第27章　使 用 Telnet

作者：Neal S. Jamison

本章内容包括：

- 理解Telnet协议
- Telnet守护进程
- 使用Telnet
- 高级主题
- 参考文献和相关RFC

虽然终端仿真已不如以前应用广泛，但是它仍然是访问 Shell帐号及其他多用户系统的重要工具。同时，它也是解决问题的有效工具。本章主要讨论互联网中的终端仿真服务：TCP/IP Telnet协议及其相关软件。

27.1　理解Telnet协议

Telnet协议是TCP/IP协议簇的早期协议之一。事实上，早期的 RFC 15(写于1969年)就曾讨论过关于Telnet的一些有趣主题。Telnet目前在RFC 854中定义。

创建Telnet协议的初衷是简化与远程主机的连接。在早期，如果用户使用 IBM框架，需要IBM终端与框架连接；如果使用DEC，则需要DEC终端。结果如图27-1所示。

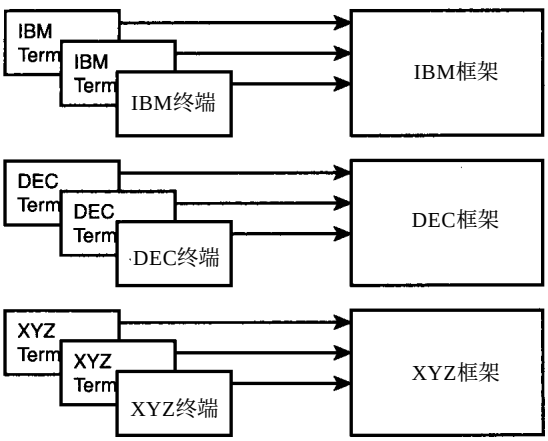

图27-1　在Telnet创建之前网络未得到广泛应用

因此，我们需要可以理解所有语言组属性的终端仿真服务。它使用户可以在一台终端前与多台互相区别的主机系统连接。因此，创建了 Telnet。

Telnet是登录远程主机的标准互联网应用协议。它提供编码规则和其他必要的服务以便用户系统与远程主机连接。

Telnet使用可靠的TCP传输机制以维护可靠、稳定的连接。Telnet的服务端口为TCP端口23。

Telnet可以以多种方式运行：

- 半双工
- 字符方式
- 行方式
- 线性方工

半双工方式已经很久不被使用了。

在字符方式中，每一个被敲入的字符立即传送到远程主机处理并将结果返回给客户。对于速度较慢的网络，其效果将不能忍受。目前许多 Telnet的实现均采用此方式。

在行方式中，文本在本地回显，一行结束时，将整行发送到远程主机处理过程。

在线性方式中，字符在本地处理，但处理过程由远程系统控制。

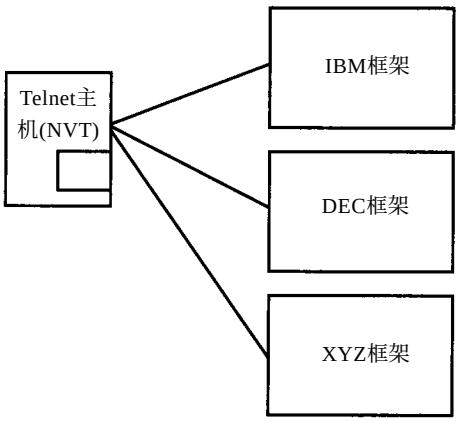

图27-2 Telnet及NVT简化终端到主机的连接

网络虚拟终端

因为我们使用多种不同类型的计算机，它们有不同的键盘和输出设备，所以 Telnet的任务十分重要。输入设备和计算机使用各种各样的语言，从ASCII码到各种EBCDIC方言。这使计算机间交流十分困难。网络虚拟终端 (NVT)的作用主要是简化计算机间的交流。客户、服务器及它们各自的网络虚拟终端工作方式如图 27-2所示。

NVT接收来自客户系统的输入并将它转化为通用语言。在主机上的 NVT接收通用语言并将它转化为主机可理解的特定语言。

NVT允许任何属性的客户与任意属性的主机，反之亦然。

27.2 Telnet守护进程

与其他TCP/IP客户/服务器服务类似，Telnet依靠守护进程响应客户请求。在UNIX系统中，守护进程为telnetd(或in.telnetd)。

注意 下面讲述的in.telnetd的用法及属性来自Linux操作系统帮助文件。用户系统的相关信息请查阅自己的操作系统文档或帮助文件。

用法：/usr/sbin/in.telnetd [-hns] [-a*认证模式*] [-D *调试模式*] [-L *登录程序*] [-S *服务类型*] [-X *认证类型*] [-edebug] [-debug *端口*]

属性：

-a 认证模式 —— 设置程序使用的认证模式。该属性仅在telnetd被编译支持认证时才可使用。下面列出了认证模式的可选值：

- debug —— 启用认证调试。
- user —— 当远程用户能够提供有效的认证信息以标识自身时才允许连接，并且允许访问无需口令的特定帐号。
- valid —— 仅当远程用户能够提供有效的认证信息标识自身时才允许连接。

• other —— 仅允许提供认证信息的连接。
• none —— 缺省状态。无需认证信息。
• off —— 关闭认证代码。

-D *调试模式* —— 该属性用于调试。它允许 telnetd打印出连接的调试信息，允许用户查看telnetd的工作过程，调试模式的可选值如下：

• options —— 打印telnet属性协商信息。
• report —— 打印属性信息及telnetd的工作信息。
• netdata —— 打印telnetd接收到的数据流。
• ptydata —— 显示发送到仿真终端的信息。

-edebug —— 启用加密调试。

-h —— 在登录完成前禁止打印与主机相关的信息。

-L*登录程序* —— 该属性用于指定不同的登录程序。缺省情况下使用 /bin/login。

-n —— 禁止TCP保持连接。通常， telnetd使用TCP保持连接机制查看已空闲一段时间的连接，以判断连接是否正常，并清除已经崩溃的连接。

-s —— 仅当telnetd被编译支持SecurID卡时，才可使用该属性。它使 -s属性应用于登录，当登录支持-s属性时，表示仅允许securID登录。它通常用于控制防火墙外的远程登录。

-S*服务类型* —— 将Telnet连接的IP服务类型(type-of-service，TOS)选项设置为tos。

-X*认证类型* —— 仅当telnetd被编译支持认证属性才可使用该属性。它禁止使用 auth 类型的认证，并且能暂时禁止特定的认证类型而无需重新编译 telnetd。

27.3 使用Telnet

Telnet非常容易使用。通常它由以下三步组成：

• 运行Telnet客户方命令初始化会话。
• 敲入登录ID和口令，
• 操作结束后，关闭会话。

Telnet有两种工作模式：输入和命令。然而，在大多数情况下，用户与 Telnet交互仅在打开或关闭会话时，并且主要以输入方式与远程操作系统或程序进行交互。

27.3.1 UNIX telnet命令

本书讨论Linux下telnet实现的用法与属性。用户将会发现大多数的 telnet实现都类似，可以从文档或帮助中获得telnet命令的详细信息。

用法：telnet [-8ELadr] [-S tos] [-e escapechar] [-l user] [-n tracefile] [host] [port]

属性：

-8 —— 请求8位操作。

-E —— 禁止ESC字符功能。

-L —— 指定8位输出数据的路径。

-a —— 尝试自动登录。如果远程主机支持，通过 USER传输用户名。

-d —— 设置调试布尔值的初始值为 True。

-r —— 仿真rlogin。

-S tos —— 设置Telnet连接的IP服务类型的值为tos。
-e escapechar —— 将esc字符的值指定为escapechar。
-l user —— 将user指定为登录到远程主机的用户名，与 -a属性类似。
-n tracefile —— 打开tracefile文件读取路径信息。
host —— 指定host为通过网络连接的主机。
port —— 指定端口号或服务名称。如果不指定，则使用 23号端口。

27.3.2 Telnet GUI应用

目前流行多种基于GUI的Telnet应用程序，它们为非UNIX用户提供方便易用的客户端程序。其中最为流行的两个版本为Microsoft Telnet和CRT。Microsoft Telnet与微软Windows操作系统(Windws NT、Windows 98等)一并发售。CRT是VanDyke技术公司的共享软件，它可从Winodws共享软件站点下载。

图27-3和图27-4显示两个应用程序的界面。

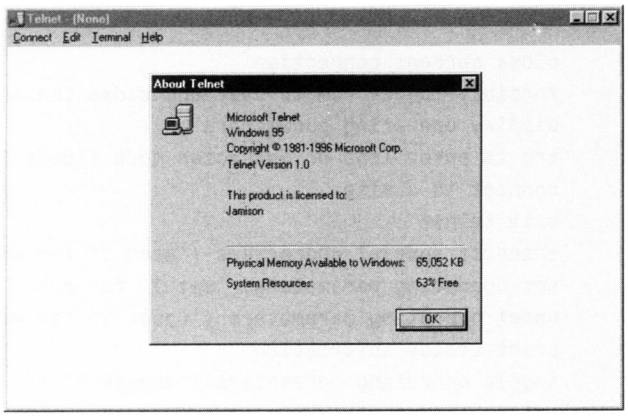

图27-3 Microsoft Telnet应用

图27-4 另外一个流行的终端仿真应用(Van Dyke技术公司的CRT)

27.3.3 Telnet命令

由于telnet简单的用户接口，因此任何用户都可轻易掌握下述 telnet命令。正如上面曾提到

过的，大多数(几乎全部)Telnet会话均采用输入模式与远程操作系统或程序会话。高级用户或系统管理员可能会发现某些命令(如TOGGLE)在查错纠错时非常有用。

Telnet命令的帮助文件可在命令行方式下通过执行 Help命令获得。例如：

```
$ telnet
telnet> help
Commands may be abbreviated.  Commands are:
close           close current connection
logout          forcibly logout remote user and close the connection
display         display operating parameters
mode            try to enter line or character mode ('mode ?' for more)
open            connect to a site
quit            exit telnet
send            transmit special characters ('send ?' for more)
set             set operating parameters ('set ?' for more)
unset           unset operating parameters ('unset ?' for more)
status          print status information
toggle          toggle operating parameters ('toggle ?' for more)
slc             set treatment of special characters

z               suspend telnet
environ         change environment variables ('environ ?' for more)
telnet>
```

要获得某个特定命令的帮助可在命令后加上“？”，例如：

```
telnet> mode ?
format is:  'mode Mode', where 'Mode' is one of:

character       Disable LINEMODE option
                (or disable obsolete line-by-line mode)
line            Enable LINEMODE option
                (or enable obsolete line-by-line mode)

                These require the LINEMODE option to be enabled
isig            Enable signal trapping
-isig           Disable signal trapping
edit            Enable character editing
-edit           Disable character editing
softtabs        Enable tab expansion
-softtabs       Disable character editing
litecho         Enable literal character echo
-litecho        Disable literal character echo

?               Print help information
telnet>
```

表27-1描述了完整的Telnet命令集合。

注意 表27-1、表27-2和表27-3中列出的Telnet命令及属性信息都来自Linux操作系统的帮助文件。用户自己的操作系统的相关信息，可从用户操作系统文档及帮助文件中获得。

表27-1 Telnet命令

命 令	描 述
CLOSE	关闭到远程主机的连接
DISPLAY	显示特定的操作参数
ENVIRON	修改或增加环境变量
HELP (?)	显示帮助信息(同样？命令可获得指定命令的帮助信息)
LOGOUT	强行退出远程用户并关闭连接。与Close类似
MODE	询问服务器是否为行或字符模式
OPEN	打开到特定主机的连接
QUIT	关闭会话，退出Telnet
SEND	传输特定的协议字符序列，见表27-3
SET	设置操作参数。参见UNSET命令
SLC	(设置本地参数)设置特殊字符的定义及意义
STATUS	显示当前状态信息，如主机、模式等等
TOGGLE	激活操作参数。表27-2列出了常用的操作参数
UNSET	取消操作参数的设置，参见SET命令
Z	挂起 Telnet(挂起命令可由fg命令恢复)
! [Command]	执行特定的shell命令。如果没有给出命令，将打开子shell

上述命令中，某些命令需要更详细的参数，如 TOGGLE和SEND。表27-2列出了TOGGLE命令的常用属性，表27-3列出Telnet SEND命令的属性集合。

TOGGLE命令激活(TRUE或FALSE)特定属性。

表27-2 Telnet中TOGGLE命令需用的属性

命 令	描 述
debug	激活socket级的调试。其初始值为FALSE
skiprc	当skiprc的值为TRUE时， Telnet不读取.telnetrc文件。初始值为FALSE
?	显示可用的toggle命令

SEND用于传输命令和属性到远程主机。表 27-3列出了SEND命令属性。

表27-3 Telnet中Send命令的属性

命 令	描 述
EOF	文件结束符
SUSP	挂起当前处理过程(作业控制)
ABORT	终止处理过程
EOR	记录结束
SE	子属性结束标记
NOP	空操作
DM	数据标记
BRK	中止
IP	中断处理
AO	终止输出
AYT	对方是否仍在运行(Are you there？)
EC	ESC字符
EL	擦除行

(续)

命 令	描 述
GA	继续
SB	子属性开始
WILL	属性协商
WONT	属性协商
DO	属性协商
DON ’ T	属性协商
IAC	数据字节255

27.3.4 示例

下述示例显示会话的属性协商过程，用户可以通过 TOGGLE OPTIONS命令获得冗余输出。

```
% telnet
telnet> toggle options
Will show option processing.
telnet> open host1.mydomain.com
Trying...
Connected to host1.mydomain.com.
Escape character is '^]'.
SENT DO SUPPRESS GO AHEAD
SENT WILL TERMINAL TYPE
SENT WILL NAWS
SENT WILL TSPEED
SENT WILL LFLOW
SENT WILL LINEMODE
SENT WILL NEW-ENVIRON
SENT DO STATUS
RCVD DO TERMINAL TYPE
RCVD DO TSPEED
RCVD DO XDISPLOC
SENT WONT XDISPLOC
RCVD DO NEW-ENVIRON
RCVD WILL SUPPRESS GO AHEAD
RCVD DO NAWS
SENT IAC SB (terminated by -1 -16, not IAC SE!) NAWS 0 95 (95) 0 29 (29)
RCVD DO LFLOW
RCVD DONT LINEMODE
RCVD WILL STATUS
RCVD IAC SB (terminated by -1 -16, not IAC SE!) TERMINAL-SPEED SEND
RCVD IAC SB (terminated by -1 -16, not IAC SE!) ENVIRON SEND
SENT IAC SB (terminated by -1 -16, not IAC SE!) ENVIRON IS
RCVD IAC SB (terminated by -1 -16, not IAC SE!) TERMINAL-TYPE SEND
RCVD DO ECHO
SENT WONT ECHO
RCVD WILL ECHO
SENT DO ECHO
```

```
Access to this system is restricted to authorized users only.
login:
```

27.4 高级主题

本节讨论与Telnet相关的主题。这些主题包括安全、 Telnet应用及使用Telnet访问其他流行的TCP/IP服务。

27.4.1 安全

与其他TCP程序及应用类似， Telnet也伴随安全问题。但是，有许多工具可以加强 Telnet的安全性或完全取代Telnet。

1. TCP Wrapper

TCP Wrapper(有时称为tcpd)包围在TCP守护进程之外，为TCP程序提供监听和过滤功能。使用TCP Wrapper，用户可以配置系统使用户的 Telnet仅响应特定网络或域中计算机的请求。TCP Wrapper由Wietse Venema开发。

Wrapper已经预装入了某些系统。用户需要根据自己的系统下载并安装正确的 TCP Wrapper。

2. 配置/etc/hosts.allow和/etc/hosts.deny文件

主机或TCP Wrapper使用这些文件来限制用户可以 /不可以使用某些特定的命令。便如hosts.deny文件包含：

In.telnetd: All

hosts.allow文件包含：

in.telnetd: *.mydomain.com

在上述示例中， hosts.deny文件拒绝任何 Telnet访问请求。 hosts.allow文件允许mydomain.com中主机的访问请求。

要查询关于 TCP Wrapper更详细的信息，参见 ftp://ftp. porcupine. org/pub /security /index.html。

3. 安全Shell

安全Shell(SSH)的功能与Telnet类似。但是它采用了加密机制，如数据加密标准 (DES)和RSA主机认证， SSH可以保护主机免受多种攻击的侵害，如 IP欺骗及口令窃听。

SSH可以免费应用于非商业应用。要了解 SSH更详细的信息，可查询 http://www. ssh.fi/sshprotocols2/。

27.4.2 Telnet应用

Telnet通常用于访问远程应用。 Hytelnet包含Telnet可访问的图书馆及各种可用资源。虽然其中部分站点已经消失或可用 Web访问，但大多数站点仍然可用。

图27-5和图27-6显示基于Winodws的Hytelnet 6.9。

其他Telnet应用包括Whois及Finger接口，其具体内容参见第 25章。

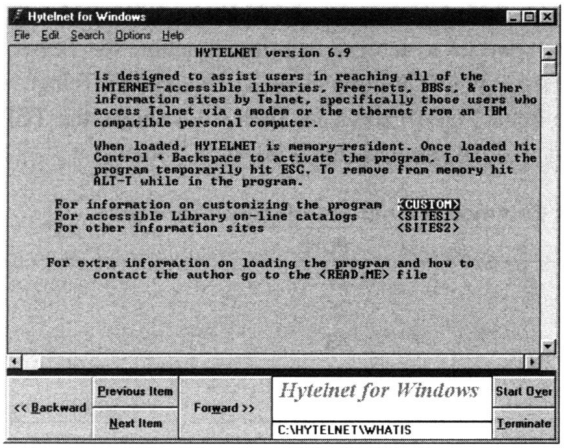

图27-5 基于Windows的Hytelnet

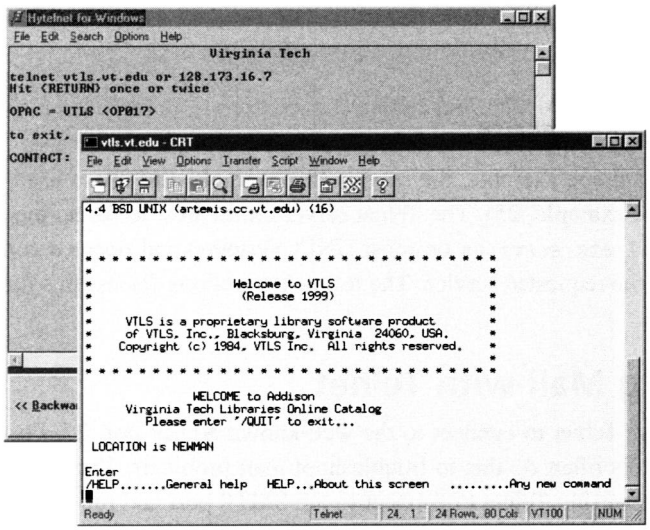

图27-6 使用基于Windows的Hytelnet和CRT访问在线图书馆

27.4.3 使用Telnet访问其他TCP/IP服务

Telnet使用端口23实现其主要功能， Telnet守护进程还可监听和响应其他 TCP端口。这一特性使Telnet可用于连接其他TCP/IP服务。表27-4列出了部分可用Telnet访问的TCP/IP服务所使用的TCP端口。

表27-4 Telnet可连接的TCP服务端口

服 务	端 口
FTP	21
SMTP	25
Whois	43
Finger	79
HTTP	80

用户可使用Telnet命令与这些服务建立连接。命令形式如下：

telnet *主机名 端口*

或

telnet *主机名 服务*

在后一种命令形式中，可用服务(如SMTP)代替端口号。运行在主机上的telnet服务器从系统文件(大多数UNIX系统中为/etc/services文件)中查找服务对应的端口并与该端口建立连接。下一节将对此作进一步讨论并给出一些示例。

1. 使用Telnet发送邮件

用户可以使用Telnet与SMTP端口25建立连接。邮局管理员及系统管理员通常使用此方法检查邮件中的问题。下面的示例说明使用Telnet与SMTP端口建立连接并运行确认(VRFY)命令。需要了解关于SMTP的更详细的信息，参见31章。

```
$ telnet host.mydomain.com SMTP
Trying...
Connected to host.mydomain.com.
Escape character is '^]'.
220 host.mydomain.com ESMTP Sendmail 8.8.8+Sun/8.8.8; 8 Aug 1999 17:14
vrfy jamisonn
250 Neal Jamison <jamisonn@host.mydomain.com>
quit
221 host.mydomain.com closing connection
Connection closed by foreign host.
```

通过执行恰当的STMP命令，甚至可以使用telnet发送邮件。

2. Finger

用户也可以使用telnet与远程主机的Finger端口(79)建立连接，如下所示：

```
$ telnet host1.mydomain.com 79
Trying ...
Connected to host1.mydomain.com.
Escape character is '^]'.
jamisonn
Login: jamisonn                         Name: Neal Jamison
Directory: /users/home/jamisonn         Shell: /bin/tcsh
On since Sun Aug  8 17:16 (EDT) on ttyp7 from pool180-68
No mail.
No Plan.
Connection closed by foreign host.
```

一旦建立连接，用户可敲入在线查询 (jamisonn)命令。Finger服务器将对查询作出响应。如果用户的主机没有安装Finger客户端，这就是一种非常方便的方法。要查看关于 Finger的更详细信息，参见第25章。

3. 使用Telnet网上冲浪

Telnet也可用于访问Web访问器的HTTP端口(80)，如下例所示：

```
$ telnet mywebserver.com 80
Trying...
Connected to mywebserver.com.
Escape character is '^]'.
```

```
GET /
<HTML>
<HEAD>
<TITLE>Makos Corporation</TITLE>
</HEAD>
<BODY>
<H1>Welcome to Makos Corporation</H1>
<p>
This is the homepage of Makos Corporation.
<br><br>
</BODY>
</HTML>

Connection closed by foreign host.
```

连接建立后，敲入HTTP命令GET/。这一命令请求Web服务器的缺省文档。除非用户可像浏览器一样理解HTML，否则返回的信息难以识别。此例仅作说明使用。要获取关于 HTTP的更详细信息，参见第32章。

27.5 相关RFC文档

下列RFC文档讨论Telnet及与Telnet有关的主题：

15	分时主机网络子系统(C.S. Carr，1969)
854	Telnet 协议规范(J.Postel, J.K. Reynolds，1983)
855	Telnet 属性规范(J.Postel, J.K. Reynolds，1983)
856	Telnet 二进制传输(J.Postel, J.K. Reynolds，1983)
857	Telnet 应答属性(J.Postel, J.K. Reynolds，1983)
858	Telnet压缩传输属性(J.Postel, J.K. Reynolds，1983)
859	Telnet 状态属性(J.Postel, J.K. Reynolds，1983)
860	Telnet 时间标记属性(J.Postel, J.K. Reynolds，1983)
861	Telnet 扩展属性：列表属性(J.Postel, J.K. Reynolds，1983)
1123	互联网主机需求 —— 应用和支持(R.T. Braden，1989)
1184	Telnet 线性模式属性(D.A. Borman，1990)
1250,5250	Telnet 接口(P. Chmielewski，1991)
1372	Telnet 远程流量控制属性(C. Hedrick, D. Borman，1992)
1408	Telnet 环境属性(D.Borman, Editor，1993)
1411	Telnet 认证：Kerberos 版本4.(D.Borman, Editor，1993)
1412	Telnet 认证：SPX(K. Alagappan，1993)
1416	Telnet 认证属性(D.Borman, Editor，1993)
1571	Telnet 环境属性互操作(D.Borman，1994)
1572	Telnet 环境属性(S. Alexander，1994)
2066	Telnet CHARSET 属性(R. Gellens，1997)
2217	Telnet Com 端口控制属性(G. Clark，1997)

以下RFC文档讨论与Telnet相关但不是很关键的主题：

748 Telnet 随机释放属性(M.R. Crispin，1978)

1097 Telnet 部分限制消息属性(B. Miller，1989)

27.6 小结

本章详细描述了TCP/IP终端仿真协议Telnet。正如本章所述，Telnet解决了由于互联网的诞生而引起的终端不兼容问题。由于Telnet和网络虚拟终端的存在，科学家及科研工作者可在同一台终端对多个主机进行操作。

本章详细讲解了通用UNIX系统的Telnet客户及服务器方命令的语法格式及相关属性(虽然它们极少被最终用户使用)。

本章还讨论了Telnet应用的安全问题。并讲解了如何使用Telnet连接和使用其他TCP/IP服务，如SMTP、mail、Finger和HTTP等。

最后，本章列出了与Telnet相关的所有RFC文档，包括最初的RFC文档：RFC 15，写于1969年。