第1章

Internet 基础

1.1 Internet 简介

Internet 已经成为目前人们生活中的一部分，早期的 Internet 网络是 1969 年美国国防部国防高级研究计划署(DoD/DARPA)资助建立的只有 4 个节点的名为 ARPAnet 的网络。它将加利福尼亚大学、斯坦福大学及犹它州州立大学等大学的计算机主机通过专门的通信线路和设备彼此连接起来进行通信。1972 年 ARPAnet 的规模已经增长到了 20 多个节点，它们彼此之间可以发送电子邮件、利用文件传输协议发送大文本文件以及提供远程登录服务。ARPAnet 网络互联使用的是 TCP/IP 协议簇，它的发展促进了 TCP/IP 协议簇的开发和使用，奠定了 Internet 存在和发展的基础，较好地解决了异种机网络互联的问题。此后，人们将以 ARPAnet 为主干网的网际互联网称为 Internet。1986 年美国国家科学基金会 NSF(National Science Foundation)建立了美国国家科学基金网 NSFnet。NSFnet 由六大超级计算机中心组成，它是基于 TCP/IP 协议簇的计算机网络，它的建成使得美国的科学家和工程师能够共享超级计算机设施。NSF 在全国建立了按地区划分的计算机广域网，并将这些地区的广域网络和超级计算中心相连接，最后将各超级计算中心互联起来。地区网的构成是由某一区域，或者是某一机构，或者在经济上有共同利益的用户的计算机互联而成，连接各地区网上主通信节点计算机的高速数据专线构成了 NSFnet 的主干网，当某地区用户的计算机与地区网相联后，既可以通过使用超级计算中心的设施同网络上的用户通信，又可以获得大量共享的网络资源。1990 年 6 月 NSFnet 取代了 ARPAnet 成为 Internet 的主干网。1990 年 9 月 Merit、IBM 和 MCI 公司联合建立了 ANS(Advanced Network&Science, Inc)公司，ANS 的目的是建立一个全美范围的 T3 级主干网，它能以 45Mbps 的速率传送数据，相当于每秒传送 1400 页文本信息。1991 年底 NSFnet 的全部主干网都同 ANS 提供的 T3 级主干网连通。随着计算机网络技术的迅猛发展，Internet 将全球数万个计算机网络、数千万台主机连接起来，向全球提供大量的信息服务和信息资源，今天的 Internet 已不再是计算机人员和军事部门进行科研的领域，而是变成了一个开发和使用信息资源的覆盖全球的信息海洋。随着商业网络和大量商业公司进入 Internet，网上商业应用取得高速的发展，同时也使 Internet 能为用户提供更多的服务，使 Internet 迅速普及和发展起来。Internet 使计算机用户不再

被局限于分散的计算机上，任何人只要进入了 Internet，就可以利用网络中和各计算机上的丰富资源。

1.2 计算机网络

计算机技术和通信技术的结合产生了今天广泛使用的计算机网络技术。计算机网络无时无刻不在影响着人们的生活并为人们的生活带来了极大的方便，如办公自动化、银行的存取款、网上订票、通过电子邮件交流信息和网上购物等。早期的计算机网络只是在铜线上传输单纯的数据，而且数据传输的速度也很慢。随着计算机网络技术的飞速发展，如今的网络不仅可以传输数据，更可以传输图像、声音和视频等多种媒体形式的信息，在人们的日常生活和各行各业中发挥着越来越重要的作用。

1.2.1 计算机网络的含义

计算机网络就是利用通信设备和线路将处于不同地理位置的、功能独立的多个计算机系统连接起来，以功能完善的网络软件（即网络通信协议、网络操作系统等）实现网络资源共享和信息传递。

两台计算机通过通信线路（包括有线和无线通信线路）连接起来就组成了一个最简单的计算机网络。全世界成千上万台计算机相互间通过电缆、电话线和卫星等连接起来构成了世界上最大的 Internet 网络。

1.2.2 计算机网络的发展

计算机网络从产生到发展经历了巨大的技术变革和应用的革命。最早的计算机网络诞生于 20 世纪 50 年代，经过了近半个世纪的发展，计算机网络已经存在于人们工作、生活、学习和娱乐等的各个角落。计算机网络从产生到发展大约经历了四个阶段。

第一阶段是在 20 世纪 50 年代出现了以一台计算机为中心，通过通信线路连接若干终端（用户端不具备数据处理和存储能力）而构成的简单的计算机网络。这种形式的网络用户通过终端连接到中心计算机，共享中心计算机的资源。随着终端与中心计算机网络通信的不断增长以及中心计算机处理数据量的不断增加，这种形式网络的问题开始显现出来。一是中心计算机既要承担数据处理的任务，又要承担通信任务，造成中心计算机负担太重；二是由于终端设备本身不具备数据处理和存储能力，因此需要不断与中心计算机交换数据，常常是每个用户独占一条通信线路，造成操作时间较长，线路利用率较低。严格地说这种连接方式还不能算作真正的计算机网络，因为网络中除了中心计算机，其他终端设备都不具备自主处理的功能。但是它为计算机网络的产生和发展奠定了理论基础。

第二阶段是 20 世纪 60 年代末由各自具有自主功能的计算机互联组成的计算机网络。早期面向终端的计算机通信网络是以单个主机为中心的星型网，各终端通过通信线路直接共享主机的硬件与软件资源。随着计算机应用的发展，来自学校、军队、科研单位、大型企业和公司的用户希望将位于不同地点的计算机通过通信线路连接起来，既可以使用本地计算机的软件、硬件与数据资源，也可以使用其他计算机的软件、硬件与数据资源

以达到计算机资源共享的目的。这种网络以美国国防部高级研究计划局的 ARPAnet 为代表。1969 年美国国防部高级研究计划局提供经费将多个大学、公司和研究所的多台计算机互连。起初 ARPAnet 只有几个节点，随着技术的进步和用户数量的增加，ARPAnet 通过有线、无线与卫星通信线路覆盖了从美国本土到欧洲等的广阔地域。ARPAnet 是计算机网络技术发展的一个里程碑。它定义了计算机网络，提出了资源子网和通信子网的网络概念，研究了报文分组交换的数据交换方法，并且采用了层次结构的网络体系结构模型与协议体系。ARPAnet 为今天广泛使用的 Internet 网络奠定了重要的基础。

第三阶段是 20 世纪 70 年代中期开始的计算机网络的标准化阶段。经过第二阶段计算机网络的快速发展，不同的计算机网络厂家分别制定了各自的网络连接标准，这样组建网络时同一个网络中的设备只能使用同一个厂家的产品，不同厂家制定的网络连接标准相互之间不兼容，使得计算机网络的互联遇到了极大的困难。国际标准化组织(ISO)经过多年的研究正式制定和颁布了“开放系统互连参考模型”(OSI RM)，即 ISO 7498 参考模型，该模型将网络分成七层，即物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。很多大的计算机厂商纷纷开始宣布支持 OSI 标准，并积极按照 OSI 所制定的标准研究和开发自己的产品。各种符合 OSI RM 与协议标准的局域网、广域网与城域网得到了广泛应用。开放系统互连参考模型对网络技术的发展和网络理论体系的形成起了重要作用。

第四阶段是从 20 世纪 90 年代开始的计算机网络的综合应用。计算机网络向综合化、高速化和智能化方向发展，并获得广泛的应用。它将语音、视频、图形、图像和数据等多媒体信息综合到一个网络中，利用综合数字业务网(ISDN)、高速局域网、异步传输模式 ATM、交换局域网和虚拟局域网等高速网络技术实现多媒体信息的传输。

随着计算机网络及 Internet 的高速发展，计算机网络的应用将向更高层次发展。计算机网络将会是开放式的网络体系结构，应用不同软硬件和操作系统以及不同协议的网络可以互联，实现资源共享。计算机网络的性能追求的是高速、高可靠和高安全性，会更多地采用多媒体技术，计算机网络的智能化程度会更高。Internet 是覆盖全球的信息基础设施之一，对于用户来说，它像是一个庞大的远程计算机网络。用户可以利用 Internet 实现全球范围的电子邮件、电子传输、信息查询、语音与图像通信服务功能，它将对推动世界经济、社会、科学和文化的发展产生不可估量的作用。

1.2.3 计算机网络的应用

随着社会及科学技术的发展，对计算机网络的发展提出了更加有利的条件。计算机网络与通信网的结合，可以使众多的个人计算机不仅能够同时处理文字、数据、图像和声音等信息，而且还可以使这些信息四通八达，及时地与全国乃至全世界的信息进行交换。企事业单位的内部计算机网络的应用主要有：会计记账系统、人事管理系统、学籍管理系统、采购订单系统、生产管理系统、业务开发系统、科技开发管理系统、内部办公系统、销售管理系统、库存管理系统、出版发行管理系统、数字化图书管理系统、医疗档案管理系统以及娱乐系统等，计算机网络已经渗透到了企事业内部管理的各个方面。

此外，随着计算机网络技术的不断更新，更进一步扩大了计算机网络的应用范围。特

别是随着 Internet 技术的深入发展和应用的普及，计算机网络还具有以下几个主要方面的应用：

① 远程登录。远程登录是指允许一个地点的用户与另一个地点的计算机上运行的应用程序进行交互对话。这种应用方式不仅方便了网络的管理，而且可以为用户之间的交流提供了一块空间，例如 BBS 的应用。

② 电子邮件。电子邮件通过 Internet 这样的全球互联网功能，用户可以在自己的计算机上把电子邮件(E-mail)发送到世界各地，邮件中可以包括文字、声音、图形、图像，甚至视频信息等，提高了用户之间资源共享和交流的效率和效益。

③ 电子数据交换。电子数据交换(EDI)是计算机网络在商业中的一种重要的应用形式。电子数据交换通过一种标准的数据格式，在贸易伙伴的计算机之间传输数据，代替了传统的贸易单据，从而节省了大量的人力和财力，节约成本并提高了效率。

④ 联机会议。利用计算机网络，人们可以通过个人计算机参加会议讨论。联机会议除了可以使用文字外，还可以传送声音和图像。

⑤ 远程医疗。通过图形和图像信息的远程传输，医疗专家可以实现异地的会诊，从而大大提高了病人被治愈的可能性。

⑥ 远程购物。随着电子商务的蓬勃发展，越来越多的人为了节省时间和精力通过互联网实现购物。这种方式不仅降低了商家的成本，而且为客户带来了很多的实惠。

总之，计算机网络的应用范围非常广泛，它已经渗透到国民经济以及人们日常生活的各个方面。

1.3 TCP/IP 协议

TCP/IP 协议可以将运行着不同操作系统的不同厂家生产的计算机相互连接起来进行通信。TCP/IP 协议是一套工业标准协议集，它制定了允许计算机通信的标准和规则。目前，TCP/IP 协议已经被广泛使用在个人计算机、UNIX 主机和 Mac 计算机等计算机系统中，并且也用于连接客户机和主机的网络设备上。

TCP/IP(Transmission Control Protocol/Internet Protocol，传输控制协议/Internet 协议)是目前应用最广泛的通信协议，它也是 Internet 的标准通信协议和局域网的首选协议。TCP/IP 可以实现不同网络结构和不同计算机操作系统的计算机之间互相通信。TCP/IP 协议集是一个分层协议模型，TCP/IP 参考模型通常被认为是一个四层模型，模型中的每一层负责完成不同的通信功能，从高层到低层的顺序依次为应用层、传输层、互联网层和网络接口层。TCP/IP 协议参考模型如图 1.1 所示。

图 1.1 TCP/IP 协议参考模型

在 TCP/IP 协议参考模型中的应用层、传输层和互联网层包含了网络连接时应用到的一些核心协议，如 Telnet、FTP、SMTP、DNS、SNMP、TCP、UDP、IP、ARP、ICMP 和 IGMP 等。通过这些协议，可以高效和可靠地实现计算机系统之间的互联。网络接口层

通常用来处理底层网络连接的物理接口。TCP/IP 参考模型中不同层次的主要协议如图 1.2 所示。

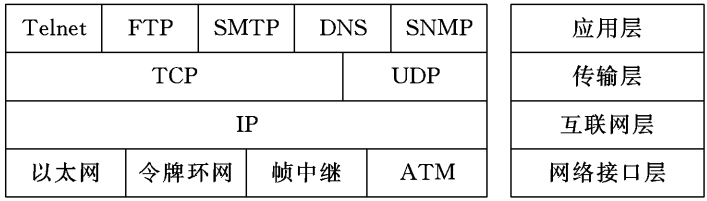

图 1.2　TCP/IP 参考模型分层协议

1.3.1　网络接口层

网络接口层是模型中的最底层，负责将数据包送到电缆上，是实际的网络硬件接口。TCP/IP 参考模型的网络接口层对应于 OSI 参考模型的物理和数据链路层。网络接口层协议定义了主机如何连接到网络，管理着特定的物理介质。在 TCP/IP 模型中可以使用任何网络接口如以太网、令牌环网、FDDI、X.25、ATM、帧中继和其他接口等。

1.3.2　互联网层

互联网层主要包括 IP、ICMP、IGMP、ARP 和 RARP 等协议。IP 协议是网络层协议，用来路由互联网上的数据包。它的功能是用来确定网络源地址和目的地址，是整个网络体系结构中的关键层。ICMP 协议是网际报文控制协议。用来控制数据流，检测 IP 传输中的错误。IGMP 提供了多点传送，该组的主机成员通过 IGMP 将信息提供给路由器。ARP 协议是地址转换协议，实现 IP 地址到 MAC 地址的转换，RARP 协议是反向地址转换协议，实现 MAC 地址到 IP 地址的转换。

1.3.3　传输层

传输层负责提供可靠的信息交换。传输层中主要包括 TCP 和 UDP 协议。TCP 协议是面向连接的协议，主要用于传递大量数据，保证了发送、接收和数据的顺序。通过总体检查以维护数据的完整性和可靠性。UDP 协议用于传递少量数据，数据传输速度比 TCP 快。UDP 协议在数据传输时不考虑数据包的顺序，它是无连接的不可靠的数据传输，数据包的可靠发送由应用程序负责。传输层接收网络互联层的 IP 数据报，IP 协议根据保存在 IP 数据报头中的协议号决定数据包是传输给 TCP 协议的还是传输给 UDP 协议的。

1.3.4　应用层

应用层是模型中的最高层，应用层中包括经常使用的一些协议，主要有 Telnet(远程登录协议)、FTP(文件传输协议)、SMTP(简单邮件传输协议)、DNS(域名系统)、SNMP(简单网络管理协议)以及 Internet 上的音频和视频传输。Telnet 的特点是终端仿真，使得远程客户机上的用户登录到服务器上，就好像在使用本地计算机一样，直接使用服务器上的资源。FTP 是文件传输协议，用户可以在任何两台使用 FTP 协议的计算机之间“下

载”和“上传”文件。“下载”文件就是将远程服务器中的文件拷贝到自己的计算机上,“上传”文件就是将自己计算机中的文件拷贝到远程服务器上。Internet 上的软件资源非常丰富,用户通过一个支持 FTP 协议的客户端程序连接到远程的 FTP 服务器上发出“下载”或“上传”的服务请求,服务器端的应用程序处理用户所发出的请求,决定是否允许用户进行“下载”或“上传”。SMTP 是简单的邮件传输协议,通过 TCP/IP 网络传输电子邮件(E-mail),并使用约定的 25 端口号。在传输 SMTP 信息之前必须建立一个 TCP 连接。建立连接之后,发送主机标识自己,并在发送者和接收者之间发送源和目标地址。SMTP 不考虑 E-mail 消息的内容。其主要目的是在计算机之间有效和可靠地传输消息。当使用浏览器访问 Internet 的信息资源时,通常是在浏览器的地址栏中输入信息资源所在的主机名字,如输入 www.ft.com 后就可以浏览相关信息了。但是计算机在 Internet 上相互通信时只能够识别如 192.168.1.1 等形式的 IP 地址,无法识别主机名字。DNS(域名系统)目前广泛应用于 Internet 上,它的主要功能就是实现计算机主机名和 IP 地址之间的转换,解决了人们在使用 Internet 时必须记住 IP 地址这些枯燥的数字所带来的不便。DNS 是一个分布式的数据库,通过层次式客户机/服务器分布式数据库管理系统完成它的功能。此外,基于 Internet 视频传输的流媒体应用和业务在国内得到了迅速的发展。视频会议、视频点播、Internet 电视和远程教学等各种应用都在逐步推广。在 Internet 中传输视频的各项技术也得到了越来越多的应用,基于视频传输的宽带流媒体应用将成为未来的 Internet 的主流应用之一。

1.4 Internet 地址

Internet 是全球范围内最大的网络系统,如果网络中的一台主机与任何其他主机进行通信,则需要标识两台需要通信的主机。Internet 网络中,使用地址来标识网络中不同的主机,这个地址就是 IP 地址。

1.4.1 IP 地址

在以 TCP/IP 为通信协议的网络上,每台网络中的主机都有一个唯一的标识地址,也就是 IP 地址。IP 地址是一个用于标识一台 TCP/IP 网络中主机的 32 位二进制数。

1.4.2 IP 地址的表示形式

1. IP 地址的组成

IP 地址用数字标识指定计算机在网络中的位置。每个 IP 地址分为网络地址(网络 ID)和主机地址(主机 ID)两部分,如图 1.3 所示,用来区分 IP 地址的网络号部分和主机号部分。

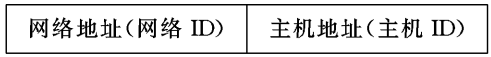

图 1.3 IP 地址的组成

2. IP 地址的格式

IP 地址由 32 位的二进制数组成。IP 地址在表示时通常将每 8 位二进制数分成一组，共四段 8 位二进制数。为了人们在使用时记忆方便，一般将四段 8 位二进制数转换成十进制数来表示，每 8 位二进制转换为相应的十进制数，中间用“.”分隔开，最终以四个十进制数来表示，这种表示方法被称为点分十进制表示法(Dotted decimal notation)，如图 1.4 所示。

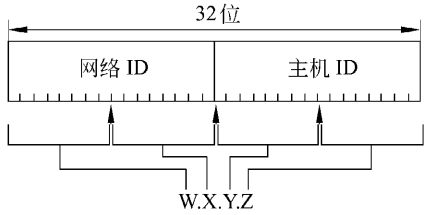

图 1.4　IP 地址格式

为了便于记忆将 IP 地址表示成 W. X. Y. Z 的形式，其中 W、X、Y 和 Z 是 0～255 的十进制数，其中网络号用于标识某个网络，主机号用来标识网络中的某台主机。例如一个十进制表示的 IP 地址转换为二进制的表示形式如下：

128.　　149.　　1.　　5

10000000.　10010101.　00000001.　00000101

1.4.3　IP 地址的分类

由于在 TCP/IP 网络上是利用 IP 地址来标识每一台主机，因此，每一台主机都必须拥有唯一的 IP 地址。为了满足不同规模的网络需求，IP 地址被分为 A 类、B 类、C 类、D 类和 E 类，如图 1.5 所示。

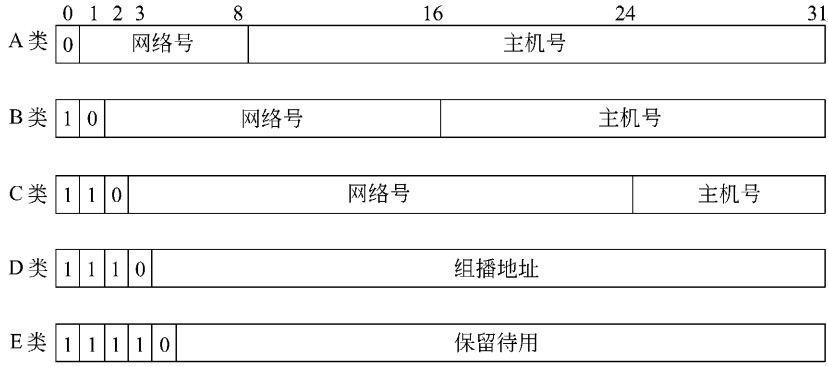

图 1.5　IP 地址分类

区分 IP 地址类别最简单的方法是看第一个 8 位的十进制的数值，A、B、C 这三类地址是网络中常用的 IP 地址。

1. A 类地址

A 类地址的网络号由 32 位 IP 地址的第一个 8 位组成，也就是图 1.4 中的“W”部分。第一个 8 位中最高位的值是“0”，剩下的 7 位是网络号，网络号部分从二进制的全 0 到全 1 的变化范围是 00000000～01111111，转换成十进制后值的范围是 0～127。其中网络号全 0 的部分 0(即 00000000)表示本网络，网络号全 1 的部分 127(即 01111111)保留作为

环回地址，所以 A 类网络的有效地址范围是 1～126。A 类地址中其余的 24 位表示主机号(图 1.4 中的 X.Y.Z 部分)，因此 A 类地址用于主机数目非常多的超大型网络，每个 A 类网络中的主机数可达 16 777 214($2^{24}-2$)台。

2. B 类地址

B 类地址的网络号由 32 位 IP 地址的前两个 8 位组成，也就是图 1.4 中的“W.X”部分。B 类地址第一个 8 位前 2 位的值是“10”，剩下的 14 位组成 B 类地址的网络号。B 类地址网络号部分中第一个 8 位二进制值的变化范围是 10000000～10111111，转换成十进制后值的范围是 128～191。B 类地址的网络数为 16 384(2^{14})个，因为 B 类地址中第一个 8 位的前 2 位的值已经固定为“10”。B 类地址中其余的 16 位表示主机号(图 1.4 中的 Y.Z 部分)，所以每个 B 类网络中的主机数可达 65 534($2^{16}-2$)台，B 类地址通常用于中型到大型的网络。

3. C 类地址

C 类地址的网络号由 32 位 IP 地址的前三个 8 位组成，也就是图 1.4 中的“W.X.Y”部分。其中，第一个 8 位的前 3 位的值是“110”，剩下的 21 位组成 C 类地址的网络号。C 类地址网络号部分中第一个 8 位二进制值的变化范围是 11000000～11011111，转换成十进制后值的范围是 192～223。C 类地址的网络数多达 2 097 152(2^{21})个，因为 C 类地址中第一个 8 位的前 3 位的值已经固定为“110”。C 类地址其余的 8 位表示主机号(图 1.4 中的 Z 部分)，因此，每个 C 类网络最多能有 254($2^{8}-2$)台主机，通常 C 类地址用于小型网络。

4. D 类地址

D 类地址不标识网络，一般用于特殊的用途。D 类地址用于组播，一个组播组可能包括一台或更多主机，或根本没有。组播数据包将传送到网络中选定的主机子集中，只有注册了组播地址的主机才能接收到数据包。D 类网络中，IP 地址第一个 8 位前 4 位的值是 1110，转换为十进制后的范围是 224～239。

5. E 类地址

E 类地址第一个 8 位的前 5 位设置为 11110，它的十进制值的范围是 240～247，专供实验或研究使用。

每类网络的 IP 地址范围见表 1.1。

表 1.1　各类网络的 IP 地址范围

类	第一个 8 位的格式	IP 地址范围	类	第一个 8 位的格式	IP 地址范围
A	0xxxxxxx	1　～126.x.y.z	D	1110xxxx	224～239.x.y.z
B	10xxxxxx	128～191.x.y.z	E	11110xxx	240～247.x.y.z
C	110xxxxx	192～223.x.y.z			

在实际应用中，主要使用的是 A、B、C 类 IP 地址，将 IP 地址分配给主机时需要遵守相应的规范。A、B、C 类 IP 地址的范围及每个网络中的最大主机数如表 1.2 所示。

表 1.2　IP 地址范围及最大主机数

类	IP 地址范围	最大网络数	每个网络中最大主机数
A	1　～126.x.y.z	126(2^7-2)	16 777 214($2^{24}-2$)
B	128～191.x.y.z	16 384(2^{14})	65 534($2^{16}-2$)
C	192～223.x.y.z	2 097 152(2^{21})	254(2^8-2)

1.4.4　特殊的 IP 地址

IP 地址中的网络号和主机号不能全为“0”或“1”。

1. 网络地址

IP 地址中的主机地址位不能是全“0”。当 IP 地址中主机地址的所有位都设置为 0 时，它表示一个网络，而不是网络上的某台特定主机。如 176.10.0.0 表明的是 176.10 这个网络。IP 地址中的主机地址位不能是全“1”，主机地址为全“1”的 IP 地址是广播地址。

2. 主机地址

IP 地址中的网络地址位不能是全“0”。当 IP 地址中的网络地址的所有位都设置为“0”时，它表示本网络的主机。

1.4.5　广播地址

网络上的一台主机向网络中所有的其他主机发送数据包时，即产生了广播。为了使网络上所有设备都能够注意到这样一个广播，TCP/IP 规定了一个可识别和侦听的 IP 地址，也就是 IP 地址的主机号部分都是“1”。广播地址包括直接广播地址和有限广播地址。

1. 直接广播地址

网络中 IP 地址的主机地址部分全为“1”的地址称为直接广播地址。网络中的主机可以利用直接广播地址向任何指定的网络直接发送广播数据包，例如在网络 176.10.0.0 中，向网络上所有的设备发送广播的地址就是 176.10.255.255。

2. 有限广播地址

IP 地址中的所有位都为“1”的地址称为有限广播地址，即 255.255.255.255。有限广播地址主要用于在本网络内广播，主机可以在不知道网络地址的情况下向本网络内的其他主机发送广播数据包。

1.4.6　环回地址

IP 地址中 127.x.x.x 的地址被称做环回地址(loopback address)，常用的环回地址

是 127.0.0.1，它是一个保留地址。这个地址用于对本地主机的网络配置进行测试，使用这个地址提供了对协议堆栈的内部回路测试，因此网络号为 127 的数据包不会出现在网络上。

1.4.7 子网掩码

与 IP 地址一样，子网掩码也是由四个 8 位的 32 位二进制组成。子网掩码的主要功能有两个，一是用来区分一个 IP 地址内的网络号和主机号；二是用来将一个网络化分为多个子网。通过使用掩码，把子网隐藏起来，使外部网络看不见它。子网掩码的格式是与 IP 地址网络号部分和子网号部分相对应的位值为“1”，与 IP 地址主机号部分相对应的位值为“0”。

如果一个网络没有被分成多个子网，则默认的子网掩码值是 A 类网络的子网掩码为 255.0.0.0、B 类网络的子网掩码是 255.255.0.0、C 类网络的子网掩码是 255.255.255.0。

1.4.8 专用 IP 地址

对于在企业内部或家庭中组成的网络，都希望网络中的每台计算机可以连接到 Internet 上。这样，就要求网络中的每台计算机配置一个合法的 IP 地址。如果已有的 IP 地址不能满足每台计算机都拥有一个合法的 IP 地址的要求，就需要考虑使用专用的 IP (Private IP)地址了。在已经介绍的 A、B、C 类 IP 地址中，还有一些只能够在公司内部的 Intranet 上或家庭网络中使用的 IP 地址，这些 IP 地址是内部专用的 IP 地址，无法直接在 Internet 上使用。可以通过防火墙、NAT(Network Address Translation)等设备间接连接到 Internet 上。专用 IP 地址如表 1.3 所示。

表 1.3 专用 IP 地址

IP 地址	子网掩码	IP 地址	子网掩码
10.0.0.0～10.255.255.255	255.0.0.0	172.16.0.0～172.31.255.255	255.255.0.0
169.254.0.0～169.254.255.255	255.255.0.0	192.168.0.0～192.168.255.255	255.255.255.0

在企业或家庭内部网络使用专用 IP 地址之后，外界的 Internet 只能看到防火墙或 NAT 设备的公用 IP 地址，看不到在公司内部所使用的专用 IP 地址。

1.4.9 自动专用 IP 地址

在为 Windows 2000 的计算机配置 IP 地址时，有一个选项是“自动获得 IP 地址”。设置这个选项后，Windows 2000 的计算机需要从网络中的 DHCP 服务器中获取 IP 地址。如果计算机经过反复请求 IP 地址后，无法从 DHCP 服务器得到一个 IP 地址，则 Windows 2000 的计算机会自动产生一个格式为 169.254.x.y 的专用 IP 地址，并在网络中使用这个 IP 地址。169.254.0.0～169.254.255.255 是为自动专用 IP(Automatic Private IP)寻址分配的专用地址。

Windows 2000 的计算机在开始使用自动专用 IP 地址之前，先发送一个广播信息给网络上的其他计算机，以便检查是否有其他的计算机在使用这个 IP 地址。如果其他的计算机没有响应信息，那么 Windows 2000 的计算机就将该 IP 地址分配给自己使用。在获得一个自动专用 IP 地址之后，Windows 2000 的计算机会继续查找网络中的 DHCP 服务器，如果从 DHCP 服务器得到了一个 IP 地址，则 Windows 2000 的计算机开始使用 DHCP 服务器分配的 IP 地址。

1.5 Internet 应用

随着 Internet 网络的不断发展壮大，它的各种应用服务越来越广泛，人们利用 Internet 这一先进的信息武器来为各行各业服务。据美国的专业统计数据，截至到 2006 年 10 月底，全球互联网网站数量已经突破 1 亿，网站数量的增加速度达到历史最快水平。Internet 已经在电子商务、远程教育、网上娱乐、即时通信、博客及信息共享等应用领域，对人类的生活产生了重大的影响。

电子商务是用户使用全球联网的 Internet 环境，任意搜索联网商家和厂家的产品，在挑选到适合的产品后向生产厂家或商家直接购买，由网络经银行直接转账付款或者是货到付款。也可以通过网络和自己认为合适的厂家进行交流，将自己的需求告诉生产厂家，进行产品定制。也就是电子商务利用互联网进行商务活动，它将顾客、销售商、供货商和雇员联系在一起。

虚拟医院是指通过互联网提供求医、电子挂号、预约门诊、预定病房、专家答疑、远程会诊、远程医务会议和新技术交流演示等服务。病人在家中通过网络就可以得到医疗救助，医生能通过网络迅速得到病人的全部病史资料从而确诊病情对症治疗。地处偏远地区的病人也可以通过网络得到著名医院的著名专家的诊断和治疗，同时普通医院在虚拟医院的帮助下，医疗水平也会得到提高。虚拟医院的形式主要表现为数字化医院、远程医疗、网上会诊以及虚拟手术等。

Internet 远程教育是指跨越地理空间进行的教育活动，主要包括授课、讨论和实习等各种教育活动，Internet 的普及和发展极大地方便了人们通过远程教育的形式自主学习各种知识和技能。远程教育的出现克服了传统教育在空间、时间、受教育者年龄和教育环境等方面的限制，满足了社会对学习文化的需求，使得网络时代的教育变得更加人性化和多样化。

随着人们生活水平的提高，各种各样的娱乐活动层出不穷，网上娱乐是互联网上一种被迅速传播的娱乐方式。网上娱乐的表现形式主要包括网络游戏、网络视频点播、网上音乐和网上聊天等。

即时通信是指互联网络用户利用计算机、手机等不同终端，及即时通信软件实时地传递文字、语音和视频等信息的一种通信方式。随着互联网应用的飞速发展，使用即时通信的用户数量也在不断的增长。即时通信的应用包括娱乐、办公和电子商务等，目前常用的即时通信软件主要有腾讯 QQ、网易泡泡、微软的 MSN 以及阿里巴巴的淘宝旺旺和贸易

通等。

博客(Blog)是 Web log 的简称,也就是网络日志。一个 Blog 就是一个网页,它通常是由简短且经常更新的张贴文章所构成,这些文章都按照年月日的顺序排列的。Blog 的内容和目的有很大的不同,有从其他网站连接过来的超级链接和评论;有关公司、个人和构想的新闻;有旅游爱好者的游记;有个人对生活的感受;有对事物的评论等包罗万象。事实上 Blog 是人们通过互联网的心灵互动工具,www. blogger. com 是比较有名的博客网站。

1.6 Internet 安全

随着 Internet 技术和应用的快速发展,Internet 已经对商业、工业、银行、财政、教育、政府和娱乐及人们的工作和生活产生了巨大和深远的影响。许多传统的信息和数据库系统正在被移植到互联网上,电子商务迅速增长,早已超过了国界。但是,互联网的不安全因素也越来越多,比如黑客、病毒、操作系统漏洞和应用软件的漏洞等,所有这些都为 Internet 的用户带来了极大的威胁,也极大地挫伤了部分用户对 Internet 应用的积极性。因此,互联网的安全也就变得越来越重要了,如何增强互联网络应用中的安全性已经成为人们在网络应用中所面临的重要问题,网络应用中的安全防范意识已深入人心。

1.6.1 Internet 网络面临的安全威胁

由于 Internet 网络是全球开放型的网络,没有管理和监控机构,因此经常会受到以下一些安全威胁。

黑客(Hacker)会经常入侵 Internet 网络中的计算机系统,破坏重要数据、窃取机密文件、更改网站主页,以及夺取系统管理员的权限等破坏系统功能,甚至导致整个系统的瘫痪。

Internet 网络上的数据传输所基于的通信协议本身无法保证数据在网络上传输的安全性,数据在网络上传输的过程中有可能被窃取。Internet 网络上的计算机操作系统本身的漏洞和缺陷为网络的不安全运行埋下了隐患。

网络中传输的数据信息有可能被假冒和伪造,也就是数据信息的来源和去向是否真实,内容是否被改动,以及是否泄露等。

计算机病毒通过 Internet 网络的传播给网络用户带来了极大的威胁,已经成为一个重要的问题。病毒可以使计算机和计算机网络系统瘫痪、数据和文件丢失,病毒可以通过多种途径和形式在网络上传播。需要采用专门的监控系统、查毒和杀毒工具来检测和清除病毒入侵系统所带来的危害,并防止病毒的再入侵。最近,赛门铁克(Symantec)公司又提出了病毒与黑客程序相结合的混合威胁新型安全概念,它通过多种途径和技术潜入企业的网络,同时具有蠕虫、特洛伊木马、恶意代码以及黑客特点,并且还具有持续发作的特点。混合威胁的发现说明病毒编写者正在利用大量的系统漏洞将病毒传播的速度最大化。

1. 黑客

黑客的普遍含义是计算机系统的非法入侵者。20 世纪 70 年代的美国麻省理工学院实验室里聚集了大批的高素质人才，他们精通计算机科学及相关的学科，具备了良好的科学素质，这些人在实验室中经常研究或开发出许多新的具有开创意义的产品或技术，黑客也起源于这里。这些人以进入他人防范严密的计算机系统为生活的一大乐趣，并以此来评定自身的价值并逐渐形成了一种独特的文化，即黑客文化。真正的黑客文化是创造与进攻，不停地创造和证明自己，但绝不轻易的破坏是真正黑客永恒的准则。

黑客是如何对计算机进行入侵和破坏的呢？黑客入侵计算机的主要方式有木马入侵、IPC$ 共享入侵、IIS 的漏洞入侵以及网页恶意代码入侵等多种途径。下面对黑客常用的一些攻击方式进行简单的介绍。

(1) 木马入侵

木马入侵是广大用户最深恶痛绝的一种入侵方式，很多用户感觉它很神秘、很深奥，事实上随着木马程序的智能化技术越来越高，很多黑客都能轻松的达到攻击目的。通过在计算机中种植木马、使用木马和隐藏木马的途径达到攻击的目的。

一个完整的“木马”程序包含“服务器”和“控制器”两部分。种植到被入侵计算机的是“服务器”部分，黑客是利用“控制器”进入到被种植了木马程序的计算机中，任意毁坏、窃取被种植者的文件，甚至远程控制被种植的计算机。被种植到受害者计算机中的木马程序具有很强的隐蔽性，用户很难发现它的存在。木马入侵通常利用操作系统或者应用软件的漏洞进入到受害者的计算机，或者通过发送 E-mail 将木马程序的服务器端作为附件发送给受害者，受害者在接收邮件时在毫无防范的情况下，下载了木马程序的服务器端并运行服务端程序，成功实现了木马的种植。例如，攻击者在向被攻击者发送电子邮件时，将木马的服务器端程序伪装成正常的文件夹带在邮件的附件中，一旦邮件的接收者将邮件附件中的文件下载，并且运行所下载的文件后，重新启动计算机系统，木马程序的服务器端就种植成功了。攻击者成功将木马的服务器端植入受害者的计算机后，需要耐心等待受害者的服务器端连线，当受害者的计算机联网后，攻击者就可以利用控制器端对服务器端进行远程控制。通过远程控制，攻击者可以对受害者计算机中的文件进行下载、新建、重命名和删除等操作，还可以使用鼠标的拖放功能，将文件或文件夹拖放到目标文件夹中；可以查看、刷新和关闭受害者计算机的进程，一旦发现受害者的计算机中有杀毒软件或者防火墙，就关闭杀毒软件或者防火墙的进程，以便保护服务器端程序的运行；可以对受害者计算机窗口中的程序进行最大化、最小化和正常关闭等操作；如果受害者的计算机安装有 USB 摄像头，还可以获取图像，并将捕获的图像保存为媒体播放机可以直接播放的文件；此外，还可以记录键盘的操作、启动或关闭受害者的计算机、远程卸载、抓屏查看密码等功能。木马程序为了长期种植在受害者的计算机中不被发现，常常采用多种方式隐藏自己。例如，对服务器端程序自动进行压缩隐藏；利用文件捆绑器把木马服务器端和正常的文件捆绑在一起，达到欺骗目的；通过使用压缩 EXE 和 DLL 文件的压缩软件对服务端进行加壳保护，让杀毒软件无法识别等手段，以便长时间躲过杀毒软件的查杀。

防止木马入侵的重要方法是防范，在计算机还没有被种植木马之前，通过安装杀毒软

件、网络防火墙，更新病毒库、更新系统的安全补丁、定时备份硬盘上的文件、不要运行来路不明的软件和打开来路不明的邮件等方法防范木马对自己所使用计算机的攻击。

(2) IPC$共享入侵

IPC$(Internet Process Connection)是为了进程间通信而开放的命名管道，连接的计算机通过提供可信任的用户名和密码，建立一个安全通信通道，通过所建立的通道进行加密数据的交换，从而实现对远程计算机的管理和查看远程计算机的共享资源。IPC$是Windows NT系统架构的功能，在同一时间两个IP之间允许建立一个连接，并且系统还打开了默认共享，这种功能为系统管理员的管理带来了极大的方便，但是也降低了系统的安全性。在IPC$共享打开的情况下，攻击者利用IPC$不需要用户名和密码就可以与目标主机建立一个空的连接，通过这个空连接攻击者还可能得到目标主机上的用户列表。

IPC$共享入侵的方法是通过猜测或破解的方法得到系统管理员的账户与密码，如果系统管理员的密码设置的位数比较短又简单，则很容易被破解。使用命令建立IPC$连接，然后将木马程序的服务器端复制到系统目录下，用相应命令查看被植入木马程序计算机的操作系统的时间，最后在指定的时间运行木马程序的服务器端，这样计算机就完全被黑客控制了。避免IPC$共享入侵的最基本的方法是给管理员账户加上强壮的口令。

(3) IIS的漏洞入侵

IIS(Internet Information Server)是微软公司的Web服务器组件，用于实现Web服务器的功能。由于Windows操作系统的普及率较高，利用IIS搭建Web服务器和FTP服务器的用户比较多，因此较容易成为黑客攻击的目标。目前所发现的IIS漏洞非常容易受到入侵者的攻击，攻击者可以轻松修改网站的默认主页，甚至删除硬盘上的数据，有些攻击者还可以轻松获取系统管理员的权限，对系统造成了极大的威胁和破坏。

IIS的漏洞入侵方法一般是攻击者利用专用的工具完成攻击。例如攻击者首先搜索网络上带有漏洞计算机的IP地址，利用所搜索到的漏洞计算机的IP地址，使用专用工具进行攻击。如果显示攻击成功，再输入相应的命令进入到被攻击服务器的系统目录中，建立一个具有系统管理员权限的用户账号，通过建立IPC$连接进行非法入侵。入侵者利用系统漏洞修改Web服务器的主页、删除硬盘上的数据以及建立代理服务器等，给服务器造成极大的危害。利用IIS漏洞攻击的最著名案例是发生在2001年7月16日的红色警戒(CodeRed)的爆发，攻击者利用IIS的漏洞攻击微软的IIS服务器，并产生拒绝服务(Denial of Service，DoS)，造成全球36万台电脑瘫痪，给全球的互联网用户带来了重大的灾难。

解决IIS漏洞攻击的一个最好的办法是密切关注微软公司的官方站点，及时将公司发布的IIS漏洞补丁安装到计算机中。

(4) 网页恶意代码入侵

用户在浏览网页时有时会发现自己浏览器的标题栏、默认的主页被修改为其他的页面、鼠标右键的菜单被修改，更严重的会发现系统被禁止使用、硬盘被格式化等，这种情况绝大部分是网页恶意代码入侵的结果。网页恶意代码(网页病毒)是利用网页来进行破坏的病毒，它是使用脚本语言编写的一些恶意代码对浏览器的漏洞进行攻击。一旦用户登录到某些含有网页恶意代码的网站时，这些恶意代码就会被激活，激活后的恶意代码通过

修改浏览者的注册表达到破坏系统的目的。

预防网页恶意代码入侵的方法主要有经常备份系统的注册表、安装具有注册表实时监控功能的防护软件、不要轻易去不太了解的网站、将浏览器的 Internet 区域的安全级别设置为高级以及在浏览器的设置中过滤不良站点等方法，这样可以极大的提高网络访问的安全性。

2. 病毒

病毒是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。随着网络的产生与发展，计算机病毒快速地在网络上传播，为网络带来了灾难性的后果。计算机病毒给用户带来了极大的危害，破坏计算机中的文件或数据造成数据的丢失或毁损，病毒抢占系统和网络的资源致使系统瘫痪或网络阻塞，破坏操作系统软件或应用软件造成计算机无法启动和使用，更严重的还会损坏计算机硬件系统。

(1) 网络病毒的传播方式

网络计算机病毒是在网络上传播并对网络造成严重危害的病毒，网络病毒的来源主要有从网络上下载文件、Internet 上 Java 和 ActiveX 的恶意小程序、接收电子邮件等都可能存在病毒。从网络上下载的文件通常是被压缩的文件，一旦将这些文件解压缩并运行，病毒随之传播和释放。有些恶意站点可能会通过将 Java 小程序植入网页中达到窃取用户个人隐私的目的，例如网页上有的 Java 小程序可以窃取用户的密码。有些 ActiveX 控件对计算机存在着很大的潜在威胁，能够破坏系统软件和磁盘中的数据，例如 Windows 媒体播放器 9 系列中包含着一个网页制作人员可以制作允许播放媒体网页的 ActiveX 控件，并在播放时提供用户界面控制播放，也就是当用户访问内嵌有媒体的网页时，ActiveX 控件将提供用户采取诸如暂停、播放、回退等控制操作的界面。但该控件在提供访问用户计算机信息的功能上存在缺陷，恶意攻击者可以通过脚本文件调用该控件，使得攻击者可以查看并操作用户计算机媒体库中的源数据，可能造成攻击者对用户磁盘中数据的破坏。另一种主要威胁是电子邮件病毒，它是利用电子邮件方式作为传播途径的计算机病毒，实际上该类病毒和普通病毒一样，只不过是传染方式改变而已。电子邮件病毒主要是通过邮件附件中夹带的. exe 文件进行传播的，例如 Navidad. exe、happy99. exe 和 Prettypark. exe，如果收到的邮件的附件是这些文件请不要运行，直接删掉该文件。有些是在 Word 文件中会潜伏宏病毒，因此对 Word 文件形式的附件，打开时也要小心。

(2) 网络病毒的防范措施

网络时代的病毒传播手段多样，病毒杀伤力更强，由病毒引发的经济损失也会更大。面对随时可能出现的更加智能化的病毒，简单的防毒和查杀病毒功能已经不能满足用户的安全需要。因此，使用综合性的防范措施，才能不断提高网络的安全性，较好的解决网络病毒带来的危害。对于网络病毒的防范措施主要包括预防、查毒、杀毒、及时扩充病毒库、数据修复和数据备份。

为了预防计算机不会感染病毒，首先需要做的就是安装防护软件，现在的防护软件主要有互联网网络防火墙、病毒实时监测和邮件实时监测。互联网防火墙用于防范黑客入

侵，监视来自局域网内部和互联网上黑客的非法扫描，阻止黑客、木马程序和恶意代码入侵，监视上网安全。病毒实时监测软件可以实时监测和防范病毒入侵，实时防范来自软盘、光盘、局域网以及互联网中已知的几万种病毒。邮件实时监测软件用于实时监控和防范邮件病毒的入侵，实时监视来往各种电子邮件，遇病毒及时报警，拦截电子邮件病毒于系统之外。其次是查毒和杀毒，查毒杀毒软件可以彻底查杀各种电子邮件病毒、各种E-mail邮箱压缩格式病毒、常见的ZIP、ARJ、RAR、CAB、LZH等十多种压缩带毒文件、查杀可执行文件的压缩格式、宏病毒、网络蠕虫病毒、黑客工具、木马程序、网络炸弹、恶意代码和网页病毒等多种病毒。第三是要及时更新查杀病毒软件的病毒库，网络上的病毒每天都在不断的更新和变化，对于这些变化生产查毒、杀毒软件的公司每天都在不断更新自己产品的病毒库，以便应对不断出现的各种形式的病毒，保证用户查杀到最新的病毒。因此，网络用户要随时更新自己的病毒库，以防漏查和漏杀最新的病毒。第四，为了保证自己的重要数据的安全，用户需要及时不断的对重要数据进行备份，这样即便计算机被病毒感染且数据被破坏，也可以使用已备份的数据，将自己的损失降到最低。另外，对于电子邮件类的病毒在使用时需注意不要轻易打开附件中的文件和不要轻易执行附件中的*.EXE、*.COM、.PIF、.BAT、SCR等文件。

目前国内外的查杀毒软件主要有江民、金辰、瑞星、赛门特克和avast等产品，用户可以根据自己的具体情况选择安装一种，以保证自己系统的安全。

1.6.2 网络安全的防护措施

一个安全的计算机网络应该具有可靠性、可用性、完整性、保密性和真实性等特点。计算机网络不仅要保护计算机网络设备安全和计算机网络系统安全，还要保护数据安全等。因此针对计算机网络本身可能存在的安全问题，实施网络安全保护方案以确保计算机网络自身的安全性是每一个计算机网络都要认真对待的一个重要问题。网络安全防范的重点主要包括计算机病毒和黑客入侵。保证网络安全的主要技术有网络防火墙技术、入侵检测技术、加密技术、虚拟专用网技术和安全隔离。本节简单介绍网络防火墙技术和入侵检测技术。

1. 防火墙技术

网络防火墙技术是一种用来将内部网络与外部网络或Internet相互隔离，以便保护内部网络或内部主机的技术。网络防火墙加强了网络之间的访问控制，防止外部网络用户以非法手段进入内部网络，访问内部网络资源。功能简单的网络防火墙可以由路由器及一台计算机来充当，复杂网络防火墙需要购买专用的硬件或软件防火墙来实现。网络防火墙对两个或多个网络之间传输的数据包按照一定的安全策略来进行检查，然后决定网络之间的数据通信是否被允许同时监视网络的运行状态。

防火墙的功能包括过滤掉网络上不安全的服务请求、控制非法用户进入到网络中、控制用户对特殊站点的访问、监视Internet安全以及使防火墙具有病毒防护功能。防火墙的优势主要包括，严密的实时监控对所有来自外部机器的访问请求进行过滤，发现非授权的访问请求后立即拒绝，随时保护用户系统的信息安全。灵活的安全规则设置了一系列

安全规则，允许特定主机的相应服务，拒绝其他主机的访问要求。用户还可以根据自己的实际情况，添加、删除和修改安全规则，保护本机安全。应用程序规则设置可以对应用程序数据包进行底层分析拦截功能，控制应用程序发送和接收数据包的类型、通信端口，并且决定拦截还是通过。详细的访问记录显示所有被拦截的访问记录，包括访问的时间、来源、类型和代码等都详细地记录下来，可以清楚地看到是否有入侵者想连接到你的机器，从而制定更有效的防护规则。完善的报警系统设置了完善的声音报警系统，当出现异常情况的时候，系统会发出预警信号，从而让用户作好防御措施。具有病毒防护功能的防火墙被称为“病毒防火墙”，这种防火墙大多是纯软件的，因此主要应用在个人防火墙中，较容易实现。病毒防火墙可以有效地防止病毒在网络中的传播，可以大大减少损失。但防火墙不是万能的，防火墙无法阻止任何绕过防火墙的攻击。如防火墙不限制从内部网络到外部网络的连接，则防火墙内部用户可能会直接连接到 Internet 上从而绕过防火墙形成一个潜在的后门，当防火墙外部用户连接到内部用户的计算机后，可以发起绕过防火墙的不受限制的攻击。多数防火墙不能拦截带病毒的数据在网络之间传播。防火墙也无法阻止数据驱动式的攻击。因此，网络安全不能过分依赖防火墙。

目前应用的防火墙根据采用的技术类型不同主要分为包过滤型、网络地址转换(NAT)、代理型和监测型。包过滤型防火墙根据网络中传输的数据被分割成数据包，防火墙通过读取数据包中的地址信息来判断这些数据包是否来自可信任的安全站点，如果发现数据包来自危险站点，防火墙会拒绝让这些数据通过。网络地址转换型防火墙是把内部网络的私有 IP 地址转换成标准 IP 地址，允许具有私有 IP 地址的内部网络访问因特网。内部网络在访问外部网络时会产生一个映射记录，隐藏真实的内部网络地址，这样防火墙根据预先定义好的映射规则来判断访问是否安全，如果符合规则防火墙认为访问是安全的，当不符合规则时防火墙认为访问是不安全的，不接受该访问。代理型防火墙通常被称为代理服务器，它位于客户机与服务器之间阻挡二者间的数据传输。当客户机需要使用服务器上的数据时向代理服务器发送请求信息，代理服务器再向服务器发送数据请求，然后再由代理服务器将服务器返回的结果传输给客户机。这种类型的防火墙由于外部系统与内部服务器之间没有直接的数据通道，因此恶意攻击很难进入到内部网络系统。监测型防火墙能够对模型中的各层数据进行主动的、实时的监测，在对所监测的数据进行分析后能够有效地判断出每一层的非法入侵。

2. 入侵检测技术

随着计算机网络技术的不断发展，网络安全的风险也越来越大。入侵检测技术(IDS)是主动保护自己免受攻击的一种网络安全技术。入侵检测技术对计算机网络或计算机系统中的多个关键点进行信息收集并对所收集到的信息进行分析，从而发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。在入侵检测技术出现之前，防火墙是网络安全最主要的防范手段，但是它已经不能满足人们对网络安全的需求。入侵检测技术是对防火墙的合理补充，能够帮助网络系统快速发现攻击的产生，扩展了系统管理员的安全管理能力。入侵监测系统位于防火墙的后方，能够对网络活动进行实时检测，监视和记录网络流量，一个配置合理的入侵监测系统会在网络活动中发出许多报警。

入侵检测系统的主要功能有监视并分析用户和系统的活动、对系统配置和漏洞进行监测、评估系统关键资源和数据文件的完整性、能够识别已知的攻击行为、统计和分析系统的异常行为、操作系统的日志管理和识别违反安全策略用户的活动。入侵检测系统一般分为主机型和网络型。主机型入侵检测系统通常以系统日志和应用程序日志等作为数据源，从所在的主机收集信息并进行分析，主机型入侵检测系统一般保护的是所在的系统。网络型入侵检测系统的数据源是网络上的数据包，通过监听本网络内所有的数据包，然后进行分析判断，网络型入侵检测系统通常负责保护网络的任务。因此，网络型入侵检测系统一般在网络上安装入侵检测系统便可以监测整个网络。主机型入侵检测系统必须为不同的操作系统平台开发不同的检测程序，并且在运行时会增加系统的负荷，但能够有效的利用操作系统本身提供的功能以及结合异常分析，得到更准确的攻击行为报告。

入侵检测系统的核心功能是对各种事件进行分析，从分析结果中发现违反安全策略的行为。入侵检测技术可分为实时入侵检测和事后入侵检测两种。实时入侵检测是一个往复循环的过程，在网络连接过程中系统根据用户的历史行为模型、存储在计算机中的专家知识以及神经网络模型对用户当前的操作进行判断，一旦发现入侵迹象立即断开入侵者与主机的连接，并收集证据和实施数据恢复。事后入侵检测是非实时的检测系统，由网络管理员依据自身掌握的网络安全知识，根据计算机系统对用户操作所做的历史审计记录判断用户是否具有入侵行为，如果发现异常行为就断开网络连接，并记录入侵证据进行数据恢复。

入侵者为什么能够进入系统呢？主要原因包括无论是服务器程序、客户端软件还是操作系统在软件编写时都存在漏洞(bug)；操作系统在安装完成后，通常都有默认的安全配置信息，这些默认的系统配置信息被攻击者利用；设置的口令太简单，攻击者不费吹灰之力就可破解造成口令被盗；由于有些网络的结构便于攻击者在网络上放置一个嗅探器就可以查看该网络上的通信数据，造成明文通信信息很容易被监听；另外就是网络协议本身在初始设计时的缺陷等。所以功能强大的入侵检测软件可以帮助网络管理员及时发现和修补网络中的安全漏洞，保证网络系统的正常运行。

习题

1. 什么是计算机网络？
2. 简述 IP 地址的组成及其格式。
3. IP 地址分几类？
4. 什么是网络地址，什么是主机地址？
5. 广播地址有几种类型？
6. 写出专用 IP 地址的范围。
7. Internet 网络面临的安全威胁有哪些？
8. 黑客常用的攻击方式有哪些？
9. 什么是入侵检测技术？
10. 入侵检测系统有几种？

第2章

Internet 的接入方式

用户希望访问 Internet 的资源，首先要将计算机连接到 Internet 上。目前常见的接入 Internet 的方式主要有拨号接入方式(PSTN)、综合业务数字网(ISDN)、数字数据专线(DDN)、非对称数字用户环路(ADSL)、甚高速数字用户环路(VDSL)、光纤接入、无线接入、线缆调制解调器(cable-modem)以及通过局域网接入 Internet 方式可供选择，本章主要介绍几种常用的接入 Internet 的方式。

2.1 拨号接入方式连接到 Internet

拨号接入方式(PSTN，公共电话网)的连接比较简单，费用低廉，用户只需要一台计算机，在安装、配置了调制解调器等连接设备后，就可通过普通的电话线和一个账号就可以接入 Internet。它的缺点是传输速度慢，线路可靠性差，适合于没有条件安装宽带的场合及临时用户使用。下面以 Windows 98 操作系统为例介绍拨号接入 Internet 的连接方法。Windows 98 操作系统设置拨号接入连接需要添加网络客户和 TCP/IP 协议、安装和配置调制解调器、申请一个上网账号以及通过拨号连接到 Internet。

2.1.1 添加网络客户和 TCP/IP 协议

1. 添加网络客户

双击 Windows 98 桌面上的【我的电脑】图标，在打开的窗口中双击【控制面板】图标，Windows 系统的设置都在控制面板中完成。网络客户的设置在控制面板中双击【网络】图标，弹出【网络】对话框如图 2.1 所示，在【网络】对话框中添加网络客户。

单击【添加】按钮，弹出【请选择网络组件类型】对话框如图 2.2 所示。在该对话框中可以添加客户、适配器、协议和服务，这里选择添加客户。

单击图 2.2 中的【添加】按钮，弹出【选择 网络客户机】对话框如图 2.3 所示，在该对话框的【厂商】选择框中选中 Microsoft 项，在【网络客户】选择框中选中【Microsoft 网络用户】，单击【确定】按钮返回【网络】对话框。

Windows 98 网络对话框的【配置】选项卡中，显示所添加的 Microsoft 网络用户。

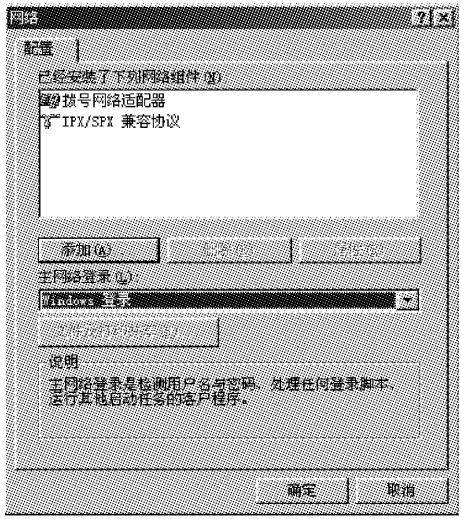

图 2.1　添加网络客户

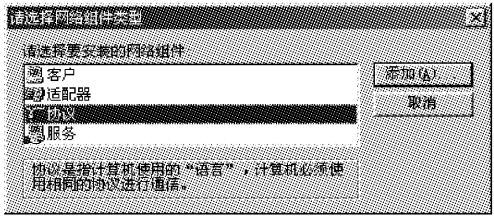

图 2.2　选择网络组件类型

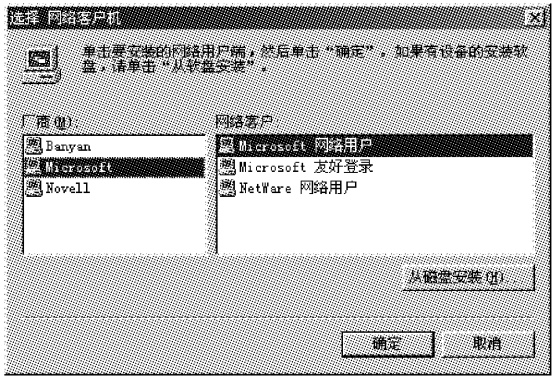

图 2.3　选择网络客户机

2. 添加 TCP/IP 网络协议

TCP/IP 协议是连接 Internet 的重要协议，在连接到 Internet 之前需要添加和配置 TCP/IP 协议。

在图 2.2 的【请选择网络组件类型】对话框中，选择添加协议。单击【添加】按钮，弹出