

网络运维管理从基础到实战

许成刚 阮晓龙 杜宇飞 刘海滨 刘明哲 编著

 中国水利水电出版社
www.waterpub.com.cn

· 北京 ·

内 容 提 要

本书以园区网运维管理为主线，精心设计了10个工程项目。内容从构建有线/无线混合园区网到接入互联网，从园区网设备的远程统一管理及基础网络服务管理到构建覆盖全网的运维监控系统，从网络安全管理的实现到基于防火墙的用户上网认证及上网行为分析，涵盖了园区网运维管理的各种关键应用。

本书注重工程项目的落地和实现。每个项目都包含了完整网络拓扑和详细的建设步骤，并且基于eNSP仿真环境和VirtualBox虚拟化技术开展实施，有效解决了读者在学习时由于设备环境的限制只能“纸上谈兵”的问题，可帮助读者在一台电脑上即可轻松构建复杂网络并开展运维管理工作，保证学习过程的顺利开展。

本书可以作为从事网络运维管理的专业技术人员的工程参考用书，也可以作为高等院校计算机相关专业，特别是网络工程、网络运维、信息管理等专业有关课程的教学用书。

策划编辑：周春元

责任编辑：王开云

封面设计：

书 名	网络运维管理从基础到实战
作 者	WANGLUO YUN-WEI GUANLI CONG JICHU DAO SHIZHAN
出版发行	许成刚 阮晓龙 杜宇飞 刘海滨 刘明哲 编著 中国水利水电出版社 (北京市海淀区玉渊潭南路1号D座 100038) 网址: www.waterpub.com.cn E-mail: mchannel@263.net (万水) sales@waterpub.com.cn 电话: (010) 68367658 (营销中心)、82562819 (万水)
经 售	全国各地新华书店和相关出版物销售网点
排 版	北京万水电子信息有限公司
印 刷	三河市鑫金马印装有限公司
规 格	184mm×240mm 16开本 28.5印张 670千字
版 次	2022年3月第1版 2022年3月第1次印刷
印 数	0001—3000册
定 价	88.00元

凡购买我社图书，如有缺页、倒页、脱页的，本社营销中心负责调换

版权所有·侵权必究

作者的话

1. 新的一员

当本书成稿的时候，我们的《互联网运维管理工程应用丛书》（以下简称《丛书》）又诞生了一个新的成员。

本书依然保持《丛书》特有的创作理念：

（1）突出主线

本书不追求技术细节上的“大而全”，而是从园区网运维管理的角度，以园区网构建为起点，内容贯穿“互联网接入管理——网络设备集中管理——网络服务管理——构建全网监控体系——网络安全管理——用户行为分析——构建 VPN 访问”这一主线，使读者能够快速、准确地把握园区网运维管理的关键点。

（2）项目驱动

本书所有章节均以项目形式展开，每个项目中包含若干子任务。所有项目任务均经过精心设计，并且在具体实施前，配有详细的拓扑规划和网络设计规划，从而使其达到企业级实际环境的应用水平，使读者能够更好地学以致用。

（3）循序渐进

本书以第一个项目“构建综合园区网”为基础，后续每一个项目都是在前一个项目的基础上，以增加设备、增加服务或优化拓扑的方式实现的，使读者能够循序渐进地开展学习实践。不仅如此，读者在实现每一个项目时，不需要反复构建基础网络，从而降低实践成本，更好把握每个项目的关键环节。

（4）注重实现

本书注重园区网建设中各个环节的落地和实现。每个项目中都包含了完整的网络拓扑以及详细的建设步骤，对于实施过程中的一些重、难点，还专门给出了特别提醒，只要跟着项目流程操作，就一定能够成功。从而帮助读者从晦涩难懂的技术理论中“跳出来”，快速投入实战，并且在实战成功的基础上，加深对网络运维技术的理解和思考。

（5）环境无忧

本书的所有项目，都是基于 eNSP 仿真环境和 VirtualBox 虚拟化技术，有效解决了读者在学习时由于设备环境的限制只能“纸上谈兵”的问题。帮助读者在一台电脑上即可轻松构建复杂园区网并开展运维管理工作，极大降低学习成本，保证了学习过程的顺利开展。

2. 内容设计

全书精心设计了 10 个工程项目。从构建有线/无线混合园区网到接入互联网，从园区网设备的远程统一管理及基础网络服务管理到构建覆盖全网的运维监控系统，从网络安全管理的实现到基于防火墙的用户上网认证及上网行为分析。可以说，全书内容涵盖了园区网运维管理的各种关键应用。

项目一，构建综合园区网。基于 eNSP 仿真环境构建有线/无线混合园区网，将该项目作为本书后续各项目的基础。

项目二，接入互联网。重点掌握 NAT 技术的应用，并且将已经建成的园区网通过 NAT 方式接入互联网。

项目三，园区网设备的集中远程管理。通过 Telnet 和 SSH 方式，实现对园区网内部各网络设备的集中远程管理。

项目四~项目六，构建网络运维管理基础服务，包括域名管理（DNS）、时间服务管理（NTP）、IP 地址管理（DHCP）。

项目七，建设覆盖全网的运维监控系统。分别通过 Cacti 和 Zabbix 构建覆盖整个园区网的监控体系，实现对所有网络服务、网络设备的监控和运行分析。

项目八，网络安全。利用防火墙加强园区网访问及服务管理。

项目九，用户行为管理。基于防火墙实现用户上网认证以及用户上网行为分析。

项目十，通过 VPN 访问园区网内部资源。通过 VPN 方式，使位于互联网上的指定用户能够安全地访问园区网内部资源。

3. 适用对象

本书适用于以下两类读者。

一是从事网络运维与管理的专业技术人员，本书可以帮助他们全面理解网络运维与管理的技术内涵，快速掌握相应的工程实现方法，为后续工作开展打下坚实基础。

二是高等院校计算机相关专业，特别是网络工程、网络运维、信息管理等专业的、具有一定计算机网络原理知识基础和网络应用技术能力的在校学生，本书可以帮助他们加深对网络原理的理解，掌握网络运维与管理技术，提升实践操作的综合能力，真正将网络技术、特别是网络运维与管理技术“学以致用”。

4. 真诚感谢

本书能顺利撰写完毕，离不开家人们的默默支持。正是他们的支持，使我们能全身心投入到本书的编写中。中国水利水电出版社万水分社的周春元副总经理对于本书的出版给予了中肯的指导和积极的帮助，在此表示深深的谢意！

本书的创作得到了教育部 2021 年第一批产学合作协同育人项目《面向新工科的网络安全实践基地与网络安全实训课程建设》（项目编号：202101035010）和《基于国产可控平台的“系统运维大数据实训”课程建设与教学实践》（项目编号：202101327018）的支持，特向项目团队和合作企业表示感谢。

本书视频由河南中医药大学信息技术学院 2019 级信息管理与信息系统专业的宋斌伟、邓汪涛、马骋彝三位同学进行操作演示，我为有此优秀的学生感到自豪，并向他们的辛勤付出表示感谢。

由于我们的水平有限，疏漏及不足之处在所难免，敬请广大读者朋友批评指正。

本书作者
2022 年 2 月于郑州

目 录

作者的话

项目一 构建综合园区网

项目介绍	1
项目目的	1
拓扑规划	1
网络规划	3
项目讲堂	6
任务一 在 eNSP 中部署网络	16
【任务介绍】	16
【任务目标】	16
【操作步骤】	17
任务二 实现用户区域内有线网络的通信	19
【任务介绍】	19
【任务目标】	19
【操作步骤】	19
任务三 实现数据中心区域网络的通信	27
【任务介绍】	27
【任务目标】	27
【操作步骤】	27
任务四 实现无线园区网通信	34
【任务介绍】	34
【任务目标】	34
【操作步骤】	34
任务五 在 eNSP 仿真环境中抓取通信报文	50
【任务介绍】	50
【任务目标】	50
【操作步骤】	50

项目二 接入互联网

项目介绍	54
项目目的	54
项目讲堂	54
任务一 在路由器上实现 NAT 服务	58
【任务介绍】	58
【任务目标】	59
【拓扑规划】	59
【网络规划】	60
【操作步骤】	62
任务二 NAT 接入互联网	72
【任务介绍】	72
【任务目标】	72
【拓扑规划】	72
【网络规划】	73
【操作步骤】	74
任务三 双链路 NAT 接入互联网	78
【任务介绍】	78
【任务目标】	78
【拓扑规划】	79
【网络规划】	79
【操作步骤】	82
任务四 园区网接入互联网	89
【任务介绍】	89
【任务目标】	90
【拓扑规划】	90

【网络规划】	90	【任务目标】	143
【操作步骤】	91	【操作步骤】	143
项目三 园区网设备的集中远程管理		任务二 配置 DNS 服务	150
项目介绍	97	【任务介绍】	150
项目目的	97	【任务目标】	150
项目讲堂	97	【操作步骤】	151
任务一 通过 Telnet 登录交换机	101	任务三 为园区网提供本地域名服务	159
【任务介绍】	101	【任务介绍】	159
【任务目标】	102	【任务目标】	159
【拓扑规划】	102	【操作步骤】	159
【网络规划】	102	任务四 DNS 通信分析	164
【操作步骤】	103	【任务介绍】	164
任务二 通过 SSH 登录网络设备	111	【任务目标】	165
【任务介绍】	111	【操作步骤】	165
【任务目标】	111	项目五 提供 NTP 时间同步服务	
【拓扑规划】	111	项目介绍	169
【网络规划】	112	项目目的	169
【操作步骤】	115	拓扑规划	169
任务三 以 SSH 方式实现园区网设备的集中 远程管理	123	网络规划	170
【任务介绍】	123	项目讲堂	171
【任务目标】	123	任务一 创建并部署 NTP 服务器	175
【拓扑规划】	123	【任务介绍】	175
【网络规划】	124	【任务目标】	175
【操作步骤】	126	【操作步骤】	175
项目四 提供本地 DNS 服务		任务二 实现园区网内部服务器时钟同步	184
项目介绍	137	【任务介绍】	184
项目目的	137	【任务目标】	184
拓扑规划	137	【操作步骤】	184
网络规划	138	任务三 通过 NTP 实现网络设备时钟同步	187
项目讲堂	140	【任务介绍】	187
任务一 创建 DNS 服务器	143	【任务目标】	187
【任务介绍】	143	【操作步骤】	188
		任务四 NTP 协议报文分析	198
		【任务介绍】	198

【任务目标】	198	【操作步骤】	198
项目六 使用 DHCP 进行地址管理			
项目介绍	201	【任务介绍】	207
项目目的	201	【任务目标】	208
拓扑规划	201	【操作步骤】	208
网络规划	202	任务二 实现 DHCP 服务	210
项目讲堂	203	【任务介绍】	210
任务一 搭建 DHCP 服务器	207	【任务目标】	210
【任务介绍】	207	【操作步骤】	210
【任务目标】	208	任务三 为园区网提供 DHCP 服务	215
【操作步骤】	208	【任务介绍】	215
任务二 实现 DHCP 服务	210	【任务目标】	215
【任务介绍】	210	【操作步骤】	215
【任务目标】	210	任务四 抓包分析 DHCP 的通信过程	226
【操作步骤】	210	【任务介绍】	226
任务三 为园区网提供 DHCP 服务	215	【任务目标】	226
【任务介绍】	215	【操作步骤】	226
【任务目标】	215	项目七 建设覆盖全网的运维监控系统	
【操作步骤】	215	项目介绍	233
任务四 抓包分析 DHCP 的通信过程	226	项目目的	233
【任务介绍】	226	拓扑规划	233
【任务目标】	226	网络规划	234
【操作步骤】	226	项目讲堂	235
项目八 网络安全			
项目介绍	233	任务一 基于开源软件 Cacti 建设运维监控系统	239
项目目的	233	【任务介绍】	239
拓扑规划	233	【任务目标】	239
网络规划	234	【操作步骤】	239
项目讲堂	235	【任务介绍】	239
任务一 基于开源软件 Cacti 建设运维监控系统	239	【任务目标】	239
【任务介绍】	239	【操作步骤】	239
【任务目标】	239	任务二 使用 Cacti 监控园区网通信	252
【操作步骤】	239	【任务介绍】	252
任务二 使用 Cacti 监控园区网通信	252	【任务目标】	252
【任务介绍】	252	【操作步骤】	252
【任务目标】	252	任务三 基于开源软件 Zabbix 建设运维监控	260
【操作步骤】	252	服务	260
任务三 基于开源软件 Zabbix 建设运维监控	260	【任务介绍】	260
服务	260	【任务目标】	260
【任务介绍】	260	【操作步骤】	260
【任务目标】	260	任务四 使用 Zabbix 实现全网运行监控	266
【操作步骤】	260	【任务介绍】	266
任务四 使用 Zabbix 实现全网运行监控	266	【任务目标】	266
【任务介绍】	266	【操作步骤】	266
【任务目标】	266	任务五 网络运维监控分析	270
【操作步骤】	266	【任务介绍】	270
任务五 网络运维监控分析	270	【任务目标】	270
【任务介绍】	270	【操作步骤】	271
【任务目标】	270	项目八 网络安全	
【操作步骤】	271	项目介绍	280
项目八 网络安全			
项目介绍	280	项目目的	280
项目目的	280	项目讲堂	280
项目讲堂	280	任务一 初识防火墙	284
任务一 初识防火墙	284	【任务介绍】	284
【任务介绍】	284	【任务目标】	284
【任务目标】	284	【拓扑规划】	284
【拓扑规划】	284	【网络规划】	285
【网络规划】	285	【操作步骤】	288
【操作步骤】	288	任务二 实现防火墙的旁挂部署	300
任务二 实现防火墙的旁挂部署	300	【任务介绍】	300
【任务介绍】	300	【任务目标】	300
【任务目标】	300	【拓扑规划】	300
【拓扑规划】	300	【网络规划】	302
【网络规划】	302	【操作步骤】	305
【操作步骤】	305		

任务三 规划整个园区网的安全设计	312	【任务目标】	386
【任务介绍】	312	【操作步骤】	386
【任务目标】	312	任务三 记录用户上网行为	394
【风险分析】	312	【任务介绍】	394
【安全方案】	313	【任务目标】	394
【拓扑规划】	313	【操作步骤】	394
【网络规划】	315	任务四 用户上网行为分析	401
【安全策略设计】	325	【任务介绍】	401
任务四 在园区网中部署防火墙并实现全网通信	326	【任务目标】	401
【任务介绍】	326	【操作步骤】	401
【任务目标】	326		
【操作步骤】	326	项目十 通过 VPN 访问园区网内部资源	
任务五 配置防火墙策略实现安全目标	362	项目介绍	408
【任务介绍】	362	项目目的	408
【任务目标】	363	项目讲堂	408
【操作步骤】	363	任务一 以 CLI 方式在防火墙上实现 SSL VPN	418
		【任务介绍】	418
项目九 用户行为管理		【任务目标】	418
项目介绍	369	【拓扑规划】	418
项目目的	369	【网络规划】	419
项目讲堂	369	【操作步骤】	421
任务一 通过防火墙实现用户上网认证	377	任务二 通过 RADIUS 服务器实现 SSL VPN 认证	435
【任务介绍】	377	【任务介绍】	435
【任务目标】	377	【任务目标】	435
【操作步骤】	377	【拓扑规划】	435
任务二 通过 RADIUS 服务器实现园区网统一认证	386	【网络规划】	436
【任务介绍】	386	【操作步骤】	437