

第2章 基础连接

正如你在第1章“网络互连协议和标准概述”中所看到的：TCP/IP的广泛使用和所有从它发展而来的标准和协议使得基础连接问题对许多机构来说都是必不可少的。的确有许多连接至因特网的方法，其中一些比另一些更有效，这应归因于这些方法与多种环境和计算机交互的能力。

不论你是将因特网看作动词——将两个LAN或WAN连接起来，还是将因特网看作名词——因特网包括了两个或多个不同的网络，当谈论连接性及如何与客户、服务器、网络（LAN和WAN）连接，并最后讨论如何对这些连接进行保护时，都不得不考虑基础连接。在第1章中，我们还提到了一些已经在因特网中使用并发挥作用的协议，以及那些正在被开发和提出的协议和标准（IPv6）。但是否因此你的机构便可使用因特网的优势或IP技术吗？你的公司使用哪种拓扑结构？在公司中是如何处理文件传输、电子邮件、主机终端仿真会话、硬件集成，最重要的是，如何处理安全问题？

这些应是你头脑中很清楚的问题，以便你与公司中的管理部门和MIS通信，并集中精力解决为有效地展开基础连接计划所需的技术，不论是刚开始进行连接，还是有了一个大型复杂网络。在进行网际互连时，你必须集中于连接的安全问题以及打算如何进行。

TCP/IP技术提供任何一个机构所需的基本连接，以收集、分析和发布信息。迅速发展的存储技术的先进知识对于声音、视频和以及其他宽带信息源是必不可少的。但你必须做好准备，为所需的安全连接类型选择和使用正确的协议和技术。随着后面对因特网的进一步论述，你将会发现它是一个荒芜之地！

因特网是一个允许用户与所有连接的服务器和主机通信的虚拟网络，就好像这些服务器和主机是本地网络的一部分。然后，需要将此网络的所有细节隐藏起来，用户不必知道。这就是基础连接要求的开始，而确实是TCP/IP协议组提供了这个虚拟网络存在的基础。在第1章中所提到的协议，制定了系统间信息交换必须遵循的格式和规则。但是，对于网络用户来说，服务是如何提供的？围绕这些服务的安全问题又是什么？

TCP/IP定义了给网络用户提供服务的多种应用层协议，包括远程登录、文件拷贝、文件共享、电子邮件、目录服务和网络管理工具。一些应用协议使用范围很广，也有一些仅仅用于特定目的。在此章中，我们仅集中于其中的一部分协议和它们的安全弱点。以下是一些常用的TCP/IP应用层协议：

PING 根据《Computer Dictionary》(<http://nightflight.com/foldoc/>)，PING可能是源于声纳回声相应的海底术语。而实际上它是一个程序，通过发送一个或重复发送多个ICMP回应请求和等待答复用来检测网络连接。PING工作在IP层，它的服务器端通常完全在操作系统内核中运行，因此是对远程主机是否活跃的最低层测试，即使高层TCP服务不能提供，PING常能响应。

Telnet 远程登录的因特网标准协议，运行于TCP/IP之上。

Rlogin 与Telnet相似，是允许用户通过网络登录到另一台主机的4.2BSD UNIX实用程序。

Rlogin与远程主机的守护进程通信。

Rsh Remote shell的缩写。这是一个Berkeley/UNIX网络命令，用于在远程主机上执行给定的命令，通过它进行输入输出。Rsh与远程主机的守护进程通信。

FTP 文件传输协议。这是一个客户/服务器协议，允许在TCP/IP网络上的两台计算机间进行文件传输。

TFTP 次要文件传输协议。与FTP极其相似。这是一个通常用于下载引导程序代码到无盘工作站的简单文件传输协议。

SMTP 简单邮件传输协议。通常用于计算机间进行电子邮件传输。

Kerberos 由麻省理工学院研制的基于对称密钥加密的认证系统。

X Windows 位图显示设备上与设备无关的窗口操作的规范。

DNS Name 多种用途的分配、复制、数据查询服务，主要用于在因特网上将主机名转换成因特网地址。

NFS 网络文件系统，允许计算机通过网络像访问本地磁盘中的文件一样访问网络上文件。

SNMP 简单网络管理协议。管理IP网络站点的因特网标准协议。

2.1 关于TTY

TTY实际上是电传打字机终端（TeleTYpe），像是一台噪音很大的机械打字机，支持一个相当有限的字符集，打印质量低劣。

但是，特别是在UNIX中，TTY却被视为任一个终端。TTY可指控制一项给定作业的指定终端，除此之外，它还是UNIX中的一条命令名：输出正在使用的控制终端名。它还可指任何一个串行端口，不管与此端口连接的是不是终端。我认为之所以如此，是因为在UNIX中这些设备有tty*.形式名。的确，该术语存在一些多义性，这正是它如今仍被使用的原因。

出于集中研究基础连接性和现在主要可用性的目的，我们认为TTY允许将文本信息转换为语言信息，反之亦然。又被称为聋哑电信设备（TDD），这是一种被聋哑人广泛使用的通过电话线进行文本通信的终端设备。

一般来说，在收发者之间没有使用TTY调制解调器的情况下，操作员是必不可少的。若要与有TTY的人通信的话，操作员将在TTY上输入该用户所说的话，然后将信息“传给”没有TTY的呼叫者，反之亦然。

TTY/TDD设备与普通调制解调器之间的不同之处是：TTY使用BAUDOT编码进行通信，而典型的调制解调器使用ASCII码进行通信。BAUDOT编码并不是一种新编码，也支持字符数有限的字符集。这正是调制解调器制造商使用ASCII码的一个原因。而且，这些设备以很低的速率通信，大约是300波特或更低，美国大多数TTY以45.45bps的速率进行通信。

尽管标准调制解调器不兼容TTY，但也有一些支持ASCII码通信的TTY调制解调器。但使用它们的时候也可能遇到一些问题，因为大多数TTY调制解调器以最大300波特的速率通信，有些却只有110波特。

也有从ASCII码到BAUDOT码转换的调制解调器，可令你得到满意的转换。

什么是BAUDOT

BAUDOT码广泛使用于电报系统，是由Emile Baudot于1870年发明的。这种异步码仅使

用5比特，可表示32个字符。为能提供所有的字符和数字，可选用两个 32字符的组合。表 2-1 列出了BAUDOT中所有可用字符。

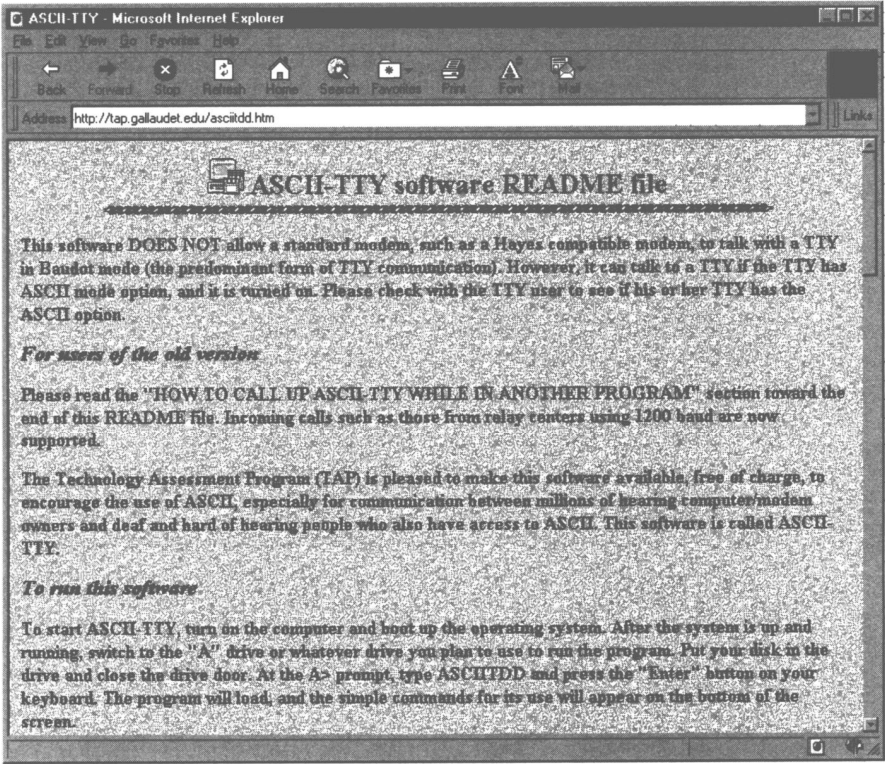


图2-1 ASCII-TTY软件的Web站点

表2-1 BAUDOT码中全部字符

二 进 制	十 六 进 制	LTRS	FIGS
00011	03	A	-
11001	19	B	?
01110	0E	C	:
01001	09	D	\$
00001	01	E	3
01101	0D	F	!
11010	1A	G	&
10100	14	H	#
00110	06	I	8
01011	0B	J	BELL
01111	0F	K	(
11100	1C	M	.
01100	0C	N	,
11000	18	O	9
10110	16	P	0
10111	17	Q	1

(续)

二 进 制	十 六 进 制	LTRS	FIGS
01010	0A	R	4
00101	05	S	'
10000	10	T	5
00111	07	U	7
11110	1E	V	;
10010	12	L)
10011	13	W	2
11101	1D	X	/
10101	15	Y	6
10001	11	Z	"
01000	08	CR	CR
00010	02	LF	LF
00100	04	SP	SP
11111	1F	LTRS	LTRS
11011	1B	FIGS	FIGS
00000	00	未使用	未使用

注意 有如图2-1所示软件，将TTY调制解调器ASCII方式选项打开，可使ASCII码调制解调器与它交谈。详情请查阅：<http://tap.gallaudet.edu/asciitdd.htm>。

CR：回车；LF：换行；BELL：铃声；SP：空格；STOP：停止

2.2 UNIX to UNIX Copy

UNIX to UNIX Copy (UUCP) 是内置连网系统，与每个 UNIX 系统一起提供，其基本用途是提供脱机访问因特网。UUCP 的特性有很多局限性，仅用于信息交换，并不像 TCP/IP 那样提供远程登录。然而，它在公告牌系统 (BBS) 中应用仍十分普遍，允许用户访问电子邮件，尽管与基于 TCP/IP 的系统相比十分缓慢和笨拙。

在 UUCP 内部有一个十分简单的程序名为 "uucp"，其基本功能是从一个主机向另一个主机拷贝文件，但也允许在远程主机上执行一定的操作。一定不要将 UUCP 和 uucp 混淆，UUCP 是在 uucp 之后才命名的，且它们并不是一回事。

提示 以下是几个主要的 UUCP 程序：

uucp——允许远程机器间进行文件传输的请求。

UUX——请求在远程机器执行命令和进行邮件传输。

UUXQT——在本地处理远程请求，uucp 和 UUX 均在后台运行。

UUCICO——由 UUCP 和 UUX 发出请求，呼叫和传输文件。主/从配置。

UUCP 的另外一个特性是允许你将作业和文件通过多个主机或协作运行的主机链进行转发。现在 UUCP 网络提供的最重要的服务是电子邮件和新闻。

最后，UUCP 还是提供公众访问的许多拨号存档站点的选择媒体。通常，用 UUCP 拨号便可访问这些站点，以宾客用户身份登录，从公共访问归档区域下载文件。这些客户帐户通常都有 uucp/nuucp 或其他相似的登录名和口令。

2.3 SLIP和PPP

串行线路网际协议（SLIP）是一种通信协议，使用 RS-232 串口与调制解调器相连，支持通过拨号方式与因特网连接（即使用 TCP/IP）。

SLIP 改变标准的因特网数据报，它在因特网数据报中添加一个 SLIP END 字符，由此而改变了数据报。数据报允许将此字符独立看待。SLIP 需要一个端口配置为八位数据，无奇偶校验，和硬件流控制。然而，SLIP 不提供错误检测，只依靠高层协议控制。如果运行特殊的有错误倾向的拨号连接，SLIP 本身的作法将不令人满意。

为正确运行，必须在每次建立连接前配置 IP 地址。

点对点协议（PPP）是一种本质上与 SLIP 相同的较新协议，然而，它的设计比 SLIP 更好更具有实用性更可接受。它在异步连接和面向位的同步连接系统中均可使用，并可动态配置与远程网络连接以及检测连接链。

注意 通过使用适当的网络控制协议（NCP），PPP 可进行配置以封装不同的网络层协议（例如：IP, IPX, AppleTalk）。详情请查阅 URL <http://www.virtualschool.edu/mon/DialupIP/slip-ppp.html>。

2.4 Rlogin

与 Telnet 相似，rlogin 将在本地主机系统 lhost 的终端连接到远程主机系统 rhost。

Cygnus Solutions (<http://www.cygnus.com>) 有一种称为 KerbNet 的产品，如图 2-2 所示，

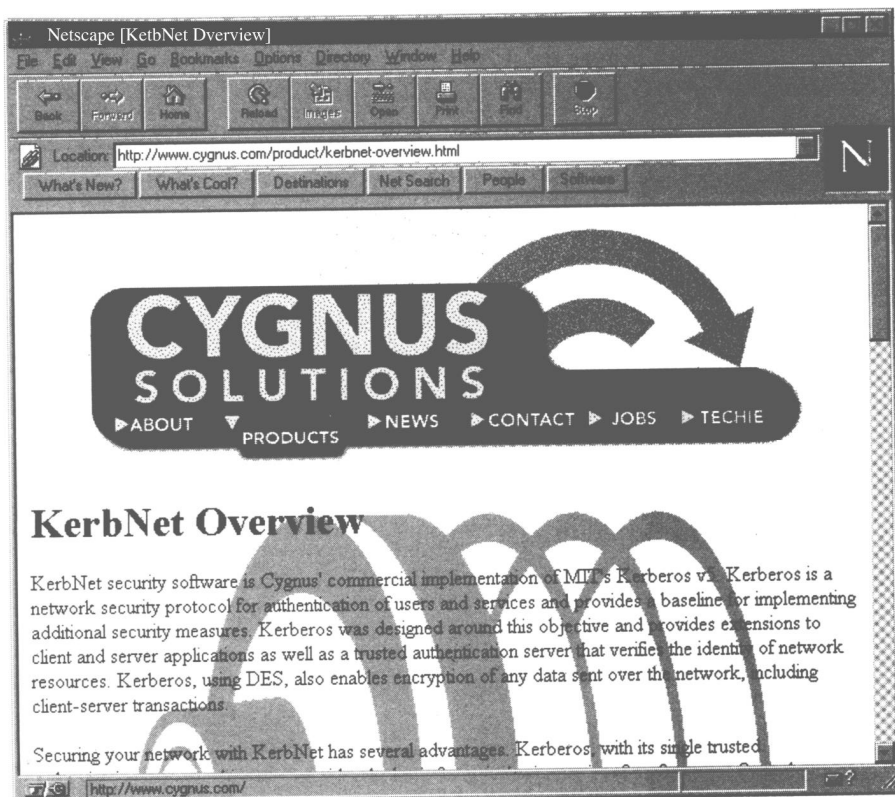


图2-2 Cygnus KerbNet页——通过Kerberos保证网络安全

可在使用rlogin时有十分安全的连接。

使用Kerberos认证与标准的Berkeley rlogin十分相似，它使用Kerberos认证而不使用rhost机制来检测用户是否被授权使用远程帐户。

在每个用户的登录目录中均有.klogin文件，保留有私有授权表。这个文件的功能与.rhosts文件很相似，允许非本地用户获得.klogin文件所在机器的Kerberos服务。例如：用户joe@EAT.COM一般来说不允许登录到MUSSELS.COM作用域的机器，然而Joe的朋友bertha@MUSSELS.COM可在她的主目录中创建包含有joe@EAT.COM的.klogin文件，便可使Joe像Bertha一样可登录到Bertha的机器中，尽管他并没有证件证明他就是Bertha。

这个文件中的每一行都包括principal.instance@realm形式的Kerberos主名。如果原始用户被认证为.klogin中的一个主名，就许可访问该帐号；如没有.klogin文件，便许可访问accountname@localrealm。

另外，往远程主机登录时会提示你登录和输入口令。为防止安全出现问题，.klogin文件必须被远程用户所有。

若在收集Kerberos认证信息中出现问题，将会有错误信息打印出来，这时将执行标准UCB rlogin以代替Kerberos rlogin。这允许使用相同的rlogin命令连接使用 and 没有使用CNS的主机。

2.5 虚拟终端协议

Telnet协议可能是使用最频繁的应用协议之一，用于登录到其他主机以获得或交换信息。所有被连接的计算机必须使用和支持Telnet协议，以便Telnet可运行。若要与一台使用Telnet的机器连接，此机器通常会提示你输入用户名和口令。如果不是与公共或通用帐户连接，必须在登录前建立好自己的帐户。

在进行Telnet连接时，应知道以下几个面向连接的安全需求：

- 保密性。

- 完整性。

- 对等实体认证。

- 基于身份的访问控制。

所有这些要求都隐含有一个前提，即基础安全实现是在连接层，面向流及使用点对点应用协议。但不能假想连接是安全的，因为不会总能找到在应用协议中实现的安全机制。必要的话，必须在较低层例如传输层或网络层实现安全机制。

传输层安全协议（TLSP）于1992年7月成为因特网的标准，是一个Telnet连接缺乏安全性的可行的解决方案。TLSP在传输层以下运行，并通过在每个连接基础上通过网络层之上提供端端加密对Telnet连接提供安全服务。

依靠这种低层安全机制的主要优点之一是可避免重复进行有关安全方面的工作。但我要再次指明的是，我不敢确认会有多少开发人员和专业人士会愿意将新软件引入操作系统的内核中。因此，最好在应用层而不是在网络层或传输层为Telnet连接提供安全保障。

2.5.1 哥伦比亚大学的Kermit：一种安全可靠的Telnet服务器

信息系统和技术已经实现了很长一段时间，但许多主要操作系统（OS）没有提供使用和

安全实现更为可靠或至少实用的 Telnet 特性。Windows NT 4.0 的确有 Telnet 界面（如图 2-3），这确是件伟大的工作，但自 Windows 98 面世以来，comp.os.ms-windows.win98.* 新闻组已接到大量对 Windows 98 的“Telnet 服务器”或“Telnet 守护进程”的请求。

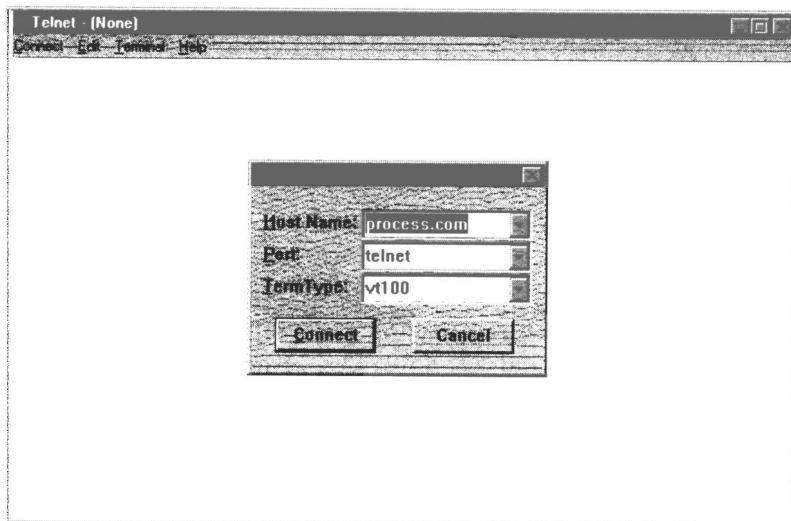


图2-3 Windows NT 4.0 Telnet 登录界面

为什么呢？在哥伦比亚大学的 Web 站点(<http://www.columbia.edu/kermit/k95host.html>) 中有大量资料讨论这一话题，并介绍一个很棒的产品 Kermit，为满足 Windows 98/NT 用户群做了大量的工作。

如文章所指出的那样：拥有 Windows 98 系统的人希望能被授权访问他们的朋友、亲属、合作者、客户或代理人——并在其他位置访问他们自己——甚至那些没有 Windows 98 或任何 Windows 版本并正在进入 Windows 98 或其他 Windows 的人或者那些甚至没有自己的个人计算机的人，在这种情形下，将不能使用像 PcAnywhere 这样的远程访问解决方案。

同时，另外的人希望他们的朋友和客户能够拨进他们的 Windows 98 个人计算机（不使用 Telnet），即使一方或者双方均未连在因特网。因为与前面概括的同样的安全原因，人们也需要 Telnet 服务器。他们希望能够使用 Telnet 登录到主机，也就是说，他们需要一个提供某种形式的认证和访问控制机制，而不仅仅是一个 DOS 提示符。

哥伦比亚大学的 Kermit-95 有很多特性可有助于 Telnet 连接，并使它更安全更便于使用。图 2-4 对 Kermit-95 (K-95) 有一个很好的概述，你可在背景画面中看到 K-95 拨号服务界面，在它的前面有个高亮度的连接界面，可进行有关设置，打开的是第一页，最前面画面是一个连接到 BBS 的对话本身。

图 2-4 背景中还显示了第二个对话，这是通过因特网连接 UNIX 服务器的对话，在此处显示一部分“手册页”，它说明 K-95 拨号程序如何管理多个对话。通常，如果要打开一个对话，所需做的工作仅仅是双击目标项。

图 2-5 显示了进入记事本的终端设置页，Kermit 为每个连接提供一个记事本，因此每个人都有不同的仿真，字体大小、字符设置、屏幕大小、颜色等。所有这些设置在拨号连接和 Telnet 或 RLOGIN 对话框中都可很好地运行并可作为连接进程的一部分自动应用。这些记事本

可使你对每个拨号因特网服务或你使用的计算机充分定制一键访问。

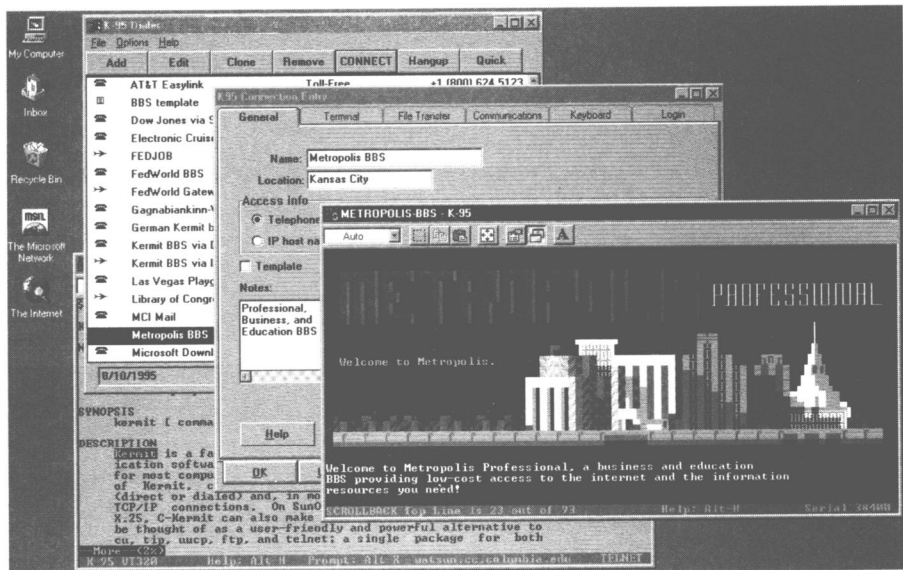


图2-4 Kermit-95拨号程序和连接界面

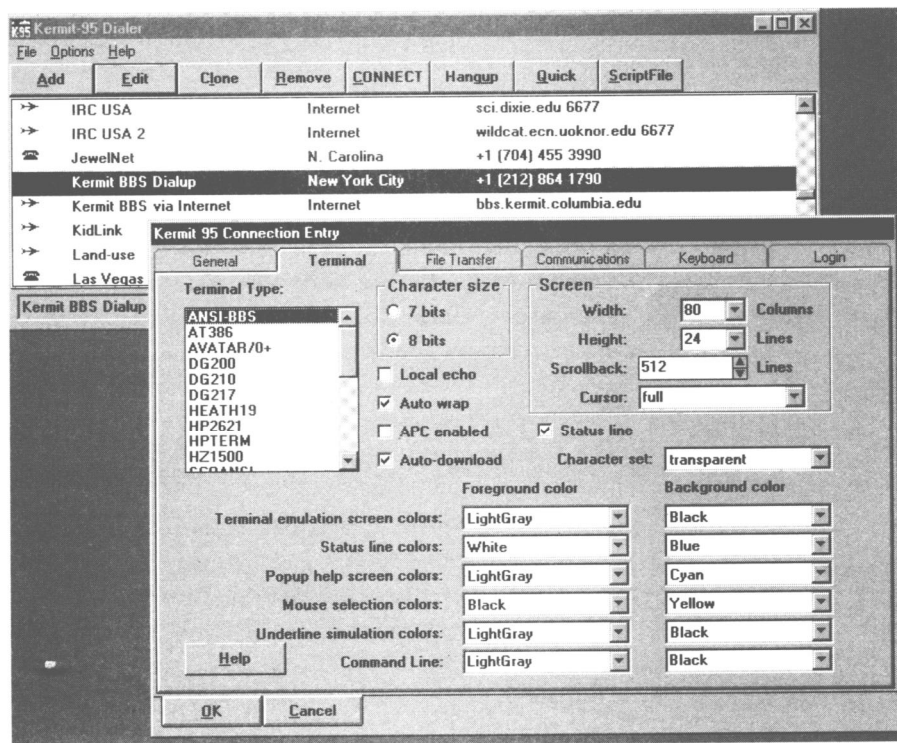


图2-5 笔记本的终端设置页

图2-6显示了K-95为正确处理你的呼叫所需的信息（不论你在何处）。如果你一直在同一个地方发出呼叫，就无需使用这些属性。但如果你是带着笔记本电脑四处旅行的话，会对这

种便利感到吃惊。只需告诉 Kermit-95或Windows 95你的位置，搜索拨号目录中所有的号码便会开始工作。

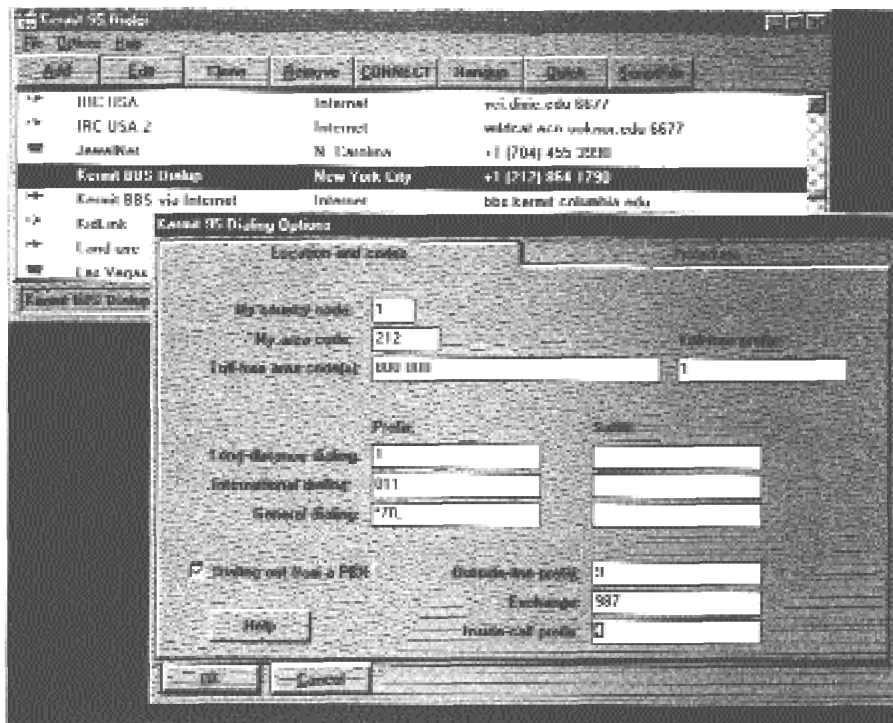


图2-6 设置拨号位置

K-95的另一个主要特性是：与需要不同的退格代码的一些计算机或 Telnet服务不同（很多时候，不得不给计算机的退格键分配合适的代码），Kermit-95允许你为目录中的每一台计算机和主机分配它们自己的键盘布局，指定在键盘布局记事本中的键盘表，如图 2-7所示。

图2-7还可显示出，要解决退格键的问题，只需按适当的按钮，如果需要的话，Kermit-95还允许你装载整个键盘常规键映射。图 2-7显示了与 Kermit-95一起发布的基于主机的 WordPerfect 5.1的键映射。

图2-8中举例说明了K-95的一些特性，如：

屏幕高度：你知道在没有 Kermit-95的Telnet会话中，Lynx的主页是在 43行的屏幕上吗？

多种尺寸屏幕：依字体大小而定。

显示Lartin-1字模 8-比特字符的能力：图 2-8中蓝屏显示了German字体的例子。

文件传输：通过使用长的信息包和滑动窗口，K-95实际上可达到很高的传输速率，甚至如图2-8所示在PC被其他进程严重超载时也是这样。

同时处理多对话正如在图 2-8中所看到的，K-95可同时处理多个会话。例如：在登录BBS的拨号会话中的ANSI终端仿真以及为每个会话设置屏幕颜色的能力。

图2-9显示了终端屏幕上各种上下文有关的弹出式帮助窗口——“重要键”，鼠标按钮及组合键功能。

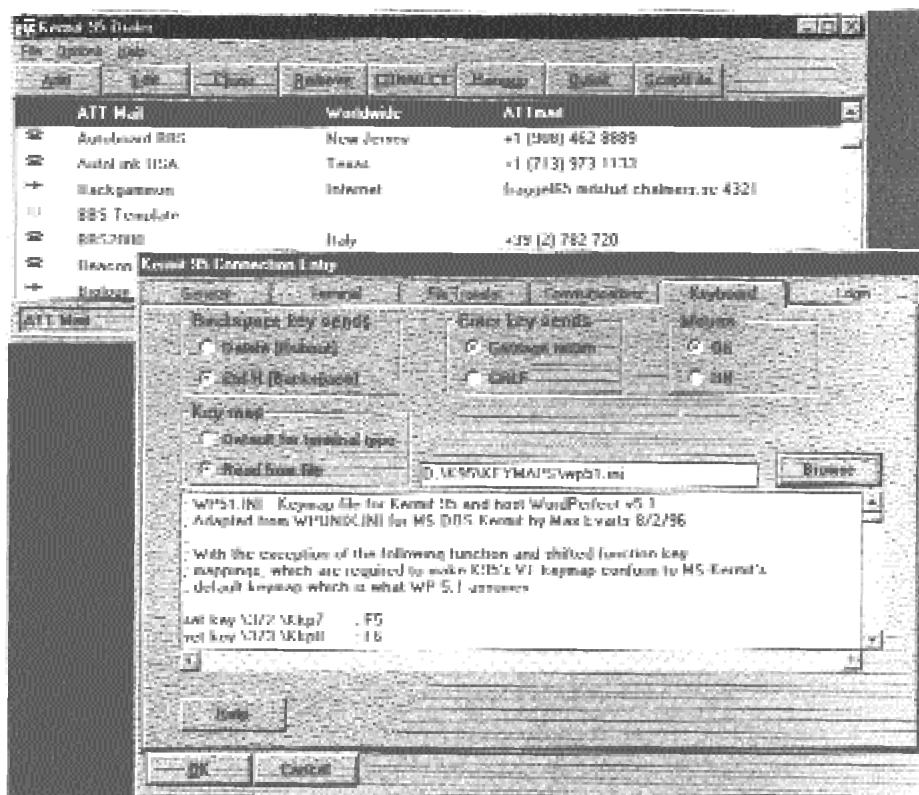


图2-7 Kermit-95的键盘设置表

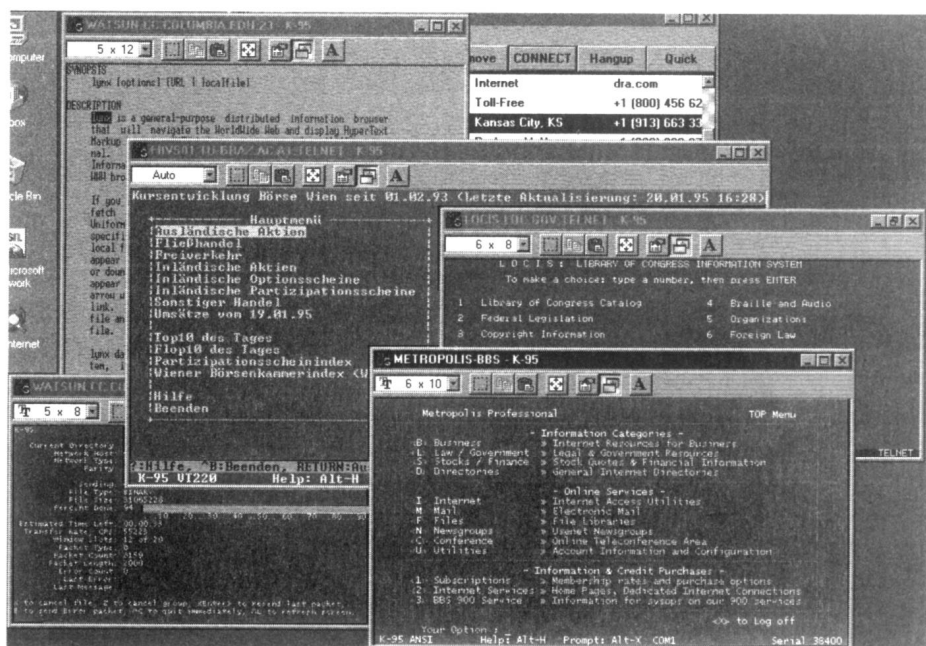


图2-8 Kermit-95 的多会话特性



图2-9 Kermit-95 上下文有关的帮助窗口

2.5.2 Telnet服务的安全考虑

尽管已实现了诸如 Kermit 及其他安全机制，但还应注意许多的可能的安全措施：

1. 超时策略

Telnet 对话长度 可设置用户的 Telnet 对话持续时间。时间长度可以基于用户类型或单个用户。例如：你公司中使用 Telnet 的宾客帐号使用较短的登录时间（5 到 10 分钟），而技术支持、上层管理或任何一个有资格的 / 指定的用户则时间较长。

会话超时 如果在指定时间范围后没有发生任何动作，可将此 Telnet 会话设为超时。

安全屏幕保护 可使用一个超时屏幕保护程序，当会话经过一定时间仍无动作发生时保护程序工作。在这种情况下，与会话超时不同，该 Telnet 会话在网络中仍保持活跃，但被保护。当超时发生前，应对用户提出警告。

2. 数据保护策略

票据交换所目录 你应建立临时法人目录以保存未经验证的数据。而且，要保证经电子签名后，这个数据不会被进入的未经授权用户修改。

保护敏感数据 一定要保护敏感数据，只允许被确认的用户访问它，并提醒每个用户所有数据都是保密的。

2.5.3 网络安全系统管理员

当我们谈论因特网安全性时，我们指的是什么？我们是指过程还是结果？我们是指建立

访问控制和授权机制，还是确保用户只能执行他们被授权的任务，只能获得他们被授权获得的信息，并不会破坏他们能访问的任何数据、应用程序和操作区域？我认为后者比前者定义了更多的网络安全环境。

问题是网络安全是要进行保护其不受黑客和入侵者的恶毒攻击。但安全还应结合控制和授权机制及阻止错误和设备故障的影响。

这一节旨在提供可用来改善网络安全性的具体措施。尽管对你的站点不能提供百分之百的安全性，你所需要的不仅是诸如加密（参见第3章）以及本书从头至尾都在讲述的防火墙技术。在学习具体方法以前，必须了解敌人是谁，危险和挑战是什么，以及为防止安全事故的发生，所使用的基本预防（不是反应）方案是什么。

1. 网络安全保护针对谁？

当然，你要保护你的网络不受黑客、密码破译者的袭击！但你应考虑这些“强盗”是谁，他们想要做什么，然后才可围绕这一点建立自己的保护机制。因此，必须了解他们的动机是什么，必须推断他们可能想做什么，及对你的网络可能会有什么危害。

但一定要切记，即使使用了所有这些安全措施，也不可能保证每一个用户不能执行未授权的任务，而只能使执行起来更困难。这个思想只是确保这些网络安全控制超出了攻击者的能力或者动机。

2. 所有所做的安全努力值得吗？

请了解这一点：你所采取的任何安全措施一般都会减少服务的便利性和可访问性。除了产生昂贵的管理和教育开销之外，还会延迟用户的生产及系统的进程（和许多专用硬件）。

因此，当我们开始设计安全措施时（本书稍后会讲到），很重要的是理解这些措施的代价并与潜在收益相比较。要做到这一点，必须理解这些措施本身的开销和破坏安全性的代价与可能性，如果安全措施的代价超出实际危险，就会得不偿失。

3. 你的感觉告诉你什么？

每个安全专业人员因为条件或观点的不同，都有他/她自己的基本设想。你可能觉得从未受到攻击，但不可能总这么确定！或许你认为比任何一个黑客懂得多，或者你的系统足够安全。不管你的设想和感觉如何，一定要小心！如果没有得到证实，任何设想都会成为潜在的安全漏洞。

4. 注意保密性

我知道你已多次听到保密性，如果你认真想一想，会发现大多数安全策略都建立在保密这一概念的基础上，口令是保密的，密钥也是保密的，对吗？

但是，如何使秘密成为秘密？这很平常，并不是一个秘密。保守机密最重要的是知道你需保护的范围并对它保密。首先你应自问，需要哪些知识，才会有人绕过你的系统。一旦你确认了这点，一定要积极地面对这一点。要保护该知识并假设其余的一切可爱的黑客们都知道。但不要大意，你拥有的秘密越多，要保守所有这些秘密也越困难。

应开发自己的因特网安全策略，以便只需保守有限的秘密，选择需知道秘密的人数。

5. 错在人

许多安全策略之所以失败是因为没有考虑到人的因素。你的用户就是实际使用、实施或违反安全策略的那些人。对他们而言，规则和过程很难记住，或者他们认为每六个月更新口令是毫无意义的，等等。

这就是为什么到现在有一种现象仍很普遍：发现口令被写在纸上，而纸则被放在键盘下；调制解调器连接上网而没有任何安全措施；逃避繁杂的上网安全过程等。最基本的是，安全措施不能较多影响系统使用，否则用户就会抵制甚至不使用这些安全措施。要想确保用户支持你的措施，必须确保你的安全过程并不妨碍用户的使用——用户仍在毫无压力的情况下完成他们的工作。你需向他们出售安全！

一定要记住：任何一个用户都可能危害你的安全措施，而且统计表明：大多数的入侵者来自内部。这未必是你的用户，只能说内部存在安全漏洞。

例如口令，只需给用户打个电话，称自己是系统管理员，要求告知口令，就会轻易地获得你的口令。如果你的用户了解安全问题，了解你所采取安全措施的原因，他们决不可能让黑客得到的如此容易。最起码，应告诉用户不要在不安全的电话线上（尤其是蜂窝电话）或电子邮件中泄露口令和其他秘密。

6. 你的弱点在哪里？

每个网络和安全策略都有弱点。你的也不例外。因为系统弱点通常是被利用的地方，你必须意识到安全性存在危险的范围并立即堵住漏洞。认识网络的弱点是开发正确安全网络的第一步。

7. KISS原则（保持简单、严谨）

在网络周围设置适当的障碍并保护它不受因特网的危害是完全正确的。但不要忘记 KISS 原则。系统的安全性与该系统中任一主机的最低安全级相同。因此，要了解你的运行环境如何，知道什么功能是期望的，什么是不期望的，并围绕这点建立你的策略。

时刻注意异常事件，这可使你在入侵者破坏系统以前追踪到入侵者，使用审计工具可帮助你检测到异常事件。

2.5.4 Telnet会话安全检查表

口令8字符以上，强制每六个月更改一次设置。

限制通过口令和终端位置进行 Telnet 对话和访问。

如果 Telnet 对话是从住宅或远程位置通过拨号开始的，应要求输入第二个口令或启动回呼过程。

口令应加密。

禁止口令共享！

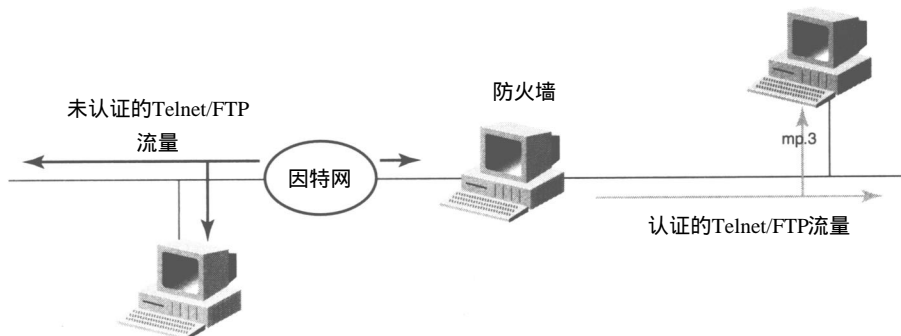


图2-10 过滤Telnet（和FTP）连接

对所有访问都用口令和网络地址进行登录，并用用户名、网络地址和日期构造使用报告（访问审计踪迹）。

开发用户的配置文件，从配置文件上监视用户动向。

Telnet用户应签署保密协议。

定期运行可用的安全测试程序进行安全检测。

实现如图2-10所示防火墙！

2.6 简单文件传输协议

简单文件传输协议（TFTP）以最低网络开销进行文件传输。尽管TFTP使用UDP在网络设备间传输文件，但它支持超时和重发技术以确保数据可靠到达。

TFTP的主要弱点之一是它允许对系统或用户文件的未授权远程访问，因为它提供无需口令的远程文件访问，这就是TFTP典型地被使用于无盘计算机、X终端或其他专用硬件初始化的原因。但由于TFTP守护进程不限制对特定文件或主机的访问，远程入侵者可以很容易地使用该服务来获得其他系统的口令文件或用户文件的拷贝，甚至远程改写文件。

因此，我建议你限制TFTP只访问服务器硬盘驱动器中有限的子目录树。决不能允许用户访问服务器的根目录，和限制使用tcp wrapper进行TFTP访问。

TFTP的安全考虑

出于安全原因，不应运行TFTP，但如果不得不运行的话，使用安全选项/标志以限制其只访问没有重要信息的目录，或者用chroot改变包装程序的根目录以控制其运行。

可使用的另一实用程序是rpcinfo，它可与端口映射表对话，并可告诉你，是否主机运行NIS（甚至主机是NIS服务器或从机），运行NFS（无盘工作站）及其他信息服务（rusersd，rstatd等）和任何不寻常程序。

安全RPC在减少远程连接危险方面可提供不少帮助，但它本身也存在问题，因为它不好管理，并且它采用的加密方法并不强壮。是的，我大概知道你在想什么，即Sun的NIS+可解决一些问题。但你是否看到随后产生的结果？不要忘记NIS+只在Sun上运行！

解决办法是什么？在此我们再次指出，如果你愿意的话可以使用包过滤或防火墙，如果你喜欢的话。如果滤除来自111端口的包，最起码可避免大多数的安全事故。

但不要仅仅依靠它，端口映射器（portmapper）仅懂得RPC服务，另外一些服务可用来强制与所有网络端口连接的方法进行定位。许多网络实用程序和窗口系统使用专用端口。如25号端口sendmail，23号端口的Telnet，6000号端口的X Windows。SATAN包括一个检测远程主机端口的程序，并以如下形式的输出告诉它的发现：

```
hacker % tcpmap poorsite.com
Mapping 148.158.28.1
port 21: ftp
port 23: telnet
port 25: smtp
port 37: time
port 79: finger
port 512: exec
port 513: login
```

```
port 514: shell
port 515: printer
port 6000: (x)
```

这段输出显示了 poorsite.com 正在运行的 X Windows，若没有适当保护（通过魔术饼干或 xhost 机制），窗口显示可被捕获或观测；用户的键击可被监视和记录，程序可远程执行等等。如果目标正在运行 X Windows 并接受 telnet 到端口 6000，则可用来进行拒绝服务攻击，因为目标窗口系统将经常“冻结”一小段时间。

提示 若想从因特网上获得一些免费安全资源，试一下这些站点：

计算机应急行动小组（CERT）顾问邮递目录，通过发送 e-mail 到 cert@cert.org 并请求被放置在他们的邮件表中。

时事通信：发送 e-mail 信息到 phrack@well.sf.ca.us 并请求添加到表中。

防火墙邮递目录：在信息正文中包含下行（空白主题行）到 najordomo@greatcircle.com：订购防火墙。

对免费软件：

Computer Oracle and Password System（COPS）：通过匿名 ftp 从 ftp://archive.cis.ohio-state.edu/pub/cops/1.04+ 获得。

tcp wrapper：通过匿名 ftp 可从 ftp://ftp.win.tue.nl/pub/security 得到。

Crack：在 ftp://ftp.uu.net/usenet/comp.sources.misc/volume28 可得到。

2.7 文件传输协议

文件传输协议（FTP）是因特网上传输文件的主要方法。使用 FTP 可在全球传输文件。虽

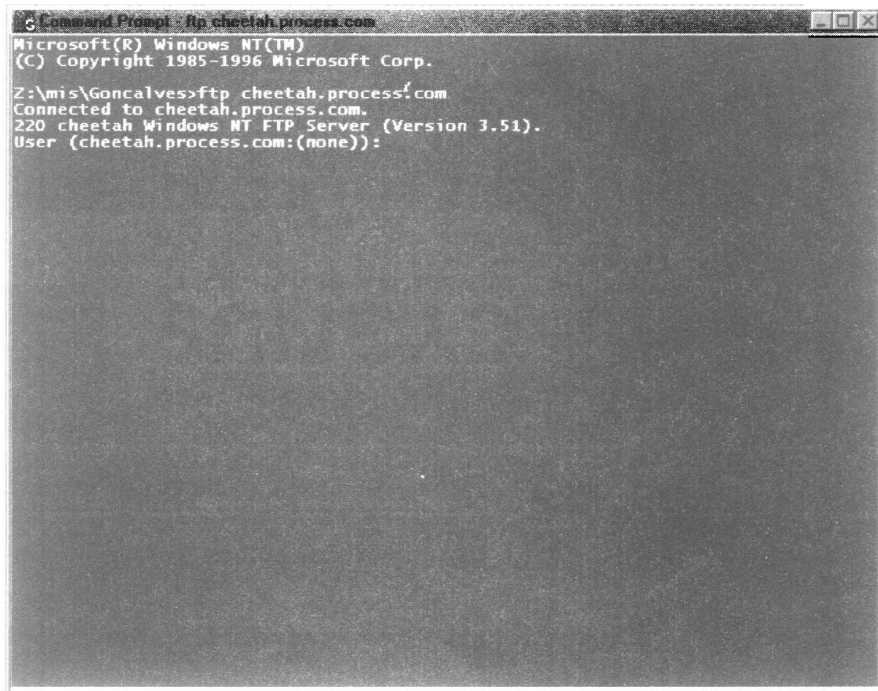
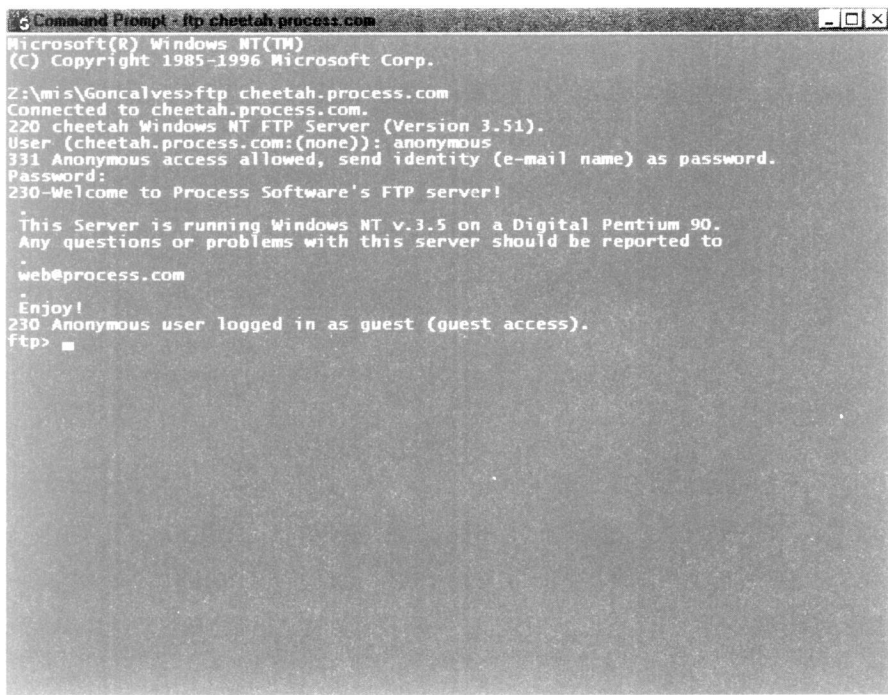


图2-11 连接至FTP站点

然有些站点或某个站点的一些领域需要认证，但通常可以匿名方式登录。

进程登录时，必须输入用户名，在匿名连接时是“anonymous”，而口令一般是你的e-mail地址（并不要求这样，而是常规的和礼节性的做法，以便站点可跟踪FTP使用级别）。

图2-11显示了与FTP站点的登录连接。图2-12显示了连接后的认证过程。



```
Microsoft(R) Windows NT(TM)
(C) Copyright 1985-1996 Microsoft Corp.

Z:\mis\Goncalves>ftp cheetah.process.com
Connected to cheetah.process.com.
220 cheetah Windows NT FTP Server (Version 3.51).
User (cheetah.process.com:(none)): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230-Welcome to Process Software's FTP server!

This Server is running Windows NT v.3.5 on a Digital Pentium 90.
Any questions or problems with this server should be reported to
web@process.com

Enjoy!
230 Anonymous user logged in as guest (guest access).
ftp>
```

图2-12 匿名进入FTP站点的认证

你必须警惕匿名FTP。它与某人在你的网络服务器上使用“宾客”帐户进行登录十分相似。一旦黑客闯入你的FTP服务器，就可利用它使你的站点置于危险之中。因此，FTP服务器最起码应置于防火墙之外，或与你的服务器或依附在服务器上的工作站没有连接。

2.8 使用防火墙的一些挑战

用Java applet建立网络连接是大多数其他基于Web的应用软件所不具有的强大功能特性。它使得在因特网使用多功能客户/服务器应用成为可能。然而，防火墙的存在是向客户与服务器之间使用持久网络连接的Java applet的一种挑战。

在客户/服务器模型中，防火墙可能存在于服务器端，也可能存在于客户端，或者两端都有。在服务器端存在防火墙的情况下，服务器存在于私有网络中，但因特网客户有权访问此服务器。获得这种外部访问相对而言比较容易，并且对客户和服务器的应用程序都是透明的。本书的重点不是针对服务器端而是客户端的防火墙访问。

像Java applet这样的客户应用程序，可下载并在受保护网络中的计算机上运行。如果像Java applet建立了到服务器端的连接，服务器通常位于客户端的防火墙之外（即服务器使用了该applet）。建立此类连接的唯一办法就是通过客户端的代理服务器。困难在于客户可能是匿名的，因此，该applet在连接之前并不知道客户端防火墙和它的代理服务器。

因此，当进行网络互连时最主要的安全挑战是，受保护的网或者企业内部网与未受保护的网如因特网进行会聚，会聚成如图 2-13 所示的互连“网团”。

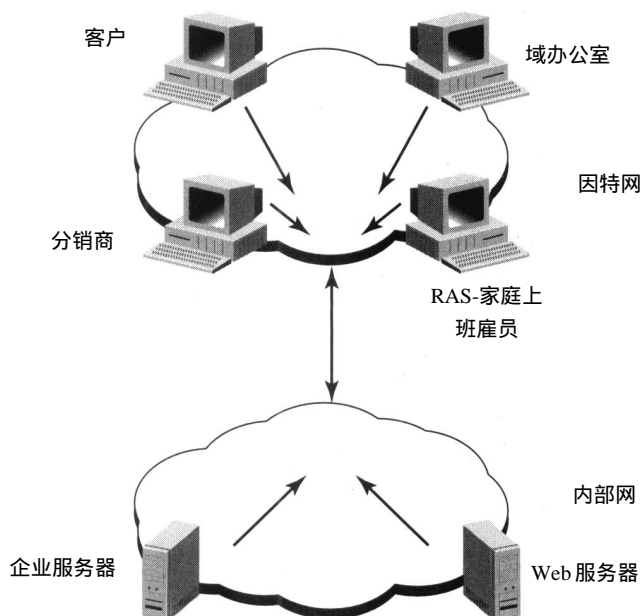


图2-13 匿名进入FTP站点的认证

图2-13 所示方案有些让人迷惑不解，因而是解决安全问题的时候了。因此，IS 部门急于设置安全工具，但多次都不太完善，不能作为一个完整的解决方案，不足以应付因特网对网络互连所带来的挑战。这就是为什么我们通常所看到的“网团”解决方案，最终结果不是一个可控、有效的网络安全系统，它的一系列安全措施就像一盘水果色拉，其中的调味品，不管是单独的或是组合的，包括（但不局限于）以下方面：

基于口令的安全性。

定制访问控制。

加密方案。

防火墙。

代理服务器。

有时我们什么也找不到！

为了利用因特网和 Web 带来的潜能，包括电子商务的巨大增长，商家应具备以下几点：

就像店铺需要向公众开门一样，向因特网开放，允许资源交易和联合识别。通过“快速穿越”环境销售商品不需太久时间。不过，在向因特网开放自己的内部网络时，公司必须保持访问控制，以控制哪些人可访问内部资源，而哪些不能。

识别和认证使用因特网访问联合网络的用户，包括使用 e-mail 和隧道连接的顾客。

确保通过公众因特网发送的私有信息安全传递，以保护客户和公司的利益。

这是在有效使用防火墙（不作为网团的一部分）时所遇到的一些主要挑战。我们，作为现在称为因特网管理员的人，有一个挑战，也是这本书的挑战，即成功有效地完成图 2-14 所

示的安全要求，在读完此书后，应完成这些要求。

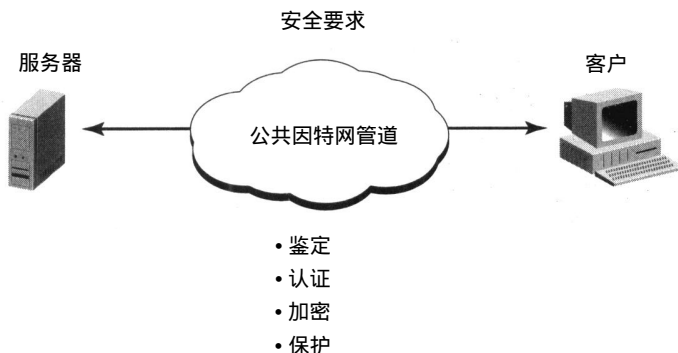


图2-14 一个组织的安全要求

2.9 IP网络日益增加的安全需求

正如你现在所意识到的那样，网络安全是一个范围很广的问题，它可能涉及数据链路层、网络或协议层和应用层。在数据链路层，包检查和加密问题可能发生；在网络或协议层，我们控制IP信息包和路由更新；在应用层，例如主机级故障成为问题。

随着你和你的机构对因特网日益增多的访问，以及机构网络的扩充，为你的 LAN/WAN和因特网提供安全这一挑战越来越困难。必须确定，所需保护的网路区域，懂得如何限制内部（和外部）用户和顾客，访问这些区域的用户权限，并确定应该过滤掉哪种类型的网络服务以防止发生潜在的违反安全的事件。

作为总结，第1章和这一章讲解了 IP协议和服务的许多特点和安全问题。本章还叙述了 IP协议和服务层的几个弱点，还提供了在 IP网络增加安全性的各种方法和可用于增强站点安全性的一些方法和过程。方法包括对通过控制台端口， Telnet， SNMP等对路由器及通信服务器的访问进行限制和控制，但这些方法是不够的，必须实现防火墙。尽管在第 1章中介绍了防火墙，但还需对它的体系结构和安装作进一步的讨论。在此之前，让我们先看一下被广泛有效使用的方法：加密。毕竟还存在这样一个问题：加密：足够吗？这就是在第 3章中所讨论的问题。