

实验(四)：基本网络测试工具及应用工具实验

一.实验目的

- 掌握基本网络测试工具及应用工具的使用方法
- 利用网络测试工具简单判断网络的具体实际状况
- 学习和实践使用 ping命令、ipconfig命令、nbtstat命令、tracert命令、net命令、route命令、nslookup命令、netsh命令、ftp命令、telnet命令等常用命令

二.实验原理

- 操作系统中也内置了一些非常有用的软件网络测试工具，使用得当并掌握一定的测试技巧一般来说是完全可以满足一般需求的，有的甚至被黑客作为黑客工具。有许多黑客工具软件也是基于这些内置的网络测试软件而编制、改写的。这些工具虽然不能称之为专业测试工具，但可以简单判断网络的具体实际状况。
- 命令的基本格式：
 - Command + option
 - 一般 cmd /? 是该命令的帮助信息。如：ipconfig /?

三.实验环境

- 操作系统：windows 11
- 网络环境：wifi连接

四.实验步骤（此处仅选取五个命令中各自一个参数执行）

- ping命令
 - ping命令是Windows9X/NT中集成的一个专用于 TCP/IP协议的测试工具，ping命令是用于查看网络上的主机是否在工作，它是通过向该主机发送 ICMP ECHO_REQUEST包进行测试而达到目的的。一般凡是应用TCP/IP协议的局域或广域网络，不管你是内部有几台电脑的家庭、办公室局域网、还是校园网、企业网甚至Internet国际互联网络，当客户端与客户端之间无法正常进行访问或者网络工作出现各种不稳定的情况时，可以用用Ping这个命令来测试一下网络的通信是否正常，多数时候是可以一次奏效的。

序号	参数	描述
1	-t	Ping 指定的计算机直到中断。

序号	参数	描述
2	-a	将地址解析为计算机名。
3	-n count	发送 count 指定的 ECHO 数据包数。默认值为 4。
4	-l length	发送包含由 length 指定的数据量的 ECHO 数据包。默认为 32 字节；最大值是 65,500。
5	-f	在数据包中发送“不要分段”标志。数据包就不会被路由上的网关分段。
6	-i ttl	将“生存时间”字段设置为 ttl 指定的值。
7	-v tos	将“服务类型”字段设置为 tos 指定的值。
8	-r count	在“记录路由”字段中记录传出和返回数据包的路由。count 可以指定最少1台，最多9台计算机。
9	-s count	指定 count 指定的跃点数的时间戳，最多也只记录4个。
10	-j computer-list	利用 computer-list 指定的计算机列表路由数据包。连续计算机可以被中间网关分隔（路由稀疏源）IP 允许的最大数量为 9。
11	-k computer-list	利用 computer-list 指定的计算机列表路由数据包。连续计算机不能被中间网关分隔（路由严格源）IP 允许的最大数量为 9。
12	-w timeout	指定超时间隔，单位为毫秒。
13	destination-list	是指要测试的主机名或IP地址。

- **ipconfig命令**

- **ipconfig命令** 主要用于发现和解决TCP/IP 网络问题，可以用该工具获得主机配置信息，包括IP 地址、子网掩码和默认网关等等

◦

序号	参数	描述
1	/all	显示与TCP/IP协议相关的所有细节信息，其中包括测试的主机名、IP地址、子网掩码、节点类型、是否启用IP路由、网卡的物理地址、默认网关等。

序号	参数	描述
2	/batch file	将测试的结果存入指定的“file”文件名中，以便于逐项查看，如果省略file文件名，则系统会把这测试的结果保存在系统的winipcfg.out文件中。
3	/renew all	更新全部适配器的通信配置情况，所有测试重新开始。
4	/release all	释放全部适配器的通信配置情况。
5	/renew n	更新第n号适配器的通信配置情况，所有测试重新开始。
6	/release n	释放第n号适配器的通信配置情况。

- **nbtstat命令**

- **nbtstat命令** 用于查看当前基于NETBIOS的TCP/IP 连接状态，通过该工具你可以获得远程或本地机器的组名和机器名。虽然用户使用ipconfig/winipcfg工具可以准确地得到主机的网卡地址，但对于一个已建成的比较大型的局域网，要去每台机器上进行这样的操作就显得过于费事了。网管人员通过在自己上网的机器上使用DOS命令 **nbtstat**，可以获取另一台上网主机的网卡地址

o.

序号	参数	描述
1	-a Remotename	使用远程计算机的名称列出其名称表，此参数可以通过远程计算机的NetBios名来查看他的当前状态。
2	-A IP address	使用远程计算机的 IP 地址并列出名称表，这个和-a不同的是就是这个只能使用IP。其实-a就包括了-A的功能了。
3	-c	列出远程计算机的NetBIOS名称的缓存和每个名称的IP地址。这个参数用来列出在你的NetBIOS里缓存的连接过的计算机的IP。
4	-n	列出本地机的NetBIOS名称。

- **tracert命令**

- **tracert命令**（跟踪路由）是路由跟踪实用程序，用于确定IP数据报访问目标所采取的路径。Tracert命令用IP生存时间(TTL)字段和ICMP错误消息来确定从一个主机到网络上其他主机的路由。

序号	参数	描述
1	-d	指定不将 IP 地址解析到主机名称。
2	-h maximum_hops	指定跃点数以跟踪到称为 target_name 的主机的路由。
3	-j host-list	指定 Tracert 实用程序数据包所采用路径中的路由器接口列表。
4	-w timeout	等待 timeout 为每次回复所指定的毫秒数

- target_name：目标主机的名称或 IP 地址。

• Route命令

- Route命令用于显示和控制机器IP的路由表，主要显示的信息有：目标地址、网络掩码、网关和本地IP地址等

序号	参数	描述
1	-f	除所有不是主路由（网掩码为255.255.255.255的路由）、环回网络路由（目标为127.0.0.0，网掩码为255.255.255.0的路由）或多播路由（目标为224.0.0.0，网掩码为240.0.0.0的路由）的条目的路由表。如果它与命令之一（例如add、change或删除）结合使用，表会在运行命令之前清除。
2	-p	与add命令共同使用时，指定路由被添加到注册表并在启动TCP/IP协议的时候初始化IP路由表。默认情况下，启动TCP/IP协议时不会保存添加的路由。与print命令一起使用时，则显示永久路由列表。所有其他的命令都忽略此参数。
3	add	添加路由
4	change	更改现存路由
5	delete	删除路由
6	print	打印路由Destination

五、实验现象

• ping -a命令

- 在命令行输入 ping -a 127.0.0.1后使用回车，得到下图所示的信息

```
C:\ 命令提示符

Microsoft Windows [版本 10.0.22631.3155]
(c) Microsoft Corporation。保留所有权利。

C:\Users\10728>ping -a 127.0.0.1

正在 Ping DESKTOP-R2A6L7J [127.0.0.1] 具有 32 字节的数据:
来自 127.0.0.1 的回复: 字节=32 时间<1ms TTL=64
来自 127.0.0.1 的回复: 字节=32 时间<1ms TTL=64
来自 127.0.0.1 的回复: 字节=32 时间<1ms TTL=64
来自 127.0.0.1 的回复: 字节=32 时间<1ms TTL=64

127.0.0.1 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
```

- 使用 `ping -a 127.0.0.1` 将ip地址127.0.0.1解析为计算机名 `DESKTOP-R2A6L7J`
- `ipconfig /all`命令
 - 在命令行输入 `ipconfig /all` 后使用回车，得到下图所示的信息

```
C:\Users\10728>ipconfig /all

Windows IP 配置

   主机名 . . . . . : DESKTOP-R2A6L7J
   主 DNS 后缀 . . . . . :
   节点类型 . . . . . : 混合
   IP 路由已启用 . . . . . : 否
   WINS 代理已启用 . . . . . : 否
   DNS 后缀搜索列表 . . . . . : tongji.edu.cn

无线局域网适配器 本地连接* 1:

   媒体状态 . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . :
   描述. . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   物理地址. . . . . : F0-9E-4A-4C-A9-15
   DHCP 已启用 . . . . . : 是
   自动配置已启用. . . . . : 是

无线局域网适配器 本地连接* 2:

   媒体状态 . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . :
   描述. . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   物理地址. . . . . : F2-9E-4A-4C-A9-14
```

```
无线局域网适配器 WLAN:

    连接特定的 DNS 后缀 . . . . . : tongji.edu.cn
    描述. . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
    物理地址. . . . . : F0-9E-4A-4C-A9-14
    DHCP 已启用 . . . . . : 是
    自动配置已启用. . . . . : 是
    IPv6 地址 . . . . . : 2001:da8:8002:6bd1:cfb2:32c9:500e:409d(首选)
    临时 IPv6 地址. . . . . : 2001:da8:8002:6bd1:f53c:41ca:c014:d10d(首选)
    本地链接 IPv6 地址. . . . . : fe80::ca4f:13f3:770b:c43f%7(首选)
    IPv4 地址 . . . . . : 100.81.229.48(首选)
    子网掩码 . . . . . : 255.254.0.0
    获得租约的时间 . . . . . : 2024年3月7日 10:00:21
    租约过期的时间 . . . . . : 2024年3月7日 12:00:21
    默认网关. . . . . : fe80::9e54:c2ff:fe0d:5002%7
                          100.81.255.254
    DHCP 服务器 . . . . . : 100.81.255.254
    DHCPv6 IAID . . . . . : 82878026
    DHCPv6 客户端 DUID . . . . . : 00-01-00-01-2A-B4-FB-A8-FC-34-97-DD-73-9D
    DNS 服务器 . . . . . : 202.120.190.208
                          202.120.190.108

    TCP/IP 上的 NetBIOS . . . . . : 已启用
```

- 使用 `ipconfig /all` 显示与TCP/IP协议相关的所有细节信息，其中包括测试的主机名、IP地址、子网掩码、节点类型、是否启用IP路由、网卡的物理地址、默认网关等信息
- `nbtstat -n`命令
 - 在命令行输入 `nbtstat -n` 后使用回车，得到下图所示的信息

```
C:\Users\10728>nbtstat -n

VMware Network Adapter VMnet1:
节点 IP 地址: [169.254.198.131] 范围 ID: []

NetBIOS 本地名称表

名称                类型                状态
-----
DESKTOP-R2A6L7J<00>  唯一                已注册
DESKTOP-R2A6L7J<20>  唯一                已注册
WORKGROUP             <00> 组              已注册

VMware Network Adapter VMnet8:
节点 IP 地址: [169.254.60.1] 范围 ID: []

NetBIOS 本地名称表

名称                类型                状态
-----
DESKTOP-R2A6L7J<00>  唯一                已注册
DESKTOP-R2A6L7J<20>  唯一                已注册
WORKGROUP             <00> 组              已注册

以太网:
节点 IP 地址: [0.0.0.0] 范围 ID: []

缓存中没有名称

蓝牙网络连接:
节点 IP 地址: [0.0.0.0] 范围 ID: []

缓存中没有名称

WLAN:
节点 IP 地址: [100.79.209.191] 范围 ID: []

NetBIOS 本地名称表

名称                类型                状态
-----
DESKTOP-R2A6L7J<00>  唯一                已注册
DESKTOP-R2A6L7J<20>  唯一                已注册
WORKGROUP             <00> 组              已注册
```

- `nbtstat -n` 是一个用于 Windows 系统的命令行工具，用于显示 NetBIOS 名称缓存的内容。NetBIOS (Network Basic Input/Output System) 是一种在局域网上用于通信的协议。`nbtstat -n` 命令的作用是列出当前系统中的 NetBIOS 名称缓存，显示本地计算机已经解析的 NetBIOS 名称及其对应的 IP 地址。通过运行 `nbtstat -n` 命令，可以了解到系统中哪些 NetBIOS 名称已经被解析，并且对应了哪些 IP 地址。这对于故障排除和网络调试是非常有用的。
- `tracert -d 127.0.0.1`命令
 - 在命令行输入 `tracert -d 127.0.0.1`后使用回车，得到下图所示的信息

```
C:\Users\10728>tracert -d 127.0.0.1

通过最多 30 个跃点跟踪到 127.0.0.1 的路由

 1    <1 毫秒    <1 毫秒    <1 毫秒 127.0.0.1
跟踪完成。
```

- `tracert` 命令用于在网络中跟踪数据包的路由路径。而 `127.0.0.1` 是一个特殊的IP地址，表示本地主机，也称为回环地址。因此，`tracert -d 127.0.0.1` 命令的作用是在本地主机上执行路由跟踪，即查看数据包从本地主机发送到本地主机的过程中经过的路由路径。`-d` 选项是用来指示不要进行反向 DNS 查询，这样会加快路由跟踪的速度。在本地主机上执行 `tracert -d 127.0.0.1` 命令将会显示本地主机到自身的路由路径，通常只会显示一个跳点，因为数据包并不会离开本地主机，而是在本地主机内部进行传输。
- `route print` 命令
 - 在命令行输入 `route print` 后使用回车，得到下图所示的信息

```
C:\Users\10728>route print

=====
接口列表
11...f0 9e 4a 4c a9 15 .....Microsoft Wi-Fi Direct Virtual Adapter
9...f2 9e 4a 4c a9 14 .....Microsoft Wi-Fi Direct Virtual Adapter #2
6...00 50 56 c0 00 01 .....VMware Virtual Ethernet Adapter for VMnet1
4...00 50 56 c0 00 08 .....VMware Virtual Ethernet Adapter for VMnet8
7...f0 9e 4a 4c a9 14 .....Intel(R) Wi-Fi 6 AX201 160MHz
17...f0 9e 4a 4c a9 18 .....Bluetooth Device (Personal Area Network)
13...fc 34 97 dd 73 9d .....Realtek PCIe GbE Family Controller
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    100.81.229.48    45
100.80.0.0      255.255.0.0      在链路上        100.81.229.48    301
100.81.229.48   255.255.255.255   在链路上        100.81.229.48    301
100.81.255.255  255.255.255.255   在链路上        100.81.229.48    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
169.254.0.0     255.255.0.0      在链路上        169.254.198.131  291
169.254.0.0     255.255.0.0      在链路上        169.254.60.1     291
169.254.60.1    255.255.255.255   在链路上        169.254.60.1     291
169.254.198.131 255.255.255.255   在链路上        169.254.198.131  291
```

- `route print` 命令是 Windows 操作系统中的一个命令行工具，其主要作用是显示计算机的路由表信息。通过该命令，可以查看当前系统的 IP 路由表，包括目标网络地址、子网掩码、网关、接口和路由指标等重要信息。此外，命令还显示与每个网络连接相关的信息，如接口名称、IP 地址和网关地址。通过分析路由表信息，网络管理员可以进行网络故障排除，例如检查路由设置或网关配置是否正确，并了解数据包的传输路径和网关选择。因此，`route print` 是管理网络连接和进行网络故障排除的重要工具之一。

六、实验结论

- 实验中，我使用了几个常用的网络测试工具及应用命令进行了测试，包括 `ping`、`ipconfig`、`nbtstat`、`tracert` 和 `route` 命令。以下是每个命令的实验结果和总结：
 - `ping` 命令：

- 实验中，我使用了 `ping -a 127.0.0.1` 命令来测试本地回环地址的连通性，并将IP地址解析为计算机名。
- 结果显示成功与本地主机进行通信，并将IP地址成功解析为计算机名 `DESKTOP-R2A6L7J`。
- 通过该命令，我们可以验证本地主机的网络连接和解析IP地址的功能。
- `ipconfig`命令：
 - 我们使用了 `ipconfig /all` 命令，查看了本地网络连接的详细信息，包括IP地址、子网掩码、默认网关等。
 - 实验结果显示了本地网络配置的各项参数，并且提供了有关网络连接的完整信息。
 - 通过 `ipconfig` 命令，我们可以全面了解本地网络配置情况，方便进行网络故障排除和配置调整。
- `nbtstat`命令：
 - 通过 `nbtstat -n` 命令，我们查看了当前系统中的NetBIOS名称缓存。
 - 结果显示了已解析的NetBIOS名称及其对应的IP地址。
 - 通过该命令，我们可以了解到系统中哪些NetBIOS名称已被解析，并且对应了哪些IP地址，方便进行网络调试和故障排除。
- `tracert`命令：
 - 使用 `tracert -d 127.0.0.1` 命令，我们在本地主机上执行了路由跟踪。
 - 实验结果显示了数据包从本地主机发送到本地主机的路由路径，通常只显示一个跳点。
 - 通过 `tracert` 命令，我们可以了解数据包的传输路径，便于进行网络调试和性能优化。
- `route`命令：
 - 我们使用了 `route print` 命令，查看了当前系统的IP路由表。
 - 结果显示了目标网络地址、子网掩码、网关、接口等信息。
 - 通过该命令，我们可以了解数据包的传输路径和网关选择，有助于网络连接的管理和故障排除。
- 综上所述，通过对这些常用网络测试工具及应用命令的实验，我掌握了它们的基本使用方法，并且能够利用它们简单判断网络的实际状况，从而更好地进行网络调试和故障排除。这将对后续的实验有所帮助。