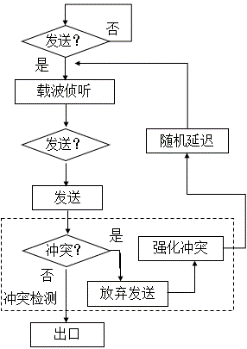
**网络分类（按地域范围划分）**：局域网 ( Local Area Networks )，城域网 ( Metropolitan Area Networks )，广域网 (Wide Area Networks )，互联网 (Internet, 因特网 )； **局域网常见结构：**总线型，星型，环形； 第N层协议来说，它有如下特性：不知道上、下层的内部结构；独立完成某种功能；为上层提供服务；使用下层提供的服务； OSI七层模型：物理层：在物理线路上传输原始的二进制数据位（**比特流，**BITs）数据链路层：在有差错的物理线路上提供无差错的数据传输（**帧，**DH+DATA+DT）；网络层：控制通信子网提供源点到目的点的数据传送（**分组,**NH+DATA）；运输层：为用户提供端到端的数据传送服务（**TPDU,** TH+DATA）；会话层：为用户提供会话控制服务（安全认证， **SPDU,** SH+DATA）；表示层：为用户提供数据转换和表示服务（**PPDU,** PH+DATA）；应用层：提供多种应用协议以满足用户的不同需求（**APDU,** AH+DATA）； TCP/IP模型：TCP/IP 参考模型把OSI模型的第一层和第二层合起来称为：网络接口层，Internet层（互连网层），运输层，应用层。OSI与TCP/IP的区别：**层次数量上的差异；OSI的网络层提供面向连接和无连接两种服务，TCP/IP的网络层只提供无连接服务，服务层提供两种服务；TCP/IP的ip协议采用尽力传递的方式，只在传输层保证传输可靠性做了保障工作，OSI几乎在每一层都要保证可靠传输。**

数据传输方式：信号类型：模拟信号，数字信号；信号发送方式：模拟信号传输（采用模拟信道），数字信号传输（采用数字信道）； 数字传输编码方式：不归零制码：低电平表示“0”，高电平表示“1”。曼彻斯特码：从低跳到高表示“0”，从高跳到低表示“1”。差分曼彻斯特码：每一位中间都有一个跳变，每位开始时有跳变表示“0”，无跳变表示“1”。位中间跳变表示时钟，位前跳变表示数据。逢“1”变化的NRZ码：在每位开始时，逢“1”电平跳变，逢“0”电平不跳变。逢“0”变化的NRZ码：在每位开始时，逢“0”电平跳变，逢“1”电平不跳变。 多路复用技术：时分复用 TDM、频分复用 FDM、波分复用 WDM 交换方式分类：电路交换（建立电路、传输数据、拆除电路）、报文交换（以报文为单位进行存储转发）、**分组交换（以分组为单位进行存储转发。源节点把报文分为分组，在中间节点存储转发，目的节点把分组合成报文）: 数据报:每个分组均带有全称网络地址（源、目的），可走不同的路径。如：IP网络;虚电路:电路交换和分组交换的结合，如：ATM网络**。混合交换。传输介质：磁介质（软盘，硬盘）、双绞线（可模拟和数字信号传输）RS232常用引脚：DB25/DB9/RJ45 双绞线（10 BASE-T）/粗缆（10 BASE-5）/细缆（10 BASE-2）/光纤（10 BASE-F）

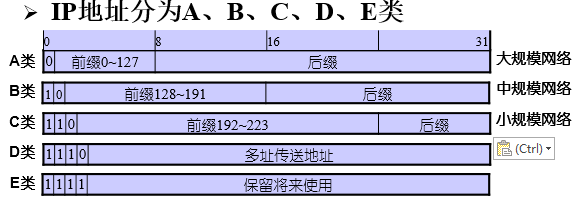
数据链路层作用：链路管理、流量控制、差错控制、帧同步（成帧）、透明传输、寻址 成帧方法：字符计数法、带字符填充的首尾字符定界法、带位填充的首尾标记定界法、物理层编码违例法 差错控制：出错情况：帧出错、帧丢失 处理差错方法：纠错码（海明校验）、检错码（奇偶校验、循环冗余校验） 流量控制策略：XON/XOFF方案、**滑动窗口：停等协议（发送、接收窗口大小均为1）、后退n帧的滑动窗口协议（发送窗口：2n-1，接收窗口：1）、选择性重发滑动窗口协议（发送、接收窗口大小均为2n-1）**

IEEE 802标准包括**CSMA/CD**（**802.3**）、令牌总线和令牌环等 传统局域网技术：纯ALOHA协议、时隙ALOHA协议、载波侦听多路访问协议CSMA（1 – 持续CSMA、非持续CSMA、持续CSMA）、**CSMA/CD（带冲突检测的载波侦听多路访问）：**二进制指数后退算法（i次冲突后，等待的时隙数将从0 ~ 2i –1中随机选择） 冲突的检测方法：信号电平法、过零点检测法、自收发检测法 **最短帧长（64字节）：10M以太网中两个收发器间（允许接4个中继器）的最大距离为2500m，往返5000m，同轴电缆的时延特性为4.33us/km，最坏情况下端到端的往返延迟为45us，再加上强化冲突需发送48bit，接受方要接受到48bit后才确认冲突，即在增加4.8us，共49.8us，所以通常以太网取51.2us为争用期的时间长度(传输512bit，即64字节时间)，即帧的长度至少为64字节。**LLC（逻辑连接控制子层，用统一的结构为网络层服务）提供的三种服务：不可靠的数据报服务、可靠的数据报服务、面向连接的服务 中继器/集线器：提供信号放大，延伸物理网段作用不具备差错识别能力，延迟小，会扩大冲突域；（能够连接不同的网段或介质类型（如细缆与双绞线），便于扩展网络的深

度和广度（如5/4/3原则）；不能连接不同存取类型的介质（如令牌网和以太网），不能分辨帧格式与内容无法隔断，不同网段的数据流，仅适合小型网络）； 网桥是连接多个局域网的工作在数据链路层的设备，可解析所收发的数据帧，知道如何把数据传送到目的地，可分割冲突网段； 以太网/IEEE 802.3：采用同轴电缆作为网络介质，传输速率达到10Mb/s；100Mb/s以太网：又称为快速以太网，采用双绞线作为网络介质，传输速率达到100Mb/s；1000Mb/s以太网：又称为千兆以太网，采用光缆或双绞线作为网络介质，传输速率达到1000Mb/s。 传统以太网的5-4-3原则：源与目的节点间最多不得超过5个网段；源与目的节点间最多不得超过4个中继器；源与目的节点间含有终端的网段最多不得超过3个。 交换机的主要功能：分割LAN的流量来提高性能，能够建立混合速率的LAN（如10M/100M），扩展LAN的范围。 交换机主要功能为通过自我学习，转发数据帧。**自我学习：当一个数据帧到达交换机的时候，交换机取出该帧携带的MAC地址与自己的所记录的地址转发表对比，若发现目的地址对应的端口与原地址对应的端口一致，说明该帧是源端口所连接网段内的数据通信，丢弃该帧；若发现目的地址对应的端口与原地址对应的端口不一致，则将数据发到对应的目的端口，进行数据转发。交换机会根据各端口流经的数据帧自我学习不同的转发方向，即记录下各端口对应的MAC地址。**转发表有静态和动态两种类型表项。数据转发策略：切入法（直接检查数据包包头，不存储，延迟小，交换速度快）和存储转发法（处理数据时延迟大，但可对进入交换机的数据帧进行错误检测，并且能支持不同速度的输入/输出端口间的交换，有效的改善网络性能）。 Vlan的功能：控制广播域范围；vlan间的相互隔离，提高网络安全；第三层地址管理；网络资源的集中管理；增加网络连接的灵活性。 Vlan的划分方法：基于端口、基于端口和ip/MAC地址、基于协议、基于ip组播

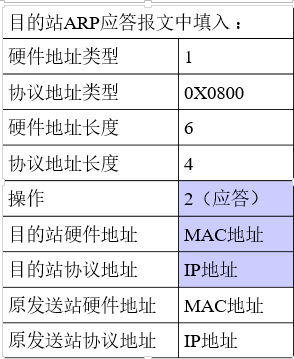
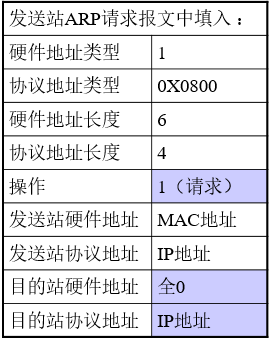
网络层主要解决的问题：路由选择、网络互联、拥塞控制、向上层提供服务 数据包的分段：按MTU的及数据包的实际负载长度计算所需段数，并划分，（各段在不大于MTU的前提下，尽可能的大；段的长度为8的整倍数）；原数据包的报头作为每段的数据包报头，并修改其中的某些字段，指明：属原来的哪个段；属原来段中的第几个分段；哪一个是段尾

数据包的重组：重组是在各分段都到达目的地后才进行（每个分段可以走不同的路径；减少路由器中保存的信息量及路由器的工作量）；途中的任意一个路由器都无法重组（重组必须在所有的分段全部收到后，才可进行）；互联网层是遵循尽力而为来传送IP包的，也存在力不从心的时候，此时只能丢弃（重组主机将遵循：要么重组成功，要么全部丢弃的原则）

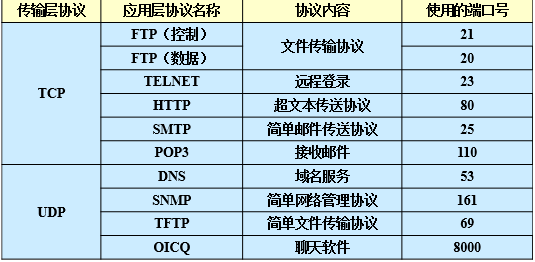
子网掩码的作用：因为子网地址是数不是固定的，所以告知设备地址的哪一部分是包含子网的网络地址段，地址哪一部分是主机地址段； 子网划分：网络地址+子网地址+主机地址（至少要借2位，至多能借6位）

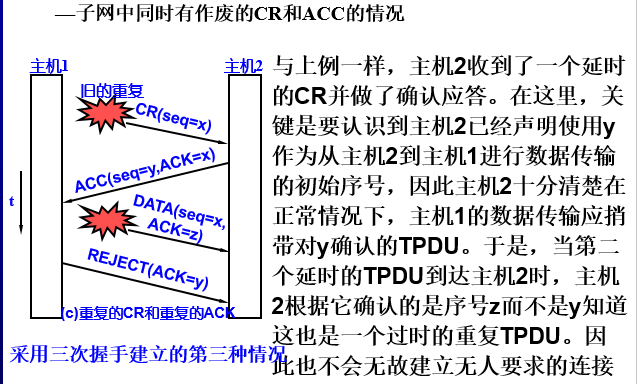
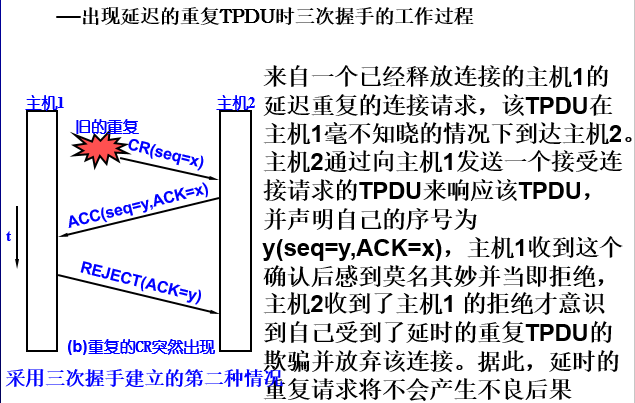
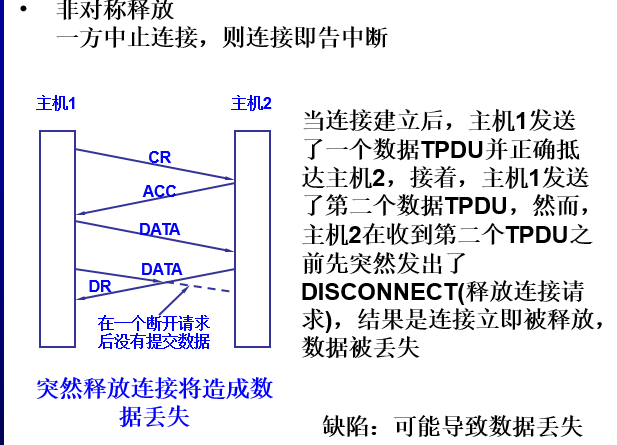
IP控制协议：**ICMP**（提供了一种把通信服务中的差错向源站点报告的机制）**、ARP（协议地址和物理地址之间的转换，如IP地址和MAC地址之间的转换 ）** 、RARP 、BOOTP **ICMP协议的运用：测试报文的可达性：ping命令：使用ping命令（即调用ping过程）时，将向目的站点发送一个ICMP回应请求报文（包括一些任选的数据），如目的站点接收到该报文，必须向源站点发回一个ICMP回应应答报文，源站点收到应答报文（且其中的任选数据与所发送的相同），则认为目的站点是可达的，否则为不可达 ；路由跟踪命令tracert： tracert过程是通过ICMP数据报超时报文来得到一张途经路由器列表的 ，源主机向目的主机发一个IP报文，并置hop为1，到达第一个路由器时，hop减1，为0，则该路由器回发一个ICMP数据报超时报文，源主机取出路由器的IP地址即为途经的第一个路由端口地址 ，接着源主机再向目的主机发第二个IP报文，并置hop为2，然后再发第三个、第四个IP数据报，… …直至到达目的主机 ；得到路径中最小的MTU：源主机发送一系列的探测IP数据报，并置DF = 1，即不允许分段，如途径某个网络的MTU较小，则路由器将丢弃该数据报并发回一个ICMP数据报参数错，要求分段，源主机则逐步减小数据报长度，并仍置DF = 1，直至某个探测报文成功到达目的主机，即得到路径中的最小MTU**

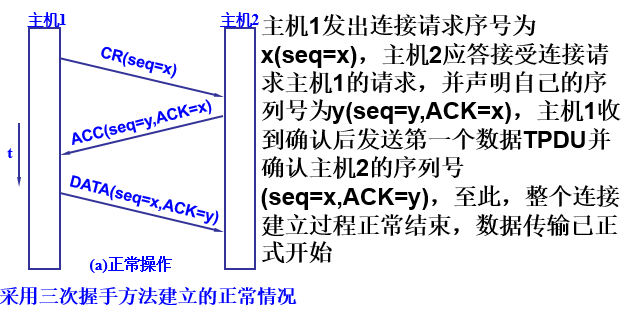
**ARP协议的工作原理： 一个ARP请求消息是一个数据帧，其中包含发送站的硬件地址和协议地址，以及目的地址的IP地址，并把此数据帧在本物理网络内广播 ；一个ARP应答消息是一个数据帧，其中包含应答站的硬件地址和协议地址，以及原发送地址的IP地址，并把此数据帧发送给原发送站 （ARP消息帧的类型值为0X806）**  暂存ARP应答和处理接收的ARP消息：暂存ARP应答于Cache或内存中，以后即可查表，不必再发询问报文，以减少网络的通信量从消息中取出发送方的协议地址和硬件地址，更新cache中已有的信息；检查消息是请求还是应答，若是应答，则接收；若是请求，检查是否为发送给本站的，如是，则发应答消息 引导协议（BOOTP）是一种基于UDP/IP的协议。这种协议允许正在启动的主机动态配置而无需用户监督。BOOTP主要用于客户机从服务器获得自己的IP地址、服务器的IP地址以及启动映像文件名。其他的一些配置信息，如本地子网掩码、本地时间偏移量、默认路由器地址和各种Internet服务器地址，都能通过BOOTP协议与客户机交流。 动态主机配置协议DHCP：从一个地址池中把IP地址分配给请求主机。该协议既允许手工分配IP地址，也允许自动分配IP地址，DHCP也能提供其他信息，如网关IP、DNS服务器、缺省域和网络范围内HOSTS文件的位置。 Internet组管理协议IGMP：IGMP用来帮助组播路由器识别加入到一个组播群组的成员主机，用于IP主机向任一个直接相邻的路由器报告他们的组成员情况。

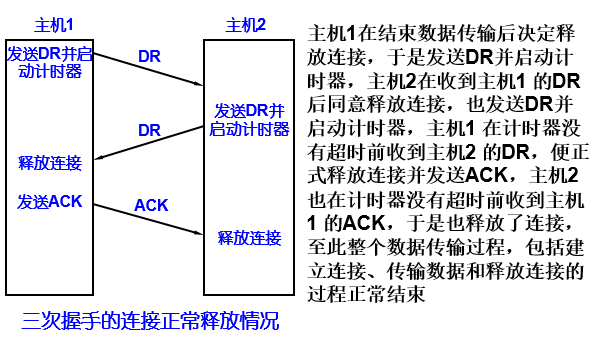


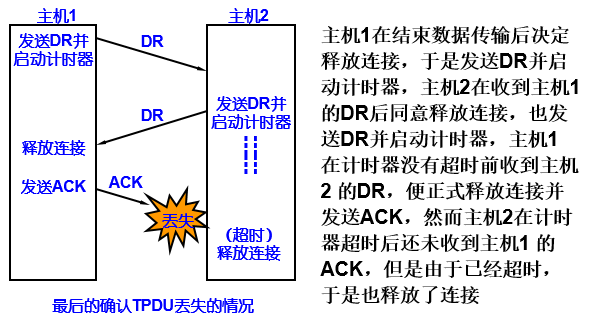
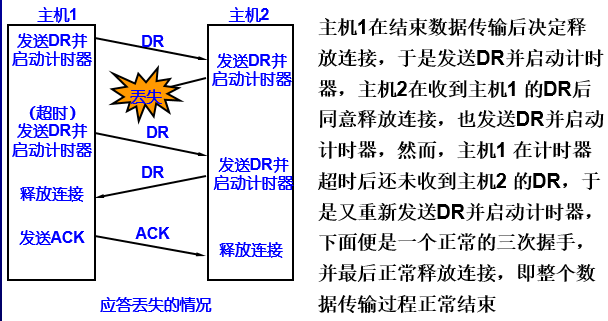
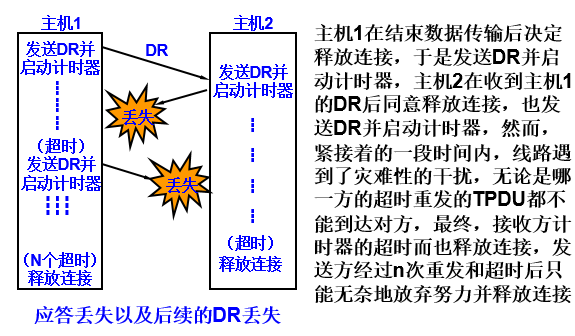
路由器是网络层的一个智能设备，承担了路由选择的任务，选择路由的依据是一张路由表，路由表指明了要到达某个地址该走哪一条路径；在路由表中，并非为每一个具体的目标IP地址指明路径，而是为目标IP地址所在的网络指明路径，这样路由表的大小才落在可操作的范围内，因此查找路由表的依据是目标主机的网络地址；路由器对每一个接收到的分组，取出它的目标IP地址，然后根据目标IP地址中的网络地址查找路由表，确定下一步的传输路径，并从相应的路由器端口将分组送出。传送路径是由所经过的路由器一步一步确定的。 路由算法分类：静态路由算法（泛射路由选择法、固定路由算法、随机路由选择法）和动态路由算法（独立式，集中式和分布式路由选择） 相关的路由算法：最短路径算法、扩散法、基于流量的路由选择、距离矢量算法、链路状态算法、广播路由、多址传输路由选择静态路由(人工在路由器上配置路由表, 缺省路由是静态路由的特例，也需要人工配置；)优点：路由器不必为路由表项的生成花费大量时间，有时可以抑制路由表的增长；缺点：人工配置开销大，网络拓扑结构变更时需重新配置路由表，一般只在小型网络或部分链路上使用。 动态路由(由动态路由协议自动生成)优点： 网络拓扑发生变化时，动态路由协议自动更新路由表；缺点：路由器路由计算开销大； RIP采用D-V路由算法，是Internet的一个主要路由协议，传输层采用UDP协议,一般为hop数，<=15 网络地址转换（NAT）允许一个机构内的局域网以一个合法地址出现在互联网上。NAT将每个局域网节点上的地址转换成一个合法的IP地址。NAT也可以应用到防火墙技术中，将个别IP地址隐藏起来，使外界无法直接访问内部网络设备。同时，NAT还可以帮助网络超越地址的限制，合理地安排网络中私有IP地址的使用。 原理：NAT的具体的做法是将IP包内的地址域用合法的IP地址替换。NAT设备维护一个状态表，用来把非法的IP地址映射到合法的IP地址上去。每个IP包在NAT设备中都会被更换相关的IP地址 分类：静态NAT、动态地址NAT、网络地址端口转换NAPT 优点：为内部主机提供了“隐私”保护，实现了内部网络的主机通过该功能访问外部网络资源可能。缺点：需要对数据报文进行IP地址转换，所以所涉及的IP地址的数据报的报头不能被加密。网络调试变得更加困难。在链路的带宽低于10Mb/s速率时，地址转换对网络性能基本不构成影响；但当速率高于10Mb/s时，地址转换将对路由器性能产生一定影响。 第三层交换机与传统路由器比较：子网间传输带宽可任意分配。因为端口数可任意指定，所以子网间传输带宽不受限制；合理配置信息资源。因为访问子网内资源速率和访问全局网中资源速率没有区别，所以子网不需要设置单独服务器；降低成本。采用三层交换机进行网络设计，既可以进行任意虚拟子网划分，又可以通过交换机三层路由功能完成子网间通信；交换机间连接灵活。三层交换机可以利用生成树算法阻塞造成回路的端口，而进行路由选择时，仍然可以把阻塞掉的通路作为可选路径参与路由选择。第三层交换技术的应用：网络的骨干交换机和服务器群交换机，也可作为网络节点交换机；支持链路聚合技；实现组播 ACL是应用到交换机端口的指令列表，这些指令列表告诉交换机哪些数据包可以接收，哪些数据包需要拒绝。接收或拒绝的条件可以根据源地址、目的地址和端口号等条件来决定。 ACL的主要功能：限制网络流量、提高网络性能。如ACL可以根据数据包的协议，指定这种类型的数据包的优先级，同等情况下可优先被交换机处理；提供网络访问的基本安全手段。如ACL允许某一主机访问某种资源，而禁止另一主机访问同样的资源；在交换机端口决定哪种类型的通信流量被转发，哪种类型的流量被阻塞。如可允许网络的E-mail通过而阻止FTP通信。

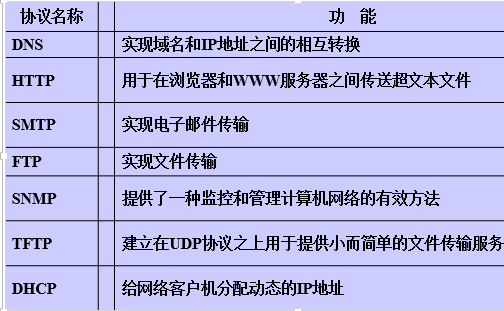
传输层要解决的问题：编址，连接标志的获取，连接的建立，连接的释放，流量控制，多路复用 传输控制协议TCP：常用于一次传输要交换大量报文的情形，如文件传输、远程登录等。它提供面向连接的流传输。 **套接字=（IP地址，端口号）** **TCP连接的建立与释放（三次握手）：建立连接（正常的三次握手过程，非正常的连接建立过程）和释放连接（非对称释放，对称释放）**

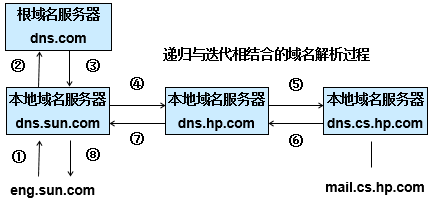
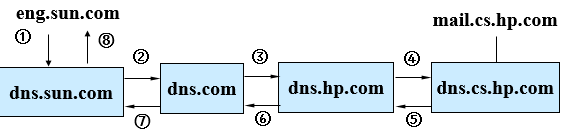








**UDP提供的是不可靠的、无连接的数据传输服务** UDP与TCP相比较：两者在如何实现信息的可靠传递方面有所不同；TCP包含了可靠性保证机制，而UDP不提供数据传送的保证机制；TCP在实际执行的过程中会占用大量的系统开销，严重地影响到传输速度。而UDP不考虑可靠性，将安全和排序等功能移交给上层应用来完成，极大地减少了时间，使速度得到了保证。

DNS包括域名、主机和域名服务器三大要素，采用层次型命名机制的命名方法（…三级域名.二级域名.顶级域名） 域名解析的查询过程可分为两部分：一是客户端本身及客户端对服务器的查询；二是服务器与服务器之间的查询。

Web服务：统一资源定位符URL格式：scheme：//host：port /path

1. ② 　　　　 ③

①服务方式或协议，除了WWW 用的HTTP 协议之外，还可以是FTP、TELNET 等②存有该资源的主机地址，有时也包括端口地址。③路径，指出服务器上某资源的具体地址

WWW服务的实现过程：客户端的工作过程：假如有用户要访问http://www.ietf.org/rfc.html，则浏览器的工作过程如下：

(1) 浏览器确定URL；(2) 浏览器向DNS询问web服务器www.ietf.org的IP 地址；(3) DNS的应答是209.173.57.180；(4) 浏览器和IP 地址为209.173.57.180的80 端口建立一条TCP 连接；(5) 浏览器执行HTTP 协议，发送GET /rfc.html 命令，请求读取该文件；(6) www.ietf.org 服务器返回/rfc.html文件到客户端；(7) 释放TCP 连接；(8) 浏览器显示/rfc.html页面。

服务器端的工作过程：(1) 接受来自客户(浏览器)的TCP连接；(2) 获取所需文件的名字；(3) 获取文件(从磁盘上)；(4) 将文件返回给客户；(5) 释放该TCP连接。

E-mail 地址的标准格式为：<收信人信箱名>@主机域名 电子邮件系统有三个主要组成构件：用户代理、邮件服务器与协议。 用户X使用“XX@sohu.com”作为发信人地址向用户YY@163.net发送一个文本格式的电子邮件过程：(1)用户XX调用用户代理编辑要发送的邮件，包括首部与内容。(2)用户代理将用户的邮件传给发送端邮件服务器;(3)发送邮件服务器smtp.sohu.com把邮件放入邮件缓存队列中，等待发送。(4)运行在发送邮件服务器smtp.sohu.com的SMTP客户进程根据邮件接收者的地址，在发送服务器与YY的接收邮件服务器之间建立SMTP连接，并通过该连接将邮件送至YY的接收服务器;(5)接收方邮件服务器smtp.163.net 接收到邮件后，根据邮件接收者的用户名将邮件放到用户的邮箱中;(6)当邮件到达邮件接收服务器后，用户随时都可以接收邮件并处理。

FTP的工作过程如下：(1)在FTP的服务器上，只要启动了FTP服务，主服务器进程就打开熟知端口(端口号为21)，使客户进程能够连接上，等待客户机的连接请求。(2)当主服务器进程监听到客户端发出的建立连接的请求时，就启动从属进程处理客户进程发来的请求，自己则回到等待状态，继续接受其它客户进程的请求。(3)从属进程有两类，其中控制进程进行用户名密码及权限的验证，验证通过后，相当于在客户机与FTP服务器之间打开了一个命令传输的控制连接，该连接在整个FTP会话期间一直存在，所有与文件管理有关的命令将通过该连接被发送至服务器端执行。并且创建“数据传输进程”与“数据连接”，用于连接客户端和服务器端的数据传输进程，完成文件的传送。 数据连接有两种传输模式：

主动传输模式和被动传输模式

VPN通信过程可简化为以下四个通用步骤:(1) 客户机向VPN服务器发出请求；(2) VPN服务器响应请求并向客户机发出身份质询，客户机将加密的用户身份验证响应信息发送到VPN服务器；(3) VPN服务器根据用户数据库检查该响应，如果账户有效，VPN服务器将检查该用户是否具有远程访问权限；如果该用户拥有远程访问的权限，VPN服务器接受此连接；(4) 最后VPN服务器用在身份验证过程中产生的客户机和服务器公有密钥来对数据进行加密，然后通过VPN隧道技术进行封装、加密、传输到目的内部网络。