

# 实验一 常用网络命令及工具实验报告

组号:         

姓名:          学号:          班级: 计算机        

## 一、 实验名称

常用网络命令及工具练习。

## 二、 实验目的

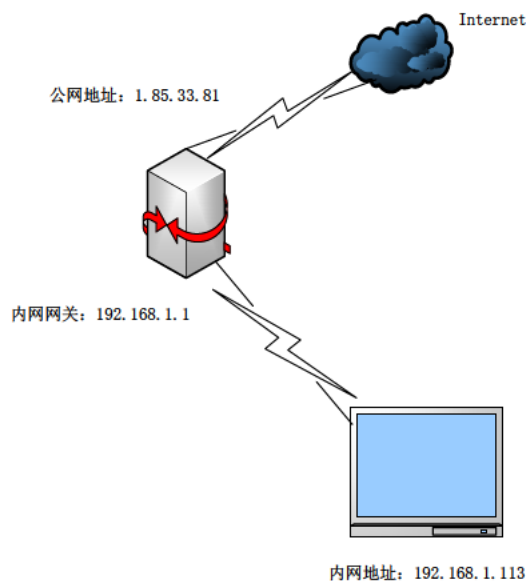
掌握常用网络命令（ping、tracert、ipconfig、route 等）的使用，掌握常用网络工具（如 Wireshark, putty 等）的使用。

## 三、 实验内容

1. 常用网络命令练习；
2. 网络分析软件练习。

## 四、 实验设备环境

按照实际网络情况绘制拓扑图，标注出内网、公网地址。【获取公网地址方式: Wireshark 抓包分析、查看路由器配置、访问 <https://ip138.com/>等网站和 HTTP File Server 软件等】。



## 五、 实验过程及结果分析

【过程记录应当详尽，截图并加以说明。以下过程和表格仅供参考。】

### 1. 常用网络命令练习

步骤 1：以命令行方式查看并记录本机的网络配置信息，查看本机共有几个网卡，哪些是物理网卡，哪些是虚拟网卡；【参考命令：ipconfig /all】

```
PS C:\Users\123> ipconfig /all

Windows IP 配置

主机名 . . . . . : LAPTOP-ROMI2L28
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. . . . . : F8-E4-E3-53-49-AA
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. . . . . : FA-E4-E3-53-49-A9
DHCP 已启用 . . . . . : 否
自动配置已启用. . . . . : 是
```

```

以太网适配器 VMware Network Adapter VMnet1:

    连接特定的 DNS 后缀 . . . . . :
    描述. . . . . : VMware Virtual Ethernet Adapter for VMnet1
    物理地址. . . . . : 00-50-56-C0-00-01
    DHCP 已启用 . . . . . : 是
    自动配置已启用. . . . . : 是
    本地链接 IPv6 地址. . . . . : fe80::139a:c90f:627e:a856%14(首选)
    自动配置 IPv4 地址 . . . . . : 169.254.8.204(首选)
    子网掩码 . . . . . : 255.255.0.0
    默认网关. . . . . :
    DHCPv6 IAID . . . . . : 771772502
    DHCPv6 客户端 DUID . . . . . : 00-01-00-01-28-14-16-6D-F8-E4-E3-53-49-A9
    TCP/IP 上的 NetBIOS . . . . . : 已启用

以太网适配器 VMware Network Adapter VMnet8:

    连接特定的 DNS 后缀 . . . . . :
    描述. . . . . : VMware Virtual Ethernet Adapter for VMnet8
    物理地址. . . . . : 00-50-56-C0-00-08
    DHCP 已启用 . . . . . : 是
    自动配置已启用. . . . . : 是
    本地链接 IPv6 地址. . . . . : fe80::598a:9c98:181f:5d12%18(首选)
    自动配置 IPv4 地址 . . . . . : 169.254.89.115(首选)
    子网掩码 . . . . . : 255.255.0.0
    默认网关. . . . . :
    DHCPv6 IAID . . . . . : 805326934
    DHCPv6 客户端 DUID . . . . . : 00-01-00-01-28-14-16-6D-F8-E4-E3-53-49-A9
    主 WINS 服务器 . . . . . : 192.168.121.2
    TCP/IP 上的 NetBIOS . . . . . : 已启用

无线局域网适配器 WLAN:

    连接特定的 DNS 后缀 . . . . . :
    描述. . . . . : Intel(R) Wireless-AC 9560 160MHz
    物理地址. . . . . : F8-E4-E3-53-49-A9
    DHCP 已启用 . . . . . : 是
    自动配置已启用. . . . . : 是
    本地链接 IPv6 地址. . . . . : fe80::c54e:a519:2a2a:28bd%13(首选)
    IPv4 地址 . . . . . : 192.168.1.113(首选)
    子网掩码 . . . . . : 255.255.255.0
    获得租约的时间 . . . . . : 2023年2月26日 12:35:10
    租约过期的时间 . . . . . : 2023年2月26日 15:21:32
    默认网关. . . . . : 192.168.1.1
    DHCP 服务器 . . . . . : 192.168.1.1
    DHCPv6 IAID . . . . . : 116974819
    DHCPv6 客户端 DUID . . . . . : 00-01-00-01-28-14-16-6D-F8-E4-E3-53-49-A9
    DNS 服务器 . . . . . : 61.134.1.4
    . . . . . : 218.30.19.40
    TCP/IP 上的 NetBIOS . . . . . : 已启用

以太网适配器 蓝牙网络连接:

    媒体状态 . . . . . : 媒体已断开连接
    连接特定的 DNS 后缀 . . . . . :
    描述. . . . . : Bluetooth Device (Personal Area Network)
    物理地址. . . . . : F8-E4-E3-53-49-AD
    DHCP 已启用 . . . . . : 是
    自动配置已启用. . . . . : 是

```

本机共有 6 个网卡,其中有 2 个物理网卡: Intel(R) Wireless-AC 9560 160MHz、Bluetooth Device (Personal Area Network), 其余 4 个为虚拟网卡。

本机上网时用的是哪一个网卡, IP 地址、子网掩码、默认网关及 DNS 服务器地址分别是多少?

字段	配置值
上网网卡描述	Intel(R) Wireless-AC 9560 160MHz
IP 地址	192.168.1.113
子网掩码	255.255.255.0
默认网关	192.168.1.1
DNS 服务器	61.134.1.4 218.30.19.40

步骤 2：用命令行修改本机 IP 地址和 DNS 服务器地址的获取方式（原来是自动获取方式则改为手动设置，原来为手动设置地址则改为自动获取）查看并记录网卡配置信息，与手动设置地址时的配置有什么不同？

【参考命令：

IP 地址手动设置命令：netsh interface ip set address name="本地连接" static 192.168.1.101 255.255.255.0 192.168.1.1；

DNS 服务器地址手动设置命令：netsh interface ip set dns name="本地连接" source=static add=202.117.1.20；

IP 地址自动获取命令：netsh interface ip set address name="本地连接" source=dhcp；

DNS 服务器地址自动获取设置命令：netsh interface ip set dns name="本地连接" source=dhcp。

（注意将 name、IP 地址等参数改为自己电脑网卡的实际参数）】

IP 地址手动设置：

```
PS C:\Users\123> netsh interface ip set address name="WLAN" static 192.168.1.113 255.255.255.0 192.168.1.1
```

无线局域网适配器 WLAN：

```

连接特定的 DNS 后缀 . . . . . :
描述. . . . . : Intel(R) Wireless-AC 9560 160MHz
物理地址. . . . . : F8-E4-E3-53-49-A9
DHCP 已启用 . . . . . : 否
自动配置已启用. . . . . : 是
本地链接 IPv6 地址. . . . . : fe80::c54e:a519:2a2a:28bd%13(首选)
IPv4 地址 . . . . . : 192.168.1.113(首选)
子网掩码 . . . . . : 255.255.255.0
默认网关. . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 116974819
DHCPv6 客户端 DUID . . . . . : 00-01-00-01-28-14-16-6D-F8-E4-E3-53-49-A9
DNS 服务器 . . . . . : fec0:0:0:ffff::1%1
                       fec0:0:0:ffff::2%1
                       fec0:0:0:ffff::3%1
TCPIP 上的 NetBIOS . . . . . : 已启用

```

DNS 服务器地址手动设置：

```
PS C:\Users\123> netsh interface ip set dns name="WLAN" source=static add=61.134.1.4
```

```

无线网络适配器 WLAN:

  连接特定的 DNS 后缀 . . . . . : 
  描述 . . . . . : Intel(R) Wireless-AC 9560 160MHz
  物理地址. . . . . : F8-E4-E3-53-49-A9
  DHCP 已启用 . . . . . : 否
  自动配置已启用. . . . . : 是
  本地链接 IPv6 地址. . . . . : fe80::c54e:a519:2a2a:28bd%13(首选)
  IPv4 地址 . . . . . : 192.168.1.113(首选)
  子网掩码 . . . . . : 255.255.255.0
  默认网关 . . . . . : 192.168.1.1
  DHCPv6 IAID . . . . . : 116974819
  DHCPv6 客户端 DUID . . . . . : 00-01-00-01-28-14-16-6D-F8-E4-E3-53-49-A9
  DNS 服务器 . . . . . : 61.134.1.4
  TCP/IP 上的 NetBIOS . . . . . : 已启用

```

恢复自动获取:

```

PS C:\Users\123> netsh interface ip set address name="WLAN" source=dhcp
PS C:\Users\123> netsh interface ip set dns name="WLAN" source=dhcp

```

手动设置地址时, DHCP 已启用字段值为否。

步骤 3: 查看并记录本机的路由表, 标记出默认路由。用命令行删除默认路由, 看看本机还能否上网并分析原因 (如果还能上网, 查看是否开启了 IPv6, 可禁用后再试)。查看网卡的默认网关配置是否还在? 【参考命令: route print, route delete, ipconfig】

默认路由如红框所示:

```

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      192.168.1.1  192.168.1.113  35
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      169.254.8.204  291
169.254.0.0      255.255.0.0      在链路上      169.254.89.115  291
169.254.8.204  255.255.255.255  在链路上      169.254.8.204  291
169.254.89.115  255.255.255.255  在链路上      169.254.89.115  291
169.254.255.255  255.255.255.255  在链路上      169.254.8.204  291
169.254.255.255  255.255.255.255  在链路上      169.254.89.115  291
192.168.1.0      255.255.255.0      在链路上      192.168.1.113  291
192.168.1.113  255.255.255.255  在链路上      192.168.1.113  291
192.168.1.255  255.255.255.255  在链路上      192.168.1.113  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      192.168.1.113  291
224.0.0.0      240.0.0.0      在链路上      169.254.8.204  291
224.0.0.0      240.0.0.0      在链路上      169.254.89.115  291
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      192.168.1.113  291
255.255.255.255  255.255.255.255  在链路上      169.254.8.204  291
255.255.255.255  255.255.255.255  在链路上      169.254.89.115  291
=====
永久路由:
无

```

删除默认路由后:

```

PS C:\Users\123> route delete 0.0.0.0 mask 0.0.0.0 192.168.1.1
操作完成!

```

```
IPv4 路由表
=====
活动路由:
网络目标      网络掩码      网关      接口      跃点数
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      169.254.8.204      291
169.254.0.0      255.255.0.0      在链路上      169.254.89.115      291
169.254.8.204      255.255.255.255      在链路上      169.254.8.204      291
169.254.89.115      255.255.255.255      在链路上      169.254.89.115      291
169.254.255.255      255.255.255.255      在链路上      169.254.8.204      291
169.254.255.255      255.255.255.255      在链路上      169.254.89.115      291
192.168.1.0      255.255.255.0      在链路上      192.168.1.113      291
192.168.1.113      255.255.255.255      在链路上      192.168.1.113      291
192.168.1.255      255.255.255.255      在链路上      192.168.1.113      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      192.168.1.113      291
224.0.0.0      240.0.0.0      在链路上      169.254.8.204      291
224.0.0.0      240.0.0.0      在链路上      169.254.89.115      291
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      192.168.1.113      291
255.255.255.255      255.255.255.255      在链路上      169.254.8.204      291
255.255.255.255      255.255.255.255      在链路上      169.254.89.115      291
=====
永久路由:
无
```

```
无线局域网适配器 WLAN:

   连接特定的 DNS 后缀 . . . . . : 
   描述. . . . . : Intel(R) Wireless-AC 9560 160MHz
   物理地址. . . . . : F8-E4-E3-53-49-A9
   DHCP 已启用 . . . . . : 是
   自动配置已启用. . . . . : 是
   IPv4 地址 . . . . . : 192.168.1.113(首选)
   子网掩码 . . . . . : 255.255.255.0
   获得租约的时间 . . . . . : 2023年2月26日 13:39:12
   租约过期的时间 . . . . . : 2023年2月26日 15:51:48
   默认网关. . . . . : 
   DHCP 服务器 . . . . . : 192.168.1.1
   DNS 服务器 . . . . . : 61.134.1.4
                           218.30.19.40
   TCP/IP 上的 NetBIOS . . . . . : 已启用
```

```
PS C:\Users\123> ping 202.117.1.13

正在 Ping 202.117.1.13 具有 32 字节的数据:
PING: 传输失败。常见故障。
PING: 传输失败。常见故障。
PING: 传输失败。常见故障。
PING: 传输失败。常见故障。

202.117.1.13 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 0, 丢失 = 4 (100% 丢失),
```

删除默认路由后，默认网关字段为空，本机无法上网，原因在于所访问的主机并不在当前路由表中，它本应通过默认路由转发数据包，但此时默认路由已被删除，无法转发数据包。

步骤 4：分别用 `route add` 和 `route add -p` 增加一条默认路由，看看它们会出现在哪个路由表里，这两个路由表中的路由有什么不同？

route add:

```
PS C:\Users\123> route add 0.0.0.0 mask 0.0.0.0 192.168.1.1 metric 35
操作完成!
```

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      192.168.1.1  192.168.1.113  70
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      169.254.8.204  291
169.254.0.0      255.255.0.0      在链路上      169.254.89.115  291
169.254.8.204  255.255.255.255  在链路上      169.254.8.204  291
169.254.89.115  255.255.255.255  在链路上      169.254.89.115  291
169.254.255.255  255.255.255.255  在链路上      169.254.8.204  291
169.254.255.255  255.255.255.255  在链路上      169.254.89.115  291
192.168.1.0      255.255.255.0      在链路上      192.168.1.113  291
192.168.1.113  255.255.255.255  在链路上      192.168.1.113  291
192.168.1.255  255.255.255.255  在链路上      192.168.1.113  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      192.168.1.113  291
224.0.0.0      240.0.0.0      在链路上      169.254.8.204  291
224.0.0.0      240.0.0.0      在链路上      169.254.89.115  291
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      192.168.1.113  291
255.255.255.255  255.255.255.255  在链路上      169.254.8.204  291
255.255.255.255  255.255.255.255  在链路上      169.254.89.115  291
=====
永久路由:
无
```

route add -p:

```
PS C:\Users\123> route add -p 0.0.0.0 mask 0.0.0.0 192.168.1.1 metric 35
操作完成!
```



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	192.168.1.1	192.168.1.113	70	
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	169.254.8.204	291	
169.254.0.0	255.255.0.0	在链路上	169.254.89.115	291	
169.254.8.204	255.255.255.255	在链路上	169.254.8.204	291	
169.254.89.115	255.255.255.255	在链路上	169.254.89.115	291	
169.254.255.255	255.255.255.255	在链路上	169.254.8.204	291	
169.254.255.255	255.255.255.255	在链路上	169.254.89.115	291	
192.168.1.0	255.255.255.0	在链路上	192.168.1.113	291	
192.168.1.113	255.255.255.255	在链路上	192.168.1.113	291	
192.168.1.255	255.255.255.255	在链路上	192.168.1.113	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	192.168.1.113	291	
224.0.0.0	240.0.0.0	在链路上	169.254.8.204	291	
224.0.0.0	240.0.0.0	在链路上	169.254.89.115	291	
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	192.168.1.113	291	
255.255.255.255	255.255.255.255	在链路上	169.254.8.204	291	
255.255.255.255	255.255.255.255	在链路上	169.254.89.115	291	
=====					
永久路由:					
网络地址	网络掩码	网关地址	跃点数		
0.0.0.0	0.0.0.0	192.168.1.1	35		
=====					

route add 在 IPv4 路由表的活动路由里增加路由，而 route add -p 在永久路由里增加路由。永久路由里的路由会保存在计算机中，计算机重启后仍然有效；而活动路由在计算机重启后会清空并重新建立。

步骤 5: 在命令行运行 ipconfig /flushdns 清除本地 DNS 缓存，ping 通一个网址（如 www.xjtu.edu.cn）后，用 ipconfig /displaydns 查看本地 DNS 缓存，记录域名与 IP 地址。

```

PS C:\Users\123> ipconfig /flushdns

Windows IP 配置

已成功刷新 DNS 解析缓存。
PS C:\Users\123> ping www.xjtu.edu.cn

正在 Ping www.xjtu.edu.cn [202.117.1.13] 具有 32 字节的数据:
来自 202.117.1.13 的回复: 字节=32 时间=1ms TTL=60
来自 202.117.1.13 的回复: 字节=32 时间=1ms TTL=60
来自 202.117.1.13 的回复: 字节=32 时间=2ms TTL=60
来自 202.117.1.13 的回复: 字节=32 时间=5ms TTL=60

202.117.1.13 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 = 5ms, 平均 = 2ms

```



```
www.xjtu.edu.cn
-----
记录名称. . . . . : www.xjtu.edu.cn
记录类型. . . . . : 1
生存时间. . . . . : 53
数据长度. . . . . : 4
部分. . . . . : 答案
A (主机)记录 . . . . : 202.117.1.13
```

域名: [www.xjtu.edu.cn](http://www.xjtu.edu.cn)

IP 地址: 202.117.1.13

步骤 6: 把网卡的 DNS 服务器地址修改为无效 DNS 地址, 分别 ping 域名和 IP 地址看能否 ping 通, 查看本地 DNS 缓存, 记录结果并分析原因。【参考命令: netsh interface ip set dns name="本地连接" source=static add=202.117.1.222】

```
PS C:\Users\123> netsh interface ip set dns name="WLAN" source=static add=10.10.10.10
配置的 DNS 服务器不正确或不存在。

PS C:\Users\123> ping www.xjtu.edu.cn
Ping 请求找不到主机 www.xjtu.edu.cn。请检查该名称, 然后重试。
PS C:\Users\123> ping 202.117.1.13

正在 Ping 202.117.1.13 具有 32 字节的数据:
来自 202.117.1.13 的回复: 字节=32 时间=2ms TTL=60
来自 202.117.1.13 的回复: 字节=32 时间=2ms TTL=60
来自 202.117.1.13 的回复: 字节=32 时间=5ms TTL=60
来自 202.117.1.13 的回复: 字节=32 时间=2ms TTL=60

202.117.1.13 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 = 5ms, 平均 = 2ms
```

域名无法 ping 通, 而 IP 地址可以 ping 通。原因在于通过域名 ping 网站主页时, 需要访问 DNS 服务器进行 IP 地址转换, 只有通过 IP 地址才能够访问网站主页, 当 DNS 服务器地址无效时, 无法得到域名所对应的 IP 地址, 自然无法 ping 通。

## 2. 网络分析工具练习

步骤 1: 将网卡禁用后再启用, 打开 Wireshark 软件抓包, 能够正常上网后 (打开网页、登录微信成功等) 停止抓包。查看捕获的数据包及涉及到的协议, 选择 2 种协议 (如 DHCP, ARP 等, 利用协议过滤筛选出该协议报文), 分析协议的功能及关键交互数据。

SSDP 协议:

1 0.000000	192.168.1.110	239.255.255.250	SSDP	179 M-SEARCH * HTTP/1.1	
2 2.448227	192.168.1.100	239.255.255.250	SSDP	243 M-SEARCH * HTTP/1.1	
4 2.970120	192.168.1.110	239.255.255.250	SSDP	179 M-SEARCH * HTTP/1.1	
23 5.929334	192.168.1.110	239.255.255.250	SSDP	179 M-SEARCH * HTTP/1.1	

> Frame 1: 179 bytes on wire (1432 bits), 179 bytes captured (1432 bits) on interface > Ethernet II, Src: ASUSTek_4c:5b:ce (24:4b:fe:4c:5b:ce), Dst: IPv4mcast_7f:ffa (01:00:5e:7f:ff:fa) > Internet Protocol Version 4, Src: 192.168.1.110, Dst: 239.255.255.250 > User Datagram Protocol, Src Port: 61682, Dst Port: 1900 > Simple Service Discovery Protocol M-SEARCH * HTTP/1.1\r\n             M-SEARCH * HTTP/1.1\r\n               [Expert Info (Chat/Sequence): M-SEARCH * HTTP/1.1\r\n]                 [M-SEARCH * HTTP/1.1\r\n]                 [Severity level: Chat]                 [Group: Sequence]                 Request Method: M-SEARCH                 Request URI: *                 Request Version: HTTP/1.1                 Host: 239.255.255.250:1900\r\n	0000 01 00 5e 7f ff fa 24 4b fe 4c 5b ce 08 00 45 00 ...\$K .L[...E- 0010 00 a5 42 6a 00 00 04 11 c1 cd c0 a8 01 6e ef ff ...Bj-...-n- 0020 ff fa f0 f2 07 6c 00 01 62 3e 4d 2d 53 45 41 52 ...-l- bM-SEAR 0030 43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48 CH * HT P/1.1-H 0040 6f 73 74 3a 20 32 33 39 2e 32 35 35 2e 32 35 35 ost: 239 .255.255 0050 2e 32 35 30 3a 31 39 30 30 0d 0a 53 54 3a 20 75 .250:190 0-ST: u 0060 72 6e 3a 73 63 68 65 6d 61 73 2d 75 70 6e 70 2d rn:schem as-upnp- 0070 6f 72 67 3a 64 65 76 69 63 65 3a 49 6e 74 65 72 org:devi ce:Inter 0080 6e 65 74 47 61 74 65 77 61 79 44 65 76 69 63 65 netGatew ayDevice 0090 3a 31 0d 0a 4d 61 6e 3a 20 22 73 73 64 70 3a 64 :1-Man: "ssdp:d 00a0 69 73 63 6f 76 65 72 22 0d 0a 4d 58 3a 20 33 0d iscover" --MX: 3- 00b0 0a 0d 0a ...
---	--

DNS 协议：

84 11.081279	192.168.1.113	61.134.1.4	DNS	75 Standard query 0xfe5a A www.xjtu.edu.cn	
85 11.089900	192.168.1.113	61.134.1.4	DNS	75 Standard query 0xdb34 A www.xjtu.edu.cn	
86 11.090372	192.168.1.113	61.134.1.4	DNS	75 Standard query 0x28c0 HTTPS www.xjtu.edu.cn	
88 11.096711	61.134.1.4	192.168.1.113	DNS	191 Standard query response 0xfe5a A www.xjtu.edu.cn A 202.117.1.13 NS ns2.xjtu.edu.cn NS dec3000.xjtu.edu.cn	
89 11.099350	61.134.1.4	192.168.1.113	DNS	124 Standard query response 0x28c0 HTTPS www.xjtu.edu.cn SOA dec3000.xjtu.edu.cn	
90 11.099350	61.134.1.4	192.168.1.113	DNS	163 Standard query response 0xdb34 A www.xjtu.edu.cn A 202.117.1.13 NS dec3000.xjtu.edu.cn NS ns2.xjtu.edu.cn	
178 14.214299	192.168.1.113	61.134.1.4	DNS	74 Standard query 0xae8 A en.xjtu.edu.cn	

> Frame 84: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface > Ethernet II, Src: IntelCor_53:49:a9 (f8:e4:e3:53:49:a9), Dst: Tp-LinkT_ac:75:a0 > Internet Protocol Version 4, Src: 192.168.1.113, Dst: 61.134.1.4 > User Datagram Protocol, Src Port: 56669, Dst Port: 53 > Domain Name System (query) Transaction ID: 0xfe5a Flags: 0x0100 Standard query Questions: 1 Answer RRs: 0 Authority RRs: 0 Additional RRs: 0 Queries www.xjtu.edu.cn: type A, class IN Name: www.xjtu.edu.cn [Name Length: 15] [Label Count: 4] Type: A (Host Address) (1) Class: IN (0x0001) [Response In: 88]	0000 64 6e 97 ac 75 a0 fa e4 e3 53 49 a9 00 00 45 00 dn-u...-SI...E- 0010 00 3d 49 31 00 00 80 11 00 00 c0 a8 01 71 3d 86 --II-...-q- 0020 01 04 dd 5d 00 35 00 29 00 de fe 5a 01 00 00 01 ...]-5-)-Z- 0030 00 00 00 00 00 03 77 77 77 04 78 6a 74 75 03 .....w ww xjtu- 0040 65 64 75 02 63 6e 00 00 01 00 01 .....edu.cn-...
---	--

协议名	描述项	配置值
例：ARP	协议功能	IP 地址对应 MAC 地址解析
	源地址-目的地址	192.168.0.101 - Broadcast
	请求/应答信息	Who has 192.168.0.1? Tell 192.168.0.101
SSDP	协议功能	为网络客户端提供了一种发现网络服务的机制
	源地址-目的地址	192.168.1.110 - 239.255.255.250
	请求/应答信息	M-SEARCH * HTTP/1.1
DNS	协议功能	将域名转换为 IP 地址
	源地址-目的地址	192.168.1.113 - 61.134.1.4
	请求/应答信息	Standard query 0xfe5a A www.xjtu.edu.cn

步骤 2: 清除本机的 DNS 缓存【参考命令: ipconfig /flushdns】,运行 Wireshark 截获报文, 浏览器访问网站 (如 <http://github.com>, 浏览新闻, 下载软件等), 利用 IP 地址过滤筛选出访问该网站的报文, 查看访问该网站时, 都用到了哪些协议, 主要作用是什么? 【域名解析为 IP 地址方法: ping 域名, 或 nslookup 域名】

```
PS C:\Users\123> ipconfig /flushdns

Windows IP 配置

已成功刷新 DNS 解析缓存。
```

No.	Time	Source	Destination	Protocol	Length	Info
222	8.704183	192.168.1.113	202.117.1.13	TCP	66	61033 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
223	8.704380	192.168.1.113	202.117.1.13	TCP	66	61034 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
233	8.705973	202.117.1.13	192.168.1.113	TCP	66	80 → 61033 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1440 SACK_PERM WS=128
234	8.705973	202.117.1.13	192.168.1.113	TCP	66	80 → 61034 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1440 SACK_PERM WS=128
235	8.706095	192.168.1.113	202.117.1.13	TCP	54	61033 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len=0
236	8.706146	192.168.1.113	202.117.1.13	TCP	54	61034 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len=0
255	8.947938	192.168.1.113	202.117.1.13	HTTP	624	GET /system/resource/code/datainput.jsp?owner=1151962237&e=1&w=1536&h=864&tree
256	8.949627	202.117.1.13	192.168.1.113	TCP	54	80 → 61033 [ACK] Seq=1 Ack=571 Win=15744 Len=0
262	8.985466	202.117.1.13	192.168.1.113	HTTP	914	HTTP/1.1 200 OK
272	9.029763	192.168.1.113	202.117.1.13	TCP	54	61033 → 80 [ACK] Seq=571 Ack=861 Win=131584 Len=0
573	13.986520	202.117.1.13	192.168.1.113	TCP	54	80 → 61033 [FIN, ACK] Seq=861 Ack=571 Win=15744 Len=0

协议名	描述项	配置值
例: TCP	协议功能	传输控制协议,在不可靠的互联网络上提供可靠的端到端传输。
	源地址-目的地址	192.168.0.101 - 182.61.200.6
	请求/应答信息	49947 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM=1
TCP	协议功能	传输控制协议,在不可靠的互联网络上提供可靠的端到端传输。
	源地址-目的地址	192.168.1.113 - 202.117.1.13
	请求/应答信息	61033 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
HTTP	协议功能	超文本传输协议,是客户端和服务端进行数据传输的一种规则。
	源地址-目的地址	202.117.1.13 - 192.168.1.113
	请求/应答信息	HTTP/1.1 200 OK

步骤 3: 运行 Wireshark 截获报文, 登陆 QQ 或微信, 和好友进行语音或者视频聊天。查看截获的报文, 找出 QQ 或微信的服务器地址, 分析语音或视频通信过程中双方的 IP 地址、协议及端口等信息。

No.	Time	Source	Destination	Protocol	Length	Info
87	4.032747	39.156.125.39	192.168.1.113	OICQ	177	OICQ Protocol
88	4.032979	192.168.1.113	39.156.125.39	OICQ	97	OICQ Protocol
89	4.034899	39.156.125.39	192.168.1.113	OICQ	225	OICQ Protocol
90	4.035346	192.168.1.113	39.156.125.39	OICQ	97	OICQ Protocol

505	8.996324	192.168.1.113	192.168.1.110	UDP	98	61591 → 64220 Len=56
506	9.015980	192.168.1.113	192.168.1.110	UDP	72	61591 → 64220 Len=30
507	9.016710	192.168.1.113	192.168.1.110	UDP	72	61591 → 64220 Len=30

Frame 506: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface Ethernet II, Src: IntelCor_53:49:a9 (f8:e4:e3:53:49:a9), Dst: ASUSTekC_4c:5b:ce (28:90:5b:4c:5b:ce), Internet Protocol Version 4, Src: 192.168.1.113, Dst: 192.168.1.110	0000	24 4b fe 4c 5b ce f8 e4
User Datagram Protocol, Src Port: 61591, Dst Port: 64220	0010	00 3a 4d 86 00 00 80 11
Source Port: 61591	0020	01 6e f0 97 fa dc 00 26
Destination Port: 64220	0030	00 00 ea 61 1e 78 a1 02
Length: 38	0040	81 06 04 00 00 00 01 00
Checksum: 0x8467 [unverified]		
[Checksum Status: Unverified]		
[Stream index: 7]		
> [Timestamps]		
UDP payload (30 bytes)		
Data (30 bytes)		

## 本机捕获信息

描述项	值
-----	---

QQ/微信服务器地址	39.156.125.39
本机 IP 地址	192.168.1.113
本机自测公网地址	1.85.33.81
通信好友的 IP 地址	192.168.1.110
通信协议 (Protocol)	UDP
通信源端口-目的端口	61591 - 64220

### 好友端捕获信息

描述项	值
QQ/微信服务器地址	222.94.109.249
本机 IP 地址	192.168.1.110
本机自测公网地址	1.85.33.81
通信好友的 IP 地址	192.168.1.113
通信协议 (Protocol)	UDP
通信源端口-目的端口	64220 - 61591

### 3. 互动讨论主题

本地计算机接入网络之后，需要通过哪些设置、启用哪些协议之后才能上网（通过域名访问网站等）。

- ①需要设置 IP 地址、子网掩码、默认网关、DNS 服务器地址；
- ②需要启用的协议有：DHCP 协议、ARP 协议、TCP 协议、UDP 协议等。

### 4. \*进阶自设计

通过 Wireshark 抓包分析 QQ 的登陆认证、消息传输、语音/视频通话、退出等过程，分析各过程中涉及到的协议、服务器地址和数据包标识等。

【OICQ 是 QQ 的专用协议类型，注意观察数据包中的标识，看看能找到多少种类型的 OICQ 数据包，可利用这些数据包区分各个功能段。综合利用 Wireshark 软件的协议过滤、IP 地址过滤、数据流追踪等功能，找出 QQ 各个过程对应的数据包段。】

#### 1) 登录认证：

##### ①DNS 协议：

36	12.563429	192.168.1.113	61.134.1.4	DNS	69 Standard query 0x430a A ts.qq.com
37	12.566522	61.134.1.4	192.168.1.113	DNS	149 Standard query response 0x430a A ts.qq.com CN

Frame 36: 69 bytes on wire (552 bits), 69 bytes captured (552 bits) on interface \Device\NPF	0000	64 6e 97 ac 75 a0 f8 e4
Ethernet II, Src: IntelCor_53:49:a9 (f8:e4:e3:53:49:a9), Dst: Tp-LinkT_ac:75:a0 (64:6e:97:a	0010	00 37 f9 ed 00 00 80 11
Internet Protocol Version 4, Src: 192.168.1.113, Dst: 61.134.1.4	0020	01 04 c5 d8 00 35 00 23
User Datagram Protocol, Src Port: 50648, Dst Port: 53	0030	00 00 00 00 00 00 02 74
Domain Name System (query)	0040	00 00 01 00 01

服务器地址：61.134.1.4

数据包标识：Standard query 0x430a A ts.qq.com

##### ②UDP 协议：

87 13.217288	117.88.120.115	192.168.1.113	UDP	449 8000 → 4017 Len=407
Frame 87: 449 bytes on wire (3592 bits), 449 bytes captured (3592 bits) on interface \Device\NPF{...} Ethernet II, Src: Tp-LinkT_ac:75:a0 (64:6e:97:ac:75:a0), Dst: IntelCor_53:49:a9 (f8:e4:e3:53:49:a9) Internet Protocol Version 4, Src: 117.88.120.115, Dst: 192.168.1.113 User Datagram Protocol, Src Port: 8000, Dst Port: 4017 Data (407 bytes)				
0000 f8 e4 e3 53 49 a9 64 6e				
0010 01 b3 72 62 40 00 35 11				
0020 01 71 1f 40 0f b1 01 9f				
0030 73 14 e8 81 06 00 00 00				
0040 f3 63 35 86 5f 60 a7 c9				
0050 c3 05 67 1f d7 00 00 00				

服务器地址：117.88.120.115

### ③OICQ 协议：

89 13.229174	192.168.1.113	117.88.120.115	OICQ	81 OICQ Protocol
90 13.229281	192.168.1.113	117.88.120.115	OICQ	81 OICQ Protocol
Frame 89: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface \Device\NPF{...} Ethernet II, Src: IntelCor_53:49:a9 (f8:e4:e3:53:49:a9), Dst: Tp-LinkT_ac:75:a0 (64:6e:97:ac:75:a0) Internet Protocol Version 4, Src: 192.168.1.113, Dst: 117.88.120.115 User Datagram Protocol, Src Port: 4017, Dst Port: 8000				
OICQ - IM software, popular in China				
Flag: Oicq packet (0x02)				
Version: 0x3b3b				
Command: Request KEY (29)				
Sequence: 4347				
Data(OICQ Number,if sender is client): 350781702				
> Data: \002				
0000 64 6e 97 ac 75 a0 f8 e4				
0010 00 43 db 45 00 00 80 11				
0020 78 73 0f b1 1f 40 00 2f				
0030 fb 14 e8 81 06 02 00 00				
0040 e1 42 8d 06 7e 47 11 f5				
0050 03				

服务器地址：117.88.120.115

数据包标识：Command 字段为 Request KEY；Data 字段为登录的 QQ 号

## 2) 消息传输与语音/视频通话：

### ①OICQ 协议：

1053 15.504743	117.88.120.115	192.168.1.113	OICQ	177 OICQ Protocol
1054 15.504743	117.88.120.115	192.168.1.113	OICQ	177 OICQ Protocol
1055 15.504743	117.88.120.115	192.168.1.113	OICQ	177 OICQ Protocol
1056 15.504743	117.88.120.115	192.168.1.113	OICQ	209 OICQ Protocol
Frame 1054: 177 bytes on wire (1416 bits), 177 bytes captured (1416 bits) on interface \Device\NPF{...} Ethernet II, Src: Tp-LinkT_ac:75:a0 (64:6e:97:ac:75:a0), Dst: IntelCor_53:49:a9 (f8:e4:e3:53:49:a9) Internet Protocol Version 4, Src: 117.88.120.115, Dst: 192.168.1.113 User Datagram Protocol, Src Port: 8000, Dst Port: 4017				
OICQ - IM software, popular in China				
Flag: Oicq packet (0x02)				
Version: 0x3b3b				
Command: Receive message (23)				
Sequence: 33415				
Data(OICQ Number,if sender is client): 350781702				
> Data:				
0000 f8 e4 e3 53 49 a9 64 6e				
0010 00 a3 78 21 40 00 35 11				
0020 01 71 1f 40 0f b1 00 8f				
0030 87 14 e8 81 06 00 00 6a				
0040 56 96 81 ee 17 4f a1 d0				
0050 1a 83 aa 7d e3 10 18 37				
0060 76 7d 71 22 42 67 2d 47				
0070 0f 69 2f c1 12 c9 90 40				
0080 32 6e e4 71 08 09 a1 5b				
0090 97 99 dc e6 51 56 7e 29				
00a0 aa 43 ce f7 58 0f dd 57				
00b0 03				

服务器地址：117.88.120.115

Command 字段分别有：Receive message、Get friend online、Group name operation、Request extra information、MEMO Operation、Heart Message、Set status、Get level 等。

### ②UDP 协议：

4387 39.478809	192.168.1.107	192.168.1.113	UDP	151 43867 → 51324 Len=109
4388 39.478809	192.168.1.107	192.168.1.113	UDP	86 43867 → 51324 Len=44
4389 39.505008	192.168.1.107	192.168.1.113	UDP	96 43867 → 51324 Len=54
4390 39.505008	192.168.1.107	192.168.1.113	UDP	88 43867 → 51324 Len=46
Frame 4388: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF{...} Ethernet II, Src: 72:a6:68:69:a4:ce (72:a6:68:69:a4:ce), Dst: IntelCor_53:49:a9 (f8:e4:e3:53:49:a9) Internet Protocol Version 4, Src: 192.168.1.107, Dst: 192.168.1.113 User Datagram Protocol, Src Port: 43867, Dst Port: 51324 Data (44 bytes)				
0000 f8 e4 e3 53 49 a9 72 a6				
0010 00 48 92 e3 40 00 40 11				
0020 01 71 ab 5b c8 7c 00 34				
0030 00 01 71 8a 3a 90 9a 98				
0040 01 4e 89 90 05 00 00 0c				
0050 0f fe 8e ab 00 00				

好友 ip 地址：192.168.1.107

在这个过程中，OICQ 协议负责传送操作命令，UDP 协议负责传送通信数据。

3) 退出:

①OICQ 协议:

4891 55.028047	192.168.1.113	117.88.120.115	OICQ	97 OICQ Protocol	
Frame 4891: 97 bytes on wire (776 bits), 97 bytes captured (776 bits) on interface \Device\NPF{...} Ethernet II, Src: IntelCor_53:49:a9 (f8:e4:e3:53:49:a9), Dst: Tp-LinkT_ac:75:a0 (64:6e:97:a0:00:00) Internet Protocol Version 4, Src: 192.168.1.113, Dst: 117.88.120.115 User Datagram Protocol, Src Port: 4017, Dst Port: 8000					0000 64 6e 97 ac 75 a0 f8 e4 0010 00 53 df 78 00 00 80 11 0020 78 73 0f b1 1f 40 00 3f 0030 66 14 e8 81 06 02 00 00 0040 84 66 57 0a dd ca 13 bb 0050 54 c4 d9 bc 89 ad 01 8f 0060 03
OICQ - IM software, popular in China					
Flag: Oicq packet (0x02)					
Version: 0x3b3b					
Command: Request login (98)					
Sequence: 2406					
Data(OICQ Number,if sender is client): 350781702					
> Data: \002					

服务器地址: 117.88.120.115

Command 字段为 Request login

②DNS 协议:

4894 55.036878	192.168.1.113	61.134.1.4	DNS	78 Standard query	0x9c32 A oth.eve.mdt.qq.com
4895 55.046271	61.134.1.4	192.168.1.113	DNS	475 Standard query response	0x9c32 A oth.eve.mdt.qq.com
Frame 4894: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF{...} Ethernet II, Src: IntelCor_53:49:a9 (f8:e4:e3:53:49:a9), Dst: Tp-LinkT_ac:75:a0 (64:6e:97:a0:00:00) Internet Protocol Version 4, Src: 192.168.1.113, Dst: 61.134.1.4 User Datagram Protocol, Src Port: 58938, Dst Port: 53 Domain Name System (query)					0000 64 6e 97 ac 75 a0 f8 e4 0010 00 40 fa 0e 00 00 80 11 0020 01 04 e6 3a 00 35 00 2c 0030 00 00 00 00 00 00 03 6f 0040 64 74 02 71 71 03 63 6f

服务器地址: 61.134.1.4

数据包标识: Standard query 0x9c32 A oth.eve.mdt.qq.com

## 六、 总结及心得体会

通过本次实验,我掌握了 ping、ipconfig、route 等常用网络命令的使用,并学会了如何通过这些命令查看及配置本机的 ip 地址、子网掩码、默认网关以及 DNS 服务器。同时,我还掌握了网络抓包工具 wireshark 的使用,利用它抓取了 QQ 登录及消息传送等过程中的数据包,并分析了在这些过程中所涉及的相关网络协议。