

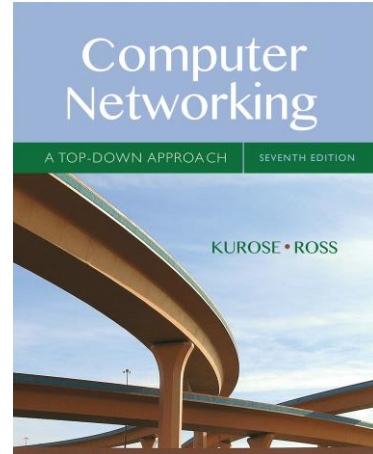
Name: Katie Schaumleffle

Wireshark Lab: Ethernet and ARP v7.0

Supplement to *Computer Networking: A Top-Down Approach*, 7th ed., J.F. Kurose and K.W. Ross

“Tell me and I forget. Show me and I remember. Involve me and I understand.” Chinese proverb

© 2005-2016 J.F Kurose and K.W. Ross, All Rights Reserved



1. What is the 48-bit Ethernet address of your computer?
68:3e:26:ec:1f:4e

Wireshark interface showing a packet capture. The packet list shows a GET request from 10.0.0.129 to 128.119.245.12. The packet details pane shows the Ethernet II frame with source MAC 68:3e:26:ec:1f:4e and destination MAC f8:a0:97:8c:59:c2. The packet bytes pane shows the raw data of the frame.

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.]

Destination: f8:a0:97:8c:59:c2

No, this is not the Ethernet address of gaia.cs.mass.edu. This is the address of my router at my house.

The image shows a Wireshark packet capture window titled "Wi-Fi". The packet list on the left shows several packets, with packet 83 highlighted. The packet details pane on the right shows the structure of packet 83, which is an ICMPv6 Router Advertisement. The destination MAC address is highlighted in red in the details pane.

No.	Time	Source	Destination	Protocol	Length	Info
71	4.827224	2620:1ec:42::132	2601:1c2:801:1e20:c...	TCP	74	443 → 63007 [FIN, ACK] Seq=1 Ack=2 Win=16381 Len=0
72	4.827370	2601:1c2:801:1e20:c...	2620:1ec:42::132	TCP	74	63007 → 443 [ACK] Seq=2 Ack=2 Win=514 Len=0
73	5.085609	10.0.0.129	128.119.245.12	TCP	66	63019 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
74	5.086330	10.0.0.129	128.119.245.12	TCP	66	63020 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
75	5.179350	128.119.245.12	10.0.0.129	TCP	66	80 → 63019 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
76	5.179477	10.0.0.129	128.119.245.12	TCP	54	63019 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
77	5.179822	10.0.0.129	128.119.245.12	HTTP	642	GET /wireshark-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
78	5.187103	128.119.245.12	10.0.0.129	TCP	66	80 → 63020 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
79	5.187268	10.0.0.129	128.119.245.12	TCP	54	63020 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
80	5.280313	128.119.245.12	10.0.0.129	TCP	56	80 → 63019 [ACK] Seq=1 Ack=589 Win=30464 Len=0
81	5.282504	128.119.245.12	10.0.0.129	HTTP	295	HTTP/1.1 304 Not Modified
82	5.327935	10.0.0.129	128.119.245.12	TCP	54	63019 → 80 [ACK] Seq=589 Ack=242 Win=131072 Len=0
83	6.144262	fe80::faa0:97ff:fe8...	ff02::1	ICMPv6	174	Router Advertisement from f8:a0:97:8c:59:c2
84	7.203456	2407:30c0:182::aa72...	2601:1c2:801:1e20:c...	TCP	74	[TCP Dup ACK 44#1] 443 → 62114 [ACK] Seq=1 Ack=1 Win=8 Len=0
85	7.203530	2601:1c2:801:1e20:c...	2407:30c0:182::aa72...	TCP	74	[TCP Dup ACK 45#1] 62114 → 443 [ACK] Seq=1 Ack=2 Win=515 Len=0
86	8.090046	10.0.0.192	224.0.0.251	MDNS	415	Standard query response 0x0000 PTR, cache flush Katies-iPhone.local PTR, cache flush Katies-iPhone...
87	8.090955	fe80::85b:8e4d:51b0...	ff02::fb	MDNS	435	Standard query response 0x0000 PTR, cache flush Katies-iPhone.local PTR, cache flush Katies-iPhone...
88	8.192139	10.0.0.192	224.0.0.251	MDNS	181	Standard query 0x0000 PTR_companion-link_tcp.local, "QU" question PTR_homekit_tcp.local, "QU" q...

Frame 77: 642 bytes on wire (5136 bits), 642 bytes captured (5136 bits) on interface \Device\NPF_{CCDC22D-0101-426D-BAD9-134DD...}

Ethernet II, Src: IntelCor_ec:1f:4e (68:3e:26:ec:1f:4e), Dst: ARRISGro_8c:59:c2 (f8:a0:97:8c:59:c2)

Destination: ARRISGro_8c:59:c2 (f8:a0:97:8c:59:c2)

Source: IntelCor_ec:1f:4e (68:3e:26:ec:1f:4e)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 10.0.0.129, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 63019, Dst Port: 80, Seq: 1, Ack: 1, Len: 588

Hypertext Transfer Protocol

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

0x0800

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
71	4.827224	2620:1ec:42::132	2601:1c2:801:1e20:c...	TCP	74	443 → 63007 [FIN, ACK] Seq=1 Ack=2 Win=16381 Len=0
72	4.827370	2601:1c2:801:1e20:c...	2620:1ec:42::132	TCP	74	63007 → 443 [ACK] Seq=2 Ack=2 Win=514 Len=0
73	5.085609	10.0.0.129	128.119.245.12	TCP	66	63019 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
74	5.086330	10.0.0.129	128.119.245.12	TCP	66	63020 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
75	5.179350	128.119.245.12	10.0.0.129	TCP	66	80 → 63019 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
76	5.179477	10.0.0.129	128.119.245.12	TCP	54	63019 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
77	5.179822	10.0.0.129	128.119.245.12	HTTP	642	GET /wireshark-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
78	5.187103	128.119.245.12	10.0.0.129	TCP	66	80 → 63020 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM WS=128
79	5.187268	10.0.0.129	128.119.245.12	TCP	54	63020 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
80	5.280313	128.119.245.12	10.0.0.129	TCP	56	80 → 63019 [ACK] Seq=1 Ack=589 Win=30464 Len=0
81	5.282504	128.119.245.12	10.0.0.129	HTTP	295	HTTP/1.1 304 Not Modified
82	5.327935	10.0.0.129	128.119.245.12	TCP	54	63019 → 80 [ACK] Seq=589 Ack=242 Win=131072 Len=0
83	6.144262	fe80::faa0:97ff:fe8...	ff02::1	ICMPv6	174	Router Advertisement from f8:a0:97:8c:59:c2
84	7.203456	2407:30c0:182::aa72...	2601:1c2:801:1e20:c...	TCP	74	[TCP Dup ACK 44#1] 443 → 62114 [ACK] Seq=1 Ack=1 Win=8 Len=0
85	7.203530	2601:1c2:801:1e20:c...	2407:30c0:182::aa72...	TCP	74	[TCP Dup ACK 45#1] 62114 → 443 [ACK] Seq=1 Ack=2 Win=515 Len=0
86	8.090046	10.0.0.192	224.0.0.251	MDNS	415	Standard query response 0x0000 PTR, cache flush Katies-iPhone.local PTR, cache flush Katies-iPhone.local
87	8.090955	fe80::85b:8e4d:51b0...	ff02::fb	MDNS	435	Standard query response 0x0000 PTR, cache flush Katies-iPhone.local PTR, cache flush Katies-iPhone.local
88	8.192139	10.0.0.192	224.0.0.251	MDNS	181	Standard query 0x0000 PTR _companion-link_tcp.local, "QU" question PTR _homekit_tcp.local, "QU" question

> Frame 77: 642 bytes on wire (5136 bits), 642 bytes captured (5136 bits) on interface \Device\NPF_{CCDC22D-0101-426D-BAD9-134DD} Ethernet II, Src: IntelCor_ec:1f:4e (68:3e:26:ec:1f:4e), Dst: ARRISGro_8c:59:c2 (f8:a0:97:8c:59:c2)

> Destination: ARRISGro_8c:59:c2 (f8:a0:97:8c:59:c2)

> Source: IntelCor_ec:1f:4e (68:3e:26:ec:1f:4e)

Type: IPv4 (0x0800)

> Internet Protocol Version 4, Src: 10.0.0.129, Dst: 128.119.245.12

> Transmission Control Protocol, Src Port: 63019, Dst Port: 80, Seq: 1, Ack: 1, Len: 588

> Hypertext Transfer Protocol

0030 02 01 82 6b 00 00 47 45 54 20 2f 77 69 7a 7a
0040 68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 54 54
0050 74 68 65 72 65 61 6c 2d 6c 61 62 2d 66 6e 6e
0060 33 2e 68 74 6d 6c 20 48 54 54 50 2f 31 2f 31
0070 0a 48 6f 73 74 3a 20 67 61 69 61 2e 63 77 63
0080 6d 61 73 73 2e 65 64 75 0d 0a 43 6f 6e 6e 6e
0090 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 6e 6e
00a0 0d 0a 43 61 63 68 65 2d 43 6f 6e 74 72 6e 6e
00b0 20 6d 61 78 2d 61 67 65 3d 30 0d 0a 55 77 63
00c0 61 64 65 2d 49 6e 73 65 63 75 72 65 2d 55 77
00d0 75 65 73 74 73 3a 20 31 0d 0a 55 73 65 77 63
00e0 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 31
00f0 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 2f 31
0100 2e 30 3b 20 57 69 6e 36 34 3b 20 78 36 36 36
0110 41 70 70 6c 65 57 65 62 4b 69 74 2f 35 35 35
0120 33 36 20 28 4b 48 54 4d 4e 2f 20 6e 69 6e 6e

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” in “GET” appears 54 bytes into the frame

Wireshark packet capture showing an HTTP response from 10.0.0.129 to 10.0.0.192. The packet list shows a GET request for /wireshark-labs/HTTP-ethereal-lab-file3.html. The packet details show the request line and headers. The packet bytes show the raw data, with a red box highlighting the first 14 bytes of the HTTP response message (0000 f8 a0 97 8c 59 c2 68 3e 26 ec 1f 4e 08 00 45 00).

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

- 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?

Ethernet Source: f8:a0:97:8c:59:c2
This is the address of my router and is coming back to my computer.

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
238	9.974635	128.119.245.12	10.0.0.129	TCP	66	80 → 55005 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK
239	9.974748	10.0.0.129	128.119.245.12	TCP	54	55005 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
240	10.0327...	128.119.245.12	10.0.0.129	TCP	56	80 → 55004 [ACK] Seq=1 Ack=502 Win=30336 Len=0
241	10.0351...	128.119.245.12	10.0.0.129	TCP	1514	80 → 55004 [ACK] Seq=1 Ack=502 Win=30336 Len=1460 [TCP segment
242	10.0355...	128.119.245.12	10.0.0.129	TCP	1514	80 → 55004 [ACK] Seq=1461 Ack=502 Win=30336 Len=1460 [TCP segme
243	10.0356...	10.0.0.129	128.119.245.12	TCP	54	55004 → 80 [ACK] Seq=502 Ack=2921 Win=131328 Len=0
244	10.0366...	128.119.245.12	10.0.0.129	TCP	1514	80 → 55004 [ACK] Seq=2921 Ack=502 Win=30336 Len=1460 [TCP segme
245	10.0366...	128.119.245.12	10.0.0.129	HTTP	535	HTTP/1.1 200 OK (text/html)
246	10.0367...	10.0.0.129	128.119.245.12	TCP	54	55004 → 80 [ACK] Seq=502 Ack=4862 Win=131328 Len=0
247	11.5338...	10.0.0.129	128.119.245.12	TCP	54	55003 → 80 [FIN, ACK] Seq=1 Ack=1 Win=131328 Len=0
248	11.5339...	10.0.0.129	128.119.245.12	TCP	54	55005 → 80 [FIN, ACK] Seq=1 Ack=1 Win=131328 Len=0
249	11.5339...	10.0.0.129	128.119.245.12	TCP	54	55004 → 80 [FIN, ACK] Seq=502 Ack=4862 Win=131328 Len=0
250	11.5340...	2601:1c2:801:1e20:c...	2001:558:feed:443:...	TCP	74	54997 → 443 [FIN, ACK] Seq=1975 Ack=1755 Win=131584 Len=0
251	11.5341...	2601:1c2:801:1e20:c...	2607:f8b0:400a:806:...	TCP	74	54996 → 443 [FIN, ACK] Seq=1472 Ack=6696 Win=132352 Len=0
252	11.5342...	2601:1c2:801:1e20:c...	2607:f8b0:400a:80a:...	TCP	74	55002 → 443 [FIN, ACK] Seq=1646 Ack=2621 Win=131584 Len=0
253	11.5342...	2601:1c2:801:1e20:c...	2001:558:feed:443:...	TCP	74	55001 → 443 [FIN, ACK] Seq=1404 Ack=1083 Win=130816 Len=0
254	11.5580...	2607:f8b0:400a:806:...	2601:1c2:801:1e20:c...	TCP	74	443 → 54996 [FIN, ACK] Seq=6696 Ack=1473 Win=68096 Len=0
255	11.5580...	2607:f8b0:400a:80a:...	2601:1c2:801:1e20:c...	TCP	74	443 → 55002 [FIN, ACK] Seq=2621 Ack=1647 Win=70400 Len=0

> Frame 245: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface 0

Ethernet II, Src: ARRISGro_8c:59:c2 (f8:a0:97:8c:59:c2), Dst: IntelCor_ec:1f:4e (68:3e:26:ec:1f:4e)

Destination: IntelCor_ec:1f:4e (68:3e:26:ec:1f:4e)

Address: IntelCor_ec:1f:4e (68:3e:26:ec:1f:4e)

.....0..... = LG bit: Global

.....0..... = IG bit: Individual

Source: ARRISGro_8c:59:c2 (f8:a0:97:8c:59:c2)

Address: ARRISGro_8c:59:c2 (f8:a0:97:8c:59:c2)

.....0..... = LG bit: Global

.....0..... = IG bit: Individual

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.129

Transmission Control Protocol, Src Port: 80, Dst Port: 55004

[4 Reassembled TCP Segments (4861 bytes): #241(1460), #242(1460), #243(1460), #244(1460)]

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]

[HTTP/1.1 200 OK\r\n]

[Severity Level: Chat]

0000 68 3e 26 ec 1f 4e f8 a0 97 8c 59 c2 08 00 45 00 h>&.N...Y...E

0010 02 09 46 8b 40 00 21 06 91 5f 80 77 f5 0c 0a 00 ..F.@!...w....

0020 00 81 00 50 d6 dc cd 5a f1 6f c9 4b ea 48 50 18 ...P...Z-o.K-HP-

0030 00 ed c8 8c 00 00 68 6d 65 6e 74 73 20 69 6e 66hm ents inf

0040 6c 69 63 74 65 64 2e 0a 0a 3c 2f 70 3e 3c 70 3e licted...</p><p>

0050 3c 61 20 6e 61 6d 65 3d 22 39 22 3e 3c 73 74 72 <str

0060 6f 6e 67 3e 3c 68 33 3e 41 6d 65 6e 64 6d 65 6e ong><h3> Amendmen

0070 74 20 49 58 3c 2f 68 33 3e 3c 2f 73 74 72 6f 6e t IX</h3> ></stron

0080 67 3e 3c 2f 61 3e 0a 0a 3c 70 3e 3c 2f 70 3e 3c g>...<p></p><

0090 70 3e 54 68 65 20 65 6e 75 6d 65 72 61 74 69 6f p>The en umeratio

00a0 6e 20 69 6e 20 74 68 65 20 43 6f 6e 73 74 69 74 n in the Constit

00b0 75 74 69 6f 6e 2c 20 6f 66 20 63 65 72 74 61 69 tion, o f certai

00c0 6e 20 72 69 67 68 74 73 2c 20 73 68 61 6c 6c 0a n rights , shall-

00d0 6e 6f 74 20 62 65 20 63 6f 6e 73 74 72 75 65 64 not be c onstrued

00e0 20 74 6f 20 64 65 6e 79 20 6f 72 20 64 69 73 70 to deny or disp

00f0 61 72 61 67 65 20 6f 74 68 65 72 73 20 72 65 74 arage ot hers ret

0100 61 69 6e 65 64 20 62 79 20 74 68 65 20 70 65 6f ained by the peo

0110 70 6c 65 2e 0a 0a 3c 2f 70 3e 3c 70 3e 3c 61 20 ple...</ p><p><a

0120 6e 61 6d 65 3d 22 31 30 22 3e 3c 73 74 72 6f 6e name="10 "><stron

0130 67 3e 3c 68 33 3e 41 6d 65 6e 64 6d 65 6e 74 20 g<h3>Am endment

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

Yes, it's coming back to my computer. 68:3e:26:ec:1f:4e

The image shows a Wireshark packet capture analysis. The top pane displays a list of captured packets. The bottom pane shows the detailed view of a selected packet (No. 245).

No.	Time	Source	Destination	Protocol	Length	Info
238	9.974635	128.119.245.12	10.0.0.129	TCP	66	80 → 55005 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK
239	9.974748	10.0.0.129	128.119.245.12	TCP	54	55005 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
240	10.0327...	128.119.245.12	10.0.0.129	TCP	56	80 → 55004 [ACK] Seq=1 Ack=502 Win=30336 Len=0
241	10.0351...	128.119.245.12	10.0.0.129	TCP	1514	80 → 55004 [ACK] Seq=1 Ack=502 Win=30336 Len=1460 [TCP segment
242	10.0355...	128.119.245.12	10.0.0.129	TCP	1514	80 → 55004 [ACK] Seq=1461 Ack=502 Win=30336 Len=1460 [TCP segment
243	10.0356...	10.0.0.129	128.119.245.12	TCP	54	55004 → 80 [ACK] Seq=502 Ack=2921 Win=131328 Len=0
244	10.0366...	128.119.245.12	10.0.0.129	TCP	1514	80 → 55004 [ACK] Seq=2921 Ack=502 Win=30336 Len=1460 [TCP segment
245	10.0366...	128.119.245.12	10.0.0.129	HTTP	535	HTTP/1.1 200 OK (text/html)
246	10.0367...	10.0.0.129	128.119.245.12	TCP	54	55004 → 80 [ACK] Seq=502 Ack=4862 Win=131328 Len=0
247	11.5338...	10.0.0.129	128.119.245.12	TCP	54	55003 → 80 [FIN, ACK] Seq=1 Ack=1 Win=131328 Len=0
248	11.5339...	10.0.0.129	128.119.245.12	TCP	54	55005 → 80 [FIN, ACK] Seq=1 Ack=1 Win=131328 Len=0
249	11.5339...	10.0.0.129	128.119.245.12	TCP	54	55004 → 80 [FIN, ACK] Seq=502 Ack=4862 Win=131328 Len=0
250	11.5340...	2601:1c2:801:1e20:c...	2001:558:feed:443::...	TCP	74	54997 → 443 [FIN, ACK] Seq=1975 Ack=1755 Win=131584 Len=0
251	11.5341...	2601:1c2:801:1e20:c...	2607:f8b0:400a:806::...	TCP	74	54996 → 443 [FIN, ACK] Seq=1472 Ack=6696 Win=132352 Len=0
252	11.5342...	2601:1c2:801:1e20:c...	2607:f8b0:400a:80a::...	TCP	74	55002 → 443 [FIN, ACK] Seq=1646 Ack=2621 Win=131584 Len=0
253	11.5342...	2601:1c2:801:1e20:c...	2001:558:feed:443::...	TCP	74	55001 → 443 [FIN, ACK] Seq=1404 Ack=1083 Win=130816 Len=0
254	11.5580...	2607:f8b0:400a:806::...	2601:1c2:801:1e20:c...	TCP	74	443 → 54996 [FIN, ACK] Seq=6696 Ack=1473 Win=68096 Len=0
255	11.5580...	2607:f8b0:400a:80a::...	2601:1c2:801:1e20:c...	TCP	74	443 → 55002 [FIN, ACK] Seq=2621 Ack=1647 Win=70400 Len=0

The detailed view of packet 245 shows the following structure:

- Frame 245: 535 bytes on wire (4280 bits), 535 bytes captured (4...)
- Ethernet II, Src: ARRISGro_8c:59:c2 (f8:a0:97:8c:59:c2), Dst: IntelCor_ec:1f:4e (68:3e:26:ec:1f:4e)
 - Destination: IntelCor_ec:1f:4e (68:3e:26:ec:1f:4e)
 - Source: ARRISGro_8c:59:c2 (f8:a0:97:8c:59:c2)
 - Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.129
- Transmission Control Protocol, Src Port: 80, Dst Port: 55004, Seq: 502, Ack: 4862, Win: 131328, Len: 0
- [4 Reassembled TCP Segments (4861 bytes): #241(1460), #242(1460), #243(1460), #244(1460)]
- Hypertext Transfer Protocol
 - [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
 - [HTTP/1.1 200 OK\r\n]
 - [Sequence: Chat]

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

The Hex value is 0x0800, which corresponds to the IP protocol.

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
238	9.974635	128.119.245.12	10.0.0.129	TCP	66	80 → 55005 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK
239	9.974748	10.0.0.129	128.119.245.12	TCP	54	55005 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
240	10.0327...	128.119.245.12	10.0.0.129	TCP	56	80 → 55004 [ACK] Seq=1 Ack=502 Win=30336 Len=0
241	10.0351...	128.119.245.12	10.0.0.129	TCP	1514	80 → 55004 [ACK] Seq=1 Ack=502 Win=30336 Len=1460 [TCP segment
242	10.0355...	128.119.245.12	10.0.0.129	TCP	1514	80 → 55004 [ACK] Seq=1461 Ack=502 Win=30336 Len=1460 [TCP segme
243	10.0356...	10.0.0.129	128.119.245.12	TCP	54	55004 → 80 [ACK] Seq=502 Ack=2921 Win=131328 Len=0
244	10.0366...	128.119.245.12	10.0.0.129	TCP	1514	80 → 55004 [ACK] Seq=2921 Ack=502 Win=30336 Len=1460 [TCP segme
245	10.0366...	128.119.245.12	10.0.0.129	HTTP	535	HTTP/1.1 200 OK (text/html)
246	10.0367...	10.0.0.129	128.119.245.12	TCP	54	55004 → 80 [ACK] Seq=502 Ack=4862 Win=131328 Len=0
247	11.5338...	10.0.0.129	128.119.245.12	TCP	54	55003 → 80 [FIN, ACK] Seq=1 Ack=1 Win=131328 Len=0
248	11.5339...	10.0.0.129	128.119.245.12	TCP	54	55005 → 80 [FIN, ACK] Seq=1 Ack=1 Win=131328 Len=0
249	11.5339...	10.0.0.129	128.119.245.12	TCP	54	55004 → 80 [FIN, ACK] Seq=502 Ack=4862 Win=131328 Len=0
250	11.5340...	2601:1c2:801:1e20:c...	2001:558:feed:443::...	TCP	74	54997 → 443 [FIN, ACK] Seq=1975 Ack=1755 Win=131584 Len=0
251	11.5341...	2601:1c2:801:1e20:c...	2607:f8b0:400a:806::...	TCP	74	54996 → 443 [FIN, ACK] Seq=1472 Ack=6696 Win=132352 Len=0
252	11.5342...	2601:1c2:801:1e20:c...	2607:f8b0:400a:80a::...	TCP	74	55002 → 443 [FIN, ACK] Seq=1646 Ack=2621 Win=131584 Len=0
253	11.5342...	2601:1c2:801:1e20:c...	2001:558:feed:443::...	TCP	74	55001 → 443 [FIN, ACK] Seq=1404 Ack=1083 Win=130816 Len=0
254	11.5580...	2607:f8b0:400a:806::...	2601:1c2:801:1e20:c...	TCP	74	443 → 54996 [FIN, ACK] Seq=6696 Ack=1473 Win=68096 Len=0
255	11.5580...	2607:f8b0:400a:80a::...	2601:1c2:801:1e20:c...	TCP	74	443 → 55002 [FIN, ACK] Seq=2621 Ack=1647 Win=70400 Len=0

> Frame 245: 535 bytes on wire (4280 bits), 535 bytes captured (4...)

▼ Ethernet II, Src: ARRISGro_8c:59:c2 (f8:a0:97:8c:59:c2), Dst: IntelCor_ec:1f:4e (68:3e:26:ec:1f:4e)

- Destination: IntelCor_ec:1f:4e (68:3e:26:ec:1f:4e)
 - Address: IntelCor_ec:1f:4e (68:3e:26:ec:1f:4e)
 - = LG bit: Globally unique address
 - = IG bit: Individual address
- Source: ARRISGro_8c:59:c2 (f8:a0:97:8c:59:c2)
 - Address: ARRISGro_8c:59:c2 (f8:a0:97:8c:59:c2)
 - = LG bit: Globally unique address
 - = IG bit: Individual address

Type: IPv4 (0x0800)

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.1

> Transmission Control Protocol, Src Port: 80, Dst Port: 55004, Seq: 55004, Win: 131328, Len: 0

> [4 Reassembled TCP Segments (4861 bytes): #241(1460), #242(1460), #243(1460), #244(1460)]

▼ Hypertext Transfer Protocol

- HTTP/1.1 200 OK\r\n
 - [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
 - [HTTP/1.1 200 OK\r\n]

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?
- 42 bytes**

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
238	9.974635	128.119.245.12	10.0.0.129	TCP	66	80 → 55005 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK
239	9.974748	10.0.0.129	128.119.245.12	TCP	54	55005 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
240	10.0327...	128.119.245.12	10.0.0.129	TCP	56	80 → 55004 [ACK] Seq=1 Ack=502 Win=30336 Len=0
241	10.0351...	128.119.245.12	10.0.0.129	TCP	1514	80 → 55004 [ACK] Seq=1 Ack=502 Win=30336 Len=1460 [TCP segment
242	10.0355...	128.119.245.12	10.0.0.129	TCP	1514	80 → 55004 [ACK] Seq=1461 Ack=502 Win=30336 Len=1460 [TCP segme
243	10.0356...	10.0.0.129	128.119.245.12	TCP	54	55004 → 80 [ACK] Seq=502 Ack=2921 Win=131328 Len=0
244	10.0366...	128.119.245.12	10.0.0.129	TCP	1514	80 → 55004 [ACK] Seq=2921 Ack=502 Win=30336 Len=1460 [TCP segme
245	10.0366...	128.119.245.12	10.0.0.129	HTTP	535	HTTP/1.1 200 OK (text/html)
246	10.0367...	10.0.0.129	128.119.245.12	TCP	54	55004 → 80 [ACK] Seq=502 Ack=4862 Win=131328 Len=0
247	11.5338...	10.0.0.129	128.119.245.12	TCP	54	55003 → 80 [FIN, ACK] Seq=1 Ack=1 Win=131328 Len=0
248	11.5339...	10.0.0.129	128.119.245.12	TCP	54	55005 → 80 [FIN, ACK] Seq=1 Ack=1 Win=131328 Len=0
249	11.5339...	10.0.0.129	128.119.245.12	TCP	54	55004 → 80 [FIN, ACK] Seq=502 Ack=4862 Win=131328 Len=0
250	11.5340...	2601:1c2:801:1e20:c...	2001:558:feed:443::...	TCP	74	54997 → 443 [FIN, ACK] Seq=1975 Ack=1755 Win=131584 Len=0
251	11.5341...	2601:1c2:801:1e20:c...	2607:f8b0:400a:806::...	TCP	74	54996 → 443 [FIN, ACK] Seq=1472 Ack=6696 Win=132352 Len=0
252	11.5342...	2601:1c2:801:1e20:c...	2607:f8b0:400a:80a::...	TCP	74	55002 → 443 [FIN, ACK] Seq=1646 Ack=2621 Win=131584 Len=0
253	11.5342...	2601:1c2:801:1e20:c...	2001:558:feed:443::...	TCP	74	55001 → 443 [FIN, ACK] Seq=1404 Ack=1083 Win=130816 Len=0
254	11.5580...	2607:f8b0:400a:806::...	2601:1c2:801:1e20:c...	TCP	74	443 → 54996 [FIN, ACK] Seq=6696 Ack=1473 Win=68096 Len=0
255	11.5580...	2607:f8b0:400a:80a::...	2601:1c2:801:1e20:c...	TCP	74	443 → 55002 [FIN, ACK] Seq=2621 Ack=1647 Win=70400 Len=0

> Frame 245: 535 bytes on wire (4280 bits), 535 bytes captured (4280 bits) on interface 0

▼ Ethernet II, Src: ARRISGro_8c:59:c2 (f8:a0:97:8c:59:c2), Dst: IntelCor_ec:1f:4e (68:3e:26:ec:1f:4e)

▼ Destination: IntelCor_ec:1f:4e (68:3e:26:ec:1f:4e)

Address: IntelCor_ec:1f:4e (68:3e:26:ec:1f:4e)

.....0..... = LG bit: Globally unique address

.....0..... = IG bit: Individual address

▼ Source: ARRISGro_8c:59:c2 (f8:a0:97:8c:59:c2)

Address: ARRISGro_8c:59:c2 (f8:a0:97:8c:59:c2)

.....0..... = LG bit: Globally unique address

.....0..... = IG bit: Individual address

Type: IPv4 (0x0800)

> Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.129

▼ Transmission Control Protocol, Src Port: 80, Dst Port: 55004, Seq: 4381, Len: 481

Source Port: 80

Destination Port: 55004

[Stream index: 13]

[Conversation completeness: Complete, WITH_DATA (31)]

[TCP Segment Len: 481]

Sequence Number: 4381 (relative sequence number)

0000 68 3e 26 ec 1f 4e f8 a0 97 8c 59 c2 08 00 45 00 h>&...N...Y...

0010 02 09 46 8b 40 00 21 06 91 5f 80 77 f5 0c 0a 00 ..F.@!...w...

0020 00 81 00 50 d6 dc cd 5a f1 6f c9 4b ea 48 50 18 ...P...Z...K-H

0030 00 ed c8 8c 00 00 68 6d 65 6e 74 73 20 69 6e 66hm ents i

0040 6c 69 63 74 65 64 2a 0a 0a 3c 2f 70 3e 3c 70 3e listed </p><

0050 3c 61 20 6e 61 6d 65 3d 22 39 22 3e 3c 73 74 72 <s

0060 6f 6e 67 3e 3c 68 33 3e 41 6d 65 6e 64 6d 65 6e ong><h3> Amendm

0070 74 20 49 58 3c 2f 68 33 3e 3c 2f 73 74 72 6f 6e t IX</h3 ></str

0080 67 3e 3c 2f 61 3e 0a 0a 3c 70 3e 3c 2f 70 3e 3c g>... <p></p

0090 70 3e 54 68 65 20 65 6e 75 6d 65 72 61 74 69 6f p>The en umerat

00a0 6e 20 69 6e 20 74 68 65 20 43 6f 6e 73 74 69 74 n in the Const

00b0 75 74 69 6f 6e 2c 20 6f 66 20 63 65 72 74 61 69 ution, o f cert

00c0 6e 20 72 69 67 68 74 73 2c 20 73 68 61 6c 6c 0a n rights , shal

00d0 6e 6f 74 20 62 65 20 63 6f 6e 73 74 72 75 65 64 not be c onstru

00e0 20 74 6f 20 64 65 6e 79 20 6f 72 20 64 69 73 70 to deny or di

00f0 61 72 61 67 65 20 6f 74 68 65 72 73 20 72 65 74 arage ot hers r

0100 61 69 6e 65 64 20 62 79 20 74 68 65 20 70 65 6f ained by the p

0110 70 6c 65 2e 0a 0a 3c 2f 70 3e 3c 70 3e 3c 61 20 ple...</ p><p><

0120 6e 61 6d 65 3d 22 31 30 22 3e 3c 73 74 72 6f 6e names="10 "><str

0130 67 3e 3c 68 33 3e 41 6d 65 6e 64 6d 65 6e 74 20 g><h3>Am endm

2. The Address Resolution Protocol

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

IP address; Physical (MAC) address; The type of ARP entry (dynamic or static)

```
PS C:\windows\System32> .\arp -a

Interface: 10.0.0.129 --- 0xd
    Internet Address      Physical Address      Type
    10.0.0.1              f8-a0-97-8c-59-c2     dynamic
    10.0.0.225            f0-46-3b-13-72-27     dynamic
    10.0.0.255            ff-ff-ff-ff-ff-ff     static
    224.0.0.2              01-00-5e-00-00-02     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

Interface: 172.21.192.1 --- 0x2f
    Internet Address      Physical Address      Type
    172.21.193.82         00-15-5d-b3-08-21     dynamic
    172.21.207.255        ff-ff-ff-ff-ff-ff     static
    224.0.0.2              01-00-5e-00-00-02     static
    224.0.0.22            01-00-5e-00-00-16     static
    224.0.0.251           01-00-5e-00-00-fb     static
    239.255.255.250       01-00-5e-7f-ff-fa     static
PS C:\windows\System32> 
```

Observing ARP in action

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

Destination: ff:ff:ff:ff:ff:ff

Source: 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>

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
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
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
6	13.5429...	CnetTech_73:8d:ce	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
7	17.4444...	192.168.1.105	128.119.245.12	TCP	62	1058 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
8	17.4659...	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
9	17.4659...	192.168.1.105	128.119.245.12	TCP	54	1058 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10	17.4664...	192.168.1.105	128.119.245.12	HTTP	686	GET /ethereal-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
11	17.4947...	128.119.245.12	192.168.1.105	TCP	60	80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=0
12	17.4989...	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	17.5000...	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	17.5000...	192.168.1.105	128.119.245.12	TCP	54	1058 → 80 [ACK] Seq=633 Ack=2031 Win=64240 Len=0

[Coloring Rule Name: ARP]
[Coloring Rule String: arp]

▼ 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)
 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
 0010 08 00 06 04 00 01 00 d0 59 a9 3d 68 c0 a8
 0020 00 00 00 00 00 00 c0 a8 01 01

Destination Hardware Address (eth.dst), 6 bytes

Packets: 17 · Displayed: 17 (100.0%)

Profile: Default

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

0x0806. The upper layer protocol is ARP

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	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
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
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
6	13.5429...	CnetTech_73:8d:ce	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
7	17.4444...	192.168.1.105	128.119.245.12	TCP	62	1058 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
8	17.4659...	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
9	17.4659...	192.168.1.105	128.119.245.12	TCP	54	1058 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10	17.4664...	192.168.1.105	128.119.245.12	HTTP	686	GET /ethereal-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
11	17.4947...	128.119.245.12	192.168.1.105	TCP	60	80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=0
12	17.4989...	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	17.5000...	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	17.5000...	192.168.1.105	128.119.245.12	TCP	54	1058 → 80 [ACK] Seq=633 Ack=2021 Win=64240 Len=0

[Coloring Rule Name: ARP]
[Coloring Rule String: arp]

▼ 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)
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
0010 08 00 06 04 00 01 00 d0 59 a9 3d 68 c0 a8
0020 00 00 00 00 00 00 c0 a8 01 01

Destination Hardware Address (eth.dst), 6 bytes

Packets: 17 · Displayed: 17 (100.0%)

Profile: Default

12. Download the ARP specification from

<http://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?

20 bytes

ethernet-ethereal-trace-1

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	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
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
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
6	13.5429...	CnetTech_73:8d:ce	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
7	17.4444...	192.168.1.105	128.119.245.12	TCP	62	1058 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
8	17.4659...	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
9	17.4659...	192.168.1.105	128.119.245.12	TCP	54	1058 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10	17.4664...	192.168.1.105	128.119.245.12	HTTP	686	GET /ethereal-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
11	17.4947...	128.119.245.12	192.168.1.105	TCP	60	80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=0
12	17.4989...	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	17.5000...	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]

[Coloring Rule String: arp]

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

> 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)

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...i

0020 00 00 00 00 00 c0 a8 01 01

Opcode (arp.opcode), 2 bytes

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

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?

0x0001

ethernet-ethereal-trace-1

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	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
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
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
6	13.5429...	CnetTech_73:8d:ce	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
7	17.4444...	192.168.1.105	128.119.245.12	TCP	62	1058 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
8	17.4659...	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
9	17.4659...	192.168.1.105	128.119.245.12	TCP	54	1058 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10	17.4664...	192.168.1.105	128.119.245.12	HTTP	686	GET /ethereal-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
11	17.4947...	128.119.245.12	192.168.1.105	TCP	60	80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=0
12	17.4989...	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	17.5000...	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]

[Coloring Rule String: arp]

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

> 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)

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...i

0020 00 00 00 00 00 c0 a8 01 01

Opcode (arp.opcode), 2 bytes

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

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

Yes, it's 192.168.1.105

ethernet-ethereal-trace-1

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	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
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
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
6	13.5429...	CnetTech_73:8d:ce	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
7	17.4444...	192.168.1.105	128.119.245.12	TCP	62	1058 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
8	17.4659...	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
9	17.4659...	192.168.1.105	128.119.245.12	TCP	54	1058 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10	17.4664...	192.168.1.105	128.119.245.12	HTTP	686	GET /ethereal-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
11	17.4947...	128.119.245.12	192.168.1.105	TCP	60	80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=0
12	17.4989...	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	17.5000...	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]

[Coloring Rule String: arp]

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

Opcode (arp.opcode), 2 bytes

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

d) Where in the ARP request does the “question” appear – the Ethernet address of the machine whose corresponding IP address is being queried?
The target MAC address (00:00:00:00:00:00) queries the machine whose IP address is 192.168.1.105

ethernet-ethereal-trace-1

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	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
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
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
6	13.5429...	CnetTech_73:8d:ce	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
7	17.4444...	192.168.1.105	128.119.245.12	TCP	62	1058 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
8	17.4659...	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
9	17.4659...	192.168.1.105	128.119.245.12	TCP	54	1058 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10	17.4664...	192.168.1.105	128.119.245.12	HTTP	686	GET /ethereal-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
11	17.4947...	128.119.245.12	192.168.1.105	TCP	60	80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=0
12	17.4989...	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	17.5000...	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]

[Coloring Rule String: arp]

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

Target MAC address (arp.dst.hw_mac), 6 bytes

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

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?

20 bytes

Wireshark packet capture showing an ARP request. The packet list shows packet 4 as the first ARP request. The packet details pane shows the Ethernet II header and the ARP payload. The packet bytes pane shows the raw data of the packet, with a red box highlighting the first 20 bytes (0000 to 0010) which contain the Ethernet II header and the start of the ARP payload.

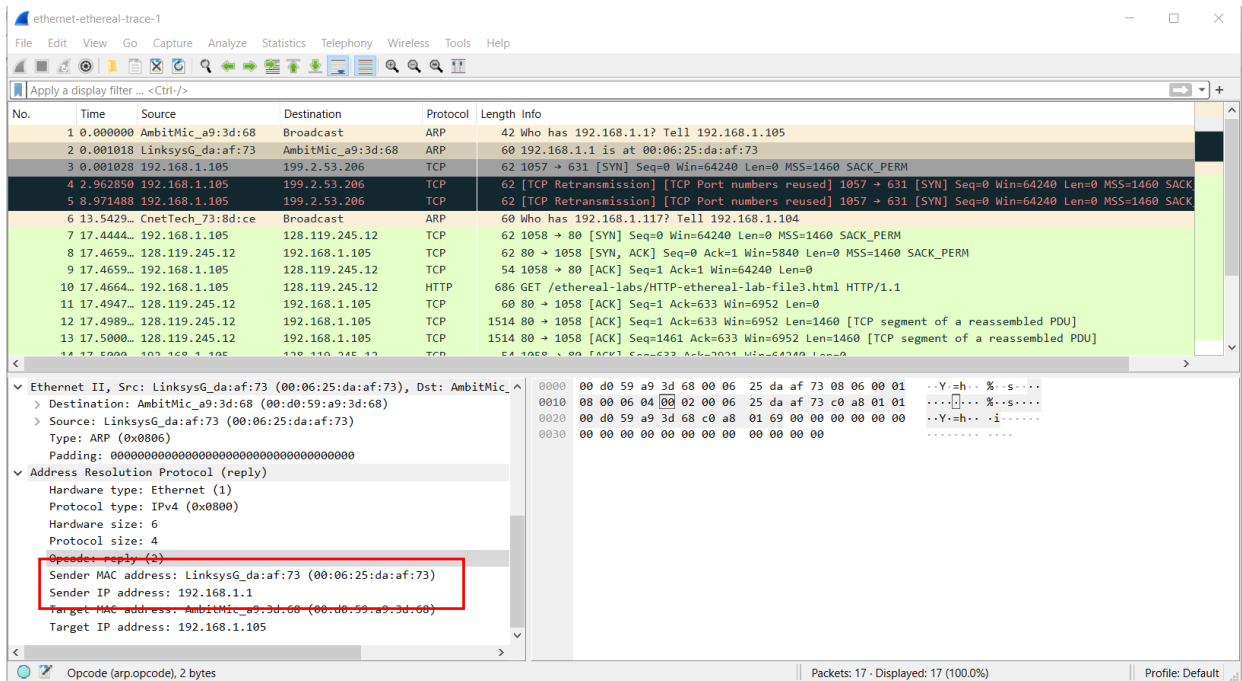
- b) What is the value of the *opcode* field within the ARP-payload part of the Ethernet frame in which an ARP response is made?

0x0002

Wireshark packet capture showing an ARP response. The packet list shows packet 6 as the first ARP response. The packet details pane shows the Ethernet II header and the ARP payload. The packet bytes pane shows the raw data of the packet, with a red box highlighting the opcode field (0002) in the ARP payload.

- 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?

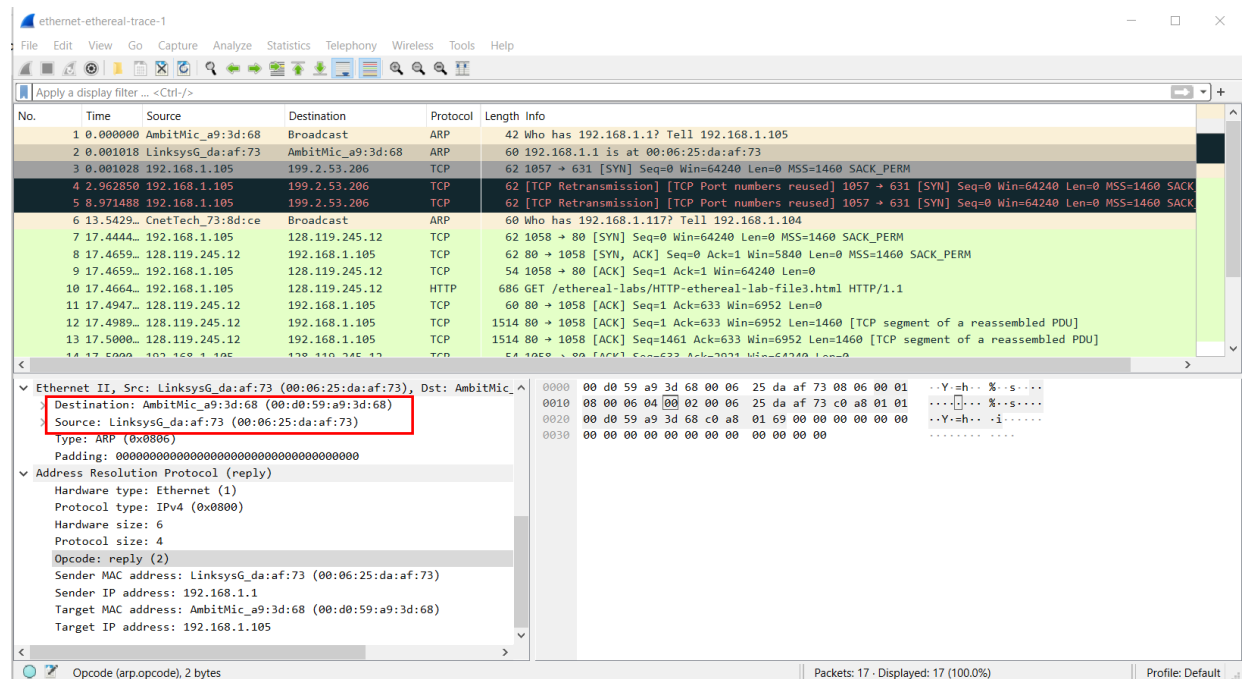
The sender IP address: 192.168.1.1 and Sender MAC address: 00:06:25:da:af:73 “answers” the earlier ARP request.



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

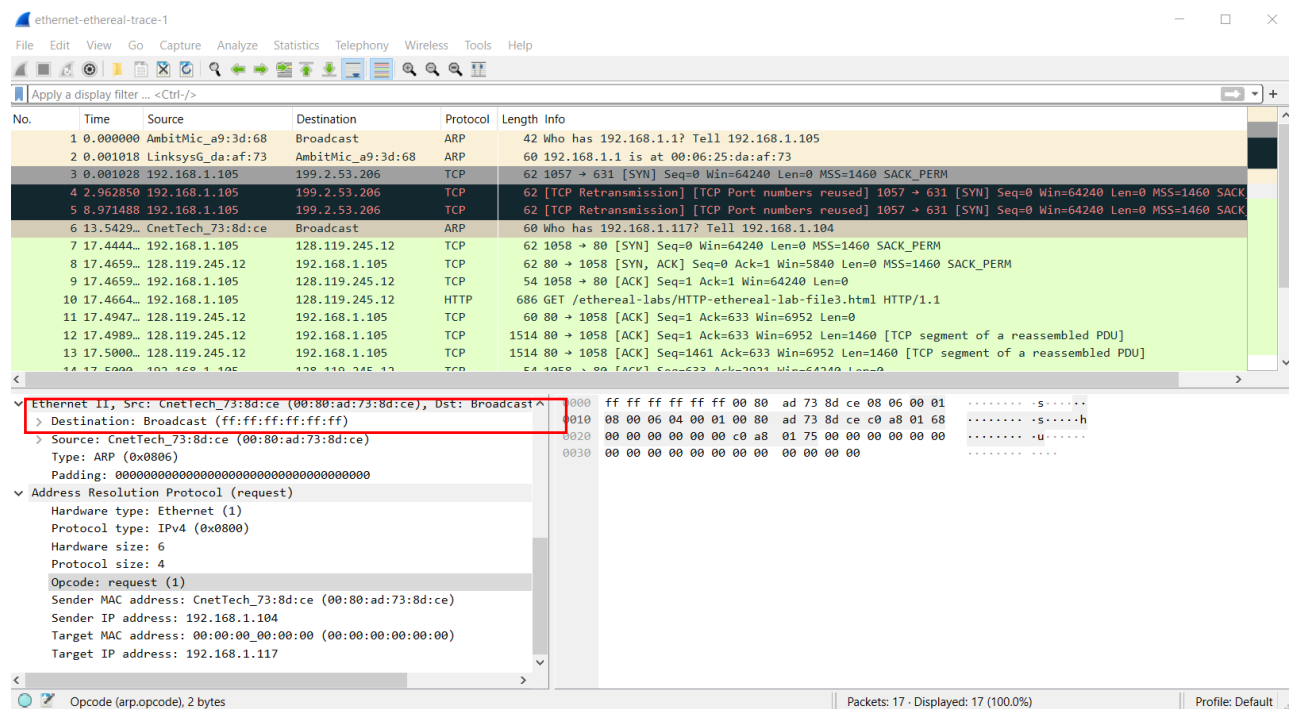
Source: 00:06:25:da:af:73

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



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 isn't an ARP reply in the packet trace because the ARP request is broadcast, and the ARP reply is not broadcast. The reply will be sent to the computer who made the request directly.



Extra Credit

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?

It will actually be ok, because when it contacts the router, the router will use ARP which will get back the correct address.

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.

20,500 ms

I found this by going to my command line, and finding the system32 directory. Then typing “.\netsh interface ipv4 show interfaces” This showed that interface #13 was my wifi, so then I typed “.\netsh interface ipv4 show interface 13” which gave me the following information, including the “Reachable Time” which gives me the amount of time that an entry remains in my ARP cache.

```
PS C:\windows\System32> .\netsh interface ipv4 show interface 13
```

Interface Wi-Fi Parameters

IfLuid	: wireless_32768
IfIndex	: 13
State	: connected
Metric	: 45
Link MTU	: 1500 bytes
Reachable Time	: 20500 ms
Base Reachable Time	: 30000 ms
Retransmission Interval	: 1000 ms
DAD Transmits	: 3
Site Prefix Length	: 64
Site Id	: 1
Forwarding	: disabled
Advertising	: disabled
Neighbor Discovery	: enabled
Neighbor Unreachability Detection	: enabled
Router Discovery	: dhcp
Managed Address Configuration	: enabled
Other Stateful Configuration	: enabled
Weak Host Sends	: disabled
Weak Host Receives	: disabled
Use Automatic Metric	: enabled
Ignore Default Routes	: disabled
Advertised Router Lifetime	: 1800 seconds
Advertise Default Route	: disabled
Current Hop Limit	: 0
Force ARPND Wake up patterns	: disabled
Directed MAC Wake up patterns	: disabled
ECN capability	: application