## TEST #1

* M-Commerce: 移动商务
* 面向连接服务以电话服务建模，无连接服务以邮政系统建模
* Max data rate (bit/sec): Nyquist: 2B \* log2(V) (V为一个信号可能的值数量); Shannon: B \* log2(1 + S/N) (S/N为信噪比)
* Message switching: 消息交换。把数据存在某些节点，随后有工作链路时转发数据。
* 流量控制：基于反馈的(feedback,接收方给发送方返回信息)，基于速率的(rate,内置机制控制流量)
* 发送方在前移到下一个数据前必须等待一个肯定确认，称为ARQ(自动重复请求)或者PAR(带重传的肯定确认),用于stop-and-wait协议中
* Go-Back-N: 出错后的后续所有帧全部丢弃并不发送确认请求
* 选择重传: 出错后发送NAK,后续帧缓存,等收到正确的出错帧后发送缓存最后一帧的ACK,而此前的ACK发送的序号是出错前最后一帧的序号
* CSMA/CD:冲突检测的载波侦听多路访问(用于以太网)；CSMA/CA:冲突避免的CSMA(用于802.11, 发送RTS, 返回/接收CTS, 最后ACK。不传输终端使用NAV保持沉默)
* 隐藏终端:节点之间无法互相监听对方,但当其不可以同时传输时，其同时传输,从而导致冲突发生; 暴露终端:节点之间能够互相监听对方,但其可以同时传输时,其不传输,从而造成浪费。
* Manchester编码: 一个波特时间里跳变1-High,Low; 0-Low,High
* Repeater, Hub: 物理层; Bridge, Switch: 链路层; Router: 网络层
* 服务质量:Class-based(无需实现设置流，不牵涉整条路径), Flow-based(与Class-based相反,需要设置流并牵涉到整条路径)
* MPLS: 基于Label&Tag的Switching(标签交换,面向连接)
* ARP(网络层): IP->MAC. RARP: MAC(Data link address)->IP
* 丢包: 有线下:降速; 无线下:Try harder(短冲突加强信号); 发送方不知网络状态: 难决策
* Email: CC:抄送(secondary recipient, Carbon Copies), BCC:密送(*Blind* Carbon Copies)
* Store-and-forward: 收到所有消息后再转发; Cut-through: 与前者相反
* PCM: Pulse Code Modulation，脉冲编码调制
* PPP(链路层)头结构: Flag-[Addr-Ctrl]-Protocol-Payload-Chksum-Flag
* ICMP(网络层): 路由器处理数据包发生意外，可由此协议报告；可用于测试Internet(ping)；拥塞时发送源抑制(抑制包)
* OSPF(传输层):内部网关链路状态(link state)路由协议
* 传输层端口前1024个被保留
* URL(统一资源定位器): 3 Parts – Protocol(如file, http[s], ftp等), DNS name of the host, Path name
* MD(Message Digest): 消息摘要，单向Hash函数(MD5, SHA-1 etc.)
* 电话系统三个组成部分：

Local Loop: 本地回路，连接电话公司的中心办公室与用户家用和商用的电话的有线连接

Trunk: 中继线, 连接交换局的数字光纤

Switching offices: 交换局，电话呼叫从一条中继线被接入另一条中继线

* Selective Repeat: 和Go back N对比。错误发生时，坏帧丢弃，好帧缓存
* NAT: 网络地址转换，本地内部专用IP<-->NAT路由转换<-->外部IP，用于短期缓解IP地址枯竭问题。(借用了传输层的端口号)
* Quality of Service (QoS): Delay, Transit time, Jitter, etc.
* 传输技术有2类：Broadcast, Point-to-point
* Flow Control: 保持快速发送方不会用数据把慢速接送方淹没(防止接收端缓存溢出, 即当接收方缓存满时会拒绝接受新消息)
* 如何判断一个帧的开头和结尾

Byte count: 在帧头记录包括头部的字节数大小

Flag bytes with byte stuffing: 在开头和结尾添加FLAG字节，内部里，FLAG->ESC+FLAG; ESC->ESC+ESC; ESC+FLAG->ESC+ESC+ESC+FLAG; ESC+ESC->ESC+ESC+ESC+ESC

Flag bits with bit stuffing: 若FLAG=01111110,则遇到5个1后面填充一个0

Physical layer coding violations(indirectly).

* HDLC(高级数据链路控制协议,链路层,面向bit): 和PPP(点对点协议, 面向byte)有类似的功能
* MACA(链路层，MAC子层): RTS(request to send), CTS(clear to send, it's a reply)
* Binary Exponential Backoff: 若冲突，则随机等待0-2^i-1个time slot时间，再发送(到10以后时间上限不增加,16次错误则放弃)
* Distance vector routing: (RIP,BGP)每个路由器维护一张表，列出当前已知到每个目标的最佳距离以及使用的链路，如何获得最佳链路，动态，会出现count-to-infinity问题.
* Link state routing: 路由状态算法(IS-IS, OSPF)，是距离矢量算法的替代，使用了Link state packet并分发它，动态
* Tunneling: 隧道技术，解决源主机与目标主机网络类型相同但是中间有不同网络类型的网络的通信问题
* DNS: Domain Name System，域名系统，以层次结构命名，协议基于UDP
* Packet Filter: 包过滤器，防火墙就像这个，丢弃不符合条件的数据包
* OSI 7层: 物理(bit)->链路(frame)->网络(packet)->传输(segment)->会话->表示->应用; TCP 4层: 链路->网络互联->传输->应用

## Test #2

* 802.3: 10Base-T; 802.3u: Fast-Ethernet; 802.3z: Gigabyte-Ethernet; 802.3ae: 10-GB; 802.3ba: 100-GB
* 100Base-TX: 100表示100Mbit/s, Base表示基带传输,T表示介质，使用4B/5B编码，最大长度100米(100Base-T4也是,而100Base-FX是光纤,2000m)
* STP：Spanning Tree Protocol, 生成树协议, 可避免链路的回环(作用于交换机上)
* IP的特点: 不可靠+无连接
* IP地址分类：

A:以0开头，8位mask;

B:以10开头，16位mask;

C:以110开头，24位mask;

D:以1110开头，后面是多播地址;

E:以1111开头，后面保留。

* 802.1q：添加了VLAN tag
* PPP 3个主要特性:

1. 成帧方法
2. 链路控制协议 - NCP(链路层): Network Control Protocol, 网络控制协议，协商网络层选项；
3. 协商网络层选项方式 - LCP(链路层): Link Control Protocol, 链路控制协议，用于启动线路、测试线路、协商参数和关闭线路

* 二进制数据的ASCII编码方式为base64 encoding(6位一个字符)；而quoted-printable encoding使用7位ASCII码
* CRC校验: 若给定G(x)位n阶(最高次为n)，则CRC校验码就有n位。步骤如下：

首先给原数据后添加n个0

然后和G(x)做竖式除法，得到的remainder是**异或出来**而不是相减出来的

最后得到的remainder前面填充必要的0到n位，这就是CRC校验码

滑动窗口大小: Go-back-N: MAX\_SEQ; 选择重传: (MAX\_SEQ + 1)/2，即有缓存的

* FDM：频分复用；TDM：时分复用；WDM：波分复用；CDM：码分复用。都是**静态的**信道分配方式。
* (其它)：网络地址(NSAP)由网络层提供, 传输服务地址(TSAP)由传输层提供；点对点的WAN连接mask最有效率的是30位。
* Switching技术(物理层): Circuit(电路交换，需要建立一条端到端路径，如电话交换), Package(包交换，无需设置专门的路径)
* LLC(Link顶部):逻辑链路控制子层，识别网络层协议.
* MAC(Link底部):介质访问控制子层，线路控制(决定如何分配共享信道的使用权)、出错通知（不纠正）、帧的传递顺序和可选择的流量控制也在这一子层实现。
* RTP(应用层): The Real-time Transport Protocol，基于UDP协议，头部包含时间戳(Timestamp)，将多路数据流复用到一个UDP包中。(RTCP, RTP姊妹协议,处理反馈、同步与用户接口消息，不传输媒体样值)
* 面向连接/无连接服务的区别: 1, 前者要建立连接，只有建立连接后才能传输，传输完必须释放连接, 而后者直接进行数据传输; 2, 前者保证数据传输可靠性和保序性, 后者不保证
* Authentication(认证) & Authorization(授权)区别：认证关注的是你是否真的在跟一个特定的进程通信；而授权关注的是允许这个进程做什么样的事情

## Test #3

* ARPANET子网由IMPSs组成(接口报文处理器)
* Communication Subnet: Physical + Data Link + Network
* 802.15: Bluetooth, 可以将电脑的配件连接在一起(802.16: 无线宽带，可能替代ADSL)
* OSI并没有提供相对于TCP/IP更加有效的实现, OSI只规定了哪一层到底有什么功能
* 传输层的功能:进程之间的通信
* X.25, Frame Relay(packet switching), ATM(异步传输模式,头部带有虚电路标识符)为面向连接的;而802.11 LAN并不是面向连接的
* Fiber: error rate最低(coax:同轴电缆，UTP:非屏蔽双绞线(连接头使用RJ-45))
* Hamming code: correct errors; Polynomial code: detect errors;
* 若要纠正d个错误，那么给定的有效码表的Hamming distance(任意2个码的最短距离)至少要2d+1; 若要检测d个错误,则有效码表的hamming distance至少为d+1
* SDLC:同步数据链路控制，衍生出HDLC, LAP(A,B),802.2,QLLC
* PPP的主要特性(组成)：成帧方法，LCP(链路控制协议)，NCP(网络控制协议)
* Collision-free protocol: **Bit-map, token passing, binary countdown**
* 利用率：0.01坚持CSMA>0.1坚持CSMA>0.5坚持CSMA>1坚持CSMA>分槽ALOHA>纯ALOHA。需要2个传输时间监听冲突；冲突连续16次后会放弃报错。
* RIP(应用层):路由信息协议，使用distance vector算法
* BGP(应用层):外部网关路由协议，使用distance vector算法(改进过的)，使用在自治系统之间（AS）
* OSPF(传输层):内部网关路由协议，使用link state算法，使用在自治系统内部（AS）
* IP分片与重组:分片根据MTU(最大传输单元，1518-18=1500Bytes，减去以太网帧头)与网络实际情况决定；分片最后只在目的地重组；DF: 禁止分片；MF:若分片了，除了最后一个，都要设为1；Offset:该值为该片相对原始数据包的偏移字节数(without header)/8
* 特殊的IP地址: 0.0.0.0(Host), 000-Host(Hosts on this network), 255.255.255.255(Broadcast on local network), Network-111(Broadcast on remote network), 127.x.y.z(Loop)
* IPv4: **20 Bytes (Version:4 bits; IHL数据包头长度: 4 bits;** Differential Services: 4 bits**; Total length: 16 bits包含头+载荷; ID: 16 bits; Fragment offset: 13 bits; TTL: 8 bits; Protocol: 8 bits; Checksum: 16 bits; Address: 32 bits)**
* IP的checksum在头部，并且头部数据使用大端表示。
* Traffic Shaping: 流量整形，可使用leak bucket algorithm, token bucket algorithm, packet scheduling algorithms
* TCP(传输层):Header-**20 Bytes**(**Port: 16 bits**; **Seq: 32 bits; Ack: 32 bits; Header length: 4 bits; Control: 8 bits; Window size: 16 bits; Checksum: 16 bits;** Urgent pointer: 16 bits).
* TCP三次握手:

1. 客户端SEQ=x(CLOSED->SYN-SENT);

2. 服务端SEQ=y,ACK=x+1(LISTEN->SYN-RCVD);

3. 客户端SEQ=x+1,ACK=y(SYN-SENT/RCVD->ESTABLISHED)

* TCP四次挥手:

1. 客户端FIN=1, seq=x(客户端ESTABLISHED->FIN-WAIT1);

2. 服务端ACK=1, seq=y, ack=x+1(服务端ESTABLISHED->CLOSE-WAIT，客户端FIN-WAIT1->FIN-WAIT2);

3.服务端FIN=1,ACK=1,seq=z,ack=x+1(CLOSE-WAIT->LAST-ACK);

4.客户端ACK=1,seq=x+1,ack=z+1(客户端FIN-WAIT2->TIME-WAIT, 服务端LAST-ACK->CLOSED)

* TCP Silly Window Syndrome: 使用Clark’s Solution, 强制接收方等待一段时间让缓冲区有足够的空间，再给发送方发送窗口通告
* Nagle’s Algorithm:首先发送第一个到达的数据字节，缓存后面的数据，等待ACK到达后将缓存全部发出
* TCP计时器: persistence timer:处理0窗口通告; keep-alive timer:处理空闲连接，检测对方是否连接上; retransmission timer:用于超时重传 ;timer-waited timer:用于关闭连接
* DNS: A: IPv4, AAAA: IPv6, MX: Email, SOA: 授权开始; HINFO: 主机OS的类型
* Message Transfer Agent: 消息传输代理，运行在ISP和服务器上，与互联网保持连接，用于在Internet中传输消息
* HTML: <ol>: ordered list; <ul>: unordered list; <li>: list item. HTML 1.1支持可**持续化**的连接
* Ethereal: 一种数据包嗅探软件
* One-time pad(OTP): 一次性密码加密,假如正确使用,不会被破解
* CA: Certification Authority, 证明公钥所属权的组织，认证中心
* KDC:Key Distribution Center, 密钥分发中心
* TLS: Transport Layer Security, 安全传输层协议用于提供通信的保密性和完整性，由TLS Record协议和TLS Handshake协议构成
* 密码学准则: Redundancy, Freshness
* 加密算法是好的: 它能在**选择明文(Chosen plaintext)**攻击下不被攻破

## Test #4

* Data movement through layers->Encapsulation
* OSI并没有提供比TCP/IP更加效率的实现。TCP/IP模型的传输层处理传输的可靠性、流量控制和错误纠正
* WDM:波(Wavelength)分(Division)复用(Multiplexing),在光纤中使用
* Wireless Communication种类:Cellular, Infrared(红外), Spread Spectrum(扩展频谱).而Broadband宽带一般指有线的.
* 802.11使用CSMA/CA避免传输冲突
* VLAN可用于划分广播域
* 交换机的地址学习：收到数据包后，读取源地址的内容并保存下来
* **Ethernet的MAC地址有6字节，即48bits**
* MAC：介质访问控制，主要功能是管理、决定共享信道的分配和使用问题
* CSMA/CD网络与以太网:在设计以太网时，认为信号都是以广播模式发送的
* Default Route(默认路由)：当目的网络不在路由表中时，选择转发到默认路由(0.0.0.0/0 next-hop)
* ICMP: Internet Control Message Protocol
* Distance Vector Algorithm优点：其计算比较简单
* Link-state Algorithm特点：重建了全网的准确的拓扑
* 某类IP地址可用主机数量要去掉全0和全1的Host地址
* 网络层的拥塞控制: **choke** packet, explicit **congestion notification,** hop-by-hop choke packet, **load shedding(负载脱落，最后的最强的一招)**
* IPv6: Header – **40** bytes (version: 4 bits; differentiated services: 8 bits; flow label: 20bits; **payload length: 16 bits**; next header: 8 bits; hop limit: 8 bits; **Address: each 128 bits, that is 16 byte, total 32 bytes**)
* **TCP重传计时器的值基于上一个RTT**，而Jacobson算法：**SRTT = a\*SRTT+(1-a)\*R,** R为确认所花时间
* TCP原语：socket:创建套接字；bind: 绑定地址/端口；**listen: 监听，给出队列长度**；accept: 被动接受连接请求；connect: 主动发起连接；send/receive/close: 如字面意思。
* UDP: 无连接不可靠的，需要指定端口，可逆多路复用。DNS, RTP等基于UDP，RPC使用UDP。其必须依靠应用层的协议来保证可靠性。
* 常用端口(**16 bits**): **Telnet: 23; FTP: 20,21; SSH: 22; SMTP: 25; HTTP: 80; POP3: 110; IMAP: 143; HTTPS: 443; RTSP: 543; IPP: 631**
* MIME：Multipurpose Internet Mail Extensions
* XHTML: Extensible Hypertext Markup Language
* HTTP请求方法：GET, POST, PUT(存储Web页面), HEAD(读取Web页面头), DELETE(删除一个Web页面), TRACE, CONNECT, OPTION
* HTTP返回码:

**1xx：Info(100:同意客户端请求)**

**2xx：成功(200:请求成功, 204:没有内容)**

**3xx：重定向(301:移动页面, 304:缓存页面有效)**

**4xx：客户错误(403:禁止页面, 404:页面没找到)**

**5xx：服务端错误(500:内部错误, 503:稍后再试)**

* Java Applet, JS, ActiveX, AJAX都可以生成Client-side动态页面，其中ActiveX最快
* X.509用于规定证书的格式
* DH密钥交换会有中间人/水桶队列攻击(man-in-middle or bucket brigade)
* ping: packet Internet groper可用于验证TCP/IP协议栈的操作并检测网络连通性
* netstat: 用于查看TCP连接情况
* telnet: 可用于登陆远程主机，测试应用层协议，测试端口号是否打开
* socket：socket()：创建服务端套接字; bind()：绑定地址/端口; **listen()：监听,指定队列大小**; accept()：接受请求; send()/recv()：发/收; close()：释放连接; connect()：创建连接
* 密码加密模式：

电码本(ECB)模式；

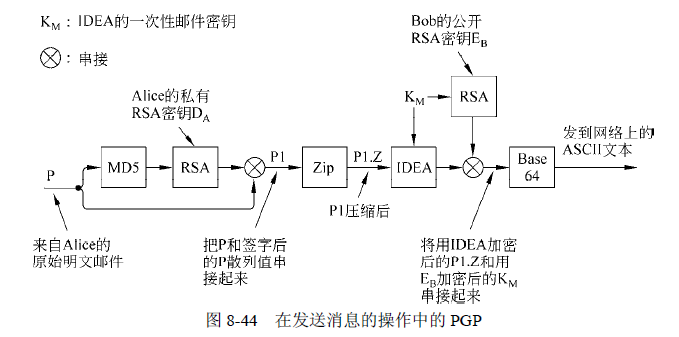
密码块链模式；

密码反馈模式: 适合byte-to-byte加密

流密码模式: 适用于实时流加密

计数器模式: 适用于加密磁盘文件

* PGP：Pretty Good Privacy, 使用IDEA块加密算法。邮件发送过程如下(使用**非对称加密**)：



## Test #5

* Link technologies: Broadcast, point-to-point (不要和C/S和P2P弄混)
* 常用的同轴电缆(Coaxial Cable)：50Ω(数字传输)和75Ω(模拟和有线电视传输)
* 微波传输: 走直线，不容易穿透建筑物，且在4GHz左右会易被雨水吸收。此外还有多径衰落(Multipath Fading)问题。
* Modem调制的技术: 调幅(Amplitude)，调频(Frequency)，调相(Phase), PCM(脉冲编码调制)不在其中
* 单工:只能传输一个方向；单双工:可以传2个方向，但传输时只能单向；全双工:可同时2个方向传输
* E1 Channel: 速率2.048Mbps；T1 Channel: 速率1.544Mbps
* 分片(fragment)发生在网络层，分段(segment)发生在传输层
* HDLC头结构: Flag, Address, Control, Data, Checksum
* Pure ALOHA(**0.184**): S = G\*e-2G; Slotted ALOHA(**0.368**): S = G\*e-G
* 1-坚持CSMA: 若空闲则立即发送，否则等待到空闲后发送。

0-坚持CSMA: 若空闲则立即发送，否则随机等待一段时间再尝试发送。

p-坚持CSMA: 若空闲则以p的概率发送消息(冲突则随机等待一段时间重新开始)，否则推到下一个slot尝试发送。

* Gigabit以太网使用802.3ab，特性有: 载波扩充(Carrier Extension), 帧突发(Frame Bursting)，以增加线缆长度(传输距离)
* 交换机不能划分隔离广播域(虽然VLAN用于划分广播域)，只能隔离冲突域；而路由器可以划分隔离广播域和冲突域。
* 在TCP/IP网络中，IP的网络ID和子网ID来决定目的地址属于哪个网络。而IP地址的格式为：网络前缀(Network ID + Subnet ID) + 主机(Host ID)
* CIDR: 合并子网，进行路由聚合的设计，其使用的是前缀的Network ID(来扩充host number), 匹配时匹配最长前缀
* OSPF中的路由器: 内部路由器(Internal Router, 全部属于一个Area的路由器), 骨干路由器(Backbone Router, 0号骨干Area的路由器), 区域边界路由器(Area Border Router, 连接到2个或更多Area的路由器), AS边界路由器(AS Boundary Router, 把通往其它AS(不是Area)的外部路由注入到本区域)。2个端的Path必须经过骨干Area，即强行变成星型拓扑。
* 三次握手解决的问题是: 延迟重复问题(Delayed Duplicate TPDUs)
* DNS查询: 客户端发送一个UDP包给本地DNS服务器(**Local Name Server**)，然后递归(即返回结果必须是完整的)/迭代(返回结果可以不完整，本地DNS服务器解析后会继续进一步发送请求以得到完整答案)查询
* RPC: Remote Procedure Call, 远程过程调用,可使用TCP/UDP
* CDN: Content Delivery Networks, 即内容分发网络, 能提高Web性能, 迅速扩大网站的服务能力
* PPP和SLIP(Serial Line Internet Protocol)对链路错误的检测和配置, 多协议以及身份认证
* PC发送接收数据包都是没有VLAN Tag的，即自己不会添加VLAN Tag到数据包中
* 网络丢包的主要原因有：网络本身问题，设备故障，线路故障，网络攻击，路由信息错误，网络拥塞，端口瓶颈，系统资源不足等。而**噪声不是主要原因**。
* RFC：Request For Comments, 请求注释，作为网络标准的技术报告
* 若光纤直径减少到几个光波的波长大小时，光只能直线传输不能反射，形成单模光纤(Single-mode Fiber)
* DMT：本地回路1.1MHz分成256个独立信道,每个4312.5Hz，作为ADSL的传输方法(ADSL：频分复用,分为voice, 上行段和下行段)

## Test #6

* Base64: 二进制的ASCII编码，将3个8-bit字节分成4个6-bit单元, 将非ASCII邮件转换成ASCII邮件
* 不同LAN的MAC层(因为依赖于物理介质)不同，但是LLC相同
* ARP广播查询MAC地址时只能查询本网络的(若无路由处理)
* TCP拥塞控制: 在Threshold以下，拥塞窗口大小以2的倍数增长(slow start)，到达Threshold，以+1线性增长; 若丢包，则Threshold设为丢包前窗口的1/2，窗口大小设为1
* 收Email: POP3: 收Email到本地磁盘，服务器不保留; IMAP: 收Email，但服务器保留
* 单播: 1对1；组播(multicast): 1对多；广播: 1对所有；选播(anycast)：传给最近的组成员
* 设传播信号的时间为t，则只有当一个站传输了2t后还没有检测到冲突，才可以确保抓到了信道(即发送一帧的时间必须大于2t)
* TCP ack：其值为期待的下一个TPDU的序号seq，seq\_next = ack = seq\_prev + size
* TCP到LISTEN状态调用listen(), 到ESTABLISHED状态服务端调用accept()
* 虚电路网络与数据包网络的比较

|  |  |  |
| --- | --- | --- |
| Problem | Datagram Network | Virtual-circuit Network |
| 电路建立 | 不需要 | 需要 |
| 寻址 | 每个包需要源地址和目标地址 | 只需要包含VC号 |
| 状态信息 | 路由器不保留连接状态 | 每条VC都要路由器保存状态 |
| 路由方式 | 每个数据包单独路由 | 建立VC时选择路由，所有包遵循该路由 |
| 路由失效影响 | 无影响，除了路由器崩溃时丢失的包 | 穿过故障路由器的VC都中断 |
| 服务质量 | 困难 | 容易，若预先建立每条VC时由足够的资源可分配 |
| 拥塞控制 | 困难 | 容易，若预先建立每条VC时由足够的资源可分配 |

## Test #7

* 蜂窝网络带宽不大
* Cookie：一段文本信息，伴随着用户请求页面在服务器和浏览器传递，缓存在客户端，临时的。包含5个字段：domain, path, content, expires, secure
* 光纤信号源: LED(只能用于多模)，半导体激光(Semiconductor Laser, 单模多模都可以)
* 电话系统中，不同的Switches(距离超过4km)由Trunk连接(即中继线)
* Circuit Switching：需要建立专门的物理路径，不使用Store-and-forward传输，延迟时间短(只有电磁信号传输延迟，只在建立路径时产生拥塞)；

Packet Switching：不需要建立专门的物理路径，通常使用Store-and-forward传输(也有Cut-through)，延迟时间较长(每个包产生延迟/拥塞)

Message Switching：将数据存在某些节点，有工作链路时再转发数据，可用于构建延迟容忍网络/中断容忍网络(DTN)，可发送任意长度数据(与Packet Switching相反)

* PCF: Point Coordination Function, 点协调功能, AP控制自己覆盖范围的所有活动(因此当该技术用于802.11时使用的是TDM静态信道分配)

DCF: Distributed Coordination Function, 分布式协调功能, 使用CSMA/CA技术和确认(ACK)技术，使用二进制回退策略避免冲突

* MAC地址: 由网卡决定，是固定的。**共48 bits (6 bytes)，可用6个2位十六进制数表示。MAC广播地址: FF-FF-FF-FF-FF-FF**。
* 如Repeater, Hub会扩大/放大(Extend)冲突域，而不能隔离冲突域
* 路由器的默认路由的地址是0.0.0.0/0
* 私有IP地址范围：**10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16**
* POP3基于TCP协议
* DES: 56位key, 加密每64位数据块, 使用了替换、迭代以及多轮的计算

AES: 128位以上的key, 加密每128位数据块, 使用了替换、迭代以及多轮的计算，其基于Galois域理论基础

* 07-08 Spring-Summer第四大题参考书4.16题

## Test #8

* 以太网帧的**Payload最大1500字节，帧最大1518字节**。目标地址第一位为0则为普通地址，若第一位为1则为组地址，若全1则为广播。

以太网最小传输的**帧大小为64字节（512bit）**

* UDP：Header: **8 bytes (Src port: 2 bytes, dest port: 2 bytes, length: 2 bytes, checksum: 2 bytes)**
* RIP(应用层):用UDP发路由消息; OSPF(传输层):用IP发路由消息; BGP(应用层):用TCP发路由消息
* 服务：层与层之间(下层给上层提供原语);协议：两个对等层直接的协定
* CDM：每个站的码片和结果相乘,然后相加得到一个整数,若>0:发送1;<0:发送0;=0:没发送
* 链路层提供3种服务：无确认无连接、有确认无连接、有确认有连接
* 802.3和经典以太网使用1坚持CSMA/CD, 802.3的长度字段对应经典以太网的类型字段
* DHCP(应用层)：动态主机配置协议，一台DHCP服务器负责配置各个主机的IP地址，使用UDP包
* IPSec：2种模式(传输模式,不添加新IP头; 隧道模式:添加IP头；IP头不被加密和验证，ESP被验证但不被加密，尾部添加HMAC认证码)
* SSL：位于HTTP下层，和HTTP组成为HTTPS

## HW

* Message Switching与Packet Switching不同: 前者可以传任意长度的数据, 而后者对数据包长度有限制(若超过最大长度将会被分成多个包发送)
* 链路层CRC放在尾部的原因: CRC在发送期间计算，一旦最后一位送出，就立即附加CRC码；若放头部则发送前就得计算一遍CRC这样每个字节要处理2遍，一遍是计算CRC，另一遍是发送；它减半了处理时间。
* Piggybacked Acknowledgement：捎带确认，确认flag包含在数据包中了
* PPP头结构(字节填充成帧): **Flag(1 byte)-[Address-Ctrl]-Protocol(1 or 2 bytes)-Payload-Checksum(2 or 4 bytes)-Flag(1 byte)**，中括号是可选字段
* Pure ALOHA带宽利用率位0.184, Slotted ALOHA带宽利用率为0.368
* 以太网帧: **Preamble & SFD(7+1=8 bytes) - Src addr(6 bytes) – Dest addr(6 bytes) – Type/Length (2 bytes) – DATA – Padding (0 ~ 46 bytes) – Checksum(4 bytes)**. 地址若开头为0则为普通,为1则为组播,全1则为广播; 除了前导码外最小长度64 bytes,若不足则需填充, 最大为1518 bytes
* IP packet fragmentation只在最后接收端重组. MF在最后一帧标为0, **offset为字节数/8**
* **RTTnext=α\* RTTcurrent + (1 – α) \* R**
* 注意TPDU中序号(seq)的回绕问题
* 静态路由和OSFP实验:

配置静态路由: (config) ip route <address> <mask> <next-hop>

激活OSPF: (config) router ospf <process-id>

宣告子网属于某个区域: (config-router) network <net-ip> <reverse-mask>(取反) area <area-id>

设置虚电路(当某area不与area 0直连的时候): (config-router) area <area-id> virtual-link <opponent-router-id> 需要双向建立虚连接

合并路由表(某area): (config-router) area <area-id> range <net-ip> <mask>(不用反)