**PUNE INSTITUTE OF COMPUTER TECHNOLOGY, PUNE**

**ACADEMIC YEAR 2024-25**

**DEPARTMENT OF COMPUTER ENGINEERING**

**CNSL ASSIGNMENT NO 1**

**NAME : MISBAH IQBAL BAGWAN ROLL NO : 31455**

**BATCH : M4 CLASS: TE-IV**

**PROBLEM STATEMENT:** Setup Wired LAN using Layer 2 switch, It includes preparation of cable, testing of cable using line tester, configuration machine using IP addresses testing using PING utility and demonstrating the PING packets captured traces using Wireshark Packet Analyser Tool

**REQUIREMENT :**

Crimping tool, RJ45 connectors, CAT5 UTP Cable, D-Link Line Tester, Wireshark Protocol Analyzer, Layer 2 switch, Layer 3 Switch

**COURSE OBJECTIVES:**

1.To understand the fundamental concept of networking standards, protocols, and technologies

**COURSE OUTCOMES:**

1.Summarise fundamental concept of Computer Network, Architecture, protocols and technologies

**Theory:**

**1.Computer Network:**

The term Computer Network refers to a collection of autonomous computers interconnected by a single technology. Two computers are said to be interconnected if they can exchange information. The connection can be established with the help of copper wire, Fiber optics, microwaves, infrared, and even communication satellites can be used.

**2.Classification Of Network**

1. Based On Network Size/Scale:

LAN, WAN, CAN, MAN, PAN, DAN

1. Based On Transmission Media:

UTP, Coaxial Cables, Fiber Optic Cables

1. Based On Management Method:

Peer-To-Peer, Client-Server

1. Based On Connectivity:

Bus, Star, Mesh, Ring, Tree, Hybrid

**3.Difference Between Cables**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Feature** | **Coaxial Cable** | **UTP -Unshielded Twisted Pair** | **STP -Shielded Twisted Pair** | **Fiber Optic Cable** |
| **Construction** | Two concentric conductors, black plastic jacket | Two insulated conductors twisted in spiral shape | Metal foil , braided Mesh included to cover each pair of twisted insulating conductors | Inner glass core surrounded by glass cladding and protective |
| **Shielding** | Yes ,plastic black jacket | No shielding | Yes | Protective cover |
| **Noise and**  **Electro-magnetic**  **Interference** | Moderate | High  (due to no shielding) | Low  (due to shielding) | No affect |
| **Bandwidth** | Large Bandwidth | Low to moderate | Low to moderate | Up to 100 Gbps or more |
| **Distance** | Up to 500 meters | Up to 100 meters | Up to 100 meters | Up to several kilometres |
| **Installation** | Moderate | Easy | complex than UTP due to shielding | More difficult, requires careful handling |
| **Cost** | Costlier than twisted pair but cheaper than fiber optic ones | Low | Higher than UTP | High |
| **Signal Degradation** | Moderate | Moderate | Lower than UTP | Very low |
| **Application** | Television,  Analog and digital telephone, traditional Ethernet | LAN, analog -digital telephony | Point to point and point to multipoint communications | In LANs ,Telephone System |

**4.LAN,WAN,MAN DIFFERENCE**

|  |  |  |  |
| --- | --- | --- | --- |
| **Parameters** | **LAN** | **MAN** | **WAN** |
| **Full Form** | Local Area Network | Metropolitan Area Network | Wide Area Network |
| **Design and Maintenance** | easy to design and maintain | Complex ,needs planning | Complex than LAN and MAN ,requires more resources and planning |
| **Speed** | Transmission > 10GBPS | Moderate to high (up to 1 Gbps) | Varies (up to 200 Gbps) |
| **Propagation Delay** | Short | Medium time | Takes Longer time |
| **Fault Tolerance** | Common-redundancy , More | depends on setup-medium | common-redundancy , will vary |
| **Congestion** | Since LAN is most likely in private /small setup ,congestion is low | More congestion than LAN, since users and devices are more than LAN | High congestion as compared to LAN ,MAN due to more users and devices |
| **Range** | Covers small areas like an office, small campus ,building | Can cover a city, or large campus , small-medium societies | Can cover countries and continent |
| **Cost** | Low | Medium to high | High |
| **Equipment needed** | Network Interface Card ,Cables like TP ,coaxial Switches, routers, | switches, fiber optic cables, switches | PSTN satellites, routers l, fiber optic cables |

**5.IP ADRESS FORMATS**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CLASS** | **RANGE** | **SUBNET MASK** | **Net id** | **host id** |
| **CLASS A** | **1.0.0.0 to 127.255.255.255** | **255.0.0.0** | **8 bits** | **Last 24 bits** |
| **CLASS B** | **128.0.0.0 to**  **191.255.255.255** | **255.255.0.0** | **First 16 bits** | **Last 16 bits** |
| **CLASS C** | **192.0.0.0 to**  **223.255.255.255** | **255.255.255.0** | **First 8 bits** | **Last 8 bits** |
| **CLASS D** | **224.0.0.0 to**  **239.255.255.255** | **Reserved for multicasting** | **-** | **-** |
| **CLASS E** | **240.0.0.0 to**  **254.255.255.255** | **Reserved for future use** | **-** | **-** |

**6.POPULAR SNIFFING TOOLS:**

Network sniffing tools, also known as packet sniffers, are software applications or hardware devices used to monitor, capture, and analyse network traffic

 **OmniPeek**: A comprehensive network analyzer and packet sniffer for real-time network monitoring and troubleshooting.

 **EtterCap**: A robust tool for network protocol analysis and security auditing, supporting man-in-the-middle attacks.

 **tcpdump**: A powerful command-line packet analyzer for capturing and inspecting network traffic on Unix-like systems.

 **WinDump**: The Windows version of tcpdump, providing similar packet capture and analysis capabilities for Windows.

 **Dsniff**: A suite of tools for network auditing and penetration testing, focusing on sniffing passwords and other sensitive data.

 **EtherApe**: A graphical network traffic viewer for Unix systems, displaying network activity in real-time with node and link visualizations.

 **MSN Sniffer**: A tool specifically designed to capture and decode MSN Messenger chat messages.

 **BetterCap**: An advanced network monitoring and attack tool with capabilities for MITM attacks, network scanning, and protocol manipulation.

 **Next Gen**: Often referring to advanced or next-generation network security tools that provide enhanced features for traffic analysis and threat detection.

 **NetWitness**: A comprehensive security platform offering deep packet inspection and real-time network forensics.

 **libpcap**: A portable C/C++ library for network traffic capture, providing the underlying packet capture and filtering capabilities for many network tools.

**7.What Is Wireshark?**

Wireshark is a network packet analyser. A network packet analyser presents captured packet data in as much detail as possible.

Wireshark is available for free and is open source

Reasons people use Wireshark:

* Network administrators use it to *troubleshoot network problems*
* Network security engineers use it to *examine security problems*
* QA engineers use it to *verify network applications*
* Developers use it to *debug protocol implementations*
* People use it to *learn network protocol* internals

Wireshark can also be helpful in many other situations.

**8.Wireshark** **Features**

The following are some of the many features Wireshark provides:

* Available for *UNIX* and *Windows*.
* *Capture* live packet data from a network interface.
* *Open* files containing packet data captured with tcpdump/WinDump, Wireshark, and many other packet capture programs.
* *Import* packets from text files containing hex dumps of packet data.
* Display packets with *very detailed protocol information*.
* *Save* packet data captured.
* *Export* some or all packets in a number of capture file formats.
* *Filter packets* on many criteria.
* *Search* for packets on many criteria.
* *Colorize* packet display based on filters.
* Create various *statistics*.

**9.Straight Through Cable And Crossover Cable**

*STRAIGHT THROUGH CABLE –* for dissimilar devices

1. A straight through cable is a type of twisted pair cable that is used in local area networks to connect a computer to a network hub such as a router.
2. On a straight through cable, the wired pins match. Straight through cable use one wiring standard: both ends use T568A wiring standard or both ends use T568B wiring standard.

1\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_1

2\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2

3\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_3

4\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_4

5\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_5

6\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_6

7\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_7

8\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_8

3

4

5

6

7

8

**Polarities (Straight-through):**

**Pin Configuration**

* **End 1 (Pins 1-8)**:
  1. White/Orange
  2. Orange
  3. White/Green
  4. Blue
  5. White/Blue
  6. Green
  7. White/Brown
  8. Brown
* **End 2 (Pins 1-8)**:
  1. White/Orange
  2. Orange
  3. White/Green
  4. Blue
  5. White/Blue
  6. Green
  7. White/Brown
  8. Brown

*CROSSOVER CABLE –* for similar devices

1. A crossover Ethernet cable is a type of Ethernet cable used to connect computing devices together directly.
2. Unlike straight through cable, the RJ45 crossover cable uses two different wiring standards: one end uses the T568A wiring standard, and the other end uses the T568B wiring standard.
3. The internal wiring of Ethernet crossover cables reverses the transmit and receive signals.
4. e.g. two computers (via network interface controller) or two switches to each other.

1 1

2 2

3 3

4\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_4

5\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_5

6 6

7\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_7

8\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_8

3

4

5

6

7

8

**Polarities (Crossover):**

**Pin Configuration (TIA/EIA-568-B to TIA/EIA-568-A):**

* **End 1 (Pins 1-8, TIA/EIA-568-B standard)**:
  1. White/Orange
  2. Orange
  3. White/Green
  4. Blue
  5. White/Blue
  6. Green
  7. White/Brown
  8. Brown
* **End 2 (Pins 1-8, TIA/EIA-568-A standard)**:
  1. White/Green
  2. Green
  3. White/Orange
  4. Blue
  5. White/Blue
  6. Orange
  7. White/Brown
  8. Brown

**10. Difference Between Various Network Devices**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Feature** | **Hub** | **Bridge** | **Switch** | **Router** |
| **Configuration required** | No | No | Layer 2 switch: No  Layer 3 switch: Yes | Yes |
| **Works up to which**  **OSI Layer** | Hub works on  Physical Layer (Layer 1) | Bridge works up to  Data Link Layer 2 and Layer 1 | Switch works up to  Data Link Layer 2 and Layer 1 | Router works up to  Network Layer, layer 2 and layer 1 |
| **Plug and Play** | Yes | Yes | Yes | No |
| **Traffic Isolation** | No | Yes | Yes | Yes |
| **Cut-through** | yes | no | Yes | No |
| **Optimal Routing** | No | No | No | Yes |
| **Function** | Concentrator,  Broadcasts data to all devices | Converts network  Filters traffic based on MAC addresses | Filters traffic based on MAC addresses | Routes data based on IP addresses |

**11.OSI (Open system Interconnections) Model**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Layer** | **Devices** | **PDU** | **Protocols** | **Address** | **Services** | **Mnemonic** |
| Application | Gateways | Data | HTTP, FTP, SMTP,DNS  TELNET | None | Network process to application | All |
| Presentation | Gateways | Data | SSL, TLS,MIME | None | Data translation, encryption/decryption | People |
| Session | Gateways | Data | NetBIOS, PPTP | Session ID | Dialog control,  Dialog separation,  synchronization | Seem |
| Transport | Gateways | Segments | TCP, UDP,RTP | Port Number | End-to-end ,host to host delivery ,congestion control | To |
| Network | Routers | Packets | IP, ICMP,  RIP  ,OSPF,BGP,  IGMP | IP Address | Routing and forwarding, logical addressing | Need |
| Data Link | Switches, Bridges | Frames | Ethernet, PPP | MAC Address | Organise bits into frame ,provide hop to hop delivery, error detection and correction | Data |
| Physical | Hubs, Repeaters | Bits | Ethernet, DSL | None | Transmit bits over a medium | Processing |

**12.TCP/IP Model**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Layer** | **Mnemonic** | **Devices** | **PDU** | **Protocols** | **Address** | **Services** |
| Application   * Application   layer   * Presentation Layer * Session Layer | All | Pcs-Phones,  Servers, Web Browsers  --------------  OpenSSL,  CODECS  --------------  Firewall , RPC,SSH  Gateways | Data ,Files | HTTP,HTTPS FTP, SMTP,TELNET, IMAP | **URL** | Network process to application,  Interface  **---------------**  Formatting,  Encryption ,  Compression  ----------------  Authentication  Authorisation |
| Transport Layer   * Transport Layer | those | Firewall,  Gateways | Segments  /Datagram | TCP, UDP,RTP,  SCTP | Port Number | End-to-end connections, host to host delivery ,flow control, error recovery |
| Network Layer   * Network Layer | New | Routers, Layer 3 Switch ,Brouter  Gateways | packets | IPv4,IPv6 ICMP,IGMP,  RIP,BGP | IP Address | Routing, Selecting best path logical addressing |
| Network Access Layer   * Data Link Layer * Physical Layer | Internet | |  | | --- | | Switches, Bridges, Hubs, Access Points, |   Cables, Modems,  Repeaters,  Gateways | Frames/bits | Ethernet,WLAN,  HDLC PPP  --------------------  CAT5 ,RJ-45, Ethernet | MAC  Address | Organise bits into frame ,provide hop to hop delivery, error detection and correction |

**13.How many links required to set up network with following topologies:**

|  |  |
| --- | --- |
| **Topology** | **Number of Links** |
| Ring | n |
| Bus | n+1 |
| Mesh | n(n−1)/2​ |
| Star | n |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Aspects** | **Bus** | **Star** | **Mesh** | **Ring** |
| **Alternate names** | Linear ,multipoint,  horizontal | **-** | **-** | **-** |
| **Maintenance** | simple | easy | complex | moderate |
| **Point of Failure** | Yes ,Main bus cable | Single point of failure | **-** | Any node |
| **Costing** | low | More cabling, higher cost | high | expensive |
| **Advantages** | Easy to implement and extend, requires less cable | Easy to install and configure, individual node failures do not affect the network | Robust and reliable, high fault tolerance, simultaneous data transmission | High-speed data transfer, no data collisions due to token passing |
| **Disadvantages** | Troubleshooting is difficult, limited cable length, prone to data collisions | Central hub failure disrupts the entire network, more cabling required | Expensive, complex installation and configuration | Single node or cable failure disrupts the network, difficult to add/remove devices |

**14.PARAGRAPH ABOUT PING -NO NET ,**

**BELOW PARAGRAPH USING MAN -PING ON LINUX TERMINAL**

NAME

ping - send ICMP ECHO\_REQUEST to network hosts

SYNOPSIS

ping [-aAbBdDfhLnOqrRUvV46] [-c count] [-F flowlabel] [-i interval] [-I interface] [-l preload]

[-m mark] [-M pmtudisc\_option] [-N nodeinfo\_option] [-w deadline] [-W timeout] [-p pattern] [-Q

tos] [-s packetsize] [-S sndbuf] [-t ttl] [-T timestamp option] [hop ...] destination

DESCRIPTION

ping uses the ICMP protocol's mandatory ECHO\_REQUEST datagram to elicit an ICMP ECHO\_RESPONSE

from a host or gateway. ECHO\_REQUEST datagrams (``pings'') have an IP and ICMP header, followed by a struct timeval and then an arbitrary number of ``pad'' bytes used to fill out the

packet.

ping works with both IPv4 and IPv6. Using only one of them explicitly can be enforced by speci‐

fying -4 or -6.

ping can also send IPv6 Node Information Queries (RFC4620). Intermediate hops may not be

allowed, because IPv6 source routing was deprecated (RFC5095).

OPTIONS

-4 Use IPv4 only.

-6 Use IPv6 only.

-a Audible ping.

-b Allow pinging a broadcast address.

-B Do not allow ping to change source address of probes. The address is bound to one selected when ping starts.

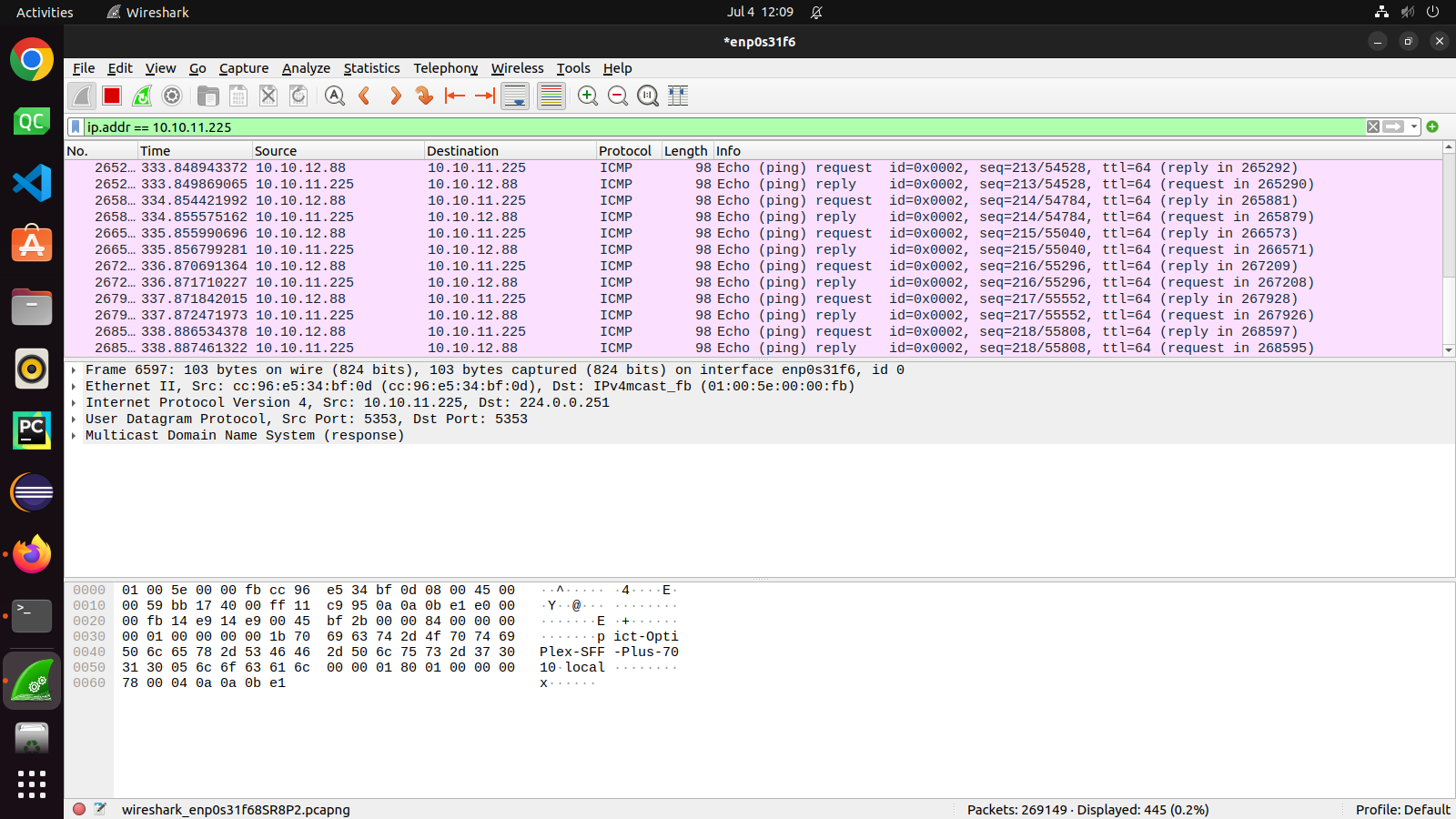
PING is used to check if a specific device is reachable over the network and how long it takes to communicate

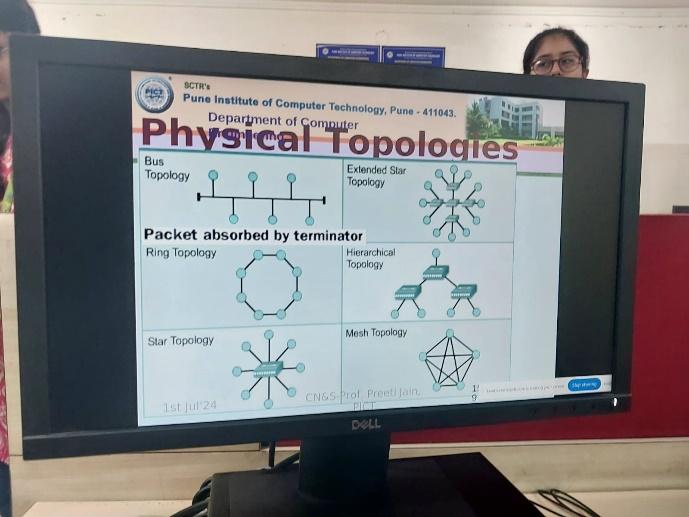
ICMP Echo Request packet is sent to that device

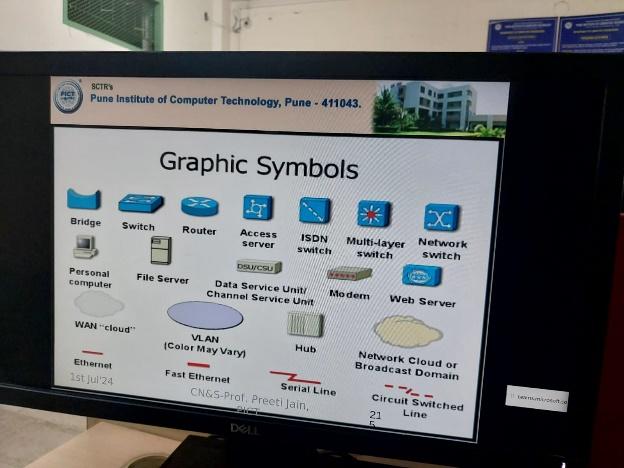
And if target is reachable and functioning It will respond with ICMP Echo Response Packet

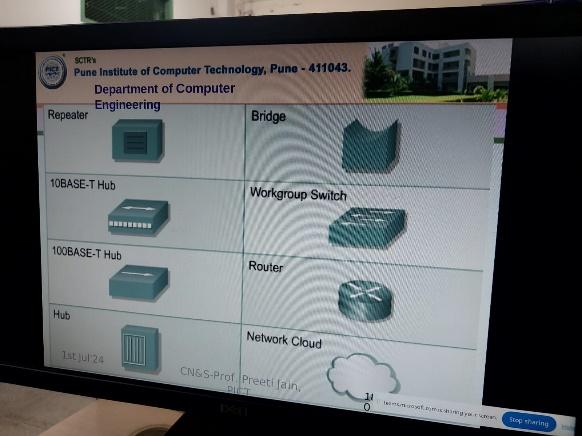
RTT(Round Trip Time):Time it takes for Echo request to go to the target and Echo response to come back is measured as RTT

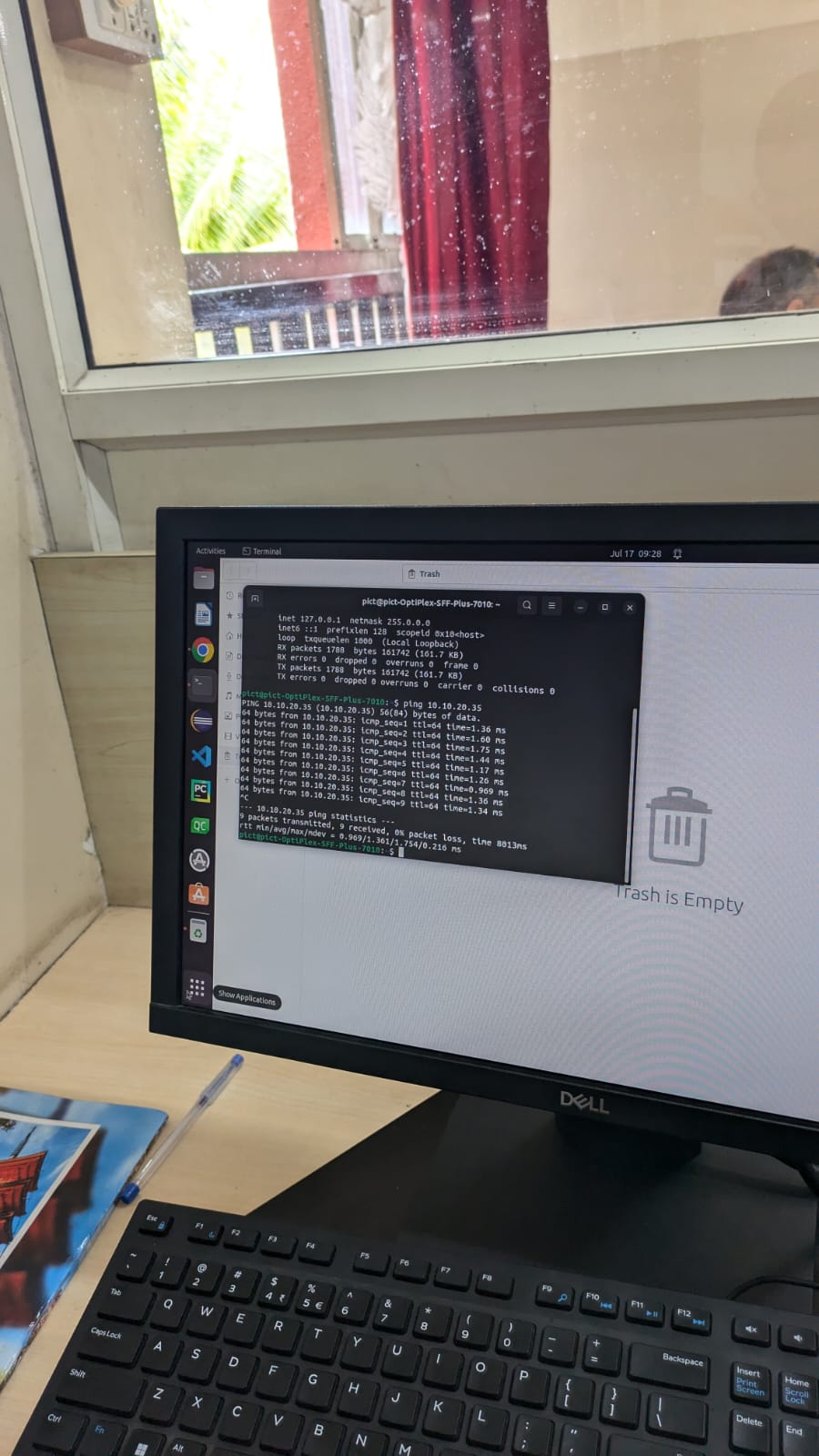
*WireShark :*

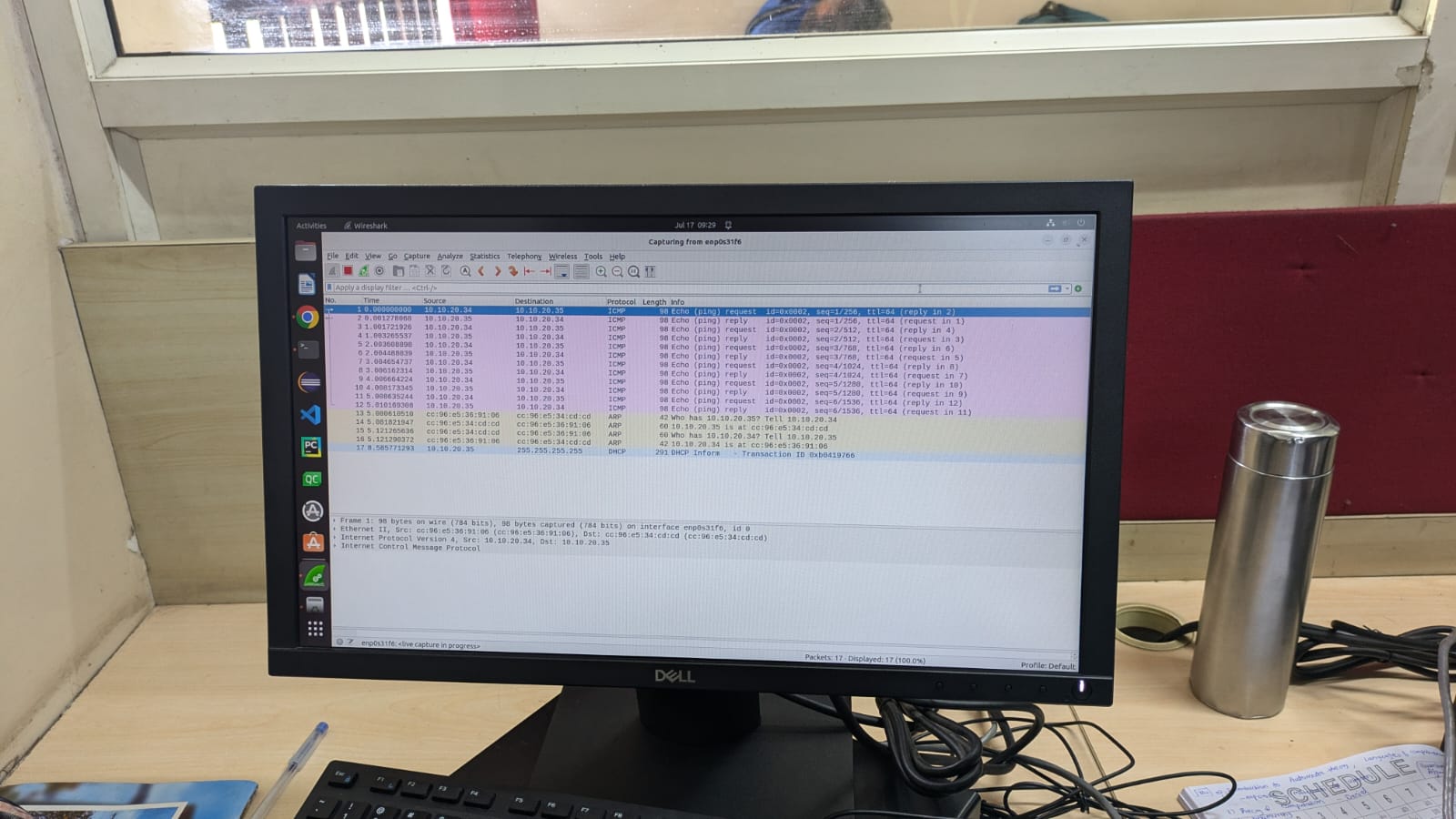
******





****

****

****

****

**PROBLEMS ENCOUNTERED(TROUBLE SHOOTING):**

1)We were assigning a different subnet mask to different class I.e. we were assigning class C subnet mask (255.255.255.0) to class A address of 10.10.10.8

we solved it by assigning correct subnet mask i.e. 255.0.0.0

2)While crimping cable was damaged ,so it was replaced with new one

**CONCLUSION(OUR TAKEAWAY):**

I learnt about wired networks , topologies .I was able to change IP Address and assign subnet mask accordingly .I understood arrangement of coloured wires to TIA/EIA 568A standards and their crimping.

While pinging from terminal and in Wireshark , I was able to understand flow of ICMP Echo request and response packets