Pune Vidyarthi Griha's
COLLEGE OF ENGINEERING, TECHNOLOGY & MANAGEMENT, PUNE 9.

Excellence in Engineering Education

Problem Definition:

Setup a 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 Analyzer Tool.

Prerequisite:

a) IP Address
b) OSI & TCP/IP Model
c) Networking Devices

Objectives:

To set up a wired Local Area Network (LAN) using a Layer 2 switch, configure IP addresses, test network connectivity using the PING utility, and analyze network traffic using Wireshark.

New Concepts:

- Wireshark

Theory:

What is a LAN (Local Area Network)?

A Local Area Network (LAN) is a network that connects computers and devices within a limited area such as a home, school, or office building. Devices are typically connected using Ethernet cables or Wi-Fi and can share files, printers, and access to the internet.

What is a Layer 2 Switch?

A Layer 2 switch operates at the Data Link Layer (Layer 2) of the OSI model. It forwards data based on MAC addresses and is used to segment a LAN into separate collision domains, improving performance and security.

Features of Layer 2 Switch:

- Uses MAC address table for forwarding
- No IP configuration required for basic operation
- Supports full duplex communication
- Reduces collisions and increases network speed

What is the PING Utility?

PING (Packet Internet Groper) is a command-line utility used to test the reachability of a

device on an IP network. It sends ICMP Echo Request packets and listens for Echo Reply.

- Helps diagnose connectivity issues
- Measures round-trip time
- Indicates packet loss or delay

Wireshark

Wireshark is a free and open-source packet analyzer used for network troubleshooting, analysis, software development, and education.

Features of Wireshark:

- Captures real-time network traffic.
- Supports deep inspection of hundreds of protocols.
- Allows filtering by protocol (e.g., icmp, tcp, udp).
- Displays details like Source/Destination IP, ports, MAC addresses, TTL, packet size.
- Offers graphical views of traffic patterns.

Materials Required

- Minimum 2 PCs/Laptops with Ethernet ports
- Layer 2 Switch (Unmanaged or Managed)
- RJ-45 connectors
- CAT5e or CAT6 Ethernet cable
- Cable crimping tool
- LAN cable tester (Line Tester)
- Wireshark Packet Analyzer installed on at least one PC
- Admin rights to configure network settings

1. **Cable Preparation**
   - Step 1: Cut the required length of CAT5e/CAT6 cable.

- Step 2: Strip about 1 inch of the cable sheath from both ends.
- Step 3: Arrange the internal wires using T568B standard:
- Step 4: Insert wires into the RJ-45 connector in the correct order.
- Step 5: Use the crimping tool to crimp the RJ-45 connector.

2. **Testing Cable with Line Tester**
   - Plug both ends of the cable into the Line Tester (one in the transmitter and one in the receiver).
   - Power ON the tester.
   - Observe the LED sequence:
   - **All 8 LEDs** should light up in order (1-8).
   - If out-of-order or missing, recheck and redo the cable crimping.

3. **IP Address Configuration on PCs**
   - Go to Control Panel → Network and Sharing Center → Change adapter settings
   - Right-click Ethernet → Properties
   - Select Internet Protocol Version 4 (TCP/IPv4) → Click Properties
   - Enter the following:
     a. PC1:
        i. IP Address: 192.168.1.1
        ii.   Subnet Mask: 255.255.255.0
     b. PC2:
        i. IP Address: 192.168.1.2
        ii.   Subnet Mask: 255.255.255.0
   - Click OK to apply.

4. **Physical Setup Using Layer 2 Switch**
   - Connect PC1 and PC2 to the **Layer 2 switch** using the tested Ethernet cables.
   - Power ON the switch and verify **link LEDs** on both ports are active.

5. **Connectivity Testing using PING**
   - On PC1:
     - Open Command Prompt
     - Run: ping 192.168.1.2
   - On **PC2**:
     - Run: ping 192.168.1.1

If you receive replies, the LAN is functioning properly.

6. **Packet Capture using Wireshark**

1. Open **Wireshark**.
2. Select the **Ethernet interface** and click **Start Capture**.
3. In Command Prompt, run the **ping** command again (as above).
4. Return to Wireshark and **stop capture** after a few seconds.
5. In the Wireshark interface:
   a. Filter using: icmp
   b. You'll see captured **ICMP Echo Request** and **Echo Reply** packets.
   c. Analyse fields like:
      i. Source & Destination IP
      ii. ICMP Type (8 = request, 0 = reply)
      iii. Packet size
      iv. Time difference