Họ tên : Lê Bảo Khánh
MSSV : 1911363
Lớp : L01

LAB 6

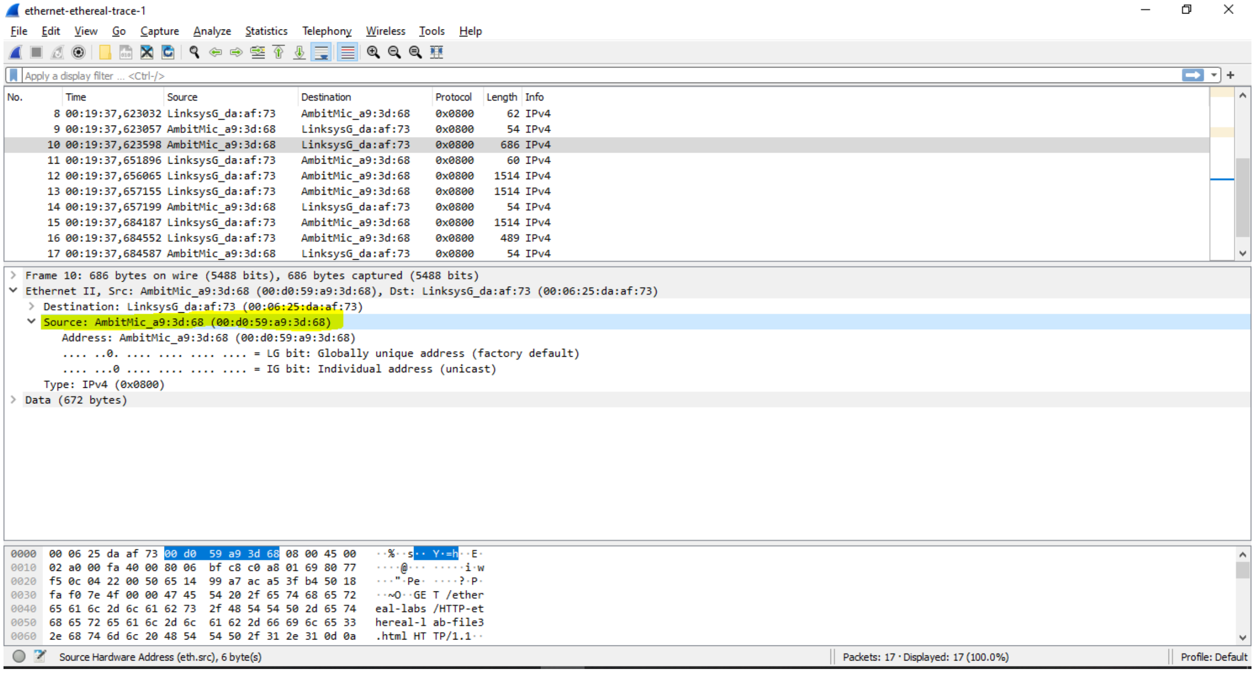
(Using the file *ethernet--ethereal-trace-1)*

1. Capturing and analyzing Ethernet frames

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

ANSWER:

My 48-bit Ethernet address is 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-/>

```
No.   Time             Source             Destination        Protocol Length Info
    8 00:19:37,623032 LinksysG_da:af:73  AmbitMic_a9:3d:68  0x0800     62 IPv4
    9 00:19:37,623057 AmbitMic_a9:3d:68  LinksysG_da:af:73  0x0800     54 IPv4
   10 00:19:37,623598 AmbitMic_a9:3d:68  LinksysG_da:af:73  0x0800    686 IPv4
   11 00:19:37,651896 LinksysG_da:af:73  AmbitMic_a9:3d:68  0x0800     60 IPv4
   12 00:19:37,656065 LinksysG_da:af:73  AmbitMic_a9:3d:68  0x0800   1514 IPv4
   13 00:19:37,657155 LinksysG_da:af:73  AmbitMic_a9:3d:68  0x0800   1514 IPv4
   14 00:19:37,657199 AmbitMic_a9:3d:68  LinksysG_da:af:73  0x0800     54 IPv4
   15 00:19:37,684187 LinksysG_da:af:73  AmbitMic_a9:3d:68  0x0800   1514 IPv4
   16 00:19:37,684552 LinksysG_da:af:73  AmbitMic_a9:3d:68  0x0800    489 IPv4
   17 00:19:37,684587 AmbitMic_a9:3d:68  LinksysG_da:af:73  0x0800     54 IPv4
```

```
> Frame 10: 686 bytes on wire (5488 bits), 686 bytes captured (5488 bits)
v 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)
  v Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
      Address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
> Data (672 bytes)
```

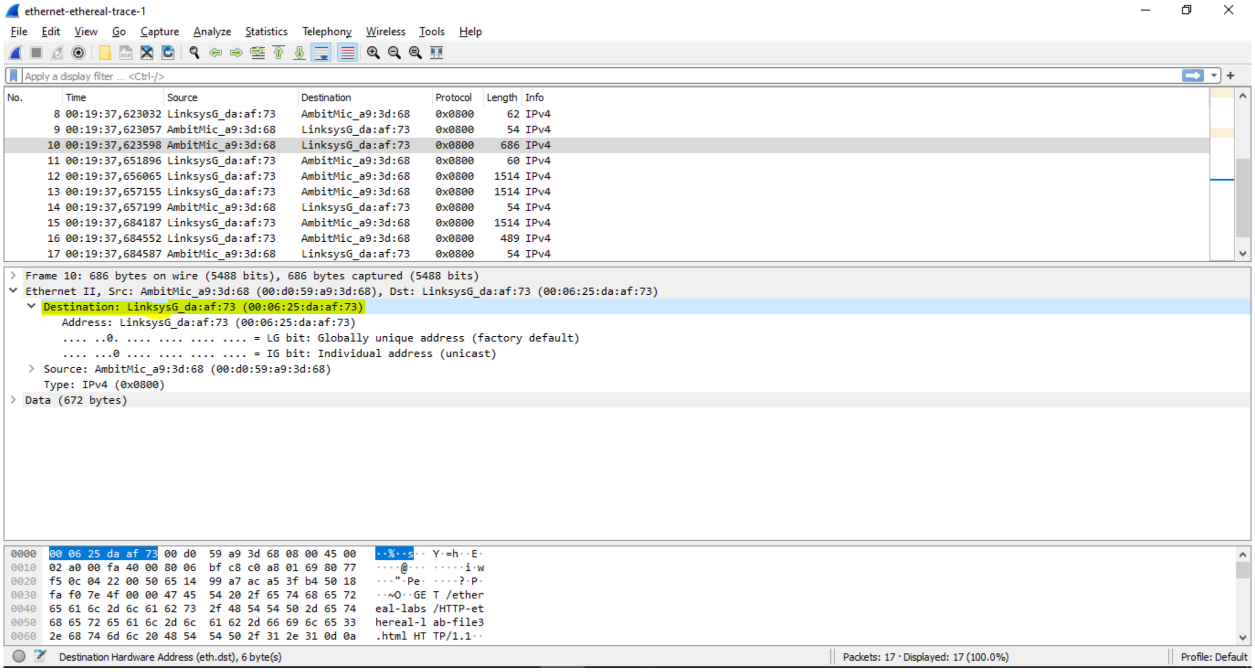
```
0000  00 06 25 da af 73 00 d0  59 a9 3d 68 08 00 45 00   ··%··s·· Y·=h··E·
0010  02 a0 00 fa 40 00 80 06  bf c8 c0 a8 01 69 80 77   ····@··· ·····i·w
0020  f5 0c 04 22 00 50 65 14  99 a7 ac a5 3f b4 50 18   ···"·Pe· ····?·P·
0030  fa f0 7e 4f 00 00 47 45  54 20 2f 65 74 68 65 72   ··~O··GE T /ether
0040  65 61 6c 2d 6c 61 62 73  2f 48 54 54 50 2d 65 74   eal-labs /HTTP-et
0050  68 65 72 65 61 6c 2d 6c  61 62 2d 66 69 6c 65 33   hereal-l ab-file3
0060  2e 68 74 6d 6c 20 48 54  54 50 2f 31 2e 31 0d 0a   .html HT TP/1.1··
```

Source Hardware Address (eth.src), 6 byte(s) | Packets: 17 · Displayed: 17 (100.0%) | Profile: Default

Question 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?

ANSWER:

The 48-bit destination address: 00:06:25:da:af:73
(This is not the Ethernet address of gaia.cs.umass.edu)
It is the address of the router which the computer has to go through in order to reach the destination. (internet gateway address)



ethernet-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

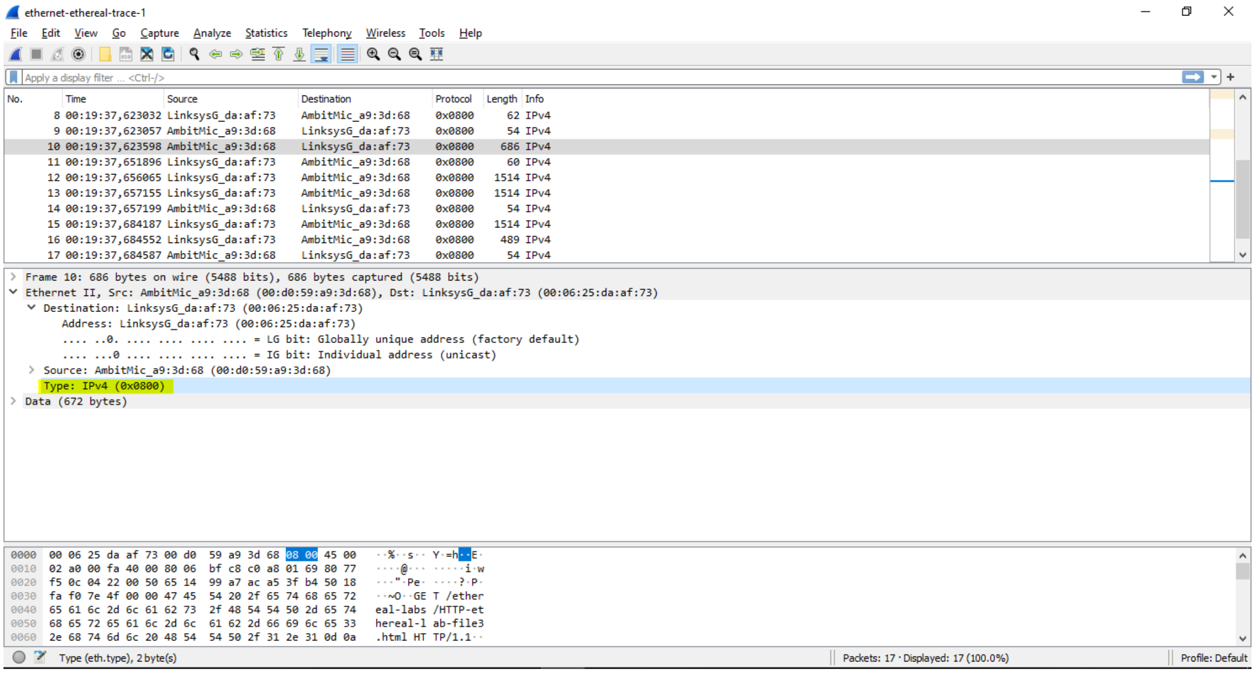
```
No.    Time              Source              Destination         Protocol  Length Info
     8 00:19:37,623032 LinksysG_da:af:73   AmbitMic_a9:3d:68   0x0800      62 IPv4
     9 00:19:37,623057 AmbitMic_a9:3d:68   LinksysG_da:af:73   0x0800      54 IPv4
    10 00:19:37,623598 AmbitMic_a9:3d:68   LinksysG_da:af:73   0x0800     686 IPv4
    11 00:19:37,651896 LinksysG_da:af:73   AmbitMic_a9:3d:68   0x0800      60 IPv4
    12 00:19:37,656065 LinksysG_da:af:73   AmbitMic_a9:3d:68   0x0800    1514 IPv4
    13 00:19:37,657155 LinksysG_da:af:73   AmbitMic_a9:3d:68   0x0800    1514 IPv4
    14 00:19:37,657199 AmbitMic_a9:3d:68   LinksysG_da:af:73   0x0800      54 IPv4
    15 00:19:37,684187 LinksysG_da:af:73   AmbitMic_a9:3d:68   0x0800    1514 IPv4
    16 00:19:37,684552 LinksysG_da:af:73   AmbitMic_a9:3d:68   0x0800     489 IPv4
    17 00:19:37,684587 AmbitMic_a9:3d:68   LinksysG_da:af:73   0x0800      54 IPv4

> Frame 10: 686 bytes on wire (5488 bits), 686 bytes captured (5488 bits)
v Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
  v Destination: LinksysG_da:af:73 (00:06:25:da:af:73)
      Address: LinksysG_da:af:73 (00:06:25:da:af:73)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  > Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
    Type: IPv4 (0x0800)
> Data (672 bytes)

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 80 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··GE T /ether
0040  65 61 6c 2d 6c 61 62 73  2f 48 54 54 50 2d 65 74   eal-labs /HTTP-et
0050  68 65 72 65 61 6c 2d 6c  61 62 2d 66 69 6c 65 33   hereal-l ab-file3
0060  2e 68 74 6d 6c 20 48 54  54 50 2f 31 2e 31 0d 0a   .html HT TP/1.1··

Destination Hardware Address (eth.dst), 6 byte(s)    Packets: 17 · Displayed: 17 (100.0%)    Profile: Default
```

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

ANSWER:

The hexadecimal value for the two-byte Frame type field: 0x00000800

=> This is correspond to IP protocol



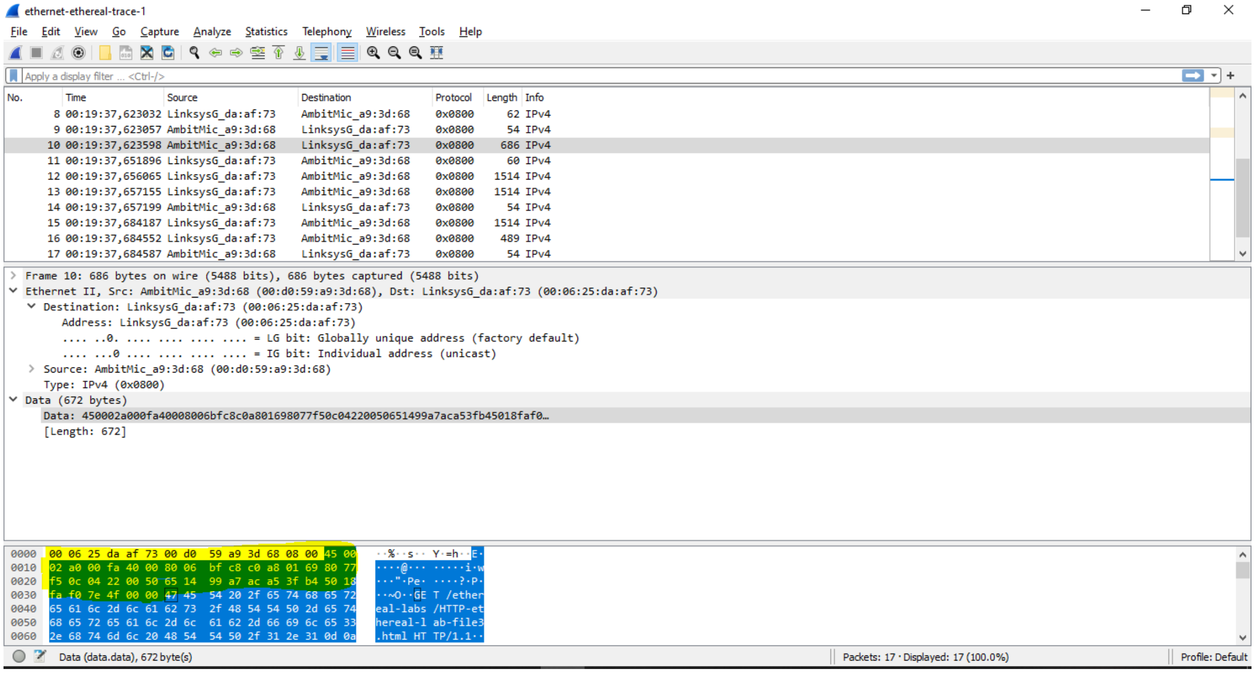
ethernet-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.    Time              Source              Destination         Protocol  Length Info
     8 00:19:37,623032 LinksysG_da:af:73   AmbitMic_a9:3d:68   0x0800      62 IPv4
     9 00:19:37,623057 AmbitMic_a9:3d:68   LinksysG_da:af:73   0x0800      54 IPv4
    10 00:19:37,623598 AmbitMic_a9:3d:68   LinksysG_da:af:73   0x0800     686 IPv4
    11 00:19:37,651896 LinksysG_da:af:73   AmbitMic_a9:3d:68   0x0800      60 IPv4
    12 00:19:37,656065 LinksysG_da:af:73   AmbitMic_a9:3d:68   0x0800    1514 IPv4
    13 00:19:37,657155 LinksysG_da:af:73   AmbitMic_a9:3d:68   0x0800    1514 IPv4
    14 00:19:37,657199 AmbitMic_a9:3d:68   LinksysG_da:af:73   0x0800      54 IPv4
    15 00:19:37,684187 LinksysG_da:af:73   AmbitMic_a9:3d:68   0x0800    1514 IPv4
    16 00:19:37,684552 LinksysG_da:af:73   AmbitMic_a9:3d:68   0x0800     489 IPv4
    17 00:19:37,684587 AmbitMic_a9:3d:68   LinksysG_da:af:73   0x0800      54 IPv4

> Frame 10: 686 bytes on wire (5488 bits), 686 bytes captured (5488 bits)
v Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
  v Destination: LinksysG_da:af:73 (00:06:25:da:af:73)
      Address: LinksysG_da:af:73 (00:06:25:da:af:73)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  > Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
    Type: IPv4 (0x0800)
> Data (672 bytes)

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 80 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··GE T /ether
0040  65 61 6c 2d 6c 61 62 73  2f 48 54 54 50 2d 65 74   eal-labs /HTTP-et
0050  68 65 72 65 61 6c 2d 6c  61 62 2d 66 69 6c 65 33   hereal-l ab-file3
0060  2e 68 74 6d 6c 20 48 54  54 50 2f 31 2e 31 0d 0a   .html HT TP/1.1··

Type (eth.type), 2 byte(s)    Packets: 17 · Displayed: 17 (100.0%)    Profile: Default
```

<u>Question 4:</u> How many bytes from the very start of the Ethernet frame does the ASCII "G" in "GET" appear in the Ethernet frame?

ANSWER:

After 54 bytes, the "G" in "GET" appears.



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
    8 00:19:37,623032 LinksysG_da:af:73   AmbitMic_a9:3d:68   0x0800      62 IPv4
    9 00:19:37,623057 AmbitMic_a9:3d:68   LinksysG_da:af:73   0x0800      54 IPv4
   10 00:19:37,623598 AmbitMic_a9:3d:68   LinksysG_da:af:73   0x0800     686 IPv4
   11 00:19:37,651896 LinksysG_da:af:73   AmbitMic_a9:3d:68   0x0800      60 IPv4
   12 00:19:37,656065 LinksysG_da:af:73   AmbitMic_a9:3d:68   0x0800    1514 IPv4
   13 00:19:37,657155 LinksysG_da:af:73   AmbitMic_a9:3d:68   0x0800    1514 IPv4
   14 00:19:37,657199 AmbitMic_a9:3d:68   LinksysG_da:af:73   0x0800      54 IPv4
   15 00:19:37,684187 LinksysG_da:af:73   AmbitMic_a9:3d:68   0x0800    1514 IPv4
   16 00:19:37,684552 LinksysG_da:af:73   AmbitMic_a9:3d:68   0x0800     489 IPv4
   17 00:19:37,684587 AmbitMic_a9:3d:68   LinksysG_da:af:73   0x0800      54 IPv4
```

```
> Frame 10: 686 bytes on wire (5488 bits), 686 bytes captured (5488 bits)
v Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
  v Destination: LinksysG_da:af:73 (00:06:25:da:af:73)
       Address: LinksysG_da:af:73 (00:06:25:da:af:73)
       .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
       .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  > Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
    Type: IPv4 (0x0800)
v Data (672 bytes)
    Data: 450002a000fa40008006bfc8c0a801698077f50c04220050651499a7aca53fb45018faf0…
    [Length: 672]
```

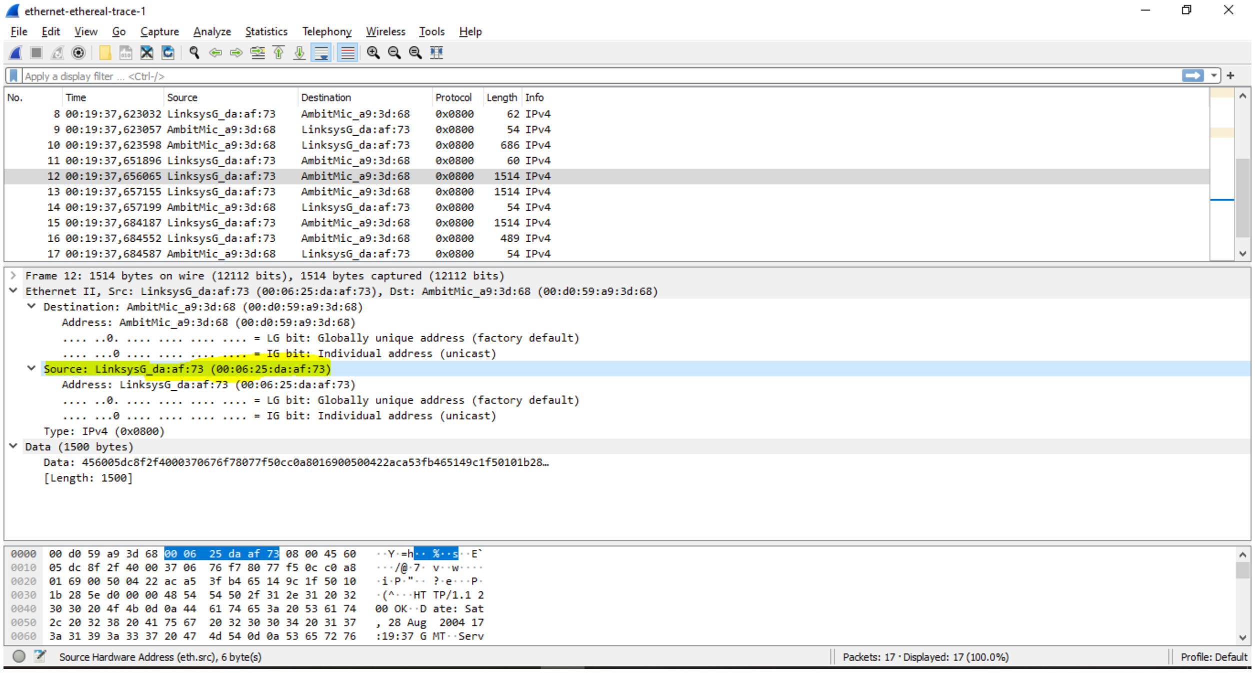
```
0000  00 06 25 da af 73 00 d0  59 a9 3d 68 08 00 45 00   ··%··s·· Y·=h··E·
0010  02 a0 00 fa 40 00 80 06  bf c8 c0 a8 01 69 80 77   ····@··· ·····i·w
0020  f5 0c 04 22 00 50 65 14  99 a7 ac a5 3f b4 50 18   ···"·Pe· ····?·P·
0030  fa f0 7e 4f 00 00 47 45  54 20 2f 65 74 68 65 72   ··~O··GE T /ether
0040  65 61 6c 2d 6c 61 62 73  2f 48 54 54 50 2d 65 74   eal-labs /HTTP-et
0050  68 65 72 65 61 6c 2d 6c  61 62 2d 66 69 6c 65 33   hereal-l ab-file3
0060  2e 68 74 6d 6c 20 48 54  54 50 2f 31 2e 31 0d 0a   .html HT TP/1.1··
```

Data (data.data), 672 byte(s) | Packets: 17 · Displayed: 17 (100.0%) | Profile: Default

<u>Question 5</u>: 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:

The value of the Ethernet source address: 00:06:25:da:af:73
This is not the address of the computer / of gaia.cs.umass.edu,
This is the address of the router


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
    8 00:19:37,623032 LinksysG_da:af:73    AmbitMic_a9:3d:68    0x0800      62 IPv4
    9 00:19:37,623057 AmbitMic_a9:3d:68    LinksysG_da:af:73    0x0800      54 IPv4
   10 00:19:37,623598 AmbitMic_a9:3d:68    LinksysG_da:af:73    0x0800     686 IPv4
   11 00:19:37,651896 LinksysG_da:af:73    AmbitMic_a9:3d:68    0x0800      60 IPv4
   12 00:19:37,656065 LinksysG_da:af:73    AmbitMic_a9:3d:68    0x0800    1514 IPv4
   13 00:19:37,657155 LinksysG_da:af:73    AmbitMic_a9:3d:68    0x0800    1514 IPv4
   14 00:19:37,657199 AmbitMic_a9:3d:68    LinksysG_da:af:73    0x0800      54 IPv4
   15 00:19:37,684187 LinksysG_da:af:73    AmbitMic_a9:3d:68    0x0800    1514 IPv4
   16 00:19:37,684552 LinksysG_da:af:73    AmbitMic_a9:3d:68    0x0800     489 IPv4
   17 00:19:37,684587 AmbitMic_a9:3d:68    LinksysG_da:af:73    0x0800      54 IPv4
```

```
> Frame 12: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
v Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
  v Destination: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
      Address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: LinksysG_da:af:73 (00:06:25:da:af:73)
      Address: LinksysG_da:af:73 (00:06:25:da:af:73)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
v Data (1500 bytes)
    Data: 456005dc8f2f4000370676f78077f50cc0a8016900500422aca53fb465149c1f50101b28…
    [Length: 1500]
```

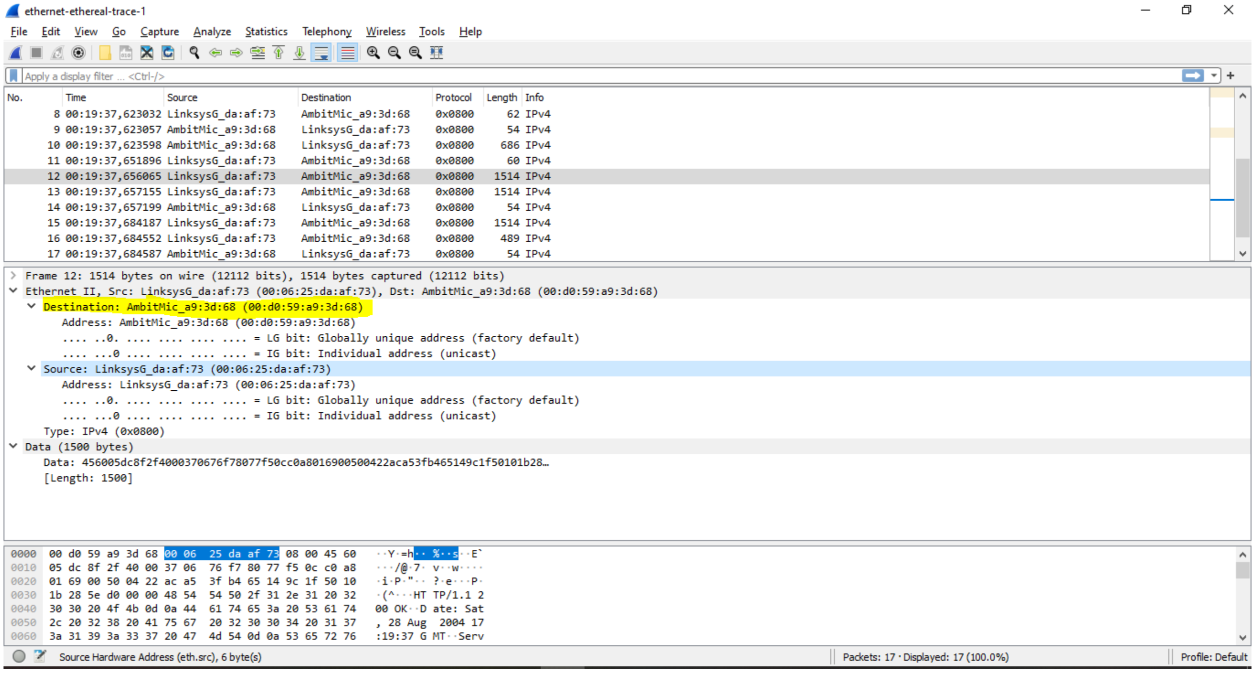
```
0000  00 d0 59 a9 3d 68 00 06  25 da af 73 08 00 45 60   ··Y·=h·· %··s··E`
0010  05 dc 8f 2f 40 00 37 06  76 f7 80 77 f5 0c c0 a8   ···/@·7· v··w····
0020  01 69 00 50 04 22 ac a5  3f b4 65 14 9c 1f 50 10   ·i·P·"·· ?·e···P·
0030  1b 28 5e d0 00 00 48 54  54 50 2f 31 2e 31 20 32   ·(^···HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 53 61 74   00 OK··D ate: Sat
0050  2c 20 32 38 20 41 75 67  20 32 30 30 34 20 31 37   , 28 Aug  2004 17
0060  3a 31 39 3a 33 37 20 47  4d 54 0d 0a 53 65 72 76   :19:37 G MT··Serv
```

Source Hardware Address (eth.src), 6 byte(s) | Packets: 17 · Displayed: 17 (100.0%) | Profile: Default

<u>Question 6:</u> What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?

ANSWER:

The destination address in the Ethernet frame is 00:d0:59:a9:3d:68
This is the Ethernet address of the computer


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
    8 00:19:37,623032 LinksysG_da:af:73    AmbitMic_a9:3d:68    0x0800      62 IPv4
    9 00:19:37,623057 AmbitMic_a9:3d:68    LinksysG_da:af:73    0x0800      54 IPv4
   10 00:19:37,623598 AmbitMic_a9:3d:68    LinksysG_da:af:73    0x0800     686 IPv4
   11 00:19:37,651896 LinksysG_da:af:73    AmbitMic_a9:3d:68    0x0800      60 IPv4
   12 00:19:37,656065 LinksysG_da:af:73    AmbitMic_a9:3d:68    0x0800    1514 IPv4
   13 00:19:37,657155 LinksysG_da:af:73    AmbitMic_a9:3d:68    0x0800    1514 IPv4
   14 00:19:37,657199 AmbitMic_a9:3d:68    LinksysG_da:af:73    0x0800      54 IPv4
   15 00:19:37,684187 LinksysG_da:af:73    AmbitMic_a9:3d:68    0x0800    1514 IPv4
   16 00:19:37,684552 LinksysG_da:af:73    AmbitMic_a9:3d:68    0x0800     489 IPv4
   17 00:19:37,684587 AmbitMic_a9:3d:68    LinksysG_da:af:73    0x0800      54 IPv4
```

```
> Frame 12: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
v Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
  v Destination: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
      Address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: LinksysG_da:af:73 (00:06:25:da:af:73)
      Address: LinksysG_da:af:73 (00:06:25:da:af:73)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
v Data (1500 bytes)
    Data: 456005dc8f2f4000370676f78077f50cc0a8016900500422aca53fb465149c1f50101b28…
    [Length: 1500]
```

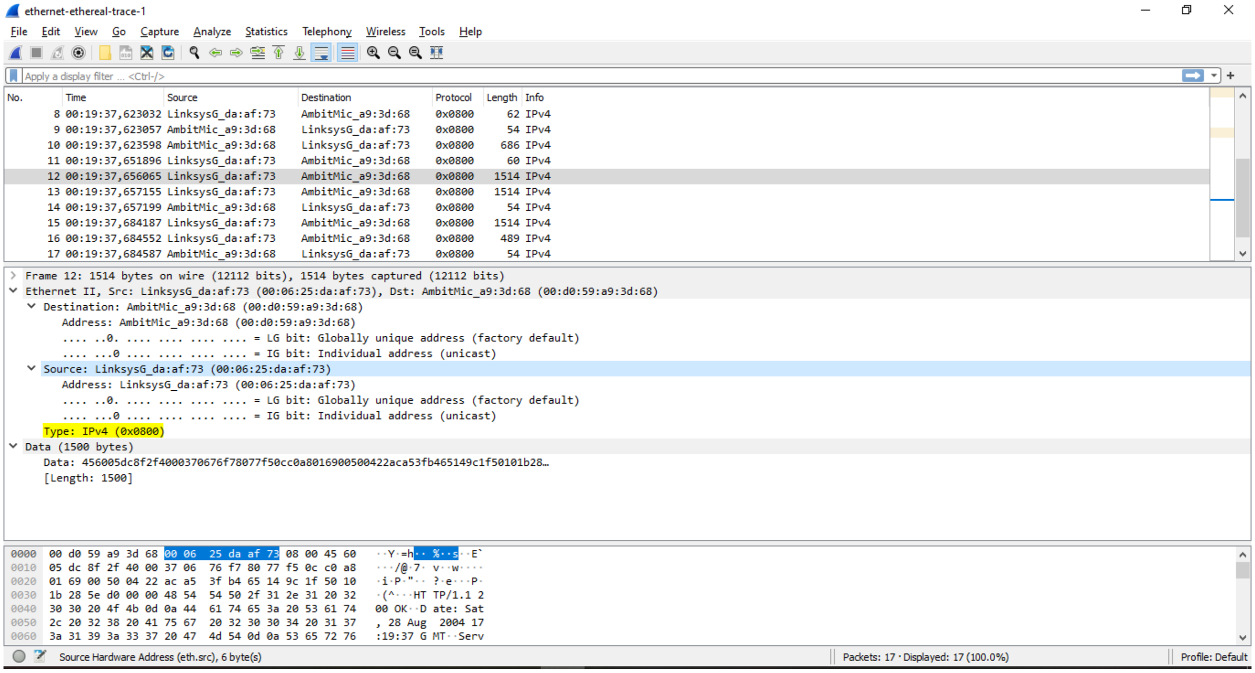
```
0000  00 d0 59 a9 3d 68 00 06  25 da af 73 08 00 45 60   ··Y·=h·· %··s··E`
0010  05 dc 8f 2f 40 00 37 06  76 f7 80 77 f5 0c c0 a8   ···/@·7· v··w····
0020  01 69 00 50 04 22 ac a5  3f b4 65 14 9c 1f 50 10   ·i·P·"·· ?·e···P·
0030  1b 28 5e d0 00 00 48 54  54 50 2f 31 2e 31 20 32   ·(^···HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 53 61 74   00 OK··D ate: Sat
0050  2c 20 32 38 20 41 75 67  20 32 30 30 34 20 31 37   , 28 Aug  2004 17
0060  3a 31 39 3a 33 37 20 47  4d 54 0d 0a 53 65 72 76   :19:37 G MT··Serv
```

Source Hardware Address (eth.src), 6 byte(s) | Packets: 17 · Displayed: 17 (100.0%) | Profile: Default

<u>Question 7:</u> Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

ANSWER:

The hexadecimal value for the two-byte Frame type field: 0x00000800
=> This is correspond to IP protocol



```
No.     Time              Source              Destination         Protocol  Length Info
      8 00:19:37,623032 LinksysG_da:af:73   AmbitMic_a9:3d:68   0x0800      62 IPv4
      9 00:19:37,623057 AmbitMic_a9:3d:68   LinksysG_da:af:73   0x0800      54 IPv4
     10 00:19:37,623598 AmbitMic_a9:3d:68   LinksysG_da:af:73   0x0800     686 IPv4
     11 00:19:37,651896 LinksysG_da:af:73   AmbitMic_a9:3d:68   0x0800      60 IPv4
     12 00:19:37,656065 LinksysG_da:af:73   AmbitMic_a9:3d:68   0x0800    1514 IPv4
     13 00:19:37,657155 LinksysG_da:af:73   AmbitMic_a9:3d:68   0x0800    1514 IPv4
     14 00:19:37,657199 AmbitMic_a9:3d:68   LinksysG_da:af:73   0x0800      54 IPv4
     15 00:19:37,684187 LinksysG_da:af:73   AmbitMic_a9:3d:68   0x0800    1514 IPv4
     16 00:19:37,684552 LinksysG_da:af:73   AmbitMic_a9:3d:68   0x0800     489 IPv4
     17 00:19:37,684587 AmbitMic_a9:3d:68   LinksysG_da:af:73   0x0800      54 IPv4
```

```
> Frame 12: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
v Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
  v Destination: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
      Address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: LinksysG_da:af:73 (00:06:25:da:af:73)
      Address: LinksysG_da:af:73 (00:06:25:da:af:73)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
v Data (1500 bytes)
    Data: 456005dc8f2f4000370676f78077f50cc0a8016900500422aca53fb465149c1f50101b28…
    [Length: 1500]
```

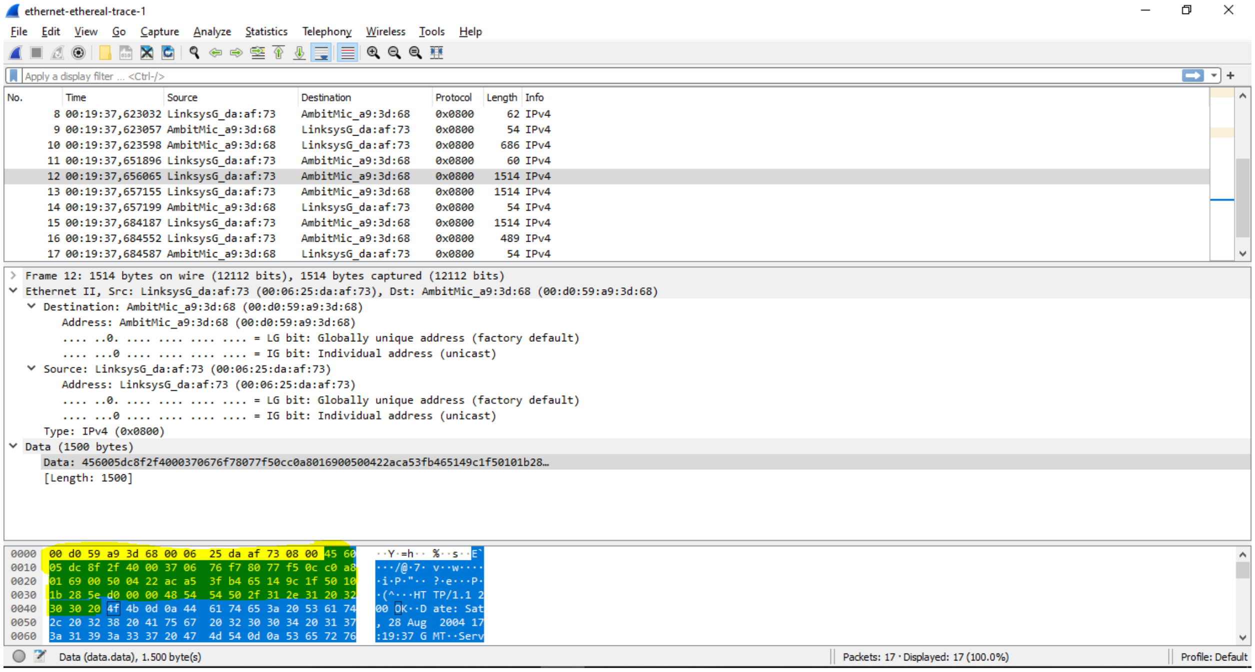
```
0000  00 d0 59 a9 3d 68 00 06  25 da af 73 08 00 45 60   ··Y·=h·· %··s··E`
0010  05 dc 8f 2f 40 00 37 06  76 f7 80 77 f5 0c c0 a8   ···/@·7· v··w····
0020  01 69 00 50 04 22 ac a5  3f b4 65 14 9c 1f 50 10   ·i·P·"·· ?·e···P·
0030  1b 28 5e d0 00 00 48 54  54 50 2f 31 2e 31 20 32   ·(^···HT TP/1.1 2
0040  30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 53 61 74   00 OK··D ate: Sat
0050  2c 20 32 38 20 41 75 67  20 32 30 30 34 20 31 37   , 28 Aug  2004 17
0060  3a 31 39 3a 33 37 20 47  4d 54 0d 0a 53 65 72 76   :19:37 G MT··Serv
```

Source Hardware Address (eth.src), 6 byte(s) | Packets: 17 · Displayed: 17 (100.0%) | Profile: Default

<u>Question 8:</u> 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:

After 67 bytes, the “O” in “OK” appears.


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
    8 00:19:37,623032 LinksysG_da:af:73   AmbitMic_a9:3d:68   0x0800      62 IPv4
    9 00:19:37,623057 AmbitMic_a9:3d:68   LinksysG_da:af:73   0x0800      54 IPv4
   10 00:19:37,623598 AmbitMic_a9:3d:68   LinksysG_da:af:73   0x0800     686 IPv4
   11 00:19:37,651896 LinksysG_da:af:73   AmbitMic_a9:3d:68   0x0800      60 IPv4
   12 00:19:37,656065 LinksysG_da:af:73   AmbitMic_a9:3d:68   0x0800    1514 IPv4
   13 00:19:37,657155 LinksysG_da:af:73   AmbitMic_a9:3d:68   0x0800    1514 IPv4
   14 00:19:37,657199 AmbitMic_a9:3d:68   LinksysG_da:af:73   0x0800      54 IPv4
   15 00:19:37,684187 LinksysG_da:af:73   AmbitMic_a9:3d:68   0x0800    1514 IPv4
   16 00:19:37,684552 LinksysG_da:af:73   AmbitMic_a9:3d:68   0x0800     489 IPv4
   17 00:19:37,684587 AmbitMic_a9:3d:68   LinksysG_da:af:73   0x0800      54 IPv4
```

```
> Frame 12: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
v Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
  v Destination: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
      Address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: LinksysG_da:af:73 (00:06:25:da:af:73)
      Address: LinksysG_da:af:73 (00:06:25:da:af:73)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
v Data (1500 bytes)
    Data: 456005dc8f2f4000370676f78077f50cc0a8016900500422aca53fb465149c1f50101b28…
    [Length: 1500]
```

```
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 4b 0d 0a 44  61 74 65 3a 20 53 61 74   00 OK··D ate: Sat
0050  2c 20 32 38 20 41 75 67  20 32 30 30 34 20 31 37   , 28 Aug  2004 17
0060  3a 31 39 3a 33 37 20 47  4d 54 0d 0a 53 65 72 76   :19:37 G MT··Serv
```

Data (data.data), 1.500 byte(s) | Packets: 17 · Displayed: 17 (100.0%) | Profile: Default

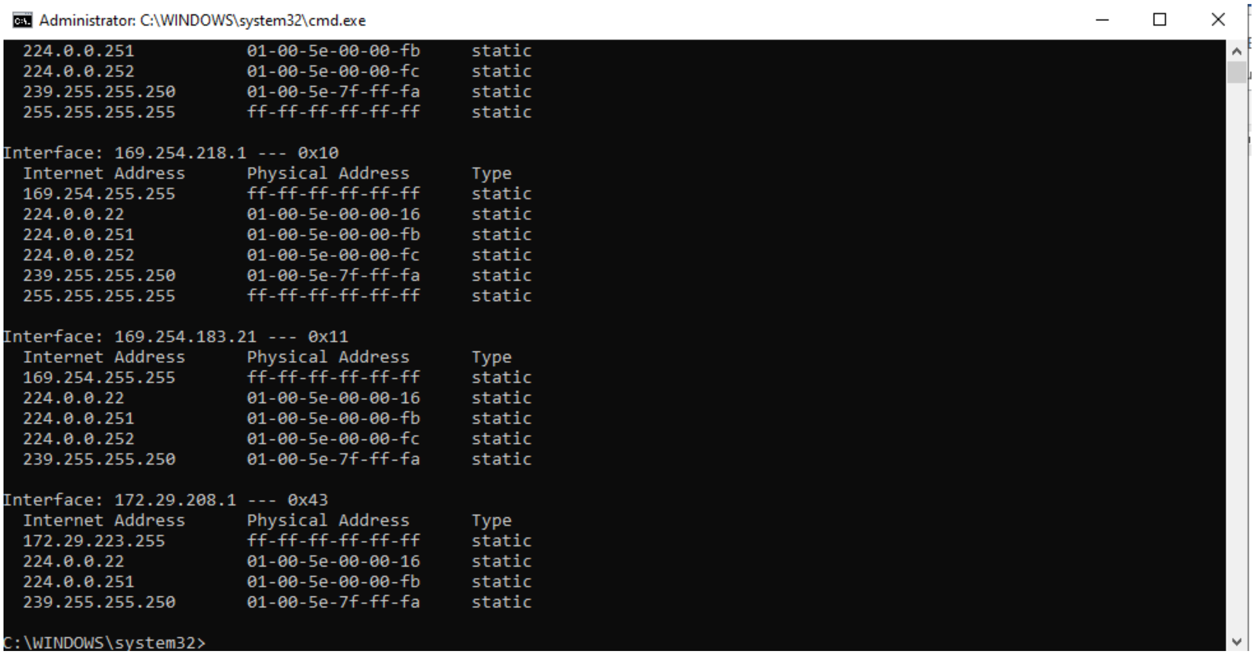
2. The Address Resolution Protocol

ARP Caching

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

ANSWER:

Internet Address column contains the IP address
Physical Address column contains the MAC address,
Type column indicates the protocol type.



```
  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: 169.254.218.1 --- 0x10
  Internet Address      Physical Address      Type
  169.254.255.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     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: 169.254.183.21 --- 0x11
  Internet Address      Physical Address      Type
  169.254.255.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     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

Interface: 172.29.208.1 --- 0x43
  Internet Address      Physical Address      Type
  172.29.223.255        ff-ff-ff-ff-ff-ff     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

C:\WINDOWS\system32>
```

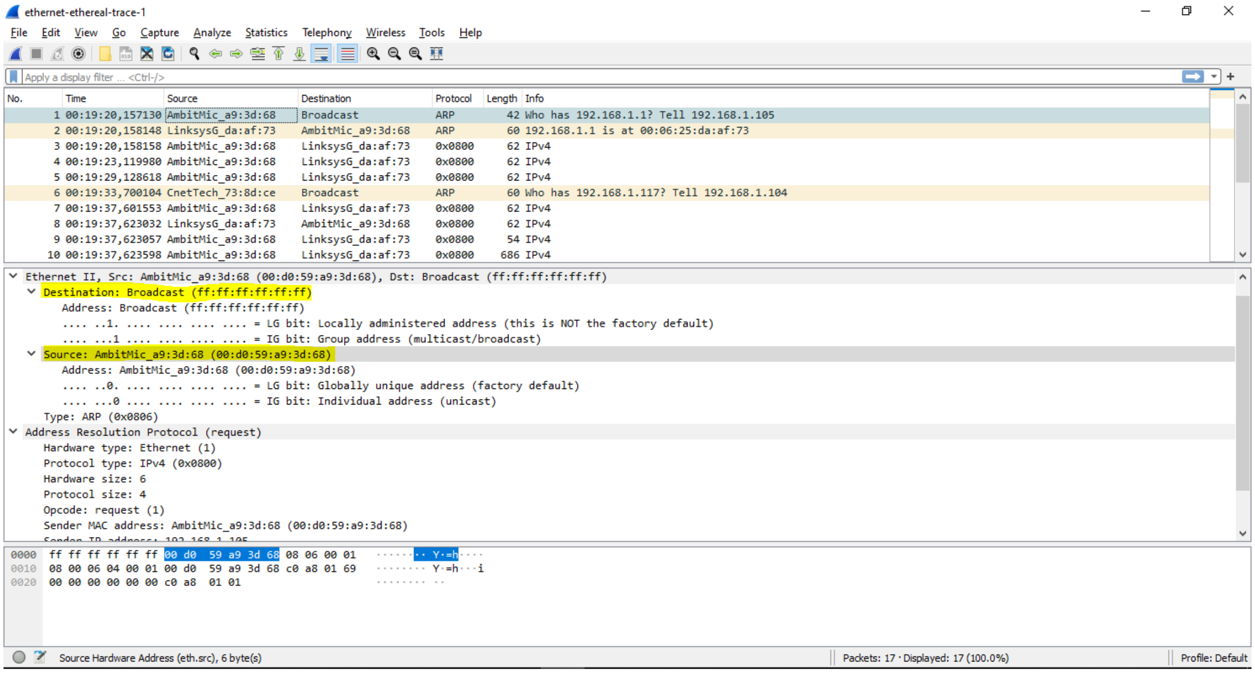
Observing ARP in action

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

ANSWER:

The Source address is 00:d0:59:a9:3d:68

The Destination address is ff:ff:ff:ff:ff:ff



```
No.  Time              Source             Destination        Protocol Length Info
   1 00:19:20,157130 AmbitMic_a9:3d:68  Broadcast          ARP        42 Who has 192.168.1.1? Tell 192.168.1.105
   2 00:19:20,158148 LinksysG_da:af:73  AmbitMic_a9:3d:68  ARP        60 192.168.1.1 is at 00:06:25:da:af:73
   3 00:19:20,158158 AmbitMic_a9:3d:68  LinksysG_da:af:73  0x0800     62 IPv4
   4 00:19:23,119980 AmbitMic_a9:3d:68  LinksysG_da:af:73  0x0800     62 IPv4
   5 00:19:29,128618 AmbitMic_a9:3d:68  LinksysG_da:af:73  0x0800     62 IPv4
   6 00:19:33,700104 CnetTech_73:8d:ce  Broadcast          ARP        60 Who has 192.168.1.117? Tell 192.168.1.104
   7 00:19:37,601553 AmbitMic_a9:3d:68  LinksysG_da:af:73  0x0800     62 IPv4
   8 00:19:37,623032 LinksysG_da:af:73  AmbitMic_a9:3d:68  0x0800     62 IPv4
   9 00:19:37,623057 AmbitMic_a9:3d:68  LinksysG_da:af:73  0x0800     54 IPv4
  10 00:19:37,623598 AmbitMic_a9:3d:68  LinksysG_da:af:73  0x0800    686 IPv4
```

```
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)
    Address: Broadcast (ff:ff:ff:ff:ff:ff)
    .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
    .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
  Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
    Address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  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
```

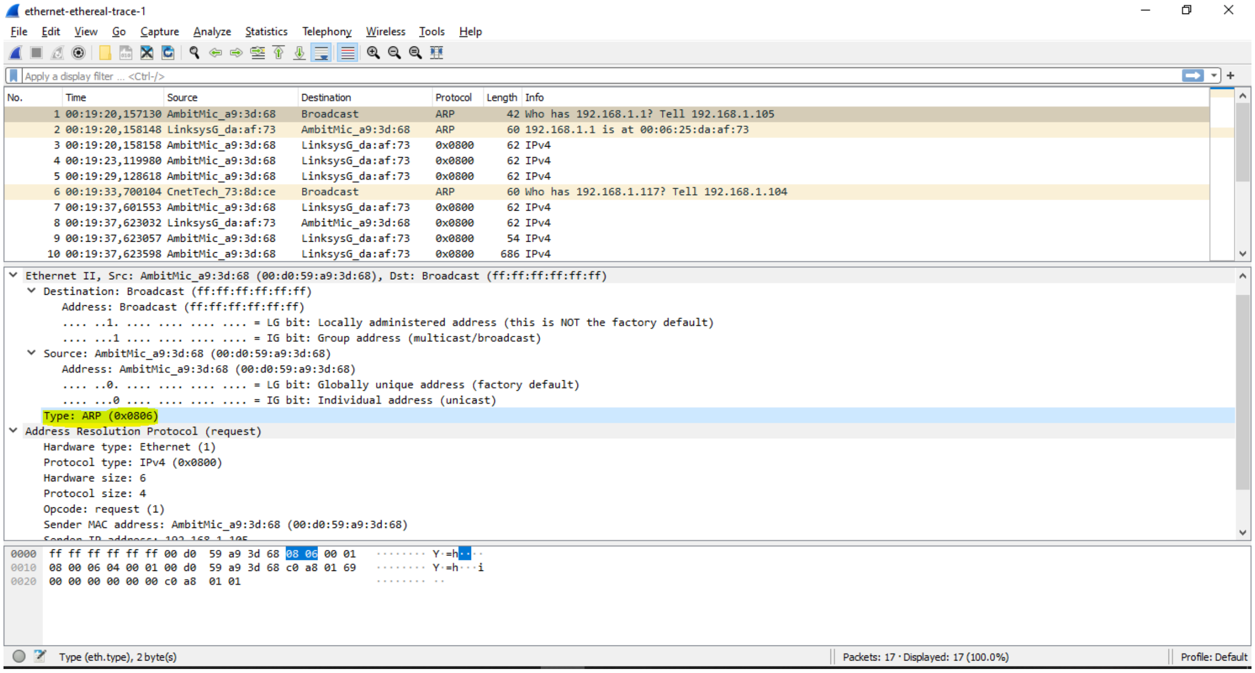
```
0000  ff ff ff ff ff ff 00 d0  59 a9 3d 68 08 06 00 01   ······· Y·=h····
0010  08 00 06 04 00 01 00 d0  59 a9 3d 68 c0 a8 01 69   ········ Y·=h···i
0020  00 00 00 00 00 00 c0 a8  01 01                     ········ ··
```

Source Hardware Address (eth.src), 6 byte(s)   Packets: 17 · Displayed: 17 (100.0%)   Profile: Default

<u>Question 11:</u> 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 0x00000806
The corresponding 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-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	00:19:20,157130	AmbitMic_a9:3d:68	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.105
2	00:19:20,158148	LinksysG_da:af:73	AmbitMic_a9:3d:68	ARP	60	192.168.1.1 is at 00:06:25:da:af:73
3	00:19:20,158158	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
4	00:19:23,119980	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
5	00:19:29,128618	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
6	00:19:33,700104	CnetTech_73:8d:ce	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
7	00:19:37,601553	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	62	IPv4
8	00:19:37,623032	LinksysG_da:af:73	AmbitMic_a9:3d:68	0x0800	62	IPv4
9	00:19:37,623057	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	54	IPv4
10	00:19:37,623598	AmbitMic_a9:3d:68	LinksysG_da:af:73	0x0800	686	IPv4

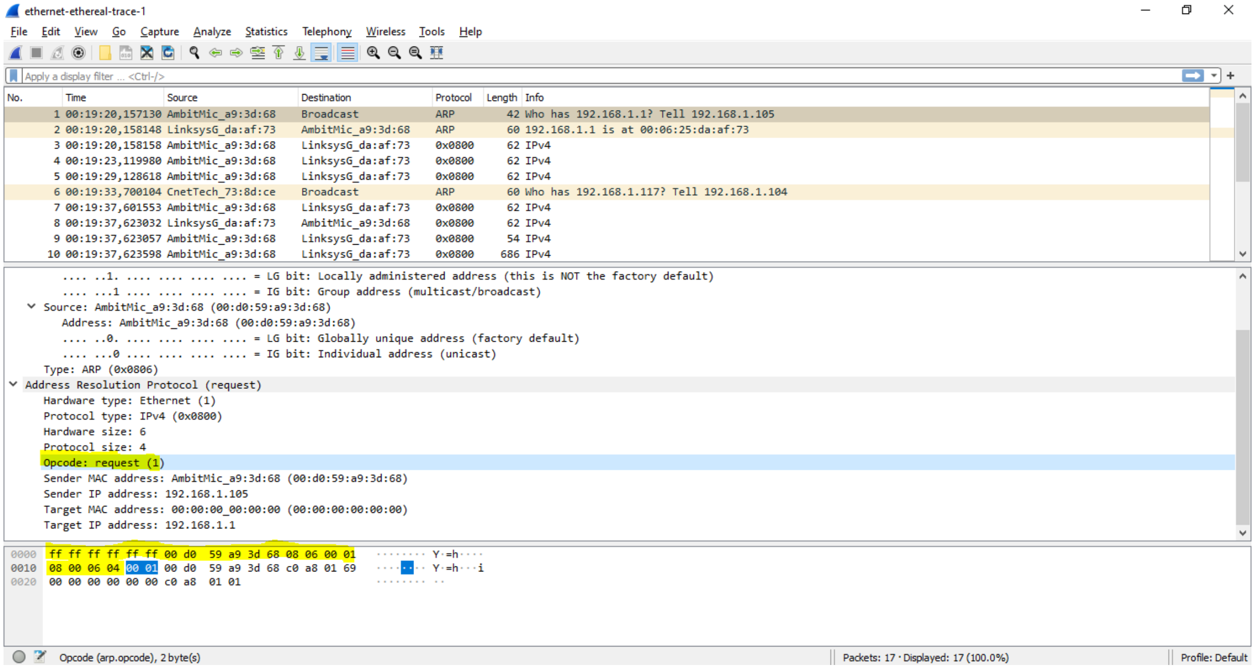
```
Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    Address: Broadcast (ff:ff:ff:ff:ff:ff)
    .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
    .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
  Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
    Address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  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
```

```
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 00 c0 a8  01 01                     ········ ··
```

Type (eth.type), 2 byte(s)
Packets: 17 · Displayed: 17 (100.0%)
Profile: Default

<u>Question 12:</u>

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-/>

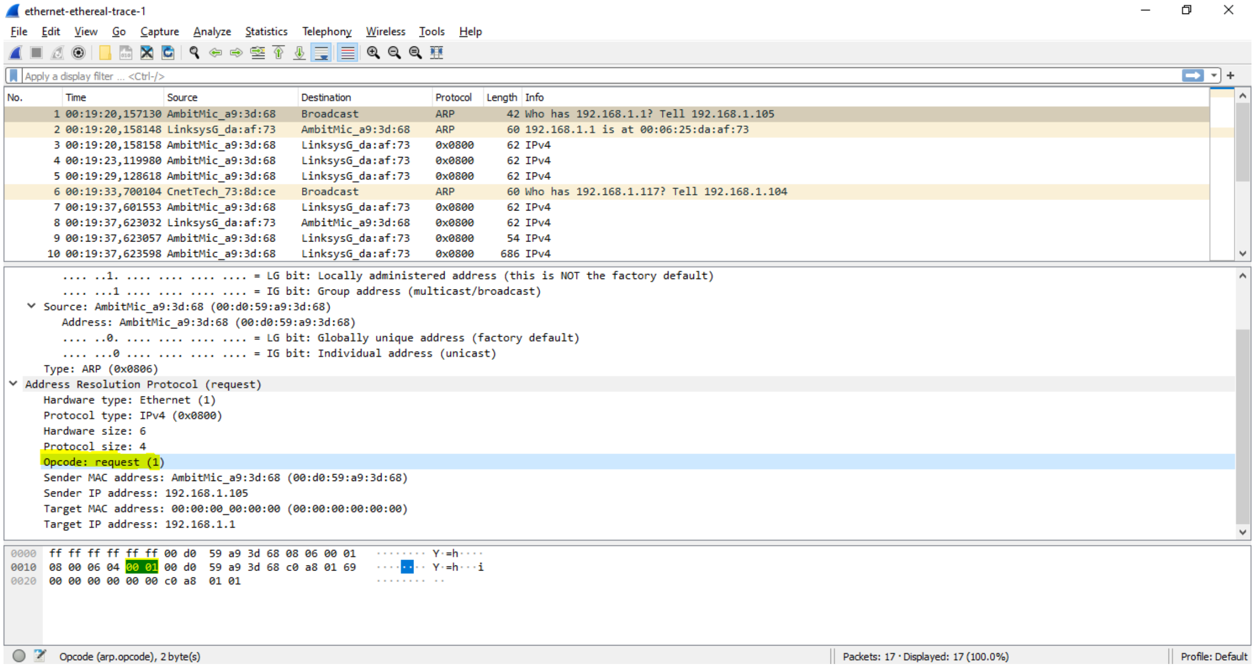
```
No.  Time             Source             Destination        Protocol Length Info
   1 00:19:20,157130 AmbitMic_a9:3d:68  Broadcast          ARP        42 Who has 192.168.1.1? Tell 192.168.1.105
   2 00:19:20,158148 LinksysG_da:af:73  AmbitMic_a9:3d:68  ARP        60 192.168.1.1 is at 00:06:25:da:af:73
   3 00:19:20,158158 AmbitMic_a9:3d:68  LinksysG_da:af:73  0x0800     62 IPv4
   4 00:19:23,119980 AmbitMic_a9:3d:68  LinksysG_da:af:73  0x0800     62 IPv4
   5 00:19:29,128618 AmbitMic_a9:3d:68  LinksysG_da:af:73  0x0800     62 IPv4
   6 00:19:33,700104 CnetTech_73:8d:ce  Broadcast          ARP        60 Who has 192.168.1.117? Tell 192.168.1.104
   7 00:19:37,601553 AmbitMic_a9:3d:68  LinksysG_da:af:73  0x0800     62 IPv4
   8 00:19:37,623032 LinksysG_da:af:73  AmbitMic_a9:3d:68  0x0800     62 IPv4
   9 00:19:37,623057 AmbitMic_a9:3d:68  LinksysG_da:af:73  0x0800     54 IPv4
  10 00:19:37,623598 AmbitMic_a9:3d:68  LinksysG_da:af:73  0x0800    686 IPv4
```

```
        .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
        .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
    Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
        Address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    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 00 c0 a8  01 01                     ········ ··
```

Opcode (arp.opcode), 2 byte(s) | 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

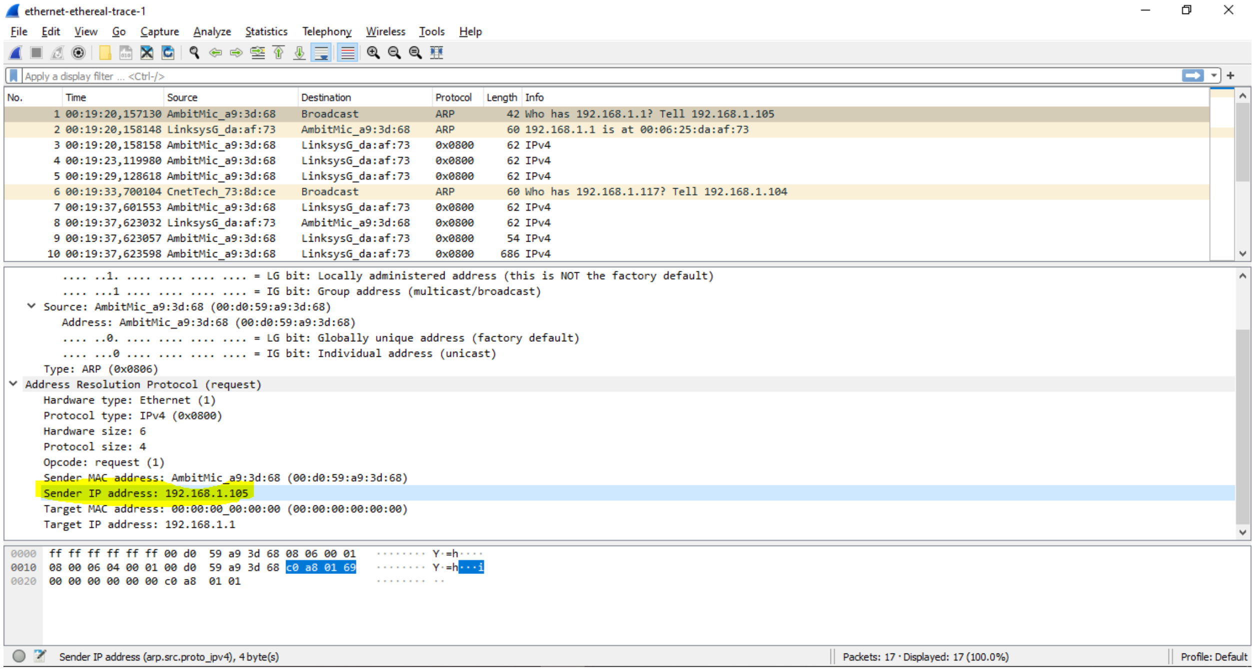
```
No.  Time             Source             Destination        Protocol Length Info
   1 00:19:20,157130 AmbitMic_a9:3d:68  Broadcast          ARP        42 Who has 192.168.1.1? Tell 192.168.1.105
   2 00:19:20,158148 LinksysG_da:af:73  AmbitMic_a9:3d:68  ARP        60 192.168.1.1 is at 00:06:25:da:af:73
   3 00:19:20,158158 AmbitMic_a9:3d:68  LinksysG_da:af:73  0x0800     62 IPv4
   4 00:19:23,119980 AmbitMic_a9:3d:68  LinksysG_da:af:73  0x0800     62 IPv4
   5 00:19:29,128618 AmbitMic_a9:3d:68  LinksysG_da:af:73  0x0800     62 IPv4
   6 00:19:33,700104 CnetTech_73:8d:ce  Broadcast          ARP        60 Who has 192.168.1.117? Tell 192.168.1.104
   7 00:19:37,601553 AmbitMic_a9:3d:68  LinksysG_da:af:73  0x0800     62 IPv4
   8 00:19:37,623032 LinksysG_da:af:73  AmbitMic_a9:3d:68  0x0800     62 IPv4
   9 00:19:37,623057 AmbitMic_a9:3d:68  LinksysG_da:af:73  0x0800     54 IPv4
  10 00:19:37,623598 AmbitMic_a9:3d:68  LinksysG_da:af:73  0x0800    686 IPv4
```

```
        .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
        .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
    Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
        Address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    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 00 c0 a8  01 01                     ········ ··
```

Opcode (arp.opcode), 2 byte(s) | Packets: 17 · Displayed: 17 (100.0%) | Profile: Default

c) Does the ARP message contain the IP address of the sender?
Yes
The ARP message contains the IP address 192.168.1.105


ethernet-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

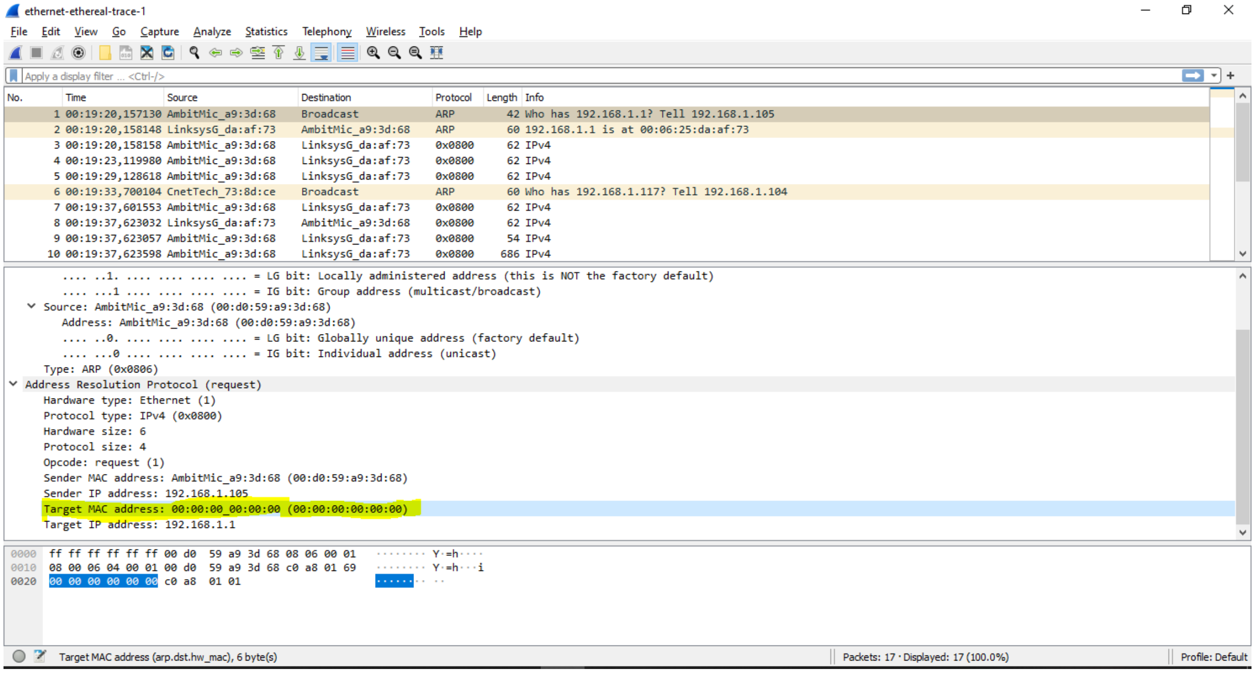
```
No.  Time              Source              Destination        Protocol Length Info
   1 00:19:20,157130 AmbitMic_a9:3d:68   Broadcast          ARP        42 Who has 192.168.1.1? Tell 192.168.1.105
   2 00:19:20,158148 LinksysG_da:af:73   AmbitMic_a9:3d:68  ARP        60 192.168.1.1 is at 00:06:25:da:af:73
   3 00:19:20,158158 AmbitMic_a9:3d:68   LinksysG_da:af:73  0x0800     62 IPv4
   4 00:19:23,119980 AmbitMic_a9:3d:68   LinksysG_da:af:73  0x0800     62 IPv4
   5 00:19:29,128618 AmbitMic_a9:3d:68   LinksysG_da:af:73  0x0800     62 IPv4
   6 00:19:33,700104 CnetTech_73:8d:ce   Broadcast          ARP        60 Who has 192.168.1.117? Tell 192.168.1.104
   7 00:19:37,601553 AmbitMic_a9:3d:68   LinksysG_da:af:73  0x0800     62 IPv4
   8 00:19:37,623032 LinksysG_da:af:73   AmbitMic_a9:3d:68  0x0800     62 IPv4
   9 00:19:37,623057 AmbitMic_a9:3d:68   LinksysG_da:af:73  0x0800     54 IPv4
  10 00:19:37,623598 AmbitMic_a9:3d:68   LinksysG_da:af:73  0x0800    686 IPv4
```

```
        .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
        .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
    Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
        Address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    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 00 c0 a8  01 01                     ········ ··
```

Sender IP address (arp.src.proto_ipv4), 4 byte(s) | 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?
In the field Target MAC address 00:00:00:00:00:00


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 00:19:20,157130 AmbitMic_a9:3d:68   Broadcast          ARP        42 Who has 192.168.1.1? Tell 192.168.1.105
   2 00:19:20,158148 LinksysG_da:af:73   AmbitMic_a9:3d:68  ARP        60 192.168.1.1 is at 00:06:25:da:af:73
   3 00:19:20,158158 AmbitMic_a9:3d:68   LinksysG_da:af:73  0x0800     62 IPv4
   4 00:19:23,119980 AmbitMic_a9:3d:68   LinksysG_da:af:73  0x0800     62 IPv4
   5 00:19:29,128618 AmbitMic_a9:3d:68   LinksysG_da:af:73  0x0800     62 IPv4
   6 00:19:33,700104 CnetTech_73:8d:ce   Broadcast          ARP        60 Who has 192.168.1.117? Tell 192.168.1.104
   7 00:19:37,601553 AmbitMic_a9:3d:68   LinksysG_da:af:73  0x0800     62 IPv4
   8 00:19:37,623032 LinksysG_da:af:73   AmbitMic_a9:3d:68  0x0800     62 IPv4
   9 00:19:37,623057 AmbitMic_a9:3d:68   LinksysG_da:af:73  0x0800     54 IPv4
  10 00:19:37,623598 AmbitMic_a9:3d:68   LinksysG_da:af:73  0x0800    686 IPv4
```

```
        .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
        .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
    Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
        Address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    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
```

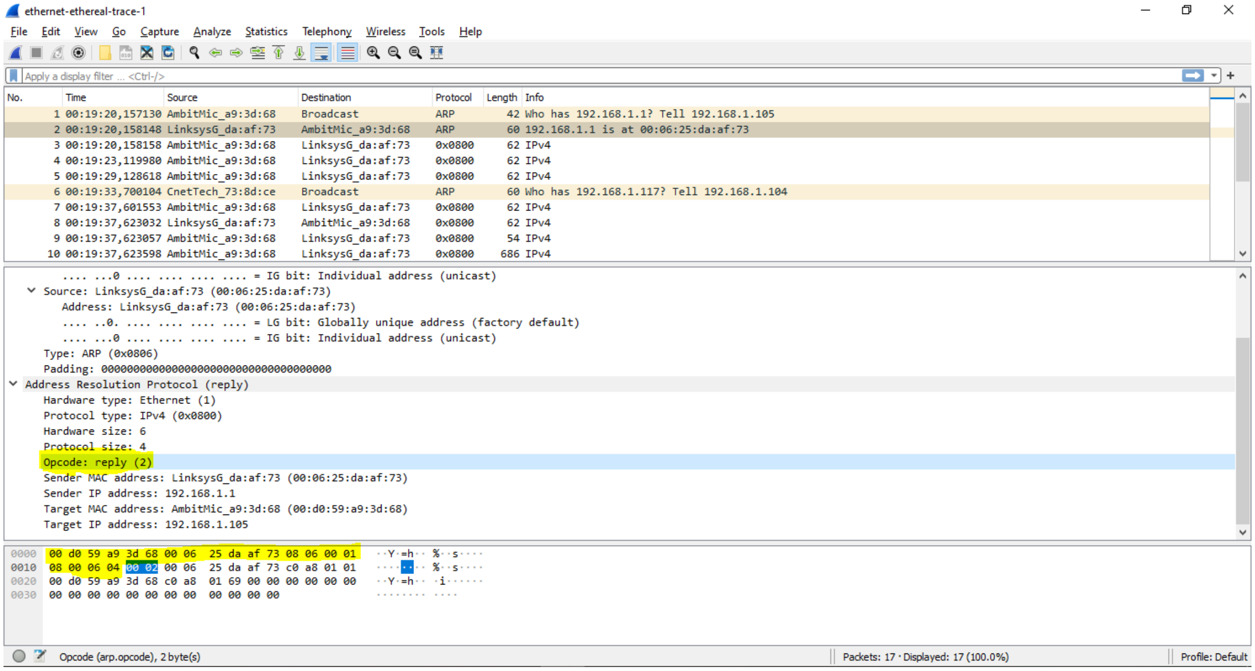
```
0000  ff ff ff ff ff ff 00 d0  59 a9 3d 68 08 06 00 01   ········ Y·=h····
0010  08 00 06 04 00 01 00 d0  59 a9 3d 68 c0 a8 01 69   ········ Y·=h···i
0020  00 00 00 00 00 00 c0 a8  01 01                     ········ ··
```

Target MAC address (arp.dst.hw_mac), 6 byte(s) | Packets: 17 · Displayed: 17 (100.0%) | Profile: Default

Question 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


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 00:19:20,157130 AmbitMic_a9:3d:68  Broadcast          ARP        42 Who has 192.168.1.1? Tell 192.168.1.105
   2 00:19:20,158148 LinksysG_da:af:73  AmbitMic_a9:3d:68  ARP        60 192.168.1.1 is at 00:06:25:da:af:73
   3 00:19:20,158158 AmbitMic_a9:3d:68  LinksysG_da:af:73  0x0800     62 IPv4
   4 00:19:23,119980 AmbitMic_a9:3d:68  LinksysG_da:af:73  0x0800     62 IPv4
   5 00:19:29,128618 AmbitMic_a9:3d:68  LinksysG_da:af:73  0x0800     62 IPv4
   6 00:19:33,700104 CnetTech_73:8d:ce  Broadcast          ARP        60 Who has 192.168.1.117? Tell 192.168.1.104
   7 00:19:37,601553 AmbitMic_a9:3d:68  LinksysG_da:af:73  0x0800     62 IPv4
   8 00:19:37,623032 LinksysG_da:af:73  AmbitMic_a9:3d:68  0x0800     62 IPv4
   9 00:19:37,623057 AmbitMic_a9:3d:68  LinksysG_da:af:73  0x0800     54 IPv4
  10 00:19:37,623598 AmbitMic_a9:3d:68  LinksysG_da:af:73  0x0800    686 IPv4
```

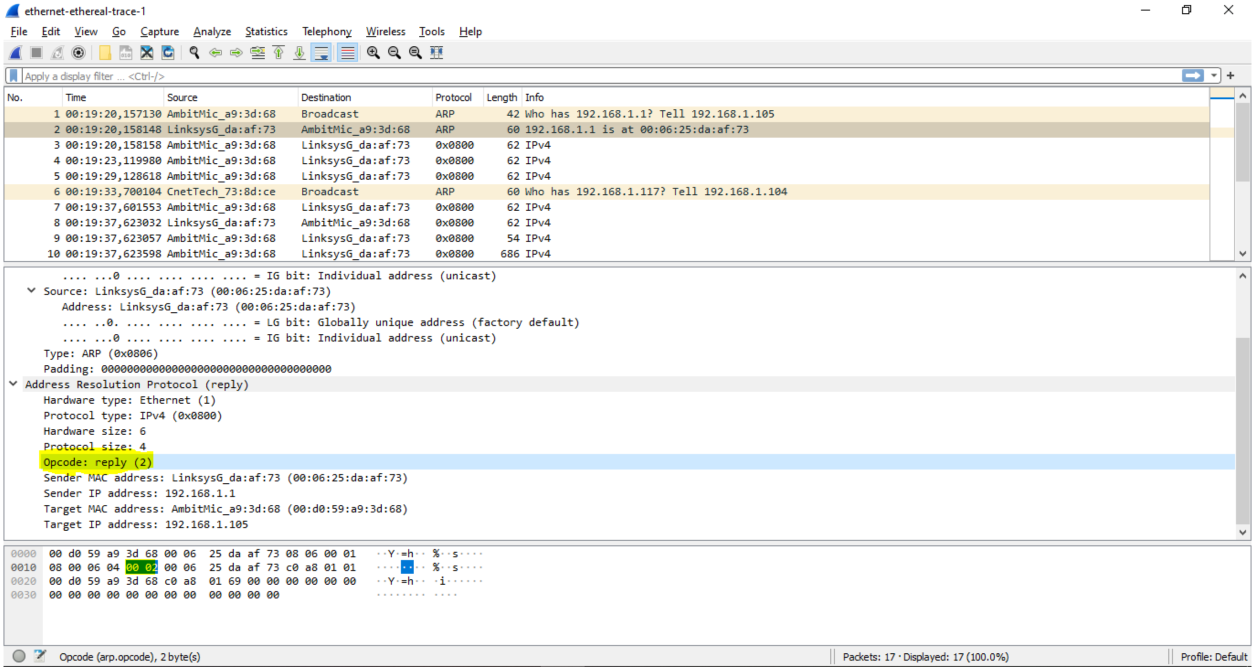
```
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: LinksysG_da:af:73 (00:06:25:da:af:73)
        Address: LinksysG_da:af:73 (00:06:25:da:af:73)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: LinksysG_da:af:73 (00:06:25:da:af:73)
    Sender IP address: 192.168.1.1
    Target MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
    Target IP address: 192.168.1.105
```

```
0000  00 d0 59 a9 3d 68 00 06  25 da af 73 08 06 00 01   ··Y·=h·· %··s····
0010  08 00 06 04 00 02 00 06  25 da af 73 c0 a8 01 01   ········ %··s····
0020  00 d0 59 a9 3d 68 c0 a8  01 69 00 00 00 00 00 00   ··Y·=h·· ·i······
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····
```

Opcode (arp.opcode), 2 byte(s) | 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 response is made?

0x0002


ethernet-ethereal-trace-1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

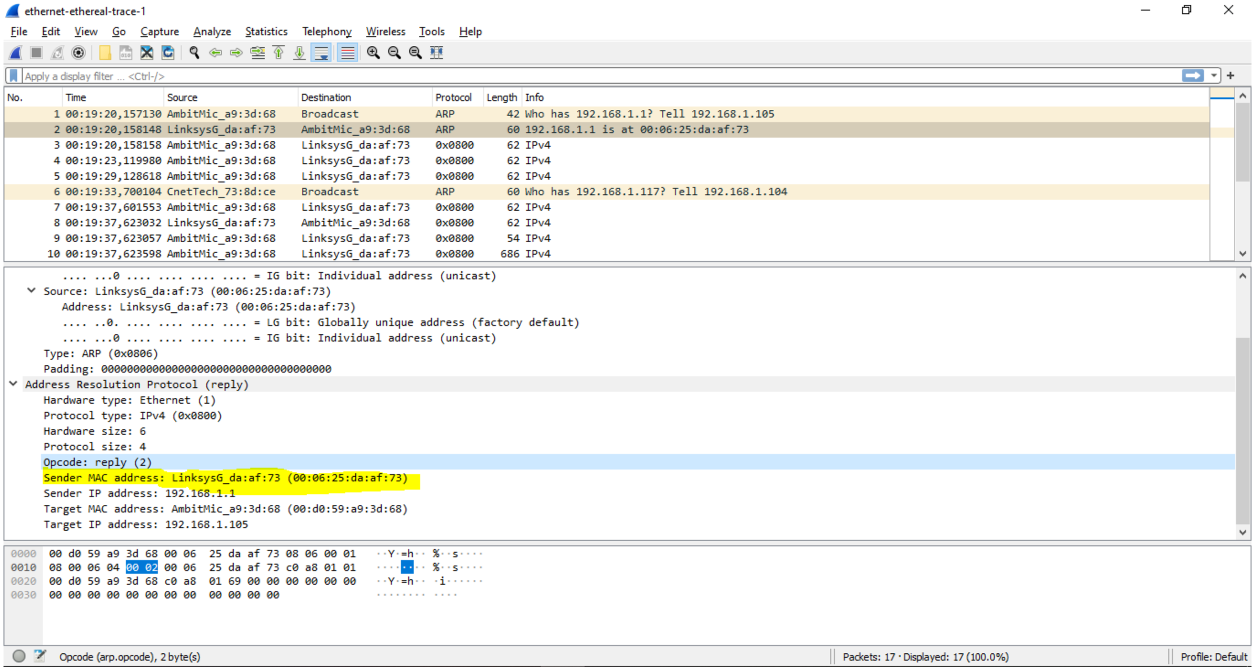
```
No.  Time               Source              Destination         Protocol  Length Info
   1 00:19:20,157130 AmbitMic_a9:3d:68  Broadcast          ARP        42 Who has 192.168.1.1? Tell 192.168.1.105
   2 00:19:20,158148 LinksysG_da:af:73  AmbitMic_a9:3d:68  ARP        60 192.168.1.1 is at 00:06:25:da:af:73
   3 00:19:20,158158 AmbitMic_a9:3d:68  LinksysG_da:af:73  0x0800     62 IPv4
   4 00:19:23,119980 AmbitMic_a9:3d:68  LinksysG_da:af:73  0x0800     62 IPv4
   5 00:19:29,128618 AmbitMic_a9:3d:68  LinksysG_da:af:73  0x0800     62 IPv4
   6 00:19:33,700104 CnetTech_73:8d:ce  Broadcast          ARP        60 Who has 192.168.1.117? Tell 192.168.1.104
   7 00:19:37,601553 AmbitMic_a9:3d:68  LinksysG_da:af:73  0x0800     62 IPv4
   8 00:19:37,623032 LinksysG_da:af:73  AmbitMic_a9:3d:68  0x0800     62 IPv4
   9 00:19:37,623057 AmbitMic_a9:3d:68  LinksysG_da:af:73  0x0800     54 IPv4
  10 00:19:37,623598 AmbitMic_a9:3d:68  LinksysG_da:af:73  0x0800    686 IPv4
```

```
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: LinksysG_da:af:73 (00:06:25:da:af:73)
        Address: LinksysG_da:af:73 (00:06:25:da:af:73)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: LinksysG_da:af:73 (00:06:25:da:af:73)
    Sender IP address: 192.168.1.1
    Target MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
    Target IP address: 192.168.1.105
```

```
0000  00 d0 59 a9 3d 68 00 06  25 da af 73 08 06 00 01   ··Y·=h·· %··s····
0010  08 00 06 04 00 02 00 06  25 da af 73 c0 a8 01 01   ········ %··s····
0020  00 d0 59 a9 3d 68 c0 a8  01 69 00 00 00 00 00 00   ··Y·=h·· ·i······
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····
```

Opcode (arp.opcode), 2 byte(s) | Packets: 17 · Displayed: 17 (100.0%) | Profile: Default

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?
Sender MAC Address field


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 00:19:20,157130 AmbitMic_a9:3d:68   Broadcast           ARP         42 Who has 192.168.1.1? Tell 192.168.1.105
   2 00:19:20,158148 LinksysG_da:af:73   AmbitMic_a9:3d:68   ARP         60 192.168.1.1 is at 00:06:25:da:af:73
   3 00:19:20,158158 AmbitMic_a9:3d:68   LinksysG_da:af:73   0x0800      62 IPv4
   4 00:19:23,119980 AmbitMic_a9:3d:68   LinksysG_da:af:73   0x0800      62 IPv4
   5 00:19:29,128618 AmbitMic_a9:3d:68   LinksysG_da:af:73   0x0800      62 IPv4
   6 00:19:33,700104 CnetTech_73:8d:ce   Broadcast           ARP         60 Who has 192.168.1.117? Tell 192.168.1.104
   7 00:19:37,601553 AmbitMic_a9:3d:68   LinksysG_da:af:73   0x0800      62 IPv4
   8 00:19:37,623032 LinksysG_da:af:73   AmbitMic_a9:3d:68   0x0800      62 IPv4
   9 00:19:37,623057 AmbitMic_a9:3d:68   LinksysG_da:af:73   0x0800      54 IPv4
  10 00:19:37,623598 AmbitMic_a9:3d:68   LinksysG_da:af:73   0x0800     686 IPv4
```

```
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    ˅ Source: LinksysG_da:af:73 (00:06:25:da:af:73)
        Address: LinksysG_da:af:73 (00:06:25:da:af:73)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
˅ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: LinksysG_da:af:73 (00:06:25:da:af:73)
    Sender IP address: 192.168.1.1
    Target MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
    Target IP address: 192.168.1.105
```

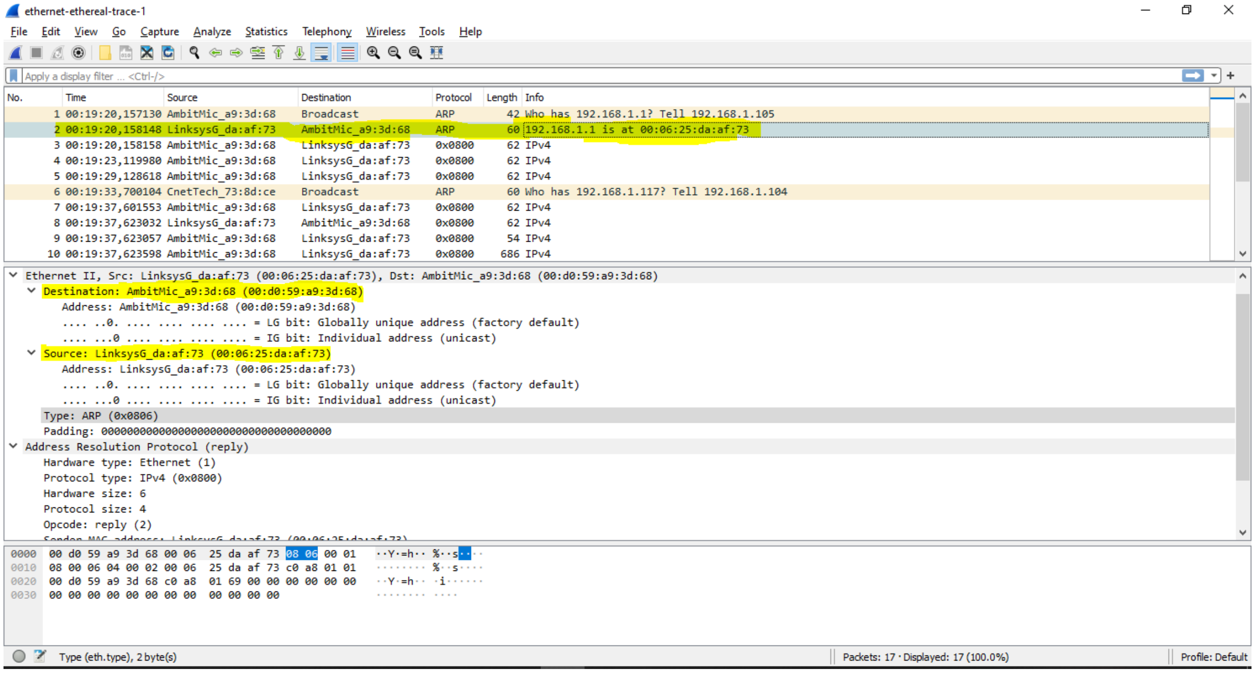
```
0000  00 d0 59 a9 3d 68 00 06  25 da af 73 08 06 00 01   ··Y·=h·· %··s····
0010  08 00 06 04 00 02 00 06  25 da af 73 c0 a8 01 01   ········ %··s····
0020  00 d0 59 a9 3d 68 c0 a8  01 69 00 00 00 00 00 00   ··Y·=h·· ·i······
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····
```

Opcode (arp.opcode), 2 byte(s)
Packets: 17 · Displayed: 17 (100.0%)
Profile: Default

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

ANSWER:

The Source address is 00:06:25:da:af:73
The Destination address is 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-/>

```
No.   Time             Source              Destination         Protocol  Length Info
    1 00:19:20,157130 AmbitMic_a9:3d:68    Broadcast           ARP          42 Who has 192.168.1.1? Tell 192.168.1.105
    2 00:19:20,158148 LinksysG_da:af:73    AmbitMic_a9:3d:68   ARP          60 192.168.1.1 is at 00:06:25:da:af:73
    3 00:19:20,158158 AmbitMic_a9:3d:68    LinksysG_da:af:73   0x0800       62 IPv4
    4 00:19:23,119980 AmbitMic_a9:3d:68    LinksysG_da:af:73   0x0800       62 IPv4
    5 00:19:29,128618 AmbitMic_a9:3d:68    LinksysG_da:af:73   0x0800       62 IPv4
    6 00:19:33,700104 CnetTech_73:8d:ce    Broadcast           ARP          60 Who has 192.168.1.117? Tell 192.168.1.104
    7 00:19:37,601553 AmbitMic_a9:3d:68    LinksysG_da:af:73   0x0800       62 IPv4
    8 00:19:37,623032 LinksysG_da:af:73    AmbitMic_a9:3d:68   0x0800       62 IPv4
    9 00:19:37,623057 AmbitMic_a9:3d:68    LinksysG_da:af:73   0x0800       54 IPv4
   10 00:19:37,623598 AmbitMic_a9:3d:68    LinksysG_da:af:73   0x0800      686 IPv4
```

```
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)
    Address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Source: LinksysG_da:af:73 (00:06:25:da:af:73)
    Address: LinksysG_da:af:73 (00:06:25:da:af:73)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Type: ARP (0x0806)
  Padding: 000000000000000000000000000000000000
Address Resolution Protocol (reply)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: reply (2)
  Sender MAC address: LinksysG_da:af:73 (00:06:25:da:af:73)
```

```
0000  00 d0 59 a9 3d 68 00 06  25 da af 73 08 06 00 01   ··Y·=h·· %··s····
0010  08 00 06 04 00 02 00 06  25 da af 73 c0 a8 01 01   ········ %··s····
0020  00 d0 59 a9 3d 68 c0 a8  01 69 00 00 00 00 00 00   ··Y·=h·· ·i······
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····
```

Type (eth.type), 2 byte(s)
Packets: 17 · Displayed: 17 (100.0%)
Profile: Default

Question 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:

Because we are not at the machine that sent the request.

(The ARP request is broadcast, but **the ARP reply is not broadcast**. The reply will be sent directly to the computer who made the request directly => We can not see it)

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?

ANSWER:

When the adapter/ router received the destination IP address, it would use the ARP to find the correct Ethernet address

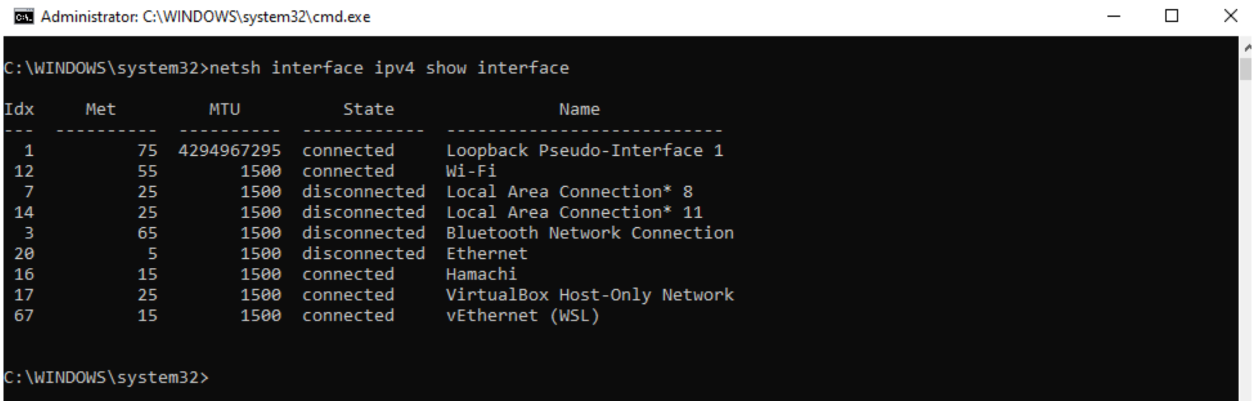
EX-2. What is the default amount of time that an entry remains in your ARP cache before being removed. You can determine this empirically (by monitoring the cache contents) or by looking this up in your operation system documentation. Indicate how/where you determined this value.

ANSWER:

I use cmd looking for this value:

1st: “netsh interface ipv4 show interface”

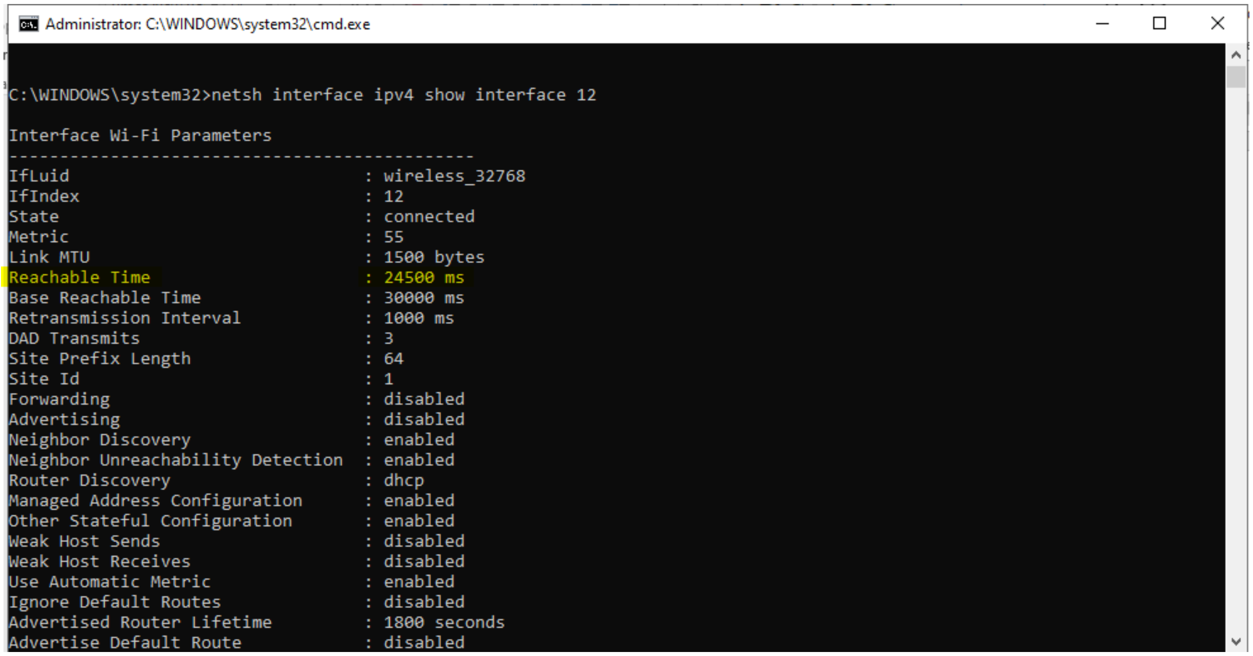
-> Get the interface ID for the required interface (12)



```
C:\WINDOWS\system32>netsh interface ipv4 show interface

Idx     Met         MTU          State                Name
---  ----------  ----------  ------------  ---------------------------
  1          75  4294967295  connected     Loopback Pseudo-Interface 1
 12          55        1500  connected     Wi-Fi
  7          25        1500  disconnected  Local Area Connection* 8
 14          25        1500  disconnected  Local Area Connection* 11
  3          65        1500  disconnected  Bluetooth Network Connection
 20           5        1500  disconnected  Ethernet
 16          15        1500  connected     Hamachi
 17          25        1500  connected     VirtualBox Host-Only Network
 67          15        1500  connected     vEthernet (WSL)


C:\WINDOWS\system32>
```

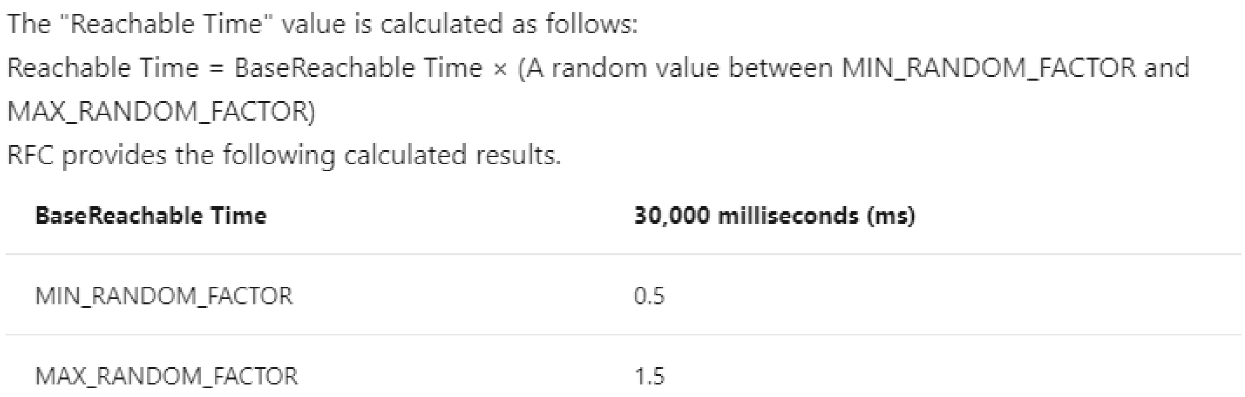
2nd: “netsh interface ipv4 show interface 12”

-> See the "Reachable Time" in the output: **24500ms**



```
C:\WINDOWS\system32>netsh interface ipv4 show interface 12

Interface Wi-Fi Parameters
----------------------------------------------
IfLuid                             : wireless_32768
IfIndex                            : 12
State                              : connected
Metric                             : 55
Link MTU                           : 1500 bytes
Reachable Time                     : 24500 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
```

*Addtion: (from docs.microsoft.com, *Description of Address Resolution Protocol (ARP) caching behavior in TCP/IP implementations)*



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