计算机学院 计算机网络 课程实验报告

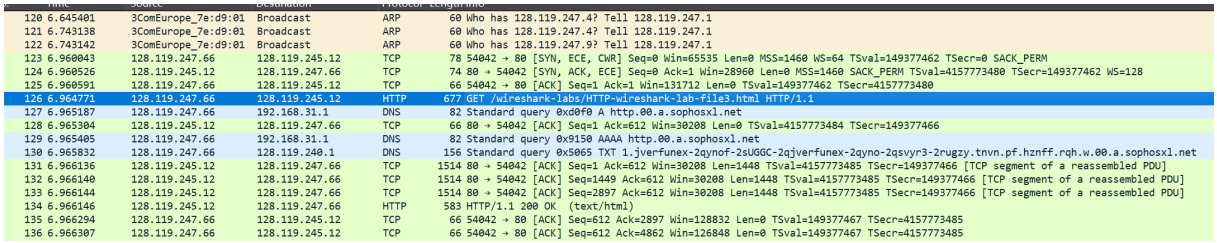
实验题目：Ethernet and ARP		学号：202200400053
日期：2024-05-23	班级： 2 班	姓名： 王宇涵
Email：1941497679@qq.com		

实验方法介绍：

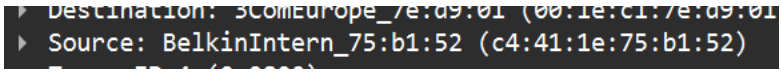
使用 wireShark 进行数据包的抓取，分别分析 Ethernet 和 ARP 协议，深刻理解链路层协议，加强对于理论课知识的理解.

实验过程描述：

一、Ethernet

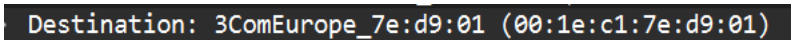


1. **你的计算机的 48 位以太网地址是什么？**



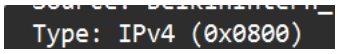
答 ：c4:41:1e:75:b1:52

2. **以太网帧中的 48 位目标地址是什么？这是 gaia.cs.umass.edu 的以太网地址吗？（提示：答案是否定的）。哪个设备具有这个以太网地址？[注意：这是一个重要的问题，也是学生有时会答错的问题。重新阅读教科书的 483-484 页，确保你理解这里的答案。]**



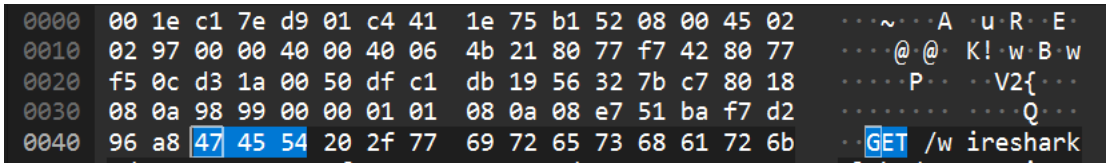
答 ：00:1e:c1:7e:d9:01，不是 gaia.cs.umass.edu 的以太网地址，应该是连接子网的路由器地址

3. **携带 HTTP GET 请求的以太网帧中，两字节帧类型字段的十六进制值是什么？这对应于哪个上层协议？**

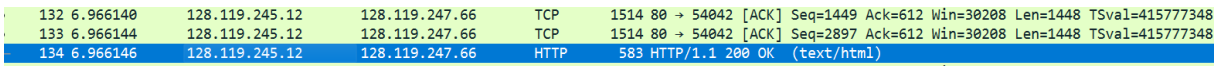


答 ：0x0800，对应着 IPv4

4. **从以太网帧的起始位置算起，“GET”中的 ASCII 字符“G”出现在以太网帧中的第几字节？不要计算任何前导比特，即假设以太网帧以以太网帧的目标地址开始。**



答 ：4 * 16 + 3 = 67



5. **以太网源地址的值是什么？这是你计算机的地址还是 gaia.cs.umass.edu 的地址？（提示：答案**

是否定的）。哪个设备具有这个以太网地址？

```
Source: 3ComEurope_7e:d9:01 (00:1e:c1:7e:d9:01)
```

答 ：00:1e:c1:7e:d9:01，这不是两者的地址，是连接该子网的路由器的地址.

6. 以太网帧中的目标地址是什么？这是你计算机的以太网地址吗？

```
Destination: BelkinIntern_75:b1:52 (c4:41:1e:75:b1:52)
```

答 ：c4:41:1e:75:b1:52，这是我计算机的以太网地址

7. 给出两字节帧类型字段的十六进制值。这对应于哪个上层协议？

```
Type: IPv4 (0x0800)
```

答 ：0x0800，对应着 IPv4

8. 从以太网帧的起始位置算起，“OK”中的 ASCII 字符“O”（即 HTTP 响应码）出现在以太网帧中的第几字节？不要计算任何前导比特，即假设以太网帧以以太网帧的目标地址开始。

```
0000  48 54 54 50 2f 31 2e 31  20 32 30 30 20 4f 4b 0d   HTTP/1.1  200 OK·
```

答 ： 出现在第 14 个字节

9. 多少以太网帧（每个帧包含一个 IP 数据报，每个数据报包含一个 TCP 段）携带了完整的 HTTP “OK 200 ...”回复消息的数据？

```
[4 Reassembled TCP Segments (4861 bytes): #131(1448), #132(1448), #133(1448), #134(517)]
```

答 ：4 个

二、ARP

命令行输入 arp -a 查看当前计算机 arp cache

```
C:\Users\Lenovo>arp -a

接口: 192.168.217.1 --- 0x9
  Internet 地址         物理地址              类型
  192.168.217.255       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
  224.0.0.252           01-00-5e-00-00-fc     静态
  234.5.6.7             01-00-5e-05-06-07     静态
  238.238.238.238       01-00-5e-6e-ee-ee     静态
  239.238.237.236       01-00-5e-6e-ed-ec     静态
  239.255.255.250       01-00-5e-7f-ff-fa     静态
  255.255.255.255       ff-ff-ff-ff-ff-ff     静态

接口: 192.168.131.1 --- 0xa
  Internet 地址         物理地址              类型
  192.168.131.255       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
  224.0.0.252           01-00-5e-00-00-fc     静态
  234.5.6.7             01-00-5e-05-06-07     静态
  238.238.238.238       01-00-5e-6e-ee-ee     静态
  239.238.237.236       01-00-5e-6e-ed-ec     静态
  239.255.255.250       01-00-5e-7f-ff-fa     静态
```

10. ARP 缓存中存储了多少条目？

答 ： 共有 10 + 9 = 19 个条目

11. ARP 缓存中每个显示的条目包含什么内容？

答 ： 包含 IP 地址，物理地址(以太网地址)和类型

```
  108 6.344929    BelkinIntern_75:b1:… Broadcast           ARP     42 Who has 128.119.247.1? Tell 128.119.247.66
  109 6.347010    3ComEurope_7e:d9:01  BelkinIntern_75:b1:… ARP     60 128.119.247.1 is at 00:1e:c1:7e:d9:01
```

12. 你的计算机发出的包含 ARP 请求消息的以太网帧中的源地址的十六进制值是什么？

```
▸ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
▸ Source: BelkinIntern_75:b1:52 (c4:41:1e:75:b1:52)
```

答 ：c4:41:1e:75:b1:52

13. 你的计算机发出的包含 ARP 请求消息的以太网帧中的目标地址的十六进制值是什么？与该地址对应的设备（如果有的话）是什么（例如，客户端、服务器、路由器、交换机或其他设备）？

答 ：ff:ff:ff:ff:ff:ff,对应的设备类型是网络上的所有设备，包括客户端、服务器、路由器、交换机等。

14. 两字节以太网帧类型字段的十六进制值是什么？这对应于哪个上层协议？

```
Type: ARP (0x0806)
```

答 ：0x0806(ARP)

15. ARP 操作码字段从以太网帧的起始位置开始算起是第几个字节？

```
0000  ff ff ff ff ff ff c4 41  1e 75 b1 52 08 06 00 01   ·······A ·u·R····
0010  08 00 06 04 00 01 c4 41  1e 75 b1 52 80 77 f7 42   ·····A ·u·R·w·B
0020  00 00 00 00 00 00 80 77  f7 01                     ·······w ··
```

答 ： 第 21 个字节

16. 你计算机发送的 ARP 请求消息中的操作码字段的值是什么？

```
Opcode: request (1)
```

答 ：1

17. ARP 请求消息是否包含发送方的 IP 地址？如果答案是肯定的，那么该值是什么？

```
Sender MAC address: BelkinIntern_75:b1:52 (c4:41:1e:75:b1:52)
Sender IP address: 128.119.247.66
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
Target IP address: 128.119.247.1
```

答 ： 包含，值为 128.119.247.66

18. 你计算机发送的 ARP 请求消息中请求的对应以太网地址的设备的 IP 地址是什么？

答 ：128.119.247.1

```
108 6.344929    BelkinIntern_75:b1:… Broadcast          ARP    42 Who has 128.119.247.1? Tell 128.119.247.66
109 6.347010    3ComEurope_7e:d9:01  BelkinIntern_75:b1:… ARP  60 128.119.247.1 is at 00:1e:c1:7e:d9:01
```

19. 你计算机接收到的 ARP 回复消息中的操作码字段的值是什么？

```
Protocol size: 4
Opcode: reply (2)
Sender MAC address: 3Com
```

答 ：2

20. 最后，让我们看看 ARP 请求消息的答案！与你计算机发送的 ARP 请求消息中指定的 IP 地址（见问题 18）对应的以太网地址是什么？

```
60 128.119.247.1 is at 00:1e:c1:7e:d9:01
```

答 ：00:1e:c1:7e:d9:01

21. 我们已经查看了通过 Wireshark 捕获到的你的计算机发送的 ARP 请求消息和响应的 ARP 回复消息。但是，在这个网络中还有其他设备也在发送 ARP 请求消息，你可以在捕获的流量中找到这些消息。为什么在你的捕获记录中没有看到响应这些其他 ARP 请求消息的 ARP 回复？

答 ： 因为响应 ARP 报文只有请求 ARP 的对应节点才能收到，而我只能看到与我的计算机直接相关的流量，而看不到其他设备之间的通信。

分析：

ARP（地址解析协议）和 Ethernet 协议是网络通信中不可或缺的两部分。

ARP 用于将网络层地址（如 IPv4 地址）映射到数据链路层地址（如 MAC 地址），当一台设备需要与同一网络中的另一台设备通信时，它会广播一个包含目标 IP 地址的 ARP 请求，目标设备收到请求后回复包含其 MAC 地址的 ARP 回复消息，这样发送设备就能将 IP 地址与 MAC 地址对应起来。

Ethernet 协议定义了数据链路层和物理层的标准，通过以太网帧在网络中传输数据，每个帧包括前导码、目标和源 MAC 地址、类型/长度字段、数据字段和帧校验序列，以确保数据正确传输。以太网协议通过交换机连接多个设备，并利用 MAC 地址进行设备间通信，处理数据传输中的冲突和错误检测，是局域网（LAN）的基础。

结论：

通过完成上述问题，我对 ARP（地址解析协议）和以太网协议有了更加深入和实际的理解。

在 ARP 协议方面，我学会了如何通过 Wireshark 捕获并分析 ARP 请求和回复消息，了解到 ARP 请求是通过广播发送的，目标地址通常是`ff:ff:ff:ff:ff:ff`，而 ARP 回复是单播的，只有请求设备可以接收到。此外，我明白了 ARP 缓存的重要性以及如何查看和解释缓存中的条目，包括 IP 地址、物理地址和类型。

在以太网协议方面，我学习了以太网帧的结构和不同字段的位置，例如目标 MAC 地址、源 MAC 地址、帧类型字段以及数据字段的位置和含义。通过计算字节偏移量，我能够准确定位和解释帧中数据的位置，例如 HTTP 请求和响应消息中的 ASCII 字符的位置。这些知识不仅帮助我理解了网络通信的基本原理，还提升了我使用网络分析工具的能力。

总的来说，这次实验使我对网络协议的实际应用有了更全面的认识，提高了我在网络工程领域的实践技能。