实验 01：网络相关进程与服务实验

姓名	学号	合作学生	指导教师	实验地点	实验时间
林继申	2250758	无	陈伟超	济事楼 330	2024/02/29

【实验目的】

1. 理解操作系统中的进程管理：通过本实验，学习和理解 Windows 操作系统中任务管理器的功能和用途，包括进程管理、应用程序管理、服务管理及网络进程的监控。
2. 掌握任务管理器的使用：学会使用 Windows 任务管理器监控计算机的性能，包括 CPU 和内存使用情况，以及进程和应用程序的管理。
3. 学习进程管理命令：通过实际操作，掌握使用 tasklist、taskkill 和 tskill 命令对进程进行查看和管理的方法。
4. 了解网络进程的特点：通过实验，认识到网络进程与一般进程的区别，特别是在传输层开启端口号的特性，以及如何查看正在使用的端口号。
5. 熟悉 Windows 服务的管理：通过使用 services.msc 命令，了解 Windows 系统服务的管理界面，学习如何查看和管理操作系统中运行的服务。

【实验原理】

一、Windows 任务管理进程

Windows 任务管理器为用户提供了一种方便的方式来监控和管理正在运行的程序和进程。任务管理器可以打开用于监视计算机性能的关键指示器，使用户能够快速了解系统的整体健康状况。在“应用程序”选项卡中，用户可以看到所有当前运行的程序及其状态。“进程”选项卡显示了系统中所有正在运行的进程的详细列表，包括每个进程对 CPU 和内存资源的使用情况。任务管理器提供了一个深入的视角来观察运行中的进程如何影响计算机的性能。用户可以根据需要对这些进程进行排序，以便快速识别出最占资源的进程。用户能够通过任务管理器结束、切换或启动新的程序和进程。这提供了一种迅速处理不响应程序和调整正在运行应用的便捷方式。

二、进程

进程是操作系统中一个重要的概念，它表示计算机中正在执行的程序的实例。每个进程都拥有独立的地址空间和系统资源，包括内存、文件句柄和执行线程等。

进程作为系统资源分配和调度的基本单位，不仅包含了程序的执行状态信息，如程序计数器、寄存器和变量等，还涉及到 CPU 和内存的使用情况、页面错误和句柄计数等多种性能指标。操作系统通过进程管理机制，如任务创建、执行、挂起、终止等操作，协调各个进程之间的运行，确保系统资源的有效分配和使用，维持系统的稳定性和效率。

- tasklist 命令：这个命令用于展示在本地或远程计算机上运行的所有应用程序和服务列表，提供了每个进程的详细信息，包括进程 ID（PID）。
- taskkill 命令：taskkill 提供了一种机制来结束一个或多个任务或进程。用户可以根据进程 ID（PID）或程序的名称来指定需要结束的进程。
- tskill 命令：tskill 功能与 taskkill 相似，同样用于结束一个或多个进程。

三、网络进程

网络进程是指在网络通信中参与数据传输的进程，它们与一般的进程共享基础属性，如占用系统资源（CPU、内存等），但独特之处在于其能够开启一个或多个网络端口。这些端口作为通信通道，允许进程接收和发送网络数据。在客户端-服务器（C/S）或浏览器-服务器（B/S）架构中，客户端网络进程通常至少开启一个端口以接收服务器发送的数据或向服务器发送请求，而服务端网络进程可能开启至少两个端口，分别用于接收来自客户端的数据和向客户端发送数据。端口号的范围从 0 到 65535，其中 0 到 1023 通常被保留为系统或标准服务端口。通过特定命令，如在 Windows 环境下，用户可以查询哪些端口当前正在被使用，以及这些端口分别属于哪些进程，从而对网络通信过程有更清晰的了解和管理。

四、服务

服务（在 Windows 环境中通常称为 Windows 服务）是一种特殊类型的进程，主要设计用来在操作系统的后台执行，提供核心功能或支持其他程序和进程。与普通的应用程序不同，服务通常不需要用户交互，也不提供图形用户界面。它们在系统启动时自动开始，并且可以配置为持续运行，即使没有用户登录到系统也能执行其功能。这些服务负责处理多种系统级任务，如文件和打印共享、网络连接管理、用户认证等。Windows 服务可以通过事件日志记录其操作和错误信息，为系统管理员提供重要的诊断信息。

【实验设备】

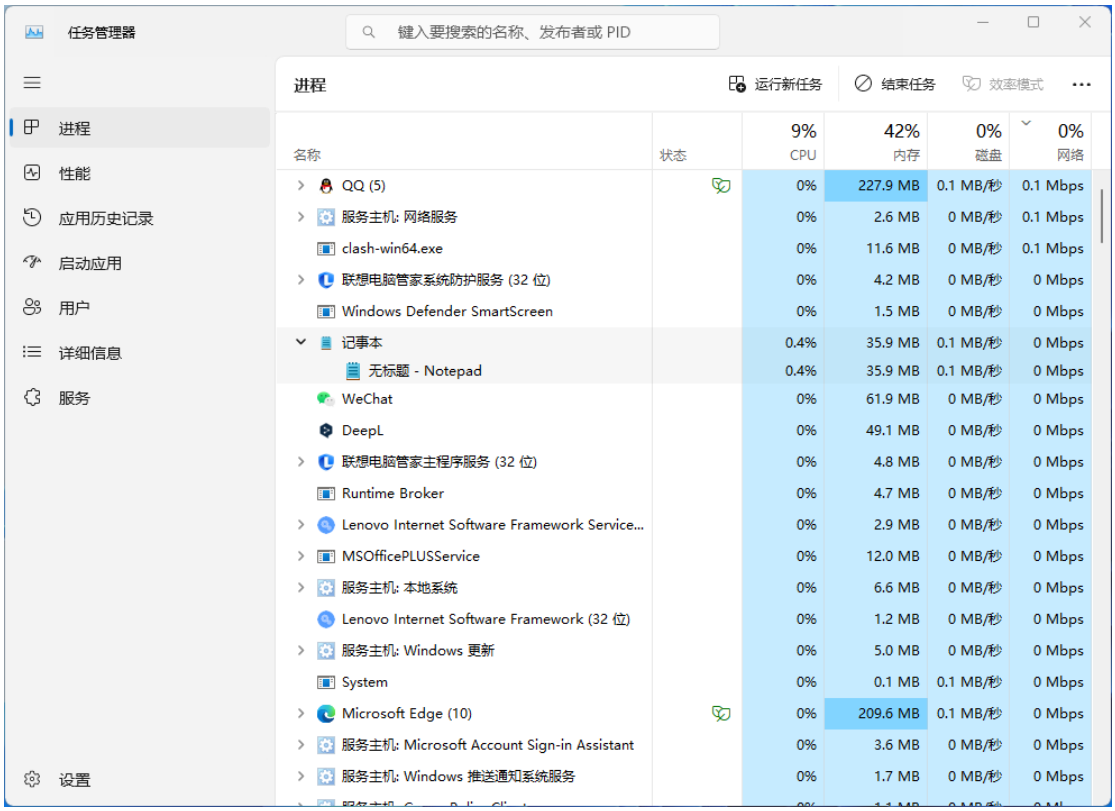
1. 操作系统：Windows 11
2. 网络环境：Wi-Fi 连接
3. 应用程序：记事本、画图

【实验步骤】

1. 启动并进入 Windows 环境，通过快捷键“Ctrl+Alt+Del”键选择“任务管理器”，或者右键点击任务栏，在快捷菜单选择“任务管理器”，或者通过命令 taskmgr 打开“任务管理器”。
2. 启动记事本应用程序。
3. 在任务管理器中，切换至“进程”选项卡，观察 CPU 和内存的使用情况。
4. 通过任务管理器和命令行工具（tasklist 命令、taskkill 命令等）查看和管理进程。
5. 通过命令 services.msc 查看系统服务。
6. 观察实验现象，记录观察到的进程、服务和相关参数。

【实验现象】

1. 在任务管理器“进程”选项卡中观察 CPU 和内存的使用情况，记事本应用程序在任务管理器“进程”选项卡中显示。



2. 在命令行通过中 tasklist 命令列出所有正在运行的进程。可以查看 Notepad.exe 的 PID 为 26604。

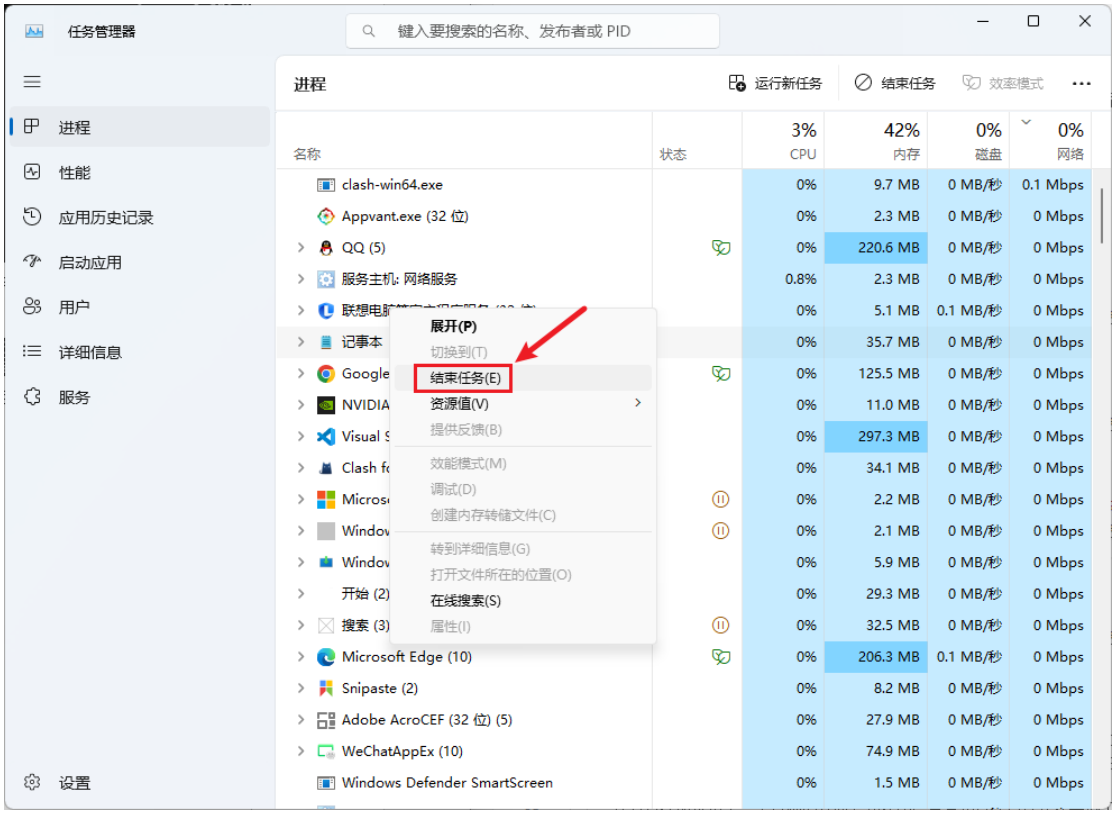
```
C:\Users\lenovo>tasklist

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      3,384 K
Registry                       216 Services                   0     30,488 K
smss.exe                       808 Services                   0        960 K
csrss.exe                     1124 Services                   0      6,296 K
wininit.exe                   1268 Services                   0      6,772 K
csrss.exe                     1280 Console                    1      6,888 K
services.exe                  1344 Services                   0      9,932 K
lsass.exe                     1372 Services                   0     22,812 K
svchost.exe                   1492 Services                   0     23,440 K
fontdrvhost.exe               1520 Services                   0      1,964 K
WUDFHost.exe                  1572 Services                   0     12,404 K
svchost.exe                   1624 Services                   0     15,816 K
svchost.exe                   1676 Services                   0      6,240 K
winlogon.exe                  1732 Console                    1      8,084 K
WUDFHost.exe                  1816 Services                   0      4,476 K
fontdrvhost.exe               1856 Console                    1     16,524 K
WUDFHost.exe                  1916 Services                   0      3,644 K
svchost.exe                   1988 Services                   0      2,980 K
dwm.exe                       2024 Console                    1    182,888 K
svchost.exe                   2036 Services                   0      4,968 K
svchost.exe                    916 Services                   0      8,156 K
svchost.exe                   1164 Services                   0     12,172 K
svchost.exe                   2084 Services                   0      8,228 K
svchost.exe                   2152 Services                   0     14,792 K
svchost.exe                   2192 Services                   0      7,136 K
svchost.exe                   2200 Services                   0      7,748 K
svchost.exe                   2212 Services                   0      7,824 K
svchost.exe                   2240 Services                   0     12,444 K
IntelCpHDCPSvc.exe            2368 Services                   0      3,712 K
svchost.exe                   2388 Services                   0     10,152 K
svchost.exe                   2396 Services                   0      6,988 K
svchost.exe                   2472 Services                   0      4,984 K
svchost.exe                   2488 Services                   0      5,312 K
svchost.exe                   2768 Services                   0      8,220 K
svchost.exe                   2860 Services                   0      7,856 K
svchost.exe                   2904 Services                   0      5,004 K
igfxCUIServiceN.exe           3008 Services                   0      7,892 K
svchost.exe                   3040 Services                   0     10,608 K
NVDisplay.Container.exe       3116 Services                   0     17,296 K
svchost.exe                   3128 Services                   0      5,936 K
svchost.exe                   3136 Services                   0      7,908 K
svchost.exe                   3296 Services                   0      7,260 K
svchost.exe                   3336 Services                   0     17,004 K
svchost.exe                   3420 Services                   0      5,808 K
svchost.exe                   3428 Services                   0     10,020 K
svchost.exe                   3508 Services                   0      8,892 K
svchost.exe                   3524 Services                   0     10,516 K
Memory Compression            3552 Services                   0    234,316 K
svchost.exe                   3608 Services                   0      8,284 K
WUDFHost.exe                  3704 Services                   0      9,372 K
svchost.exe                   3724 Services                   0     18,792 K
NVDisplay.Container.exe       3924 Console                    1     32,884 K
svchost.exe                   3944 Services                   0     23,500 K
svchost.exe                   4024 Services                   0      6,360 K
```

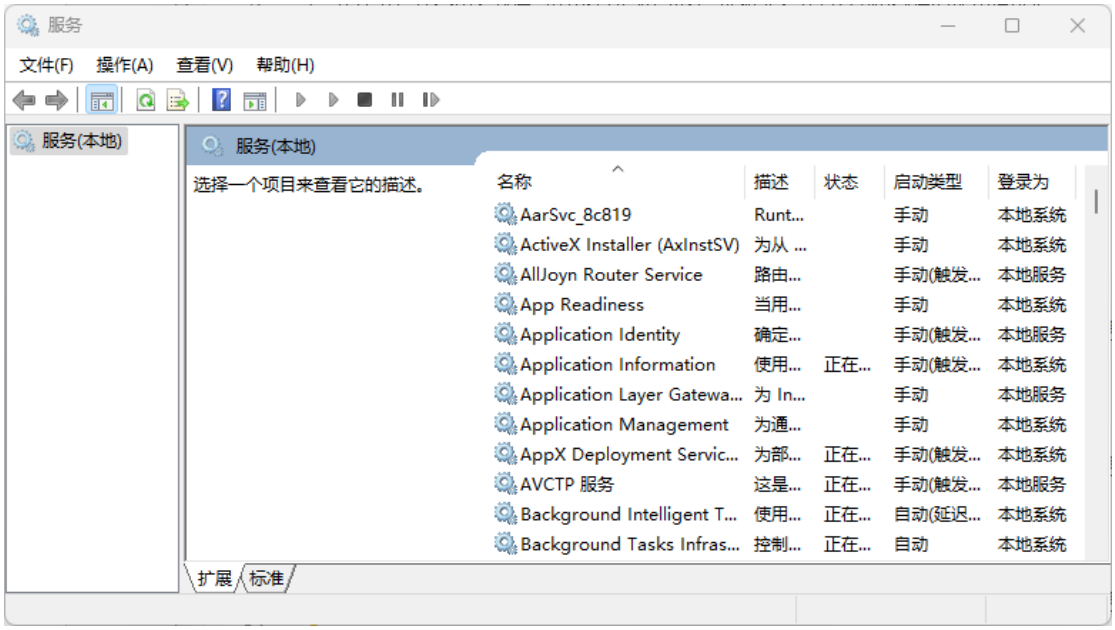
3. 在命令行通过中 taskkill /PID 26604 命令结束记事本应用程序的进程，可以观察记事本应用程序被关闭。

```
C:\Users\lenovo>taskkill /PID 26604
成功: 给进程发送了终止信号，进程的 PID 为 26604。
```

4. 在任务管理器通过中通过右键菜单选择“结束任务”结束记事本应用程序的进程，可以观察记事本应用程序被关闭。



5. 通过中 services.msc 命令列出所有的系统服务及其状态。



【分析讨论】

一、进程和网络进程的含义

- 进程：在操作系统中，进程是指一个执行中的程序。它不仅包含代码本身，还包括执行的当前活动、在内存中的数据、一个执行堆栈、至少一个执行序列（线程）以及其他用于操作系统书签的资源。简而言之，进程是系统进行资源分配和调度的基本单位，是应用程序在系统中的一次运行活动。
- 网络进程：网络进程在基本的进程属性上扩展，使其能够参与网络通信。这类进程通过开启一个或多个网络端口进行数据的发送和接收。网络进程的主要特点是其能够监听网络请求或向其他网络地址发送请求，常见于客户端-服务器（C/S）或浏览器-服务器（B/S）架构的应用中。网络进程至少需要开启一个端口号用于网络通信，使其在数据传输中扮演着至关重要的角色。

二、任务管理器的启动和使用

任务管理器是 Windows 操作系统中的一个系统监控工具，用于提供关于计算机性能及运行中程序的信息。可以通过快捷键 Ctrl+Alt+Del 并选择“任务管理器”，或者在任务栏上右键点击选择“任务管理器”来启动它，也可以通过命令 taskmgr 打开“任务管理器”。

三、图形界面方式和命令行方式显示有关服务

- 图形界面方式:用户可以通过运行 services.msc 命令打开服务管理控制台。这个图形界面显示了所有 Windows 服务的列表，包括每个服务的状态（如正在运行、已停止等），允许用户通过右键菜单进行启动、停止、暂停、恢复或重新启动服务等操作。
- 命令行方式：用户也可以通过命令行工具来管理服务。例如，使用 net start 和 net stop 命令分别启动和停止服务。对于更高级的服务管理，sc 命令提供了一套完整的服务控制功能，包括查询服务状态、配置服务启动类型等。

四、图形界面方式和命令行方式显示有关服务

- 图形界面方式：在任务管理器的“进程”选项卡中，用户可以查看到所有正在运行的进程及其资源使用情况。通过右键点击特定进程，用户可以选择“结束任务”来强制停止一个进程。
- 命令行方式：使用 tasklist 命令可以查看当前运行的所有进程及其 PID（进

程标识符)。taskkill 命令允许用户通过指定 PID 或进程名来结束一个或多个进程。如 taskkill /PID 1234 会结束 PID 为 1234 的进程。tskill 命令提供了类似 taskkill 的功能，也是用于结束进程。