CH6 链路层和局域网

一、绪论

1. 网络节点的连接方式

- 点到点连接
- 多点连接（共享型介质，通过网络交换机）

2. WAN和LAN的连接方式

WAN：网络形式采用点到点链路

带宽大、距离远、带宽时延积大。

LAN：采用多点连接

连接节点非常方便，接到共享介质（或网络交换机）上就可以连接所有其他节点

点到点连接和多点连接的区别：

多点连接：冲突代价大，通过令牌来协调代价大

点到点链路的链路层服务实现简单，封装和解封装

多点连接方式网路的链路层功能实现复杂。

- 多点接入：协调各节点对共享性介质的访问和使用
- 竞争方式：冲突之后的协调
- 令牌方式：令牌产生，占有和释放等。

3. 术语

- 主机、路由器、网桥、交换机是节点：Nodes
- 沿着通信路径，连接各相邻节点通信信道的是链路：Links
- 第二层协议数据单元帧frame，封装数据报

4. 链路层服务

数据链路层负责从一个节点通过链路将帧中的而数据报发送到相邻的物理节点。

- 将数据报封装在帧中，加上帧头、尾，在头部使用MAC地址（物理地址）来表示源和目的
- 在相邻两个节点完成可靠数据传递
- 在一个子网内进行可靠的转发
- 流量控制
- 错误检测（差错由信号衰减和噪声引起，通过重发帧或丢弃帧修复）
- 差错纠正
- 半双工和全双工
    - 半双工：链路可以双向传输，但一次只有一个方向

5. 链路层实现位置

在每一个主机上、路由器上、交换机的端口上、适配器/芯片组/网卡上实现

适配器通信：

- 发送方：在帧中封装数据报，加上差错控制编码，实现rdt和流量控制
- 接收方：检查有无差错，执行rdt和流量控制功能，解封数据报，交给上层

二、差错检验和纠正

1. 错误检测

EDC：差错检查和纠正位（冗余位）

D：数据由差错检测保护，可以包含头部字段

不是100%可靠，更长的EDC字段可以得到更好的检测和纠正效果

2. 奇偶校验

一维奇偶校验：`parity = ^in`

二维奇偶校验：`parityRow[i] = ^in[i];parityCol[i] = ^in[:, i]`

3. Internet校验和

目标：检测在传输报文段时的错误（仅仅用于传输层）

检测发送方的报文段和接收方的报文段校验字段只和是否全1。

等等

三、多点访问协议

1. 多路访问链路和协议

- 点对点：拨号访问PPP，以太网交换机和主机之间的点对点链路
- 广播：传统以太网，HFC上行链路，802.11无线局域网

2. MAC协议简介

分布式算法决定节点如何使用共享信道。

3. 理想的多路访问协议

给定：R bps的广播信道

M个节点发送，每个节点使用R/M的平均速率发送

4. 分类

- 信道划分：分配片给每个节点专用
- 随机访问：不划分，允许冲突，冲突后恢复
- 依次轮流：节点依次轮流使用

5. 信道划分

TDMA

TDMA（time division multiple access）

轮流使用信道，信道的时间分为周期

不同时刻讲话

FDMA

FDMA（frequency division multiple access）

信道的有效频率范围被分成一个个小的频段

每个站点被分配一个固定的频段

不同房间讲话

CDMA

CDMA（code division multiple access）

所有的站点在整个频段上同时进行传输，采用编码原理夹以区分，完全无冲突（假定信号同步很好，线性叠加）

不同语言讲话

6. 随机访问协议

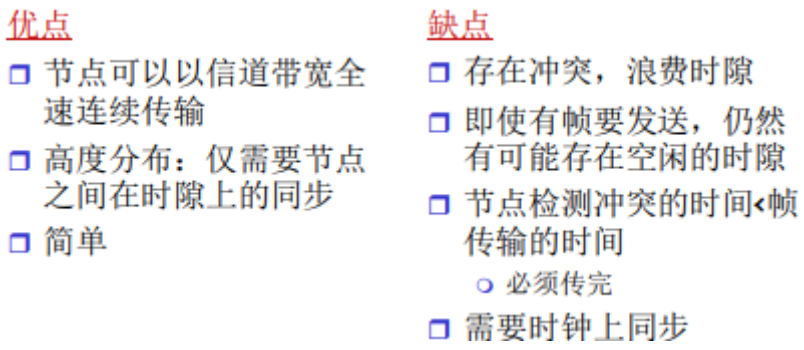
随机存取协议

节点有帧要发送时，以全部R带宽发送，没有节点间的预先协调

时隙ALOHA

假设：所有帧等长、每个时隙发送一帧、节点时钟上同步、两个以上节点在一个时隙传输，所有站点都能检测到冲突

- 节点获取新的帧，下一个时隙传输
- 传输时无冲突，成功
- 传输时有冲突，失败，帧随后重传直至成功



效率：假设一共N个节点，每个帧在每个时隙中传输概率为p

一个节点成功传输的概率为$p(1-p)^{N-1}$

任何一个节点的成功概率为$Np(1-p)^{N-1}$

最好信道利用率为$\lim_{N\to+\infty} \underset{p*\in[0,1]}{argmax} Np^*(1-p^*)^{N-1} = \frac{1}{e} = 0.37$

纯ALOHA

无需节点间在时间上同步，冲突概率增加

效率：概率为$p(1-p)^{2(N-1)}$，最佳信道利用率为$\frac{1}{2e}$

CSMA（载波侦听多路访问）

在传输前先侦听信道，空闲：传送整个帧；忙：推迟传送

由于传播延迟，两个节点可能侦听不到正在进行的传输，传播延迟决定冲突概率。

整个冲突帧的传输时间都被浪费。

CSMA/CD（冲突检测的载波侦听多路访问）

冲突检测技术：检测信号强度，比较传输与接收到的信号是否相同、通过周期的过零点检测

算法：

1. 适配器获取数据报，创建帧
2. 发送前：侦听信道CS
   1)闲：开始传送帧
   2)忙：一直等到闲再发送
3. 发送过程中，冲突检测CD
   1)没有冲突:成功
   2)检测到冲突:放弃,之后尝试重发
4. 发送方适配器检测到冲突，除放弃外，还发送一个Jam信号，所有听到冲突的适配器也是如此
   强化冲突：让所有站点都知道冲突
5. 如果放弃，适配器进入指数退避状态
   在第m次失败后，适配器随机选择一个{0，1，2，，2^m-1}中K，等待K*512位时，然后转到步骤2

指数退避：适配器试图适应当前负载。

第一次冲突：$K \in \{0,1\}$

第二次冲突：$K \in \{0,1,2,3\}$

第十次冲突：$K \in \{0,1,2,3,\cdots,1023\}$

效率：t_{prop}为LAN上2个节点的最大传播延迟，t_{trans}为传输最大帧的时间

$eff = \frac{1}{1+5t_{prop}/t_{trans}}$

$t_{prop} \to 0 \vee t_{trans} \to \infty$，$eff \to 1$

性能好、廉价、分布式

无线局域网中的MAC：CSMA/CA

802.11：CSMA - 发送前侦听信道，没有冲突检测。

无法检测冲突：自身信号远远大于其他节点信号

发送方：

- 站点检测到信道空闲持续帧间间隔长，则传输整个帧
- 如果信道忙碌，选择一个随机回退值，在信道空闲时让该值递减，到0时，发送整个帧，没有收到ACK，增加回退值，重复2

接收方：帧正确，帧间隔后发送ACK

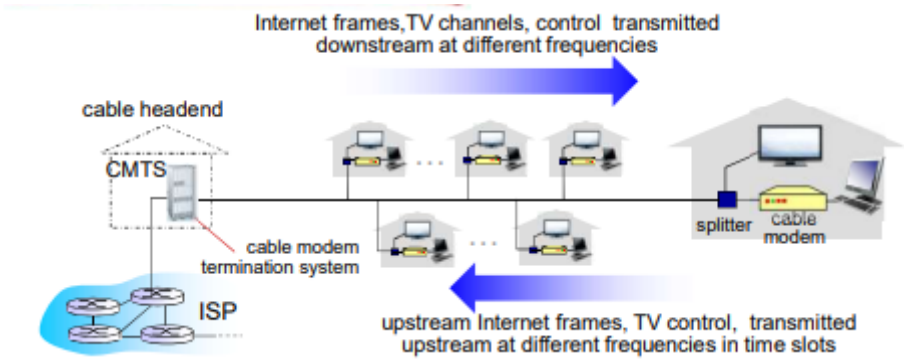
LAN CD：让发送节点发送完毕再立即发送，冲突代价不贵

WLAN CA：无法CD，一旦发送就必须发送完毕，冲突时信道浪费严重，代价高昂，故*事先避免冲突*，失败节点会冻结计数器，当胜利节点发完再发。

无法完全避免冲突：两个站点互相隐藏、选择了非常靠近的随机回退值

预约制：发送方发送一个小的Request-to-send（RTS）分组（即使冲突，代价低廉），BS广播clear-to-send（CTS）作为RTS的响应，CTS能够被所有涉及到的节点听到（发送方发送数据帧，其他节点抑制发送）。*可以完全避免冲突*。

线缆载入网络



7. 轮流MAC协议

轮询：主节点邀请从节点依次传送

令牌传递：控制令牌（token）循环从一个节点到下一个节点传递。

8. MAC协议总结

信道划分：TDMA、FDMA、CDMA

随机访问：ALOHA、S-ALOHA、CSMA（802.3 Ethernet使用）、CSMA/CD（802.11WLAN中使用）

依次轮流协议：集中（一个中心节点轮询）；分布（通过令牌控制）；蓝牙；FDDI；令牌环

四、有线局域网技术

1. MAC地址和ARP

LAN（MAC/物理/以太网）地址：

> 用于使帧从一个网卡传递到于其物理连接的另一个网卡（同一物理网络内）
>
> 48位MAC地址固化在适配器的ROM，有时也可通过软件设定
>
> 理论上全球任何两个网卡的MAC地址都不一样

mac地址为平面结构，可以完成物理网络内部节点到节点的数据交付，支持移动（IP不可以）

IP地址和mac地址分离

分离好处：可以应对网卡损坏情况，物理网络还可以支持其他网络层协议

捆绑问题：如果仅仅使用IP地址，那么网卡仅仅支持IP协议；反复重新写入IP地址；不使用mac地址，每到来一个帧都要上传至IP层次。

局域网上每个适配器都有一个唯一的LAN地址，如1A-2F-BB-76-09-AD。（广播地址：FF-FF-FF-FF-FF-FF）

mac地址由IEEE管理和分配，制造商购入mac地址空间。

ARP（Address Resolution Protocol）

通过IP地址获取mac地址：LAN上的每一个IP节点都有一个APR表（包括IP→mac的映射）【IP, MAC, TTL】

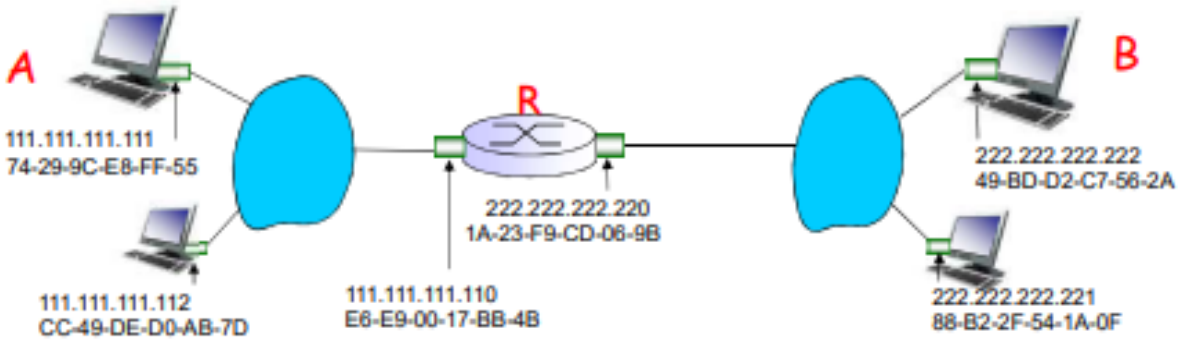
同一个网络下的发送：

A要发送帧给B，先广播（FF-FF-FF-FF-FF-FF）包含B的IP地址的ARP查询包，B收到查询包，回复自己的mac地址（用A的mac地址），A在自己的ARP表中，缓存(IP，MAC)映射关系，直至超时。

软状态：靠定期刷新维持的系统状态

ARP是即插即用的。节点自己创建ARP的表项，无需管理员干预。

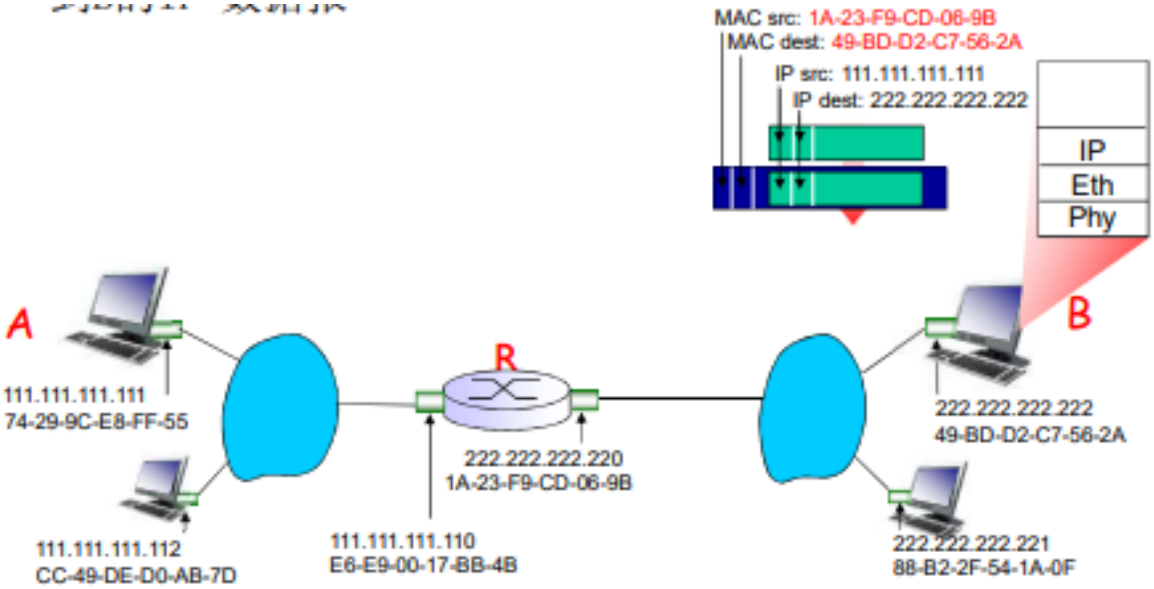
路由到其他IAN：



R上存在两个ARP表，分别对应两个LAN，（数据报封装在帧中）

A创建数据报（A，B），A的下一跳地址为（111.111.111.110，E6-E9-00-17-BB-4B）；

R转发数据报（A，B），下一跳地址为（222.222.222.22，49-BD-D2-C7-56-2A）；



2. Ethernet以太网

总线：所有的节点在一个碰撞域内，一次只允许一个节点发送；可靠性差。

星型：最主流。交换机在中间，每个节点以及相连的交换机端口使用以太网协议

以太帧：发送方适配器在以太网帧中封装IP数据报，或者其他网络层协议数据单元

> **前导码**：用来同步发送双方的时钟速率

> **地址**：6字节源mac地址，目标mac地址，只有帧的目标地址等于本站mac地址或广播地址时，传至网络层，否则忽略。

以太网是无连接（没有握手）、不可靠（出错没有反馈）的服务。

以太网的mac协议采用*二进制退避的CSMA/CD介质访问控制形式*（没有时隙）

3. 交换机

端口执行以太网协议，对帧进行存储和选择性转发，使用CSMA/CD进行接入控制，一个交换机端口一个独立网段。

主机对交换机的存在不关心。

交换机有MAC地址，无IP地址。

即插即用，自学习。

支持多路同时传输，没有碰撞。

交换表（主机MAC，该MAC对应的接口，TTL）

自学习

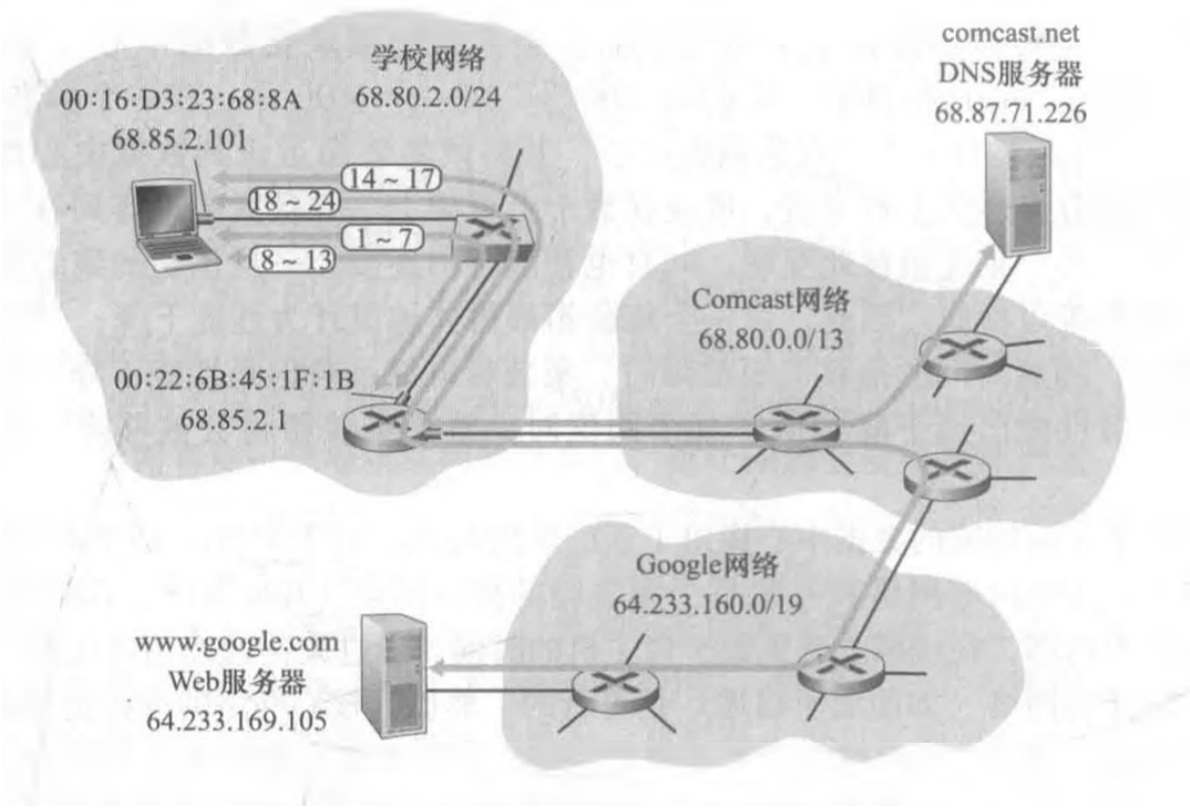
> 接收到帧时，交换机学习到发送站点所在的端口（网段）
>
> 记录发送方MAC地址/进入端口映射关系，在交换表中。

1）交换机表初始为空。

2）对于在每个接口接收到的每个入帧，该交换机在其表中存储：①在该帧源地址字段中的 MAC 地址；②该帧到达的接口；③当前时间。交换机以这种方式在它的表中记录了发送节点所在的局域网网段。如果在局域网上的每个主机最终都发送了一个帧，则每个主机最终将在这张表中留有记录。

3）如果在一段时间（称为老化期（aging time））后，交换机没有接收到以该地址作为源地址的帧，就在表中删除这个地址。以这种方式，如果一台 PC 被另一台 PC（具有不同的适配器）代替，原来 PC 的 MAC 地址将最终从该交换机表中被清除掉。

五、回顾Web网页请求过程



> 一台电脑通过以太网与学校的以太网交换机相连，交换机连接了一台路由器，该路由器连接到一个ISP中，该ISP提供了DNS服务，假设DHCP运行在路由器中。
>
> **网络配置：**该电脑的操作系统生成一个目的为广播地址255.255.255.0的**DHCP数据报**，封装为**UDP数据报**，然后封装为**IP数据报**，进一步封装为**以太帧**，目的mac地址为FF-FF-FF-FF-FF-FF，这个以太帧被广播，发送到所有交换机上，路由器也能接收到该以太帧，然后逐层解封，发现为DHCP请求，于是分配一个可用IP，和DNS服务器、默认网关路由器的IP地址和子网掩码封装好，按照来的路径发送回电脑，电脑的操作系统层层解封，获得IP地址，DNS服务器IP地址，默认网关路由器IP地址和子网掩码
>
> **获取目标IP**：该电脑操作系统生成一个包含源IP、DNS服务器IP、网址的**DNS查询报文**，发送至学校网的路由器，路由器生成**ARP查询报文**，广播至ISP，然后获取DNS服务器的MAC地址，然后路由器将通过路由算法，将DNS查询报文发送至DNS服务器，DNS将得到的目的IP地址并返回
>
> **发送请求：**该电脑生成一个HTTP GET请求，封装在**TCP数据报**中，向www.google.com发送，进行三次握手形成TCP连接，然后Web服务器将该网页的内容写入套接字，返回至电脑。

END