

Linux网络配置 与安全管理

吴培飞 主编

 北京理工大学出版社
BEIJING INSTITUTE OF TECHNOLOGY PRESS

Linux 网络配置与安全管理

吴培飞 主 编

郝阜平 林海平 宣乐飞 副主编



北京理工大学出版社

BEIJING INSTITUTE OF TECHNOLOGY PRESS

内 容 简 介

本书依据“组建基于 Linux 平台的企业网”工作任务的过程进行编写，各章节按项目编排，每个项目都需要完成一个相对独立的任务，由这些相对独立的模块搭建起一个基于 Linux 的小型企业网的完整项目。整个项目以设计、实现和维护 Linux 网络为线索来展开，将必备的网络知识融入相应的工作任务中。

本书可作为信息安全与管理等专业的教材，采用了全新的基于工作过程的项目化教材开发范式，教材编排注重学生职业能力和实际工作任务的解决和完成，理论内容围绕职业能力展开，突出了对学生可持续发展能力与职业迁移能力的培养。学习本教材的内容将为进一步学习动态网站的架设与管理技术，从而备考 LUPA 网络管理员或 H3CNE（H3C 认证网络工程师）奠定良好的基础。

版权专有 侵权必究

图书在版编目（CIP）数据

Linux 网络配置与安全管理/吴培飞主编. —北京：北京理工大学出版社，2019. 8
ISBN 978 - 7 - 5682 - 7516 - 3

I. ①L… II. ①吴… III. ①Linux 操作系统 - 高等学校 - 教材 IV. ①TP316. 85

中国版本图书馆 CIP 数据核字（2019）第 195301 号

出版发行 / 北京理工大学出版社有限责任公司

社 址 / 北京市海淀区中关村南大街 5 号

邮 编 / 100081

电 话 / (010) 68914775（总编室）

(010) 82562903（教材售后服务热线）

(010) 68948351（其他图书服务热线）

网 址 / <http://www.bitpress.com.cn>

经 销 / 全国各地新华书店

印 刷 / 涿州市新华印刷有限公司

开 本 / 787 毫米 × 1092 毫米 1/16

印 张 / 12

字 数 / 292 千字

版 次 / 2019 年 8 月第 1 版 2019 年 8 月第 1 次印刷

定 价 / 51.00 元

责任编辑 / 王玲玲

文案编辑 / 王玲玲

责任校对 / 周瑞红

责任印制 / 施胜娟

图书出现印装质量问题，请拨打售后服务热线，本社负责调换

前 言

在服务器领域，Linux 系统以稳定、安全、网络负载力强、占用硬件资源少、费用低廉等特点得到了迅速推广和应用。目前，我国正在积极推进 Linux 的普及与应用，并大力促进以 Linux 为基础的符合国际标准和我国实际需要的具有自主知识产权的软件产业发展。

Red Hat Enterprise Linux 系列产品专门为企业应用而设计，被全球众多的软、硬件厂商所支持，它将开放源代码所带来的技术创新和企业级平台的稳定性紧密结合在一起，越来越多的企业开始部署以 Linux 为主要操作系统的网络服务平台。基于此，学习、掌握和使用 Linux 操作系统已成为当务之急。

1. 指导思想

本书针对应用技能型人才的培养特点和培养目标，以 Red Hat Enterprise Linux 9 为蓝本，提炼、整合了 Linux 最通用、最核心的实用技术和原理作为教材内容。

本书的特点：

- (1) 注重实践操作，知识点围绕操作过程按需介绍。
- (2) 案例丰富，注重应用。
- (3) 由浅入深，由简入繁，循序渐进。
- (4) 侧重应用，抛开复杂的理论说教，学以致用。

2. 编写思路

本书内容主要以 Linux 网络中的安全应用环境设置为主，全部内容均来自真实案例的加工提炼，着重体现安全相关岗位工作过程，并以项目工作为主线展开理论和实践过程。

3. 本书的读者

- (1) 从事网络安全管理工作的网络管理人员。
- (2) 为终端客户提供安全解决方案的网络安全工程师。
- (3) 提供网络安全整体解决方案的售前售后工程师。
- (4) 有志于从事网络安全工程研究的网络从业者。
- (5) 希望加固自身终端系统的网络使用者。

本书由吴培飞担任主编，由郝阜平、林海平、宣乐飞担任副主编，项目 1、项目 2、项



目3的实践部分由郝阜平编写,项目4、项目5的实践部分由林海平编写,项目6、项目7的实践部分由宣乐飞编写,项目1~项目7的理论部分由吴培飞编写,全书由吴培飞统稿。

本教材全体编者衷心感谢提供各类安全资料及项目素材的杭州安恒信息技术有限公司的网络工程师、产品经理及技术部的同仁,同时也要感谢来自教育干线的合作教师们提供的大量需求建议并参与部分内容的校对和整理工作,在此一并致谢!

限于本教材编者的经验和水平,谨请使用本教材的师生和各位同仁对本版教材在内容和文字上的种种缺陷提出批评。编者邮箱 wupeifei8413@sina.com.cn。

编 者

2019年8月

目 录

项目一 岗位工作环境初识	1
一、教学目标	1
二、工作任务	1
模块1 企业局域网项目需求与需求分析	1
一、教学目标	1
二、工作任务	2
三、相关知识点	2
四、实践操作	5
模块2 认识 Linux	6
一、教学目标	6
二、工作任务	6
三、相关知识点	6
四、实现方法	8
附录	26
习题	27
项目二 连接网络——传输介质	29
一、教学目标	29
二、工作任务	29
模块1 制作双绞线	29
一、教学目标	29
二、工作任务	29
三、相关知识点	30
四、实现方法	32
模块2 认识无线网络	36
一、教学目标	36
二、工作任务	36
三、相关知识点	36
四、实现方法	39
附录	41
习题	42



项目三 连接网络——联网设备	43
一、教学目标	43
二、工作任务	43
模块1 认识局域网设备	43
一、教学目标	43
二、工作任务	43
三、相关知识点	43
四、实现方法	46
模块2 连接局域网设备	48
一、教学目标	48
二、工作任务	48
三、相关知识点	49
四、实现方法	51
附录	56
习题	57
项目四 文件系统及用户管理	59
一、教学目标	59
二、工作任务	59
模块1 磁盘文件管理	59
一、教学目标	59
二、工作任务	59
三、相关知识点	60
四、实现方法	66
附录	69
习题	69
模块2 用户和用户组管理	70
一、教学目标	70
二、工作任务	70
三、相关知识点	70
四、实现方法	75
附录	76
习题	77
项目五 进程管理	78
一、教学目标	78
二、工作任务	78
模块1 系统启动和运行级别	78



一、教学目标	78
二、工作任务	78
三、相关知识点	79
四、实现方法	80
附录	81
习题	81
模块2 系统监视与进程管理	82
一、教学目标	82
二、工作任务	82
三、相关知识点	82
四、实现方法	85
附录	86
习题	86
模块3 软件包管理	87
一、教学目标	87
二、工作任务	87
三、相关知识点	87
四、实现方法	90
附录	91
习题	91
模块4 任务调度与备份管理	92
一、教学目标	92
二、工作任务	92
三、相关知识点	92
四、实现方法	95
附录	97
习题	97
项目六 服务器管理	99
一、教学目标	99
二、工作任务	99
模块1 TCP/IP 网络管理	99
一、教学目标	99
二、工作任务	99
三、相关知识点	99
四、实现方法	105
附录	106



习题	107
模块2 DNS 服务器配置管理	107
一、教学目标	107
二、工作任务	108
三、相关知识点	108
四、实现方法	114
附录	117
习题	117
模块3 DHCP 服务器配置管理	118
一、教学目标	118
二、工作任务	118
三、相关知识点	118
四、实现方法	122
附录	123
习题	124
模块4 MySQL 服务器配置管理	125
一、教学目标	125
二、工作任务	125
三、相关知识点	125
四、实现方法	131
附录	134
习题	135
模块5 Samba 服务器配置管理	135
一、教学目标	135
二、工作任务	136
三、相关知识点	136
四、实现方法	138
附录	141
习题	141
模块6 Apache 服务器配置管理	142
一、教学目标	142
二、工作任务	142
三、相关知识点	142
四、实现方法	145
附录	148
习题	149



模块7 FTP 服务器配置管理	149
一、教学目标	149
二、工作任务	150
三、相关知识点	150
四、实现方法	152
附录	156
习题	157
模块8 SendMail 服务器配置管理	157
一、教学目标	157
二、工作任务	157
三、相关知识点	158
四、实现方法	160
附录	164
习题	165
模块9 JDK 服务器配置管理	166
一、教学目标	166
二、工作任务	166
三、相关知识点	166
四、实现方法	166
附录	167
习题	168
模块10 Tomcat 服务器配置管理	168
一、教学目标	168
二、工作任务	168
三、相关知识点	168
四、实现方法	168
附录	170
习题	170
项目七 系统安全管理	171
一、教学目标	171
二、工作任务	171
模块1 远程控制	171
一、教学目标	171
二、工作任务	171
三、相关知识点	172
四、实现方法	173



附录.....	174
习题.....	175
模块2 服务器安全	175
一、教学目标.....	175
二、工作任务.....	175
三、相关知识点.....	175
四、实现方法.....	177
附录.....	179
习题.....	180

项目一

岗位工作环境初识

本项目通过对企业网络的具体调研，让读者理解需求调研的作用，掌握需求分析的基本方法，理解用户需求的常见表现，设计园区网络并利用 PowerPoint 或 VISIO 的绘图工具绘制出标准的网络拓扑结构图。

一、教学目标

最终目标：掌握用户需求分析的基本方法，能用 PowerPoint 或 VISIO 的绘图工具绘制出标准的网络拓扑结构图，能安装和配置 Linux 系统。

促成目标：

- ①理解用户需求调研的作用。
- ②掌握用户需求分析的基本方法，理解用户需求的常见表现。
- ③理解企业网络的总体需求。
- ④掌握企业各部分网络的功能，分析各功能模块的可行性。
- ⑤熟悉网络设备的功能特性。
- ⑥能用 PowerPoint 或 VISIO 的绘图工具绘制出标准的网络拓扑结构图。
- ⑦能安装和配置 Linux 系统。

二、工作任务

- ①分析自己熟悉的园区“网络”，通过类比各种生活中的网络，重点勾勒计算机网络的组成部分，总结计算机网络的概念和主要组成部分。
- ②学会对网络用户需求进行具体调研，掌握用户需求分析的基本方法。
- ③理解园区网络的总体需求；掌握园区各部分网络的功能，分析各功能模块的可行性。
- ④掌握网络线缆和设备的基本属性，能根据实际的网络需求选择传输介质和网络设备。
- ⑤能用 PowerPoint 或 VISIO 的绘图工具绘制出标准的网络拓扑结构图。

模块 1 企业局域网项目需求与需求分析

一、教学目标

最终目标：调研园区网络，分析用户的网络业务需求。

促成目标：

- ①理解用户需求调研的作用。
- ②掌握用户需求分析的基本方法，理解用户需求的常见表现。



③掌握网络的拓扑结构知识。

二、工作任务

①会收集、整理用户的网络功能需求，并填写用户需求分析表。

②能准确分析用户的网络业务需求。

三、相关知识点

1. 网络需求分析的概念

需求分析是从软件工程和管理信息系统引入的概念，是任何一个工程实施的第一个环节，也是关系一个网络工程成功与否的最重要砝码。如果网络工程应用需求分析做得透彻，网络工程方案的设计就会赢得用户的青睐。同时，网络系统体系结构架构得好，网络工程实施及网络应用实施就相对容易得多。反之，如果网络工程设计方没有对用户方的需求进行充分调研，不能与用户方达成共识，那么随意需求就会贯穿整个工程项目的始终，并破坏工程项目的计划和预算。从事信息技术行业的技术人员都清楚，网络产品与技术发展非常快，通常是同一档次网络产品的功能和性能在提升的同时，产品的价格却在下调。这也就是网络工程设计方和用户方在论证工程方案时，一再强调的工程性价比。

因此，网络工程项目是贬值频率较快的工程，贵在速战速决，使用户方投入的有限的网络工程资金尽可能快地产生应用效益。如果用户方遭受网络项目长期拖累，迟迟看不到网络系统应用的效果，网络集成公司的利润自然也就降到了一个较低的水平，甚至到了赔钱的地步。一旦网络集成公司不盈利，用户方的利益自然难以保证。因此，要把网络应用的需求分析作为网络系统集成中至关重要的步骤来完成。应当清楚，反复分析尽管不可能立即得出结果，但它却是网络工程整体战略的一个组成部分。

需求分析阶段主要完成用户方网络系统调查，了解用户方建设网络的需求，或用户方对原有网络升级改造的要求。需求分析包括网络工程建设中的“路”“车”“货”“驾驶员”（“路”表示综合布线系统，“车”表示网络环境平台，“货”表示网络资源平台，“驾驶员”表示网络管理者和网络应用者）等方面的综合分析，为下一步制订适合用户方需求的网络工程方案打好基础。

需求分析是整个网络设计过程中的难点，需要由经验丰富的系统分析员来完成。

网络需求调研的目的是从用户方网络建设的需求出发，通过对用户方现场实地调研，了解用户方的要求、现场的地理环境、网络应用及工程预计投资等情况，使网络工程设计方获得对整个工程的总体认识，为系统总体规划设计打下基础。

2. 网络用户方调查

网络用户方调查是与需要建网的企事业单位的信息化主管、网络信息化应用的主要部门的用户进行交流。一般情况下可以把用户方的需求归纳为以下几个方面：

①网络延迟与可预测响应时间。

②可靠性/可用性。即系统（包含路由器、核心层交换机、汇聚层交换机等设备）不停机运行。



③伸缩性。网络系统能否适应用户不断增长的需求。

④高安全性。保护用户信息和物理资源的完整性,包括数据备份、灾难恢复等。概括起来,系统分析员对网络用户方调查可通过填写调查表来完成。

3. 网络应用调查

企事业单位网络建设就是变革传统的管理模式,实现管理信息化。不同的行业有不同的应用要求,切不可“张冠李戴”。应用调查就是要弄清用户方建设网络的真正目的。

从企事业单位的 OA 系统、人事档案、工资管理到企事业单位的 MIS 系统、ERP(企业资源规划)等,从文件信息资源共享到 Intranet/Internet 信息服务(WWW、E-mail、FTP 等),从数据流到多媒体的音频、视频多媒体流传输应用等,都有网络应用。只有对用户方的实际需求进行细致的调查,并从中得出用户方的应用类型,数据量的大小,数据源的重要程度,网络应用的安全性、可靠性、实时性等要求,才能设计出适合用户实际需要的网络工程方案。实际上,每一个网络工程都应该按照用户方的需求进行“量体裁衣”式的打造。

应用调查通常是由网络系统工程师深入现场,以会议或走访的形式邀请用户方的代表发表意见,并填写网络应用调查表。网络应用调查表设计要注意网络应用的细节问题,如果不涉及应用开发,则不要过细,只要能充分反映用户方比较明确的需求、没有遗漏即可。

4. 网络工程综合布线调查

网络工程综合布线调查主要是了解用户方建筑楼群的地理环境与几何中心、建筑楼内的布线环境与几何中心,由此来确定网络的物理拓扑结构、综合布线系统材料预算。通过对用户方实施综合布线的相关建筑物进行实地考察,由用户方提供建筑工程图,从而了解相关建筑结构,分析施工难易程度,并估算大致费用。需了解的其他数据包括中心机房的位置、信息点数、信息点与中心机房的最远距离、电力系统状况、建筑楼情况等。

综合布线需求分析主要包括以下 3 个方面:

①根据造价、建筑物距离和带宽要求确定光缆的芯数和种类。

②根据用户方建筑楼群间距离、马路隔离情况及电线杆、地沟和道路状况,将建筑楼群间光缆的敷设方式分为架空、直埋或是地下管道敷设等。

③对各建筑楼的信息点数进行统计,用于确定室内布线方式和配线间的位置。建筑物楼层较低、规模较小、点数不多时,只要所有的信息点与设备间的距离均在 90 m 以内,信息点布线可直通配线间。当建筑物楼层较高、规模较大、点数较多,即有些信息点与主配线间的距离超过 90 m 时,可采用信息点到中间配线间、中间配线间到主配线间的分布式布线。

5. 网络安全、可靠性分析

(1) 网络可用性、可靠性需求

校园网、企业网等行业对网络系统可用性要求很高,若网络系统崩溃或数据丢失,会造成巨大损失。可用性要求相应的网络具有高可用性设计来保障,如服务器采用磁盘镜像(RAID 1)或磁盘容错(RAID 5)、双机容错、异地备份等措施。另外,还可采用大、中、小型 UNIX 主机(如 IBM、HP、SUN 和富士通的 UNIX 服务器)。



(2) 网络安全性需求

一个完整的网络系统应该渗透到用户方业务的各个方面,其中包括比较重要的业务应用和关键的数据服务器、公共 Internet 出口或 Modem 拨号上网,这就使网络在安全方面有着普遍的强烈需求。安全需求分析具体表现在以下几个方面:

- ①分析存在弱点、漏洞与不当的系统配置。
- ②分析网络系统阻止外部攻击行为和防止内部员工违规操作行为的策略。
- ③划定网络安全边界,使园区网络系统和外界的网络系统能安全隔离。
- ④确保租用电路和无线链路的通信安全。
- ⑤分析如何监控园区网络的敏感信息,包括技术专利等信息。
- ⑥分析工作桌面系统的安全。

为了全面满足以上安全系统的需求,必须制定统一的安全策略,使用可靠的安全机制与安全技术。安全不单纯是技术问题,而是策略、技术与管理的有机结合。

6. 网络工程预算分析

首先要设法弄清建网单位的投资规模,即用户方能拿出多少钱来建设网络。一般情况下,用户方能拿出的建网经费与用户方的网络工程的规模及工程应达到的目标是一致的。也就是常说的“有多少钱就办多大的事”,切不可一味地攀比。一样的网络工程规模和建设目标,完全采用国际名牌和完全采用国内品牌,其价格相差较大。网络技术经过数年的发展,时下国内网络产品的质量已日益提高,其性能质量也在稳步上升,尤其是中高档产品完全可以取代进口设备,如华为、实达、神州数码等品牌。目前对于网络工程项目,用户方都希望经济方面最省、工期最短、工程质量最好、网络应用效果最佳。如今的网络工程市场竞争十分激烈,往往一个工程招标就有数十个系统集成商前来竞标,经过一番残酷的竞争,到最后也只有 1~3 个系统集成商入围。这种局面对用户方来说自然是好事,但用户方也不可一味地杀价。用户方在认定合作者时,要对系统集成商的工程方案、工程质量、工程效率、工程服务、工程价格等进行全面、综合考虑。

网络工程项目费用主要包括以下几个方面:

- ①网络通信设备:交换机、路由器、拨号访问服务器、集线器、网卡等。
- ②服务器及客户设备硬件:服务器群、网络存储设备、网络打印机、客户等。
- ③网络基础设施:UPS 电源、机房装修、综合布线系统及器材等。
- ④软件:网络操作系统、网管系统、计费系统、数据库、外购应用系统、集成商开发软件等。
- ⑤网络安全系统:网络安全与防病毒软件、防火墙、上网行为管理系统等。
- ⑥远程通信线路或电信租用线路费用。
- ⑦系统集成费用:包括网络设计、网络工程项目集成和布线工程施工费用。
- ⑧培训费和网络维护费。

只有知道用户方对网络投入多少,才能据此确定网络硬件设备和系统集成服务的“档次”,产生与此相配的网络设计方案。

对于系统集成商的利润,一般包括硬件差价、系统集成费、综合布线施工费用和软件开发费用四部分。



四、实践操作

以春晖中学校园网络为例来体验项目开始之前的调研工作。

背景知识/准备工作：

在本实验操作中，将使用 1 台计算机在互联网上查询有用信息。

本实验需要以下资源：

1 台安装 Windows XP Professional 系统的计算机，能够正常访问 Internet。

1) 主要要求。

- ①信息点分布情况：主要填写行政楼、教学楼和实验楼的每个房间墙壁上的网线插座的个数，并统计总数。
 - ②综合布线情况：主要填写行政楼、教学楼和实验楼原有的布线情况，简要画出拓扑图，并能用图设计出 3 个楼之间和整个校园网络的布线。
 - ③用户上网需求：根据对具体用户的调研，填写用户的主要上网需求。
 - ④用户容量：主要填写 3 个楼网络的用户的数量。
- 2) 根据实际的调研认真填写春晖中学校园网需求表（见表 1-1-1）。

表 1-1-1 用户需求调查表

春晖中学校园网整体需求	信息点分布情况	行政楼	1. 楼层数		总信息点数
			2. 每楼层的房间数		
			3. 每个房间的信息点数		
		教学楼	1. 楼层数		总信息点数
			2. 每楼层的房间数		
			3. 每个房间的信息点数		
		实验楼	1. 楼层数		总信息点数
			2. 每楼层的房间数		
			3. 每个房间的信息点数		
	综合布线情况	楼层内的布线情况	行政楼		
			教学楼		
			实验楼		
		3 个楼之间的布线情况			
		整个校园网络的布线情况			
	用户对象上网需求与用户容量	行政楼	主要上网需求：		用户最大容量数
教学楼		主要上网需求：		用户最大容量数	
实验楼		主要上网需求：		用户最大容量数	



模块 2 认识 Linux

一、教学目标

最终目标：掌握安装和配置 Linux 的方法。

促成目标：

- ①了解 Linux 操作系统的发行版本。
- ②掌握 Red Hat Linux 9 的安装方法。
- ③了解 Linux 其他版本（红旗 Linux 或 Slackware Linux）的安装方法。

二、工作任务

安装和配置一台 Linux 系统。

三、相关知识点

1. Linux 介绍

Linux 是 UNIX 克隆（UNIX clone）或 UNIX 风格（UNIX alike）的操作系统（OS），它在源代码级上兼容绝大部分 UNIX 标准（IEEE POSIX System V、BSD），是一个支持多用户、多进程、多线程、实时性较好的功能强大而稳定的操作系统。它可以运行在 x86 PC、Sun Sparc、Digital Alpha、680x0、Power PC、MIPS 等平台上，是目前运行硬件平台最多的操作系统。

Linux 最大的特点在于它是 GNU（GNU 是一种自由软件体系）的一员，遵循公共版权许可证（GPL），秉承“自由的思想，开放的源码”的原则。成千上万的专家及爱好者通过 Internet 不断地完善并维护它，可以说，Linux 是计算机爱好者自己的操作系统。

1990 年，芬兰赫尔辛基大学的一名学生 Linus Torvalds 用汇编语言写了一个在 80386 保护模式下处理多任务切换的程序，后来从 Minix（Andy Tanenbaum 教授所写的很小的 UNIX 操作系统，主要用于操作系统教学）中得到灵感，进一步产生写一个比 Minix 更出色的操作系统的想法，于是便开始写一些硬件的设备驱动程序、一些小的文件系统。这样 0.0.1 版本的 Linux 就诞生了，但是它只具有操作系统内核的雏形，甚至不能运行，必须在装有 Minix 的机器上编译以后才能运行。这时 Linus 决定抛开 Minix，于是在 1991 年 10 月 5 日发布了 Linux 0.0.2 版本。在这个版本中已经可以运行 bash（the GNU Bourne Again Shell，一种用户与操作系统内核通信的软件）和 gcc（GNU C 编译器）。从一开始，Linus 就决定自由扩散 Linux，包括源代码，他在 comp. os. mini x 新闻讨论组里发布 Linux 0.0.2 时写道：

“Do you pine for nice days of Minix - 1.1, when mem were men and wrote their own device drivers? Are you without a nice project and just dying to cut your teeth on a OS you can try to modify for your needs? Are you finding it frustrating when everything works on Minix? No more all-nighters to get a nifty program working? Then this post might be just for you.

“As I mentioned a month ago, I'm working on a free version of a Minix-lookalike for AT - 386