实验一 常用网络命令及工具实验报告

组号： 5-6

姓名： 施炎江 学号： 2186113847 班级： 计算机 82

一、 实验名称

常用网络命令及工具练习。

二、 实验目的

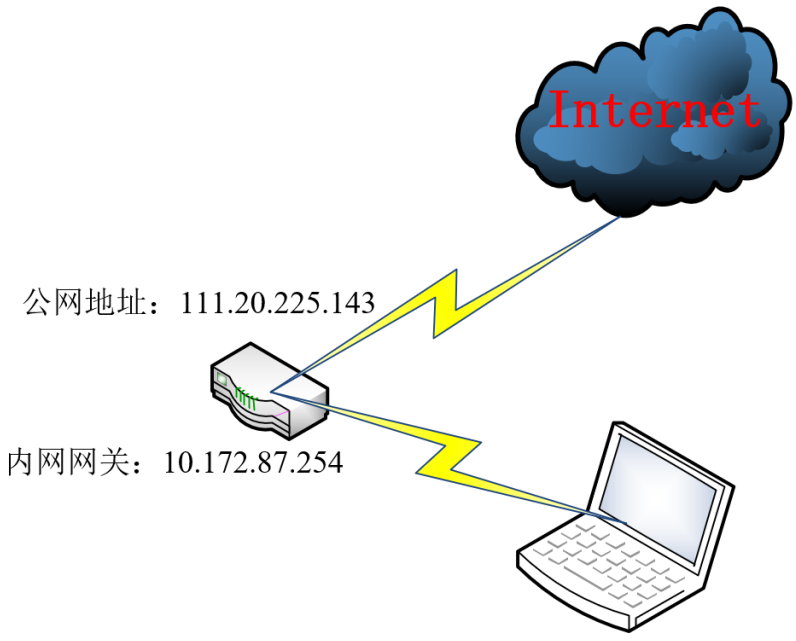
掌握常用网络命令（ping、tracert、ipconfig、route 等）的使用，掌握常用网络工具（如 Wireshark，putty 等）的使用。

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，实验结束后标注出内网、公网地址。



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】

本机共有 9 个网卡，其中有 3 个物理网卡，分别是：以太网适配器 以太网（描述为 Intel(R) Ethernet Connection (4) I219-V）；无线局域网适配器 WLAN 2（描述为 Intel(R) Dual Band Wireless-AC 8265 #2）；以太网适配器 蓝牙网络连接（描述为 Bluetooth Device (Personal Area Network)），其余的均为虚拟网卡。

```
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. . . . . . . . . . . . . . . : Intel(R) Ethernet Connection (4) I219-V
   物理地址. . . . . . . . . . . . . : 8C-16-45-60-0B-98
   DHCP 已启用 . . . . . . . . . . . : 是
   自动配置已启用. . . . . . . . . . : 是

以太网适配器 VirtualBox Host-Only Network:

   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : VirtualBox Host-Only Ethernet Adapter
   物理地址. . . . . . . . . . . . . : 0A-00-27-00-00-05
   DHCP 已启用 . . . . . . . . . . . : 否
   自动配置已启用. . . . . . . . . . : 是
   本地链接 IPv6 地址. . . . . . . . : fe80::dc09:3004:bb95:30cc%5(首选)
   IPv4 地址 . . . . . . . . . . . . : 192.168.56.1(首选)
   子网掩码  . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 101318695
   DHCPv6 客户端 DUID  . . . . . . . : 00-01-00-01-23-2A-93-D7-8C-16-45-60-0B-98
   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

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. . . . . . . . . . . . . : 0C-54-15-54-99-45
   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* 11:

   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. . . . . . . . . . . . . : 0E-54-15-54-99-44
   DHCP 已启用 . . . . . . . . . . . : 是
   自动配置已启用. . . . . . . . . . : 是

以太网适配器 以太网 2:

   媒体状态  . . . . . . . . . . . . : 媒体已断开连接
   连接特定的 DNS 后缀 . . . . . . . :
   描述. . . . . . . . . . . . . . . : Netease UU TAP-Win32 Adapter V9.21
   物理地址. . . . . . . . . . . . . : 00-FF-18-D2-4A-7B
   DHCP 已启用 . . . . . . . . . . . : 是
   自动配置已启用. . . . . . . . . . : 是
```

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？

下面是本机访问互联网时使用的网卡信息：

```
无线局域网适配器 WLAN 2:

   连接特定的 DNS 后缀 . . . . . . . : xjtu.edu.cn
   描述. . . . . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 8265 #2
   物理地址. . . . . . . . . . . . . : 0C-54-15-54-99-44
   DHCP 已启用 . . . . . . . . . . . : 是
   自动配置已启用. . . . . . . . . . : 是
   本地链接 IPv6 地址. . . . . . . . : fe80::f087:5440:32ca:3635%10(首选)
   IPv4 地址 . . . . . . . . . . . . : 10.172.85.152(首选)
   子网掩码 . . . . . . . . . . . . : 255.255.248.0
   获得租约的时间  . . . . . . . . . : 2021年3月12日 14:55:08
   租约过期的时间  . . . . . . . . . : 2021年3月12日 15:55:08
   默认网关. . . . . . . . . . . . . : 10.172.87.254
   DHCP 服务器 . . . . . . . . . . . : 10.6.18.14
   DHCPv6 IAID . . . . . . . . . . . : 437015573
   DHCPv6 客户端 DUID  . . . . . . . : 00-01-00-01-23-2A-93-D7-8C-16-45-60-0B-98
   DNS 服务器  . . . . . . . . . . . : 211.137.130.3
                                       211.137.130.19
   TCPIP 上的 NetBIOS  . . . . . . . : 已启用
```

字段	配置值
上网网卡描述	Intel(R) Dual Band Wireless-AC 8265 #2
IP 地址	10.172.85.152
子网掩码	255.255.248.0
默认网关	10.172.87.254
DNS 服务器	211.137.130.3 211.137.130.19

步骤 2：用命令行修改本机 IP 地址和 DNS 服务器地址为自动获取方式，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：手动设置地址命令：netsh interface ip set address name="WLAN 2" static 10.172.85.152 255.255.255.0 10.172.87.254，netsh interface ip set dns name="WLAN 2" source=static add=211.137.130.3。自动获取地址命令：netsh interface ip set address name="WLAN 2" source=dhcp，netsh interface ip set dns name="WLAN 2" source=dhcp】

手动设置 ip 地址、子网掩码、默认网关：

```
C:\WINDOWS\system32>netsh interface ip set address name="WLAN 2" static 10.172.85.152 255.255.248.0 10.172.87.254
```

手动设置 DNS 服务器地址：

```
C:\WINDOWS\system32>netsh interface ip set dns name="WLAN 2" source=static add=211.137.130.3
```

手动设置后用 ipconfig 查看网卡信息。通过可以发现，手动设置时“连接特定的 DNS 后缀”这行的值为空，“DHCP 已启用”这行的值为“否”；而相应的，当自动设置时这两行的值分别为“xjtu.edu.cn”和“是”。

```
无线局域网适配器 WLAN 2:

   连接特定的 DNS 后缀 . . . . . :
   描述. . . . . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 8265 #2
   物理地址. . . . . . . . . . . . . : 0C-54-15-54-99-44
   DHCP 已启用 . . . . . . . . . . . : 否
   自动配置已启用. . . . . . . . . . : 是
   本地链接 IPv6 地址. . . . . . . . : fe80::f087:5440:32ca:3635%10(首选)
   IPv4 地址 . . . . . . . . . . . . : 10.172.85.152(试验)
   子网掩码 . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . : 10.172.87.254
   DHCPv6 IAID . . . . . . . . . . . : 437015573
   DHCPv6 客户端 DUID . . . . . . . . : 00-01-00-01-23-2A-93-D7-8C-16-45-60-0B-98
   DNS 服务器 . . . . . . . . . . . : 211.137.130.3
   TCPIP 上的 NetBIOS . . . . . . . . : 已启用
```

恢复为自动获取地址：

```
C:\WINDOWS\system32>netsh interface ip set address name="WLAN 2" source=dhcp

C:\WINDOWS\system32>netsh interface ip set dns name="WLAN 2" source=dhcp
```

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。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，红框标注的为默认路由：

```
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    10.172.87.254    10.172.85.152     35
       10.172.80.0    255.255.248.0         在链路上     10.172.85.152    291
    10.172.85.152  255.255.255.255         在链路上     10.172.85.152    291
    10.172.87.255  255.255.255.255         在链路上     10.172.85.152    291
        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
    192.168.56.0    255.255.255.0         在链路上      192.168.56.1    281
    192.168.56.1  255.255.255.255         在链路上      192.168.56.1    281
  192.168.56.255  255.255.255.255         在链路上      192.168.56.1    281
   192.168.110.0    255.255.255.0         在链路上     192.168.110.1    291
   192.168.110.1  255.255.255.255         在链路上     192.168.110.1    291
 192.168.110.255  255.255.255.255         在链路上     192.168.110.1    291
   192.168.190.0    255.255.255.0         在链路上     192.168.190.1    291
   192.168.190.1  255.255.255.255         在链路上     192.168.190.1    291
 192.168.190.255  255.255.255.255         在链路上     192.168.190.1    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      192.168.56.1    281
        224.0.0.0        240.0.0.0         在链路上     192.168.190.1    291
        224.0.0.0        240.0.0.0         在链路上     192.168.110.1    291
        224.0.0.0        240.0.0.0         在链路上     10.172.85.152    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      192.168.56.1    281
  255.255.255.255  255.255.255.255         在链路上     192.168.190.1    291
  255.255.255.255  255.255.255.255         在链路上     192.168.110.1    291
  255.255.255.255  255.255.255.255         在链路上     10.172.85.152    291
===========================================================================
```

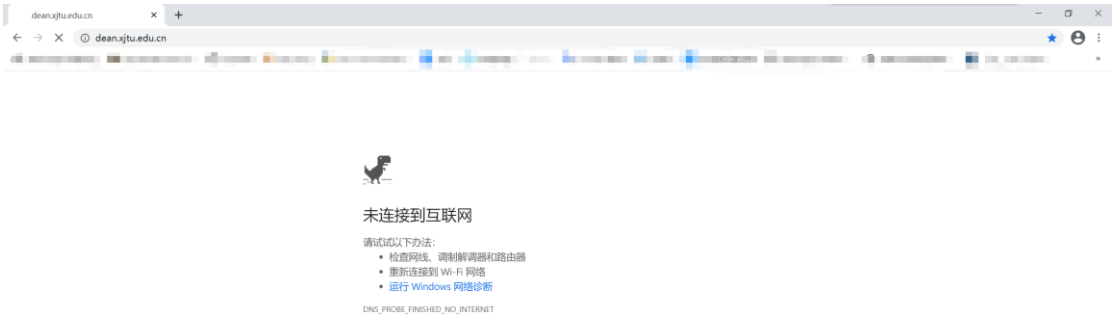
删除默认路由：

```
C:\WINDOWS\system32>route delete 0.0.0.0 mask 0.0.0.0 10.172.87.254
 操作完成!
```

再次查看路由信息，可以看出默认路由已删除：

```
IPv4 路由表
===========================================================================
活动路由:
网络目标        网络掩码          网关       接口   跃点数
      10.172.80.0    255.255.248.0         在链路上     10.172.85.152    296
    10.172.85.152  255.255.255.255         在链路上     10.172.85.152    296
    10.172.87.255  255.255.255.255         在链路上     10.172.85.152    296
        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
    192.168.56.0    255.255.255.0         在链路上      192.168.56.1    281
    192.168.56.1  255.255.255.255         在链路上      192.168.56.1    281
  192.168.56.255  255.255.255.255         在链路上      192.168.56.1    281
   192.168.110.0    255.255.255.0         在链路上     192.168.110.1    291
   192.168.110.1  255.255.255.255         在链路上     192.168.110.1    291
 192.168.110.255  255.255.255.255         在链路上     192.168.110.1    291
   192.168.190.0    255.255.255.0         在链路上     192.168.190.1    291
   192.168.190.1  255.255.255.255         在链路上     192.168.190.1    291
 192.168.190.255  255.255.255.255         在链路上     192.168.190.1    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      192.168.56.1    281
        224.0.0.0        240.0.0.0         在链路上     192.168.190.1    291
        224.0.0.0        240.0.0.0         在链路上     192.168.110.1    291
        224.0.0.0        240.0.0.0         在链路上     10.172.85.152    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      192.168.56.1    281
  255.255.255.255  255.255.255.255         在链路上     192.168.190.1    291
  255.255.255.255  255.255.255.255         在链路上     192.168.110.1    291
  255.255.255.255  255.255.255.255         在链路上     10.172.85.152    296
===========================================================================
```

不能访问互联网，分析原因是因为我想访问的网站并不在当前路由表中，因此它本应该通过默认路由转发数据包。但是上一步我们把默认路由删除了，因此主机现在并不知道应该把数据包转发到哪里，故无法建立通信，导致无法上网。



查看网卡配置，可以发现默认网关这行的值为空：

```
无线局域网适配器 WLAN 2:

   连接特定的 DNS 后缀 . . . . . : xjtu.edu.cn
   描述. . . . . : Intel(R) Dual Band Wireless-AC 8265 #2
   物理地址. . . . . : 0C-54-15-54-99-44
   DHCP 已启用 . . . . . : 是
   自动配置已启用. . . . . : 是
   本地链接 IPv6 地址. . . . . : fe80::f087:5440:32ca:3635%10(首选)
   IPv4 地址 . . . . . : 10.172.85.152(首选)
   子网掩码 . . . . . : 255.255.248.0
   获得租约的时间 . . . . . : 2021年3月13日 19:56:44
   租约过期的时间 . . . . . : 2021年3月13日 20:56:44
   默认网关. . . . . :
   DHCP 服务器 . . . . . : 10.0.10.14
   DHCPv6 IAID . . . . . : 437015573
   DHCPv6 客户端 DUID . . . . . : 00-01-00-01-23-2A-93-D7-8C-16-45-60-0B-98
   DNS 服务器 . . . . . : 211.137.130.3
                          211.137.130.19
   TCPIP 上的 NetBIOS . . . . . : 已启用
```

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 route add：

```
C:\WINDOWS\system32>route add 0.0.0.0 mask 0.0.0.0 10.172.87.254 metric 35
 操作完成!
```

查看路由表，发现默认路由添加在了 ipv4 路由表中：

```
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    10.172.87.254    10.172.85.152     36
       10.172.80.0    255.255.248.0         在链路上     10.172.85.152    291
    10.172.85.152  255.255.255.255         在链路上     10.172.85.152    291
    10.172.87.255  255.255.255.255         在链路上     10.172.85.152    291
        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
    192.168.56.0    255.255.255.0         在链路上      192.168.56.1    281
    192.168.56.1  255.255.255.255         在链路上      192.168.56.1    281
  192.168.56.255  255.255.255.255         在链路上      192.168.56.1    281
   192.168.110.0    255.255.255.0         在链路上     192.168.110.1    291
   192.168.110.1  255.255.255.255         在链路上     192.168.110.1    291
 192.168.110.255  255.255.255.255         在链路上     192.168.110.1    291
   192.168.190.0    255.255.255.0         在链路上     192.168.190.1    291
   192.168.190.1  255.255.255.255         在链路上     192.168.190.1    291
 192.168.190.255  255.255.255.255         在链路上     192.168.190.1    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      192.168.56.1    281
        224.0.0.0        240.0.0.0         在链路上     192.168.110.1    291
        224.0.0.0        240.0.0.0         在链路上     192.168.190.1    291
        224.0.0.0        240.0.0.0         在链路上     10.172.85.152    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      192.168.56.1    281
  255.255.255.255  255.255.255.255         在链路上     192.168.110.1    291
  255.255.255.255  255.255.255.255         在链路上     192.168.190.1    291
  255.255.255.255  255.255.255.255         在链路上     10.172.85.152    291
===========================================================================
```

使用 route –p add：

```
C:\WINDOWS\system32>route -p add 0.0.0.0 mask 0.0.0.0 10.172.87.254 metric 35
 操作完成!
```

默认路由添加在了永久路由中

```
===========================================================================
永久路由:
  网络地址          网络掩码  网关地址   跃点数
      172.17.0.0      255.255.0.0         10.0.2.15        1
        0.0.0.0          0.0.0.0     10.172.87.254       35
===========================================================================
```

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。

```
C:\Users\Think>ipconfig /flushdns

Windows IP 配置

已成功刷新 DNS 解析缓存。

C:\Users\Think>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=5ms TTL=59
来自 202.117.1.13 的回复: 字节=32 时间=6ms TTL=59
来自 202.117.1.13 的回复: 字节=32 时间=5ms TTL=59
来自 202.117.1.13 的回复: 字节=32 时间=5ms TTL=59

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 = 5ms，最长 = 6ms，平均 = 5ms

C:\Users\Think>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. . . . . : 3543
    数据长度. . . . . : 4
    部分. . . . . : 答案
    A (主机)记录 . . . . : 202.117.1.13
```

域名：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（如 3.3.3.3），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=3.3.3.3】

```
C:\WINDOWS\system32>netsh interface ip set dns name="WLAN 2" source=static add=3.3.3.3

配置的 DNS 服务器不正确或不存在。


C:\WINDOWS\system32>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=5ms TTL=59
来自 202.117.1.13 的回复: 字节=32 时间=5ms TTL=59
来自 202.117.1.13 的回复: 字节=32 时间=5ms TTL=59
来自 202.117.1.13 的回复: 字节=32 时间=5ms TTL=59

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 = 5ms, 最长 = 5ms, 平均 = 5ms

C:\WINDOWS\system32>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。
```

```
C:\WINDOWS\system32>ipconfig /displaydns

Windows IP 配置
```

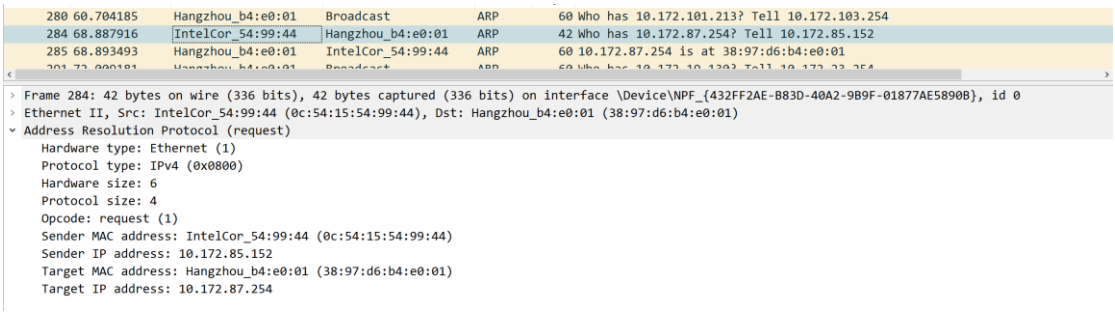
修改 DNS 服务器地址为无效地址后，通过 ip 地址 ping 学校主页可以成功，但通过域名 ping 学校主页就会失败。

分析原因是因为，当通过域名 ping 学校主页时，主机需要通过访问 DNS 服务器进行 ip 地址转换，获得真正的 ip 地址后才能再去 ping 学校主页。但是我们将 DNS 服务器地址手动更改为一个无效的地址后，主机无法通过该地址获得域名对应的 ip 地址，因此也就无法 ping 通学校主页了。而当通过 ip 地址 ping 学校主页时，主机获取到的是直接的 ip 地址，无需访问 DNS 服务器进行 ip 地址转换，因此 DNS 地址是否有效并不影响主机 ping 学校主页，仍然可以 ping 通。

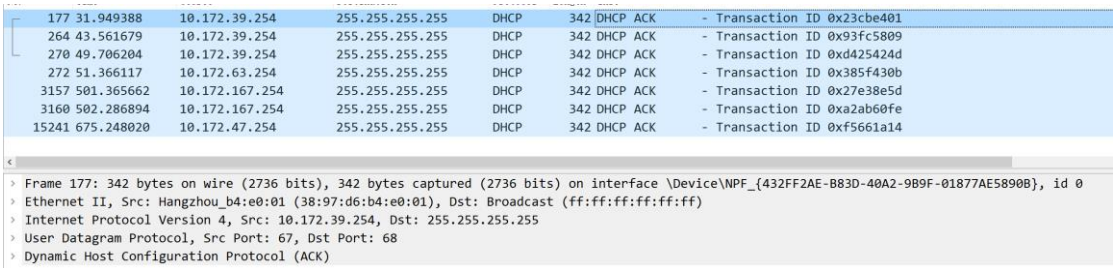
2. 网络分析工具练习

步骤 1：启动 Wireshark 软件，选择上网网卡开始抓包，将网卡 IP 地址和 DNS 服务器地址获取方式改为自动获取，能够正常上网后停止抓包。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。

ARP 报文：



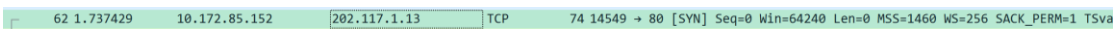
DHCP 报文：



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*
DHCP	协议功能	DHCP 使客户机登录服务器时就可以自动获得服务器分配的 IP 地址和子网掩码
	源地址-目的地址	10.172.39.254-255.255.255.255
	请求/应答信息	DHCP ACK - Transaction ID 0x23cbe401
ARP	协议功能	IP 地址对应 MAC 地址解析
	源地址-目的地址	10.172.39.254-Broadcast
	请求/应答信息	Who has 10.172.39.245? Tell 10.172.39.254

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】

TCP 报文：



HTTP 报文：

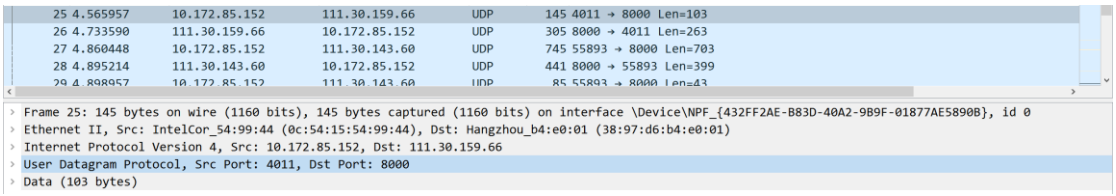
协议名	描述项	配置值
例：TCP	*协议功能*	*传输控制协议,在不可靠的互联网络上提供可靠的端到端传输。*
	源地址-目的地址	*192.168.0.101 - 182.61.200.6*
	请求/应答信息	*49947 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460*

		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	10.172.85.152-202.117.1.13
	请求/应答信息	14549 → 80[SYN] Seq=0 win=64240 Len=0 MSS=1460 WS=256 SACK PERM=1 TSval=7393736 TSecr=0
HTTP	协议功能	规定 WWW 服务器与浏览器之间信息传递规范
	源地址-目的地址	10.172.85.152-202.117.1.13
	请求/应答信息	GET/system/resource/cade/datainput.jsplowner-1151962237R8e=1&w=-1707&h=960Rtreeid-1001&nefer=-&pagename=L21uZGV4LmpzcA%3D%3D&newsid=-1 HTTP/1.1\r \n

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。

描述项	值
QQ/微信及服务器地址	111.30.159.66
本机 IP 地址	111.20.225.143
通信好友自测公网地址	202.200.231.62
通信对方 IP 地址	192.168.1.144
通信协议（Protocol）	UDP
通信源端口-目的端口	4011-8000

UDP 报文：



3. 互动讨论主题

本地计算机需要通过哪些设置、启用哪些协议之后才能上网？

需要设置路由器和网卡。

对于路由器，首先需要连接网线和电源，然后需要设置路由器的连接方式。

对于网卡，具体来说需要选择连接方式，设置 IP 地址、子网掩码、默认网关、DNS 服务器地址后才能访问互联网。

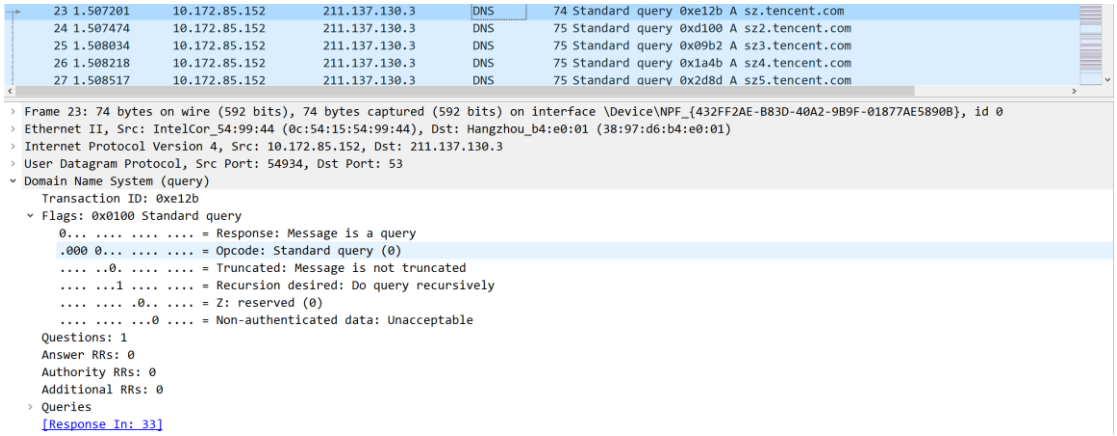
需要启用的协议有 DHCP 协议、IP 协议、ARP 协议、TCP 协议、UDP 协议、HTTP 协议等。

4. *进阶自设计

通过 Wireshark 抓包分析 QQ 或者微信的登陆认证、消息传输和退出登录过程，分析其中涉及到的主要协议、关键数据和标识。

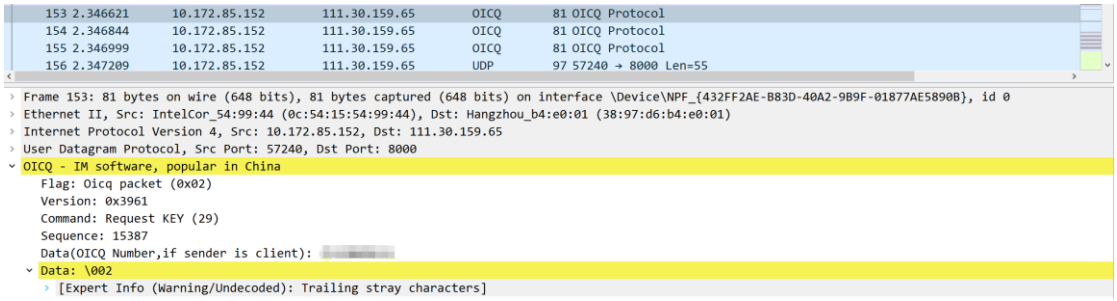
QQ 登录过程中的主要协议：

① DNS 协议



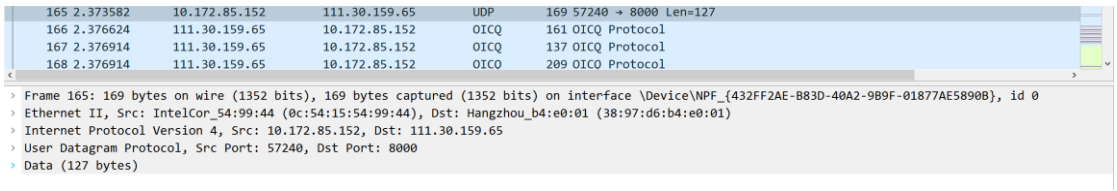
关键数据和标识：Standard query sz.tencent.com。

② OICQ 协议



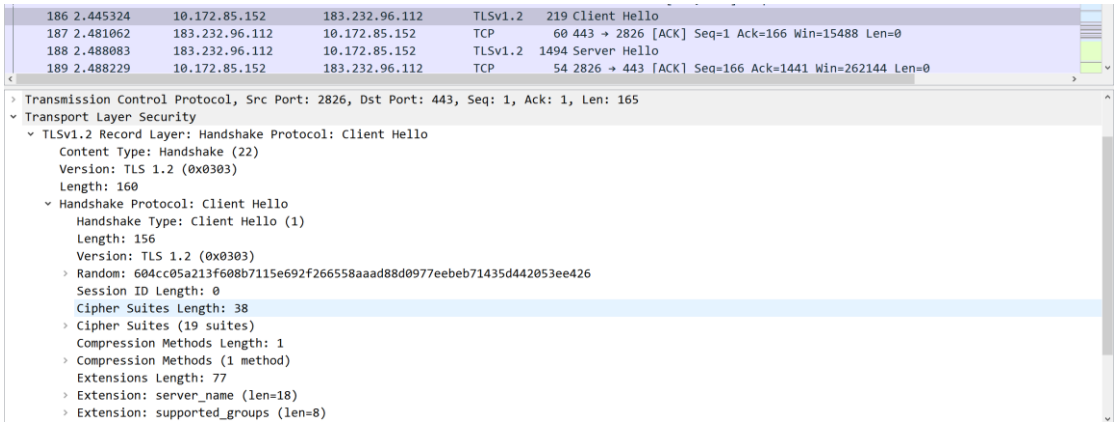
关键数据和标识：Command 行的值为 Request KEY ，Data 行的值为正在登陆的 QQ 号。

③ UDP 协议



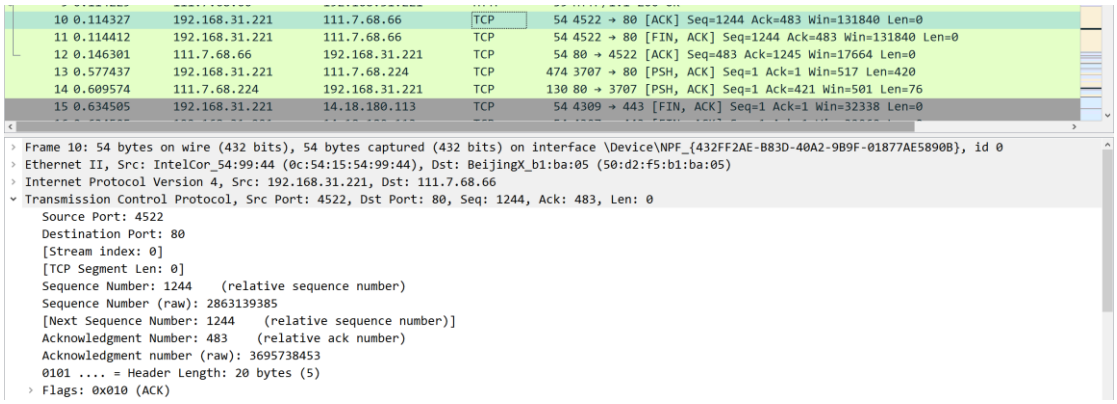
关键数据和标识：目的 ip 地址为 QQ 的服务器地址。

④ TLS 协议



关键数据和标识：TLS 协议一般在对于数据安全性和完整性要求比较高的应用中都会存在，因此我认为在登陆账号的过程中也有 TLS 协议参加。

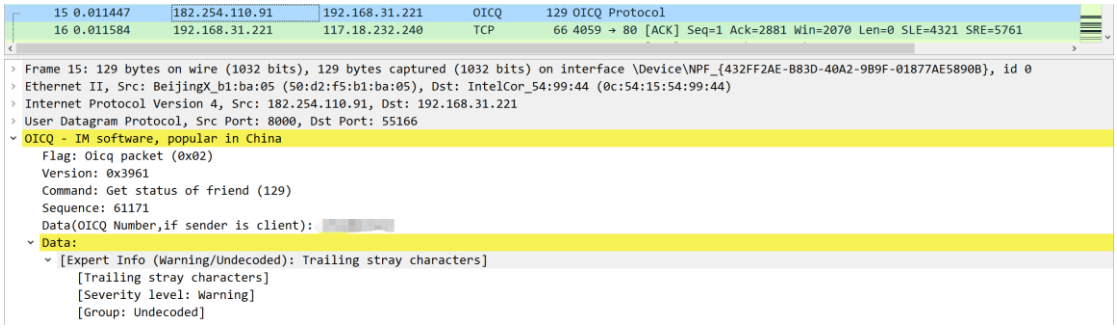
⑤ TCP 协议：



关键数据和标识：目的 ip 地址所在地为深圳市，并且端口号为 80。

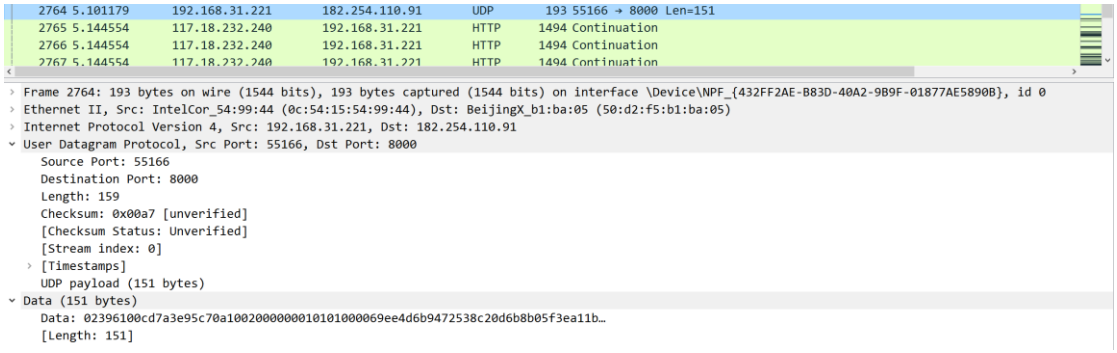
消息传输中的主要协议：

① OICQ 协议：



关键数据和标识：Command 行的值为 Get status of friend，Data 行的值为登陆的 QQ 号。

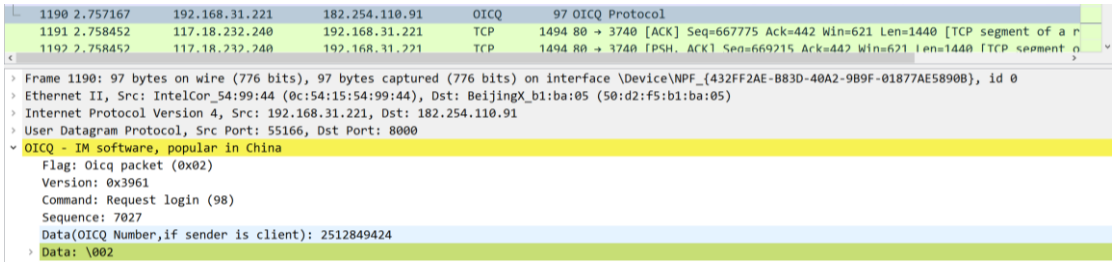
② UDP 协议



关键数据和标识：端口号 8000 一般为 QQ 服务器的端口号。

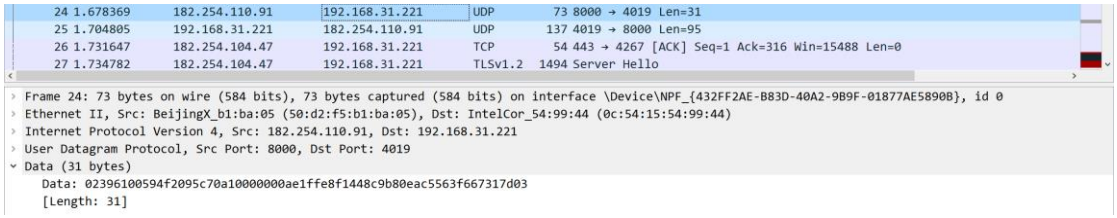
退出登录时的主要协议：

① OICQ 协议：



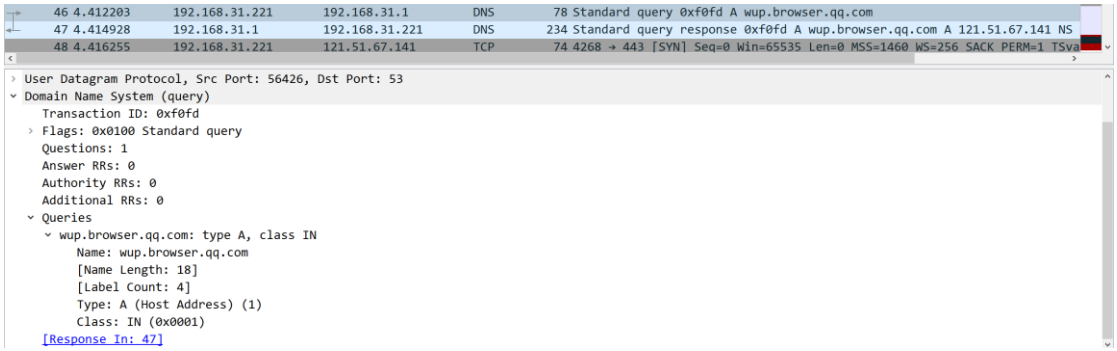
关键数据和标识：Command 行的值为 Request login。

② UDP 协议：



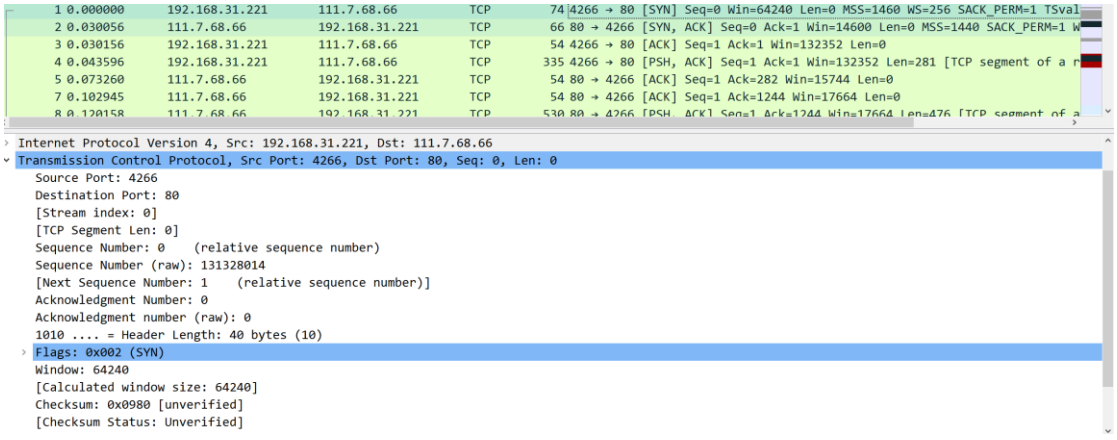
关键数据和标识：目的 ip 地址为 QQ 服务器地址，端口号为 8000。

③ DNS 协议：



关键数据和标识：后缀带有 browser.qq.com。

④ TCP 协议：



关键数据和标识：目的 ip 地址所在地为深圳市，并且端口号为 80。

六、 总结及心得体会

这次实验共分为两部分，一是利用命令行命令查看、修改网络配置，二是学习如何抓包，并对报文进行分析。其中部分内容在上学期的计算机网络课内实验中已有涉及，故总体来说比较简单。

需要注意的是在手动设置主机 ip 地址、子网掩码、网关和 DNS 服务器地址时，不能盲目照抄参考书上的命令，因为每台主机所处的网络环境不同，故对应的地址都不一样。最好的办法是在当前主机能正常访问互联网时利用 ipconfig 查看对应网卡的配置信息，然后再手动修改为和配置信息相同的地址。注意只有在以上几个地址均设置正确的情况下才能正常访问互联网。

通过这次实验我学会了用 ipconfig 命令查看主机的网络配置信息，用 netsh 语句手动或自动配置 ip 地址和 dns 服务器地址，还学会了利用 route 语句打印路由表、增删路由表条目。同时通过使用 wireshark 软件抓取并对数据包进行分析，我还了解到了在访问网页和过程中涉及到的相关协议及其对应功能。