

实验(一)：进程运行原理实验

一.实验目的

- 了解进程、网络进程和服务的基本概念
- 了解进程的基本运行原理，掌握基本进程管理技能
- 了解网络进程的特点
- 了解如何查看和管理系统服务

二.实验原理

1.基本概念

- 进程 (Process) 是计算机中程序在某数据集合上的一次运行活动，同时也是系统进行资源分配和调度的基本单位
- 网络进程: 一个与网络通讯相关的进程，它需要开启一个或多个传输端口进行数据的接收或发送
- 系统服务: 用于为内部进程提供服务的长期运行的特殊进程，无需用户界面,通常在后台运行

2.Windows任务管理器提供了计算机性能的相关信息，并展示了系统上运行的程序和进程的详细信息。通过任务管理器，用户可以查看活动程序的状态或关闭无响应的程序。与任务管理器相关的主要命令包括：

- `Tasklist` 命令：用来显示在本地或远程计算机上运行的所有任务的应用程序和服务列表，便于监控用户行为
- `Taskkill` 命令：用于终止一个或多个任务或进程，可以通过进程ID或程序名来指定要结束的进程

3.现代操作系统可以对进程实施管理

- **进程创建**：程序运行就成为进程，每个进程都分配唯一的一个进程编号，但进程编号并不固定
- **进程运行**：现代操作系统中允许同时运行多个进程，每个进程运行需要使用多种计算机部件资源，其中CPU资源是不可缺少的，当CPU核数量小于并发进程数量时，操作系统对CPU实施共享，将CPU运行时间划分成多个时间片，分配给各个进程提供运行，使所有进程都能同时运行
- **进程终止**：一般通过程序提供的退出按钮终止进程，也可以通过进程管理命令或软件结束进程

三.实验环境

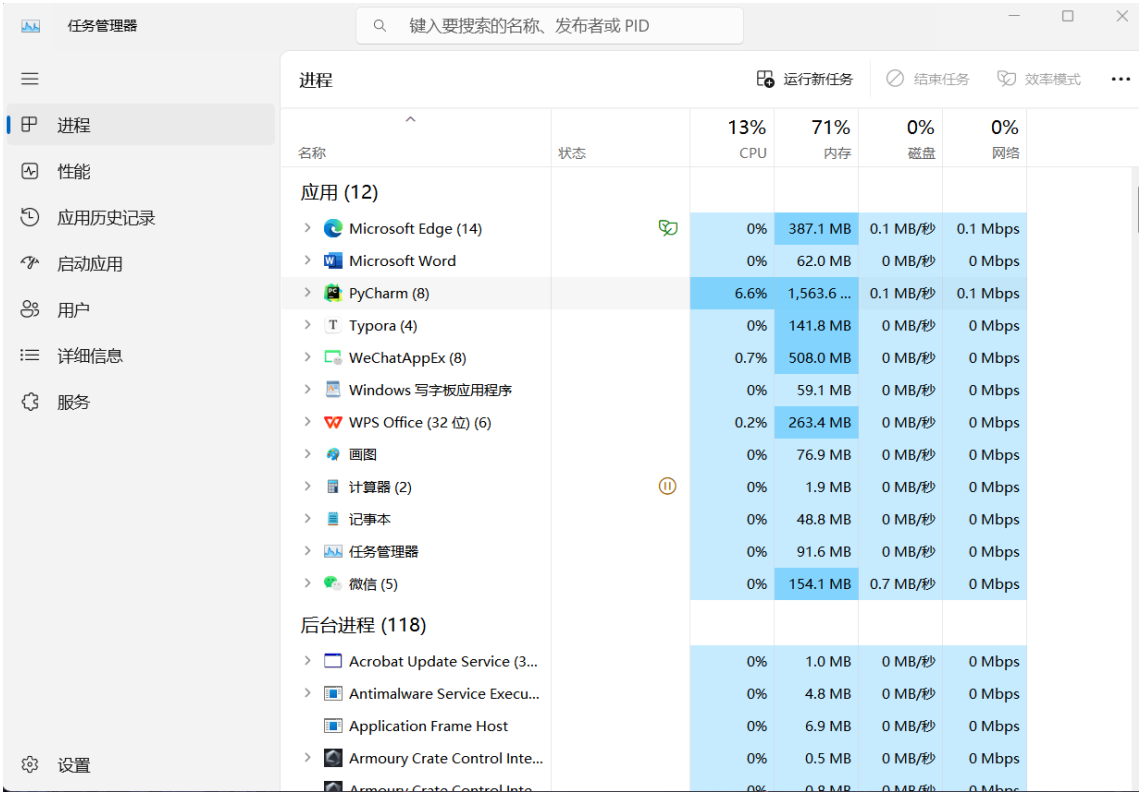
- 实验环境：Windows 11
- 相关软件：记事本、word、写字板、画图、计算器
- 网络环境：wifi连接

四.实验步骤

- 1.此实验将展示如何在Windows环境下管理进程。首先，通过按 `Ctrl` + `Alt` + `Del` 键组合并选择“任务管理器”来打开它，或者可以右键点击任务栏并选择“任务管理器”，还有一种方式是使用 `taskmgr` 命令来启动任务管理器。
- 2.在任务管理器中，观察“应用程序”和“进程”选项卡，注意CPU和内存的使用情况。
- 3.启动记事本、Word、写字板、画图、计算器等应用程序。
- 4.使用任务管理器和命令行工具(`Tasklist`, `Taskkill`)查看和管理进程。
- 5.使用命令 `services.msc` 查看系统服务。
- 6.记录实验观测的结果，现象和数据

五、实验现象

- 打开任务管理器，记事本、Word、写字板、画图、计算器等应用程序均有所显示



进程						
名称	状态	13% CPU	71% 内存	0% 磁盘	0% 网络	
应用 (12)						
> Microsoft Edge (14)		0%	387.1 MB	0.1 MB/秒	0.1 Mbps	
> Microsoft Word		0%	62.0 MB	0 MB/秒	0 Mbps	
> PyCharm (8)		6.6%	1,563.6 ...	0.1 MB/秒	0.1 Mbps	
> Typora (4)		0%	141.8 MB	0 MB/秒	0 Mbps	
> WeChatAppEx (8)		0.7%	508.0 MB	0 MB/秒	0 Mbps	
> Windows 写字板应用程序		0%	59.1 MB	0 MB/秒	0 Mbps	
> WPS Office (32 位) (6)		0.2%	263.4 MB	0 MB/秒	0 Mbps	
> 画图		0%	76.9 MB	0 MB/秒	0 Mbps	
> 计算器 (2)		0%	1.9 MB	0 MB/秒	0 Mbps	
> 记事本		0%	48.8 MB	0 MB/秒	0 Mbps	
> 任务管理器		0%	91.6 MB	0 MB/秒	0 Mbps	
> 微信 (5)		0%	154.1 MB	0.7 MB/秒	0 Mbps	
后台进程 (118)						
> Acrobat Update Service (3...		0%	1.0 MB	0 MB/秒	0 Mbps	
> Antimalware Service Execu...		0%	4.8 MB	0 MB/秒	0 Mbps	
> Application Frame Host		0%	6.9 MB	0 MB/秒	0 Mbps	
> Armoury Crate Control Inte...		0%	0.5 MB	0 MB/秒	0 Mbps	
> Armoury Crate Control Inte...		0%	0.8 MB	0 MB/秒	0 Mbps	

- 在CMD界面，通过 **Tasklist**, **Taskkill** 及相应的程序命令对进程进行管理
 - 使用 **Tasklist** 列举出当前所有正在运行的进程

```
Windows PowerShell
PS C:\Users\10728\Desktop> 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	96 K
Secure System	172	Services	0	49,336 K
Registry	216	Services	0	52,992 K
smss.exe	768	Services	0	992 K
csrss.exe	1128	Services	0	4,000 K
wininit.exe	1240	Services	0	4,960 K
csrss.exe	1260	Console	1	7,644 K
services.exe	1312	Services	0	10,708 K
LsaIso.exe	1332	Services	0	3,780 K
lsass.exe	1348	Services	0	21,496 K
svchost.exe	1480	Services	0	29,984 K
fontdrvhost.exe	1508	Services	0	4,852 K
WUDFHost.exe	1556	Services	0	4,772 K
svchost.exe	1612	Services	0	17,420 K
svchost.exe	1668	Services	0	6,820 K
WUDFHost.exe	1740	Services	0	5,420 K
WUDFHost.exe	1788	Services	0	9,868 K
winlogon.exe	1880	Console	1	8,832 K
fontdrvhost.exe	1952	Console	1	47,032 K
svchost.exe	1064	Services	0	4,120 K
svchost.exe	1416	Services	0	6,800 K
svchost.exe	1412	Services	0	11,000 K
svchost.exe	1372	Services	0	3,876 K
svchost.exe	1308	Services	0	6,288 K
svchost.exe	1628	Services	0	8,700 K
svchost.exe	1664	Services	0	9,680 K
dwm.exe	2176	Console	1	238,560 K
svchost.exe	2200	Services	0	9,100 K
svchost.exe	2280	Services	0	17,364 K
svchost.exe	2448	Services	0	8,244 K
svchost.exe	2460	Services	0	7,388 K
svchost.exe	2468	Services	0	6,628 K

- 使用 **Taskkill** 命令结束部分应用程序进程

■ **Taskkill** 用法

```
PS C:\Users\10728\Desktop> taskkill /?
```

TASKKILL [/S system [/U username [/P [password]]]]
 { [/FI filter] [/PID processid | /IM imagename] } [/T] [/F]

描述：
 使用该工具按照进程 ID (PID) 或映像名称终止任务。

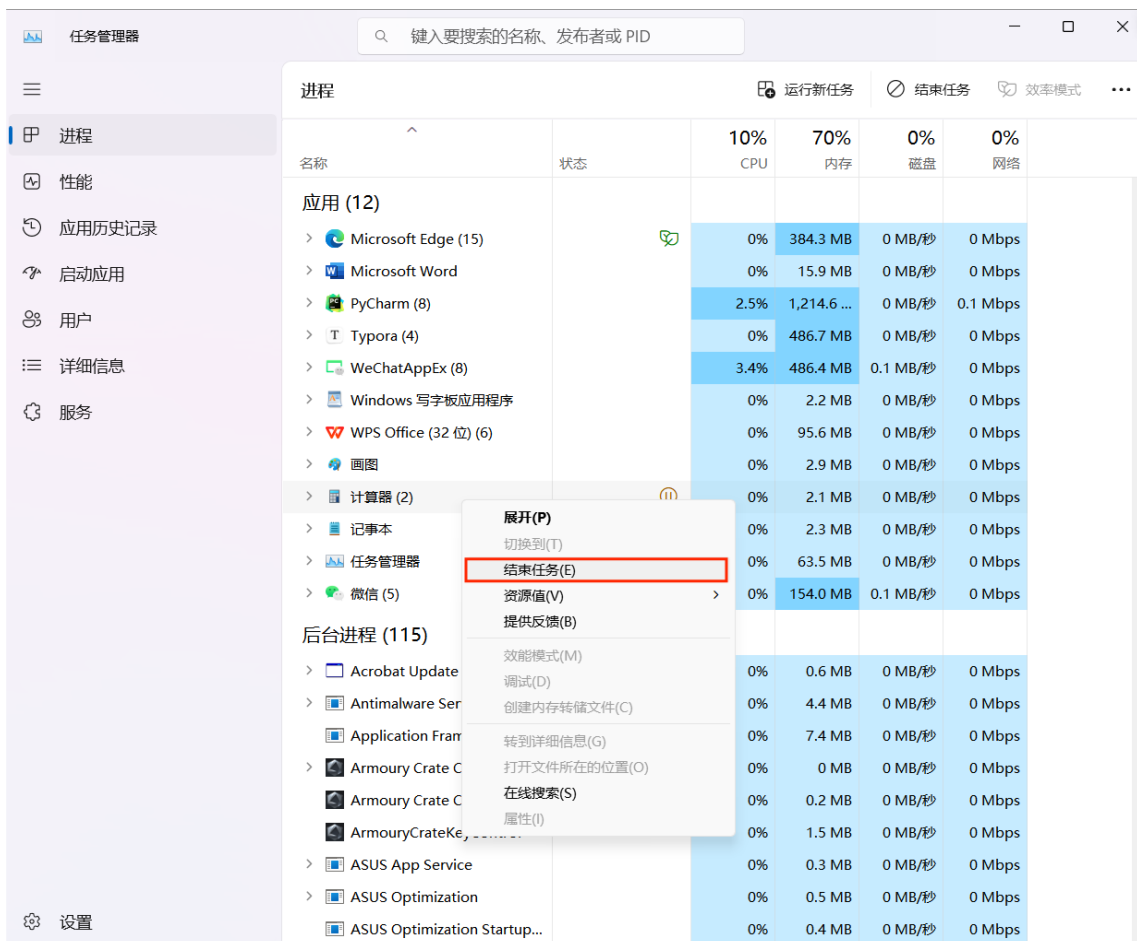
参数列表：

/S	system	指定要连接的远程系统。
/U	[domain\]user	指定应该在哪个用户上下文执行这个命令。
/P	[password]	为提供的用户上下文指定密码。如果忽略，提示输入。
/FI	filter	应用筛选器以选择一组任务。允许使用 "*"。例如，映像名称 eq acme*
/PID	processid	指定要终止的进程的 PID。使用 TaskList 取得 PID。
/IM	imagename	指定要终止的进程的映像名称。通配符 '*' 可用来指定所有任务或映像名称。
/T		终止指定的进程和由它启用的子进程。
/F		指定强制终止进程。
/?		显示帮助消息。

- 使用 **TASKKILL /PID 2356** 关闭计算器

```
Windows PowerShell
mspaint.exe           6068 Console           1    76,612 K
svchost.exe           3032 Services            0     9,168 K
CalculatorApp.exe     2356 Console           1    65,716 K
RuntimeBroker.exe    1620 Console           1    14,864 K
WINWORD.EXE          19776 Console           1    99,984 K
wordpad.exe           27688 Console           1    46,636 K
StartMenuExperienceHost.e 29632 Console           1    94,268 K
RuntimeBroker.exe    30228 Console           1    24,788 K
SearchHost.exe       13304 Console           1   107,152 K
RuntimeBroker.exe    7892 Console           1    31,844 K
Taskmgr.exe          21288 Console           1   135,768 K
msedge.exe           19652 Console           1   149,936 K
promceefpluginhost.exe 29284 Console           1    49,136 K
promceefpluginhost.exe 15040 Console           1    26,208 K
wps.exe              3300 Console           1    22,316 K
wps.exe              6612 Console           1    45,428 K
WeChatAppEx.exe     29316 Console           1    87,204 K
msedge.exe           24972 Console           1   101,096 K
msedge.exe           18208 Console           1    79,196 K
RuntimeBroker.exe    11356 Console           1    11,816 K
msedge.exe           18712 Console           1   134,300 K
msedge.exe           20804 Console           1    30,348 K
svchost.exe          29656 Services            0    11,796 K
SearchProtocolHost.exe 15812 Services            0    15,348 K
SearchFilterHost.exe 30040 Services            0     9,296 K
svchost.exe          19492 Services            0     7,668 K
SearchFilterHost.exe 24388 Services            0   10,264 K
svchost.exe          23156 Services            0    13,256 K
dllhost.exe           9768 Console           1    12,972 K
dllhost.exe          10560 Console           1    13,564 K
dllhost.exe          27004 Console           1    15,112 K
WindowsTerminal.exe  2480 Console           1   129,212 K
OpenConsole.exe       3132 Console           1     9,772 K
powershell.exe        2348 Console           1    65,476 K
tasklist.exe          29220 Console           1     8,812 K
PS C:\Users\10728\Desktop> TASKKILL /PID 2356
成功：给进程发送了终止信号，进程的 PID 为 2356。
```

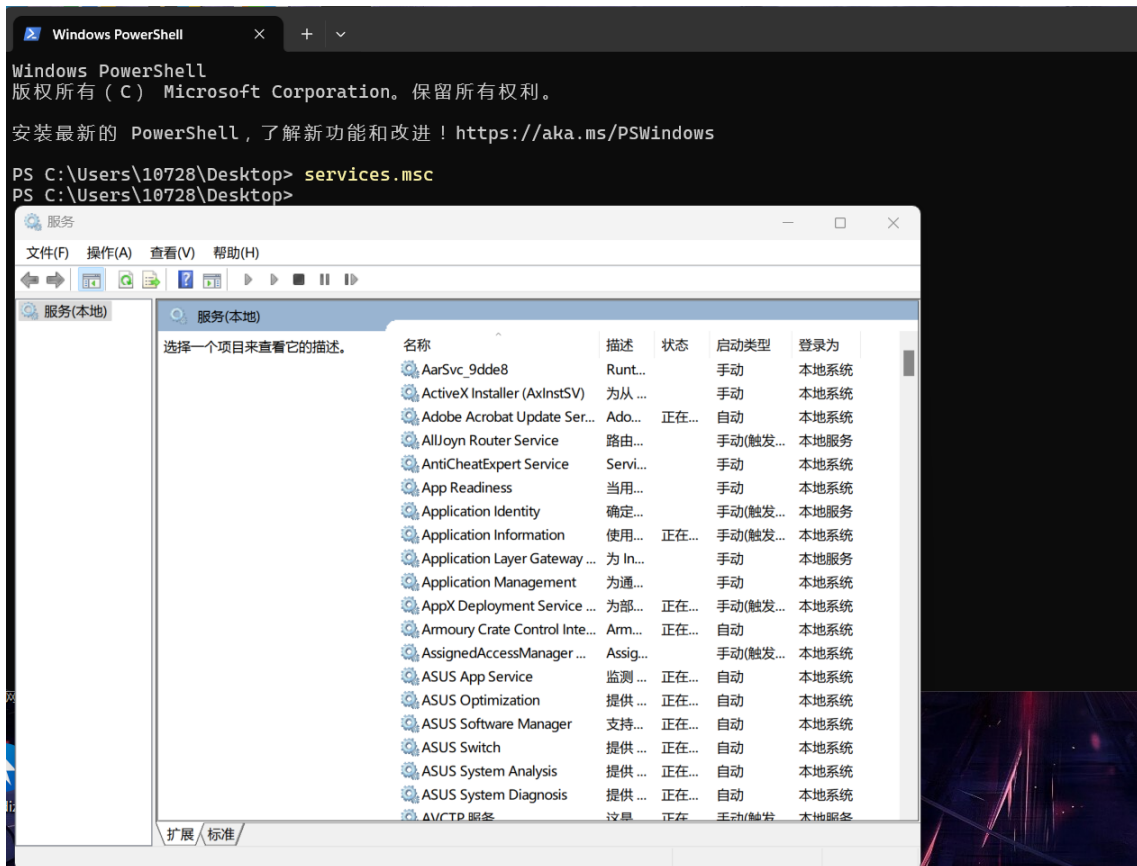
- 也可以直接在任务管理器的图形界面进行操作结束进程
 - 鼠标右键单击想要关闭的进程



- 鼠标左键单击结束任务即关闭进程



- 使用 `services.msc` 命令列出了所有的系统服务及其状态



六、实验结论

- 简单解释进程和网络进程含义
 - 进程：进程是指计算机中正在运行的程序，是操作系统进行资源分配和执行计算的基本单位。进程可以是系统进程，也可以是用户进程
 - 网络进程：网络进程是指在网络中运行的程序。这些进程通常需要与其他计算机或网络设备进行通信。网络进程可以由服务器、客户端等应用程序创建的，它们在网络中传输数据并处理网络请求
- 任务管理器的启动和使用
 - 在Windows环境中，通过 `Ctrl + Alt + Del` 键组合，选择“任务管理器”
 - 右键点击任务栏，在快捷菜单“任务管理器”命令
 - 通过命令 `taskmgr` 打开 “任务管理器” 窗口
- 显示有关服务的方式
 - 服务是设计为长时间运行并为其他进程提供功能或支持的程序
 - 在CMD窗口输入 `services.msc` 命令，我们可以查看、启动、停止或重启系统服务
- 图形和命令方式启动和停止有关进程
 - 图形方式：在Windows任务管理器中右击某个进程，选择“结束任务”或“重新启动”
 - 命令方式：在CMD中通过 `Tasklist`、`Taskkill` 等命令查看当前进程列表和停止某个进程。