Windows基础命令

一、 DOS命令简介

什么是DOS命令

DOS命令是指操作系统中使用的命令行界面命令，也称为命令提示符（Command Prompt）命令。

DOS命令是在早期的微软DOS操作系统和现代Windows操作系统中使用的命令。

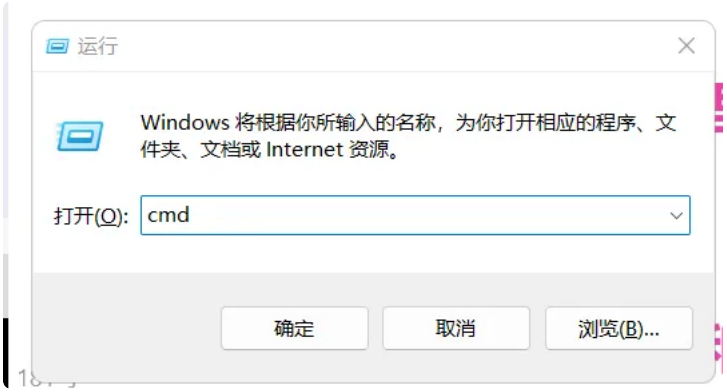
这些命令可以在DOS窗口中直接输入，以控制计算机系统的各种功能。

> DOS 命令行使用的是批处理脚本，其语法相对简单，主要是一系列的命令和参数。用于执行文件操作、管理文件系统、执行简单的系统管理任务等。
>
> PowerShell 使用的是脚本语言，其语法更加强大和灵活，支持变量、条件语句、循环结构、函数等高级编程概念。提供了更强大的功能和丰富的功能库，可以进行系统管理、网络管理、安全

> 管理、任务自动化等各种操作，并且支持.NET Framework，可以调用.NET 类库执行更复杂的操作。

如何操作（使用）DOS命令

Win + R打开运行---输入cmd --回车进入命令提示符窗口



基本命令

1. 命令：color
   作用：改变背景及字体颜色
   color /?

```
C:\Users\lenovo\Desktop>color /?
设置默认的控制台前景和背景颜色。

COLOR [attr]

  attr        指定控制台输出的颜色属性。

颜色属性由两个十六进制数字指定 -- 第一个
对应于背景，第二个对应于前景。每个数字
可以为以下任何值:

    0 = 黑色       8 = 灰色
    1 = 蓝色       9 = 淡蓝色
    2 = 绿色       A = 淡绿色
    3 = 浅绿色     B = 淡浅绿色
    4 = 红色       C = 淡红色
    5 = 紫色       D = 淡紫色
    6 = 黄色       E = 淡黄色
    7 = 白色       F = 亮白色

如果没有给定任何参数，此命令会将颜色还原到 CMD.EXE 启动时
的颜色。这个值来自当前控制台
窗口、/T 命令行开关或 DefaultColor 注册表
值。

如果尝试使用相同的
前景和背景颜色来执行
 COLOR 命令，COLOR 命令会将 ERRORLEVEL 设置为 1。

示例: "COLOR fc" 在亮白色上产生淡红色
```

2. 命令：cls

   作用：清屏

```
C:\Users\lenovo\Desktop>cls
```

二、常用DOS命令

1 、文件和目录相关命令

```
1. 命令:dir
作用：浏览当前文件夹的内容（带<dir>标识的为文件夹，否则为文件）
其他用法：
dir 要浏览的路径

dir d:\
dir d:\pic
dir /a   #浏览所有内容，包括隐藏内容
dir /s /a #列出指定目录下的所有文件和子目录，包括隐藏文件和系统文件。

2. 命令：盘符:
作用：切换分区，如：c: d:   e:

3. 命令：cd 文件夹名
作用：进入文件夹
cd..  #退出一级目录
相对路径：针对当前路径有效，如：...\456   绝对路径：从根开始写路径,如：\123\345
cd \  #直接退到根目录
cd /d D:\ #改变当前目录的同时，切换到指定的磁盘分区。

4. Tab键：补全路径功能

5. 命令：md 文件夹 [文件夹 文件夹.....]
作用：创建新的目录
.表示在当前目录；\a 表示在当前目录下创建一个名为 a 的文件夹
md .\a
md .\a\b\c

6. 命令：rd 文件夹 [文件夹 文件夹.....]
作用：删除空文件夹
命令：rd 文件夹 /s /q
rd：删除文件夹（Remove Directory）的命令。用于删除指定的文件夹。
文件夹：这是要删除的目标文件夹的名称或路径。
/s：表示删除指定目录下的所有文件和子文件夹。如果不加 /s 参数，rd 命令只能删除空文件夹。
/q：表示在删除文件夹时不要显示任何确认提示。通常在批处理脚本中使用 /q 参数，以避免用户确认。
作用：无提示删除非空文件夹

7. 创建文件方法：
echo 字符串 > [路径\]文件名.扩展名

注释：>>和>都可以将命令的输出内容输入到某文件中，若文件不存在，则同时创建该文件
   >>为追加
   >为覆盖

```

```
案例：修改hosts文件
echo 1.1.1.1 www.baidu.com >>c:\windows\system32\drivers\etc\hosts

8. 命令：type 文件名.扩展名
作用：浏览一个文件的内容，也可用于创建空的文本文件
type 1111>test.txt

9. 命令：more 文件名.扩展名
作用：逐屏的显示文本文件内容

10. 命令：findstr 要搜索的内容 文件名.扩展名
作用：在文件中搜索字符串
findstr "a" test.txt #搜索test.txt文件中包含字符 "a" 的行
findstr "^a" test.txt #搜索test.txt文件中以字符 "a" 开头的行
findstr "a$" test.txt #搜索test.txt文件中以字符 "a" 结尾的行

11. 符号：&
作用：顺序执行多条命令，而不管命令是否执行成功
D: & md test #先将工作目录切换到D盘根目录，然后创建目录test

12. 符号：&&
作用：顺序执行多条命令，当碰到执行出错的命令后将不执行后面的命令
findstr "hello" test.txt && echo 成功找到 #在当前目录下的 test.txt 文件中查找 "hello" 字样，如果找到就显示 "hello 成功找到" ，找不到就不显示任何内容（需要保证当前目录下存在test.txt文件）

13. 符号：||
作用：顺序执行多条命令，当碰到执行正确的命令后将不执行后面的命令
findstr "hello" test.txt || echo 未找到

14. 符号：|
作用：将第一个命令的输出结果作为第二个命令的操作对象
dir C:\windows | more #列出目录 C:\windows 下的内容，然后分页显示

15. 命令：del 文件名.扩展名
作用：删除文件
del test #删除当前目录下的test文件夹中的所有非只读文件
del *.txt #删除所有txt结尾的文件
del . #删除所有文件
del . /s /q #无提示删除所有文件
注：*为通配符，代表任意字符，任意长度

16. 命令：attrib 属性 文件名.扩展名
作用：显示或更改文件属性
attrib +r 文件全名/文件夹名 #添加只读属性
注释：+改为-为取消修改文件属性
```

```
17. 命令：copy [路径]源文件全名 目标路径[\新文件全名]
作用：将一份或多份文件复制到指定位置
copy c:\Users\Administrator\Desktop\test.txt d:\dir\test.txt
copy C:\Users\Administrator\Desktop\*.txt d:\dir
注释：复制目录时应使用xcopy命令

18. 命令：xcopy 源目录 目标目录 /e /i /h /s
作用：将一个目录及其所有子目录和文件复制到另一个目录中
/e：表示复制目录及其所有子目录和文件，包括空目录；
/s：表示复制目录及其所有子目录和文件，但不包括空目录。
/i：如果目标目录不存在，会先提示是否创建目标目录；
/h：表示复制隐藏文件；
xcopy /s test1 test2 #复制目录和子目录，但是不包括空目录
xcopy /e test1 test2 #复制目录和子目录，包括空目录
xcopy /e /i /h phpStudy test\phpStudy

19. 命令：move [路径]源文件全名 目标路径[\新文件全名]
作用：移动文件并重命名文件和目录，但不可以跨分区移动文件夹

20. 命令：ren 文件名或目录名 要修改成的文件名或目录名
作用：文件或目录重命名
```

2、网络操作命令

```
1. ipconfig
作用：显示当前设备的IP配置信息。
命令格式：ipconfig [参数]
常用参数：
/all #显示详细的IP配置信息
/release #释放指定适配器的IPv4地址
/renew #更新指定适配器的IPv4地址
示例：
ipconfig /all #显示详细的IP配置信息
ipconfig /release #释放所有适配器的IPv4地址
ipconfig /renew #更新所有适配器的IPv4地址

2. ping
作用：检查网络连接，测试网络延迟。
命令格式：ping [参数] 目标主机
常用参数：
-n count #发送指定次数的回显请求
-t #持续发送回显请求直到手动停止
示例：
ping www.baidu.com #向www.google.com发送4次回显请求
ping -n 10 www.baidu.com #向www.google.com发送10次回显请求
ping -t www.baidu.com #持续向www.google.com发送回显请求

3. tracert
在跟踪路由时允许的最大跳数或路由器的最大数量。换句话说，
它规定了跟踪到目标主机的最大网络跃点数。当 tracert 命令在网络中追踪路由时，
每经过一个网络节点或路由器，就会增加一个跃点数。如果达到了最大跃点数，
但目标主机仍未到达，tracert 命令将停止跟踪路由并报告该主机不可达。

作用：跟踪数据包在网络中的路由。
命令格式：tracert [参数] 目标主机
常用参数：
-d #不解析IP地址为主机名
-h maximum_hops #指定最大跳数
示例：
tracert www.google.com #跟踪到www.google.com的路由
tracert -d www.google.com #跟踪到www.google.com的路由，不解析IP地址为主机名
tracert -h 5 www.google.com
#意味着 tracert 命令将跟踪到 www.google.com 的路由，
但最多经过 5 个路由器。如果跟踪超过了 5 个路由器，tracert 命令将停止跟踪并显示结果。

4. netstat
作用：显示网络连接、路由表和网络接口的统计信息。
命令格式：netstat [参数]
常用参数：
-a #显示所有活动连接和监听端口
```

```
-o #显示拥有的与每个连接关联的进程 ID
-b #显示创建连接的可执行文件
-n #以数字形式显示地址和端口号
示例:
netstat -aon #将所有连接的地址和端口号以数字的形式显示，并显示每个连接关联的进程ID

5. nslookup
作用：查询DNS服务器以解析主机名和IP地址。
命令格式：nslookup [参数] [主机名/IP地址]
示例:
nslookup www.google.com #查询www.google.com的IP地址
```

3、系统操作命令

1、 start：启动一个单独的窗口来运行指定的程序或命令。
格式：start [选项] [程序 [参数]]
常用选项：
/d：设置应用程序的启动目录。
/b：在后台启动应用程序，不会显示新窗口。
示例：start /d "C:\Program Files\Internet Explorer" iexplore.exe
示例说明：在 "C:\Program Files\Internet Explorer" 目录下启动 iexplore.exe。

2、 tasklist：显示系统中正在运行的所有任务。
格式：tasklist [选项]
常用选项：
/S：指定远程系统。
/U：指定用户名。
/P：指定密码。
/M：显示加载的DLL模块。
示例：tasklist /S remotePC /U username /P password
示例说明：显示远程计算机 remotePC 上的任务列表，使用 username 和 password 作为登录凭据。
remotePC 应该替换为你要查询的远程计算机的名称或 IP 地址

3、 taskkill：根据进程ID或进程名称终止任务。
格式：taskkill [选项] [/PID processID | /IM imageName]
常用选项：
/F：强制终止进程。
/T：终止指定进程及其子进程。
/PID：指定要终止的进程的 PID
/IM：通过映象名称终止进程
示例：taskkill /F /IM notepad.exe
示例说明：强制终止名为 notepad.exe 的进程。

4、 shutdown：关闭、重启或注销计算机。
格式：shutdown [选项]
常用选项：
/s：关闭计算机。
/r：重启计算机。
/a：终止系统关闭
/t：设置延迟时间（以秒为单位）。
/f：强制关闭应用程序。
/c：设置一个注释
示例：shutdown /r /t 60
示例说明：在 60 秒后重启计算机。

5、 systeminfo：显示计算机的详细系统信息。
格式：systeminfo [选项]
常用选项：

```
/S：指定远程系统。
/U：指定用户名。
/P：指定密码。
示例：systeminfo /S remotePC /U username /P password
示例说明：显示远程计算机 remotePC 的系统信息，使用 username 和 password 作为登录凭据。

6. 命令：reg
作用：对注册表进行相关操作
/v  表示选项之下要添加的值名
/t  注册表项数据类型
/d  要分配给添加的注册表值的数据
/f  不提示，强行改写现有注册表项
  reg add reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v test /t REG_SZ /d "c:\windows\system32\cmd.exe" /f "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v test /t REG_SZ /d "c:\windows\system32\cmd.exe" /f  # 强制添加一条开机启动cmd的注册表项
  reg delete "hklm\software\microsoft\windows\currentversion\run" /v test /f # 强制删除值名为test的注册表项
  reg add "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters" /v DefaultTTL /t REG_DWORD /d 64 /f  # 强制修改默认TTL值

7.命令：schtasks
作用： Windows 中用于管理计划任务的命令行工具
/create 要创建一个新的任务
/tn 用于指定新任务的名称的选项
/tr 用于指定任务应该运行的程序或脚本的选项
/sc 指定任务的调度方案的选项
/st 指定任务应该在一天中的什么时间开始运行的选项
schtasks /create /tn "InternetExplorerStartTask" /tr %PROGRAM_PATH% /sc daily /st %START_TIME%


8. 命令：netsh advfirewall
作用：设置防火墙
netsh：是一个命令行工具，用于配置和管理 Windows 网络设置
advfirewall：表示高级防火墙，即 Windows 高级防火墙
set：指定要设置的操作
allprofiles：表示所有网络配置文件，包括公用网络、专用网络和域网络。
state off：将防火墙的状态设置为禁用。

例：netsh advfirewall set allprofiles state off  # 关闭所有类型网络的防火墙
例：netsh advfirewall set allprofiles state on   # 开启所有类型网络的防火墙
例：netsh advfirewall firewall add rule name=TCP-In-8888 protocol=TCP localport=8888 dir=in action=allow   #添加名为TCP-In-8888入站规则：允许TCP端口8888


```

```
例：netsh advfirewall firewall add rule name=TCP-In-8888 protocol=TCP localport=8888 dir=in action=block   #添加名为TCP-In-8888入站规则：阻止TCP端口8888

例：netsh advfirewall firewall add rule name=TCP-out-8888 protocol=TCP localport=8888 dir=out action=allow  #添加名为TCP-out-8888出站规则：允许TCP端口8888

例：netsh advfirewall firewall add rule name=TCP-out-8888 protocol=TCP localport=8888 dir=out action=block  #添加名为TCP-out-8888出站规则：阻止TCP端口8888

例：netsh advfirewall firewall add rule name=允许ping protocol=icmpv4 dir=in action=allow # 添加允许ping的规则

例：netsh advfirewall firewall delete rule name=xxx # 删除名为xxx的防火墙规
```

在 Windows 注册表中，每个文件夹代表一个命名空间，用于组织注册表中的键和值。这些文件夹通常称为“项”（Keys），而包含在其中的键则是注册表的分支。下面是一些常见的注册表文件夹及其用途：

1. **HKEY_CLASSES_ROOT**: 也称为 HKCR，包含文件扩展名和 OLE 对象类型的注册信息。它提供了文件扩展名与文件类型、文件图标和关联的应用程序之间的映射。
2. **HKEY_CURRENT_USER**: 也称为 HKCU，包含当前用户的配置信息。这包括了用户的桌面设置、应用程序首选项等信息。
3. **HKEY_LOCAL_MACHINE**: 也称为 HKLM，包含了计算机的全局配置信息。这些信息对于所有用户都是一致的，例如安装的软件信息、硬件配置等。
4. **HKEY_USERS**: 也称为 HKU，包含了系统上每个用户的配置信息。每个用户都有一个对应的子项。
5. **HKEY_CURRENT_CONFIG**: 也称为 HKCC，包含了当前计算机硬件配置的信息，它主要是指向 HKLM\SYSTEM\CurrentControlSet\Hardware Profiles\Current 的一个符号链接。

这些文件夹对于 Windows 操作系统的正常运行和应用程序的配置都非常重要，开发人员和系统管理员通常会通过编辑注册表来进行系统配置和定制。但修改注册表时需要小心，不当的修改可能导致系统不稳定或出现问题。

4、用户与组管理

1、用户概述

- 每一个用户登陆系统后拥有不同的权限。
- 每个账户有自己唯一的SID（安全标识符）

- 用户SID：S-1-5-21-1487092334-3931679330-1155163103-500
- 系统SID：S-1-5-21-1487092334-3931679330-1155163103
- **SID也就是安全标识符（Security Identifiers），是标识用户、组和计算机帐户的唯一的号码。在第一次创建该帐户时，会给帐户发布一个唯一的 SID。如果创建帐户，再删除帐户，然后使用相同的用户名创建另一个帐户，则新帐户将不具有授权给前一个帐户的权力或权限，原因是该帐户具有不同的 SID 号。**

```
• windows系统管理员administrator的UID是500
• 普通用户的UID是1000开始
• 查看当前用户的SID：whoami /user
• 查看所有用户的SID：wmic useraccount get name,sid
• Windows Server系统上，默认密码最长有效期42天
```

2、内置账户

- 给用户使用的账户
  administrator #管理员账户
  guest #来宾账户
- 计算机服务组件相关的系统账号
  system　　#系统账户，权限至高无上 ， 真正意义上的管理账户
  local services　#本地服务账户，权限略小于普通用户 ， 主要负责系统中的一些本地服务，例如音频服务、DHCP客户端服务等
  network services　　#网络服务账户，权限与普通用户相同， 主要负责一些网络相关的服务，例如DNS客户端服务

3、 账户管理命令

```
net user #查看用户列表

net user 用户名 密码 #改密码

net user 用户名 密码 /add #创建一个新用户

net user 用户名 /del #删除一个用户

net user 用户名 /active:yes #激活账户

net user 用户名 /active:no #禁用账户
```

4、组概述

- 组的作用：简化权限的赋予

  组和用户的关系：一个组可以有多个用户、一个用户可以属于多个组

- 常用内置组：内置组的权限默认已经被系统赋予

```
administrators # 管理员组

guests # 来宾组

users # 普通用户组，默认新建用户都属于该组

network # 网络配置组

print # 打印机组

Remote Desktop # 远程桌面组
```

5、组管理命令

```
net localgroup # 查看组列表

net localgroup 组名 # 查看该组的成员

net localgroup 组名 /add # 创建一个新的组

net localgroup 组名 用户名 /add # 添加用户到组

net localgroup 组名 用户名 /del # 从组中踢出用户

net localgroup 组名 /del # 删除组
```