CS 315 : Computer Networks Lab
Assignment - 11
Wireshark Lab: Ethernet and ARP

Ayush Mallick
CS22BT008

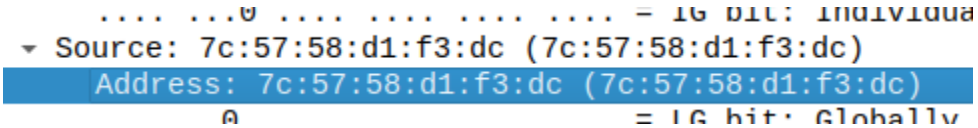
Part-0

```
cs101@sysad-HP-Elite-Tower-600-G9-Desktop-PC:~$ ifconfig
eno1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.240.118.81  netmask 255.255.248.0  broadcast 10.240.119.255
        inet6 fe80::caaa:5c87:96bd:271f  prefixlen 64  scopeid 0x20<link>
        ether 7c:57:58:d1:f3:dc  txqueuelen 1000  (Ethernet)
        RX packets 624685  bytes 408225143 (408.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 205345  bytes 66291556 (66.2 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 19  memory 0x80900000-80920000

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 17491  bytes 1713701 (1.7 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 17491  bytes 1713701 (1.7 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp0s20f3: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether b0:dc:ef:bf:4c:fd  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Part-1

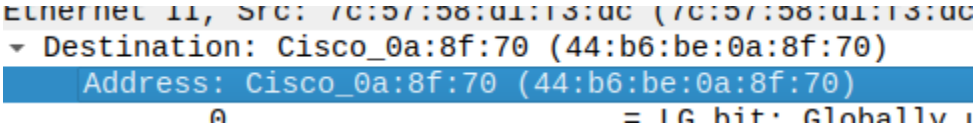
1.1

Source address : *7c:57:58:d1:f3:dc*



1.2

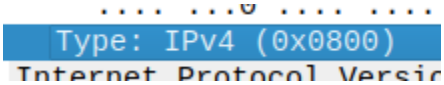
Destination address : *44:b6:be:0a:8f:70*



No, this is not the MAC address of httpforever.com. It belongs to the default gateway/router, which forwards packets to httpforever.com.

1.3

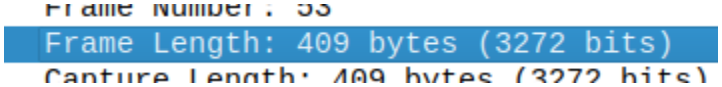
Type : *0x0800*



This indicates IPv4 as the network layer protocol.

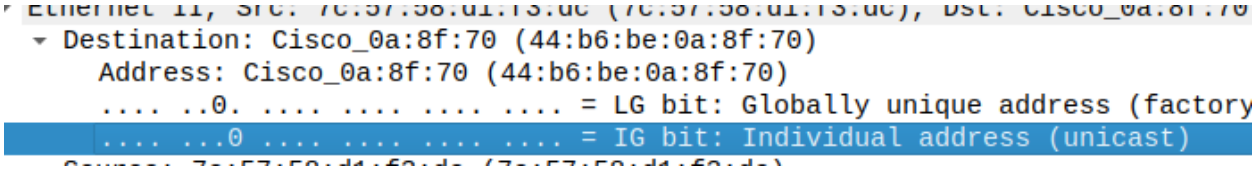
1.4

Frame length : *409 bytes*



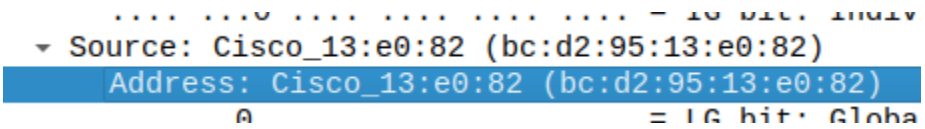
1.5

The Ethernet frame carrying the first HTTP GET request is transmitted as a *unicast* frame. This can be determined from the IG bits as well as the destination MAC address belongs to a single device (hop or router).



1.6

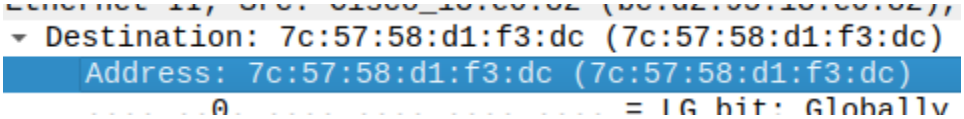
Source address : *bc:d2:95:13:e0:82*



This address belongs neither to the computer, or httpforever.com, but it is rather the MAC address of the last-hop router (default gateway) on the network.

1.7

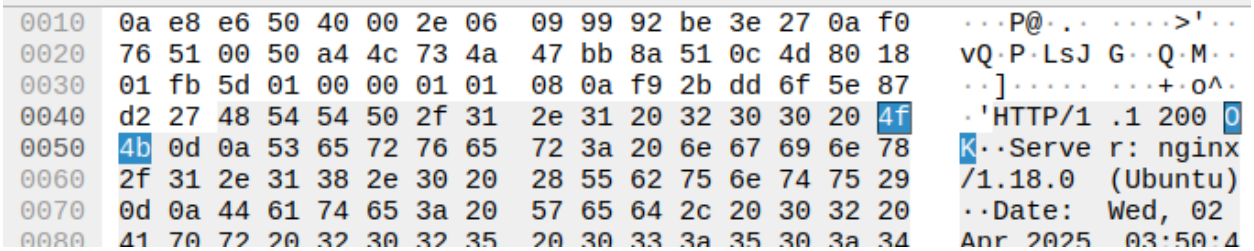
Destination address : *7c:57:58:d1:f3:dc*



Yes, this is the Ethernet MAC address of the computer.

1.8

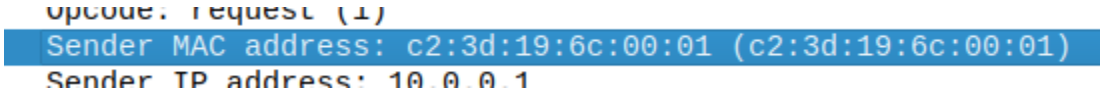
In the Ethernet frame, the ASCII “O” in “OK” appears after *79 bytes*.
In the HTTP, the ASCII “O” in “OK” appears after *13 bytes*.



Part-2

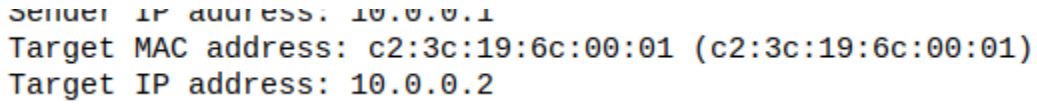
2.1

Sender MAC address : *c2:3d:19:6c:00:01*



2.2

Target IP address : *10.0.0.2*
Target MAC address : *c2:3c:19:6c:00:01*



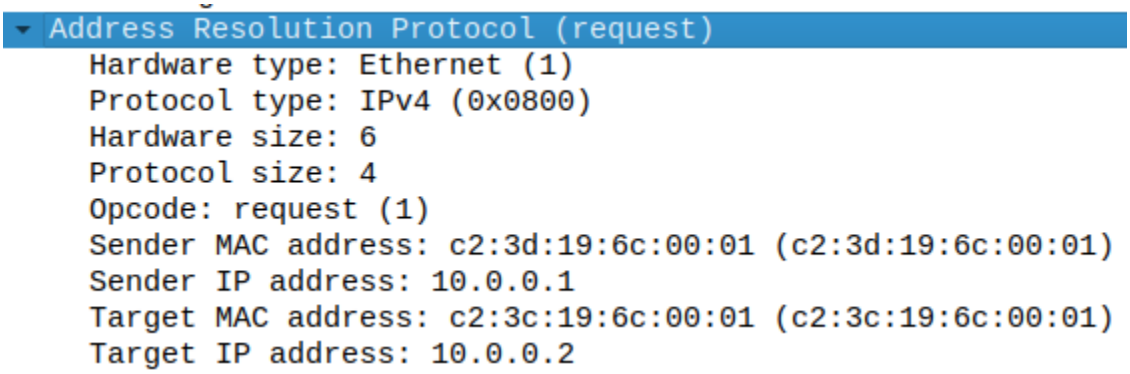
2.3

Broadcasting occurs in the ARP trace for Gratuitous ARP replies, and for ARP requests with hardware type IEEE 802. For Gratuitous ARP replies, broadcasting occurs to ensure all devices on the network update their ARP caches with the correct MAC-IP mapping, preventing outdated or incorrect entries. For ARP requests with hardware type IEEE 802, broadcasting occurs because the sender does not yet know the target’s MAC address and must ask all devices on the network to respond if they have the matching IP.

2.4

All fields and values in the ARP request :

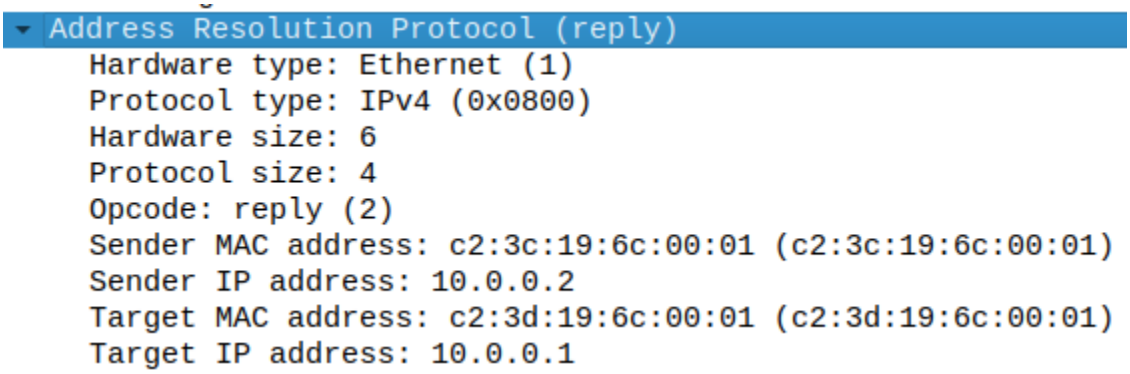
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (1)
Sender MAC address: c2:3d:19:6c:00:01 (c2:3d:19:6c:00:01)
Sender IP address: 10.0.0.1
Target MAC address: c2:3c:19:6c:00:01 (c2:3c:19:6c:00:01)
Target IP address: 10.0.0.2



2.5

All fields and values in the ARP reply :

Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: reply (2)
Sender MAC address: c2:3c:19:6c:00:01 (c2:3c:19:6c:00:01)
Sender IP address: 10.0.0.2
Target MAC address: c2:3d:19:6c:00:01 (c2:3d:19:6c:00:01)
Target IP address: 10.0.0.1



2.6

The *opcode, sender and target IP and MAC addresses* are different among the ARP request and reply fields and values.

2.7

A Gratuitous ARP packet is an ARP request or reply sent by a device for its own IP address, not to resolve another host's address. It serves two main purposes: detecting IP conflicts (checking if another device has the same IP) and updating network devices' ARP caches to ensure correct IP-to-MAC mappings.

2.8

In a Gratuitous ARP, the sender's IP and MAC addresses are the same in both the source and target fields, meaning the device announces its presence without querying another host. This helps ensure network devices correctly associate the IP with the right MAC address, preventing stale ARP cache entries and reducing misrouted traffic.

2.9

There are *8* Gratuitous ARP packets present in the trace corresponding to the sender's IP Address, 10.0.0.1, namely packet numbers : *16*, *18*, *536*, *538*, *783*, *784*, *785*, *786*.

No.	Time	Source	Destination	Protocol	Length	Text item	Info
16	113831509.157076	c2:3d:19:6c:00:01	Broadcast	ARP	60		Gratuitous ARP for 10.0.0.1 (Reply)
18	113831509.157076	c2:3d:19:6c:00:01	Broadcast	ARP	60		Gratuitous ARP for 10.0.0.1 (Reply)
536	113831625.112076	c2:3d:19:6c:00:01	Broadcast	ARP	60		Gratuitous ARP for 10.0.0.1 (Reply)
538	113831625.112076	c2:3d:19:6c:00:01	Broadcast	ARP	60		Gratuitous ARP for 10.0.0.1 (Reply)
783	113831684.128076	c2:3d:19:6c:00:01	Broadcast	ARP	60		Gratuitous ARP for 10.0.0.1 (Reply)
784	113831684.128076	c2:3d:19:6c:00:01	Broadcast	ARP	60		Gratuitous ARP for 10.0.0.1 (Reply)
785	113831684.143076	c2:3d:19:6c:00:01	Broadcast	ARP	60		Gratuitous ARP for 10.0.0.1 (Reply)
786	113831684.143076	c2:3d:19:6c:00:01	Broadcast	ARP	60		Gratuitous ARP for 10.0.0.1 (Reply)

2.10

Sender MAC address : *c2:3d:19:6c:00:01*
Target MAC address : *ff:ff:ff:ff:ff:ff*

```
[Is gratuitous: True]
Sender MAC address: c2:3d:19:6c:00:01 (c2:3d:19:6c:00:01)
Sender IP address: 10.0.0.1
Target MAC address: Broadcast (ff:ff:ff:ff:ff:ff)
Target IP address: 10.0.0.1
```