普通高等院校信息安全专业规划教材

Firewall Technology and Applications

防火墙技术与应用

免费提供电子教案

电子教案下载网址
http://www.cmpedu.com

陈 波 于 泠 编著

由各院校从事一线教学工作的教师编写
反映信息安全领域的最新技术和发展方向
注重理论性与实践性相结合
提供完善的教学配套资源

机械工业出版社
CHINA MACHINE PRESS

普通高等院校信息安全专业规划教材

防火墙技术与应用

陈 波 于 泠 编著

机械工业出版社

防火墙作为网络安全防护的一道重要防线正发挥着重要的作用。本书分为四篇，共 11 章内容，分别从技术原理和应用实践的角度，系统介绍了防火墙的工作原理、开发与测试标准、个人防火墙开发关键技术、个人防火墙及商用防火墙的选购、部署及应用等内容。本书每章均附有思考与练习题，还给出了大量的参考文献以供读者进一步阅读。

本书针对信息安全专业的教学规划，可以作为信息安全专业以及计算机应用型人才培养与认证体系中的教材，也可以作为负责安全保障的网络管理人员、信息管理人员和对计算机网络安全感兴趣读者的参考用书。

本书配套授课电子教案，需要的教师可登录 www.cmpedu.com 免费注册，审核通过后，即可下载，或联系编辑索取（QQ：2399929378，电话：010-88379750）。

图书在版编目(CIP)数据

防火墙技术与应用/陈波，于泠编著. —北京：机械工业出版社，2012.11
普通高等院校信息安全专业规划教材
ISBN 978-7-111-40081-3

Ⅰ.①防… Ⅱ.①陈… ②于… Ⅲ.①计算机网络—安全技术—高等学校—教材 Ⅳ.①TP393.08

中国版本图书馆 CIP 数据核字（2012）第 243636 号

机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）
责任编辑：郝建伟 曹文胜
责任印制：张 楠
北京圣夫亚美印刷有限公司印刷
2013 年 1 月第 1 版 · 第 1 次印刷
184mm×260mm · 13.5 印张 · 332 千字
0001—3000 册
标准书号：ISBN 978-7-111-40081-3
定价：29.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

电话服务		网络服务	
社服务中心	:(010)88361066	教材网	:http://www.cmpedu.com
销售一部	:(010)68326294	机工官网	:http://www.cmpbook.com
销售二部	:(010)88379649	机工官博	:http://weibo.com/cmp1952
读者购书热线	:(010)88379203	封面无防伪标均为盗版	

前　言

随着计算机及网络技术的不断发展和日益普及，人们对计算机及网络的依赖也越来越强，电子商务、电子政务、电子银行以及多方面的网络信息服务已经深入到人们工作和生活的方方面面。然而，非授权访问、信息窃取和网络攻击等网络安全问题已经从原来的国防军事领域扩展到了整个社会生活，网络安全问题成为人们不得不面对和解决的重要问题之一。

防火墙作为信息保障模型（PDRR）——防护、检测、反应与恢复的一个重要环节，是网络攻击防范的一道重要防线，它可以识别并阻挡许多的网络攻击行为。防火墙是在不同网络（如可信任的企业内部网络和不可信的公共网络）或不同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唯一出、入口，能根据网络安全策略控制（允许、拒绝、监测）出入网络的信息流，且自身具有较强的抗攻击能力。防火墙是保护内部网络免受网络入侵的有效屏障，能够将未授权的访问阻塞从而保障内部网络数据的安全。它是提供信息安全服务，实现网络与信息安全的基础设施。

最早的防火墙是依附于路由器的包过滤功能，即通过在路由器上创建简单的访问控制列表来实现防护功能。不过由于传递数据包的网络协议的复杂性，基于路由器的访问控制列表还是不够安全。随后，防火墙技术不断发展，先后出现了满足不同需求的状态包检测防火墙、应用级网关防火墙，以及网络地址转换 NAT、虚拟专用网 VPN 等技术。防火墙在保护网络安全方面正发挥着重要的作用。

本书针对信息安全专业的教学规划，希望读者通过本书了解防火墙的基本原理、实现技术、开发标准以及应用实例，提高安全防护能力。

全书包括 4 个部分。第 1 篇“防火墙基础技术”，包括第 1、2 两章。第 1 章介绍了防火墙在网络安全防护中的地位和作用；第 2 章从防火墙的定义出发，阐述了防火墙的功能、各项核心技术的工作原理、防火墙的结构以及下一代防火墙技术。本篇内容为读者应用和开发防火墙打下了理论基础。

第 2 篇“防火墙标准”，包括第 3、4 两章。主要依据 GB/T 20281—2006《信息安全技术 防火墙技术要求和测试评价方法》等国家标准介绍防火墙的技术要求和评测方法，对防火墙产品或系统的设计、研发和应用给予指导。

第 3 篇“个人防火墙开发技术”，包括第 5～7 共 3 章。第 5 章介绍了 Windows 系统下的网络体系结构，研究在用户层（User-mode）和内核层（Kernel-mode）下可能采用的网络数据包拦截技术；第 6 章介绍了用户层下 Winsock SPI 数据包截获技术；第 7 章介绍了内核层下 NDIS 数据包截获技术。本篇详细给出了两个开发示例。

第 4 篇“防火墙应用”，包括第 8～11 共 4 章。第 8 章介绍了个人防火墙的使用，包括 Windows 7 系统自带的 Windows 防火墙和高级安全 Windows 防火墙，以及著名的第三方防火墙软件 ZoneAlarm Pro Firewall；第 9 章介绍了 Linux 2.4 内核中一个具有包过滤、数据包处理、网络地址转换等防火墙功能框架的 netfilter/iptables，并给出了一个 iptables 综合应用实例；第 10 章对国内外一些主要的防火墙产品做了简单介绍，使读者对主流防火墙产品有

基本的了解，还给出了防火墙产品选型的一些基本原则；第 11 章介绍了用 3 种工具进行商用防火墙应用的实验，3 种工具分别是：Cisco 公司发布的网络模拟环境 Packet Tracer；自由软件、需要运行 Cisco 系统（IOS）的模拟器 GNS3 以及 Microsoft Forefront 系列中的产品 Forefront TMG。本篇给出了详细的操作和配置步骤。

本书在编写过程中力求体现如下特点。

1）跟踪技术动态。本书内容跟踪当前防火墙的技术动态，并且与实际产品相结合，保证较高的实用性，能够为网络安全管理员、工程师和相关技术人员，以及防火墙技术的初学者，应用防火墙实现网络安全防护提供切实的指导。

2）遵循国家标准。主要依据 GB/T 20281—2006《信息安全技术 防火墙技术要求和测试评价方法》等国家标准介绍防火墙的技术要求和评测方法。避免了以往教材多以各个厂商的产品功能来介绍，带来的内容凌乱、缺乏规范、让人无所适从的问题。

3）面向实际应用。从个人防火墙的开发到应用，从商业防火墙的选购到部署，层层推进，既让读者了解常见防火墙的产品特点，为实际应用的选购提供参考，又通过典型个人防火墙、开源防火墙 Linux iptables 以及商业防火墙的配置实例讲解，引领读者掌握防火墙实际操作技能，有利于用户在实际解决问题时借鉴，增强了本书的实用性。

4）方便教学练习。全书内容阐述循序渐进、深入浅出、条理清晰、图文并茂、便于自学，提供教学课件，每章配有思考与练习题，题型包括填空题、选择题、简答题、操作实验题以及撰写读书报告等，内容覆盖了每章中的重要知识点，对于读者掌握这些知识点以及使用技巧都有很大的帮助。

本书适用于高等院校、大中专学校作为相关课程的教材，亦可作为计算机职业技能考试及继续教育的培训教材或自学教材，也适用于社会各界人士以及在校学生参加“全国信息化计算机应用技术资格认证（CCAT）”、“国家信息化安全教育认证（ISEC）”考试的需求。

本书由陈波和于泠执笔完成。另外，李弼翀、秦春芳、王宁、张威威、唐相艳、林龙成也参与了本书实验初稿的整理工作。

本书的完成得到了江苏省精品教材建设项目、南京师范大学精品课程，以及南京师范大学教学改革项目的支持。本书在写作过程中，查阅、参考了大量的文献、资料，限于篇幅未能在书后的参考文献中一一列出，在此一并致谢。

由于时间仓促，加之编者水平有限，书中难免有疏漏之处，恳请广大读者批评指正。读者在阅读本书的过程中若有疑问也欢迎与作者联系，电子邮箱是：SecLab@163.com。

编　者

目　录

第 2 篇 防火墙标准

第 3 篇 防火墙实现

第 4 篇 防火墙应用

第 1 篇 防火墙基础

网络安全从其本质上来讲就是网络上的信息安全，一般是指网络信息的机密性、完整性、可用性、可控性、不可抵赖性和可认证性等。

由美国国家安全局 NSA 提出的，为保护美国政府和工业界的信息与信息技术设施提供的技术指南《信息保障技术框架》（Information Assurance Technical Framework，IATF），提出了目前信息基础设施的整套安全技术保障框架，定义了对一个系统进行信息保障的过程以及软硬件部件的安全要求。IATF 代表理论为“纵深防护战略（Defense-in-Depth）”，其中的四个技术焦点包括：保护网络和基础设施、保护边界、保护计算环境和保护基础设施。防火墙作为边界防护的一种重要工具和技术得到了广泛应用。

本篇包括第 1、2 两章。第 1 章介绍了防火墙在网络安全防护中的地位和作用，帮助读者了解防火墙在整个网络信息安全防护中所处的位置；第 2 章从防火墙的定义出发，阐述了防火墙的功能、各项核心技术的工作原理、防火墙的结构以及下一代防火墙技术。本篇内容对防火墙核心技术的分析，为读者应用和开发个人防火墙打下了理论基础。

第 1 章　防火墙在网络安全防护中的地位和作用

TCP/IP 在互联网中的应用，为因特网普及起到了关键性作用。然而，最初主要应用于学术研究的因特网以及通信协议是基于良好的应用环境而设计的。那时用户和主机之间互相信任，可以进行自由开放的信息交换的环境。而如今因特网上充斥着安全风险，如以各种非法手段企图深入计算机网络的黑客带来的危害。随着网络覆盖范围的扩大而增加，网络安全成为必须要考虑的问题。

本章首先介绍两种重要的网络体系模型 OSI 和 TCP/IP 的基础知识，接着介绍网络安全框架，由此帮助读者认识防火墙在网络安全防护中的基础性地位和作用。

1.1　网络体系结构

本书介绍两种重要的网络体系模型 OSI 和 TCP/IP 的基础知识。

1.1.1　开放系统互连参考模型 OSI

为了使不同体系结构的计算机网络能够互连，国际标准化组织 ISO 于 1977 年成立了专门的机构研究该问题。不久，他们提出了一个试图使各种计算机在世界范围内互连成网络的标准框架，即著名的开放系统互连参考模型（Open Systems Interconnection Reference Model，OSI/RM），简称 OSI。“开放”是指：只要遵循 OSI 标准，一个系统就可以和位于世界上任何地方的、也遵循同一标准的其他任何系统进行通信。“系统”是指在现实的系统中与互连有关的各部分。开放系统互连参考模型 OSI/RM 只是个抽象的概念。在 1983 年形成了开放系统互连参考模型的正式文件，即著名的 ISO 7498 国际标准。

OSI 参考模型采用结构描述方法将整个网络的通信功能划分为 7 部分（层次），在每个协议层中完成一系列的特定功能。两台网络主机之间进行通信时，发送方将数据从应用层向下传递到物理层，每一层协议模块为下一层进行数据封装，数据流经网络到达接收方，再由下而上通过协议栈传递，并与接收方应用程序进行通信。

1.1.2　TCP/IP 结构

事实上，得到广泛应用的不是国际标准 OSI，而是 TCP/IP 参考模型。OSI 的 7 层协议体系结构虽然概念清楚，但是复杂又不适用。TCP/IP 得到了全世界的承认，成为因特网使用的参考模型。

计算机网络系统可以看成是一个扩大了的计算机系统，在网络操作系统和 TCP/IP 的支持下，位于不同主机内的操作系统进程可以像在一个单机系统中一样互相通信，只不过通信时延稍大一些而已。

TCP/IP 协议族可以看做是一组不同层的集合，每一层负责一个具体任务，各层联合工作以实现整个网络通信。每一层与其上层或下层都有一个明确定义的接口来具体说明希望处

理的数据。一般将 TCP/IP 协议族分为 4 个功能层：应用层、传输层、网络层和网络接口层。这 4 层概括了相对于 OSI 参考模型中的 7 层。TCP/IP 与 OSI 这两种体系结构的对比如图 1-1 所示。

TCP/IP 层次如图 1-2 所示。

图 1-1　TCP/IP 与 OSI 体系结构对比

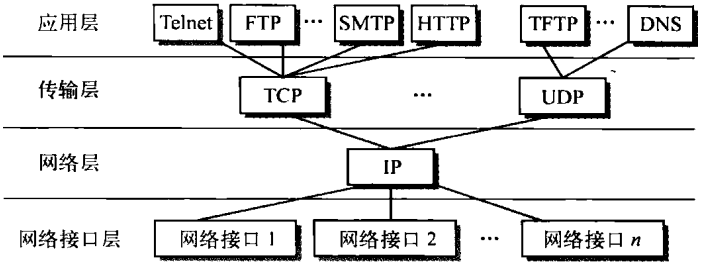

图 1-2　TCP/IP 层次

（1）应用层

应用层包含应用程序实现服务所使用的协议。用户通常与应用层进行交互。

- HTTP：超文本传输协议，提供浏览器和 WWW 服务间有关 HTML 文件传递服务。
- FTP：文件传输协议，提供主机间数据传递服务。
- Telnet：虚拟终端协议，提供远程登录服务。
- SMTP：简单消息传输协议，提供发送电子邮件服务。
- DNS：域名解析协议，完成域名解析服务。

此外，还有 POP3、OSPF、NFS 和 TFTP 等其他一些应用协议。

（2）传输层

传输层响应来自应用层的服务请求，并向网络层发出服务请求。传输层提供两台主机间透明的传输，通常用于端到端连接、流量控制或错误恢复。这一层的两个最重要协议是 TCP 和 UDP。TCP 提供可靠的数据流通信服务。TCP 的可靠性由定时器、计数器、确认和重传来实现。与 TCP 处理不同的是，UDP 不提供可靠的服务，主要用于在应用程序间发送数据。UDP 数据报有可能丢失、复制和乱序。

（3）网络层

网络层负责处理网络上的主机间路由及存储转发网络数据包。IP 是网络层的主要协议，提供无连接、不可靠的服务。IP 还给出了因特网地址分配方案，要求网络接口必须分配独一无二的 IP 地址。同时，IP 为 ICMP、IGMP 以及 TCP 和 UDP 等协议提供服务。

（4）网络接口层

网络接口层有时又称数据链路层，一般负责处理通信介质的细节问题，如设备驱动程序、以太网（Ethernet）和令牌环网（Token Ring）。ARP 和 RARP 负责 IP 地址和网络接口物理地址的转换工作。

IP、TCP 和 UDP 是必须了解的协议，下面进行简要介绍。

（1）IP

IPv4 是一个面向数据的协议，设计用于分组交换网络（例如以太网），是一个尽最大努力完成交付的协议。这意味着它并不保证一台主机发送的 IP 数据包能够被目的主机接收到。此外，它并不能保证 IP 数据包被正确接收，一个数据包可能会被乱序接收或根本接收不到。这些问题由传输层协议解决，特别是 TCP 实现的几个机制保证了在 IP 之上的可靠数据传输。

IP 通过所谓的 IP 地址实现寻址，互联网中的每台主机都有一个 IP 地址，可以把它想象为一个地址，在这一地址下主机是可达的。通常，一个 IP 地址用点分十进制法表示——也就是 4 个十进制表示的字节用圆点分隔，例如，192.0.2.1。通过这个 IP 地址，网络中的其他主机可以联络这个主机。

此外，IP 实现了分片概念。由于不同类型的网络发送数据包有不同的最大数据量限制，可能需要将一个包分解成若干较小的包，这就是 IP 分片。而且由于接收端主机不得不将不同分片重新组装起来，因此需要 IP 重组。

在 TCP/IP 的标准中，各种数据格式常常以 32bit（4 字节）为单位来描述。图 1-3 是 IP 数据包的完整格式。

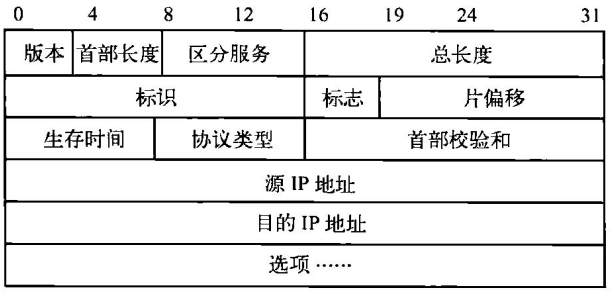

图 1-3　IP 头部结构

图 1-4 给出了一个数据包的简单表示法，即只画出 IP 首部最重要的两个字段：源 IP 地址和目的 IP 地址。数据包中的数据可以是传输层的 TCP 报文或 UDP 报文，也可以是 ICMP 报文等。

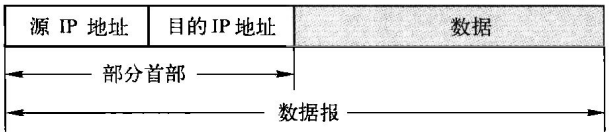

图 1-4　数据报的简单表示法

（2）TCP

TCP 是面向连接的，通过所谓的数据流，在两个网络主机之间提供一个可复用的、可靠的通信信道。TCP 保证数据从发送者到接收者可靠和有序地交付，而 UDP 不能保证这些属性。TCP 从应用层接收字节流，把它们分成适当大小的片段，然后这些片段被交给网络层（通常为 IP），对它们进行进一步的处理。TCP 给每个报文一个序列号，通过检查序列号以确保没有报文丢失。运行在接收主机上的 TCP，为所有已成功接收到的报文返回一个确认号。与序列号一起，这个确认号用于检查是否收到所有报文，如果需要，则可以对它们重新排

序。如果在合理的时间范围内没有接收到确认，则发送主机上的定时器将产生一个超时，根据这一信息，如果有需要，则可以重传丢失报文。同时，TCP 使用校验和来控制是否正确接收一个给定的报文。此外，TCP 应用拥塞控制，实现高性能和避免网络链路拥塞。

如上所述，TCP 有些复杂，但与 UDP 相比它有很多优势。如果两台主机需要可靠的网络通信，则常使用 TCP。例如，对于万维网使用的 HTTP、电子邮件相关应用程序使用的 SMTP 和 POP3/IMAP，以及数据传输使用的 FTP，这是必要的。

下面介绍 TCP 报文头，并解释如何建立 TCP 连接。图 1-5 显示了 TCP 头部结构。

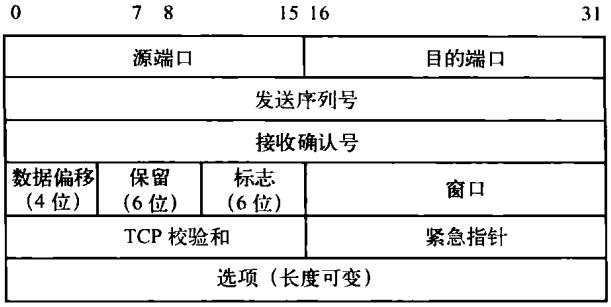

图 1-5　TCP 头部结构

一开始，两个 16 位字段指定源和目的端口，在传输层中端口用于多路复用，通过网络端口，使不同的应用程序在一个 IP 地址上监听成为可能。例如，典型地，一个 Web 服务器监听 TCP 端口 80，而一个 SMTP 服务器使用 TCP 端口 25，通过复用，两个服务器“共享”主机 IP 地址。TCP 头接下来的两个字段包含 32 位序号和确认号。序号有两个重要的作用，首先用于配置连接时设置初始序号，如果连接建立，有效载荷中的第一个数据字节就是序号。如果 ACK 标志被设置，则确认号指定发送者期望的下一个序号。

6 位的 TCP 标志用于提供有关当前 TCP 报文状态的信息。窗口大小字段用于指定发送者希望接收的从确认号开始的字节数。TCP 头还包含一个校验和，用于在目的地检验到达的报文是否未被篡改。只有设置 URG 标志时，才使用紧急指针字段，它指定了从序号开始的偏移量，指明 TCP 有效载荷中从哪个点开始的数据应立即移交给应用层。TCP 头还有其他可选字段，这里不再讨论。

因为 TCP 在发送者和接收者之间建立了一个连接，它需要在通信刚开始时创建一个连接。这是通过 TCP 握手完成的，这个握手主要通过交换序号和确认号在两个主机之间同步状态，这些数字稍后用于确认目的主机是否正确收到给定的报文，以及用于重传和拥塞控制。TCP 握手过程需要在发送者 S 和接收者 R 之间交换三个协议消息，如图 1-6 所示。

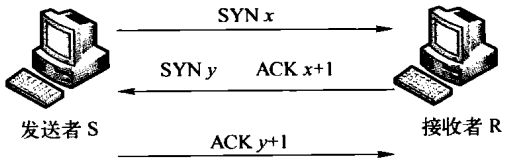

图 1-6　TCP 在发送者和接收者之间建立一个连接

1）S→R：发送方发送一个带有 SYN 标志位（置 1）和一个序号为 x 的报文。

2）S←R：接收者应答一个带有 SYN 和 ACK 标志位（都置 1）的 TCP 报文，确认号被设置为主机希望接收的下一个序号，这个例子中是 x+1。此外，接收者将它的序号设置为 y，因为它也希望与另一方同步这个序号。

3）S→R：发送方发送一个带有 ACK 标志位（置 1）的 TCP 报文，它响应的报文序号为 x+1，同时增加确认号为 y+1。

这一握手过程之后，双方都知道对方的序号和确认号的当前值，之后，此信息被用于 TCP 所有目标，例如，无差错数据传输和拥塞控制。

（3）UDP

用户数据报协议 UDP 是 IP 上面的一个层，如图 1-7 所示，UDP 有两个字段：首部字段和数据字段。

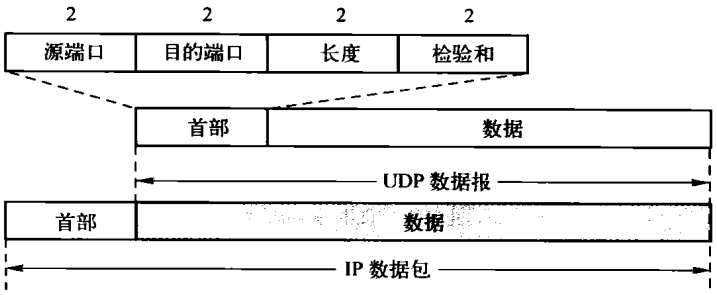

图 1-7　UDP 数据报结构

UDP 只在 IP 的数据包服务之上增加了很少一点功能，也就是端口和差错校验的功能。有了端口，就能为应用程序提供多路复用，换言之，能够为运行在同一台计算机上的多个并发应用程序产生的多个连接区分数据。因此，虽然 UDP 数据报只能提供不可靠的交付，但在许多方面还必须使用 UDP 数据报。表 1-1 给出了使用 UDP 和 TCP 的各种应用和应用层协议。

表 1-1　使用 UDP 和 TCP 的各种应用和应用层协议

应　用	应用层协议	传输层协议
域名转换	DNS	UDP
文件传送	TFTP	UDP
路由选择协议	RIP	UDP
IP 地址配置	BOOTP，DHCP	UDP
网络管理	SNMP	UDP
远程文件服务	NFS	UDP
IP 电话	专用协议	UDP
流式多媒体通信	专用协议	UDP
多播	IGMP	UDP
电子邮件	SMTP	TCP
远程终端接入	Telnet	TCP
万维网	HTTP	TCP
文件传送	FTP	TCP

UDP 最主要的缺点是，它不提供任何的可靠性和数据报有序性，数据报到达时可能是无序的、重复出现的，甚至根本没有到达目的主机。它不直接处理报文丢失或报文重新排序。没有检查每一个数据报是否都到达所需的开销，对许多轻量级或时间敏感的应用，UDP 更快更有效。因此，这一协议通常用于流媒体（IP 语音或视频聊天）和在线游戏，对于这些应用，丢失一些数据报不是至关重要的。UDP 另一个重要应用是域名系统 DNS，用来把一个给定 URL 解析为一个 IP 地址。

TCP/IP 族的另一个重要方面是 IP 路由，理解 IP 路由的重要性有多种原因：它是主机之间可以相互通信的基本方法，并提供对互联网拓扑结构和小型网络（一个企业网络）拓扑结构的深入理解。为了成功地应用防火墙，了解互联网路由也是很重要的。

读者可以进一步阅读谢希仁编著的《计算机网络（第 5 版）》（电子工业出版社），Behrouz A. Forouzan, Sophia Chung Fegan 等编著、谢希仁等翻译的《TCP/IP 协议族（第 3 版）》（清华大学出版社）等书籍。

1.1.3 网络中数据包的传输

本节通过嗅探工具 Wireshark 捕获实际的数据包来分析网络中数据包传输的细节。

数据在传输过程中，必须被分解成一个个的小碎片。这就如同我们在运送大批的货物时，因为每辆卡车所能运载的货物量是有限的，必须使用多辆卡车来执行这项任务一样。在网络世界里也是同样的道理，因为不同的网络实体层技术，其每次所能承载的数据量不同。因此，数据在传输过程中，必须先被分解成一个个的数据包才能被传输，然后一层层地传送。

例如，当用户在计算机上运行某一应用程序（如 MSN）时，该应用程序一定会先定义一种数据交换方法（应用层通信协议），接着确定数据传输方式，比如，数据在传输过程中是不可丢失或者错误的，那么就需要使用 TCP 作为数据传输的方法；接着，为了能将数据正确地传输到目的端，我们使用网络上每台计算机唯一的识别码 IP 地址，作为发送端和接收端的地址，但由于 IP 地址是属于逻辑信息，无法以光电信号呈现，而实体层的寻址方式是用 MAC 地址来识别（假设实体层是以太网），因此，当数据发送到实体层时，会在该数据中附加上发送端和接收端的 MAC 地址，这样便可以将数据传输到正确的目的地。

使用嗅探工具 Wireshark 来截取网络上所传输的数据包，即可了解整个数据包传输的过程，如图 1-8 所示。以图中编号 322 的数据包为例，中间的窗体部分就是数据包的结构，其结构分别如下。

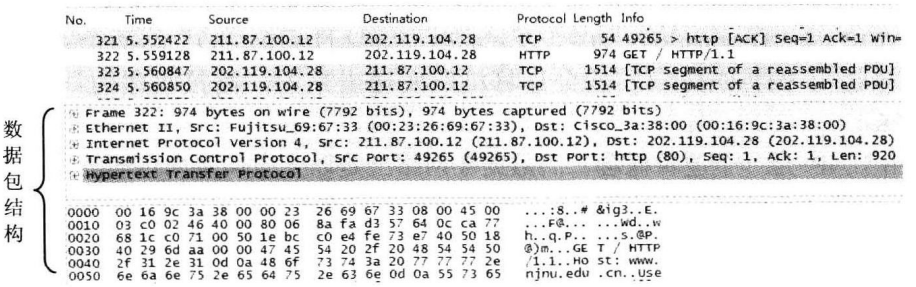

图 1-8 Wireshark 截取的数据包