全国高等农林院校“十二五”规划教材

计算机网络实验实践技术实用教程

JISUANJI WANGLUO SHIYAN SHIJIAN JISHU
SHIYONG JIAOCHENG

肖洪生　郑苑丹　主编

中国农业出版社

全国高等农林院校“十二五”规划教材

计算机网络实验实践技术实用教程

肖洪生　郑苑丹　主编

中国农业出版社

图书在版编目（CIP）数据

计算机网络实验实践技术实用教程/肖洪生，郑苑丹主编．—北京：中国农业出版社，2014.11
全国高等农林院校“十二五”规划教材
ISBN 978-7-109-19627-8

Ⅰ.①计… Ⅱ.①肖…②郑… Ⅲ.①计算机网络—实验—高等学校—教材 Ⅳ.①TP393-33

中国版本图书馆 CIP 数据核字（2014）第 226298 号

中国农业出版社出版
（北京市朝阳区麦子店街 18 号楼）
（邮政编码 100125）
策划编辑 朱 雷
文字编辑 李兴旺

北京中新伟业印刷有限公司印刷 新华书店北京发行所发行
2014 年 12 月第 1 版 2014 年 12 月北京第 1 次印刷

开本：787mm×1092mm 1/16 印张：15.75
字数：352 千字
定价：30.00 元
（凡本版图书出现印刷、装订错误，请向出版社发行部调换）

内容简介

本教材内容涵盖计算机网络、网络工程、网络安全三个方面的实验、实践中的实用技术，从组网与接入互联网、网络数据包分析、应用服务器搭建，到路由器、交换机配置，路由协议配置，高级组网技术；再到网络安全实验环境搭建，字典攻击与密码破解、PGP应用，网络攻击（DDoS）与控制（木马）的应用与预防，网络防御高级技术；对计算机网络常见应用技术都有涉及。

本教材重点在于从实践方面给出引导，便于读者自学，可作为本科电子信息类专业学生学习和掌握计算机网络应用技术、独立开设实验课的教材，或配合网络类课程作为实验教学教材，也可用于网络应用技术培训参考，亦可供组网工程技术人员、网络管理人员参考。

前言

信息社会的大厦是在计算机网络的基础上建成的，信息社会的形成、发展与纵深前行，与计算机网络技术的发展相伴而行，而网络基础架构的建立、维护、安全等实用技术对信息社会的运行至关重要。

在电子信息类专业人才培养过程中，网络技术相关理论的学习和实践技能训练，是必不可少的。培养网络使用与维护的专业人才群体，在网络实践技能训练方面如何精选内容，改革教学模式与教学手段，提高培养人才的质量和效益，是笔者及同事们一直关注并为之而努力探索的课题。

在专业实验教学平台支撑下，开设独立实验课，将实际应用技能训练构成一个相对完整的教学体系，是笔者与同事们近年来一直为之努力的主要工作。在笔者前一本书《计算机网络技术实验教程》为本校网络实验教学平台和内容主线的基础上，在时间推移与网络设备更新、独立实验课教学实践经验积累、专业实验教学平台的升级等需求推动下，升级内容，拓宽知识面，切合实际，强调实用及实践，按照理论课教材的章节结构，重新组织、扩充教学内容，撰写推出本教程。

本教程内容涵盖计算机网络、网络工程、网络安全3个方面的实验、实践中的实用技术，共分为10章，各章内容扼要介绍如下：

第1章是局域网组建与互联网接入，包括串口通信、双绞线制作、局域网组建、无线宽带网接入、常用网络命令使用诸多内容。

第2章是网络数据包捕获与分析，运用工具软件捕获网络数据包，对ARP、IP、ICMP、TCP、UDP、HTTP等常见数据包进行分析，对“TCP三次连接”过程分析、邮箱密码捕获等操作也有较多涉及。

第3章是网络服务配置与网页设计内容，对配置Web、FTP、电子邮件、DNS、DHCP服务器都有详细介绍，对HTML静态网页设计也有一定的介绍。同时提供一个时间为一周的网络基础课程设计内容，对第1、第2、第3章实验内容的综合运用，组网，配置服务器，到对网络数据包内容分析全部包含在内，设计任务、进度安排、设计指导、评分标准一应俱全。

第4章是路由器、交换机应用基础，介绍路由器、交换机的配件及工作原理，更重要的是如何访问、配置它们，了解其多种工作模式及其相互关系，静态路由、默认路由的配置与转发原理。

第5章是路由协议配置，主要介绍RIP、OSPF协议的原理与配置，对动态路由选择的实现有较为详细的介绍。

第6章是路由交换高级配置，主要是虚拟局域网技术应用，其域间路由、生成树协议、访问控制列表等内容有详细介绍，同时提供一个网络工程课程设计内容，同网络基础课程设计一样同，是对第4、第5、第6章内容的综合应用，其模式相同。

第7章是网络扫描与嗅探，是建立网络安全实验环境的基础内容，包括虚拟机配置、安装，网络扫描，嗅探3部分内容。

第8章是字典攻击、密码破解，以及PGP应用等内容。

第9章是网络攻击与控制，主要介绍DDoS攻击、典型木马（冰河、灰鸽子）控制实例应用与预防。

第10章是网络防御高级技术，介绍证书应用、常见备份与恢复工具使用、网络卫士、防火墙、入侵检测工具使用等非常实用的内容，同时提供一个网络安全综合设计内容，是对第7、第8、第9、第10章内容的综合应用，同前面网络基础、网络工程课程设计模式相同。

本教程旨在建设网络实验教学平台，开设独立、系统的网络技术实验课，配套计算机网络、网络工程、网络安全3门理论课，可根据设备实际和教学要求，每章安排3～4学时，也可只选其中某些章节，总共安排30学时左右。如果前述课程的实验学时分散到各门课程中，用本教程作为其配套实验教材，也是合适的。对于开设计算机网络理论课程，再开设网络技术实验课程，不再专门开设网络工程、网络安全后续两门网络类课程的专业，可作为重视技能培养的教学改革尝试教材。

在本教材的编著过程中，肖洪生老师编写、调试了第1、第2、第3章和第6、第7、第8、第9、第10章的全部实验内容，并对全书统稿；郑苑丹老师编写、调试了第4、第5、第6章的内容。本校信息学院网络课程组的许多老师在网络教学实践中，也提出了许多宝贵意见，对本书的撰写有重要的参考作用，在此表示感谢。

本教程在编写过程中参考了国内外有关计算机网络的著作和文献，并查阅了大量的网络资料，在此对所有作者表示感谢。

对众多网络技术爱好者，在网络上无私地交流相关技术细节，使笔者在互联网的大山上淘到所需的技术之宝，对本教程内容的充实、个别技术细节的攻克、文字图形的引用等，帮助很大，但鉴于内容零散，数量众多，未能一一标出。唯有再次感谢众多网络技术派网友，以抚心中愧疚之意。

面对迅速发展的网络应用技术，本教程只是网络技术中的沧海一粟，错误或不妥之处在所难免，欢迎广大读者批评指正，并可通过 hs _ xiao2002@163.com 与笔者交流探讨。

肖洪生

2014年6月于广东海洋大学

目录

第1章

局域网组建与互联网接入

组建局域网是网络实验技术的入门级内容，宽带网接入技术亦是社会应用的基本需求，传感网接入计算机网络时，常用串口通信。本章内容旨在对这3方面的内容，在阐述基础理论的前提下，提出相应的实验训练内容，在实验过程中体会、掌握相应的技能。

本章3项实验内容的基本任务部分属于验证性或操作性实验，组合起来就是一个综合性、设计性的实验。

1.1 RS232串口通信

1.1.1 RS232接口标准

RS232接口标准是美国电子工业协会（EIA）在20世纪60年代初推荐使用的串行通信标准，是数据终端设备（DTE）与数据通信设备（DCE）之间的接口标准，RS232在通信系统中的位置如图1-1-1所示。

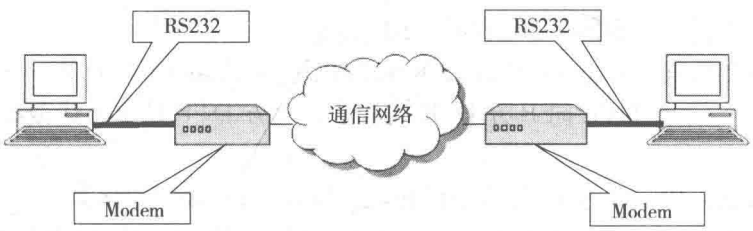

图1-1-1 RS232在通信系统中的位置

图1-1-1中，PC是数据终端设备；调制解调器（Modem）是数据通信设备；RS232是DTE与DCE之间的通信电缆，RS232即是这两者之间的通信接口技术标准。

DTE是PC、I/O设备等，面对用户收/发数据。DCE是将DTE与网络相连的通信设备，负责编码、解码、数据链路建立、维持、释放的设备，如拨号上网的调制解调器等。

物理层通信更新的标准有EIA RS499、IT-U V.24等，其性能比RS232好得多，但由于RS232标准应用早，使用广泛，至今还是计算机上的基本配置之一。RS232串行通信口及通信电缆如图1-1-2所示。

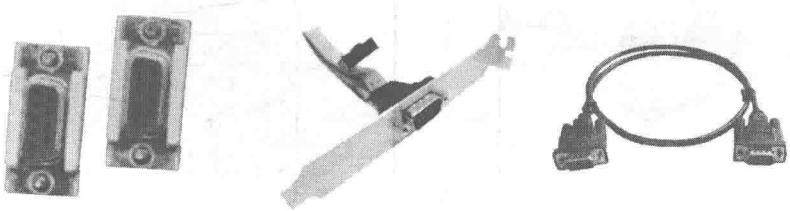

图1-1-2 RS232串行通信口与通信电缆

RS232 接口标准规定，在 DTE（计算机）上为针，DCE（Modem）上为孔。

RS232 最初的标准为 DB-25，即有 25 根信号线，其中包括主信道、辅助信道，及少数空置信号线（功能待以后扩充）几个部分。现在常用 DB-9 连接器，仅有主信道，其 9 根信号线的功能特性如表 1-1-1 所示。

表 1-1-1　DB-9 连接器各信号线功能与方向

序号	信号名称	功能	信号方向
1	DCD	数据载波检测	DCE→DTE
2	RxD	接收数据	DCE→DTE
3	TxD	发送数据	DTE→DCE
4	DTR	数据终端就绪	DTE→DCE
5	GND	信号地	—
6	DSR	数据通信设备就绪	DCE→DTE
7	RIS	请求发送	DTE→DCE
8	CTS	允许发送	DCE→DTE
9	RI	振铃指示	DCE→DTE

1.1.2　RS232 工作过程

RS232 的工作过程可用图 1-1-3 表示，其中④、⑥、⑦、⑧、③、②为信号线序号。

（1）建立连接阶段。A 方 DTE 终端准备就绪后④，A 方 DCE 向 A 方 DTE 确认⑥；B 方 DCE 就绪时⑥，B 方 DTE 向 B 方 DCE 确认④；A 方 DTE 请求发送数据⑦，A 方 DCE 允许发送⑧。

（2）发送数据阶段。A 方 DTE 发送数据③，B 方 DTE 接收数据②。

（3）三线制串口通信。在计算机之间（如 PC 和 PC、PC 和单片机或其他智能仪器）直接用 RS232 通信时，可不用建立连接，将本方的数据发送线连接到对方的数据接收线，信号共地即可；这样，通信双方一直处于工作就绪状态，不用建立连接，可直接发、收数据。

如图 1-1-4 所示，三线制通信接线方式是“2—3 交叉，5—5 对接”，其余悬空，仅用 3 根信号线，就可实现两计算机之间串口通信。

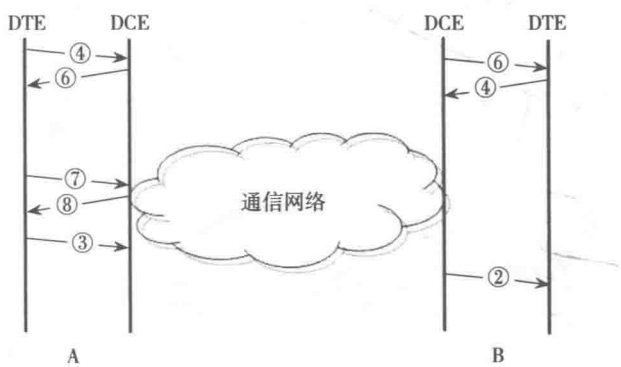

图 1-1-3　RS232 工作过程示意

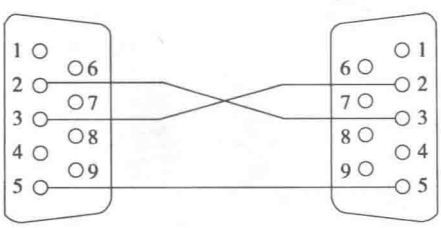

图 1-1-4　三线制通信接线

1.1.3　串口通信调试工具

(1) USB 转 RS232。目前 PC，尤其是笔记本电脑，串口配置越来越少，常用 USB 口代替串口进行通信，这需要用到一根 USB 转 RS232 通信电缆，如图 1-1-5 所示。

安装相应驱动程序 PL-2303 Driver Installer. exe，在 USB 转 RS232 电缆接入时，从桌面的“计算机—属性—设备管理器—端口”就可以看到，系统多出一个 COM5 端口，就是 USB 转换出来的，如图 1-1-6 所示。当然，端口序号也可以人工改变。

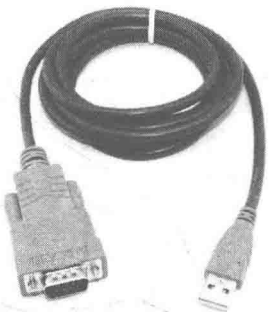

图 1-1-5　USB 转 RS232 通信电缆

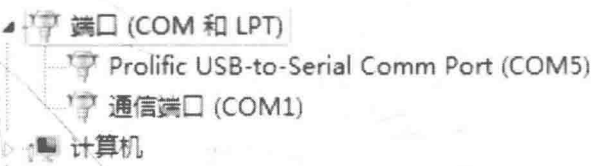

图 1-1-6　驱动安装成功后

利用 USB 转 RS232 软硬件技术，USB 通信与串口通信完全一致，在软件编程开发时尤其方便。

(2) RS485 通信接口。如前所述，RS232 是 20 世纪 60 年代初的技术标准，相对陈旧，主要指标有：传输距离 15～30m，传输率最高 20Kb/s，接口电平 (5～15V)，相对较高，元器件易损，共地传输易产生共模干扰，传输系统抗噪声干扰能力差。

串口通信标准在 RS232 之后，又有一系列与 RS232 是相兼容的系列标准被制定出来，如 V. 24、RS 449、V. 35、X. 21 等，都是 RS232 接口的升级标准，但诸多原因，这些升级的串口通信标准都没能取代 RS232 而成为市场主流。

近些年来，大量使用的 RS485 接口标准，与 RS232 配合相得益彰，市场应用效果较好。

RS485 主要指标有：传输距离最远可达 1200m，传输率最高 10Mb/s，接口电平(±2～6V) 较低，元器件寿命长，差分放大抗干扰能力强，更重要的是，用 RS 485 接口可在一条总线上连接多个收发器，构成总线式网络。

RS232 对 RS485 转换器实物如图 1-1-7 所示。

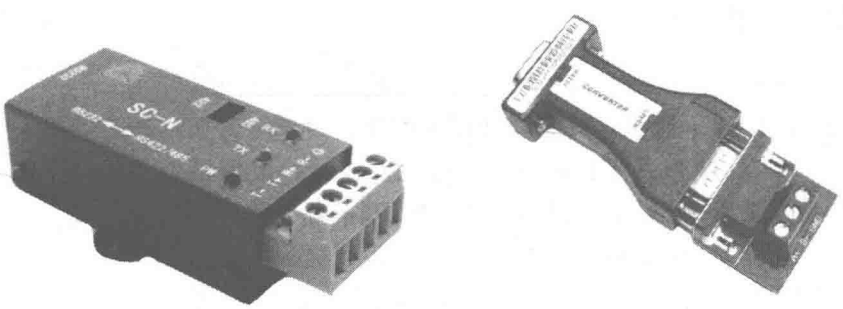

图 1-1-7　RS232 和 RS485 通信接口转换器

1.1.4 串口通信软件——串口大师

将串口交叉通信 RS232 电缆连接两台 PC，双击运行“ComMaster”（串口大师）应用程序图标，出现如图 1-1-8 所示的界面。

图 1-1-8 串口大师应用程序界面

在串口大师的应用界面上，有多个应用界面卡片，分别用于串口调试、测试、监视、过滤等，读者可在应用中进一步熟悉。这里只简单介绍如何实现双机通信操作。

在如图 1-1-8 所示的串口调试界面中，通信端口、参数选择完成后，单击“打开串口”按钮（打开串口后，该按钮变为“关闭串口”），在发送区写入发送内容字符串，单击“发送”按钮，对方的信息接收区即可收到所发字符串；当然，也可以发送文本文件，或周期多次发送信息等，可容易验证之。其他众多功能也可容易地使用，不再赘述。

要说明的是，串口大师只能辨认出本机上真实的串口，对用 USB 口模拟出来的串口探测不到。

1.2 双绞线制作与局域网组建

1.2.1 双绞线规格及接线

（1）型号与规格。双绞线是最常用的网络传输媒体，由四组双绞线组成，如图 1-2-1 所示。其型号 10BASE-T、100BASE-T 是指 10Mb/s、100Mb/s 以基带传输方式工作的双绞线。按信号线外面有无屏蔽保护层可分为：屏蔽双绞线（STP），有金属网丝套作为屏蔽层，无分类；无屏蔽双绞线（UTP），没有屏蔽层，有多个分类，如 UTP-3、UTP-5、UTP-5＋多个类别。目前常用 UTP-5 类线，用于 100Mb/s 基带网络传输；STP 与 UTP-5 的主

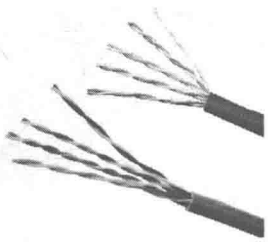

图 1-2-1 双绞线

要电气性能比较见表 1-2-1。

表 1-2-1　STP 与 UDP-5 主要电气性能比较

双绞线	传输率/Mb/s	100m 衰减/dB	近端干扰/dB	价格
STP	100	6.2	38.5	高
UTP-5	100	22.0	32	低

由表 1-2-1 可见，在双绞线规定的最大网段长度（100m），STP 衰减较小，UTP 较大，但 STP 近端干扰较强，且价格略高；在实际应用中，100Mb/s 局域网多采用 UTP-5 类线作为有线传输媒体。

（2）RJ-45 水晶头。它是一种只能沿固定方向插入并自动防止脱落的塑料接头，俗称“水晶头”。双绞线的两端必须都安装这种 RJ-45 插头，以连接网卡与交换机，实现网络通信。

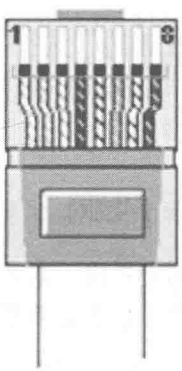

图 1-2-2　RJ-45 连接器

RJ-45 连接器（RJ-45 是一种网络接口规范，类似的还有 RJ-11 接口，用来连接电话线）的双绞线由 8 根不同颜色的信号线分成 4 对绞合在一起，成对扭绞的作用是尽可能减少电磁辐射与外部电磁干扰的影响。

RJ-45 水晶头由金属片和塑料外壳构成，前端 8 个凹槽内的金属触点共有 8 个；RJ-45 水晶头引脚序号是：金属片面对我们时，从左至右，引脚序号是 1 至 8，如图 1-2-2 所示。

双绞线的最大传输距离为 100m。如果要加大传输距离，在两段双绞线之间可安装中继器，最多可安装 4 个中继器。如安装 4 个中继器连接 5 个网段，则最大传输距离可达 500m。

EIA/TIA 的布线标准中规定了两种双绞线的线序 T568A 与 T568B，如图 1-2-3 所示。

568A 标准：白绿，绿，白橙，蓝，白蓝，橙，白棕，棕；

568B 标准：白橙，橙，白绿，蓝，白蓝，绿，白棕，棕。

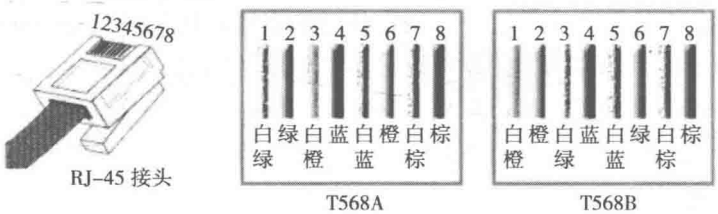

图 1-2-3　双绞线 T568A 与 T568B 线序示意

网络布线中，同一条网线两端要采用相同的接线方式，采用 568A 或 568B 均可；为了保持最佳的兼容性，普遍采用 EIA/TIA 568B 标准来制作网线。

在数据的传输中，为了减少和抑制外界的干扰，发送和接收的数据均以差分方式传输，即每一对信号线相互扭在一起传输一路差分信号（这也是双绞线名称的由来）。

（3）直通线与交叉线。

直通线（straight cable）：计算机与交换机（终端设备与通信设备）相连时采用，常用