实验一 常用网络命令及工具实验报告

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 组号： |  |  |  |  |  |
| 姓名： |  | 学号： |  | 班级： |  |
|  |  |  |  |  |  |

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。

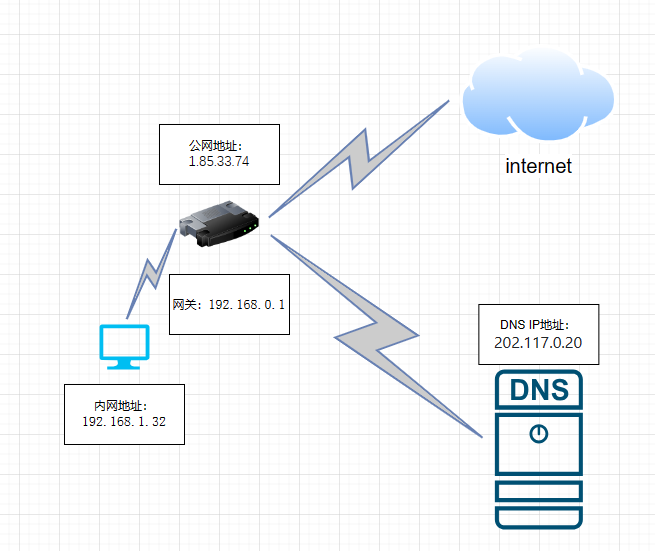
1. 实验内容

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，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】





一共有7个网卡，其中第4和第5个网卡（以VMware开头的两个网卡）为为虚拟机配置的虚拟网卡，剩余的为物理网卡

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 | 无线局域网适配器 WLAN |
| IP地址 | 192.168.1.32(首选) |
| 子网掩码 | 255.255.254.0 |
| 默认网关 | 192.168.0.1 |
| DNS服务器 | 202.117.0.20和1.2.4.8 |

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="无线局域网适配器 WLAN" static 192.168.1.123 255.255.254.0 192.168.0.1；

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；

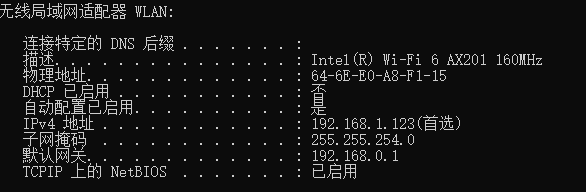
DNS服务器地址自动获取设置命令：netsh interface ip set dns name="本地连接" source=dhcp。

（注意将name、IP地址等参数改为自己电脑网卡的实际参数）】

执行命令 手动设置ip为192.168.1.123

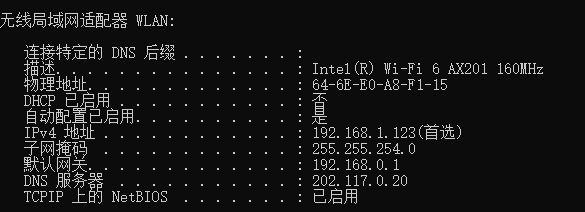
netsh interface ip set address name="WLAN" static 192.168.1.123 255.255.254.0 192.168.0.1

可以发现租约时间没有了，即持续占有



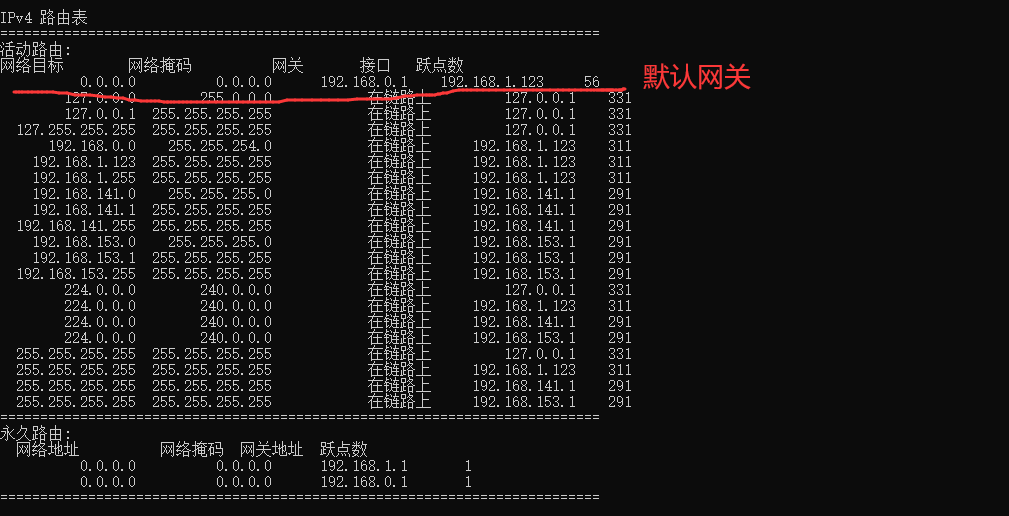
执行命令 手动设置DNS为202.117.0.20（DNS必须真实存在，否则会设置失败）

etsh interface ip set dns name="WLAN" source=static add=202.117.0.20



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】

执行route print

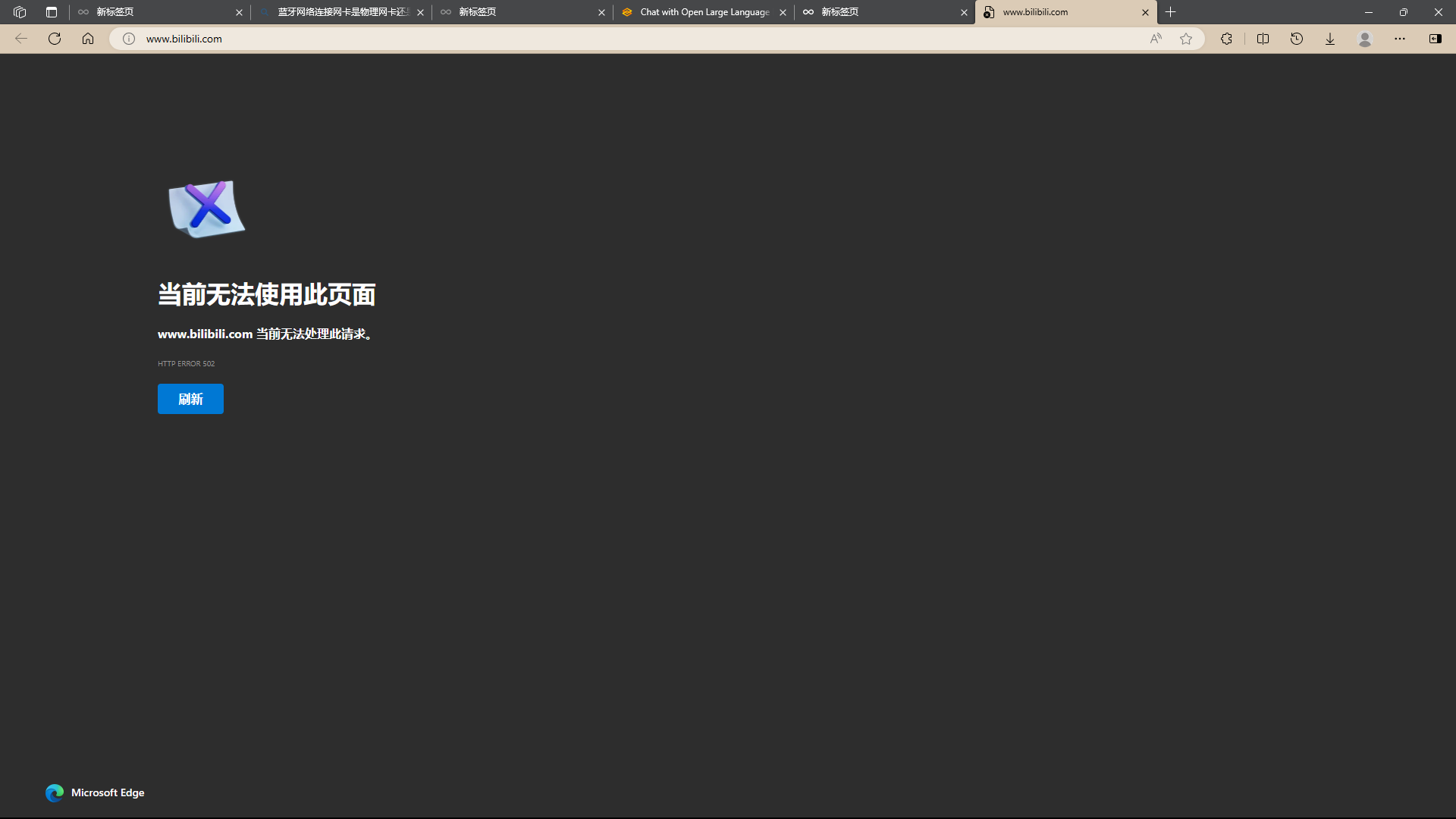


默认路由为 0.0.0.0/0.0.0.0 192.168.0.1

执行route delete 0.0.0.0 mask 0.0.0.0 192.168.0.1



已经无法上网



分析原因：路由表中除去默认路由的表项都是用于内部网络连接，当访问外部网站（此处为 [www.bilibili.com），dns](http://www.bilibili.com），dns)解析后无法与剩余的任意一个目标路由匹配。默认路由(0.0.0.0/0)是一种特殊的路由规则,它匹配所有目标IP地址。当数据包的目标IP地址不属于本地网络时,默认路由规则就会生效,将数据包发送到默认网关。如果删除了默认路由,计算机将无法与本地网络以外的设备通信,因为它不知道如何到达外部网络。

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？

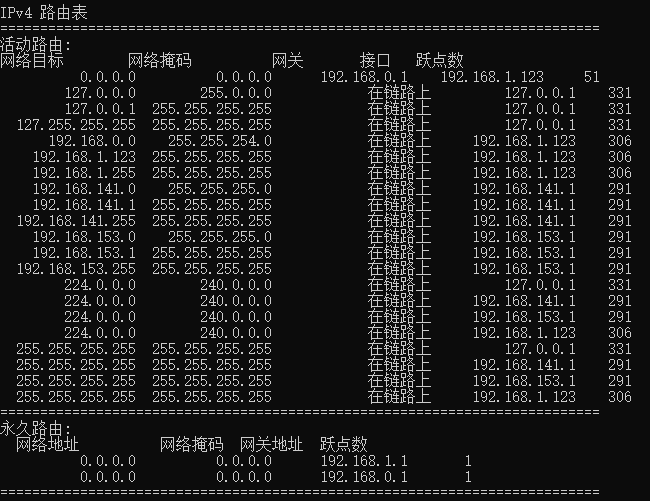
执行 route add 0.0.0.0 mask 0.0.0.0 192.168.0.1

此路由会出现在IPv4路由表中



执行 route add 0.0.0.0 mask 0.0.0.0 192.168.0.1

会添加192.168.0.0到永久路由中



1. IPv4 路由表:

1. IPv4 路由表是当前活动的路由表,它包含计算机当前使用的所有 IPv4 路由条目。

2. 这些路由条目可以通过各种方式添加,例如手动配置、DHCP、路由协议等。

3. IPv4 路由表中的条目可以被动态修改或删除,例如通过 "route add" 或 "route delete" 命令。

4. 当计算机重新启动时,IPv4 路由表中的动态条目将会丢失,需要重新建立。

5. IPv4 路由表用于确定 IPv4 数据包的转发方式,以便将数据包发送到正确的目标。

2. 永久路由表:

1. 永久路由表包含在计算机重新启动后仍然保持不变的路由条目。

2. 这些路由条目通常是在系统启动时从注册表或配置文件中加载的。

3. 永久路由表中的条目在计算机运行期间不会被动态修改或删除,除非手动编辑注册表或配置文件。

4. 当计算机重新启动时,永久路由表中的条目会自动恢复,无需重新配置。

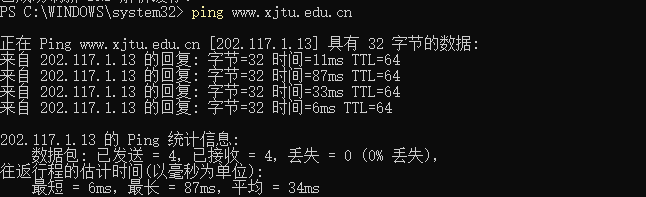
5. 永久路由表用于确保某些关键路由在计算机重启后仍然存在,例如用于连接到特定网络或设备的路由。

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。

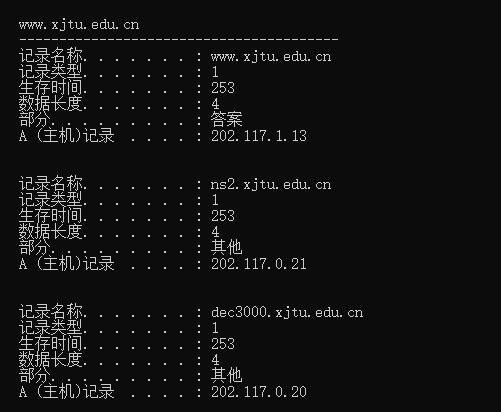
执行ipconfig /flushdns



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



执行ipconfig /displaydns



www.xjtu.edu.cn为目标网址

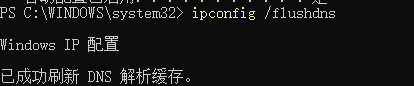
ns2.xjtu.edu.cn可能为辅助dns

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】

执行netsh interface ip set dns name="WLAN" source=static add=202.117.1.123



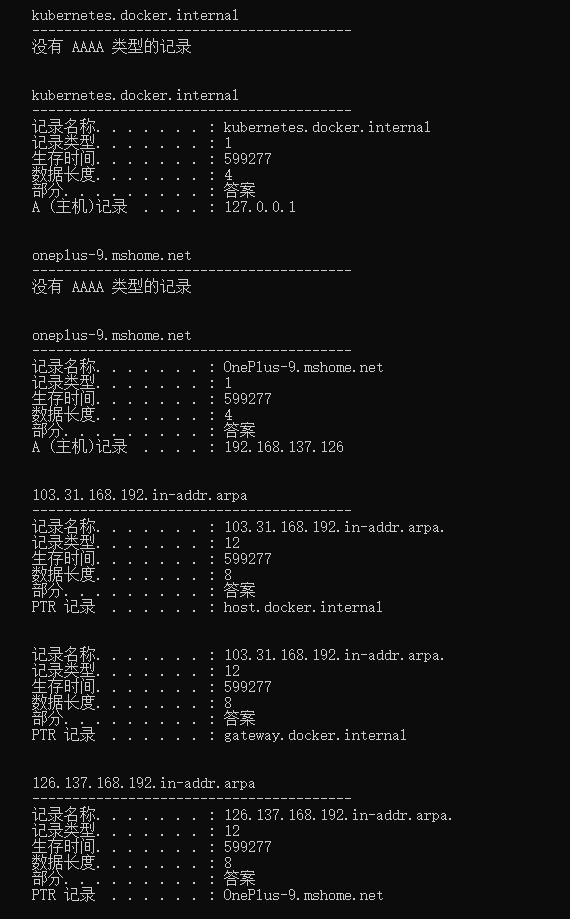
清除dns缓存以防止干扰

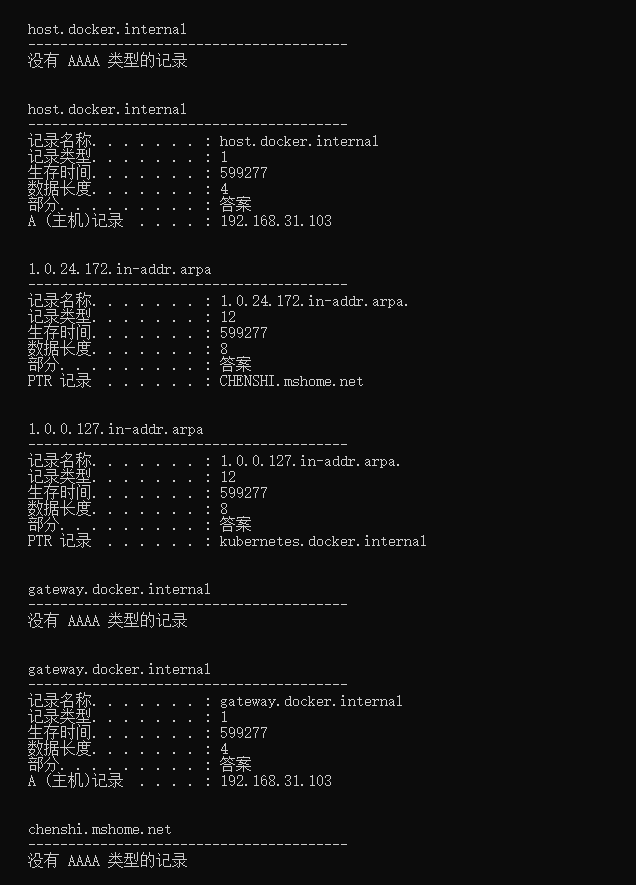


执行ping [www.bilibili.com](http://www.bilibili.com)

. 

查看dns缓存





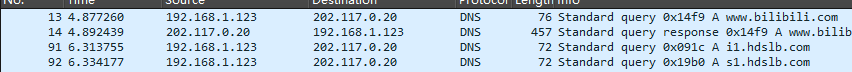
可以看到没有ping [www.bilibili.com的dns](http://www.bilibili.com的dns)缓存

原因分析：因为我们修改的dns服务器并不存在，所以当我们输入一个网址的时候，对网址的解析查询会发送到一个不存在的dns服务器，自然是查询不到目标网址所对应的ip地址，所以无法ping通

* 1. 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。

DNS协议



请求报文

Domain Name System (query)

Transaction ID: 0x14f9

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

www.bilibili.com: type A, class IN

[Response In: 14]

应答报文

Domain Name System (response)

Transaction ID: 0x14f9

Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 3

Authority RRs: 2

Additional RRs: 16

Queries

www.bilibili.com: type A, class IN

Answers

www.bilibili.com: type CNAME, class IN, cname a.w.bilicdn1.com

a.w.bilicdn1.com: type A, class IN, addr 121.194.11.73

a.w.bilicdn1.com: type A, class IN, addr 121.194.11.72

Authoritative nameservers

bilicdn1.com: type NS, class IN, ns ns3.dnsv5.com

bilicdn1.com: type NS, class IN, ns ns4.dnsv5.com

Additional records

ns3.dnsv5.com: type A, class IN, addr 36.155.149.211

ns3.dnsv5.com: type A, class IN, addr 49.234.175.103

ns3.dnsv5.com: type A, class IN, addr 125.94.59.200

ns3.dnsv5.com: type A, class IN, addr 163.177.5.75

ns3.dnsv5.com: type A, class IN, addr 1.12.0.17

ns3.dnsv5.com: type A, class IN, addr 1.12.0.18

ns3.dnsv5.com: type A, class IN, addr 1.12.0.20

ns4.dnsv5.com: type A, class IN, addr 117.89.178.200

ns4.dnsv5.com: type A, class IN, addr 120.241.130.93

ns4.dnsv5.com: type A, class IN, addr 152.136.2.235

ns4.dnsv5.com: type A, class IN, addr 1.12.0.16

ns4.dnsv5.com: type A, class IN, addr 1.12.0.19

ns4.dnsv5.com: type A, class IN, addr 1.14.119.123

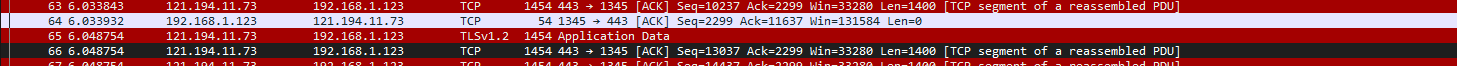
ns4.dnsv5.com: type A, class IN, addr 112.80.181.106

ns3.dnsv5.com: type AAAA, class IN, addr 2402:4e00:1430:11f9:0:983e:2e27:2604

ns4.dnsv5.com: type AAAA, class IN, addr 2402:4e00:111:fff::8

[Request In: 13]

[Time: 0.015179000 seconds]



TCP报文1

Transmission Control Protocol, Src Port: 1345, Dst Port: 443, Seq: 2299, Ack: 11637, Len: 0

Source Port: 1345

Destination Port: 443

[Stream index: 5]

[Conversation completeness: Complete, WITH\_DATA (31)]

[TCP Segment Len: 0]

Sequence Number: 2299 (relative sequence number)

Sequence Number (raw): 3435749165

[Next Sequence Number: 2299 (relative sequence number)]

Acknowledgment Number: 11637 (relative ack number)

Acknowledgment number (raw): 3486032410

0101 .... = Header Length: 20 bytes (5)

Flags: 0x010 (ACK)

Window: 514

[Calculated window size: 131584]

[Window size scaling factor: 256]

Checksum: 0xc1cd [unverified]

[Checksum Status: Unverified]

Urgent Pointer: 0

[Timestamps]

[SEQ/ACK analysis]

TCP报文2  
 Frame 66: 1454 bytes on wire (11632 bits), 1454 bytes captured (11632 bits) on interface \Device\NPF\_{949EE175-03C1-41A5-8774-29A29F050622}, id 0

Ethernet II, Src: MicroStarINT\_ae:3e:a6 (6c:62:6d:ae:3e:a6), Dst: Intel\_a8:f1:15 (64:6e:e0:a8:f1:15)

Internet Protocol Version 4, Src: 121.194.11.73, Dst: 192.168.1.123

Transmission Control Protocol, Src Port: 443, Dst Port: 1345, Seq: 13037, Ack: 2299, Len: 1400

Source Port: 443

Destination Port: 1345

[Stream index: 5]

[Conversation completeness: Complete, WITH\_DATA (31)]

[TCP Segment Len: 1400]

Sequence Number: 13037 (relative sequence number)

Sequence Number (raw): 3486033810

[Next Sequence Number: 14437 (relative sequence number)]

Acknowledgment Number: 2299 (relative ack number)

Acknowledgment number (raw): 3435749165

0101 .... = Header Length: 20 bytes (5)

Flags: 0x010 (ACK)

Window: 65

[Calculated window size: 33280]

[Window size scaling factor: 512]

Checksum: 0xa2a1 [unverified]

[Checksum Status: Unverified]

Urgent Pointer: 0

[Timestamps]

[SEQ/ACK analysis]

TCP payload (1400 bytes)

[Reassembled PDU in frame: 75]

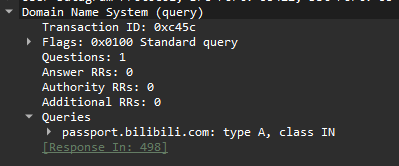
TCP segment data (1400 bytes)

|  |  |  |
| --- | --- | --- |
| 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* |
| DNS | 协议功能 | 域名解析为IP地址,实现域名到IP地址的映射 |
| 源地址-目的地址 | 请求DNS解析时,源地址是发起请求的主机IP,目的地址是DNS服务器的IP(192.168..1.123->202.117.0.20)  应答DNS解析时,源地址是DNS服务器IP,目的地址是请求主机的IP(202.117.0.20->192.168.1.123 |
| 请求/应答信息 | 请求信息包含要查询的域名,查询类型(A记录等)等(www.bilibili.com)  应答信息包含域名对应的IP地址,TTL存活时间等(121.194.11.73) |
| *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 | 192.168.1.123-> 121.194.11.73(bilibili的ip地址) |
| 请求/应答信息 | 请求：1345 → 443 [ACK] Seq=2299 Ack=11637 Win=131584 Len=0  响应：443 → 1345 [ACK] Seq=13037 Ack=2299 Win=33280 Len=1400 [TCP segment of a reassembled PDU] |

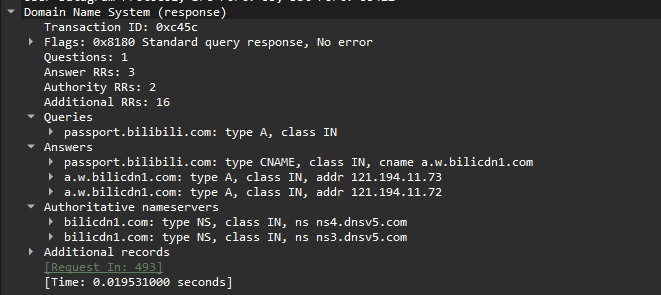
步骤2：清除本机的DNS缓存【参考命令：ipconfig /flushdns】，运行Wireshark截获报文，浏览器访问网站（如<http://github.com>，浏览新闻，下载软件等），利用IP地址过滤筛选出访问该网站的报文，查看访问该网站时，都用到了哪些协议，主要作用是什么？【域名解析为IP地址方法：ping 域名，或nslookup 域名】

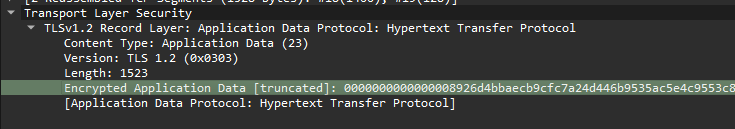
访问网址[www.bilibili.com](http://www.bilibili.com)

DNS协议请求



DNS响应

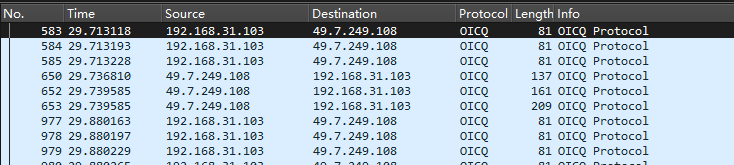


TLSv2协议  
 

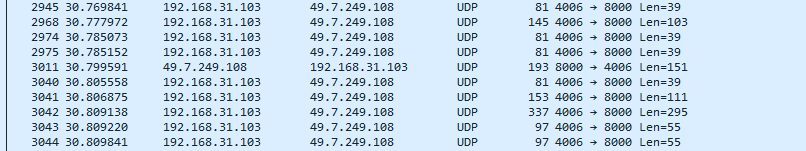
|  |  |  |
| --- | --- | --- |
| 协议名 | 描述项 | 配置值 |
| *例：TCP* | *协议功能* | *传输控制协议,在不可靠的互联网络上提供可靠的端到端传输。* |
| *源地址-目的地址* | *192.168.0.101 - 182.61.200.6* |
| *请求/应答信息* | *49947 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK\_PERM=1* |
| DNS | 协议功能 | 域名解析为IP地址,实现域名到IP地址的映射 |
| 源地址-目的地址 | 请求DNS解析时,源地址是发起请求的主机IP,目的地址是DNS服务器的IP(192.168..1.123->202.117.0.20)  应答DNS解析时,源地址是DNS服务器IP,目的地址是请求主机的IP(202.117.0.20->192.168.1.123 |
| 请求/应答信息 | 请求信息包含要查询的域名,查询类型(A记录等)等(www.bilibili.com)  应答信息包含域名对应的IP地址,TTL存活时间等(121.194.11.73) |
| TLSv1.2 | 协议功能 | 一种加密通信协议,用于在互联网上提供安全通信 |
| 源地址-目的地址 | 192.168.1.123-> 121.194.11.73(bilibili的ip地址) |
| 请求/应答信息 | Application Data（加密后的数据，长度很长，wireshark中展示是进行了截断处理） |

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。

OICQ



视频通话采用UDP协议，因为视频传输对丢包有一定容忍度,偶尔丢失一些数据对视频质量影响不大视频传输对实时性要求很高,不能容忍过多的延迟



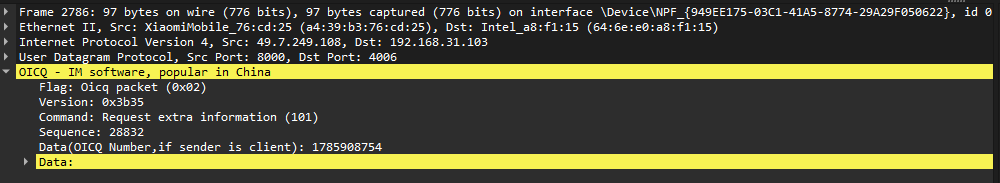
本机捕获信息（这部分是回寝室做的，所以ip和前面的不同）

|  |  |
| --- | --- |
| 描述项 | 值 |
| QQ/微信服务器地址 | 49.7.249.108 |
| 本机IP地址 | 192.168.31.103 |
| 本机自测公网地址 | 1.85.33.74 |
| 通信好友的IP地址 | 192.168.31.123 |
| 通信协议（Protocol） | UDP |
| 通信源端口-目的端口 | 192.168.31.103->49.7.249.108 |

好友端捕获信息

|  |  |
| --- | --- |
| 描述项 | 值 |
| QQ/微信服务器地址 | 49.7.249.108 |
| 本机IP地址 | 192.168.31.123 |
| 本机自测公网地址 | 111.18.34.134 |
| 通信好友的IP地址 | 192.168.31.103 |
| 通信协议（Protocol） | UDP |
| 通信源端口-目的端口 | 192.168.31.123->49.7.249.108 |

登录，发消息的时候使用oicq协议



可以发现oicq协议是使用udp协议来封装的

视频通话采用UDP协议，因为视频传输对丢包有一定容忍度,偶尔丢失一些数据对视频质量影响不大视频传输对实时性要求很高,不能容忍过多的延迟

* 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）。

IP地址设置

计算机需要获取一个有效的IP地址,可以手动设置静态IP地址,也可以启用DHCP自动获取动态IP地址。

网关设置

设置默认网关地址,通常是路由器或网络出口设备的IP地址,用于连接外部网络。

DNS设置

设置DNS服务器地址,用于将域名解析为IP地址。可以使用本地路由器提供的DNS地址,也可以使用公共DNS服务器。

启用TCP/IP协议

启用TCP/IP协议栈,它是互联网上使用的核心网络协议。

启用DNS客户端服务

启用DNS客户端服务,用于向DNS服务器发送解析请求,获取域名对应的IP地址。

检查防火墙和网络安全设置

如果计算机上启用了防火墙或网络安全软件,需要检查并确保它们允许网络访问。

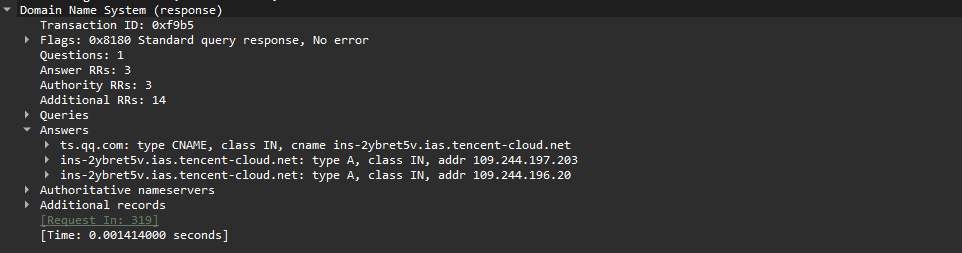
* 1. \*进阶自设计

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
2. DNS协议：查找QQ服务器的IP地址

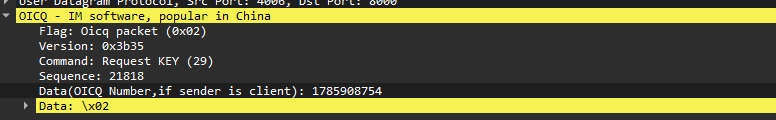




服务器地址：109.244.197.203

数据包标识：query 0xf9b5 A ts.qq.com

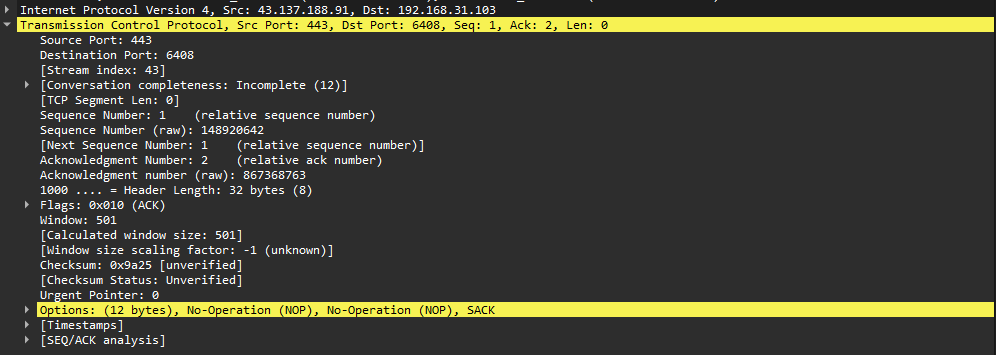
1. OICQ协议



服务器地址：49.7.249.108

该OICQ报文由本机（192.168.31.103）发送至QQ服务器（49.7.249.108），类型为Request KEY（29），目的是请求密钥，data字段为为1785908754，为登录的qq账号的qq号

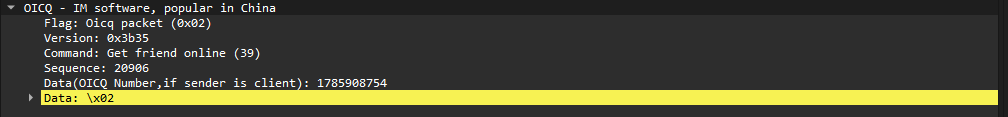
1. TCP协议

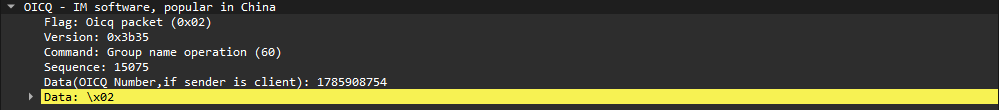


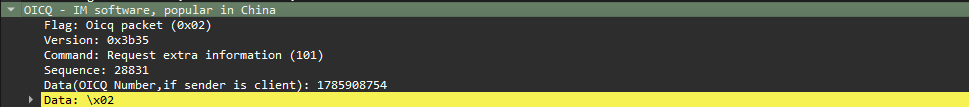
服务器地址：34.141.131.82

与qq服务器形成TCP握手连接

1. 登陆成功，信息加载
2. OICQ协议，用于命令传输，获取一些账号信息

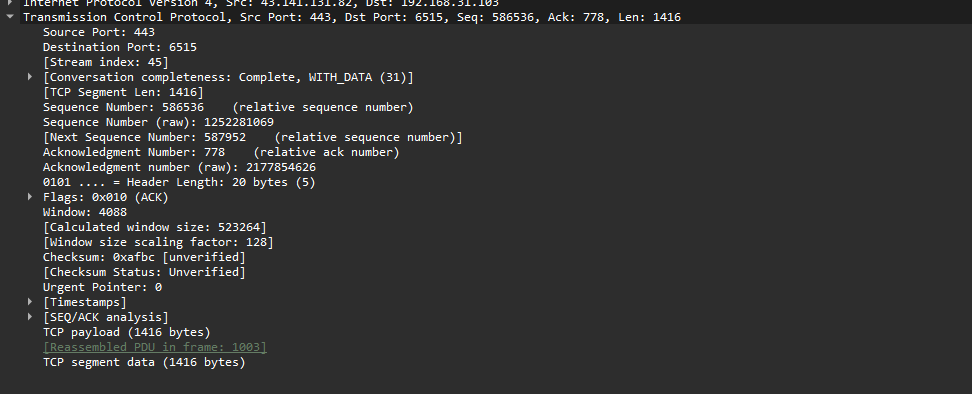






服务器地址：49.7.249.108

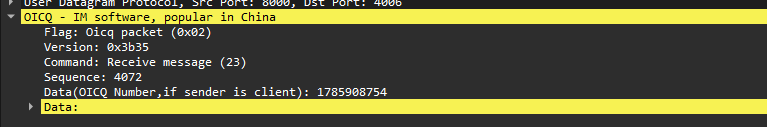
1. TCP协议，传递OICQ命令后，用于数据传输



服务器地址：43.141.131.82

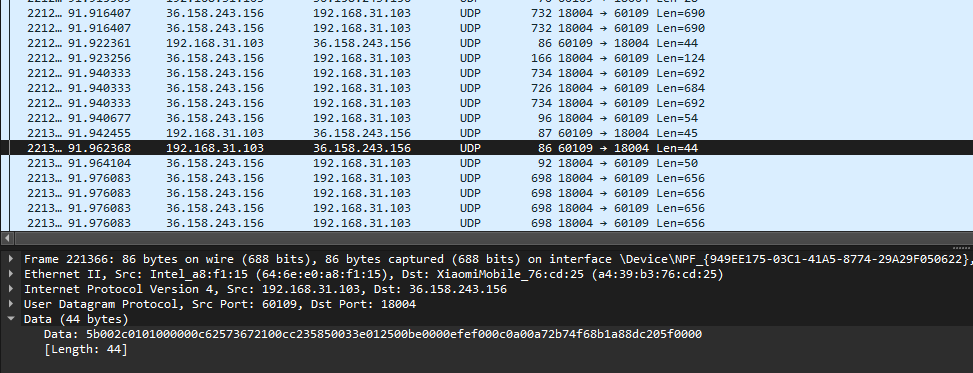
3．消息传输、语音/视频通话

1. OICQ协议：Command 字段分别有：Receive message、Get friend online、Group nameoperation、Request extra information、MEMO Operation、Heart Message、Set status、Get level 等



服务器ip：49.7.249.108

UPD协议：视频通话中进行数据交换



服务器地址：36.158.243.156

1. 登出
2. OICQ协议：



Command：Log out

服务器地址：58.60.10.45

1. 总结及心得体会

本实验旨在帮助我深入了解网络的运作原理，掌握常用网络命令的使用和网络抓包工具的应用。

网络命令使用

1. ping：用于测试网络连接性，通过向目标主机发送数据包并等待响应来判断网络是否畅通。
2. ipconfig：显示本机网络配置信息，包括IP地址、子网掩码、默认网关和DNS服务器。
3. route：查看和配置路由表，用于决定数据包在网络中传输的路径。

通过这些命令，我能够快速获取本机的网络信息，并对网络进行基本配置。

Wireshark抓包分析

Wireshark是一款强大的网络抓包工具，它可以捕获网络上传输的数据包并进行分析。本次实验中，我使用Wireshark抓取了以下网络活动：

QQ登录：分析了QQ登录过程中发送的认证请求和响应数据包，了解了QQ登录的认证机制。

消息传送：抓取了发送消息和接收消息的数据包，分析了消息传输过程中的协议交互和数据格式。

通过Wireshark的抓包分析，我深入了解了网络协议在实际应用中的工作原理，包括TCP、UDP、OICQ等协议。

实验成果

本次实验使我掌握了以下技能：

1. 熟练使用ping、ipconfig、route等网络命令。
2. 能够查看和配置本机的网络配置。

3. 能够使用Wireshark抓取和分析网络数据包。

4. 对网络协议在实际应用中的工作原理有了深入理解。

这些技能将为我今后的网络学习和应用奠定坚实的基础。