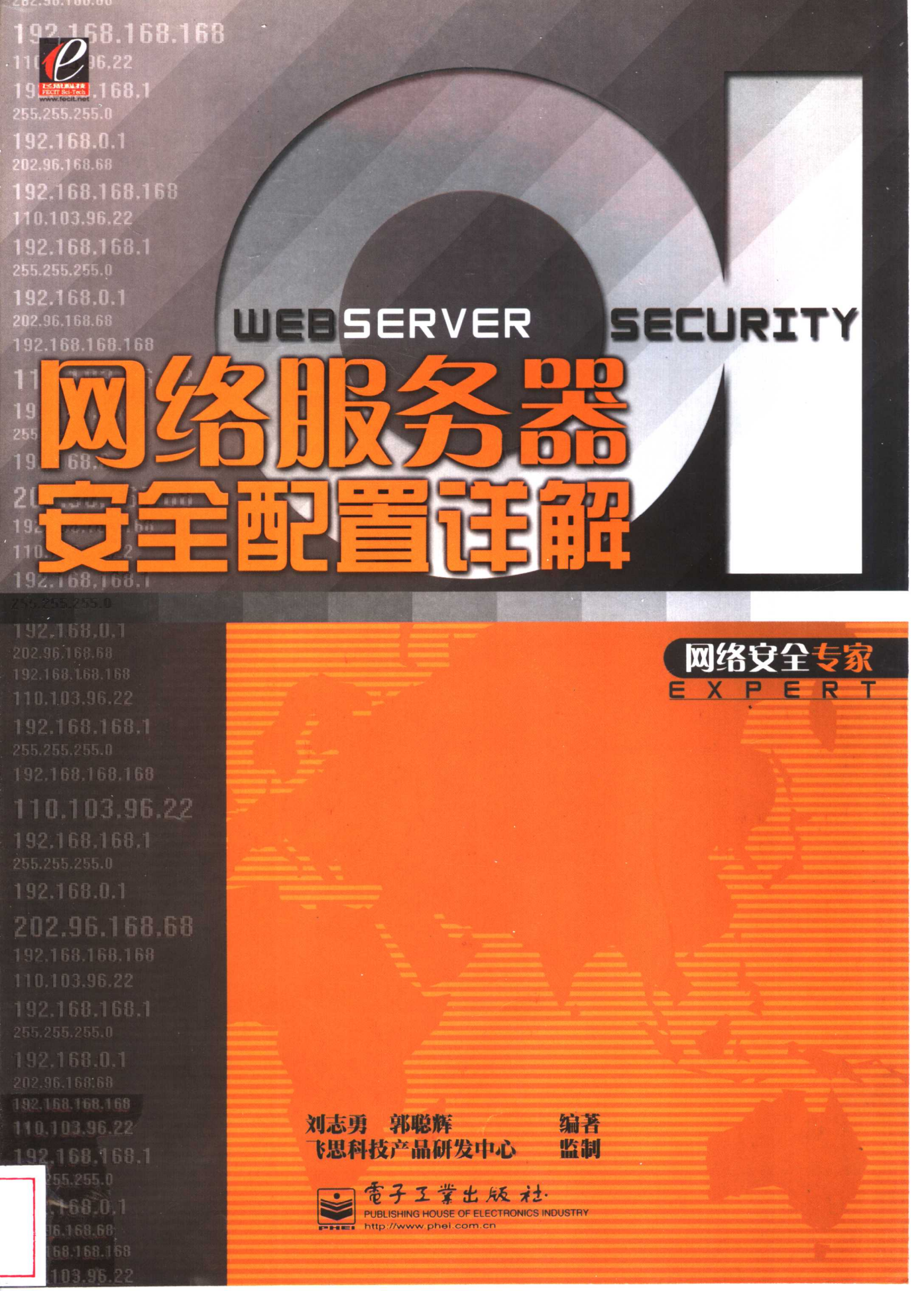
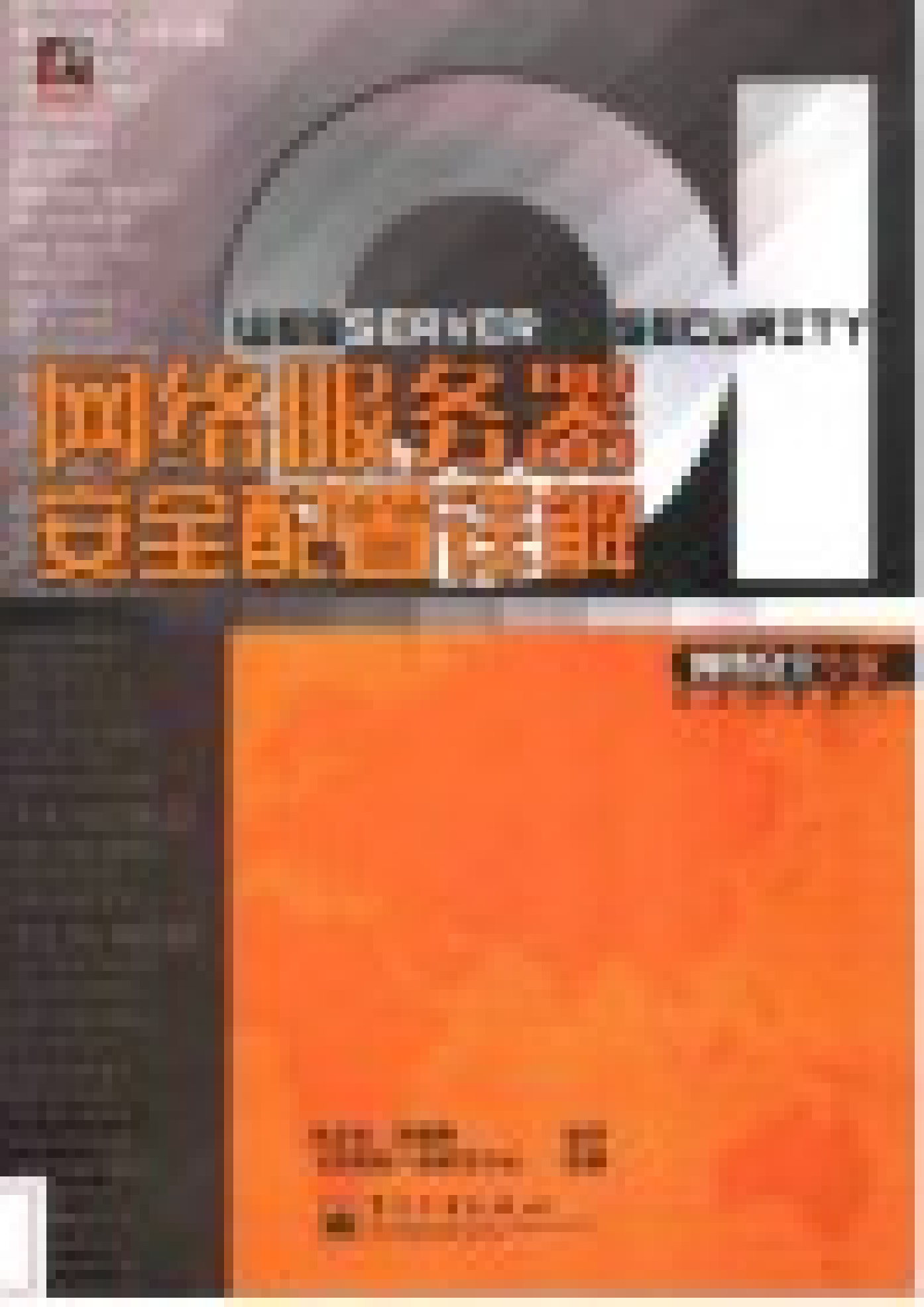

WEB SERVER SECURITY
网络服务器
安全配置详解
网络安全专家
EXPERT
刘志勇 郭聪辉 编著
飞思科技产品研发中心 监制
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn


网络服务器
安全配置

网络安全专家

网络服务器安全配置详解

刘志勇　郭聪辉　编著

飞思科技产品研发中心　监制

電子工業出版社

Publishing House of Electronics Industry

北京·BEIJING

内 容 简 介

本书以介绍网络服务器的安装和安全性配置等相关知识为主，针对时下三大主流操作系统：Linux、Windows 2000 Server 和 FreeBSD，详细介绍了它们的特点、性能和安装方法，讲解了相关的安全问题，以及如何进行安全配置和日常管理等内容。书中提供了翔实的案例和操作细节。通过本书的阅读，读者能够在企业网、校园网等实际应用中根据系统需求制定出有效的安全措施以实现网络系统的安全与管理。

本书适合系统管理员、网络管理员及对网络与系统安全感兴趣的计算机爱好者阅读。

图书在版编目（CIP）数据

网络服务器安全配置详解 / 刘志勇，郭聪辉编著. －北京：电子工业出版社，2004.3

（网络安全专家）

ISBN 7-5053-9504-1

Ⅰ.网... Ⅱ.①刘...②郭... Ⅲ.网络服务器－安全技术 Ⅳ.TP368.5

中国版本图书馆 CIP 数据核字（2003）第 119896 号

责任编辑：杨 鸽

印 刷：北京东光印刷厂

出版发行：电子工业出版社

北京海淀区万寿路 173 信箱 邮编：100036

经 销：各地新华书店

开 本：787×1092 1/16 印张：27 字数：691.2 千字

印 次：2004 年 3 月第 1 次印刷

印 数：5 000 册 定价：36.00 元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系电话：010-68279077。质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

前　言

21 世纪，信息化浪潮如日中天，它描绘了新世纪 e 时代的壮丽画卷。计算机网络信息技术如黄河之水天上来，不管人们对信息化持什么样的态度，我们都不得不迎接它汹涌而至的浪潮。

在 20 世纪 80 年代，随着网络进一步平民化、商业化，最终，它提供了自 20 世纪 50 年代以来的新信息革命后的一次伟大转机，计算机网络逐步取代电脑成为信息社会的技术核心，也就是说，电脑是网络的终端，网络并不是电脑的外围。这一革命性的变化演绎出了网络时代的意义，网络不仅能够传递信息，还能在信息存储和转换、信息处理和信息收发等方面扩展自身的功能。放眼全球，Internet 几乎遍及世界上每一个角落，由 60 多万个网络、几千万台主机组成，为上亿用户提供多样化的网络和信息服务。在信息化社会，网络信息系统已经在政治、电信、商业、金融、工业、文教、军事、交通等各方面发挥着越来越大的作用，现今社会对计算机网络信息系统的依赖程度也日益增加。

得益于网络信息系统的不断完善，敏感信息和无形财富日趋高度集中于计算机中。网络信息系统依靠计算机网络接收和处理信息，从而达到其相互间的联系和对目标的管理、控制的目的。现代信息社会的一个重要特征是以网络方式获得、交流信息。网络正在以前所未有的规模改变着人们的工作和生活方式。

随着网络的开放性、共享性、互联性的进一步扩大，特别是 Internet 的出现，以及 Internet 之后出现的 Intranet，网络的重要性和对社会的影响越来越凸现出来。网络上各种新业务的兴起，如电子商务、电子出版、数字图书馆、电子货币等，这些网络信息技术给人们带来了便利，但也留下了许多安全隐患，如病毒、黑客活动等的攻击和破坏，造成信息的泄密和巨大的经济损失，信息安全问题在今天已经成为关注的焦点。

很多组织现有的计算机网络大多数在建设之初都忽略了安全问题，即便考虑了这个问题，也只是简单地把安全机制建立在物理安全机制上，因此，随着网络的规模日趋扩大，这种安全机制对于网络环境来说就越来越形同虚设。另外，目前网络所使用的协议，在制定之初没有考虑安全方面的要求，自然也就没有安全性可言。计算机网络安全问题的主要根源就是其开放性和资源共享。它的安全性主要依赖加密、网络用户身份鉴别、存取控制策略等技术手段。

面对日趋严重危害网络系统的种种威胁，安全与保密的重要性要求越来越迫切，必须采取有力措施保证网络信息安全，满足保密的需要。一般来讲，网络安全措施分为三类：逻辑上的、物理上的和政策上的。仅仅利用物理上和政策上的手段防范黑客入侵，显得方法十分有限，实施也有一定困难。因此，必须高度重视采用逻辑上的措施，也就是运用网络安全技术保证安全。

即使有了非常完备的安全与保密的政策法规和非常先进的安全与保密技术，以及天衣无缝的物理安全机制，但如果这些得不到普及和应用，那么所有的努力都是白费。

服务器是网络信息系统的核心，其重要性不言而喻。一旦服务器被攻破，那么整个网络信息系统就暴露在光天化日下了。

在目前的网络系统中，核心是网络服务器操作系统，因此，操作系统的安全与否直接决定着信息是否安全，必须考虑主机的安全性问题。为此，电子工业出版社飞思科技产品研发中心

策划了这本书，以介绍时下主流网络服务器的安装和有关安全性方面的配置为主，针对实际威胁安全的因素，给出具体有效的解决方案，以达到网络整体安全的目的。本书分三部分，第一部分是 Linux 篇，第二部分是 Windows 2000 Server 篇，第三部分是 FreeBSD 篇。本书由刘志勇、郭聪辉主笔，李雪松、雷向利、刘峰、朱国伟、饶思贤、薛引峰等人参与了编写。由于作者水平有限，书中难免出现各种失误和不当，欢迎大家批评指正。

我们的联系方式：

咨询电话：（010）68134545　　68131648

答疑邮件：support@fecit.com.cn

网　　址：http://www.fecit.com.cn　　http://www.fecit.net

答疑网址：http://www.fecit.com.cn/下的“问题解答”专区

通用网址：计算机图书、FECIT、飞思教育、飞思科技、飞思

飞思科技产品研发中心

目　录

Linux 篇

Windows 2000 Server 篇

FreeBSD 篇

网络服务器安全配置详解

Linux 篇

第 1 章　UNIX 世界初探

Linux 是一个诞生于网络、成长于网络且成熟于网络的奇特的操作系统。1991 年，芬兰大学生 Linus Torvalds 萌发了开发一个“自由”的 UNIX 操作系统的想法。当年，Linux 就诞生了。为了不让这个羽翼未丰的操作系统夭折，Linus 通过 Internet 发布了自己的作品 Linux。从此一大批知名的、不知名的电脑黑客、编程人员加入到开发过程中来，使 Linux 逐渐成长起来。

Linux 一开始要求所有的源代码必须公开，并且任何人均不得从 Linux 交易中获利。然而，这种纯粹的自由软件的理想对于 Linux 的普及和发展是不利的，于是 Linux 开始转向 GPL，成为 GNU 阵营中的重要一员。

同时，Linux 作为 UNIX 家族的一员，许多特性与 UNIX 是相同的，它们之间的最大区别在于以下两点。

- UNIX 系统大多是与硬件配套的，而 Linux 则可运行在多种硬件平台上。
- UNIX 是商业软件，而 Linux 是自由软件，是免费并公开源代码的。

现在，Linux 凭借其优秀的设计、不凡的性能，加上 IBM、Intel、CA、Core、Oracle 等国际知名企业的大力支持，市场份额逐步扩大，逐渐成为主流操作系统之一。目前已经应用到以下各领域。

- 教育领域：设计先进、公开源代码这两大特性使得 Linux 成为了操作系统课的活教材。
- 网络服务器领域：稳定、健壮、系统要求低、网络功能强，这些优点使得 Linux 成为现在 Internet 服务器操作系统的首选，现已达到了 25%的市场占有率。
- 企业 Intranet：可以用低廉的投入架设 E-mail 服务器、WWW 服务器、代理服务器、透明网关、路由器。
- 视频制作领域：著名的电影《泰坦尼克号》中的特技效果就是由 200 多台 Linux 协作完成的。

下面我们就从 UNIX 开始，进入我们的 Linux 之旅。

1.1　UNIX 简介

UNIX 于 1969 年在美国的 AT&T 贝尔实验室诞生。在过去的 30 年里经过不断锤炼，它已经成为一个在网络功能、系统安全、系统性能等各个方面都非常优秀的操作系统，至今已风行了 30 多年。现在 UNIX 已演化出不同厂家的 20 多个分支 100 多个版本，成为世界上使用最普遍的操作系统之一。

在 UNIX 发展的早期，系统的源代码是公开的，但是从 Version 7 开始，AT&T 将 UNIX 商业化，更换了许可协议，不再公开系统的源代码，从而迈出了 UNIX 商业化的第一步。

从 20 世纪 70 年代末开始，在市场上出现了不同的 UNIX 商品化版本，比较有影响的版本包括：Sun 公司的 Sun OS、Microsoft、SCO 公司的 XENIX、Interactive 公司的 UNIX386/ix 和

DEC 公司的 Ultrix。后来陆续出现的比较著名的 UNIX 系统包括：IBM 公司的 AIX、HP 公司的 HP-UX、SCO 公司的 UNIX 和 ODT，以及 SUN 公司的 Solaris 等产品。

作为 UNIX 技术的发明者和拥有者，贝尔实验室和 AT&T 公司先后发布了一系列的 UNIX 版本，包括：Edition 1（1971 年）、Edition 3（1973 年）、Edition 6（1975 年）、Edition 7（1979 年）、PWB（1979 年）和 System Ⅲ（1981 年）、System Ⅴ（1983 年）、SVR 2（1984 年）、SVR 3（1987 年）、SVR 4（1989 年）等版本，其中，SVR 4 作为 AT&T 和 SUN 公司联合主推的工业化版本，得到了许多重要计算机厂商的支持，成为 UNIX 工业界的主流技术。

许多厂商在此技术基础上开发出自己的商业化 UNIX 产品。到 20 世纪 90 年代初，不同的 UNIX 版本已超过 100 种，形成了 UNIX 和类 UNIX 的操作系统种类繁多的局面。为了便于引用和区分，人们就将这些操作系统合称为 U*ix、*nix……后来，UNIX 分化出两大派系：AT&T System Ⅴ和 BSD UNIX。

现在，“UNIX”已经成为 X/OPEN 组织（一个 UNIX 标准化组织）的一个商标，任何操作系统只要通过了该组织的“UNIX 兼容性测试”，就可以称做“UNIX”。由于 Linux 符合 IEEE POSIX.1 的标准，源代码与 AT&T System Ⅴ和 BSD UNIX 相兼容，并且 Linux 通过了“UNIX 兼容性测试”，也就成了“UNIX”。但从传统意义上讲，Linux 与 AT&T System Ⅴ和 BSD UNIX 没有派生关系，因此不能称为“UNIX”，它只是一个遵循 IEEE POSIX.1 标准并扩展支持所有 AT&T System Ⅴ和 BSD UNIX 特性的操作系统。

1.2 UNIX 世界的新秀——Linux

Linux 是一个诞生于网络、成长于网络且成熟于网络的奇特的操作系统。1991 年 10 月 5 日，芬兰赫尔辛基大学的学生 Linus Torvalds 发往新闻组 comp.os.minix 的一封帖子，最早向全世界宣告了 Linux 的诞生。Linux 起源于 UNIX 的变种 Minix 和公开源码。Minix 是计算机科学家 Andrew Tanenbaum（1997 年图灵奖获得者）为了方便教学和研究，以 AT&T Edition V7 为蓝本，独立开发的基于 Intel i386 平台上的一个操作系统。该系统虽然在源代码级和 Edition Version 7 兼容，但是没有引用任何 UNIX 的代码，所以它不是传统意义上的 UNIX。但是 Tanenbaum 为教学科研目的，坚持保持 Minix 代码的“纯洁性”，拒绝将 Minix 用户对其所做的工作成果加入到 Minix 中。随后，作为自由软件倡导者的 Linus 以 Minix 为基础，开始动手撰写“类 Minix”的操作系统——这就是现代 Linux 的原始模型。后来 Linus 将该自由软件献给了 GNU。GNU 是自由软件积极倡导者 Richard Stallman 于 1984 年创立的一个完全基于自由软件的软件体系。它包含一份公共许可协议（General Public License，简称 GPL），其目标是开发一个完全免费的类 UNIX 系统及其应用程序。目前，众所周知的 BIND、Perl、Apache、TCP/IP 就是自由软件的经典之作。但是，GNU 开发的名为 Hurd 的类 UNIX 系统，在开发过程中遇到了较多困难而一再滞后。自 Linus 决定把他的 Linux 交给 GNU 的时候起，Linux 就由一个人的思想变成了无数志同道合的人的一场运动。Linux 填补了 GNU 应用软件系统平台的空缺，反过来，加入 GNU 极大地推动了 Linux 的发展。Linux 诞生多年来一直停留在 Hacker 和专家的圈子里，鲜为人知。直到 1998 年，随着 Linux 自身的完善，在公开源码潮流的推动下，Linux

终于登上了大众舞台。在 IBM、Oracle、Informix、CA、Sysbase、Corel、Intel、Netscape、Dell 等许多著名计算机软硬件厂商陆续宣布对 Linux 的支持后，Linux 一下子被推上了舆论的浪尖。Linux 的所有核心代码都是由 Linux Torvald 及其他全世界最优秀的程序员完全重写的，没有 AT&T System Ⅴ或 BSD UNIX 代码，然而它却继承了 UNIX 优秀的设计思想，同时拥有世界上最大的开发群体和测试队伍，这就使 Linux 拥有干净的、健壮的并且高效的内核。在其他各种 UNIX 主要用于科学工程及高端用户的同时，由于 Linux 是基于流行的 Intel i386 及在 GNU 的通用公共许可（GPL）保护下可以免费获得的特性，使得它在经历了 Internet 中众多用户苛刻考验后成为最流行的“UNIX”。

注：什么是自由软件？

自 1984 年起，麻省理工学院开始支持“世界最后一名黑客” Richard Stallman 在软件开发团体中发起的自由软件运动，从而自由软件基金会 FSF、GPL 协议和 GNU 项目就此诞生，掀开了自由软件革命的序章。

GPL（通用公共许可协议），这是与传统商业软件许可协议“CopyRight”对立的，所以又被戏称为“CopyLeft”。GPL 保证任何人有共享和修改自由软件的自由。任何人有权取得、修改和重新发布自由软件的源代码，并且规定在不增加附加费用的条件下任何人都可以得到自由软件的源代码。同时还规定自由软件的衍生作品必须以 GPL 作为它重新发布的许可协议。

而 GNU 项目的目标是建立可自由发布的、可移植的 UNIX 类操作系统。

在 2000 年的 LinuxWorld 大会上，可以明显地感觉到：社会各界对免费发布的操作系统的支持的力度大大增强了，特别是许多硬件厂商，如 IBM、HP 和 Dell 纷纷涉足 Linux 领域，极大地促进了这种操作系统的发展。

虽然，现在纷繁复杂的多种 Linux 发行版各自为营，降低了 Linux 的整体战斗力，但业界认为，不同的发行版本最终会产生不断细分的市场，各个版本将趋向于处理某一专业领域的东西。

Linux 操作系统经历过市场风暴的洗礼之后，已经逐步创造出更多的辉煌。

1.3 Linux 的特性

Linux 是一个真正的多任务、多用户的操作系统。它充分利用了 X86 CPU 的任务切换机制，实现了真正的多任务、多用户环境，允许多个用户同时执行不同的程序，并且可以分配优先级。而这个特性只有 Windows XP 实现了，之前的 Windows NT/2000 都不是真正的多任务、多用户的操作系统。

Linux 在源代码级和一定数量的 UNIX 兼容。Linux 是遵循 IEEE POSIX.1 标准开发的，它与 AT&T System Ⅴ和 BSD UNIX 在编程接口上兼容，也就是说，UNIX 下的许多应用程序可以方便地移植到 Linux 中。

Linux 支持多达 32 种文件系统。Linux 支持常见的 FAT16、FAT32、NTFS、ISO9660 等文件系统，也支持 Minix、ext、HPFS、sysv 等许多不常见的文件系统。

Linux 是一个提供完整网络集成的操作系统。Linux 内置 TCP/IP 协议，对于 Internet/Intranet