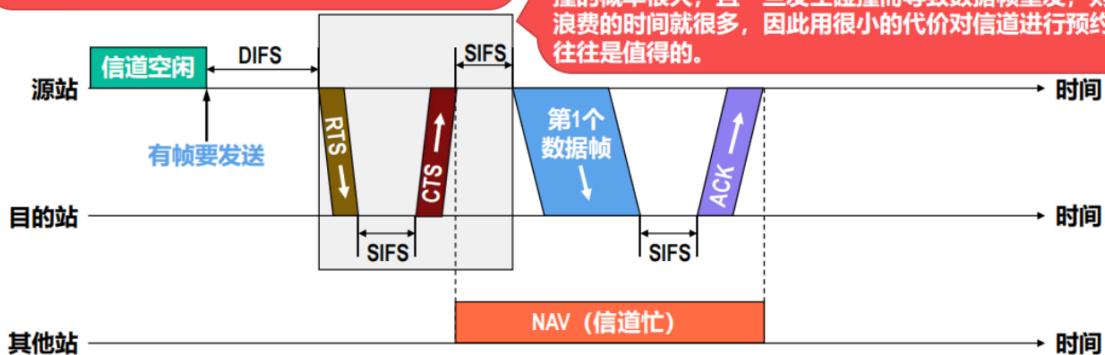
9.4.4.3. 对信道进行预约

- 为了进一步降低发生碰撞的概率，802.11无线局域网允许源站对信道进行预约。
- RTS (Request To Send) 帧是短的控制帧
 - 包括源地址
 - 目的地址
 - 本次通信（包括目的站发回确认帧所需的时间）所需的持续时间。
- CTS (Clear To Send) 帧是短的响应控制帧
 - 包括本次通信所需的持续时间（从RTS帧中将此持续时间复制到CTS帧中）。
- 除源站和目的站的其他各站，在收到CTS帧或数据帧后就推迟访问信道。这样就确保了源站和目的站之间的通信不会受到其他站的干扰
- 若RTS帧发生碰撞，源站就不可能收到CTS帧，源站会执行退避算法重传RTS帧。

尽管如此，802.11无线局域网仍为用户提供了以下三种选择：

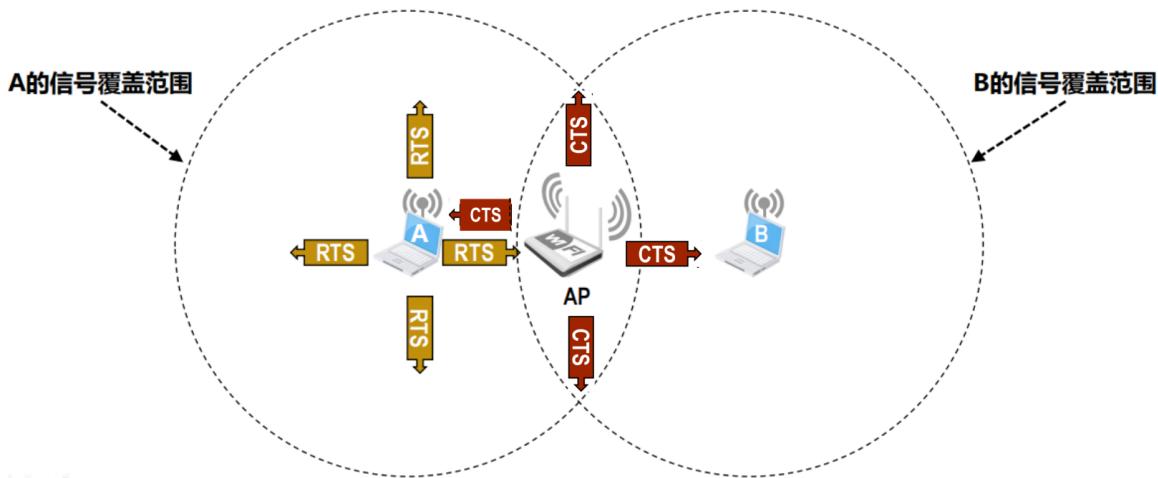
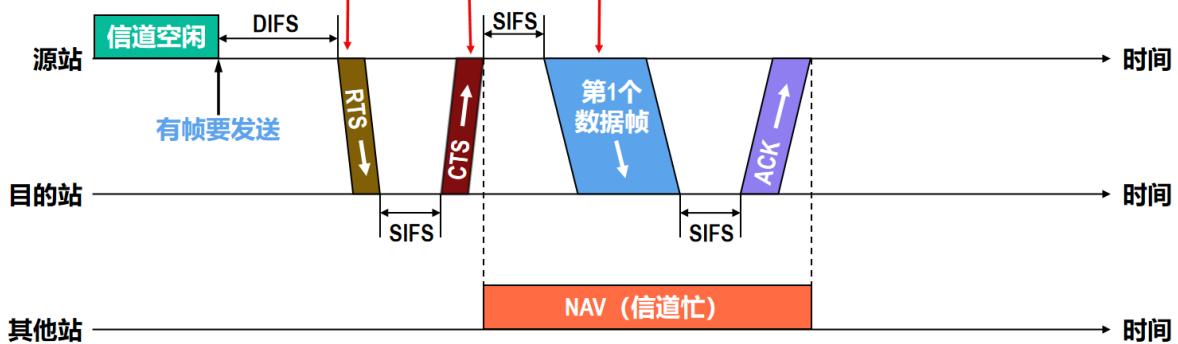
- ① 使用RTS帧和CTS帧。
- ② 只有当数据帧的长度超过某个数值时才使用RTS帧和CTS帧。
- ③ 不使用RTS帧和CTS帧。

使用RTS帧和CTS帧进行信道预约会带来额外的开销。但由于RTS帧和CTS帧都很短，发生碰撞的概率、碰撞产生的开销以及本身的开销都很小。对于一般的数据帧，其发送时延往往远大于传播时延（因为是局域网），碰撞的概率很大，且一旦发生碰撞而导致数据帧重发，则浪费的时间就很多，因此用很小的代价对信道进行预约往往是值得的。



由于RTS帧和CTS帧都会携带通信需要持续的时间，这与之前介绍过的数据帧可以携带通信所需持续时间的虚拟载波监听机制是一样的，因此使用RTS帧和CTS帧进行信道预约，也属于虚拟载波监听机制。

利用虚拟载波监听机制，站点只要监听到数据帧、RTS帧或CTS帧中的任何一个，就能知道信道将被占用的持续时间，而不需要真正监听到信道上的信号，因此虚拟载波监听机制能减少隐蔽站带来的碰撞问题。



9.5. 无线局域网的MAC帧

数据帧	控制帧	管理帧
<ul style="list-style-type: none"> ● 用于在站点间传输数据 	<ul style="list-style-type: none"> ● 通常与数据帧搭配使用 ● 负责区域的清空、虚拟载波监听的维护以及信道的接入，并于收到数据帧时予以确认。 ● ACK帧、RTS帧以及CTS帧等都属于控制帧。 	<ul style="list-style-type: none"> ● 用于加入或退出无线网络，以及处理AP之间连接的转移事宜。 ● 信标帧、关联请求帧以及身份认证帧等都属于管理帧。

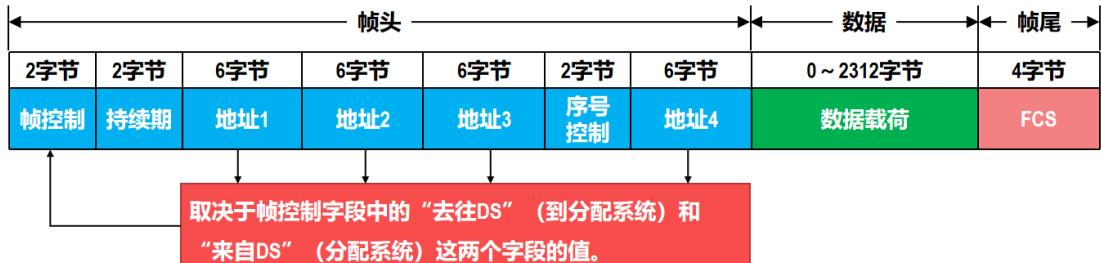


协议版本	类型	子类型	去往DS	来自DS	更多分片	重试	功率管理	更多数据	WEP	顺序
2比特	2比特	4比特	1比特	1比特	1比特	1比特	1比特	1比特	1比特	1比特



用来实现802.11的可靠传输，对数据帧进行编号。

用于实现CSMA/CA的虚拟载波监听和信道预约机制。在数据帧、RTS帧和CTS帧中用该字段指出将要持续占用信道的时长。



802.11无线局域网数据帧地址字段的4种使用情况

去往DS	来自DS	地址1	地址2	地址3	地址4
0	0	目的地址	源地址	BSSID	未被使用
0	1	目的地址	发送AP地址	源地址	未被使用
1	0	接收AP地址	源地址	目的地址	未被使用
1	1	接收AP地址	发送AP地址	目的地址	源地址

10. 题目

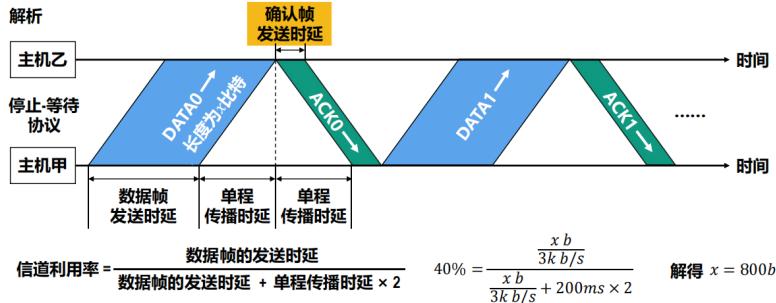
从滑动窗口的角度对比停止-等待协议、回退N帧协议和选择重传协议

停止-等待协议	回退N帧协议	选择重传协议
仅用1个比特给分组编号 $W_T = 1$ $W_R = 1$	用 $n(n > 1)$ 个比特给分组编号 $1 < W_T \leq (2^n - 1)$ $W_R = 1$	用 $n(n > 1)$ 个比特给分组编号 W_R 超过 W_T 没有意义 $1 < W_R \leq W_T$ $W_T + W_R \leq 2^n$ 确保接收窗口向前滑动后，落入接收窗口内的新序号与之前的旧序号没有重叠，避免无法分辨新旧数据分组。 当 W_R 取最大值 $2^{(n-1)}$ 时， W_T 能取到的最大值也为 $2^{(n-1)}$ 。

停止等待协议

【2018年题36】主机甲采用停-等协议向主机乙发送数据，数据传输速率是3kbps，单向传播延时是200ms，忽略确认帧的传输延时。当信道利用率为40%时，数据帧的长度为（D）。

- A. 240比特 B. 400比特 C. 480比特 D. 800比特

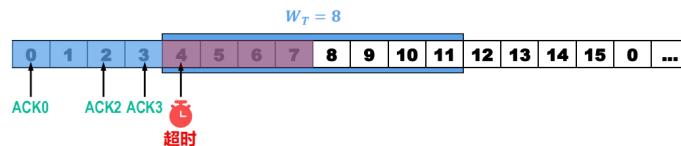


回退N帧协议

【2009年题35】数据链路层使用后退N帧（GBN）协议，发送方已经发送了编号0~7的帧。当计时器超时时，若发送方只收到了0、2、3号帧的确认，则发送方需要重发的帧数是（C）。

- A. 2 B. 3 C. 4 D. 5

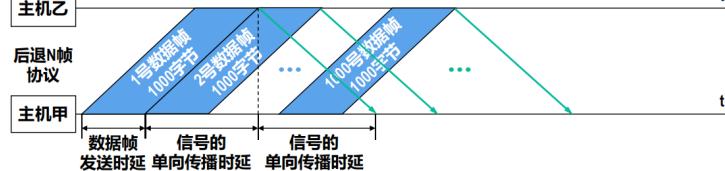
解析



【2014年题36】主机甲与主机乙之间使用后退N帧（GBN）协议传输数据，甲的发送窗口尺寸为1000，数据帧长为1000字节，信道带宽为100Mbps，乙每收到一个数据帧就立即利用一个短帧（忽略其传输延迟）进行确认，若甲乙之间的单向传播延迟是50ms，则甲可以达到的最大平均数据传输速率约为（C）。

- A. 10Mbps B. 20Mbps C. 80Mbps D. 100Mbps

解析



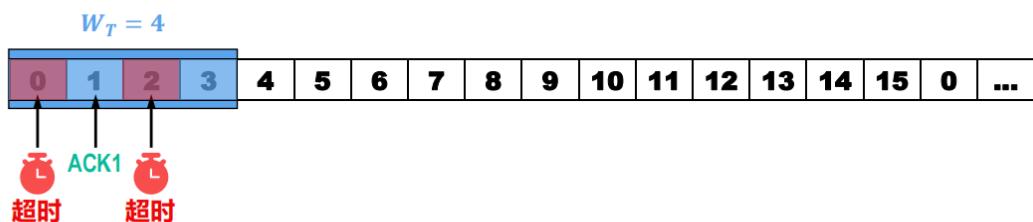
$$\begin{aligned} \text{甲可以达到的最大平均数据传输速率} &\approx \frac{\text{可发送的数据量}}{\text{(数据帧的发送时延} + \text{信号的单向传播时延} \times 2)} \\ &\approx \frac{(1000 \times 8) \times 1000}{((1000 \times 8) \div (100 \times 10^6) + (50 \times 10^{-3}) \times 2)} \\ &\approx 80Mbps \end{aligned}$$

选择重传协议

【2011年题35】数据链路层采用选择重传协议（SR）传输数据，发送方已发送了0~3号数据帧，现已收到1号帧的确认，而0、2号帧依次超时，则此时需要重传的帧数是（B）。

- A. 1 B. 2 C. 3 D. 4

解析



与回退N帧协议不同，选择重传协议不采用累积确认，接收方需要对每一个正确接收的数据分组进行逐一确认。

发送方仅重传未收到确认而超时的数据帧，因此重传0号和2号这两个数据帧。

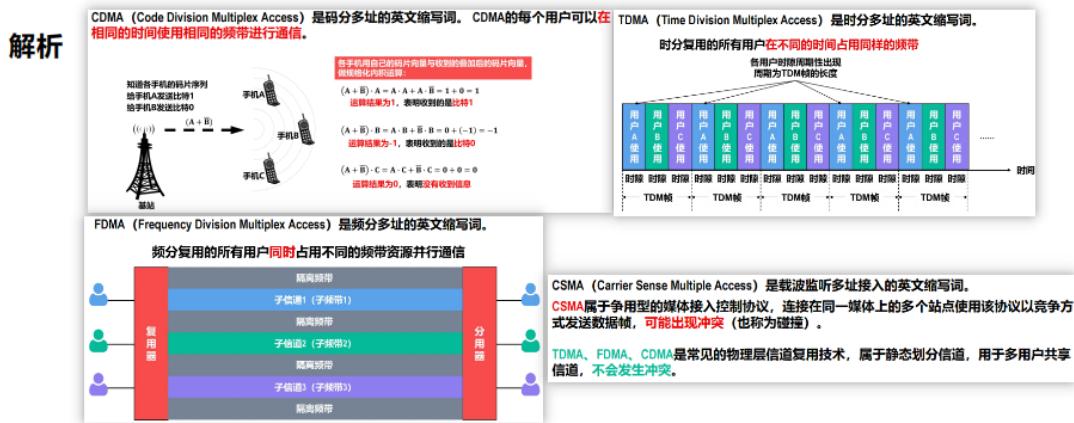
【2018年题34】下列选项中，不属于物理层接口规范定义范畴的是（C）。

- | | |
|---------|---------------------------------|
| A. 接口形状 | 物理层接口的机械特性 |
| B. 引脚功能 | 物理层接口的功能特性 |
| C. 物理地址 | 数据链路层使用的地址 又称为硬件地址或MAC地址 |
| D. 信号电平 | 物理层接口的电气特性 |

- CDMA

【2013年题36】下列介质访问控制方法中，可能发生冲突的是（B）。

- A. CDMA B. CSMA C. TDMA D. FDMA



- 争用期

【2010年题47】某局域网采用CSMA/CD协议实现介质访问控制，数据传输速率为10Mbps，主机甲和主机乙之间的距离为2km，信号传播速度是200 000km/s。请回答下列问题，要求说明理由或写出计算过程。

- (1) 若主机甲和主机乙发送数据时发送冲突，则从开始发送数据时刻起，到两台主机均检测到冲突时刻止，最短需经过多长时间？最长需经过多长时间（假设主机甲和主机乙发送数据过程中，其他主机不发送数据）？

解析



最短需要经过的时长：两主机之间信号的单程传播时延，记为 τ 。

最长需要经过的时长：两主机之间信号的往返传播时延，记为 2τ 。

$$\tau = \frac{2\text{km}}{200000\text{km/s}} = 10^{-5} \text{s}$$

- 最小帧长

【2009年题37】在一个采用CSMA/CD协议的网络中，传输介质是一根完整的电缆，传输速率为1Gbps，电缆中的信号传播速度是200 000km/s。若最小数据帧长度减少800比特，则最远的两个站点之间的距离至少需要 (D)

- | | | | |
|-----------|----------|-----------|----------|
| A. 增加160m | B. 增加80m | C. 减少160m | D. 减少80m |
| 排除 | 排除 | | |

解析

$$\text{最小帧长} = \text{数据传输速率} \times \text{争用期}2\tau$$

设最远两个站点之间的距离为 $d(m)$ ，最小帧长为 $l(b)$ ，

与题目给定相关已知量一起代入上式：

$$l = \left(\frac{d}{200000 \times 10^3} \times 2 \right) \times 10^9 \longrightarrow d = \frac{l}{10}$$

显然，若最小帧长减少800比特，最远的两个站点之间的距离至少需要减少80m。

- 共享式以太网的信道利用率

【2015年题36】下列关于CSMA/CD协议的叙述中，错误的是 (B)。

- A. 边发送数据帧，边检测是否发生冲突
- B. 适用于无线网络，以实现无线链路共享
- C. 需要根据网络跨距和数据传输速率限定最小帧长
- D. 当信号传播延迟趋近于0时，信道利用率趋近100%

解析

选项A的描述正确，其所描述的是CSMA/CD协议中的“碰撞检测（冲突检测）CD”。

选项B的描述错误，因为CSMA/CD协议不适用于无线网络。对于802.11无线局域网，可以使用CSMA/CA协议。

选项C的描述正确，因为“最小帧长 = 数据传输速率 × 争用期 2τ ”。也就是说，最小帧长取决于数据传输速率和争用期 2τ 。选项C中给出的“网络跨距”相当于给出了“端到端单程传播时延 τ ”，进而可得出“争用期 2τ ”。

选项D的描述正确，因为选项D中给出“信号传播延迟趋近于0”，这相当于信号瞬间到达整个网络，网络中各站点瞬间就知道总线被占用，因此不会出现碰撞，进而使信道利用率趋近100%。

- 10BASE-T

【2019年题34】100BaseT快速以太网使用的导向传输介质是 (A)。

- A. 双绞线
- B. 单模光纤
- C. 多模光纤
- D. 同轴电缆

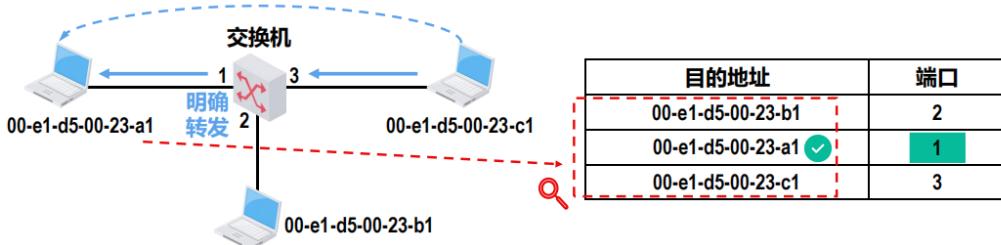
解析



- 以太网交换机

[2014年 题34] 某以太网拓扑及交换机当前转发表如下图所示，主机00-e1-d5-00-23-a1向主机00-e1-d5-00-23-c1发送1个数据帧，主机00-e1-d5-00-23-c1收到该帧后，向主机00-e1-d5-00-23-a1发送1个确认帧，交换机对这两个帧的转发端口分别是 (B)。

- A. {3}和{1} B. {2, 3}和{1} C. {2, 3}和{1, 2} D. {1, 2, 3}和{1}



解析

交换机转发数据帧的端口为{2, 3}
交换机转发确认帧的端口为{1}

[2009年 题36] 以太网交换机进行转发决策时使用的PDU地址是 (A)。

- A. 目的物理地址 B. 目的IP地址 C. 源物理地址 D. 源IP地址

解析

PDU (Protocol Data Unit) 的意思是**协议数据单元**，它是计算机网络体系结构中对等实体间逻辑通信的对象。

以太网交换机工作在数据链路层（包括物理层），它接收并转发的PDU通常称为**帧**。以太网交换机收到帧后，在转发表中查找帧的**目的MAC地址**所对应的接口号，然后通过该接口转发帧。

MAC地址又称为硬件地址或物理地址。请注意：不要被“物理”二字误导认为物理地址属于物理层范畴，物理地址属于数据链路层范畴。

[2013年 题38] 对于100Mbps的以太网交换机，当输出端口无排队，以直通交换 (cut-through switching) 方式转发一个以太网帧（不包括前导码）时，引入的转发延迟至少是 (B)。

- A. 0μs B. 0.48μs C. 5.12μs D. 121.44μs

解析

以太网帧格式	目的MAC地址 6B	源MAC地址 6B	类型 2B	数据载荷 46B~1500B	FCS 4B
--------	---------------	--------------	----------	-------------------	-----------

物理层在发送以太网帧之前还要在其前面添加8B的前导码。

题目给定：输出端口无排队 直通交换 不包括前导码

可以推出：只要接收完以太网帧的目的MAC地址就可以将帧直接转发到目的端口，而不缓存帧也不检验帧。

引入的**最小转发延迟**就是接收完目的MAC地址所耗费的时间。

$$\frac{6 \times 8}{100 \times 10^6} = 0.48(\mu\text{s})$$

- 共享式以太网与交换式以太网的对比

[2015年 题37] 下列关于交换机的叙述中，正确的是 (A)。

- A. 以太网交换机本质上是一种多端口网桥 叙述正确
B. 通过交换机互连的一组工作站构成一个冲突域
C. 交换机每个端口所连网络构成一个独立的广播域
D. 以太网交换机可实现采用不同网络层协议的网络互联

解析

网桥 (bridge) 工作在数据链路层（包含其下的物理层），因此**网桥具备属于数据链路层范畴的相关能力**。

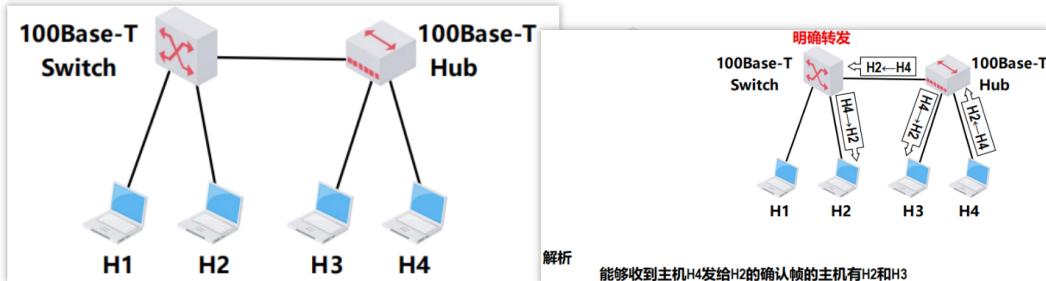
网桥的**接口数量很少**，通常只有2~4个，一般只用来**连接不同的网段**。

1990年面世的**交换式集线器** (Switching Hub)，实质上是**具有多个接口的网桥**，常称为**以太网交换机** (Switch) 或**二层交换机**。



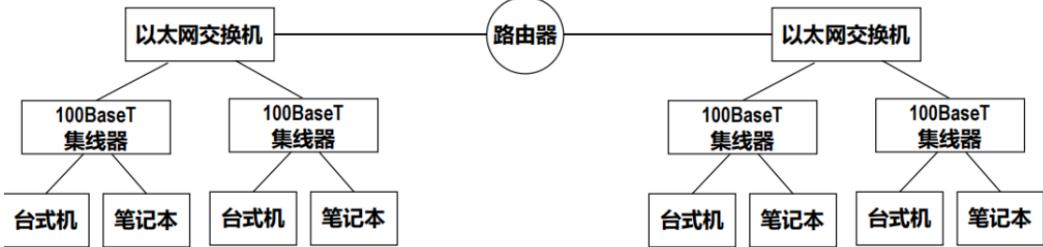
【2016年题35】若下图中的主机H2向主机H4发送1个数据帧，主机H4向主机H2立即发送一个确认帧，则除H4外，从物理层上能够收到该确认帧的主机还有（D）。

- A. 仅H2 B. 仅H3 C. 仅H1、H2 D. 仅H2、H3



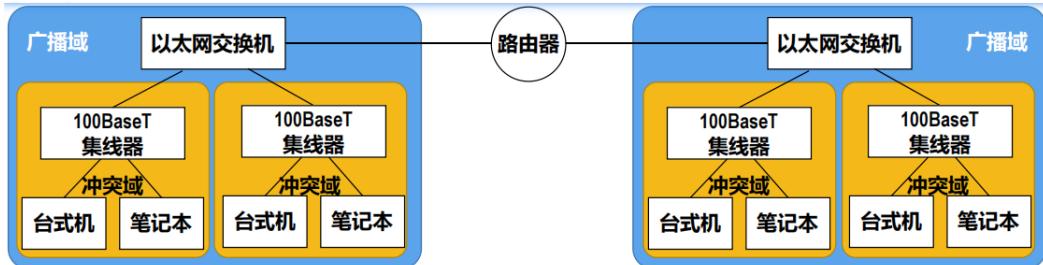
【2020年题35】在下图所示的网络中，冲突域和广播域的个数分别是（C）。

- A. 2, 2 B. 2, 4 C. 4, 2 D. 4, 4



解析

	隔离冲突域	隔离广播域
集线器	✗	
交换机	✓	
路由器		✗



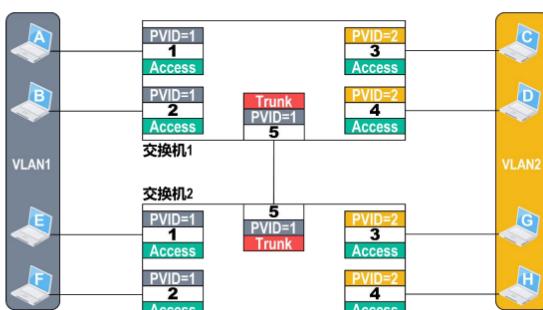
- 虚拟局域网VLAN的实现机制

【练习1】以下关于VLAN的描述中，错误的是（D）。

- A. 从数据链路层的角度看，不同VLAN中的站点之间不能直接通信。
- B. 属于同一个VLAN中的两个站点可能连接在不同的交换机上。
- C. 虚拟局域网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。
- D. VLAN使用的802.1Q帧的最大长度为1518字节。

【练习2】如右图所示，在交换机1和2上进行了VLAN划分，PVID是交换机端口的本征VLAN，Access和Trunk是交换机的接口类型，以下说法正确的是（C）。

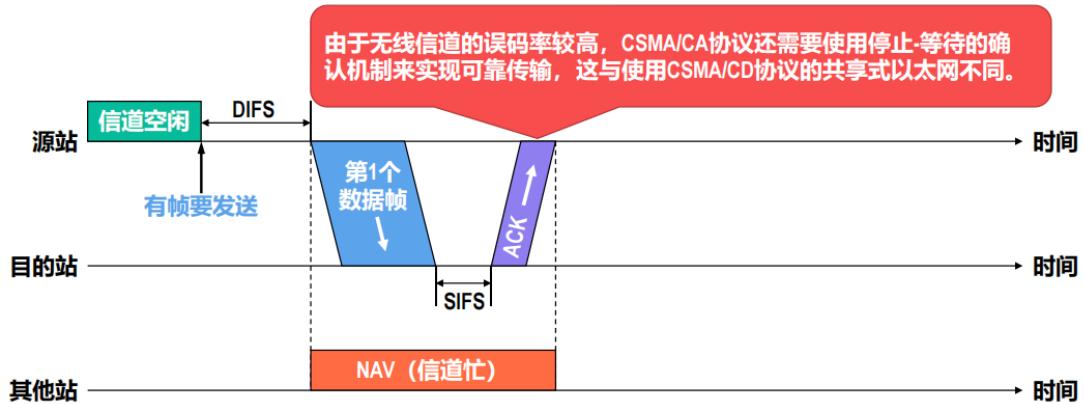
- A. B可以收到H发给B的单播帧
- B. E可以收到D发送的广播帧
- C. 能收到C发送的广播帧的有D、G和H
- D. 能收到E发送的广播帧的有A、B、F、G和H



- CSMA/CA协议的基本工作原理

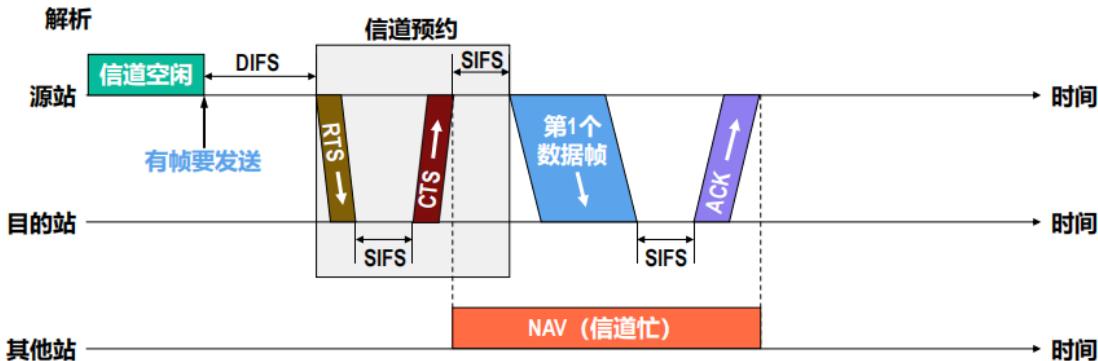
【2011年 题36】下列选项中，对正确接收到的数据帧进行确认的MAC协议是（D）。

- A. CSMA B. CDMA C. CSMA/CD D. CSMA/CA



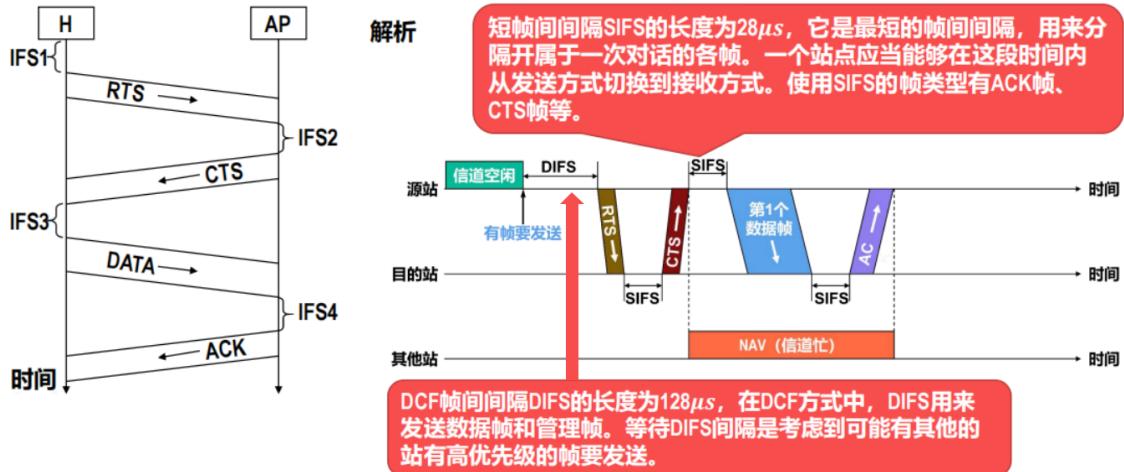
【2018年 题35】IEEE 802.11无线局域网的MAC协议CSMA/CA进行信道预约的方法是（D）。

- A. 发送确认帧 B. 采用二进制指数退避
C. 使用多个MAC地址 D. 交换RTS和CTS帧



【2020年 题37】某IEEE 802.11无线局域网中主机H与AP之间发送或接收CSMA/CA帧的过程如下图所示，在H或AP发送帧前所等待的帧间间隔时间（IFS）中最长的是（A）。

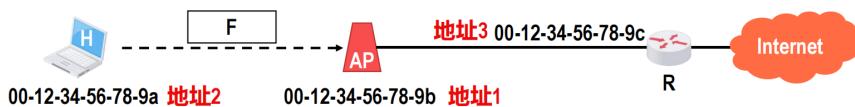
- A. IFS1 B. IFS2 C. IFS3 D. IFS4



- 802.11无线局域网的MAC帧

【2017年 题35】在下图所示的网络中，若主机H发送一个封装访问Internet的IP分组的IEEE 802.11数据帧F，则帧F的地址1、地址2和地址3分别是（**B**）。

- A. 00-12-34-56-78-9a, 00-12-34-56-78-9b, 00-12-34-56-78-9c B. 00-12-34-56-78-9b, 00-12-34-56-78-9a, 00-12-34-56-78-9c
 C. 00-12-34-56-78-9b, 00-12-34-56-78-9c, 00-12-34-56-78-9a D. 00-12-34-56-78-9a, 00-12-34-56-78-9c, 00-12-34-56-78-9l



解析

802.11无线局域网数据帧地址字段的4种使用情况

去往DS	来自DS	地址1	地址2	地址3	地址4
0	0	目的地址	源地址	BSSID	未被使用
0	1	目的地址	发送AP地址	源地址	未被使用
1	0	接收AP地址	源地址	目的地址	未被使用
1	1	接收AP地址	发送AP地址	目的地址	源地址