第3章 应用层

目前，计算技术的发展已进入以网络计算和普适计算为特征、以 Internet 为运行环境的信息化时代。Internet 上提供了丰富的计算资源和信息资源。那么我们如何去使用和访问这些资源呢？计算机网络为我们使用和访问网络资源提供了哪些服务和手段？计算机网络如何接受和响应用户的请求并为用户提供服务？这些都是应用层所要完成的功能。应用层为用户提供的具体服务包括远程登录、电子邮件、文件传输、WWW 服务等，每种服务均有对应的应用层协议来支持，这些协议规定了网络应用所应遵守的规范和准则。下面就详细介绍 Internet 的应用层所提供的各种协议及其功能，具体包括远程终端登录、电子邮件、文件传输、超文本传输等协议，以及为这些协议软件运行提供支持的域名服务等功能。

3.1 概　　述

应用层是网络协议层次模型的最高层，也是网络与用户的接口。我们通过使用 Internet 知道计算机网络提供多种类型的应用服务，如 WWW 服务、电子邮件、文件传输等。对于每种应用服务均涉及网络上不同节点间的通信以及人机间的交互过程，显然，既然涉及通信和交互过程就需要有相关的标准、规则和约定（即协议）来支撑。在 Internet 环境下，各种服务存在一定的差异，所以分别为每种服务定义了相应的应用层协议，如 WWW 服务对应 HTTP 协议，电子邮件对应 SMTP 协议，文件传输对应 FTP 协议，等等。每种服务均由相应的协议软件来支持，这些协议软件分别运行在用户端和服务器端。运行在用户端的软件称为用户软件，运行在服务器端的软件称为服务器软件。不同的服务器软件可以安装在同一台计算机上，也可以分别安装在不同的计算机上。装有服务器软件的系统启动后便创建一个服务器进程（称为守护进程），等待用户的服务请求。用户使用服务时需通过用户软件（如 WWW 浏览器等）发出请求，本地网络操作系统接受该请求并创建一个用户进程（也称为客户进程），该进程通过调用网络协议软件向服务器进程发出请求；服务器进程接受请求并按照协议来分析和响应请求，将处理结果按照通信协议返回给用户进程；协议定义了用户进程与服务器进程间交换信息的格式和顺序以及发送、接收和响应请求时所采取的操作。客户请求和服务器响应的过程如图 3.1 所示。显然，用户进程是一个请求进程，而服务器进程是一个响应进程；这种服务模式称为客户端/服

务器模式，网络上大部分服务均工作于这种模式。

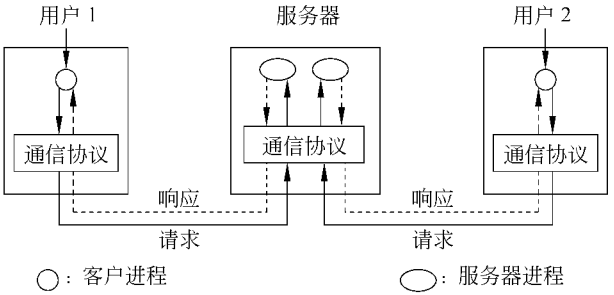

图 3.1　客户端/服务器模式的通信过程

目前，计算机网络所使用的客户端/服务器模式应该严格地称为基于 Web 的客户端/服务器模式，也简称为 B/S(Browser/Server)模式，而传统的客户端/服务器模式简称为 C/S(Client/Server)模式。基于 Web 的客户端/服务器模式与传统的客户端/服务器模式存在一定的区别。传统的客户端/服务器模式是基于不同的操作系统和数据库管理系统来开发的，当客户端的操作系统等系统运行环境发生变化时，可能需要重新开发应用软件，这样势必造成很大的浪费和不便。能否把应用都放在服务器端，而简化用户端的功能，让应用软件在服务器端运行，在这种情况下客户使用时只需要访问服务器即可，这样无论用户端的系统软件环境如何变化，只要能访问服务器就可以得到相应的服务，这就是所谓的 B/S 模式。显然，这种工作方式服务器端的负担较重，而客户机所承担的工作较少，所以也称之为瘦客户机。

现在计算机所使用的都是多任务操作系统，无论是客户机还是服务器均可能同时运行多个进程，而每个进程在通信时都将创建相应的应用层进程，这些应用层进程可能要用到相同的传输层协议。为了区分这些并发的应用层进程，我们引入端口号的概念。每个端口号是一个 16 位的二进制整数，它唯一地标识某台主机内运行的一个应用层进程，应用层进程通过对应的端口调用运输层协议，某台计算机内运行的应用层进程与端口号是一一对应的。对于服务器来讲，它可能同时提供多种网络服务，即运行多个服务器进程。当客户端想要服务器提供某种服务时，它必须事先知道向哪个服务器上的哪个进程发送请求，即必须事先知道相对应的服务器进程的端口号，所以与各种网络服务相对应的服务器进程的端口号必须是公布于众的，这些端口称为熟知端口，Internet 规定熟知端口号从 0 到 1023。表 3.1 给出了各种 Internet 服务所对应的熟知端口号以及这些应用层协议所使用的运输层协议。而客户端进程的端口号是随机产生的，称之为临时端口，其值要大于 1023，该端口号与该客户机的 IP 地址一起随请求传输给服务器进程，以便服务器进程知道是哪个客户机上的哪个进程发出的请求，以便把响应信息返回给客户机上的请求进程。服务与端口间的关系如图 3.2 所示。显然，客户机的 IP 地址和客户进程的端口号在全网范围内唯一地标识了客户进程，而服务器的 IP 地址和服务器进程的端口号也在全网范围内唯一地标识了服务器进程，我们把主机的 IP 地址以及主机上所运行进程的端口号组合在一起，称之为套接字(socket)。这样，一对套接字唯一地标识了网络上的一条通信连接，这一点在传输层介绍 TCP 协议时将详细介绍。

表 3.1　常用 Internet 服务所对应的熟知端口号以及与运输层协议间的关系

服务类型	文件传输		WWW	SMTP	远程终端	简单文件传输	域名服务
	控制连接	数据连接					
端口号	21	20	80	25	23	69	53
运输层协议	TCP 协议					UDP 协议	

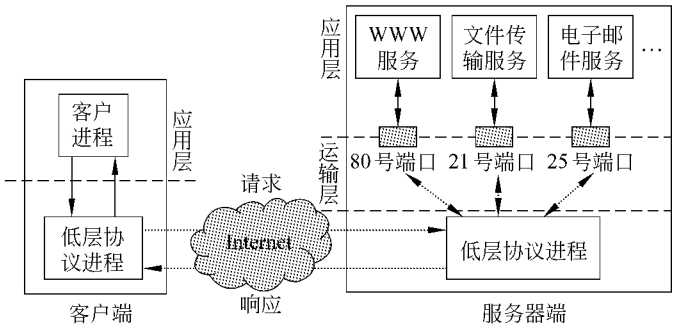

图 3.2　服务与端口间的关系

3.2　域名和域名解析

3.2.1　域名及域名结构

在日常生活中，当我们想要寻找某个地点时，应事先知道该地点的地址。同样，访问网络资源时必须知道提供该资源的服务器地址。在 Internet 上用 IP 地址就可以唯一地标识出网络节点的地址。第 1 章简单地介绍了 IP 地址的概念，实际上 IP 地址是一个 32 位的二进制串，它尽管可以用 4 位点分十进制来表示（如 202.156.122.210），但仍不利于记忆，而人们习惯于记忆名字。所以为了便于记忆，常采用字符串作为网络上各个节点的地址，如搜狐的 WWW 服务器的网址为 www.sohu.com。这种唯一地标识网络节点地址的符号名称为域名（domain name）。域名由专门的组织（不同级别的网络信息中心）进行管理和分配，用户使用域名需要向该组织申请和注册。

由于 Internet 上用户数量的膨胀，域名急剧增多，为了便于管理、记忆和查找，常按照树型层次结构组织域名。域名一般由若干个部分组成，各个部分用点分开，每个部分称为域，从层次树型结构的最顶层依次往下分别称为顶级域、二级域、三级域等，所表示的名称分别称为顶级域名、二级域名、三级域名等，排列顺序从右到左，级别从高到低，分别对应树型结构的不同层次。具体形式为：

….三级域名.二级域名.顶级域名

各级域名由上一级域名进行管理，最高层的顶级域名由因特网名字与号码指派公司 ICANN 进行管理。顶级域名分成三大类：

（1）国家顶级域名。采用了 ISO3166 的规定，例如，.cn 表示中国，.us 表示美国，.jp 表示日本，等等。

(2) 国际顶级域名。采用.int,国际性组织可在.int下面注册域名。

(3) 通用顶级域名。这些域名表示公司、政府部门、军事部门、教育机构等,共13个,如表3.2所示。

表3.2 常用的通用顶级域名

序 号	域 名	代表含义	序 号	域 名	代表含义
1	.com	公司企业	9	.coop	合作团体
2	.net	网络服务机构	10	.info	网络信息服务组织
3	.org	非赢利性组织	11	.museum	博物馆
4	.gov	政府部门	12	.name	个人
5	.mil	军事部门	13	.pro	自由职业者
6	.edu	教育机构	14		
7	.aero	航空部门	15		
8	.biz	商业			

顶级域名下面为二级域名。我国将二级域名分成“类别域名”和“行政区域名”两大类。其中类别域名6个,如表3.3所示。行政区域名有34个,用于表示全国的省、自治区、直辖市和特区,如.bj表示北京,.sh表示上海,等等。若在我国二级域名.edu下申请注册三级域名,则需要向中国教育科研计算机网络中心申请,若在其他二级域名下申请注册三级域名,则需要向中国互联网网络信息中心CNNIC申请。图3.3展示了Internet域名空间的大致情况,其中cs.pku.edu.cn表示北京大学计算机科学系的域名,从图中可以看到,一旦某个单位拥有了三级以下级别的域名,下一级域名完全由它自己决定如何去命名。

表3.3 我国二级域名中的类别域名

序 号	域 名	代表含义	序 号	域 名	代表含义
1	.com	工、商、金融等企业	4	.edu	教育机构
2	.net	网络信息中心和运行中心	5	.ac	科研机构
3	.org	非赢利性组织	6	.gov	政府部门

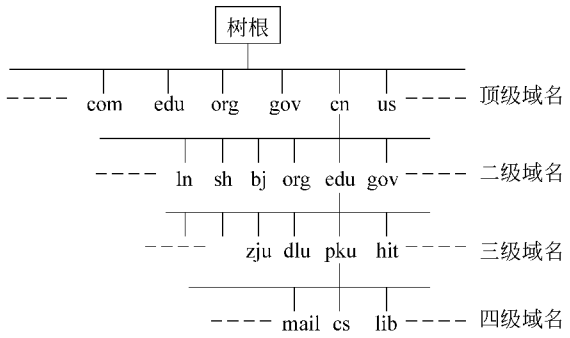

图3.3 Internet域名空间

3.2.2 域名解析

上面已经说明用域名标识某个网络节点只是为了方便记忆，但随数据包一起传输的还是 32 位的 IP 地址，而我们上网所使用的却是域名，所以就需要一种方法自动地将域名转换为 IP 地址。这种将域名转换为 IP 地址的过程称为域名解析。

域名解析的过程与打电话的过程颇为相似。当我们要给某个人打电话时，首先想到的是这个人的姓名，然后根据姓名查找电话号码簿，找到其电话号码，再使用电话号码进行拨号和通话；此时通过电话号码簿就将受话人的姓名转换为其电话号码。

在 Internet 发展初期，由于当时的网络规模比较小，采用 Host 文件来记录和管理网络上各个节点的域名和对应的 IP 地址，进而实现域名解析功能。该文件存储在网络的中心管理服务器上，每个网络节点在启动时均需要从中心服务器上下载该文件。但是，随着 Internet 主机数量的急剧增加，除了 Host 文件的大小不断增加外，每次 Host 文件的初始下载及其更新过程产生的流量也在不断增加，进而给网络通信造成了很大负担。所以迫切需要一种采用分布式管理方式、可扩展性好、支持多种数据格式的软件系统来代替 Host 文件实现域名解析功能，这就是下面将要介绍的域名服务器软件。

这种称为域名服务器的软件诞生于 1984 年，它代替了基于 Host 文件的域名解析方式来完成域名解析功能，该软件也称为 DNS(Domain Name System)服务器。域名服务器工作于应用层，它使用运输层中的 UDP 协议进行传输。Internet 上通常设有多个域名服务器，它们按着域名的层次进行组织。每一个独立的网络系统，称为自治系统(Autonomous System，AS)均设有自己的域名服务器，它负责本区域内所有网络节点域名的管理和解析，该域名服务器称为本地域名服务器，也称为授权域名服务器或者默认域名服务器，该区域的每个网络节点必须将其域名和对应的 IP 地址等信息登记在其本地域名服务器的 DNS 数据库中。此外，Internet 上还有 13 个根域名服务器，它们是负责顶级域名管理的授权域名服务器，这些域名服务器大部分位于北美洲。这些按照层次关系组织的域名服务器形成了一个相互协同工作的分布式系统，共同完成 Internet 的域名解析任务。

为了实现上述的域名解析功能，假设：

- 每个域名服务器必须知道所有根域名服务器的 IP 地址。
- 每个域名服务器必须知道其下一级的域名服务器的 IP 地址。

显然，只有满足上述条件，各个域名服务器才能知道其他相关域名服务器的地址信息，这样它们才能相互协同以共同完成域名解析工作。

通常，域名解析有两种不同的实现方式：递归解析(recursive resolution)和反复解析(iterative resolution)。

(1) 递归解析：当主机需要进行域名解析时，它就向本地域名服务器发送一个 DNS 请求报文，其中含有要解析的域名信息；若本地域名服务器找到了指定的域名，则形成响应报文将对应的 IP 地址等信息返回给主机；若本地域名服务器没有找到指定的域名，则本地域名服务器将请求根域名服务器协助查找；然后根域名服务器根据要查找域名的二级域名请求相应的二级域名服务器协助查找。重复上述过程，直到某一级的域名服务器

找到了相应的域名信息，然后它形成 DNS 响应报文，按照刚才的请求路径逆向传递，最终传递给请求域名解析的主机。上述域名解析过程如图 3.4 所示，其中的序号标明了 DNS 请求和响应的顺序。

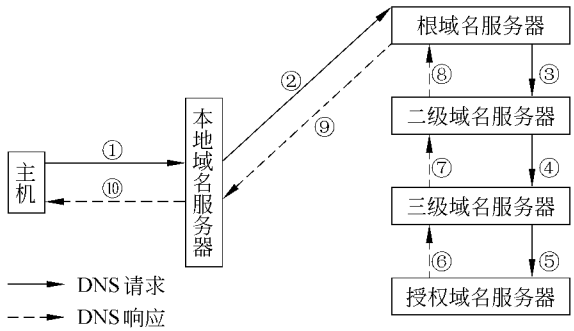

图 3.4　域名的递归解析过程

(2) 反复解析：反复解析也称为迭代解析。当主机需要进行域名解析时，它也是首先向本地授权域名服务器发送一个 DNS 请求报文。若本地域名服务器找到了指定的域名，则形成响应报文将对应的 IP 地址等信息直接返回给主机。若本地域名服务器没有找到指定的域名，则它要向相应的根域名服务器发送 DNS 请求报文要求协助查找；若根域名服务器若找到相应的域名，则形成 DNS 响应报文返回结果给本地域名服务器；否则将根据待查找域名的二级域名确定下一个域名服务器，并把该域名服务器的地址通知给本地域名服务器；然后本地域名服务器再向该二级域名服务器发出请求，要求其协助查找；若该域名服务器找到了相应的结果，则形成 DNS 响应报文，将查到的 IP 地址等信息通知给本地域名服务器；若没有找到，则再根据待查找域名的三级域名确定下一级域名服务器，并把它的地址通知给本地域名服务器。重复上述过程，直到某一级的域名服务器找到了结果，并将结果通知给本地域名服务器，本地域名服务器将查找结果形成 DNS 响应报文通知给主机，从而完成了一次域名解析工作。域名反复解析的过程如图 3.5 所示，其中的序号标明了 DNS 请求和响应的顺序。

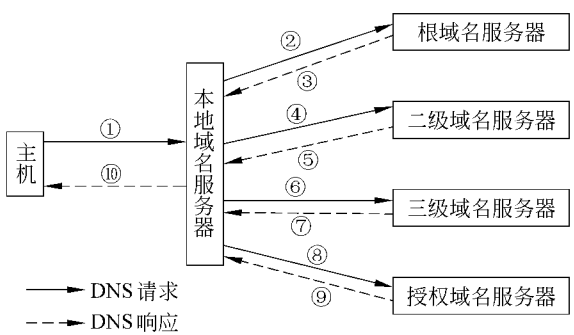

图 3.5　域名的反复解析过程

为了提高域名解析过程的查找速度，还采取了两种措施：

(1) 在本地域名服务器内设置了一个高速缓存。当本地域名服务器从其他域名服务

器得到不在其管辖范围内的域名和对应的域名服务器地址信息后，就把该域名和对应的域名服务器地址存入高速缓存。以后在域名解析过程中，一旦确定所解析的域名不在其管辖区域内，下一步就查找高速缓存，若高速缓存内仍查不到，则再向根域名服务器发出请求，要求协助查找。

(2) 许多主机在启动时从本地域名服务器中下载全部域名解析信息，同时在内存中设置了高速缓存，用于记录新得到的域名解析信息。这样，每次进行域名解析时，首先查找本地 DNS 信息，若找不到才求助于本地域名服务器，这样可以显著加快域名解析的速度。

由于网络是动态变化的，高速缓存中的内容可能因为时间过长而失效，所以为了保证高速缓存中内容的有效性，要设置时钟限制并定时更新。

此外，为了保证域名解析系统工作的可靠性，域名服务器一般均成对存在，以便一个出现问题时另一个能接替工作。

3.3 远程终端协议

在计算机发展的初期，个人计算机的功能相对简单，而更多的计算机软硬件资源和信息资源都集中在小型或者更高档次的计算机系统上，这些计算机系统运行分时操作系统，同时可以为多个用户提供服务。而功能有限的个人计算机(或者终端)为了完成复杂的功能或者为了获取更多的信息资源常常作为一个仿真终端或者智能终端登录到远程计算机系统上，以使用远程计算机系统上的资源。此时，对于用户而言，它的显示器和键盘就好像直接连接到远程计算机系统上一样，这就是远程登录服务。但随着个人计算机功能的逐渐增强，远程登录服务目前已很少使用。

Internet 使用远程终端协议(TELNET)来提供远程登录服务。这种服务也是工作在客户端/服务器模式，它由两部分组成：客户端和 TELNET 服务器。远程 TELNET 服务器上运行服务器进程，这个进程是一个守护进程，一直运行在 23 号端口，等待用户的 TELNET 请求。当用户想要申请 TELNET 服务时，它在本地计算机上启动一个 TELNET 客户进程，向 TELNET 服务器的 23 号端口发送请求，服务器进程接到该请求后，它启动一个子进程响应该 TELNET 请求，然后返回到服务器进程继续等待其他 TELNET 请求。其工作原理如图 3.6 所示。

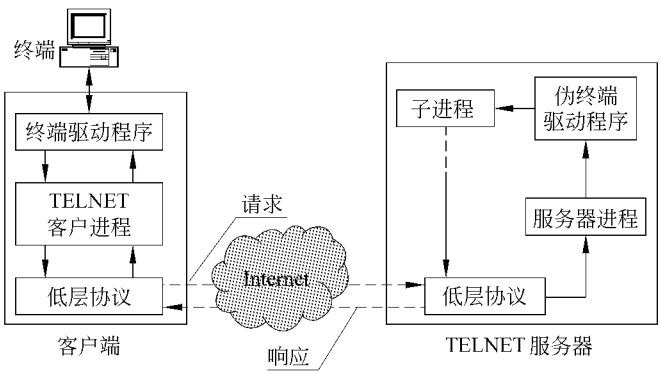

图 3.6 远程登录过程示意图

远程登录服务所涉及的一个关键问题是客户端和远程服务器可能是异构的，它们所使用的键盘输入字符格式等方面可能并不相同。如有些系统使用 ASCII 码的回车(CR)来表示文本行的结束，有些系统使用换行符(LF)来表示，而有些系统使用回车加换行符的组合来表示。为了使 TELNET 服务器能够识别远程用户所输入的命令，必须消除这些差异。Internet 采用网络虚拟终端(Network Virtual Terminal，NVT)来适应不同系统间的差异。即用户输入的命令首先由本地格式转换为 NVT 格式，然后发送给 TELNET 服务器；TELNET 服务器接收这种 NVT 格式的命令，再转换为服务器端的命令格式，然后执行，并将返回结果转换为 NVT 格式返回给用户；用户接收后再将之转换为本地格式并显示在显示器上。具体过程如图 3.7 所示。

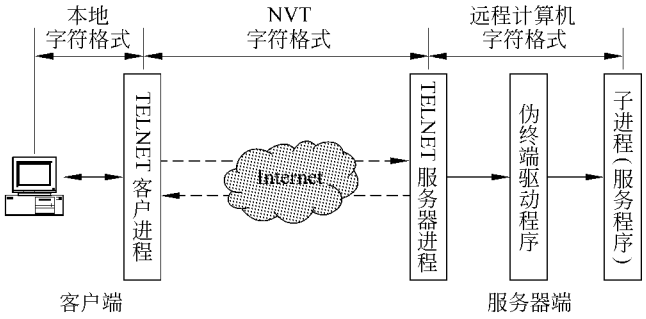

图 3.7　远程登录的 NVT 转换示意图

当本地用户想要获得远程登录服务时，首先要使用 telnet 命令在 TELNET 服务器上进行登录和注册；获得允许后就可以像本地终端一样访问 TELNET 服务器上的各种资源。

3.4　文件传输协议

计算机网络最基本的功能就是通信。数据可以通过网络从一台计算机传输到另一台计算机。而数据在计算机系统中通常以文件形式进行组织、管理和存取，所以文件传输服务是计算机网络所提供的基本功能之一，也是计算机网络产生初期使用最多的功能，目前仍在广泛使用。

文件传输服务将数据文件从一台计算机复制到另一台计算机，即实现文件的下载或上传功能，这种服务看起来似乎很简单，但是实现起来却相当复杂。我们知道，计算机网络常常由多台异构的计算机系统所组成，这些系统的操作系统、所使用的字符集、采用的文件结构及格式、目录的组织方式等均可能不同，所以文件传输必须考虑到这些差异，并能屏蔽掉这些差异，为用户提供透明的文件传输服务。Internet 采用文件传输协议(File Transfer Protocol，FTP)实现上述功能，所以文件传输服务也称为 FTP 服务。

3.4.1　FTP 的工作原理

文件传输服务工作于客户端/服务器模式，它由两部分组成：客户端和服务器端，如

图 3.8 所示。用户操作的计算机即为客户端，存储用户想要访问文件的计算机系统为服务器端，通常称该计算机系统为 FTP 服务器，用户通过 FTP 协议访问服务器端的文件。FTP 协议工作于运输层的 TCP 协议之上，它采用 21 号端口，以面向连接的方式工作，通过客户端和服务器端的交互会话过程实现它们之间的数据传输。

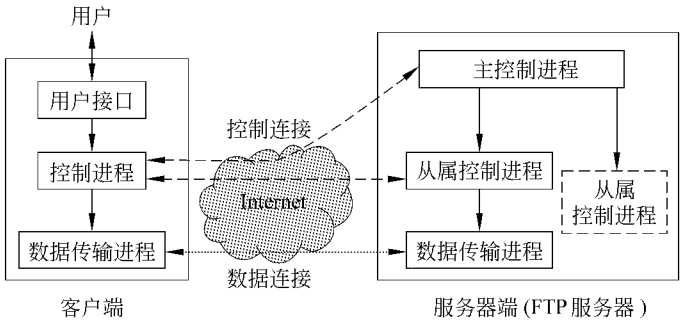

图 3.8　文件传输过程示意图

图 3.8 给出了 FTP 服务的基本模型。客户端由用户接口、控制进程和数据传输进程组成。而服务器端由主控制进程、从属控制进程和数据传输进程组成，其中主控制进程为守护进程，FTP 服务器启动后它就一直处于运行状态，该进程一直监测 21 号端口，等待用户的 FTP 请求。在文件传输过程中，用户在客户端启动一个控制进程，通过该控制进程向 FTP 服务器的 21 号熟知端口发送文件传输请求。服务器端的主控制进程接收到该 FTP 请求，创建一个从属控制进程用于建立与客户端控制进程间的连接（即控制连接），进而控制与该客户端间的数据传输过程，然后主控制进程返回并继续等待响应其他 FTP 用户的并发请求。客户端控制进程创建一个客户端的数据传输进程，并通过控制连接将该数据传输进程所使用的端口号通知给服务器端的从属控制进程，进而发出一次数据传输请求。然后，从属控制进程采用 20 号熟知端口启动一个数据传输进程，并向客户端数据传输进程的端口发送请求，进而建立与客户端数据传输进程间的连接（即数据连接）。以后的文件传输过程就在客户端的控制进程与服务器端的从属控制进程的控制下，由客户端与服务器端的数据传输进程来完成。显然，主控制进程可以创建多个从属控制进程，以响应来自多个不同客户的 FTP 请求。在文件传输期间，控制连接是一直存在的，而数据连接是在每次数据传输请求时创建，数据传输结束后撤销；随着数据连接的撤销，相应的数据传输进程也随之消亡；当有新的数据传输请求时，再由传输控制进程创建新的数据传输进程和数据连接，以再一次完成数据传输任务，直到所有的数据传输完毕，控制进程才随之消亡。

3.4.2　FTP 的使用及所传输的文件类型

FTP 提供交互式的访问操作。在使用 FTP 操作时，首先用户需要启动 FTP 客户端程序，通过传统的 FTP 命令、浏览器或者专用的下载工具向 FTP 服务器发送连接请求，通过输入自己的用户名和密码以在 FTP 服务器上进行登录。登录成功后就可以访问 FTP 服务器。通常 FTP 提供两种类型的服务：

(1) 特许 FTP 服务。特许 FTP 服务指用户在 FTP 服务器上建立有自己的账号,在访问 FTP 服务器时要求用户输入自己的用户名和密码。该种服务方式下用户拥有较高的使用权限,但对于没有开设账号的用户来讲,显然无法访问 FTP 服务器,所以 Internet 提供了另一种 FTP 服务方式,即匿名 FTP 服务。

(2) 匿名 FTP 服务。该种服务方式为用户建立了一个公开账户,用户名一般为 anonymous,密码一般为 guest。普通用户都可以使用上述用户名和密码登录 FTP 服务器,访问 FTP 服务器上的信息资源。但为了安全起见,对公众开放的信息资源是有限的,而且对用户的使用权限进行了限制,不允许用户上传文件或者修改服务器中的文件。

FTP 提供文本和二进制等两种数据格式文件的传输。文本文件的默认格式为 ASCII 码文件;传输时在发送端将每个字符采用 NVT 形式进行编码,然后进行传输;到达接收端后接收端再将 NVT 编码形式的字符转换成它本身的码制。对于二进制文件采用连续的位流形式进行传输而不需要任何编码。

3.4.3 TFTP 及与 FTP 的区别

相对于 FTP 协议而言,还有另一个更为简单的文件传输协议,即简单文件传输协议(Trivial File Transfer Protocol,TFTP)。它是一个简化的文件传输协议,其代码非常简短,可以放在无盘工作站的只读存储器中运行。TFTP 使用 69 号熟知端口,采用无连接的方式(即使用传输层中的 UDP 协议)进行文件传输;而 FTP 协议是采用面向连接的方式(即使用传输层中的 TCP 协议)。TFTP 不支持交互,因而非常适合多个文件同时传输的情况。但因为在传输层采用了不可靠的 UDP 协议,所以 TFTP 需要有自己的差错保证措施。

3.5 电子邮件服务

电子邮件服务是计算机网络所提供的基本服务方式,是目前使用最为广泛的 Internet 服务之一。电子邮件也称 E-mail,它代替了传统的电报,为通信双方提供了简单、快捷、廉价的信息传递方式,深受广大用户的欢迎。

3.5.1 电子邮件系统的组成及工作过程

电子邮件系统一般由三部分组成:用户代理、邮件服务器和邮件传输协议,如图 3.9 所示。用户代理是用户与电子邮件系统的接口,用户通过用户代理来编辑和管理电子邮件,并负责将邮件发送到发送邮件服务器以及从接收邮件服务器中读取邮件。用户代理常通过运行电子邮件应用软件来创建,目前常用的电子邮件应用软件有 Microsoft 公司的 Outlook Express 和 Netscape 公司的 Netscape Communicator 等,用户通过这些软件就可以方便地实现邮件的发送和接收。

邮件服务器由发送邮件服务器和接收邮件服务器组成,通过 Internet 分别完成邮件的发送和接收功能。

显然,无论是用户代理和邮件服务器之间,还是邮件服务器之间传递邮件时均要遵守