DOS命令之net命令详细解释

[DOS命令](https://www.lmdouble.com/tag/dos%e5%91%bd%e4%bb%a4)之[net](https://www.lmdouble.com/tag/net)命令详细解释

net命令是一个[cmd命令](https://www.lmdouble.com/tag/cmd%e5%91%bd%e4%bb%a4)行命令，net 命令有很多函数用于实用和核查计算机之间的NetBIOS连接，可以查看我们的管理网络环境、服务、用户、登陆等信息内容，是一个非常实用的cmd命令，要想获得net的HELP可以通过以下两种方式获取：

(1)在Windows下可以用图形的方式，开始->帮助->索引->输入net；

(2)在COMMAND下可以用字符方式：net /?或net或net help取得相应的方法的帮助。所net命令接受选项/yes和/no(可缩写为/y和/n)。

## net详细命令解释

net use \\ip\\ipc$ " " /user:" " ------建立IPC空链接,注意：ip是192.168.xx.xx不能是127.0.0.1

net use \\ip\\ipc$ "密码" /user:"用户名" ------ 建立IPC非空链接

net use h: ipc$ "密码" /user:"用户名" ------直接登陆后映射对方C：到本地为H:

net use h: ipc$ ------登陆后映射对方C：到本地为H:

net use ipipc$ /del ------删除IPC链接

net use h: /del ------删除映射对方到本地的为H:的映射

net user 用户名　密码　/add ------建立用户

net user用户名 /del --------删除用户

net user guest /active:yes ------激活guest用户

net user ------查看有哪些用户

net user ------帐户名 查看帐户的属性

net localgroup administrators 用户名 /add ------把“用户”添加到管理员中使其具有管理员权限,注意：administrator后加s用复数

net start ------查看开启了哪些服务

net start 服务名　 ------开启服务；(如:net start telnet， net start schedule)

net stop 服务名 ------停止某服务

net time 目标ip ------查看对方时间

net time 目标ip /set ------设置本地计算机时间与“目标IP”主机的时间同步,加上参数/yes可取消确认信息

net view ------查看本地局域网内开启了哪些共享

net view ip ------查看对方局域网内开启了哪些共享

net config ------显示系统网络设置

net logoff ------断开连接的共享

net pause ------服务名 暂停某服务

(net send ip ------"文本信息" 向对方发信息 注意)XP版本之后的windows已经没有net send命令了)

net share ------查看本地开启的共享

net share ipc$ ------开启ipc$共享

net share ipc$ /del ------删除ipc$共享

net share c$ /del ------删除C：共享

net share hao$=d: 将d盘共享并且名称为hao$

net user guest 12345 ------用guest用户登陆后用将密码改为12345

net password ------密码 更改系统登陆密码

netstat -a ------查看开启了哪些端口,常用netstat -an

netstat -n ------查看端口的网络连接情况，常用netstat -an

netstat -v ------查看正在进行的工作

netstat -p 协议名 ------例：netstat -p tcq/ip 查看某协议使用情况（查看tcp/ip协议使用情况）

netstat -s ------查看正在使用的所有协议使用情况

net use H: \\192.168.1.20\downloads /user:admin p@ssword

net use \* /d

## net部分命令使用示例

### 1. 建立空连接:

net use \\IP\ipc$ "" /user:"" (一定要注意:这一行命令中包含了3个空格)

## 2. 建立非空连接:

net use \\IP\ipc$ "密码" /user:"用户名" (同样有3个空格)

## 3. 映射默认共享:

net use z: \\IP\c$ "密码" /user:"用户名" (即可将对方的c盘映射为自己的z盘，其他盘类推)

如果已经和目标建立了ipc$，则可以直接用IP+盘符+$访问,具体命令 net use z: [\\IP\c$](file:///\\IP\c$)

net use z: [\\DESKTOP-VMVH8D4\f$](file:///\\DESKTOP-VMVH8D4\f$) 将网络共享f$映射为本地z:盘

## 4. 删除一个ipc$连接

net use \\IP\ipc$ /del

### 5. 删除共享映射

net use c: /del 删除映射的c盘，其他盘类推

net use \* /del 删除全部,会有提示要求按y确认

6. 查看远程主机的共享资源（但看不到默认共享）

net view \\IP

### 7. 查看本地主机的共享资源（可以看到本地的默认共享）

net share

### 7.1 开启一个共享

net share f$=f: ## 将f盘共享为f$

net share f=F: ## 将f盘共享为f

### 8. 得到本地主机的用户列表

net user

9.  查看远程主机的当前时间

net time \\IP

### 10. 显示本地主机当前服务

net start

### 11. 启动/关闭本地服务

net start 服务名 /y

net stop 服务名 /y

### 12. 映射远程共享:

net use z: \\IP\baby

此命令将共享名为baby的共享资源映射到z盘

### 13. 删除共享映射

net use c: /del 删除映射的c盘，其他盘类推

net use \* /del /y删除全部

### 14. 激活用户/加入管理员组

net user account /active:yes 那么禁用一个账户的命令是net user 用户名 /active:no

net localgroup administrators account /add 将用户加入管理员组

net localgroup administrators account /del 将用户从管理员组删除

net localgroup 查看本地组信息

### 15. 删除一个已建立的ipc$连接

net use \\IP\ipc$ /del

在使用过程中可能会出现一些错误，可以根据返回的错误号分析原因：

错误号5，拒绝访问：很可能你使用的用户不是管理员权限的，先提升权限；

错误号51，Windows无法找到网络路径：网络有问题；

错误号53，找不到网络路径：ip地址错误；目标未开机；目标lanmanserver服务未启动；目标有防火墙（端口过滤）；

错误号67，找不到网络名：你的lanmanworkstation服务未启动或者目标删除了ipc$；

错误号1219，提供的凭据与已存在的凭据集冲突：你已经和对方建立了一个ipc$，请删除再连；

错误号1326，未知的用户名或错误密码：原因很明显了；

错误号1792，试图登录，但是网络登录服务没有启动：目标NetLogon服务未启动；

实战应用：[通过net 命令绕过Windows登录密码](https://www.lmdouble.com/004943150.html)

# 实战：

## 用cmd命令查看端口占用处理，付命令解析

1、查看所有被占用的端口。net网络、stat统计

**netstat -ano**

        a：显示所有连接和[监听](https://so.csdn.net/so/search?q=%E7%9B%91%E5%90%AC&spm=1001.2101.3001.7020)端口

        n：以数字形式显示地址和端口号

        o：显示与每个连接相关的所属进程 ID

2、过滤所有符合要求的端口。|就是[通道](https://so.csdn.net/so/search?q=%E9%80%9A%E9%81%93&spm=1001.2101.3001.7020)的意思，过滤掉无用的不符合要求的。端口号左右可以加双引号。

**netstat -ano | findstr 端口号**

3、查看端口所属进程

**tasklist 进程pid**

4、杀掉对应的进程。task任务、kill杀掉。查看命令帮助输入taskkill /?

**taskkill -f -t -im xxx.exe**

          -f：强制终止进程

          -t：终止指定的进程和由他启动的子进程

          -im：指定要终止的进程的映像名称

# Taskkill的用法

# askkill



适用范围：Windows Server 2022、Windows Server 2019、Windows Server 2016、Windows Server 2012 R2、Windows Server 2012

结束一个或多个任务或进程。 可以通过进程 ID 或图像名称结束进程。 可以使用 [tasklist](https://learn.microsoft.com/zh-cn/windows-server/administration/windows-commands/tasklist) 命令来确定要结束的进程的进程 ID (PID)。

**备注**

该命令替换 kill 工具。

## 语法

复制

taskkill [/s <computer> [/u [<domain>\]<username> [/p [<password>]]]] {[/fi <filter>] [...] [/pid <processID> | /im <imagename>]} [/f] [/t]

### 参数

| **参数** | **说明** |
| --- | --- |
| /s <computer> | 指定远程计算机的名称或 IP 地址（请勿使用反斜杠）。 默认为本地计算机。 |
| /u <domain>\<username> | 使用 <username> 或 <domain>\<username> 指定的用户的帐户权限运行该命令。 仅当还指定了 /s 时，才能指定 /u 参数。 默认值是当前登录到发出该命令的计算机的用户的权限。 |
| /p <password> | 指定 /u 参数中指定的用户帐户的密码。 |
| /fi <filter> | 应用筛选器以选择一组任务。 可以使用多个筛选器或使用通配符 (\*) 指定所有任务或映像名称。 本文的“筛选器名称、运算符和值”部分列出了有效的筛选器。 |
| /pid <processID> | 指定要终止的进程的进程 ID。 |
| /im <imagename> | 指定要终止的进程的映像名称。 使用通配符 (\*) 指定所有映像名称。 |
| /f | 指定强制结束进程。 对于远程进程，将忽略此参数；所有远程进程都会被强制结束。 |
| /t | 结束指定的进程及其启动的任何子进程。 |

#### 筛选器名称、运算符和值

| **筛选器名称** | **有效运算符** | **有效值** |
| --- | --- | --- |
| 状态 | eq、ne | RUNNING | NOT RESPONDING | UNKNOWN |
| IMAGENAME | eq、ne | 映像名称 |
| PID | eq、ne、gt、lt、ge、le | PID 值 |
| SESSION | eq、ne、gt、lt、ge、le | 会话号 |
| CPUtime | eq、ne、gt、lt、ge、le | 采用 HH:MM:SS 格式的 CPU 时间，其中 MM 和 SS 介于 0 到 59 之间，HH 是任何无符号数字 |
| MEMUSAGE | eq、ne、gt、lt、ge、le | 内存使用量 (KB) |
| USERNAME | eq、ne | 任何有效的用户名（<user> 或 <domain\user>） |
| 服务 | eq、ne | Service name |
| WINDOWTITLE | eq、ne | 窗口标题 |
| MODULES | eq、ne | DLL 名称 |

## 注解

* 指定远程系统时，不支持 WINDOWTITLE 和 STATUS 筛选器。
* 只有在应用筛选器时，\*/im 选项才接受通配符 (\*)。
* 无论是否指定了 /f 选项，总是强制执行结束远程进程的操作。
* 向主机名筛选器提供计算机名称会导致关闭，从而停止所有进程。

## 示例

若要结束进程 ID 为 1230、1241 和 1253 的进程，请键入：

taskkill /pid 1230 /pid 1241 /pid 1253

如果进程 Notepad.exe 是由系统启动的，要强行结束它，请键入：

taskkill /f /fi "USERNAME eq NT AUTHORITY\SYSTEM" /im notepad.exe

若要结束远程计算机 Srvmain 上映像名称以 note 开头的所有进程，同时使用用户帐户 Hiropln 的凭据，请键入：

taskkill /s srvmain /u maindom\hiropln /p p@ssW23 /fi "IMAGENAME eq note\*" /im \*

若要结束进程 ID 为 2134 的进程及其它启动的任何子进程，但前提是这些进程是由管理员帐户启动的，请键入：

taskkill /pid 2134 /t /fi "username eq administrator"

若要结束进程 ID 大于或等于 1000 的所有进程，无论其映像名称如何，请键入：

taskkill /f /fi "PID ge 1000" /im \*

# taskkill /im xt.exe /f

# 扩展

## 查看一个用户的激活状态：lusrmgr.msc就可以打开一个图形界面程序来查看该用户的是否已经激活