实验一 常用网络命令及工具实验报告

组号：

姓名：李云广 学号：2193712575 班级：计算机 93

一、 实验名称

常用网络命令及工具练习。

二、 实验目的

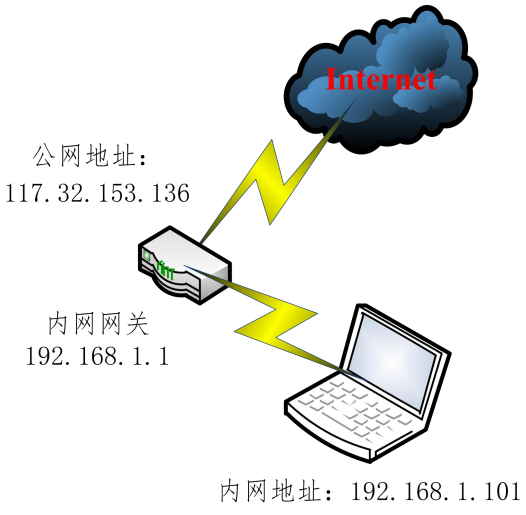
掌握常用网络命令（ping、tracert、ipconfig、route 等）的使用，掌握常用网络工具（如 Wireshark，putty 等）的使用。

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。【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】。



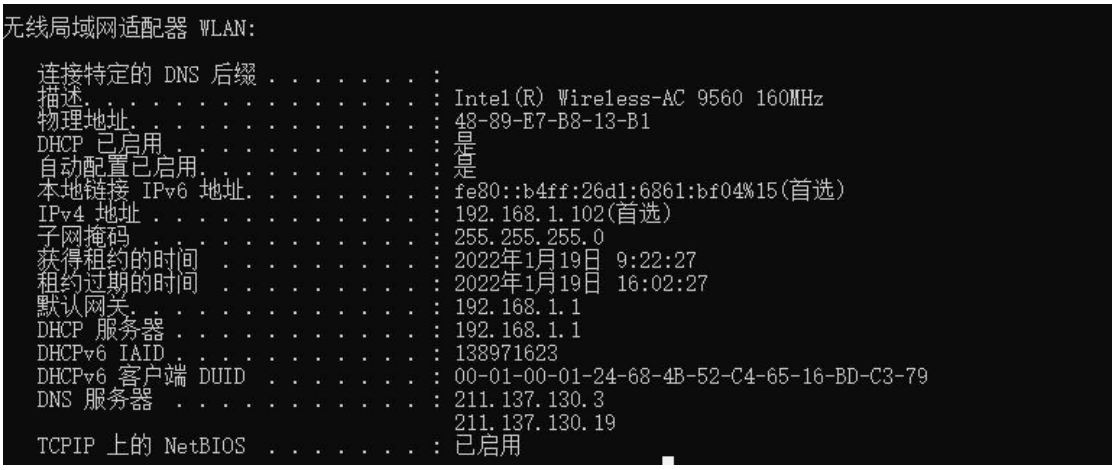
五、 实验过程及结果分析

【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】

在 cmd 中输入 ipconfig /all，得到结果，查看信息最为详尽的网卡是这个无线网卡，对应信息如下：



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	192.168.1.102
子网掩码	255.255.255.0
默认网关	192.168.1.1
DNS 服务器	211.137.130.3 211.137.130.19

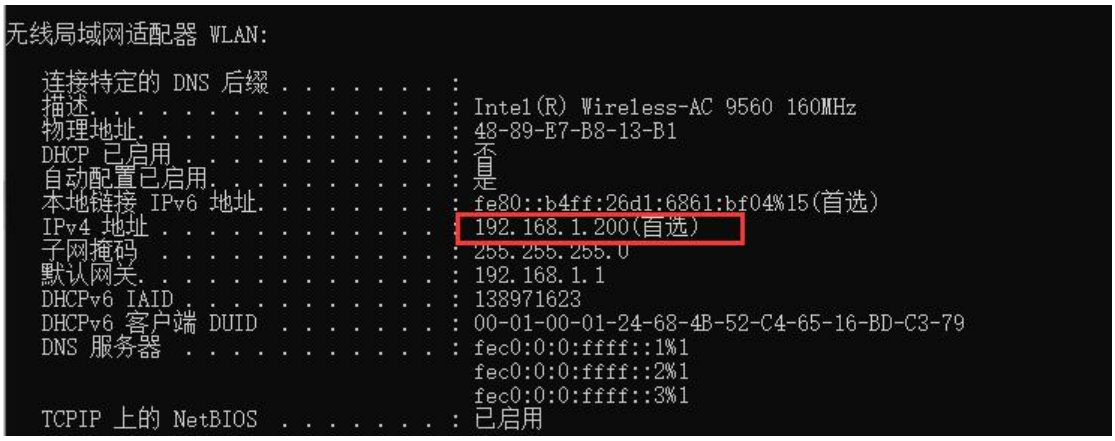
步骤 2：用命令行修改本机 IP 地址和 DNS 服务器地址的获取方式（原来是自动获取方式则改为手动设置，原来为手动设置地址则改为自动获取）查看并记录网卡配置信息，与手动设置地址时的配置有什么不同？

IP 地址手动设置

cmd 中输入命令(注意这里要求以管理员身份运行)

netsh interface ip set address name="WLAN" static 192.168.1.200 255.255.255.0 192.168.1.1

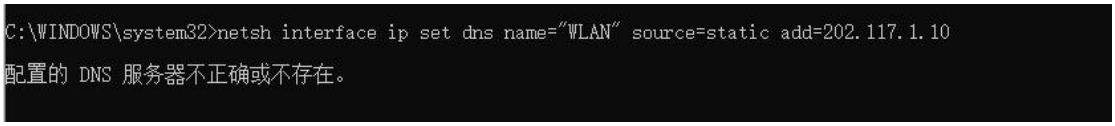
查看 ipconfig



DNS 服务器地址手动设置

cmd 中输入：（先设置一个错误的 DNS 地址）

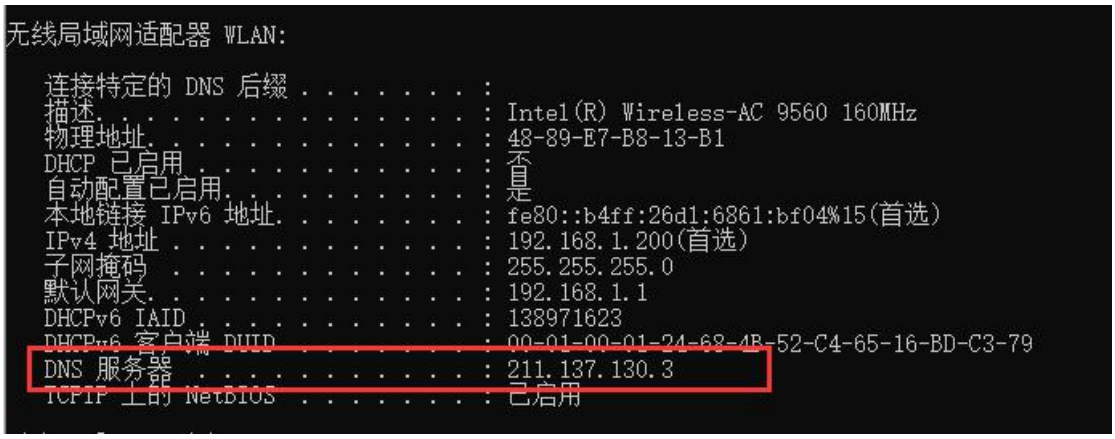
netsh interface ip set dns name="WLAN" source=static add=202.117.1.10



然后输入

netsh interface ip set dns name="WLAN" source=static add=211.137.130.3

查看 ipconfig

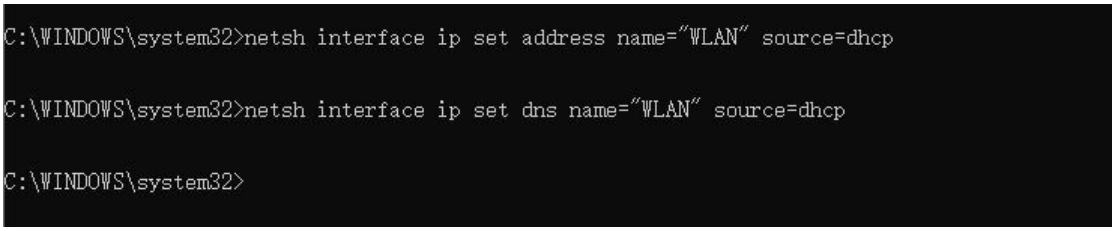


调整回自动获取：

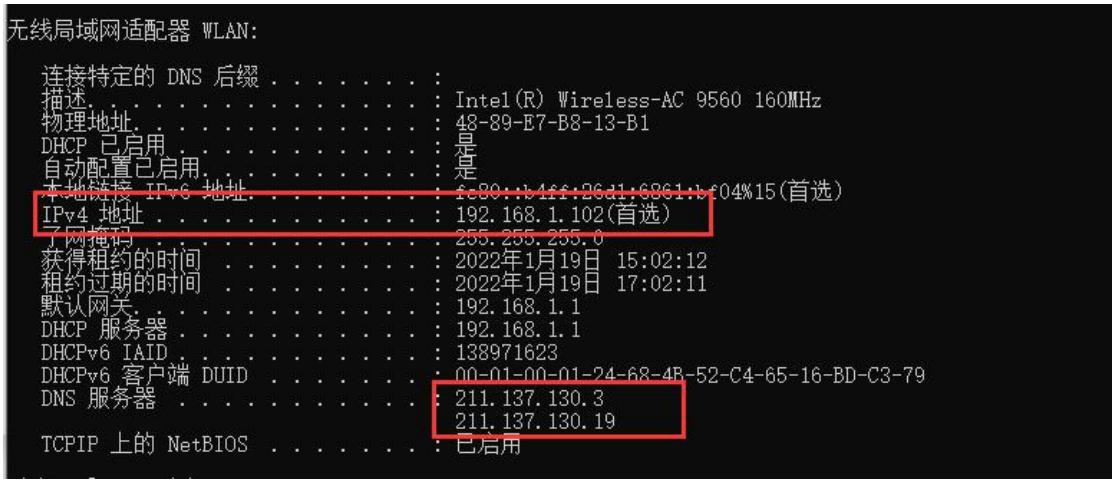
Cmd 中输入：

netsh interface ip set address name="WLAN" source=dhcp

netsh interface ip set dns name="WLAN" source=dhcp



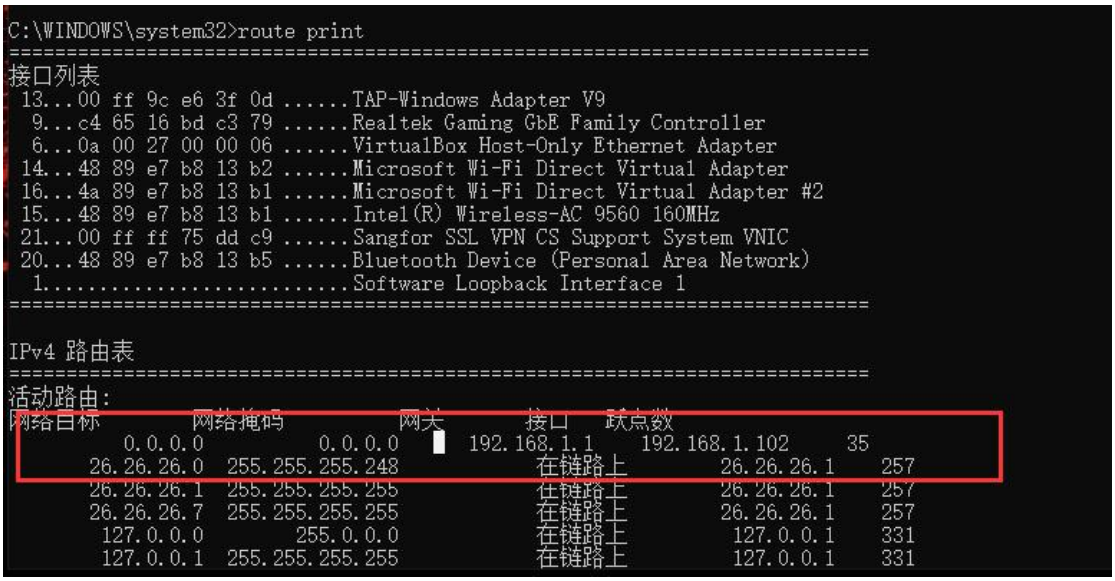
查看 ipconfig



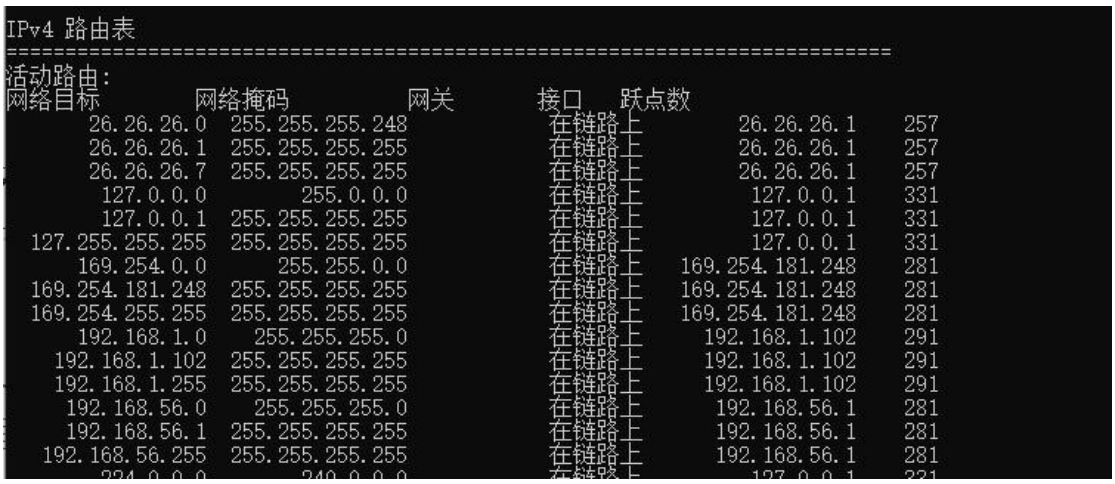
可以看到对应信息恢复到了之前的配置。

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】

Cmd 中输入 route print



可以看到这条路由信息网络掩码是 0.0.0.0，也就是默认路由，我们尝试删除这个路由信息。



发现上不去网了。

查看 ipconfig

可以看到默认网关也不见了。

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？

尝试增加一个默认路由，输入

Route add 0.0.0.0 mask 0.0.0.0 192.168.1.1

```
C:\WINDOWS\system32>route add 0.0.0.0 mask 0.0.0.0 192.168.1.1
 操作完成!

C:\WINDOWS\system32>_
```

查看路由表 route　print

```
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    192.168.1.102     36
       26.26.26.0  255.255.255.248            在链路上         26.26.26.1    257
       26.26.26.1  255.255.255.255            在链路上         26.26.26.1    257
       26.26.26.7  255.255.255.255            在链路上         26.26.26.1    257
        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    169.254.181.248    281
  169.254.181.248  255.255.255.255            在链路上    169.254.181.248    281
  169.254.255.255  255.255.255.255            在链路上    169.254.181.248    281
```

发现默认路由信息又恢复了，并且与之前的路由表在一个位置。

下面使用 route add -p 添加路由信息

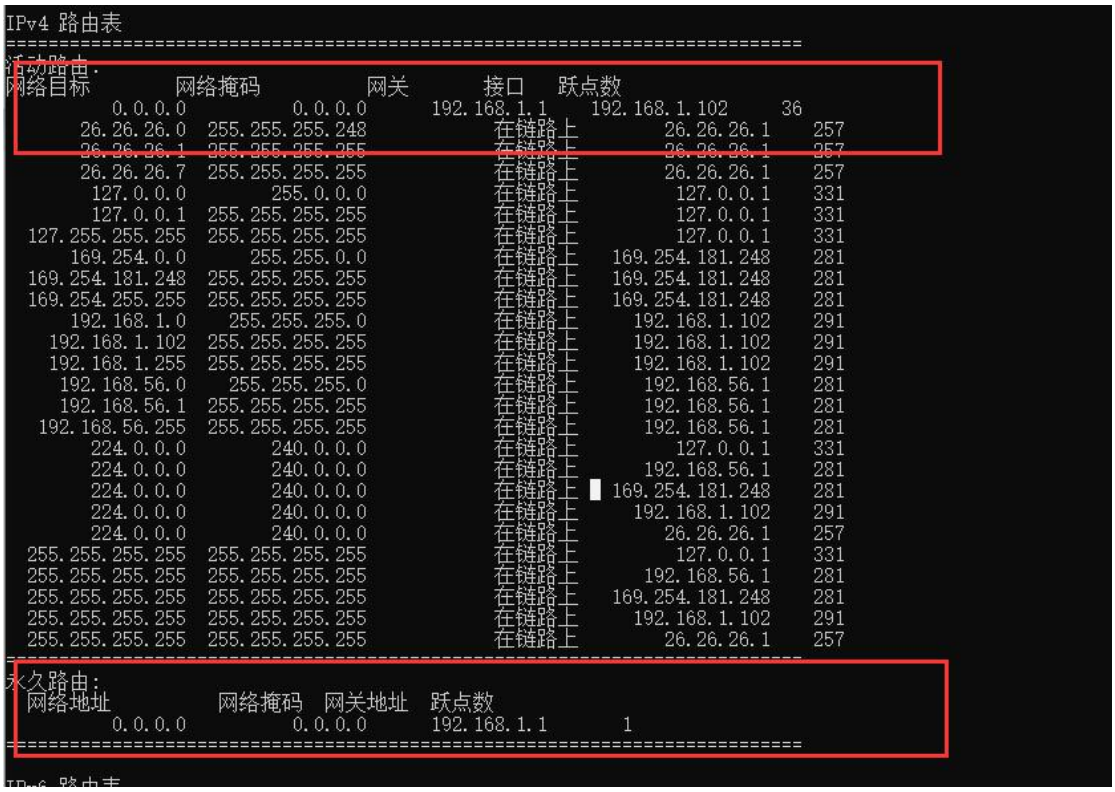
Cmd 中输入：

route delete 0.0.0.0

route add -p 0.0.0.0 mask 0.0.0.0 192.168.1.1

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

C:\WINDOWS\system32>route add -p 0.0.0.0 mask 0.0.0.0 192.168.1.1
 操作完成!
```

查看路由表 route print



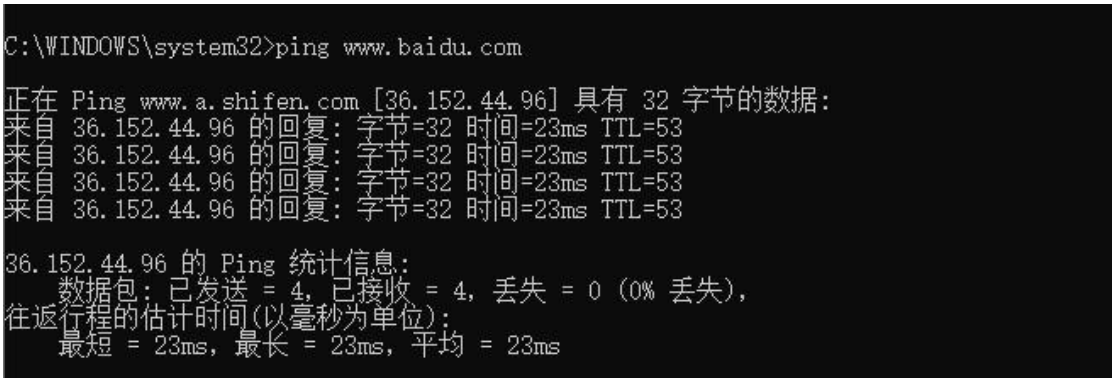
发现这两个位置都有默认路由信息。

多了一个永久路由的信息，我理解永久路由信息就是由管理员为他分配的网关地址，而不是自动获取的。

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。

然后我们 ping 一下百度官网：

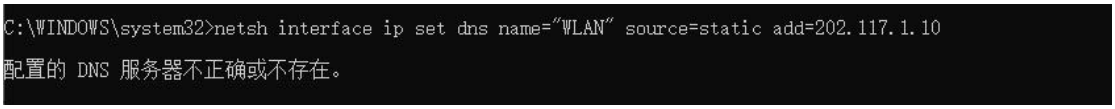
Ping www.baidu.com



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】

Cmd 中输入把 dns 地址设置为 6.6.6.6

netsh interface ip set dns name="WLAN" source=static add=202.117.1.10



```
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. . . . . : 48-89-E7-B8-13-B1
   DHCP 已启用 . . . . . : 是
   自动配置已启用. . . . . : 是
   IPv4 地址 . . . . . : 192.168.1.102(首选)
   子网掩码 . . . . . : 255.255.255.0
   获得租约的时间 . . . . . : 2022年1月19日 15:30:19
   租约过期的时间 . . . . . : 2022年1月19日 17:30:20
   默认网关. . . . . : 192.168.1.1
   DHCP 服务器 . . . . . : 192.168.1.1
   DNS 服务器 . . . . . : 202.117.1.10
   TCPIP 上的 NetBIOS . . . . . : 已启用
```

Ping 一下 xjtu 官网

Ping www.xjtu.edu.cn

```
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。
```

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先改为手动获取，再改回自动获取，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。

打开 wireshark 选择对应网卡

也就是这个 WLAN 网卡，然后进入，直接开始抓取网络包。

Cmd 中输入

netsh interface ip set address name="WLAN" static 192.168.1.200 255.255.255.0 192.168.1.1

netsh interface ip set dns name="WLAN" source=static add=211.137.130.3

手动获取 ip 和 dns 地址

Cmd 中输入

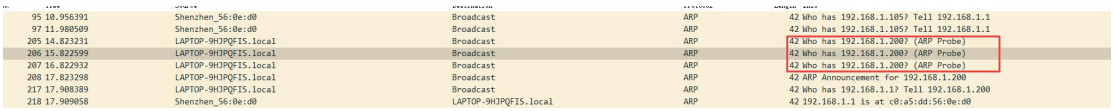
netsh interface ip set address name="WLAN" source=dhcp

netsh interface ip set dns name="WLAN" source=dhcp

改为自动获取

```
C:\WINDOWS\system32>netsh interface ip set address name="WLAN" static 192.168.1.200 255.255.255.0 192.168.1.1

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

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

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

C:\WINDOWS\system32>
```

发现可以正常上网，停止抓包，对包进行分析。



95	10.956391	Shenzhen_56:0e:d0	Broadcast	ARP	42 Who has 192.168.1.105? Tell 192.168.1.1
97	11.980509	Shenzhen_56:0e:d0	Broadcast	ARP	42 Who has 192.168.1.105? Tell 192.168.1.1
205	14.823231	LAPTOP-9HJPQFIS.local	Broadcast	ARP	42 Who has 192.168.1.200? (ARP Probe)
206	15.822599	LAPTOP-9HJPQFIS.local	Broadcast	ARP	42 Who has 192.168.1.200? (ARP Probe)
207	16.822932	LAPTOP-9HJPQFIS.local	Broadcast	ARP	42 Who has 192.168.1.200? (ARP Probe)
208	17.823298	LAPTOP-9HJPQFIS.local	Broadcast	ARP	42 ARP Announcement for 192.168.1.200
217	17.908389	LAPTOP-9HJPQFIS.local	Broadcast	ARP	42 Who has 192.168.1.1? Tell 192.168.1.200
218	17.909058	Shenzhen_56:0e:d0	LAPTOP-9HJPQFIS.local	ARP	42 192.168.1.1 is at c0:a5:dd:56:0e:d0

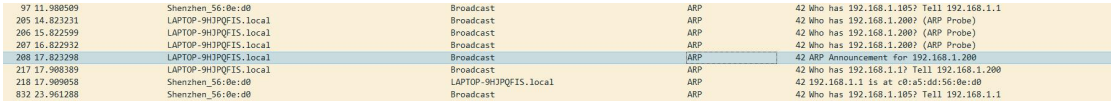
我配置的 ip 是 192.168.1.200，可以看到主机发送了三个包

内容如下：

```
Address Resolution Protocol (ARP Probe)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    [Is probe: True]
    Sender MAC address: LAPTOP-9HJPQFIS.local (48:89:e7:b8:13:b1)
    Sender IP address: 0.0.0.0 (0.0.0.0)
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: LAPTOP-9HJPQFIS.local (192.168.1.200)
```

判断这个 ip 地址是否有设备占用

然后宣布这个设备被主机占用了



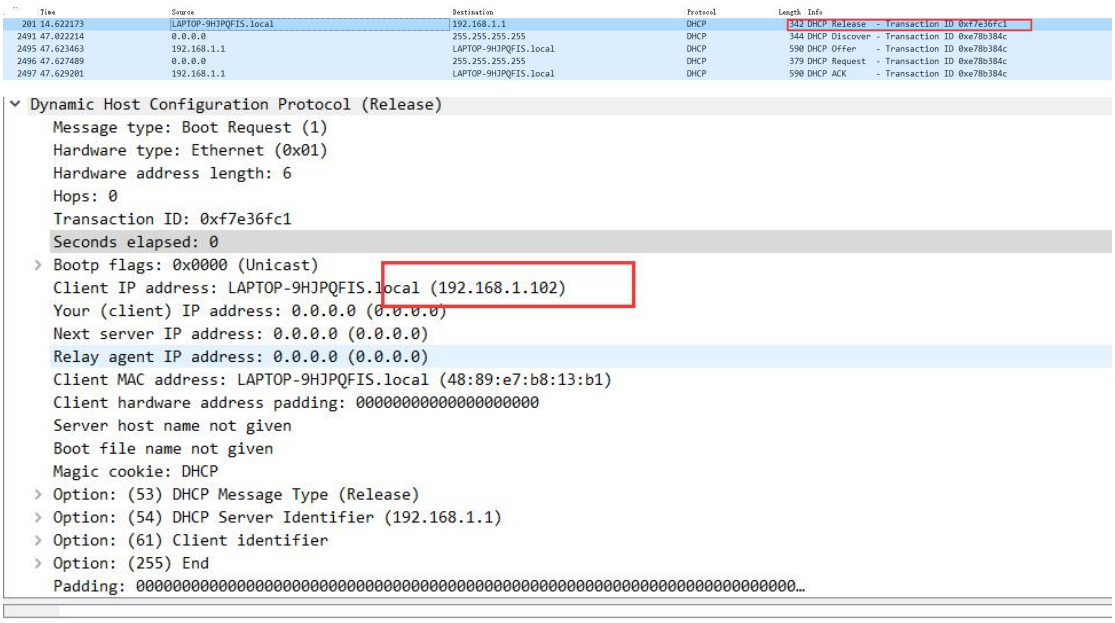
97	11.980509	Shenzhen_56:0e:d0	Broadcast	ARP	42 Who has 192.168.1.105? Tell 192.168.1.1
205	14.823231	LAPTOP-9HJPQFIS.local	Broadcast	ARP	42 Who has 192.168.1.200? (ARP Probe)
206	15.822599	LAPTOP-9HJPQFIS.local	Broadcast	ARP	42 Who has 192.168.1.200? (ARP Probe)
207	16.822932	LAPTOP-9HJPQFIS.local	Broadcast	ARP	42 Who has 192.168.1.200? (ARP Probe)
208	17.823298	LAPTOP-9HJPQFIS.local	Broadcast	ARP	42 ARP Announcement for 192.168.1.200
217	17.908389	LAPTOP-9HJPQFIS.local	Broadcast	ARP	42 Who has 192.168.1.1? Tell 192.168.1.200
218	17.909058	Shenzhen_56:0e:d0	LAPTOP-9HJPQFIS.local	ARP	42 192.168.1.1 is at c0:a5:dd:56:0e:d0
832	23.961288	Shenzhen_56:0e:d0	Broadcast	ARP	42 Who has 192.168.1.105? Tell 192.168.1.1

内容如下:

```
Address Resolution Protocol (ARP Announcement)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    [Is gratuitous: True]
    [Is announcement: True]
    Sender MAC address: LAPTOP-9HJPQFIS.local (48:89:e7:b8:13:b1)
    Sender IP address: LAPTOP-9HJPQFIS.local (192.168.1.200)
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: LAPTOP-9HJPQFIS.local (192.168.1.200)
```

然后我们来研究一下 DHCP 协议的内容，

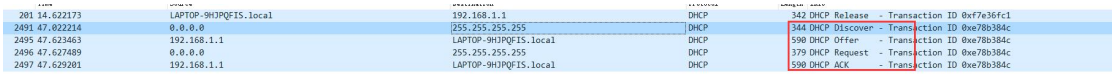
我们在调整为手动设置 ip 时：



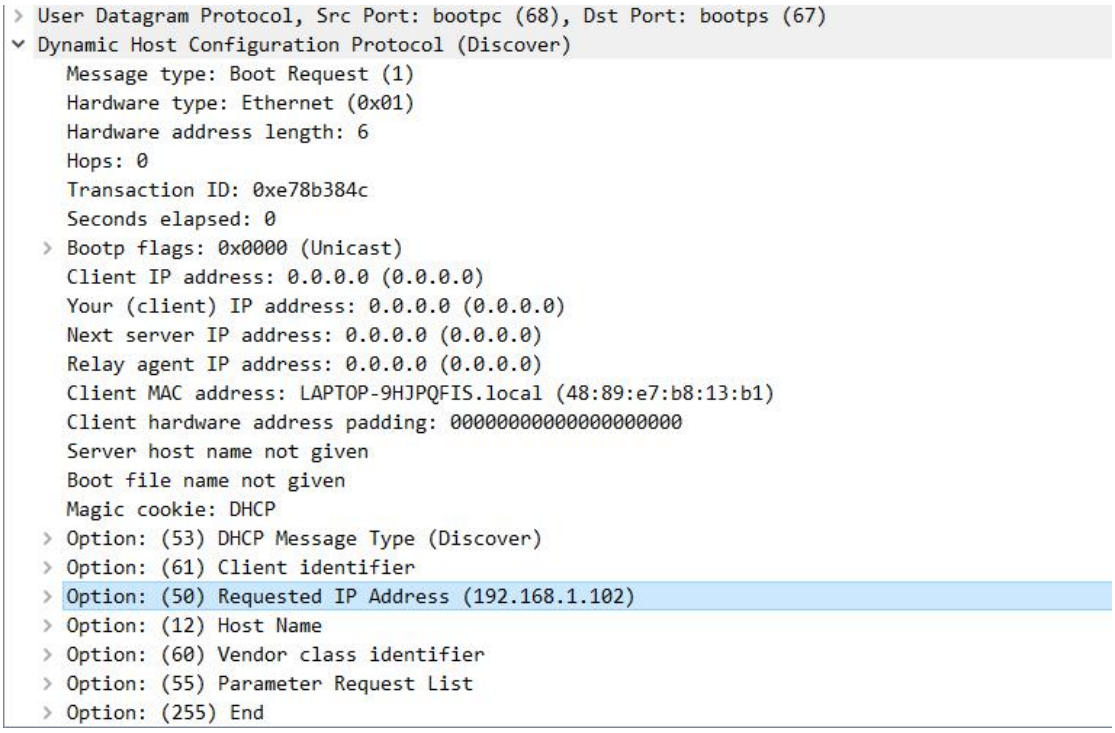
首先是由本地主机向局域网网关（也就是宿舍路由器）发出的一个 Release 包，这样我们将之前 DHCP 自动设置的 ip 地址释放掉。

然后手动设置 ip 为 192.168.1.200 与 DHCP 无关。

然后将 IP 改为自动获取之后：



可以看到这四个包都是与自动获取 IP 地址相关的，首先通过 0.0.0.0 发送到 255.255.255.255 广播 Discover 空闲的 IP 地址：



然后局域网网关 Offer 一个 IP 地址。

```
Dynamic Host Configuration Protocol (Offer)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xe78b384c
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: LAPTOP-9HJPQFIS.local (192.168.1.102)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: LAPTOP-9HJPQFIS.local (48:89:e7:b8:13:b1)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Offer)
  > Option: (54) DHCP Server Identifier (192.168.1.1)
  > Option: (51) IP Address Lease Time
  > Option: (6) Domain Name Server
  > Option: (1) Subnet Mask (255.255.255.0)
  > Option: (3) Router
  > Option: (255) End
```

然后本地主机请求 ip 地址即 Request

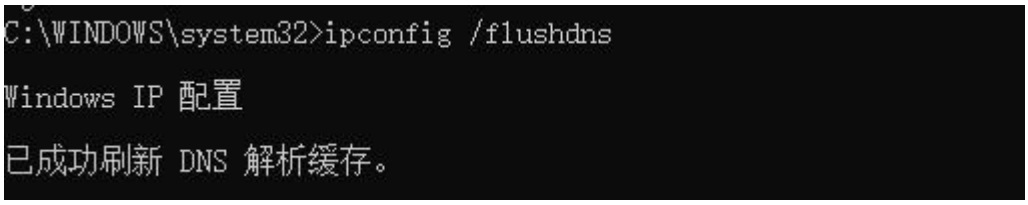
```
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: LAPTOP-9HJPQFIS.local (48:89:e7:b8:13:b1)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Request)
  > Option: (61) Client identifier
  > Option: (50) Requested IP Address (192.168.1.102)
  > Option: (54) DHCP Server Identifier (192.168.1.1)
  > Option: (12) Host Name
  > Option: (81) Client Fully Qualified Domain Name
  > Option: (60) Vendor class identifier
  > Option: (55) Parameter Request List
  > Option: (255) End
```

对应 DHCP 服务器再返回一个 ACK，这样就成功分配了。

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*
ARP	协议功能	*IP 地址对应 MAC 地址解析*
	源地址-目的地址	48-89-E7-B8-13-B1(mac 地址，因为还没分配 ip 地址) - Broadcast
	请求/应答信息	Who has 192.168.1.200？(arp probe)判断这个 ip 地址是

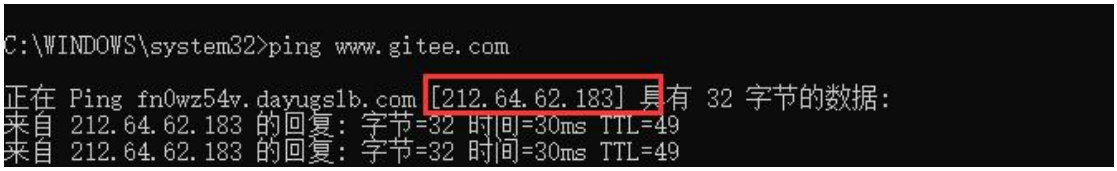
		否有设备占用
ARP	协议功能	*IP 地址对应 MAC 地址解析*
	源地址-目的地址	48-89-E7-B8-13-B1(mac 地址，因为还没分配 ip 地址) - Broadcast
	请求/应答信息	ARP Announcement 192.168.1.200，宣布这个 ip 被自己占用了。
DHCP	协议功能	*局域网内部自动分配 IP 地址*
	源地址-目的地址	*0.0.0.0-255.255.255.255*
	请求/应答信息	*Discover*
DHCP	协议功能	*局域网内部自动分配 IP 地址*
	源地址-目的地址	48-89-E7-B8-13-B1(mac 地址，因为还没分配 ip 地址) - 192.168.1.1
	请求/应答信息	*Offer*
DHCP	协议功能	*局域网内部自动分配 IP 地址*
	源地址-目的地址	192.168.1.1-48-89-E7-B8-13-B1(mac 地址，因为还没分配 ip 地址) -
	请求/应答信息	*Request*
DHCP	协议功能	*局域网内部自动分配 IP 地址*
	源地址-目的地址	48-89-E7-B8-13-B1(mac 地址，因为还没分配 ip 地址) - 192.168.1.1
	请求/应答信息	*ACK*

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】



我们访问码云主页，首先获得码云的 ip 地址

Ping www.gitee.com



在 wireshark 过滤器中输入

Ip.addr == 212.64.62.183 即可过滤出码云服务器的相关包。

但我发现 http 相关的包并没有过滤到，所以说考虑到码云公司的 http 服务器有专门的 ip 地址。

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*
DNS	协议功能	将域名解析为 ip 地址
	源地址-目的地址	192.168.1.102-211.137.130.3
	请求/应答信息	Query www.gitee.com
DNS	协议功能	将域名解析为 ip 地址
	源地址-目的地址	211.137.130.3-192.168.1.102
	请求/应答信息	Response 一个 IPv6 地址 69 Standard query 0x9787 AAAA gitee.com
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	*192.168.1.102 - 211.137.130.3*
	请求/应答信息	66 52059 → https(443) [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
TLSv1.2	*协议功能*	客户端和服务器端的通信进行加密，通过特殊的密钥交换
	源地址-目的地址	*192.168.1.102 - 211.137.130.3*
	请求/应答信息	Client Hello

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。

本机捕获信息

描述项	值
QQ/微信服务器地址	36.155.244.93（移动服务器）
本机 IP 地址	192.168.1.102
本机自测公网地址	111.20.226.1
通信好友的 IP 地址	111.20.226.27
通信协议（Protocol）	UDP
通信源端口-目的端口	52844-xxx（一直在变）

好友端捕获信息

描述项	值
QQ/微信服务器地址	36.155.244.93

通信好友 IP 地址	10.173.164.44
通信好友自测公网地址	111.20.226.27
好友看到的我的 IP 地址	111.20.226.1
通信协议（Protocol）	UDP
通信源端口-目的端口	55178-xxx（一直在变）

3. 互动讨论主题

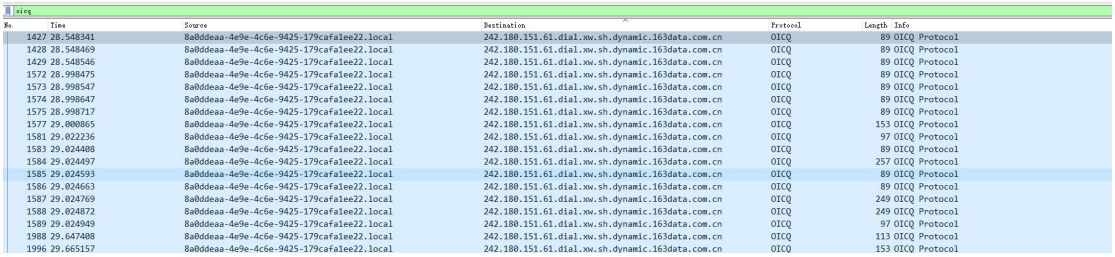
本地计算机接入网络之后，需要通过哪些设置、启用哪些协议之后才能上网（通过域名访问网站等）。

1) 通过 DHCP 服务器自动获取内网 IP 地址，在宿舍里面上网一般宿舍路由器就作为 DHCP 服务器，通过 DHCP 协议获得内网地址后，就可以通过内网地址与 ARP 协议的配合进行上网。
2)自动配置 DNS 服务器，通过 DNS 服务器可以进行域名转化为 IP 地址。
3)自动设置默认网关为宿舍的路由器。

4. *进阶自设计

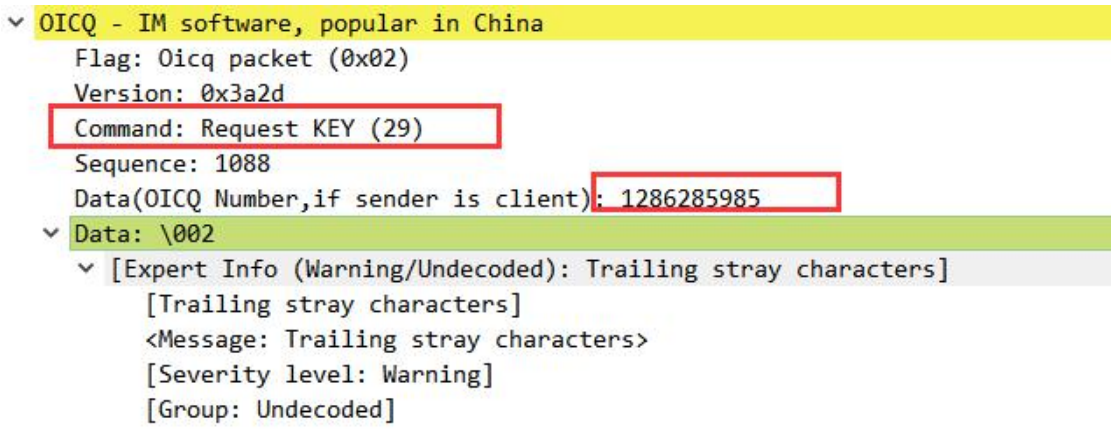
通过 Wireshark 抓包分析 QQ 的登陆认证、消息传输和退出登录过程，分析其中涉及到的主要协议、关键数据和标识。【QQ 的主要通讯协议类型是 QICQ，注意观察数据包中的标识，看看能找到多少种类型的数据包，分析各种数据包的主要作用。】

由于 QQ 使用的主要协议即为 OICQ 协议，所以这里我们直接将 OICQ 协议过滤出来进行单独分析：

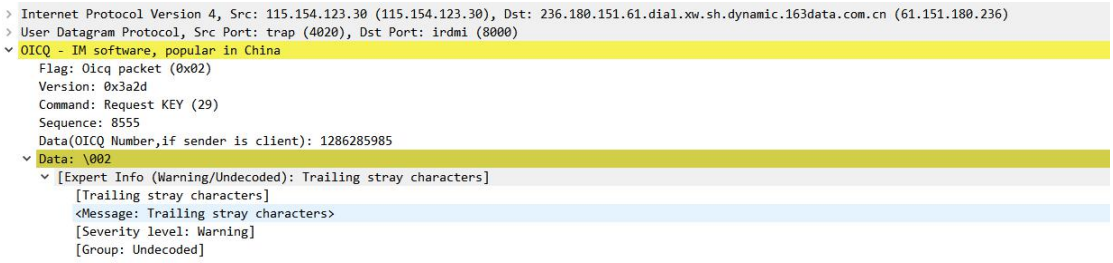


1. 本地主机发送到 QQ 服务器的 Request Key

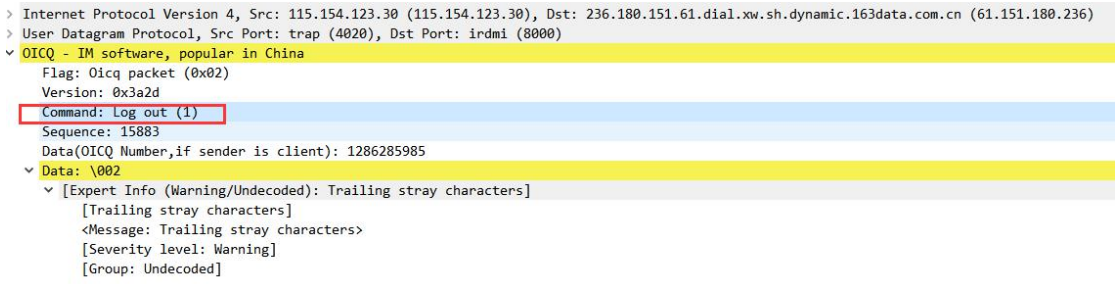
请求密钥可能想要加密通话。



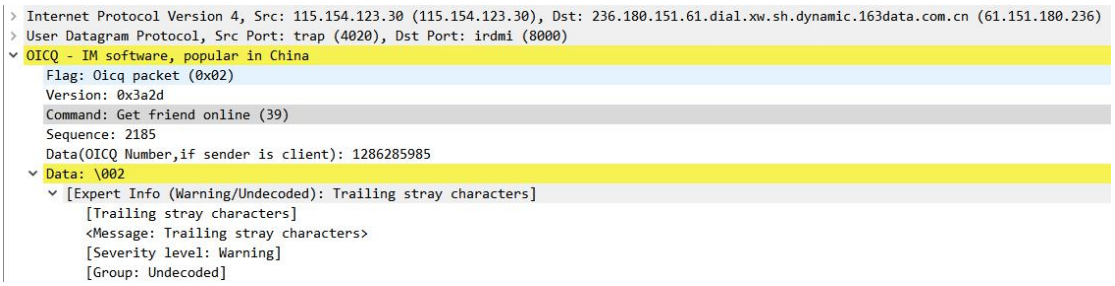
2. QQ 服务器向本地主机发送的 request key，这两个 request key 是想获取密钥，交换密钥，并且在以下的对话中加密通话。



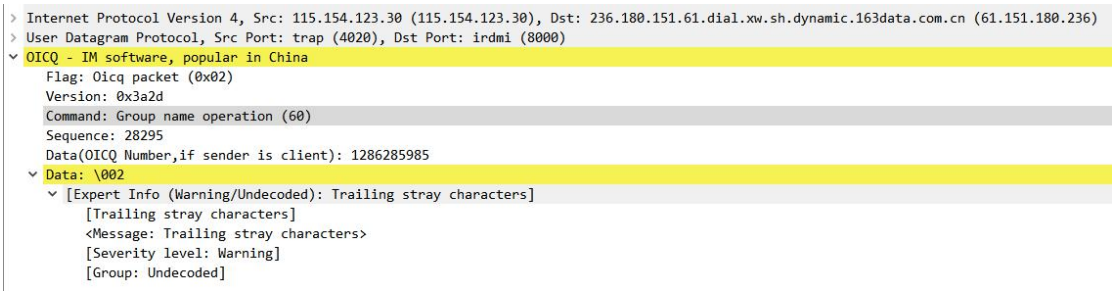
3. 本地主机发送到 QQ 服务器的 Log out



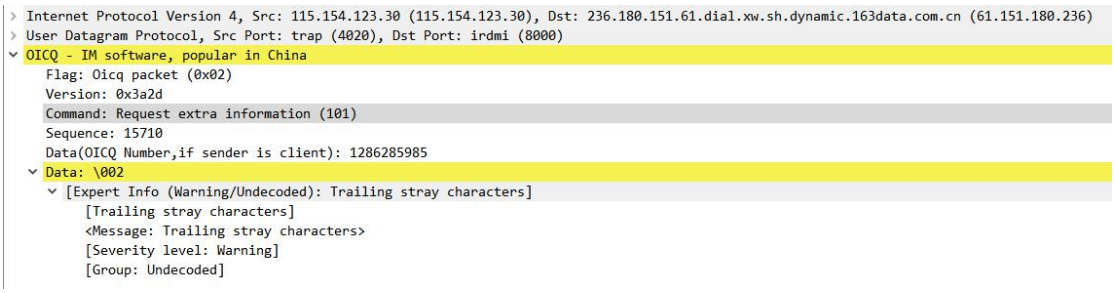
4. Get Friend Online 取得线上的好友列表。



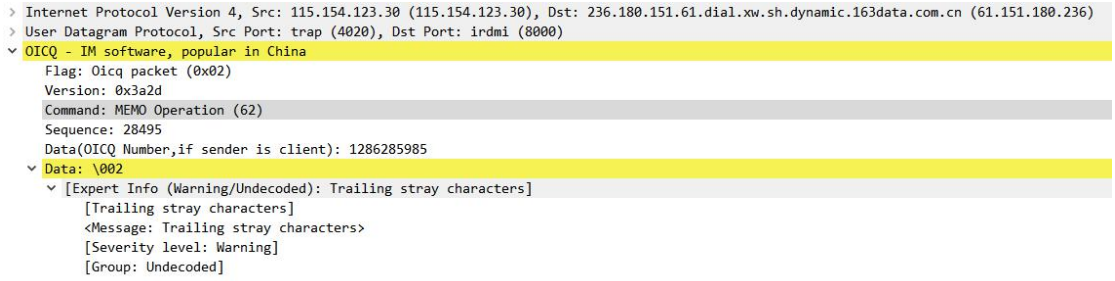
5. Group name operation 对名字进行分组显示。



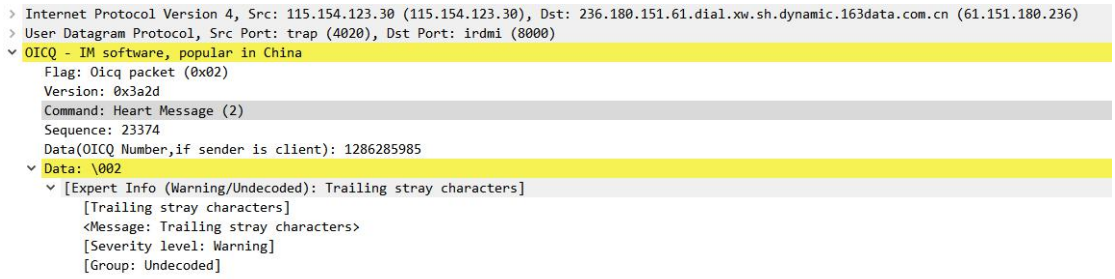
6. 请求其他的信息。



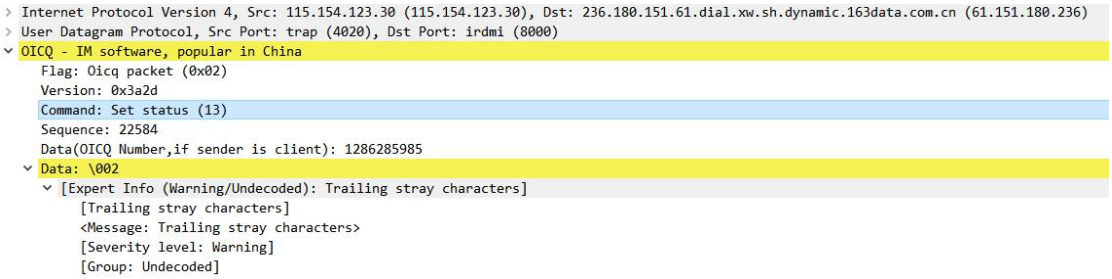
7. MEMO operation 记录登录操作。



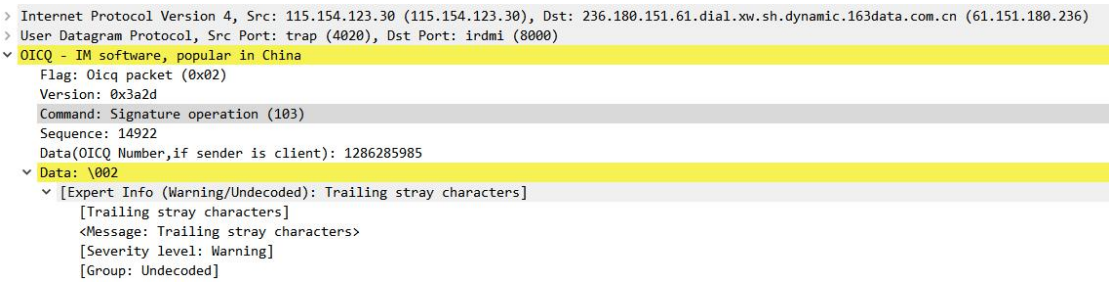
8. Heart Message 请求重要的信息。



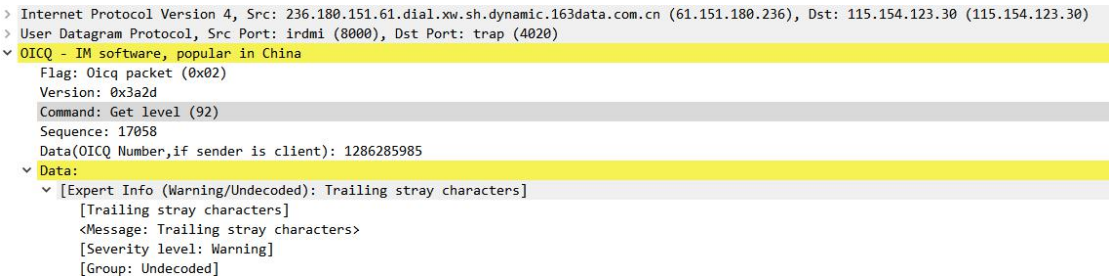
9. Set Status 设置状态为在线上。



10. Signature operatioin 得到签名。



11. GetLevel 得到等级



六、 总结及心得体会

本次实验我学会了一些基本的有关网络的 cmd 指令，可以进行手动设置 ip，手动设置 DNS 服务器地址，还可以查看 DNS 缓存表，查看路由表。

本次实验教会我使用 wireshark，教会我如何进行抓包操作，并且可以根据 wireshark 显示的信息对包进行分析，从而对整个网络连接的过程进行详细分析。

本次实验基于 OICQ 让我对 wireshark 抓包进行了实践，并且探究了 OICQ 协议的本质。