网迷宝典丛书

# 挑战黑客宝典

主编 李 冬
策划 书林创作群

INTERNET

附多媒体光盘

人民邮电出版社

Internet 网络宝典丛书

# 挑战黑客宝典

□ 主编　李 冬
□ 策划　书林创作群

人民邮电出版社

Internet 网迷宝典丛书

**挑战黑客宝典**

◆ 主　　编　李　冬
策　　划　书林创作群
责任编辑　贾福新
◆ 人民邮电出版社出版发行　北京市崇文区夕照寺街 14 号
北京密云春雷印刷厂印刷
新华书店总店北京发行所经销
◆ 开本:787 × 1092　1/16
印张:17.5
字数:437 千字　　2000 年 1 月第 1 版
印数:5 001 – 9 000 册　　2000 年 3 月北京第 2 次印刷
ISBN 7-115-08284-7/TP·1443

定价:42.00 元

# 前言

“最让人恐惧的事是恐惧本身”，这种情况同样也发生在 Internet 发展的今天。我们常常考虑到底是什么阻碍了 Internet 在社会政治和经济中的广泛应用，是什么原因使我们的顾客仍然不敢也不愿意通过 Internet 进行交易。还有，为什么在我们为企业架设网络的时候总是要问一个类似的问题：这个和 Internet 连接的计算机网络会不会被黑客利用？是的，重要的原因就是“安全”。在网络上的大多数人都或多或少地知道计算机安全的概念，哪怕是没有接触过计算机的人也能够通过电视、报纸等媒体知道诸如“美丽杀”病毒、黑客之类的名词，他们心中充满了恐惧。并不是其中的大多数人曾经被病毒感染过，也不是他们的计算机资料被窃取过，他们甚至从来不曾碰过 Internet 甚至计算机，但是这种恐惧阻碍了他们去接触和使用计算机。如果这些人在单位中处于决定性的位置，他们可以一声令下：不许碰 Internet！我们在现实生活中目睹这样的事情大量地发生着，这也是我们写这本书的初衷，至少，我们希望能够通过这本书使得人们消除无谓的恐惧，勇敢地面对 Internet!

人类对自身以及自己所拥有的安全的保护是一种自然本性，在几千年的人类社会发展过程中，人们不仅提高了保护自己的安全意识和手段，同时从对安全的保护的需求出发产生了集体和国家，大到用军队、警察等武装力量来保卫国家和社会的安全，小到用防盗锁来保卫自己的家产不被盗窃。在商业领域，除了需要保护自己的财产之外，还需要在商业交往中保护自己的利益，其中一项最为常见的要求就是有关识别的问题，我们需要用印章、签字、各种号码甚至指纹等标记来说明这就是你，而不是别人。几千年来，人类就是这样保卫着各自的安全。

今天，我们不仅把目光放到了太空和海底，我们还在电子世界中建设着一个新的世界，这个世界就是 Internet。我们通过电子邮件进行交流，在聊天室度过一天的好几个小时，在 WEB 上建立自己的企业网站，我们把企业的资料放到数据库中，然后使之和 Internet 相联，从而实现远程办公和交易。总之，这个新世界就像现实世界一样存在于我们的周围，在这个世界中生活着一群人，俗称“网虫”，在这个世界中有着庞大的产业以及人类的未来。

可是，在这个世界中没有军队，也没有警察，可能连法律都不是很完善，大多数时间里，人类就好像是回到了原始社会需要靠自身的力量去和各种危险抗争。

难道我们就因此而放弃吗？答案显然是否定的。事实上，首先我们应当做的是消除恐惧的心态，勇敢地去面对未来对我们的挑战。这本书是讲技术为主的，但是在讲技术之前，我们希望大家能够明白，迎接挑战只有技术是不够的，还需要些勇气和冒险。就像打仗一样，勇敢者的伤亡往往比恐惧者的伤亡小。其次，是掌握科学的方法和技术，毕竟在 Internet 上和人类在几十万年前面对的敌人不同，我们现在最大的威胁是我们的同类：人。人和人之间的斗争已经很多年了，这只不过是一个新的战场，在这个战场上，技术是最重要的因素，换句话说，只要拥有足够的技术，我们完全可以了解到所面临的威胁的来源并予以抵制，甚至是反击。何况，即使是没有明确的法律，仍然可以通过现实社会中的法律来维护正义，惩治邪恶。

本书将从多方面来讨论网络安全的问题。

首先讲述和网络安全有关的基础知识。网络安全实际上涉及到了计算机的各个方面，一般人可能认为只是一个软件问题，其实这种认识是错误的。Intel 最新发布的 PIII 处理器中就内置了个人标识号，这就涉及到了安全的考虑以及对个人隐私的讨论。另外，网络安全还是一个政治和社会问题。在这一部分里，我们将集中讨论和安全相关的一系列概念。

其次讲述了与网络安全相关的技术。在确定这个部分的几个标题的时候，我们想起了神话中的法和魔之间的斗争。在现实社会中正因为熟悉一些常见的犯罪行为和手段，我们才得以去有效地防范。同样，为了在网络安全战中立于不败之地，如《孙子兵法》所述：知己知彼，百战不殆，首先我们需要了解“魔”的方法，就像分析犯罪一样，我们将对威胁网络安全的各种根源进行详细的分析。当然，我们最重要的目的还是为了使我们更安全。所以，在第二、第三章里我们将从个人防卫以及系统级的安全两个方面来分析和讲解用于安全的工具。

最后将介绍网络安全协议（SSL）。SSL 对于大多数人来说还是一个陌生的名词，但是在网络安全中，SSL 是最重要的协议之一，也是网络安全交易的基础。在这一部分中，我们将讲述 SSL 的概念、原理以及如何构建一个 SSL 系统的过程和步骤。同时，在附录部分我们也将为读者附上一些有用的资料。

书林创作群

http://www.sulin.net

## 内容提要

本书详尽地讲述了黑客手段与网络安全技术。对威胁网络安全的各种根源进行了详细分析，从个人防卫以及系统级的安全两个方面讲解了用于网络安全的工具，并重点介绍了网络安全交易的基础——SSL 网络安全协议，讲述了 SSL 的概念、原理以及如何构建一个 SSL 系统的过程和步骤。

本书是一本十分有趣的书，通过这本书，读者不仅可以了解到构建一个安全网络所必需的知识，还可以了解到在网络安全这个战场上的一些逸事。我们并不指望每个读者都能成为网络安全专家，但是我们希望每个读者都能从本书得到一些有益的启示，从而尽可能地为自己的网络应用提供更多的保护。

# 我们是网迷

## 写在《Internet 网迷宝典丛书》出版之际

谁是网迷?

上网接送“伊妹儿”的是网迷;

上网搜索信息的是网迷;

上网下载软件的是网迷;

上网聊天开会的是网迷;

上网成“家”立业的是网迷;

上网求职谋生的是网迷;

上网游戏娱乐的是网迷;

上网打网络电话的是网迷;

上网炒股的是网迷;

上网购物的是网迷;

上网旅游看世界的是网迷;

上网交友征婚的是网迷;

上网者都将成为网迷。

1998 年 5 月中国的网迷突破 100 万。

1999 年 1 月中国的网迷达到 210 万。

1999 年 7 月中国的网迷达到 400 万。

2000 年中国的网迷将突破 1000 万。

我们是网迷，我们徜徉在因特网这个人类历史最大的文化宝库里，贪婪地吸取历史留给我们的宝贵财产，古金字塔的神秘、卢浮宫的瑰丽尽在指间；我们借助网

络游荡在虚拟世界之中，远程教育、网上(在家)办公、网上购物、网上炒股、电子商务……已经成为现实。网络正以让人难以置信的速度，将其无所不在的触角伸向人类社会的各个角落，让人们可以随时随地接收和处理各种信息。我们发现，因特网给网迷开启的是一片美好的天地。

海阔凭鱼跃,天高任鸟飞。网络已经为我们搭起了一个广阔无比的舞台,为我们创造了一个信息时代。网络编辑、网络记者、网络警察、网络工程师、网络设计师等新型职业应运而生。网络的发展为社会造就出一大批新兴的行业和职业,人类社会的各项活动也会因此逐步融入网络,网络将成为人类一刻也不能离开的“法宝”。

网络将极大地开阔我们的视野，改变我们的工作和思维方式，带来大量全新的概念和思想，并为我们创造出无数的机会和财富。这是一个取之不尽用之不竭的“宝藏”。

可以肯定地说，人类社会因为因特网的普及将更加美好，而《Internet 网迷宝典》将帮助网迷们更加自由自在地冲浪。

我们骄傲，我们是网迷。

我们幸运，我们拥有《Internet 网迷宝典》。

书林创作群

http://sulin.126.com

# 目　录

# 第一章

# 网络安全基础

## 第一节　网络生存环境初探

在现实生活中，如果对于周围的环境不熟悉，那么无论是生活还是工作无疑都会遇到很多麻烦，同样，在网络世界里讨论安全问题，首先需要了解网络的基本情况，尤其是我们要讨论的中心：Internet 网。

### 一、网络的形式、内容与安全的关系

当你步入网络世界之后，就意味着你踏入了一个新的世界，你可能从中获得有用的东西，也可能在网络交往中遭到损失。一般人眼里的网络只是计算机的互相连接，因此最重要的自然是保证计算机的安全。其实除了计算机本身的安全，在网络中还存在着另外一个层次的安全，那就是网络生活的安全。通常，我们需要从网络的形式和内容来考虑网络的环境。

考察网络的形式需要考察其硬件平台、网络连接方式以及使用的系统平台和常用软件。事实上，网络也正是建立在计算机、各种网络设备以及网络协议、操作平台之上的，这些不仅是网络的形式，也是网络的物质基础，就好像你走在一个城市里面，看见有房子，有街道，有住户，有商家一样。当我们需要了解网络的时候，尤其是了解网络安全的时候，就需要了解我们接触的网络是如何连入这个世界的，这种连接方式本身对我们自身的计算机安全会不会造成影响。这个问题自然是我们这些从事技术工作的人员研究的重点，现在已经有了许多成熟的网络安全产品。这些安全产品用我们日常生活中的事物来打个比方，就是门和锁。

我们当然希望我们赖以连接网络的基本设备能够为我们带来最基本的安全保障，比如说，我们希望 Windows 软件不会在我们不知晓的时候自动地通过网络泄露一些并不想公开的个人资

料，而作为网络管理人员则希望他所管理的网络平台不会为一些不法分子留下“后门”。当一个企业领导决定把他的内部网连接到 Internet 的时候，他希望有一堵墙能够使得他的内部网络不会被外面的人员随意访问，就好像有个门卫在那里看守。而要做到这一切，不坐下来好好地研究一下计算机和网络的基本概念是不行的。当我们了解了这些基本技术之后，我们至少知道计算机的哪些东西是不可避免地要暴露在网络世界之中的，而哪些东西完全可以根据我们对计算机安全问题的注意而保护起来。实际上，虽然网络运行在我们看不见的空间里面，但是你的隐私却有可能通过网络被泄露出去，比如上网一般需要一个账号，而一般人都通过电话上网，这就使得你和你的 Internet 服务商之间有了交往，从技术上讲，他们可以跟踪你在网络上的一切行为，从中就可以了解到你的爱好等一些本只应当属于你个人的信息。当然，一个信誉良好的 Internet 服务商是绝对不会滥用你的个人信息的，就像银行的职员一般不会透露你的账户的财务情况一样。另外，一般人利用电子邮件进行相互交流，但是他们可能并不了解电子邮件发送和接收的过程，如果通过一条自己并不清楚的途径发送敏感的资料的话，那本身就是极其危险的事情。

然而，网络安全的问题涉及的并不仅仅是计算机本身的问题。如果考虑到现实社会中因为犯罪行为而失去财产的情况，小偷通过破门而入自然是一种方法，但是还存在着诸如诈骗这种几乎完全和人与人之间交往直接相关的犯罪行为。当我们通过网络开始展开活动的时候，我们就开始了网上的生活，开始了和人交往的过程。首先是一个信任的问题。信任的问题在生活中也存在着：街头向你乞讨的人可能比你富有十倍，小报上的新闻实际上是谎话，你所认识而且信任的人突然向你伸出了黑手，为了能够在这个世界上顺利地生存下去，我们也有了抵御一般欺骗的能力。但是，当我们生活在网上的时候，我们甚至不能判断和自己交往了多时的人是男是女。

同时，目前的 Internet 是从一种无序的状态下发展起来的，所以，没有真正意义上的政府，也没有真正意义上的警察和法院，只有几个少数的机构充当着类似于公证机构的职责，这也是网络欺骗产生的重要原因。

从个人上网的角度来说，尽管大多数人主要是利用网络在进行 WWW 浏览，但是考虑一下上网的过程，你就会发现事情不是那么简单的了。在网上充满了各种各样的免费服务，为了获取这样或者那样的免费服务，你通常需要填写一些表单，告诉别人你的姓名、地址、电话以及邮件地址之类的内容，这些内容通常也会被这些网络服务商所利用。另外在参加到新闻组、订阅邮件列表的时候都有可能泄露一些个人的信息。关于具体的，我们在后面将详细地论述到。

除了个人的隐私之外，在网上还普遍存在着一些在日常生活并不常见的滋扰，比如说，漫天乱飞的广告邮件，在聊天室时有发生的性骚扰行为等，这些问题产生的基础都是因为有了人与人之间在网上的交流。而我们在研究这些问题的时候，除了要从技术上来分析之外，还需要从社会、文化以及法律的角度来研究这些问题的起因及其解决的方法。

应该说，网络的形式和内容在安全方面是互相联系的。不可能想象一个不安全的硬件或者软件环境会带来安全的交往。同时人们对网络安全的需求也促进了计算机技术的发展。比如说，Intel 公司新近开发出来的 PIII 芯片就内置了个人数字标识，从而试图从硬件级上解决网络的信任问题，当然，这也产生了一个新的问题，就是个人的隐私问题，并不是所有的人都希望把自己暴露在网络世界之中，网络本身为他们提供的这种“不知你我”的交流模式或许真是他们追求的理想。所以这样的硬件设施又产生了网络交流中的新问题。

涉及计算机安全的因素很多，从硬件环境一直到应用程序的使用，每一个环节都会涉及到安全因素。但是，对于大多数人来说，现在特别关心的是网络使用上的安全，而非在设计和安装上的安全问题。因此，我们在讨论网络的生存环境的时候，也主要讨论和网络相关的软件方面的知识，而对于一般和硬件相关的问题，比如说，计算机的屏蔽问题、网络通信线路的维护问题等，请读者参考其它有关书籍。

## 二、TCP/IP 协议

TCP/IP 协议，即传输控制协议和网际协议，是 Internet 的核心协议，而且随着 Internet 的普及及其在技术上的优势显现，TCP/IP 协议也将广泛地应用在局域网中(通常称之为 Interanet)。

### 1. TCP/IP 协议简介

从历史角度看，TCP/IP 协议开发的最初目的是为了实现网络和应用的兼容性，即为了能够实现异种网络、异种机器之间的互连。TCP/IP 最初用于 ARPANET（Internet 的前身）、PRNET（分组广播网）和 SANET（分组卫星网）的连接。用户所使用的计算机大多数还是大型机，用户终端通过终端服务器与计算机相连。使 TCP/IP 协议发扬光大的最重要的有两件事情：其一是将 TCP/IP 融入到 Unix 系统之中，其二就是加利福尼亚大学的伯克利分校公开了 TCP/IP 代码。

1983 年，在 DARPA（美国国防部高级计划署）的资助下，加利福尼亚大学的伯克利分校推出了内含 TCP/IP 协议的第一个 Unix 系统，这个系统的推出立即受到了广泛的欢迎，因为当时全美各个学校正缺乏一种可以用于互连的网络操作系统。值得注意的是，BSD Unix 的成功还有两个原因：第一，除了支持标准的 TCP/IP 的应用程序之外，它还提供了一套网络服务工具程序，这些工具程序的调用和标准的 Unix 的命令类似，深受 Unix 程序员的欢迎。第二，BSD Unix 提供了可以访问 TCP/IP 的应用程序：Socket，Socket 是一种进程间的通信机制，是 Unix 标准输入/输出的扩展，也正是有了 Socket，程序员可以容易地访问 TCP/IP 协议，这都推动了 TCP/IP 的发展。

TCP/IP 协议代码的公开，在业界产生了迅速而积极的影响。对于网络通信来说，设计人员可以对基于 TCP/IP 协议的网络应用有更加深入的了解，从而有利于设计出便捷、实用而且安全的程序，但是从另外一方面来说，不怀好意的人也因此可以研究这些协议中可以利用的地方，从而达到自己的目的。同样的问题也存在于现在源码开放的各个系统之中，对此问题我们应该采取什么样的态度，在后面将详细地讨论。

1996 年，Internet 在全世界蓬勃地发展起来，个人接入网络的需求也变得不容忽视。微软推出的 Windows 95 操作系统中内置了 TCP/IP 协议，从而为个人 Internet 应用奠定了基础。Windows 95 中的 TCP/IP 协议通过 Winsock 动态链接库实现，因此直接利用 Winsock 的编程也称之为 Winsock 编程。

那么 TCP/IP 到底是什么呢？它是网络中基于软件的通信协议。尽管从名字上来看，TCP/IP 协议只包括了两个协议——传输控制协议和网际协议，但实质上包括了 Internet 上的众多协议——是一系列软件的综合。它提供诸如远程登录、远程文件传送、电子邮件等网络服务，也提供诸如处理网络故障、选择传送路径和控制数据传送等功能。下面是 TCP/IP 中

一些基本的和常用的网络协议：

网络层：IP（网际协议）、ICMP（网际控制报文协议）。

传输层：TCP（传输控制协议）、UDP（用户数据报协议）。

应用层：TELNET（远程登录）、FTP（文件传输协议）、SMTP（简单邮件传输协议）、DNS（域名系统）、ASN（抽象语法）、NFS（网络文件服务器）等。

从中可以看到，除了 TCP 作为传输的协议之外， UDP 也是传输层的一个协议，它们之间的差别就在于 TCP 是面向连接的协议，而 UDP 是面向无连接的协议，详细内容读者可以参考有关介绍 TCP/IP 的书籍。而我们一般常用的 TELNET、FTP、SMTP 等都是以面向连接的协议为基础的。

TCP/IP 协议作为 Internet 的组成部分，它的组织和管理工作是由 Internet 建议委员会（IAB）承担的。而 TCP/IP 协议的来源则是 RFC（Request for Comments），每个 RFC 是对一个 Internet 请求的技术说明，它们代表了有关的 Internet 的技术文档。其中一些 RFC 最终成为 TCP/IP 的标准，而其它的则成为一般的技术信息，或者继续被研究讨论，也有许多被淘汰了。同时一个 RFC 文档被颁布的时候拥有一个号码，而当其更新的时候又会拥有一个新的号码，所以，掌握一个 RFC 文档的最新版本是非常重要的。

RFC 文档可以从网上免费获取。

网址是：http://www.cis.ohio-state.edu/hypertext/information/rfc.html

其中 http://www.cis.ohio-state.edu/htbin/std/INDEX.std.html 记录了成为 Internet 标准的 RFC 文档。

或者是从相应的 FTP 站点获取。

也可以给地址 rfc-info@isi.edu 发送电子邮件，无需标题（Subject），信体部分写明 help:way-to-get-rfc 就可得到一些相关的资料。

让我们简要地回顾一下 TCP/IP 协议发展过程中的几个重要的里程碑：

1970 年 ARPANET 主机开始便用网络控制协议（NCP）。

1972 年 第一个 TELNET 标准“Ad hoc Telnet Protocol”作为 RFC318 被提交。

1973 年 采用 RFC454“文件传输协议”。

1974 年 传输控制程序 Transmission Control Program(TCP)被详细地描述。

1981 年 IP 标准作为 RFC791 公布。

1982 年 美国国防通信研究局（DCA）和 ARPA 把 TCP 和 IP 作为 TCP/IP 协议集。

1983 年 ARPANET 由 NCP 转向 TCP/IP。

1984 年 采用域名系统 DNS。

重要的网络协议包括：

(1) 地址解析协议（ARP）

地址解析协议主要用于从互联网地址到物理地址的映射。这在网络的路由信息中至关重要。在一个报文（或其他数据）发送之前，它打包成 IP 分组报文或适合网络传输格式的信息块。这些分组报文包含了信源和信宿机的数字 IP 地址。在这个数据离开信源机之前，必须发现信宿机的硬件地址（硬件地址不同于互联网地址），这时 ARP 首次登场。一个 ARP 请求报文以广播方式在子网上传送，这个请求被一个路由器接收，该路由器用被请求的硬件地址作为应答，这个应答被信源机捕获，传输过程便开始了。要深入了解 ARP 资源的读者可以参考 RFC 826。

(2) 网络互连控制报文协议（ICMP）

网络互连控制报文协议处理传输过程中在两台（或更多台）计算机或主机间传送的错误信息和控制报文，它允许这些主机共享这些信息。在这一方面，ICMP 对于诊断网络故障是很关键的，通过 ICMP 收集到的诊断信息包括：

主机关闭；

网关阻塞或不通；

网络上的其它故障。

名为 Ping 的网络应用程序可能是最著名的 ICMP 实现。Ping 常用于测试一台远程机器是否工作。Ping 的用法很简单。当用户 Ping 一个远程主机时，报文从用户机传向远程主机，然后这些报文再被传回给用户机。如果在用户端没有接收到回应报文，Ping 程序通常产生一个错误消息，指示远程主机关闭。

有关 ICMP 深层资料请参阅 RFC 792。

(3) 网络互连协议（IP）

IP 协议属于网络层。IP 协议为 TCP/IP 协议套中的所有协议提供分组传送。因此，IP 是整个网络数据传输过程的核心。想深入了解 IP 协议的读者，参考 RFC 760。

(4) 传输控制协议（TCP）

传输控制协议是主要的互联网络协议，它所完成的任务至关重要，如文件传输、远程登录。TCP 通过可靠数据传输完成这些任务，在这一方面，TCP 不同于其它协议，在非可靠传送中，你不能保证到达的数据的完整性，而 TCP 却可以提供可靠传输。这种可靠传输确保发送数据以相同顺序、相同状态到达信宿。

(5) 文件传输协议（FTP）

文件传输协议是文件从一个系统传输到另一个系统的标准方法。

(6) 简单邮件传输协议（SMTP）

简单邮件传输协议的目的是可靠高效地传输邮件。

(7) 超文本传输协议(HTTP)

超文本传输协议可能是所有协议中最著名的协议，因为它允许用户浏览网络。在 RFC1945 中是这样简洁描述 HTTP 的，HTTP 是："一个应用层协议，具备分布、协同、超媒体信息系统所必需的轻巧和速度。它是一个普通的、面向对象的协议，可用于许多任务，比如，姓名服务器、分布式对象管理系统。HTTP 的一个特点是数据描述的归类，允许独立建立传输数据系统。"

RFC 1945 已被 RFC 2068 取代，后者是 HTTP 最新的定义，参见地址：

ftp://ds.internic.net/frc/rfc2068.txt

(8) 网络新闻传输协议（NNTP）

NNTP 是用途最广的协议之一，它提供对人所共知的 USENET 新闻的新式访问，在 RFC 977 中对其目的的定义如下：

"NNTP 是用于公布式系统的一种协议，它利用可靠的、基于流的新闻传输方式，在 ARPA 互联网世界中查询、检索和发送新闻稿。根据 NNTP 的设计，新闻稿被存储在中央数据库中，允许用户选择他想阅读的新闻文章，还提供对旧消息的索引，对照参考和舍弃功能。"

在 RFC 977 中可以找到有关 NNTP 的更多材料，你还可以在 RFC 850 中看到这一协议标准的早期实现。

## 2. TCP/IP 协议是怎样运作的

要掌握 TCP/IP 的操作，首先要了解一些术语和概念，例如网关、路由器、连接方式，还要掌握一些基本的工具。这些对于一个已经开始从技术上关心网络安全的人员来说不是问题，因此，在这里，我们只通过实例来说明一下如何直接利用 TCP/IP 的指令进行编程和设计。不过为了能够进行 TCP/IP 编程，我们首先要了解一下 Socket 的概念。

在 TCP/IP 模型中，各层使用的地址/名字方式各不相同。其中，我们比较熟悉在网络层使用 IP 地址，而在 Internet 应用中就使用“端口”。具体的互联网络应用（如文件传输和电子邮件）是由端口号标识的。常用的应用都有自己保留的端口号，被称为“众所知”的端口号。IP 地址连同端口号一起，提供了唯一的、无二义性的连接标识，这个连接叫套接字（Socket）。英语里的意思也就是像插座一样地将导线和主机连接起来。TCP 建立了一些常见的端口号，例如 TELNET 使用端口 23，HTTP 协议使用端口 80 等，以下是一些常见协议使用的端口号：

| | | |
|---|---|---|
| ECHO | 端口号 5 | 回应 |
| FTP-DATA | 端口号 20 | 文件传输（数据） |
| FTP | 端口号 21 | 文件传输（控制） |
| TELNET | 端口号 23 | 远程登录 |
| SMTP | 端口号 25 | 简单邮件传输 |
| TIME | 端口号 37 | 时间 |
| NAMESERVER | 端口号 42 | 主机名服务器 |
| DOMAIN | 端口号 53 | 域名服务器 |
| FINGER | 端口号 79 | FINGER |
| HTTP | 端口号 80 | HTTP 协议 |
| POP3 | 端口号 110 | POP3 协议 |

除了这些常见的端口号之外，0-1023 范围的端口号是保留端口，也就是说，有可能被未来的系统调用使用。而高于 1024 的端口供个人程序使用，当然也提供给一些开发 Internet 网络应用的程序使用，例如 MS SQL 数据库的 TCP/IP 连接的默认端口就是 1433。

Socket 在 C 语言的编程中可以看作是标准输入输出的一种扩展，而在 Windows 系统下，则有标准的 Winsock 控件提供给 VC、VB 程序员直接利用 Winsock 进行编程。以下是直接利用 Winsock 控件编制的一个邮件方面的程序，它可以说明如何利用 RFC 文档进行编程。

当您使用 WIN95 OSR 版本或者 WIN98 之后，因为它们都内置了 TCP/IP 协议，Winsock 控件就自然存在于您的计算机之中了。Winsock 控件对用户来说是不可见的，它提供了访问 TCP 和 UDP 网络服务器的方便途径。如果为了编写客户或服务器应用程序，您可以不必了解 TCP 的细节或调用低级的 Winsock APIs，只要通过设置控件的属性并调用其方法就可轻易连接到一台远程机器上去，并且还可双向交换数据。Microsoft Access，Visual Basic，Visual C++ 或 Visual FoxPro 的开发人员都可使用它。

(1) 建立 TCP/IP 连接

TCP 数据传输协议允许创建和维护与远程计算机的连接。而连接后的两台计算机就可以彼此进行数据传输。

对于创建客户应用程序来说，只要知道服务器计算机名或者 IP 地址（RemoteHost 属

性），以及进行“侦听”的端口（RemotePort 属性，POP3 服务器的 PORT 一般是 110，而 SMTP 一般是 25），然后调用 Connect 就可以把您的计算机和服务器连接起来。

而对于创建服务器应用程序来说，就应设置一个收听端口（LocalPort 属性）并调用 Listen 。当客户计算机需要连接时就会发生 ConnectionRequest 事件。为了完成连接，可调用 ConnectionRequest 事件内的 Accept。

建立连接后，任何一方计算机都可以收发数据。为了发送数据，可调用 SendData。当接收数据时会发生 DataArrival 事件。调用 DataArrival 事件内的 GetData 就可获取数据。

(2) 向对方发送指令和数据

如果要进一步开发一些诸如邮件程序的话，您还需要知道更多的东西，首先，就是 RFC（Request For Comments）的一些相关的协议，例如：POP3 协议规定了 POP3 的指令和格式，而 POP3 协议则是由 RFC1939 文档所描述的，而 SMTP 协议则是由 RFC821，RFC822 等一系列文档所规定的。这里，我们只就编制邮件程序所需的最基本的 POP3 协议和 SMTP 协议讲述相关的指令。

① POP3 协议：

POP3 有 3 种状态：Authopization 状态（用户认证状态）和 Transaction 状态（处理状态）和 Update 状态（更新状态），而每一条命令则需要以<CR><LF>结束，即以 Ascii 码的 13 和 10 结束。

命令列表：

USER 用户名　　登录用户名　　仅在 Authorization 状态下有效

PASS 口令　　传送密码

如果认证通过的话，则进入 Transaction 状态

STAT　　查看状态

LIST [信件号] 列信件

RETR 信件号　取指定信件

DELE 信件号　对信件做删除标记 信件号（信件将在 Update 状态下被删除）

NOOP　　空操作，仅返回 OK

RSET　　复位，取消所有标记

QUIT　　退出，进入 Update 状态

（以上命令并非需要按顺序依次执行）

另外还有些可选的 POP3 命令:

TOP 信件号 数目　　列出信件的信件头

UIDL [信件号]　　对信件的唯一标识号进行列表

② SMTP 协议

SMTP 协议则更为简单，但是除了一般的 SMTP 服务器外，现在的服务器还大量地支持 ESMTP（Extension SMTP）协议，登录到服务器后，服务器会给出一段文字表示其是否支持 ESMTP 协议。而用 HELP<CR><LF>(注意：仍然要用<CR><LF>来结尾)则可以列出所有可用的 SMTP 指令。

一般来说，一个发送邮件的过程如下：

MAIL FROM:<发件人邮件地址>

指示发件人地址,发件人为空可以为<>