普通高等教育“十二五”规划教材

计算机网络实践指导教程

王　涛　裘国永　主编

科学出版社

普通高等教育“十二五”规划教材

计算机网络实践指导教程

王　涛　裘国永　主编

科学出版社
北京

内 容 简 介

本书包含网络协议分析和套接字编程实践两部分，其中网络协议分析围绕计算机网络中 HTTP、DNS、DHCP、TCP、UDP、IP、ICMP、NAT、Ethernet、ARP、802.11 等协议展开，设计编写了 11 套 Wireshark 协议分析实验，带领读者通过分析报文格式和运行中的协议交互过程，深入了解网络协议的设计和工作原理。套接字编程实践以 TCP 和 UDP 套接字编程为基础，设计编写了 9 个编程实验，由浅入深、由易到难地覆盖了 Web 服务器、邮件客户端、Web 代理、可靠传输、路由算法以及多媒体点播等内容，涉及网络体系结构的多个层次。代码实现利用 JAVA 语言和 C 语言两大主流工具，带领读者了解、熟悉、精通套接字编程方法。

本书可作为高等院校本科生和研究生计算机网络实践课的教材，也可以作为科研和工程技术人员的参考资料。

图书在版编目(CIP)数据

计算机网络实践指导教程/王涛，裘国永主编．—北京：科学出版社，2015.9

普通高等教育“十二五”规划教材

ISBN 978-7-03-045890-2

Ⅰ.①计… Ⅱ.①王… ②裘… Ⅲ.①计算机网络-高等学校-教材 Ⅳ.①TP393

中国版本图书馆 CIP 数据核字(2015)第 234411 号

责任编辑：李 萍 杨向萍 纪四稳/责任校对：钟 洋

责任印制：赵 博/封面设计：红叶图文

科学出版社 出版

北京东黄城根北街 16 号

邮政编码：100717

http://www.sciencep.com

源海印刷厂印刷

科学出版社发行 各地新华书店经销

*

2015 年 10 月第 一 版 开本：720×1000 1/16

2015 年 10 月第一次印刷 印张：15 1/2

字数：310 000

定价：58.00 元

（如有印装质量问题，我社负责调换）

前　言

计算机网络对于相关专业的从业人员是必备知识。尤其在当今“互联网＋”的大背景下，互联网思维已经深入人心，如何更好地利用计算机网络的相关知识去解决实际问题是学习这门学科最主要的任务。然而，计算机网络是一门内容复杂的学科，涉及纷繁复杂的概念、协议和技术，同时还具备很强的实践性，因此仅凭理论学习是不足以深入了解网络协议背后的设计和工作原理的，更谈不上去设计和开发一个网络应用程序。

作者从2006年开始从事计算机网络和网络工程等课程的教学工作，经过多年的积累形成了本书协议分析和套接字编程的讲义和素材，并已在多年的内部教学使用过程中得到了检验。因此，给计算机网络的学习者提供实践指导，并对作者多年的教学实践工作进行总结正是编写本书的初衷。

本书分为两部分。第一部分是网络协议分析部分，以TCP/IP体系为线索，自顶向下地由应用层到运输层，再到网络层和数据链路层，针对最常见的一些协议如HTTP、DNS、DHCP、TCP、UDP、IP、ICMP、NAT、Ethernet、ARP、802.11等展开分析，并以Wireshark为主要工具提供实验设计和指导。带领读者通过分析协议报文格式和运行中的交互过程，深入了解网络协议的设计和工作原理。内容包括：第1章协议分析工具，第2章应用层典型协议分析，第3章运输层典型协议分析，第4章网络层典型协议分析，第5章数据链路层和局域网典型协议分析。

第二部分以Kurose等编写的国际著名教材 *Computer Networking: A Top-Down Approach* 第6版提供的编程作业为线索，利用JAVA语言和C语言两大主流工具设计9个编程实验，内容覆盖Web服务器、邮件客户端、Web代理、可靠传输、路由算法以及多媒体点播等。带领读者了解、熟悉、精通套接字编程方法。内容包括：第6章TCP和UDP套接字编程，第7章多线程Web服务器，第8章邮件客户端，第9章邮件用户代理：控制台版本，第10章用UDP实现ping功能，第11章Web代理服务器，第12章实现一个可靠传输协议，第13章一个分布式异步距离向量算法，第14章RTSP和RTP实现流媒体点播系统。

书中的理论内容由王涛、裘国永、吴振强等负责编写。第1、3章实验由秦石醉负责编写；第2、4、5章实验由张阳阳负责编写；第6～14章实验由张阳阳、秦石醉、王涛负责编写。同时感谢张夏蕾、黄亚军等在套接字编程部分源代

码实现等方面的工作。全书由王涛负责设计、规划、统稿。本书相关电子资源可参考 http：//netresearch. snnu. edu. cn。

本书的编写得到了陕西师范大学计算机科学学院的大力支持，得到了王小明、马苗等许多同事的指导和支持，也得到了陕西师范大学校级优秀教材出版项目以及陕西师范大学基地班、创新实验班专项建设项目的资助，作者在此一并表示衷心的感谢！

教材编写是在不断的教学实践中摸索总结出来的，由于作者水平有限，书中难免有一些不足之处，恳请读者多提宝贵意见，给予批评指正，不胜感激！

作　者

2015 年 7 月于西安

目　录

第二部分　套接字编程实践

第一部分

网络协议分析

第 1 章　协议分析工具

1.1　协议分析及工具

1.1.1　协议分析概述

在协议分析实验中，需要借助协议分析软件对数据进行抓包观察和分析。观察正在执行协议的两个实体间报文交互的基本工具称为分组嗅探器，一个分组嗅探器俘获（嗅探）计算机发送和接收的报文。一般情况下，分组嗅探器将存储和显示出被俘获报文的各协议首部字段的内容，它的作用相当于对报文和协议进行复制以便分析。

图 1-1 显示了分组嗅探器的结构。右侧是协议和应用程序，协议分为 5 层，自上而下分别是应用层、运输层、网络层、数据链路层和物理层，在数据链路层帧中包含了以上所有协议层的报文。左侧数据分组抓包（嗅探）器分为两部分：分组分析和分组抓包。分组分析器在协议下方显示了该协议所有的字段，分组抓包在其抓包库中存储了计算机发送和接收数据链路层帧副本。

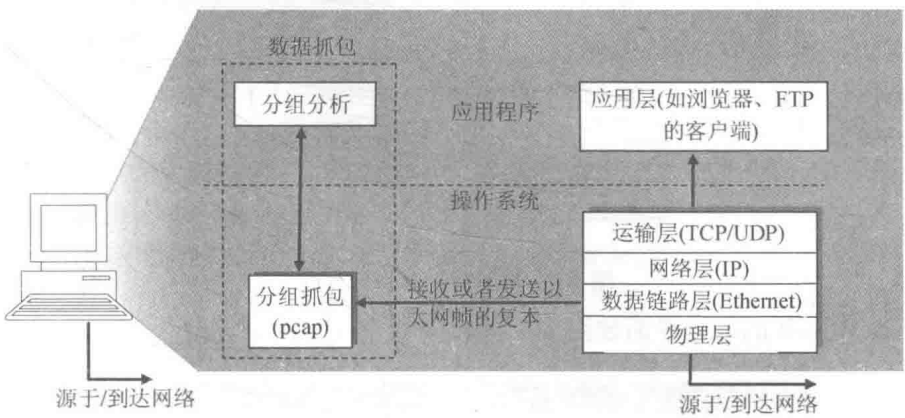

图 1-1　分组嗅探器的结构

1.1.2　协议分析工具

为了深入地理解网络协议，观察运行中的协议行为以及分析协议的交互过程是最好的途径。通过对协议使用实体间交互报文序列的观察，研究协议操作细节并且使用协议执行确切的操作及分析其结果。为此，需要利用协议分析工具进行

协议分析实验。

目前常见的网络数据抓包工具有 Wireshark、FireFox 里面的 HttpFox、Internet Explorer 里面的 HttpWatch、Fiddler2 和 SmartSniff 等。

HttpFox 的运行界面如图 1-2 所示。

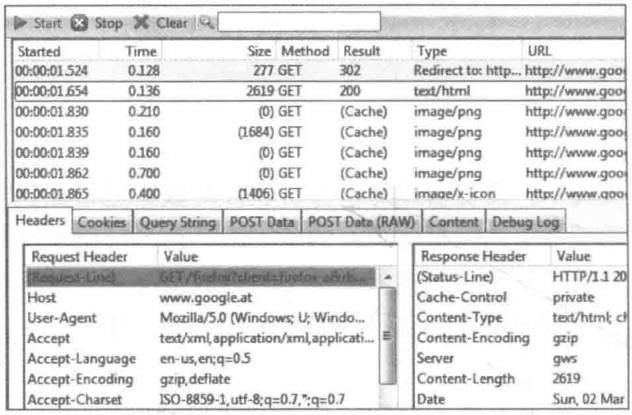

图 1-2 HttpFox 运行界面

HttpWatch 运行界面如图 1-3 所示。

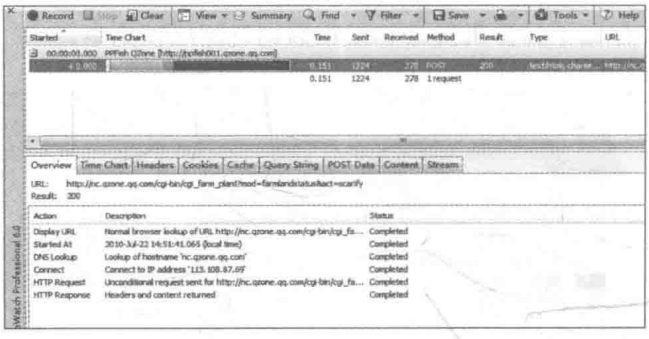

图 1-3 HttpWatch 运行界面

SmartSniff 的运行界面如图 1-4 所示。

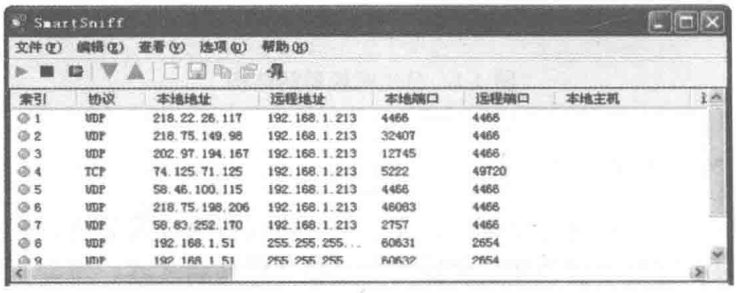

图 1-4 SmartSniff 运行界面

Wireshark 运行界面如图 1-5 所示。

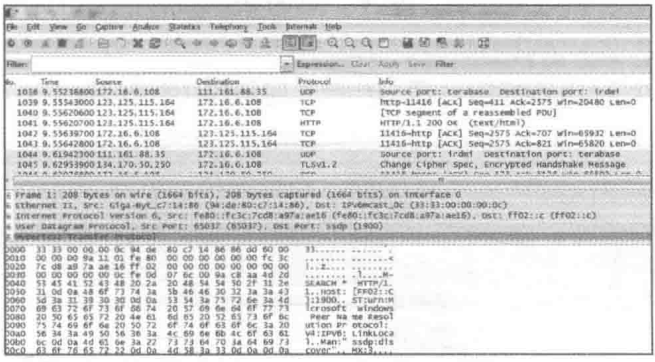

图 1-5　Wireshark 运行界面

其中，Wireshark 是免费软件，运行稳定，是目前最主流的开源网络分析软件，成为本书协议分析实验的首选。下面对 Wireshark 软件的发展历史进行简单介绍。

1.1.3　Wireshark 发展历史

1997 年年底，Combs 需要一个能够追踪网络流量的工具软件作为其工作上的辅助。因此，他开始编写 Ethereal 软件。Ethereal 在经过几次中断开发的事件过后，终于在 1998 年 7 月发布了第一个版本 V0.2.0。自此之后，Combs 收到了来自世界各地的修补程序、错误回报与鼓励信件。Ethereal 的发展就此开始。不久之后，Ramirez 看到了这套软件的开发潜力并开始参与开发。1998 年 10 月，来自 Network Appliance 公司的 Harris 在寻找一套比 TCPView（另外一个分组嗅探）更好的软件。于是，他也开始参与 Ethereal 的开发工作。1998 年底，一位教授 TCP/IP 课程的讲师 Sharpe 看到了这套软件的发展潜力，而后开始参与开发与加入新协议的功能。在当时，新的通信协议的制订并不复杂，因此他开始在 Ethereal 上新增分组嗅探功能，几乎包含了当时所有通信协议。

自此之后，数以千计的人开始参与 Ethereal 的开发，2006 年 6 月，因为商标的问题，Ethereal 更名为 Wireshark。

1.2　下载 Wireshark

为了进行 Wireshark 实验，需要下载 Wireshark 软件以及 libpcap 或者 WinPCap 分组抓包库。可访问 http：//www.Wireshark.org/download.html 选择支持的操作系统以便下载。

Wireshark 的 FAQ 有大量的有用的提示，尤其是在安装软件过程中遇到问题也可以在其中找到答案。

1.3 运行 Wireshark

当运行 Wireshark 程序时，进入开始界面如图 1-6 所示。

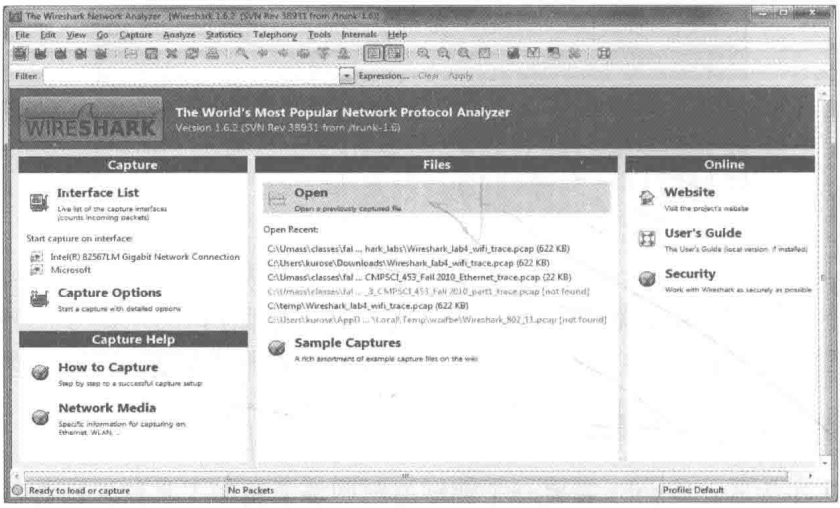

图 1-6 初始的 Wireshark 界面

观察界面左上角将会看到“接口列表”（Interface List），这是使用者计算机上网络接口的列表，一旦选择一个接口，软件将抓取该接口所有的数据分组。选中一个接口并开始数据抓包，屏幕将显示如图 1-7 所示信息，在 Capture 的下拉菜单可以选择停止数据抓包。

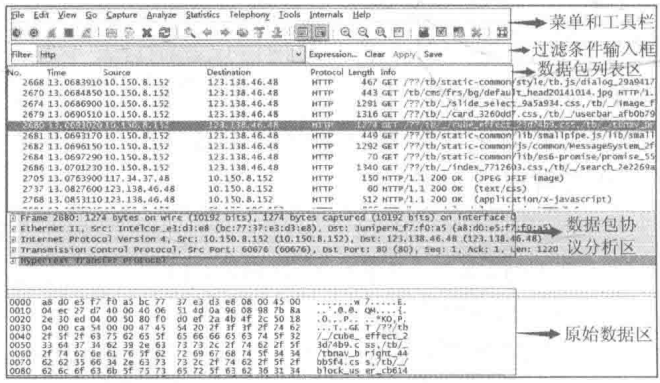

图 1-7 Wireshark 用户界面数据抓包分析

Wireshark 界面有 5 个主要部分。

(1) 菜单和工具栏。在窗口顶部，有标准的下拉菜单。主要关注 File 和 Cap-

ture菜单。File菜单有允许存取数据分组以及打开之前抓取的分组数据，以及退出应用程序等功能。Capture菜单有执行开始数据抓包等功能。

(2) 过滤条件输入框。在此可以使用多种表达式进行筛选和过滤。

(3) 数据包列表区。该区域是每一个抓取到数据分组的摘要信息，包括分组包的序号（由Wireshark分配）、分组抓取的时间、分组的源地址和目的地址、协议类型以及在分组中的特定协议信息。分组列表可以通过单击列名进行排序。协议类型显示的是发送或者接收该协议的最上层协议。

(4) 数据包协议分析区。提供了选定分组的详细信息，这些详细信息包括以太帧（假定数据分组是通过以太网发送或者接收的）和IP数据报。以太帧和IP层可以通过单击前面的“+”展开或者“-”收起。如果分组通过TCP或者UDP运输，TCP或UDP详情也会显示。在该窗口默认显示选定分组的最上层协议。

(5) 原始数据区。显示的是捕获分组的原始二进制信息，包括左边的十六进制格式以及右边的ASCII码格式。

1.4　Wireshark过滤条件表达式

1.4.1　针对IP地址的过滤

Wireshark最常用的是针对IP地址的过滤，其中有以下几种情况。

(1) 对源地址过滤。例如，对源地址为192.168.0.1的包的过滤，即抓取源地址满足要求的包，表达式为ip.src == 192.168.0.1。

(2) 对目的地址过滤。例如，对目的地址为192.168.0.1的包的过滤，即抓取目的地址满足要求的包，表达式为ip.dst == 192.168.0.1。

(3) 对源或者目的地址过滤。例如，对源或者目的地址过滤为192.168.0.1的包的过滤，即抓取满足源或者目的地址的IP地址是192.168.0.1的包，表达式为ip.addr == 192.168.0.1，或者ip.src == 192.168.0.1 or ip.dst == 192.168.0.1。

(4) 要排除以上的数据包，只需要将其用括号囊括，然后使用“!”即可。表达式为!。

1.4.2　针对协议的过滤

(1) 仅仅需要捕获某种协议的数据包，表达式仅需要把协议的名字输入即可，如表达式为http。

(2) 需要捕获多种协议的数据包，也只需对协议进行逻辑组合即可，如表达式为http or telnet（多种协议加上逻辑符号的组合即可）。

(3) 排除某种协议的数据包。表达式用“!”表示，如表达式为not arp、!tcp等。

1.4.3 针对端口的过滤（视协议而定）

（1）捕获某一端口的数据包，表达式为 tcp. port == 端口号，如 tcp. port == 80。

（2）捕获多端口的数据包，可以使用 and 来连接，下面是捕获高端口的表达式，表达式为 udp. port>=端口号，如 udp. port>= 2048。

1.4.4 针对长度和内容的过滤

（1）针对长度的过滤（长度指定的是数据段的长度），表达式为协议报文长度＋“关系算符”＋长度值，如 udp. length< 30、http. content _ length<=20。

（2）针对数据包内容的过滤，如表达式为 http. request. uri matches “vipscu”（匹配 http 请求中含有 vipscu 字段的请求信息）。

1.5 使用 Wireshark 进行测试

假定计算机通过有线以太网连接到网络，按如下步骤抓包。

（1）打开浏览器，将会显示选择的主页。

（2）打开 Wireshark 软件，将看到如图 1-6 所示的初始窗口，此时软件还没有进行数据抓包。

（3）在 Capture 下拉菜单选择接口 interface，会显示窗口：“Wireshark：Capture Interfaces”，如图 1-8 所示。

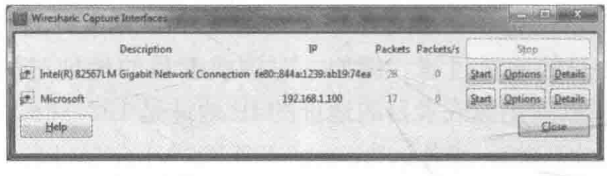

图 1-8 选择抓包接口对话框

（4）单击 Start，软件开始数据抓包，它将记录该接口所有接收和发送的数据分组。在软件运行时，在浏览器地址栏输入 www. snnu. edu. cn，按回车键运行，当跳到指定页面时选择停止数据抓包。Wireshark 软件记录了从开始以后在选定的接口中，到按 Stop，所有的接收和发送的数据分组。

（5）在协议过滤框输入 http、dns 或者其他信息，以便选择需要的信息进行选择和分析。

（6）退出 Wireshark。

在对数据抓包工具 Wireshark 及其简单的操作方法做了初步了解后，下面就可以开始本书的实验。

第 2 章　应用层典型协议分析

应用层协议定义了网络应用程序进程之间的通信规范。每个应用层协议都是为了解决某一类应用问题而出现的，例如，用于 WWW 应用的 HTTP 协议、用于文件传输的 FTP 协议、用于邮件传输的 SMTP 协议以及实现域名解析服务的 DNS 协议等。

本章首先将介绍网络应用程序的工作模式，接着重点对应用层中的 HTTP、DNS 以及 DHCP 等协议进行分析。

2.1　网络应用程序的工作模式

2.1.1　客户/服务器模式

在互联网中，最主要的进程间交互的方式是客户/服务器模式，即 Client/Server，简称 C/S 模式。在客户/服务器体系结构中，有一个（或多个）总是开机且在线的主机称为服务器，它服务于来自许多其他称为客户机的主机请求。客户机主机可能有时打开，也可能总是打开。一个典型的例子是 Web 应用程序，其中总是打开的 Web 服务器为来自运行在客户机上的浏览器的请求提供服务。在这里需要注意的是，C/S 模式中的客户机之间不直接通信。例如，在 Web 应用中，两个浏览器之间并不直接通信。C/S 体系结构的另一个特征是服务器有固定的、周知的地址，称为 IP 地址。因为服务器具有固定的、周知的地址，并且总是处于打开的状态，所以客户机总是能够向该服务器的地址发送分组来与其联系。图 2-1 显示了这种 C/S 体系结构。

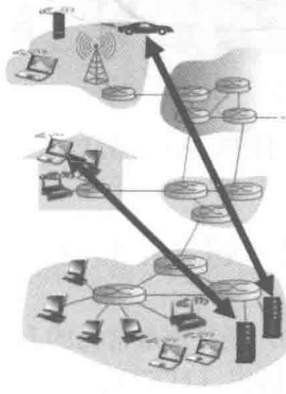

图 2-1　网络应用程序的 C/S 体系结构