LINUX NETWORKING MODULE 3 AND 4 ASSESSMENT SOLUTIONS

-BY SAKTHI KUMAR S

1.Simulate a small network with switches and multiple devices. Use ping to generate traffic and observe the MAC address table of the switch. Capture packets using Wireshark to analyze Ethernet frames and MAC addressing.

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

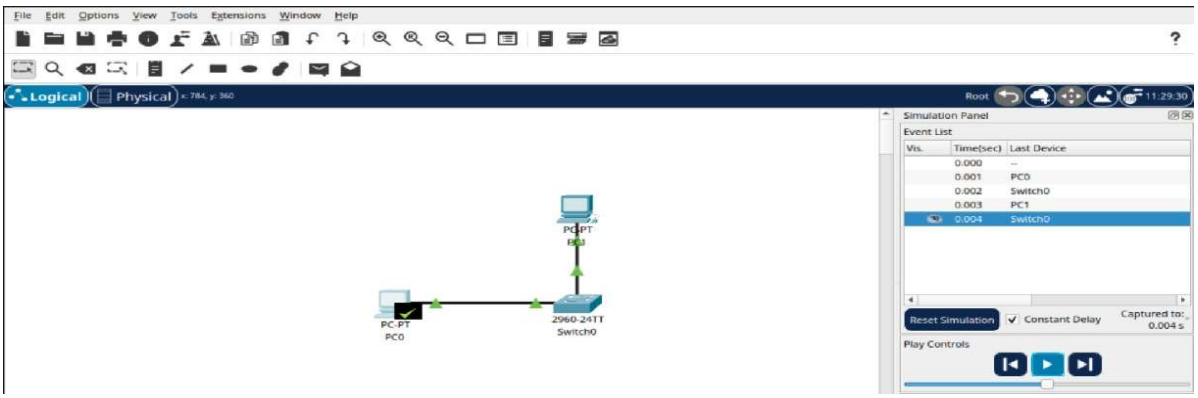
Cisco Packet Tracer:

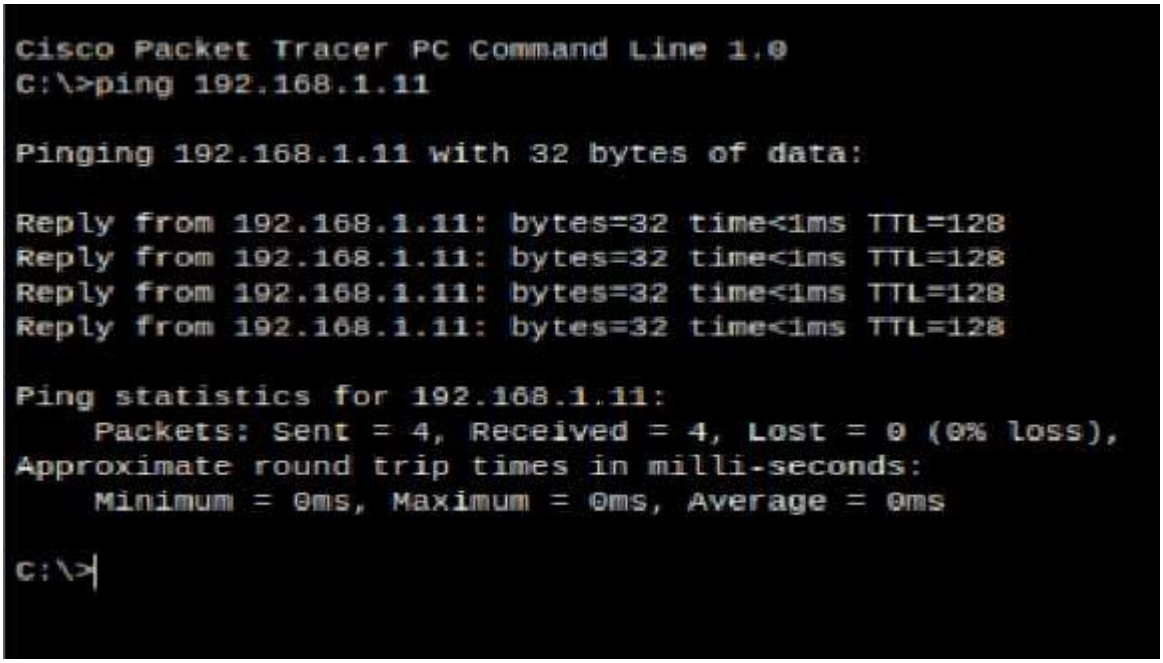
1) Basic network topology Setup in Cisco Packet Tracer

Devices Used

- 2 PCs (PC0 and PC1) (IP addresses: 192.168.1.10 and 192.168.1.11) (
- 1 Switch (Switch0 2960-24TT)
- Copper Straight-Through Cables

2) Ping Test:

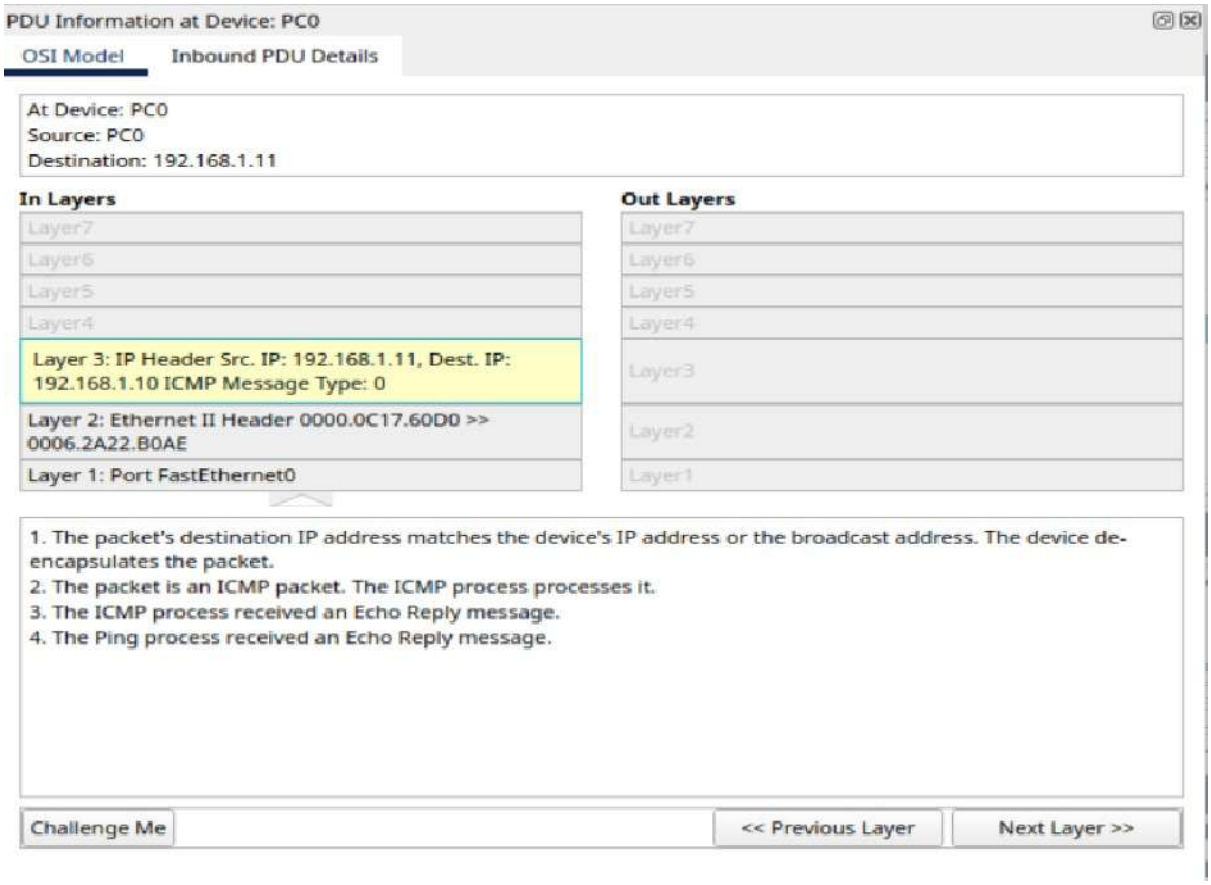


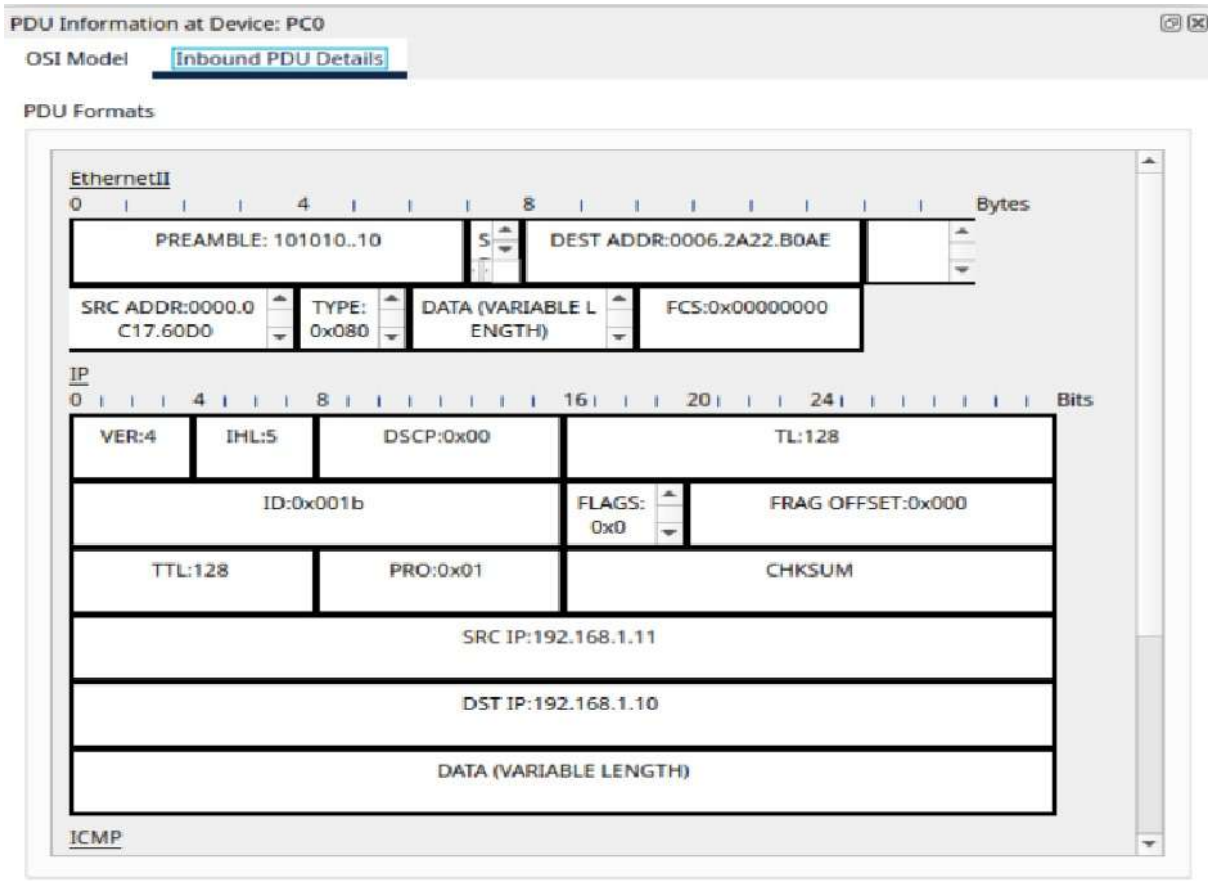


3) MAC Address Table of the Switch:

```
Switch Ports Model              SW Version            SW Image
------ ----- -----              ----------            ----------
*    1 26    WS-C2960-24TT-L    15.0(2)SE4            C2960-LANBASEK9-M

Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE4, RELEASE SOFTWARE
(fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Wed 26-Jun-13 02:49 by mnguyen


Press RETURN to get started!


%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up


Switch>show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0000.0c17.60d0    DYNAMIC     Fa0/2
   1    0006.2a22.b0ae    DYNAMIC     Fa0/1
```

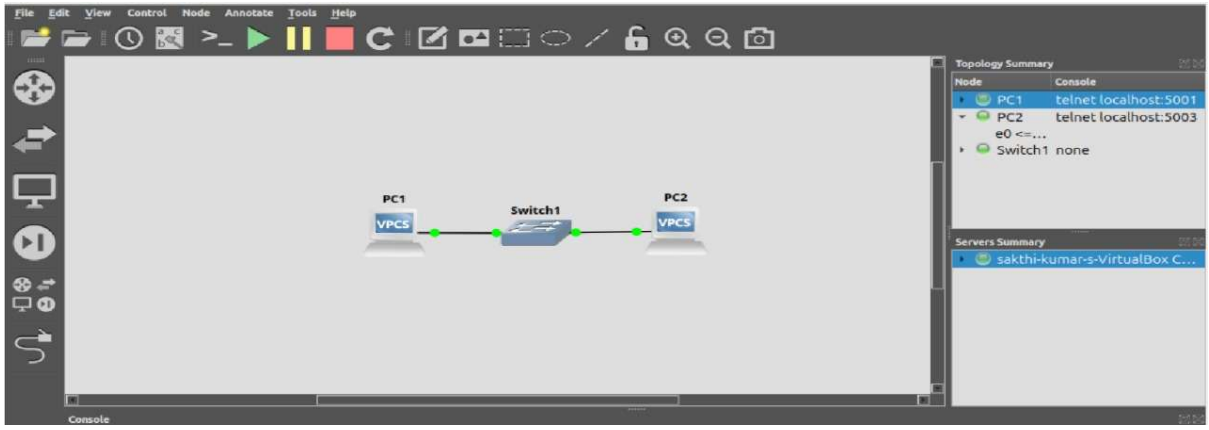
4)Frame Analysis





Using GNS3:

1)Network Setup:

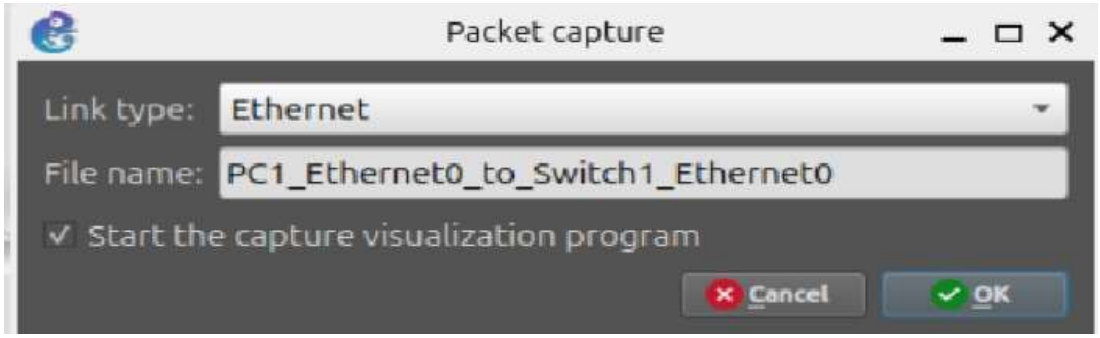


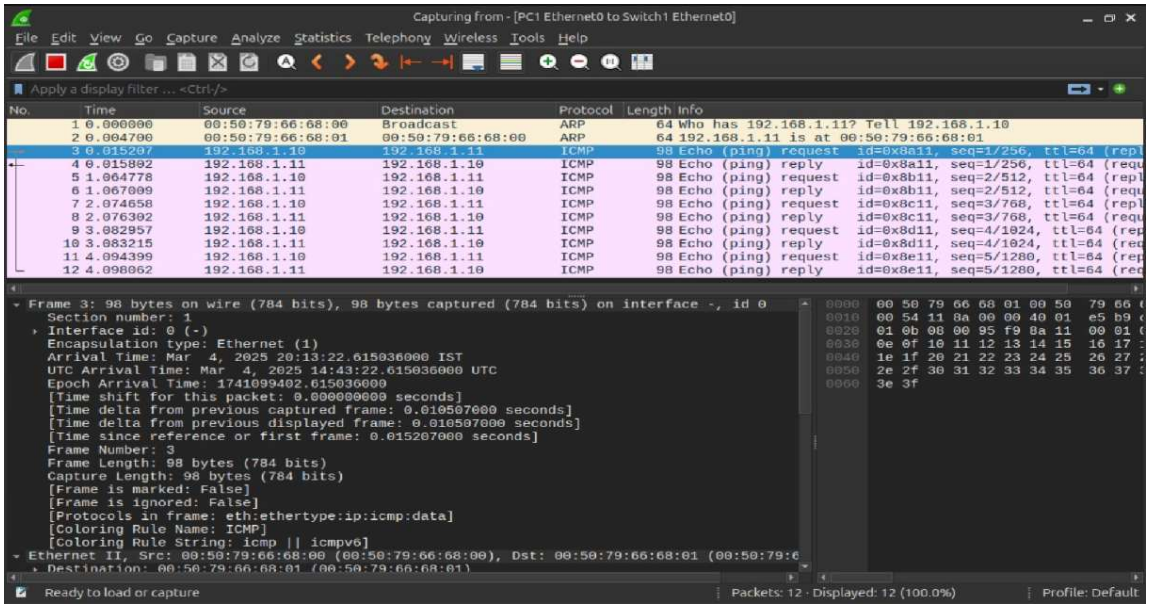
2) IP Setup and Ping Connection Check:

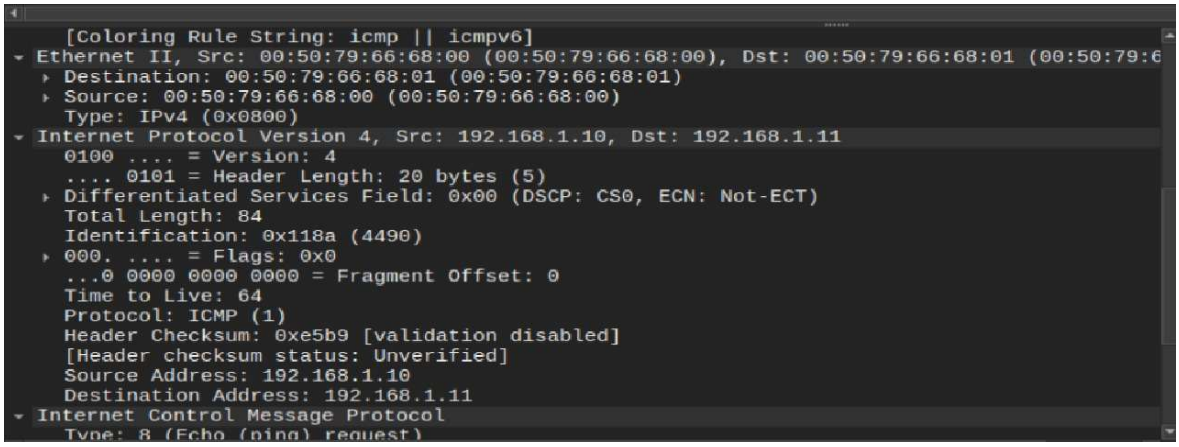
```
PC2> ip 192.168.1.11/24 192.168.1.1
Checking for duplicate address...
PC2 : 192.168.1.11 255.255.255.0 gateway 192.168.1.1

PC2> show ip

NAME        : PC2[1]
IP/MASK     : 192.168.1.11/24
GATEWAY     : 192.168.1.1
DNS         :
MAC         : 00:50:79:66:68:01
LPORT       : 10006
RHOST:PORT  : 127.0.0.1:10007
MTU         : 1500
```

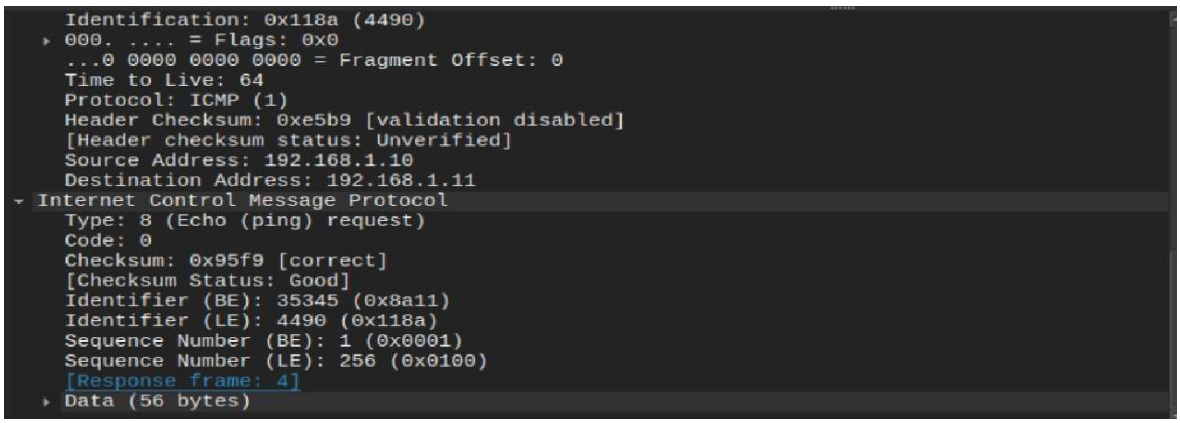
```
PC1> ip 192.168.1.10/24 192.168.1.1
Checking for duplicate address...
PC1 : 192.168.1.10 255.255.255.0 gateway 192.168.1.1

PC1> show ip

NAME        : PC1[1]
IP/MASK     : 192.168.1.10/24
GATEWAY     : 192.168.1.1
DNS         :
MAC         : 00:50:79:66:68:00
LPORT       : 10004
RHOST:PORT  : 127.0.0.1:10005
MTU         : 1500

PC1> ping 192.168.1.11

84 bytes from 192.168.1.11 icmp_seq=1 ttl=64 time=1.576 ms
84 bytes from 192.168.1.11 icmp_seq=2 ttl=64 time=6.335 ms
84 bytes from 192.168.1.11 icmp_seq=3 ttl=64 time=3.897 ms
84 bytes from 192.168.1.11 icmp_seq=4 ttl=64 time=4.190 ms
84 bytes from 192.168.1.11 icmp_seq=5 ttl=64 time=3.671 ms

PC1>
```

3) Packet Capture and Frame Analysis:




Capturing from - [PC1 Ethernet0 to Switch1 Ethernet0]
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 00:50:79:66:68:00 Broadcast ARP 64 Who has 192.168.1.11? Tell 192.168.1.10
2 0.004700 00:50:79:66:68:01 00:50:79:66:68:00 ARP 64 192.168.1.11 is at 00:50:79:66:68:01
3 0.015207 192.168.1.10 192.168.1.11 ICMP 98 Echo (ping) request id=0x8a11, seq=1/256, ttl=64
4 0.015802 192.168.1.11 192.168.1.10 ICMP 98 Echo (ping) reply id=0x8a11, seq=1/256, ttl=64
5 1.064778 192.168.1.11 192.168.1.10 ICMP 98 Echo (ping) request id=0x8b11, seq=2/512, ttl=64
6 1.067009 192.168.1.11 192.168.1.10 ICMP 98 Echo (ping) reply id=0x8b11, seq=2/512, ttl=64
7 2.074658 192.168.1.10 192.168.1.11 ICMP 98 Echo (ping) request id=0x8c11, seq=3/768, ttl=64
8 2.076392 192.168.1.11 192.168.1.10 ICMP 98 Echo (ping) reply id=0x8c11, seq=3/768, ttl=64
9 3.082957 192.168.1.10 192.168.1.11 ICMP 98 Echo (ping) request id=0x8d11, seq=4/1024, ttl=64
10 3.083215 192.168.1.11 192.168.1.10 ICMP 98 Echo (ping) reply id=0x8d11, seq=4/1024, ttl=64
11 4.094399 192.168.1.10 192.168.1.11 ICMP 98 Echo (ping) request id=0x8e11, seq=5/1280, ttl=64
12 4.098062 192.168.1.11 192.168.1.10 ICMP 98 Echo (ping) reply id=0x8e11, seq=5/1280, ttl=64
Frame 3: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface -, id 0
Section number: 1
Interface id: 0 (-)
Encapsulation type: Ethernet (1)
Arrival Time: Mar 4, 2025 20:13:22.615036000 IST
UTC Arrival Time: Mar 4, 2025 14:43:22.615036000 UTC
Epoch Arrival Time: 1741099402.615036000
[Time shift for this packet: 0.000000000 seconds]
[Time delta from previous captured frame: 0.010507000 seconds]
[Time delta from previous displayed frame: 0.010507000 seconds]
[Time since reference or first frame: 0.015207000 seconds]
Frame Number: 3
Frame Length: 98 bytes (784 bits)
Capture Length: 98 bytes (784 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:icmp:data]
[Coloring Rule Name: ICMP]
[Coloring Rule String: icmp || icmpv6]
Ethernet II, Src: 00:50:79:66:68:00 (00:50:79:66:68:00), Dst: 00:50:79:66:68:01 (00:50:79:6
Destination: 00:50:79:66:68:01 (00:50:79:66:68:01)
0000 00 50 79 66 68 01 00 50 79 66
0010 00 54 11 8a 00 00 40 01 e5 b9
0020 01 0b 08 00 95 f9 8a 11 00 01
0030 0e 0f 10 11 12 13 14 15 16 17
0040 1e 1f 20 21 22 23 24 25 26 27
0050 2e 2f 30 31 32 33 34 35 36 37
0060 3e 3f
Ready to load or capture
Packets: 12 · Displayed: 12 (100.0%)
Profile: Default


[Coloring Rule String: icmp || icmpv6]
Ethernet II, Src: 00:50:79:66:68:00 (00:50:79:66:68:00), Dst: 00:50:79:66:68:01 (00:50:79:6
Destination: 00:50:79:66:68:01 (00:50:79:66:68:01)
Source: 00:50:79:66:68:00 (00:50:79:66:68:00)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.1.10, Dst: 192.168.1.11
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 84
Identification: 0x118a (4490)
000. .... = Flags: 0x0
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: ICMP (1)
Header Checksum: 0xe5b9 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.10
Destination Address: 192.168.1.11
Internet Control Message Protocol
Type: 8 (Echo (ping) request)


Identification: 0x118a (4490)
000. .... = Flags: 0x0
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: ICMP (1)
Header Checksum: 0xe5b9 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.1.10
Destination Address: 192.168.1.11
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x95f9 [correct]
[Checksum Status: Good]
Identifier (BE): 35345 (0x8a11)
Identifier (LE): 4490 (0x118a)
Sequence Number (BE): 1 (0x0001)
Sequence Number (LE): 256 (0x0100)
[Response frame: 4]
Data (56 bytes)