实验 1_网络相关进程与服务实验

学生姓名:林觉凯　　合作同学:无

实验地点:济事楼 330　　实验时间:2024.2.26

【实验目的】

本实验的主要目的是利用操作系统的任务管理器来获得用户计算机上正在运行的程序和进程的相关信息，并且利用任务管理器来监视计算机性能。利用任务管理器可以快速查看正在运行的程序的状态、终止已停止相应的程序、评估正在运行的进程的活动和 CPU、内存使用情况的图形和数据。通过具体的实践操作，让学生对网络相关进程有进一步的理解，熟悉任务管理器的基本操作。

【实验原理】

操作系统的任务管理器提供了用户计算机上正在运行的程序和进程的相关信息，也显示了最常用的度量进程性能的单位。可以通过 ctrl＋alt＋delete 打开任务管理器图形界面执行进程管理操作，也可以通过命令的方式完成图形界面同样的功能，任务管理器主要对应的命令有：

1.Task list 命令：用于显示运行在本地或远程计算机上所有任务的应用。

2.Taskkill 命令：用于结束一个或多个任务或进程。可以根据进程 ID 或图像名来结束进程。

3.Tskill 命令：功能同 Taskkill 命令，用于结束一个或多个进程。

网络进程与一般进程具有基本相同的属性，唯一不同的特性是网络进程而要开启 1 到多个传输端口号。一般来说，对于 C/S 或 B/S 架构的网络，用户端网络进程至少需要开启 1 个端口号，用于接收数据或发送数据。服务端网络进程则可能至少开启 2 个端口号，1 个用于接受客户端的数据，1 个用于发送数据给客户，在 Windows 系统中，可以使用相关命令查看正在使用的端口号。

系统服务(Windows 服务)是主要用于为内部进程服务而长期运行的一周特殊进程(应用程序)，这类进程不需要有用户界面或打开任何模拟输出。任何的用户消息通常都是记录在 Windows 事件日志里。系统服务可以在操作系统启动的时候开始，且一直在后台运行，当有需要时也可以手动启动，我们可以通过管理工具里的服务进行统一管理。

【实验设备】

实验硬件:济事楼 330 机房电脑和本人笔记本电脑

实验软件:Windows 操作系统

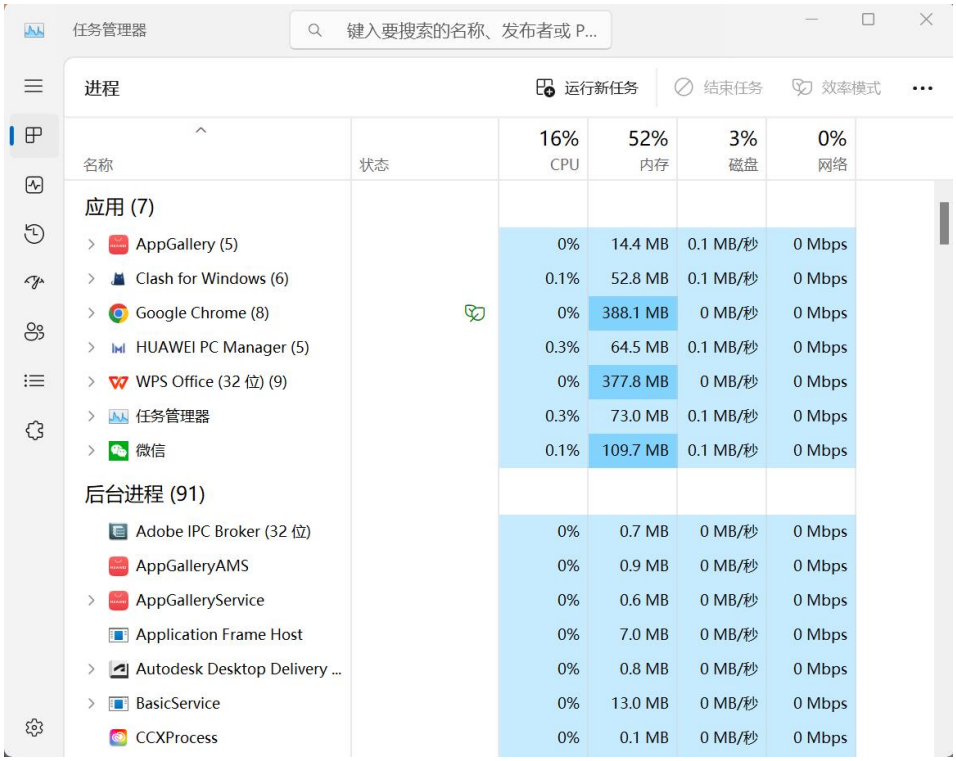
【实验步骤】

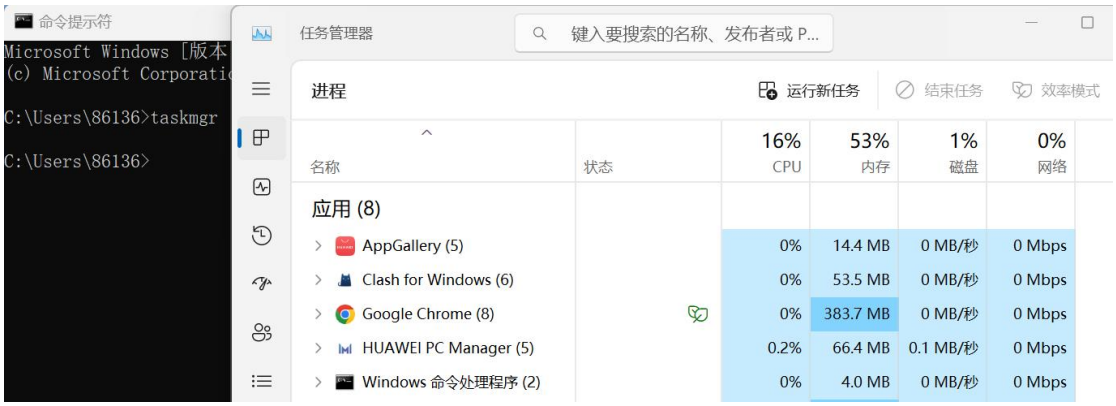
进程管理的显示：启动并进入 Windows 环境，单击 Ctrl +Alt + Del 键，选择“任务管理器”，或者右键点击任务栏，在快捷菜单“任务管理器”命令，或者通过命令 taskmgr 打开“任务管理器”窗口。在 CMD 界面，通过 Tasklist、Taskkill、Tskill 及相应的程序命令对进程进行管理。

在实验中通过界面打开记事本、word、写字板、画图、计算器等五个应用程序，并通过界面和命令显示和关闭其中几个应用程序，记录操作过程和结果。

【实验现象】

按下 ctrl+alt+delete 或者通过命令 taskmgr 打开“任务管理器”窗口，如下图：





打开 cmd，在 cmd 中执行 tasklist 命令：

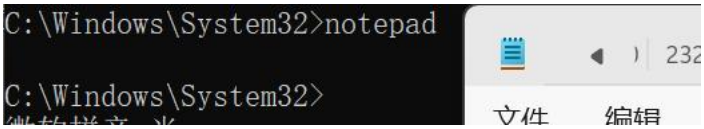
```
C:\Users\86136>tasklist

映像名称                       PID 会话名              会话#       内存使用
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0          8 K
System                           4 Services                   0        152 K
Registry                       240 Services                   0     56,664 K
smss.exe                       692 Services                   0      1,120 K
csrss.exe                      968 Services                   0      6,960 K
wininit.exe                    772 Services                   0      7,284 K
services.exe                  1040 Services                   0     19,084 K
lsass.exe                     1064 Services                   0     58,912 K
svchost.exe                   1188 Services                   0     68,532 K
fontdrvhost.exe               1216 Services                   0      3,608 K
WUDFHost.exe                  1252 Services                   0     23,240 K
svchost.exe                   1320 Services                   0     49,048 K
svchost.exe                   1380 Services                   0     21,628 K
WUDFHost.exe                  1432 Services                   0      7,748 K
WUDFHost.exe                  1500 Services                   0      7,584 K
WUDFHost.exe                  1568 Services                   0     21,904 K
svchost.exe                   1876 Services                   0     20,164 K
svchost.exe                   1892 Services                   0     20,584 K
svchost.exe                   1908 Services                   0     28,000 K
svchost.exe                   1928 Services                   0     31,296 K
svchost.exe                   2016 Services                   0     23,652 K
svchost.exe                    880 Services                   0     37,512 K
svchost.exe                   1604 Services                   0     22,992 K
svchost.exe                    864 Services                   0     20,184 K
svchost.exe                   1640 Services                   0     34,548 K
svchost.exe                   2204 Services                   0     19,092 K
svchost.exe                   2212 Services                   0     34,632 K
```

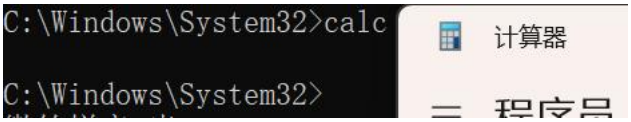
在 cmd 中使用 taskkill 命令来终止一个运行中的进程：

```
C:\Windows\System32>taskkill /pid 8944 /F
成功: 已终止 PID 为 8944 的进程。
```

在 cmd 中打开记事本：



在 cmd 中打开计算器：



在 cmd 中打开写字板：

在 cmd 中打开画图：

在 cmd 中给记事本进程发送终止信号并强制终止该进程：

【分析讨论】

1.用你的语言简单解释进程和网络进程的含义

进程是计算机系统中运行中的程序的实例。每个进程都有自己独立的内存空间和资源，可以被操作系统调度和管理。进程是程序的执行实体，可以执行各种操作，如分配资源、执行指令等。一个操作系统可以同时运行多个进程，每个进程分别进行不同的任务。每个进程通常是隔离的，一个进程崩溃一般不会影响到其他进程。

网络进程是指在网络环境中运行的进程，它们通过网络进行通信和交互。网络进程可以在不同计算机上运行，通过网络连接进行数据交换和协作。这些进程通过网络协议来进行通信，这可以是客户端进程或服务器进程。

2.任务管理器的启动和使用

任务管理器的常见启动方法一般来说如下：通过按下键盘快捷 ctrl+alt+delete 来启动任务管理器；通过在 cmd 命令行中输入 taskmgr 命令进行任务管理器的启动。在使用任务管理器方面，可以在其中获取到每一个进程各个方面的信息，从而更加直观、方便地管理。

3.显示有关服务的命令，图形和命令

图形：

图形用户界面是一种通过图形元素和鼠标操作来控制计算机的界面。

优点：直观易用：提供了直观的可视化界面，用户可以通过操作完成任务，降低了学习成本。可视化：通过图形界面，用户可以看到操作结果和反馈，更容易理解系统的状态和功能。操作便捷：提供了大量的快捷操作和可定制的选项。

缺点：资源消耗高：需要更多的系统资源，可能会导致系统运行速度变慢。不利于批量处理：对于需要批量处理的任务，它通常不如命令行方式高效，无法轻松实现自动化和脚本化操作。

命令行：

命令行命令是一种通过文本界面输入指令来控制计算机操作的方式。

优点：效率高：命令行命令通常比图形用户界面更快速，可以通过简单的命令完成任务。自动化：命令行命令可以被脚本化和自动化，能够轻松地批量处理任务和执行复杂操作。资源消耗低：相比图形用户界面，命令行界面通常占用更少的系统资源，适合在资源有限的环境下操作。

缺点：可读性较差：命令行输入的命令可能不直观，不如图形界面那样直观易懂。学习较难：对于不熟悉命令行的用户来说，学习使用命令行命令需要一定的时间和精力，可能会比较困难。

4.图形和命令方式启动和停止有关进程

用图形的方式打开和停止有关的进程方式为进入任务管理器，点击文件，运行新任务，输入相应新进程的名称；要停止有关进程则需要右击，在选择结束任务即可。用命令的方式打开和停止有关的进程方式为加入到 cmd 中，在命令行中输入相应的运行命令或者停止命令即可启动和停止有关进程。

实验 2_网络端口地址实验

学生姓名:林觉凯　　合作同学:无

实验地点:济事楼 330　　实验时间:2024.2.26

【实验目的】

端口指的是访问主机上的某一进程的标识符，通过端口实现了计算机之间进程之间的通信。当我们在浏览网页时，实际上是我们计算机上的浏览器这一进程与不同的网页服务器上的 Web 服务器程序之间在不同端口进行通信。这些正在运行的程序被称为网络进程。

网络进程与一般进程具有相似的特性，唯一不同的是，网络进程需要打开一个或多个传输端口，(传输层：0-65535，其中 0-1023 为保留端口号或系统端口)这些端口号被称为网络端口地址。

本实验目的是通过访问不同网络端口地址，观察浏览器访问网站时的行为；同时使用 netstat 命令检查端口状态，探究不同的端口对访问成功的影响。

【实验原理】

端口指的是访问主机上的某一进程的标识符。有关端口划分为：

0～1023：系统端口，这些端口只有系统特许的进程才能使用。

1024～65535 端口，用户端口；

1024～5000：临时端口，一般的应用程序使用 1024 到 4999 来进行通讯。

5001～65535：服务器端口，用来给用户自定义端口；

常用的 TCP，UDP 相关端口号如下：

DHCP：服务器端的端口号是 67；

DHCP：客户机端的端口号是 68；

POP3：POP3 接收协议，POP3 客户端使用 SMTP 向服务器发送邮件。POP3 使用的端口号是 110；

SMTP：端口号是 25，SMTP 真正关心的不是邮件如何被传送，而只关心邮件是否能顺利到达目的地；

Telnet：端口号 23 测试端口号，可以使用 telnet 命令来测试端口号是否正常打开还是关闭；

FTP：FTP 使用的端口号是 20 和 21。20 端口用于数据传输，21 端口用于控制信息的传输，控制信息和数据能够同时传输，这是 FTP 的特殊之处。

TFTP：端口号 69，使用 UDP 的连接 TFTP（Trivial File Transfer Protocol，简单文件传输协议）是 TCP/IP 协议族中的一个用来在客户机与服务器之间进行简单文件传输的协议，提供不复杂、开销不大的文件传输服务。

UDP 53 端口：DNS 域名解析服务；

TCP 80 端口：HTTP 超文本传输服务；

TCP 443 端口：HTTPS 加密的超文本传输。

【实验设备】

实验硬件:济事楼 330 机房电脑和本人笔记本电脑

实验软件:Windows 操作系统

【实验步骤】

在浏览器分别输入地址：

https://www.tongji.edu.cn:8080;

https://www.tongji.edu.cn:80;

http://www.tongji.edu.cn:8080;

http://www.tongji.edu.cn:80;

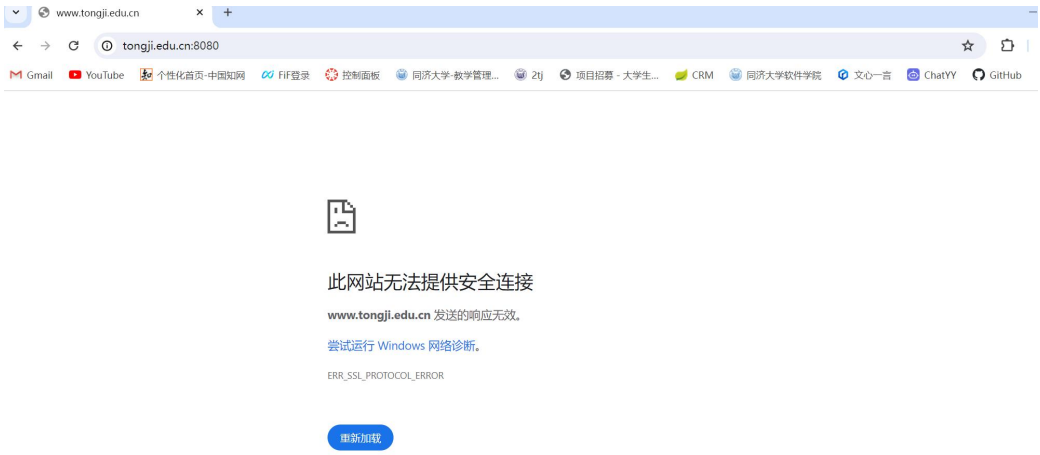
观察结果并分析。

进入 CMD 环境，输入命令：netstat -ano 观测。

【实验现象】

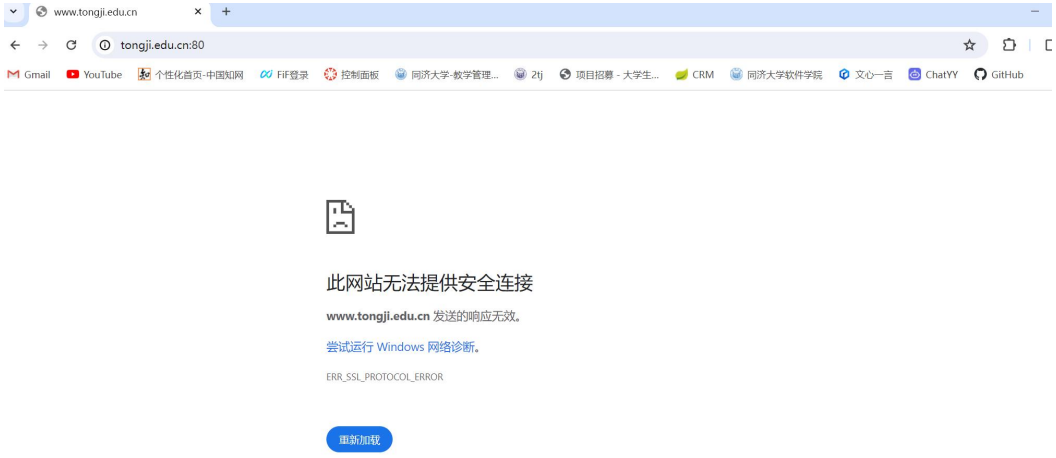
1. 在浏览器中输入地址 https://www.tongji.edu.cn:8080

这个地址使用 https 协议，并加上了自定义端口号 8080。但是 https 通常使用端口号 443，结果连接失败。



2.在浏览器中输入地址 https://www.tongji.edu.cn:80

这个地址使用 https 协议，并加上了系统标准端口号 80。但是 https 通常使用端口号 443，结果连接失败。



3.在浏览器中输入地址 http://www.tongji.edu.cn:8080

这个地址使用了 http 协议，并加上了自定义的端口号 8080。但是 http 通常使用端口 80，结果连接失败。

4.在浏览器中输入地址 http://www.tongji.edu.cn:80

这个地址使用了 http 协议，并加上了系统标准端口号 80，符合 http 的默认端口。结果连接成功。

进入 CMD 环境，输入命令：netstat -ano 观测。

输入命令，我们可以检查计算机上当前打开的端口状态 LISTEN(监听)、ESTABLISHED(已建立)、TIME_WAIT(等待期间)等等。

```
C:\Users\86136>netstat -ano

活动连接

  协议  本地地址          外部地址        状态           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1320
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       9708
  TCP    0.0.0.0:8082           0.0.0.0:0              LISTENING       23540
  TCP    0.0.0.0:28980          0.0.0.0:0              LISTENING       24796
  TCP    0.0.0.0:29034          0.0.0.0:0              LISTENING       24796
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       1064
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       772
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       2584
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING       3352
  TCP    0.0.0.0:49679          0.0.0.0:0              LISTENING       4344
  TCP    0.0.0.0:49688          0.0.0.0:0              LISTENING       1040
  TCP    100.81.193.62:139      0.0.0.0:0              LISTENING       4
  TCP    100.81.193.62:1667     202.120.190.208:53     TIME_WAIT       0
  TCP    100.81.193.62:1767     202.120.190.208:53     TIME_WAIT       0
  TCP    100.81.193.62:1774     121.194.10.213:443     TIME_WAIT       0
  TCP    100.81.193.62:1775     121.194.10.213:443     TIME_WAIT       0
  TCP    100.81.193.62:1776     122.205.109.49:443     TIME_WAIT       0
  TCP    100.81.193.62:1777     123.129.227.14:443     TIME_WAIT       0
  TCP    100.81.193.62:1779     43.141.11.229:443      TIME_WAIT       0
  TCP    100.81.193.62:1790     36.137.232.228:21011   TIME_WAIT       0
  TCP    100.81.193.62:1792     123.249.12.207:443     TIME_WAIT       0
  TCP    100.81.193.62:1795     36.137.232.228:21011   TIME_WAIT       0
  TCP    100.81.193.62:1808     36.137.232.228:21011   TIME_WAIT       0
  TCP    100.81.193.62:1810     220.181.174.166:443    TIME_WAIT       0
  TCP    100.81.193.62:1812     36.137.232.228:21011   TIME_WAIT       0
```

【分析讨论】

1.记录使用内容的过程：如上文所述。

2.举例相关端口号使用：以下是一些常见端口号及其使用：

端口 80 - HTTP (Hypertext Transfer Protocol)：Web 服务器,传输网页内容。

端口 443 - HTTPS(Hypertext Transfer Protocol Secure)：用于安全的 Web 通信。

端口 25 - SMTP(Simple Mail Transfer Protocol)：用于发送电子邮件。

端口 23 - Telnet：用于远程访问计算机，因为安全性问题，现在逐渐被 SSH 取代。

端口 110 - POP3(Post Office Protocol version 3)：用于接收电子邮件。

端口 143 - IMAP(Internet Message Access Protocol)：接收电子邮件，并提供更多的邮件管理功能。

端口 21 - FTP （File Transfer Protocol)：用于文件传输，允许用户上传和下载文件到服务器。

端口 22 - SSH(Secure Shell)：用于远程安全访问计算机，进行远程命令行操作。

端口 53 - DNS(Domain Name System)：用于将域名解析为 IP 地址。

端口 3306 - MySQL：用于访问、管理 MySQL 数据库。

端口 5432 - PostgreSQL：用于访问、管理 PostgreSQL 数据库。

端口 1521 - Oracle Database：用于访问、管理 Oracle 数据库。