DOS命令全套汇编（完整版） - 百度文库

请稍等...

百度文库

搜索文档或关键词

普通分享 >

DOS命令全套汇编(完整版)

VIP专享文档

2020-05-29

4页

用App查看

正文：

DOS命令大全  
一）MD——建立子目录 　  
1．功能：创建新的子目录　  
2．类型：内部命令　  
3．格式：MD[盘符：][路径名]〈子目录名〉　  
4．使用说明：　  
（1）“盘符”：指定要建立子目录的磁盘驱动器字母，若省略，则为当前驱动器；　  
（2）“路径名”：要建立的子目录的上级目录名，若缺省则建在当前目录下。　  
例：（1）在C盘的根目录下创建名为FOX的子目录；（2）在FOX子目录下再创建USER子目录。　  
C：、＞MD FOX （在当前驱动器C盘下创建子目录FOX）　  
C：、＞MD FOX \ USER （在FOX 子目录下再创建USER子目录）　  
（二）CD——改变当前目录　  
1．功能：显示当前目录　  
2．类型：内部命令　  
3．格式：CD[盘符：][路径名][子目录名]　  
4．使用说明：　  
（1）如果省略路径和子目录名则显示当前目录；　  
（2）如采用“CD \ ”格式，则退回到根目录；　  
（3）如采用“CD .. ”格式则退回到上一级目录。　  
例：（1）进入到USER子目录；（2）从USER子目录退回到子目录；（3）返回到根目录。　  
C:、＞CD FOX \ USER（进入FOX子目录下的USER子目录）　  
C:、FOX、USER＞CD . . （退回上一级根目录）　  
C：、FOX＞CD \ （返回到根目录）　  
C：、＞　  
（三）RD——删除子目录命令　  
1．功能：从指定的磁盘删除了目录。　  
2．类型：内部命令　  
3．格式：RD[盘符：][路径名][子目录名]　  
4．使用说明：　  
（1）子目录在删除前必须是空的，也就是说需要先进入该子目录，使用DEL（删除文件的命令）将其子目录下的文件删空，然后再退回到上一级目录，用RD命令删除该了目录本身；　  
（2）不能删除根目录和当前目录。　  
例：要求把C盘FOX子目录下的USER子目录删除，操作如下：　  
第一步：先将USER子目录下的文件删空；　  
C、＞DEL C： \ FOX \ USER \ \* . \*　  
第二步，删除USER子目录。　  
C、＞RD Ｃ： \ FOX \ USER　  
（四）DIR——显示磁盘目录命令　  
1．功能：显示磁盘目录的内容。　  
2．类型：内部命令　  
3．格式：DIR [盘符][路径][/P][/W]　  
4．  
使用说明：/P的使用；当欲查看的目录太多，无法在一屏显示完屏幕会一直往上卷，不容易看清，加上/P参数后，屏幕上会分面一次显示23行的文件信息，然后暂停，并提示；Press  
any key to continue　  
/W的使用：加上/W只显示文件名，至于文件大小及建立的日期和时间则都省略。加上参数后，每行可以显示五个文件名。　  
PATH——路径设置命令　  
1．功能：设备可执行文件的搜索路径，只对文件有效。　  
2．类型：内部命令　  
3．格式：PATH[盘符1]目录[路径名1]{[；盘符2：]，〈目录路径名2〉…}　  
4．使用说明：　  
（1）当运行一个可执行文件时，DOS会先在当前目录中搜索该文件，若找到则运行之；若找不到该文件，则根据PATH命令所设置的路径，顺序逐条地到目录中搜索该文件；　  
（2）PATH命令中的路径，若有两条以上，各路径之间以一个分号“；”隔开；　  
（3）PATH命令有三种使用方法：　  
PATH[盘符1：][路径1][盘符2：][路径2]…（设定可执行文件的搜索路径）　 PATH：（取消所有路径）　PATH：（显示目前所设的路径）　  
（六）TREE——显示磁盘目录结构命令　  
1．功能：显示指定驱动器上所有目录路径和这些目录下的所有文件名。　  
2．类型：外部命令　  
3．格式：TREE[盘符：][/F][》PRN]　  
4．使用说明：　  
（1）使用/F参数时显示所有目录及目录下的所有文件，省略时，只显示目录，不显示目录下的文件；　  
（2）选用＞PRN参数时，则把所列目录及目录中的文件名打印输出。　  
（七）DELTREE——删除整个目录命令　  
1．功能：将整个目录及其下属子目录和文件删除。　  
2．类型：外部命令　  
3．格式：DELTREE[盘符：]〈路径名〉　  
4．使用说明：该命令可以一步就将目录及其下的所有文件、子目录、更下层的子目录一并删除，而且不管文件的属性为隐藏、系统或只读，只要该文件位于删除的目录之下，DELTREE都一视同仁，照删不误。使用时务必小心！！！　  
五、磁盘操作类命令　  
（一）formAT——磁盘格式化命令　  
1．功能：对磁盘进行格式化，划分磁道和扇区；同时检查出整个磁盘上有无带缺陷的磁道，对坏道加注标记；建立目录区和文件分配表，使磁盘作好接收DOS的准备。　  
2．类型：外部命令　  
3．格式：formAT〈盘符：〉[/S][/4][/Q]　  
4．使用说明：　  
（1）命令后的盘符不可缺省，若对硬盘进行格式化，则会如下列提示：WARNING:ALL DATA ON NON  
——REMOVABLE DISK　  
DRIVE C:WILL BE LOST ！　  
Proceed with format (Y/N)？　  
（警告：所有数据在C盘上，将会丢失，确实要继续格式化吗？）　  
（2）若是对软盘进行格式化，则会如下提示：Insert mew diskette for drive A;　  
and press ENTER when ready…　  
（在A驱中插入新盘，准备好后按回车键）。　  
（3）选用[/S]参数，将把DOS系统文件IO.SYS  
、MSDOS.SYS及COMMAND.COM复制到磁盘上，使该磁盘可以做为DOS启动盘。若不选用/S参数，则格式化后的磙盘只能读写信息，而不能做为启动盘；　  
（4）选用[/4]参数，在1.2MB的高密度软驱中格式化360KB的低密度盘；　  
（5）选用[/Q]参数，快速格式化，这个参数并不会重新划分磁盘的磁道貌岸然和扇区，只能将磁盘根目录、文件分配表以及引导扇区清成空白，因此，格式化的速度较快。　  
（6）选用[/U]参数，表示无条件格式化，即破坏原来磁盘上所有数据。不加/U，则为安全格式化，这时先建立一个镜象文件保存原来的FAT表和根目录，必要时可用UNFORRMAT恢复原来的数据。　  
（二）UNformAT恢复格式化命令　  
1．功能：对进行过格式化误操作丢失数据的磁盘进行恢复。　  
2．类型：外部命令　  
3．格式：UNformAT〈盘符〉[/L][/U][/P][/TEST]　  
4．使用说明：用于将被“非破坏性”格式化的磁盘恢复。根目录下被删除的文件或子目录及磁盘的系统扇区（包括FAT、根目录、BOOT扇区及硬盘分区表）受损时，也可以用UNformAT来抢救。　  
（1）选用/L参数列出找到的子目录名称、文件名称、大孝日期等信息，但不会真的做formAT工作。　  
（2）选用/P参数将显示于屏幕的报告（包含/L参数所产生的信息）同时也送到打印机。运行时屏幕会显示：“Print out will  
be sent to LPT1”　  
（3）选用/TEST参数只做模拟试验（TEST）不做真正的写入动作。使用此参数屏幕会显示：“Simulation only”　  
（4）选用/U参数不使用MIRROR映像文件的数据，直接根据磁盘现状进行UNformAT。　  
（5）选用/PSRTN；修复硬盘分区表。　  
若在盘符之后加上/P、/L、/TEST之一，都相当于使用了/U参数，UNformAT会“假设”此时磁盘没有MIRROR映像文件。　  
注意：UNformAT对于刚formAT的磁盘，可以完全恢复，但formAT后若做了其它数据的写入，则UNformAT就不能完整的救回数据了。UNformAT并非是万能的，由于使用UNformAT会重建FAT与根目录，所以它也具有较高的危险性，操作不当可能会扩大损失，如果仅误删了几个文件或子目录，只需要利用UNDELETE就够了。  
三） CHKDSK——检查磁盘当前状态命令　  
1．功能：显示磁盘状态、内存状态和指定路径下指定文件的不连续数目。　  
2．类型：外部命令　  
3．格式：CHKDSK [盘符：][路径][文件名][/F][/V]　  
4．使用说明：　  
（1）选用[文件名]参数，则显示该文件占用磁盘的情况；　  
（2）选[/F]参数，纠正在指定磁盘上发现的逻辑错误；　  
（3）选用[/V]参数，显示盘上的所有文件和路径。　  
（四）DISKCOPY——整盘复制命令　  
1．功能：复制格式和内容完全相同的软盘。　  
2．类型：外部命令　  
3．格式：DISKCOPY[盘符1：][盘符2：]　  
4．使用说明：　  
（1）如果目标软盘没有格式化，则复制时系统自动选进行格式化。　  
（2）如果目标软盘上原有文件，则复制后将全部丢失。　  
（3）如果是单驱动器复制，系统会提示适时更换源盘和目标盘，请操作时注意分清源盘和目标盘。　  
（五）LABEL——建立磁盘卷标命令　  
1．功能：建立、更改、删除磁盘卷标。　  
2．类型：外部命令　  
3．格式：LABEL[盘符：][卷标名]　  
4．使用说明：　  
（1）卷标名为要建立的卷标名，若缺省此参数，则系统提示键入卷标名或询问是否删除原有的卷标名；　  
（2）卷标名由1至11个字符组成。　  
（六）VOL——显示磁盘卷标命令　  
1．功能：查看磁盘卷标号。　  
2．类型：内部命令　  
3．格式：VOL[盘符：]　  
4．使用说明：省略盘符，显示当前驱动器卷标。　  
（七）SCANDISK——检测、修复磁盘命令　  
1．功能：检测磁盘的FAT表、目录结构、文件系统等是否有问题，并可将检测出的问题加以修复。　  
2．类型：外部命令　  
3．格式：SCANDISK[盘符1：]{[盘符2：]…}[/ALL]　  
4．使用说明：　  
（1）CCANDISK适用于硬盘和软盘，可以一次指定多个磁盘或选用[/ALL]参数指定所有的磁盘；　  
（2）可自动检测出磁盘中所发生的交叉连接、丢失簇和目录结构等逻辑上的错误，并加以修复。　  
（八）DEFRAG——重整磁盘命令　  
1．。功能：整理磁盘，消除磁盘碎块。　  
2．类型：外部命令　  
3．格式：DEFRAG[盘符：][/F]　  
4．使用说明：选用/F参数，将文件中存在盘上的碎片消除，并调整磁盘文件的安排，确保文件之间毫无空隙。从而加快读盘速度和节省磁盘空间。　  
（九）SYS——系统复制命令　  
1．功能：将当前驱动器上的DOS系统文件IO.SYS,MSDOS.SYS和COMMAND.COM 传送到指定的驱动器上。　  
2．类型：外部命令　  
3．格式：SYS[盘符：]　  
\*使用说明：如果磁盘剩余空间不足以存放系统文件，则提示：No roomfor on destination disk.　  
文件操作类命令　  
（一） COPY文件复制命令　  
1．功能：拷贝一个或多个文件到指定盘上。　  
2．类型：内部命令　  
3．格式：COPY [源盘][路径]〈源文件名〉[目标盘][路径][目标文件名]　  
4．使用说明：　  
（1）COPY是文件对文件的方式复制数据，复制前目标盘必须已经格式化；　  
（2）复制过程中，目标盘上相同文件名称的旧文件会被源文件取代；　  
（3）复制文件时，必须先确定目标般有足够的空间，否则会出现；insufficient的错误信息，提示磁盘空间不够；　  
（4）文件名中允许使用通配举“\*”“？”，可同时复制多个文件；　  
（5）COPY命令中源文件名必须指出，不可以省略。　  
（6）复制时，目标文件名可以与源文件名相同，称作“同名拷贝”此时目标文件名可以省略；　  
（7）复制时，目标文件名也可以与源文件名不相同，称作“异名拷贝”，此时，目标文件名不能省略；　  
（8）复制时，还可以将几个文件合并为一个文件，称为“合并拷贝”，格式如下：COPY；[源盘][路径]〈源文件名1〉〈源文件名2〉…[目标盘][路径]〈目标文件名〉；　  
（9）利用COPY命令，还可以从键盘上输入数据建立文件，格式如下：COPY CON [盘符：][路径]〈文件名〉；　  
（10）注意：COPY命令的使用格式，源文件名与目标文件名之间必须有空格！　  
（二）XCOPY——目录复制命令　  
1．功能：复制指定的目录和目录下的所有文件连同目录结构。　  
2．类型：外部命令　  
3．格式：XCOPY [源盘：]〈源路径名〉[目标盘符：][目标路径名][/S][/V][/E]　  
4．使用说明：　  
（1）XCOPY是COPY的扩展，可以把指定的目录连文件和目录结构一并拷贝，但不能拷贝隐藏文件和系统文件；　  
（2）使用时源盘符、源目标路径名、源文件名至少指定一个；　  
（3）选用/S时对源目录下及其子目录下的所有文件进行COPY。除非指定/E参数，否则/S不会拷贝空目录，若不指定/S参数，则XCOPY只拷贝源目录本身的文件，而不涉及其下的子目录；　  
（4）选用/V参数时，对的拷贝的扇区都进行较验，但速度会降低。　  
（三）TYPE——显示文件内容命令　  
1．功能：显示ASCII码文件的内容。　  
2．类型：内部命令。　  
3．格式：TYPE[盘符：][路径]〈文件名〉　  
4．使用说明：　  
（1）显示由ASCII码组成的文本文件，对。EXE.COM等为扩展名的文件，其显示的内容是无法阅读的，没有实际意义2；　  
（2）该命令一次只可以显示一个文件的内容，不能使用通配符；　  
（3）如果文件有扩展名，则必须将扩展名写上；　  
（4）当文件较长，一屏显示不下时，可以按以下格式显示；TYPE[盘符：][路径]〈文件名〉|MORE，MORE为分屏显示命令，使用些参数后当满屏时会暂停，按任意键会继续显示。　  
（5）若需将文件内容打印出来，可用如下格式：　  
TYPE[盘符：][路径]〈文件名〉，＞PRN　  
此时，打印机应处于联机状态。　  
（四） REN——文件改名命令　  
1．功能：更改文件名称　  
2．类型：内部命令　  
3．格式：REN[盘符：][路径]〈旧文件名〉〈新文件名〉　  
4．使用说明：　  
（1）新文件名前不可以加上盘符和路径，因为该命令只能对同一盘上的文件更换文件名；　  
（2）允许使用通配符更改一组文件名或扩展名。　  
（五）FC——文件比较命令　  
1．功能：比较文件的异同，并列出差异处。　  
2．类型：外部命令　  
3．格式：FC[盘符：][路径名]〈文件名〉[盘符：][路径名][文件名][/A][/B][/C][/N]　  
4．使用说明：　  
（1）选用/A参数，为ASCII码比较模式；　  
（2）选用/B参数，为二进制比较模式；　  
（3）选用/C参数，将大小写字符看成是相同的字符。　  
（4）选用/N参数，在ASCII码比较方式下，显示相异处的行号。　  
（六）ATTRIB——修改文件属性命令　  
1．功能：修改指定文件的属性。（文件属性参见2.5.4（二）文件属性一节）　  
2．类型：外部命令。　  
3．格式：ATTRIB[文件名][R][——R][A][——A][H][——H][——S]　  
4．使用说明：　  
（1）选用R参数，将指定文件设为只读属性，使得该文件只能读取，无法写入数据或删除；选用——R参数，去除只读属性；　  
（2）选用A参数，将文件设置为档案属性；选用——A参数，去除档案属性；　 （3）选用H参数，将文件调协为隐含属性；选用——H参数，去隐含属性；　  
（4）选用S参数，将文件设置为系统属性；选用——S参数，去除系统属性；　 （5）选用/S参数，对当前目录下的所有子目录及作设置。　  
七） DEL——删除文件命令　  
1．功能：删除指定的文件。　  
2．类型：内部命令　  
3．格式：DEL[盘符：][路径]〈文件名〉[/P]　  
4．使用说明：　  
（1）选用/P参数，系统在删除前询问是否真要删除该文件，若不使用这个参数，则自动删除；　  
（2）该命令不能删除属性为隐含或只读的文件；  
（3）在文件名称中可以使用通配符；  
（4）若要删除磁盘上的所有文件（DEL\*·\*或DEL·），则会提示：(Arey ou sure？）（你确定吗？）若回答Y，则进行删除，回答N，则取消此次删除作业。  
    （八） UNDELETE——恢复删除命令  
    1．功能：恢复被误删除命令  
    2．类型：外部命令。  
    3．格式：UNDELETE[盘符：][路径名]〈文件名〉[/DOS]/LIST][/ALL]  
    4．使用说明：使用UNDELETE可以使用“\*”和“？”通配符。  
    （1）选用/DOS参数根据目录里残留的记录来恢复文件。由于文件被删除时，目录所记载斩文件名第一个字符会被改为E5，DOS即依据文件开头的E5和其后续的字符来找到欲恢复的文件，所以，UNDELETE会要求用户输入一个字符，以便将文件名字补齐。但此字符不必和原来的一样，只需符合DOS的文件名规则即可。  
    （2）选用/LIST只“列出”符合指定条件的文件而不做恢复，所以对磁盘内容完全不会有影响。  
    （3）选用/ALL自动将可完全恢复的文件完全恢复，而不一一地询问用户，使用此参数时，若UNDELTE利用目录里残留的记录来将文件恢复，则会自动选一个字符将文件名补齐，并且使其不与现存文件名相同，选用字符的优选顺序为：#%——0000123456789A~Z。  
        UNDELETE还具有建立文件的防护措施的功能，已超出本课程授课范围，请读者在使用些功能时查阅有关DOS手册。  
    七、其它命令  
    （一）CLS——清屏幕命令  
    1功能：清除屏幕上的所有显示，光标置于屏幕左上角。  
    2类型：内部命令  
    3格式：CLS  
    （二） VER查看系统版本号命令  
    1功能：显示当前系统版本号  
    2类型：内部命令  
    3格式：VER  
    （三） DATA日期设置命令  
    1功能：设置或显示系统日期。  
    2类型：内部命令  
    3格式：DATE[mm——dd——yy]  
    4使用说明：  
    （1）省略[mm——dd——yy]显示系统日期并提示输入新的日期，不修改则可直接按回车键，[mm——dd——yy]为“月月——日日——年年”格式；  
    （2）当机器开始启动时，有自动处理文件（AUTOEXEC.BAT）被执行，则系统不提示输入系统日期。否则，提示输入新日期和时间。  
    （四） TIME系统时钟设置命令  
    1功能：设置或显示系统时期。  
    2类型：内部命令  
    3格式：TIME[hh：mm：ss：xx]  
    4使用说明：  
    （1）省略[hh：mm：ss：xx]，显示系统时间并提示输入新的时间，不修改则可直接按回车键，[hh：mm：ss：xx]为“小时：分钟：秒：百分之几秒”格式；  
    （2）当机器开始启动时，有自动处理文件（AUTOEXEC.BAT）被执行，则系统不提示输入系统日期。否则，提示输入新日期和时间。  
    （五）MEM查看当前内存状况命令  
    1功能：显示当前内存使用的情况  
    2类型：外部命令  
    3格式：MEM[/C][/F][/M][/P]  
    4使用说明：  
    （1）选用/C参数列出装入常规内存和CMB的各文件的长度，同时也显示内存空间的使用状况和最大的可用空间；  
    （2）选用/F参数分别列出当前常规内存剩余的字节大小和UMB可用的区域及大小；    
    （3）选用/M参数显示该模块使用内存地地址、大小及模块性质；  
    （4）选用/P参数指定当输出超过一屏时，暂停供用户查看。  
    （六） MSD显示系统信息命令  
    1功能：显示系统的硬件和操作系统的状况。  
    2类型：外部命令  
    3格式：MSD[/I][/B][/S]  
    4使用说明：  
    （1）选用/I参数时，不检测硬件；  
    （2）选用/B参数时，以黑白方式启动MSD；  
    （3）选用/S参数时，显示出简明的系统报告。  
ping命令详解  
对于Windows下ping命令相信大家已经再熟悉不过了，但是能把ping的功能发挥到最大的人却并不是很多，当然我也并不是说我可以让ping发挥最大的功能，我也只不过经常用ping这个工具，也总结了一些小经验，现在和大家分享一下。   
现在我就参照ping命令的帮助说明来给大家说说我使用ping时会用到的技巧，ping只有在安装了TCP/IP协议以后才可以使用：   
ping [-t] [-a] [-n count] [-l length] [-f] [-i ttl] [-v tos] [-r count] [-s count] [[-j computer-list] | [-k computer-list]] [-wz timeout] destination-list   
Options:   
-t Ping the specified host until stopped.To see statistics and continue - type Control-Break;To stop - type Control-C.   
不停的ping地方主机，直到你按下Control-C。   
此功能没有什么特别的技巧，不过可以配合其他参数使用，将在下面提到。   
-a Resolve addresses to hostnames.   
解析计算机NetBios名。   
示例：C:＼> ping -a 192.168.1.21   
Pinging iceblood.yofor.com [192.168.1.21] with 32 bytes of data:   
Reply from 192.168.1.21: bytes=32 time<10ms TTL=254   
Reply from 192.168.1.21: bytes=32 time<10ms TTL=254   
Reply from 192.168.1.21: bytes=32 time<10ms TTL=254   
Reply from 192.168.1.21: bytes=32 time<10ms TTL=254   
Ping statistics for 192.168.1.21:   
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),Approximate round trip times in milli-seconds:   
Minimum = 0ms, Maximum = 0ms, Average = 0ms   
从上面就可以知道IP为192.168.1.21的计算机NetBios名为iceblood.yofor.com。   
-n count Number of echo requests to send.   
发送count指定的Echo数据包数。   
在默认情况下，一般都只发送四个数据包，通过这个命令可以自己定义发送的个数，对衡量网络速度很有帮助，比如我想测试发送50个数据包的返回的平均时间为多少，最快时间为多少，最慢时间为多少就可以通过以下获知：   
C:＼>ping -n 50 202.103.96.68   
Pinging 202.103.96.68 with 32 bytes of data:   
Reply from 202.103.96.68: bytes=32 time=50ms TTL=241   
Reply from 202.103.96.68: bytes=32 time=50ms TTL=241   
Reply from 202.103.96.68: bytes=32 time=50ms TTL=241   
Request timed out.   
………………   
Reply from 202.103.96.68: bytes=32 time=50ms TTL=241   
Reply from 202.103.96.68: bytes=32 time=50ms TTL=241   
Ping statistics for 202.103.96.68:   
Packets: Sent = 50, Received = 48, Lost = 2 (4% loss),Approximate round trip times in milli-seconds:   
Minimum = 40ms, Maximum = 51ms, Average = 46ms   
从以上我就可以知道在给202.103.96.68发送50个数据包的过程当中，返回了48个，其中有两个由于未知原因丢失，这48个数据包当中返回速度最快为40ms，最慢为51ms，平均速度为46ms。   
-l size Send buffer size.   
定义echo数据包大小。   
在默认的情况下windows的ping发送的数据包大小为32byt，我们也可以自己定义它的大小，但有一个大小的限制，就是最大只能发送65500byt，也许有人会问为什么要限制到65500byt，因为Windows系列的系统都有一个安全漏洞（也许还包括其他系统）就是当向对方一次发送的数据包大于或等于65532时，对方就很有可能挡机，所以微软公司为了解决这一安全漏洞于是限制了ping的数据包大小。虽然微软公司已经做了此限制，但这个参数配合其他参数以后危害依然非常强大，比如我们就可以通过配合-t参数来实现一个带有攻击性的命令：（以下介绍带有危险性，仅用于试验，请勿轻易施于别人机器上，否则后果自负）   
C:＼>ping -l 65500 -t 192.168.1.21   
Pinging 192.168.1.21 with 65500 bytes of data:   
Reply from 192.168.1.21: bytes=65500 time<10ms TTL=254   
Reply from 192.168.1.21: bytes=65500 time<10ms TTL=254   
………………   
这样它就会不停的向192.168.1.21计算机发送大小为65500byt的数据包，如果你只有一台计算机也许没有什么效果，但如果有很多计算机那么就可以使对方完全瘫痪，我曾经就做过这样的试验，当我同时使用10台以上计算机ping一台Win2000Pro系统的计算机时，不到5分钟对方的网络就已经完全瘫痪，网络严重堵塞，HTTP和FTP服务完全停止，由此可见威力非同小可。   
-f Set Don't Fragment flag in packet.   
在数据包中发送“不要分段”标志。   
在一般你所发送的数据包都会通过路由分段再发送给对方，加上此参数以后路由就不会再分段处理。   
-i TTL Time To Live.   
指定TTL值在对方的系统里停留的时间。   
此参数同样是帮助你检查网络运转情况的。   
-v TOS Type Of Service.   
将“服务类型”字段设置为 tos 指定的值。   
-r count Record route for count hops.   
在“记录路由”字段中记录传出和返回数据包的路由。   
在一般情况下你发送的数据包是通过一个个路由才到达对方的，但到底是经过了哪些路由呢？通过此参数就可以设定你想探测经过的路由的个数，不过限制在了9个，也就是说你只能跟踪到9个路由，如果想探测更多，可以通过其他命令实现，我将在以后的文章中给大家讲解。以下为示例：   
C:＼>ping -n 1 -r 9 202.96.105.101 （发送一个数据包，最多记录9个路由）   
Pinging 202.96.105.101 with 32 bytes of data:   
Reply from 202.96.105.101: bytes=32 time=10ms TTL=249   
Route: 202.107.208.187 ->   
202.107.210.214 ->   
61.153.112.70 ->   
61.153.112.89 ->   
202.96.105.149 ->   
202.96.105.97 ->   
202.96.105.101 ->   
202.96.105.150 ->   
61.153.112.90   
  
Ping statistics for 202.96.105.101:   
Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),   
Approximate round trip times in milli-seconds:   
Minimum = 10ms, Maximum = 10ms, Average = 10ms   
从上面我就可以知道从我的计算机到202.96.105.101一共通过了202.107.208.187 ，202.107.210.214 , 61.153.112.70 , 61.153.112.89 , 202.96.105.149 , 202.96.105.97这几个路由。   
-s count Timestamp for count hops.   
指定 count 指定的跃点数的时间戳。   
此参数和-r差不多，只是这个参数不记录数据包返回所经过的路由，最多也只记录4个。   
-j host-list Loose source route along host-list.   
利用 computer-list 指定的计算机列表路由数据包。连续计算机可以被中间网关分隔（路由稀疏源）IP 允许的最大数量为 9。   
-k host-list Strict source route along host-list.   
利用 computer-list 指定的计算机列表路由数据包。连续计算机不能被中间网关分隔（路由严格源）IP 允许的最大数量为 9。   
-w timeout Timeout in milliseconds to wait for each reply.   
指定超时间隔，单位为毫秒。   
此参数没有什么其他技巧。   
ping命令的其他技巧：在一般情况下还可以通过ping对方让对方返回给你的TTL值大小，粗略的判断目标主机的系统类型是Windows系列还是UNIX/Linux系列，一般情况下Windows系列的系统返回的TTL值在100-130之间，而UNIX/Linux系列的系统返回的TTL值在240-255之间，当然TTL的值在对方的主机里是可以修改的，Windows系列的系统可以通过修改注册表以下键值实现：   
[HKEY\_LOCAL\_MACHINE＼SYSTEM＼CurrentControlSet＼Services＼Tcpip＼Parameters]   
"DefaultTTL"=dword:000000ff   
255---FF   
　 128---80   
　 64----40   
　 32----20   
好了，ping命令也基本上完全讲解完了，其中还有-j,-k参数我还没有详细说明，由于某些原因也包括我自己所收集的资料过少这里也没有向大家详细介绍，请大家见谅，如果在看了这篇文章的朋友当中有知道得比我更多的，以及其他使用技巧的也希望您能告诉我，并在此先谢过。   
对于Windows下ping命令相信大家已经再熟悉不过了，但是能把ping的功能发挥到最大的人却并不是很多，当然我也并不是说我可以让ping发挥最大的功能，我也只不过经常用ping这个工具，也总结了一些小经验，现在和大家分享一下。   
现在我就参照ping命令的帮助说明来给大家说说我使用ping时会用到的技巧，ping只有在安装了TCP/IP协议以后才可以使用：   
ping [-t] [-a] [-n count] [-l length] [-f] [-i ttl] [-v tos] [-r count] [-s count] [[-j computer-list] | [-k computer-list]] [-w timeout] destination-list   
Options:   
-t Ping the specified host until stopped.To see statistics and continue - type Control-Break;To stop - type Control-C.   
不停的ping地方主机，直到你按下Control-C。   
此功能没有什么特别的技巧，不过可以配合其他参数使用，将在下面提到。   
-a Resolve addresses to hostnames.   
解析计算机NetBios名。   
示例：C:＼>ping -a 192.168.1.21   
Pinging iceblood.yofor.com [192.168.1.21] with 32 bytes of data:   
Reply from 192.168.1.21: bytes=32 time<10ms TTL=254   
Reply from 192.168.1.21: bytes=32 time<10ms TTL=254   
Reply from 192.168.1.21: bytes=32 time<10ms TTL=254   
Reply from 192.168.1.21: bytes=32 time<10ms TTL=254   
Ping statistics for 192.168.1.21:   
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),Approximate round trip times in milli-seconds:   
Minimum = 0ms, Maximum = 0ms, Average = 0ms   
从上面就可以知道IP为192.168.1.21的计算机NetBios名为iceblood.yofor.com。   
-n count Number of echo requests to send.   
发送count指定的Echo数据包数。   
在默认情况下，一般都只发送四个数据包，通过这个命令可以自己定义发送的个数，对衡量网络速度很有帮助，比如我想测试发送50个数据包的返回的平均时间为多少，最快时间为多少，最慢时间为多少就可以通过以下获知：   
C:＼>ping -n 50 202.103.96.68   
Pinging 202.103.96.68 with 32 bytes of data:   
Reply from 202.103.96.68: bytes=32 time=50ms TTL=241   
Reply from 202.103.96.68: bytes=32 time=50ms TTL=241   
Reply from 202.103.96.68: bytes=32 time=50ms TTL=241   
Request timed out.   
………………   
Reply from 202.103.96.68: bytes=32 time=50ms TTL=241   
Reply from 202.103.96.68: bytes=32 time=50ms TTL=241   
Ping statistics for 202.103.96.68:   
Packets: Sent = 50, Received = 48, Lost = 2 (4% loss),Approximate round trip times in milli-seconds:   
Minimum = 40ms, Maximum = 51ms, Average = 46ms   
从以上我就可以知道在给202.103.96.68发送50个数据包的过程当中，返回了48个，其中有两个由于未知原因丢失，这48个数据包当中返回速度最快为40ms，最慢为51ms，平均速度为46ms。   
-l size Send buffer size.   
定义echo数据包大小。   
在默认的情况下windows的ping发送的数据包大小为32byt，我们也可以自己定义它的大小，但有一个大小的限制，就是最大只能发送65500byt，也许有人会问为什么要限制到65500byt，因为Windows系列的系统都有一个安全漏洞（也许还包括其他系统）就是当向对方一次发送的数据包大于或等于65532时，对方就很有可能挡机，所以微软公司为了解决这一安全漏洞于是限制了ping的数据包大小。虽然微软公司已经做了此限制，但这个参数配合其他参数以后危害依然非常强大，比如我们就可以通过配合-t参数来实现一个带有攻击性的命令：（以下介绍带有危险性，仅用于试验，请勿轻易施于别人机器上，否则后果自负）   
C:＼>ping -l 65500 -t 192.168.1.21   
Pinging 192.168.1.21 with 65500 bytes of data:   
Reply from 192.168.1.21: bytes=65500 time<10ms TTL=254   
Reply from 192.168.1.21: bytes=65500 time<10ms TTL=254   
………………   
这样它就会不停的向192.168.1.21计算机发送大小为65500byt的数据包，如果你只有一台计算机也许没有什么效果，但如果有很多计算机那么就可以使对方完全瘫痪，我曾经就做过这样的试验，当我同时使用10台以上计算机ping一台Win2000Pro系统的计算机时，不到5分钟对方的网络就已经完全瘫痪，网络严重堵塞，HTTP和FTP服务完全停止，由此可见威力非同小可。   
-f Set Don't Fragment flag in packet.   
在数据包中发送“不要分段”标志。   
在一般你所发送的数据包都会通过路由分段再发送给对方，加上此参数以后路由就不会再分段处理。   
-i TTL Time To Live.   
指定TTL值在对方的系统里停留的时间。   
此参数同样是帮助你检查网络运转情况的。   
-v TOS Type Of Service.   
将“服务类型”字段设置为 tos 指定的值。   
-r count Record route for count hops.   
在“记录路由”字段中记录传出和返回数据包的路由。   
在一般情况下你发送的数据包是通过一个个路由才到达对方的，但到底是经过了哪些路由呢？通过此参数就可以设定你想探测经过的路由的个数，不过限制在了9个，也就是说你只能跟踪到9个路由，如果想探测更多，可以通过其他命令实现，我将在以后的文章中给大家讲解。以下为示例：   
C:＼>ping -n 1 -r 9 202.96.105.101 （发送一个数据包，最多记录9个路由）   
Pinging 202.96.105.101 with 32 bytes of data:   
Reply from 202.96.105.101: bytes=32 time=10ms TTL=249   
Route: 202.107.208.187 ->   
202.107.210.214 ->   
61.153.112.70 ->   
61.153.112.89 ->   
202.96.105.149 ->   
202.96.105.97 ->   
202.96.105.101 ->   
202.96.105.150 ->   
61.153.112.90   
Ping statistics for 202.96.105.101:   
Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),   
Approximate round trip times in milli-seconds:   
Minimum = 10ms, Maximum = 10ms, Average = 10ms   
从上面我就可以知道从我的计算机到202.96.105.101一共通过了202.107.208.187 ，202.107.210.214 , 61.153.112.70 , 61.153.112.89 , 202.96.105.149 , 202.96.105.97这几个路由。   
-s count Timestamp for count hops.   
指定 count 指定的跃点数的时间戳。   
此参数和-r差不多，只是这个参数不记录数据包返回所经过的路由，最多也只记录4个。   
-j host-list Loose source route along host-list.   
利用 computer-list 指定的计算机列表路由数据包。连续计算机可以被中间网关分隔（路由稀疏源）IP 允许的最大数量为 9。   
-k host-list Strict source route along host-list.   
利用 computer-list 指定的计算机列表路由数据包。连续计算机不能被中间网关分隔（路由严格源）IP 允许的最大数量为 9。   
-w timeout Timeout in milliseconds to wait for each reply.   
指定超时间隔，单位为毫秒。   
此参数没有什么其他技巧。   
ping命令的其他技巧：在一般情况下还可以通过ping对方让对方返回给你的TTL值大小，粗略的判断目标主机的系统类型是Windows系列还是UNIX/Linux系列，一般情况下Windows系列的系统返回的TTL值在100-130之间，而UNIX/Linux系列的系统返回的TTL值在240-255之间，当然TTL的值在对方的主机里是可以修改的，Windows系列的系统可以通过修改注册表以下键值实现：   
[HKEY\_LOCAL\_MACHINE＼SYSTEM＼CurrentControlSet＼Services＼Tcpip＼Parameters]   
"DefaultTTL"=dword:000000ff   
255---FF   
　 128---80   
　 64----40   
　 32----20   
好了，ping命令也基本上完全讲解完了，其中还有-j,-k参数我还没有详细说明，由于某些原因也包括我自己所收集的资料过少这里也没有向大家详细介绍，请大家见谅，如果在看了这篇文章的朋友当中有知道得比我更多的，以及其他使用技巧的也希望您能告诉我，并在此先谢过。   
FTP命令大全  
FTP:文件传输协议。先说说他的功能吧，主要就是从运行FTP服务器的计算机传输文件。可以交互使用。这里要注意，只有安装了tcp/ip协议的机器才能使用ftp命令。   
命令格式：ftp [-v][-d][-i][-n][-g][-s:filename][-a][-w:windowsize][computer]   
说说他们的含义吧。   
-v 不显示远程服务器响应   
-n 禁止第一次连接的时候自动登陆   
-i 在多个文件传输期间关闭交互提示   
-d 允许调试、显示客户机和服务器之间传递的全部ftp命令   
-g 不允许使用文件名通配符，文件名通配符的意思是说允许在本地文件以及路径名中使用通配字符   
-s:filename 指定包含ftp命令的文本文件。在ftp命令启动后将自动运行这些命令。在加的参数里不能有空格。   
-a 绑定数据连接时，使用任何的本地端口   
-w:windowsize 忽略默认的4096传输缓冲区   
computer 指定要连接的远程计算机的ip地址   
呵呵，理解了上面的，就说说一些具体的命令，我个人觉得虽然现在工具用起来很方便了，但懂这些命令在很多地方还是很有用的，就像现在nt下的命令提示符  
1） ?   
说明：显示ftp命令的说明。后面可以加参数，是加需要解释的命令名，不加则显示包含所有命令列表。   
2） append   
说明：使用当前文件类型设置，将本地文件附加到远程计算机中。大概格式是   
append local-file [remote-file] 其中local-file是说指定要添加的本地文件。   
remote-file是说指定要将local-file附加到远程计算机文件，要是省了这个，则是使用本地文件名做远程文件名。   
3)ascii   
说明:默认情况下，将文件传输类型设置为ASCII   
4)bell   
说明：响玲开关，意思是文件传输完成后是否有玲声提醒。默认是关闭的。   
5)binary   
说明：将文件传输类型设置为二进制。   
6)bye   
说明:结束和远程计算机的ftp会话，也就是安全断开，退出ftp.   
7)cd   
说明：更改远程计算机上的工作目录。如cd data 其中data是要进入的远程计算机的目录。   
8)close   
说明:结束与远程服务器的ftp会话，并返回命令解释程序。   
9)dir   
说明:显示远程的文件以及子目录列表。如dir data local-file   
其中data是指定要查看列表的目录，没指定的话就是当前目录。local-file是指定要保存列表的本地文件，不指定的话就在屏幕输出。   
10)debug   
说明：调试开关，打开的时候打印每个发送到远程计算机的命令，命令前有——>   
默认情况是关闭的。   
11)disconnnect   
说明：与远程计算机断开连接，但还保持着ftp命令提示符。   
12)get   
说明：使用当前文件传输类型，把远程的文件拷贝到本地计算机上。   
如get remote-file local-file   
remote-file是指定要复制的文件，local-file是指定本地计算机上的文件名，   
没有指定的话则个remote-file同名。   
13)glob   
说明：文件名通配开关   
14)hash   
说明：转换每个传输数据快的散列标记打印(#).数据快的大小是2048字节。默认情况下是关闭的，   
15)help   
说明：显示ftp命令的解释，如help commmand 其中command就是你要解释的命令，如果不加command这个参数的话就会显示所有命令的列表   
16)!   
说明:这个命令差点忘记了:)功能是在本地计算机上运行指定命令。如! command 其中command就是你要运行的命令，如果不加command这个参数的话，则显示本地命令提示， 这时你输入exit命令就能返回到ftp了。   
17)lcd   
说明:更改本地计算机的本地目录,在默认的时候是启动ftp的目录.这个不要觉得没用啊，在你使用ftp的时候为了传递文件不是常改变本地和远程计算机的目录吗?:)   
如lcd [directory] 其中[directory]是指定要进入的本地计算机的目录,如果你不加这个参数,就会显示出本地计算机的工作目录.   
18)literal   
说明:向远程ftp服务器发送协商参数,报告.   
如lireral argument [...] 其中argument是指定要发送给远程服务器的协商参数。   
19)ls   
说明:显示远程目录的文件和字目录.   
如ls remote-directory local-file   
其中remote-directory是指要查看的列表的目录,不指定的话显示的是当前工作目录。local-file是指定要保存列表的本地文件.不指定的话是在屏幕上输出.   
20)mdelete   
说明:删除远程计算机上的文件.如mdelete remote-file ...   
remote-file肯定是要删的文件啊，可以删除多个.   
21)mdir   
说明:显示远程目录的文件和子目录列表,他允许指定多个文件.   
如mdir remote-file ... local-file   
参数我想大家应该明白什么意思吧?不明白就看看前面的类似命令吧.   
22)mget   
说明:使用当前文件传输类型将多个远程文件复制到本地计算机.   
如mget remote-files ...   
其实remote-files可以指定多个，他就是指定要复制到本地计算机的远程文件.   
23)mkdir   
说明:创建远程目录.   
如mkdir directory 这个命令和nt下的命令提示符中的md directory一样，不多说了.   
24)mls   
说明:显示远程目录的文件和目录简表   
如mls remote-file ... local-file   
其中remote-file这个参数是必须要加的，’’-’’是使用远程计算机的当前工作目录.   
25)mput   
说明:使用当前文件传输类型,将本地文件复制到远程计算机.   
如mput local-files ...   
26)open   
说明:连接到指定ftp服务器上，   
如open computer port 其中computer一般是远程计算机的ip地址,port不用说就是指定端口了。   
27)prompt   
说明:转换提示,在多个文件传输的时候,ftp提示可以有选择的检索或保存文件，如果关闭提示,则mget和mput命令传输所有文件,在默认情况下是打开的.   
28)put   
说明:使用当前文件传输类型将本地文件复制到远程计算机中，   
如put local-file remote-file   
其中local-file是指定要复制的本地文件，   
remote-file是指定要复制的远程计算机上的文件名，不指定的话是和本地计算机上的文件名同名.   
29)pwd   
说明:显示远程呢感计算机上的当前目录.   
30)quit   
说明:结束与远程计算机的ftp会话,并退出ftp.   
31)quote   
说明:向远程ftp服务器发送协议,报告.期待ftp单码应答,这个命令的功能和literal相同.   
32)recv   
说明:使用当前文件传输类型将远程文件复制到本地计算机,他与get命令作用相同。   
33)remotehelp   
说明:显示远程命令的帮助.这个命令的用法和help,!一样可以参考他的用法.   
34)rename   
说明:更改远程计算机上的文件名。   
这个命令和nt的命令提示符的ren一样，如rename filename newfilename   
35)rmdir   
说明:删除远程目录.   
这个命令和nt的命令提示符的rm一样，如rmdir directory   
36)send   
说明:使用当前文件传输类型将本地文件复制到远程计算机.send和put命令的功能一样。   
如send local-file remote-file   
37)status   
说明:显示ftp连接和转换的当前状态   
38)trace   
说明:转换报文跟踪,运行ftp的命令时,trace将显示没个报文的理由。   
39)type   
说明:设置或显示文件传输类型.   
如type [type-name]   
其中type-name 的意思是文件传输的类型，默认是ASCII,没加这个参数就是显示当前的传输类型.   
40)user   
说明:指定连接到远程计算机的用户.   
如user user-name [passwd] [account]   
其中user-name不用说都是用来登陆计算机的用户名了，   
passwd是指定user-name的密码,不指定的话ftp会提示输入密码。   
account是指定用来登陆计算机的帐号,如不指定,ftp会提示输入帐号.   
41)verbose   
说明:转换冗余模式。这里如果打开,会显示所有ftp响应,文件传输结束的时候会显示传输的效率和统计信息,默认的情况是打开的.   
呵呵，命令就介绍这些了，可以自己熟悉一下,其实现在ftp的软件很多,很方便，但你说这些命令没用也是不可能的，就像windows下一样还保留着命令提示符.:)\_ 特别有些时候ftp软件很多地方做不到的，.? 什么地方。   
打个比方，我看过一种觅名ftp用户得到admin的入侵列子,就的用到他.呵呵，这里不多说了,就写到这里了。

net命令详解  
许多 Windows NT 网络命令以 net 开始。这些 net 命令有一些公共属性：   
通过键入 net /? 可查阅所有可用的 net 命令。   
通过键入 net help 命令可在命令行中获得 net 命令的语法帮助。例如，要得到 net acco  
unts 命令的帮助，请键入 net help accounts。   
所有 net 命令接受选项 / yes 和 /no（可缩写为 / y 和 /n ）。/ y 对命令产生的任何交  
互提示自动回答“是”，/n 回答“否”。例如，net stop server 通常提示确认是否根据服  
务器服务结束所有服务，net stop server /y 自动回答“是”并关闭服务器服务。   
Net Accounts   
更新用户帐号数据库、更改密码及所有帐号的登录要求。必须要在更改帐号参数的计算机上  
运行网络登录服务。   
net accounts [/forcelogoff:{minutes | no}] [/minpwlen:length] [/maxpwage:{days |  
unlimited}] [/minpwage:days] [/uniquepw:number] [/domain]   
net accounts [/sync] [/domain]   
参数   
无   
键入不带参数的 net accounts，将显示当前密码设置、登录时限及域信息。   
/forcelogoff:{minutes | no}   
设置当用户帐号或有效登录时间过期时，结束用户和服务器会话前的等待时间。no 选项禁止  
强行注销。该参数的默认设置为 no。   
指定 /forcelogoff:minutes 之后，Windows NT 在其强制用户退出网络 minutes 分钟之前  
，将给用户发出警报。如果还有打开的文件，Windows NT 将警告用户。如果 minutes 小于  
两分钟，Windows NT 警告用户立即从网络注销。   
/minpwlen:length   
设置用户帐号密码的最少字符数。允许范围是 0-14，默认值为 6。   
/maxpwage:{days | unlimited}   
设置用户帐号密码有效的最大天数。unlimited 不设置最大天数。/maxpwage 选项的天数必  
须大于 /minpwage。允许范围是 1-49,710 天 (unlimited)。默认值为 90 天。   
/minpwage:days   
设置用户必须保持原密码的最小天数。 0 值不设置最小时间。允许范围是 0-49,710 天，默  
认值为 0 天。   
/uniquepw:number   
要求用户更改密码时，必须在经过 number 次后，才能重复使用与之相同的密码。允许范围  
是 0-8。默认值为 5。   
/domain   
在当前域的主域控制器上执行该操作。否则只在本地计算机执行操作。   
该参数仅用于 Windows NT Server 域中的 Windows NT Workstation 计算机，Windows NT   
Server 计算机默认为在主域控制器执行操作。   
/sync   
当用于主域控制器时，该命令使域中所有备份域控制器同步；当用于备份域控制器时，该命  
令仅使该备份域控制器与主域控制器同步。该命令仅适用于 Windows NT Server 域成员的计  
算机。   
Net Computer   
从域数据库中添加或删除计算机。该命令仅在运行 Windows NT Server 的计算机上可用。   
net computer \computername {/add | /del}   
参数   
\computername   
指定要添加到域或从域中删除的计算机。   
/add   
将指定计算机添加到域。   
/del   
将指定计算机从域中删除。   
Net Config   
显示当前运行的可配置服务，或显示并更改某项服务的设置。   
net config [service [options]]   
参数   
无   
键入不带参数的 net config 将显示可配置服务的列表。   
service   
通过 net config 命令进行配置的服务（server 或 workstation）。   
options   
服务的特定选项。完整语法请参阅 net config server 或 net config workstation。   
Net Config Server   
运行服务时显示或更改服务器的服务设置。   
net config server [/autodisconnect:time] [/srvcomment:"text "] [/hidden:{yes | n  
o}]   
参数   
无   
键入不带参数的 net config server，将显示服务器服务的当前配置。   
/autodisconnect:time   
设置断开前用户会话闲置的最大时间值。可以指定 -1，表示永不断开连接。允许范围是 -1  
-65535 分钟，默认值是 15 分钟。   
/srvcomment:"text "   
为服务器添加注释，可以通过 net view 命令在屏幕上显示所加注释。注释最多可达 48 个  
字符，文字要用引号引住。   
/hidden:{yes | no}   
指定服务器的计算机名是否出现在服务器列表中。请注意隐含某个服务器并不改变该服务器  
的权限。默认为 no。   
Net Config Workstation   
服务运行时，显示或更改工作站各项服务的设置。   
net config workstation [/charcount:bytes] [/chartime:msec] [/charwait:sec]   
参数   
无   
键入不带参数的 net config workstation 将显示本地计算机的当前配置。   
/charcount:bytes   
指定 Windows NT 在将数据发送到通讯设备之前收集的数据量。如果同时设置 /chartime:m  
sec 参数，Windows NT 按首先满足条件的选项运行。允许范围是 0-65535 字节，默认值是  
16 字节。   
/chartime:msec   
指定 Windows NT 在将数据发送到通讯设备之前收集数据的时间。如果同时设置 /charcoun  
t:bytes 参数，Windows NT 按首先满足条件的选项运行。允许范围是 0-65535000 毫秒，默  
认值是 250 毫秒。   
/charwait:sec   
设置 Windows NT 等待通讯设备变为可用的时间。允许的范围是 0-65535 秒，默认值是 36  
00 秒。   
Net Continue   
重新激活挂起的服务。   
net continue service   
参数   
service   
能够继续运行的服务，包括： file server for macintosh（该服务仅限于 Windows NT Se  
rver）, ftp publishing service, lpdsvc, net logon, network dde，network dde dsdm  
，nt lm security support provider，remoteboot（该服务仅限于 Windows NT Server），  
remote access server, schedule，server，simple tcp/ip services 及 workstation 。  
Net File   
显示某服务器上所有打开的共享文件名及锁定文件数。该命令也可以关闭个别文件并取消文  
件锁定。   
net file [id [/close]]   
参数   
无   
键入不带参数的 net file 可获得服务器上打开文件的列表。   
id   
文件标识号。   
/close   
关闭打开的文件并释放锁定记录。请从共享文件的服务器中键入该命令。   
Net Group   
在 Windows NT Server 域中添加、显示或更改全局组。该命令仅在 Windows NT Server 域  
中可用。   
net group [groupname [/comment:"text "]] [/domain]   
net group groupname {/add [/comment:"text "] | /delete} [/domain]   
net group groupname username [ ...] {/add | /delete} [/domain]   
参数   
无   
键入不带参数的 net group 可以显示服务器名称及服务器的组名称。   
groupname   
要添加、扩展或删除的组。仅提供某个组名便可查看组中的用户列表。   
/comment:"text "   
为新建组或现有组添加注释。注释最多可以是 48 个字符，并用引号将注释文字引住。   
/domain   
在当前域的主域控制器中执行该操作，否则在本地计算机上执行操作。   
该参数仅用于作为 Windows NT Server 域成员的 Windows NT Workstation 计算机。Windo  
ws NT Server 计算机默认为在主域控制器中操作。   
username[ ...]   
列表显示要添加到组或从组中删除的一个或多个用户。使用空格分隔多个用户名称项。   
/add   
添加组或在组中添加用户名。必须使用该命令为添加到组中的用户建立帐号。   
/delete   
删除组或从组中删除用户名。   
Net Help   
提供网络命令列表及帮助主题，或提供指定命令或主题的帮助。可用网络命令列于 N 下面的  
“命令参考”中“命令”窗口内。   
net help [command]   
net command {/help | /?}   
参数   
无   
键入不带参数的 net help 显示能够获得帮助的命令列表和帮助主题。   
command   
需要其帮助的命令，不要将 net 作为 command 的一部分。   
/help   
提供显示帮助文本方式选择。   
/?   
显示命令的正确语法。   
Net Helpmsg   
提供 Windows NT 错误信息的帮助。   
net helpmsg message#   
参数   
message#   
需要其帮助的 Windows NT 消息的四位代码。   
Net Localgroup   
添加、显示或更改本地组。   
net localgroup [groupname [/comment:"text "]] [/domain]   
net localgroup groupname {/add [/comment:"text "] | /delete} [/domain]   
net localgroup groupname name [ ...] {/add | /delete} [/domain]   
参数   
无   
键入不带参数的 net localgroup 将显示服务器名称和计算机的本地组名称。   
groupname   
要添加、扩充或删除的本地组名称。只提供 groupname 即可查看用户列表或本地组中的全局   
组。   
/comment: "text "   
为新建或现有组添加注释。注释文字的最大长度是 48 个字符，并用引号引住。   
/domain   
在当前域的主域控制器中执行操作，否则仅在本地计算机上执行操作。   
该参数仅应用于 Windows NT Server 域中的 Windows NT Workstation 计算机。Windows N  
T Server 计算机默认为在主域控制器中操作。   
name [ ...]   
列出要添加到本地组或从本地组中删除的一个或多个用户名或组名，多个用户名或组名之间  
以空格分隔。可以是本地用户、其他域用户或全局组，但不能是其他本地组。如果是其他域  
的用户，要在用户名前加域名（例如，SALESRALPHR）。   
/add   
将全局组名或用户名添加到本地组中。在使用该命令将用户或全局组添加到本地组之前，必  
须为其建立帐号。   
/delete   
从本地组中删除组名或用户名。   
Net Name   
添加或删除消息名（有时也称别名），或显示计算机接收消息的名称列表。要使用 net nam  
e 命令，计算机中必须运行信使服务。   
net name [name [/add | /delete]]   
参数   
无   
键入不带参数的 net name 将列出当前使用的名称。   
name   
指定接收消息的名称。名称最多为 15 个字符。   
/add   
将名称添加到计算机中。 /add 是可选项，键入 net name name 与键入 net name name /a  
dd 相同。   
/delete   
从计算机中删除名称。   
Net Pause   
暂停正在运行的服务。   
net pause service   
参数   
service   
指下列服务： file server for macintosh（仅限于 Windows NT Server）、ftp publishi  
ng service、lpdsvc、net logon、network dde、network dde dsdm、nt lm security sup  
port provider、remoteboot（仅限于 Windows NT Server）、remote access server、sch  
edule、server、simple tcp/ip services 或 workstation 。   
Net Print   
显示或控制打印作业及打印队列。   
net print \computername sharename   
net print [\computername ] job# [/hold | /release | /delete]   
参数   
computername   
共享打印机队列的计算机名。   
sharename   
打印队列名称。当包含 computername 与 sharename 时，使用反斜杠 () 将它们分开。   
job#   
在打印机队列中分配给打印作业的标识号。有一个或多个打印机队列的计算机为每个打印作  
业分配唯一标识号。如果某个作业号用于共享打印机队列中，则不能指定给其他作业，也不  
能分配给其他打印机队列中的作业。   
/hold   
使用 job# 时，在打印机队列中使打印作业等待。打印作业停留在打印机队列中，并且其他  
打印作业只能等到释放该作业之后才能进入。   
/release   
释放保留的打印作业。   
/delete   
从打印机队列中删除打印作业。   
Net Send   
向网络的其他用户、计算机或通信名发送消息。要接收消息必须运行信使服务。   
net send {name | \* | /domain[:name] | /users} message   
参数   
name   
要接收发送消息的用户名、计算机名或通信名。如果计算机名包含空字符，则要将其用引号  
(" ") 引住。   
\*   
将消息发送到组中所有名称。   
/domain[:name]   
将消息发送到计算机域中的所有名称。如果指定 name，则消息将发送到指定域或组中的所有  
名称。   
/users   
将消息发送到与服务器连接的所有用户。   
message   
作为消息发送的文本。   
Net Session   
列出或断开本地计算机和与之连接的客户端的会话。   
net session [\computername] [/delete]   
参数   
无   
键入不带参数的 net session 可以显示所有与本地计算机的会话的信息。   
\computername   
标识要列出或断开会话的计算机。   
/delete   
结束与 \computername 计算机会话并关闭本次会话期间计算机的所有打开文件。如果省略   
\computername 参数，将取消与本地计算机的所有会话。   
Net Share   
创建、删除或显示共享资源。   
net share sharename   
net share sharename=drive:path [/users:number | /unlimited] [/remark:"text"]   
net share sharename [/users:number | unlimited] [/remark:"text"]   
net share {sharename | drive:path} /delete   
参数   
无   
键入不带参数的 net share 将显示本地计算机上所有共享资源的信息。   
sharename   
是共享资源的网络名称。键入带 sharename 的 net share 命令，只显示该共享信息。   
drive:path   
指定共享目录的绝对路径。   
/users:number   
设置可同时访问共享资源的最大用户数。   
/unlimited   
不限制同时访问共享资源的用户数。   
/remark:"text "   
添加关于资源的注释，注释文字用引号引住。   
/delete   
停止共享资源。   
Net Start   
启动服务，或显示已启动服务的列表。如果服务名是两个或两个以上的词，如 Net Logon 或  
Computer Browser，则必须用引号 (") 引住。.   
net start [service]   
参数   
无   
键入不带参数的 net start 则显示运行服务的列表。   
service   
包括下列服务： alerter、client service for netware、clipbook server、computer br  
owser、dhcp client 、directory replicator 、eventlog 、ftp publishing service 、  
lpdsvc、messenger 、net logon 、network dde 、network dde dsdm 、network monitor  
ing agent 、nt lm security support provider 、ole 、remote access connection man  
ager 、remote access isnsap service 、remote access server 、remote procedure ca  
ll (rpc) locator 、remote procedure call (rpc) service 、schedule 、server 、sim  
ple tcp/ip services 、snmp、spooler 、tcp/ip netbios helper 、ups 及 workstation  
。   
下列服务仅在 Windows NT Server 下可用：file server for macintosh、gateway servic  
e for netware、microsoft dhcp server、print server for macintosh、remoteboot、wi  
ndows internet name service 。   
Net Statistics   
显示本地工作站或服务器服务的统计记录。   
net statistics [workstation | server]   
参数   
无   
键入不带参数的 net statistics 将列出其统计信息可用的运行服务。   
workstation   
显示本地工作站服务的统计信息。   
server   
显示本地服务器服务的统计信息。   
Net Stop   
停止 Windows NT 网络服务。   
net stop service   
参数   
service   
包括下列服务： alerter（警报）、client service for netware（Netware 客户端服务）  
、clipbook server（剪贴簿服务器）、computer browser（计算机浏览器）、directory r  
eplicator（目录复制器）、ftp publishing service (ftp )（ftp 发行服务）、lpdsvc、  
messenger（信使）、net logon（网络登录）、network dde（网络 dde）、network dde d  
sdm（网络 dde dsdm）、network monitor agent（网络监控代理）、nt lm security supp  
ort provider（NT LM 安全性支持提供）、ole（对象链接与嵌入）、remote access conne  
ction manager（远程访问连接管理器）、remote access isnsap service（远程访问 isns  
ap 服务）、remote access server（远程访问服务器）、remote procedure call (rpc) l  
ocator（远程过程调用定位器）、remote procedure call (rpc) service（远程过程调用服  
务）、schedule（调度）、server（服务器）、simple tcp/ip services（简单 TCP/IP 服  
务）、snmp、spooler（后台打印程序）、tcp/ip netbios helper（TCP/IP NETBIOS 辅助工  
具）、ups 及 workstation（工作站）。   
下列服务仅在 Windows NT Server 中可用： file server for macintosh、gateway servi  
ce for netware、microsoft dhcp server、print server for macintosh、remoteboot、w  
indows internet name service。   
Net Time   
使计算机的时钟与另一台计算机或域的时间同步。不带 /set 参数使用时，将显示另一台计  
算机或域的时间。   
net time [\computername | /domain[:name]] [/set]   
参数   
\computername   
要检查或同步的服务器名。   
/domain[:name]   
指定要与其时间同步的域。   
/set   
使本计算机时钟与指定计算机或域的时钟同步。   
Net Use   
连接计算机或断开计算机与共享资源的连接，或显示计算机的连接信息。该命令也控制永久  
网络连接。   
net use [devicename | \*] [\computernamesharename[volume]] [password | \*]] [/user  
:[domainname]username] [[/delete] | [/persistent:{yes | no}]]   
net use devicename [/home[password | \*]] [/delete:{yes | no}]   
net use [/persistent:{yes | no}]   
参数   
无   
键入不带参数的 net use 将列出网络连接。   
devicename   
指定要连接到的资源名称或要断开的设备名称。有两类设备名：磁盘驱动器（D: 到 Z:）和  
打印机（LPT1: 到 LPT3）。若键入星号而不是指定设备名将分配下一个可用设备名。   
\computernamesharename   
服务器及共享资源的名称。如果计算机名包含空白字符，要用引号 (" ") 将双反斜线及计算  
机名引住。计算机名长度可以是 1-15 个字符。   
volume   
指定服务器上的 NetWare 卷。要连接到 NetWare 服务器，必须安装并运行 NetWare 客户机  
服务 (Windows NT Workstation) 或 NetWare 网关服务 (Windows NT Server)。   
password   
访问共享资源的密码。   
\*   
提示键入密码。在密码提示行中键入密码时，将不显示该密码。   
/user   
指定进行连接的另外一个用户。   
domainname   
指定另一个域。例如 net use d: \servershare /user:adminmariel 连接用户 mariel，如  
同从 admin 域连接一样。如果省略域，将使用当前登录域。   
username   
指定登录的用户名。   
/home   
将用户连接到其宿主目录。   
/delete   
取消指定网络连接。如果用户以星号指定连接，则取消所有网络连接。   
/persistent   
控制永久网络连接的使用。默认为上次使用的设置。无设备的连接不是永久的。   
yes   
保存建立的所有连接，并在下次登录时还原。   
no   
不保存建立的连接和继发连接，并在下次登录时还原现有连接。使用 /delete 开关项取消永  
久连接。   
Net User   
添加或更改用户帐号或显示用户帐号信息。   
net user [username [password | \*] [options]] [/domain]   
net user username {password | \*} /add [options] [/domain]   
net user username [/delete] [/domain]   
参数   
无   
键入不带参数的 net user 将查看计算机上的用户帐号列表。   
username   
添加、删除、更改或查看用户帐号名。用户帐号名最多可以有 20 个字符。   
password   
为用户帐号分配或更改密码。密码必须满足在 net accounts 命令 /minpwlen 选项中设置的  
最小参数。最多是 14 个字符。   
\*   
提示输入密码。在密码提示行中键入密码时，将不显示该密码。   
/domain   
在计算机主域的主域控制器中执行操作。   
该参数仅在 Windows NT Server 域成员的 Windows NT Workstation 计算机上可用。默认情  
况下，Windows NT Server 计算机在主域控制器中执行操作。   
注意：在计算机主域的主域控制器发生该动作。它可能不是登录域。   
/add   
将用户帐号添加到用户帐号数据库。   
/delete   
从用户帐号数据库中删除用户帐号。   
选项如下所示：   
/active:{no | yes}   
启用或禁止用户帐号。如果不激活用户帐号，用户就不能访问计算机上的资源。默认值是 y  
es （激活）。   
/comment:"text"   
提供用户帐号的注释。该注释最多可以有 48 个字符，文字用引号引住。   
/countrycode:nnn   
使用操作系统的国家代码以便为用户帮助和错误信息文件提供指定语言文件。0 值表示默认  
国家代码。   
/expires:{date | never}   
如果设置 date，将导致用户帐号过期，never 不对用户帐号设置时间限制。过期日期根据   
/countrycode 值可以是下列格式： mm/dd/yy、dd/mm/yy 或 mmm, dd, yy。注意帐号在指定  
日期开始时过期。月份可以是数字、全名或三个字母的简拼。年可以是两位或四位数，使用  
逗号或斜线（不要用空格） 区分日期的各部分。如果省略 yy ，则使用该日期下一次到来的  
年份（根据计算机的时钟）。例如如果在 1994 年 1 月 10 日到 1995 年 1 月 8 日之间输  
入下列日期项，那它们相同：jan,9   
1/9/95   
january,9,1995   
1/9   
/fullname:"name"   
指定用户全名而不是用户名。用引号将名字引住。   
/homedir:path   
设置用户宿主目录的路径。该路径必须存在。   
/homedirreq:{yes | no}   
设置是否需要宿主目录。   
/passwordchg:{yes | no}   
指定用户是否能改变自己的密码。默认值是 yes。   
/passwordreq:{yes | no}   
指定用户帐号是否需要密码，默认值是 yes。   
/profilepath:[path]   
设置用户登录配置文件的路径。该路径名指向注册表配置文件。   
/scriptpath:path   
为用户登录脚本设置路径。Path 不能是绝对路径；   
path 是相对于 %systemroot%SYSTEM32REPLIMPORTSCRIPTS 的相对路径：。   
/times:{times | all}   
指定允许用户使用计算机的时间。times 值表示为 day[-day][, day[-day]] , time[-time  
][, time[-time]], 增量限制为一小时。Days 可以是全名或简写（M、T、W、Th、F、Sa、S  
u）。Hours 可以是 12 小时制或 24 小时制。对于 12 小时值，使用 AM、PM 或 A.M、P.M  
。all 表示用户总可以登录。空值表示用户永远不能登录。用逗号分隔日期和时间，分隔时  
间和日期的单位用分号（例如 M,4AM-5PM; T,1PM-3PM）。指定 /times 时不要使用空格。   
/usercomment:"text "   
让管理员添加或更改帐号的“用户注释”。用引号引住文字。   
/workstations:{computername[,...] | \*}   
列出最多八个用户可以登录到网络的工作站。用逗号分隔列表中的多个项。如果 /workstat  
ions 没有列表，或如果列表是星号“\*”，则用户可以从任何一台计算机登录。   
Net View   
显示域列表、计算机列表或指定计算机的共享资源列表。   
net view [\computername | /domain[:domainname]]   
net view /network:nw [\computername]   
参数   
无   
键入不带参数的 net view 将显示当前域的计算机列表。   
\computername   
指定要查看其共享资源的计算机。   
/domain[:domainname]   
指定要查看其可用计算机的域。如果省略 domainname ，则显示网络的所有域。   
/network:nw   
显示 NetWare 网络中所有可用的服务器。如果指定计算机名，则显示 NetWare 网络中该计  
算机的可用资源。也可以用此开关指定添加到系统中的其他网络。

telnet命令详解  
除了在Telnet是如何工作的例子介绍的以外,Telnet还有很多的特点。Telnet可发送除了"escape"的任何字符到远程主机上。因为"escape"字符在Telnet中是客户机的一个特殊的命令模式，它的默认值是"Ctrl-]"。但要注意不要与键盘上的Esc键混淆，我们可以设定"escape"为任意某个字符，只是对Telnet来说以为着该字符不可能再被传送到远程主机上，而Esc键是一非打印字符，Telnet用它来删除远程系统中的命令。而且还应记住，"escape"字符并不总以"Ctrl-]"来表示。  
可以仅仅键入Telnet,后面不带机器字句。这种情况下所看到的是Telnet>,这是告知Telnet在等待键入命令，比如键入问号"?"那么就得到一个有用的命令表：  
telnet: ?  
Commands may be abbreviated, Command are:  
open connect to a site  
close close currect connection  
quit exit telnet  
display display operating parameters  
send transmit special characters ('send ?' for more)  
set set operating parameters('set ?' for more)  
status print status information  
toggle toggle operating parameters('toggle ?' for more)  
mode try to enter line-by-line or character-at-a-time mode  
? print help information  
虽然命令很多，甚至还有子命令，但只有一些是常用的。现在介绍以下的几个：  
Close：  
该命令用语终止连接。它自动切断与远程系统的连接，也可以用它退出Telnet，在冒失的进入一个网络主机时，想退出的话，就可以用到这个命令。  
open：  
用它来与一个命名机器连接，要求给出目标机器的名字或IP地址。如果未给出机器名，Telnet就将要你选择一个机器名。必须注意，在使用"Open"命令之前应该先用"close"来关闭任何已经存在的连接。  
Set ECHO：  
用于本地的响应是On或是Off。作用是是否把输出的内容显示在屏幕上。和DOS的ECHO基本上是一样。如果机器是处于ECHO ON的话，想改变为OFF，那么就可以输入SET ECHO,想再改变回ECHO OFF，那么就再键入SET ECHO就可以了。(这儿说的比较简短,如果有不明白的,可以与我联系)  
Set escape char:  
建立"escape"字符到某个特殊的符号，若想用某种控制符号来代替，可以用"asis"或者键入符号"^"加字母b(如：^b）。在正常工作时，是不需要用"escape"这个字符的，并且这个被用作"escape"的符号不应该再被使用。这类似于许多程序中对键盘上的每一个键设定其真正的涵义。但如果正在运行一个 daisy-chained 应用系统，那么可以重新议定"escape"字符的特征便是很有用的。例如：用Telnet从系统A到系统B，接着又用Telnet注册进入系统C。如果正在系统C上工作时出了故障，那么当"escape"代表符是相同时，就没法中断系统B到系统C的连接。键入"escape"代表符，将总是处于系统A的命令模式。如果在每个Telnet部分使用不同的"escape"代表符，便可以通过键入适当的符号，来选择其中一个命令模式，这也可以用于其他的应用中（像终端仿真）。  
Quit:  
用它可顺利地推出Telnet程序。  
Z:  
用语保留Telnet但暂时回到本地系统执行其他命令。并且在Telnet中的连接以及其他的选择在Telnet恢复时仍被保留。  
Carriage Return:  
用于不具体的一个命令从命令模式返回到所连接的远程机器上。另外，还有许多其他的命令可以推出命令模式。下面举一个例子，是从注册进入到porky.math.ukans.edu ,然后进入命令模式，然后返回porky::  
telnet porky.math.ukans.edu  
Trying 129.237.128.11...  
Connected to porky.math.ukans.edu.  
Escape character is '^]'.  
SunOS UNIX(porky)  
login:wl  
password:  
Last Login: Tue Mar 28 05:35 from ns.bta.net.cn  
SunOS Release 4.1.3\_U1(SLIPPERY1) #3: Sun Nov 20 23:47:23 CST 1999  
No match.  
if:Expression syntax.  
porky/serv/wl%cd/  
porky/%CTRL-]  
telnet:?  
Commands may be abbreviated, Command are:  
open connect to a site  
close close currect connection  
quit exit telnet  
display display operating parameters  
send transmit special characters ('send ?' for more)  
set set operating parameters('set ?' for more)  
status print status information  
toggle toggle operating parameters('toggle ?' for more)  
mode try to enter line-by-line or character-at-a-time mode  
? print help information  
telnet:set escape ^b  
escape character is ’^b’  
porky/%logout  
ns.bta.net.cn%  
注意：set命令也可以退出命令模式。当然，如果不行，可以回车输入一空行，也能回到porky。

NETSTAT命令详解  
netstat命令是一个监控TCP/IP网络的非常有用的工具，它可以显示路由表、实际的网络连接以及每一个网络接口设备的状态信息，在我的计算机上执行netstat后，其输出结果为：   
Active Internet connections (w/o servers)   
Proto Recv-Q Send-Q Local Address Foreign Address State   
tcp 0 2 210.34.6.89:telnet 210.34.6.96:2873 ESTABLISHED   
tcp 296 0 210.34.6.89:1165 210.34.6.84:netbios-ssn ESTABLISHED   
tcp 0 0 localhost.localdom:9001 localhost.localdom:1162 ESTABLISHED   
tcp 0 0 localhost.localdom:1162 localhost.localdom:9001 ESTABLISHED   
tcp 0 80 210.34.6.89:1161 210.34.6.10:netbios-ssn CLOSE   
Active UNIX domain sockets (w/o servers)   
Proto RefCnt Flags Type State I-Node Path   
unix 1 [ ] STREAM CONNECTED 16178 @000000dd   
unix 1 [ ] STREAM CONNECTED 16176 @000000dc   
unix 9 [ ] DGRAM 5292 /dev/log   
unix 1 [ ] STREAM CONNECTED 16182 @000000df   
从整体上看，netstat的输出结果可以分为两个部分，一个是Active Internet connections，称为有源TCP连接，另一个是Active UNIX domain sockets，称为有源Unix域套接口。在上面的输出结果中，第一部分有5个输出结果，显示有源TCP连接的情况，而第二部分的输出结果显示的是Unix域套接口的连接情况。Proto显示连接使用的协议；RefCnt表示连接到本套接口上的进程号；Types显示套接口的类型；State显示套接口当前的状态；Path表示连接到套接口的其它进程使用的路径名。   
事实上，netstat是若干个工具的汇总。   
◆ 显示路由表   
在随- r标记一起调用n e t s t a t时，将显示内核路由表，就像我们利用r o u t e命令一样。产生的输出如下：   
[root@machine1 /]$ netstat -nr   
Kernel IP routing table   
Destination Gateway Genmask Flags MSS Window irtt Iface   
210.34.6.0 0.0.0.0 255.255.255.128 U 0 0 0 eth0   
192.168.1.0 0.0.0.0 255.255.255.0 U 0 0 0 eth1   
127.0.0.0 0.0.0.0 255.0.0.0 U 0 0 0 lo   
0.0.0.0 210.34.6.2 0.0.0.0 UG 0 0 0 eth0   
- n 选项令netstat以点分四段式的形式输出IP地址，而不是象征性的主机名和网络名。如果想避免通过网络查找地址（比如避开DNS或NIS服务器），这一点是特别有用的。   
netstat输出结果中，第二列展示的是路由条目所指的网关，如果没有使用网关，就会出现一个星号（\*）或者0.0.0.0；第三列展示路由的概述，在为具体的I P地址找出最恰当的路由时，内核将查看路由表内的所有条目，在对找到的路由与目标路由比较之前，将对I P地址和genmask进行按位“与”计算；第四列显示了不同的标记，这些标记的说明如下：   
■ G 路由将采用网关。   
■ U 准备使用的接口处于“活动”状态。   
■ H 通过该路由，只能抵达一台主机。   
■ D 如果路由表的条目是由ICMP重定向消息生成的，就会设置这个标记。   
■ M 如果路由表条目已被ICMP重定向消息修改，就会设置这个标记。   
netstat输出结果的Iface显示该连接所用的物理网卡，如eth0表示用第一张，eth1表示用第二张。   
◆ 显示接口特性   
在随- i标记一起调用时， netstat将显示网络接口的当前配置特性。除此以外，如果调用时还带上-a选项，它还将输出内核中所有接口，并不只是当前配置的接口。netstat-i的输出结果是这样的：   
[root@machine1 /]$ netstat -i   
Kernel Interface table   
Iface MTU Met RX-OK RX-ERR RX-DRP RX-OVR TX-OK TX-ERR TX-DRP TX-OVR Flg   
eth0 1500 0 787165 0 0 1 51655 0 0 0 BRU   
eth1 1500 0 520811 0 0 0 1986 0 0 0 BRU   
lo 3924 0 1943 0 0 0 43 0 0 0 LRU   
MTU和Met字段表示的是接口的MTU和度量值值；RX和TX这两列表示的是已经准确无误地收发了多少数据包（ RX - OK / TX - OK）、产生了多少错误（ RX-ERR/TX-ERR）、丢弃了多少包（RX-DRP/TX-DRP），由于误差而遗失了多少包（RX-OVR/TX-OVR）；最后一列展示的是为这个接口设置的标记，在利用ifconfig显示接口配置时，这些标记都采用一个字母。它们的说明如下：   
■ B 已经设置了一个广播地址。   
■ L 该接口是一个回送设备。   
■ M 接收所有数据包（混乱模式）。   
■ N 避免跟踪。   
■ O 在该接口上，禁用A R P。   
■ P 这是一个点到点链接。   
■ R 接口正在运行。   
■ U 接口处于“活动”状态。   
◆ 显示链接   
netstat支持用于显示活动或被动套接字的选项集。选项- t、- u、- w和- x分别表示TCP、UDP、RAW和UNIX套接字连接。如果你另外还提供了一个- a标记，还会显示出等待连接（也就是说处于监听模式）的套接字。这样就可以得到一份服务器清单，当前所有运行于系统中的所有服务器都会列入其中。   
调用netstat -ta时，输出结果如下：   
[root@machine1 /]$ netstat -ta   
Active Internet connections (servers and established)   
Proto Recv-Q Send-Q Local Address Foreign Address State   
tcp 0 2 210.34.6.89:telnet 210.34.6.96:2873 ESTABLISHED   
tcp 0 0 210.34.6.89:1165 210.34.6.84:netbios-ssn ESTABLISHED   
tcp 0 0 localhost.localdom:9001 localhost.localdom:1162 ESTABLISHED   
tcp 0 0 localhost.localdom:1162 localhost.localdom:9001 ESTABLISHED   
tcp 0 0 \*:9001 \*:\* LISTEN   
tcp 0 0 \*:6000 \*:\* LISTEN   
tcp 0 0 \*:socks \*:\* LISTEN   
tcp 0 80 210.34.6.89:1161 210.34.6.10:netbios-ssn CLOSE   
上面的输出表明部分服务器处于等待接入连接状态。利用- a选项的话，netstat还会显示出所有的套接字。注意根据端口号，可以判断出一条连接是否是外出连接。对呼叫方主机来说，列出的端口号应该一直是一个整数，而对众所周知服务（well known service）端口正在使用中的被呼叫方来说，netstat采用的则是取自/etc/services文件的象征性服务名

点击加载更多

金榜VIP已享免费阅读及下载

加载失败，请重试

打开百度APP阅读全文

立即领取

VIP教育大礼包

热门小说免费读

本文配套内容

含${item.docNum}篇文档

${item.title}

￥**${item.price}**

立即购买

查看文集

### 精品课程

* ${item.title}
* 免费 ￥${item.price}￥${item.oriPrice} ￥${item.oriPrice} ${item.orgName}
* ${item.videoCount}课节

相关推荐文档

* ${searchSpecial.title}
* ${v.docTitle}
* *推荐* *热门* *好评*
* 用App查看
* 打开百度APP

返回百度搜索

下载原文档，方便随时阅读

下载文档

## 2亿文档资料库

涵盖各行课件、资料、模板、题库、报告等

## 多种记录存储好工具

提供图转文字、拍照翻译、语音速记等

## APP端内容永久保存

随时阅读，多端同步

立即下载

看视频广告，获取20元代金券礼包

看视频，立领券 视频大小约3.7M

您是老用户，送您2张代金券

* 5元
* 适用除连续包月外的其他VIP
* 24小时内有效
* 10元
* 限百度文库VIP-12个月适用
* 24小时内有效

领取优惠券

您已成功领取老用户福利

已转存到百度网盘

存储在文件夹【来自：百度文库】

去看看

文库新人专享礼包

限时免费

价值¥500+

去文库APP免费领