

计算机网络的主要优点是能够实现资源和信息的共享，并且用户可以远程访问信息。Linux 提供了一组强有力的网络命令来为用户服务，这些工具能够帮助用户登录到远程计算机上、传输文件和执行远程命令等。介绍下列几个常用的有关网络操作的命令：

ftp 传输文件

telnet 登录到远程计算机上

r - 使用各种远程命令

netstat 查看网络的状况

nslookup 查询域名和 IP 地址的对应

finger 查询某个使用者的信息

ping 查询某个机器是否在工作

使用 **ftp** 命令进行远程文件传输

ftp 命令是标准的文件传输协议的用户接口。**ftp** 是在 TCP/IP 网络上的计算机之间传输文件的简单有效的方法。它允许用户传输 ASCII 文件和二进制文件。在 **ftp** 会话过程中，用户可以通过使用 **ftp** 客户程序连接到另一台计算机上。从此，用户可以在目录中上下移动、列出目录内容、把文件从远程机拷贝到本地机上、把文件从本地机传输到远程系统中。

需要注意的是，如果用户没有那个文件的存取权限，就不能从远程系统中获得文件或向远程系统传输文件。为了使用 **ftp** 来传输文件，用户必须知道远程计算机上的合法用户名和口令。这个用户名/口令的组合用来确认 **ftp** 会话，并用来确定用户对要传输的文件可以进行什么样的访问。另外，用户显然需要知道对其进行 **ftp** 会话的计算机的名字或 IP 地址。

Ftp 命令的功能是在本地机和远程机之间传送文件。该命令的一般格式如下：

\$ ftp 主机名/IP

其中“主机名/IP”是所要连接的远程机的主机名或 IP 地址。在命令行中，主机名属于选项。如果指定主机名，**ftp** 将试图与远程机的 **ftp** 服务程序进行连接；如果没有指定主机名，**ftp** 将给出提示符，等待用户输入命令：**\$ ftp ftp >** 此时在 **ftp>**提示符后面输入 **open** 命令及主机名或 IP 地址，将试图连接指定的主机。不管使用哪一种方法，如果连接成功，需要在远程机上登录。用户如果在远程机上有帐号，就可以通过 **ftp** 使用这一帐号并需要提供口令。

在远程机上的用户帐号的读写权限决定该用户在远程机上能下载什么文件和将上载

文件放到哪个目录中。如果没有远程机的专用登录帐号，许多 ftp 站点设有可以使用的特殊帐号。这个帐号的登录名为 **anonymous**（也称为匿名 ftp），当使用这一帐号时，要求输入 **email** 地址作为口令。如果远程系统提供匿名 ftp 服务，用户使用这项服务可以登录到特殊的，供公开使用的目录。

一般专门提供两个目录：**pub** 目录和 **incoming** 目录。**pub** 目录包含该站点供公众使用的文件，**incoming** 目录存放上载到该站点的文件。一旦用户使用 ftp 在远程站点上登录成功，将得到“ftp>”提示符。现在可以自由使用 ftp 提供的命令，可以用 **help** 命令取得可供使用的命令清单，也可以在 **help** 命令后面指定具体的命令名称，获得这条命令的说明。

最常用的命令有：

ls 列出远程机的当前目录

cd 在远程机上改变工作目录

lcd 在本地机上改变工作目录

ascii 设置文件传输方式为 ASCII 模式

binary 设置文件传输方式为二进制模式

close 终止当前的 ftp 会话

hash 每次传输完数据缓冲区中的数据后就显示一个#号

get (mget) 从远程机传送指定文件到本地机

put (mput) 从本地机传送指定文件到远程机

open 连接远程 ftp 站点

quit 断开与远程机的连接并退出 ftp

? 显示本地帮助信息

! 转到 Shell 中

下面简单将 ftp 常用命令作一简介。

启动 ftp 会话 **open** 命令用于打开一个与远程主机的会话。该命令的一般格式是：

open 主机名/IP 如果在 ftp 会话期间要与一个以上的站点连接，通常只用不带参数

的 **ftp** 命令。如果在会话期间只想与一台计算机连接，那么在命令行上指定远程主机名或 IP 地址作为 **ftp** 命令的参数。

终止 **ftp** 会话 **close**、**disconnect**、**quit** 和 **bye** 命令用于终止与远程机的会话。**close** 和 **disconnect** 命令关闭与远程机的连接，但是使用户留在本地计算机的 **ftp** 程序中。**quit** 和 **bye** 命令都关闭用户与远程机的连接，然后退出用户机上的 **ftp** 程序。

改变目录 “**cd** [目录]”命令用于在 **ftp** 会话期间改变远程机上的目录，**lcd** 命令改变本地目录，使用户能指定查找或放置本地文件的位置。远程目录列表 **ls** 命令列出远程目录的内容，就像使用一个交互 **shell** 中的 **ls** 命令一样。

ls 命令的一般格式是：**ls** [目录] [本地文件] 如果指定了目录作为参数，那么 **ls** 就列出该目录的内容。如果给出一个本地文件的名称，那么这个目录列表被放入本地机上您指定的这个文件中。

从远程系统获取文件 **get** 和 **mget** 命令用于从远程机上获取文件。**get** 命令的一般格式为：

get 文件名 您还可以给出本地文件名，这个文件名是这个要获取的文件在您的本地机上创建时的文件名。如果您不给出一个本地文件名，那么就使用远程文件原来的名字。**mget** 命令一次获取多个远程文件。

mget 命令的一般格式为：**mget** 文件名列表 使用用空格分隔的或带通配符的文件名列表来指定要获取的文件，对其中的每个文件都要求用户确认是否传送。

向远程系统发送文件 **put** 和 **mput** 命令用于向远程机发送文件。

Put 命令的一般格式为：**put** 文件名 **mput** 命令一次发送多个本地文件，

mput 命令的一般格式为：**mput** 文件名列表 使用用空格分隔的或带通配符的文件名列表来指定要发送的文件。对其中的每个文件都要求用户确认是否发送。

改变文件传输模式：默认情况下，**ftp** 按 **ASCII** 模式传输文件，用户也可以指定其他模式。

ascii 和 **binary** 命令的功能是设置传输的模式。用 **ASCII** 模式传输文件对纯文本是非常好的，但为避免对二进制文件的破坏，用户可以以二进制模式传输文件。

检查传输状态：传输大型文件时，可能会发现让 **ftp** 提供关于传输情况的反馈信息是非常有用的。**hash** 命令使 **ftp** 在每次传输完数据缓冲区中的数据后，就在屏幕上打印一个 **#** 字符。本命令在发送和接收文件时都可以使用。

ftp 中的本地命令 当您使用 **ftp** 时，字符“!”用于向本地机上的命令 **shell** 传送一个命令。如果用户处在 **ftp** 会话中，需要 **shell** 做某些事，就很有用。例如用户要建立一个目录来保存接收到的文件。如果输入 **!mkdir new_dir**，那么 **Linux** 就在用户当前的本地目录中创建一个名为 **new_dir** 的目录。

从远程机 `grunthos` 下载二进制数据文件的典型对话过程如下：

```
$ ftp grunthos Connected to grunthos 220 grunthos ftp server Name
(grunthos:pc) : anonymous 33l Guest login ok, send your complete e-mail
address as password. Password: 230 Guest 1ogin ok, access restrictions apply.
Remote system type is UNIX. ftp > cd pub 250 CWD command successful. ftp > ls
200 PORT command successful. 150 opening ASCII mode data connection for
/bin/1s. total 114 rog1 rog2 226 Transfer complete . ftp > binary 200 type set to I.
ftp > hash Hash mark printing on (1024 bytes/hash mark) . ftp > get rog1 200
PORT command successfu1. 150 opening BINARY mode data connection for rog1
(14684 bytes) . ##### 226 Transfer complete. 14684 bytes
received in 0.0473 secs (3e + 02 Kbytes/sec) ftp > quit 22l Goodbye.
```

使用 `telnet` 命令访问远程计算机

用户使用 `telnet` 命令进行远程登录。该命令允许用户使用 `telnet` 协议在远程计算机之间进行通信，用户可以通过网络在远程计算机上登录，就像登录到本地机上执行命令一样。为了通过 `telnet` 登录到远程计算机上，必须知道远程机上的合法用户名和口令。虽然有些系统确实为远程用户提供登录功能，但出于对安全的考虑，要限制来宾的操作权限，因此，这种情况下能使用的功能是很少的。当允许远程用户登录时，系统通常把这些用户放在一个受限制的 `shell` 中，以防系统被怀有恶意的或不小心的用户破坏。用户还可以使用 `telnet` 从远程站点登录到自己的计算机上，检查电子邮件、编辑文件和运行程序，就像在本地登录一样。

但是，用户只能使用基于终端的环境而不是 `X Windows` 环境，`telnet` 只为普通终端提供终端仿真，而不支持 `X Window` 等图形环境。

`telnet` 命令的一般形式为：`telnet 主机名/IP` 其中“主机名/IP”是要连接的远程机的主机名或 IP 地址。如果这一命令执行成功，将从远程机上得到 `login:` 提示符。

使用 `telnet` 命令登录的过程如下：`$ telnet 主机名/IP` 启动 `telnet` 会话。一旦 `telnet` 成功地连接到远程系统上，就显示登录信息并提示用户输入用户名和口令。如果用户名和口令输入正确，就能成功登录并在远程系统上工作。在 `telnet` 提示符后面可以输入很多命令，用来控制 `telnet` 会话过程，在 `telnet` 联机帮助手册中对这些命令有详细的说明。

下面是一台 `Linux` 计算机上的 `telnet` 会话举例：

```
$ telnet server. somewhere. com Trying 127.0.0.1... Connected to serve.
somewhere. com. Escape character is '\?]\'. "TurboLinux release 4. 0 (Colgate)
kernel 2.0.18 on an I486
login: bubba password: Last login:Mon Nov 15 20:50:43 for localhost Linux 2.
0.6. (Posix) . server: ~$ server: ~$ logout Connection closed by foreign host $
```

用户结束了远程会话后，一定要确保使用 `logout` 命令退出远程系统。然后 `telnet` 报告远程会话被关闭，并返回到用户的本地机的 `Shell` 提示符下。

r-系列命令 除 `ftp` 和 `telnet` 以外，还可以使用 **r-系列命令** 访问远程计算机和在网络上交换文件。使用 **r-系列命令** 需要特别注意，因为如果用户不小心，就会造成严重的安全漏洞。用户发出一个 **r-系列命令** 后，远程系统检查名为 `/etc/hosts.equiv` 的文件，以查看用户的主机是否列在这个文件中。如果它没有找到用户的主机，就检查远程机上同名用户的主目录中名为 `.rhosts` 的文件，看是否包括该用户的主机。如果该用户的主机包括在这两个文件中的任何一个之中，该用户执行 **r-系列命令** 就不用提供口令。

虽然用户每次访问远程机时不用键入口令可能是非常方便的，但是它也可能会带来严重的安全问题。我们建议用户在建立 `/etc/hosts.equiv` 和 `.rhosts` 文件之前，仔细考虑 **r-命令** 隐含的安全问题。

rlogin 命令

`rlogin` 是“remote login”（远程登录）的缩写。该命令与 `telnet` 命令很相似，允许用户启动远程系统上的交互命令会话。`rlogin` 的一般格式是：

```
rlogin [ -8EKLdx ] [ -e char ] [-k realm ] [ -l username ] host
```

一般最常用的格式是：`rlogin host` 该命令中各选项的含义为：

-8 此选项始终允许 8 位输入数据通道。该选项允许发送格式化的 ANSI 字符和其他的特殊代码。如果不用这个选项，除非远端的终止和启动字符不是或，否则就去掉奇偶校验位。

-E 停止把任何字符当作转义字符。当和 **-8** 选项一起使用时，它提供一个完全的透明连接。

-K 关闭所有的 Kerberos 确认。只有与使用 Kerberos 确认协议的主机连接时才使用这个选项。

-L 允许 `rlogin` 会话在 `litout` 模式中运行。要了解更多信息，请查阅 `tty` 联机帮助。

-d 打开与远程主机进行通信的 TCP sockets 的 socket 调试。要了解更多信息，请查阅 `setsockopt` 的联机帮助。

-e 为 `rlogin` 会话设置转义字符，默认的转义字符是“~”，用户可以指定一个文字字符或一个 `\nnn` 形式的八进制数。

-k 请求 `rlogin` 获得在指定区域内的远程主机的 Kerberos 许可，而不是获得由 `krb_realmofhost` (3) 确定的远程主机区域内的远程主机的 Kerberos 许可。

-x 为所有通过 **rlogin** 会话传送的数据打开 **DES** 加密。这会影晌响应时间和 **CPU** 利用率，但是可以提高安全性。

rsh 命令

rsh 是“remote shell”（远程 shell）的缩写。该命令在指定的远程主机上启动一个 shell 并执行用户在 **rsh** 命令行中指定的命令。如果用户没有给出要执行的命令，**rsh** 就用 **rlogin** 命令使用户登录到远程机上。

rsh 命令的一般格式是：

```
rsh [-Kdnx] [-k realm] [-l username] host [command]
```

一般常用的格式是：

```
rsh host [command]
```

command 可以是来自 shell 提示符下键入的任何 **Linux** 命令。

rsh 命令中各选项的含义如下：

-K 关闭所有的 **Kerbero** 确认。该选项只在与使用 **Kerbero** 确认的主机连接时才使用。

-d 打开与远程主机进行通信的 **TCP sockets** 的 **socket** 调试。要了解更多的信息，请查阅 **setsockopt** 的联机帮助。

-k 请求 **rsh** 获得在指定区域内的远程主机的 **Kerberos** 许可，而不是获得由 **krb_relmofhost** (3) 确定的远程主机区域内的远程主机的 **Kerberos** 许可。

-l 缺省情况下，远程用户名与本地用户名相同。本选项允许指定远程用户名，如果指定了远程用户名，则使用 **Kerberos** 确认，与在 **rlogin** 命令中一样。

-n 重定向来自特殊设备 **/dev/null** 的输入。

-x 为传送的所有数据打开 **DES** 加密。这会影晌响应时间和 **CPU** 利用率，但是可以提高安全性。

Linux 把标准输入放入 **rsh** 命令中，并把它拷贝到要远程执行的命令的标准输入中。它把远程命令的标准输出拷贝到 **rsh** 的标准输出中。它还把远程标准错误拷贝到本地标准错误文件中。任何退出、中止和中断信号都被送到远程命令中。当远程命令终止了，**rsh** 也就终止了。

rcp 命令

rcp 代表“remote file copy”（远程文件拷贝）。该命令用于在计算机之间拷贝文件。

rcp 命令有两种格式。第一种格式用于文件到文件的拷贝；第二种格式用于把文件或目录拷贝到另一个目录中。

rcp 命令的一般格式是：

```
rcp [-px] [-k realm] file1 file2 rcp [-px] [-r] [-k realm] file
```

directory 每个文件或目录参数既可以是远程文件名也可以是本地文件名。远程文件名具有如下形式：**rname@rhost: path**，其中 **rname** 是远程用户名，**rhost** 是远程计算机名，**path** 是这个文件的路径。

rcp 命令的各选项含义如下：

-r 递归地把源目录中的所有内容拷贝到目的目录中。要使用这个选项，目的必须是一个目录。

-p 试图保留源文件的修改时间和模式，忽略 **umask**。

-k 请求 rcp 获得在指定区域内的远程主机的 **Kerberos** 许可，而不是获得由 **krb_relmofhost (3)** 确定的远程主机区域内的远程主机的 **Kerberos** 许可。

-x 为传送的所有数据打开 **DES** 加密。这会影晌响应时间和 **CPU** 利用率，但是可以提高安全性。如果在文件名中指定的路径不是完整的路径名，那么这个路径被解释为相对远程机上同名用户的主目录。如果没有给出远程用户名，就使用当前用户名。如果远程机上的路径包含特殊 **shell** 字符，需要用反斜线（****）、双引号（**"**）或单引号（**'**）括起来，使所有的 **shell** 元字符都能被远程地解释。需要说明的是，**rcp** 不提示输入口令，它通过 **rsh** 命令来执行拷贝。