

北京林业大学实验报告

2020 学年—2021 学年第 1 学期 计算机网络 实验报告

姓名： 连月菡 学号： 1810022222 班级： 计创 18

专业： 计创 实验学时： 2 学时 任课教师： 袁津生

实验题目： 实验一：网络常用命令的使用

实验环境： Windows 10 家庭版

实验目的：

掌握常用的网络命令，尤其是各命令在不同参数下的形式。

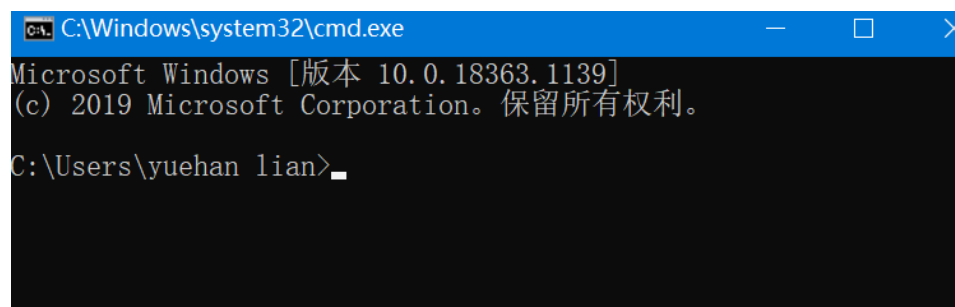
实验要求：

在《计算机网络》的课程实验过程中，要求学生做到：

- (1) 预习实验指导书有关部分，认真做好实验内容的准备，就实验可能出现的情况提前作出思考和分析。
- (2) 仔细观察上机和上网操作时出现的各种现象，记录主要情况，做出必要说明和分析。
- (3) 认真书写实验报告。实验报告包括实验目的和要求，实验环境及实验结果分析。
- (4) 实验课程不迟到。如不能出席，所缺实验一律不补。
- (5) 实验过程中要注意命令之间的空格！

实验内容：

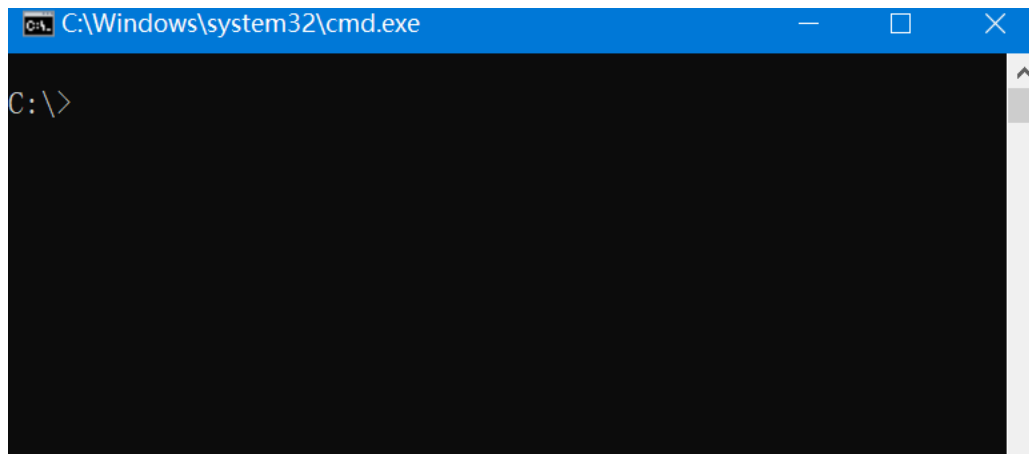
首先打开计算机，选择“VMWare”菜单，进入 Windows 操作系统。然后进入命令提示符状态。如下所示：



```
C:\Windows\system32\cmd.exe
Microsoft Windows [版本 10.0.18363.1139]
(c) 2019 Microsoft Corporation。保留所有权利。

C:\Users\yuehan lian>
```

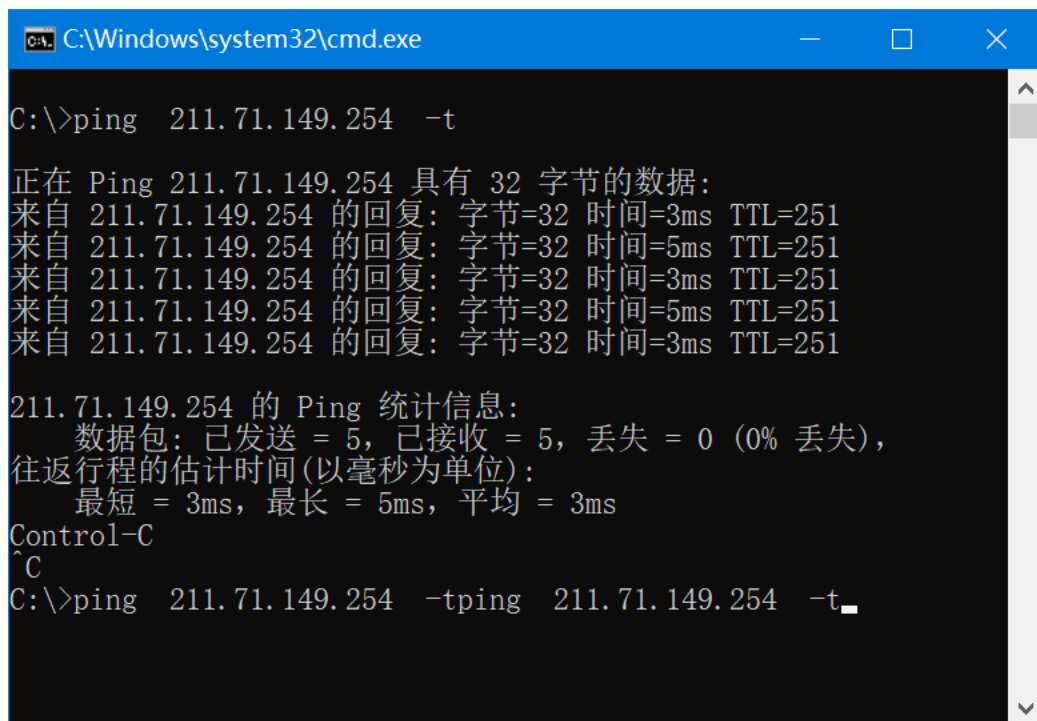
在该状态下，键入命令“cd\”回车和命令“cls”回车。如下所示：



1. 最基本，最常用的，测试网络连通性命令

`ping 211.71.149.254 -t`，参数-t 等待用户去中断测试

中断使用命令：Ctrl+c



2. 查看 DNS、IP、Mac 等

①使用命令：`ipconfig/all`

```
C:\Windows\system32\cmd.exe
C:\>ipconfig/all

Windows IP 配置

   主机名 . . . . . : DESKTOP-Q6RJGIF
   主 DNS 后缀 . . . . . :
   节点类型 . . . . . : 混合
   IP 路由已启用 . . . . . : 否
   WINS 代理已启用 . . . . . : 否

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. . . . . : 38-DE-AD-86-26-63
   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* 10:

   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. . . . . : 3A-DE-AD-86-26-62
   DHCP 已启用 . . . . . : 是
   自动配置已启用. . . . . : 是

无线局域网适配器 WLAN:

   连接特定的 DNS 后缀 . . . . . :
   描述. . . . . : Intel(R) Dual Band Wireless-AC 3165
   物理地址. . . . . : 38-DE-AD-86-26-62
   DHCP 已启用 . . . . . : 是
   自动配置已启用. . . . . : 是
   本地链接 IPv6 地址. . . . . : fe80::8906:b7f4:8803:f023%18(首选)
   IPv4 地址 . . . . . : 172.26.233.171(首选)
   子网掩码 . . . . . : 255.255.128.0
   获得租约的时间 . . . . . : 2020年11月1日 21:14:00
   租约过期的时间 . . . . . : 2020年11月3日 18:40:15
   默认网关. . . . . : 172.26.128.1
   DHCP 服务器 . . . . . : 172.26.128.3
   DHCPv6 IAID . . . . . : 121167533
   DHCPv6 客户端 DUID . . . . . : 00-01-00-01-25-E7-D4-B3-38-DE-AD-86-26-62
   DNS 服务器 . . . . . : 202.204.112.66
                           202.204.112.67
                           202.204.112.87
   TCPIP 上的 NetBIOS . . . . . : 已启用

C:\>
```

②使用命令：NSLOOKUP

```
C:\Windows\system32\cmd.exe

TCPIP 上的 NetBIOS . . . . . : 已启用

C:\>nslookup
默认服务器: beilin.bjfu.edu.cn
Address: 202.204.112.66

>
C:\>
```

4. 探测对方计算机名，所在的组、域及当前用户名

命令: ping -a IP -t

例如: ping -a 211.71.149.254 -t

```
C:\Windows\system32\cmd.exe
>
C:\>ping -a 211.71.149.254 -t

正在 Ping 211.71.149.254 具有 32 字节的数据:
来自 211.71.149.254 的回复: 字节=32 时间=4ms TTL=251
来自 211.71.149.254 的回复: 字节=32 时间=3ms TTL=251
来自 211.71.149.254 的回复: 字节=32 时间=2ms TTL=251
来自 211.71.149.254 的回复: 字节=32 时间=3ms TTL=251
来自 211.71.149.254 的回复: 字节=32 时间=3ms TTL=251
来自 211.71.149.254 的回复: 字节=32 时间=3ms TTL=251
来自 211.71.149.254 的回复: 字节=32 时间=3ms TTL=251
来自 211.71.149.254 的回复: 字节=32 时间=3ms TTL=251
来自 211.71.149.254 的回复: 字节=32 时间=3ms TTL=251
来自 211.71.149.254 的回复: 字节=32 时间=3ms TTL=251

211.71.149.254 的 Ping 统计信息:
    数据包: 已发送 = 9, 已接收 = 9, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 2ms, 最长 = 4ms, 平均 = 3ms
Control-C
^C
C:\>_
```

若要比对全的显示 NetBIOS 名可使用命令。

命令: nbtstat -a 自己当前使用的计算机 IP 地址

nbtstat -a 对方计算机 IP 地址

5. 显示出本机当前所开放的所有端口

命令: netstat -a

```
C:\Windows\system32\cmd.exe - netstat -a

C:\>netstat -a

活动连接

 协议 本地地址          外部地址          状态
TCP    0.0.0.0:135        DESKTOP-Q6RJGIF:0 LISTENING
TCP    0.0.0.0:445        DESKTOP-Q6RJGIF:0 LISTENING
TCP    0.0.0.0:1024       DESKTOP-Q6RJGIF:0 LISTENING
TCP    0.0.0.0:1080       DESKTOP-Q6RJGIF:0 LISTENING
TCP    0.0.0.0:3306       DESKTOP-Q6RJGIF:0 LISTENING
TCP    0.0.0.0:5040       DESKTOP-Q6RJGIF:0 LISTENING
TCP    0.0.0.0:33060      DESKTOP-Q6RJGIF:0 LISTENING
TCP    0.0.0.0:49664      DESKTOP-Q6RJGIF:0 LISTENING
TCP    0.0.0.0:49665      DESKTOP-Q6RJGIF:0 LISTENING
TCP    0.0.0.0:49666      DESKTOP-Q6RJGIF:0 LISTENING
TCP    0.0.0.0:49667      DESKTOP-Q6RJGIF:0 LISTENING
TCP    0.0.0.0:49668      DESKTOP-Q6RJGIF:0 LISTENING
TCP    127.0.0.1:1025     DESKTOP-Q6RJGIF:1026 ESTABLISHED
TCP    127.0.0.1:1026     DESKTOP-Q6RJGIF:1025 ESTABLISHED
TCP    127.0.0.1:1080     DESKTOP-Q6RJGIF:12920 TIME_WAIT
TCP    127.0.0.1:1080     DESKTOP-Q6RJGIF:12922 TIME_WAIT
TCP    127.0.0.1:1080     DESKTOP-Q6RJGIF:12924 TIME_WAIT
TCP    127.0.0.1:11752    DESKTOP-Q6RJGIF:0 LISTENING
TCP    127.0.0.1:12960    DESKTOP-Q6RJGIF:1080 TIME_WAIT
TCP    127.0.0.1:12992    DESKTOP-Q6RJGIF:50053 SYN_SENT
TCP    127.0.0.1:27018    DESKTOP-Q6RJGIF:0 LISTENING
TCP    127.0.0.1:28317    DESKTOP-Q6RJGIF:0 LISTENING
TCP    172.26.233.171:139 DESKTOP-Q6RJGIF:0 LISTENING
TCP    172.26.233.171:2654 40.119.211.203:https ESTABLISHED
TCP    172.26.233.171:12851 40.119.211.203:https ESTABLISHED
TCP    172.26.233.171:12909 211.71.149.87:ftp ESTABLISHED
TCP    172.26.233.171:12921 170.106.159.229:https TIME_WAIT
```

比较详细的显示本机网络资料，包括 TCP、UDP、ICMP 和 IP 的统计，可用命令：

```
netstat -s -e
```

```
C:\Windows\system32\cmd.exe
TCP 172.26.233.171:12925 170.106.159.229:https TIME_WAIT
^C
C:\>netstat -s -a

IPv4 统计信息

接收的数据包 = 6665364
接收的标头错误 = 0
接收的地址错误 = 4215
转发的数据报 = 0
接收的未知协议 = 0
丢弃的接收数据包 = 2161090
传送的接收数据包 = 6221820
输出请求 = 1568182
路由丢弃 = 0
丢弃的输出数据包 = 1201
输出数据包无路由 = 144
需要重新组合 = 907
重新组合成功 = 441
重新组合失败 = 0
数据报分段成功 = 0
数据报分段失败 = 0
分段已创建 = 0

IPv6 统计信息

接收的数据包 = 27328
接收的标头错误 = 0
接收的地址错误 = 22
转发的数据报 = 0
接收的未知协议 = 3
丢弃的接收数据包 = 10197
传送的接收数据包 = 208422
输出请求 = 187304
路由丢弃 = 0
丢弃的输出数据包 = 6
输出数据包无路由 = 0
```

6. 探测 arp 绑定（动态和静态）列表，显示所有连接本机的计算机，显示对方 IP 和 MAC 地址

首先使用网上邻居浏览临近的计算机后，使用命令：

命令：**arp -a**

```
C:\Windows\system32\cmd.exe
C:\>arp -a

接口: 172.26.233.171 --- 0x12
Internet 地址      物理地址      类型
172.26.128.1       44-a1-91-69-0a-17 动态
172.26.255.255     ff-ff-ff-ff-ff-ff 静态
224.0.0.22         01-00-5e-00-00-16 静态
224.0.0.251       01-00-5e-00-00-fb 静态
224.0.0.252       01-00-5e-00-00-fc 静态
239.255.255.250   01-00-5e-7f-ff-fa 静态
255.255.255.255   ff-ff-ff-ff-ff-ff 静态
```

我们可以捆绑 IP 和 MAC 地址，解决局域网内盗用 IP 的问题。

命令：**arp -s** 本机的 IP 地址 本机的 MAC 地址

```
管理员: C:\Windows\System32\cmd.exe
TCP/IP 上的 NetBIOS . . . . . : 已启用

C:\Windows\system32>arp -s 170.106.159.229 3A-DE-AD-86-26-62
```

解除网卡的 IP 与 MAC 地址的绑定，可使用命令：

命令：arp -d 本机的 IP 地址

C:\Windows\System32\cmd.exe

```
C:\Windows\system32>arp -d 170.106.159.229
```

7. 在网络邻居上隐藏本地计算机

隐藏命令：net config server /hidden:yes

开启命令：net config server /hidden:no

C:\Windows\System32\cmd.exe

```
C:\Windows\system32>net config server /hidden:yes  
命令成功完成。
```

```
C:\Windows\system32>net config server /hidden:no  
命令成功完成。
```

8. 几个 net 命令

(1) 显示当前工作组服务器列表，使用命令：

命令：net view

当不带选项使用本命令时，它就会显示当前域或网络上的计算机上的列表。

(2) 查看这个本机或其它计算机 IP 上的共享资源，但首先要先将本机或其它计算机设置好共享的文件夹，然后可以用命令：

命令：net view 本机的 IP 地址

可显示：资源共享名、类型、用途、注释等内容。

C:\Windows\System32\cmd.exe

```
C:\Windows\system32>net view 172.26.233.171  
在 172.26.233.171 的共享资源
```

共享名	类型	使用为	注释
-----	----	-----	----

shopping	Disk		
----------	------	--	--

命令成功完成。

3) 查看计算机上的用户帐号列表可使用命令：

命令：net user

管理员: C:\Windows\System32\cmd.exe

```
C:\Windows\system32>net user
```

\\DESKTOP-Q6RJGIF 的用户帐户

Administrator	DefaultAccount	Guest
DAGUtilityAccount	yuehan lian	

命令成功完成。

(4) 查看网络链接，可使用命令：

命令：net use

例如将本机的共享文件夹“ABC”映射为本地的 Z 盘，可使用命令：

命令：net use z: \\192.168.123.16\ABC

映射完毕之后。可以使用命令“dir z:”进行查看。

需要注意：首先要将 ABC 文件夹共享！

管理员: C:\Windows\System32\cmd.exe

```
C:\Windows\system32>net use z: \\172.26.233.171\shopping
命令成功完成。
```

```
C:\Windows\system32>net use
会记录新的网络连接。
```

状态	本地	远程	网络
OK	Z:	\\172.26.233.171\shopping	Microsoft Windows Network

命令成功完成。

(5) 记录和那些计算机有链接，可使用命令：

命令：net session

管理员: C:\Windows\System32\cmd.exe

```
C:\Windows\system32>net session
```

计算机	用户名	客户端类型	打开空闲时间
\\172.26.233.171	yuehan lian		0 00:00:24

命令成功完成。

9. netstat 命令

显示活动的 TCP 连接、计算机侦听的端口、以太网统计信息、IP 路由表、IPv4 统计信息（对于 IP、ICMP、TCP 和 UDP 协议）以及 IPv6 统计信息。使用时如果不带参数，netstat 显示活动的 TCP 连接。

语法：netstat [-a] [-e] [-n] [-o] [-p Protocol] [-r] [-s] [Interval]

参数

-a：显示所有活动的 TCP 连接以及计算机侦听的 TCP 和 UDP 端口。


```
C:\Windows\system32>netstat -a

活动连接

协议 本地地址 外部地址 状态
TCP 0.0.0.0:135 DESKTOP-Q6RJGIF:0 LISTENING
TCP 0.0.0.0:445 DESKTOP-Q6RJGIF:0 LISTENING
TCP 0.0.0.0:1024 DESKTOP-Q6RJGIF:0 LISTENING
TCP 0.0.0.0:3306 DESKTOP-Q6RJGIF:0 LISTENING
TCP 0.0.0.0:5040 DESKTOP-Q6RJGIF:0 LISTENING
TCP 0.0.0.0:33060 DESKTOP-Q6RJGIF:0 LISTENING
TCP 0.0.0.0:49664 DESKTOP-Q6RJGIF:0 LISTENING
TCP 0.0.0.0:49665 DESKTOP-Q6RJGIF:0 LISTENING
TCP 0.0.0.0:49666 DESKTOP-Q6RJGIF:0 LISTENING
TCP 0.0.0.0:49667 DESKTOP-Q6RJGIF:0 LISTENING
TCP 0.0.0.0:49668 DESKTOP-Q6RJGIF:0 LISTENING
TCP 127.0.0.1:1025 DESKTOP-Q6RJGIF:1026 ESTABLISHED
TCP 127.0.0.1:1026 DESKTOP-Q6RJGIF:1025 ESTABLISHED
TCP 127.0.0.1:14363 DESKTOP-Q6RJGIF:0 LISTENING
TCP 127.0.0.1:14729 DESKTOP-Q6RJGIF:50053 SYN_SENT
TCP 127.0.0.1:27018 DESKTOP-Q6RJGIF:0 LISTENING
TCP 127.0.0.1:28317 DESKTOP-Q6RJGIF:0 LISTENING
TCP 172.26.233.171:139 DESKTOP-Q6RJGIF:0 LISTENING
TCP 172.26.233.171:445 DESKTOP-Q6RJGIF:14687 ESTABLISHED
```

-e : 显示以太网统计信息，如发送和接收的字节数、数据包数。该参数可以与 -s 结合使用。

```
C:\Windows\system32>netstat -e

接口统计

接收的 发送的
字节 3843848608 75327752
单播数据包 5692224 678920
非单播数据包 1919680 3904
丢弃 0 0
错误 0 0
未知协议 0 0
```

-n : 显示活动的 TCP 连接，不过，只以数字形式表现地址和端口号，却不尝试确定名称。

C:\Windows\System32\cmd.exe

```
C:\Windows\system32>netstat -n
```

活动连接

协议	本地地址	外部地址	状态
TCP	127.0.0.1:1025	127.0.0.1:1026	ESTABLISHED
TCP	127.0.0.1:1026	127.0.0.1:1025	ESTABLISHED
TCP	172.26.233.171:445	172.26.233.171:14687	ESTABLISHED
TCP	172.26.233.171:2654	40.119.211.203:443	ESTABLISHED
TCP	172.26.233.171:12851	40.119.211.203:443	ESTABLISHED
TCP	172.26.233.171:12909	211.71.149.87:21	ESTABLISHED
TCP	172.26.233.171:14218	121.51.77.101:443	ESTABLISHED
TCP	172.26.233.171:14508	52.139.250.253:443	ESTABLISHED
TCP	172.26.233.171:14687	172.26.233.171:445	ESTABLISHED
TCP	172.26.233.171:14767	47.114.174.193:443	ESTABLISHED
TCP	172.26.233.171:14769	52.114.132.23:443	TIME_WAIT
TCP	172.26.233.171:14772	47.99.211.144:443	CLOSE_WAIT

-o : 显示活动的 TCP 连接并包括每个连接的进程 ID (PID)。可以在 Windows 任务管理器中的“进程”选项卡上找到基于 PID 的应用程序。该参数可以与 -a、-n 和 -p 结合使用。

C:\Windows\System32\cmd.exe

```
C:\Windows\system32>netstat -o
```

活动连接

协议	本地地址	外部地址	状态	PID
TCP	127.0.0.1:1025	DESKTOP-Q6RJGIF:1026	ESTABLISHED	5492
TCP	127.0.0.1:1026	DESKTOP-Q6RJGIF:1025	ESTABLISHED	5492
TCP	172.26.233.171:445	DESKTOP-Q6RJGIF:14687	ESTABLISHED	4

使用时如果不带参数，netstat 显示活动的 TCP 连接。

C:\Windows\System32\cmd.exe

```
C:\Windows\system32>netstat
```

活动连接

协议	本地地址	外部地址	状态
TCP	127.0.0.1:1025	DESKTOP-Q6RJGIF:1026	ESTABLISHED
TCP	127.0.0.1:1026	DESKTOP-Q6RJGIF:1025	ESTABLISHED
TCP	172.26.233.171:445	DESKTOP-Q6RJGIF:14687	ESTABLISHED
TCP	172.26.233.171:2654	40.119.211.203:https	ESTABLISHED

10. 路由跟踪命令

使用该命令可以查看由本机到目标主机所经过哪些路由器。

命令: **tracert** **www.bjfu.edu.cn**

```
C:\Windows\system32\cmd.exe
C:\Windows\system32>tracert www.bjfu.edu.cn

通过最多 30 个跃点跟踪
到 www.bjfu.edu.cn [202.204.112.10] 的路由:

 1      3 ms      1 ms      1 ms  172.26.128.1
 2     19 ms      5 ms      5 ms  10.26.0.1
 3     28 ms     45 ms     29 ms  202.204.127.18
 4      3 ms      3 ms      2 ms  202.204.127.5
 5      *         *         *    请求超时。
 6      3 ms      2 ms      2 ms  202.204.112.10

跟踪完成。
```

完整显示跟踪内容的命令：

命令：`pathping` 对方计算机的 IP 地址或网址

```
C:\Windows\system32\cmd.exe
跟踪完成。
C:\Windows\system32>pathping www.aliceshair.com

通过最多 30 个跃点跟踪
到 www.aliceshair.com [170.106.159.229] 的路由:
 0  DESKTOP-Q6RJGIF [172.26.233.171]
 1  172.26.128.1
 2  10.26.0.1
 3  10.1.1.1
 4  *         *         *
正在计算统计信息，已耗时 75 秒...
指向此处的源      此节点/链接
跃点  RTT      已丢失/已发送 = Pct  已丢失/已发送 = Pct  地址
 0                                DESKTOP-Q6RJGIF [172.26.233.171]
 1   90ms      3/ 100 = 3%      2/ 100 = 2%      172.26.128.1
 2  116ms      2/ 100 = 2%      0/ 100 = 0%      10.26.0.1
 3  102ms      2/ 100 = 2%      0/ 100 = 0%      10.1.1.1

跟踪完成。
```

12. 关于共享安全的几个命令

(1) 查看你机器的共享资源，可使用命令：

命令：`net share`

```
C:\Windows\System32\cmd.exe
跟踪完成。

C:\Windows\system32>net share

共享名      资源      注解
-----
C$          C:\       默认共享
IPC$        C:\       远程 IPC
ADMIN$      C:\Windows 远程管理
shopping    C:\Users\yuehan lian\Desktop\shopping

命令成功完成。
```

(2) 手工删除共享，可使用命令：

```
命令: net share c$ /d
命令: net share d$ /d
命令: net share ipc$ /d
命令: net share admin$ /d
```

```
C:\Windows\System32\cmd.exe
C:\Windows\system32>net share c$ /d
c$ 已经删除。

C:\Windows\system32>net share ipc$ /d
ipc$ 已经删除。

C:\Windows\system32>net share admin$ /d
admin$ 已经删除。
```

(3) 增加一个共享，同时限制链接用户数为 1 人。可使用命令：

```
命令: net share ABCD=e:\ABC /users:1
```

```
C:\Windows\System32\cmd.exe
C:\Windows\system32>Net Share Admin$ /USERS:1
Admin$ 共享成功。

C:\Windows\system32>Net Share IPC$ /USERS:1
IPC$ 共享成功。
```

心得体会：

通过这次实验掌握常用的网络命令，尤其是各命令在不同参数下的形式。

在使用命令的过程中，遇到了失败的情况，经过百度等搜索引擎的搜索查找解决方法，

发现直接 win+r 输入 cmd 回车打开的命令行没有管理员权限，需要以管理员身份来打开 cmd.exe 程序来运行相应的命令，否则命令会被拒绝。

在运行 net share admin\$ /d 之后，记得要把这些添加回去，避免影响日常的使用。