2022

实验四　网络部分综合实验

刘星雨

2020010850

目录

一、实验目的

1. 通过对网络接入过程的观察与分析，了解互连网协议栈的初始化过程，理解各层之间的地址映射机制的工作原理和实现方式
2. 以 web 网页请求为例，深入理解互连网协议栈的分层设计、封装关系与地址映射过程，体会互连网的设计理念
3. 借助 traceroute 等工具，尝试分析了解互连网网络核心的组成方式与工作原理

二、任务一 主机接入网络

1. 完成 ARP 表的清空操作后，操作系统信息：

2. 触发 DHCP 后操作系统信息：

   由下图可得到：

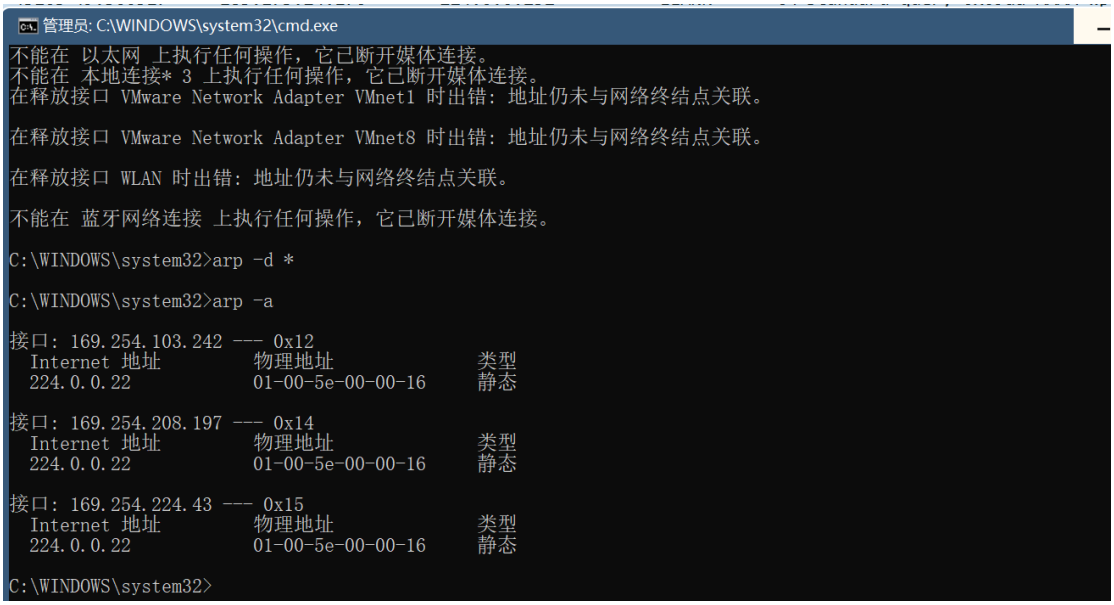
   本机 IP：183.173.100.83

   默认网关 IP：183.173.96.1

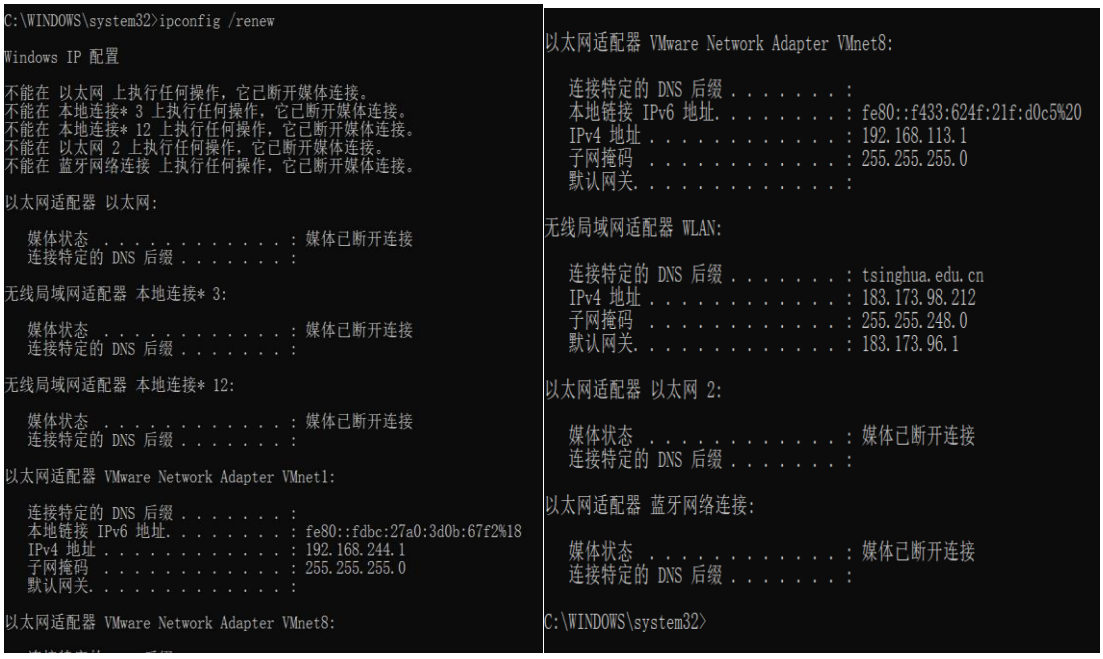
   子网掩码：255.255.248.0

   本机 MAC 地址：CC-15-31-91-58-16

   DNS 服务器：166.111.8.28　　166.111.8.29　　101.7.8.9

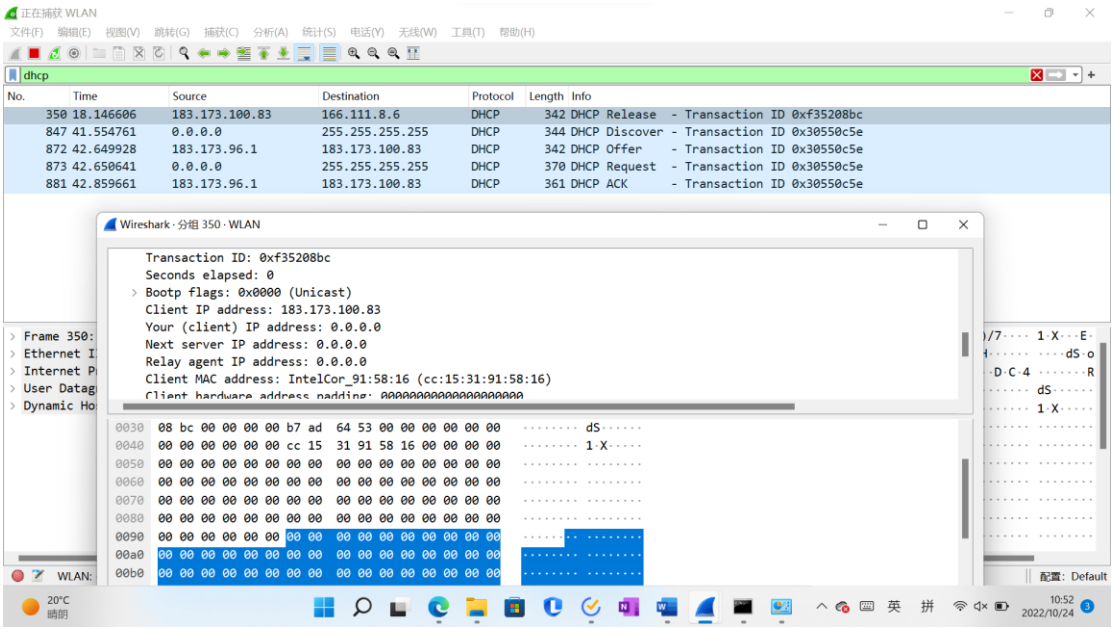


上图是清空后

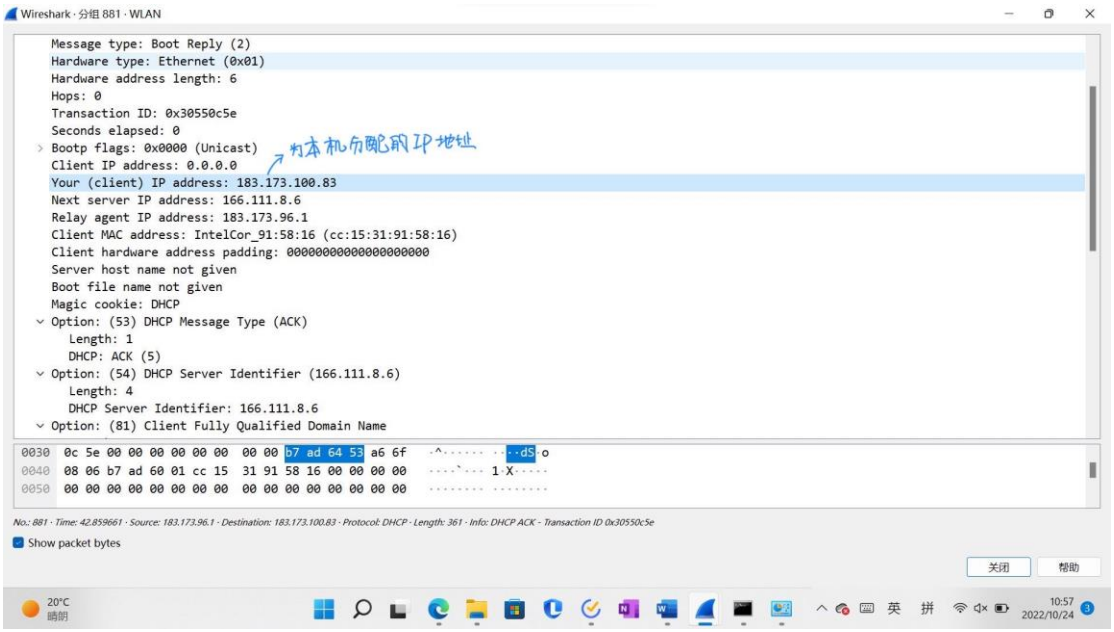


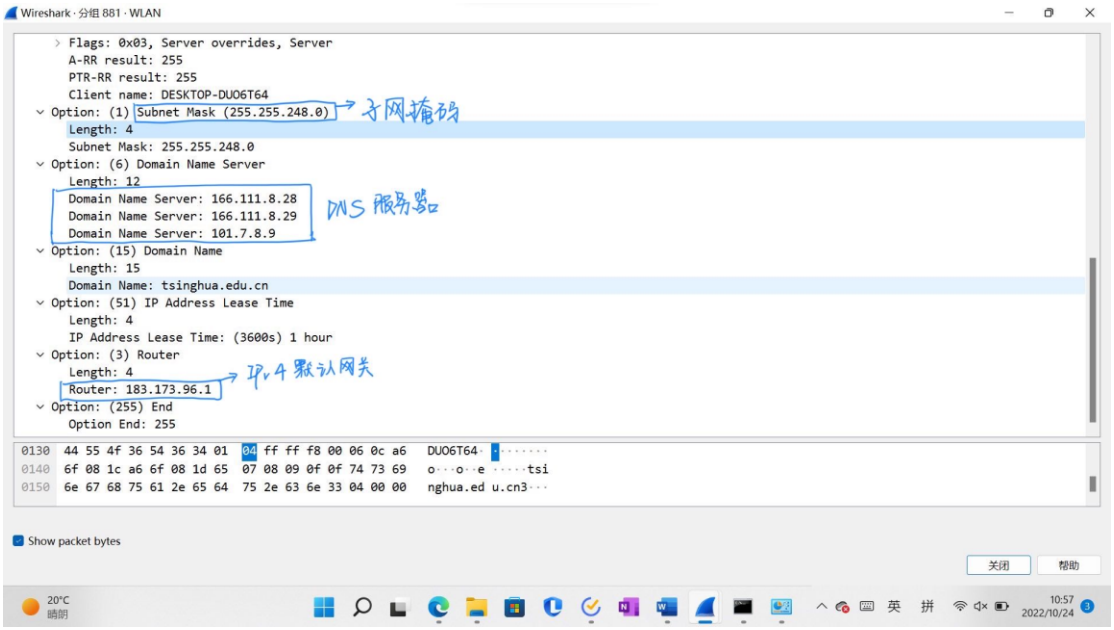
上图是是 renew 之后

3. DHCP 建立过程中的包，及其中分配的信息：



在 offer 包、ack 包中都能找到对应的信息：



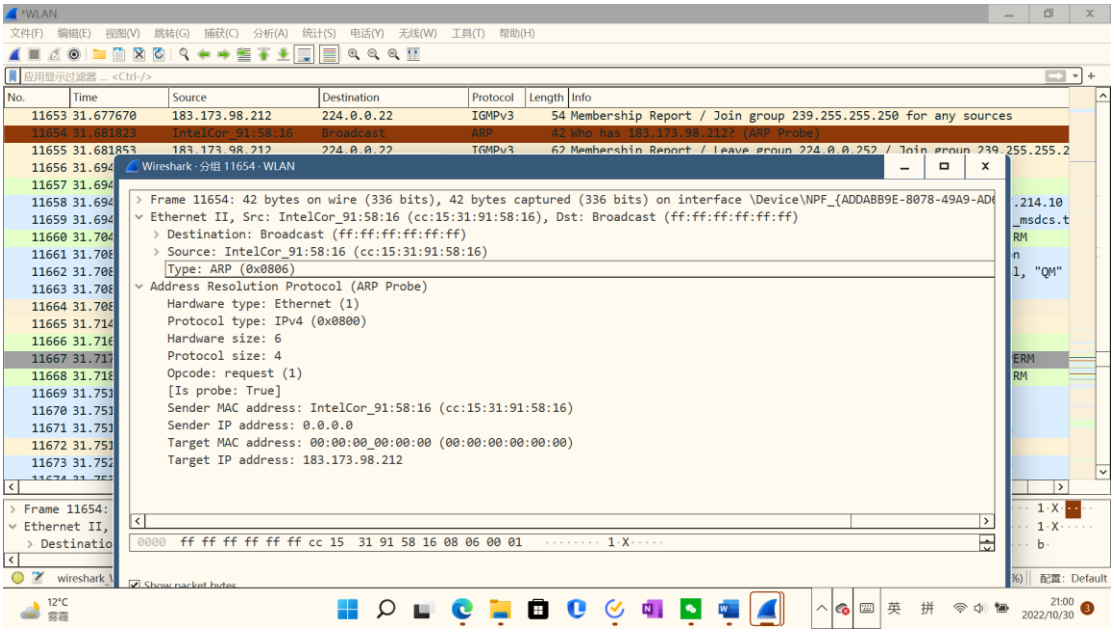


4. 对比操作系统中的信息与抓包得到的信息，指出两者之间的关系，并分析 DHCP 的工作过程。

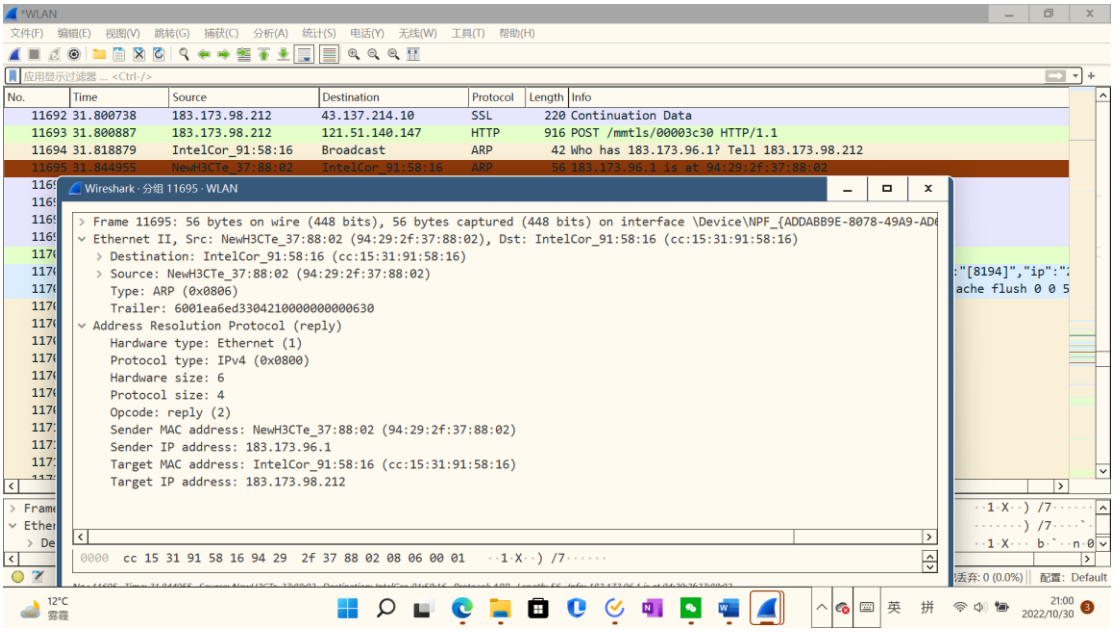
   操作系统中的 ip 地址、默认网关 ip 等信息都和抓包得到的信息一致。本机以地址 0.0.0.0 向外发送请求【discover】，DHCP 服务器 183.173.96.1 收到包并且向本机发送了尚未分配的 IP 地址以及子网掩码【offer】。本机收到【offer】，得到了 ip 地址，向所有的 DHCP 服务器再发送【request】，表示已经选择了 ip 地址。DHCP 服务器接收到【request】，回复【ack】，完成了 ip 的分配。

5. Release 包的后续报文中，找到请求网关 mac 地址对应的 arp 请求和响应

   此为请求网关 mac 地址，请求的 ip 地址为 183.173.98.212，广播的 mac 地址为 ff:ff:ff:ff:ff:ff



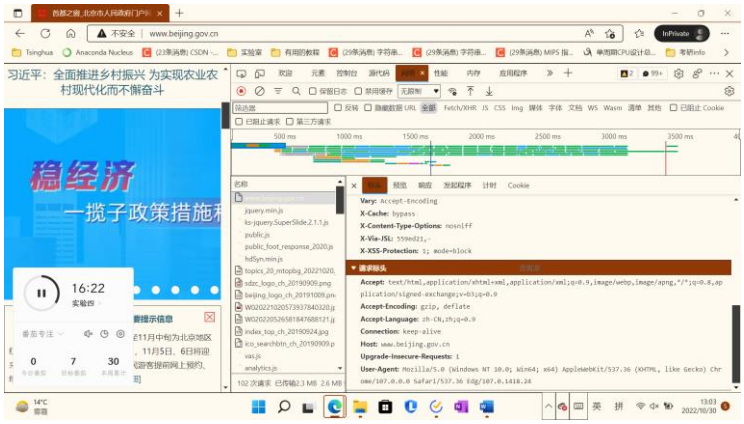
Mac 地址的相应包如下，响应的 mac 地址为 94：29：2f：37：88：02



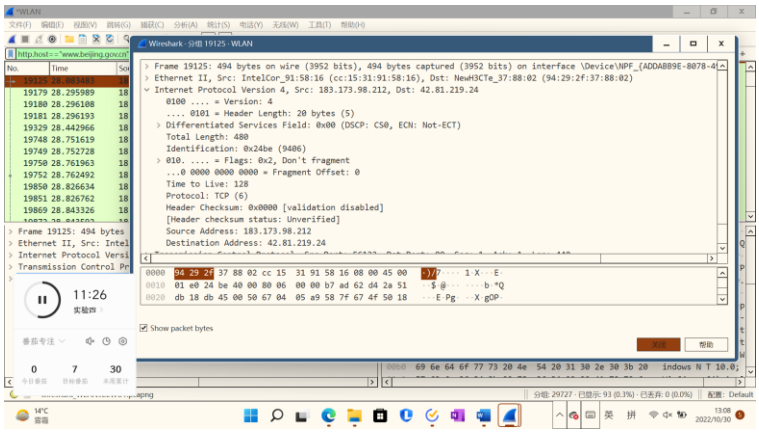
请求包的 mac 地址是相应包的 sender 的 mac 地址。本机向局域内广播请求 DHCP 服务器的 mac 地址，服务器听到后会向主机发送自己的 mac 地址。

三、 任务二 Web 网页应用

浏览器开发者工具的请求报文如图所示：



Wireshark 抓包得到的本机发出的第一条 http 请求报文如图：



1. 向 www.beijing.gov.cn 发出的第一条 http 报文

Ethernet II			
目的 mac 地址	源 mac 地址	类型	
94:29:2f:37:88:02	**Cc:15:31:91:58:16**	**Ipv4(0x0800)**	
IP(internet protocol version 4)			
版本	头部长度	服务类型	数据包长度
4	**20 bytes**	略	**480**
16bit 标识		标志	片偏移
0x24be(9406)		**0x2**	**0(not set)**
TTL	上层协议	头部检验和	
128	**TCP(6)**	**0x0000**	
32bit 源 IP 地址			
183.173.98.212			
32bit 目的 IP 地址			
42.81.219.24			
选项			
略			
TCP			
源端口号		目的端口号	

<table>
<tr><td colspan="5">56133</td><td colspan="4">80</td></tr>
<tr><td colspan="9">序号</td></tr>
<tr><td colspan="9">1728316841</td></tr>
<tr><td colspan="9">确认号</td></tr>
<tr><td colspan="9">1484744527</td></tr>
<tr><td>首部长度</td><td>保留
未用</td><td>URG</td><td>ACK</td><td>PSH</td><td>RST</td><td>SYN</td><td>FIN</td><td>接收窗口</td></tr>
<tr><td>20BYTES</td><td>略</td><td>0</td><td>1</td><td>1</td><td>0</td><td>0</td><td>0</td><td>258</td></tr>
<tr><td colspan="5">检验和</td><td colspan="4">紧急数据指针</td></tr>
<tr><td colspan="5">0x21be</td><td colspan="4">略</td></tr>
<tr><td colspan="9">选项</td></tr>
<tr><td colspan="9">略</td></tr>
<tr><td colspan="9">HTTP</td></tr>
<tr><td colspan="9">请求行：GET / HTTP/1.1\r\n</td></tr>
<tr><td colspan="4">Host:</td><td colspan="5">www.beijing.gov.cn\r\n</td></tr>
<tr><td colspan="4">User-agent:</td><td colspan="5">Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/537.36 Edg/107.0.1418.24\r\n</td></tr>
</table>

2. 自顶向下分析解释浏览器网页访问请求是如何被逐层封装的

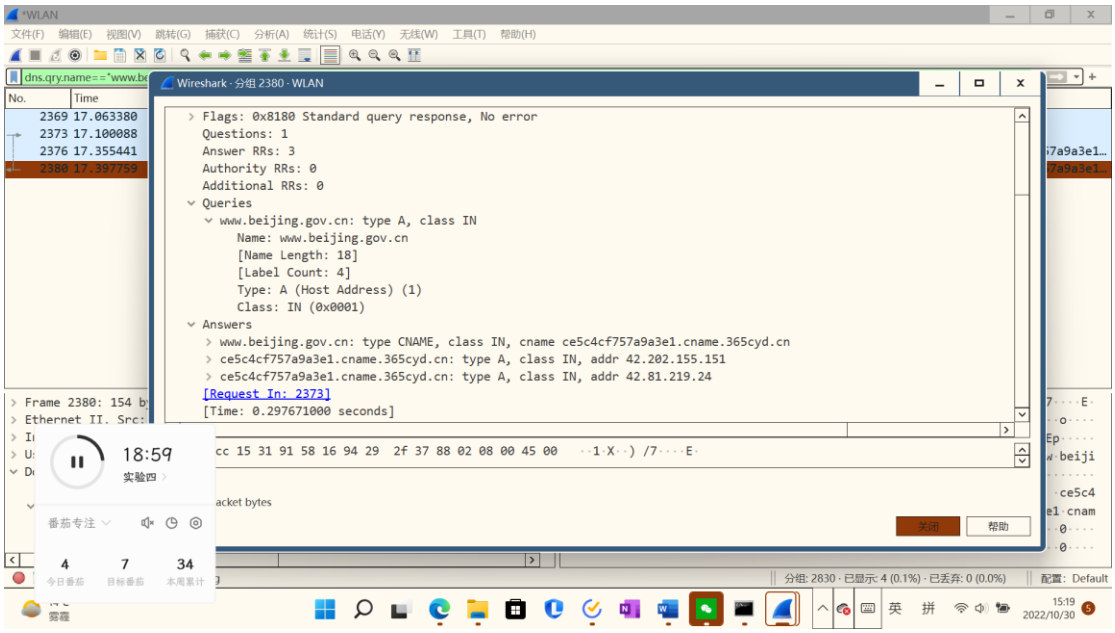
a) 应用层：此处网络应用采用 HTTP 协议，由请求行、消息头、消息体构成。请求行=请求方法【获取网页资源—GET】+URL+协议版本【HTTP/1.1】Host：访问的网址的主机 User-Agent：用户代理，即我们自己的主机。

b) 传输层：为运行在不同主机上的应用进程之间提供逻辑通信，传输层将来自应用进程的报文分组并加上传输层首部，封装为传输层报文段。源端口、目的端口使得报文段交付给正确的套接字。其中源端口来自主机，是源 IP 标识 TCP 报文的发送地，也用作返回地址。目的端口来自服务器，是目的 IP 地址标识该报文具体的发送目的地。

序号是发送的分组的第一个字节的序号，它保证了 TCP 传输的有序性。确认号即 ACK，表明下一个期待收到的字节序号，表明该序号之前的所有数据都已经准确无误地收到了。两者实现了有比特差错的丢包信道的可靠数据传输，他们由之前传输和接收的包的数目共同决定。首部长度指示了以 32bit 的字为单位的 TCP 首部长度。6bit 标志字段：URG：指示报文段里存在着被发送段的上层实体置为“紧急”的数据　ACK：指示确认字段中的值是有效的，即该报文段包括一个对已被成功接收的报文段的确认　RST、SYN、FIN 用于连接的建立和拆除　PSH 指示接收方应立即将数据交给上层接收窗口：用于流量控制。检验和：检测 TCP 包头和数据在发送端到接收端之间是否发生传输差错。

c) 网络层：网络层将传输层的报文段加上包头封装为网络层的报文。版本号规定了数据包 IP 版本，这里使用 Ipv4。头部长度，确定载荷实际开始的地方，一般为 20 字节。数据包长度指示数据包总长度。标识、标志、片偏移与 IP 分片有关。TTL 是数据包的寿命，确保数据报不会再网络中循环。上层协议指示数据应交给哪个传输层协议。头部检验和帮助路由器检测 IP 数据报中的比特错误。源 IP 地址由本机 IP 决定为 183.173.98.212，目的 IP 地址需要由 DNS 解析得到，如下图：主机发送请求给服务器 166.111.8.29 通过 dns 服务获得

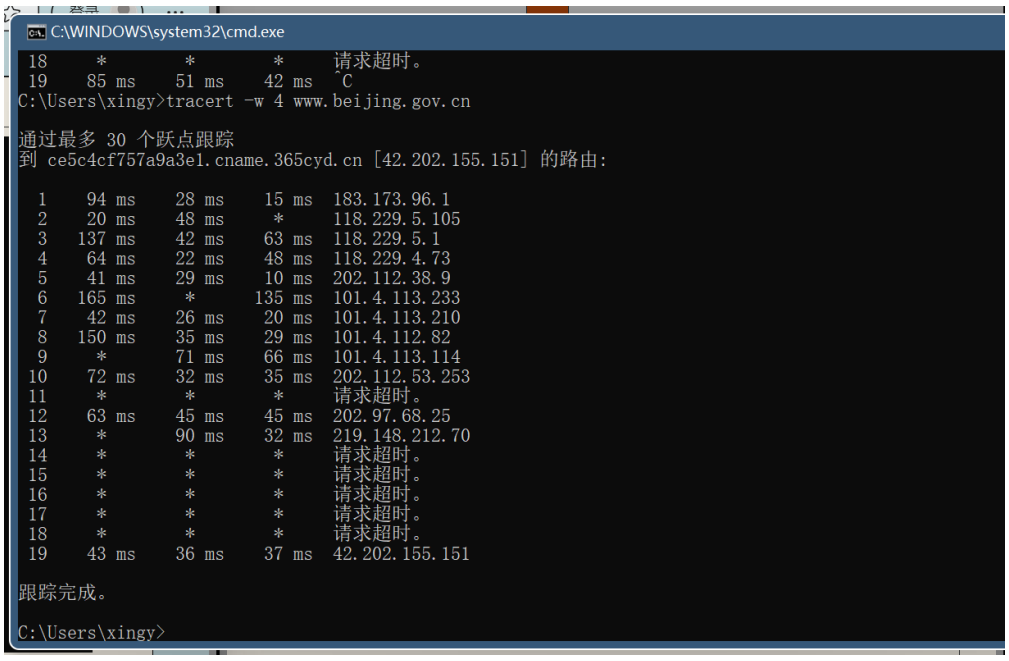
beijign.gov.cn 的 ip 地址为 42.81.219.24



d) 链路层：将网络层收到的报文加上包头封装为链路层的报文。Mac 地址由 ip 地址通过 arp 协议获得，标识了主机和客户端的物理地址。类型为 IP 协议类型。

四、任务三　traceroute

a) tracert 记录本机到 www.beijing.gov.cn 的各跳路由器 IP



b) 在线 IP 查询 tracert 中各跳路由器的物理位置

IP	物理位置
183.173.96.1	中国北京海淀　教育网
118.229.5.105	中国北京北京　教育网

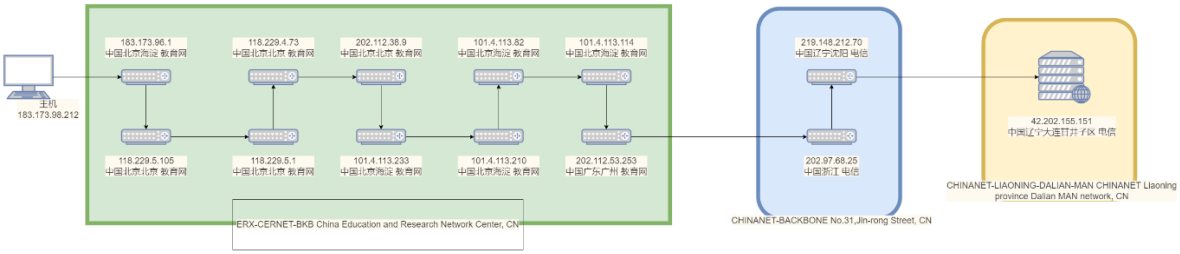
118.229.5.1	中国北京北京 教育网
118.229.4.73	中国北京北京 教育网
202.112.38.9	中国北京北京 教育网
101.4.113.233	中国北京海淀 教育网
101.4.113.210	中国北京海淀 教育网
101.4.112.82	中国北京海淀 教育网
101.4.113.114	中国北京海淀 教育网
202.112.53.253	中国广东广州 教育网
*	
202.97.68.25	中国浙江 电信
219.148.212.70	中国辽宁沈阳 电信
*****	
42.202.155.151	中国辽宁大连甘井子区 电信

c) 查找 tracert 中各跳路由对应的自治域

183.173.96.1	ERX-CERNET-BKB China Education and Research Network Center, CN
118.229.5.105	ERX-CERNET-BKB China Education and Research Network Center, CN
118.229.5.1	ERX-CERNET-BKB China Education and Research Network Center, CN
118.229.4.73	ERX-CERNET-BKB China Education and Research Network Center, CN
202.112.38.9	ERX-CERNET-BKB China Education and Research Network Center, CN
101.4.113.233	ERX-CERNET-BKB China Education and Research Network Center, CN
101.4.113.210	ERX-CERNET-BKB China Education and Research Network Center, CN
101.4.112.82	ERX-CERNET-BKB China Education and Research Network Center, CN
101.4.113.114	ERX-CERNET-BKB China Education and Research Network Center, CN
202.112.53.253	ERX-CERNET-BKB China Education and Research Network Center, CN
*	
202.97.68.25	CHINANET-BACKBONE No.31,Jin-rong Street, CN
219.148.212.70	CHINANET-BACKBONE No.31,Jin-rong Street, CN
*****	
42.202.155.151	CHINANET-LIAONING-DALIAN-MAN CHINANET Liaoning province Dalian MAN network, CN

d) 绘制本机到 www.beijing.gov.cn 的网络拓扑

利用 vscode 中的 drawio 插件的 network 标识库，绘制图如下：



五、思考题

a) 以太网数据更新

以太网帧中的数据报向下一条路由器转发时，新的以太网帧相对于当前的有哪些字段发生变化？路由器如何确定变化后的值？

以太网帧的源 mac 地址和目的 mac 地址发生了变化，新的源 mac 地址是当前路由器的 mac 地址，当前帧的目的 mac 地址。而新的目的 mac 地址是下一跳的路由器的 mac 地址，路由器通过查找路由表，并且通过 arp 协议转换得到下一跳的 mac 地址。新的帧中 TTL 应当减 1。

b) 在完成了网络部分的学习后，你有什么收获？

我清楚地了解了网络的层次结构，了解了网络发展完善的历史进程。在写代码的过程中，掌握了抓包和分析的基本能力。相对于从学长学姐们口中的通网，我能发现这个学期课程的网络部分有了很大的变化，改变了之前重通信而轻网络的格局，我觉得特别好，感谢老师和助教的辛苦付出！