

实验一 常用网络命令及工具实验报告

组号： _____

姓名： _____ 学号： _____ 班级： _____

一、 实验名称

常用网络命令及工具练习。

二、 实验目的

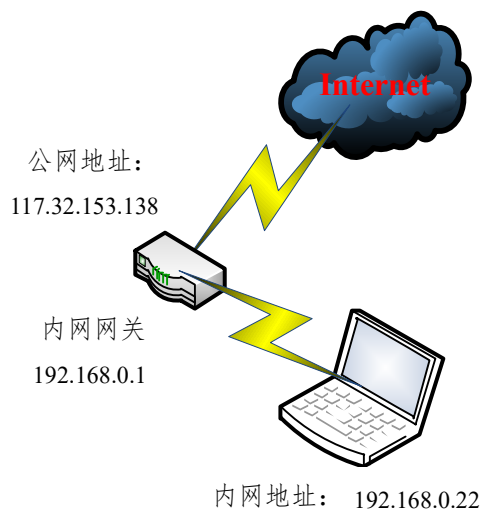
掌握常用网络命令（ping、tracert、ipconfig、route 等）的使用，掌握常用网络工具（如 Wireshark，putty 等）的使用。

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

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】

有一个物理网卡“本地连接”，相关信息见下图 2、3：

```
以太网适配器 本地连接:

    连接特定的 DNS 后缀 . . . . . : 
    本地连接 IPv6 地址. . . . . : fe80::1977:3b29:856:d7ff%11
    IPv4 地址 . . . . . : 192.168.0.22
    子网掩码 . . . . . : 255.255.254.0
    默认网关. . . . . : 192.168.0.1

隧道适配器 isatap.{554760F8-096E-4BA4-9606-1EBFAC1C35A9}:

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

图 2

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

Windows IP 配置

    主机名 . . . . . : PC022
    主 DNS 后缀 . . . . . : 
    节点类型 . . . . . : 混合
    IP 路由已启用 . . . . . : 否
    WINS 代理已启用 . . . . . : 否

以太网适配器 本地连接:

    连接特定的 DNS 后缀 . . . . . : 
    描述. . . . . : Realtek PCIe GBE Family Controller
    物理地址. . . . . : C0-3F-D5-F4-BA-29
    DHCP 已启用 . . . . . : 否
    自动配置已启用. . . . . : 是
    本地连接 IPv6 地址. . . . . : fe80::1977:3b29:856:d7ff%11<首选>
    IPv4 地址 . . . . . : 192.168.0.22<首选>
    子网掩码 . . . . . : 255.255.254.0
    默认网关. . . . . : 192.168.0.1
    DHCPv6 IAID . . . . . : 247480277
    DHCPv6 客户端 DUID . . . . . : 00-01-00-01-2D-7E-AD-67-C0-3F-D5-F4-BA-29

    DNS 服务器 . . . . . : 202.117.0.20
    . . . . . : 202.117.0.21
    TCP/IP 上的 NetBIOS . . . . . : 已禁用

隧道适配器 isatap.{554760F8-096E-4BA4-9606-1EBFAC1C35A9}:

    媒体状态 . . . . . : 媒体已断开
    连接特定的 DNS 后缀 . . . . . : 
    描述. . . . . : Microsoft ISATAP Adapter
    物理地址. . . . . : 00-00-00-00-00-00-E0
    DHCP 已启用 . . . . . : 否
    自动配置已启用. . . . . : 是
```

图 3

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？

即“本地连接”，其信息见下表：

字段	配置值
上网网卡描述	Realtek PCIe GBE Family Controller
IP 地址	192.168.0.22
子网掩码	255.255.254.0
默认网关	192.168.0.1
DNS 服务器	202.117.0.20/21

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（注意观察租约时间）？

【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。`

】

原来为手动设置地址。因此将其改为自动获取。依次将 IP 地址、DNS 服务器地址的获得方式设置为自动，得到的网卡配置信息见图 4、图 5。

可以看出与手动设置地址时的配置（参见图 3）相比，配置信息多了租约时间。这是根据 DHCP 协议生成的，IP 地址是有租约期限的，客户端必须提前续租 IP 地址，请求 DHCP 服务器更新租期。否则租约到期，就只能释放该 IP 地址，重新申请新的 IP 地址。下面给出 DHCP 协议的工作步骤：

- (1) DHCP 客户机启动时广播发送的源地址是 0.0.0.0，目标地址 255.255.255.255 的 DHCP Discover 报文来寻找 DHCP 服务器；
- (2) DHCP 服务器接收到来自客户机请求 IP 地址的信息时，在 IP 地址池中查找是否有合法的 IP 地址，如果有，DHCP 服务器将此 IP 地址做上标记，加入到 DHCP Offer 的消息中，然后广播一则 DHCP Offer 消息；
- (3) 客户端给服务器发送 DHCP request 报文广播请求使用这个 IP 地址；
- (4) 服务器发送 DHCP ACK 报文，并从可分配 IP 池中删除该 IP 地址。

```

C:\Users\Administrator>ipconfig /all

Windows IP 配置

   主机名 . . . . . : PC022
   主 DNS 后缀 . . . . . :
   节点类型 . . . . . : 混合
   IP 路由已启用 . . . . . : 否
   WINS 代理已启用 . . . . . : 否

以太网适配器 本地连接:

   连接特定的 DNS 后缀 . . . . . :
   描述. . . . . : Realtek PCIe GBE Family Controller
   物理地址. . . . . : C0-3F-D5-F4-BA-29
   DHCP 已启用 . . . . . : 是
   自动配置已启用 . . . . . : 是
   本地链接 IPv6 地址. . . . . : fe80::1977:3b29:856:d7ff%11<首选>
   IPv4 地址 . . . . . : 192.168.1.36<首选>
   子网掩码 . . . . . : 255.255.254.0
   获得租约的时间 . . . . . : 2024年3月10日 8:40
   租约过期的时间 . . . . . : 2024年3月10日 10:40
   默认网关 . . . . . : 192.168.0.1
   DHCP 服务器 . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . : 247480277
   DHCPv6 客户端 DUID . . . . . : 00-01-00-01-2D-7E-AD-67-C0-3F-D5-F4-BA-29

   DNS 服务器 . . . . . : 202.117.0.20
                           202.117.0.21
   TCP/IP 上的 NetBIOS . . . . . : 已禁用

隧道适配器 isatap.{554760F8-096E-4BA4-9606-1EBFAC1C35A9}:

   媒体状态 . . . . . : 媒体已断开
   连接特定的 DNS 后缀 . . . . . :
   描述. . . . . : Microsoft ISATAP Adapter
   物理地址. . . . . : 00-00-00-00-00-00-E0
   DHCP 已启用 . . . . . : 否
   自动配置已启用 . . . . . : 是

```

图 4

```

C:\Users\Administrator>ipconfig /all

Windows IP 配置

   主机名 . . . . . : PC022
   主 DNS 后缀 . . . . . :
   节点类型 . . . . . : 混合
   IP 路由已启用 . . . . . : 否
   WINS 代理已启用 . . . . . : 否

以太网适配器 本地连接:

   连接特定的 DNS 后缀 . . . . . :
   描述. . . . . : Realtek PCIe GBE Family Controller
   物理地址. . . . . : C0-3F-D5-F4-BA-29
   DHCP 已启用 . . . . . : 是
   自动配置已启用 . . . . . : 是
   本地链接 IPv6 地址. . . . . : fe80::1977:3b29:856:d7ff%11<首选>
   IPv4 地址 . . . . . : 192.168.1.36<首选>
   子网掩码 . . . . . : 255.255.254.0
   获得租约的时间 . . . . . : 2024年3月10日 8:40
   租约过期的时间 . . . . . : 2024年3月10日 10:40
   默认网关 . . . . . : 192.168.0.1
   DHCP 服务器 . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . : 247480277
   DHCPv6 客户端 DUID . . . . . : 00-01-00-01-2D-7E-AD-67-C0-3F-D5-F4-BA-29

   DNS 服务器 . . . . . : 202.117.0.20
                           1.2.4.8
   TCP/IP 上的 NetBIOS . . . . . : 已禁用

隧道适配器 isatap.{554760F8-096E-4BA4-9606-1EBFAC1C35A9}:

   媒体状态 . . . . . : 媒体已断开
   连接特定的 DNS 后缀 . . . . . :
   描述. . . . . : Microsoft ISATAP Adapter
   物理地址. . . . . : 00-00-00-00-00-00-E0
   DHCP 已启用 . . . . . : 否
   自动配置已启用 . . . . . : 是

```

图 5

特别地，注意到 DNS 服务器地址改为自动获取后，其 DNS 服务器的第二个 IP 地址发生了变化。

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】

默认路由见标记。使用以下命令行删除默认路由。

```
route delete 0.0.0.0
```

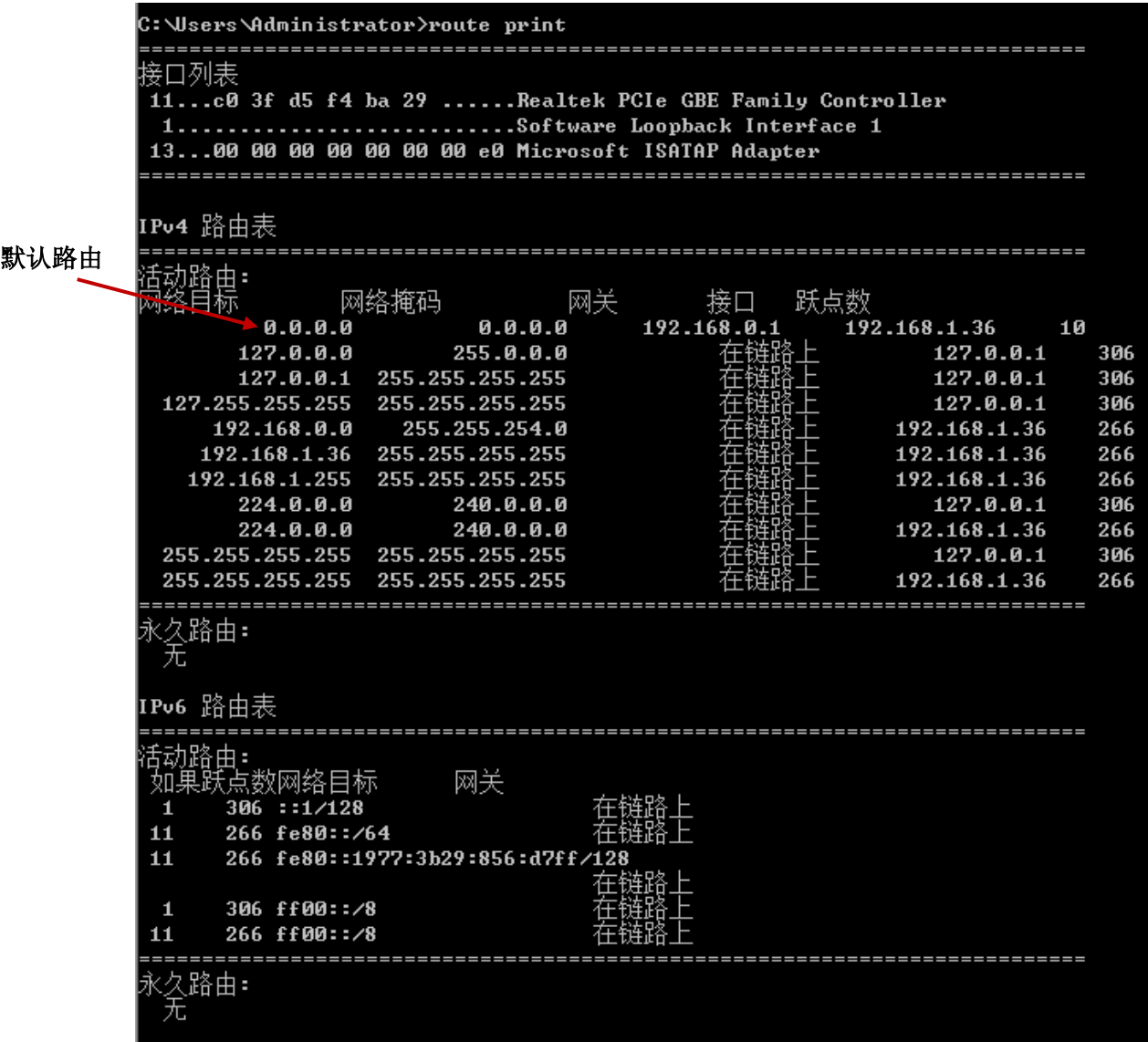


图 6

删除后无法上网。打印当前路由表和网络配置，发现路由表删除成功且默认网关配置已经没有了。具体参见图 7、图 8。

```

C:\Users\Administrator>route print
=====
接口列表
11...c0 3f d5 f4 ba 29 .....Realtek PCIe GBE Family Controller
1.....Software Loopback Interface 1
13...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
=====

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          306
127.0.0.1          255.255.255.255    在链路上          127.0.0.1          306
127.255.255.255    255.255.255.255    在链路上          127.0.0.1          306
192.168.0.0          255.255.254.0      在链路上          192.168.1.36       266
192.168.1.36        255.255.255.255    在链路上          192.168.1.36       266
192.168.1.255       255.255.255.255    在链路上          192.168.1.36       266
224.0.0.0           240.0.0.0          在链路上          127.0.0.1          306
224.0.0.0           240.0.0.0          在链路上          192.168.1.36       266
255.255.255.255     255.255.255.255    在链路上          127.0.0.1          306
255.255.255.255     255.255.255.255    在链路上          192.168.1.36       266
=====
永久路由:
无

IPv6 路由表
=====
活动路由:
如果跃点数网络目标          网关          接口          跃点数
1      306 ::1/128          在链路上          1
11     266 fe80::/64        在链路上          1
11     266 fe80::1977:3b29:856:d7ff/128 在链路上          1
1      306 ff00::/8         在链路上          1
11     266 ff00::/8         在链路上          1
=====
永久路由:
无

```

图 7

```

C:\Users\Administrator>ipconfig

Windows IP 配置

以太网适配器 本地连接:

    连接特定的 DNS 后缀 . . . . . :
    本地连接 IPv6 地址. . . . . : fe80::1977:3b29:856:d7ff%11
    IPv4 地址 . . . . . : 192.168.1.36
    子网掩码 . . . . . : 255.255.254.0
    默认网关 . . . . . :

隧道适配器 isatap.{554760F8-096E-4BA4-9606-1EBFAC1C35A9}:

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

```

图 8

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?

使用如下命令, 得路由表见图 9。

route add 0.0.0.0 MASK 0.0.0.0 192.168.0.1

```
C:\Users\Administrator>route ADD 0.0.0.0 MASK 0.0.0.0 192.168.0.1
操作完成!

C:\Users\Administrator>route print
=====
接口列表
11...c0 3f d5 f4 ba 29 .....Realtek PCIe GBE Family Controller
1.....Software Loopback Interface 1
13...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
=====

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            192.168.0.1    192.168.1.36    11
127.0.0.0          255.0.0.0          在链路上      127.0.0.1       306
127.0.0.1          255.255.255.255    在链路上      127.0.0.1       306
127.255.255.255    255.255.255.255    在链路上      127.0.0.1       306
192.168.0.0        255.255.254.0      在链路上      192.168.1.36    266
192.168.1.36       255.255.255.255    在链路上      192.168.1.36    266
192.168.1.255      255.255.255.255    在链路上      192.168.1.36    266
224.0.0.0          240.0.0.0          在链路上      127.0.0.1       306
224.0.0.0          240.0.0.0          在链路上      192.168.1.36    266
255.255.255.255    255.255.255.255    在链路上      127.0.0.1       306
255.255.255.255    255.255.255.255    在链路上      192.168.1.36    266
=====
永久路由:
无

IPv6 路由表
=====
活动路由:
如果跃点数网络目标          网关          在链路上
1      306 ::1/128                  在链路上
11     266 fe80::/64              在链路上
11     266 fe80::1977:3b29:856:d7ff/128
在链路上
1      306 ff00::/8                在链路上
11     266 ff00::/8                在链路上
=====
永久路由:
无
```

图 9

此时网络畅通。

使用如下命令, 得路由表见图 10。

route add -p 0.0.0.0 MASK 0.0.0.0 192.168.0.1

```

C:\Users\Administrator>route add -p 0.0.0.0 MASK 0.0.0.0 192.168.0.1
操作完成!

C:\Users\Administrator>route print
=====
接口列表
11...c0 3f d5 f4 ba 29 .....Realtek PCIe GBE Family Controller
1.....Software Loopback Interface 1
13...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
=====

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        192.168.0.1  192.168.1.36  11
127.0.0.0      255.0.0.0      在链路上      127.0.0.1  306
127.0.0.1      255.255.255.255  在链路上      127.0.0.1  306
127.255.255.255 255.255.255.255 在链路上      127.0.0.1  306
192.168.0.0     255.255.254.0   在链路上      192.168.1.36  266
192.168.1.36    255.255.255.255 在链路上      192.168.1.36  266
192.168.1.255   255.255.255.255 在链路上      192.168.1.36  266
224.0.0.0       240.0.0.0       在链路上      127.0.0.1  306
224.0.0.0       240.0.0.0       在链路上      192.168.1.36  266
255.255.255.255 255.255.255.255 在链路上      127.0.0.1  306
255.255.255.255 255.255.255.255 在链路上      192.168.1.36  266
=====
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    192.168.0.1    1
=====

IPv6 路由表
=====
活动路由:
如果跃点数网络目标      网关      在链路上
1  306 ::1/128              在链路上
11 266 fe80:::/64           在链路上
11 266 fe80::1977:3b29:856:d7ff/128 在链路上
1  306 ff00::/8            在链路上
11 266 ff00::/8            在链路上
=====
永久路由:
无

```

图 10

可以发现 route add 是为路由表增加活动路由，而 route add -p 是为路由表添加永久路由。

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。

清除 DNS 缓存并 ping www.xjtu.edu.cn 见图 11，查看到的 DNS 缓存见图 12。


```

C:\Users\Administrator>ipconfig /flushdns

Windows IP 配置

已成功刷新 DNS 解析缓存。

C:\Users\Administrator>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=64
来自 202.117.1.13 的回复: 字节=32 时间<1ms TTL=64
来自 202.117.1.13 的回复: 字节=32 时间<1ms TTL=64
来自 202.117.1.13 的回复: 字节=32 时间<1ms TTL=64

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 = 0ms, 最长 = 0ms, 平均 = 0ms

```

图 11

```

C:\Users\Administrator>ipconfig /displaydns

Windows IP 配置

www.xjtu.edu.cn
-----
记录名称. . . . . : www.xjtu.edu.cn
记录类型. . . . . : 1
生存时间. . . . . : 292
数据长度. . . . . : 4
部分. . . . . : 答案
A (主机)记录 . . . . : 202.117.1.13

记录名称. . . . . : ns2.xjtu.edu.cn
记录类型. . . . . : 1
生存时间. . . . . : 292
数据长度. . . . . : 4
部分. . . . . : 其他
A (主机)记录 . . . . : 202.117.0.21

记录名称. . . . . : dec3000.xjtu.edu.cn
记录类型. . . . . : 1
生存时间. . . . . : 292
数据长度. . . . . : 4
部分. . . . . : 其他
A (主机)记录 . . . . : 202.117.0.20

```

图 12

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】

如果直接按上述步骤操作，ping 网址依然会成功，这可能与之前将 DNS 服务器地址设置为自动获取有关。将网卡禁用再启动后可以发现 DNS 修改有效。命令如下：

```
netsh interface set interface "本地连接" admin=disable  
  
netsh interface set interface "本地连接" admin=enable
```

把网卡的 DNS 服务器地址修改为无效 DNS 地址。ping github.com 见图 13，发现 ping 不通。本地 DNS 缓存记录见图 14。出现图示结果是因为本地 DNS 缓存已经被删除，而 DNS 服务器地址无效，本机无法进行 DNS 查询。

```
C:\Users\Administrator>ping github.com  
Ping 请求找不到主机 github.com。请检查该名称，然后重试。
```

图 13

```
C:\Users\Administrator>ipconfig /displaydns  
  
Windows IP 配置
```

图 14

使用以下命令将 DNS 服务器设置为正确的地址，发现可以 ping 通，见图 15。

```
netsh interface ip set dns name="本地连接" source=static  
  
add=8.8.8.8
```

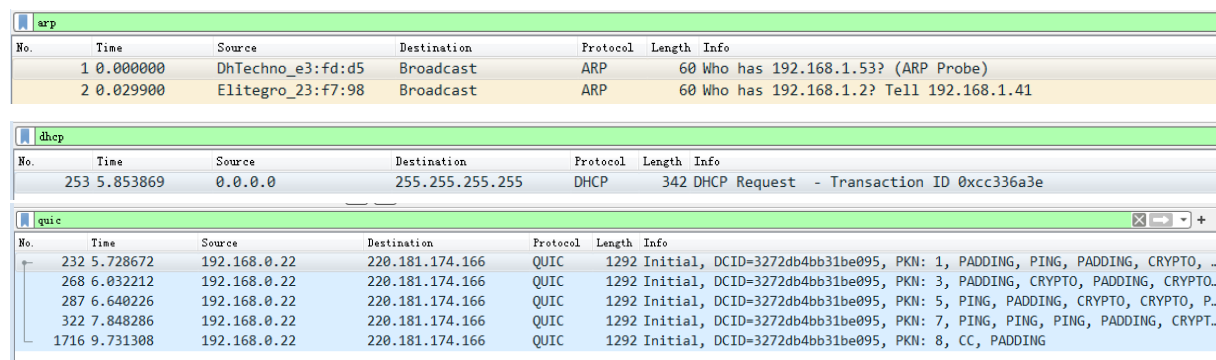
```
C:\Users\Administrator>ping github.com  
  
正在 Ping github.com [20.205.243.166] 具有 32 字节的数据:  
来自 20.205.243.166 的回复: 字节=32 时间<1ms TTL=64  
来自 20.205.243.166 的回复: 字节=32 时间<1ms TTL=64  
来自 20.205.243.166 的回复: 字节=32 时间<1ms TTL=64  
来自 20.205.243.166 的回复: 字节=32 时间<1ms TTL=64  
  
20.205.243.166 的 Ping 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
```

图 15

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。

协议名	描述项	配置值
ARP	协议功能	IP 地址对应 MAC 地址解析。
	源地址-目的地址	Elitegro_23:f7:98 - Broadcast
	请求/应答信息	Who has 192.168.1.2? Tell 192.168.1.41
DHCP	协议功能	动态管理、分配 IP 地址。
	源地址-目的地址	0.0.0.0 – 255.255.255.255
	请求/应答信息	DHCP Request – Transaction ID 0xcc336a3e
QUIC	协议功能	提供快捷、稳定、高效的网络通信。
	源地址-目的地址	192.168.0.22 – 220.181.174.166
	请求/应答信息	Initial,DCID=3272db4bb31be095,PKN:1,PADDING, PING, PADDING, CRYPTO, PING, PADDING, CRYPTO



The image shows three screenshots of Wireshark packet captures. The first screenshot is for the ARP protocol, showing two packets: packet 1 (0.000000) from DhTechno_e3:fd:d5 to Broadcast, and packet 2 (0.029900) from Elitegro_23:f7:98 to Broadcast. The second screenshot is for the DHCP protocol, showing packet 253 (5.853869) from 0.0.0.0 to 255.255.255.255, which is a DHCP Request with Transaction ID 0xcc336a3e. The third screenshot is for the QUIC protocol, showing a sequence of packets (232, 268, 287, 322, 1716) from 192.168.0.22 to 220.181.174.166, including Initial, PING, and CRYPTO messages.

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`】

协议名	描述项	配置值
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	192.168.0.22 – 20.205.243.166
	请求/应答信息	6254→80 [SYN]Seq=0Win=8192Len=0 MSS=1460 WS=256 SACK_PERM
HTTP	协议功能	从 WWW 服务器传输超文本到本地浏览器。
	源地址-目的地址	192.168.0.22 – 20.205.243.166
	请求/应答信息	GET / HTTP /1.1
TLS	协议功能	为互联网通信提供私密性和数据安全性。
	源地址-目的地址	192.168.0.22 – 20.205.243.166
	请求/应答信息	Client Hello

ip.addr == 20.205.243.166 && tcp						
No.	Time	Source	Destination	Protocol	Length	Info
189	9.999686	192.168.0.22	20.205.243.166	TCP	66	62541 → 80 [SYN] Seq=0 Win=8192 Len=0
190	10.122918	20.205.243.166	192.168.0.22	TCP	66	80 → 62541 [SYN, ACK] Seq=0 Ack=1 Win=65535
191	10.122969	192.168.0.22	20.205.243.166	TCP	54	62541 → 80 [ACK] Seq=1 Ack=1 Win=65535
192	10.123089	192.168.0.22	20.205.243.166	HTTP	346	GET / HTTP/1.1
195	10.247410	20.205.243.166	192.168.0.22	HTTP	138	HTTP/1.1 301 Moved Permanently
196	10.247447	192.168.0.22	20.205.243.166	TCP	54	62541 → 80 [ACK] Seq=293 Ack=85 Win=65535
197	10.277300	192.168.0.22	20.205.243.166	TCP	66	62542 → 443 [SYN] Seq=0 Win=8192 Len=0

ip.addr == 20.205.243.166 && http						
No.	Time	Source	Destination	Protocol	Length	Info
192	10.123089	192.168.0.22	20.205.243.166	HTTP	346	GET / HTTP/1.1
195	10.247410	20.205.243.166	192.168.0.22	HTTP	138	HTTP/1.1 301 Moved Permanently

ip.addr == 20.205.243.166 && tls						
No.	Time	Source	Destination	Protocol	Length	Info
201	10.397379	192.168.0.22	20.205.243.166	TLSv1.2	206	Client Hello
203	10.516300	20.205.243.166	192.168.0.22	TLSv1.2	1454	Server Hello
205	10.516300	20.205.243.166	192.168.0.22	TLSv1.2	621	Certificate, Server Key Exchange, S
207	10.531418	192.168.0.22	20.205.243.166	TLSv1.2	180	Client Key Exchange, Change Cipher
208	10.647922	20.205.243.166	192.168.0.22	TLSv1.2	105	Change Cipher Spec, Encrypted Hands
210	10.667615	192.168.0.22	20.205.243.166	TLSv1.2	375	Application Data

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。

从该步骤开始实验用机改为使用本人机器。

本机捕获信息

描述项	值
QQ/微信服务器地址	49.7.249.60
本机 IP 地址	192.168.31.233
本机自测公网地址	1.85.33.85
通信好友的 IP 地址	113.135.242.23
通信协议（Protocol）	UDP
通信源端口-目的端口	61014-18006

好友端捕获信息

描述项	值
QQ/微信服务器地址	43.141.131.38
本机 IP 地址	192.168.154.2
本机自测公网地址	113.135.242.23
通信好友的 IP 地址	1.85.33.85
通信协议 (Protocol)	UDP
通信源端口-目的端口	58576-8000

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) 本机 IP 地址、子网掩码、网关 IP 地址 DNS 服务器地址设置。可以通过手动设置也可以自动设置。
- (2) 查询域名 IP，若本地没有缓存则需要向域名服务器查询。
- (3) 使用 HTTP 协议等应用层协议传输相关请求、应答。
- (4) 使用 TCP、QUIC 等传输层协议传输数据包。
- (5) 网络层协议支持。
- (6) 使用 ARP 等链路层协议使数据前往正确的物理接口。

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。】

抓包，登录 QQ，与好友视频通信，登出 QQ，得到下面的结果。注意到所有 OICQ 的 data 段值都是登入的 QQ 账号。

首先出现若干个 Command 信息为 Request KEY 的 OICQ 报文，表示请求 KEY，是登录认证过程。

```

Destination Port: 8000
Length: 47
Checksum: 0x0b16 [unverified]
[Checksum Status: Unverified]
[Stream index: 9]
> [Timestamps]
UDP payload (39 bytes)
▼ OICQ - IM software, popular in China
  Flag: Oicq packet (0x02)
  Version: 0x3c3d
  Command: Request KEY (29)
  Sequence: 25949
  Data(OICQ Number,if sender is client): 2425361434
  > Data: \002

```

接着 OICQ 报文出现 Command 为 log out、Get friend online、Group name operation、Heart Message 等的报文，这是登录后做的一系列操作，包括查询好友在线状态等。

约 6s 后，出现大量 Command 为 Receive message 的 OICQ 报文，这与视频通话待接的时间吻合。

No.	Time	Source	Destination	Protocol	Length	Info
1147	6.428209	49.7.249.60	192.168.31.233	OICQ	209	OICQ Protocol
1148	6.428433	49.7.249.60	192.168.31.233	OICQ	209	OICQ Protocol
1149	6.428433	49.7.249.60	192.168.31.233	OICQ	209	OICQ Protocol
1150	6.428433	49.7.249.60	192.168.31.233	OICQ	177	OICQ Protocol
1151	6.428433	49.7.249.60	192.168.31.233	OICQ	225	OICQ Protocol
1152	6.428527	192.168.31.233	49.7.249.60	OICQ	97	OICQ Protocol
1153	6.428644	192.168.31.233	49.7.249.60	OICQ	97	OICQ Protocol
1154	6.428750	192.168.31.233	49.7.249.60	OICQ	97	OICQ Protocol
1155	6.428846	192.168.31.233	49.7.249.60	OICQ	97	OICQ Protocol
1156	6.428951	192.168.31.233	49.7.249.60	OICQ	97	OICQ Protocol
1157	6.429888	49.7.249.60	192.168.31.233	OICQ	209	OICQ Protocol
1158	6.429888	49.7.249.60	192.168.31.233	OICQ	209	OICQ Protocol
1159	6.429888	49.7.249.60	192.168.31.233	OICQ	177	OICQ Protocol
1160	6.429888	49.7.249.60	192.168.31.233	OICQ	193	OICQ Protocol
1161	6.430058	192.168.31.233	49.7.249.60	OICQ	97	OICQ Protocol
1162	6.430167	192.168.31.233	49.7.249.60	OICQ	97	OICQ Protocol
1163	6.430261	192.168.31.233	49.7.249.60	OICQ	97	OICQ Protocol
1164	6.430360	192.168.31.233	49.7.249.60	OICQ	97	OICQ Protocol

```

> Ethernet II, Src: BeijingX_7d:cf:bd (d4:35:38:7d:cf:bd)
> Internet Protocol Version 4, Src: 49.7.249.60, Dst: 192.168.31.233
▼ User Datagram Protocol, Src Port: 8000, Dst Port: 4006
  Source Port: 8000
  Destination Port: 4006
  Length: 143
  Checksum: 0x2ec7 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 9]
  > [Timestamps]
  UDP payload (135 bytes)
  ▼ OICQ - IM software, popular in China
    Flag: Oicq packet (0x02)
    Version: 0x3c3d
    Command: Receive message (23)
    Sequence: 17784
    Data(OICQ Number,if sender is client): 2425361434
    > Data:

```

接听后，出现大量 UDP 报文，持续约 10s，这与本人维持视频通话的时间一致。

1924	17.797171	120.226.165.199	192.168.31.233	UDP	118 18006 → 61014	Len=76
1925	17.808539	120.226.165.199	192.168.31.233	UDP	120 18006 → 61014	Len=78
1926	17.808539	120.226.165.199	192.168.31.233	UDP	128 18006 → 61014	Len=86
1927	17.819348	120.226.165.199	192.168.31.233	UDP	130 18006 → 61014	Len=88
1928	17.872735	120.226.165.199	192.168.31.233	UDP	146 18006 → 61014	Len=104
1929	17.872735	120.226.165.199	192.168.31.233	UDP	129 18006 → 61014	Len=87
1930	17.881295	192.168.31.233	120.226.165.199	UDP	1178 61014 → 18006	Len=1136
1931	17.881443	120.226.165.199	192.168.31.233	UDP	135 18006 → 61014	Len=93
1932	17.881565	192.168.31.233	120.226.165.199	UDP	1178 61014 → 18006	Len=1136
1933	17.881879	192.168.31.233	120.226.165.199	UDP	1178 61014 → 18006	Len=1136
1934	17.900606	120.226.165.199	192.168.31.233	UDP	131 18006 → 61014	Len=89
1935	17.954303	120.226.165.199	192.168.31.233	UDP	129 18006 → 61014	Len=87
1936	17.954303	120.226.165.199	192.168.31.233	UDP	133 18006 → 61014	Len=91
1937	17.954303	120.226.165.199	192.168.31.233	UDP	121 18006 → 61014	Len=79
1938	17.976816	192.168.31.233	120.226.165.199	UDP	207 61014 → 18006	Len=165
1939	17.978280	120.226.165.199	192.168.31.233	UDP	121 18006 → 61014	Len=79
1940	17.982282	192.168.31.233	120.226.165.199	UDP	87 61014 → 18006	Len=45
1941	18.002690	192.168.31.233	120.226.165.199	UDP	87 61014 → 18006	Len=45

最后接受到的两个 OICQ 报文 Command 信息依次为 log out 和 Request login。这是登出阶段。

除 OICQ 协议外，本机与腾讯服务器(49.7.249.60 以及 120.226.165.199)间还用到了 UDP 协议以进行数据传输。特别地，可以发现，本机与好友(113.135.242.23)只进行了少量的直接访问（约每 0.5s 向好友发送一个 UDP 报文），大量的数据通过腾讯服务器后再发至好友(向好友发送信息的服务器 IP 与本机联系的服务器亦 IP 不同)。

1875	17.166907	192.168.31.233	113.135.242.23	UDP	114 52998 → 46593	Len=72
1948	18.056857	192.168.31.233	113.135.242.23	UDP	114 52998 → 46593	Len=72
2022	18.558590	192.168.31.233	113.135.242.23	UDP	114 52998 → 46593	Len=72
2101	19.059292	192.168.31.233	113.135.242.23	UDP	114 52998 → 46593	Len=72
2227	19.559666	192.168.31.233	113.135.242.23	UDP	114 52998 → 46593	Len=72
2413	20.059250	192.168.31.233	113.135.242.23	UDP	114 52998 → 46593	Len=72
2546	20.562954	192.168.31.233	113.135.242.23	UDP	114 52998 → 46593	Len=72
2640	21.062804	192.168.31.233	113.135.242.23	UDP	114 52998 → 46593	Len=72
2779	21.565653	192.168.31.233	113.135.242.23	UDP	114 52998 → 46593	Len=72
2863	22.067005	192.168.31.233	113.135.242.23	UDP	114 52998 → 46593	Len=72
2954	22.568975	192.168.31.233	113.135.242.23	UDP	114 52998 → 46593	Len=72
3084	23.068848	192.168.31.233	113.135.242.23	UDP	114 52998 → 46593	Len=72
3212	23.569649	192.168.31.233	113.135.242.23	UDP	114 52998 → 46593	Len=72
3343	24.071056	192.168.31.233	113.135.242.23	UDP	114 52998 → 46593	Len=72
3480	24.572810	192.168.31.233	113.135.242.23	UDP	114 52998 → 46593	Len=72
3601	25.074721	192.168.31.233	113.135.242.23	UDP	114 52998 → 46593	Len=72
3748	25.575746	192.168.31.233	113.135.242.23	UDP	114 52998 → 46593	Len=72

总结及心得体会

通过本次实验，我学会了的常用网络命令以及网络分析软件 Wireshark 的使用方法，提高了我对网卡、网关、路由器、路由表等网络概念的理解，提高了我对网络协议的认识。试验过程中，我将原理课上学到的知识运用到实际中，特别是对 QQ 通信的分析，使我理解了网络是怎样建立、怎样利用协议进行信息交流的，这极大地锻炼了我的能力。