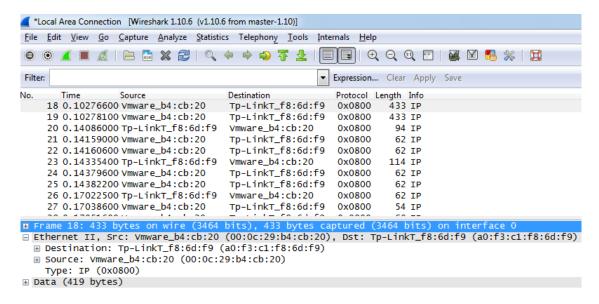
# Lab 5

Name: Bing Hao

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

#### Answer



0000	a0 f3 c1 f8 6d f9 00 0c 29 b4	4 cb 20 08 00 45 00m )E.
0010	01 a3 11 bd 40 00 80 06 00 00	0 c0 a8 01 0b 80 77@w
0020	f5 Oc fe 28 00 50 db c0 93 06	5 57 c5 83 35 50 <b>1</b> 8(.pw5p.
0030	fa f0 38 cd 00 00 47 45 54 20	D 2f 77 69 72 65 73GE T /wires
0040	68 61 72 6b 2d 6c 61 62 73 2f	f 48 54 54 50 2d 65   hark-lab s/HTTP-e
0050		l 62 2d 66 69 6c 65   thereal- lab-file
0060		4 50 2f 31 2e 31 0d
0070		9 61 2e 63 73 2e 75   .Host: g aia.cs.u
0080		a 43 6f 6e 6e 65 63   mass.edūConnec
0090		0 2d 61 6c 69 76 65   tion: ke ep-alive
00a0		0 74 65 78 7 <u>4</u> 2f 68Accept : text/h
00b0		3 61 74 69 6f 6e 2f tml,appl ication/
00c0		c 61 70 70 6c 69 63 xhtml+xm ],applic
00d0	61 74 69 6f 6e 2f 78 6d 6c 3b	o 71 3d 30 2e 39 2c
	Frame (frame), 433 bytes	Packets: 55 · Displayed: 55 (100.0%) · Dropped: 0 (0 Profile: Default

Figure 1

According to above screenshot (Figure 1), the Ethernet address of my computer is 00:0c:29:b4:cb:20.

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.]

## <u>Answer</u>

Name: Bing Hao

Home Page: <a href="http://uniteng.com">http://uniteng.com</a>

According to Figure 1, the destination address is a0:f3:c1:f8:6d:f9. This address is not the etherrnet address of gaia.cs.umass.edu, but it is the address of my TP link router (Gateway to Internet).

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

#### <u>Answer</u>

According to the Figure 1, the hexadecimal value for the frame type field is Type: IP (0x0800). This is correspond to IP protocol.

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

## Answer

According to the Figure 1, the G in the GET appears 52 bits into the frame.

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?

## Answer

```
30 0.20547700 Tp-LinkT_f8:6d:f9 Vmware_b4:cb:20
                                                       0x0800 1514 IP
⊕ Frame 30: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0

⊟ Ethernet II, Src: Tp-LinkT_f8:6d:f9 (a0:f3:c1:f8:6d:f9), Dst: Vmware_b4:cb:20 (00:0c:29:b4:cb:20)

  □ Destination: Vmware_b4:cb:20 (00:0c:29:b4:cb:20)
      Address: Vmware_b4:cb:20 (00:0c:29:b4:cb:20)
      .... .0. .... = LG bit: Globally unique address (factory default)
 \dots 0 \dots = IG bit: Ind \square Source: Tp-LinkT_f8:6d:f9 (a0:f3:c1:f8:6d:f9)
                              .... = IG bit: Individual address (unicast)
      Address: Tp-LinkT_f8:6d:f9 (a0:f3:c1:f8:6d:f9)
      ......0. .... = LG bit: Globally unique address (factory default)
           ...0 ....
                    .... = IG bit: Individual address (unicast)
   Type: IP (0x0800)
□ Data (1500 bytes)
    [Length: 1500]
      00 Oc 29 b4 cb 20 a0 f3 c1 f8 6d f9 08 00
0010
0030
```

Figure 2

According to the Figure 2, the value of the Ethernet source address is a0:f3:c1:f8:6d:f9. This address is not the address of my computer or gaia.cs.umass.edu. This is the address of my router.

Home Page: http://uniteng.com

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

Name: Bing Hao

## **Answer**

According to the Figure 2, the value of the destination address is 00:0c:29:b4:cb:20. This is the address of my computer.

Local network card information:

```
Ethernet adapter Local Area Connection:
  Connection-specific DNS Suffix .:
  Description . . . . . . . . . : Intel(R) PRO/1000 MT Network Connection
  Physical Address. . . . . . . : 00-0C-29-B4-CB-20
  DHCP Enabled. . . . . . . . : No
  Autoconfiguration Enabled . . . . : Yes
  Link-local IPv6 Address . . . . . : fe80::80c9:27d0:de44:9f03%11(Preferred)
  IPv4 Address. . . . . . . . . : 192.168.1.11(Preferred)
  Subnet Mask . . . . . . . . . : 255.255.255.0
  Default Gateway . . . . . . . : 192.168.1.1
  DHCPv6 IAID .
                                   : 234884137
  DHCPv6 Client DUID. . . . .
                               . . : 00-01-00-01-1A-6A-8A-4F-00-0C-29-B4-CB-20
                   . . . . . . . . : 8.8.8.8
  DNS Servers . . .
  NetBIOS over Topip. . . . . . .
```

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

# <u>Answer</u>

According to the Figure 2, the hex value of this field is 0x0800. It corresponds to the IP protocol.

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?

## Answer

According to the Figure 2, the O in OK appear 52 bytes in the Ethernet frame.

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

# Answer

```
Interface: 192.168.1.11 --- 0xb
  Internet Address
                        Physical Address
                                               Type
  192.168.1.1
                         a0-f3-c1-f8-6d-f9
                                               dynamic
  192.168.1.7
                        f0-de-f1-d7-1f-7a
                                               dynamic
  192.168.1.255
                        ff-ff-ff-ff-ff
                                               static
  224.0.0.22
                        01-00-5e-00-00-16
                                               static
  224.0.0.252
                         01-00-5e-00-00-fc
                                               static
 239.255.255.250
                        01-00-5e-7f-ff-fa
                                               static
```

Name: Bing Hao

Internet Address: IP address

Physical Address: the MAC address

Type: The protocol type

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

## **Answer**

```
Protocol Length Info
         Time
                        Source
                                                   Destination
                                                                                            60 Who has 192.168.1.1? Tell 192.168.1.11
       2 0.00016500 Vmware_b4:cb:20 Broadcast
3 0.00081800 Tp-LinkT_f8:6d:f9 Vmware_b4:cb:20
                                                                              ΔRP
                                                                                            60 192.168.1.1 is at a0:f3:c1:f8:6d:f9
                                                   Tp-LinkT_f8:6d:f9
Tp-LinkT_f8:6d:f9
Vmware_b4:cb:20
        4 0.00098800 Vmware_b4:cb:20
                                                                              0x0800
                                                                                            62 IP
       5 0.00100400 Vmware_b4:cb:20 6 0.10366000 Tp-LinkT_f8:6d:f9
                                                                              0x0800
                                                                              0x0800
                                                   Tp-LinkT_f8:6d:f9
Tp-LinkT_f8:6d:f9
Tp-LinkT_f8:6d:f9
        7 0.10386900 vmware b4:cb:20
                                                                             0x0800
                                                                                            54 IP
       8 0.10388300 Vmware_b4:cb:20
9 0.10422300 Vmware_b4:cb:20
                                                                              0x0800
                                                                                            60 IP
                                                                              0x0800
                                                                                          434 IP
      10 0.10423600 vmware_b4:cb:20
                                                   Tp-LinkT_f8:6d:f9
                                                                             0x0800
Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
■ Finance 1. 42 bytes of white (350 bits) of mile face of Ethernet II, Src: Vmware_b4:cb:20 (00:0c:29:b4:cb:20), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

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

Address: Broadcast (ff:ff:ff:ff:ff:ff)
   Address: Vmware_b4:cb:20 (00:0c:29:b4:cb:20)
.....0...... = LG bit: Globally unique address (factory default)
.....0 ..... = IG bit: Individual address (unicast)
Type: ARP (0x0806)

Address Resolution Protocol (request)
```

Figure 3

According to Figure 3, the Hex values for the source is 00:0c:29:b4:cb:20, the destination address is Broadcast (ff:ff:ff:ff:ff).

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

## Answer

The hex value for the two byte Ethernet frame is ARP (0x0806), the corresponding upper layer protocol is ARP.

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?
- 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?
- c) Does the ARP message contain the IP address of the sender?
- d) Where in the ARP request does the "question" appear the Ethernet address of the machine whose corresponding IP address is being queried?

#### <u>Answer</u>

- a. 20 bytes
- b. 0x0001
- c. Yes, according to following figure, the IP address of the sender is 192.168.1.11.

```
Time Source
1 0.00000000 Vmware_b4:cb:20
                                    Destination
                                     Broadcast
     2 0.00016500 Vmware_b4:cb:20
                                     Broadcast
     3 0.00081800 Tp-LinkT_f8:6d:f9
                                    Vmware_b4:cb:20
                                                        ARP
                                                                  60 192.168.1.1 is at a0:f3:c1:f8:6d:f9
     4 0.00098800 vmware b4:cb:20
                                     Tp-LinkT_f8:6d:f9
                                                        0x0800
                                                                  62 IP
                                     Tp-LinkT_f8:6d:f9
     5 0.00100400 Vmware_b4:cb:20
                                                        0x0800
                                                                  62 IP
     6 0.10366000 Tp-LinkT_f8:6d:f9
                                    Vmware_b4:cb:20
                                                        0x0800
     7 0.10386900 Vmware_b4:cb:20
                                    Tp-LinkT_f8:6d:f9
                                                        0x0800
                                                                  54 IP
     8 0.10388300 Vmware b4:cb:20
                                    Tp-LinkT_f8:6d:f9
                                                        0x0800
                                                                  60 IP
     9 0.10422300 Vmware_b4:cb:20
                                    Tp-LinkT_f8:6d:f9
                                                        0x0800
                                                                 434 IP
    10 0.10423600 Vmware_b4:cb:20
                                     Tp-LinkT_f8:6d:f9
                                                        0x0800
      Address: Vmware_b4:cb:20 (00:0c:29:b4:cb:20)
               .... = LG bit: Globally unique address (factory default)
      .... ..0.
      .... ...0 .... = IG bit: Individual address (unicast)
■ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
   Protocol type: IP (0x0800)
   Hardware size: 6
   Protocol size: 4
   Opcode: request (1)
   Sender MAC address: Vmware_b4:cb:20 (00:0c:29:b4:cb:20)
Sender IP address: 192.168.1.11 (192.168.1.11)
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00)
   Target IP address: 192.168.1.1 (192.168.1.1)
```

Figure 4

- d. The Target MAC address is 00:00:00:00:00:00, this broadcast will queries the machine which IP address is 192.168.1.1.
- 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?

Name: Bing Hao

Home Page: <a href="http://uniteng.com">http://uniteng.com</a>

- 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?
- 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?

#### <u>Answer</u>

```
Protocol Length Info
       Time Source
1 0.00000000 Vmware_b4:cb:20
2 0.00016500 Vmware_b4:cb:20
                                                                                       42 Who has 192.168.1.1? Tell 192.168.1.11 60 Who has 192.168.1.1? Tell 192.168.1.11
                                                Broadcast
Broadcast
                                                                          ARP
ARP
       3 0.00081800 Tp-LinkT_f8:6d:f9 Vmware_b4:cb:20
                                                                          ARP
                                                                                        60 192.168.1.1 is at a0:f3:c1:f8:6d:f9
  Ethernet II, Src: Tp-LinkT_f8:6d:f9 (a0:f3:c1:f8:6d:f9), Dst: Vmware_b4:cb:20 (00:0c:29:b4:cb:20)
  Destination: Vmware_b4:cb:20 (00:0c:29:b4:cb:20)
Address: Vmware_b4:cb:20 (00:0c:29:b4:cb:20)
  Address: Tp-LinkT_f8:6d:f9 (a0:f3:c1:f8:6d:f9)
.....0. ... = LG bit: Globally unique address (factory default)
     ... .... = IG bit: Individual address (unicast)
□ Address Resolution Protocol (reply)
Hardware type: Ethernet (1)
Protocol type: IP (0x0800)
Hardware size: 6
Protocol size: 4
     Opcode: reply (2)
Sender MAC address: Tp-LinkT_f8:6d:f9 (a0:f3:c1:f8:6d:f9)
     Sender IP address: 192.168.1.1 (192.168.1.1)
Target MAC address: Vmware_b4:cb:20 (00:0c:29:b4:cb:20)
Target IP address: 192.168.1.11 (192.168.1.11)
```

Figure 5

- a. 20 bytes
- b. 0x0002
- c. Sender IP address: 192.168.1.1 and Sender MAC address: a0:f3:c1:f8:6d:f9 does the "answer" to 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?

# **Answer**

According to the Figure 5, Source: a0:f3:c1:f8:6d:f9, Destination: 00:0c:29:b4:cb:20.

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?

# Answer

Name: Bing Hao

Home Page: <a href="http://uniteng.com">http://uniteng.com</a>

Because the ARP request is broadcast, but the ARP reply is not broadcast. The reply will be sent to the computer who made the request directly.

# 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?

## **Answer**

The correct entry for my web server should be:

```
192.168.1.20 b8-27-eb-b1-ae-1d dynamic
```

I cleared the ARP cache and added an error entry:

```
C:\Windows\system32>arp -s 192.168.1.20 b8-27-eb-b1-ae-27
```

After operations, I tried to ping the web server:

```
C:\Windows\system32>ping 192.168.1.20

Pinging 192.168.1.20 with 32 bytes of data:
Request timed out.
```

It seems the ICMP packages could not reach the web server.

I also tried to access the port 80 on the web server, but also could not connect:

Oops! Google Chrome could not connect to 192.168.1.20

Try reloading: 192.168.1.20

Clear the ARP cache again, and then ping the web server again:

```
C:\Windows\system32>ping 192.168.1.20

Pinging 192.168.1.20 with 32 bytes of data:

Reply from 192.168.1.20: bytes=32 time=2ms TTL=64

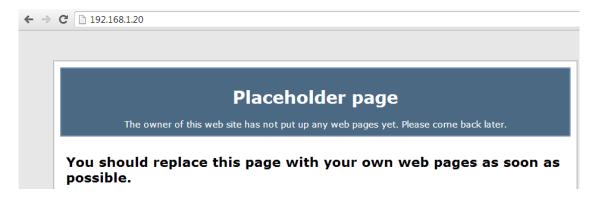
Reply from 192.168.1.20: bytes=32 time<1ms TTL=64

Reply from 192.168.1.20: bytes=32 time=1ms TTL=64
```

Name: Bing Hao

#### Success!

Accessing the port 80:



## Success!

The current APR table:

```
C:\Users\neil>arp -a

Interface: 192.168.1.11 --- 0xb

Internet Address Physical Address Type
192.168.1.1 a0-f3-c1-f8-6d-f9 dynamic
192.168.1.20 b8-27-eb-b1-ae-1d dynamic
239.255.255.250 01-00-5e-7f-ff-fa static
```

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.

#### <u>Answer</u>

According to the document from Microsoft <a href="http://support.microsoft.com/kb/949589">http://support.microsoft.com/kb/949589</a>, there is no default amount of time that an entry remains in the ARP cache now.

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.

Name: Bing Hao

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 ( $30 \times 0.5$  seconds) and 45 seconds ( $30 \times 1.5$  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.