<https://baike.baidu.com/item/Telnet>

Telnet协议是[TCP/IP协议](https://baike.baidu.com/item/TCP%2FIP%E5%8D%8F%E8%AE%AE)族中的一员，是Internet[远程登陆](https://baike.baidu.com/item/%E8%BF%9C%E7%A8%8B%E7%99%BB%E9%99%86)服务的标准协议和主要方式。它为用户提供了在本地计算机上完成远程[主机](https://baike.baidu.com/item/%E4%B8%BB%E6%9C%BA)工作的能力。在[终端](https://baike.baidu.com/item/%E7%BB%88%E7%AB%AF)使用者的电脑上使用telnet程序，用它连接到[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)。[终端](https://baike.baidu.com/item/%E7%BB%88%E7%AB%AF)使用者可以在telnet程序中输入命令，这些命令会在[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)上运行，就像直接在服务器的控制台上输入一样。可以在本地就能控制[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)。要开始一个telnet会话，必须输入用户名和密码来登录[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)。Telnet是常用的[远程控制](https://baike.baidu.com/item/%E8%BF%9C%E7%A8%8B%E6%8E%A7%E5%88%B6)Web[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)的方法。

Telnet服务虽然也属于客户机/[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)模型的服务，但它更大的意义在于实现了基于Telnet协议的远程登录（远程交互式计算），那么就让我们来认识一下远程登录。

### 定义

先来看看什么叫登录：[分时系统](https://baike.baidu.com/item/%E5%88%86%E6%97%B6%E7%B3%BB%E7%BB%9F" \t "_blank)允许多个用户同时使用一台计算机，为了保证系统的安全和记账方便，系统要求每个用户有单独的帐号作为登录标识，系统还为每个用户指定了一个口令。用户在使用该系统之前要输入标识和口令，这个过程被称为'登录'。　[远程登录](https://baike.baidu.com/item/%E8%BF%9C%E7%A8%8B%E7%99%BB%E5%BD%95" \t "_blank)是指用户使用Telnet命令，使自己的计算机暂时成为远程[主机](https://baike.baidu.com/item/%E4%B8%BB%E6%9C%BA" \t "_blank)的一个仿真[终端](https://baike.baidu.com/item/%E7%BB%88%E7%AB%AF)的过程。仿真[终端](https://baike.baidu.com/item/%E7%BB%88%E7%AB%AF)等效于一个非智能的机器，它只负责把用户输入的每个字符传递给[主机](https://baike.baidu.com/item/%E4%B8%BB%E6%9C%BA)，再将主机输出的每个信息[回显](https://baike.baidu.com/item/%E5%9B%9E%E6%98%BE)在[屏幕](https://baike.baidu.com/item/%E5%B1%8F%E5%B9%95)上。

### 产生和发展

我们可以先构想一个提供远程文字编辑的服务，这个服务的实现需要一个接受编辑文件请求和数据的[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8" \t "_blank)以及一个发送此请求的客户机。客户机将建立一个从本地机到[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)的TCP连接，当然这需要服务器的应答，然后向服务器发送键入的信息（文件编辑信息），并读取从服务器返回的输出。以上便是一个标准而普通的客户机/[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)模型的服务。

似乎有了客户机/[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)模型的服务，一切远程问题都可以解决了。然而实际并非你想象的那样简单，如果我们仅需要远程编辑文件，那么刚才所构想的服务完全可以胜任，但假如我们的要求并不是这么简单，我们还想实现远程用户管理，远程数据录入，远程[系统维护](https://baike.baidu.com/item/%E7%B3%BB%E7%BB%9F%E7%BB%B4%E6%8A%A4)，想实现一切可以在远程[主机](https://baike.baidu.com/item/%E4%B8%BB%E6%9C%BA)上实现的操作，那么我们将需要大量专用的[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)程序并为每一个可计算服务都使用一个服务器进程，随之而来的问题是：远程机器会很快对服务器进程应接不暇，并淹没在进程的海洋里（我们在这里排除最专业化的远程机器）。

那么有没有办法解决呢？当然有，我们可以用[远程登录](https://baike.baidu.com/item/%E8%BF%9C%E7%A8%8B%E7%99%BB%E5%BD%95)来解决这一切。我们允许用户在远地机器上建立一个登录会话，然后通过执行命令来实现更一般的服务，就像在本地操作一样。这样，我们便可以访问远地系统上所有可用的命令，并且系统设计员不需提供多个专用地[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)程序。

问题发展到这里好像前途一片光明了，用[远程登录](https://baike.baidu.com/item/%E8%BF%9C%E7%A8%8B%E7%99%BB%E5%BD%95)总应该解决问题了吧，但要实现远程登录并不简单。不考虑网络设计的[计算机系统](https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%B3%BB%E7%BB%9F)期望用户只从直接相连的键盘和显示器上登录，在这种机器上增加[远程登录](https://baike.baidu.com/item/%E8%BF%9C%E7%A8%8B%E7%99%BB%E5%BD%95)功能需要修改机器的[操作系统](https://baike.baidu.com/item/%E6%93%8D%E4%BD%9C%E7%B3%BB%E7%BB%9F)，这是极其艰巨也是我们尽量避免的。因此我们应该集中力量构造[远程登录](https://baike.baidu.com/item/%E8%BF%9C%E7%A8%8B%E7%99%BB%E5%BD%95)[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)[软件](https://baike.baidu.com/item/%E8%BD%AF%E4%BB%B6)，虽然这样也是比较困难的。为什么说这样做也比较困难呢？

举个例子来说：一般，[操作系统](https://baike.baidu.com/item/%E6%93%8D%E4%BD%9C%E7%B3%BB%E7%BB%9F)会为一些特殊按键分配特殊的含义，比如本地系统将'Ctrl+C'解释为：'终止当前运行的命令进程'。但假设我们已经运行了[远程登录](https://baike.baidu.com/item/%E8%BF%9C%E7%A8%8B%E7%99%BB%E5%BD%95" \t "_blank)[服务器软件](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8%E8%BD%AF%E4%BB%B6)，'Ctrl+C'也有可能无法被传送到远地机器，如果客户机真的将'Ctrl+C'传到了远地机器，那么'Ctrl+C'这个命令有可能不能终止本地的进程，也就是说在这里很可能会产生混乱。而且这仅仅是遇到的难题之一。

但尽管有技术上的困难，[系统编程](https://baike.baidu.com/item/%E7%B3%BB%E7%BB%9F%E7%BC%96%E7%A8%8B)人员还是设法构造了能够应用于大多数[操作系统](https://baike.baidu.com/item/%E6%93%8D%E4%BD%9C%E7%B3%BB%E7%BB%9F)的[远程登录](https://baike.baidu.com/item/%E8%BF%9C%E7%A8%8B%E7%99%BB%E5%BD%95)[服务器软件](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8%E8%BD%AF%E4%BB%B6)，并构造了充当客户机的[应用软件](https://baike.baidu.com/item/%E5%BA%94%E7%94%A8%E8%BD%AF%E4%BB%B6)。通常，客户机[软件](https://baike.baidu.com/item/%E8%BD%AF%E4%BB%B6)取消了除一个键以外的所有键的本地解释，并将这些本地解释相应的转换成远地解释，这就使得客户机软件与远地机器的交互，就如同坐在远程[主机](https://baike.baidu.com/item/%E4%B8%BB%E6%9C%BA)面前一样，从而避免了上述所提到的混乱。而那个唯一例外的键，可以使用户回到本地环境。

将[远程登录](https://baike.baidu.com/item/%E8%BF%9C%E7%A8%8B%E7%99%BB%E5%BD%95)[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)设计为应用级[软件](https://baike.baidu.com/item/%E8%BD%AF%E4%BB%B6)，还有另一个要求，那就是需要[操作系统](https://baike.baidu.com/item/%E6%93%8D%E4%BD%9C%E7%B3%BB%E7%BB%9F)提供对[伪终端](https://baike.baidu.com/item/%E4%BC%AA%E7%BB%88%E7%AB%AF)（pseudo terminal）的支持。我们用[伪终端](https://baike.baidu.com/item/%E4%BC%AA%E7%BB%88%E7%AB%AF" \t "_blank)描述[操作系统](https://baike.baidu.com/item/%E6%93%8D%E4%BD%9C%E7%B3%BB%E7%BB%9F)的入口点，它允许像Telnet[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)一样的程序向操作系统传送字符，并且使得字符像是来自本地键盘一样。只有使用这样的[操作系统](https://baike.baidu.com/item/%E6%93%8D%E4%BD%9C%E7%B3%BB%E7%BB%9F)，才能将[远程登录](https://baike.baidu.com/item/%E8%BF%9C%E7%A8%8B%E7%99%BB%E5%BD%95)[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)设计为应用级[软件](https://baike.baidu.com/item/%E8%BD%AF%E4%BB%B6)（比如Telnet[服务器软件](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8%E8%BD%AF%E4%BB%B6)），否则，本地操作系统和远地系统传送将不能识别从对方传送过来的信息（因为它们仅能识别从本地键盘所键入的信息），远程登录将宣告失败。

将[远程登陆](https://baike.baidu.com/item/%E8%BF%9C%E7%A8%8B%E7%99%BB%E9%99%86" \t "_blank)[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)设计为应用级[软件](https://baike.baidu.com/item/%E8%BD%AF%E4%BB%B6)虽然有其显著的优点：比将代码嵌入[操作系统](https://baike.baidu.com/item/%E6%93%8D%E4%BD%9C%E7%B3%BB%E7%BB%9F)更易修改和控制服务器。但其也有效率不高的缺点（后面的内容将会给予解释），好在用户键入信息的速率不高，这种设计还是可以接受的。

### 工作过程

使用Telnet协议进行[远程登录](https://baike.baidu.com/item/%E8%BF%9C%E7%A8%8B%E7%99%BB%E5%BD%95" \t "_blank)时需要满足以下条件：在本地计算机上必须装有包含Telnet协议的客户程序；必须知道远程[主机](https://baike.baidu.com/item/%E4%B8%BB%E6%9C%BA" \t "_blank)的Ip地址或[域名](https://baike.baidu.com/item/%E5%9F%9F%E5%90%8D" \t "_blank)；必须知道登录标识与口令。

[Telnet远程登录](https://baike.baidu.com/item/Telnet%E8%BF%9C%E7%A8%8B%E7%99%BB%E5%BD%95)服务分为以下4个过程：

1）本地与远程[主机](https://baike.baidu.com/item/%E4%B8%BB%E6%9C%BA" \t "_blank)建立连接。该过程实际上是建立一个TCP连接，用户必须知道远程[主机](https://baike.baidu.com/item/%E4%B8%BB%E6%9C%BA" \t "_blank)的Ip地址或[域名](https://baike.baidu.com/item/%E5%9F%9F%E5%90%8D" \t "_blank)；

2）将[本地终端](https://baike.baidu.com/item/%E6%9C%AC%E5%9C%B0%E7%BB%88%E7%AB%AF" \t "_blank)上输入的用户名和口令及以后输入的任何命令或字符以[NVT](https://baike.baidu.com/item/NVT)（Net Virtual Terminal）格式传送到远程主机。该过程实际上是从[本地主机](https://baike.baidu.com/item/%E6%9C%AC%E5%9C%B0%E4%B8%BB%E6%9C%BA" \t "_blank)向远程主机发送一个IP数据包；

3）将远程[主机](https://baike.baidu.com/item/%E4%B8%BB%E6%9C%BA" \t "_blank)输出的[NVT](https://baike.baidu.com/item/NVT)格式的数据转化为本地所接受的格式送回[本地终端](https://baike.baidu.com/item/%E6%9C%AC%E5%9C%B0%E7%BB%88%E7%AB%AF" \t "_blank)，包括输入命令[回显](https://baike.baidu.com/item/%E5%9B%9E%E6%98%BE)和命令执行结果；

4）最后，[本地终端](https://baike.baidu.com/item/%E6%9C%AC%E5%9C%B0%E7%BB%88%E7%AB%AF" \t "_blank)对远程主机进行撤消连接。该过程是撤销一个TCP连接。

上面的内容只是讨论了[远程登陆](https://baike.baidu.com/item/%E8%BF%9C%E7%A8%8B%E7%99%BB%E9%99%86)最基本的东西，其中的复杂和编程人员的艰辛是我们难以想象的，不知道你在舒服的使用Telnet的同时，是否想到了这些！

## 功能

### 用途

Telnet是Internet远程登录服务的标准协议和主要方式，最初由ARPANET开发，现在主要用于Internet会话，它的基本功能是允许用户登录进入远程主机系统。

Telnet可以让我们坐在自己的计算机前通过Internet网络登录到另一台远程计算机上，这台计算机可以是在隔壁的房间里，也可以是在地球的另一端。当登录上远程计算机后，本地计算机就等同于远程计算机的一个终端，我们可以用自己的计算机直接操纵远程计算机，享受远程计算机本地终端同样的操作权限。

Telnet的主要用途就是使用远程计算机上所拥有的本地计算机没有的信息资源，如果远程的主要目的是在本地计算机与远程计算机之间传递文件，那么相比而言使用FTP会更加快捷有效。

### 交互过程

当我们使用Telnet登录进入远程计算机系统时，事实上启动了两个程序：一个是Telnet客户程序，运行在本地主机上；另一个是Telnet服务器程序，它运行在要登录的远程计算机上。

本地主机上的Telnet客户程序主要完成以下功能：

* 建立与远程服务器的TCP联接。
* 从键盘上接收本地输入的字符。
* 将输入的字符串变成标准格式并传送给远程服务器。
* 从远程服务器接收输出的信息。
* 将该信息显示在本地主机屏幕上。

远程主机的“服务”程序通常被昵称为“精灵”，它平时不声不响地守候在远程主机上，一接到本地主机的请求，就会立马活跃起来，并完成以下功能：

* 通知本地主机，远程主机已经准备好了。
* 等候本地主机输入命令。
* 对本地主机的命令作出反应（如显示目录内容，或执行某个程序等）。
* 把执行命令的结果送回本地计算机显示。
* 重新等候本地主机的命令。

在Internet中，很多服务都采取这样一种客户/服务器结构。对使用者来讲，通常只要了解客户端的程序就可以了。

### 安全隐患

虽然Telnet较为简单实用也很方便，但是在格外注重安全的现代网络技术中，Telnet并不被重用。原因在于Telnet是一个明文传送协议，它将用户的所有内容，包括用户名和密码都明文在互联网上传送，具有一定的安全隐患，因此许多服务器都会选择禁用Telnet服务。如果我们要使用Telnet的远程登录，使用前应在远端服务器上检查并设置允许Telnet服务的功能。

## 协议

我们知道Telnet服务器软件是我们最常用的远程登录服务器软件，是一种典型的客户机/服务器模型的服务，它应用Telnet协议来工作。那么，什么是Telnet协议？它都具备哪些特点呢？

### 基本内容

Telnet是位于OSI模型的第7层---[应用层](https://baike.baidu.com/item/%E5%BA%94%E7%94%A8%E5%B1%82)上的一种协议，是一个通过创建[虚拟终端](https://baike.baidu.com/item/%E8%99%9A%E6%8B%9F%E7%BB%88%E7%AB%AF)提供连接到远程[主机](https://baike.baidu.com/item/%E4%B8%BB%E6%9C%BA)[终端仿真](https://baike.baidu.com/item/%E7%BB%88%E7%AB%AF%E4%BB%BF%E7%9C%9F)的TCP/IP协议。这一协议需要通过用户名和口令进行认证，是Internet[远程登陆](https://baike.baidu.com/item/%E8%BF%9C%E7%A8%8B%E7%99%BB%E9%99%86)服务的标准协议。应用Telnet协议能够把[本地用户](https://baike.baidu.com/item/%E6%9C%AC%E5%9C%B0%E7%94%A8%E6%88%B7" \t "_blank)所使用的计算机变成远程[主机系统](https://baike.baidu.com/item/%E4%B8%BB%E6%9C%BA%E7%B3%BB%E7%BB%9F)的一个[终端](https://baike.baidu.com/item/%E7%BB%88%E7%AB%AF)。它提供了三种基本服务：

1）Telnet定义一个网络[虚拟终端](https://baike.baidu.com/item/%E8%99%9A%E6%8B%9F%E7%BB%88%E7%AB%AF" \t "_blank)为远程系统提供一个标准接口。客户机程序不必详细了解远程系统，他们只需构造使用标准接口的程序；

2）Telnet包括一个允许客户机和[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8" \t "_blank)协商选项的机制，而且它还提供一组标准选项；　.

3）Telnet对称处理连接的两端，即Telnet不强迫客户机从键盘输入，也不强迫客户机在[屏幕](https://baike.baidu.com/item/%E5%B1%8F%E5%B9%95" \t "_blank)上显示输出。

### 适应异构

为了使多个[操作系统](https://baike.baidu.com/item/%E6%93%8D%E4%BD%9C%E7%B3%BB%E7%BB%9F)间的Telnet交互操作成为可能，就必须详细了解异构计算机和操作系统。比如，一些[操作系统](https://baike.baidu.com/item/%E6%93%8D%E4%BD%9C%E7%B3%BB%E7%BB%9F" \t "_blank)需要每行文本用ASCⅡ回车控制符（CR）结束，另一些系统则需要使用ASCⅡ换行符（LF），还有一些系统需要用两个字符的序列回车-换行（CR-LF）；再比如，大多数操作系统为用户提供了一个中断程序运行的[快捷键](https://baike.baidu.com/item/%E5%BF%AB%E6%8D%B7%E9%94%AE" \t "_blank)，但这个快捷键在各个系统中有可能不同（一些系统使用CTRL+C，而另一些系统使用ESCAPE）。如果不考虑系统间的异构性，那么在本地发出的[字符](https://baike.baidu.com/item/%E5%AD%97%E7%AC%A6" \t "_blank)或命令，传送到远地并被远程[系统解释](https://baike.baidu.com/item/%E7%B3%BB%E7%BB%9F%E8%A7%A3%E9%87%8A)后很可能会不准确或者出现错误。因此，Telnet协议必须解决这个问题。　为了适应异构环境，Telnet协议定义了数据和命令在Internet上的传输方式，此定义被称作网络[虚拟终端](https://baike.baidu.com/item/%E8%99%9A%E6%8B%9F%E7%BB%88%E7%AB%AF" \t "_blank)[NVT](https://baike.baidu.com/item/NVT)（Net Virtual Terminal）。它的应用过程如下：　对于发送的数据：客户机[软件](https://baike.baidu.com/item/%E8%BD%AF%E4%BB%B6" \t "_blank)把来自用户终端的按键和命令序列转换为NVT格式，并发送到[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8" \t "_blank)，服务器软件将收到的数据和命令，从NVT格式转换为远地系统需要的格式；　对于返回的数据：远地服务器将数据从远地机器的格式转换为NVT格式，而本地客户机将接收到的NVT格式数据再转换为本地的格式。　对于[NVT](https://baike.baidu.com/item/NVT" \t "_blank)格式的详细定义，有兴趣的朋友可以去查找相关资料。

### 传送远程命令

我们知道绝大多数[操作系统](https://baike.baidu.com/item/%E6%93%8D%E4%BD%9C%E7%B3%BB%E7%BB%9F" \t "_blank)都提供各种[快捷键](https://baike.baidu.com/item/%E5%BF%AB%E6%8D%B7%E9%94%AE)来实现相应的控制命令，当用户在[本地终端](https://baike.baidu.com/item/%E6%9C%AC%E5%9C%B0%E7%BB%88%E7%AB%AF)键入这些快捷键的时候，本地系统将执行相应的控制命令，而不把这些快捷键作为输入。那么对于Telnet来说，它是用什么来实现控制命令的远程传送呢？　Telnet同样使用NVT来定义如何从客户机将控制功能传送到[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8" \t "_blank)。我们知道ASCⅡ[字符集](https://baike.baidu.com/item/%E5%AD%97%E7%AC%A6%E9%9B%86" \t "_blank)包括95个可打印字符和33个控制码。当用户从本地键入普通字符时，NVT将按照其原始含义传送；当用户键入[快捷键](https://baike.baidu.com/item/%E5%BF%AB%E6%8D%B7%E9%94%AE" \t "_blank)（组合键）时，NVT将把它转化为特殊的ASCⅡ字符在网络上传送，并在其到达远地机器后转化为相应的控制命令。

将正常ASCⅡ[字符集](https://baike.baidu.com/item/%E5%AD%97%E7%AC%A6%E9%9B%86" \t "_blank)与控制命令区分的原因：

1）这种区分意味着Telnet具有更大的灵活性：它可在客户机与[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8" \t "_blank)间传送所有可能的ASCⅡ字符以及所有控制功能；

2）这种区分使得客户机可以无二义性的指定信令，而不会产生控制功能与普通字符的混乱。　.

### 数据流向

上面我们提到过将Telnet设计为应用级[软件](https://baike.baidu.com/item/%E8%BD%AF%E4%BB%B6" \t "_blank)有一个缺点，那就是：效率不高。这是为什么呢？下面给出Telnet中的数据流向：

数据信息被用户从本地键盘键入并通过[操作系统](https://baike.baidu.com/item/%E6%93%8D%E4%BD%9C%E7%B3%BB%E7%BB%9F)传到客户机程序，客户机程序将其处理后返回操作系统，并由操作系统经过网络传送到远程机器，远程操作系统将所接收数据传给[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)程序，并经服务器程序再次处理后返回到操作系统上的[伪终端](https://baike.baidu.com/item/%E4%BC%AA%E7%BB%88%E7%AB%AF)入口点，最后，远程操作系统将[数据传送](https://baike.baidu.com/item/%E6%95%B0%E6%8D%AE%E4%BC%A0%E9%80%81)到用户正在运行的[应用程序](https://baike.baidu.com/item/%E5%BA%94%E7%94%A8%E7%A8%8B%E5%BA%8F)，这便是一次完整的输入过程；输出将按照同一通路从服务器传送到客户机。　因为每一次的输入和输出，计算机将切换进程环境好几次，这个开销是很昂贵的。还好用户的键入速率并不算高，这个缺点我们仍然能够接受。　.

### 强制命令

我们应该考虑到这样一种情况：假设[本地用户](https://baike.baidu.com/item/%E6%9C%AC%E5%9C%B0%E7%94%A8%E6%88%B7)运行了远地机器的一个无休止循环的错误命令或程序，且此命令或程序已经停止读取输入，那么[操作系统](https://baike.baidu.com/item/%E6%93%8D%E4%BD%9C%E7%B3%BB%E7%BB%9F)的[缓冲区](https://baike.baidu.com/item/%E7%BC%93%E5%86%B2%E5%8C%BA)可能因此而被占满，如果这样，远程[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)也无法再将数据写入[伪终端](https://baike.baidu.com/item/%E4%BC%AA%E7%BB%88%E7%AB%AF)，并且最终导致停止从TCP连接读取数据，TCP连接的缓冲区最终也会被占满，从而导致阻止数据流流入此连接。如果以上事情真的发生了，那么本地用户将失去对远程机器的控制。

为了解决此问题，Telnet协议必须使用外带信令以便强制[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8" \t "_blank)读取一个控制命令。我们知道TCP用紧急数据机制实现外带数据信令，那么Telnet只要再附加一个被称为数据标记（date mark）的保留八位组，并通过让TCP发送已设置紧急数据比特的报文段通知[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8" \t "_blank)便可以了，携带紧急数据的报文段将绕过[流量控制](https://baike.baidu.com/item/%E6%B5%81%E9%87%8F%E6%8E%A7%E5%88%B6)直接到达服务器。作为对紧急信令的相应，[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)将读取并抛弃所有数据，直到找到了一个数据标记。[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)在遇到了数据标记后将返回正常的处理过程。

由于Telnet两端的机器和[操作系统](https://baike.baidu.com/item/%E6%93%8D%E4%BD%9C%E7%B3%BB%E7%BB%9F" \t "_blank)的异构性，使得Telnet不可能也不应该严格规定每一个telnet连接的详细配置，否则将大大影响Telnet的适应异构性。因此，Telnet采用选项协商机制来解决这一问题。

Telnet选项的范围很广：一些选项扩充了大方向的功能，而一些选项制涉及一些微小细节。例如：有一个选项可以控制Telnet是在半双工还是全双工模式下工作（大方向）；还有一个选项允许远地机器上的[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8" \t "_blank)决定用户[终端](https://baike.baidu.com/item/%E7%BB%88%E7%AB%AF)类型（小细节）。

Telnet选项的协商方式也很有意思，它对于每个选项的处理都是对称的，即任何一端都可以发出协商申请；任何一端都可以接受或拒绝这个申请。另外，如果一端试图协商另一端不了解的选项，接受请求的一端可简单的拒绝协商。因此，有可能将更新，更复杂的Telnet客户机[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8" \t "_blank)版本与较老的，不太复杂的版本进行交互操作。如果客户机和[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)都理解新的选项，可能会对交互有所改善。否则，它们将一起转到效率较低但可工作的方式下运行。所有的这些设计，都是为了增强适应异构性，可见Telnet的适应异构性对其的应用和发展是多么重要。

上面讨论了一些原理方面的东西，虽然我们在Telnet的使用过程中很难接触到这一层面，但我认为了解这些是有意义的，它会给我们带来许多启示。下面让我们来看看Win2000的Telnet服务。

### 子选项协商

有些选项不是仅仅用“激活”或“禁止”就能够表达的。指定终端类型就是一个例子，客户进程必须发送用一个A S C I I字符串来表示终端类型。为了处理这种选项，我们必须定义子选项协商机制。

在R F C 1 0 9 1 [ VanBokkelen 1989]中定义了如何表示终端类型这样的子选项协商机制。首先连接的某一方（通常是客户进程）发送3个字节的字符序列来请求激活该选项。

<IAC,WILL,24>

这里的2 4（十进制）是终端类型选项的I D号。如果收端（通常是[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8" \t "_blank)进程）同意，那么响应数据是：

<IAC,DO,24>

然后[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8" \t "_blank)进程再发送如下的字符串：

<IAC,SB,24,1,IAC,SE>

该字符串询问客户进程的终端类型。其中S B是子选项协商的起始命令标志。下一个字节的“2 4”代表这是终端类型选项的子选项（通常S B后面的选项值就是子选项所要提交的内容）。下一个字节的“ 1”表示“发送你的终端类型”。子选项协商的结束命令标志也是I A C，就像S B是起始命令标志一样。如果终端类型是i b m p c，客户进程的响应命令将是：

第4个字节“0”代表“我的终端类型是”（在Assigned Numbers RFC文档中有正式的关于终端类型的数值定义，但是最起码在U n i x系统之间，终端类型可以用任何对方可理解的数据进行表示。只要这些数据在t e r m c a p或t e r m i n f o数据库中有定义）。在Te l n e t子选项协商过程中，终端类型用大写表示，当[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8" \t "_blank)收到该字符串后会自动转换为小写字符。

## 配置

其实从[应用层](https://baike.baidu.com/item/%E5%BA%94%E7%94%A8%E5%B1%82)面上，Win2000的Telnet服务并没有什么可说的，绝大部分内容你都可以从HELP文件中得到，我在此只是把它稍微整理一下而已。　Win2000为我们提供了Telnet客户机和[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8" \t "_blank)程序：Telnet.exe是客户机程序（Client），[tlntsvr.exe](https://baike.baidu.com/item/tlntsvr.exe" \t "_blank)是服务器程序（server），同时它还为我们提供了Telnet[服务器管理](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8%E7%AE%A1%E7%90%86)程序[tlntadmn.exe](https://baike.baidu.com/item/tlntadmn.exe)。

Windows 2000 默认安装了 Telnet 服务，但是并没有默认启动。下面给出HELP文件中 Telnet 服务的一部分默认设置：

AllowTrustedDomain：是否允许域用户访问。默认值是1，允许信任域用户访问。可以改为0: 不允许域用户访问（只允许[本地用户](https://baike.baidu.com/item/%E6%9C%AC%E5%9C%B0%E7%94%A8%E6%88%B7" \t "_blank)）。

DefaultDomain：可以对与该计算机具有信任关系的任何域设置。默认值是"."。

DefaultShell：显示 shell 安装的路径位置。默认值是：%systemroot%\System32\Cmd.exe /q /k

MaxFailedLogins：在连接终止之前显示尝试登录失败的最大次数。默认是3。

LoginScript：显示 Telnet[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)登录[脚本](https://baike.baidu.com/item/%E8%84%9A%E6%9C%AC)的路径位置。默认的位置就是“%systemroot%\System32\login.cmd”，你可以更改[脚本](https://baike.baidu.com/item/%E8%84%9A%E6%9C%AC" \t "_blank)内容，这样登录进Telnet的[欢迎屏幕](https://baike.baidu.com/item/%E6%AC%A2%E8%BF%8E%E5%B1%8F%E5%B9%95" \t "_blank)就不一样了。

NTLM：NTLM[身份验证](https://baike.baidu.com/item/%E8%BA%AB%E4%BB%BD%E9%AA%8C%E8%AF%81)选项。默认是2。可以有下面这些值：

0: 不使用 NTLM[身份验证](https://baike.baidu.com/item/%E8%BA%AB%E4%BB%BD%E9%AA%8C%E8%AF%81)。

1: 先尝试 NTLM[身份验证](https://baike.baidu.com/item/%E8%BA%AB%E4%BB%BD%E9%AA%8C%E8%AF%81)，如果失败，再使用用户名和密码。

2: 只使用 NTLM[身份验证](https://baike.baidu.com/item/%E8%BA%AB%E4%BB%BD%E9%AA%8C%E8%AF%81)。

TelnetPort：显示 telnet[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)侦听 telnet 请求的端口。默认是：23。你也可以更改为其他端口。

以上各项设置你可以使用[tlntadmn.exe](https://baike.baidu.com/item/tlntadmn.exe)（Telnet[服务器管理](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8%E7%AE%A1%E7%90%86)程序）来进行非常方便的配置，配置后需要重新启动Telnet服务。如图1

## NTLM

提到了telnet就不能不提NTLM，我想这也是让入侵者最为头痛的一件事，哪怕你获得了管理员帐号和密码，想简单通过NTLM也并非易事，况且win2000中的telnet默认仅以NTLM方式验证身份，这就让我们不得不关注NTLM这个东东，那么什么是NTLM呢？

早期的SMB协议在网络上明文传输口令，后来出现了"LAN Manager Challenge/Response"验证机制，简称LM，它十分简单以至很容易被破解，[微软](https://baike.baidu.com/item/%E5%BE%AE%E8%BD%AF" \t "_blank)随后提出了WindowsNT挑战/响应验证机制，即NTLM。现在已经有了更新的NTLMv2以及Kerberos验证体系。

## 流程

1．[客户端](https://baike.baidu.com/item/%E5%AE%A2%E6%88%B7%E7%AB%AF" \t "_blank)首先在本地加密当前用户的密码成为密码散列

2．[客户端](https://baike.baidu.com/item/%E5%AE%A2%E6%88%B7%E7%AB%AF" \t "_blank)向[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)发送自己的帐号，这个帐号是没有经过加密的，明文直接传输

3．[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8" \t "_blank)产生一个16位的随机[数字发送](https://baike.baidu.com/item/%E6%95%B0%E5%AD%97%E5%8F%91%E9%80%81" \t "_blank)给[客户端](https://baike.baidu.com/item/%E5%AE%A2%E6%88%B7%E7%AB%AF)，作为一个 challenge（查问口令；盘问）

4．[客户端](https://baike.baidu.com/item/%E5%AE%A2%E6%88%B7%E7%AB%AF" \t "_blank)再用加密后的密码散列来加密这个 challenge ，然后把这个返回给[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8" \t "_blank)。作为 response（响应）

5．[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8" \t "_blank)把用户名、给[客户端](https://baike.baidu.com/item/%E5%AE%A2%E6%88%B7%E7%AB%AF)的challenge 、客户端返回的 response 这三个东西，发送[域控制器](https://baike.baidu.com/item/%E5%9F%9F%E6%8E%A7%E5%88%B6%E5%99%A8" \t "_blank)

6．[域控制器](https://baike.baidu.com/item/%E5%9F%9F%E6%8E%A7%E5%88%B6%E5%99%A8" \t "_blank)用这个用户名在 SAM密码管理库中找到这个用户的密码散列，然后使用这个密码散列来加密 challenge。

7．[域控制器](https://baike.baidu.com/item/%E5%9F%9F%E6%8E%A7%E5%88%B6%E5%99%A8" \t "_blank)比较两次加密的 challenge ，如果一样，那么认证成功。

从上面的过程我们可以看出，NTLM是以当前用户的身份向Telnet[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)发送登录请求的，而不是用你扫到的对方管理员的帐户和密码登录，显然，你的登录将会失败。举个例子来说，你家的机器名为A（[本地机器](https://baike.baidu.com/item/%E6%9C%AC%E5%9C%B0%E6%9C%BA%E5%99%A8)），你入侵的机器名为B（远地机器），你在A上的帐户是xinxin，密码是1234，你扫到B的管理员帐号是Administrator，密码是5678，当你想Telnet到B时，NTLM将自动以当前用户的帐号和密码作为登录的凭据来进行上面的7项操作，即用xinxin和1234，而并非用你扫到的Administrator和5678，且这些都是自动完成的，根本不给你插手的机会，因此你的登录操作将失败。

## 显示

由于Telnet[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)对NTLM的使用有3个选项，所以当你Telnet远地机器时，会显示下面情况中的一种：

**1）身份验证选项=0时**

=====================================

Microsoft (R) Windows (TM) Version 5.00 (Build 2195）

Welcome to Microsoft Telnet Service

Telnet Server Build 5.00.99201.1

login:

password:

\为0时不使用NTML[身份验证](https://baike.baidu.com/item/%E8%BA%AB%E4%BB%BD%E9%AA%8C%E8%AF%81)，直接输入用户名和密码，比如你可以输入扫到的Administrator和5678

**2）身份验证选项=1时**

=====================================

NTLM Authentication failed due to insufficient credentials. Please login withclear text username and password

Microsoft (R) Windows (TM) Version 5.00 (Build 2195）

Welcome to Microsoft Telnet Service

Telnet Server Build 5.00.99201.1

login:

password:

\先尝试 NTLM 身份验证，如果失败，再使用用户名和密码，其实这种方式对于我们来说，与上一种方式没什么区别

**3）身份验证选项=2时**

=====================================

NTLM Authentication failed due to insufficient credentials. Please login withclear text username and password

Server allows NTLM authentication only

Server has closed connection

遗失对[主机](https://baike.baidu.com/item/%E4%B8%BB%E6%9C%BA" \t "_blank)的连接。

C:\>

\仔细看看上面的显示，根本没有给你输入用户名和密码的机会，直接断开连接，扫到了密码也是白扫

所以对于入侵者来说，NTLM是横在我们面前的一座大山，必须要除掉它，一般我们有如下几种方法：

1通过修改远程注册表更改telnet[服务器配置](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8%E9%85%8D%E7%BD%AE)，将验证方式从2改为1或0；

2使用NTLM.exe，上传后直接运行，可将telnet[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)验证方式从2改为1；

3在本地建立扫描到的用户，以此用户身份开启telnet客户机并进行[远程登录](https://baike.baidu.com/item/%E8%BF%9C%E7%A8%8B%E7%99%BB%E5%BD%95" \t "_blank)；

4使用[软件](https://baike.baidu.com/item/%E8%BD%AF%E4%BB%B6" \t "_blank)，比如opentelnet.exe（需要管理员权限且开启IPC管道）

5使用[脚本](https://baike.baidu.com/item/%E8%84%9A%E6%9C%AC" \t "_blank)，如[RTCS](https://baike.baidu.com/item/RTCS)，（需要管理员权限但不依赖IPC管道）

基本上是以上的5种，其中后两种是我们比较常用的开telnet的手法，而且使用方法十分简单，命令如下：

OpenTelnet.exe \server username password NTLMAuthor telnetport

OpenTelnet.exe \[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)地址 管理员用户名 密码 验证方式（填0或1） telnet端口

cscript RTCS.vbe targetIP username password NTLMAuthor telnetport

cscript RTCS.vbe <；目标IP> <；管理员用户名> <；密码> <；验证方式> <tlnet端口>

## 远程登录

**Telnet**用于Internet的远程登录.它可以使用户坐在已上网的电脑键盘前通过网络进入的另一台电脑已上网的电脑，使它们互相连通.这种连通可以发生在同一房间里面的电脑或是在世界各范围内已上网的电脑.习惯上来说，被连通计算机，并且为网络上所有用户提供服务的计算机称之为[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8" \t "_blank)（Server），而自己在使用的机器称之为客户机（Client).一旦连通后，客户机可以享有服务器所提供的一切服务.用户可以运行通常的交互过程（注册进入，执行命令），也可以进入很多的特殊的服务器如寻找图书索引.网上不同的主机提供的各种服务都可以被使用.

Telnet

（telnet) (n.) A terminal emulation program for TCP/IP networks such as the Internet. The Telnet program runs on your computer and connects your PC to a server on the network. You can then enter commands through the Telnet program and they will be executed as if you were entering them directly on the server console. This enables you to control the server and communicate with other servers on the network. To start a Telnet session,you must log in to a server by entering a valid username and password. Telnet is a common way to remotely control Web servers.

Telnet命令

使用Telnet的最简单的方法是在命令行键入：

%telnet remote-computer-name(or IP)

这里使用的是UNⅨ系统的C shell，因为命令的选择是百分号"%".如果使用的是其他的[计算机系统](https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%B3%BB%E7%BB%9F" \t "_blank)（比如：Dos,VAX/VMS,Macintosh）命令，只在细节上有些差异，而在本质上是大同小异的，下面举一个基本的Telnet使用例子：

telnet porky.math.

Trying 129.237.128.11…

Connected to porky.math

Escape character is '^]'.

SunOS UNⅨ（porky)

login:wl

password:xxxxxxx

Last Login: Tue Mar 28 05:35 from ns

SunOS Release 4.1.3\_U1(SLIPPERY1） #3: Sun Nov 20 23:47:23 CST 1999

No match.

if:Expression syntax.

porky/serv/wl%ls

hello

porky/serv/wl%

porky/serv/wl%cd/

porky/%ls

Mail/ dev/ home/ mnt/ sbin/

usr/

News/ domain/ home1/ net/ serv/

var/

Record/ etc/ kadb\* pcfs/ sys@

vmunix\*

bin@ export/ lib@ print tmp/

boot gofer/ lost+found/ record tmp\_mnt/

porky/%

上述的例子是用Telnet寻找一个叫做porky.math的远程计算机.在找到这台计算机以后，已上网的用户的计算机就成为它的一个终端.这时屏幕出现的对话与用户在host上连接的终端一样。用户必须注册进入（login）和注销推出（logout).在login后，可给出任何适合远程系统的命令，因为"面向的是UNⅨ系统，所有标准的UNⅨ命令（想ls和pwd）都可以使用.当用户从远程系统退出时，也就从Telnet退出，便可以运行自己的本地系统.实际上，Telnet是一个可以注册进入远程[计算机系统](https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%B3%BB%E7%BB%9F" \t "_blank)的工具.

## 命令

help 联机求助

open后接IP地址或[域名](https://baike.baidu.com/item/%E5%9F%9F%E5%90%8D" \t "_blank)即可进行[远程登录](https://baike.baidu.com/item/%E8%BF%9C%E7%A8%8B%E7%99%BB%E5%BD%95)

close 正常结束远程会话，回到命令方式

display 显示工作参数

mode 进入行命令或字符方式

send 向远程主机传送特殊字符（键入send?可显示详细字符）

set 设置工作参数（键入set?可显示详细参数）

status 显示状态信息

toggle 改变工作参数（键入toggle?可显示详细参数）

^]换码符（escape character）， 在异常情况下退出会话，回到命令方式

quit退出telnet，返回本地机

z使telnet进入暂停状态

<cr>；结束命令方式，返回telnet的会话方式

telnet.exe 的安全问题

建议修改权限，删除所有的用户只保存Administrators 和SYSTEM为所有权限

## 常见问题

1． Telnet是什么?答：Telnet是teletype network的缩写，现在已成为一个专有名词，表示远程登录协议和方式，分为Telnet[客户端](https://baike.baidu.com/item/%E5%AE%A2%E6%88%B7%E7%AB%AF)和Telnet[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)程序. Telnet可以让用户在本地Telnet客户端上远端登录到远程Telnet[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)上.

2． Telnet有什么作用?答： Telnet提供远程登录功能，使得用户在本地主机上运行Telnet[客户端](https://baike.baidu.com/item/%E5%AE%A2%E6%88%B7%E7%AB%AF)，就可登录到远端的Telnet[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8). 在本地输入的命令可以在服务器上运行，服务器把结果返回到本地，如同直接在服务器控制台上操作. 这样就可以在本地远程操作和控制服务器.

3． Telnet工作模式有哪些?答：Telnet共有四种工作模式：

1） 半双工：[客户端](https://baike.baidu.com/item/%E5%AE%A2%E6%88%B7%E7%AB%AF)在接收用户输入之前，必须从[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)进程获得GO AHEAD (G A）命令. 现在已很少使用.

2）一次一个字符：[客户端](https://baike.baidu.com/item/%E5%AE%A2%E6%88%B7%E7%AB%AF)把用户输入的每个字符都单独发送给[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)，服务器回显字符给客户端. 是目前大多数Telnet程序的默认方式. SUPPRESS GO AHEAD选项和ECHO选项必须同时有效.

3） 准行方式（kludge line mode): 用户每键入一行信息，[客户端](https://baike.baidu.com/item/%E5%AE%A2%E6%88%B7%E7%AB%AF)向服务器发送一次. 当上面两个选项其中之一无效时采用此模式.

4） 行方式：类似准行方式，纠正了准行方式的缺点. 较新的Telnet程序支持这种方式.

4． SUPPRESS GO AHEAD和ECHO选项作用和意义是什么

答： 如果激活"GO AHEAD"选项，则是一个半双工模式，为了工作在“一次一个字符”，需要抑制此选项，即激活"SUPPRESS GO AHEAD".ECHO选项使回显功能有效.

两者同时激活表示采用“一次一个字符” 工作方式.

5． 为何有时无法成功建立Telnet连接? 如何解决

答：如果[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)不在23号端口，而在其它端口等待用户连接，此时Telnet将失败，[客户端](https://baike.baidu.com/item/%E5%AE%A2%E6%88%B7%E7%AB%AF)需要更改连接的端口.

另外Telnet是一个明文传送协议，为了安全起见，许多防火墙将其禁用，如果需要进行远程登录，可以设置防火墙以允许Telnet.

6． Telnet是明文传送的，具有安全隐患，请问该怎么办

答： Telnet将用户的所有内容，包括用户名和密码都明文在互联网上传送，具有安全隐患，因此许多[服务器](https://baike.baidu.com/item/%E6%9C%8D%E5%8A%A1%E5%99%A8)都禁用Telnet服务. 但有时又需要远程登录到服务器上进行操作，此时可以选择具有加密功能的SSH(Secure Shell）程序.