中国电脑教育报 CCID CHINA COMEPUTER EDUCATION 系列出版物

★金山毒霸完整试用版
★金山网镖完整试用版

防黑 防毒 防扰

个人网络安全三防手册

- 安全使用QQ、ICQ
- 局域网网络安全
- 网络病毒及查杀方法
- 教你用防火墙

个人网络安全三防手册

本书配有软盘，需要者请到网络光盘实验室拷贝

《中国电脑教育报》社

《个人网络安全》（含配套手册）
出版发行：《中国电脑教育报》社
地址：北京市海淀区紫竹院路 66 号 赛迪大厦 16 层
邮编：100044
电话：（010）88559698
责任编辑：李健
封面设计：关洪森

开本：787×1082 1/16 印张 13.5
字数：250 千字
版次：2002 年 3 月第一次印刷
版号：ISBN 7-900096-43-4

装订错误可随时与本单位联系更换

目录 CONTENT

第一章 网络基础 1

第一节 计算机网络的概念、特点、功能以应用 1

一、计算机网络的概念 1

二、计算机网络的特点 1

三、计算机网络的功能 1

四、计算机网络的应用 2

第二节 Internet 网的发展 3

一、Internet 网的发展过程 3

二、IPv6 技术 4

三、Internet 的发展技术 9

四、应用的发展——电子商务 10

第三节 计算机网络的分类和基本组成 11

一、局域网（LAN） 11

二、广域网（WAN） 14

第四节 网络体系结构 16

第五节 网络协议简介 20

一、TCP/IP 协议栈 21

二、四层模型 22

三、ARP 23

四、ICMP 和 IGMP 24

五、IP 25

目录 CONTENT

六、TCP 26
七、IP 地址和子网掩码 27
八、建立子网 28
九、域名系统及 DNS 服务器 29
第六节 实现 IP 路由 30
一、IP 路由简介 30
二、路由表和路由协议 31
三、路由协议的“理想” 31
四、两种路由算法 31
第七节 Internet 入门 33
一、如何成为 Internet 网络用户 33
二、Internet 所能提供的各种服务与介绍 36
三、一些网络术语的解释 38

第二章 Internet 网络安全 45

第一节 你的网络安全吗? 45
一、黑客的常用攻击手法和攻击策略 46
1. 非破坏性攻击 46
2. 破坏性攻击 46
二、黑客惯用的入侵方式 48

目录 CONTENT

数据驱动攻击 48
系统文件非法利用 48
针对信息协议弱点攻击 48
远端操纵 48
重新发送攻击 49
对 ICMP 报文的攻击 49
跳板攻击 49
窃取 TCP 协议连接 49
夺取系统的控制权 49
三、黑客经常使用的软件介绍 50
特洛伊木马 50
BO2000 53
国产木马——冰河 65
防范 71
密码破解工具 75
四、黑客的防御 77
1.黑客因何有用武之地 77
2.保障网络安全的注意事项 77
第二节 防御黑客 80
一、木马防御全攻略 80
1. 细说木马 80

目录 CONTENT

2. 冰河 84
3. 如何防范木马 90
二、病毒防预全攻略 90
三、QQ 安全手册 91
1. IP 探测 91
2. 消息炸弹 92
四、ICQ 安全手册 92
1. 从 ICQ 主页下载软件 92
2. 给你的 ICQ 加密码 93
3. 防止你的 IP 泄露 93
4. 防止 ICQ 中的“后门” 93

第三章 个人网络防火墙 94

第一节 防火墙 94
一、防火墙的定义 94
二、防火墙的基本准则 94
三、防火墙的基本类型 94
四、防火墙的局限性 95
第二节 防火墙使用详解 96
一、天网个人版防火墙 96

目录 CONTENT

二、norton 个人防火墙 107
三、金山毒霸 115
四、lockdown2000 网络防火墙 146

第四章 局域网中的网络安全 154

第一节 局域网存在的安全问题 154
1. 局域网中 Windows 2000 的安全防范 155
2. 局域网中 Windows98 的安全防范 158
第二节 文件加密 163

附录一：常用黑客软件使用介绍 174

一、NETBUS 174
二、netspy 180
三、IP 探查工具 180
1. IP hunter 181
2. NETXRAY 182
3. 追捕 183
四、扫描工具 184
1. 扫描器介绍 184
2. 扫描工具 SUPERSCAN 187

目录 CONTENT

五、攻击工具 189
1. 网络炸弹 189
2. 蓝屏炸弹 191
3. 邮件炸弹 191
4. 密码破解工具 191

附录二：典型及流行病毒介绍 203

第一章　网络基础

第一节　计算机网络的概念、特点、功能以应用

随着计算机应用的深入，特别是家用计算机越来越普及，一方面众多用户希望能共享信息资源，另一方面也希望各计算机之间能互相传递信息进行通信。由于个人计算机的硬件和软件配置一般都比较低，其功能也有限，因此，要求大型与巨型计算机的硬件和软件资源以及它们所管理的信息资源能够为众多的微型计算机所共享，以便充分利用这些资源。基于这些原因，促使计算机向网络化方向发展，将分散的计算机连接成网，从而组成计算机网络。

一、计算机网络的概念

所谓计算机网络，就是把分布在不同地理区域的计算机与专门的外部设备用通信线路互连成一个规模大、功能强的网络系统，从而使众多的计算机可以方便地互相传递信息，共享硬件、软件、数据信息等资源。它是现代通信技术与计算机技术相结合的产物。

二、计算机网络的特点

计算机网络的发展过程大致可以分为具有通信功能的单机系统、具有通信功能的多机系统和计算机网络三个阶段。

据预测，今后计算机网络具有以下几个特点：

（1）开放式的网络体系结构，使不同软硬件环境、不同网络协议的网可以互连，真正达到资源共享、数据通信和分布处理的目标。

（2）向高性能发展。追求高速、高可靠和高安全性，采用多媒体技术，提供文本、声音，图像等综合性服务。

（3）计算机网络的智能化，多方面提高网络的性能和综合的多功能服务，并更加合理地进行网络各种业务的管理，真正以分布和开放的形式向用户提供服务。

三、计算机网络的功能

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高的要求，同时也为其

发展提供了更加有利的条件。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、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。

一般来说，计算机网络可以提供以下一些主要功能：

（1）资源共享。

（2）信息传输与集中处理。

（3）均衡负荷与分布处理。

（4）综合信息服务。

通过计算机网络可以向全社会提供各种经济信息、科研情报和咨询服务。其中，国际互联网 Internet 上的环球信息网（WWW-World Wide Web）服务就是一个最典型也是最成功的例子。又例如，综合业务数据网络（ISDN）就是将电话、传真机、电视机和复印机等办公设备纳入计算机网络中，提供了数字、语音、图形图像等多种信息的传输。

四、计算机网络的应用

计算机网络目前正处于迅速发展的阶段，网络技术的不断更新，进一步扩大了计算机网络的应用范围。除了前面提到的资源共享和信息传输等基本功能外，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。

（2）传送电子邮件

计算机网络可以作为通信媒介，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，这些邮件中可以包括文字、声音、图形、图像等信息。

（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。它以共同认可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，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。

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。

计算机系统连入网络以后，具有共享资源、提高可靠性、分担负荷和实现实时管理等优点。

第二节 Internet 网的发展

一、Internet 网的发展过程

从 20 世纪 80 年代末开始，计算机网络技术进入新的发展阶段，它以光纤通信应用于计算机网络、多媒体技术、综合业务数据网络（ISDN）、人工智能网络的出现和发展为主要标志。20 世纪 90 年代至 21 世纪初是计算机网络高速发展的时期，计算机网络的应用将向更高层次发展，尤其是 Internet 网的建立，推动了计算机网络的飞速发展。Internet 网起源于美国 1969 年开始实现的 Arpanet 计划，其目的是建立分布式的、存活力极强的全国性信息网络。1972 年由 50 所大学和科研机构参与连接的 Internet 网最早的模型 Arpanet 第 4 次公开向人们展示。到 1980 年，Arpanet 成为 Internet 网最早的主干。

1984 年，美国国家科学基金会 NSF 规划建立了 13 个国家超级计算中心及国家教育科技网(NSFNET)，它替代了 Arpanet 的骨干地位。随后，Internet 网开始接受其它国家地区的接入。

最初美国的 Internet 网具有 3 级体系结构，包括 NSFNET 主干网、地区网和校园网。主干网连接地区网和超级计算中心。最终用户（一般为校园网）通过地区性网络进入 Internet网。Internet网的NSFNET主干网速率初期为T1（1.544RNb/s），现已过渡到OC3（155RNb/s）。Internet 网、地区网与校园网的连接一用速率为 56k/s 或 T1 速率的租用线。面向最终用户的校园网是多种形式的局域网，比较多的是 FDDI（100RNb/s）和以太网（10RNb/s）。

在网络应用范围上，近年来 Internet 网逐渐放宽了对商业活动的限制，已经朝商业化的方向发展。不少公司都在它上面刊登广告，用户可以通过它来订购杂志、计算机软件，以至于开展网络购物。现在，Internet 网早已从最初的学术科研网络变成了一个拥有众多的商业用户、政府部门、机构团体和个人的综合计算机信息网络。其应用除了学术科研外，远程医疗、远程教学、电子商务、娱乐休闲也等已应有尽有。Internet 网的发展速度是惊人的，只要你今天想到 Internet 网还没有实现什么，那么，明天在你连入网络时，或许就会发现它已经在 Internet 网上了。

在网络规模上，目前 Internet 网已经是全世界规模最大、发展最快的计算机互联网。从有关 Internet 网的统计资料可以看出，到 1997 年 1 月，在 Internet 网注册的域（1 个域一般都有多个局域网）已经达到 82.8 万个，1600 多万台计算机连入网络，共有 193 个国家和地区在 Internet 网注册了域名，连入的用户数按每台计算机 10 个用户计算，则共有 1.6 亿人上网。从 1991 年开始 Internet 网联网计算机的数量每年翻一番，目前每天有 4000 台计算机入网，到 2000 年则超过了 100 万个网络，有 1 亿台计算机和 10 亿个用户在使用 Internet 网。

如此蓬勃的 INTERNET 发展，也带来了一些棘手的难题。

1．带宽的短缺

据1995年的估计，有150多个国家和地区的6万多个网络同Internet连接，入网计算机约450万台，直接使用Internet的用户达4000万人。而到今天，Internet已经开通到全世界大多数国家和地区，几乎每隔三十分钟就有一个新的网络连入，主机数量与用户数量增长飞快，在21世纪初，Internet已连接近亿台计算机，达到以十亿计的用户。而对更远的将来，人们很难精确估计。不管怎么说，这些数字已足以说明Internet的危机所在：就好象一根悬挂了很多重物的钢丝绳，重量增加了，绳子就有断裂的危险；而用户在Internet上的游历实际上要走过很多根这样的“钢丝绳”，用户越多，绳子的负载越重，其中任一根不结实，都会成为瓶颈，导致网络访问的失败。因此，“钢丝绳”的加固、带宽容量的增加势在必行，从Internet主干到分支，直至最终用户的接入，都出现了许多成熟的或正在发展的链路技术来实现这项需求，我们将在后文着重介绍其中用户最为关心的几种接入技术。

2．IP地址资源的匮乏

我们曾介绍了IP地址的格式和分类，这里所指的都是现行的IPv4。它是一个32位二进制数，因此总地址容量为232，也即有数亿个左右。而按照TCP/IP协议（同很多其他协议一样）的规定，相互连接的网络中每一个节点都必须有自己独一无二的地址来作为标识，那么很显然，相对前文日益增长的用户数，现有IP地址资源已不堪重负，很快将被用光。

解决IP地址缺乏的办法之一是想办法延缓资源耗尽的时间，目前应用最广泛的技术当属NAT（Network Address Translation，网络地址翻译）——它使企业用户在内部网络应用中采用自行定义的地址，只在需要作Internet访问时才翻译为合法的Internet地址。它的最大好处是用户加入Internet时不需更改内部地址结构，而只需在内外交界处实施地址转换，并且能够实现多个用户复用同一合法地址，从而大大节省地址资源。但这里用户需注意的是：NAT转换的同时也增加了网络的复杂性，何况它并不能阻止可用地址越来越的趋势。

作为对IPv4问题的解决，一种新的IP地址定义应运而生，它便是下文要讲的IPv6。

二、IPv6技术

正当人们为IPv4面临的问题而焦头烂额时，IPv6出现了，它给人们带来了近乎完美的解决方案：

* 如同电话号码升位一样，IPv6提供了128位的IP地址，使地址数量大幅增加，从而解决了现在的IP地址资源危机。

* IPv6采用了“可聚集全球统一计算地址”的构造，这使IP地址构造同网络的拓扑结构（连接形态）相一致，从而缩小了路由表，使路由器能够高效率地决定路由。

IPv6具有自动把IP地址分配给用户的功能大大减少了网络管理费用。

* 通过增加一个作用域字段而改进了多点播送地址。

* 新的任意播送（anycast）IP地址类型用于向组内任何成员发送包，通常是最近的组

成员。

* 用可选的扩展头部替代头部中的选项字段。
* 删除头部的校验和字段。
* 删除所有分段处理所用的字段，仅执行端到端的分段。
* 新的流标号字段可用来标识特定的用户数据流或通信量类型。
* 扩展了对认、数据一致性和（可选的）数据保密的支持。

下面我们来具体介绍一下 IPV6 技术。

1. Ipv6 的产生背景

传统的 IP，即 IPv4（IP version 4）定义 IP 地址的长度为 32 位，Internet 上每个主机都分配了一个（或多个）32 位的 IP 地址。32 位的地址在 DARPA 时代的互联网络看来还是足够使用的，同时网络地址的分类（A、B、C、D、E 类）和提取也提高了路由的效率。但是在 20 世纪 80 年代早期，即使是最有远见的 TCP/IP 开发者们也没有预料到互联网会有后来的爆炸性的增长。Internet 的设计者们没有想到今天 Internet 会发展到如此大的规模，更没有预测到今天 Internet 因为发展规模所陷入的困境。1987 年统计表明可能将来需要分配多达 100,000 个网络，然而早在 1996 年这个记录已经被打破。自从 1992 年以来，特别是 WWW 服务普及之后，网络节点的数目开始几何级数的增长。

址短缺问题的根源有绝对的一面也有相对的一面。绝对的一面就是 32 位的空间是十分有限的；相对的一面就是，尽管现行的 32 位 IPv4 的地址结构可以为 1670 万个网络上的超过 40 亿台的主机分配地址，但实际上的地址分配效率远远达不到这个数值，甚至在理论上也不可能。网络增长不仅导致地址总数量的不够，也导致路由表的迅速膨胀。

在 IPv4 面临的一系列问题中，IP 地址即将耗尽无疑是最为严重的，有预测表明，以目前 Internet 的发展速度计算，所有 IPv4 地址将在 2005 ~ 2010 年间分配完毕。为了彻底解决 IPv4 存在的问题，IETF 从 1995 年开始，着手研究开发下一代 IP 协议，即 IPv6。IPv6 具有长达 128 位的地址空间，可以彻底解决 IPv4 地址不足的问题，除此之外，IPv6 还采用分级地址模式、高效 IP 包头、服务质量、主机地址自动配置、认证和加密等许多技术。

2. Ipv6 的头部结构

IPv6 使用了固定长度为 40 字节的头部。另外，可附接不同的扩展头部。每个头部的长度是 8 字节的倍数。IPv6 没有定义尾部。如图 1 所示显示了基本头部的格式。

（1）版本

在所有 IPv6 数据报中将该域置成 6。

（2）优先级

紧接版本域之后的 4 比特指示优先级。利用优先级域，首先区分两大业务量（traffic）：

* 受拥塞控制的（congestion-controlled）业务量；
* 不受拥塞控制的（noncongestion-controlled）业务量。

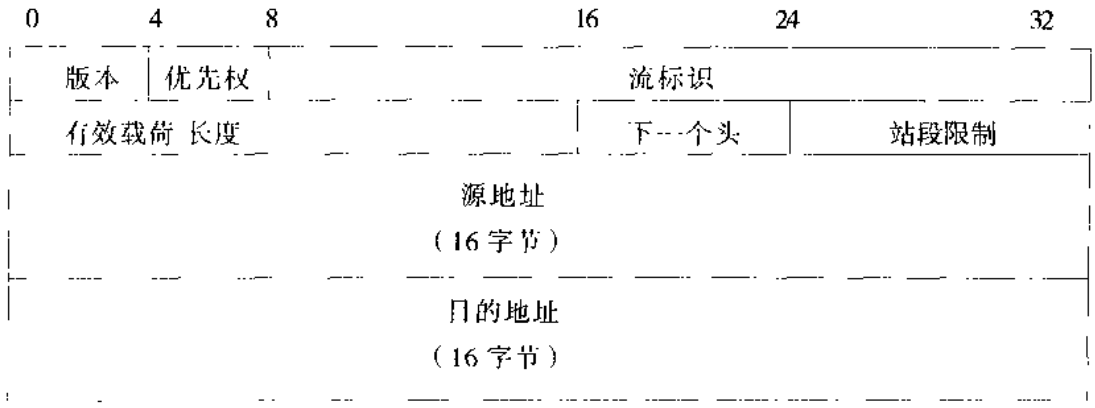

图 1　IPV6 固定的头部

在 IPv6 规范中 0 ~ 7 级的优先级为受拥塞控制的业务量，这种业务量的最低优先级为 1，Internet 控制用的业务量的优先级为 7（参阅图 2）。

不受拥塞控制的业务量是指当网络拥塞时不能进行速率调整的业务量。对时延要求很严的实时话音即是这类业务量的一个示例。在 IPv6 中，通常将其值为 8 ~ 15 的优先级分配给这种类型的业务量。

0	无特殊优先级
1	背景（background）业务量（例如网络新闻）
2	零散数据传送（如电子函件）
3	保留
4	边续批量传送（例如 FTP，NFS）
5	保留
6	会话型业务量（例如 Telnet 及宣窗口系统）
7	Internet 控制业务量（例如寻路协议及 SNMP）

图 2　受拥塞业务量中的 IP 优先级

（3）流标识

一个流由其源地址、目的地址和流序号来命名。在 IPv6 规范中对流作如下定义："流是指从某个源点向（单目或组播的）信宿发送的分组群中，源点要求中间路由器作特殊处理的那些分组"。换句话说，流是指源点、信宿和流标记三者分别相同的分组的集合。任何的流标记都不得在此路由器中保持 6 秒以上。此路由器在 6 秒之后必须删除高速缓存（cache）中的登录项，当该流的下一个分组出现时，此登录项被重新学习。并非所有的分组都属于流。实际上从 IPv4 向 IPv6 的过渡期间大部分的分组都不属于特定的流。例

如，SMTP、FTP 以及 WWW 浏览器等传统的应用均可生成分组。这些程序原本是为了 IPv4 而设计的，在过渡期为使 IPv4 地址和 IPv6 地址都能处理而进行了改进，但不能处理在 IPv4 中不存在的流。在这分组中应置入由 24 比特 0 组成的空流标记。

（4）有效载荷长度域

有效载荷长度域指示 IP 基本头标以后的 IP 数据报剩余部分的长度，单位是字节。此域占 16 比特，因而 IP 数据报通常应在 65535 字节以内。但如果使用 Hop By Hop 选项扩展头标的特大净荷选项，就能传送更大的数据报。利用此选项时净荷长度置 0。

（5）下一个头标

下一个头标用来标识数据报中的基本 IP 头标的下一个头标。在此头标中，指示选项的 IP 头标和上层协议。表 1 列出了主要的下一个头标值。其中一些值用来标识扩展头标。

表 1　IP 下一个头标值

0	中继点选项头标
4	IP
6	TCP
17	UDP
43	寻路头标
44	报片头标
45	IDRP
46	RSVP
50	封装化安全净荷
51	认证头标
58	ICMP
59	无下一个头标
60	信宿选项头标

（6）站段限制

站段限制决定了能够将分组传送的距离。主机在生成数据报时，在站段限制域中设置某一初值，然后将数据报送到网上的路由器。各路由器从该值起逐次减 1。如数据报到达信宿之前其站段限制变为 0，该数据报就被抛弃掉。使用站段限制有两个目的：一是防止寻路发生闭环（loop）。因 IP 不能订正路由器的错误信息，故无法使此数据报到达信宿。在 IP 中可以利用站段限制来防止数据报陷入寻路的死循环中；二是主机可利用它在网内进行检索。利用它，PC 可向其中任意一个服务器发送数据报，但为了减轻网络负荷，PC 希望搜索到离它最近的服务器。

（7）源地址和目的地址

基本IP头标中最后2个域是信源地址和目的地址。它们各占128比特。在此域中可置入数据报最初的源地址和最后的目的地址。

3. IP扩展头标

IPv4头标中存在可变长度的选项，利用它可以处理具有指定路径控制、路径记录、时间标记（time stamp）和安全等选项的特殊分组。但因这种分组会影响网络的性能，故此选项逐渐被废弃。根据IPv4的运用经验，IPv6中规定了使用扩展头标（extention header）的特殊处理。扩展头标加在IP分组的基本头标之后。IPv6（extention header）规范中定义了若干种不同的扩展头标（表1）。它们由下一个头标域的值来标识。每种头部都是可选的，但一旦有多于一种头部出现时，它们必须紧跟在固有头部之后，并且最好按下列次序排序。

表2　IPV6扩展头部

扩展头部	描述
站接站选项	用于路由器的各种信息
路由选择	后面跟有完整的或者部分的路由
分段	数据报分段管理
身份验证	发送者标识的验证
加密的安全性有效载荷	有关加密内容的信息
目的地选项	有关目的地的附加信息

* 站接站选项（hop-by-hop options header）：运载每个IP路由器必须解释的选项信息；例如它可以用于传送超大有效载荷信息。

* 路由选择头部（routing header）：定义了该包必须经过IP路由器（也称为源路由）。

* 分段头部（fragment header）当传送的用户数据大于有效载荷所能允许的最大长度时便要用到分段头部，分段头部传送了有效载荷携带的用户数据段在整个用户数据单元中的偏移量。

* 身份验证头部（authentication header）：可选的认证信息。

* 加密的安全性有效载荷（encapsulating security payload header）：传送有效载荷的额外保护信息。

* 目的选项头部（destination options header）：运载着仅为目的站检查用的可选信息。

4. IPv6的表示方法

IPv6地址拥有128位，故采用了一种不同于IPv4点分十进制的文本表示法。推荐的格式是将地址写成8个由“:”分开的十六进制数，例如1080:0:0:0:8:800:200C:417A。一组十六进制值0可简单压缩成“::”，但是这只能在串中出现一次，例如1080::8:800:200C:417A。