实验四 网络部分综合实验

1. 实验目的

（1）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；
（2）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；
（3）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。

2. 实验内容

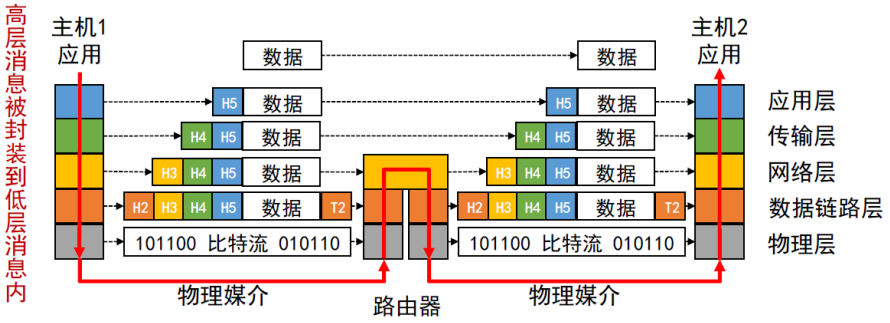
（1）回顾互联网体系结构、协议栈以及各层协议的工作原理；
（2）借助 Wireshark 抓包工具与操作系统网络工具观察并记录网络接入过程，分析了解 DHCP、ARP 等协议在互联网协议栈的初始化阶段所起的作用；
（3）以 Web 网页请求为例，借助 Wireshark 抓包工具观察、记录并深入分析 Web 请求经过各层协议封装成为链路层帧的过程；
（4）借助 traceroute 等工具，对从主机到网页服务器的路由路径进行探测，尝试分析在该路由路径上网络核心部分的拓扑关系，了解互联网网络核心部分组成方式与工作原理。

3. 实验原理

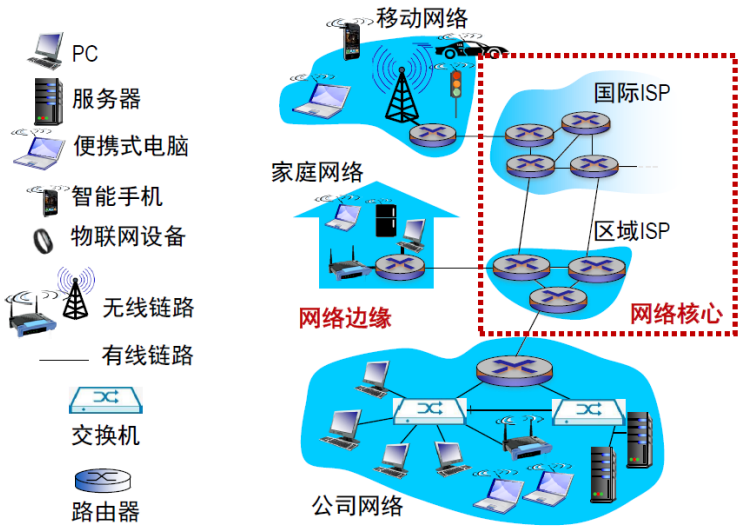
3.1 互联网体系结构与协议栈

互联网是世界上最庞大的计算机网络系统，将数十亿人与上百亿计算机设备连接在一起。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。

- 互联网协议栈



互联网的构成



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。

为了让同学们能够对互联网协议栈与互联网体系结构形成更为清晰与完整的认识，理解互联网协议栈各层次是如何在主机上工作与协作，理解以“网络的网络”为结构的互联网中数据报的路由转发过程，本次实验将分为两个环节：

（1） 理解主机接入网络的过程；

（2） 以 Web 网页应用为例分析互联网的工作过程。

在完成上述两个实验环节后，同学们应能够形成一张以 Web 应用为例的从主机角度看互联网的拓扑示意图，形成自己对于互联网工作方式与实际互联网结构的理解与认识。

3.2 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。

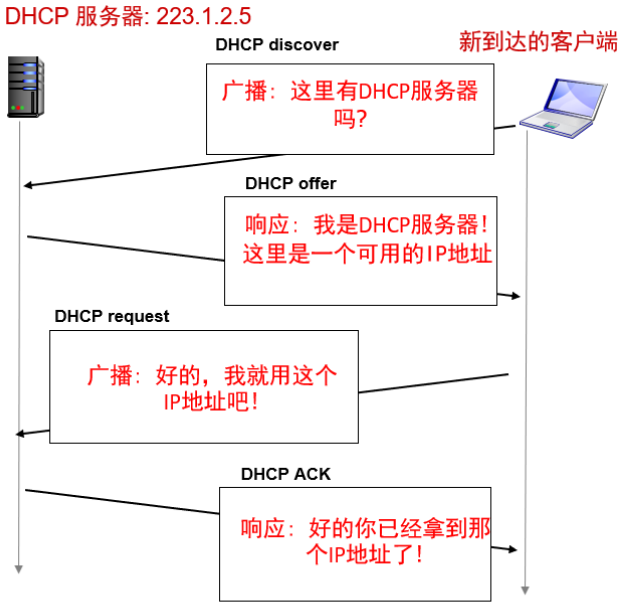
DHCP 承载于 UDP 协议，其工作流程如下：

（1）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。

（2）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）。

（3）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。

（4）DHCP 服务器收到 Request 后，回复 DHCP ACK 给客户端，完成 IP 分配。



DHCP客户–服务器交互

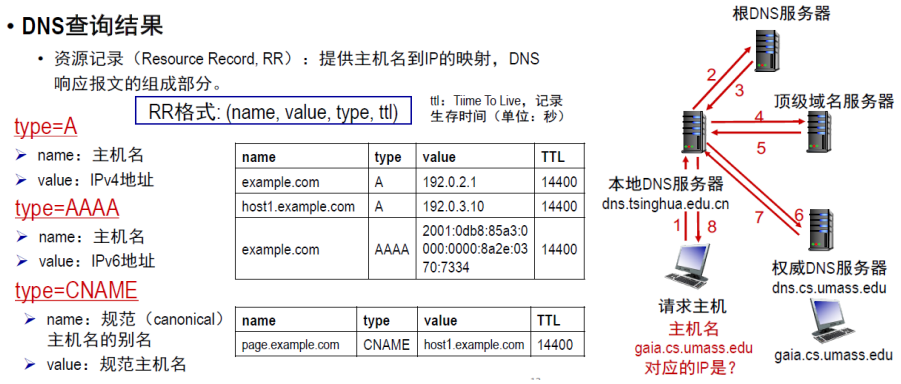
在上述四种 DHCP 包的类型中，DHCP Request 包承载了主要的网络配置分发功能，向主机提供了“Your” IP Address（服务端将要分配给客户端的 IP 地址）、Router（网关 IP 地址）、Subnet Mask（子网掩码）、Domain Name Server（DNS 服务器 IP 地址）等配置信息，实现了对于新接入主机的网络自动配置。对于 DHCP 包更详细的解析可参考[1,2]。

[1] http://www.tcpipguide.com/free/t_DHCPMessageFormat.htm
[2] https://learn.microsoft.com/en-us/windows-server/troubleshoot/dynamic-host-configuration-protocol-basics

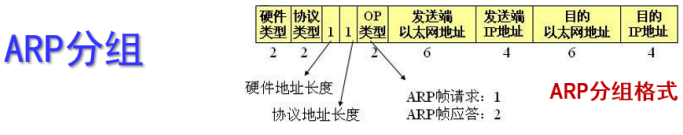
3.3 网络中的地址映射：DNS 与 ARP

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）。下面分别介绍 DNS 协议与 ARP 协议的工作原理。

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。



ARP表

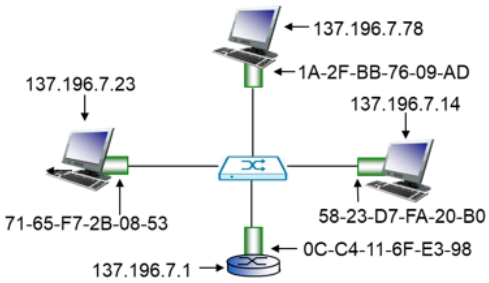
IP地址	MAC地址	TTL
137.196.7.78	1A-2F-BB-76-09-AD	12min
137.196.7.14	58-23-D7-FA-20-B0	15min
137.196.7.1	0C-C4-11-6F-E3-98	8min

```
> Ethernet II, Src: PartIIRe_3a:fd:7f (00:1c:c2:3a:fd:7f), 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: PartIIRe_3a:fd:7f (00:1c:c2:3a:fd:7f)
    Sender IP address: 59.66.203.47
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 59.66.203.1
```

ARP请求分组

```
> Ethernet II, Src: NewH3CTe_37:c9:9e (94:29:2f:37:c9:9e), Dst: PartIIRe_3a:fd:7f (00:1c:c2:3a:fd:7f)
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: NewH3CTe_37:c9:9e (94:29:2f:37:c9:9e)
    Sender IP address: 59.66.203.1
    Target MAC address: PartIIRe_3a:fd:7f (00:1c:c2:3a:fd:7f)
    Target IP address: 59.66.203.47
```

ARP响应分组



3.4 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。这一部分信息有助于理解实验中的一些现象。

在获知路径上每一跳的 IP 地址后，我们希望能进一步了解该路由器所处的自治域等信息。whois 是一个常用的域名信息搜索工具，它向不同的网络信息中心（Network Information Centers，NICs）请求某 IP 或域名的详细信息，往往包括自治域、域名拥有者联系方式等内容。本实验中我们采用互联网上公开的信息查询网站获取 IP 对应的自治域信息。

4. 实验环境和操作流程

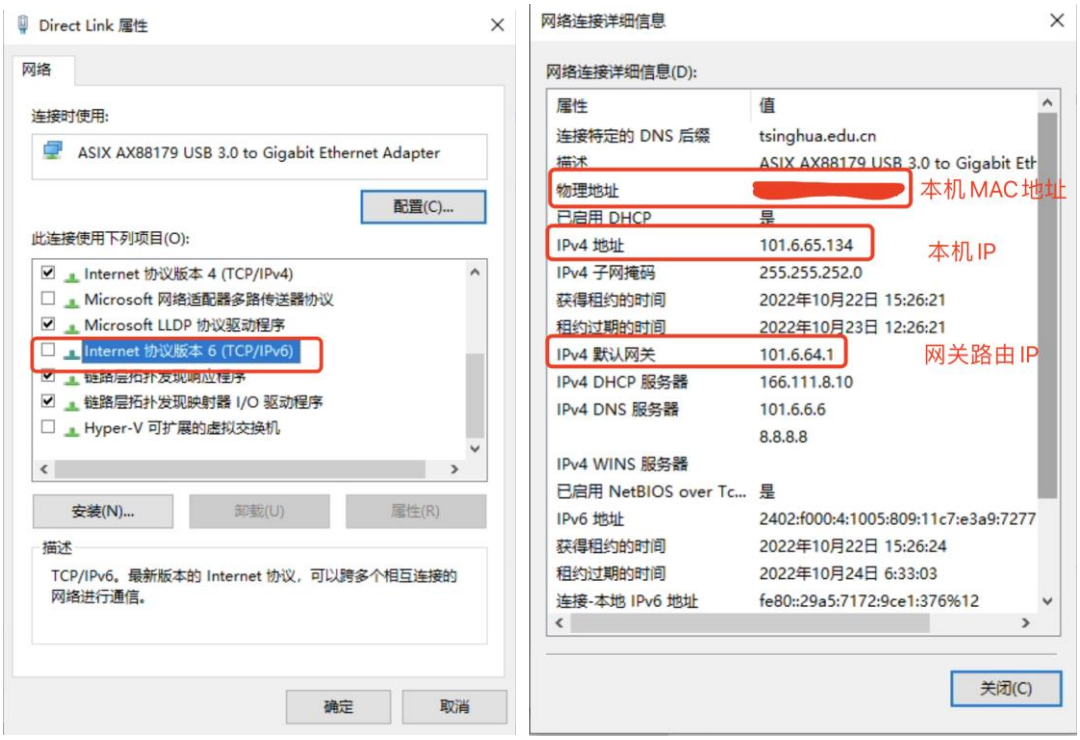
4.1 理解主机接入网络的过程

主机接入互联网时，首先需要确定各种的网络配置信息，包括网络层的本机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、默认网关MAC地址。在此，利用Wireshark进行抓包，捕获主机通过DHCP协议完成网络配置初始化的过程与获取默认网关MAC地址的ARP协议过程。本实验中，由于切换网络会中止Wireshark抓包，因此我们通过重置IP配置与ARP表来模拟接入网络的初始化过程。

首先，连接Tsinghua-Secure网络，并禁用IPv6（Windows:控制面板-网络和共享中心-更改适配器设置-双击适配器-属性-找到IPv6取消选择；macOS: 系统偏好设置-网络-Wi-Fi-高级-TCP/IP-配置IPv6-仅本地链接）以避免引入IPv6相关协

议报文。

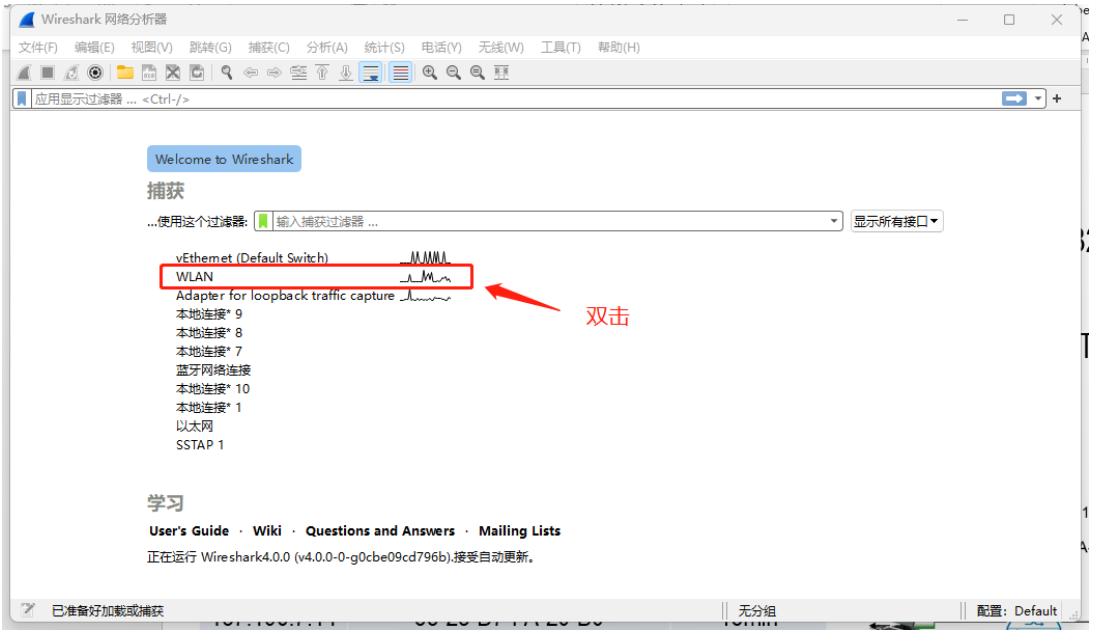
在实验开始前，查看本机IP、默认网关IP、子网掩码、本机MAC地址、DNS服务器（Windows:控制面板-网络和共享中心-更改适配器设置-双击适配器-详细信息；macOS：系统偏好设置-网络-Wi-Fi-TCP/IP（查看IP、网关）-硬件（查看本机MAC））。上述过程如下图所示。



Windows 平台禁用 IPv6 与网络关键信息记录

macOS 平台禁用 IPv6 与网络关键信息记录

打开Wireshark，选择监听WLAN链路或Wi-Fi链路（根据本机实际网络连接选择，活跃链路右侧会有流量曲线），开始抓包。

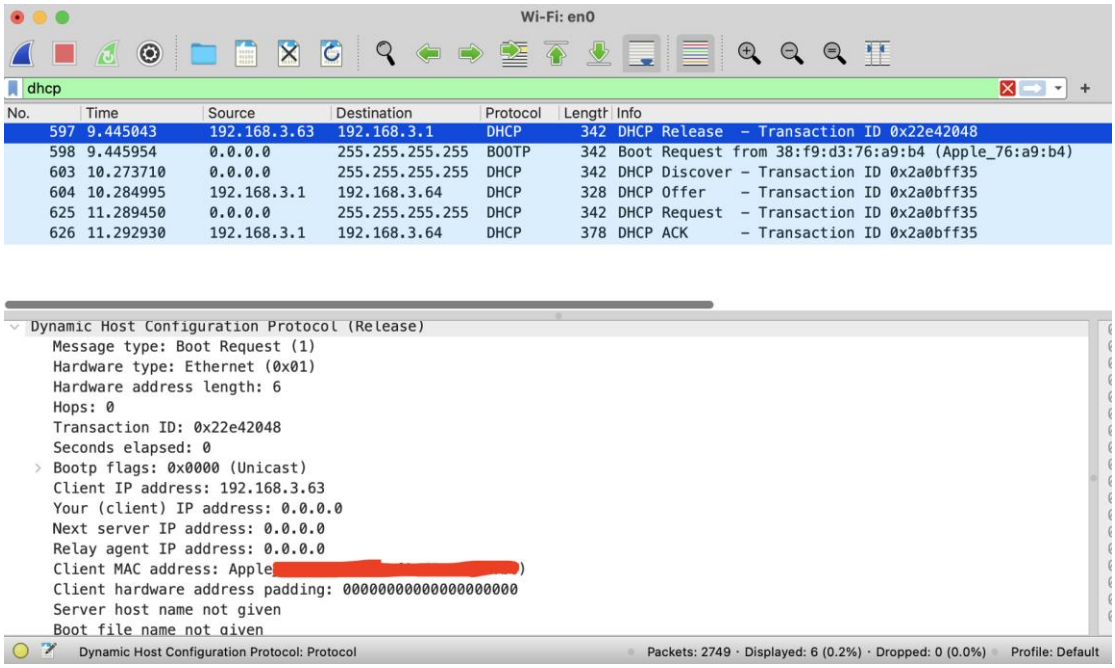


执行以下操作，对网络配置（IP配置与ARP表）进行重置，以观察网络初始化（网络接入）时的现象：

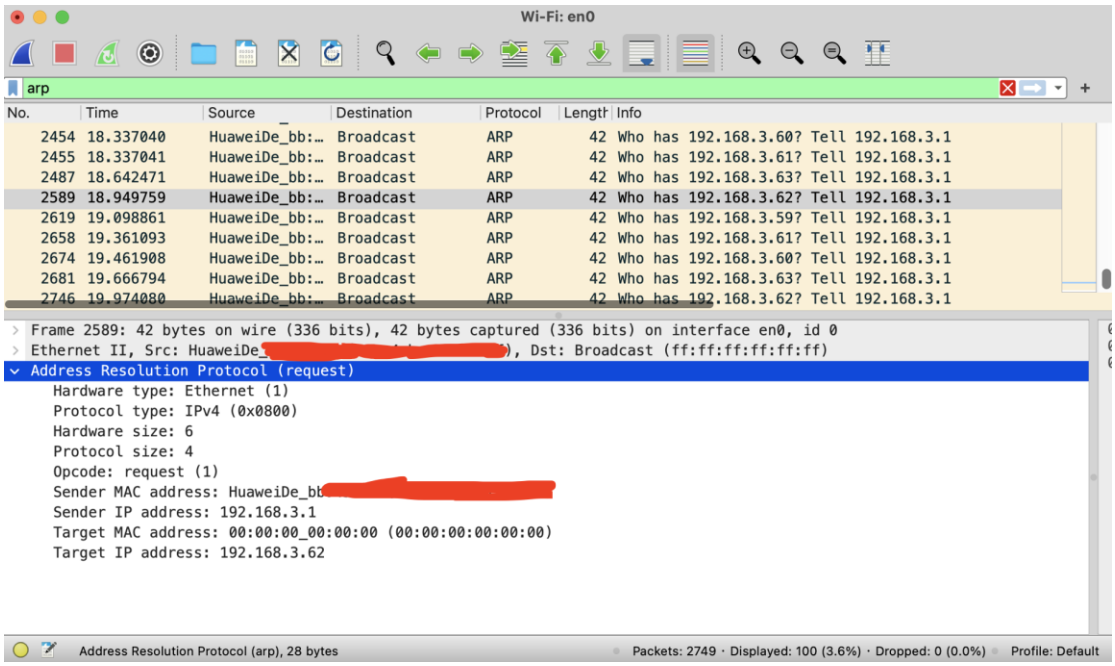
Windows 平台：
打开 powershell/CMD 管理员模式，依次输入以下命令
【查看现有 ARP 表】arp -a
【清空 IP 配置】ipconfig /release
查看当前本机 IP、默认网关 IP、本机 MAC 地址等信息是否存在，尝试能否上网
【清空 ARP 表】arp -d *
【再次查看现有 ARP 表以确认正确清空】arp -a
【触发 DHCP】ipconfig /renew
重新查看本机 IP、默认网关 IP 等信息，并与抓到的 DHCP 包进行对比
【查看新 ARP 表】arp -a
查看 ARP 表，找到默认网关对应的表项，与抓到的 ARP 包进行对比

macOS 平台：
打开 terminal，依次输入以下命令：
【查看现有 ARP 表】sudo arp -a
【清空 IP 配置】sudo networksetup -setbootp Wi-Fi
查看当前本机 IP、默认网关 IP、本机 MAC 地址等信息是否存在，尝试能否上网
【清空 ARP 表】sudo arp -a -d
【再次查看现有 ARP 表以确认正确清空】sudo arp -a
【触发 DHCP】sudo networksetup -setdhcp Wi-Fi
重新查看本机 IP、默认网关 IP 等信息，并与抓到的 DHCP 包进行对比
【查看新 ARP 表】sudo arp -a
查看 ARP 表，找到默认网关对应的表项，与抓到的 ARP 包进行对比

操作过程中可以在Wireshark的过滤器输入dhcp或arp并点击回车，可观测到对应的DHCP请求与ARP请求，如下图所示：



过滤 DHCP 包



过滤 ARP 包（内容仅供参考）

【任务一】

1. **完成 IP 配置与 ARP 表的清空操作，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；**
2. **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；**

3. **找到并截图记录 DHCP 建立过程中的 4 个包：DHCP Discover、DHCP Offer、DHCP Request、DHCP ACK，并从中找到为本机分配 IP 地址、默认网关 IP、子网掩码、DNS 服务器地址等信息的字段，标记在截图中；**
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，并根据指导书材料与个人理解，分析本实验中 DHCP 的工作过程。**
5. **在 DHCP Release 包的后续报文中，找到并截图记录本机请求网关 MAC 地址对应的 ARP 请求与响应，标记请求记录中请求的 IP 地址与响应记录中回复的 MAC 地址，与 ARP 表对比，指出两者的关系并分析本实验中 ARP 的工作过程。**

4.2 以 Web 网页应用为例分析互联网的工作过程

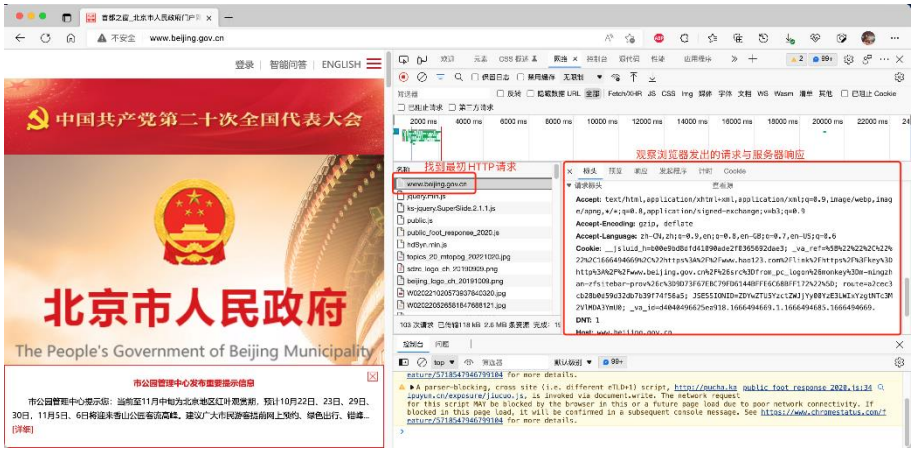
Web网页应用是最常见的互联网应用，本次实验中我们以Web网页应用为例分析互联网的工作过程。在本实验中，我们通过浏览器发起Web页面的请求，借助浏览器开发者工具查看浏览器发出的应用层原始报文，再通过Wireshark抓包获取主机实际发往网络中的以太网帧。

为了抓取到DNS请求，首先需清空本机DNS缓存且关闭网络代理：

```
Windows 平台：
打开 powershell 管理员模式，输入以下命令
ipconfig /flushdns

macOS 平台：
打开 terminal，输入以下命令：
sudo killall -HUP mDNSResponder
```

打开浏览器，进入**无痕模式（浏览器缓存会影响实际发送的数据包；重复试验时需要关闭所有开启的无痕窗口，并重新进入无痕模式）**，按F12启动开发者工具（Safari为command+option+i），切换到“网络”标签页；在地址栏输入并访问http://www.beijing.gov.cn/，观察“网络”标签栏内的变化并选择浏览器最初发出的请求，并从右侧窗口中“标头”-“请求标头”中观察请求报文，部分浏览器可以点击“查看源”获得原始的应用层请求报文。



浏览器开发者工具示例

停止抓包，在 Wireshark 中分析访问过程（提示：Wireshark 过滤设置 http.host=="www.beijing.gov.cn"），并回答以下问题。

【任务二】

1. 找到本机向 www.beijing.gov.cn 发出的第一条 HTTP 请求报文，根据包内容填写以下表格。

<table>
<tr><th colspan="10">Ethernet II</th></tr>
<tr><td colspan="4">目的 MAC 地址</td><td colspan="4">源 MAC 地址</td><td>类型</td></tr>
<tr><td colspan="4">HuaweiTe_b9:7f:04(90:03:25:b9:7f:04)</td><td colspan="4">IntelCor_6e:bf:2c(d0:ab:d5:6e:bf:2c)</td><td>IPv4(0x0800)</td></tr>
<tr><th colspan="10">IP</th></tr>
<tr><td>版本</td><td>头部
长度</td><td colspan="2">服务
类型</td><td colspan="6">数据报长度</td></tr>
<tr><td>4</td><td>20bytes</td><td colspan="2">（略）</td><td colspan="6">480</td></tr>
<tr><td colspan="4">16bit 标识</td><td colspan="3">标志</td><td>片偏移</td></tr>
<tr><td colspan="4">0xe76a</td><td colspan="3">0x2</td><td>0</td></tr>
<tr><td colspan="2">TTL</td><td colspan="2">上层协议</td><td colspan="6">头部检验和</td></tr>
<tr><td colspan="2">64</td><td colspan="2">TCP</td><td colspan="6">0x0000</td></tr>
<tr><td colspan="10">32bit 源 IP 地址</td></tr>
<tr><td colspan="10">183.172.209.142</td></tr>
<tr><td colspan="10">32bit 目的 IP 地址</td></tr>
<tr><td colspan="10">42.81.219.24</td></tr>
<tr><td colspan="10">选项</td></tr>
<tr><td colspan="10">（略）</td></tr>
<tr><th colspan="10">TCP</th></tr>
<tr><td colspan="5">源端口号</td><td colspan="5">目的端口号</td></tr>
<tr><td colspan="5">8333</td><td colspan="5">80</td></tr>
<tr><td colspan="10">序号</td></tr>
<tr><td colspan="10">1(原始为 1408879864)</td></tr>
<tr><td colspan="10">确认号</td></tr>
<tr><td colspan="10">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="2">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="2">512</td></tr>
<tr><td colspan="5">检验和</td><td colspan="5">紧急数据指针</td></tr>
<tr><td colspan="5">0x9077</td><td colspan="5">（略）</td></tr>
<tr><td colspan="10">选项</td></tr>
<tr><td colspan="10">（略）</td></tr>
<tr><th colspan="10">HTTP</th></tr>
<tr><td colspan="10">请求行：GET / HTTP/1.1\r\n</td></tr>
<tr><td colspan="3">Host:</td><td colspan="7">www.beijing.gov.cn\r\n</td></tr>
<tr><td colspan="3">User-Agent:</td><td colspan="7">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>

2. 按照自顶向下的顺序，分析解释浏览器网页访问请求是如何被逐层封装为上述记录的以太网帧，并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。

提示与说明：

（1） 应用层：可以对比通过浏览器开发者工具得到的请求源代码，并参考课程讲授的 HTTP 协议相关内容；

（2） 传输层：检验和不需要计算；

（3） 网络层：源 IP 地址参考任务一；目的 IP 地址依赖 DNS 协议，需要抓取对应 www.beijing.gov.cn 的 DNS 请求与响应（Wireshark 过滤设置 dns.qry.name=="www.beijing.gov.cn"），分析响应内容并指出何处体现了域名与 IP 的关系；检验和不需要计算；

（4） 链路层：参考任务一。

接下去，将利用 traceroute 命令追踪本机到 HTTP 服务器之间经过的核心网络路由（在 Windows 中对应命令为 tracert）：

```
Windows 平台：
打开 powershell，输入以下命令(-w 4 为设置 4 秒超时):
tracert -w 4 www.beijing.gov.cn

macOS 平台：
打开 terminal，输入以下命令（-I 为发送 ICMP 包，-w 4 设置 4 秒超时）：
traceroute -I -w 4 www.beijing.gov.cn
```

通过上述命令，得到本机到 HTTP 服务器之间的路径上的的各跳路由器 IP，如下图所示。

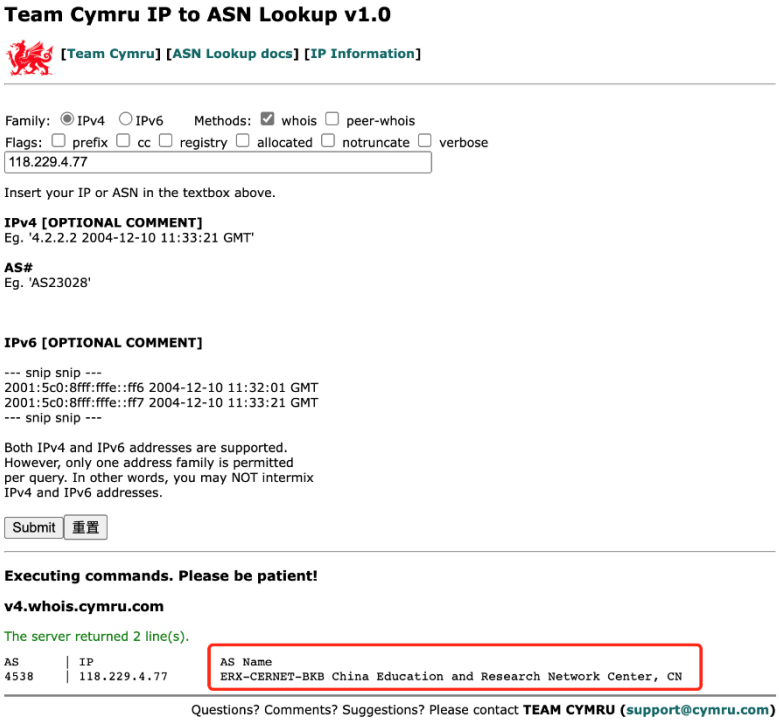
```
(base)  hanzhenyu@mbp13  ~  traceroute -I -w 4 www.beijing.gov.cn
traceroute: Warning: www.beijing.gov.cn has multiple addresses; using 42.202.
155.151
traceroute to ce5c4cf757a9a3e1.cname.365cyd.cn (42.202.155.151), 64 hops max,
 72 byte packets
 1  183.172.232.1 (183.172.232.1)  25.061 ms  21.665 ms  23.803 ms
 2  172.17.2.29 (172.17.2.29)  2.008 ms  5.945 ms  1.695 ms
 3  118.229.4.77 (118.229.4.77)  3.495 ms  3.793 ms  3.641 ms
 4  qhu0.cernet.net (202.112.38.69)  4.891 ms  4.164 ms  3.271 ms
 5  101.4.113.233 (101.4.113.233)  4.464 ms  7.905 ms  4.950 ms
```

traceroute 追踪路由

在在各类站长工具（例如 https://ip.tool.chinaz.com/）搜索对应 IP，可查找到对应路由的 IP 物理位置，如下图所示。

查询 IP 对应的物理位置

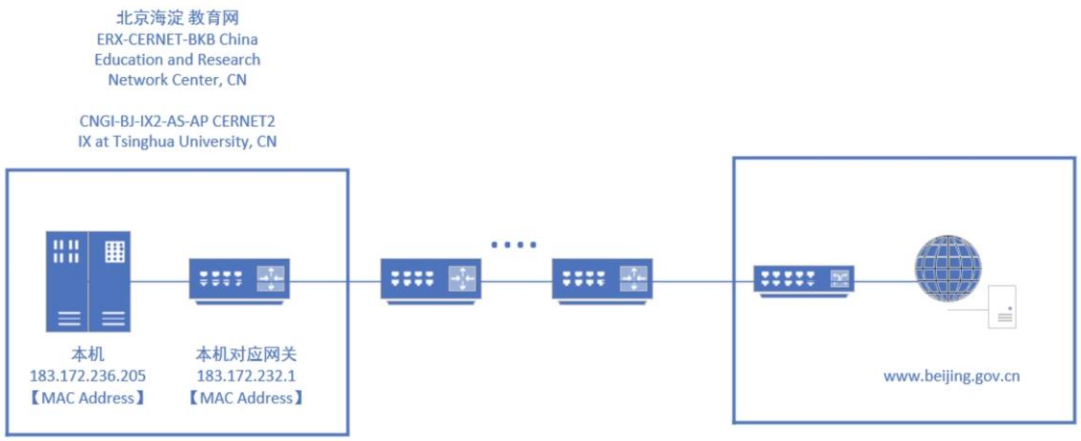
通过 whois ASN 查找表工具（https://whois.cymru.com/），可查询到 IP 或域名对应的自治域，如下图所示。



查询 IP 对应的自治域信息

【任务三】

1. **通过 tracert/traceroute 记录本机到 www.beijing.gov.cn 的各跳路由器 IP；**
2. **通过在线 IP 查询工具，查找 traceroute 中各跳路由器的物理位置并记录；**
3. **通过在线自治域查询工具，查找 traceroute 中各跳路由对应的自治域并记录；**
4. **绘制本机到 www.beijing.gov.cn 的网络拓扑，标记各个节点的 IP 地址、MAC 地址（如果可知）、IP 物理位置、自治域信息，并框出处于同一个自治域下的路由器。**



网络拓扑示例（采用 Visio 绘制）

【任务三选做】

1. 利用 Wireshark 抓包上述 traceroute 过程，分析 traceroute 命令如何实现网络拓扑的捕获（提示：过滤 ICMP 包）。

5. 实验考核

（1）抓取网络接入/初始化过程中的 DHCP 包、ARP 包，解释计算机连接至互联网的过程；

（2）抓取本机请求 www.beijing.gov.cn 网页的数据包，解释应用层报文被逐层封装的过程、各层包头字段的含义以及地址映射的过程；

（3）通过 traceroute 分析主机向目标网页服务器发出的数据报在网络中的转发过程并结合所有实验内容绘制本实验访问到的网络拓扑。

6. 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？

（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？

7. 实验参考资料总结

（1）DHCP 协议：

http://www.tcpipguide.com/free/t_DHCPMessageFormat.htm

https://learn.microsoft.com/en-us/windows-server/troubleshoot/dynamic-host-configuration-protocol-basics

（2）浏览器开发者工具使用：

https://segmentfault.com/a/1190000039336836?utm_source=sf-similar-article

（3）Wireshark 使用
https://blog.csdn.net/qq_44204058/article/details/123014013

（4）traceroute 命令使用
https://blog.csdn.net/weixin_32075603/article/details/116593870
https://blog.csdn.net/dillanzhou/article/details/125754752
https://www.cnblogs.com/zhangpeiyao/p/15433711.html
https://linux.die.net/man/8/traceroute

（5）IP 地址查询
https://ip.tool.chinaz.com/

（6）Whois 自治域在线查询工具
https://whois.cymru.com/