THE NETWORK TROUBLESHOOTING LIBRARY

TCP/IP

故障检测与维护

Mark A. Miller, P.E.

M&T BOOKS

科学出版社

龍門書局

TCP/IP 故障检测与维护

〔美〕 Mark A. Miller 著

夏春和 张 辉
郭 亮 李 莉 译

闻丹岩 校

科学出版社
龍門書局

1996

(京)新登字 092 号

内 容 简 介

本书介绍了目前在全世界广为流行的互连网络体系结构——TCP/IP和 Internet 协议，内容包括：不同的 LAN，WAN 和 MAN 的体系结构，不同层间的互连网编址；对 DARPA 体系结构模式各层的研究，及互连网络的管理等。

本书可作为网络管理员的技术参考手册，对从事网络技术工作的工程技术人员、大学计算机专业高年级学生及研究生也有较高参考价值。

需要本书的读者，请直接与北京海淀 8721 信箱书刊部联系，邮码：100080，电话：62562329。

Mark A. Miller
TROUBLESHOOTING TCP/IP
M&T Books Publishing，1993

版 权 声 明

本书英文版名为 Troubleshooting TCP/IP，由美国 M&T Books 出版公司出版，版权归 M&T Books 出版公司所有。本书中文版由美国 M&T Books 出版公司授权出版。未经出版者书面许可，本书的任何部分都不得以任何形式或手段复制或传播。

TCP/IP 故障检测与维护

〔美〕 Mark A. Miller 著
夏春和 张 辉
郭 亮 李 莉 译
闻丹岩 校
责任编辑 汪亚文
双青印刷厂印刷
北京东黄城根北街 16 号
邮政编码：100717
科学出版社
龙门书局 出版
新华书店北京发行所发行 各地新华书店经销
*
1996 年 4 月第一版 开本：787×1092 毫米 1/16
1996 年 4 月第一次印刷 印张：25¼
印数：1-5000 字数：582 426
ISBN 7-03-005027-4/TP・516
定价：39.00 元

前　言

写前言是我一直所盼望的。因为，首先它标志着写稿和订稿所花费的大量时间以及无数个电话的结束。其次，它为我提供了一个向读者绘制一张路线图的机会，从而使得读者能更快地完成旅程。最后，它提供了一个用带有感情化色彩的语言来描绘一些非感情化题目的机会。

绘制路线图

本书主要讲述 TCP/IP 及相关协议。在编写《互连网络故障检测》(Troubleshoting Internetworks, M&T Books, 1991)时所作的一些调查激起了我写这本书的愿望。在为写这本书而进行调查时，我向网络通用公司(Network General Corp.)的"Sniffer"分析仪(AnalyZer)的几个用户写信询问他们能否寄来一些保留下来的有价值的跟踪文件。这些资料在本书中将作为实例来研究。在我审查所收到的这一大堆磁盘时发现了这样一个趋势：与 TCP/IP 相关协议的邮件占的比例比其他任何协议族都多，甚至多于 DECnet, SNA 或 NetWare。突发灵感，产生了写一部整卷介绍 TCP/IP 协议的书的想法。

本书的结构组织是采用按协议的体系结构从底向上深入的。不过本书所采用的体系结构是国防部高级研究计划局(Defense Advanced Research Projects Agency DARPA)体系——即这些开发过的协议之外的体系结构。在第一章里我们将要看看这些协议在互连网的世界中所占的地位。在第二章，我们将考察一下大型机、小型机、局域网和分析仪的制造商们所提供的对这些协议的支持。第三章至第六章将分别介绍网络接口层(Network Interface)，互连网子层(Internet)，主机到主机层(Host-to-Host)和应用/处理层(Application/Process Layer)等各层的情况。每一章将先总体地介绍各层中的协议，然后通过研究一些实例来显示一下协议是如何工作的(以及工作失败的原因)。第七章介绍互连网的管理专题。第八章则大概地推导出从 TCP/IP 互连网过渡到 OSI 协议所采取的策略。附录是"参考信息"——协议的参数及需要查阅的文档，使您能够顺手查到。

鸣　谢

像往常一样，先介绍一下为本书的出版作出贡献的幕后工作者。在 M&T Books 工作的 Brenda McLanghlin, Sarah Wadsworth, Tom Woolf 和 Cheryl Goldberg 等编辑，为保证本书的按期完成花费了大量的心血和精力。

Nancy Wright 和 Krystal Valbez 对原稿进行了文字加工。集成计算机图形(Integrated Computer Graphics)公司的 David Herzke 为文字稿加上了插图，对以上三位的辛勤劳动表示感谢。

在个别情况下需要作一些特殊的测试了解协议(运行在工作状态网络下)在"如果是这

样”的条件下的完成情况。Eural Authement，Chris Dutchyn，Ross Dunthorne 和 Paul Franchois 等工作人员不辞辛劳地完成了这些测试。

我还要感谢几位在个别章节中参与了工作的朋友：Jay Allard，John Case，Dan Callahan，Bill Cohn，Michael Howard，Brian Meek，Larry Thomas，Ursula Sinlcewicz，另外还有来自 Banyan System 公司的 Eural Authement，Paul Franchois 和 Carl Shinn 阅读了全部手稿，并提出了大量的改进建议。Colorado SuperNet 公司的 David Mengers 提供了与 Internet 相关的问题并支持出版。

真正的主角是那些遍布世界的网络管理员，他们通过网络通用（Network General）Sniffer 跟踪文件交流他们的经验，这些文件是读者在后文要接触到的 29 个实例的来源。从学术的观点来讨论一种协议与接触实际来研究这些协议的感受是相当不同的。按字母表顺序排列，这些 管理员有：Rohit Aggrawal，Gelald Aster，Eural Authement，Joe Bardwell，Ross Dunthorne，chris Dunchyn，Tony Farrow，Paul Franchois，Dave Hoke，Dell Holmes，James Knights，Iwan Lie，Jeff Logullo，Dan Milligan，Tom Morocz，Mark Ryding，Bob Sherman，Mendy Valinsky 和 Wayne Veilleux。

网络通用公司（Network General Corp.）的 Ed Lucente 和 Bob Bessin 向我提供了一台 Sniffer 分析仪来研究所提出的各种各样的问题供原因分析用。Juancho Forlanda 则在我的正规来源得不到时，帮我找到一些不常见的跟踪文件。对他们的慷慨表示不胜感激。

向以下三位朋友致敬：Lloyd Boggs，Gordon England 和 MarshRiggs，他们在我写这部书时，给予了不少鼓励和帮助。

最重要的是，Holly，Nicholas 和 Nathan 为我提供了能承受如此繁重任务的一个支持环境。Boomer 早上叫醒我进行工作，而我们开始工作时，Brutus（狗名）又尽量地不叫出声来，Buster 则是我忠实的卫兵。对于以上提及的所有朋友和宠物所给予我的爱表示深切谢意。

Mark A. Miller

此为试读，需要完整PDF请访问：www.ertongbook.com

本书简介

本书介绍了一种最流行的互连网络体系结构：TCP/IP 和互连网(Internet)协议。这些协议是在 70 年代中期应美国政府的要求而制定的。这些协议的严谨性伴随着它们在不同的大学和国防部门所应用的广泛性使得它们在 80 年代进入了商业的前沿阵地。TCP/IP 在网络互联的解决方案中的主导地位一直延续到今天。

随着 TCP/IP 的普及，互连网管理员面临的一个关键问题是：假如 TCP/IP 已经被安装上了并且已经运行了一段时间，那么怎样对这些协议进行分析呢？本书的目标就是回答这个问题。讨论的专题包括：

- 不同的 LAN，WAN 和 MAN 体系结构，包括令牌环，FDDI，X.25 和 SMDS 等是如何支持 TCP/IP 的；
- 不同层的互连网编址，包括硬件地址、互连网地址和端口地址，以及它们如何协同工作来传递终端用户的应用数据的；
- 对 DARPA 体系结构模式的一层接一层的研究，演示 TCP/IP 以及相关的协议，比如 ARP，RARP，ICMP，RIP，OSPF，UDP，TELNET，FTP，TFTP，BOOTP，SMTP，SNMP 和 CMOT 是如何与体系结构相对应的；
- 从工作状态下的互连网络中所提取的超过 25 个实例进行研究，展示 TCP/IP 和使用中的相关协议、可能出现的典型问题及解决办法；
- 便捷的附录，提供了协议的参数和有助于进行故障检测的参考文献。

如果 TCP/IP 是你所使用的互连网的一部分，则本书应该成为你的参考书中的一本。

目　录

第一章　TCP/IP 以及互连网协议的使用

从表面上看，传输控制协议（Transmission Control Protocol）/网际协议（Internet Protocol）（TCP/IP）仅仅是网络上常提及的名词，但从深度看，却为实现网络互连及互操作性提供了很通用的解决方法。TCP/IP 不单是两个简单的协议，它是实现异种机（像 Digital Equipment 公司（Maynard，MA）的小型机，Sun 微系统公司（Sun Microsystem Inc.）（Mountain View，CA）的工作站）互相通讯的体系结构。这种通讯可以通过局域网（Local Area Network，LAN），城域网（Metropolitan Area Network，MAN），广域网（Wide Area Netsork，WAN）或其它异构网技术来实现，TCP/IP 支持所有类型的网络。TCP/IP 真可称为“伟大的通讯员”或“实现互操作性的途径”。

为满足互连网（Internet）的需要，TCP/IP 不断得到了发展、充实和提高。Internet 可以跨越公司甚至国界为用户对用户或主机对主机间的通讯提供全球性的服务。同样的 TCP/IP 协议能够满足 LAN 或 WAN 互连的各种要求。这只是开端。我们先回顾 TCP/IP 协议，从 Internet 着手介绍。

1.1　Internet 的挑战

不同的人对 Internet 有不同的理解，有些人把它当作动词，意为“IBM SNA 环境到 DEC DECnet 环境的网络互连”。另一些人把它当作名词，意为“由两种或多种不同网络构成的网络”，如两个分组交换公共数据网（Packet Switched Public Pata Networks，PSPDNs）之间的互连网（Internet）。Internet 还可作为专用名词，如 the Internet，意思就是全球性的用于用户和计算机通讯而互联的网络集合。

除了对 Internet 有不同的理解外，Internet 还面临着多种挑战。假设用户已经连上了 Internet，用户会像依赖公共电话网一样，依赖 Internet 跟朋友或组织进行交流通讯。当系统出故障时怎么办呢？如果是电话网出问题，用户可以跟本地交换局（Local Excharge Carrier，LEC）或市交换局（Inter Exchange Carrier，IEC）联系，它们负责提供服务。但 Internet 出现问题时，系统服务的恢复由于以下几方面的原因不那么简单。首先，Internet 协议远比用户在家或有事打电话的服务要复杂得多；其次，用户打交道的是计算机间的通讯，远比声音抽象而难以诊断故障；最后，因为 Internet 是多种计算机网络的互连，要确定故障是一个很大的挑战。除此之外，不像电话拔“0”可以跟接线员联系修复电话，Internet 没有一个组织或方法可以用来提出问题（如经允许，终端用户可以把问题提交给本地管理员处理，但往往把管理员给难住了）。碰到 Internet 的问题，只好自己去测试和诊断。

这些都是编写这本书的理由。自从 70 年代中期以来，TCP/IP 协议把 Internet 紧紧组合在一起。一些附属的协议，如地址转换协议（Address Resolution Protocol，ARP），网际控制报文协议（Internet Control Message Protocol，ICMP），用户数据报协议（User Datagram Protocol，UDP），路由信息协议（Routing Information Protocol，RIP），还有另外一些协议都通

此为试读，需要完整PDF请访问：www.ertongbook.com

过此法得到了发展。对所得到的混合体进行故障查找也是一项挑战；在许多情况下需要协议分析仪的帮助。搞清对基于 TCP/IP 互连网络的故障查找过程是出版本书的目的。为了做好故障查找工作，还应该学习 Internet 的拓扑结构，了解在 Internet 中使用的协议，检查实际 Internet 问题的各种情况。在学习原理之前，先了解 Internet 的历史。

1.2 Internet 历史简介

Internet 是世界上计算机科学与网络技术最有意义的成就之一。Internet 可以跨越公司和国界为用户对用户以及主机对主机的通讯提供全球性的服务。Internet 是自发组织的，这一点更让人惊讶。它的运行机构主要由志愿者组成。美国国防部(U. S. Department of Defense)和一些州政府机构只资助基本的开销。Internet 协议的大部分研究工作放在美国的主要大学 ，如 California 大学，Colorado 大学，Illinois 大学和 Texas 大学。这种独一无二的系统是如何形成发展的呢？

今天的 Internet 是在 1969 年作为高级研究计划局的网络(ARPANET)而诞生的，这是由美国国防部高级研究计划局(DARPA)发起研究的。ARPANET 的目的在于测试和验证像分组交换这样的通讯技术的能力[1-1]。Bolt，Baranek 和 Newman 公司(即现在的 BBN 通讯公司，剑桥，MA)得到了建立原始 ARPANET 的合同，1969 年 9 月 ARPANET 开通时只有 4 个点：斯坦福研究所(SRI)，在 Santa Barbara 的加利福尼亚大学(UCSB)，在洛杉矶的加利福尼亚大学(UCLA)和犹他大学。最初的主机为 Honeywell 316 小型机也即接口信息处理机(IMP)。

初次的试验非常成功，从此 ARPANET 发展非常迅速。同时，由于非军事研究人员也能从利用这种类型的网络而得到好处，因此一些大学和工业研究团体的领导向国家科学基金会(National Science Foundation，NSF)提出建立计算机科学研究人员的合作网络的建议[1-2]。NSF 在 1981 年为计算机科学网络(Computer Science Network，CSNET)的建立提供资金。

到 1984 年，ARPANET 分成了两个不同的网络：MILNET(为军事通讯服务)和 ARPANET(为非军事性的通讯及科研服务)。在 1984 年，NSF 为进一步发展超级计算机，并使它们得到广泛地使用建立了高级科学计算办公室(OASC)。OASC 使 NSFNET 得到了发展，它用 T-1 的线路(速率为 1.544Mbps)把美国的 6 个超级计算中心连结起来。由于这些先进技术的发展，美国国防部宣布 ARPANET 已经过时，并在 1990 年 6 月把它拆除了。

从 ARPANET 中学到的知识对一些像 LAN 和分组交换这样的数据通讯技术有深刻的影响。最近，NSFNET 主干网已改在 T-3 的线路上传输(速率为 44.736Mbps)。见参考文献[1-3]至[1-5]。在 1.4 节还将进一步讨论此项研究工作产生的系列网络。参考文献[1-6]和[1-7]为这些早期的网络提供了一些很有意思的历史信息。现在，让我们打开一本不同的历史学习互连网络通讯中用到的各种协议的发展。

1.3 Internet 的协议

在第一个 10 年，ARPANET 发展极快，几乎是平均每 20 天增加一台新计算机[1-8]。起

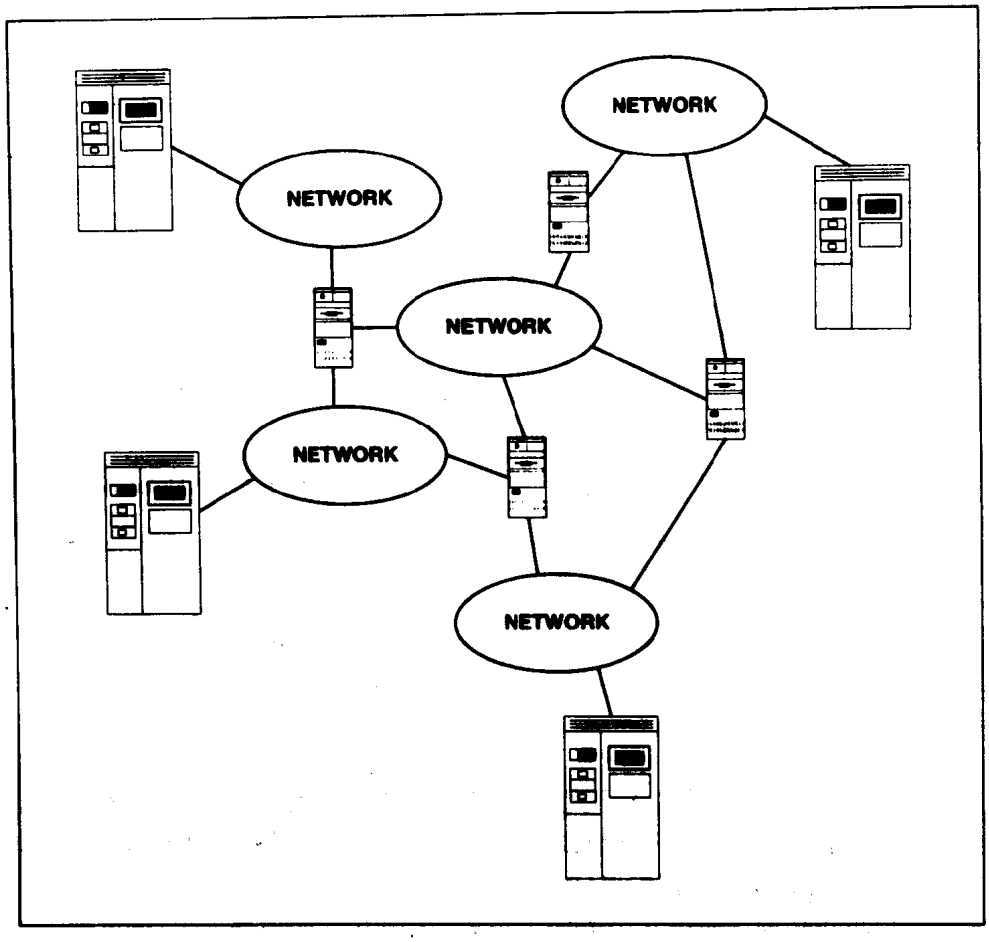

图 1-1　几个网络通过网关(路由器)的连接构成一个互连网络

始的互连网络通讯协议是网络控制程序(Network Control Program,NCP),NCP 提供了开放系统互连(OSI)参考模型的网络层和传送层的功能,在主机和网际交换机之间处理信息。NCP 是在假定基础通讯子网(即 OSI 的物理层,数据链路层、网络层)提供良好通讯通道的前提下设计的。所给予的务支持政府或军事网络的 ARPANET 的任务包括战场情况下的无线通讯,这样对通讯通道的可靠性需要重新考虑。1973 年 1 月,DARPA 使传输控制协议(TCP)成为 Internet 的一个标准就在于它的优良性能。DARPA 互连网络体系结构(图 1-1)包括由网关连接的中通过网关连接了许多网络(注意,按 OSI 的说法,这些设备实际上是运行在 OSI 网络层的路由器,按当前的定义,网关应该在 OSI 参考模型的 7 层协议上运行。这一章暂且把这些连接设备说成网关,在学习第二章时再把它叫作更为合适的术语——路由器。)在 DARPA 模型中假定每个网络都使用分组交换技术并且能跟不同的传输介质(如 LAN,WAN,无线电等等)相连。

DARPA Internet 体系结构包括四层见(1-2)。最低层叫作网络接口层(Network Interface Layer),它也指本地网络或网络存取层,是由各设备之间的物理链接(即 LAN)构成。网络接口层包括主机和网关的在所有的设备中都存在。

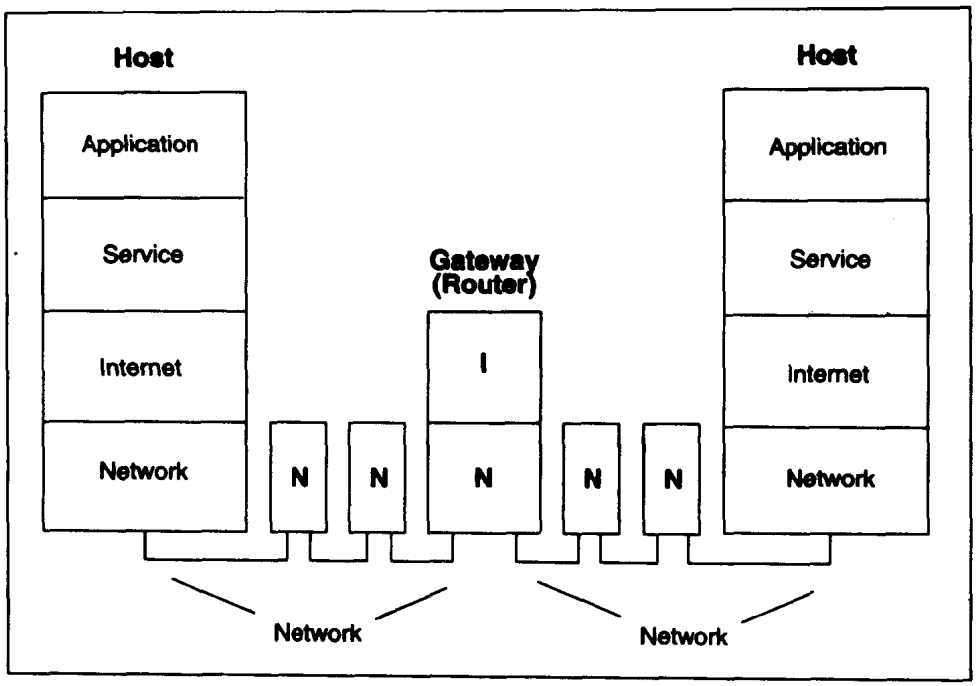

图 1-2 DARPA 分层体系结构

网际层(Internet Layer)把主机从特定的网络细节中分离出来,如寻址。在这一层上为提供端到端的数据服务而发展了网际协议(IP)(数据报类似于电报,它是按包文方式来传递信息的)。只有主机和网关才有网际层(即 IP)。

当网际层提供端到端的报文传送时并不保证这种传送的正确无误,所以在主机之间提供了第三层即服务层(现在叫主机到主机层,Host-to-Host Layer)。按字面意思理解,服务层定义了主机应用程序所需要的服务等级。服务层有两个协议:传输控制协议(TCP),为端到端的通讯提供可靠保证;另一个为用户数据报协议(UDP),为不需太高可靠性的应用提供服务。第三个协议为网际控制报文协议(ICMP),为主机和网关之间交换控制和监视信息提供服务。

DARPA 的最高层为处理/应用层,只驻留在主机中,为用户到主机或主机到主机的处理和应用提供服务。这一层开发了以下几个标准应用程序:作为远程终端访问的无线电通讯网络(TELNET);作为文件传送的文件传送协议(FTP);作为电子邮件的简单邮件传输协议(SMTP)。

图 1-3 把 OSI 与 DARPA 两者的体系结构作了比较,从中可知 OSI 的物理层和数据链路层代表了 DARPA 的网络接口(或本地网络)层;OSI 的网络层对应于网际层(Internet Layer);OSI 的传送层在功能上等同于主机到主机层(Host-to-Host Layer)也叫服务层;OSI 的会话层、表示层和应用层与 DARPA 的处理/应用层对应。参考文献[1-10]到[1-13]描述了 ARPANET 参考模型和协议的发展。参考文献[1-14]至[1-17]为描写 TCP/IP 协议历史与应用的最近期论文的一些。参考文献[1-18]对于那些想深入了解这些协议背景的读者是很好的自学指南。

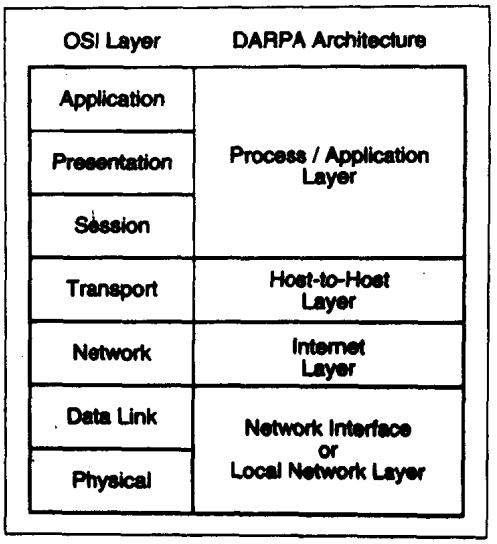

图 1-3 OSI 与 DARPA 模型的比较

对 IP 和 TCP 协议的发展背景有所了解后，就可以学习使用这些协议的各种网络的历史。

1.4 Internet 族

世界上一些网络由 ARPANET 研究产生了以满足非军事的需求。集合在一起，它们便成了人们熟知的互连网(Internet)，使用 TCP/IP 和相关的协议建立底层的通讯设施是这些网络的共同特点。目前大约有 727 000 台主机相连接[1-19]。John Quarterman 优秀的参考书 The Matrix[1-20]对这些全球性的网络作了详尽的描述。

Internet 在美国的部分(图 1-4)由连接到 NSFNET 主干网上的几个区域网和中间网络组成，里面包含有像西部网(WESTNET)这样的区域网，有像在 San Diego 的加利福尼亚大学的 San Diego 超级计算机中心(SDSCNET) 这样的许多超级计算机中心；有 NASA 使用的空间物理分析网络(SPAN)；有 NSF 提供资金的计算机科学网络(CSNET)；有全球性的“Because It's Time Network，BITNET”网络等等。

图 1-5 更为详细地显示了西部网(WESTNET)，它把 Idaho，Utah，Wyoming，Colorado，Arizona 和 New Mexico 6 个州都连接起来。西部网的里面有 Colorado 超级网和 CSN(见图 1-6)。CSN 连通了许多大学、公共图书馆、一些高技术公司(如 Cray 计算机公司，Hewlett-Packard 公司、McData 公司)和美国西部。

从总体上看，NSFNET 主干网(图 1-7)大约连接了 3000 个研究单位，拥有 500 000 个用户。随着流量的增加，包括主干网的传输线的传输速率最近已从 T-1(1.544Mbps)转换到用 T-3(44.736Mbps)。

为满足新一代计算机和新应用(如图象)[1-21]的出现，如何增加带宽的研究工作一直在不断进行。NSF 在当地交换局(LEC)，中间交换局(IXC)、计算机制造商、大学的研究单位

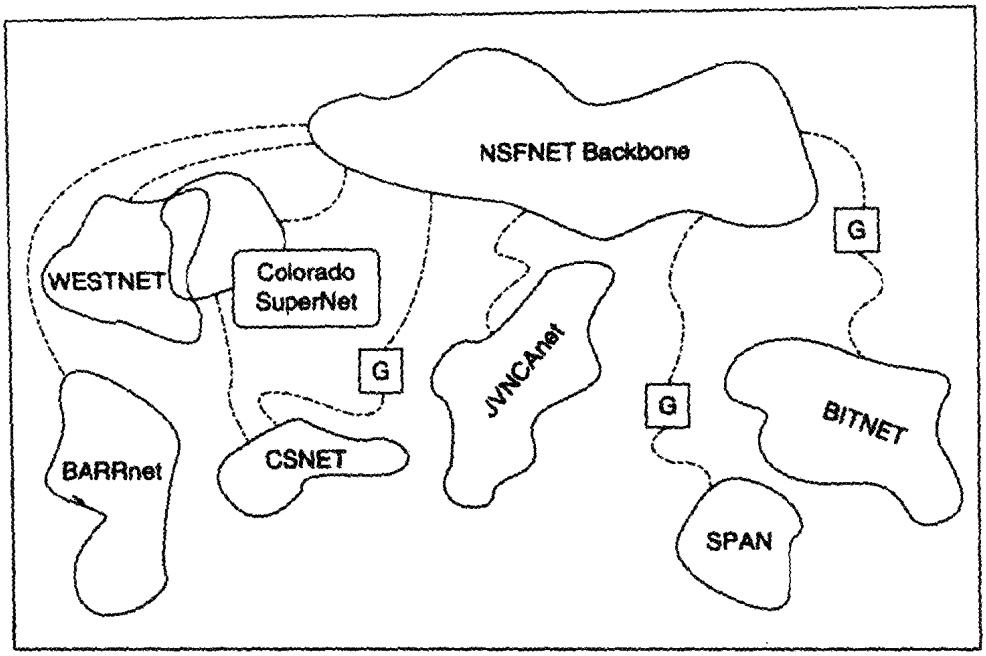

图 1-4　Internet 互连网

的帮助下发起组建了五个试验网络，这些试验网络得到了美国政府的资助[1-22]和[1-23]并为形成国家研究教育网(NREN)打下了基础，试验的技术包括以 622Mbps 传输的同步光网(SONET)数据链接、异步传输模式(ATM)的单元中继交换，连接主机的 ANSI 高性能并行接口(HPPI)。这五个试验网络分别为 Aurora(评估高速交换技术)、Blanca(测试 SONET 和 HPPI)、Casa(在广域网环境中测试高速应用情况)、Nectar(测试支持高速网络的操作系统)、Vistanet(研究流量模型及传输协议)。国家研究教育网(NREN)定于 1996 年开始运行。

Internet 历史的最后一部分内容是有关当今对商业化的争论。到现在为止，Internet 一直为政府通讯和研究服务，然而，Internet 本身及它使用的可靠的技术对商业界具有广泛的吸引力[1-24]。还有另外的服务，即为那些流量并不大的用户提供拨号服务，也正是连接 Internet 的好处。举几个这种服务的例子：加利福尼亚教育和研究联邦网络(CERFNE)，(619)534-5087；国际性能系统公司(Performance Systems International, Inc., PSINET)，(703)620-6651；UUNET 技术机构，(703)876-5050。参考文献[1-25]讨论了其中的一些用户应用内容。

1.5　Internet 文本

像 Internet 这样庞大的志愿组织，将协议和程序整理成文本是令人惊奇的事情，如何简便地获取这些文本也是很费事的。网际活动委员会(IAB)和网际注册处(Internet Registry, IR)统管着 Internet，先看看这两个组织。

网际活动委员会 IAB 负责 Internet 的设计及未来规划([1-26]。委员会确定 Internet 的

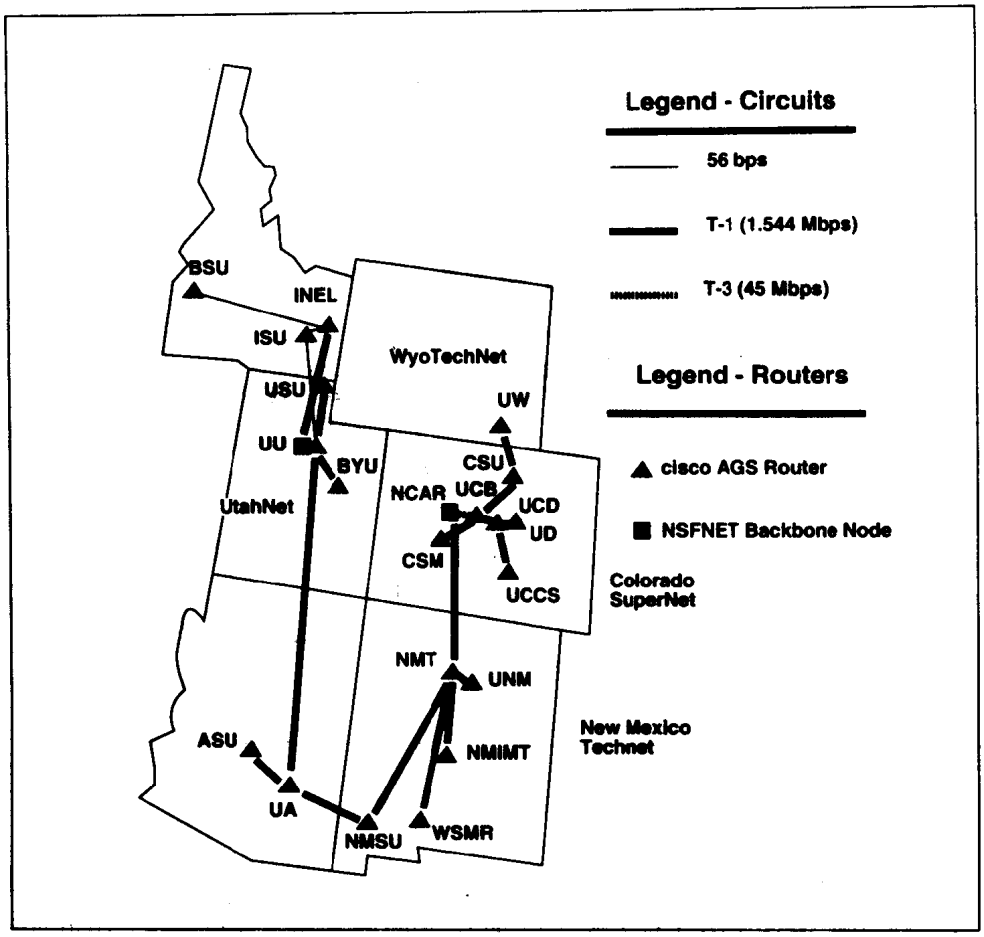

图 1-5　1992 年夏西部网络图(只标出起始节点)

标准;监督 Internet 工作成员;管理 Request for Comments(RFC)的出版;设计策略计划;在 Internet 团体中扮演国际代表的角色;解答技术问题。

IAB 有两个任务组,一个为网际工程任务组 (IETF),负责协调 Internet 的技术和协议的技术状况,并保证其功能富有成效[1-27]。另一个为网际研究任务组(IRTF),负责对新技术的研究。Internet Society 是对 Internet 的成功运行感兴趣的用户和制造商组织起来的非赢利组织,当前的计划要求 IAB 与 Internet Society 合并。

IAB 产生了许多要求散发或归档的协议标准和可操作的程序。像注释要求文本(RFCs)这样的大部分文本是众所周知的并要经过 IETF 和 IRTF 相应成员的检查。Internet 的大部分协议已成为美国军用标准并打上军用标准(MIL-STD)数字号码。例如,网际协议(IP)被写上 RFC791 和 MIL_STD_1777。用户可以从国防部 数据网(Defense Date Network)、网络信息中心(DDN NIC)或通过 Internet 的电子邮件上拷贝所需 RFC 文本。在 RFC1280"IAB 正式协议标准"中[1-29]对协议的标准化过程有详细的描述。

Internet 注册处(Internet Register,IR),就像一个中央票据交换所一样负责管理

此为试读,需要完整PDF请访问: www.ertongbook.com