实践3 命令提示符

1. 实践目的

理解命令提示符和环境变量以及二者间的联系，掌握部分命令的使用方法。

2. 实践环境

连入 Internet 的计算机一台，安装 Windows XP，Windows 7 或 Windows 8 等操作系统。

3. 名词解释

(1) **命令提示符**：命令提示符即 cmd. exe，是一个 32 位的命令行程序，微软 Windows 系统基于 Windows(视窗)上的命令解释程序，类似于微软的 DOS 操作系统。

(2) **环境变量**：环境变量一般是指在操作系统中用来指定操作系统运行环境的一些参数，例如临时文件夹位置和系统文件夹位置等。

(3) **目录与路径**：目录也称为文件夹，实际上，一个目录或文件夹就是一个装有数字文件系统的虚拟“容器”，在它里面保存着一组文件和其他一些目录(文件夹)。而用户在磁盘上寻找文件时，所历经的目录(文件夹)线路叫路径。

(4) **快捷方式**：快捷方式是 Windows 提供的一种快速启动程序、打开文件或文件夹的方法。它是应用程序的快速连接。快捷方式的一般扩展名为 lnk，并且快捷方式的图标左下角都有一个非常小的箭头。双击快捷方式就打开了这个快捷方式所指向的应用程序。

(5) **批处理**：顾名思义，批处理就是对某对象进行批量的处理。而 DOS 批处理则是基于 DOS 命令的，用来自动地批量地执行 DOS 命令以实现特定操作的脚本，扩展名为 bat。

4. 预备知识

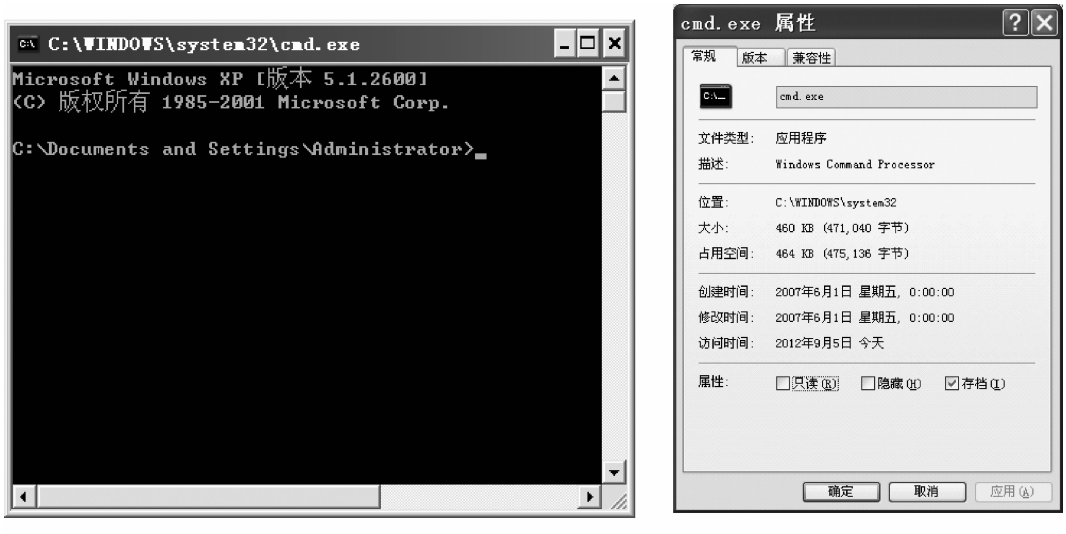
1) 命令解释程序

cmd. exe 是微软 Windows 系统基于 Windows(视窗)上的命令解释

程序，不是纯粹的系统程序，但是如果删除它，可能会导致不可知的问题。文件位置为*:\Windows\System32\cmd.exe。

cmd.exe是Windows的“标配”组件，它可以实现用户与操作系统的直接交流，并负责用户输入的所有命令的解释和支持，特点是运行快捷、安全、稳定，部分特殊功能在图形界面下是没有或难以完成的，因此cmd.exe是专业人士常用的工具。

打开方式：选择“开始”→“运行”，输入cmd，单击“确定”按钮(Vista或Windows 7的运行默认没有，调出来用“开始”→“属性”，或按Win+R键，然后输入cmd，或选择“开始”→“程序”→“附件”→“命令提示符”。cmd.exe启动后默认是黑底白字，如图3-1(a)所示，可以用color命令修改其背景或文字的颜色。cmd.exe窗口首先显示当前系统的版本和版权声明，然后显示当前默认路径是C:\Documents and Settings\Administrator>，即登录用户账户所在的文件夹，而Windows 7下是C:\Users\Administrator>。cmd.exe文件属性如图3-1(b)所示，显示文件位置、大小、创建时间、修改时间等信息，如有不同则有可能存在安全问题。



(a) (b)

图3-1 cmd.exe窗口及文件属性

cmd常用命令在C:\WINDOWS\system32目录下，命令用法如下。

(1) cd：路径的切换。

【例3-1】 执行E盘下文件夹demo中子文件夹test下的do.exe程序。

解答：

```
C:\Documents and Settings\Administrator>E:
E:\>cd demo\test
E:\demo\test>do 回车
```

或不改变当前路径，直接输入：

```
C:\Documents and Settings\Administrator>E:\demo\test\do  回车
```

另外“cd..”回到上级目录,“cd\”回到当前根目录。

(2) dir:显示目录中的文件和子目录列表。

```
C:\Documents and Settings\Administrator>dir 不显示隐藏文件夹和文件
C:\Documents and Settings\Administrator>dir /A 显示所有文件夹和文件
```

输出显示中:<DIR>表示是目录(文件夹),如果是文件则显示其大小,另外 dir 可以指定显示类型、格式和时间信息等。指定类型:/A:D 为目录;/A:R 为只读文件;/A:H 为隐藏文件;/A:A 为准备存档的文件;/A:S 为系统文件;符号“-”表示“否”的前缀,如“dir /A:-d”表示只显示文件。

(3) fsutil:Windows 下的一个强大的命令,可用于执行多种与 FAT 和 NTFS 文件系统相关的任务。典型用法如下。

① 获得各个驱动器盘符。

```
>fsutil fsinfo drives
    驱动器: C:\ D:\ E:\ F:\ G:\ H:\ I:\
```

② 创建一个大小为 300 字节的 new.txt。

```
>fsutil file createnew new.txt 300
```

(4) del (erase):删除指定文件。语法:

```
del [Drive:][Path]FileName[ …][/p] [/f] [/s] [/q] [/a[:attributes]]
```

其中,参数[Drive:][Path] FileName 指定要删除的文件或文件集的位置和名称,需要 Filename。可以使用多个文件名,用空格、逗号或分号分开文件名。典型用法如下。

【例 3-2】 要删除驱动器 C:\上名为 test 文件夹中的所有文件。

解答:

```
>del c:\test
```

或

```
>del c:\test\*.*
>del *.txt
```

删除 *.txt 文件。

```
>del /a /f/q c:\test
```

在静音模式下(不提示确认删除)删除 test 文件夹中的所有文件。

(5) MD：创建目录。RD ：删除目录。

【例 3-3】 在 E 盘下创建\test1\\test2\test3\test4 目录，其中 test1 不存在。

解答：

```
MD E:\test1\\test2\test3\test4
```

【例 3-4】 在静音模式下删除 E 盘下 test1 文件夹及其所有子文件夹及文件。

解答：

```
RD/q/s E:\test1
```

其中，/s 除目录本身外，还将删除指定目录下的所有子目录和文件，用于删除目录树；/q 表示安静模式。

(6) cacls：显示或修改文件的访问控制列表(ACL)。语法：

```
cacls FileName  [/t] [/e] [/g User:permission] [/r User [ … ]] [/p User:permission [ … ]] [/d
User [ … ]]
```

- /t：更改当前目录和所有子目录中指定文件的 ACL。
- /e：编辑 ACL，而不是替换它。
- /g User:permission：将访问权限授予指定用户。
- /p User:permission 替代指定用户的访问权限。包括：n 表示无，r 表示读取，w 表示写入，c 表示更改(写入)，F 表示完全控制。
- /r User：取消指定用户的访问权限。
- /d User：拒绝指定用户的访问。

【例 3-5】 禁止 guests 组用户使用 cmd.exe，再解禁。

解答：

```
cacls c:\windows\system32\cmd.exe /e /d guests  (禁止)
cacls c:\windows\system32\cmd.exe /e /r guests  (解禁)
```

(7) echo：打开回显或关闭请求回显功能。

当 echo 设置 off 值的时候，表示下面的指令都将只执行而不显示，当再次出现 echo on 时下面的语句才为可见的(回显)。

```
echo aaaaa > a.txt
```

即可将本在显示器上显示的信息 aaaaa 输出到文件 a.txt 中。如果文件 a.txt 本来已经存在，该命令将首先擦除 a.txt 中的所有信息，然后写入信息 aaaaa；若 a.txt 本来就不存在，该命令即可新建一个 a.txt 文件，并写入信息 aaaaa。

```
echo aaaaa >> a.txt
```

类似于“echo aaaaa＞a.txt”。区别在于，如果 a.txt 本已存在，“＞a.txt”会擦除 a.txt 中的原有内容，而“＞＞a.txt”并不擦除原有内容，仅在 a.txt 文件的末尾添加信息 aaaaa。a.txt 不存在时，二者没有差别。

(8) ATTRIB：显示或更改文件属性。语法：

```
ATTRIB [+R|-R][+A|-A][+S|-S][+H|-H][[drive:][path][filename]
```

“＋”表示设置属性，“－”表示清除属性，“R”表示只读文件属性，“A”表示存档文件属性，“S”表示系统文件属性，“H”表示隐藏文件属性。

【例 3-6】 将 E 盘 test 文件夹的属性设置为隐藏和系统。

解答：

```
attrib +h +s E:\test
```

2) 环境变量

环境变量是一个具有特定名字的对象，它包含了一个或者多个应用程序所将使用到的信息。例如 path，当要求系统运行一个程序而没有告诉它程序所在的完整路径时，系统除了在当前目录下面寻找此程序外，还应到 path 中指定的路径去找。用户通过设置环境变量可更好地运行进程。打开“我的电脑”的右键快捷菜单，选择“属性”→“高级”→“环境变量”。环境变量分为两类：用户变量与系统变量，在注册表中都有对应的项。

(1) 用户变量所在位置：HKEY_CURRENT_USER\Environment。

(2) 系统变量所在位置为：HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SessionManager\Environment。

某台计算机上 Path 的示例：

```
Path = {%systemroot%\system32;%systemroot%;%systemroot%\system32\wbem; c:\
programfiles\common files\thunder network\kankan\codecs;c:\program files\microsoft sql
server\90\tools\binn\;c:\opencv2.1\vc2008\bin;%JAVA_HOME%/bin;%JAVA_HOME%/jre/bin ;
C:\Program Files\Common Files\Autodesk Shared\;E:\WinDDK}
```

常见环境变量：

(1) %USERNAME%：返回当前登录的用户名称。

(2) %UserProfile%：返回当前用户的配置文件的位置。

(3) %WINDIR%：返回操作系统目录的位置。

(4) %OS%：返回操作系统的名称。

(5) %SYSTEMROOT%：返回 Windows 根目录的位置。

命令行查看方法：

```
>echo %USERNAME%
```

3) 批处理

批处理(Batch)，也称为批处理脚本。顾名思义，批处理就是对某对象进行批量的处理。

批处理文件的扩展名为.bat。

【例 3-7】 在这个例子中,驱动器 G 中磁盘上的所有文件均复制到 d:\back 中。显示的注释提示将另一张光盘放入驱动器 G 时,pause 命令会使程序挂起,以便更换光盘,然后按任意键继续处理。代码如下所示。

```
@echo off
:begin
copy G:*.* d:\back
echo 请插入另一张光盘…
pause
goto begin
```

5. 实践操作及步骤

1) cmd 命令的使用

【例 3-8】 在 D 盘下新建一个文件夹“test”,将 notepad.exe 复制到文件夹 test 中操作步骤如下。

(1) 打开 cmd。

(2) 输入“cd /d D:\”,将当前目录改成 D 盘。

(3) 输入“md test”,在当前目录创建一个 test 文件夹。

(4) 输入“copy %windir%\system32\notepad.exe test”,将记事本复制到 test 文件夹中。

2) 批处理文件

【例 3-9】 建立批处理文件,解释下面每行命令的意思。

```
@echo off
echo ★正在清除系统垃圾文件☆,请稍等……
del /f /s /q %systemdrive%\*.tmp
del /f /s /q %systemdrive%\recycled\*.*
del /f /s /q %windir%\prefetch\*.*
del /f /q %userprofile%\cookies\*.*
del /f /q %userprofile%\recent\*.*
del /f /s /q "%userprofile%\Local Settings\Temporary Internet Files\*.*"
del /f /s /q "%userprofile%\Local Settings\Temp\*.*"
del /f /s /q "%userprofile%\recent\*.*"
echo 清除系统垃圾完成!
```

新建一个记事本文件,将上述内容复制到该文件中,保存并关闭,重新命名为批处理并将扩展名改为.bat。双击即可运行。

6. 思考题

视窗操作界面和命令提示符对系统的操作有什么区别和联系?

实践4 注册表和组策略

1. 实践目的

掌握操作注册表和组策略的方法。

2. 实践环境

连入 Internet 的计算机一台，安装 Windows XP，Windows 7 或 Windows 8 等操作系统。

3. 名词解释

(1) **注册表**：注册表是 Windows 系统中一个非常重要的数据库，它存储着计算机的软、硬件设置。

(2) **组策略**：组策略是管理员为计算机和用户定义的，是用来控制应用程序、系统设置和管理模板的一种机制。组策略就是介于控制面板和注册表之间的一种修改系统、设置程序的工具。

4. 预备知识

1) 注册表的结构

Windows 的注册表(Registry)实质上是一个庞大的数据库，它存储着下面这些内容：软、硬件的有关配置和状态信息，应用程序和资源管理器外壳的初始条件、首选项和卸载数据；计算机整个系统的设置和各种许可，文件扩展名与应用程序的关联，硬件的描述、状态和属性；计算机性能记录和底层的系统状态信息，以及各类其他数据。注册表编辑器的打开方式：选择“开始”→“运行”，输入“regedit”，单击“确定”按钮。

注册表是按照根键(HKEY)、键、子键以及值项的层次结构来组织的，每个值项有三方面属性，即名称、数据类型和值，如图 4-1 所示。

(1) HKEY_CLASSES_ROOT：基层类别键，定义了系统中所有已经注册的文件扩展名、文件类型、文件图标等。

(2) HKEY_CURRENT_USER(HKLU)：定义了当前用户的所有权限，实际上就是 HKEY_USERS\.Default 下面的一部分内容，包含了当前用户的登录信息。

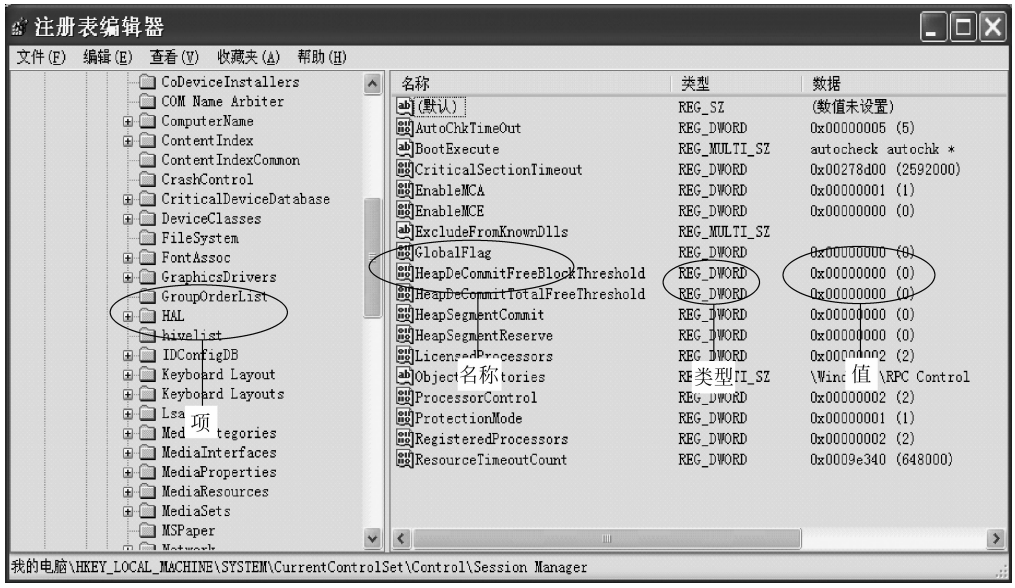


图 4-1 注册表编辑器

(3) HKEY_LOCAL_MACHINE(HKLM)：定义了本地计算机(相对网络环境而言)的软硬件的全部信息。当系统的配置和设置发生变化时，其下面的登录项也会随之改变。

(4) HKEY_USERS：定义了所有的用户信息，其中部分分支将映射到 HKEY_CURRENT_USER 关键字中，它的大部分设置都可以通过控制面板来修改。

(5) HKEY_CURRENT_CONFIG：定义了计算机的当前配置情况，如显示器、打印机等可选外部设备及其设置信息等。它实际上也是指向 HKEY_LOCAL_MACHINE\Config 结构中的某个分支的指针。

(6) 键与子键：键与子键的结构类似于文件夹与子文件夹。在键中可以包含值项与子键。

(7) 值项：每个注册表项或子项都可以包含称为值项的数据。有些值项存储特定于每个用户的信息，而其他值项则存储应用于计算机所有用户的信息。值项的数据类型说明如表 4-1 所示。

表 4-1 值项的数据类型

数 据 类 型	说 明
REG_BINARY	二进制数据。多数硬件组件信息都以二进制数据存储，而以十六进制格式显示在注册表编辑器中
REG_DWORD	双字。它占用 4 字节的长度。设备驱动程序和服务的很多参数都是采用这种类型
REG_EXPAND_SZ	长度可变的字符串，如包含变量(例如%system%)的字符串
REG_MULTI_SZ	多重字符串，包含列表或多值的值通常都是这种类型
REG_SZ	固定长度的字符串
REG_FULL_RESOURCE_DESCRIPTOR	专用于存储硬件或驱动程序所占用的资源列表。不能修改此处的数据

对注册表的编辑可以直接打开注册表编辑器进行修改，如图 4-1 所示；也可以使用控制台注册表工具 reg 命令修改，使用方法如下。

(1) REG ADD 增加注册表项命令。

```
>reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v serv /d calc.exe
```

其中，/v 指定要添加到指定子项下的注册表项名称，/d Data 指定新注册表项的数据，/ve 指定为空值的项。

(2) REG QUERY 查询注册表项命令。

```
>reg query HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

输出 Run 项下的值：

```
360Safetray   REG_SZ   "D:\Program Files\360\360Safe\safemon\360tray.exe" /start
<没有名称> REG_SZ
egui          REG_SZ   "C:\Program Files\ESET\ESET Smart Security\egui.exe" /hide
serv          REG_SZ    calc.exe
```

(3) REG DELETE 删除注册表项命令。

```
Reg deleteHKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v serv /f
```

其中，/f 表示不需要确认。

```
Reg deleteHKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /ve /f
```

可以删除上面(没有名称)的空值的项。

(4) REG EXPORT 导出注册表项命令。

```
>reg export HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run e:\1.reg
```

在注册表编辑器中，右击 Run 弹出右键快捷菜单，选择“导出”命令，则实现 REG EXPORT 命令一样的功能，如图 4-2 所示。

(5) REG IMPORT 导入注册表项命令。

```
>reg import e:\1.reg
```

其他命令还有 REG COMPARE、REG COPY、REG SAVE、REG RESTORE、REG LOAD、REG UNLOAD 等。当注册表编辑器被锁住而不能打开时，并不影响 REG 命令对注册表的修改。

2) 组策略

组策略(Group Policy)是管理员为用户和计算机定义并控制程序、网络资源及操作系统行为的主要工具。通过使用组策略可以设置各种软件、计算机和用户策略。组策略设置

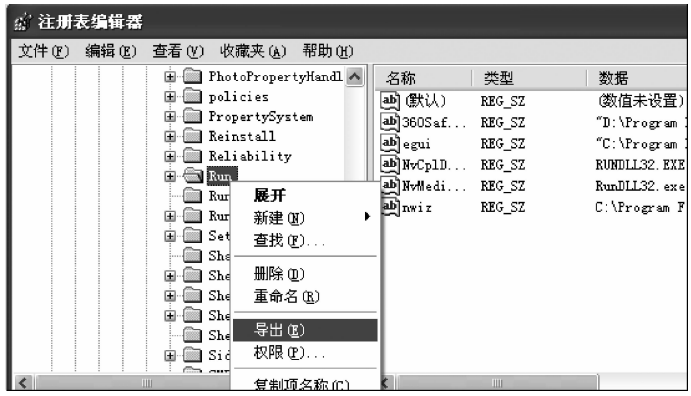


图 4-2 导出(保存)注册表项

就是在修改注册表中的配置。当然,组策略使用了更完善的管理组织方法,可以对各种对象中的设置进行管理和配置,远比手工修改注册表方便、灵活,功能也更加强大。组策略编辑器的打开方式:选择“开始”→“运行”,输入 gpedit.msc,单击“确定”按钮。如果组策略被禁用,则进入安全模式解锁即可。如图 4-3 所示。

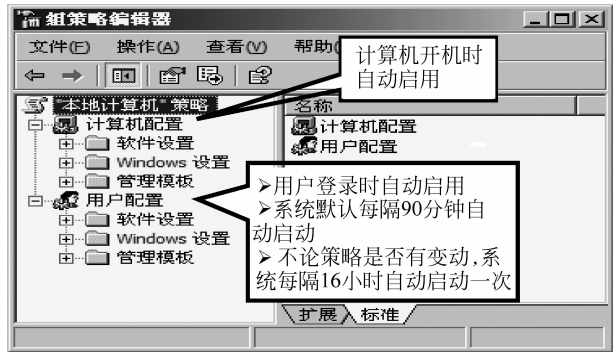


图 4-3 组策略编辑器

组策略包括计算机配置和用户配置。

(1) 计算机配置包括所有与计算机相关的策略设置,它们用来指定操作系统行为、桌面行为、安全设置、计算机开机与关机脚本、指定的计算机应用选项以及应用设置。

(2) 用户配置包括所有与用户相关的策略设置,它们用来指定操作系统行为、桌面设置、安全设置、指定和发布的应用选项、应用设置、文件夹重定向选项、用户登录与注销脚本等。

让新修改的计算机策略立即生效:

```
gpupdate /target:compute /force
```

让新修改的用户策略立即生效:

```
gpupdate /target:user/force
```