网络部分综合实验报告

无04 2019012137 张鸿琳

实验目的

- 通过对网络接入过程的观察与分析，了解互联网协议栈的初始化过程，理解各层之间的地址映射（解析、转换）机制的工作原理和实现方式；
- 以Web网页请求为例，深入理解互联网协议栈的分层设计、封装关系与地址映射过程，体会互联网的设计理念；
- 借助traceroute等工具，尝试分析了解互联网网络核心部分的组成方式与工作原理。

实验内容

- 回顾互联网体系结构、协议栈以及各层协议的工作原理；
- 借助Wireshark抓包工具与操作系统网络工具观察并记录网络接入过程，分析了解DHCP、ARP等协议在互联网协议栈的初始化阶段所起的作用；
- 以Web网页请求为例，借助Wireshark抓包工具观察、记录并深入分析Web请求经过各层协议封装成为链路层帧的过程；
- 借助traceroute等工具，对从主机到网页服务器的路由路径进行探测，尝试分析在该路由路径上网络核心部分的拓扑关系，了解互联网网络核心部分组成方式与工作原理。

实验原理

互联网体系结构与协议栈

互联网以分组交换为基础，采用抽象、分层、封装的基本设计方法，经过几十年的实践，设计并实现了包含应用层、传输层、网络层、链路层与物理层的互联网协议栈，并以网络间互联的方式形成了现有的互联网结构——网络的网络。

本课程以自顶向下的视角介绍了互联网协议栈各个层次的基本功能、提供的服务、主要的协议。

应用层，课程介绍了常见的网络应用程序结构与进程通信原理，以HTTP为代表介绍了常见的应用层协议，并通过实验一帮助同学们理解客户端/服务器结构下的网络应用实现方式与Socket编程接口。

传输层，课程首先说明了传输层要提供的基本服务——主机进程间的逻辑通信，其次深入介绍了可靠数据传输原理与UDP、TCP协议，并通过实验二帮助同学们掌握TCP协议的连接建立与拆除过程、可靠数据传输的实现、流量控制的实现、拥塞控制的实现，对Wireshark这一重要的网络抓包分析工具形成一定认识。

网络层，课程从网络边缘转向网络核心，以网络层的两个重要功能——路由与转发开始，介绍网络层的“尽力而为”的服务模型、工作原理与实现。课程依次介绍了IP协议、IP地址编址、以链路状态法、距离向量法为代表的路由算法与相应的路由协议（OSPF、RIP）、针对互联网实际结构（网络的网络）的BGP协议、路由器内数据平面转发功能的基本原理和实现。同时，课程通过实验三帮助同学们在小型的仿真网络上运行并理解路由算法在网络中的工作方式。

链路层，课程介绍了链路层提供的基本服务，以ALOHA、CSMA等多路访问协议为例介绍了链路层中的关键问题——多路访问问题的解决方式，并介绍了链路层交换局域网的寻址、地址映射、常见技术（以太网）与交换机的作用。

网络配置的自动获取：DHCP

在主机接入互联网时，各层次协议栈需要获得大量的网络配置信息，例如本机IP地址、子网内的第一跳路由器（常称为默认网关）IP、子网掩码、DNS服务器地址等。为了避免用户手动配置导致的各种问题（如IP地址错误等），动态主机配置协议（Dynamic Host Configuration Protocol，DHCP）被用于自动化地完成上述初始化工作。

DHCP承载于UDP协议，其工作流程如下：

- 新接入网络的客户端发现本机没有任何IP设定，因此以广播的方式发送DHCP Discover包（即将目的IP设置为广播IP 255.255.255.255、目的MAC设为广播地址FF:FF:FF:FF:FF:FF），等待DHCP服务器进行响应。
- DHCP服务器接收到Discover包后，从尚未分配的IP池中挑选IP，以DHCP Offer包的形式发送给该客户端（此时DHCP服务器已知客户机MAC地址，无需广播发送）。
- 客户端收到DHCP Offer后，选择最先接收到的Offer（可能有多台DHCP服务器进行了响应），并广播DHCP Request通知所有DHCP服务器。
- DHCP服务器收到Request后，回复DHCP ACK给客户端，完成IP分配。

在上述四种DHCP包的类型中，DHCP Request包承载了主要的网络配置分发功能，向主机提供了“Your” IP Address（服务端将要分配给客户端的IP地址）、Router（网关IP地址）、Subnet Mask（子网掩码）、Domain Name Server（DNS服务器IP地址）等配置信息，实现了对于新接入主机的网络自动配置。

网络中的地址映射：DNS 与 ARP

在整个互联网协议栈中，存在三套功能类似的地址，它们都被用来标识一台主机（或一台主机的某个接口），分别是应用层的域名、网络层的IP地址、链路层的MAC地址。三套地址分别在不同的协议层次中发挥作用。在互联网协议栈中，应用层的DNS协议完成域名到IP地址的映射（解析），链路层的ARP协议完成IP地址到MAC地址的映射（解析）。

DNS协议用于将域名（如tsinghua.edu.cn）转换为IP地址（166.111.4.100），DNS提供了由大量DNS服务器组成的分布式、层次化的数据库系统，并通过递归查询和迭代查询两种方式供客户端从适合的DNS服务器获取到域名与IP的映射关系（称为资源记录）。在DNS响应数据包中，资源记录存储在字段Answers中，并且根据Type的不同，提供了不同的数据结构以组织对应的信息。

ARP协议用于在交换局域网内将IP地址转换为MAC地址，ARP协议的主要组成部分包括ARP表与ARP分组。ARP表记录了交换局域网内IP地址到MAC地址的映射关系。ARP请求分组以链路层广播的方式向局域网内所有主机询问某个IP地址对应的MAC地址，对应的主机则通过ARP响应分组向其回送自己的MAC地址来完成映射关系的传递。

路由追踪工具：traceroute

路由追踪指识别主机到另一主机的（路由）路径的过程。在一个简单的网络上，这个路径可能只经过一个路由器，甚至一个都不经过。但是在复杂的网络中，网络层数据报可能要经过数十个路由器才会到达最终目的地。在通信过程中，可以通过路由追踪判断网络层数据报传输的路径。

在基于Unix/Linux的系统中，traceroute命令用来追踪发出网络层数据报的主机到目标主机之间所经过的路由器；在Windows系统中为tracert。它们利用IP协议的TTL值完成对路径的逐跳探测。在IP协议中，TTL值标记该数据报的存活时间，每到达一个路由器，该值便会减一。当其值为0时，路由器将会丢弃该数据包，以自身IP为源地址，向数据报的发送方发送数据报反馈该情况（发送ICMP TTL exceeded通知发送者TTL值超过范围，同学们可以自行了解ICMP协议）。这样，traceroute命令通过发

送TTL=1，TTL=2，TTL=3...等一系列包并等待相应的ICMP回复，便可知路径上距本机的1、2、3、...跳的路由器的IP地址，从而获知数据报在网络中的转发过程。为了区分响应来自路由器还是目标主机，traceroute设置了一个不可能的端口号，使得目的主机接收后响应特定的报文（ICMP Port unreachable），从而与路由器发送的反馈（ICMP TTL exceeded）区分开，进而停止继续追踪。

另外，traceroute默认发送UDP包进行追踪，而tracert默认发送ICMP包进行追踪。核心网中部分路由器可能阻止了ICMP TTL exceeded的回复，因此traceroute与tracert命令并不一定能够探测到数据包途径核心网每一跳的地址，但这并不意味着数据不可达。

实验过程与记录

4.1 理解主机接入网络的过程

在清空 ARP 表之前，存储的 ARP 表信息如下：

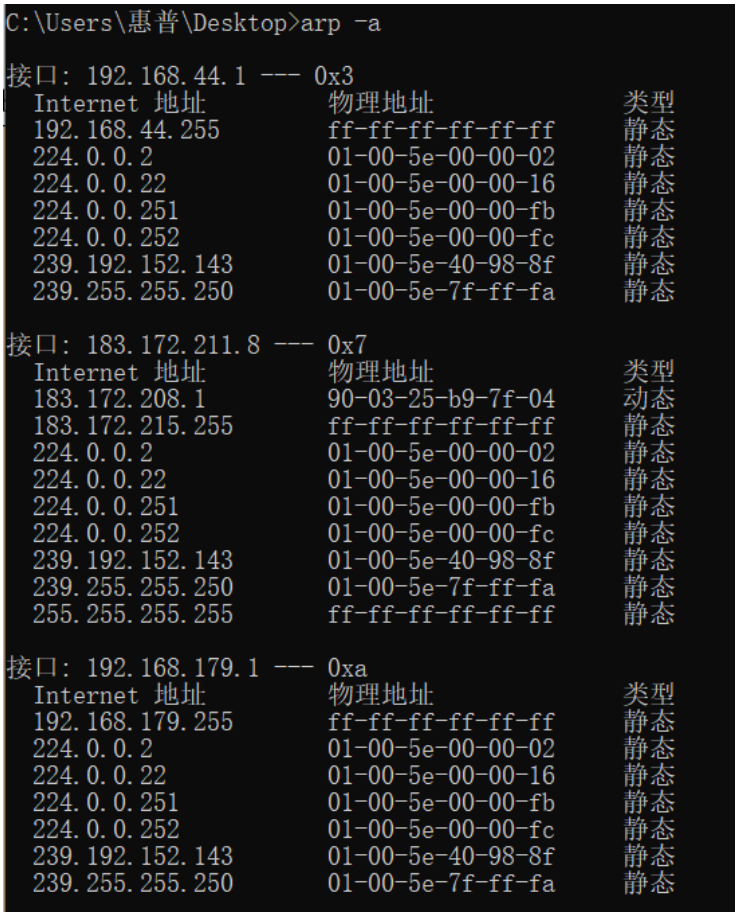
```
C:\Users\惠普\Desktop>arp -a

接口: 192.168.44.1 --- 0x3
  Internet 地址         物理地址              类型
  192.168.44.255        ff-ff-ff-ff-ff-ff     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.251           01-00-5e-00-00-fb     静态
  239.192.152.143       01-00-5e-40-98-8f     静态
  239.255.255.250       01-00-5e-7f-ff-fa     静态

接口: 183.172.211.8 --- 0x7
  Internet 地址         物理地址              类型
  183.172.208.1         90-03-25-b9-7f-04     动态
  183.172.215.255       ff-ff-ff-ff-ff-ff     静态
  224.0.0.2             01-00-5e-00-00-02     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.251           01-00-5e-00-00-fb     静态
  239.192.152.143       01-00-5e-40-98-8f     静态
  239.255.255.250       01-00-5e-7f-ff-fa     静态

接口: 192.168.179.1 --- 0xa
  Internet 地址         物理地址              类型
  192.168.179.255       ff-ff-ff-ff-ff-ff     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.251           01-00-5e-00-00-fb     静态
  239.192.152.143       01-00-5e-40-98-8f     静态
  239.255.255.250       01-00-5e-7f-ff-fa     静态
```

完成 IP 配置与 ARP 表的清空操作后，截图记录操作系统中显示的本机 IP 地址、默认网关IP、子网掩码、DNS服务器地址等信息的情况如下：


```
C:\Users\惠普\Desktop>arp -a

接口: 192.168.44.1 --- 0x3
  Internet 地址         物理地址              类型
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.251           01-00-5e-00-00-fb     静态

接口: 183.172.211.8 --- 0x7
  Internet 地址         物理地址              类型
  183.172.208.1         90-03-25-b9-7f-04     动态
  224.0.0.2             01-00-5e-00-00-02     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.251           01-00-5e-00-00-fb     静态

接口: 192.168.179.1 --- 0xa
  Internet 地址         物理地址              类型
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.251           01-00-5e-00-00-fb     静态
```

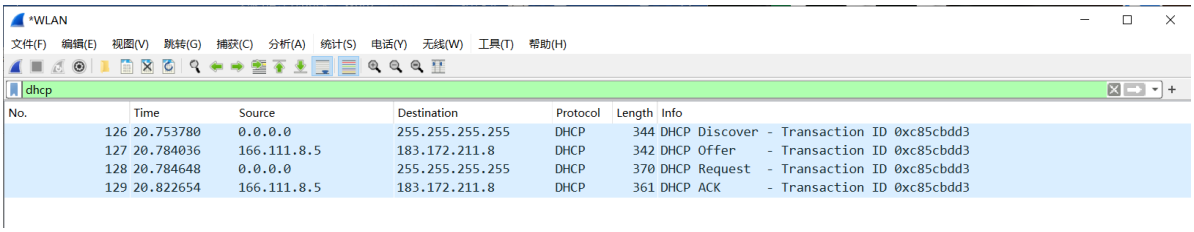
可以看到，在完成 IP 配置与 ARP 表的清空操作后，操作系统中已经没有了本地 IP 相关的信息，且 ARP 表也基本被清空了，并且经测试，在清空 IP 配置和 ARP 表后确实在短时间内无法上网，如下图。

此后触发 DHCP，截图记录操作系统中显示的本机 IP 地址、默认网关IP、子网掩码、DNS服务器地址等信息的情况如下：



如图，在触发 DHCP 后，操作系统中 IP 相关信息得以恢复，本机 IP 地址为 183.172.211.8，默认网关 IP 为183.172.208.1，子网掩码为 255.255.248.0，DNS 服务器地址为 166.111.8.28 、166.111.8.29 、 101.7.8.9，且 ARP 表相较于此前被清空的 ARP 表也大大丰富。

DHCP 建立过程中的 4 个包被 wireshark 抓包，利用 dhcp 筛选条件，得到下图：



其各自信息如下（依次为 DHCP Discover、DHCP Offer、DHCP Request、DHCP ACK，为本机分配IP地址、默认网关IP、子网掩码、DNS服务器地址等信息已标注于截图中）：

No.	Time	Source	Destination	Protocol	Length	Info
126	20.753780	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0xc85cbdd3
127	20.784036	166.111.8.5	183.172.211.8	DHCP	342	DHCP Offer - Transaction ID 0xc85cbdd3
128	20.784648	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0xc85cbdd3
129	20.822654	166.111.8.5	183.172.211.8	DHCP	361	DHCP ACK - Transaction ID 0xc85cbdd3

```
> User Datagram Protocol, Src Port: 68, Dst Port: 67
v Dynamic Host Configuration Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xc85cbdd3
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: IntelCor_6e:bf:2c (d0:ab:d5:6e:bf:2c)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Discover)
  > Option: (61) Client identifier
  > Option: (50) Requested IP Address (183.172.211.8)
  > Option: (12) Host Name
  > Option: (60) Vendor class identifier
  > Option: (55) Parameter Request List
  > Option: (255) End
```

DHCP Discover

No.	Time	Source	Destination	Protocol	Length	Info
126	20.753780	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0xc85cbdd3
127	20.784036	166.111.8.5	183.172.211.8	DHCP	342	DHCP Offer - Transaction ID 0xc85cbdd3
128	20.784648	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0xc85cbdd3
129	20.822654	166.111.8.5	183.172.211.8	DHCP	361	DHCP ACK - Transaction ID 0xc85cbdd3

```
    Hops: 0
    Transaction ID: 0xc85cbdd3
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 183.172.211.8
    Next server IP address: 166.111.8.5
    Relay agent IP address: 183.172.208.14
    Client MAC address: IntelCor_6e:bf:2c (d0:ab:d5:6e:bf:2c)
    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 (166.111.8.5)
  v Option: (1) Subnet Mask (255.255.248.0)
      Length: 4
      Subnet Mask: 255.255.248.0
  v Option: (6) Domain Name Server
      Length: 12
      Domain Name Server: 166.111.8.28
      Domain Name Server: 166.111.8.29
      Domain Name Server: 101.7.8.9
  > Option: (15) Domain Name
  > Option: (51) IP Address Lease Time
  v Option: (3) Router
      Length: 4
      Router: 183.172.208.1
  > Option: (255) End
    Padding: 00
```

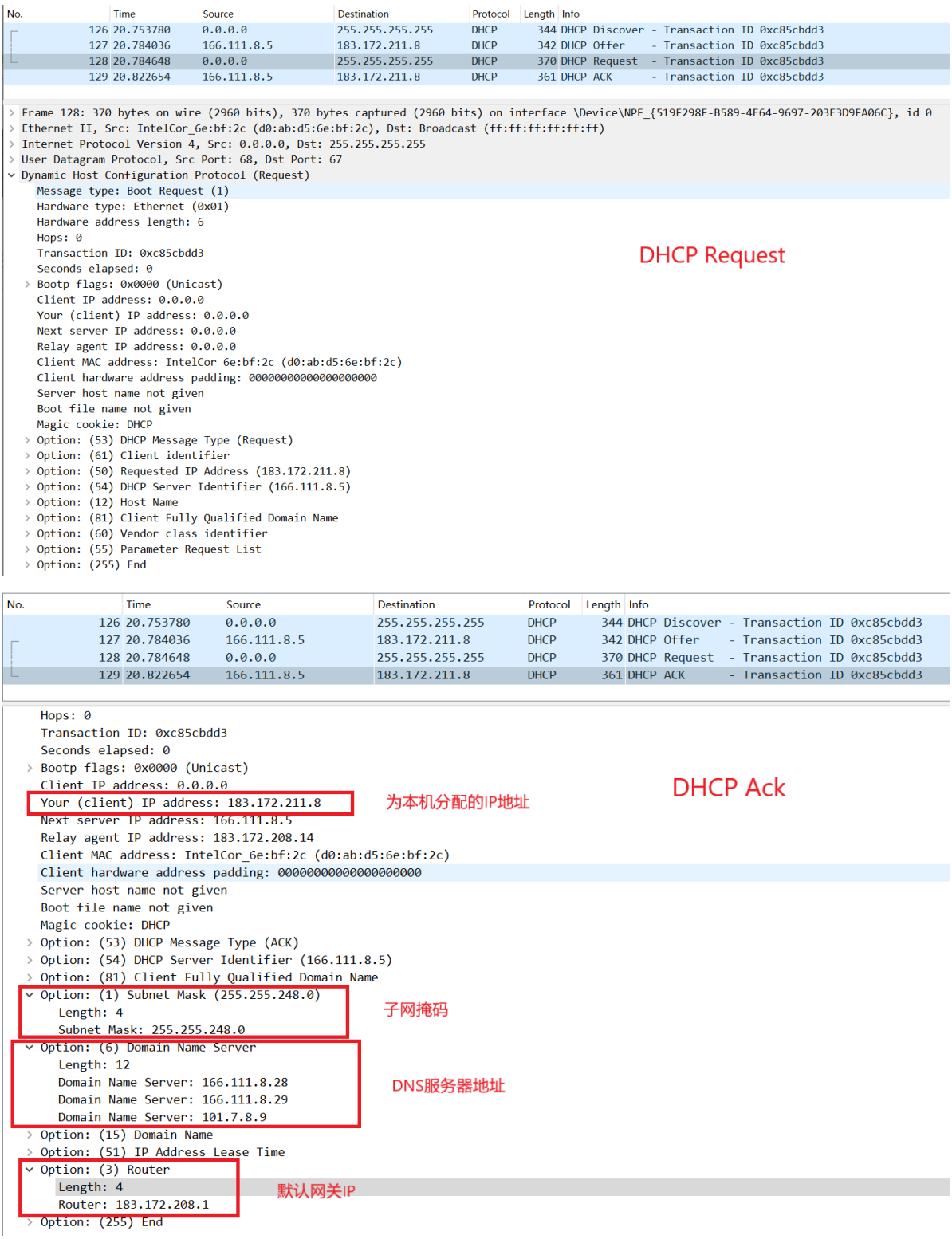
为本机分配的IP地址

子网掩码

DNS服务器地址

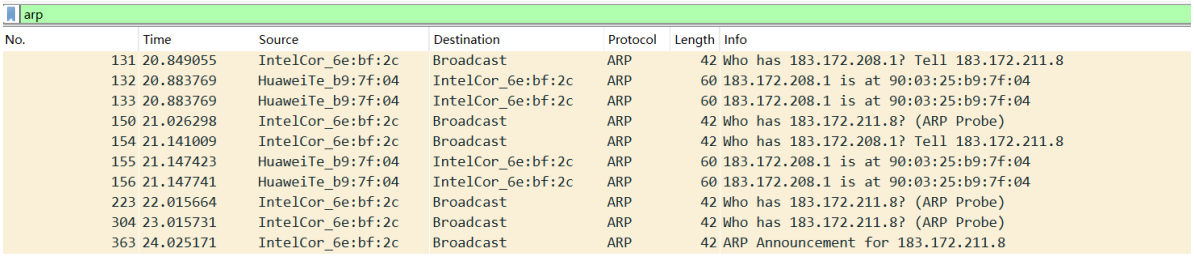
默认网关IP

DHCP Offer



将上面抓包得到的信息和从操作系统中得到的信息相对比，可以发现本机 IP 地址、子网掩码、DNS 服务器地址、默认网关 IP 都是相对应的关系，完全一致，这是因为本机联网所需的配置本质上就是通过这些数据包交换信息完成的。再根据 wireshark 中筛选出的 DHCP 数据包进行分析，可以看到四个包的顺序依次为 discover、offer、request、ack，这和指导书中所给的主机接入互联网时与 DHCP 服务器的交流过程完全一致：新接入互联网的客户端向各个 DHCP 服务器广播需要 IP 地址的消息，即广播 DHCP Discover 数据包，然后收到消息的 DHCP 服务器会响应一个 DHCP Offer 数据包，向客户端提供可行的诸如 IP 地址等配置信息，客户端收到后，则广播 DHCP Request 数据包给各个 DHCP 服务器，表示使用该包含 IP 地址等的配置，最后此前发出 offer 的 DHCP 服务器再响应 DHCP Ack 数据包，确认收到传来的 Request 数据包，至此 IP 地址分配完毕。（从 wireshark 抓包数据可以看到，在 IP 地址分配完毕前，主机认为自己的 IP 地址为 0.0.0.0，将数据包发送给 255.255.255.255，其实也就是进行广播的过程）

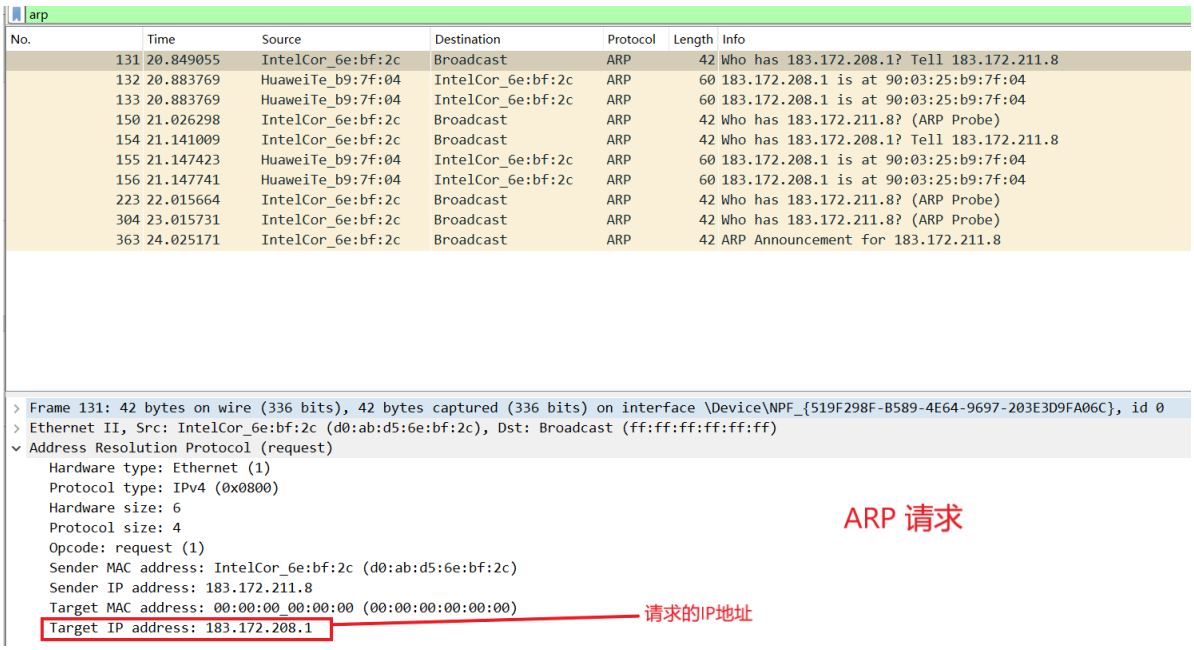
再通过 “arp” 选项筛选 wireshark 中数据包，得到下图：



arp

No.	Time	Source	Destination	Protocol	Length	Info
131	20.849055	IntelCor_6e:bf:2c	Broadcast	ARP	42	Who has 183.172.208.1? Tell 183.172.211.8
132	20.883769	HuaweiTe_b9:7f:04	IntelCor_6e:bf:2c	ARP	60	183.172.208.1 is at 90:03:25:b9:7f:04
133	20.883769	HuaweiTe_b9:7f:04	IntelCor_6e:bf:2c	ARP	60	183.172.208.1 is at 90:03:25:b9:7f:04
150	21.026298	IntelCor_6e:bf:2c	Broadcast	ARP	42	Who has 183.172.211.8? (ARP Probe)
154	21.141009	IntelCor_6e:bf:2c	Broadcast	ARP	42	Who has 183.172.208.1? Tell 183.172.211.8
155	21.147423	HuaweiTe_b9:7f:04	IntelCor_6e:bf:2c	ARP	60	183.172.208.1 is at 90:03:25:b9:7f:04
156	21.147741	HuaweiTe_b9:7f:04	IntelCor_6e:bf:2c	ARP	60	183.172.208.1 is at 90:03:25:b9:7f:04
223	22.015664	IntelCor_6e:bf:2c	Broadcast	ARP	42	Who has 183.172.211.8? (ARP Probe)
304	23.015731	IntelCor_6e:bf:2c	Broadcast	ARP	42	Who has 183.172.211.8? (ARP Probe)
363	24.025171	IntelCor_6e:bf:2c	Broadcast	ARP	42	ARP Announcement for 183.172.211.8

可以看到，最上面两条 ARP 数据包对应于本机请求网关 MAC 地址对应的 ARP 请求与响应，请求记录中请求的 IP 地址与响应记录中回复的 MAC 地址在下面截图中做了标记（上面为 ARP 请求，下面为 ARP 响应）：



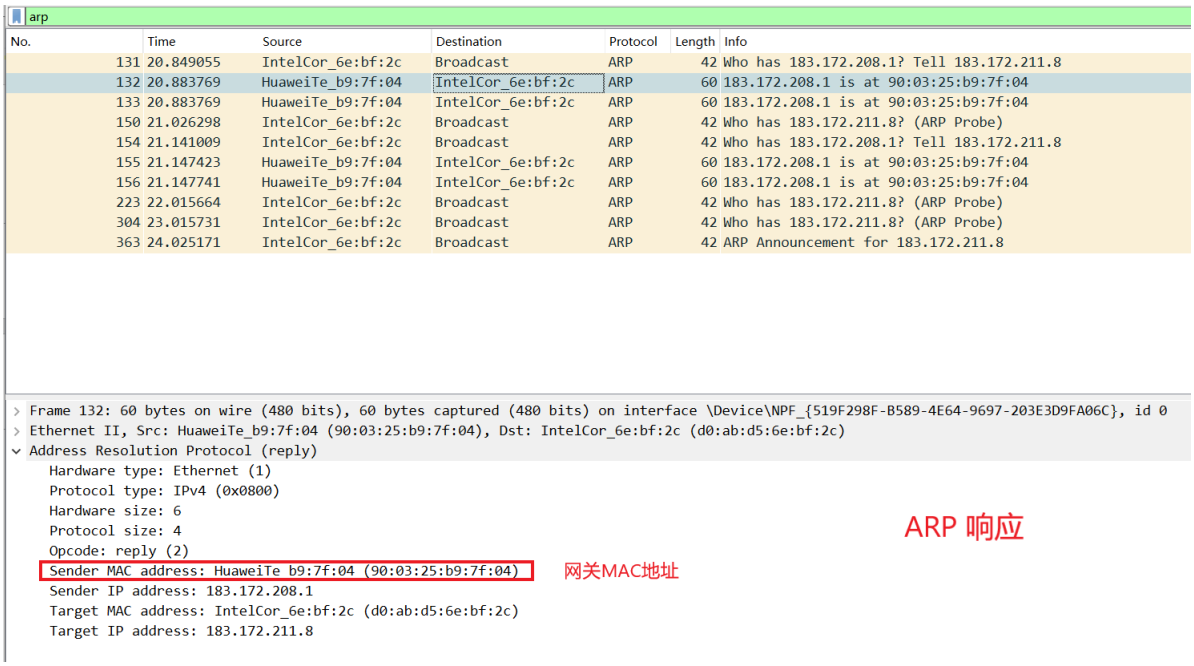
arp

No.	Time	Source	Destination	Protocol	Length	Info
131	20.849055	IntelCor_6e:bf:2c	Broadcast	ARP	42	Who has 183.172.208.1? Tell 183.172.211.8
132	20.883769	HuaweiTe_b9:7f:04	IntelCor_6e:bf:2c	ARP	60	183.172.208.1 is at 90:03:25:b9:7f:04
133	20.883769	HuaweiTe_b9:7f:04	IntelCor_6e:bf:2c	ARP	60	183.172.208.1 is at 90:03:25:b9:7f:04
150	21.026298	IntelCor_6e:bf:2c	Broadcast	ARP	42	Who has 183.172.211.8? (ARP Probe)
154	21.141009	IntelCor_6e:bf:2c	Broadcast	ARP	42	Who has 183.172.208.1? Tell 183.172.211.8
155	21.147423	HuaweiTe_b9:7f:04	IntelCor_6e:bf:2c	ARP	60	183.172.208.1 is at 90:03:25:b9:7f:04
156	21.147741	HuaweiTe_b9:7f:04	IntelCor_6e:bf:2c	ARP	60	183.172.208.1 is at 90:03:25:b9:7f:04
223	22.015664	IntelCor_6e:bf:2c	Broadcast	ARP	42	Who has 183.172.211.8? (ARP Probe)
304	23.015731	IntelCor_6e:bf:2c	Broadcast	ARP	42	Who has 183.172.211.8? (ARP Probe)
363	24.025171	IntelCor_6e:bf:2c	Broadcast	ARP	42	ARP Announcement for 183.172.211.8

```
> Frame 131: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{519F298F-B589-4E64-9697-203E3D9FA06C}, id 0
> Ethernet II, Src: IntelCor_6e:bf:2c (d0:ab:d5:6e:bf:2c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: IntelCor_6e:bf:2c (d0:ab:d5:6e:bf:2c)
    Sender IP address: 183.172.211.8
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 183.172.208.1
```

ARP 请求

请求的IP地址



arp

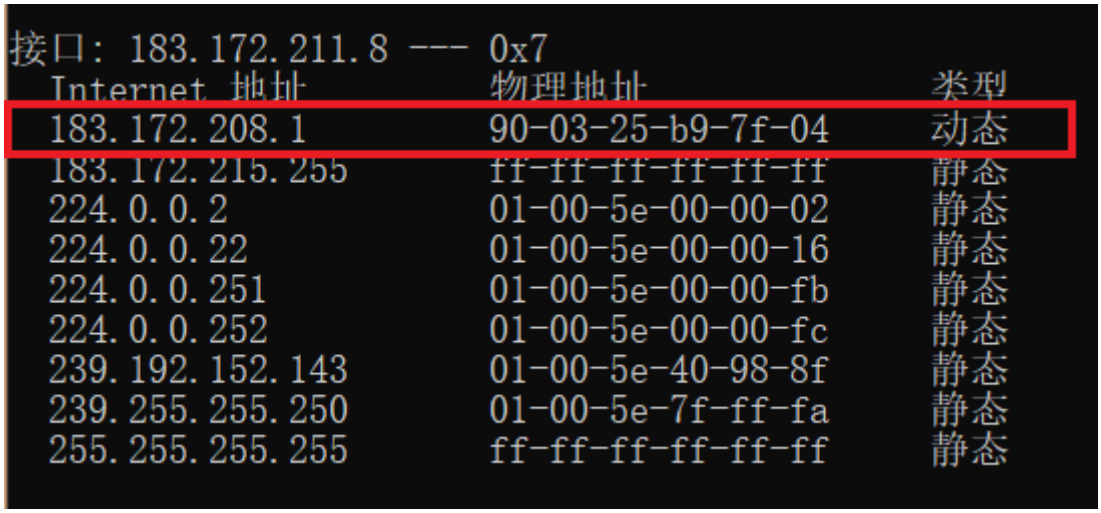
No.	Time	Source	Destination	Protocol	Length	Info
131	20.849055	IntelCor_6e:bf:2c	Broadcast	ARP	42	Who has 183.172.208.1? Tell 183.172.211.8
132	20.883769	HuaweiTe_b9:7f:04	IntelCor_6e:bf:2c	ARP	60	183.172.208.1 is at 90:03:25:b9:7f:04
133	20.883769	HuaweiTe_b9:7f:04	IntelCor_6e:bf:2c	ARP	60	183.172.208.1 is at 90:03:25:b9:7f:04
150	21.026298	IntelCor_6e:bf:2c	Broadcast	ARP	42	Who has 183.172.211.8? (ARP Probe)
154	21.141009	IntelCor_6e:bf:2c	Broadcast	ARP	42	Who has 183.172.208.1? Tell 183.172.211.8
155	21.147423	HuaweiTe_b9:7f:04	IntelCor_6e:bf:2c	ARP	60	183.172.208.1 is at 90:03:25:b9:7f:04
156	21.147741	HuaweiTe_b9:7f:04	IntelCor_6e:bf:2c	ARP	60	183.172.208.1 is at 90:03:25:b9:7f:04
223	22.015664	IntelCor_6e:bf:2c	Broadcast	ARP	42	Who has 183.172.211.8? (ARP Probe)
304	23.015731	IntelCor_6e:bf:2c	Broadcast	ARP	42	Who has 183.172.211.8? (ARP Probe)
363	24.025171	IntelCor_6e:bf:2c	Broadcast	ARP	42	ARP Announcement for 183.172.211.8

```
> Frame 132: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{519F298F-B589-4E64-9697-203E3D9FA06C}, id 0
> Ethernet II, Src: HuaweiTe_b9:7f:04 (90:03:25:b9:7f:04), Dst: IntelCor_6e:bf:2c (d0:ab:d5:6e:bf:2c)
v Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: HuaweiTe_b9:7f:04 (90:03:25:b9:7f:04)
    Sender IP address: 183.172.208.1
    Target MAC address: IntelCor_6e:bf:2c (d0:ab:d5:6e:bf:2c)
    Target IP address: 183.172.211.8
```

ARP 响应

网关MAC地址

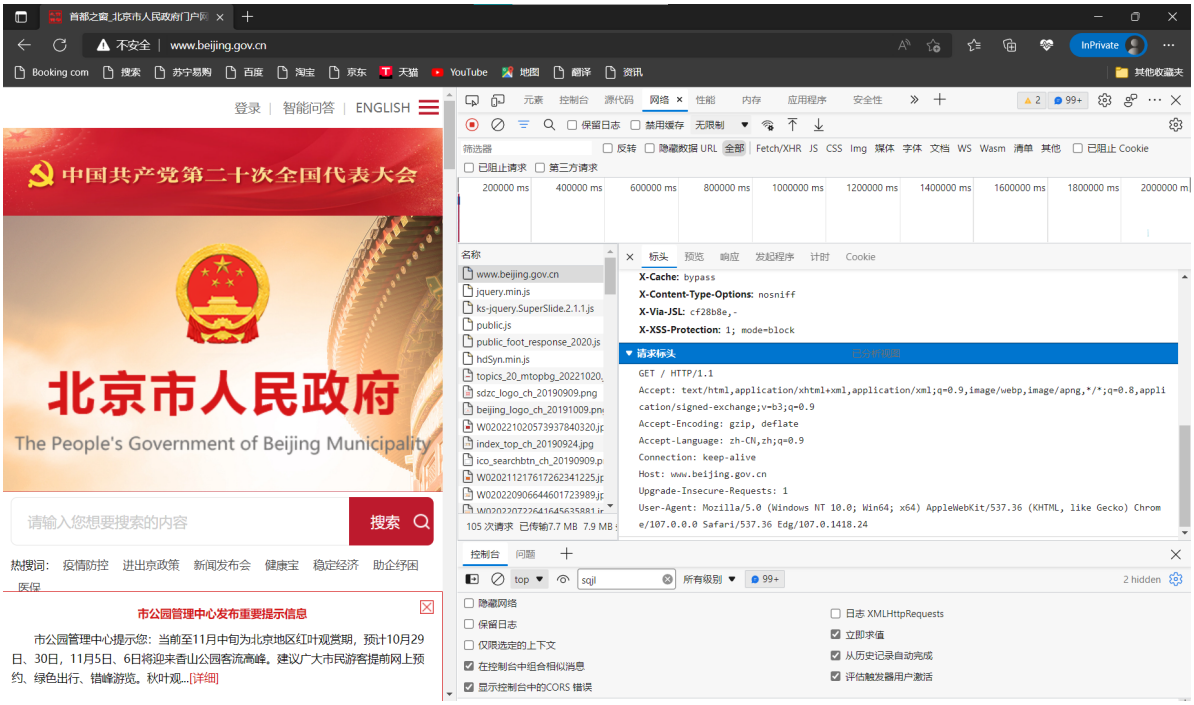
本机请求的 IP 地址为 183.172.208.1，和前面记录的默认网关 IP 地址一致，而网关回复的 ARP 响应中给出的网关 MAC 地址为 90:03:25:b9:7f:04，这也和前面截图中 ARP 表的记录一致，如下图：



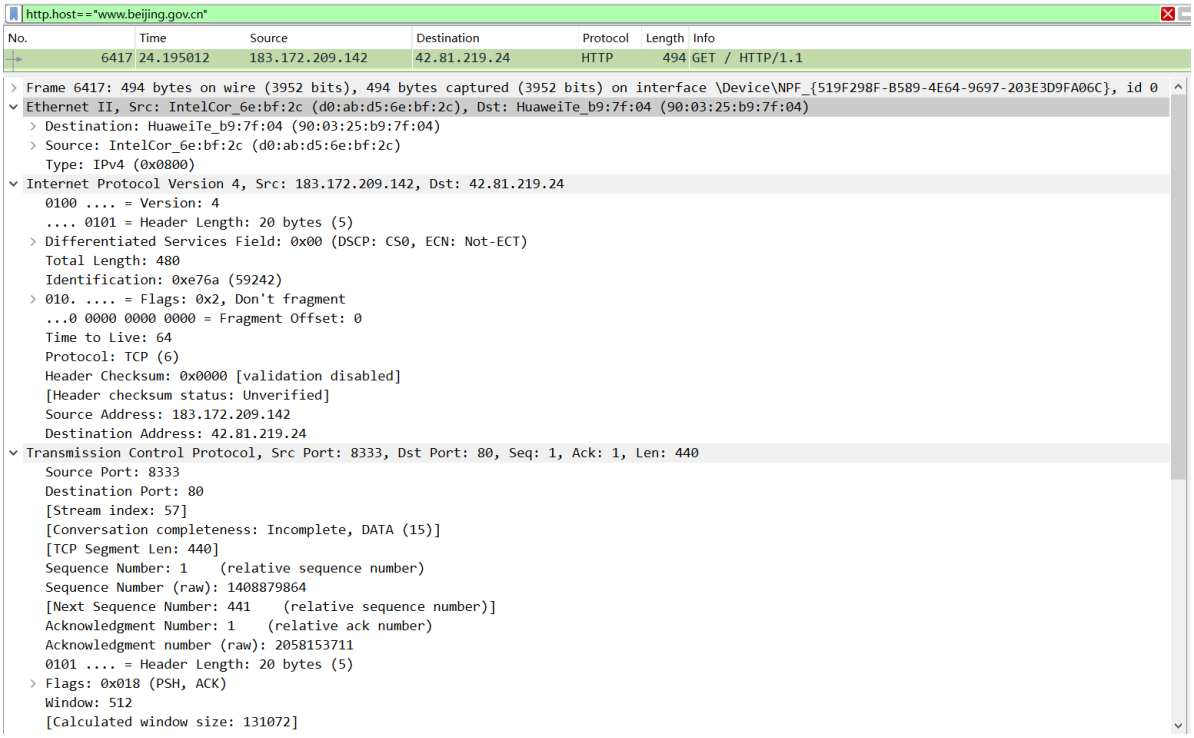
由上面信息也可以总结出本实验中 ARP 的工作过程大致为：本机向局域网内所有主机询问网关 IP 地址对应的 MAC 地址（也就是广播，在 wireshark 中也显示 ARP 请求分组的目的地为 Broadcast），网关接收到该消息后，通过 ARP 响应分组将自己的 MAC 地址回传给本机，这样本机就确定了由网关 IP 地址到其 MAC 地址的映射关系。

4.2 以 Web 网页应用为例分析互联网的工作过程

通过 Edge 浏览器访问 http://www.beijing.gov.cn/，并用 wireshark 进行抓包，在浏览器中查看到的报文信息如下：



在 wireshark 中找到向 http://www.beijing.gov.cn/ 发出的第一条 HTTP 请求报文，其详细信息如下：



根据上面信息填写报文表格，如下：

<table>
<tr><th colspan="12">Ethernet II</th></tr>
<tr><td colspan="4">目的 MAC 地址</td><td colspan="5">源 MAC 地址</td><td colspan="3">类型</td></tr>
<tr><td colspan="4">HuaweiTe_b9:7f:04(90:03:25:b9:7f:04)</td><td colspan="5">IntelCor_6e:bf:2c(d0:ab:d5:6e:bf:2c)</td><td colspan="3">IPv4(0x0800)</td></tr>
<tr><th colspan="12">IP</th></tr>
<tr><td>版本</td><td>头部
长度</td><td colspan="2">服务
类型</td><td colspan="8">数据报长度</td></tr>
<tr><td>4</td><td>20bytes</td><td colspan="2">（略）</td><td colspan="8">480</td></tr>
<tr><td colspan="4">16bit 标识</td><td colspan="4">标志</td><td colspan="4">片偏移</td></tr>
<tr><td colspan="4">0xe76a</td><td colspan="4">0x2</td><td colspan="4">0</td></tr>
<tr><td colspan="2">TTL</td><td colspan="3">上层协议</td><td colspan="7">头部检验和</td></tr>
<tr><td colspan="2">64</td><td colspan="3">TCP</td><td colspan="7">0x0000</td></tr>
<tr><td colspan="12">32bit 源 IP 地址</td></tr>
<tr><td colspan="12">183.172.209.142</td></tr>
<tr><td colspan="12">32bit 目的 IP 地址</td></tr>
<tr><td colspan="12">42.81.219.24</td></tr>
<tr><td colspan="12">选项</td></tr>
<tr><td colspan="12">（略）</td></tr>
<tr><th colspan="12">TCP</th></tr>
<tr><td colspan="6">源端口号</td><td colspan="6">目的端口号</td></tr>
<tr><td colspan="6">8333</td><td colspan="6">80</td></tr>
<tr><td colspan="12">序号</td></tr>
<tr><td colspan="12">1(原始为 1408879864)</td></tr>
<tr><td colspan="12">确认号</td></tr>
<tr><td colspan="12">1(原始为 2058153711)</td></tr>
<tr><td>首部
长度</td><td>保留
未用</td><td>U
R
G</td><td>A
C
K</td><td>P
S
H</td><td>R
S
T</td><td>S
Y
N</td><td>F
I
N</td><td colspan="6">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 colspan="6">512</td></tr>
<tr><td colspan="8">检验和</td><td colspan="4">紧急数据指针</td></tr>
<tr><td colspan="8">0x9077</td><td colspan="4">（略）</td></tr>
<tr><td colspan="12">选项</td></tr>
<tr><td colspan="12">（略）</td></tr>
<tr><th colspan="12">HTTP</th></tr>
<tr><td colspan="12">请求行：GET / HTTP/1.1\r\n</td></tr>
<tr><td colspan="3">Host:</td><td colspan="9">www.beijing.gov.cn\r\n</td></tr>
<tr><td colspan="3">User-Agent:</td><td colspan="9">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</td></tr>
</table>

按照自顶向下的顺序，首先浏览器网页根据用户给出的指令生成 HTTP 请求报文（HTTP 协议），该报文进入传输层后，被加上传输层包头（本例中采用了 TCP 连接，故而加上了 TCP 首部，报头中包含源端口号和目的端口号，以及其他 TCP 协议规定的信息），成为一个数据段，该数据段此后进入网络层，被加上 IP 首部（包含源 IP 地址和目的 IP 地址，以及其他一些 IP 协议规定的信息），成为一个数据报，最后该数据包进入链路层，再被加上一个链路层包头（包含目的 MAC 地址和源 MAC 地址并给出 IP 协议版本），就成为了一个以太网帧，这就是浏览器网页访问请求被逐层封装为以太网帧的大致过程。

下面逐一说明各层包头中各个字段的含义以及其值是如何确定的：

- **应用层（HTTP）：**

①请求行：从左至右依次表明请求方法、URL、协议版本（"\r\n"为回车换行），本例中请求方法为“GET”，表示要获取资源（其他请求方法诸如“POST”表示向服务器推送数据，而本例中是请求访问该网址，故而为“GET”），URL 为“/”（此处尚不清楚为“/”的原因），协议版本为“HTTP/1.1”，是浏览器实现的 HTTP 版本，定义剩余报文的结构与对期望的响应版本的指示符，本例中 HTTP 数据段中请求行和前面浏览器开发者工具得到的请求源代码一致；

②Host：指明对象所在的主机，本例中为“www.beijing.gov.cn”对应的主机，因为我们要访问的就是该网址，Host 和前面浏览器开发者工具得到的请求源代码一致；

③User-Agent：指明用户代理，即发送请求的浏览器类型，本例中值为“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”，可以看到这其中包含多个浏览器的标识，这样多增加一些字段都是为了让服务器检测到它支持的浏览器标识，以便获得服务器的响应，从而提升用户体验，本例中 HTTP 数据段中 User-Agent 也和前面浏览器开发者工具得到的请求源代码一致。

- **传输层（TCP）：**

①源端口号：表明了发出该数据段的应用在当前主机上的端口号，是 TCP 报文的发送地，也确定了报文的返回地址，该例中源端口号为 Edge 网页对应的端口号；

②目的端口号：表明正在通信的应用在目的主机上的端口号，是发送目的地，该例中为 “www.beijing.gov.cn” 对应服务器主机上收发信息的端口；

③序号：发送的分组的第一个字节的序号，确保了 TCP 传输的有序性，其值在理论上应该为上一次发送的数据段的序号加上一次数据段的数据部分字节数；

④确认号：即 ACK，指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已经准确无误地收到了，其值理论上为上一次收到的数据段的序号加上一次数据段的数据部分字节数；

⑤首部长度：指示了以 32 比特的字为单位的 TCP 首部长度，这是由于存在 TCP 选项字段，所以 TCP 首部长度是可变的，在该例中，由于没有选项，故而首部长度为 20 bytes；

⑥标志字段：ACK 比特用于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报文段的确认，本例中包含的确认号是有效的，故而 ACK 为 1，RST、SYN 和 FYN 比特用于连接的建立和拆除，本例不涉及建立或拆除连接，故而这些标志都为 0，PSH 比特指示接收方应立即将数据交给上层，本例中需要把数据交付给上层 HTTP，故而 PSH 为1，URG 比特用来指示报文段里存在着被发送端的上层实体置为“紧急”的数据，该例中不存在“紧急”数据，故而 URG 为0；

⑦接收窗口：用于流量控制，表明当前接受方处理收到数据的能力；

⑧检验和：用于发现 TCP 包头和数据在发送端到接收端之间发生的传输差错检测。

- **网络层（IP）：**

①版本：规定了数据报 IP 版本（v4、v6），本次实验采用的是 IPv4，故而为 4；

②头部长度：用于确定数据实际开始的地方，本例中不含选项，故而 IP 头部为 5 个字（20 bytes）；

③服务类型：标识不同类型的 IP 数据报；

④数据报长度：指示数据报总长度；

⑤16-bit 标识、标志、片偏移：与 IP 分片有关，目的主机根据数据报中的标识来判断接收到的数据报是否是一个大的数据包的分片，通过标志确定该分片是否是最后一个，通过片偏移决定重新组装的顺序；

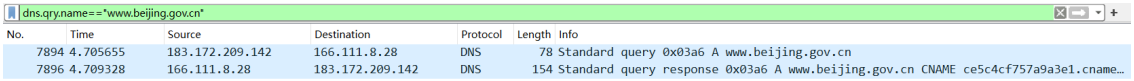
⑥寿命（TTL）：每次转发就寿命-1，确保数据报不会永远在网络中循环，本例中寿命为 64 表明该数据报最多可以转发 64 次；

⑦上层协议：指示数据应交给哪个传输层协议，本次实验为 TCP 连接，故而上层协议为 TCP；

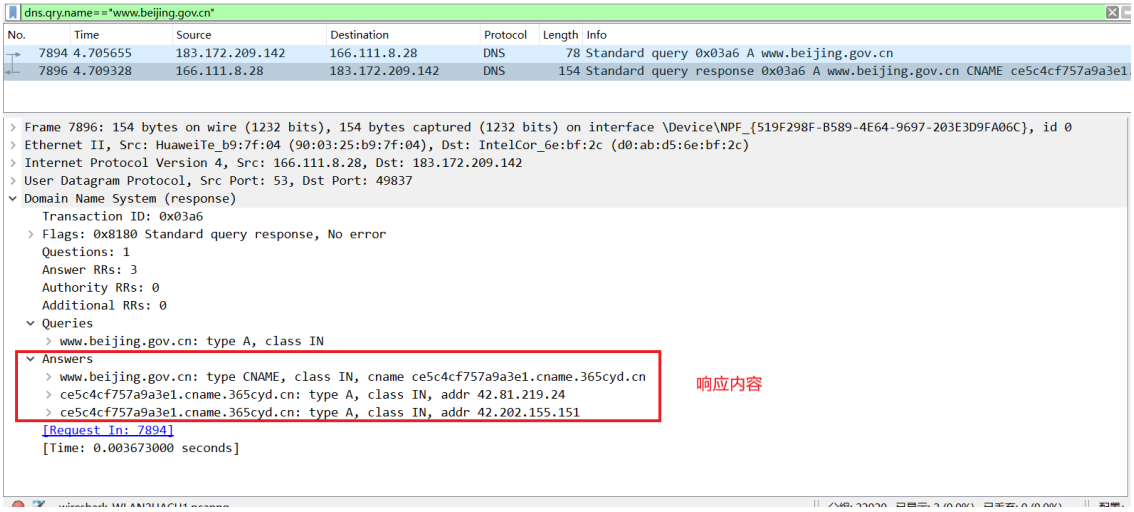
⑧头部检验和：帮助路由器检测 IP 数据报中的比特错误；

⑨源 IP 地址：发送该数据报的主机在网络中被配置的 IP 地址，本例中即对应于本机被配置的 IP 地址，即 183.172.209.142 （与上一个实验部分得到的 IP 地址不同，因为这部分实验和上一部分实验不是同时做的），获取该 IP 地址的过程和上一部分实验中的过程一致，即向 DHCP 服务器广播需要 IP 配置的需求，DHCP 服务器收到 Discover 后，回复 Offer ，当前主机收到 Offer 后再回复 Request ，最后 DHCP 服务器发送 Ack 来确认，由于和上一部分实验分析基本一致，故而不再展开；

⑩目的 IP 地址：该数据报发往的 IP 地址，在该实验中由源主机通过 DNS 查找到网址 “www.beijing.gov.cn” 对应服务器的 IP 地址，即 42.81.219.24 ，通过 wireshark 抓取对应“www.beijing.gov.cn”的 DNS 请求与响应如下图：



展开 DNS 响应的具体信息，如下：



通过分析上面的 DNS 响应数据包，可以发现 DNS 服务器（即 166.111.8.28 ）告知发出 DNS 请求的主机“www.beijing.gov.cn”域名对应的 IP 地址有两个：42.81.219.24 和 42.202.155.151 ，显然最后主机选择了前者作为目的 IP 地址，对该网站进行了访问。

- **传输层（以太网）：**

①目的 MAC 地址：目的适配器的 MAC 地址，在本例中，由于“www.beijing.gov.cn”域名对应的 IP 地址和主机 IP 地址不属于同一个局域网，所以数据帧需要经由网关转发，故而目的 MAC 地址就是默认网关的 MAC 地址，即前面实验中得到的 90:03:25:b9:7f:04 ，默认网关的 MAC 地址获取过程和上一部分实验中的过程一致，不再展开；

②源 MAC 地址：发送该数据帧的适配器的 MAC 地址，主机自身是可以获取到自身适配器的 MAC 地址的，本例中为 d0:ab :d5:6e:bf:2c ，和上一部分实验中的记录一致；

③类型：指示数据对应的高层协议类型，在本例中采用了 IPv4 协议。

此后再利用 tracert 命令追踪本机到 HTTP 服务器之间经过的核心网络路由，得到下图：

```
C:\Users\惠普\Desktop>tracert -w 4 www.beijing.gov.cn

通过最多 30 个跃点跟踪
到 ce5c4cf757a9a3e1.cname.365cyd.cn [42.81.219.24] 的路由:

  1    29 ms    23 ms     5 ms  183.172.208.1
  2     2 ms     1 ms     2 ms  172.17.2.25
  3     2 ms     4 ms     8 ms  118.229.4.77
  4     3 ms     2 ms     3 ms  qhu0.cernet.net [202.112.38.69]
  5     3 ms     3 ms     2 ms  101.4.113.233
  6    27 ms    27 ms    26 ms  101.4.115.202
  7    41 ms    44 ms    42 ms  101.4.116.225
  8     *       43 ms    46 ms  202.97.15.89
  9    44 ms     *       61 ms  202.97.81.229
 10    40 ms    39 ms    46 ms  202.97.13.202
 11    42 ms    43 ms    42 ms  202.97.22.34
 12    41 ms    43 ms    41 ms  42.81.35.54
 13     *        *        *     请求超时。
 14     *        *        *     请求超时。
 15     *        *        *     请求超时。
 16     *        *        *     请求超时。
 17     *        *        *     请求超时。
 18    43 ms    41 ms    45 ms  42.81.219.24

跟踪完成。
```

利用在线 IP 查询工具，查到各跳路由器的物理位置依次如下：

域名/IP	获取的IP地址	数字地址	IP的物理位置
183.172.209.142	183.172.209.142	3081556366	中国北京海淀 教育网 ip138提供

域名/IP	获取的IP地址	数字地址	IP的物理位置
183.172.208.1	183.172.208.1	3081555969	中国北京海淀 教育网 ip138提供

域名/IP	获取的IP地址	数字地址	IP的物理位置
172.17.2.25	172.17.2.25	2886795801	本地局域网 ip138提供

域名/IP	获取的IP地址	数字地址	IP的物理位置
118.229.4.77	118.229.4.77	1994720333	中国北京北京 教育网 ip138提供

域名/IP	获取的IP地址	数字地址	IP的物理位置
202.112.38.69	202.112.38.69	3396347461	中国北京北京 教育网 ip138提供

域名/IP	获取的IP地址	数字地址	IP的物理位置
101.4.113.233	101.4.113.233	1694790121	中国北京海淀 教育网 ip138提供

域名/IP	获取的IP地址	数字地址	IP的物理位置
101.4.115.202	101.4.115.202	1694790602	中国北京海淀 教育网 ip138提供
域名/IP	获取的IP地址	数字地址	IP的物理位置
101.4.116.225	101.4.116.225	1694790881	中国北京海淀 教育网 ip138提供
域名/IP	获取的IP地址	数字地址	IP的物理位置
202.97.15.89	202.97.15.89	3395358553	中国北京北京 电信 ip138提供
域名/IP	获取的IP地址	数字地址	IP的物理位置
202.97.81.229	202.97.81.229	3395375589	中国北京北京 电信 ip138提供
域名/IP	获取的IP地址	数字地址	IP的物理位置
202.97.13.202	202.97.13.202	3395358154	中国北京北京 电信 ip138提供
域名/IP	获取的IP地址	数字地址	IP的物理位置
202.97.22.34	202.97.22.34	3395360290	中国江西 电信 ip138提供
域名/IP	获取的IP地址	数字地址	IP的物理位置
42.81.35.54	42.81.35.54	709960502	中国天津天津 电信 ip138提供
域名/IP	获取的IP地址	数字地址	IP的物理位置
42.81.219.24	42.81.219.24	710007576	中国天津天津 电信 ip138提供

再通过在线自治域查询工具，查找各跳路由对应的自治域如下：

```
AS      | IP               | AS Name
4538    | 183.172.209.142  | ERX-CERNET-BKB China Education and Research Network Center, CN
24348   | 183.172.209.142  | CNGI-BJ-IX2-AS-AP CERNET2 IX at Tsinghua University, CN

The server returned 3 line(s).

AS      | IP               | AS Name
4538    | 183.172.208.1    | ERX-CERNET-BKB China Education and Research Network Center, CN
24348   | 183.172.208.1    | CNGI-BJ-IX2-AS-AP CERNET2 IX at Tsinghua University, CN

The server returned 2 line(s).

AS      | IP               | AS Name
NA      | 172.17.2.25      | NA

The server returned 2 line(s).

AS      | IP               | AS Name
4538    | 118.229.4.77     | ERX-CERNET-BKB China Education and Research Network Center, CN
```

The server returned 2 line(s).

```
AS      | IP               | AS Name
4538    | 202.112.38.69    | ERX-CERNET-BKB China Education and Research Network Center, CN
```

The server returned 2 line(s).

```
AS      | IP               | AS Name
4538    | 101.4.113.233    | ERX-CERNET-BKB China Education and Research Network Center, CN
```

The server returned 2 line(s).

```
AS      | IP               | AS Name
4538    | 101.4.115.202    | ERX-CERNET-BKB China Education and Research Network Center, CN
```

The server returned 2 line(s).

```
AS      | IP               | AS Name
4538    | 101.4.116.225    | ERX-CERNET-BKB China Education and Research Network Center, CN
```

The server returned 2 line(s).

```
AS      | IP               | AS Name
4134    | 202.97.15.89     | CHINANET-BACKBONE No.31,Jin-rong Street, CN
```

The server returned 2 line(s).

```
AS      | IP               | AS Name
4134    | 202.97.81.229    | CHINANET-BACKBONE No.31,Jin-rong Street, CN
```

The server returned 2 line(s).

```
AS      | IP               | AS Name
4134    | 202.97.13.202    | CHINANET-BACKBONE No.31,Jin-rong Street, CN
```

The server returned 2 line(s).

```
AS      | IP               | AS Name
4134    | 202.97.22.34     | CHINANET-BACKBONE No.31,Jin-rong Street, CN
```

The server returned 2 line(s).

```
AS      | IP               | AS Name
58542   | 42.81.35.54      | CHINATELECOM-TIANJIN Tianjij,300000, CN
```

The server returned 2 line(s).

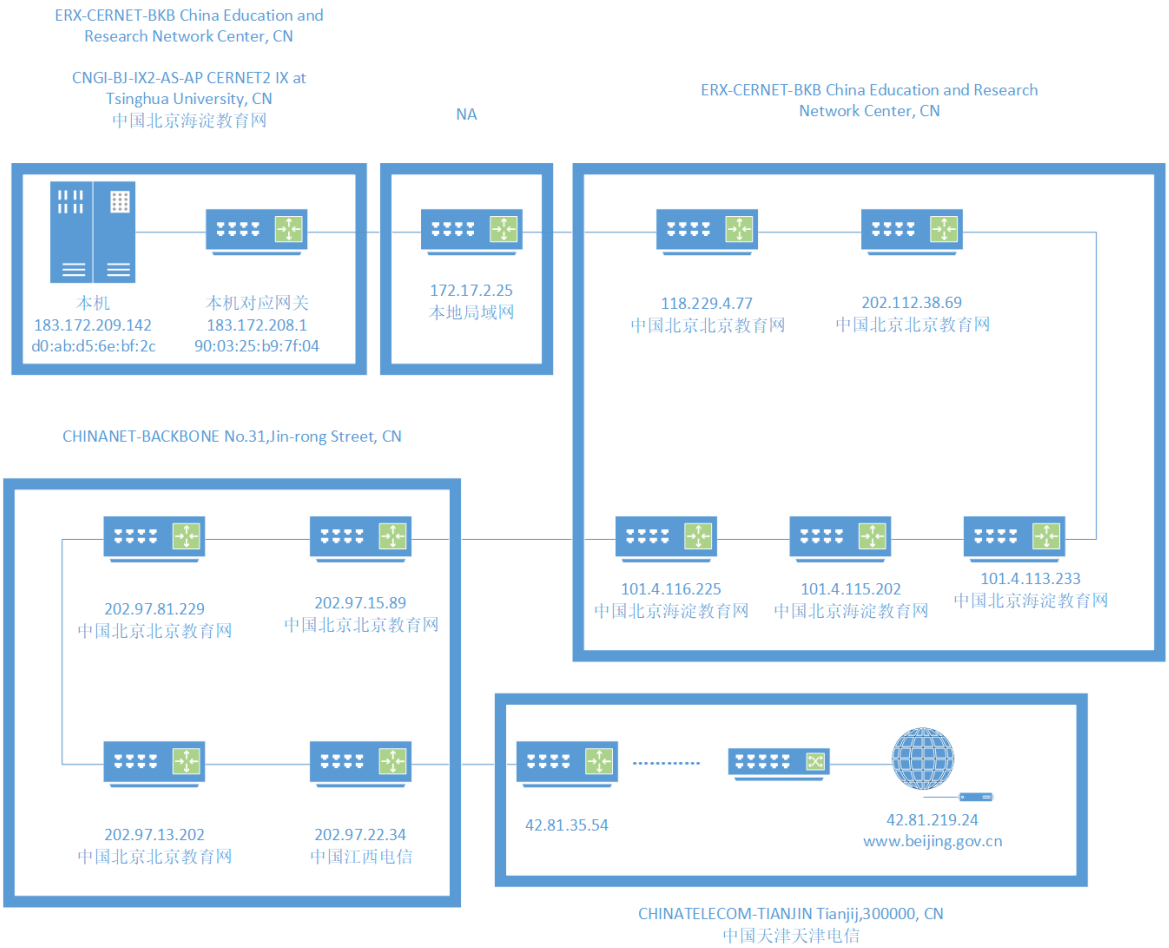
```
AS      | IP               | AS Name
58542   | 42.81.219.24     | CHINATELECOM-TIANJIN Tianjij,300000, CN
```

对上面整理出的数据进行整理，得到下表（MAC 地址未列出）：

IP地址	IP物理位置	自治域信息
183.172.209.142	中国北京海淀教育网	ERX-CERNET-BKB China Education and Research Network Center, CN；CNGI-BJ-IX2-AS-AP CERNET2 IX at Tsinghua University, CN
183.172.208.1	中国北京海淀教育网	ERX-CERNET-BKB China Education and Research Network Center, CN；CNGI-BJ-IX2-AS-AP CERNET2 IX at Tsinghua University, CN
172.17.2.25	本地局域网	NA
118.229.4.77	中国北京北京教育网	ERX-CERNET-BKB China Education and Research Network Center, CN
202.112.38.69	中国北京北京教育网	ERX-CERNET-BKB China Education and Research Network Center, CN
101.4.113.233	中国北京海淀教育网	ERX-CERNET-BKB China Education and Research Network Center, CN
101.4.115.202	中国北京海淀教育网	ERX-CERNET-BKB China Education and Research Network Center, CN
101.4.116.225	中国北京海淀教育网	ERX-CERNET-BKB China Education and Research Network Center, CN
202.97.15.89	中国北京北京教育网	CHINANET-BACKBONE No.31,Jin-rong Street, CN
202.97.81.229	中国北京北京教育网	CHINANET-BACKBONE No.31,Jin-rong Street, CN
202.97.13.202	中国北京北京教育网	CHINANET-BACKBONE No.31,Jin-rong Street, CN
202.97.22.34	中国江西电信	CHINANET-BACKBONE No.31,Jin-rong Street, CN
42.81.35.54	中国天津天津电信	CHINATELECOM-TIANJIN Tianjij,300000, CN
----------	----------	----------

IP地址	IP物理位置	自治域信息
42.81.219.24	中国天津天津电信	CHINATELECOM-TIANJIN Tianjij,300000, CN

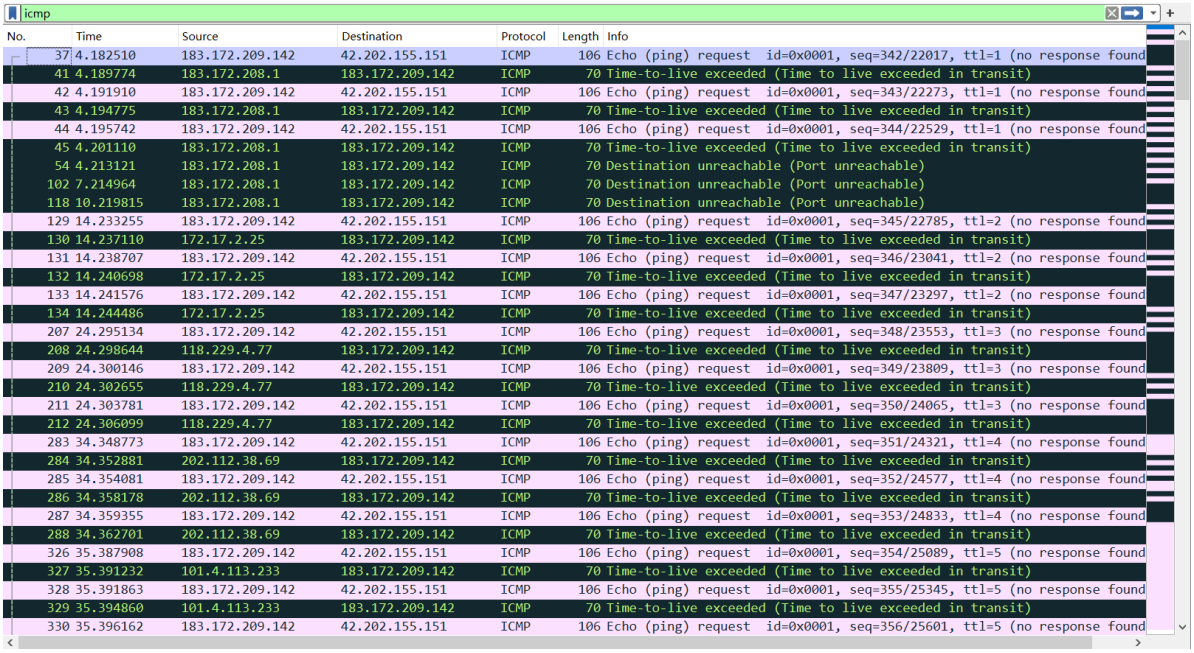
根据上表可以绘制出如下示意图：



【选做】利用 wireshark 抓包上述 traceroute 过程，在终端得到如下信息（做该部分实验时，主机采用的“www.beijing.gov.cn”域名对应的 IP 地址为 42.202.155.151 ）：

```
C:\Users\惠普\Desktop>tracert -w 4 www.beijing.gov.cn

通过最多 30 个跃点跟踪
到 ce5c4cf757a9a3e1.cname.365cyd.cn [42.202.155.151] 的路由:

  1     7 ms     2 ms     5 ms  183.172.208.1
  2     3 ms     2 ms     2 ms  172.17.2.25
  3     3 ms     2 ms     2 ms  118.229.4.77
  4     4 ms     4 ms     3 ms  qhu0.cernet.net [202.112.38.69]
  5     3 ms     3 ms     2 ms  101.4.113.233
  6     3 ms     2 ms     1 ms  101.4.113.210
  7    14 ms    13 ms    14 ms  101.4.112.82
  8   123 ms    19 ms    25 ms  101.4.113.114
  9    18 ms    18 ms    17 ms  202.112.53.253
 10     *        *        *     请求超时。
 11    19 ms    15 ms    14 ms  202.97.68.29
 12     *       21 ms    19 ms  219.148.212.46
 13     *        *        *     请求超时。
 14     *        *        *     请求超时。
 15     *        *        *     请求超时。
 16     *        *        *     请求超时。
 17     *        *        *     请求超时。
 18    22 ms    21 ms    24 ms  42.202.155.151

跟踪完成。
```

在 wireshark 中过滤出 ICMP 包，部分抓包信息如下：



观察最左侧 info 一列，可以发现由该主机发送出了一系列 ICMP 包（粉色，源 IP 地址为 183.172.209.142），其目的 IP 地址都为“www.beijing.gov.cn”域名对应的 IP 地址，即 42.202.155.151，然而发送出的各个数据包的初始寿命（ttl）一直在变化，该主机依次发送出了 3 条 ttl 为 1 、3 条 ttl 为 2 、3 条 ttl 为 3 .....的 ICMP 包给“www.beijing.gov.cn”域名对应的 IP 地址，而 ttl 值意味着该数据包被发出后在未到达目的 IP 地址前其最多可以被转发的次数，也就是说这些 ICMP 包每经过一个路由器，寿命就会减一，当其寿命衰减为 0 后，其所在的路由器会丢弃该包并向源地址（即该主机）发送 TTL = 0 的反馈，这样根据这些反馈的源 IP 地址，发送这些 ICMP 包的该主机就可以推知出为了到达某一目的 IP 地址，数据包需要依次经过哪些 IP 地址（路由器），这就是 traceroute 命令实现网络拓扑的捕获过程（要注意的是该主机只有完全接收到上一组 3 个 ICMP 包的 TTL = 0 的反馈后，才会发送下一组 3 个 ICMP 包并等待新的 3 个反馈，以避免发生混淆）。

从上面 wireshark 的抓包信息，也可以印证上述推断，不难发现，该主机依次收到了来自 183.172.208.1、172.17.2.25、118.229.4.77、202.112.38.69、101.4.113.233 的 TTL = 0 的反馈，也意味着数据包在达到目的 IP 地址前会依次经过这几个 IP 地址对应的路由器，这和前面终端给出的结果是完全吻合的。

实验思考题

(1) 当网关将本实验中记录的以太网帧中的数据报向下一跳路由器转发时，新的以太网帧相对于当前的以太网帧有哪些字段发生变化？路由器如何确定变化后的值?

发生变化的字段以及确定其变化后的值的方法如下：

- 目的 MAC 地址：把此前以太网帧中的目的 MAC 地址（应该就是网关的 MAC 地址）替换为下一跳路由器的 MAC 地址，（如果网关当前不知道下一跳路由器的 MAC 地址）而下一跳路由器的 MAC 地址的获取方法和前面任务一中提到的过程基本一致，不再展开叙述。
- 源 MAC 地址：把此前以太网帧中的源 MAC 地址替换为网关自身的 MAC 地址。
- 寿命 TTL：把此前以太网帧中的寿命 TTL 减一。
- （IP 头部检验和）：更新完上述三个字段后，将 IP 头部检验和置零，然后依据某一约定好的算法依据更新后的字段重新计算新的 IP 头部校验和，不过此处不太确定每次寿命变化是否都需要更新 IP 头部校验和。

(2) 在完成了网络部分的学习后，你有什么收获？你对于课程网络部分的教学与实验有什么意见或建议?

在完成了网络部分的学习后，我对网络的分层式架构有了比较清楚的认知，了解了一些常见的网络设备的原理和功能，以及当前的网络设计如何进行差错控制和拥塞控制。此前所谓的“网络”对于我来说就是一个“黑盒”，只知道连上这个“黑盒”就可以和指定用户或者服务端进行沟通，对它最直观的认识也无非是网速快慢，但是现在我可以利用学到的知识分析一些常见的网络通信场景了，也为未来进一步网络相关的学习打下了不错的基础。

我对课程网络部分的教学与实验的建议是希望能加入更多实践性质的更有趣味性的实验部分，目前的四个实验中大部分是验证课上所讲内容（第一个实验有较多可以自由发挥的部分），我觉得可以在每个实验的最后加入一些可选的应用部分，利用已学的知识做一些好玩的事，比如自行编写代码批量地、自动地向不同服务器请求特定的信息并筛选或者整理（大约就是自己实现一个简易的爬虫），这种自由度更高且更接近于实际应用的实验做完后，同学们应该会更有成就感，且可以鼓励他们把所学的网络知识应用到更多课堂以外的场景。