

CS372 Lab 5

Eric Rouse

1. 00:d0:59:a9:3d:68
2. 00:06:25:da:af:73. No, this is the first hop router.
3. 0x0800
4. 36 (it is the 37th byte)

The image shows a Wireshark packet capture of an Ethernet II frame, an Internet Protocol Version 4 packet, and a Hypertext Transfer Protocol (HTTP) GET request. The packet list shows 17 packets. The selected packet (No. 10) is a GET request to /etherreal-la. The packet details pane shows the request method, URI, and version. The packet bytes pane shows the raw data of the packet, with a yellow arrow pointing to the 43rd byte (0x2b) which is the first byte of the request body.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	AmbitMic_a...	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.105
2	0.001018	LinksysG_d...	AmbitMic_a...	ARP	60	192.168.1.1 is at 00:06:25:da:af:73
3	0.001028	192.168.1...	199.2.53.2...	TCP	62	1057-631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
4	2.962850	192.168.1...	199.2.53.2...	TCP	62	[TCP Retransmission] 1057-631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
5	8.971488	192.168.1...	199.2.53.2...	TCP	62	[TCP Retransmission] 1057-631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
6	13.542974	Telebit_73...	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
7	17.444423	192.168.1...	128.119.24...	TCP	62	1058-80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
8	17.465902	128.119.24...	192.168.1...	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...	128.119.24...	TCP	54	1058-80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10	17.466468	192.168.1...	128.119.24...	HTTP	686	GET /etherreal-la
11	17.494766	128.119.24...	192.168.1...	TCP	60	80-1058 [ACK] Seq=1 Ack=633 Win=6952 Len=0
12	17.498935	128.119.24...	192.168.1...	HTTP	1514	HTTP/1.1 200 OK
13	17.500025	128.119.24...	192.168.1...	TCP	1514	80-1058 [ACK] Seq=1461 Ack=633 Win=6952 Len=1460
14	17.500069	192.168.1...	128.119.24...	TCP	54	1058-80 [ACK] Seq=633 Ack=2921 Win=64240 Len=0
15	17.527857	128.119.24...	192.168.1...	TCP	1514	80-1058 [ACK] Seq=2921 Ack=633 Win=6952 Len=1460
16	17.527422	128.119.24...	192.168.1...	TCP	489	80-1058 [PSH, ACK] Seq=4381 Ack=633 Win=6952 Len=435
17	17.527457	192.168.1...	128.119.24...	TCP	54	1058-80 [ACK] Seq=633 Ack=4816 Win=64240 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: IP (0x0800)

Internet Protocol Version 4, Src: 192.168.1.105 (192.168.1.105), Dst: 128.119.245.12 (128.119.245.12)

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

Hypertext Transfer Protocol

GET /etherreal-la

[Expert Info (Chat/Sequence): GET /etherreal-la]

Request Method: GET

Request URI: /etherreal-la

Request Version:

<Request: True>

[HTTP request 1/1]

[Response in frame: 12]

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 00 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..GET/ether

0040 65 61 6c 2d 6c 61 62 73 2e 20 54 50 2d 65 74 eal-lab/HTTP-et

0050 68 65 72 65 61 6c 2d 6c 61 62 2d 66 69 6c 63 03 eal-lab-file3

0060 2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a .html HT IP/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 Ne

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/xhtml+

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=

0140 3d 30 2e 38 2c 76 69 64 65 6f 2f 78 2d 6d 6e 67 =0.8,vid eo/x-mng

0150 2c 69 6d 61 67 65 2f 70 6e 67 2c 69 6d 61 67 65 ,image/p ng,image

Expert Info (_ws.expert)

Packets: 17 · Displayed: 17 · Marked: 0 · Load time: 0:0.0

Profile: Default

5. 00:06:25:da:af:73. No, this is the "last" hop router.
6. 00:d0:59:a9:3d:68. Yes, this is the MAC address of the computer.
7. 0x800; IP
8. 43 (it is the 44th).

ethernet-ethereal-trace-1.pcapng

Apply a display filter ... <||/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	AmbitMic_a...	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.105
2	0.001018	LinksysG_d...	AmbitMic_a...	ARP	60	192.168.1.1 is at 00:06:25:da:af:73
3	0.001028	192.168.1...	199.2.53.2...	TCP	62	1057-631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
4	2.962850	192.168.1...	199.2.53.2...	TCP	62	[TCP Retransmission] 1057-631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
5	8.971488	192.168.1...	199.2.53.2...	TCP	62	[TCP Retransmission] 1057-631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
6	13.542974	Telebit_73...	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
7	17.444423	192.168.1...	128.119.24...	TCP	62	1058-80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
8	17.465902	128.119.24...	192.168.1...	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...	128.119.24...	TCP	54	1058-80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10	17.466468	192.168.1...	128.119.24...	HTTP	686	GET /ethereal-la
11	17.494766	128.119.24...	192.168.1...	TCP	60	80-1058 [ACK] Seq=1 Ack=633 Win=6952 Len=0
12	17.498935	128.119.24...	192.168.1...	HTTP	1514	HTTP/1.1 200 OK\r
13	17.500025	128.119.24...	192.168.1...	TCP	1514	80-1058 [ACK] Seq=1461 Ack=633 Win=6952 Len=1460
14	17.500069	192.168.1...	128.119.24...	TCP	54	1058-80 [ACK] Seq=633 Ack=2921 Win=64240 Len=0
15	17.527057	128.119.24...	192.168.1...	TCP	1514	80-1058 [ACK] Seq=2921 Ack=633 Win=6952 Len=1460
16	17.527422	128.119.24...	192.168.1...	TCP	489	80-1058 [PSH, ACK] Seq=4381 Ack=633 Win=6952 Len=435
17	17.527457	192.168.1...	128.119.24...	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: IP (0x0800)

Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.1.105 (192.168.1.105)

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

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

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

Request Version: HTTP/1.1

Status Code: 200

Response Phrase: OK\r

Date: Sat, 28 Aug

<Date: Sat, 28 Aug>

<Response: True>

[HTTP response 1/1]

[Time since request: 0.032467000 seconds]

[Request in frame: 10]

Data (1426 bytes)

0000 00 d0 59 a9 3d 68 00 06 25 da af 73 08 00 45 60 ..Y.=h..%.s..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 20 4f 1b 00 0a 44 61 74 65 3a 20 53 61 74 00 OK.D ate: Sat

0050 2c 20 32 38 20 75 67 20 32 30 30 34 20 31 37 , 28 Aug 2004 17

0060 3a 31 39 3a 33 37 20 47 74 65 0d 0a 53 65 72 76 :19:37 GMT..Serv

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

0080 30 20 28 52 65 64 20 48 61 74 20 4c 69 6e 75 70 0 (Red Hat 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 6f 20 32 30 : Sat, 28 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 3a 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 6e 65 63 max=100 ..Connec

0130 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 tion: Ke ep-Alive

0140 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 ..Conten t-Type:

0150 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 text/htm l; chars

HTTP Response Reason Phrase (http.response.reason.phrase), 3 bytes

Packets: 17 · Displayed: 17 · Marked: 0 · Load time: 0:0.0

Profile: Default

```
1. zsh
[~/Documents/CS372/lab5]
> arp -a                                erouse@Eric-MBP[16:36]
router.asus.com (10.0.66.1) at 40:16:7e:5b:f4:88 on en0 ifscope [ethernet]
eric-mbp (10.0.66.38) at 3c:15:c2:e2:80:2e on en0 ifscope permanent [ethernet]
? (10.0.66.255) at ff:ff:ff:ff:ff:ff on en0 ifscope [ethernet]
[~/Documents/CS372/lab5]
> []                                erouse@Eric-MBP[16:36]
```

10. source: 00:80:ad:73:8d:ce. Destination ff:ff:ff:ff:ff:ff
11. 0x0806, type is ARP
12. a. 24 b. 1 for request c. yes d. Target HA octet.
13. a. 20 b. 2 for reply c. target IP
14. Source: 00:06:25:da:af:73 Dest: 00:d0:59:a9:3d:68
15. There is no ARP reply because the packet is intended for 192.168.1.104, which is not the host computer. Therefore, no ARP reply will be given from 192.168.1.105, and would not show up on the Wireshark trace. That is why the first two packets are a request and a reply as opposed to just a request.