第1章　计算机知识快速入门

作为计算机或网络终端设备的用户，要想使自己的设备不受或少受黑客的攻击，就需要学习一些计算机安全方面的知识。本章就来介绍计算机安全的相关技术信息，主要内容包括网络中的相关概念、网络通信的相关协议、认识文件与文件夹、计算机账户、端口与服务等。

1.1　网络中的相关概念

在网络安全中，经常会接触到很多和网络有关的概念，如浏览器、URL、FTP、IP地址及域名等，理解了这些概念，对保护网络安全有一定的帮助。

1.1.1　互联网与因特网

互联网是指将两台计算机或者是两台以上的计算机终端、客户端、服务端通过计算机信息技术的手段互相联系起来的网络。互联网在现实生活中应用很广泛，人们可以在互联网上聊天、玩游戏、查阅东西等。互联网是全球性的，这就意味着这个网络不管是谁发明了它，都是属于全人类的。如图1-1为互联网的结构示意图。

图 1-1　互联网结构示意图

因特网是一个把分布于世界各地的计算机用传输介质互相连接起来的网络，因特网是基于TCP/IP协议实现的。TCP/IP协议由很多协议组成，不同类型的协议又被放在不同的层，其中，位于应用层的协议就有很多，比如FTP、SMTP、HTTP。如图1-2为因特网的结构示意图。

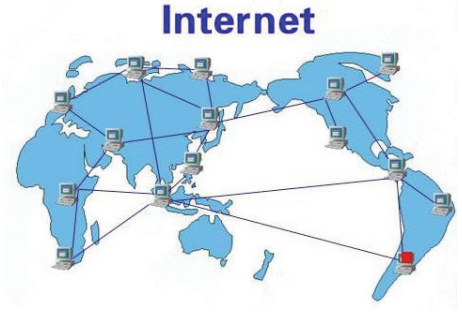

图 1-2　因特网结构示意图

1.1.2　万维网与浏览器

万维网（World Wide Web，WWW）简称为3W，它是无数个网络站点和网页的集合，也是因特网提供的最主要的服务。它是由多媒体链接而形成的集合，通常我们上网看到的内容就是万维网提供的。如图1-3为使用万维网打开的百度首页。

图 1-3　百度首页

提示： 互联网、因特网、万维网三者的关系是：互联网包含因特网，因特网包含万维网。凡是能彼此通信的设备组成的网络就叫互联网。所以，即使仅有两台机器，不论用何种技术使其彼此通信，也叫互联网。

浏览器是将互联网上的文本文档（或其他类型的文件）翻译成网页，并让用户与这些文件交互的一种软件工具，主要用于查看网页的内容。微软公司的Microsoft Edge是目前最常用的浏览器之一，如图1-4是使用Microsoft Edge浏览器打开的页面。

图 1-4　Microsoft Edge 浏览器

1.1.3　URL地址与域名

URL（Uniform Resource Locator）即统一资源定位器，也就是网络地址，是在因特网上用来描述信息资源，并将因特网提供的服务统一编址的系统。简单来说，通常在浏览器中输入的网址就是URL的一种，如百度网址https://www.baidu.com。

域名（Domain Name）类似于因特网上的门牌号，是用于识别和定位互联网上计算机的层次结构的字符标识，与该计算机的因特网协议（IP）地址相对应。相对于IP地址而言，域名更便于使用者理解和记忆。URL和域名是两个不同的概念，如https://www.sohu.com/是URL，而www.sohu.com是域名，如图1-5为使用URL地址打开的网页。

图 1-5　使用 URL 地址打开的网页

1.1.4　认识无线网络

无线网络（wireless network）是采用无线信道作为传输介质把各个结点互连所形成的网络。与有线网络的用途十分类似，无线网络最大的不同在于传输媒介。一般来说，无线网络就是我们常说的无线局域网，是基于802.11b/g/n标准的WLAN无线局域网，具有可移动、安装简单、高灵活和高扩展能力等特点。

作为对传统有线网络的延伸，这种无线网络在许多特殊环境中得到了广泛应用，如企业内部、学校内部、家庭等。这种网络的缺点是覆盖范围小，使用距离在5~30m范围内。如图1-6为一个简单的无线局域网示意图。

图 1-6　无线局域网示意图

随着无线数据网络解决方案的不断推出，全球Wi-Fi设备迅猛增长，相信在不久的将来，“不论在任何时间、任何地点都可以轻松上网”这一目标就会被实现。

1.1.5　无线路由器

无线路由器是应用于用户上网、带有无线覆盖功能的路由器。它和有线路由器的作用是一样的，唯一不同的就是无线路由器的顶部或者尾部多了一个或者几个天线，其作用就是提供无线网络支持。除此以外，其他无论是外观，或者是内在配置页面都和同款型的有线路由器一模一样。

目前，市场占有率比较高的无线路由器是TP-LINK无线路由器，其性价比较高。如图1-7为一款TP-LINK千兆无线路由器，具有高速双核、覆盖更远、家长控制、一键禁用等功能。

图 1-7　TP-LINK 千兆无线路由器

1.2　认识文件和文件夹

在Windows 10操作系统中，文件是最小的数据组织单位，文件中可以存放文本、图像和数值数据等信息。为了便于管理文件，用户还可以把文件组织到目录和子目录中，这些目录被认为是文件夹，而子目录则被认为是文件夹的文件或子文件夹。

1.2.1　文件与文件夹

文件是Windows存取磁盘信息的基本单位，是磁盘上存储的信息的一个集合，可以是文字、图片、影片或应用程序等。每个文件都有自己唯一的名称，Windows 10正是通过文件的名字来对文件进行管理的，如图1-8为一个图片文件。

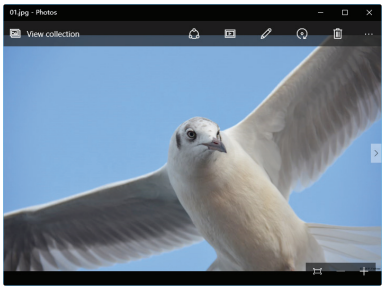

图 1-8　图片文件

文件夹是从Windows 95开始提出的一种名称，其主要用来存放文件，是存放文件的容器。在操作系统中，文件和文件夹都有名字，系统都是根据它们的名字来实现存取的。一般情况下，文件和文件夹的命名规则有以下几点。

- 文件和文件夹名称长度最多可达256个字符，1个汉字相当于2个字符。
- 文件和文件夹名中不能出现这些字符：斜线（\、/）、竖线（|）、小于号（<）、大于号（>）、冒号（：）、引号（“、”）问号（？）、星号（*）。
- 文件和文件夹不区分大小写字母。如abc和ABC是同一个文件名。
- 通常一个文件都有扩展名（一般为3个字符），用来表示文件的类型。文件夹通常没有扩展名。
- 同一个文件夹中的文件和文件夹不能同名。

如图1-9为Windows 10操作系统的“保存的图片”文件夹，双击打开这个文件夹，可以看到存放的文件。

图 1-9　“保存的图片”文件夹

1.2.2 文件和文件夹的存放位置

计算机中的文件或文件夹一般存放在本台电脑中的磁盘或Administrator文件夹当中。

1. 计算机磁盘

理论上说，文件可以被存放在计算机磁盘的任意位置，但是为了便于管理，文件的存放有以下常见的原则，如图1-10所示。

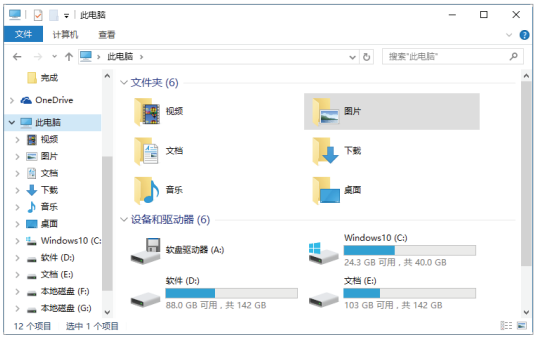

图 1-10 “此电脑”文件夹

通常情况下，用户计算机的硬盘最少也被划分为三个分区：C、D和E盘。3个盘的功能分别如下。

- C盘主要是用来存放系统文件。所谓系统文件，是指操作系统和应用软件中的系统操作部分。一般系统默认情况下都会被安装在C盘，包括常用的程序。
- D盘主要用来存放应用软件文件。比如，Office、Photoshop和3ds Max等程序，常常被安装在D盘。对于软件的安装，有以下常见的原则。

（1）一般小的软件，如 WinRAR 压缩软件等可以安装在 C 盘。

（2）对于大的软件，如 3ds Max 等，需要安装在 D 盘，这样可以少占用 C 盘的空间，从而保证系统运行的速度。

（3）几乎所有的软件默认的安装路径都在 C 盘中，电脑用得越久，C 盘被占用的空间越多。随着时间的增加，系统反应会越来越慢。所以安装软件时，需要根据具体情况改变安装路径。

- E盘用来存放用户自己的文件。比如，用户自己的电影、图片和Word资料文件等。如果硬盘还有多余的空间，可以添加更多的分区。

2. Administrator文件夹

Administrator文件夹是Windows 10中的一个系统文件夹，是系统为每个用户建立的文件夹，主要用于保存文档、图形，当然也可以保存其他文件。对于常用的文件，用户可以将其放在Administrator文件夹中，以便于及时调用，如图1-11所示。

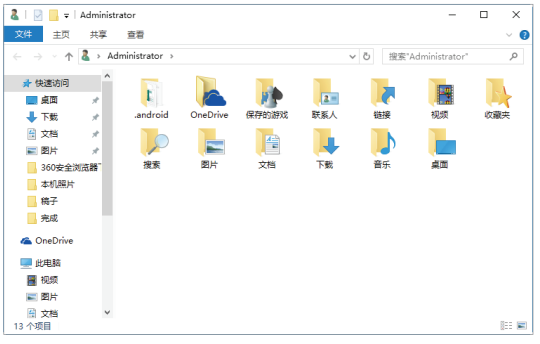

图 1-11 Administrator 文件夹

1.2.3 文件和文件夹的路径

文件和文件夹的路径表示文件或文件夹所在的位置，路径在表示的时候有2种方法：绝对路径和相对路径。

绝对路径是从根文件夹开始的表示方法，根通常用\来表示（区别于网络路径），比如c:\Windows\System32表示C盘下面Windows文件夹下面的System32文件夹。根据文件或文件夹提供的路径，用户可以在电脑上找到该文件或文件夹的存放位置。如图1-12为C盘下面Windows文件夹下面的System32文件夹。

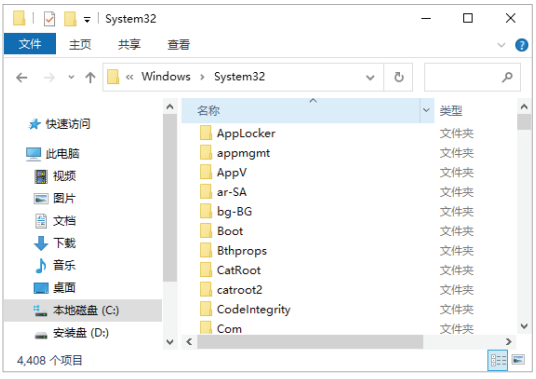

图 1-12　system32 文件夹

相对路径是从当前文件夹开始的表示方法，比如当前文件夹为c:\Windows，如果要表示它下面的System32下面的ebd文件夹，则可以表示为System32\ebd，而用绝对路径应写为c:\Windows\System32\ebd。

1.3　认识Administrator账户

Administrator账户也被称为本地账户，要想系统相对安全，需要给账户设置密码，并添加相关安全措施。

1.3.1　设置账户密码

对于添加的账户，用户可以创建密码，或对创建的密码进行更改，如果不需要密码了，还可以删除账户密码。下面介绍2种创建、更改或删除密码的方法。

1. 通过控制面板中创建、更改或删除密码

具体的操作步骤如下。

Step 01 打开“控制面板”窗口，进入“更改账户”窗口，在其中单击“创建密码”超链接，如图1-13所示。

Step 02 进入“创建密码”窗口，在其中输入密码与密码提示信息，如图1-14所示。

Step 03 单击“创建密码”按钮，返回“更改账户”窗口，在其中可以看到该账户已经添加了密码保护，如图1-15所示。

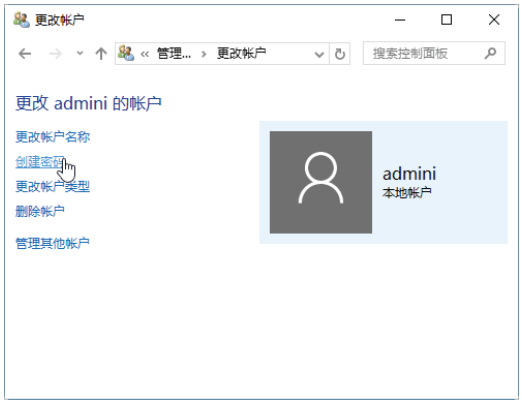

图 1-13　“更改账户”窗口

图 1-14　“创建密码”窗口

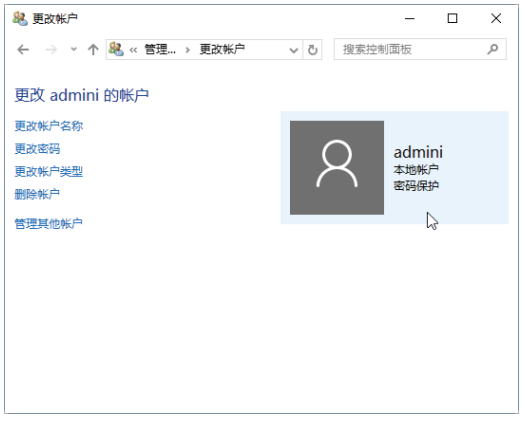

图 1-15　为账户添加密码

Step 04 如果想要更改密码，则需要在“更改账户”窗口中单击“更改密码”超链接，打开“更改密码”窗口，在其中输入新的密码与密码提示信息，最后单击“更改密码”按钮即可，如图1-16所示。

图 1-16 “更改密码”窗口

Step 05 如果想要删除密码，则需要在“更改账户”窗口中单击“更改密码”超链接，打开“更改密码”窗口，在其中设置密码为空，如图1-17所示。

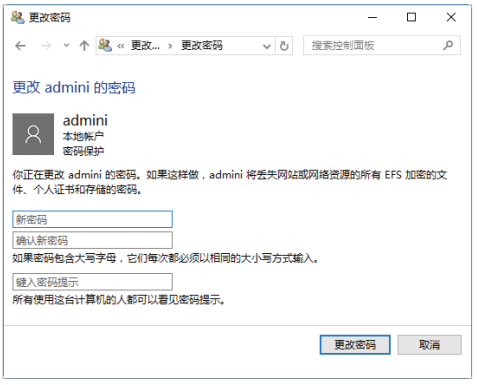

图 1-17 取消账户密码

Step 06 单击“更改密码”按钮，返回“更改账户”窗口，可以看到账户的密码保护已取消，说明已经将账户密码删除了，如图1-18所示。

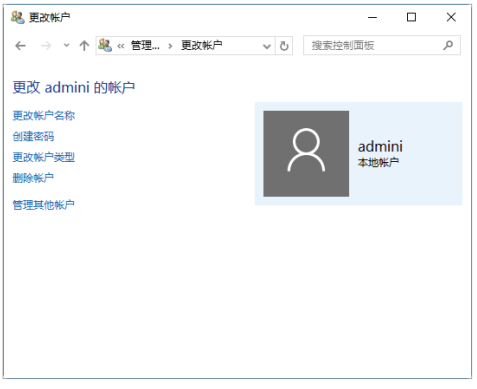

图 1-18 “更改密码”窗口

2. 在计算机设置中创建、更改或删除密码

具体的操作步骤如下。

Step 01 单击“ ”按钮，在弹出的面板中选择“设置”选项，如图1-19所示。

图 1-19 “设置”选项

Step 02 打开“设置”窗口，如图1-20所示。

图 1-20 “设置”窗口

Step 03 单击“账户”超链接，进入“设置-账户”窗口，如图1-21所示。

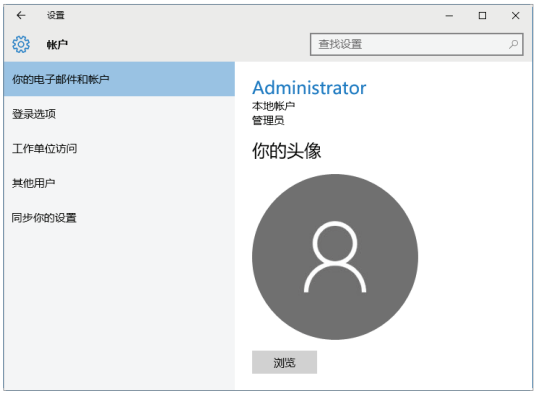

图 1-21 “设置 - 账户”窗口

Step 04 选择“登录选项”选项，进入“登录选项”窗口，如图1-22所示。

图 1-22　“登录选项”窗口

Step 05 单击“密码”区域下方的“添加”按钮，打开“创建密码”界面，在其中输入密码与密码提示信息，如图1-23所示。

图 1-23　输入密码

Step 06 单击“下一步”按钮，进入“创建密码”界面，在其中会提示用户下次登录时，请使用新密码，最后单击“完成”按钮，完成密码的创建，如图1-24所示。

Step 07 如果想要更改密码，则需要选择“设置-账户”窗口中的“登录选项”，进入“登录选项”设置界面，如图1-25所示。

Step 08 单击“密码”区域下方的“更改”按钮，打开“更改密码”对话框，在其中输入当前密码，如图1-26所示。

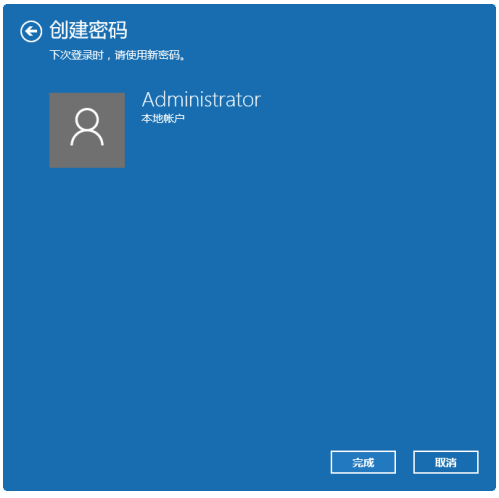

图 1-24　“创建密码”界面

图 1-25　“登录选项”窗口

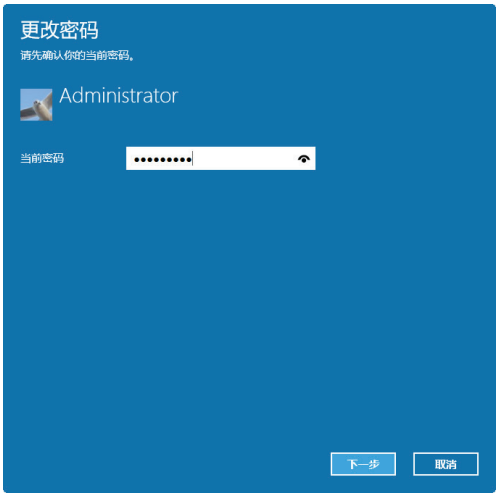

图 1-26　“更改密码”界面

Step 09 单击“下一步”按钮，打开“更改密

码”对话框，在其中输入新密码和密码提示信息，如图1-27所示。

图 1-27　输入新密码

Step 10 单击“下一步”按钮，完成本地账户密码的更改操作，最后单击“完成”按钮结束操作，如图1-28所示。

图 1-28　密码更改成功

提示：如果想要删除密码，只需要在“更改密码”界面中将密码与密码提示设置为空，然后单击“下一步”按钮，完成删除密码操作。

1.3.2　删除用户账户

对于不需要的本地账户，用户可以将其删除，具体的操作步骤如下。

Step 01 打开“管理账户”窗口，在其中选择要删除的账户，如图1-29所示。

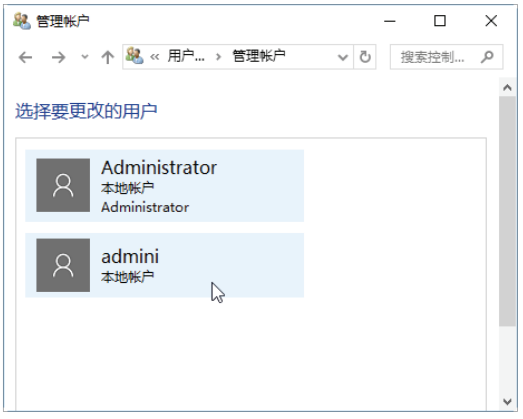

图 1-29　“管理账户”窗口

Step 02 进入“更改账户”窗口，单击左侧的“删除账户”超链接，如图1-30所示。

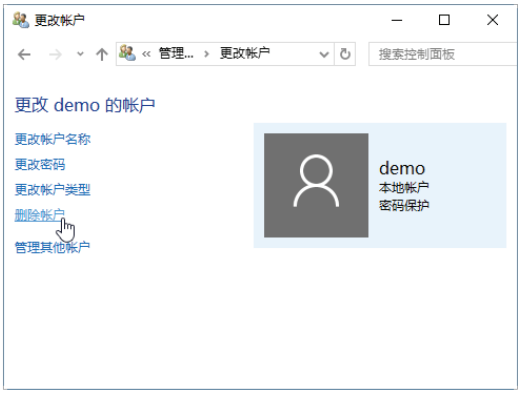

图 1-30　“更改账户”窗口

Step 03 进入“删除账户”窗口，提示用户是否保存账户的文件，如图1-31所示。

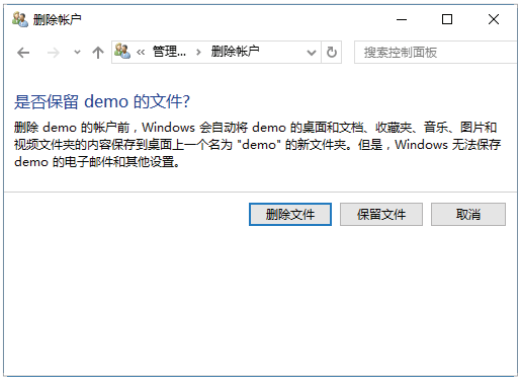

图 1-31　“删除账户”窗口

Step 04 单击“删除文件”按钮，进入“确认删除”窗口，提示用户是否确实要删除账户，如图1-32所示。

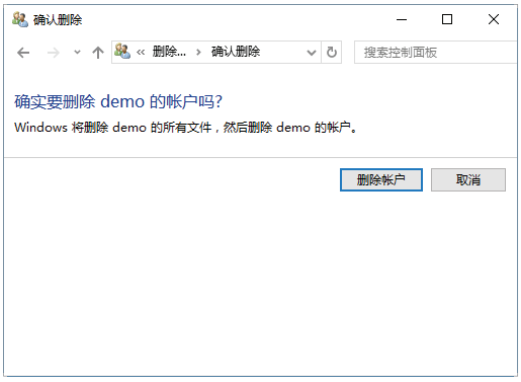

图 1-32　“确认删除”窗口

Step 05 单击“删除账户”按钮即可删除选择的账户，并返回“管理账户”窗口，在其中可以看到要删除的账户已经不存在了，如图1-33所示。

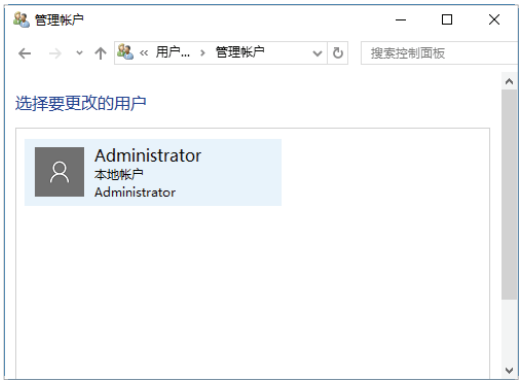

图 1-33　删除账户

提示：对于当前正在登录的账户，Windows是无法删除的，因此，在删除账户的过程中，会弹出一个“用户账户控制面板”信息提示框来提示用户，如图1-34所示。

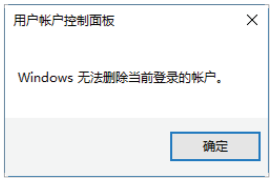

图 1-34　信息提示框

1.3.3　创建新用户账户

在Windows10操作系统中，除本地Administrator账户外，还可以添加新用户账户，具体的操作步骤如下。

Step 01 打开“计算机管理”窗口，选择“本地用户和组”下方的“用户”选项，展开本地用户列表，如图1-35所示。

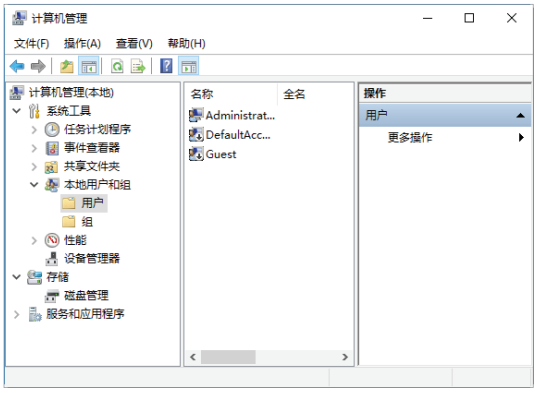

图 1-35　“计算机管理”窗口

Step 02 在用户列表窗格的空白处，单击鼠标右键，在弹出的快捷菜单中选择“新用户”菜单命令，如图1-36所示。

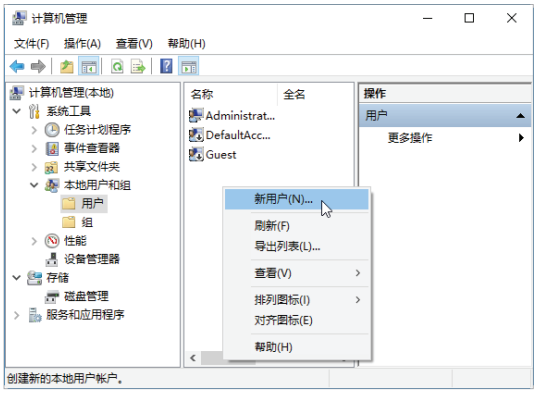

图 1-36　“新用户”菜单命令

Step 03 打开“新用户”对话框，在“用户名”和“全名”等文本框中输入新用户名称等信息，如图1-37所示。

Step 04 输入完毕后，单击“创建”按钮，返回“计算机管理”窗口中，可以看到已经创建的新用户，如图1-38所示。

图 1-37 “新用户”对话框

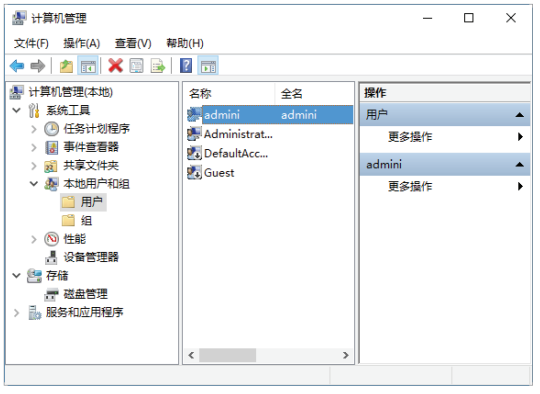

图 1-38 创建一个新用户

1.4 认识端口和服务

端口和服务是计算机操作系统中不可缺少的部分，端口和服务常常被联系在一起，一个端口对应着一个服务，如Web服务默认对应80端口等。

1.4.1 认识端口

端口可以认为是计算机与外界通信交流的出口。一个IP地址的端口可以有65536（256×256）个，端口是通过端口号来标记的，端口号只有整数，范围是0~65535（256×256－1）。

服务器上开放的端口往往是潜在的黑客入侵通道。对目标主机进行端口扫描能够获得许多有用的信息，常用的方法是使用端口扫描工具对指定IP或IP地址段进行扫描，下面介绍使用ScanPort扫描器扫描端口的方法，具体操作步骤如下。

Step 01 下载并运行ScanPort程序，打开ScanPort主窗口，在其中设置起始IP地址、结束IP地址以及要扫描的端口号，如图1-39所示。

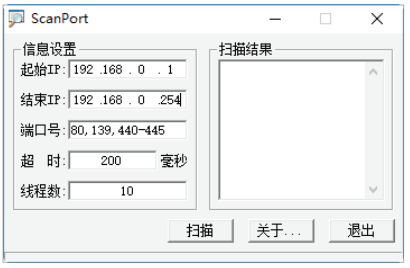

图 1-39 ScanPort 主窗口

Step 02 单击“扫描”按钮，开始进行扫描，从扫描结果中可以看出设置的IP地址段中计算机开启的端口，如图1-40所示。

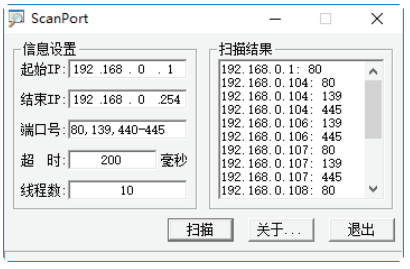

图 1-40 开始扫描

Step 03 如果扫描某台计算机中开启的端口，则需将开始IP和结束IP都设置为该主机的IP地址，如图1-41所示。

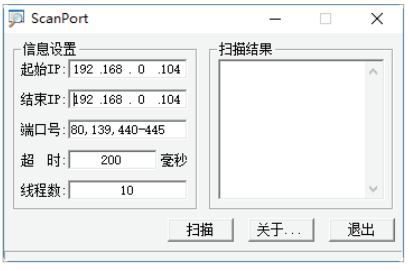

图 1-41 设置单一主机的 IP

Step 04 在设置完要扫描的端口号之后，单击“扫描”按钮，可扫描出该主机中开启的端口（设置端口范围之内），如图1-42所示。

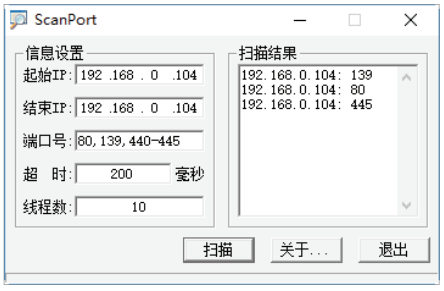

图 1-42　开始扫描单个主机的端口

1.4.2　认识服务

在计算机中安装好操作系统之后，通常系统会默认启动许多服务，且每项服务都有一个具体的文件存在，一般存储在“C:\Windows\System32”文件夹中，其扩展名一般是.exe、.dll、.sys等。另外，操作系统中的服务还可以根据自己的需要开启相应的服务或关闭不必要服务。以开启WebClient服务为例，具体操作步骤如下。

Step 01 单击“⊞”按钮，在弹出的菜单列表中选择“Windows系统”“控制面板”菜单命令，如图1-43所示。

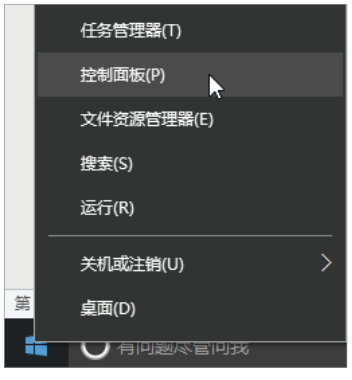

图 1-43　选择“控制面板”命令

Step 02 打开“控制面板”窗口，双击“管理工具”图标，如图1-44所示。

图 1-44　“控制面板”窗口

Step 03 打开“管理工具”窗口，双击“服务”图标，如图1-45所示。

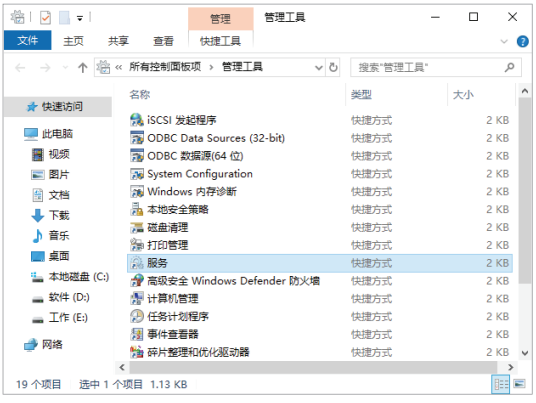

图 1-45　“服务”图标

Step 04 打开“服务”窗口，找到WebClient服务项，如图1-46所示。

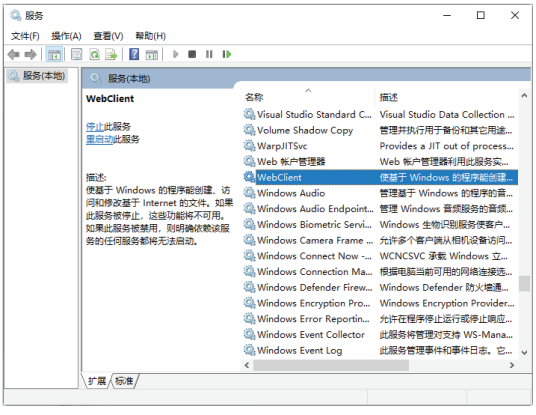

图 1-46　“服务”窗口

Step 05 双击该服务项，弹出“WebClient的属性”对话框，单击“启动类型”右侧的

下拉按钮，在弹出的下拉菜单中选择“自动”，如图1-47所示。

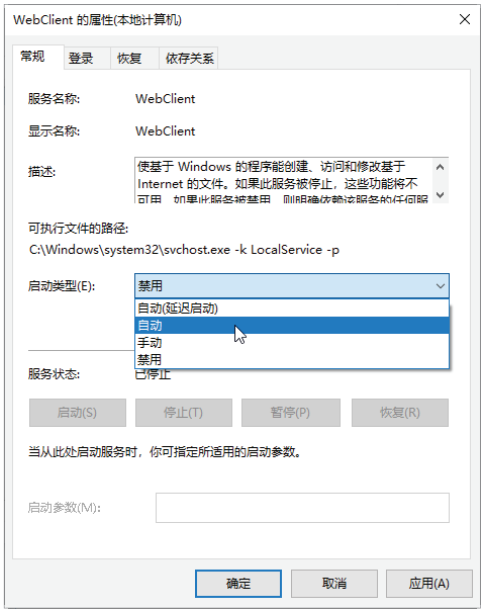

图 1-47　选择“自用”选项

Step 06 单击“应用”按钮，激活“服务状态”下的“启动”按钮，如图1-48所示。

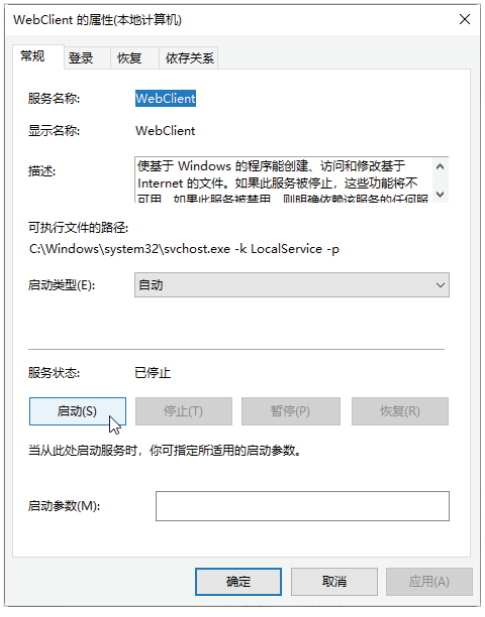

图 1-48　选择“启动”按钮

Step 07 单击“启动”按钮，可启动该项服务，再次单击“应用”按钮，在“WebClient的属性”对话框中可以看到该服务的“服务状态”已经变为“正在运行”，如图1-49所示。

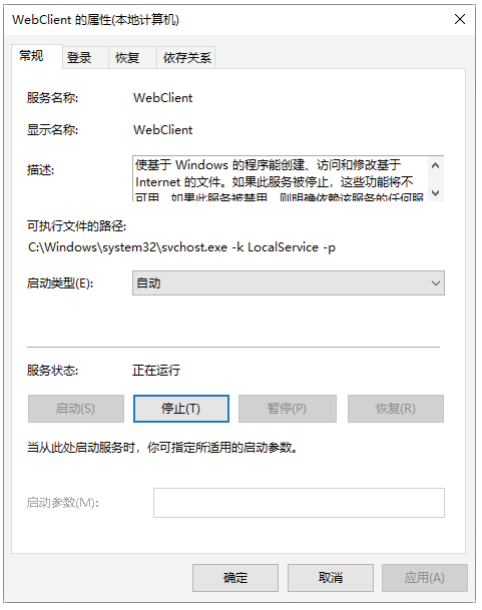

图 1-49　启动服务项

Step 08 单击“确定”按钮，返回“服务”窗口，此时即可发现WebClient服务的“状态”变为“正在运行”，这样就可以成功开启WebClient服务对应的端口，如图1-50所示。

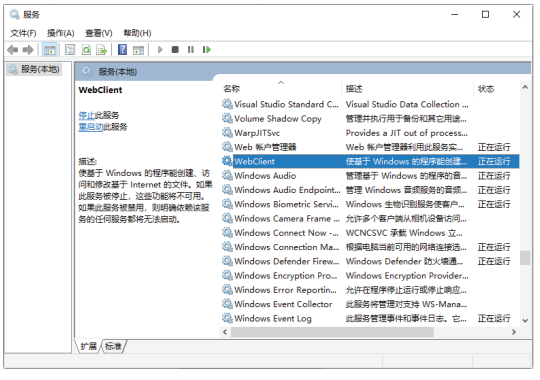

图 1-50　WebClient 服务的状态为“正在运行”

1.5　实战演练

1.5.1　实战1：关闭开机多余启动项目

在计算机启动的过程中，自动运行的程序称为开机启动项，有时一些木马程序

会在开机时就运行，用户可以通过关闭开机启动项来提高系统安全性，具体的操作步骤如下。

Step 01 按Ctrl+Alt+Del组合键，打开如图1-51所示的界面。

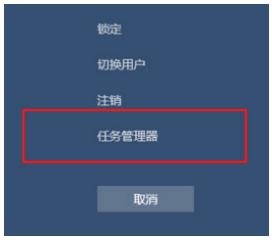

图 1-51　“任务管理器”选项

Step 02 单击“任务管理器”选项，打开“任务管理器”窗口，如图1-52所示。

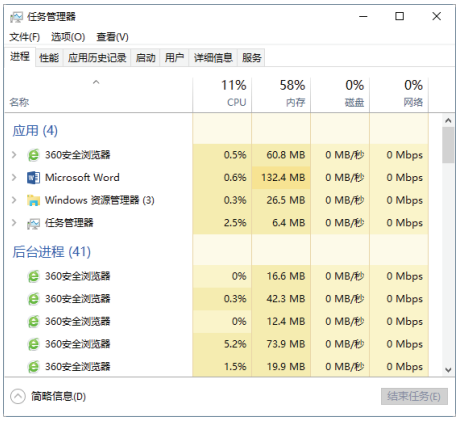

图 1-52　“任务管理器”窗口

Step 03 选择“启动”选项卡，进入“启动”界面，在其中可以看到系统中的开机启动项列表，如图1-53所示。

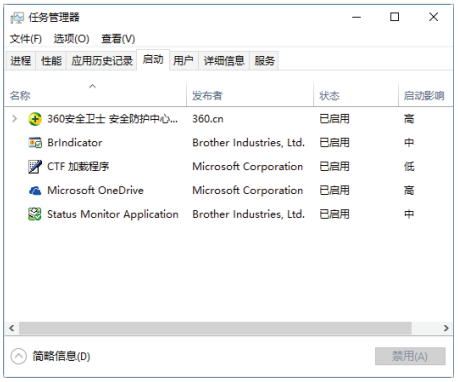

图 1-53　“启动”选项卡

Step 04 选择开机启动项列表中需要禁用的启动项，单击“禁用”按钮即可禁止该启动项开机自启动，如图1-54所示。

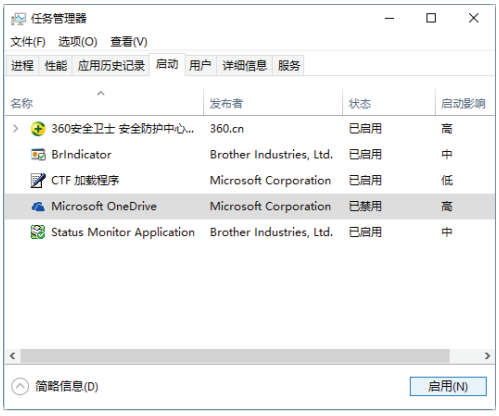

图 1-54　禁止开机启动项

1.5.2　实战2：取消Windows开机密码

虽然使用账户登录密码，可以保护电脑的隐私安全，但是每次登录时都要输入密码，对于一部分用户来讲，太过于麻烦。用户可以根据需求，选择是否使用开机密码，如果希望Windows可以跳过输入密码直接登录，可以参照以下步骤。

Step 01 在电脑桌面中，按⊞+R组合键，打开“运行”对话框，在文本框中输入netplwiz，按Enter键确认，如图1-55所示。

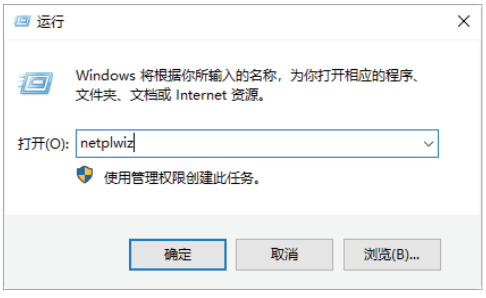

图 1-55　输入 netplwiz

Step 02 弹出“用户账户”对话框，选中本机用户，并取消勾选“要使用计算机，用户必须输入用户名和密码”复选框，单击“应用”按钮，如图1-56所示。

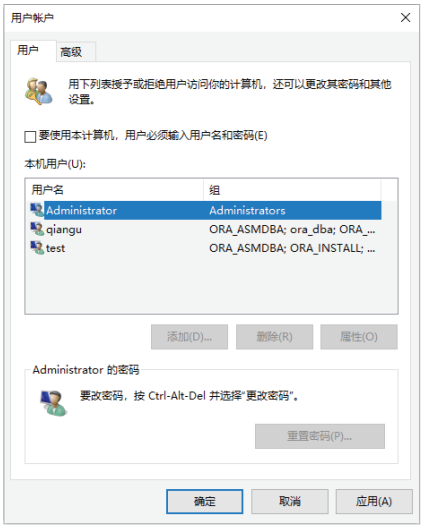

图 1-56 “用户账户”对话框

Step 03 弹出“自动登录”对话框，在“密码”和“确认密码”文本框中输入当前账户密码，然后单击“确定”按钮即可取消开机登录密码，当再次登录时，无须输入用户名和密码，直接登录系统，如图1-57所示。

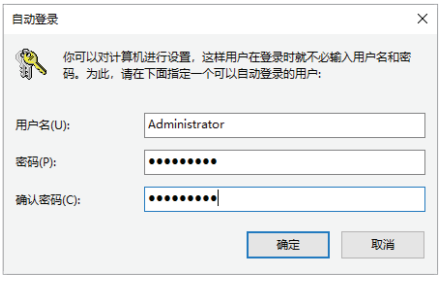

图 1-57 输入账户密码

第2章　DOS窗口与DOS系统

对于系统和网络管理者来说，繁杂的服务器管理以及网络管理是日常工作的主要内容。网络越大，其管理工作强度就越大，管理难度也随之变大。传统的可视化窗口虽然容易上手，但是对于一些后台管理操作，还需要使用DOS窗口。本章就来介绍DOS窗口与DOS系统的相关内容。

2.1　认识DOS窗口

Windows10操作系统中的DOS窗口，也被称为“命令提示符”窗口，该窗口主要以图形化界面显示，用户可以很方便地进入DOS命令窗口并对窗口中的命令行进行相应的编辑操作。

2.1.1　使用菜单进入DOS窗口

Windows10的图形化界面缩短了人与机器之间的距离，通过使用菜单可以很方便地进入DOS窗口，具体的操作步骤如下：

Step 01 单击桌面上的“ ”按钮，在弹出的菜单列表中选择“Windows系统”→“命令提示符”菜单命令，如图2-1所示。

图 2-1　“命令提示符”菜单命令

Step 02 弹出“管理员:命令提示符”窗口，在其中可以执行相关DOS命令，如图2-2所示。

图 2-2　“管理员 : 命令提示符”窗口

2.1.2　使用“运行”对话框进入DOS窗口

除使用菜单的形式进入DOS窗口中，用户还可以运用“运行”对话框进入DOS窗口，具体的操作步骤如下。

Step 01 在Windows10操作系统中，右击桌上的“ ”按钮，在弹出的快捷菜单中选择“运行”菜单命令。随即弹出“运行”对话框，在其中输入cmd命令，如图2-3所示。

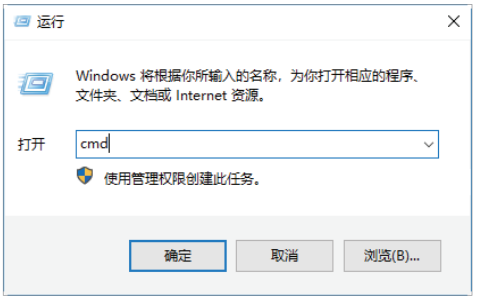

图 2-3　“运行”对话框

Step 02 单击“确定”按钮，进入DOS窗口，如图2-4所示。

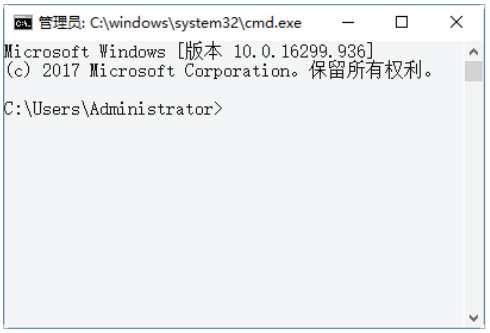

图 2-4　DOS 窗口

2.1.3　通过浏览器进入DOS窗口

浏览器和“命令提示符”窗口关系密切，用户可以直接在浏览器中访问DOS窗口。下面以在Windows10操作系统下访问DOS窗口为例，具体的方法为：在Microsoft Edge浏览器的地址栏中输入c:\Windows\system32\cmd.exe，如图2-5所示。按Enter键后即可进入DOS运行窗口，如图2-6所示。

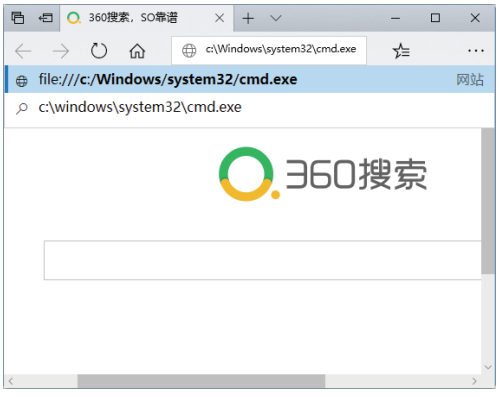

图 2-5　Microsoft Edge 浏览器

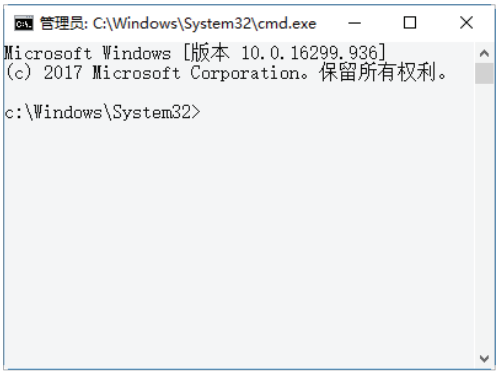

图 2-6　DOS 窗口

注意：在输入地址时，一定要输入全路径，否则Windows无法打开命令提示符窗口。

2.1.4　编辑DOS窗口中的代码

当在Windows10中启动命令行，就会弹出相应的DOS窗口，在其中显示当前的操作系统的版本号。在使用命令行时可以对命令行进行复制、粘贴等操作，具体操作步骤如下。

Step 01 右击DOS窗口标题栏，将弹出一个快捷菜单。在这里可以对当前窗口进行各种操作，如移动、最大化、最小化、编辑等。选择此菜单中的“编辑”命令，在显示的子菜单中选择“标记”选项，如图2-7所示。

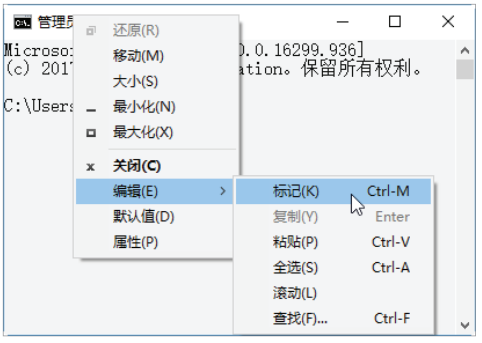

图 2-7　“标记”选项

Step 02 移动鼠标，选择要复制的内容，可以直接按Enter键复制该命令行，也可以通过选择“编辑”→“复制”选项来实现，如图2-8所示。

图 2-8　“复制”选项

Step 03 在需要粘贴该命令行的位置处单击鼠标右键，完成粘贴操作，或者右击“命令提示符”窗口的菜单栏，在弹出的快捷菜

单中选择“编辑”→“粘贴”选项，也可完成粘贴操作，如图2-9所示。

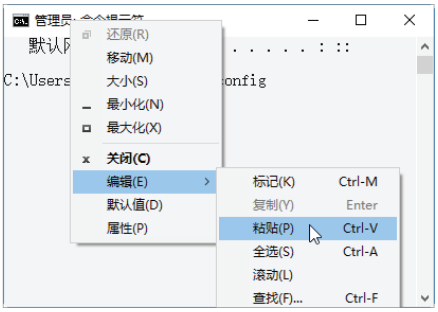

图 2-9　“粘贴”选项

提示：如果想再使用上一条命令，可以按F3键调用，要实现复杂的命令行编辑功能，可以借助于DOSKEY命令。

2.1.5　自定义DOS窗口的风格

DOS窗口的风格不是一成不变的，用户可以通过“属性”菜单选项对命令提示符窗口的风格进行自定义设置，如设置窗口的颜色、字体的样式等。自定义DOS窗口的风格的操作步骤如下。

Step 01 单击DOS窗口左上角的图标，在弹出菜单中选择“属性”选项，打开“命令提示符属性”对话框，如图2-10所示。

图 2-10　“选项”选项卡

Step 02 选择“颜色”选项卡，在其中可以对相关选项进行颜色设置。选中“屏幕文字”单选按钮，可以设置屏幕文字的显示颜色，这里选择“黑色”，如图2-11所示。

图 2-11　“颜色”选项卡

Step 03 选中“屏幕背景”单选按钮，可以设置屏幕背景的显示颜色，这里选择“灰色”，如图2-12所示。

图 2-12　设置屏幕背景颜色

Step 04 选中“弹出文字”单选按钮，可以设置弹出窗口文字的显示颜色，这里设置蓝

色颜色值为180，如图2-13所示。

图 2-13　设置文字颜色

Step 05 选中“弹出窗口的背景”单选按钮，可以设置弹出窗口的背景显示颜色，这里设置颜色值为125，如图2-14所示。

图 2-14　设置弹出窗口背景颜色

Step 06 设置完毕后单击“确定”按钮，保存设置，DOS窗口的风格会相应改变，如图2-15所示。

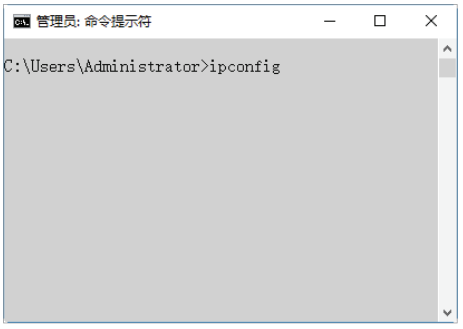

图 2-15　自定义显示风格

2.2　认识DOS系统

DOS实际上是一组控制计算机工作的程序，专门用来管理计算机中的各种软、硬件资源，同时监视和控制计算机的全部工作过程。

2.2.1　DOS系统的功能

DOS系统不仅向用户提供了一整套使用计算机系统的命令和方法，还向用户提供了一套组织和应用磁盘内信息的方法。DOS的功能主要体现在以下几个方面。

（1）执行命令和程序（处理器管理）

DOS能够执行DOS命令和运行可执行的程序。在DOS环境下（即在DOS提示符下），当用户键入合法命令和文件名后，DOS就根据文件的存储地址到内存或外存上查找用户所需的程序，并根据用户的要求使CPU开始运行之；若未找到所需文件，则出现出错信息，提醒用户。在这里，DOS正是扮演了使用者、计算机、应用程序三者之间的“中间人”。

（2）内存管理

分配内存空间，保护内存，使任何一个程序所占的内存空间不遭破坏，同硬件相配合，可以设置一个最佳的操作环境。

（3）设备管理

为用户提供使用各种输入/输出设备（如键盘、磁盘、打印机和显示器等）的操作方法。通过DOS可以方便地实现内存

和外存之间的数据传送和存取。

（4）文件管理

为用户提供一种简便的存取和管理信息方法。通过DOS管理文件目录，为文件分配磁盘存储空间，新建、复制、删除、读/写和检索各类文件等。

（5）作业管理

作业是指用户提交给计算机系统的一个独立的计算任务，包括源程序、数据和相关命令。作业管理是对用户提交的诸多作业进行管理，包括作业的组织、控制和调度等。

2.2.2　文件与目录

文件是存储于外存储器的具有名字的一组相关信息的集合，在DOS下所有的程序和数据都是以文件形式存入磁盘的，目录是Windows下的文件夹。

如果想查看计算机中的文件与目录，在“命令提示符”窗口可以输入dir命令，然后按Enter键即可看到相应的文件和目录，如图2-16所示。

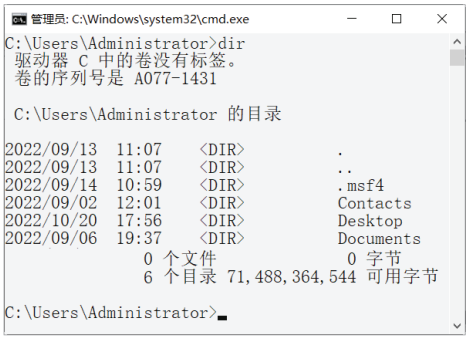

图 2-16　查看计算机文件与目录

DOS系统规定文件名由以下四个部分组成：[<盘符>][<路径>]<文件名>[<.扩展名>]。文件由文件名和文件内容组成，文件名由用户命名或系统指定，用于标识一个文件。

DOS文件名由1~8个字符组成，构成文件名的字符分为以下3类：

（1）26个英文字母：a~z 或A~Z；

（2）10个阿拉伯数字：0～9；

（3）一些专用字符：$、#、&、@、!、%、()、{}、-、一。

注意：在文件名中不能使用“<”“>”“\”“//”“[”“、”“]”“:”“!”“+”“=”等特殊符号。另外，用户可根据需要自行命名文件。

2.2.3　文件类型与属性

文件类型是根据文件用途和内容划分的不同类型，分别用不同的扩展名表示。文件扩展名由1~3个ASCII字符组成，文件扩展名有些是系统在一定条件下自动形成的，也有一些是用户自己定义的，它和文件名之间用“.”分隔，最常见的文件扩展名如表2-1所示。

表2-1　常见文件类型以及文件类型扩展名

文件类型扩展名	文 件 类 型
.com	系统命令文件
.exe	可执行文件
.bat	可执行的批处理文件
.sys	系统专用文件
.bak	后备文件
.dat	数据库文件
.txt	正文文件
.htm	超文本文件
.obj	目标文件
.tmp	临时文件
.bas	BASIC源程序文件
.C	C语言源程序文件
.cpp	C++语言源程序文件
.img	图像文件

文件属性是DOS系统下的所有磁盘文件，根据其特点和性质分为系统、隐含、只读和存档4种不同的属性。这4种属性的作用如下。

（1）系统属性（S）

系统属性用于表示文件是系统文件还是非系统文件，具有系统属性的文件不能被删除、拷贝和更名，如DOS系统文件io.sys和msdos.sys。如果可执行文件被设置为具有系统属性，则不能被执行。

（2）隐含属性（H）

隐含属性用于阻止文件在列表中显示出来，具有隐含属性的文件会被隐藏起来，也不能被删除、拷贝和更名。如果可执行文件被设置为具有隐含属性后，并不影响其正常执行。使用这种属性可以对文件进行保密。

（3）只读属性（R）

只读属性用于保护文件不被修改和删除。具有只读属性的文件，其特点是能读入内存，也能被拷贝，但不能用DOS系统命令修改，也不能被删除。可执行文件被设置为具有只读属性后，并不影响其正常执行。对于一些重要的文件，可设置为具有只读属性，以防止文件被删除。

（4）存档属性（A）

存档属性用于表示文件被写入时是否关闭。如果文件具有这种属性，则表明文件写入时被关闭。各种文件生成时，DOS系统均自动将其设置为存档属性。改动了的文件，也会被自动设置为存档属性。只有具有存档属性的文件，才可以显示出目录清单，还可以执行删除、修改、更名、拷贝等操作。

2.2.4 当前目录与磁盘

在DOS中，当前目录就是提示符所显示的目录，例如现在的提示符是C:\，那么当前目录就是C盘的根目录，这个“\”（反斜扛）就表示根目录。

如果要更改当前目录，那么可以用cd命令，例如输入“cd \”，则进入C盘，再输入cd Windows，则目录为Windows目录，按Enter键后，提示符变成了C:\Windows，这就表示当前目录变成了C盘的Windows目录，如图2-17所示。

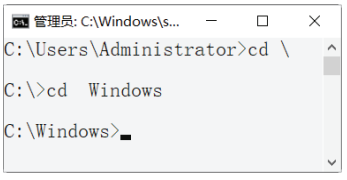

图 2-17 更改当前目录

然后输入dir命令，显示的就是Windows目录里的文件，这就说明，dir命令列出的是当前目录中的内容，如图2-18所示。

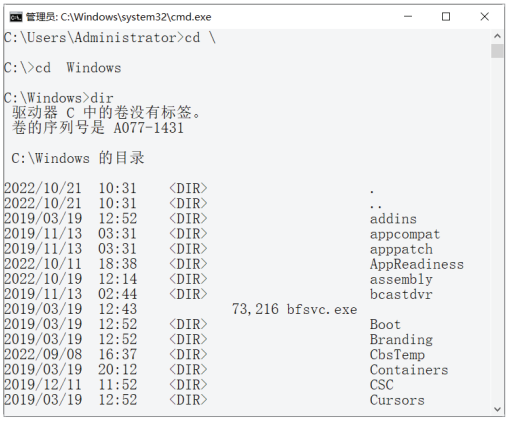

图 2-18 显示 Windows 目录的文件

DOS中目录采用的是树形结构，例如C:\Windows\System语句中，“C：”表示最上面的一层目录，Windows表示C目录的子目录，System表示Windows目录下的子目录，如图2-19所示。

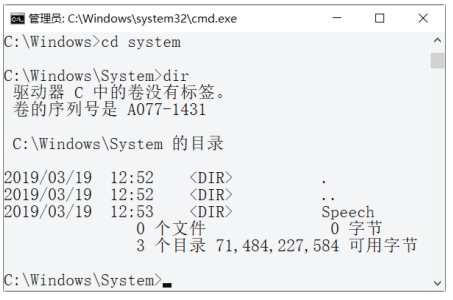

图 2-19 Windows 下的 System 目录

如果要退出子目录，可以输入“CD..”，然后按Enter键即可，在DOS中，“..”表示当前目录的上一层目录，“.”表示当前目录，这里的上一级目录为父目录，例如输入“CD..”，按Enter键，返回上一级目录，再次输入“CD..”，可回到C盘根目录，如图2-20所示。当然，如果不想多次输入“CD..”命令来返回C盘根目录，那么可以直接输入“CD\”命令来返回C盘根目录，其中“\”就表示根目录，如图2-21所示。

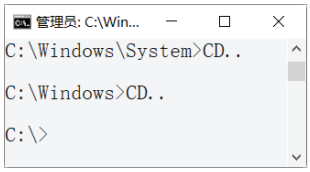

图 2-20　C 盘根目录

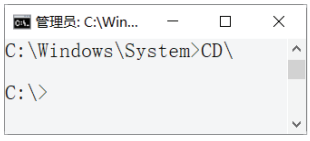

图 2-21　输入“CD\”命令

如果要更换当前目录到硬盘的其他分区，则可以输入盘符然后按Enter键，比如：要到D盘，那么就需要输入“d:”命令，然后按Enter键，现在提示符就变成了D:\>，如图2-22所示，然后输入dir命令，就可以看到D盘的文件的列表，如图2-23所示。

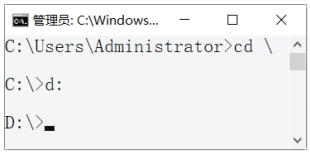

图 2-22　更改到 D 盘目录

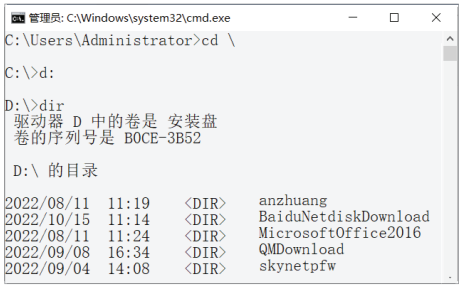

图 2-23　D 盘中的文件列表

2.3　实战演练

2.3.1　实战1：使用Windows更新修补漏洞

“Windows更新”是系统自带的用于检测系统更新的工具，使用“Windows更新”可以下载并安装系统更新，以Windows10系统为例，具体的操作步骤如下。

Step 01 单击“ ”按钮，在打开的菜单中选择“设置”选项，如图2-24所示。

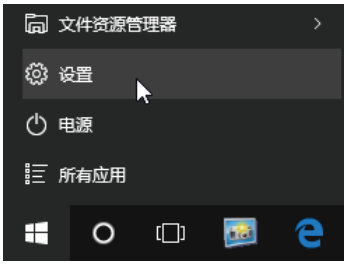

图 2-24　“设置”选项

Step 02 打开“设置”窗口，可以看到有关系统设置的相关功能，如图2-25所示。

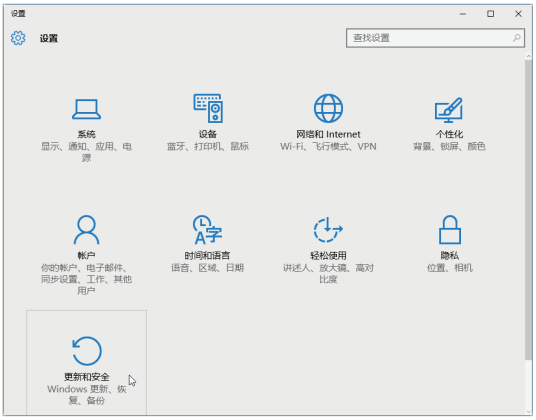

图 2-25　“设置”窗口

Step 03 单击“更新和安全”图标，打开“更新和安全”窗口，在其中选择“Windows更新”选项，如图2-26所示。

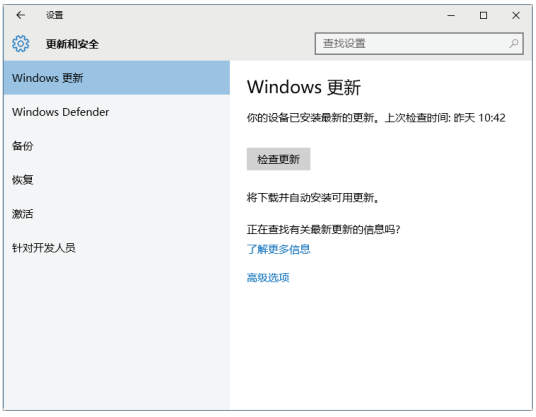

图 2-26　“更新和安全”窗口

Step 04 单击“检查更新”按钮，开始检查是否存在有更新文件，如图2-27所示。

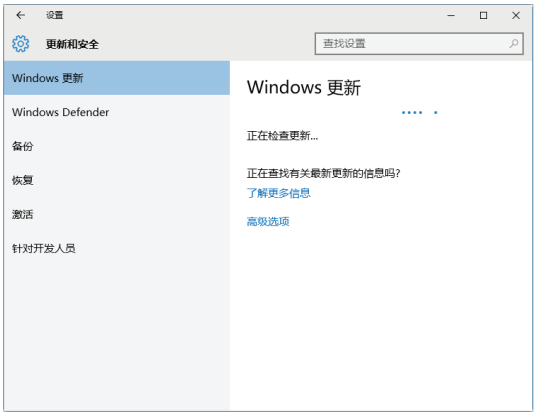

图 2-27　查询更新文件

Step 05 检查完毕后，如果存在更新文件，则会弹出如图2-28所示的信息提示，提示用户有可用更新，并自动开始下载更新文件。

图 2-28　下载更新文件

Step 06 下载完成后，系统会自动安装更新文件，安装完毕后，会弹出如图2-29所示的信息提示框。

Step 07 单击“立即重新启动”按钮，立即重新启动计算机，重新启动完毕后，再次打开“Windows更新”窗口，可以看到“你的设备已安装最新的更新”信息提示，如图2-30所示。

Step 08 单击“高级选项”超链接，打开“高级选项”设置工作界面，在其中可以选择安装更新的方式，如图2-31所示。

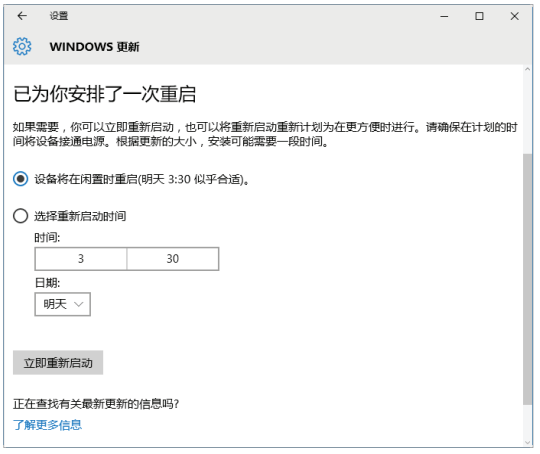

图 2-29　自动安装更新文件

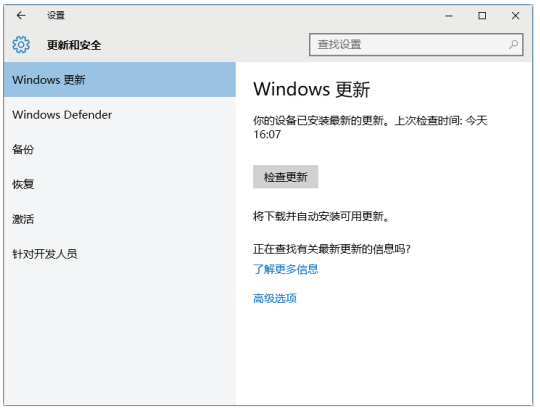

图 2-30　完成系统更新

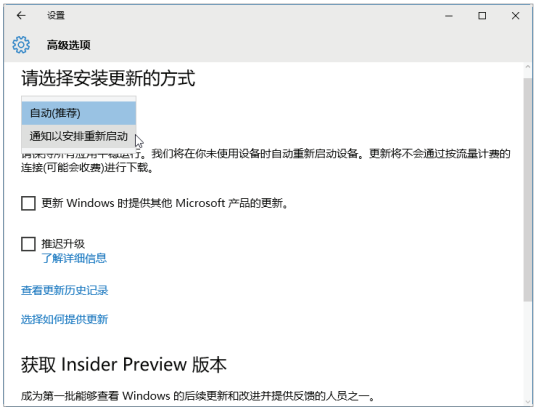

图 2-31　选择更新方式

2.3.2　实战2：修补系统漏洞后手动重启

一般情况下，在Windows10每次自动下载并安装好补丁后，就会每隔10分钟弹

出窗口要求重新启动。如果不小心单击了“立即重新启动”按钮，则有可能会影响当前计算机操作的资料。那么如何才能不让Windows10安装完补丁后自动弹出“重新启动”的信息提示框呢？具体的操作步骤如下。

Step 01 单击“ ”按钮，在弹出的快捷菜单中选择“所有程序”→“附件”→“运行”菜单命令，弹出“运行”对话框，在“打开”文本框中输入“gpedit.msc”，如图2-32所示。

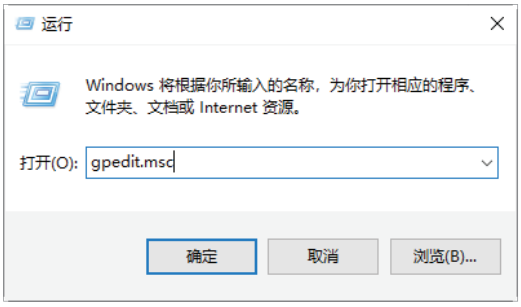

图 2-32　“运行”对话框

Step 02 单击“确定”按钮，打开“本地组策略编辑器”窗口，如图2-33所示。

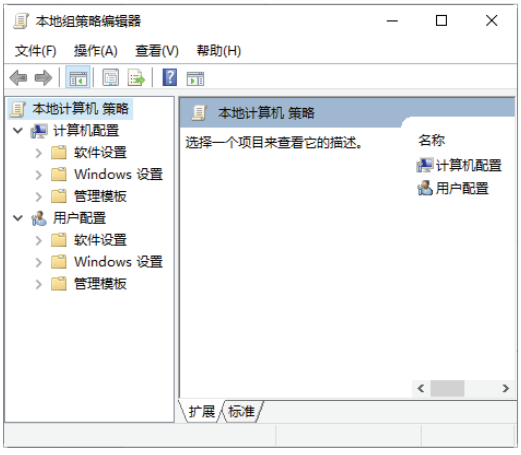

图 2-33　“本地组策略编辑器”窗口

Step 03 在窗口的左侧依次单击“计算机配置”→“管理模板”→“Windows 组件”选项，如图2-34所示。

Step 04 展开“Windows 组件”选项，在其子菜单中选择“Windows 更新”选项。此时，在右侧的窗格中将显示Windows更新的所有设置，如图2-35所示。

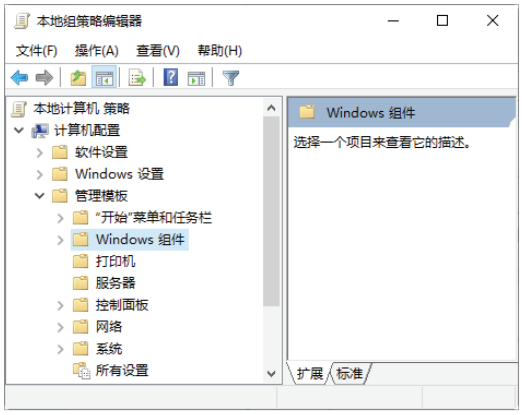

图 2-34　“Windows 组件”选项

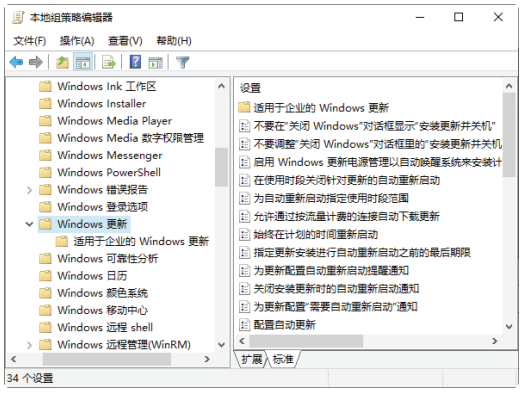

图 2-35　“Windows 更新”选项

Step 05 在右侧的窗格中选中“对于有已登录用户的计算机，计划的自动更新安装不执行重新启动”选项并右击，在弹出的快捷菜单中选择“编辑”菜单项，如图2-36所示。

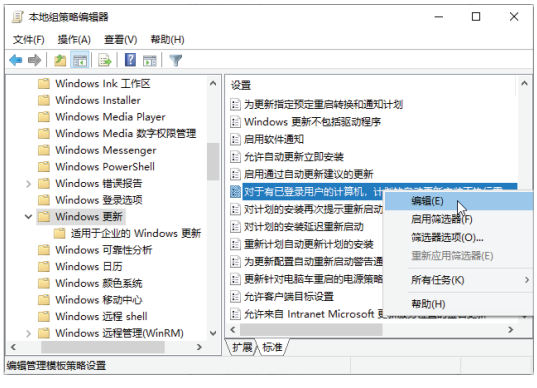

图 2-36　“编辑”选项

Step 06 打开“对于有已登录用户的计算机，计划的自动更新安装不执行重新启动”对话框，在其中选中“已启用”单选按钮，如图2-37所示。

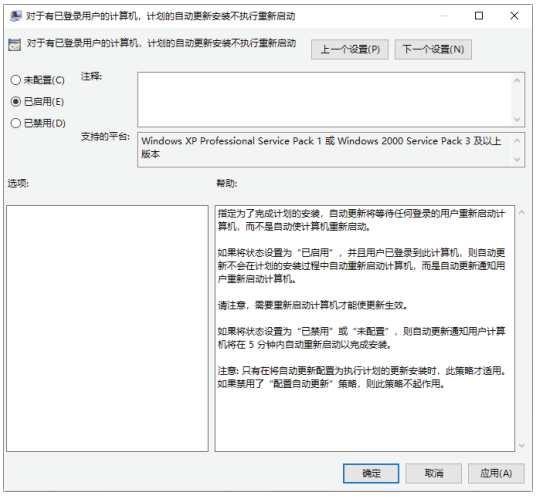

图 2-37 “已启用”单选按钮

Step 07 单击“确定”按钮，返回“组策略编辑器”窗口，此时用户可看到“对于有已登录用户的计算机，计划的自动更新安装不执行重新启动”选择的状态是“已启用”。这样，在自动更新完补丁后，将不会再弹出重新启动计算机的信息提示框，如图2-38所示。

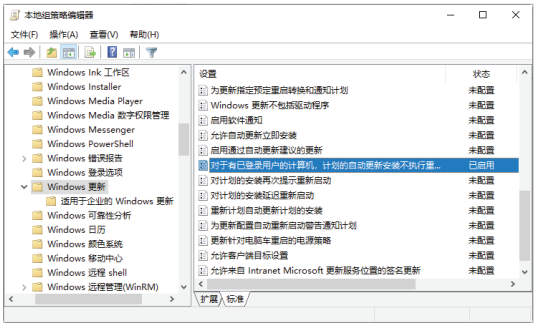

图 2-38 “已启用”状态

第3章　常见DOS命令的应用

作为计算机或网络终端设备的用户，要想使自己的设备不受或少受网络的攻击，有必要了解一些计算机中的基础知识，本章就来认识Windows系统中常见的DOS命令与批处理的应用。

3.1　常见DOS命令

熟练掌握一些DOS命令的应用是一名黑客的基本功，通过这些DOS命令可以帮助计算机用户追踪黑客的踪迹。

3.1.1　ipconfig命令

在互联网中，一台主机只有一个IP地址，因此，黑客要想攻击某台主机，必须找到这台主机的IP地址，然后才能进行入侵攻击。可以说，IP地址是黑客实施入侵攻击的一个关键。使用ipconfig命令可以获取本地计算机的IP地址，具体的操作步骤如下。

Step 01 单击“”按钮，在弹出的快捷菜单中执行“运行”命令，如图3-1所示。

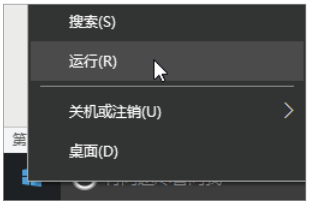

图 3-1　“运行”菜单

Step 02 打开“运行”对话框，在“打开”后面的文本框中输入cmd命令，如图3-2所示。

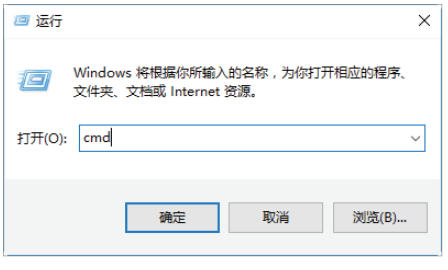

图 3-2　输入 cmd 命令

Step 03 单击“确定”按钮，打开“命令提示符”窗口，在其中输入ipconfig，按Enter键即可显示出本机的IP配置相关信息，如图3-3所示。

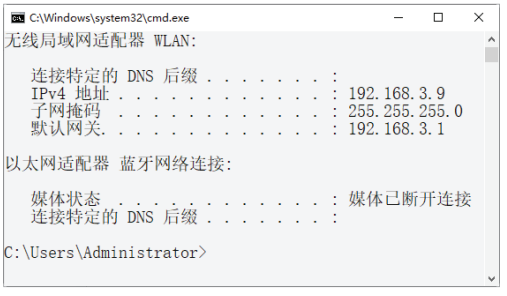

图 3-3　查看 IP 地址

提示：在“命令提示符”窗口中，192.168.3.9表示本机在局域网中的IP地址。

如果在“命令提示符”窗口中输入ipconfig /all命令，按Enter键，可以在显示的结果中看到一个物理地址：00-23-24-DA-43-8B，这就是本机的物理地址，也是本机的网卡地址，它是唯一的，如图3-4所示。

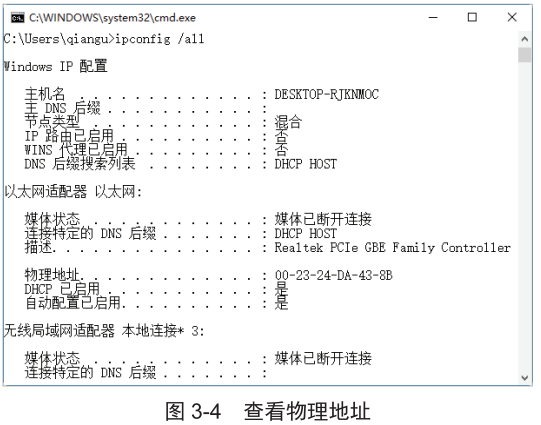

图 3-4　查看物理地址

3.1.2 TaskList命令

利用Tasklist命令可以查看本机中的进程，还可查看每个进程提供的服务。下面将介绍使用Tasklist命令的具体操作步骤。

Step 01 在“命令提示符”中输入Tasklist命令，按Enter键即可显示本机的所有进程，如图3-5所示。在显示结果中可以看到映像名称、PID、会话名、会话#和内存使用5部分。

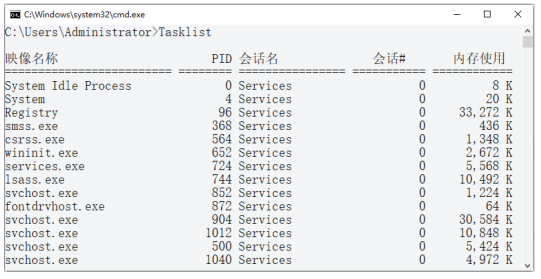

图 3-5 查看本机进程

Step 02 Tasklist命令不但可以查看系统进程，而且可以查看每个进程提供的服务。例如，要查看本机进程svchost.exe提供的服务，在命令提示符下输入“Tasklist /svc”命令即可，如图3-6所示。

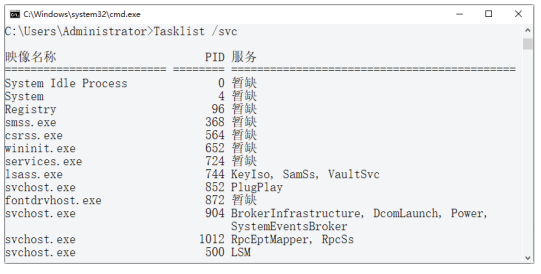

图 3-6 查看本机进程 svchost.exe 提供的服务

Step 03 要查看本地系统中哪些进程调用了shell32.dll模块文件，只需在命令提示符下输入“Tasklist /m shell32.dll”即可显示这些进程的列表，如图3-7所示。

Step 04 使用筛选器可以查找指定的进程，在命令提示符下输入TASKLIST /FI "USERNAME ne NT AUTHORITY\SYSTEM" /FI "STATUS eq running命令，按Enter键即可列出系统中正在运行的非System状态的所有进程，如图3-8所示。其中“/FI”为筛选器参数，ne和eq为关系运算符“不相等”和“相等”。

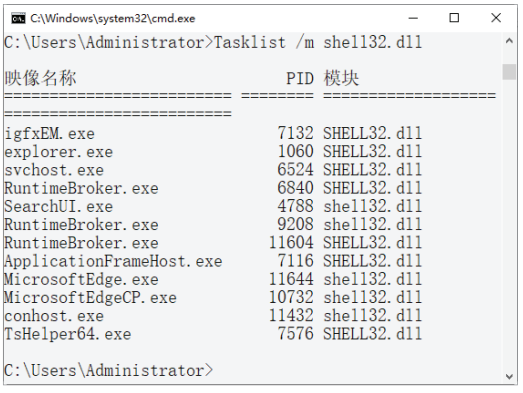

图 3-7 显示调用 shell32.dll 模块的进行

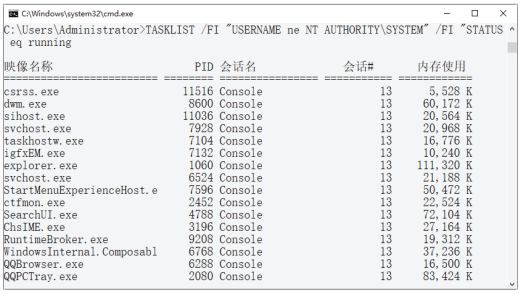

图 3-8 列出系统中正在运行的非 System 态的所有进程

3.1.3 Copy命令

Copy命令的主要作用是复制一个或多个文件到指定的位置，该命令可以被用于合并文件。使用Copy命令复制文件的操作步骤如下。

Step 01 同一磁盘上相同扩展名文件的复制，在“命令提示符”窗口中输入命令copy 123.doc 456.doc/a，按Enter键后，显示“覆盖456.doc吗？<Yes/No/All>:”信息，这里输入“y”，即可显示已复制信息，如图3-9所示。

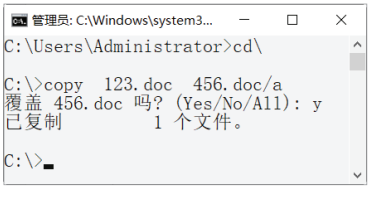

图 3-9 相同扩展名文件的复制

Step 02 从当前驱动器的当前目录复制文件，

例如复制C盘下的“bird.jpg”文件到C盘birds文件夹下，输入命令“copy bird01.jpg c:\birds”，运行结果如图3-10所示。

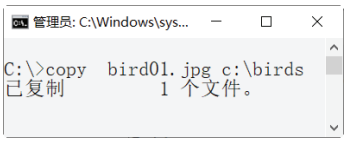

图 3-10　复制文件到文件夹

Step 03 Copy命令先将所有扩展名为.txt的文件合并到名为gushi.doc文件，然后再将所有扩展名为.xls的文件合并到gushi.doc文件，最后再将所有扩展名为.ppt的文件合并到名为gushi.doc文件中，输入命令“copy *.txt+*.xls+*.ppt gushi.doc”，运行结果如图3-11所示。

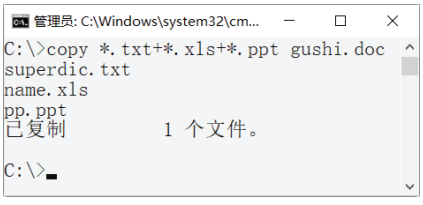

图 3-11　不同类型文件合并复制

Step 04 Copy命令把键盘上的输入复制到shuru.txt文件，输入命令“copy con shuru.txt”，按“CTRL+Z”组合键，屏幕上显示“Z”，表示结束输入复制操作，也可以按F6键，结束输入复制操作，运行结果如图3-12所示。

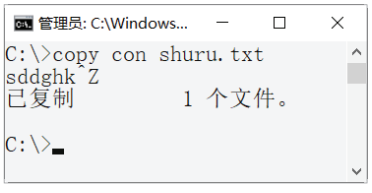

图 3-12　键盘输入内容复制

3.1.4　Del命令

Del即Delete（删除）的缩写，该命令的作用是删除文件，因此使用Del命令可以在“命令提示符”窗口中删除文件夹或文件，使用Del命令删除文件的具体操作步骤如下。

Step 01 如果想删除当前目录下的123.doc文件，可在“命令提示符”窗口中输入“del 123.doc”命令，按Enter键即可就删除该文件，如图3-13所示。

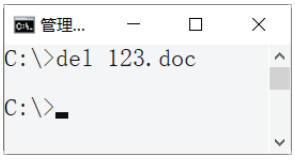

图 3-13　删除当前目录下的文件

Step 02 要删除一类文件，可以使用通配符。例如，“del *.jpg”命令就是把所有扩展名是jpg的文件都删除，如图3-14所示。

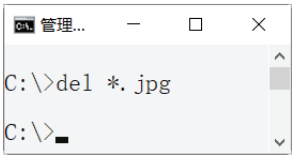

图 3-14　删除同类型文件

Step 03 如果要删除当前目录中的所有文件，可在“命令提示符”窗口中输入“del *.*”命令，按Enter键即可看到是否删除文件的提示信息，如图3-15所示。

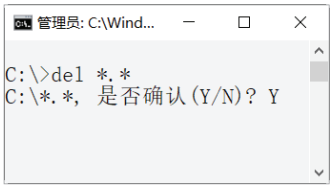

图 3-15　输入删除所有文件命令

Step 04 如果不想删除文件，则输入N，如果确定要删除，则输入Y即可成功删除当前目录下的文件，如图3-16所示。

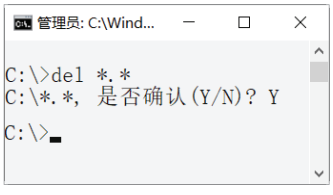

图 3-16　删除当前目录下的文件

Step 05 Del命令还可以删除非当前目录中的文件，输入“del d:\name.xls”命令，按

Enter键即可把D盘上name.xls文件删除，如图3-17所示。

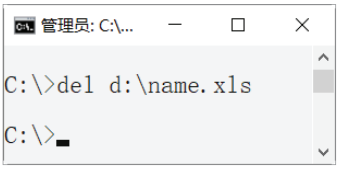

图 3-17　删除非当前目录中的文件

注意：“del *.*”或“del.”命令一般用于在删除子目录之前，先删除目录中的所有文件。但在删除文件之前，最好先确定该文件是否有用，以避免造成不必要的损失。

3.1.5　Arp命令

Arp命令是黑客和网络管理员都常用的命令，通过该命令可以进行IP地址和MAC地址欺骗，还可以使用该命令来修改ARP缓存表。具体操作步骤如下。

Step 01 想要显示所有接口的ARP缓存表，则在“命令提示符”窗口中输入“arp -a”命令，按Enter键后，其运行结果如图3-18所示。

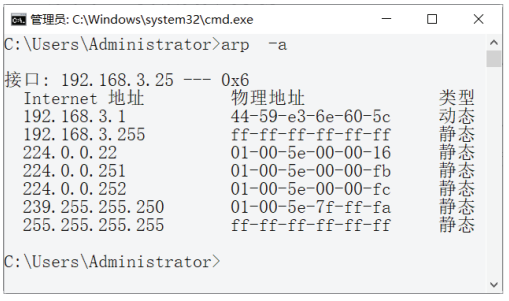

图 3-18　显示所有接口的 ARP 缓存表

Step 02 想要添加将IP地址169.254.85.214解析成物理地址00-AA-00-4F-2A-9C的静态ARP缓存项，可在“命令提示符”窗口中输入命令“arp –s 169.254.85.214 00-AA-00-4F-2A-9C”，按Enter键既可，如图3-19所示。

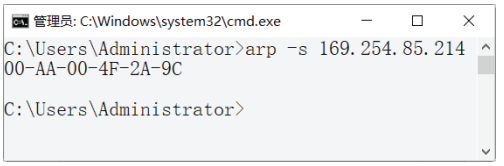

图 3-19　解析 IP 地址为物理地址

3.1.6　ping命令

ping命令是协议TCP/IP中最为常用的命令之一，主要用来检查网络是否通畅或者网络连接的速度。对于一名计算机用户来说，ping命令是第一个必要掌握的网络命令。在“命令提示符”窗口中输入ping /?，可以得到这条命令的帮助信息，如图3-20所示。

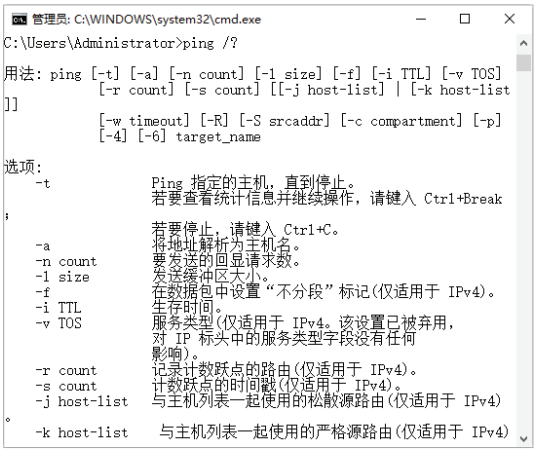

图 3-20　ping 命令帮助信息

使用ping命令对计算机的连接状态进行测试的具体操作步骤如下。

Step 01 使用ping命令来判断计算机的操作系统类型。在“命令提示符”窗口中输入“ping 192.168.3.9”命令，运行结果如图3-21所示。

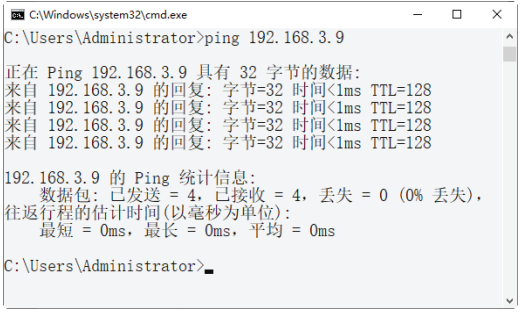

图 3-21　判断计算机的操作系统类型

Step 02 在“命令提示符”窗口中输入“ping 192.168.3.9 –t –l 128”命令，可以不断向某台主机发出大量的数据包，如图3-22所示。

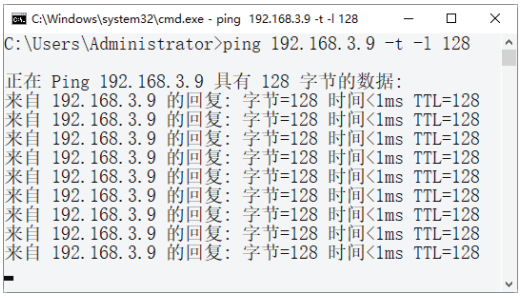

图 3-22　发出大量数据包

Step 03 判断某台计算机是否与外界网络连通，可在“命令提示符”窗口中输入“ping www.baidu.com”命令，其运行结果如图3-23所示，图中说明该计算机与外界网络连通。

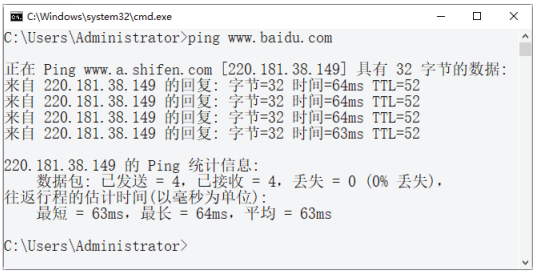

图 3-23　网络连通信息

Step 04 解析某IP地址的计算机名。在“命令提示符”窗口中输入“ping -a 192.168.3.9”命令，其运行结果如图3-24所示，可知这台主机的名称为SD-20220314SOIE。

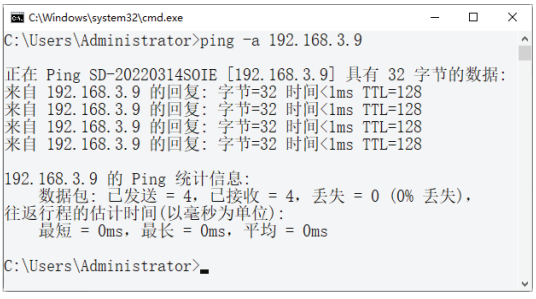

图 3-24　解析某 IP 地址的计算机名

3.1.7　net命令

使用net命令可以查询网络状态、共享资源及计算机所开启的服务等，使用net命令查询某台计算机开启哪些Windows服务的具体操作步骤如下。

Step 01 使用net命令查看网络状态。打开“命令提示符”窗口，输入net start命令，如图3-25所示。

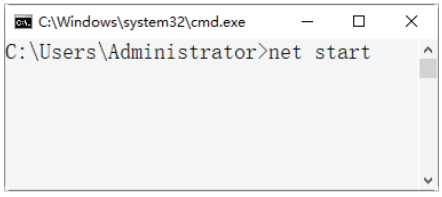

图 3-25　输入 net start 命令

Step 02 按Enter键，在打开的“命令提示符”窗口中可以显示计算机所启动的Windows服务，如图3-26所示。

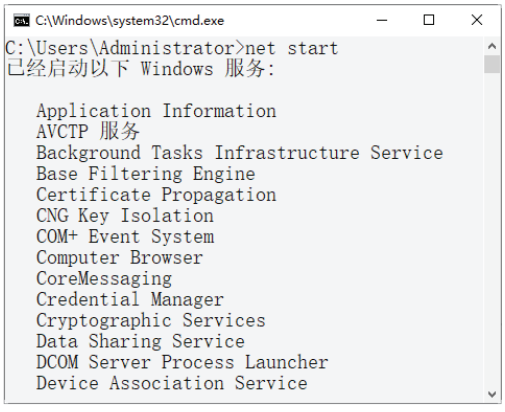

图 3-26　计算机所启动的 Windows 服务

3.1.8　netstat命令

netstat命令主要用来显示网络连接的信息，包括显示活动的TCP连接、路由器和网络接口信息，是一个非常有用的TCP/IP网络监控工具，可以让用户知晓系统中目前都有哪些网络连接正常。在“命令提示符”窗口中输入netstat/?，可以得到这条命令的帮助信息，如图3-27所示。

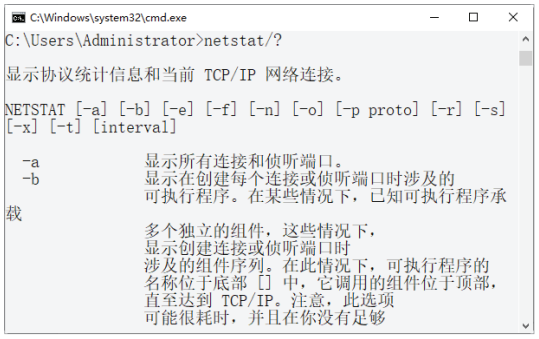

图 3-27　netstat 命令帮助信息

该命令的语法格式信息如下：

```
    NETSTAT [-a] [-b] [-e] [-n] [-o] [-p
proto] [-r] [-s] [-v] [interval]
```

其中比较重要的参数的含义如下。

（1）-a：显示所有连接和监听端口；

（2）-n：以数字形式显示地址和端口号。

使用netstat命令查看网络连接的具体操作步骤如下。

Step 01 打开“命令提示符”窗口，在其中输入netstat -n或netstat命令，按Enter键即可查看服务器活动的TCP/IP连接，如图3-28所示。

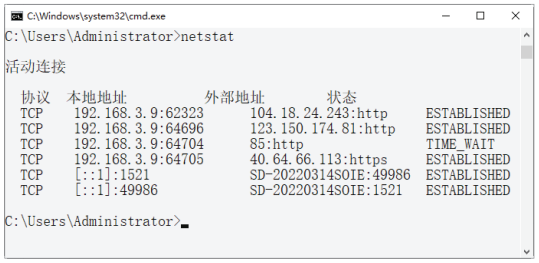

图 3-28　服务器活动的 TCP/IP 连接

Step 02 在“命令提示符”窗口中输入netstat -r命令，按Enter键即可查看本机的路由信息，如图3-29所示。

Step 03 在“命令提示符”窗口中输入netstat -a命令，按Enter键即可查看本机所有活动的TCP连接，如图3-30所示。

Step 04 在“命令提示符”窗口中输入netstat -n -a命令，按Enter键即可显示本机所有连接的端口及其状态，如图3-31所示。

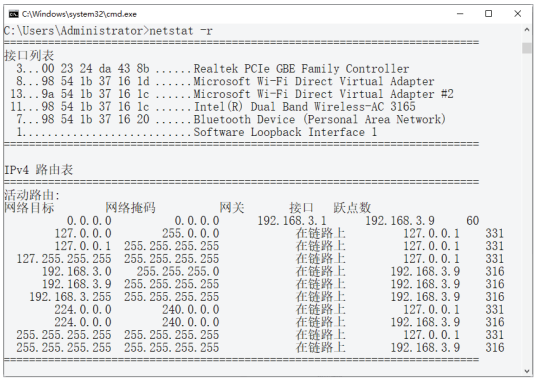

图 3-29　查看本机路由信息

图 3-30　查看本机活动的 TCP 连接

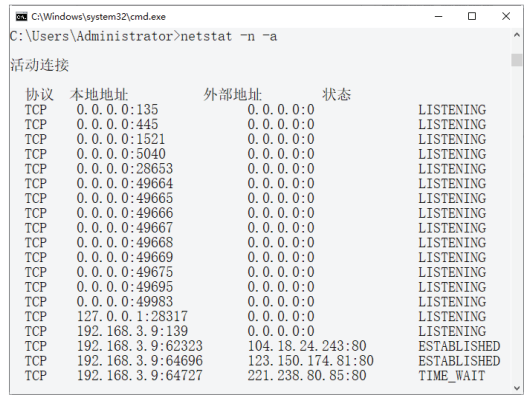

图 3-31　查看本机连接的端口及其状态

3.1.9　tracert命令

使用tracert命令可以查看网络中路由节点信息，最常见的使用方法是在tracert命令后追加一个参数，表示检测和查看连接当前主机经历了哪些路由节点，适合用于

大型网络的测试，该命令的语法格式信息如下。

```
    tracert [-d] [-h MaximumHops] [-j
Hostlist] [-w Timeout] [TargetName]
```

其中各个参数的含义如下。

（1）-d：防止解析目标主机的名字，可以加速显示tracert命令结果。

（2）-h MaximumHops：指定搜索到目标地址的最大跳跃数，默认为30个跳跃点。

（3）-j Hostlist：按照主机列表中的地址释放源路由。

（4）-w Timeout：指定超时时间间隔，默认单位为毫秒。

（5）TargetName：指定目标计算机。

例如，如果想查看www.baidu.com的路由与局域网络连接情况，可在“命令提示符”窗口中输入tracert www.baidu.com命令，按Enter键，其显示结果如图3-32所示。

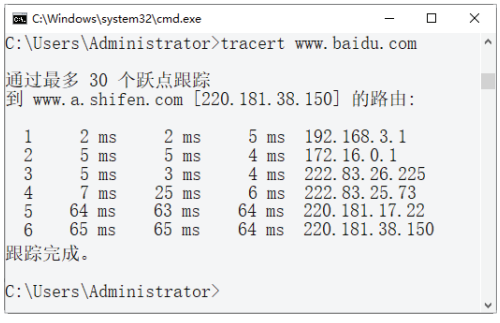

图 3-32　查看网络中路由节点信息

3.1.10　route命令

route命令主要的作用是手动配置路由表，在本地IP路由表中显示和修改条目，它是网络管理工作中应用较多的工具，使用不带参数的route可以显示其帮助信息，如图3-33所示。

使用route命令显示路由表中当前项目的方法比较简单，在“命令提示符”窗口中输入Route　print，按Enter键即可显示当前路由表信息，如图3-34所示。

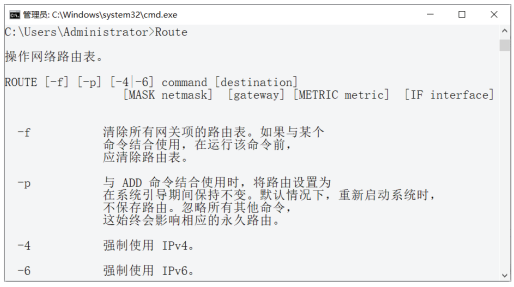

图 3-33　显示其帮助信息

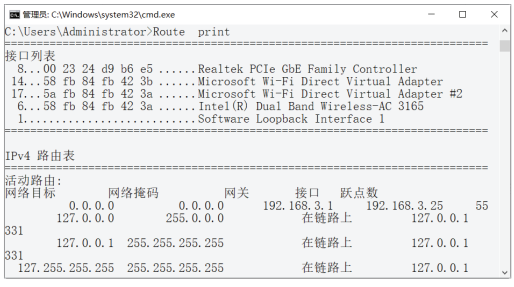

图 3-34　显示路由表中的当前项目

若想要显示IP路由表中以192开始的路由，可在命令提示符下输入“Route print 192.*”，按Enter键，运行结果显示如图3-35所示。

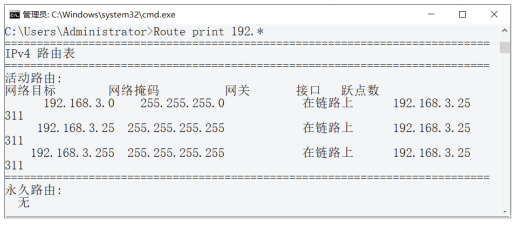

图 3-35　显示 IP 路由表中以 192 开始的路由信息

3.2　批处理的应用

批处理是一种简化的脚本语言，应用于DOS和Windows系统中，可以对某对象进行批量处理，批处理文件扩展名为.bat。

3.2.1　Echo命令

使用Echo命令可以打开/关闭请求回显功能，查看Echo状态的方法比较简单，在“命令提示符”窗口中输入echo命令，按Enter键即可，如图3-36所示。

图 3-36　查看状态

在批处理文件运行时，屏幕上没有显示文件中的命令，主要是因为用了Echo命令，在批处理文件的首行加上Echo off命令，即@ echo off，这样就可以禁止批处理程序中的命令正文显示到屏幕上。

如果只想让某一行的命令显示在屏幕上，这时可以在这一行命令的前面加上Echo命令。例如，要显示暂停命令pause执行时的状态，则需要在批处理中的pause命令前加上Echo，即：echo pause，这样，当执行到pause命令时，就会在屏幕上显示出pause命令状态。如果需要显示hello world文字信息，则使用“echo hello world”语句，如图3-37所示。

图 3-37　查看回显内容

3.2.2　清除系统垃圾

使用批处理文件可以快速地清除计算机中的垃圾文件，下面将介绍使用批处理文件清除系统垃圾文件的具体步骤。

Step 01 打开记事本文件，在其中输入可以清除系统垃圾的代码，输入的代码如下：

```
    @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%\*._mp
    del/f/s/q%systemdrive%\*.log
    del/f/s/q%systemdrive%\*.gid
    del/f/s/q%systemdrive%\*.chk
    del/f/s/q%systemdrive%\*.old
    del/f/s/q%systemdrive%\recycled\*.*
    del/f/s/q%windir%\*.bak
    del/f/s/q%windir%\prefetch\*.*
    rd/s/q%windir%\temp & md %windir%\
temp
    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!
    echo.&pause
```

将上面的代码保存为del.bat，如图3-38所示。

图 3-38　编辑代码

Step 02 在“命令提示符”窗口中输入“del.bat”命令，按Enter键，就可以快速清理系统垃圾，如图3-39所示。

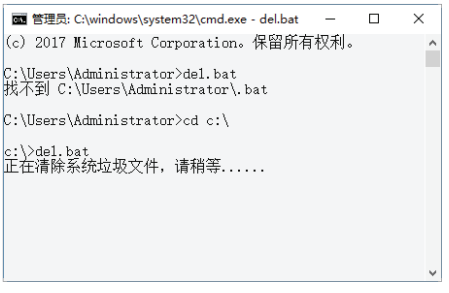

图 3-39　自动清理垃圾

3.3　实战演练

3.3.1　实战1：使用命令清除系统垃圾

使用批处理文件可以快速地清除计算机中的垃圾文件，下面将介绍使用批处理文件清除系统垃圾文件的具体步骤。

Step 01 打开记事本文件，在其中输入可以清

除系统垃圾的代码，输入的代码如下：

```
    @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%\*._mp
    del/f/s/q%systemdrive%\*.log
    del/f/s/q%systemdrive%\*.gid
    del/f/s/q%systemdrive%\*.chk
    del/f/s/q%systemdrive%\*.old
    del/f/s/q%systemdrive%\recycled\*.*
    del/f/s/q%windir%\*.bak
    del/f/s/q%windir%\prefetch\*.*
    rd/s/q%windir%\temp & md %windir%\
temp
    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!
    echo.&pause
```

将上面的代码保存为del.bat，如图3-40所示。

图 3-40　编辑代码

Step 02 在“命令提示符”窗口中输入“del.bat”命令，按Enter键，就可以快速清理系统垃圾，如图3-41所示。

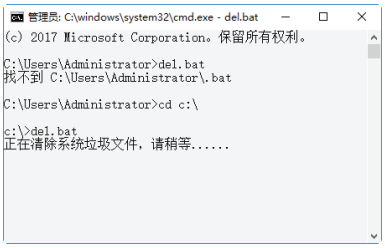

图 3-41　自动清理垃圾

3.3.2　实战2：使用命令实现定时关机

使用shutdown命令可以实现定时关机的功能，具体操作步骤如下。

Step 01 在“命令提示符”窗口中输入shutdown/s /t 40命令，如图3-42所示。

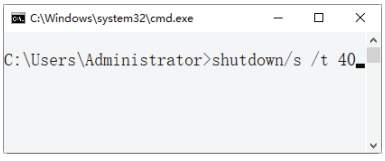

图 3-42　输入 shutdown/s /t 40 命令

Step 02 弹出一个即将注销用户登录的信息提示框，这样计算机就会在规定的时间内关机，如图3-43所示。

图 3-43　信息提示框

Step 03 如果此时想取消关机操作，可在命令行中输入命令shutdown /a后按Enter键，桌面右下角出现如图3-44所示的弹窗，表示取消成功。

图 3-44　取消关机操作