实验 04：基本网络测试工具及应用工具实验

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	2024/03/07

【实验目的】

1. 掌握基本网络测试工具的使用：熟悉并掌握操作系统中内置的网络测试工具的基本使用方法，如 Ping 命令、Ipconfig、Tracert、Net 命令等，这些工具虽然不能被视为专业级的测试软件，但对于日常网络故障的诊断与解决来说，它们是非常有效且便捷的手段。
2. 了解网络测试工具的应用场景：通过实际操作这些工具，理解各个工具的具体应用场景，例如，使用 Ping 命令检测网络连接的连通性，利用 Ipconfig 查看网络配置信息，通过 Tracert 命令追踪数据包的路由路径等。
3. 培养网络问题分析与解决能力：实验通过对各种网络命令的学习和实践，旨在培养分析和解决网络问题的能力。
4. 加深对 TCP/IP 协议的理解：通过使用这些基于 TCP/IP 协议的测试工具，可以加深对 TCP/IP 网络协议的理解，包括 IP 地址、子网掩码、默认网关等网络基本概念的实际应用。

【实验原理】

一、Ping 命令

Ping 命令是一个在各种操作系统中广泛使用的网络工具，用于测试网络连接。该命令通过发送 ICMP（Internet Control Message Protocol，互联网控制消息协议）Echo Request 消息给目标主机并等待 Echo Reply 消息来检查主机之间的连通性。它是诊断网络问题的首选工具之一，因为它不仅可以帮助确定两个节点之间是否存在通信路径，还能提供关于网络延迟和丢包率的信息。

主要参数说明：

- -t：持续 ping 目标主机，直到用户手动停止（使用 Control-C）。
- -a：解析地址到主机名。
- -n count：设置要发送的 Echo Request 消息数目，默认是 4。
- -l length：指定 ICMP 消息请求数据部分的字节大小，默认是 32 字节。最大值可达 65500 字节。

- -f：设置“不要分段”标志，告诉中间路由器不要分段 ICMP 数据包。
- -i ttl：设置生存时间 TTL（Time To Live），即数据包在网络中跳数的上限，帮助避免数据包在网络中无限循环。
- -v tos：设置服务类型（Type of Service），用于定义数据包的优先级。
- -r count：记录路由，存储经过的路由器地址，最多可记录 9 个。
- -s count：设置时间戳，记录每个跳的处理时间。
- -j host-list / -k host-list：通过指定的主机列表设置源路由，-j 允许路由分隔，-k 不允许。
- -w timeout：设置等待每次回复的超时时间（毫秒）。

使用场景：

- 网络连通性测试：验证本地主机与网络上另一台主机之间的连通性。
- 网络性能测量：通过观察 ping 回复的时间，可以评估网络延迟。
- 路由跟踪：通过修改 TTL 值，可以观察数据包通过网络到达目标的路径。
- 网络故障诊断：通过分析丢包情况和响应时间，可以帮助定位网络故障的位置。

二、Ipconfig 命令

ipconfig 是一个在 Windows 操作系统中常用的命令行工具，用于显示当前设备的网络配置信息，包括 IP 地址、子网掩码和默认网关等。该命令还可以刷新 DNS 解析缓存和重置 DHCP 配置等。ipconfig 是诊断网络问题和获取网络设置的重要工具，对网络管理员和终端用户都非常有用。

主要参数说明：

- 无参数：执行 ipconfig 命令而不带任何参数将显示所有网络接口的 IP 地址、子网掩码和默认网关。
- /all：显示所有配置信息，包括 DNS 服务器、DHCP 服务器、租约获取时间和过期时间等。
- /release：释放指定适配器的 IPv4 地址租约。如果不指定适配器名称，则会释放所有适配器的 IP 地址租约。
- /renew：更新指定适配器的 IPv4 地址租约。这通常用于从 DHCP 服务器获取新的 IP 地址。

- /flushdns：清除 DNS 解析缓存。这在更改 DNS 设置或排除 DNS 解析问题时非常有用。
- /displaydns：显示 DNS 解析缓存的内容，包括最近解析的域名及其 IP 地址。
- /registerdns：刷新所有 DHCP 租约并重新注册 DNS 名称。

使用场景：

- 查看网络配置：最基本的使用场景是查看设备的 IP 配置信息，包括 IP 地址、子网掩码、默认网关等，以便进行网络故障诊断或配置核对。
- 网络问题诊断：当遇到网络连接问题时，使用 ipconfig 检查 IP 地址是否正确分配，或者默认网关是否设置正确，是排除网络故障的第一步。
- 刷新 DNS 缓存：当网站的 IP 地址更改后，如果本地 DNS 缓存未更新，可能会导致无法访问该网站。使用/flushdns 参数可以清除 DNS 缓存，帮助解决访问问题。
- 更新 IP 地址：在使用动态主机配置协议（DHCP）环境中，如果需要更换设备的 IP 地址，可以使用/release 释放当前的 IP 地址，然后使用/renew 获取新的 IP 地址。
- 网络配置调试：在更改网络设置或进行网络优化时，可以使用 ipconfig 及其参数来验证更改的效果，确保网络配置正确应用。

三、Nbtstat 命令

nbtstat 是一个在 Windows 操作系统中用于诊断 NetBIOS（网络基本输入输出系统）名称解析问题的命令行工具。NetBIOS 是一种较旧的网络传输协议，主要用于小型网络和本地网络环境中的设备间通信。nbtstat 命令可以帮助网络管理员查看本地和远程机器的 NetBIOS 名称表，诊断网络连接问题。

主要参数说明：

- -a <名称>：显示一个远程机器的 NetBIOS 名称表，其中<名称>是远程计算机的 NetBIOS 名称。
- -A <IP 地址>：使用远程计算机的 IP 地址显示 NetBIOS 名称表。
- -c：显示 NetBIOS 名称缓存的内容，包括名称及其对应的 IP 地址。
- -n：显示本地 NetBIOS 名称表。

- -r：显示 NetBIOS 名称解析统计信息，包括成功的和失败的名称解析尝试。
- -R：清除 NetBIOS 名称缓存。
- -S：显示当前会话表，包括与远程计算机的 NetBIOS 会话。
- -s：与-S 类似，但也显示远程计算机的 IP 地址。

使用场景：

- 诊断 NetBIOS 名称解析问题：当网络上的设备通过 NetBIOS 名称无法相互识别或连接时，可以使用 nbtstat 来检查 NetBIOS 名称表和缓存，找出问题所在。
- 网络连接故障排除：通过查看本地和远程机器的 NetBIOS 会话表，可以帮助诊断连接失败的原因，如是否因为 NetBIOS 会话限制或其他网络问题。
- 查看 NetBIOS 统计信息：nbtstat 可以提供有关 NetBIOS 名称解析尝试的成功率和失败率的统计信息，有助于分析网络性能问题。
- 刷新 NetBIOS 名称缓存：在网络配置更改后，旧的 NetBIOS 名称记录可能仍保留在缓存中，使用-R 参数可以清除缓存，确保名称解析是最新的。
- 网络安全检查：通过查看会话表和 NetBIOS 名称，可以帮助识别未授权的设备试图连接到网络，或者存在的潜在安全威胁。

四、Tracert 命令

tracert（Trace Route）是一个在多种操作系统中可用的命令行工具，用于显示数据包从源计算机到目标计算机或设备在网络上的路径。它利用 Internet Control Message Protocol (ICMP)发送消息到目标设备，并记录每个路由器在路径上的跳数。每个跳的响应时间也被记录下来，从而帮助用户识别路径中可能的瓶颈或问题点。

主要参数说明：

- -d：不将地址解析成主机名，直接显示 IP 地址。
- -h maximum_hops:定义搜索目标设备的最大跳数。默认值通常为 30 跳。
- -j host-list：使用源路由选项沿指定的主机列表路径前进。
- -w timeout：设置每个响应的等待超时时间（毫秒）。

- -4：强制使用 IPv4。
- -6：强制使用 IPv6。

使用场景：

- 网络故障诊断：当用户无法访问特定网站或网络服务时，tracert 可以用来确定数据包在哪个网络跳发生了延迟或丢失，有助于定位故障点。
- 性能评估：通过测量到达每个跳的时间，tracert 可以帮助评估网络路径的性能，识别路径中可能的延迟点。
- 路由追踪：tracert 提供了一种方法来观察数据包在达到最终目标之前经过的路由器和设备，这对于理解网络拓扑结构非常有用。
- 网络安全分析：tracert 可以帮助识别数据包传输路径中未授权的或意外的路由器和交换机，这对于检测潜在的安全风险至关重要。
- ISP 连通性测试：当怀疑网络连接问题与 ISP（Internet Service Provider，互联网服务提供商）有关时，tracert 可以用来测试到 ISP 的连接质量，以及到达 ISP 之后的网络路径质量。

五、Net 命令

net 命令是 Windows 操作系统中一个非常强大的命令行工具，它用于执行与网络、共享资源、文件、打印作业和用户账户相关的各种任务。这个命令集合提供了一套广泛的网络和系统管理功能，使得管理员可以通过命令行接口快速配置和管理 Windows 网络环境。

主要参数说明：

- net user：管理用户账户。可以添加、删除、修改用户账户信息，例如密码、用户组、登录权限等。
- net view：显示网络上的计算机或设备列表，或者显示某台计算机上的共享资源。
- net share：创建、删除或管理共享资源。可以控制哪些文件夹在网络上共享以及它们的共享权限。
- net use：连接、断开与网络资源的连接，并显示网络连接的信息。这常用于映射网络驱动器和连接网络打印机。
- net localgroup：管理本地用户组，包括添加和删除用户组成员。

- net start/net stop：启动或停止 Windows 服务。
- net session：管理与本机建立的网络会话，可以查看活动的网络连接和断开这些连接。
- net statistics：显示网络服务的统计信息，如服务器或工作站服务。

使用场景：

- 用户和组管理：网络管理员可以使用 net user 和 net localgroup 命令来添加、删除或修改系统用户和用户组，包括重置密码、配置用户权限等。
- 网络资源管理：使用 net share 和 net use 命令来共享和访问网络上的文件夹和打印机，非常适合在企业环境中管理文件共享和网络打印服务。
- 服务管理:通过 net start 和 net stop 命令启动和停止 Windows 服务，这对于故障排除或系统配置调整非常有用。
- 网络诊断与管理：net view 和 net session 命令允许管理员查看网络上的计算机和资源以及管理网络会话，有助于网络维护和故障诊断。

六、Route 命令

route 命令是一个网络工具，用于查看和修改 IP 路由表。这个命令在各种操作系统中都有提供，包括 Windows、Linux 和 macOS，使网络管理员能够控制数据包从源地址到目的地址的路径。通过使用 route 命令，管理员可以指定特定的路径来优化网络流量，解决网络拥堵问题，或绕过故障的网络设备。

主要参数说明：

- add：添加一条新的路由规则到 IP 路由表中。
- delete：从 IP 路由表中删除一条路由规则。
- print：显示当前的 IP 路由表。
- -p：当添加路由时，使路由规则持久化。仅在 Windows 系统中有效，这意味着即使重启计算机路由规则也依然有效。

使用场景：

- 自定义网络流量路径：当网络管理员希望控制特定网络流量的路径时，可以通过添加自定义路由来实现。这在多网卡环境或多个网络连接存在时尤其有用。

- 网络故障诊断和规避：在网络设备或链接故障时，管理员可以临时更改路由表，将流量重新定向到备用路径，以保证网络的连通性和服务的可用性。
- 网络性能优化：通过合理配置路由规则，可以避免网络拥堵，优化网络性能。
- 安全控制：通过定义特定的路由规则，可以防止不安全的网络访问或限制访问特定网络资源。

七、Nslookup 命令

nslookup 是一个用于查询域名系统（DNS）以获取域名或 IP 地址映射的命令行工具。它对于网络管理员和普通用户来说都是诊断和解决 DNS 问题的重要工具。

主要参数说明：

- 无参数：在不带任何参数的情况下启动 nslookup 会进入交互式模式，用户可以连续执行多个查询。
- <域名>：直接查询一个域名来获取其对应的 IP 地址。
- <IP 地址>：查询哪个域名与该 IP 地址关联，进行反向 DNS 查找。
- -type=<查询类型>：指定查询类型，如 A、AAAA、MX、TXT 等。A 记录查询返回 IPv4 地址，AAAA 记录返回 IPv6 地址，MX 记录查询邮件交换服务器，TXT 记录通常包含了对域名的一些文本信息。
- -query=<查询类型>/-q=<查询类型>：同-type。
- -debug：显示查询过程中的详细技术信息。
- server <名称或 IP>：更改查询使用的 DNS 服务器。

使用场景：

- DNS 解析故障排查：当域名无法正确解析时，nslookup 可以帮助确定问题是否出在 DNS 解析上，通过比较不同 DNS 服务器的解析结果找出问题所在。
- 查看域名信息：nslookup 能查询特定域名的各类 DNS 记录，例如获取域名的邮件服务器(MX 记录)，用于邮件发送系统的配置。
- DNS 记录验证：在更改 DNS 记录，如更换网站的 IP 地址或更新邮件服务

器配置后，使用 nslookup 验证更改是否已正确生效。

- 反向 DNS 查找：通过输入 IP 地址查询关联的域名，这在识别访问网络服务的来源时非常有用。
- 测试 DNS 服务器性能：通过对比不同 DNS 服务器解析同一域名所用的时间，可以评估 DNS 服务器的响应速度。

八、Netsh 命令

netsh（Network Shell）命令是一个强大的命令行脚本工具，用于查看和修改 Windows 操作系统网络配置。它允许管理员配置几乎所有与网络相关的系统设置，包括网络接口、防火墙规则、路由策略、IP 地址配置、Wi-Fi 管理等。由于 netsh 能够导出和导入配置，它也常用于网络设置的备份和恢复。

主要参数说明：

- interface （int)：用于管理网络接口，可以配置 IP 地址、DHCP 设置等。
- firewall：用于配置 Windows 防火墙设置。
- http：管理 HTTP 协议相关设置，包括 SSL 配置。
- advfirewall：用于更高级的防火墙配置，比如入站和出站规则、安全策略等。
- wlan：管理无线网络配置，包括配置网络、显示可用网络列表等。
- dump：导出当前的网络配置到一个脚本文件。
- reset：重置网络配置到初始状态。

使用场景：

- 网络配置管理：netsh 命令可以配置网络接口的 IP 地址、子网掩码、默认网关等参数，非常适用于静态 IP 地址配置或切换不同网络配置的场景。
- 防火墙和安全策略配置：通过 netsh，管理员能够配置 Windows 防火墙的详细规则，包括允许或阻止特定端口、程序的网络访问权限。
- Wi-Fi 管理：netsh wlan 提供了一系列管理无线网络的命令，可以用来显示所有可用的无线网络、连接到无线网络、导出和导入无线网络配置。
- 故障排除和网络诊断：netsh 提供的诊断命令可以帮助分析和解决网络

连接问题，如重置网络接口、查看各种网络统计信息。

- 网络配置的备份和恢复：通过 netsh dump 命令，可以将当前的网络配置导出到一个脚本文件中，随后可以通过执行此脚本来恢复网络配置，这对于系统迁移和恢复非常有用。

九、Ftp 命令

FTP（File Transfer Protocol）是一种用于在网络上传输文件的协议，而 ftp 命令是一个基于命令行的客户端程序，用于连接到 FTP 服务器以上传、下载和管理文件。它是 Internet 上最早期的文件传输服务之一，支持在客户端和服务器之间进行交互式文件传输。

主要参数说明：

- open <hostname> [port]：连接到指定的 FTP 服务器，可选地指定端口（默认为 21）。
- user <username> [password]：登录到 FTP 服务器，可能会提示输入密码。
- ls [directory] [localfile]：列出远程目录的内容，可以将输出重定向到本地文件。
- cd <directory>：更改服务器上的当前目录。
- lcd <directory>：更改本地机的当前目录。
- get <remote-file> [local-file]：下载文件，可以指定本地文件名。
- put <local-file> [remote-file]：上传文件，可以指定远程文件名。
- mget <remote-files>：下载多个文件。
- mput <local-files>：上传多个文件。
- binary：设置二进制传输模式，用于传输非文本文件。
- ascii：设置 ASCII 传输模式，用于传输文本文件。
- quit：断开连接并退出 FTP 客户端。

使用场景：

- 文件上传：将本地文件或文件夹上传到远程服务器，用于网站更新、备份存储等。
- 文件下载：从 FTP 服务器下载文件或目录到本地，用于获取公开共享的

资源、软件更新包等。

- 网站管理：网站管理员经常使用 FTP 来部署新的网页内容或更新现有内容。
- 数据备份和恢复：通过 FTP 将重要数据备份到远端服务器，或从远端服务器恢复数据到本地。
- 文件共享：在需要共享大文件时，FTP 是一个传统但有效的选择。

十、Telnet 命令

telnet 命令是一个基于命令行的通信协议工具，用于远程登录到另一台计算机上。通过 telnet，用户可以在本地计算机上模拟终端，以访问远程服务器。它主要用于远程管理网络设备和服务器，或进行故障排除。尽管 telnet 因其不加密传输数据而逐渐被更安全的协议如 SSH（Secure Shell）所取代，但在某些特定环境和应用中，它仍然被使用。

主要参数说明：

- <hostname> 或 <IP 地址>：指定要连接的远程主机名称或 IP 地址。
- <port>：（可选）连接到远程主机的端口号，默认端口为 23。
- -l <username>：指定登录远程主机时使用的用户名。
- -a：自动登录，使用当前用户的用户名。
- -e <escape char>：设置退出 telnet 会话的转义字符，默认为 Ctrl+]。

使用场景：

- 远程设备管理：telnet 可以用于远程访问和管理网络设备，如路由器、交换机等，尤其是在这些设备尚未配置 SSH 访问时。
- 测试网络服务：通过 telnet 连接到特定的端口，可以测试网络服务（如 SMTP、HTTP、FTP 等）是否在运行，这对于网络管理员在进行故障排除时非常有用。
- 教育和学习：telnet 提供了一个简单的环境来学习网络协议和终端操作，对于网络和安全领域的学生来说，这是一个很好的学习工具。
- 旧式系统维护：在一些老旧的系统或设备中，telnet 可能是唯一可用的远程访问方法，因此在特定情况下，系统管理员可能需要使用它进行维护工作。

【实验设备】

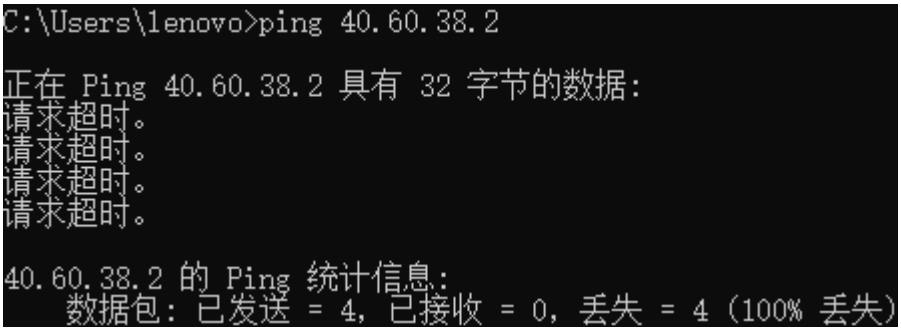
1. 操作系统：Windows 11
2. 网络环境：Wi-Fi 连接

【实验步骤】

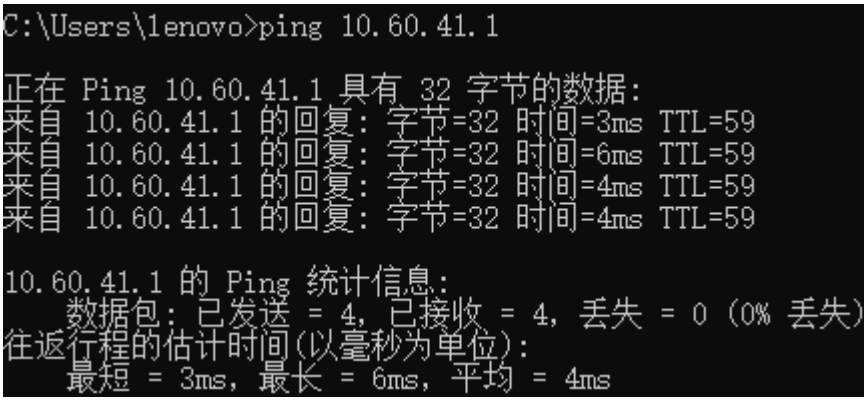
1. 测试 Ping 相关命令。
2. 测试 Ipconfig 相关命令。
3. 测试 Nbtstat 相关命令。
4. 测试 Tracert 相关命令。
5. 测试 Net 相关命令。
6. 测试 Route 相关命令。
7. 测试 Nslookup 相关命令。
8. 测试 Netsh 相关命令。
9. 测试 Ftp 相关命令。
10. 测试 Telnet 相关命令。

【实验现象】

1. 使用 ping 40.60.38.2 命令测试网络是否通畅，结果显示网络不通畅。



2. 使用 ping 10.60.41.1 命令测试网络是否通畅，结果显示网络通畅。



3. 使用 ping -a MINMUSLIN 命令获取计算机的 IP 地址。

```
C:\Users\lenovo>ping -a MINMUSLIN

正在 Ping MinmusLin [fe80::d4b1:99a9:f47d:2d51%26] 具有 32 字节的数据:
来自 fe80::d4b1:99a9:f47d:2d51%26 的回复: 时间<1ms
来自 fe80::d4b1:99a9:f47d:2d51%26 的回复: 时间<1ms
来自 fe80::d4b1:99a9:f47d:2d51%26 的回复: 时间<1ms
来自 fe80::d4b1:99a9:f47d:2d51%26 的回复: 时间<1ms

fe80::d4b1:99a9:f47d:2d51%26 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 0ms, 平均 = 0ms
```

4. 使用 ipconfig 命令显示所有网络接口的 IP 地址、子网掩码和默认网关。

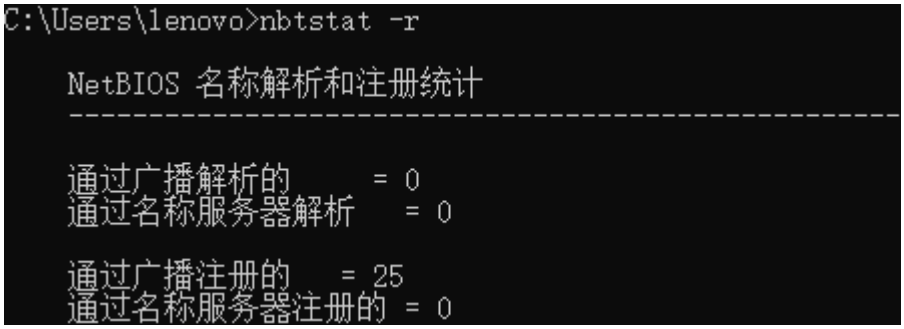
```
C:\Users\lenovo>ipconfig

Windows IP 配置


以太网适配器 以太网:

   媒体状态  . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . . . :

未知适配器 本地连接:

   媒体状态  . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . . . :

无线局域网适配器 本地连接* 3:

   媒体状态  . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . . . :

无线局域网适配器 本地连接* 12:

   媒体状态  . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . . . :

以太网适配器 以太网 3:

   媒体状态  . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . . . :

以太网适配器 VMware Network Adapter VMnet1:

   连接特定的 DNS 后缀 . . . . . . . :
   本地链接 IPv6 地址. . . . . . . . : fe80::56ef:3fcc:a3dd:cb3d%2
   IPv4 地址 . . . . . . . . . . . . : 192.168.178.1
   子网掩码  . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . :

以太网适配器 VMware Network Adapter VMnet8:

   连接特定的 DNS 后缀 . . . . . . . :
   本地链接 IPv6 地址. . . . . . . . : fe80::d4b1:99a9:f47d:2d51%26
   IPv4 地址 . . . . . . . . . . . . : 192.168.216.1
   子网掩码  . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . :
```

5. 使用 ipconfig /all 命令显示所有配置信息。

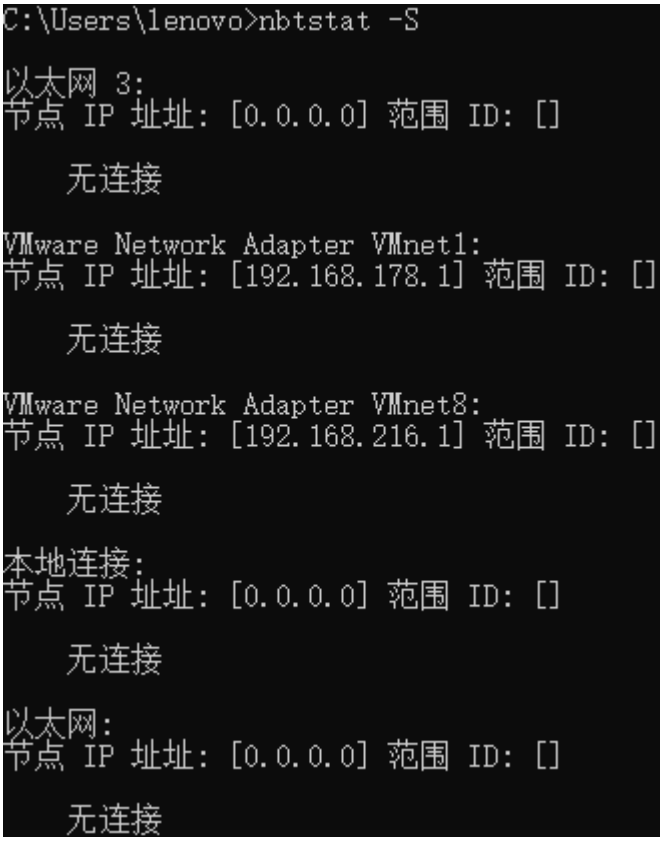
6. 使用 nbtstat -c 命令显示 NetBIOS 名称缓存的内容，包括名称及其对应的 IP 地址。

7. 使用 nbtstat -n 命令显示本地 NetBIOS 名称表。

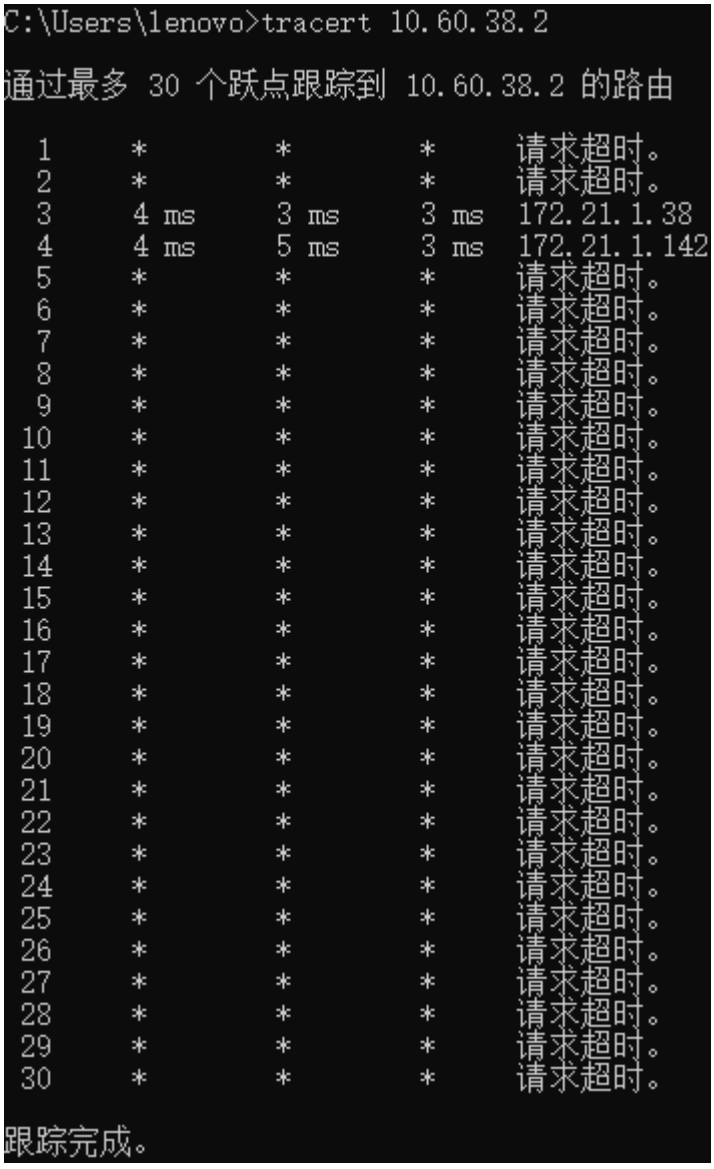
8. 使用 nbtstat -r 命令显示 NetBIOS 名称解析统计信息，包括成功的和失败的名称解析尝试。



9. 使用 nbtstat -S 命令显示当前会话表,包括与远程计算机的 NetBIOS 会话。



10. 使用 tracert 10.60.38.2 命令追踪数据包从执行该命令的设备到目的 IP 地址 10.60.38.2 的路由路径。



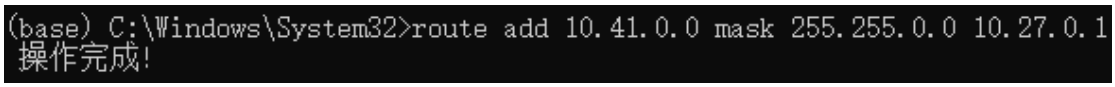
11. 使用 net start 命令显示已经启动的 Windows 服务。

12. 使用 route PRINT 命令显示当前的 IP 路由表。

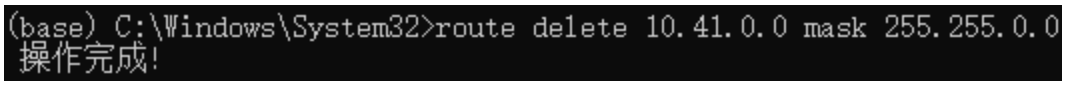
```
C:\Users\lenovo>route PRINT
===========================================================================
接口列表
 24...88 a4 c2 22 79 31 ......Realtek PCIe GbE Family Controller
 13...00 ff 47 e7 31 e5 ......Array Networks TAP-Windows Adapter
 11...d4 54 8b 33 2b 7f ......Microsoft Wi-Fi Direct Virtual Adapter #3
  7...d6 54 8b 33 2b 7e ......Microsoft Wi-Fi Direct Virtual Adapter #4
 14...00 ff 5c f8 8a 1e ......Netease UU TAP-Win32 Adapter V9.21
  2...00 50 56 c0 00 01 ......VMware Virtual Ethernet Adapter for VMnet1
 26...00 50 56 c0 00 08 ......VMware Virtual Ethernet Adapter for VMnet8
  6...d4 54 8b 33 2b 7e ......Intel(R) Wi-Fi 6 AX201 160MHz
  4...d4 54 8b 33 2b 82 ......Bluetooth Device (Personal Area Network)
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 路由表
===========================================================================
活动路由:
网络目标        网络掩码          网关       接口   跃点数
          0.0.0.0          0.0.0.0   100.81.255.254    100.81.138.91     45
        100.80.0.0      255.254.0.0         在链路上     100.81.138.91    301
     100.81.138.91  255.255.255.255         在链路上     100.81.138.91    301
    100.81.255.255  255.255.255.255         在链路上     100.81.138.91    301
        127.0.0.0        255.0.0.0         在链路上          127.0.0.1    331
        127.0.0.1  255.255.255.255         在链路上          127.0.0.1    331
  127.255.255.255  255.255.255.255         在链路上          127.0.0.1    331
    192.168.178.0    255.255.255.0         在链路上     192.168.178.1    291
    192.168.178.1  255.255.255.255         在链路上     192.168.178.1    291
  192.168.178.255  255.255.255.255         在链路上     192.168.178.1    291
    192.168.216.0    255.255.255.0         在链路上     192.168.216.1    291
    192.168.216.1  255.255.255.255         在链路上     192.168.216.1    291
  192.168.216.255  255.255.255.255         在链路上     192.168.216.1    291
        224.0.0.0        240.0.0.0         在链路上          127.0.0.1    331
        224.0.0.0        240.0.0.0         在链路上     192.168.178.1    291
        224.0.0.0        240.0.0.0         在链路上     192.168.216.1    291
        224.0.0.0        240.0.0.0         在链路上     100.81.138.91    301
  255.255.255.255  255.255.255.255         在链路上          127.0.0.1    331
  255.255.255.255  255.255.255.255         在链路上     192.168.178.1    291
  255.255.255.255  255.255.255.255         在链路上     192.168.216.1    291
  255.255.255.255  255.255.255.255         在链路上     100.81.138.91    301
===========================================================================
永久路由:
  无
```

```
IPv6 路由表
===========================================================================
活动路由:
 接口跃点数网络目标                 网关
  6    301 ::/0                     fe80::9e54:c2ff:fe0d:5002
  1    331 ::1/128                  在链路上
  6    301 2001:da8:8002:6bd1::/64  在链路上
  6    301 2001:da8:8002:6bd1:3da8:a8dd:269f:38c7/128
                                    在链路上
  6    301 2001:da8:8002:6bd1:c18e:2f3d:a347:f6fd/128
                                    在链路上
  6    301 fd14:44b7:386d::/64      fe80::53:66f3:7828:7963
  2    291 fe80::/64                在链路上
 26    291 fe80::/64                在链路上
  6    301 fe80::/64                在链路上
  2    291 fe80::56ef:3fcc:a3dd:cb3d/128
                                    在链路上
  6    301 fe80::b6ff:9493:f8d0:9a9e/128
                                    在链路上
 26    291 fe80::d4b1:99a9:f47d:2d51/128
                                    在链路上
  1    331 ff00::/8                 在链路上
  2    291 ff00::/8                 在链路上
 26    291 ff00::/8                 在链路上
  6    301 ff00::/8                 在链路上
===========================================================================
永久路由:
  无
```

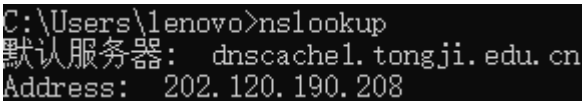
13. 使用 route add 10.41.0.0 mask 255.255.0.0 10.27.0.1 命令添加目标为 10.41.0.0，子网掩码为 255.255.0.0，下一个跃点地址为 10.27.0.1 的路由。



14. 使用 route delete 10.41.0.0 mask 255.255.0.0 移除目的地为 10.41.0.0，子网掩码为 255.255.0.0 的路由。



15. 使用 nslookup 显示域名信息。



【分析讨论】

通过本次实验，我不仅掌握了各种基本网络测试工具的使用，还加深了对 TCP/IP 协议的理解。我学会了如何利用这些工具来诊断和解决网络问题，了解了它们在不同场景下的应用。此外，本次实验还提高了我分析和解决网络问题的能力，对于将来的网络管理和维护工作打下了坚实的基础。