# Wireshark Lab  -- Ethernet and ARP

Jiaying Li
jl10919

Lab environment:

*Answer:* My PC uses macOS Catalina 10.15.6, shows the following setting with *ifconfig*:

# 1. Capturing and analyzing Ethernet frames

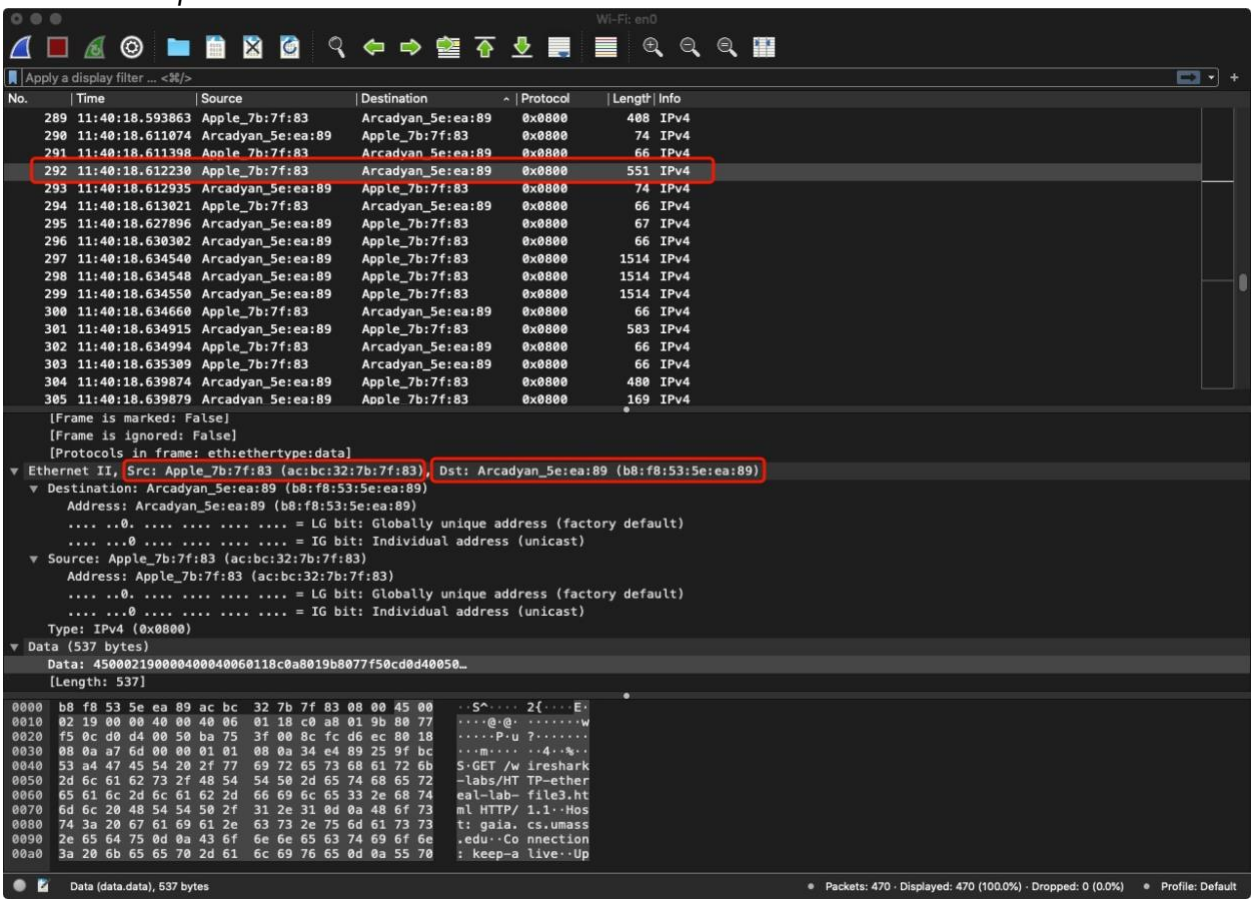
***Packet info of the Get Request:***

No. Time Source Destination Protocol Length Info
292 11:40:18.612230 Apple_7b:7f:83 Arcadyan_5e:ea:89 0x0800 551 IPv4
Frame 292: 551 bytes on wire (4408 bits), 551 bytes captured (4408 bits) on interface en0, id 0
Interface id: 0 (en0)
Encapsulation type: Ethernet (1)
Arrival Time: Dec 1, 2020 11:40:18.612230000 EST
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1606840818.612230000 seconds
[Time delta from previous captured frame: 0.000832000 seconds]
[Time delta from previous displayed frame: 0.000832000 seconds]
[Time since reference or first frame: 2.912282000 seconds]
Frame Number: 292
Frame Length: 551 bytes (4408 bits)
Capture Length: 551 bytes (4408 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:data]
Ethernet II, Src: Apple_7b:7f:83 (ac:bc:32:7b:7f:83), Dst: Arcadyan_5e:ea:89 (b8:f8:53:5e:ea:89)
Destination: Arcadyan_5e:ea:89 (b8:f8:53:5e:ea:89)
Address: Arcadyan_5e:ea:89 (b8:f8:53:5e:ea:89)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Source: Apple_7b:7f:83 (ac:bc:32:7b:7f:83)
Address: Apple_7b:7f:83 (ac:bc:32:7b:7f:83)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Data (537 bytes)

```
0000 45 00 02 19 00 00 40 00 40 06 01 18 c0 a8 01 9b E.....@.@.......
0010 80 77 f5 0c d0 d4 00 50 ba 75 3f 00 8c fc d6 ec .w.....P.u?.....
0020 80 18 08 0a a7 6d 00 00 01 01 08 0a 34 e4 89 25 .....m......4..%
0030 9f bc 53 a4 47 45 54 20 2f 77 69 72 65 73 68 61 ..S.GET /wiresha
0040 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 65 74 68 rk-labs/HTTP-eth
0050 65 72 65 61 6c 2d 6c 61 62 2d 66 69 6c 65 33 2e ereal-lab-file3.
0060 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 0a 48 html HTTP/1.1..H
0070 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 6d 61 ost: gaia.cs.uma
0080 73 73 2e 65 64 75 0d 0a 43 6f 6e 6e 65 63 74 69 ss.edu..Connecti
0090 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a on: keep-alive..
00a0 55 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65 Upgrade-Insecure
00b0 2d 52 65 71 75 65 73 74 73 3a 20 31 0d 0a 55 73 -Requests: 1..Us
00c0 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c er-Agent: Mozill
00d0 61 2f 35 2e 30 20 28 4d 61 63 69 6e 74 6f 73 68 a/5.0 (Macintosh
00e0 3b 20 49 6e 74 65 6c 20 4d 61 63 20 4f 53 20 58 ; Intel Mac OS X
00f0 20 31 30 5f 31 35 5f 37 29 20 41 70 70 6c 65 57 10_15_7) AppleW
0100 65 62 4b 69 74 2f 35 33 37 2e 33 36 20 28 4b 48 ebKit/537.36 (KH
0110 54 4d 4c 2c 20 6c 69 6b 65 20 47 65 63 6b 6f 29 TML, like Gecko)
0120 20 43 68 72 6f 6d 65 2f 38 36 2e 30 2e 34 32 34 Chrome/86.0.424
0130 30 2e 31 39 38 20 53 61 66 61 72 69 2f 35 33 37 0.198 Safari/537
0140 2e 33 36 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 .36..Accept: tex
0150 74 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 61 74 69 t/html,applicati
0160 6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 61 70 70 on/xhtml+xml,app
0170 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 lication/xml;q=0
```

0180 2e 39 2c 69 6d 61 67 65 2f 61 76 69 66 2c 69 6d .9,image/avif,im
0190 61 67 65 2f 77 65 62 70 2c 69 6d 61 67 65 2f 61 age/webp,image/a
01a0 70 6e 67 2c 2a 2f 2a 3b 71 3d 30 2e 38 2c 61 70 png,*/*;q=0.8,ap
01b0 70 6c 69 63 61 74 69 6f 6e 2f 73 69 67 6e 65 64 plication/signed
01c0 2d 65 78 63 68 61 6e 67 65 3b 76 3d 62 33 3b 71 -exchange;v=b3;q
01d0 3d 30 2e 39 0d 0a 41 63 63 65 70 74 2d 45 6e 63 =0.9..Accept-Enc
01e0 6f 64 69 6e 67 3a 20 67 7a 69 70 2c 20 64 65 66 oding: gzip, def
01f0 6c 61 74 65 0d 0a 41 63 63 65 70 74 2d 4c 61 6e late..Accept-Lan
0200 67 75 61 67 65 3a 20 65 6e 2d 55 53 2c 65 6e 3b guage: en-US,en;
0210 71 3d 30 2e 39 0d 0a 0d 0a q=0.9....
Data: 450002190000400040060118c0a8019b8077f50cd0d40050…
[Length: 537]

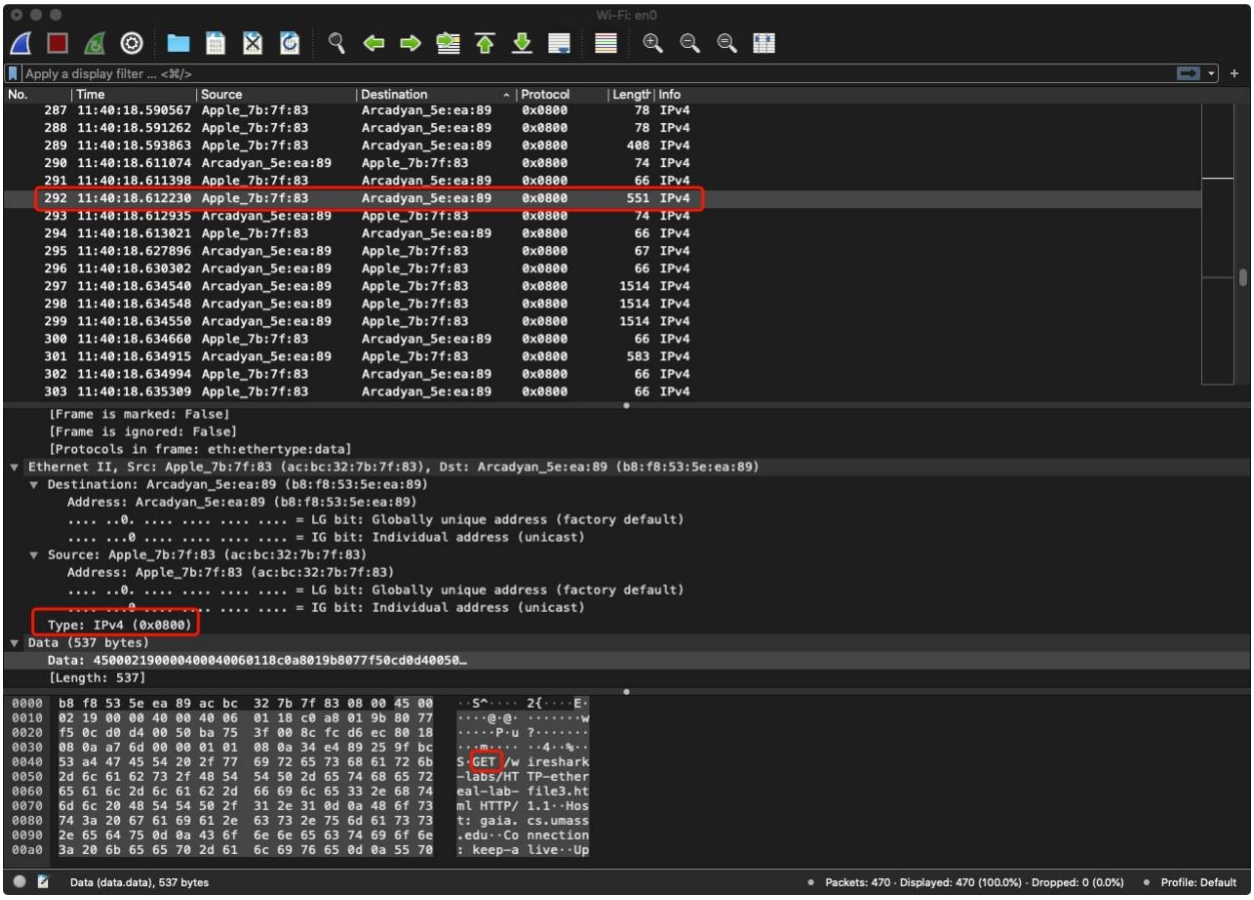
Q1. What is the 48-bit Ethernet address of your computer?
*Answer: As shown in the screenshot below, the 48-bit Ethernet address of my computer(source) is ac:bc:32:7b:7f:83*




Q2. 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.]
*Answer: As shown in the screenshot above, the 48-bit destination address in the Ethernet frame is b8:f8:53:5e:ea:89. It is not the Ethernet address of gaia.cs.umass.edu. Instead it is the address of my Verizon router, and the Manufacturer of this router is Arcadyan Technology Corporation.*

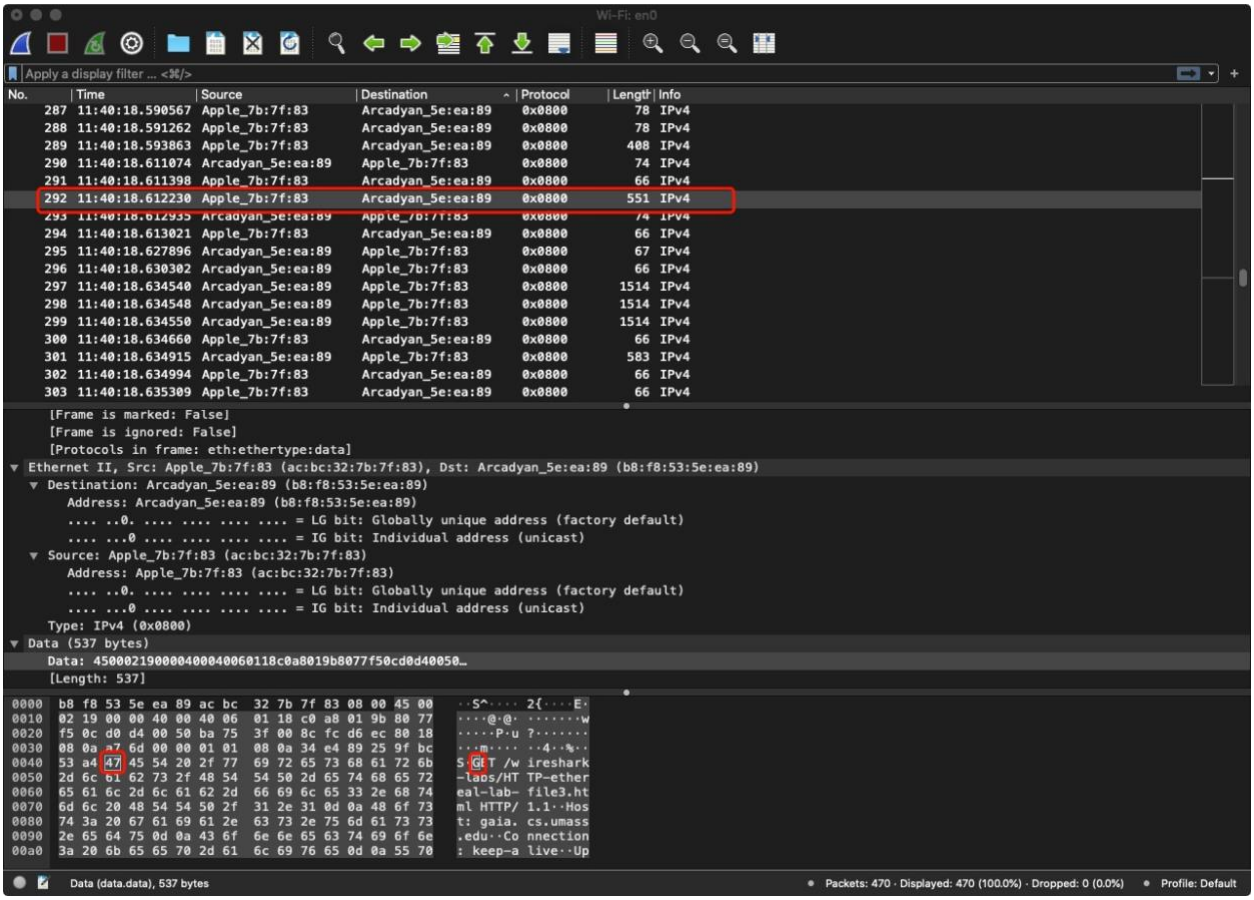
Q3. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

*Answer: As shown in the screenshot below, the hexadecimal value for the two-byte Frame type field is 0x0800, which corresponds to IP(IPv4) protocol. What this filed represents is the upper layer that receive the payload of this Ethernet frame, which is IP.*




Q4. How many bytes from the very start of the Ethernet frame does the ASCII “G” in “GET” appear in the Ethernet frame?

*Answer: As shown in the screenshot below, there are 52 bytes from the very start of the Ethernet frame does the ASCII “G” in “GET” appear in the Ethernet frame.*



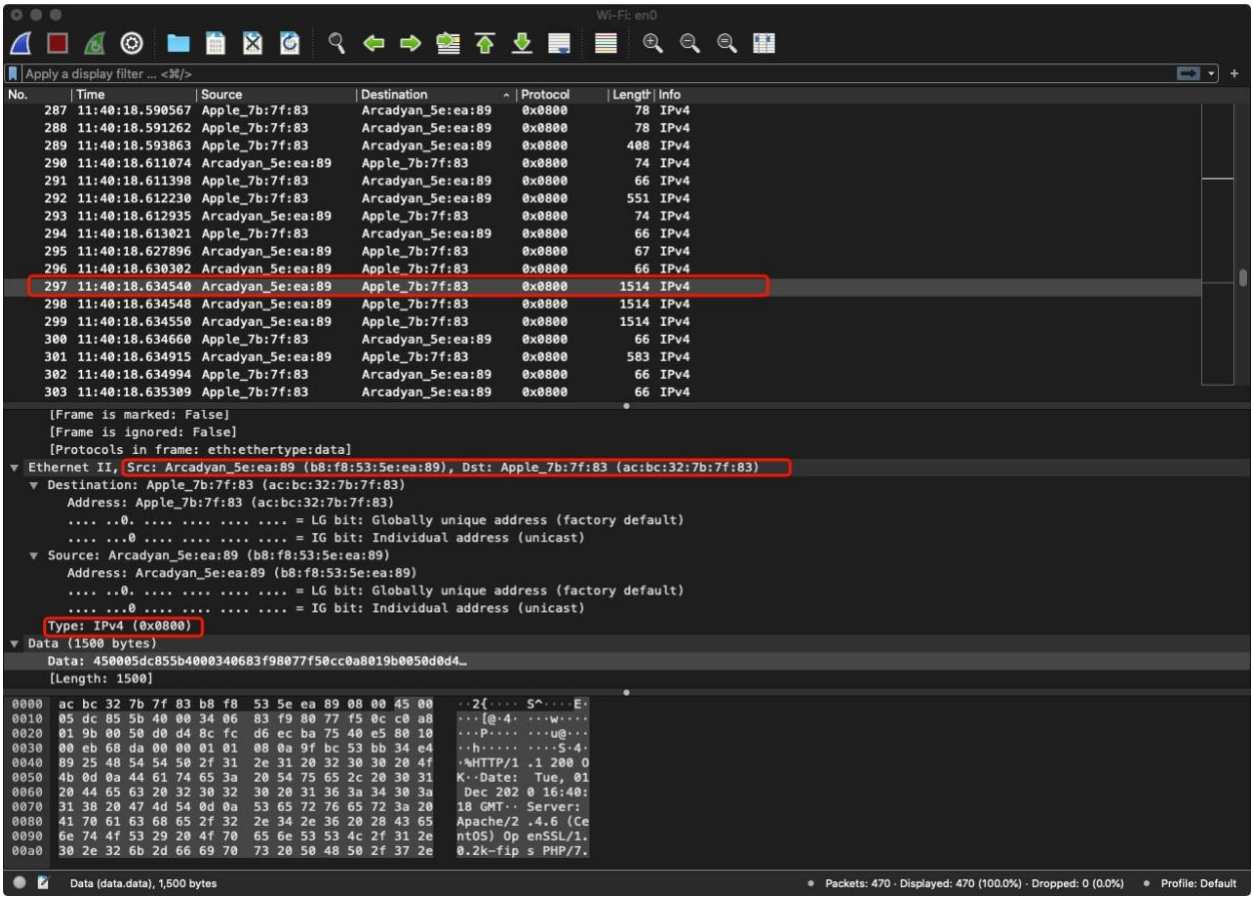

***Packet info of the Get Response:***

No. Time Source Destination Protocol Length Info
297 11:40:18.634540 Arcadyan_5e:ea:89 Apple_7b:7f:83 0x0800 1514 IPv4
Frame 297: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface en0, id 0
Interface id: 0 (en0)
Encapsulation type: Ethernet (1)
Arrival Time: Dec 1, 2020 11:40:18.634540000 EST
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1606840818.634540000 seconds
[Time delta from previous captured frame: 0.004238000 seconds]
[Time delta from previous displayed frame: 0.004238000 seconds]
[Time since reference or first frame: 2.934592000 seconds]
Frame Number: 297
Frame Length: 1514 bytes (12112 bits)
Capture Length: 1514 bytes (12112 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:data]
Ethernet II, Src: Arcadyan_5e:ea:89 (b8:f8:53:5e:ea:89), Dst: Apple_7b:7f:83 (ac:bc:32:7b:7f:83)
Destination: Apple_7b:7f:83 (ac:bc:32:7b:7f:83)
Address: Apple_7b:7f:83 (ac:bc:32:7b:7f:83)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)

Source: Arcadyan_5e:ea:89 (b8:f8:53:5e:ea:89)
Address: Arcadyan_5e:ea:89 (b8:f8:53:5e:ea:89)
.... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
.... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Data (1500 bytes)
0000 45 00 05 dc 85 5b 40 00 34 06 83 f9 80 77 f5 0c E....[@.4....w..
0010 c0 a8 01 9b 00 50 d0 d4 8c fc d6 ec ba 75 40 e5 .....P.......u@.
0020 80 10 00 eb 68 da 00 00 01 01 08 0a 9f bc 53 bb ....h.........S.
0030 34 e4 89 25 48 54 54 50 2f 31 2e 31 20 32 30 30 4..%HTTP/1.1 200
0040 20 4f 4b 0d 0a 44 61 74 65 3a 20 54 75 65 2c 20 OK..Date: Tue,
0050 30 31 20 44 65 63 20 32 30 32 30 20 31 36 3a 34 01 Dec 2020 16:4
0060 30 3a 31 38 20 47 4d 54 0d 0a 53 65 72 76 65 72 0:18 GMT..Server
0070 3a 20 41 70 61 63 68 65 2f 32 2e 34 2e 36 20 28 : Apache/2.4.6 (
0080 43 65 6e 74 4f 53 29 20 4f 70 65 6e 53 53 4c 2f CentOS) OpenSSL/
0090 31 2e 30 2e 32 6b 2d 66 69 70 73 20 50 48 50 2f 1.0.2k-fips PHP/
00a0 37 2e 34 2e 31 32 20 6d 6f 64 5f 70 65 72 6c 2f 7.4.12 mod_perl/
00b0 32 2e 30 2e 31 31 20 50 65 72 6c 2f 76 35 2e 31 2.0.11 Perl/v5.1
00c0 36 2e 33 0d 0a 4c 61 73 74 2d 4d 6f 64 69 66 69 6.3..Last-Modifi
00d0 65 64 3a 20 54 75 65 2c 20 30 31 20 44 65 63 20 ed: Tue, 01 Dec
00e0 32 30 32 30 20 30 36 3a 35 39 3a 30 31 20 47 4d 2020 06:59:01 GM
00f0 54 0d 0a 45 54 61 67 3a 20 22 31 31 39 34 2d 35 T..ETag: "1194-5
0100 62 35 36 31 61 39 35 39 65 64 63 65 22 0d 0a 41 b561a959edce"..A
0110 63 63 65 70 74 2d 52 61 6e 67 65 73 3a 20 62 79 ccept-Ranges: by
0120 74 65 73 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e tes..Content-Len
0130 67 74 68 3a 20 34 35 30 30 0d 0a 4b 65 65 70 2d gth: 4500..Keep-
0140 41 6c 69 76 65 3a 20 74 69 6d 65 6f 75 74 3d 35 Alive: timeout=5
0150 2c 20 6d 61 78 3d 31 30 30 0d 0a 43 6f 6e 6e 65 , max=100..Conne
0160 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 ction: Keep-Aliv
0170 65 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a e..Content-Type:
0180 20 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 text/html; char
0190 73 65 74 3d 55 54 46 2d 38 0d 0a 0d 0a 3c 68 74 set=UTF-8....<ht
01a0 6d 6c 3e 3c 68 65 61 64 3e 20 0a 3c 74 69 74 6c ml><head> .<titl
01b0 65 3e 48 69 73 74 6f 72 69 63 61 6c 20 44 6f 63 e>Historical Doc
01c0 75 6d 65 6e 74 73 3a 54 48 45 20 42 49 4c 4c 20 uments:THE BILL
01d0 4f 46 20 52 49 47 48 54 53 3c 2f 74 69 74 6c 65 OF RIGHTS</title
01e0 3e 3c 2f 68 65 61 64 3e 0a 0a 0a 3c 62 6f 64 79 ></head>...<body
01f0 20 62 67 63 6f 6c 6f 72 3d 22 23 66 66 66 66 66 bgcolor="#fffff
0200 66 22 20 6c 69 6e 6b 3d 22 23 33 33 30 30 30 30 f" link="#330000
0210 22 20 76 6c 69 6e 6b 3d 22 23 36 36 36 36 33 33 " vlink="#666633
0220 22 3e 0a 3c 70 3e 3c 62 72 3e 0a 3c 2f 70 3e 0a ">. <br>. .
0230 3c 70 3e 3c 2f 70 3e 3c 63 65 6e 74 65 72 3e 3c <
0240 62 3e 54 48 45 20 42 49 4c 4c 20 4f 46 20 52 49 b>THE BILL OF RI
0250 47 48 54 53 3c 2f 62 3e 3c 62 72 3e 0a 20 20 3c GHTS</b><br>. <
0260 65 6d 3e 41 6d 65 6e 64 6d 65 6e 74 73 20 31 2d em>Amendments 1-
0270 31 30 20 6f 66 20 74 68 65 20 43 6f 6e 73 74 69 10 of the Consti
0280 74 75 74 69 6f 6e 3c 2f 65 6d 3e 0a 3c 2f 63 65 tution.</ce
0290 6e 74 65 72 3e 0a 0a 3c 70 3e 54 68 65 20 43 6f nter>.. The Co
02a0 6e 76 65 6e 74 69 6f 6e 73 20 6f 66 20 61 20 6e nventions of a n
02b0 75 6d 62 65 72 20 6f 66 20 74 68 65 20 53 74 61 umber of the Sta
02c0 74 65 73 20 68 61 76 69 6e 67 2c 20 61 74 20 74 tes having, at t
02d0 68 65 20 74 69 6d 65 20 6f 66 20 61 64 6f 70 74 he time of adopt
02e0 69 6e 67 0a 74 68 65 20 43 6f 6e 73 74 69 74 75 ing.the Constitu
02f0 74 69 6f 6e 2c 20 65 78 70 72 65 73 73 65 64 20 tion, expressed
0300 61 20 64 65 73 69 72 65 2c 20 69 6e 20 6f 72 64 a desire, in ord
0310 65 72 20 74 6f 20 70 72 65 76 65 6e 74 20 6d 69 er to prevent mi

```
0320 73 63 6f 6e 73 74 72 75 63 74 69 6f 6e 0a 6f 72 sconstruction.or
0330 20 61 62 75 73 65 20 6f 66 20 69 74 73 20 70 6f abuse of its po
0340 77 65 72 73 2c 20 74 68 61 74 20 66 75 72 74 68 wers, that furth
0350 65 72 20 64 65 63 6c 61 72 61 74 6f 72 79 20 61 er declaratory a
0360 6e 64 20 72 65 73 74 72 69 63 74 69 76 65 20 63 nd restrictive c
0370 6c 61 75 73 65 73 0a 73 68 6f 75 6c 64 20 62 65 lauses.should be
0380 20 61 64 64 65 64 2c 20 61 6e 64 20 61 73 20 65 added, and as e
0390 78 74 65 6e 64 69 6e 67 20 74 68 65 20 67 72 6f xtending the gro
03a0 75 6e 64 20 6f 66 20 70 75 62 6c 69 63 20 63 6f und of public co
03b0 6e 66 69 64 65 6e 63 65 20 69 6e 20 74 68 65 0a nfidence in the.
03c0 47 6f 76 65 72 6e 6d 65 6e 74 20 77 69 6c 6c 20 Government will
03d0 62 65 73 74 20 69 6e 73 75 72 65 20 74 68 65 20 best insure the
03e0 62 65 6e 65 66 69 63 65 6e 74 20 65 6e 64 73 20 beneficent ends
03f0 6f 66 20 69 74 73 20 69 6e 73 74 69 74 75 74 69 of its instituti
0400 6f 6e 3b 20 3c 2f 70 3e 3c 70 3e 20 20 52 65 73 on; </p><p> Res
0410 6f 6c 76 65 64 2c 20 62 79 20 74 68 65 20 53 65 olved, by the Se
0420 6e 61 74 65 20 61 6e 64 20 48 6f 75 73 65 20 6f nate and House o
0430 66 20 52 65 70 72 65 73 65 6e 74 61 74 69 76 65 f Representative
0440 73 20 6f 66 20 74 68 65 20 55 6e 69 74 65 64 0a s of the United.
0450 53 74 61 74 65 73 20 6f 66 20 41 6d 65 72 69 63 States of Americ
0460 61 2c 20 69 6e 20 43 6f 6e 67 72 65 73 73 20 61 a, in Congress a
0470 73 73 65 6d 62 6c 65 64 2c 20 74 77 6f 2d 74 68 ssembled, two-th
0480 69 72 64 73 20 6f 66 20 62 6f 74 68 20 48 6f 75 irds of both Hou
0490 73 65 73 20 63 6f 6e 63 75 72 72 69 6e 67 2c 0a ses concurring,.
04a0 74 68 61 74 20 74 68 65 20 66 6f 6c 6c 6f 77 69 that the followi
04b0 6e 67 20 61 72 74 69 63 6c 65 73 20 62 65 20 70 ng articles be p
04c0 72 6f 70 6f 73 65 64 20 74 6f 20 74 68 65 20 4c roposed to the L
04d0 65 67 69 73 6c 61 74 75 72 65 73 20 6f 66 20 74 egislatures of t
04e0 68 65 20 73 65 76 65 72 61 6c 0a 53 74 61 74 65 he several.State
04f0 73 2c 20 61 73 20 61 6d 65 6e 64 6d 65 6e 74 73 s, as amendments
0500 20 74 6f 20 74 68 65 20 43 6f 6e 73 74 69 74 75 to the Constitu
0510 74 69 6f 6e 20 6f 66 20 74 68 65 20 55 6e 69 74 tion of the Unit
0520 65 64 20 53 74 61 74 65 73 3b 20 61 6c 6c 20 6f ed States; all o
0530 72 20 61 6e 79 0a 6f 66 20 77 68 69 63 68 20 61 r any.of which a
0540 72 74 69 63 6c 65 73 2c 20 77 68 65 6e 20 72 61 rticles, when ra
0550 74 69 66 69 65 64 20 62 79 20 74 68 72 65 65 2d tified by three-
0560 66 6f 75 72 74 68 73 20 6f 66 20 74 68 65 20 73 fourths of the s
0570 61 69 64 20 4c 65 67 69 73 6c 61 74 75 72 65 73 aid Legislatures
0580 2c 0a 74 6f 20 62 65 20 76 61 6c 69 64 20 74 6f ,.to be valid to
0590 20 61 6c 6c 20 69 6e 74 65 6e 74 73 20 61 6e 64 all intents and
05a0 20 70 75 72 70 6f 73 65 73 20 61 73 20 70 61 72 purposes as par
05b0 74 20 6f 66 20 74 68 65 20 73 61 69 64 20 43 6f t of the said Co
05c0 6e 73 74 69 74 75 74 69 6f 6e 2c 0a 6e 61 6d 65 nstitution,.name
05d0 6c 79 3a 20 20 20 20 3c 2f 70 3e 3c ly: </p><
Data: 450005dc855b4000340683f98077f50cc0a8019b0050d0d4…
[Length: 1500]
```

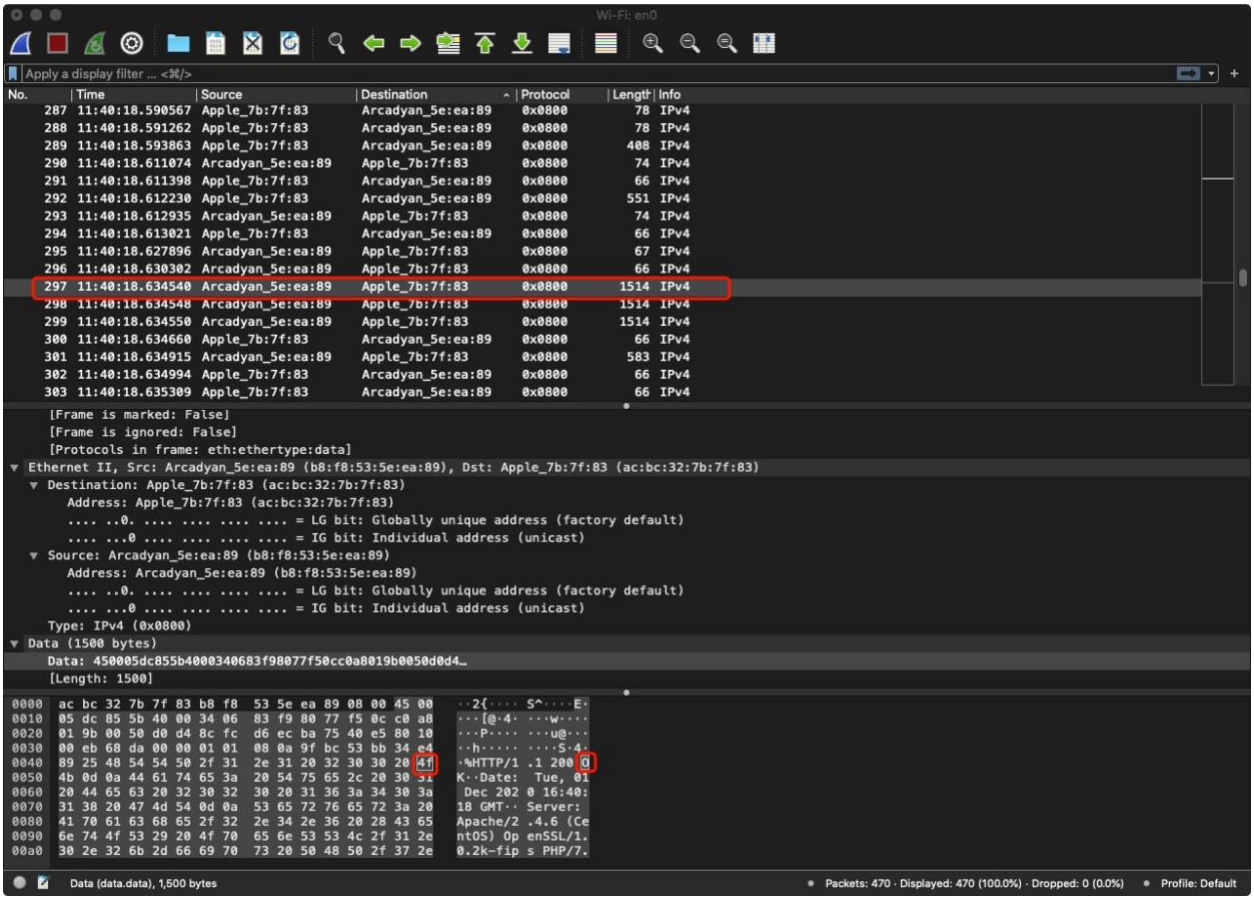
Q5. What is the value of the Ethernet source address? Is this the address of your computer, or of gaia.cs.umass.edu (Hint: the answer is no). What device has this as its Ethernet address?
*Answer: As shown in the screenshot below, the 48-bit Ethernet source address is b8:f8:53:5e:ea:89, it is not my computer or gaia.cs.umass.edu. Instead it is the address of my Verizon router, and the Manufacturer of this router is Arcadyan Technology Corporation.*




Q6. What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?
*Answer: As shown in the screenshot above, the 48-bit Ethernetdestination address is ac:bc:32:7b:7f:83, and it is my computer.*

Q7. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?
*Answer: As shown in the screenshot above, the hexadecimal value for the two-byte Frame type field is 0x0800, which corresponds to IP(IPv4) protocol. What this filed represents is the upper layer that receive the payload of this Ethernet frame, which is IP.*

Q8. 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: As shown in the screenshot below, there are 65 bytes from the very start of the Ethernet frame does the ASCII “O” in “OK” appear in the Ethernet frame.*

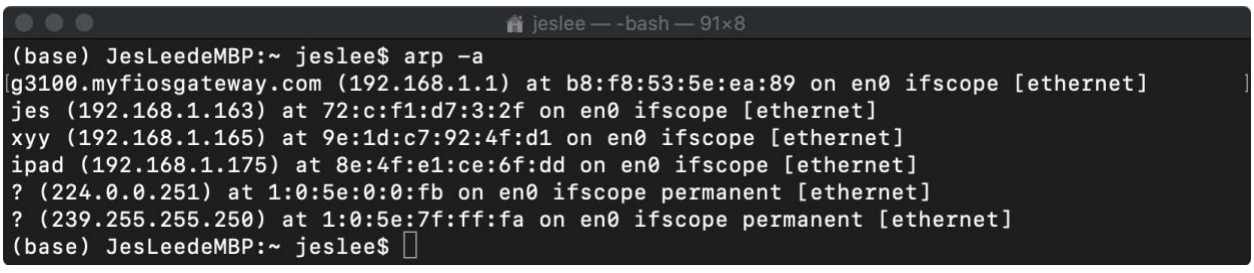



## 2. The Address Resolution Protocol

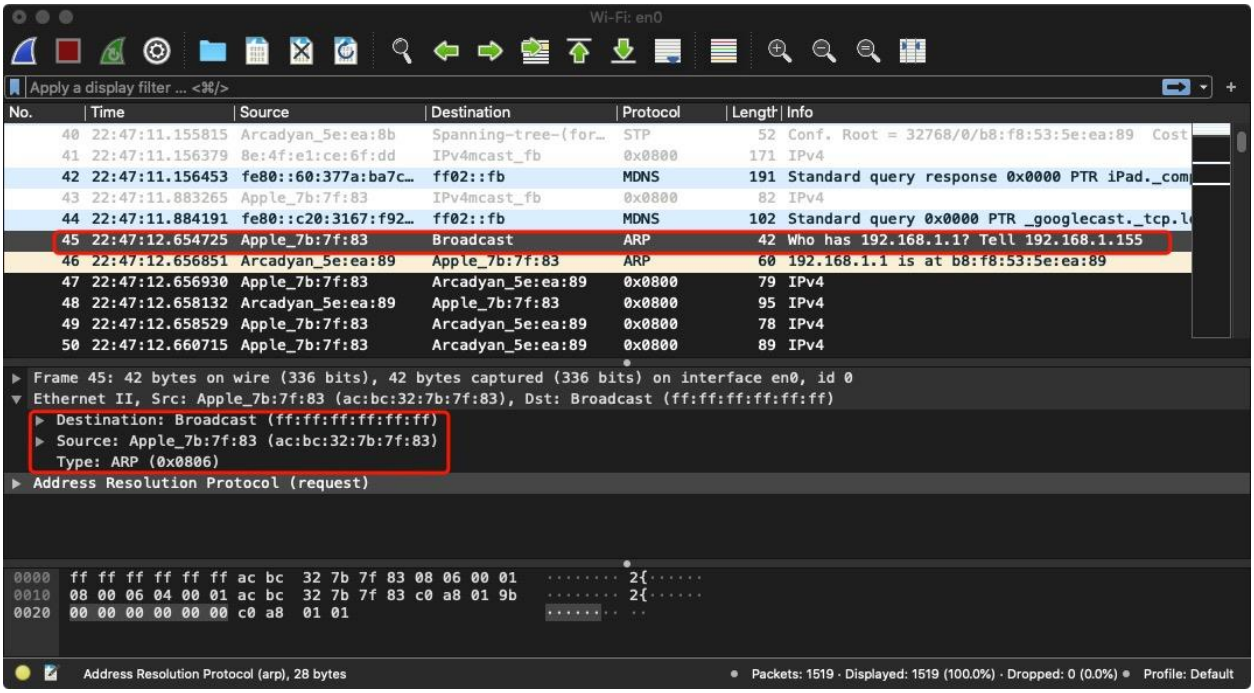
Q9. Write down the contents of your computer's ARP cache. What is the meaning of each column value? The Internet Address column contains the IP address, the Physical Address column contains the MAC address, and the type indicates the protocol type.

*Answer:* As the screenshot shown below, as we can see, the format of the ARP cache table is like:
*HOSTNAME | IP ADDRESS | MAC ADDRESS | INTERFACE | ROUTE COMMAND | ARP CACHE ENTRY STATE | HARDWARE TYPE*

*In this case,*
*HOSTNAME: Show the hostname. If the hostname can't be resolved, you get a '?'*
*ROUTE COMMAND: In this case, ifscope is used to bind a route to a specific interface.*



Q10. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?
*Answer: As the screenshot shown below, hexadecimal values for the source address is ac:bc:32:7b:7f:83 and destination address is ff:ff:ff:ff:ff:ff.*

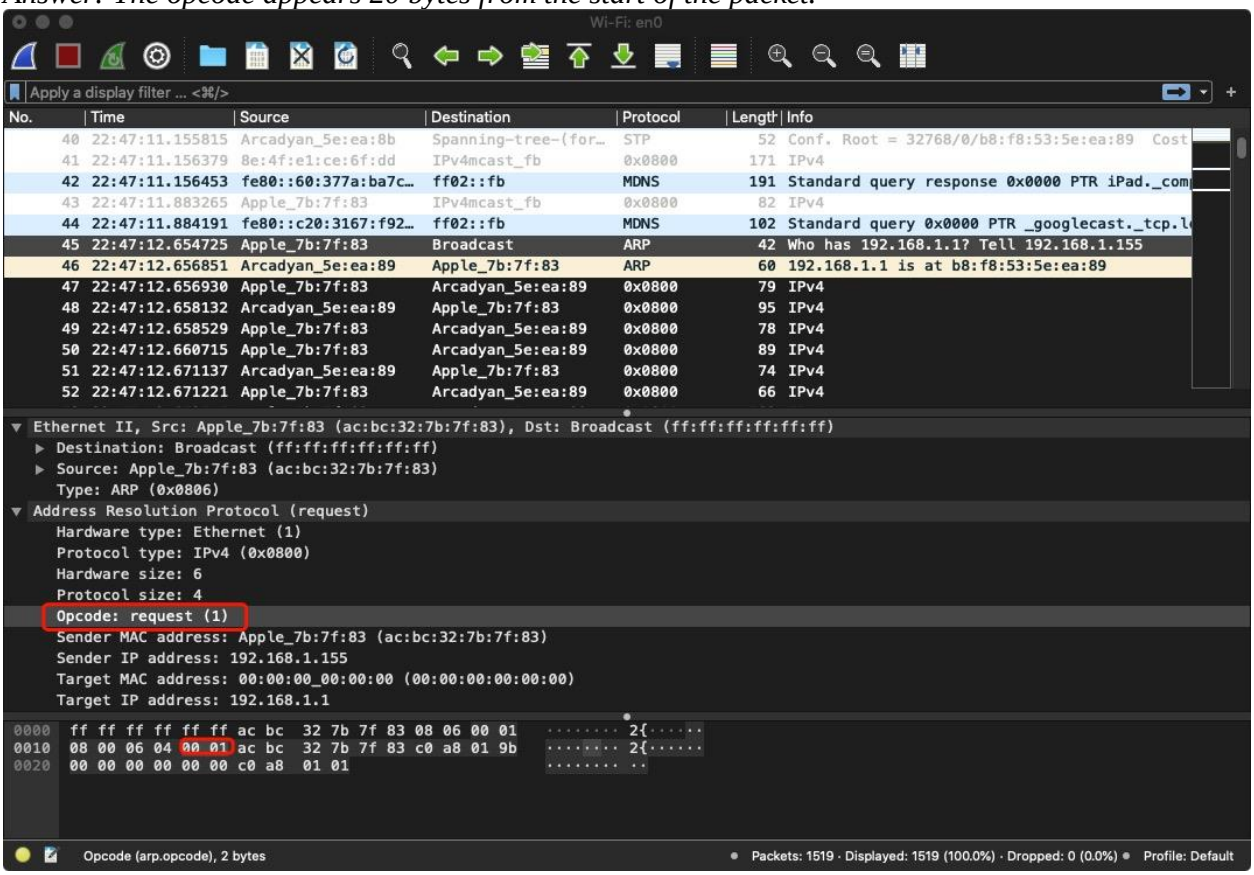



***Packet info of the ARP request:***
No. Time Source Destination Protocol Length Info
45 22:47:12.654725 Apple_7b:7f:83 Broadcast ARP 42 Who has
192.168.1.1? Tell 192.168.1.155
Frame 45: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface en0, id 0
Ethernet II, Src: Apple_7b:7f:83 (ac:bc:32:7b:7f:83), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Destination: Broadcast (ff:ff:ff:ff:ff:ff)
Source: Apple_7b:7f:83 (ac:bc:32:7b:7f:83)
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: Apple_7b:7f:83 (ac:bc:32:7b:7f:83)
Sender IP address: 192.168.1.155
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.1.1

Q11. Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?
*Answer: As the screenshot shown above, the hexadecimal value for the two-byte Ethernet Frame type field is 0x0806. It corresponds to ARP protocol.*

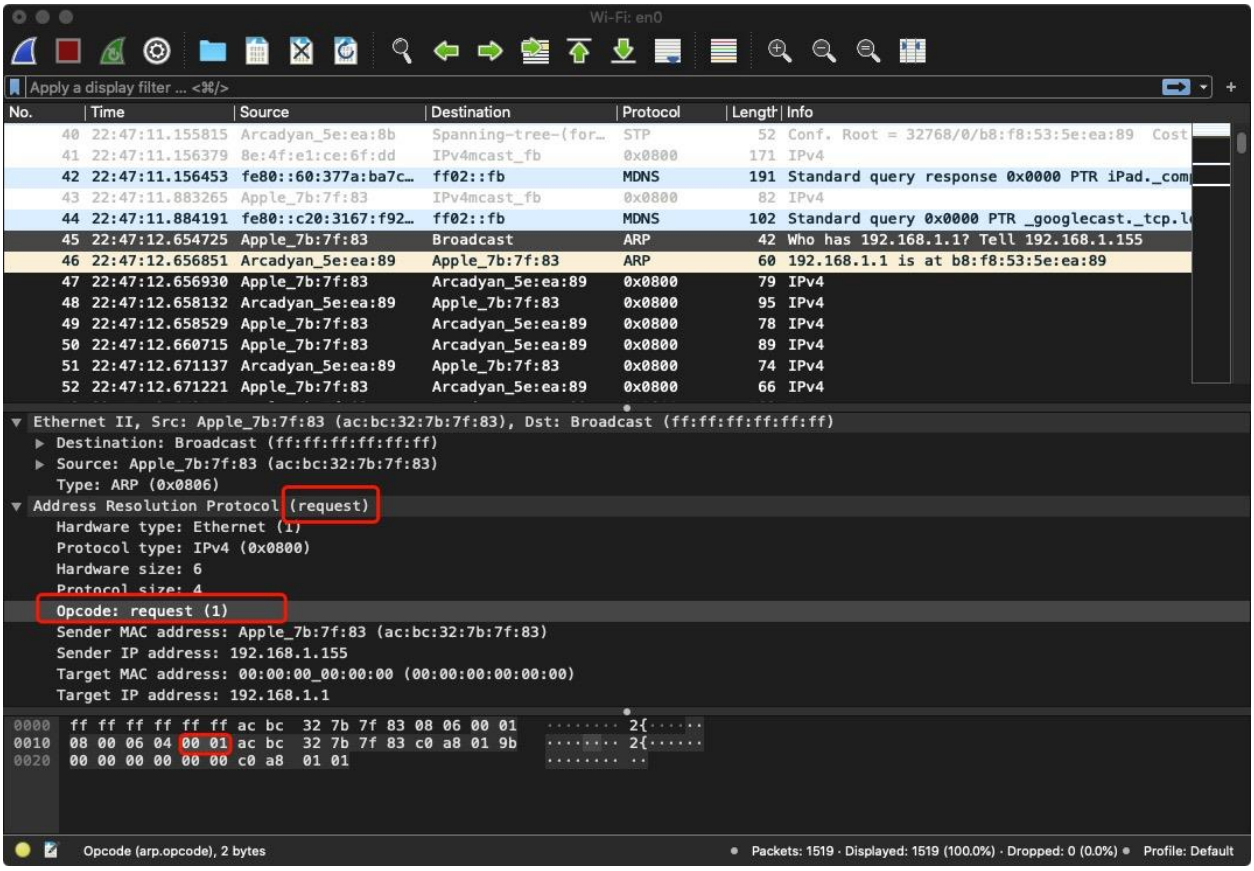
Q12. a) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

*Answer: The opcode appears 20 bytes from the start of the packet.*



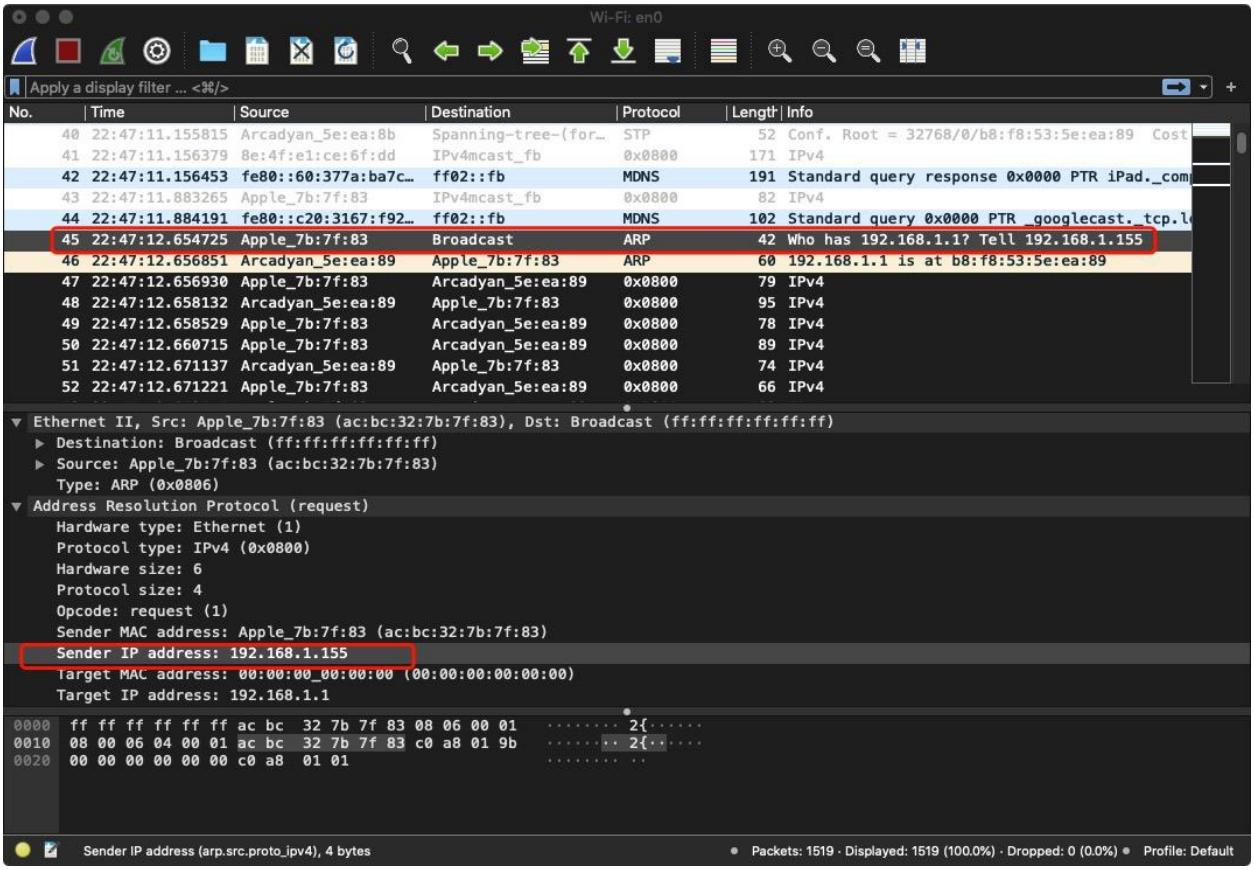

Q12. b) What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP request is made?

*Answer: 0x0001*



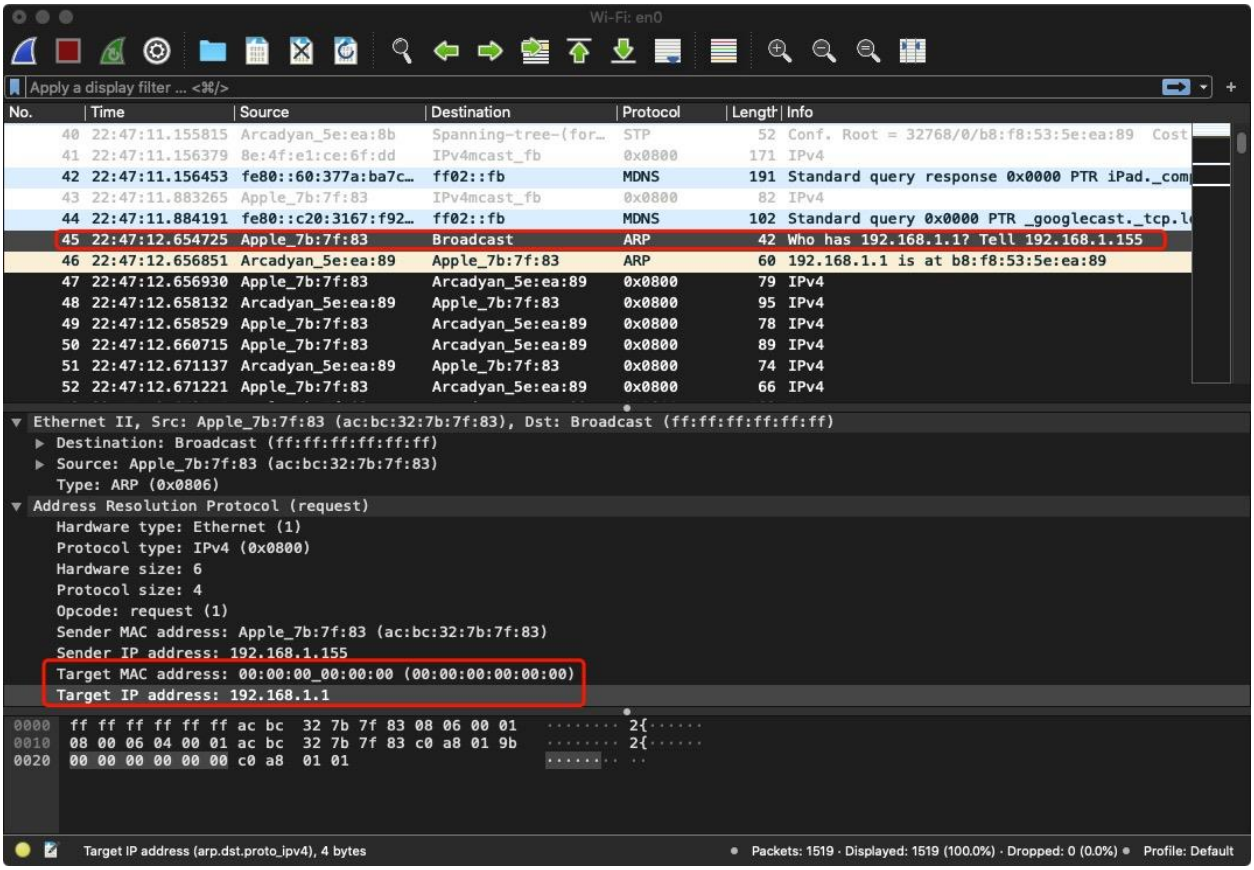

Q12. c) Does the ARP message contain the IP address of the sender?

*Answer: Yes, as the screenshot shown below, in this case, the IP address of the sender is 192.168.1.155.*




Q12. d) Where in the ARP request does the "question" appear – the Ethernet address of the machine whose corresponding IP address is being queried?

*Answer: As shown in the screenshot below, the target MAC address is 00:00:00:00:00:00, to question the device that have IP address as 192.168.1.1, which means device with 192.168.1.1 as IP address is queried.*



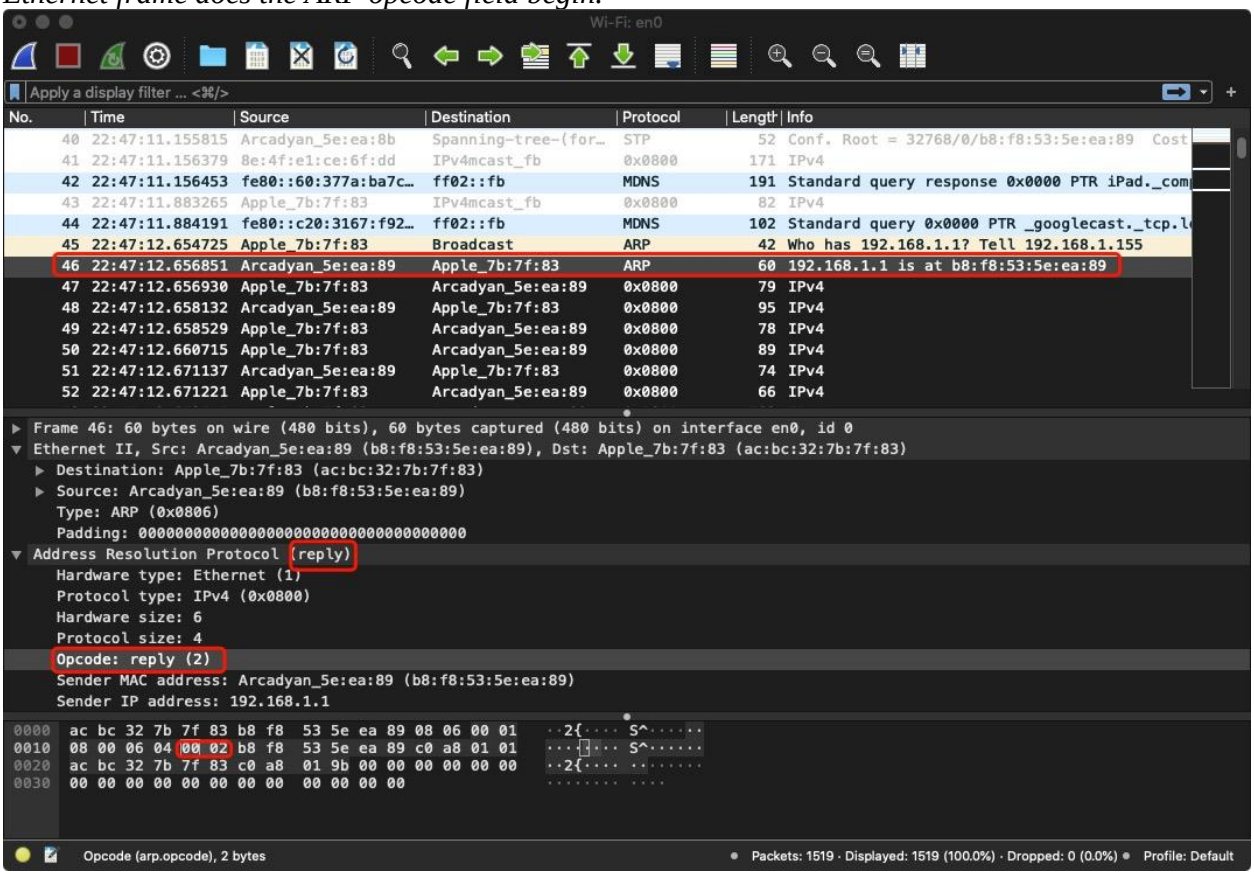

Q13. Now find the ARP reply that was sent in response to the ARP request.

***Packet info of the ARP reply:***

No. Time Source Destination Protocol Length Info
46 22:47:12.656851 Arcadyan_5e:ea:89 Apple_7b:7f:83 ARP 60 192.168.1.1
is at b8:f8:53:5e:ea:89
Frame 46: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface en0, id 0
Ethernet II, Src: Arcadyan_5e:ea:89 (b8:f8:53:5e:ea:89), Dst: Apple_7b:7f:83 (ac:bc:32:7b:7f:83)
Destination: Apple_7b:7f:83 (ac:bc:32:7b:7f:83)
Source: Arcadyan_5e:ea:89 (b8:f8:53:5e:ea:89)
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: Arcadyan_5e:ea:89 (b8:f8:53:5e:ea:89)
Sender IP address: 192.168.1.1
Target MAC address: Apple_7b:7f:83 (ac:bc:32:7b:7f:83)
Target IP address: 192.168.1.155

Q13. a) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

*Answer: As shown in the screenshot below, there are 20 bytes from the very beginning of the Ethernet frame does the ARP opcode field begin.*

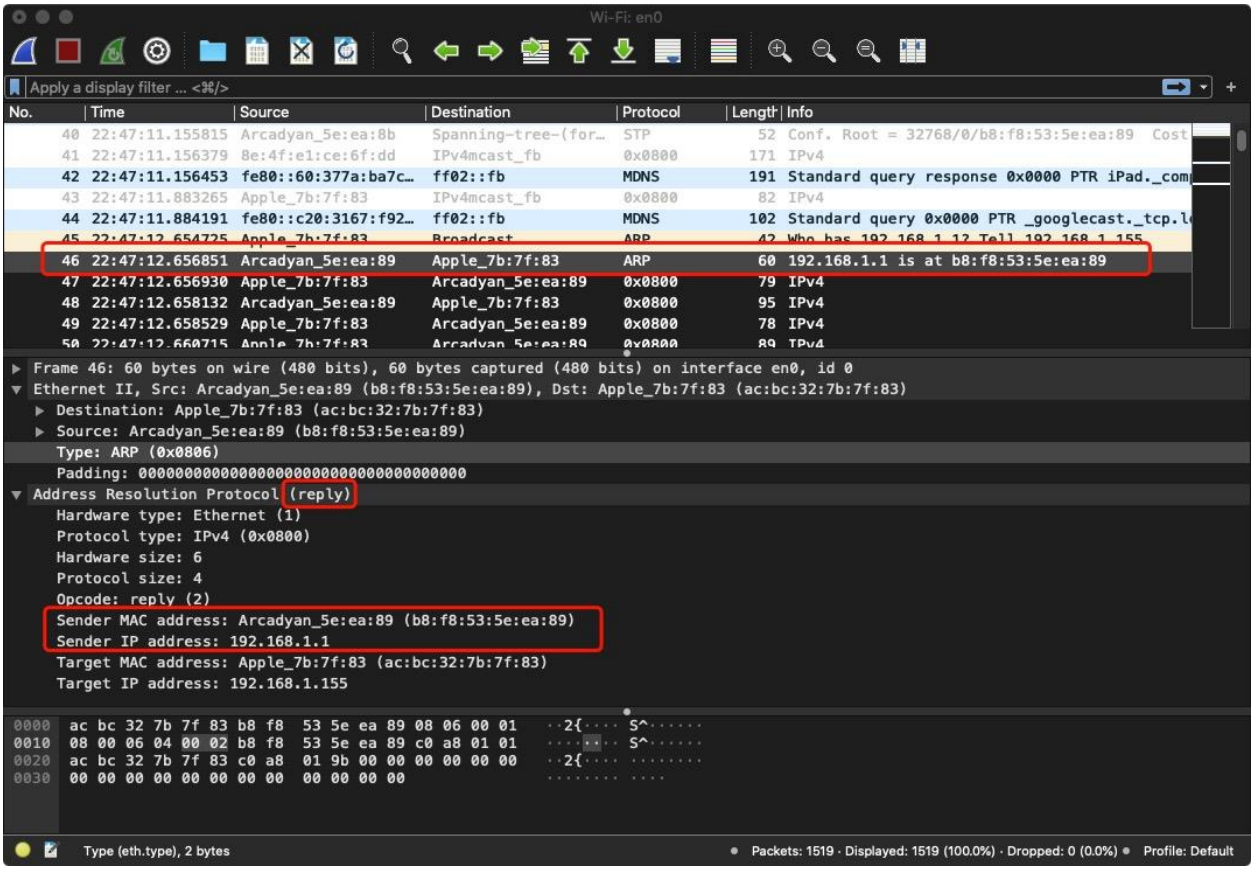



Q13. b) What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP response is made?

*Answer: As shown in the screenshot above, the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP response is 0x0002*

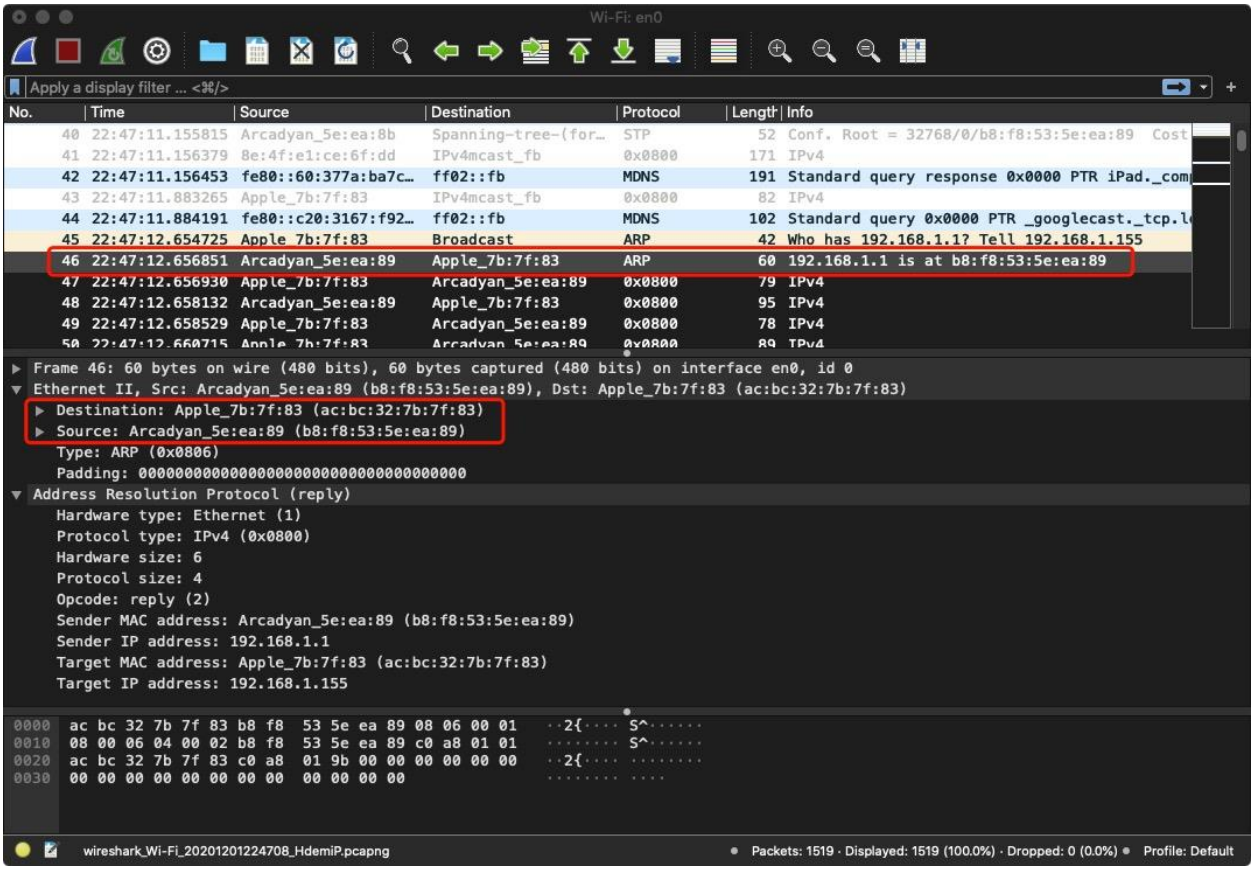
Q13. c) Where in the ARP message does the "answer" to the earlier ARP request appear – the IP address of the machine having the Ethernet address whose corresponding IP address is being queried?

*Answer: As shown in the screenshot below, the Sender IP address: 192.168.1.1 and Sender MAC address: b8:f8:53:5e:ea:89, answer to the earlier ARP request.*




Q14. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message?

*Answer: As the screenshot shown below, the source address is b8:f8:53:5e:ea:89 and the destination address is ac:bc:32:7b:7f:83*




Q15. 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: The reason why is there no ARP reply (sent in response to the ARP request in packet 6) in the packet trace is that ARP request would be broadcast, however the ARP reply would not be broadcast. Only the device that send the request would be received the corresponding reply. And since this computer is not the computer that sent this ARP request, we will not receive the reply of sent this ARP request.*