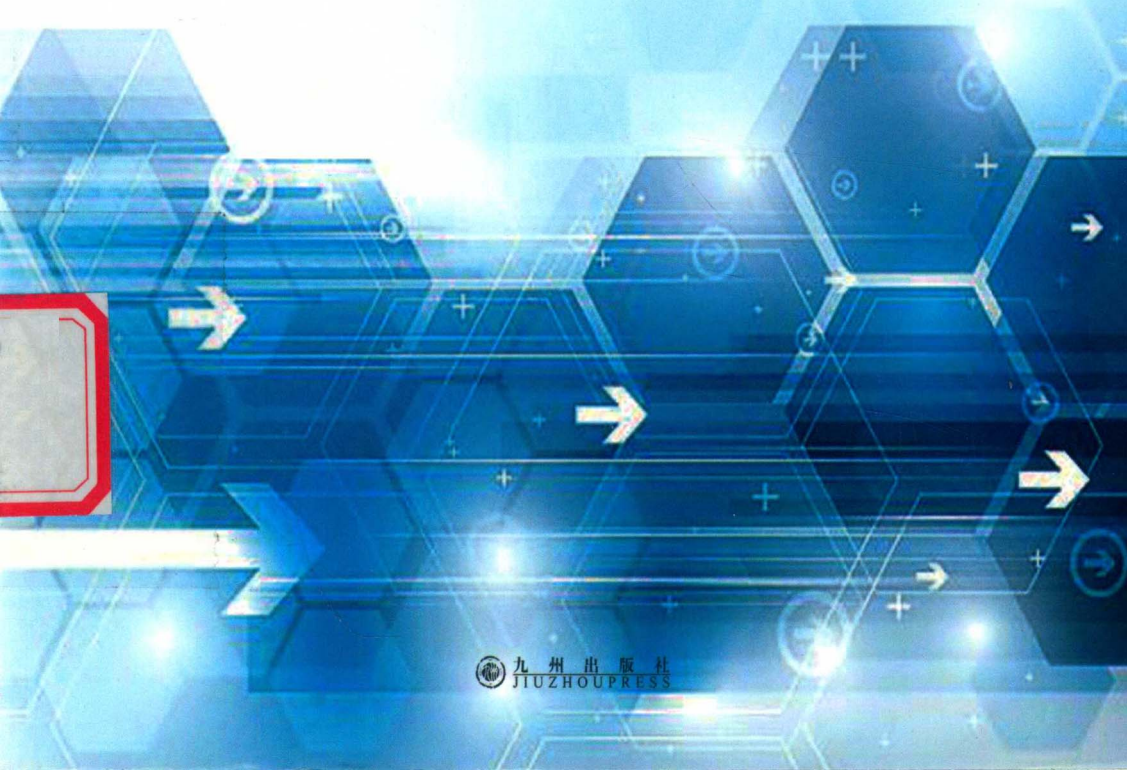
计算机网络信息安全管理

梁松柏 著



九州出版社
JIUZHOUPRESS

计算机网络信息安全管理

梁松柏　著

九州出版社
JIUZHOUPRESS

图书在版编目（CIP）数据

计算机网络信息安全管理 / 梁松柏著. -- 北京 : 九州出版社, 2017.10

ISBN 978-7-5108-6332-5

Ⅰ. ①计… Ⅱ. ①梁… Ⅲ. ①计算机网络－网络安全－安全管理 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2017)第 264265 号

计算机网络信息安全管理

作　　者：梁松柏 著

出版发行：九州出版社

地　　址：北京市西城区阜外大街甲 35 号(100037)

发行电话：(010)68992190/3/5/6

网　　址：www.jiuzhoupress.com

电子信箱：jiuzhou@jiuzhoupress.com

印　　刷：北京朗翔印刷有限公司

开　　本：710 毫米×1000 毫米　16 开

印　　张：14

字　　数：200 千字

版　　次：2018 年　6 月第 1 版

印　　次：2018 年　6 月第 1 次印刷

书　　号：ISBN 978-7-5108-6332-5

定　　价：56.00 元

前 言

随着信息社会的发展，人类的生存方式、生活方式和行为方式正发生着巨大的变化。计算机网络信息系统作为信息社会的基础性设施，已发展应用到国民经济的各个领域和社会生活的各个方面，成为国家事务、经济建设等重要领域和人们日常生活必不可少的组成部分，深深地影响并改善着人们的生活。

但是，计算机网络信息系统本身所固有的脆弱性使得信息系统安全问题无处不有、无时不在，人们的生产生活秩序也随之受到影响或破坏，信息系统安全问题也因此成为信息社会所面临的重要威胁。好在多数网络信息系统安全问题是可以通过科学的安全管理来避免的，因此，有必要深入研究信息系统安全管理问题以保证信息系统安全运行，从而保证社会活动的正常有序。

本书围绕计算机网络信息系统安全问题，针对信息系统安全所面临的威胁，依据相关标准和法律法规，从主动预防、积极应对、巡查防控和法律控制等几个方面来研究计算机网络信息系统安全管理问题。

（1）主动预防是通过信息系统安全等级保护来落实各项安全措施，通过研究信息系统安全等级保护的定级和测评来优化资源配置和全面提升系统防护能力。

（2）通过对信息安全事件的监测和响应，结合应急预案和应急联动体系，力争及早发现和及时处置信息安全事件，将信息安全事件造成的损失降到最小。

（3）通过对信息内容安全巡查系统的研究来提高巡查效率，及时发现网上违法信息并进行合理的处置，防止和控制这些信息在计算机网络上的扩散和传播。

（4）通过对现有法律体系的研究为制定实施信息系统安全管理措施寻求更好的法律依据，对网络违法犯罪活动进行更有效防范和更严厉打击，从而进一步提高信息系统安全保障能力。

本书由来自中共山东省委党校的梁松柏编写，在写作过程中，一些同行专家、学者的有关著作、论文，扩展了我的视野，提高了我的专业认识与水平，并吸取了他们的一些研究成果，在此谨致诚挚的谢意。限于作者水平，书中难免有许多不妥之处，恳请同行专家、学者和广大读者惠予批评指正。

目 录

第一章 计算机网络基础

第一节 计算机网络简介

计算机网络是计算机科学技术与通信技术逐步发展、紧密结合的产物，是信息社会的基础设施，是信息交换、资源共享和分布式应用的重要手段。随着信息社会的蓬勃发展和计算机网络技术的不断更新，计算机网络的应用已经渗透到各行各业乃至于家庭之中，并且不断地改变着人们的思想观念、工作模式和生活方式。一个国家的信息基础设施和网络化程度已成为衡量其现代化水平的重要标志。

一、网络的基本概念

计算机网络是为满足应用的需要而发展起来的，从其本质上说，它是以资源共享为主要目的，即发挥分散的、各不相连的计算机之间的协同工作功能。因此，对计算机网络可作如下定义：凡将地理位置不同、具有独立工作能力的多个计算机系统，通过通信设备和线路连接起来，并由功能完善的网络软件（网络协议、信息交换方式及网络操作系统等）实现资源共享、信息交换或协同工作的计算机系统，称为计算机网络。图 1.1 给出了一个简单的网络系统示意图，它将若干台计算机、打印机和其他外部设备互联成一个整体。连接在网络中的计算机、外部设备和通信控制设备等称为网络节点。

计算机网络涉及通信和计算机两个领域，通信技术与计算机技术的结合是产生计算机网络的基本条件。一方面，通信技术为计算机之间的数据传递和交换提供了必要手段；另一方面，计算机技术的发展应用到通信技术中，又提高了通信网络的各种性能。

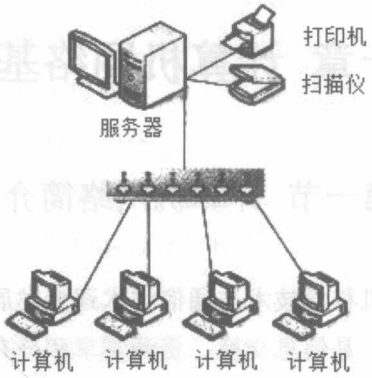


图 1.1　计算机网络系统示意图

二、网络的组成

计算机网络要实现如前所述的功能，必须具有数据处理和数据通信两种能力。从用户角度出发，计算机网络可以看成是一个透明的数据通信机构，网上用户在访问网络中的资源时不必考虑网络的存在。从网络逻辑功能来看，可以将计算机网络分成通信子网和资源子网两部分，如图 1.2 所示。

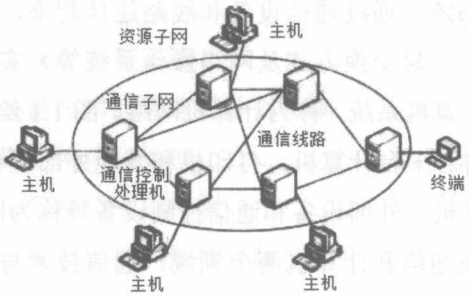


图 1.2　通信子网和资源子网

（一）通信子网

网络系统以通信子网为中心，通信子网处于网络的内层，由网络中的通信控制处理机、其他通信设备、通信线路和只用作信息交换的计算机组成。通信子网的任务是负责完成网络数据传输和转发等通信处理任务。当前的通

信子网一般由网卡、通信线路、集线器、网桥、交换机、路由器等设备和相关软件组成。

（二）资源子网

资源子网处于网络的外围，由主机系统、终端、终端控制器、外设、各种软件资源与信息资源组成。资源子网的任务是负责全网的数据处理业务，向网络用户提供各种网络资源和网络服务。主机系统是资源子网的主要组成部分，它通过高速通信线路与通信子网的通信控制处理机相互连接，普通用户终端可通过主机系统连接入网。

随着计算机网络技术的不断发展，在现代网络系统中，直接使用主机系统的用户在减少，资源子网的概念已有所变化。

三、网络的分类

计算机网络是非常复杂的系统，有多种多样的划分方法，不同类型的网络在性能、结构、用途等方面的特点也是有区别的。事实上，这些不同的分类方法对于网络本身并无实质的意义，只反映人们研究网络的角度不同。从不同的角度划分网络系统、观察网络系统，有助于全面了解网络系统的特性。

（一）按网络的覆盖范围进行分类

按覆盖范围，通常将网络划分为局域网、城域网和广域网。按覆盖范围划分是最常见的网络划分方式。

1.局域网（Local Area Network，LAN），又称为局部区域网，是目前网络技术发展最快的领域之一。一般用微型计算机通过高速通信线路相连，覆盖范围为几百米到几千米，通常用于连接一个实验室、一幢或几幢大楼。局域网的规模相对于城域网和广域网而言较小。在局域网内数据传输速率较高，目前局域网最快速率可达到 10Gbit/s；传输可靠性好，误码率低（在 10^{-7}~10^{-12} 之间）；网络结构简单，配置灵活，容易实现。局域网协议标准是美国电气工程师协会制订的 IEEE802 系列标准，根据采用的技术和协议标准的不同，局域网可分为共享式局域网与交换式局域网。

2.城域网（Metropolitan Area Network，MAN）所覆盖的地域范围介于局域网和广域网之间，一般从几十千米到几百千米的范围。城域网通常是使用高速的光纤网络，在一个特定的范围内（例如校园、社区或城市）将不同的

局级网连接起来，构成一个覆盖该区域的网络，其传输速率比局域网高。

3.广域网（Wide Area Network，WAN）又称为远程网。广域网的作用范围通常为几十千米到几千千米，覆盖一个地区、国家甚至横跨全球，形成国际性的网络。广域网的通信子网主要使用分组交换技术，它可以使用公用分组交换网、卫星通信网和无线分组网，可以适应大容量、突发性的通信需求。广域网常常借用传统的公共传输网（如电话网）进行通信，可以实现较大范围内的资源共享，但同时广域网的数据传输率比局域网系统慢，传输错误率也较高。随着新的光纤标准和能够提供更宽和更快传输率的全球光纤通信网络的引入，广域网的数据传输率也将大大提高。

（二）按网络的交换方式进行分类

按网络采用的交换方式进行分类，计算机网络可分为电路交换网、报文交换网和分组交换网。

1.电路交换网。电路交换与传统的电话转接非常相似，即在两台计算机开始通信时，必须申请建立一条从发送端到接收端的物理连接路。在通信过程中自始至终使用这条线路进行信息传输，直至传输完毕。由于通常不可能在任意两台计算机之间铺设一条线路，所以当多对计算机之间同时要求通信时，电路交换方式这种独占信道的特性使线路的利用率不能得到有效发挥，经常造成“拥塞”。

2.报文交换网。报文交换是随着计算机功能的增强，转接交换机由过去的公共电话网的机械设备变为具有存储功能的程控设备。通信开始时，发送端计算机发出的报文被存储在交换机中，交换机根据报文的目的地址选择合适的路径发送。因此，报文交换方式也称为“存储——转发”方式。

3.分组交换网。通常一个报文包含的数据量较大，转接交换机需要有较大容量的存储设备，而且需要的线路空闲时间也较长，实时性差。因此，在报文交换的基础上又提出了分组交换。在分组交换方式中，发送端先将数据划分为一个个等长的单位（即分组），这些分组逐个由各中间节点采用“存储——转发”方式进行传输，最终到达接收端并由接收端把收到的分组再拼装成一个完整的报文。由于分组长度有限而且统一，分组可以在中间节点的内存中进行存储处理，其转发速度大大提高。

（三）按网络的使用用途进行分类

按网络的使用用途，计算机网络可分为公用网和专用网。

1.公用网也称为公众网或公共网，是指为公众提供公共网络服务的网络。公用网一般由国家的电信公司出资建造，并由国家政府电信部门进行管理和控制，网络内的传输和转接装置可提供给任何部门和单位使用（需交纳相应费用）。公用网属于国家基础设施。

2.专用网是指一个政府部门或一个公司组建经营的，仅供本部门或单位使用，不向本单位以外的人提供服务的网络。例如军队、民航、铁路、电力、银行等系统均有其系统内部的专用网。一般较大范围内的专用网需要租用电信部门的传输线路。

（四）按网络的连接范围进行分类

按网络的连接范围，计算机网络可分为互联网、内联网（Intranet）和外联网（Extranet）。

1.互联网是指将各种网络互联起来形成的一个大系统。在该系统中，任何一个用户都可以使用网络的线路或资源。目前，互联网已经发展到全球范围，包含了成千上万个相互协作的组织及网络的集合。互联网的发展速度之快以至于很难有人能确切地说出它到底包含了多少用户，并且还在以惊人的速度发展着。

2.内联网是基于互联网的 TCP/IP 协议，使用 WWW 工具，采用防止入侵的安全措施，为企业内部服务，并有连接互联网功能的企业内部网络。内联网是根据企业内部的需求而设置的，它的规模和功能是根据企业经营和发展的需求而确定的。可以说，内联网是互联网的更小版本。

3.外联网是指基于互联网的安全专用网络，其目的在于利用互联网把企业和其贸易伙伴的内联网安全地互联起来，在企业和其贸易伙伴之间共享信息资源。从技术角度讲，外联网是在保证信息安全的同时扩大网络的访问范围；从企业角度讲，外联网是将企业及其供应商、销售商、客户联系在一起的合作网络。

（五）按照拓扑结构分类

根据计算机网络中各计算机之间连接方式的不同而归纳出的拓扑结构来

划分计算机网络的类型，可以分为星形、总线形、环形、树形和网状等多种类型网络。按照拓扑结构分类是对计算机网络进行分类的一种非常重要的方法，拓扑结构的有关知识将在后面的章节中详细介绍。

除了上述常见的网络划分外，还有以下分类方法。例如，按链路采用的传输介质分为有线网络和无线网络；按网络的信道带宽分为窄带网、宽带网和超宽带网；按工作原理分为以太网、令牌环网、FDDI 网、ATM 网；按网络的通信传播方式，可分为点对点网络和广播式网络等。

四、网络的主要功能

以资源共享为目标组建起来的计算机网络，一般具有如下的几个重要功能。

（一）资源共享

计算机网络最主要的功能是实现网络资源共享。资源共享对信息化建设具有重要意义。从系统投入方面考虑，网络用户可以共享计算机网络中的硬件资源，如打印机、扫描仪等，这对节省硬件设备费用意义重大。另外，由于现代社会产生的信息量越来越大，单台计算机的存储和处理能力远远不够，将这项任务分摊给网络上的不同计算机是一种有效的解决方案。特别是计算机软件是人类社会的共同财富，有大量的软件是可以免费共享的，网络中的任何计算机都可以共享这些资源。

资源共享功能不仅使网络用户可以克服地理位置上的差异，共享网络中的资源，为用户提供极大的方便，而且资源共享能有效地提高网络资源的利用率。

（二）数据通信

网络中的计算机与计算机之间交换各种数据和信息，并根据需要对这些信息进行分类或集中处理，这是计算机网络提供的最基本的数据通信功能。数据通信提供了信息快捷交流的手段，如电子邮件、电子商务、远程教育、远程医疗等，这在当今的信息化时代显得尤其重要。

（三）均衡负荷

利用计算机网络技术，在网络操作系统的调度和管理下，当某个主机系统的负担过重时，可以将某些任务通过网络转移至负荷较轻的主机系统中去

处理，以便均衡负荷，减轻局部负担，提高设备和系统的利用率，增加整个系统的可用性。

（四）分布式处理

网络技术的发展，使分布式计算与处理成为可能。对于综合性的大型问题，可以采用适当的算法，将任务分配给网络中的多台计算机，由这些计算机分工协作来完成，如分布式数据库系统。此外，利用计算机网络技术还可以把许多小型机或微机连接成具有大型机处理能力的高性能计算机系统，使其具有解决复杂问题的能力，如网格计算（Grid Computing）技术等。

（五）提高系统的可靠性

在一个单机系统中，若某个部件或计算机发生故障时，必须通过替换资源的办法来维持系统的继续运行，否则系统便无法开展正常的工作。而在计算机网络中，由于设备彼此相连，当一台机器出现故障时，可以通过网络寻找其他机器来代替本机工作；而且每种资源（尤其是程序和数据）可以存放在多个地点，用户可以通过多种途径来访问网内的某个资源，从而避免了单机失效时对用户产生的影响。因此，比起单机系统来，整个网络系统的可靠性大为提高。

事实上，从应用角度讲，计算机网络还有许多其他功能。随着网络技术的不断发展，各种网络应用将层出不穷，并将逐渐深入到社会的各个领域及人们的日常生活中，改变人们的工作、学习、生活乃至思维方式。

五、网络的拓扑结构

拓扑结构是决定通信网络性质的关键要素之一。“拓扑”一词来源于拓扑学，拓扑学是几何学的一个分支，它把实体抽象成与其大小、形状无关的点，将点到点之间的连接抽象成线段，进而研究它们之间的关系。计算机网络中也借用这种方法来描述网络节点之间的连接方式。具体而言，就是将网络中的计算机和通信设备抽象成节点，将节点与节点之间的通信线路抽象成链路。这样整个计算机网络的物理结构被抽象成由一组节点和若干链路组成的几何图形。这种计算机网络物理结构的图形化表示方法称为计算机网络拓扑结构，或称网络结构。计算机网络拓扑结构是组建各种网络的基础，不同的网络拓扑结构涉及不同的网络技术，对网络的设计、性能、可靠性和通信

费用等方面都有重要的影响。

计算机网络的拓扑结构，按通信系统的传输方式可分成两大类：点对点传输结构和广播传输结构。

（一）点对点传输结构

所谓点对点传输就是“存储——转发”传输。每条物理线路连接一对节点，没有直接链路的两节点之间必须经其他节点转发才能通信。点对点传输结构通常为远程网和大城市网所采用，网络的拓扑结构有星形、环形、树形和网状。

1.星形结构。以一台计算机为中心机，并用单独的线路使中心机与其他各节点相连，任何两节点之间的数据传输都要经过中心机的控制和转发，如图1.3 所示。中心机控制着全网的通信，故中心机的可靠性是至关重要的，它的故障可能会导致整个网络瘫痪。星形结构的优点是拓扑结构简单，易于组建和管理，对外围节点要求不高；增加节点时成本低。节点故障容易检测和隔离，单个站点的故障只影响一个设备，不会影响全网。以集线器为中心的局域网是一种最常见的星形拓扑结构网络。

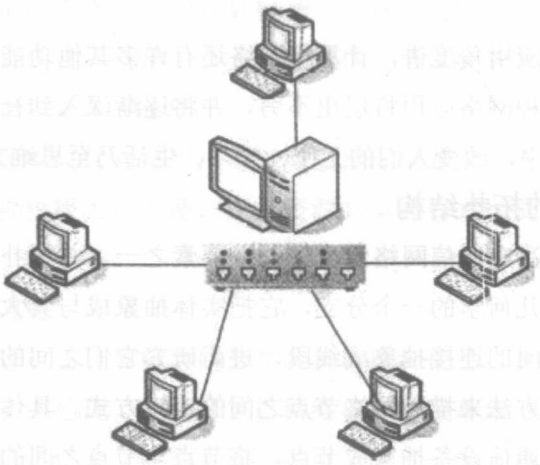


图 1.3　星型网络结构

2.树形。拓扑结构是一种分级结构，节点按层次进行连接，如图 1.4 所示。全网中有一个顶层的节点（树根节点），其余节点按上、下层次进行连接，数据传输主要在上、下层节点之间进行，同层节点之间数据传输时要经上层

转发。这种结构的优点是灵活性好，通信线路连接简单，网络管理软件也不复杂，维护方便。树根节点具有统管整个网络的能力，而且可以逐层次扩展网络；但缺点是资源共享能力差，可靠性低。若某一个子节点出故障，则和该子节点连接的终端均不能工作。

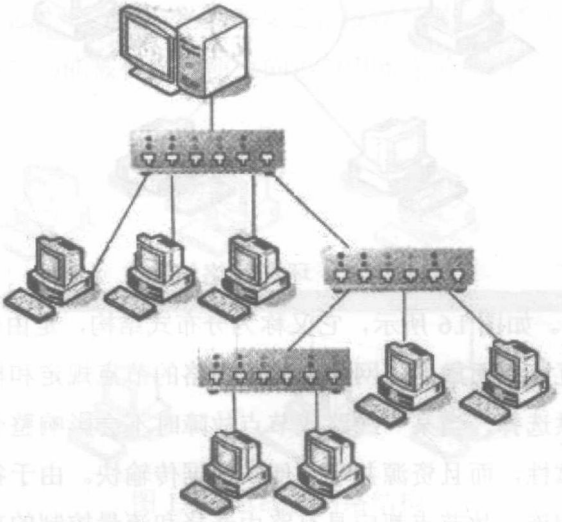


图 1.4　树形网络结构

3.环形。网络中各计算机节点通过环路接口连接到一条首尾相连的闭环通信线路中，任意两个节点之间的通信必须通过环路，如图 1.5 所示。在环形拓扑结构中，该环路是共用的，单条环路只能进行单向通信。环路中各节点的地位和作用是相同的，因此容易实现分布式控制。环形拓扑结构的优点是传输控制机制较为简单，传输速率高，网络最大传输时延固定，实时性强。其缺点是可靠性差，当环路上的一个节点出现故障时就会造成整个网络的瘫痪。在某些网络中为了提高可靠性而采用了双环结构，一旦节点出现故障，自动启动备份环工作。因此，双环的可靠性明显优于单环。由于环形网络独特的优势，它被广泛地应用在分布式处理中。

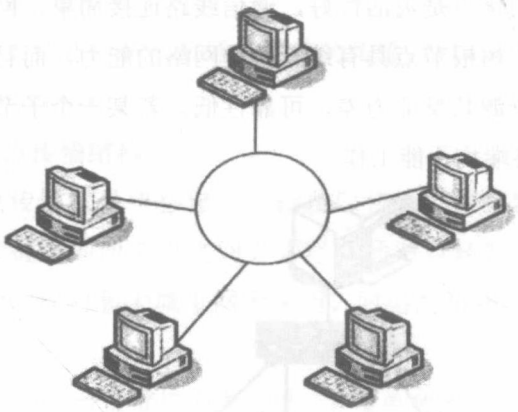


图 1.5　环形网络结构

4.网状结构。如图 1.6 所示，它又称为分布式结构，是由分布在不同地点的多个节点相互连接而成的。网状结构无严格的节点规定和构形，节点之间有多条线路可供选择，当某一线路或节点故障时不会影响整个网络的工作，具有较高的可靠性，而且资源共享方便，数据传输快。由于各个节点通常和另外多个节点相连，故节点都应具有路由选择和流量控制的功能，网络管理软件比较复杂，硬件成本较高。一般情况下，网状结构常用于广域网中，可在广域网的主要节点之间实现高速通信，在局域网中很少采用这种网状结构。

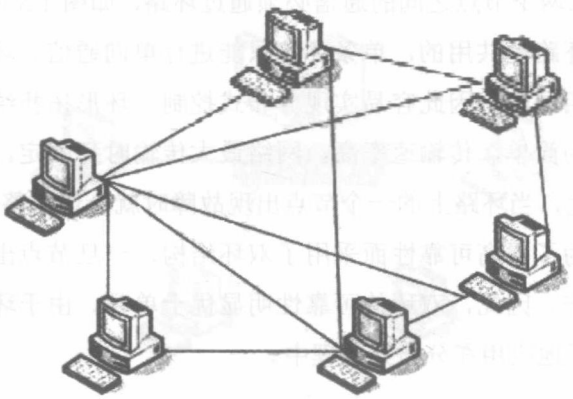


图 1.6　网状网络结构

（二）广播式传输结构

在广播式传输结构中，多个网络节点共享一个公共的传输介质。这样，