

**TRƯỜNG ĐẠI HỌC BÁCH KHOA
ĐẠI HỌC QUỐC GIA TP HỒ CHÍ MINH**



**HOMEWORK
MẠNG MÁY TÍNH (THỰC HÀNH) – LAB 6**

Giảng viên hướng dẫn: Ths. Bùi Xuân Giang

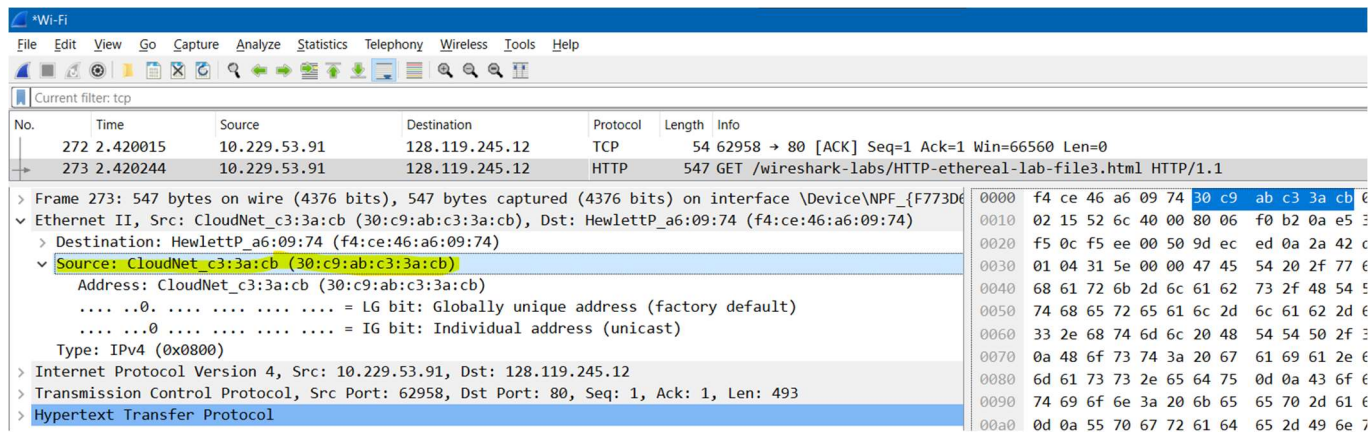
Sinh viên thực hiện: Trần Minh Tân

Mã số sinh viên: 2012018

Lớp: L10

Thành phố Hồ Chí Minh – 2022

Part 1: Capturing and analyzing Ethernet frames



Wireshark packet capture showing an HTTP GET request. The packet list shows packet 273 selected. The packet details pane shows the Ethernet II frame structure with source and destination MAC addresses. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
272	2.420015	10.229.53.91	128.119.245.12	TCP	54	62958 → 80 [ACK] Seq=1 Ack=1 Win=66560 Len=0
273	2.420244	10.229.53.91	128.119.245.12	HTTP	547	GET /wireshark-labs/HTTP-ethereal-lab-file3.html HTTP/1.1

Frame 273: 547 bytes on wire (4376 bits), 547 bytes captured (4376 bits) on interface \Device\NPF_{F773D6...}

Ethernet II, Src: CloudNet_c3:3a:cb (30:c9:ab:c3:3a:cb), Dst: HewlettP_a6:09:74 (f4:ce:46:a6:09:74)

Destination: HewlettP_a6:09:74 (f4:ce:46:a6:09:74)

Source: CloudNet_c3:3a:cb (30:c9:ab:c3:3a:cb)

Address: CloudNet_c3:3a:cb (30:c9:ab:c3:3a:cb)

.... 0. = LG bit: Globally unique address (factory default)

.... 0. = IG bit: Individual address (unicast)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 10.229.53.91, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 62958, Dst Port: 80, Seq: 1, Ack: 1, Len: 493

Hypertext Transfer Protocol

1. What is the 48-bit Ethernet address of your computer?

The Ethernet address of my computer is 30:c9:ab:c3:3a:cb

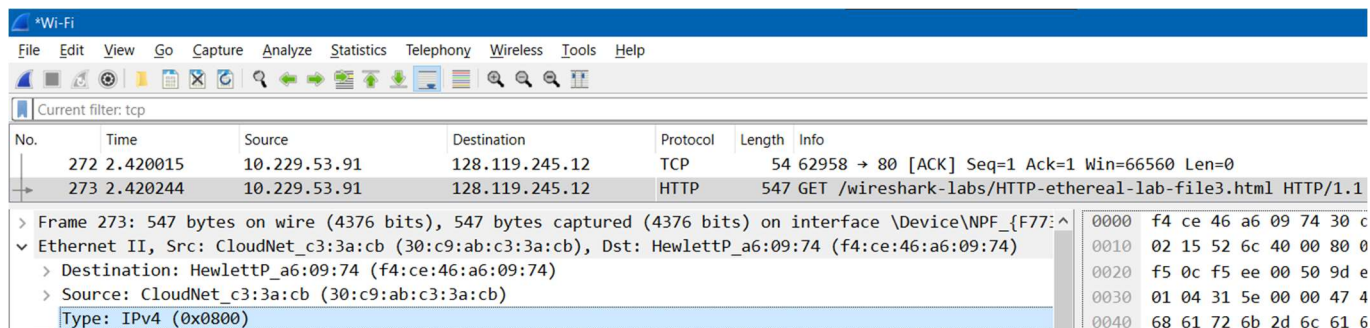
2. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? (Hint: the answer is no). What device has this as its Ethernet address? [Note: this is an important question, and one that students sometimes get wrong. Re-read pages 468-469 in the text and make sure you understand the answer here.]

The 48-bit destination address in the Ethernet frame is f4:ce:46:a6:09:74

The device has this as its Ethernet address is my router (Hewlett Package)

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

The upper layer protocol this correspond to is IP protocol (0x0800).



Wireshark packet capture showing an HTTP GET request. The packet list shows packet 273 selected. The packet details pane shows the Ethernet II frame structure with source and destination MAC addresses. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
272	2.420015	10.229.53.91	128.119.245.12	TCP	54	62958 → 80 [ACK] Seq=1 Ack=1 Win=66560 Len=0
273	2.420244	10.229.53.91	128.119.245.12	HTTP	547	GET /wireshark-labs/HTTP-ethereal-lab-file3.html HTTP/1.1

Frame 273: 547 bytes on wire (4376 bits), 547 bytes captured (4376 bits) on interface \Device\NPF_{F773D6...}

Ethernet II, Src: CloudNet_c3:3a:cb (30:c9:ab:c3:3a:cb), Dst: HewlettP_a6:09:74 (f4:ce:46:a6:09:74)

Destination: HewlettP_a6:09:74 (f4:ce:46:a6:09:74)

Source: CloudNet_c3:3a:cb (30:c9:ab:c3:3a:cb)

Type: IPv4 (0x0800)

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

The length from the very start of the Ethernet frame to the ASCII “G” in “GET” appear is 52 bytes

No.	Time	Source	Destination	Protocol	Length	Info
272	2.420015	10.229.53.91	128.119.245.12	TCP	54	62958 → 80 [ACK] Seq=1 Ack=1 Win=66560 Len=0
273	2.420244	10.229.53.91	128.119.245.12	HTTP	547	GET /wireshark-labs/HTTP-ethereal-lab-file3.html HTTP/1.1

Frame 273: 547 bytes on wire (4376 bits), 547 bytes captured (4376 bits) on interface \Device\NPF_{F773D6...}

Ethernet II, Src: CloudNet_c3:3a:cb (30:c9:ab:c3:3a:cb), Dst: HewlettP_a6:09:74 (f4:ce:46:a6:09:74)

Internet Protocol Version 4, Src: 10.229.53.91, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 62958, Dst Port: 80, Seq: 1, Ack: 1, Len: 493

Hypertext Transfer Protocol

GET /wireshark-labs/HTTP-ethereal-lab-file3.html HTTP/1.1\r\n

[Expert Info (Chat/Sequence): GET /wireshark-labs/HTTP-ethereal-lab-file3.html HTTP/1.1\r\n]

Next, answer the following questions, based on the contents of the Ethernet frame containing the first byte of the HTTP response message.

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?

The value of the Ethernet source address is f4:ce:46:a6:09:74. This is the address of my router

No.	Time	Source	Destination	Protocol	Length	Info
338	2.741002	128.119.245.12	10.229.53.91	HTTP	559	HTTP/1.1 200 OK (text/html)

Frame 338: 559 bytes on wire (4472 bits), 559 bytes captured (4472 bits) on interface \Device\NPF_{F773D6...}

Ethernet II, Src: HewlettP_a6:09:74 (f4:ce:46:a6:09:74), Dst: CloudNet_c3:3a:cb (30:c9:ab:c3:3a:cb)

Destination: CloudNet_c3:3a:cb (30:c9:ab:c3:3a:cb)

Source: HewlettP_a6:09:74 (f4:ce:46:a6:09:74)

Type: IPv4 (0x0800)

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

According to the picture above, the destination address in the Ethernet frame is 30:c9:ab:c3:3a:cb. This is the Ethernet address of my computer.

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

No.	Time	Source	Destination	Protocol	Length	Info
338	2.741002	128.119.245.12	10.229.53.91	HTTP	559	HTTP/1.1 200 OK (text/html)

Frame 338: 559 bytes on wire (4472 bits), 559 bytes captured (4472 bits) on interface \Device\NPF_{F773D6...}

Ethernet II, Src: HewlettP_a6:09:74 (f4:ce:46:a6:09:74), Dst: CloudNet_c3:3a:cb (30:c9:ab:c3:3a:cb)

Destination: CloudNet_c3:3a:cb (30:c9:ab:c3:3a:cb)

Source: HewlettP_a6:09:74 (f4:ce:46:a6:09:74)

Type: IPv4 (0x0800)

The upper layer protocol this correspond to is IP address.

8. How many bytes from the very start of the Ethernet frame does the ASCII “O” in “OK” (i.e., the HTTP response code) appear in the Ethernet frame?

The length from the very start of the Ethernet frame to the ASCII “O” in “OK” appear is 52 bytes

678	29.332343	128.119.245.12	10.229.53.91	HTTP	559 HTTP/1.1 200 OK (text/html)
>	Frame 678:	559 bytes on wire (4472 bits), 559 bytes captured (4472 bits) on interface	0030	00 ed 55 66 00 00 20 63 72 75 65 6c 20 61 6e 64	..Uf.. c ruel and
>	Ethernet II, Src:	HewlettP_a6:09:74 (f4:ce:46:a6:09:74), Dst:	0040	20 75 6e 75 73 75 61 6c 20 70 75 6e 69 73 68 6d	unusual punishm
>	Internet Protocol Version 4, Src:	128.119.245.12, Dst:	0050	65 6e 74 73 20 69 6e 66 6c 69 63 74 65 64 2e 0a	ents inf licted..
>	Transmission Control Protocol, Src Port:	80, Dst Port:	0060	0a 3c 2f 70 3e 3c 70 3e 3c 61 20 6e 61 6d 65 3d	</p><p> <a name=
>	[4 Reassembled TCP Segments (4861 bytes):	#530(1452), #675(1452), #676(1452), #	0070	22 39 22 3e 3c 73 74 72 6f 6e 67 3e 3c 68 33 3e	"9"><str ong><h3>

PART 2 The Address Resolution Protocol

9. Write down the contents of your computer’s ARP cache. What is the meaning of each column value

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

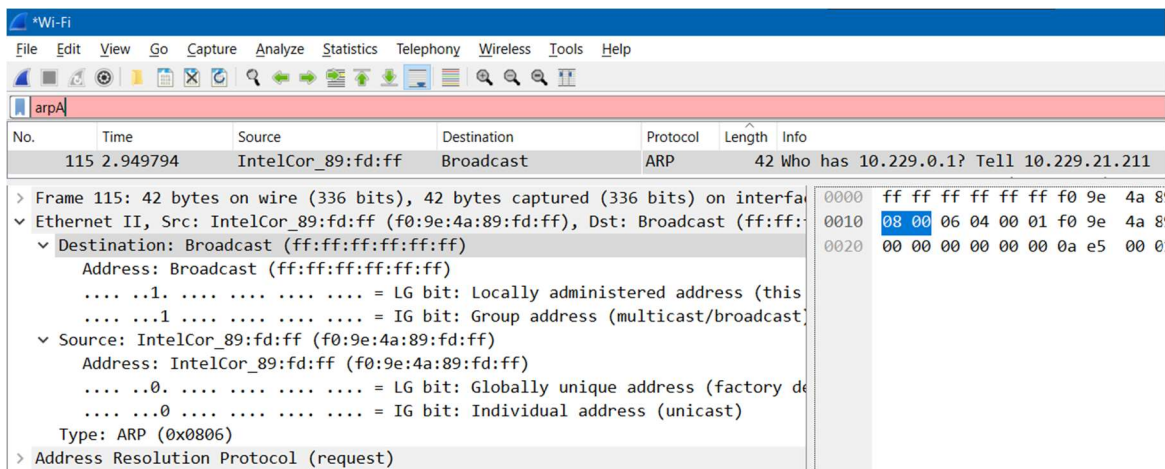
Interface: 169.254.107.79 --- 0xc
  Internet Address      Physical Address      Type
  169.254.255.255       ff-ff-ff-ff-ff-ff    static
  224.0.0.22            01-00-5e-00-00-16    static
  224.0.0.251           01-00-5e-00-00-fb    static
  224.0.0.252           01-00-5e-00-00-fc    static
  239.192.152.143       01-00-5e-40-98-8f    static
  239.255.255.250       01-00-5e-7f-ff-fa    static

Interface: 10.230.160.91 --- 0x12
  Internet Address      Physical Address      Type
  10.230.0.1            f4-ce-46-a6-09-74    dynamic
  10.230.255.255        ff-ff-ff-ff-ff-ff    static
  224.0.0.22            01-00-5e-00-00-16    static
  224.0.0.251           01-00-5e-00-00-fb    static
  224.0.0.252           01-00-5e-00-00-fc    static
  239.255.255.250       01-00-5e-7f-ff-fa    static
  255.255.255.255       ff-ff-ff-ff-ff-ff    static

C:\Users\Admin>
```

- Internet Address: IP address.
- Physical Address: MAC address.
- Type: the state of IP address (dynamic or static).

10. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?



Destination address: ff:ff:ff:ff:ff:ff

Source address: f0:9e:3a:89:fd:ff

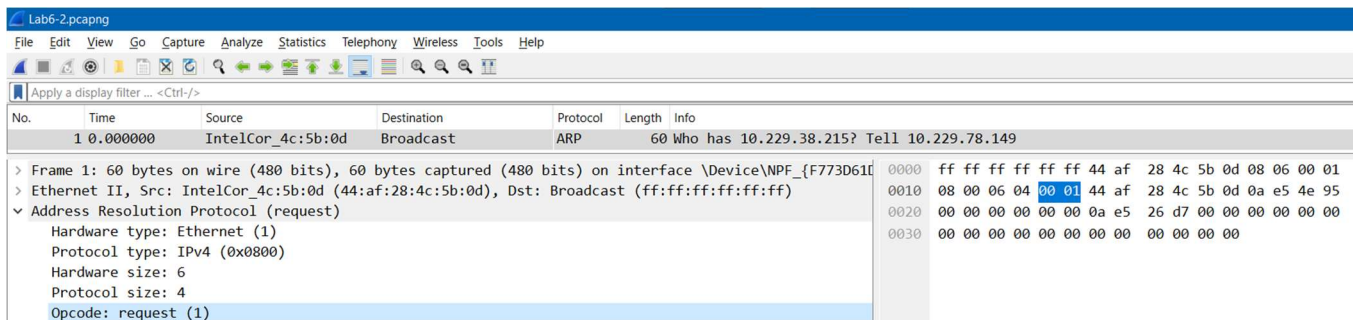
11. Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?

The hexadecimal value for the two-byte Ethernet Frame is 0x0806. The upper layer protocol this correspond to is ARP.

12. Download the ARP specification from <ftp://ftp.rfc-editor.org/in-notes/std/std37.txt>. A readable, detailed discussion of ARP is also at <http://www.erg.abdn.ac.uk/users/gorry/course/inetpages/arp.html>.

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

It begins 20 bytes from the very beginning of the Ethernet frame, as we can see in the screenshot below.



b) What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP request is made?

The hex value for opcode field withing the ARP-payload of the request is 0x0001 as we can see in the screenshot below

Lab6-2.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	IntelCor_4c:5b:0d	Broadcast	ARP	60	Who has 10.229.38.215? Tell 10.229.78.149

> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{F773D61F-0000-ff ff ff ff ff ff 44 af

> Ethernet II, Src: IntelCor_4c:5b:0d (44:af:28:4c:5b:0d), Dst: Broadcast (ff:ff:ff:ff:ff:ff) 0010 08 00 06 04 00 01 44 af

> Address Resolution Protocol (request) 0020 00 00 00 00 00 00 0a e5

Hardware type: Ethernet (1) 0030 00 00 00 00 00 00 00 00

Protocol type: IPv4 (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: request (1)

c) Does the ARP message contain the IP address of the sender?

Yes, the ARP message containing the IP address 10.229.78.149 for the sender

d) Where in the ARP request does the “question” appear – the Ethernet address of the machine whose corresponding IP address is being queried?

The field “Target MAC address” is set to 00:00:00:00:00:00 to question the machine whose corresponding IP address (192.168.1.1) is being queried

Lab6-2.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	IntelCor_4c:5b:0d	Broadcast	ARP	60	Who has 10.229.38.215? Tell 10.229.78.149

> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{F773D61F-0000-ff ff ff ff ff ff 44 af

> Ethernet II, Src: IntelCor_4c:5b:0d (44:af:28:4c:5b:0d), Dst: Broadcast (ff:ff:ff:ff:ff:ff) 0010 08 00 06 04 00 01 44 af

> Address Resolution Protocol (request) 0020 00 00 00 00 00 00 0a e5

Hardware type: Ethernet (1) 0030 00 00 00 00 00 00 00 00

Protocol type: IPv4 (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: request (1)

Sender MAC address: IntelCor_4c:5b:0d (44:af:28:4c:5b:0d)

Sender IP address: 10.229.78.149

Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)

Target IP address: 10.229.38.215

13. Now find the ARP reply that was sent in response to the ARP request.

Lab6-2.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp

No.	Time	Source	Destination	Protocol	Length	Info
412	7.972745	aa:16:c1:ab:13:58	Broadcast	ARP	60	Who has 169.254.169.254? Tell 10.229.98.45
413	7.974330	a6:97:5f:64:01:df	CloudNet_c3:3a:cb	ARP	60	Who has 10.229.53.91? Tell 10.229.10.210
414	7.974342	CloudNet_c3:3a:cb	a6:97:5f:64:01:df	ARP	42	10.229.53.91 is at 30:c9:ab:c3:3a:cb

> Frame 414: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{F773D61F-0000-a6 97 5f 64 01 df 30 c9 ab c3 3a

> Ethernet II, Src: CloudNet_c3:3a:cb (30:c9:ab:c3:3a:cb), Dst: a6:97:5f:64:01:df (a6:97:5f:64:01:df) 0010 08 00 06 04 00 02 30 c9 ab c3 3a

> Address Resolution Protocol (reply) 0020 a6 97 5f 64 01 df 0a e5 0a d2

Hardware type: Ethernet (1)

Protocol type: IPv4 (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: reply (2)

Sender MAC address: CloudNet_c3:3a:cb (30:c9:ab:c3:3a:cb)

Sender IP address: 10.229.53.91

Target MAC address: a6:97:5f:64:01:df (a6:97:5f:64:01:df)

Target IP address: 10.229.10.210

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

There are 20 bytes from the very beginning of the Ethernet frame to the ARP opcode field.

414	7.974342	CloudNet_c3:3a:cb	a6:97:5f:64:01:df	ARP	42	10.229.53.91 is at 30:c9:ab:c3:3a:cb
> Frame 414: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{F773D6...}						
> Ethernet II, Src: CloudNet_c3:3a:cb (30:c9:ab:c3:3a:cb), Dst: a6:97:5f:64:01:df (a6:97:5f:64:01:df)						
▼ Address Resolution Protocol (reply)						
Hardware type: Ethernet (1)						
Protocol type: IPv4 (0x0800)						
Hardware size: 6						
Protocol size: 4						
Opcode: reply (2)						

b) What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP response is made?

The value of opcode fields within the ARP-payload part of the Ethernet frame in which an ARP is made is 0x002

414	7.974342	CloudNet_c3:3a:cb	a6:97:5f:64:01:df	ARP	42	10.229.53.91 is at 30:c9:ab:c3:3a:cb
> Frame 414: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{F773D6...}						
> Ethernet II, Src: CloudNet_c3:3a:cb (30:c9:ab:c3:3a:cb), Dst: a6:97:5f:64:01:df (a6:97:5f:64:01:df)						
▼ Address Resolution Protocol (reply)						
Hardware type: Ethernet (1)						
Protocol type: IPv4 (0x0800)						
Hardware size: 6						
Protocol size: 4						
Opcode: reply (2)						

c) Where in the ARP message does the “answer” to the earlier ARP request appear – the IP address of the machine having the Ethernet address whose corresponding IP address is being queried?

Lab6-2.pcapng						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
arp						
No.	Time	Source	Destination	Protocol	Length	Info
412	7.972745	aa:16:c1:ab:13:58	Broadcast	ARP	60	Who has 169.254.169.254? Tell 10.229.98.45
413	7.974330	a6:97:5f:64:01:df	CloudNet_c3:3a:cb	ARP	60	Who has 10.229.53.91? Tell 10.229.10.210
414	7.974342	CloudNet_c3:3a:cb	a6:97:5f:64:01:df	ARP	42	10.229.53.91 is at 30:c9:ab:c3:3a:cb

The answer in ARP reply message to the earlier ARP request appear in the “Info” fields – 10.229.53.91 is at 30:c9:ab:c3:3a:cb.

14. What are the hexadecimal values for the source and destination addresses in the

Ethernet frame containing the ARP reply message?

- Source address: 30:c9:ab:c3:3a:cb
- Destination address: a6:97:5f:64:01:df

414 7.974342	CloudNet_c3:3a:cb	a6:97:5f:64:01:df	ARP	42 10.229.53.91 is at 30:c9:ab:c3:3a:cb	
> Frame 414: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{F773D...}					0000
> Ethernet II, Src: CloudNet_c3:3a:cb (30:c9:ab:c3:3a:cb), Dst: a6:97:5f:64:01:df (a6:97:5f:64:01:df)					0010 08 00 06 04 00 02 30 c9 ab c3 3a cb 0a e5 35 5b
> Address Resolution Protocol (reply)					0020 a6 97 5f 64 01 df 0a e5 0a d2
Hardware type: Ethernet (1)					
Protocol type: IPv4 (0x0800)					
Hardware size: 6					
Protocol size: 4					
Opcode: reply (2)					
Sender MAC address: CloudNet_c3:3a:cb (30:c9:ab:c3:3a:cb)					
Sender IP address: 10.229.53.91					
Target MAC address: a6:97:5f:64:01:df (a6:97:5f:64:01:df)					
Target IP address: 10.229.10.210					

15. Open the ethernet-ethereal-trace-1 trace file in <http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip>. The first and second ARP packets in this trace correspond to an ARP request sent by the computer running Wireshark, and the ARP reply sent to the computer running Wireshark by the computer with the ARP-requested Ethernet address. But there is yet another computer on this network, as indicated by packet 6 – another ARP request. Why is there no ARP reply (sent in response to the ARP request in packet 6) in the packet trace?

There is no reply in this trace because we are not in the machine that sent the request.

arp							
No.	Time	Source	Destination	Protocol	Length	Info	
1	0.000000	AmbitMic_a9:3d:68	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.105	
2	0.001018	Linksys_ga:af:73	AmbitMic_a9:3d:68	ARP	60	192.168.1.1 is at 00:06:25:da:af:73	
6	13.542974	CnetTech_73:8d:ce	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104	

> Frame 6: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)		0000	ff ff ff ff ff ff 00 80 ad 73 8d ce 08 06 00 01
> Ethernet II, Src: CnetTech_73:8d:ce (00:80:ad:73:8d:ce), Dst: Broadcast (ff:ff:ff:ff:ff:ff)		0010	08 00 06 04 00 01 00 80 ad 73 8d ce c0 a8 01 68
▼ Address Resolution Protocol (request)		0020	00 00 00 00 00 00 c0 a8 01 75 00 00 00 00 00 00
Hardware type: Ethernet (1)		0030	00 00 00 00 00 00 00 00 00 00 00 00
Protocol type: IPv4 (0x0800)			
Hardware size: 6			
Protocol size: 4			
Opcode: request (1)			
Sender MAC address: CnetTech_73:8d:ce (00:80:ad:73:8d:ce)			
Sender IP address: 192.168.1.104			
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)			
Target IP address: 192.168.1.117			