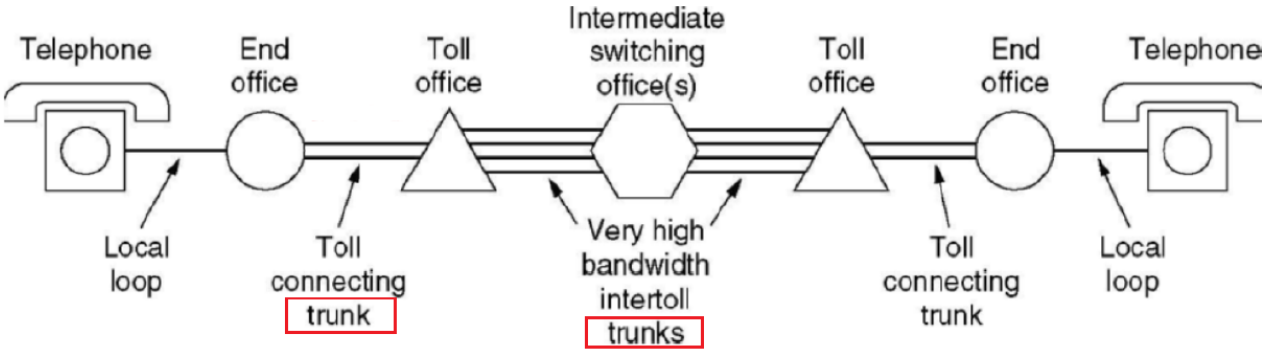
# 第2章　物理层补充

## 2.5　公用电话系统 PSTN (重要)

**电话**将模拟信号转为模拟信号。**codec**是将模拟信号转成数字信号，**modem**是将数字信号转成模拟信号。
公用电话系统用于传递人声，主要分为如下几个部分：

- 本地回路 Local loop：用来传输模拟信号的双绞线，modem, 是电话和 end office 之间的。multipath fading不能造成其信号衰减
- 干线 Trunk：数字光缆，是end office 和 switching office 之间的, FDM或者TDM
- 交换局 Switching office：进行了通话的交换，从手动切换变成了计算机切换。




其switch是一种典型的circuit switch

### 2.5.1　中继线和多路复用

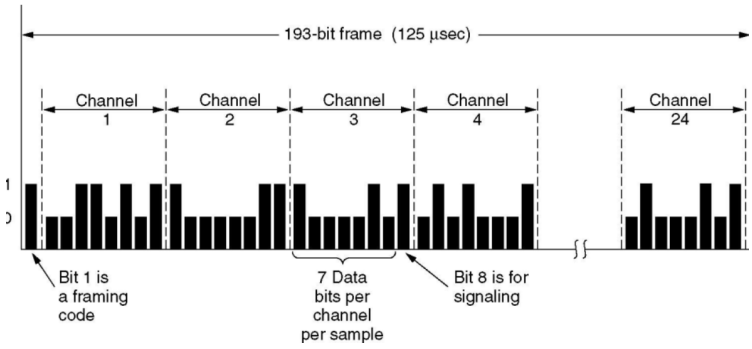
中继器用来将衰减的信号再生，想传的远用中继器。转发器放大信号
Based on the attenuation of light through fiber in the infrared region, three wave length bands are used for optical communication except 1.80

### 2.5.2　载波 Carrier

PCM 脉冲编码技术：每秒采样 8000 次，每次的采样量化成 8bit 的二进制数

**De inition 2.7** *T1 载波*：有 *24* 个 *PCM* 信号，数据传输速率是 *1.544Mbps*，一个数据帧共有 *193* 位，一共有 *24* 个信道，其中每个信道有 *8bit*，*7* 位是数据，*1* 位是信号，第 *1* 位是帧码。因此 *193bit* 中有效的数据有 *168bits*，开销率约为 *13%*

T1 carrier (1.544 Mbps): 24 voice channels multiplexed together




**De inition 2.8** *E1* 载波，数据传输速率是 *2.048Mbps*，一共有 *32* 个 *PCM* 信号，其中 *30* 个用来传数据，*2* 个传输信号，因此开销是 *6.25%*

# 第3章　数据链路层补充

## 3.2　差错检测和纠正

### 3.2.1　纠错码 Error Correcting Code

**De inition 3.1** 假设一帧由 $m$ 位数据和 $r$ 位冗余组成，记 $n = m + r$ 则该编码方式称为 $(m, n)$ 码

**De inition 3.2** **海明距离（必考）**：两个码字 *(codeword)* 中不同的位的个数，如果两个码字的海明距离为 $d$，则需要出现 $d$ 个 *1* 位的错误才能把正确的码字变成错误的码字。(即XOR后1的个数)

- 海明距离为 n 的编码方案只能检测出 n-1 个错误，因为如果 n 位都不同无法判断到底谁是对的
- 为了**检测 d** bit错误，需要 d+1 的海明距离的编码方案
- 而为了**纠正 d** bit错误，则需要 2d+1 海明距离的解决方案

对于每 $2^m$ 个合法的消息，每个消息对应有 n 个非法的码字 (即海明距离为 1 的非法码字有 n 个)，此时

# 第4章　网络层补充

网络层提供的服务都是无连接，不可靠的

### 距离矢量路由算法 Distance Vector Routing

收敛速度非常慢。距离矢量算法对好的结果反应特别迅速，对坏消息的反应非常迟钝。

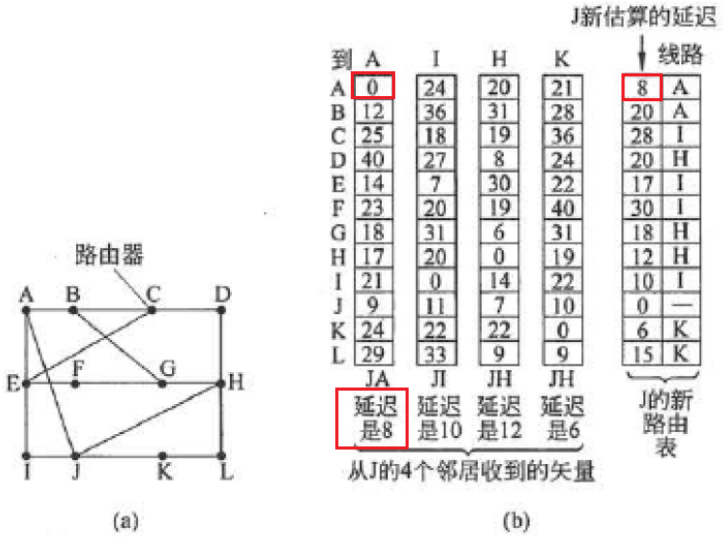



图　5-9

（a）一个网络示例；（b）来自 A、I、H、K 的输入，以及 J 的新路由表

### 链路状态路由算法 Link State Routing

当链路状态发生变化时，路由器才会向所有其他路由器发送消息。该算法需要每个路由器需要完成如下五个步骤：

- 发现邻居节点，并了解其网络地址
- 设置邻居节点的距离或者成本度量值
- 构造一个包含刚才所得信息的**链路信息包**
- 洪泛法将包发送给所有的路由器(而距离向量法只和邻居交流)，并接受来自所有其他路由器的信息包
- 用Dijkstra计算出到达每个路由器的最短路径

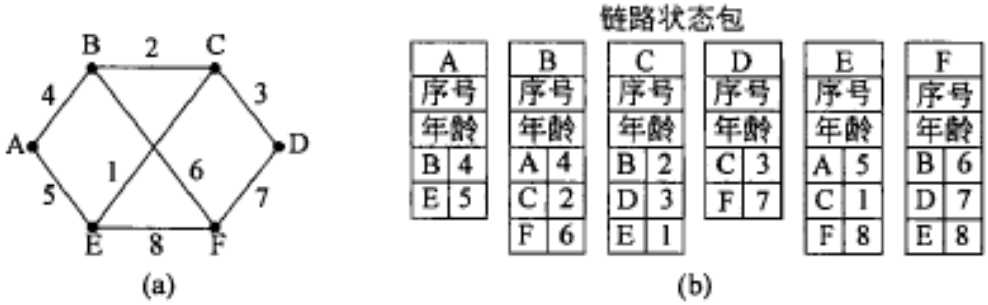



图　5-12

（a）一个网络示例；（b）该网络的链路状态包

实验补充： 抓包实验

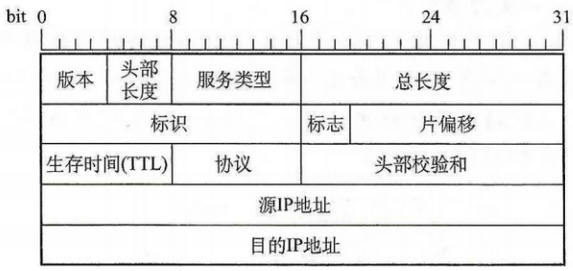



图 1 IP 分组头结构

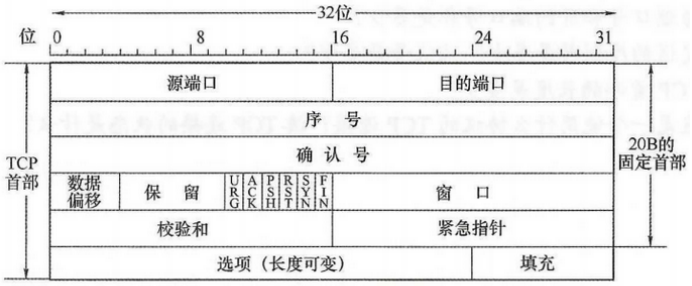
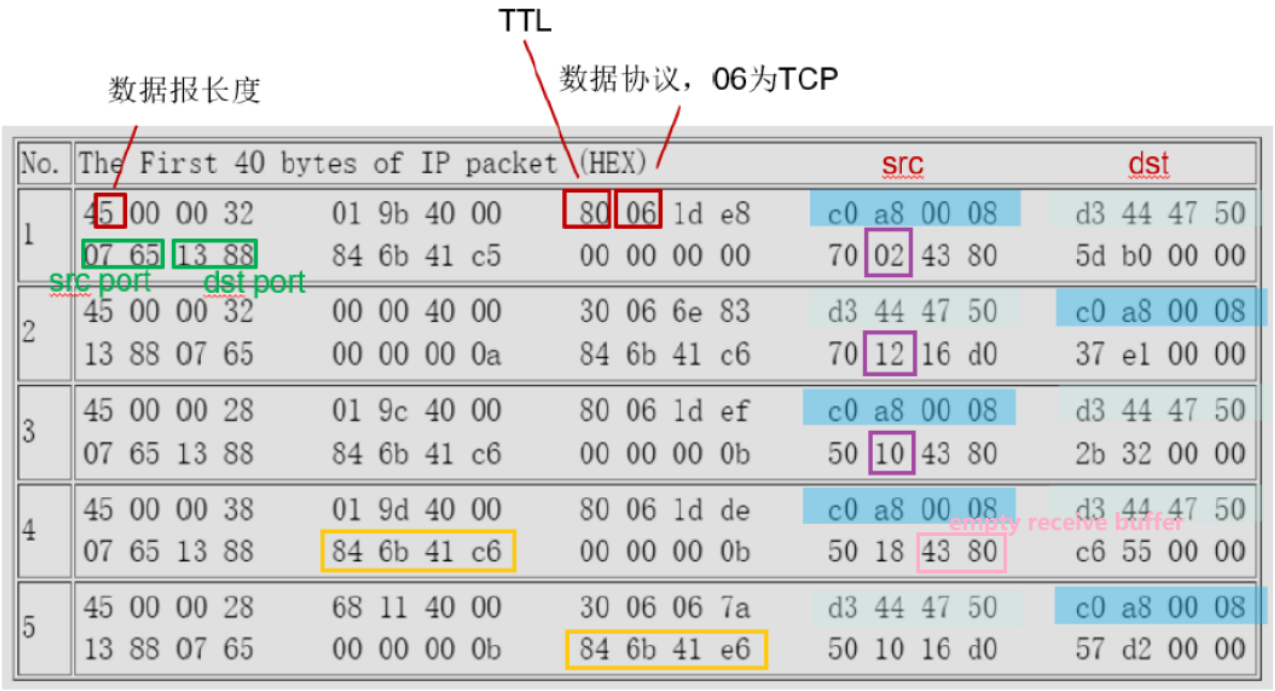



图 2 TCP 段头结构




TCP的建立：TCP的建立需要三次握手，所以要找满足【（1）SYN=1；（2）SYN=ACK=1（3）ACK=1的报文段（可以看成找02，12，10），另外第一个和第三个的序号要紧挨着（注意第一个分组的序号为84 6b 41 c5，第三个分组的序号为84 6b 41 c6，两者相差1）

通过以太网传输时需要填充：因为【快速以太网数据帧的data最小长度为46B，即IP分组（data+IP首部的总和min=46B）即小于46B的需要“填补”】，根据IP分组的第一行“总长度”字段（分组中的第二字节），从上往下的分组为00 32H、00 32H、00 28H、00 38H、00 28H，第1、2、4个分组大小分别为50B、50B、52B（均大于最小帧长46B），其中第3、5分组28H表明分组大小为40B【一种8片首饰，牢记】——指分片的数据长度必须是8B的整数倍。

dst已经收到多少字节的数据：通过序号来判断收到了多少，dst确认号-src确认号=已经确认收到的字节数。由于三次握手的“第三次”就可以开始发送数据了，第三个分组中的初始序号为 84 6b 41 c6，而第五个分组的确认号为84 6b 41 e6，两个作差得到20H，即32B (或者问题换为问通过5看4接受了多少数据，答案仍然如上，图中黄框)

若表1中的某个IP分组在S发出时的前40B如表二所示，则该IP分组到达H时经过了多少个路由器？

表 2

| | | | | | |
|---|---|---|---|---|---|
| 来自 S 的分组 | 45 00 00 28 | 68 11 40 00 | 40 06 ec ad | d3 44 47 50 | ca 76 01 06 |
| | 13 88 a1 08 | e0 59 9f f0 | 84 6b 41 d6 | 50 10 16 d0 | b7 d6 00 00 |

经过多少个路由器是要看TTL的。由于S发出的IP分组的标识为6811H，所以表2中的分组和表一中的第5个分组是“同一数据报”，S发出的IP分组的TTL=40H，而表1的第5个IP分组的TTL是31H，40H-30H，因此可以判断该IP分组到达H时经过了16个路由器。

base64编码是网络层中的一种传输编码，其转换过程如下（过程不需要掌握）：

（1）hello查ASCII表可以得到分别为0110 1000　0110 0101　0110 1100　0110 1100　0110 1111直接连接为二进制

（2）对上面从左到右，按每6位一组，进行分组，如果末尾不足6位，则自动以0补齐，得到：

011010　000110　010101　101100　011011　000110　111100

（3）对上面每个6位组前补齐00变为8位，得到如下：

00011010　00000110　00010101　00101100　00011011　00000110　00111100

（4）得到十进制为26　6　21　44　27　6　60，然后查表编码

A binary file is 3072 bytes long. How long will it be if encoded using base64 encoding, with a CR+LF pair inserted after every 80 bytes sent **and** at the end?

$$(3072 \times 8) \div 24 \times 32 \div 8 = 4096\ bytes$$

$$4096 \div 80 = 51.2 = 51\ bytes$$

$$4096 + (51 + 1(end)) \times 2 = 4200\ bytes$$

# 第8章　网络安全补充

就考2-3分

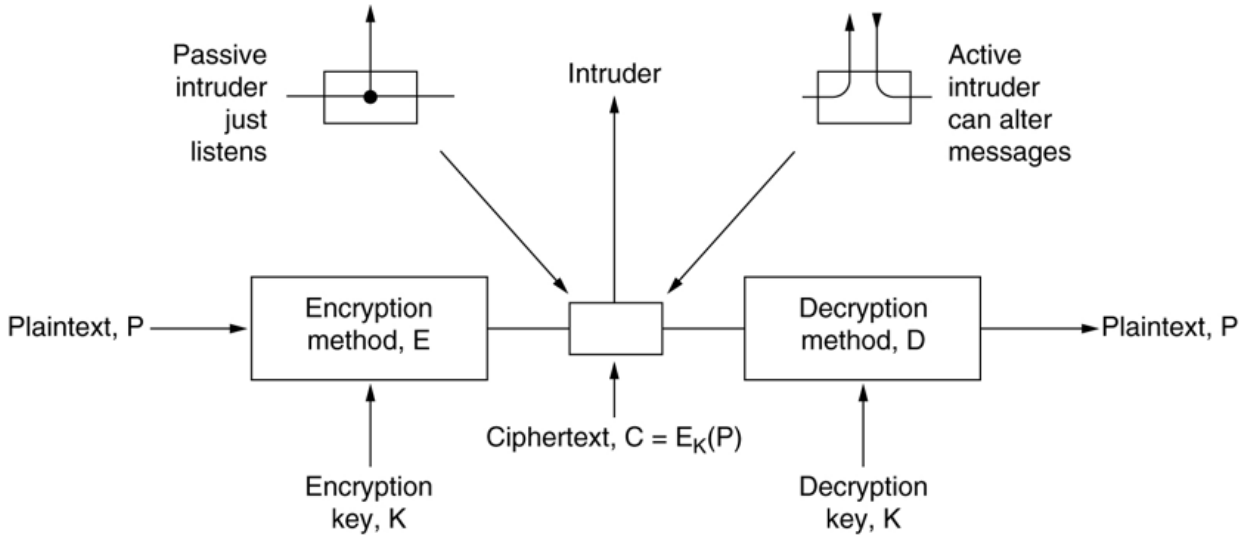
## 8.1　密码学相关知识

### 8.1.1　加密算法

古典密码学的加密算法主要有替换密码和转置密码，置换密码将每个或者每组字母用另一个或者另一组字母来代替，最古老的密码之一就是凯撒密码，采用了单个字母替换。替代密码将明文重新排序，需要密钥进行解密

### 8.1.2　加密模型

任何加密模型的安全性都取决于密钥的长度以及攻破密码所需要的计算量，加密模型可以用下面的图来表示：




### 8.1.3　两个密码学基本原则

- 原则 1：被加密后的信息一定包含了冗余信息
- 原则 2：需要采取方法来对抗重放攻击

### 8.1.4　两类密码体制

密码体制主要分为对称密钥体制和公钥密码体制，对称密钥使用相同的加密密钥和解密密钥，而公钥密码使用不同的加密密钥和解密密钥，分别叫**公钥**和**私钥**，常见的加密算法有：

- DES(数据加密标准) 是对称加密，是一种分组密码，由 IBM 公司研制，有安全性更强的三重 DES

- AES(高级加密标准) 是对称加密，由 Jaon Daemen 和 Vincent Rijmen 提出，加瓦罗域，
- RSA 公钥密码，以 Galois 的域理论为基础（不可攻破，是非对称的）。very difficult to factor large numbers，能被选择明文攻击破解的
- DES 和 AES 都是块密码，因为是以一定大小的块作为单位来加密的，可以用Cipher block chaining来防止攻击。使用公钥加密的公钥应该是**接受方的公钥， 解密用接收方的私钥**

#### 8.1.5 密码攻击

**De inition 8.1** 重放攻击（*replay-attack/reflection-attack*）：直接截取密码报文，不需要进行破译，而是伪装成发送方(挑战authentication)发给接受方，然后获取其回复消息，这种攻击方式可以使用不重数（*nonce*）来化解。

**De inition 8 .2** 中间人攻击（*man-in-the-middle*）：中间人把不重数用自己的私钥加密之后，分别向发送方和接受方发送获取密钥的请求，然后获得其密钥破译密码。

#### 8.1.6 密码散列函数

散列函数也叫做哈希函数 (hash function)，具有单向加密的特点，输入长度不固定但是输出的长度是固定的，要找到两个输出的报文在计算上是不可行的，常见的密码散列函数有：

- MD5：报文摘要算法，算法需要将报文按照规则填充成 512 的倍数，然后每个 512 位的块分成 128 位的块，128 位的再分成 32 的小块进行 hash
- SHA 是美国 NIST 机构提出的散列算法，但是码长是 160 位，比 MD5 更安全

#### 8.1.7 密钥分配

由于密码算法是公开的，网络的安全性就完全基于密钥的保护，不同的密码体系的分配方式不同，对于对称密钥：

- 设立密钥分配中心 (KDC,Key Distribution Center)，常用的密钥分配协议是 Kerberos V5，使用界别服务器 AS 和证书授予服务器 TGS
- 证书具有一定的有效期，过期就会失效，不能被用于多次重放攻击

而对于公钥的分配，可以使用认证中心 (CA) 把公钥和对应的实体进行绑定(CA的公钥可以用来验证网站证书)，ITU-T 制定了 X.509 标准，并在 RFC5280 中给出了**互联网公钥基础设施 PKI**，

### 8.2 互联网安全协议

#### 8.2.1 IPsec 协议族

IPsec 是可以在 IP 层提供互联网通信安全的协议族，分为三个部分：

- IP 安全数据报格式的两个协议：鉴别首部协议 AHP 和封装安全有效载荷协议 ESPP

- 有关加密算法的三个协议
- 互联网密钥交换协议 IKEP

IP 安全数据报有两种不同的方式，分别是运输方式和隧道方式。运输方式是在运输层的报文段的前后分别添加若干控制信息再加上 IP 头部，隧道在原始的 IP 数据报的前后添加控制信息，再加上新的 IP 首部构成一个 IP 安全数据报。

安全关联 SA 是发送 IP 安全数据报之前在源实体和目的实体之间创建一条网络层的逻辑连接，**将无连接的网络层变成了具有逻辑连接的网络层**，并且这种链接是一个单向连接。

### 8.2.2 安全套接字层 SSL

是 Netscape 提出的，运输层的安全协议，作用在 HTTP 和运输层之间，在 TCP 之上建立一个安全通道，可以提供如下服务：

- SSL 服务器鉴别，允许用户证实服务器的身份
- SSL 客户鉴别，允许服务器证实客服身份
- 加密 SSL 会话，对客户和服务器之间的报文进行加密，并且检测报文是否被篡改

### 8.2.3 应用层安全协议

PGP 是 Zimmerman 于 1995 年开发的电子邮件的标准，用于保护邮件的隐私，

## 8.3 防火墙和入侵检测

### 8.3.1 防火墙 Firewall

防火墙是一种访问控制技术，是一种特殊的路由器，可以禁止任何不必要的通信，可以实施一定的访问控制策略，防火墙内的是可信的网络，而防火墙外是不可信的网络，实现防火墙的主要技术有：

- 分组过滤路由器：按照一定的规则进行分组过滤，对进出内部网络的分组执行转发或者丢弃
- 代理服务器：在应用层通信中起到报文中继的作用，一种网络应用需要一个应用网关，所有的进出网络的应用程序都必须通过应用网关

真正的防火墙一半两种技术混合使用。