

五、链路层

在链路层中，有两种截然不同类型的链路层信道。

- 广播信道，需要所谓的媒体访问协议来协调传输和避免碰撞
 - 点对点通信，需要解决成帧、可靠数据传输、差错检测和流量控制
-

1. 链路层：概述和服务

将主机和路由器称为节点。交换机不被称为节点，因为它对于主机和路由器来说是透明的

链路层提供的服务

链路层协议用来在独立的链路上移动数据报

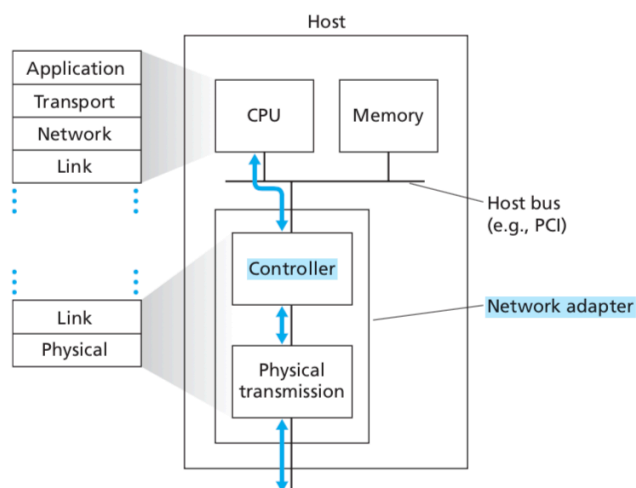
链路层的一个重要特点是数据报在路径的不同链路上可能由不同链路层协议所承载。而这些链路层协议所提供的服务可能是不同的

链路层协议可能提供的服务包括：

- 成帧（framing）
- 链路接入（link access）。媒体访问控制（Medium Access Control, MAC）协议规定了帧在链路上传输的规则
- 可靠交付（reliable delivery）。对于低比特差错的链路（光纤、同轴电缆），可靠交付是一个不必要的开销
- 流量控制
- 差错检验
- 差错纠正
- 半双工和全双工

链路层在何处实现

链路层的主体部分是在网络适配器（network adapter）中实现的，网络适配器也称为网络接口卡（Network Interface Card, NIC）。网络适配器的内核是链路层控制器，该控制器通常是实现了许多链路层服务的芯片

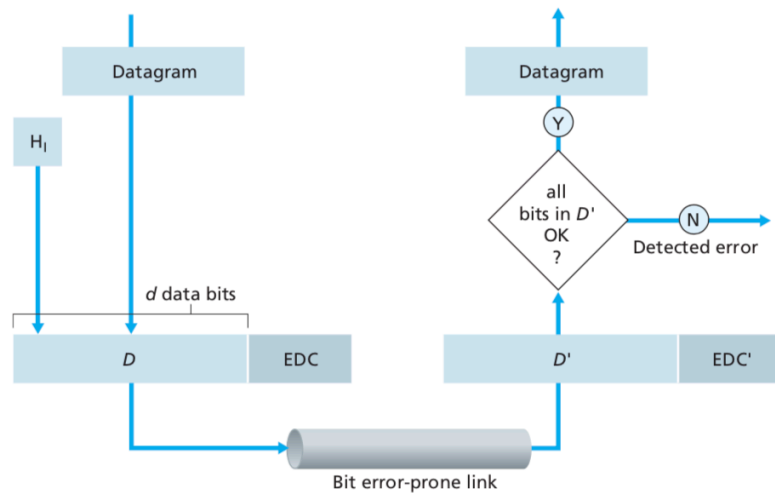


- 在发送方，控制器取得了由协议栈较高层生成并存储在主机内存中的数据报，在链路层帧中封装该数据报，然后遵循链路层接入协议将该帧传进通信链路中
- 在接收方，控制器接收整个帧，提取出网络层数据报

链路层也有软件，它通常实现了较高层次的链路层功能。所以，链路层是一种硬件和软件的结合体

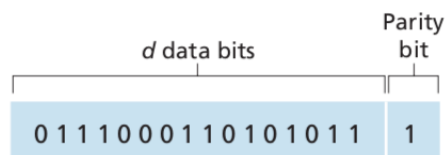
2. 差错检测和纠错技术

- 在发送节点，为了避免比特差错，使用差错检测和纠错比特（error-detection and-correction, EDC）来增强数据D。通常，要保护的数据不仅包括从网络层传递下来的数据，而且包括链路帧首部字段
- 在接收节点，接收到比特序列 D' 和 EDC' ，需要判断它们和初始值是否相同。但即使有纠正技术，也还是可能有未检出的比特差错



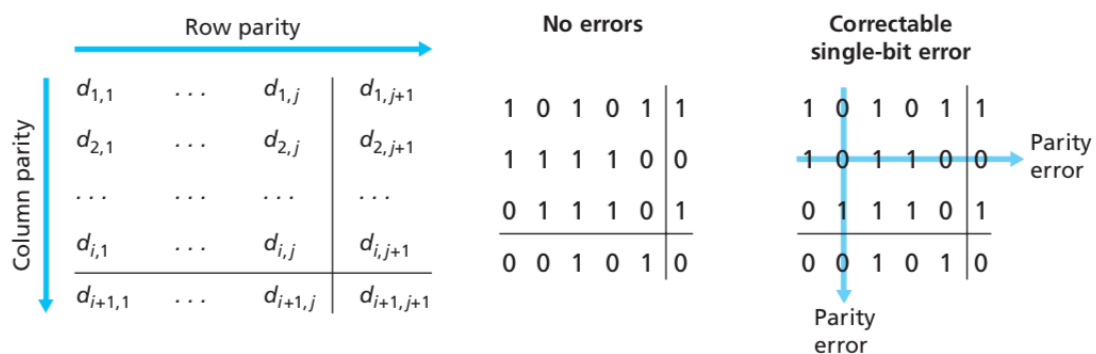
奇偶校验

使用单个奇偶校验位（parity bit），使得 $d + 1$ 个比特中1的个数是奇数/偶数个



显然，这种方法无法检测出偶数个的比特差错。而且，比特差错经常以突发（burst）的方式聚集在一起

奇偶校验可以扩展到二维。假如出现了单个比特差错，这种二维奇偶校验可以检测到差错的位置，从而纠正



接收方检测和纠正差错的能力被称为前向纠错（Forward Error Correction, FEC）

检验和方法

和传输层的checksum相同。但实际上，链路层使用的是CRC

为什么传输层使用checksum而链路层使用CRC? 因为传输层差错检测是用软件实现的，链路层差错检测是在硬件中实现的，它能够更快速地执行更复杂的操作

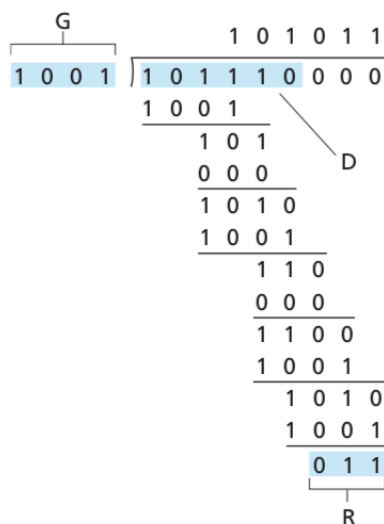
循环冗余校验 (Cyclic Redundancy Check, CRC)

- 发送方和接收方首先协商一个 $r + 1$ 比特生成多项式 (generator)，记为 G ，它的最高有效位为1
- 对于即将要发送的、长度为 d 比特的数据 D ，我们要在它的后面添加 r 个比特的数据 R ，所以传输的数据长度变为 $d + r$
- R 是怎么计算的?

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

$D \cdot 2^r$ 相当于把 D 左移 r 位。注意，这一步计算中的加法和减法是模2算术，它等价于按位异或 (XOR)

例子: $D = 101110, G = 1001$, R 的计算结果为011, 所以发送的数据为101110011



在除法的计算过程中， $1010 - 1001$ 的结果本来应该是1，但是因为是模2算术，不会有进位和借位，等价于按位异或，所以 $1010 \text{ XOR } 1001 = 0011$

假如是 $1000 \div 1001$ 怎么办? 除法结果仍然为1，否则最高位的1永远消除不了

3. 多路访问协议

广播链路，能够让多个发送和接收节点都连接到相同的、单一的、共享的广播信道上

广播的意思是，任何一个节点传输一个帧时，其他每个节点都会收到一个拷贝。以太网和WLAN是广播链路层的技术例子

节点通过多路访问协议（multiple access protocol）来规范它们在共享的广播信道上的传输行为

因为所有节点都能传输帧，两个以上的节点可能会同时传输帧，在接收方会碰撞（collide）。碰撞帧的信号纠缠在一起，所有涉及此次碰撞的帧都会丢失

多路访问协议可以划分为三类：信道划分协议、随机接入协议、轮流协议

我们希望多路访问协议能够具有的特性：

- 1) 当只有一个节点有数据发送时，该节点具有 R bps的吞吐量。
- 2) 当有 M 个节点要发送数据时，每个节点吞吐量为 R/M bps。不必要求 M 个节点中的每一个节点总是有 R/M 的瞬间速率，而是每个节点在一些适当定义的时间间隔内应该有 R/M 的平均传输速率。
- 3) 协议是分散的，这就是说不会因某主节点故障而使整个系统崩溃。
- 4) 协议是简单的，使得实现起来代价不是很高。

信道划分协议

时分多路复用（TDM）：公平，消除了碰撞；但是节点被限制于 R/N bps的平均速率，且节点必须总是等待它在传输序列中的轮次，即使它是唯一一个有帧要发送的节点

频分多路复用（FDM）：公平，消除了碰撞；但是带宽被限制

码分多址（Code Division Multiple Access, CDMA）：CDMA为每个节点分配一种不同的编码，然后每个节点用它唯一的编码来对它发送的数据进行编码

随机接入协议

一个传输节点总是以信道的全部速率（ R bps）进行发送。当有碰撞时，涉及碰撞的每个节点反复地重发它的帧，直到该帧无碰撞地通过为止

但是当一个节点经受一次碰撞时，它不必立刻重发该帧。相反，它在重发该帧之前等待一个随机时延

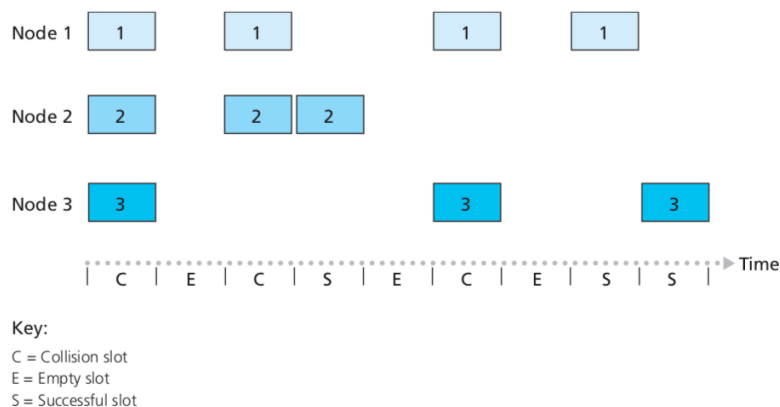
Slotted ALOHA

我们做如下假设：

- 所有帧由恰好 L 比特组成。
- 时间被划分为长度为 L/R s的时隙（这就是说，一个时隙等于传输一帧的时间）。
- 节点只在时隙起点开始传输帧。
- 节点是同步的，每个节点都知道时隙何时开始。
- 如果在一个时隙中有两个或者更多个帧碰撞，则所有节点在该时隙结束之前检测到该碰撞事件。

令 p 是一个概率，即一个在0和1之间的数。每个节点的时隙ALOHA操作是简单的：

- 当该节点有一个新帧要发送时，它等到下一个时隙开始并在该时隙传输整个帧。
- 如果没有碰撞，该节点成功地传输它的帧，从而不需要考虑重传该帧。（如果该节点有新帧要传输，它能够为传输准备新帧。）
- 如果有碰撞，该节点在该时隙结束之前检测到这次碰撞。该节点以概率 p 在后续的几个时隙中重传它的帧，直到该帧被无碰撞地传输出去。



对于 N 个节点，任意一个节点成功传输的概率是 $Np(1-p)^{N-1}$

ALOHA

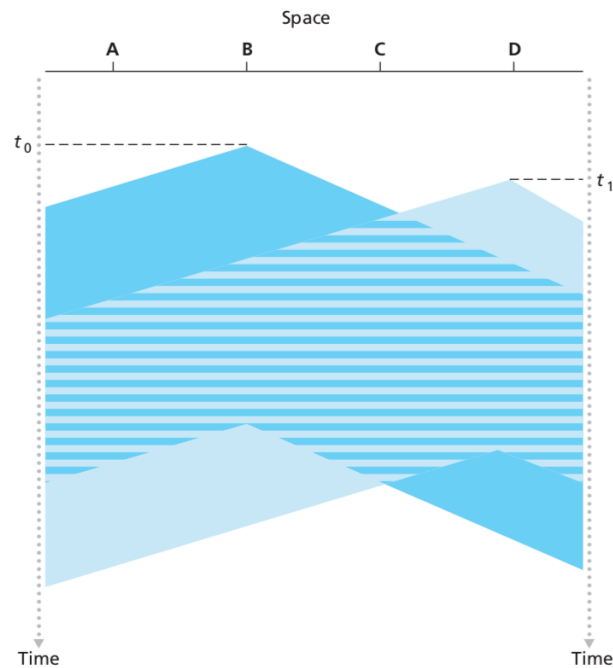
在纯ALOHA中，当一个帧首次到达，节点立刻将该帧完整地传输进广播信道。如果有碰撞，这个节点立即（在完全传输完它的碰撞帧后）以概率 p 重传该帧。否则，该节点等待一个帧传输时间，之后以概率 p 重传，或以概率 $1-p$ 等待另一个帧时间

一个给定节点成功传输一次的概率是 $p(1 - p)^{2(N-1)}$

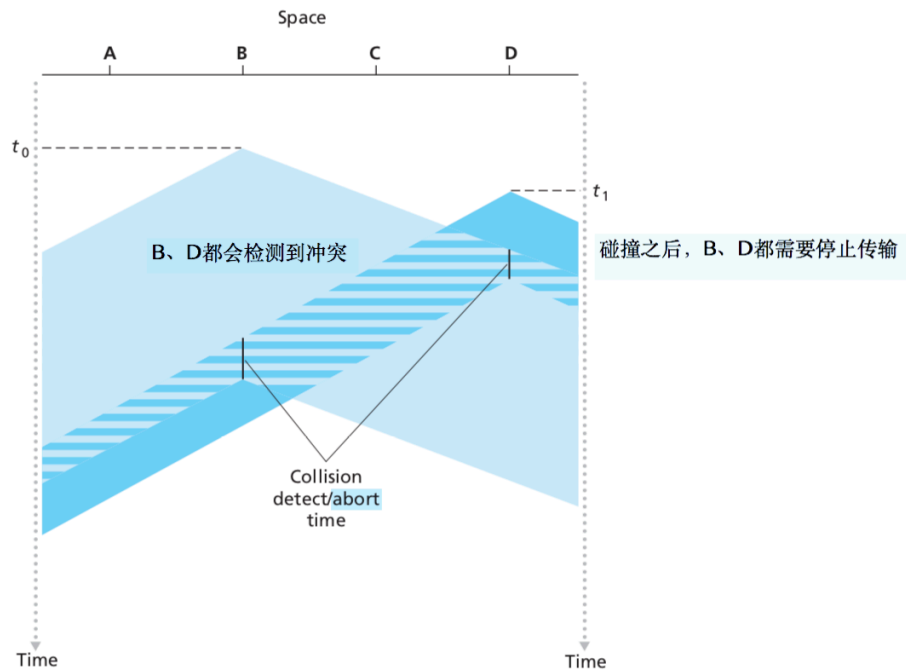
载波侦听多路访问 (Carrier Sense Multiple Access, CSMA)

- 载波侦听：一个节点在传输前 先听信道，看是否有其他节点正在发送数据
- 碰撞检测：一个传输节点在传输时一直在侦听信道。假如检测到另一个节点正在传输干扰帧，就停止传输

假如所有节点都进行载波侦听了，为什么会有碰撞？因为有信道传播时延



在上图中，尽管B和D检测到了碰撞，但是仍然继续发送剩余的比特，这是不必要的。具有碰撞检测的CSMA（CSMA with **Collision Detection**, CSMA/CD）可以解决这个问题



轮流协议

- 轮询协议。它要求某一个节点被指定为主节点，主节点以循环的方式轮询每个节点。PAN（Personal Area Network）
- 令牌传递协议。没有主节点，但有一个令牌，这是一个特殊目的帧，它会在节点之间以某种固定的次序来进行交换

局域网

早期有两类LAN技术很流行，1. 令牌环 2. 光纤式分布数据接口（FDDI）

- 令牌环LAN：LAN的N个节点通过直接链路连接成一个环。当某个节点获得了令牌并发送一个帧时，该帧围绕整个环传播，从而创建了一个虚拟广播信道。当该帧传播过来时，目的节点从链路层媒体中读取该帧。发送该帧的节点有责任从环中去除这个帧
- FDDI LAN：为地理范围更大的LAN设计。FDDI让目的节点去除这个帧