山东大学 计算机 学院

计算机网络 课程实验报告

学号：202400130240	姓名： 贾宗翰	班级：24.6
实验题目： Wireshark Lab: Ethernet and ARP v8.1		
实验学时：2h	实验日期： 2025.11.11	
实验目的： 研究以太网协议和 ARP 协议		
硬件环境： 联想拯救者		
软件环境：wireshark，edge 浏览器		

实验步骤与内容：

让我们开始捕获一组以太网帧进行研究。为了做到这一点，当然，你需要为你的 PC 或 Mac 提供有线以太网连接——考虑到无线 WiFi 和蜂窝网络日益普及，这不是一个常见的场景。如果你无法在实时以太网连接上运行 Wireshark，你可以下载一个在作者的计算机上按照以下步骤捕获的数据包跟踪。此外，即使你已经捕获了自己的跟踪，你也可能会发现下载这个跟踪很有价值，并在你探索下面的问题时使用它以及你自己的跟踪。

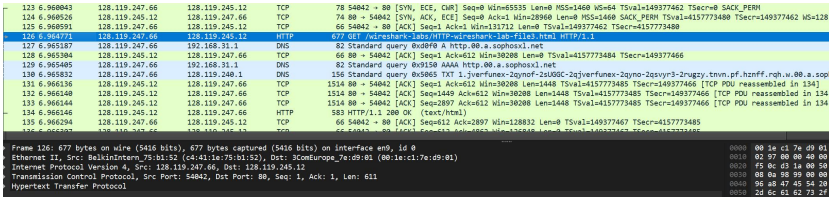
请执行以下操作：首先，确保您浏览器中之前下载的文档缓存已清空。

启动 Wireshark，并在浏览器中输入以下网址：http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html。您的浏览器应该会显示相当长的美国权利法案。

• 停止 Wireshark 数据包捕获。首先，找到从您的计算机发往 gaia.cs.umass.edu 的 HTTP GET 消息的包编号（Wireshark 窗口上方的最左列），以及 gaia.cs.umass.edu 发送给您的计算机的 HTTP 响应消息的开头。您应该会看到一个看起来像这样的屏幕（其中屏幕截图中的数据包 126 包含 HTTP GET 消息）.

由于这个实验室是关于以太网和 ARP，我们对像 IP、TCP 或 HTTP 这样的高层协议不感兴趣。我们关注的是以太网帧和 ARP 消息！

让我们先看一下包含 HTTP GET 消息的以太网帧。（回想一下，HTTP GET 消息是带在 TCP 段内的，TCP 段又带在 IP 数据报内，而 IP 数据报又带在以太网帧内；如果你觉得这个封装概念有点困惑，请重新阅读文本中的 1.5.2 节）。在数据包详情窗口中展开以太网 II 信息。注意，以太网帧的内容（头部和负载）在数据包内容窗口中显示。你的显示应该与图 2 所示的相似。



1. 你电脑的 48 位以太网地址是什么？
   BelkinIntern_75:b1:52(c4:41:1e:75:b1:52)

2. 以太网帧中的 48 位目的地址是什么？这是 gaia.cs.umass.edu 的以太网地址吗？

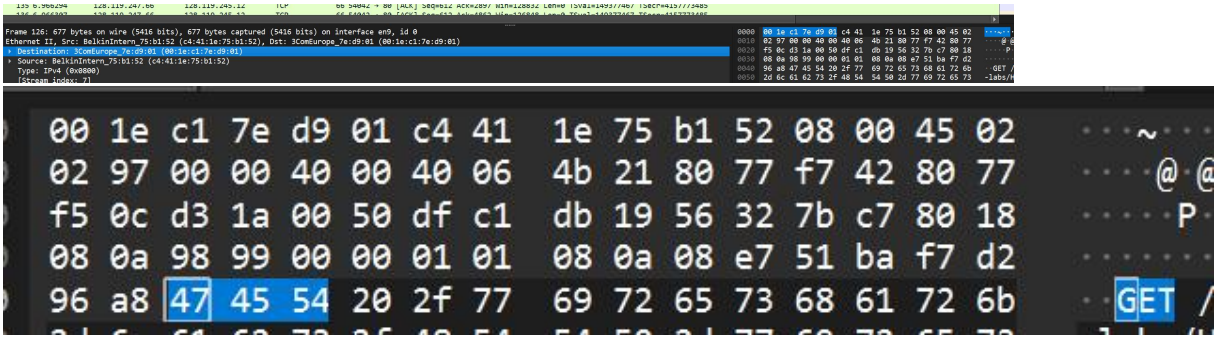
（提示：答案是否定的）。哪个设备的以太网地址是这个？【注意：这是一个重要问题，有时学生会答错。请重新阅读教材的第 483-484 页，确保你理解这里的答案。】

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

第一个路由器地址。

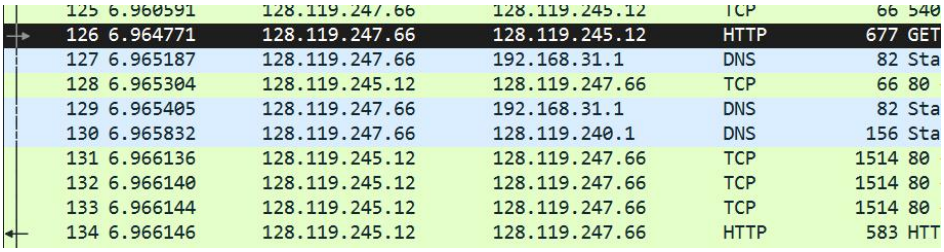
3. 在承载 HTTP GET 请求的以太网帧中，两个字节的帧类型字段的十六进制值是什么？这对应于哪个上层协议？

4. 从以太网帧的起始位置开始，ASCII 字母 “G” 在 “GET” 中出现的位置是以太网帧中的第多少个字节？请不要计算任何前导位，即假设以太网帧从以太网帧的目的地址开始。



分析得知前面有 64+2 = 66 字节，所以这是第 67 个。

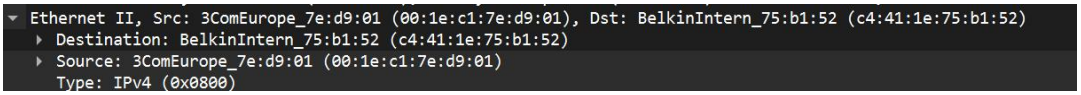
接下来，根据包含 HTTP 响应消息首字节的以太网帧的内容回答以下问题。



125	6.960591	128.119.247.66	128.119.245.12	TCP	66 540
126	6.964771	128.119.247.66	128.119.245.12	HTTP	677 GET
127	6.965187	128.119.247.66	192.168.31.1	DNS	82 Sta
128	6.965304	128.119.245.12	128.119.247.66	TCP	66 80
129	6.965405	128.119.247.66	192.168.31.1	DNS	82 Sta
130	6.965832	128.119.247.66	128.119.240.1	DNS	156 Sta
131	6.966136	128.119.245.12	128.119.247.66	TCP	1514 80
132	6.966140	128.119.245.12	128.119.247.66	TCP	1514 80
133	6.966144	128.119.245.12	128.119.247.66	TCP	1514 80
134	6.966146	128.119.245.12	128.119.247.66	HTTP	583 HTT

，134

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）。哪个设备的以太网地址是这个？



如图 source 是答案，第一个路由器的地址。

6. 在以太网帧中，目标地址是什么？这是你计算机的以太网地址吗？

如图 destination 是答案，是

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？

见上，IPv4

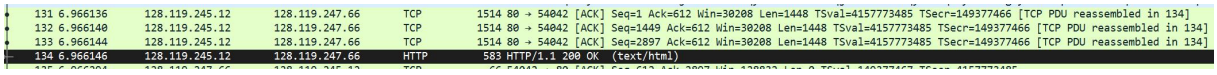
8. 从以太网帧开始的第一个字节到 ASCII 字符“O” 出现在以太网帧中的位置（即，HTTP 响应代码中的“OK”），有多少字节？不要计算任何前导比特，即假设以太网帧以以太网帧的目标地址开始。

这是分开的，在 131 里面：

```
c4 41 1e 75 b1 52 00 1e  c1 7e d9 01 08 00 45 02    ·A·u·R·· ·~····E·
05 dc ed 6c 40 00 3f 06  5b 6f 80 77 f5 0c 80 77    ···l@·?· [o·w···w
f7 42 00 50 d3 1a 56 32  7b c7 df c1 dd 7c 80 10    ·B·P··V2 {····|··
00 ec e4 36 00 00 01 01  08 0a f7 d2 96 ad 08 e7    ···6···· ········
51 ba 48 54 54 50 2f 31  2e 31 20 32 30 30 20 4f    Q·HTTP/1 .1 200 O
```

分析是第 67 个。

9. 有多少个以太网帧（每个帧包含一个 IP 数据报，每个数据报包含一个 TCP 段）携带 HTTP “OK 200 ...” 回复消息的部分数据？



分析得知，一共是 131-134 一共 4 个。

地址解析协议

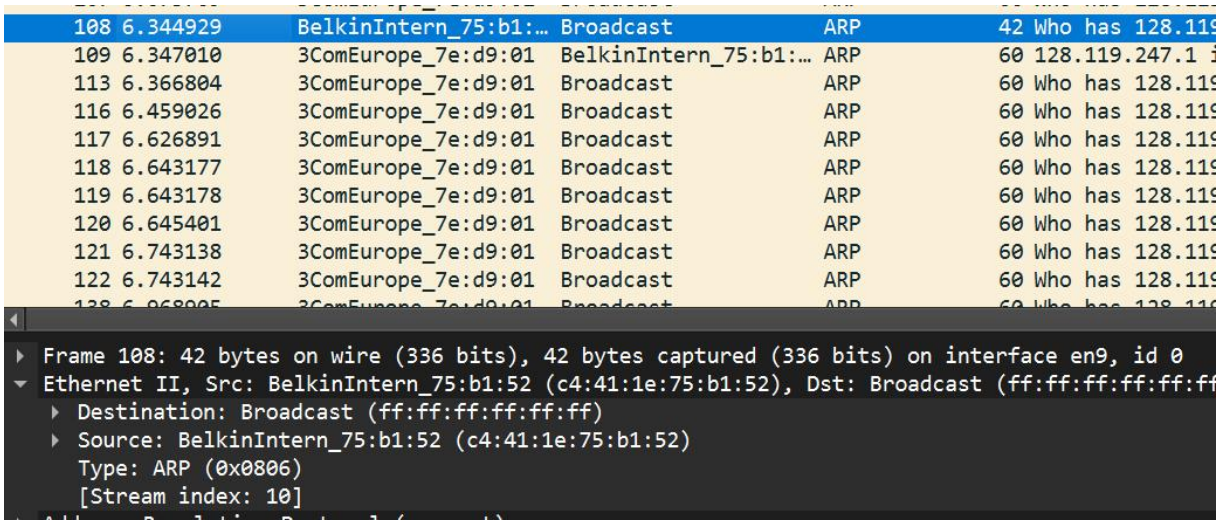
在这一节中，我们将观察 ARP 协议的实际应用。我们强烈建议您在继续之前重新阅读文本的第 6.4.1 节。 ARP 缓存 请回忆一下，ARP 协议通常会在您的计算机上维护一个 IP 到以太网地址转换对的缓存。arp 命令（在 DOS、MacOS 和 Linux 中）用于查看和操作该缓存的内容。由于 arp 命令和 ARP 协议同名，因此容易混淆。但请记住，它们是不同的——arp 命令用于查看和操作 ARP 缓存的内容，而 ARP 协议定义了发送和接收消息的格式和含义，并定义了 ARP 消息传输和接收时采取的行动。让我们看看您计算机上的 ARP 缓存内容。在 DOS、MacOS 和 Linux 中，“arp -a”命令将显示您计算机上 ARP 缓存的内容。因此在命令行中输入“arp -a”。在其中一位作者的计算机上输入该命令的结果如图 3 所示。

```
kurose@noho4 ~ % arp -a
gw-vlan-2471.cs.umass.edu (128.119.247.1) at 0:1e:c1:7e:d9:1 on en9 ifscope [ethernet]
sammac.cs.umass.edu (128.119.247.19) at (incomplete) on en9 ifscope [ethernet]
robomac.cs.umass.edu (128.119.247.79) at 78:7b:8a:ac:ad:e1 on en9 ifscope [ethernet]
```

10. 你的 ARP 缓存中存储了多少条目？ 3

11. 每个显示的 ARP 缓存条目中包含什么？

包含了 IP 地址与 MAC 地址的映射。



12. 在包含您计算机发送的 ARP 请求消息的以太网帧中，源地址的十六进制值是什么？

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

13. 在包含您计算机发送的 ARP 请求消息的以太网帧中，目标地址的十六进制值是什么？那个地址对应的设备是什么（例如，客户端、服务器、路由器、交换机或其他...）？

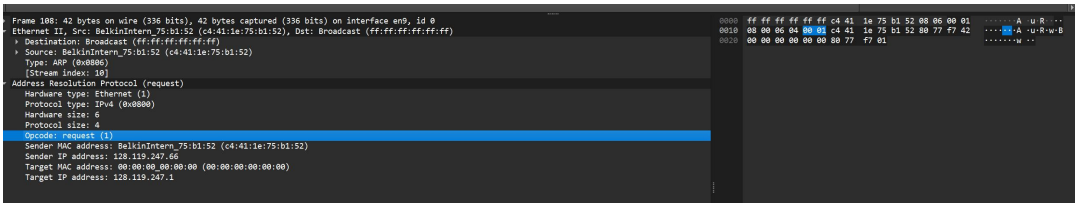
```
Destination: Broadcast (ff:ff:ff:ff:ff:ff)
```

广播，也就是子网中的所有主机。

14. 两字节的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)
```

15. ARP 操作码字段从以太网帧的开始处有多少字节？



观察得知有 16+4=20 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)
```

17. ARP 请求消息是否包含发送者的 IP 地址？如果答案是肯定的，那这个值是什么？

```
Sender IP address: 128.119.247.66
```

18. 在你的计算机发送的 ARP 请求消息中，请求的设备的 IP 地址是什么？

```
Target IP address: 128.119.247.1
```

现在找到对你的计算机的 ARP 请求消息做出的 ARP 应答消息。

找到：

108 6.344929	BelkinIntern_75:b1:…	Broadcast	ARP
109 6.347010	3ComEurope_7e:d9:01	BelkinIntern_75:b1:…	ARP

19. 你计算机收到的 ARP 应答消息中的操作码字段的值是什么？

```
Opcode: reply (2)
```

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

```
Sender MAC address: 3ComEurope_7e:d9:01 (00:1e:c1:7e:d9:01)
```

我们查看了由你计算机运行 Wireshark 发送的 ARP 请求消息，以及发送的 ARP 应答。但是在这个网络中，还有其他设备也在发送 ARP 请求，你可以在追踪中找到。

21. 我们查看了由你计算机运行 Wireshark 发送的 ARP 请求消息，以及作为回应发送的 ARP 应答消息。但在你的追踪中，为什么没有对这些其他 ARP 请求消息的 ARP 应答？

这是因为请求消息是广播的，但回复消息仅发送给发出请求的主机。

EX-1. The arp command: arp-s InetAddr EtherAddr allows you to manually add an entry to the ARP cache that resolves the IP address InetAddr to the physical address EtherAddr. What would happen if, when you manually added an entry, you entered the correct IP address, but the wrong Ethernet address for that remote interface? A security attack known as “ARP poisoning” https://www.varonis.com/blog/arp-poisoning/ spoofs ARP messages and causes incorrect entries to be made into an ARP table!

数据帧会被发送到错误的 MAC 地址：

如果该 MAC 地址不存在或不属于预期设备：数据包无法到达目的地，导致网络通信失败（如 ping 超时、TCP 连接失败）。

如果该 MAC 地址属于另一台设备：数据会被错误地发送到那台设备，可能被丢弃或引发安全问题。

此外，错误的静态条目会导致本地计算机持续向错误的设备发送数据，直到条目被修正。

EX-2. What is the default amount of time that an entry remains in your ARP cache before being removed? You can determine this empirically (by monitoring the cache contents) or by looking this up in your operating system documentation. Indicate how/where you determined this value。

在 Windows 中并没有找到具体的 ARP 缓存更新的时间，但是在 linux 上：

ARP 表项的老化超时时间：缺省值是 1200 秒；

MAC 表的老化超时时间：缺省值是 300 秒 ；

修改命令

arp expire-time 命令用来设置动态 ARP 表项的老化超时时间。

mac-address aging-time 命令用来设置动态 MAC 地址表项的老化时间

arp detect-times 命令修改 arp 探测次数。默认探测次数是 3 次

题目分析见上

结论分析与体会：

本实验通过 Wireshark 抓包分析以太网帧和 ARP 协议的工作机制，验证了 ARP 协议如何通过广播请求和单播响应实现 IP 地址到 MAC 地址的动态解析，并观察到 ARP 缓存条目具有时效性。当网络拓扑变化时（如更换网卡），ARP 协议通过定期更新的机制保证了地址映射的准确性，但这也可能被 ARP 欺骗攻击利用，实验中通过伪造 ARP 响应包可验证中间人攻击的可行性。这些现象印证了教材中关于链路层寻址和 ARP 缓存动态维护的理论描述。