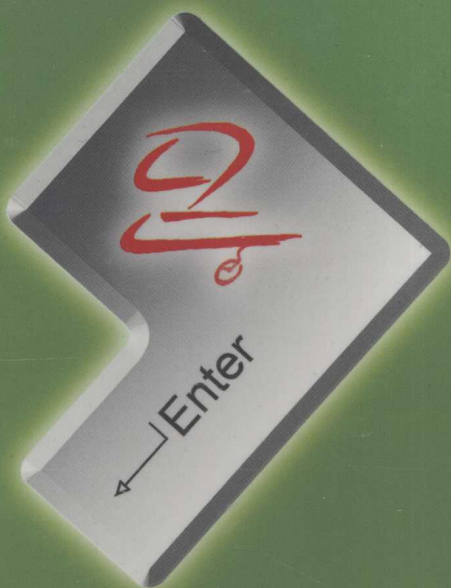


高等院校

计算机技术系列教材



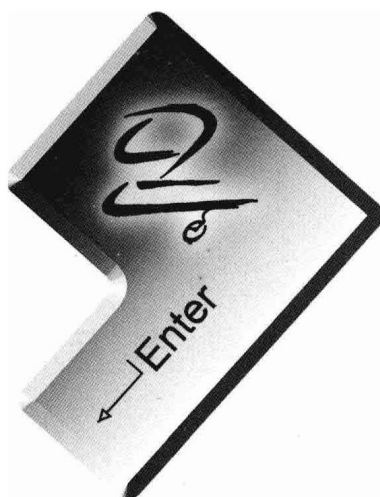
计算机网络管理与安全技术

■ 杜威 主编



WUHAN UNIVERSITY PRESS

武汉大学出版社



图书在版编目(CIP)数据

计算机网络管理与安全技术/杜威主编. —武汉:武汉大学出版社,2008.9
高等院校计算机技术系列教材
ISBN 978-7-307-06522-2

I. 计… II. 杜… III. ①计算机网络—管理—高等学校—教材 ②计
算机网络—安全技术—高等学校—教材 IV. TP393

中国版本图书馆 CIP 数据核字(2008)第 143832 号

责任编辑:杨 华 责任校对:王 建 版式设计:詹锦玲

出版发行:武汉大学出版社 (430072 武昌 珞珈山)

(电子邮件:wdp4@whu.edu.cn 网址:www.wdp.whu.edu.cn)

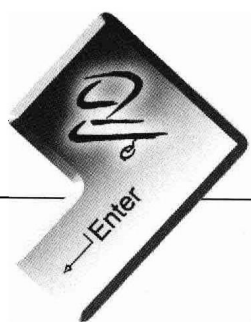
印刷:湖北金海印务公司

开本:787×1092 1/16 印张:16.25 字数:388千字 插页:1

版次:2008年9月第1版 2008年9月第1次印刷

ISBN 978-7-307-06522-2/TP·310 定价:26.00元

版权所有,不得翻印;凡购买我社的图书,如有缺页、倒页、脱页等质量问题,请与当地图书销售部门联系调换。



高等院校计算机技术系列教材 编委会

主 任

魏长华

副 主 任

朱定华 金汉均

委 员

(按姓氏笔画为序)

王敬华 王淑礼 汪金友 吴黎兵 张晓春

杜 威 倪永军 姚春荣 胡新和 胡艳蓉

岑柏兹 曾 志 鲍 琼 戴上平 魏 敏

魏媛媛



总 序



进入 21 世纪以来,人类已步入了知识经济的时代。作为知识经济重要组成部分的信息产业已经成为全球经济的主导产业。计算机科学与技术的信息产业中占据了极其重要的地位,计算机技术的进步直接促进了信息产业的发展。在国内,随着社会主义市场经济的高速发展,国民生活水平的不断提高,尤其 IT 行业在国民经济中的迅猛渗透和延伸,越来越需要大量从事计算机技术方面工作的高级人才加盟充实。

另一方面,随着我国教育的不断深入,高等教育已经完成了从精英教育向大众化教育的转变,在校大学本科和专科计算机专业学生的人数大量增加,接受计算机科学与技术教育的对象发生了变化。我国的高等教育进入了前所未有的大发展时期,时代的进步与发展对高等教育提出了更高、更新的要求。早在 2001 年 8 月,教育部就颁发了《关于加强高等学校本科教学工作,提高教学质量的若干意见》。文件明确指出,本科教育是高等教育的主体和基础,抓好本科教学是提高整个高等教育质量的重点和关键。2007 年 1 月,国家教育部和财政部又联合启动了“高等学校本科教学质量与教学改革工程”(以下简称“质量工程”)。“质量工程”以提高高等学校本科教学质量为目标,以推进改革和实现优质资源共享为手段,按照“分类指导、鼓励特色、重在改革”的原则,加强内涵建设,提升我国高等教育的质量和整体实力。

本科教学质量工程的启动对高等院校的从事计算机科学与技术教学的教师提出了一个新的课题:如何在新形势下培养高素质创新型的计算机专业人才,以适应于社会进步的需要,适应于国民经济的发展,增强高新技术领域在国际上的竞争力。

毋庸置疑,教材建设是“本科教学质量工程”的重要内容之一。新时期计算机专业教材应做到以培养学生思考问题、发现问题、分析问题和解决问题的实际能力为干线,以理论教学与实际操作相结合,“案例、实训”与应用问题相结合,课程学习与就业相结合为理念,设计学生的知识结构、能力结构、素质结构的人才培养方案。为了适应新形势对人才培养提出的要求,在教材的建设上,应该体现内容的科学性、先进性、思维性、启发性和实用性,突出中国学生学习计算机专业的特点和优势,做到“够用、能用、实用、活用”。这就需要从总体上优化课程结构,构造脉络清晰的课程群;精练教学内容,设计实用能用的知识点;夯实专业基础,增强灵活应用的支撑力;加强实践教学,体现理论实践的连接度,力求形成“基础课程厚实,专业课程宽新,实验课程创新”的教材格局。

提高计算机科学与技术课程的教学质量,关键是要不断地进行教学改革,不断地进行教材更新,在保证教材知识正确性、严谨性、结构性和完整性的条件下,使之能充分反映当代科学技术发展的现状和动态,使之能为学生提供接触最新计算机科学理论和技术的机会;教材内容应提倡学生进行创新性的学习和思维,鼓励学生动手能力的培养和锻炼。在这个问题上,计算机科学与技术这个领域表现得尤为突出。





正是在这种编写思想指导下,在武汉大学出版社的大力支持下,我们组织中南地区的华中科技大学、武汉大学、华中师范大学、武汉理工大学、武汉科技学院、湖北经济学院、武汉生物工程学院、信阳师范学院、咸宁职业技术学院、江门职业技术学院、广东警官干部学院、深圳技师学院等院校长期工作在教学和科研第一线的骨干教师,按照 21 世纪大学本科计算机科学与技术课程体系要求,反复研究写作大纲,广泛猎取相关资料,精心设计教材内容,认真勘正知识谬误。经过大家努力的工作,辛勤的劳动,这套高等院校计算机技术系列教材终于与读者见面了。我相信通过这套教材的编写和出版,能够为我国计算机科学与技术教材的建设有所贡献,能够为我国高等院校计算机专业本科教学质量的提高有所帮助,能够为更多具有高素质的、创新型的计算机专业人才的培养有所作为。

魏长华

2007 年 7 月于武昌



前 言

随着网络技术的发展,网络系统规模逐渐增大,复杂性不断增加,异构性也越来越强。同时,网络资源、网络服务的日益丰富以及网络安全矛盾的日益突出,网络管理的问题显得越来越重要。当前,如何对日益庞大、复杂的计算机网络实施有效管理已成为国际上网络领域中的一项重要研究课题。

网络管理集通信技术、网络技术和信息技术于一体,通过调度和协调资源,最大程度地增加网络的可用时间,提高网络设备的可靠性、利用率、性能、服务质量和安全性等;管理和控制多厂商混合网络环境下的网络资源和控制网络运营成本,为网络长期发展规划提供必要的依据。为了能使网络更加稳定、可靠、安全地运行,必须改变原来的重视网络基础建设,忽视网络管理的现象。在实际网络运行管理中,培养和提高网络管理与安全人员的素质是一项很迫切的任务,高素质的管理员可以采取更加合理的安全措施和技术来提高网络管理效率。因此,普及网络管理知识,提升网络管理水平,不仅是网络发展的需要,也是社会发展的需要。

本书立足于培养高素质计算机网络管理人才的目标,从实际应用角度出发,精选教学内容,全面系统地介绍了计算机网络管理、网络安全及网络故障的分析与排除等方面的技术与方法。同时,本书在编写时注重网络管理与安全技术的实用性、全面性和先进性,以提高学生所学知识的可用性。

全书共分9章:

第1章介绍了计算机网络的基础知识,包括网络的概念、功能、分类、硬件和软件、协议与体系结构等。

第2章介绍了网络管理的基本概念、重要性、主要功能、网络管理的标准以及网络管理的对象。

第3章介绍了网络管理的体系结构,包括网络管理的基本模型、网络管理的模式、网络管理软件结构以及网络管理的组织模型。

第4章介绍了OSI管理信息库的主要内容,主要包括OSI管理框架、管理对象的层次结构、管理操作、管理对象的状态、抽象语法标记ASN.1的表示方式和MIB-II的主要功能组。

第5章介绍了简单网络管理协议和远程网络监视(RMON),主要包括SNMP v1的基本操作、工作机制、SNMP MIB、SNMP v2协议和操作、SNMP v3的功能和体系结构以及远程网络监视(RMON)的管理信息库和应用。

第6章介绍了网络管理系统的结构、典型的网络管理系统(HP OpenView、IBM Tivoli NetView、Ciscoworks2000、Sun NetManager)以及HP OpenView NNM的应用。

第7章介绍了网络安全方面的基础内容,包括网络安全的概念、网络安全要素、网络





安全面临着的主要威胁、网络安全信息系统和无线网络的安全。

第8章介绍了网络安全的常用技术,包括系统入侵及检测技术、防火墙技术、VPN技术、网络病毒与防范、数据加密技术、认证技术和信息隐藏技术等。

第9章介绍了网络故障诊断与排除技术,包括常见的网络故障诊断技术、网络故障维护工具及测试命令、网络故障分析与检测方法、局域网常见的故障分析与排除等。

本书在内容的组织安排上尽量做到结构合理、内容翔实、通俗易懂、脉络清晰,各知识点之间有着严谨的连贯性。在本书的编写过程中,作者收集整理、引用了大量国内外相关资料,在此对原作者表示歉意,同时也对原作者表示感谢!

本书的第一章、第二章和第三章由邹先霞编写,第四章、第五章和第六章由杜威编写,第七章、第八章和第九章由毛莉编写,全书由杜威修改定稿。本书在编写过程中得到了武汉大学出版社的大力支持,书中内容的规划与确定得到了武汉生物工程学院信息管理学院魏长华教授的指导,在此谨向他们表示衷心感谢。

本书可作为普通本科院校、普通高等专科学校的计算机网络管理教学方面的教材,也可作为广大初级网络管理员和初级网络管理工程技术人员学习网络管理与安全技术的参考书。

由于计算机网络和安全技术是一个飞速发展变化的领域,作者掌握的信息不过是沧海一粟。限于时间和水平的不足,书中难免有不当之处,恳请读者和有关专家批评指正!

愿本书的出版能为进一步普及计算机网络管理与安全技术,提高网络管理水平尽一份力量。

作者

2008年5月



目 录

第 1 章 计算机网络基础	1
1.1 计算机网络简介	1
1.1.1 网络的基本概念	1
1.1.2 网络的组成	1
1.1.3 网络的分类	3
1.1.4 网络的主要功能	5
1.1.5 网络的拓扑结构	6
1.2 计算机网络的硬件与软件	9
1.2.1 网络硬件	9
1.2.2 网络软件	16
1.3 计算机网络的协议与体系结构	18
1.3.1 网络通信协议	18
1.3.2 网络体系结构	19
1.3.3 ISO/OSI 体系结构和 TCP/IP 体系结构	20
1.3.4 IEEE802 系统标准协议	23
本章小结	24
习题 1	25
第 2 章 网络管理基础	28
2.1 网络管理概述	28
2.1.1 网络管理的概念	28
2.1.2 网络管理的基本内容	29
2.1.3 网络管理的目标	31
2.1.4 网络管理的基本功能	32
2.1.5 网络管理的发展	32
2.2 网络管理的基本功能	33
2.2.1 故障管理	33
2.2.2 配置管理	34
2.2.3 性能管理	36
2.2.4 安全管理	37
2.2.5 计费管理	38
2.3 网络管理的标准	39





2.3.1	ISO 标准	39
2.3.2	ITU-T 标准	40
2.3.3	IETF 标准	40
2.3.4	其他标准	41
2.4	网络管理的对象	42
	本章小结	42
	习题 2	43
第 3 章	网络管理体系结构	46
3.1	网络管理的基本模型	46
3.1.1	网络管理模型	46
3.1.2	网络管理站与网管代理	47
3.1.3	网络管理协议 NMP	48
3.1.4	管理信息库 MIB	50
3.2	网络管理模式	51
3.2.1	集中式网络管理模式	51
3.2.2	分层式网络管理模式	52
3.2.3	分布式网络管理模式	53
3.2.4	混合管理模式	55
3.3	网络管理软件结构	56
3.3.1	用户接口软件	56
3.3.2	管理专用软件	57
3.3.3	管理支持软件	57
3.4	网络管理的组织模型	57
	本章小结	58
	习题 3	59
第 4 章	管理信息库	63
4.1	概述	63
4.1.1	OSI 系统管理框架	63
4.1.2	管理对象的层次结构	65
4.1.3	管理操作	67
4.1.4	管理对象的状态	68
4.2	管理信息结构	70
4.2.1	MIB 结构	70
4.2.2	ASN.1 的数据类型	71
4.2.3	管理信息结构定义	75
4.2.4	标量对象和表对象	77
4.3	MIB-II 功能组及对象	82





4.3.1	MIB-II 概述	82
4.3.2	MIB-II 的功能组及对象	82
本章小结		99
习题 4		99
第 5 章	简单网络管理协议与远程网络监视	103
5.1	SNMP 概述	103
5.1.1	SNMP 的基本概念	103
5.1.2	SNMP v1 基本操作	106
5.1.3	SNMP 工作机制	108
5.1.4	SNMP v1 管理信息结构	109
5.1.5	SNMP 管理信息库	111
5.2	SNMP v2	113
5.2.1	SNMP v2 的功能	114
5.2.2	SNMP v2 协议和操作	115
5.2.3	SNMP v2 的实现	116
5.3	SNMP v3	117
5.3.1	SNMP v3 的功能	118
5.3.2	SNMP v3 的特点	118
5.3.3	SNMP v3 体系结构	118
5.4	远程网络监视 RMON	121
5.4.1	RMON 的基本概念	122
5.4.2	RMON1 的管理信息库	123
5.4.3	RMON2 的管理信息库	126
5.4.4	RMON 在网络管理中的应用	128
本章小结		130
习题 5		131
第 6 章	网络管理系统	134
6.1	网络管理系统概述	134
6.1.1	网络管理系统的结构	134
6.1.2	网络管理系统的特点	136
6.1.3	网络管理系统的发展趋势	137
6.2	典型的网络管理系统	139
6.2.1	HP OpenView	139
6.2.2	IBM Tivoli NetView	140
6.2.3	Ciscoworks	141
6.2.4	Sun NetManager	142
6.3	网络管理系统软件应用实例	143





6.3.1	Windows 2000 环境下 NNM 安装前的配置	143
6.3.2	Windows 2000 环境下 NNM 的安装与运行	145
6.3.3	HP OpenView NNM 的使用	147
本章小结		149
习题 6		150
第 7 章	网络安全基础	152
7.1	网络安全概述	152
7.1.1	网络安全的定义	152
7.1.2	网络安全要素	153
7.1.3	网络安全面临的主要威胁	154
7.1.4	黑客攻击网络的常见手段	155
7.1.5	我国网络安全的主要问题	157
7.2	网络信息安全系统	159
7.2.1	网络信息安全系统的模型	159
7.2.2	ISO 的网络安全体系结构及各层的安全性	161
7.2.3	计算机系统安全等级评价标准	164
7.2.4	制定网络安全策略的原则	166
7.3	无线网络的安全性	167
7.3.1	无线网络概述	167
7.3.2	无线网络结构与技术实现	168
7.3.3	无线网络的安全性问题	169
7.3.4	对无线网络的入侵与防范	171
本章小结		172
习题 7		173
第 8 章	网络安全的常用技术	175
8.1	系统攻击及入侵检测技术	175
8.1.1	系统攻击概述	175
8.1.2	常见的系统攻击方法	176
8.1.3	入侵检测系统概述	178
8.1.4	入侵检测系统技术及结构	179
8.1.5	入侵检测产品简介	181
8.2	防火墙技术	183
8.2.1	防火墙的概念	183
8.2.2	防火墙的主要功能	184
8.2.3	防火墙的关键技术	185
8.2.4	防火墙的基本结构	186
8.2.5	防火墙产品的选购与安装	187





8.3 虚拟专用网(VPN)技术	189
8.3.1 VPN 概述	189
8.3.2 VPN 的关键技术	190
8.3.3 VPN 的实现方法	192
8.3.4 VPN 技术的应用	193
8.4 网络病毒与防范	195
8.4.1 病毒概述	195
8.4.2 网络病毒的传播途径与防范措施	195
8.4.3 防毒策略及常用杀毒软件	197
8.4.4 常见病毒及清除方法	199
8.5 数据加密技术	201
8.5.1 加密技术概述	201
8.5.2 数据加密的基本原理	203
8.5.3 对称密钥加密技术	205
8.5.4 非对称密钥加密技术	207
8.5.5 网络加密技术	208
8.6 认证技术	210
8.6.1 认证技术概述	210
8.6.2 消息认证	210
8.6.3 身份认证	211
8.6.4 数字签名	212
8.7 信息隐藏技术	213
8.7.1 信息隐藏技术原理	213
8.7.2 数据隐写技术	215
8.7.3 数字水印	215
本章小结	217
习题 8	218
第 9 章 网络故障诊断与排除技术	221
9.1 网络故障概述	221
9.2 网络故障诊断技术	222
9.2.1 网络层次诊断技术	222
9.2.2 常用诊断技术	224
9.3 网络故障维护的常用工具及测试命令	226
9.3.1 常用的网络测试工具	226
9.3.2 基本网络测试命令及应用	228
9.4 网络故障分析与检测方法	231
9.5 局域网中常见的故障分析与排除	232
9.5.1 配置性故障分析与排除	232





9.5.2 连通性故障分析与排除.....	232
9.5.3 协议性故障分析与排除.....	234
9.5.4 其他常见性故障分析与排除.....	235
本章小结.....	236
习题 9	237
附录 A 与网络管理有关的 ISO 标准索引	239
附录 B 计算机安全保护等级	242
附录 C 安全站点	243
参考文献.....	245



第1章 计算机网络基础

【学习目的与要求】 本章主要介绍计算机网络的基础概念、计算机网络的硬件与软件以及计算机网络的协议与体系结构。通过本章的学习，应注意掌握以下内容：

- 了解计算机网络的基本概念、组成、分类及网络的主要功能；
- 了解计算机网络的拓扑结构概念，掌握不同拓扑结构类型网络的特点；
- 掌握计算机网络硬件、软件的特点及分类；
- 掌握计算机网络的协议与体系结构。

1.1 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。

1.1.1 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，以发挥分散的、各不相连的计算机之间的协同工作功能。因此，对计算机网络可做如下定义：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连成一个整体。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方面的领域，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。

1.1.2 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



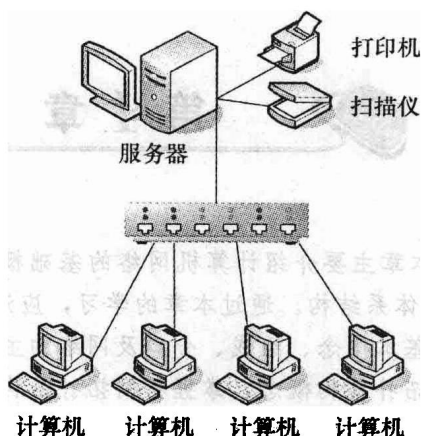


图 1-1 计算机网络系统示意图

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。

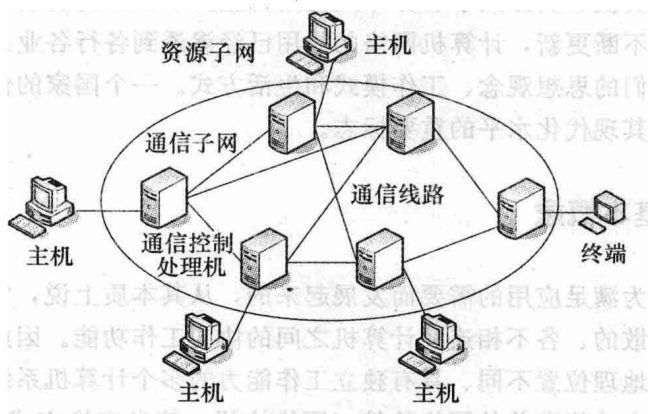


图 1-2 通信子网和资源子网

1. 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。

2. 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。

1.1.3 网络的分类

计算机网络系统是非常复杂的系统,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。

1. 按网络的覆盖范围进行分类

按覆盖范围对网络进行划分,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 $10^{-7} \sim 10^{-12}$ 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) 将不同的局域网连接起来, 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。

2. 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

