21 高等学校信息工程类“十二五”规划教材

计算机网络原理与技术实验教程

史长琼 姜腊林
廖年冬 熊 兵 编著◎

JISUANJI WANGLUO YUANLI YU JISHU SHIYAN JIAOCHENG

西安电子科技大学出版社
http://www.xduph.com

高等学校信息工程类“十二五”规划教材

计算机网络原理与技术实验教程

史长琼　姜腊林　廖年冬　熊兵　编著

西安电子科技大学出版社

内 容 简 介

本书根据高等院校不同专业的教学要求，从提高动手实践能力的角度出发，系统地介绍了网络协议分析、网络原理综合设计、网络安全编程以及无线局域网实验等内容，涵盖了 Windows 常用网络操作命令和工具、协议分析方法和工具以及 Socket 编程，着重设计了 TCP/IP 各层协议的观察和编程开发实验，以及网络安全编程实验，使学生能够更深刻理解计算机网络原理，熟练掌握网络编程技术，增强动手实践能力。

本书可作为高等院校相关专业“计算机网络”、“网络协议编程”、“网络安全”、“无线网络技术”等课程的实验辅助教材，同时还可作为相关课程的课程设计的辅助教材，也可作为计算机网络工程技术人员的参考书。

图书在版编目(CIP)数据

计算机网络原理与技术实验教程/史长琼等编著. —西安：西安电子科技大学出版社，2015.1
高等学校信息工程类“十二五”规划教材
ISBN 978-7-5606-3572-9

Ⅰ. ① 计… Ⅱ. ① 史… Ⅲ. ① 计算机网络—高等学校—教材
Ⅳ. ① TP393

中国版本图书馆 CIP 数据核字(2014)第 298020 号

策　　划　马晓娟
责任编辑　马晓娟　王　朋
出版发行　西安电子科技大学出版社（西安市太白南路 2 号）
电　　话　(029)88242885　88201467　邮　　编　710071
网　　址　www.xduph.com　　电子邮箱　xdupfxb001@163.com
经　　销　新华书店
印刷单位　陕西天意印务有限责任公司
版　　次　2015 年 1 月第 1 版　2015 年 1 月第 1 次印刷
开　　本　787 毫米×1092 毫米　1/16　印张 7
字　　数　161 千字
印　　数　1～3000 册
定　　价　15.00 元

ISBN 978 – 7 – 5606 – 3572 – 9 / TP
XDUP 3864001-1

前　言

计算机网络是支撑现代经济发展和科技创新的信息基础设施，计算机网络课程也已成为国内外高等院校不同专业广泛开设的课程。掌握计算机网络原理与技术通常需要经历理论学习、观察思考及编程实践等几个阶段。通过课堂教学和资料阅读了解网络基本原理，这是理论学习阶段；通过网络协议观察实验，进一步思考和理解协议的特点，这是观察思考阶段；根据具体功能需求，编程实现具体的协议功能，这是编程实践阶段。经过这三个阶段的学习，能使学生更深刻地理解计算机网络原理，熟练掌握网络编程技术，增强动手实践能力及创新能力。因此，网络实验是学习计算机网络原理不可或缺的重要环节。

本书在简要介绍主要的 TCP/IP 协议原理的基础上，重点讲述了怎样对这些协议进行观察与思考；阐述了编程模拟具体协议功能的基本方法；讲解了基于 TCP/IP 协议实现网络安全功能的基本方法。本书设计的实验对实验环境要求低，便于实施，即以 Windows 为操作系统平台，Wireshark 为网络协议分析工具，Socket 为网络应用编程接口，不需要大量的网络设备和复杂的网络环境。

全书分为四章。第 1 章简要介绍了 Wireshark 协议分析工具的使用方法，然后按照分层模型，自底向上安排了 11 个协议的配置观察实验，并且根据需要介绍了 Windows 操作系统常用网络命令的使用方法和常用实验工具的配置方法。第 2 章先简要介绍了 Socket 编程的一般方法，然后设计了 6 个编程实验，阐述怎样编程模拟协议功能。第 3 章安排了 6 个编程实验，阐述怎样编程实现网络安全功能，比如加密、流量统计、扫描端口、网络嗅探等。第 4 章先简要介绍无线局域网技术，然后设置了 3 个无线局域网配置实验，介绍了无线局域网的配置方法。

本书可以作为高等院校相关专业“计算机网络”、“网络协议编程”、“网络安全”、“无线网络技术”等课程的实验辅助教材，同时还可以作为相关课程的课程设计的辅助教材，也可以作为计算机网络工程技术人员的参考书。本书第 1 章思考题的参考答案及第 2 章、第 3 章的参考源程序代码，授课老师可向出版社或作者索取。

本书由史长琼、姜腊林、廖年冬和熊兵共同编写，由史长琼、姜腊林完成全书统稿。在编写过程中，吴佳英、龙际珍和向玲云等参与了实验设计和代码编写。本书是作者多年教学实践工作的总结，同时作者将从网络上收集的一些实验实例进行了加工、修改后也纳入书中，在此向实验原创者表示衷心的感谢。

计算机网络技术发展迅速，限于作者的学识，本书难免有不妥之处，恳请读者来信批评指正，作者将万分感谢。作者联系方式：shi.changqiong@163.com。

作　者

2014 年 7 月

目　录

第 1 章　网络协议分析 1

1.1　网络协议分析器 Wireshark 1

1.2　以太网链路层帧格式分析实验 7

1.3　ARP 协议分析实验 9

1.4　IP 协议分析实验 13

1.5　IP 分组分片实验 15

1.6　ICMP 协议分析实验 17

1.7　UDP 协议分析实验 22

1.8　TCP 协议分析实验 25

1.9　FTP 协议分析实验 30

1.10　DNS 协议分析实验 36

1.11　HTTP 协议分析实验 43

1.12　电子邮件相关协议分析实验 46

第 2 章　网络原理综合设计 54

2.1　Socket 与网络编程基础知识 54

2.2　以太网帧的封装与发送 63

2.3　PING 程序设计与实现 66

2.4　本地计算机网络信息的获取 71

2.5　IP 分组转发的模拟 74

2.6　滑动窗口协议的模拟 76

2.7　简单聊天程序的设计与实现 80

第 3 章　网络安全编程 82

3.1　DES 算法的实现 82

3.2　RSA 算法的原理与实现 87

3.3　简单端口扫描器的设计与实现 88

3.4　活动主机探测工具的设计与实现 90

3.5　简单网络嗅探器的设计与实现 92

3.6　网络流量统计工具的设计与实现 94

第 4 章　无线局域网实验 96

4.1　无线局域网基础知识 96

4.2　Ad-Hoc 无线局域网配置 98

4.3　Infrastructure 无线网络配置 101

4.4　MAC 地址过滤 104

第 1 章　网络协议分析

TCP/IP 协议栈分为四层(如图 1-1 所示)，从下往上依次为网络接口层、网际层、传输层和应用层，实际上网络接口层没有专门的协议，它使用连接在 Internet 网上的各通信子网本身所固有的协议，如以太网的 802.3 协议等。本章主要对网络接口层的以太网的 802.3 协议，网际层的 IP 协议、ARP 协议及 ICMP 协议，传输层的 TCP 协议和 UDP 协议，应用层的 FTP 协议、DNS 协议、HTTP 协议等 TCP/IP 的核心协议进行分析。

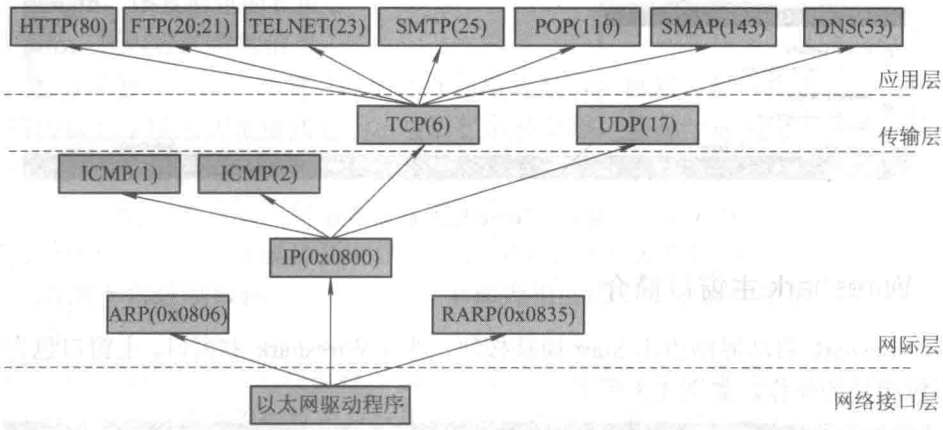

图 1-1　TCP/IP 协议簇

本章实验的基本思路是使用协议分析工具从网络中截获数据报，对截获的数据报进行分析。通过实验，使学生了解计算机网络中数据传输的基本原理，进一步理解计算机网络协议的层次结构、协议的结构、主要功能和工作原理，以及协议之间是如何相互配合来完成数据通信功能的。

Windows 环境下常用的协议分析工具有：Sniffer Pro、Netxray、Iris、Wireshark 以及 Microsoft Network Monitor 等。本书选用 Wireshark 作为协议分析工具，并在 Windows XP 环境下进行协议分析。

1.1　网络协议分析器 Wireshark

网络协议分析器 Wireshark 是目前最好的、开放源码的、获得广泛应用的网络协议分析器，支持 Linux 和 Windows 平台。Wireshark 1.12.0 版本整合了 Winpcap 4.1.3。本章以 Wireshark 1.12.0 版本为依据，介绍用 Wireshark 进行协议分析的方法。

Wireshark 的安装比较简单，下载完 Wireshark 即可进行安装。运行 Wireshark 后首先进入如图 1-2 所示的 Wireshark 启动界面。

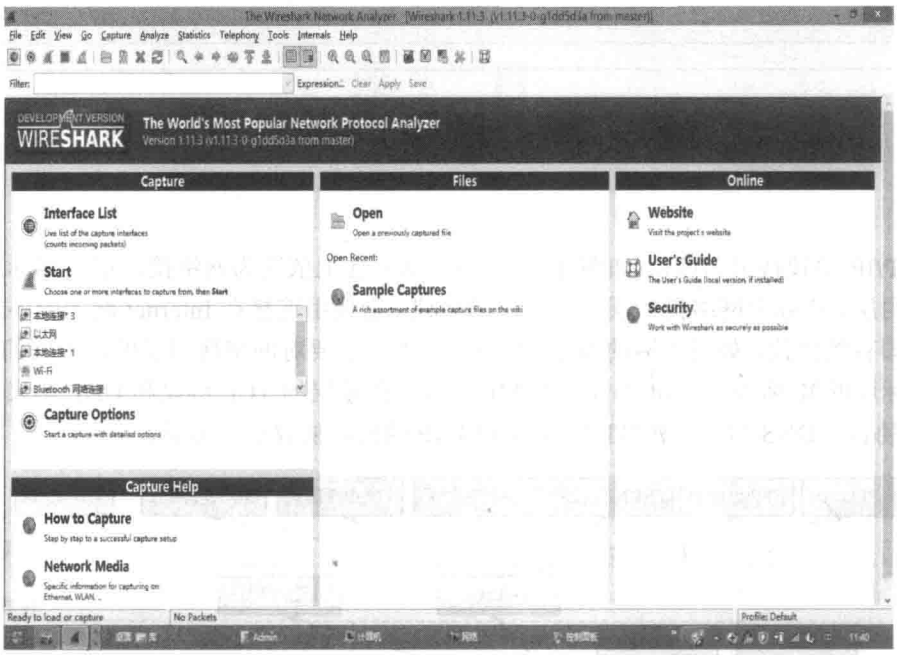

图 1-2　Wireshark 启动界面

1.1.1　Wireshark 主窗口简介

在 Wireshark 启动界面点击 Start 捕获按钮，进入 Wireshark 主窗口。主窗口包含了捕获和分析包相关的操作，如图 1-3 所示。

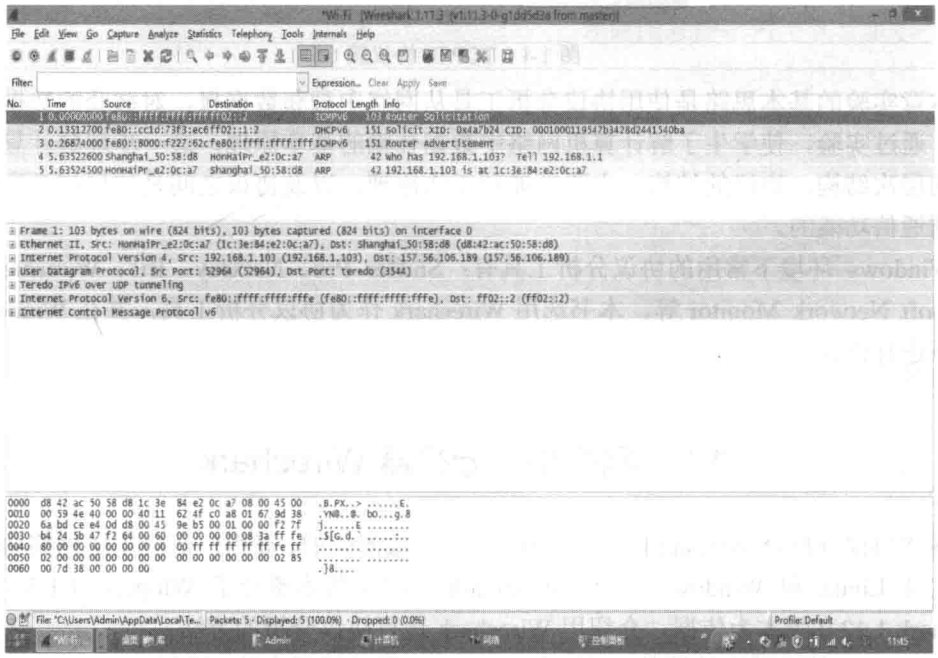

图 1-3　Wireshark 捕获数据包后的主窗口

(1) 菜单栏。菜单栏通常用来启动 Wireshark 有关操作，例如 File、Edit、Capture 等。

(2) 工具栏。工具栏提供菜单中常用项目的快速访问。

(3) 过滤器栏。过滤器栏提供一个路径，来直接控制当前所用的显示过滤器。

(4) 包列表窗口。包列表窗口显示当前捕获的全部包的摘要。包列表的每一行对应一个包，不同包有不同的颜色。如果选择了某行，则更详细的信息显示在包协议窗口和包字节数据窗口中。在包列表窗格中的每一行代表捕获的一个包，每个包的摘要信息包括：

① No：包文件中包的编号。

② Time：包的时间戳，即捕获该包的时间，该时间戳的实际格式可以改变。

③ Source：包的源地址。

④ Destination：包的目标地址。

⑤ Protocol：包协议的缩写。

⑥ Length：该数据包的长度。

⑦ Info：包内容的附加信息。

(5) 包协议窗口。包协议窗口以更详细的格式显示从包列表窗口选中的协议和协议字段。包的协议和字段用树型格式显示，可以扩展和收缩。这是一种可用的上下文菜单，单击每行前的“+”就可以展开为以“-”开头的若干行，单击“-”又可以收缩。

(6) 包字节窗口(十六进制数据窗口)。包字节窗口以十六进制形式显示出从包列表窗格中选定的当前包的数据，并以高亮度显示在包协议窗口中选择的字段。在常用的十六进制区内，左边的十六进制数据表示偏移量，中部为相应的十六进制包数据，右边为对应的 ASCII 字符。

(7) 状态栏。状态栏显示当前程序状态和捕获数据的信息。通常其左边显示相关信息的状态，右边显示捕获包的数目及百分比和丢弃包的数目及百分比。

1.1.2　Wireshark 捕获数据包的过程

使用 Wireshark 捕获数据包的一般过程为：

(1) 启动 Wireshark。

(2) 开始分组捕获。单击工具栏的◉按钮，出现如图 1-4 所示对话框，可以进行系统参数设置。在绝大部分实验中，使用系统的默认设置即可，接口卡默认工作方式为混杂模式。当计算机具有多个网卡时，需选择发送或接收分组的网络接口卡。单击“Start”按钮开始进行分组捕获。

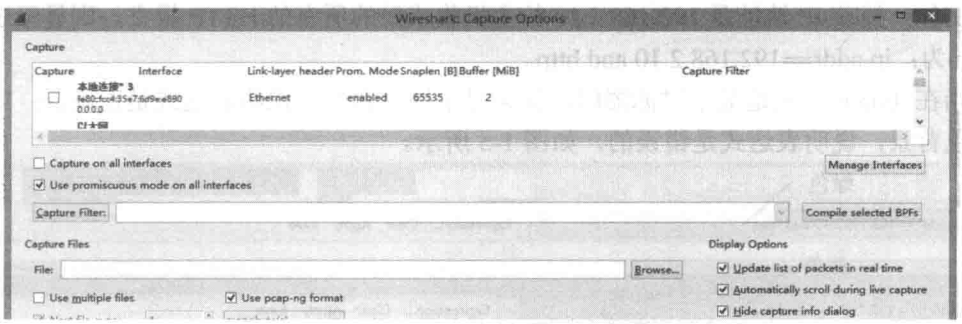

图 1-4　Wireshark 配置界面

(3) 单击捕获对话框中的“Stop”按钮，停止分组捕获。此时，Wireshark 主窗口显示已捕获的局域网内的所有协议报文。

(4) 可以筛选具体的协议。例如，如果要筛选的协议为 http 协议，只需要在协议筛选框中输入“http”，单击“Apply”按钮，分组列表窗口将只显示 HTTP 协议报文。这样就可以捕获所需要的数据包，并可以借助 Wireshark 提供的功能进行具体的网络数据包的分析了。

1.1.3 用 Wireshark 分析协议的一般过程

如前所述，Wireshark 抓包后的界面有三个部分。上部为包列表窗口，显示的是对捕获到的每个数据包进行分析后的总结型信息，包括编号、时间、源地址、目标地址、协议、协议长度、信息。中部为包协议窗口，显示的是数据包的协议信息。在包列表窗口选择不同条目，则包协议窗口的内容随之改变为相应的协议信息。下部为十六进制数据窗口，可以显示报文在物理层的数据形式。

在抓包完成后，可以利用显示过滤器找到感兴趣的包，也可根据协议、是否存在某个域、域值、域值之间的关系来查找感兴趣的包。

1. Wireshark 的显示过滤器

可以使用表 1.1 所示的操作符来构造显示过滤器。

表 1.1 操 作 符

英文名称	运算符	中文名称	应用举例
eq	==	等于	ip.addr==10.1.10.20
ne	!=	不等于	ip.addr!=10.1.10.20
gt	>	大于	frame.pkt_len>10
lt	<	小于	frame.pkt_len<10
ge	>=	大于等于	frame.pkt_len>=10
le	<=	小于等于	frame.pkt_len<=10

也可以使用下面的逻辑操作符将表达式组合起来：

逻辑与 and(&&)：如 ip.addr==10.1.10.20&&tcp.flag.fin；

逻辑或 or(||)：如 ip.addr==10.1.10.20||ip.addr==10.10.21.1；

异或 xor(^^)：如 ip.addr==10.1.10.20 xor ip.addr==10.10.21.1；

逻辑非！：如!llc。

例如：捕获 IP 地址是 192.168.2.10 的主机收或发的所有的 HTTP 报文，则显示过滤器(Filter)为：ip.addr==192.168.2.10 and http。

当在 Filter 中构造显示过滤器时，如果显示绿色背景，说明表达式是正确的；如果显示红色背景，说明表达式是错误的，如图 1-5 所示。

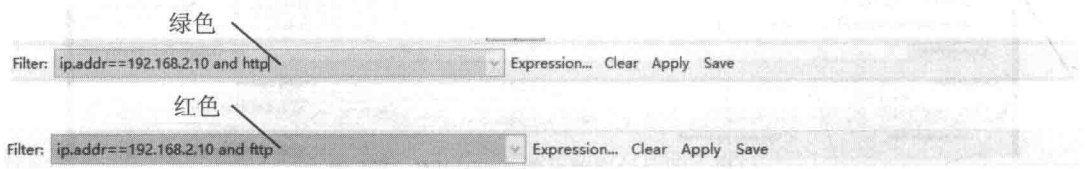

图 1-5 组合过滤器设置

2. 实例分析

下面的分析示例是通过上网查询“Wireshark”，然后运行 Wireshark 抓包。

按照 1.1.2 节所叙述抓包过程：单击 Capture→按默认过滤器→Start→抓包若干分钟→Stop，获得图 1-6 的结果。

图 1-6　上网查询抓包结果

由于 Wireshark 已经对抓包结果做了分析，所以通过协议窗口可以获得 IP 协议数据报格式和 TCP 协议报文格式的具体数据。在图 1-6 中，各个窗口都可以用拖拉方法拉大或缩小，可以与十六进制窗口相结合，清楚地看到各个字段的数据。

最初协议窗口显示了协议信息，单击第一条信息，则十六进制窗口中对应的信息变为蓝底白字，如图 1-7 所示。

图 1-7　单击第一条信息 114 432 字节改变颜色

每条信息头部有一个“＋”号，单击“＋”则变为“－”，具体的协议信息即展开并显示在协议窗口内。图 1-8 所示为 IP 协议展开的内容。

由图 1-8 可见，IP 协议源地址为 192.168.1.103，目标地址为 123.125.115.164，版本为 IPV4，报头长度为 20 字节。对应的十六进制数据为 45 00 00 28 2f 60 40 00 40 06 5a 3f c0 a8 01 67 7b 7d 73 a4。协议窗口中还有 3 个带“＋”的信息行，将 Differentiated Services Field(不同的服务字段)、标志行(Flags)和报头校验和行展开，则可以看到具体字段的数据。

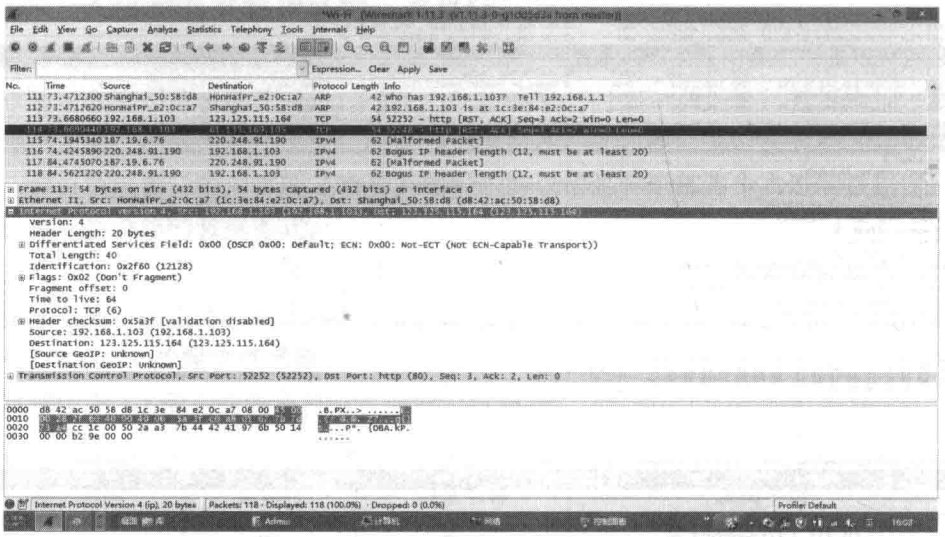

图 1-8　单击 IP 协议的展开图

图 1-9 为 TCP 协议的展开图，由图可见源端口号为 52252，对应的十六进制数据为 cc1c，目标端口号为 http(80)，顺序号为 3，确认号为 2，报头长 20 字节，还可以看到保留位和 6 个控制位的设置情况等。

从上面的例子可知 Wireshark 已经对抓包结果做了准确的分析。

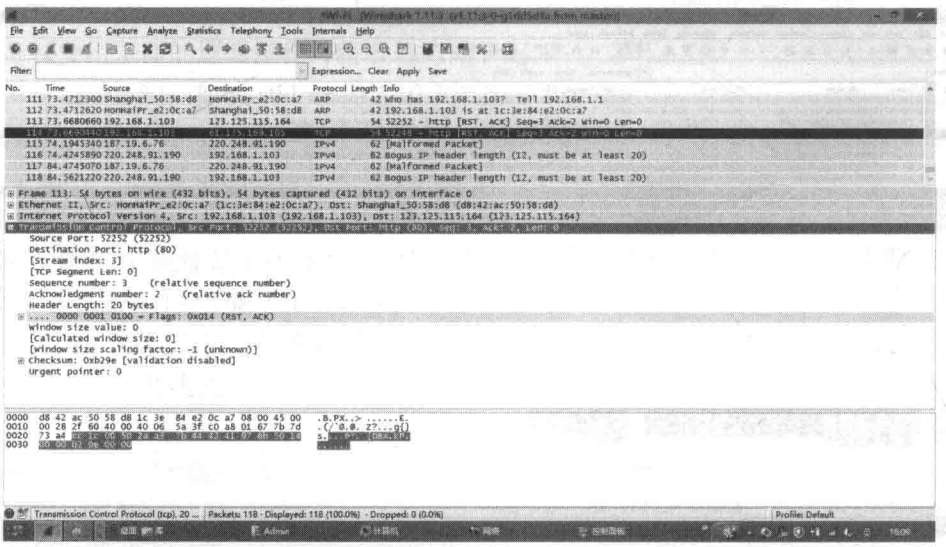

图 1-9　TCP 协议的展开图

1.2　以太网链路层帧格式分析实验

1.2.1　以太网简介

IEEE 802 参考模型把数据链路层分为逻辑链路控制子层(Logical Link Control，LLC)和介质访问控制子层(Media Access Control，MAC)。与各种传输介质有关的控制问题都放在 MAC 子层，而与传输介质无关的问题都放在 LLC 子层。因此，局域网对 LLC 子层是透明的，只有具体到 MAC 子层才能发现所连接的是什么标准的局域网。

IEEE 802.3 是一种基带总线局域网，最初是由美国施乐(Xerox)公司于 1975 年研制成功的，并以在历史上表示电磁波传播介质的“以太”来命名。1981 年，施乐公司、数字设备公司(Digital)和英特尔(Intel)联合提出了以太网的规约，1982 年修改为第二版，即 DIX Ethernet V2，该规约是世界上第一个局域网产品的规范，也是后来的 IEEE 802.3 标准的基础。

在 802.3 中使用 1- 坚持的 CSMA/CD(Carrier Sense Multiple Access with Collision Detection)协议。现在流行的以太网的 MAC 子层的帧结构有两种标准，一种是 802.3 标准，另一种是 DIX Ethernet V2 标准。图 1-10 画出了两种标准的 MAC 帧结构。它们都由五个字段组成。MAC 帧的前两个字段分别是目的地址字段和源地址字段，长度是 2 或 6 字节。两种标准的主要区别在于第三个字段(2 字节)。在 802.3 标准中，这个字段是长度字段，它指出后面的数据字段的字节数。数据字段就是 LLC 子层交下来的 LLC 帧，其最小长度为 46 字节，最大长度为 1500 字节。在 DIX Ethernet V2 标准中，这个字段是类型字段，它指出上层使用的协议类型。第四个字段为数据字段。最后一个字段是一个长度为 4 字节的帧校验序列 FCS，它对前四个字段进行循环冗余(CRC)校验。

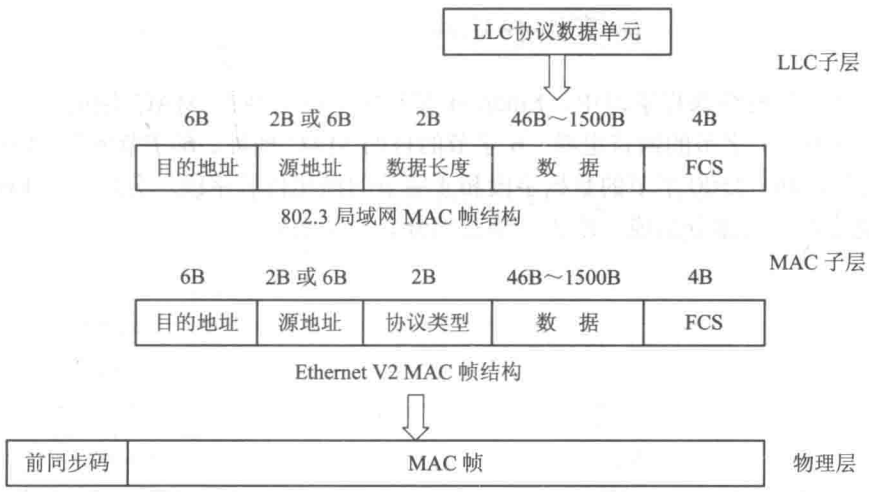

图 1-10　802.3 和 Ethernet V2 MAC 帧结构

为了使发送方和接收方同步，MAC 帧在总线上传输时还需要增加 7 个字节的前同步码字段和 1 个字节的起始定界符(它们是由硬件生成的)。其中，前同步码是 1 和 0 的交替序列，供接收方进行比特同步之用；紧跟在前同步码之后的起始定界符为 10101011，接收方一旦接收到两个连续的 1 后，就知道后面的信息就是 MAC 帧了。需要注意的是：前同步码、起始定界符和 MAC 帧中的 FCS 字段在网卡接收 MAC 帧时已经被取消，因此，在捕获的数据报中看不到这些字段。

本节实验重点分析 Ethernet V2 MAC 帧格式，对 802.3 MAC 帧不作具体讨论。

1.2.2 实验环境与说明

(1) 实验目的。了解 Ethernet V2 标准规定的 MAC 帧结构，初步了解 TCP/IP 的主要协议和协议的层次结构。

(2) 实验设备。实验设备为实验室局域网中任意两台主机 PC1、PC2。

(3) 实验分组。每两人一组，每组各自独立完成实验。

1.2.3 实验步骤

步骤 1：查看实验室 PC1 和 PC2 的 IP 地址并记录。假设 PC1 的 IP 地址为 172.16.1.101/24，PC2 的 IP 地址为 172.16.1.102/24。

步骤 2：在 PC1 和 PC2 上运行 Wireshark 捕获数据包，为了只捕获和实验内容有关的数据包，将 Wireshark 的 Capture Filter 设置为“No Broadcast and no Multicast”。

步骤 3：在 PC1 的“运行”对话框中输入命令“cmd”，在 Windows 命令行窗口输入“Ping 172.16.1.102”，单击“确定”按钮。

步骤 4：停止截获报文，将结果保存为帧实验-学号-姓名，并对截获的报文进行下列分析。

(1) 列出截获的报文中的协议类型，观察这些协议之间的关系。

(2) 在计算机网络课程学习中，Ethernet V2 规定以太网的 MAC 层的报文格式分为 7 字节的前导符、1 字节的帧首定界、6 字节的目的 MAC 地址、6 字节的源 MAC 地址、2 字节的类型、46～1500 字节的数据字段和 4 字节的帧尾校验字段。分析一个 Ethernet V2 帧，查看这个帧由几部分组成，缺少了哪几部分？为什么？

步骤 5：开启 Messenger 服务。打开“控制面板”，单击“性能和维护”，单击“管理

工具”，双击“服务”，单击“Messenger”，然后在“操作”菜单中单击“属性”，将“启动类型”改为“自动”。在 PC1 和 PC2 上运行 Wireshark 截获报文，然后进入 PC1、PC2 的 Windows 命令行窗口，执行如下命令：

```
net start messenger
```

然后进入 PC1 的 Windows 命令行窗口，执行如下命令：

```
net send 172.16.1.102 Hello
```

这是 PC1 向 PC2 发送消息的命令，等到 PC2 显示器上显示收到消息后，终止截获报文。

找到发送消息的报文并进行分析，查看 Wireshark 主窗口中数据包列表窗口和协议窗口信息，填写表 1.2。

表 1.2　数据包分析

此数据包类型		
此数据包的基本信息(数据包列表窗口中的 Information 项的内容)		
Ethernet II 协议树中	Source 字段值	
	Destination 字段值	
Internet Protocol 协议树中	Source 字段值	
	Destination 字段值	
User Datagram Protocol 协议树中	Source 字段值	
	Destination 字段值	
应用层协议树	协议名称	
	包含 Hello 的字段值	

实验完成后，要求将上述实验步骤中协议分析的结果写到实验报告中。

1.3　ARP 协议分析实验

1.3.1　ARP 协议介绍

ARP(Address Resolution Protocol，地址解析协议)，负责实现从 IP 地址到物理地址(如以太网 MAC 地址)的映射。在实际通信中，物理网络使用硬件地址进行报文传输。IP 报文在封装为数据链路层帧进行传送时，IP 地址必须转换为对应的硬件地址，ARP 正是动态地完成这一功能的协议。

1. ARP 协议格式

ARP 协议报文是定长的，其格式如图 1-11 所示，报文中每一字段的含义如下：

硬件类型：表示物理网络的类型，“0X0001”表示以太网；

协议类型：表示网络协议类型，“0X0800”表示 IP 协议；

硬件地址长度：指定源/目的站物理地址的长度，单位为字节；

协议地址长度：指定源/目的站 IP 地址的长度，单位为字节；

操作：指定该报文的类型，“1”为 ARP 请求报文，“2”为 ARP 响应报文；

源站物理/IP 地址：由 ARP 请求者填充；

目的站物理地址：在请求报文中为 0，在响应报文中由发送响应报文的主机填写自己的物理地址；

目的站 IP 地址：由 ARP 请求者填充，指源站想要知道的主机的 IP 地址。只有 IP 地址等于该 IP 地址的主机才向源主机发送相应报文。

图 1-11　ARP 报文格式

2. ARP 的工作方式

在以太网中，每台使用 ARP 协议实现地址解析的主机都在自己的高速缓存中维护着一个地址映射表，这个 ARP 表中存放着最近和它通信的同网络中的计算机的 IP 地址和对应的 MAC 地址。

当两台计算机通信时，源主机首先查看自己的 ARP 表中是否有目的主机的 IP 地址项，若有则使用对应的 MAC 地址直接向目的主机发送信息；否则就向网络中广播一个 ARP 请求报文，当网络中的主机收到该 ARP 请求报文时，首先查看报文中的目的 IP 地址是否与自己的 IP 地址相符，若相符则将请求报文中的源 IP 地址和 MAC 地址写入自己的 ARP 表中，然后创建一个 ARP 响应报文，将自己的 MAC 地址填入该响应报文中，发送给源主机。源主机收到响应报文后，取出目的 IP 地址和 MAC 地址加入到自己的 ARP 表中，并利用获得的目的 MAC 地址向目的主机发送信息。

3. ARP 命令简介

本实验使用 Windows 自带的 ARP 命令，该命令提供了显示和修改地址解析协议所使用的地址映射表的功能。

ARP 命令的格式要求如下：

```
ARP -s inet_addr ether_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr]
```

其中：

-s：在 ARP 缓存中添加表项，将 IP 地址 inet_addr 和物理地址 ether_addr 关联，物理地址由以连字符分隔的 6 个十六进制数给定，使用点分十进制标记指定 IP 地址，添加项是

永久性的。

-d：删除由 inet_addr 指定的表项。

-a：显示当前 ARP 表，如果指定了 inet_addr，则只显示指定计算机的 IP 和物理地址。

inet_addr：以点分十进制标记指定 IP 地址。

-N：显示由 if_addr 指定的 ARP 表项。

if_addr：指定需要选择或修改其地址映射表接口的 IP 地址。

ether_addr：指定物理地址。

1.3.2　实验环境与说明

(1) 实验目的。分析 ARP 协议的格式，理解 ARP 协议的解析过程。

(2) 实验设备。实验设备为实验室局域网中任意两台主机 PC1、PC2。

(3) 实验分组。每两人一组，每组各自独立完成实验。

1.3.3　实验步骤

步骤 1：查看实验室 PC1 和 PC2 的 IP 地址，并记录。假设 PC1 的 IP 地址为 172.16.1.101/24，PC2 的 IP 地址为 172.16.1.102/24。

步骤 2：在 PC1、PC2 两台计算机上执行如下命令，清除 ARP 缓存。

```
ARP –d
```

步骤 3：在 PC1、PC2 两台计算机上执行如下命令，查看高速缓存中的 ARP 地址映射表的内容。

```
ARP –a
```

步骤 4：在 PC1 和 PC2 上运行 Wireshark 捕获数据包，为了捕获和实验内容有关的数据包，Wireshark 的 Capture Filter 设置为默认方式。

步骤 5：在主机 PC1 上执行 Ping 命令向 PC2 发送数据包。

步骤 6：执行完毕，保存截获的报文并命名为 arp1-学号-姓名。

步骤 7：在 PC1、PC2 两台计算机上再次执行 ARP -a 命令，查看高速缓存中的 ARP 地址映射表的内容。

(1) 这次看到的内容和步骤 3 的内容相同吗？结合两次看到的结果，理解 ARP 高速缓存的作用。

(2) 把这次看到的高速缓存中的 ARP 地址映射表写出来。

步骤 8：重复步骤 4 和 5，将此结果保存为 arp2-学号-姓名。

步骤 9：打开 arp1-学号-姓名，完成以下各题。

(1) 在捕获的数据包中有几个 ARP 数据包？在以太帧中，ARP 协议类型的代码值是什么？

(2) 打开 arp2-学号-姓名，比较两次截获的报文有何区别？分析其原因。

(3) 分析 arp1-学号-姓名中 ARP 报文的结构，完成表 1.3。

表 1.3 ARP 协议分析

ARP 请求报文		ARP 应答报文	
字段	报文信息及参数	字段	报文信息及参数
硬件类型		硬件类型	
协议类型		协议类型	
硬件地址长度		硬件地址长度	
协议地址长度		协议地址长度	
操作		操作	
源站物理地址		源站物理地址	
源站 IP 地址		源站 IP 地址	
目的站物理地址		目的站物理地址	
目的站 IP 地址		目的站 IP 地址	

实验完成后，要求将上述实验步骤中协议分析的结果写到实验报告中。