

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

It is 00-d0-59-a9-3d-68.

The screenshot shows a Wireshark packet capture of an ARP request. The packet list shows a packet of 42 bytes on the wire (336 bits) at time 1.0.000000. The packet details pane shows the Ethernet II frame with source MAC 00:d0:59:a9:3d:68 and destination MAC ff:ff:ff:ff:ff:ff. The ARP request details show the sender IP as 192.168.1.105 and the target IP as 192.168.1.1. The packet bytes pane shows the raw data of the frame.

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] [TCP Port numbers reused] 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] [TCP Port numbers reused] 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	17.465982	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	TCP	686	1058 → 80 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=632
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
13	17.508025	128.119.245.12	192.168.1.105	TCP	1514	80 → 1058 [ACK] Seq=1461 Ack=633 Win=6952 Len=1460
14	17.508069	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
16	17.527422	128.119.245.12	192.168.1.105	TCP	489	80 → 1058 [PSH, ACK] Seq=4381 Ack=633 Win=6952 Len=435
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 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Address Resolution Protocol (request)

Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (1)
Sender MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
Sender IP address: 192.168.1.105
Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.1.1

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....1

Packets: 17 · Displayed: 17 (100.0%) Profile: Default

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.]

It is ff-ff-ff-ff-ff-ff.

The screenshot shows a Wireshark packet capture of an ARP request. The packet list shows a packet of 42 bytes on the wire (336 bits) at time 1.0.000000. The packet details pane shows the Ethernet II frame with source MAC 00:d0:59:a9:3d:68 and destination MAC ff:ff:ff:ff:ff:ff. The ARP request details show the sender IP as 192.168.1.105 and the target IP as 192.168.1.1. The packet bytes pane shows the raw data of the frame.

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] [TCP Port numbers reused] 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] [TCP Port numbers reused] 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	17.465982	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	TCP	686	1058 → 80 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=632
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
13	17.508025	128.119.245.12	192.168.1.105	TCP	1514	80 → 1058 [ACK] Seq=1461 Ack=633 Win=6952 Len=1460
14	17.508069	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
16	17.527422	128.119.245.12	192.168.1.105	TCP	489	80 → 1058 [PSH, ACK] Seq=4381 Ack=633 Win=6952 Len=435
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 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on 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)

No, it is not the Ethernet address of gaia.cs.umass.edu. The Ethernet address is indicating the broadcast all devices in the local area network.

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

It is 0x0806. The corresponding upper layer protocol is ARP in data link layer.

ethernet-ethereal-trace-1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter: (Ctrl+F)

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	AmbITM1c_a9:3d:68	Broadcast	ARP	60	42 who has 192.168.1.1? Tell 192.168.1.105
2	0.001018	LinksysG_da:af:73	AmbITM1c_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] [TCP Port numbers reused] 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] [TCP Port numbers reused] 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	TCP	686	1058 → 80 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=632
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
13	17.500025	128.119.245.12	192.168.1.105	TCP	1514	80 → 1058 [ACK] Seq=1461 Ack=633 Win=6952 Len=1460
14	17.500069	192.168.1.105	128.119.245.12	TCP	54	1058 → 80 [ACK] Seq=633 Ack=2921 Win=6952 Len=0
15	17.527857	128.119.245.12	192.168.1.105	TCP	1514	80 → 1058 [ACK] Seq=2921 Ack=633 Win=6952 Len=1460
16	17.527422	128.119.245.12	192.168.1.105	TCP	489	80 → 1058 [PSH, ACK] Seq=4381 Ack=633 Win=6952 Len=435
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 11: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)

Ethernet II, Src: AmbITM1c_a9:3d:68 (00:00:59:a9:3d:68), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

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

Source: AmbITM1c_a9:3d:68 (00:00:59:a9:3d:68)

Type: ARP (0x0806)

Address Resolution Protocol (request)

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

54 bytes.

ethernet-ethereal-trace-1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter: (Ctrl+F)

No.	Time	Source	Destination	Protocol	Length	Info
2	0.001018	LinksysG_da:af:73	AmbITM1c_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] [TCP Port numbers reused] 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] [TCP Port numbers reused] 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	TCP	686	1058 → 80 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=632
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
13	17.500025	128.119.245.12	192.168.1.105	TCP	1514	80 → 1058 [ACK] Seq=1461 Ack=633 Win=6952 Len=1460
14	17.500069	192.168.1.105	128.119.245.12	TCP	54	1058 → 80 [ACK] Seq=633 Ack=2921 Win=6952 Len=0
15	17.527857	128.119.245.12	192.168.1.105	TCP	1514	80 → 1058 [ACK] Seq=2921 Ack=633 Win=6952 Len=1460
16	17.527422	128.119.245.12	192.168.1.105	TCP	489	80 → 1058 [PSH, ACK] Seq=4381 Ack=633 Win=6952 Len=435

Frame Length: 686 bytes (5488 bits)

0000	00 06 25 da af 73 00 00	59 a9 3d 68 00 00 45 00	..X..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-...?~P:
0030	fa f0 7e 4f 00 00 47 45	54 20 2f 65 74 68 65 72	...O-GE T /ether
0040	65 61 6c 2d 6c 61 62 73	2f 48 54 54 50 2d 65 74	...eal-lab s /HTTP-et
0050	68 65 72 65 61 6c 2d 6c	61 62 2d 66 69 6c 65 33	...hereal-l ab-file3
0060	2e 68 74 6d 6c 20 48 54	54 50 2f 31 2e 31 0d 0ahtml HT TP/1.1..
0070	48 6f 73 74 3a 20 67 61	69 61 2e 63 73 2e 75 6d	...Host: ga ia.cs.um
0080	61 73 73 2e 65 64 75 0d	0a 55 73 65 72 2d 41 67	...ass.edu ~User-Ag
0090	65 6e 74 3a 20 4d 6f 7a	69 6c 6c 61 2f 35 2e 30	...ent: Moz illa/5.0
00a0	20 28 57 69 6e 64 6f 77	73 3b 20 55 3b 20 57 69	... (Window s; U; Wi
00b0	6e 64 6f 77 73 20 4e 54	20 35 2e 31 3b 20 65 6e	...ndows NT 5.1; en
00c0	2d 55 53 3b 20 72 76 3a	31 2e 30 2e 32 29 20 47	...-US; rv:1.0.2) G
00d0	65 63 6b 6f 2f 32 30 30	33 30 32 30 38 20 4e 65	...ecko/200 30208 He
00e0	74 73 63 61 70 65 2f 37	2e 30 32 0d 0a 41 63 63	...tscape/7 .02 ~Acc
00f0	65 70 74 3a 20 74 65 78	74 2f 78 6d 6c 2c 61 70	...ept: tex t/xml,ap
0100	70 6c 69 63 61 74 69 6f	6e 2f 78 6d 6c 2c 61 70	...plicatio n/xml,ap
0110	70 6c 69 63 61 74 69 6f	6e 2f 78 6d 74 6d 6c 2b	...plicatio n/xhtml1+
0120	78 6d 6c 2c 74 65 78 74	2f 68 74 6d 6c 3b 71 3d	...xml,text /html;q=
0130	30 2e 39 2c 74 65 78 74	2f 70 6c 61 69 6e 3b 71	...0.9,text /plain;q

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 address is 00-06-25-da-af-73..

This address is not for both my computer and gaia.cs.umass.edu.

Router has this address.

No.	Time	Source	Destination	Protocol	Length	Info
1 0.000000		AmbitMlc_a9:3d:68	Broadcast	ARP	42	who has 192.168.1.1? Tell 192.168.1.105
2 0.001018		LinksysG_da:af:73	AmbitMlc_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] [TCP Port numbers reused] 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] [TCP Port numbers reused] 1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
6 13.542974		CnetTech_73:8d:c6	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	TCP	686	1058 → 80 [PSH, ACK] Seq=1 Ack=1 Win=64240 Len=632
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
13 17.500025		128.119.245.12	192.168.1.105	TCP	1514	80 → 1058 [ACK] Seq=1461 Ack=633 Win=6952 Len=1460
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
16 17.527422		128.119.245.12	192.168.1.105	TCP	489	80 → 1058 [PSH, ACK] Seq=4381 Ack=633 Win=6952 Len=435
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: AmbitMlc_a9:3d:68 (00:06:25:da:af:73)

Destination: AmbitMlc_a9:3d:68 (00:06:25:da:af:73)
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

0100 = Version: 4

0000	00 00 59 a9 3d 68 00 06 25 da af 73 08 00 45 60	..Y..h..X..s..E
0010	05 dc 8f 2f 40 00 37 06 76 f7 80 77 f5 0c c0 a8	.../0.7. 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 20 4f 4b 0d 0a 44 61 74 65 3a 20 53 61 74	00 OK-D ate: Sat
0050	2c 20 32 38 20 41 75 67 20 32 30 30 34 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

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?

66 bytes.

No.	Time	Source	Destination	Protocol	Length	Info
1 0.000000		AmbitMlc_a9:3d:68	Broadcast	ARP	42	who has 192.168.1.1? Tell 192.168.1.105
2 0.001018		LinksysG_da:af:73	AmbitMlc_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] [TCP Port numbers reused] 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] [TCP Port numbers reused] 1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1

> 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: AmbitMlc_a9:3d:68 (00:06:25:da:af:73)

Destination: AmbitMlc_a9:3d:68 (00:06:25:da:af:73)
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

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS3, ECN: Not-ECT)

Total Length: 1500

Identification: 0xaf2f (36655)

> Flags: 0x00, Don't fragment

0000	00 00 59 a9 3d 68 00 06 25 da af 73 08 00 45 60	..Y..h..X..s..E
0010	05 dc 8f 2f 40 00 37 06 76 f7 80 77 f5 0c c0 a8	.../0.7. 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 20 4f 4b 0d 0a 44 61 74 65 3a 20 53 61 74	00 OK-D ate: Sat
0050	2c 20 32 38 20 41 75 67 20 32 30 30 34 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
00e0	65 70 74 2d 52 61 6e 67 65 73 3a 20 62 79 74 65	ept-Rang es: byte
00f0	73 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74	s--Conte nt-Lengt
0100	68 3a 20 34 35 30 30 0d 0a 4b 65 65 70 2d 41 6c	h: 4500-Keep-Al
0110	69 76 65 3a 20 74 69 6d 65 6f 75 74 3d 31 30 2c	ive: tim eout=10,
0120	20 6d 61 78 3d 31 30 30 0d 0a 43 6f 6e 65 63	max=100 --Connec

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

Each column means IP address, MAC address, and type of the address.

인터페이스: 10.248.188.217 --- 0x11		
인터넷 주소	물리적 주소	유형
10.248.0.1	00-00-5e-00-01-01	정적
10.249.255.255	ff-ff-ff-ff-ff-ff	동적
224.0.0.22	01-00-5e-00-00-16	정적
224.0.0.251	01-00-5e-00-00-fb	정적
224.0.0.252	01-00-5e-00-00-fc	정적
239.255.255.250	01-00-5e-7f-ff-fa	정적
255.255.255.255	ff-ff-ff-ff-ff-ff	정적
인터페이스: 192.168.56.1 --- 0x1a		
인터넷 주소	물리적 주소	유형
192.168.56.255	ff-ff-ff-ff-ff-ff	정적
224.0.0.22	01-00-5e-00-00-16	동적
224.0.0.251	01-00-5e-00-00-fb	정적
224.0.0.252	01-00-5e-00-00-fc	정적
239.255.255.250	01-00-5e-7f-ff-fa	정적

(Translation: “인터페이스” = interface, “인터넷 주소” = IP address, “물리적 주소” = Physical address

“유형” = type, “정적” = static, “동적” = dynamic)

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

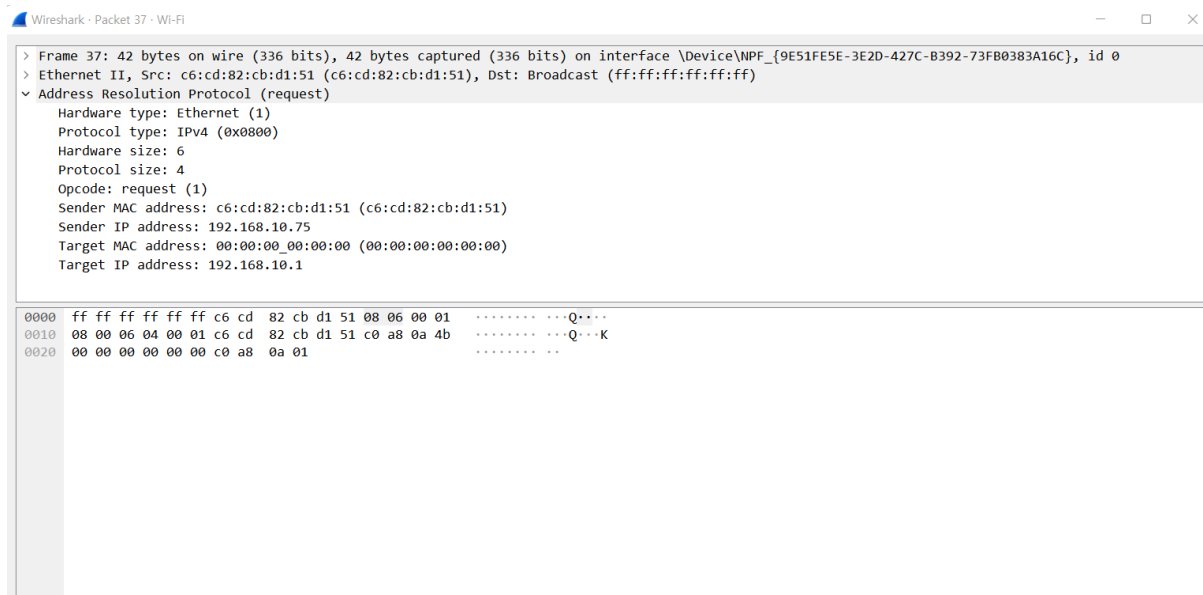
Source Address: C6-CD-82-CB-D1-51

Destination Address: 00-00-00-00-00-00

No.	Time	Source	Destination	Protocol	Length	Info
5	2.536624	Callix_11:3f:1a	c6:cd:82:cb:d1:51	ARP	60	Who has 192.168.10.75? Tell 192.168.10.1
6	2.536780	c6:cd:82:cb:d1:51	Callix_11:3f:1a	ARP	42	192.168.10.75 is at c6:cd:82:cb:d1:51
10	3.088343	Routerbo_a8:7f:d3	Broadcast	ARP	60	Who has 10.185.252.50? Tell 10.185.252.1
37	9.377811	c6:cd:82:cb:d1:51	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.75
38	9.431579	Callix_11:3f:1a	c6:cd:82:cb:d1:51	ARP	60	192.168.10.1 is at 44:65:7f:11:3f:1a

> Frame 37: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{9E51FE5E-3E2D-427C-B392-73FB083A16C}, id 0 > Ethernet II, Src: c6:cd:82:cb:d1:51 (c6:cd:82:cb:d1:51), Dst: Broadcast (ff:ff:ff:ff:ff:ff) > Destination: Broadcast (ff:ff:ff:ff:ff:ff) > Source: c6:cd:82:cb:d1:51 (c6:cd:82:cb:d1:51) Type: ARP (0x0806) > Address Resolution Protocol (request) Hardware type: Ethernet (1) Protocol type: IPv4 (0x0800) Hardware size: 6 Protocol size: 4 Opcode: request (1) Sender MAC address: c6:cd:82:cb:d1:51 (c6:cd:82:cb:d1:51) Sender IP address: 192.168.10.75 Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00) Target IP address: 192.168.10.1	
--	--

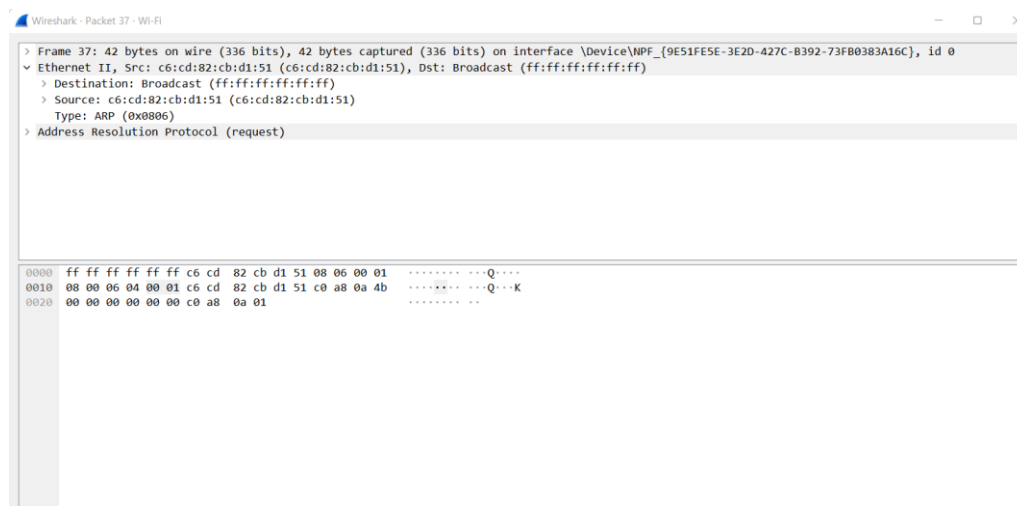
0000	ff ff ff ff ff ff c6 cd 82 cb d1 51 08 06 00 01	-----Q----
0010	00 00 06 04 00 01 c6 cd 82 cb d1 51 c0 a8 0a 4b	-----Q--K
0020	00 00 00 00 00 00 c0 a8 01	-----



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

The hexadecimal value is 0x0806.

This corresponds to ARP protocol.



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/inet-pages/arp.html>.

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

The ARP opcode field begins 20 bytes from the beginning of the Ethernet frame.

Hardware type: Ethernet (1)	
Protocol type: IPv4 (0x0800)	
Hardware size: 6	
Protocol size: 4	
Opcode: request (1)	
Sender MAC address: c6:cd:82:cb:d1:51 (c6:cd:82:cb:d1:51)	
Sender IP address: 192.168.10.75	
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)	
Target IP address: 192.168.10.1	
0000	ff ff ff ff ff ff c6 cd 82 cb d1 51 08 06 00 01
0010	08 00 06 04 00 01 c6 cd 82 cb d1 51 c0 a8 0a 4b
0020	00 00 00 00 00 00 c0 a8 0a 01

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 value of the opcode field is 0x0001.

Hardware type: Ethernet (1)	
Protocol type: IPv4 (0x0800)	
Hardware size: 6	
Protocol size: 4	
Opcode: request (1)	
Sender MAC address: c6:cd:82:cb:d1:51 (c6:cd:82:cb:d1:51)	
Sender IP address: 192.168.10.75	
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)	
Target IP address: 192.168.10.1	
0000	ff ff ff ff ff ff c6 cd 82 cb d1 51 08 06 00 01
0010	08 00 06 04 00 01 c6 cd 82 cb d1 51 c0 a8 0a 4b
0020	00 00 00 00 00 00 c0 a8 0a 01

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

The ARP message contains the IP address of the sender.

Hardware type: Ethernet (1)	
Protocol type: IPv4 (0x0800)	
Hardware size: 6	
Protocol size: 4	
Opcode: request (1)	
Sender MAC address: c6:cd:82:cb:d1:51 (c6:cd:82:cb:d1:51)	
Sender IP address: 192.168.10.75	
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)	
Target IP address: 192.168.10.1	
0000	ff ff ff ff ff ff c6 cd 82 cb d1 51 08 06 00 01
0010	08 00 06 04 00 01 c6 cd 82 cb d1 51 c0 a8 0a 4b
0020	00 00 00 00 00 00 c0 a8 0a 01

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

The question appears in the 0x0020 line of the frame.

0		8		15		16		31	
Hardware Type				Protocol Type					
HLEN		PLEN		Operation					
Sender HA (octets 0-3)									
Sender HA (octets 4-5)				Sender IP (octets 0-1)					
Sender IP (octets 2-3)				Target HA (octets 0-1)					
Target HA (octets 2-5)									
Target IP (octets 0-3)									

The opcode field begins 20 bytes from the beginning of the Ethernet frame.

```

> Frame 38: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{9E51FE5E-3E2D-B392-73FB0383A16C}, id 0
  Ethernet II, Src: Calix_11:3f:1a (44:65:7f:11:3f:1a), Dst: c6:cd:82:cb:d1:51 (c6:cd:82:cb:d1:51)
    Destination: c6:cd:82:cb:d1:51 (c6:cd:82:cb:d1:51)
    Source: Calix_11:3f:1a (44:65:7f:11:3f:1a)
    Type: ARP (0x0806)
    Padding: 00000000000000000000000000000000
  Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)

```

0000	c6	cd	82	cb	d1	51	44	65	7f	11	3f	1a	08	06	00	01	...	QDe	..?
0010	08	00	06	04	00	02	44	65	7f	11	3f	1a	c0	a8	0a	01	De	..?
0020	c6	cd	82	cb	d1	51	c0	a8	0a	4b	00	00	00	00	00	00	Q..	..K
0030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			

The value of the opcode field is 0x0002.

```
> Frame 38: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{9E51FE5E-3E2D-427C-B392-73FB0383A16C}, id 0
Ethernet II, Src: Calix_11:3f:1a (44:65:7f:11:3f:1a), Dst: c6:cd:82:cb:d1:51 (c6:cd:82:cb:d1:51)
  > Destination: c6:cd:82:cb:d1:51 (c6:cd:82:cb:d1:51)
  > Source: Calix_11:3f:1a (44:65:7f:11:3f:1a)
  Type: ARP (0x0806)
  Padding: 00000000000000000000000000000000
Address Resolution Protocol (reply)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
```

0000	c6 cd 82 cb d1 51 44 65 7f 11 3f 1a 08 06 00 01QDe --?.....
0010	08 00 06 04 00 02 44 65 7f 11 3f 1a c0 a8 0a 01De --?.....
0020	c6 cd 82 cb d1 51 c0 a8 0a 4b 00 00 00 00 00 00Q...K.....
0030	00 00 00 00 00 00 00 00 00 00 00 00

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?

The answer is in the 0x0010 line of the frame.

No.	Time	Source	Destination	Protocol	Length	Info
5	2.536624	Calix_11:3f:1a	c6:cd:82:cb:d1:51	ARP	60	Who has 192.168.10.75? Tell 192.168.10.1
6	2.536700	c6:cd:82:cb:d1:51	Calix_11:3f:1a	ARP	42	192.168.10.75 is at c6:cd:82:cb:d1:51
10	3.088343	Routerbo_a8:7f:d3	Broadcast	ARP	60	Who has 10.185.252.50? Tell 10.185.252.1
37	9.377811	c6:cd:82:cb:d1:51	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.75
38	9.431579	Calix_11:3f:1a	c6:cd:82:cb:d1:51	ARP	60	192.168.10.1 is at 44:65:7f:11:3f:1a


```

Address: Calix_11:3f:1a (44:65:7f:11:3f:1a)
....0.. = LG bit: Globally unique address (factory default)
....0.. = IG bit: Individual address (unicast)
Type: ARP (0x0806)
Padding: 00000000000000000000000000000000
▼ Address Resolution Protocol (reply)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
0000 c6 cd 82 cb d1 51 44 65 7f 11 3f 1a 00 06 00 01 .....QDe-?.....
0010 00 00 06 04 00 02 44 65 7f 11 3f 1a c0 a8 0a 01 .....De-?.....
0020 c6 cd 82 cb d1 51 c0 a8 0a 4b 00 00 00 00 00 00 .....Q--K-.....
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

```

0	8	15	16	31
Hardware Type		Protocol Type		
HLEN		PLEN		Operation
Sender HA (octets 0-3)				
Sender HA (octets 4-5)		Sender IP (octets 0-1)		
Sender IP (octets 2-3)		Target HA (octets 0-1)		
Target HA (octets 2-5)				
Target IP (octets 0-3)				

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

Source Address: 44-65-7F-11-3F-1A

Destination Address: C6-CD-82-CB-D1-51

No.	Time	Source	Destination	Protocol	Length	Info
5	2.536624	Calix_11:3f:1a	c6:cd:82:cb:d1:51	ARP	60	Who has 192.168.10.75? Tell 192.168.10.1
6	2.536700	c6:cd:82:cb:d1:51	Calix_11:3f:1a	ARP	42	192.168.10.75 is at c6:cd:82:cb:d1:51
10	3.088343	Routerbo_a8:7f:d3	Broadcast	ARP	60	Who has 10.185.252.50? Tell 10.185.252.1
37	9.377811	c6:cd:82:cb:d1:51	Broadcast	ARP	42	Who has 192.168.10.1? Tell 192.168.10.75
38	9.431579	Calix_11:3f:1a	c6:cd:82:cb:d1:51	ARP	60	192.168.10.1 is at 44:65:7f:11:3f:1a

```

> Frame 38: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{9E51FE5E-3E2D-427C-8392-73F80383A16C}, id 0
> Ethernet II, Src: Calix_11:3f:1a (44:65:7f:11:3f:1a), Dst: c6:cd:82:cb:d1:51 (c6:cd:82:cb:d1:51)
  > Destination: c6:cd:82:cb:d1:51 (c6:cd:82:cb:d1:51)
    Address: c6:cd:82:cb:d1:51 (c6:cd:82:cb:d1:51)
    ....1.. = LG bit: Locally administered address (this is NOT the factory default)
    ....0.. = IG bit: Individual address (unicast)
  > Source: Calix_11:3f:1a (44:65:7f:11:3f:1a)
    Type: ARP (0x0806)
    Padding: 00000000000000000000000000000000
  > Address Resolution Protocol (reply)

```

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 ARP request because the computer 192.168.1.105 is not the subject of the target address. The computer 192.168.1.104 broadcasts the request in the entire local area network, and the computer 192.168.1.117 replies to the request so that the computer 192.168.1.105 cannot see the ARP reply going to the computer 192.168.1.104.

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?

The packet frame will never reach the receiver if the Ethernet address is wrong while the IP address is correct. The sender sends the packet with MAC header and IP header to the receiver. Then, the LAN checks the MAC address and then sends it to correspond receiver. However, if the MAC address is wrong, then the LAN will reject that packet frame. Therefore, the packet from the sender will never arrive the receiver.

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 operation system documentation. Indicate how/where you determined this value.

There is no default amount of time that an entry remains in ARP cache before being removed in Windows operating system.

“In the new Windows Vista TCP/IP stack implementation, hosts create the neighbor cache entries when there is no matching entry in the neighbor cache. ARP cache entry for IPv4 is an example of a neighbor cache entry. After the entry is successfully created in the neighbor cache, the entry may change to the "Reachable" state if the entry meets certain conditions. If the entry is in the "Reachable" state, Windows Vista TCP/IP hosts do not send ARP requests to the network. Therefore, Windows Vista TCP/IP hosts use the information in the cache. If an entry is not used, and it stays in the "Reachable" state for longer than its "Reachable Time" value, the entry changes to the "Stale" state. If an entry is in the "Stale" state, the Windows Vista TCP/IP host must send an ARP request to reach that destination.”

“The "Reachable Time" value is calculated as follows:

Reachable Time = BaseReachable Time × (A random value between MIN_RANDOM_FACTOR and MAX_RANDOM_FACTOR)

RFC provides the following calculated results.”

BaseReachable Time	30,000 milliseconds (ms)
MIN_RANDOM_FACTOR	0.5
MAX_RANDOM_FACTOR	1.5

“Therefore, the "Reachable Time" value is somewhere between 15 seconds (30×0.5 seconds) and 45 seconds (30×1.5 seconds). If an entry is not used for a time between 15 to 45 seconds, it changes to the "Stale" state. Then, the host must send an ARP Request for IPV4 to the network when any IP datagram is sent to that destination.”

(Source from:

<https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/address-resolution-protocol-arp-caching-behavior>)