

目前,计算技术的发展已进入以 Internet 为运行环境、以网络计算和普适计算为特征、正积极向云计算推进的信息化时代。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? Internet 为我们使用和访问网络资源提供了哪些服务和手段? 计算机网络如何接收和响应用户的请求并为用户提供服务呢? 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解析、动态主机配置等协议。

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,如完成 WWW 服务的 HTTP 协议、完成电子邮件功能的 SMTP 协议和完成文件传输功能的 FTP 协议等。每种服务均由相应的协议软件来实现,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称为守护进程(Daemon)的服务器进程,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收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对应的服务器进程发出请求。服务器进程接收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/服务器模式,网络上大部分服务均工作于这种模式。

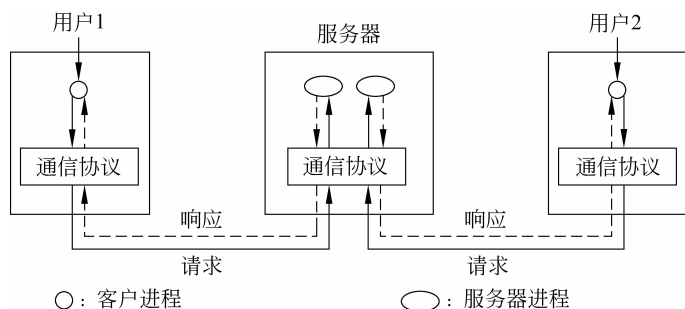


图 3.1 客户/服务器模式的通信过程

目前,计算机网络所使用的客户/服务器模式应该严格地称为基于 Web 的客户/服务器模式,简称为 B/S(Browser/Server)模式,而传统的客户/服务器模式简称为 C/S(Client/Server)模式。基于 Web 的客户/服务器模式与传统的客户/服务器模式间存在一定的区别。传统的客户/服务器模式下客户端程序承担较多的功能,是基于不同的操作系统和数据库管理系统开发的。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,而且对于不同的操作系统环境,应用软件的移植也存在一定困难。能否把应用系统都放在服务器端,而简化用户端的功能,让应用软件在服务器端运行呢?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,这种工作方式下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。目前的云计算正是贯彻这种理念,将服务集中在云端即服务器端,而客户端可以做得非常简单,只要它能通过网络访问云端就可以得到云端提供的各种服务。

现在计算机所使用的都是多任务多用户操作系统,无论是客户机还是服务器均可能同时运行多个进程。对于计算机网络而言,它可能同时提供多种类型的服务,而每种服务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运输层协议。为了区分这些并发的应用层进程,在应用层的下一协议层——运输层引入了端口号的概念。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。应用层进程在调用运输层协议时由运输层进程为其分配一个端口号,并保证在一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类型的网络服务,即运行多个服务器进程。当客户端想要得到某种类型的网络服务时,它必须事先知道向哪台服务器上的哪个服务器进程发送请求,即必须事先知道提供该服务的服务器地址和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 规定熟知端口号范围是 0~1023。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也是由它调用的运输层协议进程随机产生的,称之为临时端口,其值要大于 1023,一般在 49 152 和 65 535 之间。当客户机想要得到某种网络服务并创建一个客户进程时,客户进程将调用通信协议将所获得的端口号和客户机的 IP 地

址作为源端口号和源 IP 地址,而将提供服务的服务器进程的熟知端口号和服务器的 IP 地址作为目的端口号和目的 IP 地址,连同请求信息一起封装成请求数据包,发送给服务器。网络层的 IP 协议根据请求数据包中的目的 IP 地址控制该数据包传输到相应的服务器,服务器接收到该数据包后由运输层协议根据其中的目的端口号将该请求送给相应的服务器进程(即应用层进程)。服务器进程处理客户端的请求,然后将请求数据包中的源端口号和源 IP 地址作为目的端口号和目的 IP 地址与响应信息一起封装成响应数据包,并发送给请求服务的客户机进程。各种服务与端口间的对应关系如图 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 地址以及主机上标识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,这一点在运输层介绍 TCP 协议时将详细讲解。

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		远程终端	SMTP	WWW	域名服务	简单文件传输	简单网络管理
	数据连接	控制连接						
端口号	20	21	23	25	80	53	69	161
运输层协议	TCP 协议					UDP 协议		

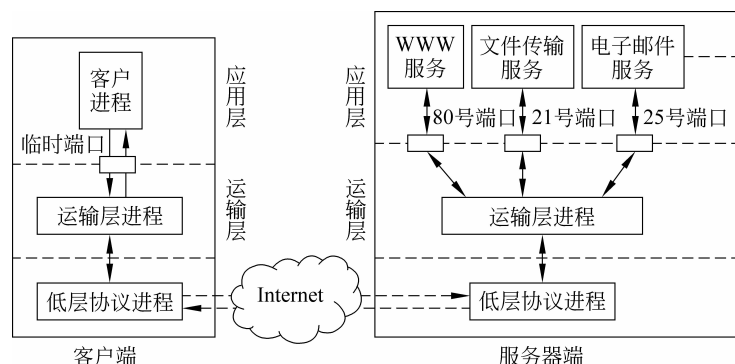


图 3.2 各种网络服务与端口间的关系

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,在访问网络资源时必须知道提供该资源的网络地址。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,在网络层我们还将详细介

绍。实际上 IP 地址是一个 32 位的二进制串,它尽管可以采用 4 位点分十进制来表示(如 202.156.122.210),但这样一串枯燥的数字仍不利于记忆,而人们习惯于记忆名字。所以为了便于记忆,常采用形象、直观的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),也称为主机名(host name)。域名是一个逻辑概念,与主机所在的地理位置没有必然联系,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,常采用树型层次结构组织域名。其中树根节点为空,以下的每级节点依次分别称为顶级域、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,如图 3.3 所示。整个域名树组成了 Internet 的域名空间,而以每个子节点为根的子树组成了 Internet 的一个域名子空间。域名树上的每个节点(除根节点)都定义了一个标签(label),它是该节点所对应级别域名的一个实例,它由字母、数字和连字符“-”组成,其最大长度为 63 个字符,而且不区分大小写。网络上每个节点的域名是从该节点开始,按照域名树的层次结构自底向上,最终结束到根节点,而形成的一个标签序列,书写时从左到右排列,中间用圆点分开,具体形式为:

...,三级域名.二级域名.顶级域名

如:北京大学图书馆的域名表示为 lib.pku.edu.cn。

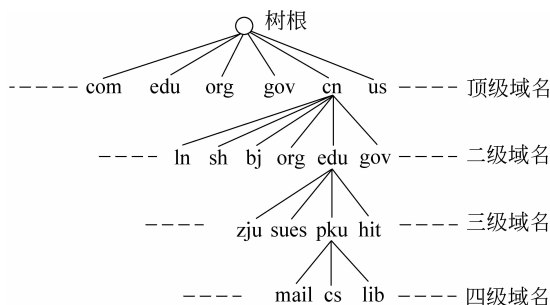


图 3.3 Internet 域名空间

注意,一个域名的最大长度为 255 个字符。各级域名由上一级域名机构进行管理,顶级域名由因特网名字与号码指派公司(The Internet Corporation for Assigned Names and Numbers, ICANN)进行管理。顶级域名分成如下三大类。

- 国家顶级域名。采用了 ISO 3166 的规定,例如,.cn 表示中国,.us 表示美国,.jp 表示日本等。
- 国际顶级域名。采用.int,国际性组织可在.int 下面注册域名。
- 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。

顶级域名下面是二级域名。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 34 个,用于表示全国的省、自治区、

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			

直辖市和特区,如.bj表示北京,.sh表示上海等。若在我国二级类别域名.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,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和管理。

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

3.2.2 域名解析

上面已经说明用域名标识某个网络节点的地址只是为了方便记忆,但随数据包一起传输的还是32位二进制数组成的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Hosts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Hosts文件存储在网络系统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Hosts文件的大小不断增加外,每次Hosts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Hosts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系统。

这种称为域名服务器的软件系统诞生于 1984 年,它代替了基于 Hosts 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 服务器(Domain Name System,DNS),它执行的协议是一个应用层协议,称之为域名解析协议。DNS 服务器上设有 DNS 数据库,用于记录和存储网络节点的域名、IP 地址等信息。

Internet 上通常设有多个域名服务器,分别负责不同域名子空间的域名解析工作。这些服务器按着域名的层次结构进行组织,分布在级别不同的各个域中,组成了一个高效、可靠、协同工作的分布式系统。域名服务器具体分为如下三类。

- 本地域名服务器。每一个独立的网络系统称之为自治系统(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 地址等信息登记在一个本地域名服务器的 DNS 数据库中。
- 授权域名服务器。Internet 上,登记有某台主机域名信息的本地域名服务器也称为这台主机的授权域名服务器。为了可靠起见,要求每台主机至少有两台授权域名服务器。
- 根域名服务器。Internet 上共有 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,其中有 10 个位于北美洲,其他三个位于欧洲和亚洲。根域名服务器的作用非常重要,若出现故障将严重影响网络的正常运行,所以每个根域名服务器一般是由多个服务器组成的分布式系统,它们协同、可靠地工作,共同完成域名的解析任务。

域名解析系统工作于客户/服务器模式,它使用运输层中的 UDP 协议进行传输,对应的端口号为 53。为了提高域名解析的速度,每个网络节点常在本地存储中开辟一块存储区域(称为 DNS 缓存),用于存储域名和对应的 IP 地址等信息。当 WWW、E-mail、FTP 等服务采用域名访问网络时,应用进程首先创建一个称为域名解析器(resolver)的本地客户端进程,该进程接收应用进程的域名解析请求,并在本地 DNS 缓存中进行查找,若找到对应域名的 IP 地址则直接将查询结果返回给应用进程。若域名解析器在本地缓存中没有找到匹配结果,则它将要进行解析的域名等信息封装成 DNS 请求报文,调用运输层的 UDP 协议,向本地域名服务器的 53 号端口发送请求,要求本地域名服务器协助查找。若本地域名服务器仍没有查找到结果,则它作为新的客户端再向其他域名服务器发送 DNS 请求,直到在某个域名服务器上查询到待解析的结果,然后形成 DNS 响应报文将查询结果返回给请求 DNS 服务的主机,该主机首先将域名和得到的 IP 地址存入自己的 DNS 缓存,然后采用该 IP 地址封装数据包,并发给相应的服务器。

显然,为了实现上述的域名解析功能,必须做如下假设。

- 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。实践已经证明 DNS 是在 Internet 上实现的最成功的分布式系统。

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但在本地没有成功时,它调用解析器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 DNS 响应报文将对应的 IP 地址信息返回给主机。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授权的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,然后由它形成 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。

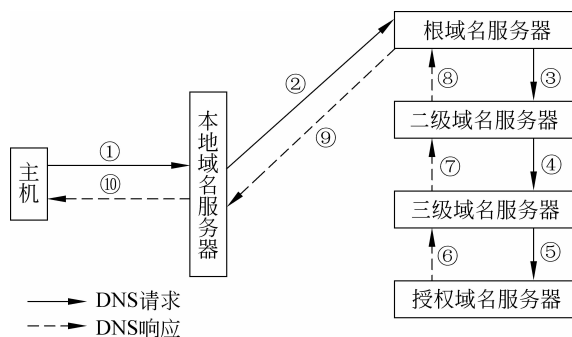


图 3.4 域名的递归解析过程

(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但在本地没有成功时,它也是首先调用解析器向本地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 DNS 响应报文将对应的 IP 地址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,则要向授权的根域名服务器发送 DNS 请求报文要求其协助查找。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;否则根域名服务器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 DNS 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。

为了提高域名解析过程的查找速度,还采取了如下三种措施。

(1) 为了减轻根域名服务器的负担,常使它工作于反复解析模式。即根域名服务器一接收到某个本地域名服务器的 DNS 协助请求,它将根据待解析的域名确定下一个负责解析该域名的域名服务器的 IP 地址,并将之通知给发出请求的本地域名服务器,让它们合作完成该次域名的解析工作,以后不再干预,从而减轻其工作负担。

(2) 在本地域名服务器内设置了一块高速缓存。当本地域名服务器从其他域名服务器得到了不在其管辖范围内的域名和对应的 IP 地址信息后,就把该域名和对应的 IP 地址等信息存入高速缓存。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。

(3) 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 DNS 高速缓存(在前面介绍域名查找算法时已经提到),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,以便一个出现故障时另一个能接替工作。

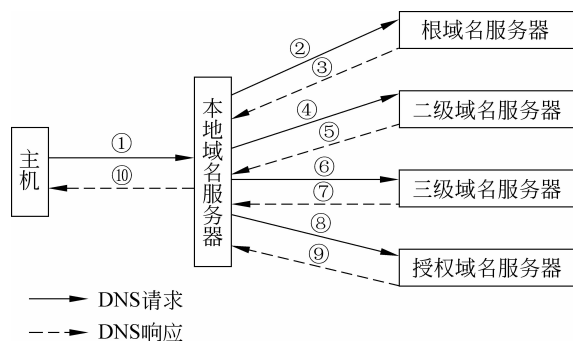


图 3.5 域名的反复解析过程

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,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,远程计算机系统就像用户的本地主机一样供用户使用,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 TELNET 协议来提供远程登录服务。这种服务工作在客户/服务器模式,它由两部分组成: TELNET 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 号端口发送连接请求。服务器进程接收该请求,建立与客户机的连接,并启动一个子进程响应该 TELNET 请求,然后返回到等待状态继续等待其他 TELNET 请求。远程登录系统的组成如图 3.6 所示。

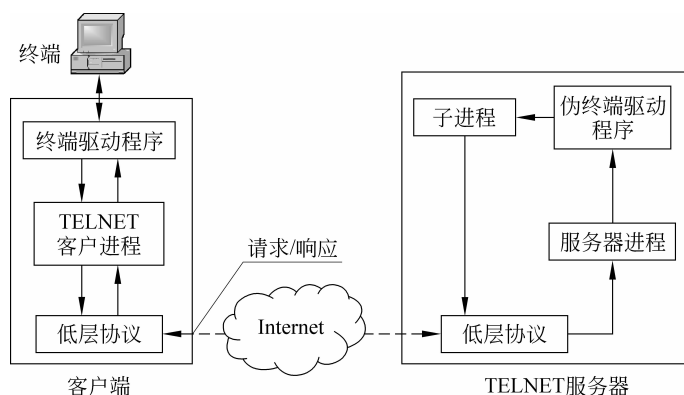


图 3.6 远程登录过程示意图

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,它们在计算机硬件、所使用的操作系统以及键盘输入字符的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(CR+LF)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,并将响应结果转换为 NVT 格式后返回给用户,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。

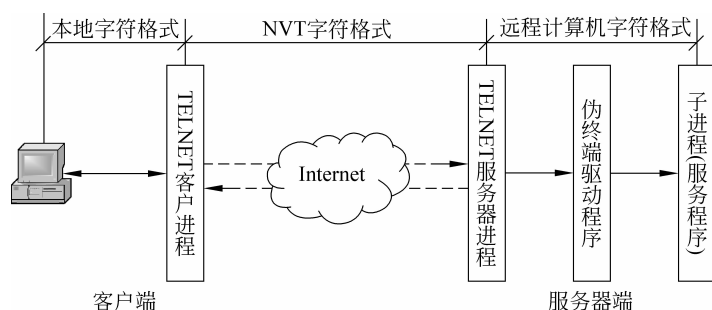


图 3.7 远程登录的 NVT 转换示意图

NVT 使用 7 位标准的 ASCII 码来表示数据,每个 7 位字符以字节为单位进行发送,字节的最高位规定为 1。7 位标准的 ASCII 码字符集包括可打印或显示的普通字符和不可显示的控制字符。对于用户输入的普通字符,NVT 将其按照原始含义进行传送;而当

输入的是控制字符或者组合字符时,NVT 将它们转换为特殊的编码然后在网络上传输。

当本地用户想要获得远程登录服务时,首先在本地计算机上启动一个 TELNET 客户进程,向 TELNET 服务器申请进行登录和注册,建立与 TELNET 服务器间的双向连接(该连接通过运输层的 TCP 协议来建立),并通过该条连接进行交互,传输命令、响应等信息。

TELNET 协议支持多种命令,这些命令用于控制客户端与服务器间的相互交互。每条 TELNET 命令一般由两个以上字节组成,第一个字节各位全为 1(即 0xFF),称为 IAC (Interpret As Command),它是一个转义字符,用于表示后续的字节为命令代码。对于某些命令代码,其后跟有选项代码,用于客户端与服务器间协商数据的传输方式、传输速度等,以增强 TELNET 协议的灵活性和对异构环境的适应能力。部分常用的 TELNET 命令如表 3.4 所示。

表 3.4 常用的 TELNET 命令

命令	命令编码	命令含义
IAC	255	表示之后的数据为命令
DON'T	254	表示选项参数所指定的请求被拒绝
DO	253	表示选项参数所指定的请求被接受
EL	248	通知服务器删除当前行
EC	247	通知服务器删除前一个字符
IP	244	中断、终止或结束某个进程
BRK	243	表示数据传输的中断
EOF	236	表示文件中的数据已全部传输出去

3.4 文件传输协议

计算机网络最基本的功能就是实现数据通信和资源共享。通过网络位于一台计算机上的文件可以传输到另一台计算机,通过网络也可以读取其他计算机上的文件。在计算机网络中,上述功能是通过文件传输协议来实现的。这种文件传输协议最初是 ARPANET 协议的一个组成部分,后来发展成 TCP/IP 协议中的一个应用层协议。这种协议实现了文件的远程传输功能,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。

文件传输服务通过网络将文件从本地计算机复制到另一台称为文件服务器的计算机,该过程称为文件的上传。相反,从文件服务器传输文件到本地计算机的过程称为文件的下载。这种文件的传输过程看起来似乎很简单,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所组成,这些计算机的操作系统、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存在一定差异,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