DVD
附赠超值光盘

网络构建与运维管理

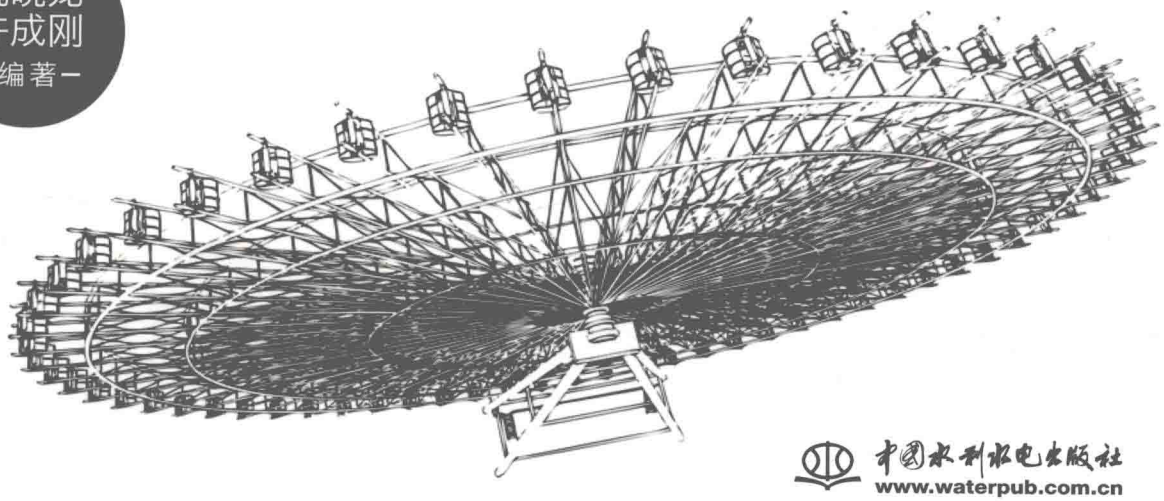
从学到用完美实践

- **无缝贴合工程实践**：实验案例均在Windows/UNIX/Linux平台实现！
- **彻底摆脱纸上谈兵**：通过GNS3网络仿真实现+VirtualBox虚拟机实现，让您在一台笔记本上完成所有复杂网络构建、管理及案例分析！
- **干货多多**：本书所有案例，均为作者多年工作经验、实践经验的结晶。
- **轻松养成工程思维**：所有案例的编写，均以“需求分析”→“规划设计”→“技术论证”→“部署实施”→“总结分析”的步骤实现，工程思维，轻松养成！

一线网络工程技术专家

阮晓龙/许成刚 倾情编写

阮晓龙
许成刚
—编著—



中国水利水电出版社
www.waterpub.com.cn

网络构建与运维管理——从学到用完美实践

阮晓龙　许成刚　编著

中国水利水电出版社
www.waterpub.com.cn

内 容 提 要

本书共 9 章，全面介绍了网络建设及运维管理技术体系。在内容组织上，包含园区网构建与 Internet 接入、网络基础服务建设、网络安全管理、网络运行监控、网络分析 5 个方面的内容，与实际网络工程实践高度融合。其中，第 1～3 章重点介绍园区网构建与 Internet 接入；第 4、5 章讲解了网络中最基础的 DHCP 和 DNS 两种服务的实现；第 6、7 章属于网络安全管理的内容，介绍防火墙和 VPN 的实现；第 8 章介绍如何通过 SNMP 实现网络运行监控；第 9 章介绍网络分析的内容，通过原理讲解及案例分析，让读者掌握网络分析系统的应用。

本书的实践内容全部在 Windows 及 UNIX/Linux 系统平台上实现，并且基于 GNS 3 网络仿真和 VirtualBox 虚拟化环境，涉及的软件全部采用开源、免费或者试用版本，有效解决了读者在学习时由于实践环境限制只能“纸上谈兵”的状况。

本书可作为从事或即将从事网络运维工作的专业技术人员的技术培训或工作参考用书，也可作为高校计算机相关专业、特别是网络工程、网络运维专业有关课程的教学用书。

本书的网络支撑平台为 http://ethernet.book.51xueweb.cn，读者可从中获得相关资源。

图书在版编目（CIP）数据

网络构建与运维管理 ：从学到用完美实践 / 阮晓龙，许成刚编著. -- 北京 ：中国水利水电出版社，2016.2
ISBN 978-7-5170-4089-7

Ⅰ. ①网… Ⅱ. ①阮… ②许… Ⅲ. ①计算机网络管理 Ⅳ. ①TP393.07

中国版本图书馆CIP数据核字(2016)第025696号

策划编辑：周春元　责任编辑：陈　洁　加工编辑：高双春　封面设计：李　佳

书　　名	网络构建与运维管理——从学到用完美实践
作　　者	阮晓龙　许成刚　编著
出版发行	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（发行部）、82562819（万水）
经　　售	北京科水图书销售中心（零售） 电话：（010）88383994、63202643、68545874 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	三河市铭浩彩色印装有限公司
规　　格	184mm×240mm　16 开本　29.25 印张　771 千字
版　　次	2016 年 2 月第 1 版　2016 年 2 月第 1 次印刷
印　　数	0001—3000 册
定　　价	68.00 元（赠 1DVD）

I 前言

作者的话

1. 引子

这本书，我们写了四个月，却用了十二年去做准备。

2003 年，我进入高校工作。由于我所在部门和工作岗位的特殊性，使我同时具有了两个身份：一是计算机课程的教师，二是负责全校计算机网络运行管理的技术人员。也就是在那一年，我第一次真正接触计算机网络：负责单位的两台 IBM 服务器的运维工作。从那时起的十二年间，除了课堂教学之外，网络建设与安全、服务器运维、各种网络应用服务与管理服务的研发工作，就成了我生活中的关键词。

2. 为什么写这本书

写这本书的一个直接起因，是因为 2015 年的选教材工作：我想给我的学生们选取一本计算机网络管理与运维方面的参考书。但是，在一番查阅和选择之后，竟然发现没有一本书能够让我们满意的。市面上该方向的书籍鱼龙混杂，普遍存在以下问题。

（1）内容结构板块单一

网络运维通常融合了网络构建技术、基础服务构建技术、网络安全技术、网络监控技术、网络分析技术五大板块，但目前市面上该类书籍通常只能包含其中一个方面，或虽有涉猎但浅尝辄止，且知识结构较为混乱，不利于学习者形成系统的知识体系。

（2）内容支撑平台单一

相关书籍多以单一系统（Windows）为基础，但服务器通常以 UNIX/Linux 系统架构，从而造成学习者知识面偏窄，不利于后期在多场景的实际工作中应用。同时，单一系统缺乏应用对比，不利于学习者的思维扩展。

（3）内容与实际工作过程脱轨

网络运维与管理是一项系统工程，有其自身特定的工作过程，但目前相关书籍多以理论阐述为主，即使搭配一些实验，也与实际的工程应用距离较远；不仅如此，这些书籍通常对传统技术或理论有较为详尽的阐述，但缺乏行业应用的前沿性和实际性。这都造成学习者在学完后无法实现从“学习”到“应用”的本质转变，即通常所说的“无法落地”。

（4）学习成本较高

相关书籍中，各种网络运维服务的实现通常是基于一定的实际硬件环境的，这也就要求学习者在学习过程中必须要有实际工作环境或实验硬件环境做支撑，从而极大提高学习成本。因为一旦失去这种环境支撑，学习者很可能无法正常开展学习过程，从而不得不中断学习。

3．编写本书的过程

于是，我们就在想：既然找不到合适的书，为什么不结合着我们实际的工作经验和技术储备，自己编写一本呢？

从2015年7月份起，在炎炎夏日中，我们开始了本书的编写过程。制定全书结构、明确内容板块、搭建工程环境、选取仿真平台、论证三级目录、实现实验验证……每天都要花费十几个小时用来进行讨论、编写和实验。就这样用了两个月完成了本书的初稿，又用了两个月进行全书通稿和修改润色。从骄阳似火到皑皑白雪，经过整整4个月的“苦行僧”式的编写生活，这本书终于完成了！

4．本书的内容

本书共9章，从内容结构上来看，包含园区网构建与Internet接入、网络基础服务建设、网络安全管理、网络运行监控、网络分析，共计5个方面的内容。

第1～3章属于园区网构建与Internet接入的内容。第1章“从建设局域网开始”主要介绍局域网的特点与分类、构建局域网的一般流程，并通过一个企业网构建案例加深读者对园区网建设的理解，从而为后续学习打下基础；第2章“越来越重要的无线局域网”主要讲解无线局域网的基本概念、常用标准等内容，并通过具体案例介绍如何构建家庭无线局域网和企业无线网，让读者对园区网构建有一个更为全面的认识；第3章“接入Internet”主要讲解接入Internet的方式和常见接入技术，并通过案例介绍家庭网络、企业网络接入Internet方式和具体实现方法。通过第1～3章的学习，完成了一个园区网络从构建到接入Internet使用的全部过程。

第4、5章属于网络基础服务建设的内容。为了让读者更好地把握重点，我们选取了所有网络建设和管理中都必须要用到的IP地址管理和域名解析服务。第4章“使用DHCP管理IP地址”主要介绍DHCP的基本概念、工作原理，并通过案例帮助读者掌握DHCP服务的具体实现与管理过程；第5章“构建DNS”主要介绍了DNS的工作原理、基本功能和高级功能的实现，以及DNS安全和DNS测试等方面内容，并通过案例帮助读者掌握DNS服务的具体实

现与管理过程。

第 6、7 章属于网络安全管理的内容。第 6 章“通过防火墙实现网络安全管理”主要从防火墙的分类、功能、安全策略、关键技术、相关标准来学习防火墙的基础知识，并通过两个案例让读者掌握企业级防火墙构建与应用；第 7 章“通过 VPN 实现远程安全接入”主要介绍 VPN 的相关协议技术及各种应用模式，并通过实践与案例帮助读者掌握构建 PPTP VPN、L2TP VPN 及 VPN 客户端的实现方法。

第 8 章“通过 SNMP 实现网络运维监控”属于网络监控管理的内容。主要对 SNMP 基础概念、安全机制、代理配置以及基于 SNMP 协议的各种网络监控系统进行介绍，并通过两个案例，让读者掌握构建网络监控服务的实现与应用。

第 9 章“学会网络分析”属于网络分析的内容。主要从网络流数据的采集、分析的原理进行讲解，并通过两个案例让读者掌握网络分析系统的应用。

本书的实践内容基于 GNS 3 仿真环境及 VirtualBox 虚拟化技术，所采用的软件和工具全部为开源、免费或试用版本，相关资源可从本书的网络支撑平台 http://ethernet.book.51xueweb.cn 获得。

5. 本书的读者对象

本书适用于以下三类读者。

一是从事网络管理，特别是网络运维工作的专业技术人员，本书可帮助他们进行深入、系统的学习，从而更好地提高工作成效。

二是准备从事网络管理和运维工作的入门者，本书可帮助他们全面理解网络建设与运维管理的技术框架，快速掌握相应的工程实现方法，为后续工作打下扎实基础。

三是高等院校中计算机相关专业、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的在校学生，本书可帮助他们加深对网络原理的理解、解决原来似是而非的理论问题、提升实践操作的综合能力，真正做到“学以致用”。

6. 本书的特点

（1）本书的内容体系以“园区网构建”→“Internet 接入”→“网络服务”→“网络监控与管理”→“网络分析”为主线，与实际网络工程实践高度融合，弥补了同类书籍知识结构体系单一的不足，有利于读者全面理解并掌握网络建设与运维管理的整体技术框架，并形成完整的知识能力体系。

（2）本书在讲解理论的同时，非常注重对学习者工程实践能力的培养。不仅如此，本书改进了同类书籍基于单一系统平台进行实践的不足，在具体的案例实现上，除了讲解在 Windows 平台实现方法之外，还着重讲解了在 UNIX/Linux 平台上的实现，拓展了读者的技术视野、满足了行业的实际工程需求。

（3）本书的实践内容基于 GNS 3 仿真环境及 VirtualBox 虚拟化技术，有效解决了读者在学习时由于实践环境的限制只能“纸上谈兵”的状况，帮助读者在一台笔记本电脑上即可轻松构建复杂网络并进行相应的管理和分析，极大降低了学习成本，保证了学习过程的顺利开展。

（4）本书中所使用的案例，均来自于作者具体的工作实践，并经过了长期具体应用的锤炼，具有很强的实用性和严谨性。不仅如此，所有案例的编写，均结合实际工作场景，通过“需求分析”→“规划设计”→“技术论证”→“部署实施”→“总结分析”的步骤来逐步实现，从而帮助学习者以工程的思维方式解决实际工作中的应用技术问题。

（5）本书在编写中充分注重互联网技术发展迅猛的特点，在内容上注入了行业前沿应用技术，具有一定的前瞻性。

7. 感谢

没有家人们的默默支持，我们不可能全身心地投入到本书的编写中，这本书也不可能在短短 4 个月内“一气呵成”，对于他们，除了感谢还有发自内心的一丝愧疚。

在本书内容框架的制定过程中，我的恩师、河南中医学院的程万里教授给予了许多颇具建设性的指导，使得本书的技术体系更加科学合理。在本书的具体编写过程中，河南中医学院信息技术开放科研创新平台的陈凯杰、杨明、路景鑫等同学参与了本书的资料收集、整理、技术研讨、实验测试及文字撰写工作，为本书的成书付出了辛勤劳动。

本书编写完成后，中国水利水电出版社万水分社的雷顺加主编、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，使得本书得以顺利出版，在此一并表示深深的谢意！

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

2015 年 11 月于河南中医学院天一湖畔

II 配套光盘使用说明

一、配套光盘有什么？

本书中配套光盘由两部分组成，具体内容为：

1．本书配套使用的多媒体教学课件，主要包含.pptx 和.pdf 两种格式，方便读者在不同的环境下浏览多媒体教学课件。

2．本光盘中所提供的软件资源，主要为本书内容中所使用的软件，方便读者直接对本书中的案例与实训进行学习。

二、为什么为本书配备光盘？

为本书增加配套光盘，是从以下几方面考虑：

1．总结、提炼书籍内容，并以多媒体课件的形式展示出来，方便读者了解本书的知识架构与体系，对书籍内容有一个更为宏观的认识。

2．提供大量真实可用软件资源，方便读者随时进行实验验证与学习，更为直观地了解书中的知识点。虽然软件均可以通过互联网下载，但是考虑到软件版本不断变化的实际情况和部分软件的文件很大，下载需要时间较长，为了方便读者能够快速进行实践，将本书中所用的软件资源统一用光盘收录。

3．提供本书撰写过程中使用的同一版本的软件资源，方便读者以更为接近本书实验环境的方式进行实验，方便读者对书籍中知识点的学习与理解。

4．本光盘提供的软件资源具有免费、开源的特点，既体现出本书的特色，又可以降低读者的学习成本，使读者轻松学习，收获更多知识。

III

目录

1 从建设局域网开始

本书的学习与实践，就从局域网的建设开始。

局域网技术是计算机网络研究和应用的一个热点，也是目前计算机网络技术发展最快的领域之一，在企业、机关、学校等各种单位中得到了广泛的应用。局域网是封闭型的，可以由办公室内的两台计算机组成，也可以由一个园区内的上千台计算机组成，不仅如此，局域网也是建立互联网络的基础。

本章着重介绍局域网的特点与分类、局域网的主要设备、构建局域网的一般流程，并通过一个企业网构建实例，加深读者的理解。

1.1 认识局域网

1.1.1 下个定义

20 世纪 70 年代中期，由于大规模集成电路和超大规模集成电路的发展，计算机的功能大大增强、成本不断降低，为计算机的普及奠定了基础。但是，当时一台计算机处理能力还是非常有限，为了实现资源共享和方便交流，就在较小范围内进行了计算机互联，因此出现了计算机网络研究的新领域，这就是计算机局域网。

局部区域网络（Local Area Network，LAN），简称局域网或 LAN，它既有计算机网络的特点，又有自己独有的特征。它是在一个局部的地理范围内（如一个学校、工厂和机关单位），将各种计算机、外部设备和数据库等互相联接起来组成的计算机通信网。它可以通过数据通信网或专用数据电路，与远方的局域网、数据库或处理中心相连接，构成一个大范围的信息处理系统。

1.1.2 局域网有什么特点

局域网与广域网不同，它的覆盖范围一般限制在一定距离区域内。正因为如此，使局域网具有以下几个主要特点。

（1）通信速率高

由于距离较近，且结构相对简单，因此局域网的数据传输速率比较高，以以太网为例，从早期的10Mb/s 到后来的 100Mb/s、1000Mb/s，目前已达到 10Gb/s。随着局域网技术的进一步发展，数据传输目前正在向着更高的速度发展。

（2）通信质量好，传输误码率低

局域网具有较低的延迟和误码率。这是因为局域网通常采用短距离传输，可以使用高质量的传输介质，从而提高传输质量。

误码率（Bit Error Rate，BER），又称位错率，指在一段时间内，传输错误的比特占所传输比特的比率。局域网的传输质量很高，它的传输误码率通常低于 10^{-7}，即平均每传送 10^{7} 个比特才会出现一个比特的错误。

（3）通常属于某一部门、单位或企业所有

局域网的经营权和管理权通常属于某个单位所有，这一点与广域网通常由服务提供商运营不同。由于局域网的范围一般在 0.1～2.5km 之内，分布简单和高速传输使它适用于一个企业、一个部门的管理，所有权可归某一单位，在设计、安装、操作使用时由单位统一考虑、全面规划，不受公用网络当局的限制。

（4）支持多种通信传输介质

根据网络本身的性能要求，局域网中可使用多种通信介质，例如电缆（细缆、粗缆、双绞线）、光纤及无线传输等。

（5）成本低，安装、扩充及维护方便

局域网是在一个局部地区范围内，把各种计算机、外围设备、数据库等相互连接起来组成的计算机通信网。相对广域网而言，局域网安装简单，可扩充性好，尤其在目前大量采用以交换机为中心的星形网络结构的局域网中，扩充服务器、工作站等十分方便，若某站点出现故障时整个网络仍可以正常工作。

（6）宽带局域网，可以实现数据、语音和图像的综合传输

宽带局域网（Broadband LAN）是一种对数据进行编码、复用以及通过载波调制来实现数据传输的局域网，使用宽带局域网可以使数据、语音和图像进行综合传输。目前宽带局域网已经成为局域网的主流，已经出现了实际应用中的万兆宽带局域网。

1.1.3 局域网能干什么

局域网最主要的功能是提供资源共享和相互通信，它可提供以下几项主要服务。

（1）资源共享

它包括硬件资源共享、软件资源共享及信息数据共享。在局域网上每个用户可共享安装的硬件资源，如大型外部存储器、绘图仪、激光打印机、图文扫描仪等特殊外设；用户可共享网络上系统软件与应用软件，避免重复投资及重复劳动；网络技术可使大量分散的数据迅速集中、分析和处理，分散在网内的计算机用户可以共享网内的大型数据库而不必重新设计这些数据库。

（2）数据传送和电子邮件

数据和文件的传输是网络的基本功能，主要完成计算机在局域网中传送文件、数据信息、声音、图像和视频等。

局域网站点之间可提供电子邮件服务，某网络用户输入信件并传送给另一用户，收信人可打开“邮箱”阅读信件后，写回信发回源用户电子邮件，既节省纸张又快捷方便。

（3）分布式处理

利用网络技术能将多台计算机连成具有高性能的计算机系统，采用适当的算法，将大型的综合性问题分给不同的计算机去完成，在网络上可建立分布式数据库系统，使整个计算机系统的性能大大提高。同时，局域网中的计算机可以互为备份系统，当一台计算机出现故障时，可以调用其他计算机代替实施任务，从而提高了系统的安全可靠性。

（4）文件共享

一个局域网内主机如果想使用别的主机上的文件，可通过文件共享服务进行获取，文件共享后同一局域网内的主机都可以访问与使用，无需复杂地使用 U 盘进行拷贝获取文件。

1.1.4 五花八门的局域网

局域网有许多不同的分类方法，如按拓扑结构分类、按传输介质分类、按介质访问控制方法分类等。

（1）按拓扑结构分类

局域网拓扑结构通常可分为：总线型拓扑结构、星型拓扑结构、环型拓扑结构、树型拓扑结构和网状型拓扑结构。

1）总线型拓扑结构。

总线型拓扑结构采用一条称为总线的中央主电缆，所有网上计算机都通过相应的硬件接口直接连在总线上（见图 1-1）。由于其信息向四周传播，类似于广播电台，故总线网络也被称为广播网络。

优点：结构简单灵活，非常便于扩充；可靠性高，网络响应速度快；设备量少，价格低，安装使用方便；共享资源能力强，便于广播式工作。

缺点：一点失效会引起多点失效，故障定位困难，任何时刻只能有一个节点发送数据，电缆连接设备有限。

总线型拓扑结构曾经是使用最广泛的结构，也是相对传统的一种主流网络结构，适合于信息管理系统、办公自动化系统等应用领域。

2）星型拓扑结构。

这种结构是目前在局域网中应用得较为普遍的一种。它是因网络中的各工作站（主机）通过一个网络集中设备（如集线器或者交换机）连接在一起，呈星状分布而得名（见图 1-2）。这类网络目前用得最多的传输介质是双绞线或光纤。

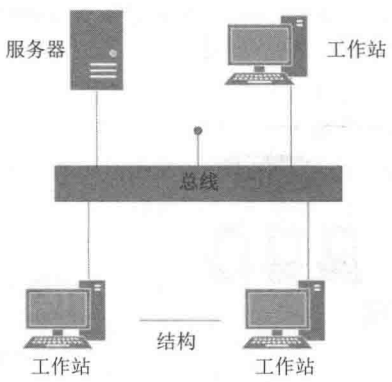


图 1-1 总线型拓扑结构

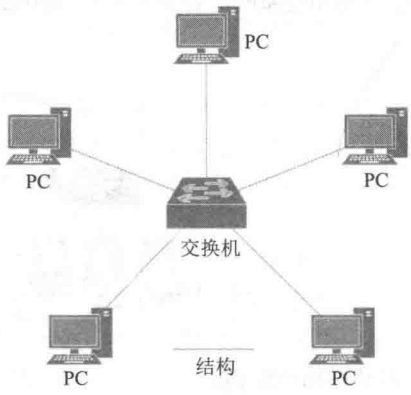


图 1-2 星型拓扑结构

优点：易于维护，安全；组网简单，易于集中控制，误码率低。

缺点：网络共享能力差，通信线路利用率低，中央节点负载过重。

3）环型拓扑结构。

环型拓扑结构中各节点通过环路接口连在一条首尾相连的闭合环形通信线路中。环路上任何节点均可以请求发送信息，也可以接收环路上的任何信息。环中维持一个“令牌”，“令牌”在环型连接中依次传递，谁获得令牌就可以进行信息发送，通常把这种拓扑结构的网络称之为“令牌环网”。图 1-3 所示为环型拓扑结构。

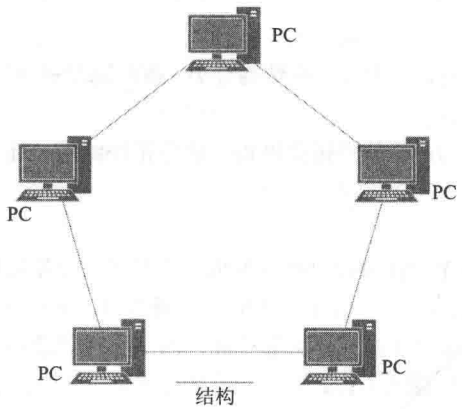


图 1-3　环型拓扑结构

优点：路由选择简单，可靠性高，时间延迟确定。

缺点：环路封闭，扩充不方便；节点过多，传输率低。

4）树型拓扑结构。

树状网络也称为多级星型网络，通常是由多个层次的星型结构连接而成的（见图 1-4）。树的每个节点一般是网络互连设备，如交换机或路由器等。一般来说，越靠近树的根部，节点设备的性能就越好。与单一星型网络相比，树状网络的规模更大，而且扩展方便，但是结构也较为复杂。在一些实际的局域网建设中（例如校园网、企业网等），采用的多是树状结构网络。

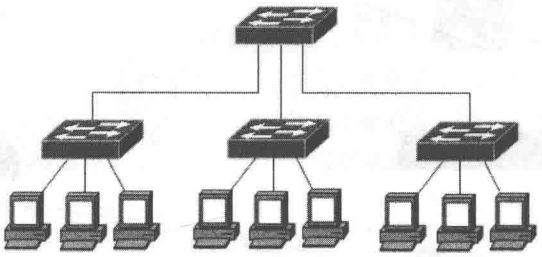


图 1-4　树型拓扑结构

5）网状型拓扑结构。

网状型拓扑结构是将多个子网或多个局域网连接起来构成的（见图 1-5）。根据组网硬件不同，主要