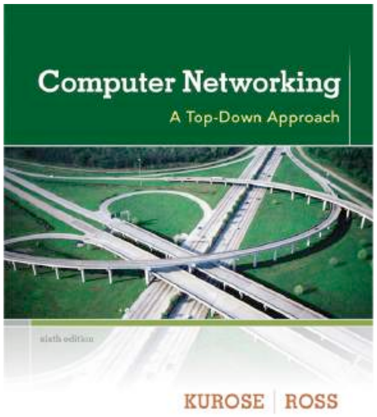
Wireshark Lab: Ethernet and ARP v6.01



Supplement to *Computer Networking: A Top-Down Approach, 6th 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

---

In this lab, we'll investigate the Ethernet protocol ~~and the ARP protocol~~. Before beginning this lab, you'll probably want to review sections 5.4.1 (link-layer addressing ~~and ARP~~) and 5.4.2 (Ethernet) in the text[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]:

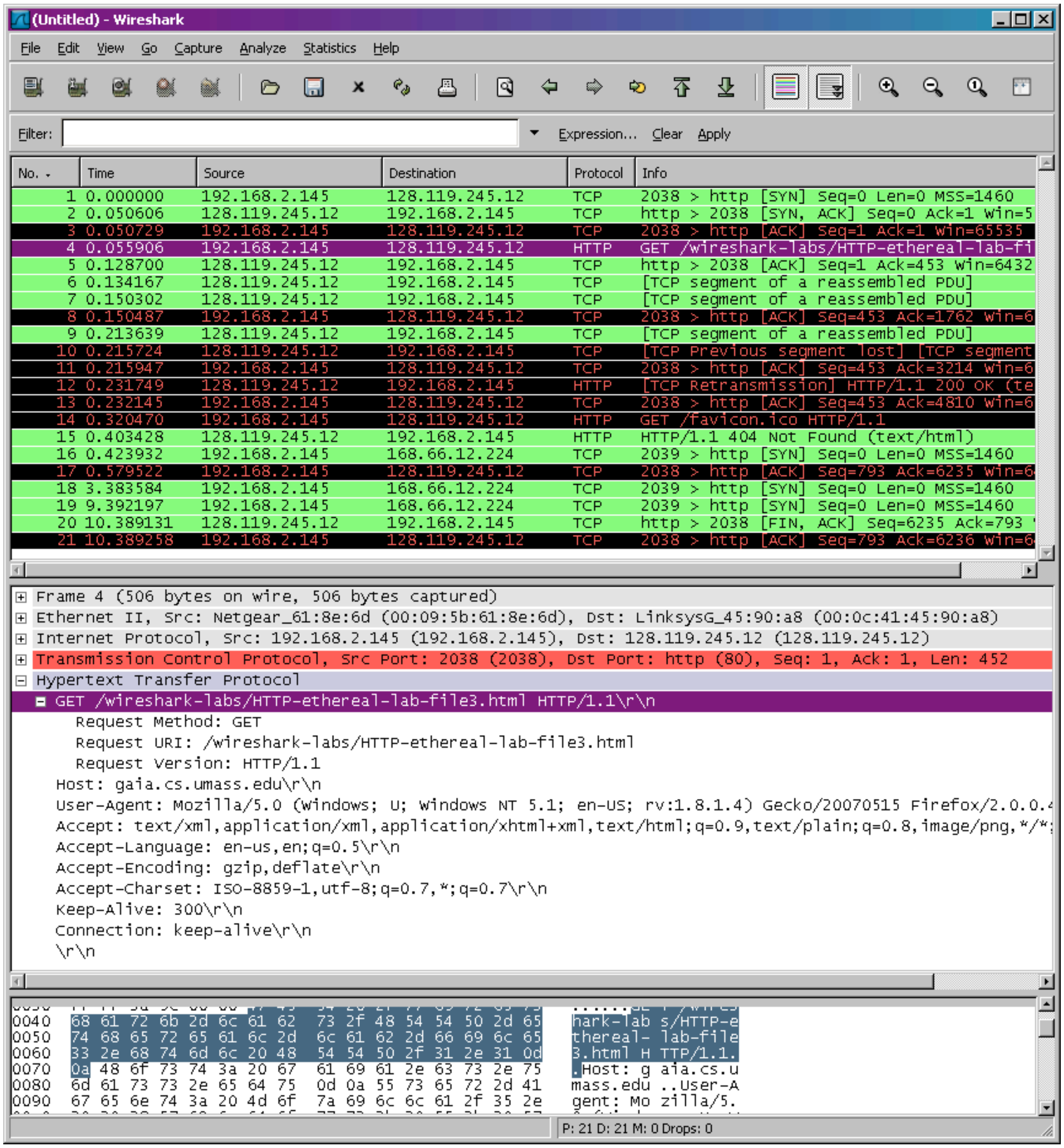
- First, make sure your browser's cache is empty. To do this under Mozilla Firefox V3, select *Tools->Clear Recent History* and check the box for Cache. For Internet Explorer, select *Tools->Internet Options->Delete Files.* Start up the Wireshark packet sniffer
- Enter the following URL into your browser
  http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html
  Your browser should display the rather lengthy US Bill of Rights.

---

[1] References to figures and sections are for the 6th edition of our text, *Computer Networks, A Top-down Approach, 6th ed.,* J.F. Kurose and K.W. Ross, Addison-Wesley/Pearson, 2012.

[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 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.

- 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)



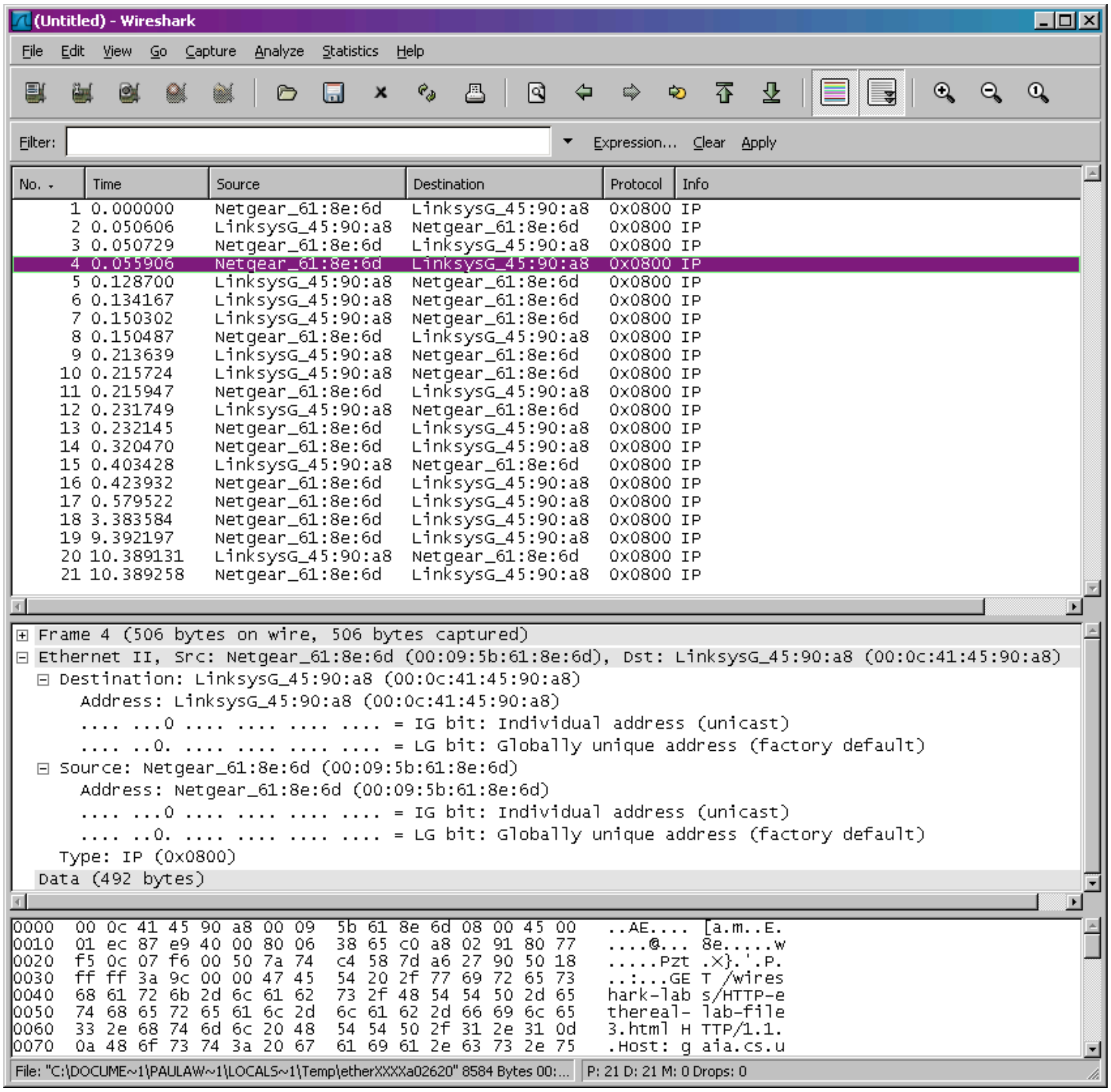
```
No. -  Time       Source           Destination      Protocol  Info
     1 0.000000   192.168.2.145    128.119.245.12   TCP       2038 > http [SYN] Seq=0 Len=0 MSS=1460
     2 0.050606   128.119.245.12   192.168.2.145    TCP       http > 2038 [SYN, ACK] Seq=0 Ack=1 Win=5
     3 0.050729   192.168.2.145    128.119.245.12   TCP       2038 > http [ACK] Seq=1 Ack=1 Win=65535
     4 0.055906   192.168.2.145    128.119.245.12   HTTP      GET /wireshark-labs/HTTP-ethereal-lab-fi
     5 0.128700   128.119.245.12   192.168.2.145    TCP       http > 2038 [ACK] Seq=1 Ack=453 Win=6432
     6 0.134167   128.119.245.12   192.168.2.145    TCP       [TCP segment of a reassembled PDU]
     7 0.150302   128.119.245.12   192.168.2.145    TCP       [TCP segment of a reassembled PDU]
     8 0.150487   192.168.2.145    128.119.245.12   TCP       2038 > http [ACK] Seq=453 Ack=1762 Win=6
     9 0.213639   128.119.245.12   192.168.2.145    TCP       [TCP segment of a reassembled PDU]
    10 0.215724   128.119.245.12   192.168.2.145    TCP       [TCP Previous segment lost] [TCP segment
    11 0.215947   192.168.2.145    128.119.245.12   TCP       2038 > http [ACK] Seq=453 Ack=3214 Win=6
    12 0.231749   128.119.245.12   192.168.2.145    HTTP      [TCP Retransmission] HTTP/1.1 200 OK (te
    13 0.232145   192.168.2.145    128.119.245.12   TCP       2038 > http [ACK] Seq=453 Ack=4810 Win=6
    14 0.320470   192.168.2.145    128.119.245.12   HTTP      GET /favicon.ico HTTP/1.1
    15 0.403428   128.119.245.12   192.168.2.145    HTTP      HTTP/1.1 404 Not Found (text/html)
    16 0.423932   192.168.2.145    168.66.12.224    TCP       2039 > http [SYN] Seq=0 Len=0 MSS=1460
    17 0.579522   192.168.2.145    128.119.245.12   TCP       2038 > http [ACK] Seq=793 Ack=6235 Win=6
    18 3.383584   192.168.2.145    168.66.12.224    TCP       2039 > http [SYN] Seq=0 Len=0 MSS=1460
    19 9.392197   192.168.2.145    168.66.12.224    TCP       2039 > http [SYN] Seq=0 Len=0 MSS=1460
    20 10.389131  128.119.245.12   192.168.2.145    TCP       http > 2038 [FIN, ACK] Seq=6235 Ack=793 
    21 10.389258  192.168.2.145    128.119.245.12   TCP       2038 > http [ACK] Seq=793 Ack=6236 Win=6
```

```
⊞ Frame 4 (506 bytes on wire, 506 bytes captured)
⊞ Ethernet II, Src: Netgear_61:8e:6d (00:09:5b:61:8e:6d), Dst: LinksysG_45:90:a8 (00:0c:41:45:90:a8)
⊞ Internet Protocol, Src: 192.168.2.145 (192.168.2.145), Dst: 128.119.245.12 (128.119.245.12)
⊞ Transmission Control Protocol, Src Port: 2038 (2038), Dst Port: http (80), Seq: 1, Ack: 1, Len: 452
⊟ Hypertext Transfer Protocol
  ⊟ GET /wireshark-labs/HTTP-ethereal-lab-file3.html HTTP/1.1\r\n
      Request Method: GET
      Request URI: /wireshark-labs/HTTP-ethereal-lab-file3.html
      Request Version: HTTP/1.1
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.4) Gecko/20070515 Firefox/2.0.0.
    Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n
    Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
    Keep-Alive: 300\r\n
    Connection: keep-alive\r\n
    \r\n
```

```
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 65   hark-lab s/HTTP-e
0050  74 68 65 72 65 61 6c 2d  6c 61 62 2d 66 69 6c 65   thereal- lab-file
0060  33 2e 68 74 6d 6c 20 48  54 54 50 2f 31 2e 31 0d   3.html H TTP/1.1.
0070  0a 48 6f 73 74 3a 20 67  61 69 61 2e 63 73 2e 75   .Host: g aia.cs.u
0080  6d 61 73 73 2e 65 64 75  0d 0a 55 73 65 72 2d 41   mass.edu ..User-A
0090  67 65 6e 74 3a 20 4d 6f  7a 69 6c 6c 61 2f 35 2e   gent: Mo zilla/5.
```

P: 21 D: 21 M: 0 Drops: 0

- 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:


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

```
No. -  Time        Source              Destination         Protocol  Info
    1 0.000000    Netgear_61:8e:6d    LinksysG_45:90:a8   0x0800    IP
    2 0.050606    LinksysG_45:90:a8   Netgear_61:8e:6d    0x0800    IP
    3 0.050729    Netgear_61:8e:6d    LinksysG_45:90:a8   0x0800    IP
    4 0.055906    Netgear_61:8e:6d    LinksysG_45:90:a8   0x0800    IP
    5 0.128700    LinksysG_45:90:a8   Netgear_61:8e:6d    0x0800    IP
    6 0.134167    LinksysG_45:90:a8   Netgear_61:8e:6d    0x0800    IP
    7 0.150302    LinksysG_45:90:a8   Netgear_61:8e:6d    0x0800    IP
    8 0.150487    Netgear_61:8e:6d    LinksysG_45:90:a8   0x0800    IP
    9 0.213639    LinksysG_45:90:a8   Netgear_61:8e:6d    0x0800    IP
   10 0.215724    LinksysG_45:90:a8   Netgear_61:8e:6d    0x0800    IP
   11 0.215947    Netgear_61:8e:6d    LinksysG_45:90:a8   0x0800    IP
   12 0.231749    LinksysG_45:90:a8   Netgear_61:8e:6d    0x0800    IP
   13 0.232145    Netgear_61:8e:6d    LinksysG_45:90:a8   0x0800    IP
   14 0.320470    Netgear_61:8e:6d    LinksysG_45:90:a8   0x0800    IP
   15 0.403428    LinksysG_45:90:a8   Netgear_61:8e:6d    0x0800    IP
   16 0.423932    Netgear_61:8e:6d    LinksysG_45:90:a8   0x0800    IP
   17 0.579522    Netgear_61:8e:6d    LinksysG_45:90:a8   0x0800    IP
   18 3.383584    Netgear_61:8e:6d    LinksysG_45:90:a8   0x0800    IP
   19 9.392197    Netgear_61:8e:6d    LinksysG_45:90:a8   0x0800    IP
   20 10.389131   LinksysG_45:90:a8   Netgear_61:8e:6d    0x0800    IP
   21 10.389258   Netgear_61:8e:6d    LinksysG_45:90:a8   0x0800    IP
```

```
⊞ Frame 4 (506 bytes on wire, 506 bytes captured)
⊟ Ethernet II, Src: Netgear_61:8e:6d (00:09:5b:61:8e:6d), Dst: LinksysG_45:90:a8 (00:0c:41:45:90:a8)
  ⊟ Destination: LinksysG_45:90:a8 (00:0c:41:45:90:a8)
      Address: LinksysG_45:90:a8 (00:0c:41:45:90:a8)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
  ⊟ Source: Netgear_61:8e:6d (00:09:5b:61:8e:6d)
      Address: Netgear_61:8e:6d (00:09:5b:61:8e:6d)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    Type: IP (0x0800)
  Data (492 bytes)
```

```
0000  00 0c 41 45 90 a8 00 09  5b 61 8e 6d 08 00 45 00   ..AE.... [a.m..E.
0010  01 ec 87 e9 40 00 80 06  38 65 c0 a8 02 91 80 77   ....@... 8e.....w
0020  f5 0c 07 f6 00 50 7a 74  c4 58 7d a6 27 90 50 18   .....Pzt .X}.'.P.
0030  ff ff 3a 9c 00 00 47 45  54 20 2f 77 69 72 65 73   ..:...GE T /wires
0040  68 61 72 6b 2d 6c 61 62  73 2f 48 54 54 50 2d 65   hark-lab s/HTTP-e
0050  74 68 65 72 65 61 6c 2d  6c 61 62 2d 66 69 6c 65   thereal- lab-file
0060  33 2e 68 74 6d 6c 20 48  54 54 50 2f 31 2e 31 0d   3.html H TTP/1.1.
0070  0a 48 6f 73 74 3a 20 67  61 69 61 2e 63 73 2e 75   .Host: g aia.cs.u
```

```
File: "C:\DOCUME~1\PAULAW~1\LOCALS~1\Temp\etherXXXXa02620" 8584 Bytes 00:...   P: 21 D: 21 M: 0 Drops: 0
```

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] 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?
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.]~~
3. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?
4. How many bytes from the very start of the Ethernet frame does the ASCII “G” in “GET” appear in the Ethernet frame?

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

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?~~
6. What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?
7. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?
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?

---

[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.