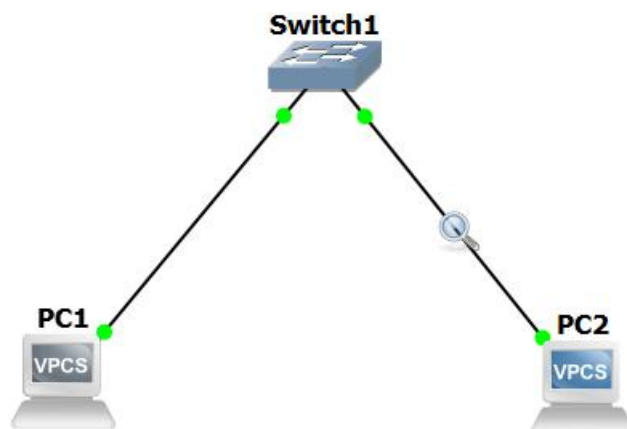


Q2. Capture and analyze Ethernet frames using Wireshark. Inspect the structure of the frame, including destination and source MAC addresses, Ethertype, payload, and FCS Use GNS3 or Packet Tracer to simulate network traffic.

Using GNS3



```
PC2>
PC2> ip 10.0.0.2 255.0.0.0 10.0.0.1
Checking for duplicate address...
10.0.0.2 is being used by MAC 00:50:79:66:68:00
Address not changed

PC2> ip 10.0.0.3 255.0.0.0 10.0.0.1
Checking for duplicate address...
PC1 : 10.0.0.3 255.0.0.0 gateway 10.0.0.1

PC2> ping 10.0.0.2
64 bytes from 10.0.0.2 icmp_seq=1 ttl=64 time=1.816 ms
64 bytes from 10.0.0.2 icmp_seq=2 ttl=64 time=1.156 ms
64 bytes from 10.0.0.2 icmp_seq=3 ttl=64 time=1.018 ms
64 bytes from 10.0.0.2 icmp_seq=4 ttl=64 time=1.162 ms
64 bytes from 10.0.0.2 icmp_seq=5 ttl=64 time=7.038 ms

PC2> ping 10.0.0.2 -t
64 bytes from 10.0.0.2 icmp_seq=1 ttl=64 time=1.182 ms
64 bytes from 10.0.0.2 icmp_seq=2 ttl=64 time=1.074 ms
64 bytes from 10.0.0.2 icmp_seq=3 ttl=64 time=1.231 ms
64 bytes from 10.0.0.2 icmp_seq=4 ttl=64 time=1.210 ms
64 bytes from 10.0.0.2 icmp_seq=5 ttl=64 time=1.115 ms
64 bytes from 10.0.0.2 icmp_seq=6 ttl=64 time=1.086 ms
```

Analysing Ethernet frames using Wireshark

Capturing from Standard input [PC2 Ethernet0 to Switch1 Ethernet2]						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
Apply a display filter ... <Ctrl-/>						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Private_66:68:01	Broadcast	ARP	64	Who has 10.0.0.2? Tell 10.0.0.3
2	0.001348	Private_66:68:00	Private_66:68:01	ARP	64	10.0.0.2 is at 00:50:79:66:68:00
3	0.014405	10.0.0.3	10.0.0.2	ICMP	98	Echo (ping) request id=0x23c3, seq=1/256, ttl=64 (reply in 4)
4	0.014405	10.0.0.2	10.0.0.3	ICMP	98	Echo (ping) reply id=0x23c3, seq=1/256, ttl=64 (request in 3)
5	1.042140	10.0.0.3	10.0.0.2	ICMP	98	Echo (ping) request id=0x24c3, seq=2/512, ttl=64 (reply in 6)
6	1.042140	10.0.0.2	10.0.0.3	ICMP	98	Echo (ping) reply id=0x24c3, seq=2/512, ttl=64 (request in 5)
7	2.066960	10.0.0.3	10.0.0.2	ICMP	98	Echo (ping) request id=0x26c3, seq=3/768, ttl=64 (reply in 8)
8	2.066960	10.0.0.2	10.0.0.3	ICMP	98	Echo (ping) reply id=0x26c3, seq=3/768, ttl=64 (request in 7)
9	3.082273	10.0.0.3	10.0.0.2	ICMP	98	Echo (ping) request id=0x27c3, seq=4/1024, ttl=64 (reply in 10)
10	3.082289	10.0.0.2	10.0.0.3	ICMP	98	Echo (ping) reply id=0x27c3, seq=4/1024, ttl=64 (request in 9)
11	4.104552	10.0.0.3	10.0.0.2	ICMP	98	Echo (ping) request id=0x28c3, seq=5/1280, ttl=64 (reply in 12)
12	4.104552	10.0.0.2	10.0.0.3	ICMP	98	Echo (ping) reply id=0x28c3, seq=5/1280, ttl=64 (request in 11)
13	5.128213	10.0.0.3	10.0.0.2	ICMP	98	Echo (ping) request id=0x29c3, seq=6/1536, ttl=64 (reply in 14)
14	5.129224	10.0.0.2	10.0.0.3	ICMP	98	Echo (ping) reply id=0x29c3, seq=6/1536, ttl=64 (request in 13)
15	6.152081	10.0.0.3	10.0.0.2	ICMP	98	Echo (ping) request id=0x2ac3, seq=7/1792, ttl=64 (reply in 16)
16	6.153153	10.0.0.2	10.0.0.3	ICMP	98	Echo (ping) reply id=0x2ac3, seq=7/1792, ttl=64 (request in 15)
17	7.173247	10.0.0.3	10.0.0.2	ICMP	98	Echo (ping) request id=0x2bc3, seq=8/2048, ttl=64 (reply in 18)
18	7.173247	10.0.0.2	10.0.0.3	ICMP	98	Echo (ping) reply id=0x2bc3, seq=8/2048, ttl=64 (request in 17)
> Frame 1: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface -, id 0						
> Ethernet II, Src: Private_66:68:01 (00:50:79:66:68:01), Dst: Broadcast (ff:ff:ff:ff:ff:ff)						
> Address Resolution Protocol (request)						
0000	ff	ff	ff	ff	ff	ff 00 50 79 66 68 01 08 06 00 01P yfh...
0010	08	00	06	04	00	01 00 50 79 66 68 01 0a 00 00 03P yfh....
0020	ff	ff	ff	ff	ff	0a 00 00 02 00 00 00 00 00 00 00P yfh.....
0030	00	00	00	00	00	00 00 00 00 00 00 00 00 00 00 00P yfh.....

Destination MAC Address

- Value: ff:ff:ff:ff:ff:ff

Source MAC Address

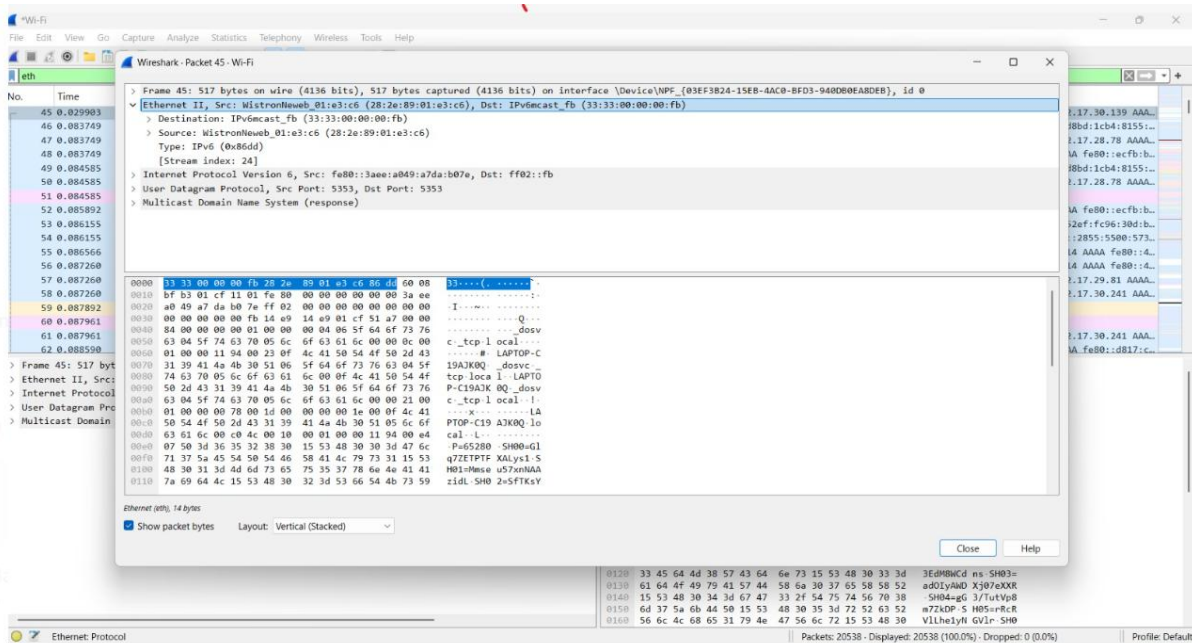
- Value: 00:50:79:66:68:01

Ethertype

- Value: 0x0806

Payload (Data Inside the Frame)

- This contains the ARP request:
 - Sender IP: 10.0.0.3
 - Sender MAC: 00:50:79:66:68:01



Ethernet frame details:

1. Destination MAC Address

MAC Address: 33:33:00:00:00:fb

2. Source MAC Address

MAC Address: 28:2e:89:01:e3:c6

3. Ethertype

Value: 0x86dd (payload contains an IPv6 packet)

4. Payload

Source IP: fe80::3aee

Destination IP: ff02::fb

Protocol: UDP

Source Port: 5353

Destination Port: 5353