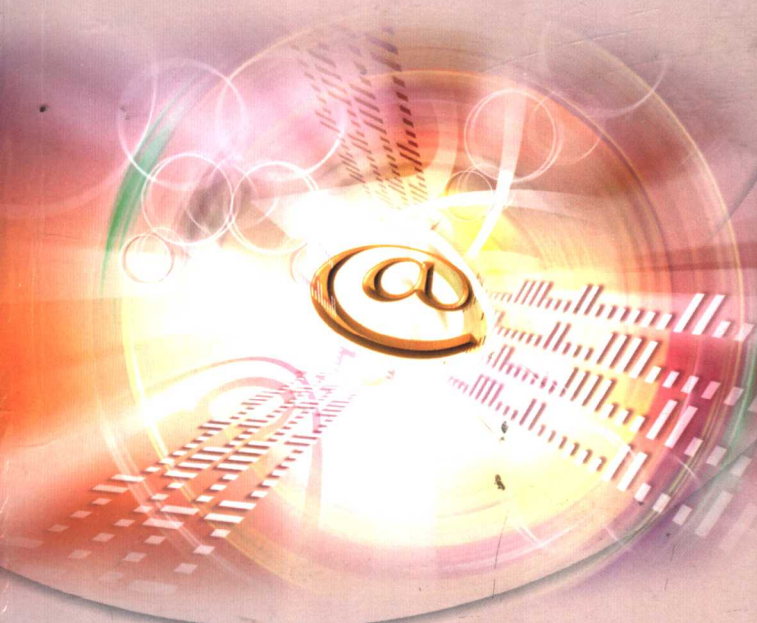


高等学校计算机科学与技术教材

网络设备安全与防火墙

杨富国 主 编
吕志军 蔡圣闻 编
郑 憬 丁 剑



清华大学出版社
<http://www.tup.tsinghua.edu.cn>
北京交通大学出版社
<http://press.bjtu.edu.cn>

高等学校计算机科学与技术教材

网络设备安全与防火墙

杨富国 主编
吕志军 蔡圣闻
郑 憬 丁 剑 编

清华大学出版社
北京交通大学出版社

· 北京 ·

内 容 简 介

本书从介绍因特网的安全问题入手,讨论了网络中各种设备的安全问题和黑客攻击方法,随后介绍了网络协议的安全性。针对政府和企业上网问题,详细讨论了对内部网络和外部网络进行安全控制的物理/逻辑隔离技术,并提供了多种解决方案。本书还对常用的网络设备及防火墙产品的安全特性进行了全面而系统的介绍。通过阅读本书,不仅可以深刻理解网络设备和防火墙的安全机制,还可以掌握对常用网络设备(例如 Cisco 路由器、交换机)的安全配置方法,并了解当前流行的防火墙系统的安全特性和功能。这是一本理想的进行网络设备安全配置和防火墙安全管理的实用参考书。

版权所有,翻印必究。

本书封面贴有清华大学出版社防伪标签,无标签者不得销售。

(本书防伪标签采用清华大学核研院专有核径迹膜防伪技术,用户可通过在图案表面涂抹清水,图案消失,水干后图案复现;或将表面膜揭下,放在白纸上用彩笔涂抹,图案在白纸上再现的方法识别真伪。)

图书在版编目(CIP)数据

网络设备安全与防火墙/杨富国主编;吕志军等编. —北京:清华大学出版社;北京交通大学出版社,2005.3

(高等学校计算机科学与技术教材)

ISBN 7-81082-356-6

I. 网… II. ① 杨… ② 吕… III. ① 计算机网络-安全技术-高等学校-教材 ② 计算机网络-防火墙-高等学校-教材 IV. TP393.08

中国版本图书馆 CIP 数据核字(2005)第 016937 号

责任编辑:孙秀翠 特邀编辑:刘 云

出版者:清华大学出版社 邮编:100084 电话:010-62776969

北京交通大学出版社 邮编:100044 电话:010-51686414

印刷者:北京鑫海金澳胶印有限公司

发行者:新华书店总店北京发行所

开 本:185×260 印张:22.25 字数:554 千字

版 次:2005 年 3 月第 1 版 2005 年 3 月第 1 次印刷

书 号:ISBN 7-81082-356-6/TP·182

印 数:1~4 000 册 定价:29.00 元

编委会成员名单

主 编：杨富国

副主编：吕志军 蔡圣闻

编 委：丁 剑 王 沂 王付海 叶传标 乔正洪
任吉治 陈兰生 严利珍 李 巍 李德水
宋 征 郑 憬 邹良群 周惠民 蒋 玲

前 言

最近几年，网络逐渐渗透到社会生活的方方面面。人们在网查询信息，企业在网发布信息，而政府则在网公开信息。这一切的一切，都预示着在不远的将来，网络的使用将同电话一样普遍。随着网络技术的发展，出现了越来越多的网络设备。与此同时，也出现了越来越多的网络安全问题。这些安全威胁极大地损害了人们对互联网的信心，从而影响了Internet更大作用的发挥。因为没有有效的安全保护，很多企事业单位放缓了将部分业务或服务转移到网上的步伐，极大地降低了工作效率。因此，如何能够为本组织的网络提供尽可能强大的安全防护就成为各企事业单位的关注焦点。

为了解决网络安全问题，需要使用一种被称为“防火墙”的安全设备。防火墙是指设置在不同网络（如可信任的企业内部网和不可信的公共网）或网络安全域之间的一系列部件的组合。它是不同网络或网络安全域之间信息的惟一出入口，能根据企业的安全策略控制（允许、拒绝、监测）出入网络的信息流，且本身具有较强的抗攻击能力。它是提供信息安全服务、实现网络和信息安全的基础设施。

除了防火墙之外，本书也对其他一些网络安全设备进行了介绍。因为最近几年是政府和企业上网的重要时期，内外网的安全管理是一个很重要的问题，所以网络的物理隔离技术也是本书的一个重点。当然，一些网络设备自身也设计了相应的安全模块。但无论从功能上还是从作用上，都不能和防火墙相比。

因此，本书从防火墙的基本概念、设计与实现、使用与维护等各方面对防火墙知识进行了详尽的阐述。最后，本书还对当前一些著名的防火墙产品做了具体的介绍。

本书的组织结构

本书在逻辑上分为两个部分，前半部分主要介绍网络设备的安全问题，而后一部分则主要介绍防火墙的相关知识。读者可以根据自己的需要，选择阅读相关的章节，如果对前面的内容很熟悉，可以跳过这些内容进行选择学习。

第1章主要概述了计算机网络的发展和安缺陷，同时还探讨了网络系统结构的复杂性，最后给出了对网络复杂性的控制办法。

第2章是对网络设备和系统的安全性分析。本章首先介绍了国际、国内的一些安全事件，然后具体描述了设备、系统漏洞及黑客的攻击方法，最后给出了网络设备的安全管理方法和策略。

第3章主要介绍了网络设备安全的物质基础，分别介绍了网络传输媒介、局域网物理设备和拓扑结构，以及广域网结构。

第4章主要讨论网络协议的安全性，分别介绍了网络基本协议、地址转换协议、路由协议、应用协议及它们的安全性。

第5章主要介绍了物理网络隔离技术及其设备。本章首先给出了物理隔离的定义和现实意义，接着分别讨论了几种物理隔离技术，然后探讨了物理隔离技术的解决方案，最后是对物理隔离技术的展望。

第6章是接入服务器的安全管理。本章给出了接入服务器的定义和作用,并结合具体的接入服务器产品进行详尽的介绍。

第7章主要介绍了交换机的安全管理。本章首先介绍了多层交换技术,然后探讨了VLAN及其安全性,最后具体说明了一些典型交换机的安全功能。

第8章介绍的是路由器。该章介绍了路由器的方方面面,从它的发展、原理、管理和安全,到路由器的具体配置(包括路由协议、服务质量、访问控制及VLAN的路由),都做了非常详尽的说明。

第9章主要介绍一些有关防火墙的背景知识、定义、职责和局限性,同时讨论了防火墙技术的演变过程和分类,最后给出了一些专用术语。

第10章主要介绍防火墙的设计和实现所涉及的相关知识。要设计和实现防火墙,首先需要了解关于防火墙等信息安全产品的国内外标准;其次需要清楚防火墙的安全需求和体系结构;最后才能在此基础上,应用相关的安全技术。在本章的最后,还介绍了特定防火墙的开发、测试和评估工作。

第11章主要介绍防火墙的使用和维护过程中所需要注意的一些问题。防火墙的使用首先要求根据组织的网络环境进行网络风险分析。在此基础上,才能选择合适的防火墙,并正确地部署到组织的网络上。最后,网络管理员要为防火墙设定正确的安全策略,并进行恰当的运行维护。只有这样,企业才能够以最小的代价得到最大的安全。本章最后还给出了一些应用案例。

第12章主要介绍了几款目前市场上常见的防火墙产品。这些产品都具有其独特的技术特点,因此能够在业界占有一席之地。本章对它们的安全功能和安全特性给出了非常全面而具体的说明。

本书的读者对象

本书适合以下读者对象:

- 涉及网络安全产品开发的计算机专业人员;
- 需要建立、实现和管理因特网和企业内部网的网络管理人员;
- 设计、开发网络相关产品的程序员、分析员和项目管理人员;
- 对因特网技术和网络设备感兴趣的技术人员;
- 关注网络安全的非专业人员。

编者
2005.3

目 录

第1章 概述	(1)
1.1 计算机网络的发展	(1)
1.1.1 资源共享	(1)
1.1.2 因特网的增长	(2)
1.1.3 基本概念解析	(2)
1.2 计算机网络的安全缺陷	(4)
1.2.1 主机安全	(4)
1.2.2 保护口令	(4)
1.2.3 加密	(5)
1.2.4 网关和防火墙	(5)
1.3 计算机网络的复杂性	(6)
1.4 对网络复杂性的控制	(6)
第2章 网络设备和系统安全分析	(8)
2.1 网络安全事件	(8)
2.1.1 国际网络安全事件	(8)
2.1.2 国内网络安全事件	(9)
2.2 设备安全分析	(10)
2.2.1 拨号接入服务器的安全问题	(10)
2.2.2 交换机的安全问题	(11)
2.2.3 路由器的安全问题	(11)
2.3 系统安全分析	(13)
2.3.1 Windows XP 漏洞	(14)
2.3.2 Web 服务器漏洞	(15)
2.4 黑客攻击方法	(17)
2.5 网络系统安全策略	(24)
第3章 网络设备安全技术基础	(27)
3.1 网络传输媒介	(27)
3.2 网络物理设备	(29)
3.2.1 网络接口卡与连接	(30)

3.2.2	调制解调器	(31)
3.2.3	中继器	(33)
3.2.4	集线器	(35)
3.2.5	交换机	(36)
3.2.6	网桥	(36)
3.2.7	路由器	(39)
3.2.8	访问服务器	(41)
3.3	广域网设备	(41)
3.3.1	广域网的构成	(42)
3.3.2	广域网的路由	(43)
第4章	网络协议的安全性	(44)
4.1	网络基本协议和安全性	(46)
4.1.1	IP	(46)
4.1.2	TCP	(50)
4.1.3	UDP	(53)
4.1.4	ICMP	(54)
4.2	地址转换协议和安全性	(57)
4.2.1	ARP	(57)
4.2.2	DNS	(60)
4.3	路由协议	(63)
4.3.1	路由选择及路由算法	(64)
4.3.2	内部网关协议 IGP	(70)
4.3.3	外部网关协议 EGP	(76)
4.4	应用协议	(78)
4.4.1	电子邮件协议 SMTP	(78)
4.4.2	远程登录协议 Telnet	(85)
4.4.3	文件传输协议 FTP, TFTP	(91)
4.4.4	超文本传输协议 HTTP	(102)
第5章	物理网络安全隔离技术及设备	(111)
5.1	什么是物理隔离	(111)
5.2	实现物理隔离中的问题	(113)
5.3	单机物理隔离技术	(113)
5.3.1	第一代技术	(114)

5.3.2	第二代技术	(114)
5.3.3	第三代技术	(115)
5.4	其他物理隔离技术	(116)
5.4.1	两个独立网络	(116)
5.4.2	安全隔离集线器	(116)
5.4.3	网络分线器、三通线	(116)
5.4.4	双硬盘计算机网络电子开关卡	(117)
5.4.5	计算机网络电子开关 (单硬盘计算机网络隔离器)	(118)
5.5	远程安全传输方式	(120)
5.6	安全网闸	(122)
5.7	内外网信息安全转发系统	(123)
5.8	物理隔离解决方案	(124)
5.8.1	单内网解决方案	(125)
5.8.2	远程解决方案	(126)
5.8.3	双网解决方案	(126)
5.8.4	单线连接双网方案	(127)
5.8.5	物理隔离产品解决方案——网络安全隔离卡	(127)
5.8.6	物理隔离产品解决方案——网络安全隔离器	(129)
5.9	物理隔离技术的展望	(136)
第6章	接入服务器的安全管理	(137)
6.1	接入服务器	(137)
6.2	接入服务器的功能模块	(140)
6.3	设备的功能要求	(140)
6.4	接入服务器的业务	(144)
6.5	常见的接入服务器的产品——Quidway 系列以太网接入服务器	(149)
6.6	接入服务器的安全	(158)
第7章	交换机的安全管理	(161)
7.1	多层交换技术	(162)
7.1.1	第二层交换	(162)
7.1.2	第三层交换技术	(166)
7.2	VLAN 及其安全性	(169)
7.2.1	VLAN 定义	(169)
7.2.2	静态 VLAN	(171)

7.2.3	动态 VLAN	(171)
7.2.4	中继	(171)
7.2.5	快速以太网和千兆以太网上的中继	(172)
7.3	典型交换机的安全管理	(173)
7.3.1	Cisco 交换机	(173)
7.3.2	3Com 交换机	(177)
7.4	生产交换机的厂商	(191)
7.5	第三层交换机的选择	(191)
第8章	路由器	(195)
8.1	路由器的发展	(195)
8.2	路由器的原理	(199)
8.3	路由器的管理	(201)
8.3.1	初始设置	(201)
8.3.2	配置主机名称和密码	(203)
8.3.3	配置1口和2口的以太网接口	(204)
8.3.4	配置快速以太网接口	(204)
8.3.5	配置异步/同步串行网络模块和WAN接口	(205)
8.3.6	配置16口和32口的异步网络模块	(206)
8.3.7	配置ISDN BRI WAN接口卡	(206)
8.3.8	配置T1和E1接口	(207)
8.3.9	配置T1 (FT1) WAN接口卡	(208)
8.3.10	配置AT复用M接口	(208)
8.3.11	配置1口ADSL WAN接口卡	(209)
8.3.12	配置G.SHDSL	(209)
8.4	路由器的安全	(210)
8.4.1	密码管理	(210)
8.4.2	控制交互权限	(211)
8.4.3	防止DDoS攻击	(212)
8.5	路由协议设置	(215)
8.5.1	RIP协议	(215)
8.5.2	IGRP协议	(216)
8.5.3	OSPF协议	(217)
8.5.4	重新分配路由	(221)
8.5.5	IPX协议设置	(223)

8.6 服务质量及访问控制 (225)

8.6.1 协议优先级设置 (225)

8.6.2 队列定制 (226)

8.6.3 访问控制 (226)

8.7 虚拟局域网 (VLAN) 路由 (227)

8.7.1 虚拟局域网 (VLAN) (227)

8.7.2 交换机间链路 (ISL) 协议 (227)

8.7.3 虚拟局域网 (VLAN) 路由实例 (228)

第9章 防火墙概述 (234)

9.1 背景 (234)

9.2 什么是防火墙 (234)

9.3 防火墙的职责和局限性 (235)

9.3.1 防火墙的职责 (235)

9.3.2 防火墙的局限性 (236)

9.4 防火墙技术的发展 (236)

9.4.1 防火墙技术演变 (236)

9.4.2 防火墙技术展望 (240)

9.5 防火墙的分类 (242)

9.6 专用术语 (243)

第10章 防火墙的设计与实现 (248)

10.1 相关标准 (248)

10.1.1 我国的信息安全标准 (248)

10.1.2 国外的信息安全标准 (251)

10.2 防火墙的需求 (253)

10.2.1 访问控制 (253)

10.2.2 管理员访问 (253)

10.2.3 个体身份记录 (254)

10.2.4 防火墙的自我保护 (254)

10.2.5 审计 (254)

10.3 防火墙的体系结构 (255)

10.3.1 双重宿主主机体系结构 (255)

10.3.2 屏蔽主机体系结构 (256)

10.3.3 屏蔽子网体系结构 (256)

10.4	防火墙中使用的安全技术	(258)
10.5	其他相关技术	(260)
10.5.1	安全操作系统	(260)
10.5.2	虚拟专用网	(261)
10.5.3	入侵检测系统	(262)
10.6	高速防火墙技术	(263)
10.6.1	专用集成电路 (ASIC) 技术	(263)
10.6.2	集群技术	(264)
10.6.3	分布式技术	(265)
10.7	防火墙开发	(265)
10.7.1	报文过滤	(265)
10.7.2	应用代理	(267)
10.7.3	地址翻译 (NAT)	(269)
10.7.4	管理控制	(270)
10.7.5	攻击检测	(271)
10.7.6	其他部分	(273)
10.8	防火墙的测试与评估	(273)
第 11 章	防火墙的使用与维护	(275)
11.1	网络环境及风险分析	(275)
11.1.1	被动攻击	(275)
11.1.2	主动攻击	(275)
11.1.3	内部攻击	(276)
11.1.4	发布攻击	(276)
11.2	防火墙的选择	(276)
11.2.1	技术因素	(277)
11.2.2	非技术因素	(279)
11.3	防火墙的部署	(280)
11.3.1	普通网络环境下的部署	(280)
11.3.2	多出口网络环境下的部署	(283)
11.3.3	高可靠性网络环境下的部署	(284)
11.3.4	分布式网络环境下的部署	(284)
11.4	防火墙安全策略的制定	(285)
11.4.1	确立指导思想	(285)
11.4.2	转化技术实现	(286)

11.4.3	建立规则集	(286)
11.4.4	优化规则集	(287)
11.4.5	维护规则集	(287)
11.5	防火墙的运行维护	(287)
11.5.1	运行环境	(288)
11.5.2	管理人员	(288)
11.5.3	管理制度	(289)
11.5.4	技术手段	(290)
11.6	典型应用案例	(291)
11.6.1	小型企业	(291)
11.6.2	中型企业	(292)
11.6.3	大型企业	(293)
第 12 章	防火墙产品介绍	(295)
12.1	Firewall-1 防火墙	(295)
12.1.1	技术特点	(295)
12.1.2	基本组成	(296)
12.1.3	产品功能	(297)
12.1.4	最新产品	(301)
12.2	NetScreen 系列防火墙	(302)
12.2.1	产品功能概述	(303)
12.2.2	产品分类介绍	(305)
12.3	FortiGate 系列防火墙	(310)
12.3.1	技术特点	(311)
12.3.2	产品功能	(312)
12.3.3	产品分类介绍	(314)
12.4	Cisco PIX 系列防火墙	(319)
12.4.1	适应性安全算法 (ASA)	(319)
12.4.2	产品功能	(320)
12.4.3	产品分类介绍	(321)
12.5	WatchGuard 防火墙	(323)
12.5.1	实时安全服务	(324)
12.5.2	产品功能	(324)
12.5.3	产品分类介绍	(326)
12.6	3Com 的嵌入式防火墙系统	(328)

12.6.1	3Com 防火墙卡	(329)
12.6.2	产品功能	(330)
12.6.3	产品介绍	(332)
12.7	CyberwallPLUS 防火墙	(333)
12.7.1	强大的入侵检测功能	(334)
12.7.2	集中的管理工具	(335)
12.7.3	其他安全功能	(336)
12.8	诺基亚硬件防火墙	(338)
12.8.1	IP 安全解决方案	(338)
12.8.2	产品功能	(339)
12.8.3	产品介绍	(340)
参考文献		(342)

第 1 章 概 述

1.1 计算机网络的发展

近年来，计算机网络获得了飞速的发展。20 年前，很少有人接触过网络。现在，计算机通信已成为社会结构的一个基本组成部分。全球因特网的持续发展是计算机网络领域最令人感兴趣的现象之一。因特网在 20 多年的时间里，从一个只有几十个站点的研究项目，发展成一个连接所有国家亿万人的通信系统。目前，计算机网络已应用到社会生活的各个领域。

网络的发展改变了人们的工作和生活。个人能方便地通过拨号网络或宽带网络与因特网相连。网络使个人化的远程通信成为可能，并改变了商业通信的模式。一个完整的用于发展网络技术、网络产品和网络服务的新兴工业已经形成，计算机网络的普及性和重要性已经导致不同岗位对具有更多网络知识的人才的大量需求。另外，计算机编程已不再局限于个人计算机，而要求程序员设计能进行网络通信的应用软件。

因特网对社会造成的影响在杂志和电视的广告中可见一斑。这些广告经常附带提供一个因特网站地址，从该处可以获得所宣传的产品或服务的补充信息。

1.1.1 资源共享

计算机可以利用网络访问外设。例如，一个网络上的计算机都能访问连入该网络的一台打印机。同样，一个网络上的计算机也能共享连入该网络的磁盘上的文件。但数据联网的最初动机并不是为了共享外设，也不是为了提供人们可以直接使用的通信手段。相反地，人们最初设计网络的目的是共享大规模的计算能力。

早期的数字计算机非常昂贵并且十分珍稀。随着计算机技术的进步，出现了具有更大计算能力和存储空间的计算机。但因为计算机被用于实验数据的分析，程序经常要运行几个小时甚至几天。而政府用于研究的预算并不足以所有的科学家和工程师提供计算机。

美国国防部高级研究计划署（Advanced Research Projects Agency, ARPA）对高性能计算机的缺乏特别关注。ARPA 的许多研究项目都需要使用最新的计算机设备，每个研究小组都希望得到所有新机型。到 20 世纪 60 年代末，ARPA 的预算已经明显不能满足需求。作为一种替代方案，ARPA 开始研究数据联网，使得每个研究小组通过网络就可以远程使用异地的高性能计算机，避免在每个研究组放置所有的高性能计算机。

ARPA 开始联网项目之初即面临着许多挑战。但 ARPA 的联网项目最后被证明是革命性的。ARPA 当时决定采用一种相对较新的联网方式，而这种方式成为后来所有数据网络的基础。

到 20 世纪 70 年代，互联网络技术成为 ARPA 研究的中心，这时早期的因特网已经出

现。研究工作持续到 20 世纪 80 年代，而因特网在 20 世纪 90 年代获得了商业成功。

1.1.2 因特网的增长

因特网 (Internet) 已经从早期的研究原型成长为覆盖世界上所有国家的全球通信系统。但是，高速的增长比单纯的规模更令人感到惊讶。因特网在 1990 年前几乎没有任何发展，所有的增长都发生在最近几年，特别是 1998 年最为显著。因特网在过去的几年中经历了指数倍增长，因特网的规模每过 9 个月到 12 个月就增长一倍。到 2003 年，仅中国就有网民 6 800 万。

1.1.3 基本概念解析

1. 万维网 (WWW)

WWW 即 World Wide Web，中文一般称为万维网，平常所说的 Web、互联网，其实与此是同一含义。创建 WWW 是为了解决 Internet 上的信息传递问题。在 WWW 创建以前，几乎所有的信息发布都是通过 E-mail，FTP，Archie 等实现的。E-mail 的使用，让不同的团体和个人之间的信息交换变得很广泛；文件传输协议 (File Transfer Protocol, FTP) 用来从一台计算机到另一台计算机进行文件传输；Archie 用来查找 Internet 上的各种文件，由于 Internet 上的信息散乱地分布在各处，因此除非知道所需信息的位置，否则无法对信息进行搜索。

由于这样或那样的限制，必须开发出一种全新的独立于各种平台的方法，以便于在 Internet 上传递信息。正是在这种需求下，瑞士日内瓦的欧洲粒子物理实验室 CERN 开发出超文本标记语言 (HTML)。HTML 是从一种称为标准化标记语言 (SGML) 的文档格式语言演化而来的。HTML 是一种易于学习、使用，在 Internet 上传递信息的文档表示语言，HTML 比 SGML 更简单易学。为了在 Internet 上传递 HTML 文档，要使用基于 TCP/IP 的协议。这种协议后来成为超文本传输协议 HTTP。WWW 是随 HTTP 和 HTML 一起出现的，Web 通过使用强有力的媒介传递信息，克服了许多早期信息传递的限制，Web 服务器利用 HTTP 传递 HTML 文件，Web 浏览器使用 HTTP 检索 HTML 文件，一旦从 Web 服务器检索到信息，Web 浏览器就会以静态和交互 (如文本、图像) 的形式显示各种对象。

随着文本、图像、影像、声音和交互式应用程序的统一，WWW 已经成为信息交换的一种很有效的方式。正是由于 WWW 的出现，我们才可以浏览各种信息来源，并且通过各种超级链接从一种信息来源转到另一种信息来源。超级链接是指向 Web 页面的统一资源定位器 (URL) 的对象。当用户单击一个超级链接时，该用户就会连接到超级链接所指向的 Web 页面。URL 可以看做是 Web 页面的地址。每个 Web 页面都有一个或多个 URL 与之相关。在特殊应用程序和浏览器的推动下，Web 很快成为 Internet 上发布文本和多媒体信息的一种有效手段。WWW 在很大程度上是在 NCSA (National Center for Supercomputing Applications) 于 1993 年发布的 Mosaic (Web 浏览器) 后得到普及的。

WWW 之所以如此流行，是因为它克服了 Web 浏览器出现之前许多应用程序的缺点，这些应用程序在 Internet 上用来发布信息。在过去，Internet 上几乎所有信息都是字符文本格

式, 这样的信息不能采用多种格式表示, 导致了浏览和搜索方面的困难。而 WWW 上的信息可以有多种格式, 易于浏览和理解。例如, 在讨论复杂问题时, 可以使用图表、影像剪辑甚至互动式应用程序, 而不仅仅是字符文本, 这样会便于解释论题, 使人一目了然。WWW 集成了所有的视觉辅助效果来表示信息。

WWW 与平台无关, 且服务器对于浏览 Web 站点的用户透明, 这是 WWW 成功的另一个原因。CERN 所定义的 Internet 标准和协议不是私有标准, 因此, 任何人都有权使用与 Internet 标准和规范一致的自己的 Web 服务器和 Web 浏览器。这种自由和开放性使得一些机构 (如 NCSA, Netscape 和 Microsoft) 能够扩充现有的 Internet 标准 (如 HTML), 满足 WWW 用户更广泛的需要。正是这些先驱机构的努力, 才使得 WWW 一直成为 Internet 的首选信息发布工具, 为 Internet 的使用者提供更多的选择权和控制权。与其他信息发布工具相比, WWW 由于所需的费用很低, 并且覆盖面广, 因而具有很大的吸引力。另外, 使用各种搜索机制在 Web 站点分类目录数据库注册一个 Web 站点, 可以使客户在需要时得到所需的信息。

2. TCP/IP 协议的历史

TCP/IP 的历史可以追溯至 20 世纪 70 年代中期, 当时 ARPA 为了实现异种网之间的互联与互通, 大力资助网间网技术的研究开发, 于 1977 年到 1979 年间推出与目前形式一样的 TCP/IP 体系结构和协议规范。

1980 年前后, ARPA 开始将 ARPANET 上的所有机器转向使用 TCP/IP 协议, 并以 ARPANET 为主干建立 Internet。

为了推广 TCP/IP 协议, 国防部高级研究计划署以低价出售 TCP/IP 的实现, 并通过资助美国加州大学伯克利分校将 TCP/IP 协议融入 BSD UNIX 版本。1983 年, 加州大学伯克利分校推出内含 TCP/IP 协议的第一个 BSD UNIX 版本。

BSD UNIX 成功的原因是多方面的。首先, 除了提供标准的 TCP/IP 应用程序外, 还包括一组网络服务工具, 这些工具和 UNIX 的使用方式相接近, 从而深受 UNIX 用户的欢迎。其次, BSD UNIX 提供一种访问通信协议的系统调用——Socket, Socket 是一种进程间通信的机制, 使程序员可以方便地访问 TCP/IP 协议, 或多或少地推动了 TCP/IP 的研究开发工作。

1985 年, 美国国家科学基金会 (National Scientific Foundation, NSF) 开始涉足 TCP/IP 的研究和开发, 并成为推动 TCP/IP 发展的重要角色。国家科学基金会资助建立了 NSFNET 网, 并采用 TCP/IP 为其传输协议。目前, NSFNET 已经取代 ARPANET 成为 Internet 的新的主干。

到今天, TCP/IP 技术及 Internet 已得到极为迅猛的发展, 出现了大量从事 Internet 技术开发和服务的公司。如今, Internet 被人们认为是一块新的淘金地, 人们从中也享受到不少 Internet 带来的便利, 如 WWW 服务、E-mail 服务和新出现的 IP 电话。

Internet 是全球最大的、开放的、由众多网络互联而成的计算机网络, 在这个庞大的网络中, 又可以分成许许多多的子网和子网的子网, 不同子网或网络可能使用不同的介质, 如 FDDI (光缆分布式数据接口)、ATM (异步传输模式)、以太网和无线网等。TCP/IP 就是用来屏蔽各种网络和机器的不同, 使它们可以相互通信, 并向上层提供一个公共的界面。