

# 计算机网络

---

计算机与信息学院

郑淑丽

Tel: 18919665418

Email: [ZSL251@163.com](mailto:ZSL251@163.com)

Office: 双子楼A604-2

## 课程内容

1. 概述
2. 网络体系
3. 物理层
4. 数据链路层
5. 网络层
6. 传输层
7. 应用层
8. 局域网与介质访问控制
9. 网络安全

# 两种类型链路

□ 点到点链路

□ 广播链路



shared wire (e.g.,  
cabled Ethernet)



shared RF  
(e.g., 802.11 WiFi)



shared RF  
(satellite)

■ 多台主机连接到**同一个、共享的广播信道**上

■ 广播？

——一台主机发送数据（帧），其他节点都能收到

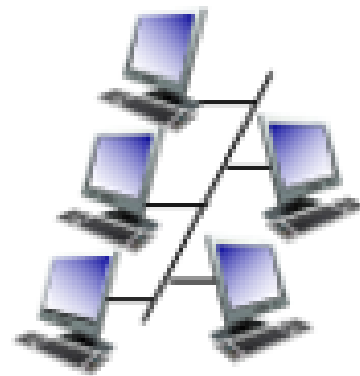
# 广播链路

---

□ 碰撞/冲突 (collision) : 多个节点同时发送帧, 这些帧相互干扰, 导致接收方都不能正确收到帧。

□ 如何协调多台主机之间的通信?

——多路访问问题

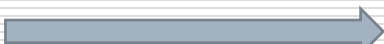


shared wire (e.g.,  
cabled Ethernet)

# 多路访问协议

---

## 1. 信道划分协议



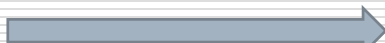
FDM、TDM、WDM、CDM

## 2. 随机接入协议



ALOHA、CSMA、.....

## 3. 轮流协议



轮询、令牌传递 (token)、预约.....

---

# 5.1 随机接入协议

---

## 1) ALOHA

ALOHAnet: 70年代, 无线网络, 连接了夏威夷群岛的大学, Norman.Albramson 设计了纯ALOHA协议。

——激励了Bob. Metcalfe, 修改了ALOHA协议, 设计了CSMA/CD协议, 并发明了以太网

---

# ALOHA

---

- 节点有数据，立即发送
  - 如碰撞，等待随机时间重发（每个节点等待的随机时间不同，降低第二次冲突的概率）
  - 负载增大，冲突加剧，吞吐率低
-

## 2) CSMA

---

□ 载波侦听多路访问 ( carrier sense multiple access )

- 局域网的特性
- 传输节点在发送数据前，先侦听信道



shared wire (e.g.,  
cabled Ethernet)



shared RF  
(e.g., 802.11 WiFi)



## 2) CSMA

---

□ 载波侦听多路访问 ( carrier sense multiple access )

■ 传输节点在发送数据前，先侦听信道

✓ 信道忙：等待

✓ 信道空闲：立即发送

——会不会产生碰撞？

---

# 三种CSMA

---

- 1-坚持CSMA：侦听到信道“忙”，持续侦听，一旦“空闲”，立即发送
  - 0-坚持CSMA：侦听到信道“忙”，等待一随机时间，重新侦听
  - P-坚持CSMA：侦听到信道“忙”，持续侦听，信道空闲，P概率发送， $(1-P)$ 概率延迟1个时隙进行侦听
-

## 5.2 局域网

---

### □ LAN: Local Area Network

- 将物理位置邻近的计算机连接起来，资源共享和信息交换，地理范围和主机数目均有限
  - IEEE802标准：局域网标准
-

802.1 参考模型

802.2 LLC

802.3 以太网

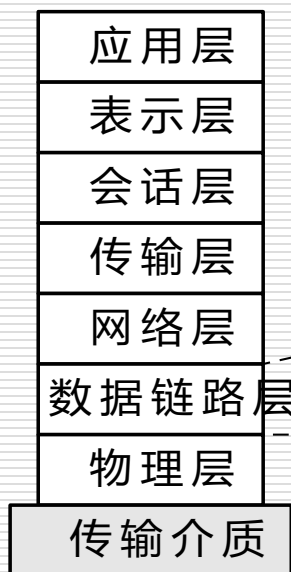
802.4 令牌总线网

802.5 令牌环网

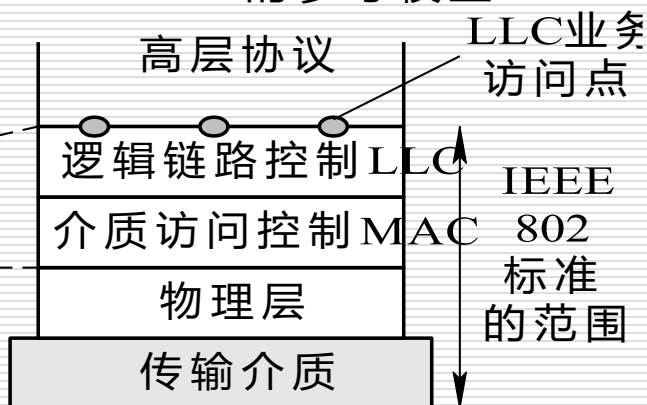
...

802.11 无线局域网

OSI参考模型



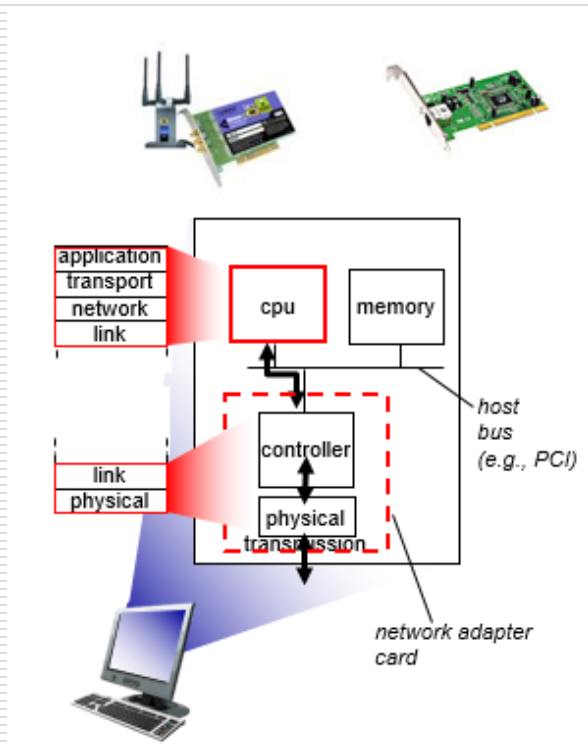
IEEE 802的参考模型



# 链路层协议与网卡

---

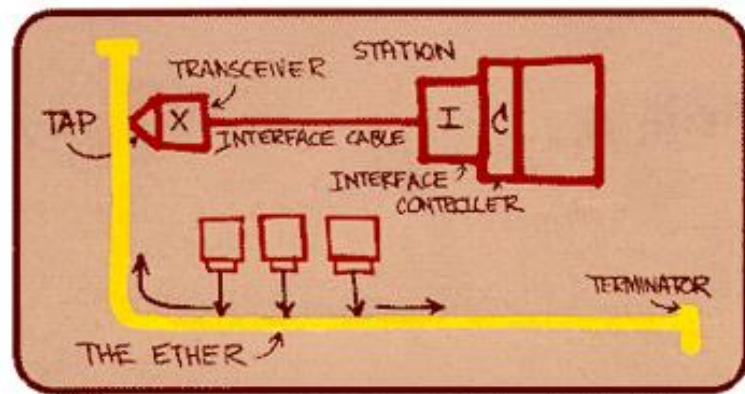
- ❑ 适配器（adapter）/网络接口卡（network interface card）



# 1) 以太网 (Ethernet)

---

- ❑ 以太网之父: Bob Metcalfe
- ❑ 1982, 第一个以太网规约 DIX Ethernet V2
- ❑ 1983, IEEE 802.3 标准



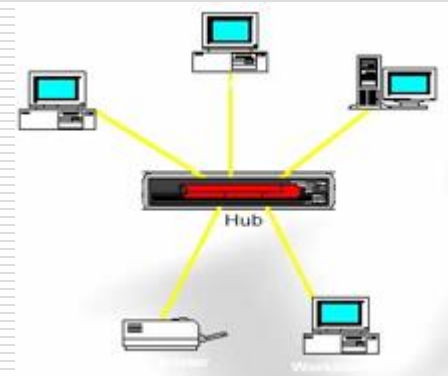
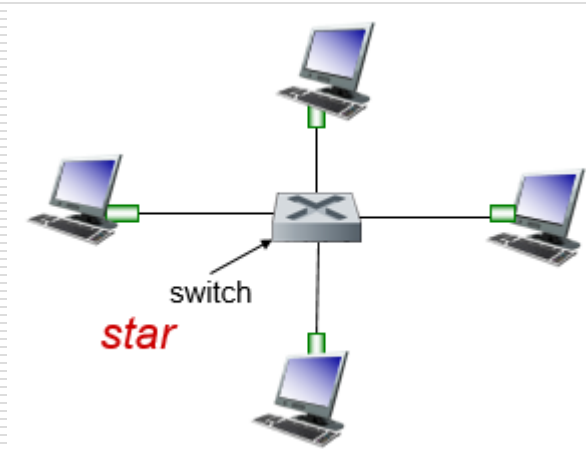
*Metcalfe's Ethernet sketch*

# 以太网拓扑结构

- ❑ 70年代中期~90年代中期：总线拓扑
- ❑ 90年代后期：星型拓扑，集线器
- ❑ 21世纪初：星型拓扑，交换机



*bus:* coaxial cable

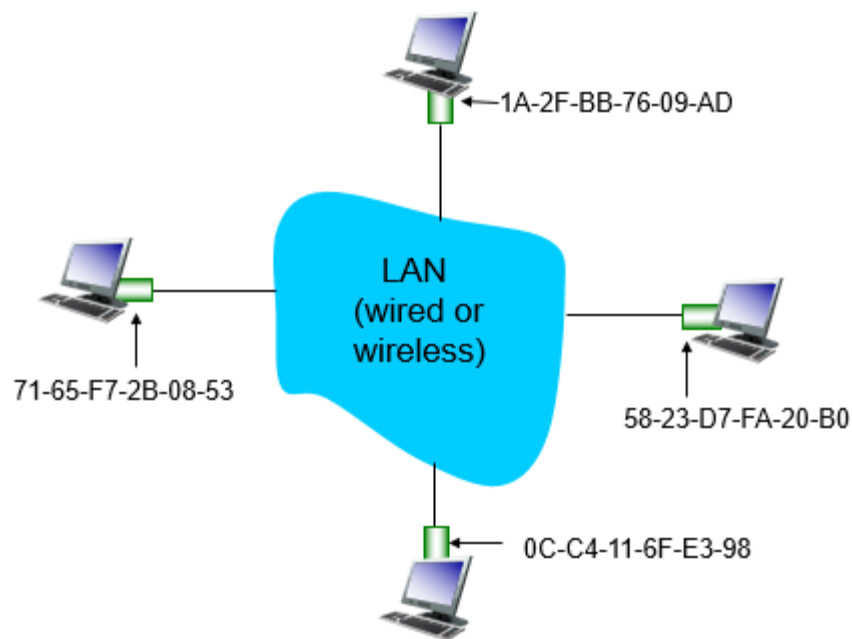


# 以太网帧结构

---

## □ MAC地址（LAN地址，物理地址）

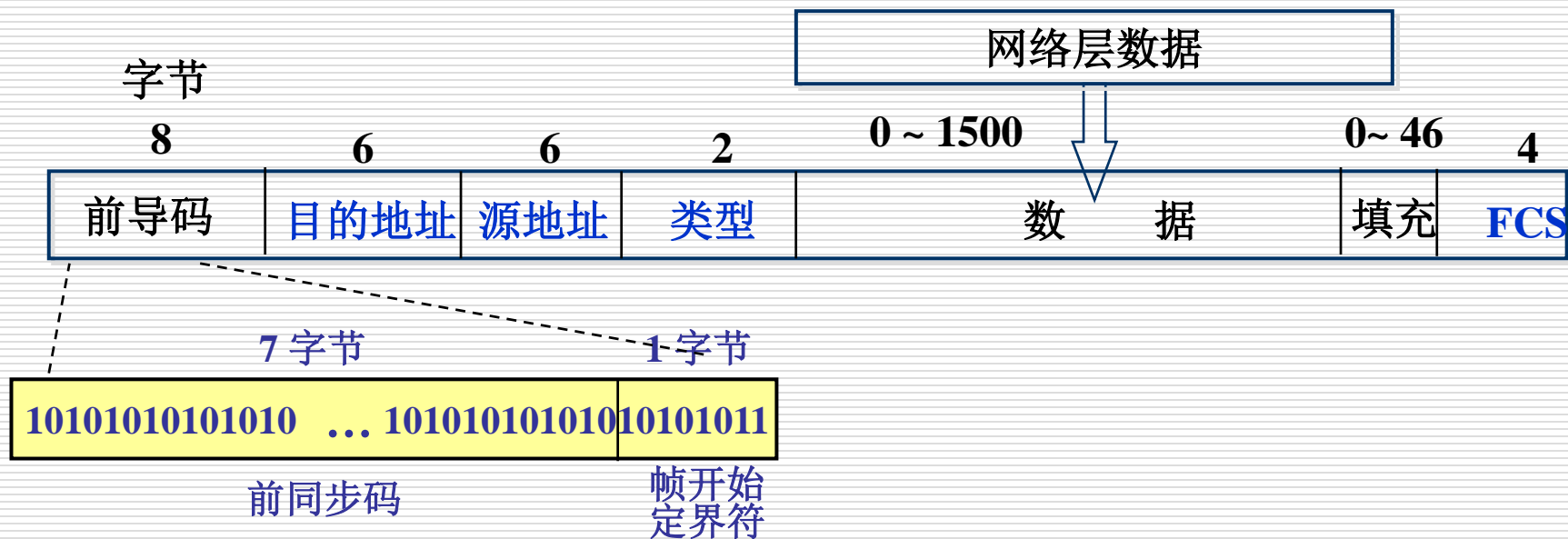
- 48位，每块网卡具有唯一的MAC地址
- IEEE分配前24位
- 全1，广播地址





# 以太网帧结构

分析：1、2、3



类型：标识数据部分封装的是上一层哪一个协议的数据，IP/ARP/.....

FCS：帧校验序列

## 2) CSMA/CD

---

### □ 1-坚持CSMA

——产生冲突：节点还在继续传输帧，造成信道的浪费

### □ CD（冲突检测）

- 节点发送帧的同时，侦听信道，一旦检测到冲突，立即停止传输
-

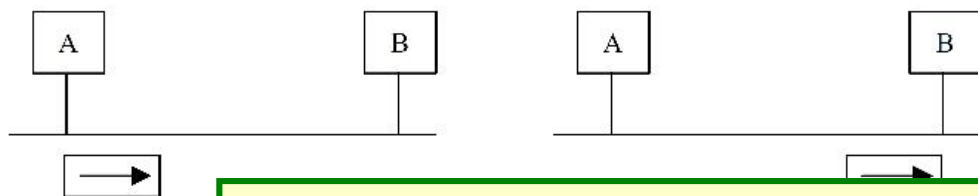
# CSMA/CD

---

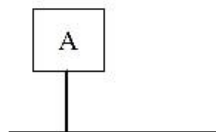
1. 节点发送数据前，先侦听信道是否空闲
  2. 若空闲，马上发送数据，若忙，则继续侦听，直到信道空闲
  3. 在传输帧的同时，持续侦听，进行冲突检测
  4. 若传输的时候，没有检测到冲突，则帧传输成功
  5. 若检测到冲突，则发出干扰信号，以使所有站点都知道发生了冲突并停止传输
  6. 发送完干扰信号，等待一段随机的时间后，再重新传输
-

# 问题1

- 一个站点在发送帧后，持续侦听多长时间才能确定此次传输会不会出现冲突？



(a) A 在时刻  $t$



(c) B 在时刻  $t+d$  开始

- 站点发送帧后，继续侦听信道，至多经过  $2d$ （两倍的端到端传播时延），就可知道此次传输是否会产生冲突
- 经过  $2d$  这段时间还没有检测到冲突，则肯定这次发送不会发生冲突

# 最短帧长

---

- 采用CSMA/CD协议，一个重要的原则：帧必须足够长，使得冲突在帧传输完成之前被检测到

帧长 $\geq 2d.C$

- 10base-5以太网的最短帧长：64字节（512bit）
-

## 问题2

---

### □ 随机时间算法：二进制指数退避算法

从整数集合  $[0, 1, \dots, (2^k - 1)]$  中随机选取一个数  $r$

$k = \text{Min}[\text{重传次数}, 10]$

退避时间：  $r \times 2^d$

---

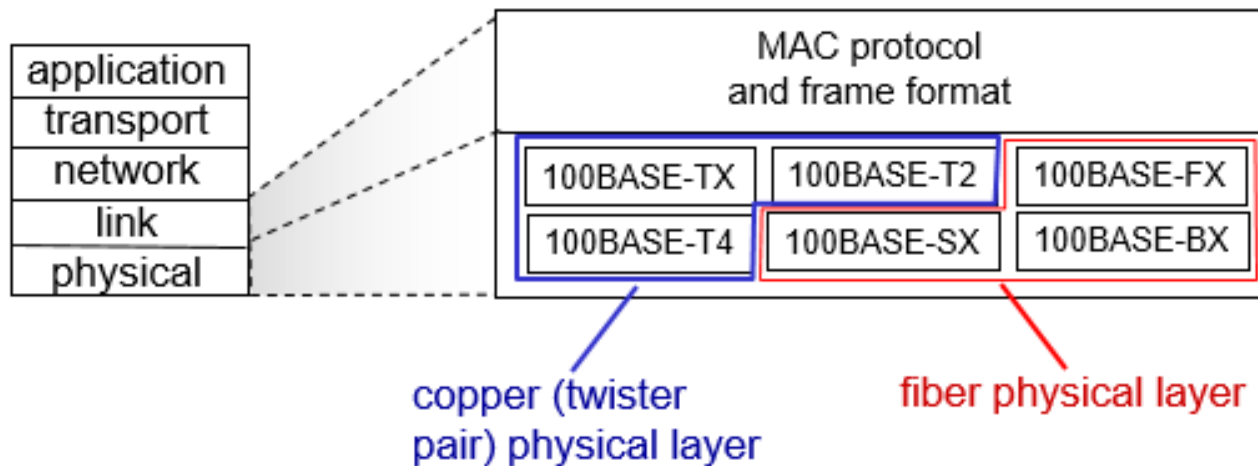
# CSMA/CD效率

---

- 当有个多个节点传输数据时，会产生冲突，信道的吞吐率会降低
  - 吞吐率分析（P130-P131）
-

# 802.3以太网标准

## □ 链路层和物理层标准



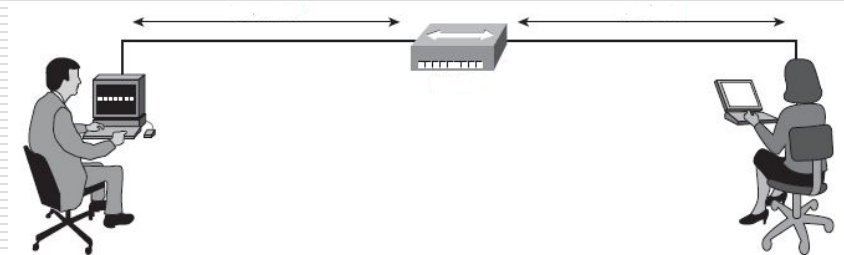


### 3) 以太网互连设备

---

#### □ 转发器/中继器 (10base-5, 10base-2)

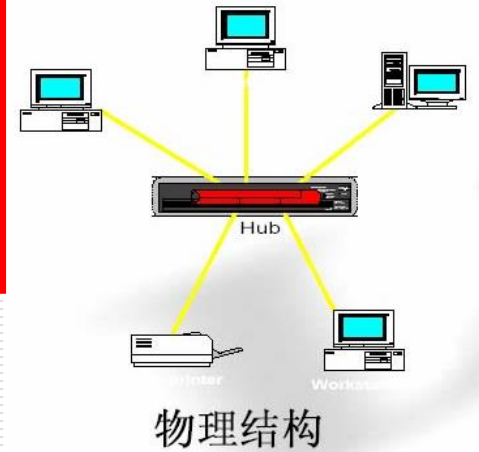
- 工作原理
- 同一个冲突域: CSMA/CD
- 两个节点之间最多4个转发器



双绞线

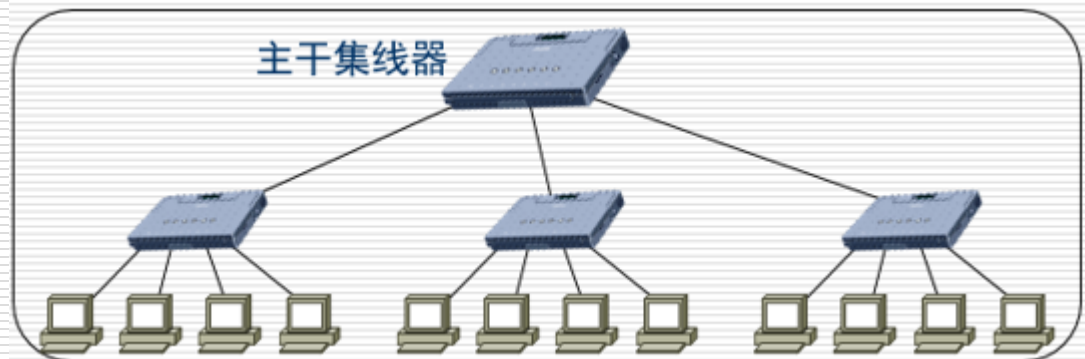
RJ-45接头（水晶头）

RJ-45接口

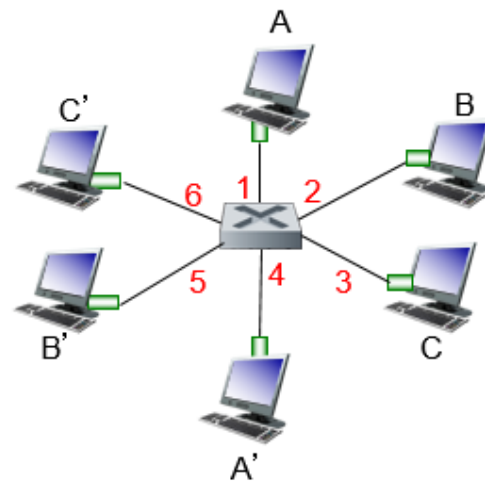


## □ 集线器（Hub）

- 工作原理：多端口的转发器，工作在物理层
- 10base-T：每台主机到集线器的距离不超过 100 m
- 同一个冲突域



# 网桥和交换机

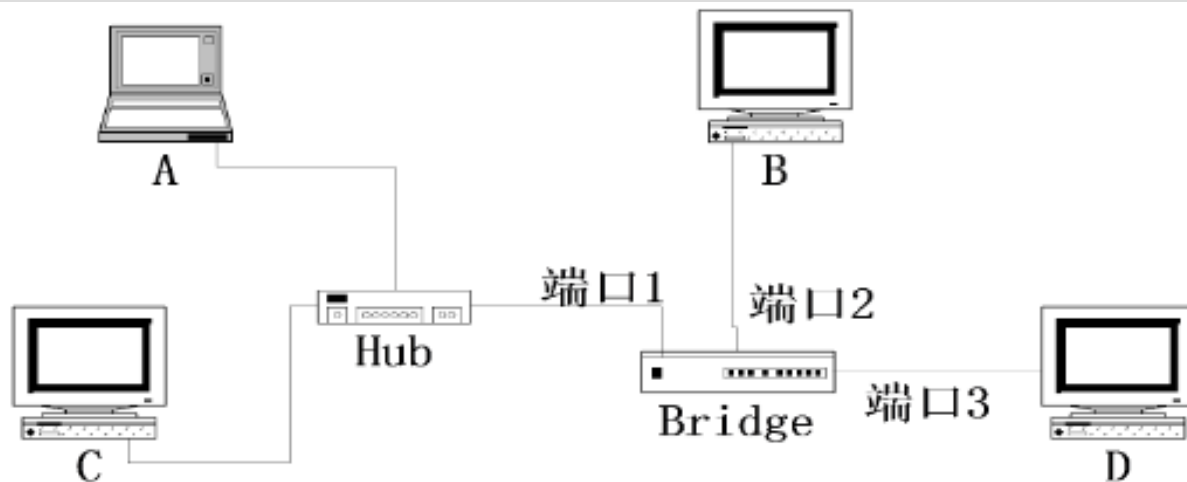


switch with six interfaces  
(1,2,3,4,5,6)

## □ 以太网交换机

- 链路层设备：存储，转发数据帧
- 根据目的MAC地址，查找转发表，向对应端口转发
- 即插即用，自学习建立转发表（P164）

MAC addr	interface	TTL
A	1	60

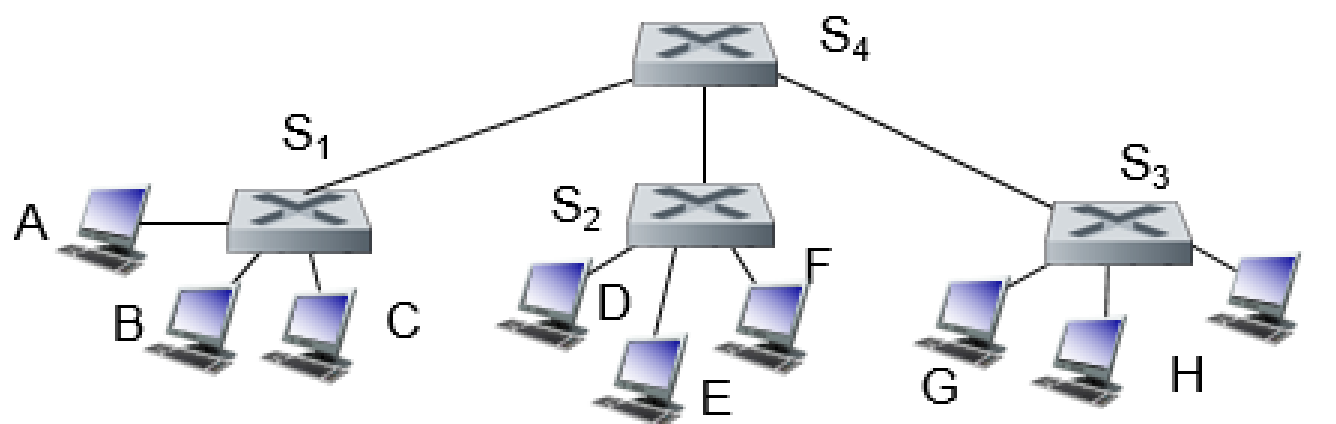


MAC	端口号	TTL

1. 学习
2. 扩散
3. 转发
4. 过滤
5. 老化

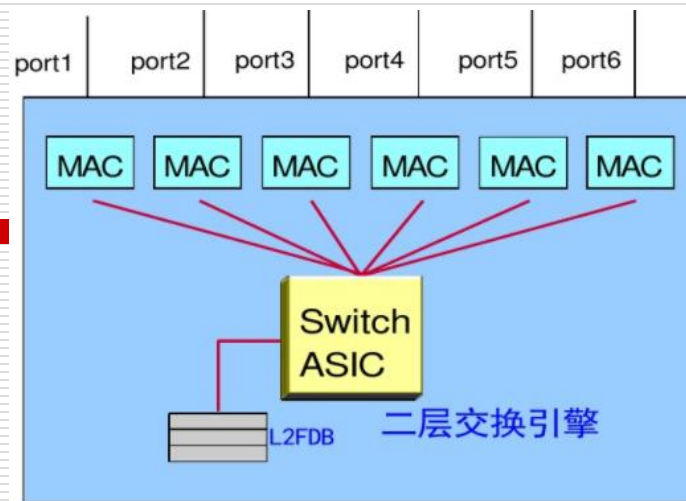
# 例

---



# 交换机的结构

---



1. 交换电路（Switch ASIC）
  2. 多个端口
  3. 转发表（L2FDB: Layer 2 forwarding database）
  4. 输入/输出缓存
-

# 交换机的特点

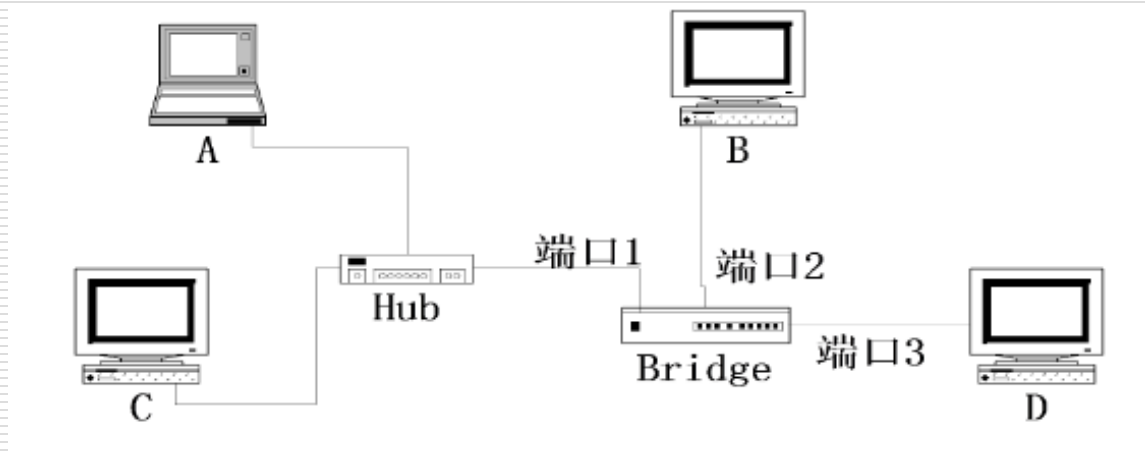
---

## 1. 隔离了冲突域

- 广播帧：向其他所有端口转发（除进入端口外）

## 2. 并行交换

## 3. 全双工通信



## 4) 以太网的发展

---

### □ 100BASE-T/F: 快速以太网 (1995)

- 拓扑结构: 星型
  - 帧格式不变, 最短帧长: 64字节
  - 网络覆盖范围缩小到200m
  - 帧间隔: 0.96us
-



---

## □ 1000BASE-LX/SX/T/CX: 千兆以太网 (1998)

- 全双工和半双工 (CSMA/CD) 两种方式。
  - 帧格式不变, 最短帧长: 64字节
    - 将帧长扩展为512字节
    - 载波扩展: 用一些特殊字符填充在帧的后面
    - 帧突发: 第一个短帧要采用载波延伸方法进行填充, 随后的一些短帧则可一个接一个地发送
-

——唯一不变的：以太网帧格式

---

## □ 10GBASE-T/R/S：万兆以太网（2002）

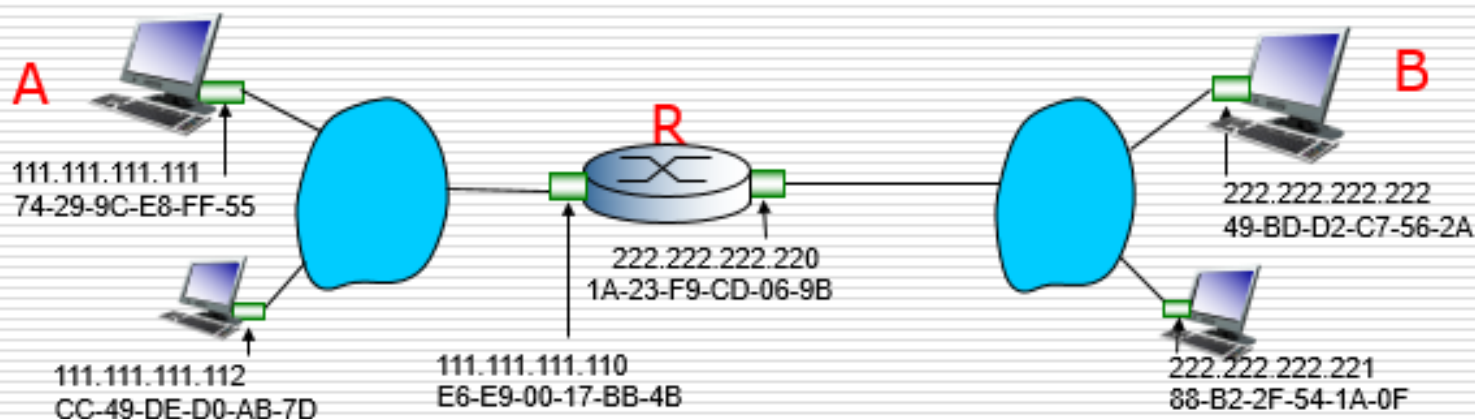
- 只工作在全双工方式，不使用CSMA/CD协议
- 保留以太网帧格式、最短帧长及最大帧长

## □ 40G/100G（2010/2015）

- 没有距离限制
  - 支持多种传输介质，光纤可以覆盖更远的距离
-

# MAC地址和IP地址

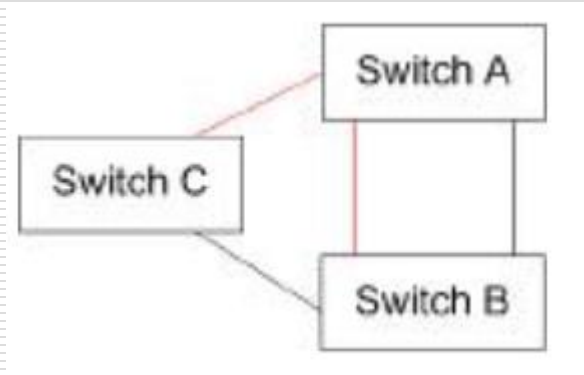
---



## 5) 交换机路由回路

---

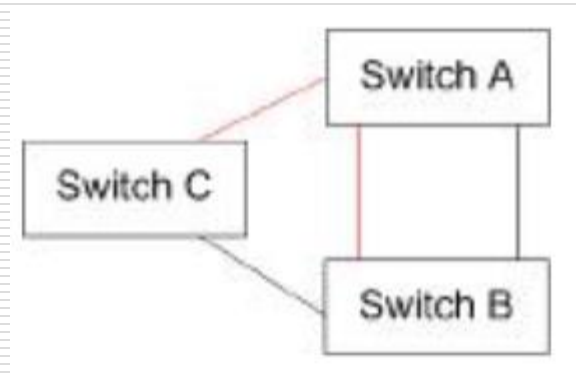
- 多个交换机连接的局域网，可能出现路由的回路
  - 冗余链路，提高网络可靠性



---

## □ 带来的问题？

- ✓ 广播风暴
- ✓ MAC转发表震荡



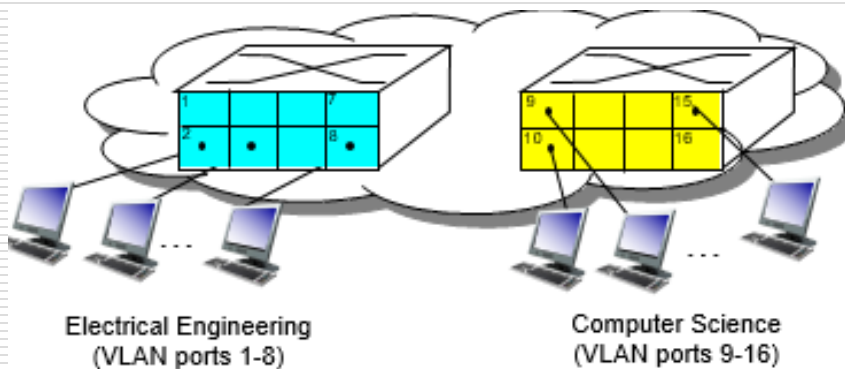
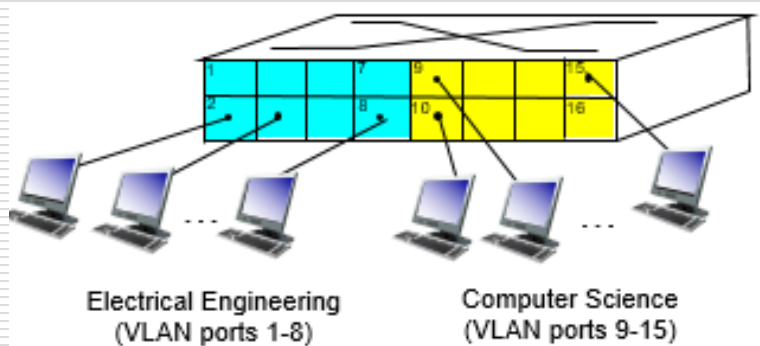
## □ IEEE802.1d制定了生成树协议（STP: Spanning Tree Protocol）

---

## 6) VLAN(虚拟局域网)

---

- 隔离流量和方便管理：配置交换机，将一个单一的物理局域网，划分为多个VLAN



## 5.3 无线LAN

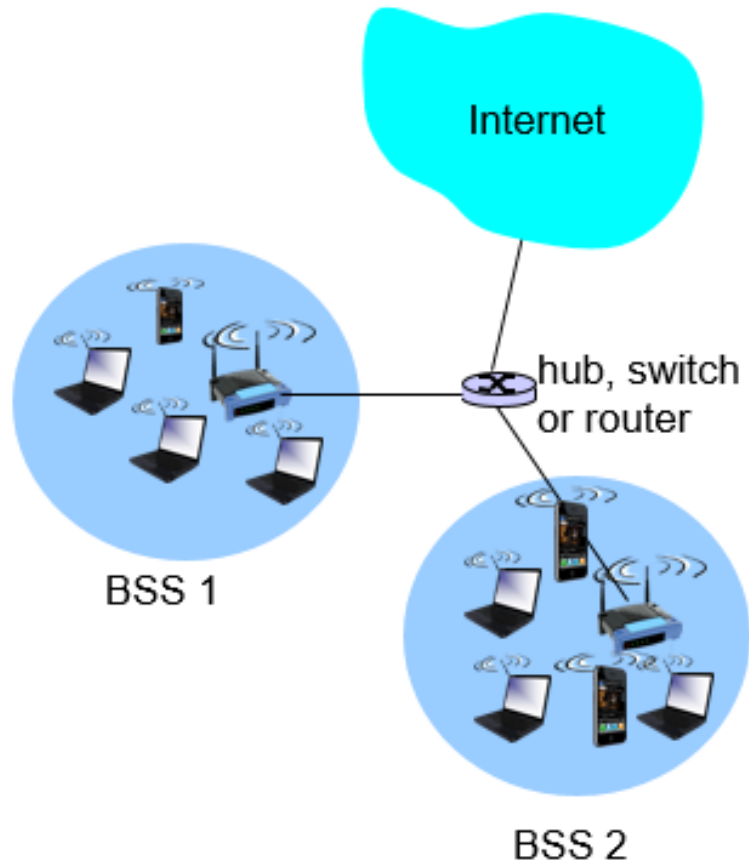
---

- 20世纪90年代，研发了许多无线LAN的标准和技术——IEEE802.11无线LAN（WiFi）

标准	频率范围	数据率（最高）
802.11b	2.4 GHz	11Mbps
802.11a	5 GHz	54Mbps
802.11g	2.4 GHz	54Mbps
802.11n	2.4-5 GHz	450Mbps
802.11ac	5 GHz	1300Mbps

---

# 802.11体系结构



无线站点：运行应用程序的端系统（6字节的MAC地址）

基站：无线接入点（AP: Access Point）

BSS: 基本服务集（Basic Service Set）包含一个AP和多个无线站点



# 802.11 MAC

---

- DCF: 分布式协调功能

- PCF: 点协调功能

- CSMA/CA (CSMA with collision avoidance)

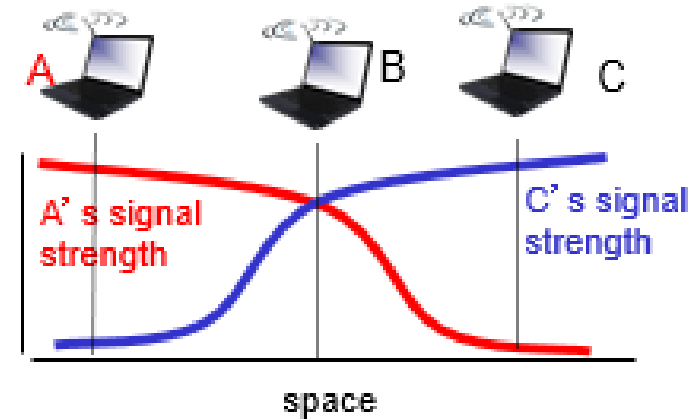
  - 碰撞避免

- 为什么不采用CD?

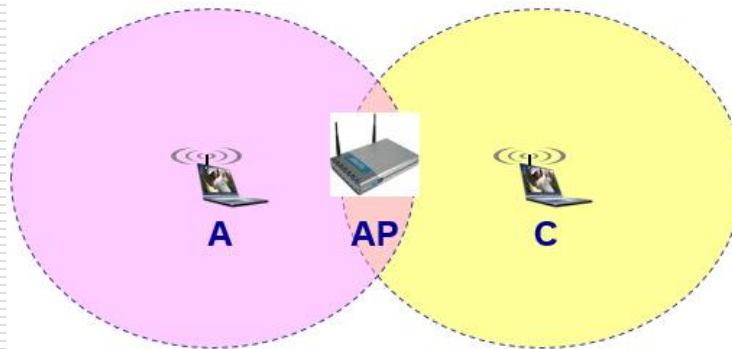
---

# 两个主要原因

1) 信号的衰减，接收信号的强度远远小于发送信号的强度，硬件代价较大

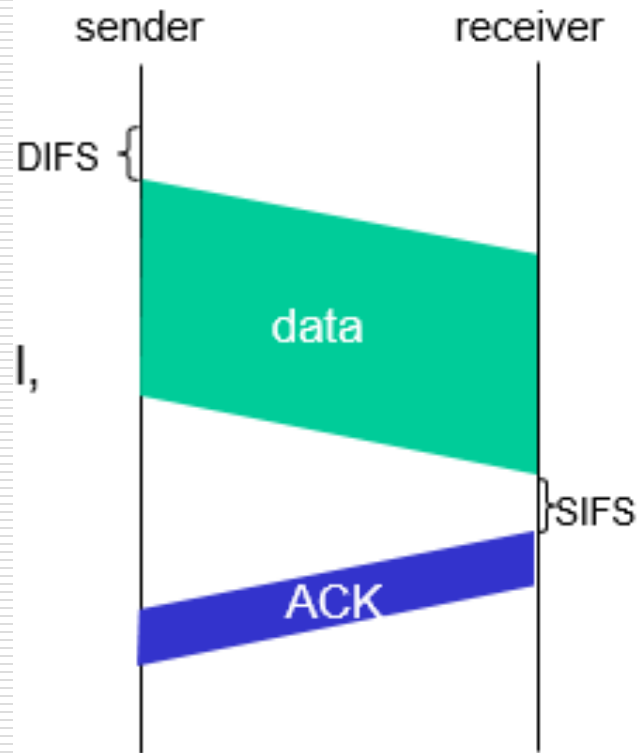


2) 隐蔽终端：无法检测到碰撞



# CSMA/CA

1. 节点发送数据前，先侦听信道是否空闲，若空闲，等待一个DIFS（分布式帧间间隔），发送数据
2. 如果信道忙，执行退避算法，在此期间继续侦听信道，如果信道空闲，递减退避值，如信道忙，计数值不变
3. 退避值减到0（信道空闲），发送数据帧并等待确认
4. 收到确认？Yes/No，go to step2/退避范围加大

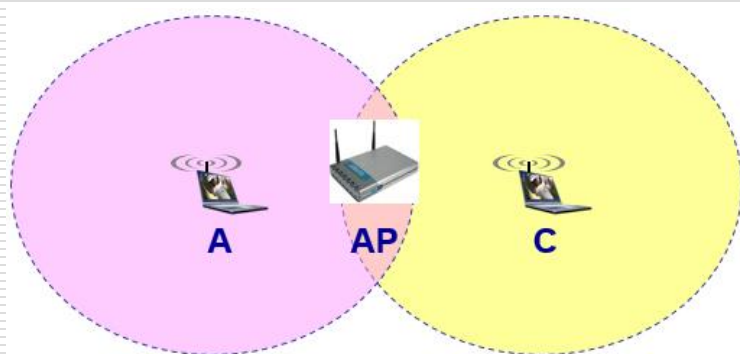


## 处理隐蔽终端：RTS和CTS

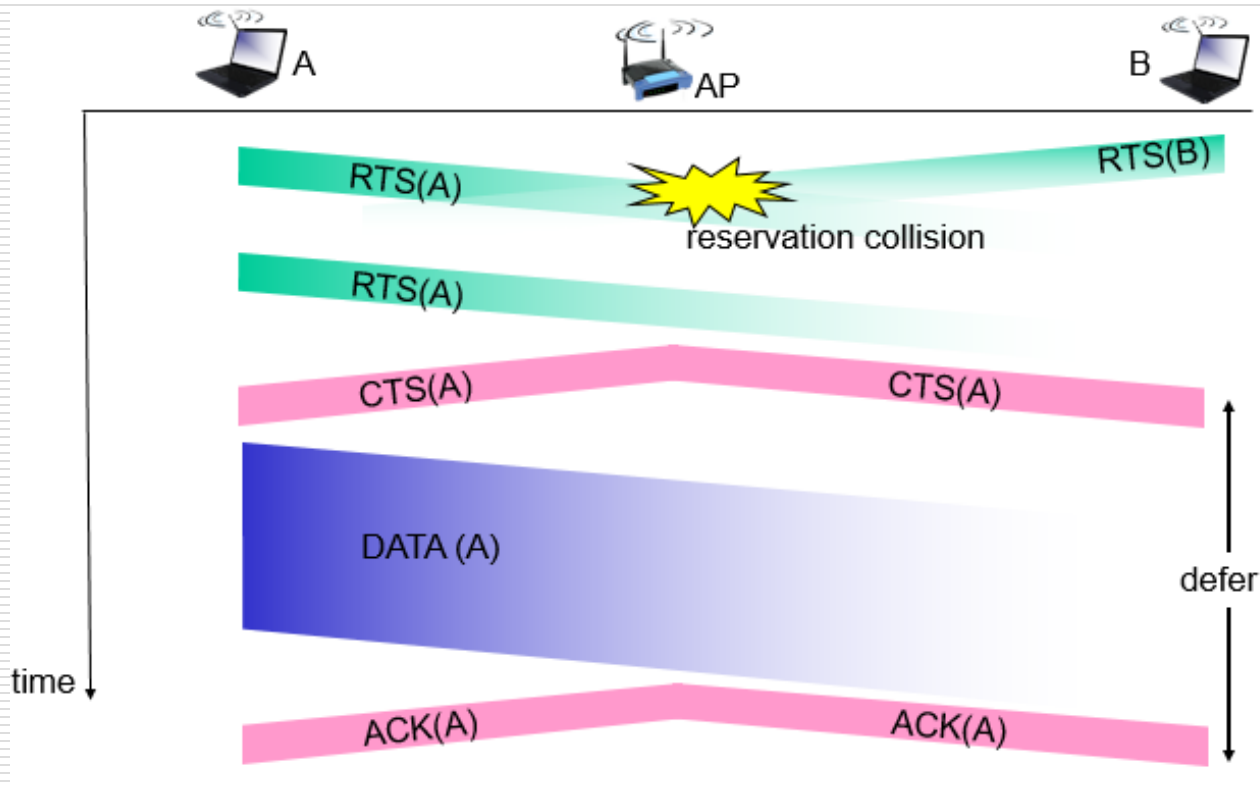
---

□ 802.11MAC协议：预约信道（可选）

- 站点采用**请求发送**（RTS：Request to Send）控制帧和**允许发送**（CTS：Clear to Send）来预约信道



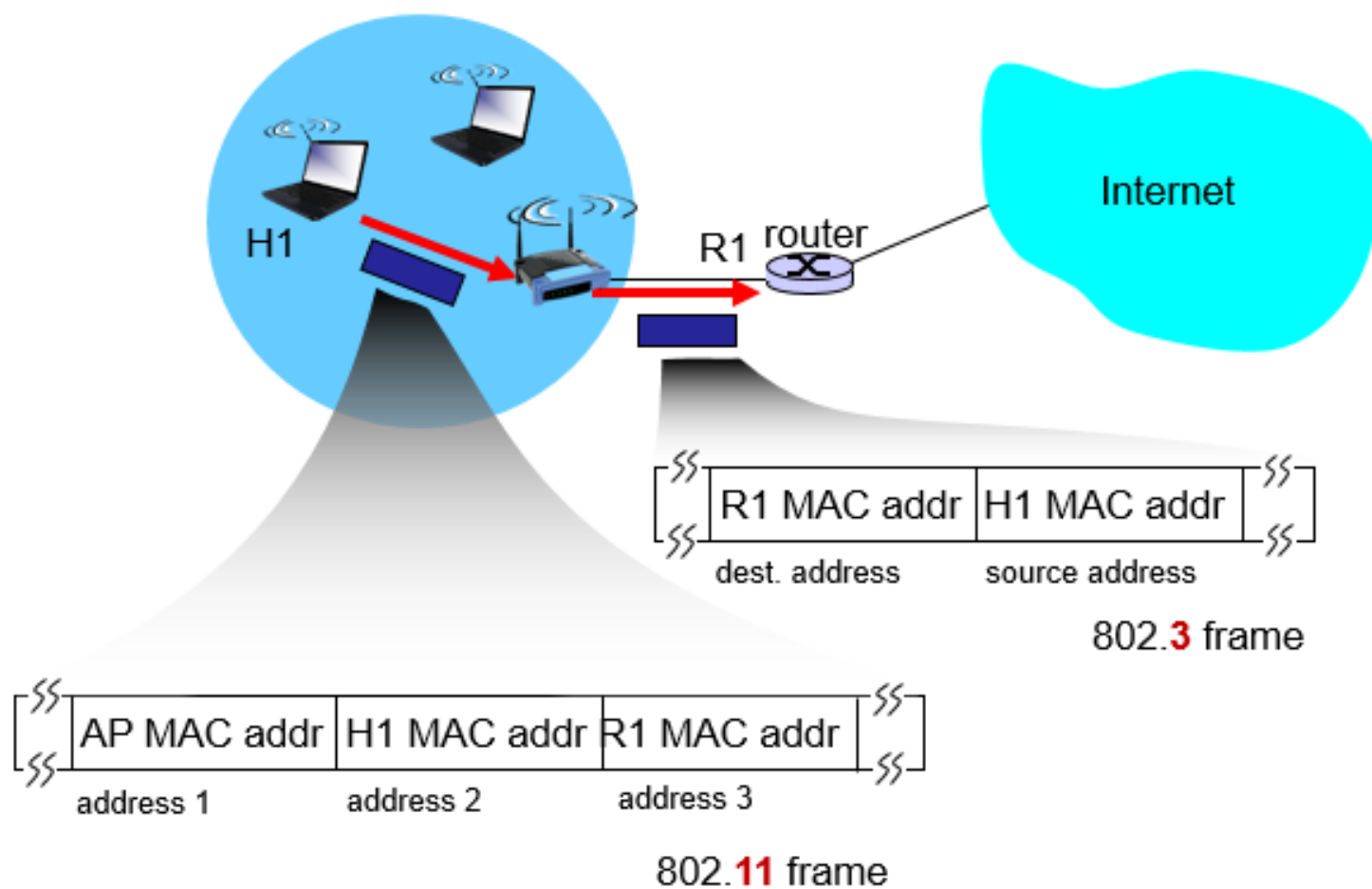
- 站点：发送数据帧前，向AP发送RTS（包括传输数据帧和ACK帧需要的总时间）
- AP：广播CTS帧，对发送站点的响应，同时也是通知其他站点在此期间不要发送



# IEEE 802.11帧格式



1. 帧主体和FCS
  2. 帧控制
  3. 序号控制
  4. 持续期
  5. MAC地址
- ✓ 类型和子类型：  
数据帧/控制帧/管理帧



---

□ 下列介质访问控制协议中，可能发生冲突的是

1) CDMA

2) CSMA

3) TDMA

4) FDMA

---



---

## □ 对正确收到的数据帧进行确认的MAC协议

- 1) CSMA
  - 2) CDMA
  - 3) CSMA/CD
  - 4) CSMA/CA
-

---

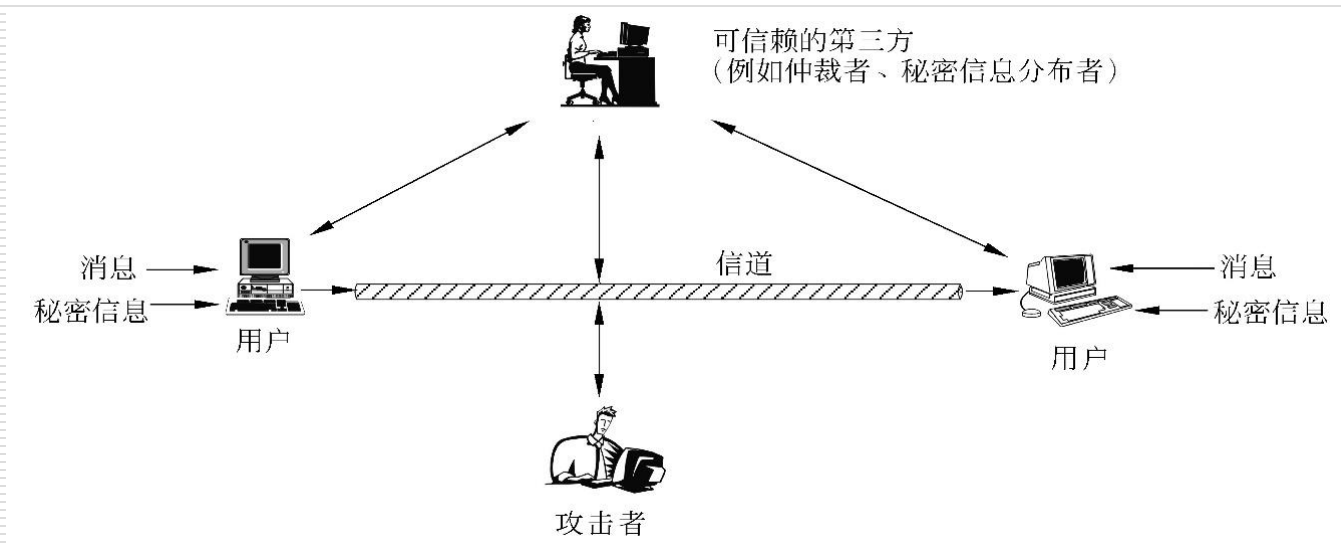
## □ 作业

P152 : 4.9, 4.10, 4.18

---

# 第九章 网络安全

- ❑ OSI和TCP/IP参考模型，在设计之初没有充分考虑网络通信中存在的安全问题



# OSI安全体系结构

---

1. 安全攻击 (security attack)
  2. 安全服务 (security service)
  3. 安全技术 (security mechanism)
-

# TCP/IP网络安全体系结构

---

Kerberos	S/MIME	PGP	SET
FTP	SMTP	HTTP	
SSL or TLS			
UDP		TCP	
IP/IPSec			