[**telnet远程登录协议**](https://www.cnblogs.com/edda/p/12937178.html)

什么是Telnet？  
　　对于Telnet的认识，不同的人持有不同的观点，可以把Telnet当成一种通信协议，但是对于入侵者而言，Telnet只是一种远程登录的工具。一旦入侵者与远程主机建立了Telnet连接，入侵者便可以使用目标主机上的软、硬件资源，而入侵者的本地机只相当于一个只有键盘和显示器的终端而已。

　　为什么需要telnet？  
　　telnet就是查看某个端口是否可访问。我们在搞开发的时候，经常要用的端口就是 8080。那么你可以启动服务器，用telnet 去查看这个端口是否可用。

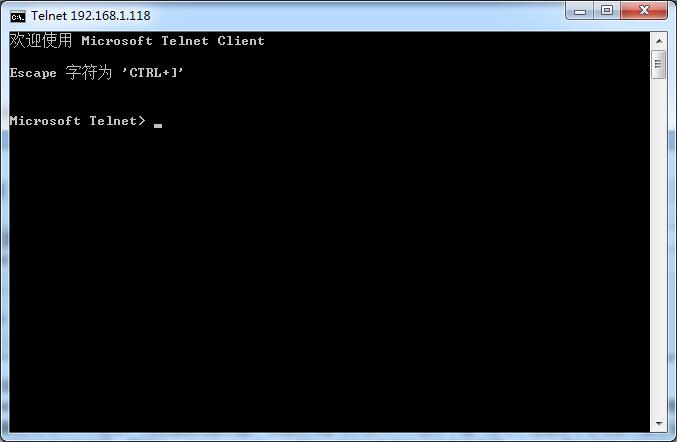
telnet用法测试端口号：<https://jingyan.baidu.com/article/a3aad71aa9e6efb1fb009694.html>  
　　Telnet协议是TCP/IP协议家族中的一员，是Internet远程登陆服务的标准协议和主要方式。它为用户提供了在本地计算机上完成远程主机工作的能力。在终端使用者的电脑上使用telnet程序，用它连接到服务器。终端使用者可以在telnet程序中输入命令，这些命令会在服务器上运行，就像直接在服务器的控制台上输入一样。可以在本地就能控制服务器。要开始一个telnet会话，必须输入用户名和密码来登录服务器。Telnet是常用的远程控制Web服务器的方法。

Windows XP怎么执行telnet 命令？

　　1、点击开始　→　运行　→　输入CMD，回车。  
　　2、在出来的DOS界面里，输入telnet[测试](http://lib.csdn.net/base/softwaretest)端口命令： telnet IP 端口 或者 telnet 域名 端口，回车。  
　　如果端口关闭或者无法连接，则显示不能打开到主机的链接，链接失败；端口打开的情况下，链接成功，则进入telnet页面（全黑的），证明端口可用。



"ctrl+]"　组合键退到telnet命令输入界面



再按下回车键就进入了远程界面



Telnet 客户端命常用命令：

　　open : 使用 openhostname 可以建立到主机的 Telnet 连接。

　　close : 使用命令 close 命令可以关闭现有的 Telnet 连接。

　　display : 使用 display 命令可以查看 Telnet 客户端的当前设置。

　　send : 使用 send 命令可以向 Telnet 服务器发送命令。支持以下命令：

　　ao : 放弃输出命令。

　　ayt : “Are you there”命令。

　　esc : 发送当前的转义字符。

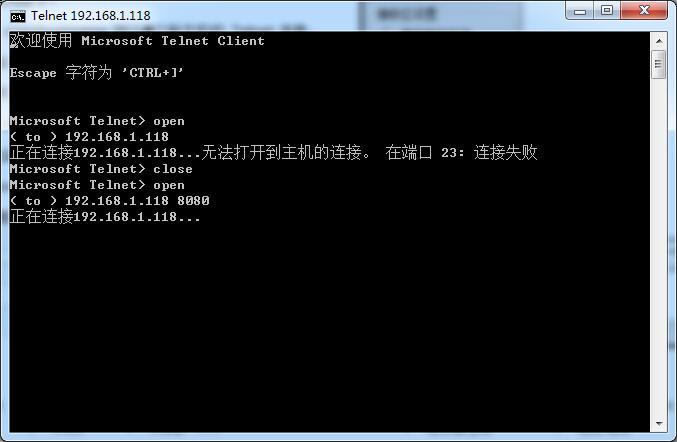
　　ip : 中断进程命令。

　　synch : 执行 Telnet 同步操作。

　　brk : 发送信号。

　　上表所列命令以外的其他命令都将以字符串的形式发送至 Telnet 服务器。例如，sendabcd 将发送字符串 abcd 至 Telnet 服务器，这样，Telnet 会话窗口中将出现该字符串。

　　quit ：使用 quit 命令可以退出 Telnet 客户端。



Telnet协议是TCP/IP协议族中的一员，是Internet远程登陆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工作的能力。在终端使用者的电脑上使用telnet程序，用它连接到服务器。终端使用者可以在telnet程序中输入命令，这些命令会在服务器上运行，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。要开始一个telnet会话，必须输入用户名和密码来登录服务器。Telnet是常用的远程控制Web服务器的方法

　　它最初是由ARPANET开发的，但是现在它主要用于Internet会话。它的基本功能是，允许用户登录进入远程主机系统。起初，它只是让用户的本地计算机与远程计算机连接，从而成为远程主机的一个终端。它的一些较新的版本在本地执行更多的处理，于是可以提供更好的响应，并且减少了通过链路发送到远程主机的信息数量。

**（一）远程登录**

　　Telnet服务虽然也属于客户机/服务器模型的服务，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。   
　　 1 远程登陆的基本概念    
　　先来看看什么叫登录：分时系统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'。   
　　远程登陆是指用户使用Telnet命令，使自己的计算机暂时成为远程主机的一个仿真终端的过程。仿真终端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，再将主机输出的每个信息回显在屏幕上。   
　　 2 远程登陆的产生及发展    
　　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/服务器模型的服务。   
　　似乎有了客户机/服务器模型的服务，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，想实现一切可以在远程主机上实现的操作，那么我们将需要大量专用的服务器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程序。   
　　问题发展到这里好像前途一片光明了，用远程登录总应该解决问题了吧，但要实现远程登陆并不简单。不考虑网络设计的计算机系统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陆功能需要修改机器的操作系统，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陆服务器软件，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陆服务器软件，'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，系统编程人员还是设法构造了能够应用于大多数操作系统的远程登陆服务器软件，并构造了充当客户机的应用软件。通常，客户机软件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。   
　　将远程登陆服务器设计为应用级软件，还有另一个要求，那就是需要操作系统提供对伪终端（pseudo terminal）的支持。我们用伪终端描述操作系统的入口点，它允许像Telnet服务器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，才能将远程登陆服务器设计为应用级软件（比如Telnet服务器软件），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），远程登陆将宣告失败。   
　　将远程登陆服务器设计为应用级软件虽然有其显著的优点：比将代码嵌入操作系统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。   
　　 3 远程登录的工作过程    
　　使用Telnet协议进行远程登陆时需要满足以下条件：在本的计算机上必须装有包含Telnet协议的客户程序；必须知道远程主机的Ip地址或域名；必须知道登录标识与口令。   
　　Telnet远程登录服务分为以下4个过程：   
　　1）本地与远程主机建立连接。该过程实际上是建立一个TCP连接，用户必须知道远程主机的Ip地址或域名；   
　　2）将本地终端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（Net Virtual Terminal）格式传送到远程主机。该过程实际上是从本地主机向远程主机发送一个IP数据包；   
　　3）将远程主机输出的NVT格式的数据转化为本地所接受的格式送回本地终端，包括输入命令回显和命令执行结果；   
　　4）最后，本地终端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！

**（二）Telnet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？   
　　 1 基本内容    
　　Telnet协议是TCP/IP协议族中的一员，是Internet远程登陆服务的标准协议。应用Telnet协议能够把本地用户所使用的计算机变成远程主机系统的一个终端。它提供了三种基本服务：   
　　1）Telnet定义一个网络虚拟终端为远的系统提供一个标准接口。客户机程序不必详细了解远的系统，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上显示输出。   
　　 2 适应异构    
　　为了使多个操作系统间的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，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或命令，传送到远地并被远地系统解释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NVT（Net Virtual Terminal）。它的应用过程如下：   
　　对于发送的数据：客户机软件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，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，而本地客户机将将接收到的NVT格式数据再转换为本地的格式。   
　　对于NVT格式的详细定义，有兴趣的朋友可以去查找相关资料。   
　　 3 传送远地命令    
　　我们知道绝大多数操作系统都提供各种快捷键来实现相应的控制命令，当用户在本地终端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地传送呢？   
　　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。我们知道USASCII字符集包括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（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字符集与控制命令区分主要有两个原因：   
　　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。   
　　 4 数据流向    
　　上面我们提到过将Telnet设计为应用级软件有一个缺点，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地机器，远地操作系统将所接收数据传给服务器程序，并经服务器程序再次处理后返回到操作系统上的伪终端入口点，最后，远地操作系统将数据传送到用户正在运行的应用程序，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。   
　　 5 强制命令    
　　我们应该考虑到这样一种情况：假设本地用户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，那么操作系统的缓冲区可能因此而被占满，如果这样，远地服务器也无法再将数据写入伪终端，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