十三五 高等职业教育“十三五”精品规划教材（计算机网络技术系列）

网络协议分析

主　编　许　爽　苏　玉
副主编　石彦华　于书红　马莹莹

中国水利水电出版社
www.waterpub.com.cn

高等职业教育“十三五”精品规划教材（计算机网络技术系列）

网络协议分析

主　编　许　爽　苏　玉

副主编　石彦华　于书红　马莹莹

中国水利水电出版社
www.waterpub.com.cn

·北京·

内 容 提 要

本书为计算机网络基础丛书。全书以 TCP/IP 协议分析为主线，按照数据链路层→网络层→传输层→应用层来组织内容，同时结合大量实例对协议进行了深入剖析，降低了读者的学习难度，激发了读者的学习兴趣和动手欲望。

本书采用任务驱动方式编写，可操作性强，内容丰富，图文并茂。可作为高职高专院校和应用型本科院校计算机类专业的教材和参考书，也可供与信息类相关的非计算机专业选用，还可作为 IT 技术人员的参考书。

本书配有电子教案，读者可以从中国水利水电出版社网站和万水书苑免费下载，网址为：http://www.waterpub.com.cn/softdown/和 http://www.wsbookshow.com。

图书在版编目（CIP）数据

网络协议分析 / 许爽，苏玉主编. -- 北京 : 中国水利水电出版社，2016.9

高等职业教育“十三五”精品规划教材. 计算机网络技术系列

ISBN 978-7-5170-4693-6

Ⅰ. ①网… Ⅱ. ①许… ②苏… Ⅲ. ①计算机网络－通信协议－高等职业教育－教材 Ⅳ. ①TN915.04

中国版本图书馆CIP数据核字(2016)第211317号

策划编辑：祝智敏　责任编辑：李　炎　加工编辑：陈宏华　封面设计：李　佳

书　名	高等职业教育“十三五”精品规划教材（计算机网络技术系列） 网络协议分析　WANGLUO XIEYI FENXI
作　者	主　编　许　爽　苏　玉 副主编　石彦华　于书红　马莹莹
出版发行	中国水利水电出版社 （北京市海淀区玉渊潭南路 1 号 D 座　100038） 网址：www.waterpub.com.cn E-mail：mchannel@263.net（万水） sales@waterpub.com.cn 电话：（010）68367658（营销中心）、82562819（万水）
经　售	全国各地新华书店和相关出版物销售网点
排　版	北京万水电子信息有限公司
印　刷	三河市铭浩彩色印装有限公司
规　格	184mm×260mm　16 开本　12.5 印张　307 千字
版　次	2016 年 9 月第 1 版　2016 年 9 月第 1 次印刷
印　数	0001—3000 册
定　价	28.00 元

前　言

目前，计算机网络技术飞速发展，而网络协议是计算机网络的基础。它规范了网络上的所有通信设备，尤其是一个主机与另一个主机之间的数据往来格式以及传送方式。

“网络协议分析”是计算机网络技术专业和信息安全专业必修的一门专业基础课，本书编者通过多年的网络协议分析教学，积累了丰富的经验。为了总结经验，结合目前国内高校网络协议分析教学的实际，融合网络协议的最新发展，系统地阐述了计算机网络协议的基础理论并结合实际对网络数据进行分析。本书共分为 9 个单元，每个单元中将关联性强的内容放在同一个任务中，除了基础知识点以外，每个任务采用“任务背景介绍”→“知识点介绍”→“任务实现”→“知识扩展”模式把理论知识、实践技能融于一个学习情境中，激发学生的学习兴趣，引导学生轻松掌握网络协议的基础知识，为学生学习计算机网络技术的相关知识奠定坚实的基础。

本书由中州大学许爽老师和苏玉老师担任主编，并负责全书的统稿、修改、定稿工作，由中州大学石彦华老师、于书红老师、马莹莹老师担任副主编，参与编写的还有中州大学的周华老师、杜舒老师，郑州科技学院的牛丹丹老师等。要特别感谢中国水利水电出版社的编辑老师，他们在本书的策划和写作中对编写方式及习题设置提出了很好的建议，使得本书能够更好地用于教学。为了配合本套教材的教学，本书还配有相关的课件。在本书编写过程中编者参考了大量国内外计算机网络协议相关文献资料，在此向这些文献资料的著作者表示感谢。

我们全体编写人员虽然尽心尽力，但由于时间仓促，加之编者水平有限，新的知识和技术资料不断涌现，书中难免有错误和疏漏之处，敬请广大师生及各位读者给予批评和指正。

编　者

2016 年 6 月

目　　录

1 网络及协议

本单元介绍一些基本概念，它们是学好本课程后面章节的基础。本单元涵盖了有关服务、分层和协议的重要信息。另外，还将学习如何捕获一段数据包以及如何对捕获的数据包进行分析。

内容摘要：

- 网络互连与 TCP/IP
- 网络协议的分层
- 网络协议的标准化

学习目标：

- 理解 TCP/IP 分层的思想
- 了解 TCP/IP 的发展过程
- 掌握 Wireshark 的使用方法

任务 1　网络的基本概念及协议

知识与技能：

- 了解网络的基本概念
- 了解协议栈的组成
- 理解进程及其相应的协议分层原因
- 解释封装和解封装的过程

一、任务背景介绍

随着计算机网络通信技术以及信息产业的高速发展，计算机网络在人们的日常工作生活及学习中扮演着越来越重要的角色，网络协议作为计算机网络通信的核心框架日渐得到广泛关注。因此对网络协议的深入学习和掌握可以帮助我们更好地了解及使用计算机网络。

二、知识点介绍

1. 计算机网络的基本概念

把分布在不同地理位置上的具有独立功能的多台计算机、终端及其附属设备在物理上互连，按照网络协议相互通信，以共享硬件、软件和数据资源为目标的系统称作计算机网络，如图 1-1-1 所示。

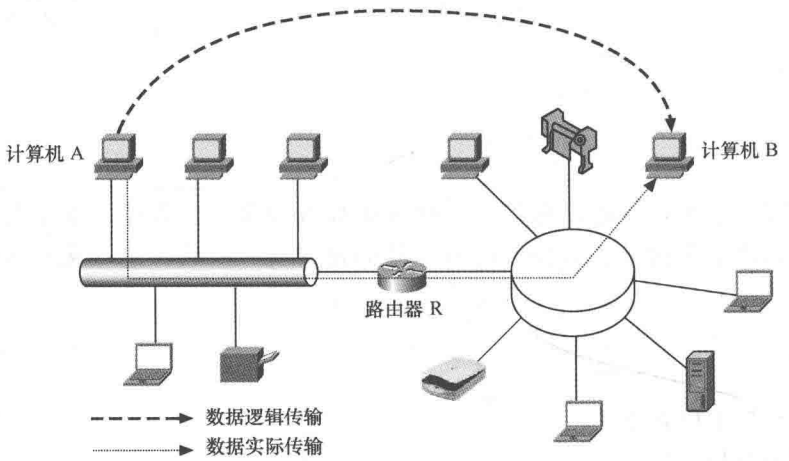

图 1-1-1　计算机网络

2. 计算机网络体系结构

网络的体系结构指的是通信系统的整体框架（包括计算机网络的各层及其协议的集合）。它的目的是为网络硬件、软件、协议、存取控制和拓扑结构提供标准。

3. 协议

协议是指在计算机网络中，为进行网络中的数据交换而建立的规则、标准或约定的集合，如交换数据的格式、编码方式、同步方式等。

协议定义了通信的方式和进行通信的时间，主要包括语法、语义和同步 3 个关键要素。其中，语法：定义了所交换数据的格式和结构，以及数据出现的顺序；语义：定义了发送者或接收者所要完成的操作，包括对协议控制报文组成成分含义的约定；同步：定义了时间实现顺序以及速度匹配，体现在两个实体进行通信时，数据发送的时间以及发送的速率。

4. OSI 体系结构与 TCP/IP 体系结构

（1）开放系统互连参考模型 OSI/RM（Open Systems Interconnection Reference Model），简称为 OSI。

OSI 模型分为物理层、数据链路层、网络层、传输层、会话层、表示层和应用层共 7 个层次。OSI 模型并没有确切地描述用于各层的协议和服务，实现起来比较困难，难以推广（在数

据链路层和网络层有很多的子层，并且每个子层都有不同的功能，使之格外复杂。数据安全与加密等问题也在设计初期被忽略了）。

（2）TCP/IP 体系结构。

TCP/IP 体系结构分为链路层、网络层、传输层和应用层 4 个层次。TCP 一开始就将面向连接服务和无连接服务并重考虑，而 OSI 开始只考虑面向连接服务，很晚才开始制定有关标准。TCP/IP 经过了实践的考验并在实践中发展完善（ARPANet），目前的 Internet 即采用的是 TCP/IP 体系结构。

（3）OSI 与 TCP/IP 体系结构对照（见图 1-1-2）。

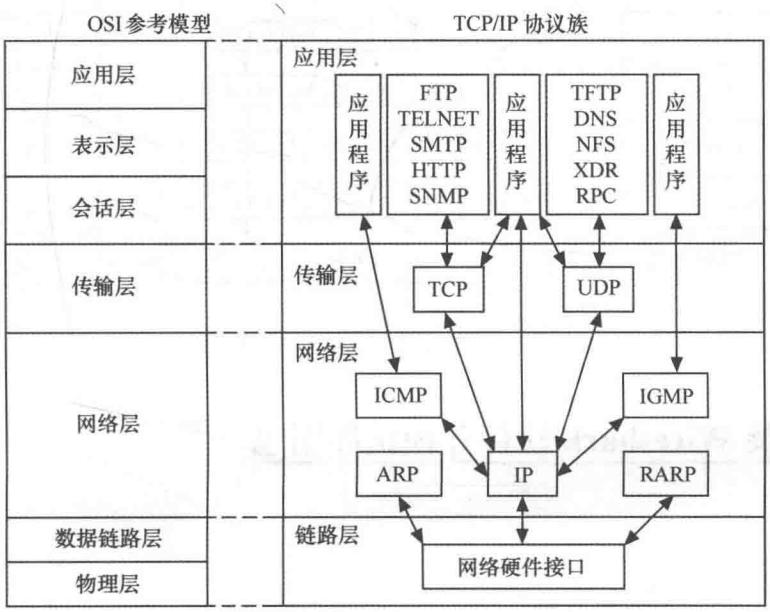

图 1-1-2　TCP/IP 体系结构

5. 数据的封装和解封装

在 OSI 参考模型中，当一台主机需要传送用户的数据（data）时，数据首先通过应用层的接口进入应用层。在应用层，用户的数据被加上应用层的报头（Application Header，AH），形成应用层协议数据单元（Protocol Data Unit，PDU），然后被递交到下一层——表示层。

表示层并不“关心”上层——应用层的数据格式而是把整个应用层递交的数据包看成是一个整体进行封装，即加上表示层的报头（Presentation Header，PH）。然后，递交到下层——会话层。

同样，会话层、传输层、网络层、数据链路层也都要分别给上层递交下来的数据加上自己的报头。它们是：会话层报头（Session Header，SH）、传输层报头（Transport Header，TH）、网络层报头（Network Header，NH）和数据链路层报头（Data link Header，DH）。其中，数据链路层还要给网络层递交的数据加上数据链路层报尾（Data link Termination，DT）形成最终的一帧数据。

当一帧数据通过物理层传送到目标主机的物理层时，该主机的物理层把它递交到上层——数据链路层。数据链路层负责去掉数据帧的帧头部 DH 和尾部 DT（同时还进行数据校验）。

如果数据没有出错，则递交到上层——网络层。

同样，网络层、传输层、会话层、表示层、应用层也要做类似的工作。最终，原始数据被递交到目标主机的具体应用程序中。

图 1-1-3 给出了数据封装及解封装的过程。

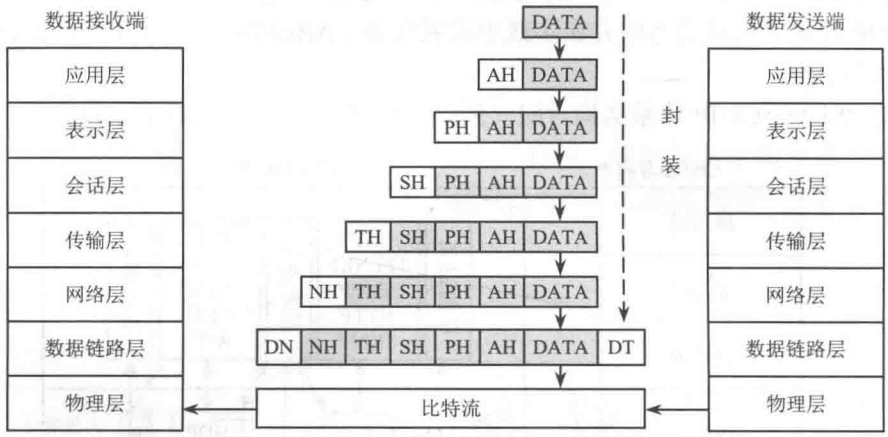

图 1-1-3　数据封装及解封装过程图

任务 2　安装 Wireshark 软件并捕获数据包

知识与技能：

- 了解协议分析仪的基本要素
- 掌握协议分析仪的规则

一、任务背景介绍

协议分析是接入网络通信系统、捕获穿行在网络中的数据、收集网络统计信息的过程。Wireshark 是当今十分流行的协议分析仪。

二、知识点介绍

1. Wireshark 简介

Wireshark（前身 Ethereal）是目前最好的、开放源码的、获得广泛应用的网络协议分析仪，支持 Linux 和 Windows 平台。在该系统中加入新的协议解析器十分简单，自从 1998 年最早的 Ethereal 0.2 版本发布以来，志愿者为 Ethereal 添加了大量新的协议解析器，如今 Ethereal 已经支持五百多种协议解析。其原因是 Ethereal 具有一个良好的可扩展的设计结构，这样才能适应网络发展的需要不断加入新的协议解析器。

2. Wireshark 主窗口组成

Wireshark 主窗口如图 1-2-1 所示，由如下部分组成：

（1）菜单：用于开始操作。

（2）主工具栏：提供快速访问菜单中经常用到的项目的功能。

（3）Filter toolbar/过滤工具栏：提供处理当前显示过滤的方法。

（4）Packet list 面板：显示打开文件的每个数据包的摘要。点击面板中的单独条目，数据包的其他情况将会显示在另外两个面板中。

（5）Packet detail 面板：显示在 Packet list 面板中选择的包的更多详情。

（6）Packet bytes 面板：显示在 Packet list 面板选择的数据包的数据，以及在 Packet details 面板高亮显示的字段。

（7）状态栏：显示当前程序状态以及捕捉数据的更多详情。

3. Wireshark 菜单栏简介

（1）File（文件）菜单

文件菜单包括打开和合并抓包文件，全部或部分存储、打印、输出抓包文件，退出 Wireshark。

（2）Edit（编辑）菜单

编辑菜单包括查询包，时间查询，标记或标识一个或多个包，设置你的选项（剪切，拷贝，粘贴当前不能实现）。

（3）View（视图）菜单

视图菜单控制抓获的数据包的显示，包括对抓获包的着色，字型的缩放，协议窗格中 协议树的压缩和展开。

（4）Go（指向）菜单

以不同方式指向特定的包。

（5）Capture（抓包）菜单

开始和停止抓包过程以及编辑抓包过滤器。

（6）Analyze（分析）菜单

包括的选项有操作显示过滤器，允许和不允许对协议解析，配置用户指定的译码器和跟踪一个 TCP 流。

（7）Statistics（统计）菜单

显示各种统计窗口的菜单项，包括已经抓到的包的摘要，显示协议的分层统计等。

（8）Help（帮助）菜单

包括帮助用户的选项，诸如一些基本帮助，所支持的协议列表，手工页面，在线访问一些 web 页面，以及常用的对话框。

4. 规则制定

Filter toolbar 中可以使用下面的操作符来构造显示过滤规则：

eq == 等于：如 ip.addr==10.1.10.20

ne != 不等于：如 ip.addr!=10.1.10.20

gt > 大于：如 frame.pkt_len>10

lt < 小于：如 frame.pkt_len<10

ge >= 大等于：如 frame.pkt_len>=10

le <= 小等于：如 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：

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

or || 逻辑或：如 ip.addr=10.1.10.20||ip.addr=10.1.10.21

xor ^^ 异或：如 tr.dst[0:3] == 0.6.29 xor tr.src[0:3] == not

! 逻辑非：如 !llc

例如：你想抓取 IP 地址是 192.168.1.121 的主机所收或发的所有的 HTTP 报文，则显示过滤规则（Filter）为：ip.addr=192.168.1.121 and http。

三、任务实现

使用 Wireshark 进行网络协议分析时应当注意：必须选择正确的网络接口来抓获数据包；必须在网络的正确的位置抓包才能看到想看到的业务流量。下面的任务实现是讲述怎样使用 Wireshark 1.12.4 在 Windows 7 专业版环境中捕获数据包的过程。

（1）启动 Wireshark 软件。

先来看看图 1-2-1“主窗口界面”，大多数打开 Wireshark 软件以后的界面都是这样子。

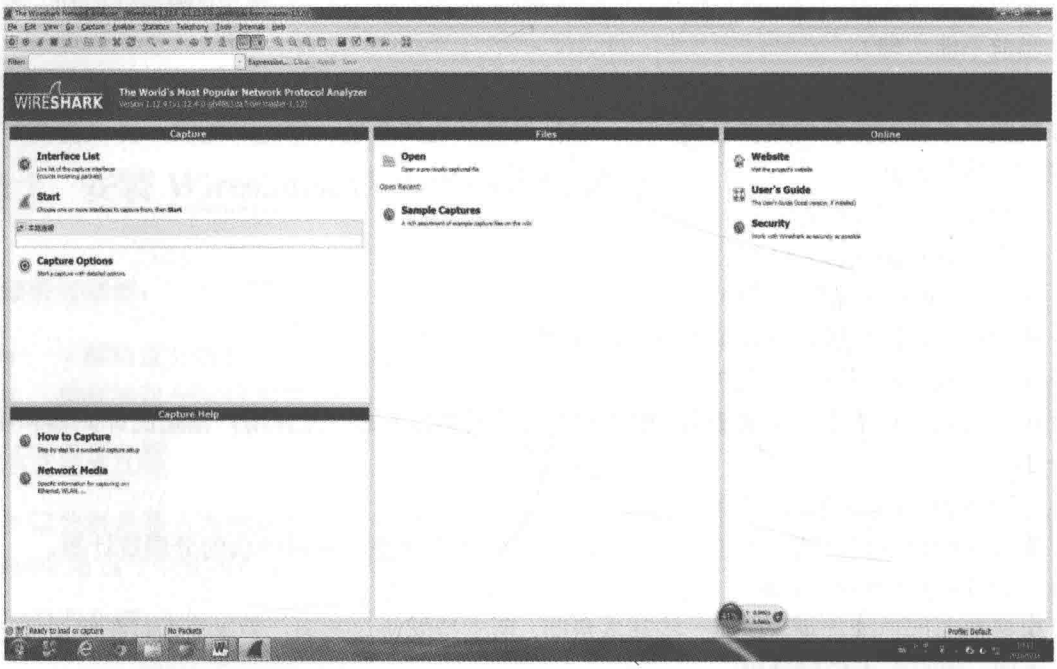

图 1-2-1 主窗口界面

（2）点击绿色的“Start”按钮，进入图 1-2-2，Wireshark 就开始捕获数据包。点击红色的“Stop”按钮，Wireshark 停止捕获数据包。主界面显示出已经捕获到的数据包。

列表中的每行显示捕捉文件的一个包。例如选择 No.9 的数据包，该包的更多情况会在新窗口中显示出来，如图 1-2-3 所示。

在分析（解剖）包时，Wireshark 会将协议信息放到各个列。因为高层协议通常会覆盖底层协议，通常在包列表面板看到的都是每个包的最高层协议描述。

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 UDP 协议报文格式的具体数据，与十六进制窗口相结合，清楚地看到各个字段的数据。

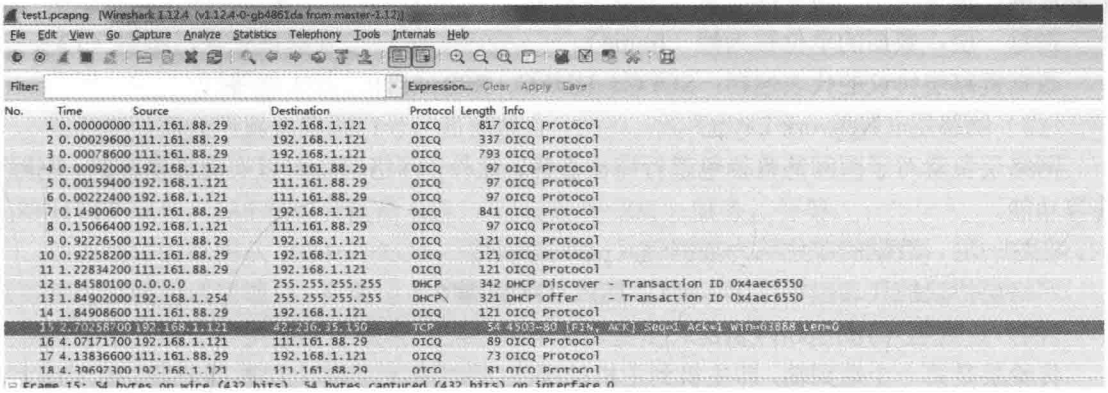

图 1-2-2　捕获到的数据包

图 1-2-3　No.9 数据包详解图

四、知识扩展

1. OSI 参考模型中各层的作用、数据单位、协议代表

在 OSI 参考模型中，从下至上，每一层完成不同的、目标明确的功能。

（1）物理层（Physical Layer）

物理层规定了激活、维持、关闭通信端点之间的机械特性、电气特性、功能特性以及过程特性。该层为上层协议提供了一个传输数据的物理介质。

在这一层，数据的单位称为比特（bit）。

属于物理层定义的典型规范包括：EIA/TIA RS-232、EIA/TIA RS-449、V.35、RJ-45 等。

（2）数据链路层（Data Link Layer）

数据链路层在不可靠的物理介质上提供可靠的传输。该层的作用包括：物理地址寻址、数据的成帧、流量控制、数据的检错、重发等。

在这一层，数据的单位称为帧（frame）。

数据链路层协议的代表包括：SDLC、HDLC、PPP、STP、帧中继等。

（3）网络层（Network Layer）

网络层负责对子网间的数据包进行路由选择。此外，网络层还可以实现拥塞控制、网际互连等功能。

在这一层，数据的单位称为数据包（packet）。

网络层协议的代表包括：IP、IPX、RIP、OSPF 等。

（4）传输层（Transport Layer）

传输层是第一个端到端，即主机到主机的层次。传输层负责将上层数据分段并提供端到端的、可靠的或不可靠的传输。此外，传输层还要处理端到端的差错控制和流量控制问题。

在这一层，数据的单位称为数据段（segment）。

传输层协议的代表包括：TCP、UDP、SPX 等。

（5）会话层（Session Layer）

会话层管理主机之间的会话进程，即负责建立、管理、终止进程之间的会话。会话层还利用在数据中插入校验点来实现数据的同步。

会话层协议的代表包括：NetBIOS、ZIP（AppleTalk 区域信息协议）等。

（6）表示层（Presentation Layer）

表示层对上层数据或信息进行变换以保证一个主机的应用层信息可以被另一个主机的应用程序理解。表示层的数据转换包括数据的加密、压缩、格式转换等。

表示层协议的代表包括：ASCII、ASN.1、JPEG、MPEG 等。

（7）应用层（Application Layer）

应用层为操作系统或网络应用程序提供访问网络服务的接口。

应用层协议的代表包括：Telnet、FTP、HTTP、SNMP 等。

2. RFC（一系列以编号排定的文件）

RFC是 Request for Comments 首字母的缩写，它是IETF（互联网工程任务推进组织）的一个无限制分发文档。RFC 被编号并且用编号来标识。每一个 RFC 文档有一个编号，这个编号永不重复，也就是说，由于技术进步等原因，即使是关于同一问题的 RFC，也要使用新的编号，而不会使用原来的编号。

文件收集了有关因特网相关资讯，以及 UNIX 和因特网社群的软件文件。目前 RFC 文件是由 Internet Society（ISOC）所赞助发行。

基本的因特网通信协议都有在 RFC 文件内详细说明。RFC 文件还在标准内额外加入了许多的论题，例如对于因特网新开发的协议及发展中所有的记录。因此几乎所有的因特网标准都收录在 RFC 文件之中。

3. 端口号

在网络技术中，端口（Port）大致有两种意思：一是物理意义上的端口，比如，ADSL Modem、集线器、交换机、路由器用于连接其他网络设备的接口，如 RJ-45 端口、SC 端口等。二是逻辑意义上的端口，一般是指 TCP/IP 协议中的端口，端口号的范围从 0～65535，比如用于浏览

网页服务的 80 端口，用于 FTP 服务的 21 端口等。

逻辑意义上的端口有多种分类标准，下面将介绍两种常见的分类：

（1）按端口号分布划分

按端口号分布划分，可以分为知名端口和动态端口。

知名端口即众所周知的端口号，范围从 0～1023，这些端口号一般固定分配给一些服务。比如 21 端口分配给 FTP 服务，25 端口分配给 SMTP（简单邮件传输协议）服务，80 端口分配给 HTTP 服务，135 端口分配给 RPC（远程过程调用）服务，等等。

动态端口的范围从 1024～65535，这些端口号一般不固定分配给某个服务，也就是说许多服务都可以使用这些端口。只要运行的程序向系统提出访问网络的申请，那么系统就可以从这些端口号中分配一个供该程序使用。比如 1024 端口就是分配给第一个向系统发出申请的程序。在关闭程序进程后，就会释放所占用的端口号。

不过，动态端口也常常被病毒木马程序所利用，如冰河默认连接端口是 7626、WAY 2.4 是 8011、Netspy 3.0 是 7306、YAI 病毒是 1024 等。

（2）按协议类型划分

按协议类型划分，可以分为 TCP、UDP、IP 和 ICMP（Internet 控制消息协议）等端口。下面主要介绍 TCP 和 UDP 端口：

TCP 端口，即传输控制协议端口，需要在客户端和服务器之间建立连接，这样可以提供可靠的数据传输。常见的包括 FTP 服务的 21 端口，Telnet 服务的 23 端口，SMTP 服务的 25 端口，以及 HTTP 服务的 80 端口等。

UDP 端口，即用户数据报协议端口，无需在客户端和服务器之间建立连接，安全性得不到保障。常见的有 DNS 服务的 53 端口，SNMP（简单网络管理协议）服务的 161 端口，QQ 使用的 8000 和 4000 端口等。

本单元小结

本单元讲述了网络协议的基本概念，并举例说明了协议分析仪 Wireshark 的使用方法。

习题 1

一、选择题

1. 当今最广泛使用的 IP 版本的名称是什么？（ ）

   A. IPv1　　B. IPv2　　C. IPv4　　D. IPv6

2. 下述哪一个机构管理 Internet 域名和网络地址？（ ）

   A. ICANN　　B. IETF　　C. IRTF　　D. ISOC

3. 下述哪一些部件工作在物理层？（可多选）（ ）

   A. 网卡　　B. 分段和重组　　C. 连接器　　D. 网线

4. 数据链路层上 PDU 的常用名称是什么？（ ）

   A. 帧　　B. 数据包　　C. 数据段　　D. 数据链路 PDU

5．下述哪两个协议运行在 TCP/IP 的传输层？（　　）

A．ARP　　B．PPP　　C．TCP

D．UDP　　E．XNET

6．下述哪一个术语是描述动态分配端口地址、用于为数据交换提供临时 TCP/IP 连接的同义词？（　　）

A．协议号　　B．公认端口号　　C．注册端口号　　D．套接字地址

7．提供可靠数据传输、流控的是 OSI 的第几层？（　　）

A．表示层　　B．网络层　　C．传输层

D．会话层　　E．链路层

8．子网掩码产生在哪一层？（　　）

A．表示层　　B．网络层　　C．传输层　　D．会话层

9．RFC 文档是下面哪一个标准化组织的工作文件？（　　）

A．ISO　　B．IETF　　C．ITU　　D．IAB

10．OSI 参考模型按顺序有（　　）。

A．应用层、传输层、网络层、物理层

B．应用层、表示层、会话层、网络层、传输层、数据链路层、物理层

C．应用层、表示层、会话层、传输层、网络层、数据链路层、物理层

D．应用层、会话层、传输层、物理层

二、填空题

1．TCP/IP 协议的体系结构分为四层，这四层由高到低分别是：_____、_____、_____和_____。

2．在 TCP/IP 层次模型的网络层中包括的协议主要有 ARP、ICMP、_____和_____。

3．传统上公认端口地址定义在_____范围。

4．在以太网中，是根据_____地址来区分不同的设备。

5．网络层最重要的功能是进行_____，即在互联网中选择一条路径，把 IP 数据报从源端送到目标端。

6．RFC 文档是由标准化组织_____定义的工作文件。

2

局域网协议和广域网协议

本单元介绍局域网和广域网协议，主要包括以太网 V2 协议、HDLC 协议和 PPP 协议帧的格式。通过帧格式和 Wireshark 捕捉的数据包解码来分析具体的案例。

内容摘要：

- 以太网 V2 帧格式
- HDLC 帧的格式
- PPP 协议帧的格式

学习目标：

- 了解局域网和广域网协议的帧格式
- 掌握局域网和广域网协议的分析方法

任务 1　以太网 V2 帧格式

知识与技能：

- 了解以太网 V2 的帧格式
- 掌握以太网 V2 的帧格式分析的规则

一、任务背景介绍

在因特网上，IP 地址用于主机间通信，无论它们是否属于同一局域网。同一局域网内主机间传输数据前，发送方首先要把目的 IP 地址转换成对应的 MAC 地址。这通过地址解析协议（ARP）实现。每台主机以 ARP 高速缓存形式维护一张地址表，已知 IP 分组就放在链路层帧的数据部分，而帧的目的地址将被设置为 ARP 高速缓存中找到的 MAC 地址。如果没有发现 IP 地址的转换项，那么本机将广播一个报文，要求具有此 IP 地址的主机用它的 MAC 地址