第一章　计算机网络及其参考模型

LAN：Local Area Network，局域网

WAN：Wide Area Network，广域网

ISP: Internet Service Provider，网络服务供应商

局域网设备：集线器(hub)、网桥(bridge)、交换机(switch)、路由器(router)

广域网设备：路由器(router)、调制解调器(modem)

以太网是局域网。

为什么要使用数据包？

1. 计算机可以轮流发送数据包；
2. 如果数据包丢失，只需重传少量的数据；
3. 数据可从不同的路径到达。

带宽：在给定时间内可传输的数据量。

吞吐量：在特定时间内所测量的出的真实的数据流量。

吞吐量 <= 带宽

使用分层模型的原因：

1. 降低复杂度；

2. 标准化接口；

3. 促进模块化工程；

4. 确保内部可操作的技术；

5. 促进发展；

6. 简化教学与学习。

OSI 层	功能	TCP/IP 协议
应用层(Application layer)	文件传输，电子邮件，文件服务，虚拟终端	TFTP，HTTP，SNMP，FTP，SMTP，DNS，Telnet
表示层(Presentation layer)	数据格式化，代码转换，数据加密	没有协议
会话层(Session layer)	解除或建立与其他接点的联系	没有协议
传输层(Transport layer)	提供端对端的接口	TCP，UDP
网络层(Network layer)	为数据包选择路由	IP，ICMP，RIP，OSPF，BGP，IGMP
数据链路层(Data link layer)	传输有地址的帧，错误检测功能	SLIP，CSLIP，PPP，ARP，RARP，MTU
物理层(Physical layer)	以二进制数据形式在物理媒体上传输数据	ISO2110，IEEE802，IEEE802.2

OSI: Open System Interconnection，开放系统互连

OSI 的七层：

第一层：物理层(Physical)，二进制传输；关键词：信号、介质。

第二层：数据链路层(Data Link)，介质访问；关键词：帧、媒介访问控制；提供数据的可靠传输，与物理寻址、网络拓扑、网络接入、错误通知、帧的顺序传送和流控制有关。

第三层：网络层(Network)，寻址和最优路径选择关键词：路径选择、路由、寻

址；在路由时提供连接和路径选择。

第四层：传输层(Transport)，终端对终端的连接；关键词：可靠性、流控制、错误校正。

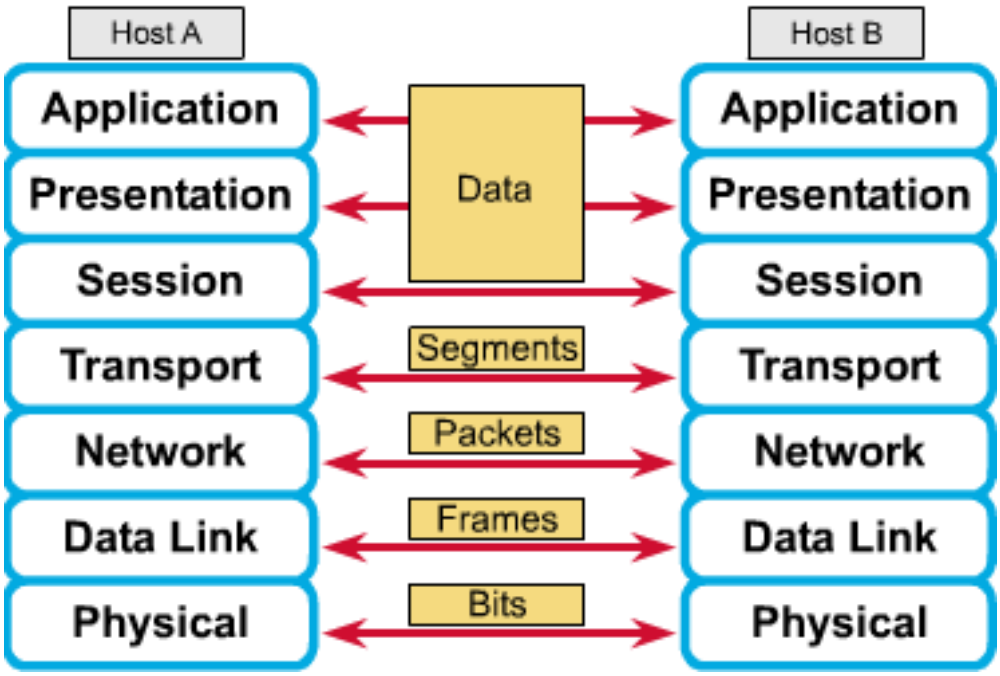
第五层：会话层(Session)，内部宿主连接；关键词：会话；管理表现层实体间的数据交换。

第六层：表现层(Presentation)，数据显示和加密；关键词：通用格式；与数据结构和数据传输语法间的协商有关。

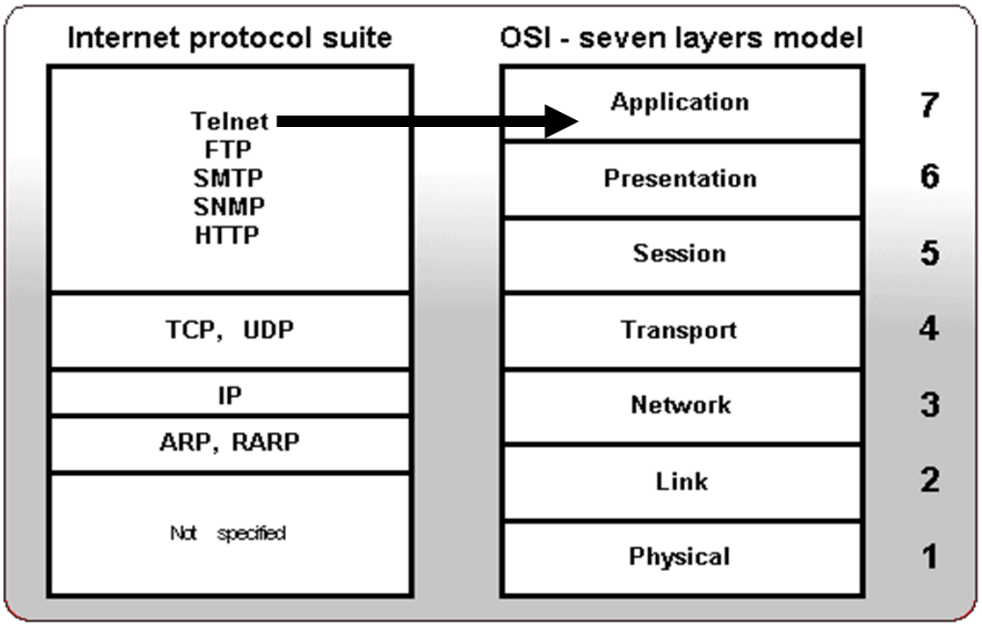
第七层：应用层(Application)，用户界面；关键词：浏览器；向用户程序提供网络服务。

5-7 层被称为应用层；1-4 层被称为数据流层。

各层传输数据类型：



各层协议：



TCP/IP 的四层：

第一层：网络接入层(Network Access)；

第二层：网际互联层(Internet)；最佳路径选择和同层的包交换。

第三层：传输层(Transport)；处理可靠性、流控制、纠错的服务质量问题，将应用层信息打包成段。

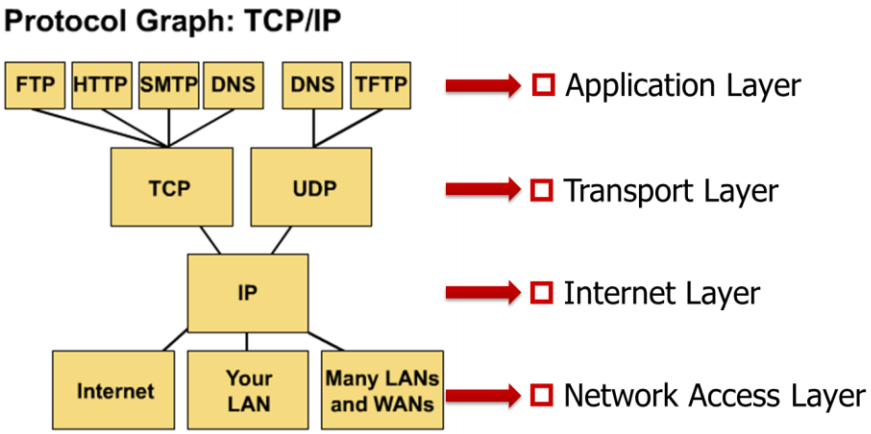
第四层：应用层(Application)；处理高层拓扑、显示问题、编码和通话控制。

TCP：Transmission Control Protocol，传输控制协议

UDP：User Datagram Protocol，用户数据电报协议

IP：Internet protocol，互联网协议

TCP/IP 拓扑层次图：



FTP - File Transfer Protocol 文件传输协议

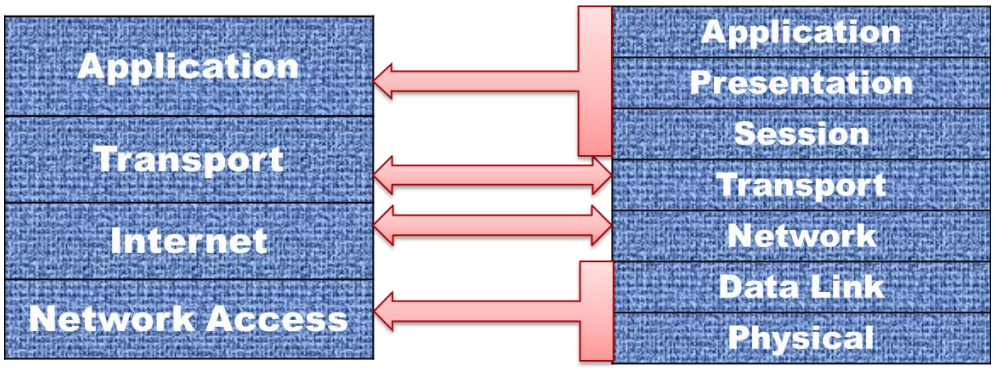
HTTP - Hypertext Transfer Protocol 超文本传输协议

SMTP - Simple Mail Transfer protocol 简单邮件传输协议

DNS - Domain Name System 域名系统

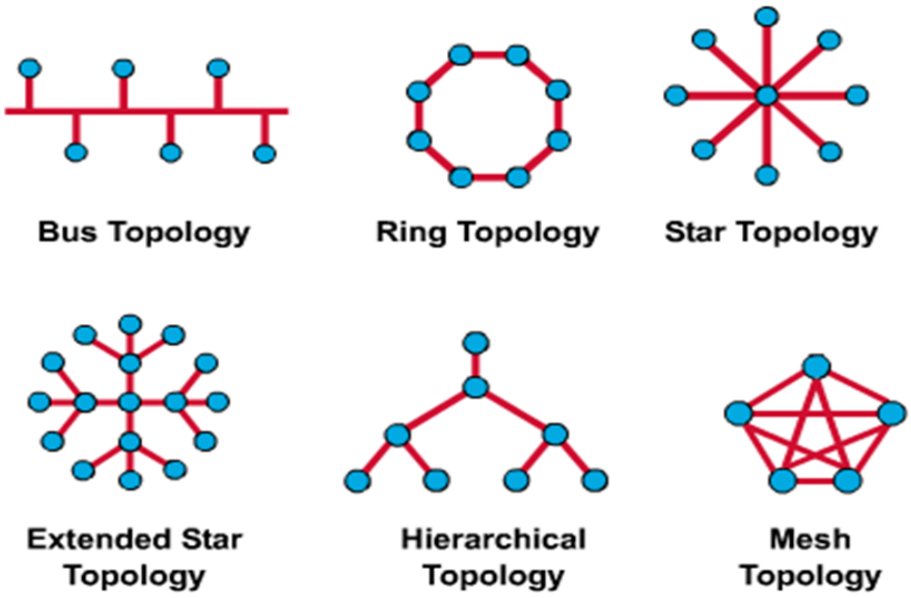
TFTP - Trivial File Transfer Protocol 简单文件传输协议

TCP/IP 和 OSI 各层的对应关系：



物理网络拓扑结构：

总线拓扑，环形拓扑，星形拓扑，扩展星形拓扑，层次型(树形)拓扑，网络拓扑



总线拓扑：

优点：所有节点之间都能直接通信。

缺点：如果线缆上的一点断开，会影响到所有两边的节点。

双环形拓扑：在环形拓扑的基础上增加一个冗余环路，提高了可靠性和灵活性。

星形拓扑：

优点：允许所有节点方便地交流，有较好的安全性和接入控制。

缺点：中间节点崩溃会使整个网络崩溃，冲突也会是一个严重的问题。

网络拓扑：

优点：连通性和可靠性最好。

缺点：介质和连接的数量无法控制。

细胞拓扑：用于无线网。

NIC：Network Interface Card，网卡

网络设备：

第一层设备：集线器(Hub)，中继器(Repeater)，网卡(NIC)*

第二层设备：网卡(NIC)，交换机(Switch)，网桥(Bridge)

第三层设备：路由(Router)

网卡：MAC 地址，接受和发送数据，实现串行信号和并行信号之间的转换。

中继器：整理、放大并重发信号，不做过滤，不划分冲突域。

集线器：多端口的中继器，整理、放大并复制电信号向所有端口转发，不做过滤，不划分冲突域。

网桥：通过 MAC 地址判断，维护 MAC 地址表，划分冲突域。

第二章　OSI 层次：物理层

网络类型：

1. 共享介质环境；
2. 点对点网络环境（广泛使用于拨号网络中）。

双绞线类型：

STP：Shielded Twisted Pair，屏蔽双绞线

ScTP：Screened Twisted Pair，网屏式双绞线

UTP：Unshielded Twisted Pair，非屏蔽双绞线

STP（屏蔽双绞线）:

由 4 对细铜线组成，每根线外使用有颜色的塑料隔离；

每两根线一个壳，八根线共一个壳，最外层一个外部护套。

ScTP（网屏式双绞线）:

由 4 对细铜线组成，每根线外使用颜色的塑料隔离；

八根线共一个壳，最外层一个外部护套。

UTP（非屏蔽双绞线）:

由 4 对细铜线组成，每根线外使用颜色的塑料隔离；

只有最外层的一个外部护套。

STP 和 ScTP 的优点：

1. 比 UTP 抗外部干扰的能力强。

STP 和 ScTP 的缺点：

1. 信号传播距离较短；
2. 隔离层极大地增加了线缆的大小、重量和价格；
3. 金属屏蔽层必须接地，线缆难以安装。

UTP 的优点：

1. 线缆不需要接地，因此便于在线缆末端加上连接器；
2. 价格低廉；
3. 直径小，因此安装简单且更适合安装在管道中；
4. 和其他铜传输介质具有一样的数据传输速率；
5. 使用 RJ 连接器后极大地降低了噪音的影响。

UTP 的缺点：

1. 更容易受到电子噪音和干扰的影响；
2. 相对于同轴电缆和光缆而言，能支持的线缆长度较短。

Coaxial（同轴电缆）:

铜导线，外部包有绝缘塑料，再外层是铜网屏蔽层，最外层是外部护套。

同轴线缆的优点：

1. 与 STP 和 UDP 相比，统战线缆可以在几乎没有中继器推动的情况下，在距离较远的两个网络节点之间传输数据；
2. 比光缆便宜（比 STP 和 UTP 贵）。

Fiber-Optic（光纤）:

硅的氧化物作纤芯，外面一层覆层用于防止光外溢，再外层是缓冲层，包裹在一层加强材料当中，最外层是外套。

Fiber-Optic 的优点：

1. 可以使用更长的距离；
2. 接口不容易损坏。

Fiber-Optic 的缺点：

1. 价格昂贵。

Single Mode（单模光纤）:

轴传播；

比多模光纤快，传输距离长；

较多使用在 WAN；

直径小；

通常使用激光器型发送器，也使用发光二极管。

Multimode（多模光纤）:

光以不同的角度进入光纤；

直径比单模光纤大；

多用在 LAN 中；

能量损耗较大。

无线介质类型：

Lasers（激光）、Infrared（红外线）、Radio（无线电）

UTP 线缆的类型：

一类线：主要用于语音传输，不用于数据传输。

二类线：用于语音和最高 4Mbps 的数据传输，常见于令牌网。

三类线：EIA/TIA568 标准指定电缆，用于语音传输及最高传输速率为 10Mbps 的数据传输，主要用于 10BASE-T。

四类线：用于语音传输和最高传输速率 16Mbps 的数据传输，主要用于令牌网和 10BASE-T/100BASE-T。

五类线：增加了绕线密度，外套高质量绝缘材料，用于语音和数据传输(主要为 100/1000BASE-T)，是最常用的以太网电缆。

超五类线：衰减小，串扰少，具有更高的衰减/串扰比和信噪比、更小的时延误差，主要用于 1000BASE-T。

六类线：性能远高于超五类标准，适用于高于 1Gbps 的应用。

七类线：带宽为 600MHz，可能用于今后的 10G 比特以太网。

UTP 线缆类型：

Straight Cable(直通线)、Rollover Cable(全反线)和 Crossover Cable(交叉线)

直通线：

1 号引脚与 1 号引脚相连，2 号与 2 号相连，其他依次类推，两端设备使用相同的引脚。

全反线：

又叫控制台线缆，1 号引脚与 8 号引脚相连，2 号与 7 号相连，其他依次类推，

用于连接 PC 的串口与路由器或交换机的控制台端口。

交叉线：

1 号引脚与 3 号引脚相连，2 号与 6 号相连，4 号与 7 号相连，5 号与 8 号相连。

线缆引脚的使用：

1. 连接计算机与网络设备的控制台端口时使用全反线；
2. 两台设备使用的传输引脚相同时使用交叉线；
3. 两台设备使用的传输引脚不同时使用直通线；
4. 计算机、路由器、服务器和无线接入点的以太网接口通常使用 1、2 号引脚；
5. 交换机、集线器和网桥通常使用 3、6 号引脚；
6. 连接两个隔离的计算机系统创建小型局域网时使用交叉线。

5-4-3-2-1 Rule：

1. 允许将网络划分为 5 个网段；
2. 在任何两台最终用户设备之间最多有 4 台中继器或集线器；
3. 5 个网段中的 3 个可以连接最终用户设备；
4. 如果在两台最终用户设备之间有 5 个网段，则其中两个网段不能连接最终用户设备，只能作中继器链路；
5. 上述将构成一个大型的冲突域，最大站点数 1024，网络直径达 2500 米。

EMI：electromagnetic interference，电磁干扰

late collision：发生在一个帧传送过程中的前 64 个字节的冲突。

consumption delay：由 late collosion 引起的延迟。

无噪信道的最高传输速率 $C = W \log_2 L$ (bps)，其中 W 为信道的带宽（以 Hz 为单位），L 为表示数据的信号电平的数量。

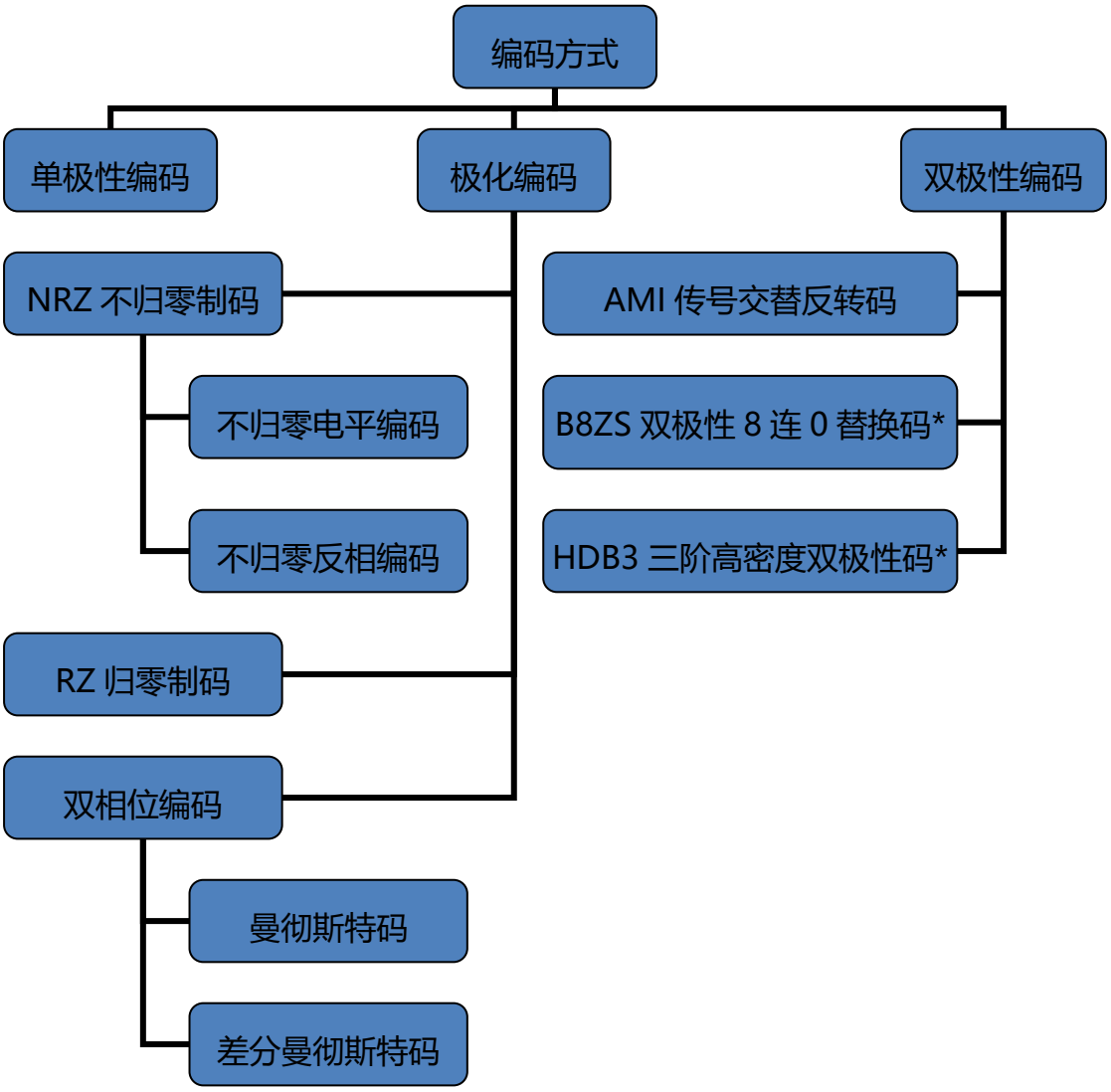
噪声信道的最高传输速率 $C = W \log_2(1+S/N)$ (bps) ,其中 W 为信道的带宽(以 Hz 为单位），S 为信道内所传信号的平均功率，N 为信道内部的高斯噪声功率，S/N 称为信噪比。

波特率/调制速率（baud）: 信号每秒钟变化的次数。

比特率（bit）: 每秒钟传送的二进制位数。

基带：基本频带，指传输变换前所占用的频带，是原始信号所固有的频带。

基带传输：在传输时直接使用基带数字信号(不转换为模拟信号，即不调制)。



NRZ： Non-Return to Zero，不归零制码

RZ： Return to Zero，归零制码

单极性编码：

用零电平表示“0”，正电平表示“1”，容易产生传播错误。

缺点：

1. 难以分辨一位的结束和另一位的开始；
2. 发送方和接收方必须有时钟同步；

3. 若信号中“0”或“1”连续出现，信号直流分量将累加，单极性编码的直流分量问题严重。

不归零电平编码：

用负电平表示“0”，正电平表示“1”（或相反）。

缺点：

1. 难以分辨一位的结束和另一位的开始；
2. 发送方和接收方必须有时钟同步；
3. 尽管没有单极性编码严重，但若信号中“0”或“1”连续出现，信号直流分量仍将累加。

不归零反相编码：

信号电平的一次翻转代表比特 1，无电平变化代表 0。

优点：

每次遇到“1”（或“0”）都要发生跃迁，可以根据电平跃迁进行有限的同步。

归零制码（RZ：Return to Zero）：

用负电平表示“0”，正电平表示“1”（或相反），比特中位跳变到零电平，从而提供同步。

优点：

信号本身带有同步信息，经济性好，且不易出错。

缺点：

需要采用三个不同电平，两次信号变化来编码 1 比特，因此增加了占用的带宽。

曼彻斯特码（Manchester）:

每一位中间都有一个跳变，从低跳到高表示“0”，从高跳到低表示“1”。

优点：

克服了 NRZ 码的不足，每位中间的跳变既可作为数据，又可作为时钟，能够自同步；同时只采用两个电平，跳变减少，比 RZ 码效率更高。

差分曼彻斯特码（Differential Manchester）

每一位中间都有一个跳变，表示时钟；位前有跳变表示“0”，无跳变表示“1”。

优点：

时钟、数据分离，便于提取。

双极性传号交替反转码（AMI）:

采用三个电平：正、负与零，零电平表示“0”，正负电平的跃迁表示“1”。

优点：

1. 对每次出现的“1”交替反转，使直流分量为 0；
2. 尽管连续“0”不能同步，但连续“1”可以同步。

多路复用：为了提高线路利用率，让多个信号共用一条物理线路。

TDM：Time Division Multiplexing，时分复用

STDM：Statistic TDM，统计时分复用

FDM：Frequency Division Multiplexing，频分复用

WDM：Wavelength Division Multiplexing，波分复用

CDM：Code Division Multiplexing，码分复用

CDMA：Code Division Multiple Access，码分多址，即码分复用

多路复用的类型：

时分复用、频分复用、波分复用（光的频分复用）和码分复用

通信方式类型：

单工、半双工和全双工

单工：信号单向传输。

半双工：信号可双向传输，但不同时。

全双工：信号可同时双向传输。

第三章　OSI 层次：数据链路层

LLC：Logical Link Control，逻辑链路控制

MAC：Media Access Control，介质访问控制

LLC 提供的服务：

1. 无应答的无连接服务；
2. 带应答的无连接服务；

3. 带应答的面向连接服务。

以太网：逻辑总线拓扑，物理星形或扩展星形拓扑。

令牌环：逻辑环形拓扑，物理星形拓扑。

FDDI：逻辑环形拓扑，物理双环形拓扑。

CSMA/CD：Carrier Sense Multiple Access with Collision Detection，带冲突检测的载波侦听多路接入

CSMA：先侦听线路，如果发现空闲，则发送数据，否则等待。

CD：在传输过程中，仍然侦听线路，如果冲突检测到，则先广播拥塞信号，后退算法决定哪个设备再次接入介质。

局域网数据传输的类型：

单播、组播和广播

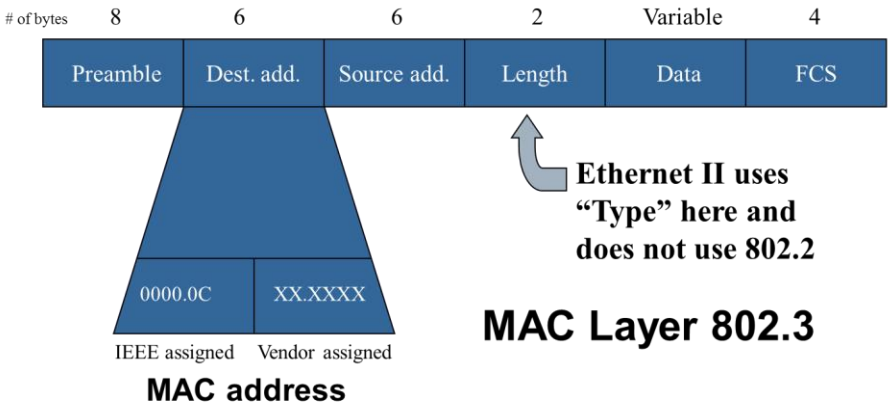
数据链路层的两个部分：

1. MAC :向下到介质的过渡;定义了怎样在物理线缆上传输帧,处理物理寻址，定义网络拓扑，定义线缆规章。
2. LLC：向上到网络层的过渡；标示不同的拓扑类型并封装他们。

以太网帧格式：

前导码，目的 MAC 地址，源 MAC 地址，长度，数据，帧校验序列

注意：目的地址在前，源地址在后



CRC：cyclic redundancy check，循环冗余校验

第二层通过 LLC 和高层通信。

第二层使用帧组织数据。

第二层使用 MAC 地址寻找目的计算机。

SAP：Service Access Point，服务接入点

DSAP：The Destination Service Access Point，目的服务接入点

SSAP：The Source Service Access Point，源服务接入点

MAC 地址：

48bits，前 6 位 16 进制数标示制造商、供货商，剩下的由供货商管理。

第二层广播地址为：FFFF.FFFF.FFFF.FFFF

广播在下面两种情况下发生：

1. 不知道目的 MAC 地址；

2. 目的地为全体主机。

PDU： protocol data unit

Sliding Window Protocol（滑动窗口协议）:

发送的信息帧都有一个序号。

发送端保持一个已发送但尚未确认的帧的序号表，称为发送窗口。

上界是要发送的下一个帧的序号，下界是未得到确认的帧的最小编号。

发送窗口大小 = 上界 - 下界，大小可变。

发送端每发送一个帧，序号取上界值，上界加 1；每接收到一个正确响应帧，下界加 1。

接收端有一个接收窗口，大小固定，但不一定与发送窗口相同。

上界是允许接收的序号最大的帧，下界是希望接收的帧。

接收窗口容纳允许接收的信息帧，落在窗口外的帧均被丢弃。序号等于下界的帧被正确接收，并产生一个响应帧，上界、下界都加 1。接收窗口大小不变。

信道利用率 = (L/b) / (L/b + R) = L / (L + Rb)

其中信道带宽 b 比特/秒，帧长度 L 比特，往返传输延迟 R 秒。

传输延迟大，信道带宽高，帧短时，信道利用率低。

pipelining（流水线技术）:

出错重传时可以从出错帧起丢弃所有后继帧或者接收窗口先暂存出错帧的后继帧，只重传坏帧。

BSS：Basic Service Set，基本服务集

BS：Base Station，基站

DS：Distribution System，分布式系统

ESS：Extended Service Set，扩展服务集

AP：Access Point，接入点

SSID：Service Set Identifier，服务集标识

主动扫描：

1. 发送探针请求（带有要连接的网络的 SSID）；
2. 匹配的 AP 发送一个探针相应；
3. 认证和连接完毕。

被动扫描：

1. 监听信标管理帧；
2. 如果监听到匹配的网络，则连接。

被动扫描是连续的过程。

随着信号的强弱变化，节点可能会连接和断开连接。

无线局域网（WLAN）中的冲突问题：

1. 隐藏站点问题（严重）；
2. 暴露站点问题。

CSMA/CA：Carrier Sense Multiple Access with Collision Avoidance，带冲突避免的载波侦听多路接入

RTS：Request To Send，请求传输帧

CTS：Clear To Send，清除传输帧

ACK：acknowledgment

CSMA/CA 原理：

发送站点在发送数据前，以控制短帧刺激接收站点发送应答短帧，使接收站点周围的站点监听到该帧，从而在一定时间内避免数据发送。

Transparent Bridge（透明网桥）:

“透明”是指局域网上的站点并不知道所发送的帧将经过哪几个网桥，因为网桥对各站来说是看不见的。透明网桥是一种即插即用设备，是目前以太网中使用得最多的网桥。

Source routing Bridge（源路由网桥）:

网桥发送帧时将详细的路由信息放在帧的首部中,从而使每个经过的网桥都了解帧的路径。在令牌环网络中被广泛使用。

二层设备还是在同一个广播域中。

网桥使用软件进行包转发，而交换机使用硬件。因此，交换机比网桥效率高。

有些交换机支持 cut-through switching（更快），而网桥只支持

store-and-forward switching。

路由器：

可划分冲突域和广播域；

通过检查目的逻辑地址转发包；

延迟更高；

可用作网关（连接使用不同介质或不同局域网技术的网络）。

第四章　OSI 层次：网络层

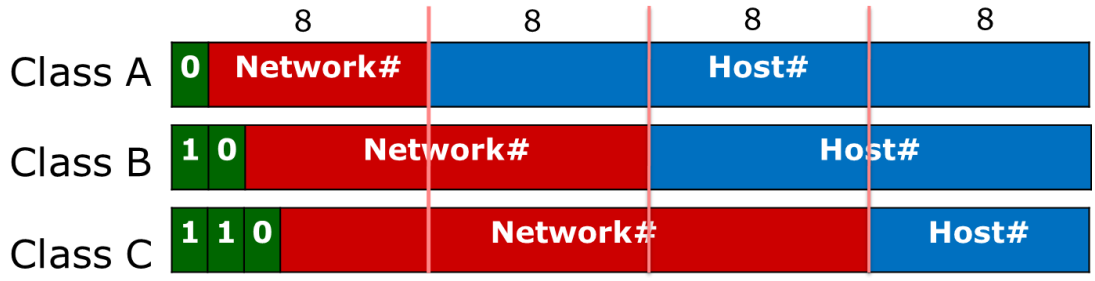
IP 地址：32Bits　　网络号+主机号

IP 地址分类：

Class A:0+7bits 网络号+24bits 主机号

Class B:10+14bits 网络号+16bits 主机号

Class c:110+21bits 网络号+8bits 主机号



IP 地址中前 8 位的含义：

0–127 Class A 地址

128-191 Class B 地址

192–223 Class C 地址

224–239 Class D – 组播

240–255 Class E - 研究

各类地址最多支持的主机数：

Class A：16,777,214 (2^{24} –2)

Class B：65,534 (2^{16} –2)

Class C：254 (2^{8} –2)

保留地址：

1. 网段地址：主机号全为 0
2. 广播地址：主机号全为 1

私有地址空间：

10.0.0.0 - 10.255.255.255 (A 类)

172.16.0.0 - 172.31.255.255 (B 类)

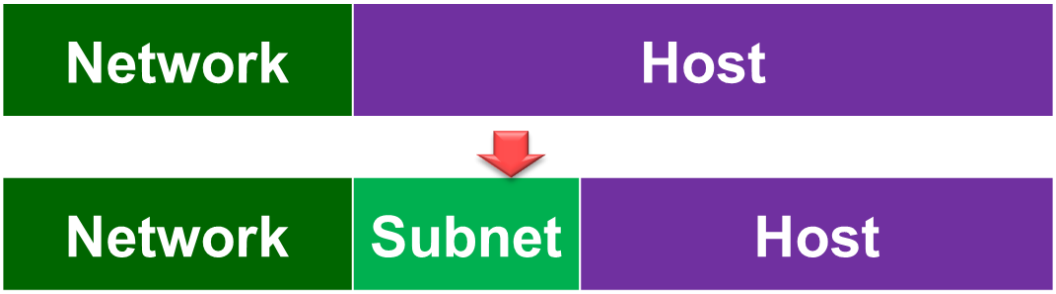
192.168.0.0 - 192.168.255.255 (C 类)

IP 地址消耗的解决办法：

1. NAT，即使用私有 IP 地址；
2. CIDR；
3. IPv6，长期解决办法。

子网：

提供灵活的寻址，通常由网管分配，能够减少广播域。



最小可借位数 = 2

最大可借位数 = host ID 位数 – 2

子网划分会造成地址的浪费。

子网划分的步骤：

1. 先确定是那类网；
2. 再确定要多少子网以及每个子网可支持的主机数；
3. 确定借位数；
4. 计算子网掩码；
5. 确定主机的可用地址范围。

计算子网地址的步骤：

1. 将 IP 地址转化为二进制；
2. 将子网掩码转化为二进制；

3. 对两个数进行与操作；

4. 将子网地址转化为带点的十进制。

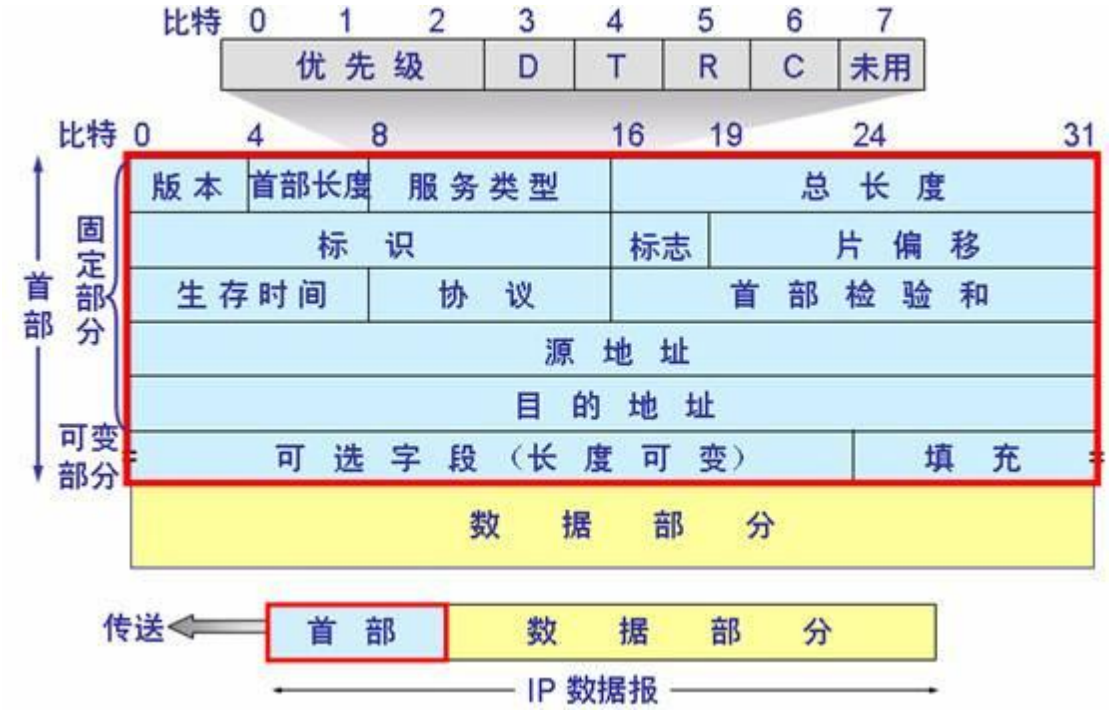
每个路由接口都必须有一个单独的网段地址。

IP 地址的分配：

1. 静态分配；

2. 动态分配。

IP 数据包的格式：



注意：源地址在前，目的地址在后。

RARP：Reverse Address Resolution Protocol，逆向地址解析协议

BOOTP：BOOTstrap Protocol，自举协议

DHCP：Dynamic Host Configuration Protocol，动态主机配置协议

RARP 的工作原理：

1. 发送主机发送一个本地的 RARP 广播，在此广播包中，声明自己的 MAC 地址并且请求任何收到此请求的 RARP 服务器分配一个 IP 地址；
2. 本地网段上的 RARP 服务器收到此请求后 ,检查其 RARP 列表 ,查找该 MAC 地址对应的 IP 地址；
3. 如果存在 ,RARP 服务器就给源主机发送一个响应数据包并将此 IP 地址提供给对方主机使用；如果不存在，RARP 服务器对此不做任何的响应；
4. 源主机收到从 RARP 服务器的响应信息，就利用得到的 IP 地址进行通讯；如果一直没有收到 RARP 服务器的响应信息，表示初始化失败。

BOOTP 的工作原理：

客户机发送 UDP 广播请求 IP 地址，服务器收到请求后返回 UDP 广播，包含请求的 IP 地址。

DHCP的工作原理：

1. 发现阶段，DHCP客户机以广播方式发送DHCP discover发现信息来寻找DHCP服务器（UDP广播）；
2. 服务器提供 IP 租用地址（UDP单播）；
3. 客户端接受 IP 租约（广播），告诉 DHCP 服务器接受了哪台服务器的租约；
4. 租约确认，服务器确认租期。

ARP Protocol：Address Resolution Protocol，地址解析协议

ARP 协议的（利用 IP 地址查询 MAC 地址）工作原理：

先查本地的 ARP 表(每个主机都维护一个 ARP 表),如果不存在目的 IP 的 MAC 地址，则广播（二层），目的主机收到广播报文之后，发现与自己的 IP 相匹配，就会发一个响应，其中包含自己的 MAC 地址，源主机收到响应报文之后，把目的主机 MAC 加入 ARP 表，然后再发送数据。

与不在一个网段的设备通信的方法：

1. 默认网关：连接这个网段的路由接口的 IP。（仍是 ARP 协议的一部分）
2. Proxy ARP(代理 ARP):中间设备(比如路由器)代表目的端发送一个 ARP 应答给发送请求的主机。

面向连接的网络服务：传输数据前会在发送者和接受者之间建立连接。

无连接网络服务 :分别对待每一个包。每个包有不同的路径 ,可以不按次序到达。IP 是无连接系统。

routed protocol/routable protocol（被路由协议/可路由协议）:

可以被路由器转发的协议，如 IP。

Non-routable protocol（不可路由协议）:

不能被路由器转发的包的协议，如 NetBEUI。

routing protocol（路由协议）:

用于路由器之间的协议，以便它们可以动态地获知路由信息，并将它们添加到路由表中。

IGP：Interior Gateway Protocols，内部网关协议

EGP：Exterior Gateway Protocols，外部网关协议

内部网关协议：

用于自治系统，包括 RIP, IGRP, EIGRP, OSPF 等。

外部网关协议：

用于自制系统之间，包括 EGP, BGP 等。

DVP：Distance-Vector Protocol，距离矢量协议

LSP：Link State Protocol，链路状态协议

距离矢量协议：

通过计算目标路由器与源路由器之间的距离矢量和来选择最佳路径，有频繁和周期性的更新，每次更新都将整张路由表发给周围的路由器，包括 RIP, IGRP 等。

链路状态协议：

每个路由器都了解整个网络的拓扑结构，利用算法计算两个路由之间的最短路径，更新由事件触发，每次更新都只像周围的路由器传递路由表的更新信息，包

括 OSPF 等。

RIP：Route Information Protocol，路由信息协议

IGRP：Interior Gateway Route Protocol，内部网关路由协议

EIGRP：Enhanced IGRP，增强的内部网关路由协议

OSPF：Open Shortest Path First，开放最短路径优先

RIP：

跳数位唯一的度量标准;

最大跳数为 15；

每 30 秒更新一次；

不总是选择最快路径；

容易产生网络拥塞。

IGRP 和 EIGRP：

以延迟、带宽、链路负载、可靠性（链路错误率）为度量标准；

最大跳数为 255；

每 90 秒更新一次。

OSPF：

以代价、速度、通信量、可靠性、安全性为度量；

更新由事件触发。

SLSM：固定长度子网掩码

VLSM：Variable-Length Subnet Mask，可变长子网掩码

CIDR：Classless InterDomain Routing，无类域间路由

Classful routing：有类路由

Classless routing：无类路由

有类路由中一个网络只能有一个子网掩码。

VLSM 的优点：

1. 更有效的使用 IP 地址
2. 使用路由汇总的能力更强

支持无类路由的协议：

OSPF，EIGRP，RIP v2，静态路由

只有未使用的子网才能在被划分。

先划分需要主机数最多的，然后接着按次序划分。

两个路由之间相连的端口各需要一个 IP 地址。

路由聚合：

减少路由表条目的数量；

隔离拓扑的变化。

隧道：

将原有的 IP 报文作为载荷，在外面包上一层新的 IP 包头，转换成为一个新的 IP 报文。

第五章　OSI 层次：传输层

TCP：可靠

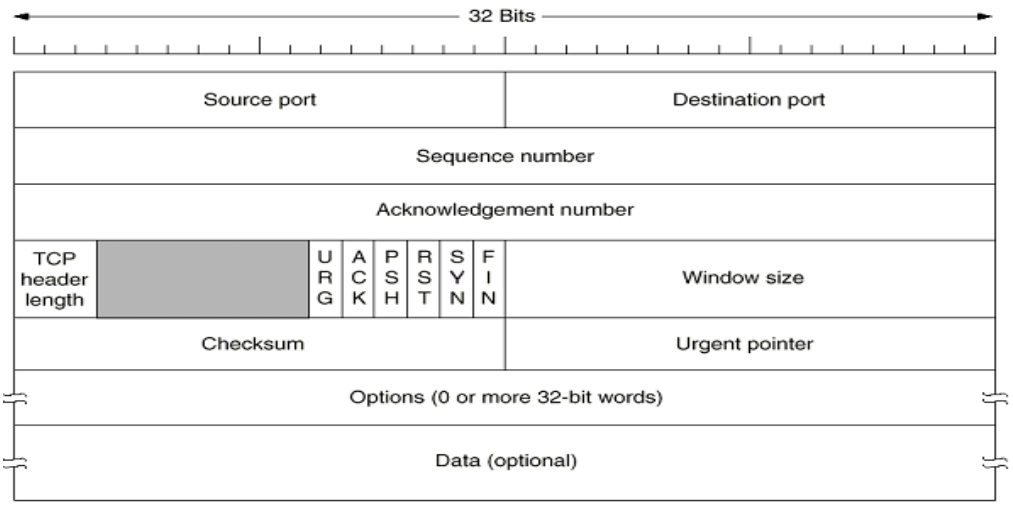
面向连接；

数据的分片、重组和有序分发；

重传所有丢失的或出错的报文；

使用确认；

提供流控制。



UDP：不可靠

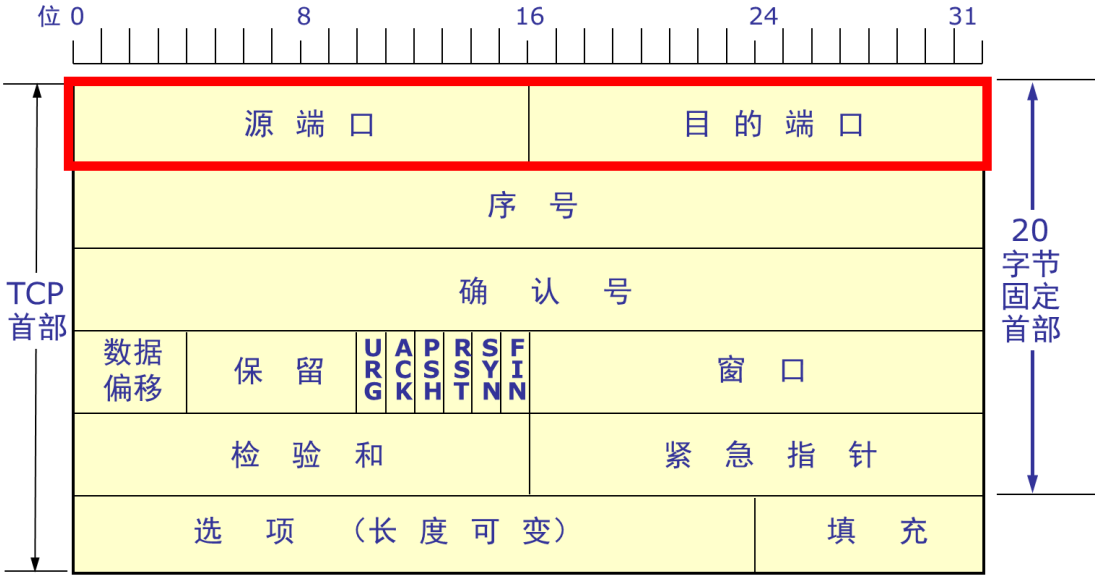
无连接；

无确认；

无流控制。

TCP 不支持单播和组播。

TCP 报头格式：



序号字段的值指本报文段所发送的数据的第一个字节的序号。

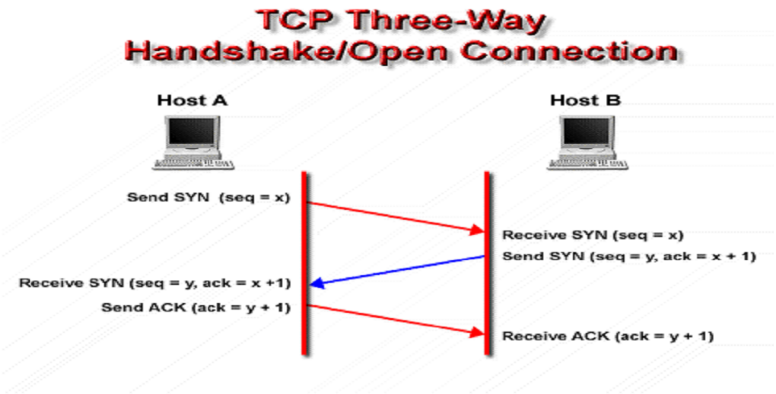
确认号是期望收到对方的下一个报文段的数据的第一个字节的序号。

代码位：URG（紧急），ACK（确认），PSH（推送），RST（复位），SYN（同步，为 1 表示是连接请求或连接接受报文），FIN（终止）

检验和字段检验的范围包括首部和数据这两部分。

注意：源端口在前，目的端口在后。

建立连接（三次握手）：



- ***The First Handshake***
  - Server: executes LISTEN and ACCEPT primitive, and monitors passively
  - Client: executes CONNECT primitive, generate a TCP segment with SYN=1 and ACK=0,which stands for connection request

- ***The Second Handshake***
  - Server checks if exists service process monitoring the port
    - If none process, answer a TCP segment with RST=1
    - If exists process, decides to reject or to accept the request
    - If accept the connection request, send a segment with SYN=1 and ACK=1

- ***The Third Handshake***
  - The client sends a segment with SYN=0 and ACK=1 to acknowledge the connection

ARQ：Automatic Repeat request，自动重复请求

stop-and-wait protocol 每发送一条报文后须等待应答再发送下一条报文。

滑动窗口：流控制机制；要求源设备在向目的设备发送一定数量数据之后接受一个确认。

拆除连接（四次握手）：

第一次：客户端 → 服务器， FIN = 1

第二次：服务器 → 客户端， ACK = 1

第三次：服务器 → 客户端， FIN = 1， ACK = 1

第四次：客户端 → 服务器， ACK = 1

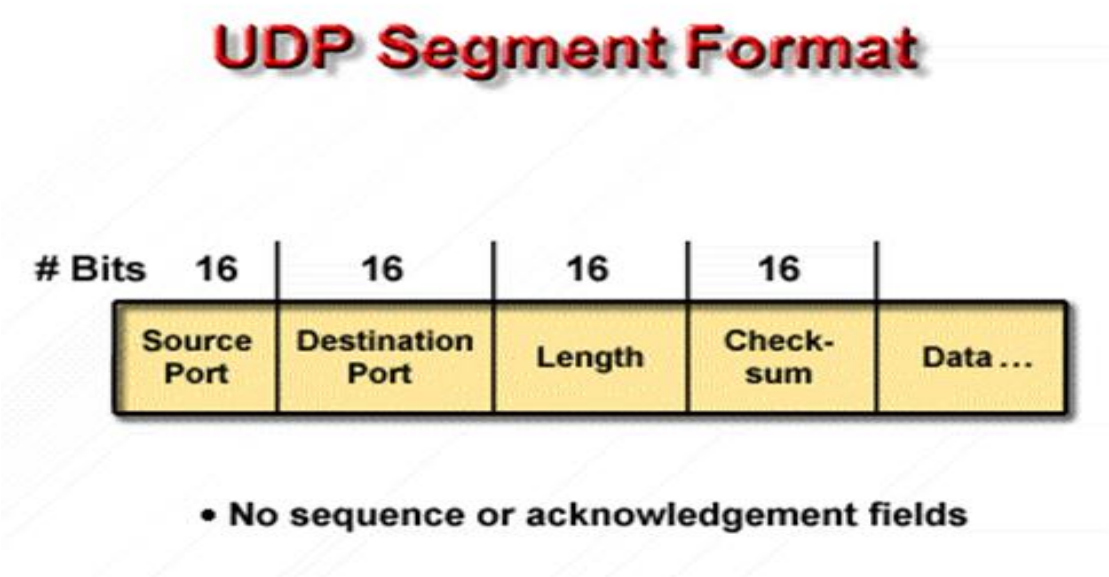
MSL：max segment lifetime，最大生存时间

UDP 用于对丢包可以忍受，但对速率敏感的场合。

用 UDP 传输的协议：

RIP，DNS，SNMP，TFTP，DHCP

UDP 报头格式：



NAT：Network Address Translator，网络地址转换

PAT：Port Address Translator，端口地址转换

NAT：

将内部（本地）网络地址转换为注册的网络地址，即全局网络地址。

Static NAT：

静态转换是指将内部网络的私有 IP 地址转换为公有 IP 地址，IP 地址对是一对一的，是一成不变的，某个私有 IP 地址只转换为某个公有 IP 地址。借助于静态转换，可以实现外部网络对内部网络中某些特定设备(如服务器)的访问。

Dynamic NAT：

动态转换是指将内部网络的私有 IP 地址转换为公用 IP 地址时，IP 地址是不确定的，是随机的，所有被授权访问上 Internet 的私有 IP 地址可随机转换为任何指定的合法 IP 地址。也就是说，只要指定哪些内部地址可以进行转换，以及用哪些合法地址作为外部地址时，就可以进行动态转换。动态转换根据先来先服务原则，可以使用多个合法外部地址集。当 ISP 提供的合法 IP 地址略少于网络内部的计算机数量时，可以采用动态转换的方式。

PAT：

PAT 是指改变外出数据包的源端口并进行端口转换，即端口地址转换(PAT，Port Address Translation)。采用端口多路复用方式。内部网络的所有主机均可共享一个合法外部 IP 地址实现对 Internet 的访问，从而可以最大限度地节约 IP 地址

资源。同时，又可隐藏网络内部的所有主机，有效避免来自 internet 的攻击。

因此，目前网络中应用最多的就是端口多路复用方式。

NAT 的优点：

可以多台机器使用少量地址。

NAT 的缺点：

只能一对一映射，同时可以接入网络的主机少。

第六章　OSI 层次：会话、表示、应用层

表示层：

数据格式化，数据压缩，数据加密

应用层：

FTP：

可靠的面向连接的服务；

使用 TCP。

TFTP：

无连接服务；

使用 UDP。

SMTP：

用于发邮件。

POP（POP3，即 POP version 3）:

用于接收邮件。

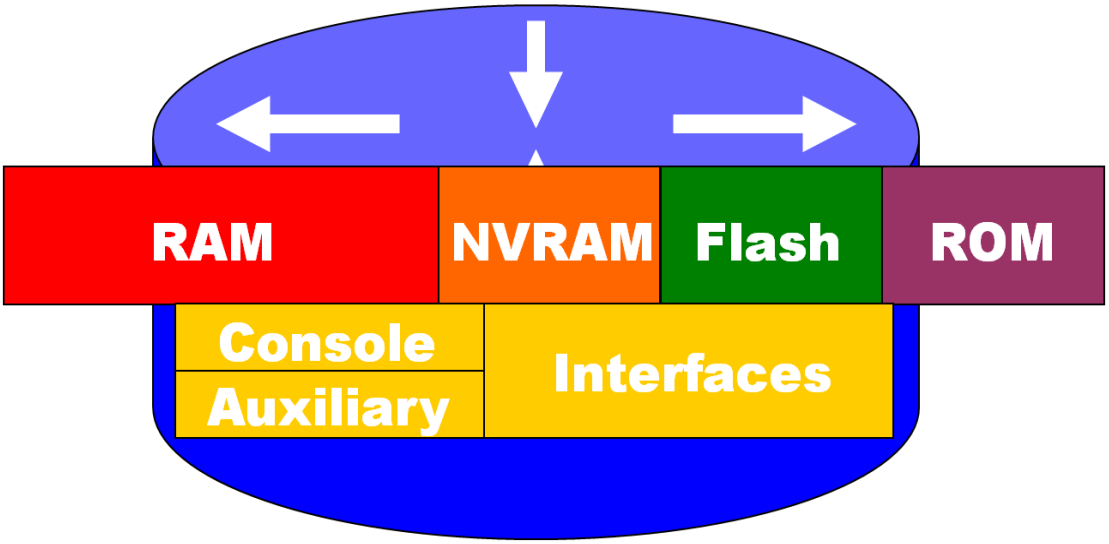
SNMP：Simple Network Management Protocol，简单网络管理协议

TLD：Top Level Domain，顶级域名

DNS 服务器系统采用树结构，每个服务器接收到域名后尝试解析，如果不能解析则传给上一层服务器。

第七章　路由与路由器

路由器的内部组件：



RAM：

临时存储路由表、ARP 缓存、快速交换缓存、包缓冲、包等待队列，关机或重启后信息会丢失。

NVRAM：

非易失 RAM，存储备份或启动配置文件，关机或重启后信息不会丢失。

FLASH：

存储 Cisco IOS，允许不更换芯片升级软件，可以存储多个版本的 IOS，断点后保留信息。

ROM：

带有加电自检，用于加载 ISO 的引导程序和操作系统的备份。

Interface：

包出入的接口。

POST：Power On Self Test，加电自检

启动过程：

1. 加电自检，对所有硬件模块执行 ROM 中的诊断程序；
2. 检验 CPU、内存和网卡端口的所有基本操作；
3. 初始化软件：在 CPU 上执行 ROM 中的引导程序；

4. 初始化软件：查找操作系统；
5. 初始化软件：加载操作系统镜像；
6. 初始化软件：加载 NVRAM 中的配置文件并执行；
7. 初始化软件：如果没有找到配置文件，操作系统进入 setup mode。

静态路由的用途：

1. 出于安全原因希望隐藏一部分网络；
2. 当一个网段只能通过一条路径被访问到，静态路由就足够了，这样的分割叫做终端网络。

administrative distance（管理距离）:

提供路由可靠性的一个可选参数，0-255；

管理值越小越可靠；

静态路由的管理距离通常为 1。

问题：路由环路 → 计数到无穷大

解决方法：

1. 定义最大跳数：当计数大于最大跳数时丢弃报文。
2. 水平分割：由一个接口发送出去的路由信息不能再朝这个接口往回发送。
3. 路由毒化：路由信息在路由表中失效的时候，把该表项的的度量值（metric）设为无穷大 16，而不是马上从路由表中删掉这条路由信息，再将其信息发布出去，这样相邻的路由器就得知这条路由已无效了。

4. 毒性反转：它是指收到路由中毒消息的路由器，不遵守水平分割原则将中毒消息转发给所有的相邻路由器，也包括发送中毒信息的源路由器，也就是通告相邻路由器这条路由信息已失效了。主要是为了达到快速收敛的目的。
5. 抑制定时器：一条路由信息无效之后，一段时间内这条路由都处于抑制状态，即在一定时间内不再接收关于同一目的地址的路由更新。如果，路由器从一个网段上得知一条路径失效，然后，立即在另一个网段上得知这个路由有效。这个有效的信息往往是不正确的，抑制计时避免了这个问题，而且，当一条链路频繁起停时，抑制计时减少了路由的浮动，增加了网络的稳定性。
6. 触发更新：当路由失效时，不再等待下一个更新周期，而是立即出发，发布毒化路由更新。

环路避免方法总结：

1. 在稳定的网络中，路由器发送定期的全部更新，更新中包括除水平分割规则所略的所有路由信息；
2. 当由于路由失效引起网络变化时，路由器用毒化路由发送触发的部分更新。并且，路由器对这条路由忽略水平分割规则，向原通告这条毒化路由的路由器通告毒性反转路由；
3. 当学到某条失效路由时，所有路由器会将此路由置于抑制状态，并启动抑制计时器，在抑制期内，忽略这条路由的新信息，除非这条信息来自于原来通告这条路由的路由器。

LSA：link-state advertisement，链路状态通告

LADB：link-state database，链路状态数据库

SPF：shortest path first，最短路径优先

两个需要考虑的问题：

1. 处理器和内存的需求：链路状态协议比距离矢量协议对处理器和内存的要求都更高；
2. 带宽的需求：初始化链路状态包洪泛的时候会临时使可用带宽减小。

距离矢量协议与链路状态协议的比较：

距离矢量协议	链路状态协议
从邻居处获得对网络拓扑的认识	获取对整个网络拓扑的认识
路由与路由间计算距离矢量	路由与路由间计算最短路径
频繁的路由更新，低收敛速度	事件驱动更新，快收敛速度
向邻居路由传递路由表的备份	传递的是链路状态更新

混合协议：

IS-IS：Intermediate System-to-Intermediate System

EIGRP：Enhanced Interior Gateway Routing Protocol

默认路由：

当目的地址不在路由表中时，将报文发给默认路由。使路由表更短。

RIP：

内部网关协议；

距离矢量协议；

每 30 秒更新一次；

以跳数作为度量；

最大跳数为 15；

适合小型网络。

RIP V1：

有类路由协议；

最多 6 路负载均衡，默认为 4 路；

不发送子网掩码；

更新信息作为广播被发送；

不支持身份验证；

不支持可变长子网掩码和无类域间路由。

RIP V2：

使用抑制定时器和水平分割防止路由环路；

支持可变长子网掩码（无类路由）；

支持验证；

以 224.0.0.9 作为路由更新的目的地址。

OSPF：

Neighborship Database(毗邻数据库)→Topology Database(拓扑数据库)→SPF→路由表；

链路状态协议；

使用代价、速度、通信量、可靠性、安全性等作为度量；

适合于大型的网络；

以后可以将网络划分为多个区域；

支持变长子网掩码；

快速收敛。

DR：Designated Router，指定路由器

BDR：Backup Designated Router，备份指定路由器

DR：

在 OSPF 多路访问网络中，在同一个区域内被选举出来代表所有路由的路由。为了减少在同一个网段中几个邻居互相交换信息的数量。

BDR：

备用 DR，当 DR 停机时发挥作用。

在单区域中，Area 号为 0。

在多区域中，所有的其他区域都要求接到 Area0，所以 Area0 称为中枢链路。

OSPF 收敛五个步骤：

1. 建立邻接关系：路由器周期性地发送 hello 报文，周围的路由器收到后将其加入自己的邻接数据库，然后根据网络类型和是否已有 DR/BDR 决定是否跳过第二步；
2. 选举 DR 和 BDR：如果只有一个路由器，则为 DR，下一个进入的路由器为 BDR，否则根据优先级和 router ID 判断；
3. 发现路由：DR/BDR 发送 LSA，其他路由器发送 DBD 和 LSR；
4. 选择合适的路由路径：使用最短路径优先算法，最多加载 4 条链路消耗相同的路由；
5. 维护路由信息：hello 报文用于发现新的邻居和停机的邻居。

OSPF 的 7 个状态：

停止，初始（Init），双向（Two-Way），准启动（EX-Start），交换（Exchange），加载（Loading），全毗邻（Full）。

OSPF 网络类型：

广播多路接入（以太网），点对点，非广播多路接入

NBMA：Nonbroadcast Multi-access，非广播多路接入

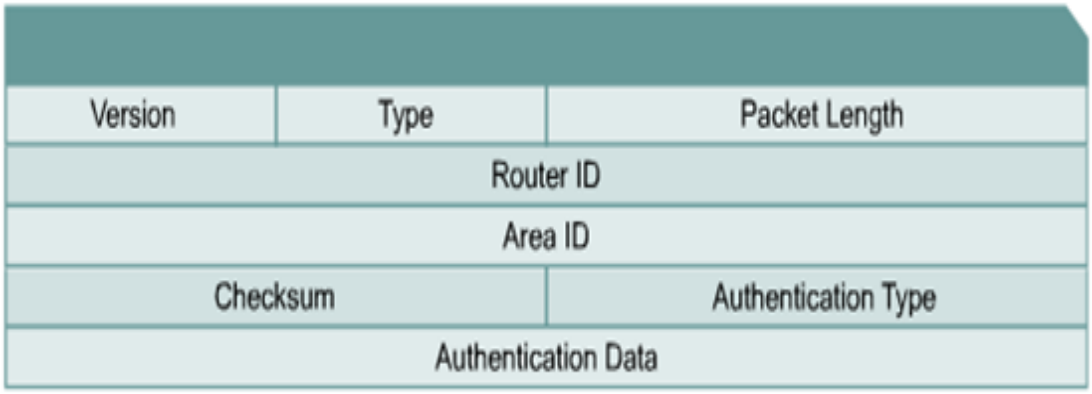
链路拓扑改变时，路由器通过 224.0.0.6 通知 DR 或 BDR。

DR 或 BDR 通过 224.0.0.5 通知该区域内的路由。

五种 OSPF 路由协议包：

1. Hello；
2. DBD，数据库描述；
3. LSR，链路状态请求；
4. LSU，链路状态更新；
5. LSAck，链路状态应答。

OSPF 报文头格式：



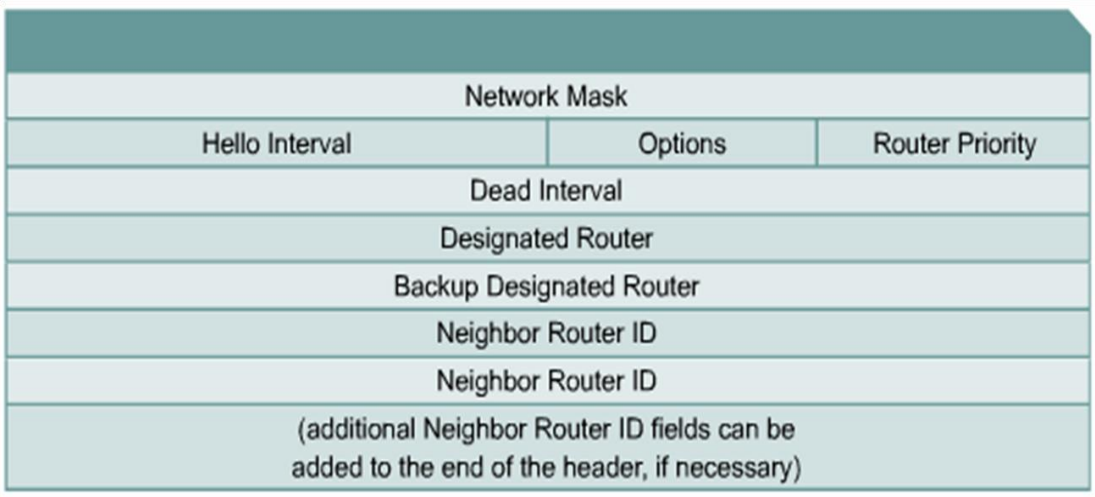
Hello 协议：

地址为 224.0.0.5；

在广播多路接入和点对点网络中，默认每 10 秒发送一次 hello 报文；

在 NBMA 网络中，每 30 秒一次。

Hello 报文头格式：



选举 DR 和 BDR：

优先级+Router ID；

默认优先级为 1，范围可以是 0-255，数字越大，优先级越高；

Router ID 是环回地址；若无环回地址则为最大的接口地址。

第九章　局域网交换与 VLAN

对称交换：

提供同带宽端口之间的交换连接。

非对称交换：

提供不同端口之间的交换连接，通过把传到服务器的数据段转到更大带宽接口来减小产生瓶颈的可能，需要内存缓冲。

内存缓冲区的两种类型：

1. 基于端口的内存缓冲区；

2. 共享的内存缓冲区。

交换方法：

1. store-and-forward（存储转发）：通过对网络帧的读取进行验错和控制；
2. cut-through 转发：

    1) Fast forward switching：快速交换前只检查目的 MAC 地址；

    2）Fragment Free：读取前 64 字节以减少错误。

每次交换机存一个 MAC 地址，都会有一个时间戳（Time-Stamped）

每次帧的到达，时间戳都会更新。

如果时间戳到期，将会从交换表中删除。

交换的好处：

有效，允许建立虚电路，更加灵活的管理网络，减少冲突域，能与 802.3 兼容。

STP：Spanning Tree Protocol，生成树协议

BPDU：bridge protocol data unit，桥接协议数据单元

生成树协议：

减少冗余路径而不导致网络延时；

通过计算稳定的生成树网络拓扑来防止网络环路。

发送 BPDU 来决定生成树拓扑。

BPDU：

STP 建立一个叫做根桥的根节点，生成树从根桥开始。非最短路径的冗余链路将被阻塞，从阻塞链路发来的数据帧将被丢弃。STP 需要网络设备互相交换消息来检测桥接环境，BPDU 是交换机发送的用于构建无环路拓扑的消息。

STP 决定顺序的步骤：

1. 最低的根网桥（BID)；
2. 到跟网桥最低的路径成本；
3. 最低的发送网桥 ID；
4. 最低的端口 ID。

BID：Bridge Identification

每个网桥都分配一个唯一的 BID，由 2 字节优先级+6 字节 MAC 地址所构成，默认优先级为 32768。

STP 五种状态：

阻塞（Blocking）：不转发帧，监听 BPDU

监听（Listening）：不转发帧，监听数据帧

学习（Learning）：不转发帧，学习地址

转发（Forwarding）：转发帧，学习地址

禁止（Disable）：不转发帧，不监听 BPDU

STP 的收敛步骤：

1. 选举根桥：根桥的所有端口都是指定端口，指定端口都处于转发状态，BID 最小的交换机被选为根；
2. 在非根桥上选举根端口：选择从非根桥到根桥的最低花费的那条路径；
3. 在每个网段中选择指定端口：指定端口是在拥有到根桥最低花费路径的网桥上选举的，所有非指定端口将被阻塞。

VLAN（虚拟局域网）

逻辑的网络设备或用户分组；

产生单一的广播域；

通过交换机实现。

两个 VLAN 中的机器通过路由器通信。

VLAN 的实现方法：

帧过滤和帧标记

帧过滤：

使用交换表。

帧标记：

在干线上传的时候加上标记位，当从干线上卸下来时，去掉标记位。

VLAN 的实现方法有静态和动态两种。

Access Links（接入链路）:

只在一个 VLAN 中的链路，任何接入的设备并不知情有 VLAN 的存在。

Trunk Links（中继链路）:

点对点，支持多个 VLAN，支持在快速以太网和 G 比特以太网，节省端口，可能有一个本地 VLAN。

第十章　广域网

CPE：Customer Premises Equipment，客户端设备

CO：Central Office，中心局

注意：1Kbit/s=1000bit/s 不是 1024

DCE：data circuit-terminating equipment，数据设备

DTE：data terminal equipment，数据终端设备

SVC：Switched Virtual Circuits，交换虚拟电路

PVC：Permanent Virtual Circuits，永久虚拟电路

CSU：channel service unit，信道服务单元

DSU：data service unit，数据服务单元

CSU/DSU：channel service unit/digital service unit，即 Modem，调制解调器

WAN 主要涉及物理层和数据链路层。

路由器的作用：

连接网络，WAN 的串行口。

路由可以作为内部路由，骨干路由，区域边界路由，自治系统边界路由。

数据链路层：

描述了数据怎样在单一的链路上在系统之间传送。

ISDN：Integrated Services Digital Networks，综合业务数字网

LAPB：Link Access Procedure, Balanced

HDLC：High-Level Data Link Control，高层数据链路控制

PAP：Password Authentication Protocol，密码验证协议

NCP：Network layer protocol，网络层控制协议

CHAP：Challenge Handshake Authentication Protocol，询问握手验证协议

综合业务数字网：

在已有的电话线上传输语音或数字信号

最常见的广域网点对点封装是 PPP 和 HDLC。

PPP：

能在连接建立时检查链路质量；

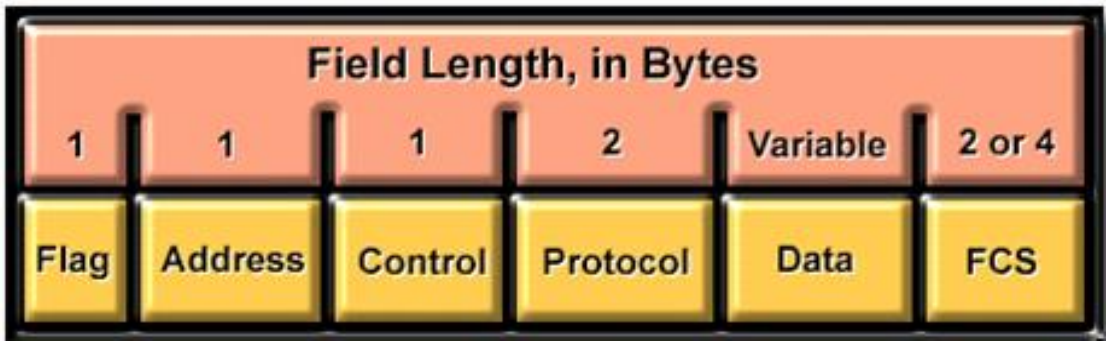
支持网络层的多链路技术；

支持 IP 地址动态分配；

提供 PAP 和 CHAP；

支持压缩和错误检测。

PPP 帧格式：



PPP 会话的建立与终止：

1. 链路的建立和配置协商（LCP）；
2. 链路的质量检测；
3. 网络协议的配置协商（NCP）；
4. 链路终止。

双向握手 PAP：

远程节点不停的在链路上反复发送用户名/密码，直到验证通过或者连接终止。

不健壮的身份认证协议，使用明文发送密码。连接建立前只有一次认证。

CHAP：

1. 链路建立阶段结束之后，认证者向对端点发送“challenge”消息；
2. 对端点用经过单向哈希函数计算出来的值做应答；
3. 认证者根据它自己计算的哈希值来检查应答，如果值匹配，认证得到承认，否则连接应该终止；
4. 经过一定的随机间隔，认证者发送一个新 challenge 给端点，重复步骤 1-3。

BRI：Basic Rate Interface，基本速率接口

PRI：Primary Rate Interface，主速率接口

ISDN 提供两种 B 信道和一种 D 信道。B 信道用于数据和语音信息，D 信道用于信号和控制（也能用于数据），告诉电话网络如何处理 B 信道。

SPID：Service Profile Identifier

SPID 是一些服务供应商用来定义 ISDN 设备用户所订购服务的号码。

计算机网络面临的四种威胁：

1. 截获——从网络上窃听他人的通信内容；
2. 中断——有意中断他人在网络上的通信；
3. 篡改——故意篡改网络上传送的报文；
4. 伪造——伪造信息在网络上传送。

被动攻击：

截获信息的攻击。

主动攻击：

更改信息和拒绝用户使用资源的攻击。

恶意程序主要包括：

1. 计算机病毒：会“传染”其他程序的程序，“传染”通过修改其他程序来把自身或其变种复制进去而完成；
2. 计算机蠕虫：通过网络的通信功能将自身从一个结点发送到另一个结点并启动运行的程序；
3. 特洛伊木马：一种程序，它执行的功能超出所声称的功能；
4. 逻辑炸弹：一种当运行环境满足某种特定条件时执行其他特殊功能的程序。

对称密钥体制：

加密密钥与解密密钥是相同的密码体制。数据加密标准 DES 属于常规密钥密码体制，是一种分组密码。DES 的保密性仅取决于对密钥的保密，而算法是公开的。

公钥密码体制：

使用不同的加密密钥与解密密钥，是一种“由已知加密密钥推导出解密密钥在计算上是不可行的”密码体制。在公钥密码体制中，加密密钥(即公钥)PK 是公开

信息，而解密密钥(即私钥或秘钥)SK 是需要保密的。加密算法 E 和解密算法 D 也都是公开的。虽然 SK 是由 PK 决定的，但却不能根据 PK 计算出 SK。公钥算法中加密和解密的运算可以对调。

任何加密方法的安全性取决于密钥的长度，以及攻破密文所需的计算量。

防火墙是由软件、硬件构成的系统，是一种特殊编程的路由器，用来在两个网络之间实施接入控制策略。防火墙内的网络称为“可信赖的网络”(trusted network)，而将外部的因特网称为“不可信赖的网络”(untrusted network)。

防火墙的功能有两个：阻止和允许。

“阻止”就是阻止某种类型的通信量通过防火墙（从外部网络到内部网络，或反过来）。“允许”的功能与“阻止”恰好相反。

VPN：Virtual Private Network，虚拟专用网络

防火墙技术的分类：

1. 网络级防火墙：用来防止整个网络出现外来非法的入侵；
2. 应用级防火墙：从应用程序来进行接入控制。

ACL：Access Control List，访问控制列表

Wildcard Mask（通配符掩码）表示地址中的某位需要匹配还是忽略。0 表示匹配，1 表示忽略。

ACL 的放置：

1. 标准 ACL 应该尽可能放在离目的端近的位置；
2. 扩展 ACL 应该尽可能放在离源端近的位置。