



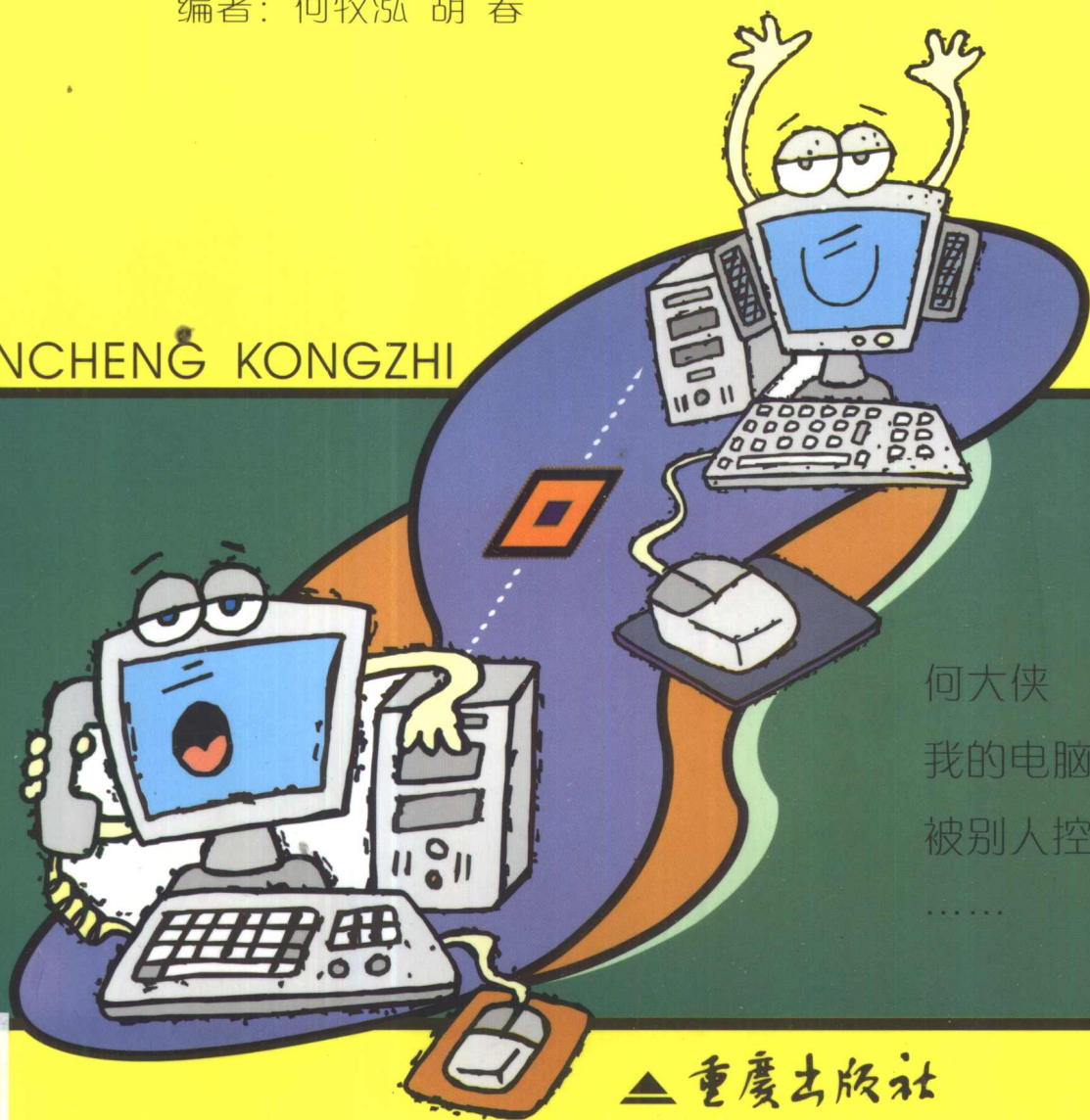
远程控制



主编：何牧泓

编著：何牧泓 胡 春

YUANCHENG KONGZHI



何大侠
我的电脑
被别人控制了
.....

▲ 重庆出版社

轻松玩转远程控制

主 编 何牧泓

编 者 何牧泓 胡 春

▲ 重庆出版社

内 容 提 要

远程访问、控制技术是软件技术支持消费中第三个增长最快的领域。本书通过几种典型的远程控制软件的介绍,让读者理解远程控制的原理,知道如何去选择远程控制软件、如何防范黑客利用远程控制软件进行的攻击以及怎样编制一个远程控制程序。本书可以让计算机初学者能够灵活使用书中介绍的远程控制软件,同时也给喜欢网络编程的朋友提供了一个如何编制远程控制程序的思路和基本实施方法。

图书在版编目(CIP)数据

轻松玩转远程控制 / 何牧泓主编. — 重庆: 重庆出版社, 2002.2

ISBN 7-5366-5620-3

I.轻… II.何…胡… III.遥控 IV.TP872

中国版本图书馆 CIP 数据核字 (2001) 第 094466 号

轻松玩转远程控制

编 著 何牧泓 胡 春

责任编辑 刘爱民 谢 先

*

重 庆 出 版 社 出 版、发 行

新 华 书 店 经 销

重 庆 电 力 印 刷 厂 印 刷

开本: 787 × 1092 1/16 印张: 19 字数: 410 千

2002 年 2 月第 1 版

2002 年 2 月第 1 次印刷

印数: 1-8 000

*

ISBN 7-5366-5620-3/TP · 85

定价: 25.00 元

序

一天，朋友的《轻松玩转远程控制》一书落稿，力邀本书为本书作序。随手翻开书稿前面几页，竟赫然瞥见敝人早先不慎之作 YAI “大名”在上，不禁惶惶然。回想当初，YAI 的出现曾引发太多争议，使得“远程控制”诡异莫测，实是有违初衷。时已两年有余，所幸 IT 发展迅猛，“黑客”、“病毒”、“木马”已不再是什么新鲜名词，人们对于发生在 Internet 这个新的生存空间里诸多的“另类”（借用时下流行网语）事情，已逐渐能以积极、理智、辩证的心态去审视和对待。认识的进步是必然的。而《轻松玩转远程控制》撩开了“远程控制”那已是薄薄的一层面纱，使之更大白于天下，借以普及网络安全知识，还“远程控制”本来面目，实是令我欣慰。

“远程控制”软件其实应用非常广泛，涉及远程教育、远程维护、远程医疗等等。Symantec 经典著名的 pcAnywhere 已经成为许多网络管理人员不可或缺的工具软件，在全球软件业更是有口皆碑。如今，计算机网络几乎无处不在，“远程控制”使人们具有了这样的能力，它可以超越地理、超越环境，延伸到原本遥不可及的位置。然而，这样的能力若被滥用，必被蒙上阴影，使之抹黑。“远程控制”是一柄锋利的双刃剑，既可

用于披荆斩棘，但也可能伤了别人、伤了自己。中华人民共和国公安部颁布了《计算机网络安全管理办法》，为中国互连网络制定了基本的行为准则，也是本书的必要辅助读物之一。

自 YAI 被人误用，引起轩然大波后，我已经停止了对其继续升级，并于 2 000 年底创建成立重庆爱思软件技术有限公司（<http://www.isofthome.com>），致力于网络安全软件产品开发，希望能为我国民族网络安全事业作一点点贡献。如果读者有兴趣，可以到我们网站做客，共同探讨网络安全的有关问题。

感谢本书出版人、《电脑报》东方工作室谭有彬先生的诚邀，盛情难却，在此妄言。

YAI 作者 杜 江

clouddu@yahoo.com

2001 年 12 月 24 日

前言

远程访问、控制技术从诞生到现在已经有很多年了——起初是为了让计算机用户不必在远程主机前进行操作而能访问远程主机硬盘中的信息，甚至可以通过计算机访问网络内的其他资源。今天，许多企业和增值分销商正在把远程控制能力作为有效的技术支持工具。IDC 预计远程控制软件市场将从 1998 年的 6.77 亿美元发展到 2002 年的 19 亿美元，年增长率达 31.5%，是软件技术支持消费中第三个增长最快的领域。

在家办公将成未来时尚。Gartner Group 预言，到 2002 年全世界将有 1 亿零 8 百万以上的人会经常不在办公室内工作。推动这个趋势的因素有：

(1) 移动的专业人员：便携式计算机将在商务旅行的人群中日益流行。便携式计算机将提高这些关键雇员的工作效率，并提供了关键的访问网络服务的能力。

(2) 电信：在大城市中，依靠越来越强的电信联系，可以减少上下班的乘车时间，这也符合当地改善环境、提高生活质量的要求。在一项由华盛顿邮报的 Web 站点进行的联机调查中，电信是 11 个改善工作环境的可选方式中的首选项。

(3) 远程 PC 用户：许多雇员——现场销售人员、技术服务人员、顾问及其他人员——实际上都不在公司总部工作，有些在部门的办公室工作，有些则在家里工作，他们总在离客户很近的位置，这样才能方便地访问客户。他们可能使用台式计算机或便携式计算机与公司总部联系。

(4) 改进的移动计算设备：便携式计算机、调制解调器、蜂窝服务以及其他远程系统和服务的不断改进和降价，正使移动计算设备更容易被人接受。这样，公司更倾向用移动访问设备装备他们的雇员。在许多公司中，便携式计算机已经成为雇员使用的惟一计算机了。

不在办公室工作的人数正在迅速增长，支持这些远程用户比支持在企业内工作的传统台式计算机用户要更复杂并且开销更大：当他们遇到问题时，不可能派技术人员

到现场去帮助解决；多数计算机只是偶尔连接到网络上并且通常是通过低带宽的电话线连接的，这样，移动计算机用户使用的软件就可能落后于本地用户一个或多个版本，而且更容易发生问题。因此，信息技术管理人员和增值分销商不断寻求更经济的途径，以解决位于企业总部之外的台式计算机和便携式计算机的技术支持问题，这就促使远程控制技术得以快速的发展并日趋完善。

随着远程控制技术逐渐进入人类的生活、工作领域，在互联网中黑客利用远程控制技术对用户计算机进行攻击、偷窃资料、破坏文件等行径时有发生。而我们看到市场上没有一本系统地介绍远程控制技术的原理、远程控制软件编制过程以及远程控制软件使用的书籍，这样我们就编写了这本《轻松玩转远程控制》。

本书由何牧泓同志主编，何牧泓和胡春编著。参与本书审校、录排工作的还有王群先生。王群先生对本书的出版给予了很大的支持和帮助，在此表示衷心的感谢。由于作者水平有限，时间比较仓促，书中错误和缺漏在所难免，恳请广大读者批评指正。

作者

2001 年 10 月 24 日

目录

第一章 远程访问、控制原理	1
1.1 远程访问、控制简述	1
1.1.1 远程访问、控制概念	1
1.1.2 客户/服务器模式 (Client/Server)	2
1.1.3 远程访问、控制的应用及其优缺点	2
1.2 远程访问、控制的原理	3
1.2.1 远程访问、控制的原理	3
1.2.2 远程访问、控制的连接类型	5
1.2.3 远程访问、控制数据链路控制协议介绍	11
1.3 远程访问、控制的分类及相关应用软件简介	12
第二章 Windows 内置的远程访问功能	13
2.1 在局域网中实现远程访问、控制	13
2.2 通过调制解调器实现远程访问、控制	18
第三章 Windows 终端的远程访问、控制	21
3.1 概述	21
3.1.1 通过 NT 实现 RAS	21
3.1.2 通过 3Com Access Builder 2000 实现 RAS	22
3.2 远程安装 Windows 2000	23
3.2.1 准备工作	24
3.2.2 安装 RIS	24
3.2.3 在活动目录中授权 RIS	25
3.2.4 设置所需用户的权限	26
3.2.5 客户机使用 RIS 安装操作系统的步骤	26

3.3	Windows 2000 的终端服务	26
3.4	利用 Win 2000 的 RunAs 特性进行远程管理	38
第四章	Windows XP 的远程桌面	43
4.1	主机的设置	43
4.2	客户机的设置	46
4.2.1	Windows XP 的客户端	46
4.2.2	一般 Windows 的客户端	48
4.3	IE 连接实战	51
4.4	Windows XP 用户实战	54
第五章	远程唤醒的设置与实现	59
5.1	远程唤醒的基本原理	59
5.2	远程唤醒的硬件需求	59
5.3	用调制解调器实现远程开机	60
5.4	用网卡实现局域网开机	61
5.5	自动关机	65
第六章	点对点的远程访问和控制实例	67
6.1	对点的远程访问、控制的程序实例	67
6.1.1	服务器端程序（被控端程序）	68
6.1.2	客户端程序（主控端程序）	72
6.1.3	运行结果	80
6.1.4	总结	81
6.2	监视远程主机的程序实例	82
6.2.1	服务器端程序（被控端）	82
6.2.2	客户端程序（主控端程序）	89
6.2.3	运行结果	110
6.2.4	总结	110
第七章	点对多的远程访问和控制实例	111
7.1	服务器端程序（主控端）	111
7.2	客户端程序（被控端）	125
7.3	运行结果	130
7.4	总结	131

第八章 远程访问及网络安全	133
8.1 远程访问带来的安全隐患	133
8.2 黑客的一般攻击方法和手段	135
8.2.1 查看他人的 IP 地址	136
8.2.2 查找可以入侵的主机	149
8.2.3 木马攻防	155
8.2.4 扫描器的使用	163
8.2.5 如何进攻 NetBIOS	169
8.2.6 黑客入侵 Win2000 Server 全过程详解	171
8.2.7 黑客突破 TCP/IP 过滤/防火墙进入内网	176
8.2.8 系统被入侵后的恢复	191
第九章 常用的远程控制软件	199
9.1 NetBus Pro	199
9.1.1 NetBus Pro 简介	199
9.1.2 NetBus Pro 安装与设置	200
9.1.3 NetBus Pro 功能剖析	205
9.1.4 防止攻击的秘诀——清除 NetBus Pro	211
9.2 RemotelyAnywhere Version 3.51	213
9.2.1 RemotelyAnywhere Version 3.51 简介	213
9.2.2 服务器端的安装	213
9.2.3 服务器端的运行	215
9.2.4 客户端的登录	215
9.2.5 客户端的操作	216
9.3 远程管理利器 SubSeven	222
9.3.1 SubSeven 简介	222
9.3.2 服务器端的设置	222
9.3.3 远程管理的基本操作	225
9.3.4 SubSeven 的清除	234
9.4 PCAnywhere 10.0	234
9.4.1 PCAnywhere 简介	234
9.4.2 PCAnywhere 的安装	235
9.4.3 PCAnywhere 的设置	237
9.4.4 使用 PCAnywhere	245
9.4.5 PCAnywhere 的卸载	249
9.5 NetSpy “网络精灵”	249
9.5.1 关于“网络精灵”远程监控系统	249
9.5.2 安装	250
9.5.3 网络精灵的使用	250

9.5.4	卸载	257
9.6	红蜘蛛软件 RED SPIDER	258
9.6.1	核心功能介绍及适用范围	258
9.6.2	软件安装	259
9.7	冰河	275
9.7.1	安装与基本使用	275
9.7.2	冰河的命令控制台	280
9.7.3	防范与清除冰河	283
9.8	虚拟远程桌面显示软件: VNC	285
9.8.1	VNC 的应用	285
9.8.2	VNC 的安装	285
9.8.3	VNC 的设置和连接	286
9.8.4	VNC 的高级应用	288
9.9	远程控制技巧	289
9.10	如何选择远程控制工具	291

第一章 远程访问、控制原理

网络从一诞生就已经具备了远程访问的能力，在网络上访问共享资源本身就是促使网络产生的基本原因。例如：在网络上访问共享文件；财务部门的职员利用网络上的打印机打印财务报表；在因特网查找资料以及上传自己的照片到 BBS 上等都是属于远程访问这一范畴。而远程控制技术，大概始于 DOS 时代，只不过当时由于技术上没有什么大的变化，网络不发达，市场没有更高的要求，所以远程控制技术没有引起更多人的注意。但是，随着网络的高度发展和 GUI 技术的成熟以及计算机的管理及技术支持的需要，远程操作及控制技术越来越引起人们的关注。

把远程控制叫做远程访问、控制我们认为更贴切。所以本书中所讲的远程访问、控制其实就是指远程控制。不过本书也将会在后面介绍一下远程访问的实例。好了，现在我们就开始了解和掌握远程访问、控制。

1.1 远程访问、控制简述

1.1.1 远程访问、控制概念

远程访问、控制用一个简单的概念来说就是允许用户对自身的网络资源进行访问和控制。远程访问、控制是在网络上由一台计算机（主控端 Remote/客户端）远距离地去控制另一台计算机（被控端 Host/服务器端）的技术，这里的远程不是字面意思的远距离，一般指的是通过网络控制远端电脑。当操作者使用主控端电脑控制被控端电脑时，就如同坐在被控端电脑的屏幕前一样，可以启动被控端电脑的应用程序，可以使用被控端的文件资料，甚至可以利用被控端电脑的外部设备（打印机、扫描仪等）和通信设备（调制解调器或者其他网络设备）来进行工作和访问互联网，就像利用遥

控器遥控电视的音量、变换频道或者开关电视一样。不过，有一个概念需要明确，那就是主控端电脑只是将键盘和鼠标的指令传送给远程电脑，同时将被控端电脑的屏幕信息通过通信线路回传过来。也就是说，我们利用被控端电脑进行操作似乎是在眼前的电脑上进行的，而实质是在远程的电脑中实现的，不论打开文件，还是上网浏览、下载，所有资料和 IE 浏览器的 Cookies 等都是存储在远程的被控端电脑中的。

要注意的是，远程访问、控制必须要有一个客户端程序和一个服务器端控制程序。客户端发送指令，服务器端接收指令并执行。如图 1.1 所示。

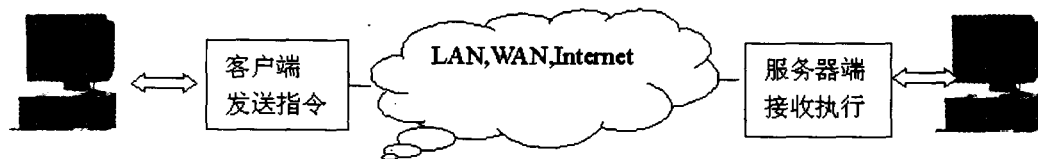


图 1.1

1.1.2 客户/服务器模式 (Client/Server)

说到远程访问、控制就一定要提到客户/服务器模式。

客户/服务器结构包括连接在一个网络中的多台计算机。那些处理应用程序、请求另一计算机服务的计算机为客户机 (Client)。而响应请求，并处理请求的计算机称为服务器 (Server)。

当客户机向服务器发出各种请求，服务器根据用户的请求对其进行相应的处理，然后将处理结果返回到客户机。

1.1.3 远程访问、控制的应用及其优缺点

远程访问、控制程序能够使用户突破地域的限制，在世界的每一个角落让远程主机执行特定的指令。下面来看看远程访问、控制技术有哪些应用：

1) 远程办公

这种远程的办公方式不仅大大缓解了城市交通状况，减少了环境污染，还免去了人们上下班路上奔波的辛劳，更可以提高企业员工的工作效率和工作兴趣。是实现 SOHO 工作方式的一种有效途径。

2) 远程技术支持

通常，远距离的技术支持必须依赖技术人员和用户之间的电话交流来进行，这种交流既耗时又容易出错。许多用户对电脑或设备知道得很少，然而当遇到问题时，他们必须向无法看到故障现象的技术人员描述问题的症状，并且严格遵守技术人员的指示精确地描述故障现象。由于他们的专业知识非常少，描述往往不得要领，说不到点子上，这就给技术人员判断故障制造了非常大的障碍。即使技术人员明白了用户电脑

或设备的问题所在，在尝试解决问题时，技术人员可能会指导用户执行一系列复杂的命令，而这个过程对用户来说是十分困难的。如果用户不能正确地遵照指示去做，问题可能会进一步恶化，电脑或设备很可能因为错误的操作导致系统的崩溃。这样一来，往往是技术人员要为一个十分简单的问题和用户说上十几分钟，甚至会专程跑到很远的用户那里去解决问题。有了远程访问、控制技术，技术人员就可远程控制用户的电脑或设备，就像本人在现场一样，只需要用户的简单帮助就可以得到该机器存在的问题的第一手资料，很快就可以找到问题的所在，并加以解决。

3) 远程交流

利用远程技术，商业公司可以实现和用户的远程交流。采用交互式的教学模式，通过实际操作来培训用户，使用户从技术支持专业人员那里学习示例知识变得十分容易。而教师和学生之间也可以利用这种远程控制技术实现教学问题的交流，学生可以不用见到老师，就得到教师手把手地辅导和听到讲授。学生还可以挂接在电脑中进行习题的演算和求解，在此过程中，教师能够轻松看到学生的思路和步骤，并加以实时的指导。

4) 远程维护和管理

网络管理员或者普通用户可以通过远程控制技术为远端的电脑安装和配置软件、下载并安装软件修补程序、配置应用程序和进行系统软件设置。

远程访问、控制的优点主要是：便于用户能够在任何地方通过网络及时、快速地访问、控制自己的远程主机。特别是对于网络管理员、技术服务人员来说，远程控制、访问提供了一种便捷、高效的手段。

而其缺点主要是：存在比较严重的安全隐患。远程访问、控制就像一把双刃剑，一方面给用户和网络管理者工作带来了很大的方便，而另一方面也给一些居心不良之人留下了后门。比如很多的木马程序，如：冰河木马、BO、广外女生，从本质上来讲就是远程访问、控制的典型应用。

1.2 远程访问、控制的原理

1.2.1 远程访问、控制的原理

远程访问、控制的原理是：用户连接到网络上，通过远程访问的客户端程序发送客户身份验证信息和要与远程主机连接的要求，远程主机的服务器端程序验证客户身份，如果验证通过，那么就与客户建立连接，并向用户发送给验证通过和已建立连接的信息。那么这个时候，用户便可以通过客户端程序监控或向远程主机发送要执行的指令，而服务器端程序则执行这些指令，并把键盘、鼠标和屏幕刷新数据传给客户端程序，客户端程序通过运算把主机的屏幕等信息显示给用户看，使得用户就像亲自在

远程主机上进行工作一样。如果没有通过身份验证的话，就是没有与用户建立连接，用户也就不能远程控制远程主机了。

远程控制软件一般可以分为两个部分：一个客户端程序 Client，一个服务器端程序 Server（或 Sysstry），在使用前需要将客户端程序安装到主控端电脑上，将服务器端程序安装到被控端电脑上。它的控制过程一般是先在主控端上执行客户端程序，像一个普通客户一样向被控端电脑中的服务器端程序发出信号，建立一个特殊的远程服务，然后通过这个远程服务，使用各种远程控制功能发送远程控制命令，控制被控端电脑中的各种应用程序运行，这种远程控制方式称为基于远程服务的远程控制（Remote Control over Remote Service）。通过远程控制软件，可以进行很多方面的远程控制，包括获取目标计算机屏幕图像、窗口及进程列表；记录并提取远端键盘事件（击键序列，即监视远端键盘输入的内容）；打开、关闭目标计算机的任意目录并实现资源共享；提取拨号网络及普通程序的密码；激活、中止远端进程；打开、关闭、移动远端窗口；控制目标计算机鼠标的移动与动作（操作）；浏览目标计算机文件目录，任意删除目标计算机的磁盘文件；上传、下载文件，就如操作自己的计算机的文件一样的简单；远程执行目标计算机的程序；强制关闭 Windows、关闭系统（包括电源）、重新启动系统；提取、创建、修改、删除目标计算机系统注册表关键字；在远端屏幕上显示消息；启动目标计算机外设进行捕获、播放多媒体/音频文件；控制远端录、放音设备音量以及进行远程版本升级更新等。此类软件可以用在一些网络使用较为复杂、需要大量维护、管理工作的环境。

由于现在实用的大多数远程控制软件支持 TCP/IP 协议，所以通过 Internet 对远程计算机进行控制为最简单易行的方式。只要两台 PC 同时接入 Internet 并同时运行远程控制软件，就可以通过 Internet 对远程 PC 进行控制。

现在很多网络管理员都采用这类软件对局域网进行管理，或者在家更新自己网站内容。这类软件对于出差在外的商务人员用处也非常大，这样他们可以随时提取自己家里计算机中的数据和资料。

前面我们所说的是一台电脑对一台电脑的情况。其实，基于远程服务的远程控制的最适合的模式是一对多，即利用远程控制软件，可以在主控端电脑上监控网络中的每一台电脑。随着网络为人们所接受，许多公司、机关、学校都建立了内部网络，并且大部分都接入了互联网。可以借助远程访问、控制技术对网络中的电脑进行监控。比如有些员工在上班时间利用网络进行网上炒股，玩游戏，网上聊天等工作以外的事情，再比如像学校的机房、网吧这类要进行登记收费上机的地方，由于电脑的数量比较多，用传统的管理方法或用非网络化的软件管理，都不能有效地防止有些人不登记就上机的情况。而利用远程访问、控制技术，可以做到先登记再上机，不登记就不能够使用电脑。如果再整合收费数据库系统就是一个非常完善的机房管理系统了。这种一对多的连接方式不仅减轻了管理人员的工作量，还使得网络的接入更加安全可靠，

管理人员也更易管理局域网上的每一台电脑。

远程访问、控制所支持的网络方式：LAN、WAN、拨号方式、Internet 方式。此外，还可以通过串口、并口、红外端口来对远程机进行控制（不过，这里说的远程计算机，只能是有限距离范围内的计算机）。

远程控制主要使用 NETBEUI, NETBIOS, IPX/SPX, TCP/IP 等协议；随着 Internet 技术的发展，目前已有许多远程控制软件通过 Web 页面以 Java 技术来控制远程计算机，这样可以实现不同操作系统环境下的远程控制。

1.2.2 远程访问、控制的连接类型

远程访问、控制主要是发生在 LAN（局域网）和 WAN（广域网）中。我们主要讨论的是在 WAN 中的连接类型。

电话公司提供了大量的 WAN 服务，如：T1、T3、ISDN、数字用户线路（Digital Subscriber Line，简称为 xDSL），简易老式电话业务（plain old telephone service, POTS）、帧中继和 X.25。

所有这些其实可以分成 3 种 WAN 连接：专用的 T1、T3、xDSL；电路交换的模拟的 POTS 和 ISDN；分组交换的 X.25 和帧中继。

1) 专用连接

专用连接常称为专用线路，在两个站点之间提供点到点的链接。最常使用的链接类型就是专用连接。图 1.2 所示为点到点专用连接的示例。

这些站点可以近得只隔一条街道，也可以相距几百英里。电话公司为客户提供的数据通道是一条预定的保留线路，也就是说，除了指定用户之外，任何人都不能使用这条数据通道。这一类连接可以使得公司最大限度地控制 WAN 连接，对于高网络信息流量、速度达 T3/E3 的连接来说是很理想的。但这种连接费用昂贵。当连接时间和距离相对较短时，这种线路从成本来说是很合算的。

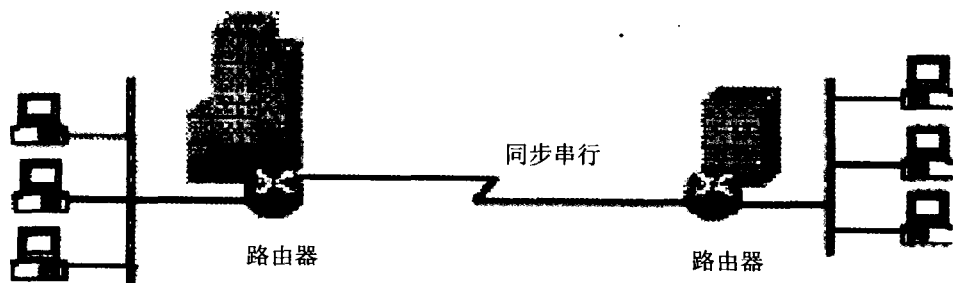


图 1.2

专用线路一般需要使用路由器的同步串行端口。

同步通信利用精确的时钟来传输数据。由于数据是按固定的已知的频率进行发送

和接收的，所以数据可以无缝地传输。异步传输将字符封装于控制位（起始位和终止位）中，由控制位来指定每个字符的开始和结束。由于添加了起始位和终止位，所以增加了负载，从而降低了效率。

2) 电路交换连接

电路交换连接是一种 WAN 交换方法。这就是说，在建立呼叫时，将通过载波网络创建专用线路，而呼叫结束时，该专用线路就崩溃了。电话是这种通信最常使用的形式。当拿起电话打电话时，呼叫就建立了；当挂断后，呼叫结束。要使用电路交换连接，首先要提前知道端头（就像是在拨打电话之前，要先知道对方的电话号码）。然而，与专用串行连接不同，我们一把电话拨打到与电话公司连接的地点，就建立了电路的目标，而且一收线，电路就会立即中断。如图 1.3 所示。

最常用的两种电路交换网络是：

模拟简易老式电话业务（Plain Old Telephone，简称为 POTS）。

数字综合业务服务网（Integrated Service Digital Network，简称为 ISDN）。

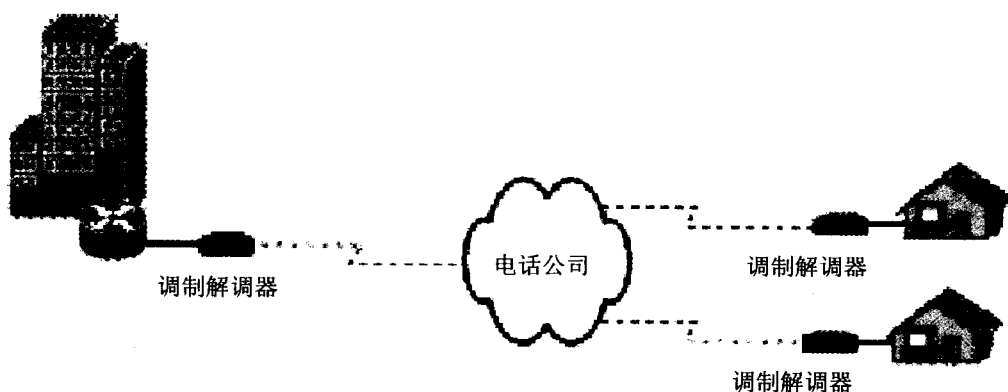


图 1.3 电路交换连接

3) 简易老式电话业务

POTS 连接是当今最盛行的电路交换连接，是世界上最大的网络，已经有 50 多年的历史了。专用的串行连接旨在将二进制数据从一点移到另一点，而电话系统输送的则是模拟数据。

数据可以以两种方案表示：模拟的和数字的。使用模拟信号进行数据传输是典型的人类通信的方式。例如，在我们说话时，产生的声音具有不同的频率和振幅。由于模拟信号非常容易地代表了诸如高、中、低等不同的值，所以可以携带大量的信息。而在计算机中，最基本的数据表示方法是用二进制（1 和 0）。采用二进制信号的数据可表示两种状态：On 和 Off。

这意味着什么呢？这就意味着必须要用携带模拟信号的系統，通过调制解调器 Modem 来传送二进制信号。图 1.4 所示为数字信号与模拟信号之间的转换。这就使得