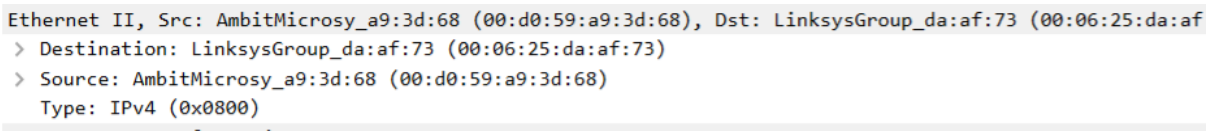
计算机学院 计算机网络 课程实验报告

实验题目： 以太网和 ARP		学号：202200130048
日期：5.14	班级： 6	姓名： 陈静雯
Email：1205037094@qq.com		

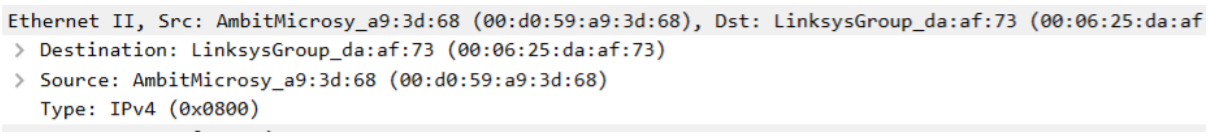
实验方法介绍：
通过 wireshark 捕获和分析以太网帧以及 ARP 协议的作用

实验过程描述：
1. 捕获和分析以太网帧
2. 地址解析协议
   ARP 缓存和作用

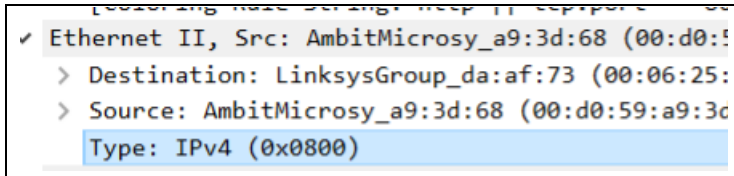
结论分析：
1. What is the 48-bit Ethernet address of your computer?
00:d0:59:a9:3d:68



2. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? (Hint: the answer is no). What device has this as its Ethernet address?
Dst：00:06:25:da:af:73
在以太网帧中的 48 位目标地址通常是接收设备在网络上的 MAC（媒体访问控制）地址。这个地址对每个网络设备来说都是唯一的，包括路由器、交换机和单个计算机。
“gaia.cs.umass.edu”它通常解析为一个 IP 地址，这是属于互联网层的地址，而不是以太网层的。以太网地址与 IP 地址不同，它用在数据链路层，用于直接在物理网络中定位设备。因此，"gaia.cs.umass.edu"的 Ethernet 地址不是 48 位目标地址所指的。这个 48 位地址实际上属于网络上的某个具体设备，比如某台服务器、电脑或网络接口卡等。



3. What is the hexadecimal value for the two-byte Frame type field in the Ethernet frame carrying the HTTP GET request? What upper layer protocol does this correspond to?
Type：0x0800。这个值对应于上层的 IPv4 协议。



4. How many bytes from the very start of the Ethernet frame does the ASCII "G" in "GET" appear in the Ethernet frame?

6+6+2+20+20=54 之后

在以太网帧中，"GET"中的 ASCII 字符"G"从帧的起始处开始计算，不包括前导码（preamble）和起始定界符，其位置如下：

目的 MAC 地址：6 字节

源 MAC 地址：6 字节

EtherType / Frame Type：2 字节

IP 报头：约为 20 字节

TCP 报头：最少 20 字节。

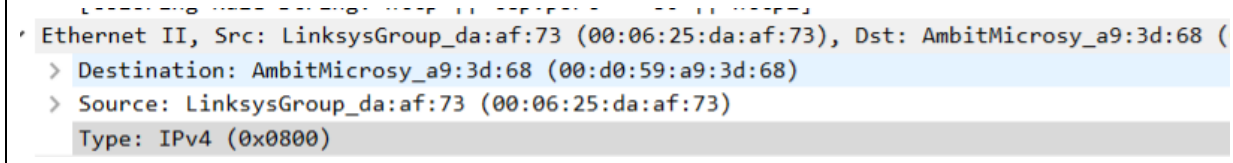
HTTP 报文：HTTP GET 请求的实际内容从这里开始。

假设 HTTP GET 请求非常简单，且没有额外的 TCP 或 IP 选项，那么"G"字符将会出现在：目的 MAC（6 字节）+ 源 MAC（6 字节）+ EtherType（2 字节）+ IP Header（20 字节）+ TCP Header（最小 20 字节）= 54 字节之后。

5. What is the value of the Ethernet source address? Is this the address of your computer, or of gaia.cs.umass.edu (Hint: the answer is no). What device has this as its Ethernet address?

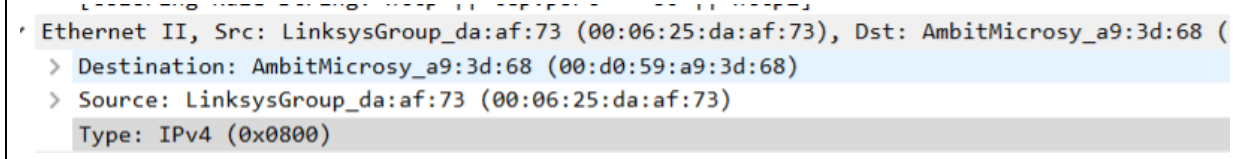
00:06:25:da:af:73，

两者都不是，是 gaia.cs.umass.edu 所在设备的 MAC 地址



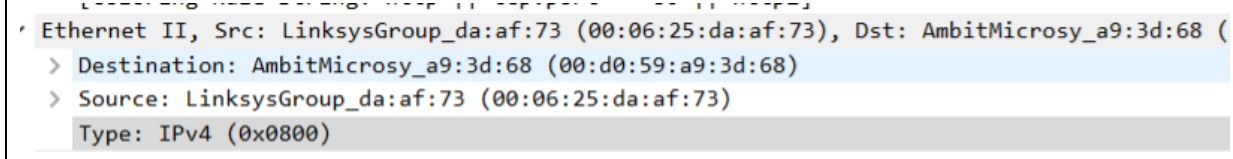
6. What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?

00:d0:59:a9:3d:68，不是，是计算机网卡的 MAC 地址



7. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

0x0800，IPv4



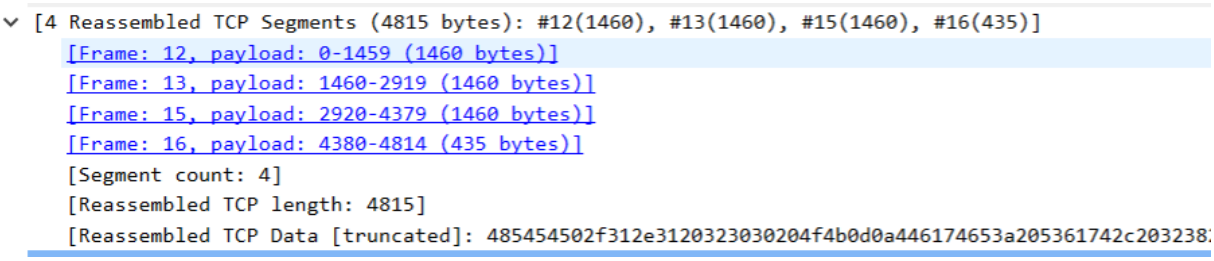
8. How many bytes from the very start of the Ethernet frame does the ASCII "O" in "OK" appear in the Ethernet frame?

8 + 12 + 2 + 20 + 20 = 62 字节，具体如下：

SFD：7 字节的前导码和 1 字节的帧开始定界符，共 8 字节。
目标 MAC 地址：6 字节。
源 MAC 地址：6 字节。
EtherType：2 字节
Payload：之后是上层协议的数据，对于 HTTP 响应，这将包括：
Ethernet -> IPv4 Header：约 20 字节（最少）。
IPv4 -> TCP Header：约 20 字节（最少）。
TCP -> HTTP Data：包含 HTTP 响应码"OK"的实际数据。
HTTP 响应码"OK"（即"HTTP/1.1 200 OK"）通常出现在 HTTP 响应的起始行，紧跟在 TCP 和 IP 头之后。

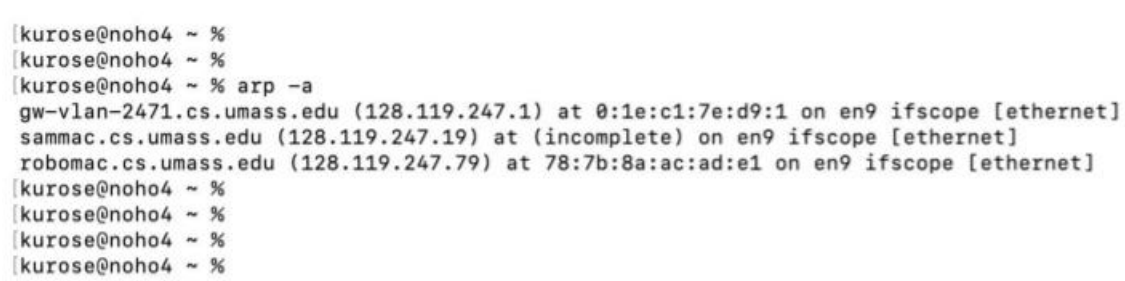
9. How many Ethernet frames carry data that is part of the complete HTTP "OK 200 ..." reply message?

4



10. How many entries are stored in your ARP cache?

3

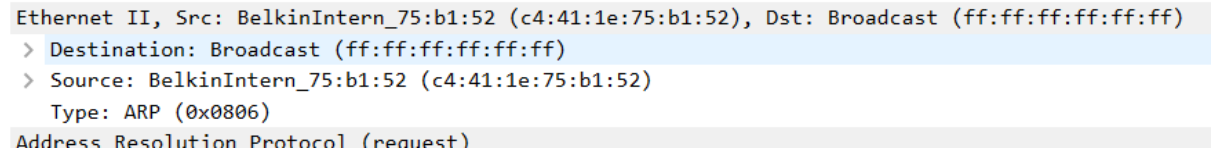


11. What is contained in each displayed entry of the ARP cache?

Internet 地址、物理地址（MAC 地址）、网络接口名（en9）、作用域（ifscope，强调这个条目是针对一个具有特定作用域的接口）

12. What is the hexadecimal value of the source address in the Ethernet frame containing the ARP request message sent out by your computer?

c4:41:1e:75:b1:52



13. What is the hexadecimal value of the destination addresses in the Ethernet frame containing the ARP request message sent out by your computer? And what device(if any) corresponds to that address

ff:ff:ff:ff:ff:ff，广播地址 broadcast

```
Ethernet II, Src: BelkinIntern_75:b1:52 (c4:41:1e:75:b1:52), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: BelkinIntern_75:b1:52 (c4:41:1e:75:b1:52)
    Type: ARP (0x0806)
Address Resolution Protocol (request)
```

14. What is the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?

0x0806，ARP

```
Ethernet II, Src: BelkinIntern_75:b1:52 (c4:41:1e:75:b1:52), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: BelkinIntern_75:b1:52 (c4:41:1e:75:b1:52)
    Type: ARP (0x0806)
Address Resolution Protocol (request)
```

15. How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

6+6+2=14 ，ARP 的操作码字段开始于以太网帧的 14 字节后

以太网帧头（Header）包含目的 MAC 地址（6 字节）、源 MAC 地址（6 字节）、类型/长度字段（2 字节）。

16. What is the value of the opcode field within the ARP request message sent by your computer?

op=1

```
    Protocol size: 4
    Opcode: request (1)
    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
```

17. Does the ARP request message contain the IP address of the sender? If the answer is yes, what is that value?

128.119.247.66

```
    Protocol size: 4
    Opcode: request (1)
    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
```

18. What is the IP address of the device whose corresponding Ethernet address is being requested in the ARP request message sent by your computer?

128.119.247.1

```
    Protocol size: 4
    Opcode: request (1)
    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
```

19. What is the value of the opcode field within the ARP reply message received by your computer?

op=2

```
Protocol size: 4
Opcode: reply (2)
Sender MAC address: 3ComEurope_7e:d9:01 (0
```

20. Finally (!), let's look at the answer to the ARP request message! What is the Ethernetaddress corresponding to the IP address that was specified in the ARP requestmessage sent by your computer (see question 18)?

00:1e:c1:7e:d9:01

```
Opcode: reply (2)
Sender MAC address: 3ComEurope_7e:d9:01 (00:1e:c1:7e:d9:01)
Sender IP address: 128.119.247.1
Target MAC address: BelkinIntern_75:b1:52 (c4:41:1e:75:b1:52)
Target IP address: 128.119.247.66
```

21. Why are there no ARP replies in your trace that are sent in response to these other ARP request messages?

(1)方向性问题：Wireshark 只能捕获到通过其所在网络接口的流量。如果 ARP 请求和应答发生在不同的子网或交换机的另一个 VLAN 中，而这些通信没有经过您正在监听的接口，那么您就无法看到那些应答。

(2)过滤设置：如果您设置了过于严格的过滤条件，可能会意外地排除了某些 ARP 应答包。请检查您的捕获或显示过滤器，确保没有无意中过滤掉了应答消息。

(3)时间窗口：ARP 请求与应答之间的间隔很短，但如果捕获窗口没有足够长，或者捕获开始得不够及时，您可能会错过看到 ARP 应答。

(4)ARP 缓存：目标设备可能已经从之前的交互中在 ARP 缓存中存储了请求设备的 MAC 地址，因此不需要再次发送 ARP 应答。这尤其可能发生在短时间内重复的 ARP 请求上。

(5)网络问题：网络中的问题，如丢包、网络拥塞或设备配置错误，也可能导致 ARP 应答没有到达正在监听的计算机。

(6)应答发送给了其他设备：ARP 应答默认是单播发送给发起请求的设备的，如果请求不是由您监控的设备发出的，那么应答也不会经过您的监控点。

结论：

1. ARP 协议数据单元（PDU）是嵌入在以太网帧中的，以太网帧头（Header）包含目的 MAC 地址（6 字节）、源 MAC 地址（6 字节）、类型/长度字段（2 字节）。ARP 协议数据紧跟在以太网帧头之后。
2. 以太网帧类型字段的 2 字节值可以有不同的十六进制数值，每个数值对应一种上层协议：
   IP 协议对应的 Type 值为 0x0800。
   ARP 协议对应的 Type 值为 0x0806。
3. 在以太网帧中，"GET"中的 ASCII 字符"G"从帧的起始处开始计算，不包括前导码（preamble）和起始定界符，其位置如下：
   目的 MAC 地址：6 字节
   源 MAC 地址：6 字节
   EtherType / Frame Type：2 字节
   IP 报头：约为 20 字节
   TCP 报头：最少 20 字节。
   HTTP 报文：HTTP GET 请求的实际内容从这里开始。