21世纪高职高专规划教材·计算机类

体现职业教育课程改革的要求
以岗位技能需求为导向的内容体系
以项目或案例为主线的编写思路
实践类课程紧密结合国家职业资格认证

计算机网络实训教程

主编　马荣飞　何志玲

北京理工大学出版社
BEIJING INSTITUTE OF TECHNOLOGY PRESS

21 世纪高职高专规划教材 · 计算机类

计算机网络实训教程

主编　马荣飞　何志玲

北京理工大学出版社
BEIJING INSTITUTE OF TECHNOLOGY PRESS

内 容 简 介

本书是与《计算机网络技术》配套的实训指导教材，全书包括17个实训，每个实训都包括实训目的、实训任务、背景知识、实训环境、实训内容及步骤和实训思考题。书中实训注重能力本位的培养，通过实训案例将“体验式学习”思想贯彻其中，可使网络学习者更好更快地掌握计算机网络技术相关知识。

本书运用简洁易懂的描述和生动直观的事例对计算机网络技术知识进行阐述，内容详实，具有较强的实用性。通过本书的学习，可以有效地帮助读者巩固所学的相关理论知识；同时可增强读者的动手能力，引导读者做到学以致用。

本书可作为计算机类及相关专业“计算机网络”、“计算机网络技术”等课程的实训指导教材，也可作为网络工程师和计算机网络爱好者的参考书。

图书在版编目（CIP）数据

计算机网络实训教程/马荣飞，何志玲主编. —北京：北京理工大学出版社，2008.8

ISBN 978-7-5640-1686-9

Ⅰ.计…　Ⅱ.①马…②何…　Ⅲ.计算机网络-教材　Ⅳ.TP393

中国版本图书馆CIP数据核字（2008）第120267号

出版发行／北京理工大学出版社

社　　址／北京市海淀区中关村南大街5号

邮　　编／100081

电　　话／(010)68914775(办公室)　68944990(批销中心)　68911084(读者服务部)

网　　址／http：// www.bitpress.com.cn

经　　销／全国各地新华书店

印　　刷／北京地质印刷厂

开　　本／787毫米×1092毫米　1/16

印　　张／10

字　　数／230千字

版　　次／2008年8月第1版　2008年8月第1次印刷

印　　数／1～4000册　　责任校对／申玉琴

定　　价／25.00元　　责任印制／边心超

前　言

随着计算机网络技术的飞速发展，计算机网络已应用于各行各业，社会对网络人才的需求量越来越大，计算机网络技术已经成为国内外高职院校计算机类及相关专业的重要课程。

本书作者在总结多年计算机网络技术课程教学经验的基础上，精心设计了17个实训，包括使用协议分析工具Sniffer pro学习TCP/IP协议，网络传输线、RJ-45接头的制作，小型局域网组建，安装Windows Server 2003，Windows Server 2003基本网络配置，对等网的组建与配置，资源共享及权限，Windows Server 2003活动目录的建立，活动目录的管理及设置目录共享，组策略配置，利用组策略管理用户环境，组策略实现安全管理，DNS服务器搭建，DHCP服务器的搭建，WINS服务器搭建，Web站点的创建与配置管理和FTP服务的配置与使用等内容。

本教材的创新之处在于：① 计算机网络技术教学中引入实训环节；② 强化了学习者的工程实践意识、提高其实际动手能力；③ 能够巩固其理论基础并加深其对理论的理解，并在此基础上，用正确的理论指导实践活动；④ 计算机网络实训方法包括预习、操作和总结；⑤ 突出能力本位。

本教材的特色是以实际计算机网络技术需求为目标，突出能力本位，培养学习者评价、选择网络技术、设备的能力，培养设计、构建局域网和对等网系统的能力，培养活动目录、组策略配置管理的能力，培养DNS服务器、DHCP服务器和WINS服务器搭建与管理能力，培养Web站点、FTP服务的创建、配置管理和使用能力。本教材适合网络专业大学生以及网络信息领域工程技术人员使用。

本书由马荣飞、何志玲担任主编并负责全书的统稿。各章节的具体编写分工是：实训一、实训六由吴响容编写，实训二、实训三由马荣飞编写，实训四、实训五由邸凤英编写，实训七由吴响容和何志玲编写，实训八至实训十二由毕晓东编写，实训十三至实训十五由楼建列编写，实训十六、实训十七由张佳编写。本书出版过程中得到了北京理工大学出版社的大力支持，在此表示衷心的感谢。

限于作者水平，书中难免有不足与疏漏之处，真诚希望广大读者朋友在使用本书过程中提出宝贵意见和建议。

目　录

实训一　使用协议分析工具 Sniffer pro 学习 TCP/IP 协议 …… 1
1.1　实训目的 …… 1
1.2　实训任务 …… 1
1.3　背景知识 …… 1
1.3.1　ISO OSI/RM …… 1
1.3.2　TCP/IP 体系结构 …… 2
1.3.3　各层的基本任务及其常用协议 …… 3
1.4　实训环境 …… 3
1.5　实训内容及步骤 …… 4
1.6　实训思考题 …… 11
实训二　网络传输线、RJ-45 接头的制作 …… 12
2.1　实训目的 …… 12
2.2　实训任务 …… 12
2.3　背景知识 …… 12
2.4　实训环境 …… 14
2.5　实训内容及步骤 …… 14
2.6　实训思考题 …… 18
实训三　小型局域网组建 …… 19
3.1　实训目的 …… 19
3.2　实训任务 …… 19
3.3　背景知识 …… 19
3.3.1　局域网的特征 …… 19
3.3.2　局域网种类 …… 20
3.3.3　局域网的网络地址 …… 21
3.4　实训环境 …… 22
3.5　实训内容及步骤 …… 22
3.6　实训思考题 …… 29
实训四　安装 Windows Server 2003 …… 30
4.1　实训目的 …… 30
4.2　实训任务 …… 30
4.3　背景知识 …… 30
4.3.1　系统和硬件设备要求 …… 30
4.3.2　安装程序来源 …… 30

4.3.3 选择安装方式 …… 30
4.3.4 选择许可证方式 …… 31
4.3.5 文件系统的选择 …… 31
4.4 实训环境 …… 31
4.5 实训要求及注意事项 …… 31
4.6 实训内容及步骤 …… 32
4.7 实训思考题 …… 36
实训五 Windows Server 2003 基本网络配置 …… 37
5.1 实训目的 …… 37
5.2 实训任务 …… 37
5.3 背景知识 …… 37
5.3.1 IP 地址 …… 37
5.3.2 子网掩码的功能 …… 37
5.3.3 默认网关 …… 37
5.4 实训环境 …… 38
5.5 实训内容及步骤 …… 38
5.6 实训思考题 …… 43
实训六 对等网的组建与配置 …… 44
6.1 实训目的 …… 44
6.2 实训任务 …… 44
6.3 背景知识 …… 44
6.3.1 局域网的网络类型 …… 44
6.3.2 组建对等网的好处 …… 45
6.4 实训环境 …… 45
6.5 实训内容及步骤 …… 46
6.6 实训思考题 …… 53
实训七 资源共享及权限 …… 54
7.1 实训目的 …… 54
7.2 实训任务 …… 54
7.3 背景知识 …… 54
7.3.1 资源共享 …… 54
7.3.2 权限的规则 …… 54
7.4 实训环境 …… 55
7.5 实训内容及步骤 …… 55
7.6 实训思考题 …… 65
实训八 Windows Server 2003 活动目录的建立 …… 66
8.1 实训目的 …… 66
8.2 实训任务 …… 66
8.3 背景知识——活动目录概述 …… 66

8.4 实训环境 …… 69
8.5 实训内容及步骤 …… 69
8.6 实训思考题 …… 72
实训九　活动目录的管理及设置目录共享 …… 73
9.1 实训目的 …… 73
9.2 实训任务 …… 73
9.3 背景知识 …… 73
9.3.1 用户账户 …… 73
9.3.2 组 …… 73
9.3.3 组织单位 …… 74
9.3.4 使用目录与文件的权限设置 …… 74
9.3.5 设置共享权限的注意事项 …… 75
9.4 实训环境 …… 75
9.5 实训内容及步骤 …… 75
9.6 实训思考题 …… 80
实训十　组策略配置 …… 81
10.1 实训目的 …… 81
10.2 实训任务 …… 81
10.3 背景知识 …… 81
10.3.1 什么是组策略 …… 81
10.3.2 组策略的版本 …… 81
10.3.3 在 Windows 中运行组策略 …… 82
10.3.4 组策略功能特点 …… 82
10.3.5 组策略对象 …… 83
10.3.6 组策略生效顺序和规则 …… 84
10.4 实训环境 …… 84
10.5 实训内容及步骤 …… 84
10.6 实训思考题 …… 87
实训十一　利用组策略管理用户环境 …… 88
11.1 实训目的 …… 88
11.2 实训任务 …… 88
11.3 背景知识 …… 88
11.3.1 用户工作环境 …… 88
11.3.2 管理用户工作环境 …… 89
11.4 实训环境 …… 90
11.5 实训内容及步骤 …… 90
11.6 实训思考题 …… 94
实训十二　组策略实现安全管理 …… 95
12.1 实训目的 …… 95

12.2 实训任务 …… 95
12.3 背景知识——组策略安全设置综述 …… 95
12.4 实训环境 …… 96
12.5 实训内容及步骤 …… 96
12.6 实训思考题 …… 98
实训十三 DNS 服务器搭建 …… 99
13.1 实训目的 …… 99
13.2 实训任务 …… 99
13.3 背景知识 …… 99
13.3.1 DNS 概述 …… 99
13.3.2 Internet 命名空间 …… 99
13.3.3 DNS 组成 …… 100
13.3.4 DNS 的工作方式 …… 100
13.4 实训环境 …… 101
13.5 实训内容和步骤 …… 101
13.6 实训思考题 …… 114
实训十四 DHCP 服务器的搭建 …… 115
14.1 实训目的 …… 115
14.2 实训任务 …… 115
14.3 背景知识 …… 115
14.3.1 DHCP 概述 …… 115
14.3.2 DHCP 工作方式 …… 115
14.4 实训环境 …… 117
14.5 实训内容与步骤 …… 117
14.6 实训思考题 …… 124
实训十五 WINS 服务器搭建 …… 125
15.1 实训目的 …… 125
15.2 实训任务 …… 125
15.3 背景知识 …… 125
15.4 实训环境 …… 127
15.5 实训内容与步骤 …… 127
15.6 实训思考题 …… 131
实训十六 Web 站点的创建与配置管理 …… 132
16.1 实训目的 …… 132
16.2 实训任务 …… 132
16.3 背景知识 …… 132
16.4 实训环境 …… 132
16.5 实训内容及步骤 …… 132
16.6 实训思考题 …… 136

实训十七　FTP 服务的配置与使用 137
17.1　实训目的 137
17.2　实训任务 137
17.3　背景知识 137
17.3.1　FTP 的工作方式 137
17.3.2　匿名 FTP 和用户 FTP 137
17.3.3　FTP 的应用 137
17.4　实训环境 138
17.5　实训内容及步骤 138
17.6　实训思考题 147
参考文献 148

实训一　使用协议分析工具 Sniffer pro 学习 TCP/IP 协议

1.1　实训目的

（1）掌握 Sniffer pro 基本功能的使用及熟悉其基本的设置；

（2）学会使用 Sniffer pro 捕获数据包，根据设计的具体应用对所捕获的数据包进行协议分析。

1.2　实训任务

（1）在一台装有 Windows Server 2003 计算机上部署 FTP 服务，在另一台装有 Windows Server 2003 计算机上安装 Sniffer pro，且作为 FTP 客户端；

（2）熟悉 Sniffer pro 的基本设置及功能使用；

（3）使用 Sniffer pro 捕获 FTP 命令操作过程中的所有数据包并对其进行分析。

1.3　背景知识

1.3.1　ISO OSI/RM

在遍及世界各地的网络中，人们使用不同厂商生产的主机、服务器、路由器、交换机、网络打印机等网络设备，并且在它们上面运行了多种操作系统。这些不同厂商生产的、运行不同操作系统的网络设备要实现数据共享，就必须遵循同一种规则。

1977 年，国际标准化组织（International Organization for Standardization，ISO）的技术委员会 TC97 成立了一个新的技术委员会 SC16 专门研究“开放系统互联（Open Systems Interconnection）”，并于 1983 年提出了标准化开放式计算机网络层次结构模型——开放系统互联参考模型（Open System Interconnection Reference Model，OSI/RM）。

OSI 参考模型包括了体系结构、服务定义和协议规范三级抽象。OSI 参考模型的体系结构定义了一个七层模型，用以进行进程间的通信，并作为一个框架来协调各层标准的制定；OSI 参考模型的服务定义描述了各层所提供的服务，以及层与层之间的抽象接口和交互用的服务原语；OSI 参考模型各层的协议规范，精确地定义了应当发送何种控制信息及用何种过程来解释该控制信息。

OSI 七层模型从上至下依次为应用层（Application Layer，AL）、表示层（Presentation Layer，

PL)、会话层（Session Layer，SL)、传输层（Transport Layer，TL)、网络层（Network Layer，NL)、数据链路层（Data Link Layer，DLL）和物理层（Physical Layer，PHL)。

1.3.2 TCP/IP 体系结构

OSI 参考模型的复杂性阻碍了其在计算机网络领域的实际应用。在现实网络世界里，TCP/IP 参考模型获得了更为广泛的应用。实际上，也是目前因特网范围内运行的唯一一种协议。

TCP/IP 协议栈是美国国防部高级研究计划局计算机网（Advanced Research Projects Agency Network，ARPANet）和其后继因特网使用的参考模型。它是以 OSI 参考模型为框架开发出来的，也是一种分层协议。TCP/IP 分层模型（TCP/IP Layering Model）被称作因特网分层模型（Internet Layering Model)、因特网参考模型（Internet Reference Model)。图 1–1 是 TCP/IP 分层模型和 OSI 参考模型的对比示意图。

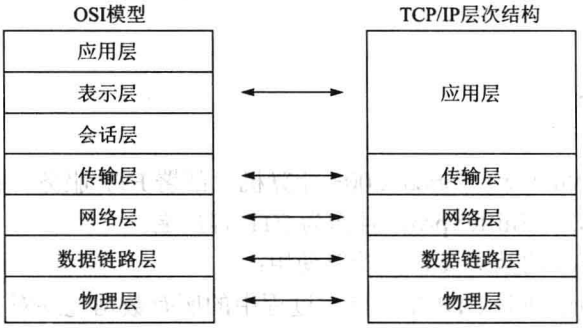


图 1–1 TCP/IP 层次结构与 OSI 参考模型的比较

TCP/IP 分层结构分为 5 个层次：应用层、传输层、网络层、数据链路层和物理层，如图 1–1 所示。TCP/IP 分层结构将 OSI 参考模型的应用层、表示层和会话层统一整合成一个单一的应用层，从而使数据格式的表示、会话的建立等功能和应用软件更紧密地结合起来，与 OSI 参考模型相比更为简单和实用。

虽然习惯上把 TCP/IP 称为协议，实际上它并不是一个单一的协议，而是一组协议的集合，称为 TCP/IP 协议族。表 1–1 展示了 TCP/IP 协议族的基本组成结构。

表 1–1 TCP/IP 协议族的基本组成结构

Telnet（虚拟终端协议）	FTP（文件传输协议）	SMTP（电子邮件传输协议）	DNS（域名服务）	其他协议（如 HTTP 等）
TCP（传输控制协议）		UDP（用户数据报协议）		
IP（网际协议）	ICMP（网际控制报文协议）	ARP（地址解析协议）		RARP（反向地址解析协议）

在 TCP/IP 协议族里，每一种协议负责网络数据传输中的一部分工作，为网络中数据的传输提供某一方面的服务。正是由于有了这些工作于各个层次的协议，使整个 TCP/IP 协议族能

够有效地协同工作。

1.3.3　各层的基本任务及其常用协议

1. 应用层

应用层位于 TCP/IP 协议族的最上层，在应用层中包括了一些高层协议，如 Telnet，FTP，SMTP，DNS，HTTP 等。不同的协议负责网络数据传输中的不同工作，如：Telnet 协议可以让用户登录到远程主机上进行操作；FTP 协议保证了数据能够有效地在主机间进行传输；SMTP 协议是专用于传送电子邮件的协议；DNS 协议用于将主机名和 IP 地址形成一对一或多对一的映射关系；HTTP 协议用于搜索 WWW 上的超文本；等等。

2. 传输层

传输层主要负责端到端的通信，源端的应用进程通过传输层，可以与目的端的相应进程进行直接会话。

在一台网络主机上，发送给网络上其他主机的数据流从应用层向下传递到传输层，并且在这一层被分割封装成“数据段（Segment）”。在向数据段中添加必要的传输层控制信息后，传输层将数据段向下传送给网络层进行处理；同时，该主机所接收的数据信息在经过网络层处理之后，向上传递到传输层，由传输层将这些数据段组装成数据流后向上传送给应用层进行处理。

传输层为数据提供可靠传输和不可靠传输两种传输方式。

TCP 协议是一个面向连接的数据传输协议，它提供数据的可靠传输。TCP 协议在把数据完整地传送到网络中的目的端的同时，对数据进行监控、纠错和重发，并且进行数据流量控制，即确保发送方的发送能力和接收方的接收能力实时、一致。但是 TCP 协议保证数据传输可靠性的这些操作，使得 TCP 协议传输数据的延迟时间大于 UDP 协议传输数据的延迟时间。

UDP 协议是一种提供无连接服务的协议。当希望减少数据在传输过程中的延迟时间时，可以使用 UDP 协议传输数据。UDP 协议提供的传输是不可靠的，它虽然实现了快速的请求与响应，但是不具备纠错和数据重发功能。

3. 网络层（IP 层）

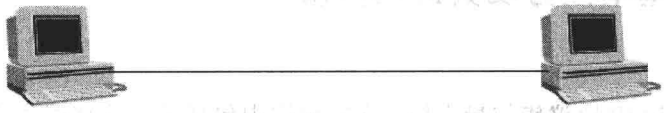
在 TCP/IP 协议族中，有多个协议工作在网络层上，如网际协议（IP）、网际控制报文协议（ICMP）、地址解析协议（ARP）、反向地址解析协议（RARP）。其中，IP 协议是一个非常重要的协议。它负责对传输层传递来的数据段进行封装，通过在其中添加 IP 地址等网络层信息，将数据段封装成数据包，并且将数据包进行无连接地传送。也就是说，IP 协议的数据传输也是无顺序的、不可靠的。它的可靠性依靠传输层的 TCP 协议提供。

另外，在网络层的其他协议中，ICMP 协议在 TCP/IP 协议族中负责发送出错和控制信息。ARP 和 RARP 负责 IP 地址与 MAC 地址之间的映射和反向映射。

1.4　实训环境

如图 1–2 所示，主机 A 安装 FTP 服务，作为 FTP 服务器，IP 地址为 192.168.0.1；主机

B 作为 FTP 客户端，并且安装协议分析工具 Sniffer Pro，IP 地址为 192.168.0.2。两台计算机都安装了 Windows Server 2003 系统。



主机 A（FTP 服务器，192.168.0.1）　　主机 B（FTP 客户端，安装 Sniffer pro，192.168.0.2）

图 1–2　实训环境

1.5　实训内容及步骤

1. Sniffer pro 界面熟悉

（1）监视器–仪表板。在此窗口中，共显示了 3 个仪表板：Utilization%、Packets/s 和 Errors/s，如图 1–3 所示，这 3 个仪表板分别用来显示网络利用率、传输的数据和错误统计，它们的作用如下。

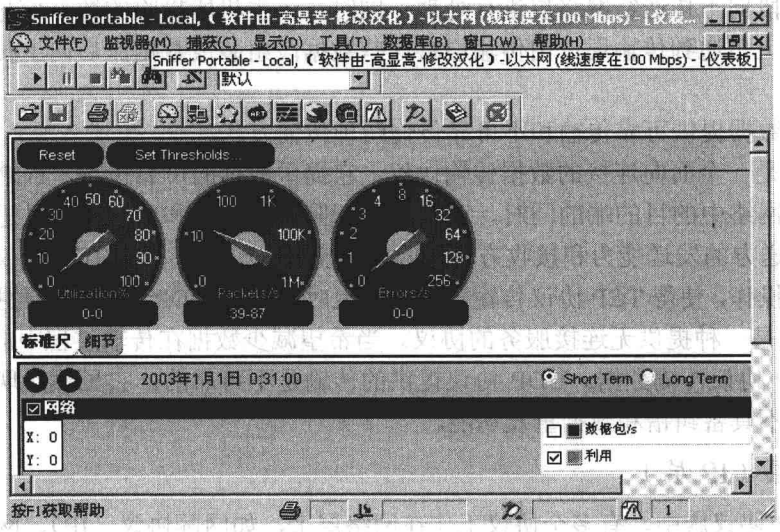


图 1–3　监视器–仪表板

① Utilization%（利用率百分比）：用传输量与端口能处理的最大带宽值的比值来表示线路使用带宽的百分比。表盘的红色区域表示警戒值，表盘下方有两个数字，第一个数字代表当前利用率百分比，第二个是最大的利用率百分比数值。监控网络利用率是网络分析中很重要的部分。表示网络利用率的理想方法要因网络不同而改变，而且很大程度上要取决于网络的拓扑结构。在以太网端口，利用率为 40%，效率可能已经很高了，但是在全双工可转换端口，80%的利用率才是高效的。

② Packets/s（每秒传输的数据包）：显示当前数据包的传输速度。同样，红色区域表示警戒值，下方的数字显示当前的数据包传输速度及其峰值。根据数据包数率可以得出网络上流量类型的一些重要信息。例如：如果网络利用率很高，而数据包传输速度相对较低，则说

明网络上的帧比较大；而如果网络利用率很高，数据包传输速度也很高，说明帧比较小。通过查看规模分布的统计结果，可以更详细地了解帧的大小。

③ Errors/s（每秒产生的错误）：该表盘可显示当前出错率和最大出错率。不过，并非所有的错误都产生故障。例如，以太网中经常会发生冲突，并不一定会对网络造成影响，但过多的冲突就会带来问题。

（2）监视器–主机列表。如图 1–4 所示，在该对话框左侧，可以单击不同的按钮，使该主机列表以不同的图形显示，如列表、柱形、圆饼形等。

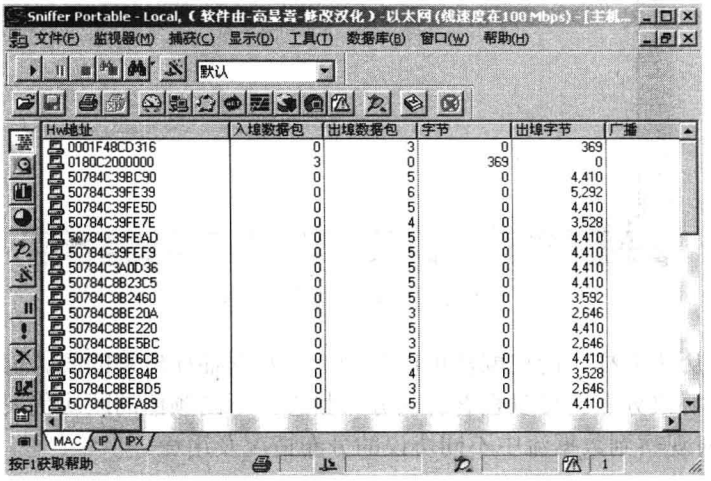


图 1–4　监视器–主机列表

（3）监视器–矩阵。如图 1–5 所示，该窗口会监控本地网络与外部网络的连接情况，并将源地址与目标地址的连接用直线表示。不过由于连接点太多而过于密集，用户难以看清楚各连接点的源地址和目的地址，此时可在该窗口上右击，选择快捷菜单中的“zoom”子菜单中的比例值来扩大图形，如 300%，500%等。该蓝色圆中的各点连线表明了当前处于活跃状态的点对点连接，也可通过将鼠标放在 IP 地址上右击“àshowselectnodes”查看特定的点对多点的网络连接。

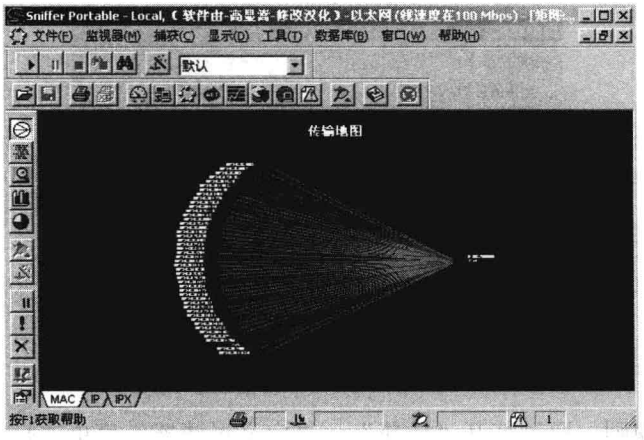


图 1–5　监视器–矩阵

（4）监视器–请求响应时间。如图 1–6 所示，请求响应时间通过不同主机间通信的最小、最大、平均响应时间方面的信息揭示回应时间，对解决 Web Server，FTP Server 和 Database Server 反应过慢十分有用。

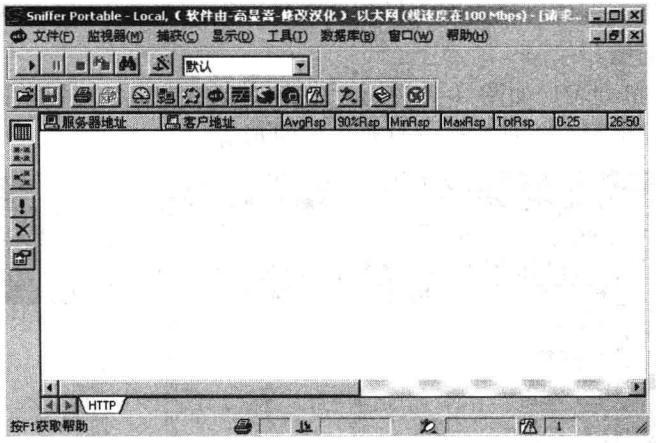


图 1–6 监视器–请求响应时间

（5）监视器–历史取样。历史取样可以看到历史数据抽样出来的统计值。

（6）监视器–协议分布。可以查看协议分布状态，不同颜色的区块代表不同的网络协议，协议分布可以实时观察到数据流中不同协议的分布情况及用途。

2. 使用 Sniffer 捕获数据包

本实例利用 Sniffer 工具捕获 FTP 命令操作过程中的所有数据包，然后对 Sniffer 工具中捕获的每一部分数据包的含义进行了详细的阐述，最后总结归纳出 TCP/IP 协议中网络接口层、网络层、传输层的数据报文结构，从而使大家加深对 TCP/IP 协议各层数据报结构的理解并掌握。

（1）选择网络适配器。在进行流量捕获之前，首先打开“文件”→“选定设置”菜单选择网络适配器，确定从计算机的哪个网络适配器上接收数据，如图 1–7 所示。如果安装了 EnterNet500 等 PPPoE 软件还可以选择虚拟的 PPPoE 网卡。

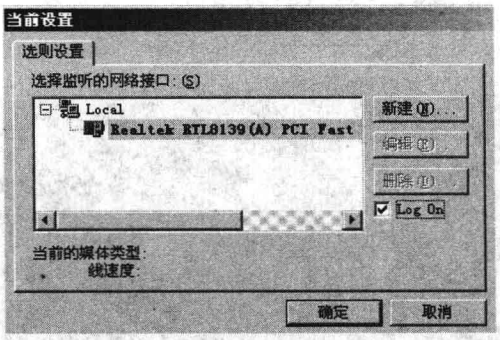


图 1–7 选择网络适配器

（2）定义捕获规则。通过打开“捕获”→“定义过滤器”菜单或打开“显示”→“定义过滤器”菜单可以设置过滤器的地址过滤规则，如图 1–8 所示。

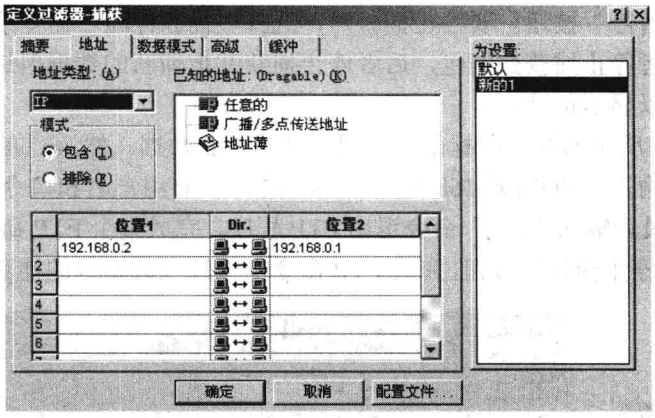


图 1–8　设置过滤器的地址过滤规则

① 地址。在图 1–8 的“地址类型”选项区域中可以设置 MAC 地址、IP 地址和 IPX 地址。以 IP 地址过滤为例，说明捕获主机 A 与主机 B 的信息。在“模式”选项区域中，选中“包含”单选按钮（选中“排除”按钮表示捕获除此地址外所有的数据包）。在位置 1 的任意一文本框中输入主机 B 的 IP 地址如 192.168.0.2，对应的位置 2 文本框输入主机 A 的 IP 地址如 10.20.44.62，单击该行 Dir.列的图标，  表示捕获位置 1 收发的数据包；  表示捕获位置 1 发送的数据包；  表示捕获位置 1 收到的数据包。选择捕获数据包的方向就完成地址的定义。

② 高级。设置完地址后，再选择“高级”标签，可以编辑协议的捕获条件。如图 1–9 所示，在协议选择树中罗列了所有可以捕获的协议，缺省时表示捕获所有协议。在“数据包大小”选项区域中，可以定义捕获包的大小，设置等于、小于、大于某个报文长度的值。在“数据包类型”选项区域中，可以选择当网络出现错误时是否捕获。选中 IP→TCP→FTP 复选框，单击“确定”按钮，即已定义好过滤器。

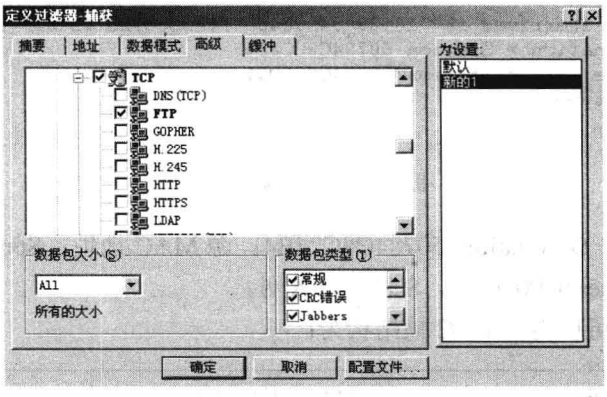


图 1–9　编辑协议的捕获条件

（3）捕获数据。在工具栏中可以看到捕获报文的工具按钮，如捕获开始、捕获暂停、捕获停止、捕获停止并查看、捕获查看、捕获条件编辑、选择捕获条件等。这些工具按钮对应的菜单命令也可以在“捕获”菜单中找到。捕获前需要单击“开始”按钮启动捕获引擎。暂

停捕获时，单击“暂停”按钮。要停止捕获时，选择“捕获停止”命令或者单击“捕获停止并显示”按钮，前者停止捕获数据包，后者停止捕获并把捕获的数据包进行解码和显示。单击“显示”按钮可以显示记录。

单击如图 1–10 所示的红色框标出的按钮，开始捕获数据。然后，在 FTP 客户端上进入 DOS 提示符窗口，输入“FTP 192.168.0.1”命令，输入 FTP 用户名和口令，登录 FTP 服务器，进行文件的下载，最后输入“bye”命令退出 FTP 程序，完成整个 FTP 命令操作过程。最后，单击 Sniffer 中的“停止捕捉”按钮，完成 FTP 命令操作过程数据包的捕获，并显示在屏幕上。

图 1–10 开始捕获数据

（4）捕获数据包后的分析工作。选择“解码”选项，对每个数据包进行解码，可以看到整个包的结构，从链路层到应用层的信息以及相应的十六机制编码，事实上，Sniffer 的使用中大部分的时间都花费在这上面的分析，同时也对使用者在网络的理论及实践经验上提出较高的要求。解码的显示通常分为 3 部分，目前大部分此类软件都采用这种结构显示。

下面对 Sniffer 捕获的底层数据包进行详细的介绍。

① 网络接口层 DLC 帧结构详解。如图 1–11 所示，在 Sniffer 捕获的 DLC 数据帧中依次包括以下信息。

```
DLC:  ----- DLC Header -----
DLC:
DLC:  Frame 1 arrived at  16:39:34.3040; frame size is 62 (003E hex) bytes.
DLC:  Destination = Station 50784C8C24B4
DLC:  Source      = Station 50784C8C1D31
DLC:  Ethertype   = 0800 (IP)
DLC:
```

图 1–11 DLC 帧头信息

目的 MAC 地址：Destination=50784C8C24B4；源 MAC 地址：Source=50784C8C1D31；以太网类型：Ethertype=0800（IP），8 表示以太网。

通过上述分析，可以得出 DLC 帧结构为：

目的 MAC 地址（6B）	源 MAC 地址（6B）	以太网类型（2B）

② 网络层 IP 数据报结构详解。如图 1–12 所示，IP 数据报中依次包括以下信息。

- Version=4：表示 IP 协议的版本号为 4。该部分占 4 位。
- header length=20 bytes：表示 IP 包头的总长度为 20 个字节。该部分占 4 位，单位为 4 个字节，因此，一个 IP 包头的长度最长为 1111，即 15×4=60 个字节。