实验一 常用网络命令及工具实验报告

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

1. 实验名称

常用网络命令及工具练习。

1. 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。

1. 实验内容

1．常用网络命令练习；

2．网络分析软件练习。

1. 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】。



1. 实验过程及结果分析

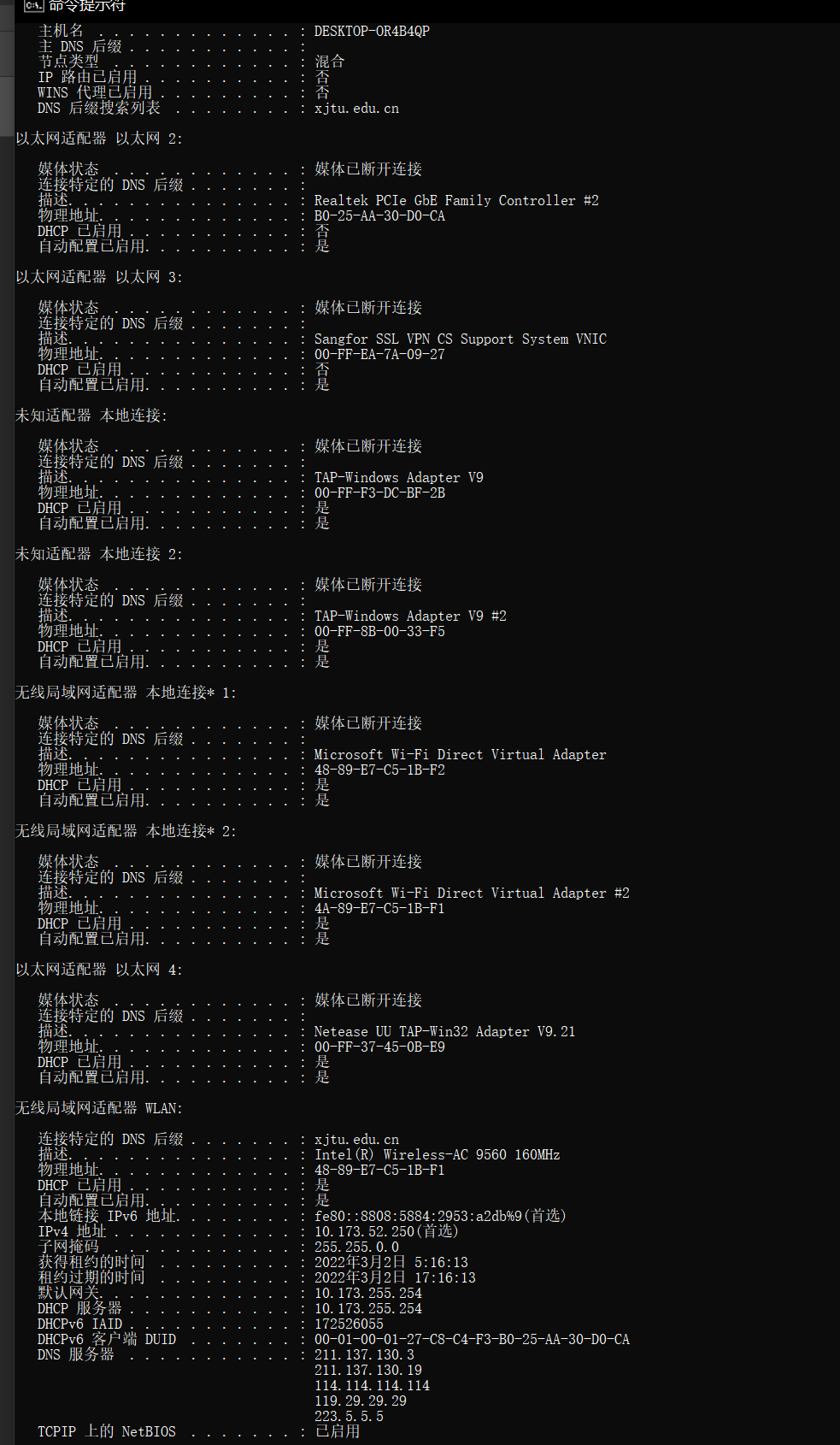
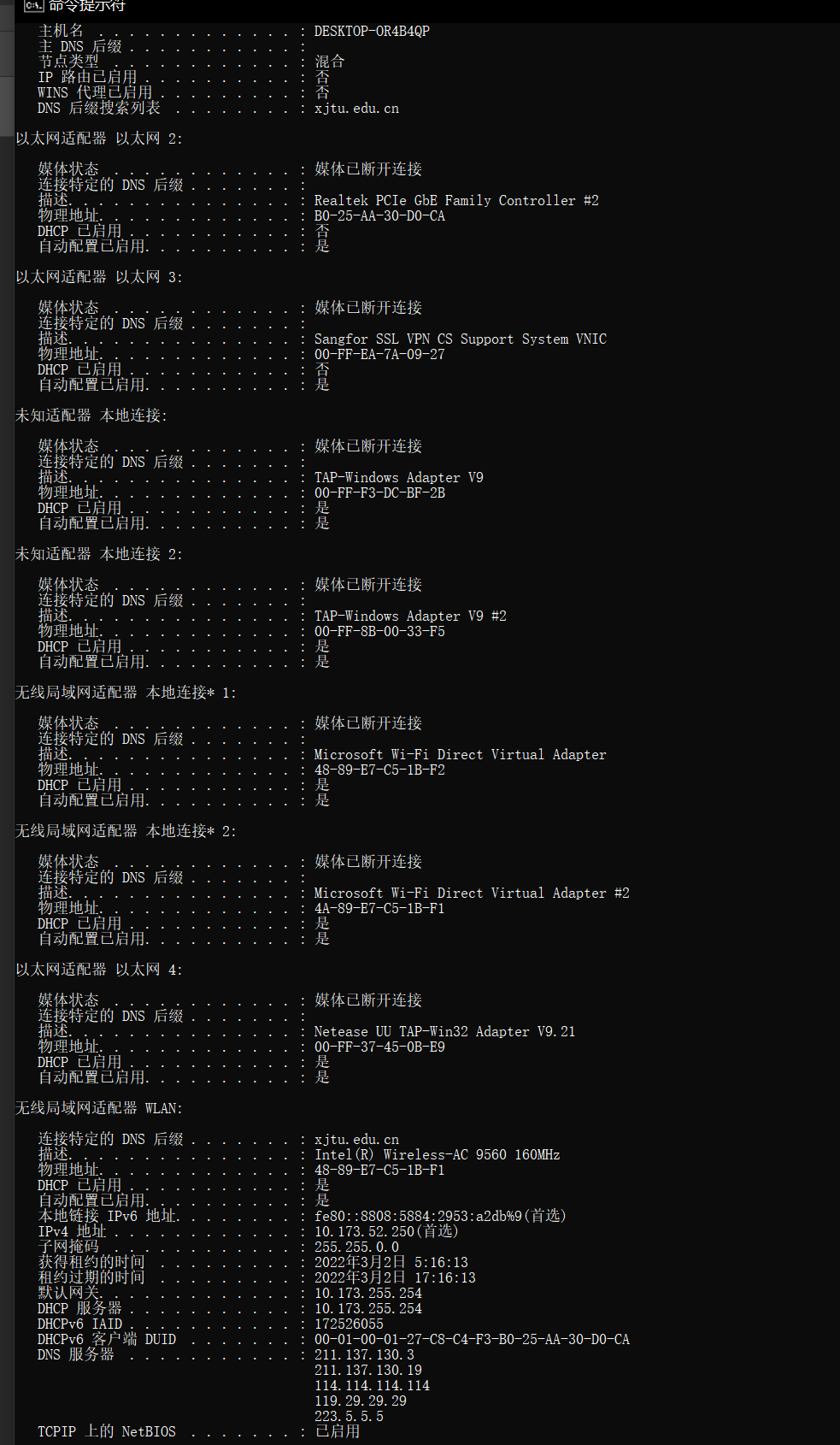
【过程记录应当详尽，截图并加以说明。以下过程和表格仅供参考。】

* 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】

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 | 10.173.52.250(首选) |
| 子网掩码 | 255.255.0.0 |
| 默认网关 | 10.173.255.254 |
| DNS服务器 | 211.137.130.3  211.137.130.19  114.114.114.114  119.29.29.29  223.5.5.5 |



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：

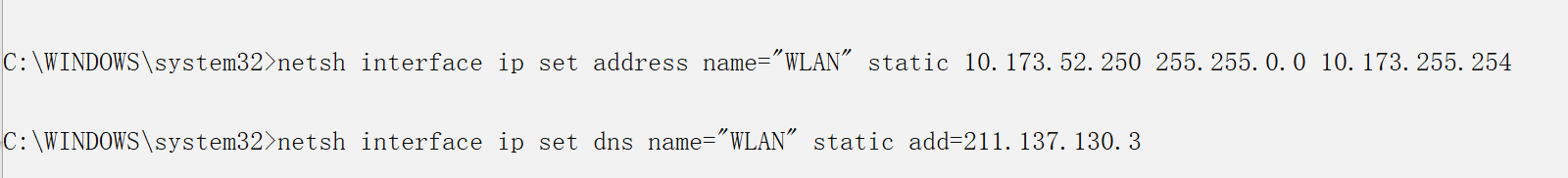
IP地址手动设置命令：netsh interface ip set address name="本地连接" static 192.168.1.101 255.255.255.0 192.168.1.1；

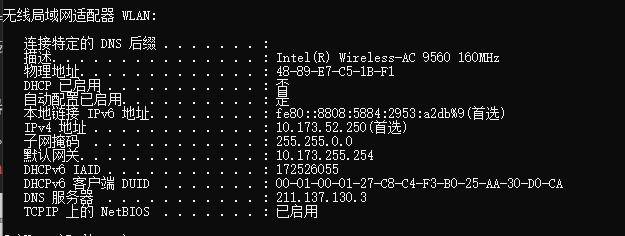
DNS服务器地址手动设置命令：netsh interface ip set dns name="本地连接" source=static add=202.117.1.20；

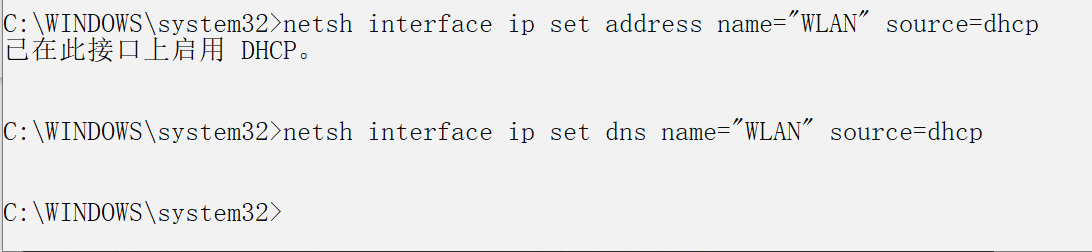
IP地址自动获取命令：netsh interface ip set address name="本地连接" source=dhcp；

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。

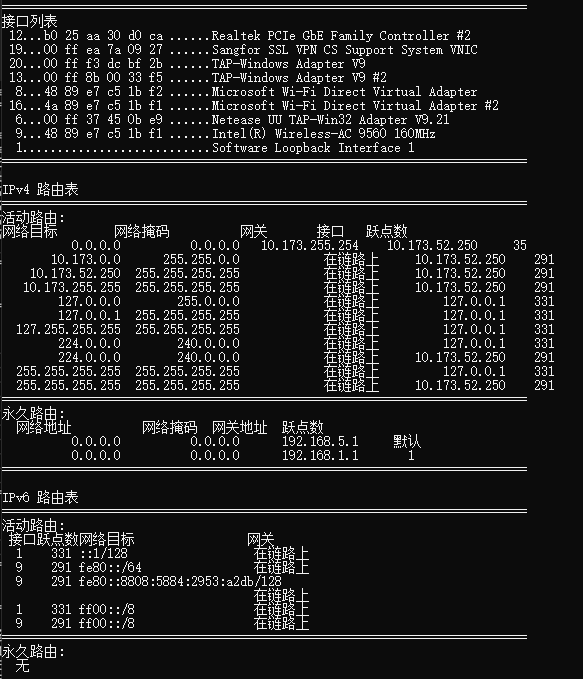
（注意将name、IP地址等参数改为自己电脑网卡的实际参数）】







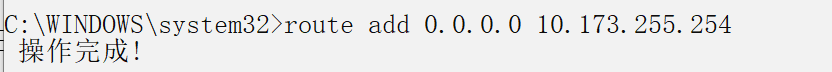
步骤3：查看并记录本机的路由表，标记出默认路由。用命令行删除默认路由，看看本机还能否上网并分析原因（如果还能上网，查看是否开启了IPv6，可禁用后再试）。查看网卡的默认网关配置是否还在？【参考命令：route print，route delete，ipconfig】

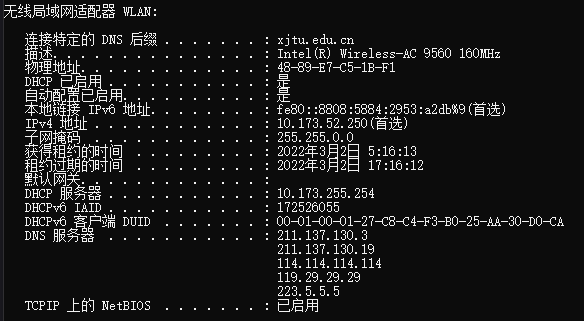




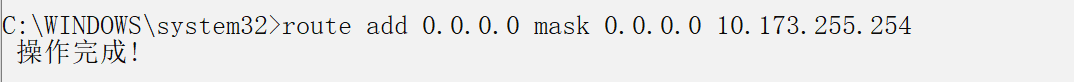


步骤4：分别用route add和route add -p增加一条默认路由，看看它们会出现在哪个路由表里，这两个路由表中的路由有什么不同？

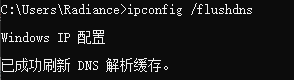


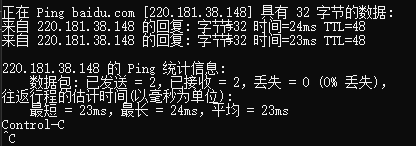


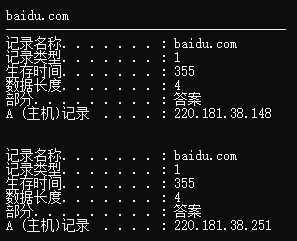




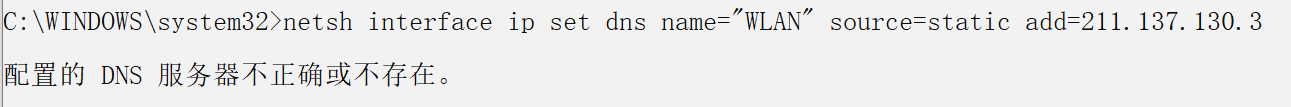
步骤5：在命令行运行ipconfig /flushdns清除本地DNS缓存，ping通一个网址（如www.xjtu.edu.cn）后，用ipconfig /displaydns查看本地DNS缓存，记录域名与IP地址。



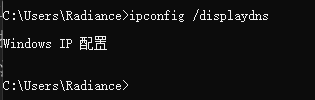




步骤6：把网卡的DNS服务器地址修改为无效DNS地址（如3.3.3.3），分别ping域名和IP地址看能否ping通，查看本地DNS缓存，记录结果并分析原因。【参考命令：netsh interface ip set dns name="本地连接" source=static add=3.3.3.3】



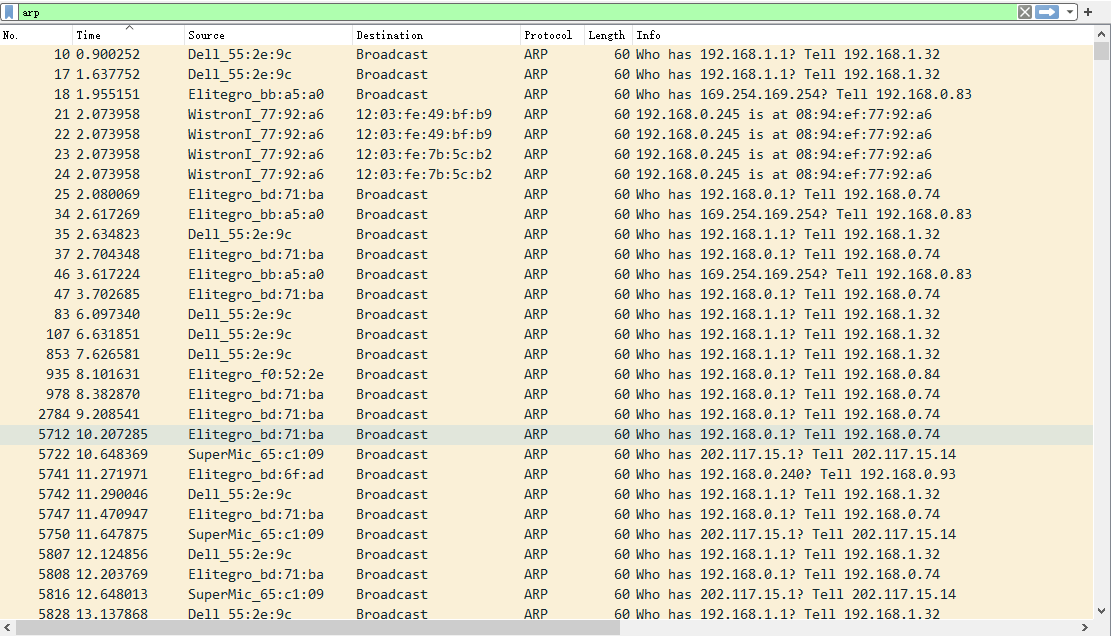


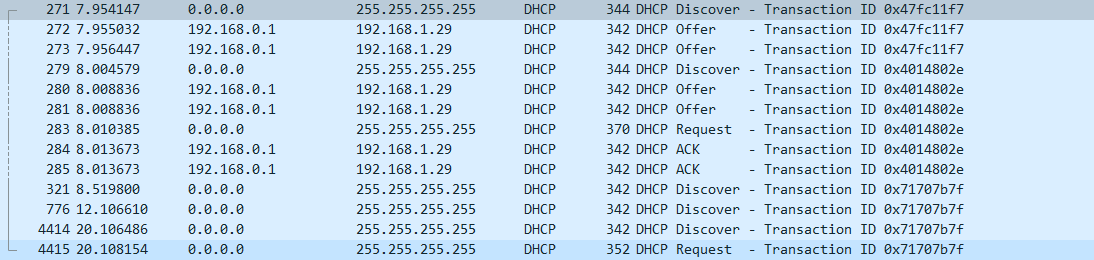


* 1. 网络分析工具练习

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。

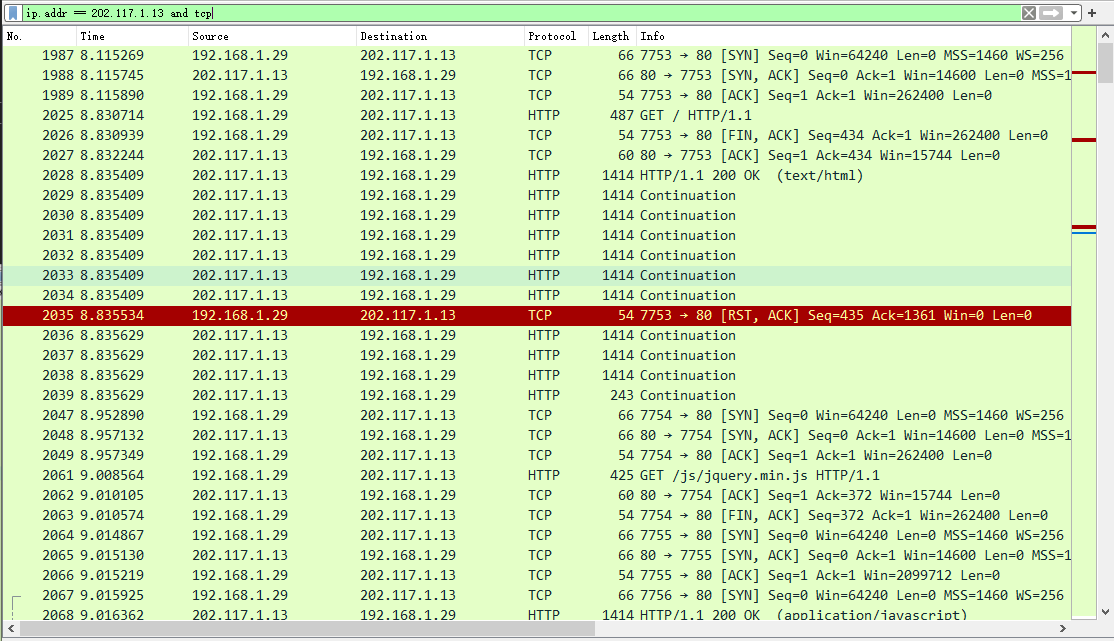
|  |  |  |
| --- | --- | --- |
| 协议名 | 描述项 | 配置值 |
| DHCP | 协议功能 | DHCP是动态主机设置协议的简称，主要用于内部网或网络服务供应商自动分配IP地址 |
| 源地址-目的地址 | 0.0.0.0（192.168.1.29） - 255.255.255.255（192.168.0.1） |
| 请求/应答信息 | DHCP Discover, Offer, Request, Ack |
| ARP | 协议功能 | IP地址对应MAC地址解析 |
| 源地址-目的地址 | 00:00:00\_00:00:03 - Private\_30:d0:ca |
| 请求/应答信息 | Who has 192.168.1.29? Tell 192.168.0.1  192.168.1.29 is at b0:25:aa:30:d0:ca |

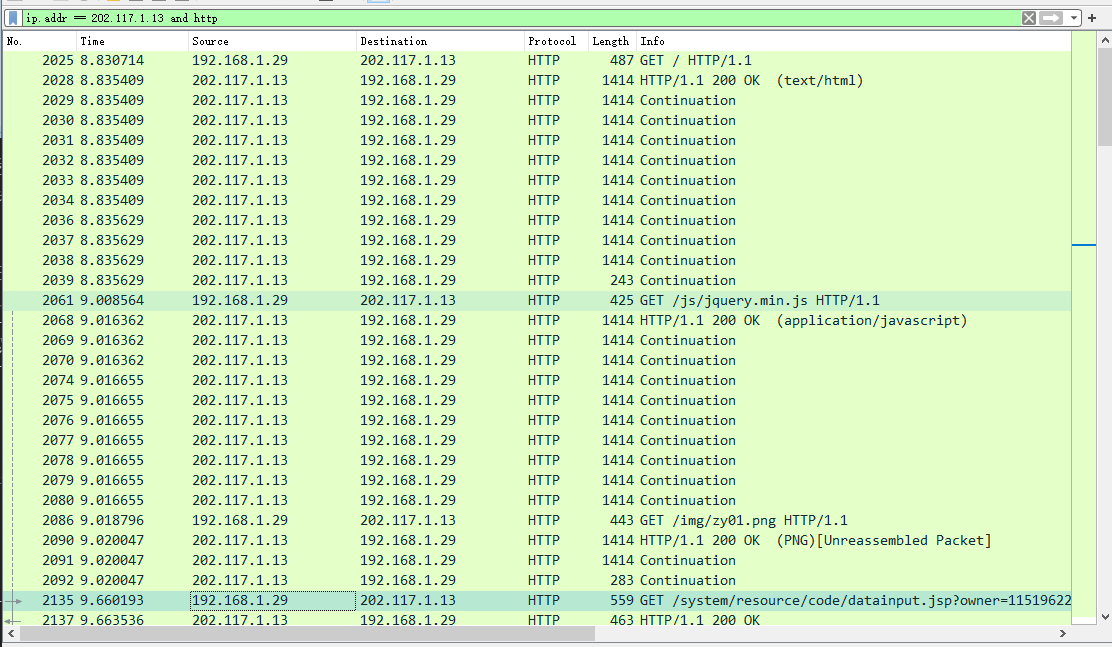




步骤2：清除本机的DNS缓存【参考命令：ipconfig /flushdns】，运行Wireshark截获报文，浏览器访问网站（如<http://github.com>，浏览新闻，下载软件等），利用IP地址过滤筛选出访问该网站的报文，查看访问该网站时，都用到了哪些协议，主要作用是什么？【域名解析为IP地址方法：ping 域名，或nslookup 域名】

|  |  |  |
| --- | --- | --- |
| 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 | 202.117.1.13 - 192.168.1.29 |
| 请求/应答信息 | 7753 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK\_PERM=1  80 → 7753 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1360 SACK\_PERM=1 WS=128  7753 → 80 [ACK] Seq=1 Ack=1 Win=262400 Len=0 |
| HTTP | 协议功能 | HTTP协议是Hyper Text Transfer Protocol(超文本传输协议)的缩写，用于从万维网服务器传输超文本到本地浏览器的传送协议。 |
| 源地址-目的地址 | 202.117.1.13 - 192.168.1.29 |
| 请求/应答信息 | 487 GET / HTTP/1.1  HTTP/1.1 200 OK (text/html) |





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 |  |
| 本机IP地址 |  |
| 本机自测公网地址 |  |
| 通信好友的IP地址 |  |
| 通信协议（Protocol） |  |
| 通信源端口-目的端口 |  |

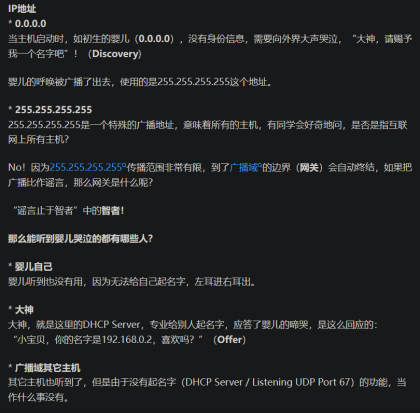
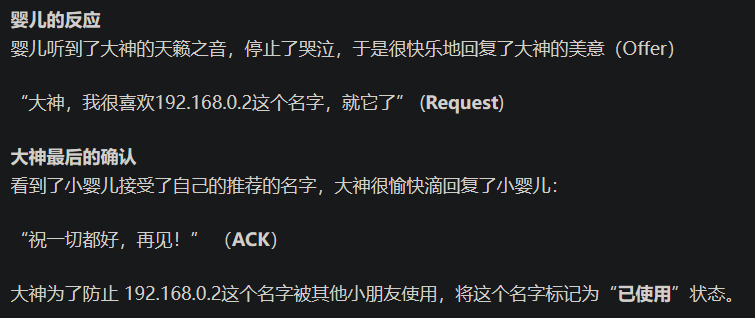
好友端捕获信息

|  |  |
| --- | --- |
| 描述项 | 值 |
| QQ/微信服务器地址 |  |
| 通信好友IP地址 |  |
| 通信好友自测公网地址 |  |
| 好友看到的我的IP地址 |  |
| 通信协议（Protocol） |  |
| 通信源端口-目的端口 |  |

* 1. 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. 主机需要获取内网IP 地址，可通过DHCP服务器自动获取，或者手动得到。

1. 选自：<https://www.zhihu.com/question/267097519/answer/318401587>
2. 路由器和主机都需要知道对方内网IP 地址到物理地址的映射，通过ARP通信得到。
3. 主机若需要访问网站域名，使用DNS 协议，域名解析总体可分为一下过程：

(1) 输入域名后, 先查找自己主机对应的域名服务器，域名服务器先查找自己的数据库中的数据.

(2) 如果没有， 就向上级域名服务器进行查找， 依次类推

(3) 最多回溯到根域名服务器, 肯定能找到这个域名的IP地址

(4) 域名服务器自身也会进行一些缓存， 把曾经访问过的域名和对应的IP地址缓存起来, 可以加速查找过程

1. 内网主机和公网通信，需要路由器通过NAT协议。

NAT不仅能解决了lP地址不足的问题，而且还能够有效地避免来自网络外部的攻击，隐藏并保护网络内部的计算机。把内网的私有地址，转化成外网的公有地址。使得内部网络上的（被设置为私有IP地址的）主机可以访问Internet。

* 1. \*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。】

1. 总结及心得体会