高职高专计算机专业系列教材

计 算 机 网 络 安 全 与 应 用 技 术

袁家政　编著

清 华 大 学 出 版 社

(京)新登字 158 号

内 容 简 介

本书是一本面向高职高专和成人高等教育的教材,是作者长期从事计算机网络教学和网络设计的经验总结。

本书主要从网络安全的基本知识、密码技术、防火墙技术、Windows 98/ NT/ 2000 系统的安全、黑客技术与防范措施、网络防毒技术、Internet/ Intranet 的安全性和实训等几个方面编写,全书共 9 章。

本书突出计算机网络安全的管理、配置及维护的操作,紧紧跟踪网络安全的最新成果和发展方向。书中提供大量网络安全与对抗的实例,并从实例中引出概念,然后进行归纳总结,帮助读者掌握计算机网络安全的基本原理,了解计算机现有系统的安全设置、安全漏洞,从而胜任一般系统的安全设计及管理维护工作。

本书适合于广大在校学生学习,也可供有关工程技术人员阅读。

图书在版编目(CIP)数据

计算机网络安全与应用技术/ 袁家政编著 .—北京:清华大学出版社,2002
高职高专计算机专业系列教材
ISBN 7-302-05636-6

Ⅰ.计… Ⅱ.袁… Ⅲ.计算机网络-安全技术-高等学校:技术学校-教材
Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字(2002)第 045426 号

出 版 者:清华大学出版社(北京清华大学学研大厦,邮编 100084)
http:// www.tup.tsinghua.edu.cn
责任编辑:徐跃进
印 刷 者:北京市人民文学印刷厂
发 行 者:新华书店总店北京发行所
开 本:787×1092 1/ 16 印张:24.25 字数:559 千字
版 次:2002 年 8 月第 1 版 2002 年 8 月第 1 次印刷
书 号:ISBN 7-302-05636-6/ TP·3322
印 数:0001～8000
定 价:30.00 元

第 1 章 计算机网络安全的基础知识

随着计算机技术的飞速发展,信息和网络已经成为社会发展的重要保证。信息与网络涉及到国家的政府、军事、文教等诸多领域,在计算机网络中存储、传输和处理的信息有许多是政府宏观调控决策、商业经济信息、银行资金转账、股票证券、能源资源数据、科研数据等重要信息,其中有很多是敏感信息甚至是国家机密,所以难免会吸引来自世界各地的各种人为攻击(例如,信息泄漏、信息窃取、数据删除与添加、计算机病毒等)。因此计算机网络安全是一个关系国家安全和主权、社会的稳定、民族文化的继承和发扬的重要问题,其重要性正随着全球信息化步伐的加快而变得越来越重要。

计算机网络安全主要涉及网络信息的安全和网络系统本身的安全。在计算机网络中存在着各种资源设施,随时存储和传输的大量数据;这些设施可能遭到攻击和破坏,数据在存储和传输过程中可能被盗用、暴露或篡改。另外,计算机网络本身可能存在某些不完善之处,网络软件也有可能遭受恶意程序的攻击而使整个网络陷于瘫痪。同时网络实体还要经受诸如水灾、火灾、地震、电磁辐射等方面的考验。

本章介绍计算机网络安全的基本知识,主要包括以下内容:

计算机网络基础知识;

计算机网络存在的安全问题;

网络安全的体系结构;

网络安全技术;

网络安全的策略及实现;

计算机网络安全立法;

计算机网络安全的发展方向。

1.1 计算机网络基础知识

为了更好地学习网络安全知识,掌握网络的攻防策略,学习一些相关的计算机网络基础知识是非常必要的。

1.1.1 计算机网络体系结构

1.计算机网络

计算机网络,可以用一句简单的话概括:“通过通信线路连接起来的自治的计算机集合”。这句话包括以下3个方面的含义。

(1) 必须有两台或两台以上的具有独立功能的计算机系统相互连接起来,以达到共享资源为目的,才能构成网络。这里所指的两台计算机系统的位置要有一定的距离,且每个计算机系统能够独立地工作,能够自行处理数据,而无需其他系统的帮助。例如:具有通信功能的单机系统(即一台主机连接多个终端的系统),因为只有一台主机,就不属于网络。并行机虽然有多个处理器,但它不属于两个具有独立功能的计算机系统互连在一起,因此也不属于网络。

(2) 两台或两台以上的计算机连接,互相通信交换信息,必须有一条通道。这条通道的连接是物理的,由物理介质和通信设备实现。它们可以是铜线、光缆等“有线”介质,也可以是微波、红外线或卫星等“无线”介质。

(3) 计算机系统之间交换信息,必须有某种约定和规则,这就是协议。这些协议可以由硬件或软件来完成。

综合以上3个方面的内容,可以把计算机网络归纳为:把分布在不同地点且具有独立功能的多个计算机系统通过通信设备和线路连接起来,在功能完善的网络软件和协议的管理下,以实现网络中资源共享为目标的系统。

2.计算机网络协议

在计算机网络中不同系统的两个实体之间只有在通信的基础上,才有可能相互交换信息,并共享网络资源。一般来说,实体是能发送和接收信息的任何东西,可以指用户应用程序、文件传送包、数据库管理系统、电子邮件设备和终端等。系统可包含一个或多个实体(如主机和终端等)。两个实体之间若要能通信,就必须能够相互理解,共同遵守有关实体的某种互相能接受的规则。这些规则的集合称为协议。因此协议可被定义为实体之间控制数据交换的规则的集合。简单说,协议就是通信双方的约定。一个网络协议主要由以下3个要素组成。

(1) 语法:即数据与控制信息的结构或格式;

(2) 语义:即需要发出何种控制信息,完成何种动作以及做出何种应答;

(3) 同步:即实体通信实现顺序的详细说明。

由此可见,网络协议是计算机网络不可缺少的组成部分。

3.通信子网及子网信道类型

计算机网络主要由计算机系统(包括计算机和终端)、网络节点(通信处理机)和通信链路(通信线路和网络设备)等网络单元组成。从功能上可以将计算机网络分为资源子网和通信子网,网络上的每一个连接称为节点,节点有两类:一类是转接节点,主要承担通信

子网的信　传输和转接的作用;另一类是访问节点,是资源子网中的计算机或终端,主要是信息资源的来源和发送信息的目的地。

不同类型的网络,其通信子网的物理组成各不相同。局域网最简单,它的通信子网由物理传媒介质和主机网络接板(网卡)组成。而广域网,除物理传媒介质和主机网络接板(网卡)外,必须靠通信子网的转接节点传递信息。

对于通信子网的设计,如果从通信信道类型分类有两种类型:点对点通信方式和广播式通信子网。

(1) 点对点通信,如图 1-1 所示。在该种类型网中,任何一段物理链路,都惟一连接一对节点。如果不在同一段物理链路的一对节点中通信,必须通过其他节点转接。采用点对点通信的基本拓扑结构有:星形、树形、环形及不规则形和全部互连等。

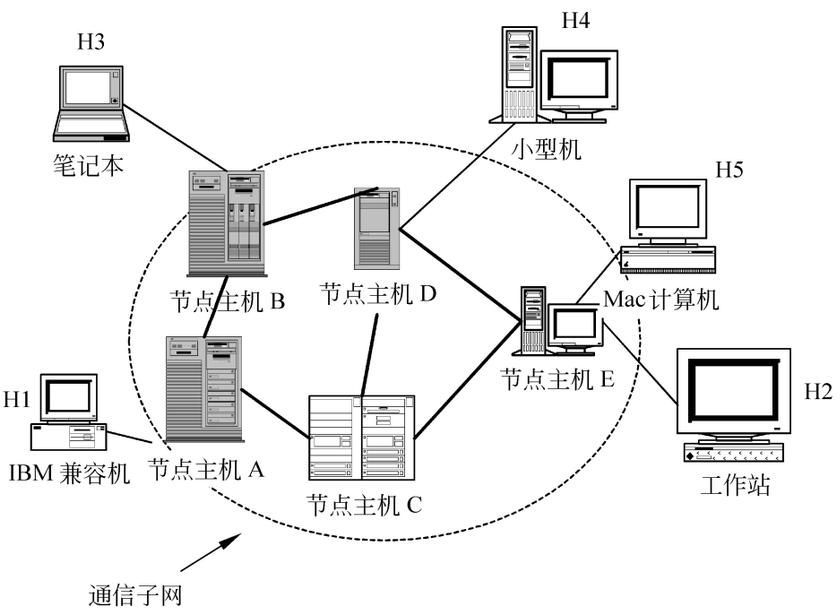

图 1-1　点对点通信方式

(2) 广播式通信,如图 1-2 所示。在该种通信子网中只有一个公共通信信道,为所有节点共享使用,任一时刻只允许一个节点使用公用信道。当一个节点利用公共通信信道发送数据时,必须携带目的地址,只有地址符合的那个节点,才能接收到数据,其他节点都不能收到数据。

4 . 计算机网络体系结构

为了简化问题、减少协议设计的复杂性,大多数网络都采用一种层次结构,按层或级的方式来组织。因此,协议也是分层次的。每一层都建立在下层之上,每一层的目的都是为上层提供一定的服务,并对上层屏蔽其服务的实现细节。各层协议互相协作,构成一个整体。常称之为协议簇(protocol family)或协议套(protocol suite)。

网络分层体系结构模型的概念,为计算机网络协议的设计和实现提供了很大的方便。在体系结构中最著名的是国际标准化组织(ISO)于 1981 年颁布的开放系统互连参考模型(open system interconnection reference model, OSI)。OSI 定义了异种互联网标准的框架结构,受到计算机和通信行业的极大关注。OSI 不断发展,得到了国际上的承

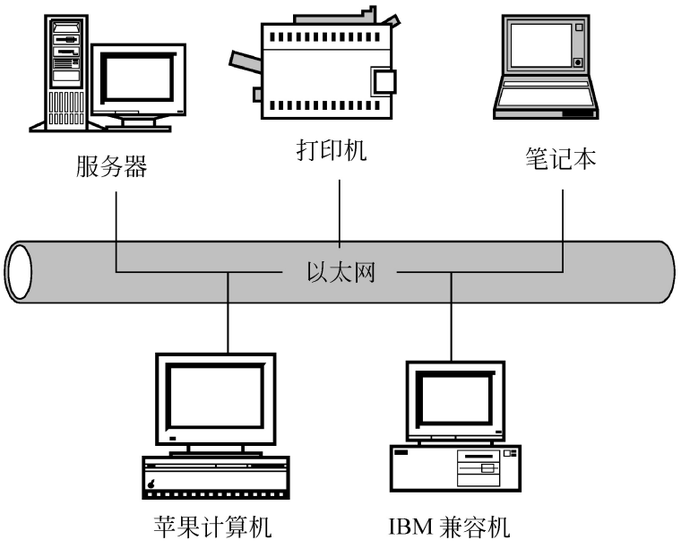

图 1-2　广播式通信方式

认,成为其他各计算机网络系统结构靠拢的标准,大大地推动了计算机网络和计算机通信的发展。

在这里“系统”是指一台或多台计算机,外部设备、终端、信息传输设备、操作员及相应软件的集合。“开放”是指按照 OSI 参考模型建立的任意两系统之间的连接或操作。当一个系统能按照 OSI 标准与另一个系统进行通信时,就称该系统为开放系统。可见,开放系统要求建立一整套能保证全部级别都能进行通信的标准。

OSI 开放系统互连参考模型,如图 1-3 所示。它采用结构描述方法,即分层描述的方法,将整个网络的通信功能划分成 7 个部分(也叫 7 个层次),每层各自完成一定的功能。由低层至高层分别称为物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。这种划分使每一层都能执行本层所承担的具体任务,且功能相对独立,通过接口与其相邻层连接。这里接口指相邻层之间的连接,依靠各层之间的接口或功能的组合,实现两系统间、各结点间信息的传输。

(1) 物理层(physical layer)

物理层涉及到通信在信道上传输的原始比特流,主要处理与物理传输介质有关的机械的、电气的、功能的和规程的接口。物理层与具体设备有关,如光纤及收发器、网卡和集线器等。

(2) 数据链路层(data link layer)

数据链路层的主要任务是加强物理层传输原始比特的功能,使之对网络层显现为一条无差错的链路。它通过将传输的数据增加同步信息、校验信息及地址信息封装成数据帧;同时提供数据帧传输顺序的控制、差错检测与控制和数据流量控制以保证数据传输的正确性。

(3) 网络层(network layer)

确定数据分组从源端到目的端如何选择路由。即通过路径选择将信息从最合适的路径由发送端传送到接收端,防止通信子网信息流量过大造成网络阻塞及数据丢失。

(4) 传输层(transport layer)

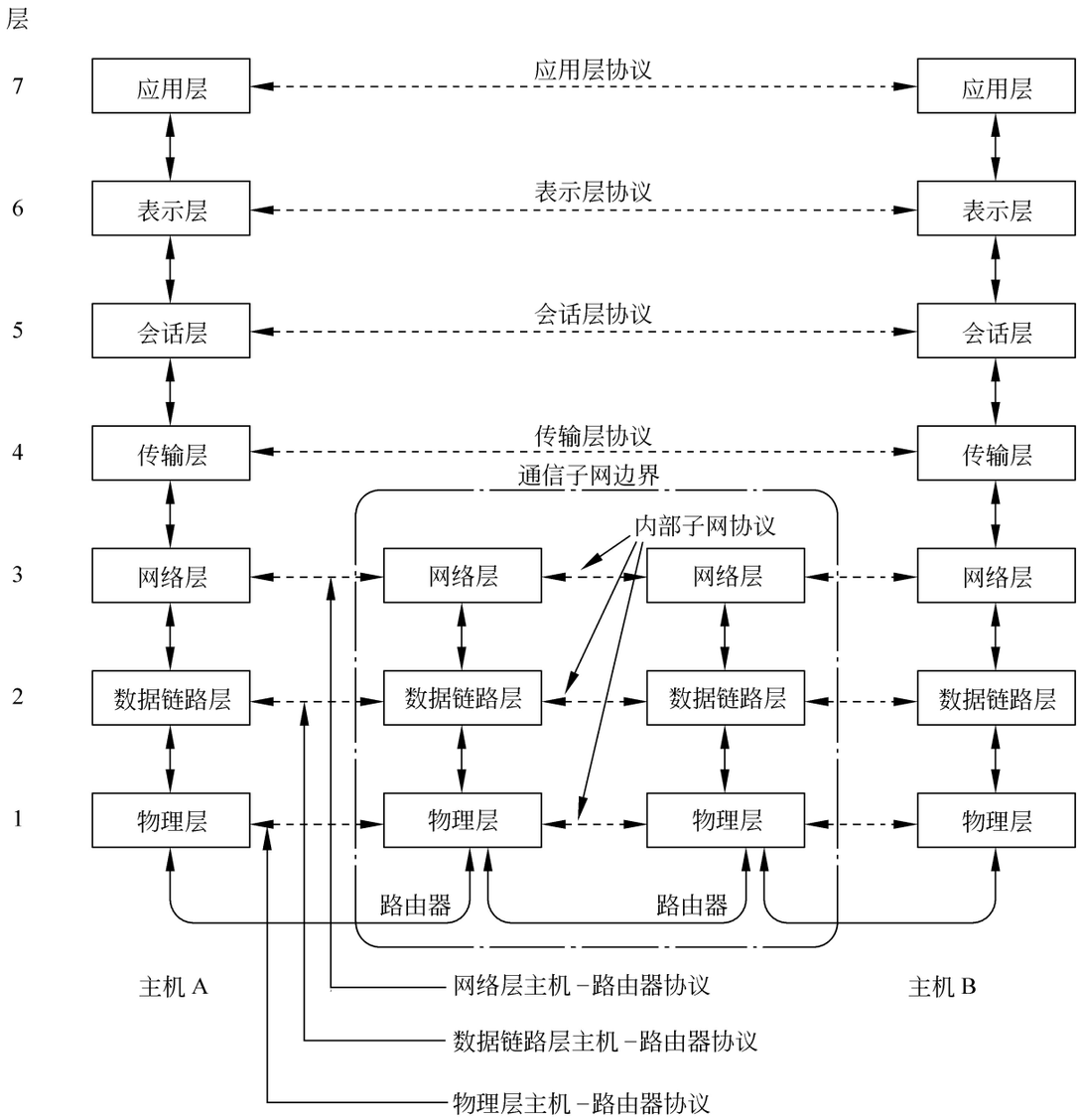

图 1-3　OSI 参考模型及协议

传输层的基本功能是从会话层接收数据，并且在必要时把它分成较小的单元，传递给网络层，并确保到达对方的各段信息正确无误，从某种意义上讲，传输层使会话层不受硬件技术变化的影响。

传输层也要决定向会话层，最终向网络用户提供什么样的服务。最流行的传输连接是一条无错的、按发送顺序传输报文或字节的点到点的信道。

传输层是真正的从源到目标（端-端）的层。也就是说，源端机上的某程序，利用报文头和控制报文与目标机上的类似程序进行对话。在传输层以下的各层中，协议是每台机器和它直接相邻的机器间的协议，而不是最终的源端机与目标机之间的协议，在它们中间可能还有多个路由器。

传输层主要完成的功能如下：

① 分割和重组报文；

② 提供可靠的“端-端”的服务；

③ 传输层的流量控制；

④ 提供面向连接的和面向无连接数据传输服务。

(5) 会话层(session layer)

会话层允许不同机器上的用户建立会话(session)关系。

会话层服务之一是管理对话。会话层允许信息同时双向传输或任一时刻只能单向传输。若属于后者,则类似半双工通信,会话层将记录此时该轮到哪一方了。

与会话有关的服务是令牌管理(token management)和同步(synchronization)。

(6) 表示层(presentation layer)

表示层主要完成以下特定的功能:

① 对数据编码格式进行转换;

② 数据压缩与恢复;

③ 建立数据交换格式;

④ 数据的安全与保密;

⑤ 其他特殊服务。

(7) 应用层(application layer)

应用层包含大量人们普遍需要的协议和提供许多应用软件包。例如 FTP、E-mail 等程序及应用软件包。

应用层完成的主要功能如下:

① 作为用户应用程序与网络间的接口;

② 使用户的应用程序能够与网络进行交互式联系。

在 OSI 7 层模型中,每一层都提供一些明确的网络功能。

一般数据通信子网中的交换节点只包含 OSI 模型的下 3 层,表示节点的这 3 个层次又称为中继开放系统。

若从功能角度看,下面 4 层主要提供通信传输功能,以节点到节点之间的通信为主;高层协议(会话层、表示层和应用层)则以提供用户与应用程序之间的处理功能为主。简而言之,低 4 层协议属于通信功能,高 3 层属于处理功能。

若从产品看,低 3 层协议一般由硬件完成,高层协议由软件完成。例如,网卡和网桥完成物理层和数据链路层的功能,路由器完成网络层的功能,而电子邮件软件完成应用层的功能。

在实际网络系统中,OSI 中的会话层和表示层很少使用。

1.1.2 Internet 网络

1. Internet 物理结构

Internet 连接了不同国家与地区无数不同类型的电脑,可能是某个校园网的大型主机,也可能是某个办公室的个人电脑。硬件千差万别,使用的操作系统与软件也各不相同,要保证这些电脑之间能够畅通无阻地交换信息,必须有相通的语言,即统一的通信协议。

Internet 是一个计算机网络的网络或叫做网间网(把全世界各种各样的网络都联接

到一起所形成的网络),那么 Internet 是怎么把这些网络连接到一起的呢?Internet 是用一种称为路由器的专用计算机将网络互联在一起的,如图 1-4 所示。当然,单纯将计算机硬件互联在一起并不能形成 Internet,互联的计算机还需要在软件的指挥下才能正常地工作。

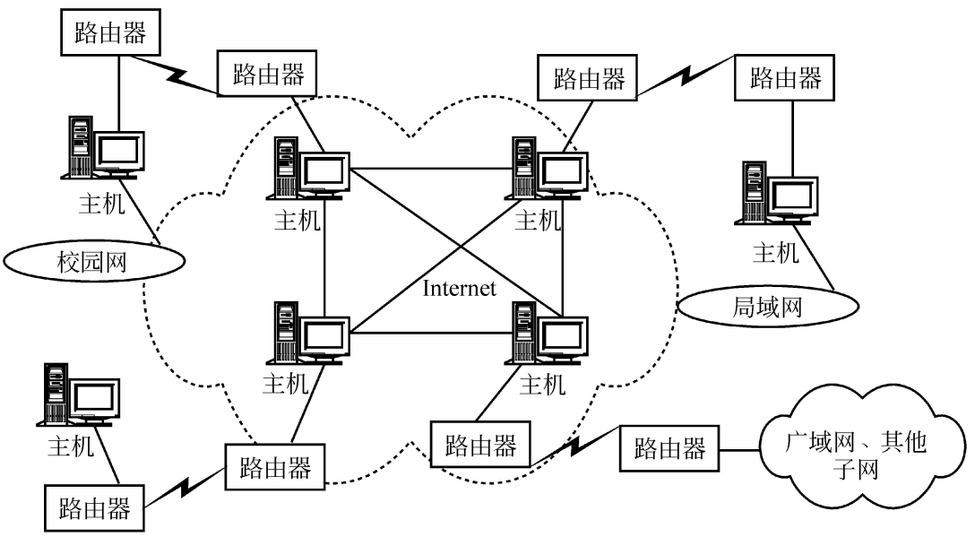

图 1-4　Internet 中路由器将全球的网络连接在一起

2 . TCP/ IP 协议

在 Internet 中使用的一个关键的协议是网与网之间的协议,也叫做网际协议(IP),IP 精确地定义了分组必须怎样组成,以及路由器必须怎样将每一个分组递交到其目的地。连接到 Internet 上的每台计算机都必须遵守网际协议 IP 的约定。每台发送信息的计算机必须按 IP 定义的格式产生分组。接收信息的计算机也需按 IP 的约定从中提取信息。由此可见,实现该操作的软件(IP 软件)是最基本的软件,所有 Internet 服务都使用 IP 来发送或接收分组,所以通常每台计算机在通信时都必须使 IP 软件驻留在内存中,以便时刻准备发送或接收分组。IP 分组也称为 IP 数据包。IP 分组的发送就像电报局处理电报一样,一旦发送方准备好一个数据包并且将其发送到 Internet 上后,发送者就可以处理其他事务。

TCP 协议的主要作用是使 Internet 工作得比较可靠。连接到 Internet 上的所有计算机都运行 IP 软件,并且其中的绝大多数还运行 TCP 软件。事实上,由于 TCP 和 IP 在 Internet 网络中的重要地位以及两者在一起工作得很好,因此,把 Internet 中所使用的整个通信协议组称为 TCP/ IP 协议组。

TCP/ IP 协议也采用了层次体系结构,所涉及的层次包括网络接口层、传输层、网间网层和应用层。每一层都实现特定的网络功能,其中 TCP 负责提供传输层的服务,IP 协议实现网间网层的功能。这种层次结构系统遵循着对等实体通信原则,即 Internet 上两台主机之间传送数据时,都以使用相同功能通信为前提,这也是在 Internet 上主机之间地位平等的一个体现。TCP/ IP 协议模型如图 1-5 所示。

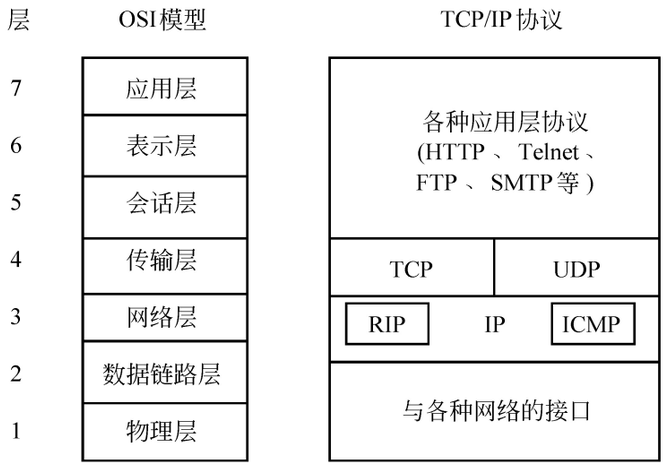

图 1-5　TCP/IP 协议模型

下面介绍 TCP/IP 协议各层实现的具体功能和作用。

(1) 网络接口层

TCP/IP 协议对这一层的描述很少,一般网络接口层提供了 TCP/IP 协议与各种物理网络的接口,为数据包的传送和校验提供了可能。这些物理网络包括各种局域网和广域网,如 Ethernet, Token Ring, X .25 公共分组交换网等。网络接口层也为在其之上的网间网层提供服务。

(2) 网间网层(internet layer)

网络接口层只提供了简单的数据流传送服务,而在 Internet 中网络与网络之间的数据传输主要依赖网间网层中的 IP 协议(internet protocol)。

IP 是构成网间网层的一个主要部分。IP 负责 Internet 上主机与主机之间的通信,即将数据包由一台主机传输到另一台主机。

具体地讲,IP 包括如下功能。

① 管理 Internet 中的地址: 由于 IP 负责将数据包由源方发送到目的方,因此要对数据包中的地址,即所谓 Internet 上的 IP 地址进行管理。而 IP 地址名称的由来就是"符合 IP 协议的地址"的简称。

IP 地址具有固定、规范的格式。它由 32 位(bit)二进制数组成,分成 4 段,其中每 8 位构成一段,一般用十进制数表示,段与段之间用小数点号"."隔开。例如,某台计算机的 IP 地址为:192 .168 .1 .25。

IP 地址根据适用范围的不同分为 3 类: A 类地址、B 类地址和 C 类地址,主要依据网络号和主机号的数量划分,如图 1-6 所示。其中 1 .x .y .z～126 .x .y .z 格式的 IP 地址,属于 A 类地址,A 类 IP 地址通常用于大型网络的管理;128 .x .y .z～191 .x .y .z 格式的 IP 地址,属于 B 类地址,B 类地址适应中等规模的网络;192 .x .y .z～223 .x .y .z 格式的 IP 地址,属于 C 类地址,这种编址适用于一些小公司或研究机构;224 .x .y .z～239 .x .y .z 格式的 IP 地址,用于特殊用途,如多目广播;240 .x .y .z～255 .x .y .z 格式的 IP 地址,暂时保留,用于某些实验和将来使用。

IP 地址中的"主机号"字段,可继续划分为"子网号"字段和"主机号"字段。一般来说,在一个单位分配到的 IP 地址中,当主机数量很大时(例如:一个 B 类地址,最多可以有

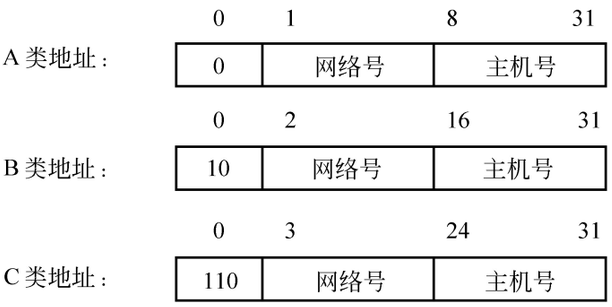

图 1-6　基本的 IP 地址

2^{16} - 2 = 65 534 台主机),为了便于隔离和管理本单位的网络,同时防止网络内由于主机数量太多以至出现广播风暴问题而采用子网划分。如图 1-7 所示,判断两台主机是否在同一个子网中,需要用到子网掩码或子网模,子网掩码同 IP 地址一样是一个 32 位的二进制数,只是网络部分(包括 IP 网络和子网)全为“1”,主机部分全为“0”。判断两个 IP 地址是否在同一个子网中,只需判断这两个 IP 地址与子网掩码做逻辑“与”运算的结果是否相同,相同则说明在同一个子网中。如 C 类地址的子网掩码为 255 255 255 0。

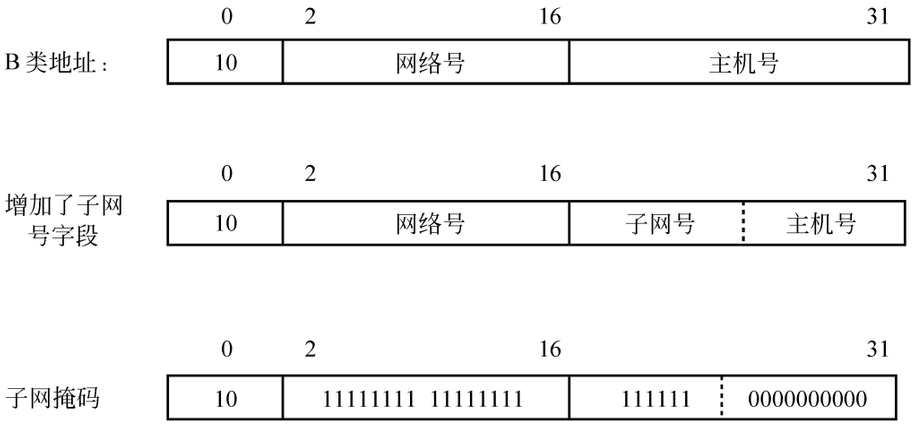

图 1-7　子网掩码的作用

② 路由选择功能：数据包在传输过程中要由 IP 通过路由选择算法,在源方与目的方之间选择一条最佳的路径。

③ 数据包的分片与重组：数据包在传输过程中要经过多个网络,因为每种网络所规定的分组长度不等,当数据包经过只能传输长度较小的分组的网络时,就需要将数据包分割成小段才能通过。当数据包全部到达目的方后,还需要由 IP 将它们重新组装。

综上所述,IP 协议规定了 Internet 上的计算机之间通信所必须遵守的规则。IP 定义了 Internet 上 IP 地址的格式,并通过路由选择,将数据包由一台计算机传递到另一台计算机。但 IP 只负责传送数据包,而不考虑传输的可靠性、数据包的流量控制等安全因素。

与 IP 配合使用的还有以下 3 个协议：

① Internet 控制报文协议 ICMP(Internet control message protocol),用于报告差错和传输控制信息;

② 地址转换协议 ARP(address resolution protocol),用于将 IP 地址转换成物理地址;

③ 反向地址转换协议 RARP(reverse address resolution protocol),用于将物理地址转换成 IP 地址。

(3) 传输层(transport layer)

传输层中的 TCP 协议提供了一种可靠的传输方法,解决了 IP 协议的不安全因素,为数据包正确、安全地到达目的地提供了保障。这里定义了两个“端-端”的协议:TCP 和 UDP。

第一个是传输控制协议 TCP(transmission control protocol)。它是一个面向连接的协议,允许从一台机器发出的字节流无差错地发往 Internet 上的其他机器。TCP 把输入的字节流分成报文段并传给网间网层。在接收端,TCP 接收进程把收到的报文再组装成输出流。TCP 还要处理流量控制,以避免高速发送方向低速接收方发送过多报文而使接收方无法处理。

第二个协议是用户数据报协议 UDP(user datagram protocol)。它是一个不可靠的、无连接协议,用于不需要 TCP 的排序和流量控制功能而是自己完成这些功能的应用程序。它也被广泛地应用于只有一次的客户机/ 服务器模式的请求-应答查询,以及快速递交比准确递交更重要的应用程序,如传输语音或影像等。自从这个模型出现以来,IP 已经在很多其他网络上实现了。

TCP 和 UDP 都使用了端口(port)进行寻址。一个主机里往往有多个进程在运行,为区分是哪一个进程在进行通信,就必须在传输层上设置一些端口。一个端口是一个 16 位的地址。对于一些最常用的应用层服务,都各有一个对应的端口号,这种端口号叫做数字端口,数字为 0～255,如应用层提供的 FTP 服务端口为 21、WWW 服务端口为 80 等。

(4) 应用层(application layer)

TCP/ IP 协议设有会话层和表示层。传输层的上面是应用层,它包含所有的高层协议。最早引入的是虚拟终端协议(Telnet)、文件传输协议(FTP)和电子邮件协议(SMTP),虚拟终端协议允许一台机器上的用户登录到远程机器上并且进行工作。文件传输协议提供了有效地把数据从一台机器传输到另一台机器的方法。电子邮件协议最初仅是一种文件传输,但是后来为它提出了专门的协议。这些年来又增加了不少新的协议,例如域名系统服务 DNS(domain name server),用于把主机名映射到网络地址;NMTP 协议,用于传递新闻文章;还有 HTTP 协议,用于在万维网(WWW)上获取主页等。从应用开发角度出发,在 Internet 上已经开发出许多实用程序,如 Netscape、Internet Explorer 浏览器等。这些实用程序通过 Socket 套接接口与各种应用协议相连接。例如,TCP/ IP 基于 Windows 的应用程序接口为 Winsock。

3 . Internet 的服务

Internet 发展迅猛,其提供的服务在不断增加,应用领域也迅速扩大,而且日益渗透到人们的生活和工作之中,成为日常交流中不可缺少的组成部分。这里所列出的只是一些基本服务与应用的概括。Internet 所提供的服务都采用客户机/ 服务器的模式。

(1) 电子邮件

E-mail(电子邮件)是 Internet 提供的一项最基本服务,它基于客户机/ 服务器的模

式,如图 1-8 所示,是用户使用最为广泛的 Internet 服务之一。电子邮件的最大特点是快速、方便,通常发送一封邮件只需几分钟就能被对方接收到,并且费用低廉,特别适合远距离用户之间的相互联系。Internet 的电子邮件系统模仿普通的邮政业务,通过在一些特定的网点(如 ISP 的主机)设定“邮局”,提供“邮局”的主机又叫邮件服务器。用户可以在该“邮局”上租用一个“电子信箱”(mail box),当用户向 ISP 申请“电子信箱”时,ISP 在邮件服务器上建立该用户的电子邮件账户,它包括用户名(user name)和用户密码(password)。当需要进行邮件的收发处理时,用户可以在任何时间、任何地点与自己的“邮局”连接,输入自己信箱的用户名和密码打开电子信箱,进行邮件的收发或存档处理等。

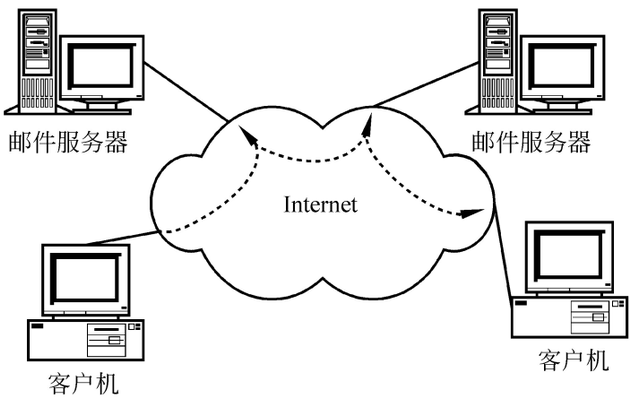

图 1-8　电子邮件服务的工作原理

每个电子信箱都有一个邮箱地址,称为电子邮件地址(E-mail address)。电子邮件地址的格式是固定的,并且在全球范围内是惟一的。用户的邮件地址格式为:用户名@主机名,其中“@”符号读作“at”。主机名指的是拥有独立 IP 地址的计算机的名字,用户名是指在该计算机上为用户建立的电子邮件账号。例如,在“sohu .com”主机上,有一个名为“jzyuan”的用户,那么该用户的 E-mail 地址为 jzyuan@sohu .com。

目前,平均每天有 5000 万份电子邮件在 Internet 上传输,处于世界不同角落的人们均可通过这种方式来进行彼此间的交流。电子邮件有着电话、传真所无法比拟的优点,例如可以将一份电子邮件同时发送给多个收件人;可以把收到的邮件立即转发(forward)出去;可以即时答复等。目前,已有越来越多的人将自己的电子邮件账号同联系电话一样印在名片上向外分发,可见它具有广泛的通信联系作用。

在使用传统的电子邮件软件时,用户需要登录到一个多用户系统上,如 UNIX 系统(一种主流网络操作系统),该系统通常是一天 24 小时都连接在 Internet 上,用户可以随时编写、发送、接收电子邮件,这种方式就是通常所说的终端方式。随着网络技术的发展,出现了大量的基于 Windows 环境下的各种客户端电子邮件软件,这些电子邮件软件允许用户脱机阅读、撰写电子邮件的内容,大大减少了用户的联机费用,而且界面友好,因此受到广大用户的欢迎。

(2) 文件传送(FTP)

FTP(file transfer protocol)是在 Internet 上进行文件传输的一种协议,其工作原理如图 1-9 所示。目前 FTP 多用于将远程 FTP 服务器上的一些共享软件或资料文件传输

到本地机上,这一过程称为下载(download)。FTP 的工作方式遵循客户机/ 服务器模式,使用 FTP 首先要有一个 FTP 的客户端软件。用户通过 FTP 网点进行连接,连接成功后查找到所需要的文件进行下载。

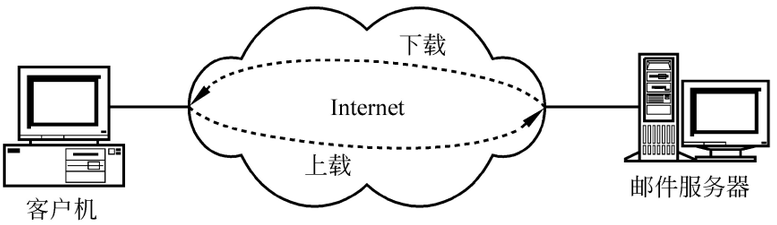

图 1-9　FTP 服务的工作过程

对于网络上众多的信息,用户在进行 FTP 传送时多是用匿名(anonymous FTP)方式,即远程 FTP 服务器允许任何用户访问该网点并可从该网点上免费下载文件。但通常情况下,用户在登录某一台 FTP 网点时,多是以 Anonymous 或 Guest 作为用户名,以电子邮件地址作为口令来进行身份注册。

(3) WWW(world wide web)浏览

在 Internet 提供的众多服务中,WWW 是最受欢迎的一种服务,特别是对于初学者。目前访问 WWW 的用户正在与日俱增。WWW 提供的不仅是文字信息,而且包括了图像、声音、动画等多媒体信息。因此,访问 WWW 会使用户感受到 Internet 更加直观、具体、生动和形象。

WWW 提供的信息量是非常丰富的,其范围包括了科技、教育、政治、军事、娱乐、商业等各个领域,可以说,不论你从事何种行业的工作,都可以在 WWW 上找到相关的内容,并且有些甚至是最前沿的信息。特别值得指出的是 WWW 在商业贸易方面具有巨大的潜力,目前一些在线的商品订购、金融投资、商业合作等已占相当数量的比例,并且日趋增长;同电视、报纸、杂志等广告宣传媒体相比,WWW 更有无可比拟的作用和效果。

从技术角度讲,WWW 提供的是一种基于页面检索的信息服务。页面的组织方式抛开了传统的连续性,而采用了符合人脑思维习惯的具有跳跃性的超链接(hyper link)技术。在其页面中经常有一些字、词或图片是以高亮、下划线或变色等特殊方式显示的,表明这些内容是可作为进一步查询的超链接,用鼠标单击它就可以进入下一页面的内容。这种超链接技术使得全球的 WWW 信息都有机地联系起来,用户可以轻松地从一幅页面跳转到另一幅页面上,从一台 Web 服务器跳转到另外一台 Web 服务器上。

这些具有超链接的页面文件在全球 Internet 上是一种通用格式,称作 Web 页面。Web 页面的编写是通过 HTML(hyper text markup language)超文本置标语言来实现的,该语言是一种类似于排版用的置标语言,通过加一些特定的标记,能够将文字、图像、声音、表格等信息有机地组织起来,使 Web 页面看上去图文并茂。

WWW 服务也采用基于客户机/ 服务器的工作模式,如图 1-10 所示。客户端要运行 WWW 客户程序,它提供良好的用户界面,将用户的查询请求送给服务器。Web 服务器上存储大量 Web 页面并连接后台数据库,随时等待响应客户端发来的请求,执行查询后将结果返回给客户端。客户端与 Web 服务器的交互是通过超文本传输协议 (hyper text

transfer protocol, HTTP)来完成的,而用户要查询某一台 Web 服务器是通过 URL (uniform resource locator)统一资源定位符来指定的,URL 地址既可以是本地硬盘上的某个文件也可以是 Internet 上的网点。例如下面 URL 所示:

http:// www .Microsoft .com/ pub/ index .html

其中 http: 为所使用的传输协议,"// "后面跟着的是 Internet 上 Web 网点的域名。如果在 URL 地址中将 http 换成 FTP 或 Gopher 协议,并在"// "后面跟上相应的 FTP 站点或 Gopher 站点,这样就可以在 WWW 客户端程序上执行 FTP 服务或 Gopher 服务。目前,WWW 客户端程序使用较广泛的是 Netscape 公司的 Netscape Navigator 和 Microsoft 公司的 Internet Explorer 两种浏览器。

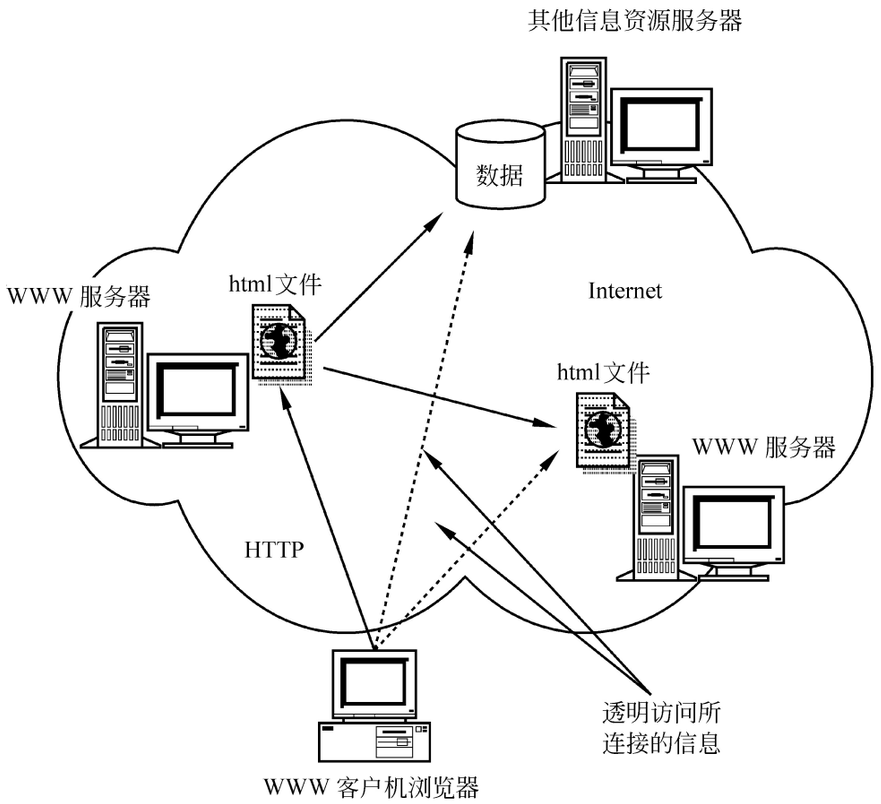

图 1-10　WWW 服务的工作原理

(4) 远程登录(telnet)

追溯到一台小型计算机相当于 3、4 个冷冻柜(更大的计算机还要用自己的空调系统)大小的时代,对科学家和工程师来说,最初对 Internet 感兴趣的原因是 Internet 使他们能得到本地得不到的计算机资源,并使他们更容易与其他城市的同行们合作。现在,具有 Internet 账号的用户可利用自己的办公室或实验室的终端与网络中任何其他计算机建立起连接,只需使用 UNIX 的 telnet 命令来建立一个远程终端连接,这种连接只需在 telnet 后面注上远处计算机的地址即可。

通过 telnet 进行远程操作有两项较普遍的应用:第一,许多系统都允许用 guest 为用户名免费访问该站点。第二,其他一些系统支持 Internet 的用户在他们的系统上建立个人账号。例如,许多图书馆都用联机系统取代了原来传统的卡片目录。只要图书馆的计

算机接在 Internet 网中,便可通过远程访问查询需要的目录。

(5) Internet 的其他服务

Internet 还提供了基于目录方式的信息检索查询工具 Gopher 分类目录服务。例如:用户可通过网络新闻(News)服务参与某个方面主题的讨论;利用在线交谈(IRC)服务进行交谈和网络的实时会议;通过网络电话(web phone)服务用市话费用拨打国际长途;虚拟时空(virtual reality)服务在电脑世界里创造一个越来越逼真的现实环境,形成另一个时空观念,在这里交友、购物、玩游戏、旅游观光等,从事着现实生活中存在的或虚拟出的各项活动。Internet 提供的远程教育与科研(remote education)服务将彻底改变人们传统的教学方式,学生可以分布在世界各地,教学资料可以搁放在任何地方,这种教学方式的改变,可以大大提高教学的灵活性,降低教学和学习成本。

Internet 上提供的各种服务已达到上万种,其中大多数服务是免费的。随着 Internet 商业化的发展趋势,它提供的服务将会进一步增多。

1.2 计算机网络存在的安全问题

迅速发展的 Internet 给人们的生活、工作带来了巨大的方便,人们可以坐在家里通过 Internet 收发电子邮件、打电话、进行网上购物、银行转账等,一个网络化社会的雏形已经展现在我们的面前。但是,在网络给人们带来巨大便利的同时,也带来了一些不容忽视的问题,网络信息的安全保密问题就是其中之一。

1.2.1 什么使网络通信不安全

随着网络特别是 Internet 的迅速发展,给网络带来的安全问题,向认为 Internet 已经完全胜任商务活动的人们泼了一盆冷水,也延缓和阻碍了 Internet 作为国家信息基础或全球信息基础设施成为大众媒体的发展进程。一些调查研究表明,许多个人和公司之所以对加入 Internet 持观望态度,其主要原因就是出于安全的考虑。尽管众说纷纭,但大家一致认为网络需要更多更好的安全机制。

生活中人们经常听说,某黑客(黑客指未经授权而获取网络资源的非法用户)入侵了某一网络,使该网络服务全部瘫痪;某黑客利用网络从某一银行盗取了大量钱财等。这说明世界上没有绝对安全的网络,只要用户使用计算机、联网以及网络连接了 Internet,它就存在危险,就必须考虑它的安全问题。此外,人为因素和自然因素也影响网络的安全性。自然因素是一些意外事故,如服务器突然断电和发大水冲坏了网络等。自然因素并不可怕,可怕的是人为因素,即人为的入侵和破坏。

网络的开放性以及黑客的攻击是造成网络不安全的主要原因。科学家在设计 Internet 之初就缺乏对安全性的总体构想和设计,所用的 TCP/ IP 协议是建立在可信的环境之下,主要考虑的是网络互联,在安全方面则缺乏考虑。这种基于地址的 TCP/ IP 协议本身就会泄露口令,而且该协议是完全公开的,远程访问使许多攻击者无须到现场就能

够得手,连接的主机基于互相信任的原则等等,这一些性质使网络更加不安全。

1.2.2 影响计算机网络安全的因素

随着计算机网络技术的发展和应用,一方面网络提供了资源共享性、系统的可靠性、工作的效率和系统的可扩充性;同时也正是这些特点,增加了网络安全的脆弱性和复杂性,资源共享和分布增加了网络受威胁和攻击的可能性。

对网络的威胁,主要有以下 4 个方面:

网络硬件设备和线路的安全问题;

网络系统和软件的安全问题;

网络管理人员的安全意识问题;

环境的安全因素。

1.网络硬件设备和线路的安全问题

(1) Internet 的脆弱性,系统的易欺骗性和易被监控性,加上薄弱的认证环节以及局域网服务的缺陷和系统主机的复杂设置与控制,使得计算机网络容易遭受到威胁和攻击。

(2) 电磁泄露: 网络端口、传输线路和处理机都有可能因屏蔽不严或未屏蔽而造成电磁泄露。目前,大多数机房屏蔽和防辐射设施都不健全,通信线路也同样容易出现信息泄露。

(3) 搭线窃听: 随着信息传递量的不断增加,传递数据的密级也在不断提高,犯罪分子为了获取大量情报,可能在监听通信线路,非法接收信息。

(4) 非法终端: 有可能在现有终端上并接一个终端或合法用户从网上断开时,非法用户乘机接入,并操纵该计算机通信接口或由于某种原因使信息传到非法终端。

(5) 非法入侵: 非法分子通过技术渗透或利用电话线侵入网络,非法使用、破坏或获取数据或系统资源。目前的网络系统大都采用口令验证机制来防止非法访问,一旦口令被窃,就无安全可言。美国国防部对计算网络安全问题进行过测试,对在 10 个月内美国军用网络 Milnet 网上的 450 台计算机受入侵的情况进行统计,其结果表明:有 2%的攻击者能攻入网络并进入节点主机,得到系统管理员的权限;有 4%的攻击者能侵入网络并进入节点主机,侵入编程环境;有 13%的攻击者可以注册侵入节点主机。在这些人中,95%的攻击者企图联网,遭到网络拒绝;有 13%的攻击者通过注册账号和口令侵入第 3 层,其成功的原因之一是使用主机系统固有的默认名-口令组合,另一原因是查询网络用户名目录窃取用户名和口令;有 9%的攻击者注册入侵,取得部分权限,进入系统第 4 层;有些攻击者能进入第 5 层,存取电子邮件和通用数据库,不少入侵者还可取得诸如核战争和生物战争的有关信息;有 2%的攻击者能侵入第 6 层,进入编程环境;还有 2%的攻击者能进入系统管理员权限。

(6) 注入非法信息: 通过电话线有预谋地注入非法信息,截获所传信息,再删除原有信息或注入非法信息后再发出,使接收者收到错误信息。

(7) 线路干扰: 当公共转接载波设备陈旧和通信线路质量低劣时,会产生线路干扰。