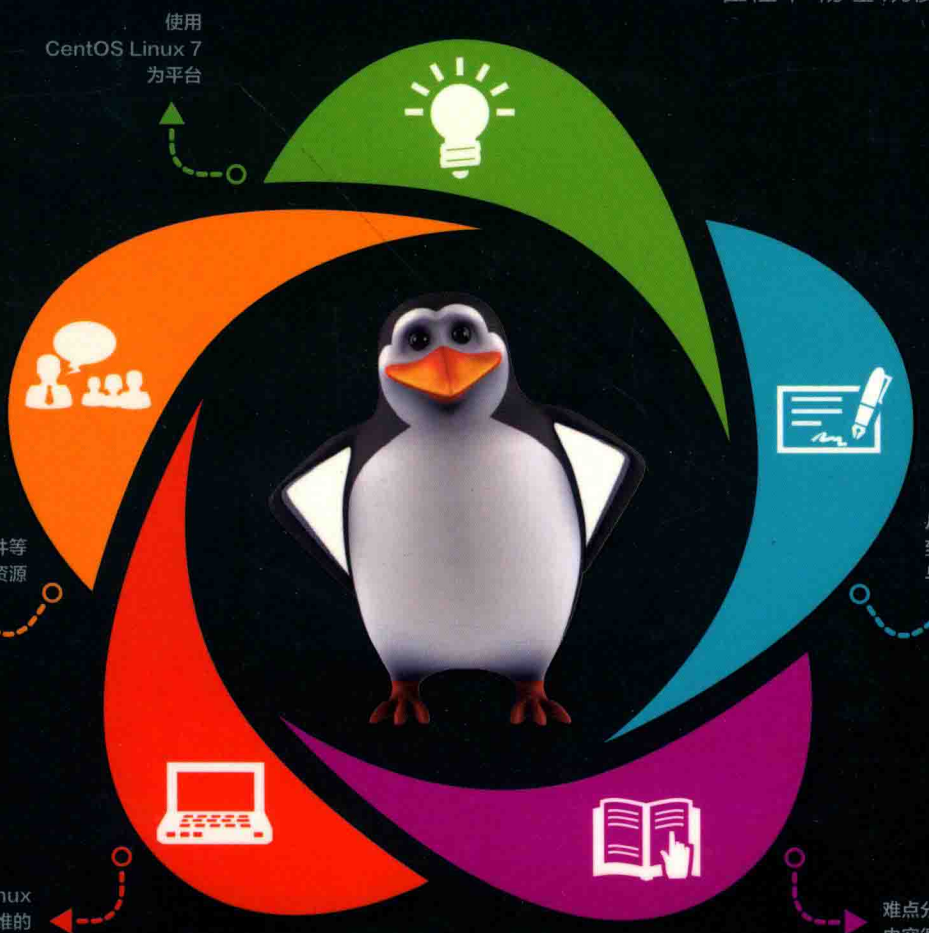
Linux
创新人才培养系列

CentOS Linux
系统管理与运维 第2版

◎ 张金石 钟小平 主编
◎ 翟社平 杨瑾 姚俊 副主编

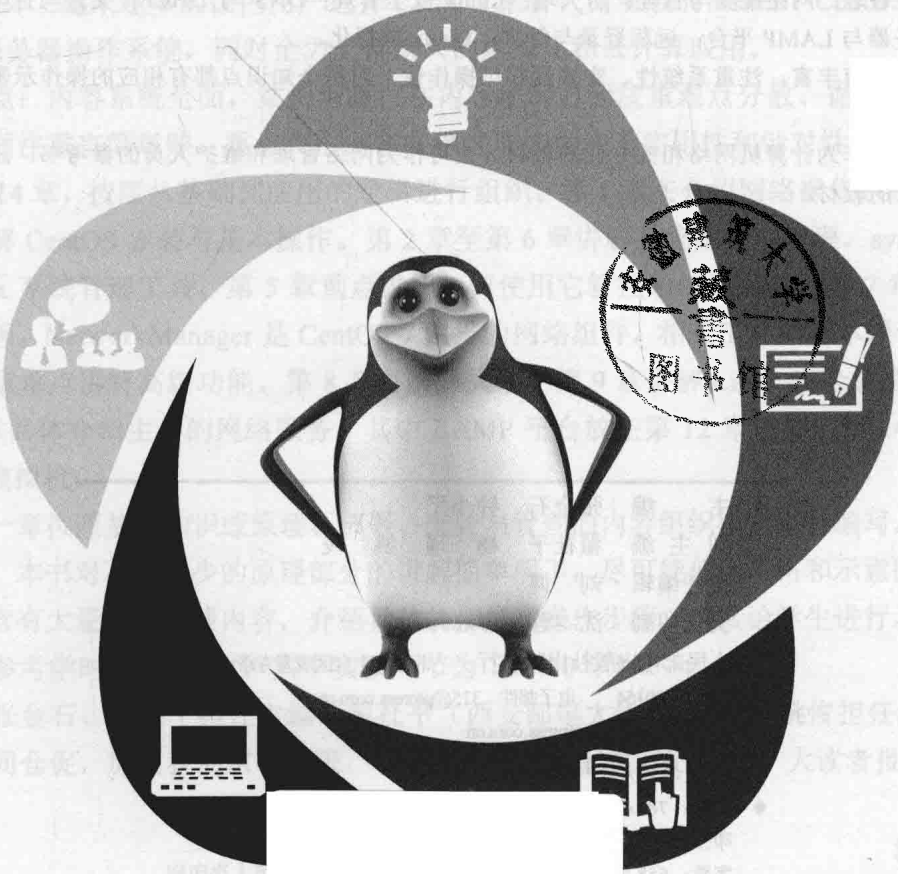


中国工信出版集团
人民邮电出版社
POSTS & TELECOM PRESS

Linux
创新人才培养系列

CentOS Linux
系统管理与运维 第2版

◎ 张金石 钟小平 主编
◎ 翟社平 杨瑾 姚俊 副主编



人民邮电出版社
北京

图书在版编目（CIP）数据

CentOS Linux系统管理与运维 / 张金石，钟小平主编. -- 2版. -- 北京 : 人民邮电出版社，2018.8
（Linux创新人才培养系列）
ISBN 978-7-115-48369-0

Ⅰ. ①C… Ⅱ. ①张… ②钟… Ⅲ. ①Linux操作系统
Ⅳ. ①TP316.89

中国版本图书馆CIP数据核字(2018)第088019号

内 容 提 要

本书基于网络工程和应用实际需求，以广泛使用的 CentOS Linux 7 平台为例，介绍网络操作系统的部署、配置与管理的技术方法。全书共 14 章，内容包括：CentOS 安装与基本操作；Linux 基本配置与管理；磁盘存储管理；Linux 进程、内核与硬件管理；systemd 管理与系统启动；系统性能监测与日志管理；网络配置与管理；防火墙；Linux 安全管理；DNS 与 DHCP；文件与打印服务器；Web 服务器与 LAMP 平台；远程登录与管理；Linux 虚拟化。

本书内容丰富，注重系统性、实践性和可操作性，对每个知识点都有相应的操作示范，便于读者快速上手。

本书可作为计算机网络相关专业的教材，也可作为网络管理和维护人员的参考书，还可作为各种培训班的教材。

◆ 主　　编　张金石　钟小平
副 主 编　翟社平　杨　瑾　姚　俊
责任编辑　刘　博
责任印制　沈　蓉　彭志环

◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路 11 号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
固安县铭成印刷有限公司印刷

◆ 开本：787×1092　1/16
印张：26.25　　2018 年 8 月第 2 版
字数：658 千字　　2018 年 8 月河北第 1 次印刷

定价：69.80 元

读者服务热线：(010)81055256　印装质量热线：(010)81055316
反盗版热线：(010)81055315

前　言

计算机网络已深入社会的各个领域，电信部门、研究部门、高科技企业乃至各行各业都对网络工程技术人才有迫切的需求，尤其需要熟练掌握网络规划、设计、组建和运维管理的高级应用型人才。

计算机网络是由硬件和软件两部分组成的，其中网络操作系统是构建计算机网络的软件核心和基础，是网络的心脏和灵魂。我国很多高等院校的网络相关专业都将“网络操作系统”作为一门重要的专业课程。为了帮助高等院校教师比较全面、系统地讲授这门课程，使学生能熟悉网络操作系统的原理，掌握网络操作系统的安装、设置和管理的方法、技能，同时考虑到越来越多的企业选择 Linux 平台，我们几位长期从事网络专业教学的教师共同编写了本书。

本书的系统平台选用 CentOS Linux 7。CentOS 是一个 Red Hat Linux 源代码的企业级 Linux 发行版本，越来越多的国内用户选择 CentOS 来替代商业版的 RHEL。CentOS 是优秀的 Internet 服务器操作系统，同时全力支持新兴的虚拟化和云计算应用。

本书特点：内容系统全面，结构清晰；在内容编写方面注重难点分散、循序渐进；在文字叙述方面注重言简意赅、重点突出；在实例选取方面注重实用性和针对性。

全书共 14 章，按照从基础到应用的逻辑进行组织。第 1 章在介绍网络操作系统知识的基础上，讲解 CentOS 安装与基本操作。第 2 章至第 6 章讲解系统配置与管理。systemd 是新一代 Linux 系统管理工具，第 5 章重点讲解如何使用它管控系统和服务。第 7 章介绍网络配置与管理，NetworkManager 是 CentOS 7 主推的网络组件，相关工具的基本操作在第 2 章讲解，本章重点讲解高级功能。第 8 章讲解防火墙。第 9 章讲解 Linux 安全管理。第 10 章至第 13 章具体介绍主要的网络服务，其中 LAMP 平台放在第 12 章讲解。第 14 章详细介绍 KVM 虚拟机。

本书每一章按照基础知识或原理、部署、配置与管理的内容组织模式进行编写。作为应用本科教材，本书对不可缺少的原理部分的讲解简单明了，尽可能使用表格和示意图。配置与管理部分含有大量动手实践内容，介绍具体的部署和操作步骤，直接给学生进行示范。

本书的参考学时为 48 学时，其中实践环节为 16～20 学时。

本书由张金石、钟小平担任主编，翟社平（西安邮电大学）、杨瑾、姚俊担任副主编。

由于时间仓促，加之我们水平有限，书中难免存在不足之处，敬请广大读者批评指正。

编　者

2017 年 2 月

目　录

第 1 章　CentOS 安装与基本操作

Linux 网络操作系统是实现网络关键性应用的理想选择。CentOS 是一个基于 Red Hat Linux 源代码的企业级 Linux 发行版本，许多要求高度稳定性的服务器用户选择 CentOS 来替代商业版的 Red Hat Enterprise Linux。本章向读者介绍 Linux 网络操作系统的基础知识，重点讲解 CentOS Linux 的安装和基本操作，以兼顾 Linux 操作系统入门读者。

1.1　网络操作系统概述

计算机网络是由硬件和软件两部分组成的，其中网络操作系统是构建计算机网络的软件核心和基础。网络操作系统与单机操作系统之间并没有本质的区别，仅仅是增加了网络连接功能和网络服务，是面向网络提供服务的特殊操作系统。由于网络操作系统是运行在服务器之上的，所以有时也将它称为服务器操作系统。

1.1.1　网络操作系统的概念

严格地说，单机操作系统只能为本地用户使用本机资源提供服务，不能满足开放的网络环境的要求。与单机操作系统不同，网络操作系统服务的对象是整个计算机网络，具有更复杂的结构和更强大的功能，必须支持多用户、多任务和网络资源共享。

对于联网的计算机系统来说，它们的资源既是本地资源，又是网络资源；既要为本地用户使用资源提供服务，又要为远程网络用户使用资源提供服务。这就要求网络操作系统能够屏蔽本地资源与网络资源的差异性，为用户提供各种基本网络服务功能，完成网络共享系统资源的管理，并提供网络系统的安全性服务。

网络操作系统是建立在计算机操作系统基础上，用于管理网络通信和共享资源，协调各主机上任务的运行，并向用户提供统一的、有效的网络接口的软件集合。从逻辑上看，网络操作系统软件由以下 3 个层次组成：位于低层的网络设备驱动程序；位于中间层的网络通信协议；位于高层的网络应用软件。

这 3 个层次之间的关系是一种高层调用低层、低层为高层提供服务的关系。

与一般操作系统不同的是，网络操作系统可以将其功能分配给连接到网络上的多台计算机；另一方面，它又依赖于每台计算机的本地操作系统，使多个用户可以并发访问共享资源。

一个计算机网络除了运行网络操作系统，还要运行本地（客户端）操作系统。网络操作系统运行在称为服务器的计算机上，在整个网络系统中占主导地位，指挥和监控整个网络的运行。网络中的非服务器的计算机通常被称为工作站或客户端，它们运行桌面操作系统或专用的客户端操作系统。

1.1.2 网络操作系统的特点

网络操作系统是基于计算机网络范围的操作系统，为网络用户提供了便利的操作和管理平台。它具有一般计算机操作系统的基本特征，也有自己的独特之处。其特点概述如下。

- 硬件独立性。网络操作系统可以运行在不同的网络硬件上。
- 网络连接。能够支持各种网络协议，连接不同的网络。
- 网络管理。支持网络应用程序及其管理功能，如系统备份、安全管理、性能控制等。
- 安全性和访问控制。能够进行系统安全性保护和各类用户的访问权限控制；能够对用户资源进行控制，提供用户对网络的访问方法。
- 网络服务。支持文件服务、打印服务、通信服务、数据库服务、Internet 服务等。
- 多用户支持。在多用户环境下，网络操作系统给应用程序及其数据文件提供了足够的标准化保护。
- 多种客户端支持。
- 用户界面。网络操作系统提供给用户丰富的界面功能，具有多种网络控制方式。

1.1.3 网络操作系统的功能

早期网络操作系统功能较为简单，仅提供基本的数据通信、文件和打印服务等。随着网络的规模化和复杂化，现代网络的功能不断扩展，除了具有一般操作系统应具有的基本功能外，网络操作系统还应具有以下几项网络功能。

- 网络通信。其任务是在源计算机和目标计算机之间，实现无差错的数据传输，包括建立与拆除通信链路、传输控制、差错控制、流量控制、路由选择等功能。
- 资源管理。对网络中的所有硬、软件资源实施有效管理，协调诸用户对共享资源的使用，保证数据的安全性、一致性和完整性，使用户在访问远程共享资源时能像访问本地资源一样方便。典型的网络资源有硬盘、打印机、文件和数据。
- 网络管理。通过访问控制来确保数据的安全性，通过容错技术来保证系统故障时数据的可靠性，此外，还包括对网络设备故障进行检测、对使用情况进行统计等。
- 网络服务。向用户提供多种有效的网络服务，如电子邮件服务、远程访问服务、Web 服务、FTP 服务及共享文件打印服务等。
- 互操作。将若干相同或不同的设备和网络互连，用户可以透明地访问各服务点、主机，以实现更大范围的用户通信和资源共享。
- 网络接口。向用户提供一组方便有效的、统一的、能获取网络服务的接口，以改善用户界面，如命令接口、菜单、窗口等。

1.1.4 网络操作系统的工作模式

早期网络操作系统采用集中模式，实际上是由分时操作系统加上网络功能演变而成的，系统由一台主机和若干台与主机相连的终端构成，将多台主机连接形成网络，信息的处理和控制都集中在主机上，UNIX 就是典型的例子。现代网络操作系统主要有以下两种工作模式。

1. 客户端/服务器模式

客户端/服务器（Client/Server）模式简称 C/S 模式，是目前较为流行的工作模式。它将

网络中的计算机分成两类站点，一类是作为网络控制中心或数据中心的服务器，提供文件打印、通信传输、数据库等各种服务；另一类是本地处理和访问服务器的客户端。客户端具有独立处理和计算能力，仅在需要某种服务时才向服务器发出请求。客户端与服务器之间的关系如图 1-1 所示。

提示：客户端与服务器的概念有多重含义，有时指硬件设备，有时又特指软件（进程）。在指软件的时候，也可以称客户（Client）和服务（Service）。

采用这种模式的网络操作系统软件由两部分组成，即客户端软件和服务器软件，两者之间的关系如图 1-2 所示，其中服务器软件是系统的主要部分。同一台计算机可同时运行服务器软件和客户端软件，既可充当服务器，也可充当客户端。

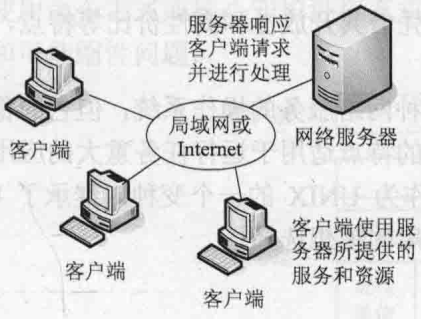


图 1-1　客户端与服务器之间的关系

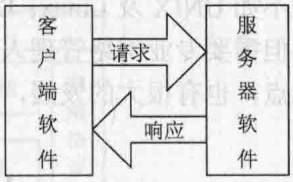


图 1-2　客户端软件与服务器软件之间的关系

这一模式的信息处理和控制都是分布式的，任务由客户端和服务器共同承担，主要优点是数据分布存储、数据分布处理、应用实现方便，适用于计算机数量较多、位置相对分散、信息传输量较大的网络。Netware 和 Windows 网络操作系统采用的就是这种模式。

2. 对等模式

采用对等（Peer to Peer）模式的网络操作系统允许用户之间通过共享方式互相访问对方的资源，联网的各台计算机同时扮演服务器和客户端两个角色，并且具有对等的地位。这种模式的主要优点是平等性、可靠性和可扩展性较好。它适用于小型计算机网络之间资源共享的场合，用户无需购置专用服务器。Windows 操作系统就内置了对等式操作系统，通过相应的设置可以方便地实现对等模式网络。

1.1.5　网络服务器

网络操作系统是在服务器上运行的系统软件，又称服务器操作系统。网络服务器是在网络环境中为用户计算机提供各种服务的计算机，承担网络中数据的存储、转发和发布等关键任务，是网络应用的基础和核心。运行网络操作系统的服务器在网络中起着关键作用。

在网络环境中，许多客户端系统可以访问并且共享一个或多个服务器上的资源。为支持本地处理，服务器系统必须支持多个并发用户和多任务，给向服务器申请远程资源的客户端服务。因此，从硬件上看，网络服务器通常是较大的系统，主要具备以下特性。

- 附加的存储器用来支持多任务，这些任务同时活动着或常驻存储器。
- 附加的磁盘空间用来存储共享文件或作为扩展的系统内存。
- 有额外的扩展槽，用于连接打印机和各种网络接口等共享设备。

- 在多处理器服务器上，附加的 CPU 用于提高处理能力。
- 采用冗余技术加入附加的硬件，建立容错系统，提高系统的可靠性和可用性。

从软件上看，服务器上的操作系统必须比客户端的具有更好的性能，支持多用户、多任务。高端服务器通常因为容量很大，可以处理大型、多个服务，而被称为企业服务器。

1.1.6 常用的网络操作系统

随着计算机网络的迅速发展，市场上出现了多种网络操作系统并存的局面。各种操作系统在网络应用方面都有各自的优势，都极力提供跨平台的应用支持。目前主流的网络操作系统主要有 Windows 系列、UNIX 或 Linux。Windows 操作系统的突出优点是便于部署、管理和使用，深受国内企业的青睐。UNIX 版本很多，大多要与硬件相配套，一般提供关键任务功能的完整套件，在高端市场处于领先地位。Linux 凭借其开放性和高性价比等特点，近年来获得了长足发展，市场份额不断增加。

Windows 系列是一个多目标、易于管理和实现各种网络服务的操作系统，但它的稳定性和可靠性不如 UNIX 及 Linux；UNIX 以其高效、稳定的特点适用于运行任务重大的应用程序的平台，但需要专业网络管理人员进行管理；Linux 作为 UNIX 的一个变种，继承了 UNIX 的全部优点，也有很大的发展，是实现网络关键性应用的理想选择。

1.2 Linux 与 CentOS

Linux 是操作系统的后起之秀，具有完善的网络功能和较高的安全性。CentOS（Community Enterprise Operating System）意为社区企业操作系统，是国内广泛使用的 Linux 网络操作系统。

1.2.1 Linux 操作系统简介

Linux 是一种起源于 UNIX，并以可移植操作系统接口（Portable Operating System Interface，POSIX）标准为框架发展起来的开放源代码的操作系统。POSIX 是 UNIX 类型操作系统接口集合的国际标准。Linux 具有完善的网络功能和较高的安全性，继承了 UNIX 系统卓越的稳定性表现，在全球各地的服务器平台市场中的份额不断增加。

1. Linux 操作系统的发展

Linux 雏形的设计始于一位名叫 Linus Torvald 的芬兰计算机业余爱好者，其目标是设计可用于 Intel 386 或奔腾处理器的 PC 上，且具有 UNIX 全部功能的操作系统。1991 年 10 月 5 日，Linus 在 comp.os.minix 新闻组上发布消息，正式向外宣布 Linux 内核系统的诞生。1994 年，Linux 第一个正式版本 1.0 发布，随后通过 Internet 迅速传播。

Linux 是一套在 GNU 公共许可权限下免费获得的自由软件，用户可以无偿地得到它及其源代码，可以无偿地获得大量的应用程序，而且可以任意地修改和补充它们。Linux 能在 PC 上实现全部的 UNIX 特性，具有多任务、多用户的能力。

从技术上说，Linux 是一个内核，也就是一个提供硬件抽象层、磁盘及文件系统控制、多任务等功能的系统软件。当然内核并不是一套完整的操作系统，一些组织和公司将 Linux 内核、源代码及相关应用软件集成为一个完整的操作系统，便于用户安装和使用，从而形成 Linux 的发行版本。国外知名的 Linux 版本有 Red Hat、Slackware、Debian、SuSE、Ubuntu，

国内知名的 Linux 版本有红旗等。这些软件包不仅包括完整的 Linux 系统，而且包括文本编辑器、高级语言编译器等应用软件，以及 X Windows 图形用户界面。

由于具有完善的网络功能和较高的安全性，Linux 主要用作服务器操作系统，可实现各种网络服务，如邮件服务、Web 服务、DNS 服务、防火墙、代理服务器等。企业级应用是 Linux 增长最迅速的领域，Linux 现已成为企业中重要服务器的首选系统之一。

2. Linux 操作系统的体系结构

Linux 采用分层设计，体系结构如图 1-3 所示。它基本上是单内核操作系统，但模块化的内核结构将微内核的许多优点引入其设计中，特别是提出了一种称为模块（module）的机制，设备驱动程序、伪设备驱动程序、文件系统都组织成模块。每当系统启动后，模块可以根据需要使用命令方式或核心守护进程方式动态地装载和卸载，一定程度上解决了核心功能的灵活性和可伸缩性问题。

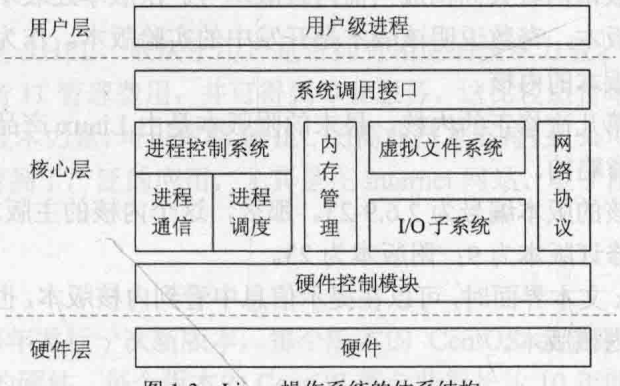


图 1-3　Linux 操作系统的体系结构

3. Linux 操作系统的特性

Linux 操作系统得到了非常迅猛的发展，这与 Linux 具有良好的特性是分不开的，它包含了 UNIX 的全部功能和特性。总的来说，Linux 具有以下主要特性。

- 可以自由、免费使用。Linux 源代码开放，因而从可靠性和安全性上来讲，更适合政府、军事、金融等关键性机构使用。
- 开放性。开放性是指系统遵循世界标准规范，特别是遵循开放系统互联（OSI）国际标准。凡遵循国际标准所开发的硬件和软件，都能彼此兼容，可方便地实现互联。
- 性能好，功能完善，具有超强的稳定性和可靠性，适合需要连续运行的服务器系统。
- 可以进行内核定制。Linux 可以根据自己的需要对系统内核进行定制，从而构建一个新的符合服务器角色的内核，减少不必要的内存占用，提升系统的整体性能。
- 支持多种硬件平台，包括 PC、笔记本、工作站，甚至也有大型机。
- 完善的网络与 Internet 支持。
- 可靠的系统安全。Linux 为网络多用户环境中的用户提供了必要的安全保障。
- 提供可选的类 Windows 图形界面。
- 设备独立性。操作系统把所有外部设备统一当作文件来看待，只要安装它们的驱动程序，任何用户都可以像使用文件一样操纵、使用这些设备。
- 良好的可移植性。这为运行 Linux 的不同计算机平台与其他任何机器进行准确而有效

的通信提供了手段，不需要额外增加特殊的和昂贵的通信接口。

1.2.2 Linux 操作系统的版本

Linux 操作系统的版本分为两种，即内核版本和发行版本。

1. 内核版本

内核版本是指内核小组开发维护的系统内核的版本号。内核版本也有两种不同的版本号，即实验版本和产品版本。实验版本还将不断地增加新的功能，不断地修正 BUG 从而发展到产品版本；而产品版本不再增加新的功能，只是修改错误。在产品版本的基础上再衍生出一个新的实验版本，继续增加功能和修正错误，由此不断循环。

内核版本的每一个版本号都是由 4 个部分组成的，其格式为：

[主版本].[次版本].[修订版本]-[附版本]

其中主版本和次版本两者共同构成当前内核版本号。次版本还表示内核类型，偶数说明该版本是稳定的产品版本，奇数说明该版本是开发中的实验版本。作为正式用途的网络操作系统，建议使用稳定版本的内核。

修订版本表示是第几次修正的内核。最末的附版本是由 Linux 产品厂商所定义的版本编号，这组版本是可以省略的。

例如，有一个内核的版本编号为 2.6.9-23。那么，这个内核的主版本为 2；次版本为 6，是一个稳定的版本；修订版本为 9；附版本为 23。

用户在登录 Linux 文本界面时，可以在提示信息中看到内核版本，也可以随时执行 uname –r 命令来查看系统的内核版本。

2. 发行版本

对操作系统来说，仅有内核是不够的，还需配备基本的应用软件。一些组织和公司将 Linux 内核、源代码及相关应用软件集成为一个完整的操作系统，便于用户安装和使用，从而形成 Linux 发行版本。

Linux 发行版本通常包含一些常用的工具性的实用程序（Utility），供普通用户日常操作和管理员维护操作使用。此外，Linux 系统还可选用成百上千的第三方应用程序，如数据库管理系统、文字处理系统、Web 服务器程序等。

Linux 发行版本主要有 3 个主要分支——Red Hat、Slackware 和 Debian，每一个分支都拥有一个代表性的企业服务器级版本，分别是 Red Hat Enterprise Linux（简称 RHEL）、SuSE Linux Enterprise（简称 SUSE）和 Ubuntu Server（简称 Ubuntu）。这些发行版本相互借鉴，取长补短，它们之间并没有本质的差别。

发行版本的版本号随着发行者的不同而不同。以 Red Hat Linux 为例，其发行版本 Enterprise Linux 5.3 采用的内核版本是 2.6.18，这二者并不矛盾。用户可以自行下载最新的内核版本，进行编译安装。

1.2.3 CentOS Linux

Red Hat Enterprise Linux 是目前由众多厂商支持的主流的 Linux 发行版，对 KVM 虚拟机的全力支持，使它成为许多企业的 Internet 服务器首选。但是如果要得到 Red Hat 的服务与技术支持，用户必须向 Red Hat 付费。CentOS 是一个基于 Red Hat Linux 提供的源代码的企业

级 Linux 发行版本。由于出自与 RHEL 相同的源代码，有些要求高度稳定性的服务器用户会选择 CentOS 来替代商业版的 RHEL。

1. CentOS 与 RHEL 的关系

RHEL 的发行有两种方式。一种是二进制的发行方式，另外一种是源代码的发行方式。无论是哪一种发行方式，RHEL 都可以免费获得，并再次发布。但如果要使用在线升级（包括补丁）或咨询服务，则必须付费。CentOS 就是将 RHEL 发行的源代码重新编译一次，重新形成一个具有自己风格的可使用的二进制版本，其中一切与 Red Hat 有关的商标都被去除了。CentOS 可以得到 RHEL 的所有功能，而且在 RHEL 的基础上修正了不少已知的 Bug，相对于其他 Linux 发行版本，其稳定性值得信赖。CentOS 是免费的，用户可以使用它搭建企业级 Linux 系统环境，达到与 RHEL 一样的效果，而无须向 Red Hat 支付任何费用。CentOS 并不向用户提供商业支持，当然也不负任何商业责任，其技术支持主要通过社区的官方邮件列表、论坛和聊天室。

选用 CentOS 还是 RHEL，取决于用户是否拥有相应的技术力量。选购 RHEL 软件并购买相应服务，可以节省 IT 管理费用，并可得到专业服务，这比较适合单纯的业务型企业。如果具有足够的 Linux 技术力量，可以忽略 RHEL 的商业技术支持，那么可以放心选择 CentOS。目前 CentOS 在国内得到了广泛的应用，尤其是在 Internet 网站、电子商务、大数据、云计算等领域。

2. CentOS 版本

CentOS 大约每两年发行一次新版本，每个版本的 CentOS 会定期（大概每 6 个月）更新一次，以便支持新的硬件。每个版本的 CentOS 都会获得长达 10 年的支持，这是通过安全更新方式实现的，当然支持期的长短还要取决于 Red Hat 发行的源代码的更改。CentOS 7 于 2014 年 7 月正式发布，首个正式版的版本号为 7.0.1406。CentOS 7 主要特点如下：仅提供 64 位版本；内核更新至 3.10.0；支持 Linux 容器（Docker），使用轻量级的 Docker 进行容器实现；默认使用 XFS 文件系统；使用 systemd 后台程序管理 Linux 系统和服务；使用 firewalld 后台程序管理防火墙服务等。

1.3　安装 CentOS Linux 服务器

本书的网络操作系统平台采用 CentOS 7 版本。

1.3.1　组建 Linux 实验网络

在学习网络操作系统配置与管理的过程中，虽然多数功能可以直接在服务器上进行测试，但是为了达到好的测试效果，往往需要两台或多台计算机进行联网测试。在实际工作中，正式部署服务器之前也需要先进行测试。如果有多台计算机，可以组成一个小型网络用于测试。本书实例运行的网络环境至少涉及 3 台计算机，内部网络域名为 abc.com，如图 1-4 所示。

- 主要服务器：运行 CentOS 7，名称为 srv1，IP 地址为 192.168.0.1/24；主要用于安装各类网络服务。
- 用作网关的服务器：运行 CentOS 7，名称为 srv2，配置两个网络接口，内网接口 IP