

Lachlan Sinclair

Lab 5: CS 372

12/7/2019

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

00:d0:59:a9:3d:68 is the 48 bit address of “my” computer.

The image shows a Wireshark packet capture of network traffic. The top pane displays a list of packets. Packet 10 is selected, showing details of an Ethernet II frame, an Internet Protocol Version 4 packet, and a Hypertext Transfer Protocol (HTTP) GET request.

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	LinksysG_da:af:73	AmbitMic_a9:3d:68	ARP	60	192.168.1.1 is at 00:06:25:da:af:73
3	0.001028	192.168.1.105	199.2.53.206	TCP	62	1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
4	2.962850	192.168.1.105	199.2.53.206	TCP	62	[TCP Retransmission] 1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
5	8.971488	192.168.1.105	199.2.53.206	TCP	62	[TCP Retransmission] 1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
6	13.542974	CnetTech_73:8d:ce	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
7	17.444423	192.168.1.105	128.119.245.12	TCP	62	1058 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
8	17.465902	128.119.245.12	192.168.1.105	TCP	62	80 → 1058 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
9	17.465927	192.168.1.105	128.119.245.12	TCP	54	1058 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10	17.466468	192.168.1.105	128.119.245.12	HTTP	686	GET /ethereal-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
11	17.494766	128.119.245.12	192.168.1.105	TCP	60	80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=0

Packet 10 details:

- Frame 10: 686 bytes on wire (5488 bits), 686 bytes captured (5488 bits)
- Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
 - Destination: LinksysG_da:af:73 (00:06:25:da:af:73)
 - Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
 - Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 192.168.1.105, Dst: 128.119.245.12
- Transmission Control Protocol, Src Port: 1058, Dst Port: 80, Seq: 1, Ack: 1, Len: 632
- Hypertext Transfer Protocol
 - GET /ethereal-labs/HTTP-ethereal-lab-file3.html HTTP/1.1\r\n
 - Host: gaia.cs.umass.edu\r\n
 - User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.2) Gecko/20030208 Netscape/7.02\r\n
 - Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-mng,image/png,image/jpeg,image/gif;q=0.2,text/css,*/*;q=0.1\r\n
 - Accept-Language: en-us, en;q=0.50\r\n
 - Accept-Encoding: gzip, deflate, compress;q=0.9\r\n
 - Accept-Charset: ISO-8859-1, utf-8;q=0.66, */q=0.66\r\n
 - Keep-Alive: 300\r\n
 - Connection: keep-alive\r\n
 - If-Modified-Since: Sat, 28 Aug 2004 17:00:40 GMT\r\n
 - If-None-Match: "1b8c3-1194-c578fe00"\r\n
 - Cache-Control: max-age=0\r\n
 - \r\n
 - [Full request URI: http://gaia.cs.umass.edu/ethereal-labs/HTTP-ethereal-lab-file3.html]
 - [HTTP request 1/1]
 - [Response in frame: 16]

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 is 00:06:25:da:af:73

This is the address of the router in the subnet that is being used by “my” computer to leave said subnet.

ethernet-ethereal-trace-1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

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	LinksysG_da:af:73	AmbitMic_a9:3d:68	ARP	60	192.168.1.1 is at 00:06:25:da:af:73
3	0.001028	192.168.1.105	199.2.53.206	TCP	62	1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
4	2.962850	192.168.1.105	199.2.53.206	TCP	62	[TCP Retransmission] 1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
5	8.971488	192.168.1.105	199.2.53.206	TCP	62	[TCP Retransmission] 1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
6	13.542974	CnetTech_73:8d:ce	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
7	17.444423	192.168.1.105	128.119.245.12	TCP	62	1058 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
8	17.465902	128.119.245.12	192.168.1.105	TCP	62	80 → 1058 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
9	17.465927	192.168.1.105	128.119.245.12	TCP	54	1058 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10	17.466468	192.168.1.105	128.119.245.12	HTTP	686	GET /ethereal-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
11	17.494766	128.119.245.12	192.168.1.105	TCP	60	80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=0

> Frame 10: 686 bytes on wire (5488 bits), 686 bytes captured (5488 bits)

▼ Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)

> Destination: LinksysG_da:af:73 (00:06:25:da:af:73)

> Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)

Type: IPv4 (0x0800)

> Internet Protocol Version 4, Src: 192.168.1.105, Dst: 128.119.245.12

> Transmission Control Protocol, Src Port: 1058, Dst Port: 80, Seq: 1, Ack: 1, Len: 632

▼ Hypertext Transfer Protocol

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

Host: gaia.cs.umass.edu\r\n

User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.2) Gecko/20030208 Netscape/7.02\r\n

Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-mng,image/png,image/jpeg,image/gif;q=0.2,text/css,*/*;q=0.1\r\n

Accept-Language: en-us,en;q=0.50\r\n

Accept-Encoding: gzip, deflate, compress;q=0.9\r\n

Accept-Charset: ISO-8859-1, utf-8;q=0.66,*/*;q=0.66\r\n

Keep-Alive: 300\r\n

Connection: keep-alive\r\n

If-Modified-Since: Sat, 28 Aug 2004 17:00:40 GMT\r\n

If-None-Match: "1b8c3-1194-c578fe00"\r\n

Cache-Control: max-age=0\r\n

\r\n

[Full request URI: <http://gaia.cs.umass.edu/ethereal-labs/HTTP-ethereal-lab-file3.html>]

[HTTP request 1/1]

[Response in frame: 16]

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

The hexadecimal for the two-byte frame type is 0x0800. This refers to the IPv4 protocol.

ethernet-ethereal-trace-1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F> Expression...

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	LinksysG_da:af:73	AmbitMic_a9:3d:68	ARP	60	192.168.1.1 is at 00:06:25:da:af:73
3	0.001028	192.168.1.105	199.2.53.206	TCP	62	1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
4	2.962850	192.168.1.105	199.2.53.206	TCP	62	[TCP Retransmission] 1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
5	8.971488	192.168.1.105	199.2.53.206	TCP	62	[TCP Retransmission] 1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
6	13.542974	CnetTech_73:8d:ce	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
7	17.444423	192.168.1.105	128.119.245.12	TCP	62	1058 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
8	17.465902	128.119.245.12	192.168.1.105	TCP	62	80 → 1058 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
9	17.465927	192.168.1.105	128.119.245.12	TCP	54	1058 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10	17.466468	192.168.1.105	128.119.245.12	HTTP	686	GET /ethereal-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
11	17.494766	128.119.245.12	192.168.1.105	TCP	60	80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=0

> Frame 10: 686 bytes on wire (5488 bits), 686 bytes captured (5488 bits)

✓ Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)

> Destination: LinksysG_da:af:73 (00:06:25:da:af:73)

> Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)

Type: IPv4 (0x0800) 3

> Internet Protocol Version 4, Src: 192.168.1.105, Dst: 128.119.245.12

> Transmission Control Protocol, Src Port: 1058, Dst Port: 80, Seq: 1, Ack: 1, Len: 632

✓ Hypertext Transfer Protocol

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

Host: gaia.cs.umass.edu\r\n

User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.2) Gecko/20030208 Netscape/7.02\r\n

Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-mng,image/png,image/jpeg,image/gif;q=0.2,text/css,*/*;q=0.1\r\n

Accept-Language: en-us,en;q=0.50\r\n

Accept-Encoding: gzip, deflate, compress;q=0.9\r\n

Accept-Charset: ISO-8859-1, utf-8;q=0.66,*;q=0.66\r\n

Keep-Alive: 300\r\n

Connection: keep-alive\r\n

If-Modified-Since: Sat, 28 Aug 2004 17:00:40 GMT\r\n

If-None-Match: "1b8c3-1194-c578fe00"\r\n

Cache-Control: max-age=0\r\n

\r\n

[Full request URI: http://gaia.cs.umass.edu/ethereal-labs/HTTP-ethereal-lab-file3.html]

[HTTP request 1/1]

[Response in frame: 16]

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

The G appears 54 bytes into the frame. When mousing over the byte, the visible byte count at the bottom of the window uses base 0 counting so that’s what I am going to use base 0 counting.

ethernet-ethereal-trace-1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

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	LinksysG_da:af:73	AmbitMic_a9:3d:68	ARP	60	192.168.1.1 is at 00:06:25:da:af:73
3	0.001028	192.168.1.105	199.2.53.206	TCP	62	1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
4	2.962850	192.168.1.105	199.2.53.206	TCP	62	[TCP Retransmission] 1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
5	8.971488	192.168.1.105	199.2.53.206	TCP	62	[TCP Retransmission] 1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
6	13.542974	CnetTech_73:8d:ce	Broadcast	ARP	60	Who has 192.168.1.11? Tell 192.168.1.104
7	17.444423	192.168.1.105	128.119.245.12	TCP	62	1058 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
8	17.465902	128.119.245.12	192.168.1.105	TCP	62	80 → 1058 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
9	17.465927	192.168.1.105	128.119.245.12	TCP	54	1058 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10	17.466468	192.168.1.105	128.119.245.12	HTTP	686	GET /ethereal-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
11	17.494766	128.119.245.12	192.168.1.105	TCP	60	80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=0

> Frame 10: 686 bytes on wire (5488 bits), 686 bytes captured (5488 bits)

> Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)

> Destination: LinksysG_da:af:73 (00:06:25:da:af:73)

> Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)

Type: IPv4 (0x0800)

> Internet Protocol Version 4, Src: 192.168.1.105, Dst: 128.119.245.12

> Transmission Control Protocol, Src Port: 1058, Dst Port: 80, Seq: 1, Ack: 1, Len: 632

> Hypertext Transfer Protocol

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

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

Request Method: GET

Request URI: /ethereal-labs/HTTP-ethereal-lab-file3.html

Request Version: HTTP/1.1

Host: gaia.cs.umass.edu\r\n

User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.2) Gecko/20030208 Netscape/7.02\r\n

Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-mng,image/png,image/jpeg,image/gif;q=0.2,text/css;*/q=0.1\r\n

Accept-Language: en-us,en;q=0.50\r\n

Accept-Encoding: gzip, deflate, compress;q=0.9\r\n

Accept-Charset: ISO-8859-1, utf-8;q=0.66,*/*;q=0.66\r\n

Keep-Alive: 300\r\n

Connection: keep-alive\r\n

If-Modified-Since: Sat, 28 Aug 2004 17:00:40 GMT\r\n

If-None-Match: "1b8c3-1194-c578fe00"\r\n

Cache-Control: max-age=0\r\n

\r\n

[Full request URI: http://gaia.cs.umass.edu/ethereal-labs/HTTP-ethereal-lab-file3.html]

0000 00 06 25 da af 73 00 d0 59 a9 3d 68 08 00 45 00 ...s...Y=h...E-

0010 02 a0 00 fa 40 00 80 06 bf c8 c0 a8 01 69 80 77 ...@...i-w

0020 f5 0c 04 22 00 50 65 14 99 a7 ac a5 3f b4 50 18 ...".Pe...r.p

0030 fa f0 7e 4f 00 00 47 48 54 20 2f 65 74 68 65 72 ...O.../ether

0040 65 61 6c 2d 6c 61 62 73 2f 48 54 54 50 2d 65 74 eal-labs /HTTP-et

0050 68 65 72 65 61 6c 2d 6c 61 62 2d 66 69 6c 65 33 hereal-l ab-file3

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 source address is 00:06:25:da:af:73

As in question 2 this is the address of the external router used by “my” computer.

ethernet-ethereal-trace-1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
8	17.465902	128.119.245.12	192.168.1.105	TCP	62	80 → 1058 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
9	17.465927	192.168.1.105	128.119.245.12	TCP	54	1058 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10	17.466468	192.168.1.105	128.119.245.12	HTTP	686	GET /ethereal-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
11	17.494766	128.119.245.12	192.168.1.105	TCP	60	80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=0
12	17.498935	128.119.245.12	192.168.1.105	TCP	1514	80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=1460 [TCP segment of a reassembled PDU]
13	17.500025	128.119.245.12	192.168.1.105	TCP	1514	80 → 1058 [ACK] Seq=1461 Ack=633 Win=6952 Len=1460 [TCP segment of a reassembled PDU]
14	17.500069	192.168.1.105	128.119.245.12	TCP	54	1058 → 80 [ACK] Seq=633 Ack=2921 Win=64240 Len=0
15	17.527057	128.119.245.12	192.168.1.105	TCP	1514	80 → 1058 [ACK] Seq=2921 Ack=633 Win=6952 Len=1460 [TCP segment of a reassembled PDU]
16	17.527422	128.119.245.12	192.168.1.105	HTTP	489	HTTP/1.1 200 OK (text/html)
17	17.527457	192.168.1.105	128.119.245.12	TCP	54	1058 → 80 [ACK] Seq=633 Ack=4816 Win=64240 Len=0

> Frame 12: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)

> Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)

> Destination: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)

> Source: LinksysG_da:af:73 (00:06:25:da:af:73)

Type: IPv4 (0x0800)

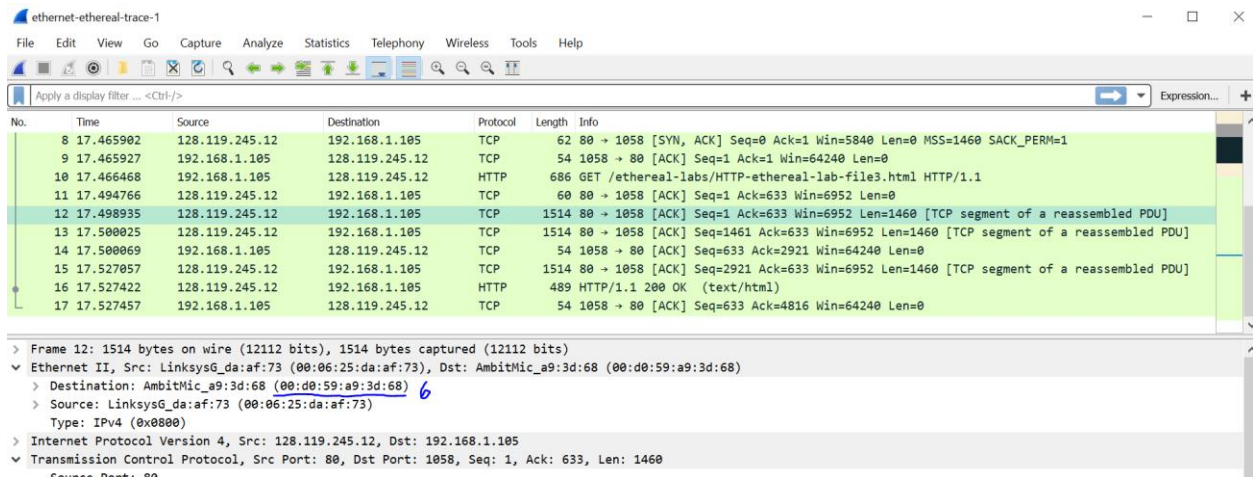
> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.105

> Transmission Control Protocol, Src Port: 80, Dst Port: 1058, Seq: 1, Ack: 633, Len: 1460

Source Port: 80

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

00:d0:59:a9:3d:68 which is the ethernet address of “my” computer.



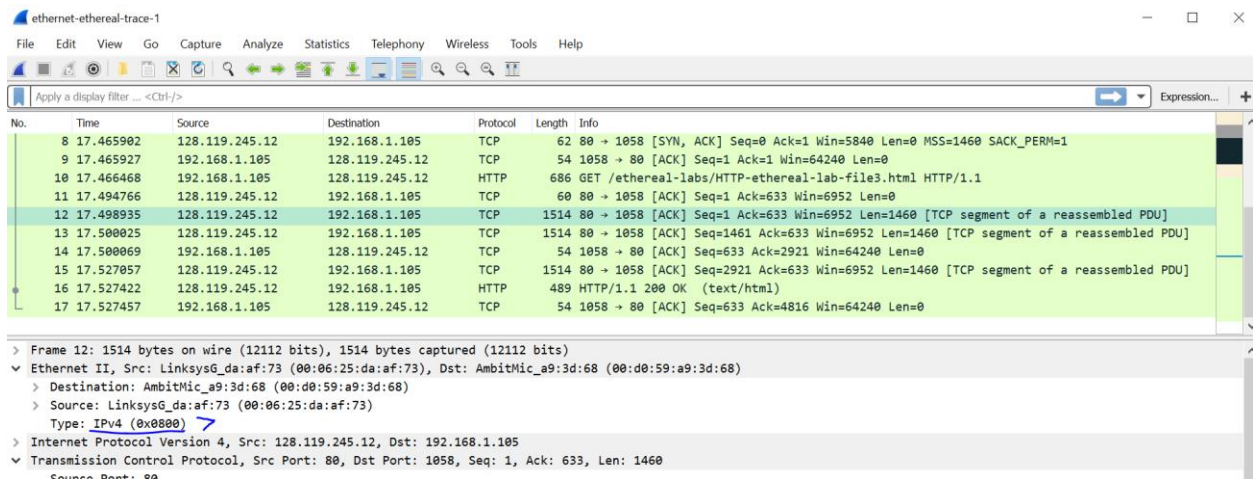
The screenshot shows a Wireshark capture of an Ethernet frame. The packet list on the left shows a packet at time 17.465902, source 128.119.245.12, destination 192.168.1.105, protocol TCP, length 62. The packet details pane on the right shows the Ethernet II header with source LinksysG_da:af:73 and destination AmbitMic_a9:3d:68. The Internet Protocol Version 4 header shows source 128.119.245.12 and destination 192.168.1.105. The Transmission Control Protocol header shows source port 80, destination port 1058, sequence 1, and acknowledgment 633.

No.	Time	Source	Destination	Protocol	Length	Info
8	17.465902	128.119.245.12	192.168.1.105	TCP	62	80 → 1058 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
9	17.465927	192.168.1.105	128.119.245.12	TCP	54	1058 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10	17.466468	192.168.1.105	128.119.245.12	HTTP	686	GET /ethereal-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
11	17.494766	128.119.245.12	192.168.1.105	TCP	60	80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=0
12	17.498935	128.119.245.12	192.168.1.105	TCP	1514	80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=1460 [TCP segment of a reassembled PDU]
13	17.500025	128.119.245.12	192.168.1.105	TCP	1514	80 → 1058 [ACK] Seq=1461 Ack=633 Win=6952 Len=1460 [TCP segment of a reassembled PDU]
14	17.500069	192.168.1.105	128.119.245.12	TCP	54	1058 → 80 [ACK] Seq=633 Ack=2921 Win=64240 Len=0
15	17.527057	128.119.245.12	192.168.1.105	TCP	1514	80 → 1058 [ACK] Seq=2921 Ack=633 Win=6952 Len=1460 [TCP segment of a reassembled PDU]
16	17.527422	128.119.245.12	192.168.1.105	HTTP	489	HTTP/1.1 200 OK (text/html)
17	17.527457	192.168.1.105	128.119.245.12	TCP	54	1058 → 80 [ACK] Seq=633 Ack=4816 Win=64240 Len=0

> Frame 12: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
▼ Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
 > Destination: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
 > Source: LinksysG_da:af:73 (00:06:25:da:af:73)
 Type: IPv4 (0x0800)
 > Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.105
 ▼ Transmission Control Protocol, Src Port: 80, Dst Port: 1058, Seq: 1, Ack: 633, Len: 1460
 Source Port: 80

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

The hexadecimal for the two-byte frame type field is 0x0800. This refers to the IPv4 protocol.



The screenshot shows a Wireshark capture of an Ethernet frame. The packet list on the left shows a packet at time 17.465902, source 128.119.245.12, destination 192.168.1.105, protocol TCP, length 62. The packet details pane on the right shows the Ethernet II header with source LinksysG_da:af:73 and destination AmbitMic_a9:3d:68. The Internet Protocol Version 4 header shows source 128.119.245.12 and destination 192.168.1.105. The Transmission Control Protocol header shows source port 80, destination port 1058, sequence 1, and acknowledgment 633.

No.	Time	Source	Destination	Protocol	Length	Info
8	17.465902	128.119.245.12	192.168.1.105	TCP	62	80 → 1058 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
9	17.465927	192.168.1.105	128.119.245.12	TCP	54	1058 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10	17.466468	192.168.1.105	128.119.245.12	HTTP	686	GET /ethereal-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
11	17.494766	128.119.245.12	192.168.1.105	TCP	60	80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=0
12	17.498935	128.119.245.12	192.168.1.105	TCP	1514	80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=1460 [TCP segment of a reassembled PDU]
13	17.500025	128.119.245.12	192.168.1.105	TCP	1514	80 → 1058 [ACK] Seq=1461 Ack=633 Win=6952 Len=1460 [TCP segment of a reassembled PDU]
14	17.500069	192.168.1.105	128.119.245.12	TCP	54	1058 → 80 [ACK] Seq=633 Ack=2921 Win=64240 Len=0
15	17.527057	128.119.245.12	192.168.1.105	TCP	1514	80 → 1058 [ACK] Seq=2921 Ack=633 Win=6952 Len=1460 [TCP segment of a reassembled PDU]
16	17.527422	128.119.245.12	192.168.1.105	HTTP	489	HTTP/1.1 200 OK (text/html)
17	17.527457	192.168.1.105	128.119.245.12	TCP	54	1058 → 80 [ACK] Seq=633 Ack=4816 Win=64240 Len=0

> Frame 12: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
▼ Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
 > Destination: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
 > Source: LinksysG_da:af:73 (00:06:25:da:af:73)
 Type: IPv4 (0x0800)
 > Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.105
 ▼ Transmission Control Protocol, Src Port: 80, Dst Port: 1058, Seq: 1, Ack: 633, Len: 1460
 Source Port: 80

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 O appears 66 bytes in, using a base 0 counting system.

ethernet-ethereal-trace-1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
8	17.465992	128.119.245.12	192.168.1.105	TCP	62	80 → 1058 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
9	17.465927	192.168.1.105	128.119.245.12	TCP	54	1058 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10	17.466468	192.168.1.105	128.119.245.12	HTTP	686	GET /etherreal-labs/HTTP-etherreal-lab-file3.html HTTP/1.1
11	17.494766	128.119.245.12	192.168.1.105	TCP	60	80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=0
12	17.498935	128.119.245.12	192.168.1.105	TCP	1514	80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=1460 [TCP segment of a reassembled PDU]
13	17.500025	128.119.245.12	192.168.1.105	TCP	1514	80 → 1058 [ACK] Seq=1461 Ack=633 Win=6952 Len=1460 [TCP segment of a reassembled PDU]
14	17.500069	192.168.1.105	128.119.245.12	TCP	54	1058 → 80 [ACK] Seq=633 Ack=2921 Win=64240 Len=0
15	17.527057	128.119.245.12	192.168.1.105	TCP	1514	80 → 1058 [ACK] Seq=2921 Ack=633 Win=6952 Len=1460 [TCP segment of a reassembled PDU]
16	17.527422	128.119.245.12	192.168.1.105	HTTP	489	HTTP/1.1 200 OK (text/html)
17	17.527457	192.168.1.105	128.119.245.12	TCP	54	1058 → 80 [ACK] Seq=633 Ack=4816 Win=64240 Len=0

> Frame 12: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)

▼ Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)

> Destination: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)

> Source: LinksysG_da:af:73 (00:06:25:da:af:73)

Type: IPv4 (0x0800)

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.1.105

▼ Transmission Control Protocol, Src Port: 80, Dst Port: 1058, Seq: 1, Ack: 633, Len: 1460

Source Port: 80

Destination Port: 1058

[Stream index: 1]

[TCP Segment Len: 1460]

Sequence number: 1 (relative sequence number)

[Next sequence number: 1461 (relative sequence number)]

Acknowledgment number: 633 (relative ack number)

0101 = Header Length: 20 bytes (5)

> Flags: 0x010 (ACK)

Window size value: 6952

[Calculated window size: 6952]

[Window size scaling factor: -2 (no window scaling used)]

Checksum: 0x5ed0 [unverified]

[Checksum Status: Unverified]

Urgent pointer: 0

> [SEQ/ACK analysis]

> [Timestamps]

TCP payload (1460 bytes)

[Reassembled PDU in frame: 16]

0000 00 d0 59 a9 3d 68 00 06 25 da af 73 08 00 45 60 ...Y..h...%.:.E

0010 05 dc 8f 2f 40 00 37 06 76 f7 80 77 f5 0c c0 a8 .../@.7. v..w...

0020 01 69 00 50 04 22 ac a5 3f b4 65 14 9c 1f 50 10 ...i.P..."?e..P

0030 1b 28 5e d0 00 00 48 54 54 50 2f 31 2e 31 20 32 ...(^...HT TP/1.1 2

0040 30 30 30 4f 4b 0d 0a 44 61 74 65 3a 20 53 61 74 00 00 Date: Sat

0050 2c 20 32 38 20 41 75 67 20 32 30 30 3a 20 31 37 , 28 Aug 2004 17

0060 3a 31 39 3a 33 37 20 47 4d 54 0d 0a 53 65 72 76 :19:37 G MT: Serv

0070 65 72 3a 20 41 70 61 63 68 65 2f 32 2e 30 2e 34 er: Apac he/2.0.4

0080 30 20 28 52 65 64 20 48 61 74 20 4c 69 6e 75 78 0 (Red H at Linux

0090 29 0d 0a 4c 61 73 74 2d 4d 6f 64 69 66 69 65 64)..Last- Modified

00a0 3a 20 53 61 74 2c 20 32 38 20 41 75 67 20 32 30 : Sat, 2 8 Aug 20

00b0 30 34 20 31 37 3a 31 38 3a 35 33 20 47 4d 54 0d 04 17:18 :53 GMT-

00c0 0a 45 54 61 67 3a 20 22 31 62 61 35 63 2d 31 31 -ETag: " 1ba5c-11

00d0 39 34 2d 36 39 65 64 39 34 30 22 0d 0a 41 63 63 94-69ed9 40"-Acc

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

The internet address column lists the IP addresses.

The physical address column lists the MAC addresses.

The type column lists whether the entry is dynamic or static, static being the manually entered entries and dynamic being a entry that that is kept for a specific amount of time.

Internet Address	Physical Address	Type
192.168.0.1	dc-bf-e9-f6-64-61	dynamic
192.168.0.14	d8-31-34-32-2c-1f	dynamic
192.168.0.16	02-0f-b5-71-7d-d4	dynamic
192.168.0.23	02-0f-b5-9a-94-42	dynamic
192.168.0.27	02-0f-b5-e3-97-e4	dynamic

192.168.0.30	60-6d-3c-12-e1-47	dynamic
192.168.0.36	9c-5a-44-58-4a-00	dynamic
192.168.0.255	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:\Windows\System32>arp -a -v

Interface: 127.0.0.1 --- 0x1
  Internet Address      Physical Address      Type
  224.0.0.0             static
  224.0.0.22            static
  224.0.0.251           static
  239.255.255.250       static
  255.255.255.255       static

Interface: 192.168.0.19 --- 0xe
  Internet Address      Physical Address      Type
  192.168.0.1           dc-bf-e9-f6-64-61    dynamic
  192.168.0.14          d8-31-34-32-2c-1f    dynamic
  192.168.0.16          02-0f-b5-71-7d-d4    dynamic
  192.168.0.23          02-0f-b5-9a-94-42    dynamic
  192.168.0.27          02-0f-b5-e3-97-e4    dynamic
  192.168.0.30          60-6d-3c-12-e1-47    dynamic
  192.168.0.36          9c-5a-44-58-4a-00    dynamic
  192.168.0.255         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
```

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: 00:d0:59:a9:3d:68

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	LinksysG_da:af:73	AmbitMic_a9:3d:68	ARP	60	192.168.1.1 is at 00:06:25:da:af:73
3	0.001028	192.168.1.105	199.2.53.206	TCP	62	1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
4	2.962850	192.168.1.105	199.2.53.206	TCP	62	[TCP Retransmission] 1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
5	8.971488	192.168.1.105	199.2.53.206	TCP	62	[TCP Retransmission] 1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
6	13.542974	CnetTech_73:8d:ce	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
7	17.444423	192.168.1.105	128.119.245.12	TCP	62	1058 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
8	17.465902	128.119.245.12	192.168.1.105	TCP	62	80 → 1058 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
9	17.465927	192.168.1.105	128.119.245.12	TCP	54	1058 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10	17.466468	192.168.1.105	128.119.245.12	HTTP	686	GET /ethereal-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
11	17.494766	128.119.245.12	192.168.1.105	TCP	60	80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=0

> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
 > Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
 > Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68) **10**
 Type: ARP (0x0806)
 > Address Resolution Protocol (request)

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

The two-byte the ethernet frame type field is 0x0806 which corresponds to the ARP protocol.

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	LinksysG_da:af:73	AmbitMic_a9:3d:68	ARP	60	192.168.1.1 is at 00:06:25:da:af:73
3	0.001028	192.168.1.105	199.2.53.206	TCP	62	1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
4	2.962850	192.168.1.105	199.2.53.206	TCP	62	[TCP Retransmission] 1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
5	8.971488	192.168.1.105	199.2.53.206	TCP	62	[TCP Retransmission] 1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
6	13.542974	CnetTech_73:8d:ce	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
7	17.444423	192.168.1.105	128.119.245.12	TCP	62	1058 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
8	17.465902	128.119.245.12	192.168.1.105	TCP	62	80 → 1058 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
9	17.465927	192.168.1.105	128.119.245.12	TCP	54	1058 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10	17.466468	192.168.1.105	128.119.245.12	HTTP	686	GET /ethereal-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
11	17.494766	128.119.245.12	192.168.1.105	TCP	60	80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=0

> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
 > Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
 > Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
 Type: ARP (0x0806) **11**
 > Address Resolution Protocol (request)

12. a) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?
 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? c) Does the ARP message contain the IP address of 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?

a) The opcode field begins of byte 20, when using a base 0 counting system.

b) The opcode field value is 1, designating it as a request.

c) The message does contain the IP address of the sender. Its 192.168.1.105

d) You can see in the screenshot below where the request defines the target MAC (Ethernet) address which is the question. The target MAC address is 00:00:00:00:00:00 which signifies it is requesting the mac address from that machine with the IP 192.168.1.105

ethernet-ethereal-trace-1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F> Expression...

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	LinksysG_da:af:73	AmbitMic_a9:3d:68	ARP	60	192.168.1.1 is at 00:06:25:da:af:73
3	0.001028	192.168.1.105	199.2.53.206	TCP	62	1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
4	2.962850	192.168.1.105	199.2.53.206	TCP	62	[TCP Retransmission] 1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
5	8.971488	192.168.1.105	199.2.53.206	TCP	62	[TCP Retransmission] 1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
6	13.542974	CnetTech_73:8d:ce	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
7	17.444423	192.168.1.105	128.119.245.12	TCP	62	1058 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
8	17.465902	128.119.245.12	192.168.1.105	TCP	62	80 → 1058 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
9	17.465927	192.168.1.105	128.119.245.12	TCP	54	1058 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10	17.466468	192.168.1.105	128.119.245.12	HTTP	686	GET /ethereal-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
11	17.494766	128.119.245.12	192.168.1.105	TCP	60	80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=0

> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)

▼ Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

> Destination: Broadcast (ff:ff:ff:ff:ff:ff)

> Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)

Type: ARP (0x0806)

▼ Address Resolution Protocol (request)

Hardware type: Ethernet (1)

Protocol type: IPv4 (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: request (1) **b**

Sender MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)

Sender IP address: 192.168.1.105 **c**

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

Target IP address: 192.168.1.1 **d**

```

0000 ff ff ff ff ff ff 00 d0 59 a9 3d 68 08 06 00 01 .....Y..h....
0010 08 00 06 04 00 01 00 d0 59 a9 3d 68 c0 a8 01 69 .....Y..h....i
0020 00 00 00 00 00 c0 a8 01 01 .....

```

a

13. Now find the ARP reply that was sent in response to the ARP request. a) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin? 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? 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?

a) The opcode field begins on byte 20, when using a base 0 counting system.

b) The opcode field value is 2, designating it as a reply.

c) The message includes the answer in the sender MAC address section, so the answer is 00:06:25:da:af:73

ethernet-ethereal-trace-1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

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	LinksysG_da:af:73	AmbitMic_a9:3d:68	ARP	60	192.168.1.1 is at 00:06:25:da:af:73
3	0.001028	192.168.1.105	199.2.53.206	TCP	62	1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
4	2.962850	192.168.1.105	199.2.53.206	TCP	62	[TCP Retransmission] 1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
5	8.971488	192.168.1.105	199.2.53.206	TCP	62	[TCP Retransmission] 1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
6	13.542974	CnetTech_73:8d:ce	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
7	17.444423	192.168.1.105	128.119.245.12	TCP	62	1058 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
8	17.465902	128.119.245.12	192.168.1.105	TCP	62	80 → 1058 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
9	17.465927	192.168.1.105	128.119.245.12	TCP	54	1058 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10	17.466468	192.168.1.105	128.119.245.12	HTTP	686	GET /ethereal-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
11	17.494766	128.119.245.12	192.168.1.105	TCP	60	80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=0

> Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)

▼ Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)

> Destination: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)

> Source: LinksysG_da:af:73 (00:06:25:da:af:73)

Type: ARP (0x0806)

Padding: 00000000000000000000000000000000

▼ Address Resolution Protocol (reply)

Hardware type: Ethernet (1)

Protocol type: IPv4 (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: reply (2) **b**

Sender MAC address: LinksysG_da:af:73 (00:06:25:da:af:73) **c**

Sender IP address: 192.168.1.1

Target MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)

Target IP address: 192.168.1.105

```

0000  00 d0 59 a9 3d 68 00 06 25 da af 73 08 06 00 01  ..Y=h..%.s....
0010  00 06 06 04 00 02 00 06 25 da af 73 c0 a8 01 01  ..Y=h..%.s....
0020  00 d0 59 a9 3d 68 c0 a8 01 69 00 00 00 00 00 00  ..Y=h..%.i....
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ..Y=h..%.i....

```

a.

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

Source address: 00:06:25:da:af:73

Destination address: 00:d0:59:a9:3d:68

ethernet-ethereal-trace-1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F> Expression...

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	LinksysG_da:af:73	AmbitMic_a9:3d:68	ARP	60	192.168.1.1 is at 00:06:25:da:af:73
3	0.001028	192.168.1.105	199.2.53.206	TCP	62	1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
4	2.962850	192.168.1.105	199.2.53.206	TCP	62	[TCP Retransmission] 1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
5	8.971488	192.168.1.105	199.2.53.206	TCP	62	[TCP Retransmission] 1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
6	13.542974	CnetTech_73:8d:ce	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
7	17.444423	192.168.1.105	128.119.245.12	TCP	62	1058 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
8	17.465902	128.119.245.12	192.168.1.105	TCP	62	80 → 1058 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1
9	17.465927	192.168.1.105	128.119.245.12	TCP	54	1058 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10	17.466468	192.168.1.105	128.119.245.12	HTTP	686	GET /ethereal-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
11	17.494766	128.119.245.12	192.168.1.105	TCP	60	80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=0

> Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)

▼ Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)

> Destination: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)

> Source: LinksysG_da:af:73 (00:06:25:da:af:73) 14

Type: ARP (0x0806)

Padding: 00000000000000000000000000000000

▼ Address Resolution Protocol (reply)

Hardware type: Ethernet (1)

Protocol type: IPv4 (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: reply (2)

Sender MAC address: LinksysG_da:af:73 (00:06:25:da:af:73)

Sender IP address: 192.168.1.1

Target MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)

Target IP address: 192.168.1.105

15. 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 was not ARP reply sent because there isn't a computer in the subnet that has the Ethernet address requested in packet 6 (192.168.1.104).

EX-1: In theory I think it would cause problems any time that entry was used, until at some point it gets updated or removed by the ARP protocol. I tried testing this but was encountering permissions errors.

EX-2: My ARP cache uses a default reachable time of 4000ms as seen below in the screen shot.

```
C:\Windows\System32>netsh interface ipv4 show interface 1

Interface Loopback Pseudo-Interface 1 Parameters
-----
IfLuid                               : loopback_4
IfIndex                              : 1
State                                : connected
Metric                               : 75
Link MTU                             : 4294967295 bytes
Reachable Time                        : 40000 ms
Base Reachable Time                   : 30000 ms
Retransmission Interval               : 1000 ms
```