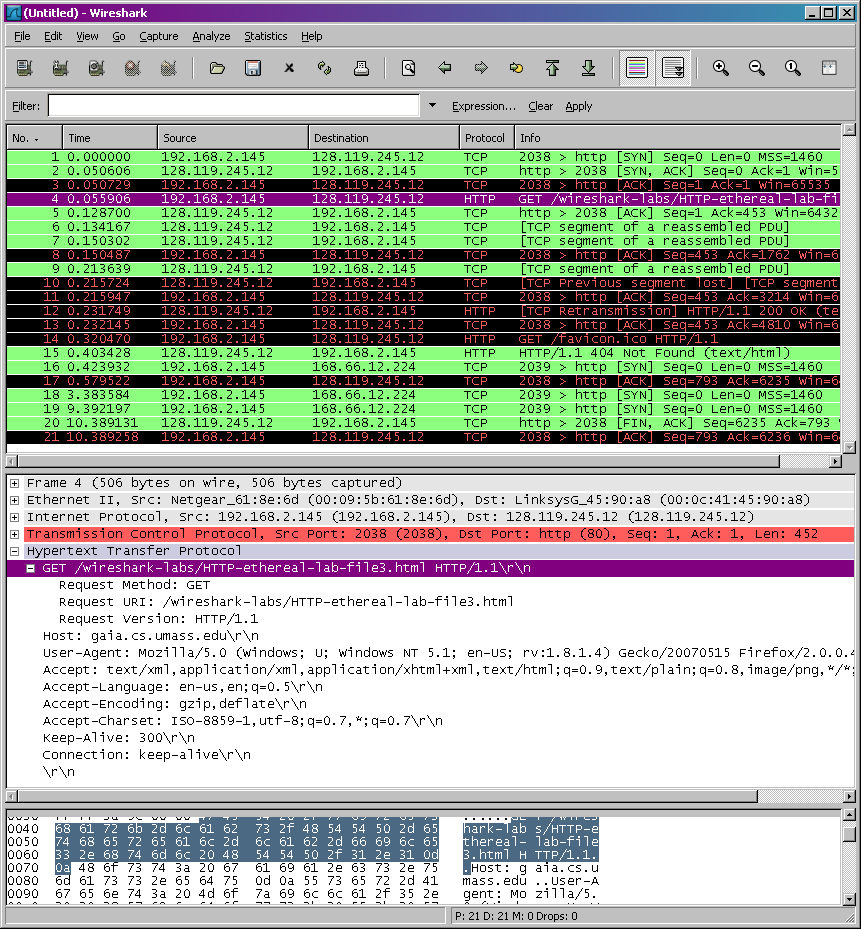
|  |  |
| --- | --- |
| Wireshark Lab: Ethernet and ARP v7.0  Supplement to *Computer Networking: A Top-Down Approach, 7th ed.,* J.F. Kurose and K.W. Ross  *“Tell me and I forget. Show me and I remember. Involve me and I understand.”* Chinese proverb  © 2005-2016 J.F Kurose and K.W. Ross, All Rights Reserved | *kurose7e_cover_small* |

In this lab, we’ll investigate the Ethernet protocol and the ARP protocol. Before beginning this lab, you’ll probably want to review sections 6.4.1 (Link-layer addressing and ARP) and 6.4.2 (Ethernet) in the text[[1]](#footnote-1). RFC 826 (<ftp://ftp.rfc-editor.org/in-notes/std/std37.txt>) contains the gory details of the ARP protocol, which is used by an IP device to determine the IP address of a remote interface whose Ethernet address is known.

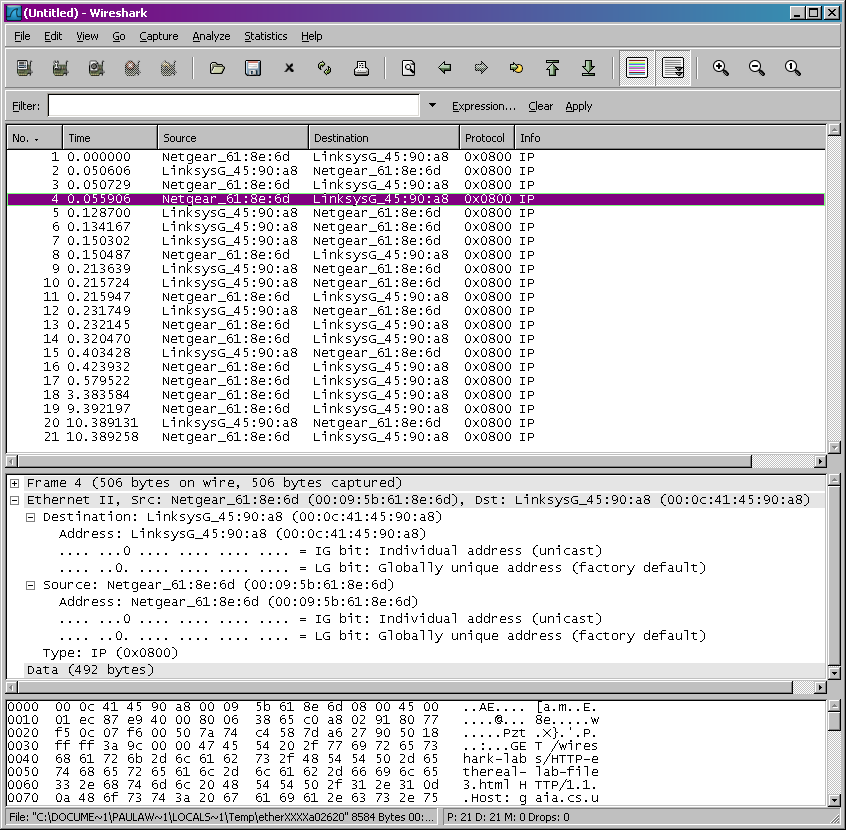
1. Capturing and analyzing Ethernet frames

Let’s begin by capturing a set of Ethernet frames to study. Do the following[[2]](#footnote-2):

* First, make sure your browser’s cache is empty. To do this under Mozilla Firefox V3, select *Tools->Clear Recent History* and check the box for Cache. For Internet Explorer, select *Tools->Internet Options->Delete Files.* Start up the Wireshark packet sniffer
* Enter the following URL into your browser  
  http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html  
  Your browser should display the rather lengthy US Bill of Rights.
* Stop Wireshark packet capture. First, find the packet numbers (the leftmost column in the upper Wireshark window) of the HTTP GET message that was sent from your computer to gaia.cs.umass.edu, as well as the beginning of the HTTP response message sent to your computer by gaia.cs.umass.edu. You should see a screen that looks something like this (where packet 4 in the screen shot below contains the HTTP GET message)



* Since this lab is about Ethernet and ARP, we’re not interested in IP or higher-layer protocols. So let’s change Wireshark’s “listing of captured packets” window so that it shows information only about protocols below IP. To have Wireshark do this, select *Analyze->Enabled Protocols.* Then uncheck the IP box and select *OK*. You should now see an Wireshark window that looks like:



In order to answer the following questions, you’ll need to look into the packet details and packet contents windows (the middle and lower display windows in Wireshark).

Select the Ethernet frame containing the HTTP GET message. (Recall that the HTTP GET message is carried inside of a TCP segment, which is carried inside of an IP datagram, which is carried inside of an Ethernet frame; reread section 1.5.2 in the text if you find this encapsulation a bit confusing). Expand the Ethernet II information in the packet details window. Note that the contents of the Ethernet frame (header as well as payload) are displayed in the packet contents window.

Answer the following questions, based on the contents of the Ethernet frame containing the HTTP GET message. Whenever possible, when answering a question you should hand in a printout of the packet(s) within the trace that you used to answer the question asked. Annotate the printout[[3]](#footnote-3) to explain your answer. To print a packet, use *File->Print*, choose *Selected packet only*, choose *Packet summary line,* and select the minimum amount of packet detail that you need to answer the question.

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

d4:3d:7e:bd:70:f5

1. 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.]

00:af:1f:78:dc:43

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

0x0800, IPv4

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

1. 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?

00:af:1f:78:dc:43

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

d4:3d:7e:bd:70:f5

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

0x0800, IPv4

Raw packets: GET req.

0000 d4 3d 7e bd 70 f5 00 af 1f 78 dc 43 08 00 45 00

0010 00 74 68 a9 00 00 31 11 64 3d ac 62 c1 2a c0 a8

0020 8e 5d 00 35 c3 e7 00 60 29 69 f6 4c 81 80 00 01

0030 00 00 00 01 00 00 04 67 61 69 61 02 63 73 05 75

0040 6d 61 73 73 03 65 64 75 00 00 1c 00 01 c0 11 00

0050 06 00 01 00 00 0e 10 00 29 05 75 6e 69 78 31 c0

0060 11 0a 68 6f 73 74 6d 61 73 74 65 72 c0 11 78 59

0070 36 99 00 00 46 50 00 00 0e 10 00 04 9d 40 00 01

0080 51 80

Response:

0000 d4 3d 7e bd 70 f5 00 af 1f 78 dc 43 08 00 45 00

0010 05 8c 9b 80 40 00 2b 06 ea 61 80 77 f5 0c c0 a8

0020 8e 5d 00 50 07 de 32 a1 78 33 f6 0d 2b 9c 50 10

0030 00 ed 09 22 00 00 48 54 54 50 2f 31 2e 31 20 32

0040 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 54 75 65

0050 2c 20 30 33 20 44 65 63 20 32 30 31 39 20 32 33

0060 3a 35 31 3a 31 33 20 47 4d 54 0d 0a 53 65 72 76

0070 65 72 3a 20 41 70 61 63 68 65 2f 32 2e 34 2e 36

0080 20 28 43 65 6e 74 4f 53 29 20 4f 70 65 6e 53 53

0090 4c 2f 31 2e 30 2e 32 6b 2d 66 69 70 73 20 50 48

00a0 50 2f 35 2e 34 2e 31 36 20 6d 6f 64 5f 70 65 72

00b0 6c 2f 32 2e 30 2e 31 31 20 50 65 72 6c 2f 76 35

00c0 2e 31 36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69

00d0 66 69 65 64 3a 20 54 75 65 2c 20 30 33 20 44 65

00e0 63 20 32 30 31 39 20 30 36 3a 35 39 3a 30 32 20

00f0 47 4d 54 0d 0a 45 54 61 67 3a 20 22 31 31 39 34

0100 2d 35 39 38 63 37 33 62 33 36 36 30 33 30 22 0d

0110 0a 41 63 63 65 70 74 2d 52 61 6e 67 65 73 3a 20

0120 62 79 74 65 73 0d 0a 43 6f 6e 74 65 6e 74 2d 4c

0130 65 6e 67 74 68 3a 20 34 35 30 30 0d 0a 4b 65 65

0140 70 2d 41 6c 69 76 65 3a 20 74 69 6d 65 6f 75 74

0150 3d 35 2c 20 6d 61 78 3d 31 30 30 0d 0a 43 6f 6e

0160 6e 65 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c

0170 69 76 65 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70

0180 65 3a 20 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68

0190 61 72 73 65 74 3d 55 54 46 2d 38 0d 0a 0d 0a 3c

01a0 68 74 6d 6c 3e 3c 68 65 61 64 3e 20 0a 3c 74 69

01b0 74 6c 65 3e 48 69 73 74 6f 72 69 63 61 6c 20 44

01c0 6f 63 75 6d 65 6e 74 73 3a 54 48 45 20 42 49 4c

01d0 4c 20 4f 46 20 52 49 47 48 54 53 3c 2f 74 69 74

01e0 6c 65 3e 3c 2f 68 65 61 64 3e 0a 0a 0a 3c 62 6f

01f0 64 79 20 62 67 63 6f 6c 6f 72 3d 22 23 66 66 66

0200 66 66 66 22 20 6c 69 6e 6b 3d 22 23 33 33 30 30

0210 30 30 22 20 76 6c 69 6e 6b 3d 22 23 36 36 36 36

0220 33 33 22 3e 0a 3c 70 3e 3c 62 72 3e 0a 3c 2f 70

0230 3e 0a 3c 70 3e 3c 2f 70 3e 3c 63 65 6e 74 65 72

0240 3e 3c 62 3e 54 48 45 20 42 49 4c 4c 20 4f 46 20

0250 52 49 47 48 54 53 3c 2f 62 3e 3c 62 72 3e 0a 20

0260 20 3c 65 6d 3e 41 6d 65 6e 64 6d 65 6e 74 73 20

0270 31 2d 31 30 20 6f 66 20 74 68 65 20 43 6f 6e 73

0280 74 69 74 75 74 69 6f 6e 3c 2f 65 6d 3e 0a 3c 2f

0290 63 65 6e 74 65 72 3e 0a 0a 3c 70 3e 54 68 65 20

02a0 43 6f 6e 76 65 6e 74 69 6f 6e 73 20 6f 66 20 61

02b0 20 6e 75 6d 62 65 72 20 6f 66 20 74 68 65 20 53

02c0 74 61 74 65 73 20 68 61 76 69 6e 67 2c 20 61 74

02d0 20 74 68 65 20 74 69 6d 65 20 6f 66 20 61 64 6f

02e0 70 74 69 6e 67 0a 74 68 65 20 43 6f 6e 73 74 69

02f0 74 75 74 69 6f 6e 2c 20 65 78 70 72 65 73 73 65

0300 64 20 61 20 64 65 73 69 72 65 2c 20 69 6e 20 6f

0310 72 64 65 72 20 74 6f 20 70 72 65 76 65 6e 74 20

0320 6d 69 73 63 6f 6e 73 74 72 75 63 74 69 6f 6e 0a

0330 6f 72 20 61 62 75 73 65 20 6f 66 20 69 74 73 20

0340 70 6f 77 65 72 73 2c 20 74 68 61 74 20 66 75 72

0350 74 68 65 72 20 64 65 63 6c 61 72 61 74 6f 72 79

0360 20 61 6e 64 20 72 65 73 74 72 69 63 74 69 76 65

0370 20 63 6c 61 75 73 65 73 0a 73 68 6f 75 6c 64 20

0380 62 65 20 61 64 64 65 64 2c 20 61 6e 64 20 61 73

0390 20 65 78 74 65 6e 64 69 6e 67 20 74 68 65 20 67

03a0 72 6f 75 6e 64 20 6f 66 20 70 75 62 6c 69 63 20

03b0 63 6f 6e 66 69 64 65 6e 63 65 20 69 6e 20 74 68

03c0 65 0a 47 6f 76 65 72 6e 6d 65 6e 74 20 77 69 6c

03d0 6c 20 62 65 73 74 20 69 6e 73 75 72 65 20 74 68

03e0 65 20 62 65 6e 65 66 69 63 65 6e 74 20 65 6e 64

03f0 73 20 6f 66 20 69 74 73 20 69 6e 73 74 69 74 75

0400 74 69 6f 6e 3b 20 3c 2f 70 3e 3c 70 3e 20 20 52

0410 65 73 6f 6c 76 65 64 2c 20 62 79 20 74 68 65 20

0420 53 65 6e 61 74 65 20 61 6e 64 20 48 6f 75 73 65

0430 20 6f 66 20 52 65 70 72 65 73 65 6e 74 61 74 69

0440 76 65 73 20 6f 66 20 74 68 65 20 55 6e 69 74 65

0450 64 0a 53 74 61 74 65 73 20 6f 66 20 41 6d 65 72

0460 69 63 61 2c 20 69 6e 20 43 6f 6e 67 72 65 73 73

0470 20 61 73 73 65 6d 62 6c 65 64 2c 20 74 77 6f 2d

0480 74 68 69 72 64 73 20 6f 66 20 62 6f 74 68 20 48

0490 6f 75 73 65 73 20 63 6f 6e 63 75 72 72 69 6e 67

04a0 2c 0a 74 68 61 74 20 74 68 65 20 66 6f 6c 6c 6f

04b0 77 69 6e 67 20 61 72 74 69 63 6c 65 73 20 62 65

04c0 20 70 72 6f 70 6f 73 65 64 20 74 6f 20 74 68 65

04d0 20 4c 65 67 69 73 6c 61 74 75 72 65 73 20 6f 66

04e0 20 74 68 65 20 73 65 76 65 72 61 6c 0a 53 74 61

04f0 74 65 73 2c 20 61 73 20 61 6d 65 6e 64 6d 65 6e

0500 74 73 20 74 6f 20 74 68 65 20 43 6f 6e 73 74 69

0510 74 75 74 69 6f 6e 20 6f 66 20 74 68 65 20 55 6e

0520 69 74 65 64 20 53 74 61 74 65 73 3b 20 61 6c 6c

0530 20 6f 72 20 61 6e 79 0a 6f 66 20 77 68 69 63 68

0540 20 61 72 74 69 63 6c 65 73 2c 20 77 68 65 6e 20

0550 72 61 74 69 66 69 65 64 20 62 79 20 74 68 72 65

0560 65 2d 66 6f 75 72 74 68 73 20 6f 66 20 74 68 65

0570 20 73 61 69 64 20 4c 65 67 69 73 6c 61 74 75 72

0580 65 73 2c 0a 74 6f 20 62 65 20 76 61 6c 69 64 20

0590 74 6f 20 61 6c 6c 20 69 6e 74

1. References to figures and sections are for the 7th edition of our text, *Computer Networks, A Top-down Approach, 7th ed.,* J.F. Kurose and K.W. Ross, Addison-Wesley/Pearson, 2016. [↑](#footnote-ref-1)
2. If you are unable to run Wireshark live on a computer, you can download the zip file [http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip](http://gaia.cs.umass.edu/ethereal-labs/ethereal-traces.zip) and extract the file *ethernet--ethereal-trace-1*. The traces in this zip file were collected by Wireshark running on one of the author’s computers, while performing the steps indicated in the Wireshark lab. Once you have downloaded the trace, you can load it into Wireshark and view the trace using the *File* pull down menu, choosing *Open*, and then selecting the ethernet-ethereal-trace-1 trace file. You can then use this trace file to answer the questions below. [↑](#footnote-ref-2)
3. What do we mean by “annotate”? If you hand in a paper copy, please highlight where in the printout you’ve found the answer and add some text (preferably with a colored pen) noting what you found in what you ‘ve highlight. If you hand in an electronic copy, it would be great if you could also highlight and annotate. [↑](#footnote-ref-3)