本书编写委员会　编著

電子工業出版社
Publishing House of Electronics Industry
URL:http://www.phei.com.cn

98

e网打尽

网上安全与防毒

本书编写委员会　编著

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

内容简介

随着Internet和Intranet的迅速发展，计算机网络对安全的要求已经越来越高。当今，网络技术已被广泛应用于社会生活直至军事战略等各个方面，因此网络安全问题已超越其本身而达到国家安全问题的高度。

本书介绍了计算机网络的各种基本知识、网络安全的概念、黑客的概念、计算机病毒知识和防范技术、电子邮件攻击、防火墙技术等，详细讲述了两款最流行的杀毒软件：超级巡捕KV3000和瑞星2001版。本书从普通用户的角度出发，在内容的编写上着重讲述与用户个人密切相关的内容，使用户对网上安全与防毒有一个整体认识，从而有效地防止和处理他人的攻击和病毒的攻击。

本书图文并茂，循序渐进，讲解清晰，适合于初学者和培训班学员使用。

图书在版编目（CIP）数据

网上安全与防毒 /《网上安全与防毒》编写委员会编著. -北京：电子工业出版社，2001.8
（e网打尽）
ISBN 7-5053-6989-X

Ⅰ.网… Ⅱ.网… Ⅲ.①计算机网络—安全技术 ②计算机病毒—防治 Ⅳ.TP393.08

中国版本图书馆CIP数据核字（2001） 第057454号

丛 书 名：e网打尽
书　　名：**网上安全与防毒**
编 著 者：本书编写委员会
责任编辑：梁卫红
排版制作：今日电子公司制作部
印 刷 者：北京市增富印刷有限责任公司
出版发行：电子工业出版社 www.phei.com.cn
北京市海淀区万寿路173信箱 邮编：100036
经　　销：各地新华书店
开　　本：787 × 980 1/16 印张：13.25 字数：305千字
版　　次：2001年8月第1版 2001年8月第1次印刷
书　　号：ISBN 7-5053-6989-X / TP · 4002
定　　价：19.00元

序

在“e网”世界里自由翱翔

“世界”变得如此之小，无限风光近在咫尺。

“空间”变得如此之小，地球村里的人们不再发出天高地迥的感喟。

世界也同时变得如此之大，绚丽多姿、五光十色的事物浩浩荡荡、横无际涯，如不尽长江滚滚来。在新世纪来临之际，我们已进入了伟大的“网络”信息时代。

从结绳记事到电子计算机，人类走过了漫长坎坷的探求之路，终于在20世纪末缔造了一个信息传播的奇迹——Internet（因特网）。它是世纪的骄子，技术的宠儿，人类的智慧。Internet已经改变了人类世界；Internet正在改变着世界人类；Internet还将以更快的速度、更大的规模、更加磅礴的气势改变整个人类和世界。

咫尺屏幕将整个世界展现在您面前。四海波涛、五洲风雷，点击间尽收眼底。南国椰风、北疆冰雪，敲打间俱入眸中；政坛乍变、商场硝烟，凝视中已经了然于胸；绿茵健影、影视趣闻，谈笑中已经悦情尽享。

我们不再孤独，Internet把不同地域、不同种族、不同语言的兄弟姐妹“联”在了一起。我们不再弱小，Internet把有限聚集起来成为澎湃汹涌的无限，使个体生命感到从此傲然于天地之间，不再畏葸和恐惧。我们不再局限，小国寡民的男耕女织演变成为世界的现代文明。我们不再被束缚，Internet正帮助我们摆脱种族的歧见、地域的狭窄、分工的不同、贫富的悬殊。我们正从有形和无形的奴役中走出来，迈向真正的自由空间。

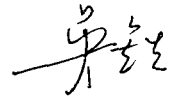
Internet使四海一家，它将“平等”一词赋予了前所未有的崭新含义。我们在Internet前，或平静、或安宁、或兴奋、或激动。Internet将真实的世界虚拟，又将虚拟的世界还原为真实，从来没有哪种技术手段使我们获得如此巨大的自由。您是真实的您，又是虚拟的您。我是我，我又是非我。我们的思想可以天马行空，漫游九垓，纵横驰骋于“e网”世界。

“e网打尽”——打尽外部世界的一切信息；打尽网络技术的一切内容。

“e网打尽”系列，是本丛书编创人员精心设计、精心施工的作品。我们带着美好的祝福，将这套最适用的丛书献给您，为您成为“网络高手”铺路搭桥。

掌握“e网”技术，不但获得了21世纪的工作签证，而且拥有了世界公民的无纸认证。洲界、国界，在鼠标移动的方寸之间早已不复存在。

本书编委会主任



原中国计算机用户协会网络分会副理事长

e网打尽

编写委员会

主　　任　吴金生　原中国计算机用户协会网络分会副理事长

委　　员

（按姓氏笔划顺序排列）

史美林　清华大学计算机科学与工程系教授、博士生导师

申江婴　《中国网友报》主编

陈宗周　《电脑报》社长

吴朝晖　浙江大学计算机科学与工程系副主任、教授、博士生导师

鲍　泓　北京联合大学信息学院教授

编写成员　巩　英　丁　磊　李　华　单　盈　于鲁泉

张　彬　袁建洲　刘亚秋　吕云峰　刘宗键

梁兴东　刘丽芳

编辑委员会

主　　任　杜振民　电子工业出版社副社长

副 主 任　文宏武　电子工业出版社副社长

编辑成员　谭海平　徐津平　焦桐顺　李秦华　张月萍　窦　昊

郝志恒　梁卫红　赵红燕　牛　勇　周宏敏

出 版 前 言

关于“e网打尽”

“网络”可以说是近代史上最为悬妙、发展最快、最难预测、最难把握，而且对人们的生活影响非常巨大的一章。“网络在下世纪一定会普及”、“网络就是计算机”、“计算机就是网络”、“明天就不再有网络公司了”……诸多的学者、专家、哲人在津津乐道地大胆畅想着网络的未来。但是很少有人能准确、全面地预计明天网络的“庐山真面目”。

有一点是明白无误的，即网络正深入地渗透到我们生活的方方面面。把握住今天，把握住网络，才有基础、有条件去畅想明天！这里的“把握”并不是希望大家都成为网络行家里手。了解网络的意义、知道网络的作用、能够使用网络的基本功能是不是“把握”呢？我们的回答是肯定的！在专家和外行之间有一条快捷、实用的“链接”，只要轻触它，便可很容易地把握网络、把握明天！

帮助读者了解网络，与读者一起学会最简单、最基础的网络使用知识——即简单地“把握”住网络，便是我们这套丛书的出版目标。起名“e网打尽”，我们借用了成语“一网打尽”的谐音。显然我们不是要“打鱼”，也不是要读者对网络“尽详尽知”。我们想告诉读者，这套书籍介绍的是“网络”——“e网”，并且包括了日常使用网络所需要的各种常用知识和经验——“打尽”。

本丛书的读者对象

本套丛书是为普通读者编写的。阅读本书只需具备中等及其以上的文化水平，不需要高深的计算机和网络专业知识。只要会操作计算机、具备基本的上网条件（拨号上网或通过局域网上网），便可以参考、阅读本书，学会和掌握在网上冲浪的各种技巧。

本丛书的编委和作者

为了保证本套丛书在贴近大众、方便实用的同时保证技术的准确性，我们聘请了国内著名的计算机专家和教育专家、计算机与网络专业媒体出版专家组成本书的编委会。编委会对本书的体系结构、写作风格、篇幅以及内容的详简等都提出了认真可行的建议和要求。在书籍手稿脱稿后他们又抽时间审阅了部分内容，为书籍质量的保证做出了贡献。

本套丛书的作者多是从事计算机教育、研究和工程工作的专家、学者，有着深厚的技术理论根底，同时又具有丰富的教学和写作经验。他们以很高的热情和高度的负责精神，使本书能在较短的时间内完成。在此，我们向本丛书的编委成员和作者们表示由衷的感谢。

本丛书的特点

本着尊重认知规律、注重实践、注重实用的原则，本套丛书采用了“面向应用、面向任务”

的写作风格。从实例出发，一边介绍实例或实际应用，一边介绍相关软件的使用方法和简单原理。

在内容的组织上，由于所用工具等方面的局限（例如大量网上工作都使用IE浏览器），个别书籍在内容上有少量重复，具体内容请见每本书的内容简介和“导读”。读者可根据需要，有选择地选购本套丛书中的一部分。

本丛书声明

本丛书中介绍或提及的网址或链接，仅作为资料和帮助读者理解网络使用之用，不含有任何宣传或贬低的含义，也无优劣、高低的分类或排序。如果其中的网址或内容发生变化或其他情况，给读者造成不便，我们谨表歉意。

欢迎读者反馈信息

出版社离开了读者，就像鱼儿离开了水。我们非常重视读者对我们书籍的评价，真诚地希望读者能把有关的意见和建议反馈给我们。反馈信息请寄ET@PHEI.COM.CN（看完本系列丛书后，肯定不需要再用传统手段来交流了吧！）

电子工业出版社

《网上安全与防毒》导读

Internet的迅速发展可谓有目共睹，但随之而来的网络安全问题越来越影响到了网络应用的各个方面，黑客的攻击、电子邮件炸弹、计算机病毒，尤如洪水猛兽，时时刻刻威胁着我们。

要防止他人的攻击，就必须了解网络的体系结构和网络的各层协议之间是如何工作的，以及一些网络安全的基本概念。

本书介绍了关于网络安全和病毒防护等方面的内容，包括了Internet的安全状况、常见的攻击方法、Internet安全防范技术和相关法律法规等。通过本书的学习，读者应当对网络安全有一个整体的认识，并能够有效地防止和处理他人的攻击和病毒的攻击。

本书由下列人员共同编写：孙弘洋、程波、赵金海、李伟兵、赵忠、向峰、王建平、刘卫国、孙德胜、付楷、李沙、武为仁、高德华、黎平、吴运佳、宋红燕、朱丽、张福海等。

目　　录

第 1 章

Internet 基础

本章要点

- Internet 历史与现状
- Internet 基本知识
- Internet 服务
- Internet 技术要素

本章将介绍 Internet 的一些基础知识，包括 Internet 的现状、技术要素和常用的服务。这些知识有助于读者理解网络安全。

1.1 Internet 历史与现状

Internet 的迅速发展可谓有目共睹。Internet 从 1969 年开始，最初起源于军事领域应用的目的。直到 1993 年以后，才开始应用于商业。它的发展速度是惊人的，现在，它已经覆盖了 175 个国家和地区，上网机器达数千万台，而用户数量已达到几亿人。

我国国内 Internet 的发展也是极其迅速的。1987 年 9 月 20 日，钱天白教授发出我国第一封电子邮件“越过长城，通向世界”，拉开了中国人使用 Internet 的序幕。而后的这十几年里，国内 Internet 的发展日新月异。我们可以看看下面的时间表：

- 1993 年 3 月 2 日，中国科学院高能物理研究所租用 AT&T 公司的国际卫星信道接入美国斯坦福线性加速器中心（SLAC）的 64k 专线正式开通。专线开通后，美国政府以 Internet 上有许多科技信息和其他各种资源，不能让社会主义国家接入为由，只允许这条专线进入美国能源网而不能连接到其他地方。尽管如此，这条专线仍是我国部分连

入 Internet 的第一条专线。专线开通后，国家自然科学基金委员会大力配合并投资 30 万元，使各个学科的重大课题负责人能够拨号连入高能物理研究所的这条专线，几百名科学家得以在国内使用电子邮件。

- 1994 年 4 月 20 日，NCFC 工程通过美国 Sprint 公司连入 Internet 的 64k 国际专线开通，实现了与 Internet 的全功能连接。从此我国被国际上正式承认为有 Internet 的国家。此事被我国新闻界评为1994年中国十大科技新闻之一，被国家统计公报列为中国1994年重大科技成就之一。
- 1995 年 5 月，中国电信开始筹建中国公用计算机互联网（CHINANET）全国骨干网。
- 1995 年 7 月，中国教育和科研计算机网（CERNET）连入美国的 128k 国际专线开通。
- 1995 年 8 月 8 日，建在中国教育和科研计算机网（CERNET）上的水木清华 BBS 正式开通，成为中国大陆第一个 Internet 上的 BBS。
- 1996 年 1 月，中国公用计算机互联网（CHINANET）全国骨干网建成并正式开通，全国范围的公用计算机互联网络开始提供服务。
- 1997 年，中国公用计算机互联网（CHINANET）实现了与中国其他 3 个互联网络（即中国科技网（CSTNET）、中国教育和科研计算机网（CERNET）、中国金桥信息网（CHINAGBN））的互联互通。

现在我国上网情况如下：

- 上网计算机数达到 650 万台，其中专线上网计算机 101 万台，拨号上网计算机 549 万台。
- 上网用户人数为 1690 万，其中专线上网的用户人数约为 258 万，拨号上网的用户人数约为 1176 万，同时使用专线与拨号的用户人数为 256 万。
- 除计算机外同时使用其他设备（移动终端、信息家电）上网的用户人数为 59 万。
- CN 下注册的域名数为 99734。
- 国际线路的总容量为 1234M。

1.2 Internet 技术要素

庞大的 Internet 由以下几个技术要素构成：

- 使用了一个统一有效的网络互联协议族 TCP / IP。
- 在 TCP / IP 之上开发了许多出色的服务软件。
- 采用主干 - 地区 - 园区的分层网络结构。
- 较早利用光缆，保持了信息传输通畅。
- NSFnet 作为主干网络，连接大学和科研机构。

在这些要素中，TCP / IP 协议族是最基本的。TCP / IP 协议族中的协议共同工作，提供对 Internet 上数据传输的支持。也可以这么说，这些协议几乎提供了当今 Internet 上所有的实用服务，在 1.1.3 节中将会有这些服务的简单介绍。

TCP / IP 族可以分为两类，下面分别介绍。

一、网络层协议

网络层协议管理数据传输的具体结构，这些协议在系统一级运行，对于用户一般是不透明的（不可见的）。

比如IP（网际）协议。IP是无连接的、不可靠的数据报协议，主要负责在主机之间寻址和选择数据包的路由。

无连接意味着交换数据之前不能建立会话。不可靠意味着传递没有担保。IP总是尽力传递数据包。IP数据包可能丢失、不按顺序传递、重复或延迟。IP不尝试从这些错误类型中恢复。所传递的数据包的确认以及丢失数据包的恢复是更高层协议的责任，如 TCP。

IP 数据包，也称作 IP 数据报，由 IP 报头和 IP 负载组成，如图 1-1 所示。

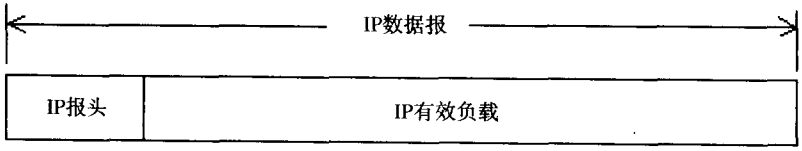


图 1-1　IP 数据包的格式

IP 报头包含表 1-1 所示的字段用于寻址和路由。

表 1-1　IP 报头字段及其功能

IP 报头字段	功能
源 IP 地址	IP 数据报最初的源 IP 地址
目标 IP 地址	IP 数据报最终的目标 IP 地址
生存时间（TTL）	指定数据报被路由器丢弃之前允许通过的网段数量。TTL是由发送主机设置的，以防止数据包不断在IP互联网络上永不终止地循环。转发 IP 数据包时，要求路由器至少将 TTL 减小 1

除非用户使用一些监听工具（比如 Sniffer），否则用户不会看到系统中 IP 的工作。

为使数据的路由选择和传递成为可能，连接到Internet上的计算机都必须有一个惟一的地址，也就是 IP 地址。

每个 TCP / IP 主机由逻辑 IP 地址标识。这个地址对每个使用 TCP / IP 通讯的主机来说是惟一的。每个32位IP地址标识网络上系统的位置，就像街道地址标识城市街道上的住宅一样。每个 IP 地址内部都分成两部分，网络 ID 和主机 ID：

- 网络ID，也叫做网络地址，标识大规模TCP / IP网际网络（由网络组成的网络）内的单个网段。连接到并共享访问同一网络的所有系统在其完整的IP地址内都有一个公用的网络ID。这个ID也用于惟一地识别大规模的网际网络内部的每个网络。
- 主机ID，也叫做主机地址，识别每个网络内部的TCP / IP节点（工作站、服务器、路由器或其他TCP / IP设备）。每个设备的主机ID惟一地识别所在网络内的单个系统。

下面是一个32位IP地址的例子：

10000011 01101011　00010000 11001000

要简化IP地址，IP地址用带句点的十进制符号表示。32位IP地址分成4个8位字节。8位字节数转换成十进制数（基数是10的编号系统），并用英文句号分隔。因此，前面的IP地址范例转换成带句点的十进制数就是131.107.16.200。

Internet团体定义了5种类型的地址：A类、B类和C类地址，用于指派TCP / IP节点，D类、E类保留。

地址类定义了每个地址的网络ID和主机ID使用哪些位。地址类还定义了每个网络能支持多少网络和主机。

表1-2用w.x.y.z指定任意给定IP地址中的4个8位字节数。这个表用于显示：

- 任意给定IP地址的第1个8位字节数（w）如何有效地表示地址类。
- 地址中的8位字节数如何分成网络ID和主机ID。
- 每个网络可用于每个类的可能网络和主机数量。

表1-2　IP地址类定义结构

类别	W的值	网络ID	主机ID	网络数量	每个网络的主机数量
A	1~126	w	x.y.z	126	16777214
B	128~191	w.x	y.z	16384	65534
C	192~223	w.x.y	z	2097152	254
D	224~239	为多播寻址保留	N/A	N/A	N/A
E	240~254	为实验性应用保留	N/A	N/A	N/A

因为IP地址标识网络上的设备，所以网络上的每个设备都必须分配惟一的IP地址。通常，多数计算机只安装一个网卡，因此只需要一个IP地址。如果计算机安装了多个网卡，则每个适配器都需要自己的IP地址。

显然，IP地址是难以被用户记住的。于是，Internet允许为每台计算机命名，并允许用户通过输入计算机名字来代替其IP地址。为了实现计算机名到IP地址的转换，Internet提供了专门的服务：DNS（Domain Name System）。

计算机在Internet上的名称称为域名（Domain Name）。下面就是一台服务器的域名：