

浙大城市学院实验报告

- 课程名称：计算机网络实验
- 实验项目名称：实验10_网络基本命令
- 学生姓名：徐彬涵
- 专业班级：软件工程2003
- 学号：32001272
- 实验成绩：
- 指导老师：霍梅梅
- 日期：2022/04/28

一. 实验目的和要求

1. 熟悉Windows平台下常用网络命令的使用：
arp, ftp, ipconfig, nbtstat, net, netstat, ping, route, telnet, tracert, pathping
2. 操作环境：硬件：PC机；软件：Windows 2000/XP操作系统

二. 实验内容、原理及实验结果与分析

在系统DOS命令提示符下运行arp命令（**-a**、**-s**、**-d**等参数）

```
18:14:18 871ms
arp --help

显示和修改地址解析协议(ARP)使用的“IP 到物理”地址转换表。

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

-a      通过询问当前协议数据，显示当前 ARP 项。
        如果指定 inet_addr，则只显示指定计算机
        的 IP 地址和物理地址。如果不止一个网络
        接口使用 ARP，则显示每个 ARP 表的项。
-g      与 -a 相同。
-v      在详细模式下显示当前 ARP 项。所有无效项
        和环回接口上的项都将显示。
inet_addr 指定 Internet 地址。
-N if_addr 显示 if_addr 指定的网络接口的 ARP 项。
-d      删除 inet_addr 指定的主机。inet_addr 可
        以是通配符 *，以删除所有主机。
-s      添加主机并且将 Internet 地址 inet_addr
        与物理地址 eth_addr 相关联。物理地址是用
        连字符分隔的 6 个十六进制字节。该项是永久的。
eth_addr 指定物理地址。
if_addr  如果存在，此项指定地址转换表应修改的接口
        的 Internet 地址。如果不存在，则使用第一
        个适用的接口。

示例：
> arp -s 157.55.85.212 00-aa-00-62-c6-09.... 添加静态项。
> arp -a              .... 显示 ARP 表。
```

1. 要求显示当前主机的所有ARP信息

【命令】

```
1 | arp -a
```

【实验结果与分析】

```
18:36:51 80ms
arp -a

接口: 192.168.123.111 --- 0x5
Internet 地址      物理地址      类型
192.168.123.1      f0-b4-29-dc-b2-54 动态
192.168.123.255    ff-ff-ff-ff-ff-ff 静态
224.0.0.2           01-00-5e-00-00-02 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
239.11.20.1         01-00-5e-0b-14-01 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

接口: 192.168.153.1 --- 0x29
Internet 地址      物理地址      类型
192.168.153.254     00-50-56-fd-f0-b7 动态
192.168.153.255     ff-ff-ff-ff-ff-ff 静态
224.0.0.2           01-00-5e-00-00-02 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
239.11.20.1         01-00-5e-0b-14-01 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

接口: 192.168.64.1 --- 0x2a
Internet 地址      物理地址      类型
192.168.64.128      00-0c-29-84-21-46 动态
192.168.64.254      00-50-56-fc-aa-55 动态
192.168.64.255      ff-ff-ff-ff-ff-ff 静态
224.0.0.2           01-00-5e-00-00-02 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
239.11.20.1         01-00-5e-0b-14-01 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

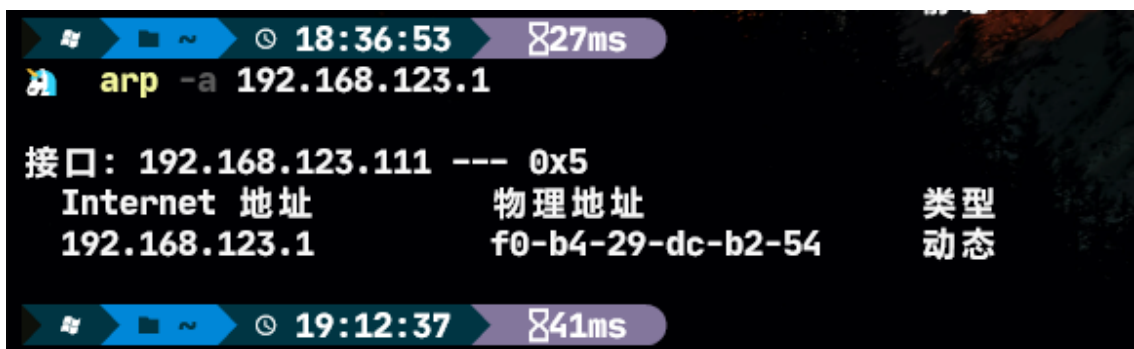
18:36:53 827ms
```

2. 要求显示某指定主机IP的ARP信息

【命令】

```
1 | arp -a 192.168.123.1
```

【实验结果与分析】

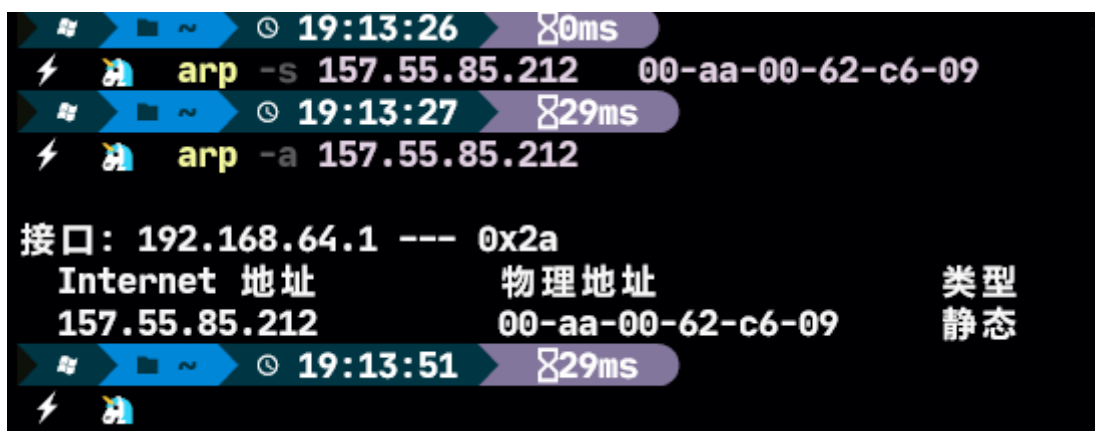


3. 静态添加某指定主机IP对应的物理地址

【命令】

```
1 | arp -s 157.55.85.212 00-aa-00-62-c6-09
```

【实验结果与分析】



4. 删除刚添加的指定主机的ARP信息

【命令】

```
1 | arp -d 157.55.85.212
```

【实验结果与分析】



在系统DOS命令提示符下运行ftp命令（cd dir get等命令）

```
© 19:14:39 822ms
ftp --help

将文件传送到运行 FTP 服务器服务(经常称为后台程序)的计算机以及将文件从该计算机
传出。可以交互使用 Ftp。

FTP [-v] [-d] [-i] [-n] [-g] [-s:filename] [-a] [-A] [-x:sendbuffer] [-r:recvbuffer] [-b:asyncbuffers] [-w:windows
ize] [host]

-v          禁止显示远程服务器响应。
-n          禁止在初始连接时自动登录。
-i          关闭多文件传输过程中的
            交互式提示。
-d          启用调试。
-g          禁用文件名通配(请参阅 GLOB 命令)。
-s:filename 指定包含 FTP 命令的文本文件; 命令
            在 FTP 启动后自动运行。
-a          在绑定数据连接时使用所有本地接口。
-A          匿名登录。
-x:send sockbuf 覆盖默认的 SO_SNDBUF 大小 8192。
-r:recv sockbuf 覆盖默认的 SO_RCVBUF 大小 8192。
-b:async count 覆盖默认的异步计数 3
-w:window size 覆盖默认的传输缓冲区大小 65535。
host        指定主机名称或要连接到的远程主机
            的 IP 地址。

注意:
- mget 和 mput 命令将 y/n/q 视为 yes/no/quit。
- 使用 Ctrl-C 中止命令。

© 19:15:29 871ms
```

1. 连接到某FTP站点（如10.66.28.222）

【命令】

```
1 | ftp
2 | open 10.66.28.222 2007
```

【实验结果与分析】

```
© 19:28:26 80ms
ftp
ftp> open 10.66.28.222 2007
连接到 10.66.28.222。
220 Serv-U FTP Server v6.3 for WinSock ready...
501 Invalid option.
用户(10.66.28.222:(none)): huommdownload
331 User name okay, need password.
密码:
230 User logged in, proceed.
ftp>
```

2. 登录某FTP站点，下载某一文件

【命令】

```
1 | get downloadtest.txt
```

【实验结果与分析】


```
C:/Life/Desktop 20:37:59 82m 42.995s
ftp
ftp> open 10.66.28.222 2007
连接到 10.66.28.222。
220 Serv-U FTP Server v6.3 for WinSock ready...
501 Invalid option.
用户(10.66.28.222:(none)): huommdownload
331 User name okay, need password.
密码:
230 User logged in, proceed.
ftp> get downloadtest.txt
200 PORT Command successful.
150 Opening ASCII mode data connection for downloadtest.txt (13 Bytes).
```

3. 尝试其他相关FTP命令

【命令】

```
1 | pwd
2 | bye
3 | put C:\Life\Desktop\downloadtest.txt
```

【实验结果与分析】

```
19:40:02 813.247s
ftp
ftp> open 10.66.28.222 2007
连接到 10.66.28.222。
220 Serv-U FTP Server v6.3 for WinSock ready...
501 Invalid option.
用户(10.66.28.222:(none)): huommdownload
331 User name okay, need password.
密码:
230 User logged in, proceed.
ftp> pwd
257 "/" is current directory.
ftp> bye
221 Goodbye!
```

```
19:42:09 81m 1.822s
ftp
ftp> open 10.66.28.222 2007
连接到 10.66.28.222。
220 Serv-U FTP Server v6.3 for WinSock ready...
501 Invalid option.
用户(10.66.28.222:(none)): huomupload
331 User name okay, need password.
密码:
230 User logged in, proceed.
ftp> put C:\Life\Desktop\downloadtest.txt
200 PORT Command successful.
150 Opening ASCII mode data connection for downloadtest.txt.
```

在系统DOS命令提示符下运行ipconfig命令（/all, /displaydns等参数）

用法:

```
ipconfig [/allcompartments] [/? | /all |  
/renew [adapter] | /release [adapter] |  
/renew6 [adapter] | /release6 [adapter] |  
/flushdns | /displaydns | /registerdns |  
/showclassid adapter |  
/setclassid adapter [classid] |  
/showclassid6 adapter |  
/setclassid6 adapter [classid] ]
```

其中

adapter 连接名称
(允许使用通配符 * 和 ?, 参见示例)

选项:

/?	显示此帮助消息
/all	显示完整配置信息。
/release	释放指定适配器的 IPv4 地址。
/release6	释放指定适配器的 IPv6 地址。
/renew	更新指定适配器的 IPv4 地址。
/renew6	更新指定适配器的 IPv6 地址。
/flushdns	清除 DNS 解析程序缓存。
/registerdns	刷新所有 DHCP 租用并重新注册 DNS 名称
/displaydns	显示 DNS 解析程序缓存的内容。
/showclassid	显示适配器允许的所有 DHCP 类 ID。
/setclassid	修改 DHCP 类 ID。
/showclassid6	显示适配器允许的所有 IPv6 DHCP 类 ID。
/setclassid6	修改 IPv6 DHCP 类 ID。

默认情况下, 仅显示绑定到 TCP/IP 的每个适配器的 IP 地址、子网掩码和默认网关。

对于 Release 和 Renew, 如果未指定适配器名称, 则会释放或更新所有绑定到 TCP/IP 的适配器的 IP 地址租用。

对于 Setclassid 和 Setclassid6, 如果未指定 ClassId, 则会删除 ClassId。

示例:

> ipconfig	... 显示信息
> ipconfig /all	... 显示详细信息
> ipconfig /renew	... 更新所有适配器
> ipconfig /renew EL*	... 更新所有名称以 EL 开头的连接
> ipconfig /release *Con*	... 释放所有匹配的连接, 例如“有线以太网连接 1”或“有线以太网连接 2”
> ipconfig /allcompartments	... 显示有关所有隔离舱的信息
> ipconfig /allcompartments /all	... 显示有关所有隔离舱的详细信息

1. 获取本地基本TCP/IP配置值

【命令】

```
1 | ipconfig
```

【实验结果与分析】

```
C:/Life/Desktop 19:45:38 80ms
ipconfig

Windows IP 配置

以太网适配器 以太网 2:

    连接特定的 DNS 后缀 . . . . . :
    本地链接 IPv6 地址 . . . . . : fe80::38ba:db69:dce6:34a7%44
    IPv4 地址 . . . . . : 10.69.240.134
    子网掩码 . . . . . : 255.255.255.0
    默认网关 . . . . . :

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 . . . . . :

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 . . . . . :

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 . . . . . :

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::30cb:bf8:cbd6:8b97%41
    IPv4 地址 . . . . . : 192.168.153.1
    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::f119:c8d4:485:a85b%42
    IPv4 地址 . . . . . : 192.168.64.1
    子网掩码 . . . . . : 255.255.255.0
    默认网关 . . . . . :

无线局域网适配器 WLAN:

    连接特定的 DNS 后缀 . . . . . : lan
    本地链接 IPv6 地址 . . . . . : fe80::d0b6:9da5:c7e9:a445%5
    IPv4 地址 . . . . . : 192.168.123.111
    子网掩码 . . . . . : 255.255.255.0
    默认网关 . . . . . : 192.168.123.1
```

2. 获取本地详细TCP/IP配置值（包括物理地址等信息）

【命令】

```
1 | ipconfig /all
```

【实验结果与分析】


```
C:/Life/Desktop 19:46:07 838ms
ipconfig /all

Windows IP 配置

主机名 . . . . . : DESKTOP-04JCLRP
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 . . . . . : lan

以太网适配器 以太网 2:

连接特定的 DNS 后缀 . . . . . :
描述. . . . . : Sangfor SSL VPN CS Support System VNIC
物理地址. . . . . : 00-FF-FE-41-AA-2B
DHCP 已启用 . . . . . : 是
自动配置已启用. . . . . : 是
本地链接 IPv6 地址. . . . . : fe80::38ba:db69:dce6:34a7%44(首选)
IPv4 地址 . . . . . : 10.69.240.134(首选)
子网掩码 . . . . . : 255.255.255.0
默认网关. . . . . :
DHCPv6 IAID . . . . . : 738263038
DHCPv6 客户端 DUID . . . . . : 00-01-00-01-29-FB-13-7A-54-05-DB-03-3A-FA
DNS 服务器 . . . . . : 127.0.0.1
TCP/IP 上的 NetBIOS . . . . . : 已启用

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 . . . . . :
描述. . . . . : Realtek PCIe GbE Family Controller
物理地址. . . . . : 54-05-DB-03-3A-FA
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* 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. . . . . : 38-68-93-7E-28-91
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-68-93-7E-28-90
```

在系统DOS命令提示符下运行nbtstat命令（-a -n等参数）

```
C:/Life/Desktop 19:48:59 103ms
nbtstat

显示协议统计和当前使用 NBI 的 TCP/IP 连接
(在 TCP/IP 上的 NetBIOS)。

NBTSTAT [ [-a RemoteName] [-A IP address] [-c] [-n]
          [-r] [-R] [-RR] [-s] [-S] [interval] ]

-a (适配器状态) 列出指定名称的远程机器的名称表
-A (适配器状态) 列出指定 IP 地址的远程机器的名称表。
-c (缓存)       列出远程[计算机]名称及其 IP 地址的 NBT 缓存
-n (名称)       列出本地 NetBIOS 名称。
-r (已解析)     列出通过广播和经由 WINS 解析的名称
-R (重新加载)   清除和重新加载远程缓存名称表
-S (会话)       列出具有目标 IP 地址的会话表
-s (会话)       列出将目标 IP 地址转换成计算机 NETBIOS 名称的会话表。
-RR (释放刷新) 将名称释放包发送到 WINS，然后启动刷新

RemoteName  远程主机计算机名。
IP address  用点分隔的十进制表示的 IP 地址。
interval    重新显示选定的统计、每次显示之间暂停的间隔秒数。
             按 Ctrl+C 停止重新显示统计。
```

1. 列出某一特定主机的NETBIOS信息（指出物理地址）

【命令】

```
1 | nbtstat -a f0-b4-29-dc-b2-54
```

【实验结果与分析】

```
C:/Life/Desktop 20:06:36 20ms
nbtstat -a f0-b4-29-dc-b2-54

以太网:
节点 IP 地址: [0.0.0.0] 范围 ID: []

找不到主机。

蓝牙网络连接:
节点 IP 地址: [0.0.0.0] 范围 ID: []

找不到主机。

WLAN:
节点 IP 地址: [192.168.123.111] 范围 ID: []

找不到主机。

本地连接* 1:
节点 IP 地址: [0.0.0.0] 范围 ID: []

找不到主机。

本地连接* 10:
节点 IP 地址: [0.0.0.0] 范围 ID: []

找不到主机。

VMware Network Adapter VMnet1:
节点 IP 地址: [192.168.153.1] 范围 ID: []

找不到主机。

VMware Network Adapter VMnet8:
节点 IP 地址: [192.168.64.1] 范围 ID: []

找不到主机。

以太网 2:
节点 IP 地址: [0.0.0.0] 范围 ID: []

找不到主机。
C:/Life/Desktop 20:07:15 18.213s
```

2. 列出本地主机的NETBIOS信息

【命令】

```
1 | nbtstat -n
```

【实验结果与分析】

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: [192.168.123.111] 范围 ID: []

NetBIOS 本地名称表

名称	类型	状态

DESKTOP-04JCLRP<20>	唯一	已注册
DESKTOP-04JCLRP<00>	唯一	已注册
WORKGROUP <00>	组	已注册

本地连接* 1:

节点 IP 地址: [0.0.0.0] 范围 ID: []

缓存中没有名称

本地连接* 10:

节点 IP 地址: [0.0.0.0] 范围 ID: []

缓存中没有名称

VMware Network Adapter VMnet1:

节点 IP 地址: [192.168.153.1] 范围 ID: []

NetBIOS 本地名称表

名称	类型	状态

DESKTOP-04JCLRP<20>	唯一	已注册
DESKTOP-04JCLRP<00>	唯一	已注册
WORKGROUP <00>	组	已注册

VMware Network Adapter VMnet8:

节点 IP 地址: [192.168.64.1] 范围 ID: []

NetBIOS 本地名称表

名称	类型	状态

在系统DOS命令提示符下运行net命令（share start use等命令）

```
C:/Life/Desktop 20:07:35 81ms
net
此命令的语法是:

NET
[ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
  HELPMMSG | LOCALGROUP | PAUSE | SESSION | SHARE | START |
  STATISTICS | STOP | TIME | USE | USER | VIEW ]
```

1. 使用net share命令查看网络共享信息

【命令】

```
1 | net share
```

【实验结果与分析】

```
C:/Life/Desktop 20:07:36 847ms
net share

共享名      资源              注解
-----
C$          C:\               默认共享
D$          D:\               默认共享
IPC$        C:\Windows        远程 IPC
ADMIN$      C:\Windows        远程管理
命令成功完成。
```

2. 使用net start/stop启动/停止某一服务

【命令】

```
1 | net start 数据使用量
```

```
1 | net stop 数据使用量
```

【实验结果与分析】

设备管理注册服务	为设...	手动	本地系统
手机网络时间	此服...	手动(触发...	本地服务
数据使用量	网络...	自动	本地服务
同步主机_6f28c	此服...	正在运行	自动(延迟...
无线电管理服务	无线...	正在运行	手动
显示策略服务	管理...	正在运行	自动(延迟...



在系统DOS命令提示符下运行netstat命令（-a -s -e等参数）



1. 显示所有本地连接和侦听的端口

【命令】

```
1 | netstat -a
```

【实验结果与分析】

协议	本地地址	外部地址	状态
TCP	0.0.0.0:135	DESKTOP-04JCLRP:0	LISTENING
TCP	0.0.0.0:445	DESKTOP-04JCLRP:0	LISTENING
TCP	0.0.0.0:902	DESKTOP-04JCLRP:0	LISTENING
TCP	0.0.0.0:912	DESKTOP-04JCLRP:0	LISTENING
TCP	0.0.0.0:2869	DESKTOP-04JCLRP:0	LISTENING
TCP	0.0.0.0:5021	DESKTOP-04JCLRP:0	LISTENING
TCP	0.0.0.0:5040	DESKTOP-04JCLRP:0	LISTENING
TCP	0.0.0.0:5357	DESKTOP-04JCLRP:0	LISTENING
TCP	0.0.0.0:7680	DESKTOP-04JCLRP:0	LISTENING
TCP	0.0.0.0:7890	DESKTOP-04JCLRP:0	LISTENING
TCP	0.0.0.0:15000	DESKTOP-04JCLRP:0	LISTENING
TCP	0.0.0.0:49392	DESKTOP-04JCLRP:0	LISTENING
TCP	0.0.0.0:49664	DESKTOP-04JCLRP:0	LISTENING
TCP	0.0.0.0:49665	DESKTOP-04JCLRP:0	LISTENING
TCP	0.0.0.0:49666	DESKTOP-04JCLRP:0	LISTENING
TCP	0.0.0.0:49667	DESKTOP-04JCLRP:0	LISTENING
TCP	0.0.0.0:49668	DESKTOP-04JCLRP:0	LISTENING
TCP	0.0.0.0:49670	DESKTOP-04JCLRP:0	LISTENING
TCP	0.0.0.0:54321	DESKTOP-04JCLRP:0	LISTENING
TCP	127.0.0.1:4096	DESKTOP-04JCLRP:0	LISTENING
TCP	127.0.0.1:4301	DESKTOP-04JCLRP:0	LISTENING
TCP	127.0.0.1:4709	DESKTOP-04JCLRP:0	LISTENING
TCP	127.0.0.1:7890	DESKTOP-04JCLRP:52696	ESTABLISHED
TCP	127.0.0.1:7890	DESKTOP-04JCLRP:52698	ESTABLISHED
TCP	127.0.0.1:7890	DESKTOP-04JCLRP:55907	ESTABLISHED
TCP	127.0.0.1:7890	DESKTOP-04JCLRP:55946	ESTABLISHED
TCP	127.0.0.1:7890	DESKTOP-04JCLRP:55962	ESTABLISHED
TCP	127.0.0.1:7890	DESKTOP-04JCLRP:55980	ESTABLISHED
TCP	127.0.0.1:7890	DESKTOP-04JCLRP:55991	ESTABLISHED
TCP	127.0.0.1:7890	DESKTOP-04JCLRP:56048	ESTABLISHED
TCP	127.0.0.1:7890	DESKTOP-04JCLRP:56068	ESTABLISHED
TCP	127.0.0.1:7890	DESKTOP-04JCLRP:56117	ESTABLISHED
TCP	127.0.0.1:7890	DESKTOP-04JCLRP:56127	ESTABLISHED
TCP	127.0.0.1:7890	DESKTOP-04JCLRP:56156	ESTABLISHED
TCP	127.0.0.1:7890	DESKTOP-04JCLRP:56192	ESTABLISHED
TCP	127.0.0.1:7890	DESKTOP-04JCLRP:56194	ESTABLISHED
TCP	127.0.0.1:7890	DESKTOP-04JCLRP:56195	ESTABLISHED
TCP	127.0.0.1:7890	DESKTOP-04JCLRP:56197	ESTABLISHED
TCP	127.0.0.1:7890	DESKTOP-04JCLRP:56200	ESTABLISHED
TCP	127.0.0.1:7890	DESKTOP-04JCLRP:56226	TIME_WAIT
TCP	127.0.0.1:7890	DESKTOP-04JCLRP:56245	TIME_WAIT
TCP	127.0.0.1:7890	DESKTOP-04JCLRP:56249	TIME_WAIT
TCP	127.0.0.1:7890	DESKTOP-04JCLRP:56257	ESTABLISHED
TCP	127.0.0.1:7890	DESKTOP-04JCLRP:56263	ESTABLISHED
TCP	127.0.0.1:7890	DESKTOP-04JCLRP:56297	ESTABLISHED

2. 显示本地连接常见协议的统计信息

【命令】

```
1 | netstat -s
```

【实验结果与分析】

3. 显示本地以太网统计信息

【命令】

```
1 | net share
```

【实验结果与分析】

```
C:/Life/Desktop 20:18:05 10.53s
netstat -s

IPv4 统计信息

接收的数据包                = 20175596
接收的标头错误                = 0
接收的地址错误                = 676
转发的数据报                = 0
接收的未知协议                = 0
丢弃的接收数据包            = 19939
传送的接收数据包            = 20184137
输出请求                    = 16261503
路由丢弃                    = 0
丢弃的输出数据包            = 6531
输出数据包无路由            = 6
需要重新组合                = 0
重新组合成功                = 0
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                = 3786
接收的标头错误                = 0
接收的地址错误                = 801
转发的数据报                = 0
接收的未知协议                = 0
丢弃的接收数据包            = 4
传送的接收数据包            = 8341
输出请求                    = 7103
路由丢弃                    = 0
丢弃的输出数据包            = 0
输出数据包无路由            = 0
需要重新组合                = 0
重新组合成功                = 0
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

ICMPv4 统计信息

                已接收    已发送
消息            12945      7829
错误              0          0
```

在系统DOS命令提示符下运行ping命令（-a -n -t等参数）

```
C:/Life/Desktop 20:19:12 81ms
ping

用法: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
          [-r count] [-s count] [[-j host-list] | [-k host-list]]
          [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
          [-4] [-6] target_name

选项:
    -t          Ping 指定的主机, 直到停止。
                若要查看统计信息并继续操作, 请键入 Ctrl+Break;
                若要停止, 请键入 Ctrl+C。
    -a          将地址解析为主机名。
    -n count    要发送的回显请求数。
    -l size     发送缓冲区大小。
    -f          在数据包中设置“不分段”标记(仅适用于 IPv4)。
    -i TTL      生存时间。
    -v TOS      服务类型(仅适用于 IPv4。该设置已被弃用,
                对 IP 标头中的服务类型字段没有任何影响)。
    -r count    记录计数跃点的路由(仅适用于 IPv4)。
    -s count    计数跃点的时间戳(仅适用于 IPv4)。
    -j host-list 与主机列表一起使用的松散源路由(仅适用于 IPv4)。
    -k host-list 与主机列表一起使用的严格源路由(仅适用于 IPv4)。
    -w timeout  等待每次回复的超时时间(毫秒)。
    -R          同样使用路由标头测试反向路由(仅适用于 IPv6)。
                根据 RFC 5095, 已弃用此路由标头。
                如果使用此标头, 某些系统可能丢弃回显请求。
    -S srcaddr  要使用的源地址。
    -c compartment 路由隔离舱标识符。
    -p          Ping Hyper-V 网络虚拟化提供程序地址。
    -4          强制使用 IPv4。
    -6          强制使用 IPv6。
```

1. 使用ping命令的常见参数显示返回信息

【命令】

```
1 ping 192.168.123.1
2 ping -a 192.168.123.1
3 ping -n 8 192.168.123.1
4 ping -r 5 192.168.123.1
5 ping -t www.baidu.com
```

【实验结果与分析】


```
C:/Life/Desktop 20:19:13 846ms
ping 192.168.123.1

正在 Ping 192.168.123.1 具有 32 字节的数据:
来自 192.168.123.1 的回复: 字节=32 时间=1ms TTL=64
来自 192.168.123.1 的回复: 字节=32 时间=1ms TTL=64
来自 192.168.123.1 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.123.1 的回复: 字节=32 时间=1ms TTL=64

192.168.123.1 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 = 1ms, 平均 = 0ms

C:/Life/Desktop 20:19:56 3.049s
```

```
C:/Life/Desktop 20:42:29 10.739s
ping -a 192.168.123.1

正在 Ping MI-NANO.lan [192.168.123.1] 具有 32 字节的数据:
来自 192.168.123.1 的回复: 字节=32 时间=2ms TTL=64
来自 192.168.123.1 的回复: 字节=32 时间=9ms TTL=64
来自 192.168.123.1 的回复: 字节=32 时间=5ms TTL=64
来自 192.168.123.1 的回复: 字节=32 时间=8ms TTL=64

192.168.123.1 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 = 2ms, 最长 = 9ms, 平均 = 6ms
```

```
C:/Life/Desktop 20:42:37 3.087s
ping -n 8 192.168.123.1

正在 Ping 192.168.123.1 具有 32 字节的数据:
来自 192.168.123.1 的回复: 字节=32 时间=4ms TTL=64
来自 192.168.123.1 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.123.1 的回复: 字节=32 时间=1ms TTL=64
来自 192.168.123.1 的回复: 字节=32 时间=3ms TTL=64
来自 192.168.123.1 的回复: 字节=32 时间=1ms TTL=64
来自 192.168.123.1 的回复: 字节=32 时间=2ms TTL=64
来自 192.168.123.1 的回复: 字节=32 时间=4ms TTL=64
来自 192.168.123.1 的回复: 字节=32 时间<1ms TTL=64

192.168.123.1 的 Ping 统计信息:
    数据包: 已发送 = 8, 已接收 = 8, 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 = 4ms, 平均 = 1ms

C:/Life/Desktop 20:43:01 7.053s
```

```
C:/Life/Desktop 20:43:01 87.053s
ping -n 5 192.168.123.1

正在 Ping 192.168.123.1 具有 32 字节的数据:
来自 192.168.123.1 的回复: 字节=32 时间=4ms TTL=64
    路由: 192.168.123.1 →
            192.168.123.1
来自 192.168.123.1 的回复: 字节=32 时间=1ms TTL=64
    路由: 192.168.123.1 →
            192.168.123.1
来自 192.168.123.1 的回复: 字节=32 时间=2ms TTL=64
    路由: 192.168.123.1 →
            192.168.123.1
来自 192.168.123.1 的回复: 字节=32 时间=258ms TTL=64
    路由: 192.168.123.1 →
            192.168.123.1

192.168.123.1 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 = 1ms, 最长 = 258ms, 平均 = 66ms

C:/Life/Desktop 20:43:33 83.301s
ping -t www.baidu.com

正在 Ping www.a.shifen.com [180.101.49.12] 具有 32 字节的数据:
来自 180.101.49.12 的回复: 字节=32 时间=12ms TTL=53
来自 180.101.49.12 的回复: 字节=32 时间=12ms TTL=53
来自 180.101.49.12 的回复: 字节=32 时间=11ms TTL=53
来自 180.101.49.12 的回复: 字节=32 时间=11ms TTL=53
来自 180.101.49.12 的回复: 字节=32 时间=10ms TTL=53
来自 180.101.49.12 的回复: 字节=32 时间=11ms TTL=53
来自 180.101.49.12 的回复: 字节=32 时间=10ms TTL=53
来自 180.101.49.12 的回复: 字节=32 时间=10ms TTL=53
来自 180.101.49.12 的回复: 字节=32 时间=10ms TTL=53
来自 180.101.49.12 的回复: 字节=32 时间=16ms TTL=53
来自 180.101.49.12 的回复: 字节=32 时间=18ms TTL=53
来自 180.101.49.12 的回复: 字节=32 时间=11ms TTL=53
来自 180.101.49.12 的回复: 字节=32 时间=11ms TTL=53
来自 180.101.49.12 的回复: 字节=32 时间=11ms TTL=53

180.101.49.12 的 Ping 统计信息:
    数据包: 已发送 = 14, 已接收 = 14, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 10ms, 最长 = 18ms, 平均 = 11ms
Control-C

C:/Life/Desktop 20:44:27 813.643s
```

2. 结合ping命令和arp命令获取子网中某一主机的物理地址

【命令】

```
1 ping 192.168.123.1
2 arp -a 192.168.123.1
```

【实验结果与分析】

```
C:/Life/Desktop 20:46:30 842.153s
ping 192.168.123.1

正在 Ping 192.168.123.1 具有 32 字节的数据:
来自 192.168.123.1 的回复: 字节=32 时间=2ms TTL=64
来自 192.168.123.1 的回复: 字节=32 时间=13ms TTL=64
来自 192.168.123.1 的回复: 字节=32 时间=1ms TTL=64
来自 192.168.123.1 的回复: 字节=32 时间=1ms TTL=64

192.168.123.1 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 = 1ms, 最长 = 13ms, 平均 = 4ms

C:/Life/Desktop 20:46:49 83.048s
arp -a 192.168.123.1

接口: 192.168.123.111 --- 0x5
Internet 地址          物理地址          类型
192.168.123.1          f0-b4-29-dc-b2-54 动态

C:/Life/Desktop 20:46:59 830ms
```

在系统DOS命令提示符下运行route命令（print, add, delete等命令）

C:/Life/Desktop

20:47:25

81ms

route

操作网络路由表。

ROUTE [-f] [-p] [-4|-6] command [destination]
[MASK netmask] [gateway] [METRIC metric] [IF interface]

-f	清除所有网关项的路由表。如果与某个命令结合使用，在运行该命令前，应清除路由表。
-p	与 ADD 命令结合使用时，将路由设置为在系统引导期间保持不变。默认情况下，重新启动系统时，不保存路由。忽略所有其他命令，这始终会影响相应的永久路由。
-4	强制使用 IPv4。
-6	强制使用 IPv6。
command	其中之一： PRINT 打印路由 ADD 添加路由 DELETE 删除路由 CHANGE 修改现有路由
destination	指定主机。
MASK	指定下一个参数为“netmask”值。
netmask	指定此路由项的子网掩码值。 如果未指定，其默认设置为 255.255.255.255。
gateway	指定网关。
interface	指定路由的接口号码。
METRIC	指定跃点数，例如目标的成本。

用于目标的所有符号名都可以在网络数据库文件 NETWORKS 中进行查找。用于网关的符号名称都可以在主机名称数据库文件 HOSTS 中进行查找。

如果命令为 PRINT 或 DELETE。目标或网关可以为通配符，(通配符指定为星号“*”)，否则可能会忽略网关参数。

如果 Dest 包含一个 * 或 ?，则会将其视为 Shell 模式，并且只打印匹配目标路由。“*”匹配任意字符串，而“?”匹配任意一个字符。示例：157.*.1、157.*、127.*、*224*。

只有在 PRINT 命令中才允许模式匹配。

诊断信息注释：
无效的 MASK 产生错误，即当 (DEST & MASK) ≠ DEST 时。
示例：> route ADD 157.0.0.0 MASK 155.0.0.0 157.55.80.1 IF 1
路由添加失败：指定的掩码参数无效。
(Destination & Mask) ≠ Destination。

1. 列出本地已存在的路由信息

【命令】

```
1 | route print
```

【实验结果与分析】


```
C:/Life/Desktop 20:47:31 838ms
route print
=====
接口列表
21...00 ff fe 41 aa 2b .....Sangfor SSL VPN CS Support System VNIC
17...54 05 db 03 3a fa .....Realtek PCIe GbE Family Controller
20...38 68 93 7e 28 91 .....Microsoft Wi-Fi Direct Virtual Adapter
18...3a 68 93 7e 28 90 .....Microsoft Wi-Fi Direct Virtual Adapter #2
9...00 50 56 c0 00 01 .....VMware Virtual Ethernet Adapter for VMnet1
13...00 50 56 c0 00 08 .....VMware Virtual Ethernet Adapter for VMnet8
5...38 68 93 7e 28 90 .....Intel(R) Wi-Fi 6 AX201 160MHz
7...38 68 93 7e 28 94 .....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      192.168.123.1 192.168.123.111 40
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
192.168.64.0      255.255.255.0 在链路上      192.168.64.1 291
192.168.64.1      255.255.255.255 在链路上      192.168.64.1 291
192.168.64.255 255.255.255.255 在链路上      192.168.64.1 291
192.168.123.0      255.255.255.0 在链路上      192.168.123.111 296
192.168.123.111 255.255.255.255 在链路上      192.168.123.111 296
192.168.123.255 255.255.255.255 在链路上      192.168.123.111 296
192.168.153.0      255.255.255.0 在链路上      192.168.153.1 291
192.168.153.1      255.255.255.255 在链路上      192.168.153.1 291
192.168.153.255 255.255.255.255 在链路上      192.168.153.1 291
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      192.168.153.1 291
224.0.0.0      240.0.0.0      在链路上      192.168.64.1 291
224.0.0.0      240.0.0.0      在链路上      192.168.123.111 296
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      192.168.153.1 291
255.255.255.255 255.255.255.255 在链路上      192.168.64.1 291
255.255.255.255 255.255.255.255 在链路上      192.168.123.111 296
=====
永久路由:
无

IPv6 路由表
=====
活动路由:
接口跃点数网络目标      网关
1      331 ::1/128      在链路上
9      291 fe80::/64      在链路上
13     291 fe80::/64      在链路上
5      296 fe80::/64      在链路上
```

2. 添加到达某一网络或主机的路由

【命令】

```
1 | route add 10.64.1.0 mask 255.255.255.0 10.64.1.1 metric 3
```

【实验结果与分析】


```
C:/Life/Desktop 20:48:39 873ms
route add 10.64.1.0 mask 255.255.255.0 10.64.1.1 metric 3
操作完成!
C:/Life/Desktop 20:49:59 812ms
route print

=====
接口列表
21...00 ff fe 41 aa 2b .....Sangfor SSL VPN CS Support System VNIC
17...54 05 db 03 3a fa .....Realtek PCIe GbE Family Controller
20...38 68 93 7e 28 91 .....Microsoft Wi-Fi Direct Virtual Adapter
18...3a 68 93 7e 28 90 .....Microsoft Wi-Fi Direct Virtual Adapter #2
9...00 50 56 c0 00 01 .....VMware Virtual Ethernet Adapter for VMnet1
13...00 50 56 c0 00 08 .....VMware Virtual Ethernet Adapter for VMnet8
5...38 68 93 7e 28 90 .....Intel(R) Wi-Fi 6 AX201 160MHz
7...38 68 93 7e 28 94 .....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      192.168.123.1  192.168.123.111  40
10.64.1.0    255.255.255.0  10.64.1.1    192.168.123.111  43
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
192.168.64.0    255.255.255.0  在链路上      192.168.64.1  291
192.168.64.1    255.255.255.255  在链路上      192.168.64.1  291
192.168.64.255  255.255.255.255  在链路上      192.168.64.1  291
192.168.123.0    255.255.255.0  在链路上      192.168.123.111  296
192.168.123.111  255.255.255.255  在链路上      192.168.123.111  296
192.168.123.255  255.255.255.255  在链路上      192.168.123.111  296
192.168.153.0    255.255.255.0  在链路上      192.168.153.1  291
192.168.153.1    255.255.255.255  在链路上      192.168.153.1  291
192.168.153.255  255.255.255.255  在链路上      192.168.153.1  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      192.168.153.1  291
224.0.0.0      240.0.0.0      在链路上      192.168.64.1  291
224.0.0.0      240.0.0.0      在链路上      192.168.123.111  296
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      192.168.153.1  291
255.255.255.255  255.255.255.255  在链路上      192.168.64.1  291
255.255.255.255  255.255.255.255  在链路上      192.168.123.111  296
=====
永久路由:
无

IPv6 路由表
=====
活动路由:
接口跃点数 网络目标      网关
```

3. 删除刚添加的路由选项，并显示删除后的路由信息

【命令】

```
1 | route delete 10.64.1.0
```

【实验结果与分析】

```
C:\Life\Desktop 20:51:10 812ms
route delete 10.64.1.0
操作完成!
C:\Life\Desktop 20:51:17 812ms
route print
=====
接口列表
21...00 ff fe 41 aa 2b .....Sangfor SSL VPN CS Support System VNIC
17...54 05 db 03 3a fa .....Realtek PCIe GbE Family Controller
20...38 68 93 7e 28 91 .....Microsoft Wi-Fi Direct Virtual Adapter
18...3a 68 93 7e 28 90 .....Microsoft Wi-Fi Direct Virtual Adapter #2
9...00 50 56 c0 00 01 .....VMware Virtual Ethernet Adapter for VMnet1
13...00 50 56 c0 00 08 .....VMware Virtual Ethernet Adapter for VMnet8
5...38 68 93 7e 28 90 .....Intel(R) Wi-Fi 6 AX201 160MHz
7...38 68 93 7e 28 94 .....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      192.168.123.1 192.168.123.111 45
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
192.168.64.0      255.255.255.0 在链路上      192.168.64.1 291
192.168.64.1      255.255.255.255 在链路上      192.168.64.1 291
192.168.64.255 255.255.255.255 在链路上      192.168.64.1 291
192.168.123.0      255.255.255.0 在链路上      192.168.123.111 301
192.168.123.111 255.255.255.255 在链路上      192.168.123.111 301
192.168.123.255 255.255.255.255 在链路上      192.168.123.111 301
192.168.153.0      255.255.255.0 在链路上      192.168.153.1 291
192.168.153.1      255.255.255.255 在链路上      192.168.153.1 291
192.168.153.255 255.255.255.255 在链路上      192.168.153.1 291
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      192.168.153.1 291
224.0.0.0      240.0.0.0      在链路上      192.168.64.1 291
224.0.0.0      240.0.0.0      在链路上      192.168.123.111 301
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      192.168.153.1 291
255.255.255.255 255.255.255.255 在链路上      192.168.64.1 291
255.255.255.255 255.255.255.255 在链路上      192.168.123.111 301
=====
永久路由:
无
```

在系统DOS命令提示符下运行telnet命令

```
C:\Life\Desktop 20:54:41 818.108s
telnet /?

telnet [-a][-e escape char][-f log file][-l user][-t term][host [port]]
-a      企图自动登录。除了用当前已登陆的用户名以外, 与 -l 选项相同。
-e      跳过字符来进入 telnet 客户端提示。
-f      客户端登录的文件名
-l      指定远程系统上登录用的用户名。
-t      要求远程系统支持 TELNET ENVIRON 选项。
-t      指定终端类型。
        支持的终端类型仅是: vt100, vt52, ansi 和 vtnt。
host    指定要连接的远程计算机的主机名或 IP 地址。
port    指定端口号或服务名。
C:\Life\Desktop 20:54:50 812ms
```

```
欢迎使用 Microsoft Telnet Client

Escape 字符为 'CTRL+]'

Microsoft Telnet> ?

命令可能是缩写。支持的命令为:

c      - close           关闭当前连接
d      - display         显示操作参数
o      - open hostname [port] 连接到主机(默认端口 23)。
q      - quit            退出 telnet
set    - set             设置选项(键入 'set ?' 获得列表)
sen    - send            将字符串发送到服务器
st     - status          打印状态信息
u      - unset           解除设置选项(键入 'set ?' 获得列表)
?/h   - help            打印帮助信息

Microsoft Telnet> |
```

1. 使用telnet命令连接BBS站点：10.13.21.88

【命令】

```
1 telnet
2 open 10.13.21.88
3 open bbs.zju.edu.cn
```

【实验结果与分析】

```
Microsoft Telnet> open 10.13.21.88
正在连接10.13.21.88...无法打开到主机的连接。 在端口 23: 连接失败
Microsoft Telnet>
```

```
Microsoft Telnet> open bbs.zju.edu.cn
正在连接bbs.zju.edu.cn...

遗失对主机的连接。
```

2. 使用telnet命令检测特定主机的某一端口有否开启

【命令】

```
1 telnet
2 open 10.66.28.222 80
3 open 10.66.28.222 2007
```

【实验结果与分析】

```
欢迎使用 Microsoft Telnet Client

Escape 字符为 'CTRL+]'

Microsoft Telnet> telnet 10.66.28.222 80
无效指令。需要帮助，请键入 ?/help
Microsoft Telnet> open 10.66.28.222 80
正在连接10.66.28.222...无法打开到主机的连接。 在端口 80: 连接失败
Microsoft Telnet> open 10.66.28.222 2007

220 Serv-U FTP Server v6.3 for WinSock ready...
quit
530 Not logged in.
quit
221 Goodbye!
```

在系统DOS命令提示符下运行tracert命令

```
C:/Life/Desktop 21:03:19 81ms
⚡ 🐞 tracert

用法: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
        [-R] [-S srcaddr] [-4] [-6] target_name

选项:
    -d          不将地址解析成主机名。
    -h maximum_hops  搜索目标的最大跃点数。
    -j host-list  与主机列表一起的松散源路由(仅适用于 IPv4)。
    -w timeout    等待每个回复的超时时间(以毫秒为单位)。
    -R          跟踪往返行程路径(仅适用于 IPv6)。
    -S srcaddr    要使用的源地址(仅适用于 IPv6)。
    -4          强制使用 IPv4。
    -6          强制使用 IPv6。
```

1. 使用tracert命令显示连接到校园网某一主机的路由信息

【命令】

```
1 | tracert 10.61.2.6
```

【实验结果与分析】

```
C:/Life/Desktop 21:04:58 81m 8.194s
⚡ 🐞 tracert 10.61.2.6

通过最多 30 个跃点跟踪到 10.61.2.6 的路由

 1      2 ms      2 ms      1 ms    1.1.1.4
 2      3 ms      3 ms      2 ms    10.69.255.123
 3      2 ms      2 ms      2 ms    10.69.255.90
 4      2 ms      2 ms     13 ms    10.61.2.6

跟踪完成。
```

2. 使用tracert命令显示连接到Internet某一站点的路由信息

【命令】

```
1 | tracet www.baidu.com
```

【实验结果与分析】

```
C:/Life/Desktop 21:06:13 26.074s
tracet www.baidu.com

通过最多 30 个跃点跟踪
到 www.baidu.com [112.80.248.76] 的路由:

 1    3 ms    7 ms    <1 毫秒 MI-NANO.lan [192.168.123.1]
 2   17 ms    2 ms    1 ms  122.235.96.1
 3    2 ms    1 ms    2 ms  host53-97.hz.zj.cn [202.96.97.53]
 4    *      *      *      请求超时。
 5   10 ms   20 ms   10 ms  202.97.101.122
 6    *      *      *      请求超时。
 7    *      *      *      请求超时。
 8    *      *      *      请求超时。
 9   16 ms   21 ms   17 ms  153.3.228.198
10   15 ms   17 ms   20 ms  153.3.226.18
11   15 ms   16 ms   17 ms  182.61.216.0
12    *      *      *      请求超时。
13   83 ms  149 ms  304 ms  112.80.248.76

跟踪完成。
C:/Life/Desktop 21:08:36 1m 50.325s
```

在系统DOS命令提示符下运行pathping命令

```
C:/Life/Desktop 21:08:36 1m 50.325s
pathping /?

用法: pathping [-g host-list] [-h maximum_hops] [-i address] [-p period] [-q num_queries] [-w timeout]
              [-4] [-6] target_name

选项:
  -g host-list      与主机列表一起的松散源路由。
  -h maximum_hops   搜索目标的最大跃点数。
  -i address        使用指定的源地址。
  -n                不将地址解析成主机名。
  -p period         两次 Ping 之间等待的时间(以毫秒为单位)。
  -q num_queries    每个跃点的查询数。
  -w timeout        每次回复等待的超时时间(以毫秒为单位)。
  -4                强制使用 IPv4。
  -6                强制使用 IPv6。
C:/Life/Desktop 21:09:03 50ms
```

1. 使用pathping命令显示连接到某一主机的路由信息

【命令】

```
1 | pathping 10.61.2.6
```


【实验结果与分析】

```
C:/Life/Desktop 21:09:03 50ms
pathping 10.61.2.6

通过最多 30 个跃点跟踪到 10.61.2.6 的路由

0  DESKTOP-04JCLRP [10.69.240.248]
1  1.1.1.4
2  10.69.255.123
3  10.69.255.90
4  10.61.2.6

正在计算统计信息，已耗时 100 秒 ...
C:/Life/Desktop 21:10:24 48.813s
```

2. 比较使用ping和tracert命令连接到相同主机返回信息与使用pathping命令的异同点

【命令】

```
1 pathping 10.61.2.6
2 traccert 10.61.2.6
```

【实验结果与分析】

```
C:/Life/Desktop 21:09:03 50ms
pathping 10.61.2.6

通过最多 30 个跃点跟踪到 10.61.2.6 的路由

0  DESKTOP-04JCLRP [10.69.240.248]
1  1.1.1.4
2  10.69.255.123
3  10.69.255.90
4  10.61.2.6

正在计算统计信息，已耗时 100 秒 ...
C:/Life/Desktop 21:10:24 48.813s
tracert 10.61.2.6

通过最多 30 个跃点跟踪到 10.61.2.6 的路由

1      4 ms      2 ms      2 ms      1.1.1.4
2      5 ms      3 ms      8 ms      10.69.255.123
3      2 ms      2 ms      2 ms      10.69.255.90
4      5 ms      2 ms      2 ms      10.61.2.6

跟踪完成。
```

Tracert命令用来显示数据包到达目标主机所经过的路径（路由器），并显示到达每个节

点（路由器）的时间。命令功能同Ping类似，但它所获得的信息要比Ping命令详细得多，它把数据包所走的全部路径、节点的IP以及花费的时间都显示出来。该命令比较适用于大型网络。

pathping 命令是一个路由跟踪工具，它将ping 和 tracert 命令的功能与这两个工具所不提供的其他信息结合起来，综合了二者的功能。pathping会先显示中间的通过的路由器（类似tracert命令得到的信息），然后对每个中间路由器（节点）发送一定数量的ping包，通过统计他们对ping包响应的数据包来分析通信质量

三. 讨论、心得

记录实验感受、上机过程中遇到的困难及解决办法、遗留的问题、意见和建议等。

学到了各种指令的使用方式及作用，收获很大