21世纪高等学校规划教材 | 计算机科学与技术

TCP/IP协议分析教程与实验

陈 年 主编

清华大学出版社

TCP/IP协议分析教程与实验

陈 年 主编

清华大学出版社
北京

内 容 简 介

本书采用理论与实践相结合的方法介绍 TCP/IP 协议族各层协议。选取 TCP/IP 协议框架中每一层的主要协议，包括以太网和 IEEE 802.3、ARP、ICMP、IP、RIP、OSPF、UDP、TCP、DNS、DHCP、SNMP、Telnet、HTTP 和 FTP 等协议。在介绍协议基本原理的基础上，利用在网络仿真环境和真实环境中捕获协议数据包，对协议工作过程进行深入的分析。本书突出通过实验直观地再现协议工作机制，激发学生的学习兴趣，提高学生的工程实践能力。

本书可作为计算机及相关专业本科生学习 TCP/IP 协议原理的教材，也可作为高职院校协议分析技术的教材，还可作为计算机网络从业人员的参考书。

图书在版编目(CIP)数据

TCP/IP 协议分析教程与实验/陈年主编. —北京：清华大学出版社，2016
(21 世纪高等学校规划教材 · 计算机科学与技术)
ISBN 978-7-302-45355-0

Ⅰ. ①T…　Ⅱ. ①陈…　Ⅲ. ①计算机网络－通信协议－高等学校－教材　Ⅳ. ①TN915.04

中国版本图书馆 CIP 数据核字(2016)第 260935 号

责任编辑：付弘宇　王冰飞
封面设计：傅瑞学
责任校对：李建庄
责任印制：刘海龙

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课 件 下 载：http://www.tup.com.cn，010-62795954

印 刷 者：北京富博印刷有限公司
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：13.5　　**字　　数**：325 千字
版　　次：2016 年 12 月第 1 版　　**印　　次**：2016 年 12 月第1次印刷
印　　数：1～2000
定　　价：29.00 元

产品编号：069560-01

出版说明

随着我国改革开放的进一步深化，高等教育也得到了快速发展，各地高校紧密结合地方经济建设发展需要，科学运用市场调节机制，加大了使用信息科学等现代科学技术提升、改造传统学科专业的投入力度，通过教育改革合理调整和配置了教育资源，优化了传统学科专业，积极为地方经济建设输送人才，为我国经济社会的快速、健康和可持续发展以及高等教育自身的改革发展做出了巨大贡献。但是，高等教育质量还需要进一步提高以适应经济社会发展的需要，不少高校的专业设置和结构不尽合理，教师队伍整体素质亟待提高，人才培养模式、教学内容和方法需要进一步转变，学生的实践能力和创新精神亟待加强。

教育部一直十分重视高等教育质量工作。2007 年 1 月，教育部下发了《关于实施高等学校本科教学质量与教学改革工程的意见》，计划实施“高等学校本科教学质量与教学改革工程”（简称“质量工程”），通过专业结构调整、课程教材建设、实践教学改革、教学团队建设等多项内容，进一步深化高等学校教学改革，提高人才培养的能力和水平，更好地满足经济社会发展对高素质人才的需要。在贯彻和落实教育部“质量工程”的过程中，各地高校发挥师资力量强、办学经验丰富、教学资源充裕等优势，对其特色专业及特色课程（群）加以规划、整理和总结，更新教学内容、改革课程体系，建设了一大批内容新、体系新、方法新、手段新的特色课程。在此基础上，经教育部相关教学指导委员会专家的指导和建议，清华大学出版社在多个领域精选各高校的特色课程，分别规划出版系列教材，以配合“质量工程”的实施，满足各高校教学质量和教学改革的需要。

为了深入贯彻落实教育部《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》精神，紧密配合教育部已经启动的“高等学校教学质量与教学改革工程精品课程建设工作”，在有关专家、教授的倡议和有关部门的大力支持下，我们组织并成立了“清华大学出版社教材编审委员会”（以下简称“编委会”），旨在配合教育部制定精品课程教材的出版规划，讨论并实施精品课程教材的编写与出版工作。“编委会”成员皆来自全国各类高等学校教学与科研第一线的骨干教师，其中许多教师为各校相关院、系主管教学的院长或系主任。

按照教育部的要求，“编委会”一致认为，精品课程的建设工作从开始就要坚持高标准、严要求，处于一个比较高的起点上。精品课程教材应该能够反映各高校教学改革与课程建设的需要，要有特色风格、有创新性（新体系、新内容、新手段、新思路，教材的内容体系有较高的科学创新、技术创新和理念创新的含量）、先进性（对原有的学科体系有实质性的改革和发展，顺应并符合 21 世纪教学发展的规律，代表并引领课程发展的趋势和方向）、示范性（教材所体现的课程体系具有较广泛的辐射性和示范性）和一定的前瞻性。教材由个人申报或各校推荐（通过所在高校的“编委会”成员推荐），经“编委会”认真评审，最后由清华大学出版

社审定出版。

目前，针对计算机类和电子信息类相关专业成立了两个“编委会”，即“清华大学出版社计算机教材编审委员会”和“清华大学出版社电子信息教材编审委员会”。推出的特色精品教材包括：

(1) 21 世纪高等学校规划教材·计算机应用——高等学校各类专业，特别是非计算机专业的计算机应用类教材。

(2) 21 世纪高等学校规划教材·计算机科学与技术——高等学校计算机相关专业的教材。

(3) 21 世纪高等学校规划教材·电子信息——高等学校电子信息相关专业的教材。

(4) 21 世纪高等学校规划教材·软件工程——高等学校软件工程相关专业的教材。

(5) 21 世纪高等学校规划教材·信息管理与信息系统。

(6) 21 世纪高等学校规划教材·财经管理与应用。

(7) 21 世纪高等学校规划教材·电子商务。

(8) 21 世纪高等学校规划教材·物联网。

清华大学出版社经过三十多年的努力，在教材尤其是计算机和电子信息类专业教材出版方面树立了权威品牌，为我国的高等教育事业做出了重要贡献。清华版教材形成了技术准确、内容严谨的独特风格，这种风格将延续并反映在特色精品教材的建设中。

清华大学出版社教材编审委员会

联系人：魏江江

E-mail：weijj@tup.tsinghua.edu.cn

前言

TCP/IP 原理是网络工程专业的主干专业课程内容，同时也是计算机应用相关学科专业学生深入学习计算机网络技术的主要内容。实现掌握 TCP/IP 协议族中协议工作原理这一学习目标的主要途径需要通过网络协议分析来达成。针对协议分析具有很强的理论性和实践性的特点，同时考虑到计算机及相关专业的本科教育多强调应用能力的培养，编者旨在将本书编写成为一种注重网络协议分析实验及操作，把 TCP/IP 原理的理论学习和实验相互融合的教材。

本书按照 TCP/IP 协议框架的层次结构对网络互连中的主要协议进行分析，采用实例分析的方法学习 TCP/IP 基本原理。选取 TCP/IP 协议框架中每一层的主要协议，包括链路层以太网和 IEEE 802.3、ARP、ICMP、IP、RIP、OSPF、UDP、TCP、DNS、DHCP、SNMP、Telnet、HTTP 和 FTP 等协议，由下而上地设计了 26 个实验，利用在网络仿真环境和真实环境中捕获协议数据包，将抽象的网络协议的 PDU 构成和工作原理通过实验直观形象地展示出来，使学生能将理论与实践结合起来，加深对网络协议的理解并掌握协议分析的基本方法。

本书编写上特点突出，强化了在阐述 TCP/IP 协议概念和原理的基础上动手实践的内容。首先是重构实验内容，把 TCP/IP 原理课程中对 TCP/IP 各个协议工作原理的学习，用当今主要的网络协议学习工具和协议分析工具进行教学内容和实验形式的重新设计，通过实验强化学生的网络工程实践能力。其次，融合了多种当今主流的网络协议分析和学习工具，综合国内外相关教程的内容，可以使学生以不同的方式，从不同的角度来理解和掌握协议原理，获得更大的学习自主性和积极性。实验既可以在真实网络设备上进行，也可以在虚拟或仿真环境中完成，使学生即使在课余时间也可以自己学习，更好地提高学习效果。第三是改变网络协议的讲解形式，采用基于协议分析工具的讲解方式，让学生在实际的网络环境中通过再现网络协议工作过程和解析网络协议，真正做到“做中学”，全面彻底改变学生死记硬背网络协议的学习方式，让网络协议的工作过程变得触手可及，大大地提高了学生的学习兴趣和学习效果，有效地提高学生的网络工程实践能力和应用能力。第四是教材中对路由器和交换机等网络设备有要求的实验都可在仿真条件下进行，因此即便实验条件不够完备，也可以完成相关的实验教学。

本书适合已经学习过计算机网络基础课程且已掌握计算机网络基本体系结构，需要进一步学习掌握具体的网络协议工作原理的读者使用。书中各章安排的实验按学生实验指导书的形式编写，能够直接满足教学需要，因而也适合作为高校计算机网络原理教学中协议分析实验课程的教材使用。

全书共 8 章。除第 1 章外，其余各章的基本结构都按照先介绍基本概念和理论，再安排实验内容的方式编排，实验内容上覆盖了各章主要的知识点。第 1 章为 TCP/IP 协议概述，介绍 TCP/IP 协议分层、封装与分用的概念、RFC、应用编程的套接字和 Libpcap 编程接口。第 2 章为协议分析和学习工具，介绍协议分析器的基本原理和用途、Cisco Packet Tracer、

Wireshark、GNS3、Sniffer pro 和科来网络分析系统的特点和用法，实验内容安排了 Cisco Packet Tracer、Wireshark、GNS3 的使用方法学习。第 3 章为链路层协议分析，介绍链路层的作用、以太网的帧结构、SLIP 和 PPP 帧结构、MTU 和环回接口，实验内容安排了 DIX Ethernet V2 帧、IEEE 802 帧和 PPP 帧分析、环回接口实验。第 4 章为 ARP 协议分析，介绍地址变换的概念、ARP 协议的工作过程、协议报文格式和特殊的 ARP，实验内容安排了 arp 命令用法、ARP 请求与应答、ARP 代理和免费 ARP 实验。第 5 章为 ICMP 协议分析，介绍 ICMP 的作用、ICMP 报文及类型，分析 ICMP 差错报告、控制报文和查询报文的特点、ping 程序和 Traceroute 程序的机制和用法，实验内容安排了 ICMP 回显查询报文、ping 程序和 IP 选项、ICMP 重定向差错报文和 Traceroute 程序实验。第 6 章为 IP 协议和 IP 选路协议，介绍 IP 协议的特点、IP 数据报格式、路由表及选路基本原理、RIP 协议和 OSPF 协议、IP 分片与路径 MTU 发现，实验内容安排了 route 命令与静态路由、ICMP 主机和网络不可达差错、RIP 协议分析、OSPF 协议分析、IP 分片和路径 MTU 发现实验。第 7 章为 UDP 及应用协议分析，介绍 UDP 协议特点、UDP 的报文格式，基于 UDP 的应用协议 DNS、DHCP 和 SNMP 的有关概念、协议工作基本原理、报文格式和报文实例解析，实验内容安排了 DNS 协议分析、DHCP 协议分析和 SNMP 协议分析实验。第 8 章为 TCP 及应用协议分析，介绍 TCP 段格式，TCP 连接建立和拆除过程，Telnet 远程登录的工作机制和报文实例解析，HTTP 协议的工作特点、报文格式和实例解析，FTP 协议的工作原理和报文实例解析，实验内容安排了 Telnet 程序和 TCP 连接分析、HTTP 协议分析、FTP 协议分析实验。附录中给出了 Cisco 常用命令，以方便读者使用 Packet Tracer 时查阅。

根据教学时数和不同的要求，可以在本书的范围内选择相应的实验内容，以满足不同的教学需求。如 8 学时的实验可采用以太网链路层帧格式分析实验、ARP 协议分析实验、ICMP 协议分析实验、TCP 及应用协议分析实验 4 个实验组合；16 学时的实验可采用以太网链路层帧格式分析实验、ARP 协议分析实验、ICMP 协议分析实验、RIP 协议分析实验、DHCP 协议分析实验、SNMP 协议分析实验、Telnet 协议分析实验、HTTP 协议分析实验 8 个实验组合；其余的实验可以作为任选实验或者课后学生自主安排实验。SNMP 协议涉及的相关原理内容较多一些，可视学时情况安排。如果能够在实验室以讲练结合的方式使用本书进行教学，应当能用较少的学时获得较好的学习效果。

本书的所有实验全部经过在教学过程中实际上机操作，读者也可以根据自己的实验网络环境进行实验内容调整。

在清华大学出版社的网站（http://www.tup.tsinghua.edu.cn）上提供了本书的多媒体课件，读者可下载使用。本书与课件使用中的相关问题请联系 fuhy@tup.tsinghua.edu.cn。

本书由陈年主编，各章的内容尤其是实验内容是近年来在 TCP/IP 原理课程教学实践中不断地进行补充完善和总结的结果。在此，对本书的编写和出版给予支持和帮助的所有老师、同学和朋友表示衷心的感谢。

限于编者的水平，不当之处在所难免，敬请各位读者批评指正。任何意见、建议可以发至邮箱 chennian_zg@126.com。

编　者

2016 年 9 月

目 录

第1章 TCP/IP协议概述

TCP/IP起源于20世纪60年代末美国的分组交换网络项目，但其真正被广为使用是伴随着20世纪80年代Internet的诞生，如今它是计算机网络特别是Internet的基础，也是计算机网络事实上的工业标准。

TCP/IP协议是一组开放式协议，可以进行任何组合间的通信，能够满足长距离互联系统的要求。同时，其分组交换的方式使得网络中只要存在有效路由，网络通信就可以可靠进行。TCP/IP的开放是指它对异构系统是开放的。不同厂家生产的不同型号的计算机，它们运行完全不同的操作系统，使用不同的网络硬件，TCP/IP协议族也允许它们互相通信。

TCP/IP具有下列主要特点。

- 开放的协议标准，可以免费使用，并且独立于特定的计算机硬件与操作系统。
- 独立于特定的网络硬件，可以在局域网、广域网中运行，更适用于互联网。
- 统一的网络地址分配方案，使得所有TCP/IP设备在网络中都具有唯一的地址。
- 标准化的高层协议，可以提供多种可靠的用户服务。

1.1 TCP/IP协议体系结构

1.1.1 TCP/IP协议分层

TCP/IP协议实际是指一个4层的协议系统，也称为TCP/IP协议族。计算机网络基础课程中介绍的OSI/RM(Open System Interconnection Reference Model，开放系统互联参考模型)采用7层的体系结构，其与TCP/IP协议族分层情况的对应关系如图1-1所示。

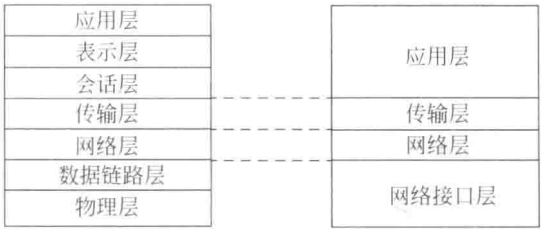

图1-1 OSI/RM与TCP/IP各层的对应关系

计算机网络中，实际应用的网络协议是TCP/IP协议族，TCP/IP的应用层大体上对应着OSI/RM模型的应用层、表示层和会话层，TCP/IP的网络接口层对应着OSI/RM的数

据链路层和物理层，而传输层和网络层在两个模型中对应得很好。

在计算机网络基础课程中已经学习过 TCP/IP 各层的具体功能，这里只对各层的功能进行简要表述，如表 1-1 所示。

表 1-1 TCP/IP 协议分层

TCP/IP 层次	主 要 协 议	主 要 功 能
应用层	HTTP、Telnet、FTP、SMTP 等	按照不同应用的特定要求和方式负责把数据传输到传输层或者接收从传输层返回的数据
传输层	TCP、UDP	TCP 为两台主机提供高可靠性的数据通信，其工作包括把应用程序交来的数据分成合适的小块交给下面的网络层，确认接收到的分组，设置发送最后确认分组的超时时钟等。UDP 则为应用层提供一种非常简单的服务，它只是把数据报的分组从一台主机发送到另一台主机但并不保证该数据报能到达另一端
网络层	IP、ICMP、IGMP	有时也称作互联网层，主要为数据包选择路由。其中，IP 是 TCP/IP 协议族中最为核心的协议。所有的 TCP、UDP、ICMP、IGMP 数据都以 IP 数据报格式传输
链路层	ARP、RARP 和设备驱动程序及接口	发送时将 IP 包作为帧发送，接收时把接收到的比特组装成帧；提供链路管理错误检测等

- 链路层有时也称作数据链路层或网络接口层，通常包括操作系统中的设备驱动程序和计算机中对应的网络接口卡。它们一起处理与电缆（或其他任何传输媒介）的物理接口细节。把链路层地址和网络层地址联系起来的协议有 ARP（Address Resolution Protocol，地址解析协议）和 RARP（Reverse Address Resolution Protocol，逆地址解析协议）。
- 网络层处理分组在网络中的活动，例如分组的选路。在 TCP/IP 协议族中，网络层协议包括 IP 协议（Internet Protocol，网际协议）、ICMP 协议（Internet Control Message Protocol，网际控制报文协议）和 IGMP 协议（Internet Group Management Protocol，网际组管理协议）。
- 传输层主要为两台主机上的应用程序提供端到端的通信。在 TCP/IP 协议族中，有两个互不相同的传输协议：TCP（Transmission Control Protocol，传输控制协议）和 UDP（User Datagram Protocol，用户数据报协议）。
- 应用层负责处理特定的应用程序细节。几乎各种不同的 TCP/IP 实现都会提供下面这些通用的应用程序：Telnet 远程登录、SMTP（Simple Mail Transfer Protocol，简单邮件传输协议）、FTP（File Transfer Protocol，文件传输协议）、HTTP（HyperText Transfer Protocol，超文本传输协议）等。

构造互联网最简单的方法是把两个或多个网络通过路由器进行连接。图 1-2 所示是一个包含两个网络的互联网：一个以太网和一个令牌环网。它们通过一个路由器连接，应用层运行 FTP 协议，传输层使用 TCP 协议。

在图 1-2 中，可以划分出端系统（end system）（两边的两台主机）和中间系统（intermediate system）（中间的路由器）。应用层和运输层使用端到端（end-to-end）协议。在图 1-2 中，只有端系统需要这两层协议。但网络层提供的是逐跳（hop-by-hop）协议，两个端系统和每个

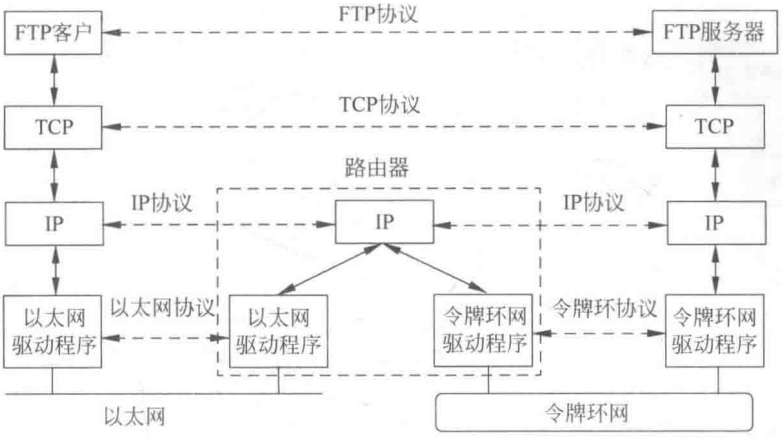

图 1-2 TCP/IP 协议的通信模型

中间系统都要使用它。

这里端到端和逐跳的概念对协议的学习、理解有特别的意义。前一个概念意味着应用层和传输层的协议主要关心的是通信的信源和信宿，也就是端系统如何通信的问题；后一个概念意味着网络层和网络接口层的协议主要关心的是下一跳，也就是相邻节点间如何通信的问题。

互联网的目的之一是在应用程序中隐藏所有的物理细节。例如，图 1-2 中的一台主机是在以太网上，而另一台主机是在令牌环网上，它们通过路由器互联。随着不同类型的物理网络的增加，会不断增加运行着各种网络接口层协议的路由器，这些路由器只解决相邻的下一跳节点间的通信问题。不论中间有多少个路由器，都不涉及应用层，所以应用层仍然是一样的。物理细节的隐藏使得互联网功能非常强大，也非常有用。

实际的系统中，应用层由用户进程实现，而传输层及以下的各层都在操作系统内核中实现。从这个意义上看，网络通信的物理细节对用户进程隐藏的特点和操作系统中讲述的设备无关性原理是一致的。

1.1.2 IP 地址和端口

互联网上参与通信的每个节点可能有不止一个网络接口，因此每一个接口都应有一个唯一的 IP 地址。同时，每个节点上都可能运行着多个通信进程，因此需要通过端口号来标识参与通信的进程。实际上，通信的主体总是进程。互联网上唯一能标识出通信的实体的方法是，用 IP 地址来区分不同节点的不同接口，用端口号来区分同一个节点上的不同进程。

需要注意的是，一个节点可以有多个网络接口，因此就有多个 IP 地址。所以 IP 地址标识的是网络接口。

IPv4 采用的是 32 位地址，其分类和点分十进制表示法在计算机网络基础课程中已经学习过，这里不再详细介绍。5 类 IP 地址的格式如图 1-3 所示。

按目的端主机的范围可将 IP 地址分为以下 3 类。

- 单播地址：目的端为单个主机。

图 1-3 5 类 IP 地址的格式

- 广播地址：目的端为给定网络上的所有主机。
- 多播地址：目的端为同一组内的所有主机。

TCP 和 UDP 采用 16 位的端口号来识别应用程序，这意味着相同的端口号对于不同的传输层协议，表示的是不同的进程。例如，TCP 端口号 23 和 UDP 端口号 23 是不同的。

服务器一般都是通过熟知端口号（又称保留端口号）来识别的，由 IANA（Internet Assigned Numbers Authority，Internet 号码分配机构）管理，目前为 1～1023。客户端口号又称为临时端口号，通常只是在用户运行该客户程序时才存在，通常为 1024～5000。从 32 768 开始的端口号通常作为 TCP 和 UDP 的默认临时端口号。也有把 1024～65 535 的端口号统称为动态端口号，即这些端口号一般不固定分配给某个服务使用。

对 UNIX 类系统来说，文件/etc/services 中包含了熟知端口号。具有超级用户（即 root 用户）权限的进程，允许分配 1～1023 之间的端口号。

1.2 封装与分用

网络通信过程中，协议栈有两个非常重要的操作：封装（发送数据时）和分用（接收数据时）。把握这两点对准确理解 TCP/IP 协议的具体工作过程十分有帮助。

1.2.1 封装

在图 1-2 所示的通信过程中，当应用程序用 TCP 传送数据时，数据被送入协议栈中，然后逐个通过每一层，直到被当作一串比特流送入网络。其中每一层对收到的数据都要增加一些首部信息（有时还要增加尾部信息），这种“加头加尾”的过程称为封装。该过程如图 1-4 所示。

TCP 传给 IP 的数据单元称为 TCP 报文段，简称为 TCP 段（TCP segment）。IP 传给网络接口层的数据单元称为 IP 数据报（IP datagram）。通过以太网传输的比特流称为帧（frame）。

更确切地说，网络接口层和 IP 层之间传送的数据单元应该是分组（packet），分组既可以是一个 IP 数据报，也可以是 IP 数据报的一个部分（分片）。

UDP 数据与 TCP 数据基本上是一致的。唯一不同的是，UDP 传给 IP 的信息单元一般称为 UDP 用户数据报，且其首部长度和 TCP 的不同。

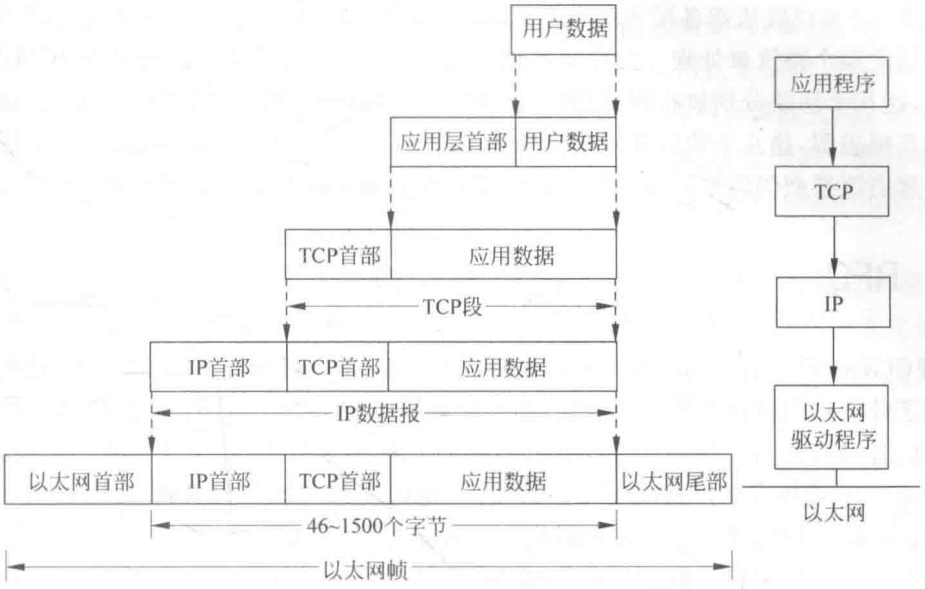

图 1-4 TCP/IP 协议数据封装过程

不同的网络接口层协议，其帧结构是不同的，使用的网络接口层帧的长度也是不一样的。一般来说，以太网协议的帧长度是 46～1500 个字节，其实是指以太网帧的数据部分的长度。网络接口层协议的帧结构将在第 3 章学习。

封装使得上一层协议数据单元的结构在本层中被隐藏，其所有的内容在本层都作为数据来传送。

1.2.2 分用

当目的主机收到一个以太网数据帧时，数据就开始从协议栈中由底向上升，同时去掉各层协议添加的报文首部。每层协议都要检查报文首部中的协议标识，以确定接收数据的上层协议。这个过程称为分用(demultiplexing)，如图 1-5 所示。

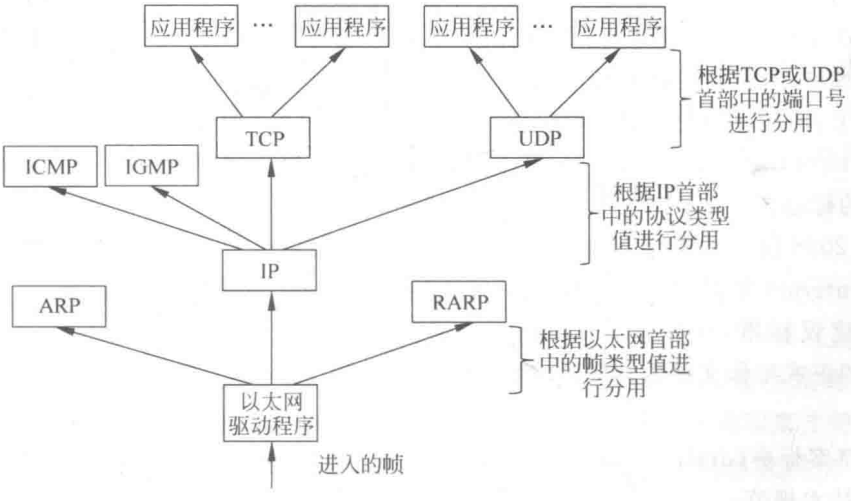

图 1-5 TCP/IP 协议数据分用过程