Assignment 5
Ritik Garg | 2018305

Answer 1.

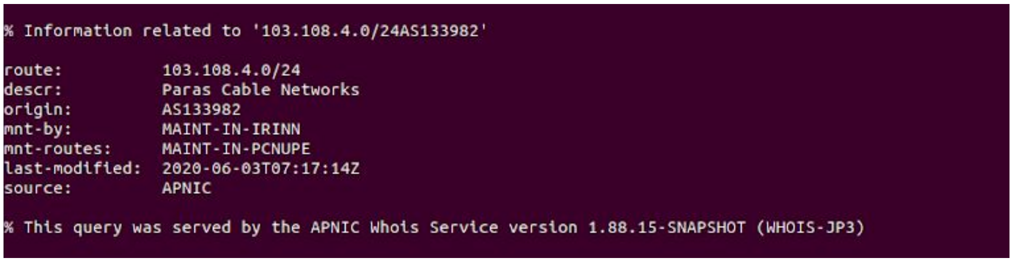
(a).For the Asn number I firstly found my public IP address using whatismyip.com

Public IP Address: 103.108.4.171

Now I will search for the Asn number using the command:

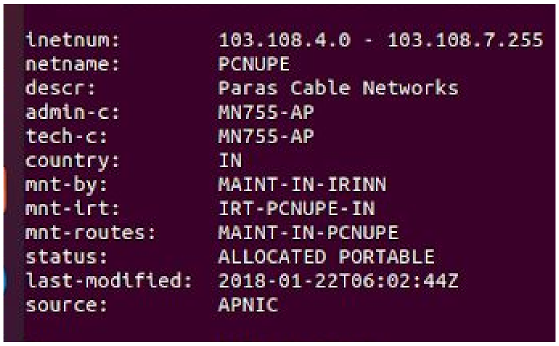
whois 103.108.4.171

Here the Asn number is : **origin: AS133982**

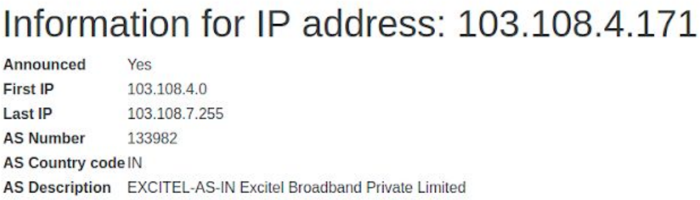


```
% Information related to '103.108.4.0/24AS133982'

route:          103.108.4.0/24
descr:          Paras Cable Networks
origin:         AS133982
mnt-by:         MAINT-IN-IRINN
mnt-routes:     MAINT-IN-PCNUPE
last-modified:  2020-06-03T07:17:14Z
source:         APNIC

% This query was served by the APNIC Whois Service version 1.88.15-SNAPSHOT (WHOIS-JP3)
```

(b). Owner of the AS to which your system belongs : **Paras Cables / Excitel**



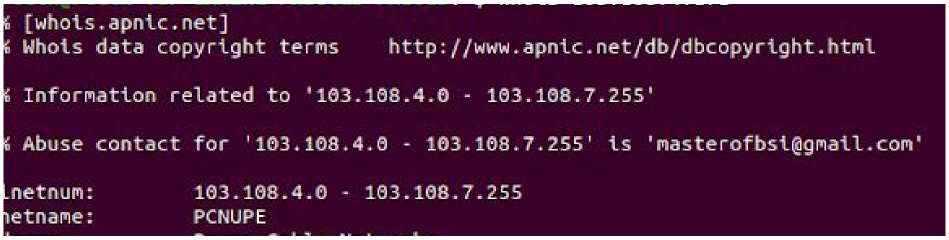
```
inetnum:        103.108.4.0 - 103.108.7.255
netname:        PCNUPE
descr:          Paras Cable Networks
admin-c:        MN755-AP
tech-c:         MN755-AP
country:        IN
mnt-by:         MAINT-IN-IRINN
mnt-irt:        IRT-PCNUPE-IN
mnt-routes:     MAINT-IN-PCNUPE
status:         ALLOCATED PORTABLE
last-modified:  2018-01-22T06:02:44Z
source:         APNIC
```



Information for IP address: 103.108.4.171

Announced	Yes
First IP	103.108.4.0
Last IP	103.108.7.255
AS Number	133982
AS Country code	IN
AS Description	EXCITEL-AS-IN Excitel Broadband Private Limited

(c). Range of IPs: **103.108.4.0 - 103.108.7.255**

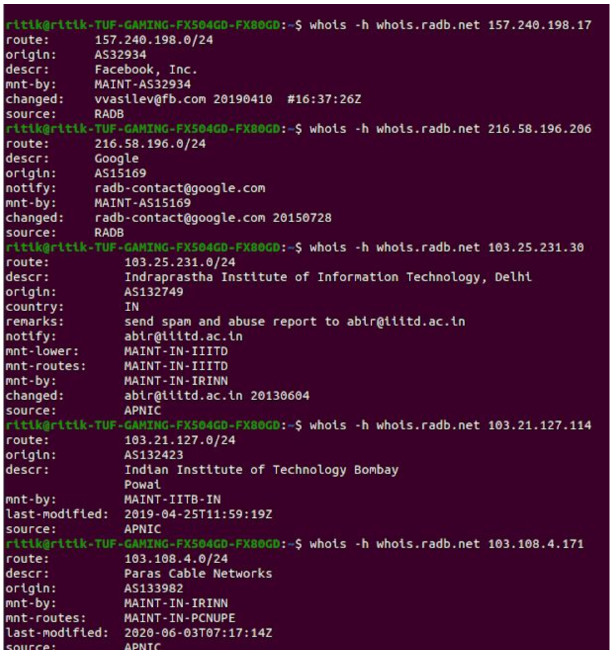


```
% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

% Information related to '103.108.4.0 - 103.108.7.255'

% Abuse contact for '103.108.4.0 - 103.108.7.255' is 'masterofbsi@gmail.com'

inetnum:        103.108.4.0 - 103.108.7.255
netname:        PCNUPE
```

(d).For Asn number, first find the public IPs for them using ‘ping’ command and then ‘whois’

	Public Ips	Asn number
(i). iiitd.ac.in :	103.25.231.30	AS132749
(ii) iitb.ac.in :	103.21.127.114	AS132423
(iii) google.com :	216.58.196.206	AS15169
(iv) facebook.com :	157.240.198.17	AS32934 (not visible directly)

Command: whois -h whois.radb.net 157.240.198.17



```
ritik@ritik-TUF-GAMING-FX504GD-FX80GD:~$ whois -h whois.radb.net 157.240.198.17
route:      157.240.198.0/24
origin:     AS32934
descr:      Facebook, Inc.
mnt-by:     MAINT-AS32934
changed:    vvasilev@fb.com 20190410  #16:37:26Z
source:     RADB
ritik@ritik-TUF-GAMING-FX504GD-FX80GD:~$ whois -h whois.radb.net 216.58.196.206
route:      216.58.196.0/24
descr:      Google
origin:     AS15169
notify:     radb-contact@google.com
mnt-by:     MAINT-AS15169
changed:    radb-contact@google.com 20150728
source:     RADB
ritik@ritik-TUF-GAMING-FX504GD-FX80GD:~$ whois -h whois.radb.net 103.25.231.30
route:          103.25.231.0/24
descr:          Indraprastha Institute of Information Technology, Delhi
origin:         AS132749
country:        IN
remarks:        send spam and abuse report to abir@iiitd.ac.in
notify:         abir@iiitd.ac.in
mnt-lower:      MAINT-IN-IIITD
mnt-routes:     MAINT-IN-IIITD
mnt-by:         MAINT-IN-IRINN
changed:        abir@iiitd.ac.in 20130604
source:         APNIC
ritik@ritik-TUF-GAMING-FX504GD-FX80GD:~$ whois -h whois.radb.net 103.21.127.114
route:          103.21.127.0/24
origin:         AS132423
descr:          Indian Institute of Technology Bombay
                Powai
mnt-by:         MAINT-IITB-IN
last-modified:  2019-04-25T11:59:19Z
source:         APNIC
ritik@ritik-TUF-GAMING-FX504GD-FX80GD:~$ whois -h whois.radb.net 103.108.4.171
route:          103.108.4.0/24
descr:          Paras Cable Networks
origin:         AS133982
mnt-by:         MAINT-IN-IRINN
mnt-routes:     MAINT-IN-PCNUPE
last-modified:  2020-06-03T07:17:14Z
source:         APNIC
```

Answer 2.

(a) .To get the arp packets,

Firstly get the default router gateway using: **‘ip route show’ : 192.168.1.1**

After that use arp -a to view the cache and then remove the default gateway using: **arp -d 192.168.1.1**

After removing the , create a pcap file using tcpdump and ping the gateway parallelly using:

sudo tcpdump -i wlo1 -w r1.pcap; ping 192.168.1.1

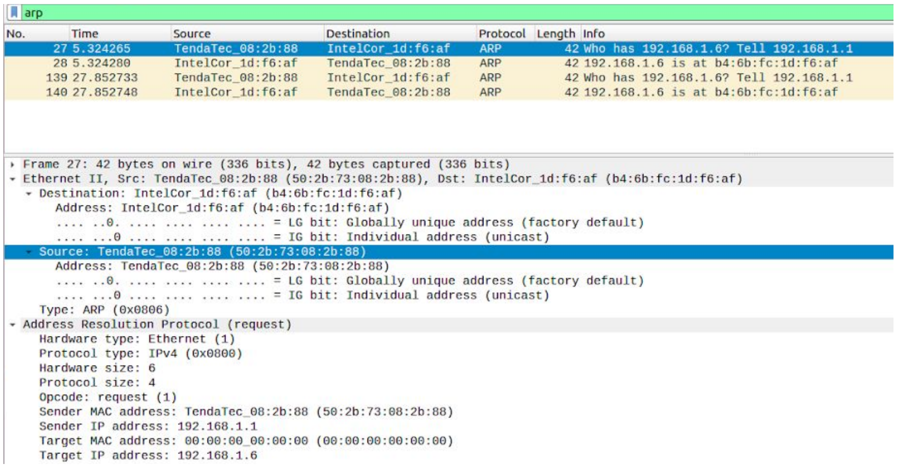
Now open the pcap file in wireshark and apply the filter: **arp** to display the arp packets.

Click on the packets and you can view the arp request and reply packet.

Differences:

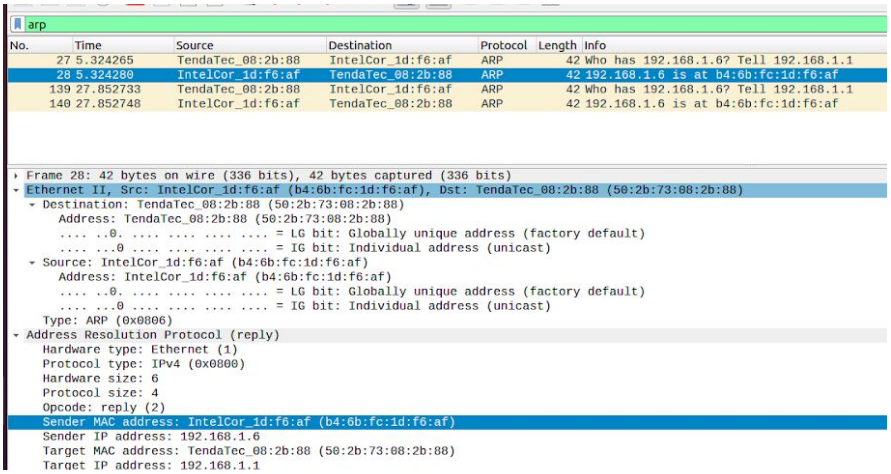
- Request packet has no target mac address, while the reply packet contains the source and destination mac addresses.
- Difference in the opcodes - request and reply

Request Packet:



```
No.      Time         Source               Destination          Protocol Length Info
      27 5.324265     TendaTec_08:2b:88    IntelCor_1d:f6:af    ARP          42 Who has 192.168.1.6? Tell 192.168.1.1
      28 5.324280     IntelCor_1d:f6:af    TendaTec_08:2b:88    ARP          42 192.168.1.6 is at b4:6b:fc:1d:f6:af
     139 27.852733    TendaTec_08:2b:88    IntelCor_1d:f6:af    ARP          42 Who has 192.168.1.6? Tell 192.168.1.1
     140 27.852748    IntelCor_1d:f6:af    TendaTec_08:2b:88    ARP          42 192.168.1.6 is at b4:6b:fc:1d:f6:af

› Frame 27: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
▾ Ethernet II, Src: TendaTec_08:2b:88 (50:2b:73:08:2b:88), Dst: IntelCor_1d:f6:af (b4:6b:fc:1d:f6:af)
  ▾ Destination: IntelCor_1d:f6:af (b4:6b:fc:1d:f6:af)
      Address: IntelCor_1d:f6:af (b4:6b:fc:1d:f6:af)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: TendaTec_08:2b:88 (50:2b:73:08:2b:88)
      Address: TendaTec_08:2b:88 (50:2b:73:08:2b:88)
      .... ..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: TendaTec_08:2b:88 (50:2b:73:08:2b:88)
    Sender IP address: 192.168.1.1
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.1.6
```

Reply packet:



```
No.      Time         Source               Destination          Protocol Length Info
      27 5.324265     TendaTec_08:2b:88    IntelCor_1d:f6:af    ARP          42 Who has 192.168.1.6? Tell 192.168.1.1
      28 5.324280     IntelCor_1d:f6:af    TendaTec_08:2b:88    ARP          42 192.168.1.6 is at b4:6b:fc:1d:f6:af
     139 27.852733    TendaTec_08:2b:88    IntelCor_1d:f6:af    ARP          42 Who has 192.168.1.6? Tell 192.168.1.1
     140 27.852748    IntelCor_1d:f6:af    TendaTec_08:2b:88    ARP          42 192.168.1.6 is at b4:6b:fc:1d:f6:af

› Frame 28: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
▾ Ethernet II, Src: IntelCor_1d:f6:af (b4:6b:fc:1d:f6:af), Dst: TendaTec_08:2b:88 (50:2b:73:08:2b:88)
  ▾ Destination: TendaTec_08:2b:88 (50:2b:73:08:2b:88)
      Address: TendaTec_08:2b:88 (50:2b:73:08:2b:88)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: IntelCor_1d:f6:af (b4:6b:fc:1d:f6:af)
      Address: IntelCor_1d:f6:af (b4:6b:fc:1d:f6:af)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
▾ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: IntelCor_1d:f6:af (b4:6b:fc:1d:f6:af)
    Sender IP address: 192.168.1.6
    Target MAC address: TendaTec_08:2b:88 (50:2b:73:08:2b:88)
    Target IP address: 192.168.1.1
```

(b). Opcode for request packet : **request (1)**

Opcode for reply packet : **reply (2)**

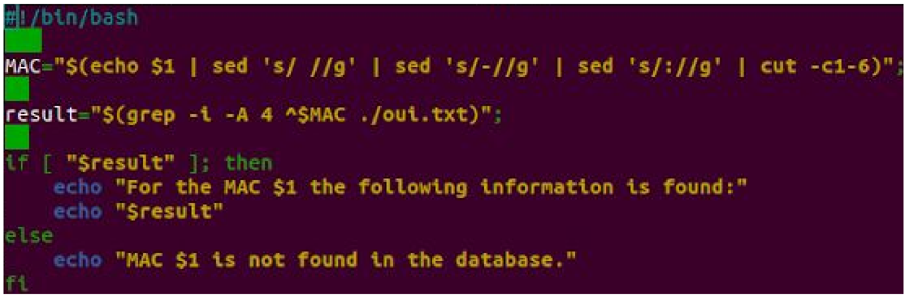
(can be seen in the above screenshot)

(c). Yes we can easily find the manufacturer using the mac address

For that firstly, download the oui.txt file: **wget http://standards-oui.ieee.org/oui/oui.txt**

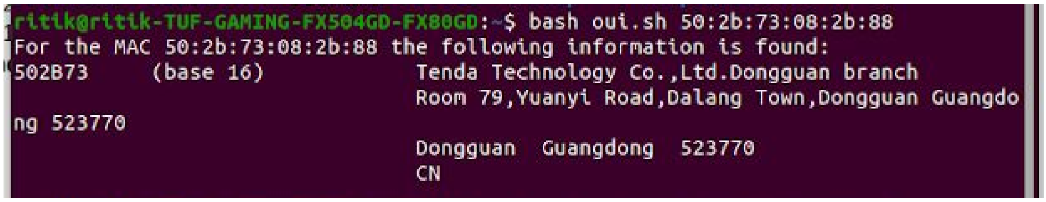
Now create a bash file: out.sh to get the data from the file

Paste the code below:



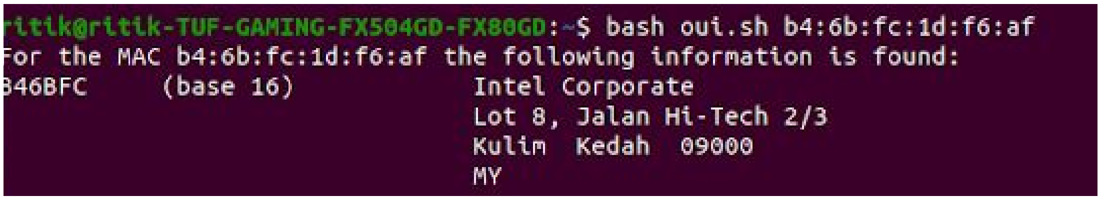
```
#!/bin/bash

MAC="$(echo $1 | sed 's/ //g' | sed 's/-//g' | sed 's/://g' | cut -c1-6)";

result="$(grep -i -A 4 ^$MAC ./oui.txt)";

if [ "$result" ]; then
    echo "For the MAC $1 the following information is found:"
    echo "$result"
else
    echo "MAC $1 is not found in the database."
fi
```

Now simply run: **bash oui.sh <mac address>** to get the details of the manufacturer.
Sender :



```
ritik@ritik-TUF-GAMING-FX504GD-FX80GD:~$ bash oui.sh 50:2b:73:08:2b:88
For the MAC 50:2b:73:08:2b:88 the following information is found:
502B73     (base 16)           Tenda Technology Co.,Ltd.Dongguan branch
                               Room 79,Yuanyi Road,Dalang Town,Dongguan Guangdo
ng 523770
                               Dongguan  Guangdong  523770
                               CN
```

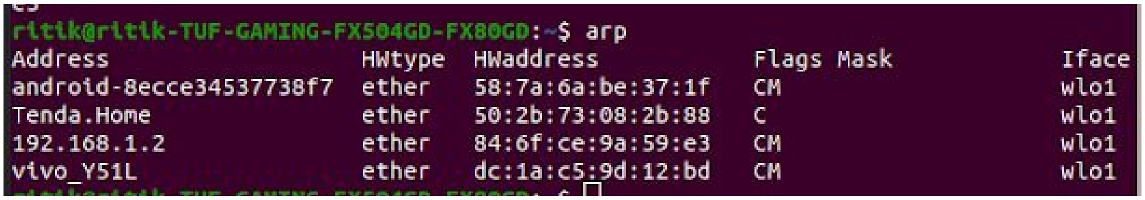
Receiver:



```
ritik@ritik-TUF-GAMING-FX504GD-FX80GD:~$ bash oui.sh b4:6b:fc:1d:f6:af
For the MAC b4:6b:fc:1d:f6:af the following information is found:
B46BFC     (base 16)           Intel Corporate
                               Lot 8, Jalan Hi-Tech 2/3
                               Kulim  Kedah  09000
                               MY
```

(d).Clear the using : sudo arp -d 192.168.1.1
Add a static entry using: **arp -s <ip address> <mac address>**

1. arp -s 192.168.1.3 58:7a:6a:be:37:1f
2. arp -s 192.168.1.3 58:7a:6a:be:37:1f
3. arp -s 192.168.1.4 dc:1a:c5:9d:12:bd



```
ritik@ritik-TUF-GAMING-FX504GD-FX80GD:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
android-8ecce34537738f7  ether   58:7a:6a:be:37:1f   CM                    wlo1
Tenda.Home               ether   50:2b:73:08:2b:88   C                     wlo1
192.168.1.2              ether   84:6f:ce:9a:59:e3   CM                    wlo1
vivo_Y51L                ether   dc:1a:c5:9d:12:bd   CM                    wlo1
```

Dynamic ARP table entries are created when a client makes an ARP request, whereas static ARP table entries are entered manually using the ARP utility. Dynamic ARP table are dropped after a certain time while not so with the static ARP table.

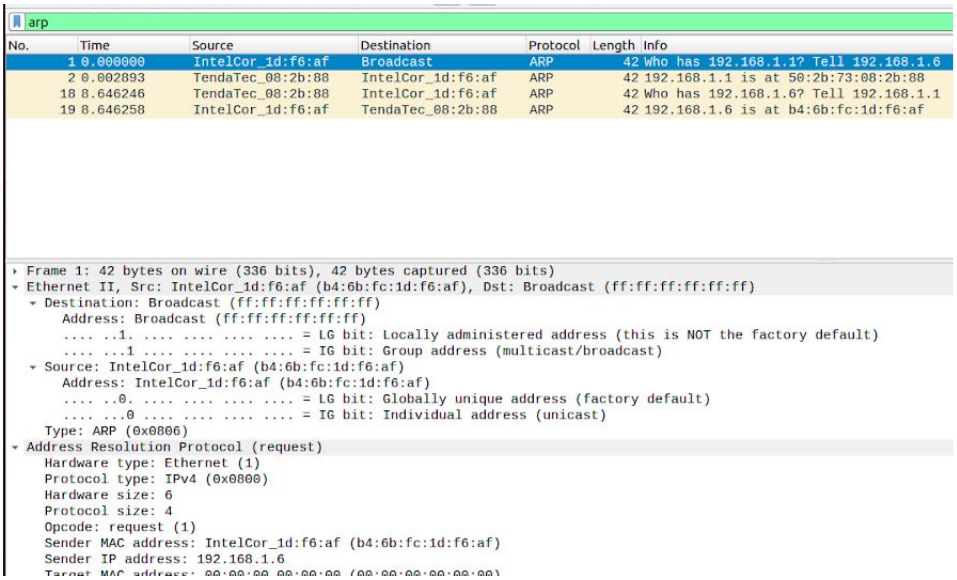
Answer 3.

(a). No, the destination address is 00:00:00:00:00:00. It is because the target host is not known but the ip address is of the default gateway. It reaches all the machines on the network. The machine bearing IP address mentioned in the ARP request packet responds by sending an ARP response packet with its MAC address.

Now, the source machine gets back the ARP response with the target MAC address and puts it into an ARP table in memory so that it doesn't need to use ARP each time till the ARP table entry expires.

Filter is the 'arp', after that click on the packet to view if it is a request or a reply packet.

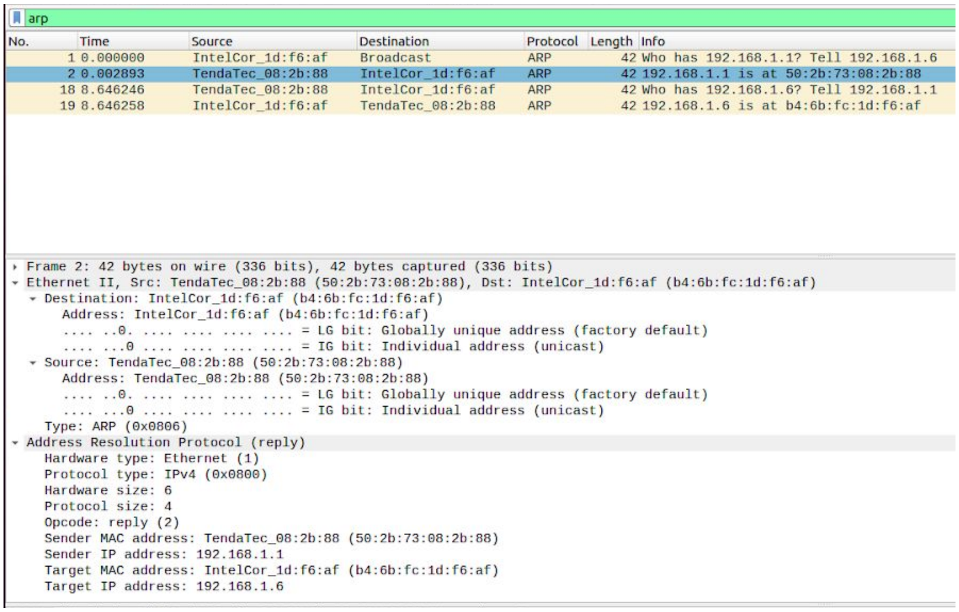
Request packet:



```
arp
No.     Time        Source              Destination         Protocol Length Info
      1 0.000000    IntelCor_1d:f6:af   Broadcast           ARP        42 Who has 192.168.1.1? Tell 192.168.1.6
      2 0.002893    TendaTec_08:2b:88   IntelCor_1d:f6:af   ARP        42 192.168.1.1 is at 50:2b:73:08:2b:88
     18 8.646246    TendaTec_08:2b:88   IntelCor_1d:f6:af   ARP        42 Who has 192.168.1.6? Tell 192.168.1.1
     19 8.646258    IntelCor_1d:f6:af   TendaTec_08:2b:88   ARP        42 192.168.1.6 is at b4:6b:fc:1d:f6:af
```

```
› Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
▾ Ethernet II, Src: IntelCor_1d:f6:af (b4:6b:fc:1d:f6:af), 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: IntelCor_1d:f6:af (b4:6b:fc:1d:f6:af)
      Address: IntelCor_1d:f6:af (b4:6b:fc:1d:f6:af)
      .... ..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: IntelCor_1d:f6:af (b4:6b:fc:1d:f6:af)
    Sender IP address: 192.168.1.6
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
```

Reply packet:



```
arp
No.     Time        Source              Destination         Protocol Length Info
      1 0.000000    IntelCor_1d:f6:af   Broadcast           ARP        42 Who has 192.168.1.1? Tell 192.168.1.6
      2 0.002893    TendaTec_08:2b:88   IntelCor_1d:f6:af   ARP        42 192.168.1.1 is at 50:2b:73:08:2b:88
     18 8.646246    TendaTec_08:2b:88   IntelCor_1d:f6:af   ARP        42 Who has 192.168.1.6? Tell 192.168.1.1
     19 8.646258    IntelCor_1d:f6:af   TendaTec_08:2b:88   ARP        42 192.168.1.6 is at b4:6b:fc:1d:f6:af
```

```
› Frame 2: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
▾ Ethernet II, Src: TendaTec_08:2b:88 (50:2b:73:08:2b:88), Dst: IntelCor_1d:f6:af (b4:6b:fc:1d:f6:af)
  ▾ Destination: IntelCor_1d:f6:af (b4:6b:fc:1d:f6:af)
      Address: IntelCor_1d:f6:af (b4:6b:fc:1d:f6:af)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: TendaTec_08:2b:88 (50:2b:73:08:2b:88)
      Address: TendaTec_08:2b:88 (50:2b:73:08:2b:88)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
▾ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: TendaTec_08:2b:88 (50:2b:73:08:2b:88)
    Sender IP address: 192.168.1.1
    Target MAC address: IntelCor_1d:f6:af (b4:6b:fc:1d:f6:af)
    Target IP address: 192.168.1.6
```

(b). Yes, it is the address of the default gateway.

(c). This means that a dynamic ARP entry will remain for that many time in the cache table before the router attempts to refresh the entry. If the entry is no longer needed it will be removed.

To get the timeout values, go to the

cd /proc/sys/net/ipv4/route and display the gc_timeout (cat gc_timeout) : 300

cd /proc/sys/net/ipv4/neigh/wlo1 and display the gc_interval (cat gc_interval) : 60